Unit IV

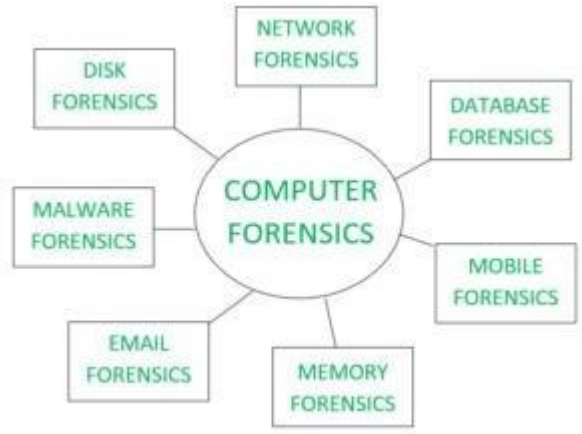
Unit IV: Digital Forensic: Introduction: What is Forensic Science? – What is Digital Forensic? – Uses ofDigital Forensic – Locard's Exchange Principle – Scientific Method – Role of the Forensic Examiner in the Judicial System. Labs and Tools: Forensic Laboratories – Policies and Procedures – Quality Assurance – Digital Forensic Tools

INTRODUCTION TO DIGITAL FORENSICSINTRODUCTION

Computer Forensics is a scientific method of investigation and analysis in order to gather evidence from digital devices or computer networks and components which is suitable for presentation in a court of law or legal body. It involves performing a structured investigationwhile maintaining a documented chain of evidence to find out exactly what happened on a computer and who was responsible for it.

TYPES

- Disk Forensics: It deals with extracting raw data from the primary or secondary storage ofthe device by searching active, modified, or deleted files.
- Network Forensics: It is a sub-branch of Computer Forensics that involves monitoring andanalyzing the computer network traffic.
- Database Forensics: It deals with the study and examination of databases and their relatedmetadata.
- Malware Forensics: It deals with the identification of suspicious code and studying viruses,worms, etc.
- Email Forensics: It deals with emails and their recovery and analysis, including deletedemails, calendars, and contacts.
- Memory Forensics: Deals with collecting data from system memory (system registers,cache, RAM) in raw form and then analyzing it for further investigation.
- Mobile Phone Forensics: It mainly deals with the examination and analysis of phones andsmartphones and helps to retrieve contacts, call logs, incoming, and outgoing SMS, etc., and other data present in it.



CHARACTERISTICS

- Identification: Identifying what evidence is present, where it is stored, and how it is stored(in which format). Electronic devices can be personal computers, Mobile phones, PDAs, etc.
- Preservation: Data is isolated, secured, and preserved. It includes prohibiting unauthorized personnel from using the digital device so that digital evidence, mistakenly or purposely, is not tampered with and making a copy of the original evidence.
- Analysis: Forensic lab personnel reconstruct fragments of data and draw conclusions based on evidence.
- Documentation: A record of all the visible data is created. It helps in recreating and reviewing the crime scene. All the findings from the investigations are documented.
- Presentation: All the documented findings are produced in a court of law for further investigations.

PROCEDURE:

The procedure starts with identifying the devices used and collecting the preliminary evidence on the crime scene. Then the court warrant is obtained for the seizure of the evidence which leads to the seizure of the evidence. The evidence are then transported to the **forensics lab** for further investigations and the procedure of transportation of the evidence from the crime sceneto labs are called chain of custody. The evidence are then copied for analysis and the original evidence is kept safe because analysis are always done on the copied evidence and not the original evidence.

The analysis is then done on the copied evidence for suspicious activities and accordingly, the findings are documented in a nontechnical tone. The documented findings are then presented ina court of law for further investigations.

APPLICATIONS

- Intellectual Property theft
- Industrial espionage
- Employment disputes
- Fraud investigations
- Misuse of the Internet and email in the workplace
- Forgeries related matters
- Bankruptcy investigations
- Issues concerned the regulatory compliance

Advantages of Computer Forensics :

- To produce evidence in the court, which can lead to the punishment of the culprit.
- It helps the companies gather important information on their computer systems or networks potentially being compromised.
- Efficiently tracks down cyber criminals from anywhere in the world.
- Helps to protect the organization's money and valuable time.
- Allows to extract, process, and interpret the factual evidence, so it proves the cybercriminalaction's in the court.

Disadvantages of Computer Forensics :

- Before the digital evidence is accepted into court it must be proved that it is not tamperedwith.
- Producing and keeping electronic records safe is expensive.
- Legal practitioners must have extensive computer knowledge.
- Need to produce authentic and convincing evidence.
- If the tool used for digital forensics is not according to specified standards, then in a courtof law, the evidence can be disapproved by justice.
- A lack of technical knowledge by the investigating officer might not offer the desired result

WHAT IS FORENSIC SCIENCE?

The term *forensic science* involves *forensic* (or *forensis*, in Latin), which means a public discussion or debate. In a more modern context, however, *forensic* applies to courts or the judicial system. Combine that with *science*, and forensic science means applying scientificmethods and processes to solving crimes.

