Digital Forensics

Ravneet Kaur, Amandeep Kaur
Assistant Professor in Computer Science
SDSPM College for Women, Rayya (Asr)
Guru Nanak Dev University, India

ABSTRACT
Digital forensics is a branch of forensic science concerned with the use of digital information produced, stored and transmitted by computers as source of evidence in investigations and legal proceedings. Digital forensics has existed for as long as computers have stored data that could be used as evidence. For many years, digital forensics was performed primarily by government agencies, but has become common in the commercial sector over the past several years. Originally, much of the analysis software was custom and proprietary and eventually specialized analysis software was made available for both the private and public sectors. The first part of this paper provides a brief overview of digital forensics Process, followed by the models of digital forensics. In the further part of the paper, we consider 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. At last, we discuss challenges and future scope of digital forensics.

General Terms
Cyber Crime, forensics models, Investigation, Analysis, digital devices.

Keywords
Digital forensics, Investigation model, forensics process, digital crime, digital 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. Digital Forensic can be defined as

> "The use of scientifically derived and proven methods toward the preservation, validation, identification, analysis, interpretation, documentation 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 unauthorized actions shown to be disruptive to planned operations." [4]

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), Laboratory Accreditation Board (ASCLD-LAB), 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 [2]. International Data Corporation (IDC) reported that the market for intrusion-detection and vulnerability-assessment software will reach 1.45 billion dollars in 2006.

Major initiatives
- National White Collar Crime Center (NW3C)
- National Center for Forensic Sciences (NCFS)
- Digital Forensics Research Workshop (DFRW)
- Computer Forensic Educator's Working Group (CFEWG)
- Cyber Tools Online Search for Evidence (CTOSE) – European

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, reproductivity, non-interference and minimization.

2. 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 [5]. Research done by the scientific community has been fairly recent, and has concentrated mostly upon coming up with good models that can be practiced [7]. Yet, it can be safely said that these models are mainly ad-hoc and much needs to be accomplished in this particular domain.

3. INVESTIGATION PROCESS OF DIGITAL FORENSICS

Investigative process of digital forensics can be divided into several stages. There are four major stages: preservation, collection, examination, and analysis see figure 1.

Figure1. Digital forensics Process

- **Preservation:** Preservation stage corresponds to \freezing the crime scene". It consists in stopping or preventing any activities that can damage digital information being collected. Preservation involves operations such as preventing people from using computers during collection, stopping ongoing deletion processes, and choosing the safest way to collect information.
- **Collection:** Collection stage consists in finding and collecting digital information that may be relevant to the investigation. Since digital information is stored in computers, collection of digital information means either collection of the equipment containing the information, or recording the information on some medium. Collection may involve removal of personal computers from the crime scene, copying or printing out contents of files from a server, recording of network traffic, and so on.
- **Examination:** Examination stage consists in a \in-depth systematic search of evidence" relating to the incident being investigated. The outputs of examination are data objects found in the collected information. They may include log files, data files containing specific phrases, times-stamps, and so on.
- **Analysis:** The aim of analysis is to "draw conclusions based on evidence found".
- **Reporting:** This entails writing a report outlining the examination process and pertinent data recovered from the overall investigation.

4. THE ABSTRACT DIGITAL FORENSIC MODEL

The abstract digital forensics model [1] proposes a standardized digital forensics process that consists of nine components:

1. Identification: It recognizes an incident from indicators and determines its type.

2. Preparation: Preparation entails the preparation of tools, techniques, search warrants, and monitoring authorizations and management support.

Figure2: The abstract digital forensic model

3. Approach strategy: It develops a procedure to use in order to maximize the collection of untainted evidence while minimizing the impact to the victim.

4. Preservation: Preservation which involves the isolation, securing and preservation of the state of physical and digital evidence.

5. Collection: It entails the recording of the physical scene and duplicate digital evidence using standardized and accepted procedures.

6. Examination: It involves an in-depth systematic search of evidence relating to the suspected crime.

7. Analysis: Analysis involves determination of the significance**,** reconstructing fragments of data and drawing conclusions based on evidence found.

