Digital Forensics

CONTENTS :-

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

Cyber 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 FORENISCS

- 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.

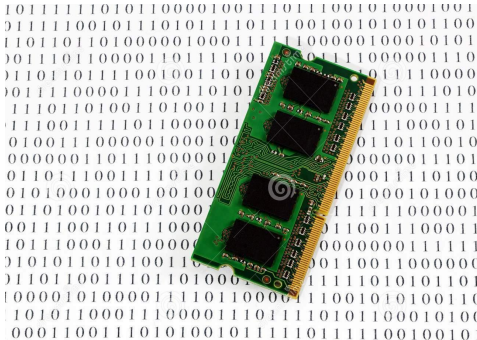
Types Of Digital Evidence

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

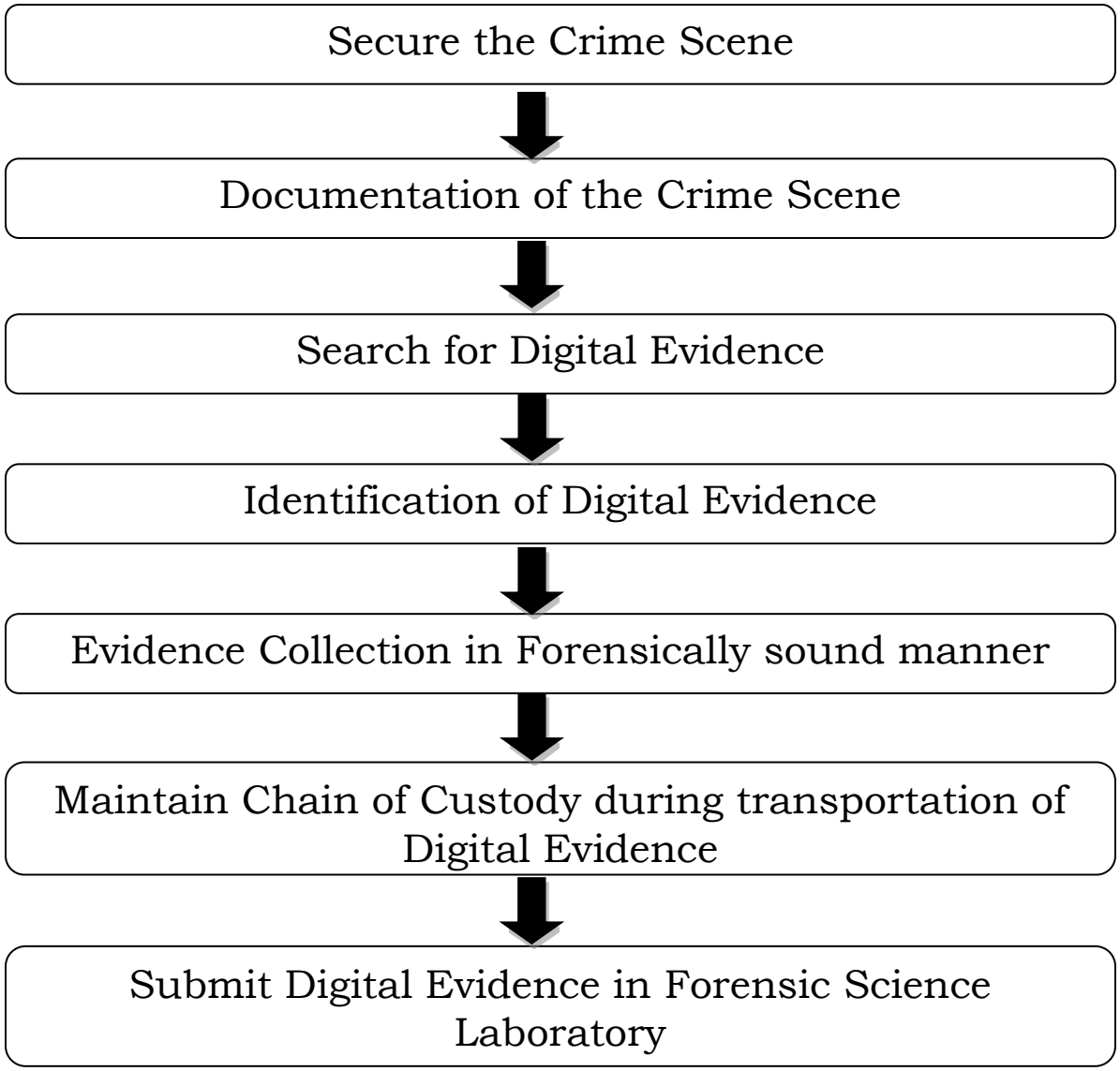
USB Teddy Bear

USB Cork

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)


Maxtor
OLD MAIL SERVER
TABLEAU
FireWire 800+USB2.0 SATA Bridge


1
Nikon
EVIDENCE


SATA/IDE
USB 2.0
3.5" HDD
CD-ROM
CD-RW
COMBO
DVD-ROM
DVD-RW
USB 2.0 to SATA/IDE cable

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

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.

