Systematic Digital Forensic Investigation Model

Mr. Ankit Agarwal cs.ankit11@gmail.com
Sr. Lecturer,Northern India Engineering College, GGSIPU
Delhi- 110053 India

Ms. Megha Gupta meghag2@gmail.com
Lecturer,Northern India Engineering College, GGSIPU
Delhi- 110053 India

Mr. Saurabh Gupta er.saurabh@gmail.com
HOD,Northern India Engineering College, GGSIPU
Delhi- 110053India

Prof. (Dr.) Subhash Chandra Gupta gupta_subhash@yahoo.com
Director,Northern India Engineering College, GGSIPU
Delhi- 110053 India

Abstract

Law practitioners are in an uninterrupted battle with criminals in the application of digital/computer technologies, and require the development of a proper methodology to systematically search digital devices for significant evidence. Computer fraud and digital crimes are growing day by day and unfortunately less than two percent of the reported cases result in confidence. This paper explores the development of the digital forensics process model, compares digital forensic methodologies, and finally proposes a systematic model of the digital forensic procedure. This model attempts to address some of the shortcomings of previous methodologies, and provides the following advantages: a consistent, standardized and systematic framework for digital forensic investigation process; a framework which work systematically in team according the captured evidence; a mechanism for applying the framework to according the country digital forensic investigation technologies; a generalized methodology that judicial members can use to relate technology to non-technical observers.

This paper present a brief overview of previous forensic models and propose a new model inspired from the DRFWS Digital Investigation Model, and finally compares it with other previous model to show relevant of this model. The proposed model in this paper explores the different processes involved in the investigation of cyber crime and cyber fraud in the form of an eleven-stage model. The Systematic digital forensic investigation model (SRDFIM) has been developed with the aim of helping forensic practitioners and organizations for setting up appropriate policies and procedures in a systematic manner.

keywords : Digital Crime, Digital Devices, Forensic Investigation, Search & Seizure, Wireless devices.

1. INTRODUCTION

Computer forensics emerged in response to the escalation of crimes committed by the use of computer systems either as an object of crime, an instrument used to commit a crime or a repository of evidence related to a crime. Computer forensics can be traced back to as early as 1984 when the FBI laboratory and other law enforcement agencies begun developing programs to examine computer evidence. Research groups like the Computer Analysis and Response Team (CART), the Scientific Working Group on Digital Evidence (SWGDE), the Technical Working Group on Digital Evidence (TWGDE), and the National Institute of Justice (NIJ) have since been formed in order to discuss the computer forensic science as a discipline including the need for a standardized approach to examinations [1].

Digital forensics has been defined as the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal or helping to anticipate the unauthorized actions shown to be disruptive to planned operations. One important element of digital forensics is the credibility of the digital evidence. Digital evidence includes computer evidence, digital audio, digital video, cell phones, digital fax machines etc. The legal settings desire evidence to have integrity, authenticity, reproductively, non-interference and minimization [2].

Since computer forensics is a relatively new field compared to other forensic disciplines, which can be traced back to the early 1920s, there are ongoing efforts to develop examination standards and to provide structure to computer forensic examinations. This paper attempts to address the methodology of a computer forensic investigation.

2. PREVIOUS INVESTIGATION

Computer and network forensics methodologies consist of three basic components that Kruse and Heiser[3] refer to as the three as of computer forensics investigations. These are:

- Acquiring the evidence while ensuring that the integrity is preserved;
- Authenticating the validity of the extracted data, which involves making sure that it is as valid as the original
- Analyzing the data while keeping its integrity.

The field of digital forensics is undergoing a rapid metamorphosis: it is changing from skilled craftsmanship into a true forensic science. Part of this change is expressed by the interest in this field as an academic study. Ironically, the teaching portion of academe has led the way and research is trying to catch up.

Research usually starts with a literature review. That is particularly difficult in this field for a number of reasons. Some of the work predates the Internet and therefore is only available in paper form, in largely obscure or unavailable documents. Much discussion and learning has not been published at all. And few are familiar with the work that has been published.

