



Prifysgol Cymru

Y Drindod Dewi Sant

University of Wales

Trinity Saint David

Trawsnewid Addysg, Trawsnewid Bywydau
Transforming Education, Transforming Lives

Digital Forensics



Lecture Notes

ACCA7031

Applied Computing - WISA



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Trawsnewid Addysg, Trawsnewid Bywydau
Transforming Education, Transforming Lives

Introduction

Digital Forensics (ACCA7031)

Applied Computing - WISA

Discussion

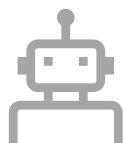
During this discussion, we shall get introduced to this module, discuss the plan, coursework and the tools to be used in this module.

We also discuss the overview of Cybercrime, the principles of Digital Forensics, Digital Evidence and roles and responsibilities of a Forensic Investigator.

In continuation, let us try to understand to the Law Enforcement and the key aspects on Security Vs Privacy.



Introduction



Cybercrime and
Digital Forensics



Digital Evidence and
Law Enforcement



Security Vs Privacy

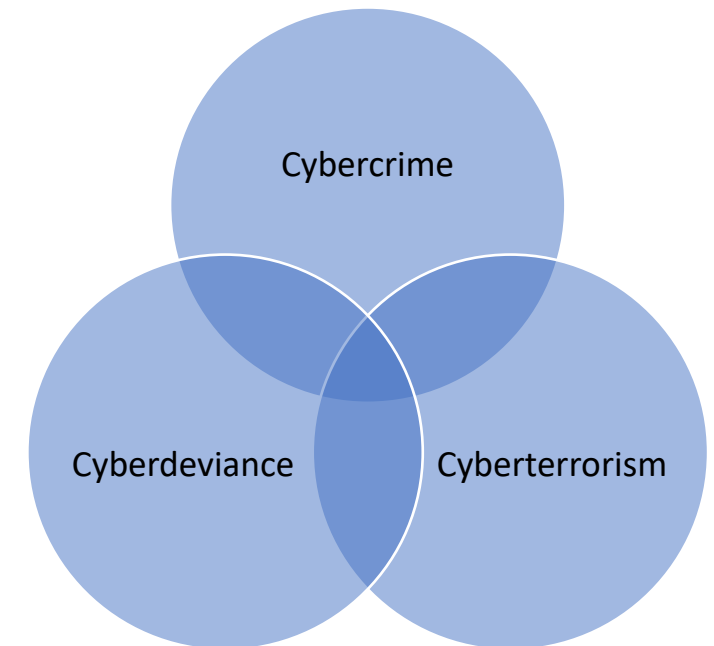


Forensic
Investigator

Cybercrime

To start from a discussion during our other lecture....

- Proliferation of Technology
 - *(Zickuhr, 2011) – Individuals under the age of 20 regularly send texts and prefer that rather than making calls.*
- *Digital Migrants*
- **Technology in Crime:**
 - Communication Medium
 - Target Sensitive Resources
 - Engage in Crime
 - Facilitate the offense
- **Dark Web – via The Onion Router/ TOR Service**
- **Use of Digital Currency**
- **Cyberdeviance**



Forensic Science!!!

Forensic Science is the application of science to the law, meaning the scientific process of gathering and examining information to be used by the criminal justice system (Saferstein, 2010)

There are different fields in Forensic Science. Forensic Art, Nursing, Accounting, Engineering, Firearm, Serology, Document Examination, Digital Forensics, Psychology etc.

Digital Forensics

The application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence after proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possible expert presentation.

(Casey, 2011)

Definition from ISO/IEC 27037

Digital forensics is defined as "the process of identifying, preserving, analyzing, and presenting digital evidence in a manner that is legally acceptable."

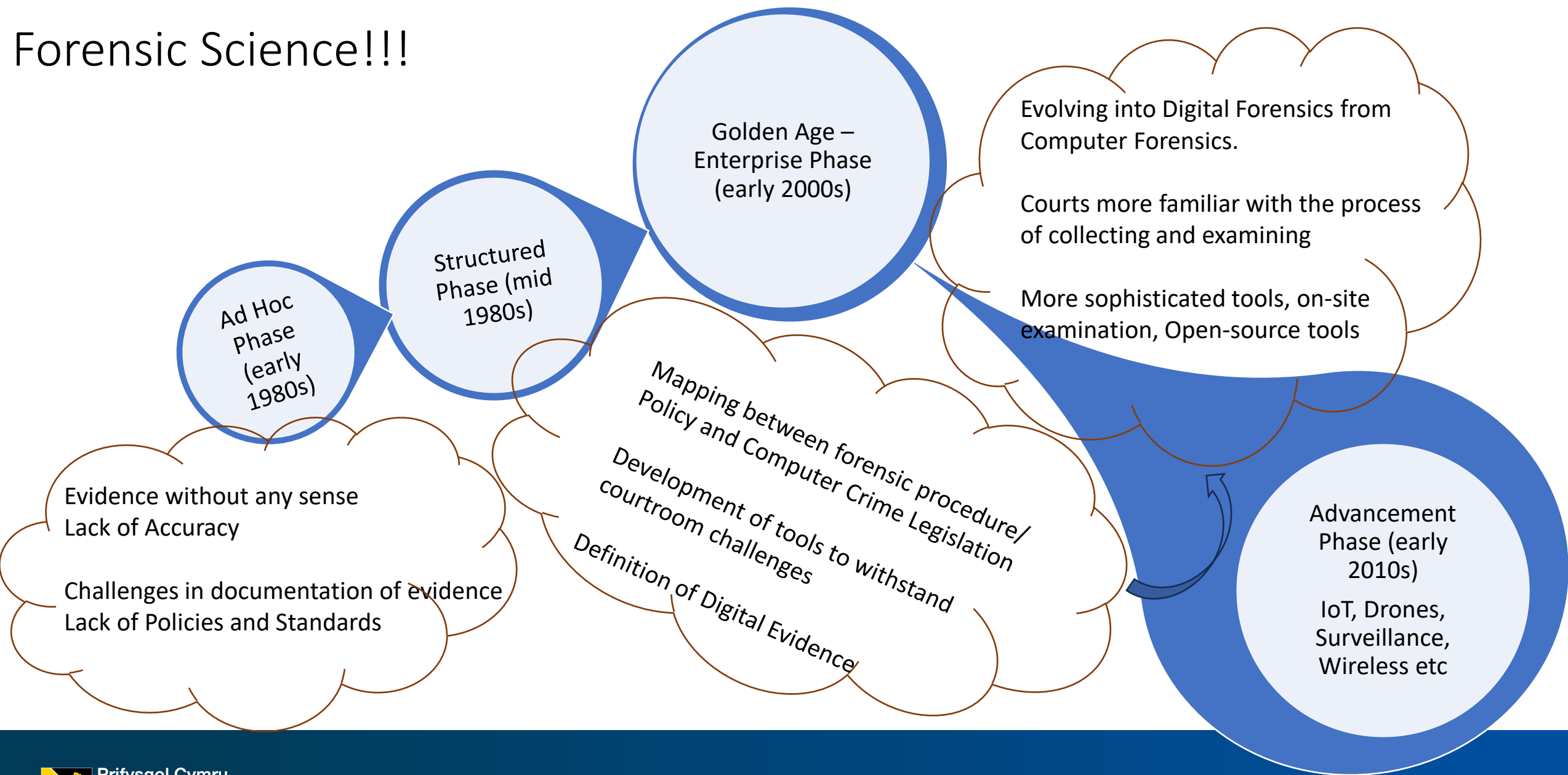
Forensic Science!!!

Computer ? Digital ? Forensic

- ▶ *The National Institute of Standards and Technology (NIST) defines digital forensics as "the application of science to the identification, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data."*
- ▶ *NIST defines computer forensics as "the discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law."*
- ▶ *Are you confused??? Just to back to the past and try to clarify things!!!*
- ▶ **Late 1970's**
 - ▶ **1976 – Council of Europe Conference on Criminology Aspects of Economic Crime – Strabourg, France: Identified several categories of Cyber Crime.** Schjolberg, S. (2004).
 - ▶ **1977 – The Federal Computer Systems Protection Act – USA – not passed**

This Act would make "the use, for fraudulent or other illegal purposes, of any computer owned or operated by the United States, certain financial institutions, and entitles affecting interstate commerce" a federal crime.
 - ▶ **1978 – Florida Computer Crimes Act – based on a scandal**
 - ▶ **1986 – Computer Fraud and Abuse Act – USA**

Forensic Science!!!



Definition of Computer Forensics:

- ✍ Subset of digital forensics focused on crimes across computing devices.

Objectives:

- ✍ Identify, gather, preserve, extract, interpret, document, and present evidence.
- ✍ Ensure evidence admissibility in legal/administrative proceedings.

Scope:

- ✍ Involves networks, computers, digital storage media.

Methodology:

- ✍ Utilizes specific procedures and techniques.

Outcome:

- ✍ Facilitates finding admissible evidence for legal action against perpetrators.



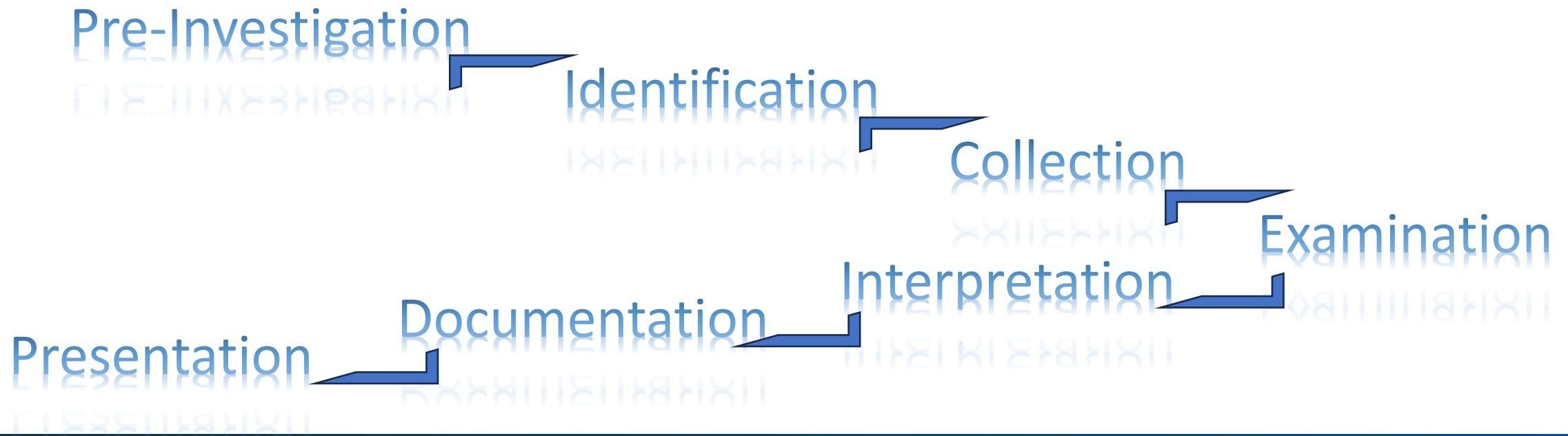
[This Photo](#) by Unknown Author
is licensed under [CC BY-SA](#)

[This Photo](#) by Unknown Author
is licensed under [CC BY-NC-ND](#)

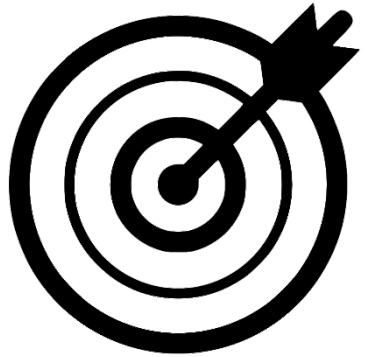
Forensic Science!!!

Digital Forensics

- ▶ Digital forensics refers to the analysis of digital evidence, which includes network forensics (Internet traffic), computer forensics, mobile device forensics (e.g., cell phone), and malware forensics (e.g., viruses). Overall, digital forensics included a whole array of digital devices. (Bossler)
- ▶ Note that, in most cases the development of new technology required new forensic tools. (Bossler)



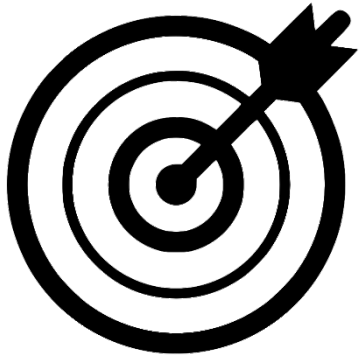
Objectives



[This Photo](#) by Unknown Author is licensed under [CC BY-NC](#)

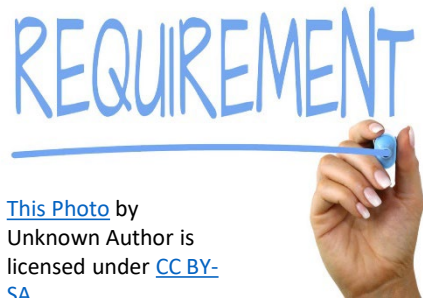
- ✍ Identify, gather, and preserve the **evidence** of a cybercrime
- ✍ Track and prosecute the perpetrators in a **court of law**
- ✍ Interpret, document, and present the evidence such that it is **admissible during prosecution**
- ✍ Estimate the **potential impact of malicious activity** on the victim and assess the intent of the perpetrator
- ✍ Find **vulnerabilities and security loopholes** that help attackers

Objectives



[This Photo](#) by Unknown Author is licensed under [CC BY-NC](#)

- ✍ Understand the **techniques and methods** used by attackers to avert prosecution and overcome them
- ✍ **Recover** deleted files, hidden files, and temporary data that can be used as evidence
- ✍ Perform **incident response** (IR) to prevent further loss of intellectual property, finances, and reputation during an attack
- ✍ **Know the laws** of various regions and areas, as digital crimes are widespread and remote
- ✍ Know the **process of handling multiple platforms, data types, and operating systems**
- ✍ Learn to identify and use the **appropriate tools** for forensic investigations



- ✍ Ensure the **overall integrity and the continued existence** of an organization's computer system and network infrastructure
- ✍ Help the organization **capture important information** if their computer systems or networks are compromised. Forensic evidence also helps **prosecute the perpetrator** of a cybercrime, if caught.
- ✍ **Extract, process, and interpret the actual evidence** so that it proves the attacker's actions and their guilt or innocence in court
- ✍ Efficiently **track down perpetrators/terrorists** from different parts of the world. Terrorists who use the Internet as a communication medium can be tracked down, and their plans can be discovered. IP addresses are vital to finding the geographical location of the terrorists.
- ✍ Save the **organization's money and valuable time**. Many managers allocate a large portion of their IT budget for computer and network security.
- ✍ **Track complex cases** such as email spamming and other nefarious activities, etc.



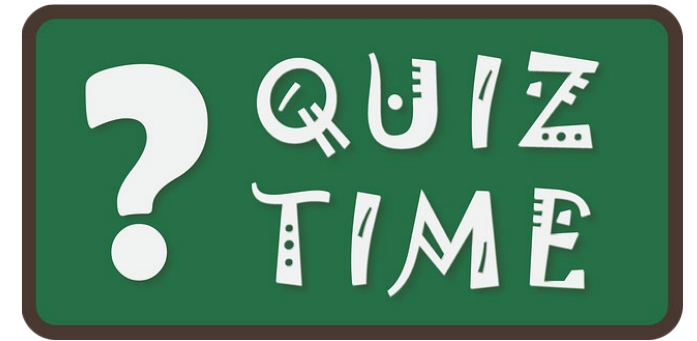
Recall...

Why should Computer Forensics be used?

- A. Ensure network integrity and evidence gathering.
- B. Protect data, compliance, and prevent future incidents.
- C. Combat online crimes, protect reputation, and minimize losses.
- D. Support prosecution of cybercrime perpetrators.

How can computer forensics assist organizations in addressing security and criminal incidents involving computer systems?

- A. Prepare for incidents and secure defenses.
- B. Comply with cyber laws and regulations.
- C. Report breaches and identify response actions.
- D. Address theft, settle disputes, minimize damage, and establish security parameters.





Cybercrime

- You are in a Coffee Shop. You could see a wifi which is password protected.
- You used your knowledge and proficiency to guess the password
 - You didn't use any tools to break in / brute force
 - You just guessed the password (or) googled for a default password and used that
- You successfully connected to the network
- Is that a CRIME?

Cyber-trespass



Cybercrime

- You create an email in the name of your friend/ (or) your Lecturer and send it to just your (close) friends in the class for fun. The email claims that there's a change in the lecture time for this week.
- Is that a CRIME?

Cyber Deception



Discussion Point:

“The cyber deception in this scenario involves the email sender pretending to be a trustworthy entity to gain your trust and prompt you to take certain actions.” –

“If you follow the instructions in the deceptive email, you may unknowingly provide your sensitive information to cybercriminals, who can then use it for identity theft, financial fraud, or other malicious purposes.”

From the above example,

Will you be providing any sensitive information?

Is there any chance of Fraud (Financial, etc)?

Any Damage?

Is it a Crime?

Cybercrime



- You use CMC (Computer Mediated Communication) to form a flash mob without alerting local citizens or law enforcement.

Cyber Violence

- Is that a CRIME?

Three arrested on suspicion of planning flash mob event



Bev Holder

19 May 2023 · 2-min read



Police have made arrests after they received information about a flash mob event (Image: Getty/WEKWEK)

POLICE have arrested three men and put a dispersal order in place across Birmingham city centre after receiving information about an event that was due to take place today (Friday May 19).

West Midlands Police received information that a flash mob event, organised through social

Cybercrime

Rap star 'used Twitter to organise flash mob at suburban Ohio mall food court'

By HANNAH ROBERTS

UPDATED: 07:43, 22 August 2011



Share



View comments 1

Rapper Machine Gun Kelly has been accused of organised a flash mob at a suburban Ohio mall. He is charged with disorderly conduct.

Police say the group gathered Saturday, and mall management asked three people standing on a table near a second-floor railing to step down. Kelly was among the three. When they refused, police were called.

Police say they're no longer in custody. Kelly, real-name Colson Baker, tweeted later that 'today was a statement.'

Cyber Violence



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Trawsnewid Addysg, Trawsnewid Bywydau
Transforming Education, Transforming Lives

Question:

“How much overlap do you see between real-world crimes and cybercrimes? Should we have distinct terms to recognize crime or deviance in online environments, or should all offenses just be classified as crimes, regardless of where and how they occur?” – (Bossler, 2018)

Cybercrime

- ✍ Espionage
- ✍ Theft of Intellectual Property
- ✍ Manipulation of Data
- ✍ Trojans Horse Attack
- ✍ Structured Query Language Attack
- ✍ Brute-force Attack
- ✍ Phishing/Spoofing
- ✍ Privilege Escalation Attacks
- ✍ Denial of Service Attack/ Distributed DoS
- ✍ Cyber Defamation
- ✍ Cyberterrorism
- ✍ Cyberwarfare

✍ (Zickuhr, 2011)

Individuals under the age of 20 regularly send texts and prefer that rather than making calls.

Cybercrime Investigation

Approaches to Cybercrime Investigation:

- ✍ Types of approaches vary based on the nature of the case
- ✍ Collection, analysis, and presentation of data differ accordingly



[This Photo](#) by Unknown Author
is licensed under [CC BY-NC](#)

Types

- ✍ Civil
- ✍ Criminal
- ✍ Administrative

Cybercrime Investigation

Civil

- ✍ Disputes between parties (individuals, companies, or government agencies)
- ✍ Involve violations of contracts
- ✍ Lawsuits result in monetary compensation
- ✍ Usually, poorly documented or unknown chain of custody
- ✍ Evidences Gathering: Mutual Understanding

Criminal

- ✍ Actions harmful to society
- ✍ Law enforcement respond to suspected law violations
- ✍ Verdict may lead to fines, imprisonment, or both
- ✍ A formal investigation is required.
- ✍ Standard of proof needs to be very high
- ✍ Challenges in gathering evidences



[This Photo](#) by Unknown Author
is licensed under [CC BY-NC](#)



[This Photo](#) by Unknown Author
is licensed under [CC BY-NC](#)

Administrative

- ✍ Internal investigations by organizations
- ✍ Aim to ensure compliance with rules and policies
- ✍ Involves inquiries by agency or government
- ✍ Non-criminal, focused on employee misconduct
- ✍ Includes violations like policy breaches, resource misuse, threatening behavior, etc.
- ✍ Disciplinary actions may include demotion, suspension, penalties, etc.
- ✍ Potential positive outcomes include modifications to policies, promotions, etc.

Digital Evidences

- ▶ “Any information of probative value that is stored or transmitted in a binary form” – Whitcomb, 2007
- ▶ Information that is either transferred or stored digitally.
- ▶ Digital Evidence is only admissible if its authenticity can be verified in a court of law.
- ▶ Key Challenges: Different stages of data/ information

Digital Evidences



[This Photo](#) by Unknown Author is licensed under [CC BY-NC](#)

- ✍ Data on digital devices can be categorized into **volatile and non-volatile**.
 - ✍ **Volatile data requires constant power** and is lost upon power interruption.
 - ✍ **Key Volatile Data:** System time, Logged-on user(s), Open files, Network information, Process details, Clipboard contents, Command history, etc.
 - ✍ **Non-volatile data remains intact even without power.**
 - ✍ **Key non- Volatile Data:** Hidden files, Slack space, Swap files, Index.dat files, Unallocated clusters, Unused partitions, Hidden partitions, Registry settings, Event logs
- ✍ Digital Evidences are essential for forensic analysis and investigation.
- ✍ Understanding the types helps in identifying and preserving critical evidence.
- ✍ Understanding volatility aids in data recovery and analysis processes.

