DIGITAL EVIDENCE: A CASE STUDY OF LEGISLATION IN PAKISTAN IN THE LIGHT OF OTHER JURISDICTIONS

A dissertation submitted in partial fulfillment of the requirements for the degree of PhD (Law)

Submitted by:

Mahboob Usman

Registration no:

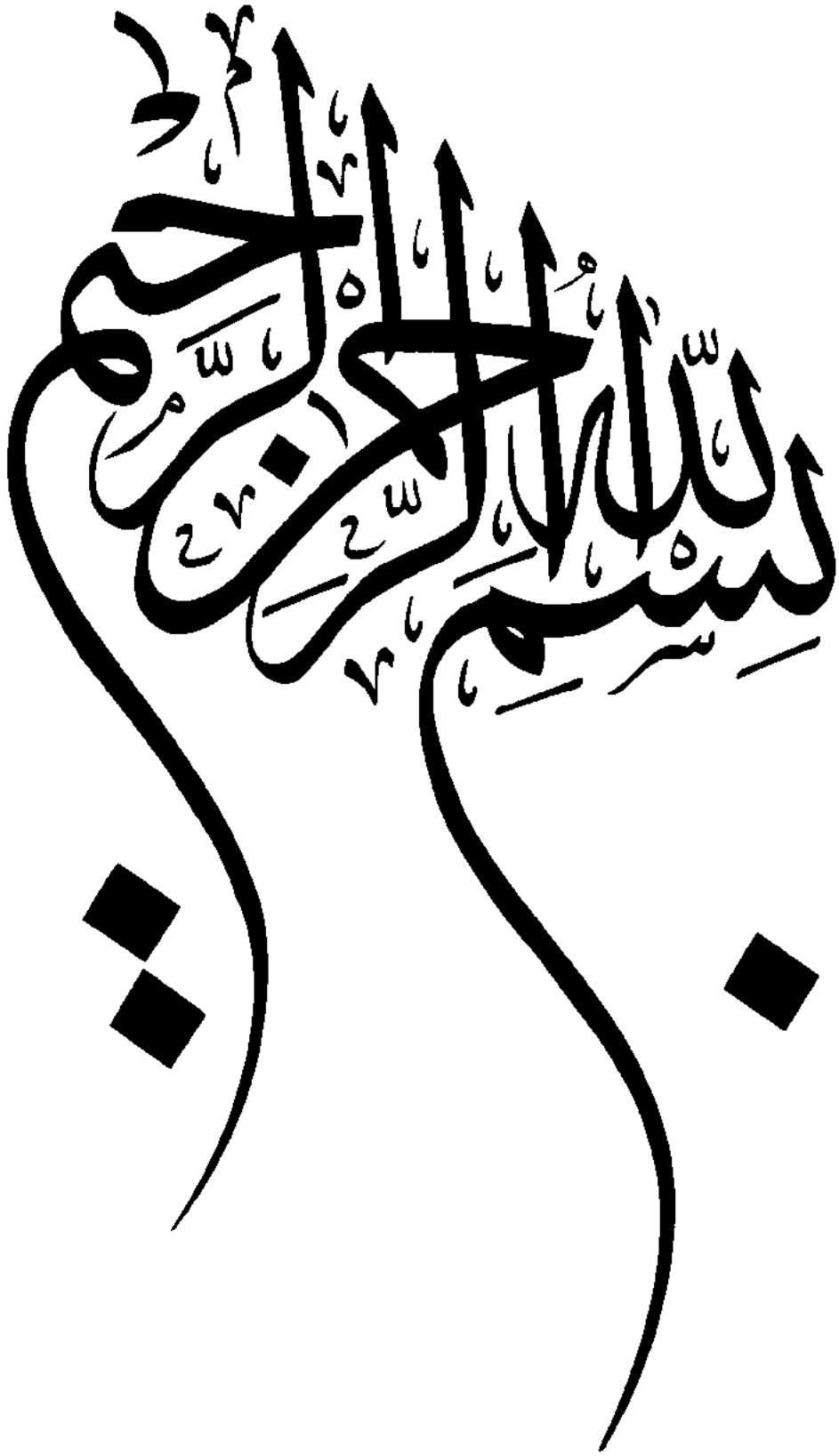
92-SF/PHDLAW/F16

Supervised by:

Dr. Muhammad Mushtaq Ahmad

Faculty of Shariah and Law

International Islamic University Islamabad


بسم الله الرحمن الرحيم

Dedicated to

My family

FACULTY OF SHARIAH & LAW
INTERNATIONAL ISLAMIC UNIVERSITY, ISLAMABAD

FINAL APPROVAL CERTIFICATE

It is certify that we have evaluated the thesis "**Digital Evidence: A Case Study of Legislation in Pakistan in the Light of Other Jurisdictions**" submitted by Mr. Mahboob Usman, Registration No.92-SF/PHDLAW/F16, in partial fulfillment of the requirements of the degree of Ph.D Law at the International Islamic University, Islamabad. The thesis fulfills the requirements in its core and quality for the award of the degree of Ph.D Law.

COMMITTEE

Supervisor

Dr. Muhammad Mushtaq Ahmad
Ex-Associate Professor, Deptt. of Law
FSL, IIU, Islamabad

External Examiner-1

Dr. Nadia Khadam
Assistant Professor, Deptt. of Law,
Fatima Jinnah Women University,
Rawalpindi

External Examiner-2

Dr. Muhammad Asif Khan
Associate Professor.
NUST University,
Islamabad

Internal Examiner

Prof. Dr. Muhammad Munir
Professor, Deptt. of Law,
FSL, IIU, Islamabad

DECLARATION

I, **Mahboob Usman,** hereby declare that this dissertation is original and has never been presented in any other institution. I, moreover, declare that any secondary information used in this dissertation has been duly acknowledged.

Student: Mahboob Usman

Signature: _____

Date: _____

Supervisor: Dr. Muhammad Mushtaq Ahmad, Associate Professor

Signature: _____

Date: _____

ACRONYMS

ACPO	Association of Chief Police Officers
ATM	Automated Teller Machine
AuC	Authentication Center
BSC	Base Station Controller
CALEA	Communications Assistance for Law Enforcement Act
CCTV	Closed-circuit television
CD	Compact Disc
PECO	Prevention of Electronic Crimes Ordinance
CDMA	Code-Division Multiple Access
CDR	Call Detail Record
CLOUD Act	Clarifying Lawful Overseas Use of Data Act 2018
CoE	Council of Europe
CPC	Code of Civil Procedure, 1908
CrPC	Code of Criminal Procedure, 1898
DNS	Domain Name Server
DVD	Digital Optical Disc
ESI	Electronically Stored Information
ESN	Electronic Serial Number
ETO	Electronic Transactions Ordinance, 2002
FAT	File Allocation Table
FBI	Federal Bureau of Investigation
FDMA	Frequency Division Multiple Access
FIA	Federal Investigation Agency
FRE	Federal Rules of Evidence

GPS	Global Positioning System
GSM	Global System for Mobile Communications
HD	hard disk drive
HLR	Home Location Register
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
ICC-ID	Integrated Circuit Card Identifier
ICT	Information Communication Technology
IFTA	Investigation for Fair Trial Act, 2013
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IOCE	International Organization of Computer Evidence
IP address	Internet Protocol address
ISPs	Internet Service Providers
IT	Information technology
LAN	Local Area Network
LEAs	Law Enforcement Agencies
LHC	Lahore High Court
MAC	Media Access Control
MIN	Mobile Identification Number
MSC	Mobile Switching Center
MTA	Message Transfer Agents
NIC	Network Interface Cards
NIJ	National Institute of Justice
NIST	National Institute of Standards and Technology

NSP	network service providers
NTFS	New Technology File System
OS	operating systems
PDA	Personal Digital Assistant
PECA	Prevention of Electronic Crimes Act, 2016
PIN	personal identification number
PUK	Personal Unlock Key
QSO	*Qanun-e-Shahadat* Order, 1984
SANs	Storage Area Networks
SD card	Secure Digital Cards
SHC	Sindh High Court
SIM	Subscriber Identity Module
SWGDE	Scientific Working Group on Digital Evidence
TCP	transmission control protocol
TDMA	Time Division Multiple Access
TLD	Top Level Domain
TMSI	Temporary Mobile Subscriber Identity
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USA	United States of America
USB	Universal Serial Bus
VLR	Visitor Location Register
VoIP	Voice over Internet Protocol
WAN	Wide Area Network

LIST OF CASES

United States v. Wiest, 596 F.3d 906 (8th Cir.2010).

United States v. Wood, No.08-CR-92A, 2009 WL 2157128 (W.D.N.Y. July 15, 2009).

United States vs. Miller, 771 F.2d 1219, (9th Cir. 1985).

United States vs. Simpson, 152 F.3d 1241 (10th Cir. 1998).

Wady v. Provident Life & Accident Ins. Co. of America, 216 F. Supp. 2d 1060 (C.D. Cal. 2002).

Watan Party v. Federation of Pakistan, PLD 2012 SC 292.

Williams v. Long, 2008 WL 4848362 (D. Md., November 7, 2008).

Williams v. Long, 585 F.Supp.2d 679 (D. Md. 2008).

Williams v. Sprint/United Management Co., 230 F.R.D. 640 (D.Kan. 2005).

Yasir Ayyaz v. the State, PLD 2019 Lahore 366.

Zakir Hussain v. The State, 2017 PCrLJ 757.

Zubulake v. UBS Warburg LLC, 217 F.R.D. 309 (S.D.N.Y. 2003).

Zubulake v. UBS Warburg LLC, 230 F.R.D. 290 (S.D.N.Y. 2003).

Zubulake v. UBS Warburg, 216 F.R.D. 280 (S.D.N.Y. 2003).

Zubulake v. UBS Warburg, 220 F.R.D. 212 (S.D.N.Y. 2003).

Zubulake v. UBS Warburg, 229 F.R.D. 422 (S.D.N.Y. 2004).

ACKNOWLEDGEMENT

All Praise be to Allah, the Sustainer of the worlds, the Merciful, the Compassionate! By whose grace and help this thesis has been completed. May His everlasting blessings and peace be upon Muhammad, the last of His Messengers!

I would like to extend my gratitude to my honorable teachers and mentors. I would have never been able to reach this milestone without their help and support, especially the support and guidance provided by Dr. Muhammad Mushtaq Ahmad, Associate Professor (Law), Department of Law, who has been a major source of inspiration for me regarding legal research and writing. I am highly obliged to him, as he kept guiding me before and during my thesis irrespective of his other engagements. Without his push I would have not been able to complete this dissertation within such a short period. I am also thankful to my teacher and mentor Professor Imran Ahsan Khan Nyazee, because of him, today, I am able to understand, think critically, shape my ideas and compile them into my PhD research.

In addition, I would also like to offer special gratitude to Dr. Attaulllah Khan Mahmood Wattoo, Assistant Professor (Law) who taught me and always encouraged me. I am also thankful to the university in general and the faculty of Shari'ah and Law in particular for providing me this environment of research and encouraging me to achieve academic excellence. In particular, I am thankful to Mr. Noman Shahid (Deputy Director), Raja Hamid, Mr. Muhammad Sharif, Mr. Safdar Khattak, and Mr. Muhmmad Ali for their extensive cooperation.

Special thanks go to Mr. Zeeshan Ashraf Qureshi (my close friend and PhD candidate in Malaysia), because of his push (rather he forced me to apply) I planned for admission in PhD. Thereafter, I must mention here the support of Mr. Sohail Khan for helping me in translation and formatting.

And finally, I must acknowledge the contribution of my friends who supported me in writing my thesis. I must mention here the support of Mudassar Ikram Ch, Muhmmad Yar Khan and Sabir Hussain (Advocates High Court) for providing me relevant judgements.

CONTENTS

THESIS STATEMENT

The rapid technological advancements occurring in our society through the digitalization of data and information are presenting new challenges to the investigators, making digital evidence difficult to detect, preserve and produce before the courts, therefore, strengthening the existing legislation on the subject, in the light of legislative measures in different countries is imperative for an effective law enforcement system.

ABSTRACT

In 2002, *Qanun-e-Shahadat* Order, 1984 (QSO) was amended through section 29 of the Electronic Transactions Ordinance (ETO) to recognize electronic documents in evidence. Instead of adhering, or understanding this section, the amendment brought in QSO was applied to all situations ignoring this fact that this particular amendment was meant for ETO only. Even otherwise, if these amendments are applied to every situation this does not cover many aspects of digital evidence which needs special consideration and proper mechanism to handle and deal with digital evidence. Digital evidence is not like paper based evidence which is totally different i.e. from identification to presentation in the court.

In this dissertation, all the necessary aspects of digital evidence including the definition of digital evidence, chain of custody, print out, evidence collection, preservation, storage, transportation, and digital evidence on windows and mobile phone has been thoroughly examined. Besides, the collection of evidence from the internet and network servers has also been examined. Almost, all the latest known device containing digital evidence have been discussed. In addition to this, the interpretation of digital evidence by the courts is also examined. Moreover, the digital evidence is usually presented through the expert, therefore, the role of expert witness is also discussed. Finally, on the basis of United States of America (USA) legislation and various judgments, some recommendation have given for legislatures, Law Enforcement Agencies (LEAs) and professionals.

This dissertation has concluded that the existing law of evidence is not sufficient to prosecute the criminals, therefore, a specialized law is a need of the hour to provide relief to the cybercrime victims. At the end, it is also suggested to start online courts for expeditious justice as envisaged in the Constitution of the Islamic Republic of Pakistan, 1973.

INTRODUCTION

The fast advancements in virtual world occurring in existing regime of information communication technology is presenting new challenges to the investigators, making digital evidence difficult to detect, preserve and produce before the courts, therefore, strengthening the existing legislation on the subject, in the light of legislative measures in different countries is imperative for an effective law enforcement system. In Pakistan, first ever legislation on electronic subject was "Electronic Transactions Ordinance, 2002,"[1] (ETO) which criminalized few offence known at the time. Whereas the basic purpose of the ETO was "to recognize and facilitate documents, records, information, communications and transactions in electronic form, and to provide for the accreditation of certification service providers."[2] This Ordinance also amended few provisions of the *Qanun-e-Shahadat* Order, 1984 (QSO). The provisions of this Ordinance were used to cover many aspects of cyber-crimes till 2016. Although, during the trial many of the criminals were acquitted due to non-applicability of the Ordinance, hence this Ordinance was not sufficient to cover many aspects of cyber-crimes particularly digital evidence.

With the beginning of new crimes, the legislature felt demand for legislation on new issues. Subsequently, President of the Islamic Republic of Pakistan promulgated "the Prevention of Electronic Crimes Ordinance, 2007,"[3] to criminalize many illegal acts of the regime. Similarly, the same Ordinance was again promulgated in 2008,[4] and in 2009; the last promulgation took place on 8th July 2009. These Ordinances were a stop gap arrangement, which borne no fruit for law enforcement agencies as well as for judiciary. Somehow, Prevention of Electronic Crimes Act, (PECA) 2016 strengthened the LEAs by extending International cooperation for investigation

[1] Electronic Transactions Ordinance, 2002 (LI of 2002).
[2] Ibid., Preamble.
[3] Ordinance No. LXXII OF 2007.
[4] Ordinance no. IX of 2008.

purposes,[5] which is a good step to enhance the powers of LEA. Henceforth, LEA will be able to collect evidence from other jurisdictions for investigation.

The world is full of digital devices and without them, society will probably collapse. Many devices "even the most innocuous device may contain information which is relevant in a criminal investigation."[6] Therefore, it is stated that "a criminal action of an individual cannot occur without leaving a mark,"[7] or evidence, which is useful for the investigator to trace out the criminal or offender. Thus, we can say that the evidence is the most important thing for investigation and prosecution. Evidence in "its purest form is information presented in testimony or in documents that is used to persuade the fact finder to decide the case for one side or the other."[8] Whereas the electronic evidence is the "information and data of investigative value that is stored on or transmitted by an electronic device."[9] Such evidence is "acquired when data or physical items are collected and stored for examination purposes."[10] Evidence[11] is defined in Pakistani legal system, however, electronic evidence is not defined anywhere in existing laws.

There are many stages in evidence from evidence collection to production before the court.[12] However, conventional evidence identification, collection, preservation and production

---

[5] S. 42 of PECA, 2016.

[6] Angus Marshall. Digital Forensics Digital Evidence in Criminal Investigation (Willey-Blackwell, 2008), ix.

[7] Richard Boddington. *Practical Digital Forensics* (Birmingham: Packet Publishing Ltd., 2016), 3.

[8] Albert J. Marcella and Doug Menendez. *Cyber Forensics A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes. 2nd ed.* (New York: Auerbach Publications, 2008), 11.

[9] Ibid.

[10] Ibid.

[11] QSO defines evidence as evidence includes;

"(i) all statements which the Court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry, such statements are called oral evidence, and

(ii) all documents produced for the inspection of the Court; such documents are called documentary evidence." Article 2 (C) of QSO.

[12] Chapter X of the QSO, 1984 provides the detail procedure for examination of witnesses. Chapter XL and XLI of the Code of Criminal Procedure, 1898 provides for the commissions for the examination of witnesses and special rules of evidence. Under CPC, 1908, the High Courts have been granted power to make rules for their respective provinces. Thus, for civil matters rules are framed under CPC to tackle evidence which are normally called

before the court is easy but in the case of digital evidence, it is difficult for the investigator to handle the situation, therefore, he has to make maximum efforts for all stages of the evidence. Preserving the crime scene is the primary objective of the investigator because "if the evidence is contaminated, lost, or simply not identified and overlooked, then all that follows may be of limited value to the investigators putting together the case evidence."[13] However, in digital evidence it is not a piece of cake for the investigator to preserve digital crime scene. There are many things involved in this procedure, as "evidence cannot be viewed in isolation and should be compared with other evidence, and corroborating evidence should be identified."[14]

The main issue with digital evidence is that, "it is actually just a collection of ones and zeros represented by magnetization, light pulses, radio signals or other means. This type of information is fragile and can be easily lost or changed."[15] Whereas

> protecting the integrity of evidence and maintaining a clear chain of custody is always important in a criminal case, but the nature of the evidence in a cybercrime case makes that job far more difficult. An investigator can contaminate the evidence simply by examining it, and sophisticated cybercriminals may set up their computers to automatically destroy the evidence when accessed by anyone other than themselves.[16]

In many situations, i.e. if the compromised system is not adequately secured than it will be very challenging to determine or prove an allegation against the culprit, as since someone else can hack into a system without the authorization of the lawful user. In many cases, mostly the criminals removes the logs to hide what actually happened, "so that there is no evidence to prove that a crime

---

Orders. Order, 11 (discovery and inspection), 13 (production, impounding and return of documents), 16 (summoning and attendance of witnesses), and 18 (examination of witnesses) are relevant for this study.

[13] Boddington. *Practical Digital Forensics*, 5.

[14] Ibid.

[15] http://www.techrepublic.com/blog/it-security/what-makes-cybercrime-laws-so-difficult-to-enforce/ (accessed on 5th July 2017).

[16] Ibid.

even occurred."[17]Although, the PECA has criminalized many cyber-crimes but it is far away to offer comprehensive mechanism for digital evidence collection, preservation and production of the same. So far, Pakistani legal system is lacking in proper legislation to deal with such type of issues. Therefore, it is important to work on this topic to bring existing legislation with conformity of international standards to enable the legislature in Pakistan to strengthen the investigator and LEA by legislating on the topic. The same has been discussed in this dissertation.

The following questions are framed to be discussed and examined in the light of Pakistani law of evidence:-

i. Whether the Pakistani legislation on law of evidence is keeping pace with advancement of Information Technology and it covers all aspects of the Information Communication Technology era?

ii. What are the issues and problems faced by the law enforcement personnel due to non-availability of proper legislation on the digital evidence?

iii. Whether existing legislation provides an effective mechanism for identification, collection, preservation, and production of digital evidence?

iv. Whether under the existing legal regime evidence collected through modern devices is sufficient to convict the criminal or decide the case or any corroborated evidence is required?

v. What is the significance of the chain of custody in relation to the preservation of digital evidence from its collection up to its tendering in legal proceedings?

[17] Ibid.

vi. What is the recovery of digital evidence through forensic imaging processes, (also known as dead recovery) and the acquisition of digital evidence through live recovery processes?

vii. What amendment is needed in the *Qanun-e-Shahadat* Order, 1984 for imposing a more rigorous requirement for the presumption of reliability and accuracy of computer-produced evidence?

viii. To what standard of authentication do judges hold digital forensic evidence compared to traditional physical forensic evidence?

ix. Whether the Judges and Lawyers in Pakistan have adequate exposure to the ICT enabling them to determine reliability, relevance, and veracity of digital Evidence?

x. What are the common issues which judges face when deciding on admissibility issues related to digital evidence?

xi. What amendments are needed in the Code of Criminal Procedure (CrPC), particularly regarding the testimony and report of IT or forensic expert, for regulating the digital evidence more reliable in court?

This dissertation highlight the importance of the digital evidence, particularly the digital evidence collection, preservation and production in the competent court. The dissertation is divided into 8 chapters and last chapter is about conclusion and recommendations.

Chapter one explorers the brief history of evidence and cyber laws in Pakistan. Thereafter, it also explores various definitions of digital evidence to provide a working definition for this study, which has also been critically examined. In addition, the important sources of digital evidence have been discussed.

Chapter two elaborates the identification, creation, and collection of digital evidence. In this respect different methods and approaches of digital evidence collection has been explained. While seizing digital evidence, the investigator can face many seizure issues and different errors can occur in this process, which has been highlighted in some detail. Besides, there are certain challenges and problems which are faced by the examiner, hence, to some extent, these have also been discussed along with forensic imaging.

Chapter three highlights the digital forensic, its phases, handling of digital evidence and authentication of digital evidence on computer, websites and email. Later on, challenges of authentication has also been highlighted.

Chapter four discuss various basic operations of computer, volatile data, storage media, importance of crime scene, crime scene investigation, electronic crime scene, handling digital crime scenes, possession and chain of custody. Later, in this chapter evidence preservation, transportation and storage has been examined.

Chapter five is about digital evidence on computers, wherein windows, file systems, hard drive, metadata, encryption and digital evidence as alibi, computer print outs are also discussed.

Chapter six is regarding digital evidence on mobile devices. In this chapter many aspects of mobile evidence has been discussed in particular, mobile operations, CDR, IMEI, SIM, cellular networks and their components. Besides, handling of mobile device is also examined as the process is little bit different from computer handling. In later part, GPS and Cloud systems have been examined as these are integral part of virtual world.

Chapter seven examines digital evidence on networks and the internet. In particular, IP address, ISP, social networking sites, websites and email evidence has been examined.

Chapter eight examines the production of evidence in courts. As digital evidence is presented through expert witness, thus, forensic education for experts, prosecution, lawyers and judges is also discussed in the light of judgements of various courts. At the end, it is examined that how judges access the digital evidence. Lastly, online courts and recording of evidence through video conferencing is discussed.

The last chapter, is about conclusion and recommendations.

The methodology of this research is based on multiple approaches of legal scholarship, including a comparative law approach and case laws of the Pakistani and United States Courts. Moreover, major portion of this research is based on library research that references are in the form of books, Statutes, Articles, Reports and decided cases of superior courts including foreign courts and tribunals. While reading other jurisdictions' legislation and cases main principles are taken and then applied to Pakistani legal system where there is any lacuna or ambiguity in contemporaneous legislation than recommendations are given to amend the law accordingly.

Chicago manual of style is used for citation purposes in this research.

CHAPTER ONE:

DIGITAL EVIDENCE: SOME BASIC ISSUES

1.1 INTRODUCTION

After the invention of computer, many problems are being face by the law enforcement agencies (LEAs) to prosecute the criminal involved in cybercrimes. This chapter explorers the brief history of digital evidence and cyber laws in Pakistan. Thereafter, it examines various definitions of digital evidence, provided by the scholars and institutions, to provide a working definition for this study. Besides, sources of digital evidence are not like other conventional evidence, therefore, the same have been discussed briefly to know the exact available sources of digital evidence.

1.2 A BRIEF OVERVIEW OF DIGITAL EVIDENCE

The fast growth of information technology[1] is creating many issues, among them, is a Cybercrime. It has almost affected everyone in the virtual world. Whilst people in Pakistan are not much conversant with information technology, notably they lag in technological advancement that leads to computer crimes and other associated problems. Digital evidence's many aspects are not covered under any Pakistani law particularly PECA, QSO, ETO or any other legislation, which weaken the judicial procedure and the law enforcement agencies. Consequently, the criminals are

[1] "*Information technology* is a contemporary term that describes the combination of *computer technology* (hardware and software) with *telecommunications technology* (data, image, and voice networks). Data and information are the central focus of an information system; this is the electronic evidence that proves or disproves the facts at issue in the litigation."

https://www.crl.edu/sites/default/files/d6/attachments/pages/Thomson-E-evidence-report.pdf (accessed: 30th November, 2019).

likely to be caught and prosecuted due to noavailabilty of proper legisaltion on handing of degital evidence and allied matters.

Whereas, any conventional evidence is, somehow, difficult to collect, in any criminal investigation or civil proceeding, but when that evidence is in digital form then "an investigator faces some extra complexities."[2] As compared to conventional evidence, digital evidence is easily lost, damaged, corrupted and erased. In fact, it is the basic responsibility of any investigator to show that the evidence is what he says it is, collected from the crime scene and since obtaining it, the same had not been altered or modified. Wacks has described this in a very beautiful manner:

> The emergence of information technology, to select only one obvious instance, poses enormous challenges to the law. Attempts legally to control the Internet, its operation or content, have been notoriously unsuccessful. Indeed, its very anarchy and resistance to regulation is, in the minds of many, its strength and attraction. But is cyberspace beyond regulation?[3]

The existing rules related to evidence have been developed over many centuries, and these rules were meant only for conventional documents. However, the digital evidence is totally different from the former. In Pakistan, first ever legislation on electronic subject was the "Electronic Transactions Ordinance, 2002,"[4] which criminalized certain crimes of the time, as the basic object of the ordinance was "to recognize and facilitate documents, records, information, communications and transactions in electronic form, and to provide for the accreditation of certification service providers."[5] Likewise, ETO also amended few provisions of the QSO. Although, during the trial many of these criminals were acquitted due to non-applicability of the ordinance on those situations as the same were not covered under ETO, hence, it can safely be

---

[2] John R Vacca, *Computer Forensics: Computer Crime Scene Investigation*. 2nd ed. (Massachusetts: Charles River Media, Inc., 2005), 217.

[3] Raymond Wacks, *Law A Very Short Introduction* (Oxford: Oxford University Press, 2008), 133.

[4] Electronic Transactions Ordinance, 2002 (LI of 2002).

[5] Ibid. Preamble.

concluded that ETO was not satisfactory to cover many aspects of cyber-crimes particularly digital evidence.

The rapid technological advancements occurring in our society through the digitalization of data and information are presenting new challenges to the investigators, making digital evidence difficult to detect, collect, preserve and produce before the courts, therefore, strengthening the existing legislation on the subject, in the light of legislative measures in different countries is imperative for an effective law enforcement system.

Evidence is defined as "separating the wheat from the chaff" though in conventional methods it is not difficult to identify and collect but in digital form it is very difficult to collect due to volatile nature. Digital evidence is defined as any "information and data of investigative value that is stored on or transmitted by an electronic device." Such evidence is acquired when data is collected for investigation.[6] The basic problem with digital evidence is that, after all, "it is actually just a collection of ones and zeros represented by magnetization, light pulses, radio signals or other means. This type of information is fragile and can be easily lost or changed."[7] In other words:

> Protecting the integrity of evidence and maintaining a clear chain of custody is always important in a criminal case, but the nature of the evidence in a cybercrime case makes that job far more difficult. An investigator can contaminate the evidence simply by examining it, and sophisticated cybercriminals may set up their computers to automatically destroy the evidence when accessed by anyone other than themselves.[8]

Digital evidence is information in digital form which is found "on a wide range of computer devices; in fact, it is anything that has a microchip or has been processed by one and then stored

---

[6] Albert J. Marcella and Doug Menendez, *Cyber Forensics A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*, 2nd ed. (New York: Auerbach Publications, 2008), 11;

[7] http://www.techrepublic.com/blog/it-security/what-makes-cybercrime-laws-so-difficult-to-enforce/ (accessed on 5th July 2017).

[8] Ibid.

on other media. Digital data is a numerical representation that is usually in binary form, as distinct from electronic data stored in analog form."[9]

As the subject of digital evidence is new thus only "few people are well versed in the evidential, technical, and legal issues related to digital evidence and as a result, digital evidence is often overlooked, collected incorrectly, or analyzed ineffectively."[10] This is the situation in the developed countries. However, the developing countries are far away from accepting this demand. It is so powerful that it can "reveal communications between suspects and the victim, online activities at key times, and other information that provides a digital dimension to the investigation."[11]

The topic of digital evidence is extensive, and it covers "diverse issues ranging from the collection, storage, and preservation to the authentication, validation, and application of electronic evidence, and raising questions on privacy, cost, ethics, and procedural management."[12] With the passage of time, devices containing digital data may "deteriorate over time or when exposed to fire, water, jet fuel, and toxic chemicals."[13] Besides, while examining, interpreting and presenting digital evidence certain errors can be introduced, complicating the job of investigators, prosecutors, defense lawyers and judges.

---

[9] Richard Boddington, *Practical Digital Forensics* (Birmingham: Packt Publishing, 2016), 56.

[10] Eoghan Casey, *Digital Evidence and Computer Crime,* 3rd ed. (New York: Elsevier, 2011), 8.

[11] Casey, *Digital Evidence and Computer Crime,* 16.

[12] Xandra Kramer, "Challenges of Electronic Taking of Evidence: Old Problems in a New Guise and New Problems in Disguise," *Jornadas Iberoamericanas de Derecho Procesal IIDP & IAPL*, XXVI (2018): 391-410 at 393.

[13] Casey, *Digital Evidence and Computer Crime,* 27.

1.3 General Rules of Evidence

There are five important rules for evidence collection, which are also applicable to digital evidence, in addition to other related rules. These relate to "five properties that evidence must have to be useful."[14] If any of the below mentioned rule is missing from the evidence, then that will make the evidence weak. These are briefly stated as under:

1. **Admissible**: Admissible[15] is the fundamental rule for collecting evidence, if it is not admissible in the court of law according to law, then this evidence will not be collected. The first question which is raised by the courts is that whether the evidence is admissible or not?[16]
2. **Authentic:** The investigator should establish the link that the evidence is related to the crime or incident. If the investigator is unable to link the evidence to the incident, then for him proving the fact is very difficult.[17] Therefore, the evidence collected by the investigator must be relevant to the claims asserted.
3. **Complete:** While collecting the evidence, the investigator should collect complete evidence. If half evidence is collected or some part of it is missing, then it will lead to the acquittal of the criminal. It is not enough for investigator to "collect evidence that just shows one perspective of the incident,"[18] rather it should accumulate all the relevant evidence which links the criminal to the act.

---

[14] Vacca, *Computer Forensics: Computer Crime Scene Investigation*, 220.

[15] In Pakistan which things are considered admissible and what are not inadmissible, detail of this can be found in the QSO.

[16] For detail analysis of admissibility see, *Mst. Akhtar Sultana v. Major ® Muzaffar Khan Malik*, PLD 2021 SC 715.

[17] Vacca, *Computer Forensics: Computer Crime Scene Investigation*, 220.

[18] Ibid.

4. **Reliable:** The evidence collected must be reliable and authentic and its "collection and analysis procedures must not cast doubt on the evidence's authenticity and veracity."[19] It should be established by the investigator by cogent evidence that the digital data is what it is represented to by.
5. **Believable:** The evidence presented should be clearly understandable and believable to a judge or presiding officer of the court. It must also show the relationship (i.e. strong chain of custody) between the occurrence and the accused.

In any legal system, an important evidentiary issue with respect to digital evidence is "reliability." Rule 702 of Federal Rules of Evidence (FRE), requires that scientific and expert testimony "must be reliable both with respect to the principles and methods used by the expert and application of the principles and methods to the specific facts."[20] The criteria laid down by the USA Courts will be examined in coming pages.

When the investigator has gone through the whole procedure and collected relevant data; now he will proceed with identification, preservation, analysis and presentation to the court for prosecution. In legal proceedings, in last century, concerns were raised "about the lack of understanding among various legal practitioners and lawmakers for failing to address the problems brought about by the increasing reliance of digital evidence."[21] However, by the turn of the century "researchers at the time raised concerns about widespread misunderstanding as to the true nature of digital evidence. More worrying to them was the inefficiency and ineffectiveness of some forensic processes used in its recovery, analysis, and subsequent use in legal proceedings."[22]

---

[19] Ibid.
[20] https://www.rand.org/pubs/research_reports/RR890.html (accessed: 25th October, 2019).
[21] Boddington, *Practical Digital Forensics*, 10.
[22] Ibid.

As the criminal may leave many artifacts in hurry, therefore, it is imperative for the investigator to carefully collect the artifacts, as the artifacts has lot of importance in data collection,[23] which are very useful for tracing the suspect, Yet, these are difficult to discover, and if these are found successfully, then they have a lot of significance for investigator to link and trace the culprit.

1.4 Different Types of Evidence

Understanding the various types of evidence is vital for LEAs and investigators to collect proper evidence in a given situation. For not understanding or lack of proper understanding may lead to wastage of time as the evidence collected after utilization of valuable resources is useless. There are many types of evidence, each of them has unique characteristics these includes, personal or real (testimony), documentary, digital, demonstrative, exculpatory, inculpatory, physical, *prima facie* and scientific evidence.[24] However, each type is discussed below very briefly.

1.4.1 Personal or Real: Personal evidence (also known as testimony) is the most important form of evidence which is given by a witness, in the judicial proceedings, under oath. "It includes all kinds of statements regarded as possessed of probative force in respect of the facts stated."[25]

1.4.2 Digital Evidence: Digital evidence is "any probative information stored or transmitted in digital form that a party to a court case may use at trial."[26] To put it another way, digital evidence is "any data stored or transmitted using a computer that support or refute a theory

[23] These are code fragments, trojaned programs, running processes, or sniffer log files etc.
[24] https://www.universalclass.com/articles/law/types-of-evidence.htm (accessed: 13th July 2018).
[25] Imran Ahsan Khan Nyazee, *Jurisprudence* (Rawalpindi: Federal Law House, 2015), 325.
[26] Casey. *Digital Evidence and Computer Crime,* 7.

of how an offense occurred or that address critical elements of the offense such as intent or alibi."[27]

1.4.3 **Documentary Evidence:** Documentary evidence consists of any proof that can be presented in writing (i.e. contracts, letters, wills and invoices). However, term documentary evidence can technically include any number of media upon which such documentation can be recorded and stored (i.e. photographs, recordings, films, and printed emails).[28]

1.4.4 **Exculpatory Evidence**: Exculpatory evidence is an evidence that is in favor of the accused person either partially or totally removing their guilt, in a criminal trial that exonerates or tends to exonerate the defendant of guilt.[29] In other words, "it is evidence favorable to the defendant or information that leads to evidence that is favorable to the defendant. It is not only evidence inconsistent with guilt, but also evidence for impeachment of a witness or that may mitigate the sentence."[30] It is necessary for the Police and prosecutors to reveal exculpatory evidence to the accused persons. In *Brady v. Maryland*, the USA court held that "withholding exculpatory evidence violates due process where the evidence is material either to guilt or to punishment."[31]

1.4.5 ***Prima Facie* Evidence:** *Prima facie* means on its first appearance. Prima facie evidence "is presented before a trial that is enough to prove something until it is successfully

---

[27] Ibid.

[28] https://www.universalclass.com/articles/law/types-of-evidence.htm (accessed: 13th July 2018).

[29] *The Free Dictionary by Farlex*, s.v. "exculpatory evidence."

[30] James W. H. McCord and Sandra L. McCord. *Criminal Law and Procedure for the Paralegal: A Systems Approach*. 3r ed. (New York: Thomson Delmar Learning, 2005),447

[31] *Brady v. Maryland*, 373 U.S. 83 (1963). Thereafter, in various case this has been discussed in detail are: *United Stated v. Moussaoui,* 591 F.3d 263 (2010); Turner v. United States 582 U.S.____. 2017; *United Stated v. Moussaoui,* 382 F.3d 453 (4th Cir. 2010); In the *United Stated v. Perdomo,* 929 F.2d 967 (3d Cir. 1991), the court held that the prosecution is obligated under *Brady* case to disclose all exculpatory evidence.

disproved or rebutted at trial."[32] *Prima facie* evidence is also called "presumptive evidence."

1.4.6 Scientific Evidence: Scientific (also known as forensic) evidence is "evidence which serves to either support or counter a scientific theory or hypothesis. Such evidence is expected to be empirical evidence and interpretation in accordance with scientific method."[33] Scientific evidence is, such as deoxyribonucleic acid (DNA), computer evidence, trace evidence, fingerprints or ballistics reports.

1.4.7 Demonstrative Evidence: An object or document is considered to be demonstrative evidence when it directly demonstrates a fact. This is a common and reliable kind of evidence, which includes photographs, videotapes, movies, sound recordings, diagrams, charts, x-rays, maps, drawings, graphs, simulations, sculptures, forensic animation, animation and models.[34] To be admissible, "a demonstrative exhibit must fairly and accurately represent the real object at the relevant time."[35]

1.4.8 Circumstantial Evidence: Circumstantial evidence is evidence that "relies on an inference to connect it to a conclusion of fact. Stating differently, circumstantial evidence allows a trier of fact to infer that a fact exists."[36]

1.4.9 Direct Evidence: Direct evidence is "testimony relating immediately to the principal fact, while all other evidence is circumstantial."[37]

---

[32] https://i-sight.com/resources/15-types-of-evidence-and-how-to-use-them-in-investigation/ (accessed: 13th July, 2018).

[33] https://en.wikipedia.org/wiki/Scientific_evidence (accessed: 7th August, 2018).

[34] https://i-sight.com/resources/15-types-of-evidence-and-how-to-use-them-in-investigation/ (accessed: 13th July, 2018).

[35] FRE.

[36] https://en.wikipedia.org/wiki/Circumstantial_evidence (accessed: 7th August, 2018).

[37] Nyazee, *Jurisprudence*, 325.

1.5 HEARSAY

Hearsay is unverified information heard or received from another person which is not the personal knowledge of the witness. According to Federal Rules of Evidence (FRE) hearsay is "a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted."[38]

Normally, courts do not permit witnesses to testify which he has heard or other people told him about the incident or occurrence of an offence. Same is the case in Pakistan, where hearsay evidence is not admitted in Pakistani legal system. However, there are few exceptions to this. In U.S.A, few questions must be answered by the witnesses to determine "whether a piece of digital evidence is hearsay or not." However, hearsay rule has a narrow scope.[39] Generally, courts do not admit hearsay evidence "because the speaker or author of the evidence is not present in court to verify its truthfulness."[40]

If an organization prints data and the same is offered in evidence, whether these prints constitutes hearsay or not? The courts in USA after recognizing the prints in evidence held that any computer records result from a process thus they are not statements of persons meaning thereby that they are not hearsay at all. Thus, in the case of *United States v. Washington*, the court has held that "printed result of computer-based test was not the statement of a person and thus would not be excluded as hearsay"[41] whereas in the case of *United States v. Hamilton,* the court

---

[38] Rule 801(c) of Federal Rules of Evidence.

[39] In *New York v. Microsoft Corp.,* 2002 WL 649951 (D.D.C., April 12, 2002), the Microsoft challenged several emails inadmissible being hearsay. The court excluded multiple email messages using the following reasoning:

1. they were offered for the truth of the matters asserted,
2. were not shown to be business records as required under Rule 803(6), and
3. contained multiple levels of hearsay for which no exception had been established.

[40] Casey, *Digital Evidence and Computer Crime,* 64.

[41] *United States v. Washington*, 498 F.3d 225, 230-31 (4th Cir. 2007).

held that "computer-generated header information was not hearsay as there was neither a 'statement' nor a 'declarant' involved here within the meaning of Rule 801."[42] But in the case of *United States v. Khorozian*,[43] the court concluded that "header information automatically generated by fax machine was not hearsay because "nothing said by a machine . . . is hearsay." At the time when QSO was enacted by the President of Pakistan, in USA in *People v. Holowko*,[44] court after examining printouts concluded "that the printout of results of computerized telephone tracing equipment is not hearsay evidence" but rather "a self-generated record of its operations, much like a seismograph [or] ... a flight recorder." In Pakistan, QSO was amended in 2002, which prescribed printout as primary evidence.

It can safely be said that a computer-generated print out does not involve a person therefore it cannot be hearsay. Whereas, Global Positioning System (GPS) records falls under the business exception as held in the case of *United States v. Wood*.[45]

1.6 DEFINING DIGITAL EVIDENCE

Defining any term in law or in any discipline is not easy or simple. Same is the issue with digital evidence. Various terms have been used for defining or describing the digital evidence including electronic evidence, computer evidence and digital evidence. All these terms definite some features of digital evidence. Yet, "defining what these distinguishing features are is far from straightforward."[46] As the fast growth and changes in Information Communication Technology (ICT) may make any definition obsolete.

---

[42] *United States v. Hamilton*, 413 F.3d 1138, 1142-43 (10th Cir. 2005).
[43] *United States v. Khorozian*, 333 F.3d 498, 506 (3d Cir.2003).
[44] *People v. Holowko*, 109 Ill.2d 187, 93 Ill.Dec. 344, 486 N.E.2d 877, 878 (1985).
[45] *United States v. Wood*, No.08-CR-92A, 2009 WL 2157128 (W.D.N.Y. July 15, 2009).
[46] Mason and Seng, *Electronic Evidence*, 19.

The use of digital evidence has increased exponentially since last few decades. There is no uniformity in use of electronic evidence or digital evidence terms. Both terms are accepted and used globally in the writings of scholars and legal fraternity. Besides, there are various definitions of "digital or electronic evidence." However, every definition highlights some important features. Simply stated, digital evidence is any kind of evidence that comes in digital form rather than to paper or any tangible form.

There are various, worldly, accepted definitions which have been provided by different organizations and scholars. The followings are some of the definitions:

The Scientific Working Group on Digital Evidence (SWGDE) defined digital evidence as "any information of probative value that is either stored or transmitted in a digital form."[47] While the International Organization of Computer Evidence (IOCE) defined it as "any information stored or transmitted in binary form that may be relied upon in court."[48] However, these definitions "focus on proof in court and neglect data that can make an investigation advance further. That the term binary is inexact describing just one of many common representations of computer data."[49] This term is no more in use and SWGDE changed the term "binary" with "digital" to include digital audio, video, cell phones, and digital fax machines.[50]

The Brian Carrier proposed the definition of digital evidence as "digital data that support or refute a hypothesis about digital events or the state of digital data."[51] However, Eoghan Casey[52]

---

[47]https://www.swgde.org/documents/Archived%20Documents/SWGDE-SWGIT%20Digital%20and%20Multimedia%20Evidence%20Glossary%20v2-8 (accessed: 9th August, 2018).

[48] The definition was adopted by IOCE in 2000.

[49] Casey, *Digital Evidence and Computer Crime,* 7.

[50] Carrie Morgan Whitcomb, "An Historical Perspective of Digital Evidence: A Forensic Scientist's View," *International Journal of Digital Evidence* 1 (2002): n.d.

[51] Brian D. Carrier, "A hypothesis-based approach to digital forensic investigations," (Ph.D. diss., Purdue University, 2006), 11.

[52] Eoghan Casey is the author of *Digital Evidence and Computer Crime,* and coauthor of *Malware Forensics.*

proposed the following definition that digital evidence is "any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi."[53] Whitcomb has criticized this definition in the following words:

> Although the emphasis of this definition is on criminal investigations, it is a wider definition than the previous definitions, and it usefully explicates certain important aspects of electronic evidence. For instance, the reference to 'data' is to information that is held in electronic form, such as text, images, audio and video files. Also, the word 'computer' must be understood in its widest possible sense, and incorporates any device that stores, manipulates or transmits data. In addition, the definition implies that the evidence must be relevant and admissible, a question that can only be answered after we know what the electronic evidence, whether admissible or inadmissible, actually is.[54]

Definition of digital evidence by Casey is wider as compared to other definitions, proposed before him, as the word 'data' is to information means data which is held in electronic form and the word 'computer' is to be understood to its widest possible sense, i.e., any device which stores, transmits or manipulates data.[55]

The Association of Chief Police Officers (ACPO),[56] defines digital evidence that "information and data of investigative value that are stored on or transmitted by a computer."[57] However, the focus of this definition is on the device. Whereas, the in the Guide of Council of Europe (CoE) this is defined as "any information generated, stored or transmitted using electronic devices that may be relied upon in court. To guarantee that the evidence is accepted in court, it is necessary to obtain the information following very well-defined processes using specialized personnel and operating within an adequate legal framework."[58]

---

[53] Casey, *Digital Evidence and Computer Crime,* 7.

[54] Mason and Seng, *Electronic Evidence*, 19.

[55] Data is defined in section 2 (xiii) of the PECA which says that data "includes content data and traffic data."

[56] The Association of Chief Police Officers.

[57] Association of Chief Police Officers UK, *Good Practice Guide for Computer-Based Electronic Evidence*, 6.

[58] In the Guide of CoE, the term electronic evidence is used to "include all possible devices that generate and / or store potential Electronic Evidence."

The scholars Schafer and Mason[59] has proposed the following definition:

> Electronic Evidence is data (comprising the output of analogue devices or data in digital format) that is manipulated, stored or communicated by any man-made device, computer or computer system or transmitted over a communication system, that has the potential to make the factual account of either party more probable or less probable than it would be without the evidence.[60]

According to the scholars Schafer and Mason this definition consists of three elements:

i. reference to 'data' includes "all forms of evidence created, manipulated or stored in a device that can, in its widest meaning, be considered a computer."[61]

ii. this definition includes "the various devices by which data can be stored or transmitted, including analogue devices that produce an output. Ideally, this definition will include any form of device, whether it is a computer as we presently understand the meaning of a computer, telephone systems, wireless telecommunications systems and networks, such as the Internet, and computer systems that are embedded into a device, such as mobile telephones, smart cards and navigation systems."[62]

iii. this definition restricts "the data to information that is relevant to the process by which a dispute, whatever the nature of the disagreement, is decided by an adjudicator, whatever the form and level the adjudication takes."[63]

Mason has proposed another definition which means "evidence derived from data contained in or produced by any device the functioning of which depends on a software program or from data stored on or communicated over a computer system or network."[64]

---

[59] Stephen Mason *Barrister of the Middle Temple.*

[60] Stephan Mason and Daniel Seng. *Electronic Evidence.* 4th ed. (London: School of Advanced Study, University of London, 2017) 19.

[61] Mason and Seng, *Electronic Evidence*, 19.

[62] Ibid., 20.

[63] Ibid.

[64] Stephen Mason, Draft Convention on Electronic Evidence. http://journals.sas.ac.uk/deeslr/article/viewFile/2321/2245 (accessed: 7th November, 2019).

USA, National Institute of Justice (NIJ) defines digital evidence as any "information and data of value to an investigation that is stored on, received, or transmitted by an electronic device."[65] The following definition is adopted by the EVIDENCE Project:

> "Electronic Evidence is any information of potential or tangible probative value that is generated through, stored on or transmitted by any electronic device."[66]

Another definition is also proposed by the EVIDENCE Project, which is as under:

> Electronic evidence is any data resulting from the output of an analogue device and/or a digital device of potential [probative] value that are generated, processed, stored or transmitted using any electronic device. Digital evidence is that electronic evidence that is generated or converted to a numerical format.[67]

This definition is very important as it clarifies various definitions proposed in recent years, as it includes both evidence that is "born digital, and that which in the course of its life is transformed and then stored or exchanged in electronic form."[68]

Other than the EVIDENCE project definition, proposed by the various scholars and institutions are missing some of the elements which may be important for the proper understanding of digital evidence. However, the definition proposed by the EVIDENCE project clarifies various ambiguities.

> The rapid technological change in the field of information technology means that any definition narrowly tailored to the current state of technology faces the risk of becoming obsolete rapidly. Definitions that are suitably future proof by contrast tend to be too abstract and will cut across traditional divisions and categories in the law of evidence.[69]

The term digital or electronic evidence is not defined in Pakistani legal system. However, the term evidence is defined in QSO and the term electronic is defined in ETO and PECA

TH24966

---

[65] *Electronic Crime Scene Investigation: A Guide for First Responders,* 2nd ed. (Washington, D.C: National Institute of Justice, 2008), ix; http://www.forensicsciencesimplified.org/digital/ (accessed: 31st July, 2018).

[66] Maria Angela Biasiotti et al. *Handling and Exchanging Electronic Evidence Across Europe* (Cham: Springer, 2018), 175.

[67] Biasiotti et al. *Handling and Exchanging Electronic Evidence,* 4.

[68] Ibid.

[69] Mason and Seng, *Electronic Evidence*, 19.

respectively. The ETO defines the term electronic which includes "electrical, digital, magnetic, optical, biometric, electrochemical, wireless or electromagnetic technology."[70] Although, the PECA has adapted the same definition of the term electronic, but an additional word electromechanical has been made part of the definition, which provides that "electronic" includes electrical, digital, magnetic, optical, biometric, electrochemical, electromechanical, wireless or electromagnetic technology"[71] and the term evidence has been defined which includes;

> "(i) all statements which the Court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry; such statements are called oral evidence; and
>
> (ii) all documents produced for the inspection of the Court; such documents are called documentary evidence."[72]

In the Pakistani legislation (such as Cr.PC, CPC, QSO, PECA, ETO), there is no definition of digital evidence. However, there is only definition of electronic in ETO and PECA respectively and evidence in QSO. As such the existing law of evidence is meant for the facts of physical-world only.

Thus, on the basis of above-mentioned discussion, it can safely be concluded that it does not fulfill the purpose of a comprehensive and precise definition creating difficulties for the LEAs, Judiciary and other persons working on the field to understand the digital evidence as it ought to be. Instead of using the term 'electronic' the term digital evidence will be used throughout the thesis.

---

[70] Section 2(1) (l) of the ETO.
[71] Section 2 (1) (xvii) of the PECA.
[72] Section 2 (1) (c) of the QSO.

1.7 SOURCES OF DIGITAL EVIDENCE

Digital devices are found everywhere in contemporary Information Technology era, helping people communicate easily locally and across the border. Computers, mobiles phones and the Internet are not the only sources of digital evidence, but there are many digital devices which are source of digital evidence.

Sometimes irrelevant thing also carries digital evidence which are normally ignored by the investigators. Games can also carry encoded messages between offenders. Besides, new household machines, "such as a refrigerator with a built-in TV, could be used to store, view and share illegal images. The important thing to know is that responders need to be able to recognize and properly seize potential digital evidence."[73]

It should be borne in mind by the LEAs, Lawyers, and Judges that digital evidence comes in many forms including hard drives, mobile phone, personal digital assistant (PDA), compact disc (CD), digital optical disc (DVD), Voice over Internet Protocol (VoIP) devices, floppy disks, memory cards,[74] memory sticks, credit card skimmers, a flash card in a digital camera or mobile phone, e-mail, electronic financial transactions records, audit trails, application logs, badge reader logs, Universal Serial Bus (USB), digital cameras, electronic organizers, printers, biometrics data, biometric scanners, application metadata, digital photographs, word processing documents, instant message histories, answering machines, telephones, photo copiers, digital watches, spreadsheets, network traffic, internet browser histories, databases, printers with an internal hard drive, the Internet, Internet service provider logs, windows registry, system logs, system files, filesystem

[73] http://www.forensicsciencesimplified.org/digital/ (accessed: 31st July, 2018).

[74] In *Nazim Ali v. Additional Sessions Judge,* 2016 MLD 25, the Lahore High Court (LHC), considered memory card as an evidence and directed the prosecuting agency to provide the same to the accused. Similarly, in *Muhammad Irfan v. The State*, 2018 PCRLJ 1319, the LHC accepted the evidence on mobile phone memory card and upheld the conviction of the accused.

data, intrusion detection system reports, wireless telecommunication systems, the contents of computer memory, firewall logs, digital picture frames, database contents, gaming systems, computer backup, audio and video files.[75] In addition to this, digital evidence may also be available on "any server or device that stores data, including some lesser-known sources such as home video game consoles, GPS, sport watches and internet-enabled devices used in home automation."[76] Even, today microwave oven can also contain digital evidence.[77]

Digital data can be stored remotely on various devices including "network-attached storage, remote networks or 'cloud' facilities."[78] Thus, creating more difficulties for the digital investigators to locate and obtain legal access to data "that is stored remotely from an individual's computer."[79] Due to introduction of new devices every day, comprehensive and exhaustive list of all the sources of digital evidence cannot be provided. However, effort has been made to mention the maximum sources of digital evidence.

> In addition to the Internet, digital evidence may exist on commercial systems and privately owned networks. These privately owned networks can be a richer source of information than the public Internet. These networks can have databases, document management systems, time clock systems, and networked systems that contain information about the individuals who use them. Also, private organizations often configure their networks to monitor individuals' activities more than the public Internet. Some organizations monitor which Web pages were accessed from computers on their networks. Other organizations even go so far as to analyze the raw traffic flowing through their network for signs of suspicious activity.[80]

---

[75] Boddington, *Practical Digital Forensics*, 26 & 212; Thomas A. Johnson. *Forensic Computer Crime Investigation* (New York: CRC, 2005), 10; Casey, *Digital Evidence and Computer Crime,* 8, 230-31, 488-69; *Investigative Uses of Technology: Devices, Tools, and Techniques,* (Washington, D.C: National Institute of Justice, 2007), 12; Mason and Seng, *Electronic Evidence*, 4;

[76] https://i-sight.com/resources/15-types-of-evidence-and-how-to-use-them-in-investigation/ (accessed: 13th July, 2018); https://definitions.uslegal.com/d/digital-evidence/ (accessed: 7th August, 2018).

[77] Casey, *Digital Evidence and Computer Crime,* 8.

[78] Mason and Seng, *Electronic Evidence*, 5.

[79] Ibid.

[80] Casey, *Digital Evidence and Computer Crime,* 31.

1.8 DIGITAL EVIDENCE AND CYBER LAWS IN PAKISTAN

The nature of evidence has been changed worldwide and has expanded significantly in the modern digital era. A lot of data or information is created in digital form and most of the data or information is never printed. Information technology (IT) has revolutionized, which caused a paradigm shift from manual to digital. In Pakistan, legislation on criminal and civil procedures were enacted long before the appearance of information technologies, thus not considering them. Moreover, the law of evidence was also enacted long before the invention of computer. So, rules of evidence are not comprehensive to deal with technological advancements, consequently, there is dire need to be modernized to strengthen the judiciary, prosecution and LEAs.

