

Digital Forensics



CONTENTS :-

- Definitions
- Branches of Digital Forensics
- Digital Evidence
- Crime Scene Management
- Windows Forensic Artifacts
- Demonstration

C y b e r Crime

“Any Crime Committed By Using Computer, Internet Or Any Other Digital Medium As A Tool Or Target.”

Digital Forensics

“Cyber Forensics is the process of Identifying, Collecting, preserving, analyzing and presenting the digital evidence in such a manner that the evidence are legally accepted.”

BRANCHES OF DIGITAL FORENSICS

- Computer Forensics
- Mobile Device Forensics
- Network Forensics
- E-mail and Social Media Forensics
- Database Forensics

What Is Digital Evidence

- ❑ “Digital Evidence Is Any Information Or Data Related To The Case, That Is Stored On, Received By, Or Transmitted By An Electronic Device That May Be Relied In The Court Of Law.”

Properties of Digital Evidence

- It can be duplicated exactly and a copy can be examined as if it were the original.
 - Examining a copy will avoid the risk of damaging the original.
- With the right tools it is very easy to determine if digital evidence has been modified or tampered with by comparing it with the original.
- It is relatively difficult to destroy.
 - Even if it is “deleted,” digital evidence can be recovered.
- When criminals attempt to destroy digital evidence, copies can remain in places they were not aware of.

Types Of Digital Evidence

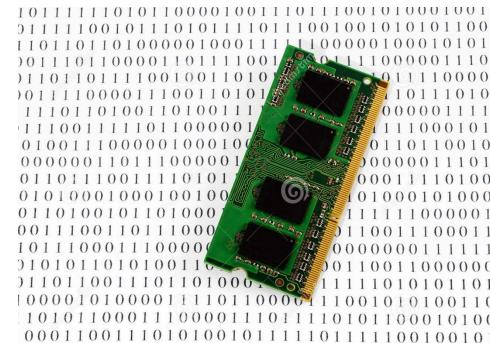
1. Persistent (Non-volatile) Data :-

- ❑ It Means Data That Remains Intact When The Computer Is Turned Off.
- ❑ E.G. Hard-disk, Flash-drives



2. Volatile Data :-

- ❑ It Means Would Be Lost When The Computer Is Turned Off.
- ❑ E.G. Temp. Files, Unsaved Open Files Etc.



Source Of Digital Evidence

- Hard-Drive (Desktop, Laptop, External, Server)
- Flash Drive
- SD Cards
- Floppy Disks
- RAIDs
- Optical Media (CD, DVD)
- CCTV/DVR
- Internal Storage of Mobile Device
- GPS (Mobile/Car)
- Call Site Track (Towers)
- RAM



USB Bottle Opener



USB Gun



USB Comb



USB Pen



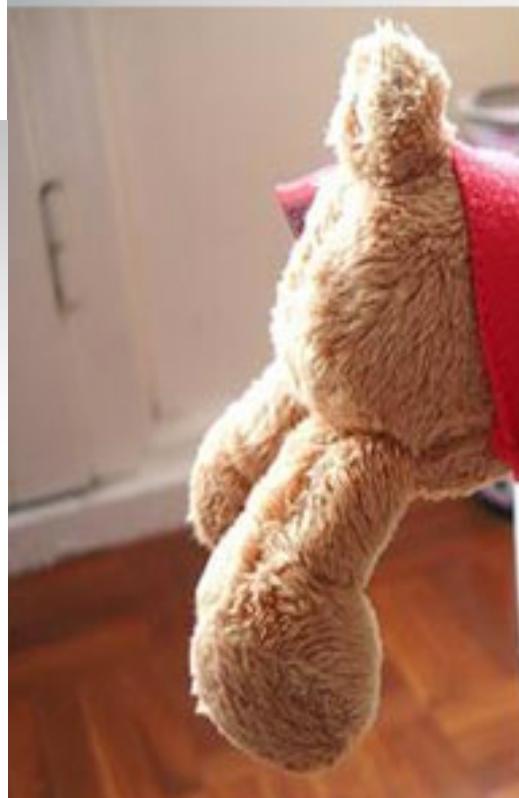
USB Cookies



USB Cork



USB Teddy Bear

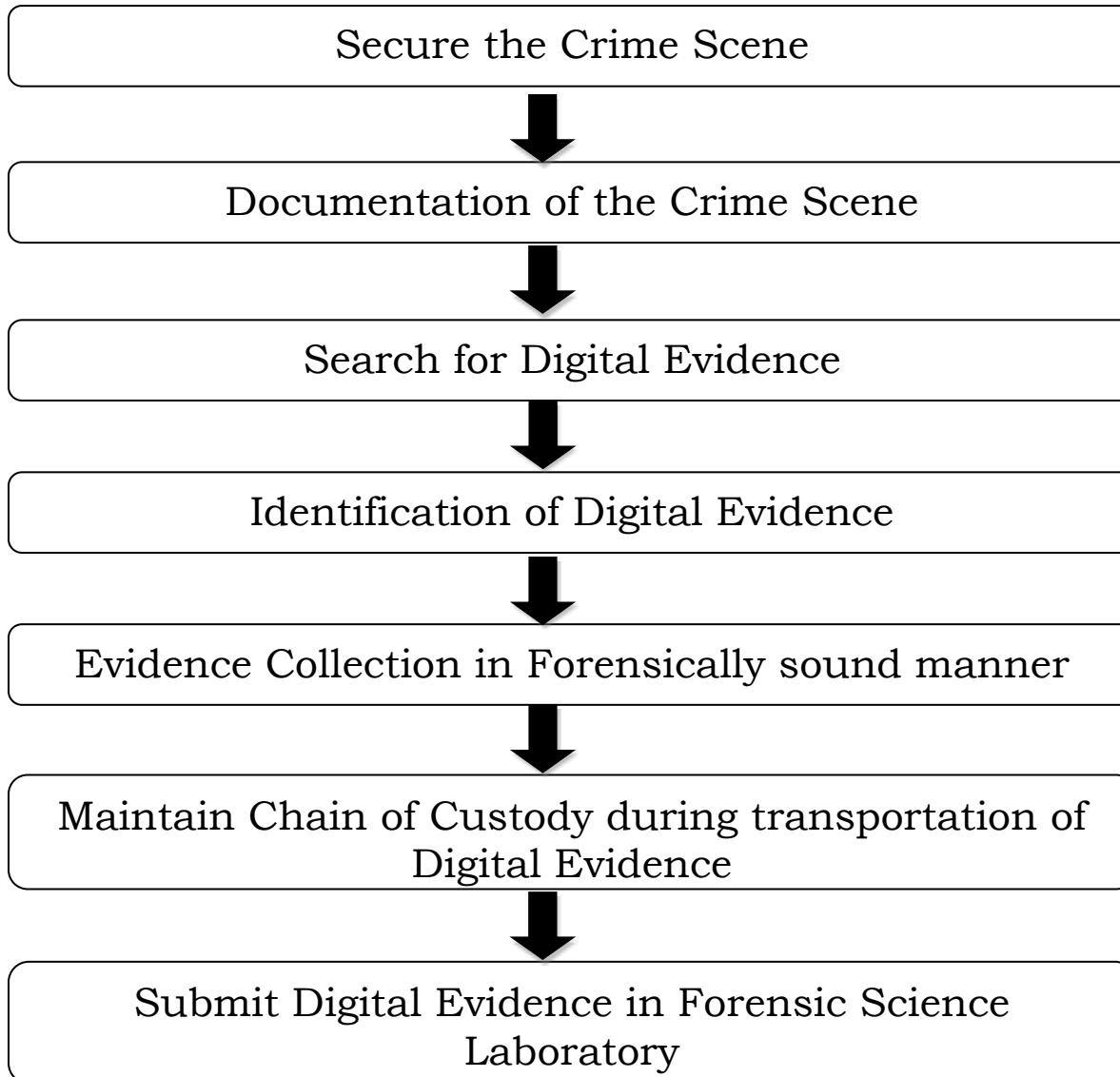


DIGITAL FORENSIC PROCESS



CRIME SCENE MANAGEMENT

Important steps at crime scene



Investigative Tools and Equipment

- Crime scene securing tapes
- Digital Camera
- Extra batteries
- Video cameras
- Note/sketch pads
- Blank sterile storage media: Portable USB hard disks and pen drives
- Write-Blocker device
- Labels
- Pens, permanent markers

.....cont. in next slide

- Storage containers
- Anti-static bags
- Faraday bags
- Toolkit containing screwdrivers (nonmagnetic), pliers, forceps, scissors, clips, pins, cutters etc.
- Rubber gloves
- Incident response toolkit (Software)
- Converter / Adapter: USB, SATA, IDE, SCSI
- Forensic Imaging software
- Tools to collect volatile data (FTK Imager, Magnet Forensics Ram Capture)



Types Of Cyber Crime

- Hacking
- Phishing
- Spoofing
- Cyber Stalking
- Cyber Terrorism
- Data Theft
- Social Engineering
- Morphing
- Skimming
- Identity Theft
- Malware Attack
- Drug Trafficking
- Spamming
- Web Jacking
- Child Pornography
- Piracy
- Piggy Banking
- Online Fraud

Facebook - log in or sign up X +

https://www.facebook.com

Email or Phone
Password

Log In

Forgot account?

facebook

Facebook helps you connect and share with the people in your life.



Create an account

It's free and always will be.

First name ! Surname

Mobile number or email address

New password

Birthday

3 Sept 1993 Why do I need to provide my date of birth?

Female Male

By clicking Sign Up, you agree to our [Terms](#), [Data Policy](#) and [Cookie Policy](#). You may receive SMS notifications from us and can opt out at any time.

Sign Up

Activate Windows
Go to Settings to activate Windows.



Search the web and Windows



6:24 PM
9/3/2018



Facebook helps you connect and share with
the people in your life.

Sign Up

It's free and anyone can join



First Name:

Last Name:

Your Email:

New Password:

I am: Select Sex:

Birthday: Month: Day: Year:

Why do I need to provide this?

Sign Up

Create a Page for a celebrity, band or business.

Non-electronic Evidence Collection

- Recovery of non-electronic evidence can be crucial in the investigation of electronic crimes. Take proper care to ensure that such evidence is recovered and preserved.
- Items relevant to subsequent examination of electronic evidence may exist in other forms (**written passwords and other handwritten notes, blank pads of paper with indented writing, hardware and software manuals, calendars, literature, text or graphical computer printouts, and photographs**) and should be secured and preserved for future analysis.
- These items are frequently in close proximity to the computer or related hardware items. All evidence should be identified, secured, and preserved in compliance with departmental procedures.

Digital Evidence Collection process from computer

Situation 1: The Monitor Is On And The Work Product and/or Desktop is Visible



Digital Evidence Collection process from computer

Situation 1: The Monitor Is On And The Work Product and/or Desktop are Visible

- Photograph the screen and record the information displayed.
- Collect volatile data using memory capturing tools.
- Check for virtual drives. If yes, collect logical copies of mounted data.
- Label all connections and ports.
- Photograph them.
- Disable network connectivity to prevent remote access.
- Disconnect the power/shutdown.
- Open CPU chassis to locate Hard disk and disconnect it.
- Seize and package all evidence in Anti magnetic (Faraday) bags.
- Transport evidence to forensic laboratory.
- Maintain chain of custody.

Situation 2: The Monitor Is On and The Screen Is Blank (Sleep Mode) Or The Screensaver (Picture) Is Visible

Download more graphics at www.psdgraphics.com



Situation 2: The Monitor Is On and The Screen Is Blank (Sleep Mode) Or The Screensaver (Picture) Is Visible

- Move the mouse slightly (without pushing buttons). The screen should change and show the work product or request a password.
- Do not perform any other keystrokes or mouse operations if mouse movement does not cause a change in the screen.
- Photograph the screen and record the information displayed.
- Collect volatile data using memory capturing tools (Mind that always use write blocker to prevent any kind of manipulation during data collection).
- Follow further steps as per situation 1.

Situation 3: The Monitor Is Off

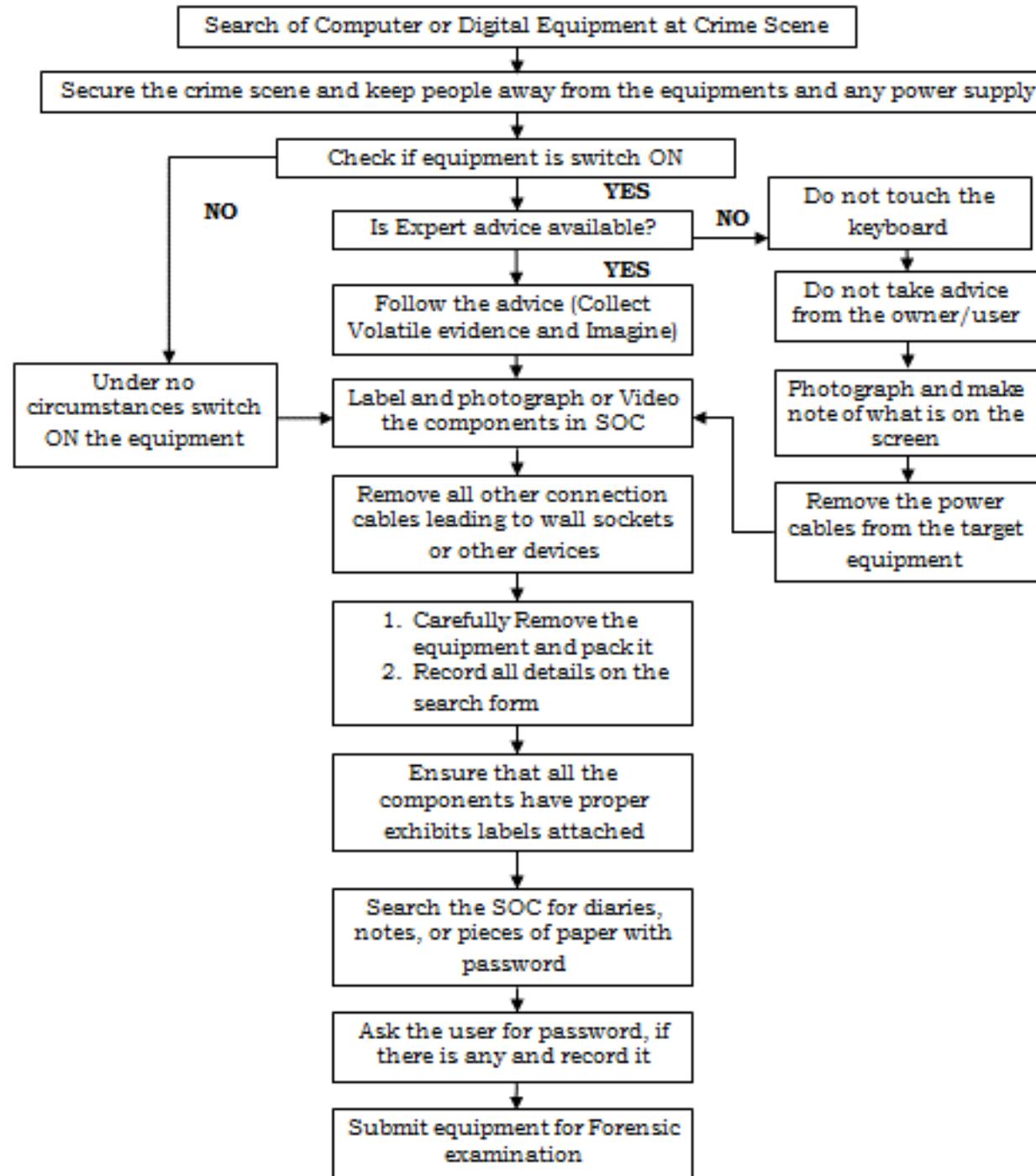
- Make a note of the “off” status.
- Turn the monitor on, then determine if the monitor status is as described in either situation 1 or 2 above and follow those steps.
- Check for outside connectivity (telephone modem, cable, integrated services digital network [ISDN], and digital subscriber line [DSL]). If a telephone connection is present, attempt to identify the telephone number.
- Avoid damage to potential evidence by removing any floppy disks that are present, packaging the disk separately, and labeling the package. If available, insert either a seizure disk or a blank floppy disk. Do not remove CDs or touch the CD drive.
- Place tape over all the drive slots and over the power connector.
- Record the make, model, and serial numbers.

- Photograph and diagram the connections of the computer and the corresponding cables.
- Label all connectors and cable ends (including connections to peripheral devices) to allow for exact reassembly at a later time. Label unused connection ports as “unused.” Identify laptop computer docking stations in an effort to identify other storage media.
- Collect non-volatile data, i.e. storage media (Hard Disk, Pen drives, Optical Disks, Mobile phones, Memory card etc.)
- Seize and package all evidence in anti-magnetic (Faraday) bags.
- Tag/label each bag.
- Transport evidence to forensic laboratory.
- Maintain chain of custody.

Digital Evidence Collection process from computer

Situation 3: The Monitor Is Off





Complaint/FIR No.	Police Station:	
Date:	Time:	Organization:
Examiner Name(s):		
Location:		

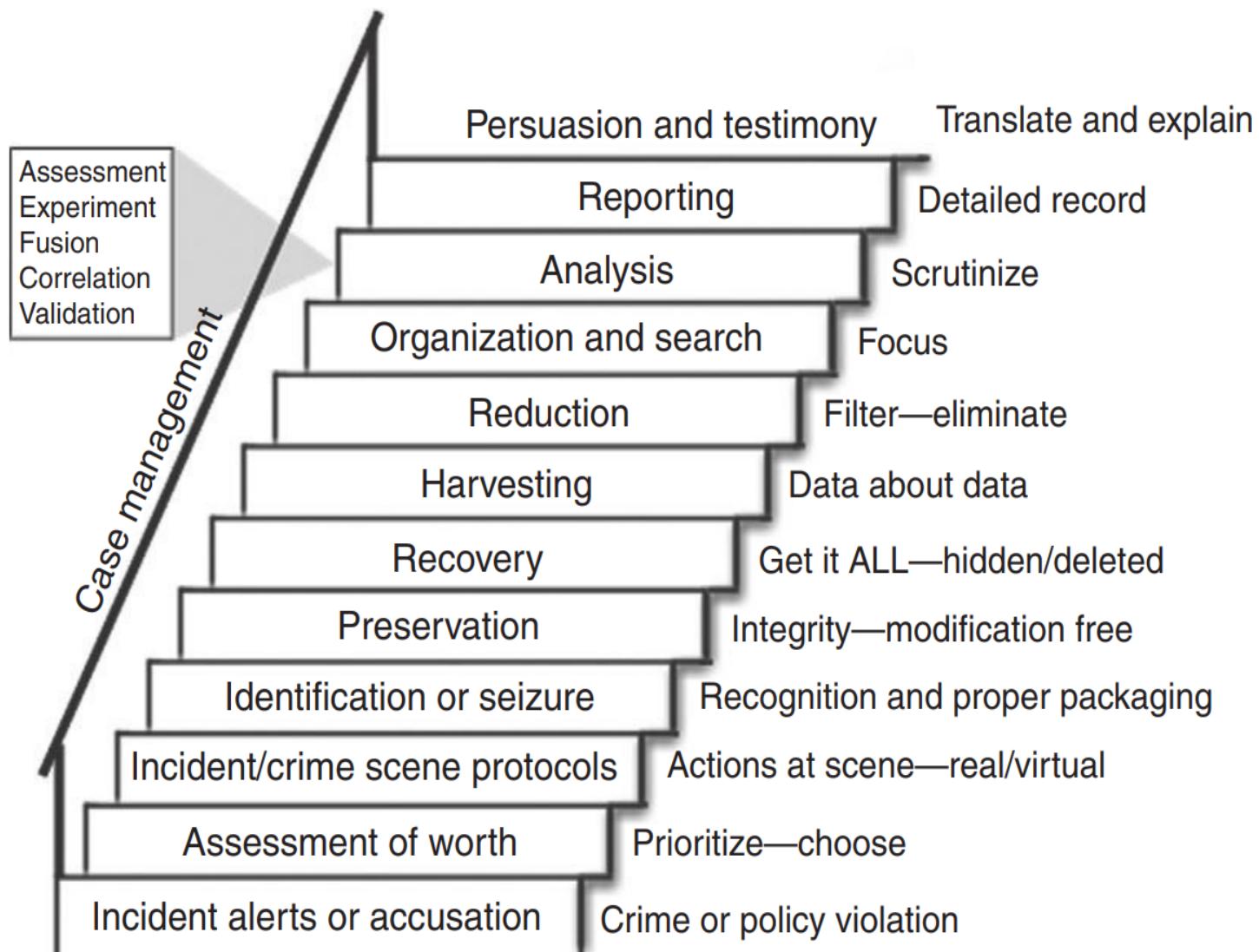
Method of evidence received (i.e. delivered, seized, discovered)

System Information	
Date of Purchase	
System Manufacturer	
System Serial Number	
System Name	
System Model Number	
System Date/Time	
Other Identifying Date (i.e. damage, label etc.)	
Processor	
Memory	
Network Card	
SCSI Card	
Modem	
Keyboard	
Monitor	
Mouse	
Floppy Disk Drive (s)	
CD/DVD Drive (s)	
Printer (s)	
Other Cards	
Other Devices and Drives	
Size of Hard-drive	
Hash Value if obtained	

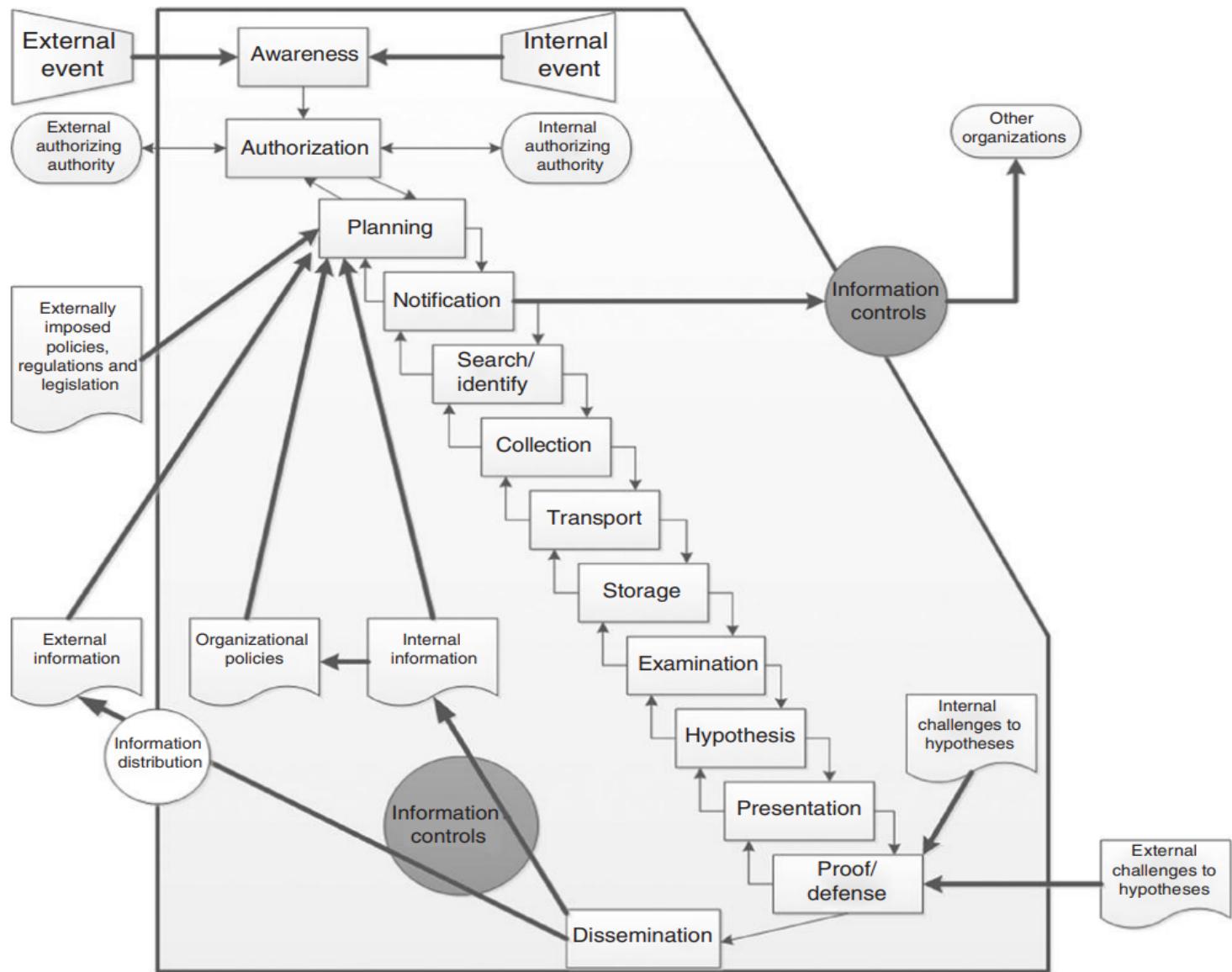
Physical Model: Investigation Process model

	Phase Goals (Physical)	Phase Goals (Digital)
Crime scene preservation	Securing entrances and exits and preventing physical changes to evidence	Preventing changes in potential digital evidence, including network isolation, collecting volatile data, and copying entire digital environment
Crime scene survey	Walking through scene, identifying obvious and fragile physical evidence	Identification of obvious evidence by searching in digital evidence (typically in lab)
Crime scene documentation	Photographs, sketches, maps of evidence, and crime scene	Photographs of digital devices and individuated descriptions of digital devices
Crime scene search and collection	In-depth search for physical evidence	Analysis of system for nonobvious evidence (typically in lab)
Crime scene reconstruction	Developing theories based on analysis results and testing against evidence	

Staircase Model: The investigative process model



Evidence Flow Model



Evidence Packaging, Transporting, and Storing

Packaging

- If multiple computer systems are collected, label each system so that it can be reassembled as found (system A: mouse, keyboard, monitor, and main base unit; system B: mouse, keyboard, monitor, and main base unit).

When packaging evidence at a crime scene—

- Ensure that all collected electronic evidence is properly documented, labeled, and inventoried before packing.
- Pay special attention to latent or trace evidence and take action to preserve it.
- Pack magnetic media in antistatic packaging (paper or antistatic plastic bags). Avoid using materials that can produce static electricity, such as standard plastic bags (Faraday bags).
- Avoid folding, bending, or scratching computer media, such as a diskette, compact disk-read only memory (CD-ROM), or tape.
- Ensure that all containers used to hold evidence are properly labeled.

Evidence Packaging, Transporting, and Storing

Transporting

- Ensure that computers and other components that are not packaged in containers are secured in the vehicle to avoid shock and excessive vibrations.
- For example, computers may be placed on the vehicle floor and monitors placed on the seat with the screen down and secured by a seat belt. When transporting evidence—

- Keep all electronic evidence away from magnetic sources. Radio transmitters, speaker magnets, and heated seats are examples of items that can damage electronic evidence.
- Avoid storing electronic evidence in vehicles for prolonged periods of time. Conditions of excessive heat, cold, or humidity can damage electronic evidence.
- Maintain the chain of custody on all evidence transported.

Storing

- Store evidence in a secure area away from temperature and humidity extremes.
- Protect it from magnetic sources, moisture, dust, and other harmful particles or contaminants.
- Be aware that potential evidence, such as dates, times, and system configurations may be lost as a result of prolonged storage.
- Since batteries have a limited life, data could be lost if they fail. Therefore, appropriate personnel (such as the evidence custodian, laboratory chief and forensic examiner) should be informed that a device powered by batteries is in need of immediate attention.

Non-electronic Evidence Collection

- Recovery of non-electronic evidence can be crucial in the investigation of electronic crimes.
- Take proper care to ensure that such evidence is recovered and preserved.
- Items relevant to subsequent examination of electronic evidence may exist in other forms (**written passwords and other handwritten notes, blank pads of paper with indented writing, hardware and software manuals, calendars, literature, text or graphical computer printouts, and photographs**) and should be secured and preserved for future analysis.

