COE589: Digital Forensics

Introduction to Digital Forensics

Dr. Ahmad Almulhem

KFUPM - Fall 2012 (T121)
Outline

• Forensic Science (Forensics)
  – Classic (Analog) vs Digital Forensics
• Branches of Digital Forensics
• Digital Forensics vs Other Fields
• Digital Evidences
• Computer Crimes
• Computer Forensics History
• Digital Forensics Process
• Case Study
Forensics Science

Forensics (noun): Latin meaning public, forum, discussion

Forensic science (forensics) is the application of a broad spectrum of sciences to answer questions of interest to a legal system

– whose fingerprints, bloodstains are those?
– age, gender of found bones?
Forensics

• divide forensic sciences by **domain of evidence** *(Bohme 2009)*
  – analog (physical)
  – digital

• what do you think?
  – are they exclusive?
  – examples or counterexamples?
Classic (Analog) Forensics (Bohme 2009)

Based on two principles:

1. **Divisibility of Matter**: matter divides into smaller parts when sufficient force is applied. The smaller parts retain characteristics of the original matter as well as acquire characteristics generated by the separation itself (examples: shattered glass)

2. **Exchange (Locard’s) Principle**: whenever two entities interact in the real world each entity will retain some physical matter of the other (examples: fingerprints, footprints, ..etc.)
Debate

• Does those two principles apply in the digital world?
  – example?
  – counterexamples?
Digital Forensics

Digital

**adjective**

1 Relating to or using signals or information represented by discrete values (digits) of a physical quantity, such as voltage or magnetic...: "digital TV"

2 Involving or relating to the use of computer technology: "the digital revolution".

Digital Forensics

“the application of proven scientific methods and techniques in order to recover data from electronic / digital media”

“Tools and techniques to recover, preserve, and examine digital evidence on or transmitted by digital devices.”
Branches of Digital Forensics

• **Computer Forensics** mainly focuses on computer’s hard disk and OS artifacts

• **Live forensics** considers data that may be lost by powering down a system and collect it while the system is still running (processes list, network connections)

• **Multimedia Forensics** is concerned with authenticity and origin of digital media (text, images, audio, video)

• **Network Forensics** relating to the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection

• **Mobile Forensics** recovery of digital evidence or data from a mobile device under forensically sound conditions (contacts, SMS messages)
Examples of Multimedia Forensics

“Typical image manipulation and detection with multimedia forensics. Presumably original photograph of Iranian missile test with one non-functioning missile (left, source: online service of the Iranian daily Jamejam today) which was replaced by a copy and paste forgery (middle, source: Iranian Revolutionary Guards). The detector output marks regions which were copied with high probability (right)” (Bohem 2009)
DF vs other Fields

• **Computer Security**: protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users
  – Security is mainly preventative, while DF is investigation after the fact

• **Data Recovery** concerns recovering information that was deleted by mistake or lost during a power surge or server crash
  – Apply similar tools and techniques
  – Typically you know what you’re looking for
DF vs other Fields

• Computational forensics concerns the development of algorithms and software to assist forensic examination

• Forensic engineering is the scientific examination and analysis of structures and products relating to their failure or cause of damage (Titanic?)

• Reverse Engineering is taking apart an object to see how it works in order to duplicate or enhance the object
Digital evidences

• **Digital evidence** or electronic evidence is any information stored or transmitted in digital form that may be used in a court
  – has to be relevant and authentic
  – can be anything: from few bytes to complete files

• Examples of digital evidences:
  – digital photos (fake?)
  – video (who is it?)
  – audio (who is speaking?)
  – documents (deleted)
  – emails
  – log files
Computer Crimes

- Two categories of crimes that involve computers:
  - Computer as target—computer or its data is the target of the crime
  - Computer as instrument—computer is used to commit the crime
Digital Forensic Process (wikipedia)

1. **Seizure**: actual digital media is seized to ensure preservation of evidence

2. **Acquisition**: exact sector level duplicate (or "forensic duplicate") of the media (also called imaging)

3. **Analysis**: analyze images to identify evidences that either supports or contradicts a hypothesis or for signs of tampering

4. **Reporting**: report results in a form suitable for non-technical individuals
By the 1970s, electronic crimes were increasing, especially in the financial sector
   - Most law enforcement officers didn’t know enough about computers to ask the right questions
     * Or to preserve evidence for trial

1980s
   - PCs gained popularity and different OSs emerged
   - Disk Operating System (DOS) was available
   - Forensics tools were simple, and most were generated by government agencies
A Brief History of Computer Forensics (continued)

• Mid-1980s
  – Xtree Gold appeared on the market
    • Recognized file types and retrieved lost or deleted files
  – Norton DiskEdit soon followed
    • And became the best tool for finding deleted file

• 1987
  – Apple produced the Mac SE
    • A Macintosh with an external EasyDrive hard disk with
      60 MB of storage
A Brief History of Computer Forensics (continued)

Figure 1-3  An 8088 computer
A Brief History of Computer Forensics (continued)

Figure 1-4  A Mac SE with an external EasyDrive hard disk
A Brief History of Computer Forensics (continued)

• Early 1990s
  – Tools for computer forensics were available
  – International Association of Computer Investigative Specialists (IACIS)
    • Training on software for forensics investigations
  – IRS created search-warrant programs
  – ExpertWitness for the Macintosh
    • First commercial GUI software for computer forensics
    • Created by ASR Data
Case Study

• http://www.youtube.com/watch?v=Gp7SDi-lJbU