



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

Today's Discussion

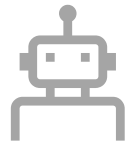
During this week, we shall get introduced to this module, discuss the plan, coursework and the tools to be used in this module.

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

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



Digital Evidence and
Law Enforcement



Security Vs Privacy



Forensic
Investigator



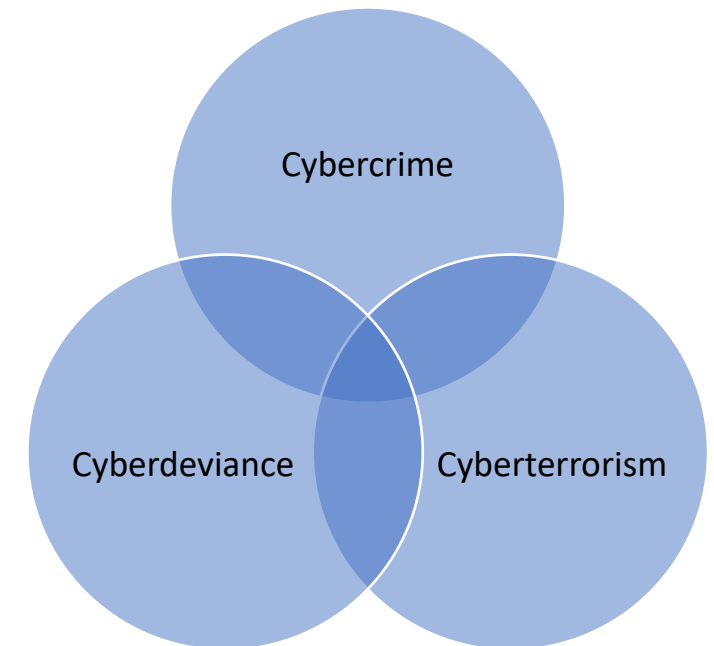
Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Trawsnewid Addysg, Trawsnewid Bywydau
Transforming Education, Transforming Lives

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."

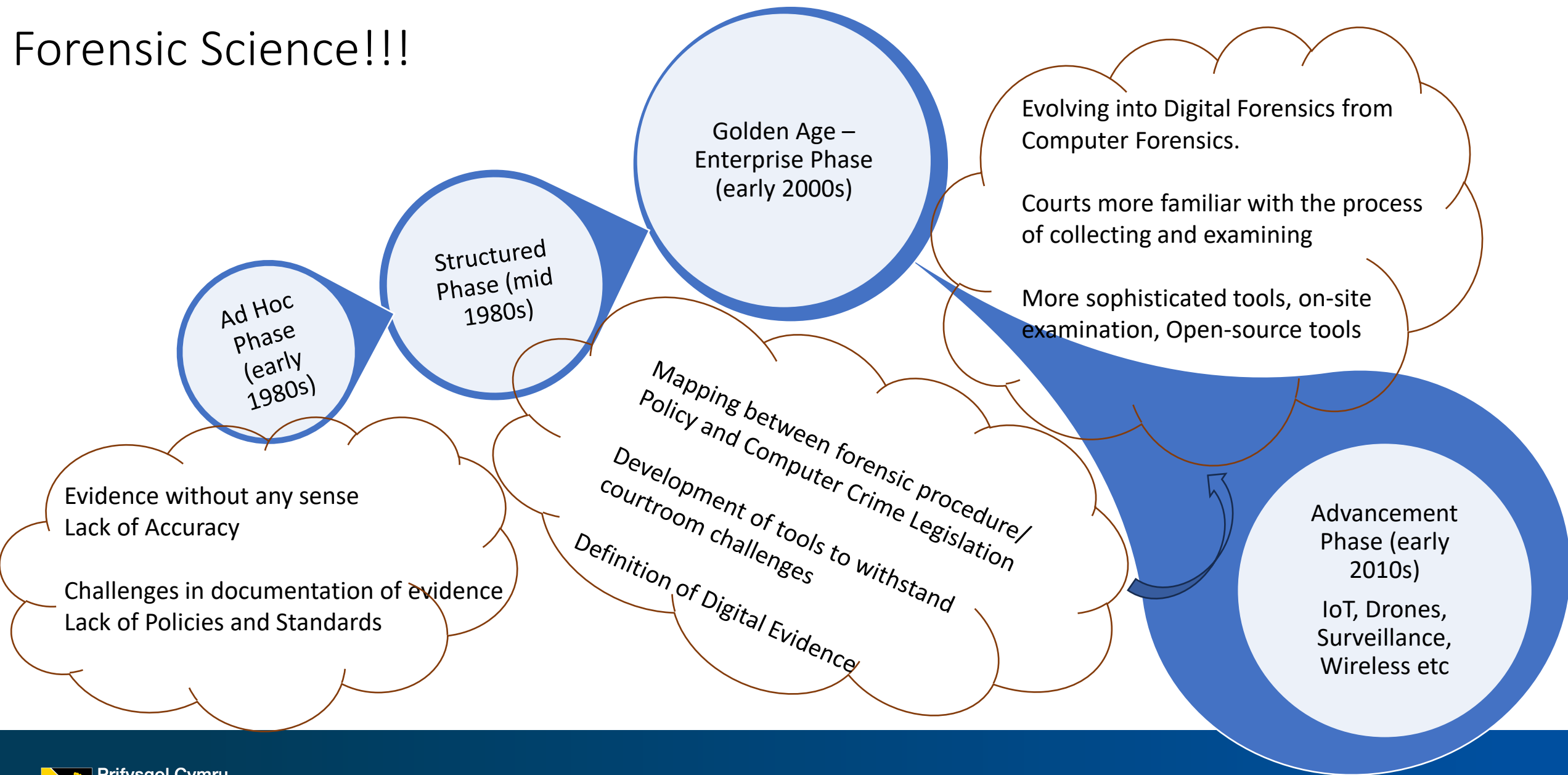
Forensic Science!!!

