Universiti Malaysia PAHANG
Engineering • Technology • Creativity

Computer Forensic & Investigation

Editors
Dr. Abdulghani Ali Ahmed
Wan Nurulsafawati Wan Manan
Faculty of Computer Systems & Software Engineering
abdulghani@ump.edu.my

Source: (Nelson, Guide to Computer Forensics and Investigations, 2015).

Content

- Principles of Evidence
- The Courts
- Computer Forensics Elements
- Computer Forensics Process
  - Imaging and Verification of Integrity
- Evidence Presentation

Source: (Nelson, Guide to Computer Forensics and Investigations, 2015).

Best Evidence…

- Best Evidence Rule
  - Original document , not a copy
  - If the original is not available, a copy may be admitted if:
    - The content of the copy truly and accurately reflects the original
    - There is a satisfactory reason why the original is not submitted to the court

Source: *(Nelson, Guide to Computer Forensics and Investigations, 2015).*

Best Evidence…

- Evidence can be found in many forms such as:
- Document:
  - paper records
  - computer records
    - files, disks, tapes, CDs, DVDs, magnetic media etc

Source: (Nelson, Guide to Computer Forensics and Investigations, 2015).

The Courts

- Courts
  - Court Types
- All of these Courts deal with criminal and civil matters.
- Court’s presentation Goal:
  - Persuade the audience
  - Prove facts
- Rules of court
- Criminal offence

Source: (Nelson, Guide to Computer Forensics and Investigations, 2015).

The Courts

- Criminal Matters
  - a law has been broken
  - law enforcement has detected the crime
  - prosecution
    - Attorney General (AG), Director of Public Prosecutions (DPP)
  - defense
  - presumption of innocence
  - prosecution **<u>must</u>** prove otherwise

Source: (Nelson, Guide to Computer Forensics and Investigations, 2015).

The Courts

- Onus of Proof
  - Different in criminal and civil matters
    - Criminal matters
      - prosecutor acting for the public authority has the onus of proof
      - proof beyond reasonable doubt
      - defense has to show reasonable doubt
    - Civil matters
      - plaintiff has the onus of proof
      - exceptions include
        - » negligence where “Res Ipsa Locutur” is claimed
        - » tax cases
      - proof is on balance of probabilities
        - » >50%

Source: (Nelson, Guide to Computer Forensics and Investigations, 2015).

- Common Law Rules of Evidence
  - some developed by the courts
  - some developed by legislators
  - Hearsay rule
  - Best Evidence rule

Source: (Nelson, Guide to Computer Forensics and Investigations, 2015).

The Hearsay Rules

- The Hearsay Rule
  - – Subramanian v DPP (Director Public Prosecution)
  - – If Person A testifies that they heard Person B admitting to committing a particular act, then the testimony is hearsay as to whether the act occurred, but it is direct evidence of the admission
  - – hearsay generally not admissible
  - – business records or public records may be admissible

Source: (Nelson, Guide to Computer Forensics and Investigations, 2015).

Some Interesting Cases

Source: (Nelson, Guide to Computer Forensics and Investigations, 2015).

Cases…..

- Zubulake vs UBS Warburg
  - E-Discovery, Deleted Records
- Scarfo
  - Key loggers, PGP Encryption
- Regina v Caffrey
  - The Self Deleting Trojan Defense
- Lisa M. Montgomery
  - an attempt to kidnap her unborn baby
- State v. Cook, WL31045293 Ohio Ct. App. (2002)
- Kleiner v. Burns, WL 1909470 (2000).

Source: (Nelson, Guide to Computer Forensics and Investigations, 2015).

Computer Forensic Elements

Source: (Nelson, Guide to Computer Forensics and Investigations, 2015).

- Parallels of “logical” crime with “physical” crime or event
  - Crime scene must be protected against contamination or interference
  - State of the area is recorded
  - Conduct a search for evidence
  - “Chain of custody”
  - Many stages at which evidence can be corrupted
  - Many detective skills are like programming
    - logical thinking, understanding effect of actions, finding a solution

Source: (Nelson, Guide to Computer Forensics and Investigations, 2015).

- Problems with computer-related crime or misconduct
  - locating the “scene”
  - identifying the “crime”
  - identifying the victim and/or target
  - identifying the suspect
  - demonstrating intent
  - too much potential evidence
  - evidence is easily contaminated
  - evidence is highly integrated
  - information is “media-independent”

Source: (Nelson, Guide to Computer Forensics and Investigations, 2015).

- Objectives of Computer Forensics
  - both formal and informal
    - Acquisition: search and seizure
    - Analysis
    - Report results
  - formal
    - Give evidence in court

Source: (Nelson, Guide to Computer Forensics and Investigations, 2015).