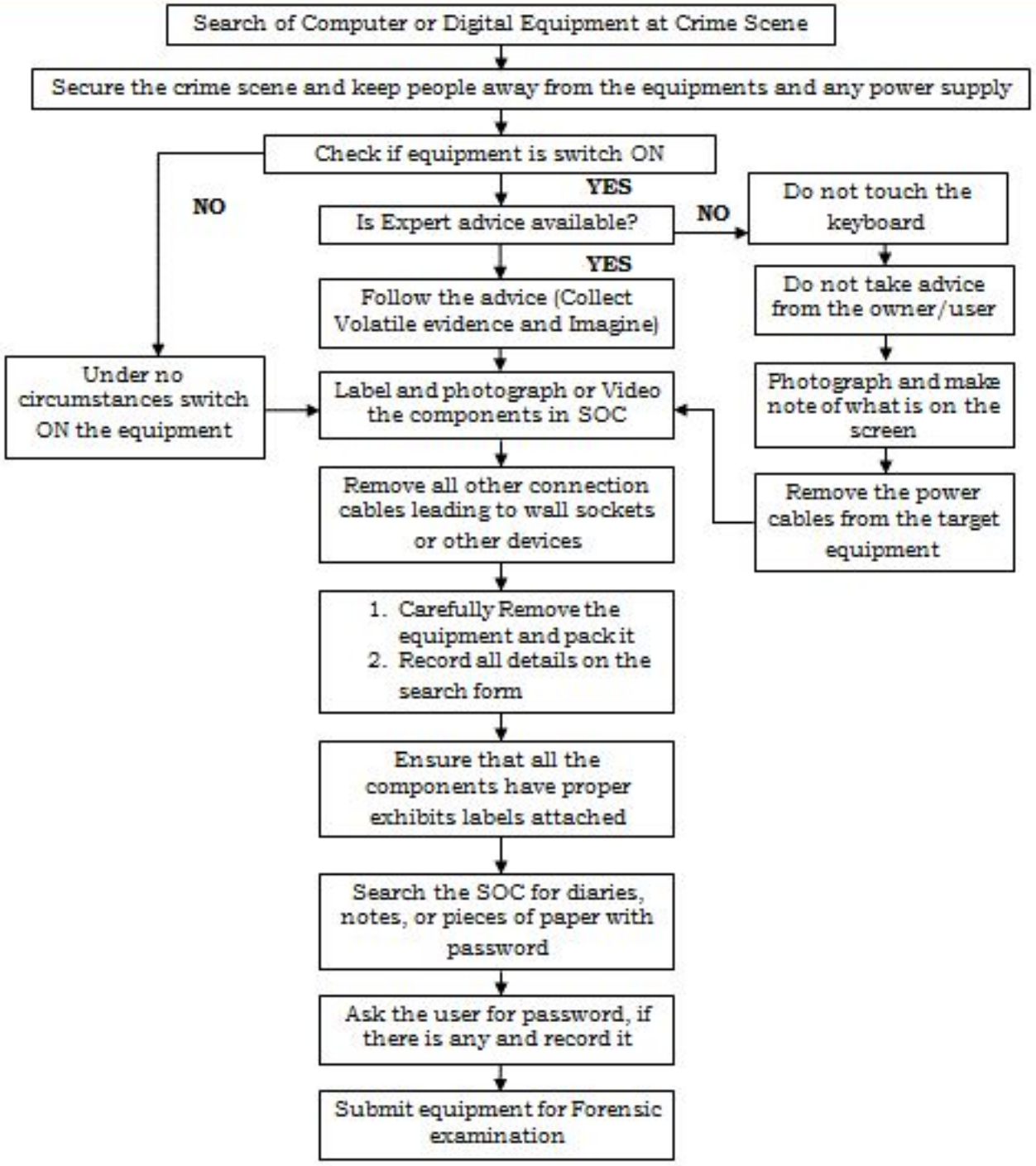
Situation 3: The Monitor Is Off

- 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


Search of Computer or Digital Equipment at Crime Scene
Secure the crime scene and keep people away from the equipments and any power supply
Check if equipment is switch ON
NO
YES
Is Expert advice available?
NO
YES
Do not touch the keyboard
Do not take advice from the owner/user
Photograph and make note of what is on the screen
Remove the power cables from the target equipment
Follow the advice (Collect Volatile evidence and Imagine)
Under no circumstances switch ON the equipment
Label and photograph or Video the components in SOC
Remove all other connection cables leading to wall sockets or other devices
1. Carefully Remove the equipment and pack it
2. Record all details on the search form
Ensure that all the components have proper exhibits labels attached
Search the SOC for diaries, notes, or pieces of paper with password
Ask the user for password, if there is any and record it
Submit equipment for Forensic examination

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

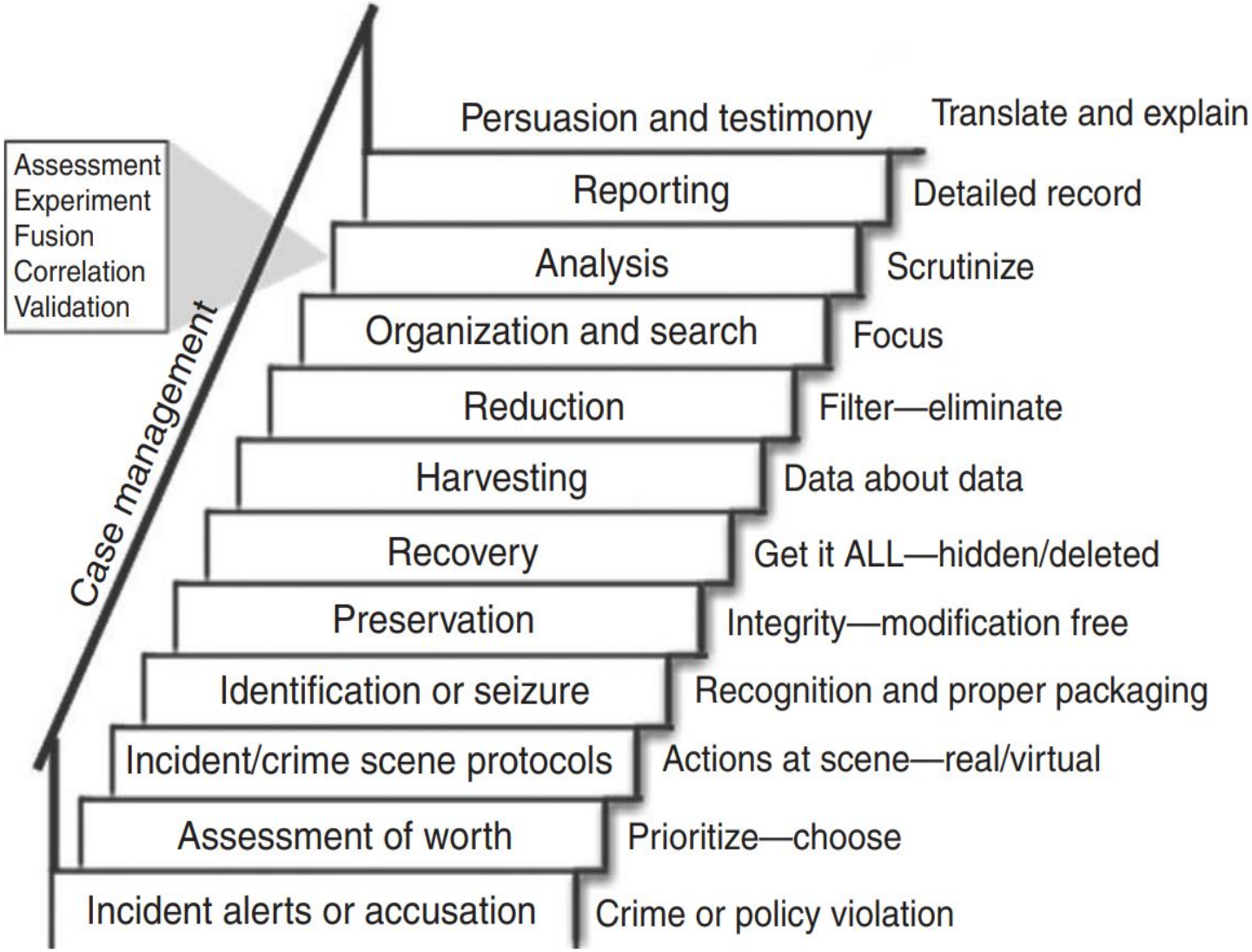
Method of evidence received (i.e. delivered, seized, discovered)

