Enhancing Data Integrity and Documentation Procedure for Digital Forensics Investigation Model

(In Pakistan Perspective)

By:
Talat Ahmad Bhutta
404-FBAS/MSCS/S08

Supervisor:
Prof. Dr. Muhammad Sher
Chairman DCS & SE
Dean FBAS

Department of Computer Science and Software Engineering
Faculty of Basic and Applied Sciences,
International Islamic University, Islamabad.
2013

1- Computer systems

2. Data processing

Department of Computer Science and Software Engineering Faculty of Basic and Applied Sciences, International Islamic University, Islamabad

Date: ___________

Final Approval

It is certified that I have examined the thesis titled "Enhancing Data Integrity and Documentation Procedure for Digital Forensics Investigation Model (In Pakistan Perspective)" submitted by Talat Ahmad Bhutta, Registration no 404-FBAS/MSCS/S08, and found as per standard. In my judgment, this research thesis is sufficient to warrant it is acceptance by the International Islamic University, Islamabad for the award of the degree of Master of Science in Computer Science.

Committee

External Examiner:
Dr. Mureed Hussain
GM (Tech), NESCOM,
Islamabad

Internal Examiner:
Syed Muhammad Saqlain
Assistant Professor,
DCS & SE, FBAS, IIUI

Supervisor:
Professor Dr. Muhammad Sher
Chairman, DCS & SE,
Dean FBAS,
International Islamic University,
Islamabad

A thesis submitted to the

Department of Computer Science and Software Engineering

Faculty of Basic and Applied Sciences,

International Islamic University, Islamabad

in partial fulfillment of the requirements for the award of

the Degree of

Master of Science in Computer Science

This dissertation is dedicated to my father

Ghazanfar Ali Bhutta

Who was always a proud father and supportive of my interest in

continuing my education at every possible opportuity and condition.

Sadly, he is not able to see me

Declaration

I hereby declare that this work, neither as a whole nor as a part has been copied out from any source. It is further declared that I have conducted this research and have accomplished this thesis entirely on the basis of my personal efforts and under the sincere guidance of my supervisor Professor Dr. Muhammad Sher. If any part of this thesis is proved to be copied out from any source or found to be reproduction of some other thesis, I shall stand by the consequences. No portion of the work presented in this dissertation has been submitted in support of any application for any other degree or qualification of this or any other university or institute of learning.

Talat Ahmad Bhutta
(404-FBAS/MSCS/S08)

Acknowledgement

All praise to Almighty Allah who has all the names and who need no name the most generous, considerate and compassionate who has blessed mankind with this verdict to think, explore, to learn and discover the hidden secrets of this universe and helped me to broaden the veils of my thought and enabling me to get through the difficulties indulged during this thesis. Also admiration to our beloved Prophet Muhammad (PBUH) who is always a great source of inspiration of divine devotion and dedication to me.

Several people gave me support to achieve this thesis and I would like to take this opportunity to thank them all for their help and assistance.

First of all, I would like to express my deep and gratitude to my supervisor, Professor Dr. Muhammad Sher. His wide knowledge and his logical way of thinking have been of great value for me. His invaluable comments, ideas, encouragement and guidance have provided a good basis for the present thesis.

Special thanks to Mr. Ammar Hussain Jaffri former Project Director National Response Center for Cyber Crimes Federal Investigation Agency Government of Pakistan, for motivation toward Digital Forensic field. Mr. Ammar Hussain Jaffri provided much of the forensic background and initial guideline for this dissertation.

I would cordially pay my special appreciations and whole heartedly considerations to National Response Center for Cyber Crimes team members Mr. Mahmood, Mr. Amir, Mr Ali Imran (Forensic Experts NR3C), Mr. Muhammad Nasim and Mr. Akram Mughal for their kind guidance and endless support.

I would also like to pay my gratitude to all my respected teachers making me capable of what I am today due to their guidance and help.

Thanking my friends Mr. Hidayat Ullah Khan, Mr. Shahzad Ch and Mr. Zahid Mahmood for always being there for me whenever I needed them for their help, generosity and moral support.

It is difficult to explain how grateful I am to one person who is there for me literally since the first day of my birth. My Mother is truly incredible person and I am extremely thankful for everything she is doing for me.

Finally my beloved family who deserve the credit more than I could ever express for always being completely supportive to me. They have been a constant source of advice, love and devotion to me. From moral to financial they have been blessing me with all the support that I have needed up till now in my life. Lastly but least, I thank God and His Prophet Muhammad (PBUH) for the health and protection They enabled me to enjoy.

Abbreviation Used

Abbreviations	**Acronyms**
IT	Information Technology
IDS	Intrusion Detection System
FTK	Forensic Tool Kit
Three A's	Acquiring, Authenticating, Analyzing
DOJ	Department of Justice
DFRWG	Digital Forensic Research Working Group
US	United States
CERTs	Computer Emergency Response Teams
ISACs	Information Sharing and Analysis Centers
ICIM	Independent Center for Incident Management
NR3C	National Response Centre for Cyber Crimes
PGI3C	Procedure Guide for Investigating Cyber Crime Cases
SOPs	Standard Operating Procedures
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
JTC	Joint Technical Committee
SC	Sub Committee
IRT	Incident Response Team
ISP	Internet Service Provider
IP	Internet Protocol

DNS	Domain Name Server
NIST	National Institute of Standards and Technology
MD5	Message Digest 5
SHA1	Secure Hash Algorithm 1
GPS	Global Positioning System
AFF	Advanced Forensic Format
RDF	Resource Description Framework

Abstract

In the present global environment, the threats to computer systems and critical infrastructure have increased as never before. The misuse of digital devices in every day life is common example of crime that may be locally or remotely from global environment. Cyber crime is a major threat to global peace, security and stability, which affect individual country, organization, company and corporate environment at different levels and ways.

Computer forensics is an emerging research topic it is a sub field of information security. Several digital forensics investigation models are used for forensic investigation. Set of procedures are used by modification in previous model without concentration on information process flow, chain of custody and standardization. In existing models, less work has been done on Integrity of Data / Information and Documentation (in Pakistan's perspective). The existing models typically concentrate just a part of the investigative method and not provide a universal view of the total investigation process. This research studied the discipline of Digital Forensic from the prospective of enhancing data integrity and documentation procedure for digital forensics investigation model (in Pakistan's perspective). In proposed model, a new phase i.e. hypothesis is introduced. Data integrity and documentation procedure is proposed to continue throughout the proposed model. At every phase, hash or backup of drives is taken along with chain of custody. Procedures, methodologies, policies and rules to overcome cyber crime and safety measures to save digital evidence / crime scene are an important part of the proposed model.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1. Introduction

To enhance productivity, output and security in every sector of every economy, computer/internet is used as tool. The digital technologies are used as criminal tool in recent era which may be used to perpetrate unlawful activities because criminal groups or individual know and learn in-depth technical knowledge.

In present Global Era, Cyber-crime is becoming more organized and transnational business due to availability of high technology skills available online for rent or free of cost, to individuals or groups or nations. Officials in organization and industry experts agree that Cyber-crime and Cyber-attack services are available to criminals due to which security threat to organization, nation and international peace is growing as never before [2].

It is also clear that race between criminals and law enforcement is never ending field. In order to overcome cyber criminals, the investigators, security experts and law enforcement agencies must use well defined and consistent forensic procedures to develop such tools that cover all areas of forensic analysis and models.

1.1 Forensics

"Forensics is the application of scientific methods in criminal investigations. It is a unique field of study that draws from all areas of science [4]". Basically Forensic is a Latin Word which means "to bring into Court or Forum or Jewry".

1.2 Digital Forensics

"According to academia Digital Forensics is said a discipline of science. Therefore digital forensics is a combination of research in the area of computer hardware and software that use and provide way to Digital Forensics for community development [4]"

1.2.1 Definition of Digital Forensics

"Digital Forensics is the collection, preservation, analysis and presentation of digital evidence that is admissible in a court of Law, usable for Organization internal Disciplinary Action or Hearing, internal Incident reports and helping or assisting further investigations [1]".

1.2.2 Digital Evidence

"Digital evidence is a digital data which is used to rebuild past events or action and shows control of Digital data. Digital evidence may be defined as information stored or transmitted in binary form that may be relied upon in court [18]".

Through Digital Evidence, we come to know the use or misuse of IT infrastructure and services, and how policy is violated which result in illegal activity [1].

1.2.3 Sources of Digital Evidence

"Sources of Digital evidence are Hard Disks, Tapes, Firewall, Proxy, External or Removable media, Intrusion Detection Systems, software application, Audit log files, E-mails, Database system, Mobile Devices, Web servers, Captured Network traffic [1]".

1.3 Areas of Digital Forensics

"The main areas of Digital Forensics are Computer Forensics (Hard disk, removable media), Network Forensics (network intrusion), Software Forensics (malicious code, malware) and Live System Forensics (compromised hosts or system) [1]".

1.3.1 Computer Forensic

A commonly referenced definition of computer forensics is that it "involves the preservation, identification, extraction, documentation and interpretation of computer data" [19].

"Computer Forensic studies how computer are involved in the commission of crimes. In cases ranging from accounting fraud to blackmail, identity theft and child pornography [4]". Usage of computer forensics in different areas is vast and growing field. Computer forensic is used in litigation, educational fields, research and in corporate world. In different field of life computer forensics is taught to improve the utilization.

1.4 Implementation of Digital Forensics

Digital Forensics is implemented in Law Enforcement, Military, Government Agencies, Law and Private Forensic Firms and Corporate Organization. Internal demands and External Factors are driving the implementation of Digital Forensics importance within organizations so that to fulfill legal and regulatory requirements. Every organization has specific requirements for Digital Forensics [1].

The corporate world use digital forensics for civil litigation and trying to discover how employees have been using corporate network.

1.5 Evolution of Digital Forensics

In the evolution of digital forensics computer scientists, law experts, intelligence persons, network administrators, program developers and academia play an important role. According to experts, digital forensics is still an evolving area of science. It is one of the most powerful and intrusting investigative technique.

1.6 Digital Forensics Principles and Methodologies

Digital forensic is a growing community of professional involved in digital forensic industry. Basically it is free for all to access and to use, due to which digital investigation and crime crosses international and language borders and provide a single global virtual environment. Anyone can access and use / misuse resources from any corner of the world to other without any permission or visa as in human case to cross border, which results the cyber crime[21].

"Digital Forensics experts face practical, lawful, operational, criminal and technical difficulties/challenges due to new technological modernism and complexity of cyber criminals activities which result Digital Forensics principles and methodologies evolve. Digital Forensics principle means a complete and basic law, set of guidelines or ruling while a procedure is a exacting way or method of accomplishing somewhat or of activity [3]".

Digital forensics is necessary for successful trial or understanding of digital crime. The main reason of emergence of digital forensics is incidents of criminal, illegal, unauthorized and inappropriate behaviors. The investigation process has to be able to retrieve the digital evidence, which is acceptable at any forum. Forensics methodologies, techniques, procedures and models / framework play an important role in digital forensics world. There are a number of necessary points to be performed for successful digital forensic investigation. Proper documentation in digital forensic investigation plays a vital role to maintain integrity of digital evidence.

1.6.1 Digital Forensic Investigation Model

Different digital forensic investigation models have been developed so that systematic and planned examination process of digital evidence may be carried out. The model should provide a clear picture to digital evidence examiners or investigators. Digital forensic model provides principles, procedures and ways to investigate digital crime. In the model there are number of phases or steps or stages which should be adopted by victim of crime, first responder, investigator, examiner and all other persons who are directly or indirectly involved in investigation process.

Comprehensive digital forensic investigation model should provide standardized terminology, define requirements, standard operating procedures and guidelines to develop new tools and be able to fulfill requirements of future technology.

According to literature, over hundreds of digital forensics models are developed in different area of world. Majority of digital forensics investigation models are developed on the basis of technology and tools for investigation available in market. Some organizations have developed there own models on the basis of their requirements and internal laws. Most models are developed to fulfill the requirements for specific device investigation, with the result that a new model has to be developed as technology of device change.

1.6.2 Tools

The term "tool" is used to describe analytical methods and procedures, and the method used to facilitate that analysis, which mean "anything used regularly in the course of a particular profession or occupation" [22, 23]. Tool may be defined as "any instrument which conveys some advantage to its user in the execution of a task" [23]. There is no single definable set of tools that encapsulates all the technology that is required for examination or analysis. Digital forensic investigator use different tools to search, examine, analyze, compare and back up digital evidence.

A research is going on to define the toolkit methodology, each toolkit procedure is correct in its own way but researchers agree that a principled approach is required to develop tool. Standards are emerging that do not dictate the equipment but the process or steps must be followed for tool development and forensic investigation [23}. Both open source and licensed tools are available for digital forensics investigation. A periodic update in tools development procedure is required as technology emerges.

Forensic tools are categories into combinatorial or multifunction tools and single function tools. Forensic toolkit, EnCase, Pro Discover, SMART, Sleuth Kit, Pyflag and Nuix Desktop/Enterprise are popular tools. Other forensic supporting software are Imaging tools, ByteBack, DriveSpy, SafeBack, X-Ways Capture, Paraben Replicator, Norton Ghost [23].

1.6.2.1 Forensic toolkit

"Forensic toolkit ® (FTK ®) is familiar around the information technology world as the standard in computer forensic software. This software supports to perform complete, technical and comprehensive computer forensic analysis and examinations [25]. FTK® provides features to support powerful filtering methods and searching functionality, and is accepted by law enforcement agencies and professionals serving in corporate security as the important forensic tool [25]".

1.7 Federal Government Organization policy

For improvement of efficiency in governments offices GoP enforces different government organizations, officials and their employees to use different information technology tools. According to policy, officials are allowed to get expertise to communicate with public to perform duties in a batter way. To use electronic tools and services, Cabinet Division of Government of Pakistan – with the consultation of various stake holders, technical and security related organizations – has formulated a policy framework for organizations to support organizations, ministries, divisions, individuals to take benefit from information technology tools. It is also the part of policy to take such security measures to ensure that national security is not violated. The policy provides guidelines for usage of IT infrastructure, periodic technical audit to maintain security and ensure departmental security standards [26]".

1.8 Cyber Laws in Pakistan

There are different laws which are promulgated in Pakistan. These laws not only deal with crime of internet but with all dimensions related to computer, network and digital devices.

1.8.1 Electronic Transactions Ordinance, 2002

Electronic Transactions Ordinance, 2002 was the first IT relevant legislation introduced by national lawmakers. It is the first step and a solid foundation for legal sanctity and protection for Pakistani e-commerce locally and globally. There are forty three sections in this ordinance. It deals with areas relating to recognition of electronic documents, records, information, communications and transactions in electronic form, accreditation of certification service providers and for matters connected therewith [28].

1.8.2 Prevention of Electronic Crimes Ordinance

Prevention of Electronic Crimes Ordinance deals with the electronic crimes included cyber terrorism, unauthorized acts with respect to information systems, establish related offences, provides mechanisms for investigation, prosecution, trial and international cooperation [29]. It will apply to every person who commits an offence, irrespective of his nationality or citizenship. Every respective offence under this law has its distinctive punishment which can be imprisonment or fine.

1.8.3 Investigation for Fair Trial Act, 2013

Investigation for Fair Trial Act, 2013 provides 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 [30].

1.9 Outline of Dissertation

The chapter 1 of thesis is introduction. It includes the overview of Digital Forensic, different areas, sources, evolution, implementation, principles/methodology, models and tools used for Digital Forensic are discussed in detail. Also the need of Digital Forensic Investigation Model and phases are discussed.

Chapter 2 is literature survey; it provides a comprehensive exploration of the literature and it discusses the researchers' previous research work in Digital Forensic Investigation Model.

Chapter 3 consists of problem domain and objective of research. The main problem of digital forensics on which this research work focuses is explained in detail and objectives related to this thesis.

Chapter 4 consists of proposed solution; a new Digital Forensic Investigation Model is proposed which will enhance data integrity and documentation procedure. Some new phases are propped in this solution.

Chapter 5 is implementation methodology of proposed model; in this chapter different steps have been taken one by one to implement the proposed model in a way that data integrity and documentation procedure may not compromise. Forensic toolkit ® and FTK Imager are used.

Chapter 6 is results and discussion; in this chapter analysis of different phases of proposed model with studied models is discussed along with terminology and then phases of hypothesis is given and data integrity issues are discussed.

Chapter 7 consists of conclusion and future work in the studied area; in this chapter I have concluded my research work and a few necessary future issues are discussed for further enhancement in digital forensics area.

Chapter 8 is references; it includes complete list of references which have been discussed and studied in our research work.

Chapter 2

Literature Survey

2. Literature Survey

An important job before starting a research work in any science field is review of the related material in that area. So I have completed the same work as per criteria. For the purpose of literature survey I have studied research papers, articles, thesis, books, guidelines, reports and standards etc. to decide what has been done so far in the field.

The goal of literature review is as under:

- Understanding of search area to collect relevant literature
- Formulation of the research questions
- Evidence gathering for existing research area
- Identification of research gaps in literature
- Identification of future direction in field

Many researchers, authors and forensics investigators have prepared a lot of Digital Forensic Investigation Models in literature. Those models which I have studied during our research and satisfied our criteria are as follows:

2.1 M. Pollitt Model [5]

The early methodology for computer forensic was suggested by M. Pollitt in 1995. In this paper the term computer forensic is defined and discussed that how digital media fulfill the legal requirements for acceptability of paper based evidence. Paper suggested a method that how to deal with potential evidence. In paper based world all parties accept the law which is mutually updated, understood and acceptable by all the concerns parties these are four steps methodology which include acquisition, identification, evaluation and admission of evidence in court.

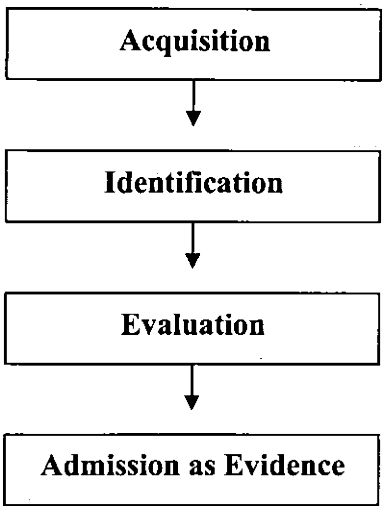


Fig 2.1: M. Pollitt Model [5]

In case of digital evidence a person who can explain the mechanism of acquisition, identification and evaluation so that it may be tested for reliability and acceptance. When these four steps were applied to digital evidence a new set of problems arrived, like:

- What this binary form of data means and represents, from where did it come from?
- A binary data file requires conversion in the form of a program which is human readable.
- Evaluation of electronic context of a file.

In digital paradigm the digital evidence is invisible to the human eye; therefore, a tool should be used to make evidence visible for every human eye. The process to make evidence visible requires the use of tools or knowledge; therefore, it is suggested to prepare complete documentation to make evidence reliable and repeatable. It was further proposed to make all process of digital evidence gathering mechanism more understandable to the member of court.

The outcome of these steps was media, data, information and evidence. This was first step toward digital evidence. Computer Forensic process was mapped to documentary evidence. No framework or principle was suggested in this paper.

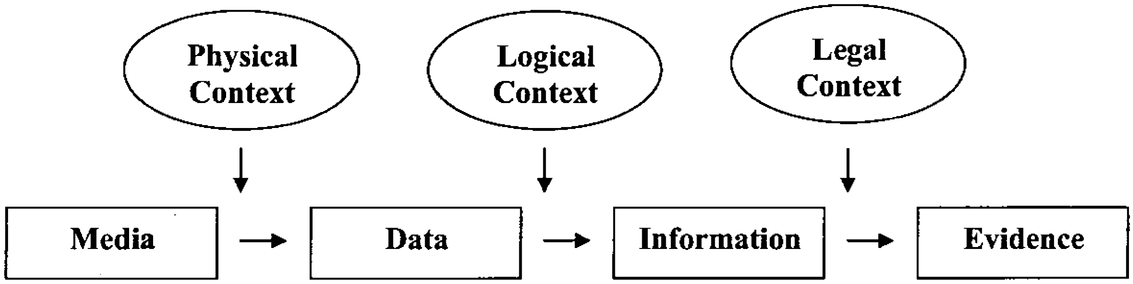


Fig 2.2: Path of digital evidence [5]

2.2 Kruse and Heiser Model [13]

The model proposed by Kruse and Heiser (2001) consist of three step forensic methodology, which is also referred as the “Three A’s of Computer Forensics investigation”. The given stages were acquiring evidence, authenticating evidence and analyzing evidence. Three A’s model provide techniques to solve crime cases at that time. According, to this model computer forensic was coherent application of methodological investigation technique to solve crime cases. This model was dependent on specific technology because forensic issues related to UNIX and Windows NT/2000 operating systems were thoroughly discussed. No information flow and data integrity issues were discussed.

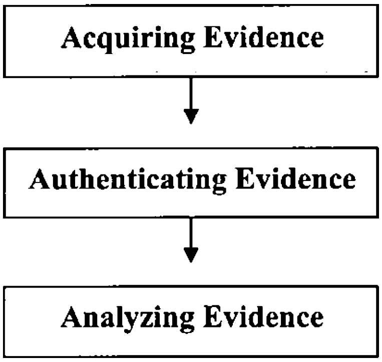


Fig 2.3: Kruse and Heiser Model [13]

2.3 America's Department of Justice Model [14]

To investigate electronic crime scene America's department of justice (DOJ) proposed a process model which was a guide for first responders, by adding a new component called reporting to "Kruse and Heiser model". It included collection, examination, analyzing and report phase. This was a guide to first responders. In this model, firstly forensic procedure was identified and then was discussed how to support it. In this paper, traditional physical forensic method and knowledge was applied to digital electronic evidence. The process given in this model was generic and has capacity to be used for most digital devices. In this model, three things regarding evidence were discussed: first location of evidence where possibly it presence, secondly type of crime which is possible with that evidence and lastly the types of evidence that may be present on electronic devices. The analysis of this model looks as the product of examination phase and was improperly defined. Examination and Analysis phases were confusing.

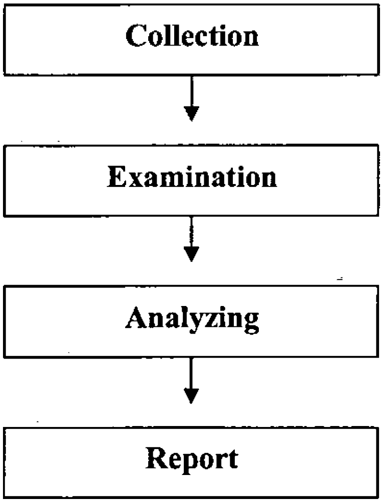


Fig 2.4: America's Department of Justice Model [14]

2.4 Digital Forensic Research Working Group Model [8]

Digital Forensic Research Working Group (DFRWS) developed a model having seven stages. The basic stages were identification, preservation, collection, examination, analysis, presentation and decision. This was a comprehensives model as it suggested new stage i.e. presentation. A very unique and important thing of this model was that it was not developed by law enforcement. This model was developed by a group of experts which was lead by academia. This effort was accepted by scientific community and they became aware of challenges of digital forensic. DFRW pointed out that "analytical procedures and protocols are not standardized nor do practitioners and researchers use standard terminology". This was a generic model which was used for all digital systems present at that time. It was so simple to provide tool requirements and test procedures.