1.8.1 EVIDENCE ACT, 1872

During the British Raj, the Imperial Legislative Council passed the Indian Evidence Act,[81] in 1872 which was enacted on 15th March and came into force on 1st September, 1872. However, since its enactment, very few amendments were made but basically this Act remained in its original form. After the independence of Pakistani, this Act continued throughout Pakistan[82] and Republic of India. But, in Pakistan, this Act was repealed through QSO in 1984. The Indian Evidence Act was mainly based on Taylor's work on Evidence, and in the words of Sir James Fitzjames Stephen who framed it, was an "attempt to reduce the English Law of evidence in the form of express propositions arranged in their natural order with some modifications rendered necessary by the peculiar circumstances of India."[83]

---

[81] Act no. 1 of 1872.

[82] Section 18(3) of the Indian Independence Act, 1947 provides that the Laws of British India and of the several parts thereof existing immediately before 15 August 1947 would, as far as applicable and with necessary adaptations, continue as the laws of each of the new dominions and the several parts thereof until other provisions were made by laws of the legislature of the dominion in question or by any other legislature or other authority having power in that behalf.

[83] *Ram Kirpal vs. Shri Krishna Deo,* AIR 1948 All. 109.

1.8.2 *Qanun-e-Shahadat* Order, 1984

The *Qanun-e-Shahadat* Order, 1984 (QSO) [84] is the basic legal instrument on evidence in Pakistan which repealed the Evidence Act of 1872,[85] to bring the existing law of evidence in conformity with the injunctions of Islam.[86] It is an admitted position that all Articles of the QSO are substantially and subjectively mere reproduction of all sections of the repealed Act with few exceptions.[87]

The objective of introduction of QSO was to bring "all laws of evidence in conformity with the injection of Islam as laid down in the Holy Qur'an and *Sunnah*." However, this law does not apply in arbitration proceedings.[88]

When QSO was made by the President of Islamic Republic of Pakistan in 1984, it was just the start of IT era the QSO was introduced, thus it was not in the minds of legislatures to legislate for the future evidence issues covering the emerging technologies. So, it was difficult to imagine, discuss, legislate and handle the 21st century's demands of digital evidence. For this reason, it can safely be said that legislations on law of evidence in Pakistan was enacted before these technologies appeared, while not considering them at the time of preparing of legislation.

---

[84] The term "*Qanun-e-Shahadat*" is only an Urdu translation of English term "Law of Evidence". *Qanun-e-Shahadat* Order, 1984 was promulgated by the then President of Pakistan Zia-ul-Haq in 1984. (Order no. X of 1984).

[85] Article 166 of QSO.

[86] This is the story which is being told that the QSA was Islamised in 1984. However, this is not the case. For detail see Lucy Carroll, "Pakistan Evidence Order ("Qanun-i-Shahdat"), 1984: General Zia"a Anti-Islamisation Coup", in *Dispensing Justice in Islam: Qadis and their Judgments*, eds. Muhamamd Khalid Masud, Rudolph Peters & David S. Powers, Brill, Leiden-Boston, 2006, p. 519.

[87] For example, Article 3, Article 4 to 6, Article 44, Article 42. Moreover, ETO has also added few new sections in QSO which are discussed under the ETO.

[88] Article 1 (2) of the QSO.

1.8.3 ARTICLE 164 OF THE QSO

Notwithstanding, the most significant development of the QSO was Article 164, which provided for the admissibility of the modern devices which reads as "[i]n such cases as the Court may consider appropriate, the Court may allow to be produced any evidence that may have become available because of modern devices or techniques: Provided that conviction on the basis of modern devices or techniques may be lawful."[89]

Although, the above-mentioned article was not remarkable to address IT related issues comprehensively and provide proper mechanism for electronic evidence. Nevertheless, it provided the recognition and acceptance of the new devices at the time as evidence. With the passage of time, it failed to deliver, hence, legal practitioners, lawyers, judges, civil society and academician started criticizing this article[90] and emphasized that law of evidence must be changed, to avoid the misuse of this article and to bring with the requirement of contemporary requirements of the legal system of Pakistan.

---

[89] Article 164 of QSO. Subs. and added by the Criminal Laws (Amendment) Act, 2017 (Act No. IV of 2017), s.5.

[90] Muhammad Aqil, ASC expressed grave concerns "over misuse of modern devices and techniques for ulterior motives, illegal & wrongful gains and called for repealing Article 164 of the Qanun-e-Shahadat Order, 1984. He further stated that this order was promulgated "as tool for denial of justice to private parties by providing legality to conversations (recorded through use of modern electronic devices and techniques) in private/personal disputes of civil and commercial nature as evidence in courts." Besides, criticizing the QSO he stressed that in modern technological and computer age, "it has become far more easier to fake up evidence by using, erasing, tampering and making interpolations in audio/video cassettes/CDs and preparing fake and fabricated tapes/cassettes/CDs and morphed up images by parties trying to establish false, fake and fabricated claims against rivals in all types of litigations, be it civil, commercial or criminal." Moreover, he also expressed great concern about the misuse of this article that "even the government and the politicians have felt the brunt of this Article 164 of the Qanun-e-Shahadat 1984 as with the help of mimickers, camera-tricks and various electronic devices and techniques, including computer soft-wares blackmailing, false, fabricated and frivolous claims have been made by vested interests to exploit and use against adversaries in courts." Further, he feared that "such dirty tricks not only destabilizes the social structure of a society but also promotes immorality, extortion, terrorization, scandalization, forced marriages and sometimes sensationalization of issues."

In 2017 at Islamabad, a "National Conference on Law and Technology in the Digital Age" was organized by the civil society[91] in which various speakers[92] expressed grave concerns "over misuse of modern devices and techniques for ulterior motives, illegal & wrongful gains and called for repealing Article 164 of the *Qanun-e-Shahadat* Order, 1984."[93] However, the QSO was not amended, while criticizing the QSO, they said that "gross injustices existing in the society along with evils of harassment, blackmailing and frivolous litigations based on evidence procured through illegal use of modern devices and techniques for ulterior motives, illegal and wrongful gains."[94] They also demanded a "fair and just law of evidence as the need of the hour."[95] Justice Tassaduq Hussain Jillani (retd), said

> the gap between technological innovation and the legal rules necessary to govern such developments is ever-widening. It is must to develop and pursue rational efficient policies in order to ensure that Pakistan makes the best possible use of technology as a driving and democratizing force, accommodating business and entrepreneurs, while protecting the rights and the privacy of the consumers and the public at large. Keeping this in view, regulation must ensure that the internet and the world of technology is a safe and equitable place.[96]

In the same year i.e. 2017, another seminar was organized by the RAC in collaboration with IHRA to create awareness of the flaws in the Law of Evidence of 1984 in which the members' of the Civil Society requested the Supreme Court of Pakistani to take notice of misuse of *Qanoon-e-Shahadat.*[97] However, the speaker ignored the fact that legislator has imposed many restrictions

---

[91] This conference was organized by the CLEIP and CLDP of US Department of Commerce and USAID in collaboration with Anti-Counterfeit Forum (ACIF), INBOX Technologies, PlanetN Group, TPL Trakker Ltd, National Incubation Center and Bytes for All on 3rd August, 2017, at Marriott Hotel, Islamabad.

[92] Few of the eminent speakers, jurists and panelists were Hildy Bowbeer (from USA), Muhammad Amir Munir from PJA, Justice (retd) Tassaduq Hussain Jillani, Justice (retd) Shakirullah Jan, Dr. Tariq Hassan, Advocate Supreme Court of Pakistan and Muhammad Aqil, Advocate Supreme Court and member Pakistan Bar Council.

[93] https://fp.brecorder.com/2017/08/20170804205160/ (accessed: 21st February, 2018).

[94] Ibid.

[95] Ibid.

[96] Ibid.

[97] In the RAC seminar, Mian Javed Anwar Advocate observed that "the faulty Articles 46-A & 164 of Qanoon-e-Shahadat' Order, 1984 should be a matter of immediate attention of the top judiciary keeping in view that the flaws in these articles are grossly being misused." Some people think that the tape-recorded conversations should not be made admissible in the law of evidence. One of the critics is Syed Ghulam Raza Shah Naqvi who explained

through the Investigation for Fair Trial Act, 2013 (IFTA)[98] on LEA for interception of digital data. This Act is discussed in chapter 2.

It is very interesting that when this Article was made part of QSO in Pakistan then a complete Act on the modern devices and techniques was enacted in USA under the title of the U.S. Federal Computer Fraud and Abuse Act[99] which was passed in 1984 and was subsequently amended various times.[100] Even before USA, the Canada was first country in the world to enact a law in 1983 to address computer related crimes while amending their Criminal Code.

Nonetheless, with the emergence of IT, ETO was promulgated in 2002 to legislate on the subject of electronic transactions and few of the cyber-crimes (as discussed in next section), still many technology related issues were not covered. First time in Pakistan, through the enactment of ETO, electronic record was made acceptable in judicial proceedings.

Because of technological advancements, what is the nature if threshold requirement needed to admit these kinds of evidence? Would an electronic record constitute a document?[101] Are the contents of electronic records writings?[102] Can electronic records be accepted as an evidence?[103] These are the few issues tackled by the recent amendment in *Qanun-e-Shahadat* Order, 1984

---

this phenomenon in the above-mentioned seminar of RAC and said that "the tape-recorded conversations inclusive of privileged relating to private, personal matters such as between the husband-wife, lawyer-client, doctor-patient or relatives, etc., should not be made admissible under the law of evidence." https://www.dawn.com/news/1348889 (23rd Feb. 2018)

[98] The Investigation for Fair Trial Act 2013 (Act No. 1 of 2013).

[99] It is placed in section 1030 of the 18 United States Code (18 U.S.C).

[100] This Act was amended in 1988 (by the Minor and Technical Criminal Law Amendments Act), 1989 (by the Financial Institutions Reform, Recovery, and Enforcement Act), 1990 (by the Financial Institutions Anti-Fraud Enforcement Act), 1994 (by the Computer Abuse Amendments Act), 1996 (National Information Infrastructure Protection Act), 2001(by the USA PATRIOT Act), 2002 (by the Criminal Law Technical Amendments Act and by the Cyber Security Enhancement Act) and 2008 (by the Identity Theft Enforcement and Restitution Act) respectively.

[101] Article 2 (1) (e) of the QSO.

[102] Ibid., Article 78-A.

[103] Ibid., Article 73.

through the enactment of ETO. Question arises whether this amended is ETO specific or it has amended QSO? This will be discussed in coming pages.

Digital evidence is new as comparted to contemporary evidence. Whereas, the existing rules of evidence, being centuries-old, are still being applied to digital evidence. Question arises whether the current evidence rules recognized the unique nature of digital evidence? This will be discussed in coming chapters.

While Article 164 of the QSO cannot provide a thorough consideration of each of digital era issues, as various issues of digital evidence have not been adequately addressed by this Article. This will be examined in coming pages that how courts currently address electronic discovery issues and specifically how Article 164 (and other Articles as amended by ETO) has been applied to the digital evidence issues and the manner in which electronic documents are produced in the courts and whether the duplicate hard drive copy in digital evidence will be accepted in evidence.

Now, after four decades of insertion of Article 164 in the QSO, and after two decades of amendment of Article 2 in the QSO, the need to "accord with changing technology" is not fulfilled yet. Forms of digital evidence that could not have been foreseen in 1984 or in 2002 do not easily fall within the domain of amending QSO are now very common. Electronically stored information (ESI), such as embedded data, web caches, browsing history, temporary, cookie and backup files do not cover many aspects of the digital evidence.

QSO was adopted in early days of 80s, when the legislature (President) could have hardly foreseen that the future of evidence that how many organizations store vast volumes of data, and how data is stored beyond national boundaries such as cloud system, which are providing cross-border services to many companies around the globe.

1.8.4 MODIFICATIONS AND ADDITION IN QSO

In Pakistan, the rules of evidence (Evidence Act, 1872) were written at a time when information was stored primarily on paper, in the form of documents and these rules were designated to deal with information stored on papers. However, the current rules of QSO do not deal adequately with information stored in electronic forms. Astoundingly, Article 164 does not mention information stored in electronic form. After all, how can it be expected that a rule primarily meant to deal with paper documents to function in an increasingly paperless world?

Whether the QSO be modified to impose severe requirements for the acceptance of digital/computer related evidence or not? In 2002, first time in Pakistani legal history, need was felt that the QSO should be amended and computer-generated evidence may be made admissible. Although, Article 164 of the QSO was there in the field but a need was felt by the legislature to address the un-addressed issues. Therefore, the QSO was amended and the following developments took place with the promulgation of ETO.

Article 2 of the QSO was amendment and two new sub-clauses namely (e) and (f) were added and the following expressions were given the meaning which were attributed in ETO. These expressions are automated, electronic, information, information system, electronic document, electronic signature, advanced electronic signature, and security procedure. And in sub-clause (f) the expression 'certificate' was defined.

To provide for the admission of automated generated information, in Article 30 of the QSO, an explanation was added, after the amendment the article read as under;

> **Article 30.** An admission is a statement, oral or documentary which suggests any inference as to any fact in issue or relevant fact, and which is made by any of the persons and under the circumstances, hereinafter mentioned.
>
> *Explanation.* – Statements generated by automated information systems may be attributed to the person exercising power or control over the said information system.

Before the enactment of ETO, electronic documents were not accepted in evidence. Therefore, this amendment created an opportunity for acceptance of electronic documents. Consequently, a new Article 46-A, for acceptance of electronic documents in evidence, was inserted which read as "[s]tatements in the form of electronic documents generated, received or recorded by an automated information system while it is in working order, are relevant facts."

Opinion of experts has a lot of significance in Islamic Law as well as in English common law. Thus, keeping in view the requirements of contemporary world, Article 59 of the QSO was also amended and few words were added and substituted to clarify the situation/position. This is discussed in chapter eight in detail.

Basically, Article 73 is about primary document. In this Article, for the recognition of electronic documents, the following two explanations were incorporated;

> *Explanation 3.* – A printout or other form of output of an automated information system shall not be denied the status of primary evidence solely for the reason that it was generated, sent, received or stored in electronic form if the automated information system was in working order at all material times and, for the purposes hereof, in the absence of evidence to the contrary, it shall be presumed that the automated information system was in working order at all material times.
>
> *Explanation 4.* – A printout or other form of reproduction of an electronic document, other than a document mentioned in Explanation 3 above, first generated, sent, received or stored in electronic form, shall be treated as primary evidence where a security procedure was applied thereto at the time it was generated, sent, received or stored.

These two explanations will be examined in chapter 5, whether these fulfill the requirements of law of evidence or not?

Basic purpose of ETO was to recognize and facilitate electronic documents. Since, before the 2002, electronic signature was not accepted in Pakistani legal system. To recognize the electronic signature and documents, a new Article 78-A was introduced which is says "[i]f an electronic document is alleged to be signed or to have been generated wholly or in part by any person through the use of an information system, and where such allegation is denied, the application of a security procedure to the signature or the electronic document must be proved."

There are two types of documents public and private. Article 85 of the QSO deals with public documents. Keeping in view the requirement of business community, this article was also amended in 2002, and certificates deposited in repository was recognized as public documents. The following new clause (6) was inserted, which read as under;

> "(6) certificates deposited in a repository pursuant to the provisions of the Electronic Transactions Ordinance, 2002."

Afore discussed modifications which took place with the promulgation of ETO. Here question arises whether these modifications are applicable to all proceeding either civil, criminal or commercial or to the selected laws? This will be examined in chapter 8.

1.8.5 THE CODE OF CRIMINAL AND CIVIL PROCEDURES

The Code of Criminal Procedure, 1898 (CrPC)[104] was promulgated to provide procedure for criminal proceedings which came into force on first day of July, 1898.[105] CrPC is procedural law which provides complete procedure for all criminal matters. Chapter XL and XLI of the CrPC provides for the commissions for the examination of witnesses and special rules of evidence. It is clear from

[104] Act no. V of 1898.
[105] Section 1 of the CrPC, 1898.

this law that this was enacted when there was no concept of information technology, computer, and the internet. This law covers almost all the material issue of the time but it lacks the requirement of present era.

The Code of Civil Procedure, 1908 (CPC) [106] was promulgated to provide procedure for civil proceedings which came into force on first day of January, 1909.[107] CPC is procedural law which provides complete procedure for all civil matters. Section 138, Order 18 of the CPC provides for the the examination of witnesses and special rules of evidence. It is clear from this that this law was enacted when there was no concept of IT. Like CrPC, CPC was also enacted before the invention of computer and the internet. Lacking many essential components of digital era.

1.8.6 ELECTRONIC TRANSACTIONS ORDINANCE, 2002[108]

ETO, is the first legal instrument enacted in Pakistan to legislate on the issue of electronic transactions to provide a mechanism to tackle the technology related issues and crimes. Preamble of the ordinance explains its purpose in the following words, "it is expedient to provide for the recognition and facilitation of documents, records, information, communications and transactions in electronic form, accreditation of certification service providers." In the light of this preamble, it can safely be concluded that this instrument only covers limited area of IT related issues. LEA's personal, without bothering its true spirit, were using two sections of this ordinance to apply in every cyber-crime situation but the same have been amended by PECA.[109] However, ETO amended few Articles of the QSO,[110] defined some expression, added few new Articles[111] and also

[106] Act no. V of 1908.
[107] Section 1 (2) of the CPC, 1908.
[108] Ordinance No. LI of 2002.
[109] Section 36 and 37 were being applied by the LEA to every type of cyber-crime till the enactment of PECA. However, the PECA have omitted both sections from ETO. Section 54 of PECA, 2016.
[110] In Article 2 (1) the sub-clauses (e) and (f) were inserted. There were few other articles which were amended.
[111] Section 46-A and section 78-A were instead in QSO.

added some explanations[112] in the Articles of the QSO, which is a good step towards the legislation on cyber related issues.

Through, this ordinance, the electronic documents were recognized and given proper status. The relevant section says that "[n]o document, record, information, communication or transaction shall be denied legal recognition, admissibility, effect, validity, proof or enforceability on the ground that it is in electronic form and has not been attested by any witness."[113] Before the promulgation of ETO, it was mandatory for documents to be in written form but the same has been dispensed by the ETO.[114] Similarly, the requirement of original form[115] and retention[116] have also been waved when the original is in electronic form. Besides, where the signatures are required the electronic signatures have been legally recognized.[117] Question arise whether these are applicable to the extent of ETO or other laws? This will be discussed in coming pages.

It can safely be stated that this ordinance provided a legal system for recognition of electronic records. But this ordinance was not meant to penalize the criminals therefore it was not sufficient to tackle the cybercrimes prevailing at that time. Whenever any issue was brought in the knowledge of LEAs, due to lack of proper legislation on the subject, they used to apply section 36 and 37 of the ETO. Resultantly, the accused were acquitted from the charges, due to improper application of law. Keeping in view this situation, a need of a comprehensive law on the subject was felt which lead to the promulgation of Prevention of Electronic Crimes Ordinance, 2007.

---

[112] In Article 30 and 73 explanations were inserted.
[113] Section 3 of ETO.
[114] Section 4 of ETO.
[115] Section 5 of ETO.
[116] Section 6 of ETO.
[117] Section 7 of ETO.

The most important development of the ETO is the establishment of the Certification Council,[118] which is responsible to grant and renew accreditation certificates to certification service providers and allied matters.

As already discussed that ETO's main purpose was to recognize the electronic documents as record. The intention of the legislature is very much clear from the preamble of the ordinance that the focus of the law-makers was not penalization of the cybercrimes rather it was for the recognition and facilitation of the electronic records. Although section 36 and 37 were added to penalize the damage to information system and violation of privacy.

1.8.7 THE PAYMENT SYSTEMS AND ELECTRONIC FUND TRANSFERS ACT, 2007

This Act[119] was enacted "to supervise and regulate Payment Systems and Electronic Fund Transfers in Pakistan and to provide standards for protection of the consumer and to determine respective rights and liabilities of the financial institutions and other Service Providers, their consumers and participants." Thus, it is obvious from preamble of this Act that this Act does not deal or provide any mechanism related to digital evidence.

1.8.8 THE INVESTIGATION FOR FAIR TRIAL ACT, 2013 (IFTA).

The Investigation For Fair Trial Act, 2013 (IFTA)[120] provides for investigation for "collection of evidence by means of modern techniques and devices to prevent and effectively deal with scheduled offences and to regulate the powers of the law enforcement and intelligence

---

[118] Section 18 of ETO. To run the affairs of the Certification Council certain rules were made, as envisaged under section 43 of the ETO. These are the Rules of the Certification Council "Certification Council Transaction of Business Regulations, 2004" notified on 10th January, 2007; "Electronic Certification Accreditation Council Service Regulations, 2008" notified on 5th March, 2008; "Information Security Auditors Regulation Regulations, 2008" notified on 2nd April, 2008; "Accredited Certification Service Provider's Audit Regulations, 2008" notified on 3rd April, 2008; and "Certification Service Providers' Accreditation Regulations, 2008" notified on 4th April, 2008.

[119] The Payment Systems and Electronic Fund Transfers Act (IV of 2007).

[120] Act No. I of 2013. To carry out the purpose of this Act, the Investigation for Fair Trail Rules, 2013 have been made on 31st March, 2013.

agencies and for matters connected therewith or ancillary thereto."[121] The purpose of this Act is obvious that this Act is meant for collection of evidence to the extent of scheduled offences which are mentioned at the Schedule I of the Act. Evidence collected under this Act, to the extent of offences mentioned in Schedule I of the Act, is admissible[122] and the report of expert is also admissible under this Act.[123] The provision of this Act has the overriding effect upon the QSO and CrPC.[124] Thus, it is obvious that this Act is meant for specific offences and a special treatment has been provided for the offences under this Act. Meaning thereby that it does not cover all aspects of digital evidence and related matters. In the USA, the Wiretap Statute prohibits the interception of oral, wire and electronic communications. The same is prohibited in PECA and IFTA respectively.

1.8.9 THE PREVENTION OF ELECTRONIC CRIMES ACT, 2016

The PECA[125] is an Act which provides provisions for prevention of electronic crimes. In other words, it is an Act which make provisions to "prevent unauthorized acts with respect to information systems and provide for related offences as well as mechanisms for their investigation, prosecution, trial and international cooperation."[126] Under section 29 of this Act, for investigation of offences, the Federal Government has been authorized "to establish or designate a law enforcement agency for the investigation."[127] But this Act is also silent on what is electronic evidence; how it will be collected, preserved and produced

---

[121] Preamble of the IFTA, 2013.

[122] Section 23 of the IFTA, 2013.

[123] Section 24 of the IFTA, 2013.

[124] Section 38 of the IFTA, 2013.

[125] Act No. XL of 2016. To carry out the purpose of this Act, the Prevention of Electronic Crimes Investigation Rules, 2018 have been made on 20th July, 2018.

[126] Ibid., Preamble.

[127] The Federal Government has designated the Federal Investigation Agency as the investigations agency for the purpose of investigation of offences under the Act, through S.R.O. 897 (I)/ 2016, dated 22nd September 2016.

in the court? Therefore, it can easily be concluded that PECA does not provide any systematic response to the new challenges of digital evidence. Thus, leaving options for the legislature to make laws on these issues.

Courts in Pakistan have started deciding cases on the basis of, partly or entirely, on digital evidence. Although, no specific procedure for the handling of digital evidence has been provided by the legislature. Because of this issue, there should be a legal framework which will define the procedure for identification, collection, preservation, transportation; storage, forensic acquisition, analysis and presentation of digital evidence. In the absence of proper legislation on the subject of digital evidence, nothing can be said about what will be the future of seized digital. As digital evidence can be easily altered, changed and modified. Can it be guaranteed that nothing will be changed with seized evidence? Normally, it is an apprehension in Pakistan, that LEAs personal are not reliable and trustworthy. Then, in absence of proper legislation, nothing can be said about the safety of collected digital evidence that the same shall not be compromised? In addition to this, the procedural law in Pakistan is also silent about the digital evidence that how it will be acquired, preserved, and transported and presented.

1.9 SUMMARY

In every legal or quasi-judicial proceedings evidence plays a significant role. Because of various characteristics of evidence, it can be divided into different types enabling the executive, judiciary and prosecution to understand the nature of evidence. The first thing for the LEAs is to know that how many types are there of evidence? What is digital evidence? If the LEAs are unaware of different types of evidence then how will they collect relevant, reliable, admissible and authentic evidence? Second thing is that what are the sources of digital evidence? Lacking proper knowledge of these sources, will lead the investigator to the collection of unnecessary things and

missing the important evidence. These sources, digital evidence identification, collection, preservation, storage and presentation will be discussed in the light of US Federal legislation and cases of the US Courts. However, Pakistani cases related to cyber-related issues will also be discussed and recommendation will be given in the last chapter for legislation on the subject. As for the law-makers it cannot be expected to predict for the future, therefore, legislation designed for a specific objective may fail when a new situation arises. This is true in existing era when all the previous instrument does not cover many aspects of the digital evidence.

CHAPTER TWO:
DIGITAL EVIDENCE IDENTIFICATION, COLLECTION AND PRESERVATION

2.1 INTRODUCTION

In every investigation, identification, collection and preservations of evidence plays an important role. This becomes very difficult in case of digital evidence. Therefore, this chapter elaborates the identification, creation, and collection of digital evidence. In this respect different methods and approaches of digital evidence collection will also be explained in some details. Moreover, in the process of seizing digital evidence, investigator can face many seizure issues and errors, and various errors can occur in this process as well, thus, this aspect will also be highlighted in some detail. Besides, there are certain challenges and problems which are faced by the examiner during the process, hence, to some extent, these will also be discussed along with forensic imaging.

2.2 IDENTIFICATION OF DIGITAL EVIDENCE

Acquiring of evidence begins with identifying the crime scene. Identification of crime scene in cybercrime cases is not an easy job as the cyberspace may have international aspects attached to it. Identification of sources of digital evidence is important before starting collection of digital evidence (these sources have been discussed in chapter no.1). However, there are various challenges associated in identification and collection of Electronically Stored Information (ESI), as there are variety of digital storage devices. The LEAs or investigator by a comprehensive mechanism, diligent investigation and examination will be able to identify all important ESI in preparation for collection and preservation of digital evidence. Johnson says that the

> first step in gathering evidence is identifying possible sources of evidence for collection. It is fairly common that identified evidence includes too little or too much information. If too much is identified, then search and seizure limitations may be exceeded, whereas if too little is identified, then exculpatory or inculpatory evidence may be missed.[1]

Imagine a situation where investigator is assigned a task to investigate a crime, let say fraud. When the investigator enters the office, he finds twenty computer, ten backup hard drives, fifty CDs, ten USBs and ten DVDs. Without examining these devices, the investigator will not be able to know where the relevant information or data is stored. Each device may be using different operating system, searching every device can be time consuming and searching all of them at the crime scene will be more complicated. Thus, it is very important for investigator to identify the potential sources of digital evidence.

Investigator requires the proper assistance and help from the management of the organization or the owner of the digital device "to make a determination as to exactly what might be a source of evidence."[2] These sources can be either electronic or manual and these includes but not limited to PDAs, pagers, mobile phones, memory cards, laptops, hard drives and storage area networks (SANs).

Before evidence gathering, it is important for the investigator to identify which documents are to be collected. In other words, what, where, when, whose and how is important for identification of evidence gathering. What type of evidence is required? Where is the evidence located? When the crime was committed? It means what period is required? Whose data is relevant? As in digital environment, many people are working in an office, therefore, it is necessary for the investigator to specify and indicate the specific person from whose data is to be collected

---

[1] Johnson, *Forensic Computer Crime Investigation,* 152.

[2] Marcella and Menendez, *Cyber Forensics*, 5-6.

and lastly how the digital evidence will be collected? The investigator should observe, at least, these things while collecting evidence.[3]

Digital evidence is fragile and it can easily be manipulated, changed, modified, encrypted, and destroyed, making the job more difficult for the investigator to identify the relevant evidence. In addition to this, digital "evidence is comprised of three main elements, the first being binary data, the second being a storage device on which to store that binary data and thirdly, software to read and interpret the binary data."[4]

Digital evidence may be altered, changed or modified by the criminals to remove all traces of its existence on computer, mobile phone and computing devices. Making more difficult for the investigator to trace "evidence of such modification may not always be possible to identify."[5] Criminal use sophisticated techniques to alter the digital information. Therefore, it is an established fact that "digital evidence may be modified without leaving any obvious trace of the commission of a transgression."[6] Therefore, LEAs requires expertise and considerable efforts to identify the modification of evidence.

2.3 DIGITAL EVIDENCE COLLECTION

When a crime is committed on cyber-space, the investigator's job starts and the most important thing in investigation is 'preservation of data', which is recovered from the crime scene or the tool which is used for committing the crime. In many cases, the criminal may destroy the evidence, therefore, it is necessary for the investigator to know how to recover the destroyed or

[3] Allison Rebecca Stanfield, "The Authentication of Electronic Evidence," (Ph.D. diss., Queensland University of Technology, 2016), 124.

[4] Stanfield, "The Authentication of Electronic Evidence," 4.

[5] Boddington, *Practical Digital Forensics,* 72.

[6] Ibid., 296.

deleted data. Whereas, in case, when the investigator is unable to recover the destroyed or deleted data or files, he may not be able to proceed with the investigation. In fact, the investigator makes maximum efforts, as much as possible to recover deleted data or files. Thus, the process of "acquiring, examining, and applying digital evidence is crucial to the success of prosecuting a cyber-criminal, with the continuous evolution of technology, it is difficult for LEAs and computer professionals to stay one step ahead of technologically savvy criminals."[7]

The most important thing in investigation of any crime is collection of evidence and preservation of the same. Every type of evidence is difficult to "collect at the best of times, but when that evidence is in electronic form, an investigator faces some extra complexities, as it has none of the permanence that conventional evidence has."[8] Stating it differently, the collection of electronic evidence is "very expensive to collect, the processes are strict and exhaustive, the systems affected may be unavailable for regular use for a long period of time, and analysis of the data collected must be performed."[9] In many cases, the victim is unaware of fraud, and sometime the LEA are informed too late which creates several obstacles for the investigator to properly investigate the case and collect the relevant evidence to prosecute the lawbreakers. Evidence can be useful information "for resolving a dispute, or completely worthless, depending on its reliability."[10]

Electronic crime is difficult to "investigate and prosecute, investigators have to build their case purely on any records left after the transactions have been completed."[11] In addition, electronic records are very malleable and electronic transactions currently have fewer limitations,

---

[7] Vacca, *Computer Forensics: Computer Crime Scene Investigation*, 4.
[8] Ibid., 217.
[9] Ibid.
[10] Ann D. Zigler and Ernesto F. Rojas, *Preserving Electronic Evidence for Trial a team approach to the Litigation Hold, Data Collection, and Evidence Preservation* (New York: Elsevier Inc., 2016), xiv.
[11] Vacca, *Computer Forensics: Computer Crime Scene Investigation*, 218.

which make it further difficult to investigate properly as computer records can be straightforwardly modified or destroyed. Moreover, computer transactions are very much fast, "they can be conducted from anywhere, can be encrypted or anonymous, and have no intrinsic identifying features such as handwriting and signatures to identify those responsible."[12]

Digital evidence can provide a rich treasure chest of clues about a transgression and a "clue may be considered a mistake by another name, and finding and interpreting them is what really adds to the excitement of a forensic examination. Analyzing digital evidence can be rewarding, disappointing, and often a frustrating process, but a greater understanding is always gained."[13]

In Pakistan, many problems are being faced by the investigator and LEAs, even if the details of the "transactions can be restored through analysis, it is very difficult to tie the transaction to a person."[14] Such information merely shows that "whoever did it either knew or could get past those identifiers, as the identifying information (such as passwords or PIN numbers or any other electronic identifier) does not prove who was responsible for the transaction."[15] As everyone knows that technology is "constantly evolving, investigating electronic crimes will always be difficult because of the ease of altering the data and the fact that transactions may be done anonymously."[16] The best way for the investigator is to adopt rules of evidence collection and be as diligent as possible.

In Pakistani legal system, evidence collection by the police officer (i.e. Investigation Officer) or any authorized person is considered as Investigation.[17] Collection of evidence, in other words, is not defined anywhere in the Pakistani legal system except the Cr.P.C. Whereas collection

---

[12] Ibid., 219.
[13] Boddington, *Practical Digital Forensics*, 23.
[14] Vacca, *Computer Forensics: Computer Crime Scene Investigation*, 219.
[15] Ibid.
[16] Ibid.
[17] Section 4(l) of the CrPC, 1898.

of evidence, in civil, criminal and corporate affairs, is difficult but when the evidence is in digital or electronic form, it proves more difficulties for investigator to collect the digital data due to some extra complexities attached to the digital evidence. Before accepting any evidence as admissible, it is the responsibility of the courts to check whether the evidence is admissible, relevant, authentic, and original, not modified or altered, not a copy and not hearsay. Generally, it is considered that the collection of digital evidence is very expensive and needs strict and exhaustive processes to collect the digital data and artifacts. There are two reasons for this; one is future prevention (as someone broke your door and steal few goods from your home, you will put lock to avoid future theft) and second is responsibility (as to assign the responsibility on wrong doer).[18]

While collecting digital evidence, the investigator should try to proceed from the most volatile to the least, avoiding the loss of evidence. If there is no prescribed procedure, or defined procedures are lacking the requirements of digital era or law for recovery, collection, storage, preservation, examination and protection of digital evidence, then the criminal are likely to go unpunished and the efforts made by the LEAs will be wasted and of no use. As it is not difficult to change, manipulate and destroy electronic information or data. Hence, digital evidence collection, and its admission in the courts for effective trial in cybercrimes is very difficult due to technical nature of the crimes and for want of expertise.

Because of its very nature, digital evidence is fragile, and sensitive to "extreme temperatures, humidity, physical shock, static electricity, and magnetic fields,"[19] therefore, it can be "altered, damaged, or destroyed by improper handling or improper examination."[20]

---

[18] Vacca, *Computer Forensics: Computer Crime Scene Investigation*, 218.
[19] National Institute of Justice, *Electronic Crime Scene Investigation*, 31.
[20] Marcella and Menendez. *Cyber Forensics*, 287.

Consequently, special expertise and precautions are required to be followed to document, collect, preserve, transport, examine and present this type of evidence. Otherwise, this evidence may be unusable or of no value for the LEAs. Thus, once the digital data has been collected properly,

> it must be protected from contamination. Originals should never be used in forensic examination; verified duplicates should be used. This not only ensures that the original data remains clean, but also enables examiners to try more dangerous, potentially data-corrupting tests. Of course, any tests done should be done on a clean, isolated host machine.[21]

Attribution of specific role is very important in digital investigation. Whether the entire computer should be collected, in case of few pieces of digital data? Or the relevant data should be copied? Casey explains as under:

> When a computer contains only a few pieces of digital evidence, investigators might not be authorized to collect the entire computer. However, when a computer is the key piece of evidence in an investigation and contains a large amount of digital evidence, it is often necessary to collect the entire computer and its contents. Additionally, when a computer plays a significant role in a crime, it is easier to obtain a warrant to search and seize the entire computer.[22]

Most of the digital evidence is collected electronically i.e. through electromagnetic emanations. Consequently, it is imperative for the investigator to establish that the evidence is collected from a particular system meaning thereby that the proper chain of custody is maintained by the investigator as held by the Supreme Court of Pakistan in *Ishtiaq Ahmed Mirza v. Federation of Pakistan*.[23] Thereafter, the investigator make sure that the person is himself using the said system as the passwords can be stolen or shared by the individual making it more difficult that who used the system at given time. So, the investigator should establish the presence of the alleged accused.

---

[21] Vacca, *Computer Forensics: Computer Crime Scene Investigation*, 228.
[22] Casey, *Digital Evidence and Computer Crime*, 39.
[23] *Ishtiaq Ahmed Mirza v. Federation of Pakistan*, PLD 2019 SC 675.

Typical audit trails are also important in digital evidence which includes "the date and time of creation, last use, and/or modification as well as identification information such as program names, function performed, user names, owners, groups, IP addresses, port numbers, protocol types, portions or all of the content, and protection settings."[24] This type of information will make the case strong otherwise, it may be very difficult for the prosecution to prove the case in the competent court.

As discussed, proper chain of custody should be maintained properly by the investigator, if the same is not done, there are reasonable questions about the authenticity of the evidence collected. All the records do not exist in proper order on all systems. Therefore, due to various reasons, "some records get lost, others end up out of order, and times fluctuate to some extent."[25] So instead of providing paper copy of the digital evidence, the more accurate evidence, the original copy of the device should be provided in the court.

Certain legal requirements must be met in digital evidence collection. However, such requirements in any legal system are "vast, complex, and vary from country to country."[26] In Pakistan, in criminal matter, section 154 till section 176 of CrPC deals with evidence collection and presentation in courts. As per CrPC investigation "includes all the proceedings under this Code for the collection of evidence conducted by a police officer or by any person (other than a Magistrate) who is authorized by a Magistrate in this behalf."[27] Section 1732 of the US Code provides that log files are admissible in evidence if these files are collected "in the regular course of business or activity has kept or recorded."[28] Besides, FRE provides that logs, which "might

[24] Johnson, *Forensic Computer Crime Investigation,* 155.
[25] Ibid.,156.
[26] Vacca, *Computer Forensics: Computer Crime Scene Investigation*, 247.
[27] Section 4 (l) of the Code of Criminal Procedure, 1898 (Act No. V of 1898).
[28] U.S.C 28, section 1732.

otherwise be considered hearsay, are admissible as long as they are collected in the course of regularly conducted business activity."[29]

There are many faults which can occur during the digital evidence collection. Therefore, investigator must be aware of these faults, these includes "process failures or inaccuracies, missed opportunities caused by inadequate collection technology or skill, missed relationships, missed timing information, missed location information, missed locations containing information, missed corroborating content, and missed consistencies."[30]

The investigator should also make ensure that evidence collected is "properly documented, labeled, marked, photographed, video recorded or sketched, and inventoried before it is packaged."[31] He should also ensure that all connected devices and equipment are clearly and properly labeled, digital evidence in packed[32] in antistatic bags. While collecting mobile phone, her status should not be changed. If that is on then leave it on.[33] Casey says that

> Failures to collect digital evidence have undermined investigations, preventing the apprehension or prosecution of offenders and wasting valuable resources on cases abandoned due to faulty evidence. If this situation is not corrected, the field will not develop to its full potential, justice will not be served, and we risk a crisis that could discredit the field.[34]

The investigator should also collect storage devices, networked computer contents, deleted file areas from disks, and other similar data. Thereafter, he must also ensure that the collected evidence is stored "in a secure, climate-controlled environment or a location that is not subject to

---

[29] Rule 803(6) of the Federal Rules of Evidence.

[30] Johnson, *Forensic Computer Crime Investigation*, 164.

[31] National Institute of Justice, *Electronic Crime Scene Investigation*, 31.

[32] For packing digital evidence, investigator should only use approved evidence containers such as bags, envelopes and other digital evidence container which are specifically designed for the purpose. Otherwise, evidence may loss, its value. Nonetheless, while collecting digital evidence, the investigator must not use plastic materials which may damage or destroy the evidence.

[33] National Institute of Justice, *Electronic Crime Scene Investigation*, 32.

[34] Casey, *Digital Evidence and Computer Crime*, 11.

extreme temperature or humidity."[35] Besides, he also ensures that the digital evidence is "not exposed to magnetic fields, moisture, dust, vibration, or any other elements that may damage or destroy it."[36]

Collection of digital evidence stored in cloud system is difficult due to various legal constrains. *Microsoft v. United States,*[37] is classic example of cloud computing, which is discussed in chapter 6 and 8 respectively. Various methods have been adopted by the forensic examiners and investigators for collection of digital evidence. These are discussed briefly.

2.3.1 METHODS OF DIGITAL EVIDENCE COLLECTION

Basic rule of law of evidence are followed in cases where digital evidence is involved. However, there are some specific rules, in addition to these rules, as any other investigation of civil, corporate or criminal matter. However, in digital evidence, it is imperative for the investigator that "collection should be done with the least detriment to its condition."[38] Instead of working on the original storage device, it is preferable for the investigator to work on a copy, of the original evidence, to prevent damage or changing the original evidence.[39]

Collection, by the investigator, is the process of actually gathering the digital evidence, "which will eventually be copied several times, using specialty software and hardware. This copying process allow the investigator to work on and examine an identical, forensically sound,

---

[35] National Institute of Justice, *Electronic Crime Scene Investigation,* 32.

[36] Ibid.

[37] *Microsoft v. United States,* No. 14-2985 (2d Cir. 2016).

[38] Brett Shavers, *Placing the Suspect behind the Keyboard Using Digital Forensics and Investigative Techniques to Identify Cybercrime Suspects* (New York: Elsevier, 2013), 2.

[39] Shavers, *Placing the Suspect behind the Keyboard,* 2.

yet duplicate copy of the original electronic evidence."[40] Digital evidence should be collected in a forensically sound manner.

Investigator collecting digital evidence should have knowledge about the computer systems "that are running are constantly changing data naturally. These changes may be minimal variations occurring through normal operating system tasks, or the changes can be dramatic depending upon specific programs that may be employed."[41] There are different methods and approaches adopted by forensic examiners for digital evidence collection, which are discussed below:

2.3.1.1 FREEZING THE SCENE

There are various methods of evidence collection, among them is freezing the scene which is described as "taking a snapshot of the system in its compromised state."[42] At the earliest, the investigator, without wasting the precious time, must start collecting the data in a standard format. Besides, the investigator should make sure that "the programs and utilities used to collect the data are also collected onto the same media as the data. All data collected should have a cryptographic message digest created, and those digests should be compared to the originals for verification."[43]

2.3.1.2 HONEYPOTTING

Honeypotting is described as "the process of creating a replica system and luring the attacker into it for further monitoring."[44] While performing honeypotting the investigator should

---

[40] Marcella and Menendez. *Cyber Forensics,* 287.
[41] Shavers, *Placing the Suspect behind the Keyboard*, 3.
[42] Vacca, *Computer Forensics: Computer Crime Scene Investigation*, 225.
[43] Ibid., 226.
[44] Vacca, *Computer Forensics: Computer Crime Scene Investigation*, 226.

make sure that "any data on the system related to the attacker's detection and actions is either removed or encrypted; otherwise they can cover their tracks by destroying it. Honeypotting and sandboxing are extremely resource intensive, so they may be infeasible to perform."[45]

2.3.1.3 SIMPLE FILE COPYING

Copying the files is described as by dragging the files "from the evidence computer to an external hard drive."[46] This is very simple method, but forensically this is not sound as this "will alter the metadata of the files and if the evidence computer is live, then the data on that system will also be altered."[47] In such like circumstances, where only file copying is necessary, then it is the responsibility of the investigator to maintain the original metadata by using the specialized software. Nonetheless, in computer forensic, simple file copying is not the accepted method for digital evidence collection.[48]

Thus, copying files by the forensic examiner or investigator through drag and dropping files is the less complete method of data collection. In this method, investigator should keep in mind that he has only "one chance to collect the evidence reasonably. Every other attempt on a live machine results in the original evidence being higher at risk of modification."[49]

2.3.1.4 DEAD BOX APPROACHES

Sometimes when the investigators reach at the crime scene they find that computer systems are not running ("dead"). Keeping in view the nature of digital evidence, investigators do not turn

---

[45] Ibid.
[46] Shavers, *Placing the Suspect behind the Keyboard*, 4.
[47] Ibid.
[48] Ibid.
[49] Ibid., 5.

on the computer, but just they image the computer by using "write protection to the evidence hard drive. Sometimes, it may be a necessary and acceptable practice to boot the system and create a forensic image from the live system."[50] Forensic imaging is discussed in detail at the end of this chapter. Dead box images are created by "removing the hard drive and then connecting it to a hardware write blocker or booting into a forensic operating system."[51] Besides, this approach also applies to "digital media that is not connected to a computer system, such as external hard drives, USB flash drives, compact disks, and other small media."[52]

2.3.1.5 LIVE BOX APPROACHES

Sometimes when the investigators reach at the crime scene they find that computer systems are running, this is called live box approach. Running computer creates a time sensitive situation "in which a decision must be made as to the method of data collection."[53] Resultantly, it is imperative for the investigator to make fast decision, as due to running of operating system may change the data on the evidence drive.

2.4 DIGITAL EVIDENCE SEARCH AND SEIZURE ISSUES AND ERRORS

As discussed, that digital evidence collection, storage, packaging and transportation requires special attentions as the same can be changed, altered, modified or damaged from "electromagnetic fields such as those generated by static electricity, magnets, radio transmitters, and other devices."[54]

---

[50] Shavers, *Placing the Suspect behind the Keyboard*, 5.
[51] Ibid.
[52] Ibid.
[53] Ibid., 10.
[54] Marcella and Menendez. *Cyber Forensics*, 287.

For collection of digital evidence from crime scenes, the search and seizure of computers or other digital device by the LEAs or investigators should be done within the prescribed limits of a lawful search and seizure.[55] The investigator searching a computer "must be sufficiently trained and educated in the use of appropriate software utilities used in scanning hard drives"[56] or other digital devices. Computer and digital device are dealt differently, therefore, the Tenth Circuit Court, in *United States v. Walser*, held as under:

> The advent of the electronic age and... the development of desktop computers that are able to hold the equivalent of a library's worth of information, go beyond the established categories of constitutional doctrine. Analogies to other physical objects, such as dressers or file cabinets, do not often inform the situations we now face as judges when applying search and seizure law. This does not, of course, mean that the Fourth Amendment does not apply to computers and cyberspace. Rather, we must acknowledge the key differences and proceed accordingly.[57]

The computer is "evidence" only to the extent that some of the data it stores is evidence. In the case of *United States v. Giberson,*[58] the Ninth Circuit Court held that "computers, like briefcases and cassette tapes, can be repositories for documents and records." Criminals and suspects can easily change the "date created" entry for file to any arbitrary value by using *Bulk File Changer,*[59] or any other software program. Therefore, while seizing any digital device, the investigator should also keep this aspect in mind

It is important for the investigators to secure the crime scene by moving away all the irrelevant people from the targeted computers and digital devices which will assure that the equipment is fully protected. For not following the basic safely principle, valid evidence may be

---

[55] In section 35 (3) of the PECA, it is stated that "When seizing or securing any data or information system, the authorized officer shall make all efforts to use technical measures to maintain its integrity and chain of custody."

[56] Johnson, *Forensic Computer Crime Investigation,* 8.

[57] *United States v. Walser,* 275 F.3d 981 (10th Cir. 2001) at 986.

[58] *United States v. Giberson,* 527 F.3d 882, 887 (9th Cir. 2008).

[59] This software is freely available on the internet.

lost by the investigator. However, there are various issues faced by the investigators while seizing the evidence and sometimes error can occur while collecting digital evidence. These, are discussed below.

2.4.1 DIGITAL EVIDENCE SEIZURE

It is important for the investigator to discover the computer containing the relevant data and source of content to be seized. The investigator searching for digital evidence will, at some time, may lead to various concealed different devices connected to a network or computer, in a wide variety of ways. It is not possible to collect every piece of evidence, especially when the same is intentionally concealed by the author of the evidence while using different techniques thus creating difficulties for the investigator what to seize? Therefore, the investigator should seize the following equipment "the main system box, monitor, keyboard, mouse, leads and cables, power supplies, connectors, modems, floppy disks, DATs, tapes, Jazz and Zip disks and drives, CDs, hard disks, manuals and software, papers, circuit boards, keys, printers, printouts, and printer paper."[60] In addition to these items the investigator should also seize the following items containing digital evidence, "mobile phones, pagers, organizers, palm computers, land-line telephones, answering machines, audio tapes and recorders, digital cameras, PCMCIA cards, integrated circuits, credit cards, smart cards, facsimile machines, and dictating machines."[61] Every item mentioned above may have some or a lot of important evidence and the same may be beneficial for operating the system again. So, a good rule of thumb is, "If in doubt, seize it."[62]

---

[60] Johnson, *Forensic Computer Crime Investigation*, 154.
[61] Ibid.
[62] Johnson, *Forensic Computer Crime Investigation*, 154.

The investigator should also photograph the screen or note its content, the printing (if any) should continue to finish, and the device ought to be "powered off by pulling out all plugs."[63] In *Soldal v. Cook County,* the Court held that "seizure" constitutes an interference with somebody's possession and property.[64] Therefore, any interference with any digital device is a seizure. The investigator, while seizing any digital object should observe the constitutional and statutory obligation. However, the investigator should not change the computer mode, if the system is running do not switch off and if the operating system is off do not switch on. This is discussed in more detail in coming sections.

Johnson has described a comprehensive list, which should be observed by the investigator, he says:

> The investigator should label and photograph or videotape all components; remove and label all connection cables; remove all equipment, label, and record details; and note serial numbers and other identifying information associated with each component. The area should be searched for diaries, notebooks, papers, and for passwords or other similar notes. The user should be asked for any passwords, and these should be recorded.[65]

In addition to above mentioned list, the investigator should also gather all associated documents and relevant material present at the crime scene. If the user is present at the crime scene, passwords of the device may be asked and if the system is encrypted then the encryption key may also be obtained.[66] Moreover, the investigator should also ensure that serial numbers of the devices are correctly recorded, if serial numbers are missing or incorrect, so this will destroy the chain of evidence by creating various challenges such as what was actually present at the crime scene.

---

[63] Ibid., 163.

[64] *Soldal v. Cook County*, 506 U.S. 56 (1992).

[65] Johnson, *Forensic Computer Crime Investigation,* 163-164.

[66] Angus M. Marshall. *Digital Forensics Digital Evidence in Criminal Investigation* (West Sussex: John Wiley & Sons, Ltd, 2008), 26.

Generally, in every office, computers are networked, if this is so, then this becomes a more complex issue for the investigator. Therefore, he needs to adopt extra measures for collection of digital evidence. As the criminals knowing that the investigation is being carried out, may destroy the data remotely. Brown has discussed in detail, in the following words:

> Today most any computer seized involves a network environment of some type. Even home computer seizures can involve complex local area networks (LANs), wide area networks (WANs), virtual private networks (VPNs), wireless local area networks (WLANs), and even personal area network (PANs) using Bluetooth technologies.[67]Walking around any national electronics store that specializes in computers these days, an investigator will see network-attached storage (NAS), firewalls, Gigabit Ethernet, and other advanced networking technologies being marketed to home users.[68]

2.3.2 SEIZURE ISSUES

After identification of the digital devices, it is not fair and legal, without adopting the due process of law and following the prescribed guidelines and instruction for seizing of electronic devices, for the investigator to seize the equipment immediately as the devices may be vital for the business entity. Thus due "care must be taken to ensure that any seizure is justified, appropriate and proportionate."[69] Otherwise, this exercise will be fatal and negate the whole efforts. Therefore, investigator must link the relevant evidence related to the activity. Besides, any item seized "must be a major source of material and any problems presented by its seizure must be outweighed by its value in the investigation."[70]

While seizing digital device any interface with a device may cause changes to the device. This is alarming situation for authentication of evidence. If interface with the seized device is

---

[67] Christopher L.T. Brown. *Computer Evidence: Collection and Preservation,* 2nd ed. (Boston: Course Technology PTR, 2010), 96.

[68] Brown, *Computer Evidence: Collection and Preservation*, 96.

[69] Marshall, *Digital Forensics Digital Evidence in Criminal Investigation*, 21.

[70] Ibid.

established, then the integrity of "all data on that device can be challenged, effectively accusing someone involved in handling the device of tampering with it."[71]

Nowadays, it is common that the LEAs during the arrest of suspects, seize their mobile phones as well. Later on, these phones are examined for evidence collection. Question arise "whether the police can, without a warrant, search digital information on a cell phone seized from an individual who has been arrested?" In *Riley v. California*,[72] the US Supreme Court in the warrantless search and seizure of the contents of a mobile phone held that an arrest is unconstitutional without search warrant. Therefore, now it is necessary for LEAs to obtain separate search warrant to examine the seized phone.

Sometimes investigators observe a screensaver on the computer. Whether this should be allowed to continue the operation or instantly stop running? As we do not know what "the safe way of stopping the screensaver is, it should be allowed to continue running, even if it starts during the seizure process."[73] The investigators should also remember that screensaver is another program in the device, which is "capable of running other programs designed to cause damage."[74] So, it must be careful about the screensaver. Otherwise, collected evidence may cause problems for the investigators during the trial.

2.3.3 SEIZURE ERRORS

Under the PECA, 2016, in Pakistan, the investigator has been authorized to search or seize the information system, device or data,[75] and if the investigator has entered any premises without

---

[71] Marshall, *Digital Forensics Digital Evidence in Criminal Investigation*, 30.

[72] *Riley v. California*, 573 U.S. 373 (2014). This is a landmark judgement of the United States Supreme Court on seizure of mobile phones.

[73] Marshall, *Digital Forensics Digital Evidence in Criminal Investigation*, 22.

[74] Ibid., 22.

[75] Section 22 of PECA, 2016.

obtaining the search warrant, in which the search warrant was required, he will report to the court within twenty-four hours from the entrance of the premises, and seizure of any information system, device or data.[76] In digital evidence seizure process, there is possibility of various errors which can occur during this process. Thus, these errors cannot be ignored, otherwise these may lead to challenging the veracity of it.

Under the PECA, 2016, procedure for search and seizure has been provided for the seizure of information system, device, data or storage medium[77] and it is provided in this Act that the investigator will make a list of the seized items, give a copy to the parties, and provide a forensic image to the owner of the device or data.[78] If the PECA and other applicable laws applicable to seizure are not adhered, then it will cause challenges for investigator while producing the evidence before courts. Similarly, the investigator will not go beyond the scope envisaged in the warrant. However, whenever any new digital evidence is found by the investigator during the search which is not permitted in the original search warrant or which is not sought in the original search warrant by the investigator and the investigator continues such search before obtaining a new search warrant, this will pose a serious risk in the trial.

Life spam of digital evidence is very short which can easily be destroyed to due to various reasons. In the words of Casey:

> Media containing digital evidence can deteriorate over time or when exposed to fire, water, jet fuel, and toxic chemicals. Errors can also be introduced during the examination and interpretation of digital evidence. Digital evidence examination tools can contain bugs that cause them to represent data incorrectly, and digital evidence examiners can misinterpret data.[79]

[76] Section 22 of PECA, 2016.
[77] Section 33 of PECA, 2016.
[78] Section 36 of PECA, 2016.
[79] Casey, *Digital Evidence and Computer Crime,* 28.

For the first time in Pakistan, through the IFTA, 2013,[80] powers of the LEAs and intelligence agencies were curtailed. The preamble of this Act provides that "for investigation for collection of evidence by means of modern techniques and devices to prevent and effectively deal with scheduled offences and to regulate the powers of the law enforcement and intelligence agencies and for matters connected therewith or ancillary thereto."[81] In keeping the requirement of the existing scenario, the legislator in Pakistani observed in the preamble of IFTA that the existing laws neither "comprehensively provide for nor specifically regulate advance and modern investigative techniques such as covert surveillance and human intelligence, property interference, wiretapping and communication interception that are used extensively in other jurisdictions to successfully prevent the offences and as an indispensable aid to the law enforcement and administration of justice."[82] Through, this Act, the legislator has imposed many restrictions on the LEAs for interception of digital device and regularized the collection of digital evidence.

