Universiti Malaysia PAHANG
Engineering • Technology • Creativity

Computer Forensic & Investigation

Understanding Computer Investigations

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

Source: (Nelson et al., Guide to Computer Forensics and Investigations 3rd Edition, 2015).

Objectives

- Explain computer investigation process
- Explain systematic method of an investigation
- Explain procedures for corporate high-tech investigations
- Describe requirements of data recovery
- Explain method of conducting an investigation
- Discuss completing and criticizing a case

Source: (Nelson et al., Guide to Computer Forensics and Investigations 3rd Edition, 2015).

Preparing a Computer Investigation

- Main task of digital forensics expert is to collect evidence for proving that a computer digital crime is committed by a particular suspect
- To collect evidence admissible in court or at a corporate inquiry, forensic investigator should consider:
  - – Investigate the computer/device of the suspect

Source: (Nelson et al., Guide to Computer Forensics and Investigations 3rd Edition, 2015).

Preparing a Computer Investigation (cont.)

  - Preserving obtained evidence on a different computer or different media.

- Practice a standard procedure on case preparation.

Source: (Nelson et al., Guide to Computer Forensics and Investigations 3rd Edition, 2015).

An Overview of a Computer Crime

- Law enforcement officers use information which they may find on Computers for determining:
  - Chain of events leading to a crime
  - Evidence that can lead to a conviction
- In acquiring crime evidence, law enforcement officers have to practice appropriate procedure especially when the evidence is subjected to be altered by an overeager investigator

Source: (Nelson et al., Guide to Computer Forensics and Investigations 3rd Edition, 2015).

An Overview of a Computer Crime

- Information on computer disks may be encrypted, hidden or protected by password

Source: (Nelson et al., Guide to Computer Forensics and Investigations 3rd Edition, 2015).

An Overview of a Company Policy Violation

Abusing resources by employees causes a heavy loss to the company. Such resources include:

