Cyber Forensics

CS 4241

Dr. Anand Kumar Mishra

NIIT University

Who can use Computer Forensic Evidence

- **Criminal prosecutors** use computer evidence in a variety of crimes
  - Financial fraud, drug and embezzlement record-keeping, and child pornography
  - **Embezzlement** takes place when a person uses funds for a different purpose than they were intended to be used
- **Civil litigations** can readily make use of personal and business records found on computer systems
  - Fraud, divorce, discrimination, and harassment cases.

Who can use Computer Forensic Evidence

- Insurance companies may be able to mitigate costs by using discovered computer evidence :
  - Possible fraud in accident, and workman’s compensation cases
- Corporations often hire computer forensics specialists to find evidence relating to :
  - Sexual harassment, embezzlement
  - Theft or misappropriation of trade secrets
  - Other internal and confidential information

Who can use Computer Forensic Evidence

- **Law enforcement** officials frequently require assistance in :
  - Pre-search warrant preparations and post-seizure handling of the computer equipment
- **Individuals** sometimes hire computer forensics specialists in support of :
  - Possible claims of wrongful termination, Sexual harassment, or age discrimination

Computer Forensics

- **Well-defined procedures** to address the various tasks
- An anticipation of likely criticism of each methodology on the grounds of failure to demonstrate **authenticity, reliability, completeness, and possible contamination** as a result of the forensic investigation
- The possibility for **repeat tests** to be carried out, if necessary, by experts hired by the other side
- **Checklists** to support each methodology
- An anticipation of any problems in formal legal tests of **admissibility**

Broad tests for evidence - Authenticity

- Does the material come from where it purports?
- Proven of an original when it was written, printed, executed, or signed as it claims to have been
- Proven of a copy when it is a true copy of the original
    - True Copy: A copy of a legal document exactly the same as the original with notations, court stamps, signatures of parties and the court registrar, insertions and corrections written in the copy within quotation marks

Broad tests for evidence - Reliability

- Can the substance of the story the material tells be believed and is it consistent?
- In the case of computer-derived material, are there reasons for doubting the correct working of the computer?

Broad tests for evidence - Completeness

- Is the story that the material purports to tell complete?
- Are there other stories that the material also tells that might have a bearing on the legal dispute or hearing?

Broad tests for evidence - Freedom from interference and contamination

- Are these levels acceptable as a result of forensic investigation and other post-event handling?

Cloud Forensics

Digital Forensics

- Scientific acquisition,
- Analysis, and preservation of data
- Contained in electronic media
- Information can be used as evidence in a court of law
- "*Digital forensics* is the scientific acquisition, analysis, and preservation of data contained in electronic media whose information can be used as evidence in a court of law."

Digital Forensics and Analyzing Data Dale Liu, in Cisco Router and Switch Forensics, 2009

Digital Forensics

- Digital forensics is performed
  - In response to an incident
  - Focuses on determining the root cause for what prompted the incident
- Purpose - To establish evidence and facts from
  - Digital information existing on any number of different technologies e.g.
    - game consoles, mobile devices, computer systems,
    - across dissimilar network architectures (eg, private, public, cloud), or
    - varying states - volatile, static

2016 Implementing digital forensic readiness - from reactive to proactive process

Digital Forensic Science Disciplines

- **Computer forensics**
  - relates to the gathering and analysis of digital information as digital **evidence on computer systems** and electronic storage medium
- **Network forensics**
  - relates to the monitoring and analysis of **network traffic** for the purposes of information gathering, gathering of digital evidence, or intrusion detection
- **Incident response**
  - relates to reducing business impact by **managing the occurrence of computer security events**

2016 Implementing digital forensic readiness - from reactive to proactive process

Digital Forensic Science Disciplines

- **Memory forensics**
  - relates to the gathering and analysis of digital information as digital evidence contained **within a system's RAM**
- **Electronic discovery (e-discovery)**
  - relates to the discovery, preservation, processing, and production of electronically stored information (ESI) in support of legal or regulatory litigation matters
- **Cloud forensics**
  - relates to the gathering and analysis of digital information as digital evidence from **cloud computing systems**

2016 Implementing digital forensic readiness - from reactive to proactive process

Cloud Forensics

- Cloud computing has revolutionized the methods by which digital data is stored, processed, and transmitted.
- Challenge
  - How to perform digital forensics in various types of cloud computing environments
  - Conducting forensics in different cloud deployment models
    - Issue - Cross geographic or legal boundaries

NISTIR 8006 NIST Cloud Computing Forensic Science Challenges

Cloud Forensics

- Cloud computing forensic science
  - The application of scientific principles,
  - technological practices, and derived and proven methods
  - To reconstruct
    - past cloud computing events
    - through the identification, acquisition, preservation, examination, interpretation, and reporting of potential digital evidence

NISTIR 8006 NIST Cloud Computing Forensic Science Challenges

Cloud Forensics

- Application of digital forensic science in cloud computing environments.
- **Technically - C**onsists of a hybrid forensic approach
  - e.g., remote, virtual, network, live, large-scale, thin-client, thick-client towards the generation of digital evidence
- **Organizationally** - Involves interactions among cloud actors
  - cloud provider, cloud consumer, cloud broker, cloud carrier, cloud auditor
  - For the purpose of facilitating both internal and external investigations
- **Legally** - often implies multi- jurisdictional and multi-tenant situations

K. Ruan and J. Carthy, "Cloud forensic maturity model," in Digital Forensics and Cyber Crime. Springer, 2013, pp. 22–41.