Many errors occur during the seizure process, in the words of Casey:

> Computers can introduce errors and uncertainty in various ways, including in the time and location of events. The system clock on a computer can be incorrect, and date-time stamps can be interpreted incorrectly. The source IP address of network traffic may be assigned to a proxy device rather than the actual originating computer, and GPS coordinates on a mobile device or satellite navigation system can be inaccurate.[83]

In many security related cases of Pakistan surveillance or interception is used to trace the criminal. Before the enactment of IFTA, these powers were vested arbitrarily with the LEAs but the IFTA has provided a proper mechanism for the scheduled offences.[84] In a case where a wiretap

---

[80] The Investigation for Fair Trial Act 2013 (I of 2013).

[81] Preamble of the Investigation for Fair Trial Act 2013.

[82] IFTA, Preamble.

[83] Casey, *Digital Evidence and Computer Crime,* 69.

[84] As per section 3 (1) of the IFTA these are scheduled offence provided in Schedule I of the Act.

1. The Private Military Organizations Abolition and Prohibition Act, 1974, (IV of 1974) to the extent of terrorist activities;
2. Offences under the Prevention of Anti National Activities Act, 1974 (VII of 1974) to the extent of terrorist activities;

is used, if proper procedure for surveillance or interception is not adopted, then there will be some issues linked with the legitimacy of such a wiretap. Under IFTA, permission for recording of telephonic communication, video recording, interception, obtaining of electronic transaction including SMS and email, and permission for collection of evidence through modern devices has been provided.[85] It is clearly established that without such permission from the competent court, recording of such evidence will not be inadmissible, and the person (LEAs personal) doing the recording may be legally liable for a criminal act under the relevant legislation. The information collected or gathered though adopting the prescribed procedure is admissible in law and have the overriding effect on QSO and CrPC.[86]

2.3.3.1 SHUT DOWN OR NOT?

While seizing the evidence, whether it is recommended to shut down the computer or not? It has lot of significance for seizing the device, as not handling the evidence may lead to lose of the digital evidence. Hence, with the exception of portable devices, "it is recommended that all systems to be seized should be shut down as soon as possible after their discovery."[87] However, operating system's (OS) "shut down" or "halt" command is not a best option, and simply pressing the power button is also not good.

It is very dangerous for the investigator to turn off the "cleanly" during seizure for two main reasons.

---

3. Offences under the Anti-Terrorism Act, 1997 (XXVII of 1997);
4. Offences under the Pakistan Nuclear Regulatory Authority Ordinance, 2001 (III of 2001) to the extent of terrorist activities; and
5. Offences under the National Command Authority Act, 2010 (V of 2010) to the extent of Anti-Terrorism Act, 1997 (XXVII of 1997) only.

[85] Section 16 of the IFTA, 2013.

[86] Section 23 and 38 of the IFTA, 2013.

[87] Marshall, *Digital Forensics Digital Evidence in Criminal Investigation*, 23.

> Firstly, and perhaps most importantly, the O/S shut down is a software process, potentially made up of several programs. Each one of these may cause data to be written to the storage devices. As soon as this happens, ACPO's first principle has been violated and we have created a problem with the integrity of the devices. Secondly, the shut-down process may not be the same on all machines. Because shut down is a software process, it can be modified at will by knowledgeable users. They may, if they choose to, plant programs in the process in order to damage evidence – or worse.[88]

Even shut down for a shorter time may kill the system completely causing damage to the data. The best method, however, is to remove the power directly from the main connection. Although, doing this action has also potential of damaging evidence. Hence, due care is required for treating OS shut down. The suggested process is "to pull the power lead from the socket on the device itself, or as close as possible to the device."[89] Moreover, if anything is under printing or CD or DVD is under the process of writing, then the same may be allowed to finish producing the permanent record of the activity.

Shut down or not is the crucial point in digital evidence collection. Generally, it is suggested that "the investigator should not turn on the computer if it is off, not touch the keyboard if the computer is on, and not take advice from its owner or user."[90] Because if a computer is not in on mode, turning on the computer may alter or destroy the evidence. The investigator should not "pull the power on a running computer."[91] In it is required to turn off the computer then "the correct way to do this would appear to be by switching power off at the wall socket and then removing the plug."[92] Situation is departmental factor in any matter, as per a phrase "Situational

---

[88] Marshall, *Digital Forensics Digital Evidence in Criminal Investigation*, 24.

[89] Ibid., 26.

[90] Johnson, *Forensic Computer Crime Investigation,* 163.

[91] John Sammons, *The Basics of Digital Forensics the Primer for Getting Started in Digital Forensics*. 2nd ed. (Amsterdam: Elsevier, 2015), 58.

[92] Marshall, *Digital Forensics Digital Evidence in Criminal Investigation*, 25.

awareness and experience will win the fight."[93] Thus, the investigator must keep in mind the situation before acting on anything.

If mobile phone is password protected and encrypted than turning down such device "may make it impossible to regain access to the device."[94]

2.5 CHALLENGES AND PROBLEMS OF DIGITAL EVIDENCE

Because of technological advancements and rapid changes in electronic devices, acquiring digital evidence involves specialized skills which are not required for physical evidence collection. In existing legal systems of the world, there are various methods which are being used by the investigators for extracting digital evidence from diverse variety of electronic devices. Still, these devices change rapidly. Therefore, investigators "need to either develop specific technical expertise or rely on experts to do the extraction for them."[95]

Unlike physical evidence, preserving digital evidence is also problematic as this can be easily changed, altered, modified or deleted remotely. Thus, due to the modification in digital evidence, "investigators need to be able to authenticate the evidence, and also provide documentation to prove its integrity."[96]

In the words of Mason and Seng:

> Technology changes rapidly in operating systems, application software and hardware. As a result, data in digital form may reach a point when they cannot be read, understood or used with new software or hardware. For instance, a software company may no longer produce software that is backward compatible or 'downward compatible' Technical

---

[93] Brown, *Computer Evidence: Collection and Preservation*, 60.

[94] Boddington, *Practical Digital Forensics*, 27.

[95] https://i-sight.com/resources/15-types-of-evidence-and-how-to-use-them-in-investigation/ (accessed: 13th July, 2018).

[96] Ibid.

> obsolescence is a major problem that affects every aspect of the legal process, especially because the rate of change has now become so rapid.[97]

Now this is an admitted fact that digital evidence in existing regime can easily be altered, manipulated, changed and destroyed creating new challenges for digital investigators. Thus, digital evidence can be "altered or obliterated either maliciously by offenders or accidentally during collection without leaving any obvious signs of distortion."[98] Therefore, digital evidence creates many challenges for LEAs, prosecution, lawyers, judiciary, digital forensic examiner and analysts. As digital evidence is circumstantial in nature, therefore, it is difficult to attribute to some specific computer activity or to an individual. In some cases, the digital evidence is the sole evidence in any criminal or civil investigation. If a case is established on a single piece of digital evidence then the case is "unacceptably weak" for prosecution point of view. Thus, without providing additional information, "it could be reasonably argued that someone else used the computer at the time."[99] Nowadays, it is common in institutions to use any computer without entering the password as these computers are not password protected or to bypass password protection mechanisms. So, at the time of prosecution, if the defense lawyer is successful in establishing that certain digital evidence was not obtained from the specific system, then this situation will weaken the case to award punishment on the basis of this evidence alone.

More specifically, evidence dynamics create both investigative and legal challenges for digital forensic examiners and legal fraternity, making it further problematic "to determine what occurred and making it more difficult to prove that the evidence is authentic and reliable."[100] There are some special problems attached with computer data as computer data changes every moment

---

[97] Mason and Seng, *Electronic Evidence*, 23.
[98] Casey, *Digital Evidence and Computer Crime,* 26.
[99] Ibid.
[100] Ibid., 28.

which is invisible to human eye, process of data collection may change, and computer technologies are always changing.[101] Besides, digital evidence presents unique challenges which are not found in paper based evidence such as it is "easily modified, volatile, and easily duplicated and dispersed."[102]

Almost every device is now password protected and encryption software are being used to protect the data from unauthorized users. Thus, both are the ultimate challenges faced by the investigators. Although, password protection is straightforward challenge as there are variety of tools "available for obtaining, circumventing, or guessing passwords on different file types."[103] Encryption protected data is very difficult to unlock as "encryption locks data with a key and only people with the appropriate key can unlock the data."[104] Whereas to de-encrypt the encrypted data specialized knowledge and equipment are required.

There are many challenges associated to the computer evidence authenticity, which pose a serious challenge for the LEAs, prosecuting agency, judiciary, forensic expert and the investigators, making it very difficult to understand the exact nature and authenticity of the same. The following are the main challenges:

i. Whether the data was altered?

ii. Whether the program, which was used for generating the data, is reliable?

iii. Identity of the author?

---

[101] Vacca, *Computer Forensics: Computer Crime Scene Investigation*, 19.
[102] Sammons, *Basics of Digital Forensics*, 114.
[103] Casey, *Digital Evidence and Computer Crime,* 458.
[104] Ibid.

The utmost care is exercised by the investigator to avoid the allegation of alteration of data or evidence, while collecting the data the investigator maintains proper chain of custody, document every action performed or taken to reply in case of question regarding the alteration of data, more specifically to counter the challenge of "was the data altered?" Reliability of programs is substantiated in the light of principles set out in the case of *Lorraine v. Markel American Insurance Company.*[105] However, author's identification is often countered with corroboration of circumstantial evidence. Regardless of complexity and detailed nature of computer forensics, instead of drawing the conclusions too quickly, "it is important for forensics investigators to focus on the facts of the collected data in their reports."[106]

There are some programs and processes which cause problems in digital investigation. In the words of Shavers:

> Other problematic programs and processes that will interfere in the collection of evidence include peer-to-peer networking applications, open remote connections, active file deletion or file copying, and active program installations. Closing some programs, such as Internet Explorer, may cause user created data to be written to the drive, which may be beneficial to the examination. Some applications may lose data when they are closed on a running system.[107]

As discussed digital evidence is "identified, collected, transported, stored, analyzed, interpreted, reconstructed, presented, and destroyed through a set of processes."[108] If the process performed during any stage from collection to presentation in the court, which is imperfect, this may cause a challenge. Although, there are valid legal challenges, that needs to be addressed by the presenter of evidence.

---

[105] *Lorraine v. Markel American Insurance Company,* 241 F.R.D. 534 (D. Md. 2007)
[106] Brown, *Computer Evidence: Collection and Preservation*, 21.
[107] Shavers, *Placing the Suspect behind the Keyboard,* 15.
[108] Johnson, *Forensic Computer Crime Investigation,* 149.

Multiply challenges (both legal and political) are faced by LEA which includes access to cross-border data, data retention, lacunas in legal system, an increasingly globalized online environment, lengthy and outdated procedures and practices, lack of proper education and training, lack of proper and up-to-date tools and resource to manage highly expensive investigation and if the evidence is in other country then outdated and lengthy mutual legal assistance practices.[109] In view of emerging requirements of LEAs, legal issues may be addressed by providing legal cover to the issues faced by LEAs. In addition to legal solutions, "professionalisation in the field of digital forensics is necessary."[110] Therefore, proper education and training in imperative.

One of the greatest challenges faced by the LEAs is cloud computing system. Where data is stored in cross-border servers, making more difficult for LEAs to trace and collect the data. Getting access on cloud system, recovering required data, and processing for prosecution is very difficult. Even the US government, after getting search warrant from the competent court, was not able to get evidence from the Microsoft[111] until she enacted the "Clarifying Lawful Overseas Use of Data Act (CLOUD Act, 2018)."

2.6 DIGITAL EVIDENCE CREATION

Every day, without realizing we create digital evidence by using different devices, whenever someone operates his computer, surfers the internet, plays online games, makes a phone

---

[109] In the murder case of Muttahida Qaumi Movement leader Dr. Imran Farooq the UK Central Authority provided copies of the relevant record to the FIA in view of MLA treaty. This process took about two years to get this evidence from UK. The UK agency produced the "original map of the crime scene, post-mortem and forensic reports, CCTV footage of the incident, murder weapons, fingerprints of the accused persons, their passports, details of bank accounts, record related to admission of accused Mohsin Ali in the London Academy of Management Sciences (Lams) and his emails" to the Pakistani Anti-Terrorism Court, Islamabad. https://www.dawn.com/news/1520097 (accessed: 7th April, 2020).

[110] Biasiotti et al. *Handling and Exchanging Electronic Evidence across Europe*, 382.

[111] *Microsoft v. United States,* No. 14-2985 (2d Cir. 2016). US Department of Justice filled appeal to the US Supreme Court. While pendency of the case, US Congress passed the CLOUD Act, 2018, by amending the SCA to resolve controversy of jurisdiction related to the initial warrant.

call, writes an e-mail, or writes a document, takes a ride while using the GPS unit, take a picture or makes a video by using digital cameras, web cams, or shops online or pays bill, all such devices generate some type of digital evidence. Even the copy machine, fax and scanner also contain digital evidence. Moreover, as we see every day, that the CCTV cameras are also a source of digital evidence. In addition to this, credit card and debit card also contains digital evidence. Recently, installed traffic enforcement cameras (these are installed at Lahore and Islamabad, in other cities the installation is under process) are also a source of digital evidence creation, which capture the license plate number and e-challan is directly sent to the vehicle owner.

Nowadays, nothing is immune from creating or storing digital evidence is some prospects, and this can be found on everything "from floppy disks to media cards, solid-state memory sticks, solid-state hard drives, cell phones, network attached storage devices, game consoles, media players, hard drives, and the Internet cloud."[112]

Nowadays various online backup services are available, therefore more and more people are using these services to store their data. Thus, it is becoming more challenging for the investigator to "track down where all the data might reside in a forensic case. And speaking of the cloud, there are now many applications and storage options available through such services."[113] One of the commonly used application is the email. While any e-mail is stored on "mail servers in large databases, on personal computers in the form of personal folder files, offline folder files, or e-mail databases created by the e-mail client being used."[114] Email services are entirely browser-

[112] Larry E. Daniel and Lars E. Daniel. *Digital Forensics for Legal Professionals Understanding Digital Evidence from the Warrant to the Courtroom* (New York: Elsevier, 2012), 5-6.

[113] Daniel et al. *Digital Forensics for Legal Professionals*, 6.

[114] Ibid., 7.

based which can be found in the internet cache, the same can be recovered from the concerned mail provider's server.

Another source of creation of digital evidence is social media, which creates a lot of digital evidence of the activities of the users including the personal information, location and thought of the user can be ascertained. Moreover, several social applications and chatrooms are also source of digital evidence. Today, there are various services which offer users "the ability to chat with one another, both one-on-one via a friends list or in public and private rooms created by the users themselves."[115] Thus, we can safely conclude that digital evidence is everywhere.

2.7 FORENSIC IMAGING

The traditional method used by the forensic examiner is forensic imaging. The forensic image is "a file format that contains every bit of data on the original storage media, such as a hard drive or flash drive."[116] In other words, forensic imaging is a "process of creating an exact bit-for-bit replica of the data stored on an original electronic medium."[117] This process is beneficial in such an aspect that all data on the device is copied including deleted files (file slack) and data residing in unallocated space. Thereafter, a forensic copy of the "original evidence should be made for working purposes, so the original can be secured and remain untouched and any examination is best conducted on a copy of the original evidence."[118] After performing his examination, the forensic examiner "may be required to give evidence of how they have handled the evidence and may have to show that the evidential integrity remains intact."[119]

---

[115] Daniel et al. *Digital Forensics for Legal Professionals*, 8.
[116] Shavers, *Placing the Suspect behind the Keyboard,* 2.
[117] Stanfield, "The Authentication of Electronic Evidence," 125.
[118] Ibid.
[119] Ibid.,125-126.

There are various file formats, which are being used by forensic examiner, such as "Data Description format" (dd) and "Advanced File Format." Forensic examiner chose which format to utilize to copying data from the storage devices. Besides, there are forensic imaging applications, which are being used "in conjunction with a write protection device. Most of these same forensic imaging applications can also be used on a live machine when necessary."[120]

Whether the imaging process can be verified or not? The answer is yes, this process can be "verified using a hash algorithm such as MD5 or SHA-1 which can be used to determine if the image has been tampered."[121]

Digital forensic investigation "will begin by 'imaging' the device on which electronic evidence may reside. The imaging process is a non-destructive process that creates an exact external digital copy of any data on the device."[122] In every investigation, to avoid decay and corruption of original evidence and examination is performed on copy instead of the original. However, the process of imaging should be performed in such a way that accurately reflect the original content, the National Institute of Standards and Technology (NIST) has provided limitations of "imaging hardware and software, as well as standards for forensic imaging."[123] If standards provided by NIST are not fulfilled, then "there may be a challenge to the evidence; however, such challenges can often be defeated if proper experts are properly applied."[124]

By every investigator, in almost every investigation, original evidence device is retained intact. So, if there is a need in future to produce the original artifact, the same may be reimaged

---

[120] Shavers, *Placing the Suspect behind the Keyboard,* 7.
[121] Stanfield, "The Authentication of Electronic Evidence," 125.
[122] Mason and Seng, *Electronic Evidence*, 7.
[123] Johnson, *Forensic Computer Crime Investigation,* 157.
[124] Ibid.

and the full content by examined by the third party to perform the digital forensic process. However, the image "taken with dd is accurate except for that last sector, so all of the evidence provided using it is still accurate."[125] Whereas, the image with "dd is only inaccurate on disks of certain sizes."[126] Almost in every imaging product there is a flaw but according to NIST dd is more accurate.

Johnson has discussed this process in comprehensive manner, the relevant part is reproduced as under:

> Proper technique in forensic imaging starts with a clean palate for the results of the image. Typically, to assure that no evidence is left over from previous content of the media, the media is first cleared of data through a forensically sound erasure process. This is often not done. After clearing of the information, it is common to put a known pattern that is unlikely to appear in normal evidence on the media to later detect failures to properly image the media. After verifying this content is correct, the image is then taken. The original media is cryptographically checksummed, either in parts or as a whole, the image is made, then the result is verified with the cryptographic checksums. The result can be tested for the presence of the identifiable cleared content, and the start and end of the evidence can be clearly verified by these patterns.[127]

If examiner fails any of these steps, this will not invalidate the image, but many question may be raised for authentication of this evidence. When the forensic examiner makes the copy through approved methods, then he analyzes the copy not the original. However, whether "files that were captured as part of the snapshot image were altered prior to the image being taken can be difficult to prove."[128]

In addition to advantages of imaging, there are also some disadvantages. The disadvantage of imaging is that "the process recovers every bit of data from the device being imaged, and

---

[125] Ibid.
[126] Johnson, *Forensic Computer Crime Investigation,* 157.
[127] Ibid., 158.
[128] Mason and Seng, *Electronic Evidence*, 228.

because of the size of the drives, images are now significantly large in size."[129] Why the size is significant? As the whole drives is imaged in forensic process therefore it also contains mostly irrelevant data. This makes imaging difficult and time-consuming. May be, only a small percentage of relevant data be available for the case. Moreover, the forensic practitioner has to travel to the crime scene location "to access the computer device and complete the imaging process by connecting to the device or hard drive."[130] Hence, this also increase the cost and expense.

Another disadvantage is that forensic imaging tools "do not effectively recover evidence from web-based e-mail accounts, Dropbox, or other accounts held in the cloud or other remote locations."[131]

2.8SUMMARY

Due to sensitiveness of the digital evidence, job of investigators is very sensitive. Therefore, he must use cautions while collecting, packing, transporting, or storing digital devices to avoid the alteration, damage or destruction of digital evidence. Collecting digital is not an easy task as specific expertise, training, techniques and software are used for this purpose. Hence, various legal and technical issue such as privacy and collection beyond the border are faced by the investigator. In addition, privacy, search and seizure issues are also faced. Sometime, in this procedure error can also occur making the job of investigator more difficult. Moreover, establishing link with the actual culprit is also difficult. Therefore, laws regarding securing, preserving, retrieving, collecting, packing, storing, presenting and exhibiting of digital evidence

[129] Boddington, *Practical Digital Forensics,* 139.
[130] Ibid.
[131] Ibid.

have to be developed to make ensure that proper chain of custody and integrity of the digital evidence remains forensics.

CHAPTER THREE:

DIGITAL FORENSIC AND AUTHENTICATION OF DIGITAL EVIDENCE

3.1 INTRODUCTION

Different complications are involved in digital evidence authentication. Mainly, all the processes of digital evidence are based upon digital forensic. It cannot be said that there is any discipline which does not require digital forensic. In this chapter digital forensic, its phases, handling of digital evidence is highlights. Thereafter, authentication of digital evidence on computer, websites and email is examined in the light of decisions of courts. At the end, challenges of authentication have also been discussed precisely.

3.2 HISTORY OF DIGITAL FORENSICS

Initially, investigators involving in computer related investigation were only concerned with merely computer or floppy disk. However, due to expansion in networks and the internet this field has grown. Network forensics is "the process of figuring out how a network has been attacked, stopping the attack, and attempting to locate the attacker. The incident response team that performs the network forensics will examine routers, firewalls, server logs, and other data to attempt to remediate and prosecute network intrusions."[1] As the new devices have been introduced by the latest technologies, therefore new areas of digital forensics have also been established. Yet, it is not possible to consider that some piece of digital evidence in available in isolation.

Companies, organizations and institutions, which provide online services to their client and customers, are protecting "their customers' private data stored on their servers by maintaining

[1] Daniel et al. *Digital Forensics for Legal Professionals*, 15.

constant vigilance against attacks. A breach by hackers into a corporate network poses a great financial and reputation risk to any company that is a victim of such an attack."[2] For instance, in Pakistan private banks' data bases were attacked by the hackers and obtained data of their customers. In this case, the private information of millions of customers to these bank was stolen, putting this information at risk "of being used for nefarious purposes by the hackers who breached these networks."[3] A recent case was discussed in the Senate Standing Committee on Interior (in April 2020), and the Chairman directed the FIA "to inquire into the breach and subsequent sale of the personal data of Pakistani mobile phone users on the dark web."[4]

Initially computer forensics was considered a task rather than a profession, as many of these people were from different backgrounds to collect digital artifacts. Nowadays, computer forensics is "a meta-profession comprising the skill sets of several professions and subspecialties, such as law enforcement, information technology, and the legal services field."[5] Now, all over the world, various educational courses have been started in computer forensics.

Originally digital forensics was concerned a single discipline, and the mere focus was on the computer. Because of the technological evolution digital forensics has increasingly moving "towards mobile devices, connectivity has assumed a global dimension and the use of increasingly newer and more complex devices and systems is spreading."[6] The rapid and continuous

---

[2] Daniel et al. *Digital Forensics for Legal Professionals*, 15.

[3] https://www.thenews.com.pk/latest/390450-data-of-major-pakistani-banks-hacked-fia-official (accessed: 6th October, 2019); https://www.dawn.com/news/1443970 (accessed: 6th October, 2019); https://www.pakistantoday.com.pk/2018/11/06/hackers-steal-data-from-almost-all-pakistani-banks-fia/ (accessed: 6th October, 2019).

[4] https://propakistani.pk/2020/04/13/fia-to-investigate-data-breach-of-115-million-pakistani-mobile-phone-users/ (accessed: 14th April, 2020).

[5] Brown, *Computer Evidence: Collection and Preservation*, 4.

[6] Ibid.

technological evolution has developed sub disciplines of digital forensics, including but not limited to computer, mobile, network, memory, and malware forensics.

Computer forensic is an indispensable tool for LEAs for provision of evidence in computer related crimes which plays an important role for prosecution of the criminals in courts and maximizing chances of conviction. Computer forensic is an integral part of digital evidence, without proper understanding the computer forensics, digital evidence cannot be understood in isolation. About the emergence of this, it is stated that "the origins of digital forensics in the public domain emerged later and may be traced back to as early as 1984, when the FBI[7] laboratory and other LEAs started developing programs for examination of computer evidence. Whereas, the computer forensics is "the art and science of applying computer science knowledge and skills to aid the legal process."[8] In other words it is "the discovery, analysis, and reconstruction of evidence extracted from any element of computer systems, computer networks, computer media, and computer peripherals that allow investigators to solve a crime"[9] and it also "involves the preservation, identification, extraction, and documentation of computer evidence stored as data or magnetically encoded information."[10] Later on, this evidence is used as legal evidence in court proceedings.

3.3 DIGITAL FORENSICS

The term "forensics" can be defined as "the application of science to a matter of law."[11] Digital forensics (computer forensics) is "the collection, preservation, analysis, and presentation of electronic evidence for use in a legal matter using forensically sound and generally accepted

---

[7] Federal Bureau of Investigation.

[8] Brown, *Computer Evidence: Collection and Preservation*, 4; Stanfield, "The Authentication of Electronic Evidence," 124.

[9] Vacca, *Computer Forensics: Computer Crime Scene Investigation*, 35.

[10] Ibid., xxv; Marcella and Menendez, *Cyber Forensics*, 5.

[11] Daniel et al, *Digital Forensics for Legal Professionals*, 3.

processes, tools, and practices."[12] It is pertinent to mention here that computer forensics is merely for accepted techniques, tools and technological standards, "but above all focuses on the study of the scientific processes, procedures, technologies and rules to use, develop, adapt or propose to improve the results achievable while at the same time better protecting the integrity of digital evidence."[13]

As computer forensics is the "process of methodically examining computer media (hard disks, diskettes, tapes, etc.) for evidence."[14] As generally people think, that after deleting the files on computer it can-not be recovered or restored, it is not true. *Inter alia*, in computer forensics, it can "often find evidence of, or even completely recover, lost or deleted information, even if the information was intentionally deleted."[15] In digital forensics, the goal is to recover data and interpret the collected information at the maximum level as compared to data recovery, the goal is to retrieve the lost data.

Now turning to its legal aspects. Computer forensics is actually a branch of forensic science concerning to "legal evidence found in computer systems and digital storage medium. It is to perform forensic investigation on digital evidence while maintaining the documented chain of custody so that it can be presented as evidence in the court of law."[16] Stating differently, it is the discipline that "combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law."[17]

---

[12] Ibid.

[13] Biasiotti et al, *Handling and Exchanging Electronic Evidence across Europe*, 6.

[14] Vacca, *Computer Forensics: Computer Crime Scene Investigation*, 4.

[15] Ibid.

[16] http://pfsa.gop.pk/?page_id=20 (accessed: 23rd February 2018).

[17] Marcella and Menendez, *Cyber Forensics*, 5.

The most imperative thing in digital forensics is to "collect, preserve, filter, and present computer system artifacts of potential evidentiary value."[18] Nowadays, in computer forensics various tools are available which enables investigators to examine digital evidence without tampering the same. This is not an easy task that everyone can perform, only specifically trained digital forensics examiners can "reliably preserve data for presentation in court and even recover deleted data, and the legal system is evolving and new procedures being adopted to deal with the special challenges presented by the nature of digital evidence."[19] When the investigators, in criminal investigation, are able to locate the Internet Protocol (IP) address of the accused, then the criminals can be traced easily and by clues they often leave behind them, even the cleverest criminals also leave clues because "they get careless or are arrogant and overly confident."[20]

3.4 PHASES OF COMPUTER FORENSICS

As discussed, that digital forensics is "the application of forensic science to electronic evidence in a legal matter." This includes "collecting, preserving, filtering, and presenting digital artifacts"[21] enabling the LEAs to use for the computer forensics process. These are described as phases of the computer forensics process. There are few important phases in computer forensics which are as under:

i. Acquisition

ii. Preservation

iii. Analysis

iv. Presentation

---

[18] Brown, *Computer Evidence: Collection and Preservation*, 4.

[19] http://www.techrepublic.com/blog/it-security/what-makes-cybercrime-laws-so-difficult-to-enforce/ (accessed: 5th July 2017).

[20] Ibid.

[21] Brown, *Computer Evidence: Collection and Preservation*, 7.

Every phase includes "specific forensic processes and procedures."[22] Therefore, every investigator is responsible for securing the crime scene of electronic crimes besides performing other functions of investigation, from evidence collection to presentation in the courts enabling the courts to decide the matter on the basis of digital data.

3.4.1 ACQUISITION

The first thing in forensic process is collection (also known as acquisition) of evidence which is critical in cyberspace for ensuring the authenticity and integrity of the digital evidence. While evidence collection is the first interaction with the evidence by the first responders or investigators, thus, due care is must, as digital evidence can be damaged or destroyed with mishandling or little negligence. In collection of digital evidence turning on a computer "can lead to the modification of hundreds of evidentiary items including files, date and time stamps, introduction of new Internet history, and the destruction of files that could be recovered from areas of the hard drive that are in the area of unallocated space."[23]

Acquisition of evidence is the basis of any investigation. If the evidence is not collected in accordance with law and accepted standards then what will be the value of such investigation. Therefore, acquisition is the process of collecting digital data for investigation, such as "seizing a computer at a crime scene or taking custody of a computer."[24] In addition to this, making a "forensic copy of a computer hard drive is also acquisition."[25] During the acquisition process, someone may be assigned a task for "gathering associated documents such as notebooks, printed

[22] Daniel et al. *Digital Forensics for Legal Professionals*, 11.
[23] Ibid., 12.
[24] Ibid.
[25] Ibid.

documents etc. that contain notes of passwords or other relevant material."[26] The investigator should also ask about passwords and encryption key from the user.

In the collection phase of digital forensics, artifacts having evidentiary value are identified by the investigator and the same are collected, these are "digital data in the form of disk drives, flash memory drives, or other forms of digital media and data, but they can include supporting artifacts such as corporate security policies, operating manuals, and backup procedures."[27]

Proper documentation in digital forensic has lot of significance, as the authenticity and integrity is based upon the chain of custody such as how the evidence originated and how it was handled by the investigators and examiners. In the process of acquisition, the original evidence can change therefore "any changes should be documented and assessed in the context of the final analytical results."[28] While preserving volatile data, the "digital investigators must document the date and time that data were preserved and the tools that were used."[29]

3.4.2 PRESERVATION

After collection of evidence, the same must be preserved, in accordance with law and accepted procedures, in such state that is defendable in court. Preservation starts prior to collection of evidence and finishes when the evidence is presented in the competent court or destroyed as per law or returned (such as computer, laptop, mobile phone, and other digital devices) to the owner. In other words, chain of custody should be maintained any discontinuity in chain of custody may lead to challenging the authenticity of its validity. Moreover, the investigator should also preserve

---

[26] Marshall, *Digital Forensics Digital Evidence in Criminal Investigation*, 26.
[27] Brown, *Computer Evidence: Collection and Preservation*, 8.
[28] Casey, *Digital Evidence and Computer Crime,* 20.
[29] Ibid.

the evidence "safe from intentional destruction by malicious persons or accidental modification by untrained personnel."[30]

The focus of computer forensic is on preservation of "original artifacts in a way that is reliable, complete, accurate, and verifiable. Cryptographic hashing, checksums, and documentation are all key components of the preservation phase."[31] Even though, in cyberspace environment, preservation of digital evidence is undoubtedly "an identifiable phase, it should be considered iterative throughout the computer forensics process."[32]

3.4.3 ANALYSIS

Analysis (also known as interpretation and filtering) is "the process of locating and collecting evidentiary items from evidence that has been collected in a case."[33] Which evidence will be analyzed by the investigator, depends upon the nature of crime such as in fraud case, the financial records of the organization will be analyzed and in cyber-staking case the email will be analyzed. After all, "the individual skills, tools used, and the training of the forensic examiner have the greatest impact on the outcome of the examination."[34] Digital evidence appears in numerous forms and is available on different devices, thus "the training and experience of the examiner begins to have an ever-greater impact on the success of the examination."[35] Instead of analyzing original data, forensics experts use copies of original data to keep it in original form and avoid alteration during the analysis.

---

[30] Daniel et al, *Digital Forensics for Legal Professionals*, 12.
[31] Brown, *Computer Evidence: Collection and Preservation*, 8.
[32] Ibid.
[33] Daniel et al, *Digital Forensics for Legal Professionals*, 12.
[34] Ibid., 13.
[35] Ibid.

On every digital artifact, forensic analysis is performed to prepare expert report. Therefore, forensic analysis of digital devices may "result in extensive historical records of geolocation points along with the dates and times of each point. Tying these locations of devices to specific persons gives a clear picture of activity and the identity of the suspect in control of the device."[36] In cyber-crime investigation, digital evidence provides many clues about an accused such clue "may be considered a mistake by another name, and finding and interpreting them is what really adds to the excitement of a forensic examination. Analyzing digital evidence can be rewarding, disappointing, and often a frustrating process, but a greater understanding is always gained."[37]

Thus, it can safely be concluded that "the acquisition of technical skills is critical for prosecutors and judges, so they can understand the processes behind the collection and analysis of digital evidence."[38]

3.4.4 PRESENTATION

Presentation is the last phase of computer forensics of digital evidence in which "the potential artifacts of evidentiary value are presented in various forms. Presentation normally starts with artifacts being extracted from original media, moves to staging on temporary digital media, and finally progresses to being organized on CD-ROM or DVDROM."[39] There is no specific pattern or standard of examiner's report. Generally, the forensic examiner's report or findings are written and this may be written "clearly, concisely, and accurately, explaining what was examined, the tools used for the examination, the processes used by the examiner, and the results of that examination."[40] Further, it is the responsibility of the forensic examiner to include in his report the

---

[36] Shavers, *Placing the Suspect behind the Keyboard*, 90.
[37] Boddington, *Practical Digital Forensics*, 23.
[38] Biasiotti et al, *Handling and Exchanging Electronic Evidence Across Europe*, 8
[39] Brown, *Computer Evidence: Collection and Preservation*, 9.
[40] Daniel et al, *Digital Forensics for Legal Professionals*, 13.

collection methods used mentioning the "specific steps taken to protect and preserve the original evidence and how the verification of the evidence was performed."[41] Presentation can be in any form including investigator's reports, "presentations, supporting documentation, declarations, depositions, and testimony in court."[42]

This is not clear from any phase that how much time will be consumed during the entire process and how much time the forensic examiner will take. This is linked with the size of hard drive, if the hard drive is small and have small capacity then it will take "an average of 25 to 35 hours to complete."[43]

3.5 Handling Digital Evidence

In any cyber-crime or computer related investigation, how the investigator will handle the digital evidence? How he will collect digital evidence without any alteration or modification? Whether there is any accepted practice for digital evidence handling, if so, then what is that? These questions have lot of significance in digital crime investigation. These will be discussed in briefly.

As discussed earlier that digital evidence is extremely volatile and can easily be compromised by poor handling or negligence. Therefore, probabilities of effective criminal prosecution by LEAs "depend heavily on the availability of strong evidence."[44] Thus, efforts should be made to keep the digital evidence in its original form. Problems and challenges are also associated with digital evidence as with any other form of evidence, "there are a number of discrete

---

[41] Ibid.

[42] Brown, *Computer Evidence: Collection and Preservation*, 9.

[43] Ibid.

[44] Peter Sommer. *Digital Evidence, Digital Investigations and E-Disclosure: A Guide to Forensic Readiness for Organisations, Security Advisers and Lawyers.* 4th ed. (Swindon: Information Assurance Advisory Council, 2013), 14.

elements that accompany the collection and handling of digital evidence."[45] Consequently, digital evidence professional, LEAs and the investigator should undertake their duties and responsibilities against the highest standards irrespective of the nature of a case.

The handling of digital evidence can be analyzed "from different perspectives, including legal, operational, technical, and data protection, while bearing in mind sociological and other relevant aspects."[46] Investigators are least bother with handling of digital evidence as they are unaware about the nature of digital evidence. Therefore, all perspectives taken by LEAs and investigators are required to be improved related to handling of digital evidence in Pakistan.

It is now not a new phenomenon that the ICT has created new methods of crimes as well as new types of evidence. Although, physical evidence is handled according to criminal procedural and civil procedural laws respectively. However, the new types of evidence, which are born due to ICT, needs "additional and specific ways of handling to maintain the authenticity and integrity of the electronic evidence."[47] Now, it is not disputed that the digital evidence can easily be manipulated as compared to traditional forms of data. Therefore, it must be proved by the prosecution that the digital evidence has not been changed, modified or altered since it was created.

In Pakistan, instrument of legislations on criminal procedure and civil procedure including the law of evidence were enacted before the emergence of existing technologies developments, thus, these issues were not considered then. Consequently, the handling of digital evidence, as well as transportation of evidence between investigator and forensic labs, are based on diverse uncertain criteria, and procedures. What is missing in law of evidence or procedures to guide legislatures,

---

[45] Mason and Seng, *Electronic Evidence*, 287.
[46] Biasiotti et al, *Handling and Exchanging Electronic Evidence across Europe*, 377.
[47] Ibid., 378.

judiciary, LEAs and legal fraternity when dealing with digital evidence handling? No doubt, in Pakistan, there is a need for a strong and comprehensive legal framework and standardized procedures regulating the collection, preservation, analysis, presentation, use and transportation of digital evidence.

3.6 AUTHENTICATION OF DIGITAL EVIDENCE

Courts in Pakistan have applied ETO amendments of the QSO to various cases involving computer, internet or mobile phone, without considering that the amendments brought in QSO through ETO are just applicable to ETO not to any other law, in a similar way to traditional documents. Digital evidence, however, is more voluminous, expressive and readily available. Besides, digital evidence is difficult to destroy, easily modified and duplicated. As such, no court (although the courts have allowed in some circumstance to use e-mails, Automated Teller Machine (ATM) transaction, online transactions, computer generated evidence, Call Detail Records (CDR), Global Positioning System (GPS), Closed-circuit television (CCTV) footage, audio and video recording) in Pakistan has treated digital evidence differently for the purposes of authentication due to lack of proper understanding of digital forensics.

Digital evidence is not like physical traditional evidence, in authentication of digital evidence, it is indispensable to evaluate its trustworthiness. There are various approaches adopted globally, but two approaches for evaluating the authentication of digital evidence is discussed. For instance, the first approach is "to focus on whether the computer that generated the evidence was functioning normally, and the other approach is to examine the actual digital evidence for evidence of tampering and other damage."[48] In *Arif Hashwani v. Sadruddin Hashwani*,[49] the Sindh High

[48] Casey, *Digital Evidence and Computer Crime,* 60.
[49] *Arif Hashwani v. Sadruddin Hashwani,* PLD 2007 Karachi, 448.

Court (SHC) held that "Audio, video-records cassettes CDs are admissible piece of evidence, however, the authenticity of same is always subject to proof in case the party against which it can be used disputed and or denied the authenticity and information contained in the said electronic documents."

Like other types of evidence, authenticity and integrity of digital evidence must also be established, which is critical in digital evidence and challenging. In paper based evidence either the original document was presented in court or original's copy, but in case of electronic documents, somehow, it is very difficult for the examiner to "prove which 'document' is the 'original' since two electronic documents can be identical."[50] The most important part of digital evidence is that it is "dynamic and changeable and this is what gives most concern when it comes to authentication."[51] In cyber-crimes cases, investigators use centuries old procedure for authentication of digital evidence. Instead, the investigators should adopt ICT compatible procedures in which all the relevant data or entire hard drive is hashed.

Three aspects of ICT are important for authentication of digital evidence such a people (creator of evidence), process and the technology (what technology was used). Besides, chain of custody also plays an important role. There are also three challenges to authentication of digital evidence such as who is the author of the document, is the computer program reliable and was the record, after its creation, changed, altered, modified, manipulated or damaged? At least following questions may be asked in relation to computer generated evidence:

i. How reliable is the computer equipment used for the purpose which kept the records and produce the print-out?

[50] Stanfield, "The Authentication of Electronic Evidence," 123.
[51] Ibid., 6.

ii. How reliable is the computer program (including all types of soft wares used)?

iii. How accurate is the program?

iv. Ratio of error in program?

v. How the data was entered?

vi. Whether the data was entered in the normal course of business or otherwise?

vii. Whether adequate measures were taken (or in place) to ensure the accuracy and safety of the digital data?

viii. What was the storing method of data? Whether the storage method is generally accepted or not?

ix. When this printout was made, and how it was prepared?

x. Whether the authenticity of the electronic data has been challenged, if so, on what basis?

xi. Metadata?

In any case, proponent is under obligation to lay the proper foundation of evidence. Whereas courts prime concern is with the reliability evidence. Whether the evidence is reliable or not? As such, "early court decisions required that authentication called for a more comprehensive foundation."[52] Now the question of familiarity of court, particularly, in legislation, in developed countries, with digital evidence is out of context. Thus, the courts have adopted little bit lower standards as held in *United States v. Vela*, that "computer data compilations... should be treated as any other record."[53]

[52] *United States v. Scholle,* 553 F.2d 1109 (8th Cir. 1977).

[53] *United States v. Vela*, 673 F.2d 86 (5th Cir. 1982).

Initially, in the USA, courts have applied the FRE to digital evidence, without realizing important difference between both types of evidence, in a similar way to traditional documents. In 2006, new rules were enacted to accommodate ESI. Digital evidence is often challenged for its authenticity that it can easily be modified.

In the USA, the requirement of authentication is governed by the FRE,[54] which provides that "to satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is."[55] Several examples have been provided under this rule, but these examples are not exclusive. Only genuine evidence is admissible in court. In USA legal system, authentication of evidence is a prerequisite for admitting any document or data into evidence,[56] and the bar for authentication of evidence is not as such high.[57] Though, this rule discusses the requirement of authenticating ESI, but it does not provide procedure for authentication of digital evidence. Nonetheless, this rule just provides some examples that how authentication can be achieved.

In USA, a proponent of evidence should authenticate every evidence through testimony that the evidence "is what it is claimed to be."[58] However, in digital evidence, this process is little bit different. In this case, the witness providing testimony shall be the person who has created the electronic document or who is responsible, under any law or obligation, to maintain the evidence in its electronic form.[59] Therefore, a witness authenticating digital evidence should "provide

---

[54] Rule 901 of FRE.

[55] Ibid.

[56] *United States v. Vayner,* 769 F.3d 125 (2d Cir. 2014); *United States v. Sliker*, 751 F.2d 477 (2d Cir. 1948); *United States v. Maldonado-Rivera*, 922 F.2d 934 (2d Cir. 1990).

[57] *United States v Gagliardi*, 506 F.3d 140 (2d Cir. 2007).

[58] Federal Rules of Evidence, Rule 901(b) (1).

[59] In *United States v. Barlow,* 568 F.3d 215 (5th Cir. 2009), the court held that a chat log was properly "authenticated by the testimony of a witness who participated in, and thus created, the chat."

factual specificity about the process by which the electronically stored information is created, acquired, maintained, and preserved without alteration or change, or the process by which it is produced if the result of a system or process that does so."[60] Whereas failure to provide required testimony in digital evidence may held to be inadmissible.[61] Under FRE, an expert witness can authenticate digital evidence by comparing it to already collected specimens.[62] Initially this rule[63] was not meant for authentication of digital evidence as this was meant for authentication of handwriting and signatures,[64] now this rules has also been applied to authenticate electronic communications.[65]

If it is established that the computer-generated records were changed or modified then the computer-generated records will not be admissible.[66] Besides, for computer-generated records, reliability of the computer program that created the records can also be challenged.[67] Moreover, authenticity of digital evidence can be challenged by questioning the author's identity.[68]

Metadata (discussed in detail in chapter 5) is an integral part of electronic documents. When documents are printed then metadata is invisible. Therefore, it may be ensured by the investigator that the electronic version of documents is available, and if required in future the document can be properly authenticated.

3.6.1 AUTHENTICATION OF DIGITAL EVIDENCE ON COMPUTER

---

[60] *Lorraine v. Markel American Insurance Co.*, 241 F.R.D. 534 (D. Md. 2007).

[61] In *American Express Travel Related Services Co. v. Vinhnee (In re Vinhnee)* 336 B.R. 437 (B.A.P. 9th Cir. 2005), the court held that where "the authenticating witness' testimony was vague, unpersuasive, and conclusory, and demonstrated a lack of knowledge regarding the relevant hardware and software, computer records were not properly authenticated."

[62] FRE, Rule 901(b) (3).

[63] Ibid.

[64] *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534 (D. Md. 2007).

[65] In *United States v. Safavian*, 435 F. Supp. 2d 36 (D.D.C. 2006), the court permitted the authentication of "e-mails by comparison to other e-mails already authenticated" under FRE, rule 901(b)(4)).

[66] *People v. Morrow*, 628 N.E.2d 550 (111. App. 1993).

[67] *Potamkin Cadillac Corp. v. B.R.I. Coverage Corp.*, 38 F.3d 627 (2d Cir. 1994).

[68] *Lenzini v. Columbia Foods*, 829 S.W.2d 482 (Mo. App. 1992).

In court proceedings, showing of the authenticity of digital evidence in crucial, therefore, evidence is not accepted by the courts until or unless same is proved to be authentic to the satisfaction of the court that a complete and true copy of digital evidence was collected from a specific computer and remained unchanged since it was collected by the investigator.

Professor Imwinkelried considered electronic records as scientific evidence and provided eleven-step foundation,[69] which are as under: -

1. The business uses a computer.
2. The computer is reliable.
3. The business has developed a procedure for inserting data into the computer.
4. The procedure has built-in safeguards to ensure accuracy and identify errors.
5. The business keeps the computer in a good state of repair
6. The witness had the computer readout certain data.
7. The witness used the proper procedures to obtain the readout.
8. The computer was in working order at the time the witness obtained the readout.
9. The witness recognizes the exhibit as the readout.
10. The witness explains how he or she recognizes the readout.
11. If the readout contains strange symbols or terms, the witness explains the meaning of the symbols or terms for the trier of fact.[70]

Stanfield criticize these steps that "this statement while helpful at the time to make sense of electronic evidence, is still based on print outs from a computer, and makes no reference to the computer system itself and its integrity."[71]

Question arises whether the acquired evidence is the same as the originally seized media or there is some difference between both of them? Casey says from a technical perspective, "it is not always possible to compare the acquired data with the original. The contents of RAM on a running computer are constantly changing."[72] Network traffic is captured in transit, once it is

---

[69] These points were discussed in *Re: VeeVinhnee,* 336 B.R. 437 (B.A.P, 9th Cir, 2005).

[70] Edward J. Imwinkelreid, *Evidentiary Foundations,* 10th ed. (Durham, North Carolina: Carolina Academic Press, 2018), 87-88.

[71] Stanfield, "The Authentication of Electronic Evidence," 206.

[72] Casey, *Digital Evidence and Computer Crime,* 20.

seized, then "only copies remain and the original data are not available for comparison."[73] This was from technical angle and from legal angle, authentication of evidence is the method for determination whether it is reliable or not. Casey has discussed in the following words: -

> Authentication means satisfying the court that (a) the contents of the record have remained unchanged, (b) that the information in the record does in fact originate from its purported source, whether human or machine, and (c) that extraneous information such as the apparent date of the record is accurate. As with paper records, the necessary degree of authentication may be proved through oral and circumstantial evidence, if available, or via technological features in the system or the record.[74]

Whether mere raising the possibility of tempering is sufficient to challenge the admissibility of digital evidence or some more evidence is required to strengthen the evidence or merely on the allegation of tempering this will lose weight? In *United States v. Allen,*[75] authenticity of digital evidence was challenged and the court found that "Merely raising the possibility of tampering is insufficient to render evidence inadmissible." Furthermore, general allegations of tampering are not sufficient, specific evidence of tampering is required, allegations that "computer records have been altered are applied to their weight, not their admissibility."[76] In *United States v. Bonallo,*[77] the court held that, "The fact that it is possible to alter data contained in a computer is plainly insufficient to establish untrustworthiness."

Before moving to the court for admission of a computer record as an evidence, the proponent should establish that the evidence presented is authentic. As per rule 901 (a),[78] the

[73] Ibid., 20-21.
[74] Casey, *Digital Evidence and Computer Crime,* 21.
[75] *United States v. Allen,* 106 F.3d 695 (6th Cir. 1997).
[76] Brown, *Computer Evidence: Collection and Preservation*, 37.
[77] *United States v. Bonallo,* 858 F.2d 1427 (9th Cir. 1988).
[78] Rule 901 (a) of the FRE.

proponent is required to offer evidence "sufficient to support a finding that [the computer record or other evidence in question] is what the proponent claims it is."[79]

Nonetheless, the "more comprehensive" foundation required by *Scholle*[80] is upright approach. The American Law Reports provides various means to establish this comprehensive foundation. It suggests that the proponent demonstrate "the reliability of the computer equipment," "the manner in which the basic data was initially entered," "the measures taken to ensure the accuracy of the data as entered," "the method of storing the data and the precautions taken to prevent its loss," "the reliability of the computer programs used to process the data," and "the measures taken to verify the accuracy of the program."[81]

Although, witnesses testifying in the court regarding authenticity of computer records is not required special education. Besides, he must not be the person who has programmed the computer himself.[82] Instead, at least, he should have basic knowledge of the relevant facts to which he testifies in the court.[83]

Because of different sources of digital evidence, authentication nature of digital evidence will also differ, depending upon the nature of the evidence, such as pages from the Internet and websites; use of an ATM card or other card; social media sites, e-mails, chat rooms,[84] messengers, social mobile application, instant messages.[85]

---

[79] For more detail on this issue see, *United States vs. Simpson*, 152 F.3d 1241 (10th Cir. 1998).

[80] *United States v. Scholle,* 553 F.2d 1109 (8th Cir. 1977), the court held that "the complex nature of computer storage calls for a more comprehensive foundation."

[81] https://en.wikipedia.org/wiki/Digital_evidence (accessed: 4th April, 2017).

[82] *United States v. Moore,* 923 F.2d 910 (1st Cir. 1991).

[83] In *United States v. Whitaker*, 127 F.3d 595, (7th Cir. 1997), the court held that FBI agent "who was present when the defendant's computer was seized can authenticate seized files"; In *United States v. Moore*, 923 F.2d 910 (1st Cir. 1991), the court held that "head of bank's consumer loan department can authenticate computerized loan data."

[84] *United States v. Simpson*, 152 F.3d 1241 (10th Cir. 1998); *United States v. Tank*, 200 F.3d 627 (9th Cir. 2000); *United States v. Gagliardi*, 506 F.3d 140 (2nd Cir, 2007); *United States v. Barlow*, 568 F.3d 215 (5th Cir. 2009).

[85] *Adams v. Disbennett,* 2008 WL 4615623 (Ohio App. 3 Dist., Oct 20, 2008).

To authenticate digital evidence, the author and the date of creation of document are important. Change of computer's clock is quite easy, therefore, it can easily be changed to give the impression that a curtain document was created on such a date and time, suppose an earlier date. Hence, this will make it extra complex for investigators "to determine who wrote a document and when it was created. However, there are various approaches that forensic analysts can use to authenticate a digital document."[86] He can use various methods and approaches including the date-time stamps "on files and in log files to determine the provenance of a document."[87] False documents can be detected. For example, it is possible "to detect staging and document falsification by looking for chronological inconsistencies in log files and file date-time stamps. Nuances in the way computers maintain different date-time stamps can help forensic analysts reconstruct aspects of the creation and modification of a document."[88]

Courts in USA, in 2007, observed that digital evidence is creating unique set of issues. These issues (admissibility problems of e-mail) were discussed by Judge Grimm in *Lorraine v. Markel.*[89] In many cases, metadata is also be used for establishing the authenticity of digital evidence, as Grimm Judge (USA) noted regarding Federal Rule of Civil Procedure[90] which allows parties to discovery of ESI. Any party can request the court for production of ESI "in its 'native format' which includes the metadata for the electronic document. The metadata shows the date, time and identity of the creator of the electronic record, as well as changes made to it. Accordingly,

---

[86] Casey, *Handbook of Digital Forensics and Investigation*, 31.
[87] Ibid
[88] Ibid.
[89] *Lorraine v. Markel*, 241 F.R.D. 534 (D.Md. May 4, 2007).
[90] Rule 34 of the Federal Rule of Civil Procedure (USA).

metadata is a distinctive characteristic of all electronic evidence that can be used to authenticate"[91] an electronic document under rule 901 (b) (4).

Further the Judge Grimm, in *Lorraine v. Markel*, case quoted the *Weinstein's Federal Evidence Manual* (1997) as follows:

> The need for authentication and an explanation of the computer's processing will depend on the complexity and novelty of the computer processing. There are many states in the development of computer data where error can be introduced, which can adversely affect the accuracy and reliability of the output. Inaccurate results occur most often because of bad or incomplete data inputting, but can also happen when defective software programs are used or stored-data media become corrupted or damaged.
>
> .....Factors that should be considered in evaluating the reliability of computer-based evidence include the error rate in data inputting, and the security of the systems. The degree of foundation required to authenticate computer-based evidence depends on the quality and completeness of the data input, the complexity of the computer processing, the routineness of the computer operation, and the ability to test and verify results of the computer processing.[92]

Grimm Judge stated that a witness must

> "provide factual specificity about the process by which electronic evidence is created, acquired, maintained, and preserved without alteration or change, or the process by which it is produced if the result of a system or process that does so, as opposed to boilerplate, conclusory statements that simply parrot the elements of the business records exception, ... or public record exception."[93]

Grimm Judge recognized this fact that authenticating ESI presents a many concern because "technology changes so rapidly that it is often new to many judges."[94]

3.6.2 AUTHENTICATION OF WEBSITES

Every organization maintains her website for various purpose including but not limited to business, education, entertainment and banking.

---

[91] *Lorraine v. Markel*, 241 F.R.D. 534 (D.Md. May 4, 2007).
[92] *Lorraine v. Markel*, 241 F.R.D. 534 (D.Md. May 4, 2007), at 543 and 544.
[93] Ibid., at 545 and 546.
[94] Ibid., at 544.

In USA, courts authenticating web pages in digital evidence drive powers from "warrant a reasonable person in determining that the evidence is what it purports to be,"[95] through testimony of expert opinion, public records evidence[96] process or system evidence[97] and an official publication is self-authenticating.[98] In *Lorraine v. Markel* case the court suggested some additional factors that should also be considered while authenticating web pages: -

> The length of time the data was posted on the site; whether others report having seen it; whether it remains on the website for the court to verify; whether the data is of a type ordinarily posted on that website or websites of similar entities (e.g. financial information from corporations); whether the owner of the site has elsewhere published the same data, in whole or in part; whether others have published the same data, in whole or in part; whether the data has been republished by others who identify the source of the data as the website in question including length of time that the data was on the site and whether the owner of the data has republished it elsewhere.[99]

In USA, witness's testimony with personal knowledge rule[100] is accepted to authenticate websites, but how much knowledge is required to authenticate? This is to be seen from the court decisions. Dealing with authentication of websites is not an easy task, thus these questions must be answered with respect to websites:

i. What was originally available on the website?

ii. Does the testimony of a witness or exhibits accurately reflect it?

iii. If testimony or exhibits reflects it, then whether the same can be attributed to the website owner or not?

iv. Whether the website was hacked?

