2024

Digital Records and Cyber Forensics

Dr. Babasaheb Ambedkar Open University

Digital Records and Cyber Forensics

Course Writer

Mr.Yogesh Thandge	Cyber Forensic Analysts & Independent Consultant,Pune, Maharashtra
Dr.Deesha Khaire	Assistant Professor (Law), Gujarat National Law University, Gandhinagar, Gujarat

Content Editors

Prof. (Dr.) Nilesh K. Modi	Professor & Director, School of Computer Science Dr. Babasaheb Ambedkar Open University, Ahmedabad, Gujarat

ISBN: 978-81-949119-2-0

Printed and published by: Dr. Babasaheb Ambedkar Open University, Ahmedabad

While all efforts have been made by editors to check accuracy of the content, the representation of facts, principles, descriptions and methods are that of the respective module writers. Views expressed in the publication are that of the authors, and do not necessarily reflect the views of Dr. Babasaheb Ambedkar Open University. All products and services mentioned are owned by their respective copyrights holders, and mere presentation in the publication does not mean endorsement by Dr. Babasaheb Ambedkar Open University. Every effort has been made to acknowledge and attribute all sources of information used in preparation of this learning material. Readers are requested to kindly notify missing attribution, if any.

Dr. Babasaheb Ambedkar Open University

MCA-E4-305

Digital Records and Cyber Forensics

Block-1: INTRODUCTION TO FORENSIC CONCEPTS

Block-2: CYBER FORENSICS PROCESS, STANDARDS AND CHALLENGES

Block-3: ROLE AND ANALYSIS OF CYBER FORENSICS

Block-4: CYBER FORENSICS FROM LAW ENFORCEMENT PERSPECTIVE

Block-1
Introduction to Forensics Concept

1

Unit 1: Basics of Forensic Concepts

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Evolution of Computer Forensics
- Scope of Cyber Forensics
- Investigation process

1.2 INTRODUCTION

The advancement of Information and Communication Technologies (ICT) opens new avenues and ways for cybercriminals to commit crime. The recent development in Information Communication Technology (ICT) has made tremendous changes in every aspect of our life. These changes have been clearly reflected in cyberspace-related areas.[1] Cybercrime describes a wide range of circumstances in which technology is involved in the commission of a crime. It presents numerous and constantly evolving challenges to government and law enforcement. Cybercrime is an umbrella term used to describe two distinct but closely related criminal activities i.e., ***Cyber-dependent and Cyber-enabled crimes.*** The former are offences that can only be committed by using a computer, computer networks, or another form of ICT. These acts include the spreading of viruses and other malicious software and distributed denial of service (DDoS) attacks. Cyber-dependent crimes are primarily acts directed against computers or network resources, although there may be secondary outcomes from the attacks, such as fraud and the latter, Cyber-enabled crimes, are traditional crimes that are increased in their scale or reach by the use of computers, computer networks or another form of ICT.

Computer forensics is the practice of collecting, analysing and reporting on digital data in a way that is legally admissible. It can be used in the detection and prevention of crime and in any dispute where evidence is stored digitally. It deals with the preservation, identification, extraction and documentation of computer evidence. Like many other forensic sciences, computerforensics involves the use of sophisticated technological tools and procedures that must be followed to guarantee the accuracy of the preservation of evidence and the accuracy of results concerning computer evidence processing. The use of specialized techniques for recovery,authentication, and analysis of computer data, typically of data which may have been deletedor destroyed.[2]

Digital forensics is the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating

[1] "Bridging the gap in Legislation, Investigation <https://vc.bridgew.edu/ijcic/vol2/iss1/5/>

[2] Cybercrime and Digital Forensics: Bridging the gap <https://vc.bridgew.edu/cgi/viewcontent.cgi?article=1014&context=ijcic>

or furthering the reconstruction of events found to be criminal; or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

1.3 EVOLUTIONS OF COMPUTER FORENSICS

The field of Computer Forensics began to evolve more than 30 years ago. The field began in the United States, in large part, when law enforcement and military investigators started seeing criminals get technical. The fields of information security which focuses on protecting information and assets, and computer forensics, which focuses on the response of hi-tech offenses, started to intertwine. The history of forensic science dates back thousands of years. Fingerprinting was one of its first applications. The ancient Chinese used fingerprints to identify business documents. In 1892, a eugenicist named Sir Francis Galton established the first system for classifying fingerprints. Sir Edward Henry, the commissioner of the Metropolitan Police of London, developed his own system in 1896 based on the direction, flow, pattern and othercharacteristics in fingerprints.[3] The Henry Classification System became the standard forcriminal fingerprinting techniques worldwide.The timeline of the evolution of computer forensics are as follows:-

YEAR	EVENT
1835	Scotland Yard's Henry Goddard became the first person to use physical analysis to connect a bullet to murder weapon. Later, a team of scientists at the Aerospace Corporation in California developed a method for detecting gunshot residue using scanning electron microscopes.
1836	James Marsh developed a chemical test to detect arsenic, which was used during the murder trial.
1892	Sir Francis Galton established the first system for classifying fingerprints.
1896	Sir Edward Henry, based on the direction, flow, pattern and other characteristics in

[3] Richard III GG, Roussev V Next-generation digital forensics. Communications of the ACM 2006 Feb 1;49(2):76-80

	fingerprints.
1920	American physician Calvin Goddard created the comparison microscope to help determine which bullets came from which shell casings.
1930	Karl Landsteiner won the Nobel Prize for classifying human blood into its various groups.
1970	Aerospace Corporation in California developed a method for detecting gunshot residue using scanning electron microscopes.
1984	FBI Magnetic Media program, which was later renamed to Computer Analysis and Response Team (CART), was created and it is believed to be the beginning of computer forensic.
1988	International Association of Computer Investigative Specialists (IACIS) was formed.
1995	International Organization on Computer Evidence (IOCE) was formed.
1997	G8 nations declared that "Law enforcement personnel must be trained and equipped to address high-tech crimes".
1998	- G8 appointed IICE to create international principles, guidelines and procedures relating to digital evidence. - 1st INTERPOL Forensic Science Symposium was held.
2000	First FBI Regional Computer Forensic Laboratory was established.

1.4 OBJECTIVES OF COMPUTER FORENSICS

The objectives of Computer forensics are to provide guidelines for:[4]

- Following the first responder procedure and access the victim's computer after the incident.

[4] Rogers MK, Seigfried K The future of computer forensics: a needs analysis survey Computers & Security. 2004 Feb 29;23(1):12-6

- Designing procedures at a suspected crime scene to ensure that the digital evidence obtained is not corrupted.
- Data acquisition and duplication.
- Recovering deleted files and deleted partitions from digital media to extract the evidence and validate them.
- Provide guidelines for analysing digital media to preserve evidence, analysing logs and deriving conclusions, investigate network traffics and logs to correlate events, investigate wireless and web attacks, tracking emails and investigate email crimes.
- Producing computer forensic report which provides complete report on computer forensic investigation process.
- Preserving the evidence by following the chain of custody.
- Employing the rigorous procedures necessary to have forensic results stand up to scrutiny in a court of law.
- Presenting digital forensics results in a court of law as an expert witness.

1.5 BASIC CONCEPT OF COMPUTER FORENSIC

Regardless of specific case or technology used, the concept of computer forensics is constant and consists of four basic steps which include:

- ***Preparation***

  Preparation includes understanding local laws, legal issues and determination of tools and procedures to employ in carrying out computer forensics tasks. This step also includes understanding the assignment at hand, preparing the team, and checking equipment.

- ***Collection***

  This involves on-site acquisition of digital evidence by making binding copy of hard drives and learning the unusual or evidence collection and taking the collected evidence to the laboratory where evidence acquisition is made. Another method of collection is live forensics when evidence is collected from powered-on computers.

- ***Examination and Analysis***

This is a key area of computer forensics and involves examination of data, internet artefacts, temporary files, spool files, shortcuts, keywords search and dealing with encryption.

- ***Reporting***

This involves a court expert report being made according to valid templates. The reports are written the way the judges and prosecutors understand it.[5]

1.6 USES OF COMPUTER FORENSICS

The uses of computer forensics include the following:

- Detecting a cybercrime.
- Solving an alleged criminal activity provided the medium used in perpetrating the crime is a digital device.
- Forestalling a crime from taking place.
- Computer forensics investigations are often used to refute or support a supposition during civil, criminal and corporate litigations.
- Computer forensics is used in the private sector by companies who are undergoing internal investigations into unauthorized technical and network transgressions.

Computer forensics is used in a variety of cases such as:-

- Intellectual Property Theft
- Industrial espionage
- Employment disputes
- Fraud investigations
- Forgeries
- Bankruptcy investigations
- Inappropriate email and internet use in the workplace
- Regulatory compliance

[5] Prasanthi, B. V. "Cyber Forensic Tools: A Review" International Journal of Engineering Trends and Technology (IJETT) 41.Number-5 (2016): 6

1.7 ETHICS TO BE FOLLOWED BY DIGITAL FORENSICS EXPERT

Digital Forensic expert is an investigator that investigates the digital evidence. The task of the Digital Investigator is very crucial as any information left can lead the case in a different situation.[6] So some ethics are expected to be followed by the Digital Investigator while conducting the investigation such as:

- The investigator should not delete or alter any evidence i.e., any proof related to the case should be kept at secure place and should not be damaged.
- Should protect the computer/digital devices against viruses viz-a-viz viruses should be removed so that they don't destroy any information.
- Keep a log of all work done.
- Keep any Client Attorney information that is gained confidential.

The role of Digital Investigator in a Forensic investigation of a crime is complicated which starts at the crime scene, continues into the computer labs for deep investigation, and ends in the court where the final judgment is done. There is no scope of negligence at all.

1.8 IMPLICATIONS OF DIGITAL FORENSICS

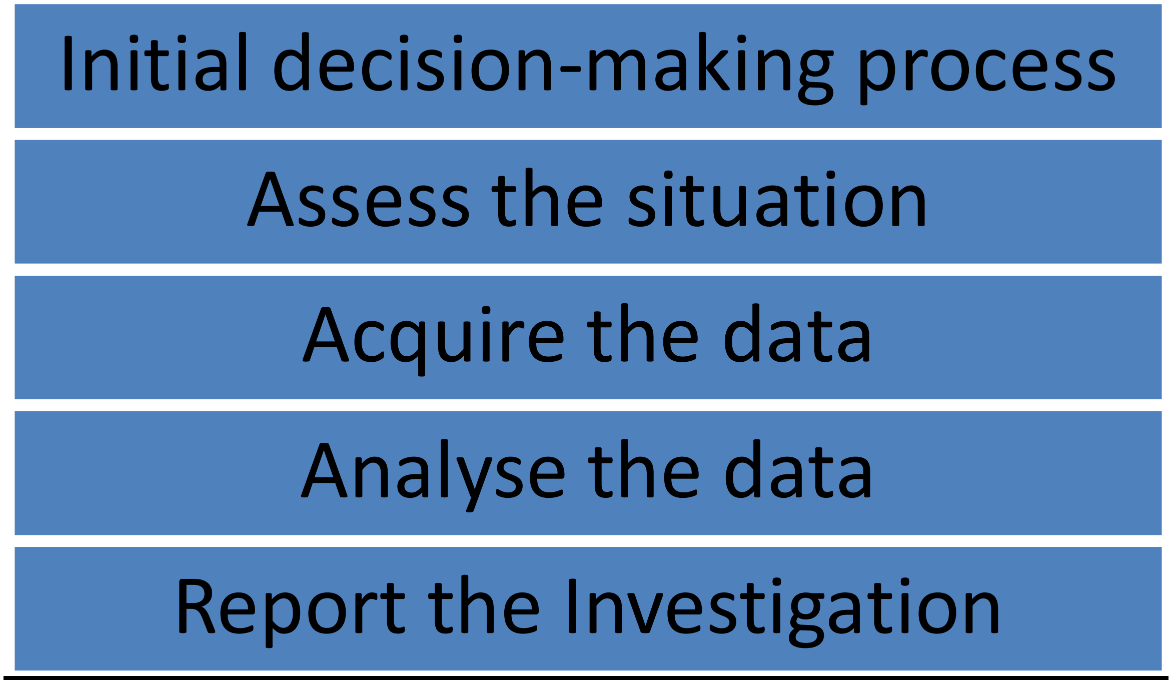
Digital forensics is commonly used in both criminal law and private investigation. Traditionally, it has been associated with criminal law, where the evidence is collected to support or oppose a hypothesis before the court of law. As with other areas of forensics, this is often a part of wider investigation spanning a number of disciplines. In some cases, the collected evidence is used as a form of intelligence gathering, used for other purposes than court proceedings.[7] As a result, intelligence gathering is sometimes held to a less strict forensic standard. In civil litigation or corporate matters, digital forensics forms part of the electronic discovery process. Forensic procedures are similar to those in criminal investigations, often with different legal requirements and limitations. Outside of the courts, digital forensics can form a part of internal corporate

[6] Sekar, Vyas, et al "Toward a framework for internet forensic analysis." ACM HotNets-III 2004

[7] Prasanthi, B V (2017). Cyber Forensic Science to Diagnose Digital Crimes- A study. International Journal of Computer Trends and Technology (IJCTT)

investigations.The main focus of digital forensics investigations is to recover objective evidence of criminal activity (termed actusreus in legal parlance). However, the diverse range of data held in digital devices can help with other areas of inquiry.

1.9 COMPUTER FORENSICS INVESTIGATION PROCESS



Initial decision-making process

Assess the situation

Acquire the data

Analyse the data

Report the Investigation

The investigation process of computer forensics are as follows:-

- **Initial Decision-Making Process**

One must determine whether or not to involve law enforcement with the assistance of legal advisors. If the determination of law enforcement is needed, then the internal investigation must continue unless law enforcement officials advise otherwise. Depending on the type of incident being investigated, the primary concern should be to prevent further damage to the organization by those person(s) who caused the incident. The investigation is important but is secondary to protecting the organization unless there are national security issues.[8]

- **ASSESS THE SITUATION**

The assessment of situation establishes the required resources for an internal investigation. There is a five-step process that must be followed which is as follows:-

a) Notify decision-makers and acquire authorization

To conduct a computer investigation, one must first need to obtain proper authorization unlessexisting policies and procedures provide incident response authorization. One must need to conduct a thorough assessment of the situation and define a course of action. The following are some of the best practices:

- If no written incident response policies and procedures exist, notify decision-makers and obtain written authorization from an authorized decision-maker to conduct the computer investigation.

- Document all actions you undertake that are related to this investigation. Ensure there is a complete and accurate documented summary of the events and decisions that occurred during the incident and the incident response. This documentation may ultimately be used in court to determine the course of action that was followed during the investigation.[9]

- Depending on the scope of the incident and absent any national security issues or life safety issues, the first priority is to protect the organization from further harm.

[8] Digital Forensics in Law Enforcement: A Needs Based Analysis of Indiana Agencies by Teri A. Cummins Flory (Purdue University),2016

[9] What Is Computer Forensics? (GUIDE) | Forensic Control <https://www.forensiccontrol.com/what-is-computer-forensics>

After the organization is secure, restoration of services (if needed) and the investigation of the incident are the next priorities.

Decisions made may be questioned as much as the evidence. Because computer evidence is complex, different investigations (such as those conducted by an opposing party) may make different decisions and reach different conclusions.

b) Review policies and laws

At the start of a computer investigation, it is important to understand the laws that might applyto the investigation as well as any internal organization policies that might exist. The following are the best practices:-

- Determine if you have the legal authority to conduct an investigation. Many organizations state in their policies and procedures that there is no expectation of privacy in the use of the organization's equipment, e-mail, Web services, telephone, or mail and that the company reserves the right as a condition of employment to monitor and search these resources. Such policies and procedures should be reviewed by the organization's legal advisors, and all employees, contractors, and visitors should be notified of their existence. If you are uncertain about your authority, contact your management, your legal advisors, or (if necessary) your local authorities.
- Consult with legal advisors to avoid potential issues from improper handling of the investigation.[10] These issues may include:

    - Compromising customers' personal data.
    - Violating any state or federal law, such as federal privacy rules.
    - Incurring criminal or civil liability for improper interception of electronic communications. Consider warning banners.

[10] Forensic Examination of Digital Evidence: A Guide for Law Enforcement

- Viewing sensitive or privileged information. Sensitive data that may compromise the confidentiality of customer information must only be made available as part of investigation-related documentation if it directly pertains to the investigation.

- Maintain digital copies of evidence, printouts of evidence, and the chain of custody for all evidence, in case of legal action. Preservation of the chain of custody is accomplished by having verifiable documentation that indicates who handled the evidence when they handled it, and the locations, dates, and times of where the evidence was stored. Secure storage of evidence is necessary, or custody cannot be verified.

c) Identify Investigation Team Members

Ideally, team members should be established before the team is needed for an actual investigation. It is important that investigation teams be structured appropriately and have appropriate skills. The following are the best practices for forming an investigation team:-

- Identify a person who understands how to conduct an investigation. Remember that the credibility and skills of the person performing the investigation are often scrutinized if a situation results in legal proceedings in a court of law.
- Identify team members and clarify the responsibilities of each team member.
- Assign one team member as the technical lead for the investigation. The technicallead usually has strong technical skills and is experienced in computer investigations. In investigations that involve suspected parties who are technicallyskilled, you might need to select investigation team members who are more skilled than the suspected parties.
- Keep the investigation team as small as possible to ensure confidentiality and toprotect your organization against unwanted information leaks.
- Engage a trusted external investigation team if your organization does not have personnel with the necessary skills.

- Ensure that every team member has the necessary clearance and authorization toconduct their assigned tasks. This consideration is especially important if any third-party personnel, such as consultants, are involved in the investigation.[11]

d) *Conduct a thorough assessment*

Clearly documented assessment of the situation is required to prioritize your actions and justify the resources for the internal investigation. This assessment should definethe current and potential business impact of the incident, identify affected infrastructure, and obtain as thorough an understanding as possible of the situation. This information will help you define an appropriate course of action. The following are the best practices to conduct a thorough assessment:-

- Use all available information to describe the situation, its potential severity, potentially affected parties, and (if available) the suspected party or parties.
- Identify the impact and sensitivity of the investigation on your organization. For example, assess whether it involves customer data, financial details, health care records, or company confidential information. Remember to evaluate its potentialimpact on public relations. This assessment will likely be beyond the expertise of IT and should be done in conjunction with management and legal advisors.
- Analyse the business impact of the incident throughout the investigation. List thenumber of hours required to recover from the incident, hours of downtime, cost of damaged equipment, loss of revenue, and value of trade secrets. Such an assessment should be realistic and not inflated. The actual costs of the incident willbe determined at a later date.
- Analyse affected intangible resources, such as the future impact on reputation, customer relationships, and employee morale. Do not inflate the severity of the incident. This analysis is for informational purposes only to help understand the scope of the incident. The actual impact will be determined at a later date. This

[11] Barrett, Neil, Computer Forensics Jump Start: Computer Forensics Basics, Solomon, Sybex Printing, 2005

assessment will likely be beyond the expertise of IT and should be done in conjunction with management and legal advisors.

e) Prepare for Evidence Acquisition

A detailed document containing all information must provide a starting point for the next phase and for the final report preparation. In addition, understand that if the incident becomes more than just an internal investigation and requires court proceedings, it is possible that all processes used in gathering evidence might be used by an independent third party to try and achieve the same results. The document that provides detailed information about the situation and must include the following:-

- An initial estimate of the impact of the situation on the organization's business.
- A detailed network topology diagram that highlights affected computer systems and provides details about how those systems might be affected.
- Summaries of interviews with users and system administrators.
- Outcomes of any legal and third-party interactions.
- Reports and logs generated by tools used during the assessment phase.
- A proposed course of action.

- ACQUIRE THE DATA

Somecomputer investigation data is fragile, highly volatile, and can be easily modified or damaged.Therefore, one needs to ensure that the data is collected and preserved correctly prior toanalysis. There is a three-step process that must be followed which is as follows:-

a) Build computer investigation toolkit

A toolkit might contain a laptop computer with appropriate software tools, operating systems and patches, application media, write-protected backup devices, blank media, basic networking equipment, and cables. Ideally, such a toolkit will be created in advance, and team members will be familiar with the tools before they have to conduct an investigation.The following are the guidelines that needs to be followed when building and using a computer investigation toolkit:-

- Decide which tools you plan to use before you start the investigation. The toolkit will typically include dedicated computer forensics software, such as Sysinternals, Encase, The Forensic Toolkit (FTK), or ProDiscover.
- Ensure that you archive and preserve the tools. You might need a backup copy of the computer investigation tools and software that you use in the investigation to prove how you collected and analysed data.
- List each operating system that you will likely examine, and ensure you have the necessary tools for examining each of them.
- Include a tool to collect and analyse metadata.
- Include a tool for creating bit-to-bit and logical copies.
- Include tools to collect and examine volatile data, such as the system state.
- Include a tool to generate checksums and digital signatures on files and other data, such as the File Checksum Integrity Validator (FCIV) tool.
- If you need to collect physical evidence, include a digital camera in the toolkit.

b) Collect the data

Data collection of digital evidence can be performed either locally or over a network. Acquiring the data locally has the advantage of greater control over the computer(s) and datainvolved. However, it is not always feasible. Other factors, such as the secrecy of the investigation, the nature of the evidence that must be gathered, and the timeframe for the investigation will ultimately determine whether the evidence is collected locally or over the network.

c) Store and archive

When evidence is collected and ready for analysis, it is important to store and archive the evidence in a way that ensures its safety and integrity. The best practices for data storage and archival include the following:-

- Physically secure and store the evidence in a tamper-proof location.
- Ensure that no unauthorized person has access to the evidence, over the network orotherwise. Document who has physical and network access to the information.
- Protect storage equipment from magnetic fields. Use static control storage solutions toprotect storage equipment from static electricity.
- Make at least two copies of the evidence you collected, and store one copy in a secureoffsite location.
- Ensure that the evidence is physically secured as well as digitally secured.
- Clearly document the chain of custody of the evidence. Create a check-in / check-outlist that includes information such as the name of the person examining the evidence,the exact date and time they check out the evidence, and the exact date and time they return it.

- ANALYSE THE DATA

There is a three step process to analyse the evidence that is gathered during the acquisition of data phase of an internal investigation.

a) Analyse network data

When network analysis is required, the following procedure is followed:-

- Examine network service logs for any events of interest. Typically, there will be large amounts of data, so you should focus on specific criteria for events of interest such as username, date and time, or the resource being accessed.
- Examine firewall, proxy server, intrusion detection system (IDS), and remote access service logs. Many of these logs contain information from monitored incoming and outgoing connections and include identifying information, such as IP address, time of the event, and authentication information.

- View any packet sniffer or network monitor logs for data that might help you determine the activities that took place over the network. In addition, determine whether connections you examine are encrypted-because you will not be able to read the contents of an encrypted session.

b) Analyse Host Data

Host data includes information about such components as the operating system and applications. The following procedure is used to analyse the copy of the host data obtained in the acquisition of the data phase.

- Identify what you are looking for. There will likely be a large amount of host data, and only a portion of that data might be relevant to the incident. Therefore, you should try to create search criteria for events of interest.
- Examine the operating system data, including clock drift information, and any data loaded into the host computer's memory to see if you can determine whether any malicious applications or processes are running or scheduled to run.
- Examine the running applications, processes, and network connections.

c) Analyse storage media

The following procedure is to be followed to extract and analyse data from the storage media collected:-

- Whenever possible, perform offline analysis on a bit-wise copy of the original evidence.
- Determine whether data encryption was used, such as the Encrypting File System (EFS) in Microsoft Windows. Several registry keys can be examined to determine whether EFS was ever used on the computer. If you suspect data encryption was used, then you need to determine whether or not you can actually recover and read the encrypted data.

- If necessary, uncompress any compressed files and archives. Although most forensic software can read compressed files from a disk image, you might need to uncompress archive files to examine all files on the media you are analysing.
- Create a diagram of the directory structure. It might be useful to graphically represent the structure of the directories and files on the storage media to effectively analyse the files.
- Identify files of interest.
- Examine the registry, the database that contains Windows configuration information, for information about the computer boot process, installed applications (including those loaded during startup), and login information such as username and logon domain.
- Study the metadata of files of interest, using tools such as Encase by Guidance Software, The Forensic Toolkit (FTK) by AccessData, or ProDiscover by Technology Pathways. File attributes such as timestamps can show the creation, last access, and last written times, which can often be helpful when investigating an incident.
- Use file viewers to view the content of the identified files, which allow you to scan and preview certain files without the original application that created them. This theapproach protects files from accidental damage and is often more cost-effective than using the native application. Note that file viewers are specific to each type of file; if a viewer is not available, use the native application to examine the file.[12]

- **REPORT THE INVESTIGATION**

There is a two-step process to organize the information that you gather and the documentation that you create throughout a computer investigation.

a) *Gather and Organize information*

The following procedure is to be followed to gather and organize the required documentation for the final report.

[12] Legal Aspects of Digital Forensics by Daniel J. Ryan and Gal Shpantzer

- Gather all documentation and notes from the Assess, Acquire, and Analyse phases. Include any appropriate background information.
- Identify parts of the documentation that are relevant to the investigation.
- Identify facts to support the conclusions you will make in the report.
- Create a list of all evidence to be submitted with the report.
- List any conclusions you wish to make in your report.
- Organize and classify the information you gather to ensure that a clear and concise report is the result.

b) Write a report

The following list identifies recommended report sections and information that should be included:-

- Purpose of report
- Author of report
- Incident summary
- Evidence
- Details i.e., description of what evidence was analysed and the analysis methods that were used.
- Conclusion
- Supporting documents

1.10 LET'S SUM UP

In this chapter, we have studied the evolution of computer forensics along with the basic concepts and objectives of computer forensics. We also studied the uses and ethics that need to be followed by the digital forensics expert. Finally, we ended our discussion with the Computer Forensics Investigation process.

1.11 FURTHER READING

- P. Y. S. B. D. C. A. U. Bansal, "Cyber Forensics-The art of Decoding the Binary Digits," International Journal of Emerging Technology and advanced engineering, vol. 2.
- Rogers MK, Seigfried K. The future of computer forensics: a needs analysis survey. Computers Security 2004 Feb;23(1): 12-16.
- MansonD,CarlinA,RamosS,GygerA,KaufmanM,TreicheltJ. Is the open way a better way? Digital Forensics using Open Source Tools. Proceedings of the 40th Hawaii International Conference on System Sciences, 2007.
- Karyda M, Mitrou L. Internet forensics: legal and technical issues. Second International Workshop on Digital Forensics and Incident Analysis (WDFIA), 2007.
- Garfinkel SL. Automating Disk Forensic Processing with SleuthKit, XML and Python, 2009. Fourth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering. Conference at Berkeley, California, USA.

1.12 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What are the objectives of computer forensics?**

The objectives of Computer forensics are to provide guidelines for:

- Following the first responder procedure and access the victim’s computer after incident.
- Designing procedures at a suspected crime scene to ensure that the digital evidence obtained is not corrupted.
- Data acquisition and duplication.
- Recovering deleted files and deleted partitions from digital media to extract the evidence and validate them.
- Provide guidelines for analysing digital media to preserve evidence, analysing logs and deriving conclusions, investigate network traffics and logs to correlate events, investigate wireless and web attacks, tracking emails and investigate email crimes.
- Producing computer forensic report which provides a complete report on computer forensic investigation process.
- Preserving the evidence by following the chain of custody.
- Employing the rigorous procedures necessary to have forensic results stand up to scrutiny in a court of law.
- Presenting digital forensics results in a court of law as an expert witness.

2. **What are the uses of computer forensics?**

The uses of computer forensics include the following:

- Detecting a cybercrime.
- Solving an alleged criminal activity provided the medium used in perpetrating the crime is a digital device.
- Forestalling a crime from taking place.
- Computer forensics investigations are often used to refute or support a supposition during civil, criminal and corporate litigations.
- Computer forensics is used in the private sector by companies who are undergoing internal investigations into unauthorized technical and network transgressions.

3. **What are the implications of digital forensics?**

   Digital forensics is commonly used in both criminal law and private investigation. Traditionally, it has been associated with criminal law, where the evidence is collected to support or oppose a hypothesis before the court of law. As with other areas of forensics, this is often a part of wider investigation spanning a number of disciplines. In some cases, the collected evidence is used as a form of intelligence gathering, used for other purposes than court proceedings. As a result, intelligence gathering is sometimes held to a less strict forensic standard. In civil litigation or corporate matters, digital forensics forms part of the electronic discovery process. Forensic procedures are similar to those in criminal investigations, often with different legal requirements and limitations. Outside of the courts, digital forensics can form a part of internal corporate investigations. The main focus of digital forensics investigations is to recover objective evidence of criminal activity (termed actusreus in legal parlance). However, the diverse range of data held in digital devices can help with other areas of inquiry.

1.13 ACTIVITY

Explain the different phases of investigation process with the help of diagram? Explain it with an example. (1000-1500 words)

Unit 2: Overview of Digital Records and Cyber Forensics

2

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Define digital records, its types and characteristics
- Forensic Science and Definition of Cyber Forensics
- Key Elements and Classification of Cyber Forensics

- Know how Cyber Forensics is used by investigating officer

1.2 INTRODUCTION TO DIGITAL RECORDS

In the current era of digitalisation, use of technology to transfer the paper-based information into digital information is very much common with every organisation. Technological advancement has made this change easier through different means. Digitalised information does not only give us the ease of access but also better storage in comparison with paper-based data. But digitalisation is not only limited to convert information from traditional way to technological way. Whatever new data is getting generated, gather and created is directly getting digitalised and it leads to new concepts like big data because the number of digital records is increasing tremendously day by day.[13]

The information residing in computing devices is in the form of 0's and 1's, this is also known as the mother tongue of computers (binary). All the information is nothing but the combination of digits (0's and 1's) hence we call them digital. Whatever the information is being stored in the digital format is been accessed with the help of software in human understandable form. Together this digital information is called as digital records. This digital information is mainly stored in different storage devices in different formats.

1.3 DEFINITION AND SCOPE

Digital record is the information which is mainly stored in computing devices in the form of 0's and 1's.

Digital record is a form of electronic record which is electronically generated or stored in different storage devices.

[13] The Role and Impact of Forensic Evidence in the Criminal Justice Process by Joseph Peterson, Ira Sommers, Deborah Baskin, and Donald Johnson,2010

Digital record is also defined as a record created or maintained by means of digital computer technology which includes records that are born digital or have undergone conversion from a non-digital format.[14]

It is a record which is maintained in a coded numeric format that can be accessed using a combination of hardware and software which translates them into text or images which can be comprehended by the human eye.

1.4 CHARACTERISTICS AND TYPES

The information in the form of digital records correctly reflects certain characteristics

- ***Confidentiality***

  Confidentiality refers to only the authorized person could have access to the information. It is also equivalent to the privacy of data. In simple language, confidentiality is the measures undertaken to prevent sensitive information from reaching to wrong people while making sure the right people can access it.

  Example: Data encryption, User ID-Passwords etc.[15]
- ***Availability***

  Availability simply means the information should be available in required format whenever needed. That means protecting the information from intentional as well as non-intentional loses. It is making sure that information is available for use all the time.

  Example: Performing hardware repairs, troubleshooting operating system issues, enough bandwidth availability preventing bottlenecks etc.
- ***Integrity***

  Integrity means maintaining the state of the information constant throughout its lifecycle. It also means consistency accuracy and trustworthiness of the data. The information should not change in transit also, it should be protected from alteration by unauthorized people.
- ***Authenticity***

[14] Digital Forensics in Law Enforcement: A Needs Based Analysis of Indiana Agencies by Teri A. Cummins Flory (Purdue University),2016

[15] Forensic Examination of Digital Evidence: A Guide for Law Enforcement

The authenticity of the information mainly involves proof of identity. Which means it is the assurance that the information is from the source it claims to be from. Authentication is used to verify authenticity.

- ***Reliability***

  A reliable record is the one whose content is full, accurate and trustworthy. Reliable records are mainly used for interpretation and conclusion.

- ***Usability***

  It is the characteristic is recorded which mainly addresses further use of the digitally stored information. It is the record which should be located, retrieved and interpreted.

TYPES OF DIGITAL RECORDS

Based on the type of information, Digital records are classified as follows:

- ***Image File***

  This record mainly contains still images in the form of photographs. These images are stored in a variety of data formats such as JPEG (Joint Photographic Experts Group), TIFF (Tagged Image File Format), GIF (Graphic Interchange Format) etc.[16]

- ***Text File***

  This digital record mainly consists of different type of text which includes Tables, Databases, and Logs etc. These digital records also contain File format like .DOC, .PPT, .XLS, .PDF (Portable Document Format).

- ***Audio File***

  In this type of digital records,the sound is recorded which can be originally produced from analogue or digital formats. The audio files have several characteristics like Sampling Frequency, Bit-depth, Mono or Stereo. The examples of audio files are.WAV, MP3 etc.

- ***Video File***

  Video file is nothing but moving images recording which can be synced with audio. Pixel array, Frame rate per second, Aspect Ratio, Bit Rate, High Definition are important

[16] Arkfeld, M R (2002-2006), Electronic Discovery and Evidence. Law Partner Publishing, LLC. Phoenix, Arizona

characteristics of video files. The examples of video files are.AVI (Audio Video interleave), .MXF (Material Exchange Format), .WMV (Windows Media File) etc.

- ***Mark-up Language***

  This file format mainly contains embedded instruction for displaying the content over the website. This file is responsible for the text and graphical representation of the information over the World Wide Web. Examples of these files are.HTML (HyperText Mark-up Language), .XML (Extensible Mark-up Language) etc.

1.5 ADVANTAGES AND DISADVANTAGES

ADVANTAGES OF DIGITAL RECORDS

- **Easy to gather, store and access**

  Due to the different types of input available, it becomes very easy to collect and store information digitally. Example: Barcode reader, Document scanner, Touch screen etc.[17]

- **Speed**

  Because of high computing power an advanced networking devices, it's becoming faster to transmit, search and processing of the digital information.

- **Cost**

  Cost for overall digital records is comparatively cheaper in many aspects like storage, transmission etc.

- **Multimedia**

  This gives added advantage to represent the information in more presentable and active ways.

DISADVANTAGES OF DIGITAL RECORDS

- **Equipment Cost**

  When an organisation goes paperless there isa huge volume of data which is held on paper have to be converted to digital format. The cost of hardware and software needed

[17] Boucher, K, and Endicott-Popovsky, B (2008), "Digital Forensics and Records Management: What We can Learn from the Discipline of Archiving"

for this holds a substantial amount of money. This infrastructure also becomes obsolete in a relatively short time.

- **Privacy and security issue**

  As digital information increases, the functionality aspect like access and availability, privacy and security decreases reciprocally.

1.6 RELAVENCE TO E-COMMERCE AND E-GOVERNANCE

The digital India programme is a flagship program of the Government of India with a vision to transform India into digitally empowered society and knowledge economy. Information technology Act 2000 mainly addresses the legal recognition of digital records in e-commerce and e-governance.[18]

E-commerce is also known as electronic commerce is the activity of commercial transactions carried through computing and networking devices. E-commerce activity is rapidly growing in India which adds around 6 million new entrants every month. Amazon, Flipkart, Paytm, Snapdeal are few examples of E-commerce companies in India.

E-governance is defined as the use of computing technology and networking across government departments. It mainly involves the conversion of the paper base transaction into digital records. This has bought many projects under digitalisation namely Income Tax, Passport, Land records, Insurance, Visa immigration etc.

1.7 INTRODUCTION TO CYBER FORENSICS

Cyber Forensics is a rapidly growing field of forensics which mainly addresses all sort of digital evidence. Due to the increasing use of technology in everyday life, there are lots of digital records gets generated every now and then in different computing devices. These digital footprints come very handily during the investigation of all sort of criminal activities. Cyber

[18] Richard III GG, Roussev V Next-generation digital forensics Communications of the ACM. 2006 Feb 1;49(2):76-80

forensics gives us an in-depth view and understanding of these digital records in various situations. Hence, cyber forensics is not only used by the government but also private organisations.

1.8 DEFINITION

Cyber Forensics mainly consists of the integration of two terminologies as Cyber and Forensics. Cyber is defined as a space created by interconnected computer devices across the globe. The word cyber refers to digitalisation, the culture of computers and information technology.

Forensic means suitable for use in a court of law. Hence, Cyber forensics is defined as a branch of forensic science which addressed the recovery and investigation of the evidence found in digital devices. It is also sometimes referred to as digital forensics because of the direct relation with digital records.

Cyber forensics is a branch of forensic science which aims at a constructive way of identifying, reserving analysing, recovering and presenting the digital evidence in a court of law.

Cyber forensics is the application of investigation to search, gather and preserve the evidences from computing device in a way that is suitable for presentation in a court of law. CERT (Computer Emergency Response Team) defines cyber forensics as the process of using scientific knowledge for collecting analysing and presenting evidence to the court.

1.9 FORENSIC SCIENCE

Forensic science deals with recovery and analysis of latent evidence. Latent evidence may have different forms right from fingerprints on the glass to DNA evidence recovered from blood stains to the deleted SMS of mobile phones. The main objective of forensic science is to find out what has happened, who is affected, what has been used, how it has been used and who has committed the act. The first objective is to gather all the facts around this. Next objective is to present the data in a manner which is acceptable for the court. Forensic science is the application of science governed by legal standards of admissible evidence and criminal procedures. Forensic scientists are the group of people responsible to carry out the tasks of forensics namely collecting, preserving and analysing scientific evidence during the course of the investigation. Many times forensic scientist visits the scene of the crime to collect the evidence in a proper forensic manner. Forensic scientist also gets testified as an expert witness in both criminal and civil cases.[19]

In the recent decade, documenting forensic science has become more efficient. Forensic scientists have started using advanced technologies in forensic processes. It has resulted in the accuracy of findings and also helped into logical reasoning of the incident. Unlike other areas of technology, forensic science has made significant growth and contributed to the court proceedings by eliminating all the doubts of prosecution towards the evidence.

1.10 ELEMENT OF CRIME

The legal definition of all crimes contains certain elements. If the government is not able to prove the existence of these elements then the conviction cannot be obtained in a court of law. That means crime can be broken down into elements which should be proved beyond a reasonable doubt by the prosecution. There are three main elements of every crime:

1. ***Criminal Act***

   It is the activity prohibited by law. It is also referred to as conduct which means an action carried out by accuse.