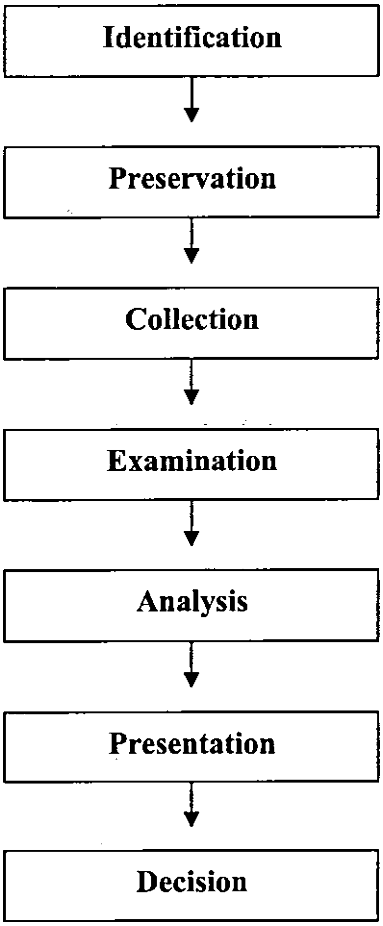


Fig 2.5: Digital Forensic Research Working Group Model [8]

2.5 Reith, Carr and Gunch Model [9]

Reith, Carr and Gunch improved the model and proposed an Abstract model of the digital forensic procedures by adding three new stages. The stages in this model were preparation, approach, strategy, preservation, collection, examination, analysis, presentation and returning evidence. An abstract model of the digital forensic procedure was given after exploring the development of the digital forensic process, their comparisons, analysis and contrasts four particular forensic methodologies. This model addressed some of the shortcomings of previous models.

This model focused in-depth investigation procedures. The dependency of this model was not on any electronic crime and also on particular technology available at that time but provided no easy method for testing the model. Chain of custody during the investigation was missing. Categories of the model were defined too general for practical use.

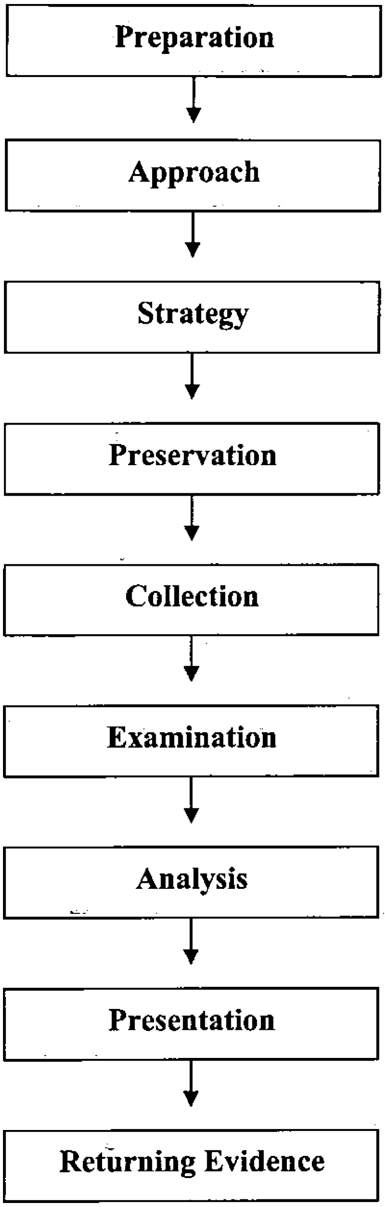


Fig 2.6: Reith, Carr and Gunch Model [9]

2.6 Sundresan Perumal Model [7]

Sundresan Perumal proposed a “Digital Forensic Model Based on Malaysian Investigation Process”. This was based on Malaysia Cyber Law. Fragile evidence collection phase, data collection phase and analysis phase were more focused in this model. The given model composed of seven stages including planning, identification, reconnaissance, analysis, result, proof and defense and diffusion of information. Malaysia Cyber Law was in focus in Sundresan model in all investigation processes. Very little reliability and accepted standards were present in the model. No evidence data mining system was discussed.

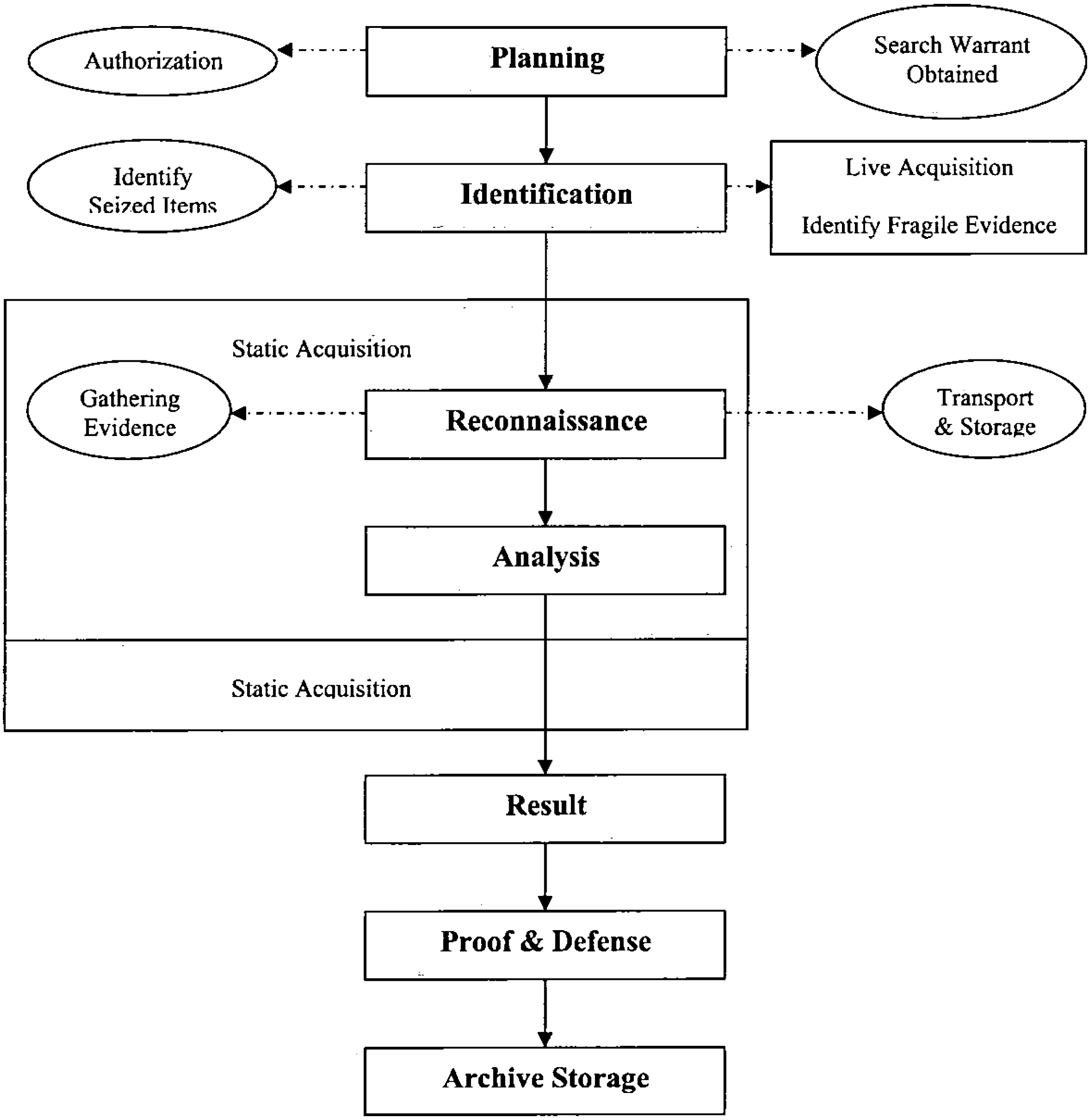


Fig 2.7: Sundresan Perumal Model [7]

2.7 Palantir Model [10]

Palantir proposed to design a framework through which effective partnership among organizations, so that they share information about incident, incident response, investigation tasks and resources as the result of which to eliminate the incidents, threat, attacks and pursue trial. Palantir [10] approach was motivated by *Incident 216* [6] attack, which was a distributed attack that took placed in 2004. In this incident the attacker launched attack on commercial institutions, higher education institutions and government offices of USA from foreign country, as a result of which integrity was compromised in multiple countries. To overcome such multi site attack, it was proposed to setup Information Sharing and Analysis Centers (ISACs), Incident Response Teams and Computer Emergency Response Teams (CERTs) globaly. Four phase Process model executed at Independent Center for Incident Management (ICIM) Palantir [10]. Chain of custody and data integrity issues was missing. No clear cut phase demarcation was discussed.

2.8 A Generic Model for Network Forensics [20]

A generic model for network forensics was presented by Emmanuel, Joshi and Rajdeep Niyogi. The model was built on the basis of previous digital forensic investigation models. The model was only for network forensics; therefore, only steps related to network forensics were included in this model. In this model, nine phases were included i.e. Preparation and authorization, Detection of incident / crime, incident response, collection of network traces, preservation and protection, examination, analysis, investigation and attribution and finally presentation. Majority of the proposed phases were present in studied investigation models but a few was different. No new and different phase and idea was suggested in this model.

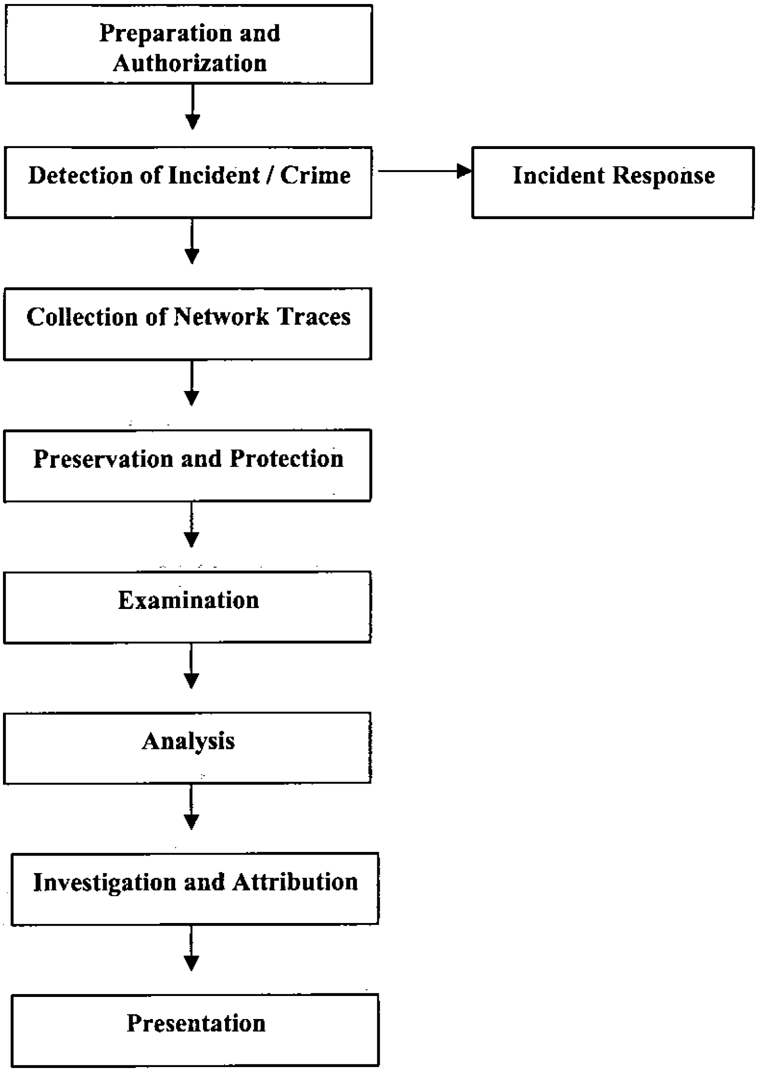

Preparation and Authorization
Detection of Incident / Crime
Incident Response
Collection of Network Traces
Preservation and Protection
Examination
Analysis
Investigation and Attribution
Presentation

Fig 2.8: A Generic Model for Network Forensics [20]

2.9 NR3C Procedure Guide [15]

National Response Centre for Cyber Crimes (NR3C) FIA Pakistan developed a Procedure Guide for Investigating Cyber Crime Cases (PGI3C). PGI3C basically provides Standard Operating Procedures (SOPs) for investigation officer. This guideline provides standard operating procedure to maintain integrity of electronic device so that law enforcement officers may fight against cyber crimes and cyber terrorism in a batter way. This guide is specially designed for the first responders, who are responsible for protecting an electronic crime scene and for the recognition, collection and preservation of electronic evidence.

2.10 Proactive and Reactive Digital Forensics Investigation Process [12]

In this paper, systematic literature review approach was adopted to identify and map the processes in digital forensics investigation. Two components proactive and reactive were proposed in this paper. Five phases i.e. identification, preservation, collection, analysis and final report are part of reactive component while proactive collection, event triggering function, proactive preservation, proactive analysis, preliminary report, decision and exit investigation are part of proactive component. Need of new forensic techniques and tools able to investigate anti forensic methods were given in this paper. Proposed process is not fully implemented due to more requirements. Information flow in model is not given. The need to move from proactive to reactive component or to exit whole investigation is confusing.

2.11 Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems [17]

In this paper, it is proposed to change the concept of traditional chain of custody of evidence. GPS, time stamp generator and biometrics devices are suggested in this paper to maintain chain of custody. New advanced forensic format (AFF) and resource description framework (RDF) are used to maintain chain of custody. Proposed model is for live data acquisition that is major problem where internet facility is not available. The need for common standard forensic format is required for this model which is missing. Information flow, polices and procedures are not given in this model.

2.12 Digital Forensic Standards

The digital forensic discipline developed rapidly, but very little international standardization with regard to processes, procedures or management has been developed so far [16]. It is hard and difficult to point out world wide standards in computer forensics, reasons of this is differences in legal system. Efforts are being made to change it. Many organizations, institutions, investigating and law enforcement agencies presents its best practices [24].

The only current work related to digital forensic is done by International Organization for Standardization (ISO). ISO/IEC 27037 standard was published in October 2012. The standard provides guidance on the identification, collection/gathering acquisition, marking, storage, transport and preservation of digital evidence. The scope covers traditional IT systems and media rather than vehicle systems, cloud computing etc. Prior to the release of ISO/IEC 27037, there were no globally accepted standards on acquiring digital evidence. Police have developed their own national guidelines and procedures for the acquisition and protection of digital evidence [11].

Every country has its own unique legislative system. A crime committed in one jurisdiction may not be crime in other. The standard will not replace specific legal requirements of any jurisdiction, but may assist in the facilitation of potential digital evidence exchange between jurisdictions [11].

The major problems regarding digital forensic standards are:

- Jurisdictional differences
- Training, Certification and Competence discrepancies
- Availability of experts [16]

The standard avoids using jurisdiction specific terminology. It will not cover analysis of digital evidence, nor its admissibility and weight. It mandates is not to use particular tools[11].

S .No	Model Name	Inventors	No of Phases
1	Computer Forensic Process	M. Pollitt	4
2	Kruse and Heiser Model	Kruse, Warren and Jay, G. Heiser	3
3	America's Department of Justice Model	Department of Justice	4
4	Digital Forensic Research Working Group Model	DFRWS	7
5	Abstract Model of the Digital Forensic Procedures	Reith, Carr and Gunch	9
6	Digital Forensic Model Based on Malaysian Investigation Process.	Sundresan Perumal	7
7	Palantir Model	Palantir	4
8	A Generic Model for Network Forensics	Emmanuel S. Pilli, R.C. Joshi, Rajdeep Niyogi	9

Table 2.1: Digital Forensic Investigation Models

Majority of Digital Forensic models give importance on technical accomplishment of investigation process as more of the model are developed by traditional forensic expert and technologist. Active and reactive strategy is given in studied models. No proactive approach was give to overcome cyber crimes.

Chapter 3

Problem Domain

3. Problem Domain

We have studied a number of digital forensic investigation models and methodologies in literature but there is no reliable and standard digital forensic model. Only set of actions and forensic tools are built from the experience of law enforcement officers, investigators, hackers and system administrators. The studied models do not provide a complete investigation method. Majority of the models concentrate on phase of the investigative process. Therefore, it is said that many cyber crimes are not investigated due to non-availability of standardized forensic model [9].

3.1 Problem Scenario

After cross examination of literature, survey of digital forensic models, some of common problems which I have drawn from all studied models are as follows:

- Modification in Previous Model
- Similar Approaches in Model
- Concentration on different areas of the investigation
- Concentration on sufficient evidence collection
- Focus on technical implementation of the investigation process
- Focus on efficiency and accuracy of evidence
- Information process flow
- Chain of custody
- Limited Scope on the model
- Lake of Standardization

3.1.1 Modification in Previous Model

It is studied after comparison and contrast of different models [5, 8, 9, 13, 14] that each preceding model modifies the previous model by adding some new process or stages or steps or components.

3.1.2 Similar Approaches in Models

In some of studied models [5, 8, 9, 13, 14] very similar approach has been adopted which has already been used in early model. Very few new and innovative approach has been discussed or adopted in any studied model. Sundresan Perumal Model [7], Palantir Model [10] and Generic Model for Network Forensics [20] adopted some different approach.

3.1.3 Concentration on different areas of the investigation

Some on the models [5, 13, 14] concentrate on different areas of the investigation i.e. preparation, analysis, examination and presentation, which means the other areas of entire model has been neglected. Digital Forensic Research Working Group Model [8], Reith, Carr and Gunch Model [9], Sundresan Perumal Model [7], Palantir Model [10] and Generic Model for Network Forensics [20] introduced some new stages.

3.1.4 Concentration on sufficient evidence collection

The main aim of these models [5, 7, 8, 9, 13, 14, 20] is to produce sufficient evidence that is presentable in the court of law. As an outcome, they do not give importance to main digital forensic investigation model [7]. A model should provide proactive approach to reduce the incident attacks.

3.1.5 Focus on technical implementation of the investigation process

After study and analysis of the digital forensic investigation models, it becomes clear that majority models focus on technical accomplishment of the investigation process. The reason is developed by traditional investigators and forensic experts [7]. Due to technical implementation the data integrity, chain of custody and information flow is reduced.

3.1.6 Focus on efficiency and accuracy of evidence

On the basis of existing models [5, 8, 9, 13, 14] forensic investigators focuses more into efficiency, accuracy and how to prepare the fragile evidence rather they should adopt proper methodology and procedure [7]..

3.1.7 Information process flow

Due to lack of information process flow, these models have very little integrity because no relation with internal and external rules, procedures standards etc. One of the major gaps in the existing models design is that they do not show the information process flow [7].

3.1.8 Chain of custody

Most of the existing models do not focus on issue such as chain of custody. For example, Reith themselves have noticed the absence of any explicit chain of custody in their model. This is a major flaw when one considers the different laws, practices, languages and so on [7].

3.1.9 Limited Scope of the model

Existing models are less extensive in their scope because majority models focus only on investigation process and do not present a comprehensive model focusing on entire processes of model [7].

3.1.10 Lack of Standardization

Lack of standardization has been studied in the existing model due to which there is no abstract reference model. This results in lack of standardized terminology, defining requirements, development of new techniques and tools for investigation [9].

3.2 Problem Statement

In existing literature, data integrity and documentation issues have been given no priority. Information process flow and backtrack were not followed in any model for processing, acquisition and preservation of evidence in such a way to maintain integrity through out the digital evidence collection method.

3.3 Research Objective

The aim of this research is a necessary feature of the academic thesis and to pay thanks to the researchers in this area who have contributed and enhanced much in the field of digital forensic investigation model. This research will provide the chance for researchers and academia to work in the field of digital forensic investigation. The main emphasis of this research is to discuss enhancing data integrity and documentation for digital forensic investigation model. During the research, different aspects, standards, requirements and procedures of digital forensic investigation models are discussed and analyzed along with positive and negative aspects.

In this thesis, I have compared and contrasted different forensic method, procedures, framework and principles on the basis of which I discuss the main and necessary components and phases any digital forensic investigation model should have.

Chapter 4

Proposed Solution

4. Proposed Solution

With the advancement of technology and new requirements such a model should be designed to fulfill new requirements. The main emphasis of our research is to design a Digital Forensic Investigation Model through which integrity of information and data remain save.

4.1 Main Features of Proposed Model

In proposed model, a new phase Hypothesis has been introduced, which will enhance data integrity and documentation procedure for digital forensic investigation model. Following are the main features of the proposed model:

- Concentration on all Phases of Model
- Documentation and Chain of Custody
- Data Integrity
- Iteration in Phases
- Information Flow

4.1.1 Concentration on all Phases of Model

In the proposed model, equal concentration has been given on all phases of models. I observed in studied models that more concentration was on investigation processes. So, there was need to be balanced in the every process or phase identified by a model and not to concentrate on a single process.

4.1.2 Documentation and Chain of Custody

In proposed model, documentation and chain of custody has been given most priority in order to maintain integrity. Since beginning to the last phase, complete documentation procedure has been followed. Every internal and external person who has any relation throughout the model has been documented.

4.1.3 Data Integrity

Data integrity in the proposed model is achieved by restricting any involvement or influence of any internal and external factor. For this purpose, all types of security and technical measures have been adopted throughout the proposed model implantation.

4.1.4 Iteration in Phases

One of the main features of proposed model is that iteration in the phases has been proposed at any stage of a phase. If there is any error or mistake observed, you may go to previous phase and recheck the phase or procedure adopted in previous phase. In this way, chance of mistake has been minimized. This idea was not present in any of previous studied models.

4.1.5 Information Flow

In every phase of proposed model, information flow remains continue. Major information flow contains cyber crime law, policy, procedures, organization internal / external policy, standard operating procedures, legislation and instruction from Computer Emergency Response Team, Incident Response Team and Information Sharing and Analysis Centers.

Proposed model have eighteen phases i.e. Awareness, Preparation, Reporting, Authorization, Planning, Notification, Identification, Preservation, Search & Seizure, Collection, Transportation, Storage, Examination, Analysis, Hypothesis, Presentation, Proof/Defense and Archive.