---

[95] *United States v. Cameron,* 762 F. Supp. 2d 152, (D. Maine 2011); *United States v. Holmquist*, 36 F.3d 154 (1st Cir. 1994)

[96] Rule 901 (b) (7) of FRE.

[97] Rule 901 (b) (9) of FRE.

[98] Rule 902 (5) of FRE.

[99] *Lorraine v. Markel American Insurance Co.*, 241 F.R.D. 534 (D. Md. 2007).

[100] Rule 901(b) (1) of FRE, which states "that an item is what it is claimed to be."

v. Whether the website was accessed by unauthorized person?

Thus, a witness who testify before the court should authenticate website data by means of showing that the particular person typed in the URL, logged into the website, reviewed what was there on website, and printouts properly and exactly reflects the data. Some courts in USA, however, authenticate website content on the basis of presentation of printouts containing the website URL and the date of printing of web pages.[101] Duty of the lawyers cannot end here, but lawyers are required to "present evidence from a witness with personal knowledge of the website . . . stating that the printout accurately reflects the content of the website and the image of the page on the computer at which the printout was made."[102]

In *St. Luke's Cataract & Laser Inst., P.A. v. Sanderson*,[103] the court rejected affidavits regarding authentication of webpages where deponent lacked personal knowledge of the relevant facts. Similar, view was taken in *Wady v. Provident Life.*[104] In *United States v. Jackson*,[105] the court rejected the evidence on the basis that the "proponent failed to authenticate exhibits taken from an organization's website."

In *Estate of Konell v. Allied Prop*[106] the court held that:

> to authenticate a printout of a web page, the proponent must offer evidence that: (1) the printout accurately reflects the computer image of the web page as of a specified date; (2) the website where the posting appears is owned or controlled by a particular person or

---

[101] *U.S. Equal Employment Opportunity Commission v. E.I. DuPont De Nemours & Co.*, 347 F. Supp. 2d 284 (E.D. La. 2004)

[102] *Toytrackerz, LLC v. Koehler*, No. 08-2297-GLR, 2009 U.S. Dist. LEXIS 74484, (D. Kan. Aug. 21, 2009); *Nightlight Sys., Inc. v. Nitelites Franchise Sys., Inc.*, No. 1:04-CV-2112-CAP, 2007 U.S. Dist. LEXIS 95538, (N.D. Ga. May 11, 2007), the court held that "In addition to a witness with personal knowledge of the web page at issue, to authenticate a printout from a web page, the proponent must present evidence from a percipient witness stating that the printout accurately reflects the content of the page and the image of the page on the computer at which the printout was made."

[103] *St. Luke's Cataract & Laser Inst., P.A. v. Sanderson*, 2006 WL 1320242 (M.D. Fla. May 12, 2006.

[104] *Wady v. Provident Life & Accident Ins. Co. of America*, 216 F. Supp. 2d 1060 (C.D. Cal. 2002).

[105] *United States v. Jackson*, 208 F.3d 633, 638 (7th Cir. 2000).

[106] *Estate of Konell v. Allied Prop. & Cas. Ins. Co.*, 2014 U.S. Dist. LEXIS 10183 (D. Or. Jan. 28, 2014).

entity; and (3) the authorship of the web posting is reasonably attributable to that person or entity.

In *Buzz Off Insect Shield, LLC v. S.C. Johnson*[107] the court held that defendant "could authenticate its printouts of various websites by calling witnesses who could testify that they viewed and printed the information, or supervised others in doing so, and that the printouts were accurate representations of what was displayed on the listed website on the listed day and time."

Whereas, in USA government departments' websites are considered as self-authenticating as per the decision in *Williams v. Long.*[108] In another case of *Paralyzed Veterans of America v. McPherson*, the same view was taken and the court held that documents were self-authenticating from government websites.[109] Whereas in many cases Pakistani courts refused bail on the basis of uploading material on social media such as Facebook. For example, in *Farhan Kamrani v. the State,*[110] bail of the accused was refused on the basis of creating fake Facebook ID of the complaint which was proved through investigation by the FIA on the basis of IP address. Similarly, in *Junaid Arshad v. the State,*[111] the court also refused bail on the basis of evidence collected from cell phone and IP address. Whereas, in Denial Pearl murder case, Pakistani Anti-Terrorism Court convicted the accused persons on the basis of IP address. However, the SHC acquitted the accused persons[112] and the same decision was maintained by the SC.[113]

---

[107] *Buzz Off Insect Shield, LLC v. S.C. Johnson & Son, Inc.*, 2009 U.S. Dist. LEXIS 17530 (M.D.N.C. Mar. 6, 2009.

[108] *Williams v. Long,* 585 F.Supp.2d 679 (D. Md. 2008).

[109] *Paralyzed Veterans of America v. McPherson*, 2008 WL 4183981 (N.D. Cal. Sept. 9, 2008).

[110] *Farhan Kamrani v. the State*, 2018 YLR 329 (Sindh).

[111] *Junaid Arshad v. the State,* 2018 PCrLJ 739 (Lahore).

[112] *Ahmed Omar Sheikh v. the State,* 2021 YLR 1777.

[113] *The State through P.G. Sindh v. Ahmed Omar Sheikh,* 2021 SCMR 873.

3.6.3 AUTHENTICATION OF E-MAIL

Nowadays, everywhere in the world email is being used to correspond and communicate with other entities for personal as well as business purposes. Therefore, it is a great source of evidence and hence it is being used in evidence for proving or disproving the facts, which is routinely being used in evidence. Email is not as such as known mail which is prevailing since centuries. Therefore, email has some distinctive characteristics which are not prevailing in daily mail, which includes "its 'contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances' may be sufficient for authentication."[114]

In cyber-world, proving of authorship of e-mail is very complicated (i.e., who is the author of e-mail), therefore other means (circumstantial evidence) are required to authenticate it. For this purpose, different technical means are available which can be used to trace its origins including assistance from ISPs, cellular network companies, and password of the email. Still, identifying the actual person may not be an easy task.

In USA, rule 901(b) (4)[115] accompanied by rule 901(b) (1)[116] is used for authentication of e-mail messages and other electronic records. Further, under rule 902(7), an email can be self-authenticating and courts have admitted e-mails into evidence.[117]

In *Lorraine v. Markel* case, the court has deliberated on the authentication of e-mail evidence as held as under:

---

[114] *Lorraine v. Markel American Insurance Co.,* 241 F.R.D. 534 (D. Md. 2007).

[115] Rule 901 (b) (4) of the FRE.

[116] Rule 901 (b) (1) of the FRE.

[117] In *United States v. Safavian,* 435 F. Supp. 2d 36 (D.D.C. 2006), the court accepted emails as admissible evidence as "e-mails were properly authenticated by the government"; In *People v. Downin*, 828 N.E.2d 341 (Ill. App. Ct., April 29, 2005), the appellate court held that "the trial court did not abuse its discretion in admitting the e-mail copies into evidence."; in *Kearley v. State,* 843 So. 2d 66 (Miss. Ct. App. 2002), the court accepted the victim's testimony related to the e-mails on her computer; and in *Fenje v. Feld,* 2003 LEXIS 24387 (N.D. Ill., December 8, 2003), the court discussed the standards of authentication of e-mail messages.

> Printouts of e-mail messages ordinarily bear the sender's e-mail address, providing circumstantial evidence that the message was transmitted by the person identified in the e-mail address. In responding to an e-mail message, the person receiving the message may transmit the reply using the computer's reply function, which automatically routes the message to the address from which the original message came. Use of the reply function indicates that the reply message was sent to the sender's listed e-mail address.

Although, e-mail is being used as a common form of correspondence, but it is unique as it does not have signature of any person, which was a common feature in hard copy correspondence. In the past, signatures were the best way to authenticate a document, but the signature are removed in email. Therefore, it is necessary to develop a method of digital signature which is accepted as a replacement of handwritten signature. In Pakistan, ETO has recognized electronic signatures,[118] and has also discussed the proof[119] and presumption of electronic signatures.[120] Resultantly, to prove someone was the real author of an email, either to call the author or use circumstantial evidence. In *Talada v. City of Martinez*,[121] the court held that an e-mail is properly authenticated by the testimony of the sender.

In 2005, first time in the USA legal history, the courts in *International Casings Group Inc v. Premium Standard Forms*,[122] accepted email as a document and the court held that a string of "emails between parties' could be read to infer an agreement and the emails could be read together to locate all the terms of the contract."

Digital data can easily be created, changed, manipulated or forged without apparent detection as it can be forged by any lay person having some basic knowledge, especially criminals adopt this technique to conceal their identity. Therefore, admissibility must be considered in the light of these facts. While forwarding an e-mail, it can be edit easily by the sender without leaving

---

[118] Section 7 of the ETO.
[119] Section 8, Ibid.
[120] Section 9, Ibid.
[121] *Talada v. City of Martinez*, 656 F. Supp. 2d 1147, (N.D. Cal. 2009).
[122] *International Casings Group Inc. v. Premium Standard Forms*, 358 F.Supp.2d 863 (W.D. Mo. 2005).

any sign of edition making it difficult for recipient to detect alterations. Thus, it is a basic requirement of law to establish that "the information system was correctly designed, configured and maintained."[123]

Next issue is whether in criminal investigation forensics expert's report can be relied upon to authentic emails or not? Whether e-mails can be authenticated with already authenticated e-mails or not? In *Kupper v. State,*[124] the court held that e-mails acquired by a qualified computer forensics expert may be used for authentication of emails. Whereas, in *United States v. Safavian,*[125] the court held that comparing an e-mail with other e-mails of the accused already collected and authenticated may serve to authenticate new e-mails under authentication. However, this method is "particularly useful in cases where the sender/recipient's e-mail address does not bear any indicia of identification."[126]

In *New York v. Microsoft Corp.*,[127] the court concluded that how can one person prove that e-mail is what it purports to be? Nonetheless, it is not an easy task to prove or establish the authorship of email messages. Similarly, in *Lorraine v. Markel* case the court held that whatever the offered ESI counsel have to prove its origins and chain of custody of the evidence.[128] Further, the court in *Lorraine v. Markel* observed that "it may be difficult to show that the e-mails are 'kept' for a 'business activity' if they are routinely and automatically deleted without being saved to a

---

[123] https://www.crl.edu/sites/default/files/d6/attachments/pages/Thomson-E-evidence-report.pdf (accessed: 30th November, 2019).

[124] In *Kupper v. State* 2004 WL 60768 (Tex. App. Jan. 14, 2004), the court concluded "that the computer forensic expert's testimony established that the appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with the circumstances, authenticated the computer evidence."

[125] *United States v. Safavian,* 435 F. Supp. 2d 36 (D.D.C. 2006).

[126] Ibid.

[127] *New York v. Microsoft Corp.,* 224 F. Supp. 2d 76 (D.D.C. 2002).

[128] *Lorraine v. Markel American Insurance Co.,* 241 F.R.D. 534 (D. Md. 2007).

file where they will continue to be available for business purposes."[129] Furthermore, the Judge Grimm in *Lorraine* case has warned, though, that "simply because an individual's sending address is present on an e-mail does not constitute definitive proof that the person actually sent the e-mail, and authentication of an e-mail could still possibly require testimony from a person with personal knowledge of the transmission or its receipt to ensure its trustworthiness."[130]

When e-mail evidence is offered in proceedings, lawyers should establish that the information under review of the court is self-authenticating under rule 902[131] or at least meets the standards of authentication mentioned in rule. 901.[132] With regard to any other evidence, lawyer should prove that the e-mail is "what it purports to be." Still, testimony of a witness, before the competent court, with personal knowledge regarding e-mail under consideration is an accepted method for showing e-mail's authenticity.[133]

3.7 AUTHENTICATION CHALLENGES

Any evidence to be admissible in Pakistani legal system, or any of the legal systems of the world, it must meet certain well established minimum criteria. Before accepting the same evidence in court, courts usually examine about any evidence that whether the evidence is authentic, admissible, whether the copy is acceptable or original is required.

As discussed earlier, digital evidence is altogether different from paper-based evidence, and by "its very nature gives rise to complex questions about its integrity, reliability and accuracy. The very question of authentication comes down to whether electronic evidence is the same as it

---

[129] Ibid.

[130] Ibid.

[131] Rule 902 of the FRE.

[132] Rule 902 of the FRE; In *United States v. Safavian,* 435 F. Supp. 2d 36 (D.D.C. 2006), the court discussed that how e-mail may be authenticated under the FRE.

[133] *Lorraine v. Markel American Insurance Co.,* 241 F.R.D. 534 (D. Md. 2007).

was when it was created."[134] Though, this evidence can easily be changed or modified by any person having access to it. Nonetheless, this access does not mean that the content has been changed or modified altogether. However, this raise some serious questions about its authenticity.

FRE are applicable to computerized data as these rules are applicable to other types of conventional evidence.[135] Yet this raise some unique issues of correctness and genuineness of computerized data. Manual of complex litigation described the accuracy and integrity issues as under: -

> Accuracy may be impaired by incomplete data entry, mistakes in output instructions, programming errors, damage and contamination of storage media, power outages, and equipment malfunctions. The integrity of data may also be compromised in the course of discovery by improper search and retrieval techniques, data conversion, or mishandling. The proponent of computerized evidence has the burden of laying a proper foundation by establishing its accuracy.[136]

More specifically, challenges to the authenticity of digital evidence can include, alteration, manipulation or damaged of data; "reliability of the program that generated the record,"[137] identity of the author of digital evidence; "the reliability of the evidence from a social networking website;"[138] "failing to prove the message was directed to a particular person,"[139] mainly when more than one person has access to the device and "whether the person alleged to have used his PIN, password or clicked the 'I accept' icon was the person who actually carried out the action."[140] These challenges makes complication for dealing digital evidence. Yet, it is undefined that whether

---

[134] Stainfield, "The Authentication of Electronic Evidence," 11.

[135] Gregory P. Joseph, "A Simplified Approach to Computer-Generated Evidence and Animations," *New York Law School Law Review* 43 (1999–2000), 875.

[136] Federal Judicial Centre, *Manual for Complex Litigation*, 4th ed. (Washington: Federal Judicial Centre, 2004), 82.

[137] Mason and Seng, *Electronic Evidence*, 196.

[138] Ibid., 197.

[139] Ibid.

[140] Ibid.

an attorney challenging authenticity of digital evidence "can ever raise sufficient doubt about the authenticity of digital data because of the complexity of the systems and the difficulty of obtaining evidence from the various owners of the different part of any given system."[141]

All the institutions (first respondents, investigation agency, prosecution, forensic examiner, and legal fraternity) dealing with digital evidence should manage/discuss the admissibility and authentication issues prior to presentation of evidence before the court that may arise in legal proceedings. In existing regime, there are different means "to cast doubt on the authenticity of electronic evidence. Sound and informed practices must be adopted to determine whether the evidence fulfills the legal requirements for authenticity, reliability and integrity."[142]

3.8 SUMMARY

The marvelous evolution of the Internet in ICT regime has enlarged the demand for experienced professional particularly computer (digital) forensics to assist the LEAs, first respondents, prosecution, forensic examiner, and legal fraternity in dealing with cyber-space issues. Thus, it is crucial for them to understand the basic concepts of digital forensic to deal with digital evidence.

Digital evidence is not like paper-based evidence, as it can be changed, manipulated and altered without the noticeable edition. Thus, it raises many authentication challenges for LEAs, making their task more difficult. Nevertheless, the information created by computer or digital device is not immune to be questioned. So, assistance of the digital forensic professional cannot be ruled out.

---

[141] Mason and Seng, *Electronic Evidence*, 197; Stanfield, "The Authentication of Electronic Evidence," 187.

[142] https://www.crl.edu/sites/default/files/d6/attachments/pages/Thomson-E-evidence-report.pdf (accessed: 30th November, 2019).

CHAPTER FOUR:

COMPUTER BASICS AND CRIME SCENE

4.1 INTRODUCTION

In almost every case, the digital evidence is collected from live system. A small mistake or negligence can lead to collection of wrong evidence or destruction of the entire digital evidence. Specialized guidelines have been prescribed by the concerned LEAs for collection of digital evidence from live system. In this chapter various basic operations of computer have been discussed. Thereafter, volatile data, which has a lot of importance in any investigation, is also discussed, which helps investigators in collecting digital evidence from live system. Storage media is vital in evidence preservation; therefore, digital evidence preservation and storage media is also discussed in this chapter.

Qualified experts can only deal with the investigation of digital evidence. Otherwise, a lay man or the investigator who is not familiar with digital environment may cause the destruction of entire digital evidence, therefore, importance of crime scene, crime scene investigation, electronic crime scene, digital crime scenes handling, possession and chain of custody of digital evidence is discussed. After the collection of evidence preservation, transportation and storage stages plays an important role, thus, at the end these are examined.

4.2 BASIC OPERATION OF COMPUTERS

Conventional evidence has shape, substance, and form; therefore, people can see it and touch it. Traditional or conventional evidence can last for decades, if preserved properly. Unless the investigator understands the basic operation of computers, he will not be able to collect digital evidence as computer evidence is entirely different from conventional evidence. Computer

evidence cannot be "seen, touched or smelled and it often lasts for only very short periods of time."[1]

In existing regime, computers data is stored in three different ways including magnetic,[2] semiconductor (chip), and optical. There are other methods of data storage which are less common these includes "magneto-optical disk storage, optical jukebox storage and ultra-density optical disk storage."[3]

In cyber-crime investigation, knowledge and skills required for investigator vary depending upon the nature of crime, though, the knowledge and skills that how computer operates and how each component interact with other component is not necessary. The following are the import components of the computer: -

i. CPU and how it works with random access memory (RAM)
ii. How RAM works with different operating systems (OS)
iii. How data is stored and retrieved from storage media

In addition to the above-mentioned components, the investigator is also required to understand the operating systems, their functions and working, applications, and filesystems (FAT, NTFS). Having knowledge of these things, will ease the burden of the investigator as he will be

[1] Marcella and Menendez, *Cyber Forensics*, 298.

[2] "Using a magnetically coated surface, a computer can magnetically arrange that surface to create patterns that store information. This form of memory provides great flexibility because it allows relatively fast reading and writing of data, and it can be reused. This means that when the computer is no longer using a portion of the magnetically coated surface for a particular task, it is free to write over that surface with new data. Computer hard drives and removable floppy disks use magnetic storage." Marcella and Menendez, *Cyber Forensics*, 298.

[3] Marcella and Menendez, *Cyber Forensics*, 298.

able to collect and analyze digital evidence without wastage of any time. Further, he will not collect irrelevant data or digital devices for investigation purposes.

4.3 VOLATILE DATA

Digital evidence is collected through forensics processes. Therefore, in forensics processes legal acceptance of digital evidence by ensuring the data is reliable, accurate, verifiable and complete is always required. On the basis of above-mentioned rules, at least, few things must be observed by the investigator while collecting digital evidence, these are as under:[4]

a- Minimize handling and corruption of original data.[5]

b- Account for any changes and keep detailed logs of actions.[6]

c- Comply with the five rules of evidence.[7]

d- Do not exceed knowledge.[8]

e- Follow local security policy.[9]

f- Capture as accurate an image of the system as possible.[10]

---

[4] Vacca, *Computer Forensics: Computer Crime Scene Investigation*, 221. Below mentioned points in main text are taken from the above mentioned book.

[5] Once the investigator have created a master copy of the original data, don't touch it or the original. Always handle secondary copies. Any changes made to the originals will affect the outcomes of any analysis later done to copies. The investigator should make sure that he don't run any programs that modify the access times of all files (such as tar and xcopy). He should also remove any external avenues for change and, in general, analyze the evidence after it has been collected.

[6] Sometimes evidence alteration is unavoidable. In these cases, it is absolutely essential that the nature, extent, and reasons for the changes be documented. Any changes at all should be accounted for—not only data alteration but also physical alteration of the originals (the removal of hardware components).

[7] The five rules are there for a reason. If investigator don't follow them, he will be probably wasting time and money. Following these rules is essential to guaranteeing successful evidence collection.

[8] If investigator does not understand what he is doing, he cannot account for any changes he made and he cannot describe what exactly he did. If he ever find himself "out of his depth," either go and learn more before continuing (if time is available) or find someone who knows the territory. Never soldier on regardless. Otherwise he is just damaging the case.

[9] If investigator fails to comply with government or company's security policy, he may find himself with some difficulties. Not only may he end up in trouble (and possibly fired if he has done something really against policy), but he may not be able to use the evidence he has gathered. If in doubt, talk to those who know.

[10] Capturing an accurate image of the system is related to minimizing the handling or corruption of original data. Differences between the original system and the master copy count as a change to the data. Investigator must be able to account for the differences.

g- Be prepared to testify.[11]

h- Work fast.[12] (work fast does not mean to work in hurry, it means when it comes to the knowledge of the investigator, he must immediately go to the place of occurrence without wasting any further time, otherwise data may be changed or modified)

i- Proceed from volatile to persistent evidence.[13]

j- Don't shutdown before collecting evidence.[14]

k- Don't run any programs on the affected system.[15]

In addition to collecting volatile data/evidence, the investigator must not waste time on unimportant things, but he must draw a list of volatility, otherwise rather than collecting the important data he will collect less important and useless things. No doubt that acquisition of volatile digital evidence with existing tools is not possible to present evidence in court and confirm their integrity and completeness. The volatility list would be:

a- Registers and cache

b- Routing tables

---

[11] If investigator is not willing to testify to the evidence he has collected, he might as well stop before he start. Without the collector of the evidence being there to validate the documents created during the evidence-collection process, the evidence becomes hearsay, which is inadmissible. Remember that the investigator may need to testify at a later time. No one is going to believe the investigator if he cannot replicate his actions and reach the same results. This also means that investigator plan of action shouldn't be based on trial-and-error.

[12] The faster the investigator work, the less likely the data is going to change. Volatile evidence may vanish entirely if investigator does not collect it in time. This is not to say that he should rush. He must still collect accurate data. If multiple systems are involved, work on them in parallel (a team of investigators would be handy here), but each single system should still be worked on methodically. Automation of certain tasks makes collection proceed even faster.

[13] Some electronic evidence is more volatile than others are. Because of this, investigator should always try to collect the most volatile evidence first.

[14] Investigator should never, ever shutdown a system before he collect the evidence. Not only do he lose any volatile evidence, but also the attacker may have trojaned (via a trojan horse) the startup and shutdown scripts, plug-and-play devices may alter the system configuration, and temporary file systems may be wiped out. Rebooting is even worse and should be avoided at all costs. As a general rule, until the compromised disk is finished with and restored, it should never be used as a boot disk.

[15] Because the attacker may have left trojaned programs and libraries on the system, investigator may inadvertently trigger something that could change or destroy the evidence he is looking for. Any programs investigator uses should be on read-only media (such as a CD-ROM or a write-protected floppy disk) and should be statically linked.

c- Arp cache

d- Process table

e- Kernel statistics and modules

f- Main memory

g- Temporary file systems

h- Secondary memory

i- Router configuration

j- Network topology

Generally, it is suggested that the investigator should collect maximum volatile data "because all opportunities to collect such volatile data will be lost once the computer is powered down. Later, a determination can be made as to which collected volatile data should be examined. An automated script on a toolkit CD can be used for consistency in collecting volatile data."[16]

Volatile data can change with passage of time; thus, order and timeliness of volatile data collection is significant in digital investigation. Therefore, the cyber forensic investigators "should first collect information on network connections and login sessions, because network connections may time out or be disconnected and the list of users connected to a system at any single time may vary."[17] Whereas network configuration information volatile data's chances of change are less, therefore, this data may be collected later. The collection of volatile data priority should be as under:

1. Network connections
2. Login sessions
3. Contents of memory
4. Running processes

[16] Marcella and Menendez, *Cyber Forensics*, 150-151.
[17] Ibid., 151.

5. Open files
6. Network configuration
7. Operating system time[18]

4.4 VOLATILE OPERATING SYSTEM DATA

In many cases, the investigator has to collect data from live system when the network or system is in working condition. Therefore, volatile operating system data is collected from a live system. While collecting the volatile data, any action performed by the investigator on the system, "will almost certainly alter the volatile operating system data in some way. Therefore, cyber forensic investigators should decide as quickly as possible whether the volatile operating system data should be preserved."[19] The cyber forensic investigator should make this decision immediately, otherwise, making decision after lapse of time or making wrong decision will be fatal for volatile data as "powering off the system or even disconnecting it from a network can eliminate the opportunity to collect potentially important information."[20]

There are some inherent risks in collection of volatile operating system data from a running computer. Due to volatility nature of this evidence there is always a possibility that "files on the computer might change and other volatile operating system data might be altered. In addition, a malicious party might have installed root kits designed to return false information, delete files, or perform other malicious acts."[21]

---

[18] Marcella and Menendez, *Cyber Forensics*, 151.
[19] Ibid, 148.
[20] Ibid.
[21] Ibid., 149.

In collection of volatile data, the investigator should not ignore the risk associated with evidence. Efforts should be made by the investigator to recover the important data. In case of important evidence, then

> the cyber forensic investigator should fully document what is seen on the screen before touching the system. If a live system is in sleep mode or has visible password protection, cyber forensic investigators should also decide whether to alter the state of the system by waking it from sleep mode or attempting to crack or bypass the password protection so that cyber forensic investigators can attempt to collect volatile data. If the effort needed to collect the volatile data is not merited, cyber forensic investigators might instead decide to perform a shutdown.[22]

Collection of information from live computer systems and mobile devices can alter, change, modify. This change or modification in data is, however, recognized and accepted in digital forensics practice. Keeping in view the importance of preservation of data from live systems, the courts in USA realized this fact in *Columbia Pictures Indus. v. Bunnell*,[23] and the court held that RAM on a "web server could contain relevant log data and was within the scope of discoverable information under the Federal Rules of Civil Procedure." This case is an example of volatile computer data preservation. Thus, now, investigators are under obligation to preserve data on live systems.

There are few types of volatile operating system data which help in identification of the most valuable in a specific condition enabling the investigator to prioritize the collection of volatile data. Thus, it is the responsibility of the investigator to follow the volatile list.

---

[22] Marcella and Menendez, *Cyber Forensics*, 149.

[23] *Columbia Pictures, Inc. v. Bunnell,* 245 F.R.D. 443 (C.D. Cal. 2007).

4.5STORAGE MEDIA

Removable media and portable devices are any devices which can easily be carried by hand and used for mobile computing. Many portable devices are available in market which is a big form of storage media. Removable media and portable devices, however, sits outside the computer system. A lot of data can be stored on any of these devices depending upon the size of such devices as size of these device varies. These devices include, but not limited to, external hard drive,[24] portable hard drive, laptop, table computer, notebook computers, cell phones, digital cameras, digital audio devices, memory cards, Compact Disks (CDs),[25] Digital Versatile Disks (DVDs),[26] Blu-ray, USB,[27] Secure Digital Cards (officially abbreviated as SD card), and memory sticks.

A Blu-ray disk (abbreviated as BD) is "an optical storage device similar to CD and DVD technology. It also uses a laser to read and write to disk.....it uses a blue-violet laser beam."[28] This is specifically designed to store large data, which is normally used to store high definition films (HD). This can store "25GB whilst a double layer Blu-ray can hold up to 50GB of data."[29]

4.6IMPORTANCE OF CRIME SCENES

Traditional crime scenes are very easy to seize but due to complexity of the situation, the digital crime scenes are difficult to seize. Although, at the very instant, conventional crime scenes procedures are followed for the digital crime scenes but it is not sufficient for investigator to merely

---

[24] External hard drive's capacity is 4TB.

[25] One CD can store up-to 700 MB of data. CDs are not best storage media as they can be corrupted easily.

[26] DVD specification provides that a DVD can store 4.7 GB for a single-layered.

[27] USB is available in 1TB capacity.

[28] http://www.teach-ict.com/gcse_new/computer%20systems/storage_devices/miniweb/pg9.htm (accessed: 18th April, 2020)

[29] Ibid.

rely on these methods rather he must develop expertise in digital forensic. Further, the investigator should avoid negligence in the digital scene as a little disturbance will affect the seizure. Therefore, before starting work on seizure, it is very important for the investigator that "a thorough visual inspection is carried out with appropriate use of photographs and note-taking to ensure that nothing has been missed and that all risks have been fully considered."[30]

Digital evidence can be easily altered, changed, manipulated and modified, the investigator should therefore remove away everybody from the crime scene to ensure that nobody has access to tamper with the evidence media, equipment or device. Consequently, this will remove the like hood of "any accusations of evidence being "planted" or for the user/owner to attempt to damage any evidence of which they are aware."[31]

Thereafter, the investigator should also check that the system or software is running or not? Either way, "its status should be recorded as completely as possible using sketches, photographs and comprehensive notes which describe exactly what can be seen. The temptation to use one's own knowledge of digital devices should be resisted."[32]

Where the electronic media is present at crime scene, the investigator should not ignore the importance of this media. He has to provide required security for proper safety of the media "to ensure protection of potential evidence located on hard drives and file servers as the case moves from a preliminary investigation to a full investigation."[33]

---

[30] Marshall, *Digital Forensics Digital Evidence in Criminal Investigation*, 22.
[31] Ibid.
[32] Ibid.
[33] Johnson, *Forensic Computer Crime Investigation*, 8.

Nowadays, every computer is connected to networks and communications system, however, the best option is to "disconnect the system from communications devices as quickly as possible, often before the status recording is complete."[34] Moreover, the system connected to the live network or communications may not be disconnected as it may cause some risks as it may alert the members of the gang or deletion of data or in the case of mobile phones, "switching the phone off to remove it from the network causes the phone to change internal data which might have been useful to the investigation."[35]

Integrity of the collected digital evidence depends upon the seizure process, that no human interaction is involved during or after the seizure, if any interaction with the seized evidence or device is established, then its integrity will be challenged by the defense lawyer, which is a real risk. Thus, it may be ensured by the investigator that no such activity is happened with digital evidence or electronic equipment at crime scene.

4.7 Crime Scene Investigation

Basic training of LEAs, was restricted to the physical documentation and collection of evidence. Now, in prevailing technology regime, besides collecting physical evidence, forensics investigators are using "scientific knowledge and forensics techniques to identify evidence and generate leads to assist in solving a crime."[36] Requiring more specialized knowledge for digital crime scene investigations. In electronic crime scenes, there is always a possibility that the criminal will always leave any object, password, key, clue, sign, identification or evidence. Besides, finger prints, DNA and any physical evidence may also be available.

---

[34] Marshall, *Digital Forensics Digital Evidence in Criminal Investigation*, 23.
[35] Ibid.
[36] Brown, *Computer Evidence: Collection and Preservation,* 5.

In many cases, particularly in cyber-crime and computer related crimes, an investigator may not be the first person to visit the crime scene. Due to delay conveying of the information of the crime or any other reason, the investigator will come after lapse of sometime. In other cases, the investigator may be the first responded as in case of hacking of government computers or data basis. In the first situation, there may be many difficulties in collection of digital evidence but in second situation, it will depend on the investigator how quickly he responded to the attack. Whatever the situation is, investigations of cyber-crime are a technical job. The investigator or first responder should adopt the following steps:

1. Establish and following the standard of the crime scene investigation.[37]
2. Initiate safety measures.[38]
3. Provide emergency care.[39]
4. Physically secure the scene.[40]
5. Logically secure the scene.[41]
6. Physically secure any evidence.[42]
7. Release the scene.[43]

---

[37] Brown, *Computer Evidence: Collection and Preservation,* 6.

[38] Ibid.

[39] Ibid.

[40] Ibid.

[41] "This step is unique to digital investigations, where a computer may need to be left operating because of the service it provides or to collect live and volatile data.....Experience and situational awareness will drive to what extent the scene will need to be logically secured." Brown, *Computer Evidence: Collection and Preservation*, 6.

[42] Brown, *Computer Evidence: Collection and Preservation*, 6

[43] "After all other steps have been completed, the scene should be released to the proper authorities. The proper authorities can differ from case to case but can include law enforcement in criminal investigations or corporate information technology system administrators in corporate incident response. Essentially, this step is intended to ensure that it is clear to all concerned when evidence collection is completed and systems can be returned to their normal operation if they were taken out of operation during the collection." Brown, *Computer Evidence: Collection and Preservation,* 7.

8. Finalize documentation.[44]

In any investigation, crime scene is important in reaching conclusion, but the securing of electronic crime scene is more important as compared to physical crime scene. Therefore, the investigator must "secure the crime scene to prevent contamination of the scene or destruction of materials that may possess evidentiary value."[45]

The main purpose of any investigation is "to follow the trails that offenders leave during the commission of a crime and to tie perpetrators to the victims and crime scenes."[46] Although, if digital data does not provide "a link between a crime and its victim or a crime and its perpetrator, they can be useful in an investigation. Digital evidence can reveal how a crime was committed, provide investigative leads, disprove or support witness statements, and identify likely suspects."[47]

4.8 Digital Crime Scenes Handling

Electronic crime scene is not like physical crime scenes, these creates new challenges for LEAs, investigators, forensic examiners, legal fraternity and judiciary alike. These challenges exist due to its environment that in many cases evidence may be difficult to detect and, in some cases, "how its evidentiary value may be hidden through steganography and/or encryption."[48] Besides, culprits can easily hide their true identity making more difficult for the investigator to trace the perpetrators. Thus, the rapid ICT "advancements occurring in our society through the digitalization of data and information are presenting new challenges to investigators. This electronic evidence is both difficult to detect and quite fragile; therefore, the latent nature of electronic evidence requires

---

[44] Brown, *Computer Evidence: Collection and Preservation*, 7.
[45] Johnson, *Forensic Computer Crime Investigation*, 11.
[46] Casey, *Digital Evidence and Computer Crime Forensics Science*, 16.
[47] Ibid., 6.
[48] Johnson, *Forensic Computer Crime Investigation*, 5.

very skilled investigators."[49] It must be kept in mind that no one can "be certain of what occurred at a crime scene when we only have a limited amount of information."[50] Thus, the investigator generally presents likelihoods based on insufficient amount of data collected from the crime scene.

At the first instance, the investigator should move people away from the crime scene to secure computers, digital devices and power. This will assure the safety of people, investigators, and equipment. In case of failure to move away people from the crime scene, it may result "in the loss of otherwise valid evidence."[51] Thereafter, the investigator have to "disable biometric access and video surveillance equipment in and around the office. This action not only increases the protection of the scene from outside invasion, but it also preserves these biometric and CCTV systems as potential sources of evidence."[52] Thereafter, to provide its authenticity, the investigator will testify in the court that "how the digital evidence was found."[53]

Flaws in the crime scene handling process may considerably affect digital investigation by rendering it unusable. For instance, in *Zubulake v. UBS Warburg LLC*,[54] the court in USA, decided the case against the defended for failure to locate and preserve backup tapes related to e-mails. Ideal handing of digital crime scene is where all the relevant data and contents are mapped, and these are recorded properly "with accompanying photographs and basic diagrams to document important areas and items."[55]

---

[49] Ibid.

[50] Casey, *Digital Evidence and Computer Crime Forensics Science,* 14.

[51] Johnson, *Forensic Computer Crime Investigation,* 163.

[52] Casey, *Digital Evidence and Computer Crime,* 245.

[53] National Institute of Justice, *Digital Evidence in the Courtroom*, 41.

[54] This case has long history and details can be found in following case: *Zubulake v. UBS Warburg LLC*, 230 F.R.D. 290 (S.D.N.Y. 2003); *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003) *Zubulake v. UBS Warburg,* 216 F.R.D. 280 (S.D.N.Y. 2003); *Zubulake v. UBS Warburg,* 220 F.R.D. 212 (S.D.N.Y. 2003); and *Zubulake v. UBS Warburg,* 229 F.R.D. 422 (S.D.N.Y. 2004).

[55] Casey. *Digital Evidence and Computer Crime,* 229.

Digital investigators must be better equipped (with resources i.e. personal, capacity, skill, necessary and up to date equipment) in handling digital crime scenes in any cyber-crime related investigation, therefore, it is beneficial for LEAs and investigators "to obtain information about computers and storage media of interest, including their characteristics, physical locations, and whether encryption or other security mechanisms are in use."[56] In addition to this, the digital crime scene investigators must consider the culprits' technical knowledge and skills. Whereas, if the offender is highly technical, then the more experience digital investigators should deal this case. Further, forensic consultant may request for assistance, if there is any issue with handling of digital crime scene.[57]

The investigator should also bring a tool kit for "proper dismantling of computer systems as well as for their packaging and removal."[58] These items includes but not limited to property register, labels, tape, several types of pliers (including needle nose), evidence containers, tools (flathead and crosshead screw drivers, wire cutters), bags, flashlight, cable ties, flat pack assembly boxes (use original boxes of device, if available), color markers and pens. In addition, investigator should also bring a digital camera. If digital camera is required to be used in crime scene then while using a digital camera, "it is advisable to use a blank, sanitized removable storage card to avoid confusion between photographs taken at different crime scenes."[59] The most difficult situation for the investigator is when the data is stored in online servers such as cloud system.

In many cases, while handling a digital crime scene additional equipment are also required such as "hardware duplicators, boot CDs, data cables, crossover network cables, and mobile device

---

[56] Ibid., 238.
[57] Sammons, *The Basics of Digital Forensics the Primer for Getting Started in Digital Forensics*, 48.
[58] ACPO, *Guide for Computer-Based Electronic Evidence*, 21.
[59] Casey, *Digital Evidence and Computer Crime,* 239.

forensic kits and associated cables."[60] As digital evidence can be used to prosecute the criminals, therefore, it should be handled "in a scrupulously careful manner to avoid later allegations of tampering or misconduct, which can compromise the case of the prosecution toward acquittal or to overturning a guilty verdict upon appeal."[61]

When computers, mobile phones, digital devices, and networks are not directly involved in facilitating the commission of crime, then these gadgets may be, however, considered an extension of the crime scene. For example, "they can contain useful information and provide a digital dimension."[62] In many prospects, digital crime scenes are identical with physical crime scene which contain many pieces of digital evidence, therefore, it is mandatory for the investigator "to apply forensic principles to survey, preserve, and document the entire scene."[63] Hence, the investigator should processed both the crime scenes in a mechanical manner "to ensure the integrity of potential evidence, physical and digital."[64]

Handling of digital evidence is very sensitive. Therefore, digital evidence should be handled by the investigators and forensic examiner carefully to preserve its integrity. Whereas digital data can be "damaged or altered by electromagnetic fields such as those generated by static electricity, magnets, radio transmitters, and other devices."[65] In view of the nature of digital evidence, it requires special methods for collection, packaging and transportation. So, keeping in view the special requirements for digital evidence "communication devices such as mobile phones,

---

[60] Ibid.
[61] Marcella and Menendez, *Cyber Forensics*, 12.
[62] Casey, *Digital Evidence and Computer Crime*, 227.
[63] Ibid.
[64] Ibid.
[65] National Institute of Justice, *Electronic Crime Scene Investigation*, 21.

smart phones, PDAs, and pagers should be secured and prevented from receiving or transmitting data once they are identified and collected as evidence."[66]

Proper documentation of the crime scene is central in any investigation. Therefore, it is very important for the investigator "to accurately record the location of the scene; the scene itself; the state, power status, and condition of computers, storage media, wireless network devices, mobile phones, smart phones, PDAs, and other data storage devices; Internet and network access; and other electronic devices."[67] The investigator should keep in mind that all digital evidence may not "be in close proximity to the computer or other devices."[68]

The documentation of the scene should be complete in all aspects as after collection of evidence from the scene this will be open for anyone to access this area and the documents will be the only evidence before court. Documentation of the crime scene by the investigator should not miss any essential item, *inter alia*, it should include "a detailed record using video, photography, and notes and sketches to help recreate or convey the details of the scene later. All activity and processes on display screens should be fully documented."[69] Further, everything done during "the seizure, transportation, and storage of digital evidence should be fully documented, preserved, and available for review."[70]

Moreover, proper documentation of the crime scenes must also include "the entire location, including the type, location, and position of computers, their components and peripheral equipment, and other electronic devices."[71] The digital crime scene may have multiple locations,

---

[66] Ibid.
[67] Ibid., 19.
[68] Ibid.
[69] Ibid.
[70] Ibid., vii.
[71] Ibid.,19-20.

so the investigator have to properly document "all physical connections to and from the computers and other devices."[72] Besides, the investigator should also record the linking computers, device and the Internet. Later on, each person who involved in digital evidence collection may be required to testify in court that the evidence is accurate and authenticate and not altered or manipulated at any stage during the investigation. For instance, in *United States v. Bunty*,[73] the court discussed the handling and inspection of the laptop by U.S. Customs and Border Protection agents and concluded that the government's (Customs and Border Protection agent's) handling of "the evidence was in good faith and that their alterations of the evidence were not sufficient to exclude the evidence."

In has been seen, in Pakistan, that in most police-driven investigations (including the FIA and other investigation departments) conventional evidence-handling techniques are used for digital evidence. Generally, an inventory list is prepared of all seized items/equipment, crime scene is photographed, people at the spot are investigated/interviewed, passwords are retrieved etc. If the proper procedure for evidence seizure is not followed then the evidence collected in violation of legal procedure and approved techniques may invalidate the same.

4.9 Possession and Chain of Custody

Great care must be taken by the investigator while collecting or taking possession of any physical objects which may potentially be used in legal proceedings as evidence. Therefore, it is important to safeguard the evidence from contamination. If the evidence is not maintained "in pristine condition, some inconvenient and probing challenge from the opposing legal team may

[72] National Institute of Justice, *Electronic Crime Scene Investigation,* 20.
[73] *United States v. Bunty,* 617 F. Supp. 2d 359 (E.D. Pa. 2008).

well be anticipated."[74] After recovery of evidence, the investigator should be able to show that evidence was "accurate when recovered, and be able to demonstrate the chain of possession of the evidence from the time it was recovered up to the time it was introduced as evidence to the court."[75] Therefore, the investigator must show that the evidence has not been tampered with.[76]

It is a common practice, beside legal requirement, among the investigators to record the evidence collection process and maintain chain of custody. During the investigation, if evidence collection process is not accurately maintained then it may create difficulty, at the time of trial, for proving the authenticity. "In simple terms, a chain of custody is a roadmap that shows how evidence was collected, analyzed, and preserved in order to be presented as evidence in court."[77] The NIJ defines chain of custody as "A process used to maintain and document the chronological history of the evidence."[78]

The chain of custody is a theory which applies to the handling of any evidence that ensures the authenticity and integrity of the evidence. During the court proceedings, chain of custody shows how the evidence was seized, taken into custody, how it was transferred from one place to another for examination and analysis and finally presentation into the court. Stating differently, chain of custody commences with the collection of evidence and ends when the same is presented into the court. The basic purpose of this is to assure that the evidence is accurate and authentic and have not be changed or modified since it was collected. In addition to this, "the proponent of a piece of evidence must demonstrate that it is what it purports to be."[79] In every case, establishing

---

[74] Boddington, *Practical Digital Forensics*, 92.

[75] Johnson, *Forensic Computer Crime Investigation*, 108.

[76] *State vs. Roszkowski*, 129 N.J. Super. 315, 323 A2d 531 (App. Div. 1974).

[77] Vacca, *Computer Forensics: Computer Crime Scene Investigation*, 247.

[78] https://nij.ojp.gov/topics/articles/glossary-crime-scene-investigation-guides-law-enforcement (Accessed: 21st December, 2019).

[79] Marcella and Menendez, *Cyber Forensics,* 279.

the chain of custody is critical particularly when the evidence is in the form of fungible things. However, this is not easy in digital environment, particularly when the defended or accused claims that he never had such computer or device or never had access to such device. For not maintaining proper chain of custody may lead to challenges of accuracy of the data.

Digital evidence is very sensitive in nature; therefore, this evidence be handover to such a person for safe custody who is trustworthy and assume the responsibility for its safe custody. To avoid manipulation of digital evidence, it is imperative "to establish procedures for creating a custody chain, to include a running log of who has had contact with (access to) an item of evidence, for how long, and for what reason(s) (why?)."[80]

Proper documentation and the chain of custody is the most significant characteristics of authentication of evidence. Thus, without documentation of evidence collection may raise many issues including improper handling, alteration, and contamination. In court proceeding, the first attack on evidence will be on documentation of chain of custody. Without recording and documenting details (such as collection, storage, transportation, and analysis), the evidence will be deemed, by the presiding officers untrustworthy and inadmissible. This detail makes the chain of custody.[81] Thus, significance of comprehensive and correct "documentation can't be overstated. There is an old phrase which say that "if you didn't write it down, it didn't happen are truly words to live by in this industry."[82] As held by the SC in *Ishtiaq Ahmed Mirza v. Federation of Pakistan*[83] case that the proper chain of custody is necessary i.e. safe custody of the digital evidence from its preparation till its production before the court.

---

[80] Ibid.
[81] Sammons. *The Basics of Digital Forensics the Primer for Getting Started in Digital Forensics*, 53.
[82] Ibid., 35.
[83] *Ishtiaq Ahmed Mirza v. Federation of Pakistan,* PLD 2019 SC 675.

If chain of custody is broken at any stage, it does not affect as such, as held in *United States v. Campbell*,[84] that a "defect in the chain of custody goes to the weight, not the admissibility, of the evidence introduced." Earlier, the similar view was taken in *United States v. Howard-Arias*,[85] where the court held that chain of custody process is not an "iron-clad requirement" and a "missing link does not prevent the admission of real evidence, so long as there is sufficient proof that the evidence is what it purports to be and has not been altered in any material aspect." Whereas, in *Muhammad Hussain v. State,*[86] the Supreme Court of Pakistan held as under:

> it is a case of circumstantial evidence, therefore, as a rule of prudence, it is required that each piece of circumstantial evidence shall be supported by independent corroborations, which by itself would be sufficient to establish the guilt of the accused, however, each circumstances should be so connected with each other that it shall make one complete chain without their any broken link.

4.10 ELECTRONIC CRIME SCENE

In addition to the general procedures, the investigator involved in investigation needs to know the various digital device and their operations, in particular: -

i. How computer (including all various and types of operating systems) works and what are their components
ii. Work of access control and hand-held (such as PDA and digital watches) devices
iii. How answering, facsimile machines and fax machines functions
iv. Modems and their function
v. Storage media (external and removable hard drive, memory cards) and credit card skimmers

---

[84] *United States v. Campbell,* No. 94-30295, 1996 WL 241545 (9th Cir. May 9, 1996). Similar, view was taken in the *United States v. Matta-Ballesteros,* 71 F.3d 754, 768-69 (9th Cir. 1995).

[85] *United States v. Howard-Arias,* 679 F.2d 363 (4th Cir. 1982).

[86] *Muhammad Hussain v. State,* 2011 SCMR 1127.

vi. Cloud systems

vii. Digital cameras and their storage capacity and functions

viii. Network components including network cables connectors, local area network (LAN) cards, network interface cards (NICs), servers, routers, hubs, and switches

ix. Pagers, printers, scanners, copiers

x. Telephones including as cordless and mobile phones

xi. ATM

xii. Working of GPS[87]

4.11 DIGITAL EVIDENCE PRESERVATION

After the collection of digital evidence, the preservation stage of evidence comes, which is important in case of digital data. Preservation of evidence is the primary element of any investigation, and electronic data is certainly no exception to this rule as the basic rules never change. In any investigation or decision, time line is critical. Due to its nature, it is required from the investigator to preserve digital evidence without wastage of precious time, as it may be lost within short span of time. If, the evidence is to be collected from service providers then necessary arrangement may be made by the investigator to avoid the destruction of digital evidence. In USA, the investigator can request the service provides to preserve such evidence. Under the USA law, the service provides is bound to preserve evidence, the relevant section states: "A provider of wire or electronic communication service or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process."[88] However, this type of

[87] Johnson, *Forensic Computer Crime Investigation,* 10.
[88] 18 U.S.C. § 2703(f)(1).

evidence shall be kept at least "for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity."[89]

Digital evidence can be preserved by storing the device in secure storage, extracting of required data or information from the device and acquiring everything related to evidential device. Which approach will be adopted by the investigator in a giving situation, it is the pure discretion of the investigators depending upon the nature of every case. In one case, there will not be an immediate need to extract digital evidence from an evidential device. In other case, however, there may be an immediate need to extract digital evidence from relevant media, as there may be irrelevant data on that device and only selected data is available on this device. So, it's better to obtain data and preserve for future analysis.

Integrity of the digital evidence collected in any investigation "is tightly coupled to ensuring that there is in place a solid documentation process. The documentation process should be designed to authenticate and substantiate each step taken to identify, collect, preserve, and interpret or analyze, the electronic evidence as well as each individual who may have in any way."[90] Further, the investigator will ensure that no human being has interfered with this evidence during the preservation period and it is safe from contamination or destruction.

After the collection of the evidence, the first step for the investigator is to pack digital forensic evidence which has the same requirements of packaging those for conventional evidence. Thereafter, it is the responsibility of the investigator or evidence handler to transport it in a proper way, following the laid down procedure, in a timely way to a facility (station of the investigator or the forensic lab) where the same can be kept in safe custody, without the chances of intervention

[89] 18 U.S.C. § 2703(f)(2).
[90] Marcella and Menendez. *Cyber Forensics,* 5.

of human being, in a suitable environment for the preservation of the digital data or device. So, the chances and allegation of tampering be avoided. However, during the safe custody, maximum measures should be adopted to avoid the chances of alteration or deletion of the digital evidence. Moreover, for the due care of digital evidence, following things should be observed, "keep it away from magnetic sources such as loudspeakers, heated seats, and radios; place boards and disks in antistatic bags; transport monitors face down buckled into seats; place organizers and palmtops in envelopes; and place keyboards, leads, mouse, and modems in aerated bags."[91]

4.12 TRANSPORTATION OF EVIDENCE

Transportation of evidence (from crime scene to police station, then from police station to forensic laboratory, and back to police station from laboratory and lastly to court for examination of court and back to police station) is the vital part of any investigation, so the digital evidence is no exception to this process. Transportation of evidence is for various purpose including transportation from crime scene to LEAs office for safe custody, from LEAs office to forensic laboratory and back and from LEAs office to court for production in the court proceedings. Extra care is required in digital evidence transportation, as it can be destroyed due to heat or other elements. However, transportation should be done with care. At least, the following things should be observed by the investigator "handle everything with care; keep it away from magnetic sources such as loudspeakers, heated seats, and radios; place boards and disks in antistatic bags; transport monitors face down buckled into seats; place organizers and palmtops in envelopes; and place keyboards, leads, mouse, and modems in aerated bags."[92] Therefore, the investigator do not forget that no "one rarely gets a second chance to re-collect evidence that has been lost or rendered

[91] Johnson, *Forensic Computer Crime Investigation,* 165.
[92] Ibid.

unusable."[93] In addition to the above rules, investigator should also observe the following things for transportation of digital evidence:

> When planning for movement of evidence, investigators should consider whether the evidence will be physically in the possession of the investigator at all times, environmental factors, and the potential consequence of chance events. For example, packing digital evidence into luggage that will be placed in the cargo hold of an airplane creates serious risks that can have an adverse impact on digital evidence such as loss of luggage, rough handling, and significantly different environmental conditions.[94]

4.13 STORAGE OF EVIDENCE

For protection of digital evidence, this should be stored in a safe and secure environment to ensure its integrity that from the collection of evidence till presentation in the court is safe and no alteration was made during storage period and nobody except the authorized persons had access to the storage area. However, due to special nature of digital evidence, special precautions are required to be adopted to protect this type of evidence from any interference.[95] As in digital device deteriorations can occur with the passage of time which may produces errors as due to excessive heat or electromagnetic effects. Thus, it is important to store the digital data in safe, and secure environment. Surrounding environment around the digital evidence plays an important role for its preservation and destruction. A small mistake or negligence of any responsible person, may cause the destruction of whole evidence. Therefore, all the necessary rules for digital evidence should be adhered to avoid any contamination of digital evidence.

After taking custody of digital evidence, the investigator should take appropriate measures to make ensure "that it is not damaged or destroyed, that it is properly labeled and kept together,

---

[93] Casey, *Digital Evidence and Computer Crime,* 200.
[94] Ibid.
[95] Johnson, *Forensic Computer Crime Investigation,* 165.

and that it is not mixed up or otherwise tainted. If these precautions are not taken, the results can be effectively challenged."[96] Besides, the investigator make sure that the evidence is stored in modern systems, as the technology is changing rapidly, therefore, the stored evidence may not become redundant.

Due to rapid evolution of IT and invention of latest techniques in contemporary world no one distinguishes certainly that whether any evidence which is being collected is absolutely uncontaminated and free from modification or not. Purity of evidence, accidental overwrite protected may be established. If the investigator failed to establish the link between collection and storage and onwards, it may lose the weightage before the competent courts.

4.14 SUMMARY

In any investigation volatile data and crime scene has very importance for the purpose of prosecution, a small mistake or a little bit negligence may cause many problems including the destruction of digital evidence. Digital crime scene, however, are not per se with the conventional crime scene. Non expertise or little negligence will affect the volatile digital evidence. Besides, digital crime scene handling is also different and difficult in electronic environment, which cannot be handled without having proper knowledge of the basics of computer and digital devices. Further, maintaining proper chain of custody is vital for proving the authentication of evidence collected. Recording and maintaining proper procedure for digital evidence preservation, transportation and storage is essential to avoid any allegation of alteration of digital evidence.

[96] Johnson, *Forensic Computer Crime Investigation,* 164.

CHAPTER FIVE:

DIGITAL EVIDENCE ON COMPUTERS

5.1 INTRODUCTION

Computer is a main focus of investigators in cybercrime investigations. Therefore, investigators make maximum efforts to secure the computer at the earliest. In this chapter digital evidence on computers in discussed. Currently, different operating systems and windows are being used by the individuals and organizations. Thus, these operating systems use different file systems, and the data is stored on hard drives. Hard drive is not only the media of storage, there are certain other media which store the memory and data. Every file which exists on computer contains metadata leaving the trace of the criminal. Sometime data on computer is encrypted to avoid the interception of data, all these things along with digital evidence as alibi, and computer print outs are discussed in this chapter.

5.2 DIGITAL EVIDENCE ON COMPUTERS

Digital devices are everywhere in our surroundings. In computer crime investigations, the proof is "to be found in digital traces, while for ordinary crimes the evidence is to be found among more traditional sources, is no longer valid: investigations of common crimes increasingly rely on searches for digital evidence."[1]

Nowadays in 21st century, it is not a new phenomenon "that computers can be involved in a crime, or be the instrument of a crime."[2] As discussed earlier that "computer can be a victim; a

[1] Biasiotti et al, *Handling and Exchanging Electronic Evidence across Europe*, 14. In a number of traditional crimes, in Pakistan, digital evidence was used and punishment was awarded to the criminal. These cases have been discussed in chapter 8.