- These items are frequently in close proximity to the computer or related hardware items.
- All evidence should be identified, secured, and preserved in compliance with departmental procedures.

COPY, IMAGING AND CLONING

- Disk cloning and disk imaging are two processes that accomplish the same goal: They copy all of a hard drive's contents.
- It's possible to clone a disk by using a disk image, but the two are distinctly different in the process they use to copy hard drives.
- Disk cloning creates a functional one-to-one copy of a hard drive, while disk imaging creates an archive of a hard drive that can be used to make a one-to-one copy.

Copy and Paste

- Disk images and disk clones are different than just copying and pasting the entire contents of one hard drive to another.
- When you copy and paste files from one drive to another you're copying only the actual files and not the additional data the hard drive uses to locate and access those files.
- Things like the master boot record and the file allocation table are not copied to the new hard drive when you copy and paste. A copy and paste backup drive won't boot.

Disk Cloning

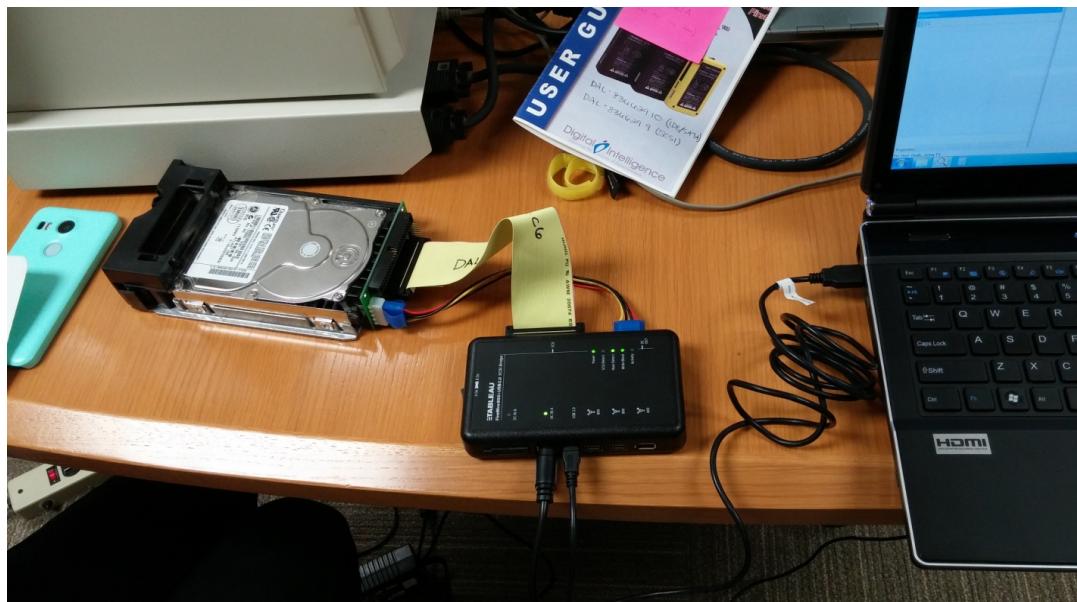
- Disk cloning is the process of copying the entire contents of one hard drive to another including all the information that enables you to boot to the operating system from the drive.
- A cloning program enables you to make a one-to-one copy of one of your computer's hard drives on another hard drive.
- This second copy of the hard drive is fully operational and can be swapped with the computer's existing hard drive.
- If you boot to the cloned drive, its data will be identical to the source drive at the time it was created.
- A cloned drive can be used to replace its source drive in a computer in the event that something bad happens to the original drive.

Disk Imaging

- Disk imaging is the process of making an archival or backup copy of the entire contents of a hard drive.
- A disk image is a storage file that contains all the data stored on the source hard drive and the necessary information to boot to the operating system.
- However, the disk image needs to be applied to the hard drive to work.
- You can't restore a hard drive by placing the disk image files on it; it needs to be opened and installed on the drive with an imaging program.
- Unlike cloned drives, a single hard drive can store several disk images on it. Disk images can also be stored on optical media and flash drives.

Write blocker

- A write blocker is any tool that permits read-only access to data storage devices without compromising the integrity of the data. A write blocker, when used properly, can guarantee the protection of the data chain of custody.
- There are both hardware and software write blockers. Some software write blockers are designed for a specific operating system. One designed for Windows will not work on Linux. Most hardware write blockers are software independent.



Examples of computer crimes

- Copyright violation - Stealing or using another person's Copyrighted material without permission.
- Cracking - Breaking or deciphering codes designed to protect data.
- Cyber terrorism - Hacking, threats, and blackmailing towards a business or person.
- Cyberbully or Cyberstalking - Harassing or stalking others online.

- Cybersquatting - Setting up a domain of another person or company with the sole intention of selling it to them later at a premium price.
- Creating Malware - Writing, creating, or distributing malware (e.g., viruses and spyware.)
- Data diddling - Computer fraud involving the intentional falsification of numbers in data entry.
- Denial of Service attack - Overloading a system with so many requests it cannot serve normal requests.
- Doxing - Releasing another person's personal information without their permission.
- Espionage - Spying on a person or business.
- Fraud - Manipulating data, e.g., changing banking records to transfer money to an account or participating in credit card fraud.
- Green Graffiti - A type of graffiti that uses projectors or lasers to project an image or message onto a building.

- • Harvesting - Collect account or account-related information on other people.
- • Human trafficking - Participating in the illegal act of buying or selling other humans.
- • Identity theft - Pretending to be someone you are not.
- • Illegal sales - Buying or selling illicit goods online, including drugs, guns, and psychotropic substances.
- • Intellectual property theft - Stealing practical or conceptual information developed by another person or company.
- • IPR violation - An intellectual property rights violation is any infringement of another's Copyright, patent, or trademark.

- Phishing or vishing - Deceiving individuals to gain private or personal information about that person.
- Ransomware - Infecting a computer or network with ransomware that holds data hostage until a ransom is paid.
- Salami slicing - Stealing tiny amounts of money from each transaction.
- Scam - Tricking people into believing something that is not true.
- Slander - Posting slander against another person or company.
- Software piracy - Copying, distributing, or using software that was not purchased by the user of the software.
- Spamming - Distributed unsolicited e-mail to dozens or hundreds of different addresses.

- • Spoofing - Deceiving a system into thinking you are someone you're not.
- • Swatting - The act of calling in a false police report to someone else's home.
- • Theft - Stealing or taking anything (e.g., hardware, software, or information) that doesn't belong to you.
- • Typosquatting - Setting up a domain that is a misspelling of another domain.
- • Unauthorized access - Gaining access to systems you have no permission to access.
- • Vandalism - Damaging any hardware, software, website, or other object.
- • Wiretapping - Connecting a device to a phone line to listen to conversations.

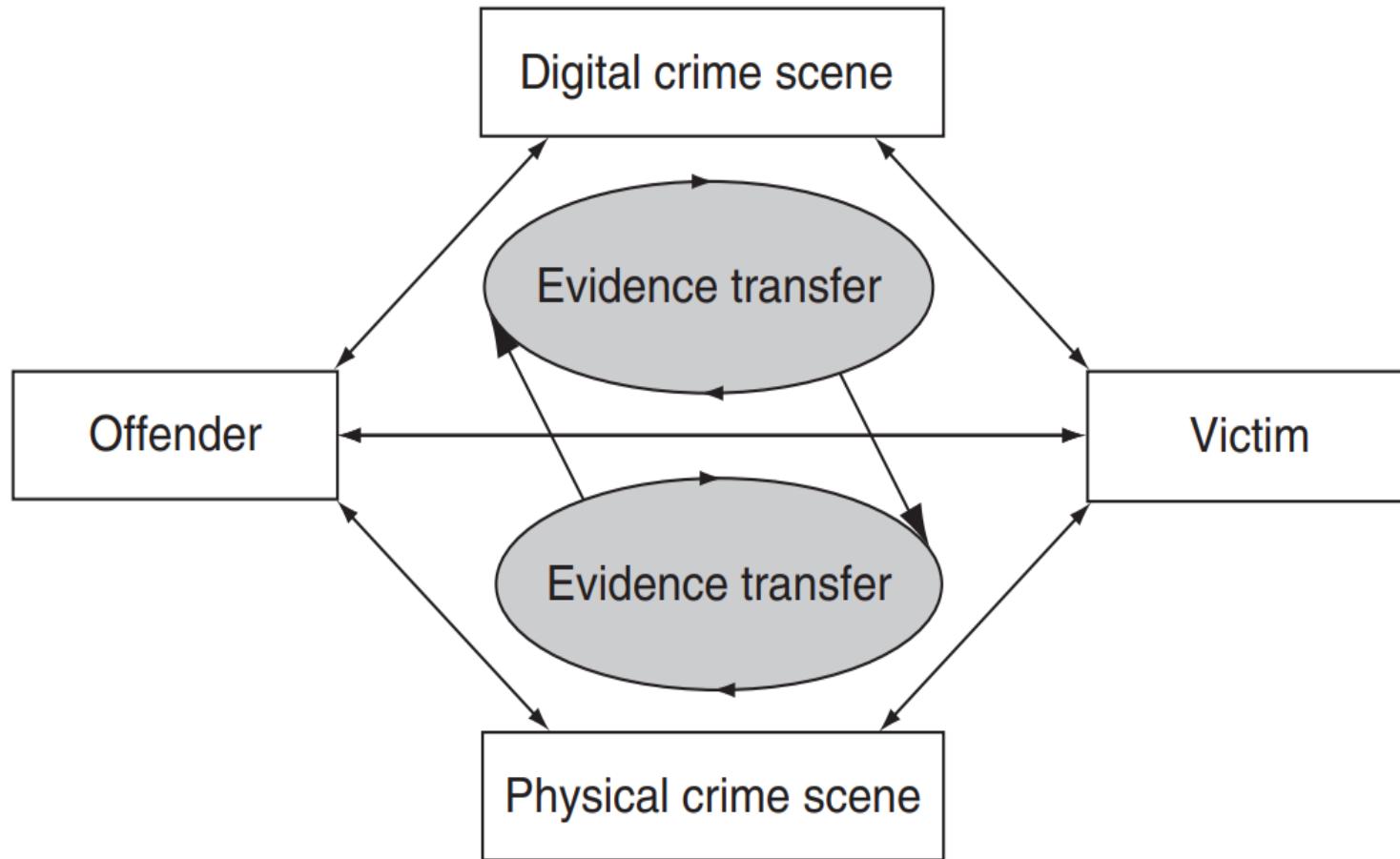
Locard's Principle

- "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 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 evidences 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."

Evidence Exchange

- The main goals in any investigation are to follow the trails that offenders leave during the commission of a crime.
- According to Locard's Exchange Principle also, contact between two items will result in an exchange.
- This principle applies to any contact at a crime scene, including between an offender and victim, between a person with a weapon, and between people and the crime scene itself.
- There will always be evidence of the interaction, although in some cases it may not be detected easily (note that absence of evidence is not evidence of absence).
- This transfer occurs in both the physical and digital realms and can provide links between them.

Evidence transfer in the physical and digital dimensions helps investigators establish connections between victims, offenders, and crime scenes



- The attackers will leave multiple traces of their presence throughout the environment, including in the file systems, registry, system logs, and network-level logs.
- The attackers could transfer elements of the crime scene back with them, such as stolen user passwords or PII in a file or database.
- Such evidence can be useful to link an individual to an intrusion.

- In an e-mail harassment case, the act of sending threatening messages via a Web-based e-mail service such as Hotmail can leave a number of traces.
- The Web browser used to send messages will store files, links, and other information on the sender's hard drive along with date-time-related information.
- Therefore, forensic analysts may find information relating to the sent message on the offender's hard drive, including the original message contents.

- **Digital evidence** is usually not in a format that is directly readable by human.
- Therefore it requires some additional steps to convert it into a human readable form in the form of writing.
- Digital evidence can be duplicated exactly and a copy can be examined as if it were the original.
- It is common practice when dealing with digital evidence to examine a copy, thus avoiding the risk of altering or damaging the original evidence.

- With the right tools, it is very easy to determine if digital evidence has been modified or tampered with by comparing it with an original copy.
- Digital evidence is not difficult to destroy. Even when a file is “deleted” or a hard drive is formatted, digital evidence can be recovered.
- When criminals attempt to destroy digital evidence, copies and associated remnants can remain in places that they were not aware of.
- Digital evidences must follow the requirements of the **Best Evidence Rule**.

Best Evidence Rule

The best evidence rule, states that the court prefers the original evidence at the trial rather than a copy, but will accept a duplicate under these conditions:

1. 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.
2. The original was destroyed in the normal course of business.
3. The original is in possession of a third party who is beyond the court's 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.

Characteristics of Digital Evidence

- **Admissibility:** It must be in conformity with common law and legislative rules.

There must be relationship between the evidence and the fact being proved.

Digital evidence is often ruled inadmissible by courts if 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.

- **Reliability:** The evidence must be from indisputed origin.

- **Completeness:** The evidence should prove the culprit 's actions and help to reach a conclusion.
- **Convincing to Judges:** The evidence must me 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.
 - ✓ the measures taken to ensure the accuracy of the data as entered.
 - ✓ the method of storing the data and the precautions 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.

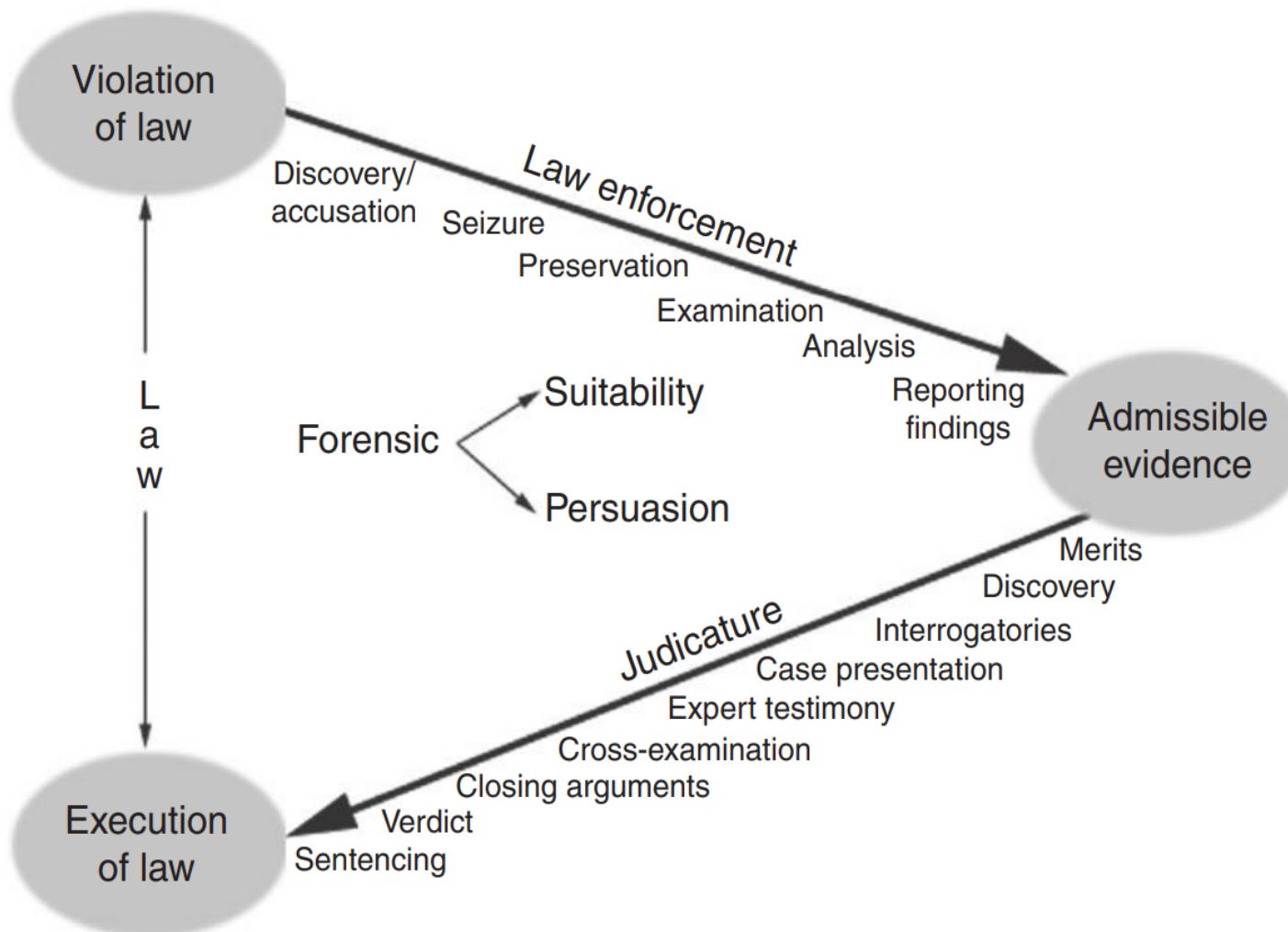
- **Evidence Dynamics and the Introduction of Error**
- Investigators and digital evidence examiners will rarely have an opportunity to examine a digital crime scene in its original state
- and should therefore expect some evidence dynamics: any influence that changes, relocates, obscures, or obliterates evidence, regardless of intent between the time evidence is transferred and the time the case is resolved.
- Offenders, victims, first responders, digital evidence examiners, and anyone else who had access to digital evidence prior to its preservation can cause evidence dynamics.

- **Examples of Evidence Dynamics**
- A system administrator attempted to recover deleted files from a hard drive by installing software on an evidential computer, saving recovered files onto the same drive.
- Consultants installed a pirated version of a forensic tool on the compromised server.
- In addition to breaking the law by using an unlicensed version of digital forensic software, the installation altered and overwrote data on the evidential computer.

- A system administrator intentionally deleted an account that the intruder had created and attempted to preserve digital evidence using the standard backup facility on the system.
- This backup facility was outdated and had a flaw that caused it to change the times of the files on the disk before copying them.
- Thus, the date-time stamps of all files on the disk were changed to the current time, making it nearly impossible to reconstruct the crime.

- During an investigation involving several machines, a first responder did not follow standard operating procedures and failed to collect important evidence.
- Evidence collected from several identical computer systems was not thoroughly documented, making it very difficult to determine which evidence came from which system.

Overview of case/incident resolution process



Search Warrants:

- The most common mistake that prevents digital evidence from being admitted by courts is that it is obtained without authorization.
- Generally, a warrant is required to search and seize evidence.
- To obtain a warrant, investigators must demonstrate probable cause and detail the place to be searched and the persons or things to be seized.
- Investigators have to convince a judge or magistrate that, in all probability:
 - 1. a crime has been committed;
 - 2. evidence of crime is in existence; and
 - 3. the evidence is likely to exist at the place to be searched.

- In urgency, a **warrantless search** can be made for any emergency threatening life or in which digital evidence is likely to be altered or destroyed.
- In these circumstances, it may be necessary to seize the computing device immediately to reduce the potential of destruction of evidence.
- After the digital evidence is preserved, it is prudent to obtain a warrant to conduct a forensic examination of the digital evidence.

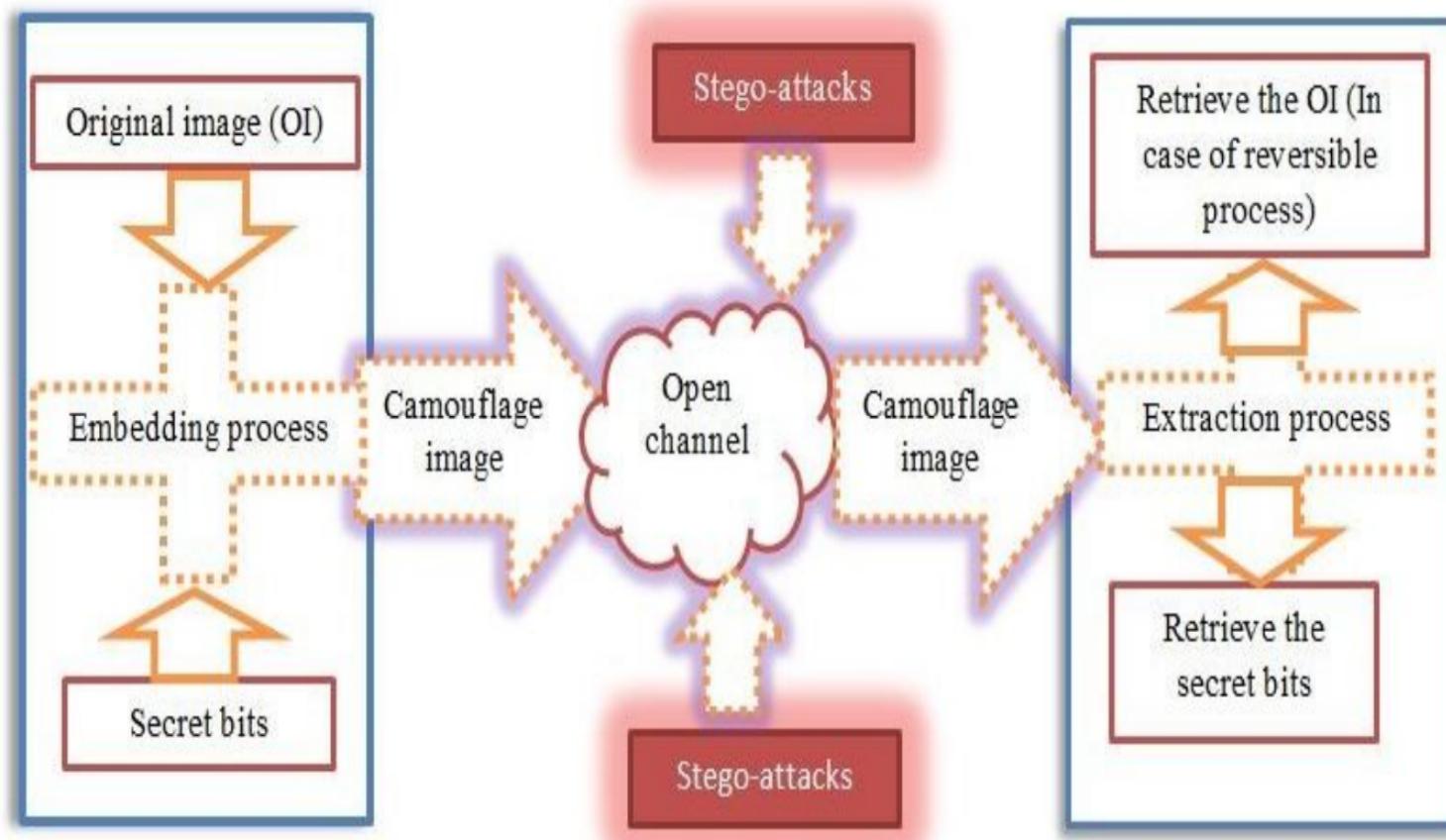
Types of Digital Forensics Tools

- Hardware Forensics Tools - T35es-R2 SATA
- Software Forensics Tools - AccessData FTK

Steganography

- The word is derived from two Greek words- ‘stegos’ meaning ‘to cover’ and ‘grayfia’, meaning ‘writing’, thus translating to ‘covered writing’, or ‘hidden writing’.
- **Steganography** is a method of hiding secret data, by embedding it into an audio, video, image, or text file.
- It is one of the methods employed to protect secret or sensitive data from malicious attacks.

Structure of the steganographic communication process.



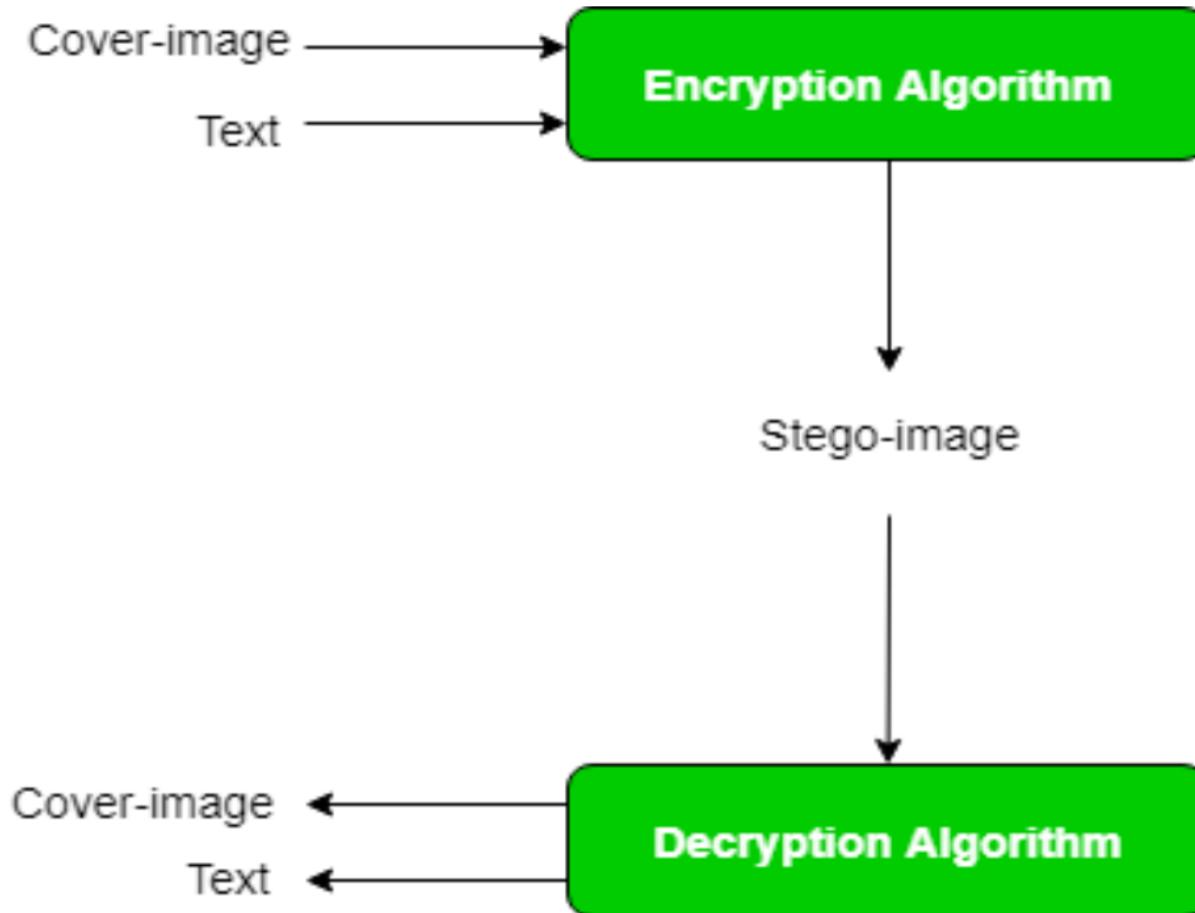
- **Image Steganography –**
- Process of hiding data within an image file. The image selected for this purpose is called the **cover image** and the image obtained after steganography is called the **stego image**.
- Due to the property of innocence of digital images, researchers have preferred images as the carrier signal for hiding secret information. Also, the presence of redundant pixels in an image makes it even more suitable for embedding secret information.
- Hiding confidential information inside the image is known as image steganography (IS)

- **How IS it done?**

An image is represented as an $N \times M$ (in case of grayscale images) or $N \times M \times 3$ (in case of color images) matrix in memory, with each entry representing the intensity value of a pixel.

- In image steganography, a message is embedded into an image by altering the values of some pixels, which are chosen by an encryption algorithm.
- The recipient of the image must be aware of the same algorithm in order to know which pixels he or she must select to extract the message.

Process of Image Steganography



What is Steganography, Cryptography and Steganalysis?