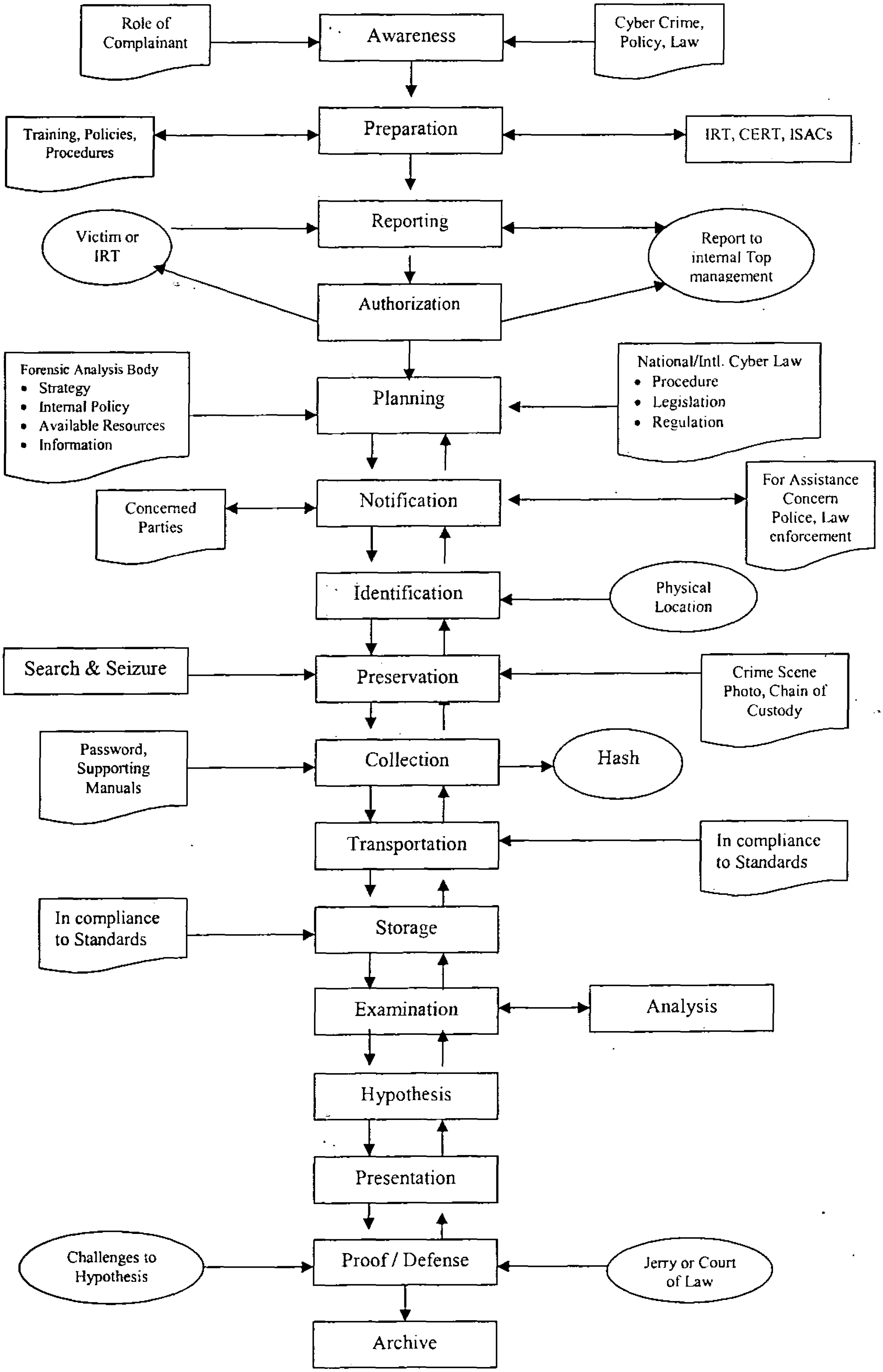


Fig 4.1: Proposed Model

4.2 Awareness

The first phase introduced in proposed model is awareness. Due to awareness phase, users of computer or electronic device, System / Network / Security administrator, IT Managers / Expert, Security person, first responder, victim, witness of events, IT Staff etc. come to know what to do, how to do it and what not to do to save evidence. A layman will be aware of what is cyber crime, unauthorized access, misuse of computer or electronic device, copy / delete / change in any electronic data or file, email data without authorization, cyber crime law / punishment and digital forensic investigation. The awareness should be created in every organization, institutions, universities, Govt. offices, public and private companies and at every place where computer / digital device is used.

The awareness phase is made explicit in this model. Most of earlier models do not show this phase which is a weakness of such models. A documented campaign for awareness should be started for batter understanding.

4.3 Preparation

The primary and major role of preparation phase is to create and develop the capability and capacity of appropriate people to handle incidents based on risk assessment and previous experiences. One of the important parts of preparation phase is to take necessary steps to prevent incidents from accruing. Security / Network administrators will provide a mechanism for the incident to be detected and confirmed for this purpose intrusion detection systems, firewalls, traffic flow measurement software are deployed at various strategic points and should be monitor regularly.

Regular training of all concerned individuals should be arranged to keep up to date with the latest security threats and security tools. Detailed documentation of previous incidents, policies, strategy, procedures should be prepared for internal and external communication for investigation of incident if required.

Basically preparation phase occurs prior to the incident and investigation. Training, education, experience and awareness of security threats will contribute in this phase. A thorough preparation phase increases the quality of incident handling and minimizes the risks and threats associated with as investigation. It is proposed to establish an Incident Response Team in every organization, which will coordinate with Local Incident Response Team or Computer Emergency Response Team (CERT) and Information Sharing and Analysis Centers (ISACs) to handle incidents.

4.4 Reporting

The main focus of this phase is to accurately detect and confirm that as serious incident or attack occurred as the result of which various security policies are violated and has been observed by Security / Network administrator by checking logs and alerts of intrusion detection systems, firewalls and other monitoring software. In a corporate environment, incident response team will do a brief analysis of a system to confirm that it has indeed been compromised.

After the confirmation of attack or incident, a response will be initiated depending upon the type of incident, organization internal policy / procedure and local law. Top management of organization will be informed immediately and permission will be taken to report to the Local Incident Response Team along with law enforcement and cyber crime investigator. Victim of cyber crime will report to Authority after filling or registering the case. Organization internal incident response team will document all procedures, timing of incident, information shared within / outside the organization and preserve all logs and equipment for investigation.

4.5 Authorization

In proposed model, Authorization phase starts after reporting to cyber crime investigator or law enforcement agency or Computer Emergency Response Team or police when the need for an investigation is identified / confirmed. In authorization phase, a proper authorization is given to start investigation about reported incident. Authorization is obtained from both internal and external management and also from the local enforcement team, in some cases company's management – where incident took place – may give verbal authorization to proceed in detailed investigation. In some cases, legal authorization with precise detail about what to investigate and what not, is required. The investigation should base on the local legal constraints, policies, law and jurisdiction as well as organization's rules and procedures. In this phase, search warrants are also obtained from management. Privacy rights of individuals and organization are not violated.

4.6 Planning

In proposed model, planning phase occurs before the actual notification of investigation is issued. This phase involves an initial understanding of the nature of the crime and activities like selection of tools required for electronic device investigations, building an appropriate team, assigning roles to each personal and history of previous investigation, if any, in that organization and issues faced at that time.

In planning phase, flow of information from both inside and outside of organization is required which may influence investigation. To finalize the planning, the investigator should know external rules, procedures, regulation, legislation and policies because they influence the investigation and are not in control of investigator. The investigating organization has its own policies, strategy and information which also play an important role in planning. Planning phase may need backtracking to obtain more authorization as the scope of investigation become larger. All the information of rules and policies are properly documented for further references.

4.7 Notification

In notification phase, concerned parties are informed that the investigation is taking place on their complaint of incident. Notification is issued by investigating agency which will further describe the investigating team members and scope of investigation.

In some cases, there is no need of notification where chance of destruction of digital evidence is realized and surprise rid policy may be adopted.

Notification may be sent to local law enforcement and police for awareness of investigation.

4.8 Identification

In identification phase, the exact physical location of digital device is searched where evidence is present. For identification, the iteration and trace back of previous phase may be needed. In the simplest cases, this may involve finding the computer used by attacker and confirming that it is the interest to the investigator.

In some cases, the physical crime scene and devices that were used to perform attack or unauthorized activity are difficult to identify. It may require tracing computers through multiple ISPs and possibly in other countries based on the knowledge of public and private IP addresses. IP addresses can easily be obtained by using the ping, nslookup, dig, tracert from a DNS server.

4.9 Preservation

In proposed model, preservation phase provide mechanism to secure the crime scene from all persons present at location from unauthorized access so that potential evidence may not be tempered or destroyed due to careless situation.

The original data in the form of logs is stored on a back up device. A hash of all the data is taken and the data is protected. Standard procedures are used to ensure accuracy, reliability and integrity of preserved data. Chain of custody is strictly enforced so that there is no unauthorized use or tampering. Another copy of data will be used for next phase of investigation so that original data is preserved. Crime scene is preserved by disallowing all people present near the scene from using any kind of digital device and other electromagnetic signal producing devices to be used within an affected radius.

Ensuring the necessary security and safety measures of all officials and related people at the crime scene and caring the integrity of all potential evidence is the target of preservation phase. It is necessary for the investigators to control the crime scene so that all kind of interference from surplus people should be restricted and completely prohibited. The greater the number of many people at the crime scene, the greater will be the chance to increase the possibilities for the corruption and damage of evidence.

To maintain integrity, suitable documentation and photography of the crime scene is an important part of preservation phase. All accessories present at crime scene, appearing screen of device, date and time, circumstance around the incident, reporting person, people present at crime scene names, ages and role should be properly documented.

4.10 Search and Seizure

The investigator should conduct an initial search and survey for evaluating the crime scene identifying potential sources of evidence and formulating an appropriate search plan. All the electronic equipment, personal computer, laptop, power adapter, cradle, external memory card, cable, accessories, communication device may contain evidence so investigating team should seize all the items.

4.11 Collection

After identification and preservation, the most important phase in proposed model is collection of evidence from digital device. Collection of evidence is the most tricky and complicated part because data may be of huge quantity and possibility of any change.

It is proposed to lay down standard procedures, software, hardware and reliable forensic tools to gather maximum potential evidence so that to minimize the impact to the victim which will ensure evidence acceptability in court or disciplinary action. In collection phase, the investigating organization or law enforcement person will take custody of the evidence so that to preserve and analyze normal procedures are imaging of hard disk, hashing, write protection. It is also proposed to collect written passwords, all type of manuals and related documents, printout etc. Integrity, authenticity and vahdity of digital evidence in collection phase is ensured by using standardized and accepted procedures.

4.12 Transportation

In proposed model, transportation of digital evidence and all equipments present at crime scene play an important role for further investigation. During transportation integrity, chain of custody, documentation and packing are very necessary steps. Appropriate procedures should be followed during physical transfer of computer and devices to a secure environment. Before packing in separate anti-static bags, all collected sources of evidence should be marked, recognized and labeled properly. All accessories and devices should be put in separate anti-static envelop and sealed before putting in evidence bag. To avoid communication, radio frequency and electromagnetic waves evidence bag should be in complete isolation state. Safety precautions to avoid shock, excessive pressure, humidity or temperature are necessary to move evidence bags to safe place where further investigation may be started.

4.13 Storage

In proposed model, storage has been given importance after transportation to forensic lab because in most cases examination cannot take place immediately. The evidence should be stored in secure area where any electromagnetic radiations, dust, heat, moisture and unauthorized entry be avoided completely, so that integrity and safety of potential evidence not be compromised. To maintain chain of custody, National Institute of Standards and Technology (NIST) provides a guideline for proper transportation and storage mechanism.

4.14 Examination

On the basis of identification and collection phase, large amount of collected data having potential evidence will be examined in detail in examination phase of proposed model. Before starting examination of evidence, suitable number of evidence backups should be taken and preserved to maintain integrity and further investigation / proof in court. The main aim of this phase is to recognize obvious piece of digital evidence and make evidence visible on the basis of its originality, integrity and location.

It is proposed to convert huge data into manageable size by clustering into groups for further analysis. Tampered, damaged, hidden and camouflaged data should be retrieved and repaired by the forensic experts in examination phase of proposed model. Unrelated, redundant and duplicate data / information should be removed from huge data and only minimum representative form of data having digital evidence should be saved for further investigation. Automated and systematic techniques to exam the data will be used to reach the evidence. For this purpose, proper tools should be used. The major steps performed in examination phase of proposed model are searching specific words, data filtering, pattern recognition related to crime or incident, personal information like contact list, personal appointments, email, work scheduler, sms, voice messages, documents, passwords, files, directories, signature, file extension checking. The capabilities and limitations of the forensic tools used by examiner or investigator for evidence examination play an important part in this phase.

After completion of examination phase, date and exact time of examination performed, name of examiner or investigator, results and finding and other details performed in examination through tool must be documented.

4.15 Analysis

On the basis of results of examination phase, analysis is performed using forensic tool. As analysis is complicated phase so a toolbox of utilities is required to built for complete data analysis. In analysis phase, specific indicators of crime are extracted which will be correlated to the specific group of data to reconstruct the attack. Important steps performed in analysis phase of proposed model are reconstruction of event, significance of the results of examination phase, identification / relationship between fragments of data, analysis of hidden data, arriving at proper conclusion, confirmation of suspicious activity, data mining; using tools for the purpose of analysis will give up better output. All results and finding of analysis phase should be documented completely and accurately.

4.16 Hypothesis

In proposed model, hypothesis is very important phase because on the basis of examination and analysis, incident is reconstructed to answer the questions of what, when, who, why, how and where it happened. For creation of hypothesis, the role of each object is examined and classified. For example, the investigator or examiner, after checking an executable file will conclude and make hypothesis that this executable file play a role for incident by creating port or damaging data. After identification of all objects, they are grouped and sequence of event will be created to finalize the hypothesis.

After creating sequence of events / incidents and finalizing hypothesis, they must be properly documented.

4.17 Presentation

In proposed model, presentation phase is the most essential phase because it provides the requirements precise in word “Digital Forensic”. The presentation phase will prove the hypothesis results. Hypothesis must be presented in an understandable language to a verity of people within and outside the organization where incident happen, it may include company internal management, police, legal persons, law enforcement officials, technical expert, corporate manager, court of law, jury and other investigators for questioning.

Various standard procedures, tools, techniques, statistical data, methodology and terminology used and are part of various phases of investigation should be given in easy words so that a layman can understand it. A detailed summary of outcome / results of different phases of proposed model and conclusion should be presented. Along with report, the digital evidence, complete backup of extracted data, chain of custody documents, printouts etc. are necessary to provide.

Depending of the nature of crime, presentation may be organization internal management, in some court or jury; therefore, a systematic documentation procedure will be adopted throughout the model so that to meet the requirements as may be.

4.18 Proof / Defense

After presentation phase, proof / defense to hypothesis or digital evidence starts. The experience of forensic examiner, forensic tools used, investigator knowledge, standards and procedures, chain of custody and integrity, printout, copy of digital evidence, crime scene etc. are all challenged before court or jury or disciplinary committee. The forensic examiner has to prove the validity of his / her hypothesis, results and finding against the criticism and challenges. Successful challenge to the finding wills rollback whole process of investigation and forensic experts have to bring more evidence with strong hypothesis.

4.19 Archive

The final phase in the proposed model is archive phase. In this phase, all the steps and phases adopted in investigation and evidence finding will be reviewed for improvement. Review will identify the areas where improvement of procedures; polices and standards is required for future investigation.

Information will be disseminated from investigating agency to victim, other organizations, researcher, security experts, computer emergency response team and law maker to improve policies and procedures for future challenges. Physical and digital property will be returned to owner.

All documentation and copy of evidence will be deposited into database to make archive for future references. This collection is a fruitful area for researchers and investigators to develop advance forensic tools, software, future security polices and techniques to enhance digital forensic investigation field.

The main benefit of this archive is that other Independent Center for Incident Management (ICIM), Computer Emergency Response Teams (CERTs) in and outside the country, local Information Sharing and Analysis Centers (ISACs), digital forensic investigating agencies around the world can get benefits for their forensic investigation.

Chapter 5

Implementation

5. Implementation

5.1 Step 1: Documented procedure for awareness

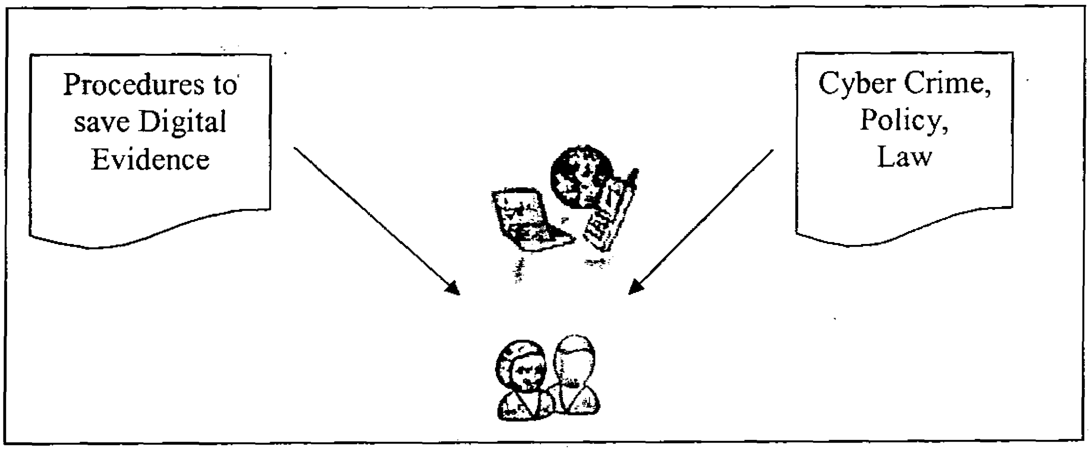


Fig 5.1 Step 1: Documented procedure for awareness

In step 1, a documented procedure will be adopted for awareness about cyber crime, misuse of IT infrastructure and how to know about incident happening and then to save digital evidence for further phase.

5.2 Step 2: Preparation for incident

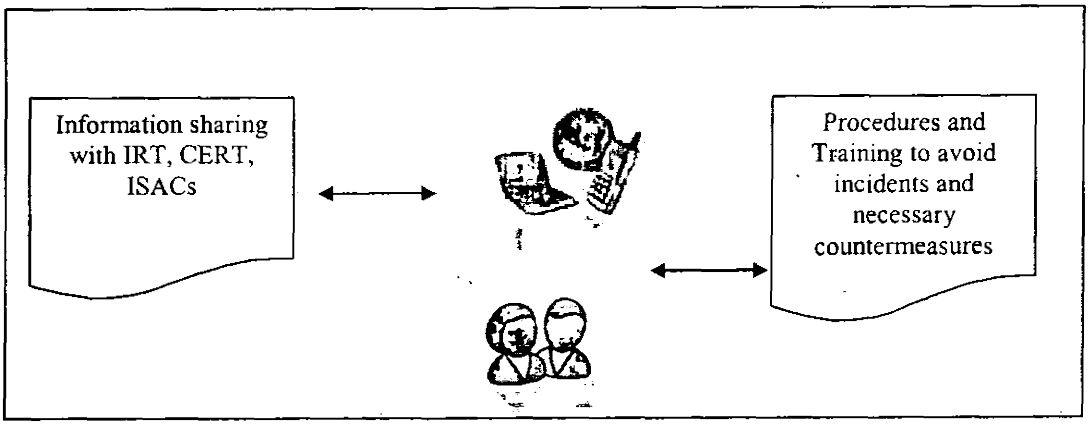

Information sharing with IRT, CERT, ISACs
Procedures and Training to avoid incidents and necessary countermeasures

Fig 5.2 Step 2: Preparation for incident

To avoid and overcome the incidents continuous training of IT staff, interaction with IRT, CERS and ISACs is very important.

5.3 Step 3: Reporting of incident

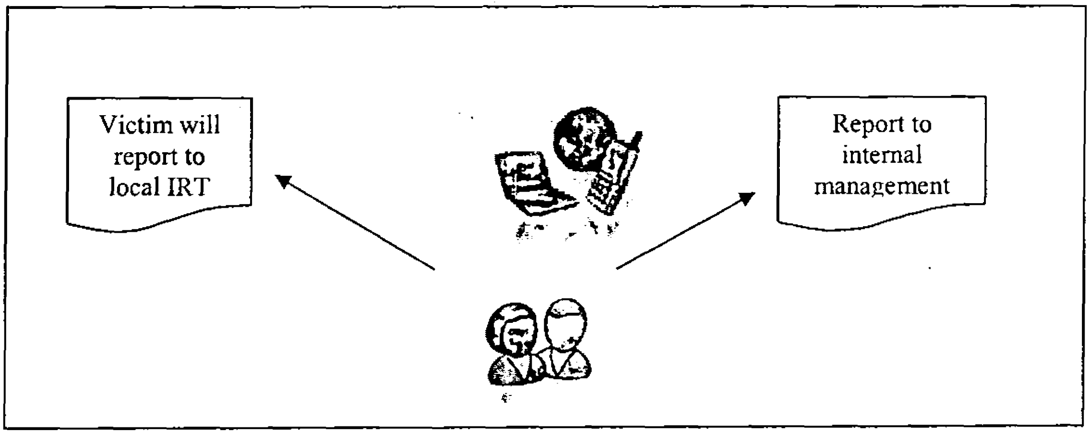

Victim will report to local IRT
Report to internal management

Fig 5.3 Step 3: Reporting of incident

In step 3, victims will report to internal or local incident response team and may be internal management about incident. On the basis of reporting, management or investigation authority will analyze whether to proceed further or to decide that there is no need to investigate.

5.4 Step 4: Finding of incident

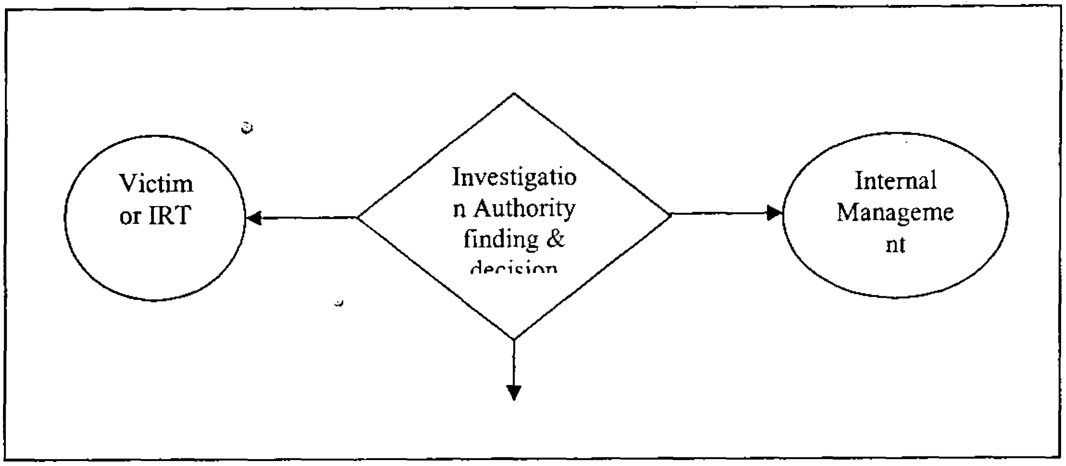


Fig 5.4 Step 4: Finding of incident

In step 4, investigating authority will analyze the reported incident and will find if there some real incident happened and there is a need to proceed further. If there is no need then it will inform victim or local IRT and management that there is nothing and whether there is a need for proceed further and start next phase.