From the 16th century, when medical practitioners began using forensic science to writings in the late 18th century that revealed the first evidence of modern pathology, to the formation of the firstschool of forensic science in 1909; the development of forensic science has been used to uncover mysteries, solve crimes, and convict or exonerate suspects of crime for hundreds of years.

The extraordinary scientific innovations and advancements in forensic science have allowed it to become a highly developed science that involves a number of disciplines and thousands of forensic scientists specializing in everything from DNA and botany to dentistry and toolmarks. The Application of Forensic Science

The field of forensic science draws from a number of scientific branches, including physics, chemistry, and biology, with its focus being on the recognition, identification, and evaluation ofphysical evidence. It has become an essential part of the judicial system, as it utilizes a broad spectrum of sciences to achieve information relevant to criminal and legal evidence.

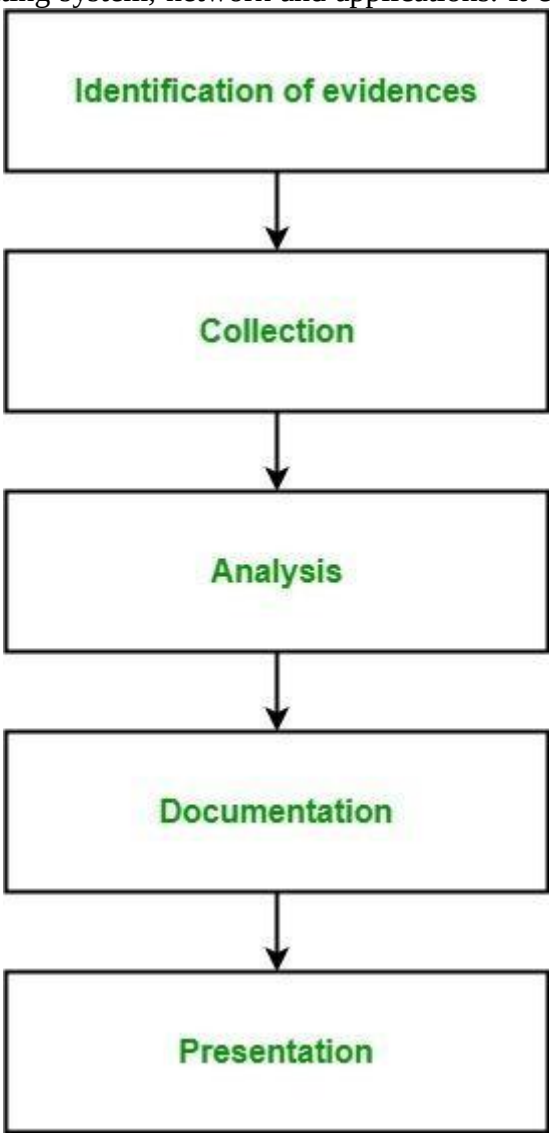
Forensic science may prove the existence of a crime, the perpetrator of a crime, or a connectionto a crime through the:

- Examination of physical evidence
- Administration of tests
- Interpretation of data
- Clear and concise reporting
- Truthful testimony of a forensic scientist

Forensic science has become an integral part of many criminal cases and convictions, with objective facts through scientific knowledge serving both defense and prosecution arguments. The testimony of forensic scientists has become a trusted component of many civil and criminalcases, as these professionals are concerned not with the outcome of the case; only with their objective testimony based purely on scientific facts.

WHAT IS DIGITAL FORENSIC

Digital Forensics is a branch of forensic science which includes the identification, collection, analysis and reporting any valuable digital information in the digital devices related to the computer crimes, as a part of the investigation. In simple words, Digital Forensics is the process of identifying, preserving, analyzing and presenting digital evidences. The first computer crimes were recognized in the 1978 Florida computers act and after this, the field ofdigital forensics grew pretty fast in the late 1980-90's. It includes the area of analysis like storage media, hardware, operating system, network and applications. It consists of 5 steps at high level:



1. **Identification of evidence:** It includes of identifying evidences related to the digital crimein storage media, hardware, operating system, network and/or applications. It is the most important and basic step.
2. **Collection:** It includes preserving the digital evidences identified in the first step so that they doesn't degrade to vanish with time. Preserving the digital evidences is very importantand crucial.
3. **Analysis:** It includes analyzing the collected digital evidences of the committed computercrime in order to trace the criminal and possible path used to breach into the system.

4. **Documentation:** It includes the proper documentation of the whole digital investigation, digital evidences, loop holes of the attacked system etc. so that the case can be studied andanalysed in future also and can be presented in the court in a proper format.
5. **Presentation:** It includes the presentation of all the digital evidences and documentation inthe court in order to prove the digital crime committed and identify the criminal.