Privacy Vs Security



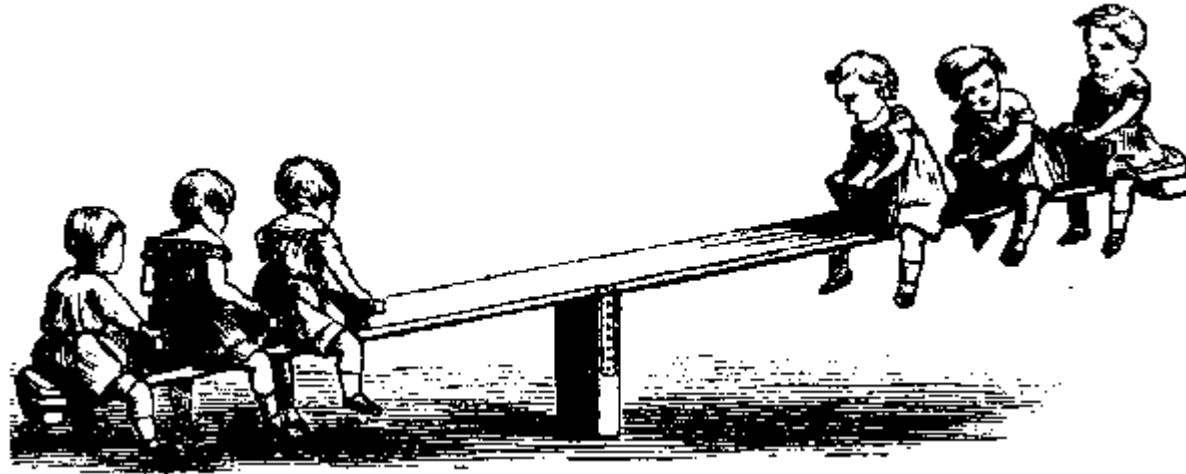
Privacy is the freedom from being observed or disturbed by other people, or the state of not being observed or disturbed in this way. It is the right to keep one's personal matters and relationships secret

(International Association of Privacy Professionals (IAPP))

Information security is the preservation of confidentiality, integrity, and availability of information. It also involves maintaining authenticity, possession, or control of that information

International Organization for Standardization (ISO)

Privacy



[This Photo](#) by Unknown Author is licensed under [CC BY-SA](#)

Security

Discussion Point:

“KARMA POLICE” program was a surveillance initiative conducted by GCHQ that sparked controversy due to its extensive data collection and privacy implications. It contributed to a broader global debate on the balance between national security and individual privacy in the digital age.

- What is the concept of privacy?
- Why it is important in the context of digital surveillance programs like the above?
- How do you define the boundaries between individual privacy and government surveillance in today’s scenario?
- What do you think as an impact of mass surveillance on individual’s freedom of expression?
- How can technology be used to enhance the security while minimizing the impact on individual privacy?

Discussion Point

- *Victor Collins Case – Smart Home Devices – Alexa as an evidence*

Summary:

Victor Collins was found dead in a hot tub at a friend's residence in Bentonville, Arkansas, in November 2015. The friend, James Bates, was the owner of the residence and was present at the time of the incident. Bates initially reported finding Collins' body the next morning and called 911

☐ *Case Overview*

☐ *Role of Digital Forensics*

☐ *Privacy and Legal Issues*

☐ *Reflection*

Summary

- **Cybercrime**
- **Types of Crime**
 - Economic Crimes – CMC, ID Theft, Email Scams, Stolen Data Market
 - Intellectual Property Theft
 - Sexual Crimes – Pornography, Child Pornography, Sexual Exploitation and Sex Crimes
 - Cyberbullying, Online Harassment, Cyberstalking
 - Online Extremism, Cyber Terror, Cyberwarfare
- **Privacy Vs Security**
- **Digital Forensics**

History

Digital Forensics (ACCA7031)

Applied Computing - WISA

Earlier, we started with an introduction to this module and started our lecture with an overview of Cybercrime, the principles of Digital Forensics and continued discussing about Digital Evidence. We touch based the Law Enforcement and the key aspects on Security Vs Privacy.

In this part we shall discuss about the History of Digital Forensics and its attributes. We shall try to understand the importance of Incident Response. We shall move forward and discuss about the principles of Digital Forensics, its process, different roles and finally getting to understand the technology's role in the crime and Legal Compliances.



*DIGITAL
EVIDENCES*



*ROLES AND
RESPONSIBILITIES*



*INCIDENT
RESPONSE*



*CHALLENGES
FACED*



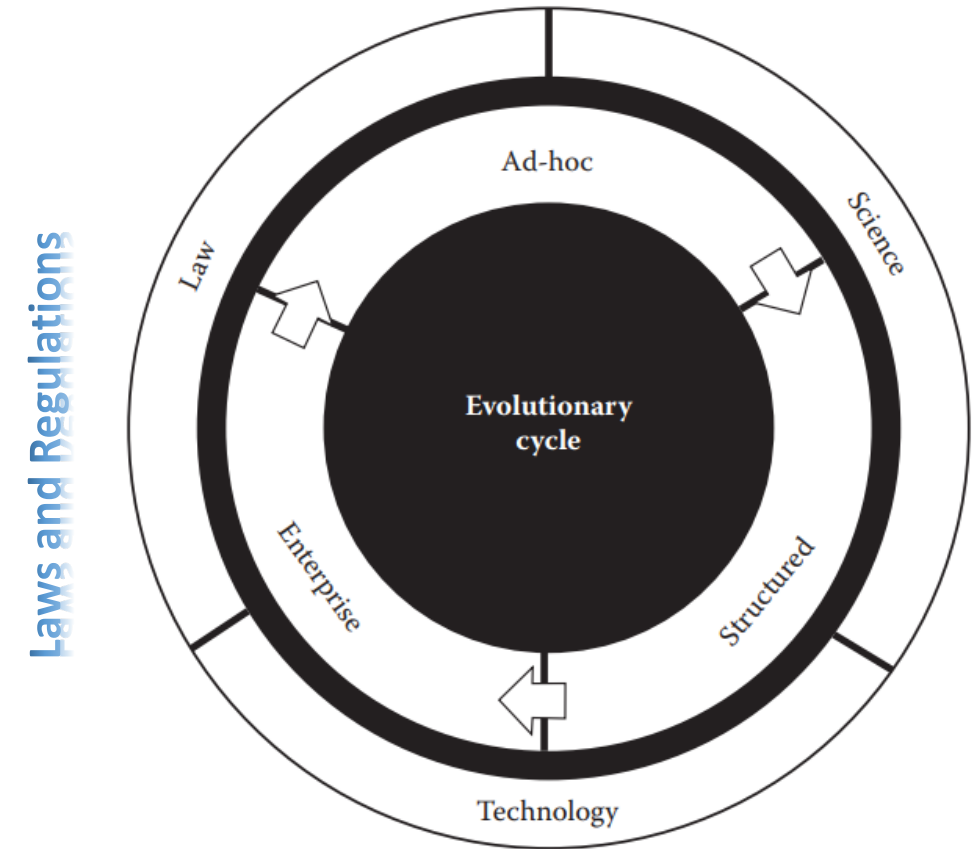
*LEGAL
COMPLIANCE*

Discussion

History

- 1960 – 1980
 - Computers were used for data processing operations
 - Focus on efficiency and accuracy of the functionality
 - **Data Recovery and Backup**
- 1980-1995
 - Personal Computers
 - **Development of specific Software's for digital forensics activities**
 - Training to gather evidence from Computer Systems
- 1995 - 2005
 - **Principles, Methodologies and Techniques to standardize computer forensics**
 - Computer Forensics into Digital Forensics
 - DF was recognized as a Science
- 2005 - 2015
 - Academic and Professional Curriculum
 - Major Evolution in DF Tools
 - **Tools focusing on Incident Response, Electronic Discovery, Information Governance**

Technological Evidence & Legal Precedence

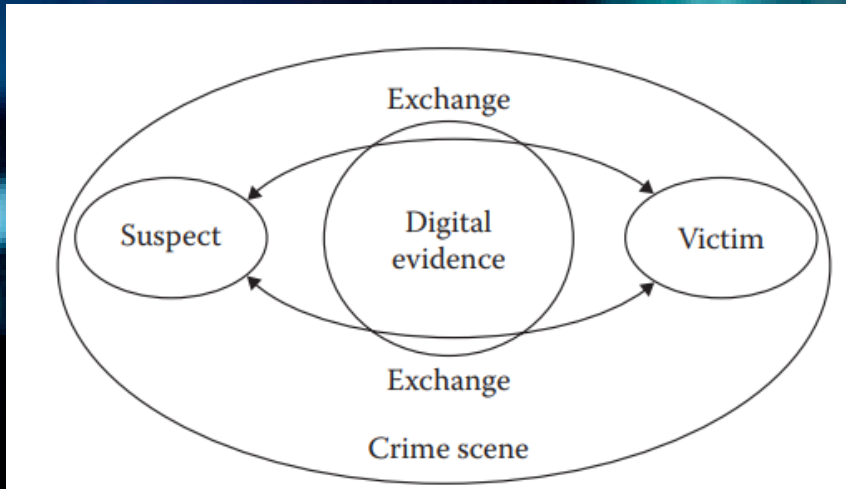


Effective Tools and Processes, Automation



Principles of Digital Forensics

- Digital forensics is the **application of science to law**, and, subsequently, must **follow the scientific principles, methodologies, and technique** required for **admissibility** in a court of law.
- Conducting a forensic investigation is to **establish factual conclusions based on credible evidence**.



Discussion Point:

Locard's Exchange Principle

What is this Principle?

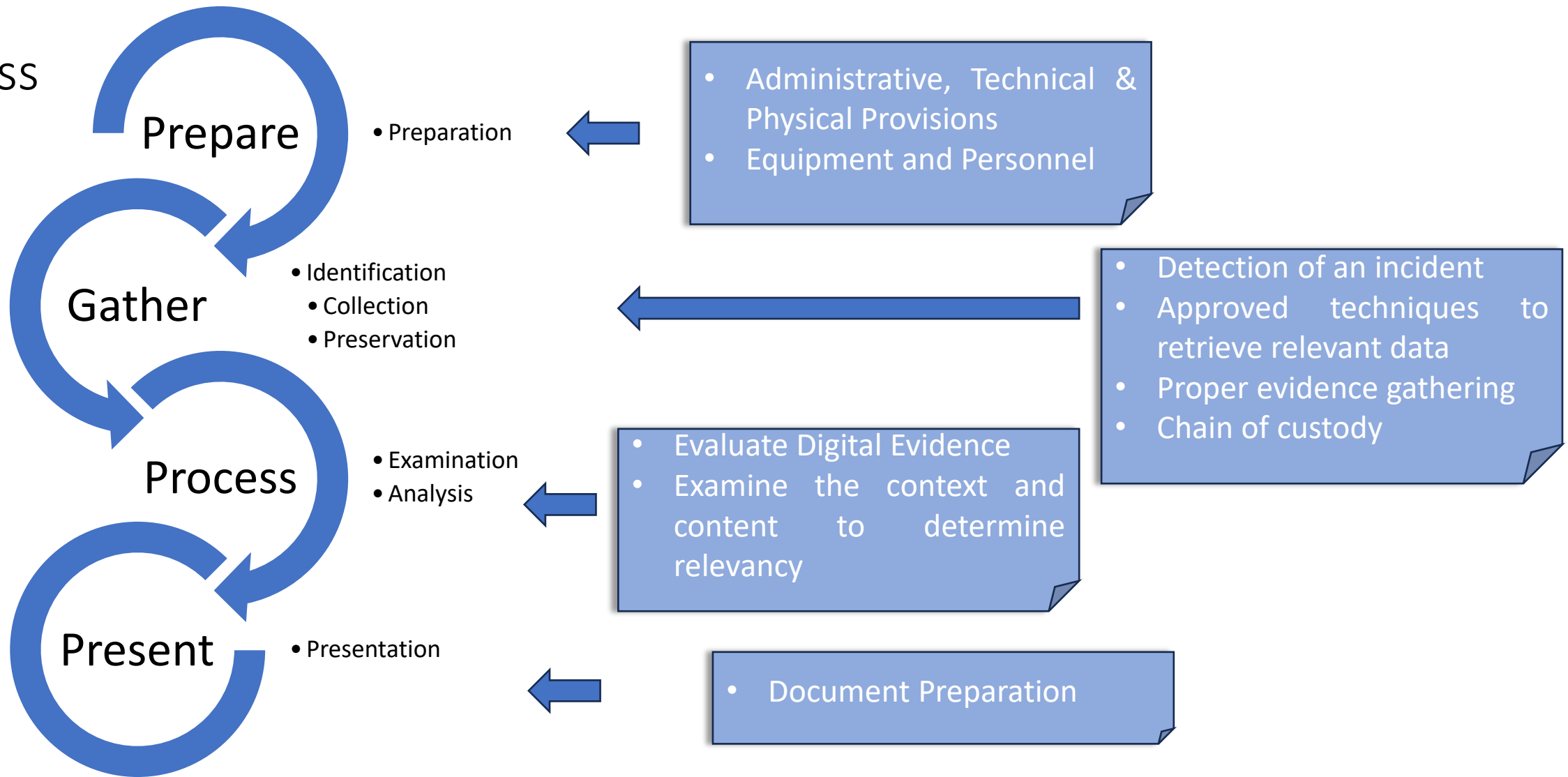
How do you think it will be helpful for your DF Investigations?

What are the limitations and challenges?

Principles of Digital Forensics

- Digital forensics is the **application of science to law**, and, subsequently, must **follow the scientific principles, methodologies, and technique required for admissibility** in a court of law.
- Conducting a forensic investigation is to **establish factual conclusions based on credible evidence**.
- It is critical that “evidence” is handling in a way that will not raise questions when presented in a court of law.
- Evidence exists in a logical state that is intangible in comparison to physical evidence.
 - ✓ Evidence Exchange
 - ✓ Forensic Soundness (*Minimally Handle the Original, Account for Any Change, Comply with the Rules of Evidence, Avoid Exceeding One’s Knowledge*)
 - ✓ Authenticity and Integrity (*Chain of Custody*)

Process



Process

- Preparation

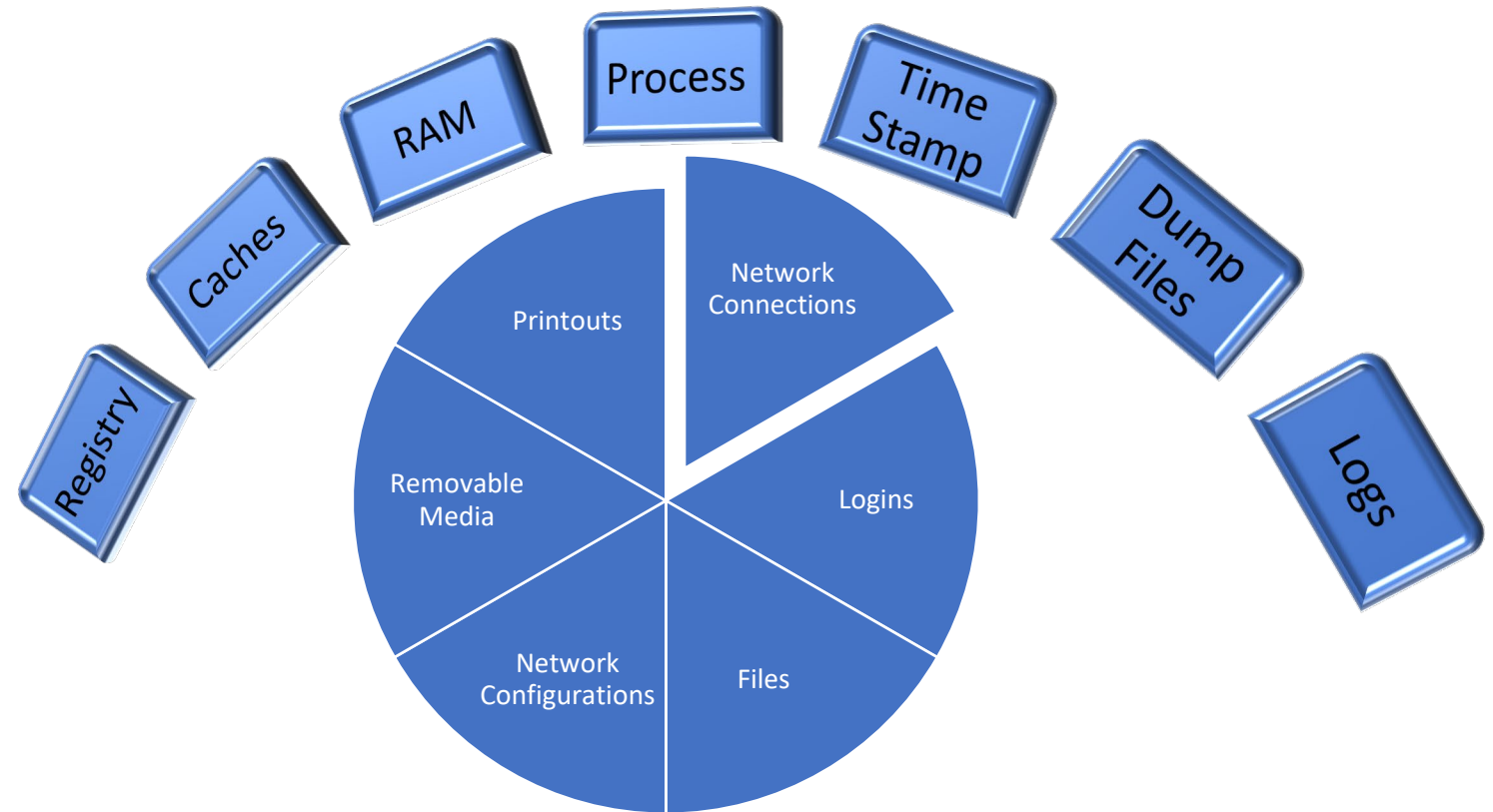
- Process and Procedure (Framework, SOP)
- Education, Training and Awareness
- Technology and Toolsets

- Gathering

- Electronically Stored Evidence
- Evidence Handling Techniques
- Securing the Scene
- Documenting the Scene
- Search and Seizure
- Collection and Preservation

Always remember

“maintaining the authenticity and integrity of evidence is essential for guaranteeing a forensically sound investigation”



Process

Always remember

“maintaining the authenticity and integrity of evidence is essential for guaranteeing a forensically sound investigation”

■ Processing

- Always in a controlled environment
- Follow the least privilege access methodology
- Look for encrypted/ deleted files

■ Presentation

- Content should be clear and concise to accurately demonstrate a chronology of events
- Use of jargon, slang, and technical terminology should be limited or avoided.
- Where used, a glossary should be included to define terms in a layperson’s language.
- Where acronyms and abbreviations are used, they must be written out in full expression on the first use.
- Because final reports are written after the fact, meaning after an investigation, content should be communicated in the past tense, but can change tense where conclusions or recommendations are being made.
- Format a final report not only for distribution within the organization, but also with the mindset that it may be used as testimony in a court of law.

Digital Evidences



[This Photo](#) by Unknown Author is licensed under [CC BY-NC](#)



Last week review...

[This Photo](#) by Unknown Author is licensed under [CC BY-NC](#)

- ✍ Data on digital devices can be categorized into **volatile and non-volatile**.
 - ✍ **Volatile data requires constant power** and is lost upon power interruption.
 - ✍ **Key Volatile Data:** System time, Logged-on user(s), Open files, Network information, Process details, Clipboard contents, Command history, etc.
 - ✍ **Non-volatile data remains intact even without power.**
 - ✍ **Key non- Volatile Data:** Hidden files, Slack space, Swap files, Index.dat files, Unallocated clusters, Unused partitions, Hidden partitions, Registry settings, Event logs
- ✍ Digital Evidences are essential for forensic analysis and investigation.
- ✍ Understanding the types helps in identifying and preserving critical evidence.
- ✍ Understanding volatility aids in data recovery and analysis processes.

Digital Evidences

- ✍ Investigators can collect **digital evidence from multiple sources**.
- ✍ Apart from stand-alone computing systems, digital evidence can be acquired from **storage, peripheral and network and handheld devices** that are found on the crime scene.
- ✍ Potential sources of evidence should be acquired in a **forensically sound manner to preserve their integrity**.
- ✍ Investigators should use **valid and reliable forensic tools and techniques** while acquiring digital evidence to **prevent data alterations**.



This Photo by Unknown Author is licensed under [CC BY-NC](#)



Tra
ans

Evidences

- ✍ Hard Drive/ Thumb Drive/ Memory Card/ Smart Card
- ✍ Dongle/ Biometric Scanner/ Answering Machine
- ✍ Digital Camera/Surveillance cameras
- ✍ Random Access Memory (RAM) and Volatile storage
- ✍ Handheld Devices
- ✍ Local Area Network (LAN) Card/ Network Interface Card (NIC)
- ✍ Routers, Modem, Hubs, and Switches/ Network Cables and Connectors
- ✍ Server/ Computer system Printer/ Scanner/ Telephones / Copiers/
- ✍ Internet of Things and wearables
- ✍ Removable Storage Device and Media
- ✍ Credit Card Skimmers
- ✍ Digital Watches
- ✍ Facsimile (Fax) Machines
- ✍ Global Positioning Systems (GPS)

Rules Evidences

✍ **Understandable:**

- ✍ clear and comprehensible manner
- ✍ clear explanation of facts
- ✍ expert opinion.

✍ **Admissible:**

- ✍ evidence in an admissible manner,
- ✍ should be relevant to the case,
- ✍ act in support of the client presenting it,
- ✍ well-communicated and non-prejudiced

✍ **Authentic:**

- ✍ ownership needs to be clarified.
 - ✍ source of the evidence and its relevance to the case.
 - ✍ furnish details such as the author of the evidence or path of transmission.

Rules Evidences

✍ **Reliable:**

- ✍ extract and handle the evidence
- ✍ maintain a record of the tasks performed during the process
- ✍ investigations must be conducted only on copies of the evidence

✍ **Complete:**

- ✍ either prove or disprove the consensual fact in the litigation.
- ✍ If the evidence fails to do so, the court is liable to dismiss the case, citing a lack of integral evidence.

Discussion Point:

Read “The Association of Chief Police Officers (ACPO) Principles of Digital Evidence”.

10 Minutes: Read the principles of digital evidence – 4 Principles

8 Minutes: Each highlight on 1 Principle with a simple use-case example. (2 Minutes for each Principle)

Forensic Readiness

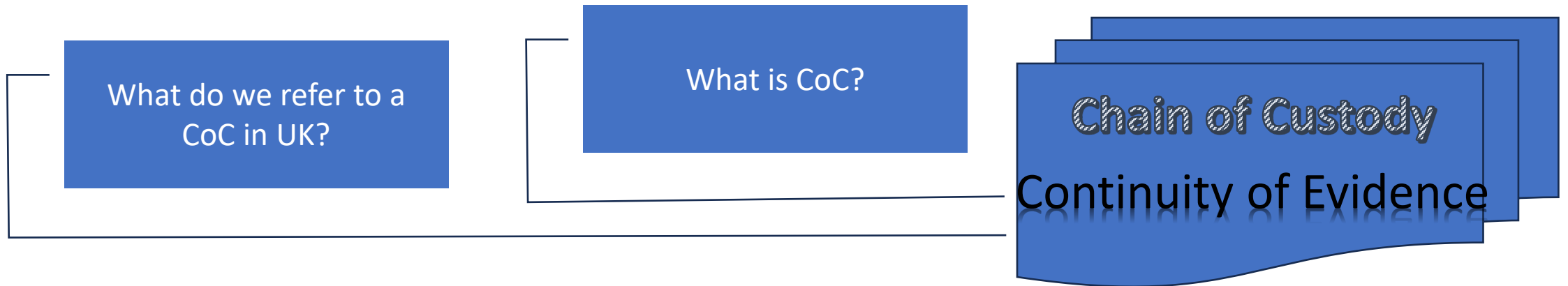
- ✍ **Need:** Optimally use digital evidence.
- ✍ **Effectiveness:** limited time and minimal investigation costs.
- ✍ **Include:** Technical and Non-Technical actions
- ✍ **Establish:** Specific incident response procedures
- ✍ **Employ:** Designated Trained Personnel

“State of readiness, along with an enforceable security policy, helps the organization mitigate the risk of insider threat from employees and prepare pre-emptive measures”

A forensically trained and well-prepared incident response team ensures an appropriate reaction against any mishap and handles the evidence in compliance with the relevant legal procedures for its potential use in a court of law.

