Week 2

Computer Forensics
Semester 2 -2024

Lecturer : Dr. Mbemba HYDARA

Week 2

Session 2:
Computer Forensics and admissibility of Evidence

2

Computer Forensics

- Application of investigation and analysis to collect, preserve, analyze, and present digital evidence in a court of law.
- Specialized tools and techniques are used to recover data from digital devices such
- Computers, mobile phones, and storage media.

Evolution of Computer Forensics

- Computer forensics has evolved significantly since its inception in the 1980s
- Initially focused on recovering deleted files and investigating fraud
- Later expanded to include digital crime investigation, cybersecurity, and incident response.
- Advances in technology led to the development of sophisticated forensic tools and techniques

Importance of Computer Forensics

- Computer forensics plays a crucial role in digital investigations
- Provide investigators with the means to gather evidence from digital devices
- Evidence can be used to reconstruct events, identify perpetrators, and support or refute claims in legal proceedings
- Without computer forensics, it would be challenging to investigate and prosecute cybercrimes effectively.

Legal and Ethical Considerations in Computer Forensics

- Legal and ethical considerations are paramount in computer forensics
- Investigators must adhere to laws and regulations governing the collection, preservation, and analysis of digital evidence
- Ensure the integrity of the evidence
- Respect the privacy rights of individuals.
- Non-compliance with legal and ethical standards can result in evidence being deemed inadmissible in court

Admissibility of Evidence

Week 2

- Evidence that a judge, jury, or tribunal may use in order to decide a case.
- Admissible evidence is evidence properly collected
- Relevant to an underlying case
- Can be properly presented in court.

Common Terms

Week 2

Authentic Evidence

- Evidence that is in its original or genuine state (i.e integrity preserved)

Credible Evidence

- Evidence worthy of belief and comes from a source that is reliable

Common Terms contd.

Week 2

Digital Evidence

- Evidence is a legal concept.
- Any writing, testimony, or other material objects that is offered as proof of an alleged fact or hypothesis.
- Anything, information or object used to support the existence of an assertion/claim

Common Terms Contd.

Week 2

Digital Evidence contd.

- The identification, preservation, collection, analysis, and presentation of digital evidence
- According to generally accepted processes and procedures for use in a legal matter.

Common Terms Contd.

Forensics

- The use of science to process evidence in order to establish facts for a legal matter.

Common Terms Contd.

Persistent Data

- Data that is stored on storage media and is preserved when an electronic device is turned off.

Provenance

- The origin of a piece of evidence

Common Terms Contd.

Volatile Data

- Data stored in the memory or connections that one electronic device might have with another device when connected.

Common Terms Contd.

Relevant Evidence

- Evidence that tends to prove (or disprove) a key legal element in a case.

Common Terms Contd.

Week 2

Reliable Evidence

- Evidence that can be trusted to be truthful and reliable
- Whether or not the evidence is reliable is a legal decision
- Evidence that is not reliable is inadmissible

Common Terms Contd.

Valid Evidence

- Scientific evidence that has been collected with the proper formalities to support its admissibility.

Common Terms Contd.

Fragility

- Evidence is generally fragile
- Evidence loses its value if it is not collected, preserved, and protected in a proper and timely manner
- Chain of custody must be maintained

Common Terms Contd.

Fragility contd.

- Items and objects that lose their evidentiary value quickly are considered fragile.
- Easily destroyed by a simple keystroke, sent across a network and
- Possibly changed, or damaged by intervening physical forces, such as electromagnetic fields.

Evidence Authenticity and Reliability

- Evidence also must be authentic and reliable in order to be admissible.
- Authentic evidence is evidence in its original form

Evidence Authenticity and Reliability contd.

- Party wishing to use the evidence must provide additional facts or evidence to show original evidence is what it says it is
- Show the evidence's provenance
- Evidence not admissible in court unless it is reliable
- Evidence is reliable if it can be trusted to be truthful

Rule of Evidence

Week 2

- Rules of Evidence are used to ensure the quality of evidence offered in a legal proceeding
- For example, chain of custody rule is used to establish the reliability of evidence.

Rule of Evidence contd.

Week 2

- Whether or not evidence is reliable is a legal decision.
- Evidence that is not reliable is inadmissible.
- Meaning it cannot be used in court at all.

Validity and Credibility

Week 2

- Demonstrate that digital evidence is reliable
- Collected in a valid manner
- Collected in a scientific way
- In accordance with generally accepted standards

Validity and Credibility Contd.

- One set of generally accepted cyber forensics standards was created by the International Organization for Standardization
- ISO/IEC 27037:2012, and the International Electrotechnical Commission (IEC).

Validity and Credibility Contd.

- These organizations work together to create standards for electronic technologies.
- The document provides guidelines for specific activities in the handling of digital evidence in order to preserve its evidentiary value

Computer Crimes

- Refers to two categories of offenses involving computers

Computer as target

- Computer or data is the target of a crime
- Example: attacks on networks that cause them to crash (Morris worm), unauthorized access, tempering with, information systems, programs or data.

Computer Crimes Contd.

Computer as Instrument

- A computer used to commit the crime
- Examples: theft, fraud, forgery, stalking, or distribution of illegal materials

End of Lecture