Surfing the Internet

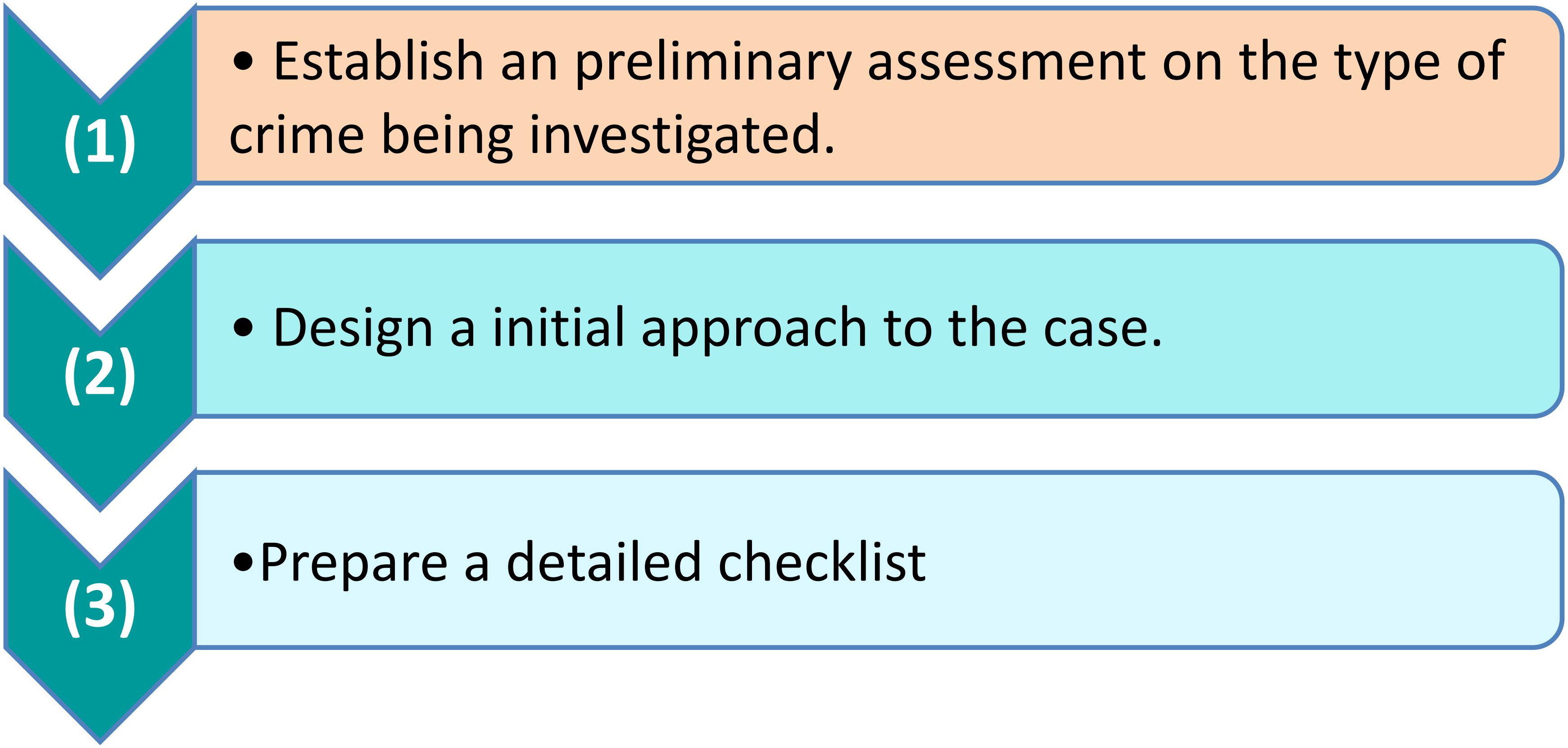
Sending personal e-mails

Using company computers for personal purposes

Source: (Nelson et al., Guide to Computer Forensics and Investigations 3rd Edition, 2015).

Taking a Systematic Approach

- Steps for digital crime investigation



(1)

- Establish an preliminary assessment on the type of crime being investigated.

(2)

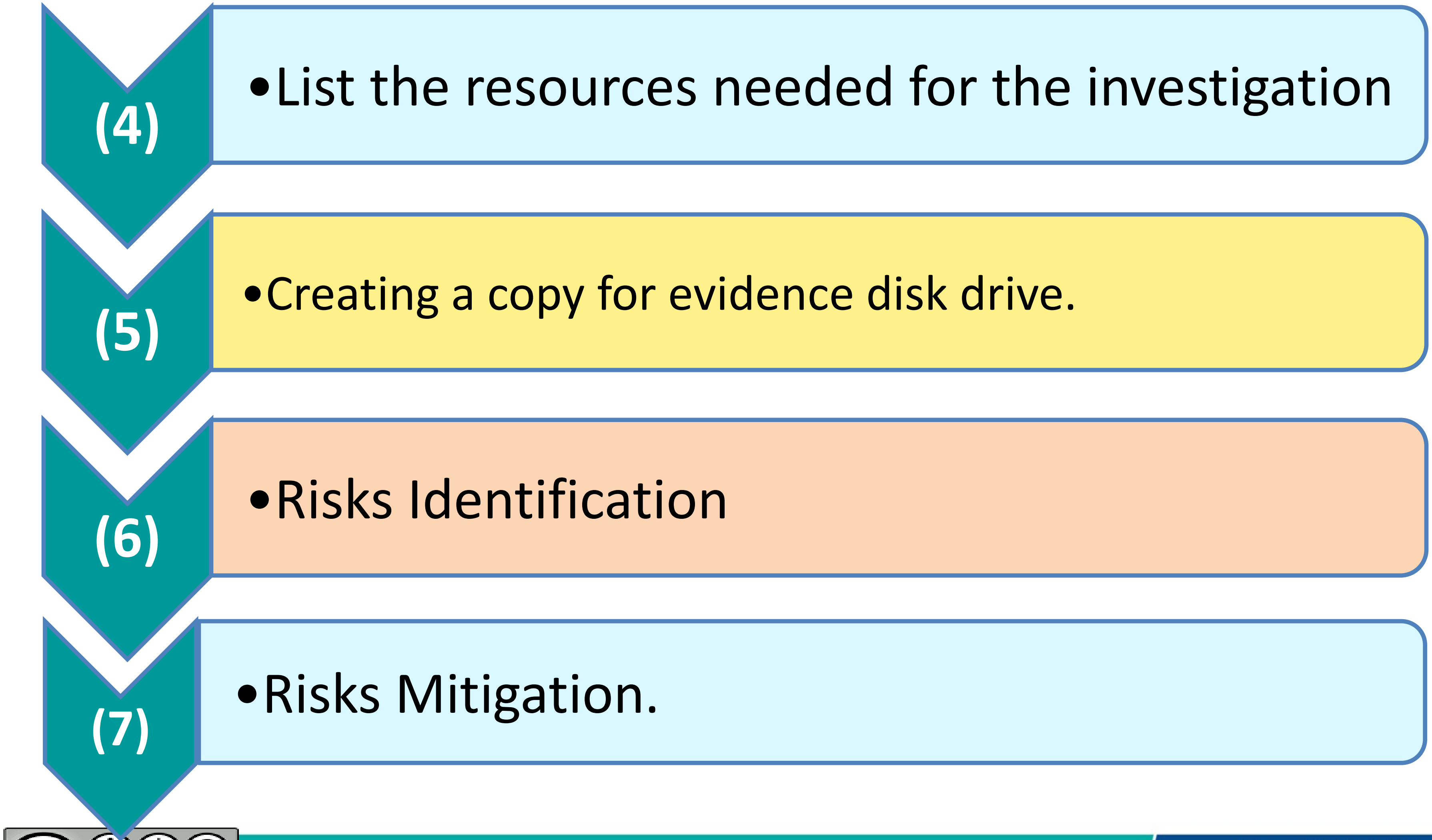
- Design a initial approach to the case.