Forensic Readiness

- ✍ Identify the potential evidence required for an incident
- ✍ Determine the sources of evidence
- ✍ Define a policy that determines the pathway to legally extract electronic evidence with minimal disruption
- ✍ Establish a policy for securely handling and storing the collected evidence
- ✍ Identify if the incident requires full or formal investigation
- ✍ Create a process for documenting the procedure
- ✍ Establish a legal advisory board to guide the investigation process
- ✍ Keep an incident response team ready to review the incident and preserve the evidence



Roles and Responsibilities



TECHNICIAN



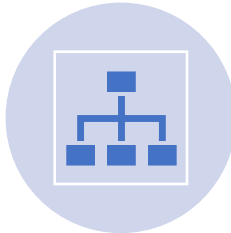
EXAMINER/ANALYST



INVESTIGATOR



TEAM LEAD



MANAGER/
DIRECTOR

Analytical Skills

Leadership

Strategic Mindset

Time Management

Critical Thinking

Project Management

Communication Skills

Interrogation

Conflict Resolution

Technical Writing

Interpersonal Skills

Resource Management

Roles and Responsibilities

- ✍ Evaluates the damages of a security breach
- ✍ Identifies and recovers data required for investigation
- ✍ Extracts the evidence in a forensically sound manner
- ✍ Ensures appropriate handling of the evidence
- ✍ Acts as a guide to the investigation team
- ✍ Creates reports and documents about the investigation for presenting in a court of law
- ✍ Reconstructs the damaged storage devices and uncovers the information hidden on the computer
- ✍ Updates the organization about various methods of attack and data recovery techniques, and maintains a regularly updated record of them (by determining and using the relevant documentation method)
- ✍ Addresses the issue in a court of law and attempts to win the case by testifying in court

Forensic investigators should be familiar with the current Linux, Macintosh, and Windows platforms

Investigation - Attributes

Considerations

- Consistency with all legal systems
- Allowance for the use of a common language
- Durability
- Ability to cross international boundaries
- Ability to instill confidence in the integrity of evidence
- Applicability to all forensic evidence
- Applicability at every level, including that of individual, agency, and country

Investigation - Attributes

Standardized International Principles

- Upon seizing digital evidence, actions taken should not change that evidence.
- When it is necessary for a person to access original digital evidence, that person must be forensically competent.
- All activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved, and available for review.
- An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession.
- Any agency that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for compliance with these principles

Investigation - Attributes

G8 Subgroup:

Principles On Transborder Access to Stored Computer Data— Data Principles on Accessing Data Stored in a Foreign State

- Preservation of stored data in a computer system
- Expedited mutual legal assistance
- Transborder access to stored data not requiring legal assistance
 - a State need not obtain authorization from another State
 - Accessing publicly available (open source) data, regardless of where the data is geographically located
 - Accessing, searching, copying, or seizing data stored in a computer system located in another State, if acting in accordance with the lawful and voluntary consent of a person who has the lawful authority to disclose to it that data.
 - The searching State should consider notifying the searched State, if such notification is permitted by national law and the data reveals a violation of criminal law or otherwise appears to be of interest to the searched State

Investigation - Attributes

According to SWGDE:

The standards and principles are

- Forensic Organisations must establish an effective quality system. (Standard Operating Procedures – SOP)
 - All agencies that seize and/or examine digital evidence must **maintain an appropriate SOP document**.
 - All elements of an agency's policies and procedures concerning digital evidence must be **clearly set forth in this SOP document**, which must be issued under the agency's management authority.
 - Agency management must **review the SOPs on an annual basis** to ensure their continued suitability and effectiveness.
 - Procedures used must be generally accepted in the field or supported by data gathered and **recorded in a scientific manner**.
 - The agency must **maintain written copies of appropriate technical procedures**.
 - The agency must **use hardware and software that is appropriate and effective** for the seizure or examination procedure.
 - All activity relating to the seizure, storage, examination, or transfer of digital evidence must be **recorded in writing and be available for review and testimony**.
 - Any action that has the potential to alter, damage, or destroy any aspect of original evidence must be **performed by qualified persons in a forensically sound manner**.

Investigation - Attributes

According to SWGDE:

The standards and principles are

- Forensic Organisations must establish an effective quality system. (Standard Operating Procedures – SOP)
 - All agencies that seize and/or examine digital evidence must **maintain an appropriate SOP document**.
 - All elements of an agency's policies and procedures concerning digital evidence must be **clearly set forth in this SOP document**, which must be issued under the agency's management authority.
 - Agency management must **review the SOPs on an annual basis** to ensure their continued suitability and effectiveness.
 - Procedures used must be generally accepted in the field or supported by data gathered and **recorded in a scientific manner**.
 - The agency must **maintain written copies of appropriate technical procedures**.
 - The agency must **use hardware and software that is appropriate and effective** for the seizure or examination procedure.
 - All activity relating to the seizure, storage, examination, or transfer of digital evidence must be **recorded in writing and be available for review and testimony**.
 - Any action that has the potential to alter, damage, or destroy any aspect of original evidence must be **performed by qualified persons in a forensically sound manner**.

Incident Response

- ✍ Process of **responding to incidents** that may have occurred due to a security breach or other incidents that potentially compromise the system or network.
- ✍ Aims to **find the incident** when it occurred, its impact, and cause and handle it such that the damage is minimized, and the recovery time and costs are reduced.
- ✍ Accomplish:
 - ✍ Develop and implement a **strong security policy**
 - ✍ Effectively **monitor and analyze** the systems and network traffic
 - ✍ Ensure the usage **operational logs and logging** mechanisms
 - ✍ Handle the incidents such that the **damage is minimized**, and the **recovery time and costs** are reduced
 - ✍ Map the pathway for extracting evidence in a **legally sound and acceptable** manner
 - ✍ Define the **role of an incident response professional**, such as identifying how a breach occurred, how to locate the method of the breach, and how to mitigate the breach

Incident Response in DF

✍ Digital (Computer) Forensics:

- ✍ The legal process of collecting, analyzing, and presenting evidence in court to prosecute perpetrators, **commonly integrated into incident response plans for tracking and justice**

✍ Incident Response Process:

- ✍ Prepare for incidents in advance to ensure the integrity and continuity of network infrastructure
- ✍ Identify and gather evidence of cybercrimes in a forensically sound manner
- ✍ Determine the exact cause, nature, and impact of the incident
- ✍ Generate a timeline for the incident that helps correlate different incidents
- ✍ Conduct a forensic analysis of the affected system that helps determine the nature of the incident and its impact
- ✍ Identify and track the perpetrators of the crime or incident
- ✍ Extract, process, and interpret the factual evidence so that it proves the attacker's actions in the court

Incident Response in CF

✍ **Digital (Computer) Forensics:**

- ✍ The legal process of collecting, analyzing, and presenting evidence in court to prosecute perpetrators, **commonly integrated into incident response plans for tracking and justice**

✍ Incident Response Process:

- ✍ Offer ample protection to data resources and ensure regulatory compliance
- ✍ Protect organizations from similar incidents in the future
- ✍ Counteract online crimes such as abuse, bullying, and reputation damage
- ✍ Minimize the tangible and intangible losses to an organization or an individual
- ✍ Support the prosecution of the perpetrator of an incident
- ✍ Save organizations' money and time by conducting a damage assessment of the victimized network
- ✍ Save organizations from legal liabilities and lawsuits

Incident Response

Scenario:

The security team has detected an unauthorized user attempting to access the organization's network. This user has successfully bypassed several layers of security and gained access to a critical server.

Discuss the action plan for this scenario!!!



Digital forensics serves as the mechanism for understanding the technical aspects of the incident, potentially identifying the root cause, and discovering unidentified access or other malicious activity.

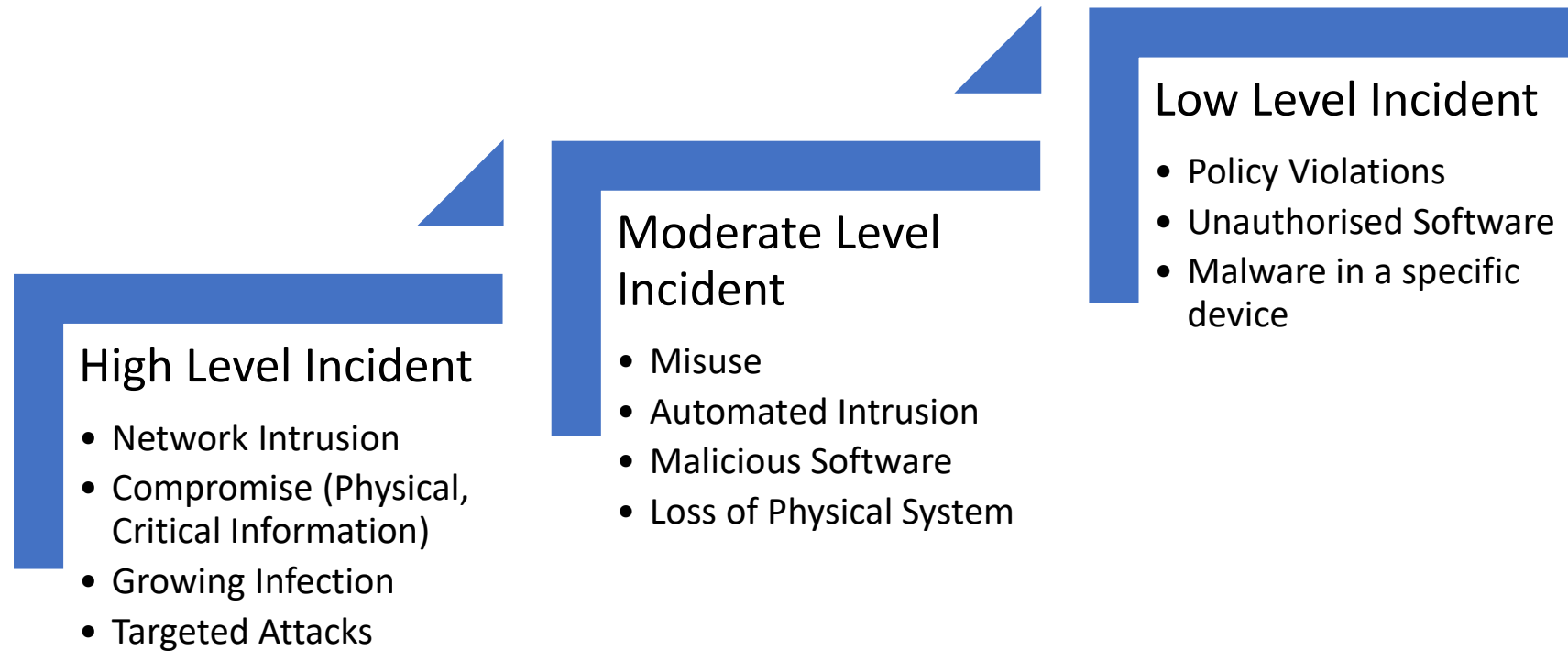
Incident Response

Computer Security Incident Response Team (CSIRT)

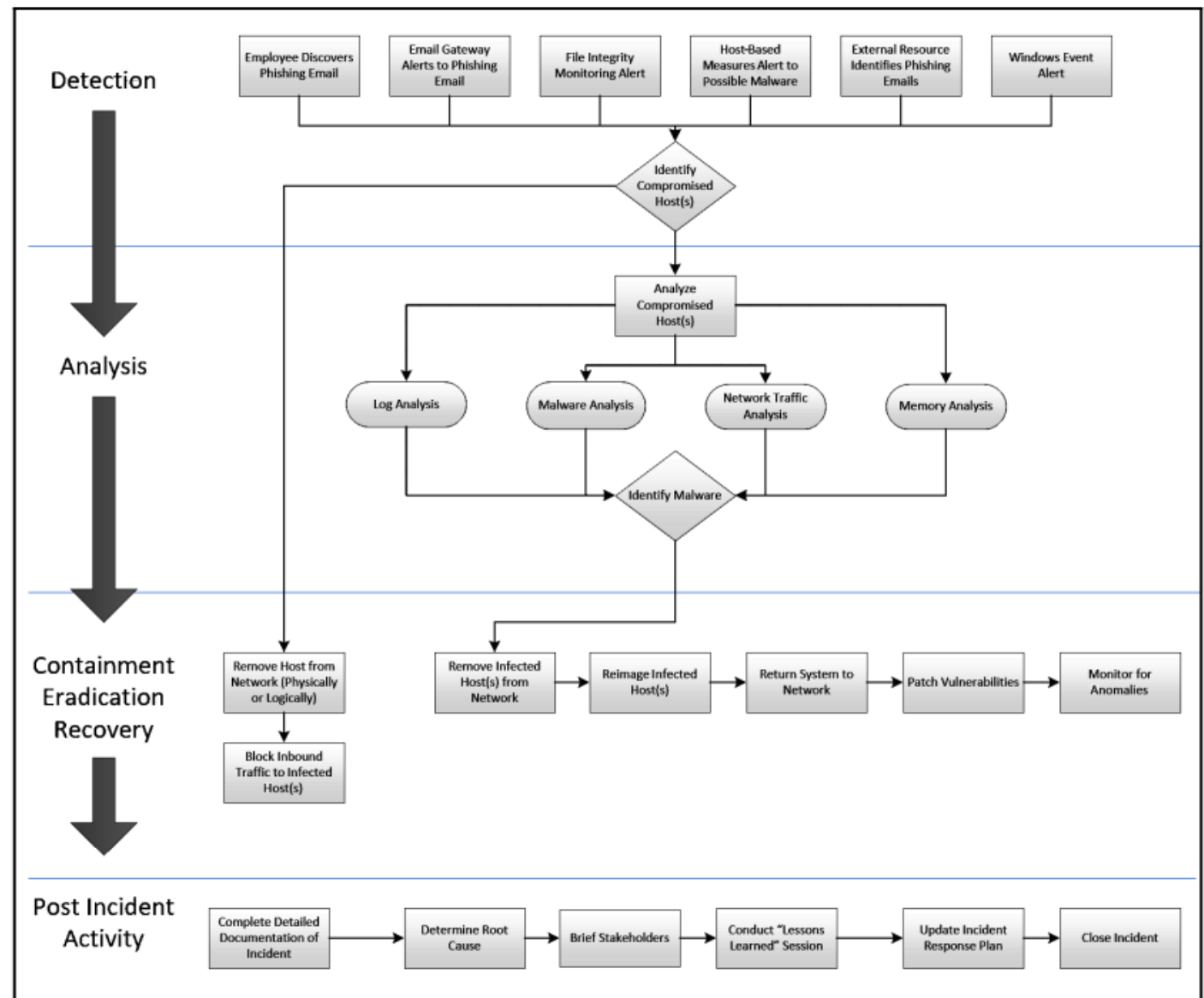
Roles

- INCIDENT RESPONSE COORDINATOR
- SENIOR ANALYST(S)
- CSIRT ANALYST
- SOC ANALYST
- SECURITY ENGINEER
- NETWORK ARCHITECT
- NETWORK ADMINISTRATORS
- APPLICATION SUPPORT
- HELP DESK
- LEGAL SUPPORT
- CORPORATE SECURITY

Incident Response



Incident Response



Challenges

✍ General Challenges

- ✍ Speed
- ✍ Anonymity
- ✍ Volatile nature of evidence
- ✍ Evidence Size and Complexity
- ✍ Anti-Digital Forensics (ADF)
- ✍ Global origin of crimes and difference in laws
- ✍ Limited legal understanding

Challenges

✍ Legal Challenges

✍ Fragility of Digital Evidence:

- ✍ Susceptibility to changes during investigation process.
- ✍ Mishandling can render evidence inadmissible in court.
- ✍ Handling and safeguarding are challenging due to volatility.

✍ Preservation Challenges:

- ✍ Intruders can alter system data.
- ✍ Importance of gathering system data promptly.

✍ Circumstantial Nature of Digital Evidence:

- ✍ Difficulty in tracing system activity.
- ✍ Evidence may be circumstantial, impacting investigation.

✍ Remote Nature of Cybercrimes:

- ✍ Attackers can operate remotely across borders.
- ✍ Difficulty in evidence collection and prosecution.

Challenges

- ✍ Jurisdictional Differences:
 - ✍ Legal systems vary across jurisdictions.
 - ✍ Different legal processes impact prosecution efforts.
- ✍ Compliance with Regional Rules:
 - ✍ Need to understand rules of investigation in relevant regions.
 - ✍ Strict compliance required for effective prosecution.
- ✍ Technological Advancements:
 - ✍ Rapid changes pose challenges for investigators.
 - ✍ Importance of staying updated with technological advancements.
- ✍ Training and Adaptation:
 - ✍ Need for investigators to adapt to changing technologies.
 - ✍ Challenges in training investigators to handle technological changes.

Challenges

✍ Privacy Challenges

✍ Obtaining Warrants:

- ✍ Investigators need warrants to search victim or attacker systems.
- ✍ Warrants must specify devices to be investigated.

✍ Compliance with Fourth Amendment:

- ✍ Avoid charges of unlawful search and seizure.
- ✍ Compliance with Fourth Amendment's restrictions on searches.

✍ Fourth Amendment Guidelines:

- ✍ Prohibits search or seizure without a warrant.
- ✍ Protects areas or things with a reasonable expectation of privacy.

Challenges

✍ Privacy Challenges

✍ Private Intrusions:

- ✍ Non-governmental intrusions aren't governed by the Fourth Amendment.

✍ Preserving Anonymity:

- ✍ Important when dealing with evidence related to internet usage.
- ✍ Protects identities of other users connected to the target system.

✍ Permission for Data Publication:

- ✍ Investigators should obtain permission before publicizing data.
- ✍ Actions should not raise privacy concerns for system owner.

Technology: Crime and Law

- Object of Crime
- Subject of Crime
- Tool of Crime
- Symbol of Crime

- Civil Law
- Criminal Law
- Tort Law
- Private Law
- Public Law

United Kingdom (UK) Computer Misuse Act

- 1990
- Unauthorized access to computer material
- Unauthorized access with intent to commit or facilitate commission of further offences
- Unauthorized acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.

Payment Card Industry: Data Security Standard (PCI-DSS):

- 2008 (revised frequently)
- Cover both technical and operational system components included in or connected to cardholder data (i.e., credit cards).

Sarbanes-Oxley Act (SOX):

- 2002
- this legislation is mandatory for all organizations as regulation of financial practice and corporate governance

Note that, Computers and networks can be tools used to commit crimes. Many states have added specific language to criminal codes to define crimes involving computers

Technology: Crime and Law

- Object of Crime
- Subject of Crime
- Tool of Crime
- Symbol of Crime
- Civil Law
- Criminal Law
- Tort Law
- Private Law
- Public Law

Health Insurance Portability and Accountability Act (HIPAA):

- 1996
- This mandates industry-wide standards for the protection and confidential handling of protected health information to reduce fraud and abuse.

General Data Protection Regulation (GDPR):

- 2016
- This addresses the unified protection of personal data outside of the European Union (EU) with the primary objectives to
 - give control back to citizens and residents over their personal information,
 - simplify the regulatory environment for businesses to operate internationally.

European Union (EU) ePrivacy Act

- (Directive 2002/68/EC)
- this 2002 act defines rules to ensure the security in the processing of personal data, the notification of personal data breaches, the confidentiality of communications, and bans unsolicited communications where the user has not given consent.

Discussion Point:

“There are different laws – that support any forensic investigator: However, a few challenges as well.” With the discussions so far, could you form a Team and explore any other laws (focused on UK/France) that focuses on activities by public bodies including local government and law enforcement agencies?

5 Minutes Time to do a quick search and answer:

**Yes – If yes, which Act?
or NO**

Regulation of Investigatory Powers Act 2000 (RIPA):

- Enacted to regulate **implicit surveillance, interceptions, and undercover operations.**
- Governs activities by public bodies including local government and law enforcement agencies.

Scope of RIPA:

- Covers video surveillance and interceptions of private communications (emails, phone calls, etc.).
- Allows for the use of undercover agents for authorized governmental purposes.

Legal Framework:

- Actions breaching individual privacy are illegal if conducted by private individuals.
- Can be lawful if carried out for authorized governmental purposes, such as crime detection.

Authority and Oversight:

- Provides legal authority for surveillance activities by public bodies.
- Requires adherence to specified procedures and safeguards to protect privacy rights.

Discussion Point:

“There are different laws – that support any forensic investigator: However, a few challenges as well.” With the discussions so far, could you form a Team and explore any other laws (focused on UK/France) that focuses on activities by public bodies including local government and law enforcement agencies?

RIPA 2000!!!