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	

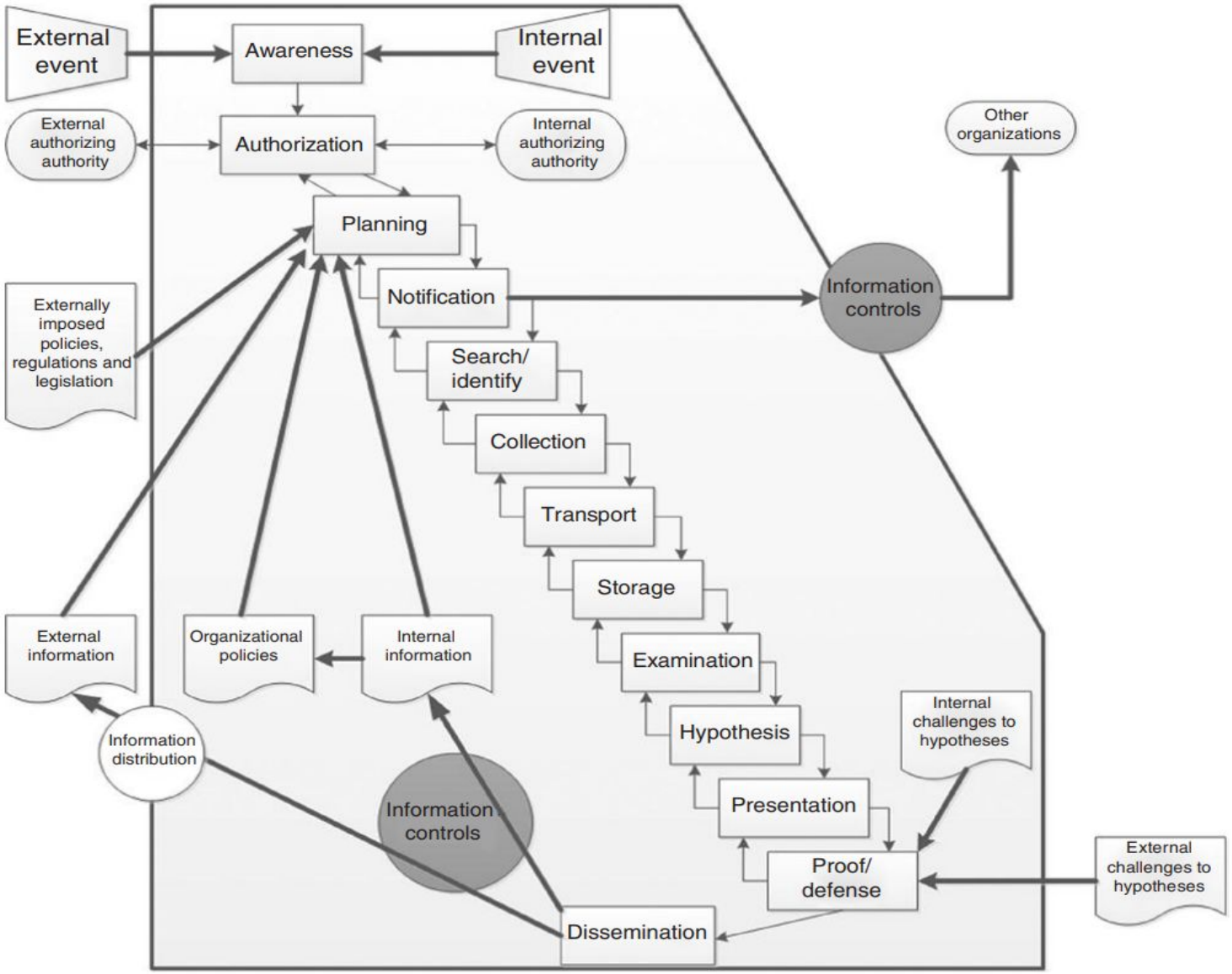
Physical Model: Investigation Process model

	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.

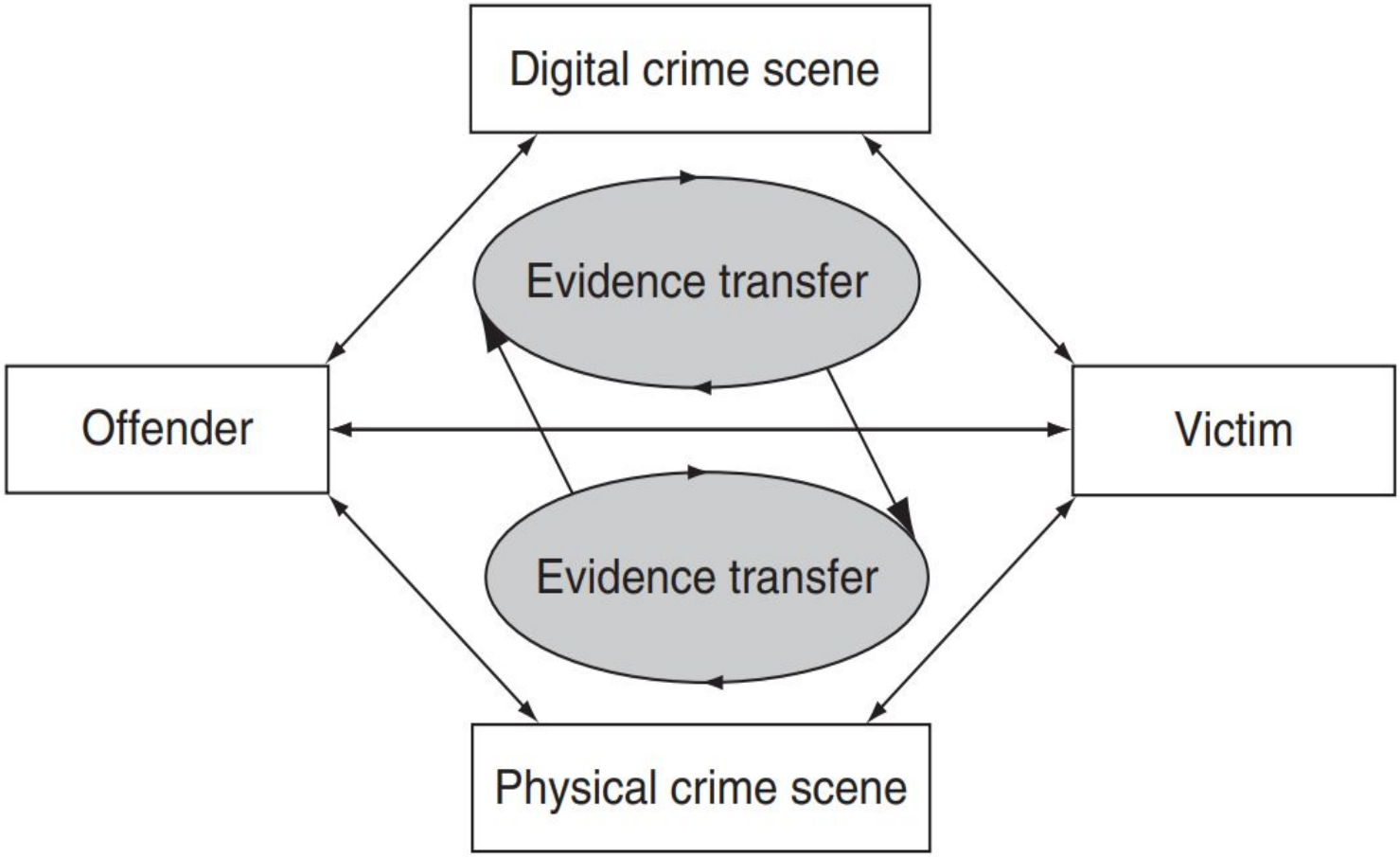
Locard's Principle

- "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 confirmity 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.