5.5 Step 5: Authorization for investigation

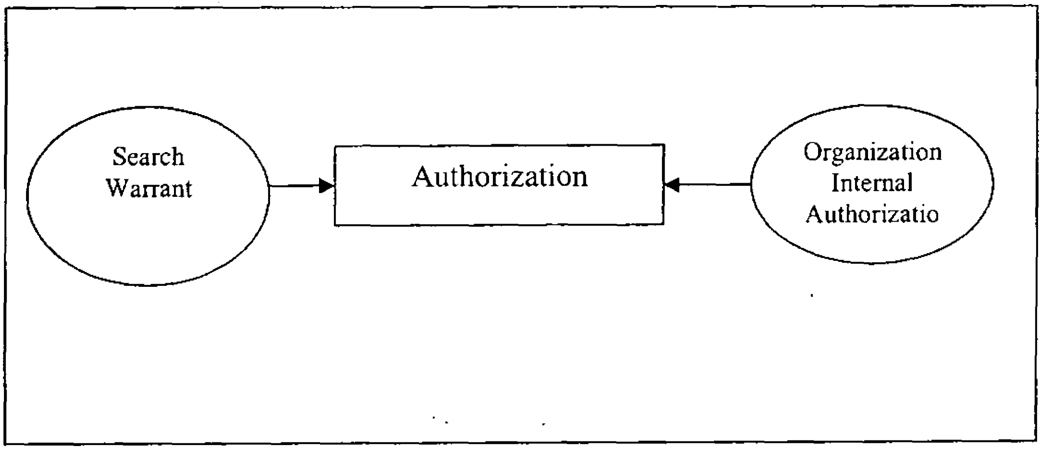


Fig 5.5 Step 5: Authorization for investigation

In step 5, investigation authority will take written permission from victim or organization where incident happened to start investigation and will decide the scope of investigation. Search warrant will be obtained to start finding.

5.6 Step 6: Planning to start investigation

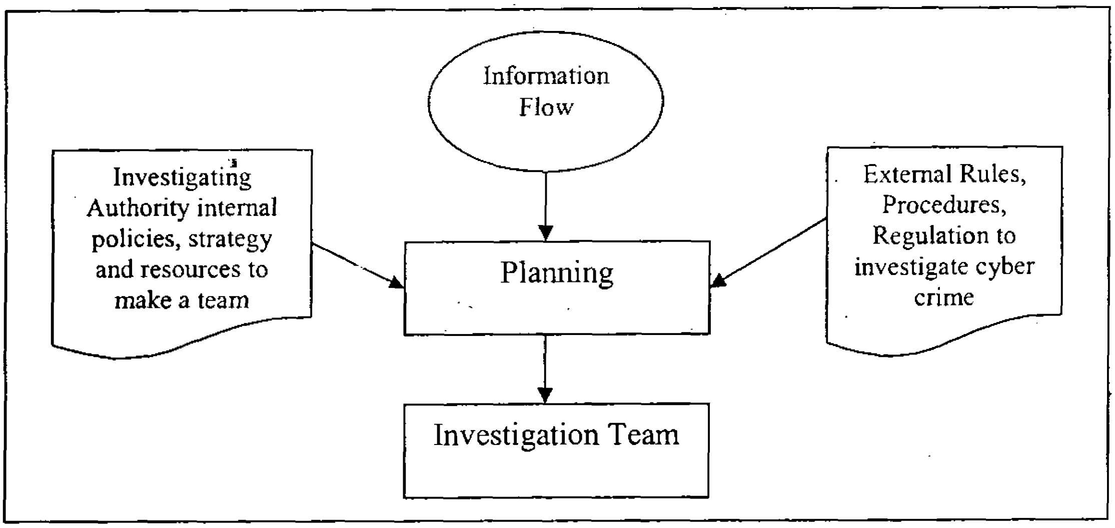

Information Flow
Investigating Authority internal policies, strategy and resources to make a team
Planning
External Rules, Procedures, Regulation to investigate cyber crime
Investigation Team

Fig 5.6 Step 6: Planning to start investigation

In step 6, investigation team will be prepared on the basis of available human resource capacity, tools, internal and external rules, procedures, policies and regulation. Team will prepare investigating plan to proceed further.

5.7 Step 7: Notification for investigation

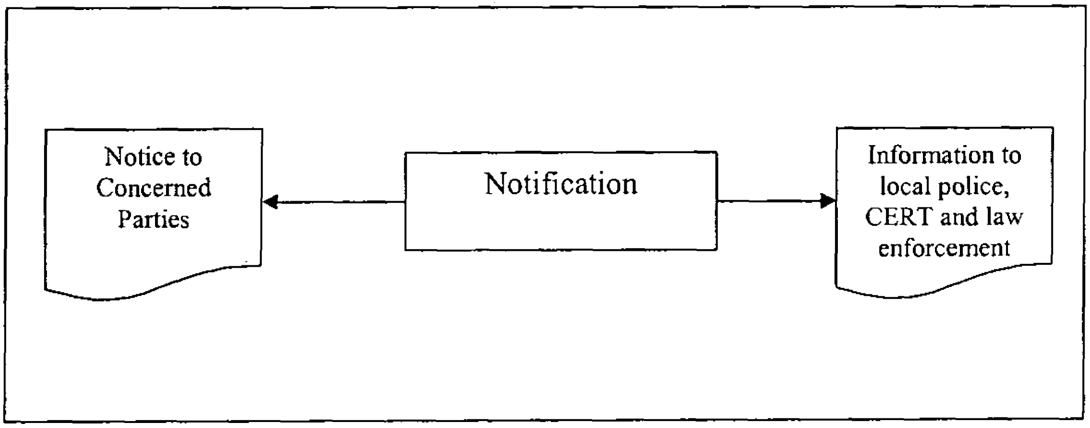

Notice to Concerned Parties
Notification
Information to local police, CERT and law enforcement

Fig 5.7 Step 7: Notification for investigation

In step 7, notification will be issued to victim or organization where incident happened to inform that investigation team has been announced to start investigation. Further, local police, law enforcement and local CERT will be informed for cooperation.

5.8 Step 8: Identification of incident location

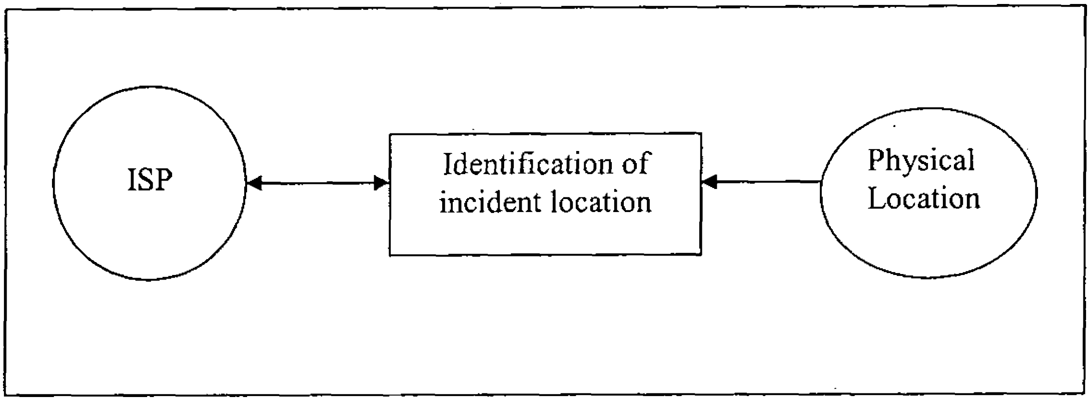


Fig 5.8 Step 8: Identification of incident location

In step 8, actual physical location of incident will be searched. Form this purpose, information sharing with ISP is done.

5.9 Step 9: Preservation of crime scene

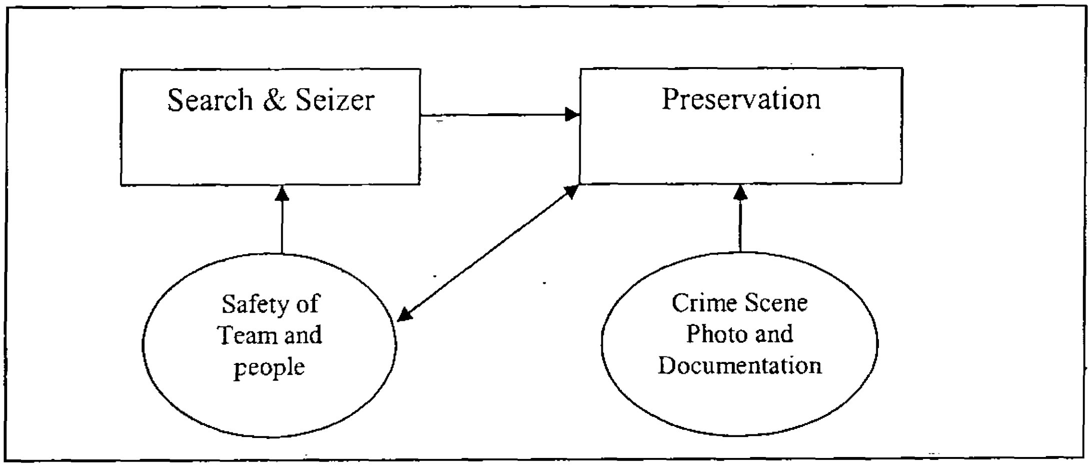
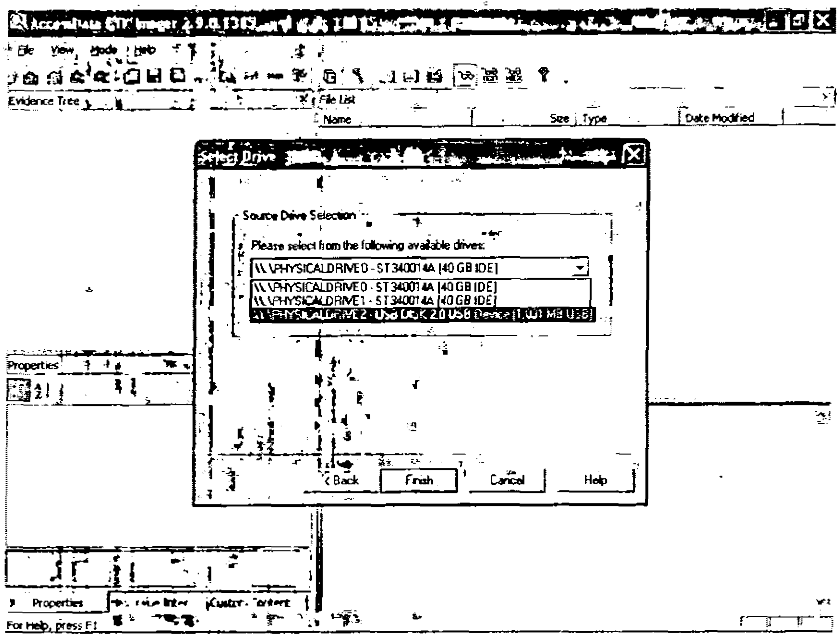

Search & Seizer
Preservation
Safety of Team and people
Crime Scene Photo and Documentation

Fig 5.9 Step 9: Preservation of crime scene

In step 9, crime scene will be preserved in order to search and seize all equipment and accessories. All electronic equipments that are involved in crime will be preserved in the presence of witness and necessary safety measures will be adopted. Chain of custody, data integrity and documentation procedure are necessary actions to be taken at the spot.

5.10 Step 10: Selection of source drive for image



Source Drive Selection

Please select from the following available drives:

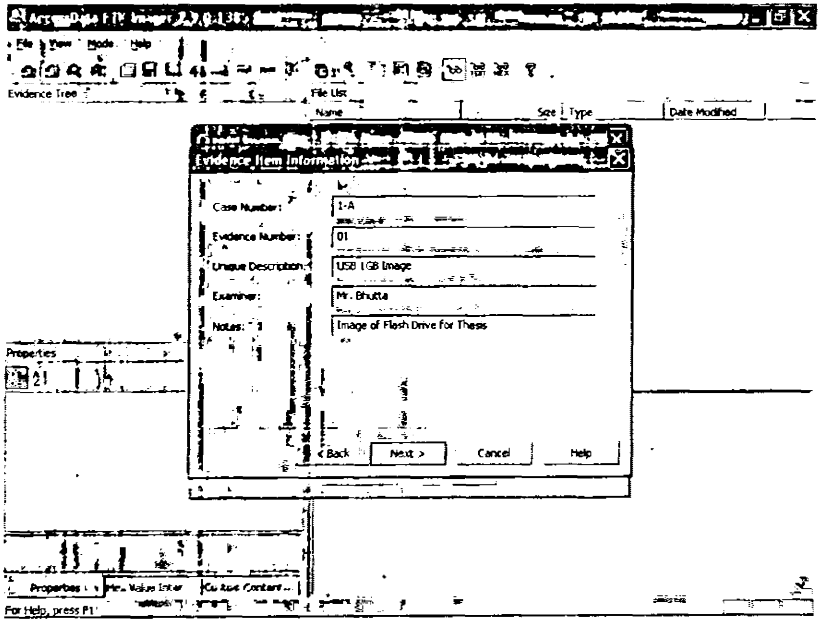
\\.\PHYSICALDRIVE0 - ST340014A [40 GB IDE]

\\.\PHYSICALDRIVE0 - ST340014A [40 GB IDE]
\\.\PHYSICALDRIVE1 - ST340014A [40 GB IDE]
\\.\PHYSICALDRIVE2 - USB DISK 2.0 USB Device [1,031 MB USB]

Fig 5.10 Step 10: Selection of source drive for image

In step 10, image of physical derive will be taken by using FTK Imager.

5.10.1 Step 10.1: Evidence item information



Case Number: 1-A

Evidence Number: 01

Unique Description: USB 1GB Image

Examiner: Mr. Bhutta

Notes: Image of Flash Drive for Thesis

Fig 5.10.1 Step 10.1: Evidence item information

In step 10.1, evidence item information i.e. Case Number, Evidence Number, Unique Description, Examiner name and Notes will be given for unique reference.

5.10.2 Step 10.2: Creation of image

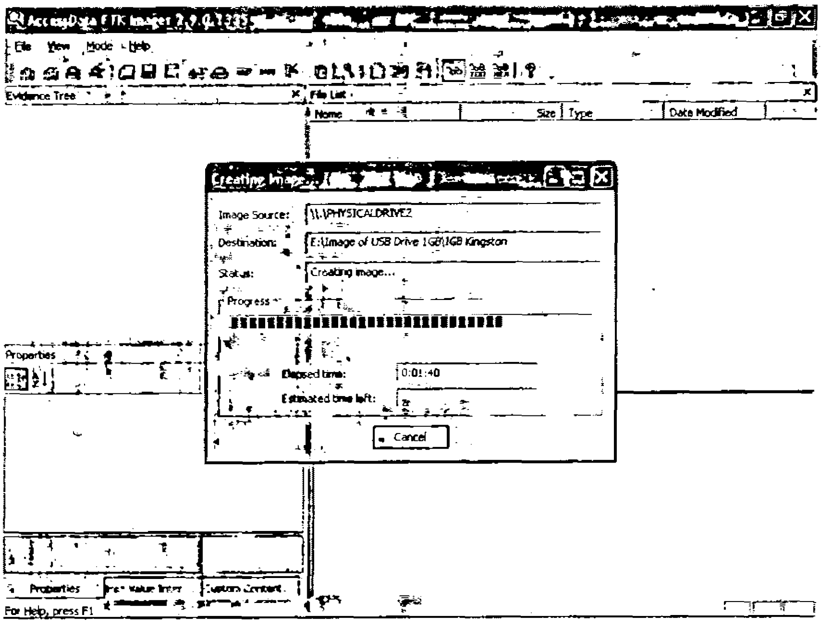


Image Source: \\.\PHYSICALDRIVE2

Destination: E:\Image of USB Drive 1GB\1GB Kingston

Status: Creating image...

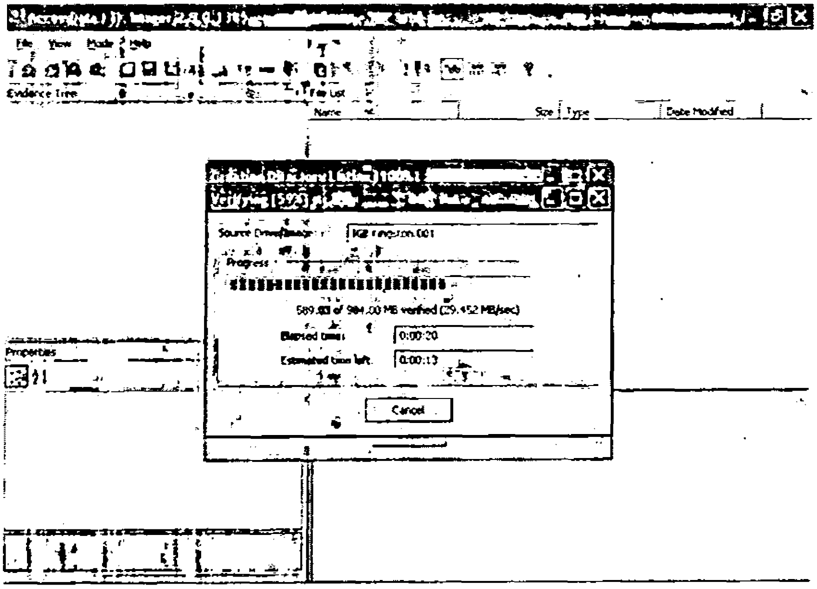
Elapsed time: 0:01:40

Estimated time left:

Fig 5.10.2 Step 10.2: Creation of image

In step 10.2, image storage location will be selected. On the basis of drive size more space will be required if compression option is not selected.

5.10.3 Step 10.3: Verification of image



Source Drive/Image: 1GB Kingston.001

589.[illegible] of 984.00 MB verified (29.452 MB/sec)

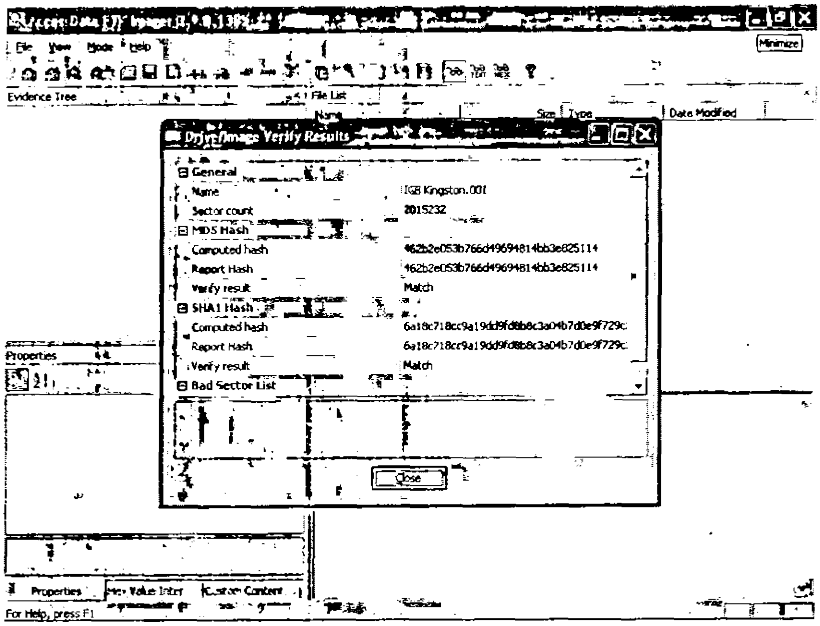
Elapsed time: 0:00:20

Estimated time left: 0:00:13

Fig 5.10.3 Step 10.3: Verification of image

In step 10.3, after completion of image, verification process will be started and total image size will be displayed after calculation.

5.10.4 Step 10.4: Verified results



General
Name 1GB Kingston.001
Sector count 2015232
MD5 Hash
Computed hash 462b2e053b766d49694814bb3e825114
Report Hash 462b2e053b766d49694814bb3e825114
Verify result Match
SHA1 Hash
Computed hash 6a18c718cc9a19dd9fd8b8c3a04b7d0e9f729c
Report Hash 6a18c718cc9a19dd9fd8b8c3a04b7d0e9f729c
Verify result Match
Bad Sector List

Fig 5.10.4 Step 10.4: Verified results

In step 10.4, after completion of drive image, verified result will be collected including MD5 and SHA1 hash, total sector of drive and bad sector result. Hash information will be documented and signed by victim and witness.