2.1 The Forensic Process Model [4]

The U.S. Department of Justice published a process model in the Electronic Crime Scene Investigation: A guide to first responders that consists of four phases: -

- **Collection**

which involves the evidence search, evidence recognition, evidence collection and documentation.

- **Examination**

This is designed to facilitate the visibility of evidence, while explaining its origin and significance. It involves revealing hidden and obscured information and the relevant documentation.

- **Analysis**: This looks at the product of the examination for its significance and probative value to the case.

Reporting: This entails writing a report outlining the examination process and pertinent data recovered from the overall investigation.

here. Write the body of the paper here. Write the body of the paper here. Write the body of the paper here.

2.2 The Abstract Digital Forensic Model [5]

The Abstract Digital Forensics model proposes a standardized digital forensics process that consists of nine components:

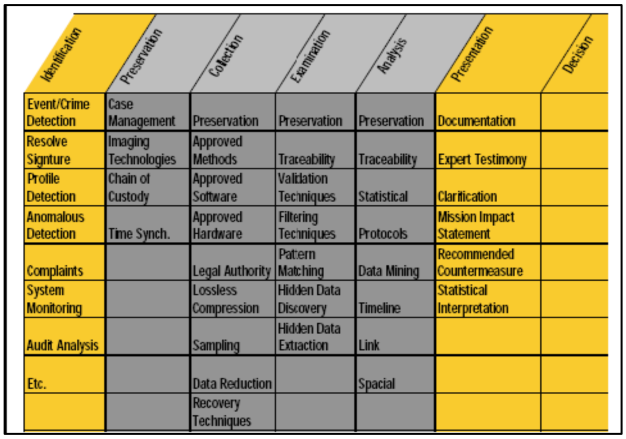
1. **Identification:** which recognizes an incident from indicators and determines its type.
2. **Preparation:** which entails the preparation of tools, techniques, search warrants, and monitoring authorizations and management support.

3. **Approach strategy**: that develops a procedure to use in order to maximize the collection of untainted evidence while minimizing the impact to the victim.
4. **Preservation:** which involves the isolation, securing and preservation of the state of physical and digital evidence.
5. **Collection:** that entails the recording of the physical scene and duplicate digital evidence using standardized and accepted procedures.
6. **Examination:** which involves an in-depth systematic search of evidence relating to the suspected crime.
7. **Analysis:** which involves determination of the significance, reconstructing fragments of data and drawing conclusions based on evidence found.
8. **Presentation:** that involves the summary and explanation of conclusions.
9. **Returning evidence:** that ensures physical and digital property is returned to proper owner.

2.3 Digital Forensic Research Workshop 2001[6]

At the first Digital Forensic Research Workshop held in Utica, NY in 2001, the group created a consensus document which outlined the state of digital forensics at that time. Among their conclusions was that digital forensics was a process with some reasonably agreed upon steps

.



Identification	Preservation	Collection	Examination	Analysis	Presentation	Decision
Event/Crime Detection	Case Management	Preservation	Preservation	Preservation	Documentation	
Resolve Signture	Imaging Technologies	Approved Methods	Traceability	Traceability	Expert Testimony	
Profile Detection	Chain of Custody	Approved Software	Validation Techniques	Statistical	Clarification	
Anomalous Detection	Time Synch.	Approved Hardware	Filtering Techniques	Protocols	Mission Impact Statement	
Complaints		Legal Authority	Pattern Matching	Data Mining	Recommended Countermeasure	
System Monitoring		Lossless Compression	Hidden Data Discovery	Timeline	Statistical Interpretation	
Audit Analysis		Sampling	Hidden Data Extraction	Link		
Etc.		Data Reduction		Spacial		
		Recovery Techniques				

FIGURE 1: DFRW Model

2.3 The Integrated Digital Investigation Model(IDIP)

Brian Carrier and Eugene Spafford [7] proposed yet another model that organizes the process into five groups consisting all in all 17 phases.

