



Prifysgol Cymru

Y Drindod Dewi Sant

University of Wales

Trinity Saint David

Trawsnewid Addysg, Trawsnewid Bywydau
Transforming Education, Transforming Lives

Digital Forensics



Digital Forensics *ACCA7031*

Applied Computing - WISA



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

Trawsnewid Addysg, Trawsnewid Bywydau
Transforming Education, Transforming Lives

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 today's lecture 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*



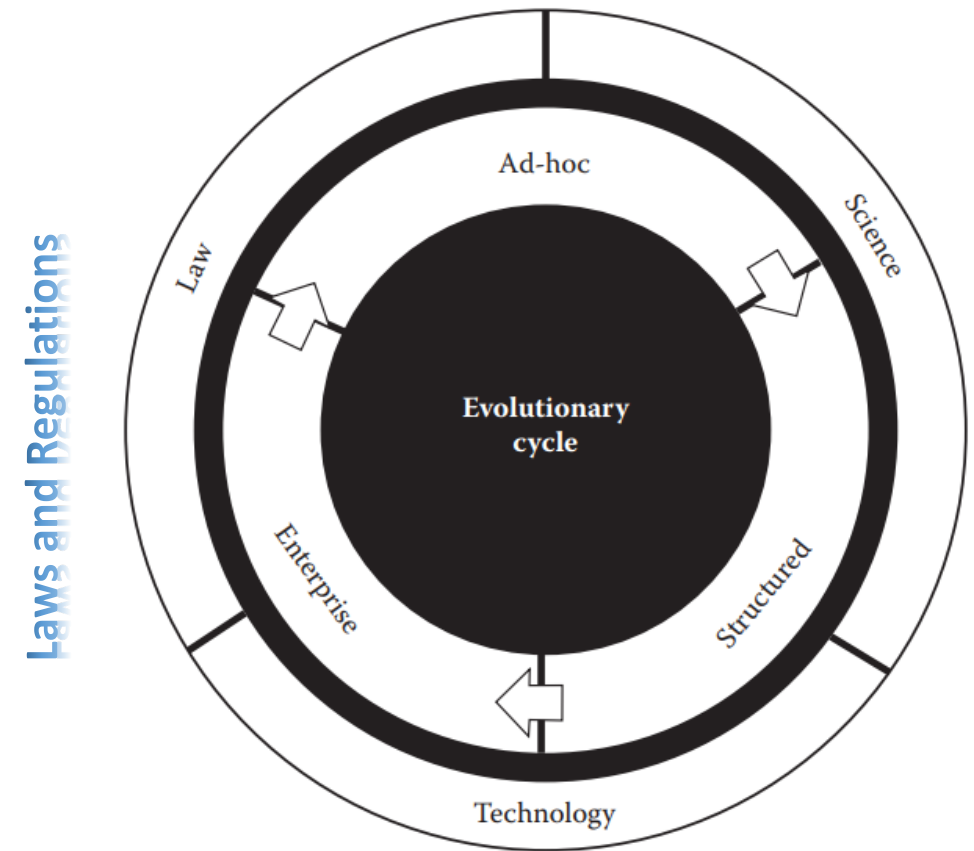
*LEGAL
COMPLIANCE*

Today's 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**

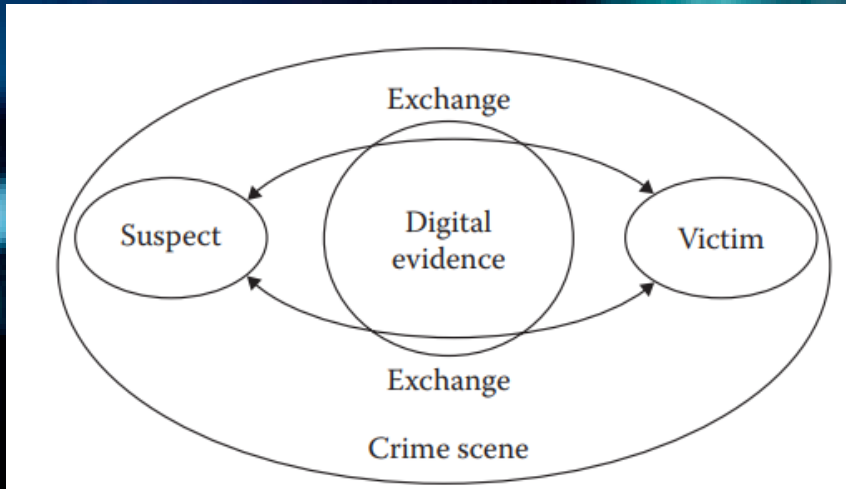
Technological Evidence & Legal Precedence



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?