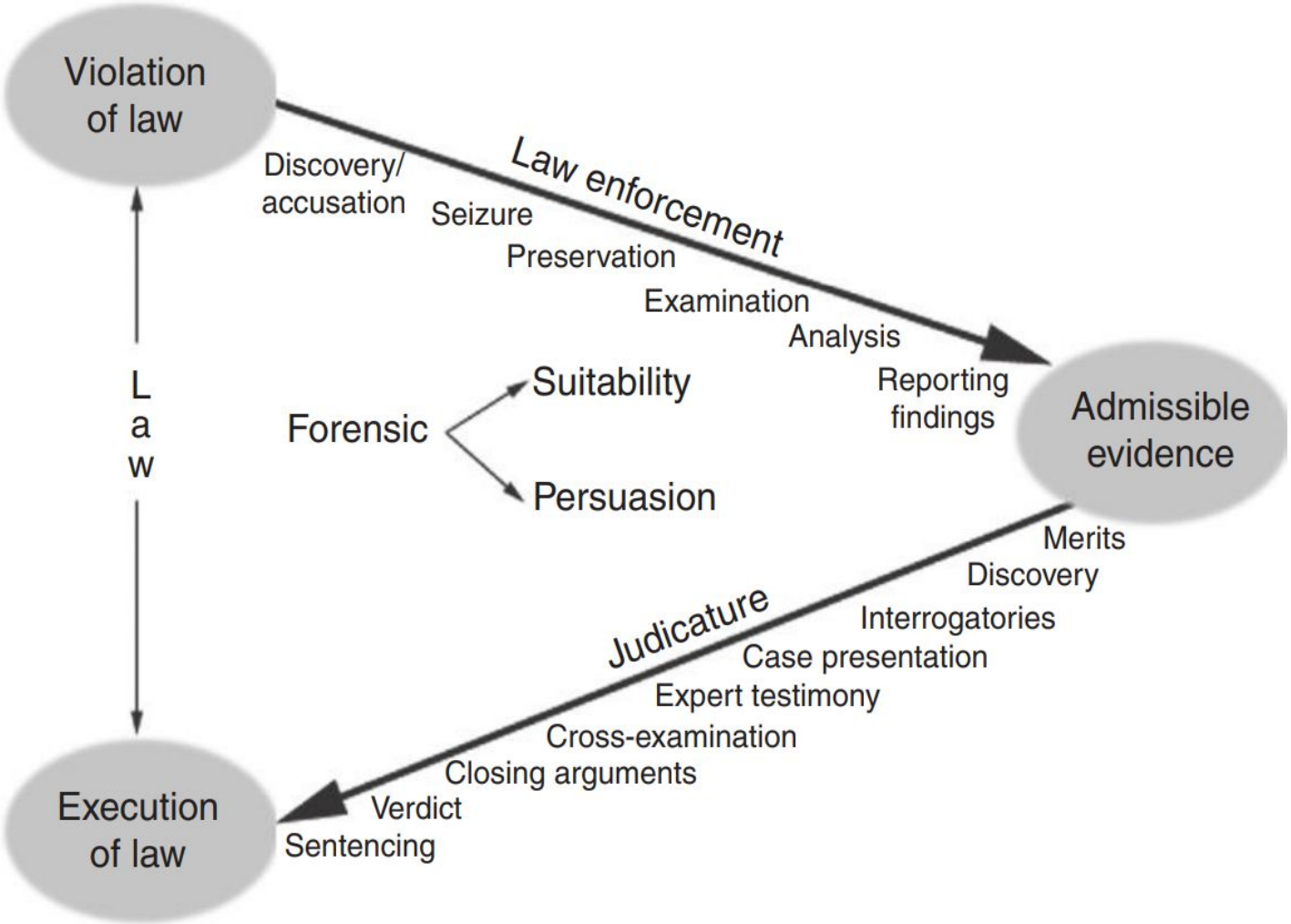
- This backup facility was outdated and had a flaw that caused it to change the times of the files on the disk before copying them.

- 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

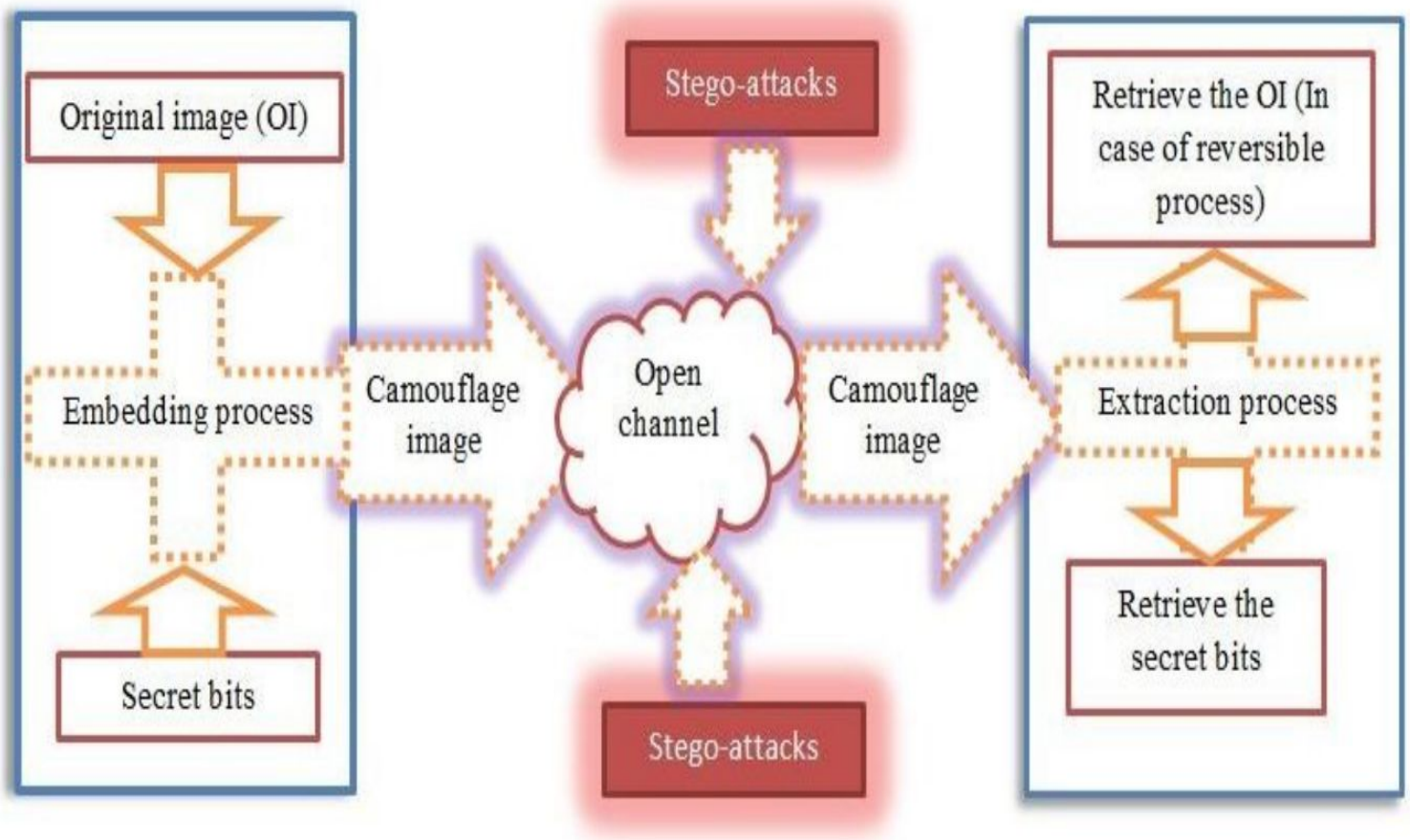
Steganography

- 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.

