Universiti Malaysia PAHANG
Engineering • Technology • Creativity

Computer Forensic & Investigation

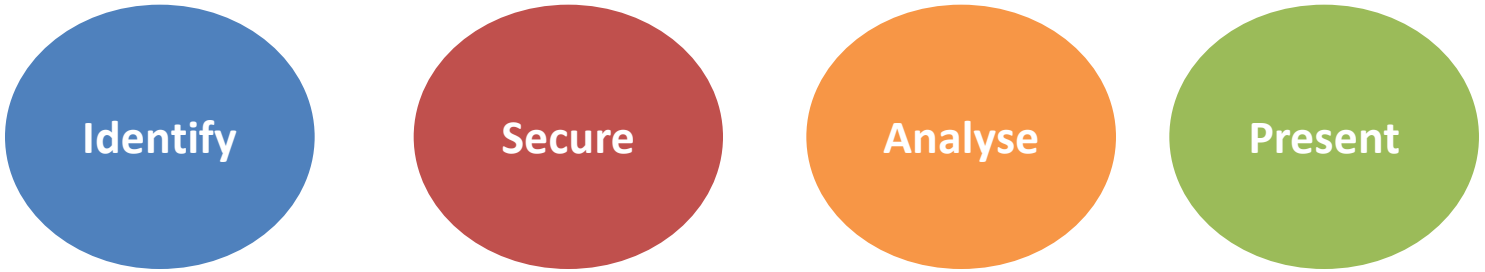
Processes of Computer Forensics

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

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

Computer Forensic Process

Main processes of Computer Forensics



Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

Computer Forensic Process

- Evidence must be managed in a manner that
  - Retains safe custody
  - Maintains a log recording all access to and handling
  - Ensures personnel have adequate training

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

Computer Forensic Process

- Admissible digital evidences

– Electronic Device generated

- not subject to hearsay considerations
- does not contain 'human statements'

– Must satisfy

- generated as part of routine business procedures
- attested by the testimony of the custodian or qualified witness
- absence of specific lack of trustworthiness

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

Computer Forensic Process

- Admissibility of computer evidence
  - **Electronic Device stored**
    - subject to hearsay
    - these are representations of ‘human statements’
  - some evidences are mix of the two

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

Computer Forensic Process

- Admissibility of computer evidence
  - **post-creation authenticity**
    - but the mere possibility of tampering is insufficient
    - proof needs to be given to prevent admissibility
  - **reliability of programs that generated computer-generated records.**
  - **authorship identity of computer-stored records**
    - unlike handwriting
    - generally proven through circumstantial evidence

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

Computer Forensic Process

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

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

This Week

- Computer Forensics Process
  - **Identify**
  - Secure
  - Analyse
  - Present

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

Identify

- Preparation
  - CF Investigator usually called in by case investigator
    - discuss case
      - current intelligence
      - need for other forensic processes
      - need for additional digital evidence
      - consider potential evidence being sought
      - consider skill levels of computer user(s)
      - prioritize examination
      - consider personnel
      - determine required equipment

Identify

- Onsite Assessment
  - identify number of computers
  - determine presence of network
  - interview system administrators and users
  - document the scene
    - still and video camera
  - identify and document types and volume of media
    - removable media
  - identify proprietary software and Operating System

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

Identify

- estimate time needed onsite to complete imaging
- consider impact on business/organization while imaging
- stay within bounds of search warrant
  - if evidence located that falls outside of warrant, take necessary action

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

This Week

- Computer Forensics Process
  - Identify
  - **Secure**
  - Analyse
  - Present

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

Secure

- 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

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

Secure

- using subject system for acquisition
  - controlled boot to determine CMOS/BIOS settings
  - use forensic boot disk
  - prevent computer accidentally booting from subject storage devices
- 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

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

Secure

- Non-invasiveness
  - where suspect computer has to be used to image files/media a trusted boot disk (DOS or Linux) must be used
  - provides
    - a secured command line interface
    - forensically sound copying program
  - execute from removable media
    - floppy
    - CD/DVD
  - alternatively imaging across a network link is possible

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

Secure

- Non-invasiveness
  - tools must be statically linked
  - must not rely on any dynamic link libraries (DLLs) on target machine
    - DLLs may not be trustworthy given that the target is suspected of being compromised in some way
  - boot source may need to be changed
    - access the BIOS settings to ensure this
    - ensure target disk drive is removed to do this

Secure

- Non-invasiveness
  - secure boot and statically linked tools guarantee nothing is written to the evidence disks
  - prevents registry updates and file decompressions which will result in file metadata and timestamps being altered

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

Secure

- software tools offer choices of
  - copying selected files
  - creating a **bit by bit** or **bit stream** image of the entire disk
- hardware tools offer bit stream image only