2. ***Criminal Intent***

   It is also called a purpose or state of mind resulted in a criminal act. It is further classified into four categories

- Purposely
- Knowingly
- Recklessly
- Negligently

3. ***Concurrence***

   Concurrence means the occurrence of both the above two elements at the same time.

Apart from these three, there are other elements of crime such as

[19] Carrier B Defining digital forensic examination and analysis tools using abstraction layers. International Journal of digital evidence. 2003 Jan;1(4):1-2

- ***Law***

  There must be some law which addresses the act. That may sound obvious but there are certain acts which are objectionable but not criminal. Example Parking a vehicle in front of someone's gate.

- ***Burden of Proof***

  Depending on the case, the allegations or defence made in the court has to be proved beyond a reasonable doubt. The burden of the proof mainly lies with the one who makes certain statements in the court.

- ***Exculpatory Evidence***

  This is an important concept regarding the evidence that proves the accused innocence. In a criminal case, prosecutors have a legal duty to turnover exculpatory evidence to the defence.

1.11 KNOWLEDGE REQUIRED FOR CYBER FORENSICS

Cyber Forensics requires an understanding of various computing and networking concepts.[20] As cyber forensics consists of different technologies related to digital devices, the investigator should have solid background knowledge of the following topics:-

Hardware

On cannot perform forensic analysis without the knowledge of computer paths. That means the investigator should have a working knowledge of motherboard, Processor, Hard Drives, RAM and Expansion slots.

Hard Drives

Hard drives record and store the data in magnetic form on platters. The platters are organised on the spindle with Reading/Write head.

The data is organised as follows

- A sector is a basic unit of data storage on the hard disk which consists of 512 bytes.
- A cluster is a logical group of sectors.

[20] Breeuwsma, Marcel, et al "Forensic data recovery from flash memory." Small Scale Digital Device Forensics Journal 1.1 (2007): 1-17

- Sectors are in turn organised by tracks.

There are four types of hard drives:

1. SCSI- Small Computer System Interface
2. IDE- Integrated Drive Electronics
3. SATA- Serial Advanced Technology Attachment
4. SSD- Solid State Drive

RAM (Random Access Memory)

RAM plays a vital role ina forensic investigation point of view. Sometimes it's important to carry out forensics of running machine. For that, live memory capture is required. That means to take what is currently in RAM. Hence, live memory capture become quite important.

Following are the different types of RAM:

- DRAM (Dynamic RAM)
- SGRAM (Synchronous Graphic RAM)
- PSRAM (Pseudo-Static RAM)
- RLDRAM (Reduced Latency RAM)

Operating System

Operating systems are responsible for different operations on the machine. Cyber forensic approach changes with different operating systems. Hence, detailed knowledge of operating system enhances forensic investigation.[21]

Following are some of the examples of Operating System:

- Windows
- LINUX
- Macintosh
- IOS
- Android

Files and File Systems

The file system is the way through which computer organises data on a disk. Knowledge of file system gives added advantage to the investigator.

Following are some examples of file systems:

[21] SWGDE Best Practices for Computer Forensics, Scientific Working Group for Digital Evidence, Version 2.1

- FAT (File Allocation Table)
- NTFS (New Technology File System)
- EXT (Extended File System)

Networks

Many cybercrimes take place across the network. Strong understanding of the basics of networking helpsthe forensic investigator to unearth the important findings to different networking devices and related technologies. Hence, it is advised to have the following device and technologies:

Network topologies, Types of the network (LAN, WAN etc),Types of cables, WiFi, Hub, Switch, Router,Networking protocols etc.

1.12 CLASSIFICATION OF CYBER FORENSICS

Cyber forensics is an emerging practice to discover digital evidence through different computing devices and prosecute the criminals in a court of law. These digital footprints spread across multiple gadgets used by criminals. Cyber forensics is classified into many sub-branches depending upon the technology used for the storage of information in different computing devices around us.

Disk Forensics

It is also called as storage device forensics. It mainly deals with extracting information by searching the required data through active and deleted files. This field of forensics also targets unallocated and slack spaces of storage media.

Mobile Device Forensics

This branch mainly addresses forensics of all cellular devices like mobile, tablet, pagers etc. Mobile forensic retrieves the information like address book, call logs, SMS, photos, videos, audios etc.

Network Forensics

It mainly focuses on monitoring and analysing network traffic for the purpose of intrusion detection, information gathering, legal evidence etc. It is one of the proactive forensic investigation techniques. It also includes a log analysis of different networking devices.

Database Forensics

In many software, information is stored in the form of a database. Hence, database forensics comes very handy in order to retrieve information related to databases. It mainly consists of metadata analysis, timestamp analysis and deleted record recovery of the databases.

Malware Forensics

It mainly deals with investigating and analysing malicious code in the system which may be in the form of Virus, Worm, Trojan, and Rootkit etc.

Email Forensics

This branch of forensics is responsible for recovery and analysis of emails which includes email source investigations, email attachments, contacts and calendar invites of email etc.

Memory Forensics

It aims at collecting and analysing information from system memory in the raw form. The system memory mainly consists of system register, cache and RAM.

Wireless Forensics

It is a subcategory of Network Forensics which targets the methodology and tools required to collect and analyse wireless network traffic data.

1.13 KEY ELEMENTS OF CYBER FORENSICS

Following are the key elements which encompass cyber forensics:

The Identification and Acquisition of Digital Evidence

It is important to have knowledge of possible evidences lying around the crime scene. The cyber forensic investigator should be able to identify the type of information stored in a device and also the format of that data. With the help of this information, the appropriate technology can be decided to extract the evidence. The acquisition process can vary device to device. During the acquisition process, the investigator can acquire the evidence either by creating an image or by cloning the disk.

Preservation of Digital Evidence

This is a critical element of forensic investigation in which the evidence is stored by protecting it against any type of alteration or tampering.

The Analysis of Digital Evidence

This element consists of loading, processing, extracting of the identified evidence. This is the main element of cyber forensics. The extraction produces a binary data which should be analysed and processed to convert it into human-readable form.

The Reporting of Digital Evidence

This element consists of a collection of all the findings stated in such a way that it can be understood by any person. The report should be in very simple terms giving the description of the item mainly findings and conclusion.

Presentation of the Digital Evidence

This element is directly related to the representation to the court of law. The proper representation increases the chances of admissibility of the evidence.

1.14 HOW CYBER FORENSICS HELP INVESTIGATING OFFICER

Discover all files

A casual viewer may not able to view all the files present over the system. Through forensic view, investigator can discover all the files which are present on the system which includes hidden files, password-protected files, encrypted files, hidden files etc.

Data Recovery

Cyber forensics helps into the recovery of the deleted files from the disc. Cyber forensics can also carve overwritten files to extract data to some extent. Data recovery also unearths the files from unallocated or slacks space of the discs.

Keyword Search

Cyber forensics helps to index of the hug information which ultimately helps investigator to find out the relevant evidences effectively and faster.

Timeline Analysis

Cyber forensics can give the proper timeline of the identified evidence with the help of different metadata and event logs of the system. With the help of timeline analysis, the investigator can have detailed knowledge of when particular evidence been created, accessed and used for the crime.

Volatile Evidence Analysis

Forensics of volatile data helps the investigator to know what is currently happening on the system. It can be done by the analysis of RAM and cache memory. This also gives added advantage to monitor live attacks.

Root Cause Analysis (RAC)

Cyber Forensics can help the investigator to identify the root cause of the said crime by complete analysis of the computing devices involved in a particular act.

Despite all above cyber forensics can also be used for some other reasons like

Operational Troubleshooting

Better incidence response and recovery

Log Monitoring

Data Preservation

Business Continuity

Better Vulnerability Detection

1.15 LET'S SUM UP

In this chapter, we have studied the concept of digital records and cyber forensics along with its characteristics, advantages and disadvantages and types. We also studied how it is relevant to e-commerce and e-governance. Finally, we ended our discussion with how cyber forensics can help the investigating officers.

1.16 FURTHER READING

- Nina Godbole and SunitBelapore; "Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives", Wiley Publications, 2011.
- Bill Nelson, Amelia Phillips and Christopher Steuart; "Guide to Computer Forensics and Investigations" – 3rd Edition, Cengage, 2010 BBS.

1.17 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What are digital records?**

Digital record is a form of electronic record which is electronically generated or stored in different storage devices.

2. **What are the different types of digital records?**

Digital records are classified as follows:

- Image File
- Text File
- Audio File
- Video File
- Mark-up Language

3. **What is cyber forensics?**

Cyber forensics is a branch of forensic science which aims at a constructive way of identifying, reserving analysing, recovering and presenting the digital evidence in a court of law.

4. **What are the different types of cyber forensics?**

Cyber forensics is classified into many sub-branches depending upon the technology used for storage of information in different computing devices around us.

- Disk Forensics
- Mobile Device Forensics
- Network Forensics
- Database Forensics
- Malware Forensics
- Email Forensics
- Memory Forensics
- Wireless Forensics

1.18 ACTIVITY

Briefly explain the meaning of cyber forensics along with its elements that are used in crime scene and its classification? Also, elucidate in what way cyber forensics can help the investigating offices with a case study. (1500 words)

Unit 3: Investigation Process 3

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- The process of investigation
- Different guidelines for digital evidence
- Understand step wise instruction of investigation in different scenarios

1.2 INTRODUCTION

Nowadays investigation is been carried out at a very fast pace. Thanks to technology that help investigating officer to gather the relevant information at very high speed and act upon it. Investigation process used needs to update and enhance with net types of technological advancement. In this chapter, we will understand the different investigation processes, guidelines and standard operating procedure which investigation officer needs to be followed while dealing with cyber-crimes and other crimes where digital evidence are involved.[22]

1.3 ACPO GUIDELINES

The Association of Chief Police Officers (ACPO) was a not-for-profit private limited company that for many years led the development of policing practices in England, Wales, and Northern Ireland. It has contributed a lot in terms of guidelines for handling digital evidence.

The Association of Chief Police Officers (ACPO) Good Practice Guide for Computer-based Electronic Evidence [ACPO] –for reference

- No actions performed by investigators should change data contained on digital devices or storage media that may subsequently be relied upon in court.
- Individuals accessing original data must be competent to do so and have the ability to explain their actions.
- A trail or other record of applied processes, suitable for replication of the results by an independent third-party, must be created and preserved, accurately documenting each investigative step.
- The person in charge of the investigation has overall responsibility for ensuring the above-mentioned procedures are followed and in compliance with governing laws.

Apart from ACPO guidelines there are several guidelines out there and mainly used by Indian law enforcement agencies as given below.[23]

1.4 DIGITAL EVIDENCE GUIDELINES

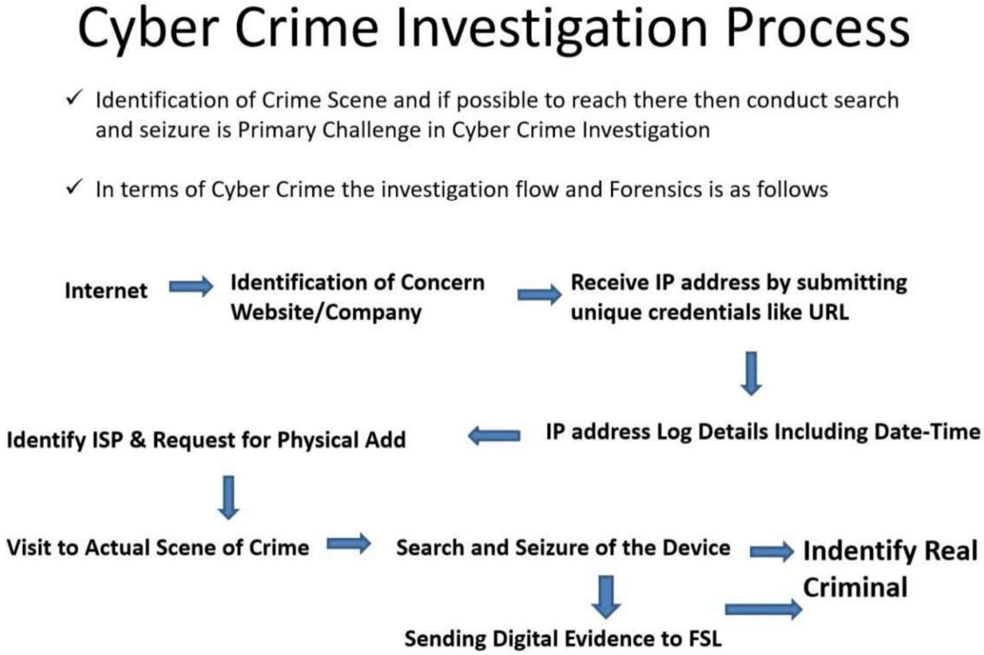
- Identify the computer system, Secure the scene, preserve the traced evidence
- If the computer is switched off, then Photograph, label and document the system details on collection form and collect related software peripherals, removable media, passwords if any

[22] See the Digital Records Forensics Project website at
<http://digitalrecordsforensics.org>

[23] Adams, Richard & Hobbs, Val & Mann, Graham.(2014). Journal of Digital Forensics, Security & Law.Journal of Digital Forensics, Security & Law. 8. 25-48

- If the computer is on and prompts for any password simply disconnect the power and then Photograph, label and document the system details on collection form and collect related software peripherals, removable media, passwords if any
- If it does not prompts for any password, then document screen, system time, network activity. Preserve the RAM content if needed using Authorized tools and procedures.
- Depending upon the case Scenario, the entire computer can be seized or any particular suspected hardware can be seized[24]

Following is the simple diagram which represents how exactly the cybercrime investigation is been carried out.[25]



Cyber Crime Investigation Process

✓ Identification of Crime Scene and if possible to reach there then conduct search and seizure is Primary Challenge in Cyber Crime Investigation

✓ In terms of Cyber Crime the investigation flow and Forensics is as follows

Internet
Identification of Concern Website/Company
Receive IP address by submitting unique credentials like URL
IP address Log Details Including Date-Time
Identify ISP & Request for Physical Add
Visit to Actual Scene of Crime
Search and Seizure of the Device
Indentify Real Criminal
Sending Digital Evidence to FSL

Figure 1.1 Cyber Crime Investigation Process

In the above diagram, the cyber space-related investigation is described. It mainly explains the flow of investigation where the place of incident is the internet.

Now let's understand the step by step approach of the investigating officer in crime investigation.

[24] Adams, R (2013) Doctoral Thesis. The Advanced Data Acquisition Model (ADAM): A process model fordigital forensic practice Murdoch University Retrieved from <http://researchrepository.murdoch.edu.au/14422/2/02Whole.pdf>

[25] Agarwal, A, Gupta, M, Gupta, S, & Gupta, S C (2011).Systematic digital forensic investigation model. International Journal of Computer Science and Security, 5(1), 118-130

1.5 STEPS IN CRIME SCENE INVESTIGATION

1. Identifying and securing the crime scene[26]
2. ‘As is where is’ documentation of the scene of the offence
3. Collection of evidence
4. Procedure for gathering evidences from switched-off Systems
5. Procedure for gathering evidence from live systems
6. Forensic duplication
7. Conducting interviews
8. Labelling and, documenting the evidence
9. Packaging, and transportation of the evidences

THE PROCESS OF EVALUATION OF THE SCENE OF OFFENCE

- Secure the Scene of Crime
- Identify all the potential evidences
- Conventional evidences like sticky slips, manuals, bank account numbers etc., to be part of the search process.
- If the system is OFF, leave it OFF
- Special care to be taken for perishable evidence eg., volatile data
- After identifying the scene of the offence, IO should secure it and, take note of every individual physically present at the scene of offence and, their role at the time of securing the scene of offence.
- From the information gathered and based on visual inspection of the scene of offence, IO should identify all the potential evidence. These physical evidences may include conventional physical evidences like the manuals, user guides and, other items left behind like passwords on slips, bank account numbers etc. it is also important to note the position of the various equipment and items at the scene of offence. For example,

[26] Ciardhuain, S O (2004)An extended model of cybercrime investigations. International Journal of Digital Evidence, 3(1)

a mouse on the left-hand side of the desktop possibly indicates the person operating the computer is a left-handed user.[27]

- While identifying the digital evidence, IO should make sure that the potentially perishable evidence is identified and, all the precautions are put in place for its preservation.

FOLLOWING IS THE PROCEDURE FOR CONDUCTING SEARCH

1. Secure the spot
2. Preserve the fingerprints
3. Restrict the access to a computer (s)
4. Don't accept the help of the suspect for operating computer.
5. Make the Computers Standalone (Remove LAN / Telephone / Wi-Fi / Blue tooth etc)
6. If the computer is/are "OFF"; don't turn "ON"
7. Some screen savers will show that computer is off hence to make sure by checking the light of CPU.
8. If the computer is "ON" then note down the date and time of computer system, don't try to correct it.
9. Documentation
10. Take the photograph of the Monitor screen
11. Don't shutdown the computer in a normal manner but for shutting down pull the power cord from CPU and not from wall point.
12. Place the unformatted blank floppies in each drive for preventing accidental booting of the computer.
13. Photograph the scene, then disconnect all power source; unplug from wall and also from the back of the system.
14. Draw the sketch of the scene of the spot.
15. Label all the equipment, connectors and cables ends to allow reassemble as needed.
16. Seal all the ports and also screws of the CPU with paper seal.

[27] Freiling, F C, &Schwittay, B (2007) A common process model for incident response and computer forensics. Paper presented at the Conference on IT Incident Management and IT Forensics, Germany

17. Pack and seal the equipment carefully and a sample of the same seal must be sent to the FSL where the analysis of the CPU will be carried out.
18. Examine the persons, including suspect for the passwords, username etc.
19. Search the premises for the printouts, handwritten notes, diary, notebooks etc., for the passwords, username etc.
20. Search the premises for the software/programs, printouts, handwritten notes, financial transactions, books etc., which may be of vital importance to the investigation.
21. In personal search look for the pen/flash drives which might be attached to a key chain and may contain vital data.

PRELIMINARY INTERVIEWS AT THE SCENE OF OFFENCE

Following are some of the key questions which should be discussed during this phase of the investigation.[28]

- What steps were taken to contain the issue?
- Were there any logs (system access, etc.) present that cover the issue?
- Are there any suspicious entries present in them?
- Did anyone use the system after the issue occurred?
- Did you observe any similar instance before?
- Were there any alarms that were set off by the firewall/IDS/network security devices?
- Please give detailed documentation on the set of commands or processes run on the affected system or on the network after the issue occurred.
- Do they have similar systems in any of the branch/other offices?
- Whether log register of the Internet users/other users is maintained?
- Are there any questions about the issue that have not been answered?

AT THE SCENE OF OFFENCE, IO SHOULD GATHER THE FOLLOWING INFORMATION DURING THE INTERVIEWS PHASE

[28] Palmer, G (2001) A Road Map for Digital Forensic Research. Digital Forensics Research Workshop, Utica, New York

- Identify the complainant/owner (s) of the various devices and obtain the access details, usernames, and service providers' details.
- Gather information as provided in the questionnaire(s) above, on all the security systems
- Identify the list of the people who can identify the network and a schematic diagram of the network

Let's take some examples in order to understand the investigation process of the different scene of the crime.[29]

SCENE OF OFFENCE: CYBER CAFÉ

1. Identify the number of computer systems present in the cyber café.
2. Identify the number of computer systems connected to the Internet.
3. Obtain details about the network topology and architecture (client — Server).
4. Obtain the CCTV/Web camera clippings, if any.
5. Whether any user management software is used by the cyber café owner?
6. Obtain the log register of Internet users for the relevant period.
7. Check the formatting of storage devices policy adopted by the cyber café owner.
8. Check the hardware replacements done by the cyber café owner.
9. Check the policy regarding removal media usage on the cyber café systems.

SCENE OF OFFENCE: HOME

1. Identify the type of connection (Wi-Fi/Ethernet).
2. How many computer systems are used for the Internet connection?
3. Location of the system and details of persons with access to system(s).
4. Obtain the details about the removable storage media (including external hard disk) used/owned by the user.
5. Obtain details about the network topology and architecture (client — Server), if any.
6. Obtain the details about other computer peripherals (printer/scanner/modem, etc.).

ISSUANCE OF THE PRESERVATION NOTICE

[29] Selamat, S R, Yusof, R, & Sahib, S (2008) Mapping process of digital forensic investigation framework. International Journal of Computer Science and Network Security, 8(10)

Preservation notice is the formal and legal document made in order to request to preserve the information which is important for further investigation. This is the vital document in the investigation process of the digital evidence.

Based on the information gathered, the IO should come out with issues to be complied immediately by issuing specific do’s and don’ts to the complainant/company/agency.

e.g. stopping the access, taking backups, or preserving log information, etc. till further orders. For example, continuing access to the e-mail by the accused can enable him to delete the mails which are incriminating in nature.

A preservation notice needs to be sent to all affected parties to make sure that they do not delete any data that could be relevant to the case. It is ideal to issue this notice, which is necessary for preserving evidence.

GATHERING EVIDENCE

In this phase it is important to know the standard operating procedures for gathering information from different pieces of evidence. SOP gives step by step approach to gather evidence in a legal manner and preserve its admissibility by protecting the integrity of the evidence

PROCEDURE FOR GATHERING EVIDENCES FROM SWITCHED-OFF SYSTEMS

- Secure and take control of the scene of crime both physically and electronically.
- Make sure that the computer is switched OFF- some screen savers may give the appearance that the computer is switched OFF, but hard drive and monitor activity lights may indicate that the machine is switched ON.
- Be aware that some laptop computers may power ON by opening the lid.
- Remove the battery from laptop computers.
- Unplug the power and other devices from sockets.
- Never switch ON the computer, in any circumstances.
- Label and photograph (or video) all the components in-situ and if no camera is available, draw a sketch plan of the system.
- Label the ports and (in and out) cables so that the computer may be reconstructed at a later date, if necessary

- Carefully open the side casing of the CPU or laptop and identify the Hard disk. Detach the hard disk from the motherboard by disconnecting the data transfer cable and power cable.
- Take out the storage device (Hard disk) carefully and record unique identifiers like make, model, and serial number.
- Get the signature of the accused and witness on Hard disk, by using a permanent marker. Ensure that all items have signed and completed exhibit labels.
- Search scene of the crime for Non-electronic evidences like diaries, notebooks or pieces of paper with passwords.

PROCEDURE FOR GATHERING EVIDENCES FROM LIVE SYSTEMS (SWITCHED-ON SYSTEMS)

- Record what is on the screen by a photograph and by making a written note of the content of the screen.
- Do not touch the keyboard or click the mouse and if the screen is blank or a screen saver is present, the case officer should be asked to decide if they wish to restore the screen. If so, a short movement of the mouse will restore the screen or reveal that the screen saver is password protected. If the screen restores, photograph/video and note its content. If password protected is shown, continue as below without any further disturbing the mouse. Record the time and the activity of the use of the mouse in these circumstances.
- Take the help of technical expert to use live forensics tool to extract the information that is present in the temporary storage memory like RAM.
- If no specialist advice is available, remove the power supply from the back of the computer without closing down any programs. When removing the power supply cable, always remove the end attached to the computer and not that attached to the socket, this will avoid any data being written to the hard drive if an uninterruptible power protection device is fitted.

PROCEDURE FOR GATHERING EVIDENCES FROM MOBILE PHONES

- If the device is “OFF”, do not turn “ON”.
- With PDAs or cell phones, if the device is ON, leave ON. Powering down device could enable password, thus preventing access to evidence.
- Photograph device and screen display (if available).

- Label and collect all cables (including power supply) and transport with device.
- If device cannot be kept charged, analysis by a specialist must be completed prior to battery discharge or data may be lost.
- Seize additional storage media (memory sticks, compact flash, etc).
- Document all steps involved in the seizure of device and components.

USE OF FARADAY BAD IN MOBILE SEIZURE

Benefits for the investigator if a faraday bag is used are:

1) Potentially avoids the problem of the mobile phone becoming PIN locked.
2) Faraday Window ensures the examiner to view the phone in a 'faraday' condition, thus enabling an 'immediate preview of evidence'.
3) Re-usable
4) To prevent the data from the networks communicating with the device, therefore, stops any chance of evidence being tainted.
5) Prevents any chance of evidence being manipulated during covert acquisition.

After gathering the evidence it needs to be sent to Forensic lab for the analysis and reporting of it. With the evidence, the investigation officer needs to send certain points which act as guidelines for the forensic expert to retrieve the evidence from the sent media. Hence to get the best of the expert opinion IO should follow the following process.[30]

EXPERT OPINION FROM FORENSIC EXAMINER

- The forwarding letter to the FSL for scientific analysis and opinion should mention the following information.
- A brief history of the case
- The details of the exhibits seized and their place of seizure
- The model, make and description of the hard disk or any storage media
- The date and time of the visit to the scene of the crime
- The condition of the computer system (on or off) at the scene of the crime
- Is the photograph of the scene of crime is taken?

[30] Venter, J P (2006). Process flows for cyber forensics training and operations Retrieved from <http:researchspace.csir.co.za/dspace/bitstream/10204/1073/1/Venter_2006.pdf>

- Is it a stand-alone computer or a network?
- Is the computer has an Internet connection or any means to communicate with external computers?

MODEL QUESTIONS TO BE ASKED IN CASE OF "COMPUTER AS A TARGET" CYBERCRIME

- What type of operating system has been installed on the computer?
- When was the operating system installed?
- Please provide the user names/users present in the system
- What programs or software is installed on the computer?
- What is the IP address assigned to the system, if any?
- What is the MAC address of the system?
- Are there any information relating e-mail addresses present in the computer system?
- Are there any chat messenger software installed. If so, are there any chat IDs/profiles?
- Any suspicious or malicious software installed?
- Please provide the Internet history of the computer (Web sites accessed, files uploaded, downloaded, etc.)?
- Are there any firewall logs available in the system?

QUESTIONS TO BE ASKED IN CASE OF "SENDING THREATENING E-MAIL"

- Whether the sender's e-mail address is present in the seized hard disk.
- Whether the receiver's e-mail address is present in the seized hard disk.
- Whether the contents of the e-mail message (subject mail of case) is present in the hard disk.
- Any information relating to the IP addresses are available?

QUESTIONS TO BE ASKED IN CASE OF "COMPUTER AS AN INSTRUMENT/REPOSITORY"

- Which are the user accounts that are present on the computer?
- What financial applications/software applications are installed in the system?
- Are there any logs available for these applications?
- Please provide the list of files/filenames that were recently accessed
- What external devices (like thumb drives/external hard drives) were connected to the computer?

- Are there any databases and excel spreadsheets available inactive or deleted state?
- Are there any accounting packages/software installed?
- Are there any encrypted or password-protected files available? If so, please extract the content from them?
- Are there any pornographic images/videos present in the computer system?
- Was the system date and time changed at any point in time?

1.6 LET'S SUM UP

In this chapter, we have studied about the investigation process along with the ACPO guidelines. We also studied about the different guidelines with respect to digital evidence. Finally, we ended our discussion with the steps in crime scene investigation.

1.7 FURTHER READING

- ➢ Shon Harris; "All in One CISSP Guide, Exam Guide Sixth Edition", McGraw Hill, 2013.
- ➢ LNJN National Institute of Criminology and Forensic Science, "A Forensic Guide for Crime Investigators – Standard Operating Procedures", LNJN NICFS, 2016.
- ➢ Anthony Reyes, Jack Wiles; "The Best Damn Cybercrime and Digital Forensic Book", Syngress, USA, 2007.
- ➢ Cory Altheide and HalanCarvey; "Digital Forensics with Open Source Tools", Syngress Publication.

1.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What is ACPO?

The Association of Chief Police Officers (ACPO) was a not-for-profit private limited company that for many years led the development of policing practices in England, Wales, and Northern Ireland. It has contributed a lot in terms of guidelines for handling digital evidence.

2. What are the guidelines for digital evidence?

- Identify the computer system, Secure the scene, preserve the traced evidence
- If the computer is switched off, then Photograph, label and document the system.details on collection form and collect related software peripherals, removable media, passwords if any.

- If the computer is on and prompts for any password simply disconnect the power and then Photograph, label and document the system details on collection form and collect related software peripherals, removable media, passwords if any.
- If it does not prompts for any password, then document screen, system time, network activity. Preserve the RAM content if needed using Authorized tools and procedures.
- Depending upon the case Scenario, the entire computer can be seized or any particular suspected hardware can be seized.

3. Explain the scene of offence in cyber café?

- Identify a number of computer systems present in the cyber café.
- Identify a number of computer systems connected to the Internet.
- Obtain details about the network topology and architecture (client — Server).
- Obtain the CCTV/Web camera clippings, if any.
- Whether any user management software is used by the cyber café owner?
- Obtain the log register of Internet users for the relevant period.
- Check the formatting of storage devices policy adopted by the cyber café owner.
- Check the hardware replacements done by the cyber café owner.
- Check the policy regarding removal media usage on the cyber café systems.

1.9 ACTIVITY

Briefly explain the steps in a Crime Scene Investigation along with a case study? (1000 – 1500 words)

Unit 4: Electronics Discovery: An Introduction

4

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Legal basis of electronic discovery
- ESI preservations: Obligations and Penalties
- Utilizing criminal procedure to accentuate E-discovery

1.2 INTRODUCTION

Electronic discovery or "e-discovery" is the exchange of data between parties in civil or criminal litigation. The process is largely controlled by attorneys who determine what data should be produced based on relevance or withheld based on claims of privilege. Forensic examiners, however, play crucial roles as technical advisors, hands-on collectors, and analysts.

Some examiners view electronic discovery as a second-class endeavour, void of the investigative excitement of a trade secret case, an employment dispute, or a criminal "whodunit." These examiners, however, overlook the enormous opportunities and challenges presented by electronic discovery.[31]

In technical terms,electronic discovery also poses a variety of daunting questions: Where are all the potentially relevant data stored? What should a company do to recover data from antiquated, legacy systems or to extract data from more modern systems like enterprise portals and cloud storage? Does old data need to be converted? If so, will the conversion process result in errors or changes to important metadata? Is deleted information relevant to the case? What types of false positives are being generated by keyword hits? Did the tools used to process relevant data cause any errors or omissions in the information produced to lawyers? What file server data can be attributed to specific custodians? How can an examiner authenticate database reports? What can an examiner do to fill in the gaps after the e-mail has been erroneously deleted?

Confusion over terminology between lawyers, forensic examiners, and laypeople add to the complexity of e-discovery. For instance, a forensic examiner may use the term "image" to describe a forensic duplicate of a hard drive, whereas an IT manager may call routine backups an "image" of the system, and a lawyer may refer to a graphical rendering of a document (e.g., in TIFF format) as an "image." These differing interpretations can lead to misunderstandings and major problems in the e-discovery process, adding frustration to an already pressured situation.George Socha and Thomas Gelbman have created a widely accepted framework for e-discovery consulting known as the Electronic Discovery Reference Model (EDRM).The Electronic Discovery Reference Model outlines the objectives of the processing stage, which include:

a) Capture and preserve the body of electronic documents;
b) Associate document collections with particular users (custodians);
c) Capture and preserve the metadata associated with the electronic files within the collections;
d) Establish the parent-child relationship between the various source data files;

[31] Stander, Adrie& Val, Kevin & Hooper, Val (2015).Ediscovery in South Africa and the Challenges it Faces

e) Automate the identification and elimination of redundant,duplicate data within the given dataset;

f) Provide a means to programmatically suppress material that is not relevant to the review based on criteria such as keywords, date ranges or other available metadata;

g) Unprotect and reveal information within files; and

h) Accomplish all of these goals in a manner that is both defensible with respect to clients' legal obligations and appropriately cost-effective and expedient in the context of the matter.[32]

1.3 LEGAL BASIS FOR ELECTRONIC DISCOVERY

In civil litigation throughout the United States, courts are governed by their respective rules of civil procedure. Each jurisdiction has its own set of rules, but the rules of different courts are very similar as a whole.1 As part of any piece of civil litigation, the parties engage in a process called discovery. In general, discovery allows each party to request and acquire relevant, nonprivilegedinformation in possession of the other parties to the litigation, as well as third parties (F.R.C.P. 26(b)). When that discoverable information is found in some sort of electronic or digital format (i.e., hard disk drive, compact disc, etc.), the process is called electronic discovery or e-discovery for short.

The right to discover ESI is now well established. On December 1, 2006, amended F.R.C.P. went into effect and directly addressed the discovery of ESI. Although states have not directly adopted the principles of these amendments en masse, many states have changed their rules to follow the 2006 F.R.C.P. amendments.

In ***Coleman vs Morgan Stanley***[33]***,*** after submitting a certificate to the court stating that all relevant e-mail had been produced, Morgan Stanley found relevant e-mail on 1600 additional backup tapes. The judge decided not to admit the new e-mail messages, and based on the company's failure to comply with e-discovery requirements, the judge issued an "adverse inference" to the jury, namely that they could assume MorganStanley had engaged in fraud in the underlying investment case. As a result, Morgan Stanley was ordered to pay $1.5 billion in

[32] Arkfeld, M R (2005), Electronic Discovery and Evidence, Law Partner Publishing, LLC, Phoenix, AZ

[33] *Coleman v Morgan Stanley*20 So 3d 952 (Fla Dist Ct App) [2009]

compensatory and punitive damages. An appeals court later overturned this award, but the e-discovery findings were left standing, and the company still suffered embarrassing press like The Wall Street Journal article, "How Morgan Stanley botched a big case by fumbling e-mails" (Craig, 2005).

1.4 ESI PRESERVATION: OBLIGATIONS AND PENALTIES

Recent amendments to various rules of civil procedure require attorneys—and therefore digital examiners—to work much earlier, harder, and faster to identify and preserve potential evidence in a lawsuit. Unlike paper documents that can sit undisturbed in a filing cabinet for several years before being collected for litigation, many types of ESI are more fleeting. Drafts of smoking-gun memos can be intentionally or unwittingly deleted or overwritten by individual users, server-based e-mail can disappear automatically following a systematic purge of data in a mailbox that has grown too large, and archived e-mail can disappear from backup tapes that are being overwritten pursuant to a scheduled monthly tape rotation.[34]

The seminal case of ***Zubulake v. UBS Warburg***[35] outlined many ESI preservation duties in its decision. Laura Zubulake was hired as a senior salesperson to UBS Warburg. She eventually brought a lawsuit against the company for gender discrimination, and she requested, "all documents concerning any communication by or between UBS employees concerning Plaintiff." UBS produced about 100 e-mails and claimed that its production was complete, but Ms.Zubulake's counsel learned that UBS had not searched its backup tapes. What began as a fairly mundane employment action turned into a grand e-discovery battle, generating seven different opinions from the bench and resulting in one of the largest jury awards to a single employee in history.[36]

The court stated that "a party or anticipated party must retain all relevant documents (but not multiple identical copies) in existence at the time the duty to preserve attaches, and any relevant

[34] Carrier, B. 'Open Source Digital Forensics Tools: The Legal Argument', @stake Research Report, October 2002

[35] *Zubulake v UBS Warburg*217 F R D 309 (S D N Y) [2003]

[36] Federal rules of evidence. Available online at <www.law.cornell.edu/rules/fre/rules.htm>

documents created thereafter," and outlined three groups of interested parties who should maintain ESI:

- **Primary players:** Those who are "likely to have discoverable information that the disclosing party may use to support its claims or defenses" (F.R.C.P. 26(a)(1)(A)).
- **Assistants to primary players:** Those who prepared documents for those individuals that can be readily identified.
- **Witnesses:**The duty also extends to information that is relevant to the claims or defenses of any party, or which is 'relevant to the subject matter involved in the action'" (F.R.C.P. 26(b)(1)).

The Zubulake court realized the particular difficulties associated with retrieving data from backup tapes and noted that they generally do not need to be saved or searched, but the court noted:

"It does make sense to create one exception to this general rule. If a company can identify where particular employee documents are stored on backup tapes, then the tapes storing the documents of "key players" to the existing or threatened litigation should be preserved if the information contained on those tapes is not otherwise available. This exception applies to all backup tapes".[37]

In addition to clarifying the preservation obligations in e-discovery, the Zubulake case revealed some of the penalties that can befall those who fail to meet these obligations.The court sanctioned UBS Warburg for failing to preserve and produce e-mail backup tapes and important messages, or for producing some evidence late. The court required the company to pay for additional depositions that explored how data had gone missing in the first place. The jury heard testimony about the missing evidence and returned a verdict for $29.3 million, including $20.2 million in punitive damages.

The Zubulake court held the attorneys partially responsible for the lost e-mail in the case and noted, "It is not sufficient to notify all employees of a litigation hold and expect that the party will then retain and produce all relevant information. Counsel must take affirmative steps to monitor compliance so that all sources of discoverable information are identified and searched." (Zubulake v. UBS Warburg, 2004). Increasingly, attorneys have taken this charge to heart and

[37] Magic Quadrant for E-Discovery Software, Gartner, 2014

frequently turn to their digital examiners to help assure that their discovery obligations are being met.

1.5 DETERMINING VIOLATIONS OF THE ELECTRONIC DISCOVERY PARADI

As pointed out by the Zubulake decision, the consequences of failing to preserve data early in a case can be severe. Under F.R.C.P. Rule 37, a court has broad latitude to sanction a party in a variety of ways. Of course, courts aremost concerned about attorneys or litigation parties that intentionally misrepresent the evidence in their possession, as seen in the Qualcomm case.[38]

The following 10 recommendations are provided for investigators and in-house counsel to avoid the same fate as Qualcomm (Roberts, 2008):

a) Use checklists and develop a standard discovery protocol;
b) Understand how and where your client maintains paper files and electronic information, as well as your client's business structures and practices;
c) Go to the location where information is maintained—do not rely entirely on the client to provide responsive materials to you;
d) Ensure you know what steps your client, colleagues, and staff have actually taken and confirmed that their work has been done right;
e) Ask all witnesses about other potential witnesses and where and how evidence was maintained;
f) Use the right search terms to discover electronic information;
g) Bring your own IT staff to the client's location and have them work with the client's IT staff, employ e-discovery vendors or both;
h) Consider entering into an agreement with opposing counsel to stipulate the locations to be searched, the individuals whose computers and hard copy records are at issue, and the search terms to be used;
i) Err on the side of production;
j) Document all steps are taken to comply with your discovery protocol.