Branches of Digital Forensics:

- **Media forensics:** It is the branch of digital forensics which includes identification, collection, analysis and presentation of audio, video and image evidences during theinvestigation process.
- **Cyber forensics:** It is the branch of digital forensics which includes identification, collection, analysis and presentation of digital evidences during the investigation of a cybercrime.
- **Mobile forensics:** It is the branch of digital forensics which includes identification, collection, analysis and presentation of digital evidences during the investigation of a crimecommitted through a mobile device like mobile phones, GPS device, tablet, laptop.
- **Software forensics:** It is the branch of digital forensics which includes identification, collection, analysis and presentation of digital evidences during the investigation of a crimerelated to softwares only.

USES OF DIGITAL FORENSIC

Application of Digital Forensics

Digital Forensics is a branch of forensic science that deals with digital evidences in solving a crime under the regulations of law. With the wide availability and use of various digital media and devices, and social media there are various branches of digital forensics such as mobile forensics, network forensics, database forensics, email forensics, etc. With increasing digital crime in each branch, digital forensics has wide applicability.

The major applications of digital forensics are

- Crime Detection- There are various malwares and malicious activities that happen over digital media and networks, such as phishing, spoofing, ransomware, etc.
- Crime Prevention- There are various cyber crimes that happen due to lack of security or existing unknown vulnerabilities, such as zero-day vulnerability. Hence, cyber forensics helps in finding out these vulnerabilities and avoiding such crimes to occur.
- Crime Analysis- This is the main application of digital forensics. It involves- [2]
- Preservation- This process involves protecting the crime scene and the digital evidence or setup from further manipulation and photographing and video graphing the crime scene, for future reference. Also this process involves stopping any ongoing command that may be linked to the crime.
- Identification- This process involves identifying the digital media and devices that can serve as the potential evidence.
- Extraction- This process involves the imaging of the digital evidence, (to maintain the authenticity of the original evidence), for further analysis.
- Documentation- This involves maintaining the chain of custody and documenting all the evidence collected from the crime scene.
- Interpretation- This involves making of a report by the digital forensic expert about the analysis conducted on the digital evidence using various tools such as FTK (for imaging and mounting of evidences),Sleuth Kit and Autopsy (analyzes disk images and recover files from them) etc. and presenting it in the court of law. The conclusion is based on the evidence collected and reconstructing data fragments.

Challenges in Digital Forensics

The major challenges faced by digital forensic professionals are the growing number and size of evidence to be analyzed and the cybercriminals being equally equipped with anti-forensic tools to erase that

digital evidence or to produce a delay in the digital evidence generation process.
Few of the current challenges in the field of digital forensics are listed as follows-[3]

- Digital Media types- There are various digital devices used these days. The technique used for one specific device cannot be used for some other device because of the different characteristics of each device. Moreover, the digital forensic expert must be equippedwith the use of software for analysis and also the device being analysed.
- Online Disks- The large firms store their data on online disks. These generate a huge amount of data on online disks, and thus, imaging of such huge data takes a lot of time and also requires the firm to shut their services until the imaging is complete.
- Anonymity of the IP- This is one of the big challenge to cyber forensics. IP address allows network identification and location addressing of a device connected to a network. However, IP address can easily be spoofed by cybercriminals and hence can become a hindrance in the address location of the device. Similar to IP address spoofing, there is MAC address and email address spoofing as well that becomes a challenge for the digital forensic expert.
- Anti- Digital Forensic- This is used by cybercriminals and also used legitimately by individuals who want to protect their privacy. Anti-digital forensics is a set of techniques and measures used to slow down or incapacitate the process of investigation by manipulating, erasing, or obscuring the data. One of the most commonly used anti-digital forensic techniques is RootKit that has been used by cybercriminals for years to hide the activities of the malicious code.
- Testing and Validation- With the cybercriminals getting more equipped, there is always aneed to update the software to efficiently analyze the evidences and also provide valid results that can be made admissible in the court of law, like the use of Virtual Machines. It is a forensic investigation tool that allows the investigators to clone the image from the target computer, virtually, but when the image is booted on a machine with different hardware, it installs the missing drivers and thus makes the image a modified one, thus renders it inadmissible in the court of law.

LOCARD'S EXCHANGE PRINCIPLE

The application of Locard's Exchange Principle to a cyber crime, we take the example of identitytheft where someone's identity is stolen and the perpetrator intends to use the stolen information for doing crime again.

Let us further suppose the perpetrator steals the identity through the use of a Trojan horse and keyboard logger ("stupid key logger" is most popular with hackers)on the victim's computer. One could contend that during this type of cyber crime Locard's Exchange Principle does not apply because a human is not at the crime scene & there is no trace evidence from the human on the computer or digital media at the scene. However, in actuality there may be lots of #Digital- evidences such as the Trojan horse itself, changed passwords, digital logs, and so on. Thus,there is a trace "at, to, and from," the scene. It may involve finding the trace evidence at other physicallocations than just the one scene of the crime. Additionally , if an unauthorized user gains accessto an unsecured system to ex-filtrate information to a remote site, he will, on the surface, leave no direct evidence because no files were altered. However, if file access logs were maintained, a record will be made of the file access and subsequent network transmission. Even if no log of thefiles are kept, a side-channel analysis of disk activity, system calls, and network operations may be available as evidence. Even if theses are also not available then network logs at the ISP level might provide evidence related to the unauthorized access, even if the exfiltrated data itself cannot be identified , but in both cases it remains behind for an investigator to discover.