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

Secure

- must not alter contents of disk being imaged
- write blockers
  - software
    - software write blockers rely on intercepting BIOS INT 0x13 interrupts
  - hardware (preferred)
    - physical device between evidence drive/device and copy storage device

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

Secure

- verification tools
  - md5sum (32 bytes)
  - sha1sum (40 bytes)
- verification
  - MD5 and/or SHA1 digest values calculated as data is imaged
- hash values must be recorded

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

Secure

- Chain of Evidence/Custody
  - Both disk and file images need to conform to chain of evidence/chain of custody requirements are about:
    - Available Evidence?
    - How such evidence have been got?
    - Time of evidences collection?
    - Handled by whom?
    - How that person is chosen to handle it?
    - Locations where it has travelled, and stored?

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

Secure

- Encase disk acquisition
  - start Encase
    - without dongle → acquisition edition
    - with dongle → forensic edition
  - create a new case
  - select Devices view
  - from menu select File, Add Device…
  - select which option you are going to use
    - Local Drives
  - press Next

Secure

- so far you have just added a preview of a device or drive
- acquisition has not started
- return to Cases view
  - the newly added device or drive will show up
  - you can preview the data on the device or drive
- right click the newly added device or drive OR from the menu select Edit, Acquire…

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

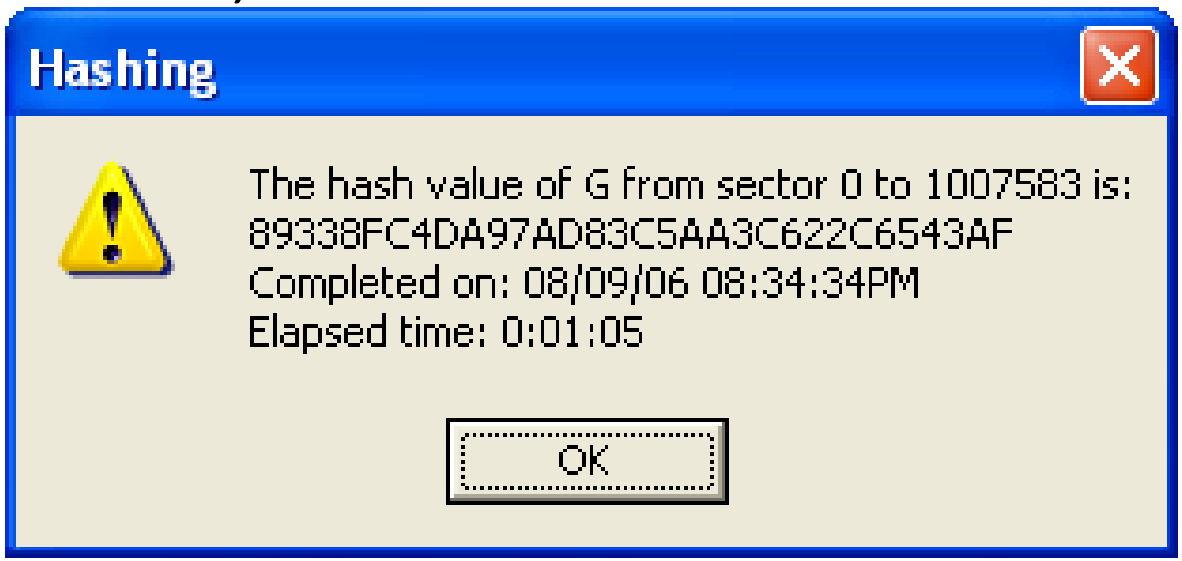
Secure

- this creates an evidence file (*.E01) in the directory you requested
- the image file now has to be added to the case
- EnCase only creates evidence files in Guidance software's own proprietary format
- EnCase can read other types of disk images
- Other toolkits (e.g. Access Data's FTK) can read EnCase's proprietary format

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

Secure

- hash generation
  - in Cases view, right click the device to be imaged
  - select Hash…
  - OR select Edit, Hash from the menu



Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

Secure

- Adding evidence files
  - Open a case
  - Select Add Device (button or right click or File menu)
  - Select Evidence Files
  - Right click evidence files
  - select directory where evidence file was stored
  - select evidence file
  - press Next

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

Secure

- Access Data's tools include
  - Forensic Tool Kit
  - FTK Imager
  - PRTK (Password Recovery Toolkit)
  - KFF (Known File Filter)

  - FTK Imager, PRTK and KFF integrate into FTK
    - no need to run separately but you can

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

Secure

- Once an image is created, it can be added to:
  - FTK Imager using File, Add Evidence Item
  - Forensic Toolkit
    - evidence will be indexed before it can be viewed

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

This Week

- Computer Forensics Process
  - Identify
  - Secure
  - **Analyse**
  - Present

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).