[2] Marcella and Menendez, *Cyber Forensics*, 269.

weapon; a witness, an accomplice and a computer can also provide a record of all that has passed through its electronic memory."[3] In many cases, sometime information stored on a computer or digital device including the cell phone is the only clue in an investigation. Therefore, need has been felt by the LEAs to consider digital device in any type of crime either the crime is committed in cyber-space or in traditional form.

In the USA legal system, the computer has been defined as the term "computer" means

> an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.[4]

Professor Kerr explains the computer, in the following words:

> Just think of the common household items that include microchips and electronic storage devices, and thus will satisfy the statutory definition of "computer." That category can include coffeemakers, microwave ovens, watches, telephones, children's toys, MP3 players, refrigerators, heating and air-conditioning units, radios, alarm clocks, televisions, and DVD players, in addition to more traditional computers like laptops or desktop computers.[5]

In *United States v. Kramer*,[6] the court held that the cellular phone is included in the definition of computer.

Considering the complication attached to the computer and allied devices, probing a computer "for evidence of crime is nearly always a time-consuming process. Even if the agents know specific information about the files they seek, the data may be mislabeled, encrypted, stored

---

[3] Marcella and Menendez, *Cyber Forensics*, 269.

[4] 18 U.S.C. Section 1030 (e) (1).

[5] Orin S. Kerr, "Vagueness Challenges to the Computer Fraud and Abuse Act," *Minnesota Law Review* 94 (2010): 1561-1587 at 1577-78.

[6] *United States v. Kramer*, 631 F.3d 900 (8th Cir. 2011).

in hidden directories, or embedded in slack space that a simple file listing will ignore."[7] In *United States v. Hill,*[8] and *United States v. Gray,*[9] the courts in USA observed that investigators performing duties in execution of a search for computer files "are not required to accept as accurate any file name or suffix and [to] limit [their] search accordingly," as delinquents can "intentionally mislabel files, or attempt to bury incriminating files within innocuously named directories." Thus, it can safely be concluded that, obtaining digital evidence from computer is not an easy task.

In *Muhammad Nasir v. Mahmood Shaukat Bhatti*[10] case the Lahore High Court (LHC) held that "computer technically is a modern technique and is well within the ambit of" Article 164 of the QSO. Same view was also affirmed by the Election Tribunal Balochistan in *Muhammad Akram Baloch v. Akbar Askani.*[11] Further, the tribunal observed that: -

> Similarly, electronic records mean, data, record or data generated, image or sound stored, received or sent in an electronic form or microfilms or computer generated microfiche. Thus, an electronic record can safely be considered as a document, because matter is recorded on the computer as bits and bytes, which are the digital equivalent of figures or marks, therefore, any document produced by a computer can be produced as evidence so long as it could be shown that the computer was functioning properly and was not misused.

5.3 WINDOWS

In 1985, Microsoft Corporation launched an operating system under the name of "Windows."[12] Thereafter, she introduced different versions and the older versions[13] of Windows

---

[7] Office of Legal Education Executive office for United States Attorneys, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal investigations,* 76.

[8] *United States v. Hill,* 322 F.Supp.2d 1081(C.D.Cal.2004).

[9] *United States v. Gray,* 78 F. Supp. 2d 524 (E.D. Va. 1999).

[10] *Muhammad Nasir v. Mahmood Shaukat Bhatti,* PLD 2003 Lahore 231.

[11] *Muhammad Akram Baloch v. Akbar Askani,* 2014 CLC 878, the tribunal held that "Computer technology being a modern device is well within the ambit of Article 164 of the Order of 1984."

[12] https://www.thoughtco.com/unusual-history-of-microsoft-windows-1992140 (accessed: 25th March, 2020).

[13] Microsoft's Windows operating system i.e. Windows 1 was first introduced in November 1985. Since then, Microsoft has introduced 9 versions of Windows and the latest version is Windows 10 which was released on 15th July, 2015.

are now somewhat outdated and are no longer in use. Although, mostly all the corporations, government entities and organization including the individual have switched to the newer versions of windows. It is possible that the investigator may have to examine the oldest versions of windows. Therefore, he must be aware of older versions as well.

In digital era, because of popularity of Microsoft Windows, LEAs, and investigators will encounter these systems "as sources of digital evidence in the majority of cases."[14] Whereas, various tools have been developed worldwide by the various organizations and departments "to facilitate the forensic examination of Windows systems."[15] Because of variety of Windows operating systems (OS) and applications, every sources of data cannot be described. As each case is different from other, therefore, it depends upon the digital investigator to explore "specific artifacts and operations on Windows systems."[16]

Windows OS registry stores a lot of data that "contains a great deal of information, including a comprehensive database containing information on every program that is compatible with Windows that has been installed on the computer."[17] Besides, it also consists of information about "the purported user of the computer, the preferences exercised by the user, information about the hardware components, and information about the network."[18] In this chapter, only Windows XP, Windows Vista and Windows 10 will be discussed briefly as old windows are no more in use in government departments and private organizations. It is pertinent to mention here, however, that complete working of windows is not concern of this research.

---

[14] Casey, *Digital Evidence and Computer Crime,* 513.
[15] Ibid.
[16] Ibid.
[17] Mason and Seng, *Electronic Evidence*, 8.
[18] Ibid.

5.3.1 WINDOWS XP

Since it hit the scene in 2001, Windows XP has been used as a standard Microsoft OS for many years. If it is seen in perspective of file systems, windows XP "continues to run on top of the File Allocation Table (FAT) and New Technology File System (NTFS) structures with which examiners have grown familiar."[19] FAT and NTFS will be discussed in detail in this chapter.

In Windows XP, there are certain features that can be very valuable in investigation for the digital investigators. Whereas, evidence of user activities is regularly recorded in such areas[20] which are easy to view by using right tool for the trained digital investigator. However, "other challenges (such as analyzing restore points, analysis of data in the Windows registry, collection and analysis of memory, dealing with RAIDs and dynamic disks, ovsercoming Windows encryption, and documenting data destruction) can present a much greater challenge, even for more experienced digital investigators."[21]

5.3.2 WINDOWS VISTA

Windows Vista was officially released in 2007. This Windows is available in multiple editions having its own abilities and features. For instance, Windows Vista Home "allows users to back up documents, and Vista Enterprise allows the creation of true-clone copies of the entire hard disk/partitions for later recovery or creation of identical systems."[22]

Windows vista, windows 2008, and windows 2007, shares many features and capabilities with Windows XP. Nonetheless, these operating systems are fundamentally different "from their

---

[19] Casey, *Handbook of Digital Forensics and Investigation,* 211.

[20] Event logs, Internet history, Prefetch files, thumbs.db files, and link files can be very useful in computer related investigation.

[21] Casey, *Handbook of Digital Forensics and Investigation,* 212.

[22] Ibid., 213.

older cousin in many aspects. Vista, Server 2008, and 7 depart from XP's tried-and-true path, even at such a basic level as the boot sequence, introducing things like the Windows Boot Loader and Boot Configuration Data (BCD)."[23]

There are few things in Windows Vista that make it unique which help the examiners in their investigations. For instance, in Windows Vista the Shadow Copy feature is enabled by default which "makes incremental backup copies of files and folders to aid in document recovery. The Windows Search feature in Vista indexes most of the user files and folders to aid users in searching for particular files."[24] Only these features are available in windows vista. Further, this makes "greater use of metatags and encourages users to add their own information to important files."[25] In addition, windows vista has the following features:

> The indexes created from the included locations can be searched by the examiner using keywords, which can be particularly fruitful if Windows indexed encrypted, encoded, or obfuscated files while they were open, decoded, and being worked with, thereby providing the examiner with access to information that is no longer readily available elsewhere on the system.[26]

5.3.3 WINDOWS 10

From the OS of Microsoft, the Windows 10 is the latest OS for computer. This was released on July 15, 2015.[27] There are many unique features in windows 10, which were not available in pervious windows. *Inter alia,* is "its support for universal apps. Universal apps can be designed to run across multiple Microsoft product families with nearly identical code."[28]

---

[23] Casey, *Handbook of Digital Forensics and Investigation,* 213.

[24] Ibid., 214.

[25] Ibid.

[26] Casey, *Handbook of Digital Forensics and Investigation,* 269.

[27] https://blogs.windows.com/windowsexperience/2015/06/01/hello-world-windows-10-available-on-july-29/ (accessed: 25th March, 2020)

[28] https://en.wikipedia.org/wiki/Windows_10 (accessed: 25th March, 2020).

Windows 10 also introduced "the Microsoft Edge web browser, a virtual desktop system, a window and desktop management feature called Task View, support for fingerprint and face recognition login, new security features for enterprise environments, and DirectX 12."[29]

5.4 FILE SYSTEMS

A file system (also known as file management and abbreviated as FS) is defined as "a process that manages how and where data on a storage disk, is stored, accessed and managed."[30] In addition, file naming, folders/directories, and metadata is also managed by the file system. Typically, a hard disk drive is used for this purpose which is "a logical disk component that manages a disk's internal operations as it relates to a computer and is abstract to a human user."[31] Initially, the FAT was used in windows but nowadays, "the most commonly used file system with Windows is NTFS."[32]

Without file management, "all files would have no organization and it would be impossible for a file with the same name to exist."[33] In any computer, normally files are managed in a hierarchy, which allows user "to view files in the current directory and then navigate into any subdirectories."[34] Understanding file systems for investigators and forensic examiner is important which helps them that "how information is arranged, giving insight into where it can be hidden on a Windows system and how it can be recovered and analyzed."[35]

---

[29] Ibid.
[30] https://www.techopedia.com/definition/5510/file-system (accessed: 25th March, 2020).
[31] Ibid.
[32] https://www.computerhope.com/jargon/f/filesyst.htm (accessed: 25th March, 2020).
[33] Ibid.
[34] Ibid.
[35] Casey, *Digital Evidence and Computer Crime,* 513.

There are several file systems having "different structure and logic, properties of speed, flexibility, security, size and more."[36] Some file systems, however, have been specially intended for specific applications. Generally, file systems which are being used nowadays includes "File Allocation Table 32 (FAT 32), New Technology File System (NTFS) and Hierarchical File System (HFS)."[37] FAT and NTFS are discussed below in detail.

5.4.1 FILE ALLOCATION TABLE

File systems are central in every cyber-crime case. A file allocation table (FAT) is a "file system developed for hard drives that originally used 12 or 16 bits for each cluster entry into the file allocation table."[38] FAT is used in operating systems to manage files on hard disk drives and other computer systems. Further, FAT is also "found on in flash memory, digital cameras and portable devices. It is used to store file information and extend the life of a hard drive."[39] The purpose of designation of FAT was "to reduce the amount of seeking and thus minimize the wear and tear on the hard disc."[40]

The earlier FAT12 "had a cluster addresses to 12-bit values with up to 4078 clusters.... The more efficient FAT16 increased to 16-bit cluster address allowing up to 65,517 clusters per."[41] Moreover, FAT32 has a 32-bit cluster address "with 28 bits used to hold the cluster number for up to approximately 268 million clusters. The highest-level division of a file system is a partition.

---

[36] https://en.wikipedia.org/wiki/File_system (accessed: 25th March, 2020).
[37] https://www.techopedia.com/definition/5510/file-system (accessed: 25th March, 2020).
[38] https://www.techopedia.com/definition/1369/file-allocation-table-fat (accessed: 25th March, 2020).
[39] Ibid.
[40] Ibid.
[41] Ibid.

The partition is divided into volumes or logical drives. Each logical drive is assigned a letter such as C, D or E."[42]

Remarkably, FAT file systems "do not record the last accessed time, but only the last accessed date. Listing the contents of a volume using the dir command displays some of this information but does not show the starting cluster—a critical component from the file system perspective."[43] So, the clusters containing a zero in any file system "are those free for allocation. If a FAT entry is greater than zero, this is the number of the next cluster for a given file or folder."[44]

5.4.2 NEW TECHNOLOGY FILE SYSTEM

The New Technology File System (NTFS) is an alternative to FAT file systems (i.e. FAT12, FAT16 and FAT32). The NTFS is "the standard file structure for the Windows NT operating system. It is used for retrieving and storing files on the hard disk."[45] Further, this file system also introduced "a number of enhancements, including innovative data structures that increased performance, improved metadata, and added expansions like security access control (ACL), reliability, disk space utilization, and file system journaling."[46] The NTFS is being used on all latest Windows. Further, the NTFS has replaced the earlier High-Performance File System and the FAT.

There are many beneficial features of the NTFS. The new reliable features of the NTFS "include a fault tolerance system that automatically repairs hard drive errors without error messages. The NTFS also retains detailed transaction records that keep track of hard drive errors.

---

[42] https://www.techopedia.com/definition/1369/file-allocation-table-fat (accessed: 25th March, 2020).
[43] Casey, *Digital Evidence and Computer Crime,* 515.
[44] Ibid., 516.
[45] Ibid.
[46] Ibid.

This feature is beneficial in recovering files if the hard drive crashes; it also helps to prevent hard disk failures."[47] In addition, these features include "security access control, improved metadata, file system journaling and disk space utilization. NTFS allows authorizations (like write, read or execute) to be set for files and specific directories. These file directories can also be located across more than one hard drive, but appear as one volume called a spanned volume."[48]

5.4.3 NTFS File Deletion

Whether make different between file deletion in NTFS and simply file being sent to recycle bin? In other words, what happens when a file is deleted in NTFS? Because of using deletion command, many things happen "under the hood," however, from the perspective of digital forensic examiner, important things are discussed as under:

i. The metadata of the file is changed: By delating any file, the deleted file's entry in the system "is removed from its parent index, and the file system metadata for the file's parent folder are updated."[49] There is a possibility that the metadata of the deleted file may be updated automatically. Nonetheless, the investigators should "exercise caution before drawing any conclusions from the metadata of a deleted file without other supporting or related evidence found elsewhere on the file system."[50]

ii. The two bytes "located at record offset 22 within the file's MFT record are changed from \x01\x00 (allocated file) to \x00\x00 (unallocated file)."[51]

---

[47] https://www.techopedia.com/definition/24482/new-technology-file-system-ntfs (accessed: 25th March, 2020); Casey, *Digital Evidence and Computer Crime,* 522.

[48] Ibid.

[49] Casey, *Handbook of Digital Forensics and Investigation*, 229.

[50] Ibid.

[51] Ibid.

iii. The appropriate locations "in $Bitmap are modified to show that both the space occupied by the MFT record and the space previously occupied by the file itself are now unallocated and ready for reuse."[52]

iv. Moreover, in any file system, deleting a file "in NTFS can also cause changes to the $LogFile, \$Extend\$UsrJrnl, and \$Extend\$Quota internal files."[53]

5.5 HARD DRIVE

Computer are composed of many compartments, *inter alia,* is hard drive and windows. Whereas hard drive[54] is composed of many platters or disks. A hard disk drive (HD, or HDD) is a non-volatile data[55] storage device. Normally, a hard drive is divided into many partitions. Commonly, a master boot record is "found at the beginning of the hard drive and contains a table of partition information. Each logical drive contains a boot record, a file allocation table (FAT) and a root directory for the FAT file system."[56] Whereas hard drive is "a non-volatile computer storage device containing magnetic disks or platters rotating at high speeds. It is a secondary storage device used to store data permanently, random access memory (RAM) being the primary memory device."[57] It is usually installed "internally in a computer, attached directly to the disk controller of the computer's motherboard. It contains one or more platters, housed inside of an air-sealed casing. Data is written to the platters using a magnetic head, which moves rapidly over them as they spin."[58]

---

[52] Ibid.

[53] Casey, *Handbook of Digital Forensics and Investigation*, 229.

[54] A hard drive is a "high-capacity self-contained storage unit containing a read-write mechanism together with one or more hard disks inside a sealed unit. *Oxford English Dictionary*, 2nd ed., s.v. "hard drive."

[55] Non-volatile means data is retained when the computer is turned off.

[56] https://www.techopedia.com/definition/5288/hard-disk-drive (accessed: 25th March, 2020).

[57] Ibid.

[58] https://www.computerhope.com/jargon/h/harddriv.htm (accessed: 25th March, 2020).

In a computer, a hard drive "fits inside a computer case and is firmly attached with the use of braces and screws to prevent it from being jarred as it spins. Typically, it spins at 5,400 to 15,000 RPM. The disk moves at an accelerated rate, allowing data to be accessed immediately."[59] However, hard drives operates "on high speed interfaces using serial ATA (SATA) or serial attached technology. When the platters rotate, an arm with a read/write head extends across the platters. The arm writes new data to the platters and reads new data from them."[60] But nowadays, hard drives use "enhanced integrated drive electronics (EIDE) including cables and connectors to the motherboard. All data is stored magnetically, allowing information to be saved when power is shut off."[61] The operating system data, installed software (all types of software), and the user's personal files are stored on hard drives. However, acquiring data from a computer hard drive many alter "the original state of the hard drive."[62]

As by the computer users, digital data and information is created, copied, stored, backed up, modified, altered and backed up on various hard drives. Therefore, this increase the chance of finding of digital evidence by the investigator that "a suspect may have destroyed on any other hard drive."[63] Instead of focusing on single hard drive, the investigator should also try to find digital evidence on other hard drives.

5.6 COPYING THE HARD DRIVE

The investigator must be having some basic knowledge with respect to operating systems, files systems and applications. Besides, he also be aware where information or data is stored or

---

[59] https://www.techopedia.com/definition/5288/hard-disk-drive (accessed: 25th March, 2020); https://www.computerhope.com/jargon/h/harddriv.htm (accessed: 25th March, 2020).

[60] https://www.techopedia.com/definition/5288/hard-disk-drive (accessed: 25th March, 2020).

[61] Ibid.

[62] Casey, *Digital Evidence and Computer Crime,* 19.

[63] Shavers, *Placing the Suspect behind the Keyboard,* 198.

hidden, how information in arranged and recovered, who has the access to the computer or network, whether it was possible for "an unauthorized outsider to obtain access to the computer from the Internet."[64]

Hard disk in a computer is very important in any investigation as the hard disk is a main internal storage of digital evidence. Therefore, an investigator must prefer to "remove the hard disk from the computer and attach it to a specialist 'write protected' interface that is attached to an 'imaging' device capable of copying the forensic image stored on the media on to a previously cleaned storage device."[65] In certain situations, removal of the hard drive "from a computer may not be possible or advisable, in which case it is common to leave the hard disk installed in the host computer and obtain access to it."[66]

In any case, instead of seizing an entire computer for examination at forensic laboratory or lab, the investigator should make a digital copy of the hard disk at the spot, which is the same as original. Whereas, this copy is called "an image copy or a copy that duplicates every bit and byte on the target drive including all files, the slack space, Master File Table, and metadata in exactly the order they appear on the original."[67] The image copy can be created as under:

> An image copy cannot be created by simply dragging and dropping icons or running conventional backup programs; the process of making one usually involves opening the computer case and connecting the investigator's own hardware directly to the hard drive. In some cases, investigators will make the image copy on-site; in others, investigators will seize the computer hardware from the premises and make the image copy off-site.[68]

---

[64] Mason and Seng, *Electronic Evidence*, 309.

[65] Ibid.

[66] Ibid.

[67] *United States v. Vilar*, 2007 WL 1075041 (S.D.N.Y. Apr. 4, 2007); *United States v. Stierhoff*, 477 F. Supp. 2d 423, 439 & n.8 (D.R.I. 2007).

[68] *Searching and Seizing Computers*, 78.

In many cases, copying entire hard drive is not required, as only limited portion is containing evidence. Keeping this situation in mind, various forensic imaging tools have been introduced which instead of imaging an entire hard disk copies specific data only. This technique has substantial benefits "where it is impractical to image an entire drive due to the amount of data required to be copied or because of time constraints. It should be noted that file hashing and image hashing techniques are still used to ensure the integrity of the data that is collected."[69]

In USA, any party can request the court to provide the record of any hard drive from the other party. In this situation, a forensic expert is appointed "to make a mirror image of the computer hard drive and perform the analysis with a protective order prohibiting disclosure of privileged information," as held by the court in *Sony BMG Music Entertainment v. Arellanes,*[70] where the court refused direct access to the computer hard drive. The forensic expert provides his report to the party who can review and separate the privileged documents. In *State v. Cook*,[71] the court, held that after the testimony of expert witness regarding imaging process, authenticity and possibilities of tampering the evidence was admissible. In *Ahmad Omar Sheikh v. the State*,[72] the trial court convicted the appellants, *inter alia,* on the basis of mirror image of accused's laptop. However, the SHC on the basis of contradiction in evidence acquitted the appellants. The SHC decision was maintained by the SC in appeal.[73]

---

[69] Mason and Seng, *Electronic Evidence*, 310.

[70] *Sony BMG Music Entertainment v Arellanes,* LEXIS 78399 (E.D. Tex. Oct. 27, 2006).

[71] *State v. Cook*, WL31045293 Ohio Ct. App. (2002).

[72] *Ahmad Omar Sheikh v. the State*, 2021 YLR 1777 (Sindh).

[73] *The State through P.G. Sindh v. Ahmed Omar Sheikh*, 2021 SCMR 873.

A forensic report should clearly record all steps undertaken by the forensic examiner to make it more authentic that if in future, any objection is raised the third party may perform such procedures. In *Nucor Corp v. Bell,*[74] the court accepted expert witness testimony and held that the method used by the expert, for examination of hard drive, "sufficiently filled the analytical gap between the data and the opinion." The court also admitted the evidence as the expert had systematically documented each step in the test.[75]

5.7METADATA

Metadata is "data about data."[76] Metadata is information "that describes or places data in context, without being part of the data that is the primary focus of the user."[77] In other words, it is an indispensable element of electronic documents, while printing the documents it can be lost, thus it will be very difficult to refer back to the original files, though some important information is not recorded. In fact, metadata[78] is gold mine of valuable information in any case for the investigator. It can be found "inside a file, kind of behind the scenes where an ordinary computer user will not see it, or in an external data store such as Internet history files that record information about files."[79] Besides, if the time on the computer or digital device is not correct, then the metadata will be false.[80]

---

[74] *Nucor Corp v. Bell,* 251 F.R.D. 191 (D.S.C. 2008).

[75] Ibid.

[76] *Netword LLC v. Centraal Corp.,* 242 F.3d 1347 (Fed. Cir. 2001).

[77] Casey, *Handbook of Digital Forensics and Investigation*, 230; Daniel et al, *Digital Forensics for Legal Professionals*, 179.

[78] In USA, LEAs collected metadata which was criticized there. For detail, Margaret Hu, "Bulk Biometric Metadata Collection," *North Carolina Law Review*, 96 (2018): 1425-1474.

[79] Daniel et al, *Digital Forensics for Legal Professionals*, 179.

[80] Mason and Seng, *Electronic Evidence*, 28.

Metadata is a unique characteristic and feature of electronic documents, which does not exist in conventional paper-based documents. Tamberlin Judge in *Jarra Creek Central Packing Shed Pty Ltd v. Amcor Limited* held as under:

> Meta-data can be used to ascertain the author and origin of a document, the existence of any attachments, and whether the document was sent or received by any particular individual. The information which is contained in the meta-data is not visible on a print-out of the relevant document, which shows only the face content and does not disclose the layers of electronic data beneath the visually readable information.[81]

Metadata is used by "the file system for system administration tasks, and for the generation, handling, transfer and storage of data within the system. This metadata can contain a plethora of information about the document itself, which would not be visible if the document is printed out."[82] Generally, it will include creation date, accessed date, modification date, and the data sent and received. In the words of Mason and Seng:

> All documents in electronic format will contain metadata in one form or another, including email communications, spreadsheets, websites and word processing documents. In fact, an electronic document has to have metadata to help interpret the purpose of the digital document. Such data can include, and be taken automatically from the originating application software, or supplied by the person who originally created the record. The list of information that is available includes, but is not limited to: when and how a document was created, the file type, the name of the purported author, the location from which the file was opened or where it was stored, when the file was last opened, when it was last modified, when the file was last saved, when it was last printed, the identity of the purported previous authors, the location of the file on each occasion it was stored, the details of who else may be able to obtain access to it, and, in the case of email, blind carbon copy (bcc) addresses.[83]

In any electronic document, metadata of the said document provides "an additional layer of encoded information within the main file."[84] Metadata is "typically created automatically by the software and without knowledge of the user, it is therefore also more difficult to alter, manipulate

---

[81] *Jarra Creek Central Packing Shed Pty Ltd v. Amcor Limited* [2006] FCA [11].
[82] Stanfield, "The Authentication of Electronic Evidence," 62.
[83] Mason and Seng, *Electronic Evidence*, 27.
[84] https://www.rand.org/pubs/research_reports/RR890.html (accessed: 25th October, 2019).

or delete."[85] Thus, it is established no human intervention is required in creation of metadata. Same is created for mobile devices as well. Although, there are various options available to disable encoding on these devices. Metadata, is very important for investigators in any investigation of computer related crimes. Nevertheless, this must be kept in mind that "this data can be altered either directly or remotely by a knowledgeable technology consumer—as a result, investigation protocols will need to become more sophisticated as strategies shift focus onto metadata validation."[86] It is pertinent to mention here that investigators should be aware "that metadata associated with Microsoft Office documents can be altered using freely available tools."[87]

In *Armstrong v. Executive Office of the President, Office of Administration*[88] with respect to hard copy printed version of the documents the court held that printed version "may omit fundamental pieces of information which are an integral part of the original electronic records, such as the identity of the sender and/or recipient and the time of receipt." In *United States v. Hamilton,*[89] the U.S. Court of Appeals held:

> that the District Court had correctly concluded that the header information that accompanied each pornographic image was not hearsay. Of primary importance to this ruling is the uncontroverted fact that the header information was automatically generated by the computer hosting the newsgroup each time Hamilton uploaded a pornographic image to the newsgroup. In other words, the header information was generated instantaneously by the computer without the assistance or input of a person. As concluded by the district court, this uncontroverted fact clearly places the header information outside of Rule 801(c)'s definition of "hearsay." In particular, there was neither a "statement" nor a "declarant" involved here within the meaning of Rule 801.

---

[85] Mason and Seng, *Electronic Evidence*, 27.
[86] https://www.rand.org/pubs/research_reports/RR890.html (accessed: 25th October, 2019).
[87] Casey, *Handbook of Digital Forensics and Investigation*, 235.
[88] *Armstrong v. Executive Office of the President,* 1 F.3d 1274 (D.C. Cir. 1993).
[89] *United States v. Hamilton,* 413 F.3d 1138 (10th Cir. 2005).

There is disadvantage for the criminal that "there is a good probability that old data can be recovered using appropriate tools."[90] As files can be deleted easily, therefore "their meta-data can no longer be considered entirely reliable, so information such as the MAC (modified, accessed, created) times cannot be relied upon in the same way as it is for live data."[91]

Metadata-based recovery "may be required to look for that missing or elusive file and is used when metadata from the deleted file has not been erased. The file may have been relocated, such as being moved from one folder to another."[92] However, this may prove problematic "to detect as it is not uncommon when a file has been reallocated to recover two or more unallocated metadata entries that have the same file address."[93] Whereas opening the file may recover the author of a text document but without using some form of write protection "such action may contaminate the file metadata. Preserving the file in pristine condition to prevent unintentional modification to the file contents and metadata is an overriding requirement of sound forensic practice."[94]

In *Lorraine v. Markel*[95] the court held that any electronic document can be authenticated using metadata. In the words of court, "Because metadata shows the date, time, and identity of the creator of an electronic record, as well as all changes made to it, metadata is a distinctive characteristic of all ESI that can be used to authenticate it under Rule 901(b)(4)."[96] Metadata, being a very important piece of evidence, whether the electronic documents are to be produced with metadata included or

---

[90] Marshall, *Digital Forensics Digital Evidence in Criminal Investigation*, 50.
[91] Ibid.
[92] Boddington, *Practical Digital Forensics*, 36.
[93] Ibid.
[94] Ibid., 38.
[95] *Lorraine v. Markel American Insurance Co.*, 241 F.R.D. 534 (D. Md. 2007).
[96] Ibid.

not. A Kansas federal court held that "when a party is ordered to produce electronic documents as they are maintained in the ordinary course of business, the producing party should produce the electronic documents with their metadata intact, unless that party timely objects to production of metadata, the parties agree that the metadata should not be produced, or the producing party requests a protective order."[97]

5.7.1 THE PURPOSE OF METADATA

Everything has its own purpose but the purpose of metadata is "to store information about other data. This can help with the organization and retrieval of data."[98] It has been pointed out by the forensic examiner that web pages on the Internet have metadata in the form of meta-tags whereas a meta-tag is coded into a website where lay man cannot see it, but "it contains information about a website, such as keywords so that it can be easily found when those keywords match your Google search."[99] This can help the investigator to apprehend the accused.

Metadata can also be found inside pictures[100] and videos. Metadata of pictures and videos can contain information such as "when the picture was taken and the make and model of the camera the picture was taken with."[101] In case of Microsoft office documents, the investigator can get the details of "the author, the creation date, the last modified date, and so forth. All of this information is contained in the document's metadata."[102]

---

[97] *Williams v. Sprint/United Management Co.*, 230 F.R.D. 640, 652 (D.Kan. 2005).

[98] Daniel et al, *Digital Forensics for Legal Professionals,* 179.

[99] Ibid.

[100] *United States v.Christopher R. Metsos,* is the case of USA, which was filled before the Honorable Judge L.Cott of the United States Magistrate Judge (Southern District of New York), on 15th June 2010, where the alleged Russian used the websites to send data. On 8th July, 2010, the FBI website reported that the "Ten Russian agents pleaded guilty and are to be removed from the United States." https://archives.fbi.gov/archives/newyork/press-releases/2010/nyfo070810a.htm (accessed: 21st April, 2020).

[101] Daniel et al, *Digital Forensics for Legal Professionals,* 180.

[102] Ibid.

5.7.2 TYPES OF METADATA

There are three types of metadata, such as descriptive, structural and administrative metadata. These are discussed briefly in this study.

i. Descriptive metadata: As this is clear from its name, it describes "a resource for a particular purpose, such as a disclosure or discovery exercise. The metadata may include such information as title, key words, abstract and the name of the person purporting to be the author."[103]

ii. Structural metadata: It describe "how a number of objects are brought together. Some examples of structural metadata include file identification, file encoding, file rendering, content structure and source."[104]

iii. Administrative metadata: This provides information "to help with the management of a resource. Administrative data is further divided into rights management metadata and preservation or record-keeping metadata."[105]

5.8 ENCRYPTION

Encryption (or enciphering) is the mechanical process by which a readable digital object (cleartext) is converted into an unreadable digital object using a mathematical function to hide the substance of the content which cannot be easily understood by unauthorized persons without using a key or password.[106] However, encryption can be "bypassed with sophisticated software and

---

[103] Mason and Seng, *Electronic Evidence,* 28.

[104] Ibid.

[105] Ibid.

[106] Casey, *Digital Evidence and Computer Crime,* 458; Mason and Seng, *Electronic Evidence,* 261; Sammons, *Basics of Digital Forensics*, 85.

hardware which can try thousands of potential passwords per second in the attempt to guess the password." Yet, accessing the stronger and complex encryption algorithm is very difficult.

Whereas decryption is the reverse of encryption which is defined as "the transformation of encrypted data back into an intelligible form."[107] Some clients support encryption, "making it more difficult for investigators to monitor communications and recover digital evidence."[108]

Encryption has both advantages (legitimate use) and disadvantages (illegitimate use) alike. Because of its legitimate use, everybody is enjoying the service of the internet. Users have "less direct control over these secrets as they travel over the Internet or fly through the air on a wireless network. It is encryption that provides us with both the mechanism and confidence to store and transmit our most sensitive digital information."[109] For instance, encryption build the confidence of the consumer to buy their favorite products from online service and stores. Without using encryption, running online business is not safe and secure. Whereas, this technique is also being used by the criminals to gain benefits for their purpose. Still, the complexity of encryption prevents attacks on data basis and online transactions.

Technology has provided ample opportunity to encrypt any live system, either as a whole or in part. Nowadays, in new operating systems this feature is built in, there is no need for separate software installation as was required in previous operating systems to install the encryption software. There are many freely encryption programs available, which can be used for encryption purpose, if this feature is not built in. Thus, ignoring encryption possibilities "on a suspect computer will eventually lead to extremely short forensic examinations because when encrypted,

---

[107] Marcella and Menendez, *Cyber Forensics,* 51.
[108] Casey, *Digital Evidence and Computer Crime,* 694.
[109] Sammons, *The Basics of Digital Forensics the Primer for Getting Started in Digital Forensics*, 85.

there is little that can be done to examine an encrypted system without the decryption keys."[110] So, the investigator should be aware about encryption programs as well and he should also keep in mind that files, folders, the Internet use, calls, and electronic communication can also be encrypted.

Encryption has presented significant challenge for investigator and "digital forensic practitioners, particularly full disk encryption. Even when full disk encryption is not used or can be circumvented, additional effort is required to salvage data from password protected or encrypted files."[111]

In Pakistan, encrypted data was defined in the Prevention of Electronic Crimes Ordinance, 2007 (PECO),[112] thereafter the same definition was adopted in PECO, 2008 and PECO 2009[113] respectively. Further, misuse of encryption was made an offence under these ordinances.[114] Since these Ordinances lapsed after completion of their constitutional time and never promulgated again, thus, this definition is not in field now. Instead, PECA was promulgated in 2016 which covered many aspects of cyber-crimes.

In addition, a huge challenge for LEAs and investigator is "in the context of collecting e-evidence and criminal intelligence is the growing misuse of legitimate anonymity and encryption

---

[110] Shavers, *Placing the Suspect behind the Keyboard*, 15.

[111] Casey, *Handbook of Digital Forensics and Investigation*, 39.

[112] Section 2 (1) (m) of the PECO defines encrypted data which means "data which has been transformed or scrambled from its plain version or text to an unreadable or incomprehensible format and is recoverable by an associated decryption or decoding technique, regardless of the technique utilized for such transformation or scrambling and irrespective of the medium in which such data occurs or can be found for the purposes of protecting such data."

[113] It is penitent to mention here that this Ordinance was enacted twice in 2009 (VIII of 2009 & XIV of 2009).

[114] Section 11 of these ordinances provides as "Whoever for the purpose of commission of an offence or concealment of incriminating evidence, knowingly and willfully encrypts any incriminating communication or data contained in electronic system relating to that crime or incriminating evidence, commits the offence of misuse of encryption shall be punished with imprisonment of either description for a term which may extend to five years, or with fine, or with both."

services and tools for illegal purposes. This poses a serious impediment to the detection, investigation and prosecution of crime."[115] In USA, *In re Grand Jury Subpoena to Sebastien Boucher*[116] is a case of laptop hard drive encryption in which subpoena was issued for the accused (i.e. Boucher), instructing him to provide all documents reflecting passwords (if any) used or associated with the laptop. Moreover, a similar approach in a laptop matter was taken by the court in *United States of America v. Gavegnano.*[117] However, the honorable Judge Borman of the Eastern District of Michigan in *United States of America v. Kirschner*[118] has taken a different view and decided that the subpoena demanding the defended to give password should be quashed on the basis that government is not pursuing for documents rather testimony from the defendant which would be used against the defendant to incriminate him. In *United States v. Ramona Camelia Fricosu,*[119] the court held as "unless the government establishes by at least a preponderance of the evidence that the laptop that is the subject of the application belonged to defendant, requiring her to provide the password thereto would force her to admit ownership of the laptop, in ostensible violation of the Fifth Amendment."

In re Grand Jury Subpoena Duces Tecum[120] the Tjoflat Judge held that:

> ... the decryption and production of the hard drives would require the use of the contents of Doe's mind and could not be fairly characterized as a physical act that would be nontestimonial in nature. We conclude that the decryption and production would be tantamount to testimony by Doe of his knowledge of the existence and location of potentially incriminating files; of his possession, control, and access to the encrypted portions of the drives; and of his capability to decrypt the files.

---

[115] Biasiotti et al. *Handling and Exchanging Electronic Evidence across Europe*, 144.

[116] *In re Grand Jury Subpoena to Sebastien Boucher*, 2007 WL 4246473 (D.Vt.); *In re Grand Jury Subpoena to Sebastien Boucher*, 2009 WL 424718 (D.Vt.). This case has long story, which need not to discuss here. However, the court directed to the Boucher to provide password of encrypted drive of his laptop.

[117] *United States of America v. Gavegnano,* 305 Fed.Appx. 954 (4th Cir. 2009).

[118] *United States of America v. Kirschner*, 2010 WL 1257355 (E.D.Mich.).

[119] *United States v. Ramona Camelia Fricosu a/k/a/ Ramona Smith,* 2012 WL 182121 (D.Colo.).

[120] *In re Grand Jury Subpoena Duces Tecum,* 670 F.3d 1335 (11th Cir. 2012).

> We are unpersuaded by the Government's derivation of the key/combination analogy in arguing that Doe's production of the unencrypted files would be nothing more than a physical nontestimonial transfer. The Government attempts to avoid the analogy by arguing that it does not seek the combination or the key, but rather the contents. This argument badly misses the mark.

In USA, the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR) impose controls on the export of certain forms of encryption. But, section 103(a) of the CALEA[121] has imposed certain capabilities requirements on the telecommunications carriers.

Investigator are capable to defeat encryption which is created by common use applications by using right tools at the right time. If encryption is created by using sophisticated techniques and technology, still, sometime this is beyond the capability of the trained professional investigator to decrypt any digital data by using software. Though, there exist possibility to decrypt the data by extending the scope of investigation and taking help from other specialized LEAs in the subject.

5.9 DIGITAL EVIDENCE AND *ALIBI*

Alibi is Latin word which means "somewhere else." An *alibi* is a defense plea used by the accused in criminal proceedings wherein he attempts to prove that he was not present at the time of occurrence of a crime rather he was somewhere else at the time of commission of alleged offense. In Pakistan, Article 24 of QSO discuss the plea of alibi.

In case the accused takes the plea of alibi then the main parts of information "are time and location. When an individual does anything involving a computer or network, the time and location are often noted, generating digital evidence that can be used to support or refute an alibi." For instance, let say in a murder case (suppose a murder is committed at Islamabad), defendant claims

[121] Communications Assistance for Law Enforcement Act also known as the "Digital Telephony of 1994.

that he was in office at Karachi at the time of occurrence of crime and working on a company (organization or entity) computer. So, activities of the accused on certain computer or computing device can help in establishing or refuting an *alibi.*

Many organizations keep the records of various activities including dates, times and locations. For example, if a person uses his ATM, the CCTV will record his footage, besides recording the date, time and location of transaction. Similarly, other companies and departments will record such details. These records remain for indefinite time period of the system of the organization.

In addition to this, sometimes the internet also contains a lot of information about an activity. In case of email message, when an email is dispatched, then its time, originating IP address are noted in the header of the said email. Besides, log files "that contain information about activities on a network are especially useful when investigating an alibi because they contain times, IP addresses, a brief description of what occurred, and sometimes even the individual computer account that was involved."[122]

The investigator must be vigilant while dealing with digital evidence on plea of an alibi, as IP address of computer can easily be manipulated by the criminal to create a false alibi. Further, anyone having basic knowledge of the computer can easily change the clock time making more difficult for the investigator to know the exact time. Likewise, IP addresses can easily "be changed, allowing individuals to pretend that they are connected to a network from another location."[123]

---

[122] Casey, *Digital Evidence and Computer Crime,* 324.
[123] Ibid.

It should be noted by the investigator that in case of investigating an alibi that no "supporting evidence can prove conclusively that an individual was in a specific place at a specific time. When dealing with digital evidence it is often difficult to prove that a specific person was using the computer or mobile device at the time in question." Even otherwise, when "a person's mobile device can be tracked to a location, it does not necessarily prove that the person was there."[124] In any case, additional corroborating evidence is always required to link the accused with the act.

5.10 COMPUTER PRINTOUTS

Everywhere in the world, computer printout is being used in evidence. In 2002, first time in Pakistan this issue was discussed by the legislature and legislated through the ETO on print out. In USA, through the FRE this concern has been expressly addressed. The Rule 1001 (3) of FRE states that "[i]f data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original'."[125] The best evidence rule generally requires that parties must provide original to prove the contents of a document.[126] In computer, the original is in either 1 or 0. How it will be presented in evidence? In recognition the demands of practicality and common usage, the legislature in Pakistani provided the print out the status of original and amended Article 73 of the QSO in 2002 in line with the rule 1001 (3) FRE of USA. Whereas, in *Doe v. United States*, it was concluded by the court than an authentic/true printout of computer data will satisfies the best evidence rule.[127] On the basic of this rule, the computer forensics investigators in USA "treated bit-stream images as originals." In a recent case of *Ohio v.*

---

[124] Casey, *Digital Evidence and Computer Crime,* 324.
[125] Rule 1001(3) of FRE.
[126] Article 73 of the QSO.
[127] *Doe v. United States*, 805 F. Supp. 1513 (D. Haw. 1992).

Michael J. Morris,[128] the Court in USA accepted the evidence "presented from a bit stream copy of an evidence disk."

In this technological regime, keeping in view the compelling circumstance of digital world and requirements of existing ICT scenario, Article 59 of the QSO was also amended and few words were added and substituted to clarify the situation/position, after the amendment the Article 59 is read as under;

> **Article 59.** When the Court has to form an opinion upon a point of foreign law, or of science/or art, or as to identity of hand-writing or finger impressions, **or as to authenticity and integrity of electronic documents made by or through an information system;** the opinions upon that point of persons specially skilled in such foreign law science or art, or in questions as to identity of hand-writing or finger impressions **or as to the functioning, specifications, programming and operations of information systems, are relevant facts.** (The words in bold were added and substituted by the ETO)

In Pakistan, Article 73 of the QSO is about primary document. In this Article, for the recognition of print out electronic documents, the following two explanations were inserted in 2002:

> *Explanation 3.* – A printout or other form of output of an automated information system shall not be denied the status of primary evidence solely for the reason that it was generated, sent, received or stored in electronic form if the automated information system was in working order at all material times and, for the purposes hereof, in the absence of evidence to the contrary, it shall be presumed that the automated information system was in working order at all material times.
>
> *Explanation 4.* – A printout or other form of reproduction of an electronic document, other than a document mentioned in Explanation 3 above, first generated, sent, received or stored in electronic form, shall be treated as primary evidence where a security procedure was applied thereto at the time it was generated, sent, received or stored.

In *Arif Hashwani v. Sadruddin Hashwani*,[129] the SHC held that:

> .....opinion of a forensic witnesses relating to authenticity or integrity of electronic document made, by or through any information system also made admissible from the Explanations 3 and 4 to Article 73 of the Qanun-e-Shahadat Order, 1984 relating to

---

[128] *Ohio v. Michael J. Morris,* Court of Appeals of Ohio, Ninth District, Wayne County, No. 04CA0036, Feb. 16, 2005.

[129] *Arif Hashwani v. Sadruddin Hashwani,* PLD 2007 Karachi, 448.

preliminary evidence, it is evident that printout or other form of reproduction of another electronic document be made admissible, in evidence as preliminary evidence.

In *Mst. Rehana Anjum v. Additional Sessions Judge,*[130] the above said explanation was referred in a murder case, without mentioning whether this is applicable or not? Thus, nothing was proved or disproved except the Statistical Assistant's report was allowed to be produced in the evidence.

In United States v. Catabran,[131] the court held that computer printouts are admissible and held that "[a]ny question as to the accuracy of the printouts, whether resulting from incorrect data entry or the operation of the computer program, as within accuracies in any other type of business records, would have affected only the weight of the printouts, not their admissibility." Earlier, the court in *United States v. Vela,*[132] accepted computerized telephone bills in evidence and held that computerized reports "would be even more reliable than... average business record(s) because they are not even touched by the hand of man."

Authentication of computer printouts is also required under the evidence law of Pakistan and USA which can be authenticated by a witness by testifying before the competent court that the printout constitutes a complete record of all the relevant events or transactions.[133] As discussed earlier in this chapter, that encryption make it very difficult to accesses the content of any document, hard drive or digital device. This has also strengthen the authenticity of the relevant

---

[130] *Mst. Rehana Anjum v. Additional Sessions Judge,* PLD 2016 Lahore 570.

[131] *United States v. Catabran,* 836 F.2d 453 (9th Cir. 1988).

[132] *United States v. Vela,* 673 F.2d 86 (5th Cir. 1982).

[133] In *United States v. Melenberg,* 263 F.3d 1177 (10th Cir. 2001), the court held that printouts were "a record of all transactions and reflected the underlying records"; in *People v. Markowitz*, 721 N.Y.S.2d 758 (Sup. Ct. February 9, 2001), the court held that testimony of a company employee who prepared the databases was sufficient foundation for admission of the electronic evidence. In *United States vs. Miller*, 771 F.2d 1219, (9th Cir. 1985), the court held that "telephone company billing supervisor can authenticate phone company records."

information.[134] If there is any issue regarding admissibility of computer generated records that can be handled by the forensics expert.[135] Whereas, in case of authentication of the internet chat logs the court in *United States v. Tank*[136] held that "printouts of computer-generated logs of 'chat room' discussions may be established by evidence showing how they were prepared, their accuracy in representing the conversations, and their connection to the defendant."[137] However, in the *Griffin v. State*[138] the court held that the " potential for abuse and manipulation of a social networking site by someone other than its purported creator and/or user leads to our conclusion that a printout of an image from such a site requires a greater degree of authentications."

There are various problems[139] linked with the computer print-outs. The first is that only print out of the documents is submitted in the court, whereas copies in the electronic forms are not provided to the defense counsel, rather the same is declined. If the opposite counsel request for the electronic copies of the relevant documents than what will happen? Whether the prosecution will provide the electronic copies or not? If it is supposed, for the sake of arguments, that the print out is real evidence, and the same is received as prime facie evidence of the relevant entries of the said document (which have been provided in evidence in court). Whether this will add extra cost and burden upon the prosecution or not? Whether this request will be unreasonable?

---

[134] In *State v. Levie,* 695 N.W.2d 619 (Minn. Ct. App. June 10, 2005), the court "admitted testimony of a computer forensic expert about defendant's computer usage and the presence of an encryption program on his computer deemed admissible."

[135] In *Galaxy Computer Services, Inc. v. Baker*, 2005 WL 2171454 (E.D.Va. 2005), the court discussed the "testimony of a computer forensics expert concerning files deleted from a computer hard drive"; in *Kupper v. State of Texas*, 2004 WL 60768 (Ct.Ap. Texas, January 14, 2004), the court discussed the "testimony of a computer forensics expert concerning chain of custody and examination of a computer hard drive."

[136] *United States v. Tank*, 200 F.3d 627 (9th Cir. 2000).

[137] Casey, *Digital Evidence and Computer Crime,* 61.

[138] *Griffin v. State,* 19 A.3d 415 (Md.2011).

[139] All these questions, which are raised in these pages are taken from *Electronic Evidence* book by Mason and Seng.

The second issue is that the technical literature on the subject shows that all programs have significant error[140] rates, if the defense counsel raises this issue that "there must be some errors in the documents that affect the figures." Thus, it will not be right to accept any document without the electronic versions of the printed documents presented in the evidence which may also be required to be examined by the appropriate digital evidence professional.

The third issue is that there is a presumption that all the mechanical instruments were in working order at the material time. There is no justification to include the computer in this category. If print out of any document is considered to be business record. In the words of Mason:

> The exception permits records to be adduced because, in the past, employees entered information into physical books by hand, and this meant they could be relied upon as a record made at that point in time, and one could ascertain at a glance whether somebody tried to change the entries. The justification was that such records were more reliable than the memory of a witness. This might have been so, but records in electronic form are notorious for being inaccurate for a variety of reasons, and it must be common sense that this rule cannot be relied upon in the twenty-first century.[141]

The fourth issue is that whether the computers are reliable? Does computer print-out is authentic, in a sense that they have not been tampered with? Does the computer-print out are valid? That they contain the information that is claimed of them? If it is presumed that computer-print out documents are valid, then what evidence is there that the users of the document checked that the algorithms (and other formulas) were correct? If it is presumed that the computers are reliable includes the maintenance of the documents and who wrote them, and what qualification they had to be able to program reliably. If it is presumed that the software code of the operating system is reliable? How does he know? How many updates have there been since the document began to

---

[140] The most obvious example of software error is the ATM, which is very common nowadays and almost everybody is aware of this. Sometime, when someone withdraw the money from the bank ATM, he receives the receipt and does not receive the money. In some cases, amount withdrawn from bank ATM is greater or less than the amount keyed in. There are certain reasons of software failure, which are discussed by Mason, in *Electronic Evidence* book, along with examples. For further details, see Mason and Seng, *Electronic Evidence*, 120-143.

[141] Mason and Seng, *Electronic Evidence,* xii-xiii.

operate? Were all updates applied? When updates occurred, how did they affect the application software? What is his measure of reliability?

While entering the data in the computer or in data base, errors can often occur. Besides, many electronic and mechanical errors can also cause inaccuracies in the output (print out). If it is presumed that there are no errors of logic that can lead to an incorrect result? What evidence does he have of this, considering the number of software code updates to the documents? What are the number and purposes of each software (used in the preparation of the documents) update since its inception.

Whether the employees that input the figure are always accurate? And whether the system is so reliable that inaccurate inputs are recognized and corrected, and that these corrections are recorded?

Whether there are no errors or omission where the formula is wrong? In printed document, which process is reliable? All of it? Parts of it? If part of it, which part and for what reason?

Finally, that if only paper versions (print-outs) of the record are to be admitted, that the full information will be provided by the prosecution side?

Thus, in many cases, the soft-ware users many not discover errors in the system until after many months or years. Therefore, the reliability and accuracy of computer printouts, inter alia, depend upon the trustworthiness and accuracy of a computer system's hardware, software,[142] data entry procedures, and system security.

[142] Computer software is divided into two categories: system software and application software. System software is also referred as operating system.

5.11 SUMMARY

Digital evidence is fragile as it can easily be manipulated. Collecting digital evidence is very difficult in live system, when the data is constantly changing. In computer this can be collected from windows. Metadata and encryption create more problems for the investigators to properly investigate and authenticate the evidence. Whereas, in case of printing of any document, metadata of the said document is never printed on the documents. Moreover, the metadata can easily be changed. However, there are certain characteristics which help the expert to examine the alteration in digital evidence.

CHAPTER SIX:

DIGITAL EVIDENCE ON MOBILE DEVICES AND CLOUD SYSTEMS

6.1 INTRODUCTION

Everyone is using mobile phone for various purpose. This can also be used for business, education, health, entertainment and criminal activities. All such activities leave some evidence, which can be very helpful for the investigator to investigate the behavior and activities of the user. In other words, this is a useful and important tool to investigate any crime in existing regime as in every case, mobile phone is being used. This chapter discuss the digital evidence on mobile devices. Keeping in view the volubility of mobile phone, many aspects of mobile evidence has been discussed in this chapter in particular, mobile operations, CDR, International Mobile Equipment Identity (IMEI), Subscriber Identity Module (SIM), cellular networks and their components. Besides, handling of mobile device is also discussed as the process is little bit different from computer handling. In later part of this chapter, GPS has also been discussed as these are integral part of virtual world.

Now, the world is moving fast and moving towards paper less environment. Even, many organization and departments (including government departments) avoid to purchase expensive hardware and software for their usual and routine operations. Instead they rely on cloud systems, making job of investigator more difficult as the cloud server are located beyond the territorial jurisdiction of the country which is using the cloud system. In many of the cases, different law applies on both countries and acquiring the requisite data from the cloud system host may be very difficult. Hardware and software both can be hired in cloud environment. Microsoft is the famous

case on cloud system, which is also discussed that how the cloud system affected their legal system. This, aspect is also discussed in this chapter as well.

6.2 Digital Evidence on Mobile Devices

Almost, every one, in today's world, is using mobile phones creating and transmitting large amount of digital data. This data and information is valuable in investigation. These devices are creating various types of data. In addition to this, e-mails are being accessed through these devices and social media is also being used through mobile phones. Though, with the availability of these devices, every day, masses are creating evidence around the world. These items can be used to establish the intent, alibi, location and contact with last person (in case of murder or kidnapping). Now, mobile devices have stared diverse services, including "communication (e.g., voice, SMS, e-mail), Internet access (web browsing), and satellite navigation (GPS). These technological advances create new opportunities for criminals while providing valuable sources of evidence."[1] No one can rule the possibility of getting information from these devices. These are a rich source of digital evidence.

Understanding what mobile device[2] is imperative for investigator. A mobile is defined as "any instrument that can connect to and operate on a mobile network, including cellular telephones, wireless modems, and pagers."[3] As compared to computer, it is person specific, it is carried by everyone irrespective of his status, and it help the investigator to trace the person using mobile devices. No other device is capable to help locate the criminal.[4] Due to its volubility,

---

[1] Casey, *Handbook of Digital Forensics and Investigation*, 517.

[2] Mobile device in Pakistan is defined in "Mobile Device Identification, Registration and Blocking Regulations, 2017 which means "a communicating device that uses SIM(s) (Subscriber Identity Module) such as mobile phone, SIM based tablet, SIM Based Router etc."

[3] Casey, *Handbook of Digital Forensics and Investigation,* 518.

[4] Casey, *Digital Evidence and Computer Crime,* Chapter 20, page no. 1.

investigators have started its use "for conventional crimes, often focusing on location information, logs of telephone calls, printouts of SMS messages, and associated metadata."[5]

Cellular phones could do no more than connecting two or more people on phones "over a short distance for the purpose of voice communications between two parties on the same radio network."[6] These days, mobile phones can do everything which a computer can do, as they are easy to carry. Every time, when a mobile device is used to "make a call, send an e-mail or text message, or used as a push-to-talk radio, a record is created by the cell phone company that can later be retrieved and used as evidence."[7] Further, these devices atomically records "contact lists, call logs, pictures, video, e-mail, text messages, and in some cases, even GPS location information."[8] Thus, everything is recorded by the cellular network provides. But, it must not be ignored that every cellular company has different policy for data retention.

Many mobile phones which are easily available in market are equipped with high quality cameras "that have the ability to capture pictures and even video clips with audio. These pictures or video clips can then be sent to e-mail addresses or other mobile phones."[9] Such data may contain potential evidence for forensic examination, which "the cyber forensic investigator must be prepared to analyze."[10]

---

[5] Casey, *Handbook of Digital Forensics and Investigation*, 517.

[6] Daniel et al. *Digital Forensics for Legal Professionals*, 8.

[7] Daniel et al. *Digital Forensics for Legal Professionals*, 8; Casey, *Digital Evidence and Computer Crime*, Chapter 20, page no. 1.

[8] Daniel et al. *Digital Forensics for Legal Professionals*, 8; Casey, *Digital Evidence and Computer Crime*, Chapter 20, page no. 1.

[9] Marcella and Menendez, *Cyber Forensics*, 141.

[10] Ibid.

A mobile device seized during the investigation in a power mode is able to receive calls and messages. However, when any call or SMS is received on the mobile device, the phone is updated automatically. By switching of the mobile phone, it may not be possible to be restarted again without the password, if the mobile is password protected. One solution is that the mobile phone may be put into Faraday bag[11] to stop the receiving of signals.