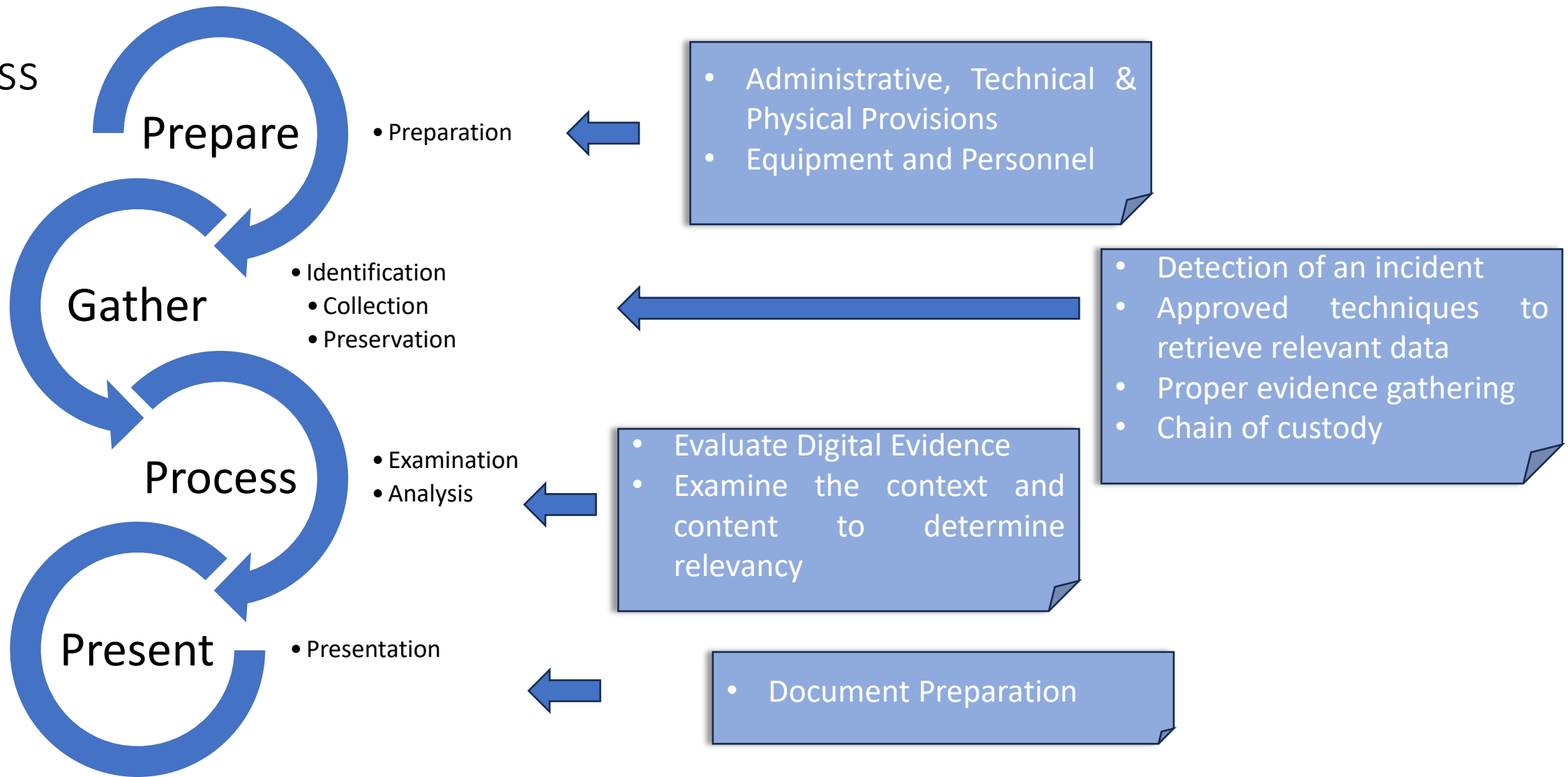
How do you think it will be helpful for your DF Investigations?

