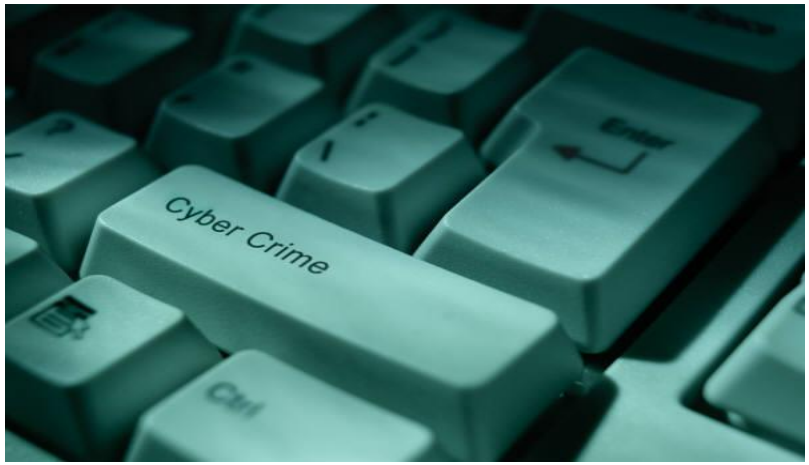
Introduction to Computer Forensics

Prof. Zaheed Shaikh



Computer Crime

- Computer crime is any criminal offense, activity or issue that involves computers (http://www.forensics.nl).
- Computer misuse tends to fall into two categories [1]:
  - Computer is used to commit a crime
  - Computer itself is a target of a crime. Computer is the victim. Computer Security Incident.
- Computer Incident Response.

Computer is Used to Commit a Crime

- Computer is used in illegal activities: child pornography, threatening letters, e-mail spam or harassment, extortion, fraud and theft of intellectual property, embezzlement – all these crimes leave digital tracks [1, 2].
  - Investigation into these types of crimes include searching computers that are suspected of being involved in illegal activities
  - Analysis of gigabytes of data looking for specific keywords, examining log files to see what happened at certain times

Computer Security Incident [2]

- Unauthorized or unlawful intrusions into computing systems
- Scanning a system - the systematic probing of ports to see which ones are open [3]
- Denial–of–Service (DoS) attack - any attack designed to disrupt the ability of authorized users to access data [2, 3].
- Malicious Code – any program or procedure that makes unauthorized modifications or triggers unauthorized actions (virus, worm, Trojan horse) [3]

Computer Forensics

- Computer Forensic Analysis
- Electronic Discovery
- Electronic Evidence Discovery
- Digital Discovery
- Data Recovery
- Data Discovery
- Computer Analysis
- Computer Examination

Definitions

- **Computer Forensics** involves the preservation, identification, extraction, documentation and interpretation of computer data [1]
- **Computer Forensics** is the application of science and engineering to the legal problem of digital evidence. It is a synthesis of science and law. [Mark Pollitt, 5, 6]
- **Computer forensics,** still a rather new discipline in computer security, focuses on finding digital evidence after a computer security incident has occurred (http://www.forensics.nl)

Definitions

- **Computer Forensics** is the process of methodologically examining computer media (hard discs, diskettes, tapes, etc.) for evidence. [4]
- *Computer Evidence* is often transparently created by the operating system (OS) without the knowledge of the computer user. The information may be hidden from view. To find it, special forensic software tools and techniques are required. [4]
- **Computer forensics** is about evidence from computers that is sufficiently reliable to stand up in court and be convincing [4]

Methodology

- Treat every case as if it will end up in the court [1]
- Forensics Methodology [1]:
  - Acquire the evidence without altering or damaging the origin
  - Authenticate that your recovered evidence is the same as the originally seized data
  - Analyze the data without modifying it
- There are essentially three phases for recovering evidence from a computer system or storage medium. Those phases are: (1) acquire, (2) analyze, and (3) report (http://www.forensics.nl).

The Goal

The goal of **computer forensics** is to do a structured investigation and find out exactly what happened on a digital system, and who was responsible for it. (http://www.forensics.nl)

The Goals of Incident Response [2]

- Accumulation of accurate information
- Establishment of control for proper retrieval and handling of evidence
- Protection of privacy rights established by law and policy
- Minimization of disruption to business and network operations
- Preparation of accurate reports and useful recommendations
- Minimization of exposure and compromise of proprietary data
- Protection of organization reputation and assets
- Education of senior management
- Promotion of rapid detection/or prevention of such incidents in the future (via lessons learned, policy changes, etc)

References

[1] Computer Forensics, Incident Response Essentials, Warren G. Kruse II, Jay G. Heiser, Addison-Wesley

[2] Incident Responce and Computer Forensics, Kevin Mandia, Chris Prosise, Matt Pepe, McGraw-Hill

[3] Information Security Illuminated, Michael G. Solomon, Mike Chapple, Jones and Bartlett Publishers, Inc

[4] Computer Forensics, Computer Crime Scene Investigation, John R. Vacca, Charles River Media Inc

[5] Forensic Computing, A Practitioner's Guide, Tony Sammes and Brian Jenkinson, Springer.

[6] Mark Pollitt, Computer Forensics: An Approach to Evidence in Cyberspace, http://www.digitalevidencepro.com/Resources/Approach.pdf