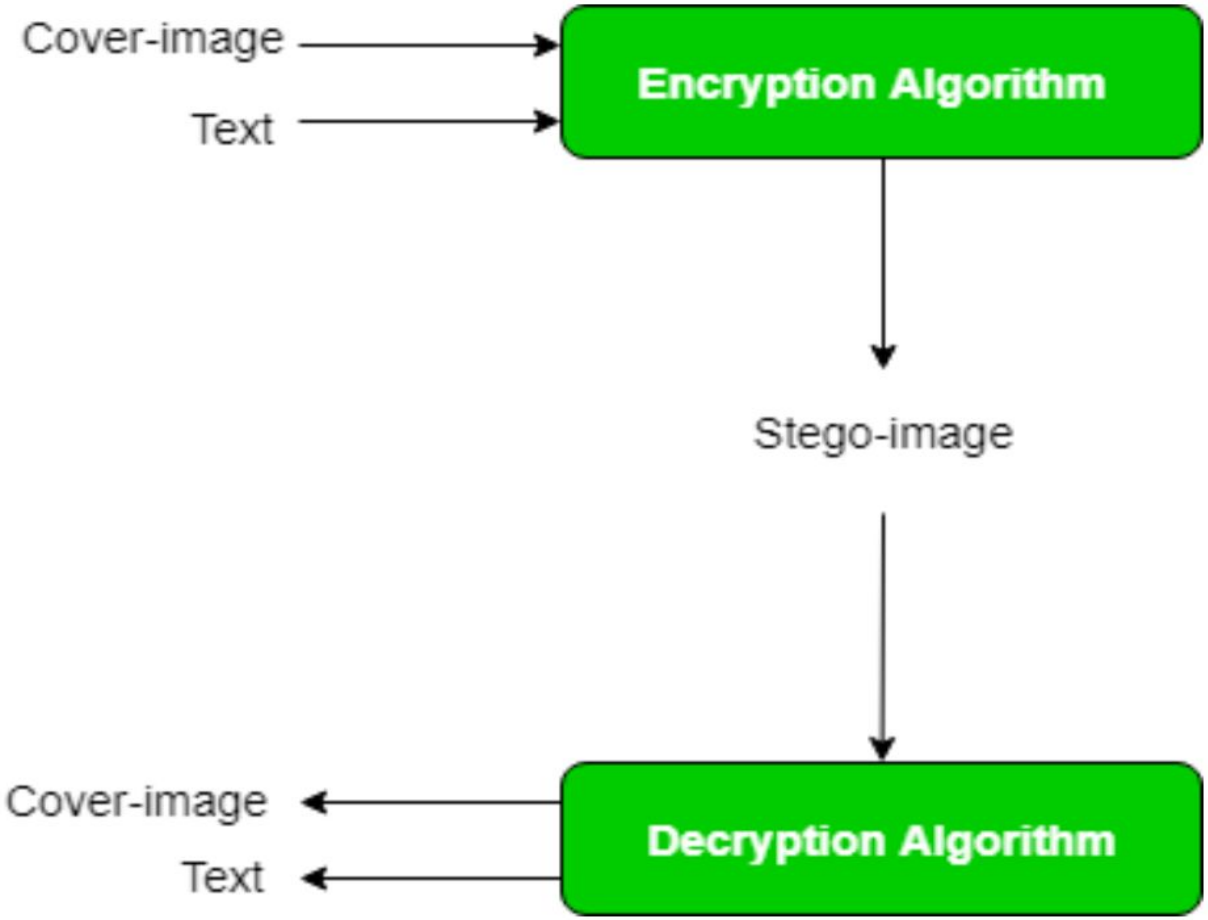
- Hiding confidential information inside the image is known as image steganography (IS)

- **How IS it done?**

An image is represented as an N*M (in case of grayscale images) or N*M*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; ques 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.

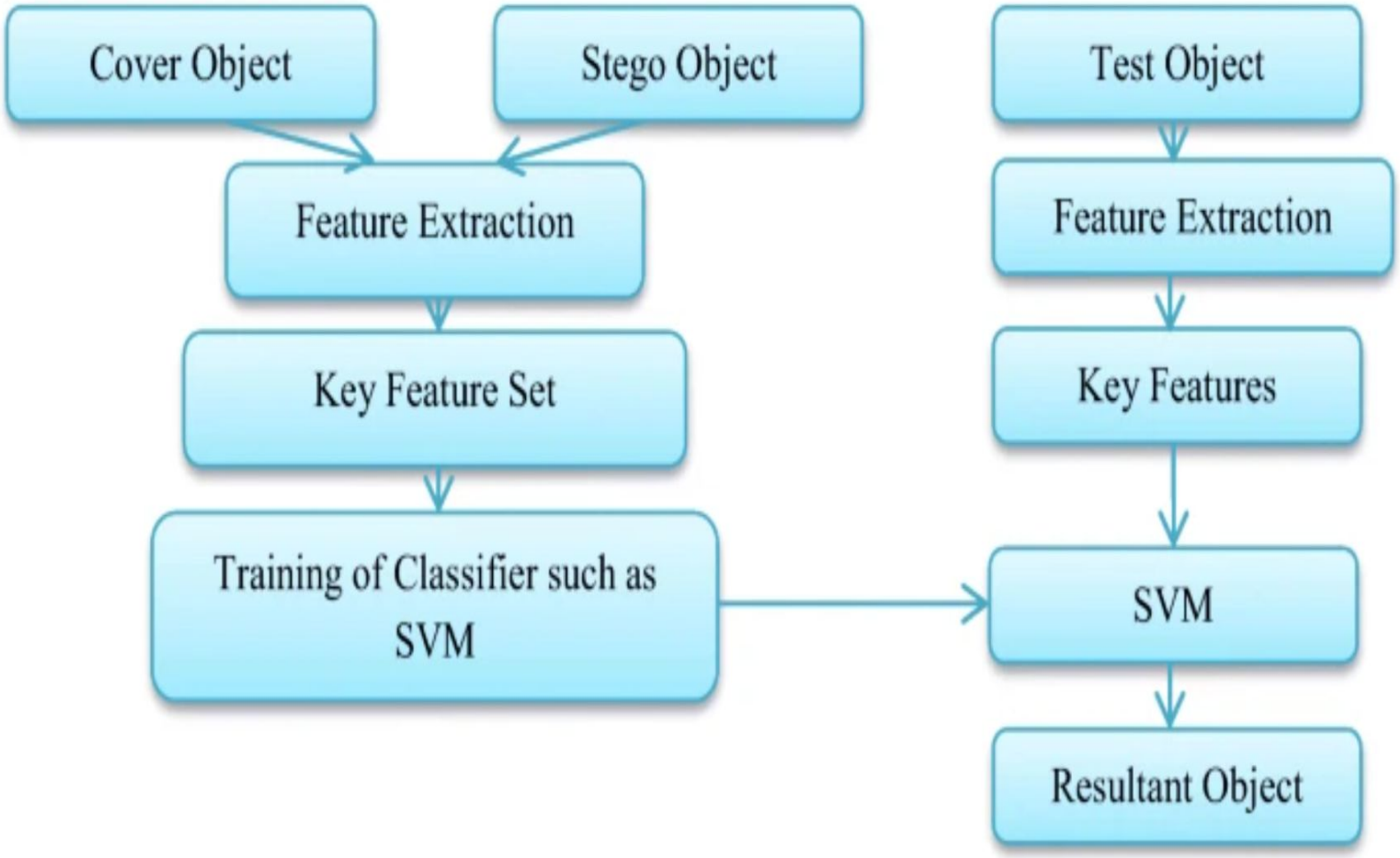
- The first one refers to extraction of statistical features from stego and clean images. These statistical features are compared then, in order to discriminate clean from stego images.

- 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.