[38] Computer Technology Review, Sharon Isaacson, March 2003

This is a useful and thorough set of guidelines for investigators to use for preservation of data issues, and can also serve as a quick factsheet in preparing for depositions or testimony.

1.6 ASSESSING WHAT DATA IS REASONABLY ACCESSIBLE

Electronic discovery involves more than the identification and collection of data because attorneys must also decide whether the data meets three criteria for production. Namely, whether the information is (1) relevant, (2) nonprivileged, and (3) reasonably accessible (F.R.C.P. 26(b)(2)(B)). The first two criteria make sense intuitively. Nonrelevant information is not allowed at trial because it simply bogs downs the proceedings, and withholding privileged information makes sense in order to protect communications within special relationships in our society, for example, between attorneys and clients, doctors and patients, and such. Whether information is "reasonably accessible" is harder to determine, yet this is an important threshold question in any case.[39]

In the Zubulake case described earlier, the employee asked for "all documents concerning any communications by or between UBS employees concerning Plaintiff," which included "without limitation, electronic or computerized data compilations," to which UBS argued the request was overly broad. In that case, Judge Shira A. Scheindlin, United States District Court, Southern District of New York, identified three categories of reasonably accessible data: (1) active, online data such as hard drive information, (2) near-line data to include robotic tape libraries, and (3) offline storage such CDs or DVDs. The judge also identified two categories of data generally not considered to be reasonably accessible: (1) backup tapes and (2) erased, fragmented, and damaged data. Although there remains some debate about the reasonable accessibility of backup tapes used for archival purposes versus disaster recovery, many of Judge Scheindlin's distinctions were repeated in a 2005 Congressional report from the Honorable Lee H. Rosenthal,

[39] Ward, Burke and Sipior, Janice and Hopkins, Jamie and Purwin, Carolyn and Volonino, Linda, Electronic Discovery: Rules for a Digital Age (February 27, 2011) Boston University Journal of Science and Technology Law, Vol. 18, No. 150, 2012

Chair of the Advisory Committee on the Federal Rules of Civil Procedure (Rosenthal, 2005), and Zubulake's categories of information remain important guideposts (Mazza, 2007).[40]

The courts use two general factors—burden and cost—to determine the accessibility of different types of data. Using these general factors allows the courts to take into account the challenges of new technologies and any disparity in resources among parties (Moore, 2005). If ESI is not readily accessible due to burden or cost, then the party possessing that ESI may not have to produce it (see F.R.C.P. 26(b)). Some parties, however, make the mistake of assessing the burden and cost on their own and unilaterally decide not to preserve or disclose data that is hard to reach or costly to produce. The rules require that a party provide"a description by category and locations, of all documents" with potentially relevant data, both reasonably and not reasonably accessible (F.R.C.P. 26(a)(1)(B)). This allows the opposing side a chance to make a good cause showing to the court why that information should be produced (F.R.C.P. 26(a)(2)(B)).

1.7 UTILIZING CRIMINAL PROCEDURE TO ACCENTUATE E-DISCOVERY

In some cases, such as lawsuits involving fraud allegations or theft of trade secrets, digital examiners may find that the normal e-discovery process has been altered by the existence of a parallel criminal investigation. In those cases, digital examiners may be required to work with the office of a local US Attorney, State Attorney General, or District Attorney, since only these types of public officials, and not private citizens, can bring criminal suits.[41]

A criminal agency can preserve data early in an investigation by issuing a letter under 18 U.S.C. 2703(f) to a person or an entity like an Internet Service Provider (ISP). Based on the statute granting this authority, the notices are often called "f letters" for short. The letter does not force someone toproduce evidence but does require they preserve the information for 90 days (with the chance of an additional 90-day extension). This puts the party with potential evidence on notice

[40] Friedberg, E, & McGowan, M (2003).Electronic discovery technology. In A Cohen & D. Lender (Eds.), Electronic discovery: Law and practice, Aspen Publishers

[41] See Jonathan M Redgrave & Kristin M. Nimsger, Electronic Discovery and Inadvertent Productions of Privileged Document, THE FED. LAWYER, July 2002, at 37, available at <http://www.jonesday.com/files/>

and buys the agency some time to access that information or negotiate with the party to surrender it.[42]

Another less popular method of obtaining evidence is through a court “d” order, under 18 U.S.C. §2703(d). This rule is not used as often because an official must be able to state with “specific and articulately” facts that there is a reasonable belief that the targeted information is pertinent to the case. However, this method is still helpful to obtain more than just subscriber information—data such as Internet transactional information or a copy of a suspect’s private homepage.

There are five digital storage locations that are the typical focus of e-discovery projects (Friedberg & McGowan, 2006):

- Workstation environment, including old, current, and home desktops and laptops
- Personal Digital Assistants (PDAs), such as the BlackBerry® and Treo®
- Removable media, such as CDs, DVDs, removable USB hard drives, and USB “thumb” drives
- Server environment, including file, e-mail, instant messaging, database, application and VOIP servers
- Backup environment, including archival and disaster recovery backups

Although these storage locations are the typical focus of e-discovery projects, especially those where the data are being collected in a corporate environment, examiners should be aware of other types of storage locations that may be relevant such as digital media players and data stored by third parties (for example,Google Docs, Xdrive, Microsoft SkyDrive, blogs, and social networking sites such as MySpace and Facebook).

Informational interviews and documentation requests are the core components of a comprehensive and thorough investigation to identify the potentially relevant ESI in these five locations, followed by review and analysis of the information obtained to identify inconsistencies and gaps in the data collected. In some instances a physical search of the company premises and off-site storage is also necessary.

1.8 LET’S SUM UP

[42] Kidwell, B, Neumeier, M, & Hansen, B (2005) Electronic discovery. Law Journal Press

The e-discovery field is complex, and the technical and logistical challenges routinely found in large e-discovery projects can test even the most experienced digital forensic examiner. The high stakes nature of most e-discovery projects leave little room for error at any stage of the process—from initial identification and preservation of evidence sources to the final production and presentation of results—and to be successful, an examiner must understand and be familiar with their role at each stage. The size and scope of e-discovery projects require effective case management, and essential to effective case management is establishing a strategic plan at the outset, and diligently implementing constructive and documented quality assurance measures throughout each step of the process.

1.9 FURTHER READING

- ACPO. (2008). The Good Practice Guide for Computer-based Electronic evidence. (4th ed.). Available online at www.7safe.com/electronic_evidence/
- Craig, S. (2005). How Morgan Stanley botched a big case by fumbling emails. The Wall Street Journal, A1.
- Mazza, M., Quesada, E., & Sternberg, A. (2007). In pursuit of FRCP1: Creative approaches to cutting and shifting the costs of discovery of electronically stored information, 13 Rich. J.L. & Tech., 11, 101.
- Howell, B. (2009). Lawyers on the Hook: Counsel's professional responsibility to provide quality assurance in electronic discovery. Journal of Securities Law, Regulation & Compliance, 2(3).
- Sedona Conference. (2008). "Jumpstart Outline": Questions to ask your client and your adversary to prepare for preservation, rule 26 obligations, court conferences and requests for production, May 2008. Available online at www.thesedonaconference.org/dltForm?did=Questionnaire.pdf.

1.10 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) What is the meaning of E-discovery?

Electronic discovery or “e-discovery” is the exchange of data between parties in civil or criminal litigation.

2) What are the objectives of EDRM?

The Electronic Discovery Reference Model outlines the objectives of the processing stage, which include:

a) Capture and preserve the body of electronic documents;

b) Associate document collections with particular users (custodians);

c) Capture and preserve the metadata associated with the electronic files within the collections;

d) Establish the parent-child relationship between the various source data files;

e) Automate the identification and elimination of redundant,duplicate data within the given dataset;

f) Provide a means to programmatically suppress material that is not relevant to the review based on criteria such as keywords, date ranges or other available metadata;

g) Unprotect and reveal information within files; and

h) Accomplish all of these goals in a manner that is both defensible with respect to clients’ legal obligations and appropriately cost-effective and expedient in the context of the matter.

3) Write any 3 recommendations that are provided for investigators and in-house counsel to avoid the same fate as Qualcomm?

- Use checklists and develop a standard discovery protocol;
- Go to the location where information is actually maintained—do not rely entirely on the client to provide responsive materials to you;
- Ensure you know what steps your client, colleagues, and staff have actually taken and confirmed that their work has been done right;

4) What are the five digital storage locations?

- Workstation environment, including old, current, and home desktops and laptops
- Personal Digital Assistants (PDAs), such as the BlackBerry® and Treo®
- Removable media, such as CDs, DVDs, removable USB hard drives, and USB “thumb” drives

- Server environment, including file, e-mail, instant messaging, database, application and VOIP servers
- Backup environment, including archival and disaster recovery backups

1.11 ACTIVITY

Explain the meaning of electronic discovery and the violations with respect to it? Also, how it is utilized in the criminal procedure? Briefly explain it with relevant case laws? (800 – 1000 words)

Block 2

Cyber Forensics Process, Standards and Challenges

Unit 1: Digital Evidence and Processes involved in Digital Forensics

1

UNIT STRUCTURE

1.1 LEARING OBJECTIVES

After going through this chapter, you should be able to understand:

- Challenges in cyber forensics

- Principles in evidence management
- Role of First Responder

1.2 INTRODUCTION

The field of cyber forensics is still in its infancy stage as it possesses a strong need for direction and definition. Areas of speciality within a professional environment, certifications, and/or curriculum development are still questioned. With the continued need to standardize parts of the field, methodologies need to be created that will allow for uniformity and direction. To date, huge volumes of data, heterogeneous information and communication technologies, and borderless cyberinfrastructure create new challenges for security experts and law enforcement agencies investigating cybercrimes.[43] The future of digital forensics is explored, with an emphasis on these challenges and the advancements needed to effectively protect modern societies and pursue cybercriminals. Today the technology in cyber forensic is utilizing the application of scientific methods and technics to recover data from electronic and digital media. The increase in the growth of computer and the Internet use has changed the human behaviour and ways of communication, this growth in technology has given rise to the rise in cybercrime which is now sophisticated and difficult to trace, investigate, and prosecute of criminals without reliable and accurate data collection.[44]

1.3 DIGITAL EVIDENCE

Digital evidence or electronic evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial. Before accepting digital evidence a court will determine if the evidence is relevant, whether it is authentic if it is hearsay and whether a copy is acceptable or the original is required. The digital evidence is used to establish a credible

[43] ORGANIZING RESEARCH AND DEVELOPMENT IN CYBER FORENSICS <https://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=1075&context=techmasters>

[44] Adelstein F (2006) Live forensics: diagnosing your system without killing it first. Commun ACM 49(2):63–66

link between the attacked, victim, and the crime scene. Some of the information stored in the victim's system is based on the IP address, system log-in & remote log-in details, browsing the history, log files, emails, images etc.

1.4 LOCARD'S PRINCIPLE

Wherever a criminal, steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him. Not only his fingerprints or his footprints but his hair, the fibers from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more, bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it, can diminish its value. Digital evidence is usually not in a format that is directly readable by a human. Therefore it requires some additional steps to convert it into a human-readable form in the form of writing. Digital evidences must follow the requirements of the Best Evidence Rule.[45]

1.5 BEST EVIDENCE RULE

The Best Evidence Rule, which has been established to deter any alteration of evidence, either intentionally or unintentionally, states that the court prefers the original evidence at the trial rather than a copy, but will accept a duplicate under these conditions:

- The original was lost or destroyed by fire, flood, or other acts of God. This has included such things as careless employees or cleaning staff.
- The original was destroyed in the normal course of business.
- The original is in possession of a third party who is beyond the court's subpoena power.

[45] Rahayu, S. &Robiah, Y. & Sahib, Shahrin.(2008). Mapping Process of Digital Forensic Investigation Framework. 8

This rule has been relaxed to allow duplicates unless there is a genuine question as to the original's authenticity, or admission of the duplicate would, under the circumstances, be unfair.[46]

1.6 CHARACTERISTICS OF DIGITAL EVIDENCE

The following are the essential characteristics of digital evidence:-

- ***Admissibility***

It must be in conformity with common law and legislative rules. There must be a relationship between the evidence and the fact being proved. Digital evidence is often ruled inadmissible by courts because it was obtained without authorization. In most jurisdictions, a warrant is required to seize and investigate digital devices. In a digital investigation this can present problems where, for example, evidence of other crimes are identified while investigating another.[47]

- ***Reliability***

The evidence must be from undisputed origin

- ***Completeness***

The evidence should prove the culprit's actions and help to reach a conclusion.

- ***Convincing to Judges***

The evidence must be convincing and understandable by the judges.

- ***Authentication***

The evidence must be real and related to the incident. Courts largely concerned themselves with the reliability of such digital evidence. The investigator must be able to prove to the authenticity of the digital evidence by explaining:

- The reliability of the computer equipment.
- The manner in which the basic data was initially entered.

[46] Hewling, Moniphia&Sant, Paul. (2012). Digital Forensics: An integrated approach

[47] Carrier B. D., Spafford E, (2004) "An event based Digital forensics Investigation Framework"Center for Education and Research in Information Assurance and Security

- The measures taken to ensure the accuracy of the data as entered.
- The method of storing the data and the precautions are taken to prevent its loss.
- The reliability of the computer programs used to process the data, and
- The measures taken to verify the accuracy of the program.

1.7 TYPES OF INVESTIGATION

There are four main types of investigation performed by digital forensics specialists.

a) Criminal Forensics

Criminal forensics is the largest form of digital forensics and falling under the remit of law enforcement (or privatecontractors working for them). Criminal forensics is usually a part of a wider investigationconducted by law enforcement and other specialists with reports being intended to facilitate that investigation and, ultimately, to be entered as expert evidence before the court. Focus is on forensically sound data extraction and producing report/evidence in simple terms that a layman will understand.

b) Intelligence gathering

Intelligence gathering is a type of investigation associated with crime, but in relation to providing intelligence to help track, stop or identify criminal activity. Unless the evidence is later to be used before the court of law, forensic soundness is less of a concern in this form of investigation, instead speed can be a common requirement.

c) Electronic discovery (eDiscovery)

Electronic discovery or eDiscovery is similar to ***"Criminal Forensics"*** but in relation to civil law. Although functionally identical toits criminal counterpart, eDiscovery has specific legal limitations and restrictions, usually in relation to the scope of any investigation. Privacy laws (for example, the right of employeesnot to have personal conversation intercepted) and human rights legislation often affect electronic discovery.

d) Intrusion Investigation

The final form of investigation is different from the above-mentioned three types of investigation. Intrusion investigation isinstigated as a response to a network intrusion, for example, a hacker trying to steal corporatesecrets. The investigation focuses on identifying the entry point for such attacks, the scope of access and mitigating the hacker's activities. Intrusion investigation often occurs ***"live"*** (i.e. in real-time) and leans heavily on the discipline of network forensics.

1.8 CHALLENGES IN DIGITAL FORENSICS IN PRESENT ERA

Digital forensics is facing a crisis. Hard-won capabilities are in jeopardy of being diminished or even lost as the result of advances and fundamental changes in the computer industry:

- The growing size of storage devices means that there is frequently insufficient time to create a forensic image of a subject device or to process all of the data once it is found.
- The increasing prevalence of embedded flash storage and the proliferation of hardware interfaces means that storage devices can no longer be readily removed or imaged.
- The proliferation of operating systems and file formats is dramatically increasing the requirements and complexity of data exploitation tools and the cost of tool development.[48]
- Whereas cases were previously limited to the analysis of a single device, increasingly cases require the analysis of multiple devices followed by the correlation of the found evidence.
- Pervasive encryption means that even when data can be recovered, it frequently cannot be processed.
- Use of the ***"cloud"*** for remote processing and storage, and to split a single data structure into elements, means that frequently data or code cannot even be found.
- Malware that different programmed information to persistent storage necessitates the need for expensive RAM forensics.
- Legal challenges increasingly limit the scope of forensic investigations.

These problems are most obvious to examiners faced with cell phones and other mobile computing platforms. It is vital for forensics examiners to be able to extract data from cell

[48] Brill AE, Pollitt M (2006)The evolution of computer forensic best practices: an update on programs and publications. Journal of Digital Forensic Practice, 1:3–11

phones in a principled manner, as mobile phones are a primary tool of criminals and terrorists. But there is no standard way to extract information from cell phones. In recent years there has been substantial interest in RAM-based forensics to defeat encryption and to find malware that is not written to persistent storage. RAM forensics can capture the current state of a machine in a way that is not possible using disk analysis alone. But RAM Digital Forensics tools are dramatically more difficult to create than disk tools. Unlike information written to disk, which is stored with the intention that it will be read back in the future possibly by different programmed information in RAM is only intended to be read by the running program. As a result, there is less reason for programmers to document data structures or conserve data layout from one version of a program to another. Both factors greatly complicate the task of the tool developer, which increases tool cost and limits functionality.

1.9 PROCESSES INVOLVED IN DIGITAL FORENSICS

The digital forensics process involves the following five levels of investigation:-

a) ***Identification of the Digital Evidence***

This step involves the identification of any digital evidence which might be present at the crime scene. This can involve computers, pen drives, hard disks or any other electronic device that can store digital data. Also, it needs to be taken care of that the processes followed when the computer is found in on or off state are different.

b) ***Acquisition of the Identified Evidence***

This step comes after the identification step as after the evidence has been identified it needs to be acquired in the most appropriate manner such that the integrity of the data stored in the evidence remains intact. The sub-steps followed during this part of the investigation can be seizing the crime scene, forensically acquiring the data stored in the found devices for further investigation. The two sources of evidence: ***volatile and non-volatile data*** have different methods of acquisition. In the case of volatile data, the order in which the data is collected is of utmost importance. One suggested order can be network connections, ARP cache, login session, running processes, open files and the contents of RAM. Meanwhile, in case of non-volatile data i.e. from hard-disk the bitstream image can be done using three strategies: using a hardware device such as write blocker where the system is taken offline and the hard drive is removed, using a forensic tool Helix which is used to boot the system or using a live system acquisition which can be done either locally or remotely in case of encrypted systems that cannot be taken offline or are only accessible remotely.[49]

c) Preservation of the acquired evidence

The evidence acquired should be kept in such a way that it remains the same even after the investigation process has been completed as it was first acquired. This is done via a well-defined process known as the chain of custody which ensures that the evidence remains protected from the unintended alterations. In order to achieve this, read-only copies are made by the practitioners or experts to work upon whereas, the original evidence is kept in a secured location.

d) Examination and Analysis stage

This is the most crucial step of any investigative procedure as it is the strongest as well as the most vulnerable part where any minor mistake can lead up to the evidence's ineffectiveness to be presented in the court of law. Examining the evidence involves the step of categorizing the digital evidence and the tools which would be used to analyse that evidence. For instance, a received email can include multiple information regarding the source's email address, metadata as well as the data which can be used to find the IP address of the sender's workstation. One important advice which needs to be taken care of at this stage of analysis involves the difference in the data generated from different devices. For instance, the data and the metadata generated from an image and an email would be different. Evidence's correctness and authenticity to be presented in the court of law totally depends upon the expert's experience and skill.

e) Presentation or Documentation of Evidence

This is the last stage of the investigation procedure which includes the process of presenting a report or documentation on what type of evidence was obtained, the description about the experts who worked upon the evidence, the methods followed and the tools used in a specific

[49] Carrier, B, &Spafford, E H (2004) An Event-based Digital Forensic Investigation Framework.Proceedings of Digital Forensics Research Workshop. Baltimore, MD

format. The report can also include the protocols and legal policies followed. It should be presented in the most understandable way stating its findings to be very accurate.

1.10 ROLE OF FIRST RESPONDER

The first responder is the person who first accesses the victim's computer. He must be prepared well to collect the evidence for the crime scene in a manner that is accepted by the court.[50] Therefore, the availability of trusted digital forensics toolkit is necessary for the first responder. Some of the important steps in preparing the first responder's toolkit are:

a) Create a forensics tool testbed

The testbed should be created from the trusted source and functionality of the testbed should be checked in advance before using them in the field. Some of the guidelines are:

- Identify the appropriate OS type your organization is using, based on which the testbed is created. An organization may have a verity of OS deployed in its network. For example, it may have Linux based servers and Windows and Mac-based PC/Laptop. In that case, one has to create multiple testbeds for each OS type.
- Disinfect the testbed from the availability of any data on the machine. Preferably use a new/fresh machine. In case, a new machine is not available to use wiping tools to wipe out any data from the machine.[51]
- Install the OS and all the necessary software to conduct the forensic investigation.
- Ensure that the OS and all the programmes installed in the testbed are updated to the latest version. If any patch is required for the successful operation of the system, the same should also be installed.
- Compute Hash to ensure the integrity of the file system.

b) Document the Forensics tool testbed

It includes the following:-

- Name, type and version of OS.

[50] Casey, E (2004) Digital Evidence and Computer Crime (2 ed) Elsevier Academic Press

[51] K.Rogers, M., Goldman, J., Mislan, R, Wedge, T, &Debrota, S (2006) Computer Forensics Field Triage Process Model. Proceedings of Conference on Digital Forensics, Security and Law, (pp 27-40)

- Details of the types of various applications/software installed in the testbed along with the details of the upgrades and patches.
- Details of various types of hardware installed in the testbed.
- Details pertaining to hash and checksum of the testbed.

c) Document the summary of the forensic tools

For every tool that is acquired for the testbed, the following information is documented for easy reference and record.

- Details about the source from where the software was brought. In case it's a freeware, mention the site/source from where the tool was downloaded.
- Detailed description about the purpose, working and compatibility of the tool with OS and other software.
- Details of tool dependencies and the system effects which include the details about the required system access levels by the user to run a tool and the details of shared libraries.

d) Test the tools

Now the tools selected and installed are tested in the testbed and its performance and output is examined.

1.11 LET'S SUM UP

In this chapter, we have studied digital evidence and its characteristics along with the best evidence rule. Finally, we also studied the challenges faced in digital forensics in the present era and the processes involved in digital forensics.

1.12 FURTHER READING

- ➢ Rahayu, S. &Robiah, Y. & Sahib, Shahrin. (2008). Mapping Process of Digital Forensic Investigation Framework. 8.
- ➢ Adams, Richard & Hobbs, Val & Mann, Graham. (2014). Journal of Digital Forensics, Security & Law. Journal of Digital Forensics, Security & Law. 8. 25-48.

- Hamidovic, Haris&Salkic, Hadzib. (2016). THE BASIC STEPS OF DIGITAL EVIDENCE HANDLING PROCESS. International Journal of information and communication technologies. 2.
- Prasad, Ajay &Pandey, Jeetendra. (2016). Digital Forensics.

1.13 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is Locard's Principle?**

Wherever a criminal, steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him. Not only his fingerprints or his footprints but his hair, the fibers from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more, bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it, can diminish its value. Digital evidence is usually not in a format that is directly readable by a human. Therefore it requires some additional steps to convert it into a human-readable form in the form of writing.

2. **What are the different types of investigation?**

There are four main types of investigation performed by digital forensics specialists.

a) Criminal Forensics

Criminal forensics is the largest form of digital forensics and falling under the remit of law enforcement (or privatecontractors working for them). Criminal forensics is usually a part of a wider investigationconducted by law enforcement and other specialists with reports being intended to facilitate that investigation and, ultimately, to be entered as expert evidence before the court. Focus is on forensically sound data extraction and producing report/evidence in simple terms that a layman will understand.

b) Intelligence gathering

Intelligence gathering is a type of investigation associated with crime, but in relation to providing intelligence to help track, stop or identify criminal activity. Unless the evidence is later to be used before the court of law, forensic soundness is less of a concern in this form of investigation, instead of speed can be a common requirement.

c) *Electronic discovery (eDiscovery)*

Electronic discovery or eDiscovery is similar to ***"Criminal Forensics"*** but in relation to civil law. Although functionally identical toits criminal counterpart, eDiscovery has specific legal limitations and restrictions, usually in relation to the scope of any investigation. Privacy laws (for example, the right of employeesnot to have personal conversation intercepted) and human rights legislation often affect electronic discovery.

d) *Intrusion Investigation*

The final form of investigation is different from the above-mentioned three types of investigation. Intrusion investigation isinstigated as a response to a network intrusion, for example, a hacker trying to steal corporatesecrets. The investigation focuses on identifying the entry point for such attacks, the scope of access and mitigating the hacker's activities. Intrusion investigation often occurs ***"live"*** (i.e. in real-time) and leans heavily on the discipline of network forensics.

3. What is Best Evidence Rule?

The Best Evidence Rule, which has been established to deter any alteration of evidence, either intentionally or unintentionally, states that the court prefers the original evidence at the trial rather than a copy, but will accept a duplicate under these conditions:

- The original was lost or destroyed by fire, flood, or other acts of God. This has included such things as careless employees or cleaning staff.
- The original was destroyed in the normal course of business.
- The original is in possession of a third party who is beyond the court's subpoena power.

This rule has been relaxed to allow duplicates unless there is a genuine question as to the original's authenticity, or admission of the duplicate would, under the circumstances, be unfair.

1.14 ACTIVITY

Explain the challenges and the process involved in digital forensics along with the Role of the First Responder and the important steps in preparing the toolkit? (1000-1500 words)

2

Unit 2: Overview of First Responder

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Understand Cyber forensics investigation Phases
- The process of forensic duplication
- Role of First responder ,its toolkit and procedure

1.2 PHASES OF CYBER FORENSIC INVESTIGATION

We all know that cyber forensics is a branch of forensic science which mainly includes the different stages of digital evidence namely Identification, Acquisition, Analysis and Presentation.[52]

Despite these stages, there are different phases of cyber forensics. Lets' us understand every phase in detail.

1. Planning

In this phase, investigator does all the necessary arrangement to carry out the actual forensic investigation. This phase mainly consists of requirement and information gathering. This phase ensures high quality investigations output. In this phase, the forensic investigator gathers all related information of the incident actively and passively. He also prepares toolkit required for the investigation by understanding the scope. The forensic investigator obtains permission from authorities to conduct further steps. This permission is formerly known as Search Warrant. With the proper execution of the planning phase, the forensic investigator gets in-depth knowledge of facts of the case which is required to decide further approach. The key elements of this phase are interviewing the victims, identifying affected computing devices and deciding the digital forensic procedure to be used. In this process, the forensic investigator has given instructions, clarification and guidelines for performing activities. Allocation of roles and resources is been decided in this phase. Obtaining approval for forensic investigation is the key factor of this phase.[53]

2. Search and Identification

[52] Nelson, Bill. Guide to Computer Forensics and Investigations. Boston, MA: Thomson Course Technology, 2004 (ISBN 0-619- 13120-9)

[53] National Institute of Justice. Forensic Examination of Digital Evidence: A Guide for Law Enforcement <http://www.ncjrs.org/pdffiles1/nij/199408.pdf >

This phase mainly deals with identifying the affected people and the infrastructure of the given incident. This can be done effectively with the proper inputs obtained from the previous phase. Different tools and methods can be used to identify the type of attack. Search facilitates examination of the suspected people as well as systems. This phase also contributes to deciding the scope of the overall investigation. Proper approval is a necessity to conduct this phase. The output of this phase clarifies the number of people and the system to be examined in further investigation.

3. SEIZER

This phase starts with securing the crime scene. Before the actual examination of digital evidence in the forensic lab, it should be properly seized. There are different seizer procedures for different types of evidences. As per the requirement, scientific and legal seizer procedure is used like Isolation of system from the network, a photograph of the running machine skill. Applying forensic shutdown processes. Removing storage media like hard disk, memory card without any damage etc. The seizer memo is been created which is signed by the investigator and the witnesses. Seizer memo contains a brief description of evidence and procedure followed to seize particular evidence. The digital evidence collection form is been also prepared and filled accordingly for the sized evidence.[54]

4. ACQUIRE

The acquisition phase mainly consists of bit by bit forensic disk imaging, disk cloning, taking memory dump and creating evidence file suitable for analysis purpose. The hardware and software write blockers are used in this process to avoid any unintentional alteration or modification in digital evidence. To ensure the admissibility and integrity of the evidence a hash value is been calculated in this phase. There are different forensic tools available for different evidences to acquire entire evidence in a forensic manner.

[54] National Institute of Standards and Technology. CFTT Methodology Overview <http://www.cftt.nist.gov/Methodology_Overview.htm>

The acquisition can be physical or logical. In a physical acquisition, the entire disk is been acquired. In a logical acquisition, logical partition of the disk is been acquired. In both cases write blocker are required. In this process, copies of evidence are made and its hash value is been verified.

5. COLLECT AND PRESERVE

In this phase, sealing, labelling and bagging of the evidence is been done at the crime scene. At most care is been taken while packing digital evidences is been taken in order to avoid physical damage during transportation. Chain of custody document is been created and properly filled. This document gives the information regarding accountability of the evidence in terms of who, when, why and for how much duration was handling that evidence. Properly sealed evidence is been created and preserved in an evidence storage box. The preserved evidence will be further transported to the location where the actual analysis will be carried out.

6. ANALYSIS

The acquired information needs forensic examination. When the evidence is been transported to the forensic lab before analysis, the hash value is been verified by the forensic experts. This helps to prove the integrity of digital evidence before analysis. Every file out there is with some purpose and proper analysis of the available data can reveal many ways to proceed in further investigation. For the said purpose, the appropriate techniques and tools need to be used to make a relevant mole-hill out of the mountain of the data, consistently yielding exemplary and concise results.

The examiner may use additional tools to recover deleted information. The used tools must be validated to ensure their reliability and correctness. Forensic expert analyze the evidence twice to verify the correctness of the findings. During analysis, the evidence found is been assembled to reconstruct event or actions to provide the facts.

7. REVIEW AND REPORT

After the examination is complete, the findings are reviewed and documented in the report. It includes a detailed description of the conducted steps during the investigation. The examination report typically contains following details:

Name of the examiner who did the examination, Date and time when is been done, Software and hardware that were used, their version numbers, Hash value verification and related clicked photographs.

The information related to the acquired evidence such as hard disk and mobile device details should be also included. The report generated should be easy to understand and explain in precise details. Further actions are determined after the report is reviewed

8. Presentation

Presenting an understandable, defendable and complete report is the key to gettingthe desired outcome of the whole process. Expert witness testimony is one of the most important tasks of presentation finding. Success of the forensic investigation is very much dependent upon the way it has been presented and defended in a court of law.

1.3 FORENSIC DUPLICATION

Forensic duplication refers to bitstream imaging of data from the digital media in question. Data resides in all sorts of storage media present in computers, smartphones, GPS devices, USB drives, and so on.[55] We need to be able to get to this information in a manner that it does not change the information on the devices themselves. If the evidence is not collected properly, we face an issue where the results of the forensic exam will be put in doubt. Hence it is necessary to copy the data carefully in a forensically sound manner.

LOGICAL BACKUP	BITSTREAM IMAGING
A logical backup copies the directories and files of a logical volume. It does not capture	Also known as disk imaging/ cloning/ bitstream imaging generates a bit-for-bit copy

[55] Kruse, Warren G., Heiser, Jay G.; Computer Forensics: Incident Response Essentials, Addison Wesley, Boston, Massachusetts, September 2001, ISBN: 0-201-70719-5

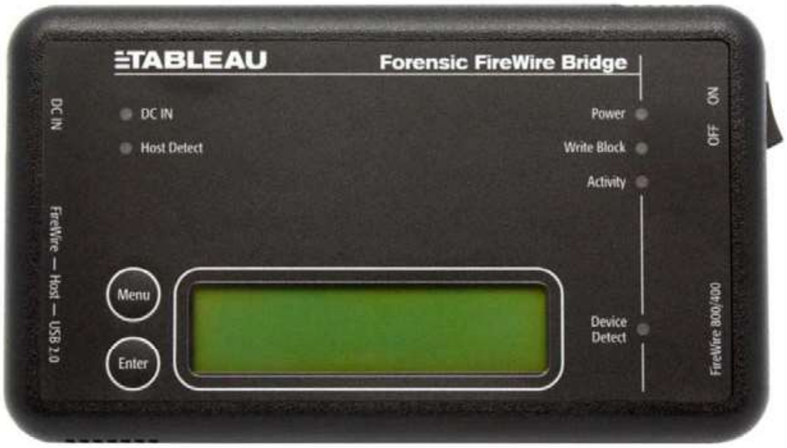
other data that may be present on the media, such as deleted files or residual data stored in slack space.	of the original media, including free space and slack space. Bitstream images require more storage space and take longer to perform than logical backups.

The Important thing required for forensic Investigation is Write blocker

WRITE BLOCKER

A write-blocker is hardware or software-based tool that prevents a computer from writing to computer storage media connected to it. Hardware write-blockers are physically connected to the computer and the storage media being processed to prevent any writes to that media.
Features:-

- Prevents any writes to the seized media
- Suspect hard disk connected to the forensic computer via a write blocker



Things to understand and remember about Digital evidence

- Almost every type of crime has digital evidence in it.
- The investigator must apply the same level of maturity, knowledge, security and safety while dealing with digital evidence likewise other traditional evidence

- Nature of Digital Evidence is delicate and fragile. Hence improper handling may result in damage or tampering of the evidence.
- Digital Evidence can be easily altered or manipulated without intention
- Never Assume Digital evidence is destroyed completely

RULES OF DIGITAL FORENSICS

- Never work on original evidence.
- Never mishandle evidence.
- Use proper software utilities to retrieve evidence from the media.
- Document everything while handling the suspected media.[56]

THE FOUR PRINCIPLES FOR THE AUTHENTICATION AND INTEGRITY OF EVIDENCE ARE

PRINCIPLE 1:

No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.

PRINCIPLE 2:

In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

PRINCIPLE 3:

An audit trail or another record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

PRINCIPLE 4:

The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

HASHING

Hashing is a process of converting large, possibly variable-size amount of data into a small datum by well-defined procedure or mathematical function.[57]

[56] Mandia, Kevin, Prosise, Chris; Incident Response: Investigating Computer Crime, New York, 2001, ISBN: 0-07-213182-9

Salient features of the process of the hashing

- The integrity of the seized evidence through the forensically proven procedure.
- Produces fixed length unique value representing the data on the seized media.
- Any changes in the evidence will result in a change in the hash value
- Hashing is a process of converting the large, possibly variable-size amount of data into a small datum by well-defined procedure or mathematical function.
- Hashing is mainly done to check the integrity of the data.
- Values returned after hashing is commonly called as hash values, hash sums or hashes
- Commonly used Hash functions are
- MD5 Hash Algorithm
- SHA1 Hash Algorithm
- While imaging the original Hard disk, a hash value is generated.
- After imaging,the hash value will be generated.
- The hash value of the original Harddisk = Hash value of the imaged Hard Disk, then we can say that the Message integrity is 100%

Commonly used Software for Imaging will calculate this Hash Values. Say for example

1. C-DAC's Cyber Check Suite
2. FTK Imager
3. Win Hex
4. Encase

1.4 INTRODUCTION TO FIRST RESPONDER

The first responder is the person who plays a vital role in the overall investigation. The tasks performed by the first responder are very much crucial for the investigation. Any mistake by the first responder may lead to tampering of the evidence or wrong direction of the investigation. Hence, the first responder is very much responsible for the further success of the investigation. The first responder is defined as a person who arrives first at the crime scene and accesses the

[57] Nelson, Bill; Phillips, Amelia; Enfinger, Frank &Steuart, Chris; Guide to Computer Forensics and Investigations, Boston, Massachusetts, Course Technology, 2004, ISBN: 0-619-13120-9

victims computing devices after the incident. Protection, Integration and Preservation of the digital evidence are the key responsibilities of the first responder. He may be network administrator, investigation officer, law enforcement officer etc.[58]

Following are the important roles of First Responder:

- Identify the crime scene, affected people and affected computing devices.
- Protect the identified subject of the crime scene.
- Preserve the temporary and fragile evidence.
- Gather detailed information about the incident.
- Document all the findings.
- Seizer of the identified Digital Evidences.
- Package and transport of the Digital Evidence.

1.5 FIRST RESPONDER TOOLKIT

First Responder Toolkit defined as a collection of tools required to seize digital evidence in a genuine and presentable way. The toolkit helps First Responder to understand the limitations and capabilities of digital evidence at the time of collection.

The first responder is responsible to select a trusted forensic tool that gives the desired output. While creating first responder toolkit, the tools must be tested and validated before actual use. The details of every tool should be documented. Along with version name and hardware requirements. Multiple tools for similar functionality should be available in the toolkit. First responder toolkit should consist of a collection of following a different set of tools.

Disassembly Tools- Screw Drivers, Wire Cutters, Tweezers etc.

Documentation Tools- White Papers, Markers, Tag, Stick-on papers etc.

Packaging Tools- Evidence Bags, Bubble Wrap, Tape, Cable ties, Anti-static bubble wrap, Anti-static bags etc.

[58] US Department of Justice; Electronic Crime Scene Investigation: A Guide for First Responders, Washington D.C., July 2001, NCJ-187736<http://www.ojp.usdoj.gov/nij/pubs-sum/187736.htm>

Forensic Equipment- Bootable Disk, External Hard Drives, Pen Drives, Write Blockers, Data Acquisition Software and Hardware field response Kit.

1.6 FIRST RESPONDER BASICS

THERE ARE SOME GROUND RULES OF FIRST RESPONSE[59]

Rule 1- The first responder must be competent and experience in handling technological gadgets.

Rule 2- The first responder should not do any such act which may tamper the digital evidence. The first responder should have knowledge of data acquisition technique mainly imaging and cloning.

Rule 3- He should secure the crime scene and maintain a secure state until the forensic team advises.

Rule 4- He should never take help of suspect to access the computing devices which may hold possible digital evidence.

Rule 5- He should document all the details of the crime scene and handed over those notes to forensic experts.

1.7 FIRST RESPONDER PROCEDURE

Following are different steps which should be taken by the first responder.[60]

Step 1. After planning for search and seizer and obtaining search warrant the first responder should secure and evaluate crime scene and conduct the initial search.

Step 2. In order to gather information regarding the incident, the first responder supposed to conduct the interviews.