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.



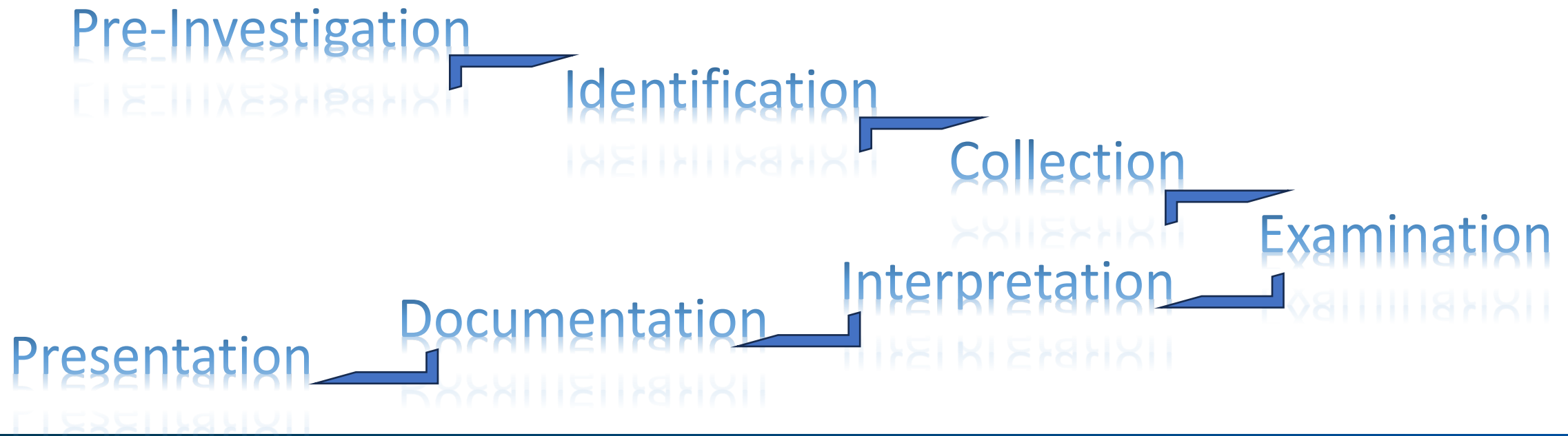
[This Photo](#) by Unknown Author
is licensed under [CC BY-SA](#)

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

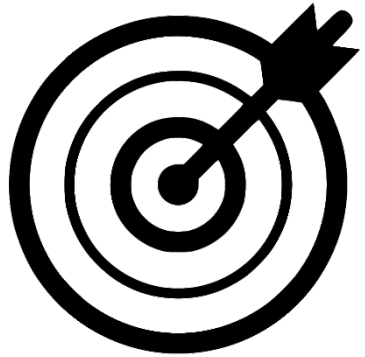
Forensic Science!!!