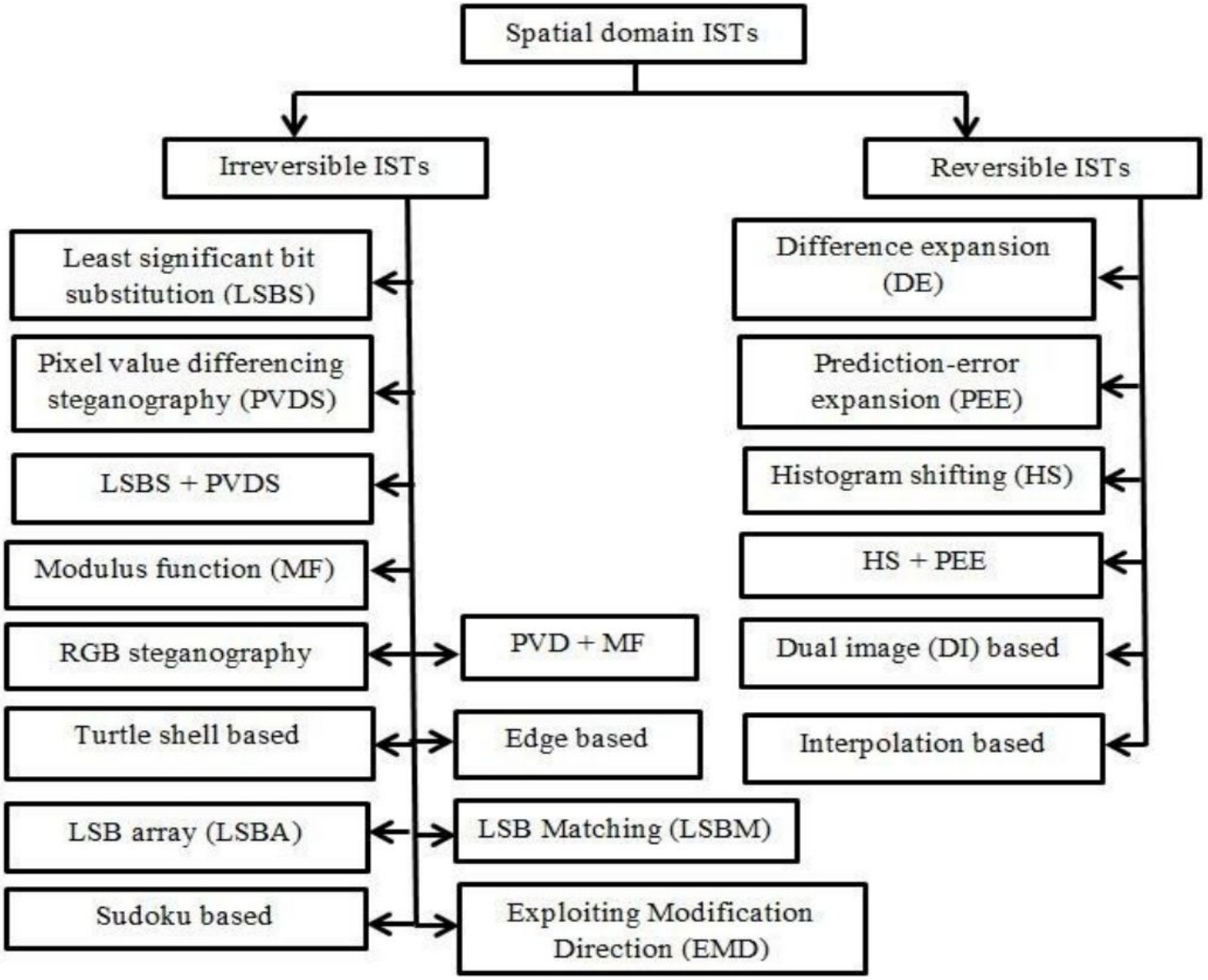
Paradigm For Machine Learning Classifiers



- **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.


Spatial domain ISTs
Irreversible ISTs
Reversible ISTs
Least significant bit substitution (LSBS)
Pixel value differencing steganography (PVDS)
LSBS + PVDS
Modulus function (MF)
RGB steganography
Turtle shell based
LSB array (LSBA)
Sudoku based
PVD + MF
Edge based
LSB Matching (LSBM)
Exploiting Modification Direction (EMD)
Difference expansion (DE)
Prediction-error expansion (PEE)
Histogram shifting (HS)
HS + PEE
Dual image (DI) based
Interpolation based

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.

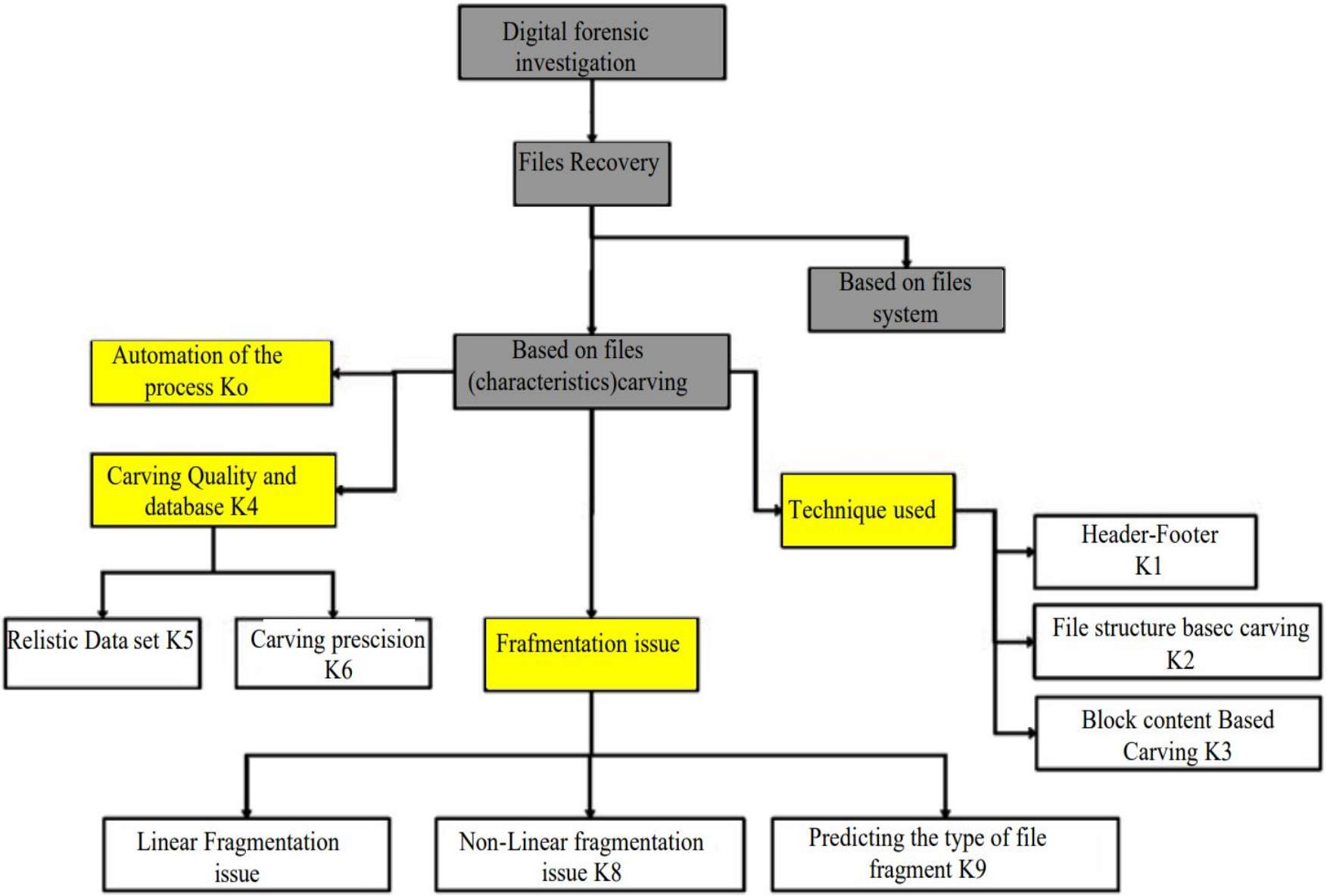
- HC refers to the ability to hide the maximum number of secret data. It is usually computed in bits.

- 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 originality 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 NTUSER.DAT	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.