Step 3. The first responder needs to photograph the crime scene and draw sketches of the scene.

[59] <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/394779/ediscovery-digital-forensic-investigations-3214.pdf>

[60] <https://forensiccontrol.com/resources/beginners-guide-computer-forensics/>

Step 4. The first responder needs to document all the findings and create a note of it.

Step 5. The first responder needs to remove the storage device and note down its details.

Step 6. The first responder needs to exhibit numbering to the seized evidence and preserve them.

Step 7. Packaging and selling of the collected evidence should have been properly carried out with labelling upon it.

Step 8. The first responder should make sure that the evidence will be transported to a forensic lab safely.

SECURING CRIME SCENE

It is important to follow a certain procedure in order to secure the crime scene. Properly secured crime scene help forensic investigator to carry out further tasks.

Following are some guidelines to the first responder in order to effectively secure the crime scene.

a. Understand and verify the type of incident and prepare accordingly.
b. Make sure that the premise is safe for investigators.
c. Find and help the victim.
d. Ensure that nobody will access the computer systems by isolating the people out there.
e. Document all connection of the suspected device and disconnect to make the system stand alone.
f. Observe the situation at the crime scene and note down all these observations.
g. Protect the fingerprints that can be found on the suspected computing devices.
h. All the forensic investigator should wear hand gloves and anti-static wrist belts.

COLLECTING PRELIMINARY INFORMATION

In order to collect initial information, the interviews of the related people should be carried out. For that questionnaire according the incident needs to be prepared. Search warrant act as permission to conduct the interviews. If required the written consent of the interviewer should be obtained before the interview. If required witness signature can also be obtained over the important documents such as search warrant, consent form etc. While conducting interviews different question should be asked to get detailed knowledge about certain facts e.g. owner and user of the computing device, internet service provider, purpose of using the system, offsite data storage, password required to access system software or data etc.

The first responder can also create a checklist of the expected information which needs to be collected as per the type of the incident.

Following are some of the key questions which should be discussed during this phase of the investigation.

- What steps were taken to contain the issue?
- Were there any logs (system access, etc.) present that cover the issue?
- Are there any suspicious entries present in them?
- Did anyone use the system after the issue occurred?
- Did you observe any similar instance before?
- Were there any alarms that were set off by the firewall/IDS/network security devices?
- Please give detailed documentation on the set of commands or processes run on the affected system or on the network after the issue occurred.
- Do they have similar systems in any of the branch/other offices?
- Whether log register of the Internet users/other users is maintained?
- Are there any questions about the issue that have not been answered?

At the scene of the offence, IO should gather the following information during the interviews phase

- Identify the complainant/owner (s) of the various devices and obtain the access details, usernames, and service providers' details.
- Gather information as provided in the questionnaire(s) above, on all the security systems.

- Identify the list of the people who can identify the network and a schematic diagram of the network.

DOCUMENTING THE SCENARIO

It is important to create certain records by documenting the crime scene. This may give certain findings which can be used further. All the observation of the crime scene should be properly documented such as the position of the screen, mouse and other components of the system. Listing down all the components and its connections help to understand the technique used by the criminal. Documenting also includes a detailed description of different facts of computing devices such as power status, storage devices etc. Photograph of the screen of running computing devices should be clicked and write down the notes of the observations in it. A video camera can be used to capture the entire scene of the crime. A still camera should be used to take the photographs of the important object at the crime scene. Photography helps to notice even the smallest piece of evidence. In the documentation of the crime scene, sketches should be drawn for the layout of the area.

COLLECTING AND PRESERVING EVIDENCE

Nowadays there are many storage media available. As an Investigator one should know where the Digital Evidence is.The investigator should not ignore even a small piece of paper. It may contain valuable information that can be a Substantial Evidence to catch hold a criminal or culprit. This is a very important task for the Investigator.[61]

List of Storage Device to be collected from the scene of the offence

- CPU
- Hard Disk
- Floppy Drive
- CD’s & DVD’s Drive

[61] <https://en.wikibooks.org/wiki/Introduction_to_Digital_Forensics/Types>

- USB Memory Sticks
- Pen Drives
- Memory Cards
- Portable Hard Disks
- Tape Drives

The very important stage of Investigation is to isolate all the Memory Components from the Computer or computer Network. That simply means making computer Standalone. This has to be done in order to avoid manipulation, alteration or deletion of Digital Evidence. As far as possible cover the mouse and keyboard with polythene covers to preserve fingerprints.

PACKAGING AND TRANSPORTING EVIDENCE

PACKAGING

Following are the important points to be considered while packaging the evidence.

- Evidence should be properly documented
- The evidence should be labelled as per the type of evidence.
- The evidence should be inventoried
- Evidence should always be packed in antistatic packaging.
- Avoid folding, bending, or scratching the evidence.
- Seized / Confiscated Material should be properly packed in the box.
- Place labels (Exhibit No :) on the top of the package
- Check the size of the Hard Disk before seizing.
- Bring One Blank hard disk with the exact capacity (or more) that of suspect's HDD for forensic duplication process.

TRANSPORTATION

- The utmost care has to be taken while carrying the Seized components from one place to another.

- Ignorance while transportation may lead towards Tampering of Evidence
- Due to the sensitive and fragile nature of the computer evidence, place the computer in a box properly cushioned with non-static material.
- All the Seized Components should be packed with proper Packing material (Cello Tape, Boxes, Anti-Static Bags, Thermacol etc.)
- The Components should be kept properly.
- Store the computer is secure and dust-free place.
- The storage should not come in contact with water.
- Vibration Free Transportation.
- Evidence should not be kept in contact with any Electro-Magnetic field.
- As far as possible cover the mouse and keyboard with polythene covers to preserve fingerprints.
- Don’t bend the Pen drives, Floppy, CDs etc.
- Don’t place labels directly on Floppy drive/CD.
- Store it in normal temperature.

CRIME SCENE REPORTING

In order to explain what exactly has happened during the investigation, the investigator should document all the actions performed over the evidence. The overall responsibility of any changes in the evidence goes with the forensic investigator. Hence, the proper documentation is very much an important aspect of digital forensics.

Following are some of the key documents which every investigator should create during his investigation.

- Search warrant

- Chain of custody
- Digital evidence collection form
- Digital forensic report

Preparing a good and admissible report is the skilful work and the most important phase of the forensics process. The investigator's knowledge is judged by what he writes. The court cases can be won or lost because of the reports and its quality. Hence the investigator should have the knowledge to represent the facts and findings in a simple and understandable manner through the report. The report should be written in such a way that it should speak for the investigator for itself and it will exist as an official record for that case.

SALIENT FEATURES OF GOOD REPORT

- It perfectly describes the incident and its details
- It should be easy to understand by decision-makers.
- It gives a clear picture of the investigation without any open-end conclusion.
- It defines the proper timeline of the investigation.
- It omits irrelevant information.
- It clearly states what the investigator has done, which facts are uncovered and how these facts lead to the final conclusion.
- It provides supporting material such as equation, data, tables and figures.
- Anyone who is new to the situation should be able to understand it through the report.

1.8 LET'S SUM UP

In this chapter, we have studied the different phases of cyber forensic investigation along with forensic duplication. We also studied the basics and toolkit of First Responder and have ended our discussion with the First Responder Procedure.

1.9 FURTHER READING

- "Electronic Crime Scene Investigation – A Guide for First Responders" by National Institute of Justice, USA; (http://www.ojp.usdoj.gov/nij)
- Mugisha, David. (2019). ROLE AND IMPACT OF DIGITAL FORENSICS IN CYBER CRIME INVESTIGATIONS. International Journal of Cyber Criminology. 47. 3.
- Resources.sei.cmu.edu (2019), https://resources.sei.cmu.edu/asset_files/Handbook/2005_002_001_14429.pdf (last visited Nov 25, 2019).
- Ncjrs.gov (2019), https://www.ncjrs.gov/pdffiles1/nij/187736.pdf (last visited Nov 25, 2019).

1.10 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What are the different phases of cyber forensic investigation?**

   - Planning
   - Search and Identification
   - Seizer
   - Acquire
   - Collect and Preserve
   - Analysis
   - Review and Report
   - Presentation

2. **What are the ground rules of the first responder?**

Rule 1- The first responder must be competent and experience in handling technological gadgets.

Rule 2- The first responder should not do any such act which may tamper the digital evidence. The first responder should have knowledge of data acquisition technique mainly imaging and cloning.

Rule 3- He should secure the crime scene and maintain a secure state until the forensic team advises.

Rule 4- He should never take help of suspect to access the computing devices which may hold possible digital evidence.

Rule 5- He should document all the details of the crime scene and handed over those notes to forensic experts.

3. **What are the steps that needs to be taken by the first responder?**

Following are different steps which should be taken by the first responder.

Step 1. After planning for search and seizer and obtaining search warrant the first responder should secure and evaluate crime scene and conduct the initial search.

Step 2. In order to gather information regarding the incident, the first responder supposed to conduct the interviews.

Step 3. The first responder needs to photograph the crime scene and draw sketches of the scene.

Step 4. The first responder needs to document all the findings and create a note of it.

Step 5. The first responder needs to remove the storage device and note down its details.

Step 6. The first responder needs to exhibit numbering to the seized evidence and preserve them.

Step 7. Packaging and selling of the collected evidence should have been properly carried out with labelling upon it.

Step 8. The first responder should make sure that the evidence will be transported to a forensic lab safely.

4. **What are the salient features of a good report?**

- It perfectly describes the incident and its details
- It should be easy to understand by decision-makers.
- It gives a clear picture of the investigation without any open-end conclusion.
- It defines the proper timeline of the investigation.
- It omits irrelevant information.
- It clearly states what the investigator has done, which facts are uncovered and how these facts lead to the final conclusion.
- It provides supporting material such as equation, data, tables and figures.
- Anyone who is new to the situation should be able to understand it through the report.

1.11 ACTIVITY

Briefly explain the procedure that needs to be undertaken by the First Responder along with a case study? (1000-1500 words)

Unit 3: Evidence Management and Anti-Forensics

3

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you will be able to understand:

- Difference between physical and digital evidence
- Detail procedure of seizure proceedings by Investigation officer
- What are challenges to cyber forensics
- Definition of Anti-forensics and its types

1.2 DIGITAL EVIDENCE

In this chapter, we will understand the different basic concepts related to the entire technical investigation of digital evidence and its management.

Digital evidence or electronic evidence is ***"any probative information stored or transmitted in digital form that a party to a court case may use at trial".*** Section 79A of IT (Amendment) Act, 2008 defines electronic form evidence as "any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones and digital fax machines"

1.3 DIFFERENCE BETWEEN PHYSICAL AND DIGITAL EVIDENCE

Digital Evidence	**Physical Evidence**

It can be duplicated and the duplicated copy can be analyzed as if it was original.[62]	It cannot be duplicated as Digital Evidence
Modification or Tampering of Digital Evidence can be easily identified by using appropriate Software by comparing with the original.	If any modification or Tampering is done it would be highly difficult to identify the changes happened.
It cannot be destroyed easily. Even if the evidence is destroyed, recovery is possible(not all times)	If the Evidence is destroyed it is highly impossible to bring back to its original form.
It facilitates working on duplicate copies of the digital media, original along with copies will still remain to help the investigators in the event of damage to the copies.	Since duplication is not possible, once the evidence is destroyed, the evidence cannot remain.
Less Tangible when compared with physical evidence	Tangible in nature

1.4 SOURCES OF DIGITAL EVIDENCE

Following are the different sources of digital evidence:-

[62] Scientific Working Group on Digital Evidence (SWGDE) of the National Center for Forensic Science (NCFS). Best Practices for Computer Forensics V2, 2006a. Retrieved From the World Wide Web on 07/07/12: URL <http://ncfs.org/swgde/documents/swgde2006/Best_Practices_for_Computer_Forensics%20V 2.0.pdf>

VOLATILE EVIDENCE

Volatile data will include information about the running process, network connections, clipboard contents, and data in memory.[63]

Volatile Evidence can be found on:

- Ram Memory
- Temporary file System / Swap Space
- Cache Memory etc.

NON-VOLATILE EVIDENCE

The data can be retrieved even when the computer is switched off.

Examples of Non-Volatile Data commonly includes:

- Flash Memory
- Hard Disk, Magnetic Tape
- Optical Disc etc.

Examples of digital evidence:

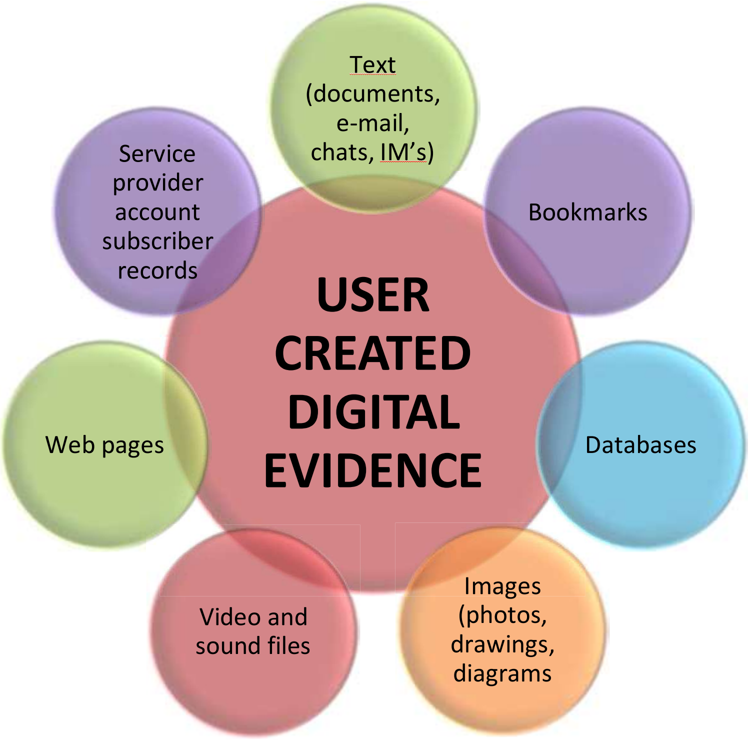
- Emails
- Web Server Logs
- Digital Photographs
- ATM Transaction logs
- Word processing documents
- Instant message histories
- Files saved from accounting
- Programs
- Spreadsheet
- Internet browser histories
- Databases,

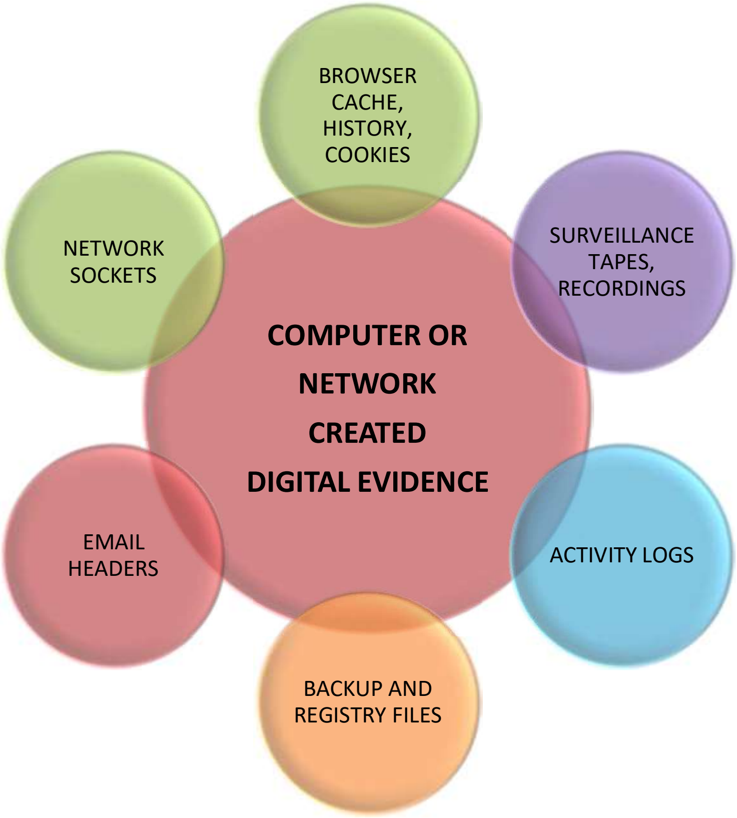
[63] Mason, D, Carlin, A, Ramos, S, Gyger, A, Kaufman, M, Treichelt, J, (2007)Is the open way a better way? Digital forensics using open source tools.The Computer Society. 1-10

- The contents of Computer Memory,
- Computer backups,
- Computer printers
- Global Positioning System tracks,
- Logs from a hotel's electronic door locks,
- Digital video or audio files.

We can categorize digital evidence in two main subcategories:-

1. User-Created digital evidence
2. Computer Created Digital evidence


USER CREATED DIGITAL EVIDENCE
Text (documents, e-mail, chats, IM's)
Bookmarks
Databases
Images (photos, drawings, diagrams
Video and sound files
Web pages
Service provider account subscriber records


BROWSER CACHE, HISTORY, COOKIES
NETWORK SOCKETS
SURVEILLANCE TAPES, RECORDINGS
COMPUTER OR NETWORK CREATED DIGITAL EVIDENCE
EMAIL HEADERS
ACTIVITY LOGS
BACKUP AND REGISTRY FILES

1.5 SEIZURE PROCEEDINGS

Following is the probable list of equipment's which can be seized in technology-based crimes

- CPU
- Hard Disk
- Floppy Drive
- CD's & DVD's Drive
- USB Memory Sticks
- Pen Drives
- Memory Cards
- Portable Hard Disks
- Tape Drives
- Various Hi-Tech Gadgets
- & in some cases Cell phone / Mobile Handset

PANCHANAMA (SEIZURE MEMO)

The legal provisions empowering the investigation officer to conduct search and seizure are provided under section 165Cr PC and section 80 of the ITAA 2008.Panchanama and seizure procedure is as important in cybercrime investigation as in any other crime. Make sure one of the technical people from the responder side along with two independent witnesses is part of the search and seizure proceedings, to identify the equipment correctly and to guide the IO and witnesses.[64] Please refer to the notes made during the pre-investigation assessment for cross verifying and correctly documenting the technical information regarding the equipment, networks and other communication equipment at the scene of the crime.Time Zone/System Time Play a very curtail role in the entire investigation. Please make sure this information is noted carefully in the panchanama, from the system that is in "switch on" condition. Please Don't switch On any device. Please make sure serial number is allotted for each device and the same should be duly noted not only in the panchanama but also in the chain of custody and digital evidence form.[65]Make sure each device is photographed before starting of the investigation process at their original place along with a respective reference.Make sure the photograph hard disk drive or any other internal part along with the system, once removed from the system

Capture the information about the system and dada you are searching and seizing in the Panchanama .Brief the witnesses regarding the tools used to perform search and seizure of digital evidence

Hence following are the important points to be considered while drafting a seizure memo.

- Power to search, seize under Section 165 Cr PC and, Section 80 of the ITAA 2008.
- Independent Witnesses.
- Time Zone/System Time
- The serial number for each seized device
- Chain of Custody & Digital Evidence Collection forms

DIGITAL EVIDENCE COLLECTION FORM

[64] Kruse W Heiser J G (2001) Computer Forensics: Incident Response Essentials (1st ed), Addison Wesley Professional. USA

[65] Casey, E (2004). Digital Evidence and Computer Crime, Forensic science, Computers and the Internet. Academic Press, London, UK

Digital Evidence Collection form is one of the most important elements of the forensic process. It is necessary that the steps taken for collection should be accurate and repeatable with the same results every time it is done. For this to happen, proper documentation of the process used for collection needs to be maintained for every device that is collected. This documentation should contain all the information about the evidence that is visible to the naked eye. It should contain information about the kind of software and version used and the time when the collection process started and ended. This documentation called as the Digital Evidence Collection (DEC) form thus consists of the information on the evidence and the media on which the evidence is being copied to.[66]

DIGITAL EVIDENCE COLLECTION (DEC) FORM SHOULD HAVE THE FOLLOWING FIELDS

- System Information
- Type — Device type which is produced to extract evidence like desktop, laptops, etc.
- Manufacturer — The device manufacturer information to be documented.
- Model Number — The device model number information to be documented.
- Serial Number / any unique identification feature — The device serial number information to be documented.
- BIOS Date/Time — BIOS information of the device.
- Property Form Number / Evidence Number — Unique number assigned to each device for easy identification by the unit after it is brought to the police station/unit.
- It is one most important element of the forensic process.
- Proper documentation of the process used for the collection of evidence must be maintained for every device collected.
- This document should contain all information about the evidence visible to naked eye
- It should contain information about the kind of software and version used and the time collection process started and ended.
- During the process of digital evidence collection, if the IO is trained or has a technical expert to support him, He should forensically image the evidence and acquire the hash value and note the same in DEC form as well as in panchanama.

[66] Cuardhuain S O, (2004) An Extended Model of Cyber Crime Investigation Journal of Digital Evidence. Vol 3 Issue 1

- The process, the tool and the hashing algorithm used should be reflected in DEC form the report generated by forensic tool should form as an enclosure to DEC.

CHAIN OF CUSTODY

Chain of custody refers to the documentation that shows the people who have been entrusted with the evidence. These would be people who have seized the equipment, people who are in charge of transferring the evidence from the crime scene to the forensic labs, people in charge of analysing the evidence, and so on. As electronic evidence is easy to tamper or to get damaged, it is necessary for us to know exactly who, when, what, where, and why was the evidence transferred to the Concerned person.[67]

- It refers to the documentation that shows the people who have been entrusted with the evidence.
- These would be people who have seized the device-
  - people who are in charge of transferring the evidence from the crime scene to forensic lab,
  - people in charge of analysing the evidence and so on.
- Due to the sensitive nature of digital evidence, it necessary to know who, when, what, where, and why was the evidence transferred to the concerned person.
- It is difficult to prove the integrity of the evidence if the chain of custody is not properly maintained.
- Lack of integrity in the process of custody and absence of appropriate documentation in this regard, will not be detrimental to the cybercrime investigation, during the trial but also, exposé the IO's to criminal liability under section 72 of the ITAA 2008.

IMPORTANT POINTS TO CONSIDER FOR CHAIN OF CUSTODY

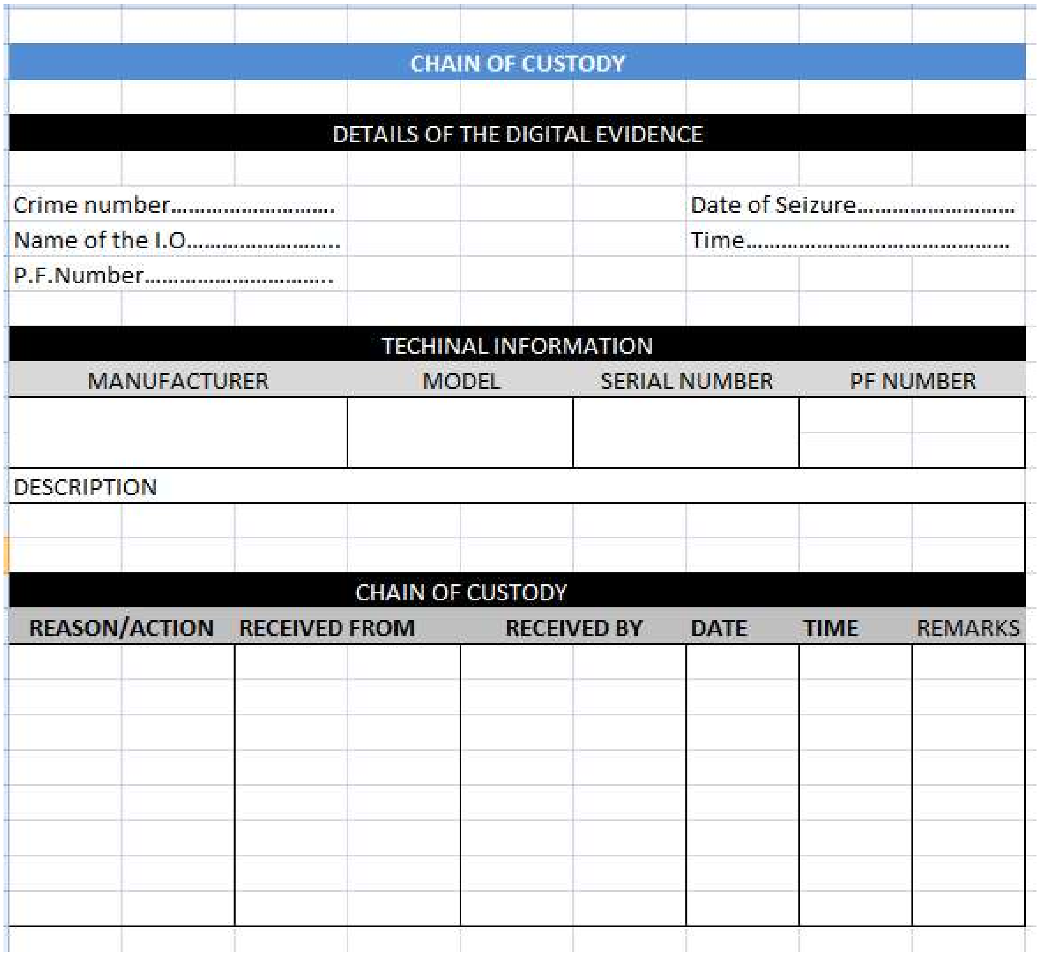
- Physically inspect the storage medium – take photographs and systematically record observations[68]
- Guard against hazards like theft and mechanical failure.

[67] Yong-Dal S, (2008) New Digital Forensics Investigation Procedure Model. Proceedings of Fourth International Conference on Networked Computing and Advanced Information Management. Available at: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4624063>

[68]Kuchta K J, (2000) 'Computer Forensics Today Law, Investigations and Ethics Available from: <http://www.liv.ac.uk/library/ohecampus/>

- Use good physical security and data encryption.
- Keep multiple copies in a different location.
- Protect digital magnetic media from external electric and magnetic fields.
- Ensure protection of optical media from scratches.
- Account for all people with physical or electronic access to the data.
- Keep the number of people involved in collecting and handling the devices and the data to a minimum.
- Always accompany evidence with their chain of custody forms.
- Give the evidence positive identification all the times i.e. legible and written with termagant ink.
- Establishing the integrity of the seized evidence through the forensically proven procedure by a technically trained IO.
- The seized original evidence can be continued to check for its integrity by comparing its hash value to identify any changes to it.

FORM



CHAIN OF CUSTODY

DETAILS OF THE DIGITAL EVIDENCE

Crime number............................ Date of Seizure...........................

Name of the I.O......................... Time..

P.F.Number...............................

TECHINAL INFORMATION

MANUFACTURER	MODEL	SERIAL NUMBER	PF NUMBER

DESCRIPTION

CHAIN OF CUSTODY

REASON/ACTION	RECEIVED FROM	RECEIVED BY	DATE	TIME	REMARKS

1.6 CHALLENGES TO FORENSICS

The Direct Challenge to forensic is the use of anti-forensics by the attacker. In this chapter, we will see the different methods by which the forensic investigation process may become difficult for the investigating officer.

1.7 INTRODUCTION TO ANTI-FORENSICS

The objective of cyber forensics is to collect, analyse the evidence from the seized devices in such ways so that they are admissible in a court of law. There are many computer criminals are aware of this issue. They try to find a countermeasure technique and even developing tools specifically designed to conceal their activities and destroy digital evidence. Anti-forensics is a collection of tricks and techniques that are used and applied with the clear aim of forestalling the forensic investigation. Anti- forensics works in the exact opposite direction of the cyber forensics. These methods make investigation much time consuming or more expensive to carry out.

1.8 DEFINITION

Harris (2006) stated that anti-forensic is a method used to prevent (or act against) the application of science to those criminal and civil laws that are enforced by police agencies in a criminal justice system.

Pajeket all (2012) defining the methodologies used against the computer forensics processes are collectively called Anti-Forensics.[69]

John Barbara defines anti-forensic as an approach to manipulate, erase, or obfuscate digital data or to make its examination difficult, time-consuming, or virtually impossible.

1.9 PRIMARY GOALS OF ANTI-FORENSICS

- Avoiding detection of the traces created by a certain incident.
- To make it hard or impossible to retrieve information.
- Increase the time of forensic examination.
- Casting doubt on a forensic report or testimony.
- Misguide the forensic investigator by producing false results.
- Intentional destruction of possible evidence.
- Create inaccuracy in forensic findings.

1.10 TYPES OF ANTI-FORENSIC TECHNIQUES

[69] Liu, V, & Brown, F. (2006, April 3). Bleeding-Edge Anti-Forensics.Presentation at InfoSec World 2006. Retrieved September 11, 2007, from <stachliu.com/files/InfoSecWorld_2006-K2-Bleeding_Edge_ AntiForensics.ppt>

In order to act against the forensics one has to have sound knowledge of cyber forensics. The basic stages involve in cyber forensics are identification, collection, preservation, analysis and presentation to make digital evidence admissible in a court of law. So, basically all kind of anti-forensic technique is trying to break in one of this stage.[70]

CREATING PROBLEMS AT THE EVIDENCE SOURCE

This technique is used to create more hurdles for a forensic investigator. It may result in time increased for analysis of the evidence. Sometimes this technique does not let computing device create any logs or the traces related to any event over the device. This technique also suggests permanent deletion of the information within the device. Following are some of the methods used to apply this technique

A. ***Disk Wiping* -** Data can be still recovered if it is a normal delete over computing device. Hence disk wiping technology is been used by an attacker to make data recovery more difficult task for the forensic investigator.

B. ***Disabling the log creating system software***- Disabling tool called as Event manager which is responsible for creation of source such as modified windows registry, logon user, computer setting, application software installation etc.

C. *Live CDs and Virtual Disks*-

Live CDs are an operating system distribution that boots and runs from a read-only device. Live CDs typically have a window system, web browser and SSH client, and run with virtual memory disabled.

D. ***Bootable USB tokens* -** These are similar to a Live CD except that the operating system is contained within an attachable USB device. These tokens can typically store more information thanCDs and allow information to be saved, generally via encryption.

[70] Metasploit LLC. (2007a). Metasploit Anti-forensics home page. Retrieved September 11, 2007, from <http://www.metasploit.com/projects/antiforensics/>

E. ***Virtual Machine-*** These are the "client" operating systems run inside a virtualization program such as VMWare Player, Parallels, or Microsoft Virtual PC.

F. ***Cloud Storage*** **-**In this method fraudster creates the anonymous account with different email service providers and keep the data on their cloud service which is entirely different computers. An attacker may also use some cloud services for launching an attack.

G. Live CDs are an operating system distribution that boots and runs from a read-only device. Live CDs typically have a window system, web browser and SSH client, and run with virtual memory disabled.

HIDING EVIDENCE

It mainly addresses the methods by which the data can be hidden inside the device or over transit. It makes cyber examination process more difficult. The more hurdles have been created when multiple data hiding techniques are clubbed together.[71]

A. ***Encryption-*** Encryption techniques transparently encrypt data when it is written to the disk and decrypt data when it is read back.
B. ***Steganography-***Steganography can be used to embed encrypted data in a cover text to avoid detection. This technique mainly used to embeds text in JPEG, MBP, MP3, WAV and other multimedia files.
C. ***Slack space-***Data can also be hidden in unallocated or otherwise unreachable locations that are ignored by the current generation of forensic tools.
D. Data can also be hidden in unallocated or otherwise unreachable locations that are ignored by the current
E. Generation of forensic tools

[71] Palmer, G (2001, November 6) A Road Map for Digital Forensics Research. Digital Forensic Research Workshop (DFRWS) Technical Report (DTR) T001-01 Final. Retrieved September 11, 2007, from <http://www.dfrws.org/2001/dfrws-rm-final.pdf>

F. ***HPA*** **-**Information can be stored in the Host Protected Area (HPA) and the Device Configuration Overlay (DCO) areas of modern ATA hard drives. Data in the HPA and DCO is not visible to the BIOS or operating system, although it can be extracted with special tools.

G. ***Program packers*** **-** Packers are commonly used by attackers so that attack tools will not be subject to reverse engineering or detection by scanning.

H. ***Onion Routing*** **-** It combines both approaches with multiple layers of encryption so that no intermediary knows both ends of the communication and the plaintext content.

DESTROYING EVIDENCE

This technique is used to make the evidence useless or unavailable. Evidence can be partly or completely destroyed.

A) ***Bad Sector-*** Attacker intentionally converts good sectors into bad sectors to make data recovery difficult in this scenario.

B) ***Disk degaussing-*** It is a process by which a magnetic field is applied to a digital media device. This may partially or permanently wipe the data within the disk.

COUNTERFEITING EVIDENCE

If computer criminal can found digital evidence he can create inconsistency in data retrieval, it will not credible enough to be presented in a court. Examples of this are timestamp modification and hash collision. Hence counterfeiting can be used to create fake evidence to mislead the forensic investigator.

a) OVERWRITING DATA

Overwriting programs typically operate in one of three modes:

- The program can overwrite the entire media.
- The program can attempt to overwrite individual files. This task is complicated by journaling file systems. The file itself may be overwritten, but portions may be left in the journal.
- The program can attempt to overwrite files that were previously “deleted” but left on the drive.

b) OVERWRITING METADATA

Meta Data is the extra relevant data created by files which may contain vital information. For example, it is frequently possible to determine which files the attacker accessed, by examining file "access" times for every file on the system. Metadata over wiring can confuse the investigator regarding the timeline analysis of the evidence.

c) ARTEFACT WIPING

The methods used in artefact wiping are tasked with permanently eliminating particular files or entire file systems. This can be accomplished through the use of a variety of methods that include disk cleaning utilities.

1.11 CONCLUSION

Sometimes, the process of deleting the evidence itself also create other evidence. Hence it's up to the persistent effort of the forensic investigator. Attacker sometimes ends up creating more traces while trying to use these anti-forensics techniques. Investigation of such expert criminals is very much possible. The golden rule here is not a single crime is full proof. The mistake is the part of human behaviour and criminals are no exception to this. Hence even though there are such techniques available forensics investigation achieve its goal and reveals the facts.

1.12 LET'S SUM UP

In this chapter, we have studied the meaning of digital evidence and the difference between physical and digital evidence. We also studied the detailed procedure of seizure proceedings by Investigation officer. Finally, we ended our discussion with the primary goals of anti-forensics and the different types of anti-forensics.

1.13 FURTHER READING

- https://www.academia.edu/26177741/Computer_Anti-forensics_Methods_and_Their_Impact_on_Computer_Forensic_Investigation
- Beer, Richard &Stander, Adrie& Van Belle, Jean-Paul. (2014). Anti-Forensic Tool Use and Their Impact on Digital Forensic Investigations: A South African Perspective.
- Conlan, Kevin &Baggili, Ibrahim &Breitinger, Frank. (2016). Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. Digital Investigation. 18. 10.1016/j.diin.2016.04.006.

➢ R. Harris, “Arriving at an anti-forensics consensus: examining how to define and control the anti-forensics problem,” Digital Investigation, vol. 3, pp. 44-49, 2006.

➢ C. S. J. Peron and M. Legary, “Digital anti-forensics: emerging trends in data transformation techniques,” in Proceedings of E-crime and Computer Evidence Conference, Technip, Monaco, 2005.

1.14 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What is digital evidence?

Digital evidence or electronic evidence is “any probative information stored or transmitted in digital form that a party to a court case may use at trial”.

2. What are the 2 sources of digital evidence?

- Volatile Evidence
- Non-Volatile Evidence

3. What is anti-forensics?

Anti-forensic is a method used to prevent (or act against) the application of science to those criminal and civil laws that are enforced by police agencies in a criminal justice system.

4. What are the primary goals of anti-forensics?

- Avoiding detection of the traces created by a certain incident.
- To make it hard or impossible to retrieve information.
- Increase the time of forensic examination.
- Casting doubt on a forensic report or testimony.
- Misguide the forensic investigator by producing false results.
- Intentional destruction of possible evidence.
- Create inaccuracy in forensic findings.

1.15 ACTIVITY

Explain the different types of anti-forensic techniques along with a case study in which one of the technique is used? (1000 words)

Unit 4: Network Investigations 4

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Overview of enterprise networks and protocols
- Collecting and interpreting network device configuration
- Forensic examination of network traffic

1.2 INTRODUCTION

Tracking down computer criminals generally requires digital investigators to follow the cybertrail between the crime scene and the offender's computer. The cybertrail can cross multiple networks and geographical boundaries, and can be comprised of many different kinds of digital evidence, including proxy and firewall logs, intrusion detection systems, and captured network traffic. Dialup server logs at the suspect's Internet Service Provider (ISP) may show that a specific IP address was assigned to the suspect's user account at the time. The ISP may also have Automatic Number Identification (ANI) logs—effectively Caller-ID—connecting the suspect's home telephone number to the dialup activity. Routers on the ISP network that connect the suspect's computer to the Internet may have associated NetFlow logs containing additional information about the network activities under investigation. Each of these logs would represent steps on the trail.[72]

Ideally, each step in the cybertrail can be reconstructed from one or more records from this evidence, enabling digital investigators to connect the dots between the crime scene and the offender's computer and establish the continuity of offense. If there is more than one type of evidence for a particular step, so much the better for correlation and corroboration purposes. Your reconstruction of events is like a scientific hypothesis. The more evidence you collect that is consistent with the hypothesis, the stronger the case for that hypothesis becomes.

Networks present investigators with a number of challenges. When the networks are involved in a crime, evidence is often distributed on many computers making a collection of all hardware or even the entire contents of a network unfeasible.

1.3 OVERVIEW OF ENTERPRISE NETWORKS

Digital investigators must be sufficiently familiar with network components found in a typical organization to identify, preserve, and interpret the key sources of digital evidence in an Enterprise. This chapter concentrates on digital evidence associated with routers, firewalls, authentication servers, network sniffers, Virtual Private Networks (VPNs), and Intrusion Detection Systems (IDS).