SCIENTIFIC METHOD

The Nine Phases of Digital Forensics

There are nine steps that digital forensic specialists usually take while investigating digitalevidence.

1. First Response

   As soon as a security incident occurs and is reported, a digital forensic team jumps into action.

2. Search and Seizure

   The team searches devices involved in the crime for evidence and data. Investigators seize thedevices to make sure the perpetrators can’t continue to act.

3. Evidence Collection

   After seizing the devices, professionals collect the data using forensic methods to handle theevidence.

4. Securing of the Evidence

   Investigators store evidence in a safe environment. In the secure space, the data can beauthenticated and proved to be accurate and accessible.

5. Data Acquisition

   The forensic team retrieves electronically stored information (ESI) from the devices. Professionals must use proper procedure and care to avoid altering the data and sacrificing theintegrity of the evidence.

6. Data Analysis

   Team members sort and examine the authenticated ESI to identify and convert data that is usefulin court.

7. Evidence Assessment

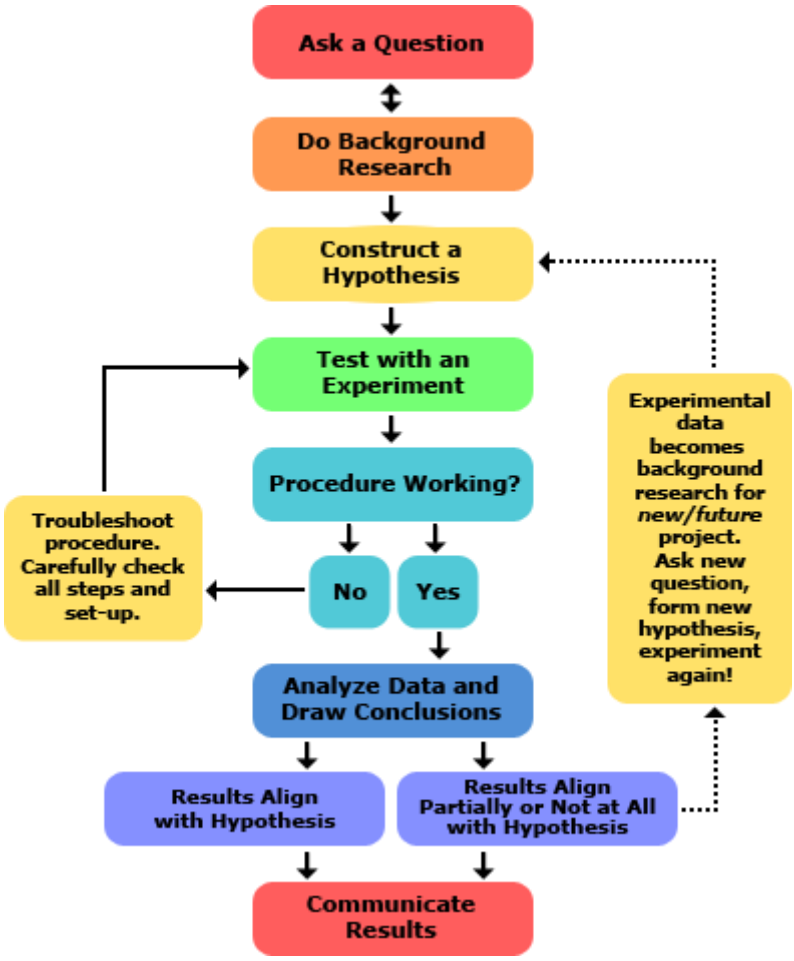
   Once ESI is identified as evidence, investigators assess it in relation to the security incident. Thisphase is about relating the data gathered directly to the case.

8. Documentation and Reporting

   This phase happens once the initial criminal investigation is done. Team members report anddocument data and evidence in accordance with the court of law.

9. Expert Witness Testimony

   An expert witness is a professional who works in a field related to the case. The expert witnessaffirms that the data is useful as evidence and presents it in court.



ROLE OF THE FORENSIC EXAMINER IN THE JUDICIAL SYSTEM

A Digital Forensic Examiner job is to help in the investigation of crimes and cyber-attacks. Digital forensic examiners are primarily responsible for retrieving, organizing, and protecting digital evidence in cybercrime investigations. Information can be recovered from computers andother electronic storage devices by a digital forensic examiner. The Digital Forensic Examiner job description includes keeping track of evidence so that it can be used in court. They conduct

or participate in suspect or victim interviews. In addition, before criminal trials, the Digital Forensic Examiner job description includes assisting in the preparation of evidence. They mayprovide recommendations to other investigators on the importance of digital evidence.

Mentoring

The Digital Forensic Examiner job is to oversee the junior or less experienced scientists and interns. They mentor them and assign the tasks. A Digital Forensic Examiner job is to mentor and provide specific comments on specific forensic interviews, participate in group discussions, generate suitable research linked to the subject of forensic interviewing, and continue to improvepeople skills.