5.11 Step 11: Storage and transportation of evidence

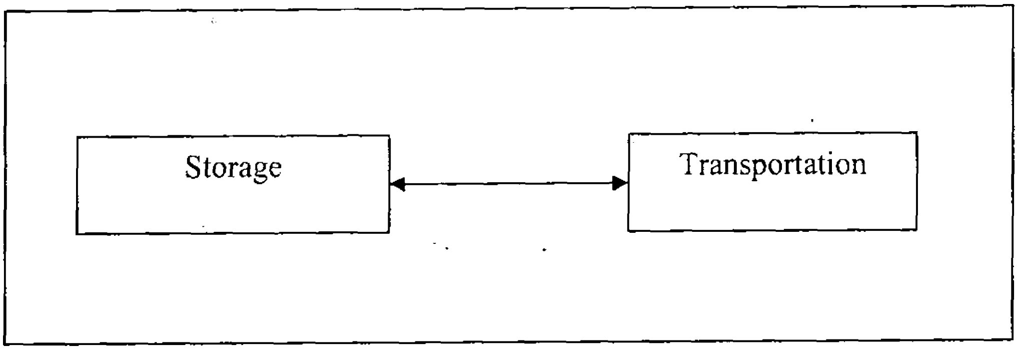
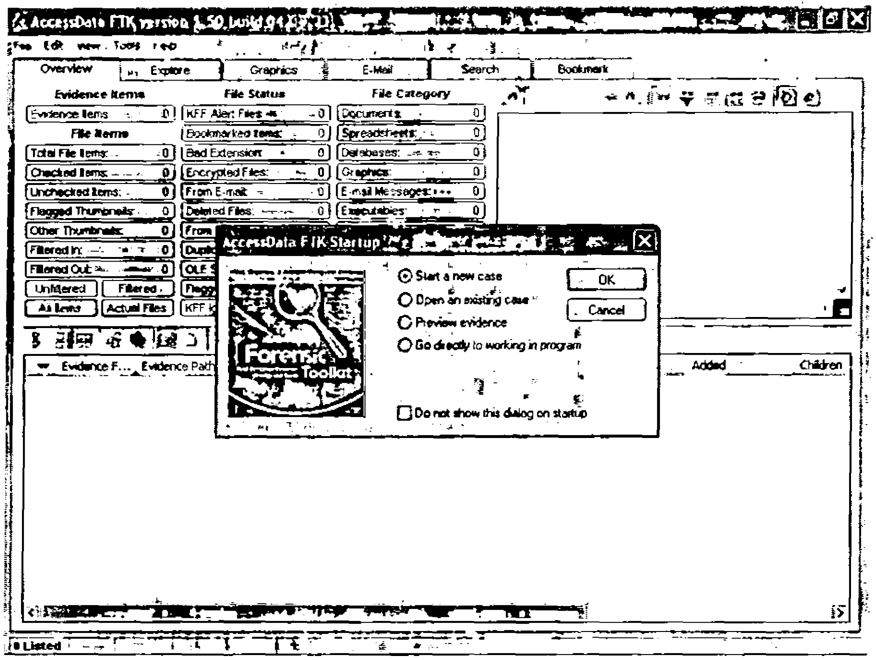


Fig 5.11 Step 11: Storage and transportation of evidence

In step 11, all equipment, accessories and electronic devices will be tagged individually and packed in anti-static bags after marking them. During transportation and storage, all bags should be in complete isolation so that any type of signals, communication and electromagnetic waves may not destroy the evidence.

5.12 Step 12: New case startup



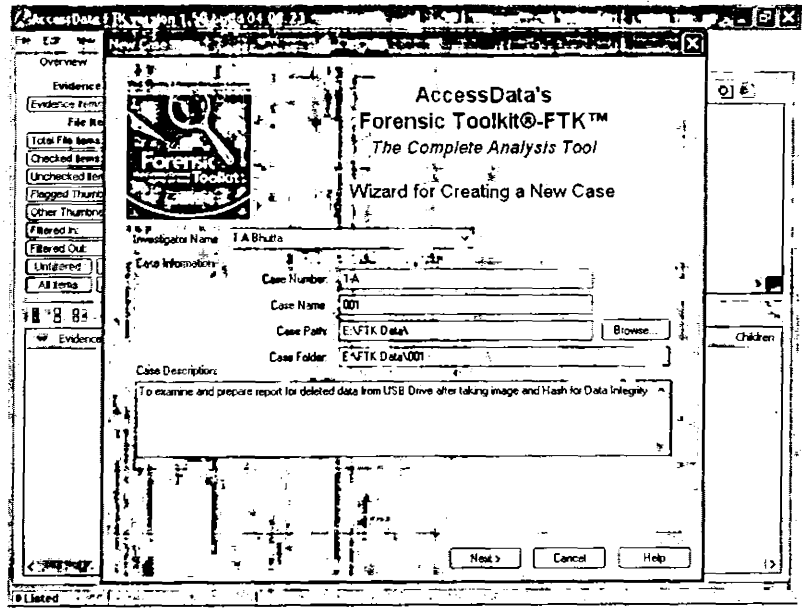
Evidence Items: 0
Total File Items: 0
Checked Items: 0
Unchecked Items: 0
Flagged Thumbnails: 0
Other Thumbnails: 0
Filtered In: 0
Filtered Out: 0
KFF Alert Files: 0
Bookmarked Items: 0
Bad Extension: 0
Encrypted Files: 0
From E-mail: 0
Deleted Files: 0
Documents: 0
Spreadsheets: 0
Databases: 0
Graphics: 0
E-mail Messages: 0
Executables: 0

● Start a new case
○ Open an existing case
○ Preview evidence
○ Go directly to working in program
□ Do not show this dialog on startup

Fig 5.12 Step 12: New case startup

In step 12, a new case will be started by using FTK 1.50 to examine and analyze the potential evidence collected in the form of Hash.

5.12.1 Step 12.1: New case information

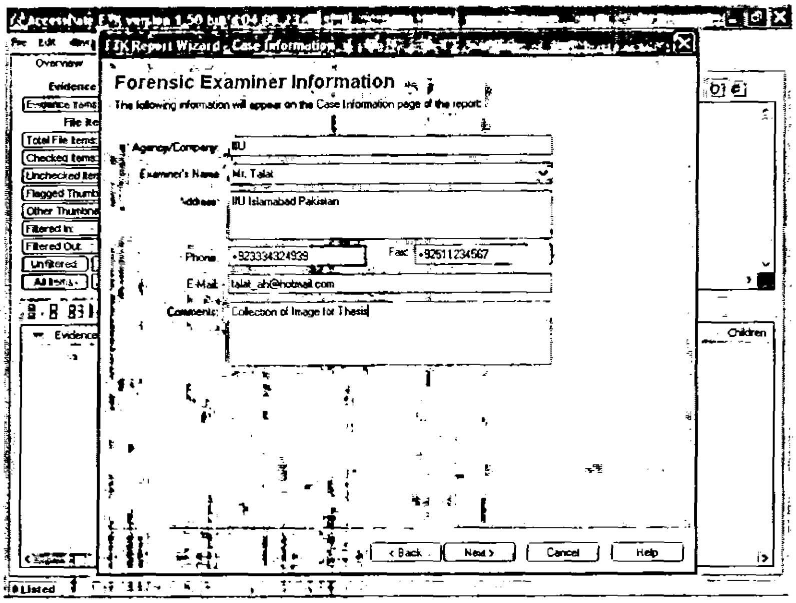


Investigator Name: T A Bhutta
Case Information
Case Number: 1-A
Case Name: 001
Case Path: E:\FTK Data\
Case Folder: E:\FTK Data\001
Case Description: To examine and prepare report for deleted data from USB Drive after taking image and Hash for Data Integrity

Fig 5.12.1 Step 12.1: New case information

In new case wizard some information will be given for record, that include examiner name, case number, case name, path to save all evidence data for further reference and usage and finally case description.

5.12.2 Step 12.2: New case examiner information

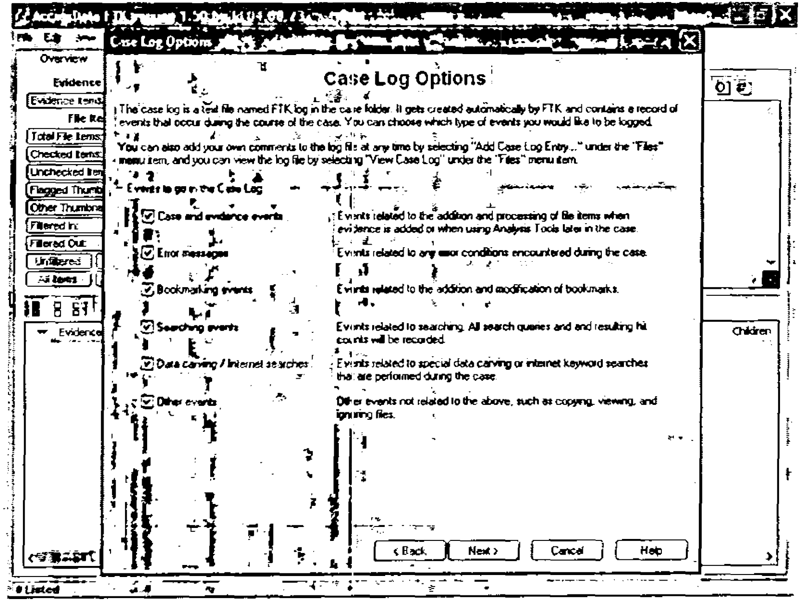


Forensic Examiner Information
The following information will appear on the Case Information page of the report:
Agency/Company: IIU
Examiner's Name: Mr. Talat
Address: IIU Islamabad Pakistan
Phone: +923334324939
Fax: +92511234567
E-Mail: talat_ah@hotmail.com
Comments: Collecion of Image for Thesis

Fig 5.12.2 Step 12.2: New case examiner information

In step 12.2, detailed information of examiner will be noted for reference.

5.12.3 Step 12.3: Selection of options for new case



Case Log Options

The case log is a text file named FTK.log in the case folder. It gets created automatically by FTK and contains a record of events that occur during the course of the case. You can choose which type of events you would like to be logged.

You can also add your own comments to the log file at any time by selecting "Add Case Log Entry..." under the "Files" menu item, and you can view the log file by selecting "View Case Log" under the "Files" menu item.

Events to go in the Case Log

☑ Case and evidence events — Events related to the addition and processing of file items when evidence is added or when using Analysis Tools later in the case.

☑ Error messages — Events related to any error conditions encountered during the case.

☑ Bookmarking events — Events related to the addition and modification of bookmarks.

☑ Searching events — Events related to searching. All search queries and and resulting hit counts will be recorded.

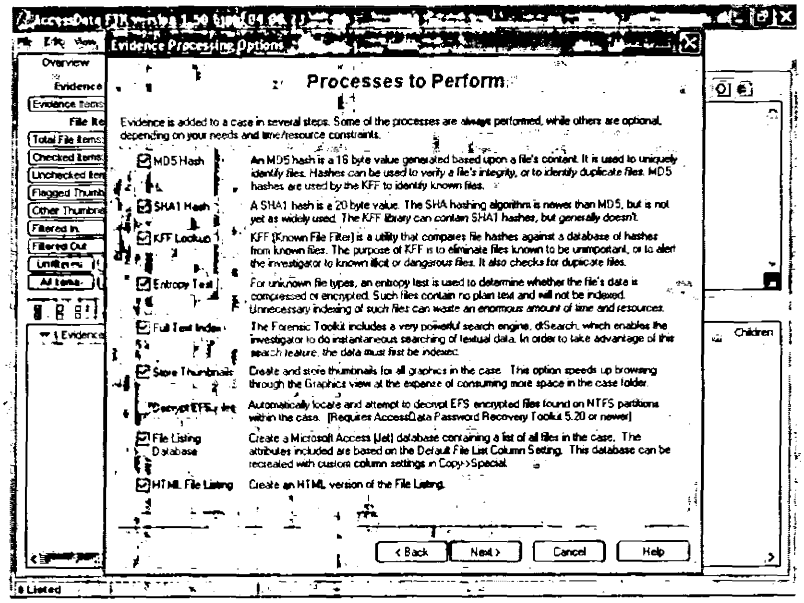
☑ Data carving / Internet searches — Events related to special data carving or internet keyword searches that are performed during the case.

☑ Other events — Other events not related to the above, such as copying, viewing, and ignoring files.

Fig 5.12.3 Step 12.3: Selection of options for new case

To maintain integrity and documentation of all events performed by examiner, case log options are selected. By default all events are checked.

5.12.4 Step 12.4: Evidence processing options



Processes to Perform

Evidence is added to a case in several steps. Some of the processes are always performed, while others are optional, depending on your needs and time/resource constraints.

☑ MD5 Hash — An MD5 hash is a 16 byte value generated based upon a file's content. It is used to uniquely identify files. Hashes can be used to verify a file's integrity, or to identify duplicate files. MD5 hashes are used by the KFF to identify known files.

☑ SHA1 Hash — A SHA1 hash is a 20 byte value. The SHA hashing algorithm is newer than MD5, but is not yet as widely used. The KFF library can contain SHA1 hashes, but generally doesn't.

☑ KFF Lookup — KFF (Known File Filter) is a utility that compares file hashes against a database of hashes from known files. The purpose of KFF is to eliminate files known to be unimportant, or to alert the investigator to known illicit or dangerous files. It also checks for duplicate files.

☑ Entropy Test — For unknown file types, an entropy test is used to determine whether the file's data is compressed or encrypted. Such files contain no plain text and will not be indexed. Unnecessary indexing of such files can waste an enormous amount of time and resources.

☑ Full Text Index — The Forensic Toolkit includes a very powerful search engine, dtSearch, which enables the investigator to do instantaneous searching of textual data. In order to take advantage of this search feature, the data must first be indexed.

☑ Store Thumbnails — Create and store thumbnails for all graphics in the case. This option speeds up browsing through the Graphics view at the expense of consuming more space in the case folder.

Decrypt EFS Files — Automatically locate and attempt to decrypt EFS encrypted files found on NTFS partitions within the case. [Requires AccessData Password Recovery Toolkit 5.20 or newer]

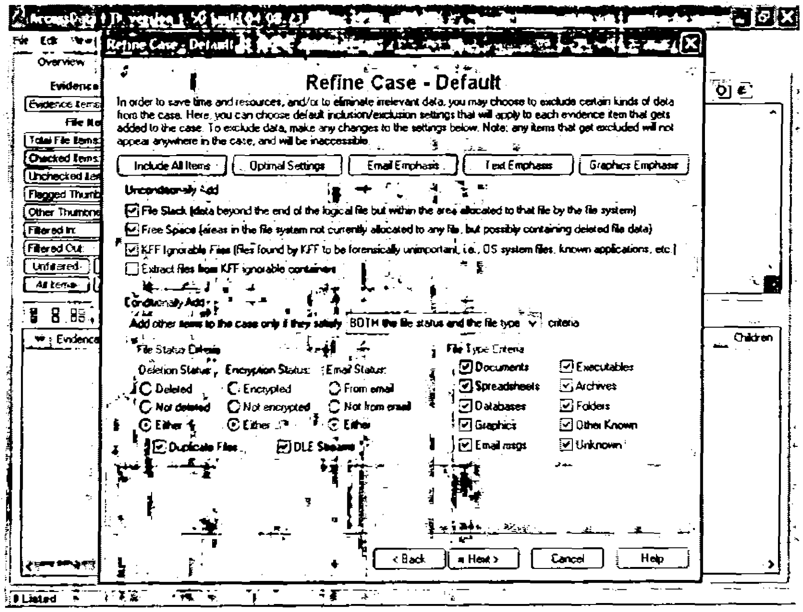
☑ File Listing Database — Create a Microsoft Access (Jet) database containing a list of all files in the case. The attributes included are based on the Default File List Column Setting. This database can be recreated with custom column settings in Copy->Special

☑ HTML File Listing — Create an HTML version of the File Listing.

Fig 5.12.4 Step 12.4: Evidence processing options

Processes to perform on evidence are selected; some processes are performed every time while others are on choice of examiner and resources.

5.12.5 Step 12.5: New case refinement



Refine Case - Default

In order to save time and resources, and/or to eliminate irrelevant data, you may choose to exclude certain kinds of data from the case. Here, you can choose default inclusion/exclusion settings that will apply to each evidence item that gets added to the case. To exclude data, make any changes to the settings below. Note: any items that get excluded will not appear anywhere in the case, and will be inaccessible.

Unconditionally Add

☑ File Slack (data beyond the end of the logical file but within the area allocated to that file by the file system)
☑ Free Space (areas in the file system not currently allocated to any file, but possibly containing deleted file data)
☑ KFF Ignorable Files (files found by KFF to be forensically unimportant, i.e., OS system files, known applications, etc.)
□ Extract files from KFF ignorable containers

Conditionally Add

Add other items to the case only if they satisfy BOTH the file status and the file type criteria

File Status Criteria

Deletion Status: ○ Deleted ○ Not deleted ● Either
Encryption Status: ○ Encrypted ○ Not encrypted ● Either
Email Status: ○ From email ○ Not from email ● Either
☑ Duplicate Files ☑ OLE Streams

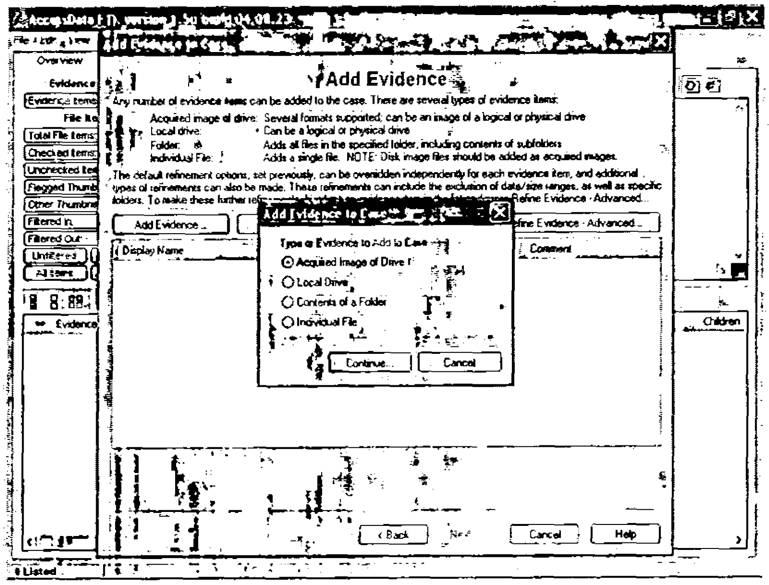
File Type Criteria

☑ Documents ☑ Executables
☑ Spreadsheets ☑ Archives
☑ Databases ☑ Folders
☑ Graphics ☑ Other Known
☑ Email msgs ☑ Unknown

Fig 5.12.5 Step 12.5: New case refinement

In this step, case is refined on the bases of required evidence. Emphasis on email, text and graphics are selected if required to save time and may be included all items to check.

5.12.6 Step 12.6: Addition of evidence



Add Evidence

Any number of evidence items can be added to the case. There are several types of evidence items:

Acquired image of drive:	Several formats supported; can be an image of a logical or physical drive
Local drive:	Can be a logical or physical drive
Folder:	Adds all files in the specified folder, including contents of subfolders
Individual File:	Adds a single file. NOTE: Disk image files should be added as acquired images.

The default refinement options, set previously, can be overridden independently for each evidence item, and additional types of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specific folders. To make these further ref[illegible] Refine Evidence - Advanced...

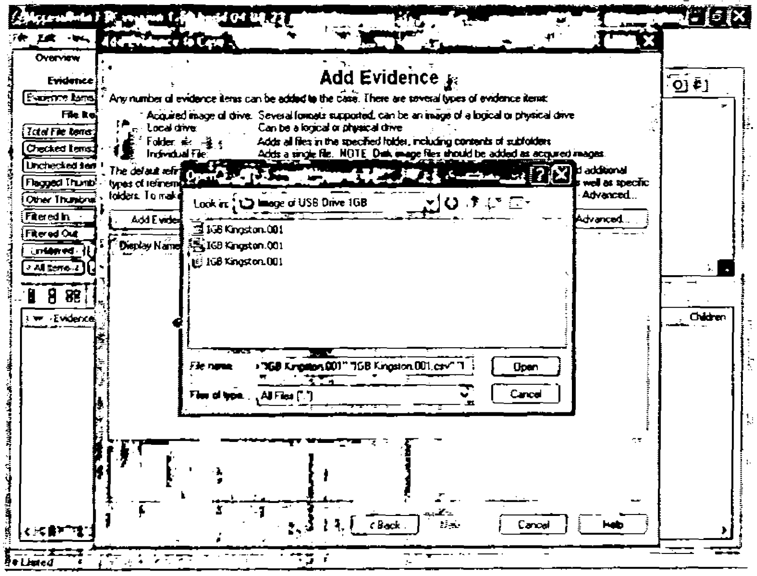
Type of Evidence to Add to Case

● Acquired Image of Drive
○ Local Drive
○ Contents of a Folder
○ Individual File

Fig 5.12.6 Step 12.6: Addition of evidence

In step 12.6, type of collected evidence is selected, that may be hash of disk or folder or local drive. There may be more then one evidence to be included to examine and analyze.

5.12.7 Step 12.7: Selection of evidence



Any number of evidence items can be added to the case. There are several types of evidence items:

Acquired image of drive:	Several formats supported, can be an image of a logical or physical drive
Local drive:	Can be a logical or physical drive
Folder:	Adds all files in the specified folder, including contents of subfolders
Individual File:	Adds a single file. NOTE: Disk image files should be added as acquired images.

Look in: Image of USB Drive 1GB

1GB Kingston.001
1GB Kingston.001
1GB Kingston.001

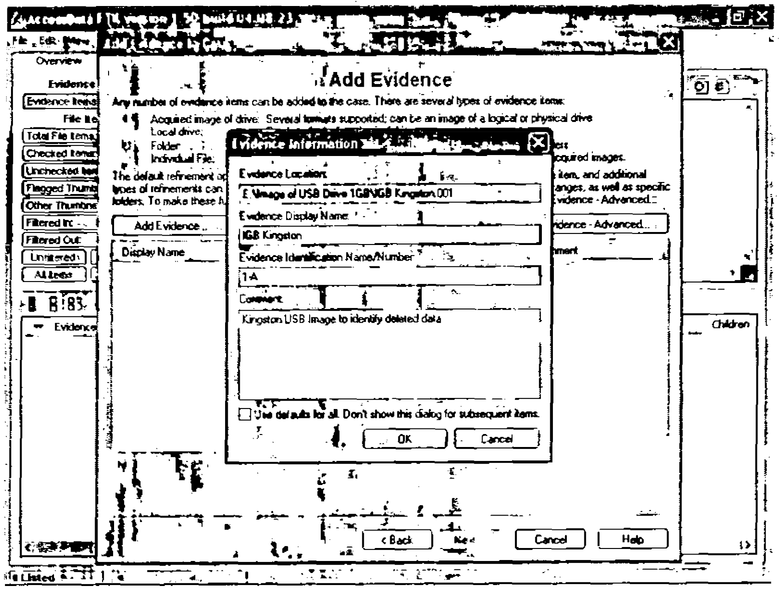
File name: "1GB Kingston.001" "1GB Kingston.001.csv" "1

Files of type: All Files (*.*)

Fig 5.12.7 Step 12.7: Selection of evidence

In step 12.7, the path of evidence is given and collected evidence is included to examine and process.