Logs generated by network security devices like firewalls and IDSs can be a valuable source of data in a network investigation. Access attempts blocked by a firewall or malicious activities

[72] Spiekermann, Daniel &Eggendorfer, Tobias (2017) Challenges of Network Forensic Investigation in Virtual Networks. Journal of Cyber Security and Mobility

detected by an IDS may be the first indication of a problem, alarming system administrators enough to report the activity to digital investigators.Routers form the core of any large network, directing packets to their destinations. Routers can be configured to log summary information about every network connection that passes through them, providing a bird's eye view of activities on a network. For example, suppose you find a keylogger on a Windows server, and you can determine when the program was installed. Examining the NetFlow logs relating to the compromised server for the time of interest can reveal the remote IP address used to download the keylogger. Furthermore, NetFlow logs could be searched for that remote IP address to determine which other systems in the Enterprise were accessed and may also contain the keylogger. As more organizations and ISPs collect NetFlowrecords from internal routers as well as those at their Internet borders, digital investigators will find it easier to reconstruct what occurred in a particular case.

Digital investigators may be able to obtain full network traffic captures, which are sometimes referred to as logging or packet capture, but are less like a log of activities than like a complete videotape of them—recorded network traffic islive, complete, and compelling. Replaying an individual's online activities as recorded in a full packet capture can give an otherwise intangible sequence of events a very tangible feel.[73]

1.4 OVERVIEW OF PROTOCOLS

To communicate on a network, computers must use the same protocol. For example, TCP/IP is the standard for computers to communicate across the Internet. The principle is fairly straightforward. Information is transmitted from a networked system in chunks called packets or datagrams. The chunks contain the data to be transferred along with the information needed to deliver them to their destination and to reconstruct the chunks into the original data. The extra information is added in layers when transmitted and stripped off in layers at the destination.[74] This layering effectively wraps or encapsulates control details around the data before they are sent to the next layer, providing modular functionality at each layer. One layer, for instance, is

[73] Spiekermann, Daniel & Keller, Jörg&Eggendorfer, Tobias(2017) Network forensic investigation in OpenFlow networks with ForCon. Digital Investigation

[74] Stevens, S W (1994) In TCP/IP Illustrated, Volume 1: The Protocols. Addison Wesley

used to specify the IP address of the destination system, and another layer is used to specify the destination application on that system by specifying the port being used by that application (there may be several ports on a server willing to receive data, and you don't want your request for a web page to end up in an SSH server). Bothof these layers will contain instructions for reconstructing the separated chunks, how to deal with delayed or out-of-order deliveries, and so forth.

To communicate with machines on different networks, computers must run higher-level protocols such as Internet Protocol (IP) at the network layer and Transport Control Protocol (TCP) at the transport layer.The Transmission Control Protocol (TCP) is a connection-mode service, often called a virtual-circuit service that enables transmission in a reliable, sequenced manner that is analogous to a telephone call. TCP differs from the User Datagram Protocol (UDP), which is connectionless, meaning that each datagram is treated as a self-contained unit rather than part of continuous transmission, anddelivery of each unit is not guaranteed—analogous to a postal letter. Both TCP and UDP use ports to keep track of the communication session.[75]

1.5 EVIDENCE PRESERVATION ON NETWORKS

There are some unique forensic challenges associated with preserving digital evidence on networks. Although some network-related data are stored on hard drives, more information is stored in the volatile memory of network devices for a short time or in-network cables for an instant. Even when collecting relatively static information such as firewall log files, it may not be feasible to shut down the system that contains these logs and then make a bitstream copy of the hard drive. The system may be a part of an organization's critical infrastructure and removing it from the network may cause more disruption or loss than the crime. Alternately, the storage capacity of the system may be prohibitively large to copy. So, how can evidence on a network be collected and documented in a way that demonstrates its authenticity, preserves its integrity and maintains the chain of custody?

[75] Davie, B and Gross, J (2016)A Stateless Transport Tunneling Protocol for Network Virtualization. Internet Draft, Informational: New York, NY

In the case of log files, it is relatively straightforward to make copies of the files, calculate their message digest values (or digitally sign them), and document their characteristics (e.g., name, location, size, MAC times). All this information can be useful for establishing the integrity of the data at a later date and digitally signing files is a good method of establishing chain of custody, provided only a few people have access to the signing key. A failure to take these basic precautions can compromise an investigation. In 2000, for example, an individual known as Maxus stole credit card numbers from the Internet retailer CD Universe and demanded a $100,000 ransom. When denied the money, he posted 25,000numbers on a web site. Employees from one or more of the computer security companies that handled the break-in inadvertently altered log files from the day of the attack—this failure to preserve the digital evidence eliminated the possibility of a prosecution.[76]

Networked systems can also contain crucial evidence in volatile memory, evidence that can be lost if the network cable is disconnected or the computer is turned off. For instance, active network connections can be used to determine the IP address of an attacker. Methods and tools for preserving volatile data on Windows and UNIX systems are covered in Malware Forensics.

In addition to preserving the integrity of digital evidence, it is advisable to seek and collect corroborating information from multiple, independent sources. Last but not least, when collecting evidence from a network, it is important to keep an inventory of all the evidence with as much information describing the evidence as possible (e.g., filenames, origin, creation times/dates, modification times/dates, a summary of contents). Although time-consuming, this process facilitates the pin-pointing of important items in the large volume of data common to investigations involving networks.

1.6 COLLECTING AND INTERPRETING NETWORK DEVICE CONFIGURATION

Network devices are generally configured with minimal internal logging to conserve storage space and for optimal performance. Some network device functions are so thoroughly engineered to optimize performance that they are not normally logged at all. Although these devices can be

[76] MosharafKabirChowdhury, N M, and Boutaba, R (2009) Network virtualization: state of the art and research challenges. IEEE Commun. Mag. 47, 20–26

configured to generate records of various kinds, the logs must be sent to a remote server for safekeeping because these devices do not contain permanent storage. Central syslog servers are commonly used to collect the log data.

In addition to generating useful logs, network devices can contain crucial evidence in volatile memory, evidence that can be lost if the network cable is disconnected or the device is shut down or rebooted. Routers are a prime example of this. Most routers are specialized devices with a CPU; ROM containing power-on self-test and bootstrap code; flash memory containing the operating system; nonvolatile RAM containing configuration information; and volatile RAM containing the routing tables, ARP cache, limited log information, and buffered packets when traffic is heavy.[77]

Routers are responsible for directing packets through a network to their destination and can be configured using Access Control Lists (ACLs) to make basicsecurity-related decisions, blocking or allowing packets based on simple criteria. For instance, some organizations implement simple egress and ingress filtering in their border routers (blocking outgoing packets that have source addresses other than their own, and blocking incoming packets that contain source addresses belonging to them). This simple concept—only data addressed from the organization should be allowed out—greatly limits a malicious individual's ability to conceal his location. In some cases, digital investigators must document how a router is configured and other data stored in memory.

1.7 VIRTUAL PRIVATE NETWORKS

Many organizations use Virtual Private Networks (VPN) to allow authorized individuals to connect securely to restricted network resources from a remote location using the public Internet infrastructure. For instance, an organization might use a VPN to enable travelling sales representatives to connect to financial systems that are not generally available from the Internet. Using a VPN, sales representatives could dial into the Internet as usual (using low cost, commodity Internet service providers) and then establish a secure, encrypted connection the

[77] Corey, V, Peterman, C, Shearin, S., Greenberg, M S, and Van Bokkelen, J (2002) Network forensics analysis. IEEE Int. Comput. 6, 60–66

organization’s network. A VPN essentially provides an encrypted tunnel through the public Internet, protecting all data that travels between the organization’s network and the sales representative’s computer.

Newer operating systems, including Windows 2000/XP/Vista, have integrated VPN capabilities, implementing protocols like Point to Point TunnelingProtocol (PPTP) and IPsec to establish VPN. Newer network security devices like the Cisco ASA and Juniper SA Series also support VPN services via SSL, enabling users to establish a virtual connection simply using a web browser.Digital investigators most commonly encounter VPN logs as a source of evidence associated with remote users accessing secured resources within the network from the Internet.

1.8 FORENSIC EXAMINATION OF NETWORK TRAFFIC

The contents of network traffic can be invaluable in a network investigation, because some evidence exists only inside packet captures. Many host-based applications do not keep detailed records of network transmissions, and so capturing network traffic may provide you with information that is not recorded on a host. Furthermore, captured network traffic can contain full packet contents, whereas devices like firewalls and routers will not. Even an IDS, which may record some packet contents, typically only does so for packets thatspecifically trigger a rule, whereas a sniffer can be used to capture all traffic based upon the requirements of the investigator.[78]

Extracting Statistical Information From Network Traffic

Whether you are approaching network traffic without any leads or you have some items like IP addresses that you can use to filter or search, you should examine the set of packets in a methodical manner to extract data of interest for your investigation.[79] Examples of data you might want to extract include:

- Statistics
- Alert data

[78] Hunt, R, and Zeadally, S (2012) Network forensics: an analysis of techniques, tools, and trends. IEEE Comput. 45, 36–43

[79] Jain, R, and Paul, S (2013). Network virtualization and software defined networking for cloud computing: a survey. IEEE Commun. Mag. 51, 24–31

- Web pages
- E-mails
- Chat records
- Files being transferred
- Voice conversations

Extracting Statistics

You can easily generate a set of statistics regarding a set of network traffic that may help to guide your investigation. Common statistics that you will find useful include:

- Protocol usage
- Network endpoints
- Conversations
- Traffic volumes

1.9 INTRUSION DETECTION SYSTEMS

In addition to programs that simply capture and display network traffic based on general rules, there are programs that monitor network traffic and bring attention only to suspicious activity. These programs are called Intrusion Detection Systems (IDS). Some of these systems such as Bro (www.bro-ids.org) can be configured to store all traffic and then examine it for known attacks and to archive significant features of network traffic for later analysis. Other systems such as Snort (www.snort.org) inspect the traffic and store only data that appear to be suspicious, ignoring anything that appears to be acceptable. These systems are not primarily concerned with preserving the authenticityand integrity of the data they collect, so additional measures must be taken when using these tools.[80]

Although they are not designed specifically for gathering evidence, logs from an IDS can be useful in the instance of an offender breaking into a computer. Criminals who break into computers often destroy evidence contained in log files on the compromised machine to make an investigator's job more difficult. However, an IDS keeps a log of attacks at the network level that investigators can use to determine the offender's IP address. For example, if fraud is committed

[80] Delgadillo, K (2015)Netflow services and applications. Cisco Whitepaper, 1996 (accessed November 5, 2015)

using a networked computer and investigators find that the computer was compromised and then scrubbed of all evidence, they may be able to determine which IP address was used by examining the log file from an IDS on the network.

While investigating a large-scale network intrusion, network traffic showed the intruder connecting to a compromised system and placing an unknown executable on the system via SMB. A subsequent forensic examination of the compromised computer revealed that the intruder had deleted the unknown executable and it could not be recovered from thehard drive. Although available tools for examining network traffic could not extract the file automatically, we were able to recover the unknown executable manually and examine it to determine its functionality. The information obtained from this executable helped advance the investigation in a variety of ways.

For example, A financial services company offered customers personalized web service to monitor their financial information, including credit ratings. Each customer had an account that could be verified for two levels of access, Tier 1 and Tier 2. The Tier 1 authentication would allow a customer to view commercially available information collected at the site. To view or to makechanges to their financial data, they needed a Tier 2 authentication, which required a different password and answers to some challenge questions.[81]

Web administrators would authenticate to both servers as well, but at Tier 2 their accounts had administrative access tothe web site and its databases and thus to everyone's financial information.During routine maintenance, several fixes to minor problems were implemented simultaneously. As a result of the interactions of these fixes, every account on the system had full administrative access to all the accounts at Tier 2.

The problem went undetected for several months until reported by one of the customers. The administrative accesswas not obvious and could be discovered only by trying to access someone else's financial information. It would not occur to most customers to try the experiment. Since it was one of the customers who discovered the problem, though, it obviously could happen.Forensic investigators were asked to analyze available logs covering the vulnerable

[81] Khan, S, Gani, A, Abdul Wahab, A W, Shiraz, M, and Ahmad, I (2015) Network forensics: review, taxonomy, and open challenges JNetwComputAppl 66, 214–235

period to determine whether it was likely that any customers had exploited the information of others.

1.10 LET' S SUM UP

In order to conduct an investigation involving computer networks, practitioners need to understand network architecture, be familiar with network devices and protocols, and have the ability to interpret the various network-level logs. Practitioners must also be able to search and combine large volumes of log data using search tools like Splunk or custom scripts. Perhaps most importantly, digital forensic analysts must be able to slice and dice network traffic using a variety of tools to extract the maximum information out of this valuable source of network-related digital evidence.

1.11 FURTHER READING

- Bunker, M., & Sullivan, B. (2000). CD Universe Evidence Compromised. MSNBC, June 7.
- Comer, D. E. (1995). Internetworking with TCP/IP Volume I: Principles, Protocols, and Architecture (Third Edition). Upper Saddle River, NJ: Prentice Hall.
- Villano, M. (2001). Computer Forensics: IT Autopsy, CIO Magazine, March (http://www.cio.com/article/30022/Computer_Forensics_IT_Autopsy).
- Plonka, D. (2000). FlowScan: A Network Traffic Flow Reporting and Visualization Tool. Usenix.
- Casey, E. (2004a). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press.

1.12 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) What are Intrusion Detection Systems?

In addition to programs that simply capture and display network traffic based on general rules, there are programs that monitor network traffic and bring attention only to suspicious activity. These programs are called Intrusion Detection Systems (IDS).

2) Short note on protocols?

To communicate on a network, computers must use the same protocol. Information is transmitted from a networked system in chunks called packets or datagrams. The chunks contain the data to be transferred along with the information needed to deliver them to their destination and to reconstruct the chunks into the original data. The extra information is added in layers when transmitted and stripped off in layers at the destination. This layering effectively wraps or encapsulates control details around the data before they are sent to the next layer, providing modular functionality at each layer.

3) How to generate statistics from a set of network traffic?

You can easily generate a set of statistics regarding a set of network traffic that may help to guide your investigation. Common statistics that you will find useful include:

- Protocol usage
- Network endpoints
- Conversations
- Traffic volumes

1.13 ACTIVITY

Explain briefly about Network investigations along with how networks are used in the forensic examination? Write a relevant case study pertaining to network traffic and examination? (800-1000 words)

Block 3
Role and Analysis of Cyber Forensics

Unit 1: Computer Forensics and Its Significance

1

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- The relevance of cyber forensics
- The concept of cyber forensics
- The various tools used in the implementation of cyber forensics

1.2 INTRODUCTION

The concept of cyber forensics is relatively new in India. The advent of high-speed broadband and mobile internet network at affordable rates has made internet highly accessible to people. However, the improving infrastructure has also contributed to a rise in cyber crimes in India.[82]Cyber forensic is the tool which is employed to detect cybercrimes and to prevent cybercrimes before the crime is committed.

1.3 RELEVANCE OF CYBER FORENSICS

In the case of traditional crimes, the investigating agency visits the crimes scene and collects evidence through various means such as collecting various objects of interest from the crime scene, interacting with the witnesses to the crime, etc. Thus, there is a sense of tangibility to a crime which takes place in the physical world.

However, in the case of cyber crime, the said act is devoid of the same sense of physicality. Since a cybercrime takes place using a computer or such other devices from a remote location, the methods used to detect a traditional crime cannot be employed. One must also remember that since a majority of people are not as well versed with cyberspace, i.e. the notional environment in which communication over computer networks take place, detecting cyber crimes is way more difficult than that of traditional crimes.

Using cyber forensics, the investigating agency is able to gather the evidence pertaining to the commission of cybercrime, including the identity of the perpetrator. The chief objective of cyber forensics is to obtain evidence using various techniques which can be used to make a case before the court of law. A number of cyber crimes such as phishing, hacking, fraud, cyber espionage, cyber terrorism are investigated with the help of cyber forensics. It can be said that without employing the necessary measures afforded by cyber forensics, a number of crimes would have remained unproved and inconclusive.[83]

An important example of the effectiveness of cyber forensics is the BTK serial killer case. From 1974 to 1991 a number of murders took place in Kansas, the United States of America which

[82] Armstrong, I (2002) Computer Forensics Detecting the Imprint. SC Magazine

[83] Sadiku, Matthew &Tembely, Mahamadou& Musa, Sarhan.(2017) Digital Forensics. International Journal of Advanced Research in Computer Science and Software Engineering

were suspected to have been committed by a serial killer. However, the investigating authorities were unable to find the culprit behind the killings. In 2004, the investigating agencies started receiving a number of communications from the perpetrator. Some of these communications were sent on a floppy drive. On examination of the floppy disk by cyber forensic experts, it was found that a Microsoft Word document had been deleted from the floppy drive. By analysing the metadata related to the Word document, the investigating agency were able to determine the identity of the perpetrator and the said evidence was considered by the courts while finding Dennis Rader guilty of committing the murders.

1.4 THE CONCEPT OF CYBER FORENSICS

In order to connect to the cyberspace, a user requires to connect to the internet through an Internet Service Provider (ISP). In order to connect to the internet, a user utilises a dial up connection / broadband connection or a mobile network.[84] Thus, in order to obtain evidence, an investigation agency can gather evidence from the following sources:

- The user's computer;
- The servers of the ISP used by the user

Computers maintain data related to the files used by the user in the form of logs. Even if the data is deleted, the logs related to such data is stored in the hard drive through swap files, memory dumps and other unallocated spaces in the hard drive.

Further, when accessing websites, the information is cached in the machine accessing the website. The Oxford Learners Dictionary defines a "cache" as a part of computer's memory that stores copies of data that is often needed while a program is running. "Caching" stores the data related to the web page on the hard drive of the computer.

ISPs maintain logs of the websites visited by users availing internet services through its portals including the IP address and machine ID (Mac ID) of the user.

Using various techniques of cyber forensics, an investigation agency can gather evidence to prove that a machine has been used by the user to commit a cyber crime.

[84] Mandia, Prosise, Pepe Incident Response & Computer Forensics Second Edition. McGraw-Hill 2003

1.5 VARIOUS TOOLS OF CYBER FORENSICS

Before dealing with the various techniques of cyber forensics, it is pertinent to discuss the legal framework.[85]

Section 76 in The Information Technology Act, 2000 ("**IT Act**") deals with confiscation of data.[86]

> ***76. Confiscation***.*-Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made thereunder has been or is being contravened, shall be liable to confiscation:*
>
> *Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made thereunder, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorised by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made thereunder as it may think fit.*

Further Section 77A of the IT Act provides for compounding of offences committed under the IT Act.

> ***77A. Compounding of Offences****- (1) A Court of competent jurisdiction may compound offences other than offences for which the punishment for life or imprisonment for a term exceeding three years has been provided under this Act.*

[85] US Department of Justice Computer Crime and Intellectual Property Section, Criminal Division. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. July 2002 NIJ Electronic Crime Scene Investigation – A Guide for First Responders 2001. NHTCU Good Practice Guide for Computer Based Electronic Evidence 2003

[86] IT Act: Offences (Section 65 to 78)
<https://informationtechnologyactindia.blogspot.com/p/offences-section-65-to.html>

Provided that the Court shall not compound such offence where the accused is by reason of his previous conviction, liable to either enhanced punishment or to a punishment of a different kind.

Provided further that the Court shall not compound any offence where such offence affects the socio-economic conditions of the country or has been committed against a child below the age of 18 years or a woman.

(2) The person accused of an offence under this act may file an application for compounding in the court in which offence is pending for trial and the provisions of section 265 B and 265 C of Code of Criminal Procedures, 1973 shall apply.

Section 265B, Code of Criminal Procedure, 1973

265B. Application for plea bargaining *-A person accused of an offence may file an application for plea bargaining in the Court in which such offence is pending for trial.*

The application under Sub-Section (1) shall contain a brief description of the case relating to which the application is filed including the offence to which the case relates and shall be accompanied by an affidavit sworn by the accused stating therein that he has voluntarily preferred, after understanding the nature and extent of punishment provided under the law for the offence, the plea bargaining in his case and that he has not previously been convicted by a Court in a case in which he had been charged with the same offence.

After receiving the application under Sub-Section (1), the Court shall issue a notice to the Public Prosecutor or the complainant of the case, as the case may be, and to the accused to appear on the date fixed for the case.

When the Public Prosecutor or the complainant of the case, as the case may be, and the accused appear on the date fixed under Sub-Section (3), the Court shall examine the accused in camera, where the other party in the case shall not be present, to satisfy itself that the accused has filed the application voluntarily and where-

the Court is satisfied that the application has been filed by the accused voluntarily, it shall provide time to the Public Prosecutor or the complainant of the case, as the case *may be, and the accused to work out a mutually satisfactory disposition of the case which may include giving to the victim by the accused the compensation and other expenses during the case and thereafter fix the date for further hearing of the case;*

the Court finds that the application has been filed involuntarily by the accused or he has previously been convicted by a Court in a case in which he had been charged with the same offence; it shall proceed further in accordance with the provisions of this Code from the stage such application has been filed under Sub-Section (1).

Section 265C of Criminal Procedure Code, 1973

S. 265C Guidelines for mutually satisfactory disposition In working out a mutually satisfactory disposition under clause (a) of Sub-Section (4) of section 265B, the Court shall follow the following procedure, namely;

in a case instituted on a police report, the Court shall issue a notice to the Public Prosecutor, the police officer who has investigated the case, the accused and the victim of the case to participate in the meeting to work out a satisfactory disposition of the case;

Provided that throughout such process of working out a satisfactory disposition of the case, it shall be the duty of the Court to ensure that the entire process is completed voluntarily by the parties participating in the meeting;

Provided further that the accused may, if he so desires, participate in such meeting with his pleader, if any, engaged in the case;

in a case instituted otherwise than on police report, the Court shall issue a notice to the accused and the victim of the case to participate in a meeting to work out a satisfactory disposition of the case;

Provided that it shall be the duty of the Court to ensure, throughout such process of working out a satisfactory disposition of the case, that it is completed voluntarily by the parties participating in the meeting;

Provided further that if the victim of the case or the accused, as the case may be, so desires, he may participate in such meeting with his pleader engaged in the case.

To give effect to the content addressed through such aforementioned provisions of the legal framework in the country, there are various techniques implemented that act as tools. Such tools are majorly used for collecting digital evidence related to various limbs of cyberlaw such as disk forensics, network forensics, device forensics, live forensics, enterprise forensics, photo forensics and virtualized environment forensics.

Disk Forensics Tool aims at addressing concerns arising in association with data recovery, data analysis, tracking senders of emails, analysing forensic registry, extracting forensic thumbnail, etc.

Network Forensics Tool aims at addressing concerns arising in association with analysis of forensic log, tracing sender of emails, analysing network sessions, etc.

Mobile Device Forensics Tool aims at addressing concerns arising in association with the acquisition of software, analysis of mobile phones and smartphones, analysis of mobile devices, analysis of call data records of various service providers, creation of forensic solution for imaging, analysis of sim cards, etc.[87]

Live Forensics Tool aims at addressing concerns arising in association with arriving at software solutions related to acquisition and analysis of volatile data in systems.

Tools of cyber forensics are used and implemented to extract digital evidence that can be used and admitted in courts of law. Since electronic evidence plays a vital and pivotal role in cybercrimes, tools of cyber forensics act as the basis of digital media by allowing anti-forensic techniques to be countered.

The most useful tool used in cyber forensics is the Digital Evidence Search Kit (DESK), which is a machine that law enforcement agents; it further involves the use of a subject machine, which is the device used by the suspect. These two machines communicate with each other using a serial. The DESK system searches for and identifies the keywords in Chinese and/or English using a text pattern file, to locate the words searched for on the subject machine. The DESK function

[87] Bynum, T. (2001) Computer Ethics: Basic Concepts and Historical Overview Stanford Encyclopedia of Philosophy Retrieved 12 January 2007 from
<http:// plato.stanford.edu/archives/win2001/entries/ethics-computer/>

further uses the hash value database that contains fingerprints of certain systems of the file so as to enable verification of file integrity.

The DESK function involves three types of searches:

a Physical Search – This involves performing a search of patterns of individual physicalsectors in the storage of the subject machine. Owing to such physical search, evidence of cybercrime stored in unused sectors can be discovered with ease. It further allows locating files independent of the specific file systems.

b Logical Search – This kind of search involves making use of information regarding the file system concerned. A file, which is conceptually a sequence of bytes, is placed in portions of the sequence into different sectors by the file system, in accordance with the logical continuity of the contents thereof.

c Deleted File Search – File deletion, in most file systems, is accomplished by way of modifying only a few bytes of the file system, thereby allowing the content of a deleted file to subsist in the storage system, unless overwritten. Therefore, patterns in deleted files can be traced back until the time that the disk sectors are overwritten by other new files.

1.6 CONCLUSION

Digital forensics is a rapidly advancing field that has many challenges and crosswinds. The opportunities are endless, but they are not for the faint of heart. Frustration is a common partner, so the ability and mentality to press on through is a key characteristic an investigator should have. Someone who needs to be shown how to do everything may want to rethink their career options. A can-do attitude is essential, but the investigator does not need to go it alone. A variety of resources are available to assist, and most of the investigators who have worked through the learning curve to achieve competence are more than eager to help others do the same. Usually, they had others to lean on, so once you reach a level of expertise with the assistance of others, do not forget to return the favor.

1.7 LET'S SUM UP

In this chapter, we studied the significance of computer forensics and its relevancy. We discussed the concept of cyber forensics and finally, ended the discussion with various tools used in cyber forensics and provisions pertaining to it under the Information Technology Act.

1.8 FURTHER READING

- Bell, G., and Boddington, R. (2010). Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery? The Journal of Digital Forensics, Security and Law, Vol 5(3).
- De Forest, P. R., Gaensslen, R. E., and Lee, H. C. (1983). Forensic Science: An Introduction to Criminalistics, McGraw-Hill, New York.
- Menn, J. (2010). Fatal System Error: The Hunt for the New Crime Lords Who Are Bringing Down the Internet, PublicAffairs, New York.
- Gogolin, G. (2010). The Digital Crime Tsunami. Digital Investigation, Vol. 7(1-2).
- Kind, S., and Overman, M. (1972). Science against Crime, Aldus Books, London, UK

1.9 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) **What is the meaning of cyber forensic?**

Cyber forensic is the tool which is employed to detect cybercrimes and to prevent cybercrimes before the crime is committed.

2) **What are the methods/sources that need to be used to obtain evidence in cyber forensic?**

In order to obtain evidence, an investigation agency can gather evidence from the following sources:

- The user's computer;
- The servers of the ISP used by the user

3) **What is the most important tool in cyber forensic?**

The most useful tool used in cyber forensics is the Digital Evidence Search Kit (DESK), which is a machine that law enforcement agents; it further involves the use of a subject machine, which is the device used by the suspect.

4) **What are the 3 types of searches under desk function?**

The DESK function involves three types of searches:

a Physical Search
b Logical Search
c Deleted File Search

1.10 ACTIVITY

Explain the concept and relevancy of cyber forensics in the present era, along with the various tools that are used to gather evidence and relevant provisions under the I.T. Act? (800-1000 words)

Unit 2: Windows Forensics Analysis 2

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- The process of Windows XP, Vista etc under forensics
- Forensic analysis of the NTFS Master file table
- Data access control and file deletion

1.2 INTRODUCTION

Despite the proliferation and growing popularity of other user interfaces, such as Macintosh OS X and Ubuntu (a flavor of Linux), Microsoft's Windows operating systems remain the most popular in the world. Sources have reported that over 90% of the computers in use today are running some version of the Windows operating system.1 This is not surprising given the almost endless variation that can be found in Windows products, their relative ease of use for the average computer owner, and the virtual stranglehold on marketing Microsoft has enjoyed for so many years (particularly before recent inroads by a resurgent Apple, Inc.). Microsoft operating systems have even found an audience in non-traditional quarters, as scores of Macintosh users have learned to use products like Apple's Boot Camp or Parallels virtualization software to run Windows on their Intel-based Macintosh hardware. Private users, Fortune 500 companies, and government agencies alike all overwhelmingly have chosen Windows systems as their primary technology infrastructures.[88]

In light of this, it should not be surprising that the majority of systemsthat digital investigators will be called upon to examine will be running a Windows operating system. The ease of use of Windows appeals to criminals and "evil-doers" the same as it does to the grandmother downthe street. And both the longevity and popularity of Windows have made it a favorite target of virus authors, hackers, and industrial saboteurs. So, whether investigating child pornography, intellectual property theft, or Internet Relay Chat (IRC) botinfection, it is a safe bet that knowledge of Windows operating systems, and its associated artifacts, will aid investigators in their task.

1.3 WINDOWS XP

Windows XP has been a standard Microsoft OS for workstations for years. Since it hit the scene in 2001, millions of Windows users have grown comfortable with its user-friendly interface,

[88] Brill, A (2006b) The Brill files: An investigative report on data wiping utilities—Part two. Kroll Ontrack Newsletter, 4(6). Available online at <www.krollontrack.com/ newsletters/cccfn_0606.html>

comparatively efficient operation, and improvements over previous versions such as Windows 2000 and Windows ME. Windows XP comes in three primary editions (i.e., Home, Media Center, and Professional), which were targeted at different parts of Microsoft's work-station computing customers. From a file system standpoint, XP continues to run on top of the File Allocation Table (FAT) and New Technology File System (NTFS) structures with which examiners have grown familiar.[89]

There are many features in Windows XP that can be very useful for forensic examiners. Evidence of user actions is often recorded in areas (such as Internet history, Event logs, Prefetch files, thumbs.db files, and link files) that are easy to view for the trained digital investigator with the right tool. However, other challenges (such as analyzing restore points, analysis of data in the Windows registry, collection and analysis of memory, dealing with RAIDs and dynamic disks, overcoming Windows encryption, and documenting data destruction) can present a much greater challenge, even for more experienced digital investigators. Regardless of its utility, Microsoft stopped selling XP in 2008 but plans to continue support for this beloved Windows version until 2014, which means it will most likely be a big part of examiners' lives for many years to come.[90]

1.4 WINDOWS VISTA (AND RELATED SYSTEMS)

Windows Vista, which many still remember under its development code name of "Longhorn," was officially released in 2007 and, like XP before it, was intended by Microsoft to become the de facto OS for workstations. Vista, like XP (and the upcoming Windows 7), is available in multiple editions(i.e., Starter, Home Basic and Basic N, Home Premium, Business and Business N, Enterprise, and Ultimate), each with its capabilities and features; for example, Vista Home allows users to back up documents, and Vista Enterprise allows the creation of true-clone copies of the entire hard disk/partitions for later recovery or creation of identical systems.[91]

[89] Geiger, M (2005). Evaluating commercial counter-forensic software.In Proceedings of DFRWS 2005. Available online at <www.dfrws.org/2005/proceedings/geiger_ counterforensics_slides.pdf>

[90]Grand, J, & Carrier, B (2004) A hardware-based memory acquisition procedure for digital investigations.Journal of Digital Investigation, 1(1), 1742–2876. Available online at <www.digitalevidence.org/papers/tribble-preprint.pdf>

[91]Hargreaves, C, Chivers, H, &Titheridge, D (2008) Windows Vista and digital investigations. Digital Investigation Journal, 5(1–2), 34–48

Also similar to XP, Vista, 2k8, and 7 take advantage of the NTFS file system and add the concept of Transactional NTFS (TxF). Implemented together with the Kernel Transaction Manager (KTM), TxFwas designed to make NTFS more robust by treating file operations as transactions that can be rolled back or reapplied as necessary in the case of catastrophic system failure.[92] Most of Microsoft's official literature suggests that Vista cannot be installed and run on FAT32. However, although this may be true from a simplistic or tech support stand-point, there are several tips and tweaks that will allow Vista to be installed on a FAT32 partition, so it is possible the digital investigator could encounter such a scenario. Before Vista was released, it was thought it would be based on a new file system (WinFS) under development by Microsoft. However, shortly before Vista's release, problems in development caused Microsoft to shelve the new file system temporarily, leaving Vista to utilize NTFS as its primary base.

1.5 OVERVIEW OF NTFS

While the world waits for WinFS, most modern Windows workstations and servers are using the much more familiar NTFS. NTFS is an alternative to FAT file systems (e.g., FAT12, FAT16, FAT32) and can be utilized by Windows NT/2k/XP/2k3/Vista/2k8 operating systems. The current version is NTFS 3.1, which has been used in Windows XP and later OS releases. Among improvements in NTFS file systems are increased file size potential (roughly 16TB versus 4GB for FAT32), increased volume size potential (roughly 256TB versus 2TB for FAT32), and the recording of Last Accessed times (in Windows NT/2k/XP/2k3, and Vista/2k8/7 if enabled). In addition, NTFS uses a data structure called the Master File Table (MFT) and entries called index attributes instead of a file allocation table (FAT) and folder entries in order to make the access and organization of data more efficient. These and other key features of NTFS of interest to forensic examiners are covered in this section.[93]

The primary internal files that NTFS uses to track data sometimes referred to as metadata files. The presence of these internal files on a system being examined (or traces of these files in unallocated space) should indicate to an examiner that the system was formatted as NTFS.It

[92] Kessler, M. (2007).Maintaining Windows 2000 peak performance through defragmentation. Microsoft Technet. Available online at <http://technet.microsoft.com/en-us/library/ bb742585.aspx>

[93] Lee, R (2008) VISTA shadow volume forensics.SANS Computer Forensics and E-Discovery Blog. Available online at <http://sansforensics.wordpress.com/2008/10/10/shadowforensics/>

general, the dates and times associated with these files are set when the files are first created on the volume and do not change over time with the use of the system. As such, the dates and times of these internal files (particularly the Created Date) can be used as an indication of when the volume was last formatted as NTFS. All of these files have their function and can be analyzed to the nth degree, but a few of them can be very useful to the investigator.

In ***Johnson vs Wells Fargo,***[94] a U.S. District Court in Nevada heard a motion on behalf of a defendant alleging that the plaintiff in the case reformatted two hard disk drives possibly containing evidence that the plaintiff falsified documentation to support his claims. The defendant informed the plaintiff of the intent to compel production of the hard disk drives in September 2007; however, the defendant's "forensic computer expert" (the label applied to the defendant's digital investigator in court filings)concluded, upon examination of the system files on the reformatted hard disk drives, that one of the drives was reformatted a mere five days after the plaintiff was notified that he would be compelled to produce it, and the second drive was reformatted only 10 days later. As a result, the Court found that the plaintiff destroyed potential evidence, and a jury instruction adverse to the plaintiff was ordered in the case as a result of his actions.

1.6 DATA ACCESS CONTROL

One of the key features of NTFS is its increased security over FAT file systems. This security manifests itself in many ways, but perhaps the most noticeable is an access control list (ACL) that governs read-write-execute access to Windows files and folders.[95] Security descriptors stored in the $Secure file, an internal NTFS file that is three data streams, details ownership and access information for files and folders on the file system. This ownership and access information is often quite important to an examiner attempting to determine who had accessto (or who is responsible for) a particular data object. For example, an examiner seeking a clue as to which user account was used to download a particular pornographic picture usually need only look at the picture's owner in NTFS.

[94] *Johnson v Wells Fargo* 635 F 3d 401 (9th Cir) [2011]

[95] Malin, C, Casey, E, &Aquilina, J (2008) Malware forensics Syngress Media

Although these ownership and access values in the $Secure file can be interpreted manually, it is fairly complex and requires data from several different internal NTFS files, so it is far easier for examiners to use a third-party tool.

1.7 FORENSIC ANALYSIS OF THE NTFS MASTER FILE TABLE (MFT)

$MFT RECORD BASICS

Each MFT record has its data structure, to include slack that occurs between the end of the last attribute in the record and the beginning of the subsequent MFT record. Decoding the data in the records can sometimes be tricky, and is normally handled by a forensic tool, but it can be done by hand in the absence of one of these tools or for validation purposes.[96]

In addition to data such as the file status flag described earlier, which resides in each record header (normally the first 56 bytes of the record in XP and later), MFT records are composed of attributes that each have a specific function and structure. Each attribute has its header, which (among other things) identifies the attribute and gives the size of the attribute. It is also useful to understand that these attributes can be resident (meaning, they exist within a given MFT record) or nonresident (meaning, they exist outside a given MFT record, elsewhere on the disk, and are referenced within the record). Among these attributes, the Standard Information Attribute (SIA), Filename Attribute (FNA), and Data Attribute can be most helpful from a forensic perspective.

DATA-TIME STAMP DIFFERENCES BETWEEN NTFS AND FAT

NTFS date-time stamps differ from those recorded on FAT systems in several key ways. First, it is important to note that NTFS and FAT date-time stamps do not reside in the same locations; whereas NTFS uses the $MFT as a primary repository for date and time metadata, FAT systems record dates and times within folder entries. Another major difference is that NTFS date-time stamps are recorded in UTC, regardless of the time zone set for the system, whereas FAT date-time stamps are recorded in local time; this distinction is important, particularly when interpreting the date-time stamps manually. In addition, NTFS represents date-time stamps using the FILETIME format, which represents the number of 100 nanosecond intervals since January

[96] Mueller, L. (2009). Detecting timestamp changing utilities.Professional Blog. Available online at <http://www.forensickb.com/2009/02/detecting-timestamp-changingutlities.html>

1, 1601, and can be interpreted by most forensic tools, including free tools such as DCode by Digital Detective.[97]

The FILETIME format is different from the DOSDATETIME that is primarily used in FAT, which is 4 bytes and starts onJanuary 1, 1980. To confuse matters, on FAT systems the resolution of create time on FAT is 10 milliseconds (additional bytes are used to record hundredths of a second), whereas write time has a resolution of 2 seconds, and access time has a resolution of 1 day, allowing the examiner to be less specific about when a file or folder was last accessed on the file system (Microsoft, 2009a). Even within NTFS, the use of Last Accessed date-stamps can vary. For example, NTFS delays updates to the last access date-time stamps by up to 1 hour after the last access (Microsoft, 2009a).

DATA ATTRIBUTE

An MFT record's Data Attribute can be very important to examiners, chiefly because it contains either the actual data itself (resident) or a pointer to where the data resides on the disk (nonresident). A resident Data Attribute contains the actual data of the file referenced by the MFT record; this occurs when the data the file contains is relatively small in size (usually less than 600 bytes), so small text files (such as boot.ini or Internet cookies) are often held as resident files. For larger files, the MFT contains a list of the clusters allocated to that file, called data runs.