- Steganography refers to modifying a digital object (cover) to encode and conceal a sequence of bits (message) to facilitate covert communication.
- Steganalysis refers to efforts to detect (and possibly prevent) such communication.
- Cryptography, on the other hand, fails at this, as it is possible to detect (the presence of) encrypted-communication.
- Steganalysis has been used to detect the presence of steganography and acts as a countermeasure to it.
- Steganalysis is the study of detecting messages hidden using steganography; this is analogous to cryptanalysis applied to cryptography.
-

- Steganalysis detection methods can be classified into two categories: specific and general detection.
- The specific detection methods deal with the targeted steganographic systems, while the general detection methods provide detection regardless of what the steganographic systems are.
- Example: for copyright protection; used by criminals or terrorists for malicious purposes; used to transmit the secret plan of terror attacks.

Cryptography/Cryptanalysis	Steganography/Steganalysis
Combining plaintext and a cryptographic tool yields cipher-text.	Combining text with a steganographic tool yields a stego-object.
Plaintext and cipher-text are utilized when performing cryptanalysis.	The carrier, stego-object and hidden message may be used when performing steganalysis.
A cipher-text only attack is where only the cipher-text is known to the analyst.	A stego-only attack is where only the stego-object is available for attack.
A chosen plain-text attack is where a portion of the plain-text, which corresponds to a portion of the cipher-text, are available for analysis.	A chosen stego attack is where the Steganography tool (algorithm) and the stego object are known.

Types of Technical Steganalysis

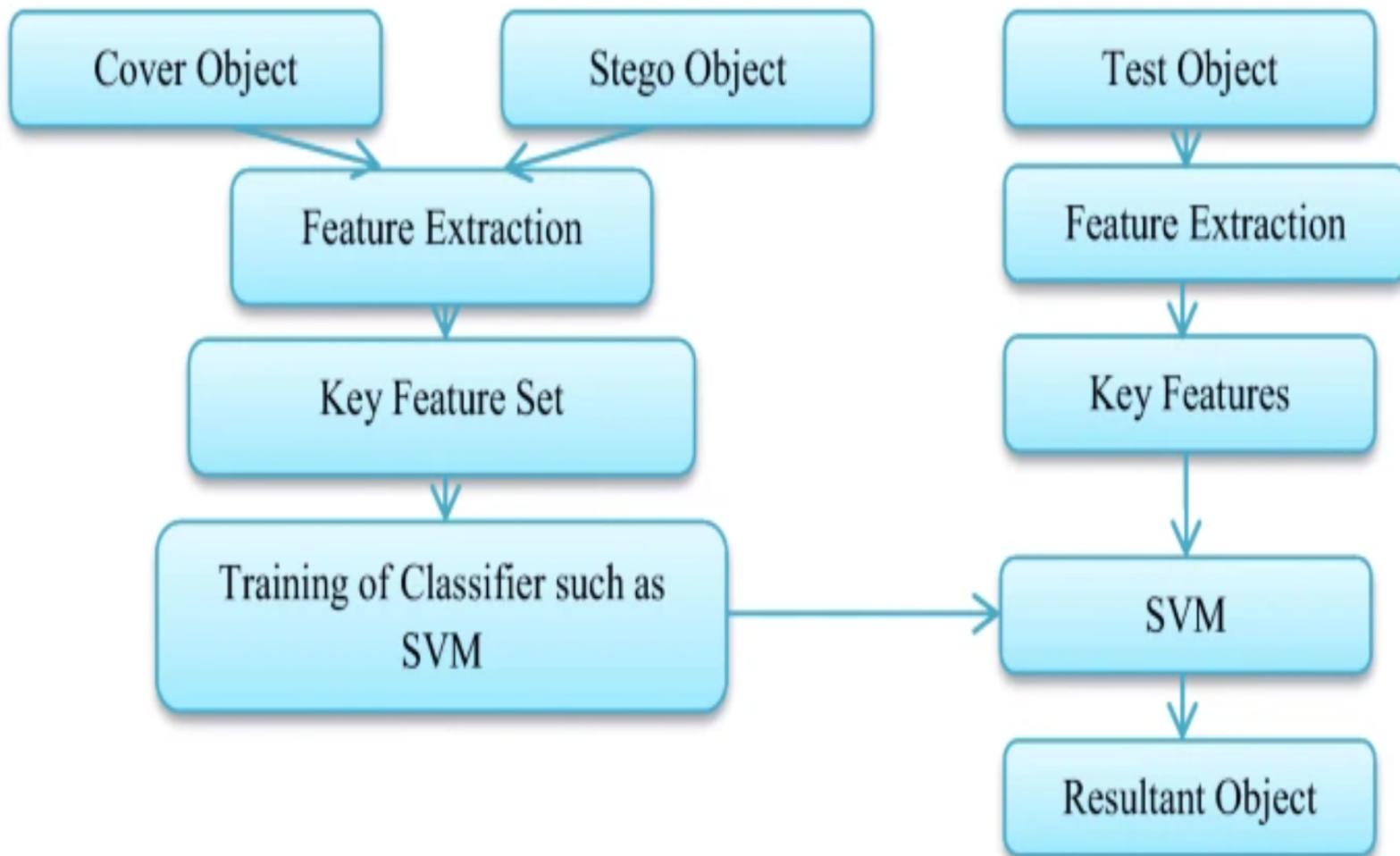
- Stego only attack - only the stego object is available for analysis.
- Known cover attack - the cover and the stego object are both available for analysis.
- Known message attack - the message is known and can be compared with the stego object.
- Chosen stego attack - the stego object and the stego tool (algorithm) are available for analysis.
- Chosen message attack - the steganalyst generates stego-media from some steganography tool or algorithm from a known message. The goal in this attack is to determine corresponding patterns in the stego-media that may point to the use of specific steganography tools or algorithms.
- Known stego attack - the steganography tool (algorithm) is known and both the original and stego-object are available.

- Cover medium can be an image file, an audio file, a video file, a network packet or even a text file.
- As more elements are known to a digital forensics examiner, the more effective steganalysis will be.
- Steganalysis becomes more complex when moving from detection only, to detecting and deciphering the embedded message i.e. moving from **passive to active steganalysis**.
- Theoretically, this concerns any type of digital objects, but practically -in most cases- audiovisual files are more frequently met.

- Two major approaches were adopted by scientists.
- The first one refers to extraction of statistical features from stego and clean images. These statistical features are compared then, in order to discriminate clean from stego images.
- The second general approach is by employing machine learning techniques. Thus, features are extracted from images (both clean and stego), a classifier is trained, and finally unseen images are presented to the model for evaluation.

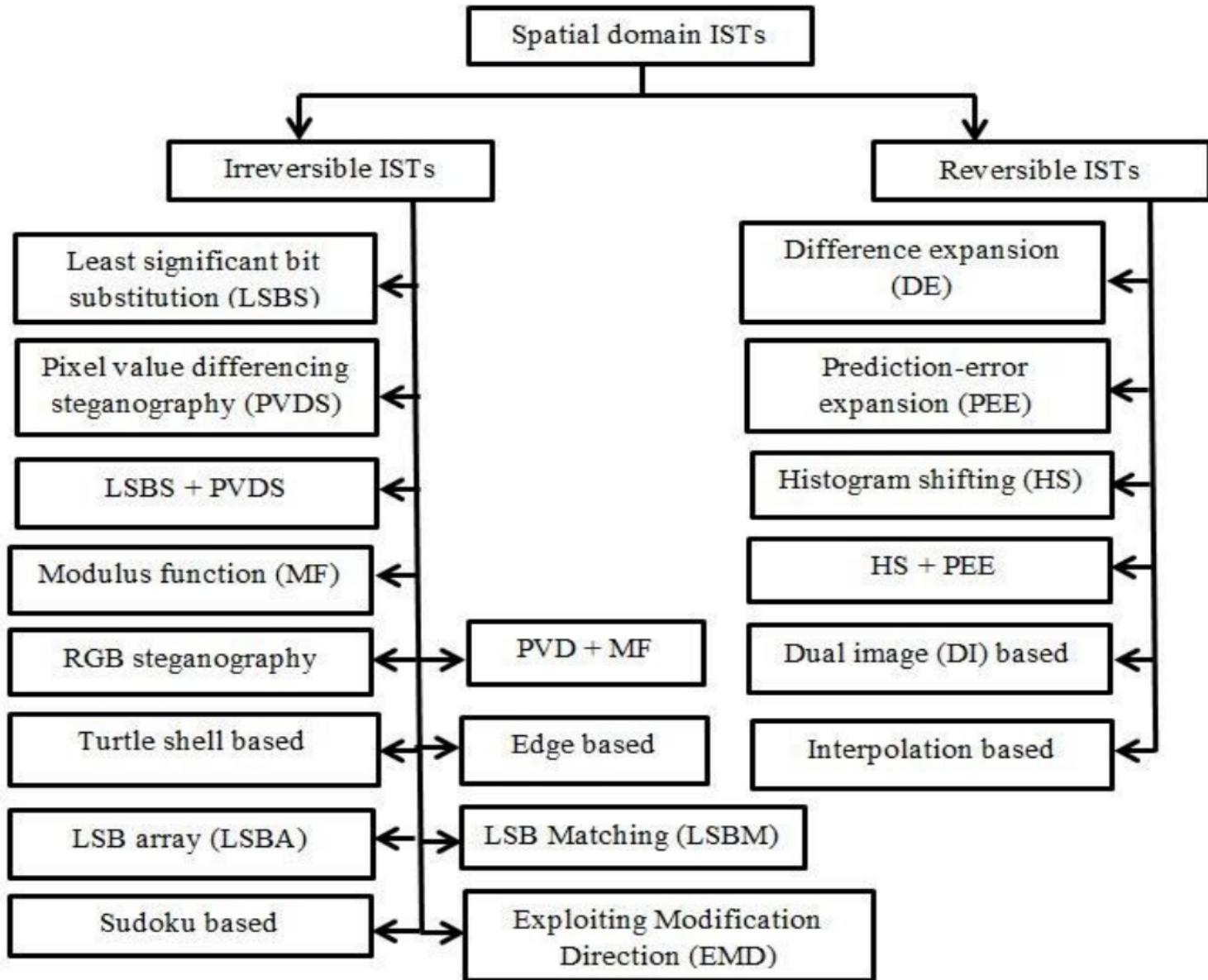
- Classifiers like Support Vector Machines (SVM) and Artificial Neural Networks (ANN) were used.
- Recent days we employ deep learning techniques such as convolutional neural networks or deep autoencoders, where feature extraction and selection is made in an almost automatic way.

Paradigm For Machine Learning Classifiers



- **Spatial domain techniques** depend solely on the pixels of the image for data embedding.
 - Here direct manipulation of the OI (original image) pixels is performed to achieve the objective. Therefore, spatial domain techniques are simple and less time-consuming.
-
- **Transform domain techniques** utilize the frequency content, and they are based on orthogonal transformation (frequency and phase) to the image.
 - Here applying various transformations and inverse transformations, such as Fourier, Laplace, and Z the embedding process is carried out.
 - Common transform domain techniques are (1) discrete Fourier transformation (DFT) (2) discrete wavelet transformation (DWT) (3) discrete cosine transformation (DCT), and (4) singular value decomposition.

- In the context of IS, the original image (OI) is the one input image that is used for sending the secret data.
- The camouflage image (CI) is the output image which carries the secret information.
- The secret information is the confidential message that the sender wants to transmit to the receiver.
- Finally, the embedding and extraction algorithms are the data hiding algorithms that are used to embed and extract the secret bits, respectively.



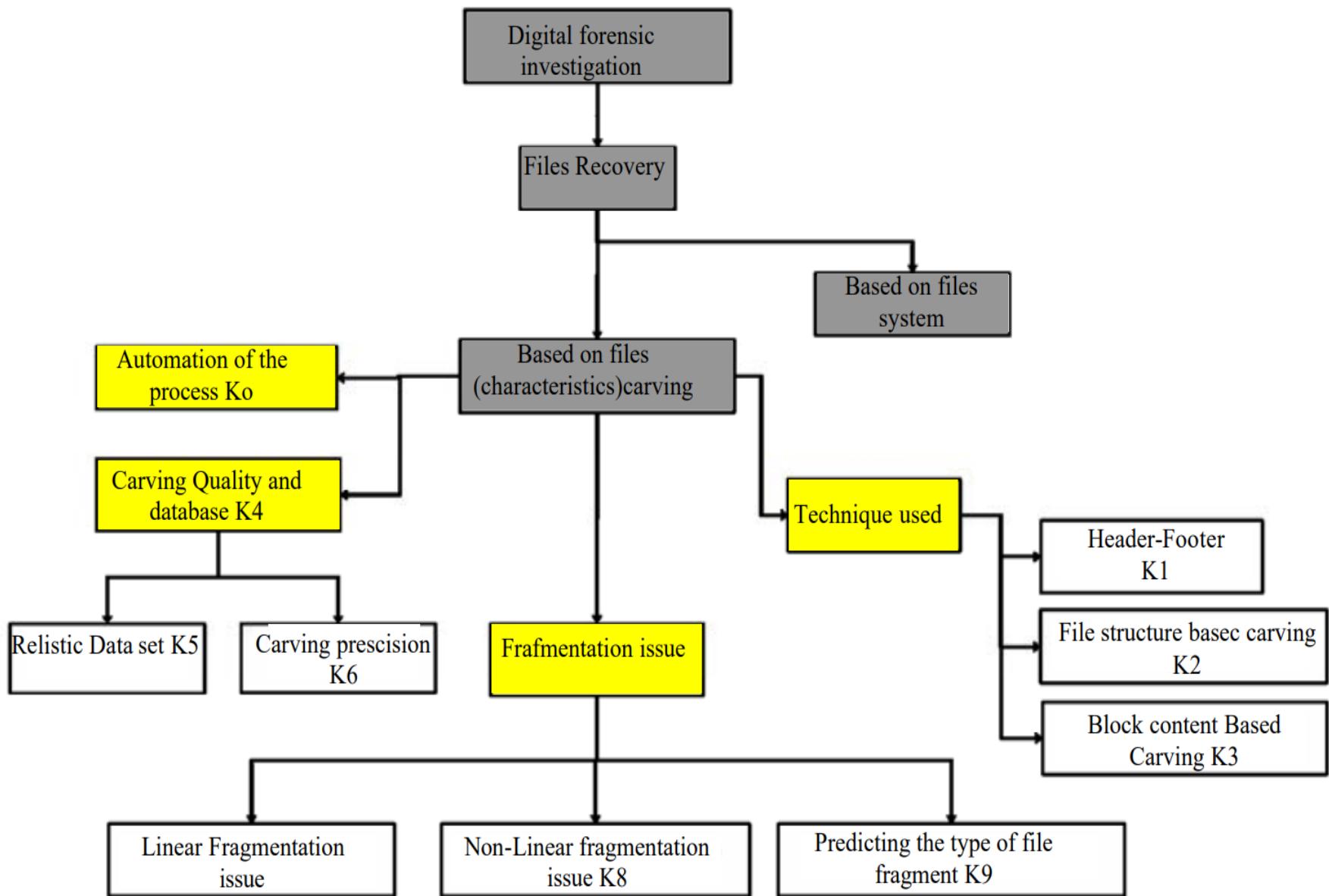
Performance appraisal metrics for the ISTs

- The primary objectives for any ISTs are to simultaneously achieve:
 - (1) high HC (Hiding capacity)
 - (2) better imperceptibility (high perceptual quality)
 - (3) greater robustness or security.
- HC refers to the ability to hide the maximum number of secret data. It is usually computed in bits.
- Imperceptibility suggests CI quality. The CI and OI should be visually indistinguishable.

Metric	Condition
HC	Should be High
Imperceptibility	Should be High
Security or ARA	Should be High
Tamper resistance	Should be High
Computation complexity	Should be Low

- The quality of CI can be computed using various image quality assessment metrics such as
 - (1) mean square error (MSE),
 - (2) peak signal-to-noise ratio (PSNR),
 - (3) weighted PSNR (WPSNR)
 - (4) root mean square error (RMSE),
 - (5) universal image quality index (Q),
 - (6) structural similarity index (SSIM),
 - (7) normalized cross-correlation (NCC),
 - (8) Kullback-Leibler (KL) divergence (DKL),
 - (9) Manhattan distance (MD) and
 - (10) Euclidean distance (ED).
 - (11) Attack resistance ability (ARA) related to security.

Data Recovery Research Areas



- **Data recovery** is a process of retrieving deleted, inaccessible, lost, corrupted, damaged, or formatted data from secondary storage, removable media or files, when the data stored in them cannot be accessed in a usual way.
- Recovery may be required due to physical damage to the storage devices or logical damage to the file system that prevents it from being mounted by the host operating system (OS).
- Logical failures occur when the hard drive devices are functional but the user or automated-OS cannot retrieve or access data stored on them.
- Logical failures can also occur due to corruption of the chip, lost partitions, firmware failure, or failures during formatting/re-installation.

- **Data Recovery Scenarios** are an operating system failure, malfunction of a storage device, logical failure of storage devices, accidental damage or deletion, etc. in which case the ultimate goal is simply to copy all important files from the damaged media to another new drive.
- This can be accomplished using a **Live CD/USB**, or DVD by booting directly from a ROM or a USB drive instead of the corrupted drive in question.
- A **live CD/USB Or live operating system** is a complete bootable computer installation including operating system which runs directly from a CD-ROM or similar storage device into a computer's memory, rather than loading from a hard disk drive.
- A live CD/USB allows users to run an operating system for any purpose without installing it or making any changes to the computer's configuration.
- Live CD/USB can run on a computer without secondary storage, such as a hard disk drive, or with a corrupted hard disk drive or file system, allowing data recovery.

- Second scenario involves a **drive-level failure**, such as a compromised file system or drive partition, or a hard disk drive failure.
- In any of these cases, the data is not easily read from the media devices. Depending on the situation, solutions involves:
 1. repairing the logical file system,
 2. partition table,
 3. master boot record,
 4. updating the firmware
 5. drive recovery techniques ranging from software-based recovery of corrupted data to hardware, and software-based recovery of damaged service areas to hardware replacement on a physically damaged drive
- If a drive recovery is necessary and the drive itself has typically failed permanently, then focus is on a one-time recovery, saving whatever data can be read.

- Third scenario is where **files have been accidentally** "deleted" from a storage medium by the users.
- Usually the contents of deleted files are not removed immediately from the physical drive; instead, references to them in the directory structure are removed, and thereafter space the deleted data occupy is made available for later data overwriting.
- In the mind of end users, deleted files cannot be discoverable through a standard file manager, but the deleted data still technically exists on the physical drive.
- In the meantime, the original file contents remain, often several disconnected fragments, and may be recoverable if not overwritten by other data files.

Physical damage

- Human errors, natural disasters. CD-ROMs can have their metallic substrate or dye layer scratched off; hard disks can suffer from a multitude of mechanical failures, such as head crashes, PCB failure, and failed motors; tapes can simply break.
- Physical damage to a hard drive, even in cases where a head crash has occurred, does not necessarily mean there will be a permanent loss of data.
- The techniques employed by many professional data recovery companies can typically salvage most, if not all, of the data that had been lost when the failure occurred.
- Severe damage to the hard drive platters may have occurred. However, if the hard drive can be repaired and a full image or clone created, then the logical file structure can be rebuilt in most instances.

- Most physical damage cannot be repaired by end users.
- **For example**, opening a hard disk drive in a normal environment can allow airborne dust to settle on the platter and become caught between the platter and the read/write head.
- During normal operation, read/write heads float above the platter surface. When these dust particles get caught between the read/write heads and the platter, they can cause new head crashes that further damage the platter and thus compromise the recovery process.
- Furthermore, end users generally do not have the hardware or technical expertise required to make these repairs.
- Consequently, data recovery companies are often employed to save important data.

File Carving

- File carving is a process used in computer forensics to extract data from a disk drive or other storage device without the assistance of the file system that originally created the file.
- This process may be successful even after a drive is formatted or repartitioned.
- File carving can be performed using free or commercial software and is often performed in conjunction with computer forensics examinations or alongside other recovery efforts (e.g. hardware repair) by data recovery companies.
- Whereas the primary goal of data recovery is to recover the file content, computer forensics examiners are often just as interested in the metadata such as who owned a file, where it was stored, and when it was last modified.

- File carving is the process of trying to recover files without this metadata.
- This is done by analyzing the raw data and identifying what it is (text, executable, png, mp3, etc.).
- This can be done by file signature or "magic numbers" that mark the beginning and/or end of a particular file type.
- Like every Java class file has as its first four bytes the hexadecimal value CA FE BA BE.
- Some files contain footers as well, making it simple to identify the ending of the file.

- FAT family and UNIX's Fast File System, work with the concept of clusters of an equal and fixed size.
- For example, a FAT32 file system might be broken into clusters of 4 KiB each. Any file smaller than 4 KiB fits into a single cluster, and there is never more than one file in each cluster.
- Files that take up more than 4 KiB are allocated across many clusters.
- Sometimes these clusters are all contiguous, while other times they are scattered across two or potentially many more so called fragments, with each fragment containing a number of contiguous clusters storing one part of the file's data.
- Large files are more likely to be fragmented.

- While fragmentation in a typical disk is low, the fragmentation rate of forensically important files such as email, JPEG and Word documents is relatively high.
- Research shows that the fragmentation rate of JPEG files was found to be 16%, Word documents had 17% fragmentation, AVI had a 22% fragmentation rate and PST files (Microsoft Outlook) had a 58% fragmentation rate (the fraction of files being fragmented into two or more fragments).
- There are efficient algorithms based on a greedy heuristic and pruning for reassembling fragmented images.
- Scalpel, an open-source file-carving tool existing since 2005.
- File carving is a highly complex task, with a potentially huge number of permutations to try. To make this task tractable, carving software makes extensive use of models and heuristics.
- This is necessary not only from a standpoint of execution time, but also for the accuracy of the results.

Carving Schemes

I. Bifragment gap carving

- Garfinkel introduced the use of fast object validation for reassembling files that have been split into two pieces.
- This technique is referred to as Bifragment Gap Carving (BGC).
- A set of starting fragments and a set of finishing fragments are identified.
- The fragments are reassembled if together they form a valid object.

II. SmartCarving

- Pal developed a carving scheme that is not just limited to bifragmented files.
- The technique, known as SmartCarving, makes use of heuristics regarding the fragmentation behavior of known filesystems.
- The algorithm has three phases: preprocessing, collation, and reassembly.
- In the preprocessing phase, blocks are decompressed and/or decrypted if necessary.
- In the collation phase, blocks are sorted according to their file type.
- In the reassembly phase, the blocks are placed in sequence to reproduce the deleted files.
- The SmartCarving algorithm is the basis for the Adroit Photo Forensics and Adroit Photo Recovery applications from Digital Assembly.

III. Carving Memory Dumps

- Snapshots of computers' volatile memory (i.e. RAM) can be carved.
- Memory-dump carving is routinely used in digital forensics, allowing investigators to access ephemeral evidence.
- Ephemeral evidence includes recently accessed images and Web pages, documents, chats and communications committed via social networks.

- **File carving vs Data carving**
- File carving is used as an attempt to use file header to reconstruct the whole file. If a file header were damaged, recovery of a file would be impossible.
- Data carving can be seen as carving of parts of a file in order to try to collect bits of data that might be relevant to the case.

Forensic Data Carving method uses the following methods:

1. Header/Footer carving
2. Header/Embedded length carving
3. File structure based carving
4. Carving with validation and
5. Header/Maximum file size carving

Recovery Techniques

- Recovering data from physically damaged hardware can involve multiple techniques.
- Some damage can be repaired by replacing parts in the hard disk, but there may still be logical damage.
- A specialized disk-imaging procedure is used to recover every readable bit from the surface.
- Once this image is acquired and saved on a reliable medium, the image can be safely analyzed for logical damage and will allow much of the original file system to be reconstructed.

Hardware Repair

- Media that has suffered a catastrophic electronic failure requires data recovery in order to salvage its contents
- A damaged printed circuit board (PCB) cannot be simply replaced during recovery procedures by an identical PCB from a healthy drive.
- Electronics boards of modern drives usually contain drive-specific adaptation data and other information required to properly access data on the drive.
- Replacement boards need this information to effectively recover all of the data.
- The replacement board may need to be reprogrammed.
- Some manufacturers store this information on a serial EEPROM chip, which can be removed and transferred to the replacement board.

Logical Damage

- “Logical damage” refers to situations in which the error is not in the hardware but is in software and so it requires software-level solutions.
- **Corrupt partitions and file systems, media errors**
- Data on a hard disk drive can be unreadable due to damage to the partition table or file system, or to (intermittent) media errors.
- In the majority of these cases, at least a portion of the original data can be recovered by repairing the damaged partition table or file system using specialized data recovery software.
- Recovering image media despite intermittent errors, and image raw data when there is partition table or file system damage.

Overwritten Data

- After data has been physically overwritten on a hard disk drive, it is generally assumed that the previous data are no longer possible to recover.
- But overwritten data could be recovered through the use of magnetic force microscopy.
- Irreversibly scrubbing data is used by several disk-scrubbing software packages.
- Solid-state drives (SSD) overwrite data differently from hard disk drives which makes at least some of their data easier to recover.
- Most SSDs use flash memory to store data in pages and blocks, referenced by logical block addresses (LBA) which are managed by the flash translation layer (FTL).
- When the FTL modifies a sector it writes the new data to another location and updates the map so the new data appear at the target logical block addresses.
- This leaves the pre-modification data in place, with possibly many generations, and recoverable by data recovery software.

Lost, Deleted, And Formatted Data

- Sometimes, data present in the physical drives (Internal/External Hard disk, Pen Drive, etc.) gets lost, deleted and formatted due to circumstances like virus attack, accidental deletion or accidental use of SHIFT+DELETE.
- In these cases, data recovery software is used to recover/restore the data files.

Logical Bad Sector

- A logical bad sector is the most common fault which makes data not to be readable.
- Sometimes it is possible to sidestep error detection even in software, and perhaps with repeated reading and statistical analysis recover at least some of the underlying stored data.
- Sometimes prior knowledge of the data stored and the error detection and correction codes can be used to recover even erroneous data.
- If the underlying physical drive is degraded badly enough, at least the hardware surrounding the data must be replaced, or we may apply laboratory techniques to the physical recording medium.
- Each of the approaches is progressively more expensive, and as such progressively more rarely sought.
- If the final, physical storage medium has been disturbed badly enough, recovery will not be possible using any means; the information has irreversibly been lost.

Remote Data Recovery

- Recovery experts do not always need to have physical access to the damaged hardware.
- When the lost data can be recovered by software techniques, they perform the recovery using remote access software to the physical location of the damaged media.
- Remote recovery requires a stable connection with an adequate bandwidth.
- However, it is not applicable where access to the hardware is required, as in cases of physical damage.

Four Phases Of Data Recovery

- **Phase 1: Repair the hard disk drive.**

The hard drive is repaired in order to get it running in some form, or at least in a state suitable for reading the data from it. For example, if heads are bad they need to be changed; if the PCB is faulty then it needs to be fixed or replaced; if the spindle motor is bad the platters and heads should be moved to a new drive.

- **Phase 2: Image the drive to a new drive or a disk image file.**

When a hard disk drive fails, the importance of getting the data off the drive is the top priority. The longer a faulty drive is used, the more likely further data loss is to occur. Creating an image of the drive will ensure that there is a secondary copy of the data on another device, on which it is safe to perform testing and recovery procedures without harming the source.

- **Phase 3: Logical recovery of files, partition, MBR and file system structures**

After the drive has been cloned to a new drive, it is suitable to attempt the retrieval of lost data. If the drive has failed logically, there are a number of reasons for that. Using the clone it may be possible to repair the partition table or master boot record (MBR) in order to read the file system's data structure and retrieve stored data.

- **Phase 4: Repair damaged files that were retrieved**

Data damage can be caused when, for example, a file is written to a sector on the drive that has been damaged. This is the most common cause in a failing drive, meaning that data needs to be reconstructed to become readable. Corrupted documents can be recovered by several software methods or by manually reconstructing the document using a hex editor.