2.3.1 Readiness phases

The goal of this phase is to ensure that the operations and infrastructure are able to fully support an investigation. It includes two phases:

- **Operations Readiness phase**
- **Infrastructure readiness phase**

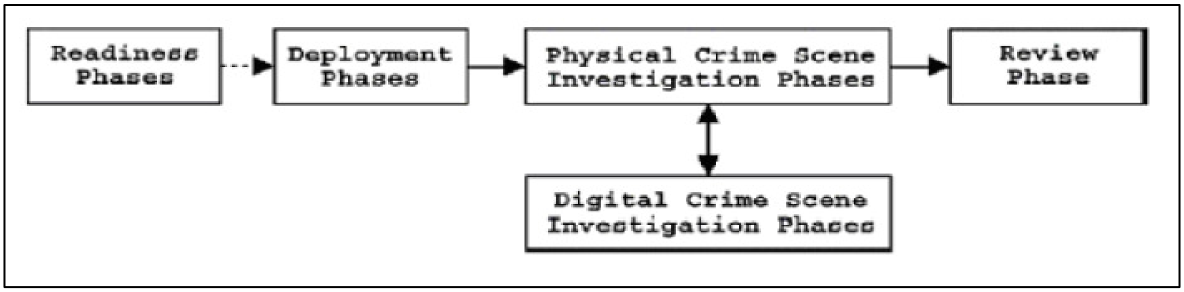

Readiness Phases
Deployment Phases
Physical Crime Scene Investigation Phases
Review Phase
Digital Crime Scene Investigation Phases

FIGURE 2: Phases of the IDIP Model

2.3.2 Deployment phases

The purpose is to provide a mechanism for an incident to be detected and confirmed. It includes two phases:

1. Detection and Notification phase; where the incident is detected and then appropriate people notified.
2. Confirmation and Authorization phase; which confirms the incident and obtains authorization for legal approval to carry out a search warrant.

2.3.3 Physical Crime Scene Investigation phases

The goal of these phases is to collect and analyze the physical evidence and reconstruct the actions that took place during the incident. It includes six phases:-

1. Preservation phase; which seeks to preserve the crime scene so that evidence can be later identified and collected by personnel trained in digital evidence identification.
2. Survey phase; that requires an investigator to walk through the physical crime scene and identify pieces of physical evidence.
3. Documentation phase; which involves taking photographs, sketches, and videos of the crime scene and the physical evidence. The goal is to capture as much information as possible so that the layout and important details of the crime scene are preserved and recorded.
4. Search and collection phase; that entails an in-depth search and collection of the scene is performed so that additional physical evidence is identified and hence paving way for a digital crime investigation to begin.
5. Reconstruction phase; which involves organizing the results from the analysis done and using them to develop a theory for the incident.
6. Presentation phase; that presents the physical and digital evidence to a court or corporate management.

2.3.4 Digital Crime Scene Investigation phases

The goal is to collect and analyze the digital evidence that was obtained from the physical investigation phase and through any other future means. It includes similar phases as the Physical Investigation phases, although the primary focus is on the digital evidence. The six phases are:-

1. Preservation phase; which preserves the digital crime scene so that evidence can later be synchronized and analyzed for further evidence.
2. Survey phase; whereby the investigator transfers the relevant data from a venue out of physical or administrative control of the investigator to a controlled location.
3. Documentation phase; which involves properly documenting the digital evidence when it is found. This information is helpful in the presentation phase.
4. Search and collection phase; whereby an in-depth analysis of the digital evidence is performed. Software tools are used to reveal hidden, deleted, swapped and corrupted files that were used including the dates, duration, log file etc. Low-level time lining is performed to trace a user’s activities and identity.

5. Reconstruction phase; which includes putting the pieces of a digital puzzle together, and developing investigative hypotheses.
6. Presentation phase; that involves presenting the digital evidence that was found to the physical investigative team.

3. The Need For Digital Forensic Investigation Models

It is important to understand the need of the “Digital Forensic Investigation Model” which is currently an active area of research in the academic world, which aims to ameliorate procedures followed in this field. The way Digital Forensic Science is implemented has a direct impact on

- The prevention of further malicious events occurring against the intended “target".
- The successful tracing back of the events that occurred which led to the crime, and determining the guilty parties involved.
- Bringing the perpetrators of the crime to justice.
- The improvement of current prevention mechanisms in place to prevent such an event from occurring again.
- Improving standards used by corporate security professionals to secure their respective corporate networks.
- How everyone “plugged" into this digital environment can increase their awareness about current vulnerabilities and prevention measures.

