A Study of Digital Forensic: Process and Tools

Ms. Sandhya Dahake
MCA, GHRIIT
G. H. Raisoni Institute of Information Technology.
Nagpur

Ms. Shubhangi Daware
MCA, GHRIIT
G. H. Raisoni Institute of Information Technology
Nagpur

ABSTRACT
This paper deals with the study of digital tools and techniques used in the field of digital forensic and evidences handled. Today's major problem is about the reliability and in field of computer science it is focused on information assurance. In this paper we focused on on an emerging subspecialty within information assurance that is largely driven by software technology -- that of Digital Forensics. Digital forensics is a combination of the use of software, computer science, software engineering, and criminal justice procedures to explore and or investigate digital media with the objective of finding evidence to support a criminal or administrative case. It involves the preservation, identification, extraction, and documentation of computer or network evidence. Digital forensic is part of forensic science that implicitly covers crime that is related to computer technology. In a cyber crime, digital evidence investigation requires a special procedures and techniques in order to be used and be accepted in court of law.

Keywords
forensic, digital, evidence,investigation, abstract

INTRODUCTION
Digital forensic is a collection of specialized techniques, processes, and procedures used to preserve, extract, analyze, and present electronic evidence. It is also a methodology for computer investigation and analysis techniques in the interest of determining potential legal evidence. It is a process of extracting ***evidence*** from computers or other digital devices Usually involves extracting the contents of files and interpreting their meanings.

Digital forensics - "computer forensics" in older terminology - is the discovery, recovery, and investigation of digital information. The term "digital forensics" is usually used in connection with the investigation of a crime. But it also applies to recovery of an accidentally deleted file, or a forgotten password. Digital forensic techniques involve the application of science to the identification, collection, examination, and analysis of data in ways that preserve the integrity of the information and maintain a strict chain of custody for the data. Organizations have the means to collect growing amounts of data from many sources. Data is stored or transferred by standard IT systems, networking equipment, computing peripherals, personal digital assistants (PDAs), consumer electronic devices, and various types of media. When information security incidents occur, organizations that have established a capability to apply digital forensic techniques can examine and analyze the data that they have collected, and determine if their systems and networks may have sustained any damage and if sensitive data may have been compromised. Digital forensic techniques can be used for many purposes, such as supporting the investigation of crimes and violations of internal policies, analyses of security incidents, reviews

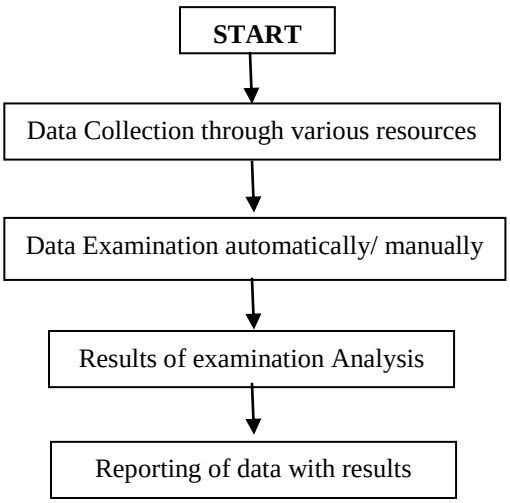
1. THE FORENSIC PROCESS
A four-step process for applying digital forensic techniques in consistent manner:

1.1 Collection:
Data is identified, labeled, recorded and acquired from all of the possible sources of relevant data, using procedures that preserve the integrity of the data. Data should be collected in a timely manner to avoid the loss of dynamic data, such as a list of current network connections, and the data collected in cell phones, PDAs, and other battery-powered devices.

1.2 Examination:
The data that is collected should be examined using a combination of automated and manual methods to assess and extract data of particular interest for the specific situation, while preserving the integrity of the data.

1.3 Analysis:
The results of the examination should be analyzed, using well-documented methods and techniques, to derive useful information that addresses the questions that were the impetus for the collection and examination.

1.4 Reporting:
The results of the analysis should be reported. Items to be reported may include: a description of the actions employed; an explanation of how tools and procedures were selected; a determination of any other actions that should be performed, such as forensic examination of additional data sources, securing identified vulnerabilities, and improving existing security controls; and recommendations for improvements to policies, guidelines, procedures, tools, and other aspects of the forensic process.



2. THE ABSTRACT DIGITAL FORENSIC MODEL

This model is advanced and extra featured model used for digital forensics. The components of model are elaborated and presented in detailed manner. There are nine components used.

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

This model is generally a good reflection of the forensic process, it is open to at least one criticism. Its third phase (the approach strategy) is to an extent a duplication of its second phase (the preparation phase). This is because at the time of responding to a notification of the incident, the identification of the appropriate procedure will likely entail the determination of techniques to be used.

3. AVAILABLE TOOLS FOR DIGITAL FORENSIC

Tools are the predefined software or methods which are available for application of digital forensic.

The following tools are available:

i. FTK
ii. ENCASE
iii. SELUTHKIT
iv. AUTOPSY
v. FOREMOST AND SCALPEL
vi. PYFLAG
vii. PTK
viii. FIT4D

3.1 FTK

IT is an advanced Code Breaking and Password Recover. This tool is full Unicode and provides code Page Support. It also gives advanced Email support. Powerful Search Functionality. Registry Supplemental Reports are provided by FTK. It is very easy to use as interface.

