BCN3139– 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 3rd Edition).

Chapter Description

- Aims
  - Explain the process of forensic investigation
  - Describe the rules of digital evidences
  - Explain the general service of computer forensic
- Expected Outcomes
  - Students can explain the purpose computer forensic investigation
  - Show some examples to support their understanding
  - Students can explain on What, How, Why Digital Forensic
- Other related Information
  - …..
- References

– Vacca, J.R., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005, Charles River Media Inc.

– nelson, B., Philips, A., Enfinger, F. and Steuart, C., Guide to Computer Forensics and Investigations 3rd Edition, Thomsan Course Technology.

Source: (Nelson, Guide to Computer Forensics and Investigations 3rd Edition).

Computer / Digital Forensic

- **P**rocess/study of identifying, preserving, analyzing and presenting digital evidence in a format that is admissible in the court.

- Collecting evidences of cybercrime from computers that is admissible in court and be convincing.

Source: (Nelson, Guide to Computer Forensics and Investigations 3rd Edition).

Computer / Digital Forensic

- **Requires knowledge on computer components hardware and software.**
- **Practitioner on DF domains should understand the local, national, regional and international law which are significant to the legibility of evidence collection process.**

Source: (Nelson, Guide to Computer Forensics and Investigations 3rd Edition).

Categories of Computer crime

1. Computer as a target

2. Computer as an instrument of the

3. Computer as incidental to a crime

4. Crimes associated with the prevalence of a computer

Source: (Nelson, Guide to Computer Forensics and Investigations 3rd Edition).

Other Cyber-Crimes

- Device (Laptop, mobile, phone) theft
- Denial of Service (DoS) Attack
- System Penetration
- Wardriving: wireless network abuse
- Intellectual Property theft
- Financial fraud (credit card theft)

Source: (Nelson, Guide to Computer Forensics and Investigations 3rd Edition).

Common Reported Cybercrime

- Financial Fraud (scams) - 26%
- Child pornography - 17%
- Stalking - 11%
- E-mail abuse - 9%
- Harassment/Threats - 9%
- Hacking/Viruses - 9%
- Children Related - 6%
- Copyright Violations - 4%
- Terrorism -3%
- Chat room abuse - 2%
- Other - 4%
- **Complaints under investigation**: 26,834

Source: (Nelson, Guide to Computer Forensics and Investigations 3rd Edition).

Computer crime vs computer security violations

- Any violations in computer security is generally considered a computer crime
  - – unauthorized access
- Not all computer crimes are always violations of computer security
  - – Harassment, child pornography, cyberstalking

Source: (Nelson, Guide to Computer Forensics and Investigations 3rd Edition).

Computer crime Analysis

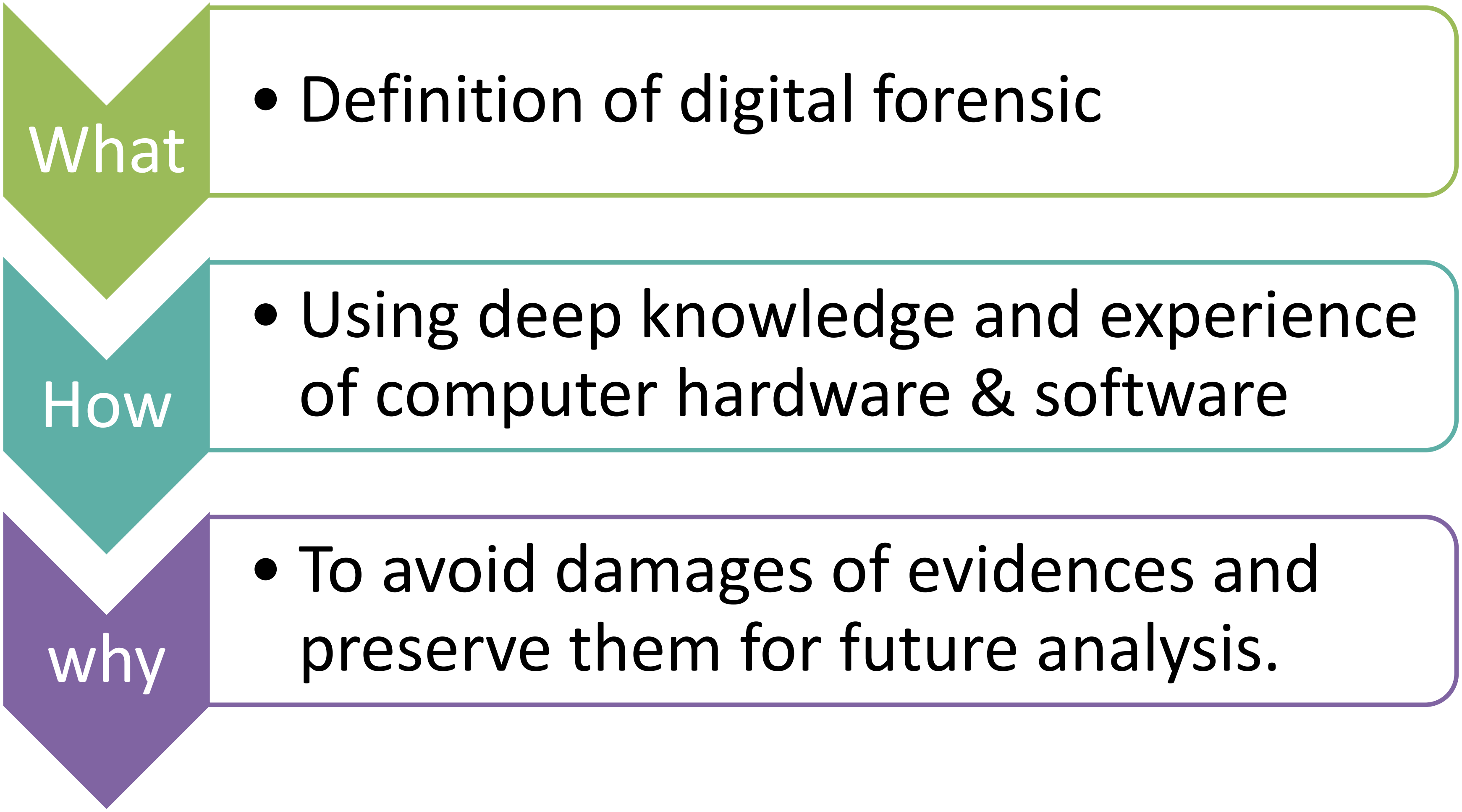
- Motive
  - Hacker motivation to perpetrate the crime
- Target
  - Hacking victims
- Role of the computer
  - As a tool or a target
- Type of “security incident”
  - What kind of incident used for hacking
- Level of skill
  - Hacker skills level (basic , advanced, professional)
- Level of privilege
  - Using outsider or insider privilege