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)



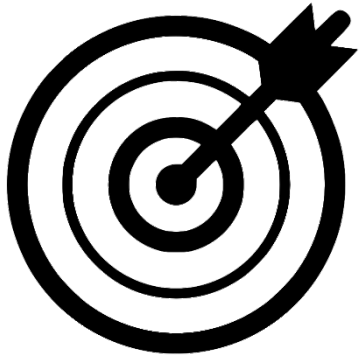
Objectives



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

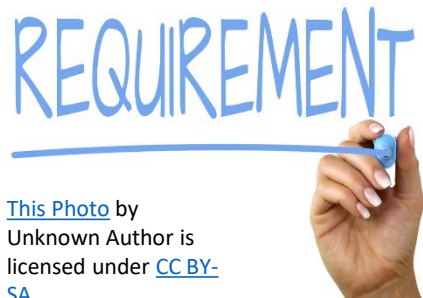
- ✍ Identify, gather, and preserve the **evidence** of a cybercrime
- ✍ Track and prosecute the perpetrators in a **court of law**
- ✍ Interpret, document, and present the evidence such that it is **admissible during prosecution**
- ✍ Estimate the **potential impact of malicious activity** on the victim 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.

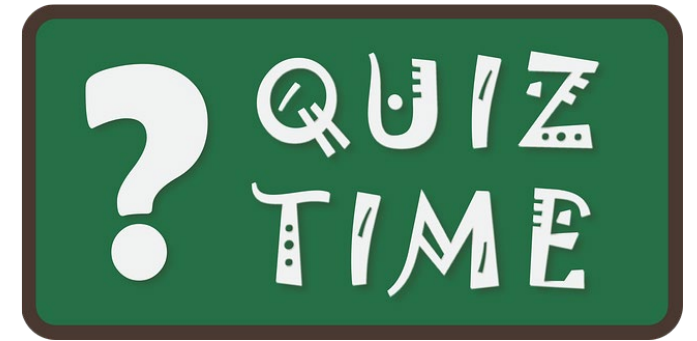
Recall...

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.



A photograph of a coffee shop table. In the foreground, there is a white cup of latte with a leaf-shaped foam design on a white saucer. Behind it is a clear glass bottle of water and a clear glass. The table is made of wood. A white silhouette of a person's head and shoulders is overlaid on the right side of the image, pointing towards the text.

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

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



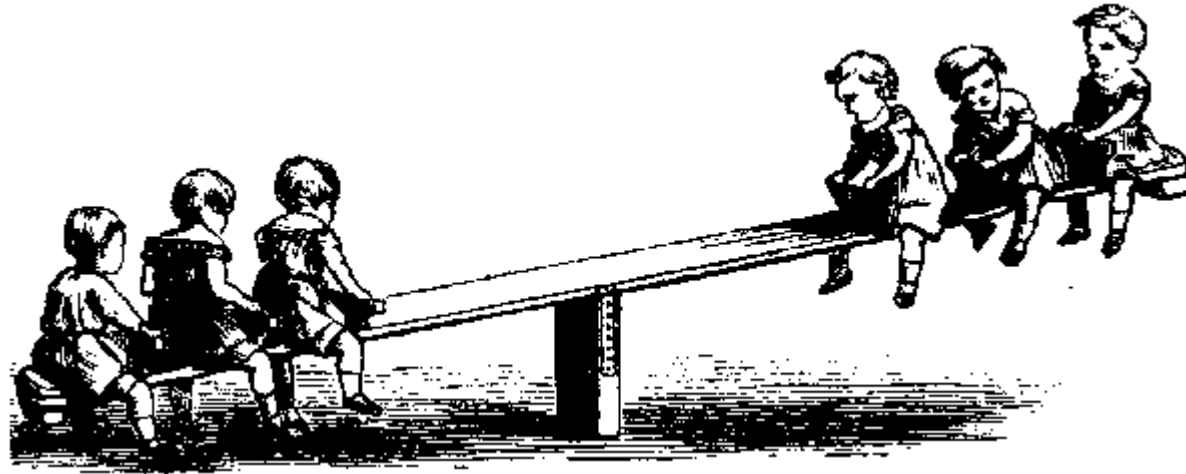
Privacy is the freedom from being observed or disturbed by other people, or the state of not being observed or disturbed in this way. It is the right to keep one's personal matters and relationships secret

(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**

Any Questions?

References

- **EC-Council CEH**
- **Cisco Networking Academy**
- **Tevel Cyber Corps**
- **Certified Ethical Hacker (CEH) Version 10 Cert Guide, 3rd edition**
- **Wikipedia**
- **Other website sources given in this presentation**
- *** The intension of usage is for Educational Purpose Only**