- Briefly understand RIPA’s Scope, any recent amendments, Practical Applications and reflect on Compliance and Best Practices. – Submit your reflection in Moodle – Group Discussion Forum

Technology: Crime and Law

- Object of Crime
- Subject of Crime
- Tool of Crime
- Symbol of Crime

- Civil Law
- Criminal Law
- Tort Law
- Private Law
- Public Law

Professional conduct

- ⌚ Determines your credibility
- ⌚ Includes ethics, morals, and standards of behavior
- ⌚ Enhance your professional conduct by continuing your training
- ⌚ Record your fact-finding methods in a journal
- ⌚ Attend workshops, conferences, and vendor courses
- ⌚ Membership in professional organizations adds to your credentials

Maintaining objectivity

- ⌚ you must form and sustain unbiased opinions of your cases

Maintaining credibility

- ⌚ by keeping the case confidential
- ⌚ In the corporate environment, confidentiality is critical
- ⌚ In rare instances, your corporate case might become a criminal case as serious as murder
- ⌚ Achieve a high public and private standing and maintain honesty and integrity

Discussion Point:

“You are a digital forensics investigator working for a cybersecurity firm. A major corporation has reported a significant data breach. The company suspects that sensitive customer data, including financial information and personal details, has been compromised. The company's reputation and legal obligations are at stake. You are the team investigating the breach”

Private or corporate investigations

- Deal with private companies, non-law-enforcement government agencies, and lawyers
- Aren't governed directly by criminal law or Fourth Amendment issues
- Governed by internal policies that define expected employee behavior and conduct in the workplace
- Private corporate investigations also involve litigation disputes
- Investigations are usually conducted in civil cases

Discussion Point:

“You are a digital forensics investigator working for a cybersecurity firm. A major corporation has reported a significant data breach. The company suspects that sensitive customer data, including financial information and personal details, has been compromised. The company's reputation and legal obligations are at stake. You are the team investigating the breach”

Scenario 1: As you begin the investigation, the company's IT department, to mitigate the breach, has shut down the breached server. **Discuss the implications of this action and how it may affect the investigation.**

Best Practices for Computer based Electronic Evidence

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

Discussion Point:

“You are a digital forensics investigator working for a cybersecurity firm. A major corporation has reported a significant data breach. The company suspects that sensitive customer data, including financial information and personal details, has been compromised. The company's reputation and legal obligations are at stake. You are the team investigating the breach”

Scenario 2: During the investigation, it becomes apparent that some of the company's IT staff with limited digital forensics knowledge have accessed the breached server. They may have unintentionally tampered with evidence. **Discuss how competence and the ability to explain actions are crucial in preserving the integrity of the evidence.**

Best Practices for Computer based Electronic Evidence

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

Discussion Point:

“You are a digital forensics investigator working for a cybersecurity firm. A major corporation has reported a significant data breach. The company suspects that sensitive customer data, including financial information and personal details, has been compromised. The company's reputation and legal obligations are at stake. You are the team investigating the breach”

Scenario 3: The investigation reveals that there is no established audit trail for the processes applied to the electronic evidence. There is no clear record of who accessed the server and what actions were taken. **Discuss the importance of maintaining an audit trail and how it would have aided the investigation.**

Best Practices for Computer based Electronic Evidence

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

Discussion Point:

“You are a digital forensics investigator working for a cybersecurity firm. A major corporation has reported a significant data breach. The company suspects that sensitive customer data, including financial information and personal details, has been compromised. The company's reputation and legal obligations are at stake. You are the team investigating the breach”

Scenario 4: As the investigation unfolds, it becomes apparent that the case officer responsible for the investigation has not been overseeing the actions of the IT staff effectively. **Discuss how the case officer's responsibility is central to ensuring that the investigation adheres to the law and these principles.**

Best Practices for Computer based Electronic Evidence

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

Discussion Point:

What if: A person uses their corporate email account to send confidential customer data to their friend, and that act is flagged in security-monitoring technologies?

After investigation, it was found that unauthorized access to the person's email was gained to send the confidential customer data through email;

The 1st one is Inculpatory Evidence, that demonstrates a person's involvement in an act of guilt.

The 2nd one is Exculpatory Evidence, that is favourable to a person who is cleared from their involvement of act.



Ethics

- Personal Ethics
- Professional Ethics
- Computer Ethics
- Business Ethics

- **Research, Discuss and Articulate: Code of Ethics**
 - **There are various organisations/ Boards that have their own code of Ethics.**
 - **Few to say:**
 - Digital Forensics Certification Board (DFCB),
 - International Society of Forensic Computer Examiners (ISFCE) etc.
 - Discuss about their code of ethics and how it could help you in ethically handling forensic analysis.

Analyzing Evidence

Digital Forensics
(ACCA7031)

Applied Computing - WISA

➤ **Analysing Evidences**

➤ **Disk**

➤ **Partitions**

➤ **File System**

➤ **Attributes**

In continuation to our earlier lecture, we discussed about the History of Digital Forensics and its attributes. Understood the importance of Incident Response and discussed about the principles of Digital Forensics, its process, different roles and finally getting to understand the technology's role in the crime and the law framed around it to prevent various crimes.

In this part, lets move forward and discuss about various digital forensics capabilities and the appropriate method to acquire data. We shall also discuss the challenges in acquiring data and the area in which keen attention is required. Our discussion this week will cover digital evidences storage formats, Acquisition Methods, Contingency Planning for Data Acquisition, Use and Validate Data Acquisition, RAID Acquisition, Remote Network Acquisition and Forensic Tools used for Data Acquisition.



Understanding the silent witness!!!

- Gives OS a road map to data on a disk
- Type of file system determines how data is stored on the disk
- A file system is directly related to an OS
- On investigating a suspect's computer to acquire or inspect data, You should be familiar with the computer's platform



Storage Drives and its characteristics



Logical Structure of a Disk



Booting Process



File Systems and Storage Systems



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Trawsnewid Addysg, Trawsnewid Bywydau
Transforming Education, Transforming Lives

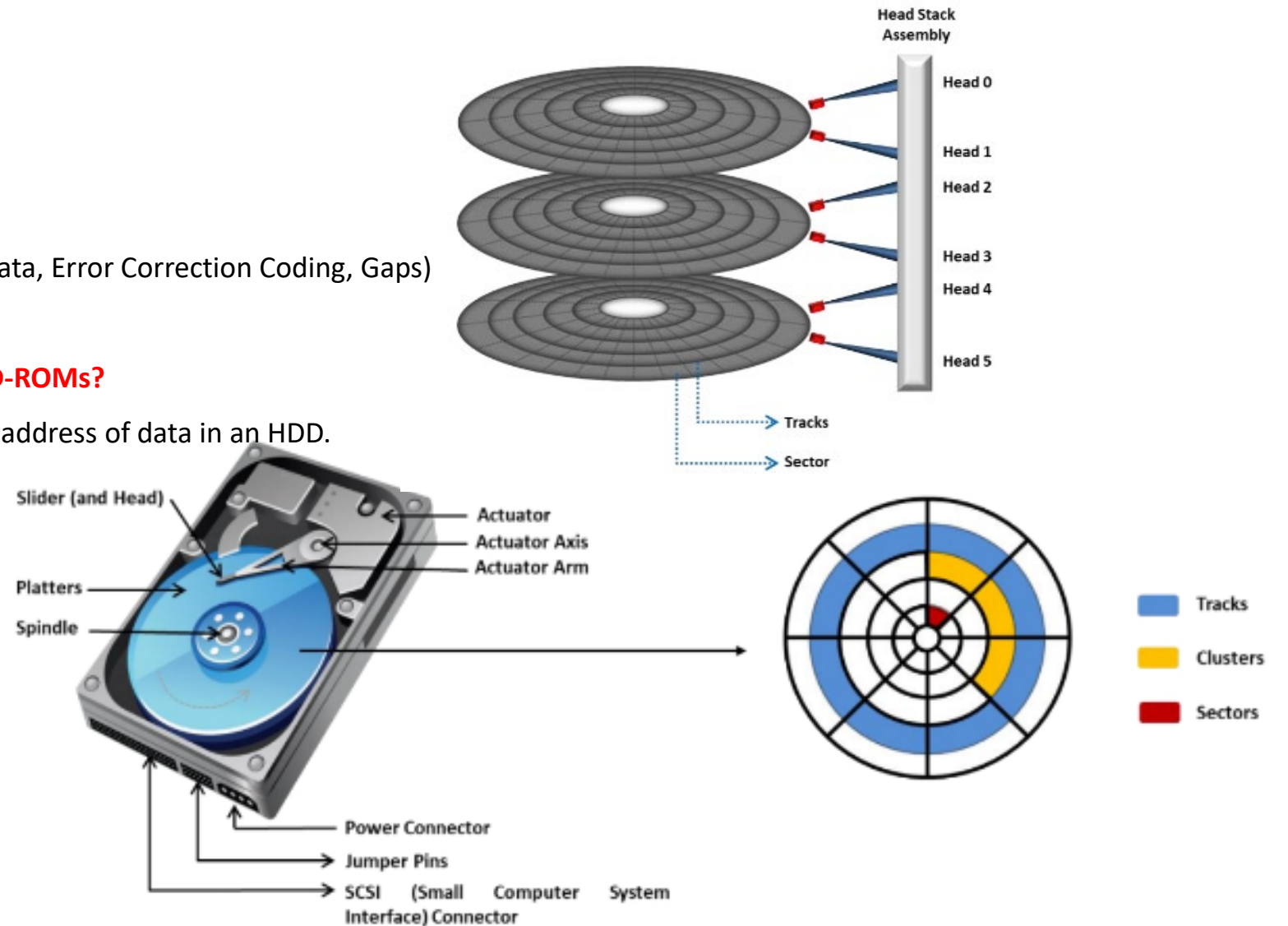
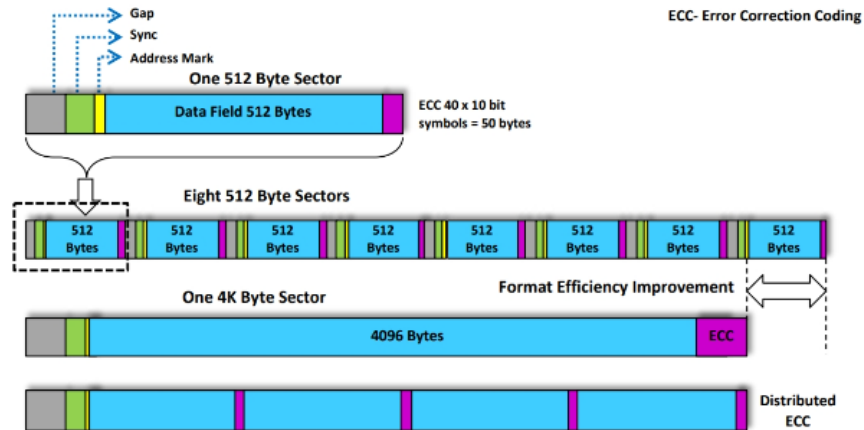
Discussion Point

- Understand file systems and its unique characteristics – for digital forensics
- HDD vs SSD
 - Data is the Key – a silent witness – Unlock and interpret this silence
 - File systems are blueprints
 - Storage drives are digital evidences
 - Knowing the ins and outs of file system, its characteristics help in extracting and analysing the data
 - Working on this area will help you uncover challenges and opportunities
- HDD File Structure and Characteristics
- SSD File Structure and Characteristics
- File Systems in Digital Forensics

Storage Disks

○ HDD

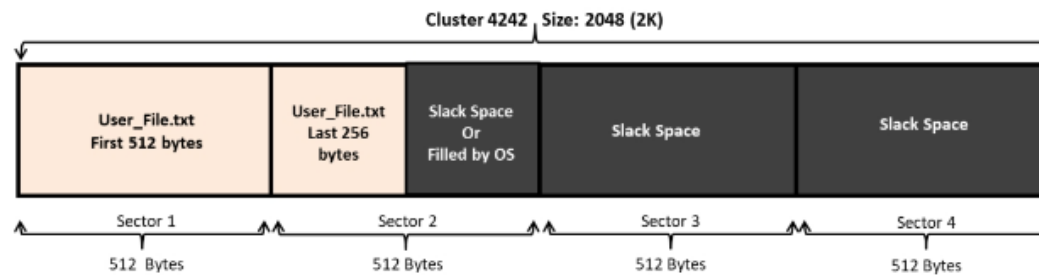
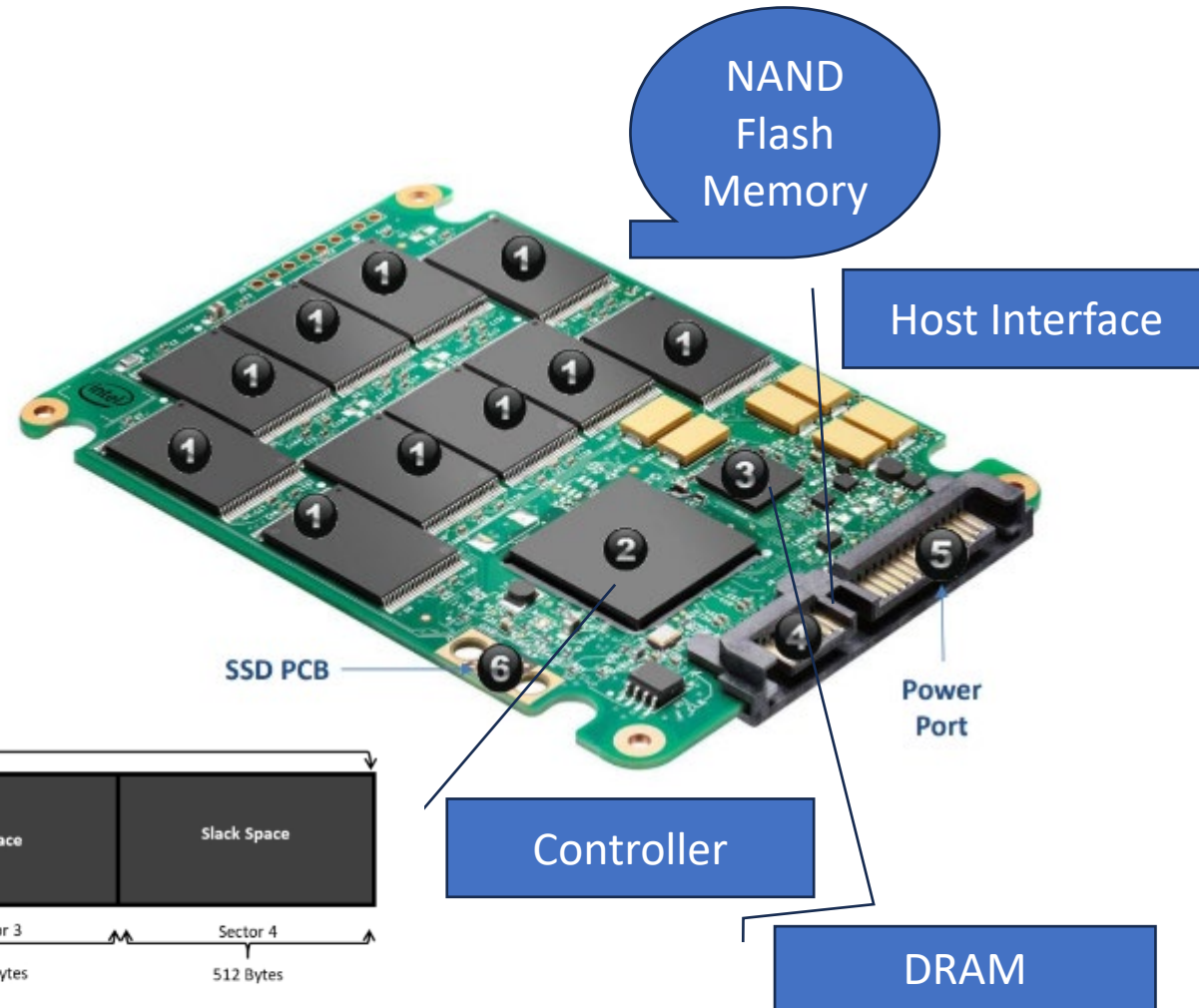
- Track Numbering
- Sector (ID Information, Synchronization Fields, Data, Error Correction Coding, Gaps)
- The data is stored is placed in a 512 bytes.
- **What is the bytes of data for CD-ROMs and DVD-ROMs?**
- The track number and sector number points the address of data in an HDD.
- **What is 4K Sectors?**



The images in this slide are used from Computer Hacking Forensic Investigator V10 eBook

Storage Disks

- SSD
 - NAND-based SSDs
 - Volatile RAM-based SSDs
 - Advantages: Faster data access, lower power usage, High
- Data Addressing
 - Allotting addresses to each physical block of data
 - CHS (Cylinder-Head-Sector)
 - LBA (Logical Block Address)



○ What is Slack Space?

- RAM Slack and Drive Slack

The images in this slide are used from Computer Hacking Forensic Investigator V10 eBook

Logical View

```
C:\Windows\system32>chkdsk
The type of the file system is NTFS.
Volume label is Local Disk.

WARNING! /F parameter not specified.
Running CHKDSK in read-only mode.

Stage 1: Examining basic file system structure ...
 830464 file records processed.
File verification completed.
Phase duration (File record verification): 17.41 seconds.
14047 large file records processed.
Phase duration (Orphan file record recovery): 0.00 milliseconds.
 0 bad file records processed.
Phase duration (Bad file record checking): 0.26 milliseconds.

Stage 2: Examining file name linkage ...
68622 reparse records processed.
1198424 index entries processed.
Index verification completed.
Phase duration (Index verification): 25.71 seconds.
 0 unindexed files scanned.
Phase duration (Orphan reconnection): 8.98 seconds.
 0 unindexed files recovered to lost and found.
Phase duration (Orphan recovery to lost and found): 0.30 milliseconds.
68622 reparse records processed.
Phase duration (Reparse point and Object ID verification): 163.55 milliseconds.

Stage 3: Examining security descriptors ...
Security descriptor verification completed.
Phase duration (Security descriptor verification): 39.63 milliseconds.
183981 data files processed.
Phase duration (Data attribute verification): 0.37 milliseconds.
CHKDSK is verifying Usn Journal...
35299040 USN bytes processed.
Usn Journal verification completed.
Phase duration (USN journal verification): 218.86 milliseconds.

Windows has scanned the file system and found no problems.
No further action is required.

248730623 KB total disk space.
240123288 KB in 631396 files.
478400 KB in 183982 indexes.
 0 KB in bad sectors.
995623 KB in use by the system.
65536 KB occupied by the log file.
7133312 KB available on disk.

    4096 bytes in each allocation unit.
62182655 total allocation units on disk.
1783328 allocation units available on disk.
Total duration: 52.55 seconds (52558 ms).

C:\Windows\system32>
```

- The logical view of the storage!!! – The File System
- File system is a controller of the physical disks (storage)
- File system is structured to focus on Performance, Consistency, Expandability and Compatibility of the physical disks
- **What happens when a cluster is marked as used but not allocated to any file?**
- **Lost Clusters**
 - What is the reason for Lost Clusters?
 - Does your storage have lost clusters? Find out.
- **“Bad Sectors” – What happens to a data in the bad sector? Could it be recovered?**



Disk Partitions

BIOS Parameter Block

- It is a data structure in the partition boot sector
- Defines the Filesystem Structure
- Assist investigations by locating the file table on the hard drive

Master Boot Record

- First sector of a data storage device (HDD)
- The information about the files on the disk is stored in the MBR
- 512 Byte Boot Sector

Let's look and analyse a MBR Structure: In Class Activity – Refer to our lecture demonstration about analysing MBR

MBR

To recall, the MBR holds 512 bytes (1 sector)– containing bootstrapping code, details of hard disk partition scheme etc. We just discussed and analysed about Sector 0, that has boot indicator, CHS Values, Partition Type, Size etc. Using MBR, what could be the maximum size of a Hard Disk?

A 512 GB

B 500 GB

C 1 TB

D 2 TB

Why?

446 CODE AREA

16 Bytes/row
2 Hexa - 1 Byte

Offset (d)	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	Decoded text
000000000000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000000016	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000000032	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000000048	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000000064	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000000096	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000000112	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000000128	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000000144	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000000160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000000176	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000000192	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000000208	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000000224	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000000240	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000000256	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000000272	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000000288	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000000304	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000000320	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000000336	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000000352	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000000368	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000000384	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000000400	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000000416	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000000432	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000000448	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000000464	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000000480	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000000496	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000000512	45	16	19	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000000528	80	E5	81	A5	00	00	00	00	01	00	00	00	00	00	00	00	
000000000544	AF	32	CF	1D	00	00	00	00	22	00	00	00	00	00	00	00	
000000000560	5E	32	CF	1D	00	00	00	00	4F	35	4E	C1	A9	4F	49	22	
000000000576	A1	EF	B1	FA	C8	C8	F2	F5	02	00	00	00	00	00	00	00	

64 MASTER PARTITION TABLE

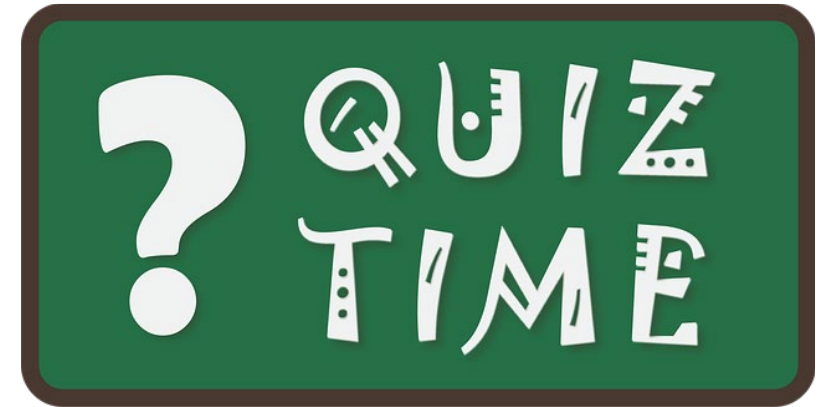
END OF MBR

BOOT RECORD SIGNATURE

Sample MBR in a Hexadecimal display

4 Partition
16 Bytes each

1st-Byte - Boot Indicator
NEXT 3 -Byte - Starty CHS values
CYLINDER - HEAD - SECTOR
NEXT 1 -Byte - Partition Type Descrptn
NEXT 3 -Byte - END CHS VALUE
NEXT 4 -Byte - STARTING SECTOR
NEXT 4 -Byte - PARTITIONS SIZE



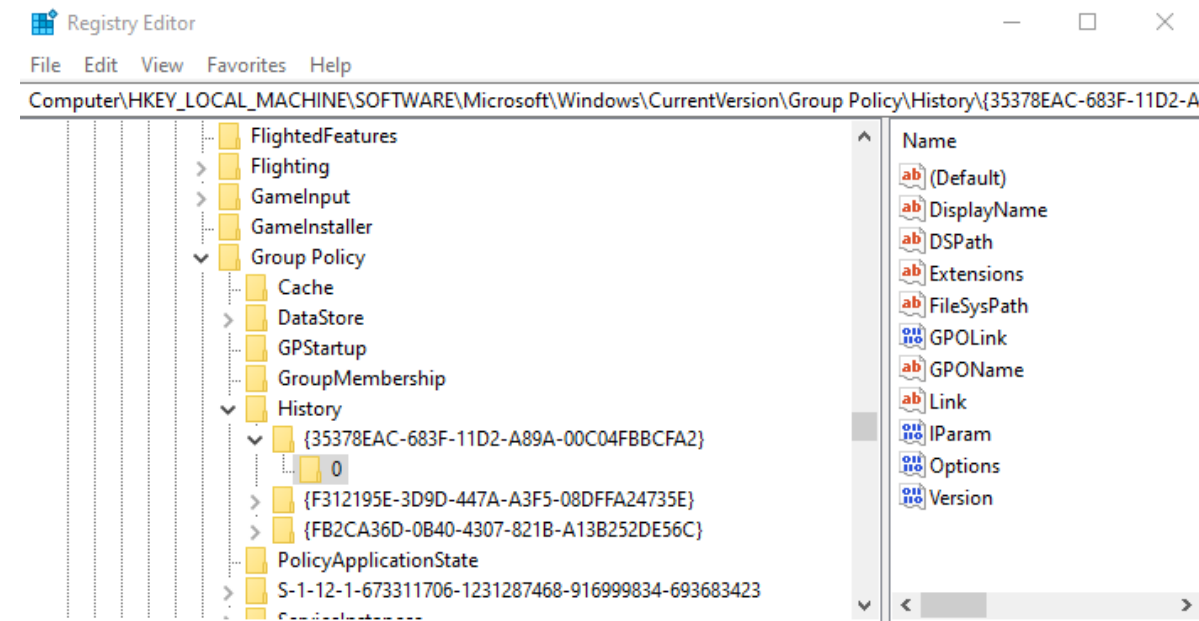
Disk Partitions

Globally Unique Identifier (GUID)

- 128-bit **unique** number generated by the Windows OS
- 32 Hexadecimal digits
- Identify a specific device, a document, a database entry, and/or user

Globally Unique Identifier (GUID) Partition Table

- Modern and Standardized Partitioning Scheme.
- Replacement for MBR
- Part of UEFI
- MBR uses _____ bits for storing LBAs and the Size information on _____ byte sectors.
- GPT uses LBA instead of CHS
- Each block is 512 bytes, and each partition entry is 128 bytes.