1.8 NTFS FILE DELETION

In the same vein, it is quickly worth mentioning what happens in NTFS when a file is deleted (as opposed to being sent to the Recycle Bin). When a file is deleted in NTFS, many different things happen "under the hood," but among the observable behaviors important to examiners are:

- The deleted file's entry is removed from its parent index, and the file system metadata (i.e., Last Written, Last Accessed, Entry Modified) for the file's parent folder are updated. It is also possible that the metadata for the deleted file itself may be updated because of how the user interacted with the file to delete it (e.g., right-click on the file).

[97] Park, B, Park, J, & Lee, S. (2008). Data concealment and detection in Microsoft Office 2007 files Journal of Digital Investigation, 5(3–4), 104–114

However, examiners should exercise caution before drawing any conclusions from the metadata of a deleted file without other supporting, or related evidence found elsewhere on the file system.

- The two bytes located at record offset 22 within the file's MFT record are changed from \x01\x00 (allocated file) to \x00\x00 (unallocated file).
- The appropriate locations in $Bitmap are modified to show that both the space occupied by the MFT record and space previously occupied by the file itself is now unallocated and ready for reuse.

A recent investigation focused on a government server, which was found to be beaconing out to another country. The start date of the beaconing traffic gave investigators an approximate date for the compromise of the victim machine, as they began developing their timeline. However, during the forensic examination of the compromised system, the source of the beaconing was found to be a piece of malware (keylogger) whose File Created date-time stamp (as displayed by several different forensic tools) predated the beginning of the beaconing by almost two years.[98] Investigators began to wonderif the system had been compromised much earlier than they originally thought. But, upon more detailed examination of the file's MFT record, and manual translation of the dates and times held in the FNA for the malware and associated files, investigators confirmed that the malware had most likely been created on the system at a date and time that very nearly matched the start of the beaconing traffic, confirming their original timeline. This discovery led to suspicion of SIA date-time stamp alteration on the part of the intruder and the location of a date-time stamp modification utility.

Evidence of file deletion (as opposed to destruction/wiping) by a particular user presents its own set of challenges, particularly since no specific program or utility is required to delete a file in Windows. Simply sending a file to the Recycle Bin is not (by the most common forensic definition) actual deletion of the file; however, a user sending a file to the Recycle Bin is often viewed as legally significant in a case where the user was supposed to be preserving or protecting data. Further, a file in the Recycle Bin is usually easy to identify, and data provided by INFO2 records or $I files (Vista/7 Recycle Bin operation) can help the investigator pinpoint

[98] Parsonage, H (2008).The forensic recovery of instant messages from MSN Messenger and Windows Live Messenger. Available online at <http://computerforensics.parsonage. co.uk/downloads/MSNandLiveMessengerArtefactsOfConversations.pdf>

where the file was when it was deleted, as well as when the data was sent to the Bin and by which user account. Even if the Recycle Bin is empty, looking at the Last Written date-time stamp on the associated INFO2 record can provide the investigator with valuable data about the approximate time the Recycle Bin was cleared.

Forensic examiners can often recover data and associated metadata for deleted files, even when Recycle Bin information is not available. In particular, when dealing with NTFS, a recovered MFT entry can provide all the information a forensic examiner needs about deleted data. For digital investigators, knowing the mechanics is often a far cry from knowing who deleted the file and when. Most forensic suites have the ability to identify deleted and partially overwritten files, distinguishing them via different icons or information in the files' descriptions.

DETERMINING TIME OF DELETION

A common mistake that forensic examiners can make is to assume that the Last Accessed date-time stamps of deleted files show when the files were deleted. Although it may seem logical in theory that a file would be accessed at the time, it was deleted, this is not always true. For instance, deleting an entire folder does not update the Last Accessed date-time stamp of the files it contains (try it!). As another example, when a user causesInternet Explorer to clear the Temporary Internet Files (e.g., Tools→Delete Browsing History…→Delete Files…, in Internet Explorer 7), it does not update the Last Accessed dates of the files. Without other supporting evidence, the only statement an examiner can safely make about a deleted file based solely on its Last Accessed date-time stamp is that it was not deleted prior to the date indicated by that piece of metadata.[99]

Determining who deleted the file can be even more difficult and often has to be obliquely proven by attempting to correlate system usage data (such as logged on users, etc.) with the last date-time stamps on the deleted file. A determination regarding who deleted a file can also be circumstantially supported by file permissions data (file owner, who has deletion rights, etc.), clues from the location of the deleted file (e.g., c:\Documents and Settings\<username>\My Documents), and link files and MRU registry data that pointed to the data in its active state, but

[99] Mueller, L (2008) Incident response—Recovering a BitLocker recovery password before system shutdown. Professional Blog Available online at <www.forensickb.com/2008/01/ incident-response-recovering-bitlocker.html>

the investigator must correlate and weigh each piece of evidence carefully before opining on the source of a file's deletion.

1.9 LET'S SUM UP

In this chapter, we studied the concept of Windows XP, Vista etc and the process of forensics with respect to it. We also discussed the new technology file system and data access control. Finally, we ended the discussion with forensic analysis of the NTFS MFT and the process of file deletion.

1.10 FURTHER READING

- Carrier, B. (2005). File system forensic analysis. Addison-Wesley.
- Dickson M. (2006). An examination into MSN Messenger 7.5 contact identification. Journal of Digital Investigation, 3(2), 79–83.
- Carvey, H. (2009). Windows forensic analysis (2nd ed.). Syngress Media.
- Geiger, M. (2005). Evaluating commercial counter-forensic software. In Proceedings of DFRWS 2005. Available online at www.dfrws.org/2005/proceedings/geiger_counterforensics_slides.pdf
- Hargreaves, C., Chivers, H., &Titheridge, D. (2008). Windows Vista and digital investigations. Digital Investigation Journal, 5(1–2), 34–48.

1.11 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) How are the evidence gathered by the examiners in Windows XP?

There are many features in Windows XP that can be very useful for forensic examiners. Evidence of user actions is often recorded in areas (such as Internet history, Event logs, Prefetch files, thumbs.db files, and link files) that are easy to view for the trained digital investigator with the right tool.

2) What is the key feature of NTFS?

One of the key features of NTFS is its increased security over FAT file systems. This security manifests itself in many ways, but perhaps the most noticeable is an access control list (ACL) that governs read-write-execute access to Windows files and folders. Security descriptors stored in the $Secure file, an internal NTFS file that is three data streams, details ownership and access information for files and folders on the file system.

3) What is the process post deletion of files in NTFS?

When a file is deleted in NTFS, many different things happen “under the hood,” but among the observable behaviors important to examiners are:

- The deleted file’s entry is removed from its parent index, and the file system metadata (i.e., Last Written, Last Accessed, Entry Modified) for the file’s parent folder are updated. It is also possible that the metadata for the deleted file itself may be updated because of how the user interacted with the file in order to delete it (e.g., right-click on the file). However, examiners should exercise caution before drawing any conclusions from the metadata of a deleted file without other supporting, or related evidence found elsewhere on the file system.
- The two bytes located at record offset 22 within the file’s MFT record are changed from \x01\x00 (allocated file) to \x00\x00 (unallocated file).
- The appropriate locations in $Bitmap are modified to show that both the space occupied by the MFT record and space previously occupied by the file itself sis now unallocated and ready for reuse.

1.12 ACTIVITY

Explain the concept of forensic analysis in Windows XP, Vista and 7 along with the process of deletion of files in NTFS and the process of post deletion? Briefly explain the same with a relevant case study in the present era? (1000 words)

Unit 3: Data Recovery Function Testing For Digital Forensic Tools

3

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Data recovery function mapping
- Validation and verification framework
- Recovered objects and reference set development and testing

1.2 INTRODUCTION

Many digital forensic tools used by investigators were not originally designed for forensic applications. Even in the case of tools created with the forensic process in mind, there is the issue of assuring their reliability and dependability. Given the nature of investigations and the fact that the data collected and analyzed by the tools must be presented as evidence, it is important that digital forensic tools be validated and verified before they are deployed.Digital forensics is the process of identifying, preserving, analysing and presenting digital evidence in a manner that is acceptable in court-room proceedings.

1.3 VALIDATION AND VERIFICATION FRAMEWORK

Our validation and verification framework is function-oriented and incorporates detailed specifications that are absent in other work. The methodology begins with a systematic description of the digital forensic field using a formal model and function mapping. Digital forensiccomponents and processes are defined in this model , and fundamentalfunctions in the investigative process such as searching, data preservation andfile identification are specified (i.e., mapped). Having developed the model and function mapping, the validation and verification of a digital forensic tool is accomplished by specifying its requirements for each mapped function. Next, a reference set is developed comprising a test case (or scenario) corresponding to each functional requirement. The reference set enables the forensic tool and/or its functions to be validated and verified independently.When a tool is tested, a set of metrics can also be derived to determine the fundamental scientific measurements of accuracy and precision.[100] In summary, if the discipline is mapped in terms of functions (and their specifications) and, for each function, the expected results are identified and mapped as a reference set, then any tool, regardless of its original design intention, can be validated against known elements. The function-oriented validation and verification regime has severaldistinctive features such as detachability, extensibility, tool version neutrality and transparency.

[100] J Beckett and J. Slay, Digital forensics: Validation and verification in a dynamic work environment, Proceedings of the Fortieth Annual Hawaii International Conference on System Sciences, p 266, 2007

1.4 DATA RECOVERY FUNCTION MAPPING

Data recovery is generally regarded as the process of salvaging data partially or completely from damaged, failed, corrupted or inaccessible storage media. Recovery may be required due to physical damage to the storage device or logical damage to the file system that prevents it from being mounted by the host operating system.[101]

A variety of failures can cause physical damage to storage media. CD-ROMs can have their metallic substrate or dye layer scratched off; hard disks can suffer any of several mechanical failures; tapes can break. The logical damage to the data may take the form of corrupt or missing boot-related records (e.g., main boot record, disk partition table and directories) or the loss of file signatures (e.g., header and footer). Since our focus is on validating and verifying digital forensic tools in terms of the data recovery function, the consideration of physical damage recovery techniques is outside the scope of this paper and is considered to be complementary to logical damage recovery techniques. Consequently, in the rest of this paper, data recovery refers to logical damage recovery unless otherwise stated.

Data recovery in the context of digital forensics has its peculiarities and differs from traditional data recovery in the computer science discipline. First, data recovery in the digital forensic context is a process by which digital evidence is recovered for use in court. Therefore,it should be conducted by certfied investigators, conform to standard operating procedures, utilize tools that are validated and verified by the appropriate authorities, and be supervised and documented. Traditional data recovery does not have these requirements because its goal is to recover as much data as possible without concern for its forensic soundness. Second, the techniques used in traditional data recovery and the digital forensic context differ because of the forensic soundness issue. For example, in traditional data recovery, a corrupted main boot record may be repaired by laying a FAT2 over a FAT1 if the FAT2 is intact. However, this is not an appropriate forensic data recovery technique because the original evidence (FAT1) is modfied. Instead, it would be necessary to repair the corrupted main boot record in duplicate (i.e., image). Finally, forensic data recovery embraces a broader view of recovering data than traditional data recovery and,

[101] Y Guo, J Slay and J. Beckett, Validation and verification of computer forensic software tools – Searching function, Digital Investigation, vol 6(S1), pp S12–S22, 2009

consequently, must consider issues (e.g., hidden data and trace data) that are beyond the purview of traditional data recovery.

The data recovery function is mapped by detailing its components, processes and relevant factors. Since the goal of data recovery is to retrieve data due to storage media abnormalities and/or intentional human manipulation, the function mapping is performed from three angles: (i) storage media; (ii) recovery object; and (iii) recovery reason.

1.5 REASONS FOR DATA RECOVERY

A data recovery method is used when data is unavailable. In the context of digital forensics, data is unavailable and must be salvaged for various reasons, including damage, corruption or hiding. From thepoint of view of the user (e.g., investigator), we assume that the data is unavailable because it is inaccessible or hidden. By inaccessible data, we mean that the user is aware of the existence of the data, but is unable to access it in a normal manner. On the other hand, hidden data is invisible to the user, and the user does not know of its existence.[102]

- ***Inaccessible data***

"Orphaned" files are inaccessible to users under normal operations. An orphaned file is one that no longer has a parent (the parent is the folder in which it was originally located). The term orphaned is a broad concept that includes deleted files. In most cases, orphaned files are deleted files, but a file can be orphaned when the association with its parent is lost through other means (e.g., byremoving a symbolic link in a Unix environment).

- ***Hidden Data***

In the digital forensic context, it may be necessary to recover data that has intentionally been hidden. Data hiding methods may be categorized as hardware-based or software-based, Hardware-based methods hide data in specific areas of storage media. For example, data on a hard disk may be stored in the HPA (host protected area), DCO (device configuration overlay), UPA (unused partition area) and inter-partition space.

[102] National Institute of Standards and Technology, Computer Forensics Tool Testing Program, Gaithersburg, Maryland <www.cftt.nist .gov>

Software-based methods hide data using thefile system and/or operating system utilities . For example, modern hard disk controllers handle bad sectors without the involvement of the operating system by slipping (modifying the LBN (logical block number) to physical mapping to skip the defective sector) or remapping (reallocating the LBN from a defective area to a spare sector). For older hard disks that do not have this capability, the operating system and file system have to retain the ability to detect and mark defective sectors and clusters as damaged. This feature can be used to exclude undamaged clusters from normal file system activities and use them to hide data.

Software-based data hiding methods may also use ambient space. Slack space, which includes file slack space, volume slack space and partition slack space, are areas on the disk that cannot be used by the file system because of the discrete nature of space allocation. Data can be hidden in any of these locations.

1.6 REQUIREMENT SPECIFICATION

Requirements specification is the second step of the validation and verification framework. The data recovery function requirements are specified in the same way as the search function requirements in. The method of specifying requirements is highly abstract and generalized. We use italicized "variables" to reflect these variations.[103] Thus, when a requirement has to be changed, it is only necessary to adjust (add, delete or modify) the variables. Moreover, the requirements can be unwrapped when it is necessary to develop a specific test scenario in a reference set. For example, the requirement: "The tool shall be able to accurately recover inaccessible recovery objects" may be unwrapped and instantiated as "The tool shall be able to accurately recover deleted JPG files" or "The tool shall be able to accurately recover hidden data in file slack."

A digital forensic tool has the following eight requirements with respect to the data recovery function:

- The tool shall operate in at least one operational environment.

[103] RMcKemmish, What is forensic computing? Trends and Issues in Crime and Criminal Justice, no 118 <www.aic.gov.au/publications /tandi/ti118.pdf>

- The tool shall operate under at least one operating system.
- The tool shall operate on at least one type of storage media.
- The tool shall be able to accurately render system data.
- The tool shall be able to accurately recover inaccessible (recovery)objects.
- The tool shall be able to accurately recover hidden (recovery) objects.
- If there are unresolved errors when reconstructing data, then thetool shall report the error types and error locations.
- The tool shall report the attributes of the recovered data.

1.7 RECOVERED OBJECTS

File system data to be recovered belongs to one of four categories: system data, user data, metadata and trace data.[104]

- ***System data***

System data includes general hardware and software information. Data recovery techniques include hardware rendering and software (operating system and file system) rendering. Hardware rendering refers to the ability to accurately identify particular types of devices and media. This is accomplished through physical interaction with the device or media or by using metadata located on the device or media.

The goal of the operating system orfil e system rendering is to reveal the underlying structure. Operating systems andfile systems have a general structure, but each instance is unique. In addition, many of these systems are proprietary in nature and, as a result, are poorly documented (e.g., the detailed structure of NTFS has not been publicly released). Operating system andfile system rendering may specify where certain structures are found and the data unit size that enables file folders, data and metadata to be accurately retrieved. For example, thevolume label and the associated data are indicators of the method usedto create the allocated components of a device. Different file systemsrecord this information differently, so a digital forensic tool must be able to render the volume label(s) from a device or partition.

[104] Guo, Yinghua& Slay, Jill (2010) Data Recovery Function Testing for Digital Forensic Tools. IFIP Advances in Information and Communication Technology.

- ***User Data***

User data is the principal object of data recovery. User data are categorized as document, graphic, sound or Internetfiles.This classification is by no means exhaustive and will have to be updated constantly to accommodate new applications andfile formats. Note that user datafiles may be in special forms (e.g., compressed and encrypted), which should be taken into account by forensic examiners.

- ***Meta Data***

Metadata is data that describes data or files. It includesdata about where the file content is stored, file size, dates and times of the last read and write, and access control information. Metadata must be analyzed to determine details about a specific file or to search for a file that meets certain requirements.

- ***Trace Data***

Data recovery in the digital forensic context is a much broader concept than traditional data recovery. Trace data is the data that remains on the storage media after operationssuch as hard drive partitioning, formatting andfile deletion . Trace data may not be substantial but may constitute important digital evidence. For example,file operations (e.g., creation, modfication and deletion) leave traces in the form of temporaryfiles. Mo st temporary files are deleted by the operating system after the file operations are completed. However, if a temporaryfile is deleted, its contents can be recovered if the clusters allocated to the file are not reallocated. Also, even if the allocated clusters are reallocated, file metadata (e.g., name and timestamp) may exist and may prove to be useful in a digital forensic investigation.

1.8 REFERENCE SET DEVELOPMENT AND TESTING

A reference set consists of test scenarios (cases) against which a digital forensic tool or its individual function is validated. The development of test scenarios is based on the specfic ation of function requirements. Using the requirements specification, it is possible to establish a referenceset for testing the data recovery function of various digital forensic tools.Since the functional requirements are specified in an extensible manner, the corresponding reference set is also extensible. This would enable practitioners, tool developers and researchers to identify critical needsand to target deterministic reference sets.We have identfied eight requirements for the data recovery function. Since each requirement has several variables, multiple test scenarios have to be designed for each requirement. Each scenario represents a single instantiation of each variable. The following are some pilot samples of the reference set for the data recovery function:

- A deleted JPG file in a FAT32 file system on an IDE hard disk.
- A deleted JPG file in an NTFS file system on a SCSI hard disk.
- A deleted WAV file in a UDF file system on a CD.
- A deleted Microsoft Word file in an FFS file system on flash memory.
- A deleted compressed HTML file in an NTFS file system on anIDE hard disk.
- An encrypted MP3 file in a FAT32 file system on an ATA harddisk.

1.9 CONCLUSION

Mapping the fundamental functions of the digital forensic discipline is a powerful approach for creating a function-oriented validation and verification paradigm for digital forensic tools. The utility of the approach is demonstrated in the context of the data recovery function via the specification of data recovery requirements and a reference set for testing tools that implement the data recovery function. Validating a digital forensic tool is reduced to testing the tool against the reference set. Compared with traditional testing methods, this testing paradigm is extensible and neutral and transparent to specific tools and tool versions.

1.10 LET'S SUM UP

More work remains to be done to complete the validation paradigm. Although the methodology holds promise, it needs to be tested extensively to evaluate its utility and identify potential weaknesses and shortcomings. Tests would have to be implemented against popular tools such as EnCase and FTK. A quantitative model is also required to evaluate the results of validation and verification. Metrics are needed to measure the accuracy and precision of testing results, and it is necessary to specify rules for judging the validity of digital forensic tools. Is a tool validated only when it passes all the test cases? Or is a tool validated when it passes the test cases for certain scenarios?

It is important to recognize that numerous variables are involved in function requirements specification and that the corresponding reference set can be very large. Indeed, the number of possible combinations for validating a single function in a digital forensic tool may well be in the thousands (even discounting the different versions of the tool). Interestingly, this problem is also faced by the Computer Forensics Tool Testing (CFTT) Program created by the National Institute of Standards and Technology (NIST) to validate and verify digital forensic tools.

1.11 FURTHER READING

- E. Huebner, D. Bem and C. Wee, Data hiding in the NTFS file system, Digital Investigation, vol. 3(4), pp. 211–226, 2006.
- Y. Guo, J. Slay and J. Beckett, Validation and verification of computer forensic software tools – Searching function, Digital Investigation, vol. 6(S1), pp. S12–S22, 2009.
- R. McKemmish, What is forensic computing? Trends and Issues inCrime and Criminal Justice, no. 118 (www.aic.gov.au/publications/tandi/ti118.pdf), 2002.
- G. Mohay, A. Anderson, B. Collie, O. de Vel and R. McKemmish,Computer and Intrusion Forensics, Artech House, Norwood, Massachusetts, 2003.
- A. Pal and N. Memon, The evolution offile carving, IEEE SignalProcessing, vol. 26(2), pp. 59–71, 2009.

1.12 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) What is data recovery?

Data recovery is generally regarded as the process of salvaging data partially or completely from damaged, failed, corrupted or inaccessible storage media.

2) How is the function mapping being performed?

The function mapping is performed from three angles: (i) storage media; (ii) recovery object; and (iii) recovery reason.

3) What are the requirements of digital forensic tool for data recovery function?

A digital forensic tool has the following eight requirements with respect to the data recovery function:

- The tool shall operate in at least one operational environment.
- The tool shall operate under at least one operating system.
- The tool shall operate on at least one type of storage media.
- The tool shall be able to accurately render system data.
- The tool shall be able to accurately recover inaccessible (recovery)objects.
- The tool shall be able to accurately recover hidden (recovery) objects.
- If there are unresolved errors when reconstructing data, then thetool shall report the error types and error locations.
- The tool shall report the attributes of the recovered data.

4) What is a reference set?

A reference set consists of test scenarios (cases) against which a digital forensic tool or its function is validated.

1.13 ACTIVITY

Explain briefly the process involved in data recovery and the tools required for digital forensic with respect to recovered objects and testing? (800-1000 words)

Unit 4: Avenues for Prosecution and Government Efforts

4

SUBJECT CODE: PGDCL 104

DIGITAL RECORDS AND CYBER FORENSICS

BLOCK 3 – ROLE AND ANALYSIS OF CYBER FORENSICS

UNIT 4 – AVENUES FOR PROSECUTION AND GOVERNMENT EFFORTS

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- The evolution of computer-specific statutes
- Terrorist surveillance program
- Virtual Global Taskforce

1.2 INTRODUCTION

The advent of computer crime has resulted in a myriad of problems for law enforcement administrators. The lack of resources available to small agencies, the traditional apathy toward nonviolent crime, and the reluctance of legislative action have enabled many computer criminals to act with virtual impunity. While it is anticipated that an increase in technology-specific legislation and the modification of extant statutes are forthcoming, lawmakers should evaluate existing federal and state law for prosecutorial avenues currently available. This would empower local agencies and reduce demands on federal agencies.[105]

Traditionally, state and local officials have been forced to rely exclusively on the expertise of better-trained, better-funded federal agencies. Unfortunately, these agencies are incapable of addressing every call for assistance. In addition, they are often unwilling to expend resources on crimes which do not constitute threats to institutional security, the economic infrastructure, the exploitation of children, individual safety, or violation of federal law. (It is unlikely, for example, that a federal agency would assist law enforcement in cases constituting misdemeanour offenses or those offenses which appear to be minor—e.g., installation of Back Orifice on a personal computer, a currently contained virus which destroyed two computers.) Law enforcement administrators should carefully evaluate state statutes. When used creatively, many can be directly applied to criminal activity involving computers. Remember, the method of execution is not an essential element in criminal law. Intent, action, and illegality are inherent in every case of larceny, for example. The method is irrelevant. Thus, an individual who utilizes a computer to steal money from a bank is just as culpable as the individual who resorts to physical theft. At the

[105] Adams, D (2003, December 16) Police prove a match for electronic foe. The Sydney Morning Herald. Retrieved on 28th January 2015 from <http://www.smh.com.au/articles/2003/12/15/1071336882279.html?from=storyrhs>

same time, criminal mischief or vandalism statutes may be utilized to prosecute an individual who remotely alters data. Investigators and administrators must be encouraged to look for the obvious! While there are a variety of statutes which have been enacted to specifically address technological crime, traditional statutes should be utilized where the former is lacking.

1.3 THE EVOLUTION OF COMPUTER-SPECIFIC STATUTES

While many state legislatures have been slow to enact computer-specific statutes, U.S. Congress has reacted more quickly. Thus, measures enabling the prosecution of electronic fraud, hacking, and the theft of intellectual property may be found at thefederal level. Unfortunately, this legislation has been buffeted by a variety of legal challenges, the language characterized by jurists as vague and ambiguous.[106] Such efforts can be traced back to 1977 when Senator Abraham Ribicoff (Connecticut) introduced the Federal Computer Systems Protection Act (FSCPA). Although the bill died in committee, it was responsible for initiating dialogue and communication about the threat and potentiality of computer crime.

1.4 COMPUTER FRAUD AND ABUSE ACT, 1986

Originally known as the Counterfeit Access Device and Computer Fraud and Abuse Act (CFAA), Section 1030 of Title 18 of the U.S. Code quickly became the federal government's main weapon in fighting computer crime. Known as the hacking statute, the act in its original form was very narrow in scope, making it a felony to knowingly

> [a]ccess a computer without authorization, or in excess of authorization, in order to obtain classified United States defense or foreign relations information with the intent or reason to believe that such information would be used to harm the United States or to advantage a foreign nation. Second, the 1984 Act made it a misdemeanor knowingly to access a computer without authorization, in excess of authorization, in order to obtain information contained in a financial record of a financial institution or in a consumer file of a consumer reporting agency. Third, the 1984 Act made it a misdemeanour knowingly

[106] Nicholson, Laura J; Shebar, Tom F.; and Weinberg, Meredith R. (2000). "Computer Crimes: Annual White Collar Crime Survey" American Criminal Law Review, 37(2): 207–210

> to access a computer without authorization, or in excess of authorization, in order to use, modify, destroy, or disclose information in, or prevent authorized use of, a computer operated for or on behalf of the United States if such conduct would affect the government's use of the computer. The 1984 Act also made it a crime to attempt or to conspire to commit any of the three acts described above.

This legislation proved to be largely ineffective due to the ambiguity of the statutory language and an overemphasis on financial information. (Only one person was successfully prosecuted under the original provisions.)Finally, the 1986 revisions specifically targeted hackers by criminalizing password trafficking.[107]

The act was also used to prosecute early hackers, Herbert Zinn (aka Shadowhawk) and Kevin Mitnick. Shadowhawk was an 18-year-old high school dropout and hacker extraordinaire. Herbert Zinn considered a juvenile at the time of his arrest, was sentenced to nine months and fined $10,000 for breaking into computers of various organizations ranging from NATO to the U.S. Air Force. In addition, Zinn stole 52 AT&T programs valued at over $1 million. Provisions under the act could have resulted in a prison term of 20 years for an adult charged with the same range of offenses. Unlike Zinn, Kevin Mitnick, one of the most infamous hackers in history, had a criminal history the length of which rivals that of many organized crime figures. His successful conviction under this act was a result of his theft of programs valued at more than $1 million from Digital Equipment Corporation and the illegal manipulation of MCI service codes. Since its inception, the act has been modified several times, primarily to clarify terms.

1.5 NATIONAL INFORMATION INFRASTRUCTURE PROTECTION ACT, 1996

While the CFAA was successfully used to prosecute hackers and individuals who exceeded their authorized use, it contained significant limitations in that it only involved those cases in which computer data was a target. It neither included other offenses committed via or in conjunction with computer technology nor included noninterest computers. To remedy this, Congress passed the National Information Infrastructure Protection Act (NIIPA).[108] Originally conceived in 1996,

[107]Pastrikos, Catherine (2004). "Identity Theft Statutes: Which Will Protect Americans the Most?" Albany Law Review, 67(4): 1137–1157

[108] 18 U S C § 1030

NIIPA amended the CFAA to provide for any computer attached to the Internet even if the said computer was not one defined as a federal interest computer or if multiple computers were located in one state. In addition, NIIPA identified broad areas of computer-related crime which involve either accessing computer systems without/or in excess ofauthorization or causing damage to computers.

These modifications served to close numerous loopholes in the original legislation. By extending protection to all computers connected to the Internet, NIIPA provides for the prosecution of hacker attacks on both intrastate government and financial institution computers. In addition, by removing the trespass requirement and adding an intent or recklessness element, NIIPA provides for the prosecution of insiders who intentionally damage computers. The act further provides for the prosecution of individuals trafficking in passwords or those who attempted to extort money or values from an individual or entity by threatening computer harm. Finally, and perhaps more importantly, NIIPA successfully eliminates several defenses predicated on intent, implied authorization, or value of access. More specifically, NIIPA requires only an intent to access not an intent to cause damage. Thus, individuals attempting to access a protected computer may be prosecuted even if their motivation was not fiduciary.

1.6 EVOLVING CHILD PORNOGRAPHY STATUTES

Although a variety of laws have been enacted to combat the increase in technological crime, none are more emotionally charged than those dealing with child pornography. Beginning in 1977, Congress has attempted to eliminate child pornography. Originally criminalized at the federal level with the Protection of Children against SexualExploitation Act of 1977 (PCSE), Congress has periodically revised the legislation to protect children from sexual exploitation in keeping with emerging legal doctrine. However, lower courts have remained divided on new legislation, and the Supreme Court has denied cert on the majority of cases. Traditionally, evaluations of child pornography statutes relied primarily on two Supreme Court decisions, whose interpretation of and application to emerging laws have been diverse.[109]

[109] Stevens, Gina and Doyle, Charles (2003) Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping. Report for Congress: 98-326. Retrieved from <www.epic.org>on March 23, 2012.

In 1982, the Supreme Court evaluated free-speech challenges to child pornography and found them wanting ***(New York v. Ferber).***[110] Uncharacteristically emphatic,the Court ruled that child pornography was outside the scope of the First Amendment, and allowed states to enact blanket prohibitions against visualizations of children engaged in sexual situations. The Child protection act of 1984 (CPA) incorporated this decision. Although the CPA lacked technological specificity, it was widely used against online offenders until the emergence of the Child Protection and Obscenity act of 1988. While both of these acts were designed to protect children from exposure to and inclusion in material deemed to be obscene, these and future acts are continuously challenged by freespeech advocates. At the same time, the Supreme Court has remained resolutely silent.

The Congress passed the Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today (PROTECT) Act. Although it sought to reinstate the original provisions housed within the CPPA, it also included a variety of other measures designed to protect children both online and offline. The most important of these included the following:

- Mandatory life sentences for offenders involved in a sex offense against a minor if such offender has had a prior conviction of abuse against a minor;
- The establishment of a program to obtain criminal history/background checks for volunteer organizations;
- Authorization for electronic eavesdropping in cases related to child abuse or kidnapping;
- Prohibition against the pre-trial release of persons charged with specific offenses against children;
- Elimination of the statutes of limitation for child abduction or child abuse;

1.7 IDENTITY THEFT AND ASSUMPTION DETERRENCE ACT, 1998

In October 1998, the Identity Theft and Assumption Deterrence Act (ITADA) waspassed by Congress. It was the first act to make the possession of another's personal identifying

[110] *New York v Ferber*458 U S 747

information a crime, punishable by up to 20 years in prison. More specifically, the act stated that it is unlawful if an individual,[111]

> [k]nowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.

In addition, the law expanded the traditional definition of "means of identification" to include:

- name, social security number, date of birth, official State or government-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer-identification number;
- unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
- unique electronic identification number, address, or routing code; or
- telecommunication identifying information or access device.

1.8 IDENTITY THEFT ENFORCEMENT AND RESTITUTION ACT, 2008

In 2008, Congress formally recognized the financial impact of identity theft by passingthe identity theft enforcement and restitution act. Among other provisions, the act broadened the scope of activities which may be prosecuted as identity theft and provided mechanisms for the recovery of direct funds stolen from victims. For example, this act removed the $5,000 threshold for legal action and granted federal jurisdiction in cases involving same state victimization (i.e., it removed the traditional interstate commerce requirement). Perhaps most importantly, the act also provided for the recovery of indirect costs of victimization including lost wages and credit rehabilitation.[112]

1.9 AUTOMATED TARGETING SYSTEM (ATS)

[111] Seifert (2007) Data Mining and Homeland Security

[112] Broadhurst, Roderic (2006) "Developments in the Global Law Enforcement of Cyber-Crime" Policing: An International Journal of Police Strategies and Management, 29(3): 408–433

The Automated Targeting System (ATS) was developed by the Department of Homeland Security within the Treasury Enforcement Communications System. It was designed to screen travellers entering the United States by automobile, aeroplane, or rail. Housed within the Bureau of Customs and Border Protection (CBP), ATS assesses risks for cargo, conveyances, and travellers. There are six categories, or modules, of activity:

- ATS-Inbound—inbound cargo and conveyances (rail, truck, ship, and air);
- ATS-Outbound-outbound cargo and conveyances (rail, truck, ship, and air);
- ATS-Passenger-travelers and conveyances (air, ship, and rail);
- ATS-Land-private vehicles arriving by land;
- ATS-International-cargo targeting for CBP's collaboration with foreign customs authorities; and
- ATS-Trend Analysis and Analytical Selectivity Program (ATS-TAP)-analytical module.

Like other data-mining practices by law enforcement, ATS has been harshly criticized by privacy advocates. In 2006, a suit was filed to suspend the systems as it applied to individuals, or, in the alternative, fully apply all Privacy Act safeguards to any person subjected to the system.Although it was originally designed to enhance customer service in the private sector through customizing profiles of individual shoppers, it has increasingly been employed by criminals and law enforcement alike.[113]

1.10 TERRORIST SURVEILLANCE PROGRAM

First disclosed to the public in December 2005 via a news report, the Terrorist Surveillance Program has been employed by the National Security Agency (NSA) since 2002. Among other things, the program includes the domestic collection, analysis, and sharing of telephone call information. According to statements issued by the president and the Department of Justice, the program is reserved for international calls with links to al Qaeda or related terrorist groups and requires review and reauthorization every 45 days. Privacy advocates have repeatedly expressed concerns over the potential for abuses. Recently, such concerns were validated when it was

[113] Frost and Sullivan (2003) "U S CALEA Market Insight: 6841–63" Retrieved from <http://www.corp.att.com/stateandlocal/docs/US_ CALEA_Market_Insight.pdf on February 12, 2013>

revealed that the NSA had contracted with AT&T, Verizon, and BellSouth to collect information about domestic telephone calls. Although the content of such disclosures is not entirely clear, the compromise of privacy expectations and subsequent erosion of public trust occurred.

CASE STUDY – PRIVACY IN IRAN

In 2010, Nokia Siemens Network was sued by Iranian dissidents who alleged that Nokia had provided the Iranian regime with devices which monitored, eaves-dropped, filtered, and tracked mobile phones.[114] The suit was filed after Isa Sakarkhiz, a prominent Iranian journalist who was instrumental in illuminating Iran's oppression of the press was arrested by government agents who had tracked his mobile phone using Nokia's Intelligence Solutions tool which had been sold to the state-owned telecommunicationsprovider. This Nokia system, which was sold and specifically modified to the government's needs, was composed of (1) a monitoring area which provided for the centralized deep packet inspection of both voice and data communications, and (2) an intelligence area which provided for real-time data mining. Although Nokia claims to have abandoned the software which provides for monitoring of communications, they have declared themselves immune from responsibility as they are a corporation.[115]

1.11 VIRTUAL GLOBAL TASKFORCE (VGT)

In 2003, the Virtual Global Taskforce was created as a collaborative effort between the Australian High Tech Crime Centre, the Child Exploitation and Online Protection Centre (UK), the Royal Canadian Mounted Police, the U.S. Department of Homeland Security, and Interpol.[116] It is designed to deliver low-cost, high-impact initiatives that deter pedophiles and prevent the online exploitation of children. By reducing the confidence of potential perpetrators through the removal of perceptions of anonymity, the group aims to deter online misconduct. Their most notable initiative is to know as Operation Pin. This program involves a Web site which claims to contain images of child exploitation and pornography. Visitors to the site who attempt to

[114] United Nations (2000) "United Nations Manual on the Prevention and Control of Computer-related Criteria"

[115] Department of Defense (May 20, 2003) Report to Congress Regarding the Terrorism Informational Awareness Program, Detailed Information. Retrieved from<www.epic.org on March 23, 2012>

[116]<http://www.virtualglobaltaskforce.com>the homepage of the Virtual Global Taskforce. The group, dedicated to the prevention and prosecution of online child abuse, provides access to the latest news regarding online predators and law enforcement successes

download images are confronted by an online law enforcement presence and informed that they have committed a criminal offense and that information about them has been forwarded to appropriate authorities.

1.12 LET'S SUM UP

Although recognition of the insidious nature of computer crime is increasing, much work remains to be completed on all levels of government. Legislation and the codification of computer criminality must keep abreast of emerging technology. Until such a time, investigators should look to traditional statutes to prosecute individuals committing traditional crimes via electronic means.

Even in areas where state, local, and federal government agencies have enacted regulations to specifically address online criminal behavior, some activity is sure to be over-looked. Thus, law enforcement officials must continue to evaluate the applicability of traditional legislation. The Federal Wire Fraud Act, for example, enables prosecutors to pursue individuals illegally transferring funds, accessing bank computers, and the like. While most computer-specific legislation has tended to be enacted on the federal level,state and local agencies may be able to implement generic statutes of enforcement. For example, although many states have not formally encoded electronic vandalism statutes, innovative departments may still pursue individuals responsible for computer worms or viruses through criminal mischief and destruction of property codes. Local and state law enforcement officials should carefully evaluate local regulations and identify applicable statutes.

1.13 FURTHER READING

- Seifert, Jeffrey W. (2007). Data Mining and Homeland Security: An Overview. CRS Report for Congress. Order Code RL 31798. January 18, 2007.
- International Review of Criminal Policy—United Nations Manual on the Prevention and Control of Computer-Related Crime. Retrieved from http://www.uncjin.org/Documents/EighthCongress.html on February 12, 2013.

- ➢ Nicholson, Laura J.; Shebar, Tom F.; and Weinberg, Meredith R. (2000). "Computer Crimes: Annual White Collar Crime Survey." American Criminal Law Review, 37(2): 207–210.
- ➢ Stevens, Gina and Doyle, Charles (2003). Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping. Report for Congress: #98-326. Retrieved from www.epic.org on March 23, 2012.
- ➢ Seifert, Jeffrey W. (2007). Data Mining and Homeland Security: An Overview. CRS Report for Congress. Order Code RL 31798.
- ➢ Poulsen, Kevn (2005). "FBI Retires Its Carnivore." Security Focus. Retrieved from www.securityfocus.com on March 23, 2012.