FTK (Forensic Tool Kit)

- FTK is a court-accepted digital investigations platform that is built for speed, analytics and enterprise-class scalability.
- Known for its intuitive interface, email analysis, customizable data views and stability, FTK lays the framework for seamless expansion.
- It also offers new expansion modules delivering an industry-first malware analysis capability.
- These modules integrate with FTK to create the most comprehensive computer forensics platform.
- Cerberus is a malware triage technology that is available as an add-on for FTK. It is first layer of evidence against risk of imaging unknown devices and allows to identify infected files.

Explanation on the usage of WinHex, Autopsy and Recuva

Event Logs and Password Cracking

- Log management and intelligence, log analysis (or system and network log analysis) is an art and science seeking to make sense out of computer-generated records (also called log or audit trail records).
- The process of creating such records is called data logging.
- Why perform log analysis are:
 - ❑ Compliance with security policies
 - ❑ Compliance with audit or regulation
 - ❑ System troubleshooting
 - ❑ Forensics (during investigations or in response to subpoena)
 - ❑ Security incident response

- The Security Log, in Microsoft Windows, is a log that contains records of login/logout activity or other security-related events specified by the system's audit policy.
- Auditing allows administrators to configure Windows to record operating system activity in the Security Log.
- Event logging provides system administrators with information useful for diagnostics and auditing.
- The different classes of events that will be logged, as well as what details will appear in the event messages, are often considered early in the development cycle.
- Many event logging technologies allow or even require each class of event to be assigned a unique "code", which is used by the event logging software or a separate viewer (e.g., Event Viewer) to format and output a human-readable message.
- This facilitates localization and allows system administrators to more easily obtain information on problems that occur.

- Windows registry is also a very important source to maintain and manage logs.
- Registry also has variety of controls/keys where general records pertaining events etc. are maintained which can be very vital during digital forensics.
- The purpose of password cracking might be to help a user recover a forgotten password, to gain unauthorized access to a system, or as a preventive measure by System Administrators to check for easily crack-able passwords.
- On a file-by-file basis, password cracking is utilized to gain access to digital evidence for which a judge has allowed access but the particular file's access is restricted.

Windows Registry

- Windows registry keeps most of the information pertaining policies, status etc. in form of keys, sub keys and values.
- The Registry is a database of configurations used by applications, services, and all other aspects of Windows.
- It can be worked upon by administrator through application like 'regedit'.
- The Registry Editor, known as "regedit," allows to make high-level changes to the system by adding, removing, or modifying keys and values.
- Incorrectly editing the Registry can permanently damage your PC.
- Windows can also be supplied with a command like tool like 'reg' to help users work on registry.
- Registry contains hives under which sub keys are present.
- These hives play important role in the overall functioning of the system.

Registry And Forensics

- An investigator can acquire quite a good deal of information by studying and analysing registry.
- Many tools like ProDiscover, ProScript can be very handy to get a good deal of analysis of registry entries.
- Registry entries can be used to acquire and analyse many important information necessary for forensics analysis.
- These information use system, time zone, shares, audit policy, wireless SSIDS, auto start locations, user login, activities, USB removable devices, trusted devices, cache, cookie and history etc.

Log Attributes and Respective Registry Keys

System Information	Key
Computer Name	SYSTEM\CurrentControlSet\Control\ComputerName\ActiveComputerName
Time of last shutdown	SYSTEM\ControlSet00x\Control\Windows
Product name ,build, version etc.	SOFTWARE\Microsoft\Windows NT\CurrentVersion
Time zone settings	SYSTEM\CurrentControlSet\Control\TimeZoneInformation
User created shares	SYSTEM\CurrentControlSet\Services\lanmanserver\Shares
Audit policy	\SECURITY\Policy\PolAdtEv
Wireless SSIDs	SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces\{GUID}
USB devices connected	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Enum\USBSTOR
last time	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses
Mounted Devices	HKEY_LOCAL_MACHINE\System\MountedDevices
User	SAM\SAM\Domains\Account\Users\{RID}

information stored in the user's	Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{GUID}\Count
most recently used	\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
most recently used	\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
Search Assistant MRU Lists	Software\Microsoft\Search Assistant\ACMru
Internet downloads directory	Computer\HKEY_CURRENT_USER\Software\Microsof
Restore points	HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\SystemRestore

Few important keys and their paths, These information acquired using these keys has to be recorded using EnCase and can lead to many conclusions while putting up the case.

The proven, powerful, and trusted EnCase®, Forensic solution, lets examiners acquire data from a wide variety of devices, unearth potential evidence with disk level forensic analysis, and craft comprehensive reports on their findings, all while maintaining the integrity of their evidence.

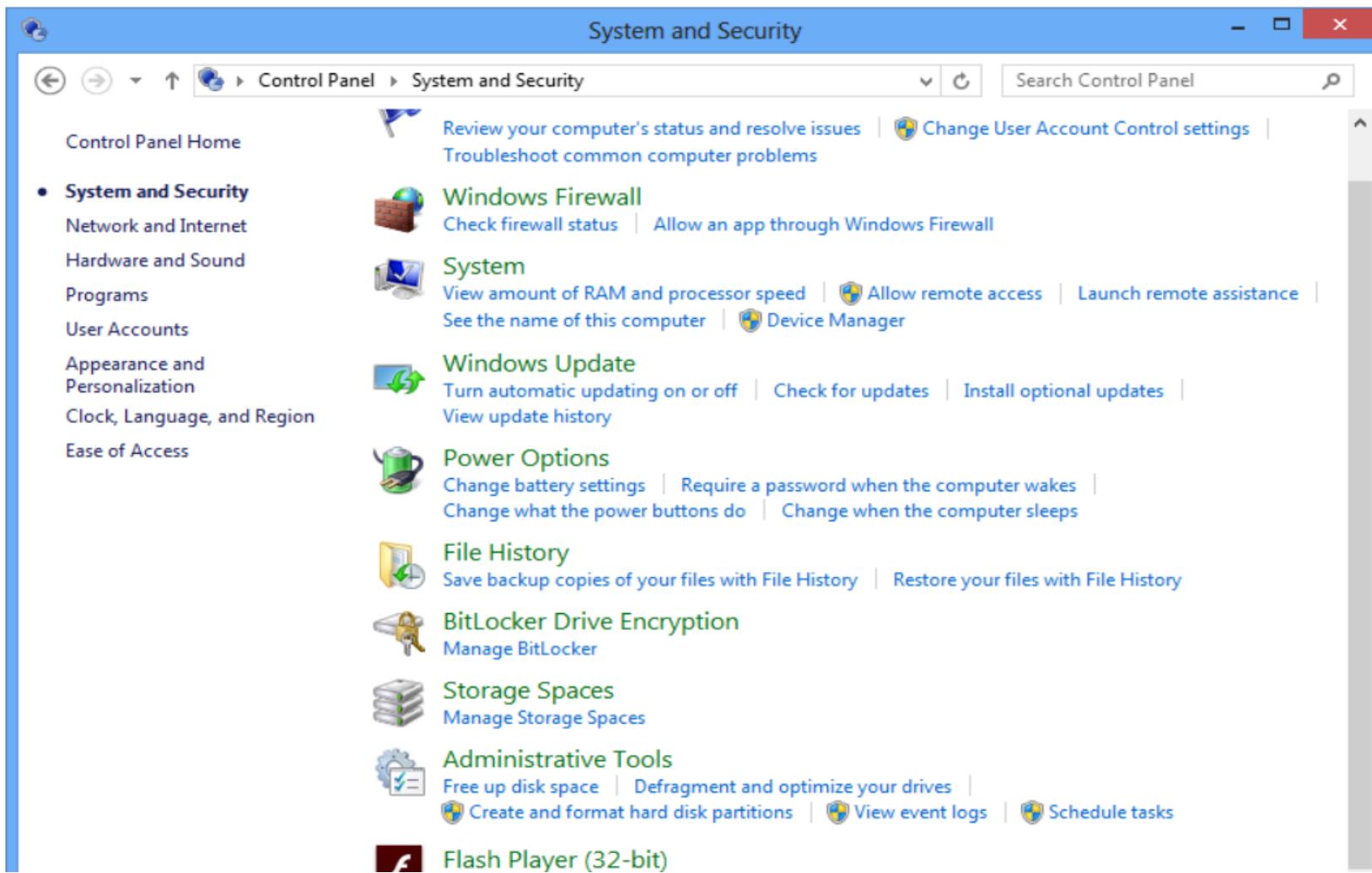
- ‘Computers’ here is the name that the user gives to its computer.
- The name of computer generally is made once in the lifetime usage of the system and hence it can be used to trace various activities on network and internet carried by the user.
- Time of last shutdown is the time at which the system was completely shut down. This information can lead us to know the status of the user and time stamps of various files and can co-relate to give an idea of the mental status of the suspect.
- Sometime user themselves create shared folders and applications for others to use over local network or internet (remote desktops).
- This information can be traced out to find and analyse what kind of things or information the user was trying to share and thus stamps of the shared files/folders can also be analysed.
- Audit policy information can be very useful as it can let us know about what types of information/events an investigator should look for in the event log.
- Service set identifications (SSIDs) maintained by Windows can be useful in situations where unauthorized access is need to be investigated and IP addresses needs to be traced.

- A USB mass storage device yields a lot of artifacts when connected to a system.
- These artifacts are persistent in nature and are retained even after the system has been shut down and the information they contain may assist in carrying out forensic analysis on a suspect system.
- Artefacts of a USB devices connected to computer are also registered via PnP (plug and play) manager.
- The sub key is formed for every USB device under the key path “Disk &Ven_###&Prod_###&Rev###”.
- This and other information can be used to trace and collect vital evidences pertaining to a case

- Similar is the case with mounted devices information under registry.
- Many applications maintain MRU (Most Recently Used) lists i.e. they keep a list of recently used files or opened/created files.
- Also search assistant MRU lists are also maintained by search applicants.
- MRU lists of connected systems etc. are also maintained.
- This information can of genuine help to understand victim's state of mind or condition just before the crime.
- System restore points can be studied to understand how and when the user created back-ups.
- Restore points can be used to understand long back status of the user work.

- Events are any occurrences or triggering of an activity.
- The operating system logs some of these occurrences or events.
- However, the key PolAdEvt in registry can be used to set audit configuration in order to log events based on user requirements.
- Other key available for logging events is:
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\<Event Log>

- One can view events logs from the control panel also.



Event Viewer

File Action View Help



- Event Viewer (Local)
 - Custom Views
 - Administrative Events
- Windows Logs
 - Application
 - Security
 - Setup
 - System**
 - Forwarded Events
- Applications and Services Logs
- Subscriptions

System Number of events: 40,561

Level	Date and Time	Source
Information	10/21/2015 10:24:47 AM	Group...
Information	10/21/2015 9:56:38 AM	Windo...
Information	10/21/2015 9:56:38 AM	Windo...
Information	10/21/2015 9:53:40 AM	Group...
Warning	10/21/2015 9:53:40 AM	Group...
Information	10/21/2015 9:37:05 AM	Service...
Information	10/21/2015 9:37:04 AM	Service...
Information	10/21/2015 9:37:04 AM	Service...
Information	10/21/2015 9:37:03 AM	Service...
Information	10/21/2015 9:37:03 AM	Service...
Information	10/21/2015 9:27:02 AM	Service...

Event 1501, GroupPolicy

General Details

The Group Policy settings for the user were processed. No errors were detected since the last successful processing of Group Policy.

Actions

System

- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Find...
- Save All Events As...
- Attach a Task To this Log...

View

Refresh

Help

Event 1501, GroupPolicy (Mic... ▾

- Event Properties
- Attach Task To This Event...
- Copy

Windows Event Log File

- A log file is a computer-generated data file that contains information about usage patterns, activities, and operations within an operating system, application, server or another device.
- Log files show whether resources are performing properly and optimally.
- In windows event logs are stored in binary format. Event logs are stored in form of headers and set of records.
- The event logs are in form of headers and set of records. The event logs are also in form of pipe or buffer where event addition can lead to several of older events out of the file.

Windows Event Log File Format

- Each log file consists of a Header record (given as `ELF_LOGFILE_HEADER` structure) and the Body.
- The body again consists of Event records, the Cursor record and unused space.
- The body could form a ring buffer, where the cursor record will mark the border between the oldest and the newest event record.
- Unused space could be empty, slack and padding.

Windows Event Log (EVT)– ForensicsWiki,

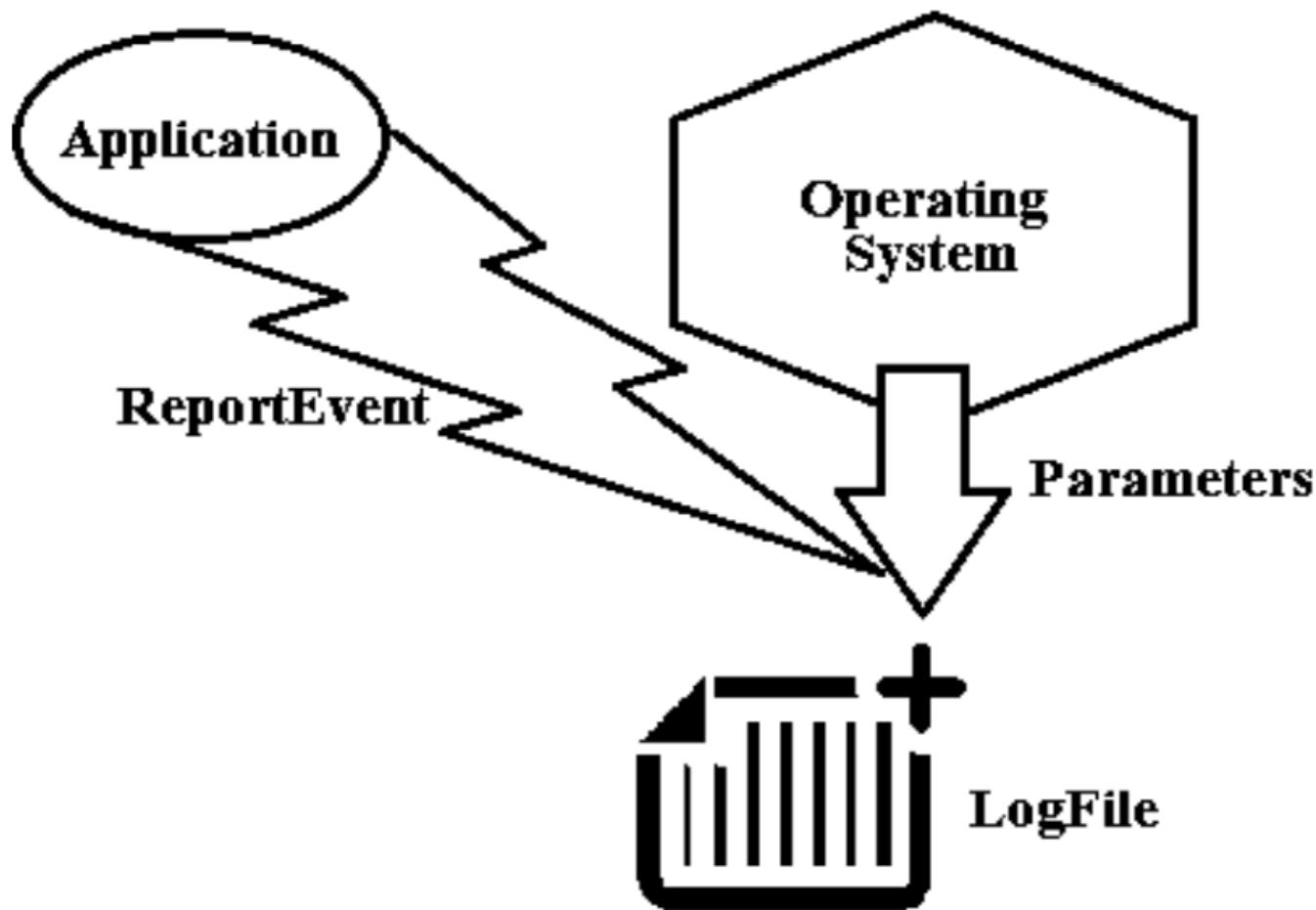
[www.forensicswiki.org/wiki/Windows_Event_Log_\(EVT\)](http://www.forensicswiki.org/wiki/Windows_Event_Log_(EVT))

The Windows XML Event Log (EVTX) format was introduced in Windows Vista as a replacement for the Windows Event Log (EVT) format.

Whenever an event has to be written/created/updated ELF_LOGFILE_HEADER and the ELF_EOF_RECORD structures are written in the event log.

(ELF - Executable and Linkable Format)

Whenever an application needs to log (or is set in registry to log an event) it calls ReportEvent function which adds an EVENTLOGRECORD structure taking the parameters from the system.



- The event records are organized in either non-wrapping or wrapping way.
- The non-wrapping is a simple one where records are added between header and EOF record structures.

- **Non-wrapping:**
- HEADER (ELF_LOGFILE_HEADER) 105
- EVENT 1 (EVENTLOGRECORD)
- .
- .
- .
- EVENT 2 (EVENTLOGRECORD)
- EOF RECORD (ELF_EOF_RECORD)

- The Wrapping mode uses circular way of adding new records.
In this an old record is overwritten as new records come in.
- Where ELF – Event Log File

- **Wrapping:** The Wrapping mode uses circular way of adding new records. In this an old record is overwritten as new records come in.
- HEADER (ELF_LOGFILE_HEADER)
- PART OF EVENT N (EVENTLOGRECORD)
- EVENT N+1 (EVENTLOGRECORD)
- .
- .
- .
- EOF RECORD (ELF_EOF_RECORD)
- Wasted space
- EVENT 1 (EVENTLOGRECORD)
- EVENT 2 (EVENTLOGRECORD)
- .
- .
- .
- PART OF EVENT N (EVENTLOGRECORD)

Reading from an Windows event log file

- On Windows the event logs can be managed with "Event Viewer" (eventvwr.msc) or "Windows Events Command Line Utility" (wevtutil.exe).
- Event Viewer can represent the EVTX (XML format) files in both "general view" (or formatted view) and "details view" (which has both a "friendly view" and "XML view").
- The formatted view can hide significant event data that is stored in the event record and can be seen in the detailed view.
- An event viewer application like Windows Event Viewer or log parser uses the OpenEventLog function to open the event log for an event source. Then the viewer application uses the ReadEventLog function to read event records from the log

Windows Password Storage

- User and passwords in a window system are stored in either of two places:
 - a) SAM(Security Account Manager)
 - b) AD(Activity directory)
- **SAM**
- The Security Account Manager (SAM) is a database file in Windows XP, Windows Vista and Windows 7 that stores users' passwords.
- It can be used to authenticate local and remote users. SAM uses cryptographic measures to prevent forbidden users to gain access to the system.
- The user passwords are stored in a hashed format in a registry hive either as a LM hash or as a NTLM hash. This file can be found in %SystemRoot%/
system32/config/SAMand is mounted on HKLM/SAM.

- To improve the security of the SAM database against offline software cracking, Microsoft introduced the SYSKEY function in Windows NT 4.0.
- When SYSKEY is enabled, the on-disk copy of the SAM file is partially encrypted, so that the password hash values for all local accounts stored in the SAM are encrypted with a key (usually also referred to as the "SYSKEY").
- It can be enabled by running the syskey program. Since a hash function is one-way (data is mapped to a fixed length value and is irreversible), this provides some measure of security for the storage of the passwords. However in two way encryption each me
- In the case of online attacks, it is not possible to simply copy the SAM file to another location. The SAM file cannot be moved or copied while Windows is running, since the Windows kernel obtains and keeps an exclusive filesystem lock on the SAM file, and will not release that lock until the operating system has shut down or a "Blue Screen of Death" exception has been thrown.

Password cracking methods

Password crackers can use many ways to identify a password. The most important methods are:

- a) Brute force method
- b) Dictionary searches
- c) Syllable attack
- d) Rule based attack
- e) Hybrid attack
- f) Password guessing
- g) Rainbow attack

Brute force attack

- Brute force attacks work by calculating every possible combination that could make up a password and testing it to see if it is the correct password.
- As the password's length increases, the amount of time, on average, to find the correct password increases exponentially.
- This means short passwords can usually be discovered quite quickly, but longer passwords may take decades.

Dictionary attack

- In cryptanalysis and computer security, a dictionary attack is a technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by trying hundreds or sometimes millions of likely possibilities, such as words in a dictionary.
- A dictionary attack is based on trying all the strings in a pre-arranged listing, typically derived from a list of words such as in a dictionary (hence the phrase dictionary attack).
- In contrast to a brute force attack, where a large proportion of the key space is searched systematically, a dictionary attack tries only those possibilities which are deemed most likely to succeed.
- Dictionary attacks succeed when people choose short passwords that are ordinary words or common passwords, or simple variants obtained,
- Dictionary attacks are relatively easy to defeat.

Syllable attack

- It is a combination of the Brute Force and Dictionary attacks methods.
- Many times the passwords does not contain a dictionary word and in these cases syllables form dictionary words use token and combined to every possible ways to do brute force searches.

Rule Based Attack

- The attackers has many/ some preoccupied information using which the set of rules can be formed and then the possible searches can be narrowed down to a great extent.
- This type of attack is the most powerful one.

Hybrid attack and password guessing

- It is also based on dictionary attack. In this if the old password is known than concatenating it with other symbols can yield the right password.
- In case of guessing the common passwords that are mostly used by novice users are used to crack codes.

Rainbow Attacks

- Any computer system that requires password authentication must contain a database of passwords, either hashed or in plaintext, and various methods of password storage exist.
- Because the tables are vulnerable to theft, storing the plaintext password is dangerous.
- Most databases therefore store a cryptographic hash of a user's password in the database. In such a system, no one—including the authentication system—can determine what a user's password is simply by looking at the value stored in the database.
- Instead, when a user enters his or her password for authentication, it is hashed and that output is compared to the stored entry for that user (which was hashed before being stored). If the two hashes match, access is granted.

- Someone who gains access to the (hashed) password table cannot merely enter the user's (hashed) database entry to gain access (using the hash as a password would of course fail since the authentication system would hash that a second time, producing a result which does not match the stored value, which was hashed only once).
- In order to learn a user's password, a password which produces the same hashed value must be found.
- Rainbow tables are one tool that has been developed in an effort to derive a password by looking only at a hashed value. Rainbow tables are not always needed, for there are simpler methods of hash reversal available.
- Brute-force attacks and dictionary attacks are the simplest methods available; however these are not adequate for systems that use large passwords, because of the difficulty of storing all the options available and searching through such a large database to perform a reverse-lookup of a hash.

- To address this issue of scale, reverse lookup tables were generated that stored only a smaller selection of hashes that when reversed could generate long chains of passwords.
- Although the reverse lookup of a hash in a chained table takes more computational time, the lookup table itself can be much smaller, so hashes of longer passwords can be stored.
- Rainbow tables are a refinement of this chaining technique and provide a solution to a problem called chain collisions.
- A rainbow table is a pre-computed table for reversing cryptographic hash functions, usually for cracking password hashes.
- Tables are usually used in recovering a plaintext password up to a certain length consisting of a limited set of characters.
- It is a practical example of a space/time trade-off, using less computer processing time and more storage than a brute-force attack which calculates a hash on every attempt, but more processing time and less storage than a simple lookup table with one entry per hash.

Tools for passwords cracking

CMOSPwd

- CmosPwd decrypts password stored in cmos used to access BIOS SETUP.
- Works with the following BIOSes - ACER/IBM BIOS - AMI BIOS - AMI WinBIOS 2.5 - Award 113
- 4.5x/4.6x/6.0 - Compaq (1992) - Compaq (New version) - IBM (PS/2, Activa, Thinkpad) - Packard Bell - Phoenix 1.00.09.AC0 (1994), a486 1.03, 1.04, 1.10 A03, 4.05 rev 1.02.943, 4.06 rev 1.13.1107 - Phoenix 4 release 6 (User) - Gateway Solo - Phoenix 4.0 release 6 - Toshiba - Zenith AMI

ERDCommander

- Microsoft DaRT is a successor of ERD Commander, which was part of the *Winternals Administrator Pack* from Winternals. ERD Commander later became a Microsoft property with its acquisition of Winternals on 17 July 2006.
- Microsoft DaRT is based on Windows Preinstallation Environment now referred to as the Windows Recovery Environment.
- The tool set includes:
 - Registry editor: Edits Windows Registry
 - Locksmith: Resets a user account's password
 - Crash Analyzer: Analyzes crash dumps
 - File Restore: Restores deleted files

- · Disk Commander: Repairs volumes, master boot records and partitions
- · Disk Wipe: Irrecoverably erases data from hard disk
- · Computer Management: A group of utilities that help retrieve system information, enable, disable or manage device drivers, Windows services and software that run during computer startup, inspect the event logs of the offline system and manage partitions.
- · Explorer: A file manager
- · Solution Wizard: A guidance tool that helps user choose the proper repair tool
- · TCP/IP Config: Displays and modifies TCP/IP configuration
- · Hotfix Uninstall: Uninstalls Windows hotfixes
- · SFC Scan: Revives corrupted or deleted system files by copying them from the Windows installation source
- · Search: Searches a disk for files
- · Defender: An antivirus that scans a system for malware, rootkits, and potentially unwanted software. Uses the same engine as Microsoft Security Essentials and other Microsoft antivirus products.

Office Password Recovery

- Office Password Recovery Toolbox is software which recovers lost password to any Microsoft Office document effectively. It can also recover read only files password.
- It allows several features to users letting them to set parameters to the searching password range like shape and length of the password.
- It enables users to search for string documents more efficiently and quickly.
- It recovers read only passwords from Microsoft Office Access.
- It is such type of application that can recover lost or forgotten password for Microsoft PowerPoint presentations, Microsoft Excel spreadsheets, Microsoft Access databases, Microsoft Outlook e-mail accounts.
- It can recover passwords instantly and helps in modifying sheet protection passwords, workbook passwords, email account password, database passwords etc.
- It has user friendly interface which helps in extracting searches. The Office Password Recovery Tool provides an efficient access to MS Office documents.

Passware kit

- Passware Kit Enterprise and Forensics Passware Kit can recover the password of up to 150 different file types.
- It is trade, not exactly cheap tools, but can be very useful in different circumstances.
- This complete electronic evidence discovery solution reports all password-protected items on a computer and gains access to these items using the fastest decryption and password recovery algorithms.
- Many types of passwords are recovered or reset instantly, and advanced acceleration methods are used to recover difficult passwords.

- Passware Kit Forensic introduces a new attacks editor, which sets up the password recovery process in the most precise way to provide the quickest decryption solution possible.
- The highest performance is achieved with Distributed Password Recovery, using the computing power of multiple computers.
- Passware Kit Forensic includes a Portable version that runs from a USB drive and finds encrypted files, recovers files and websites passwords without modifying files or settings on the host computer.
- Perform a complete encrypted evidence discovery process without installing Passware Kit on a target PC.
- Passware Kit Forensic, complete with Passware FireWire Memory Imager, is the first commercial software that decrypts BitLocker and TrueCrypt hard disks of the seized computers without applying a time-consuming brute-force attack.

PDF Password Crackers

- CrackPDF, Abcom PDF Password Cracker, and Advanced PDF Password Recovery can all be used to access password-protected Adobe PDF files.
- CrackPDF and Abcom PDF Password Cracker use brute force attacks to discover the passwords.
- Advanced PDF Password Recovery simply removes the password protection entirely.

IT Act - 2000 And Punishable Offences

Section	Offence	Description	Penalty
65	Tampering computer documents with source	If a person knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force.	Imprisonment up to three years, or/and with fine up to ₹200,000
66	Hacking with computer system	If a person with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack.	Imprisonment up to three years, or/and with fine up to ₹500,000

66B	Receiving stolen computer or communication device	A person receives or retains a computer resource or communication device which is known to be stolen or the person has reason to believe is stolen.	Imprisonment up to three years, or/and with fine up to ₹100,000
66C	Using password of another person	A person fraudulently uses the password, digital signature or other unique identification of another person.	Imprisonment up to three years, or/and with fine up to ₹100,000
66D	Cheating using computer resource	If a person cheats someone using a computer resource or communication.	Imprisonment up to three years, or/and with fine up to ₹100,000
66E	Publishing private images of others	If a person captures, transmits or publishes images of a person's private parts without his/her consent or knowledge.	Imprisonment up to three years, or/and with fine up to ₹200,000
66F	Acts of cyber terrorism	If a person denies access to authorized personnel to a computer resource, accesses a protected system or introduces contaminant into a system, with the intention of threatening the unity, integrity, sovereignty or security of India, then he commits cyber terrorism.	Imprisonment up to life.