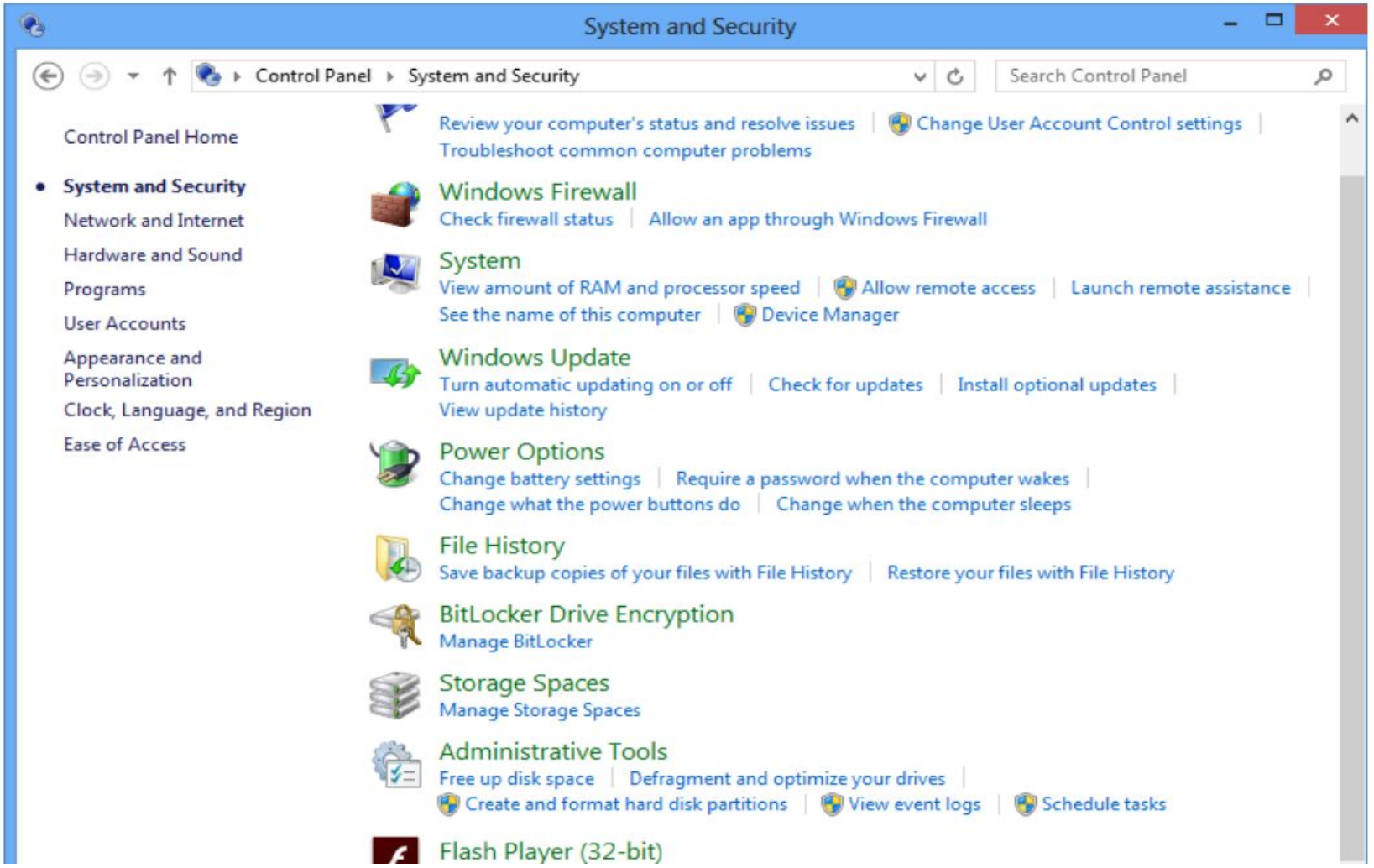
- ‘Computers‘ here is the name that the user gives to its computer.
- The name of computer generally is made once in the lifetime usage of the system and hence it can be used to trace various activities on network and internet carried by the user.
- Time of last shutdown is the time at which the system 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.

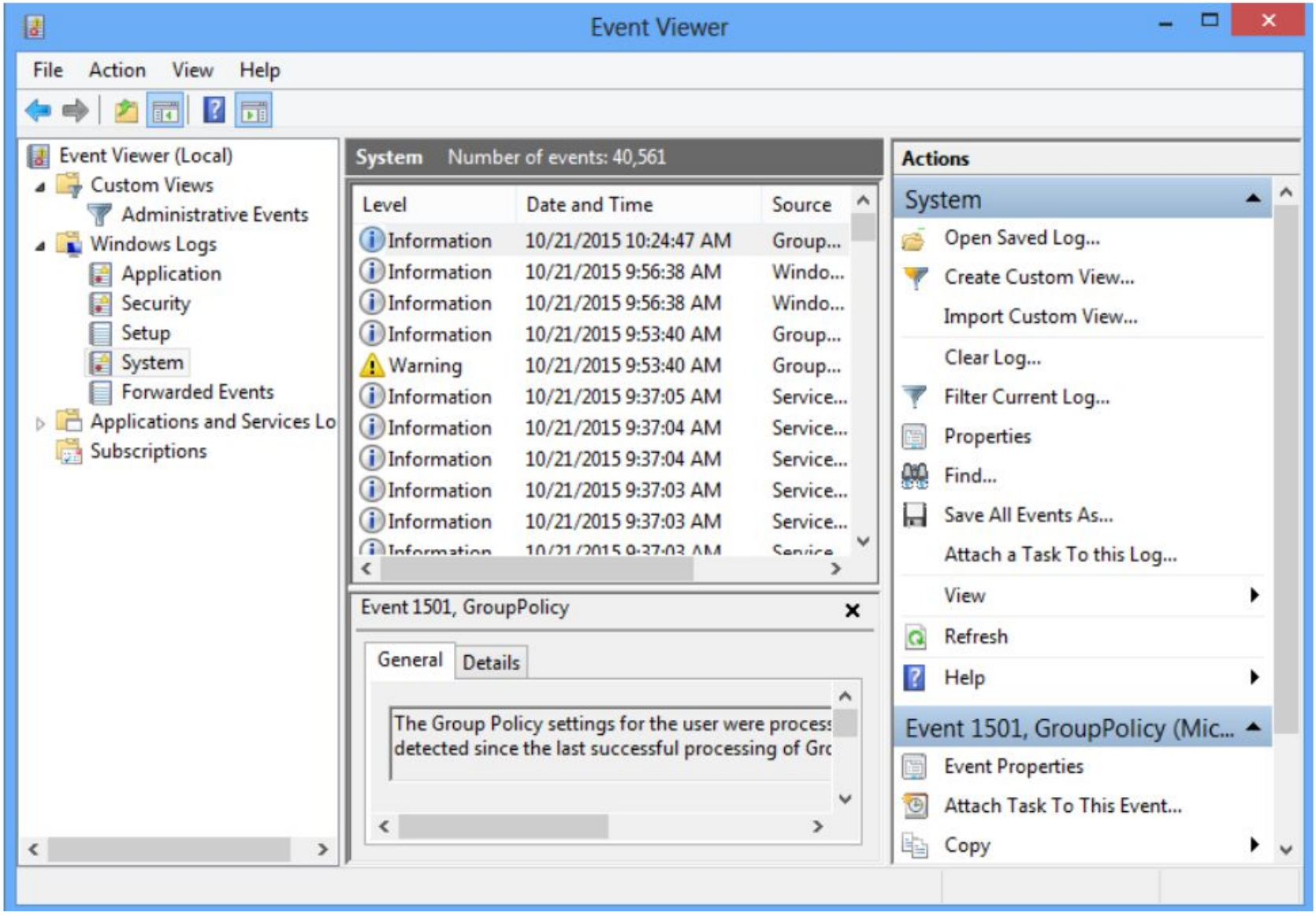
- A USB mass storage device yields a lot of artifacts when connected to a system.
- These artifacts are persistent in nature and are retained even after the system has been shut down and the information they contain may assist in carrying out forensic analysis on a suspect system.
- Artefacts of a USB 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 Lo
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...
Event 1501, GroupPolicy
General Details
The Group Policy settings for the user were process
detected since the last successful processing of Gro
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,