Let's look and analyse a GPT Structure: In Class Activity – Refer to our lecture demonstration about analysing GPT

Disk Partitions

Globally Unique Identifier (GUID) Partition Table

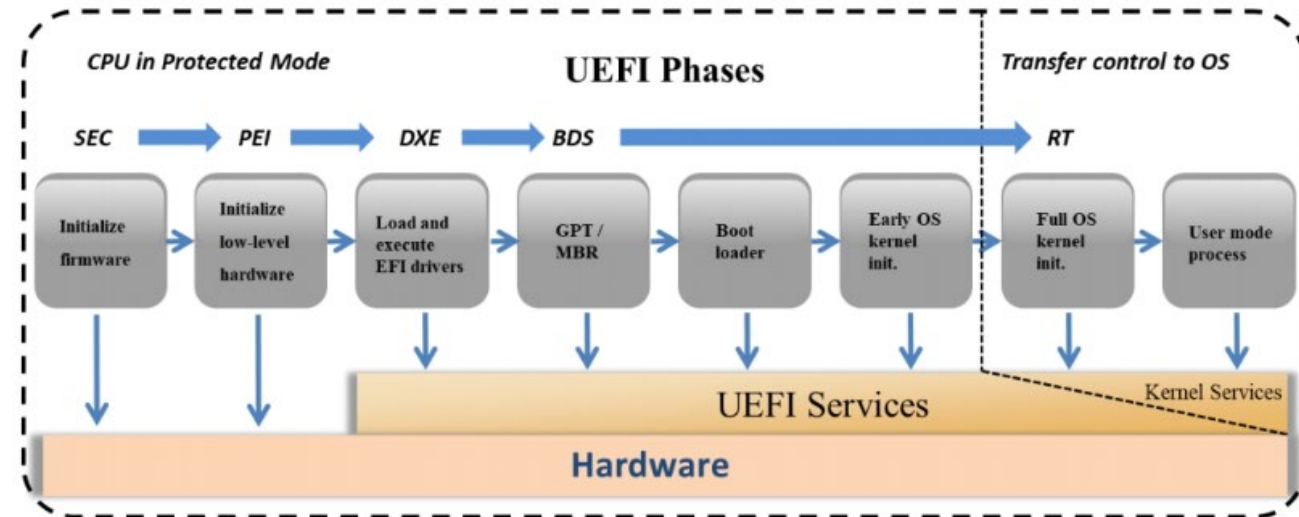
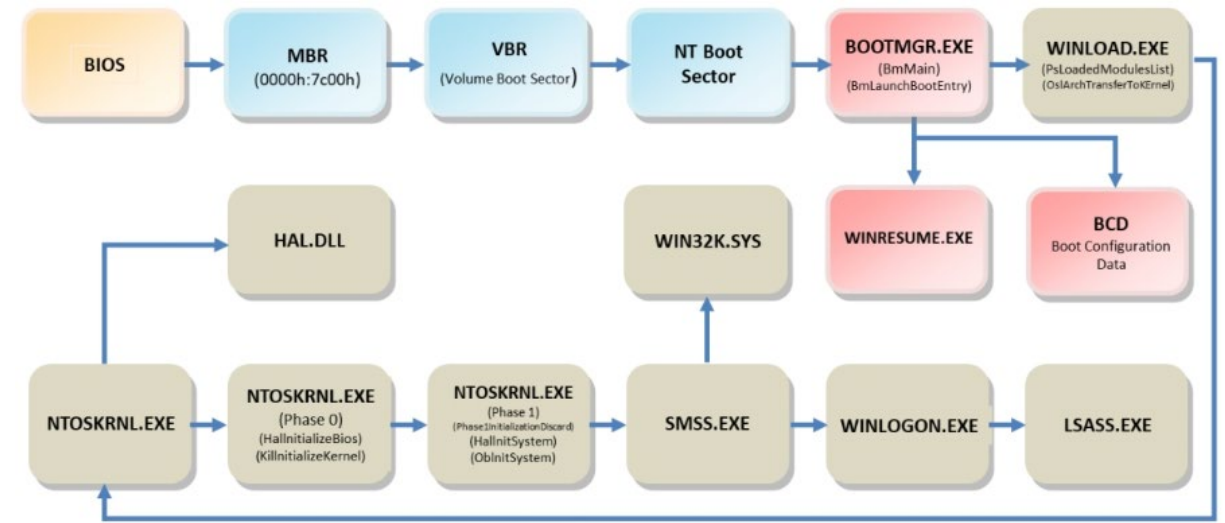
- Allows 128 partitions – MBR allows 4 partitions
- By default, all Hard Disks come with GUID Partition Table, however, you still have the option for MBR while re-formatting or re-partitioning disks

Booting

- Booting is a process of starting/ restarting a computer
- Cold Booting/ Hard Booting
- Warm Booting

The UEFI boot process has the following **five phases**,

Security phase , Pre-EFI initialization phase, Driver Execution Environment phase, Boot Device Selection phase and Runtime phase



Disk Partitions

Five Phases

Security phase , Pre-EFI initialization phase, Driver Execution Environment phase, Boot Device Selection phase and Runtime phase

Identifying the GUID Partition Table (GPT)

Get-GPT –Path [\\.\PHYSICALDRIVE0](#)

Disk formatted using the GPT partitioning scheme

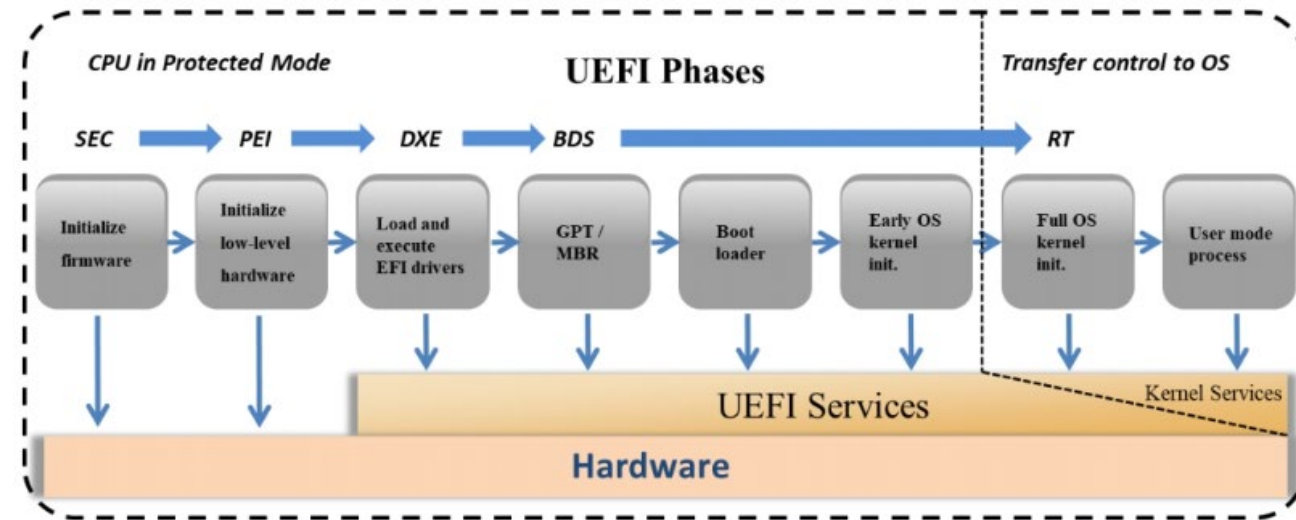
Get-BootSector –Path [\\.\](#)

Disk formatted using the MBR partitioning scheme

Get-ForensicBootSector –Path [\\.\](#)

MBR formatted Disk – Partition Table

Get-ForensicPartitionTable –Path [\\.\](#)



diskpart

detail disk

select partition=0

File System

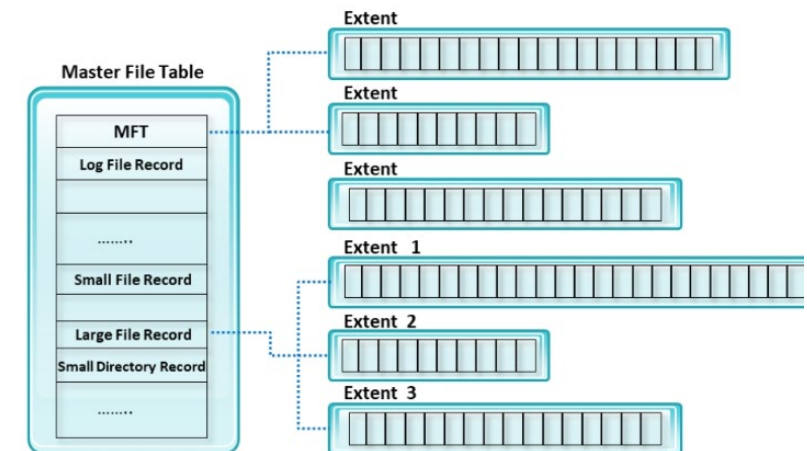
New Technology File System (NTFS)

- Introduced with Windows NT
 - Recommended file system for Windows 2000 Pro, XP, and later versions
 - Improvements over FAT file systems
 - NTFS provides more information about a file
 - NTFS gives more control over files and folders
 - NTFS was Microsoft's move towards a journaling file system
 - In NTFS, everything written to the disk is considered a file
 - On an NTFS disk
 - **First data set is the Partition Boot Sector**
 - **Next is Master File Table (MFT)**
 - NTFS results in much less file slack space
 - Clusters are smaller for smaller disk drives
 - NTFS also uses Unicode (*An international data format*)
- ❖ MFT contains **information about all files on the disk** (*Including the system files the OS uses*)
 - ❖ In the MFT, the first 15 records are reserved for system files
 - ❖ Records in the MFT are called **METADATA**

File System

- In the NTFS MFT, All files and folders are stored in separate records of 1024 bytes each
- Each record contains file or folder information which is further divided into record fields containing metadata
- A record field is referred to as an attribute ID
- File or folder information is typically stored in one of two ways in an MFT record: Resident and nonresident
- Files larger than 512 bytes are stored outside the MFT.
- MFT record provides cluster addresses where the file is stored on the drive's partition which is referred to as data runs
- Each MFT record starts with a header identifying it as a resident or nonresident attribute

System File	Filename	MFT Record	Purpose of the File
Master File Table	\$Mft	0	It contains a record of all the files and folders on an NTFS volume
Master File Table mirror	\$MftMirr	1	It contains a backup of the MFT and is used when the MFT is corrupt/damaged
Log file	\$LogFile	2	It stores the logs pertaining to changes in file system metadata, and is used for file system recovery in case of a system crash
Volume	\$Volume	3	It contains information about the volume
Attribute definitions	\$AttrDef	4	It lists attributes and their details such as names, numbers, and descriptions
Root filename index		5	It is the root folder
Cluster bitmap	\$Bitmap	6	It maintains a list of all the used and unused clusters on an NTFS volume
Boot sector	\$Boot	7	It includes the BPB and bootstrap code, and is essential for booting the system
Bad cluster file	\$BadClus	8	It contains the bad clusters on a volume
Security file	\$Secure	9	It lists all the security descriptors within a volume
Uppcase table	\$Uppcase	10	It is used for converting lowercase characters to uppercase characters
NTFS extension file	\$Extend	11	It is used for various optional extensions



File System

- In the NTFS MFT, All files and folders are stored in separate records of 1024 bytes each
- Each record contains file or folder information which is further divided into record fields containing metadata
- A record field is referred to as an attribute ID
- File or folder information is typically stored in one of two ways in an MFT record: Resident and nonresident
- Files larger than 512 bytes are stored outside the MFT.
- MFT record provides cluster addresses where the file is stored on the drive's partition which is referred to as data runs
- Each MFT record starts with a header identifying it as a resident or nonresident attribute

Attribute Type	Purpose of the Attribute
Standard information	Lists the information regarding the time stamp data and link count information
Attribute list	List of attributes that are not in the MFT
Filename	Stores the filename, which can be long or short
Security descriptor	Lists the ownership and access rights to the file
Data	Stores file data
Object ID	File identifier volume –unique identifier
Logged tool stream	Used by the encrypted file system service
Reparse point	Volume mount point used for installable file system filter drivers
Index root	Employed for use of folders and files
Index allocation	Employed for use of folders and files
Bitmap	Employed for use of folders and files
Volume information	Lists the version number of the volume
Volume name	Lists the volume label

File System

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
035B3400	46	49	4C	45	30	00	03	00	9B	99	98	00	00	00	00	00
035B3410	02	00	01	00	38	00	01	00	A8	01	00	00	00	04	00	00
035B3420	00	00	00	00	00	00	00	00	04	00	00	00	A2	17	00	00
035B3430	03	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00
035B3440	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00
035B3450	62	16	9B	68	0A	7C	C9	01	BC	78	9D	68	0A	7C	C9	01
035B3460	BC	78	9D	68	0A	7C	C9	01	BC	78	9D	68	0A	7C	C9	01
035B3470	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
035B3480	00	00	00	00	09	01	00	00	00	00	00	00	00	00	00	00
035B3490	00	00	00	00	00	00	00	00	30	00	00	00	70	00	00	00
035B34A0	00	00	00	00	00	00	02	00	52	00	00	00	18	00	01	00
035B34B0	8A	00	00	00	00	00	01	00	62	16	9B	68	0A	7C	C9	01
035B34C0	BC	78	9D	68	0A	7C	C9	01	BC	78	9D	68	0A	7C	C9	01
035B34D0	BC	78	9D	68	0A	7C	C9	01	00	00	00	00	00	00	00	00
035B34E0	00	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00
035B34F0	08	03	42	00	65	00	6E	00	31	00	2E	00	74	00	78	00
035B3500	74	00	00	00	00	00	00	00	40	00	00	00	28	00	00	00
035B3510	00	00	00	00	00	00	03	00	10	00	00	00	10	00	00	00
035B3520	F4	7C	F1	27	DF	E7	DD	11	A8	3F	00	22	15	D5	88	06
035B3530	80	00	00	00	70	00	00	00	00	00	18	00	00	00	01	00
035B3540	54	00	00	00	18	00	00	00	41	20	63	6F	75	6E	74	72
035B3550	79	6D	61	6E	20	62	65	74	77	65	65	6E	20	74	77	6F
035B3560	20	6C	61	77	79	65	72	73	20	69	73	20	6C	69	6B	65
035B3570	20	61	20	66	69	73	68	20	62	65	74	77	65	65	6E	20
035B3580	74	77	6F	20	63	61	74	73	2E	0D	0A	42	65	6E	6A	61
035B3590	6D	69	6E	20	46	72	61	6E	6B	6C	69	6E	00	00	00	00
035B35A0	FF	FF	FF	FF	82	79	47	11	00	00	00	00	00	00	00	00

- A: All MFT records start with FILE0
- B: Start of attribute 0x10
- C: Length of attribute 0x10 (value 60)
- D: Start of attribute 0x30
- E: Length of attribute 0x30 (value 70)
- F: Start of attribute 0x40
- G: Length of attribute 0x40 (value 28)
- H: Start of attribute 0x80
- I: Length of attribute 0x80 (value 70)
- J: Attribute 0x80 resident flag
- K: Starting position of resident data

	A: Starting position of attribute 0x80 \$Data	B: Length of attribute 0x80 in little endian format	C: Interpreted little endian value
035B3530	80	70	00 00 18 00 00 00 01 00
035B3540	54	18	41 20 63 6F 75 6E 74 72
035B3550	79	6D	77 65 65 6E 20 74 77 6F
035B3560	20	6C	6B 65
035B3570	20	61	65 6E 20
035B3580	74	77	6A 61
035B3590	6D	69	00 00 00 00
035B35A0	FF	FF	00 00 00 00

NTFS – MFT Resident

- A: Start of nonresident attribute 0x80
- B: Length of nonresident attribute 0x80
- C: Attribute 0x80 nonresident flag
- D: Starting point of data run
- E: End-of-record marker (FF FF FF FF) for the MFT record

NTFS – MFT Non-Resident

035B3CD0	6A	22	16	88	0B	7C	C9	01	00	00	00	00	00	00	00	00
035B3CE0	00	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00
035B3CF0	08	03	42	00	65	00	6E	00	32	00	2E	00	72	00	74	00
035B3D00	66	00	00	00	00	00	00	00	40	00	00	00	28	00	00	00
035B3D10	00	00	00	00	00	00	00	04	10	00	00	00	18	00	00	00
035B3D20	F7	7C	F1	27	DF	E7	DD	11	A8	3F	00	22	15	D5	88	06
035B3D30	80	00	00	00	48	00	00	00	01	00	00	00	00	03	00	00
035B3D40	00	00	00	00	00	00	00	00	02	00	00	00	00	00	00	00
035B3D50	40	00	00	00	00	00	00	00	00	06	00	00	00	00	00	00
035B3D60	78	05	00	00	00	00	00	00	78	05	00	00	00	00	00	00
035B3D70	31	03	15	55	01	00	01	00	FF	FF	FF	FF	82	79	47	11



File System

New Technology File System (NTFS)

- When a disk is created as an NTFS file structure, **OS assigns logical clusters to the entire disk partition**
- These assigned clusters are called **logical cluster numbers (LCNs)**.
- These LCN's become the addresses that allow the **MFT to link to nonresident files** on the disk's partition

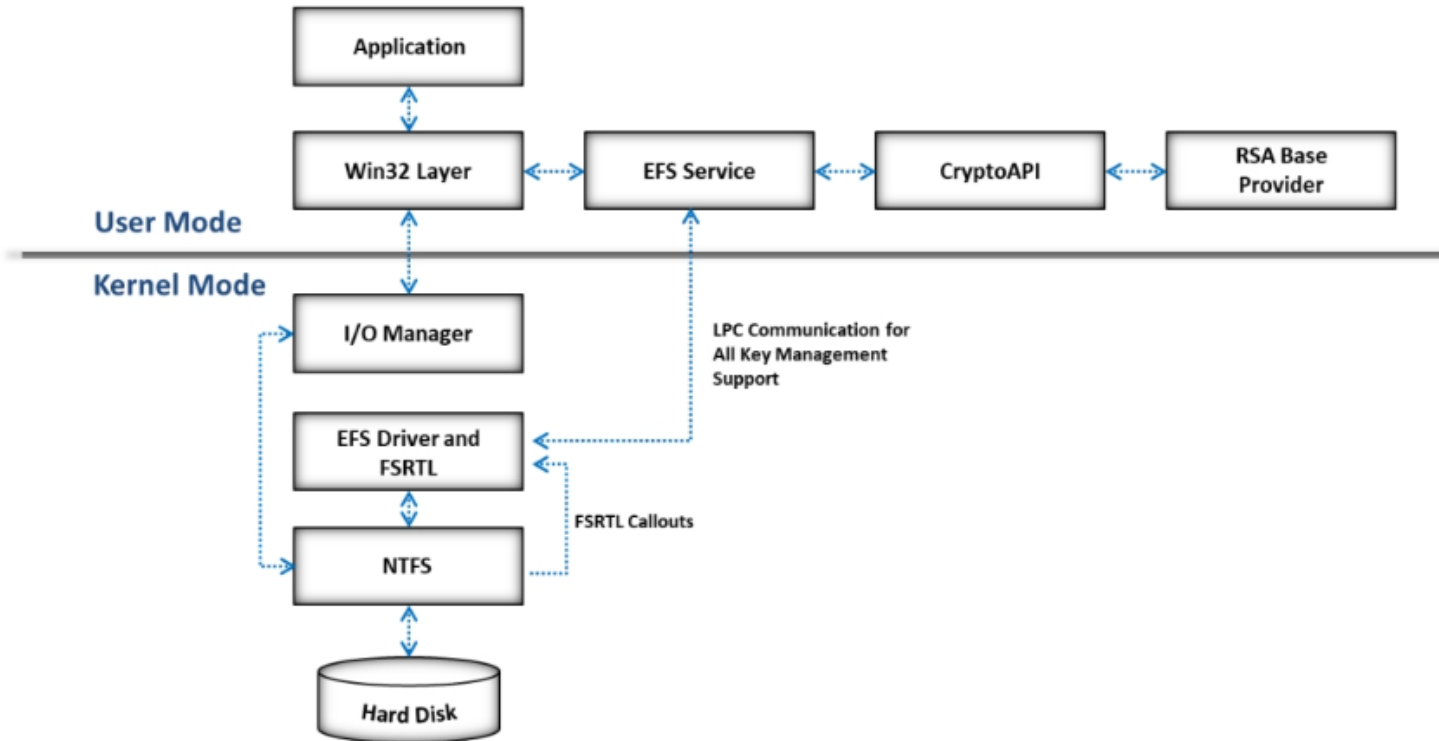
Data streams

- Ways data can be appended to existing files
- Can obscure valuable evidentiary data, intentionally or by coincidence
- In NTFS, a data stream becomes an additional file attribute which Allows the file to be associated with different applications

File System

New Technology File System (NTFS)

- Compressed Files
- Encryption (EFS – Encrypting File Systems)
 - Built-in Feature
 - Uses Symmetric Key Encryption technology with Public Key Technology
 - Users can manually encrypt a file using GUI/CLI
 - The system issues a file encryption certificate whenever a user encrypts a file.
 - If the user loses that certificate and related private key, they can perform data recovery through the recovery key agent.
 - The recovery agent holds a special certificate and related private key, which help in data recovery



File System

New Technology File System (NTFS)

- Compressed Files
- Encryption (EFS – Encrypting File Systems)
 - Built-in Feature
 - Uses Symmetric Key Encryption technology with Public Key Technology
 - Users can manually encrypt a file using GUI/CLI
 - The system issues a file encryption certificate whenever a user encrypts a file.
 - If the user loses that certificate and related private key, they can perform data recovery through the recovery key agent.
 - The recovery agent holds a special certificate and related private key, which help in data recovery