Source: (Nelson, Guide to Computer Forensics and Investigations 3rd Edition).

What, How, Why Digital Forensic

Source: (Nelson, Guide to Computer Forensics and Investigations 3rd Edition).

Cont…



What

- Definition of digital forensic

How

- Using deep knowledge and experience of computer hardware & software

why

- To avoid damages of evidences and preserve them for future analysis.

Source: (Nelson, Guide to Computer Forensics and Investigations 3rd Edition).

Digital Evidence

- Any and all digital data that may be used to recognize cybercrime perpetrators.
- Digital Evidence vs Physical Evidence
  - Electronic Material
  - Less capacity - easier to hide
  - easy to be forged/tampered
  - It may be stored with many formats
  - Difficult to be destroyed once it is created
- Ubiquitous

Source: (Nelson, Guide to Computer Forensics and Investigations 3rd Edition).

Digital Evidence

- Some Digital Evidence Sources
  - Devices and Peripherals
    - Disks – hard, floppy, USB, tapes, RAID arrays, Memory cards/sticks
    - Mobile phones, PDAs, Smart phones, Blackberry
    - iPod, MP3 players
    - Cameras – still, video
    - Smart cards
    - Embedded devices – cars, washing machines, appliances
    - Dictation recorders
    - Fax machines

Source: (Nelson, Guide to Computer Forensics and Investigations 3rd Edition).

Digital Evidence

- Applications
  - Web browsers
  - Email
- Data
  - Documents
  - Databases
- Logs
  - Servers – web, proxy, SSL, file, web app
  - Transactions - Bank, EFTPOS, Credit card
  - Phone records, SMS, MMS
  - Web searches
  - Physical access records
  - Bookings, Tickets, Parking records
- CCTV
- and more...

Source: (Nelson, Guide to Computer Forensics and Investigations 3rd Edition).

Categories of Digital Evidence

- normal data
  - Normal data files
- meta-data
  - Data about data
- system data
  - Data about implementation of policy and operations in a particular environment
  - Records computer events

Source: (Nelson, Guide to Computer Forensics and Investigations 3rd Edition).

Digital Evidence

- Deleted data
  - "Computers do not destroy data, they ignore it"
- Hidden, lost and ambient data
  - Hidden files and directories
  - Lost files
  - Ambient data
  - Encrypted files
  - Ghost data

Source: (Nelson, Guide to Computer Forensics and Investigations 3rd Edition).

Digital Evidence

- Garbage retrieval
  - print spoolers
  - swap files
  - cache
  - recycle bins
  - intermediate servers

Source: (Nelson, Guide to Computer Forensics and Investigations 3rd Edition).

Questions

Have Question ?

Source: (Nelson, Guide to Computer Forensics and Investigations 3rd Edition).