How mobile phone makes and receives telephone calls? Every mobile phone gets its identity through several numbers. The manufacturer of the mobile phone includes an "*Electronic Serial Number* (ESN) or the *International Mobile Equipment Identity* (IMEI) number as a code to uniquely identify mobile devices. The International Mobile Subscriber Identity (IMSI) number is a unique identification number, typically provisioned in the SIM card of the telephone to identify the subscriber of a cellular network."[12] IMSI number is withheld to prevent the subscriber's identification, instead in its place "the *Temporary Mobile Subscriber Identity* (TMSI), which is randomly generated and assigned to the telephone the moment it is switched on, to enable the communications between the mobile device and the base station."[13] Lastly, the "Mobile Identification Number or Mobile Subscription Identification Number is the unique telephone directory number for that mobile subscription that is used to identify a telephone. It is derived from the last part of the IMSI."[14]

Usually cell phones have two numbers "that uniquely identify them—an Electronic Serial Number (ESN) and a telephone number or Mobile Identification Number (MIN)."[15] At the time of

---

[11] A Faraday bag is "a special container constructed with conductive material that effectively blocks radio signals."

[12] Mason and Seng, *Electronic Evidence*, 13.

[13] Ibid.

[14] Ibid.

[15] Casey, *Digital Evidence and Computer Crime,* 618.

manufacturing a mobile phone, its microchip is programmed by the manufacturer with a unique ESN. Thereafter, the consumer/subscriber buy a SIM card from the cellular companies, this is the number where people use to call the subscriber. Then, by telephone the companies call is direct to these. Later on, these numbers help the investigators to locate the phone.

Owing to development of new technology and sophisticated operating system, mobile technology is also creating complexity for the investigators, as after every few days a new smart phone is introduced in the market. This makes the investigator's task more complex.

The LHC (Rawalpindi Bench) in *Hashim Jamal v. the State,*[16] refused the bail of the accused on the basis of forensic evidence collected from cell phone handset. In *Junaid Arshad v. the State,*[17] the court also refused bail on the basis of evidence collected from cell phone and IP address. In *Munas Parveen v. Additional Sessions Judge,*[18] the LHC held that the "Introduction of the modern devices including the SMS through computer is one of the means of communication which are validly accepted all over the world. However, the witness in whose presence the information is conveyed or received are always important to prove a fact through its verification." In *Muhammad Irfan v. The State,*[19] the LHC accepted the evidence on mobile phone memory card and upheld the conviction of the accused. In a latest judgment of the Sindh jurisdiction, in *Kashif Dars v. the State,*[20] the court refused the bail of accused on the basis of IP address and mobile

[16] *Hashim Jamal v. the State,* 2018 YLR Note 105.
[17] *Junaid Arshad v. the State,* 2018 PCrLJ 739 (Lahore).
[18] *Munas Parveen v. Additional Sessions Judge*, PLD 2015 Lahore 231
[19] *Muhammad Irfan v. The State*, 2018 PCRLJ 1319.
[20] *Kashif Dars v. the State,* 2020 PCrLJ 259 (Sindh).

phone. Whereas in *Yasir Ayyaz v. the State,*[21] the LHC upheld the conviction of the accused on the basis of video recorded in mobile phone and memory card.

6.2.1 CALL DETAIL RECORDS

In tracing the criminal, more particularly, the moment of any accused, it plays an important role. A call detail record (CDR) is a "data record produced by a telephone exchange or other telecommunications equipment that documents the details of a telephone call or other telecommunications transaction (e.g., text message) that passes through that facility or device."[22] During the call, the network records CDR for billing purposes. However, this is also used by the LEAs and investigators to check the movement of a handset, which enables them to trace the suspects accused. Generally, CDR can be obtained from cellular service provider, which contains call durations, date and time of the call, type of call (voice call or text message), call status (incoming or outgoing), disposition of the call (such as busy and call failed), location, cell site accessed, originating and terminating towers, source and destination number are record. Further, an analysis of "the geolocation information from accessed cell sites from the CDR is a contributing source of a suspect's history location points and travels."[23] Although, CDR tell a lot, but it cannot tell exactly "who actually made the call."[24]

Combing CDR evidence with other types of evidence (such as interviews, surveillance and analysis of electronic device), can help the investigator to narrow the list of suspects. As CDR "can place their cell phones at specific locations by date and time."[25] Before assuming the

---

[21] *Yasir Ayyaz v. the State,* PLD 2019 Lahore 366.
[22] https://en.wikipedia.org/wiki/Call_detail_record (accessed: 26th March, 2020).
[23] Shavers, *Placing the Suspect behind the Keyboard*, 100.
[24] Sammons, *Basics of Digital Forensics*, 151.
[25] Shavers, *Placing the Suspect behind the Keyboard*, 126.

geolocation in a certain device that belongs to a suspect, it must be linked/established by the investigator that the device belongs to the specified individual. Whereas, this can be done in diverse ways, "such as reviewing the call records and verifying calls made were the suspect's. These calls can be to the suspect's home, workplace, or to witnesses corroborating the calls."[26]

For LEAs, CDR provide a "wealth of information that can help to identify suspects, in that they can reveal details as to an individual's relationships with associates, communication and behavior patterns, and even location data that can establish the whereabouts of an individual during the entirety of the call."[27]

Whether the CDR is protected under the privacy law or not? The U.S. Supreme Court held that CDR are not protected under the Fourth Amendment of the US Constitution because the caller "voluntarily conveyed numerical information to the telephone company."[28] However, this issue was not discussed in any case in Pakistan. In 2013, a top-secret order of US Court was leaked to the public, which defined the CDR as follows:

> IT IS HEREBY ORDERED that, the Custodian of Records shall produce to the National Security Agency (NSA) upon service of this Order, and continue production on an ongoing daily basis thereafter for the duration of this Order, unless ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata" created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls.... "Telephony metadata includes comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call. Telephony metadata does

[26] Shavers, *Placing the Suspect behind the Keyboard*, 153.
[27] https://en.wikipedia.org/wiki/Call_detail_record (accessed: 26th March, 2020).
[28] *Smith v. Maryland,* 442 U.S. 735 (1979).

not include the substantive content of any communication, as defined by 18 U.S.C. § 2510(8), or the name, address, or financial information of a subscriber or customer.[29]

In *Abdul Ghaffar v. State,*[30] the LHC held that the telephone call-history is a valuable piece of evidence in order to trace out the culprits and to connect them with the charge.

6.2.2 MOBILE LOCATION

Determining the mobile location is very important in any investigation. The ability of investigator "to determine the location of mobile devices during a period of interest is a powerful investigative capability. Some mobile devices record the location of cellular towers they contacted, potentially providing a historical record of the user's whereabouts over a given period."[31] Network service providers records the information of any communication made using mobile phone, therefore, they can provide the record of any cell phone. Thus, it can safely be said that these records "can provide useful historical details that are no longer recoverable from the mobile device itself."[32]

It is not possible to obtain this information without using special electronic tracking equipment those "enables investigators to lock onto an ESN/MIN pair and track it to a general geographical area. Within a given geographical area, triangulation can be used to pinpoint the cellular telephone."[33] Investigators will ask the cellular network providers for assistance in performance of tracking. Thereafter, the compilation of geolocations "obtained from connections to wireless networks, geotagged photos, and cellular tower connections can give a thorough picture

---

[29] In re "*Application of the Federal Bureau of Investigation for an Order Requiring the production of tangible things from Verizon Business Network Services, Inc. on behalf of MCI Communication Services, Inc. d/b/a Verizon Business Services*"

[30] *Abdul Ghaffar v. State,* PLJ 2009 Cr.C (Lahore), 271.

[31] Casey, *Digital Evidence and Computer Crime,* Chapter 20, 10.

[32] Casey, *Digital Evidence and Computer Crime,* Chapter 20, 13-14.

[33] Casey, *Digital Evidence and Computer Crime,* 618.

of locations the device traveled."[34] In addition to this information, locations saved by the device are a great source in tracing a location. All these device can be very helpful "in showing a suspect's location at or near a crime scene or incident or corroborating an alibi away from the scene."[35] However, it must be kept in mind that this is not an authentic such as "a SIM card used in a mobile telephone, and purportedly its user, were at a particular location or moved from location to location."[36] Stating differently, mobile phone location "is not exact and does not place an individual at a specific place."[37] As it is very difficult to prove "who was using the mobile telephone at a specific time, particularly when telephones or SIM cards are shared among members of a group or family."[38]

6.2.3 COLLECTION AND HANDLING OF MOBILE PHONE EVIDENCE

Fundamental principles of digital evidence handling also apply to mobile phones as well. Since mobile phone data is not like other forms of digital evidence, therefore, some extra care is also required in cell phone handling. The first thing the investigator do is to isolate the target mobile from the network which is imperative in mobile phone evidence collection. Otherwise, connection with network may overwrite any potential evidence. As discussed, for isolation Faraday bag is used.

Unlike other digital devices, it is important for investigators "to collect all synchronization and power cables."[39] If power cables are not collected then if cell phone is allowed to run, its battery will not last. Hence, a recharge or battery will be required to switch on the phone. Besides,

---

[34] Shavers, *Placing the Suspect behind the Keyboard*, 100.
[35] Ibid., 101.
[36] Mason and Seng, *Electronic Evidence*, 97.
[37] Casey, *Handbook of Digital Forensics and Investigation*, 29.
[38] Ibid.
[39] Brown, *Computer Evidence: Collection and Preservation*, 331.

investigator should be capable to retrieve information from different models of mobile phones. As diversity of products "pose challenges because there is no uniform process to obtain information across makes and models."[40]

Collecting digital data from any mobile device such as "cellular phone or tablet requires a wider variety of tools and skillsets than those needed with computer hard drives. Mostly, this is due to the difficulty in being able to access and extract the memory physically or logically from the devices while reducing the amount of file modification."[41] Therefore, methods and software are also vary due to number of different devices. In addition to this, the investigator should be able to extract data from social networking websites and GPS devices as many people share their location using consumer services.

When extracting data from mobile devices, the investigator should remove SIM cards from the mobile devices. Besides, he should also switch the devices to "flight mode to prevent them from communicating with external communication points. This prevents new data being downloaded to the device or existing data being modified or deleted."[42]

The investigator and forensic examiner should be aware that "data associated with mobile phones is found in a number of locations; embedded memory, attached removable memory, and the Subscriber Identity Module (SIM) card."[43] Now almost every smart phone has the "Internet capability rivalling that on many computers. A more advanced smart phone will additionally store an Internet history, Internet cache, Internet bookmarks, MMS, e-mail, photographs, videos, and

[40] https://www.rand.org/pubs/research_reports/RR890.html (accessed: 25th October, 2019).
[41] Shavers, *Placing the Suspect behind the Keyboard*, 98.
[42] Boddington, *Practical Digital Forensics*, 135.
[43] Casey, *Digital Evidence and Computer Crime,* Chapter 20, 6.

installed third-party applications and may be used for transferring computer files."[44] All these things are a gold mine of information for investigators. Nonetheless, the investigator may not find all these things at crime scene or in the possession of the accused, but in some cases "there may be multiple SIM cards, removable media, or even more than one mobile device."[45] Moreover, the investigator should also collect SD cards as they contain many GB of data.

Whether a mobile phone constitutes a computer device or not? In *United States v. Neil Scott Kramer*,[46] the court held that a mobile phone may be considered a computer if "the phone perform[s] arithmetic, logical, and storage functions."

6.2.4 INTERNATIONAL MOBILE EQUIPMENT IDENTITY (IMEI)

Global System for Mobile Communications (GSM) devices are assigned "a unique number called the International Mobile Equipment Identity (IMEI), which includes a serial number for the device."[47] Whereas on Code-Division Multiple Access (CDMA) phones, the ESN is "an 11-digit number with the first three digits designating the manufacturer and the remainder unique to the device."[48]

The IMEI[49] is very important in digital evidence, which allows the investigators to collect important evidence "associated with a particular mobile device even if a subject uses different network service providers (NSPs) or accounts with the same device."[50] Besides, collecting data

---

[44] Casey, *Digital Evidence and Computer Crime,* Chapter 20, 10.
[45] Casey, *Digital Evidence and Computer Crime,* Chapter 20, 6.
[46] *United States v. Neil Scott Kramer,* 631 F. 3d 900 (8th Cir. 2011).
[47] Casey, *Digital Evidence and Computer Crime,* Chapter 20, 4-5.
[48] Casey, *Digital Evidence and Computer Crime,* Chapter 20, 5.
[49] IMEI in Pakistan is defined in "Mobile Device Identification, Registration and Blocking Regulations, 2017 which means "an International Mobile Equipment Identity issued by GSMA and it comprises unique 15 (fifteen) digits decimal numbers required to identify a mobile device(s) on mobile networks."
[50] Casey, *Handbook of Digital Forensics and Investigation,* 521.

from NSPs, investigators may use "the IMEI to monitor telephone traffic associated with a particular device, obtaining voice communication, attempted calls, SMS, MMS, and video calls."[51] The IMEI is normally used by the investigator to identify the handset in use with a particular IMSI and if the mobile phone is stolen, to report to the service provider to block the same.

In *Saifal v. the State,*[52] the court upheld the accused's conviction on the basis of IMEI number of the mobile phone which was provided by the complaint to the Investigation Officer (IO). After obtaining the record of mobile, in which three different SIMs were used, from the cellular company, the IO traced and apprehended the accused. The trial court convicted the accused and the punishment was upheld by the appellate court. Whereas, in *Naveed Asghar v. the State,*[53] the Lahore High Court, considered the International Manufacturer Equipment Identification Number (IMEI) as circumstantial evidence and while upholding trial court's decision, the court also maintained conviction of the accused.

6.3 SUBSCRIBER IDENTITY MODULES CARD

Subscriber Identity Modules (SIM)[54] card provides "a way of associating a handset with a subscriber to allow access to the mobile phone network."[55] Any network requires logical and physical (IMSI)[56] address. The logical address is "the telephone number associated with the SIM

---

[51] Casey, *Handbook of Digital Forensics and Investigation,* 521.

[52] *Saifal v. the State,* 2013 PCrLJ 1082 (Sindh).

[53] *Naveed Asghar v. the State,* PLD 2016 Lahore 467.

[54] SIM in Pakistan is defined in "Subscribers Antecedents Verification Regulations, 2015" which means "Subscriber Identity Module to be provided by a cellular mobile Operators as a connection for cellular mobile services."

[55] Marshall, *Digital Forensics Digital Evidence in Criminal Investigation*, 114.

[56] Generally, IMSI is comprised of a country code, a mobile network code, and subscriber identification number. IMSI in Pakistan is defined in "Mobile Device Identification, Registration and Blocking Regulations, 2017 which means "the International Mobile Subscriber Identity that is used to identify the subscriber(s) of a particular mobile network operator and is unique with all the cellular networks. IMSI consists of mobile county code, mobile network code."

through a database which maps the telephone number to the IMSI."[57] Further, the SIM can also contain "a Temporary Mobile Subscriber Identity (TMSI) and Location Area Identity (LAI). The TMSI is often used over the radio link to avoid revealing the IMSI number to others who may be eavesdropping with radio-related interception equipment."[58] However, TMSI and LAI always changes when a device is moved to a new place.

SIM cards are "comprised of a microprocessor, ROM, and RAM, and are assigned a unique Integrated Circuit Card Identifier (ICC-ID). The ICC-ID contains the mobile country code (MCC), mobile network code (MNC), and a serial number of the card. These smart cards are used to authenticate users on GSM and UMTS networks."[59] Moreover, the body of the phone has "an area of addressable data storage and this can include, contact details, SMS messages and will also contain details of recent phone calls made, received and missed."[60] It must not be ignored by the investigators that nowadays various mobile devices have slots for external storage cards as well. The investigator must be aware that criminals also use multiple SIM cards for short periods. Nevertheless, a "limited amount of storage capacity available on a mobile phone's SIM card."[61]

Last detailed regulations[62] for issuance of SIMs were issued by the Pakistan Telecommunication Authority in 2015. Until promulgation of PECA, there was no specific law for issuance of SIM card. Hence, section 17 of the PECA[63] specifically provided punishment for

---

[57] Marshall, *Digital Forensics Digital Evidence in Criminal Investigation*, 114.

[58] Casey, *Digital Evidence and Computer Crime,* Chapter 20, 6.

[59] Casey. *Digital Evidence and Computer Crime,* Chapter 20, 5.

[60] Sommer, *Digital Evidence, Digital Investigations and E-Disclosure*, 93.

[61] Marcella and Menendez, *Cyber Forensics*, 139.

[62] Subscribers Antecedents Verification Regulations, 2015. Before these regulations, in 2010, these regulations were issued which were amended in 2012 twice.

[63] Section 17 of the PECA is read as: **17. Unauthorized issuance of SIM cards etc.**—Whoever sells or otherwise provides subscriber identity module (SIM) card, reusable identification module (RIUM) or universal integrated circuit card (UICC) or other module designed for authenticating users to establish connection with the network and to be used in cellular mobile, wireless phone or other digital devices such as tablets, without obtaining

three years and fine which may extend to five hundred thousand rupees. In *Saifal v. the State,*[64] the court accepted the record of mobile SIMs collected from the cellular company and upheld the conviction of the accused.

6.4SIM SECURITY

SIM is also protected from unauthorized access as other device. However, security codes also restrict investigators access to SIM, creating additional barriers to acquire data from SIM cards. Hence, it is important for investigators to "understand how such security protection can be overcome. Users can set a personal identification number (PIN) to restrict access to their SIM card."[65]

Generally, people use PIN to protect their SIM data, which is normally four to eight digits. If an incorrect PIN is entered to unlock the SIM, after three unsuccessful attempts Personal Unlock Key (PUK) will be required to access the SIM. However, PUK attempts are also limited (depending upon the country policy), after few attempts, SIM cards will be blocked permanently. Therefore, investigators should take care in attempting to access SIM cards. Legal authorization and Network Service Provides (NSP) contact can help the investigators "to obtain a PUK in a matter of minutes. However, not all NSPs retain the PUK for the SIM cards they sell, and in some situations, it may not be feasible to involve the NSP."[66]

6.5GLOBAL POSITIONING SYSTEMS (GPS)

---

and verification of the subscriber's antecedents in the mode and manner for the time being approved by the Authority shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to five hundred thousand rupees or with both.

[64] *Saifal v. the State,* 2013 PCrLJ 1082 (Sindh).

[65] Casey, *Digital Evidence and Computer Crime,* Chapter 20, 40.

[66] Ibid.

Nowadays, almost every device is having GPS feature, which help the investigator to trace the criminal or record his movement. GPS is "a constellation of satellites operated by the U.S. Air Force. A device communicating with the GPS satellites can calculate its own velocity and location in three dimensions."[67] There are "twenty-seven GPS satellites in the GPS system."[68] Whereas a GPS relies "on a constellation of 24 satellites only."[69] The remaining three satellites "are held in reserve in case one of the primary satellites goes down. A GPS receiver calculates its position through a mathematical process known as trilateration."[70] Because of advancement of technology, almost nowadays all mobile phones are GPS-enabled. Initially, GPS technology in mobile phones was not accurate. Earlier, GPS location was not precise, now the newer devices made it possible as held in the *United States v. Jones*[71] in which the court noted that "newer smart phones equipped with GPS device permit more precise tracking than older devices." But due to improvement in technology it is almost accurate. However, a user can disable her mobile phone's GPS.

Each satellite in orbit has "a unique identity and a well-defined orbital path combined with an accurate clock. Each satellite broadcasts information about the current time and its orbit."[72] Whereas, by identifying the satellites "visible from any point on the planet and performing a calculation based on the data sent by the satellites, a GPS receiver can calculate exactly where it is above the surface of the planet."[73] GPS devices can be separated into four different categories such as simple, smart, hybrid and connected.

---

[67] Jeremy H. Rothstein, "Track Me Maybe: The Fourth Amendment and the Use of Cell Phone Tracking to Facilitate Arrest" *Fordham Law Review* 81 (2012): 489-535 at 493.

[68] Sammons, *Basics of Digital Forensics*, 157.

[69] Vacca, *Computer Forensics: Computer Crime Scene Investigation*, 557.

[70] Sammons, *Basics of Digital Forensics*, 157.

[71] *United States v. Jones*,5 65 U.S 132 S.Ct. 945 L.Ed. .2d 911 (2012).

[72] Marshall, *Digital Forensics Digital Evidence in Criminal Investigation*, 116.

[73] Ibid.

The accuracy of GPS position calculations depends on two things one is measurement accuracy and second is satellite configuration. Whereas measurement errors "depend on physical parameters, such as ionospheric delays and orbital uncertainties and on the selective availability factor."[74] And the configuration of the GPS satellites "at the time of the measurements adds further distortion. If those in sight are scattered throughout the sky, the measurement error is multiplied by about 1.5. If they are clustered together, the multiplier is 5 or more."[75] Measurement errors are combined with the errors introduced by the spatial disposition of the satellites to estimate actual position accuracy. For determination of its position, a GPS receiver "calculates its x, y, and z coordinates as well as the time the satellite signals arrive."[76] In any situation, at least data must be acquired from four observable GPS satellites. For determination of locator's position "the use of two GPS satellites and two cellular base stations would suffice."[77]

GPS is an incredible source of evidence, which is used to determine the location of criminals and accused alike. Besides, GPS can also be used to record the movement of intended suspects. Furthermore, some GPS units "can provide a great deal more evidence, including mobile phone logs, SMS messages, and images. Given these capabilities, along with large storage capacities, examining these devices is well worth the time."[78] GPS devices are installed in vehicles and mobile phones alike. GPS device are almost similar to the mobile phones; therefore, the investigator should handle such devices in the same way as cell phones.

---

[74] Vacca, *Computer Forensics: Computer Crime Scene Investigation*, 558.
[75] Ibid.
[76] Ibid.
[77] Ibid.
[78] Sammons, *Basics of Digital Forensics*, 157.

GPS devices instead of blessing are becoming more problematic "to retrieve data from, particularly those inbuilt in vehicle dashboards. More often than not, the device provides no more data than the home location and locations keyed in as potential destinations."[79] Whereas examination of GPS equipment is "more problematic than examination of phones. Some systems use versions of the operating systems designed for PDAs, while others are based on entirely proprietary navigation software."[80]

In *United States v. Brooks*,[81] the US 8th Circuit Court upheld the conviction of the accused on the basis of GPS evidence and CCTV. It was upheld by the US court that "current GPS technology would almost certainly enable law enforcement to locate the subject telephone with a significantly greater degree of accuracy."[82]

6.6 Cell Phone Towers

A mobile phone without communicating a cell phone tower cannot make and receive call. While communicating with cell phone towers, "the provider of the cell phone service generates a log of the connections. The phone service provider maintains those logs of communication with the cell towers for a length of time."[83] However, the data retention policy varies country to country.

Mobile devices use "radio waves to communicate over networks with various frequencies and standard communication protocols."[84] GSM and CDMA are the two most common mobile communication protocols. While moving from one place to another, the connection to the network

---

[79] Boddington, *Practical Digital Forensics*, 283.

[80] Marshall, *Digital Forensics Digital Evidence in Criminal Investigation*, 117.

[81] *United States v. Brooks*, 715 F.3d 1069 (8th Cir.2013).

[82] In re *Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 538 (D. Md. 2011).*

[83] Shavers, *Placing the Suspect behind the Keyboard*, 73.

[84] Casey, *Digital Evidence and Computer Crime,* Chapter 20, 4.

is transferred from one cell tower to another cell tower, which is known as a handoff. However, handoffs are handled differently. For example, GSM and CDMA for networks both handle them differently. It is important to know that a GSM network phone at a time can only attach to one tower only. In contrast, CDMA "phone can connect to multiple towers at once, using the tower with the strongest signal."[85]

Obtaining and analyzing cell tower records "allow the investigator to track the movements of the phone through a given time period."[86] Whether cell tower information is always accurate? It depends upon various factors such as "the type of tower, number of towers in the area, terrain, buildings, weather, and even the time of day will affect the accuracy of location."[87] However, this information is not always accurate. In an investigation, merely relying on cell tower does not confirm the suspected person possessed the phone, instead it only confirms the location of the mobile phone. Stating differently, even otherwise when "a person's mobile device can be tracked to a location, it does not necessarily prove that the person was there. Additional corroborating evidence is generally needed to establish a compelling link between digital evidence and a person."[88]

Generally, each cell tower "will have three panels per side. The middle panel is usually the transmitter, with the other two being receivers. The receiver panels constantly listen for incoming radio signals."[89] It is important to mention here every mobile phone is "regularly communicating with the nearest cellular antennae."[90] When mobile phone is turned on, "it automatically begins

---

[85] Sammons, *Basics of Digital Forensics*, 148.
[86] Shavers, *Placing the Suspect behind the Keyboard*, 74.
[87] Ibid.
[88] Casey, *Digital Evidence and Computer Crime,* 324.
[89] Sammons, *Basics of Digital Forensics*, 147.
[90] Ibid.

searching for the nearest cell site. Once the antenna is found, the phone then transmits identification data so the network can verify who you are and whether you have authorized access."[91] Usually, this information consists of phone number and service provider's name.

6.7 CELLULAR NETWORKS

Cellular network is made of individual cells. A cellular network is a "communications network that enables portable devices such as cellular telephones to communicate with each other."[92] This network is established within a specified area consisting of cell sites (base stations). Any subscriber can make and receives calls while connecting over the cell site. Whereas each cell site "is connected to a central computing infrastructure, comprising telephone exchanges or switches, which are in turn connected to the public telephone network."[93] This structure routes the calls, retains logs and is used for investigation purposes, as evidence can be located on the network.[94]

Developments in cellular technology has provided "for faster transmission rates and enable applications such as mobile web access, IP telephony, gaming services, high-definition mobile TV, and video conferencing."[95] Now cellular networks are being used to connect computers for the internet. Cellular companies track the mobile phone constantly to direct the call to correct number. Thus, it can safely be concluded that "there is a broad range of electronic evidence associated with the use of a mobile telephone, including where the telephone was located

---

[91] Ibid., 147-48.
[92] Mason and Seng, *Electronic Evidence*, 12.
[93] Ibid.
[94] Sammons, *Basics of Digital Forensics*, 146; Casey, *Digital Evidence and Computer Crime*, 617.
[95] Mason and Seng, *Electronic Evidence*, 12.

geographically, details of calls made and received, and the recovery of the contents of text messages."[96]

Cellular networks are using "Frequency Division Multiple Access (FDMA), Code Division Multiple Access (CDMA), Time Division Multiple Access (TDMA), or a combination of these technologies to transmit data via radio waves."[97] Thus, these technologies facilitate various mobile telephones "to share a single communications channel on a mobile telephone network by dividing the channel into several time slots, and assigning each telephone its own slot."[98] For communication on the Internet, cellular service providers has started using a protocol Cellular Digital Packet Data (CDPD). But, CDPD has been "largely replaced with the higher speed General Packet Radio Service (GPRS)—part of GSM technology that uses a combination of TDMA and FDMA and has Internet Protocol capabilities."[99] Cellular technology is evolving so fast which is providing higher data transmission services.

6.8 Cellular Network Components

Cellular network components are very important which keep the record of movement of cell phone. These components can "potentially provide information relevant to an investigation."[100] These includes Base Station Controller (BSC), Mobile Switching Center (MSC), Visitor Location Register (VLR), Home Location Register (HLR), and Short Message Service Center (SMSC). Thus, the investigator should be aware of these components.

---

[96] Ibid., 13.
[97] Casey, *Digital Evidence and Computer Crime,* 617.
[98] Casey, *Digital Evidence and Computer Crime,* 617-18.
[99] Ibid.
[100] Sammons, *Basics of Digital Forensics*, 147.

In any cellular network, base station is basic entity which "consists of the antennas and related equipment."[101] Whereas a Base Station Controller (BSC) "regulates the signals between base stations. This function is critical as phones move from place to place."[102]

The MSC processes calls within the network and "holds a tremendous amount of possible evidence. It also coordinates calls between different wireless networks as well as landlines. The MSC handles SMS messages as well. The call detail records and logs are found here."[103] Whereas, the VLR is a database which "is linked to an MSC. All mobile devices currently being controlled by that MSC are recorded in the VLR. Interworking functions serve as doorways outside data networks such as the Internet."[104]

Consequently, the individual subscribers' information is recorded in the HLR.[105] Further, the HLR also stores encryption keys and "supports the Authentication Center (AuC), which is used to control access to the network. The AuC screens connections, blocking unauthorized users."[106] The SMSC is responsible for text messages and later on investigators can recover messages from the SMSC.

6.9 Cloud Systems

There are various definitions of cloud computing. The cloud system generally is defined as "a general term for anything that involves delivering hosted services over the Internet."[107] Whereas, the NIST defines as "Cloud computing is a model for enabling ubiquitous, convenient,

---

[101] Ibid.
[102] Ibid.
[103] Ibid.
[104] Ibid.
[105] Ibid.
[106] Ibid.
[107] Sammons, *Basics of Digital Forensics*, 165.

on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[108]

There are different storage options in this system. However, the potential storage options "for electronic evidence are expanding every day, from data stored on cell phones and pad computers to storage in the cloud where a third-party service provides hard drive space on the Internet for people and businesses to store data."[109] Due to cost reductions, many organizations and departments "are outsourcing their information technology to cloud service providers, resulting in the storage of digital information in cloud environments. Similarly, individuals are using cloud services for e-mail, social media, and storage of a broad array of digital data from documents to photographs."[110]

Individuals, government entities and organizations have started "moving away from traditional devices towards a completely interconnected world where digital traces left by each person are on the rise, locally recorded on different devices or remotely in the cloud even beyond national borders."[111] However, there are two types of clouds system i.e. private clouds and public clouds. Public clouds sell services on the open market such as Microsoft, Amazon, and Google.

---

[108] https://www.nist.gov/programs-projects/nist-cloud-computing-program-nccp (accessed: 24th April, 2020); https://csrc.nist.gov/publications/detail/sp/800-145/final (accessed: 24th April, 2020); https://www.nist.gov/news-events/news/2011/10/final-version-nist-cloud-computing-definition-published (accessed: 24th April, 2020).

[109] Daniel et al. *Digital Forensics for Legal Professionals*, 4.

[110] Lucy L. Thomson, Esq. "Admissibility of Electronic Documentation as Evidence in U.S Courts," Centre for Research Libraries Human Rights Electronic Evidence Study, 4.

[111] Biasiotti et al, *Handling and Exchanging Electronic Evidence across Europe*, 7.

There are three generally accepted cloud service delivery models, these are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).[112] On payment of service charges for these services, these are delivered over the Internet to the purchaser of these services.

6.8.1 INFRASTRUCTURE AS A SERVICE (IaaS)

This model provides "the closest comparison to a physical network that can be purchased in the Cloud service world."[113] With IaaS, individuals, organizations, and entities after paying the running and maintenance cost "outsource their hardware needs to a service provider."[114] This includes servers, storage media.

In an IaaS, the service provider "gives the user access to a console that enables the user to create a logical-based computing environment with servers, storage, databases, and other functions."[115] Furthermore, the virtual server users "are sharing the physical hardware with multiple other organizations. This is what is referred to as a public Cloud. The same can be accomplished in a private Cloud, where the physical Cloud at one server center is dedicated to only one customer."[116] In a shared environment, risks cannot be ruled out.

The data owner does not have full control on IaaS, as there are limitations on the degree of control which the user can exercise such as "ability to collect and preserve data in support of

---

[112] Sammons, *Basics of Digital Forensics*, 21-22 & 165; https://www.nist.gov/programs-projects/nist-cloud-computing-program-nccp (accessed: 22nd November, 2016); Ann D. Zeigler and Ernesto F. Rojas. *Preserving Electronic Evidence for Trial A team Approach to the Litigation Hold, Data Collection, and Evidence Preservation* (Amsterdam: Elsevier, 2016), 109; John Viega, "Cloud computing and the common man" IEEE Computer 42 (2009), 106-8.

[113] Zeigler and Rojas, *Preserving Electronic Evidence for Trial*, 110.

[114] Sammons, *Basics of Digital Forensics*, 22.

[115] Zeigler and Rojas, *Preserving Electronic Evidence for Trial*, 110.

[116] Ibid., 111.

litigation and investigations."[117] Further, the user is dependent on the service provider "to collect data, and more importantly to properly document that collection."[118] Lacking of education, knowledge and training by the evidence collector may cause many issue for admissibility in the court proceedings.

6.8.2 PLATFORM AS A SERVICE (PaaS)

This model provides "the Cloud provider delivers space on a logical server to run an application designed by the user."[119] In PaaS, different program developers develop "software to function in specific computing environments. PaaS gives developers the ability to rent the environment on an as-needed basis."[120] PaaS provides "excellent flexibility in that the operating system can be modified or upgraded frequently."[121]

In PaaS, for example, if an organization "wants to develop a mobile application would outsource all the operating and administrative requirements of the computing environment to the Cloud, and only control the programming and user interface portions of the task."[122] However, collecting evidence from PaaS Cloud-based resources is similar to those of IaaS. But, this problem can be avoided "if the developer has programmed an interface to collect each application user's data individually."[123] Nevertheless, remaining data which is not in the control of cloud use, would have to be collected from the Cloud provider.

---

[117] Zeigler and Rojas, *Preserving Electronic Evidence for Trial*, 111.
[118] Ibid.
[119] Ibid.
[120] Sammons, *Basics of Digital Forensics*, 22.
[121] Ibid.
[122] Zeigler and Rojas, *Preserving Electronic Evidence for Trial*, 111.
[123] Ibid., 111-12.

6.8.3 SOFTWARE AS A SERVICE (SaaS)

This model provides "applications on demand to customers over the Internet. These applications are hosted and maintained by the service provider."[124] In other words, "SaaS is the sale of an application on a subscription basis—applications that previously had to be purchased and installed on a local physical server or workstation."[125]

In SaaS, the responsibility of maintenance is shifted to the third party. This is best option for limited resource organizations. In this situation, the provider has "total control, and can change the software at any time to add or delete features, fixes, or operation of the product, generally without notice to or approval by the end user."[126] However, data collection is very difficult in this category.

6.10 CHALLENGES OF CLOUD COMPUTING

Traditional digital forensic practices adopted by forensic community are "based on the collection of data from physical devices, such as memory, hard drives, servers, etc., at specific physical locations."[127] In cloud environment, where these services are provided to many clients, the investigator "cannot image data in a traditional forensic method as used in a physical environment that only contains one client's data."[128] Using traditional methods for evidence collection from cloud environment, may cause the collection of data of the other clients. There are lack of recognized "forensic tools and procedures for acquiring and analyzing digital evidence in

---

[124] Sammons, *Basics of Digital Forensics*, 22.
[125] Zeigler and Rojas, *Preserving Electronic Evidence for Trial*, 112.
[126] Ibid.
[127] Ibid.
[128] Ibid.

the cloud."[129] Current tools and methodologies used by forensic examiners are not effective in cloud environment.

In some cases, however, the cloud storage is "spread over a number of storage application server locations, serving thousands of Cloud users, with the data simply identified in a way that presents the viewer with a logical storage unit associated with the user."[130] Whereas, this data may be stored on servers in various continent. Stating differently, cloud creates legal and technical challenges for LEAs. Technically, the cloud "presents a very complicated, virtualized environment that frustrates."[131] The Cloud leads to "legal issues that have not been considered previously, such as jurisdictional issues, potential confidentiality issues, data ownership and loss of data if a Cloud Provider becomes insolvent."[132] The data in cloud can be stored in many countries and continents.

Because of various challenges posed by the public cloud system, now the large cloud users are shifting to private clouds. In private clouds, "the Cloud hardware environment of a specific server group is dedicated to one Cloud user. This limits the potential commingling of data from another organization with the client's data."[133] However, the private cloud is very expensive.

In *Microsoft v. United States,*[134] the court held that:

> Accordingly, the SCA does not authorize a U.S court to issue and enforce an SCA warrant against a United States-based service provider for the contents of a customer's electronic communications stored on servers located outside the United States. The SCA warrant in this case may not lawfully be used to compel Microsoft to produce to the government the contents of a customer's e-mail account stored exclusively in Ireland.

---

[129] Sammons, *Basics of Digital Forensics*, 166.

[130] Zeigler and Rojas, *Preserving Electronic Evidence for Trial*, 113.

[131] Sammons, *Basics of Digital Forensics*, 22.

[132] Stanfield, Authentication of Electronic Evidence," 6.

[133] Zeigler and Rojas, *Preserving Electronic Evidence for Trial*, 113.

[134] *Microsoft v. United States,* No. 14-2985 (2d Cir. 2016). US Department of Justice filed an appeal before to the US Supreme Court. While pendency of the case, Congress passed CLOUD Act, 2018, by related to warrant. Hence, the Supreme Court remanded case back to the 2nd Circuit Court of Appeal. *United States v. Microsoft Corp.*, 584 U.S. ___, 138 S. Ct. 1186 (2018).

However, this case created many problems for USA government, thus, congress passed the CLOUD Act, 2018 for amendment of section 2701.

6.11 SUMMARY

Advancement in technologies have providing new and sophisticated ways to record human activities. Thus, volumes of digital data and information is available on smart phones enabling LEAs to collect the data for investigation purposes. The data collected from cell phones and mobile devices are particularly sensitive to change and more often it is not possible to establish that the device is used by a specific person as these devices only provides that a certain device was available at certain point.

This complexity is increased when the data is not in physical control of the user and the same is on cloud system. Besides technical issues, there are various legal issues attached to the cloud system such as jurisdiction, confidentiality and data ownership and loss of data issues. Therefore, specific legislation is required to handle these issues.

CHAPTER SEVEN:

DIGITAL EVIDENCE ON THE INTERNET

7.1 INTRODUCTION

All the computer are either connected through networks (for internal use in an office) or either connected through the internet. In case of network, the relevant network on the crime scene is squared as the main evidence is available on all connected networks and servers. While in the case of the internet, this email is available on different locations and on different servers, which is critical for digital investigation. In this situation, the investigator has multiple option to square the evidence.

The internet is itself is nothing without the website. Internet Protocol address helps the investigator to reach the exact location in many of the cases. Therefore, IP address has been discussed in a detail in this chapter. IP address is obtained from Internet Service Provider; therefore, this aspect is also examined in the light of prevailing Pakistani laws. Almost, all the important topics related to digital evidence on the internet have been examined in this chapter.

7.2 DIGITAL EVIDENCE ON NETWORKS

Few years ago, it was sufficient to collect sole computers as a digital evidence. Collection of computers, cables and attached accessories were considered collection of digital evidence. Now, however, it has expended just one computer to a network where people are relying "on e-mail, e-commerce, and other network resources. It is no longer adequate to think about computers in

isolation as many of them are connected together using various network technologies."[1] Besides, these networks are extended in different global locations.

A computer "that is attached to one or more other computers, is known as a computer network and can include other devices such as printers, external hard drives, modems and routers. These are linked together and use software commands to exchange data."[2] A Local Area Network (LAN) is an example of a network within a building. Whereas a Wide Area Network (WAN) extends from geographical location to another geographical location, networking computers between different places such as offices located at Islamabad and New York. In many cases, it is possible that the only available evidence is network, as the criminal may have destroyed the hardware leaving no tangible thing to examiner in cyber-space. Therefore, understanding the working of network and the internet is important for investigation purposes.

7.3 Evidence Preservation on Networks

In existing corporate culture as well as in government organization, networking is used to communicate and exchange the electronic data, which besides extending many benefits also cause various challenges for organizations as well as for investigators alike. However, there are few unique forensic challenges "associated with preserving digital evidence on networks. Although some network-related data are stored on hard drives, more information is stored in volatile memory of network devices for a short time or in network cables for an instant."[3]

During the collection of static information, it may not be feasible for the investigator to shut down the system. As the victim system may be "part of an organization's critical infrastructure

---

[1] Casey, *Digital Evidence and Computer Crime,* 607.
[2] Stanfield, "The Authentication of Electronic Evidence," 70-71.
[3] Casey, *Handbook of Digital Forensics and Investigation*, 457.

and removing it from the network may cause more disruption or loss than the crime."[4] There is a possibility that the storage capacity of the system may be too large. Thus, "how can evidence on a network be collected and documented in a way that demonstrates its authenticity, preserves its integrity, and maintains chain of custody?"[5] Networked systems "can also contain crucial evidence in volatile memory, evidence that can be lost if the network cable is disconnected or the computer is turned off."[6] These network connections also assist the investigator to trace the IP address of criminal.

7.4 An Overview of the Internet

Any webpage can be accessed after entering "the web address or Uniform Resource Locator (URL) into the address bar of a browser."[7] Whereas a URL consists of host, domain name, and the file name.[8] The internet browser, Hypertext Transfer Protocol (HTTP) and Top Level Domain (TLD) are an integral part of the internet.

While accessing a website, during the browsing process, internet browser is used, which is an "application that is used to view and access content on the Internet,"[9] such as Google Chrome, Internet Explorer and Mozilla. Browser uses HTTP, which "sends a get request to the web server hosting" the website.[10] Furthermore, HTTP is "used on the Internet to browse and interact with websites."[11] Domain name is the name assigned for any website such as google. There is a TLD

[4] Ibid.
[5] Casey, *Handbook of Digital Forensics and Investigation*, 457.
[6] Ibid., 458.
[7] Sammons, *Basics of Digital Forensics*, 119.
[8] Ibid.
[9] Ibid., 120.
[10] Ibid.
[11] Ibid., 119.

such as .com., .org., .net., and .edu. It's called a TLD because "it is at the top of the hierarchy that makes up the Internet's domain name system."[12]

After pressing the Enter command, the domain name is converted to an Internet Protocol address. Whereas a "Domain Name Server (DNS) is responsible for mapping domain names to specific IP addresses. After the DNS makes the conversion, the request is then sent on to the server that's hosting the website. After receiving the request, the server returns the requested web page and associated content."[13]

7.4.1 INTERNET PROTOCOL (IP) ADDRESS

Like every home, each computer "attached to the Internet has a unique address, called an IP address. Each IP address is comprised of two parts, the network number and the host number."[14] This is similar to telephone number which has a country code, an area code and a local number. Whereas network number, in a digital environment, is a unique number which "identifies a computer network attached to the Internet and the host number is a unique number that identifies a computer on that network."[15]

The Internet Assigned Numbers Authority, and its Regional Internet Registries assigns IP addresses under a scheme. This fact must not be ignored that the IP address is not a person and it is just a numerical number of the device which uses the IP. However, this may be traced to a physical location, but in many cases, it may not be possible to link this with accurate location. After all, an IP address is just a clue about the presence of a device at a physical location. Whatever

---

[12] Ibid., 119.
[13] Sammons, *Basics of Digital Forensics*, 120.
[14] Casey, *Digital Evidence and Computer Crime,* 740.
[15] Ibid.

the situation, this cannot establish that the person is the same who was using the IP address, as in case of wireless network, it will be very difficult to link with the actual user, as many people outside the building may access the network by bypassing the security measures. This is circumstantial evidence; therefore, the investigator should collect other circumstantial evidence to link with the accused.

There are three classes of IP address such as class A, B and C, whereas class A can accommodate up to 16,777,214 hosts, and a class C network can just accommodate 254 hosts. Moreover, the class A and B networks "are usually divided into subnets to make them more manageable. The most common subnet size is 254 hosts, but subnet masks permit few hosts per subnet."[16]

In *Farhan Kamrani v. the State*,[17] the court, refused accused's bail on the basis of creating fake Facebook ID of the complaint which was provided through investigation by the FIA on the basis of IP address. In *Junaid Arshad v. the State*,[18] the court also refused bail on the basis of evidence collected from cell phone and IP address.

It is pertinent to mentioned here that an IP addresses can be spoofed by the criminals to hide their true identity.

7.4.2 TRANSMISSION CONTROL PROTOCOL (TCP)/IP

The Internet is international network of interconnected computers and networks "that operates using a standard set of communication protocols called transmission control

[16] Casey, *Digital Evidence and Computer Crime*, 740.
[17] *Farhan Kamrani v. the State*, 2018 YLR 329 (Sindh).
[18] *Junaid Arshad v. the State*, 2018 PCrLJ 739 (Lahore).

protocol/Internet protocols (TCP/IP)."[19] As TCP/IP is an open source and "there are very large numbers of network devices and software which support it,"[20] therefore, almost in every operating system TCP/IP is built in.

Whereas TCP/IP is a "combination of protocols that includes the IP, TCP, and User Datagram Protocol (UDP). IP functions at the network layer, addressing and routing data. TCP operates on the transport layer—acknowledging receipt of information and resending information when necessary."[21] Although, UDP is a simple protocol "that some applications use instead of TCP when an acknowledgment of receipt is not desired or when acknowledgments are handled by the application."[22] Nowadays, every host that is linked to the internet use TCP/IP for communication purposes. These are very important to tackle the "common problems that arise on a network, including hardware failure, network congestion, data delay, loss, and corruption as well as sequencing errors."[23] However, the TCP should be "able to operate above a wide spectrum of communication systems ranging from hard-wired connections to packet-switched or circuit-switched networks."[24]

The investigator does not forget that "TCP streams are bidirectional, enabling a host to both send and receive data. Each TCP stream comprises two flows, one for receiving data and the other for sending data."[25] Furthermore, the TCP is a "connection-mode service, often called a virtual-circuit service that enables transmission in a reliable, sequenced manner that is analogous to a telephone call."[26] It is necessary for the forensic examiner and investigator to know TCP can

---

[19] Stanfield, "The Authentication of Electronic Evidence," 71.
[20] Sommer, *Digital Evidence, Digital Investigations and E-Disclosure,* 111.
[21] Casey, *Digital Evidence and Computer Crime,* 738.
[22] Ibid.
[23] Ibid.
[24] Marcella and Menendez, *Cyber Forensics*, 59.
[25] Casey, *Digital Evidence and Computer Crime,* 748.
[26] Casey, *Handbook of Digital Forensics and Investigation,* 444.

differ from the UDP. It is pertinent to mention here that UDP is also connectionless, and its each unit's delivery is not guaranteed.

As discussed, that TCP/IP plays an important role in networks, so, the investigator should know that "IP addresses, port numbers, TCP flags, and other TCP/IP-related data accumulate in many places."[27] Therefore, proper understanding that how to collect digital evidence on TCP/IP is imperative in any on networks. Generally, sniffer logs contain TCP/IP-related information. However, "it is not feasible to capture all network traffic in all situations, making it necessary to rely on other sources of evidence such as log files that show past connections, and state tables that show recent and current connections between hosts."[28]

TCP/IP is commonly used globally to provide network communications. Generally, TCP/IP communications are "composed of four layers that work together. When a user wants to transfer data across networks, the data is passed from the highest layer through intermediate layers to the lowest layer, with each layer adding additional information."[29] The TCP keeps a record of everything until it reaches its end/target. In case, if the concerned TCP does not receive "an acknowledgment after a set amount of time, it assumes that the information was lost and resends it. So, if one packet is lost or damaged in transit, TCP will resend just that packet, not the entire message."[30]

The existing TCP/IP scheme is IPv4 and the new scheme IPv6. Whereas, in an IP address "four decimal-separated numbers, which allows for a total of 256^4 or 1,099,511,627,776 unique

---

[27] Casey, *Digital Evidence and Computer Crime,* 754.
[28] Ibid.
[29] Marcella and Menendez, *Cyber Forensics*, 155.
[30] Casey, *Digital Evidence and Computer Crime,* 748.

addresses,"[31] is being used. Because of growth of new devices, a new scheme IP version is introduced to meet the need of existing devices. In IPv6, these addresses "are represented as eight groups of four hexadecimal digits separated by colons."[32] The most important thing in IPv6 is that encryption is add in this which will eliminate spoofing threats.

7.4.3 TCP/IP Layers and their significance in Network Forensics

There are four TCP/IP layers which are important for the purpose of cyber forensics investigation. These layers are application, transport, Internet Protocol and hardware layer. These are discussed briefly:

1. Application Layer: Application layer "sends and receives data for particular applications, such as Domain Name System (DNS), Hypertext Transfer Protocol (HTTP), and Simple Mail Transfer Protocol (SMTP)."[33]
2. Transport Layer: This layer provides "connection-oriented or connectionless services for transporting application layer services between networks. The transport layer can optionally ensure the reliability of communications."[34] TCP and UDP are generally used transport layer protocols.
3. Internet Protocol Layer (or Network Layer): The IP layer "routes packets across networks. IP is the fundamental network layer protocol for TCP or IP."[35]

---

[31] National Institute of Justice, *Investigations Involving the Internet and Computer Networks* (Washington, D.C: National Institute of Justice, 2007), 6.

[32] Stanfield, "The Authentication of Electronic Evidence," 71.

[33] Marcella and Menendez, *Cyber Forensics,* 155.

[34] Ibid., 156.

[35] Ibid.

4. Hardware Layer (or Data Link Layer): Hardware layer "handles communications on the physical network components. The best-known data link layer protocol is Ethernet."[36]

Each of these TCP/IP protocol suites contains significant information for the investigators in any investigation. For instance, the hardware layer (data link layer) provides "information about physical components, while other layers describe logical aspects."[37]

An investigator can map an IP address to the MAC address and the MAC is a "unique code assigned to most forms of networking hardware. The address is permanently assigned to the hardware, so limiting a wireless network's access to hardware is a security feature employed by closed wireless networks."[38] Still an experienced criminal can "figure out an authorized MAC address, masquerade as a legitimate address and access a closed network of a particular NIC, thereby identifying a host of interest."[39] Thus, it can be said these layers are gold mine for the forensic investigators.

7.4.4 TRACING AN INTERNET PROTOCOL ADDRESS TO A SOURCE

Without having any identity, it is not possible to reach a specific house or office. Normally, house numbers are assigned to reach the destination. "Just as every house has an address, every computer connected to the Internet has an address. This is referred to as an Internet Protocol (IP) address."[40] Therefore, every computer or device involved in communicating on the Internet, needs a unique address, which is an IP address.[41]

---

[36] Marcella and Menendez, *Cyber Forensics,* 156.
[37] Ibid.
[38] Ibid.
[39] Ibid.
[40] National Institute of Justice, *Investigations Involving the Internet and Computer Networks*, 5.
[41] Ibid.

Likewise, domain names are "IP addresses of computers which have been translated to a World Wide Web address that we can understand. Domain Name Service providers keep a database of all domain names, so that the various domain names can be located."[42] For instance, when a computer user types into a web browser, the home page is actually from the IP address of the concern website's server. When the server is connected, website server displays information using HTTP.

In *Qurban Ali v. The State* the SHC held that:

> There are several free software tools available on Internet which can trace back the IP Address of the Sender through the header text of the E-mail received. After getting the IP of the sender, the concerned ISP can be contacted to get further information..... The address of the telephone holder/owner can obtained from PTCL/NTC. In this way the E-mail sending computer can be identified and the data of the E-mail can be retrieved from it by using Computer Forensics Tools. It is also possible to prove it in Court of Law provided proper chain of custody of maintained. However, it is difficult to identify the particular person who sent the E-mail; this is the area where investigation by some police agency is required.[43]

In *Ahmad Omar Sheikh v. the State*,[44] the trial court convicted the appellants, *inter alia,* on the basis of IP address. However, the SHC on the basis of contradiction in evidence acquitted the appellants but the provincial government challenged the decision of SHC before the SC and the SC maintained the SHC decision.[45]

In *Farhan Kamrani v. the State*,[46] the FIA traced the accused persons using IP address. Similarly, the accused *Muhammad Ashraf v. the State,*[47] was traced on the basis of IP address and

---

[42] Stanfield, "The Authentication of Electronic Evidence," 72.
[43] *Qurban Ali v. The State,* 2007 PCr L J 675 Karachi.
[44] *Ahmad Omar Sheikh and other v. the State*, 2021 YLR 1777 (Sindh).
[45] *The State through P.G. Sindh v. Ahmed Omar Sheikh*, 2021 SCMR 873.
[46] *Farhan Kamrani v. the State*, 2018 YLR 329 (Sindh).
[47] *Muhammad Ashraf v. the State,* 2018 PCrLJ 1667 (Lahore).

hence his bail was refused. In a latest judgment of the Sindh jurisdiction, in *Kashif Dars v. the State*,[48] the court refused the bail of accused on the basis of IP address and mobile phone.

Furthermore, obtaining an IP address is not difficult, anyone can obtain IP address easily. However, tracing a specific user's IP address, is very difficult "and is complicated by factors such as whether the IP address is static or dynamic and whether the user was on an unsecured[49] or secured network."[50] Besides, while investigating cybercrimes, the investigator must keep in mind that "IP addresses can be changed and concealed, allowing individuals to pretend that they are connected to a network from another location."[51]

It cannot be safely concluded that the IP address is used by the actual person, as Larson say "IP address is analogous to locating the phone tower that a cell phone connected to, rather than the actual phone used."[52]

7.4.5 DYNAMIC AND STATIC IP ADDRESSES

In ICT regime, there are two different types of IP address existing in the digital world, such as dynamic and static. For instance, dynamic IP addresses "are temporarily assigned from a pool of available addresses registered to an ISP. These addresses are assigned to a device when a user begins an online session."[53] Therefore, it is possible, that a certain device use different IP address for each session. However, there is a problem that after an incident, certain IP address may be assigned to any other person, making the investigation more difficult. In other words, dynamic IP

---

[48] *Kashif Dars v. the State,* 2020 PCrLJ 259 (Sindh).

[49] There are two types of networks: secured and unsecured network.

[50] Erin Larson, "Tracking Criminals with Internet Protocol Addresses: Is Law Enforcement Correctly Identifying Perpetrators?" *North Carolina Journal of Law & technology* 18 (2017): 316-358, at 318.

[51] Casey, *Handbook of Digital Forensics and Investigation*, 29.

[52] Larson, "Tracking Criminals with Internet Protocol Addresses," 319.

[53] National Institute of Justice, *Investigations Involving the Internet and Computer Networks*, 7.

address "can make it more difficult to determine who was using an IP address at a given time. Fortunately for investigators, ISPs often maintain a log of dynamic IP address assignments, listing who was assigned a particular IP address during a specific period."[54]

Dynamic IP is used by the ISPs to adjust the use of available public addresses, as the number of customers are more than the IP addresses. Therefore, each ISP has collection of addresses to facilitate the customers. This is used where, consumers do not want "to be communicating on the Internet all of the time. So, the opportunity exists to let a customer lease an IP address for a short period when needed as opposed to having a permanent fixed address."[55]

In contrast, static IP addresses are "permanently assigned to devices configured to always have the same IP address. A person, business, or organization maintaining a constant Internet presence, such as a Web site, generally requires a static IP address."[56] Therefore, this is easy in any investigation.

7.4.6 PROXIES

Criminals are using proxies to conceal their identities. This is done concealing an IP address while surfing the web "to direct all page requests through a proxy. Web servers that are accessed via a proxy record the IP address of the proxy rather than that of one's computer."[57] There are several web proxies available freely.