00000000	C8 03 00 00	00 00 00 00	01 00 00 00 00 00 00 00	И....
00000010	D7 4C 90 99	3D 90 68 42	B4 FA DF CF E1 9E B1 D9	ЧLh™=hBrъЯПCh+ll
00000020	93 A5 51 37	83 A7 77 13	81 F7 63 AD AB 7C A9 AB	"IQ7fSw.fyc-« @«
00000030	00 00 00 00	00 00 00 00	00 00 00 00 00 00 00 00	
00000040	54 00 00 00	54 02 00 00	00 00 00 00 00 00 00 00	T...T.....
00000050	00 00 00 00	01 00 00 00	FC 01 00 00 14 00 00 00	b.....
00000060	80 00 00 00	7C 01 00 00	00 00 00 00 68 01 00 00	Ъ... h...
00000070	1C 00 00 00	03 00 00 00	30 01 00 00 38 00 00 00	0...8...
00000080	00 00 00 00	00 00 00 00	01 05 00 00 00 00 00 05	
00000090	15 00 00 00	5A 56 B3 78	1C 36 54 29 A8 51 FF 09	2Vix.6T)EQя.
000000A0	D0 04 00 00	14 00 00 00	14 00 00 00 28 00 00 00	P.....(...
000000B0	72 00 00 00	C8 00 00 00	F7 C4 91 89 AD 29 24 D7	р...И...чД'%-) \$Ч
000000C0	78 6E 6E 9B	EE CC 64 D5	14 6D 71 55 36 00 35 00	xnn>oMdX.mgU6.5.
000000D0	39 00 37 00	64 00 31 00	64 00 62 00 2D 00 31 00	9.7.d.1.d.b.-.1.
000000E0	63 00 32 00	63 00 2D 00	34 00 31 00 36 00 31 00	c.2.c.-.4.1.6.1.
000000F0	2D 00 62 00	32 00 37 00	66 00 2D 00 32 00 65 00	-.b.2.7.f.-.2.e.
00000100	66 00 31 00	38 00 36 00	65 00 39 00 36 00 64 00	f.1.8.6.e.9.6.d.
00000110	65 00 63 00	00 00 4D 00	69 00 63 00 72 00 6F 00	e.c...M.i.c.r.o.
00000120	73 00 6F 00	66 00 74 00	20 00 42 00 61 00 73 00	s.o.f.t. .B.a.s.
00000130	65 00 20 00	43 00 72 00	79 00 70 00 74 00 6F 00	e. .C.r.y.p.t.o.
00000140	67 00 72 00	61 00 70 00	68 00 69 00 63 00 20 00	g.r.a.p.h.i.c. .
00000150	50 00 72 00	6F 00 76 00	69 00 64 00 65 00 72 00	P.r.o.v.i.d.e.r.
00000160	20 00 76 00	31 00 2E 00	30 00 00 00 4F 00 55 00	.v.1...0...O.U.
00000170	3D 00 45 00	46 00 53 00	20 00 46 00 69 00 6C 00	=.E.F.S. .F.i.l.
00000180	65 00 20 00	45 00 6E 00	63 00 72 00 79 00 70 00	e. .E.n.c.r.y.p.
00000190	74 00 69 00	6F 00 6E 00	20 00 43 00 65 00 72 00	t.i.o.n. .C.e.r.
000001A0	74 00 69 00	66 00 69 00	63 00 61 00 74 00 65 00	t.i.f.i.c.a.t.e.
000001B0	2C 00 20 00	4C 00 3D 00	45 00 46 00 53 00 2C 00	,. .L.=.E.F.S.,.
000001C0	20 00 43 00	4E 00 3D 00	6F 00 6C 00 65 00 67 00	.C.N.=.o.l.e.g.
000001D0	61 00 00 00	EB 11 78 3E	0E 4B 72 0A 65 80 08 24	a...л.x>.Kr.eP.\$
000001E0	86 08 C4 43	73 C3 5D 1A	6F 77 76 8D 7C DC F5 C1	†.HCsГ].owvK BxB
000001F0	44 25 55 4C	C5 15 84 39	32 BD B0 50 63 4A 0E C3	D%ULE.,,92S°PcJ.Г
00000200	32 BC C4 A3	28 6D 29 D3	C6 71 DA AA 56 8E 5F 02	2jDJ(m)YЖqbeVh.
00000210	AE 66 D7 22	17 D0 D1 AD	5C EF D1 A2 83 19 0A 3E	@f4".PC-\nCŸf..>
00000220	4E 9A 3E 7C	74 66 E5 AD	C5 D1 26 41 04 E7 1E BD	Nz> tfe-EC&A.з.S
00000230	6C C0 5C 39	C2 F6 32 28	A5 25 4A AD 42 BF 10 5F	lA\9Bu2(I%J-Bi._
00000240	70 5C 9D 6E	34 09 25 25	1B 53 4D D8 2E F2 38 2D	p\kn4.%%.SMIII.t8-
00000250	7F 49 28 52	01 00 00 00	6C 01 00 00 14 00 00 00	CI(R....l.....

File System

New Technology File System (NTFS)

- Deleting a File
 - When a file is deleted, the OS renames it and moves it to the Recycle Bin
 - Can use the Del (delete) MS-DOS command to eliminate the file from the MFT listing in the same way FAT does
- Registry
 - A database that stores hardware and software configuration information, network connections, user preferences, and setup information
 - For investigative purposes, the Registry can contain valuable evidence
 - Registry
 - Registry Editor
 - HKEY
 - Key
 - Subkey
 - Branch
 - Value
 - Default value and Hives

Group Activity!!!

Identify and discuss the Linux and Macintosh boot process with suitable flow diagrams and examples.

Use the existing images in our shared folder to analyse and discuss Windows File System

- **FAT File System Layout**
- **FAT Partition Boot Sector**
- **FAT Folder Structure**
- **NTFS Architecture**
- **NTFS Master File Table**

Anti Forensics Techniques

Digital Forensics
(ACCA7031)

Applied Computing - WISA

- **Understand Anti-Forensics Techniques**
- **Data Deletion and Recycle Bin Forensics**
- **File Carving**
- **Password Cracking**
- **Detecting Steganography**
- **Artifact Wiping Techniques**
- **Countermeasures**

In continuation to our earlier lectures, where we discussed about various Digital Forensics aspects, now lets discuss about “Anti-forensics techniques”.

They are used by cyber-criminals to complicate or prevent proper forensics investigation. Cyber-criminals employ these techniques to make evidence collection extremely difficult and to compromise the accuracy of a forensics report.

Let's discuss and try to understand what AFT is? Its Goals, Techniques and concepts around this.

Anti Forensics

- Anti-forensics, also known as counter forensics,
- It is a set of techniques that attackers or perpetrators use to sidetrack the forensic investigation process

(try to make the investigations much harder).

- It will negatively affect the quantity and quality of evidence from a crime scene.

(making the forensic investigation process difficult).

- As an investigator, you might have to perform additional steps to fetch the data.

(leading to a delay in the investigation process).

Anti Forensics

Goals

- Interrupt and prevent information collection
- Make the investigator's task of finding evidence difficult
- Hide traces of crime or illegal activity
- Compromise the accuracy of a forensics report or testimony
- Delete evidence that an anti-forensics tool has been run

Techniques

- Data/File Deletion
- Password Protection
- Steganography
- Data Hiding in File System Structures
- Trail Obfuscation
- Artifact Wiping
- Overwriting Data/Metadata
- Encryption
- Program Packers
- Minimizing Footprint

Anti Forensics – Deletion

Deleting files/data is a common anti-forensics technique used by attackers.

- What happens when a file is deleted from the hard drive?
- How will you try to recover the deleted data?
- What tools will you use?

Discuss with your group and share your thoughts!!!

Duration: 5 Mins Discussion – 5 Mins Presentation

Anti Forensics – Deletion

E5h!

Rings a bell? What is it?

\$BitMap

Rings a bell? What is it?

Recycle Bin

What is it? – Storage Location – Maximum Limit – How it restores?

Anti Forensics – Deletion

- INFO2 is the master database file and is very crucial for the recovery of data.
- It contains various details of deleted files such as their original file name, original file size, date and time of deletion, unique identifying number, and the drive number in which the file was stored.

```
C:\Windows\system32>dir /a /p %systemdrive%\$Recycle
Volume in drive C is Local Disk
Volume Serial Number is 0E67-EEA4

Directory of C:\$Recycle.bin

12/09/2023  13:25    <DIR>        .
12/09/2023  13:25    <DIR>        ..
07/12/2023  06:20    <DIR>        S-1-12-1-6733117
12/09/2023  13:25    <DIR>        S-1-5-18
               0 File(s)                0 bytes
               4 Dir(s)  9,313,476,608 bytes free
```

```
Directory of C:\$Recycle.bin\S-1-12-1-673311706-123

07/12/2023  06:20    <DIR>        .
07/12/2023  06:20    <DIR>        ..
14/11/2023  06:55                270 $I0EBOXE.lck
14/11/2023  06:55                328 $I1BLN4C.lck
07/12/2023  06:20                182 $I1XPG46.docx
14/11/2023  07:04                370 $I21Y0B4.lck
14/11/2023  06:55                256 $I3KMVD9.lck
14/11/2023  07:05                292 $IAP249Y
14/11/2023  06:57                236 $IBEHK49
10/11/2023  19:40                256 $IC2FUCT.lck
14/11/2023  07:04                384 $IF27WHD.lck
21/11/2023  14:34                260 $IL0CE51.pdf
07/11/2023  13:46                238 $INM2166.lnk
07/12/2023  06:20                146 $IUACFEC.pdf
14/11/2023  07:03                374 $IUQG0CS.lck
07/12/2023  06:20                130 $IX9E1TH.PNG
14/11/2023  07:05                374 $IY91PG0.lck
14/11/2023  06:55    <DIR>        $R0EBOXE.lck
14/11/2023  06:55    <DIR>        $R1BLN4C.lck
06/11/2023  17:57            203,332 $R1XPG46.docx
14/11/2023  07:04    <DIR>        $R21Y0B4.lck
14/11/2023  06:55    <DIR>        $R3KMVD9.lck
14/11/2023  07:05    <DIR>        $RAP249Y
14/11/2023  06:57    <DIR>        $RBEHK49
Press any key to continue . . .
08/11/2023  21:30    <DIR>        $RC2FUCT.lck
14/11/2023  07:04    <DIR>        $RF27WHD.lck
21/11/2023  06:03            272,770 $RL0CE51.pdf
12/09/2023  15:49            2,432 $RNM2166.lnk
21/11/2023  06:08            164,726 $RUACFEC.pdf
14/11/2023  07:03    <DIR>        $RUQG0CS.lck
21/11/2023  20:07            130,516 $RX9E1TH.PNG
14/11/2023  07:04    <DIR>        $RY91PG0.lck
12/09/2023  13:10                129 desktop.ini
               21 File(s)            778,001 bytes
               12 Dir(s)  9,315,942,400 bytes free
```



Anti Forensics – Deletion

Recycle Bin Forensics

- The original files pertaining to the \$I files are not visible in the Recycle Bin folder when \$I file is corrupted or damaged
(The attacker/insider deletes \$I files from the Recycle Bin)
- Check for the \$R files in the Recycle Bin directory
(to counter the anti-forensic technique used by the attacker)
- If the metadata files related to the original files are not present in the folder,
 - Recover the deleted files from Recycle Bin for further analysis.



Anti Forensics – Deletion

Deleting files/data is a common anti-forensics technique used by attackers.

- During your investigation, the file system metadata is not present. What will you do? Or How will you proceed further?

Discuss with your group and share your thoughts!!!

Duration: 5 Mins Discussion – 5 Mins Presentation

File carving refers to a technique that is used to recover deleted/lost files and fragments of files from the hard disk when file system metadata is missing.

Anti Forensics – Deletion

File Carving Techniques

- helps to ***extract data from a storage medium without any support from the file system*** used in the creation of the file.

- Understand – Unallocated Space

- Observe – Characteristics of file headers and footer

identify the files using file header and footer (the first and last few bytes)

- Identify – the elements

- Fragments of data present

- Deletion Technique used

- Type of Storage



Tools such as 010 Editor, CI Hex Viewer, Hexinator, Hex Editor Neo, Qiew, WinHex, etc.



File carving does not require file system structure to recover data from the disk whereas file recovery requires knowledge of the file system structure to recover deleted data.

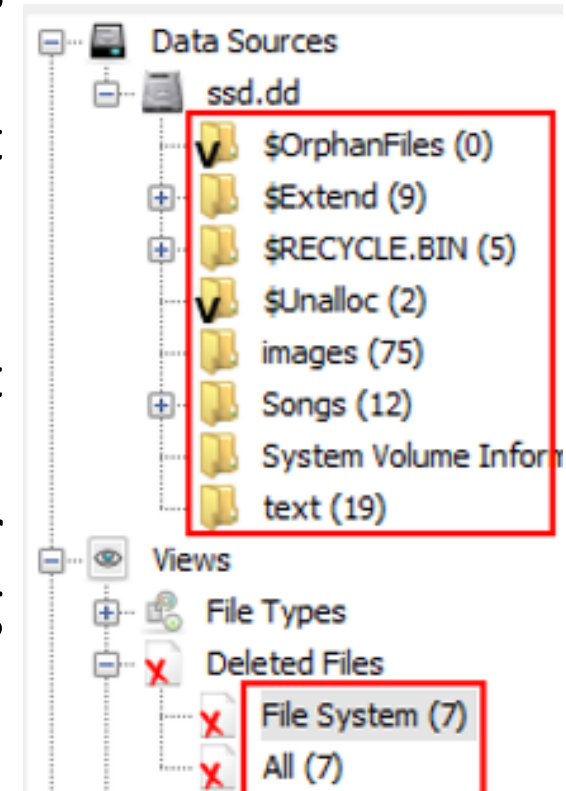
Anti Forensics – Deletion

File Carving – Windows SSD/HDD File

- **The recovery of deleted files in SSD becomes difficult as TRIM is enabled by default** (*mostly not possible*)
- With Autopsy, the file names are listed but the deleted data cannot be recovered
- Check status of the SSD's TRIM feature
- In TRIM disabled SSD's, you can perform file carving to recover lost data from the drive

Discuss with your group about TRIM Feature and share your thoughts!!! – Recommendations on Disabling and Enabling TRIM Feature. What it is?

Duration: 5 Mins Discussion – 5 Mins Presentation



Anti Forensics – Passwords

- **Cleartext Passwords**
- **Obfuscated passwords**
- **Password hashes**

This attack is applicable in two situations:

- In cryptanalysis (*it helps find out the decryption key for obtaining the plaintext from the ciphertext*)
- In computer security, (*it helps avoid authentication and access to a computer by guessing passwords*)

Dictionary Attacks

Methods to improve the success of a dictionary attack:

- Using a greater number of dictionaries, (technical dictionaries and foreign dictionaries etc)
- Using string manipulation

Anti Forensics – Passwords

- **Cleartext Passwords**
- **Obfuscated passwords**
- **Password hashes**

This attack

- involves testing all possible keys to recover the plaintext, which is the base for producing a particular ciphertext.
- Brute-force attacks need more processing power compared to other attacks. The detection of keys or plaintext at a rapid pace in a brute-force attack results in breaking of the cipher.

Brute Force Attacks

Some considerations for brute-force attack are as follows:

- It is a time-consuming process
- It can eventually trace all passwords
- An attack against Networking Technology (NT) hash is much harder against LAN Manager (LM) hash

Anti Forensics – Passwords

- **Cleartext Passwords**
- **Obfuscated passwords**
- **Password hashes**

This attack

- Is possible with some credible information about the password
- *Eg: Password Rule, Algorithms, Strings, Characters etc*

Rule Based Attack

- This technique involves brute-force, dictionary, and syllable attacks
- The attackers may use multiple dictionaries, brute-force techniques, or simply try to guess the password.

Anti Forensics – Passwords

BIOS Passwords

- A BIOS password protects the computer system from unauthorized access.
- In the BIOS setup, there are three types of passwords
 - System Password
 - Admin Password
 - HDD Password
- Bypassing BIOS password can unlock System and Admin password but not the HDD password
- Using a manufacturers' backdoor password to access the BIOS password
- Using password cracking software
- Resetting the CMOS using the jumpers or solder beads
- Removing the CMOS battery for at least 10 minutes

Anti Forensics – Steganography



Medium/ Message



Embedding
Function



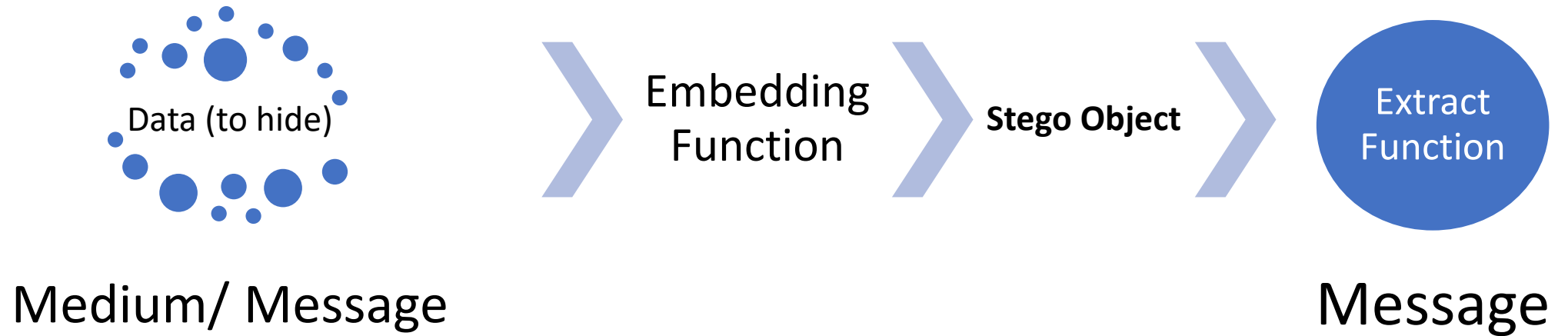
Stego Object



Message

- Steganography refers to the art of hiding data “behind” other data without the target’s knowledge
- It replaces bits of unused data in usual files such as graphic, sound, text, audio, video, etc. with some other surreptitious bits. The hidden data can be plaintext or cipher text, or it can be an image.
- Utilizing a graphic image as a cover is the most popular method to conceal data in files.
- Steganography is preferred by attackers because, unlike encryption, it is not easy to detect.

Anti Forensics – Steganography



Steganalysis

- Process of discovering the existence of the hidden information in a medium.
- Steganalysis is the reverse process of steganography
- A Steganalyst tries to detect the hidden messages embedded in images, text, audio and video carrier mediums using steganography.
- Locate encoded hidden message and recovers it if recovery is possible.
- It can identify the hidden message by comparing the differences in the bit patterns of files.

Anti Forensics – Steganography

Steganalysis

- Detection and Distortion of messages.
 - In the detection phase, relationships between the steganography tools, stego-media, cover, and message is observed.
 - In the distortion phase, the stego-media is manipulated to extract the embedded message and decides whether it is of any use or whether it should be removed altogether.
- The first step in steganalysis is to discover a suspicious image that may be harboring a message.
- There also are other types of attack against steganography such as **Stego-only, Known-stego, known-message, known-cover, chosen-message, and chosen-stego.**

Anti Forensics – Steganography

Steganalysis

- Challenges
- Suspect information stream may or may not have encoded hidden data
- Efficient and accurate detection of hidden content within digital images is difficult
- The message might have been encrypted before being inserted into a file or signal
- Some of the suspect signals or files may have irrelevant data or noise encoded into them

Anti Forensics – Steganography

Text Files

- The positions of characters are altered in the text files to hide the data.
- Investigators can detect these changes by looking for text patterns, the language used, height of lines and unusual number of blank spaces.
- A simple word processor can reveal text steganography sometimes as it displays the spaces, tabs, and other characters that distort the text's presentation during text steganography.

To detect text steganography

- Unusual patterns used in stego-object
- Appended extra spaces and invisible characters

Anti Forensics – Steganography

Image Files

- The information that is hidden in the image can be detected by observing changes in size, file format, last modified time stamp, and color palette of the file.

The following points can help detect image steganography:

- Too many display distortions in images
- Sometimes images may become grossly degraded
- Detection of anomalies when evaluating original images and stego-images with respect to color composition, luminance, pixel relationships, etc.
- Exaggerated "noise"
- Observe the LSB's
 - By using statistical analysis on the LSB, the difference between random values and real values can be identified.

Anti Forensics – Steganography

Audio Files

- Audio steganography is the process of embedding confidential information such as private documents and files in digital sound.
- Statistical analysis methods can be used for detecting audio steganography as it too modifies LSB.
- Especially, inaudible frequencies should be scanned for hidden information.
- Odd distortions and patterns can also indicate the presence of secret data.

Anti Forensics – Steganography

Video Files

- Detection of secret data in video files involves a combination of methods used in image and audio files.
- Special code signs and gestures help in detecting secret data.
- Both audio and video steganography are quite difficult to detect, as compared to the other types.
- Moreover, it is very hard to detect any type of steganography that has been well executed.
- However, careful analysis of audio and video signals for hidden information may increase the chances of detection.

Anti Forensics – Data Hiding

- Data hiding is making the data inaccessible.
- NTFS-based hard disks contain
 - bad clusters in a metadata file as \$BadClus and the MFT entry 8 represents these bad clusters.
 - \$BadClus is a sparse file, which allows attackers to hide unlimited data as they can allocate more clusters to \$BadClus to hide more data.
- Some hard disks have a **host protected area** (HPA) in which the developers can store data they want to protect (and hide) from normal use.
- The attackers use DPAs, DCOs, and slack spaces to hide data, which will not be visible to either BIOS or OS and requires special tools to detect and view.

Anti Forensics – Data Hiding

- ADS, or an alternate data stream, is a NTFS file system feature that helps users find a file using alternate metadata information such as author title.
- It allows files to have more than one stream of data, which are invisible to Windows Explorer and require special tools to view.
- Files/ Data/ Executables may be hidden and accessed when required using CL - Utility.
- An ADS contains metadata such as access timestamps, file attributes, etc.
- Investigators need to **find ADS and extract the information**.
 - Retrieving ADS can offer raw details of the file and execution of malware.
 - Use software tools to identify ADS files and extract the additional streams.

Anti Forensics – Program Packers

- Program packers are to hide their data. (*similar to cryptography*)
- The packers compress the files using various algorithms. Unless the investigators know the tool that has been used to pack the file and have a tool to unpack it, they will not be able to access it.
- Evidence files may be hidden into containers, (*making them hard to detect*)
- As an Investigator,
 - mount compound files.
 - Program packers that are password-protected is a challenge
 - You need to first decrypt the password to unpack the file.
- Intruders use packers to hide attack tools by reverse engineering or scanning techniques.