Assessment

A Digital Forensic Examiner is in charge of conducting investigations. An assessment is a usefultool for assessing criminal investigations and conditions.

Documentation

The Digital Forensic Examiner job description includes recording his or her findings and submitting a report to the court. The forensic analysis of suspicious documents is part of digitalforensic documentation analysis.

Types of a Digital Forensic Examiner

Forensic Psychologist: This expertise focuses on detecting criminals through questioning criminals and relevant evidence to assist in determining motives and mental states. They focuson issues including the ability to stand trial, provide information, and make significant judgments. They also assess mental illness in relation to criminal risk.

Forensic Scientist: Forensic scientists investigate crime scenes, conduct scientific analysis, andgive factual evidence that can be presented in court. To find clues and assist police investigations, they use cutting-edge technologies and scientific concepts.

Forensic Anthropologist: Forensic Anthropologists evaluate age, gender, nationality, and othertraits that distinguish a crime victim by examining human bones and structural abnormalities.

LABS AND TOOLS

Forensic Laboratories

Forensic Lab Components

Forensic science requires an understanding of all the scientific disciplines, including biology, chemistry, and physics. A full-service forensic science laboratory requires professionals who understand the influence of each discipline on the specific circumstances of crime scenes, as wellas the principles of the scientific method. The scientific method, first developed in the 17th century, is a problem-solving method that involves observation, asking questions, and finding answers supported by evidence gathered from testing and experimenting.

Crime scene investigation is a classic application of the scientific method since investigators must test and analyze various scenarios as they answer the question of how a crime is committedand who the likely perpetrator is. In addition to standard scientific equipment, specific equipmentto analyze bodily fluids, hairs, fibers, paint samples, fingerprints, weapons ballistics, foot, and tire tracks, and more is necessary.

Another component of a forensic lab is access to databases developed and maintained by nationaland regional law enforcement agencies and colleges or universities. Forensic investigators use databases to pinpoint answers to questions about evidence collected from the crime scene. Some databases contain

specific records of fingerprints, DNA, stolen guns, and crimes committed. Investigators access these to identify potential suspects.

Forensic Lab Services

A forensic lab provides a wide variety of services, including:

- Collection and processing of physical evidence from crime scenes
- DNA/Serology analysis
- Analysis of chemistry of substances seized in controlled substance arrests
- Analysis of evidence from firearms
- Examination and analysis of latent prints of fingers, hands, and feet at crime scenes
- Toxicology testing of blood, urine, and other bodily fluids collected from suspects andvictims to identify the presence of alcohol, illegal drugs, or other ingested substances

DNA/Serology Analysis

The **forensic analytical tools** of DNA/Serology identification involve collecting and identifyingfluids from crime or death scenes. Fluids present at the scene need to be identified as human or non-human. Forensic scientists specializing in serology determine what type of human fluid samples are present and if any diseases are present. The fluids can be blood, urine, sweat, saliva,semen, or even breast milk. Once the fluid is identified, serological forensic scientists can isolateand identify the DNA in the sample. *DNA (deoxyribonucleic acid)* is the genetic information present in all human tissue. DNA is unique to every individual, which makes it a valuable tool for identifying victims and suspects.

The technology of DNA analysis first became available in 1986. There were many initial challenges to DNA evidence, but as the technology has improved, it's become widely accepted asa means of identifying likely criminal suspects and excluding those unlikely to have involvement. Many cold cases have been solved, and accused offenders have been cleared through DNA evidence.

Today, law enforcement officials enter DNA profiles of those involved in criminal activity into the *Combined DNA Index System*, known as *CODIS*. The CODIS database helps generate leads in cases where human biological evidence has been collected. It combines results of DNA screenings from the Convicted Offender database, including sexual offenses, and the Forensic Index database, which includes DNA information collected from all crime scenes. Forensic labsenter DNA profiles collected from crime scenes into the CODIS database and search for matches, enabling law enforcement to match crime scenes and individuals at the local, state, andfederal levels.

POLICIES AND PROCEDURES

POLICY

The Forensic Laboratory policy for issuing confidentiality agreements shall be that:

1.

All Forensic Laboratory employees must be issued with, and sign, a confidentiality agreement (agreements are normally issued at time of recruitment and form a part of thecontract of employment).

2.

No employee shall be allowed access to Forensic Laboratory and Client informationor information processing systems without signing the agreement.

3.

The Forensic Laboratory confidentiality agreement must define the undertakings to whichan employee agrees with respect to maintenance of confidentiality and information security.

The confidentiality agreement is subject to periodic reviews by the Human ResourcesDepartment as follows:

• reviews must be conducted following changes to:

•

job roles;

•

legislation;

•

the Forensic Laboratory policy on Information Security.

•

any changes to the confidentiality agreement must be implemented by the Human Resources Department with suitable input from the General Counsel or specializedexternal legal sources.