There has been a need for a standard methodology used for all Digital Forensics investigations. There have been many initiatives made to have models that have a general process to be followed for such investigations [8]. Research done by the scientific community has been fairly recent, and has concentrated mostly upon coming up with good models that can be practiced [9]. Yet, it can be safely said that these models are mainly ad-hoc and much needs to be accomplished in this particular domain.

4. KEY CHALLENGES

At the 2006 DFRWS conference, the keynote speech, “Challenges in Digital Forensics” was delivered by Ted Lindsey a computer scientist at the FBI [9]. In his speech, a number of the challenges were identified.
These are presented in Table 1.

Device diversity	Volume of evidence
Video and rich media	Whole drive encryption
Wireless	Anti-forensics
Virtualization	Live response
Distributed evidence	Usability & visualization

TABLE 1: Challenges in digital forensics - DFRWS 2006 keynote

These challenges as enumerated by Lindsey at DFRWS 2006 are a mix of: new technologies (e.g. wireless, whole drive encryption), situational technology trends (e.g. device diversity, volume of evidence, distributed evidence), and techniques (e.g. Live response, usability & visualization).
In 2005, the following list of challenges was presented by Mohay [10]:

- Education & certification
- Embedded systems
- Corporate governance and forensic readiness
- Monitoring the internet
- Tools
- Data volumes

In 2005 and 2004, Casey summarized the key challenges as:

- Counter forensics
- Networked evidence

- Keeping pace with technology
- Tool testing
- Adapting to shifts in law
- Developing standards and certification [11, 12]