5.12.8 Step 12.8: Information related to added evidence



Evidence Location: E:\Image of USB Drive 1GB\1GB Kingston.001

Evidence Display Name: 1GB Kingston

Evidence Identification Name/Number: 1-A

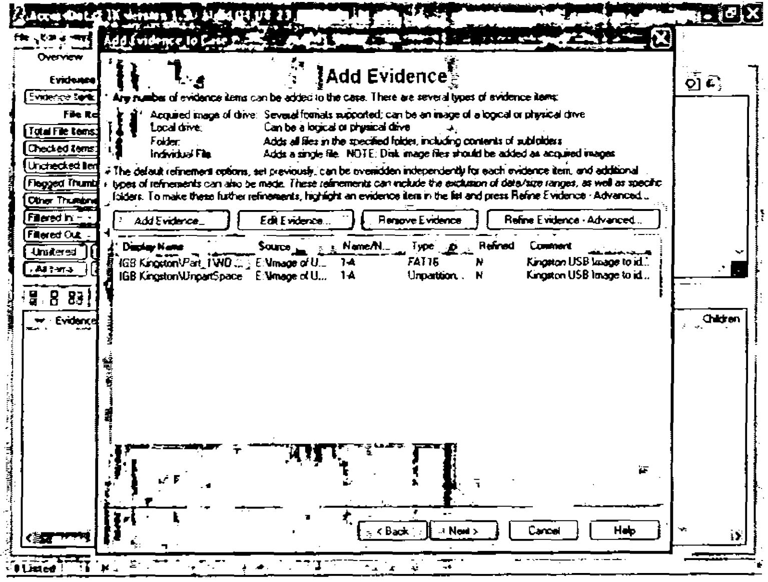
Comment: Kingston USB Image to identify deleted data

□ Use defaults for all. Don't show this dialog for subsequent items.

Fig 5.12.8 Step 12.8: Information related to added evidence

In step 12.8, evidence display name, identification name/number and comments are added that will appear in report.

5.12.9 Step 12.9: Name, type and source of evidence



Add Evidence

Any numbes of evidence items can be added to the case. There are several types of evidence items:

Acquired image of drive:	Several formats supported; can be an image of a logical or physical drive
Local drive:	Can be a logical or physical drive
Folder:	Adds all files in the specified folder, including contents of subfolders
Individual File	Adds a single file. NOTE: Disk image files should be added as acquired images

The default refinement options, set previously, can be overridden independently for each evidence item, and additional types of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specific folders. To make these further refinements, highlight an evidence item in the list and press Refine Evidence - Advanced...

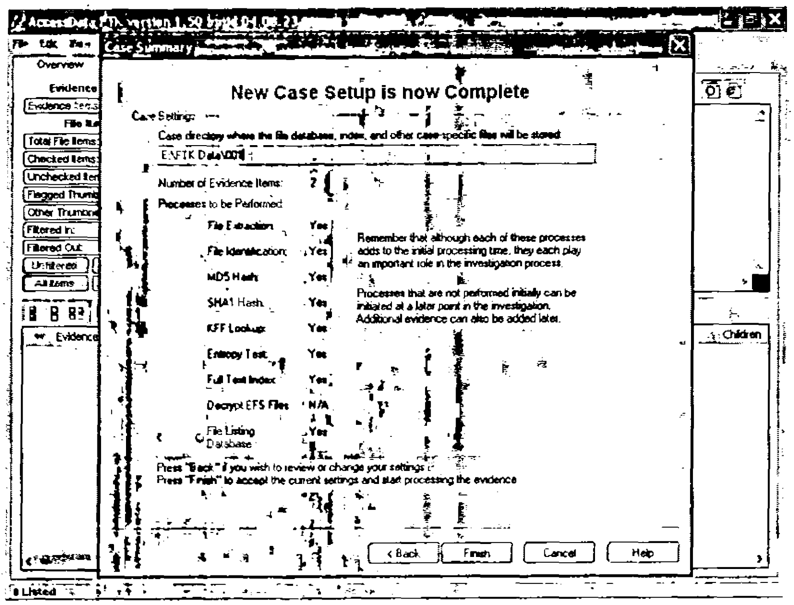
Add Evidence... | Edit Evidence... | Remove Evidence | Refine Evidence - Advanced...

Display Name	Source	Name/N...	Type	Refined	Comment
1GB Kingston\Part_1\NO...	E:\Image of U...	1-A	FAT16	N	Kingston USB Image to id...
1GB Kingston\UnpartSpace	E:\Image of U...	1-A	Unpartition...	N	Kingston USB Image to id...

Fig 5.12.9 Step 12.9: Name, type and source of evidence

In step 12.9, added evidence display name, source/location, name, type and comments will appear to read and check before proceeding further.

5.12.10 Step 12.10: Completion of setup



New Case Setup is now Complete

Case Settings:

Case directory where the file database, index, and other case-specific files will be stored

E:\FTK Data\001

Number of Evidence Items: 2

Processes to be Performed:

File Extraction	Yes
File Identification:	Yes
MD5 Hash:	Yes
SHA1 Hash:	Yes
KFF Lookup:	Yes
Entropy Test:	Yes
Full Text Index:	Yes
Decrypt EFS Files:	N/A
File Listing Database:	Yes

Remember that although each of these processes adds to the initial processing time, they each play an important role in the investigation process.

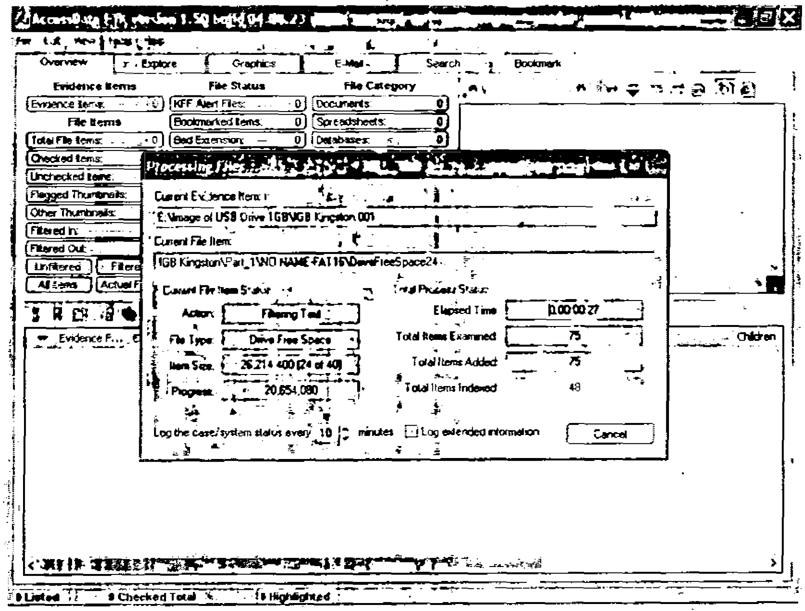
Processes that are not performed initially can be initiated at a later point in the investigation. Additional evidence can also be added later.

Press "Back" if you wish to review or change your settings
Press "Finish" to accept the current settings and start processing the evidence

Fig 5.12.10 Step 12.10: Completion of setup

In step 12.10, on completion of case setup all selected processes to perform on evidence will be displayed to change or may add more if required on the basis of requirements.

5.12.11 Step 12.11: Processing of evidence



Evidence Items: 0
KFF Alert Files: 0
Documents: 0
Bookmarked Items: 0
Spreadsheets: 0
Total File Items: 0
Bad Extension: 0
Databases: 0
Checked Items:
Unchecked Items:
Flagged Thumbnails:
Other Thumbnails:
Filtered In:
Filtered Out:

Processing Files

Current Evidence Item:
E:\Image of USB Drive 1GB\IGB Kingston.001
Current File Item:
IGB Kingston\Part_1\NO NAME-FAT16\DriveFreeSpace24

Current File Item Status
Action: Filtering Text
File Type: Drive Free Space
Item Size: 26,214,400 (24 of 40)
Progress: 20,654,080

Total Process Status
Elapsed Time: 0:00:00:27
Total Items Examined: 75
Total Items Added: 75
Total Items Indexed: 48

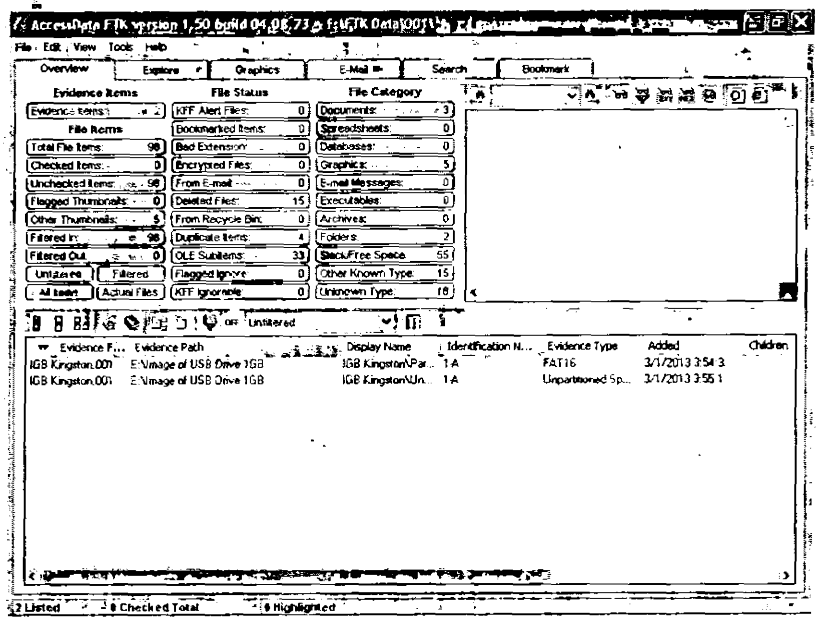
Log the case/system status every 10 minutes □ Log extended information

0 Listed 0 Checked Total 0 Highlighted

Fig 5.12.11 Step 12.11: Processing of evidence

On completion of case setup processing will be started on the evidence. All included evidences will be processed that take time on the bases of size of data.

5.12.12 Step 12.12: Results after processing



AccessData FTK version 1.50 build 04.08.73 F:\FTK Data\001

Evidence Items: 2	KFF Alert Files: 0	Documents: 3
Total File Items: 98	Bookmarked Items: 0	Spreadsheets: 0
Checked Items: 0	Bad Extension: 0	Databases: 0
Unchecked Items: 98	Encrypted Files: 0	Graphics: 5
Flagged Thumbnails: 0	From E-mail: 0	E-mail Messages: 0
Other Thumbnails: 5	Deleted Files: 15	Executables: 0
Filtered In: 98	From Recycle Bin: 0	Archives: 0
Filtered Out: 0	Duplicate Items: 4	Folders: 2
	OLE Subitems: 33	Slack/Free Space: 55
	Flagged Ignore: 0	Other Known Type: 15
	KFF Ignorable: 0	Unknown Type: 18

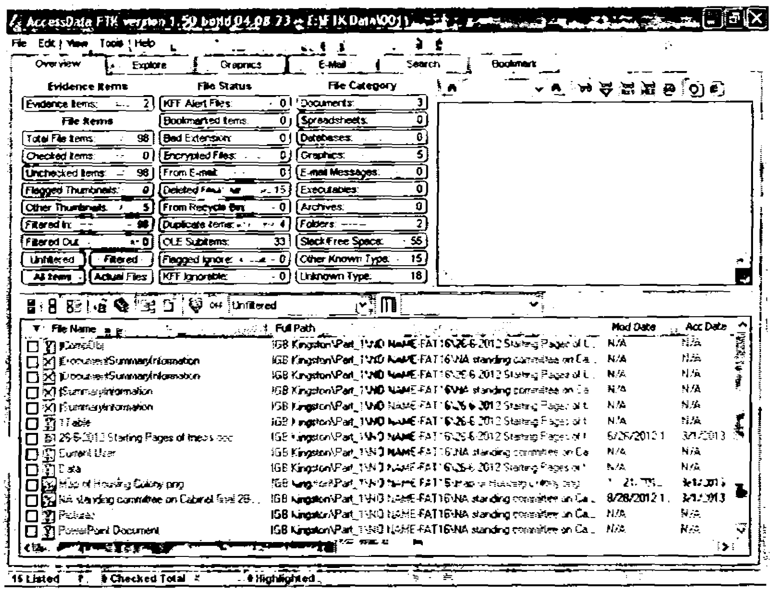
Evidence F...	Evidence Path	Display Name	Identification N...	Evidence Type	Added	Children
IGB Kingston.001	E:\Image of USB Drive 1GB	IGB Kingston\Par...	1A	FAT16	3/1/2013 3:54 3	
IGB Kingston.001	E:\Image of USB Drive 1GB	IGB Kingston\Un...	1A	Unpartitioned Sp...	3/1/2013 3:55 1	

2 Listed 0 Checked Total 0 Highlighted

Fig 5.12.12 Step 12.12: Results after processing

In step 12.12, after completion of processes No. of evidence items, file items, file status and file category will appear to tell deleted files or other required information.

5.12.13 Step 12.13: Deleted file list


AccessData FTK version 1.50 build 04.08.23 - E:\FTK Data\001
File Edit View Tools Help
Overview
Explore
Graphics
E-Mail
Search
Bookmark
Unfiltered
Filtered
All Items
Actual Files

Evidence Items		File Status		File Category	
Evidence Items:	2	KFF Alert Files:	0	Documents:	3
File Items		Bookmarked Items:	0	Spreadsheets:	0
Total File Items:	98	Bad Extension:	0	Databases:	0
Checked Items:	0	Encrypted Files:	0	Graphics:	5
Unchecked Items:	98	From E-mail:	0	E-mail Messages:	0
Flagged Thumbnails:	0	Deleted Files:	15	Executables:	0
Other Thumbnails:	5	From Recycle Bin:	0	Archives:	0
Filtered In:	98	Duplicate Items:	4	Folders:	2
Filtered Out:	0	OLE Subitems:	33	Slack/Free Space:	55
		Flagged Ignore:	0	Other Known Type:	15
		KFF Ignorable:	0	Unknown Type:	18

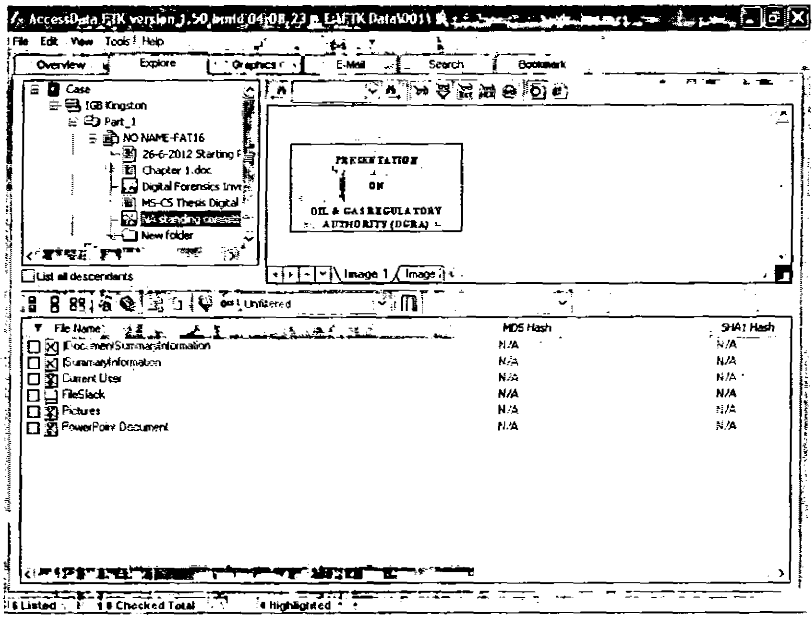
File Name	Full Path	Mod Date	Acc Date
☐ CompObj	1GB Kingston\Part_1\NO NAME-FAT16\26-6-2012 Starting Pages of t...	N/A	N/A
☐ DocumentSummaryInformation	1GB Kingston\Part_1\NO NAME-FAT16\NA standing committee on Ca...	N/A	N/A
☐ DocumentSummaryInformation	1GB Kingston\Part_1\NO NAME-FAT16\26-6-2012 Starting Pages of t...	N/A	N/A
☐ SummaryInformation	1GB Kingston\Part_1\NO NAME-FAT16\NA standing committee on Ca...	N/A	N/A
☐ SummaryInformation	1GB Kingston\Part_1\NO NAME-FAT16\26-6-2012 Starting Pages of t...	N/A	N/A
☐ 1Table	1GB Kingston\Part_1\NO NAME-FAT16\26-6-2012 Starting Pages of t...	N/A	N/A
☐ 26-6-2012 Starting Pages of thesis.doc	1GB Kingston\Part_1\NO NAME-FAT16\26-6-2012 Starting Pages of t...	6/26/2012 1	3/1/2013
☐ Current User	1GB Kingston\Part_1\NO NAME-FAT16\NA standing committee on Ca...	N/A	N/A
☐ Data	1GB Kingston\Part_1\NO NAME-FAT16\26-6-2012 Starting Pages of t...	N/A	N/A
☐ Map of Housing Colony.png	1GB Kingston\Part_1\NO NAME-FAT16\[illegible]	[illegible]	[illegible]
☐ NA standing committee on Cabinet Secretariat 28...	1GB Kingston\Part_1\NO NAME-FAT16\NA standing committee on Ca...	8/28/2012 1	3/1/2013
☐ Pictures	1GB Kingston\Part_1\NO NAME-FAT16\NA standing committee on Ca...	N/A	N/A
☐ PowerPoint Document	1GB Kingston\Part_1\NO NAME-FAT16\NA standing committee on Ca...	N/A	N/A

15 Listed 0 Checked Total 0 Highlighted

Fig 5.12.13 Step 12.13: Deleted file list

On selecting the Deleted Files tab all deleted files name, path and other detail will be displayed.

5.12.14 Step 12.14: Deleted file information



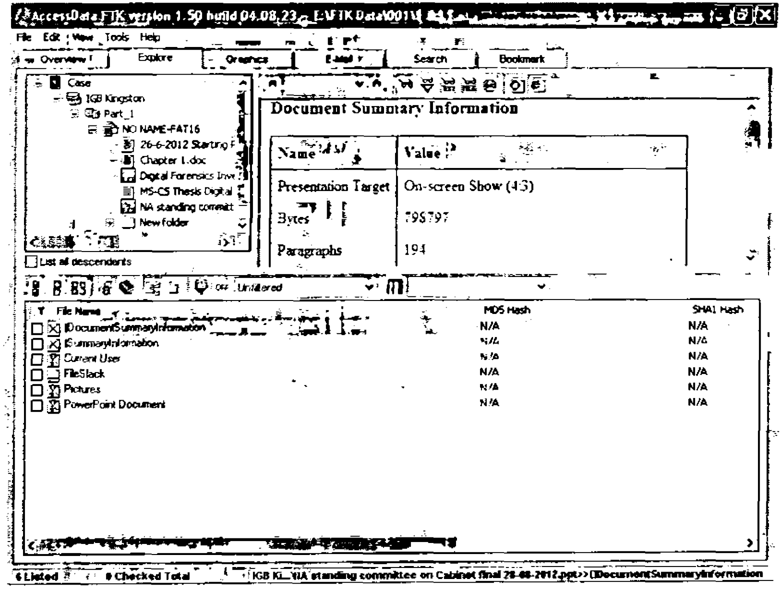
File Name	MD5 Hash	SHA1 Hash
☐ DocumentSummaryInformation	N/A	N/A
☐ SummaryInformation	N/A	N/A
☐ Current User	N/A	N/A
☐ FileSlack	N/A	N/A
☐ Pictures	N/A	N/A
☐ PowerPoint Document	N/A	N/A

6 Listed 0 Checked Total 0 Highlighted

Fig 5.12.14 Step 12.14: Deleted file information

In step 12.14, deleted files detail may be examined in detail in Explore tab to proceed further.

5.12.15 Step 12.15: Selection of file



Document Summary Information

Name	Value
Presentation Target	On-screen Show (4:3)
Bytes	798797
Paragraphs	194

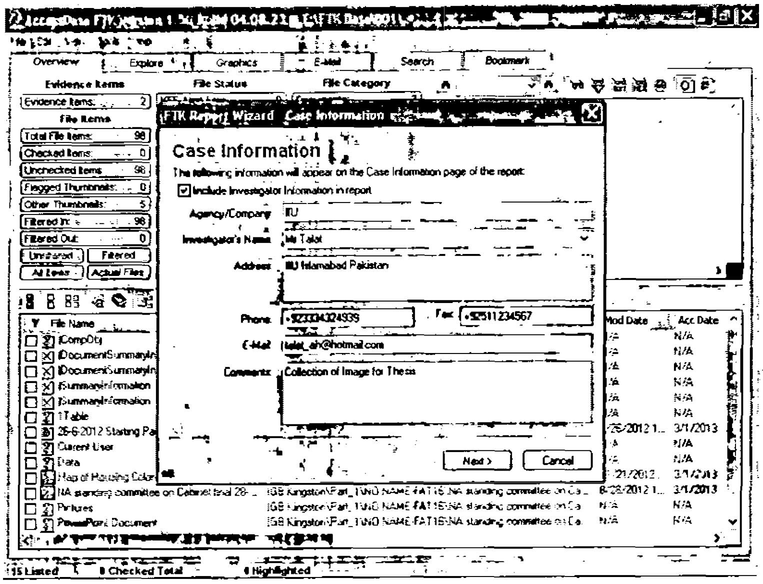
File Name	MD5 Hash	SHA1 Hash
☐ ☒ DocumentSummaryInformation	N/A	N/A
☐ ☒ SummaryInformation	N/A	N/A
☐ Current User	N/A	N/A
☐ FileSlack	N/A	N/A
☐ Pictures	N/A	N/A
☐ PowerPoint Document	N/A	N/A

6 Listed | 0 Checked Total | IGB Ki...\NA standing committee on Cabinet final 28-08-2012.ppt>>DocumentSummaryInformation

Fig 5.12.15 Step 12.15: Selection of file

In step 12.15, required deleted file or files will be selected to take related information for making report.