67	Publishing information which is obscene in electronic form.	If a person publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.	Imprisonment up to five years, or/and with fine up to ₹1,000,000
67A	Publishing images containing sexual acts	If a person publishes or transmits images containing a sexual explicit act or conduct.	Imprisonment up to seven years, or/and with fine up to ₹1,000,000
67B	Publishing child porn or predating children online	If a person captures, publishes or transmits images of a child in a sexually explicit act or conduct. If a person induces a child into a sexual act. A child is defined as anyone under 18.	Imprisonment up to five years, or/and with fine up to ₹1,000,000 on first conviction. Imprisonment up to seven years, or/and with fine up to ₹1,000,000 on second conviction.
67C	Failure to maintain records	Persons deemed as intermediary (such as an ISP) must maintain required records for stipulated time. Failure is an offence.	Imprisonment up to three years, or/and with fine.

68	Failure/refusal to comply with orders	<p>The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under. Any person who fails to comply with any such order shall be guilty of an offence.</p>	<p>Imprisonment up to three years, or/and with fine up to ₹200,000</p>
----	---------------------------------------	---	--

69

Failure/refusal
to
decrypt data

If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource. The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed, must extend all facilities and technical assistance to decrypt the information. The subscriber or any person who fails to assist the agency referred is deemed to have committed a crime.

Imprisonment up to seven years and possible fine.

70	Securing access or attempting to secure access to a protected system	<p>The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system.</p> <p>The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems. If a person who secures access or attempts to secure access to a protected system, then he is committing an offence.</p>	Imprisonment up to ten years, or/and with fine.
71	Misrepresentation	If anyone makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate.	Imprisonment up to three years, or/and with fine up to ₹100,000

Browser Investigation

- Browser investigation is tricking a user into visiting a malicious link and downloading a malicious executable, This is one of most used techniques by offenders to infect users' machines.
- Analyzing the browsing activities of the victim can identify the first infection vector and how it worked.
- In case of analyzing a criminal machine, browsing through the history would help the user and clarify their intentions by identifying the types of websites that they usually visit and the contents of their downloaded files.
- Analyzing browser activities requires that the investigator understand the different artifacts of the browser with their locations and the data structure of each one.
- It is tricky to conduct in-depth browser forensics. There are many browsers that are currently on the market, and a single user can be using more than one browser

Memory Forensics

- System memory is the working space of the operating system.
- The operating system uses memory to place the data that is needed to execute programs and the programs themselves.
- This is why acquiring the system memory is one of the steps that must be performed when applicable in digital forensics.
- Analyzing the memory may reveal the existence of a malicious process or program that has no traces in the machine hard disk.
- Memory also contains the opened network connections, which could include the connection of an attacker controlling the machine or stealing user data and information

Memory Structure

- Each process that runs in memory allocates space in memory to store its code and data.
- This space consists of memory pages. Each memory page is 4 KB in size in x86 systems.
- All the processes address their memory spaces with virtual addresses, which are translated into physical addresses by the system itself with no interaction by any process.
- In today's operating systems, there are two categories of the running processes: processes run in user mode and others run in kernel mode.
- The difference between both modes is the level of access that is granted to the operating system.
- In the user mode, the processes can't modify paging or access other processes' memory locations except some inter-process communications using Windows APIs.

Memory Acquisition

- In todays Windows operating system, the different security controls forbid processes to access the whole memory, and the step which is required by any acquisition tool to acquire the system memory.
- This may cause a system crash and the loss of system memory, or the whole hard disk in the case of active hard disk encryption.
- So digital forensics acquisition tools tend to install a driver first to the operating system and then use this driver to access the system memory, which will need higher privileges on the system.

The sources of memory dump

- We can consider a memory dump during the incident response process as the main source for memory forensics. However, what if we have a powered off machine or, for any reason, we couldn't acquire the memory of the machine? The question here is do we have any other way to conduct memory forensics?

Hibernation file

- Hibernation is a power option in most operating systems, including Windows OS. In this mode, the system copies the memory. When the user turns the machine on again from hibernation, the system copies the contents of this file again to memory and resumes the execution of the previous processes.

- If the investigator has a forensic image of the victim's or suspect's hard disk, they can extract the hibernation file and conduct memory forensics on this file using the memory analysis tools.
- The hibernation file will provide the investigator or the analyst with a memory image from specific time in the past that may contain traces to the malicious activities or important evidence related to the case under investigation.
- The filesystem's last modification time of the hibernation file will indicate the time when the hibernation was used in the system.
- The structure of the hibernation file is different but known, which makes it possible to convert it to a raw memory image in order to conduct analysis on it using the memory forensics tools.
- Although it contains most of the memory data, the hibernation file won't contain some data, such as the dynamically obtained network information using DHCP.

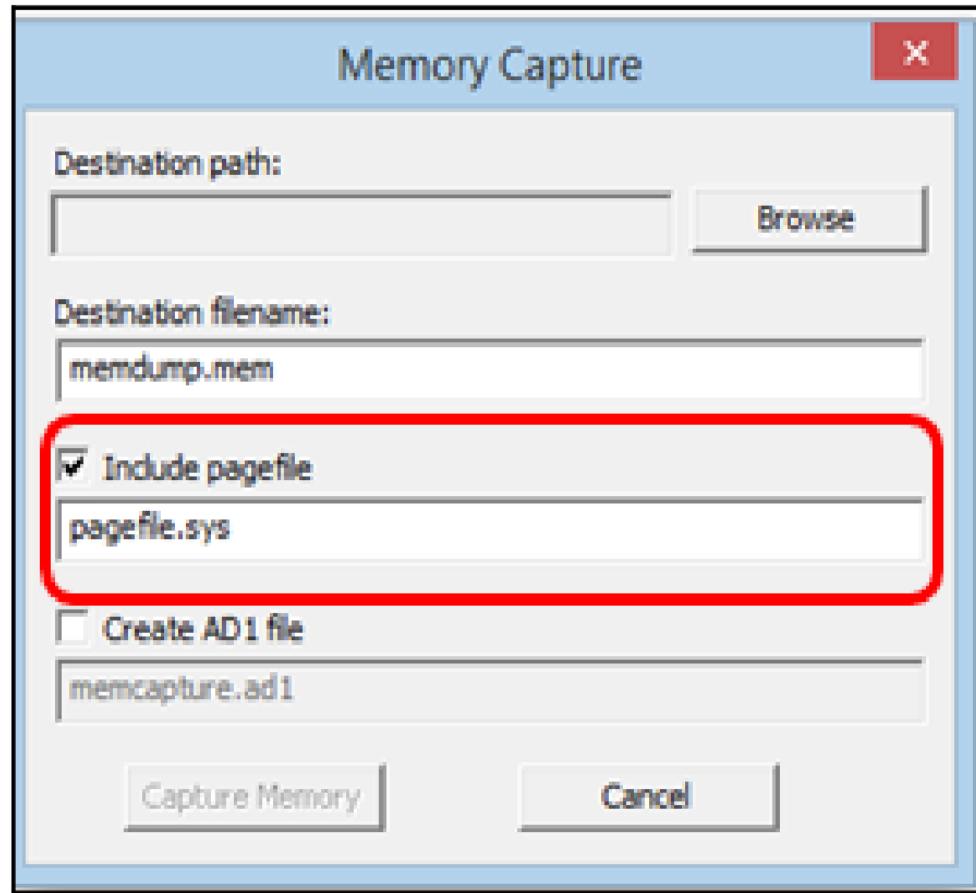
Crash dump

- If the Windows system crashed, it is designed to store information about the system state at the time of the crash for future troubleshooting of the crash after recovering the system. Crashing the system was an old way to dump the memory to the crash dump file.
- Better methods and tools are available nowadays. The crash dump file is named MEMPRY.DMP by default and is located under system root directly.
- The crash dump file can hold different data depending on the settings of the crash dumps, as follows:
 1. Complete memory dump: This contains the physical memory at the time of the crash with a 1 MB header. This type is not common because it has a large size especially for systems with a large memory.
 2. Kernel memory dump: This is when the system dumps the memory pages in the kernel mode only and ignores the pages in the user mode.
 3. Small dump files: These are small files that have a size of 64 KB in 32bit systems and 128 KB in 64bit systems. This contains information about running processes and loaded drivers in the system.

- For the investigator to know which type of dump file is present in the case, they can determine this from the size of the file.
- They can also open the registry location of HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl, under a value called CrashDumpEnable, which will be one of the following four values:
 - 0: This is when debugging information is not written to a file
 - 1: This is when the complete crash dump is written to a file
 - 2: This is when the kernel memory dump is written to a file
 - 3: This is when a small memory dump is written to a file

Page files

- Paging is a memory management technique that works as a secondary storage for Windows memory.
- It speeds up the system by moving the least-used pages in memory to the hard drive in a file named pagefile.
- By applying such techniques, the user will have more memory space to use. When the user starts using the saved pages again, the system restores these pages to memory again.
- This can be noticed in small lagging while accessing some opened applications that haven't been used for some time. The page files on the hard drive can be up to 16 files, and not only under the root directory.
- To find out the locations of the page files from the registry, check HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Memory Management\ExistingPageFiles and PagingFiles.
- Some memory acquisition tools, such as FTK imager can add the page file to memory image during live acquisition:



Page files store unordered data, which make it more difficult for in-depth analysis.

This means that string search in the page files may give some clues about the contents of the page files and the case under investigation, such as the IP, path, or the registry key. File carving also can be conducted in the page files in order to recover some related files.

Scanning the page files for a malware signature may uncover malware running in memory.

Processes in memory

- A process is an instance of a program that has been executed in the system.
- Each process in memory has a private isolated memory space.
- A process contains the execution code and the data that is required to complete the execution of the code, such as files, DLLs, and user input.
- All this data and code are located in a memory space allocated for this process.
- Many processes can be in the memory at the same time.
- All the processes are listed in one structure called `_EPROCESS` in the memory of the running Windows operating system.

Network Connections In Memory

- Usually, networks are used by attackers to control the machine remotely, to send captured user information, or to receive new commands.
- Checking the network connections, which were opened in the system at the time of acquisition, would provide clues about the attack.
- Network activities in general leave traces in memory. Investigating network connections could lead to discovery of a hidden connection created by rootkits.
- These connections can be hidden from normal listing tools in the same way that can be done with the processes.
- Carving for the network connection structure in memory can reveal such connections.
- Another technique to hide a connection is to inject code into a legitimate process to open a malicious connection, so we need to check all the connections in the memory file.

- **The DLL injection** **DLL or Dynamic Link Libraries** are resources and functions that are shared among different processes running within the system.
- Some processes and programs require special external DLLs, which can be included with the program to run properly.
- As DLLs usually run within the processes in memory, they are usually targeted by the malware as a way to access and control other processes in memory. DLLs are loaded into the process with different ways:
 - Dynamic linking: This is when an executable has an Import Address Table (IAT), which describes the resources needed for this executable to load along with their addresses, which are loaded in the process memory space.
 - Runtime Dynamic Linking: Some DLLs may not be mentioned in the IAT, but are called out by the program itself during execution, by calling out one of the Windows functions such as LoadLibrary.
 - Injection: DLLs can be injected into a process by different techniques. Let's see what they are.

- **Remote DLL injection** A malicious process allocates memory space in a legitimate process with read/write protection and writes the path to the malicious DLL in the legitimate process memory space. Then, the malicious process opens a remote thread to force open the DLL in the legitimate process and then removes the DLL path. In this way, the malicious process controls the legitimate one by the code in the DLL. It won't be easy to detect this type of injection. We need to list all the DLLs loaded by the legitimate process and check the names, paths, and time of loading of all the DLLs.
- **Remote code injection** We follow the same steps of the Remote DLL injections, but instead of writing the path to the DLL in the hard drive, the malicious process injects the code directly to the allocated memory space. Here, the protection of the allocated memory space will be read/write and execute. This protection scheme, which isn't popular, is found a lot in memory that is used to detect this kind of injection.

- Reflective DLL injection

The hybrid technique combines the previous two methods. The malicious process loads the DLL directly into the legitimate process's allocated memory space. In this way, DLL won't ever be written to the hard drive and won't go through the normal loading process, so it won't be found while listing the process's loaded DLLs.

API hooking

- Hooking is forcing the kernel to hide all activities that are related to the malware and to intercept the user input in order to steal sensitive information from the user.
- This can be deceptive in live analysis during the incident-handling process.
- In depth analysis of the memory image acquired during the evidence acquisition of the infected system would making it much easier to detect such behavior.
- Hooking is done simply by redirecting the normal flow of one process execution to execute malicious code in another location in the memory, and then return back to complete the normal process code

- **Memory analysis:** After a successful memory acquisition process, the investigator will have a single dump file that contains the full memory.
- The structure of the memory can be parsed by many analysis programs, including **volatility**, which is the most famous memory analysis framework.
- **The volatility framework:** A free memory forensics framework supports many versions of Windows, Mac, and Linux operating systems.
- An independent book called Art of Memory Forensics was released with volatility. It explains in detail different operating systems' artifacts in memory and how to extract and analyze them using the volatility framework.

- Each operating system has a different memory structure.
- Volatility has the ability to understand different structures.
- Using this profile, volatility can understand the correct data structures of the image under investigation and apply the right analysis and parsing tools.
- Volatility works with plugins, each plugin performs specific tasks with the memory dump file.

- **Volatility plugins:**
- A complete list of volatility plugins can be found in the tool's documentation.
- Some plugins which are used to discover the discussed malware techniques:
- **Imagecopy:** In case the available memory file is a hibernation file or a crash dump file, volatility can convert this file to the raw format using the imagecopy plugin.

- **Imageprofile:**
- Before starting the analysis you can run the **imageinfo** plugin against the image file and volatility will suggest the right profile to you.
- Imageinfo uses another plugin called **kdbgscan**, which scans a part of the kernel module for specific unique strings which identifies the image profile.

- **pslist** This plugin lists the processes from the memory image file. It walks through the doublelinked list in the `_EPROCESS` structure and prints all the processes in the list.
- It displays the process name, ID, offset, parent process ID, number of threads and handles, and timestamp of the start and end of the process.

- **Psscan:** This plugin lists the processes in the memory dump file by carving the dump for any process structure, and it **doesn't consider the EPROCESS** structure. It can get all the processes in the memory, including active, terminated, and hidden processes.
- **The pstree plugin** lists the processes in a tree view, identifying the parent and child processes. It lists the process using the **same method that** is used by the **pslist plugin**, so it won't detect hidden or unlinked processes.

- **getsids** Each process has the privilege of the user who started it. The security identifier of the user, the SID, describes the user's privilege in the system.
- The process has a copy of the access token that is created for the user when they logged on to the system.
- Use the getsids plugin and the process ID to provide the SID of the user who started the process

- **Dlls:** This plugin lists all the DLLs that are called and added to the process using the normal way in the operating system. It shows all the DLLs for all the processes in memory. If the investigator used the option with specific PID, then in this case, this will list only the DLLs of that specific process.
- **Memory Forensics** While addressing hidden or unlinked processes, we need to use the physical address of its structure in memory. So, if we need to list the DLLs of an unlinked or hidden process, we need to provide the plugin with the physical offset of the process in the psscan plugin output.

- **Handles:**
- A process can have many handles to many objects in the operating system.
- Analysis of these handles can be difficult because of the huge number of handles for each process.
- **This could play an important role in proving a theory about the incident.**
- It could provide the investigator with proof that one process has requested a handle to access a specific file in the filesystem or to create a specific mutant used as a signature for specific malware.
- Using the handles plugin, we can display all the plugins of one process by the process ID and choose which type of handles will be displayed in the results

- **Filescan:** For any process to create or read a file, it needs to open this file first in memory. The volatility plugin, filescan, parses for the file object tag in memory and lists all the opened files or the files hidden from ordinary file-scanning tools by the rootkit.
- This plugin will display the physical offset of the detected file object and the filename with the permissions on the file.
- Like the handles plugin, filescan will be useful in confirming the existence of specific malware by scanning for its specific files that are opened in memory.

- **Memdump:** When the process starts executing, it uses some space in memory to store its code and data that is required during execution.
- This area could contain important information about the malware, such as strings, code, file paths, contents of files, and so on.
- Volatility can dump this whole area into a single file for further analysis.
- We can run this file against the Linux native command-Strings in order to extract all the strings in the file

- **svscan**
- Windows services are usually run in the background with higher privileges than other programs, which are run by system users.
- Some malware samples run as services to work in the background and to ensure the malware's existence in the system after reboot.
- A plugin called svscan, which, besides listing the services by normal means, also parses the memory space that is owned by the services process, searching for unique tags for services.
- This method will reveal any hidden process in memory.
- The output displays the process ID of each service, the service name, service display name, service type, and current status.
- It also shows the binary path for the registered service, and a driver name for services that run from kernel mode.

- **Connections:** network traces are very important while analyzing memory samples.
- Volatility has plugins to scan opened TCP connections in memory with different methods.
- The first plugin is **connections**, which displays the TCP connections as Windows tools would do.
- This lists all the connections in a linked list structure.

- **connscan** Just like the psscan plugin, connscan searches for connection object structure instead of listing all the connections in the linked list only. It will also list the terminated connections.
- **sockets** Another plugin is sockets, which lists all the opened sockets on the system with any protocol. This lists the connection in the way that any Windows API would use for this purpose by walking though the sockets-linked list. This won't be able to find closed sockets or residuals from old sockets.

- **sockscan** Like the connscan plugin, sockscan searches for the socket structure in memory, which makes it possible to recover residual sockets that were previously opened
- **Netscan**, the netscan plugin checks network traces. This plugin finds TCP endpoints, TCP listeners, UDP endpoints, and UDP listeners.
- It prints the local and remote IP, the local and remote port, and the time when the socket was bound or when the connection was established

- **malfind** The malfind volatility plugin finds hidden injected code or DLLs that are based on the permissions granted for specific pages in memory. It detects DLLs or code injected in a suspicious way,
- **vaddump** The VAD (Virtual Address Descriptor) is used in Windows memory to describe memory locations that are allocated by a process running in memory. Every time the process allocates new memory, a new VAD entry is created in what is called a VAD tree.
- Each VAD entry has a start and end, and it covers a specific area in the process memory space. plugin, vaddump, which can dump each VAD area separately if we are interested in only one VAD entry.
- This is helpful if code or DLL injection has occurred, where we can extract the VAD that contains the malicious code.

- **apihooks** The apihooks plugin detects hooks. It detects CALLs and JMPs to other locations in memory. The function being imported or exported begins with the following instructions.
- **mftparser** The mftparser volatility plugin scans memory file for master file table MFT entries

NETWORK FORENSICS

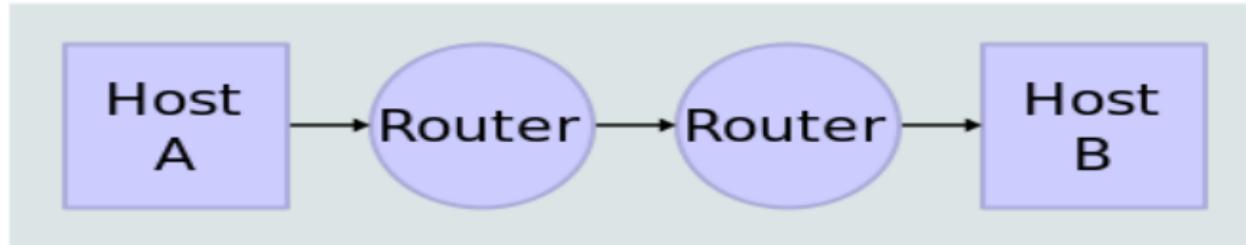
- There are many systems that track and record network activities and data. The network forensics adds vital information to investigations.
- Tools can be used to do time line analysis, email reconstruction, Metadata analysis, packet frame analysis or checksum on data exchanged.
- Another aspect of network forensics is to make/ get capabilities of capturing and investigating a suspect's computer over network.
- There are methods of making an image/clone of a suspect/ victims computer over network connection from the forensics lab itself.
- However, legal aspects must be considered before capturing/ intruding over other system.

- Network forensics is a sub-branch of digital forensics relating to the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection.
- Unlike other areas of digital forensics, network investigations deal with volatile and dynamic information.
- Network traffic is transmitted and then lost, so network forensics is a **pro-active investigation**.

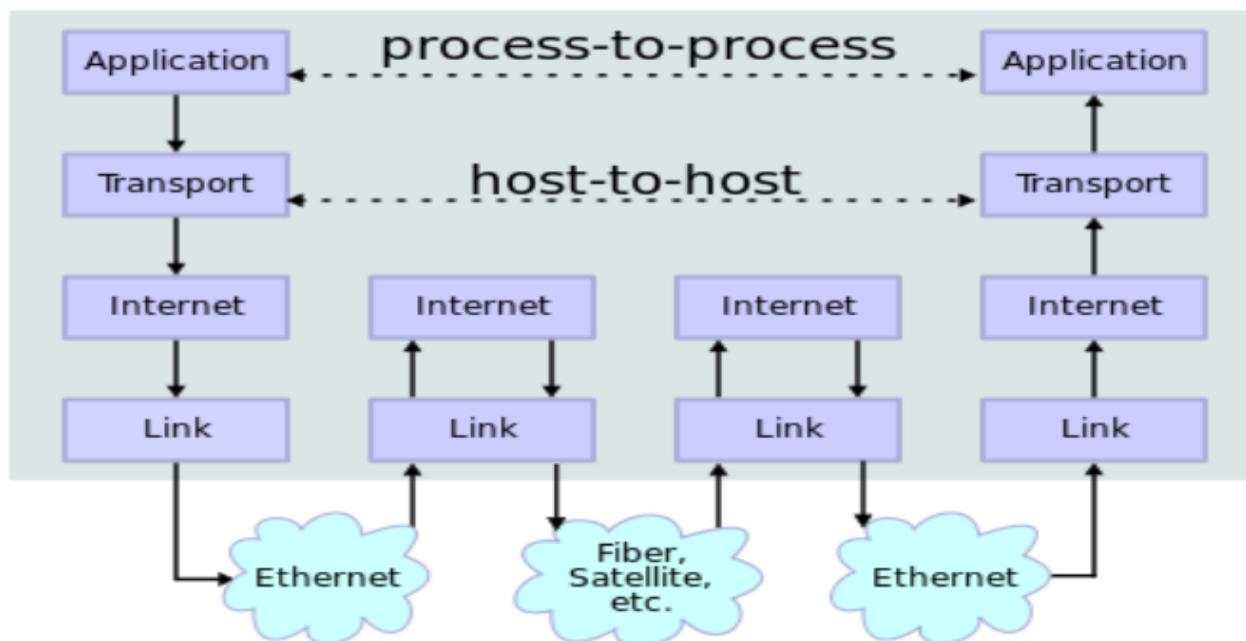
- Network forensics generally has two uses:
 1. The first, relating to **security**, involves monitoring a network for anomalous traffic and identifying intrusions. An attacker might be able to erase all log files on a compromised host; network based evidence might therefore be the only evidence available for forensic analysis.
 1. The second form relates to **law enforcement**. In this case analysis of captured network traffic can include tasks such as reassembling transferred files, searching for keywords and parsing human communication such as emails or chat sessions.

Network Components And Their Forensics Importance

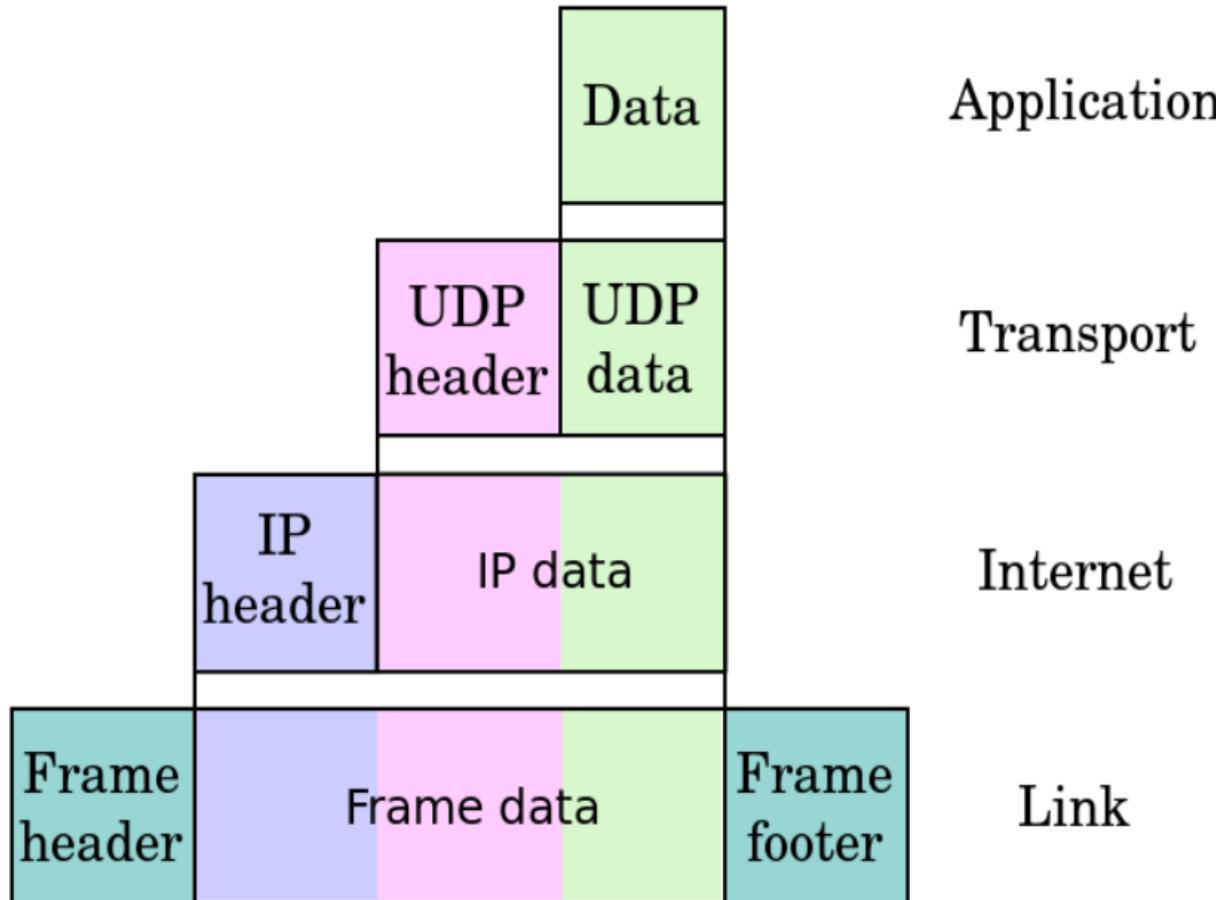
Network Topology



Data Flow



Encapsulation of application data descending through the layers



- Applying forensic methods on the **Ethernet layer** is done by eavesdropping bit streams with tools called monitoring tools or sniffers.
- The most common tool on this layer is **Wireshark** (formerly known as **Ethereal**) and **tcpdump** where **tcpdump** works mostly on unix-like operating systems.
- These tools collect all data on this layer and allow the user to filter for different events.
- With these tools, websites, email attachments, and other network traffic can be reconstructed only if they are transmitted or received unencrypted.
- An advantage of collecting this data is that it is directly connected to a host.
- If the IP address or the MAC address of a host at a certain time is known, all data sent to or from this IP or MAC address can be filtered.