---

[54] Casey, *Digital Evidence and Computer Crime,* 753.
[55] Sommer, *Digital Evidence, Digital Investigations and E-Disclosure,* 112.
[56] National Institute of Justice, *Investigations Involving the Internet and Computer Networks*, 7.
[57] Casey, *Digital Evidence and Computer Crime,* 693.

When criminal use proxies "to conceal their identities, it makes tracking more difficult because investigators must obtain information from the server running the proxy to determine the actual IP addresses of the offenders."[58] This makes the task of investigator more difficult and time consuming. And if the proxy server is another county, then, it adds additional problems for the investigators.

7.4.7 IP SPOOFING

Criminals have employed various tactics on the internet to hide their true identity, *inter alia*, is IP spoofing. Spoofing[59] has been used by the criminal in conventional crimes too. This technique is old but the method employed is new. "IP spoofing is one of the most common forms of online camouflage. In IP spoofing, an attacker gains unauthorized access to a computer or a network by making it appear that a malicious message has come from a trusted machine by spoofing the IP address of that machine."[60]

More specifically, spoofing is the conception of "TCP/IP packets using somebody else's IP address. Routers use the destination IP address to forward packets through the Internet, but ignore the source IP address. That address is only used by the destination machine when it responds back to the source."[61] Stating differently, users having some basic knowledge of technology and

---

[58] Casey, *Digital Evidence and Computer Crime,* 693.

[59] Spoofing is an offence under section 26 of the PECA, which is as under:

26. Spoofing.— (1) Whoever with dishonest intention establishes a website or sends any information with a counterfeit source intended to be believed by the recipient or visitor of the website, to be an authentic source commits spoofing.

(2) Whoever commits spoofing shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to five hundred thousand rupees or with both.

[60] Marcella and Menendez, *Cyber Forensics*, 58.

[61] Ibid., 59.

operation of the internet system can easily spoof "their IP address to re-route to another address,"[62] and ISPs similarly allow users to obtain new IP addresses when they desire."[63] It is not difficult to spoof an IP address rather "it's very easy to mask a source address by manipulating an IP header,"[64] therefore an investigator should "establish beyond reasonable doubt that the e-evidence collected from the suspect's machine was, in fact, generated from the suspect's machine and not via an external source."[65] In addition to IP spoofing, e-mails can also be spoofed and there are free software available on the internet.

In Pakistan, however, general spoofing is a criminal offence which was criminalized first time in 2007 through section 15 of the PECO, 2007 and after the expiry of this ordinance, PECO, 2008 and PECO, 2009 retained this provision. But, after lapse of these ordinances there was a gap till 2016 when, spoofing was again criminalized through section 26 of the PECA, 2016, however, this was made sever offence and punishment of fine was increased to five hundred thousand rupees which was not mentioned in PECOs.

7.4.8 INTERNET SERVICE PROVIDERS (ISPS)

The ISPs are the richest source of digital evidence in internet related investigation. Everywhere in the world, legally all service providers are keeping "some information about their customers. These records can reveal the location and time of an individual's activities, such as

---

[62] "Spoofing" is used to disguise IP addresses by re-routing through those trying to determine where the "router is to another computer or by providing a false IP address." For instance, *In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 759 (S.D. Tex. 2013).

[63] Erin Larson, "Tracking Criminals with Internet Protocol Addresses: Is Law Enforcement Correctly Identifying Perpetrators?" *North Carolina Journal of Law & technology* 18 (2017): 316-358, at 344-345.

[64] https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=9d18fc06-b229-4c4a-8ca5-7386d0870c01&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments (accessed: 25th April, 2020).

[65] Marcella and Menendez, *Cyber Forensics*, 60.

items purchased in a supermarket, car rentals and gasoline purchases, automated toll payment, mobile telephone calls, Internet access, online banking and shopping, and withdrawals from automated teller systems."[66] Which can be very useful in investigation perspective.

Although, telephone companies "and ISPs try to limit the amount of information that they keep on customer activities, to limit their storage and retrieval costs and their liability, law makers in some countries are starting to compel some communications service providers to keep more complete logs."[67] ISPs provides various services to their customers, including but not limited to "providing connections to the Internet, email, and web site hosting. ISPs generate log files in relation to each of these services, such as details of emails held on the ISP's mail server computers."[68] Remote Authentication Dial in User Service (RADIUS) logs is very important which "identify the person who was using a specific IP address while accessing the Internet via the ISP."[69] However, due to storage cost, ISPs do not retain logs files for indefinite period. But in Pakistan, this duration is one year as prescribed in section 32 of the PECA, and in case of violation the violator shall be punishable with fine.

ISPs can store different kinds of information including subscriber's information such as name, address, phone number, credit card number, date, time, IP addresses, and customer's activities. Moreover, the ISP can have "the customer's opened, unopened, draft, and sent emails."[70]

---

[66] Casey, *Digital Evidence and Computer Crime,* 46.

[67] Ibid.

[68] David Chaikin, "Network investigations of cyberattacks: the limits of digital evidence," *Crime, Law and Social Change* 46 (2006): 239-256 at 244-245.

[69] Ibid.

[70] *Searching and Seizing Computers,* 121.

Likewise, in USA the Stored Communications Act (SCA),[71] which was enacted in 1986, provides statutory rights for the customers and subscribers of computer network service providers. This Act provides that how government can get the stored information from ISPs. Besides, it also provides the process for the LEAs. Under this Act, the service provider will provide the following details to the investigator, such as name, address and credit card of the subscriber.

Section 2510(15),[72] defines an electronic communication service (ECS) provides which "means any service which provides to users thereof the ability to send or receive wire or electronic communications." Whereas, section 2711(2)[73] defines a remote computing service as "the provision to the public of computer storage or processing services by means of an electronic communications system." In all these definitions, all the service provider falls. However, a criminal agency under section 2703 (f) can request a person or an entity such as ISP to preserve data. Section 2703(f) (1) states that "A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process."[74]

---

[71] 18 U.S.C. §§ 2701-2712. Generally, known as the Stored Communications Act (SCA). The SCA is sometimes referred to as the Electronic Communications Privacy Act. The SCA was included as Title II of the Electronic Communications Privacy Act of 1986 ("ECPA"), but ECPA itself also included amendments to the Wiretap Act and created the Pen Register and Trap and Trace Devices statute addressed in Chapter 4. See Pub. L. No. 99-508, 100 Stat. 1848 (1986). Although 18 U.S.C. § 2701-2712 is referred to as the "Stored Communications Act" here and elsewhere, the phrase "Stored Communications Act" appears nowhere in the language of the statute.

[72] 18 U.S.C. § 2510(15).

[73] 18 U.S.C.§ 2711(2).

[74] 18 U.S.C. § 2703 (f)(1).

7.5 SOCIAL NETWORKING SITES

Social media (social networking sites[75]) technologies, websites and applications[76] were not common before few years, and these have now gained widespread acceptance across the globe. It cannot be ignored that it may be superseded by the other forms of technologies in coming years. Whereas, the explosion of participants in social networking venues, "including the creation of business and professional groups hosted on these sites, has resulted in information creation that is outside the knowledge and control of any specific organization."[77]

Social media sites are gold mine of digital evidence. Whereas, "the expression 'social media' encompasses a variety of platforms and includes social networking sites where users can create their own webpages and communicate with others via online chat, instant messaging services, blogging and even by voice or video."[78] Many people on daily basis share their thoughts, audios, video, photos and even their movement (locations) using smart phones. Besides, GPS in mobile phone can also help the investigator that from which location the image or any information was shared on the internet. Thus, it can be said that social media is completely new and unique in ICT era. Therefore, this also creates new challenges (technically and legally) such as whether the existing rules of evidence will apply or new rules will be required?

In fact, acceptance of social networking sites requires a stricter standard of authentication of digital information because of lack of restrictions on creation of such sites.[79] Thus, anyone

---

[75] Such as Facebook, LinkedIn, MySpace and Twitter.

[76] WhatsApp and Imo.

[77] https://www.crl.edu/sites/default/files/d6/attachments/pages/Thomson-E-evidence-report.pdf (accessed: 30th November, 2019).

[78] Stanfield, "The Authentication of Electronic Evidence," 88.

[79] These are some of the cases in which the fake social networking sites' ID were made. *Farhan Kamrani v. the State*, 2018 YLR 329 (Sindh); *Muhammad Ashraf v. the State,* 2018 PCRLJ 1667 (Lahore); *Aamir Shmas v. the State,* 2019 PCrLJ 41 (Islamabad).

having basic knowledge of computer can "create a social network profile anonymously, using a pseudonym, or in someone else's name. Since one or many people may post messages on a social networking site, courts cannot necessarily attribute a particular message to the person who owns the site." Further, it is more difficult to determine when the accused is using public library computer.

Certainly, social networking sites are very difficult to authenticate, therefore, in *Griffin v. State,*[80] the court held that "a person observing the online profile of a user with whom the observer is unacquainted has no idea whether the profile is legitimate." It is not disputed now that anybody can easily "create a fictitious account and masquerade under another person's name or can gain access to another's account by obtaining the user's username and password." Initially, there was no specific enactment dealing such types of activities in Pakistan which can prevent someone from creating a fake account under some other person's name, but section 16[81] of the PECA has prohibited such act.[82]

In Pakistan, evidence from social networking sites is admitted. In *Farhan Kamrani v. the State,*[83] the court, refused the bail of the accused on the basis of creating fake Facebook ID of the complaint which was provided through investigation by the FIA on the basis of IP address.

---

[80] *Griffin v. State,* 419 Md. 343, 19 A. 3d 415 (2011).

[81] Section 16 is read as under: **16. Unauthorized use of identity information.**— (1) Whoever obtains, sells, possesses, transmits or uses another person's identity information without authorization shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to five million rupees, or with both.

(2) Any person whose identity information is obtained, sold, possessed, used or transmitted may apply to the Authority for securing, destroying, blocking access or preventing transmission of identity information referred to in subsection (1) and the Authority on receipt of such application may take such measures as deemed appropriate for securing, destroying or preventing transmission of such identity information.

[82] Courts have also awarded punishment on the basis of creation of fake IDs.

[83] *Farhan Kamrani v. the State*, 2018 YLR 329 (Sindh).

Similarly, the court in *Muhammad Ashraf v. the State,*[84] refused the bail of the accused on the basis of creating fake Facebook ID.

7.6 WEBSITES

The first website was launched in 1991 and now it is "mistakenly referred to as the Internet."[85] Generally, a website is referred as "a collection of related Web pages or files that is stored on a Web server."[86] A website has many components. Among these components, the first thing is the HTML in which these pages are written. HTML allows users "to easily navigate between related pages or files in the collection. It also allows a related collection of pages to be linked to another related collection of pages."[87] The HTML also defines "the content and format of a page. In addition to the graphical representation provided to the viewer, the page may contain additional information related to its author, programming code, metadata, and other identifying information that may not be displayed in Web page view."[88]

Websites are both used for legal and illegal purpose. Some websites those have an illegal purpose "attempt to obfuscate their actual location by using Web redirection services. This type of redirection simply embeds the page within a frame and can be seen clearly by viewing the source HTML through a Web browser or from the server directly."[89] However, other websites use "redirection to forward the individual to a completely different server so investigators must remain alert and verify which server they are connected to when collecting digital evidence."[90]

---

[84] *Muhammad Ashraf v. the State,* 2018 PCRLJ 1667 (Lahore).
[85] Casey, *Digital Evidence and Computer Crime,* 674.
[86] National Institute of Justice, *Investigations Involving the Internet and Computer Networks*, 27.
[87] Ibid.
[88] Ibid., 28.
[89] Casey, *Digital Evidence and Computer Crime,* 675.
[90] Ibid., 676.

Now website evidence is admitted in courts. However, any information copied from a website is required tough criteria as the web pages are normally unreliable. As the content of a web site can easily be forged and modified.

Information on websites is not always credible and it may be completely and intentionally falsified. Thus, anything which is posted on a website cannot be said that is genuine and backed by any physical proof. With this type of "free-for-all wild west of publishing information on the Internet, why would any investigator consider using it at all? The answer lies in the source of the information."[91] However, web pages generated from official government websites are considered to be authenticate and admitted in evidence.[92] Certainly, "notwithstanding the genuine risk of unreliability due to hacking or other malicious changes, the courts continue to admit such information into evidence."[93]

But situation gets worst when the criminals use dark web browsers. In the words of Larson:

> Matters are further complicated when criminals use dark web browsers to remain private. Dark web browsers attempt to safeguard user's information by allowing "users to access the Internet in an anonymous fashion," helping users to remain private on the seemingly non-private web.[94] The advantage of using a dark web browser, particularly for criminal activity, is that the IP address location is hidden, and therefore not easily ascertainable.[95]

In one situation, capturing the information from one page will be sufficient in an investigation. However, in other investigation, entire contents will be required. Therefore, it depends upon the investigator either to capture the relevant page or the entire web, on the basis of specific nature of investigation.

---

[91] Shavers, *Placing the Suspect behind the Keyboard*, 212.

[92] *Williams v. Long*, 2008 WL 4848362 (D. Md., November 7, 2008).

[93] https://www.crl.edu/sites/default/files/d6/attachments/pages/Thomson-E-evidence-report.pdf (accessed: 30th November, 2019).

[94] *United States v. Matish*, 193 F. Supp. 3d 585, 593 (E.D. Va. 2016).

[95] Larson, "Tracking Criminals with Internet Protocol Addresses," 325.

7.7 INTERNET EXPLORER

There are various browsers which are being used by the internet user to access websites. Similarly, the Internet Explorer is the web browser "that Microsoft has integrated with its products since the late 1990s, and remains one of the most popular web browsers in circulation today."[96] Although, there are many other browsers available.[97] Internet Explorer is used on every Windows computer. Every few years, new version of the internet explorer is introduced.

In internet related investigation, an investigator will be able to find several artifacts on the Internet Explorer, if the internet is being used by the offender. The investigator will find the registry artifacts, typed URLs, cookies, web cache and the Internet history.

Generally, the term cookie refers to "a small text file usually downloaded to user workstations from web servers when sites hosted by those web servers are visited. The purpose of cookies varies depending on the web server, but they can be used for authentication or session tracking, as well as communicating user preferences to the server."[98] Though, in some cases, these text files may be "difficult to decode, they often contain references to URLs, domain names, usernames, and dates and times that can be of use to the investigator."[99] The presence of "a URL in a cookie is not proof positive that the user visited that URL, it is strong circumstantial evidence."[100]

The values stored in any registry of the Internet Explorer are "in hexadecimal format, but can be converted to ASCII. An example of the type of information that the registry can provide to

---

[96] Casey, *Handbook of Digital Forensics and Investigation*, 280.
[97] Such as Firefox, Opera, and Google Chrome.
[98] Casey, *Handbook of Digital Forensics and Investigation*, 280.
[99] Ibid.
[100] Ibid.

an investigator is the Auto Complete data for a user of Internet Explorer visiting a particular website such as his name, address, telephone number, email address and passwords."[101] Moreover, it can be help for investigator "to establish when the user last downloaded a file from the Internet, and the first page the user visited from the registry."[102]

7.8E-MAIL EVIDENCE

Electronic mail (e-mail) is a service "that enables people to send electronic messages to each other. Provided a message is correctly addressed, it will be delivered through cables and computers to the addressee's personal electronic mailbox."[103] It has also various components, which can be used by the investigator. In every e-mail message, there is a header which is important for investigation purposes "that contains information about its origin and receipt. It is often possible to track e-mail back to its source and identify the sender using the information in e-mail headers."[104] However, this factor should not be ignored that the information in an e-mail header can be forged, therefore, the investigator should use precautionary measures.

E-mail is widely used services by the individuals and organization on the Internet, thus it is "one of the most important vehicles for criminal activity, offering a high level of privacy, especially when encryption or anonymous services are used, making it difficult to determine if e-mail is being used to commit or facilitate a crime."[105] However, proving that a specific message was sent by a certain individual is not easy, as email can be created easily without the knowledge and authorization of any person by using his name and credential.

---

[101] Mason and Seng, *Electronic Evidence*, 8.
[102] Ibid.
[103] Casey, *Digital Evidence and Computer Crime*, 677.
[104] Ibid.
[105] Ibid.

Most e-mail applications are being used for receiving and sending of e-mails. However, some e-mail application also "provide an address book that can hold contact information, such as e-mail addresses, names, and phone numbers. Encryption programs are sometimes used in conjunction with e-mail clients to encrypt an e-mail's body or attachments."[106] Thus, an email's information can be obtained from various sources as a single e-mail message can "be recorded in several places—the sender's system, each e-mail server that handles the message, and the recipient's system, as well as antivirus, spam, and content filtering servers."[107] In other words, it is "persistent, residing in multiple locations, making it harder to get rid of."[108] Thus, if the efforts are made then there is a possibility to track the actual culprit. Some of the relevant information that can be obtained by the investigator in any investigation is e-mail addresses (sender and receiver), IP addresses, subject of email, date and time.

In *United States v. Councilman*,[109] is a criminal case where an e-mail in temporary storage *en route* to its destination was intercepted by the LEAs in USA, in which the court ruled that "the term electronic communication includes transient electronic storage that is intrinsic to the communication process, and hence that interception of an e-mail in such storage is an offense under the Wiretap Act." Whereas, in an earlier case *United States v. Ferber,*[110] the court held that e-mail messages are admissible in evidence.

In *Ahmad Omar Sheikh v. the State*,[111] the trial court convicted the appellants, *inter alia,* on the basis of email allegedly sent by the appellants. However, the SHC on the basis of

---

[106] Marcella and Menendez, *Cyber Forensics*, 173.
[107] Ibid.
[108] Sammons, *Basics of Digital Forensics*, 127.
[109] *United States v. Councilman,* 418 F.3d 67 (1st Cir. 2005).
[110] *United States v. Ferber,* 966 F. Supp. 90 (D. Mass. 1997).
[111] *Ahmad Omar Sheikh v. the State*, 2021 YLR 1777 (Sindh).

contradiction in evidence acquitted the appellants and the same decision was maintained in appeal by the SC.[112]

7.8.1 ISSUES TO BE AWARE OF REGARDING EMAILS

There are some very serious issue regarding emails which are important for investigator to keep in mind while investigation email related crimes such as spoofed email headers, anonymizers, remote location, delayed sending and an email location. These are discussed briefly.

Spoofed e-mail headers: It must be noted that in email "anything up to the last (topmost) Received: line in the message header can be spoofed, or faked."[113]

Anonymizers: Anonymizers are actually e-mail servers "that strip identifying information from the message before forwarding it. Although valid reasons exist for using an anonymizer service, many individuals use the service to conceal their identity."[114] Therefore, it is very difficult to trace the email, if an anonymizer is used.

Remote locations: Nowadays, everywhere in many public places the Internet is available "such as libraries, schools, airports, hotels, and Internet cafes. If an e-mail message is sent from one of these locations, determining the actual sender may be difficult."[115] As these places are used by various people making it further complicate for the investigator to link the actual culprit.

Delayed send: Now almost everywhere many e-mail service providers provider facility which "have the ability to allow the sender to schedule the time an e-mail is sent. Also, some

---

[112] *The State through P.G. Sindh v. Ahmed Omar Sheikh*, 2021 SCMR 873.
[113] National Institute of Justice, *Investigations Involving the Internet and Computer Networks*, 23.
[114] Ibid.
[115] Ibid.

servers send e-mail at a certain prescheduled time. Either of these situations could allow an individual to be at another location at the time the mail is actually sent."[116] Plea of *alibi* can be taken while using this technique. Therefore, this angle must also be examined by the investigator.

E-mail location: "Regardless of the type of e-mail being used, the message can be stored in multiple locations." Therefore, the investigator should consider obtaining it from maximum possible sources. This is not out of context to remember that many email service providers does not retain data for long time, thus, the investigator, without wasting precious time should proceed to collect the relevant data the earliest possible time.

Moreover, the email may be tampered or encrypted, therefore, this aspect also not be ignored by the LEAs.

7.8.2 E-MAIL TRACKING

Although technology has made it possible for the trained digital forensic examiners and investigators to track e-mail back to its source, but it is not very difficult to reach the actual culprit and identify the email sender by using the e-mail headers information. Therefore, it is imperative for the investigator to know how the email can be forged and how to extract information from its headers. There can be many reasons for forged email such as false impression and concealment of their true identity. But, this approach "to anonymity is ineffective because forgeries usually contain the sender's IP address."[117]

---

[116] National Institute of Justice, *Investigations Involving the Internet and Computer Networks*, 24.
[117] Casey, *Digital Evidence and Computer Crime*, 699.

It is crucial for the investigator to understand that how an email message is created and transmitted. Whenever on the internet an e-mail message is sent, "it first goes to a local Message Transfer Agents (MTAs) and the local MTA puts the current time and the name of the MTA along with some technical information at the top of the e-mail message."[118] Thereafter, this message is delivered from "one MTA to another until it reaches its destination."[119] Hence, every MTA which receives the said message "puts a received header at the top of the message. This means that the last computer to handle the message is listed at the top of the header, and the first computer is listed near the bottom."[120] Consequently, the investigator will make appropriate efforts to track an e-mail by using the route that the e-mail traveled.

In *Qurban Ali v. The State*, the SHC held that

> An E-mail address can be created by anybody under any name, therefore, the person who created the E-mail address is required to be examined in Court so as to prove its authenticity otherwise it will adversely affect the authenticity of the E-mail. Further, E-mail must have been mailed through a computer by using internet, which can be connected through a telephone. The E-mail could have been traced through telephone number about the identity of the person who sent the E-mail.[121]

7.9 HYPER TEXT TRANSFER PROTOCOL (HTTP)

HTTP is another important component of the internet which is "an application layer protocol used for transferring information between computers on the World Wide Web. HTTP is based on a request/response standard between a client; usually the host and a server, a web site."[122] The client establishes a TCP connection with a server. Thereafter, the said server responds to the request. Stating differently, HTTP allows "a web browser on a user's computer to send requests to

---

[118] Ibid.
[119] Ibid.
[120] Ibid., 700.
[121] *Qurban Ali v. The State,* 2007 PCrLJ 675 Karachi.
[122] Casey, *Handbook of Digital Forensics and Investigation,* 448.

web servers to download data from those web servers. A web server can refer to the entire computer system, an appliance, or specifically to the software that accepts and supervises the HTTP requests."[123] However, it is important to note "that HTML is not a programming language."[124]

Understanding of the basic structure of HTTP is very important for the investigators, as web browsing are used for online communication. Normally, HTTP is configured on TCP port 80, but the administrator can change it to any port and he can also configure on any port. Likewise, HTTP traffic "can be encrypted with HTTP over TLS (Transport Layer Security), also called Secure HTTP (HTTPS). HTTPS typically uses TCP port 443, and though HTTPS still follows the HTTP standards, all the contents of the messages are encrypted, making it difficult to analyze the network traffic."[125] Therefore, the investigator should be aware of request method used and the corresponded status code. Whereas HTTP defines "eight methods indicating the desired action to be performed on the requested resource."[126] Further, the investigator should also understand the status code as well.

7.10 SUMMARY

The internet is a gold mine of information, many people are using internet for various purpose including illegitimate purpose. Everybody who use the internet, also use the email and social networking sites, where he shares his thoughts, ideas, photos, video and location. These can help the investigator in any investigation. But the crucial point is that it cannot be certain that the

[123] Stanfield, "The Authentication of Electronic Evidence," 72.
[124] Sammons, *Basics of Digital Forensics,* 120.
[125] Casey, *Handbook of Digital Forensics and Investigation,* 448.
[126] Ibid.

device was used by the actual person as the email and webpages can be forged besides using spoofing techniques.

A website consists of various web pages, where different domain name, webserver, IP address, URL, LAN, HTTP, the Internet addresses and other related things are used to communicate online. Besides, webpages are dynamic and are changing and updating frequently. Therefore, authentication can be challenged easily. Moreover, if the black web is used then it will make the task of investigator more difficult.

CHAPTER EIGHT:

DIGITAL EVIDENCE IN THE COURTROOM AND LEGAL FRATERNITY

8.1 INTRODUCTION

There are many stages in digital evidence collection to evidence production and the last stage is the production of evidence before the courts. This chapter examines the production of evidence in courts. Digital evidence is presented in the courts through expert witness, therefore, forensic education for experts, prosecution, lawyers and judges is also discussed in the light of judgements of various courts. At the end, it is examined that how judges access the digital evidence. Lastly, online courts and recording of evidence through video conferencing is discussed.

8.2 DIGITAL EVIDENCE PRODUCTION

Before the introduction of technologies in the courts, the only recognized medium was direct evidence recorded in physical presence of the witnesses of the parties and documents exhibited in physical form in the trial. However, technologies have introduced various complications in the evidence production in the courts.

The use of digital evidence "in courts can effectively be considered a major innovation in the sphere of justice. In fact, as the justice system becomes increasingly digitized, many see the use of electronic evidence as a means of simplification, facilitation, acceleration, and rationalization, depending on the circumstances."[1] This can provide better service and inexpensive and expeditious justice to citizens of Pakistan as envisaged in the Constitution of Pakistan.[2]

---

[1] Biasiotti et al. *Handling and Exchanging Electronic Evidence across Europe*, 289.

[2] Article 37 (d) of the Constitution of Pakistan.

It is the prime duty of the investigating agency to ensure that "the evidence was not altered between its acquisition and its presentation in legal proceedings and even before its acquisition by the practitioner. If it was altered for some reason, then this must be disclosed to the court and other parties to the trial."[3] Moreover, chain of custody of the exhibit "must be fully documented to account for its location and custodianship between seizure and presentation."[4] Furthermore, the investigator should also establish that the evidence was "protected from physical damage while being transported from the crime scene to the place of safekeeping and laboratories."[5]

Digital data is not like other type of data, as digital data "is not directly observable by the finder of fact, it must be presented through expert witnesses using tools to reveal its existence, content, and meaning to the fact finders." About digital evidence, it can be said it is hearsay evidence which is presented "by an expert who asserts facts or conclusions based on what the computer recorded, not what they themselves have directly observed." Moreover, in digital evidence, the expert witness plays an important role. Therefore, "it depends on the quality and unbiased opinion of the experts for each side."[6]

8.3 Forensics Education and Training

In existing environment, law cannot be separated from science and technology. As the technology progress, the demand to understand the link between two is also increasing to adjudicate it properly. Whereas, forensic evidence "lies at the juncture between science, technology, and the law. In the age of information, everyone who plays a role in the justice system

[3] Boddington, *Practical Digital Forensics*, 93.
[4] Ibid., 94
[5] Ibid.
[6] Johnson, *Forensic Computer Crime Investigation*, 150-51.

must be accountable to increased learning and knowledge in and around their domain."[7] Therefore, it is imperative for the legal fraternity "to understand the role of the expert witness, the attorney, the judge and the admission of forensic science evidence in litigation in our criminal justice system."[8]

To handle digital evidence in courts properly, courts and lawyers should have "sufficient knowledge of technical aspects to have an understanding of how to preserve evidence and how to evaluate and interpret the materials presented."[9] This also requires having "a basic knowledge of the technicalities of, software used in the discovery process, but also an understanding of social media, the technical options, and the way people use these media."[10] It has been observed in Pakistan that the lawyers and judges lack of expertise in this field. Thus, it is the need of the hour to get, at least, some basic knowledge to proceed properly.

The existing judicial system, in Pakistan, is full of judges and lawyers "who generally lack the scientific expertise necessary to comprehend and evaluate forensic evidence in an informed manner."[11] Nevertheless, the assessment of digital evidence is more complex than other type of evidence. Therefore, to assist the courts involving experts and "a proper understanding of their findings by courts and lawyers, the digitisation of society and proceedings requires tech-savvy judges and lawyers."[12] Somehow, the need of basic education and training in digital forensic is imperative for judges and lawyers alike. Thus, learning basis forensics will help the lawyers to

---

[7] Amy Lynnette, "Digital and Multimedia Forensics Justified: An Appraisal on Professional Policy and Legislation," (M.S. diss., University of Colorado Denver, 2015), 27.

[8] Amy Lynnette, "Digital and Multimedia Forensics Justified," 27.

[9] Kramer, "Challenges of Electronic Taking of Evidence," 409.

[10] Ibid.

[11] Amy Lynnette, "Digital and Multimedia Forensics Justified," 29.

[12] Kramer, "Challenges of Electronic Taking of Evidence," 410.

understand what type of evidence can be found on any operating system (on computers as well as mobile devices) and what skills will be required to get it from the relevant device legally.

8.3.1 LAWYERS

Because of lack of awareness related to technological advancements, many advocates worldwide neither understand the basic working of technology, nor the way in which digital documents and data is managed. However, with the reliance of computer in business activities, many concerns were "raised about the lack of understanding among various legal practitioners and lawmakers for failing to address the problems brought about by the increasing reliance of digital evidence in legal proceedings."[13] By the turn of the century, various countries around the globe established special centers which finds solutions to the forensic issues faced by the legal fraternity.

Digital evidence and computer forensics are new additions in legal proceedings. Thus, it has caused "considerable and often controversial, discussion among legal professionals."[14] Therefore, lawyers and judges in Pakistan are not comfortable with technology, as the basic training have not been imparted to legal fraternity. Because of advancement of technology lawyers are required to offer appropriate advice and defend to their "clients in relation to the disclosure or discovery of data in electronic form. If lawyers fail in their duty to more fully understand the issues surrounding digital data, they may find themselves subject to actions for negligence."[15] Therefore, it can safely be concluded that lawyers are required to be familiar with digital forensic techniques to properly understand, help and defend their clients.

---

[13] Boddington, *Practical Digital Forensics*, 10.
[14] Mason and Seng, *Electronic Evidence*, 18.
[15] Ibid.

Digital evidence has some unique characteristics which were not present in paper-based evidence such as volatile nature of evidence, easy to alter and destroy. Moreover, this is in huge volume, which is another issue for lawyers. However, Social media is more problematic in digital evidence arena, therefore the lawyers should perform their "due diligence to investigate the media and hardware involved, the applications used to generate content and the indicia of reliability in the content itself."[16]

8.3.2 THE PROSECUTION AGENCY

Unfortunately, the prosecutors in Pakistan lack basic knowledge regarding digital evidence. In addition to this, they are unable to address privacy-related legal objections to digital evidence. This happens due to difficulties in understanding elements of digital evidence. Another issue is lack of coordination between the LEAs and prosecutors, thus, it burdening the prosecutors with a lot of data being most of the data irrelevant as only some data may be relevant on a device.

Digital evidence in criminal investigation may show "that a crime was committed from the defendant's computer, the prosecution may need to directly connect the defendant to that computer."[17] Whereas, defendant can be tied in several ways, including confession, circumstantial evidence, content analysis and corroboration of other evidence. There are several issues attached in digital evidence which are not found in paper-based evidence. Though, "the most obvious point is that the presentation of digital evidence requires familiarity with specialized, evolving, and sometimes complex technology."[18] Therefore, it is crucial for prosecutors to have some basic knowledge of the technical aspects of digital evidence, which will help them to present digital

---

[16] Kenneth N. Rashbaum, Matthew F. Knouff & Dominique Murray, "Admissibility of Non-U.S. Electronic Evidence," *Richmond Journal of Law & Technology* 18 (2012), 1-76 at 65.

[17] National Institute of Justice, *Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors,* 44.

[18] National Institute of Justice, *Digital Evidence in the Courtroom,* 44.

evidence in court proceedings. Meaning thereby, that professionals should equip themselves with technical expertise.

In some cases, prosecutions agency does not work hard in collecting or presenting digital evidence. Hence, their focus is to prove the defendant guilty irrespective of the legal requirements, which make the prosecution case weak. Therefore, in such cases "the defense should vigorously challenge the courts to require that the prosecution present all of the evidence gathered in the same form as it was made available to them and for a similar amount of time."[19]

In *Umair Ashraf v. the State*,[20] the SHC, held that "evidence which has been collected by the prosecution by way of modern device cannot be disallowed," and the SHC allowed to play the CD. In *Muhammad Sadiq v. the State,*[21] the LHC held that "Under the law evidence collected through modern devices is admissible in evidence and the same can be used against the accused during judicial proceedings to determine the questions of criminal liability or as the case may be." Therefore, the LHC on the basis of confession recorded by the police on CD upheld the conviction of the accused.

Under the PECA, FIA is authorized to investigate the cyber-crime. But, in practice, police is also investigating these crime. Due to lack of expertise by the police, many criminals are acquitted by the courts. Therefore, there is dire need that this aspect may also be considered by the concerned authorities.

---

[19] Johnson, *Forensic Computer Crime Investigation,* 156.
[20] *Umair Ashraf v. The State,* 2008 MLD 1442 (Karachi).
[21] *Muhammad Sadiq v. the State,* 2016 PCRLJ 1390.

8.3.3 JUDGES

The Pakistani judicial system has QSO to govern the evidence related issues, whereas some issues related to presentation and allied matters have been discussed in CPC and CrPC. However, courts in Pakistan are struggling (as digital evidence has not be addressed properly) to determine how to address the numerous issues of admissibility of digital evidence that arise when digital data is presented in the courts. Whereas, the widespread use of IT has created unprecedented challenges for the LEAs, prosecutors, judges and lawyers in legal proceedings. The legal fraternity and the judges in Pakistan hardly understand the scholarship that is presented by the expert witnesses, which can create disaster for the accused or prosecution for not understanding the basics of computer operations.

Digital evidence in courts is presented through experts. In the words of Marcella and Menendez:

> There are typically several tests, which the court may apply to determine relevancy, admissibility and reliability of an expert's testimony and methodologies and ultimately his or her opinion regarding the evidence in question. In cyber forensics, an effort by counsel to place into question the methods used by an investigator, to assail the reliability of the tools employed by the investigator, and to attempt to make suspect the investigator's competency, is generally referred to as a "junk science" attack.[22]

It has been observed that some judges are not much unfamiliar with technology, therefore, the lawyers do not assist the courts properly resulting in the challenging of integrity of evidence or acquittal of the accused. If data is created in other than Pakistan, then this also pose additional challenges for judges to adjudicate upon the case on the basis of said evidence. Nonetheless, the following issues are required to be adjudicated by the judge for accepting the evidence, such as what security measures were adopted for authenticity and reliability of the digital content?

[22] Marcella and Menendez, *Cyber Forensics*, 277-278.

Therefore, while deciding any matter judges must deliberate on the authenticity and trustworthiness of computerized data in the light of precedent and legislation. Another challenge is when digital data is voluminous, thus, verification of all items may not be possible.

Training of legal professionals without including the judicial officers is of no use. Hence, Judges must possess "a strong basic knowledge of computers, the Internet and cyber forensics. They must make decisions regarding probable cause in the issuance of search warrants and in preliminary hearings, the admissibility of cyber evidence, the appropriateness of expert testimony and many other significant legal issues."[23] This issue can also be handled by designation of special judges, in case there is limited capacity. Thus, it can safely be concluded that judges and lawyers both are required to have some basic understanding of forensic science and digital evidence.

8.4 Expert Witnesses

Regarding conventional evidence Boddington in this treatise said, that "evidence is blind and cannot speak for itself, so it needs an interpreter to explain what it does or might mean and why it is important to the case, among other things."[24] Same is the case in case of digital evidence, where expert witness is required to interpret the evidence.

In particular, in case of digital evidence, an investigator or forensic expert will collect and preserve the relevant digital information or data according to the law of evidence of the country.[25] The computer forensics expert has various responsibilities including identification, collection, preservation, examination, analysis, transportation and presentation of the digital data before the

[23] Marcella and Menendez, *Cyber Forensics*, 308.

[24] Boddington, *Practical Digital Forensics*, 14.

[25] In Pakistan, QSO, ETO, PPC, CrPc, PPC, and IFTA are relevant. In particular, PECA and QSO are very important in digital evidence.

courts. Nothing is easy in digital evidence from identification to presentation in court. Every investigator in investigation "plow through thousands of active files and fragments of deleted files to find just one that makes a case. Computer forensics has been described as looking for one needle in a mountain of needles."[26]

In any case, services of an individual having expertise in digital forensic will be required who will testify before the courts to explain what he did to the computer and its data during examination of digital evidence. Besides, the court may ask the expert about his education, level of training and experience. Therefore, the investigating agency should make sure the expert not only "has the expertise and experience, but also the ability to stand up to the scrutiny and pressure of cross-examination."[27] Further, it is also important for an expert to have "up-to-date knowledge and receives constant training, which are more important than experience in this field."[28] Furthermore, he should also be "knowledgeable in the law, particularly legal jurisdictions, court requirements, and the laws on admissible evidence and production."[29]

In USA, testimony of an expert has been discussed in Rule 702, which means that a computer expert under rule 702 must certify the validity, reliability and accuracy of the source of information, the computer process and the results. This can be shown by demonstrating that the computer was in proper working order, proper procedures were followed, equipment was functionally correct and reliable software was used. Hence, expert testimony before the court will be presented in the form of an opinion only.

---

[26] Vacca, *Computer Forensics: Computer Crime Scene Investigation*, 59.
[27] Ibid., 9.
[28] Mason and Seng, *Electronic Evidence*, 23-24.
[29] Vacca, *Computer Forensics: Computer Crime Scene Investigation*, 155.

However, generally expert witnesses' opinion is challenged by the opposing lawyer. The court should be sensitive in respect of expert testimony relating to digital evidence. Therefore, at least, the court should observe the *Daubert*[30] standards which were prescribed by the USA Supreme Court. Thereafter, *Daubert* standard is applied by the courts to expert witnesses and the court in *Kumho Tire v. Carmichael*,[31] extended the *Daubert* standard to experts with technical or specialized knowledge.

The U.S.A. Supreme Court prescribed various factors in *Daubert v. Merrell* which are to be used by the courts in appraising expert witness's testimony. However, these factors as discussed in this case are not limited and it may be possible that in certain circumstance some of these factors or all of them may not apply in a specific situation, but their significance cannot be ignored. The factors are as under:

i. Whether the theory or technique can be (and has been) tested.
ii. Whether the theory or technique has been subject to peer review and publication.
iii. The known or potential rate of error of the technique or theory used.
iv. The existence and maintenance of standards and controls
v. Whether the technique or theory has been generally accepted in the scientific community

In Pakistan, Article 59 of the QSO defines expert as under: -

> When the Court has to form an opinion upon a point of foreign law, or of science, or art, or as to identity of handwriting or finger impressions, [32][or as to authenticity and integrity of electronic documents made by or through an information system], the opinions upon that point of persons specially skilled in such foreign law, science or art, or in questions as to identity of handwriting or finger impressions [33][or as to the functioning, specifications, programming and operations of information systems, are relevant facts.]
>
> Such persons are called experts.

---

[30] *Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579 (1993).
[31] *Kumho Tire v. Carmichael,* 526 U.S. 137 (1999).
[32] Inserted by ETO.
[33] Subs., by ETO.

Besides, the Punjab Forensic Science Agency Act, 2007 defines expert as "expert includes a qualified foreign expert working in a forensic science facility and whose evidence is admissible in the country of his origin."[34] Whereas, the IFTA, 2013 defines experts as "expert means a person qualified or trained or experienced in conducting surveillance or interception who is nominated by the applicant or the federal Government as an expert for analysis of the intercepted material."[35] However, section 510 of the CrPC discuss the reports of experts but forensic expert is not mentioned there. Punjab Government has amended the said section to include the forensic expert. Therefore, it is a necessary, at federal level, to amend the section 510 of the CrPC to include the forensic expert as an expert witness. Whereas, in section 40 of PECA,[36] it is provided that Federal Government shall establish a forensic laboratory to provide expert opinion before the Court and in section 46 of the same Act, court is authorized to appoint *amicus curiae* or seek expert opinion on any matter.

In *Abdul Ghani v. the State,*[37] the SHC held that the report of expert is after all "an opinion which can be fallible and not immune from judicial scrutiny. The opinion of an expert is received in evidence because it either confirms or falsifies other evidence on record."

In *Arif Hashwani v. Sadruddin Hashwani,*[38] the SHC held that

> .....opinion of a forensic witnesses relating to authenticity or integrity of electronic document made, by or through any information system also made admissible from the Explanations 3 and 4 to Article 73 of the Qanun-e-Shahadat Order, 1984 relating to

[34] Section 2(f) of the Punjab Forensic Science Agency Act, 2007 (Act No. XIII of 2007). Experts are discussed in section 9 of this Act.

[35] Section 3(f) of the IFTA.

[36] **40. Forensic laboratory**. "The Federal Government shall establish or designate a forensic laboratory, independent of the investigation agency, to provide expert opinion before the Court or for the benefit of the investigation agency in relation to electronic evidence collected for purposes of investigation and prosecution of offences under this Act."

[37] *Abdul Ghani v. the State,* 2007 YLR 969.

[38] *Arif Hashwani v. Sadruddin Hashwani,* PLD 2007 Karachi, 448.

preliminary evidence, it is evident that printout or other form of reproduction of another electronic document be made admissible, in evidence as preliminary evidence.

In the *Land Acquisition Collector vs. Muhammad Sultan,* the SC held as under:

> The provisions of the Qanun-e-Shahadat Order, 1984 including Article 59 thereof make it clear that the opinion of a witness is only relevant and carries some probative value if he is an expert in the fields specified in the said Article. Furthermore, even for the purpose of giving an opinion, the witness has firstly to establish the expertise vested in him either on account of academic qualification or experience or otherwise. Without such foundation, an opinion cannot by itself, be taken as having evidentiary value for proving a fact in issue.[39]

In *Ahmad Omar Sheikh v. the State,*[40] the trial court convicted the appellants, *inter alia,* on the basis of expert report regarding IP address, emails and laptop recovery. However, the SHC on the basis of contradiction in evidence acquitted the appellants and the SC maintained the decision of SHC.[41]

8.5DIGITAL EVIDENCE IN THE COURTS

All over the world, the basic purpose of any court (either criminal, civil or any other special court) is to administer justice between the parties. Whereas, the role of investigators in investigation is to present supporting evidences enabling the courts to reach a just decision. Thus, the courts are depending on the credibility and reliability of the evidence presented by the prosecution (plaintiff in case of civil matter), especially in cyber-crime cases where the courts heavily rely on the "digital investigators and their ability to present technical evidence accurately; it is their duty to present findings in a clear, factual, and objective manner."[42] In addition, courts are more "concerned with the authenticity of the digital evidence they present."[43] The evidence

---

[39] *Land Acquisition Collector v. Muhammad Sultan,* PLD 2014 Supreme Court 696.

[40] *Ahmad Omar Sheikh v. the State*, 2021 YLR 1777. The Sindh Government challenged the decision of SHC in the Supreme Court of Pakistan, by filling three different appeals, which were dismissed by maintaining the SHC decision.

[41] *The State through P.G. Sindh v. Ahmed Omar Sheikh*, 2021 SCMR 873.

[42] Casey, *Digital Evidence and Computer Crime,* 49.

[43] Ibid.

presented by the experts must meet the criteria set out by the USA Supreme Court in *Daubert*[44] case and Supreme Court of Pakistan in *Ishtiaq Ahmad Mirza*[45] case.

Before admitting evidence, courts require certain requirements to be fulfilled. For example, court will ensure that every evidence which is presented before him "is relevant and will evaluate it to determine if that is what its proponent claims, if the evidence is hearsay, if it is unduly prejudicial, and if the original is required or a copy is sufficient."[46] In case of failure to consider these issues, the evidence may not be accepted and the same will be rejected according to law of evidence. Therefore, it is imperative for judges to acquire some basic technical skills to understand the basic processes and methods of digital forensic related to digital evidence collection and analysis.

The main purpose of evidence collection by the LEAs and the investigator is to present the accurate and authentic evidence before the court to prosecute the criminals. Therefore, without some technical competence, judges will not be able to properly understand the digital evidence process which is a key in successful adjudication. Further, LEAs aim must be "to further strengthen their communication channels with those in the justice system, as this can contribute to enhancing the understanding of digital evidence within the judiciary, thereby potentially also alleviating LEAs from unnecessarily burdensome analysis requests."[47]

The widespread use of ICT such as variety of operating systems and various digital devices the courts are "struggling to determine how to address the myriad of evidentiary issues that arise

---

[44] *Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579 (1993).
[45] *Ishtiaq Ahmad Mirza v. Federation of Pakistan*, 2019 PLD SC 675.
[46] Ibid.
[47] Biasiotti et al, *Handling and Exchanging Electronic Evidence across Europe*, 382.

when digital images and other computer-generated information is presented in court."[48] Further, it has also created "unprecedented challenges in legal proceedings as the courts decide how to properly authenticate digital information under the current judicial rules and procedures." While in conventional method used by the courts for establishing admissibility in Pakistani court is well-settled now. However, "their applicability to digital data and devices from which electronic evidence is generated raise complex issues and questions."[49] This has to be resolved in the light of latest developments.

While amending the QSO, it was specifically stated that these amendments shall apply to the extent of this Ordinance (Electronic Transactions Ordinance, 2002) but without reading of ETO, the provisions of ETO have been applied to every situation which is against the spirit of enactment. Section 29 of the ETO provides that "For the purposes of this Ordinance, the Qanun-e-Shahadat Order, 1984, (P.O. No. 10 of 1984) shall be read subject to the amendments specified in the Schedule to this Ordinance."[50] Therefore, it can easily be concluded that this modification to the QSO are just for the ETO and thus not applicable to any other proceedings. Then question arises why these amended were incorporated in QSO and applied to all laws? This issue has not been discussed or addressed anywhere in Pakistani legal system. The reason appears that actually section 29 of the ETO was ignored and applied to other laws, which need to be rectified or the ETO should be amended.

Production of computer and network related evidence is very difficult because of various legal and technical complications attached to these devices such as making of forensic image of

---

[48] https://www.crl.edu/sites/default/files/d6/attachments/pages/Thomson-E-evidence-report.pdf (accessed: 30th November, 2019).

[49] Ibid.

[50] Section 29 of the ETO.

the hard drive. However, collection of data "may be relatively easy to acquire in a small forensic examination but may be too difficult and too costly to gather for all custodians over time in a large e-discovery case."[51] Therefore, instead of requiring to produce the original digital device, courts generally accept the forensic examiner's report and decide the issue on the basis of said evidence.

8.6 How Courts Assess the Evidence

Even in the developed countries, the judges, lawyers and prosecutors have little knowledge about the technology, particularly digital forensics. Then how can we expect that the legal fraternity in Pakistan will be having some expertise in the technology related issues?

Digital evidence is often challenged in court, *inter alia*, on the basis of lack of proper legislation on the subject. However, some judges accept it without questioning, whereas other ask a lot before accepting this type of evidence due to technicalities attached to it. In almost, every Pakistani case in which digital evidence has been discussed, it has not properly been examiner by the Pakistani courts. However, in *Ishtiaq Ahmad Mirza v. Federation of Pakistan*,[52] the honorable Supreme Court of Pakistan has provided some guidelines about acceptance of digital evidence. In particular, with respect to how video is to be established as a genuine piece of evidence, the court observed as under:

> With the advancement of science and technology it is now possible to get a forensic examination, audit or test conducted through an appropriate laboratory so as to get it ascertained as to whether an audio tape or a video is genuine or not and such examination, audit or test can also reasonably establish if such audio tape or video has been edited, doctored or tampered with or not.....The advancement of science and technology has now made it very convenient and easy to edit, doctor, superimpose or photoshop a voice or picture in an audio tape or video and, therefore, without a forensic examination, audit or test of an audio tape or video it is becoming more and more unsafe to rely upon the same as a piece of evidence in a court of law.

---

[51] Casey, *Handbook of Digital Forensics and Investigation*, 72.

[52] *Ishtiaq Ahmad Mirza v. Federation of Pakistan*, 2019 PLD SC 675.

Almost in every case there is some type of digital evidence either computer, email, cell phone or the internet. Therefore, everywhere courts have recognized "that with the pervasiveness and increasing significance of digital evidence, there is a concomitant increase of risk of evidence being tampered with. Many courts recognize that digital evidence presents more complicated variations of the authentication problem than do paper documents."[53] As discussed earlier, that digital evidence is not like other types of evidence which has been discussed since long in courts, but in case of digital evidence, however, by the judges "some forensic expertise may be required to verify that the evidence is trustworthy."[54] Otherwise, untrustworthy will be considered inadmissible in legal proceedings which may be detrimental to parties. Thus, courts dealing with the matter of digital evidence needs "to satisfy themselves as to the reliability of the evidence and the integrity of the forensic processes and tools used to procure, secure, and analyze the evidence throughout the entire forensic process."[55]

Failure to authentic digital evidence or any other reason, the presiding officer must apply his mind in the circumstance. In *Lorraine v. Markel*, the Judge Grimm observed that "the inability to get evidence admitted because of a failure to authenticate it almost always is a self-inflicted injury which can be avoided by thoughtful advance preparation."[56]

In court proceedings, while discussing "the admission of evidence from devices controlled by software code, judges do not distinguish between a single, highly specialist device that is self-contained, and a linked network containing any number of devices each independently operating on its own set of software code."[57] Therefore, it is very useful for Pakistani judiciary to consider

---

[53] Boddington, *Practical Digital Forensics,* 86.
[54] Ibid.
[55] Ibid., 91.
[56] *Lorraine v. Markel American Insurance Co.,* 241 F.R.D. 534 (D. Md. 2007).
[57] Mason and Seng, *Electronic Evidence*, 113.

the case law of USA where such media has been analyzed by the courts. In the light of USA case law, Pakistani case law on the subject has been also discussed, where the latest techniques and technology has been examined.

Under the ETO, digital (electronic) evidence has been made admissible. However, in perspective of Pakistani legal system, how far the computer expert's evidence meets the criteria prescribed by the QSO to prove the guilt of a wrong doer? Besides, the lack of proper chain of custody may also compromise the legal stance. As the digital evidence may be easily changed, modified and altered, therefore, the courts adopt extra restraint that the digital evidence has not been changed, modified or altered.

At the time of enactment of QSO, hardly few people were using ICTs and no one was aware that what the outcome will be of modern devices. Thus, we cannot safely say that the drafter of the QSO were aware of modern day digital devices.[58] Hence, we can conclude that the existing digital devices were not covered under the Article 164 of QSO, which provided that "*the Court may allow to be produced any evidence that may have become available because of modern devices or techniques.*"[59] Because of this Article the courts allowed to produce evidence through modern devices but almost we see that Audio/Video cassette were produced and courts decided many case on the basis of this evidence and observed that statement recorded through audio cassette would be additional circumstance to lend support to assertions.[60] However, SHC in *Qurban Ali v. the State*, held that "the conversation in the audio cassettes cannot be safely relied upon unless the voices are identified by the, concerned persons."[61] In *Hakim Ali Bhatti v. Abdul*

[58] Hard Disk, C.D, D.V.D, Internet, Mobile and USB etc.
[59] Article 164 of the QSO. {Emphasized added}.
[60] *Khanzada Inamulah Khan v. Mst. Zakia Qutab*, PLD 1998 Peshawar 52.
[61] *Qurban Ali v. The State*, 2007 PCr L J 675 Karachi.

Hakim,[62] the election tribunal rejected the tape recorded evidence as the same was not prepared under the independent supervisor and control, however, in the *Arif Hashwani v. Sadruddin Hashwani*, the SHC held that tape recorded cassettes are admissible piece of evidence, but while accepting the same, extra care is to be taken to declare and satisfy that the voice of the alleged, and there is no tampering with the recorded statement.[63] Whether there was any tempering, whether voice recoded in the cassette is the voice of defended/responded and whether there was any editing in the conversion can be decided by the court.[64] In *Dr. Mobashir Hassan v. Federation of Pakistan*,[65] it was held by the Supreme Court that the reports of electronic and print media are relevant. In *Kh. Ijaz Ahmad v. D.R.O*, the LHC held that neither the person who produced the video had recorded the video nor any affidavit of the person was produced, therefore, the video/film was not a legal piece of evidence and not accepted in evidence. In *Ali Naqi v. Government of the Punjab*,[66] the termination of services of the accused was upheld on the basis of making of video of female patient in the operation theater.

In *Muhammad Nasir v. Mahmood Shaukat Bhatti*[67] case the LHC held that "computer technically is a modern technique and is well within the ambit of" Article 164 of the QSO. Same view was also affirmed by the Election Tribunal Balochistan in *Muhammad Akram Baloch v. Akbar Askani.*[68]Further, the tribunal observed that: -

> Similarly, electronic records mean, data, record or data generated, image or sound stored, received or sent in an electronic form or microfilms or computer generated microfiche.

---

[62] *Hakim Ali Bhatti v. Abdul Hakim*, 1986 CLC 1784.

[63] *Arif Hashwani v. Sadruddin Hashwani*, PLD 2007 Karachi 448. Earlier in *Saifur Rehman Khan v. Shahab ud Din*, 1995 MLD 1485, the LHC, allowed the production of audio-cassette in evidence.

[64] Ibid.

[65] *Dr. Mobashir Hassan v. Federation of Pakistan*, PLD 2010 SC 265.

[66] *Ali Naqi v. Government of the Punjab*, 2019 PLC (C.S.) 952 Lahore.

[67] *Muhammad Nasir v. Mahmood Shaukat Bhatti*, PLD 2003 Lahore 231.

[68] *Muhammad Akram Baloch v. Akbar Askani*, 2014 CLC 878, the tribunal held that "Computer technology being a modern device is well within the ambit of Article 164 of the Order of 1984."

> Thus, an electronic record can safely be considered as a document, because matter is recorded on the computer as bits and bytes, which are the digital equivalent of figures or marks, therefore, any document produced by a computer can be produced as evidence so long as it could be shown that the computer was functioning properly and was not misused.

In *Mst. Marium Haji v. Mrs. Yasmin R. Minhas,* the SHC held as under: -

> In so far as the photographs are concerned....learned counsel for plaintiffs was specifically asked as to how photographs could be exhibited and made part of evidence as the defendant did not have an opportunity or there was no occasion for him to cross-examine the witness with regard to the genuineness of the photographs. She was not able to give any explanation worth consideration. Even no explanation was forthcoming as to how the case of the plaintiffs, could be proved on the basis of photographs sought to be produced in evidence. Learned counsel for plaintiffs has specifically relied upon the England Case to argue that the photographs could be admissible-in-evidence. The photographs may have been admissible in evidence, subject, however, it was proved through witness that the prints are taken from the negatives that are untouched as has been observed in the very authority relied upon by the learned counsel for plaintiffs. The fact which cannot be lost sight of, is, that this authority relates to the year 1965, and, now technology has so immensely advanced, that the photographs or even Video tapes can be manipulated and maneuvered. .....unless it is proved that the photographs are not manipulated, these could not be allowed to be produced in evidence.[69]

In *Umair Ashraf v. the State,*[70] the SHC allowed the production of C.D in a criminal proceeding. In *Rehmat Shah Afridi v. The State,*[71] it was held that the tape-recorded conversion is real evidence and can be accepted in the court proceedings. *In Sikandar Ali Lashari v. the State,*[72] the court allowed to provide USB and CD to the accused. Nowadays, CCTV cameras are installed everywhere and same is being used by the investigating agency to prove or disprove a fact. Mason has discussed about CCTV cameras in the following words:

> Surveillance cameras are very much part of life in the twenty-first century, ever since the foundations of their use were laid in the latter decades of the twentieth century. Evidence of images from security cameras can be very helpful in identifying the perpetrators of crimes. Such evidence has been admitted in English courts, mainly in criminal cases.[73]

---

[69] *Mst. Marium Haji v. Mrs. Yasmin R. Minhas*, PLD 2003 Karachi 148.
[70] *Umair Ashraf v. The State,* 2008 MLD 1442.
[71] *Rehmat Shah Afridi v. The State*, PLD 2004 Lahore 829.
[72] *Sikandar Ali Lashari v. the State,* 2016 YLR 62 (Sindh).
[73] Mason and Seng, *Electronic Evidence*, 61.