5.13 Step 13: Report wizard



Evidence Items: 2

File Items

Total File Items: 98
Checked Items: 0
Unchecked Items: 98
Flagged Thumbnails: 0
Other Thumbnails: 5
Filtered In: 98
Filtered Out: 0

FTK Report Wizard Case Information

Case Information

The following information will appear on the Case Information page of the report:

☑ Include Investigator Information in report

Agency/Company: IIU

Investigator's Name: Mr Talat

Address: IIU Islamabad Pakistan

Phone: +923334324939

Fax: +92511234567

E-Mail: talat_ah@hotmail.com

Comments: Collection of Image for Thesis

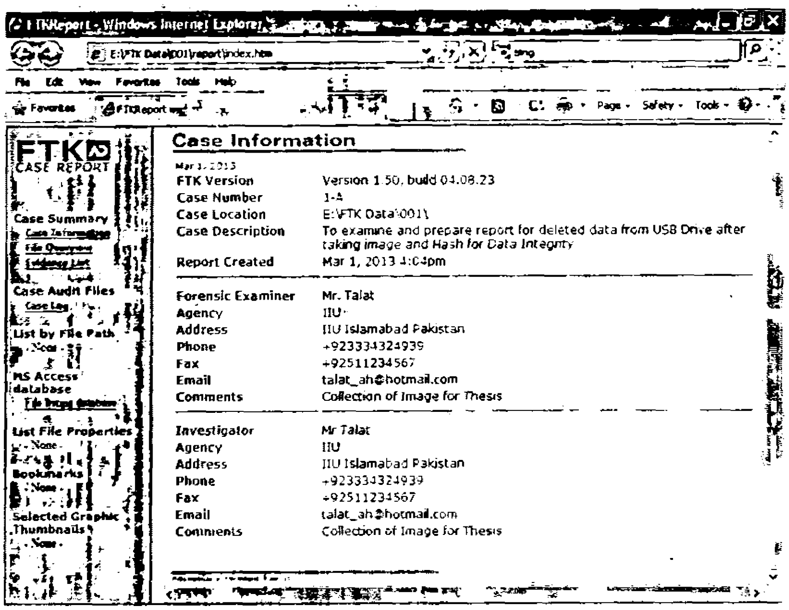
File Name		Mod Date	Acc Date
☐ CompObj		N/A	N/A
☐ ☒ DocumentSummaryIn		N/A	N/A
☐ ☒ DocumentSummaryIn		N/A	N/A
☐ ☒ SummaryInformation		N/A	N/A
☐ ☒ SummaryInformation		N/A	N/A
☐ 1Table		N/A	N/A
☐ 26-6-2012 Starting Pa		6/26/2012 1...	3/1/2013
☐ Current User		N/A	N/A
☐ Data		N/A	N/A
☐ Map of Housing Color		6/21/2012	3/1/2013
☐ NA standing committee on Cabinet final 28-...	IGB Kingston\Part_1\NO NAME-FAT16\NA standing committee on Ca...	8-28-2012 1...	3/1/2013
☐ Pictures	IGB Kingston\Part_1\NO NAME-FAT16\NA standing committee on Ca...	N/A	N/A
☐ PowerPoint Document	IGB Kingston\Part_1\NO NAME-FAT16\NA standing committee on Ca...	N/A	N/A

15 Listed | 0 Checked Total | 0 Highlighted

Fig 5.13 Step 13: Report wizard

In step 13, case related information will be added to be display on the report, that include investigating agency name, investigator's name, address, ph no, email and comments to explain the type of investigation.

5.13.1 Step 13.1: Case information for report



Case Information

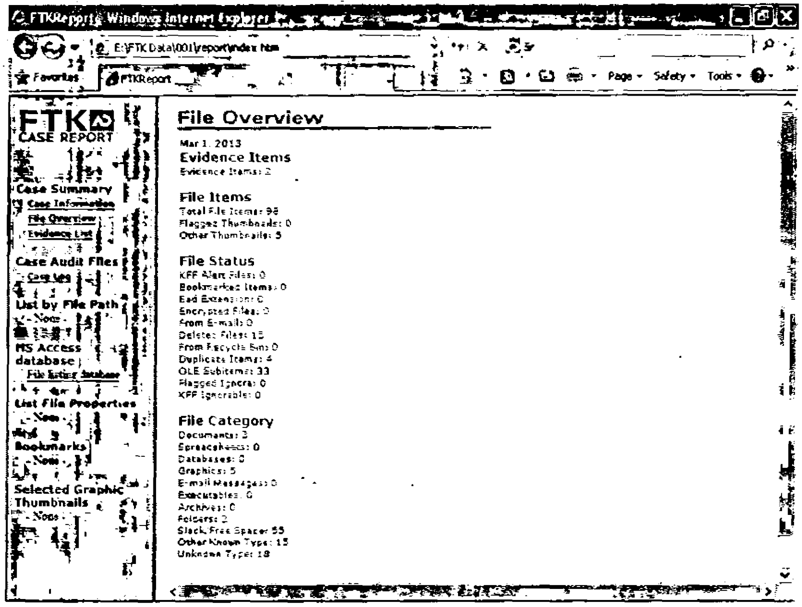
Mar 1, 2013

FTK Version	Version 1.50, build 04.08.23
Case Number	1-A
Case Location	E:\FTK Data\001\
Case Description	To examine and prepare report for deleted data from USB Drive after taking image and Hash for Data Integrity
Report Created	Mar 1, 2013 4:04pm
Forensic Examiner	Mr. Talat
Agency	IIU
Address	IIU Islamabad Pakistan
Phone	+923334324939
Fax	+92511234567
Email	talat_ah@hotmail.com
Comments	Collection of Image for Thesis
Investigator	Mr Talat
Agency	IIU
Address	IIU Islamabad Pakistan
Phone	+923334324939
Fax	+92511234567
Email	talat_ah@hotmail.com
Comments	Collection of Image for Thesis

Fig 5.13.1 Step 13.1: Case information for report

In step 13.1, complete case information will be given in report to present. Case information include FTK version used for examination and analysis, date report created, forensic examiner and investigator name and addresses.

5.13.2 Step 13.2: File overview



File Overview

Mar 1, 2013

Evidence Items

Evidence Items: 2

File Items

Total File Items: 98
Flagged Thumbnails: 0
Other Thumbnails: 5

File Status

KFF Alert Files: 0
Bookmarked Items: 0
Bad Extension: 0
Encrypted Files: 0
From E-mail: 0
Deleted Files: 15
From Recycle Bin: 0
Duplicate Items: 4
OLE Subitems: 33
Flagged Ignore: 0
KFF Ignorable: 0

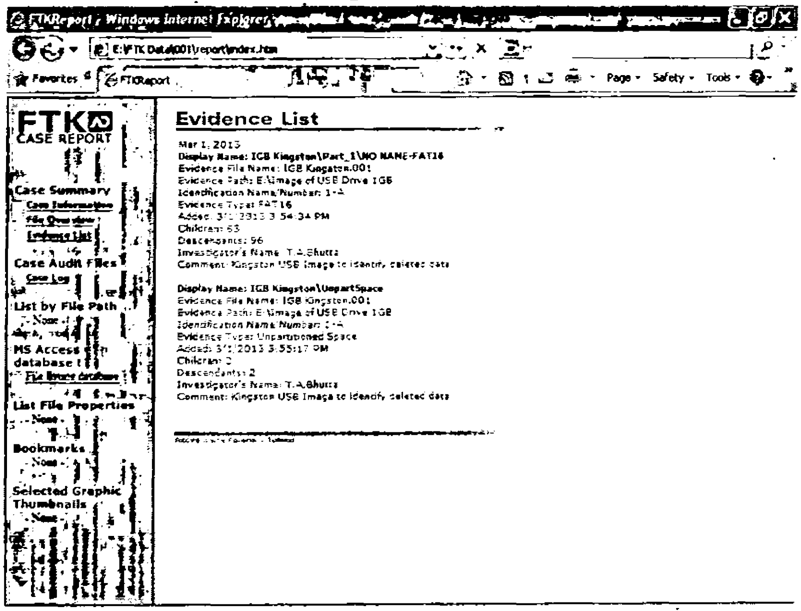
File Category

Documents: 3
Spreadsheets: 0
Databases: 0
Graphics: 5
E-mail Messages: 0
Executables: 0
Archives: 0
Folders: 2
Slack/Free Space: 55
Other Known Type: 15
Unknown Type: 18

Fig 5.13.2 Step 13.2: File overview

In step 13.2, a detail of evideñce items, files items, status and category will be displayed.

5.13.3 Step 13.3: Evidence list



Evidence List

Mar 1, 2013
Display Name: 1GB Kingston\Part_1\NO NAME-FAT16
Evidence File Name: 1GB Kingston.001
Evidence Path: E:\Image of USB Drive 1GB
Identification Name/Number: 1-A
Evidence Type: FAT16
Added: 3/1/2013 3:54:34 PM
Children: 63
Descendants: 96
Investigator's Name: T.A.Bhutta
Comment: Kingston USB Image to identify deleted data

Display Name: 1GB Kingston\UnpartSpace
Evidence File Name: 1GB Kingston.001
Evidence Path: E:\Image of USB Drive 1GB
Identification Name/Number: 1-A
Evidence Type: Unpartitioned Space
Added: 3/1/2013 3:55:17 PM
Children: 2
Descendants: 2
Investigator's Name: T.A.Bhutta
Comment: Kingston USB Image to identify deleted data

Fig 5.13.3 Step 13.3: Evidence list

In step 13.3, complete detail of all evidences included for examination and analysis and related information will be given in report.

5.14 Step 14: Formulation of hypothesis

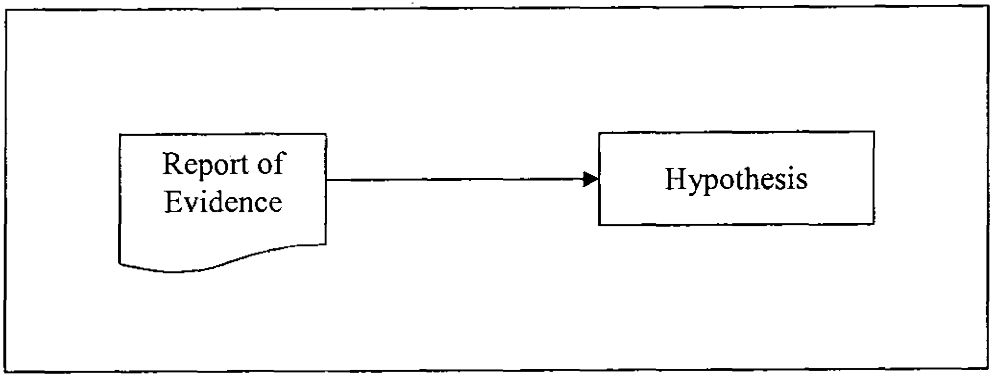


Fig 5.14 Step 14: Formulation of hypothesis

In step 14, on the bases of report which is prepared after examination and analysis, a hypothesis will be constructed that how incident occurred, what type of activity happened and how IT infrastructure was misused.

5.15 Step 15: Preservation of finding

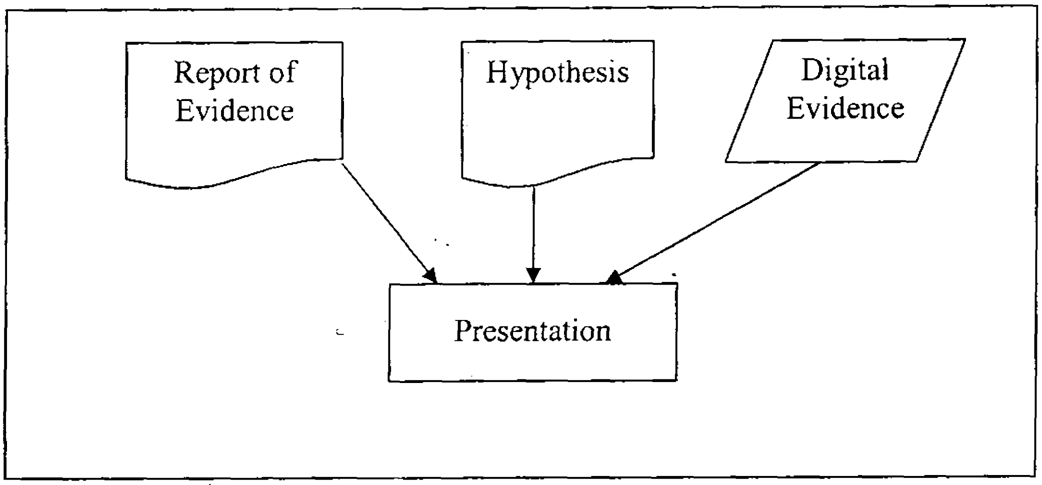


Fig 5.15 Step 15: Preservation of finding

In step 15, all the finding including digital evidence, report of evidence and hypothesis will be presented in human readable form.

5.16 Step 16: Proof and defense

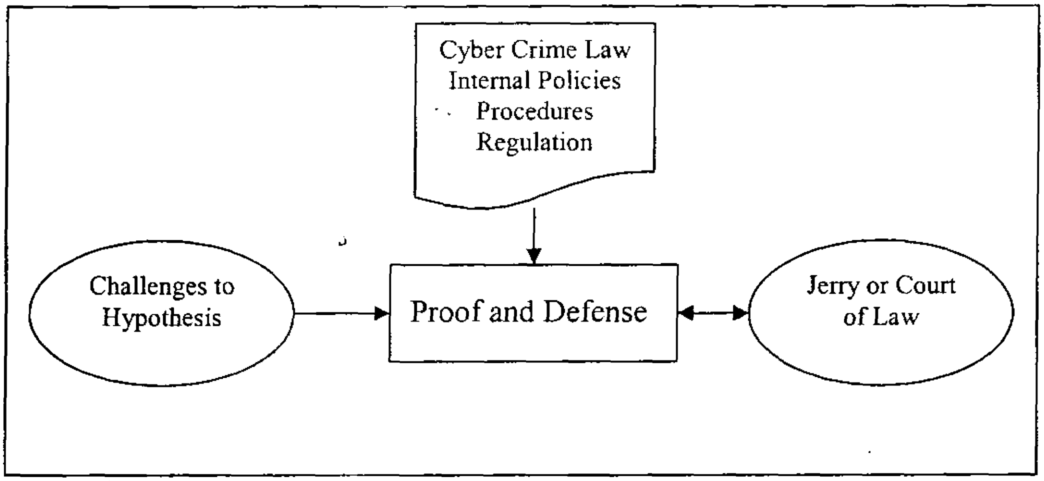


Fig 5.16 Step 16: Proof and defense

In step 16, all investigation result will be presented in jury or court of law for necessary action. Hypothesis will be challenged by concern parties in the light of law or internal policies to reach a final decision about incident.

5.17 Step 17: Archive

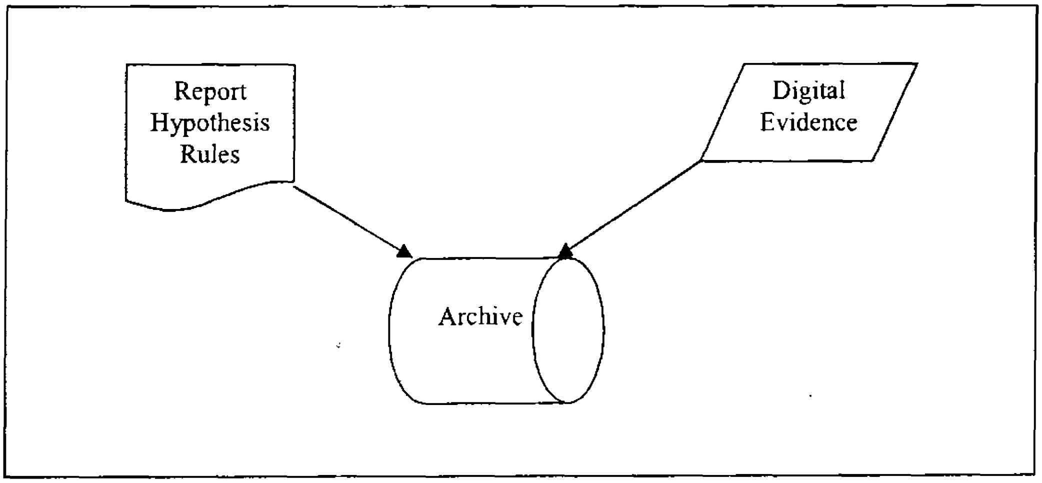


Fig 5.17 Step 17: Archive

In step 17, all the result, findings, digital evidence, documentation, hypothesis and report will be saved in Archive for further reference and research. Archive will provide opportunity to researcher to enhance safety measures and digital forensic investigation method.

Chapter 6

Results and Discussions

6. Results and Discussions

Table 6.1 gives analysis of the phases in the proposed model and draw comparison studied models. In proposed model, relevant activities of other models are integrated to enhance it. A new phase Hypothesis is made explicit in the proposed model.

Phases in Proposed Model	M. Pollitt Model.	Kruse and Heiser Model.	America's Department of Justice Model.	Digital Forensic Research Working Group Model	Reith, Carr and Gunch Model	Sundresan Perumal Model	A Generic Model for Network Forensics
Awareness							
Preparation					✓		✓
Reporting							✓
Authorization					✓	✓	✓
Planning					✓	✓	
Notification						✓	
Identification	✓	✓		✓		✓	✓
Preservation				✓	✓	✓	✓
Search & Seizure						✓	
Collection	✓	✓	✓	✓	✓	✓	✓
Transportation						✓	
Storage						✓	
Examination	✓		✓	✓	✓		✓
Analysis		✓	✓	✓	✓	✓	✓
Hypothesis							
Presentation	✓		✓	✓	✓	✓	✓
Proof / Defense				✓	✓	✓	
Archive				✓	✓	✓	

Table 6.1: Analysis of Phases in Proposed and Existing Models

Data Integrity, Documentation and Information flow are unique features of the proposed model. One of the main features of proposed model is that awareness for end user, ordinary user, IT experts, System/Network administrators, incident responders, victims, witness and law enforcement persons has been introduced. Due to this awareness, a lot of problems and issues have been resolved in a batter way. This awareness process tells all those who are present at the crime scene how to protect the digital evidence from lose.

From analysis of studied models, it is also clear that some phases are included in every model i.e. identification, collection, examination, analysis and presentation. It is also clear that with the advancement of technology, requirements and procedure more phases have been included to fulfill demands of Digital Forensic Investigation Model.

A good and comprehensive model for cyber crime investigations is important so that it support new technologies and tools for investigation, independent of any particular technology or organizational environment and provide security features in all aspect of model.

One to one mapping of proposed model phases and studied models phases not possible but overall phases are similar in some of there functionality. Some phases functionality is same but the terminology used / studied forensic models may differ. Table 6.2 gives mapping of studied forensic models to the proposed model. It is also clear from table that the phases' terminology of proposed model to those found in other studied models is different.

In some of studied model phases two or more phases functionality has been combined in one phase which result not clear cut boundary of next phase. For example, in Generic Model for Network Forensics preparation and authorization phase is combined in one phase and when I compared with proposed model there are two separate and independent phases.

Phases in Proposed Model	M. Pollitt Model.	Kruse and Heiser Model.	America's department of justice Model.	Digital Forensic Research Working Group Model	Reith, Carr and Gunch Model	Sundresan Perumal Model	A Generic Model for Network Forensics
Awareness							
Preparation					Preparation		Preparation and Authorization
Reporting							Incident Response
Authorization					Approach	Authorization	
Planning					Strategy	Planning	
Notification						Search Warrant	
Identification	Identification	Authentication		Identification		Identification	Detection of Incident/Crime
Preservation				Preservation	Preservation	Reconnaissance	Preservation and Protection
Search & Seizure						Identify Seized Items	
Collection	Acquisition	Acquisition	Collection	Collection	Collection	Gathering Evidence	Collection of Network Traces
Transportation						Transport	
Storage						Storage	
Examination	Evaluation		Examination	Examination	Examination		Examination
Analysis		Analyzing	Analysis	Analysis	Analysis	Analysis	Analysis
Hypothesis							
Presentation	Admission		Reporting	Presentation	Presentation	Result	Presentation
Proof / Defense				Decision	Returning Evidence	Proof & Defense	
Archive							

Table 6.2: Mapping of Studied Forensic Models to the Proposed Model

6.1 Hypothesis

One of the main purposes of Hypothesis is to answer the questions related to digital forensic investigation model and to maintain data integrity. Hypothesis must be formulated and tested to answer the previous states and activities in a scientific method. A hypothesis has four phases i.e. observation, hypothesis formulation, prediction and testing/searching

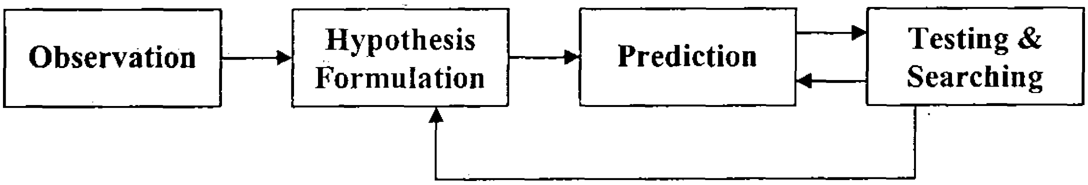


Fig 6.1 Four Phases of Hypothesis

6.1.1 Observation

In the observation phase, an investigator makes observations about events and activities for the purpose of formulation of hypothesis. Sources of observations are information, resources related to evidence, data and output from analysis tools i.e. FTK. Some examples are:

- List of deleted files is observed using FTK
- List of files in a directory is observed using FTK
- Contents of e-mail is observed using FTK

6.1.2 Hypothesis Formulation

In hypothesis formulation phase, an investigator interprets the observed data and formulate hypothesis. In formal approach, the hypotheses are about the variables in the incident that what and how crime happen. Some examples are:

- Deletion of files from USB
- Storage capability of a system
- Download images from prohibited site

6.1.3 Prediction

In prediction phase, an investigator identifies evidence that if it exists and would support or refute a hypothesis. The characteristics of an incident observed to make hypothesis will also support to the prediction. Based on the predication, experiments are conducted. Some common types of predictions are:

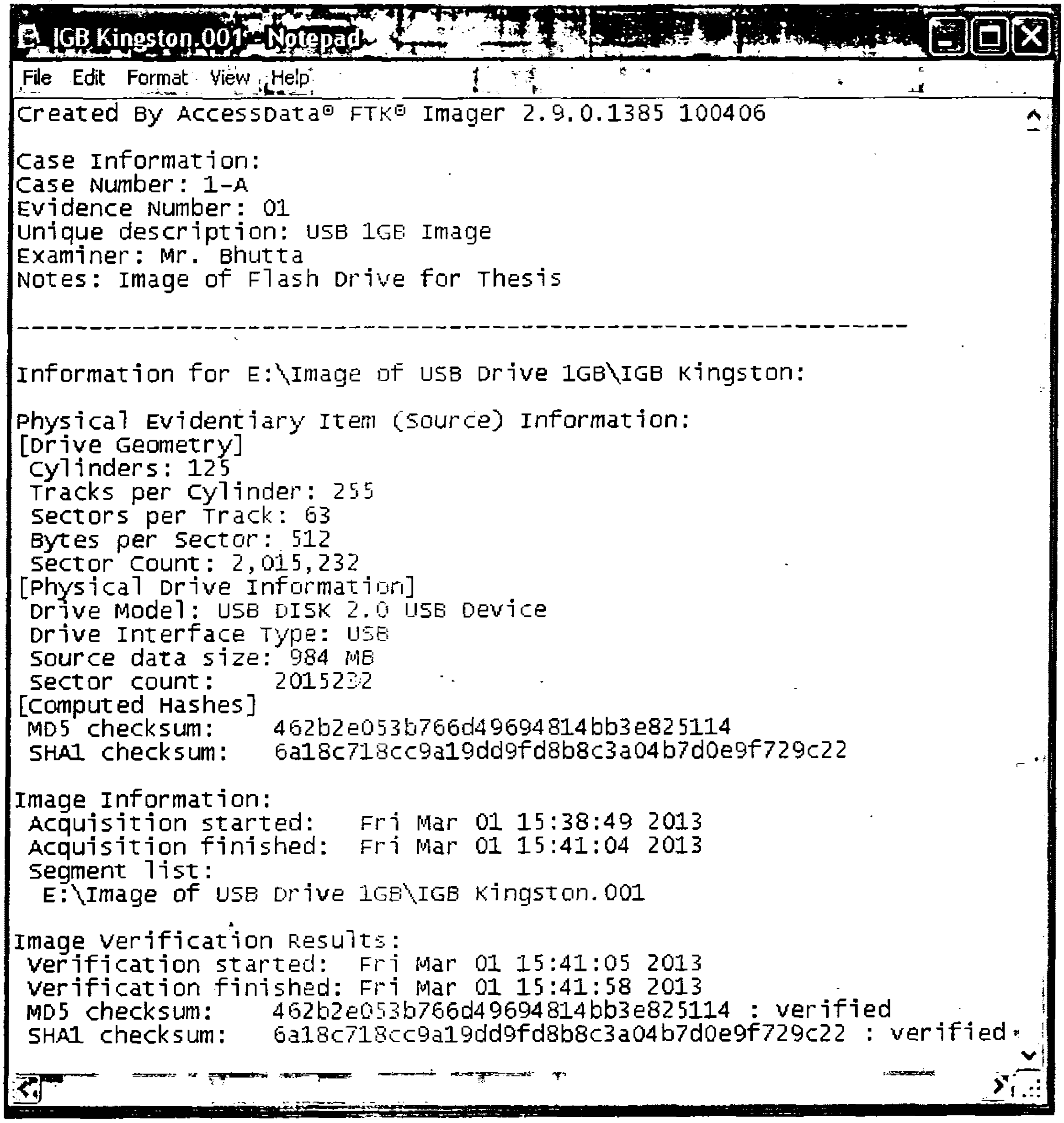
- Contents of a file in the incident history
- Contents of JPEG files
- Output of executable file

6.1.4 Testing and Searching

In the testing phase, an investigator tests the prediction and hypothesis. Test and experiment involve the potential evidence of the incident. Based on the test results new predictions may be made and hypothesis may be revised.