5. Proposed Work: Systematic Digital Forensic Investigation Model (SRDFIM)

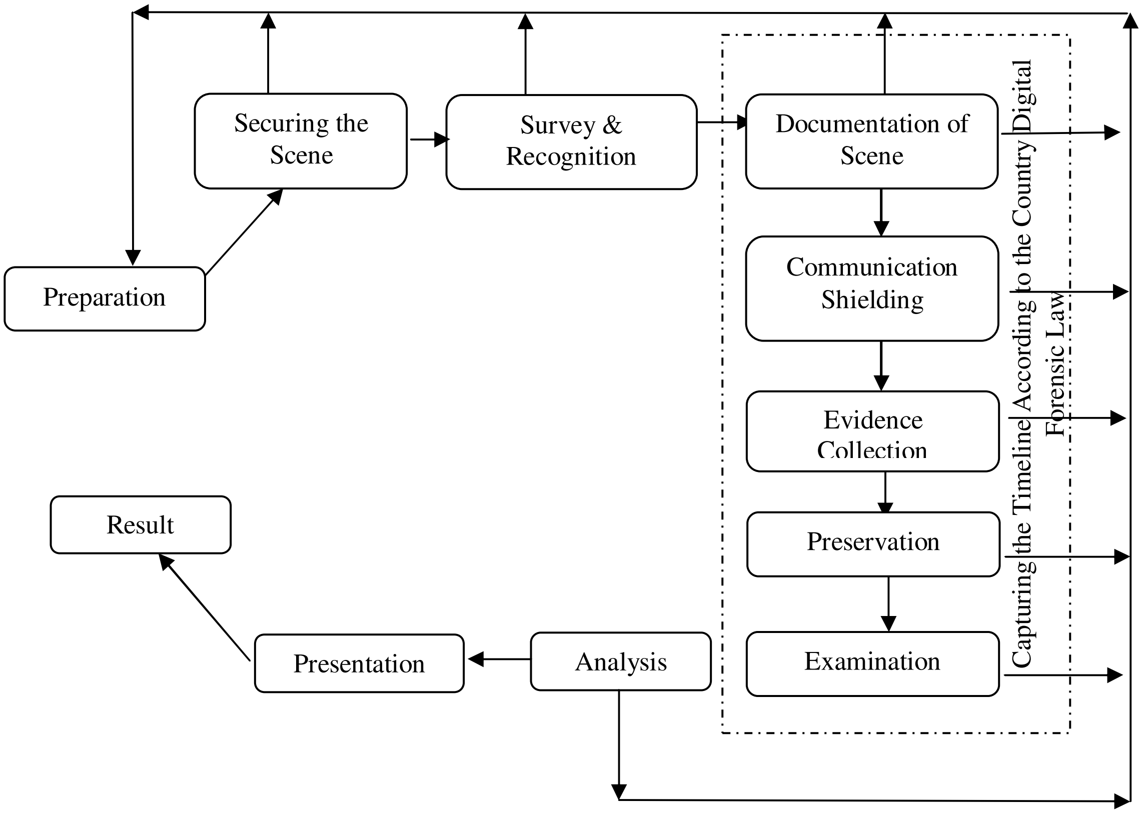


FIGURE2: Phases of Systematic Digital Forensic Investigation Model (SRDFIM)

5.1 Phase One - Preparation

The preparation phase occurs prior to the actual investigation. This involves getting an initial understanding of the nature of the crime and activities, prepare accumulating materials for packing evidence sources etc. It is very important to obtain the best possible assessment of the circumstances relating to the crime, prior to proceeding to the crime scene. A critical issue in the investigations involving digital devices is that the power runs out before evidence collection is over. The investigation should follow the various legal constraints and jurisdictional as well as organizational restrictions. This stage also involves obtaining search warrants, support from the management, required authorizations etc. before proceeding to the crime scene. The privacy rights of suspects should be taken into account. Legal notice must be provided to all concerned parties notifying about the forensic investigation. An appropriate strategy for investigation should be developed, having taken into account the nature of the incident and various technical, legal and business factors. Having a thorough preparation phase increases the quality of evidence and minimizes the risks and threats associated with an investigation.

5.2 Phase Two - Securing the Scene

This stage primarily deals with securing the crime scene from unauthorized access and preserving the evidence from being contaminated. There should be a formal protocol for handing over a crime scene in order to ensure that the chain of custody is properly followed. It will be difficult to judge how much at the crime scene actually the evidence is? The investigators should identify the scope of the crime and establish a perimeter. Ensuring the safety of all people at the scene and protecting the integrity of all evidence should also be the targets at this stage. The investigators should have absolute control of the scene and interference from unwanted people should be avoided. As the number of people at the crime scene increases, the possibilities for the contamination and destruction of evidence also increase. The crime scene investigation should follow Association of Chief Police Officers (ACPO), in conjunction with the National Hi-Tech Crime Unit (NHCTU) [13] guideline for securing the scene. Top priority should be given at this stage in minimizing the corruption of evidence. Any item that could be of evidence should not be tampered with. This phase plays a major role in the overall investigative process as it determines the quality of evidence.

5.3 Phase Three – Survey and Recognition

This stage involves an initial survey conducted by the investigators for evaluating the scene, identifying potential sources of evidence and formulating an appropriate search plan. In a complex environment, this may not be straightforward. In the case of Windows mobile devices, the major sources of evidence other than the device itself are the power adaptor, cradle, external memory cards, cables and other accessories. Since the information present in these devices can be easily synchronized with computers, any personal computer or laptop at the crime scene may also contain evidence. Evaluate the electronic equipments at the scene to determine whether any expert assistance is required in processing the scene. Identifying people in the scene and conducting preliminary interviews are extremely important. The owners or users of the electronic devices or system administrators can provide valuable information like the purpose of the system, security schemes, various applications present in the devices, user names, passwords, encryption details etc. Without violating the jurisdictional laws and corporate policies, the investigators must try to obtain the maximum information from the various people present in the scene. If it becomes necessary to search for items that are not included in the search warrant, appropriate amendments must be made to the existing warrant or a new warrant must be obtained, which includes the additional items. An initial plan for collecting and analyzing evidence must be developed at the end of the survey and recognition phase.

5.4 Phase Four - Documenting the Scene

This stage involves proper documentation of the crime scene along with photographing, sketching and crime-scene mapping. All the electronic devices at the scene must be photographed along with the power adaptors, cables, cradles and other accessories. If the digital or mobile device is in the on state, what is appearing on the screen should also be documented. A record of all visible data must be created, which helps in recreating the scene and reviewing it any time. This is particularly important when the forensic specialist has to do a testimony in a court, which could be several months after the investigation. Circumstances surrounding the incident, including those who reported the incident initially and at what date and time, should be included. It is necessary to keep a log of those who were present on the scene, those who arrived, those who left etc., along with the summary of their activities while they were at the scene. It is necessary to classify the people into separate groups like victims, suspects, bystanders, witnesses, other assisting personnel etc. and record their location at the time of entry. Documentation is a continuous loop back activity, required in all the stages of the investigation and required for maintaining proper chain of custody.