Procedures

Digital forensics entails the following steps:

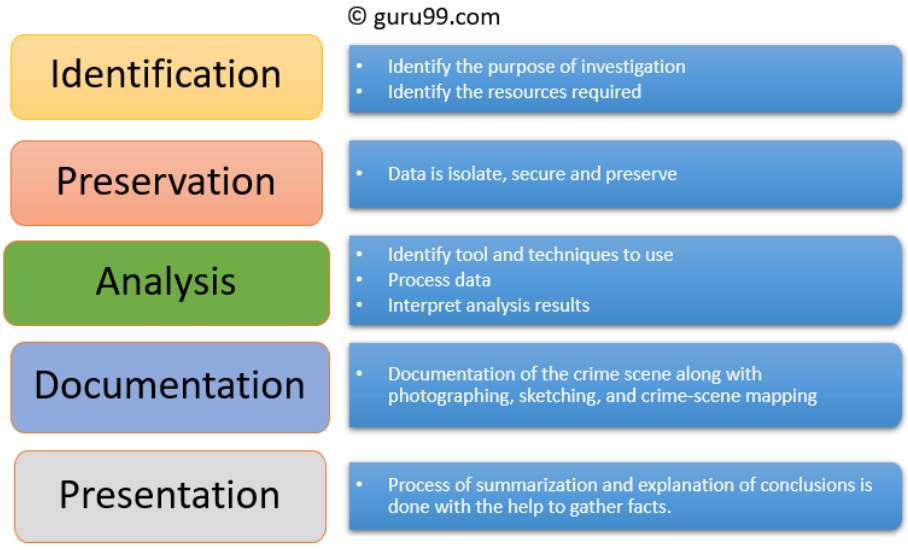
Identification

Preservation

Analysis

Documentation

Presentation
EXPLORE MORELearn Java Programming with Beginners Tutorial08:32Linux Tutorial for Beginners: Introduction to Linux Operating...01:35What is Integration Testing Software Testing Tutorial03:04What is JVM (Java Virtual Machine) with Architecture JAVA...02:24How to writea TEST CASE Software Testing Tutorial01:08Seven Testing Principles Software Testing05:01Linux File Permissions Commands with Examples13:29How to use Text tool in Photoshop CC Tutorial08:32What is NoSQL Database Tutorial02:00Important Linux Commands for Beginners Linux



ForensicsProcess of Digital

Let’s study each in detail

Identification

It is the first step in the forensic process. The identification process mainly includes things likewhat evidence is present, where it is stored, and lastly, how it is stored (in which format).
Electronic storage media can be personal computers, Mobile phones, PDAs, etc.

Preservation

In this phase, data is isolated, secured, and preserved. It includes preventing people from usingthe digital device so that digital evidence is not tampered with.

Analysis

In this step, investigation agents reconstruct fragments of data and draw conclusions based on evidence found. However, it might take numerous iterations of examination to support a specific crime theory.

Documentation

In this process, a record of all the visible data must be created. It helps in recreating the crimescene and reviewing it. It Involves proper documentation of the crime scene along with photographing, sketching, and crime-scene mapping.

Presentation

In this last step, the process of summarization and explanation of conclusions is done. However, it should be written in a layperson's terms using abstracted terminologies. Allabstracted terminologies should reference the specific details

QUALITY ASSURANCE

Digital forensic examinations require an examiner to apply a wide range of techniques to retrieve data, and frequently examiners must interpret data to offer an expert opinion on what the data mean. These opinions can affect the outcomes of investigations, prosecutions, or other remedies. It is therefore essential that organizations have a management system to engender confidence in the quality of forensic work performed. The quality management system is the consolidation of practices and procedures used to ensure the quality of the workand products that the organization produces.

Administrative Review—All digital forensic examination reports must be administrativelyreviewed for consistency with agency policy and for editorial correctness.

Technical Review—At least 10 percent of final digital forensic examination reports must be technically reviewed by another qualified digital forensic examiner (peer reviewed) before the reports are published.

The reviewing examiner may be from the same or a different organization. The purpose of the technical review is to ensure the following:
The report is clear and understandable.
The procedures performed were adequately documented and forensically sound.
The exam documentation was sufficiently detailed to enable reproduction of the results.
The interpretations and conclusions of the examiner were reasonable, supported by theexamination documentation, and scientifically valid.
Validation Testing—Acquiring digital data for forensic examination is a critical phase of the forensic process. Forensic personnel will often have only one opportunity to obtain the data, and using untested tools could unintentionally alter the data. To the extent possible, organizations should ensure the tools they use to acquire digital evidence are validated to operate as intended and accurately acquire the data. The validation testing may be performed by the organization or other reputable entity (for example, another digital forensic laboratory).The organization performing the validation test must document the test, including the requirements that were tested, the expected results, and the actual results of the testing. To comply with this standard, the organization must be able to produce the report if requested.
Review of Quality System—An organization should review its quality management system at least once every 3 years to ensure the system is meeting the quality needs of the organization.