8. Presentation: It involves the summary and explanation of conclusions.

9. Returning evidence: It ensures physical and digital property is returned to proper owner.

5. THE INTEGRATED DIGITAL INVESTIGATION MODEL (IDIP)

5.1 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

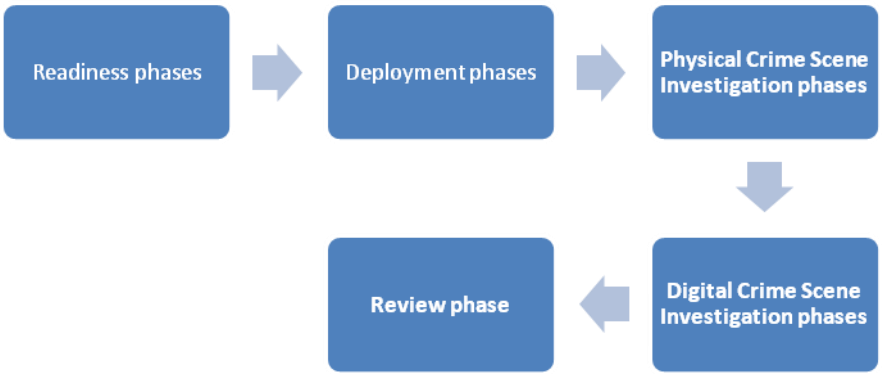

Figure3. The integrated digital investigation model (IDIP)

5.2 Deployment phases

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

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

5.3 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:-

- **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.
- **Survey phase;** that requires an investigator to walk through the physical crime scene and identify pieces of physical evidence.
- **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.
- **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
- **Reconstruction phase;** which involves organizing the results from the analysis done and using them to develop a theory for the incident.
- **Presentation phase;** that presents the physical and digital evidence to a court or corporate management.

5.4 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:-

- **Preservation phase;** which preserves the digital crime scene so that evidence can later be synchronized and analyzed for further evidence.
- **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.
- **Documentation phase;** which involves properly documenting the digital evidence when it is found. This information is helpful in the presentation phase.
- **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.

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

5.5 Review phase

This entails a review of the whole investigation and identifies areas of improvement.

The IDIP model does well at illustrating the forensic process, and also conforms to the cyber terrorism capabilities [6] which require a digital investigation to address issues of data protection, data acquisition, imaging, extraction, interrogation, ingestion/normalization, analysis and reporting. It also highlights the reconstruction of the events that led to the incident and emphasizes reviewing the whole task, hence ultimately building a mechanism for quicker forensic examinations.

6. RESEARCH CHALLENGES & OPEN PROBLEMS[9]

6.1 Research challenges

- Device Diversity
- Volume of Evidence
- Distributed Evidence
- Trust of Audit Trails
- Testing and Validation
- Anti-forensics

Challenge 1: Device Diversity

- **Traditional storage devices**: Simple data and image files.
- **We are seeing**
  - Video, audio, GIS materials, VoIP systems, sensor net data, SCADA systems, etc.
  - Increasing usage of USB thumb drive, iPod, cell phone/PDA, digital camera, remote storage devices, removable media
  - Long-term storage in appliances and home media blur the notion of "local storage"
  - Peer-to-peer file sharing
  - Data outsourcing: Google Docs, Yahoo Photo Album, and many others

Challenge 2: Image Large, Active Disk Farms

- How to image large, active disk farms dynamically?
  - Imagine asking amazon.com or ebay to discontinue service while the drives are being copied

Challenge 3: Anti Forensics

- Encryption
  - Encrypted files & Whole drive encryption (EFS)
- Steganography and other information hiding
- Evidence elimination tools

Challenge 4: Trust of Audit Trails

- How can we trust audit trails?
  - Always possible that an intruder may edit or delete the audit trail on a computer, especially weakly-protected PC.
  - Increasingly sophisticated rootkits that dynamically modify the kernels of running systems to hide what is happening, or even to produce false results

6.2 Open Problems

There are various open hard problems. Here is just a list of samples:

- Forensic tool testing and validation Open vs. Close Source
- Solutions against anti-forensics techniques
- Network attack attribution
  - Botmasters
  - Criminals using stepping stones or Tor
  - Anonymous VoIP threatening callers
- Fighting against online fraudsters
  - Click fraud
  - Auction frauds
  - Spammers
  - Phishing
- Insiders
- Digital right management related issues.

7. 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. Future research should sample a larger number of respondents, collect detailed demographics information and not only look at identifying issues, but also obtain feedback on methods for addressing these issues.

2. Application of the new model in variety of cases and improvement in light of feedback.

3. Identification of new constraints in terms of technological advancement will require model to be updated with time.

8. REFERENCES

[1] 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.

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

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

[4] 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).

[5] 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.

[6] National Institute of Justice. (2002). **Results from Tools and Technology Working Group, Governors Summit on Cybercrime and Cyberterrorism**, Princeton NJ.

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

[9] Dr. Yong Guan, Digital Forensics: Research Challenges and Open Problems December 4, 2007