5.5 Phase five - Communication Shielding

This step occurs prior to evidence collection. At this stage, all further possible communication options of the devices should be blocked. Even if the device appears to be in off state, some communication features like wireless or Bluetooth may be enabled. This may result in overwriting the existing information and hence such possibilities should be avoided. In other situations where the device is in the cradle connected to a computer, synchronization mechanisms using ActiveSync might be enabled. This may also lead to the corruption of evidence. The best option after seizing a device is to isolate it by disabling all its communication capabilities. If the device is in the cradle, remove any USB or serial cable, which connects it to a computer.

5.6 Phase Six - Evidence Collection

Evidence collection of the digital or mobile devices is an important step and required a proper procedure or guideline to make them work. We can categorize evidence collection of the digital devices into two categories:

- Volatile Evidence Collection
- Non-Volatile Evidence Collection
-

5.6.1 Volatile Evidence Collection

Majority of the evidence involving mobile devices will be of volatile nature, being present in ROM. Collecting volatile evidence presents a problem as the device state and memory contents may be changed. The decision whether to collect evidence at the crime scene or later at a secured forensic workshop depends on the nature of the particular situation including the current power state. If the device is running out of battery power, the entire information will be lost soon. In that case, adequate power needs to be maintained if possible by using the power adaptor or replacing batteries. If maintaining the battery power seems doubtful, the contents of the memory should be imaged using appropriate tools as quickly as possible. A combination of tools must be used to obtain better results. If possible, an adequate power supply must be maintained by recharging the device or replacing the battery, whichever is appropriate. If it is not possible to provide sufficient power, the device must be switched off to preserve battery life and the contents of the memory. The presence of any malicious software installed by the user should also be checked at this stage.

5.6.2 Non-volatile Evidence Collection

This phase involves collecting evidence from external storage media supported by these devices, like MMC cards, compact flash (CF) cards, memory sticks, secure digital (SD) cards, USB memory sticks etc. Evidence from computers, which are synchronized with these devices, must be collected. Appropriate forensic tools must be used for collecting evidence to ensure its admissibility in a court of law. The integrity and authenticity of the evidence collected should be ensured through mechanisms like hashing, write protection etc. All power cables, adaptors, cradle and other accessories should also be collected. Care should be also taken to look for evidence of non-electronic nature, like written passwords, hardware and software manuals and related documents, computer printouts etc.

5.7 Phase Seven: Preservation

This phase includes packaging, transportation and storage. Appropriate procedures should be followed and documented to ensure that the electronic evidence collected is not altered or destroyed. All potential sources of evidence should be identified and labeled properly before packing. Use of ordinary plastic bags may cause static electricity. Hence anti-static packaging of evidence is essential. The device and accessories should be put in an envelope and sealed before placing it in the evidence bag. The evidence bag must be kept in a radio frequency isolation container to avoid further communications with any other device. All the containers holding these evidence bags must also be properly labeled. Adequate precautions are necessary as the sources of evidence could be easily damaged while transportation because of shock, excessive pressure, humidity or temperature. Afterwards the device can be moved to a secure location where a proper chain of custody can be maintained and examination and processing of evidence can be started. The evidence should be stored in a secure area and should be protected from electromagnetic radiations, dust, heat and moisture. Unauthorized people should not have access to the storage area. ***National Institute of Standards and Technology*** guideline highlights the need of proper transportation and storage procedures, for maintaining a proper chain of custody.

