Computer Forensics

3207 Computer Security

Dr. Marriette Katarahweire,
Mr. Denish Azamuke

March 28, 2025

Outline

Introduction

- Forensic computing is the process of:
  - Identifying,
  - Preserving,
  - Analyzing, and
  - Presenting digital evidence in a manner that is legally acceptable.

Need for Computer Forensics

- To produce evidence in court that can lead to the punishment of the perpetrator.
- To ensure the integrity of the computer system.
- To focus on the response to high-tech offenses.

Characteristics of Computer Forensics

- Identifying - Detecting and labeling digital evidence.
- Preserving - Safeguarding digital evidence from alteration or corruption.
- Analyzing - Examining and interpreting the evidence.
- Presenting - Compiling evidence in a structured and legally admissible format.

History of Computer Forensics

- Originated over 30 years ago in the US with law enforcement and military investigators.
- Significant growth in the field, with ongoing developments in forensic software and training.

Goal of Computer Forensics

The primary goal is to identify criminals, uncover evidence, and ensure the evidence is presented legally to facilitate judicial action.

Cyber Crime and Evidence

Cyber crime involves the use of information technology to commit or conceal offenses.

Examples of Cyber Crimes

- Breach of computer security
- Child pornography
- Fraud and theft
- Copyright violations
- Identity theft
- Narcotics trafficking
- Threats and harassment
- Stalking
- Sexual assault

Digital Evidence

Digital evidence is any data stored or transmitted in digital form that can be used in the court.

Characteristics include:

- Latent like fingerprints or DNA.
- Fragile and easily alterable.
- Time-sensitive.

Types of Digital Evidence

- Persistent data: Remains intact when the computer is turned off.
- Volatile data: Lost when the computer is turned off or rebooted.

Rules of Evidence

- Admissible: Must be legally acceptable.
- Authentic: Directly related to the incident.
- Complete: Includes evidence that could exonerate the suspect.
- Reliable: Trustworthy and verifiable.
- Believable: Clear and comprehensible to juries.

Location for Evidence

- Internet history files
- Temporary internet files
- Slack and unallocated space
- Chat records and buddy lists
- File storage metadata
- Emails and file sharing data

Computer Forensics Methodology

Detailed steps from securing the scene to documenting findings.

- Shutdown the computer
- Document the hardware configuration of the system
- Transport the computer system to a secure loaction
- Make backups, verify data on all storage devices
- Document the system date and time, make a list of key search words
- Evaluate the windows swap file, file slack, unallocated space (erased files)
- Search files and unallocated space using keywords
- Document file names, dates and times
- Identify file, program and storage anomalies
- Evaluate program functionality
- Document your findings

Application of Computer Forensics

- Financial fraud detection
- Criminal prosecution and civil litigation
- Enhancing corporate security policies

Computer Forensic Expert

Essential skills and knowledge required for professionals in the field.

- Programming or computer-related experience
- Broad understanding of operating systems and applications
- Analytical skills
- Computer science fundamentals
- System administration skills
- Knowledge of intrusion detection systems and tools
- Knowledge of cryptography
- Understanding of rules of evidence and evidence handling
- Ability to be an expert witness in courts of law

Thank You!

References

Rogers, M. K., & Seigfried, K. (2004). *The future of computer forensics: a needs analysis survey.* Computers & Security, 23(1), 12-16.

Dixon, P. D. (2005). *An overview of computer forensics.* IEEE Potentials, 24(5), 7-10.

Maras, M. H. (2015). *Computer forensics. Jones and Bartlett Learning*.