1.14 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) What is the main aim/objective of the National Information Infrastructure Protection Act, 1996?

NIIPA provides for the prosecution of hacker attacks on both intrastate government and financial institution computers.

2) What are the six categories of Automated Targeting System?

- ATS-Inbound—inbound cargo and conveyances (rail, truck, ship, and air);
- ATS-Outbound-outbound cargo and conveyances (rail, truck, ship, and air);
- ATS-Passenger-travelers and conveyances (air, ship, and rail);
- ATS-Land-private vehicles arriving by land;
- ATS-International-cargo targeting for CBP's collaboration with foreign customs authorities; and
- ATS-Trend Analysis and Analytical Selectivity Program (ATS-TAP)-analytical module.

3) What was the reason behind the enactment of Identity Theft Enforcement and Restitution Act, 2008?

The act broadened the scope of activities which may be prosecuted as identity theft and provided mechanisms for the recovery of direct funds stolen from victims. For example, this act removed the $5,000 threshold for legal action and granted federal jurisdiction in cases involving same state victimization (i.e., it removed the traditional interstate commerce requirement). Perhaps most importantly, the act also provided for the recovery of indirect costs of victimization, including lost wages and credit rehabilitation.

4) Short notes on the evolution of child pornography?

- Mandatory life sentences for offenders involved in a sex offense against a minor if such offender has had a prior conviction of abuse against a minor;
- The establishment of a program to obtain criminal history/background checks for volunteer organizations;
- Authorization for electronic eavesdropping in cases related to child abuse or kidnapping;
- Prohibition against the pre-trial release of persons charged with specific offenses against children;
- Elimination of the statutes of limitation for child abduction or child abuse;

1.15 ACTIVITY

Explain briefly the evolution of different statutes that was brought to light with respect to computer-based crimes and the after-effects with respect it? Also, How may traditional statutes be applied to the contemporary phenomenon of computer crime? (1000 words)

Block 4

Cyber Forensics from Law Enforcement Perspective

Unit 1: Computer Forensics and the Process of Confiscation

1

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Concept of computer forensics
- Techniques in computer forensic
- Preserving Computer Evidence

1.2 INTRODUCTION

The term ***'computer forensic'*** was coined for the first time by the International Association of Computer Specialists (IACS) in Oregon (USA) in the year 1191. It is a branch of forensic science which is devised to identify local preserve of extract digital information from the computer system to produce and store evidence of the cybercrime beforethe law court.[117]Dr Clifford Stall, an astronomer and professor in theUniversity of Berkeley has defined - computer forensic, as that branch offorensic science wherein cybercrime investigation and analysistechniques are applied to determine potential legal evidence in acomputer environment. Internet-related forensics broadly cover threeareas, namely (i) computer forensics, (ii) cyber forensics, and (iii)software forensics.

Cyber forensics plays a crucial role in solving crimes. The collection of forensic evidence serves an important key role that sometimes it is the only way to establish or exclude any case between suspect and victim or crime scene, eventually to establish a final verdict. As Internet technologies associate with us into everyday life, we come close to realizing new and existing online opportunities. One such opportunity is in Cyber forensics, unique process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally accepted which helps in the investigation process.

1.3 CONCEPT OF COMPUTER FORENSIC

An individual uses his computer to connect the internet via an ***Internet Service Provider (ISP)***by using either a dial-up connection or a leased line/broadband/ mobile network facility.[118]

There are two levels at which evidence of Internet usage exists:

a) Individual Level
   - On an individual's own computer, computer system or computer network.
   - On the websites assessed by the individual using his own computer, computer system or computer network and

b) ISP Level

[117] Rohas N, "Understanding Computer Forensics", Asian school of cyber law, 2009

[118] Cyber Forensics and Indian Approach
<http://ptlb.in/cfrci/?p=15>

- On the service of an individual's ISP.

1.4 COLLECTING EVIDENCE AT INDIVIDUAL'S LEVEL

Computers usually store text, graphic, image files, e-mails messages etc. in the hard disk during its routine use. User may keep on deleting the unwanted material regularly to free up disk space. Similarly, Chat rooms, Internet Relay Chat (IRC), Internet telephony sessions are real-time discussions happening on the Internet; it is optional for the user to maintain logging files of these sessions.[119]

Caching means copying of a web page/site and storing that copy for the purpose of speeding up subsequent access. It ensures that the load on the servers of origin will be reduced as they can be accessed from the cached servers. With the help of browser software, a user can retrieve any web page from the computer's cache memory rather than going back to the original source site. From the legal standpoint, the information saved in a web-browser cache whether or not intentionally retained constitutes ***'possession'.***

1.5 COLLECTING EVIDENCE AT ISP LEVEL

Logs maintained by the ISPs of the users using dial-up/leased line/ broadband/mobile-Internet connections to connect to ISP indicate the time and duration of Internet usage/connectivity along with the IP address. It will corroborate other types of evidence that has already been gathered during the investigation. Admissibility of such evidence cannot be questioned as it clearly highlights not only the time and duration of computer's Internet usage/connectivity but also the fact that during a specific time period, the user's computer had been working as a sort of *'computer network'*. It is important to note that ISPs under the licensing conditions are collecting traffic data in the form of IP addresses, machine IDs (Mac ids), date and time (of communication), size of data (received/sent) and other related information.

[119] Cyber Forensic Investigation Solutions in India Are Needed
<http://ptlb.in/cfrci/?p=9>

1.6 PROCESS OF CYBER FORENSIC

- As soon as the crime is reported and is registered with the police, the investigation starts and data is collected from the place of crime/computer system and is examined using forensic techniques.[120]
- The computer system seized is examined thoroughly to find out the digital data which can act as evidence.
- Important data which can help as a clue or evidence can remain hidden in different file formats like deleted files, hidden files, password-protected files, log files, system files etc.
- After all the information is gathered from the computer system the original form of evidence is recovered. It must very importantly be kept in mind that never to harm the originally recovered data while applying forensics.
- Create a mirror image of the original evidence using a different mechanism like bitstream etc. and use this mirror image of the original evidence. Never tamper the original copy of evidence for the investigation.
- Digital evidences are highly volatile and can be easily misinterpreted so care must be taken be.
- Enough supporting data/information must be gathered before presenting the digital evidence in front of the court of law.

1.7 PROBLEMS WITH PRESERVING COMPUTER EVIDENCE

Preserving evidence is not an easy task.[121] There exist both human and technical barriers to the evidence gathering mechanism. One must be aware of such limitations:

- Some of the facilities within the browsers to save WWW pages to the hard disk are imperfect- as it may save the text but not the associated images.

[120] Cyber Forensics
<http://www.cyberlawsindia.net/computerforensics1.html>

[121] Sadiku, Matthew &Tembely, Mahamadou& Musa, Sarhan.(2017) Digital Forensics. International Journal of Advanced Research in Computer Science and Software Engineering

- In case of some very complex pages, involving *'frames'* and *'templates',* there could be a perceptible difference in what is seen on screen and what is saved on the hard disk.
- The method used to save a file to the hard disk may not carry any individual labelling, which shows where and when it was obtained. The problem with such saved files is that they could be easily modified or forged.
- It is difficult to tell when a specific page was last acquired due to the browser cache facility. Thus if one examines a whole series of cached pages, it is not easy to pinpoint which page came first and which later.
- It should not be forgotten that many ISPs use proxy servers to speed up the delivery of popular pages. Thus a user of such an ISP may not be sure that what he has received on his computer is the latest version from the source computer (website) as opposed to an earlier cached version held by his ISP.

1.8 VARIOUS BRANCHES OF DIGITAL FORENSICS

Digital Forensics has a very wide scope.[122] The branches of digital forensics are as follows:

a) Disk Forensics

Disk Forensics is the science of extracting forensic information from digital storage media like Hard disk, USB devices, FireWire devices, CD, DVD, Flash drives, Floppy disks etc.

b) Printer Forensics

Printed material is a direct accessory to many criminals and terrorist acts. In addition, printedmaterial may be used in the course of conducting illicit or terrorist activities. In both cases,the ability to identify the device or type of device used to print the material in question wouldprovide a valuable aid for law enforcement and intelligence agencies.

c) Network Forensics

Network forensics is a branch of digital forensics that focuses on the monitoring and analysisof network traffic. Network forensics is the process of gathering and examining raw

[122] I. Resendez, P Martinez, and J Abraham, "An Introduction to Digital Forensics," June 2014, <https://www.researchgate.net/publication/228864187_An_Introduction_to_Digital_Forensics>

dataof network and systematically tracking and monitoring the traffic of the network to make sure ofhow an attack took place.

Traffic is usually intercepted at the packet level, and either stored for later analysis or filteredin real-time. Unlike other areas of digital forensics network data is often volatile and rarelylogged, making the discipline often reactionary. Security professionals routinely use suchtools to analyze network intrusions not to convict the attacker but to understand how theperpetrator gained access and to plug the hole.

It also helps to investigate offences after the event, determine how they occurred and identify the party or parties responsible. A digital forensic investigator will gather network based evidence from a particular computing device in the network so that it can be presentedin court, conducting a thorough digital investigation and building a documented chain ofevidence.

d) Mobile Device Forensics

Mobile phone forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods. Mobile phones, especially thosewith advanced capabilities, are a relatively recent phenomenon, not usually covered inclassical computer forensics. Cell phones vary in design and are continually undergoing change as existing technologies improve and new technologies are introduced. Developing anunderstanding of the components and organization of cell phones is a prerequisite to understanding the criticalities involved when dealing with them forensically. Similarly, features of cellular networks are an important aspect of cell phone forensics, since logs of usage and other data are maintained therein. Cell phone forensics includes the analysis of both SIM and phone memory, each requires a separate procedure to deal with.

It differs from Computer forensics in that a mobile device will have an inbuilt communication system (e.g. GSM) and, usually, proprietary storage mechanisms. Investigations usually focus on simple data such as call data and communications (SMS/Email) rather than in-depth recovery of deleted data.

e) Database Forensics

Database forensics is a branch of digital forensics relating to the forensic study following the normal forensic process and applying investigative techniques to database contents and metadata. Cached information may also exist in a servers RAM requiring live analysis techniques.

A forensic examination of a database may relate to the timestamps that apply to the update time of a row in a relational table being inspected and tested for validity in order to verify theactions of a database user. Alternatively, a forensic examination may focus on identifyingtransactions within a database system or application that indicate evidence of wrongdoing,such as fraud.

Third-party software tools which provide a read-only environment can be used to manipulateand analyze data. These tools also provide audit logging capabilities which providedocumented proof of what tasks or analysis a forensic examiner performed on the database.

f) Digital Music Device Forensics

Large storage capacities and personal digital assistant (PDA) functionalities have made the digital music device a technology that should be of interest to the cyber forensic community.The digital music revolution has also seen the digital music device become a commonhousehold item. It is only a short time until they too make a natural progression into thecriminal world. This progression has already begun. Some of the hard-drive-based deviceshave capacities upwards of 60GB. With this much storage space for music, developers havebranched out and included features like a calendar and contact book (Apple iPod-Musicand more). These devices are simply a portable hard drive and have the ability to store othertypes of files besides music; such as documents or pictures.

An employee could take sensitive information by using the capabilities of a digital music device. Suspects could potentially store critical evidence on these types of devices. It must bedetermined if current frameworks of cyber forensic science are applicable and to what extentcurrent guidelines can be applied to digital music device forensics.

g) Scanner Forensics

A large portion of digital image data available today is created using acquisition devices suchas digital cameras and scanners. While cameras allow digital reproduction of natural scenes,scanners are used to capture hardcopy art in more controlled scenarios. For a forensic approach, a non-intrusive scanner model identification, which can be further extended to authenticatescanned images is a necessity.

Using only scanned image samples; a robust scanner identifier should determine the brand/model of the scanner used to capture individual scanned images. A proposal for such ascanner identifier is based on statistical features of scanning noise. Scanning noise of the images can be done from multiple perspectives, including image denoising, wavelet analysis,and neighbourhood prediction, and obtain statistical features from each characterization. Thesame approach can be extended to digital cameras and other imaging devices. The mostsignificant challenge is that ***"analytical procedures and protocols"*** are not standardized nor dopractitioners and researchers use the standard terminology.

The technology change will result in new devices emerging in the digital world. Whenever anew digital device enters the market a forensic methodology has to evolve to deal with it. This phenomenon will expand the field of device forensics.

h) PDA Forensics

In the modern era, Personal Digital Assistants (PDAs) are getting immensely popular. They are no longer meagre electronic devices holding personal information, appointments and address book. Modern PDAs are hybrid devices integrating wireless, Bluetooth, infrared, WiFi, mobile phone, camera, global positioning system, basic computing capabilities, Internet etc., in addition to the standard personal information management features.

Investigating crimes involving PDAs are more challenging than those involving normal computers. This is mainly because these devices are more compact, battery-operated and store data in volatile memory. A PDA is never really turned off as long as it has sufficient battery power. Evidence residing in PDA is of highly volatile in nature. It can be easily altered or damaged without getting noticed. In order to collect such evidence and ensure its admissibility in a court of law, sound forensic techniques and a systematic approach are needed. A standard forensic model for PDAs, which provides an abstract reference framework is particularly important in digital crime investigations. In addition to law enforcement officials, such a model can also benefit IT auditors, information security experts,IT managers and system administrators, as often they are the first responders related to anysort of computer crime in an organization.

1.9 PROCESS OF CONFISCATION

Section 76 of the Information Technology Act, 2000 highlights that all devices whether computer, computer system, floppies, compact disks, tape drives or any other storage, communication, input or output device which helped in the contravention of any provision of this Act, rules, orders or regulations made thereunder are liable to be confiscated.[123]

The proviso to the section further highlights that in case if the person concerned in whose possession, power or control computer, computer system, floppies, compact disks, tape drives or any other storage, communication, input or output device is found, establishes to the satisfaction of the court that he was in no way responsible for any of the contraventions, the adjudicating court not to confiscate such devices, under such circumstances. In such a case, the court may make such other order authorized by this Act, against the person contravening provisions of this Act, rules, orders or regulations made thereunder.

1.10 ADMISSIBILITY OF DIGITAL EVIDENCE

Digital evidence usually takes the form of writing or at least a form which can be analogized to writing, it must be authenticated and satisfy the requirements of the Best Evidence Rule.

The proponent of the evidence need not present testimony by a programmer, but should present some witnesses who can describe how information is processed through the computer and used by the organization.

[123] N Kumari and A KMohapatra, “An insight into digital forensics branches and tools,” Proceedings of the International Conference on Computational Techniques in Information and Communication Technologies, 2016

With regard to hearsay, most courts have dealt with the objection to the introduction of computer records by relying on the business record exception. Such an approach may work for audit logs, provided they satisfy the rule, which might not be the case for computer records collected as part of an investigation rather than as the result of a routine, periodic process. The following are some guidelines to preserve admissibility of digital evidence:

- Upon seizing digital evidence, action should not change that evidence.
- When it is necessary for a person to access original digital evidence, that person must be forensically competent.
- All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review.
- An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession.
- Any agency that is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles.

In the case of ***P.V. Anwar v P.K.Basheer,***[124]the Court in ***PARAGRAPH 24 OF ITS JUDGMENT***held that the electronic evidencewhich is a primary document can be admitted without producing certificate and thereis no obligation to satisfy the condition laid down in Section 65B of the Evidence Act, 1872. If that electronicrecord satisfies the condition under Section 62 then it can be unequivocally admitted as evidence.The same will not be covered either under Section 65A or 65B of the Evidence Act, 1872.Primary evidence is a ***'document'***which is defined under Section 3 of Evidence Act, 1872.[125]

1.11 CONCLUSION

Cyber forensics plays a significant role in the criminal justice systemas we continue to incorporate a range of technologies into our everyday lives. Evidence of allmost the types of crime is increasingly found in digital devices that either the perpetrator orthe victim used. As a

[124]*P V Anwar v P K Basheer* [2014] 10 SCC 473

[125] M Reith, C Carr, and GGunsch, "An examination of digital forensic models," International Journal of Digital Evidence, vol 1, no 3, Fall 2002

result of this potential evidence which did not exist in the past,investigators of conventional crimes increasingly need to consider any digital evidence thatmay be available.

In addition, Security professionals routinely use such tools to analyze network intrusions notto convict the attacker but to understand how the perpetrator gained access and to plug the hole. Data recovery firms rely on similar tools to resurrect files from drives that have been inadvertently reformatted or damaged.

1.12 LET'S SUM UP

In this chapter, we have studied the concept of computer forensic along with how the evidence is collected at each level. We also studied the process of cyber forensic and the problems faced in preserving the evidence. Finally, we ended the discussion with the process of confiscation and admissibility of digital evidence.

1.13 FURTHER READING

- The Role and Impact of Forensic Evidence in the Criminal Justice Process by JosephPeterson, Ira Sommers, Deborah Baskin, and Donald Johnson,2010
- Digital Forensics in Law Enforcement: A Needs Based Analysis of Indiana Agencies byTeri A. Cummins Flory (Purdue University),2016
- STANDARD OPERATING PROCEDURE OF DIGITAL EVIDENCECOLLECTION (Digital Forensics Department, CyberSecurity Malaysia)

1.14 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is cyber forensics?**

The term *'computer forensic'* was coined for the first time by the International Association of Computer Specialists (IACS) in Oregon (USA) in the year 1191. It is a branch of forensic science which is devised to identify local preserve of extract digital information from thecomputer system to produce and store evidence of the cybercrime before the law court.

2. Explain the concept of Computer Forensic?

An individual uses his computer to connect the internet via an ***Internet Service Provider (ISP)*** by using either a dial-up connection or a leased line/broadband/ mobile network facility.

There are two levels at which evidence of Internet usage exists:

a) Individual Level

- On an individual's own computer, computer system or computer network.
- On the websites assessed by the individual using his own computer, computer system or computer network and

b) ISP Level

- On the service of an individual's ISP.

3. Explain the process of cyber forensic?

The process of cyber forensic is as follows:

- As soon as the crime is reported and is registered with the police, the investigation starts and data is collected from the place of crime/computer system and is examined using forensic techniques.
- The computer system seized is examined thoroughly to find out the digital data which can act as evidence.
- Important data which can help as a clue or evidence can remain hidden in different file formats like deleted files, hidden files, password-protected files, log files, system files etc.
- After all the information is gathered from the computer system the original form of evidence is recovered. It must very importantly be kept in mind that never to harm the originally recovered data while applying forensics.

- Create a mirror image of the original evidence using a different mechanism like bitstream etc. and use this mirror image of the original evidence. Never tamper the original copy of evidence for the investigation.
- Digital evidences are highly volatile and can be easily misinterpreted so care must be taken be.
- Enough supporting data/information must be gathered before presenting the digital evidence in front of the court of law.

4. What are the various branches of digital forensics?

- Disk Forensics
- Printer Forensics
- Network Forensics
- Mobile Device Forensics
- Database Forensics
- Digital Music Device Forensics
- Scanner Forensics
- PDA Forensics

1.15 ACTIVITY

Explain the different branches of digital forensics with illustrations along with the procedure for admissibility of electronic evidence and case laws with respect to it? (1500-2000 words)

Unit 2: Relevance of Indian Evidence Act to Cyber Forensics

2

SUBJECT CODE – PGDCL 104

DIGITAL RECORDS AND CYBER FORENSICS

BLOCK 4 – CYBER FORENSICS FROM LAW ENFORCEMENT PERSPECTIVE

UNIT 2 – RELEVANCE OF INDIAN EVIDENCE ACT TO CYBER FORENSICS

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- The different laws with respect to cyber forensics

- Relevance of Indian Evidence Act
- Amendments made in Indian Evidence Act for the recognition of digital evidence

1.2 INDIAN LAWS RELEVANT TO CYBER FORENSICS

Cyber forensics is becoming vast due to the use of technology in the commitment of a crime. Technological advancements have brought convenience in many daily activities. Now a day's human is living in two interrelated worlds namely Real World and Cyber World. Any act of a human is likely to create multiple traces in both worlds and that's why cyber forensics is not only related cybercrime but also very well utilised in traditional crime investigation. This resulted in the need of amendments in existing laws of the real world. IT Act 2000 is mainly enforced for legal recognition of electronic records in cyberspace.[126]

1.3 INTRODUCTION TO INDIAN EVIDENCE ACT

The Indian Evidence Act, 1872 resulted in changes in the definition of evidence because of the IT Act 2000. These two acts are directly related to cyber forensics in India. Cyber forensics and related investigation procedures have also led to some amendments in IPC and CRPC. In many circumstances, IT Act is having an overriding effect over IPC and CRPC.[127]

With the help of evidence, facts related to the incident are established at trial. Indian Evidence Act contains a set of rule and related issues governing the admissibility of evidence in the Indian Courts of Law. It has introduced a standard set of law applicable to all Indians. This act is divided into 3 parts and there are 11 chapters in total.

PART 1

Part 1 deals with relevancy of the facts. There are two chapters under this part: the first chapter is a preliminary chapter which introduces to the Evidence Act and the second chapter specifically deals with the relevancy of the facts.

PART 2

[126] Shrivastava, Gulshan& Sharma, Kavita&Khari, Manju&Zohora, Syeda. (2018) Role of Cyber Security and Cyber Forensics in India

[127] Ahmad, Farooq, Cyber Law in India (Law on Internet), Pioneer Books

Part 2 consists of chapters from 3 to 6. Chapter 3 deals with facts which need not be proved, chapter 4 deals with oral evidence, chapter 5 deals with documentary evidence and chapter 6 deals with circumstances when documentary evidence has been given preference over the oral evidence.

PART 3

The last part, that is part 3, consists of chapter 7 to chapter 11. Chapter 7 talks about the burden of proof. Chapter 8 talks about estoppels, chapter 9 talks about witnesses, chapter 10 talks about the examination of witnesses, and the last chapter which is chapter 11 talks about improper admission and rejection of evidence.

The Evidence Act provisions can be divided into 2 categories:

- Taking the evidence (By Port) - This means to take the evidence for the facts. The fact means the things which are said before the court in connection with the matter. These facts are given to the court either orally or documentary (also electronic documents).[128]
- Evaluation – In evaluation court check whether the facts produce are capable to prove the evidence. Forensics plays a vital role in the evaluation phase.

1.4 AMENDMENTS TO INDIAN EVIDENCE ACT WITH RESPECT TO ELECTRONIC EVIDENCE

Indian evidence Act is applicable to criminal and civil cases. The evidence produce in these cases may belong to Digital Records. Whenever any Digital Record is submitted as evidence in a court of law many sections of Indian Evidence Act comes into the picture.

Following are certain amendments made in the evidence act for the legal recognition of electronic records as evidence.

AMENDMENTS TO THE INDIAN EVIDENCE ACT, 1872 (See section 92) [1 OF 1872]

1. IN SECTION 3,-

[128] André Årnes, 'Cybercrime Law', Published Online: 23 MAY 2017, DOI: 10.1002/9781119262442.ch3, Available at: <http://onlinelibrary.wiley.com/doi/10.1002/9781119262442.ch3/>

(a) in the definition of "Evidence", for the words "all documents produced for the inspection of the Court", the word "all document including electronic records produced for the inspection of the Court" shall be substituted;

(b) after the definition of "India", the following shall be inserted, namely :- the expressions; "Certifying Authority", "digital signature", "Digital Signature Certificate", "electronic form", "electronic records". "Information", "secure electronic record", "secure digital signature" and "subscriber" shall have the meanings respectively assigned to them in the Information Technology Act, 2000.

2. IN SECTION 17,

For the words "oral or documentary", the words "oral or documentary or contained in electronic form" shall be substituted.

3. AFTER SECTION 22,

The following section shall be inserted, namely: - relevant. Oral admissions as to the contents of electronic records are not relevant unless the genuineness of the electronic record produced is in question."

4. IN SECTION 34,

For the words ***"Entries in the books of account",*** the words ***"Entries in the books of account, including those maintained in an electronic form"*** shall be substituted.

5. IN SECTION 35,

For the word ***"record"*** in both the places where it occurs, the words ***"record or an electronic record"*** shall be substituted.

6. FOR SECTION 39,

The following section shall be substituted, namely: - "39. What evidence to be given when statement forms part of a conversation, document, electronic record, book or series of letters or papers.[129] When any statement of which evidence is given forms part of a longer statement, or of a conversation or part of an isolated document, or is contained in a document which forms part of a book, or is contained in part of electronic record or of a connected series of letters or papers, evidence shall be given of so much and no more of the statement, conversation, document, electronic record, book or series of letters or papers as the Court considers necessary in that particular case to the full understanding of the nature and effect of the statement, and of the circumstances under which it was made".[130]

7. AFTER SECTION 47,

The following sections shall be inserted, namely: - "47A.Opinion as to digital signature where relevant. When the Court has to form an opinion as to the digital signature or any person, the opinion of the Certifying Authority which has issued the Digital Signature Certificate is a relevant fact."

8. IN SECTION 59,

For the words ***"contents of documents"*** the words ***"contents of documents or electronic records"*** shall be substituted.

9. AFTER SECTION 65,

The following sections shall be inserted, namely: - 65A.special provisions as to evidence relating to the electronic record. The contents of electronic records may be proved in accordance with the provisions of section 65B i.e., ***Admissibility of electronic records.***[131]

(1) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further

[129] Caloyannides, Michael A, (2001), Computer Forensics and Privacy, Artech House <www.artechhouse.com>

[130] Casey, Eoghan (3rd Ed), Digital Evidence(Forensic Science, Computers & the Internet Computer Crime), Academic Press

[131] Justice Singh, Yatindra (2nd Ed), Cyber Laws, Universal Law Publishing Co Pvt Ltd

proof or production of the original, as evidence of any contents of the original or of any fact stated therein or which direct evidence would be admissible.

(2) The conditions referred to in sub-section (1) in respect of a computer outputshall be the following, namely:-

(a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;

(b) during the said period, information of the kind contained in the electronicrecord or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;

(c) throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and

(d) the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.

(3) Where over any period, the functions of storing or processing information for the purposes of any activities of any regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by a computer, whether-

(a) by a combination of computers operating over that period; or

(b) by different computers operating in succession over that period; or

(c) by different combinations of computers operating in succession over that period; or

(d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers. all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer, and references in this section to a computer shall be construed accordingly.

(4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say,-

(a) identifying the electronic record containing the statement and describingthe manner in which it was produced;

(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;

(c) dealing with any of the matters to which the conditions mentioned in subsection (2) relate, and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purpose of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

(5) For the purposes of this section,-

(a) information shall be taken to be supplied to a computer if it is supplied

thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;

(b) whether in the course of activities carried on by any official, information is supplied with a view to it is being stored or processed for the purposes of those activities by a computer-operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;

(c) a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

Explanation.- For the purposes of this section, any reference to information being derived from other information shall be a reference to its being derived therefrom by calculation, comparison or any other process;

10. AFTER SECTION 67,

The following section shall be inserted, namely: - "67A. Proof as to digital signature. Except in the case of a secure digital signature, if the digital signature of any subscriber is alleged to have been affixed to an electronic record the fact that such digital signature is the digital signature of the subscriber must be proved;"

11. AFTER SECTION 73,

The following section shall be inserted, namely: - "73A. Proofs as to verification of the digital signature. In order to ascertain whether a digital signature is that of the person by whom it purports to have been affixed, the court may direct-

(a) that person or the Controller or the Certifying Authority to produce the Digital Signature Certificate;

(b) any other person to apply the public key listed in the Digital Signature Certificate and verify the digital signature purported to have been affixed by the person.

Explanation.- For the purpose of this section "Controller" means the Controller appointed under sub-section (1) of section 17 of the Information Technology Act, 2000.

12. AFTER SECTION 81,

The following section shall be inserted, namely:- "81A. Presumption as to Gazettes in electronic forms. The Court shall presume the genuineness of every electronic record purporting to be the Official Gazette, or purporting to be electronic record directed by any law to be kept by any person if such electronic record is kept substantially in the form required by law and is produced from proper custody."

13. AFTER SECTION 85,

The following sections shall be inserted, namely: - "85A. Presumption as to electronic agreements. The Court shall presume that every electronic record purporting to be an agreement containing the digital signature of the parties was so concluded by affixing the digital signature of the parties. 85B. Presumption as to electronic record and digital signatures.

(1) In any proceedings involving a secure electronic record, the Court shall presume unless the contrary is proved, that the secure electronic record has not been altered since the point of time to which the secure status relates.

(2) In any proceedings, involving secure digital signature, the Court shall presume unless the contrary is proved that

(a) the secure digital signature is affixed by the subscriber with the intention of signing or approving the electronic record;

(b) except in the case of a secure electronic record or a secure digital signature, nothing in the section shall create any presumption relating to the authenticity and integrity of the electronic record or any digital signature. 85C. Presumption as to Digital Signature Certificates. The Court shall presume, unless the contrary is proved, that the information listed in a Digital Signature Certificate is correct, except for information specified as subscriber information which has not been verified, if the certificate was accepted by the subscriber."

14. AFTER SECTION 88,

The following section shall be inserted, namely:- 88A. Presumption as to electronic messages. The Court may presume that an electronic message forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission, but the Court shall not make any presumption as to the person by whom such message was sent. Explanation.- For the purposes of this section, the expressions ***"addressee"*** and ***"originator"*** shall have the same meanings respectively assigned to them in clause (b) and (za) of sub-section (1) of section 2 of the Information Technology Act, 2000;

15. AFTER SECTION 90,

The following section shall be inserted, namely: - "90A. Presumption as to electronic records five-year-old. Where any electronic record, purporting or proved to be five years old, is produced from any custody which the Court in the particular case considers proper, the Court may presume that the digital signature which purports to be the digital signature of any particular was so affixed by him or any person authorised by him in this behalf.[132]

Explanation.- Electronic records are said to be in proper custody if they are in the place in which, and under the care of the person with whom, they naturally be; but no custody is improper if it is proved to have had a legitimate origin, or the circumstances of the particular case are such as to render such an origin probable. This Explanation applies also to section 81A."

16. For section 131,

The following section shall be substituted, namely: - "131. Production of documents or electronic records which another person, having possession, could refuse to produce. No one shall be compelled to produce documents in his possession or electronic records under his control, which any other person would be entitled to refuse to produce if they were in his possession or control unless such last-mentioned person consents to their production."

1.5 EVIDENTIARY VALUE OF ELECTRONIC RECORDS

The evidentiary value of an electronic record is directly proportional to its quality. The Indian Evidence Act, 1872 has widely dealt with the evidentiary value of the electronic records.[133] According to section 3 of the Act, “evidence” means and includes all documents including electronic records produced for the inspection of the court and such documents are called documentary evidence. Thus the section clarifies that documentary evidence can be in the form of electronic record and stands at par with the conventional form of documents.

The evidentiary value of electronic records is elaborated under sections 65A and 65B of the Evidence Act, 1872. These sections provide that if the four conditions listed are satisfied

[132] Submitting an Email or Electronic Record <https://lawgic.info/submitting-an-email-or-electronic-record-as-evidence-in-an-indian-court/>

[133] Cyber Forensics & Electronic Evidences: Challenges <http://www.legalservicesindia.com/article/975/Cyber-Forensics-&-Electronic-Evidences:-Challenges-In-Enforcement-&-Their-Admissibility.html>

any information contained in an electronic record which is printed on paper, stored, recorded or copied in an optical or magnetic media, produced by a computer is deemed to be a document and becomes admissible in proceedings without further proof or production of the original, as evidence of any contacts of the original or any facts stated therein, which direct evidence would be admissible.

1.6 LET'S SUM UP

In this chapter, we have studied the relevance of Indian laws to cyber forensics along with the amendments that took place in the Indian Evidence Act with respect to Electronic evidence. Finally, we ended the discussion with the evidentiary value of electronic records.

1.7 FURTHER READING

- Rodriguez, Glen & Molina, Fernando. (2017). The preservation of digital evidence and its admissibility in the court. International Journal of Electronic Security and Digital Forensics. 9. 1. 10.1504/IJESDF.2017.10002624.
- Medcraveonline.com (2019), http://medcraveonline.com/FRCIJ/FRCIJ-04-00109.pdf (last visited Nov 26, 2019).
- https://www.ncjrs.gov/pdffiles1/nij/211314.pdf
- https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf

1.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **How does evidence help in a case?**

With the help of evidence, facts related to the incident are established at trial. Indian Evidence Act contains a set of rule and related issues governing the admissibility of evidence in the Indian Courts of Law.

2. **What are the 2 divided categories of the provisions of Evidence Act?**

The Evidence Act provisions can be divided into 2 categories:

- Taking the evidence (By Port) - This means to take the evidence for the facts. The fact means the things which are said before the court in connection with the matter. These facts are given to the court either orally or documentary (also electronic documents).
- Evaluation – In evaluation court check whether the facts produce are capable to prove the evidence. Forensics plays a vital role in the evaluation phase.

3. What does the evidentiary value of electronic records mean?

The evidentiary value of an electronic record is directly proportional to its quality. The Indian Evidence Act, 1872 has widely dealt with the evidentiary value of the electronic records. According to section 3 of the Act, "evidence" means and includes all documents including electronic records produced for the inspection of the court and such documents are called documentary evidence. Thus the section clarifies that documentary evidence can be in the form of electronic record and stands at par with the conventional form of documents.

1.9 ACTIVITY

Elucidate the amendments made in the Indian Evidence Act with respect to electronic evidence also briefly explain the admissibility of electronic records with relevant case laws? (1000 – 1500 words)

Unit 3: Cyber Forensics Labs and Challenges before Law Enforcement Agencies

3

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- The requirement for cyber forensics lab and how to build it.
- The details of examiner of electronic evidence by government of India.
- Computer Emergency Response Team India.
- Challenges before law enforcement agencies in India while investigation.
- Dark web and how Law enforcement deals with it.

1.2 INTRODUCTION TO CYBER FORENSIC LABS

Cyber Forensic lab is a facility where digital evidences are examined, analysed and the forensic report is been produced. There is a specific way to establish a cyber-forensic facility. Let's discuss certain points which are taken into consideration for setting up a cyber-forensic lab.

1.3 CYBER FORENSIC LAB STRUCTURE

- **LAB SPACE**

  The cyber forensic facility should be located at secured premises. The facility should not be congested and should have enough working space. There should be adequate and uninterrupted electricity. The forensic lab should have an effective cooling system without any humidity present inside the lab. There should be good internet connectivity at high speed. There should be enough desk and benches with the antistatic floor. There should be a lock for every room with an access control mechanism to prevent unauthorised access.[134]

- **REQUIRED EQUIPMENTS**

  There should be multiple hardware write blockers which supports all types of connectivity. E.g. SATA, Firewire, USB etc. There should be a high configuration computer system with the fastest speed of processing. There should be multiple good monitor. The forensic lab should have hardware filled kit. There should be enough blank hard disk and storage container which is called as evidence vault. There should be all sort of data and power cables with static bags. There should be enough supplies of packaging and labelling material. For network connectivity, there should be enough networking devices.

- **APPROPRIATE SOFTWARE**

  Forensic lab requires different types of software for different analysis purpose. There are a few examples like Encase, Accessdata FTK, Net force suit, Oxygen mobile forensic, Passware password recovery, Helix live CD etc.

[134] meity.gov.in. <https://meity.gov.in/writereaddata/files/annexure-i-pilot-scheme-for-notifying-examiner-of-electronic-evidence-under-section-79a-of-the-information-technology-act-2000.docx>

- **CYBER FORENSIC EXPERT**

  The cyber lab requires a team of cyber forensic expert with detailed knowledge of computing technology. These experts should be certified for the software and hardware installed in a forensic lab. These experts should have experience of expert witness testimony at court trials.

- **SOP(STANDARD OPERATING PROCEDURE)**

  There should be an established set of policies and procedures to be followed in a forensic lab for different purposes. E.g. wearing gloves before handling any evidence etc.

  There should be standard and approved format to prepare a chain of custody form. Examination notes, observation, finding and reports etc.

- **TRAINING AND UPGRADATION**

  To cop up with changing technology, the experts working with the forensic lab should undergo training every six months. The hardware and software used for the forensic examination should be upgraded as per requirement.

  The cyber forensic lab is a dedicated facility to carry out a forensic examination of digital evidence. These labs are mainly setup by government centrally and state wise.

1.4 EXAMINER OF ELECTRONIC EVIDENCE

The Information Technology Act, 2000 empowers the Central Government under section 79A to notify any Department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence for the purposes of providing expert opinion on electronic form evidence before any court or other authority specified by notification in the Official Gazette. The Explanation clause of section 79A further articulates that the “Electronic Form Evidence” means any information of probative value that is either stored or transmitted in electronic form and includes evidence, digital data, digital video, cell phones, digital fax machine etc.[135]

a) In line with the above requirement, MeitY has formulated a scheme for notifying the Examiner of Electronic Evidence. The objective of the scheme is to ascertain the competence of all the desiring Central Government or a State Government agencies and to qualify them to act as Examiner of Electronic evidence as per their scope of approval through a formal accreditation process. Once notified, such Central, State Government agencies can act as the "Examiner of Electronic Evidences", and provide an expert opinion of digital evidence before any court.

The scheme is based on international standards like ISO/IEC 17025 (A Standard on General requirements for the competence of testing and calibration laboratories) and ISO/IEC 27037 (A Standard on Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence). The evaluation process includes an examination of the technical, skilled professional manpower in digital forensics, licensed tools and equipment, availability of suitable environment to carry out such evaluation as also the availability of a proper quality management system and reasonable experience to demonstrate their overall competency in this area.

Following is the listed lab of government as Examiner of Electronic Evidence

1. Cyber Forensic Laboratory, Army Cyber Group, DGMO, Signals Enclave, New Delhi
2. State Forensic Science Laboratory, Madiwala, Bangalore
3. Central Forensic Science Laboratory(CFSL), Hyderabad
4. Directorate of Forensic Science, Gandhi Nagar Gujarat
5. Computer Forensic and Data Mining Laboratory (CFDML), Serious Fraud Investigation Office (SFIO),
6. Notification of Forensic Science Laboratory Govt of NCT, Rohini New Delhi

1.5 INTRODUCTION TO COMPUTER EMERGENCY RESPONSE TEAM INDIA (CERT-In)

[135] The Impact of Technology on Organized Crime<https://www.sydneycriminallawyers.com.au/blog/the-impact-of-technology-on-organised-crime/>

CERT-In is a government body working under the ministry of electronics and information technology.It is operational since 2004. CERT-In is a national nodal industry responding to the computer security incident as and when they occur. As per the amendment in IT Act, CERTIN has been designated to serve the following functions in the area of cybersecurity as a national agency.[136]

- Collection analysis and examination of cyber incident.
- Forecast and alert cybersecurity incident.
- Co-ordination of cybersecurity responsibilities.
- Emergency measures for handling cybersecurity incidents.
- Issue guideline advisory, notes, whitepapers related to information security practices, procedures, preventions, response and reporting of cyber incidents.