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

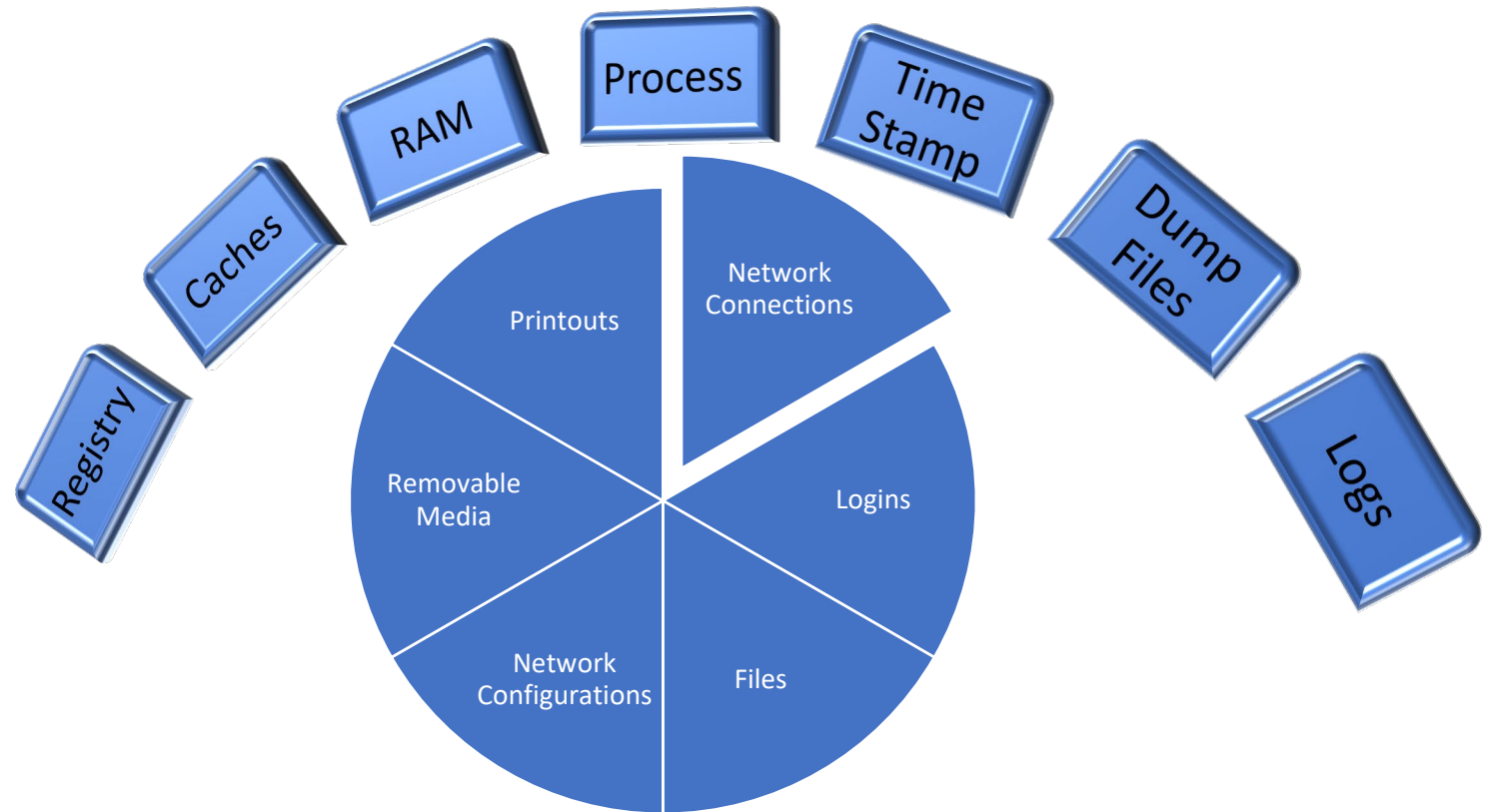
- Process and Procedure (Framework, SOP)
- Education, Training and Awareness
- Technology and Toolsets

- 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.



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

Trawsnewid Addysg, Trawsnewid Bywydau
Transforming Education, Transforming Lives

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](#)



