Course scope
• Multi disciplinary
  – Computer Science
  – Information Security
    • Technical
    • Non-technical
  – Forensics
  – Digital Forensics
  – Law
  – Ethics
• An interesting course!
Course overview

- Introduction to Digital Forensics
- The Digital Forensic Process
- Hardware Forensics
- Digital Forensics Tools (software)
- Practical: data acquisition and preservation
- Network (live) Forensics
- Cloud Forensics

Contents – Introduction to digital forensics

- History
- Forensic Science
- What is Digital Forensics?
- Digital Forensic Techniques
- Common mistakes
- Illegal and legal activities warranting digital forensic investigations
- Types of digital forensic investigations
- Conclusion
History

• 40 years ago…
  – People did not think computers will be an integral part of our lives
• Now computer technology’s commonplace but…
  – So are computer crimes, however…
  – Evidence, by its nature, stored on computers!
• In 1970’s computer crimes started to happen
  – Usually in financial sector
  – Because mainly mainframe computers were used
  – In banks, engineering, academia
  – White collar crimes started when people in these areas saw ways in manipulating computer data

• Example
  – One of most well known crimes: “half-cent crime”
  – Banks round interest calculations up
  – Computer programmers corrupted this method by opening up an account for themselves and writing programs that diverted all the fractional monies into the account
  – In bigger banks with their thousands/millions of subsidiaries this amounted to hundreds of thousand of dollars
  – What is this attack also called?
History

• PCs emerged in 1980s replacing mainframes
  – Many different OSs emerged
    • DOS
      – PC DOS, DR DOS, IBM DOS, MS-DOS
    • MAC OS (UNIX)
  – Hardware
    • Apple Macintosh
    • Commodore 64
    • PC – 8086, 8088
• Digital forensic tools were simple and programmed in C by federal law enforcement agencies

• By 1990s specialised digital forensic tools
  – International Association of Computer Investigative Specialists (IACIS) introduced training in the field
  – First commercial software
    • Expert Witness for Mac by ASR Data
      – Recover deleted fragments
      – Later became EnCase
    • Access Data’s FTK
    • iLook
    • Today, many more…
    • Industry leading: Encase and FTK
    • Open/free: SIFT, ProDiscover, Volatility, The Sleuth Kit (+Autopsy), dd, CAINE, Oxygen, Hex, Bulk extractor…
• 2000s large drives became a problem
The field of Forensic Science

• Historically
  – Romans meet in a public place called a “forum”
  – The term “forensic” means “of the forum”

• Forensics definitions
  – The methods of science applied to public matters
  – A “mixed science”: associating people, places, and things involved in – usually criminal – activities

• Forensic fields
  – criminalistics, pathology, odontology, engineering, entomology and many more
What is Digital Forensics?

• Definitions
  – a means for gathering electronic evidence during a forensic investigation
  – the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations

What is Digital Forensics?

• Definitions
  – Any information of probative value that is either stored or transmitted in binary form
    • The Scientific Working Group for Digital Evidence
  – The application of Science and Engineering to the legal problem of digital evidence – it is a syntheses between science and the law
    • Mark Pollitt – retired FBI special agent
  – The discipline that combines elements of law and digital science to collect and analyse data from digital systems in a way admissible in court
    • US-CERT
What is Digital Forensics?

- The main problem with DF
  - Many people involved in investigation
  - Evidence need to be presented in the same way as used to in “normal” forensics
  - Requirements (Daubert):
    - DF theory or technique must have been reliably tested
    - Must have been subject to peer review and publication
    - Potential error rate of DF method used should be known
    - Must be generally accepted by scientific community
    - An acceptable process needs to be followed in acquiring and presenting the digital evidence
  - Establishing a true science

Digital Forensic Techniques

- Software assisted
- Hidden files
- Deleted files
- Slack space
- File type/extension modification
- Alternate data streams (ADS) in NTFS
- Live digital forensics
- Self-organised maps (SOMs) using AI
- Many other/new techniques
Common mistakes