3.2 Encase

It securely investigate/analyze many machines simultaneously. Limit incident impact and eliminate system downtime with immediate response capabilities. Investigates and analyze multiple platforms. Efficiently collect only potentially relevant data. Audit large groups of machines for sensitive or classified information. Identify fraud, security events and employee integrity issues.

3.3 Seluthkit

Collection of UNIX-based command line file and volume system forensic analysis tools. Analyzes raw (i.e. *dd*), Expert Witness (i.e. EnCase) and AFF file system and disk images. Various analysis Techniques-meta-data structure analysis, time line generation, sort files based on their types etc.

3.4 Autopsy

It is a GUI for *Sleuthkit* . Dead analysis and live analysis is done with the help of autopsy. Case management using client server model. Various analysis Techniques-meta-data structure analysis, keyword search, time line generation, sort files based on their types etc.

3.5 Foremost and scalpel:

Linux program to recover files based on their headers and footers. Can work on image files, such as those generated by *dd*, Safeback, Encase, etc, or directly on a drive. The headers and footers are specified by a configuration file, so you can pick and choose which headers you want to look for.

3.6 Pyflag:

PyFlag is a forensic and log analysis GUI and computer forensics framework written in python. Basically it provides features for log analysis, disk forensic and network forensic.
Disk forensic -extracting forensic information from hard disk images, keyword search , MD5 hash comparison. Used in log analysis. It works as network forensic.

3.7 PTK:

Enhanced GUI for *Sleuthkit*-extended version of autopsy. Indexing Engine. Disk image integrity. Various analysis Techniques-meta-data structure analysis, keyword search, time line generation, gallery, file filtering etc.

3.8 FIT4D:

A software toolkit utilizes the limited resources in developing countries. Improves the efficiency, privacy and usability. Addresses the problem of lack of forensic experts in developing countries. A low-cost, distributed infrastructure to deploy the FIT4D software toolkit.

3.DIGITAL FORENSIC TECHNIQUES

Digital forensic techniques involve the application of science to the identification, collection, examination, and analysis of data in ways that preserve the integrity of the information and maintain a strict chain of custody for the data. Organizations have the means to collect growing amounts of data from many sources. Data is stored or transferred by standard IT systems, networking equipment, computing peripherals, personal digital assistants (PDAs), consumer electronic devices, and various types of media. When information security incidents occur, organizations that have established a capability to apply digital forensic techniques can examine and analyze the data that they have collected, and determine if their systems and networks may have sustained any damage and if sensitive data may have been compromised. Digital forensic techniques can be used for many purposes, such as supporting the investigation of crimes and violations of internal policies, analyses of security incidents, reviews of operational problems, and recovery from accidental system damage.

4. WHAT IS EVIDENCE?

The degree of the reliability, integrity, and availability of information in organizations can determine the credibility of the organization. As people and applications generate information, the information is stored in various places. It is vital for the organization to know where information is stored, what format it

is, and how to access it. Not all information will be evidence but it is essential that organizations identify potential evidence proactively. Good evidence is a business enabler. Organizations require `good' evidence to demonstrate due diligence with respect to good corporate and IT governance and to investigate and manage internal and external incidents. All internal and external forensic investigations hinge on `good' evidence. Evidence in itself is not absolute, but is valuable when used to establish the truth about a particular incident. Digital forensic evidence is and must be considered in light of the legal context of the matter at hand.

5.APPLICATIONS AND FUTURE SCOPE

Digital Forensic is very widely used and applicable in identification of criminals as well as crimes. There are almost all areas and branches in which this technique is used successfully. Depending on the evidence and the constraints the procedure can be modified and the desired results can be obtained effectively.

7.1 APPLICATIONS

1. Digital forensic is applicable in the future Enterprise Resource Planning Systems.
2. Recent development in digital image processing
3. Accuracy enhancement in environment sound recognition using ZC features and MPEG-7 with modified K-NN classifier feature
4. Digital forensic in VoIP Networks
5. Development and Application of Digital Forensic Logging System for Data from a Keyboard and Camera
6. An Analysis of the Digital Forensic Examination of Mobile Phones

REFERENCES

[1] G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[4] K. Elissa, “Title of paper if known,” unpublished.

[5] R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[7] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[8] Computer Forensic Tool Testing Program, *Computer Imaging Specification*, Version 3.1.6, National Institute of Standards and Technology. Available at: www.cftt.nist.gov

[9] Eckert, W. G., *Introduction to Forensic Sciences*, 1997, CRC Press.

[10] Federal Rules of Evidence, Article VII. Opinion and Expert Testimony, Rule 702 & Rule 703. Available at: www.house.gov/judiciary/evid00.pdf

[11] Foster, K., R Huber, *Judging Science: Scientific Knowledge and the Federal Courts*, 1997, MIT Press.

[12] Koehler, J. J., A. Chia, S. Lindsey, , “The Random Match Probability in DNA evidence: Irrelevant or Prejudicial,” *Jurimetrics Journal*, 1995, Winter, pp. 201-219.

[13] Pollack J., US District Court, PA: U.S. v Plaza, Acosta (Cr. No. 98-362-10, 11,12), “Strengthening the Criteria for Admissibility of Fingerprint Evidence,” *Judicial Opinion*. Available at: www.paed.uscourts.gov/documents/opinions/02D0046P.htm