The SHC in *Ammar Yasir Ali v. the State*,[74] held that: -

> However, mere producing CCTV video as piece of evidence and its watching in open court is not sufficient to be relied upon unless and until corroborated and proved to be genuine. As a proof of genuineness of such CCTV video, it was incumbent upon the prosecution to examine the person who recorded the video to testify the same, which requirement the prosecution has failed to fulfill even failed to point out the source of providing the CCTV video, the Investigating Officer who received the CCTV video in his evidence has categorically stated that during investigation he received CCTV movie from a person who did not want to disclose his name or identity being a man of some surveillance. During cross-examination he has further admitted that nothing was visible and identifiable in the video as such the CCTV is not reliable piece of evidence.

In *Asfandyar v. Kamran*,[75] the SC held that: -

> Mere producing any footage of C.C.T.V. as a piece of evidence in the Court is not sufficient to be relied upon unless and until the same is proved to be genuine. In order to prove the genuineness of such footage it is incumbent upon the defence or prosecution to examine the person who prepared such footage from the C.C.T.V system.

In *United States v. Brooks*,[76] the US 8th Circuit Court upheld the conviction of the accused on the basis of GPS evidence and CCTV footage. In *United States v. Wiest*,[77] the court convicted on the basis of surveillance tapes. In *Government of Sindh v. Fahad Naseem*[78] the SHC directed the prosecution agency to provide video cassette to the defendants or his counsels as the video cassette is accepted in evidence. Similarly, in *Nazim Ali vs. Additional Sessions Judge*,[79] the LHC directed prosecution agency to provide memory card to the accused.

In *Dolan v. State*,[80] the court upheld the conviction on the basis of video tape footage and observed as:

---

[74] *Ammar Yasir Ali v. The State*, 2013 PCRLJ 783. In *Babar Ahmad v. The State*, 2017 YLR 153, the Gilgit-Baltistan Chief Court, accepted CCTV footage in evidence.

[75] *Asfandyar v. Kamran*, 2016 SCMR 2084.

[76] *United States v. Brooks*, 715 F.3d 1069 (8th Cir.2013). The court affirmed the district court's judicial notice of data from "a GPS tracker that a teller placed in an envelope of stolen money during a bank robbery."

[77] *United States v. Wiest*, 596 F.3d 906 (8th Cir.2010).

[78] *Government of Sindh v. Fahad Naseem*, 2002 PCRLJ 1765 Karachi.

[79] *Nazim Ali v. Additional Sessions Judge*, 2016 MLD 25.

[80] *Dolan v. State of Florida* 743 So.2d 544 (1999).

> Once the tape is authenticated and the forensic analyst explains the computer enhancement process and establishes that the images were not altered or edited, then the computer enhancements become admissible as a fair and accurate replicate of what is on the tape, provided the original tape is in evidence for comparison.

The LHC (Rawalpindi Bench) in *Hashim Jamal v. the State,*[81] refused bail of the accused on the basis of forensic evidence collected from cell phone handset. In *Junaid Arshad v. the State,*[82] the court also refused bail on the basis of evidence collected from cell phone and IP address.

In *Zakir Hussain v. the State,*[83] the Chief Court of Gilgit-Baltistan, upheld the conviction of the accused on the basis of confection recorded on CD.[84] As in this case, the CD was played in the trial court, and the trial court observed in the order that the narration of occurrence by the accused was natural, and the same was neither shattered in cross-examination nor its admissibility was challenged. In *Muhammad Jawad Hamid v. Muhammad Nawaz Sharif,*[85] the LHC held that video recording statements of accused had to be proved by its author and creator. In *Shahid Zafar v. the State,*[86] the court accepted the DVD cassette/video recording, produced in trial court as admissible evidence.

The SHC in *Government of Sindh v. Fahad Naseem,* held that "There can be no two opinions on the point that a still photograph is a document, I, therefore, do not find any reason to exclude the movie film, which is also a photograph, from the purview of "document"[87]In

---

[81] *Hashim Jamal v. the State,* 2018 YLR Note 105.

[82] *Junaid Arshad v. the State,* 2018 PCrLJ 739 (Lahore).

[83] *Zakir Hussain v. The State*, 2017 PCrLJ 757. The same view was taken by the LHC in *Muhammad Sadiq v. State,* 2016 PCrLJ 1390, in which the LHC held that evidence recorded on CD is admissible in criminal cases.

[84] The SC of Pakistan also upheld the conviction on the basis of CD in *Shahid Zafar v. the State*, PLD 2014 SC 809.

[85] *Muhammad Jawad Hamid v. Muhammad Nawaz Sharif,* 2019 PCrLJ 665 (Lahore).

[86] *Shahid Zafar v. the State,* 2015 PCrLJ 628 (Sindh).

[87] *Government of Sindh v. Fahad Naseem,* 2002 PCRLJ 1765 Karachi.

Muhammad Irfan v. The State,[88] the LHC accepted the evidence on mobile phone memory card and upheld the conviction of the accused.

The SC in *Ali Raza v. the State*,[89] held as under:

> Article 164 of the Order *ibid* invests the Court with wide powers to make use of evidence generated by modern devices and techniques; Articles 46-A and 78-A of the Order ibid as well as provisions of Electronic Transactions Ordinance (LI of 2002) have smoothened the procedure to receive such evidence, subject to restrictions/limitations provided therein.

The SC has taken an exhaustive survey of jurisprudence on the subject of digital evidence in the case of *Ishtiaq Ahmed Mirza v. Federation of Pakistan*[90] and authoritatively settled parameters to receive forensic evidence through modern devices and techniques. These are discussed below.

For relying upon any audio or video recording by the court, it is necessary to prove before the court that the said audio or video is genuine and not tempered, if the said audio or video is examined by the forensic analyst, the report of forensic analyst of forensic agency will admissible in evidence. However, for relying upon such report, it is the discretion of the court to accept or reject the said evidence, if accepted that needs to be proved in accordance with settled law of Pakistan. Thereafter, the source of audio or video becoming available along with the date of acquiring of the said audio or video tape is to be disclosed by the person producing the audio or video. The person desiring to produce the audio or video tape has to make an application before the court for bringing on the record, however, if the audio or video tape is produced at a later stage, then the same may be looked with suspicion.

---

[88] *Muhammad Irfan v. The State*, 2018 PCRLJ 1319.

[89] *Ali Raza v. the State,* 2019 SCMR 1982.

[90] *Ishtiaq Ahmed Mirza v. Federation of Pakistan,* PLD 2019 SC 675.

To prove the accuracy of the audio or video recording other evidence must be provided to rule out any possibility of tampering with the video. In addition to this, the said video must be actual recording of the conversation of any event and the person recording the video has to be produced before the court to produce the said recording himself in the court which same must be played before the court and person recording the conversation must identity the voice of the person speaking or the person seen in the video, however, the video produced before the court should be clearly audible or viewable. Besides, any other person presents at the time of making any video may also testify about the event. Moreover, the person shown in the video must be properly identified.

The evidence produced through audio or video recording must be admissible and relevant to the controversy. Proper chain custody of the said evidence i.e. safe custody of the evidence after its preparation till its production before the court must be proved. If the transcript of the audio or video is prepared then the same must be prepared under the independent supervision and control.

Further, in the *Ishtiaq Ahmed Mirza v. Federation of Pakistan* case, the SC held that:

> The person recording an audio tape or video may be a person whose part of routine duties is recording of an audio tape or video and he should not be a person who has recorded the audio tape or video for the purpose of laying a trap to procure evidence.[91]

With respect to the use of digital information in evidence on CD, DVD, USB or other device such as audio or video, these are very important aspects of any digital data which need to be examined by the judge. In Pakistani jurisprudence nothing has been discussed about these things. Here some questioned are raised about the video, *mutatis mutandis*, these can be asked about any digital evidence.

---

[91] *Ishtiaq Ahmed Mirza v. Federation of Pakistan,* PLD 2019 SC 675.

i. Who created or recorded the video?

ii. Who copied the video?

iii. What is the date, time and place of recording of the video?

iv. How it was maintained?

v. Whether proper chain of custody is maintained?

vi. In case of CCTV, character of the person who operate the system

vii. Whether the metadata is intact? If so, whether the same is original or altered?

viii. What devices (i.e. cell phone, digital camera or any other) were used to create the video?

ix. Whether the video remained in safe custody?

x. What is the security control procedure?

xi. If video is posted on social networking website, who posted them? What is the source of video?

xii. Who can testify about accuracy of the video? What will be the procedure of authentication?

xiii. Whether by the forensic expert any analysis was done?

xiv. Whether the law will accept it primary or secondary evidence?

xv. Whether the video was encrypted or not?

Digital Evidence has not been discussed as such in Pakistani courts. Just, few things have been discussed which are of initial stage. There is a dire need to examine digital evidence in every case on the basis of above raised questions.

8.7 THE CONCEPT OF E-COURTS IN PAKISTAN

In May 2019, the Supreme Court of Pakistan, first time in Pakistani legal history started the hearing of appeal through video conferencing. In Pakistan, no such example exists before May, 2019. However, electronic trials have not been introduced yet. Although, trial courts have stared

installing computer equipment in courtrooms. When courts are fully equipped with latest digital device which enables the courts to proceed with online trial, this will save valuable time and resources occurred on trials reducing the burden on courts and making easy for the litigants to easy justice at the earliest.

In an electronic trial documents are "available electronically via online systems, directly to the court, and where the documents themselves can be displayed electronically to those in the courtroom."[92] There are many benefits of electronic trials which are not available in manual trials such as "they can save an inordinate amount of time as the lawyers involved in the hearing do not have to spend time finding each individual page being referred during the hearing, as the document is available on screen within seconds of counsel referring to the document identifier."[93]

Moreover, benefits of electronic trials in small and complex matters are same, such as "they result in the display of documents much more quickly, allowing those present in the courtroom to view the documents quickly and easily, without the need for each party to go to cumbersome hard copies and wait for everyone else to be on the same page."[94] Hence, a very short time is consumed by the courts as compared to conventional system. Whatever the matter is, the end result will be "the more efficient use of technology to enable documents to be accessed quickly and easily, with cost savings to the litigant."[95] Any case can be tried electronically especially terrorism case must be tried by the trial court using computer and the internet enabling the safety of prosecution witness, lawyers and judges alike. In Pakistan like country, electronic trial will save a lot of budget.

---

[92] Stanfield, "The Authentication of Electronic Evidence," 181.
[93] Ibid.
[94] Ibid., 183.
[95] Ibid., 184.

The Constitution in Pakistan provides that "the state shall ensure inexpensive and expeditious justice."[96] For fulfillment of constitutional obligations various concrete steps have been taken by the Government and Judiciary, in Pakistan, to provide speedy and inexpensive justice to the people, *inter alia*, is e-courts introduced by the SC, to hear cases and appeals from its registries through video links.

On 27th May 2019, in the judicial history of Pakistan first time the SC connected through by using latest technology systems to its registries and decided various appeals while facilitating the speedy disposal of outstanding legal matters.[97] This system, if continued successfully, will benefit the legal fraternity as well as the litigants by making judicial system more responsive to the needs of Pakistani people in redressing their grievances, and will save the precious time and reduce the burden on the litigants.

8.8 RECORDING OF EVIDENCE THROUGH VIDEO CONFERENCING

In conventional evidence recording procedures, presence of witness was must in the court. However, with the use of technology this requirement can be relaxed to accommodate the witness traveling from far flung areas where some time in various situations the evidence of the witness is not recorded and the witness faces embracement and hardship besides spending huge money on boarding and lodging. Generally, video conferencing is used when witnesses are unable to travel. In other words, video conferencing "will be available for those witnesses who are unable to travel

[96] Article 37 (d) of the Constitution of Pakistan, 1973.

[97] https://www.dawn.com/news/1484248 (accessed: 6th October, 2019); https://www.thenews.com.pk/latest/475315-pakistans-supreme-court-to-start-e-court-system-from-monday (accessed: 6th October, 2019); https://www.thenews.com.pk/latest/477081-e-court-system-successfully-launched-in-supreme-court (accessed: 6th October, 2019).

long distances and are able to appear remotely, and the use of streaming video across the internet means cost effective video is much more accessible."[98]

The SC of Pakistan in *Watan Party v. Federation of Pakistan*[99] appointed a commission and directed to record evidence through video conferencing. This issue has been discussed in Indian jurisprudence in detail. In *Amitabh Bagchi cs. Ena Bagchi*[100] the court held that the physical presence of person in Court may not be required for purpose of adducing evidence and the same can be done through medium like video conferencing. Similarly, in *State of Maharashtra vs. Dr Praful B Desai*[101] the Supreme Court of India observed that video conferencing is an advancement of science and technology which permits seeing, hearing and talking with someone who is not physically present with the same facility and ease as if they were physically present. The legal requirement for the presence of the witness does not mean actual physical presence. Thus, the court allowed examination of witnesses through video conferencing.

In *Aijazur Rehman v. the State*,[102] the SHC held as under: -

> Because of modern devices and technologies the trials through video conferences are growing fast which are not only advancing the cause of justice but catering various problems such as production of accused in Court, recording of evidence of witnesses from far a place, so on and so forth. The evidence of witnesses can also be recorded through video conference while the accused remains in jail.

Further, the SHC held in the same *Aijazur Rehman v. the State*,[103] case that:

> It is pointed out that if the procedure of video conferences is enforced then the problems faced by the Government, accused persons, particularly women and juvenile prisoners can be solved to a greater extent. It is not out of place to mention here that one of the causes of delay in disposal of the cases is non-production of the accused from jail to the Court. The situation is more grave in the cases of women accused and juvenile offenders. If the

---

[98] Stanfield, "The Authentication of Electronic Evidence," 184.
[99] *Watan Party v. Federation of Pakistan*, PLD 2012 SC 292.
[100] *Amitabh Bagchi s. Ena Bagchi* (AIR 2005 Cal 11).
[101] *State of Maharashtra v. Dr Praful B Desai* (AIR 2003 SC 2053).
[102] *Aijazur Rehman v. the State*, PLD 2006 Karachi 629.
[103] Ibid.

> procedure of video conferences is applied then the case of dangerous criminals can very well be tried without taking them out from the jail involving security risk. Not only the Government will be benefited but the accused and the society will also get benefit from such procedure. Therefore, the Government should actively consider to introduce video conferences facilities in the jail and the courts and to provide infrastructure at the relevant places.

Furthermore, it was held n *Aijazur Rehman v. the State*,[104] as under: -

> Thus, the law permits the trial through video conferences. It is further pointed out that if any party wants to record evidence through video conferences and if the Government has not provided such facility then the party after bearing the expenses of such facility can requests the Court for such trial. It is emphasized that the Courts should encourage such practice keeping in view the facts and circumstances of each case so that all the Courts of Pakistan should stand equal with the Courts of developed countries.

In a recent decision of the IHC in *Muhammad Nawaz Sharif v. the State*,[105] the court upheld the decision of the trial court for recording of evidence through video link. The relevant portion of the order of the trial court is as under:

> Statements of above said two witness shall be recorded through video link. Witness shall remain present in office of the High Court London. High Commissioner of Pakistan there shall ensure that the witness are not under any pressure, coercion or influence at relevant time, and their identity shall also be verified by him.

Thus, the evidence was record through video conferencing. Similarly, evidence through video conferring was also recorded in Imran Farooq murder case by the Anti-Terrorism Court, Islamabad as discussed earlier.

In the province of Punjab, the government amended[106] the Family Court Act, 1964 to provide for recording of evidence through video recording in family cases. The same is reproduced below:

---

[104] Ibid.

[105] *Muhammad Nawaz Sharif v. the State,* PLD 2018 Islamabad 148.

[106] Sub-section (1A) inserted by the Punjab Family Courts (Amendment) Act, 2015 (Act XI of 2015).

> The Family Court shall record or cause to be recorded, the substance of the statement of a witness or may record or cause to be recorded, the statement of a witness through audio or video recording.[107]

Since the introduction of this section, evidence can be recorded through video conferencing. One family court ordered the recording of evidence through video link/skype but the same was challenged in the LHC in the case of *Salman Ahmad Khan v. Judge Family Court*[108] through writ petition but the LHC upheld the decision of family court on the ground that section 11 (1A) provides for recording of evidence through this mechanism.

Similarly, the Government of Punjab introduced another law in 2018 in the province of Punjab for recording of evidence through video link which says that "the court may examine a witness through video link."[109] However, this law is specific to few situations such as sexual offence, terrorism, and serious offences.

In a recent case of *Muhammad Arif Chaudhry v. Muhammad Suleman*[110] the two-member bench of the SC proposed the following for hearing of cases through video conferencing.

(i) Each Courtroom/Bench to be provided with a wifi connected cell phone and number of the cell phone be mentioned in the cause lists and on the web site of the Supreme Court;

(ii) Applications such as Skype, WhatsApp, Telegram or any other suitable video conferencing platform be installed in the said Supreme Court cell phone and counsel be asked to install the same application in their cell phones;

(iii) After the identity of counsel is verified, cases may also be heard by use of the said video conferencing application;

(iv) To maintain transparency and openness, the screen of the court cell phone be mirrored on the television sets already installed in every courtroom;

---

[107] Section 11 (1A) of the Family Courts Act, 1964 (Act XXV of 1964).

[108] *Salman Ahmad Khan v. Judge Family Court,* PLD 2017 Lahore 698.

[109] Section 10 of the Punjab Witness Protection Act, 2018 (Act XXI of 2018).

[110] *Muhammad Arif Chaudhry v. Muhammad Suleman*, Civil Petition No. 1945 of 2018. This order was passed by the two member bench (Mr. Justice Qazi Faez Isa and Mr. Justice Sardar Tariq Masood) of the Supreme Court of Pakistan on 16.04.2020.

(v) The possibility of preserving the recording of court proceeding (say for six months) be explored; and

(vi) The Supreme Court IT Wing be assigned this task however before using the proposed system the IT Wing should ensure successful trial runs and the Pakistan Bar Council, the Supreme Court Bar Association, offices of the Attorney-General for Pakistan, the Advocate-Generals and the Prosecutor-Generals be given a demonstration of the workability of the proposed system and to consider their suggestions.

However, this is yet to be decided by the Chief Justice that whether this proposal is feasible or not. This is effective mechanism for adjudication of cases in any emergency situation.

Therefore, it can safely be concluded that recording evidence through video conferencing is blessing which can be utilized to save resource and expedite the process of conclusion of trial.

8.9 SUMMARY

The presentation of evidence is last stage in investigation. In Digital evidence instead of presenting original object, the print out or the expert report is presented in court proceedings. Thus, it is necessary that the expert must be having some basic education, skill and training in digital forensic. Besides, judges, lawyers and prosecution should also be having some basic understanding of digital forensic to examine, scrutinize and present digital evidence in proper admissible way. Failing to understand digital forensic by the professionals may lead to wrong conviction or acquittal of the accused. Moreover, the criminal procedure code does not include forensic expert in the category of experts which is a legal lacuna, therefore, there is a dire need to be amend section 510 of the CrPC to include the forensic expert and remove the said lacuna.

The world is moving too fast and have adopted various technique to expedite the trial process. Thus, have adopted video conferencing method for trial as well as for appeal. Although, the Supreme Court of Pakistan has adopted this method for appeal, which is not sufficient. This

should be extended to all the High Courts and same should also be used for trial purposes, which will save time and resources of the government as well as litigants.

CHAPTER NINE:

CONCLUSION AND RECOMMENDATIONS

CONCLUSION

Objective of this research was to suggest enhancement in the legal framework of Pakistan. Therefore, the USA jurisprudence was studied to get help from the USA legal system particularly digital evidence. Currently, in Pakistani legal system there is no comprehensive legal framework which deal with this issue. However, a patchwork of legislation has been implemented by enacting different instrument of legislation such as ETO, IFTA and PECA. More specifically, Pakistani existing legislation does not address the specific features of digital evidence, which is a serious issue in quickly evolving technologies.

In Pakistan, the application of general rules of evidence by the investigator is not sufficient in the identification, collection, preservation, transportation of digital evidence due to its specific nature. Therefore, a legal framework should provide clear and precise legal definitions, concepts and standards and protection of privacy.

Besides, there is lack of specific investigation measure and methods, which need to be addressed for digital evidence collection, such as search and search of digital evidence and privacy. In digital data, privacy is a serious risk, which need to be protected by the LEAs. Thus, a clear and specific method should be prescribed for collection of digital evidence. While legislating on the issue, rule of law and respect for fundamental rights must be adhered and these methods or techniques should be amended from time to time to accommodate new emerging technologies.

Handling of digital evidence is another issue in Pakistan. In every case, the investigators apply physical evidence rules, in many circumstances, these are not capable of handling digital evidence. Therefore, either a distinction is made between the both or new law related to handing of digital evidence be introduced.

Thereafter, comes the stage of digital evidence preservation. This aspect is also ignored in Pakistani legal system. Such as that how the digital evidence will be preserved and stored? Therefore, the legislature must legislate on the preservation, storage, transportation aspects of digital evidence. Besides, for the protection of digital evidence from alteration and contamination security measure and safeguards may also be provided.

Another major challenge for investigators in Pakistan is cloud computing. There is no rule which deals with the investigation of cloud system. Therefore, it is important for Pakistani legal framework to include specific provisions related to cloud service. This issue can cause problems with respect to international cooperation.

The internet is a gold mine of information, many people are using internet for various purposes including illegitimate activities. Everybody who use the internet, also use the email and social networking sites, where he shares his thoughts, ideas, photos, video and location. These can help the investigator in any investigation. But the crucial point is that it cannot be certain that the device was used by the actual person as the email and webpages can be forged besides using spoofing techniques. The presentation of evidence is last stage in investigation. In Digital evidence instead of presenting original object, the print out or the expert report is presented in court proceedings. Thus, it is necessary that the expert must be having some basic education, skill and training in digital forensic. Besides, judges, lawyers and prosecution should also be having some

basic understanding of digital forensic to examine, scrutinize and present digital evidence in proper admissible way. Failing to understand digital forensic by the professionals may lead to wrong conviction or acquittal of the accused. Moreover, the criminal procedure code does not include forensic expert in the category of expert which need to be amended to include the forensic expert and remove the lacuna.

The world is moving too fast and have adopted various technique to expedite the trial process. Hence, have adopted video conferencing method for trial as well as for appeal. Although, the Supreme Court of Pakistan has adopted this method for appeal, which is not sufficient. This should be extended to all the High Courts and same should also be used for trial purposes, which will save time and resources of the government as well as litigants.

In Pakistan, legislation on the cyber-crime particularly the digital evidence is not keeping pace with the advancement of ICT. Thus, it is the demand of the emerging regime to bring it with the requirement of the 21st Century.

RECOMMENDATIONS

Law:

- Law on digital evidence may be enacted to cover legal aspects of digital evidence in particular process of evidence recovery, collection, storage, packing, preservation, transportation, examination and presentation to be regulated in conformity with international best practices.
- All laws related to cyber-crime, cyber-space and computer evidence should be updated and revised after every few years to ensure that they are suitable and effective for the new situations.

- Under PECA, only FIA is authorized to investigate the crimes under this Act, therefore, as per law, other agencies do not have any authorization to collect the evidence and conduct investigation. Keeping in view the sensitive nature of digital evidence, this authorization should also be extended to other LEAs including Police.
- The Code of Civil Procedure, 1908, in particular section 2 for inclusion of definitions of e-filling, e-notices, e-summons, e-hearing, r-records, e-evidence be amended. Besides amending section 27, section 28, section 31, section 128, section 129, section 131, section 142, section 143 and Order III, Rules 1,3,5,6; Order IV, Rules 1 and 2; Order IX; Order X; Order XII, Rules 14, 16; Order 12, Rule 8; Order XVI, Rule 8; Order XXIV; Order XXVI; Order XXVII; Order XXIX; Order XXX; Order XXVII; XXXIX; Order XLV; Order XLVI and Order XLVIII.
- The Code of Criminal Procedure 1898, in particular section 4 for inclusion of definitions related to online proceedings, sections 16, 68, 69, 70, 71, 72, 73, 74, 75, 94 and more importantly section 510 of the CrPC should be amended to include forensic expert in the category of experts.
- Procedures for issuance of search-warrants in case of cyber-crime needs to be changed to protect the privacy of individuals.
- Legislation on encryption and metadata is necessary to safeguard the privacy of Pakistani people.
- QSO may be amended either partly or as a whole and at least a new chapter regarding digital evidence may be inserted. In particular, section 2, 30, 46-A, 59, 73, 74, 78-A and 164 of the QSO be amended.

- Section 29 of the ETO be amended to apply, the QSO, to all the situations as existing section 29 is only meant to the extent of ETO not whole QSO.
- Supreme Court Rules 1980 and High Court Rules should also be amended to make space for online court proceedings.
- Before a witness is examined in the court, in relation to recording of evidence through video link or video conferencing, witness testifying before should be required to file an affidavit or give an undertaking duly verified by the High Commissioner (in case witness is in abroad), or a Judge that this person is same person who is deposing on the screen. In other words that an identification affidavit should be introduced and the same may be provided to the opposite counsel. After recording the evidence of the deponent/witness, the same should be sent to the witness and his signature must be obtained on that evidence.

Education:

- LEAs personal should be trained in forensic science and law equally to be able to handle digital evidence.
- LEAs should have qualified personal who must having specialized education, knowledge, advanced skills, training, relevant experience in handling digital evidence and electronic media. Personal other than qualified may not be allowed to touch the digital evidence.
- Digital evidence must only be examined by the trained computer forensic professional specifically trained for the purpose.
- Prosecutors, lawyers and judges may also be trained and basic training may be imparted upon them for better understanding of the digital evidence.
- Digital analysts' courses be introduced at educational institutes; besides, refresher courses may also be arranged for judges, lawyers, prosecutors and LEAs officials.

- Basic forensic education, specialized training and awareness by raising campaigns, must be provided to all professionals dealing with digital evidence.

LEA:

- LEAs must use the latest hardware and software for seizure and examination of digital evidence.
- Five Ws, Who, What, When, Where and Why standard must be kept for dealing with digital evidence.
- Chain of custody by the LEAs, at any cost, must be maintained for all types of digital evidence.
- Digital evidence must be collected, or dealt by the qualified and competent persons or personals.
- For proper and timely examination of computer evidence, computer forensic labs, at least, in each Provincial Capital be established.
- For the sake of collection of digital evidence, it must be made compulsory and necessary for the individual as well as for organizations to report the cybercrime immediately enabling the LEAs to collect the relevant data in shortest possible time.
- Only skilled computer forensic investigator should be allowed to collect digital evidence and precede with investigation.
- Investigator should make the duplicate of the hard drive before examining of the hard drive and the original should be moved to secured environment to prevent tampering.
- It must be ensured by the Investigation Agency that the persons involved in digital evidence collection are specially trained personal.
- Proper training of LEAs in handling digital evidence is essential.

- The investigator must ensure that no part of any evidence is compromised by the methods applied by the experts to investigate the computer, internet and mobile devices.
- The investigator must ensure that digital evidence is suitably handled and protected from any kind of damage, alteration or modification.
- The investigator must be familiar with various operating system (Windows, Linux) and network operating systems.
- Investigator must not use or install any pirated version of a software or forensic tool on the compromised server. This, may alter and overwrote data on the evidential computer.
- Evidence collected from several identical computer systems should be documented separately, otherwise it will be very difficult to determine which evidence came from which system.
- All seized items must be packed in suitable seized containers which prevent contamination of evidence.
- The investigator must ensure that all digital evidence is accurately documented, labeled, marked and photographed and a list of all collected items is prepared.
- On all devices label should be clear and proper.
- All devices should be numbered separately and if there is case number the same may also be written.
- All digital evidence should be packed in anti-static bags and containers.
- Maximum efforts should be made by the LEAs to pack the evidence is such way that the collected evidence is safe from bent and scratch.
- No power cable, adapters and other cable are left at the crime scene.

- All collected evidence should be stored in secure environment to avoid extreme temperature and humidity.
- Mobile devices if they are in power mode, should be packed in Faraday bags to isolate it from connecting cellular network.
- Proper chain of custody of the evidence collected should be maintained by the investigator
- Digital evidence should be kept away from magnetic fields

BIBLIOGRAPHY

Articles:

Chaikin, David. "Network investigations of cyberattacks: the limits of digital evidence," *Crime, Law and Social Change* 46 (2006): 239-256.

Hu, Margaret. "Bulk Biometric Metadata Collection," *North Carolina Law Review*, 96 (2018): 1425-1474.

Joseph, Gregory P. "A Simplified Approach to Computer-Generated Evidence and Animations," *New York Law School Law Review* 43 (1999–2000): 875.

Kerr, Orin S. "Vagueness Challenges to the Computer Fraud and Abuse Act," *Minnesota Law Review* 94 (2010): 1561-1587.

Kramer, Xandra. "Challenges of Electronic Taking of Evidence: Old Problems in a New Guise and New Problems in Disguise," *Jornadas Iberoamericanas de Derecho Procesal IIDP & IAPL,* XXVI (2018): 391-410.

Larson, Erin. "Tracking Criminals with Internet Protocol Addresses: Is Law Enforcement Correctly Identifying Perpetrators?" *North Carolina Journal of Law & technology* 18 (2017): 316-358.

Rashbaum, et al. "Admissibility of Non-U.S. Electronic Evidence," *Richmond Journal of Law & Technology* 18 (2012): 1-76.

Rothstein, Jeremy H. "Track Me Maybe: The Fourth Amendment and the Use of Cell Phone Tracking to Facilitate Arrest" *Fordham Law Review* 81 (2012): 489-535.

Viega, John. "Cloud computing and the common man" *IEEE Computer* 42 (2009): 106-108.

Whitcomb, Carrie Morgan. "An Historical Perspective of Digital Evidence: A Forensic Scientist's View," *International Journal of Digital Evidence* 1 (2002): n.d.

Books:

Biasiotti, Maria Angela et al. *Handling and Exchanging Electronic Evidence across Europe.* Cham: Springer, 2018.

Boddington, Richard. *Practical Digital Forensics*. Birmingham: Packt Publishing, 2016.

Brown, Christopher L.T. *Computer Evidence: Collection and Preservation,* 2nd ed. Boston: Course Technology PTR, 2010.

Casey, Eoghan. *Digital Evidence and Computer Crime,* 3rd ed. New York: Elsevier, 2011.

Casey, Eoghan. *Handbook of Digital Forensics and Investigation.* ed. New York: Elsevier, 2010.

Daniel, Larry E. and Lars E. Daniel. *Digital Forensics for Legal Professionals Understanding Digital Evidence from the Warrant to the Courtroom*. New York: Elsevier, 2012.

Mason, Stephan and Daniel Seng. *Electronic Evidence*. 4th ed. London: School of Advanced Study, University of London, 2017.

Electronic Crime Scene Investigation: A Guide for First Responders. 2nd ed. Washington, D.C: National Institute of Justice, 2008.

Gatchel, Robert J. and Izabela Z. Schultz. *Handbook of Musculoskeletal Pain and Disability Disorders in the Workplace.* New York: Springer, 2014.

Imwinkelreid, Edward J. *Evidentiary Foundations,* 10th ed. Durham, North Carolina: Carolina Academic Press, 2018.

Johnson, Thomas A. *Forensic Computer Crime Investigation.* New York: CRC, 2005.

Marcella, Albert J. and Doug Menendez, *Cyber Forensics A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*, 2nd ed. New York: Auerbach Publications, 2008.

Marshall, Angus M. *Digital Forensics Digital Evidence in Criminal Investigation.* West Sussex: John Wiley & Sons, Ltd, 2008.

McCord, James W. H. and Sandra L. McCord. *Criminal Law and Procedure for the Paralegal: A Systems Approach.* 3r ed. New York: Thomson Delmar Learning, 2005.

Nyazee, Imran Ahsan Khan. *Jurisprudence.* Islamabad: Federal Law House, 2015.

Sammons, John. *The Basics of Digital Forensics the Primer for Getting Started in Digital Forensics*. 2nd ed. New York: Elsevier, 2015.

Shavers, Brett. *Placing the Suspect behind the Keyboard Using Digital Forensics and Investigative Techniques to Identify Cybercrime Suspects.* New York: Elsevier, 2013.

Sommer, Peter. *Digital Evidence, Digital Investigations and E-Disclosure: A Guide to Forensic Readiness for Organisations, Security Advisers and Lawyers.* 4th ed. Swindon: Information Assurance Advisory Council, 2013.

Vacca. John R. *Computer Forensics: Computer Crime Scene Investigation.* 2nd ed. Massachusetts: Charles River Media, Inc., 2005.

Wacks, Raymond. *Law A Very Short Introduction.* Oxford: Oxford University Press, 2008.

Zeigler, Ann D. and Ernesto F. Rojas. *Preserving Electronic Evidence for Trial a team Approach to the Litigation Hold, Data Collection, and Evidence Preservation.* New York: Elsevier, 2016.

Cases:

Aamir Shmas v. the State, 2019 PCrLJ 41 (Islamabad).

Abdul Ghaffar v. State, PLJ 2009 Cr.C (Lahore), 271.

Abdul Ghani v. the State, 2007 YLR 969.

Adams v. Disbennett, 2008 WL 4615623 (Ohio App. 3 Dist., Oct 20, 2008).

Ahmad Omar Sheikh v. the State, 2021 YLR 1777.

Aijazur Rehman v. the State, PLD 2006 Karachi 629.

Ali Naqi v. Government of the Punjab, 2019 PLC (C.S.) 952 Lahore.

Ali Raza v. the State, 2019 SCMR 1982.

American Express Travel Related Services Co. v. Vinhnee (In re Vinhnee) 336 B.R. 437 (B.A.P. 9th Cir. 2005).

Amitabh Bagchi s. Ena Bagchi (AIR 2005 Cal 11).

Ammar Yasir Ali v. The State, 2013 PCrLJ 783.

Arif Hashwani v. Sadruddin Hashwani, PLD 2007 Karachi 448.

Armstrong v. Executive Office of the President, 1 F.3d 1274 (D.C. Cir. 1993).

Asfandyar v. Kamran, 2016 SCMR 2084.

Babar Ahmad v. The State, 2017 YLR 153.

Brady v. Maryland, 373 U.S. 83 (1963).

Buzz Off Insect Shield, LLC v. S.C. Johnson & Son, Inc., 2009 U.S. Dist. LEXIS 17530 (M.D.N.C. Mar. 6, 2009.

Columbia Pictures, Inc. v. Bunnell, 245 F.R.D. 443 (C.D. Cal. 2007).

Daubert v. Merrell Dow Pharmaceuticals, 509 U.S. 579 (1993).

Doe v. United States, 805 F. Supp. 1513 (D. Haw. 1992).

Dolan v. State of Florida 743 So.2d 544 (1999).

Dr. Mobashir Hassan v. Federation of Pakistan, PLD 2010 SC 265.

Estate of Konell v. Allied Prop. 2014 U.S. Dist. LEXIS 10183 (D. Or. Jan. 28, 2014).

Farhan Kamrani v. the State, 2018, YLR 329 (Sindh).

Farooq Ahmad Khan v. Nawaz Sharif, PLD 1996 Lah 512.

Fenje v. Feld, 2003 LEXIS 24387 (N.D. Ill., December 8, 2003).

Galaxy Computer Services, Inc. v. Baker, 2005 WL 2171454 (E.D.Va. 2005).

Government of Sindh v. Fahad Naseem, 2002 PCrLJ 1765 Karachi.

Griffin v. State, 19 A.3d 415 (Md.2011).

Griffin v. State, 419 Md. 343, 19 A. 3d 415 (2011).

Hakim Ali Bhatti v. Abdul Hakim, 1986 CLC 1784.

Hashim Jamal v. the State, 2018 YLR Note 105.

In re *Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 538 (D. Md. 2011).*

In re Grand Jury Subpoena Duces Tecum, 670 F.3d 1335 (11th Cir. 2012).

In re Grand Jury Subpoena to Sebastien Boucher, 2007 WL 4246473 (D.Vt.)

In re Grand Jury Subpoena to Sebastien Boucher, 2009 WL 424718 (D.Vt.).

International Casings Group Inc. v. Premium Standard Forms, 358 F.Supp.2d 863 (W.D. Mo. 2005).

Ishtiaq Ahmad Mirza v. Federation of Pakistan, 2019 PLD SC 675.

Jarra Creek Central Packing Shed Pty Ltd v. Amcor Limited [2006] FCA [11].

Junaid Arshad v. the State, 2018 PCrLJ 739 (Lahore).

Kashif Dars v. the State, 2020 PCrLJ 259 (Sindh).

Kearley v. State, 843 So. 2d 66 (Miss. Ct. App. 2002).

Khanzada Inamulah Khan v. Mst. Zakia Qutab, PLD 1998 Peshawar 52.

Kumho Tire v. Carmichael, 526 U.S. 137 (1999).

Kupper v State 2004 WL 60768 (Tex. App. Jan. 14, 2004)

Land Acquisition Collector v. Muhammad Sultan, PLD 2014 SC 696.

Lenzini v. Columbia Foods, 829 S.W.2d 482 (Mo. App. 1992).

Lorraine v. Markel American Insurance Company, 241 F.R.D. 534 (D. Md. 2007)

Microsoft v. United States, No. 14-2985 (2d Cir. 2016).

Mst. Akhtar Sultana v. Major ® Muzaffar Khan Malik, PLD 2021 SC 715.

Mst. Marium Haji v. Mrs. Yasmin R. Minhas, PLD 2003 Karachi 148.

Mst. Rehana Anjum v. Additional Sessions Judge, PLD 2016 Lahore 570.

Muhammad Akram Baloch v. Akbar Askani, 2014 CLC 878,

Muhammad Arif Chaudhry v. Muhammad Suleman, Civil Petition No. 1945 of 2018 (Order dated 16.04.2020).

Muhammad Ashraf v. the State, 2018 PCrLJ 1667 (Lahore).

Muhammad Din v. the State, PLD 1995 Kar 469.

Muhammad Hussain v. State, 2011 SCMR 1127.

Muhammad Irfan v. The State, 2018 PCrLJ 1319.

Muhammad Jawad Hamid v. Muhammad Nawaz Sharif, 2019 PCrLJ 665 (Lahore).

Muhammad Nasir v. Mahmood Shaukat Bhatti, PLD 2003 Lahore 231.

Muhammad Nawaz Sharif v. the State, PLD 2018 Islamabad 148.

Muhammad Sadiq v. State, 2016 PCrLJ 1390.

Munas Parveen v. Additional Sessions Judge, PLD 2015 Lahore 231.

Naveed Asghar v. the State, PLD 2016 Lahore 467.

Nazim Ali v. Additional Sessions Judge, 2016 MLD 25.

Netword LLC v. Centraal Corp., 242 F.3d 1347 (Fed. Cir. 2001).

New York v. Microsoft Corp., 224 F. Supp. 2d 76 (D.D.C. 2002).

Nightlight Sys., Inc. v. Nitelites Franchise Sys., Inc., No. 1:04-CV-2112-CAP, 2007 U.S. Dist. LEXIS 95538, (N.D. Ga. May 11, 2007).

Nucor Corp v. Bell, 251 F.R.D. 191 (D.S.C. 2008).

Ohio v. Michael J. Morris, Court of Appeals of Ohio, Ninth District, Wayne County, No. 04CA0036, Feb. 16, 2005.

Paralyzed Veterans of America v. McPherson, 2008 WL 4183981 (N.D. Cal. Sept. 9, 2008).

People v. Downin, 828 N.E.2d 341 (Ill. App. Ct., April 29, 2005).

People v. Holowko, 109 Ill.2d 187, 93 Ill.Dec. 344, 486 N.E.2d 877 (1985).

People v. Markowitz, 721 N.Y.S.2d 758 (Sup. Ct. February 9, 2001).

People v. Morrow, 628 N.E.2d 550 (111. App. 1993).

Potamkin Cadillac Corp. v. B.R.I. Coverage Corp., 38 F.3d 627 (2d Cir. 1994).

Qurban Ali v. The State, 2007 PCrLJ 675 Karachi.

Ram Kirpal vs. Shri Krishna Deo, AIR 1948 All. 109.

Re: VeeVinhnee, 336 B.R. 437 (B.A.P, 9th Cir, 2005).

Rehmat Shah Afridi v. The State, PLD 2004 Lahore 829.

Riley v. California, 573 U.S. 373 (2014).

Saifal v. the State, 2013 PCrLJ 1082 (Sindh).

Saifur Rehman Khan v. Shahab ud Din, 1995 MLD 1485.

Salman Ahmad Khan v. Judge Family Court, PLD 2017 Lahore 698.

Shahid Zafar v. the State, 2015 PCrLJ 628 (Sindh).

Shahid Zafar v. the State, PLD 2014 SC 809.

Sikandar Ali Lashari v. the State, 2016 YLR 62 (Sindh).

Smith v. Maryland, 442 U.S. 735 (1979).

Soldal v. Cook County, 506 U.S. 56 (1992).

Sony BMG Music Entertainment v Arellanes, LEXIS 78399 (E.D. Tex. Oct. 27, 2006).

St. Luke's Cataract & Laser Inst., P.A. v. Sanderson, 2006 WL 1320242 (M.D. Fla. May 12, 2006).

State of Maharashtra v. Dr. Praful B Desai (AIR 2003 SC 2053).

State v. Cook, WL31045293 Ohio Ct. App. (2002).

State v. Levie, 695 N.W.2d 619 (Minn. Ct. App. June 10, 2005),

State vs. Roszkowski, 129 N.J. Super. 315, 323 A2d 531 (App. Div. 1974).

Talada v. City of Martinez, 656 F. Supp. 2d 1147 (N.D. Cal. 2009).

The State through P.G. Sindh v. Ahmed Omar Sheikh, 2021 SCMR 873.

Toytrackerz, LLC v. Koehler, No. 08-2297-GLR, 2009 U.S. Dist. LEXIS 74484 (D. Kan. Aug. 21, 2009).

Turner v. United States 582 U.S.____. 2017.

U.S. Equal Employment Opportunity Commission v. E.I. DuPont De Nemours & Co., 347 F. Supp. 2d 284 (E.D. La. 2004).

Umair Ashraf v. The State, 2008 MLD 1442 (Karachi).

United Stated v. Moussaoui, 382 F.3d 453 (4th Cir. 2010).

United Stated v. Moussaoui, 591 F.3d 263 (2010).

United Stated v. Perdomo, 929 F.2d 967 (3d Cir. 1991).

United States of America v. Gavegnano, 305 Fed.Appx. 954 (4th Cir. 2009).

United States of America v. Kirschner, 2010 WL 1257355 (E.D.Mich.).

United States v Gagliardi, 506 F.3d 140 (2d Cir. 2007).

United States v. Allen, 106 F.3d 695 (6th Cir. 1997).

United States v. Barlow, 568 F.3d 215 (5th Cir. 2009).

United States v. Bonallo, 858 F.2d 1427 (9th Cir. 1988).

United States v. Brooks, 715 F.3d 1069 (8th Cir.2013).

United States v. Bunty, 617 F. Supp. 2d 359 (E.D. Pa. 2008).

United States v. Cameron, 762 F. Supp. 2d 152 (D. Maine 2011).

United States v. Campbell, No. 94-30295, 1996 WL 241545 (9th Cir. May 9, 1996).

United States v. Catabran, 836 F.2d 453 (9th Cir. 1988).

United States v. Councilman, 418 F.3d 67 (1st Cir. 2005).

United States v. Ferber, 966 F. Supp. 90 (D. Mass. 1997).

United States v. Gagliardi, 506 F.3d 140 (2nd Cir, 2007).

United States v. Giberson, 527 F.3d 882 (9th Cir. 2008).

United States v. Gray, 78 F. Supp. 2d 524 (E.D. Va. 1999).

United States v. Hamilton, 413 F.3d 1138 (10th Cir. 2005).

United States v. Hill, 322 F.Supp.2d 1081(C.D.Cal.2004).

United States v. Holmquist, 36 F.3d 154 (1st Cir. 1994).

United States v. Howard-Arias, 679 F.2d 363 (4th Cir. 1982).

United States v. Jackson, 208 F.3d 633 (7th Cir. 2000).

United States v. Jones, 565 U.S 132 S.Ct. 945 L.Ed. 2d 911 (2012).

United States v. Khorozian, 333 F.3d 498 (3d Cir.2003).

United States v. Kramer, 631 F.3d 900 (8th Cir. 2011).

United States v. Maldonado-Rivera, 922 F.2d 934 (2d Cir. 1990).

United States v. Matish, 193 F. Supp. 3d 585 (E.D. Va. 2016).

United States v. Matta-Ballesteros, 71 F.3d 754 (9th Cir. 1995).

United States v. Melenberg, 263 F.3d 1177 (10th Cir. 2001).

United States v. Microsoft Corp., 584 U.S. ___, 138 S. Ct. 1186 (2018).

United States v. Moore, 923 F.2d 910 (1st Cir. 1991).

United States v. Neil Scott Kramer, 631 F. 3d 900 (8th Cir. 2011).

United States v. Ramona Camelia Fricosu a/k/a/ Ramona Smith, 2012 WL 182121 (D.Colo.).

United States v. Safavian, 435 F. Supp. 2d 36 (D.D.C. 2006)

United States v. Scholle, 553 F.2d 1109 (8th Cir. 1977).

United States v. Simpson, 152 F.3d 1241 (10th Cir. 1998).

United States v. Sliker, 751 F.2d 477 (2d Cir. 1948).

United States v. Stierhoff, 477 F. Supp. 2d 423 (D.R.I. 2007).

United States v. Tank, 200 F.3d 627 (9th Cir. 2000).

United States v. Vayner, 769 F.3d 125 (2d Cir. 2014).

United States v. Vela, 673 F.2d 86 (5th Cir. 1982).

United States v. Vilar, 2007 WL 1075041 (S.D.N.Y. Apr. 4, 2007).

United States v. Walser, 275 F.3d 981 (10th Cir. 2001).

United States v. Washington, 498 F.3d 225, 230-31 (4th Cir. 2007).

United States v. Whitaker, 127 F.3d 595 (7th Cir. 1997).

United States v. Wiest, 596 F.3d 906 (8th Cir.2010).

United States v. Wood, No.08-CR-92A, 2009 WL 2157128 (W.D.N.Y. July 15, 2009).

United States vs. Miller, 771 F.2d 1219, (9th Cir. 1985).

United States vs. Simpson, 152 F.3d 1241 (10th Cir. 1998).

Wady v. Provident Life & Accident Ins. Co. of America, 216 F. Supp. 2d 1060 (C.D. Cal. 2002).

Watan Party v. Federation of Pakistan, PLD 2012 SC 292.

Williams v. Long, 2008 WL 4848362 (D. Md., November 7, 2008).

Williams v. Long, 585 F.Supp.2d 679 (D. Md. 2008).

Williams v. Sprint/United Management Co., 230 F.R.D. 640, 652 (D.Kan. 2005).

Yasir Ayyaz v. the State, PLD 2019 Lahore 366.

Zakir Hussain v. The State, 2017 PCrLJ 757.

Zubulake v. UBS Warburg LLC, 217 F.R.D. 309 (S.D.N.Y. 2003).

Zubulake v. UBS Warburg LLC, 230 F.R.D. 290 (S.D.N.Y. 2003).

Zubulake v. UBS Warburg, 216 F.R.D. 280 (S.D.N.Y. 2003).

Zubulake v. UBS Warburg, 220 F.R.D. 212 (S.D.N.Y. 2003).

Zubulake v. UBS Warburg, 229 F.R.D. 422 (S.D.N.Y. 2004).

Documents and Reports:

Association of Chief Police Officers UK, *Good Practice Guide for Computer-Based Electronic Evidence.*

Carrier, Brian D. "A hypothesis-based approach to digital forensic investigations," (Ph.D. diss., Purdue University, 2006).

Federal Judicial Centre, *Manual for Complex Litigation*, 4th ed. Washington: Federal Judicial Centre, 2004.

Investigative Uses of Technology: Devices, Tools, and Techniques. Washington, D.C: National Institute of Justice, 2007.

Lucy L. Thomson, Esq. "Admissibility of Electronic Documentation as Evidence in U.S Courts," Centre for Research Libraries Human Rights Electronic Evidence Study, 4.

Lynnette, Amy. "Digital and Multimedia Forensics Justified: An Appraisal on Professional Policy and Legislation," (M.S. diss., University of Colorado Denver, 2015).

National Institute of Justice, *Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors,* 44.

Stanfield, Allison Rebecca. "The Authentication of Electronic Evidence," (Ph.D. diss., Queensland University of Technology, 2016).

Statutes:

18 United States Code (18 U.S.C).

28 United States Code (28 U.S.C)

Code of Civil Procedure 1908 (V of 1908).

Code of Criminal Procedure, 1898 (V of 1898).

Constitution of the Islamic Republic of Pakistan, 1973.

Criminal Laws (Amendment) Act, 2017 (IV of 2017)

Electronic Transactions Ordinance, 2002 (LI of 2002).

Evidence Act, 1872 (I of 1872).

Family Courts Act, 1964 (Act XXV of 1964).

Federal Rules of Civil Procedure, USA

Federal Rules of Evidence, USA

Indian Independence Act, 1947

Investigation for Fair Trial Act, 2013 (I of 2013).

Mobile Device Identification, Registration and Blocking Regulations, 2017

Payment Systems and Electronic Fund Transfers Act, 2007 (IV of 2007).

Prevention of Electronic Crimes Act, 2016 (XL of 2016).

Prevention of Electronic Crimes Ordinance, 2007 (LXXII OF 2007)

Prevention of Electronic Crimes Ordinance, 2008 (IX of 2008).

Prevention of Electronic Crimes Ordinance, 2009 (VIII of 2009).

Prevention of Electronic Crimes Ordinance, 2009 (XIV of 2009).

Punjab Family Courts (Amendment) Act, 2015 (Act XI of 2015).

Punjab Forensic Science Agency Act, 2007 (XIII of 2007).

Qanun-e-Shahadat Order, 1984 (P.O. No. 10 OF 1984)

Subscribers Antecedents Verification Regulations, 2015

The Punjab Witness Protection Act, 2018 (Act XXI of 2018).

Webliography

http://journals.sas.ac.uk/deeslr/article/viewFile/2321/2245 (accessed: 7th November, 2019).

http://pfsa.gop.pk/?page_id=20 (accessed: 23rd February 2018).

http://www.forensicsciencesimplified.org/digital/ (accessed: 31st July, 2018).

http://www.teach-ict.com/gcse_new/computer%20systems/storage_devices/miniweb/pg9.htm (accessed: 18th April, 2020)

http://www.techrepublic.com/blog/it-security/what-makes-cybercrime-laws-so-difficult-to-enforce/ (accessed: 5th July 2017).

https://archives.fbi.gov/archives/newyork/press-releases/2010/nyfo070810a.htm (accessed: 21st April, 2020).

https://blogs.windows.com/windowsexperience/2015/06/01/hello-world-windows-10-available-on-july-29/ (accessed: 25th March, 2020)

https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=9d18fc06-b229-4c4a-8ca5-7386d0870c01&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments (accessed: 25th April, 2020).

https://csrc.nist.gov/publications/detail/sp/800-145/final (accessed: 24th April, 2020)

https://definitions.uslegal.com/d/digital-evidence/ (accessed: 7th August, 2018).

https://fp.brecorder.com/2017/08/20170804205160/ (accessed: 21st February, 2018).

https://i-sight.com/resources/15-types-of-evidence-and-how-to-use-them-in-investigation/ (accessed: 13th July, 2018).

https://nij.ojp.gov/topics/articles/glossary-crime-scene-investigation-guides-law-enforcement (Accessed: 21st December, 2019).

https://propakistani.pk/2020/04/13/fia-to-investigate-data-breach-of-115-million-pakistani-mobile-phone-users/ (accessed: 14th April, 2020).

https://www.computerhope.com/jargon/f/filesyst.htm (accessed: 25th March, 2020).

https://www.computerhope.com/jargon/h/harddriv.htm (accessed: 25th March, 2020).

https://www.crl.edu/sites/default/files/d6/attachments/pages/Thomson-E-evidence-report.pdf (accessed: 30th November, 2019).

https://www.dawn.com/news/1348889 (23rd Feb. 2018)

https://www.dawn.com/news/1443970 (accessed: 6th October, 2019).

https://www.dawn.com/news/1484248 (accessed: 6th October, 2019).

https://www.nist.gov/news-events/news/2011/10/final-version-nist-cloud-computing-definition-published (accessed: 24th April, 2020).

https://www.nist.gov/programs-projects/nist-cloud-computing-program-nccp (accessed: 24th April, 2020).

https://www.pakistantoday.com.pk/2018/11/06/hackers-steal-data-from-almost-all-pakistani-banks-fia/ (accessed: 6th October, 2019).

https://www.rand.org/pubs/research_reports/RR890.html (accessed: 25th October, 2019).

https://www.swgde.org/documents/Archived%20Documents/SWGDE-SWGIT%20Digital%20and%20Multimedia%20Evidence%20Glossary%20v2-8 (accessed: 9th August, 2018).

https://www.techopedia.com/definition/1369/file-allocation-table-fat (accessed: 25th March, 2020).

https://www.techopedia.com/definition/24482/new-technology-file-system-ntfs (accessed: 25th March, 2020);

https://www.techopedia.com/definition/5288/hard-disk-drive (accessed: 25th March, 2020).

https://www.techopedia.com/definition/5510/file-system (accessed: 25th March, 2020).

https://www.thenews.com.pk/latest/390450-data-of-major-pakistani-banks-hacked-fia-official (accessed: 6th October, 2019).

https://www.thenews.com.pk/latest/475315-pakistans-supreme-court-to-start-e-court-system-from-monday (accessed: 6th October, 2019).

https://www.thenews.com.pk/latest/477081-e-court-system-successfully-launched-in-supreme-court (accessed: 6th October, 2019).

https://www.thoughtco.com/unusual-history-of-microsoft-windows-1992140 (accessed: 25th March, 2020).

https://www.universalclass.com/articles/law/types-of-evidence.htm (accessed: 13th July 2018).