- Principles of CF
  - On seizing, actions should not be taken to change that evidence
  - Only forensically competent persons should access the evidence
  - Document all steps in seizure, access, storage or transfer of evidence
  - Individuals are responsible for the evidence while in their possession
  - Agencies responsible for seizure, access, storage or transfer are also responsible for compliance

Source: (Nelson, Guide to Computer Forensics and Investigations, 2015).

- Values for the process
  - Sterile operating tools
    - boot disks, copiers etc must be certified free of viruses etc. (“trusted”?)
  - Stay within the warrant
    - enough but not too much
  - Accuracy of image
    - correctly copied
  - Integrity of image and investigation
    - all conclusions drawn from original data
    - original data is never altered
  - Document the process at each step
    - nothing added or deleted
    - reproducibility

Source: (Nelson, Guide to Computer Forensics and Investigations, 2015).

Requisite computer forensic functionality

- Imaging tools
  - volatile memory
  - disk and file
  - write blockers
  - integrity creating and checking

- Analysis tools
  - ambient data recovery
  - text searching
  - data and file recovery
  - integrity checking tools
  - file conversion
  - data filtering
  - fuzzy search tools
  - file carving

- Reporting tools
  - time-lining
  - case logging
  - report generators

Source: (Nelson, Guide to Computer Forensics and Investigations, 2015).

Computer Forensic Process

- Identify, Secure, Analyse, Present
  - Identify
    - where and what is the relevant evidence
  - Secure
    - Remove from scene
    - Copy
    - Validate and verify
  - Analyse
    - Determine meaning
    - Discover intent
  - Present
    - What does it mean to others
    - … including quite possibly in a court of law

Source: (Nelson, Guide to Computer Forensics and Investigations, 2015).

Imaging and Verification of Integrity

- Acquisition
  - To pull the plug or to not pull the plug?
    - depends on situation
    - impact on organization
  - disassemble case
  - document components
    - make, model, geometry, size, bus type etc.
  - disconnect storage devices
  - preference
    - hardware acquisition
      - Logicube or similar
    - acquire using examiner’s system
    - acquire using suspect’s system (least preferred)

Source: (Nelson, Guide to Computer Forensics and Investigations, 2015).

Imaging and Verification of Integrity

- target storage must be sanitized prior to use
  - remove all traces of any previous contents
  - US Department of Defense standard
    - write a byte, then its complement, then a random byte and verify
  - Gutmann

- Hardware
  - Logicube OmniClone 2Xi
  - Image MASSter Solo 3

Source: (Nelson, Guide to Computer Forensics and Investigations, 2015).

Imaging and Verification of Integrity

Source: (Nelson, Guide to Computer Forensics and Investigations, 2015).

Imaging and Verification of Integrity

- Software tools offer choices of
  - copying selected files
    - OK but not forensically thorough
  - creating a **bit by bit** or **bit stream** image of the entire disk
    - this is preferred (if space allows)
    - allows investigator to look for
      - partitions
      - hidden data
      - deleted data
      - slack space
- Hardware tools offer bit stream image only

Source: (Nelson, Guide to Computer Forensics and Investigations, 2015).

Imaging and Verification of Integrity

- Software
  - Encase
  - Access Data FTK Imager
  - ILook IXimager
  - Safeback
  - Snapback DatArrest
  - *nix dd (copy and convert)
- Forensic Boot CDs
  - Helix – Computer Forensics & Incident Response
  - F.I.R.E. – Forensics, Incident Response
  - FCCU – Lnx 4n6

Source: (Nelson, Guide to Computer Forensics and Investigations, 2015).

Imaging and Verification of Integrity

- Image Integrity
  - must not alter contents of disk being imaged
  - write blockers used to ensure this
    - software and hardware (preferred)
  - software write blockers rely on intercepting BIOS INT 0x13 interrupts
    - work by substituting another interrupt routine for the existing one
    - not all hard drive device drivers use BIOS INT 0x13 interrupts
  - Hardware write blockers

Source: (Nelson, Guide to Computer Forensics and Investigations, 2015).

Imaging and Verification of Integrity

- verification tools
  - md5sum
  - sha1sum
- verification
  - MD5 and/or SHA1 digest values calculated as data is imaged
- hash values must be recorded
- Logicubes and other devices have built in printers

Source: (Nelson, Guide to Computer Forensics and Investigations, 2015).

Imaging and Verification of Integrity

- Chain of Evidence/Custody
  - Both disk and file images need to conform to chain of evidence/chain of custody requirements
    - What is the evidence?
    - How did you get it?
    - When was it collected?
    - Who has handled it?
    - Why did that person handle it?
    - Where has it travelled, and where was it ultimately stored?
  - Maintaining the Digital Chain of Evidence
    - Patzakis

Source: (Nelson, Guide to Computer Forensics and Investigations, 2015).

Questions

Have Question ?

Source: (Nelson, Guide to Computer Forensics and Investigations, 2015).