DIGITAL FORENSIC TOOLS

FEATURED DIGITAL FORENSICS AND CYBERSECURITY TOOLS

Autopsy

Autopsy is a digital forensics platform and graphical interface that forensic investigators use to understand what happened on a phone or computer. It aims to be an end-to-end, modular solution that is intuitive out of the box. Select modules in Autopsy can do timeline analysis, hash filtering, and keyword search. In addition, they can extract web artifacts, recover deleted files from unallocated space, and find indicators of compromise. All of this can be done relatively rapidly.

Autopsy runs background jobs in parallel so that even if a full search takes hours, a user will know within minutes whether targeted keywords have been found. In addition, investigators working with multiple devices can create a central repository through Autopsy that will flag phone numbers, email addresses, or other relevant data points.

Developed by the same team that created The Sleuth Kit, a library of command line tools for investigating disk images, Autopsy is an open-source solution, available for free in the interests of education and transparency. Unfortunately, the latest version is written in Java, and it is currently only available for Windows.

Bulk Extractor

Bulk Extractor scans a file, directory, or disk image. It extracts information without parsing the file system or file system structures, allowing it to access different parts of the disk in parallel, making it faster than the average tool. The second advantage of Bulk Extractor is that it can be used to process practically any form of digital media: hard drives, camera cards, smartphones, SSDs, and optical drives.

The most recent versions of Bulk Extractor can perform social network forensics and extract addresses, credit card numbers, URLs, and other types of information from digital evidence. Other capabilities include creating histograms based on frequently used email addresses and compiling word lists, which can be helpful for password cracking.

All extracted information can be processed either manually or with one of four automated tools, one of which incorporates context-specific stop lists (i.e., search terms flagged by the investigator) that remove some human error from digital forensics investigation. The software is available for free for Windows and Linux systems.

COFEE

Microsoft's Computer Online Forensic Evidence Extractor (COFEE) is a forensic toolkit that extracts evidence from Windows computers. Developed in 2006 by a former Hong Kong police officer turned Microsoft executive, the toolkit acts as an automated forensic tool during a live analysis. It contains more than 150 features and a graphical user interface that guides an investigator through data collection and examination and helps generate reports after extraction. Password decryption, internet history recovery, and other data collection forms are all included in the toolkit.

Microsoft claimed that COFEE had reduced three- to four-hour tasks to under 20 minutes at the time of its release. In addition, thousands of law enforcement agencies worldwide (including INTERPOL) use COFEE, and Microsoft provides free technical support.

In November 2009, COFEE was leaked onto multiple torrent sites. So while it is possible— though incredibly tricky—for criminals to build around the features in COFEE, it is also possiblefor the average citizen to now get a look at what was once the industry standard across the world for digital forensics.

Computer Aided Investigative EnvironmentCAINE offers a full-scale forensic investigation platform designed to incorporate other tools and modules into a user-friendly graphic interface. Its interoperable environment is intended to assist investigators in all four stages of an investigation: preservation, collection, examination, and analysis. In addition, it comes with dozens of pre-packaged modules (Autopsy, listed above, is among them). Developed on Linux, the tool is entirely open source and available for free.

Digital Forensics FrameworkDigital Forensics Framework (DFF) is an open-source computer forensics platform built upon a dedicated Application Programming Interface (API). Equipped with a graphical user interface forsimple use and automation, DFF guides a user through the critical steps of a digital investigation and can be used by both professionals and amateurs alike.

The tool can be used to investigate hard drives and volatile memory and create reports about system and user activity on the device in question. The DFF was developed with the three main goals of modularity (allowing for changes to the software by developers), scriptability (allowing for automation), and genericity (keeping the operating-system agnostic to help as many users as possible). The software is available for free on GitHub.

DumpZilla

DumpZilla performs browser analysis, specifically of Firefox, Iceweasel, and Seamonkey clients.In addition, it allows for the visualization and customized search and extraction of cookies, downloads, history, bookmarks, cache, add-ons, saved passwords, and session data.

Developed in Python, it works under Linux and Windows 32/64 bit systems and DumpZilla is available for free from the developer's website. While this was created as a standalone tool, its specific nature and lean packaging make it a vital component of future digital forensics suites.

EnCase

The recipient of *SC Magazine's* "Best Computer Forensic Solution" award for ten consecutive years, EnCase is considered the gold standard in forensic cybersecurity investigations, including mobile acquisitions. Since 1998, EnCase has offered forensic software to help professionals find evidence to testify in criminal investigation cases involving cybersecurity breaches by recoveringevidence and analyzing files on hard drives and mobile phones.

Offering a comprehensive software lifecycle package from triage to final reports, EnCase also features platforms such as OpenText Media Analyzer, which reduces the amount of content for investigators to review to close cases faster manually. With four site license options for small companies; federal, state, and local law enforcement; consulting organizations; and colleges and universities, it offers criminal justice evidence analysis through just a few clicks.

ExifTool

ExifTool is a platform-independent system for reading, writing, and editing metadata across various file types. Of particular interest to the digital investigator is the reading of metadata, which can be achieved through command-line processes or a simple GUI. For example, investigators can drag and drop different files, such as a PDF, or a JPEG, and learn when and where the file was created—a crucial component in establishing a chain of evidence.