Eavesdropping Attack

- Eavesdropping attack also called as sniffing or snooping attack is a major concern in cyber security.
- Through these attacks, the information like passwords, card details, and other sensitive data is easily stolen while it is getting transferred from one device to another.
- These kinds of attacks are most successful because they don't raise any kind of alert while the transmission is taking place because they take advantage of unsecured network communications to access data while it is being sent or received by its user.

- As Tom King, applications and security manager at 3i writes- “*Eavesdropping attacks are insidious because it's difficult to know they are occurring. Once connected to a network, users may unwittingly feed sensitive information — passwords, account numbers, surfing habits, or the content of email messages — to an attacker.*”
- **Example of an eavesdropping attack:** Consider that you are a remote employee and you are transmitting some sensitive business information to your boss over the open network. At this point, a cyber attacker can silently intrude and place some software through which he can eavesdrop in the network pathway and capture all the important information. These attacks can result in financial loss, identity theft or privacy loss, etc.

Eavesdropping Methods

- Pickup devices pick up sounds or images, from the attached microphones and video cameras, and then the attackers can convert them into an electrical format to eavesdrop on targets.
- Attackers may also use mini amplifiers that help them in minimizing the background noise.
- A transmission link between a sender and the receiver would be tapped to eavesdrop.
- This can be done with the radiofrequency transmission or a wire, which can include active or unused telephone lines, electrical wires, or ungrounded electrical conduits.
- Some transmitters can operate continuously, but another approach can be remote activation.

- A **listening post** is when we put bugs on telephones to hear the conversations taking place.
- It uses triggers that records when a telephone is picked up to make or take a call and it is automatically turned off when the call ends.
- Secure areas where these recordings are monitored are known as listening posts.
- It can be anywhere, and they have voice-activated equipment available to eavesdrop and record every activity.
- It is easier for attackers to gain unauthorized access to user accounts when weak passwords are used.
- It gives them a way to intrude into corporate systems and networks.
- Cyber attackers use these to their advantage and access confidential communication channels, intercepting activity, to listen in on conversations between colleagues to steal confidential business data.

- Users who connect to open networks that do not require any password and do not use encryption for the transmission of data provide an ideal situation for attackers for eavesdropping.
- Attackers can easily monitor user activity and listen to the communications that take place on the network.

- To establish the connection between IP and MAC address
- The Address Resolution Protocol (ARP) tables list the MAC addresses with the corresponding IP addresses.
- To collect data on this layer, the network interface card (NIC) of a host can be put into "promiscuous mode".
- In so doing, all traffic will be passed to the CPU, not only the traffic meant for the host.
- However, if an intruder or attacker is aware that his connection might be eavesdropped, he might use encryption to secure his connection.
- It is almost impossible to break nowadays encryption but the fact that a suspect's connection to another host is all the time encrypted might indicate that the other host is an accomplice of the suspect.

PRS (Packet Resonance Strategy), use similar protocols like IP, so the methods described for IP work with them as well.

- For the correct routing, every intermediate router must have a routing table to know where to send the packet next.
- These routing tables are one of the best sources of information if investigating a digital crime and trying to track down an attacker.
- To do this, it is necessary to follow the packets of the attacker, reverse the sending route and find the computer the packet came from (i.e., the attacker).

- The internet can be a rich source of digital evidence including web browsing, email, newsgroup, synchronous chat and peer-to-peer traffic.
- For example web server logs can be used to show when (or if) suspect accessed information related to criminal activity.
- Email accounts contain useful evidence; but email headers are easily faked and, so, network forensics may be used to prove the exact origin of incriminating material.
- Network forensics can also be used in order to find out who is using a particular computer by extracting user account information from the network traffic.

Sources of Forensics Information From Network

A forensic investigator needs to collect data from these sources:

1. **Hosts:** Forensics makes use of agents (Software) to gather and send Host data to remote forensic server. The agents collect real time data stream passing through the network interface card (NIC) and send for analysis study.
2. **Routers:** Router logs can be useful in many cases, Like Information of status details, errors, IP and MAC addresses getting resolved to other networks or hosts can be used to trace a suspect as well as can be helpful in getting to the chain of events while restructuring the crime.
3. **Firewalls:** Firewalls maintain logs of every internet/ network access by the host user. These logs are like dropped packets, unallowed application, filtered websites, recognised attacks, etc. Many times the logs of the host firewall or the network firewall is enough to trace the links to a crime or suspicious activity.
4. **Switch:** Switches have a CAM (context addressable memory) which keeps information about mappings of MAC address to ports. CAM is also used to keep information about VLAN

- Two popular methods that are specifically designed to allow a network analyst to monitor traffic :
 - 1. Port mirroring - the switch sends a copy of network packets to a monitoring network connection.
 - 2. SMON - "Switch Monitoring" is described by RFC 2613 and is a protocol for controlling facilities such as port mirroring.

Port Mirroring

- Port mirroring is a technique that copies **network traffic** from one port on a switch or router to another for analysis.
- The copied traffic is then sent to a network analyzer, intrusion detection system, or another monitoring device.
- The original traffic is not affected by copying the traffic to a different port.
- Moreover, the copy can be analyzed without impacting network performance.
- **Configuration of port mirroring**
- Port mirroring can be configured differently depending on the switch or router being used.
- Process involves **selecting a source port** to mirror traffic from and send copied traffic to a destination port.
- Some switches and routers may also allow you to **set up filters to limit** the amount of traffic being mirrored.
- Port mirroring can be configured through a **command-line interface** or a **web-based management console**.

Types Of Port Mirroring

- **Local port mirroring:** It involves copying traffic from one switch port to another on **the same switch**.
- **Remote port mirroring:** It involves copying traffic from one switch to a port on a **different switch**.
- **Encapsulated Remote Port Mirroring (ERPM):** A form of remote port mirroring that can encapsulate mirrored traffic and send it across a Layer 3 network.
- **Two-switch port mirroring:** This is a configuration that uses two switches to mirror traffic, **providing redundancy** and improved scalability.
- **VLAN-based port mirroring:** It allows the mirroring of specific VLAN traffic to a specific port.
- **RSPAN (Remote Switched Port Analyzer):** A Cisco proprietary protocol that allows for remote port mirroring across **Layer 2 and Layer 3 networks**.
- **GRE (Generic Routing Encapsulation) Tunneling:** It is a Cisco proprietary protocol. Encapsulating packets within other packets is called tunneling. GRE tunnels are configured between two routers with each router acting like one end of the tunnel.

- **Port mirroring can be useful in a variety of scenarios:**
- **Network troubleshooting:** Port mirroring can be used to monitor network traffic and identify issues. For example, if a particular user is experiencing slow network speeds, port mirroring can help identify which devices or applications are causing the slowdown.
- **Security monitoring:** Port mirroring can be used to detect security breaches or suspicious activity by monitoring traffic patterns. It can also help identify potential insider threats.
- **Compliance and auditing:** Port mirroring can help organizations comply with various regulatory requirements by monitoring and logging network traffic. This is particularly important for industries such as finance and healthcare that have strict data privacy regulations.

- **Performance monitoring:** Port mirroring can be used to monitor network performance and ensure that applications are running smoothly. It can help identify bandwidth-intensive applications that may be affecting network performance and identify opportunities for optimization.
- **Traffic analysis:** Port mirroring can provide detailed insight into network traffic patterns, which can be used to optimize network infrastructure and plan for future capacity requirements.
- **Application monitoring:** Port mirroring can be used to monitor specific applications and identify issues related to their performance or usage. For example, it can help identify which users are accessing a particular application and how frequently they are using it.
- **Intrusion detection and prevention:** Port mirroring can be used to detect and prevent unauthorized access to the network by monitoring traffic patterns and detecting potential security threats

Risks of port mirroring: While port mirroring can be a useful tool, there are some risks to be aware of.

- Port mirroring can violate privacy concerns or compliance regulations if sensitive data is copied without proper authorization.
- If port mirroring is not configured properly, it can impact network performance or potentially cause a denial-of-service attack.

Best Practices For Port Mirroring

- It's important to follow best practices to minimize risks and ensure proper functionality.
- Appropriately configuring the destination port, setting appropriate filters to limit the amount of traffic being mirrored, and regularly monitoring the port mirroring configuration.
- It is vital to use port mirroring as a part of a comprehensive network monitoring and security strategy that incorporates other tools and techniques.

Port mirroring tools

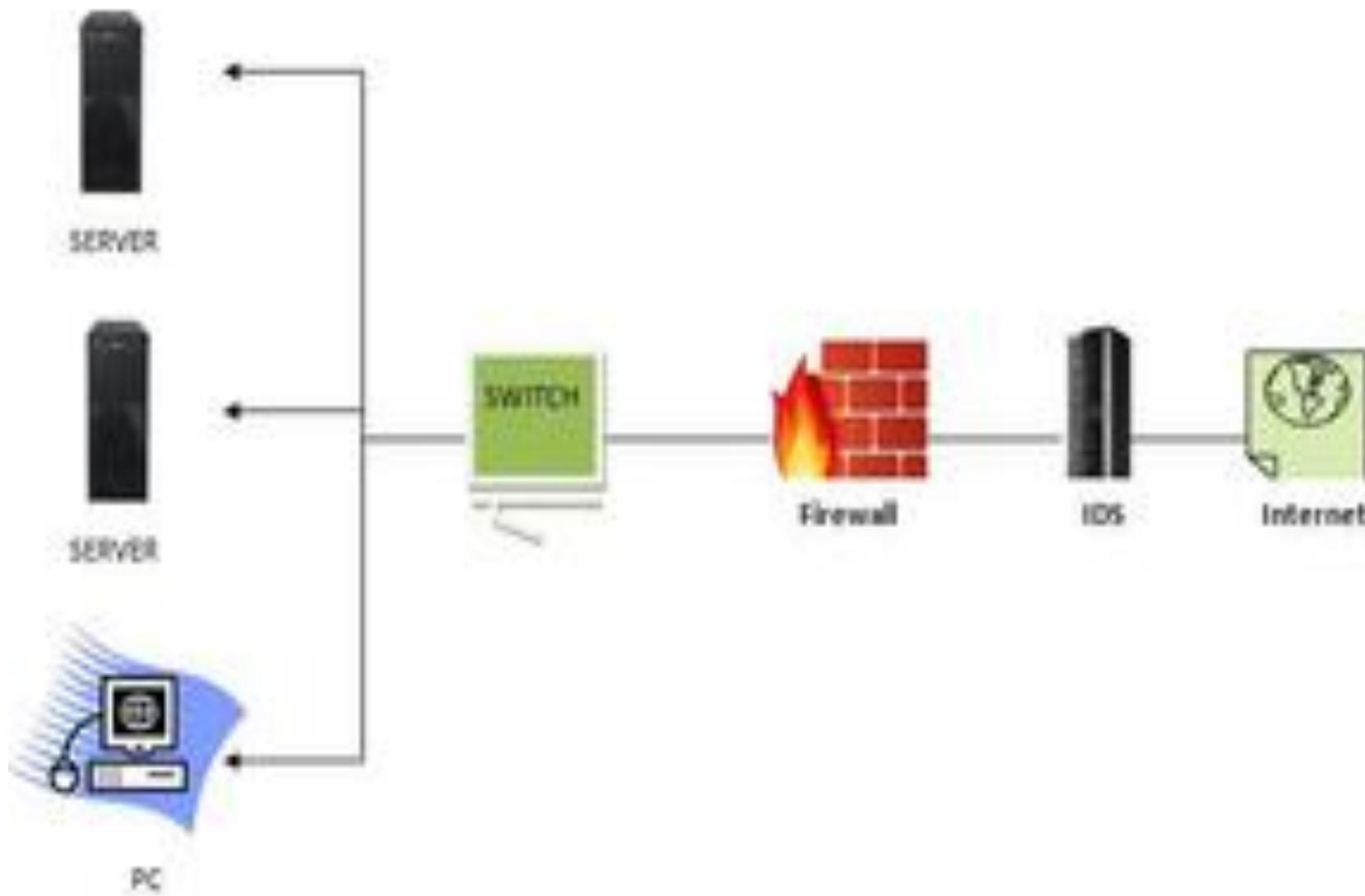
- Port mirroring tools can help network administrators configure, monitor, and analyze network traffic.
- These tools range from basic command-line interfaces to advanced graphical user interfaces that provide real-time traffic analysis and alerts.
- Port Mirroring Tools include Wireshark, Tcpdump, SolarWinds Network Performance Monitor, and PRTG Network Monitor.

- Forensic information from network via:
 - IDS
 - WAP

Intrusion Detection System (IDS)

- Intrusion detection system (IDS) observes network traffic for malicious transactions and **sends immediate alerts** when it is observed.
- It is **software** that checks a network or system for malicious activities or policy violations.
- Each illegal activity or violation is recorded either centrally using a SIEM (Security Information And Event Management) system or notified to an administration.
- IDS monitors a network or system for malicious activity and protects a computer network from unauthorized access from users, including insiders.
- The intrusion detector learning task is to build a predictive model (i.e. a **classifier**) capable of distinguishing between ‘bad connections’ (intrusion/attacks) and ‘good (normal) connections’.

- An IDS (Intrusion Detection System) monitors the traffic on a computer network to detect any suspicious activity.
- It analyzes the data flowing through the network to look for patterns and signs of abnormal behaviour.
- The IDS compares the network activity to a set of predefined rules and patterns to identify any activity that might indicate an attack or intrusion.
- If the IDS detects something that matches one of these rules or patterns, it sends an alert to the system administrator.
- The system administrator can then investigate the alert and take action to prevent any damage or further intrusion.

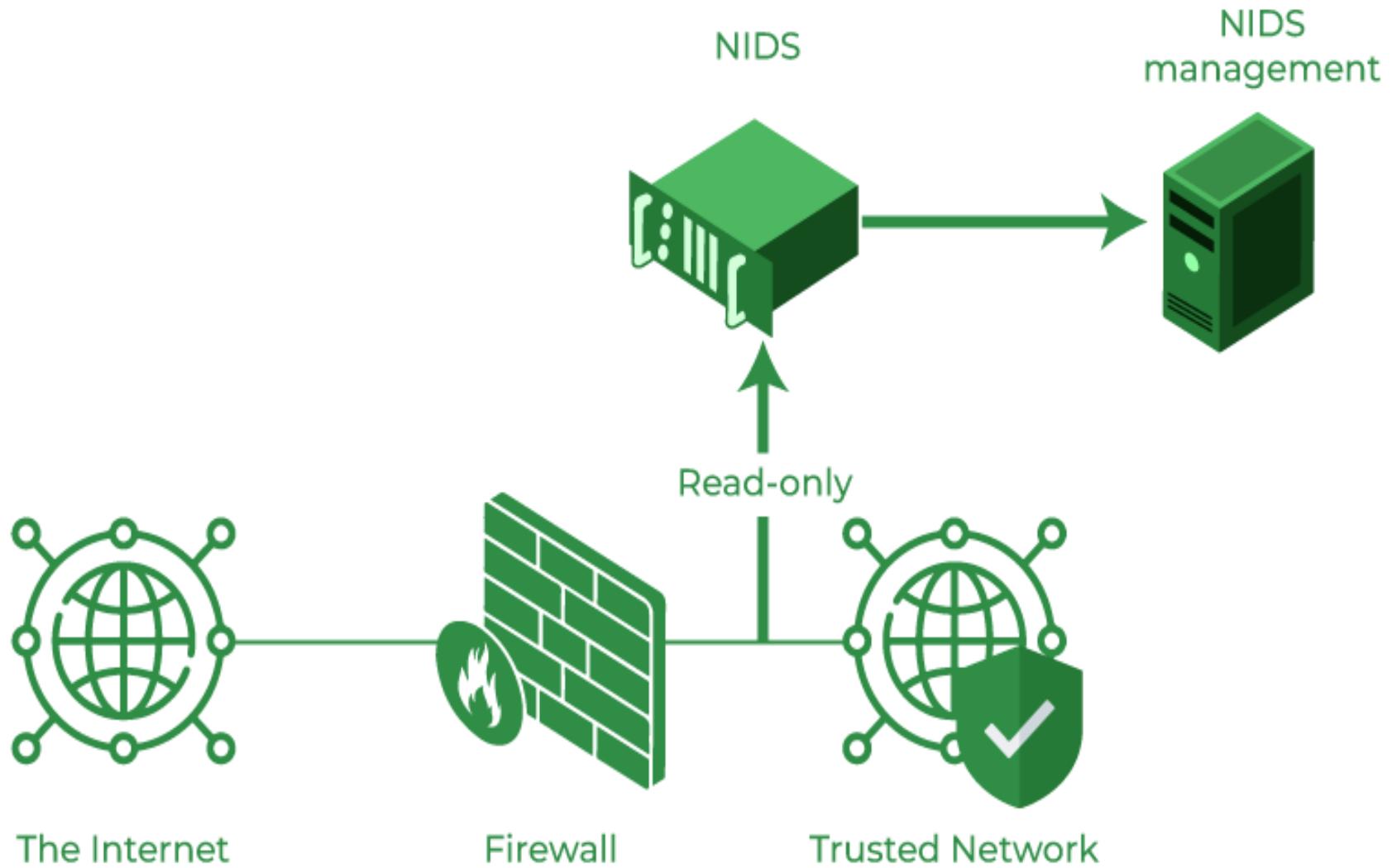


Classification of Intrusion Detection System

- 1. Network Intrusion Detection System (NIDS)**
- 2. Host Intrusion Detection System (HIDS)**
- 3. Protocol-based Intrusion Detection System (PIDS)**
- 4. Application Protocol-based Intrusion Detection System (APIDS)**
- 5. Hybrid Intrusion Detection System**

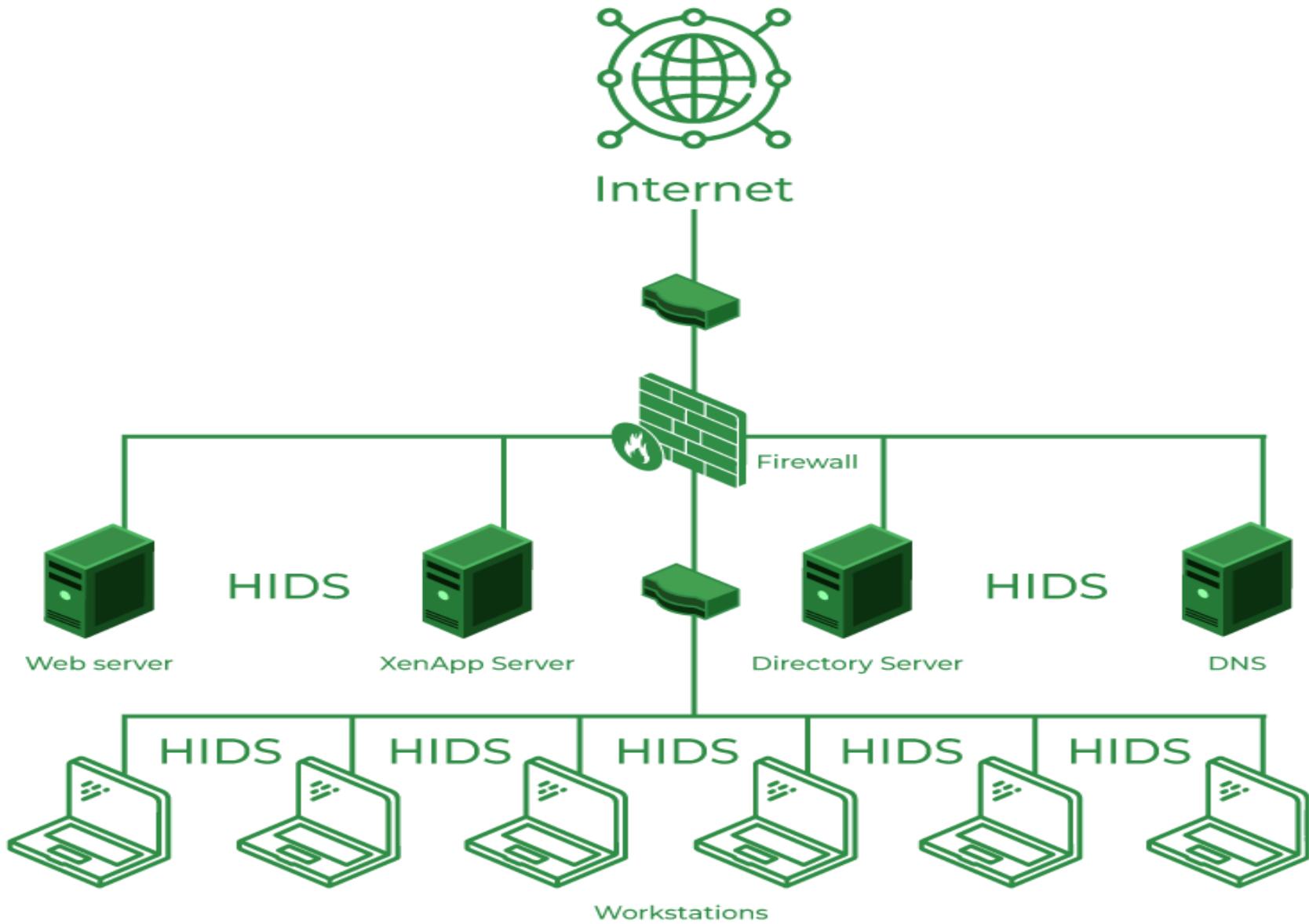
Network Intrusion Detection System (NIDS)

- NIDS are set up at a planned point within the network to examine traffic from all devices on the network.
- It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks.
- Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator.
- Example of a NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying to crack the firewall.



Host Intrusion Detection System (HIDS)

- Host intrusion detection systems (HIDS) run on independent hosts or devices on the network.
- An HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected.
- It takes a snapshot of existing system files and compares it with the previous snapshot.
- If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate.
- An example of HIDS usage can be seen on mission-critical machines, which are not expected to change their layout.



Protocol-based Intrusion Detection System (PIDS)

- PIDS comprises a system or agent that would consistently reside at the front end of a server, controlling and interpreting the protocol between a user/device and the server.
- It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accepting the related HTTP protocol.
- As HTTPS is unencrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPS.

Application Protocol-based Intrusion Detection System (APIIDS)

- APIIDS is a system or agent that generally resides within a group of servers.
- It identifies the intrusions by monitoring and interpreting the communication on application-specific protocols.
- For example, this would monitor the SQL protocol explicitly to the middleware as it transacts with the database in the web server.

Hybrid Intrusion Detection System

- Hybrid intrusion detection system is made by the combination of two or more approaches to the intrusion detection system.
- In the hybrid intrusion detection system, the host agent or system data is combined with network information to develop a complete view of the network system.
- The hybrid intrusion detection system is more effective in comparison to the other intrusion detection system.
- Prelude is an example of Hybrid IDS.

Wireless Access Points

- A Wireless Access Point (WAP) is a networking device that allows connecting the devices with the wired network. WAP is used to create the WLAN (Wireless Local Area Network), used in large offices and buildings which have expanded businesses.
- WAP maintains logs of almost all routing type activities like SSIDs and incoming connections etc.
- Looking at the amount of traffic that follows in and out of a network it is important to understand the storage aspects also. That is, how we will be storing these logs etc. for future analysis as well as evidence building.
- The investigators can use one or more of the available bulk storage technologies like SAN (storage area network), network attached storage (NAS), direct attached storage (DAS) etc. for the purpose.
- Also, tape drives were in use since older days and still play a vital role in mass storages

LOG ANALYSIS

- The analysis of large volumes of data collected during IDPS (intrusion detection and prevention system) is performed in a separate database system run by the analysis team.
- Live systems are not dimensioned to run extensive individual analysis without affecting the regular users.
- It is methodically preferable to analyse data copies on separate systems and protect the analysis teams against the accusation of altering original data.
- Due to the nature of the data, the analysis focuses more often on the content of data than on the database it is contained in.

- If the database itself is of interest then Database forensics are applied.
- In order to analyze large structured data sets with the intention of detecting financial crime it takes at least three types of expertise in the team:
 1. A **data analyst** to perform the technical steps and write the queries,
 2. A **team member** with extensive experience of the processes and internal controls in the relevant area of the investigated company and
 3. A **forensic scientist** who is familiar with patterns of fraudulent behaviour.
- After an initial analysis phase using methods of explorative data analysis the following phase is usually highly iterative.
- Starting with a hypothesis on how the intruder might have created a personal advantage the data is analyzed for supporting evidence.

- Following that the hypothesis is refined or discarded.
 - The combination of different databases, in particular data from different systems or sources is highly effective.
 - These data sources are either unknown to the intruder or he/she cannot manipulate them afterwards.
 - Data Visualization is used to display the results.
-
- There are many tools that can be used to analyse the logs captured during above sources of information.
 - We need to understand how these analysis are done and how actually a criminal event can be re-created.
 - Major activities during log analysis are:
 - a) Analysing time stamps
 - b) Analysing data

Analyzing Time Stamps

- Time and its synchronization in network are very important.
- A smart criminal can use certain methodologies to put false time stamps in their communication.
- However with advent of technologies like **Network Time Protocol (NTP)** this issue is more or less minimized.
- The investigator needs to find out whether the NTP has been incorporated or not before proceeding into the analysis.
- Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable latency data networks.
- In operation since before 1985, NTP is one of the oldest Internet protocols in current use.
- NTP was originally designed by David L. Mills of the University of Delaware, who still oversees its development.
- NTP is intended to synchronize all participating computers to within a few milliseconds of Coordinated Universal Time (UTC).

Analyzing Data

- Data over network in Transmission Control Protocol/ Internet Protocol (TCP/IP) is broken into pieces which are further broken into smaller pieces called as packets to be transported over networks.
- The packets are re-assembled at the other end.
- Different packets of the same message might take different paths before reaching at other end. This adds to the complexity of reassembling the packets.
- To overcome this issue TCP/IP follows a mechanism of numbering each packet based on sequences.
- The receiver node sends acknowledgment based on these sequence numbers.
- The message is reconstructed and the sending host gets acknowledgement of all the packets sent over the network.
- The times stamps in these acknowledgement packets are in GMT (UTC) format and can give vital clues during analysis.
- Address resolution protocol (ARP) is used to map MAC address to an IP and vice-versa.
- This resolution protocols can help an investigator get vital traces into IP addresses and MAC addresses of any individual in a case

FORENSICS TOOLS

- Forensic tools that are used for forensic activities like seizure, capture, analysis etc. in network is categorized in two forms:
 - a. Technology tools
 - b. Software tools
- Technology tools are like methodologies to track, trace or identify hidden artefacts in any network system.
- The software tools are software solutions which can specifically assist forensic collection etc.

Network Tools Used For Forensics

- **Network tap**
- A network tap is a hardware device which provides a way to access the data flowing across a computer network.
- In some cases, it is desirable for a third party to monitor the traffic between two points in the network.
- If the network between points A and B consists of a physical cable, a "network tap" may be the best way to accomplish this monitoring.
- The network tap has (at least) three ports: an A port, a B port, and a monitor port.
- A tap inserted between A and B passes all traffic through unimpeded, but also copies that same data to its monitor port, enabling a third party to listen.

- Network taps are used for network intrusion detection systems, VoIP recording, network probes, RMON probes, packet sniffers, and other monitoring and collection devices and software that require access to a network segment.
- Taps are used in security applications because they are non-obtrusive, are not detectable on the network (having no physical or logical address), can deal with full-duplex and non-shared networks.
- Once a network tap is in place, the network can be monitored without interfering with the network itself.

- Other network monitoring solutions require in-band changes to network devices, which meant that monitoring can impact the devices being monitored.
- Once a tap is in place, a monitoring device can be connected to it as-needed without impacting the monitored network.
- Putting a network tap into place will disrupt the network being monitored for a short time.
- Even so, a short disruption is preferable to taking a network down multiple times to deploy a monitoring tool.
- Establishing good guidelines for the placement of network taps is recommended.