Anti Forensics – Program Packers

- Packers can carry executable files, malware, and other attack elements.
- In case of executable files, these programs carry unpackers built into them, which unpack the file when user tries to run it and installs the executable on the host system.
- Some of the widely used packers are UPX, PECompact, BurnEye, Exe Stealth Packer, Smart Packer Pro, etc.
- You can dynamically analyze these packed executables by running them in a controlled environment and observing their behavior.
- Packed programs that are not password-protected are vulnerable to static analysis.

Anti Forensics – Countermeasures

- Train and educate the forensic investigators about anti-forensics
- Validate the results of examination using multiple tools
- Impose strict laws against illegal use of anti-forensics tools
- Understand the anti-forensic techniques and their weaknesses
- Use latest and updated CFTs and test them for vulnerabilities
- Save data in secure locations
- Use intelligent decompression libraries to defend against compression bombs
- Replace weak file identification techniques with stronger ones

Mobile Phone Forensics

Digital Forensics
(ACCA7031)

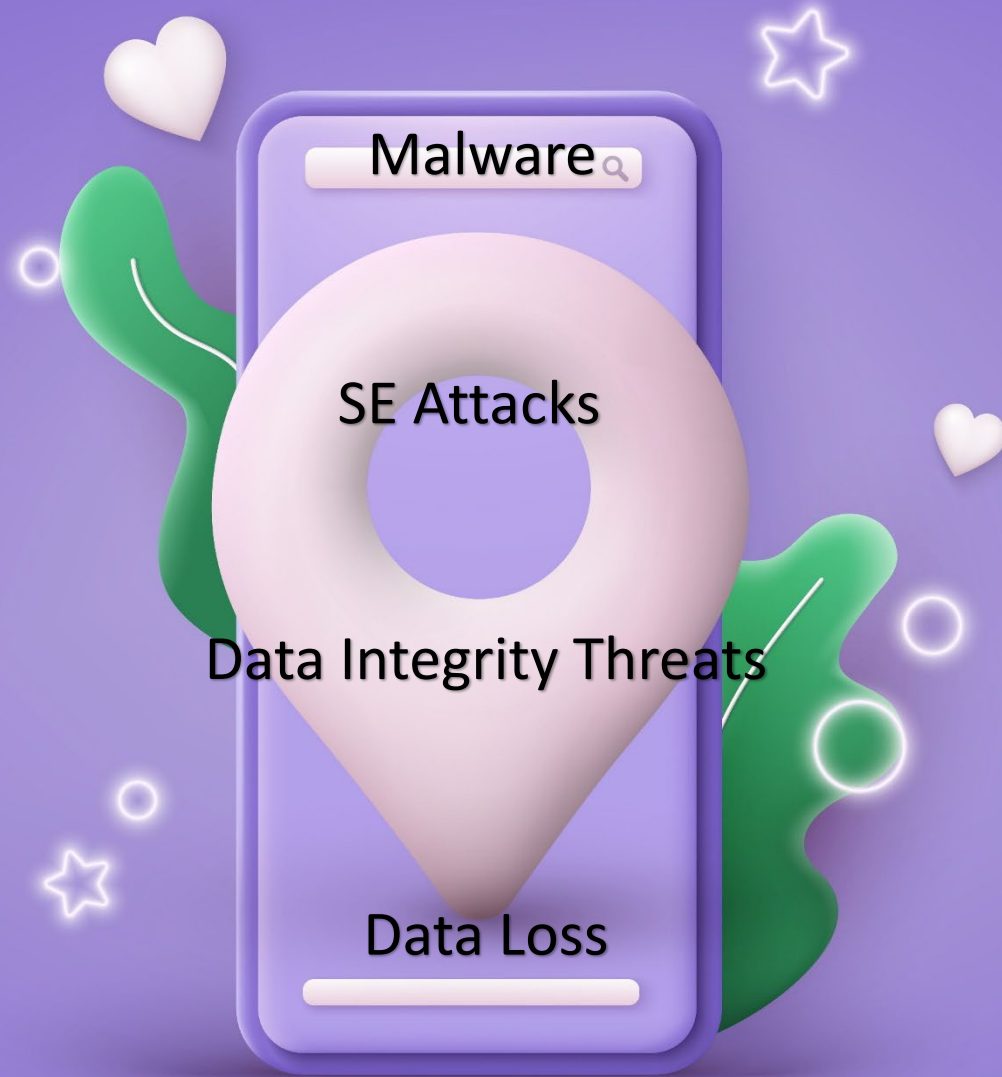
Applied Computing - WISA

➤ **Mobile Phone Forensics**

In continuation to our earlier lecture, we discussed about the History of Digital Forensics and its attributes. Understood the importance of Incident Response and discussed about the principles of Digital Forensics, its process, different roles and finally getting to understand the technology's role in the crime and the law framed around it to prevent various crimes.

Here, lets move forward and discuss about various digital forensics capabilities and the appropriate method to acquire data. We shall also discuss the challenges in acquiring data and the area in which keen attention is required. Our discussion this week will cover digital evidences storage formats, Acquisition Methods, Contingency Planning for Data Acquisition, Use and Validate Data Acquisition, RAID Acquisition, Remote Network Acquisition and Forensic Tools used for Data Acquisition.

Web and Network based Attacks



Resource Abuse

Understanding Mobile Device Forensics

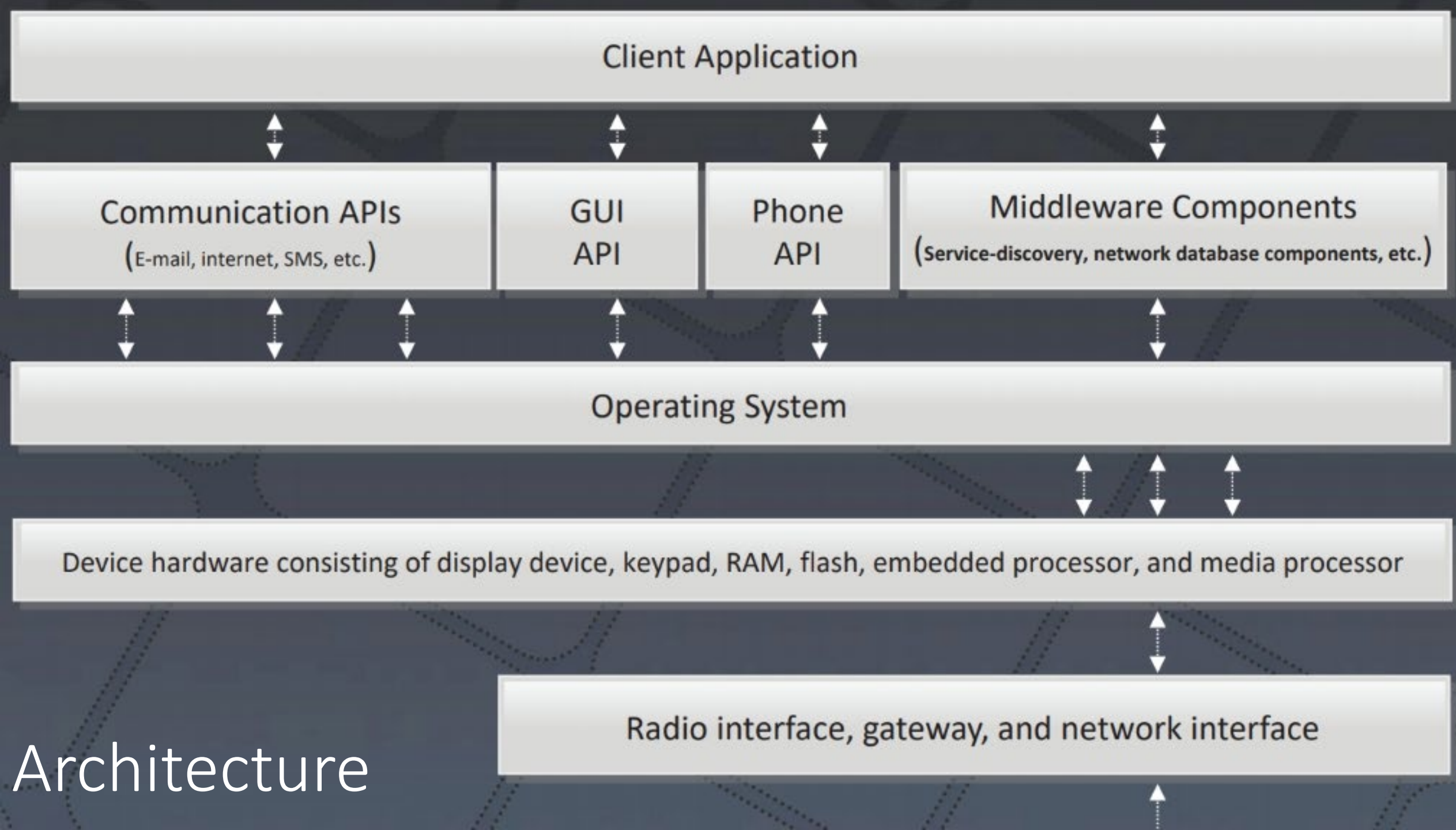
- Mobile phone forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions.
- It includes recovery and analysis of data from mobile device
 - internal memory, SD cards
 - SIM cards
- Mobile forensics aims to trace the perpetrators of crimes that involve the use of mobile phones

Mobile Hardware and Forensics

- Mobile device forensics is highly dependent on the underlying hardware of mobile devices
- Investigators need to take different approaches for mobile forensics depending upon the mobile hardware architecture
- Proprietary hardware of mobile devices makes forensics acquisition difficult
- Knowledge of mobile hardware also becomes essential in case of a broken or damaged device when it is not possible to access device using data ports

Mobile Hardware and Forensics

- A mobile operating system determines the functions and features available on mobile devices
- It manages the communication between the mobile device and other compatible devices
- This diversity in the mobile OS architecture may impact forensics analysis process
- Investigators require knowledge of underlying OS, architecture, and file systems of mobile device under investigation
- Knowledge of mobile OS booting process helps investigator to gain lower-level access



Architecture

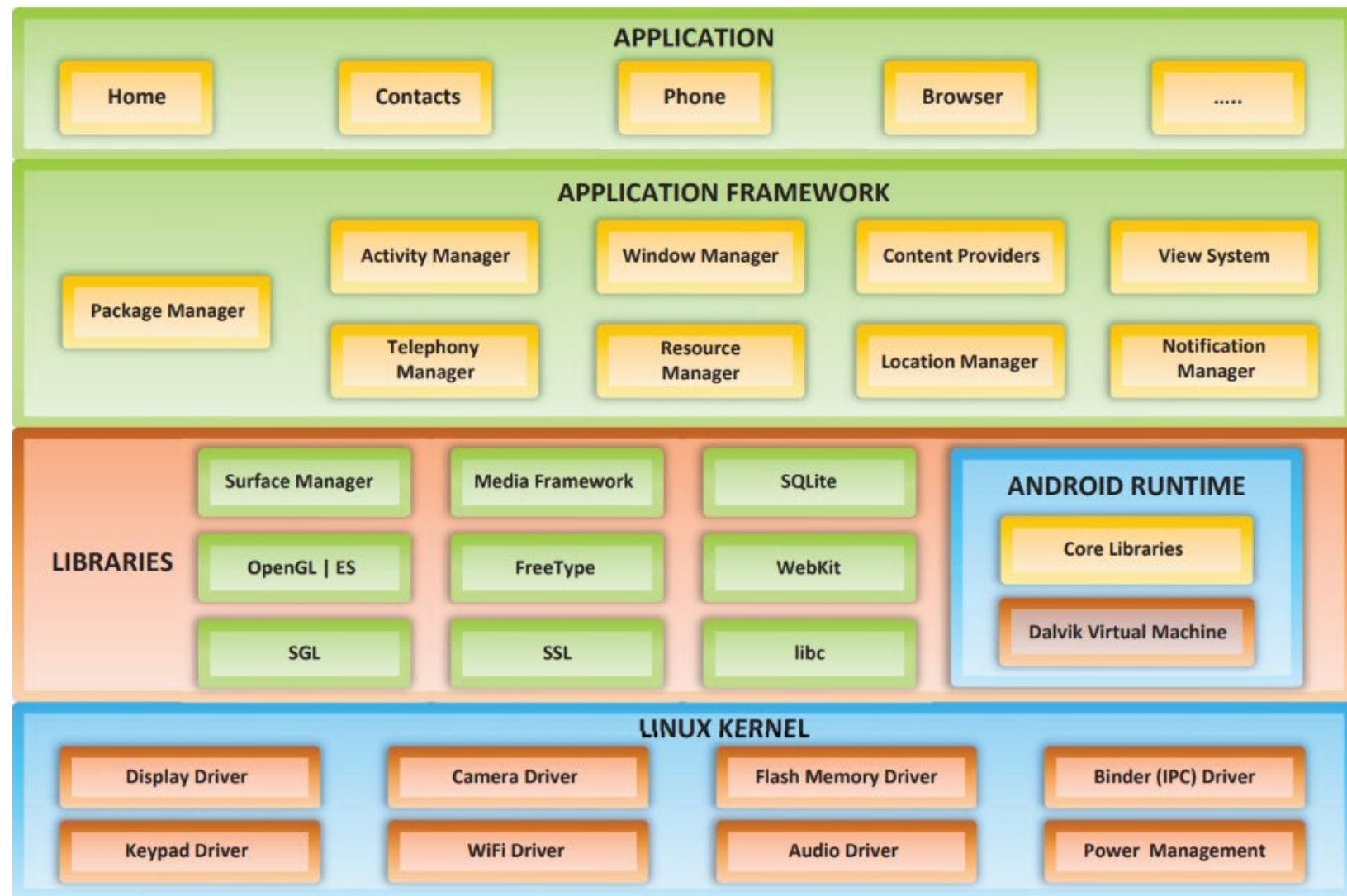
Android Architecture

User defined – Standard Applications

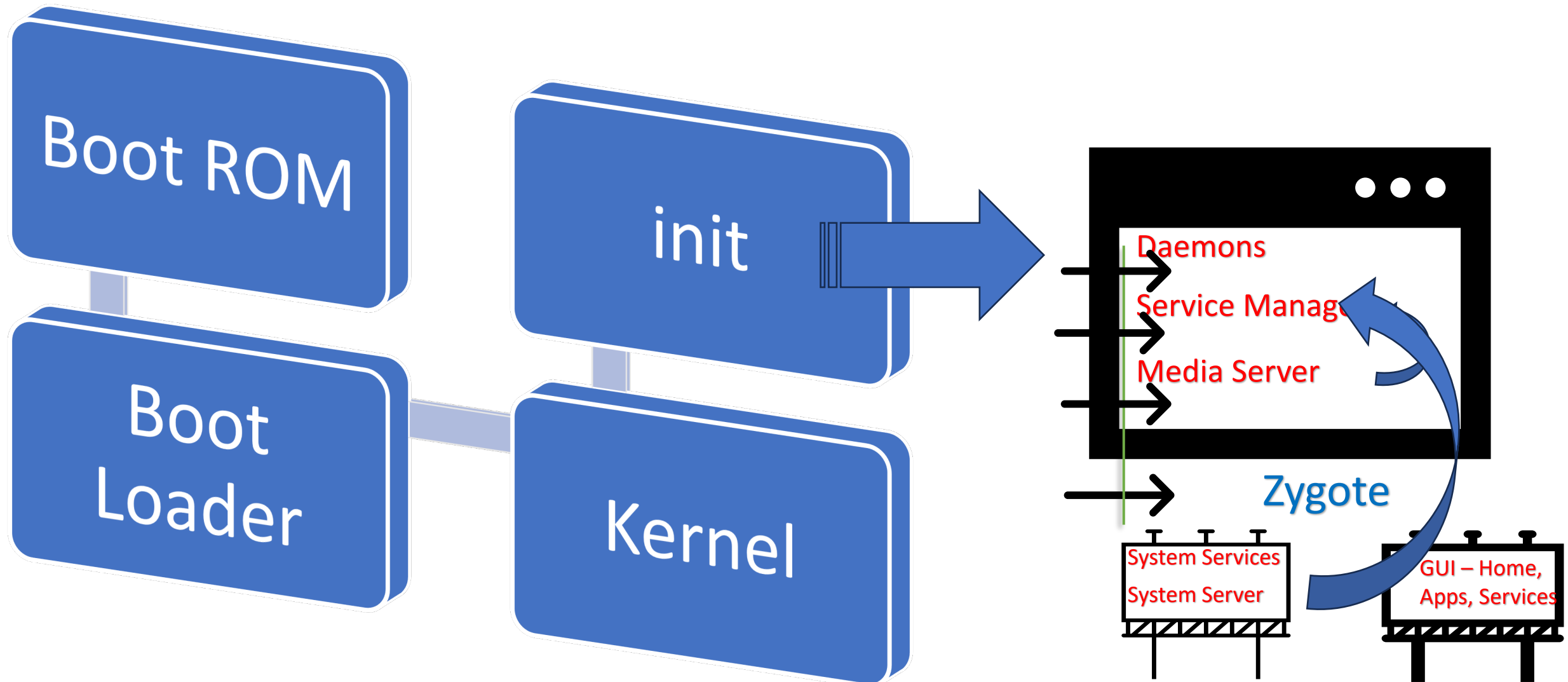
Support Applications – API Interfaces

Custom Built, Native Libraries

Interacting with the Hardware



Android Boot Process



iPhone Boot Process

Provides frameworks for iPhone app development

Map Kit, iAD, Game Kit, Events (Touch),
View Controllers, and UIKit

Provide audio, video, animation, and graphics capabilities
to the iPhone

Provide audio, video, animation, and graphics
capabilities to the iPhone

Provides foundation to upper layers

Threading, File Access, Preferences, Collections
(NSArray, NSDictionary, NSSet), Networking,
Address Book, and High Level Features
(iCloud, InApp Purchase, and SQLite)

Provides low-level services

Cocoa
Touch

Media
Services

Core
Services

Core OS

iPhone Hardware

Key Locations

Internal Memory

- RAM, ROM or flash memory (NAND / NOR) is used to store mobile phone's OS, applications and data

SIM Card

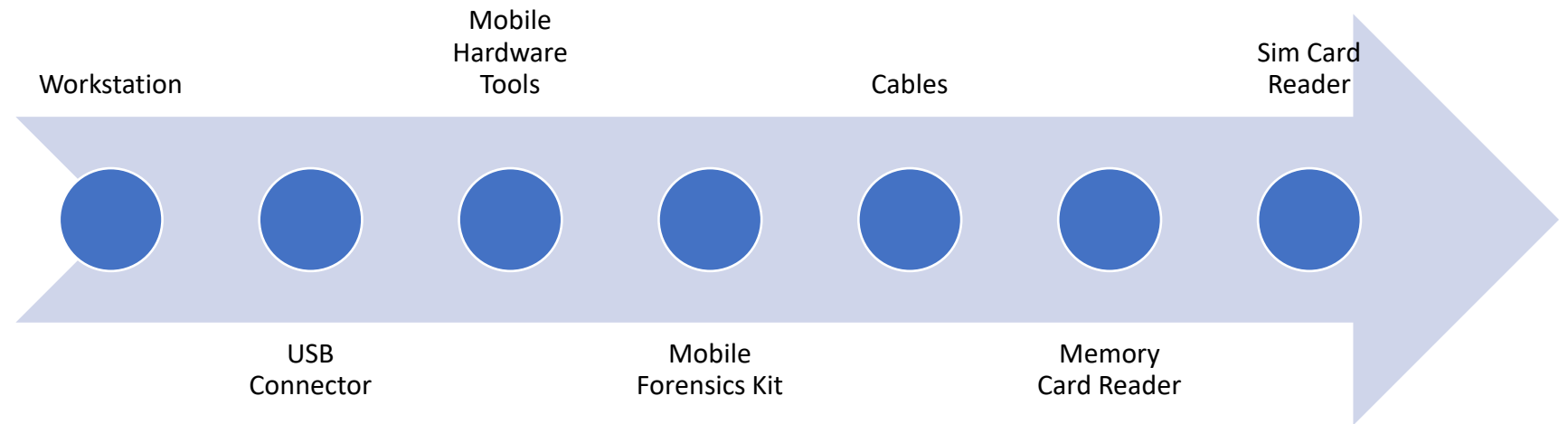
- Stores personal information, address books, messages, and service-related information

External Memory

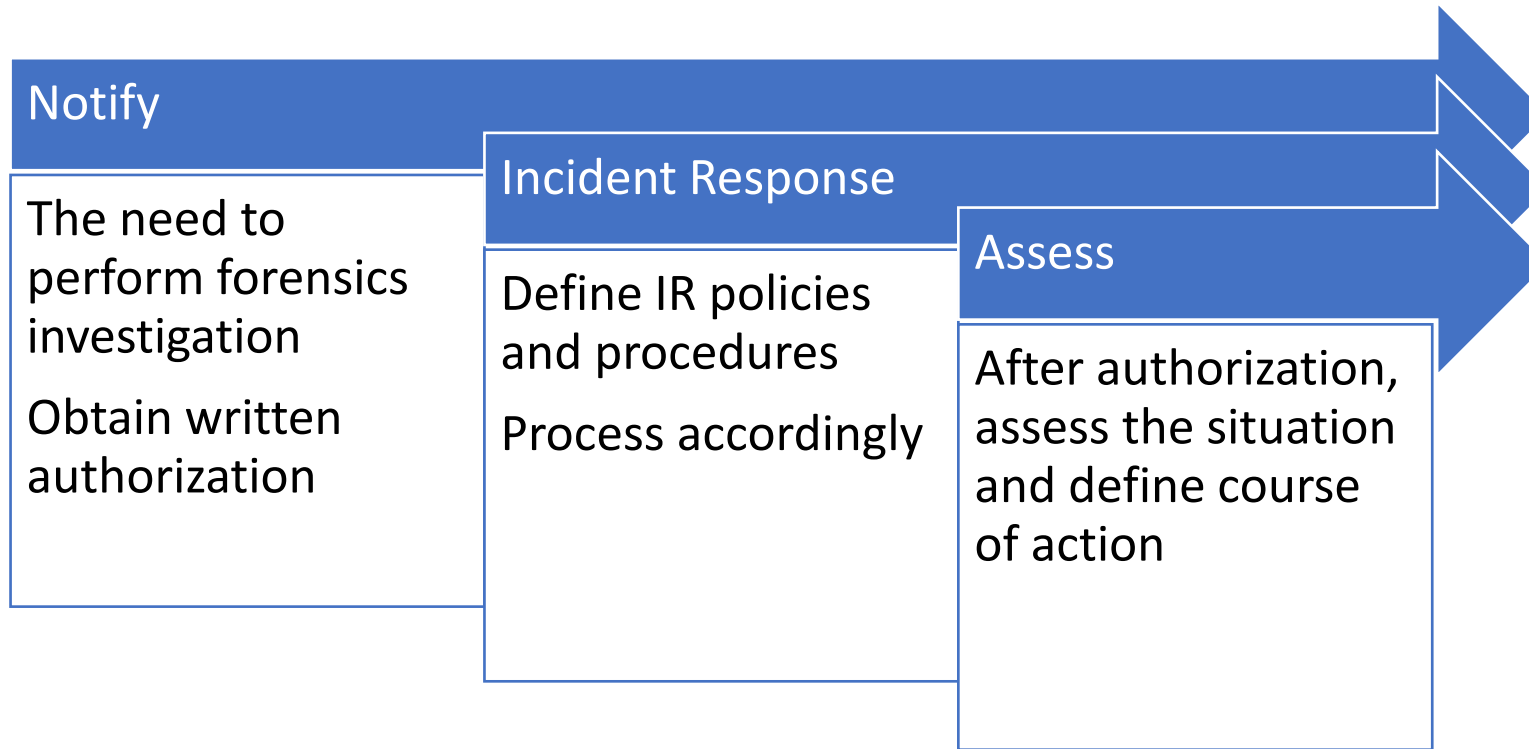
- Stores personal information such as audio, video, images, etc.