5.8 Phase Eight: Examination

This phase involves examining the contents of the collected evidence by forensic specialists and extracting information, which is critical for proving the case. Appropriate number of evidence back-ups must be created before proceeding to examination. This phase aims at making the evidence visible, while explaining its originality and significance. Huge volumes of data collected during the volatile and non-volatile collection phases need to be converted into a manageable size and form for future analysis. Data filtering, validation, pattern matching and searching for particular keywords with regard to the nature of the crime or suspicious incident, recovering relevant ASCII as well as non- ASCII data etc. are some of the major steps performed during this phase. Personal organizer information data like address book, appointments, calendar, scheduler etc, text messages, voice messages, documents and emails are some of the common sources of evidence, which are to be examined in detail. Finding evidence for system tampering, data hiding or deleting utilities, unauthorized system modifications etc. should also be performed. Detecting and recovering hidden or obscured information is a major tedious task involved. Data should be searched thoroughly for recovering passwords, finding unusual hidden files or directories, file extension and signature mismatches etc. The capabilities of the forensic tools used by the examiner play an important part in the examination phase. When the evidence is checked-out for examination and checked-in, the date, time, name of investigator and other details must be documented. It is required to prove that the evidence has not been altered after being possessed by the forensic specialist and hence hashing techniques like md5 must be used for mathematical authentication of data.

5.9 Phase Nine: Analysis

This step is more of a technical review conducted by the investigative team on the basis of the results of the examination of the evidence. Identifying relationships between fragments of data, analyzing hidden data, determining the significance of the information obtained from the examination phase, reconstructing the event data, based on the extracted data and arriving at proper conclusions etc. are some of the activities to be performed at this stage. ***The National Institute of Justice(2004)*** guidelines recommend timeframe analysis, hidden data analysis, application analysis and file analysis of the extracted data. Results of the analysis phase may indicate the need for additional steps in the extraction and analysis processes. It must be determined whether the chain of evidence and timeline of the events are consistent. Using a combination of tools for analysis will yield better results. The results of analysis should be completely and accurately documented.

5.10 Phase Ten: Presentation

After extracting and analyzing the evidence collected, the results may need to be presented before a wide variety of audience including law enforcement officials, technical experts, legal experts, corporate management etc. Depending on the nature of the incident or crime, the findings must be presented in a court of law, if it is a police investigation or before appropriate corporate management, if it is an internal company investigation. As a result of this phase, it should be possible to confirm or discard the allegations regarding the particular crime or suspicious incident. The individual results of each of the previous phases may not be sufficient to arrive at a proper conclusion about the crime. The results of examination and analysis must be reviewed in their entirety to get a complete picture. A report consisting of a detailed summary of the various steps in the process of investigation and the conclusions reached must be provided. In many cases, the forensic specialist may have to give an expert testimony in court. The complex terms involved in various stages of investigation process needs to be explained in layman’s terminology. The expertise and knowledge of the forensic examiner, the methodology adopted, tools and techniques used etc. are all likely to be challenged before a jury. Along with the report, supporting materials like copies of digital evidence, chain of custody document, printouts of various items of evidence etc. should also be submitted.

5.11 Phase Eleven - Result & Review

The final stage in the model is the review phase. This involves reviewing all the steps in the investigation and identifying areas of improvement. As part of the review phase, the results and their subsequent interpretation can be used for further refining the gathering, examination and analysis of evidence in future investigations. In many cases, much iteration of examination and analysis phases are required to get the total picture of an incident or crime. This information will also help to establish better policies and procedures in place in future.

6. Comparison With Existing Models

Table below gives a comparison of the activities in the proposed model with those in the major existing models described in the previous chapter. Some of the relevant activities in other models are incorporated in the proposed model. However there are many activities like communication shielding and bifurcation of evidence collection, which are unique for this model, as it is clear from the table.

ital Forensic odel	NIJ Law Enforcement Model	DRFWS Model	Abstract Digital Forensic Model	IDIP Model
			✓	✓
ene		✓		✓
gnition		✓	✓	✓
of Scene				✓
Shielding				
ce Collection				
idence Collection	✓	✓	✓	✓
		✓	✓	✓
	✓	✓	✓	✓
	✓	✓	✓	
	✓	✓	✓	✓
w				✓

TABLE 2: Mapping of Major Forensic Models to the Proposed Model

There may not always be a one-to-one mapping between the activities in the proposed model and other previous models. In some cases, though the process is similar, the terms used in other existing forensic models may differ. Table 2 gives a comparison of terminology used for different processes in the proposed model and various other models discussed in the previously.