Trans

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

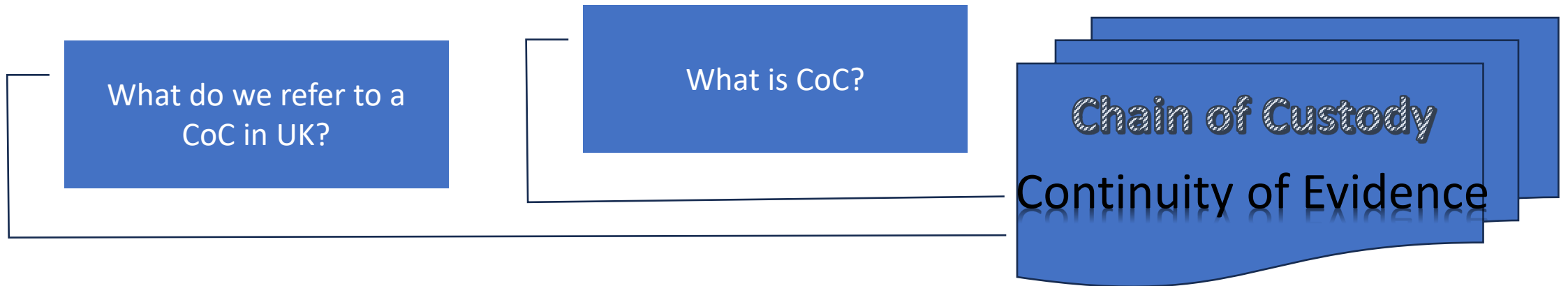
- ✍ **Need:** Optimally use digital evidence.
- ✍ **Effectiveness:** limited time and minimal investigation costs.
- ✍ **Include:** Technical and Non-Technical actions
- ✍ **Establish:** Specific incident response procedures
- ✍ **Employ:** Designated Trained Personnel

“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



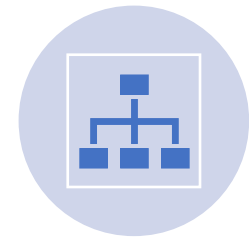
EXAMINER/ANALYST



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.

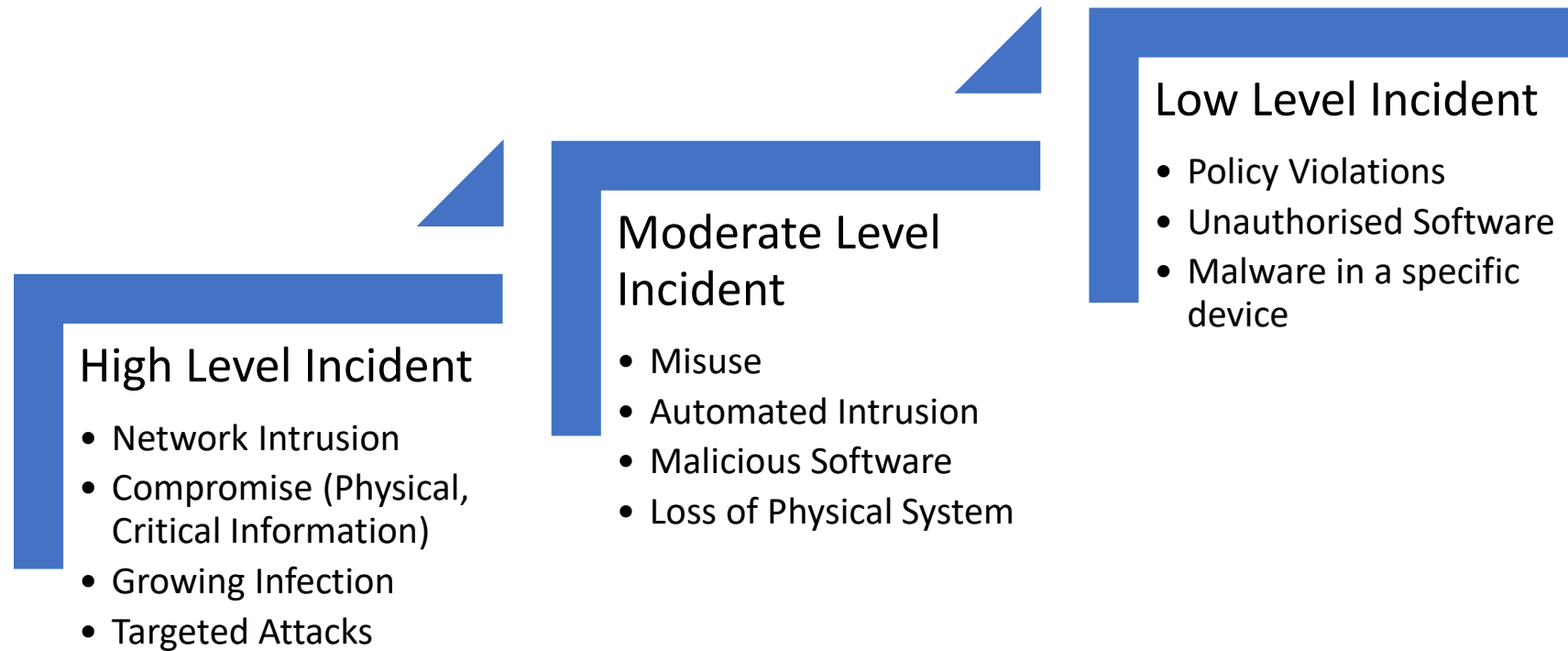
Incident Response

Computer Security Incident Response Team (CSIRT)