The data integrity is maintained and checked through hash verification, which was taken in collection phase through Imager. After examination and analysis phase with FTK, hash of total evidence or all evidences added to FTK have the same hash as previous. All files present in evidence or may be deleted will have MD5 and SH1 value which can be verified through Imager. Hash value is saved and documented at every phase for testing and verification of integrity.

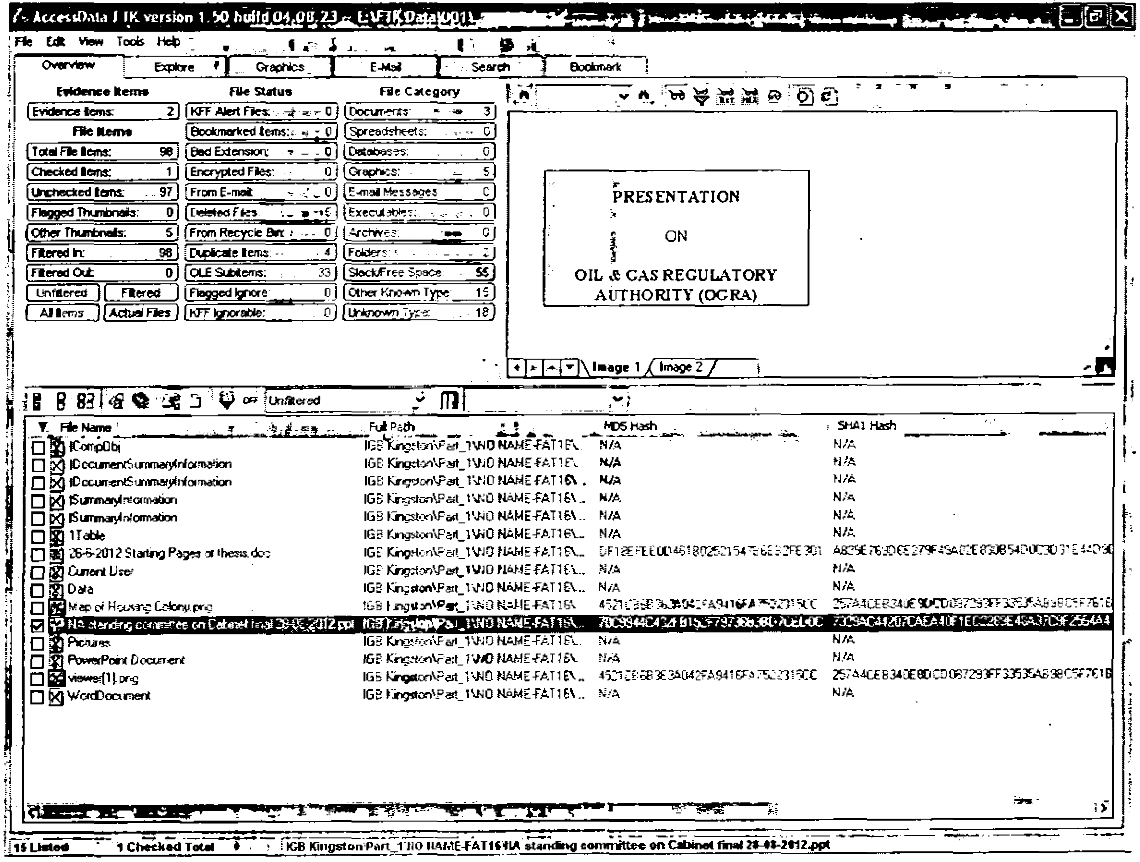
Access Data FTK Imager is used to take image of hard disk, USB drive, folder and files for investigation. Access Data FTK Imager is used to take complete hash of USB Drive as USB Drive is potential evidence. After taking the image complete drive volume, cylinder, track, sector, bytes, drive interface type, MD5 and SHA1 values are given in a report. Complete detail of image result is given in fig 6.2. MD5 and SHA1 values are verified and checked and result is given for further documentation. Image is stored on multiple drive and location for backup and further investigation.



```
Created By AccessData® FTK® Imager 2.9.0.1385 100406

Case Information:
Case Number: 1-A
Evidence Number: 01
Unique description: USB 1GB Image
Examiner: Mr. Bhutta
Notes: Image of Flash Drive for Thesis

--------------------------------------------------------------

Information for E:\Image of USB Drive 1GB\IGB Kingston:

Physical Evidentiary Item (Source) Information:
[Drive Geometry]
 Cylinders: 125
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 2,015,232
[Physical Drive Information]
 Drive Model: USB DISK 2.0 USB Device
 Drive Interface Type: USB
 Source data size: 984 MB
 Sector count:    2015232
[Computed Hashes]
 MD5 checksum:    462b2e053b766d49694814bb3e825114
 SHA1 checksum:   6a18c718cc9a19dd9fd8b8c3a04b7d0e9f729c22

Image Information:
 Acquisition started:   Fri Mar 01 15:38:49 2013
 Acquisition finished:  Fri Mar 01 15:41:04 2013
 Segment list:
  E:\Image of USB Drive 1GB\IGB Kingston.001

Image Verification Results:
 Verification started:  Fri Mar 01 15:41:05 2013
 Verification finished: Fri Mar 01 15:41:58 2013
 MD5 checksum:    462b2e053b766d49694814bb3e825114 : verified
 SHA1 checksum:   6a18c718cc9a19dd9fd8b8c3a04b7d0e9f729c22 : verified
```

Fig 6.2 Hash value information of USB Drive image

FTK is used to analyze and examine the image taken by imager. FTK gives the complete detail of files present in image including deleted files, there path, size, location, hash value, partition detail etc. Fig 6.3 gives detail of deleted files after analysis of evidence image. MD5 and SHA1 value of file is also calculated for verification of data integrity.



AccessData FTK version 1.50 build 04.08.23 - E:\FTKData\001\

Evidence Items	File Status	File Category
Evidence Items: 2	KFF Alert Files: 0	Documents: 3
File Items	Bookmarked Items: 0	Spreadsheets: 0
Total File Items: 98	Bad Extension: 0	Databases: 0
Checked Items: 1	Encrypted Files: 0	Graphics: 5
Unchecked Items: 97	From E-mail: 0	E-mail Messages: 0
Flagged Thumbnails: 0	Deleted Files: 5	Executables: 0
Other Thumbnails: 5	From Recycle Bin: 0	Archives: 0
Filtered In: 98	Duplicate Items: 4	Folders: 2
Filtered Out: 0	OLE Subitems: 33	Slack/Free Space: 55
Unfiltered / Filtered	Flagged Ignore: 0	Other Known Type: 15
All Items / Actual Files	KFF Ignorable: 0	Unknown Type: 18

PRESENTATION

ON

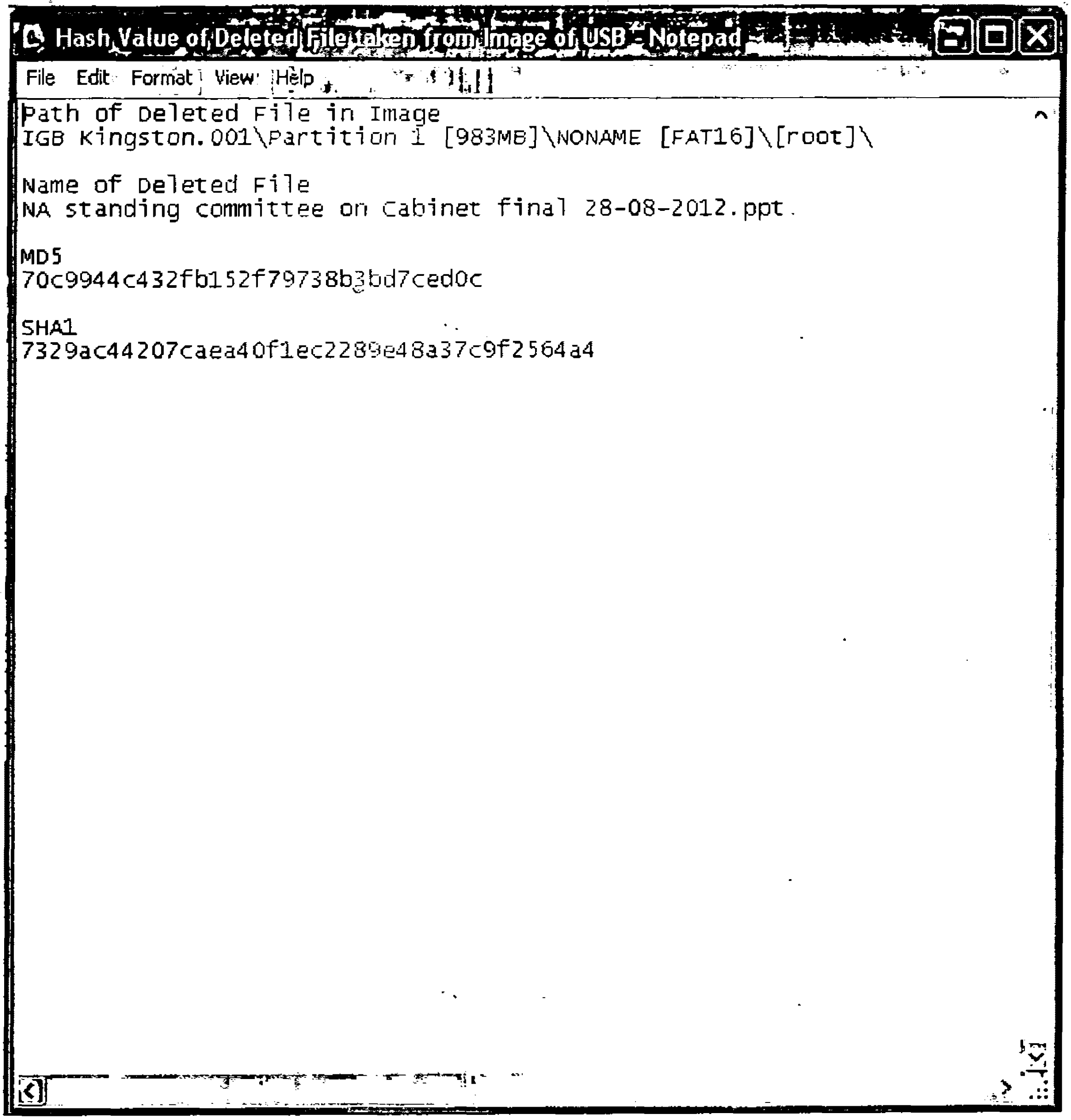
OIL & GAS REGULATORY AUTHORITY (OGRA)

	File Name	Full Path	MD5 Hash	SHA1 Hash
□	!CompObj	IGB Kingston\Part_1\NO NAME-FAT16\...	N/A	N/A
□	!DocumentSummaryInformation	IGB Kingston\Part_1\NO NAME-FAT16\...	N/A	N/A
□	!DocumentSummaryInformation	IGB Kingston\Part_1\NO NAME-FAT16\...	N/A	N/A
□	!SummaryInformation	IGB Kingston\Part_1\NO NAME-FAT16\...	N/A	N/A
□	!SummaryInformation	IGB Kingston\Part_1\NO NAME-FAT16\...	N/A	N/A
□	1Table	IGB Kingston\Part_1\NO NAME-FAT16\...	N/A	N/A
□	26-6-2012 Starting Pages of thesis.doc	IGB Kingston\Part_1\NO NAME-FAT16\...	DF12EFEE0D46180252154 7E6E32FE301	A825E763D6E279F45A02E830B54D0C3031E44D3
□	Current User	IGB Kingston\Part_1\NO NAME-FAT16\...	N/A	N/A
□	Data	IGB Kingston\Part_1\NO NAME-FAT16\...	N/A	N/A
□	Map of Housing Colony.png	IGB Kingston\Part_1\NO NAME-FAT16\	4521CB6B3638042FA9416FA75223150C	257A4CEB340E8DCD087293FF33535A838C5F761B
☑	NA standing committee on Cabinet final 28-08-2012.ppt	IGB Kingston\Part_1\NO NAME-FAT16\...	70C9944C434B15C79736380 70EL0C	73C9AC44207CAEA40F1EC0269E45A37C9F2564A4
□	Pictures	IGB Kingston\Part_1\NO NAME-FAT16\...	N/A	N/A
□	PowerPoint Document	IGB Kingston\Part_1\NO NAME-FAT16\	N/A	N/A
□	viewer[1].png	IGB Kingston\Part_1\NO NAME-FAT16\...	4521CB6B3E3A042FA9416FA75223150C	257A4CEB340E8DCD087293FF33535A838C5F761B
□	WordDocument	IGB Kingston\Part_1\NO NAME-FAT16\...	N/A	N/A

15 Listed 1 Checked Total IGB Kingston\Part_1\NO NAME-FAT16\NA standing committee on Cabinet final 28-08-2012.ppt

Fig 6.3 Deleted file Hash value information through FTK

Hash value of required file is accessed from image of evidence through imager to compare and verify. Fig 6.4 gives the detail of MD5 and SHA1 value. After comparing values of hash in fig 6.4 with fig 6.3, it is clear that both are same which means integrity of data in maintained on every step of proposed model.


Hash Value of Deleted File taken from Image of USB - Notepad
File
Edit
Format
View
Help

```
Path of Deleted File in Image
IGB Kingston.001\Partition 1 [983MB]\NONAME [FAT16]\[root]\

Name of Deleted File
NA standing committee on Cabinet final 28-08-2012.ppt

MD5
70c9944c432fb152f79738b3bd7ced0c

SHA1
7329ac44207caea40f1ec2289e48a37c9f2564a4
```

Fig 6.4 Hash value of file taken from image of evidence

Chapter 7

Conclusion and Future Work

7. Conclusion and Future Work

In this research thesis, methodologies to enhance data integrity and documentation procedure for digital forensic investigation model have been introduced. At each phase of proposed model, documentation, chain of custody, safety of evidence/data and standard procedures are adopted. Each phase is well defined and has very clear cut boundary. Proposed model has eighteen phases including awareness the first most phase, which plays a vital role for all users at every level to know about cyber crime and procedure to save infected digital device. In preparation phase, the concept of incident response teams both local and within the organization as well as computer emergency response team and information sharing and analysis centers are introduced to overcome the incident as early as possible. Backtracking, information flow and policies are the main features of this model. Incident may be reported to local incident response team or forensic investigating agency with the approval of higher management in case of organization. Proper planning on the basis of internal procedures, policy and available resources is introduced. On the basis of examination and analysis, a hypothesis will be constructed to know that how actual incident happened and what type of policy violation occurred.

7.1 Recommendation

The researcher believes that prevention is best solution to overcome increasing number of security violation and cyber crime. However, it may not be feasible to prevent all incidents unless proper forensic knowledge, expertise and awareness of incidents/attacks are created. For prosecution against cyber crime, researchers, academia, policy makers and IT experts should play their role.

Local Incident Response Team (Local IRT), Computer Emergency Response Team (CERT) and Information Sharing and Analysis Centers (ISACs) should be formulated in every organization in order to take necessary steps to overcome cyber crime and incidents on urgent bases.

7.2 Future Work

The proposed forensic model focuses exclusively on our environment which is a minor step towards removing the gap between academia, technologists, law enforcement officials, researchers and digital forensic investigators. Following work should be done in future:

- The proposed model must be implemented in our environment under different circumstances and environments.
- The model needs to be tested for its practicality under different conditions.
- The application of model in different context should be checked.
- With the passage of time when new laws, technology, awareness and requirements arise; therefore, model needs to be constantly reviewed, updated and extra phases may be added or removed on the basis of situation.

Chapter 8

References

8. References

[1] B. J. Nikkel, The Role of Digital Forensics within a Corporate Organization, May 2006, Last accessed on 14 August 2012 at http://www.digitalforensics.ch/nikkel06a.pdf.

[2] C. Wilson, Botnets, Cybercrime and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, CRS Report RL32114, January 2008.

[3] Digital Forensics: An Overview, Last accessed on 14 August 2012 at http://www.syngress.com.

[4] Robert Jones, Internet Forensics, 1st Edition, O'Reilly, October 2005.

[5] M. Pollitt, Computer Forensics: An Approach to Evidence in Cyberspace, National Information System Security Conference, Baltimore, MD, 1995, Vol. 2, pp. 487-491.

[6] S. Schechter, J. Jung, W. Stockwell, C. McLain, Inoculating SSH Against Address Harvesting, The 13th Annual Network and Distributed System Security Symposium, San Diego, CA, Februery 2006.

[7] S. Perumal, Digital Forensic Model Based on Malaysian Investigation Process, International Journal of Computer Science and Network Security, August 2009, Vol. 9, No.8, pp. 38-44.

[8] G. Palmer, A Road Map for Digital Forensic Research, Report from the First Digital Forensic Research Workshop, Utica New Yark , November 2001, pp. 15-30.

[9] M. Reith, C. Carr, G. Gunsch, An Examination of Digital Forensic Models, International Journal of Digital Evidence, 2002, Vol. 1, Issue 3, pp. 1-12.

[10] H. Khurana, J. Basney, M. Bakht, M. Freemon, V. Welch, R. Butler, Palantir: A Framework for Collaborative Incident Response and Investigation, Gaithersburg, MD, April 2009, pp. 1-14.

[11] ISO/IEC 27037, IT Security, Security Techniques and Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence, Last accessed on 14 August 2012 at http://www.iso27001security.com/html/27037.html.

[12] S. Alharbi, J.W.Jahnke, I.Traore, Proactive and Reactive Digital Forensics Investigation Process: A Systematic Literature Review, International Journal of Security and its Applications, October 2011, Vol. 5, No. 4, pp. 59-71.

[13] I. Kruse, G. Warren, J. Heiser, Computer Forensics: Incident Response Essentials, Addison Wesley, 2002.

[14] J. Ashcroft, National Institute of Justice, Electronic Crime Scene Investigation A Guide for First Responder, July 2001, Last accessed on 25 August 2012 at https://www.ncjrs.gov/pdffiles1/nij/187736.pdf

[15] Procedure Guide for Investigating Cyber Crime Cases, National Response Centre for Cyber Crime, Federal Investigation Agency, Last accessed on 14 August 2012 at http://www.nr3c.gov.pk/images/pdf/sops.pdf

[16] M. Grobler, Digital Forensic Standards: International Progress, South African Information Security Multi-Conference, 2010, pp. 261-271.

[17] G.Giova, Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems, International Journal of Computer Science and Network Security, January 2011, Vol. 11, No.1, pp. 01-09.

[18] International Organization on Computer Evidence, G8 Proposed Principles for the Procedures Relating to Digital Evidence, Last accessed on 14 September 2011 at http://www.ilook-forensics.org.

[19] G.Warren, I. Kruse, J. Heiser, Computer Forensics: Incident Response Essentials, Addison Wesley, 2001.

[20] E.S. Pilli, R.C. Joshi, R. Niyogi, A Generic Framework for Network Forensics, International Journal of Computer Applications, 2010, Vol. 1, No. 11, pp. 1-6.

[21] P. Gupta, J. Singh, A.K. Arora, S. Mahajan, Review Research Paper Digital Forensics- A Technological Revolution in Forensic Sciences, J Indian Acad Forensic Med. April-June 2011, Vol. 33, No. 2, pp. 971-973.

[22] Macquaire Dictionary, Macquaire Consice Dictionary-Australia's National Dictionary, 2006, 4th Edition, Macquaire Dictionary Publishers Ptv. Ltd.

[23] Jason Beckett, Forensic Computing: A Deterministic Model for Validation and Verification through an Ontological Examination of Forensic Functions and Processes, Research Thesis for the Degree of Doctor of Philosophy, 2010.

[24] Computer forensics and Anti-Forensics Research, Last accessed on 14 August 2012 at http://www.forensics-research.com/index.php/computer-forensics/concepts-and-standards.

[25] Forensic Tool Kit, Last accessed on 14 May 2012 at http://accessdata.com/support/product-downloads.

[26] Policy for Internet, Intranet, Website and E-mail in Federal Government Organizations, Last accessed on 14 May 2012 at

http://202.83.164.29/egdsite05/downloads/InternetE.MailsPolicy_Final%20Edition-EGD.pdf.

[27] S.O. Ciardhuain, An Extended Model of Cybercrime Investigations, International Journal of Digital Evidence, 2004, Vol. 3, pp. 1

[28] Electronic Transactions Ordinance, 2002. Last accessed on 3rd March 2013 at http://www.fia.gov.pk/ETO.pdf

[29] Prevention of Electronic Crimes Ordinance. Last accessed on 3rd March 2013 at http://www.na.gov.pk/uploads/documents/1302739058_910.pdf

[30] The Investigation for Fair Trial Act, 2013. Last accessed on 3rd March 2013 at http://www.na.gov.pk/uploa