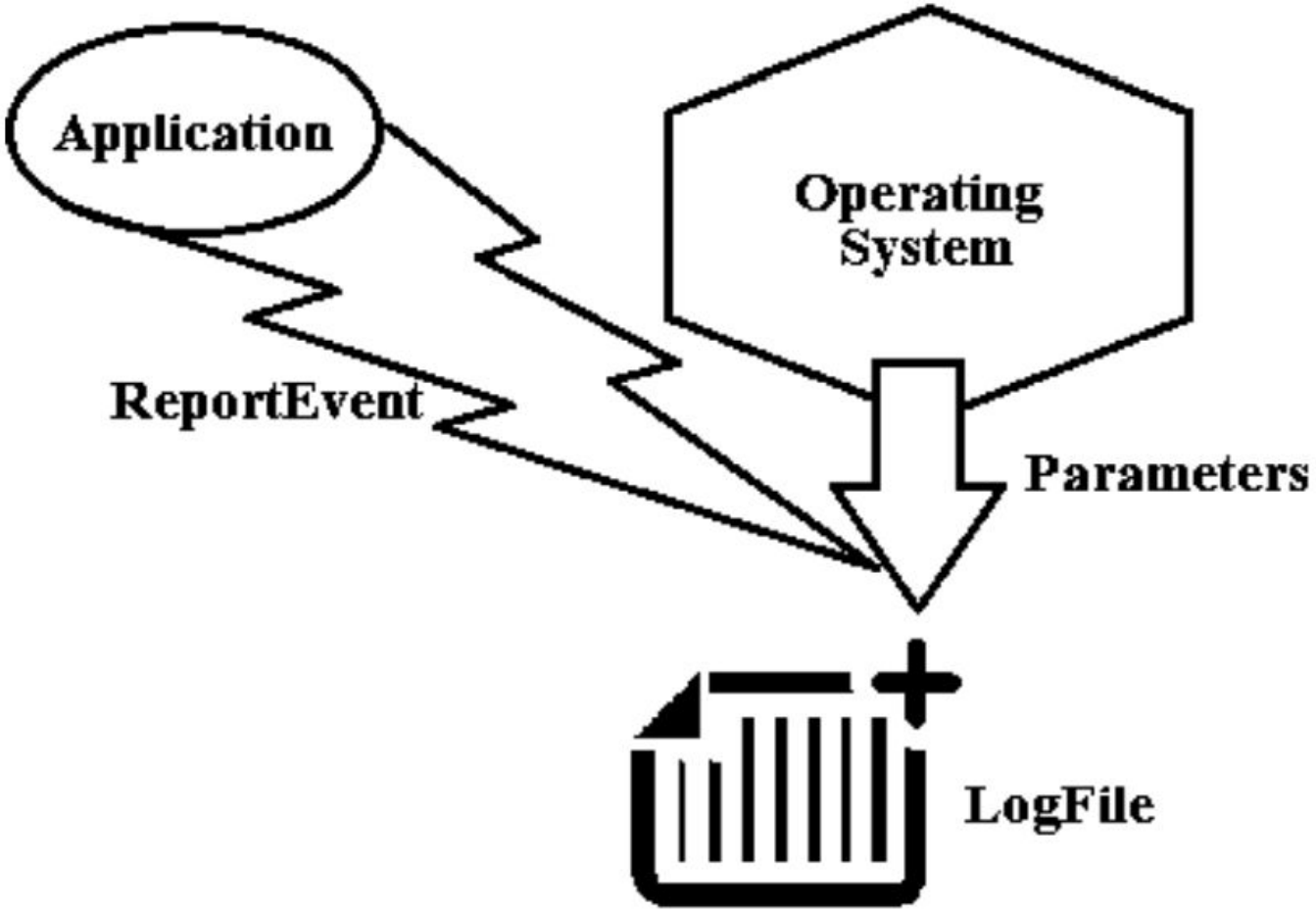
www.forensicswiki.org/wiki/Windows_Event_Log_(EVT)

The Windows XML Event Log (EVTX) format was introduces 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 and 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.


Application
Operating System
ReportEvent
Parameters
LogFile

- 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 with computer source documents	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 intermediatary (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	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.	Imprisonment up to three years, or/and with fine up to ₹200,000

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 Stales 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	The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system. 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.	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

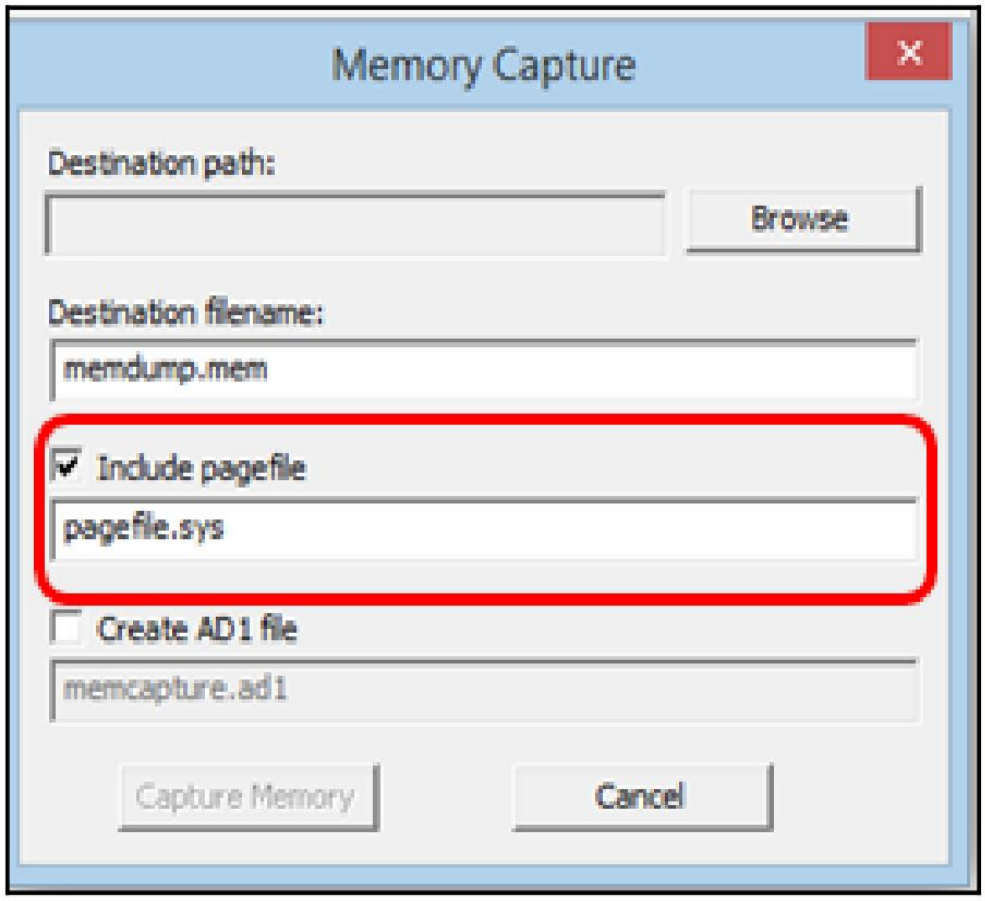
- If the Windows system crashed, it is designed to store information about the system state at the time of the crash for future troubleshooting of the crash after recovering the system. Crashing the system was an old way to dump the memory to the crash dump file.
- Better methods and tools are available 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:

1. 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.
2. 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.
3. Injection: DLLs can be injected into a process by different techniques.

- **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. I
- n 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, 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.