Promiscous Mode

- In networking, promiscuous mode (often shortened to "promisc mode) is a mode for a wired network interface controller (NIC) or wireless network interface controller (WNIC) that causes the controller to pass all traffic it receives to the central processing unit (CPU) rather than passing only the frames that the controller is intended to receive.
- This mode is used for packet sniffing that takes place on a router or on a computer connected to a hub (instead of a switch) or one being part of a WLAN.
- Interfaces are placed into promisc mode by software bridges often used with hardware virtualization.

- Promisc mode is used to diagnose network connectivity issues.
- There are programs that make use of this feature to show the user all the data being transferred over the network.
- Some protocols like FTP and Telnet transfer data and passwords in clear text, without encryption, and network scanners can see this data.
- Therefore, users are encouraged to stay away from insecure protocols like telnet and use more secure ones such as SSH (Secure Shell).

Software Tools For Network Forensics

- **Wire shark**
- Wireshark is a free and open-source packet analyzer.
- It is used for network troubleshooting, analysis, software and communications protocol development, and education.
- Originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues.

Wireshark – Packet Capturing and Analyzing

- Reconnaissance (recon) is the information-gathering stage of ethical hacking, where you collect data about the target system.
- This data can include anything from network infrastructure to employee contact details.
- The goal of recon is to identify as many potential attack vectors as possible
- Packet sniffing is an essential form of network recon as well as monitoring.
- Wireshark captures the data coming or going through the Network Interface Cards (NICs) on its device by using an packet capture library.
- Wireshark captures on-device data only, but it can capture almost all the data on its LAN if run in promisc mode.
- Wireshark uses NMAP's (Network Mappers) Packet Capture library (called npcap).

- **Getting Up and Running:** After installation launch Wireshark, approve the administrator privileges and window that looks like this (next two slides).
- This window shows the interfaces on your device.
- To start sniffing select one interface and click on the bluefin icon on the top left.
- **The data capture screen has three panes:** The top pane shows real-time traffic, the middle one shows information about the chosen packet and the bottom pane shows the raw packet data.
- The top pane shows source address, destination address, source and destination ports, protocol to which the packet belongs to and additional information about the packet.
- Since there are a lot of packets going in and out every second, looking at all of them or searching for one type of packets will be tedious. This is why packet filters are provided.
- Packets can be filtered based on many parameters like IP address, port number or protocol at capture level or at display level.

The Wireshark Network Analyzer

- □ X

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help



Apply a display filter ... <Ctrl-/>

→ +

Welcome to Wireshark

Capture

...using this filter: Enter a capture filter ...

All interfaces shown ▾

Bluetooth Network Connection 2	
Local Area Connection* 3	
Local Area Connection* 13	
Local Area Connection* 12	
Local Area Connection* 15	
Local Area Connection* 14	
VMware Network Adapter VMnet1	
Wi-Fi	
VMware Network Adapter VMnet8	
Adapter for loopback traffic capture	
Ethernet	
Ethernet 6	

Learn

[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#)

You are running Wireshark 3.2.2 (v3.2.2-0-ga3efec3d640). You receive automatic updates.

Activate Windows

Go to Settings to activate Windows.

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help



Apply a display filter ... <Ctrl-/>



No.	Time	Source	Destination	Protocol	Length	Info
622	58.596644	172.217.166.206	192.168.43.236	TCP	54	443 → 37692 [RST] Seq=41 Win=0 Len=0
623	58.597421	172.217.161.10	192.168.43.236	TCP	54	443 → 37699 [RST] Seq=41 Win=0 Len=0
624	58.597880	172.217.166.206	192.168.43.236	TCP	54	443 → 37692 [RST] Seq=41 Win=0 Len=0
625	58.598037	172.217.166.206	192.168.43.236	TCP	54	443 → 37692 [RST] Seq=41 Win=0 Len=0
626	59.731513	192.168.43.236	172.217.166.232	TLSv1.2	93	Application Data
627	59.731863	192.168.43.236	172.217.166.232	TLSv1.2	78	Application Data
628	59.732085	192.168.43.236	172.217.166.232	TCP	54	1160 → 443 [FIN, ACK] Seq=103 Ack=40 Win=67 Len=0
629	60.626397	172.217.166.232	192.168.43.236	TCP	66	[TCP Dup ACK 66#1] 443 → 1160 [ACK] Seq=40 Ack=40 Win=248 Len=0 SLE=103 SRE=104
630	60.626580	172.217.166.232	192.168.43.236	TCP	54	443 → 1160 [FIN, ACK] Seq=40 Ack=104 Win=248 Len=0
631	60.626840	192.168.43.236	172.217.166.232	TCP	54	1160 → 443 [ACK] Seq=104 Ack=41 Win=67 Len=0
632	60.627657	172.217.166.232	192.168.43.236	TCP	54	[TCP Keep Alive] 443 → 1160 [ACK] Seq=40 Ack=104 Win=248 Len=0

```
> Frame 626: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface \Device\NPF_{0FB0F21F-6972-411E-8642-F017607CD388}, id 0
> Ethernet II, Src: IntelCor_da:d1:67 (18:3d:a2:da:d1:67), Dst: HuaweiTe_06:c2:66 (94:0e:6b:06:c2:66)
> Internet Protocol Version 4, Src: 192.168.43.236, Dst: 172.217.166.232
> Transmission Control Protocol, Src Port: 1160, Dst Port: 443, Seq: 40, Ack: 40, Len: 39
> Transport Layer Security
```

0000	94 0e 6b 06 c2 66 18 3d a2 da d1 67 08 00 45 00	..k..f = ..g..E
0010	00 4f 1e d2 40 00 80 06 9b 80 c0 a8 2b ec ac d9	0..@.....+....
0020	a6 e8 04 88 01 bb a7 61 2b f9 b8 d2 b0 af 50 18a +.....P
0030	00 43 59 c6 00 00 17 03 03 00 22 d5 8b 6f 2b aa	CY....."..o+
0040	30 16 8e f5 6a 1b 10 5d 03 4b 97 e9 99 86 9d 59	0...j..] .K.....Y
0050	74 04 53 b9 21 56 f8 6d df 17 fa 00 18	t.S..!V.m

Activate Windows

Go to Settings to activate Windows.

- Some of the general capture filters are:
- host (capture the traffic through a single target)
- net(capture the traffic through a network or sub-network). “net” can be prefixed with “src” or “dst” to indicate whether the data coming from or going to the target host(s).)
- port (capture the traffic through or from a port). “port” can be prefixed with “src” or “dst” to indicate whether the data coming from or going to the target port.
- “and”, “not” and “or” logical connectives. (Used to combine multiple filters together).

- Packet capture is a networking practice involving the interception of data packets travelling over a network.
- Once packets are captured they can be stored by IT teams for further analysis.
- **pcap** saves lot of time for security analysis by extracting files instead of full analysis on a machine.
- Process of pcap starts with packet sniffers (can be hardware device called taps or software tools)

- Wireshark is software that "understands" the structure (encapsulation) of different networking protocols.
 -
 - It can display the fields, along with their meanings as specified by different networking protocols.
-
- Wireshark uses pcap to capture packets, so it can only capture packets on the types of networks that pcap supports.
 1. Data can be captured "from the wire" from a live network connection or read from a file of already-captured packets.
 2. Live data can be read from a number of types of networks.
 3. Captured network data can be browsed via a version of the utility, TShark.
 4. Captured files can be programmatically edited or converted via the "editcap" program.
 5. Data display can be refined using a display filter.
 6. Plug-ins can be created for dissecting new protocols.

- **Plugins** are extra pieces of codes that can be embedded into the native Wireshark. Plugins help in analysis by:
 1. Showing parameter specific statistics and insights.
 2. Handling capture files and issues related to their formats.
 3. Collaborating with other tools and frameworks to set up an all-in-one network monitoring solution.

- With just the basic capability to see all the traffic going through your device or in your LAN and the tools and plugins to help you in analysis, you can do a great deal of things with your device. Like:
 1. Troubleshooting Internet connectivity problems with your device or WiFi.
 2. Monitoring your device for unwanted traffic that may be an indication of a malware infection.
 3. Testing the working of your application that involve networking.
 4. Using it to just understand how computer networks work.

TCPDUMP

- tcpdump is a packet sniffing and packet analyzing tool for a System Administrator to troubleshoot connectivity issues in Linux.
- It is used to capture, filter, and analyze network traffic such as TCP/IP packets going through your system.
- It is many times used as a security tool as well.
- It saves the captured information in a pcap (packet capture) file, these pcap files can then be opened through Wireshark.

- Many Operating Systems have tcpdump command pre-installed but to install it, use the following commands:
 - **For RedHat based linux OS**
yum install tcpdump
 - **For Ubuntu OS**
apt install tcpdump

- It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached.
- Distributed under the BSD (Berkeley Source Distribution) license, tcpdump is free software.
- Tcpdump works on most Unix-like operating systems.
- Tcpdump prints the contents of network packets.
- It can read packets from a network interface card or from a previously created saved packet file.
- It is also possible to use tcpdump for the specific purpose of intercepting and displaying the communications of another user or computer.

Cyber Warfare and cyber terrorism

- **Cyber warfare** utilizes techniques of defending and attacking information and computer networks that inhabit cyberspace, often through a prolonged Cyber campaign or series of related campaigns.
- It denies an opponent's ability to do the same, while employing technological instruments of war to attack an opponent's critical computer systems.
- **Cyber terrorism**, on the other hand, is –the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population.
- That means the end result of both cyber warfare and cyber terrorism is the same, to damage critical infrastructures and computer systems linked together within the confines of cyberspace.

INVESTIGATING WEB ATTACKS

- **Cyber-attack** is any type of offensive activity employed by individuals or whole organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by hacking into a susceptible system.
- These can be labelled as either a Cyber campaign, cyber warfare or cyber terrorism in different context.
- Cyber-attacks can range from installing spyware on a PC to attempts to destroy the infrastructure of entire nations.
- Cyber-attacks have become increasingly sophisticated and dangerous.

- **Web servers** are where websites are stored. A web server's primary responsibility is to show website content by storing, processing, and distributing web pages to users.
- **Web Server Attack:**
- Any attempt by a malicious actor to undermine the security of a Web-based application is referred to as a Web Application Attack or Web Server Attack.
- Web application attacks can either target the application itself in order to get access to sensitive data, or they can use the application as a staging area for attacks against the program's users.

- **TYPES OF MAJOR WEB ATTACKS**

1. Denial-of-Service (DoS) / Distributed Denial-of-service (DDoS)
2. Web Defacement Attack
3. Cross-site scripting (XSS)
4. SQL injection attacks
5. Directory Traversal
6. DNS Server Hijacking
7. SSH Brute Force Attack
8. Spoofing
9. Website spoofing
10. Repudiation
11. Non-Repudiation
12. Privacy attacks
13. Privilege escalation
14. MITM Attack
15. HTTP Response Splitting Attack

DENIAL-OF-SERVICE (DOS) / DISTRIBUTED DENIAL-OF-SERVICE (DDOS)

- Denial of Service is when an internet hacker causes the web to provide a response to a large number of requests. This causes the server to slow down or crash and users authorized to use the server will be denied service or access.
- A denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.
- A distributed denial-of-service(DDoS) is where the attack source is more than one-and often thousands-of unique IP addresses.
- Criminal perpetrators of DoS attacks target sites or services hosted on high profile web servers such as banks, Government services, credit card companies under large corporations, credit card payment gateways; also motives of revenge, blackmail or activism can be behind other attacks.

- A denial-of-service attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service.
- **There are two general forms of DoS attacks: those that crash services and those that flood services.**
- A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers.
- Such an attack is the result of multiple compromised systems (for example a botnet) flooding the targeted system with traffic.
- A botnet is a network of zombie computers programmed to receive commands without the owners' knowledge.
- When a server is overloaded with connections, new connections can no longer be accepted.

WEB DEFACEMENT ATTACK

- In a Web Defacement Attack, the hacker gains access to the site and defaces it for a variety of reasons, including humiliation and discrediting the victim.
- The attackers hack into a web server and replace a website hosted with one of their own.
- An example of defacement is when a hacker replaces the original content of a website with their own messages, images, or videos, often containing political or social messages.

CROSS SITE SCRIPTING (XSS)

- This type of attack is more likely to target websites with scripting flaws (Typographical errors, Global variables with unexpected values, Uninitialized variables, Global and local variables with the same name, Incorrect values for loop variables, Checking the precedence of operators, Incorrect uses of break statements, Infinite loops.)
- The injection of malicious code into web applications is known as Cross-Site Scripting.
- The script will give the hacker access to web app data such as sessions, cookies, and so on.

Types of XSS attacks

- **Reflected XSS**, where the malicious script comes from the current HTTP request. This type of attack is also referred to as “type-I XSS.”
- **Stored XSS**, where the malicious script comes from the website's database. This type of attack is also referred to as “type-II XSS.”
- **DOM (document object model)-based XSS**, where the vulnerability exists in client-side code rather than server-side code.
- This attack happens when a threat actor modifies the document object model (DOM) environment in the victim's browser. So, while the HTML itself doesn't change, the code on the client side executes differently. This type of attack is also referred to as “type-0 XSS.”

SQL Injection Attacks

- SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).
- SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered or user input is not strongly typed and unexpectedly executed.
- SQL injection is known as an attack vector for websites but can be used to attack any type of SQL database.

XSS Vs SQL

Category	XSS	SQL Injection
Definition	It is a technique of injecting client-side scripts using JavaScript on users' browsers to compromise the website.	It is a code injection technique that uses SQL statements for queries database in an abnormal manner to get information stored in the database.
Vulnerability Percentage	According to OWASP reports, around 65% of websites are vulnerable to XSS attacks.	According to Invicti Security reports, around 32% of government websites are vulnerable to SQL Injection.
Practice Websites	Google XSS Game, alert(1) to win, prompt(1) to win, etc. are some websites to practice XSS attacks.	hacksplaining.com , portswigger.net , acunetix, etc. are common SQL injection practicing websites.
Vulnerable Object	All input fields and URLs are vulnerable objects.	URLs interacting with the database, cookies storing data, Input fields, etc.
Language Used	It uses JavaScript to write scripts for attacking.	It uses Structured Query Language for compromising database.
First Attack	First XSS attack happened in 1999 where attackers maliciously injected the image tags.	First SQL Injection attack was documented in 1998.
Rating	It is the third most dangerous vulnerability.	It is the second most powerful vulnerability.

DIRECTORY TRAVERSAL

- Directory Traversal Attack is effective on older servers with vulnerabilities and misconfiguration.
- It is a type of HTTP exploit in which a hacker uses the software on a web server to access data in a directory other than the server's root directory.
- If the attempt is successful, the threat actor can view restricted files or execute commands on the server.
- This type of attack is commonly performed using web browsers.
- Any server that fails to validate input data from web browsers is vulnerable to a directory traversal attack.
- Directory traversal is also known as directory climbing, backtracking and file path traversal vulnerabilities.
- It is similar to Structured Query Language injection and cross-site scripting in that they all involve code injection.

- **How does directory traversal work?**
- Hackers use guesswork to find paths to restricted files on a web server. However, a skilled hacker can search the directory tree and easily execute this type of attack on an inadequately protected server.
- **Only a few resources are needed to perform a directory traversal attack, including the following ones:**
 1. access to a web browser;
 2. some knowledge about where to find directories; and
 3. basic knowledge of Hypertext Transfer Protocol (HTTP) requests.
- **IT security professionals minimize the risk of a directory traversal with the following techniques:**
 1. careful web server programming;
 2. installation of software updates and patches;
 3. filtering of input from browsers; and
 4. using vulnerability scanners.

- **What can an attacker do with directory traversal?**
- Once attackers access the root directory, they can enter other parts of the computer system.
- They may also be able to read and write arbitrary files on the server, enabling them to manipulate applications and associated data, read sensitive information like password files or take control of the server.
- Attackers can also gain control of access control lists (ACLs), which administrators use to grant various levels of file access to users.
- With access to ACLs, attackers can impersonate privileged users in the system to inflict damage.

DNS SERVER HIJACKING

- **DNS hijacking, DNS poisoning, or DNS redirection** is the practice of subverting the resolution of Domain Name System (DNS) queries.
- This can be achieved by malware that overrides a computer's TCP/IP configuration to point at a rogue DNS server under the control of an attacker, or through modifying the behaviour of a trusted DNS server so that it does not comply with internet standards.
- It refers to any attack that tricks the end-user into thinking he or she is communicating with a legitimate domain name when in reality they are communicating with a domain name or IP address that the attacker has set up.

SSH (Secure Socket Shell) Brute Force Attack

- By brute-forcing SSH login credentials, an SSH Brute Force Attack is performed to attain access.
- This exploit can be used to send malicious files without being noticed.
- Unlike a lot of other tactics used by hackers, brute force attacks aren't reliant on existing vulnerabilities
- **5 Best Practices to Prevent SSH Brute-Force Login Attacks in Linux**
 1. Disable **SSH Password Authentication** and Enable **SSH-Key Authentication**
 2. Implement **Fail2ban Intrusion Prevention Tool**
 3. Implement **TCP Wrappers** to Limit SSH Access From Clients
 4. **Limit** Maximum Number of SSH Authentication Attempts
 5. Implement SSH **Two Factor** Authentication

Source: <https://www.tecmint.com/prevent-ssh-brute-force-login-attacks/>

SPOOFING

Email spoofing

- Email spoofing is the creation of email messages with a forged sender address. Spam and phishing emails use such spoofing to mislead the recipient about the origin of the message.
- When an email is sent, the initial connection provides two pieces of address information:
 1. a. MAIL FROM: - generally presented to the recipient as the Return-path: header but not normally visible to the end user, and by default no checks are done that the sending system is authorized to send on behalf of that address.
 2. b. RCPT TO: - specifies which email address the email is delivered to, is not normally visible to the end user but may be present in the headers as part of the "Received:" header.
- Together these are referred as the "envelope" addressing, by analogy with a traditional paper envelope.

Website spoofing

- Website spoofing is the act of creating a website, as a hoax, with the intention of misleading readers that the website has been created by a different person or organization.
- The spoof website will adopt the design of the target website and sometimes has a similar URL.
- A more sophisticated attack results in an attacker creating a "shadow copy" of the World Wide Web by having all of the victim's traffic go through the attacker's machine, causing the attacker to obtain the victim's sensitive information.
- Another technique is to use a 'cloaked' URL. By using domain forwarding, or inserting control characters, the URL can appear to be genuine while concealing the address of the actual website.

Repudiation

- Repudiation makes data or information to appear to be invalid or misleading (Which can even be worse).
- For example, someone might access your email server and inflammatory information to others under the guise of one of your top managers.
- This information might prove embarrassing to your company and possibly do irreparable harm.
- This type of attack is easy to accomplish because most email systems don't check outbound email for validity.
- Repudiation attacks like modification attacks usually begin as access attacks.

Non-Repudiation

- Non-repudiation refers to a state of affairs where the author of a statement will not be able to successfully challenge the authorship of the statement or validity of an associated contract.
- The term is often seen in a legal setting wherein the authenticity of a signature is being challenged. In such an instance, the authenticity is being "repudiated".
- In a general sense non-repudiation involves associating actions or changes to a unique individual.
- For computer accounts, the individual owner of the account must not allow others to use that account, especially, for instance, by giving away their account's password, and a policy should be implemented to enforce this.
- This prevents the owner of the account from denying actions performed by the account.

Privacy attack

- Internet privacy involves the right or mandate of personal privacy concerning the storing, repurposing, provision to third parties, and displaying of information pertaining to oneself via the Internet.
- Internet privacy is a subset of data privacy. Privacy can entail either Personally Identifying Information (PII) or non-PII information such as a site visitor's behaviour on a website.
- PII refers to any information that can be used to identify an individual. For example, age and physical address alone could identify who an individual is without explicitly disclosing their name, as these two factors are unique enough to typically identify a specific person.
- Privacy concerns exist wherever personally identifiable information or other sensitive information is collected and stored – in digital form or otherwise.
- Improper or non-existent disclosure control can be the root cause for privacy issues.

- Data privacy issues can arise in response to information from a wide range of sources, such as:
 1. Healthcare records
 2. Criminal justice investigations and proceedings
 3. Financial institutions and transactions
 4. Biological traits, such as genetic material
 5. Residence and geographic records
 6. Ethnicity
 7. Privacy breach
 8. Location-based service and geo-location
- The challenge in data privacy is to share data while protecting personally identifiable information.

Privilege Escalation

- Privilege escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user.
- The result is that an application with more privileges than intended by the application developer or system administrator can perform unauthorized actions.
- Most computer systems are designed for use with multiple users. Privileges mean what a user is permitted to do. Common privileges include viewing and editing files, or modifying system files.
- Privilege escalation means a user receives privileges they are not entitled to. These privileges can be used to delete files, view private information, or install unwanted programs such as viruses.
- It usually occurs when a system has a bug that allows security to be bypassed or, alternatively, has flawed design assumptions about how it will be used.

- **Privilege escalation occurs in two forms:**
- **Vertical privilege** escalation, also known as privilege elevation, where a lower privilege user or application accesses functions or content reserved for higher privilege users or applications (e.g. Internet Banking users can access site administrative functions or the password for a smartphone can be bypassed).
- **Horizontal privilege** escalation, where a normal user accesses functions or content reserved for other normal users (e.g. Internet Banking User A accesses the Internet bank account of User B)

Man-In-The-middle (MITM) Attack

- A **Man-In-The-middle (MITM) Attack** Or On-path Attack is a cyber attack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other, as the attacker has inserted themselves between the two parties.
- One example of a MITM attack is active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.
- In this scenario, the attacker must be able to intercept all relevant messages passing between the two victims and inject new ones.
- This is straightforward in many circumstances; for example, an attacker within the reception range of an unencrypted Wi-Fi access point could insert themselves as a man-in-the-middle.

HTTP Response Splitting Attack

- HTTP response splitting occurs when Data enters a web application through an untrusted source, most frequently an HTTP request.
- The data is included in an HTTP response header sent to a web user without being validated for malicious characters.

WEB ATTACK FORENSICS

- There are mechanisms to protect our applications etc. from web attacks but it's quite difficult to find the attacker and book him/her under law.
- The difficulty in traceability of the hackers/offenders prompts them to do more crimes.
- The major objective of web forensics is to trace the attacker and in line collect enough evidence that can be presented and accepted in the court of law.
- The aspects of investigation into web attacks can be viewed in two areas: **web application forensics** and **web services forensics**

Web Services Forensics

- "Web services" describes a standardized way of integrating Web-based applications using the XML, SOAP, WSDL and UDDI open standards over an Internet protocol backbone.
- XML is used to tag the data, SOAP is used to transfer the data, WSDL is used for describing the services available and UDDI lists what services are available.
- A Web service is a method of communication between two electronic devices over a network.
- It is a software function provided at a network address over the Web with the service always on as in the concept of utility computing.

- As in a document by NIST [csrc.nist.gov/publications/nistir/.../nistir-7559_forensics-webservices.pdf] we need to provide two features into web services forensics:
 1. **Pairwise evidence generation:** Collect transactional evidence that occur between pairs of services at service invocation times.
 2. **Comprehensive evidence generation:** On demand, compose pairs of transactional evidence collected at service invocation times and reveal global views of complex transactional scenarios that occurred during specified periods, and provide them for forensic examiners.

Web Parameter Tampering

- The Web Parameter Tampering attack is based on **the manipulation of parameters** exchanged between client and server in order to modify application data, such as user credentials and permissions, price and quantity of products, etc.
- This attack can be performed by a malicious user who wants to exploit the application for their own benefit, or an attacker who wishes to attack a third-person using a Man-in-the-middle attack. In both cases, tools like **Webscarab** and **Paros proxy** are mostly used.
- The attack success depends on integrity and logic validation mechanism errors, and its exploitation can result in other consequences including XSS, SQL Injection, file inclusion, and path disclosure attacks.

The Major tasks an investigator needs to do while performing web application forensics are:

PRELIMINARY ANALYSIS:

- to focus on evidence **collection and protection** which are in form of logs.
- the investigator needs to **build in confidence** by using robust supporting forensic tools.
- Above all it all depends upon the abilities of the investigator to procure and correlate all data for inferences and conclusion

STANDARD METHODOLOGY: methodologies that are standard are easily addressable and heard in the court of law.

Preliminary Analysis

- **Application Forensics Readiness**
- In this the web application should be well prepared for a forensics investigation.
- Major activities in it are evidence collection and evidence protection, use of supportive forensics and investigator abilities and more.

1. Evidence collection

- A proper Evidence collection is to be done in order to prepare a web application for a forensics investigation.
- Mostly all the logging options of the web application are enabled so as to collect maximum digital evidences.
- The application logs have to be set according to the case requirement and not be left in default mode which are very basic and might not log important aspects.

2. Evidence protection

- Log files are the main source of digital evidence, hence, proper mechanisms must be incorporated in order to protect these logs files and ensure that these are digitally procured and signed to be presented in court as evidence.
- This will certainly guarantee the accuracy of the digital evidences provided.
- Log files can be protected using actions like setting permissions of log files, ensuring out of reach of these log files from the hackers and following checksums to ensure integrity.

3. Supportive forensics

- Mere collection of logs will not help, we must see that these logs are supported by forensics tools evidence gathering.
- That is, forensic tools can help gather those information which might not be recorded in any application logs.
- Network or an operating system forensics tools or a third party extra logging facilities can be utilized to achieve this.

4. Forensics investigator abilities

- The forensics investigator must have a sound knowledge and understanding of web application and its architecture etc.
- Better understanding of security aspects and issues pertaining these applications will be required to have a forethought approach in cracking the case.

Methodology

- Certain prescribed standard methodologies exist in investigation of web application and these needs to be followed. The cruxes of these standard methodologies are:
 1. Protect the web application (could be several servers) during the forensic examination so that their logs etc. can't be modified.
 2. Extract all evidence files needed for the forensics investigation:
 - Web servers and application servers logs.
 - Server side scripts which are used by the web application.
 - Web servers and application servers configuration files.
 - All third party software log files.
 - Operating system log files.

3. After collecting the files **perform analysis of those files** to determine the sequence of events and the aspects where security was compromised.

- To carrying out analysis **divide the log files according to user sessions**, by doing this we will be able to remove distortions and can confine to the culprit's sessions.
- **Fingerprints of a web application security attack** needs to be explored. The following are examples of fingerprints and patterns left by web application hacking attempts:
 1. Unusual entries in the Logs
 2. Script abuse (multi java pages)
 3. Excessive attempts from the same IP address.
 4. Unusually long processing times (SQL Injection attempt)
 5. Files created or modified around the time of the suspected attack.
etc.

4. Prepare a report based on the data extracted from the web application logs and other aspects.

Website Traffic Analysis

- Website traffic analysis is produced by grouping and aggregating various data items captured by the web server in the form of log files while the website visitor is browsing the website.
- **Commonly used website traffic analysis terms are:**
- **URL** - A Uniform Resource Locator (URL) uniquely identifies the resource requested by the user's browser.
- **Hit** - Each HTTP request submitted by the browser is counted as one hit. HTTP requests may be submitted for non-existent content, in which case they still will be counted. For example, if one of the five image files referred by the example page mentioned above is missing, the web server will still count six HTTP requests, but in this case, five will be marked as successful (one HTML file and four images) and one as a failed request (the missing image)

- **Page** - A page is a successful HTTP request for a resource that constitutes primary website's content. Pages are usually identified by a file extension (e.g. .html, .php, .asp, etc.).
- **File** - Each successful HTTP request is counted as a file.
- **Visitor** - A visitor is the actual person browsing the website. A website serves content to anonymous visitors and cannot associate visitors with the actual person browsing the website. Visitor identification may be based on their IP address or an HTTP cookie. The former approach is simple to implement, but results in all visitors browsing the same website from behind a firewall counted as a single visitor. The latter approach requires special configuration of the web server (i.e. to log HTTP cookies) and is more expensive to implement. Neither of the approaches identifies the actual person browsing the website and neither provides 100% accuracy in determining that the same visitor has visited the website again

- **Visit** - A visit is a series of HTTP requests submitted by a visitor with the maximum time between requests not exceeding a certain amount configured by the webmaster.
- **Host** - A host is the visitor's machine running the browser. Hosts are identified by IP addresses or domain names.
- **User Agent** - User agent is a synonym for a web browser.