CERTIN not only provides incident response services but also security quality management services. CERTs vision is to proactively contribute to securing cyberspace for India. CERTs mission to enhance the security of India's technology infrastructure through pro-active actions and effective collaborations. CERTIN has signed a memorandum of understanding with 7 countries of Shanghai Co-operation Organisation. With this MOU, participating countries can exchange technical information on cyber-attacks, incident response and solution to counter global cyber-attacks.

1.6 OBJECTIVES OF CERT-In

- Preventing cyber-attacks against the country's cyberspace.
- Enhancing security awareness among common citizen.
- Responding to cyber-attacks and minimizing the damage as well as recovery time.

CERTIN function on 24 hours basis on all days of the year including government and other holidays. The contact details of CERTIN are published on website www.cert-in.org.in

[136] Nouh, Mariam & Nurse, Jason & Webb, Helena & Goldsmith, Michael (2019) Cybercrime Investigators are Users Too! Understanding the Socio-Technical Challenges Faced by Law Enforcement

Following are the types of cybersecurity incident need to be reported to CERTIN

- Targeted scanning of critical network systems.
- Compromise of critical system information.
- Unauthorized access to IT systems.
- Defacement of website or intrusion of the website.
- Malicious code attacks such as spreading virus, worm, Trojan, botnet, spyware etc.
- Attacks on the server such as database, mail and DNS.
- Identity theft, spoofing phishing attacks.
- Denial of service and distributed denial of service attacks.
- Attack on critical infrastructure, SCADA systems and wireless networks.
- Attacks on applications such as e-commerce and e-governance.

1.7 CHALLENGES BEFORE LAW ENFORCEMENT AGENCIES

As technology has brought lots of many changes into every organization, Law enforcement agencies (LEA) are not the exception for it.[137] Many LEAs are going under transformation and still in the adoption phase for this technological advancements. Make in India and Digital India is the current era for our country. But we are still in the process of replacing traditional ways while these positive changes around us. This has created a crucial challenge in the field of investigations as well. Let's understand the real situation and challenges faced by LEA in this digital era.

1.8 CHALLENGES WHILE INVESTIGATION

Due to the use of technology by criminals in their act the speed of execution of any crime has increased a lot.[138] LEA has to compete with the speed of the fraudster. Criminals are real users of advanced technology and find out many new technological ways to commit crimes. LEA's challenges start from understanding the use of technology by criminals in the given scenario.

[137] S W Brenner Cybercrime: Criminal Threats from Cyberspace, 2nd Edition. Praeger Security International. ABC-CLIO, LLC, 2018

[138] Hunton, PaulManaging the technical resource capability of cybercrime investigation.A UK law enforcement perspective. Public Money &Management, 32(3):225–232, 2012

Let’s divide the changes faced by LEA into 3 categories:-

1) ***Pre Investigation***

a) Not clear Understanding of the Jurisdictions:-

Due to jurisdictional issues of the cyberspace, many Investigation officers are not clear about who should investigate the scenario which involves different geographically distant location. For example, Person who is living in Bangalore who is over business trip in Pune receives the SMS which says his debit card is used in Delhi and his bank belongs to Chennai. Such a Situation confuse the Investigation officer that which state investigation agency is the right authority to investigate the given situation.

b) Lack of technological background

Nowadays, Criminals are using technology not only in cybercrimes but also in traditional crimes.IO are mainly Police Inspectors which may not be from a technical background. It becomes very difficult for them to understand the overall situation and that’s why it affects the speed of execution

2) ***During Investigation***

A. Lack of technological expertise
B. Availability of the required equipment’s
C. Absence of standard operating procedures for investigation
D. In Adequate expert witness

3) ***During Court trials***

- Cross border investigation
- Admissibility of electronic evidence
- Hash Value calculation

One challenge computer investigators face is that while computer crimes know no borders, laws do. What's illegal in one country may not be in another. Moreover, there are no standardized nternational rules regarding the collection of computer evidence. Some countries are trying to change that. [139]

1.9 DARK WEB (DARKNET)

The dark web, which is also called a darknet, is an encrypted portion of the internet which cannot be indexed by search engines. It is purposefully created portion of the internet which is not for public view.In order to access the dark web, the special anonymous browser is used. Websites on the dark web have an unconventional naming structure. Hence, anyone who wants to access such websites needs to know them in advance.

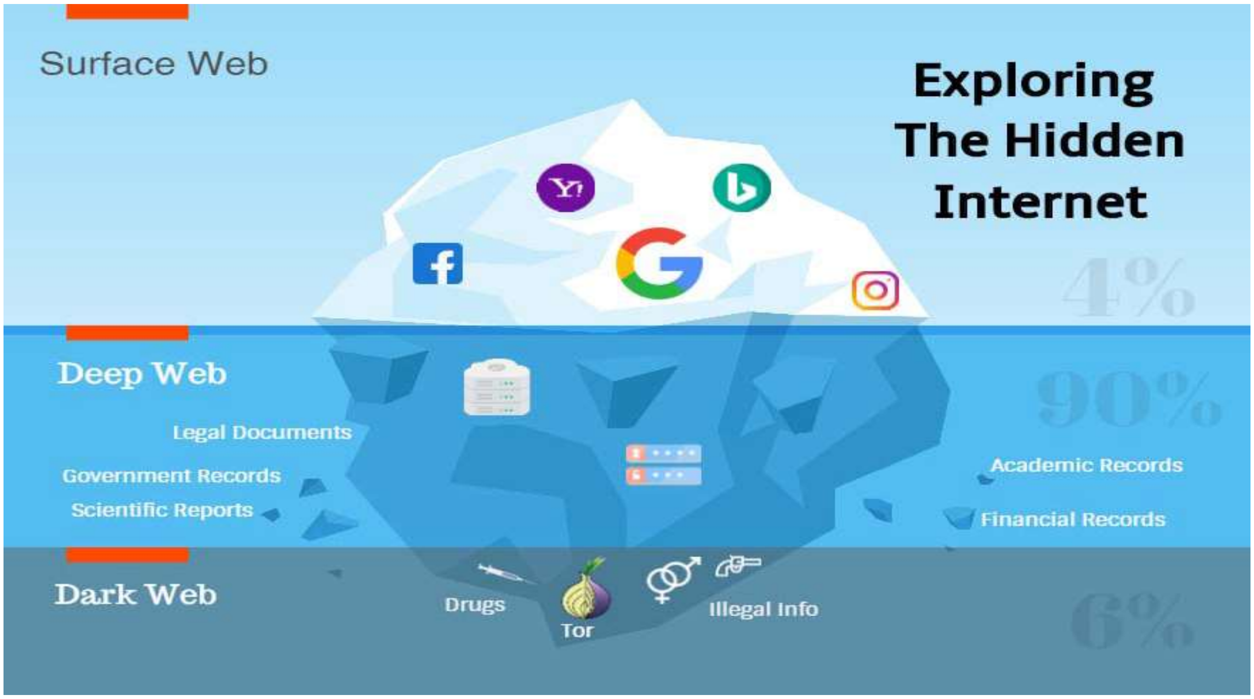


Figure 4.1:- The Internet is like an iceberg where most of the people can see only the surface and majority of the portion stays hidden.

The World Wide Web is considered as an iceberg, in which the regular sites that common people visit isthe top layer of the iceberg. This includes common sites such as Wikipedia, Google and

[139] Scott R Senjo An analysis of computer-related crime: Comparing police officer perceptions with empirical data. Security Journal, 17(2):55–71, 2004

even the millions of blogs that come and go daily. This portion is just 4% of the overall internet is known as surface web.[140]

Then it comes the portion of the deep web in which personal records, government documents and confidential information which are not meant for public view and are understandably kept safe. This information forms an ecosystem for many surface web applications. Hence, they are many times directly connected to the surface web. In order to dive into the Deep web pages one has to know that URL beforehand.[141]

The dark web is the underworld of the internet. It is the subsection of the deep web. But if anyone who is seeking access to Dark web pages, requires special software with the correct decryption key, as well as access rights and knowledge of where to find the content. The Dark Web is slightly more complicated because most of the times it runs on networks of the private servers, allowing communication only via specific means. This enables a high degree of anonymity and makes it difficult for authorities to shut down or monitor it.

If a cyber-attacker hacks into your organization and exfiltrates valuable business information such as customer records, or a disgruntled insider decides to try and sell some stolen intellectual property, they will simply prefer the dark web.

Unfortunately, the highest amount of anonymity and privacy has led to Dark Web to become a place where many illegal activities take place.[142]

DARK WEB BROWSER

Accessing the dark web requires the use of an anonymizing browser which is called Tor. It is free software that users download from the Internet to anonymously access the dark web.

Thousands of volunteers around the globe host and operate series of proxy servers through which tor browser routes the webpage request, rendering the real IP address unidentifiable and untraceable.

[140] Michael Chertoff and Toby Simon, The Impact of the Dark Web on Internet Governance and Cyber Security, Global Commission on Internet Governance, Paper Series: No 6, February 2015, p 1

[141]Verisign, The Domain Name Industry in Brief, Volume 13, Issue 3, September 2016. A top-level domain is one at the top of the Internet's domain name system (DNS) hierarchy. For instance, the top-level domain is .com

[142] Stephanie Pappas, "How Big Is the Internet, Really?," Live Science, February 18, 2016

This process works well for the anonymity and privacy of the user, the Tor browser experience is typically unreliable and slow. One does not have direct control over his surfing because it is routed through different server hence use of credential seems to be unreliable via such service.

DARK WEB WEBSITES

The websites which are hosted over the surface web have ended in .com or other common suffixes, but the dark web URLs typically end in .onion which is a special-use domain suffix. Dark web sites are not easy to remember as well because of its URLs are a mix of letters and numbers. For example, one of the most infamous dark web marketplaces was the Silk Road, best known for selling illegal drugs that was eventually busted by the FBI which went by the URLs silkroad6ownowfk.onion and silkroad7rn2puhj.onion.

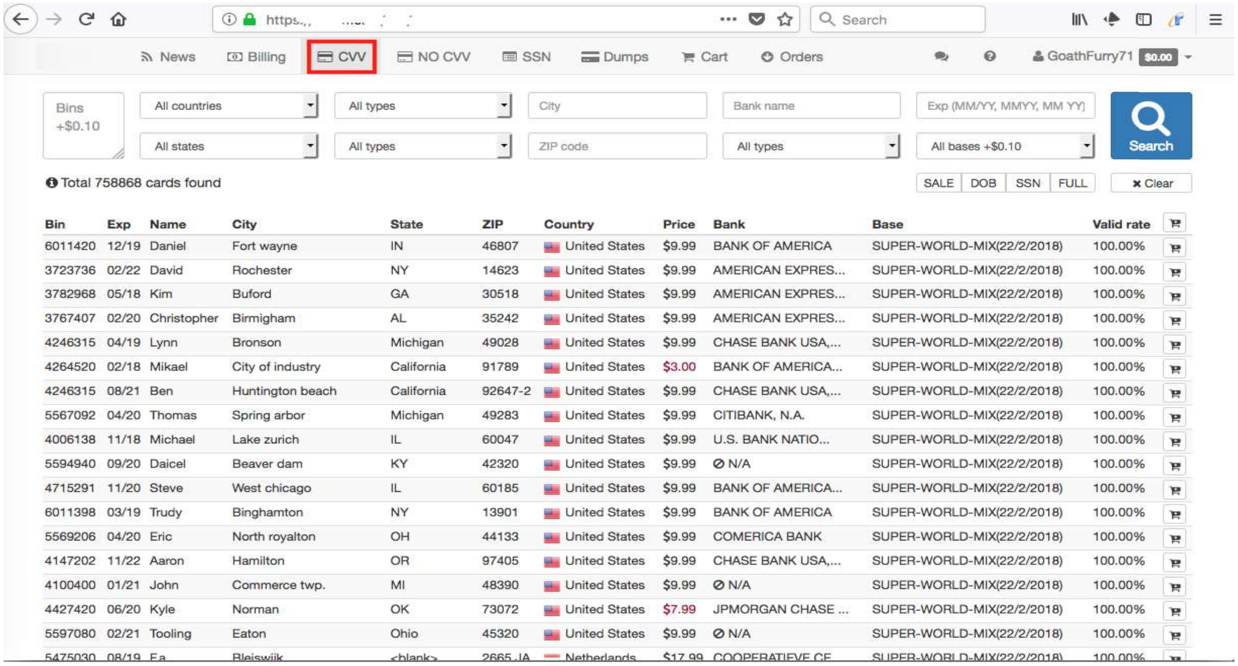
WHAT YOU CAN DO AT DARKNET?

As darknet is famous for anonymous surfing one can buy credit card numbers, all types of drugs, guns, counterfeit money, stolen subscription credentials, hacked subscription like Netflix accounts and software that is created and used by criminals to break into someone’s computer. One can buy login credentials to a $50,000 Bank of America account for $500 or get $3,000 in counterfeit $20 bills for $600. One can buy illegal drugs with express shipping included in it. One can hire a hacker to attack computers for you. One can buy a lifetime subscription for Netflix account or pornographic websites just for 6$. One can buy usernames and passwords of business rivals.[143]

Hence, more legitimate companies are beginning to have a presence on the dark web. The cryptocurrency is very much useful for the users who can purchase anything on the dark web without revealing their identity.

Darknet acts as freedom which is given at large to do whatever you want without being identified. This thing provokes the criminal intentions of the person to strongly come out and to be followed by one.

[143] Andy Greenberg, “An Interview with Darkside, Russia’s Favorite Dark Web Drug Lord,” Wired.com, December 4, 2014



Total 758868 cards found

Bin	Exp	Name	City	State	ZIP	Country	Price	Bank	Base	Valid rate
6011420	12/19	Daniel	Fort wayne	IN	46807	United States	$9.99	BANK OF AMERICA	SUPER-WORLD-MIX(22/2/2018)	100.00%
3723736	02/22	David	Rochester	NY	14623	United States	$9.99	AMERICAN EXPRES...	SUPER-WORLD-MIX(22/2/2018)	100.00%
3782968	05/18	Kim	Buford	GA	30518	United States	$9.99	AMERICAN EXPRES...	SUPER-WORLD-MIX(22/2/2018)	100.00%
3767407	02/20	Christopher	Birmigham	AL	35242	United States	$9.99	AMERICAN EXPRES...	SUPER-WORLD-MIX(22/2/2018)	100.00%
4246315	04/19	Lynn	Bronson	Michigan	49028	United States	$9.99	CHASE BANK USA,...	SUPER-WORLD-MIX(22/2/2018)	100.00%
4264520	02/18	Mikael	City of industry	California	91789	United States	$3.00	BANK OF AMERICA...	SUPER-WORLD-MIX(22/2/2018)	100.00%
4246315	08/21	Ben	Huntington beach	California	92647-2	United States	$9.99	CHASE BANK USA,...	SUPER-WORLD-MIX(22/2/2018)	100.00%
5567092	04/20	Thomas	Spring arbor	Michigan	49283	United States	$9.99	CITIBANK, N.A.	SUPER-WORLD-MIX(22/2/2018)	100.00%
4006138	11/18	Michael	Lake zurich	IL	60047	United States	$9.99	U.S. BANK NATIO...	SUPER-WORLD-MIX(22/2/2018)	100.00%
5594940	09/20	Daicel	Beaver dam	KY	42320	United States	$9.99	⊘ N/A	SUPER-WORLD-MIX(22/2/2018)	100.00%
4715291	11/20	Steve	West chicago	IL	60185	United States	$9.99	BANK OF AMERICA...	SUPER-WORLD-MIX(22/2/2018)	100.00%
6011398	03/19	Trudy	Binghamton	NY	13901	United States	$9.99	BANK OF AMERICA	SUPER-WORLD-MIX(22/2/2018)	100.00%
5569206	04/20	Eric	North royalton	OH	44133	United States	$9.99	COMERICA BANK	SUPER-WORLD-MIX(22/2/2018)	100.00%
4147202	11/22	Aaron	Hamilton	OR	97405	United States	$9.99	CHASE BANK USA,...	SUPER-WORLD-MIX(22/2/2018)	100.00%
4100400	01/21	John	Commerce twp.	MI	48390	United States	$9.99	⊘ N/A	SUPER-WORLD-MIX(22/2/2018)	100.00%
4427420	06/20	Kyle	Norman	OK	73072	United States	$7.99	JPMORGAN CHASE ...	SUPER-WORLD-MIX(22/2/2018)	100.00%
5597080	02/21	Tooling	Eaton	Ohio	45320	United States	$9.99	⊘ N/A	SUPER-WORLD-MIX(22/2/2018)	100.00%
5475030	08/19	Ea	Bleiswijk	<blank>	2665 JA	Netherlands	$17.99	COOPERATIEVE CE	SUPER-WORLD-MIX(22/2/2018)	100.00%

Figure 4.2:- stolen card details are sold in the underground market on the Internet.

DARKNET USERS

Out of the billions of internet users accessing the internet on an everyday basis, Dark Web use remains around 3 percent. Because of the nature of stuff over the dark web, one can easily understand that the dark web is mainly used by criminals, terrorist and activist but that is not the only case.[144]

The ethical use of the dark web is done by law enforcement or threat intelligence agencies. Security professionals may search through the dark web for signs of security or data breaches, evidence of illegal activity or newly emerging cyber threats. The dark web also hosts a large amount of educational information that cannot be found elsewhere, such as banned books, collections of news articles and discussion forums.

DANGERS OF THE DARK WEB

[144] Beshiri, Arbër&Susuri, Arsim (2019) Dark Web and Its Impact in Online Anonymity and Privacy: A Critical Analysis and Review. Journal of Computer and Communications.

Accessing the dark web and using the tools or services found there, can be associated with high risks for an individual user or an enterprise. A few dangers that users should be aware of before browsing the dark web includes:

- Unknown Infection of viruses or malware especially ransomware,
- Installation of spyware such as key loggers.
- Infection of the system with Remote access tools (RAT) with new signatures.
- Distributed denial of service (DDoS) attacks.
- Identity theft, credential theft or phishing.
- Compromise of personal, customer, financial or operational data.
- Leaks of your own intellectual property or trade secrets.
- Spying, webcam hijacking or cyberespionage.

DARK WEB FROM LAW ENFORCEMENT VIEW POINT

Use of the dark web brings in unique challenges for law enforcement agencies in India. The law enforcement officer feels that if there were some police presence on the dark web, they will be in a better position to deal with the possible attack. Cyber experts say that some officers go undercover on the dark web to keep track of illegal activities going on there. That monitoring the dark web can help to boost cybersecurity, identify breaches and vulnerabilities. An officer said that prior to the Cosmos Bank fraud in Pune in which Rs 94 crore was fraudulently transferred from the bank, there was chatter on the dark web about people looking for details on Indian banks. This shows the Indian LEA officers mainly believes gathering evidence on the dark web activity is comparatively difficult but not impossible.[145]

In order to combat with such highly technical types of criminal activities, there is a need for police officers to be trained in changing cyber trends who are dedicated only to cyber-crime and not transferred to other police units. Hence, this leaves us with the hope that the expert criminals

[145] Dilipraj, E (2014) Terror in the Deep and Dark Web. 9. 121-140

cannot permanently hide in places like darknet and they are under radar even they stay in this underworld of the internet.

1.10 LET'S SUM UP

In this chapter, we have studied about the cyber forensic labs and the structure of it. We also studied about Computer emergency response team India and its objectives. Finally, we ended the discussion with the Dark web and challenges while investigation.

1.11 FURTHER READING

- Saran, Vaibhav& A.K.GUPTA,. (2014). Cyber Crime & Their Forensic Investigation.
- Yeboah-Boateng, Ezer&Akwa-Bonsu, Elvis. (2016). Digital Forensic Investigations: Issues of Intangibility, Complications and Inconsistencies in Cyber-crimes. Journal of Cyber Security and Mobility. 4. 87-104. 10.13052/jcsm2245-1439.425.
- Ficci.in (2019), http://ficci.in/spdocument/22982/FICCI%20-%20EY%20Report%20-%20Confronting%20the%20New%20Age%20Cyber%20Criminal.pdf (last visited Nov 27, 2019).
- Digitalcommons.law.scu.edu (2019), https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1219&context=scujil (last visited Nov 27, 2019).

1.12 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **Summarize about cyber forensic lab structure?**

- Lab Space
- Required Equipments
- Appropriate Software
- Cyber Forensic Expert

- SOP(Standard Operating Procedure)
- Training and upgradation

2. What is CERT-In?

CERT-In is a government body working under the ministry of electronics and information technology.It is operational since 2004. CERT-In is a national nodal industry responding to the computer security incident as and when they occur.

3. What are the objectives of CERT-In?

- Preventing cyber-attacks against the country's cyberspace.
- Enhancing security awareness among common citizen.
- Responding to cyber-attacks and minimizing the damage as well as recovery time.

4. What is the Dark Web?

The dark web, which is also called a darknet, is an encrypted portion of the internet which cannot be indexed by search engines. It is purposefully created portion of the internet which is not for public view.In order to access the dark web, the special anonymous browser is used. Websites on the dark web have an unconventional naming structure. Hence, anyone who wants to access such websites needs to know them in advance.

1.13 ACTIVITY

Briefly explain what is dark web, how it is being used and the dangers pertaining to it? Elucidate the illicit activities that has been taking place via the dark web with a case study? (1000 words)

Unit 4: Mobile Network Investigations

4

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Mobile Network Technology
- Types of evidence
- How data may be acquired

1.2 INTRODUCTION

The use of mobile devices is increasing rapidly, with devices like the BlackBerry, iPhone, and G1 providing a wide variety of services, including communication (e.g., voice, SMS, e-mail), Internet access (web browsing), and satellite navigation (GPS). These technological advances create new opportunities for criminals while providing valuable sources of evidence. The bombs in the 2004 train bombings in Madrid apparently used cellular telephones as timers. The terrorists in the recent Mumbai attacks communicated using satellite telephones. Drug dealers and organized criminals are heavily dependent on inexpensive prepaid cellular telephones that are essentially anonymous and disposable.[146]

Mobile network investigations are also commonly performed for “conventional crimes,” often focusing on location information, logs of telephone calls, printouts of SMS messages, and associated metadata.A mobile device is generally defined as any instrument that can connect to and operate on a mobile network, including cellular telephones, wireless modems, and pagers.

1.3 MOBILE NETWORK TECHNOLOGY

In the late 1980s, the mobile telephony system in Europe was based exclusively on the ETACS network created by various telephone companies and consisting of analog radio links operating at the frequency of 800 MHz. Although at the time it was considered to be the start of a revolution, few would have imagined how quickly the phenomenon would burgeon both into a fad and into a system for keeping close track of individuals.

The weak points of the ETACS network were the lack of coverage abroad, continuing interference with other users, and the ease of cloning. It often happened that some unknown party obtained possession of the serial number of a mobile device, combined it with a new account to elude the NSP and generated telephone traffic paid for by the unwitting victim. In the mid-1990s, the GSM network was introduced. It operated at a frequency of 900 MHz and later 1.8 GHz. GSM was introduced precisely to eliminate once and for all the problem of interference among radio links and, being digital, to make conversations more secure.[147]

The next revolution in mobile network technology came about in 2003 when the Japanese colossus Hutchinson Whampoa entered the European market with H3G, the third generation of mobile telephony. The telephone now became a video-telephone, using the 2.1 GHz band.In the

[146] Curran, Kevin & Robinson, Andrew &Peacocke, Stephen & Cassidy, Sean (2010) Mobile Phone Forensic Analysis
[147](Bucks.edu, 2020)
<https://www.bucks.edu/media/bcccmedialibrary/con-ed/itacademy/IntroToMobileForensics.pdf>

area of electronic communication services, it is necessary to distinguish between “telephony” and “telematic” services.

TELEPHONY	TELEMATIC
Telephone calls, including voice calls, voice messaging, conference calls, and data transmitted via telefax.	Internet access, E-mail.
Supplementary services, including call forwarding and call transfers	Fax, SMS and MMS messages via the Internet
Messaging and multimedia services, including SMS services	Telephony via Internet (Voice over Internet Protocol-VoiP)

A mobile device begins to leave its traces on the mobile network the moment it is turned on. When a device is powered on, it announces itself to the mobile network, generating a refresh of the authentication process. Like every technical device, a mobile device also releases technically sensitive information.[148] For example, an International Mobile Subscriber Identity (IMSI) is essentially a unique number that is associated with a particular subscriber on a GSM or UMTS mobile network. The IMSI is stored on the SIM card in a mobile device and is used to authenticate the device on the mobile networkand to control the other details such as HLR (Home Location Register) or copied locally in the VLR (Visitor Location Register). In order to avoid interception of this sensitive number, the IMSI is not directly sent over the network. It is substituted by a TMSI (Temporary Mobile Subscriber Identity), which is a temporary number, usually created for a single session. At the request of digital investigators, NSPs can use these unique identifiers to query their systems for all activities relating to a particular subscriber account.[149]

1.4 INVESTIGATIONS OF MOBILE SYSTEMS

Investigations used to be carried out exclusively by people. In the pure spirit of investigation, you started from information obtained through an undercover agent followed by operations

[148] ACPO (2009) Practice Guide for Computer-Based Electronic Evidence, (2009), <www.acpo.police.uk/asp/policies/Data/ACPO%20Guidelines%20v18.pdf>

[149]Gratzer,V, Naccache, D., Znaty, D (2006) Law Enforcement, Forensics and Mobile CommunicationsPerCom Workshop, Pisa - Italy, 13-17 March 2006, pp: 256-260

involving trailing suspects and intercepting ordinary mail. Without the help of technological systems, these investigations tended to last much longer than their more modern counterparts.[150]

Today, the initiation of an investigation may involve, in addition to verbal information, an anomalous bank record, an image from a surveillance camera, or of course highly visible crimes such as theft or murder.

The first phase of the investigation involves interviewing people who may have relevant information and continues with monitoring the means of communication of suspects or others associated in some way with the case. In addition to the traditional telephone, there are other monitoring points such as electronic mailboxes, places visited by the suspect, Telepass accounts (devices used for automatic highway toll payment), credit card accounts, and other financial operations.

Nowadays, investigations are supported by software that is customized to meet different requirements. The investigator enters all the data available on a subject into the interception system, and the server performs a thorough analysis, generating a series of connections via the mobile devices involved, the calls made or received, and so on, providing criminal police with a well-defined scheme on which to focus the investigation, and suggesting new hypotheses or avenues that might otherwise be hard to identify. Thanks to the support of the NSP, the data can be supplemented with historical information or other missing data such as other mobile devices connected to a given BTS on a given date and time. Data can also be provided for public payphones, which are often used to coordinate crimes. Again, thanks to a connection with the NSP, it ispossible to obtain a historical record of telephone calls made and the location of the payphone with respect to other mobile devices. The same sort of record may also be obtained for highway travel using Telepass (the conventional name for automatic wireless toll payment), including average speed and stops.[151]

Having historical data of various kinds relating to an investigation accessible in a database can greatly assist the initial examination of a newly acquired mobile device. By extracting all

[150]Harrill, D C, Mislan, R. P. (2007) A Small Scale Digital Device Forensics ontology, Small Scale Digital Device Forensics journal, Vol 1, No 1, June 2007

[151] McCarthy, P. (2005) Forensic Analysis of Mobile Phones <http://esm.cis.unisa.edu.au/new_esml/resources/publications/forensic%20analysis%20of%20mobile%20phones.pdf>

telephone numbers in the phonebook of a mobile device seized during a search and entering names and numbers into the electronic system, digital investigators perform powerful analysis even in the initial phases of the investigation thanks to cross-referencing capabilities.

1.5 TYPES OF EVIDENCE

Mobile networks can provide information of relevance to an investigation, including the location of a mobile device, the past usage associated with a particular device or subscriber, as well as the context of communications.[152]

- ***Localization Parameters***

The term localization parameters describe the information that can be combined to localize an active mobile device and its related user. These localization parameters can be useful to track the position of a mobile device user, for several purposes, both for prosecution and defense.

- ***Determining the position of a given mobile device***

The simple act of turning on a device and leaving it in an idle state will generate data on the network that can be used to determine its approximate location. As a mobile device is moved from one location to another, it updates the network. Speaking, there is a timeframe where the mobile device “announces” itself to the network. The possible alternatives as follows:

a) Cell identification

The mobile device can be reached by looking at the cell to which it is currently connected. There is a range of accuracy that starts from a few hundred meters in urban areas, up to 32 km in suburban areas and rural zones. The accuracy depends on the known range of the particular base station serving the mobile device at the time of positioning. The poor value of 32 km can be enhanced with the use of the so-called Enhanced Cell Identification (general accuracy of 550 meters).

b) Time difference of arrival (TDOA)

[152] McCarthy, P and Slay, J (2006) Mobile phones: admissibility of current forensic procedures for acquiring data. In Proceedings of the Second IFIP WG 11.9 International Conference on Digital Forensics, 2006

This method also referred to as multilateration, measures the time it takes for a signal to travel from a mobile device to multiple base stations to estimate the device location. “It is a method commonly used in civil and military surveillance applications to accurately locate an aircraft, vehicle or stationary emitter by measuring the time difference of arrival (TDOA) of a signal from the emitter at three or more receiver sites.”

c) Time of arrival (TOA)

This approach is effectively the same as TDOA, but this technology uses the absolute time of arrival at a certain base station rather than the difference between multiple stations.

d) Enhanced Observed Time Difference (E-OTD)

This method is similar to TDO, but in this case, the position is calculated by the mobile device, not the base station. In essence, the mobile device receives signals from multiple base stations at the same time that a specially placed receiver receives the signals. The precision of this method can vary from 50 to 200 m.

e) Assisted-GPS

A third-party service that generally relies on Cell Identification.

Determining the location of a mobile device can be important for assessing alibis of suspects or the whereabouts of victims in the past, and ongoing tracking of the location can be useful in cases of abduction, missing persons, and other ongoing criminal activities.[153]

From a practical perspective, there are tools that perform these techniques and display the results for digital investigators. Some of the information transmitted by the NSP to a monitoring centre is the position on the basis of cell and the IMSI code. This is extremely important information in that it makes it possible to track the people responsible for serious crimes as they move.

- ***Remote Activation of Electronic Devices***

Once, organized crime just used old-fashioned weapons. Now, with a mobile device and an Internet connection many more crimes can be committed. From the massacres of the 1990s to the latest terrorist attacks, mobile devices have played a fundamental role in the organization

[153] National Institute of Standards and Technology (2007) Guidelines on cell phone forensics, <http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf>

ofcrimes. With a ring or an SMS containing a code, it is possible to activate or deactivate an electronic device in any part of the world. This is why the ability to trace an SMS or even a simple ring signal is particularly important, along with the refinement of technology for capturing any signal or use, even if innocuous, of mobile phones.[154]

Unfortunately, organized criminal groups, having considerable financial resources, enjoy various advantages in terms of budget and decision-making speed in undertaking countermeasures to thwart the various investigation and law-enforcement bodies. They hire experts in technology as well as researchers who spend their days seeking out the latest solutions in terms of protection.

When criminal figures meet for business, they often protect their privacy by jamming signals in the area around their meeting place. This prevents mobile devices from linking to the BTS and thus connecting to the network. This prevents investigators from connecting to the cell and getting an idea of the geographical location of the meeting. The jamming mechanism also temporarily interrupts the operation of mobile phones in the area that might represent a threat of interception.

A mobile device jamming system emits a signal to prevent the use of mobile phones within a certain radius. It emits a wideband radio signal at the same frequency range used for transmitting signals from the BTS to the mobile phones. This signal prevents the mobile device from decoding the network signal and thus causes the mobile device to disconnect from the network.

- ***Usage Logs/Billing Records***

The logs maintained by an NSP can help digital investigators determine past usage of a mobile device, as well as communications between individuals. These logs are generated from Call Detail Records (CDR) maintained for billingpurposes. The data in the resulting logs that are commonly provided to investigators are summarized here:

- Telephone number of user
- Numbers called
- IMEI number of mobile device

[154] Punja, S, Mislan, R (2008) Mobile Device Analysis, Small scale digital device forensics journal, Vol 2, No 1, pp: 1-16, June 2008, ISSN: 1941-6164

- Information about the cell: provides information about the location of the calling phone on the basis of the BTS where the connection was made
- SMS sent: excluding the text, which is available only via decodification using a telephone signal interception system.
- Date, time, and duration of calls

Depending on the equipment used, the logs generated on a particular mobile network may include a variety of other details.The Oracle Communications Services Gatekeeper is used by many NSPs world-wide for service delivery platform (SDP) infrastructure in a controlled, optimized, and automated way.Many external operators, including police units, have direct access to mobile network usage data via the Oracle Communications Services Gatekeeper solution, which is based on information technology, web and telecommunications industry standards such as Java Platform, Enterprise Edition (Java EE), web services, Session Initiation Protocol (SIP), IP Multimedia Sub-systems (IMS), Simple Object Access Protocol (SOAP) and Representational State Transfer (REST). Investigators will find this data interesting for their activity.

- ***Text/Multimedia Messages***

A common use of mobile devices is to send messages in text or multimedia format. The Short Message Service (SMS) communication service, which has been in use for some fifteen years, allows transmission of a limited number of text characters using the telephony channel. The advantages of the service include the possibility of transmitting messages even in areas of very low GSM signal coverage, where a voice call would be disturbed or fail due to insufficient signal strength, and even when the voice channel is being used for a conversation.

SMS messages are intercepted using the same systems as used for intercepting voice calls. These systems not only record the telephone numbers of the originator and the recipient but also the entire text of the message. On some networks, the SMS messages are archived for extended periods.The Multimedia Message Service (MMS) is a more evolved form of SMS, where it is possible to attach other multimedia content to a classic text message, such as an audio, video, or photo file. Current interception systems also capture the multimedia content, saving it to a special folder for display or listening.

1.6 HOW DATA MAY BE ACQUIRED

Various laws have been enacted to define how traffic data retained by NSPs may be acquired. Therefore, it is essential for investigators to be familiar with the legislation in force in the country or jurisdiction in which they are operating. In certain countries, for example, the defendant's counsel or suspect's lawyer has the right to request directly from the NSP only those traffic data that refer to the "accounts registered in the name of the client."[155]

In other countries, on the other hand, there are authorities specifically assigned by law to identify measures for guaranteeing the rights of the parties involved in questions of telephone and telematic traffic data retention for detecting, investigating, and prosecuting crime. Precisely for this reason, anyone accessing or processing these data must adhere to certain principles:

- The legislated requirement to provide specific safeguards regarding the type and quantity of data to protect and the risks correlated with said protection. Providers are already required to prevent said risks by upholding common security obligations that go beyond merely the minimum measures required by law or regulation. These risks are then assumed by those who receive the data.
- The advisability of identifying, given the current situation, protective measures to be implemented in the processing of data by all providers so that the integrity of said data can be verified in an inspection (and admissible in dealings with the suspect or defendant's counsel) to ensure more effective security for telephone and telematic traffic data.
- The need to keep in mind the costs deriving from the implementation of the measures in the various countries or jurisdictions, also regarding the different technical and financial capacities of the parties involved.
- The transnational legislative context, especially in light of the opinions expressed by the various groups working to protect personal privacy.
- The technological state of the art, meaning that the various measures have to be periodically updated.

[155] Willassen, S Y (2003) Forensics and the GSM mobile telephone system, International Journal of Digital Evidence, Spring 2003, Vol 2, No 1, pp:12-24

These are important matters with which to be familiar, especially in the field of cross-border investigations and litigation.[156]

1.7 LET'S SUM UP

In this chapter, we studied the technology-based investigations and acquisition of data with respect to it. We discussed the investigations of mobile systems and finally, ended the discussion with different types of evidence that would be collected via mobile systems.

1.8 FURTHER READING

- Gibbs, K. E., & Clark, D. F. (2001). In E. Casey (Ed.), Handbook of computer crime investigation. Academic Press.
- International Engineering Consortium. (2007). Time Division Multiple Access (TDMA). Available online at www.iec.org/online/tutorials/tdma/index.asp
- Prevelakis, V., &Spinellis, D. (2007). The Athens affair, IEEE spectrum. Available at www.spectrum.ieee.org/jul07/5280
- EDRI (2006). Telecom Italia wiretapping scandal. Available on EDRI Online, www.edri.org/edrigram/number4.15/italy

1.9 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) Define mobile device?

A mobile device is generally defined as any instrument that can connect to and operate on a mobile network, including cellular telephones, wireless modems, and pagers.

2) Differentiate between Telephony and Telematic?

TELEPHONY	TELEMATIC
Telephone calls, including voice calls, voice	Internet access, E-mail.

[156] Casey, E, Bann, M, & Doyle, J (2009) Introduction to windows mobile forensics. Digital Investigation, 6(3–4)

messaging, conference calls, and data transmitted via telefax.	
Supplementary services, including call forwarding and call transfers	Fax, SMS and MMS messages via the Internet
Messaging and multimedia services, including SMS services	Telephony via Internet (Voice over Internet Protocol-VoiP)

3) How is the cell identified in the process of investigation?

The mobile device can be reached by looking at the cell to which it is currently connected. There is a range of accuracy that starts from a few hundred meters in urban areas, up to 32 km in suburban areas and rural zones. The accuracy depends on the known range of the particular base station serving the mobile device at the time of positioning. The poor value of 32 km can be enhanced with the use of the so-called Enhanced Cell Identification (general accuracy of 550 meters).

4) What is localization parameters?

The term localization parameters describe information that can be combined to localize an active mobile device and its related user.

1.10 ACTIVITY

Explain how the data is acquired through mobile device investigations along with how and what are the different types of evidence that are collected through the process? Briefly explain it with a relevant case study? (1000 words)