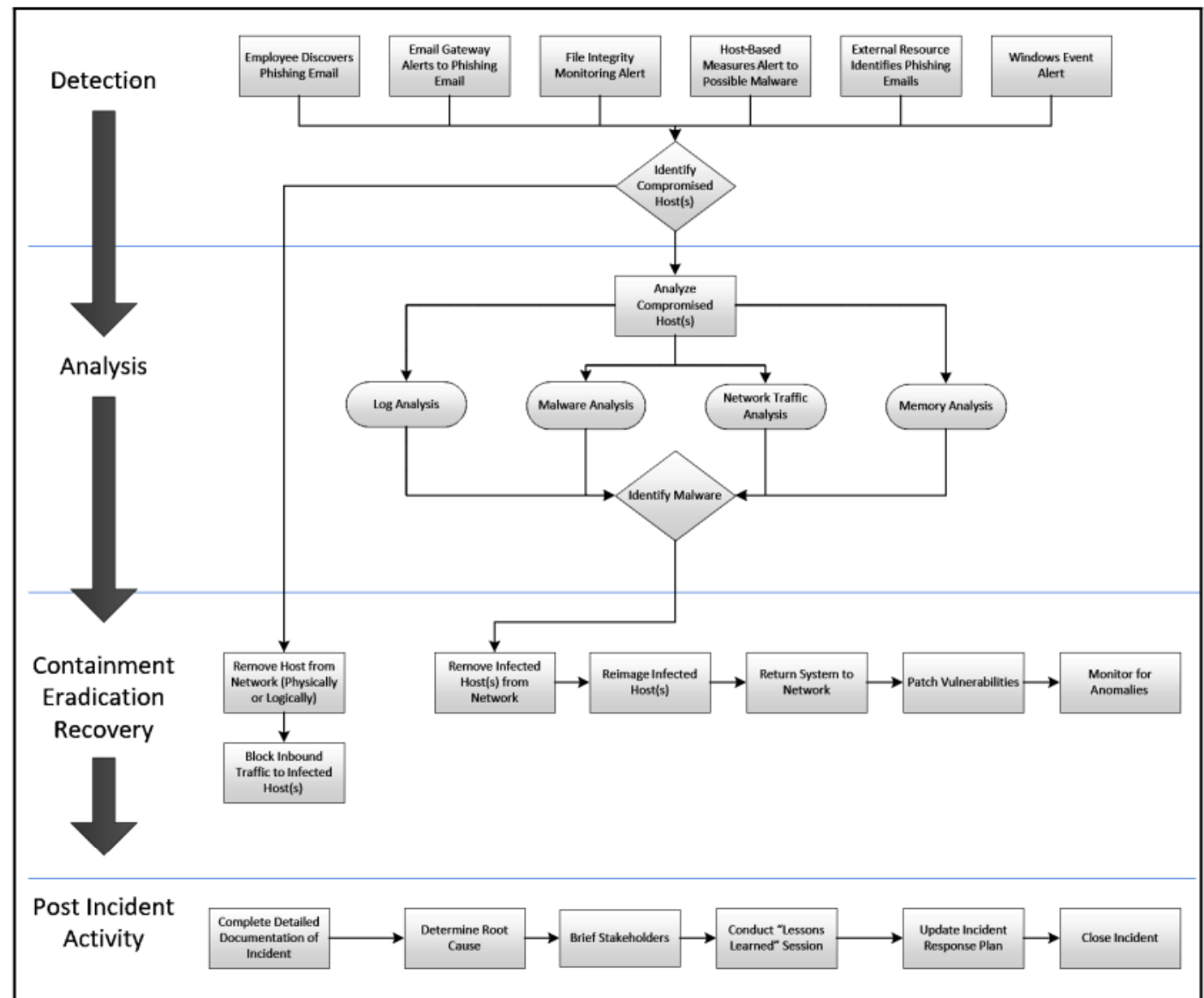
Roles

- 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.

Any Questions?