WEB APPLICATION FORENSICS TOOLS

- Tools that are useful for web application forensics are Microsoft LogParser, EventLogAnalyzer, Http-analyze, Pyflag, Analog, Open Web Analytics, Mywebalizer, CORE Wisdom, Logjam, Sawmill, and Lire
- **Logparser**
- logparser is a flexible command line utility that was initially written by Gabriele Giuseppini, a Microsoft employee, to automate tests for IIS logging.
- It was intended for use with the Windows operating system.
- The default behaviour of logparser works like a "data processing pipeline", by taking an SQL expression on the command line, and outputting the lines containing matches for the SQL expression.
- Microsoft describes Logparser as a powerful, versatile tool that provides universal query access to text-based data such as log files, XML files and CSV files, as well as key data sources on the Windows operating system such as the Event Log, the Registry, the file system, and Active Directory.
- The results of the input query can be custom-formatted in text based output.

EventLog Analyzer

- Event log analysis is used for pattern matching, filtering of event occurrences, and aggregation of event occurrences into composite event occurrences.
- Dynamic programming strategies from algorithms are employed to save results of previous analyses for future use, since, for example, the same pattern may be match with the same event occurrences in several consecutive analysis processing.
- EventLog Analyzer provides the most cost-effective Security Information and Event Management (SIEM) software on the market.
- Using this Log Analyzer software, organizations can automate the entire process of managing terabytes of machine generated logs by collecting, analyzing, correlating, searching, reporting, and archiving from one central location.
- This event log analyzer software helps to monitor file integrity, conduct log forensics analysis, monitor privileged users and comply to different compliance regulatory bodies by **intelligently** analyzing your logs and instantly generating a variety of reports like user activity reports, historical trend reports, and more.

Web Log Analyzer

- Web log analysis software (also called a web log analyzer) is a kind of web analytics software that passes a server log file from a web server, and based on the values contained in the log file, derives indicators about when, how, and by whom a web server is visited.
- Reports are generated from the log files immediately, but the log files can alternatively be passed for a database and reports generated on demand.

INTELLIGENT LOG ANALYTICS

**Make smarter, faster decisions when troubleshooting and measuring
the health of your application environments.**

- Automatically unify logs, traces, and metrics of events in real time. Unified logs are entries from the Traffic, Threat, URL Filtering, WildFire Submissions, and Data Filtering logs displayed in a single view.
- Unified log view enables you to investigate and filter the latest entries from different log types in one place, instead of searching through each log type separately.
- WildFire combines dynamic and static analysis, innovative machine learning techniques, re-cursive analysis, to analyze, identify, and prevent the most sophisticated and evasive threats.

- Navigate from traces to logs to user sessions and vice versa to get full stack visibility
- Resolve issues faster with AI-powered root cause analysis
- Instantly understand business impact and dependencies
- Reduce MTTR (mean time to recovery or mean time to restore) by eliminating manual correlation between multiple tools, alerts, and data silos.
- A data silo is a repository of data that's controlled by one department or business unit and isolated from the rest of an organization. Siloed data is stored in a standalone system and often is incompatible with other data sets. That makes it hard for users in other parts of the organization to access and use the data.

- Data silos can have technical, organizational or cultural roots. They arise naturally in large companies because separate business units may operate independently and have their own goals, priorities and IT budgets. But any organization can end up with data silos if it doesn't have a well-planned data management strategy.
- Improve cluster health and ensure performant applications across complex multi-cloud environments
- Store, analyze, and query cluster-level logs
- Filter by namespace, workload, node etc to simplify analysis

- Optimize storage costs.
 - Collect and parse log data in real-time without indexing
 - Replace alert storms with AI-powered baselining and anomaly detection
 - Filter, monitor, and transform log fields to meet policy and compliance requirements.
-
- **Resolve incidents faster**
 - Analyze and isolate attack patterns and impact
 - Make any query, at any time, on any data set without reindexing.
 - Retain logs from days to years to meet your audit requirements

Open Web Analytics

- Open Web Analytics (OWA) is open source web analytics software created by Peter Adams. It is written in PHP and uses a MySQL database.
- OWA is comparable to Google Analytics (Google Analytics is used to track website performance and collect visitor insights), though OWA is server software anyone can install and run on their own host, while Google Analytics is a software service offered by Google.
- OWA supports tracking with WordPress and MediaWiki, two popular web site frameworks.
- WordPress is a content management system (CMS) that allows to host and build websites. WordPress contains plugin architecture and a template system, so you can customize any website to fit your business, blog, portfolio, or online store
- MediaWiki is a collaboration and documentation. The MediaWiki software is used by tens of thousands of websites and thousands of companies and organisations. It is used as a knowledge management and content management system on websites such as wikiHow, Intellipedia and Diplopedia (online encyclopedia of foreign affairs information).
- This application helps keep track of and observe the influx of views on your website. The program also tracks your competitors and their company's growth compared to yours.

Webalizer

- The Webalizer is a GPL (General public liscense) application that generates web pages of analysis, from access and usage logs, i.e. it is web log analysis software.
- It is one of the most commonly used web server administration tools.
- It was initiated by Bradford L. Barrett in 1997. Statistics commonly reported by Webalizer include hits, visits, referrers, the visitors' countries, and the amount of data downloaded.
- These statistics can be viewed graphically and presented by different time frames, such as by day, hour, or month.

- The Webalizer is a command line application and is launched from the operating system shell prompt.
- Besides the command line options, the Webalizer may be configured through parameters of a configuration file. By default, The Webalizer reads the file and interprets each line as a processing instruction.
- By default, The Webalizer produces two kinds of reports - a yearly summary report and a detailed monthly report, one for each analyzed month.
- The yearly summary report provides such information as the number of hits, file and page requests, hosts and visits, as well as daily averages of these counters for each month. The report is accompanied by a yearly summary graph.

Reports Generated:

1. Each of the monthly reports is generated as a single HTML page containing a monthly summary report (listing the overall number of hits, file and page requests, visits, hosts, etc.).
2. A daily report (grouping these counters for each of the days of the month).
3. An aggregated hourly report (grouping counters for the same hour of each day together).
4. A URL report (grouping collected information by URL),
5. A host report (by IP address),
6. Website entry and exit URL reports (showing most common first and last visit URLs),
7. A referrer report (grouping the referring third-party URLs leading to the analyzed website),
8. A search string report (grouping items by search terms used in such search engines as Google),
9. A user agent report (grouping by the browser type) and
10. A country report (grouping by the host's country of origin).

- Each of the standard HTML reports described in previous slide lists only top entries for each item (e.g. top 20 URLs). The actual number of lines for each of the reports is controlled by configuration.
- The Webalizer may also be configured to produce a separate report for each of the items, which will list every single item, such as all website visitors, all requested URLs, etc.
- In addition to HTML reports, The Webalizer may be configured to produce comma-delimited dump files, which list all of the report data in a plain-text file.
- Dump files may be imported to spreadsheet applications or databases for further analysis.

- **Internationalization**
- HTML reports may be produced in over 30 languages, including Catalan, Croatian, Czech, Danish, Dutch, English, Estonian, Finnish, French, Galician, German, Greek, Hungarian, Icelandic, Indonesian, Italian, Japanese, Korean, Latvian, Malay, Norwegian, Polish, Portuguese, Portuguese (Brazil), Romanian, Russian, Serbian, Simplified Chinese, Slovak, Slovene, Spanish, Swedish, Turkish, Ukrainian.
- To generate reports in an alternate language requires a separate webalizer binary compiled specifically for that language.
- Generated statistics do not differentiate between human visitors and robots. As a result, all reported metrics are higher than those due to people alone.
- Many webmasters claim that webalizer produces highly unrealistic figures of visits, which are sometimes 200 to 900% higher than the data produced by Javascript based web statistics such as Google Analytics or StatCounter.

AI Can Revolutionize Digital Forensics

- AI algorithms and techniques offer a range of benefits, enhancing the efficiency and effectiveness of investigations and helping organizations proactively mitigate data-based security risks.
- From automated log analysis and malware detection to network traffic analysis and forensic triage, AI can play a crucial role in several digital forensic activities and have a transformative impact on investigations.

Automated Log Analysis

- Security teams deal with a massive volume of log files generated by various systems, applications, and network devices, but analyzing these logs manually can be time-consuming and error-prone. That's where automated log analysis comes in.
- AI algorithms excel at processing vast quantities of log files and analyzing them for patterns and anomalies.
- With AI-powered log analysis, investigators can swiftly identify suspicious activities, potential security incidents, and areas requiring further investigation.
- AI enhances the speed and accuracy of log analysis, enabling investigators to focus their efforts on relevant areas of interest and avoid spending time and resources on manual review.

Malware Detection

- The rapid evolution of malware calls for advanced detection methods.
- AI-powered malware detection systems:
 1. leverage machine learning to review and scan code and study user behavior patterns,
 2. detecting malicious software more effectively and
 3. helping investigators remove malware from compromised systems to safeguard against further attacks.
- For instance, security companies employ AI algorithms to continuously learn from known malware samples and their characteristics.
- By training these algorithms on large datasets, they can detect and classify new and previously unknown malware strains based on similarities to previously identified threats and flag a potential attack before it happens.

Image and Video Analysis

- The analysis of digital images and videos is a critical component of digital forensics.
- For example, AI algorithms can sift through large volumes of multimedia content — quickly identifying faces, objects, or text within images and videos, thus significantly speeding up the process of finding and extracting crucial evidence — and support a wide range of investigation scenarios.
- Consider a case where investigators need to identify a suspect captured in surveillance footage from a crowded area. Reviewing video footage is often tedious and can take hours.
- AI-powered facial recognition technology can rapidly scan through vast amounts of video data, pinpointing individuals of interest and significantly reducing the manual effort required.
- This technology expedites the identification process, enabling investigators to focus their efforts on the most relevant leads and accelerate the progress of the investigation.

Natural Language Processing

- Natural language processing (NLP) enable the analysis of pertinent information from large volumes of text data.
- For example, text-based data, including emails, chat logs, and documents, contain valuable evidence in digital investigations.
- Extractive AI can be more efficient and accurate to uncover relationships, detect patterns, and identify key individuals during text-focused investigations.
- Imagine a scenario where investigators are examining a massive collection of chat logs to identify potential collaborators in a cybercrime.
- AI-powered NLP algorithms can rapidly process and analyze the text data, identifying recurring phrases, suspicious patterns, and connections between individuals.
- This enables investigators to pinpoint key persons of interest and uncover hidden networks, expediting the investigative process and enabling timely interventions.

Network Traffic Analysis

- Monitoring and analyzing network traffic patterns is essential for detecting and responding to cyber attacks.
- Rather than conducting a manual audit and analyzing network traffic patterns at predetermined intervals, forensics teams can train AI algorithms
 1. to analyze network packets automatically,
 2. identify deviations from normal traffic patterns, and
 3. issue alerts when an anomaly merits further investigation.
- AI can also assist in correlating network events with known attack patterns, providing valuable insights for incident response teams.

Forensic Triage

- Forensic triage (or "digital forensic triage") is the process by which you collect, assemble, analyze, and prioritize digital evidence from a crime or investigation.
- Digital investigations involve massive volumes of data, requiring investigators to quickly sift through and prioritize relevant evidence.
- AI in forensic triage involves the use of machine learning algorithms to classify and categorize large numbers of digital files based on their relevance to an investigation.
- These tools analyze file metadata, content, and other attributes to prioritize files for closer scrutiny, continually "learning" to identify relevant material with increasing accuracy as new data is added to the investigation.
- Forensics teams are able to quickly identify and focus on the most important evidence earlier, leading to faster and more effective investigations while optimizing resource allocation.

AIBFT

Artificial Intelligence Browser Forensic Toolkit

p

MOBILE DEVICE FORENSICS

MOBILE DEVICE FORENSICS

- Mobile device forensics is a branch of digital forensics relating to recovery of digital evidence or data from a mobile device under forensically sound conditions.
- The phrase mobile device usually refers to mobile phones; however, relate to any digital device that has both internal memory and communication ability, including PDA devices, GPS devices and tablet computers.
- Mobile devices can be used to save several types of personal information such as contacts, photos, calendars and notes, SMS and MMS messages.
- Smartphones contain video, email, web browsing information, location information, and social networking messages and contacts.

- There is growing need for mobile forensics due to several reasons and some of the prominent reasons are:
 1. Use of mobile phones to store and transmit personal and corporate information
 2. Use of mobile phones in online transactions
 3. Law enforcement, criminals and mobile phone devices.

Challenges In Mobile Forensics

- Evidential and technical challenges exist. For example, cell site analysis following from the use of mobile phone usage coverage, is not an exact science.
- It is possible to determine roughly the cell site zone from which a call was made or received, but it is not yet possible to say with any degree of certainty, that a mobile phone call emanated from a specific location e.g. a residential address.
- To remain competitive, original equipment manufacturers frequently change mobile phone form factors, operating system file structures, data storage, services, peripherals, and even pin connectors and cables.
- As a result, forensic examiners must use a different forensic process compared to computer forensics.

- Storage capacity continues to grow for more powerful "minicomputer" type devices.
- Not only the types of data but also the way mobile devices are used constantly evolve.
- Hibernation behaviour in which processes are suspended when the device is powered off or idle but at the same time, remaining active.
- As a result of above challenges, a wide variety of tools exist to extract evidence from mobile devices; one tool or method cannot acquire all the evidence from all devices.
- It is recommended that forensic examiners, especially those wishing to qualify as expert witnesses in court, undergo extensive training in order to understand how each tool and method acquires evidence.

- Mobile communication means can be categorized in basically three modes:
 - WiFi
 - Bluetooth
 - Infrared Device Authentication (IrDA)

Evidences In A Mobile Device

- As mobile device technology advances, the amount and types of data that can be found on a mobile device is constantly increasing.
- Evidence that can be potentially recovered from a mobile phone come from several different sources, including handset memory, SIM card, and attached memory cards such as SD cards.
- Traditionally mobile phone forensics has been associated with recovering SMS and MMS messaging, as well as call-logs, contact lists and phone IMEI/ESN information.
- Newer generations of smartphones include wider varieties of information:
 1. from web browsing,
 2. Wireless network settings,
 3. geo-location information (including geo-tags contained within image metadata),
 4. e-mail and other forms of rich internet media,
 5. social networking service posts and
 6. contacts now retained on smartphone 'apps.

Service Provider Logs

- Although not technically part of mobile device forensics, the call detail records (and occasionally, text messages) from wireless carriers serve as "back up" evidence obtained after the mobile phone has been seized.
- These are useful when the call history and/or text messages have been deleted from the phone, or when location-based services are not turned on.
- Call detail records and cell site (tower) dumps can show the phone owner's location, and whether they were stationary or moving (i.e., whether the phone's signal bounced off the same side of a single tower, or different sides of multiple towers along a particular path of travel).
- Carrier data and device data together can be used to corroborate information from other sources, for instance, video surveillance footage or eyewitness accounts; or to determine the general location where a non-geo-tagged image or video was taken.

- The **European Union** requires its member countries to retain certain telecommunications data for use in investigations.
 - This includes data on calls made and retrieved.
 - The location of a mobile phone can be determined and this geographical data must also be retained.
-
- In the **United States**, no such requirement exists, and no standards govern how long carriers should retain data or even what they must retain.
 - For example, text messages may be retained only for a week or two, while call logs may be retained anywhere from a few weeks to several months.
 - To reduce the risk of evidence being lost, law enforcement agents must submit a preservation letter to the carrier, which they then must back up with a search warrant.

Subscriber Identification Module

- A subscriber identity module (SIM) is a smart card inside of a GSM cellular phone that encrypts voice and data transmissions and stores data about the specific user so that the user can be identified and authenticated to the network supplying the phone service.
- The SIM also stores data such as personal phone settings specific to the user and phone numbers.
- If the phone not uses SIM cards then the identity information is stored in the phone hardware itself.
- This identification information can be used to trace a victim using service provider logs.

Mobile Logs

- Mobile phones are capable to maintain logs of calls that were made, missed and received. This information can be crucial forensically.
- Other logs that are also maintained mostly in the background are GPS information, connection information, etc. Using these we can track the locations of mobile phones quite easily.

Phone books/contact lists

- Phonebook names and numbers give investigative leads to potential witnesses and victims.
- Phone book can have typical information such as e-mail addresses, home addresses, phone numbers, profile photographs, and even alternative phone numbers.

Text messages

- Text messages can have bits of evidence as well as date and time stamps, which can be very valuable to investigators. Often deleted messages can be recovered along with time stamps and can be used into establishing leads in an investigation.

Application files

- Smart phones etc. have an operating system and the applications installed on these operating systems maintain lots of files and data logs which can be vital sometimes during forensic investigations.
- Forensically important data sources in a mobile devices can be Calendars and event's organizers, E-mail, Instant messages, Photos, Audio recordings etc.

MOBILE FORENSIC PROCESS

- 1. Seizure**
- 2. Acquisition**
- 3. Analysis**

SEIZURE

- Seizing mobile devices is covered by the same legal considerations as other digital media.
- Mobiles will often be recovered switched ON. As the aim of seizure is to preserve evidence, the device will be transported in the same state to avoid a shutdown, which would change files.
- The investigator or first responder would risk user lock activation.
- Leaving the phone ON carries another risk **the device can still make a network/cellular connection**. This may bring in new data, overwriting evidence.
- To prevent a connection, mobile devices will often be transported and examined from **within a Faraday cage** (or bag).
- Even so, there are two disadvantages to this method. **First**, it renders the device unusable, as its touch screen or keypad cannot be used. **Second**, a device's search for a network connection will drain its battery more quickly.
- While devices and their batteries can be recharged, again, the investigator risks that the phone's user lock will have activated.
- Therefore, **network isolation is advisable** either through placing the device in Airplane Mode, or cloning its SIM card.
- At all costs, you must keep new data from contaminating the mobile device after it has been seized.

Mobile devices can be isolated in many ways:

1. **Isolating its wireless features:** By using a Faraday bag or a jamming device/mobile phones i.e, can be isolated to network till the battery drains completely. Devices increase their strength to search a network; this drains the battery very fast.
2. **Switch off the device:** This method is fine however on switching ON, the phone lock or sim lock can be activated which can lead the phone unusable. Unlocking can be possible but is quite tricky.
3. **Airplane mode:** Airplane mode when activated, suspends many of the device's signal transmitting functions, thereby disabling the device's capacity to place or receive calls or use text messaging – while still permitting use of other functions that do not require signal transmission (e.g., games, built-in camera, MP3 player). When the "airplane mode" is activated, it will disable all cellular services as well as other signal-transmitting technologies such as Wi-Fi and Bluetooth. Wi-Fi and Bluetooth can be enabled separately even while the device is in airplane mode.

ACQUISITION

- It is referring to retrieval of material from a device (as compared to the bit-copy imaging used in computer forensics).
- Due to the proprietary nature of mobiles it is often not possible to acquire data with it powered down; most mobile device acquisition is performed live.
- With more advanced smartphones using advanced memory management, connecting it to a recharger and putting it into a faraday cage may not be good practice.
- The mobile device would recognize the network disconnection and therefore it would change its status information that can trigger the memory manager to write data.

- Most acquisition tools for mobile devices are commercial in nature and consist of a hardware and software component, automated.
- Acquiring data from mobile phones can be very tricky and need lot of training and expertise. The acquisition can vary from mobile device to mobile device.
- Devices, such as cameras, are treated as storage devices in much the same way as USB drives.
- Mobile phones, require specific forensic software tools to extract data in a forensic way.
- Basic guidelines while handling digital forensic data is to be careful and see that the data on the original media is not altered in any way either by chance or intentionally.
- We need to document every aspect of the investigation and need to keep things centralized with proper responsibility attached to all investigators and companies involved.
- Fundamentally we look into three components in a mobile device they are **Read only Memory (ROM), Random Access Memory (RAM) and Data Storage.**
- These components and their forensics can be very similar to that of Memory Forensics.

Acquisition involves following things to be done:

1. Type of Cellular Network, Code Division Multiple Access (CDMA), Global System for Mobile Communication (GSM), Integrated Digital Enhanced Network (iDEN) (A proprietary system, developed by Motorola, that uses advanced SIM cards (USIMs) and is expected to replace both CDMA and GSM).
2. Manufacturer Information of the mobile phone can be identified by Logos, Serial numbers, manufacturing codes (like IMEI: International Mobile Equipment Identifier) etc. It is advisable to cross verify the facts through Internet from online databases of the manufacturer or contact the manufacturers.
3. Phone characteristics of the device can be found from the manufacturer advertisements blogs etc. The characteristics can also guide us find areas for initial search for evidence. Some of these characteristics can be Operating system, Wireless access methods (Bluetooth, WiFi, or infrared), Camera, manufacturer applications, internet access methods, messages etc

Examination And Analysis

- Mobile phone forensics analysis involves the technical examination of mobile phones and the retrieval of data from these devices.
- Data for analysis can be obtained from SIM cards, memory cards and from the phone handset itself. Forensic analysis of mobile phones can be carried out on various forms of data, including textual (SMS Messages), Graphic (Images), Audio Visual (Videos) and Audio (Sound recordings).
- Mobile phone have large storage capacities, has meant that increasingly, larger amounts of personal information is now being stored on these devices.
- Individuals are now becoming increasing reliant on their mobile phones as part of their daily lives.
- The variety of applications and facilities these devices provide including Internet, Wi-Fi, email, document viewing and editing software along with the more common mobile phone features of phonebook, call history, text messaging, voice mail, built in camera and audio facilities have seen it overlap with computer technology.

- The existing generation of mobile phones is sophisticated and increasingly difficult to examine however they can ultimately provide valuable evidence in prosecuting individuals.
- The information obtained from a phone, after intensive analysis techniques proves to be adequate for a conviction of a criminal by detectives involved with the case.
- Internal memory and external memory as well as the call and text records can all be analyzed to gain an insight into the activities of the mobiles owner as well as who they have been speaking or exchanging messages with.
- The area is ever expanding and allows for cutting edge technology to be used to keep up with the ever growing array of mobile phones on the market today and the ever increasing feature list of these phones.
- Mobile forensic analysis will continue to be a specialised field while technology progresses rapidly with the sheer number of phones to be examined posing a challenge for the police.

FORENSIC ACQUISITION TOOLS

- There are two categories of forensics acquisition tools. They are:
 1. Hardware acquisition tools.
 2. Software acquisition tools.

Hardware Acquisition Tools

Faraday bag

- A Faraday bag keeps a mobile device from communicating with an external wireless device, by intercepting radio waves and effectively acting as a large, external antenna that redirects the radio energy away from the device.
- Faraday bags work to keep data from reaching the mobile device and keep the mobile device from transmitting any data outward.
- A Faraday bag can be as small as the device you're isolating to as large as a tent when you need to do field work and need to isolate the device and your acquisition equipment at the same time.
- In the mobile forensic environment, isolating the device is of prime importance when you arrive on-scene.

SIM card reader

- A card reader is used to read SIM and USIM cards without having to use the handset.
- Some card readers are built into the computer platform, and other card readers use a USB interface.

Cable connections

- With the multitude of mobile devices now on the market, having just one mobile device connector seriously hampers your ability to do an investigation.
- Different mobile device manufacturers have not only different data cable connections but also different power connection interfaces.
- At the top of your list should reside the standard USB cable followed by the USB cable with a mini-USB connection.

Software Acquisition Tools

www.MobileForensicsCentral.com

- This web site provides access to a comprehensive database of phones supported by various software suppliers.
- A user of the web site can enter a model of a phone and the site will return a detailed report of which software and cables support it, as well what information can be retrieved from the device with the software.
- The goal of the site is to enable users to more efficiently find the right tool for the device they are confronted with.

BITPIM35

- **BitPim** is an open source program designed for managing content on CDMA devices. BitPim might be taken for a "personal information manager" (PIM), its name derives from.
- Allows to view and manipulate data on specific cell phones.
- This includes the phonebook, calendar, wallpapers, ringtones (functionality varies by phone) and the file system.

CELLDEK36

- The revolutionary celldek has been developed in cooperation with the UK's forensic science service.
- The portable celldek acquires data from over 200 of the most popular cell phones and PDA's.
- Built to perform in the field (not just in the lab), investigators can immediately gain acces to vital information, saving days of waiting for a report from a crime lab.

Cell Seizure37

- Cell seizure allows you to acquire, analyze, and report on cell phone data for certain models of GsmSim Cards, Nokia, Samsung, Motorola, Sony-Ericsson, Lg, And Siemens cell phones.
- It can also acquire data from CDMA/TDMA phones.
- Designed for computer forensic examiners, cell seizure offers complete forensic examinations that can be presented in court with hash verification, write protection, html reporting, and full data dumps on some models. Version 3.0 adds support for LG, updates model support for other manufacturers, and updates sim card support

Mobilyze38

- Mobilyze is a mobile data triage tool, designed to give users immediate access to data from iOS and Android devices.
- Specifically designed with ease of use in mind, Mobilyze was built to respond to the mounting backlogs of evidentiary mobile devices in law enforcement agencies, both domestically and overseas.
- The Mobilyze application runs on either Mac or Windows and can be effectively deployed in the field or within a forensics lab.
- Once Mobilyze has been installed, simply plug the smartphone or tablet into a USB port, and Mobilyze will begin collecting all relevant user data.
- This data is then available for viewing, searching, and filtering within minutes.
- Mobilyze allows users of all technical abilities to quickly ascertain whether a device contains relevant forensic evidence, whether immediate action needs to be taken, and/or whether the device needs to be sent to a forensics lab for a comprehensive analysis.
- Once relevant data is discovered, Mobilyze provides one-click reporting in a clean and easily readable format.
- If further analysis is required, users can seamlessly import Mobilyze data for a more comprehensive forensic analysis.

Oxygen Phone Manager II (Forensic Version)

- A special software for police departments, law enforcement units and all government services that wish to use the power of Oxygen Phone Manager II for investigation purposes.
- Forensic edition secures phone data to remain unchanged during extraction and exporting.

Oxygen Phone Manager II

- Oxygen phone manager II offers management for phonebook, call register, calendar, todo lists, SMS and MMS messages, logos, tones, GPRS and WAP settings, profiles, phone dictionary, FM stations, Java games and applications.

Paraben's SIM Card Seizure

- Paraben's SIM card seizure takes the SIM card acquisition and analysis components from paraben's cell seizure and puts it into a specialized SIM card forensic acquisition and analysis tool.
- SIM card seizure includes the software as well as a forensic SIM card reader.
- If you already have cell seizure & the cell seizure toolbox, there's no need for you to get SIM card seizure as well because they contain the components to perform a forensic SIM card acquisition and analysis.
- This tool is for the investigator who only wants to acquire SIM cards and does not want to perform forensic exams of all cell phone data.

Paraben's PDASeizure

- Paraben's PDA seizure is a commercially available forensic software toolkit that allows forensic examiners to acquire and examine information on PDA s for both the pocket pc (PPC) and palm OS platforms.
- PDA seizure's features include the ability to acquire a forensic image of palm OS, pocket PC, and Blackberry devices, to perform examiner-defined searches on data contained within acquired files, generate hash values of individual files and to generate a report of the findings.
- PDA seizure also provides book-marking capabilities to organize information, along with a graphics library that automatically assembles found images under a single facility, based on the graphics file extension of the acquired files.

The forensicsim toolkit

- The forensicsim toolkit gives today's law enforcement agencies the capability to safely and confidently recover digital evidence from GSM SIM and 3G USIM devices.
- Acquisition, analysis and reporting form the three key stages of the forensically sound process that will save critical time and provide a cost effective solution to SIM card examinations.
- As an increasing number of mobile devices use high-level file systems, similar to the file systems of computers, methods and tools can be taken over from hard disk forensics or only need slight changes.