NIJ Law Enforcement Model	DRFWS Model	Abstract Digital Forensic Model	D
--	--	Preparation	
--	Preservation	--	
--	Identification	Identification	
--	--	--	
--	--	--	
--	--	--	D
--	--	--	
--	--	--	
Collection	Collection	Collection	
--	Preservation	Preservation	
Examination	Examination	Examination	R
Analysis	Analysis	Analysis	
Reporting	Presentation	Presentation	
--	--	--	

TABLE 3: Mapping of Major Forensic Models to the Proposed Model

CONCLUSION

Motivated by the rapid increase in computer frauds and cyber crimes, this research work took the challenge to explore some of the open issues of digital forensic research. This paper starts with the discussion digital forensic technology then the discussion moves on to digital forensic investigation models. Some of the open problems of digital forensic research have been identified.

Then the proposed work provides Systematic Digital Forensic Investigation Model which is very use-full variety of digital forensic investigation.
The benefits of work are as follows:

- This will help in evidence dynamics and reconstruction of events by realizing the properties of Individuality, Repeatability, Reliability, Performance, Testability, Scalability, Quality and Standards in analysis of computer frauds and cyber crimes (CFCC).
- It will serve as benchmark and reference points for investigating cases of computer frauds and cyber crimes.
- It will help in the development of generalized solutions, which can cater to the need of rapidly changing and highly volatile digital technological scenario.
- The integrity and admissibility of digital evidence can be attained.

FUTURE SCOPE

In this study, work has been done in development of Systematic Digital Forensic Investigation Model. Following are few pointers for direction of future scope of research in these areas:

1. Application of the new model in variety of cases and improvement in light of feedback.
2. Identification of new constraints in terms of technological advancement will require model to be updated with time.

REFERENCES

1. Michael Noblett, Mark.M.Pollitt and Lawrence Presley. (2000) Recovering and Examining Computer Forensic Evidence, Forensic Science Communications, Volume 2, Number 4.

2. Gary L Palmer.(2001). A Road Map for Digital Forensic Research. Technical Report DTR-T0010-01, DFRWS. Report for the First Digital Forensic Research Workshop (DFRWS).

3. Kruse II, Warren and Jay, G. Heiser (2002) Computer Forensics: Incident Response Essentials. Addison-Wesley.

4. National Institute of Justice. (July 2001) Electronic Crime Scene Investigation. A Guide for First Responders.
Available from: http://www.ncjrs.org/pdffiles1/nij/187736.pdf.

5. Mark Reith, Clint Carr and Gregg Gunsch.(2002)An Examination of Digital Forensic Models International Journal of Digital Evidence, Fall 2002,Volume 1, Issue 3.

6. Digital Forensic Research Workshop (DFRWS) Research Road Map, Utica, NY. (2001) http://www.dfrws.org/archive.html

7. Brian Carrier and Eugene H Spafford,(2003) Getting Physical with the Investigative Process International Journal of Digital Evidence.Fall 2003,Volume 2, Issue 2.

8. M. M. Pollitt. An ad hoc review of digital forensic models. In Systematic Approaches to Digital Forensic Engineering, 2007, pages 43{54. University of Central Florida, USA, IEEE, April 10-12, 2007 2007.

9. Lindsey, T. Challenges in Digital Forensics. 2006
Available from: http://www.dfrws.org/2006/proceedings/Lindsey-pres.pdf.

10. Toward Models for Forensic Analysis, Sean Peisert, Matt Bishop, Sidney Karin, Keith Marzullo.Mohay, G. Technical Challenges and Directions for Digital Forensics. in 1st International Workshop on Systematic Approaches to Digital Forensic Engineering,. 2005.

11. Casey, E., State of the field: growth, growth, growth. Digital Investigation, 2004.

12. Casey, E., Digital arms race, The need for speed. Digital Investigation, 2005.

13. ACPO. Good Practise Guide for Computer based Electronic Evidence. 2006
Available from:
http://www.acpo.police.uk/asp/policies/Data/gpg_computer_based_evidence_v3.pdf.