The software itself is lightweight and quick, making it an ideal inclusion in future digitalforensics suites and easy to use. ExifTool is updated regularly and is available for both Windowsand OSx from the developer's website.

FTK Imager

For tools such as The Sleuth Kit by Autopsy to work correctly, original digital copies of hard drives must be preserved before evidence can be extracted. Enter FTK Imager, a free tool that analyzes images of a drive and preserves the original integrity of the evidence without affecting its original state.

This tool can read all operating systems and enables users to recover files that have been deleted from digital recycle bins. In addition, it can parse XFS files and create hashes of files to check data integrity.

MAGNET RAM CaptureAnalyzing a computer's physical random access memory (RAM), MAGNET RAM Capture enables cybersecurity investigators to recover and analyze digital artifacts stored in a computer's

memory. Using a small memory footprint, digital forensic investigators can use the tool and minimize the amount of overwritten memory data.

This tool can export raw memory data in raw formats (.DMP, .RAW, .BIN), which can be uploaded to other forensics analysis tools such as Magnet AXIOM and Magnet IEF. This free tool supports several versions of Windows operating systems.

Nagios

Considered by many as a standard network monitoring tool for large organizations, Nagios helps cybersecurity professionals monitor computer networks in real-time. In addition, the Nagios platform alerts network security professionals via email or text message if a security threat occurs.

Nagios supports standard enterprise-level network services such as ICMP, POP3, SMTP, and HTTP. It is compatible with Linux, Windows, server, application, SNMP, and log monitoring services and integrates with third-party addons. Free trials are available.

Redline

Initially a product of Mandiant, but later taken over by FireEye, a cybersecurity firm, Redline isa freeware tool that provides endpoint security and investigative capabilities to its users. It is mainly used to perform memory analysis and look for infection or malicious activity signs. Still, it can also be used to collect and correlate data around event logs, the registry, running processes,file system metadata, web history, and network activity.

Offering much more technical and under-the-hood capability than most digital forensics investigations necessitate, Redline has more applications in cybersecurity and other tech-driven criminal behavior where a granular analysis is critical. Redline currently only functions on Windows-based systems, but it is regularly updated by FireEye for optimum performance andcan be downloaded for free on the FireEye website.

SIFT Workstation

The SANS Investigative Forensics Toolkit (SIFT) is a collection of open-source incident response and forensics technologies designed to perform detailed digital investigations in varioussettings. The toolkit can securely examine raw disks and multiple file formats in a secure, read- only manner that does not alter the evidence it discovers.

SIFT is flexible and compatible with expert witness format (E01), advanced forensic format (AFF), and raw evidence formats. Built on Ubuntu, it incorporates many separate tools

(including some on this list, such as Autopsy and Volatility) and puts them at an investigator's disposal. SIFT is available for free and updated regularly.

SNORT

SNORT is an open-source network security tool that performs three tasks: sniffs for packets, logspackets, and has comprehensive network intrusion features. Because it is open-source, it can be downloaded and used for personal ($29.99 per year) and professional ($399 per year) applications.

SNORT helps IT security professionals analyze network security vulnerabilities and preventthem from happening. When a network intrusion occurs, cybersecurity professionals are notified while the software blocks security intrusions.

Tor

When surveillance is a security threat, applications like Tor help PC and mobile device users be undetectable. Tor allows users to browse anonymously and prevent identity theft through increased internet security. This is useful when users need to access websites while visiting othercountries, protect their identity, or be difficult to trace. In addition, it blocks browser pluginssuch as Flash, Real Player, QuickTime, and others. Finally, while it works on the iOS platform, Tor suggests iOS users use their Onion Browser for private browsing that automatically closes browsing history and extra tabs.

Tor's mission is to "advance human rights and freedoms by creating and deploying free and open-source anonymity and privacy technologies, supporting their unrestricted availability and use, and furthering their scientific and popular understanding."

Volatility

The Volatility Foundation is a nonprofit organization whose mission is to promote the use of memory analysis within the forensics community. Its primary software is an open-source framework for incident response and malware detection through volatile memory (RAM) forensics. This allows the preservation of evidence in memory that would otherwise be lost during a system shutdown.

Written in Python and supportive of almost all 32-bit and 64-bit machines, it can sift through cached sectors, crash dumps, DLLs, network connections, ports, process lists, and registry files. The tool is available for free, and the code is hosted on GitHub.

Wireshark

Wireshark is the world's most-used network protocol analysis tool, implemented by governments, private corporations, and academic institutions worldwide. As the continuation of aproject that began in 1998, Wireshark lets a user see what is happening on a network at the microscopic level. By capturing network traffic, users can then scan for malicious activity.

Captured network data can be viewed on a graphical user interface on Windows, Linux, OSx,and several other operating systems. The data can be read from Ethernet Bluetooth, USB, and several others, while the output can be exported to XML, PostScript, CSV, or plain text.

Wireshark's applications remain primarily in cybersecurity, but there are digital forensics investigation applications. Less about the smoking gun than the breadcrumb trail, Wireshark can point an investigator in the direction of malicious activity so that it can be tracked down and investigated.