Investigations

- Build a Forensics Workstation
- Build the Investigation Team
- Review Policies and Laws
- Notify Decision Makers and Acquire Authorization
- Risk Assessment
- Build a Mobile Forensics Toolkit



Investigations



Risk Assessment

- To prevent new data from contaminating the evidence, **seal the device** in an isolation container properly
- **Do not use plastic bags** to carry out seized mobile device. Use recommended isolation containers
- **Consider the power state** of mobile device seized
- Expiration of the battery would be disastrous as important data may reside in **battery-dependent volatile memory**
- Handle and transport mobile devices carefully as they are **fragile** and can be **easily damaged**

Tools

- Selecting correct tools is the key.
- The mobile forensics toolkit includes both hardware and software tools required to recover and analyze data from mobile devices

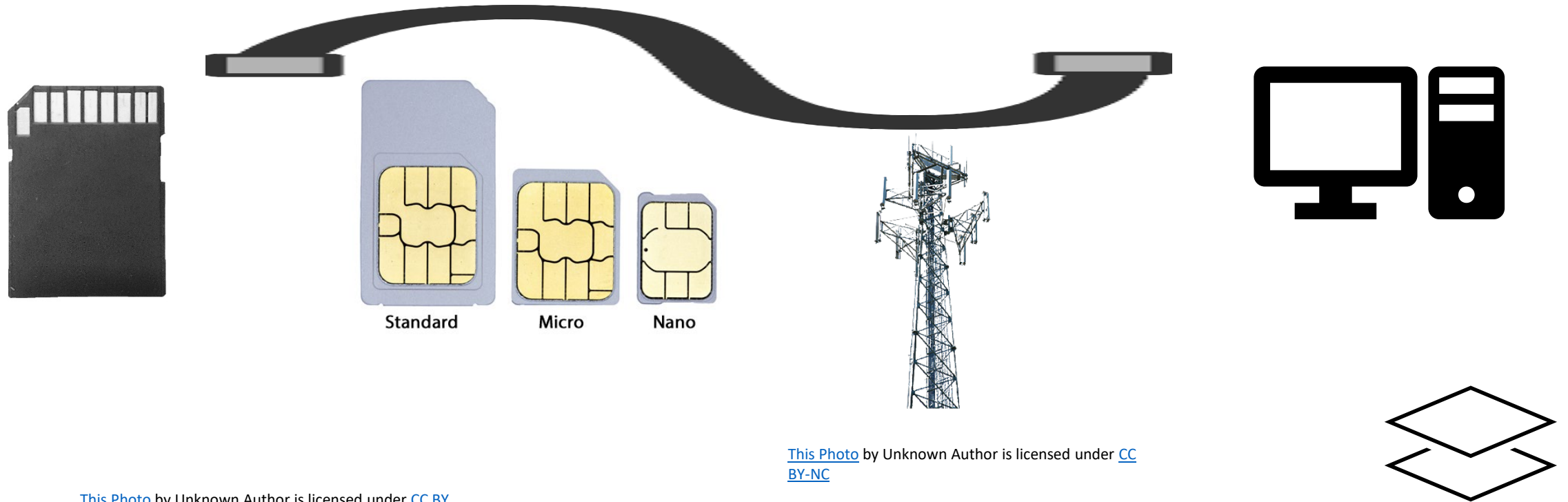
Few Tools are

- Cellebrite UFED System
- Secure ViewKit for Forensics
- DS-Device Seizure & Toolbox
- USB reader for SIM cards
- iGo
- DC Lab Power Supply 0 15V/3A
- Digital Display with Backlight
- Paraben's Phone Recovery Stick

- SEARCH Investigative Toolbar
- BitPim
- Oxygen Forensics Analyst
- Paraben's Sim Card Seizure
- MOBILedit! Forensic
- TULP2G
- iDEN Phonebook Manager
- SUMURI's PALADIN
- XRY Logical & XRY Physical

Process

- Selecting correct tools is the key.
- The mobile forensics toolkit includes both hardware and software tools required to recover and analyze data from mobile devices



Process

- **Collect and Preserve the Evidence**
 - Document the Scene
 - Imaging and Profiling
 - Acquire and Analyze Information
 - Generate Report
- Protect the integrity of traditional and electronic evidence
 - Prevent unauthorized users from entering at the scene and touching the evidence
 - Collect all the electronic devices found at the crime scene
 - Check whether the mobile device is connected to a computer
 - Confirm the power state of the devices by checking flashing light
 - Collect non-electronic evidence such as written passwords, handwritten notes, and computer printouts

Process

- **Collect and Preserve the Evidence**
 - Document the Scene
 - Imaging and Profiling
 - Acquire and Analyze Information
 - Generate Report
- The aim of the preservation step is to seize the suspect mobile phone and its associated peripherals without altering the data in it
 - It is the first step carried out prior to the actual investigation
 - It involves discovering, recognizing, documenting, and collecting the digital evidence obtained at the crime scene

Process

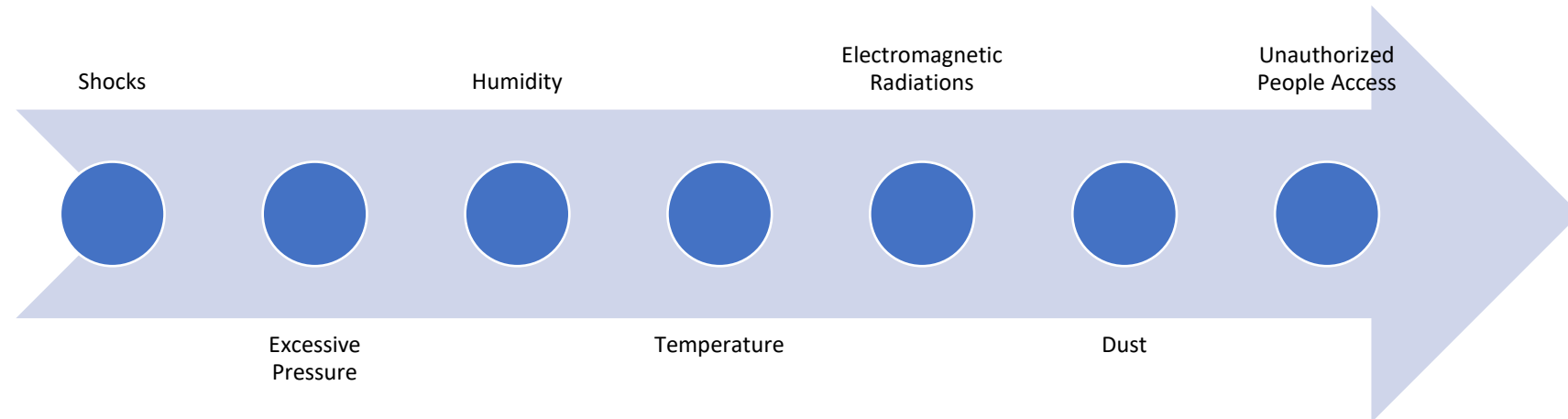
- Collect and Preserve the Evidence
- **Document the Scene**
- Imaging and Profiling
- Acquire and Analyze Information
- Generate Report
- Document all the electronic devices found at the crime scene
- Take photographs of all evidence at the scene, and write notes on what you have seen on the screen
- Document the state of the device during seizure
- Document any activity on the electronic devices found at the crime scene

- 🧠 Identify the brand, model, operating system, and the network service provider
- 🧠 It helps to choose an appropriate forensics tool for the data acquisition
- 🧠 Identify the type of connection used to connect to the forensics workstation
- 🧠 It may be a cable, Infrared, or Bluetooth
- 🧠 This depends upon the phone, forensics tool and acquisition conditions
- 🧠 Based on the mobile device model and the connection, select a forensics tool that have the following capabilities:

Usable, Comprehensive, Accurate, Deterministic, Verifiable

Process

- If the device is "ON", do not turn it "OFF". Turning it off could activate lockout feature
- Write down all information on display (photograph if possible)
- Power down prior to transport (take any power supply cord present)
- If the device is "OFF", leave it "OFF"
- Turning it on could alter evidence on device (same as computers)
- Mobile device should be protected from signal interruption, and data overwriting
- Use signal containment devices and bags to achieve and maintain network isolation



Process

- Collect and Preserve the Evidence
 - Document the Scene
 - **Imaging and Profiling**
 - Acquire and Analyze Information
 - Generate Report
- A forensics investigator **should not directly work on the original evidence.**
 - He/she should instead create a forensics image of the mobile device obtained at the crime scene
 - File carving and forensics analysis is conducted on forensics image in order to leave the actual evidence intact
 - Possible mobile phone storage for imaging:
 - Mobile phone memory
 - SD card memory
 - SIM card memory

Process

- Collect and Preserve the Evidence
- Document the Scene
- **Imaging and Profiling**
- Acquire and Analyze Information
- Generate Report

Locks

- Mobile phones use three types of phone lock schemes to prevent unauthorized user access
- If phone device obtained at a crime scene is in a locked state, the challenge of unlocking it arises
- Forensics investigator needs to bypass the phone lock to forensically investigate the mobile phone

ByPassing – Locks/ Passwords

Connect the device to the forensics workstation through USB Launch adb shell using ViaExtract Remove password.key file from android directory

Enable USB Debugging

Jail Break (If Necessary)

Process

- Collect and Preserve the Evidence
 - Document the Scene
 - Imaging and Profiling
 - **Acquire and Analyze Information**
 - Generate Report
- The seized mobile phone undergoes data acquisition and forensics imaging process at the forensics workstation
 - During the acquisition process, all possible data from internal and external memory of the mobile phone is extracted for forensics analysis
 - Data acquisition and forensics analysis requires:
 - Unlocking the device
 - Rooting or Jailbreaking of the device
 - Enabling USB debugging mode in the device

Process

- Collect and Preserve the Evidence
- Document the Scene
- Imaging and Profiling
- **Acquire and Analyze Information**
- Generate Report
- Cellular Data Acquisition
- SIM File System Acquisition
- Logical Acquisition
- Physical Acquisition
- File System Acquisition

Code Division Multiple Access (CDMA) | Enhanced Data Rates for GSM Evolution (EDGE) |

Integrated Digital Enhanced Network (iDEN) | General Packet Radio Service (GPRS) | Global System for Mobile Communications (GSM)

High Speed Downlink Packet Access (HSDPA) | Time Division Multiple Access (TDMA) | Universal Mobile Telecommunications System (UMTS) | Unlicensed Mobile Access (UMA)

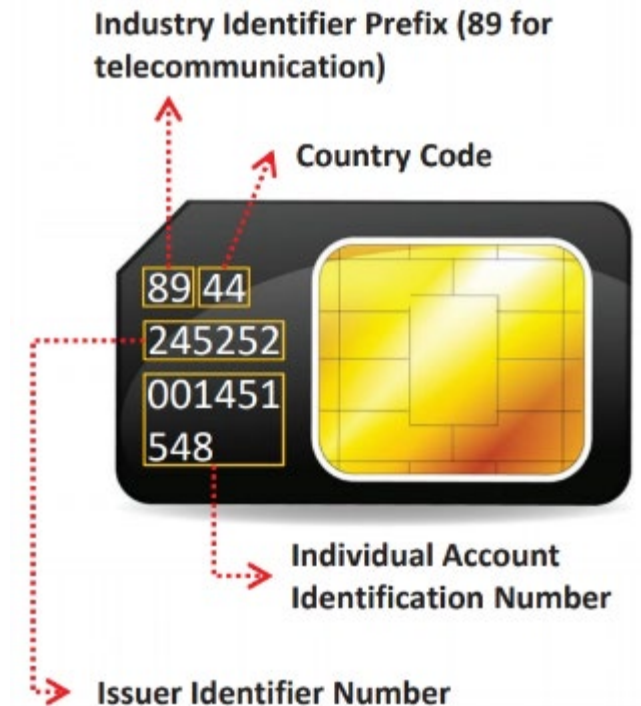
Process

- Collect and Preserve the Evidence
 - Document the Scene
 - Imaging and Profiling
 - **Acquire and Analyze Information**
 - Generate Report
 - Cellular Data Acquisition
 - SIM File System Acquisition
 - Logical Acquisition
 - Physical Acquisition
 - File System Acquisition
-
- Service provider data can act as back up evidence for the mobile forensics' investigator
 - It is useful when the attacker or owner of the mobile phone has deleted call history and/or text messages from the device to wipe out evidence
 - It can also be required in the following cases:
 - When recovering of deleted data is not possible
 - When location-based services are not turned ON in the phone

Process

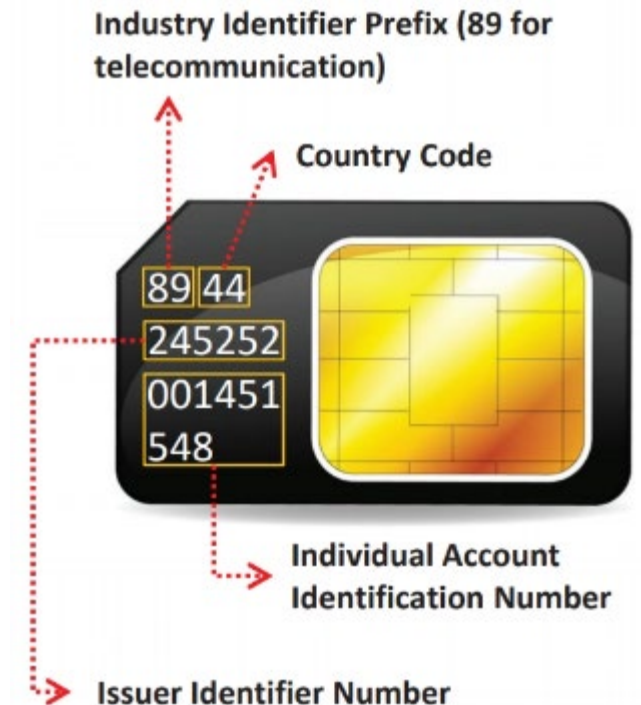
- Collect and Preserve the Evidence
 - Document the Scene
 - Imaging and Profiling
 - **Acquire and Analyze Information**
 - Generate Report
- Cellular Data Acquisition
 - SIM File System Acquisition
 - Logical Acquisition
 - Physical Acquisition
 - File System Acquisition

- SIM is a removable component that contains essential information about the subscriber
- It has both volatile and non-volatile memory
- The file system of a SIM resides in non-volatile memory
- The SIM's main function entails authenticating the user of the cell phone to the network to gain access to subscribed services



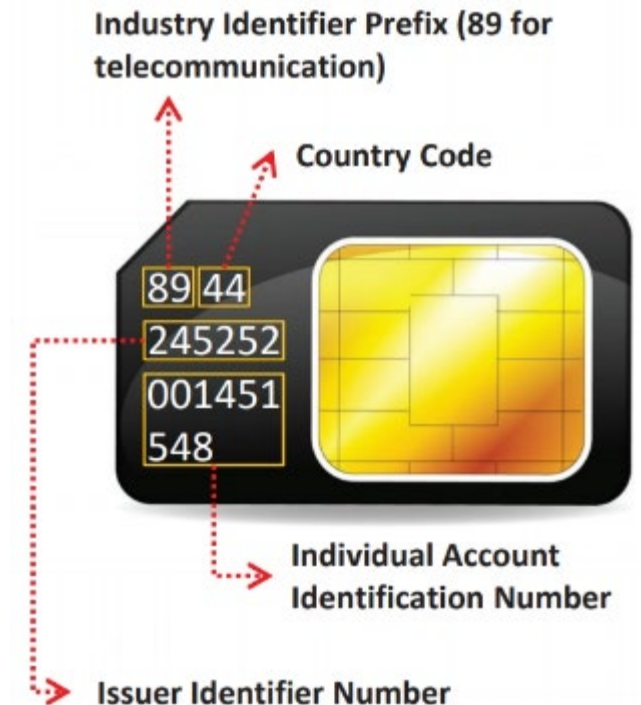
Process

- Collect and Preserve the Evidence
 - Document the Scene
 - Imaging and Profiling
 - **Acquire and Analyze Information**
 - Generate Report
-
- IMEI is a 15-digit number that indicates the manufacturer, model type, and country of approval for GSM devices
 - First eight digits, known as the Type Allocation Code (TAC), give the model and origin
 - For powered on GSM and UMTS phones, the IMEI can be obtained by keying in *#06#
- Cellular Data Acquisition
 - SIM File System Acquisition
 - Logical Acquisition
 - Physical Acquisition
 - File System Acquisition



Process

- Collect and Preserve the Evidence
 - Document the Scene
 - Imaging and Profiling
 - **Acquire and Analyze Information**
 - Generate Report
-
- Cellular Data Acquisition
 - SIM File System Acquisition
 - Logical Acquisition
 - Physical Acquisition
 - File System Acquisition
-
- Duplicating a SIM card for further investigation in order to avoid accidental tampering of original SIM data



Process

- Collect and Preserve the Evidence
 - Document the Scene
 - Imaging and Profiling
 - **Acquire and Analyze Information**
 - Generate Report
- Cellular Data Acquisition
 - SIM File System Acquisition
 - Logical Acquisition
 - Physical Acquisition
 - File System Acquisition
- Logical acquisition involves creating a bit-by-bit copy of logical storage of mobile phone
 - Logical storage includes data stored within mobile files and directories
 - Mobile data is extracted through mobile device's OS, using a known set of commands

Process

- Collect and Preserve the Evidence
 - Document the Scene
 - Imaging and Profiling
 - **Acquire and Analyze Information**
 - Generate Report
 - Cellular Data Acquisition
 - SIM File System Acquisition
 - Logical Acquisition
 - Physical Acquisition
 - File System Acquisition
-
- Physical acquisition involves creating a bit-by-bit copy of data stored in the internal flash memory of mobile phone
 - It extracts maximum amount of data directly from the mobile device's flash memory(s)
 - It can also extract hidden or deleted data from flash memories
 - It is the most difficult extraction as manufacturers of mobile devices often do not allow arbitrary reading of the device's memory

Process

- Collect and Preserve the Evidence
 - Document the Scene
 - Imaging and Profiling
 - **Acquire and Analyze Information**
 - Generate Report
- Cellular Data Acquisition
 - SIM File System Acquisition
 - Logical Acquisition
 - Physical Acquisition
 - File System Acquisition
- Logical acquisition **cannot help in extracting deleted data from the file and directory of mobile phone**
 - File system acquisition helps in recovering and extracting deleted data
 - Moreover, the file system acquisition shows file structure, application data, and web artifacts available in the mobile

Process

- Collect and Preserve the Evidence
- Document the Scene
- Imaging and Profiling
- **Acquire and Analyze Information**
- Generate Report

- File carving involves recovering deleted or hidden data from mobile phones
- Persons involved in the incident may delete certain data, and wipe out potential evidence from the mobile phone
- You should try to recover such deleted data for forensics analysis

Use file carving tools to recover:

- Keyboard caches
- Deleted photos
- Browser cache items and other personal data
- Call history data
- Map tiles from maps application
- Cached, and deleted email messages
- SMS messages with timestamp data Deleted voicemails

Process

- Collect and Preserve the Evidence
 - Document the Scene
 - Imaging and Profiling
 - **Acquire and Analyze Information**
 - Generate Report
- After logical, physical, and file system acquisition, forensics examination and analysis is carried out on the extracted data
 - It involves **finding out source of evidence from information obtained by extraction**

The forensics Examiner should investigate:

- ❖ Mobile phone data artifacts such as contacts, call history, browser, SMS/MMS, and geolocation
- ❖ Raw data artifacts
- ❖ Timeline of activities

Process

- Collect and Preserve the Evidence
 - Document the Scene
 - Imaging and Profiling
 - Acquire and Analyze Information
 - **Generate Report**
- The results obtained in all the steps of forensics process needs to be presented in a **prescribed standard format**
 - A forensics report should include the complete forensics investigation process followed along with supporting documents such as **photographs, notes, and signatures of specialists**
 - A forensics tool is used to prepare reports to present the forensics result in a prescribed format

Your report must include:

Summary, Objectives, Date and time the incident allegedly occurred, Date and time the incident was reported to agency personnel, Name of the person or persons reporting the incident, Examination start date and time, The physical condition of the phone, Photos of the phone and individual components, Phone status when received turned on or off, Make and Model, Mobile Subscriber International ISDN Number (MSISDN), Integrated Circuit Card ID (ICCID), Service Provider Name (SPN), Abbreviated dialing numbers, Last Numbers received.

Process

- Collect and Preserve the Evidence
 - Document the Scene
 - Imaging and Profiling
 - Acquire and Analyze Information
 - **Generate Report**
- The results obtained in all the steps of forensics process needs to be presented in a **prescribed standard format**
 - A forensics report should include the complete forensics investigation process followed along with supporting documents such as **photographs, notes, and signatures of specialists**
 - A forensics tool is used to prepare reports to present the forensics result in a prescribed format

Your report must include: Last Numbers dialed, Missed calls, Short Message Services (SMS), Calendar entries, Photographs stored in the handset, Video stored in the handset Smart Media/ Compact Flash, MMS, International Mobile Subscriber Identity (IMSI), Mobile Country Code (MCC), Mobile Network Code (MNC), Mobile Subscriber Identification Number (MSIN), Preservation of the evidence, Investigative techniques, Tools used for the acquisition, Tools used for the examination, Data found during the examination, Notes from peer review, Supporting expert opinion

References

- EC Council – CHFI V10 Ebook
- Bossler, Adam M._ Holt, Thomas J._ Seigfried-Spellar, Kathryn C –
- Cybercrime and digital forensics_ an introduction-Routledge (2017_2018)
- Digital Forensics and Incident Response:
- A practical guide to deploying digital forensic techniques in
- response to cyber security incidents
- Jason Sachowski - Digital Forensics and Investigations –
- People, Process, and Technologies to Defend the Enterprise
- Whitcomb, C. (2007). The evolution of digital evidence in
- forensic science laboratories. The Police Chief, 74(11).