• Failure to maintain proper documentation
  – Tedious and demanding, which is why it can fail

• Inadvertent modification of data
  – By opening files on original evidence
  – Doing so will change date/time stamps
  – May hinder subsequent investigation
  – May render evidence unusable in court
  – By installing investigation software on orig. evidence

• Complicated by live forensics
• Improper access control to evidence and chain of custody

Common mistakes

• Failure to realise that the limits of the investigator’s knowledge have been reached and then to ask for assistance
  – Area is vast and complex – ask for help!
  – Once investigator exceeds their level of expertise, any such evidence recovered will be questioned in a court of law.

• Failure to follow the DF investigation process to the letter
Illegal activities warranting digital forensic investigations

- Two main categories
  - Criminal investigations
  - Civil litigation investigations

- Fraud audits
- Identity theft
- Hacking
- Embezzlement (misappropriation)
- Instances of homicide
- Drug trafficking
- Child pornography
- Civil litigation in cases of divorce, age or race discrimination, sexual harassment, wrongful dismissal/termination
Illegal activities warranting digital forensic investigations 2015

- Compromise of customer privacy data stored electronically
- Peer-to-peer file sharing
- Leak and unauthorised disclosure of internal and confidential information
- Theft of trade secrets/intellectual property
- Unlawful access to company computers
- Use of company computers or technology for personal gain
- Violation of company acceptable use policy
- Launching DoS attacks against competitors

Legal activities warranting digital forensic investigations 2015

- Two main categories
  - Data discovery
    - Volumes upon volumes of digitally filed documents
    - E-discovery
  - Data recovery of data that was lost due to
    - Corrupted partition tables/boot sectors/FATs
    - Mechanical problems – HDD crashes
    - Accidental deletion/formatting/deletion of partitions
    - Malicious software/viruses/Trojans
    - Lost or forgotten passwords
    - Physical damage to disks due to fires, floods etc.
Types of digital forensic investigations (DF 2015)

- Dealing with a single computer(s)
  - Also known as postmortem or dead forensics
  - Stand-alone PCs/laptops
  - Easiest type of investigation, but...
  - Becoming more complex as storage capacities grow and getting more inter connected through non-physical interfaces such as WiFi, Bluetooth
  - Specific elements of PC to be considered
    - The PC itself
    - Peripheral devices
    - Storage media (internal and external)
    - Associated material

- Dealing with a networked computer(s)
  - Also refer to live or cloud forensics
  - Capture, recording and analysis of network data (often in the Cloud)
  - Careful not to contravene laws (privacy?)
  - Specific elements in network to be considered
    - Routers
    - Hubs/switches
    - Servers
    - Volatile information (RAM)
Types of digital forensic investigations

• Dealing with handheld devices
  – Also known as mobile forensics
  – Includes electronic organisers, PDAs, mobile phones, music/media players, portable storage devices, pagers, digital cameras, game consoles, hybrids
  – Volatile memory
  – Often need to switch them on

• Dealing with live (cloud) forensics
  – Collection of volatile evidence at real time
  – Large servers/networks that are mission critical and cannot be taken offline for a forensic investigation
  – Types of information that can be retrieved:
    • Running processes
    • Recent emails
    • Recently visited web sites
    • Chat rooms
  – Can be retrieved from memory, swap file, networked/system processes, file system info
Conclusion

• Digital forensics is not a new field anymore
• But it is a young science (still becoming)
• Many Digital Forensic Techniques
• There are illegal and legal activities warranting digital forensic investigations
• Law intertwined with digital forensics
• Many types of digital forensic investigations
• A specialisation field in the broader scope of Information and Computer Security

Other background textbooks

• Guide to Computer Forensics and Investigations
  – Course Technology; 4 edition (September 28, 2009)
• Cyber Forensics
• Building a digital forensic laboratory
  – Butterworth Heinemann and Syngress; 1 edition
• Google for more recent ones