(3)

- •Prepare a detailed checklist

Source: (Nelson et al., Guide to Computer Forensics and Investigations 3rd Edition, 2015).

Taking a Systematic Approach (Cont.)



(4)

- List the resources needed for the investigation

(5)

- Creating a copy for evidence disk drive.

(6)

- Risks Identification

(7)

- Risks Mitigation.

Source: (Nelson et al., Guide to Computer Forensics and Investigations 3rd Edition, 2015).

Taking a Systematic Approach (Cont.)

(8)

- Design Testing.

(9)

- Evidence analysis and recovering.

(9)

- Examine the data recovered.

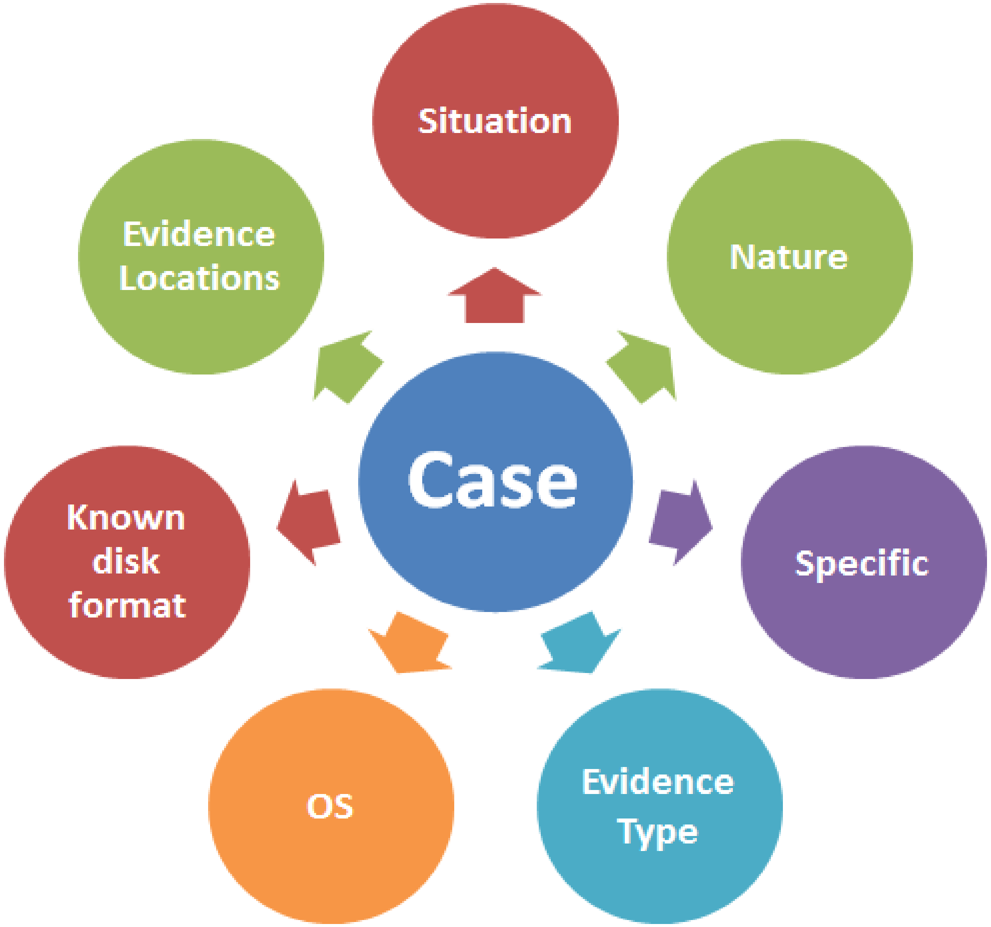
(10)

- Create a report for the case being investigated.
- Criticize the investigated case

Source: (Nelson et al., Guide to Computer Forensics and Investigations 3rd Edition, 2015).

Assessing the Case

- Systematically outline the case details



Source: (Nelson et al., Guide to Computer Forensics and Investigations 3rd Edition, 2015).

Assessing the Case (cont.)

- Using the case details, forensic investigator determines case requirements as below,
  - **Evidence type**
  - **Forensics investigation tools**
  - **Special OS if needed**

Source: (Nelson et al., Guide to Computer Forensics and Investigations 3rd Edition, 2015).

Planning Your Investigation

- A standard plan of investigation encompasses:
  - Acquire possible evidence
  - Establishing a chain of custody and completing form of evidence
  - Bring the obtained evidence into forensics lab
  - Use an **approved secure container to** secure the obtained evidence

Source: (Nelson et al., Guide to Computer Forensics and Investigations 3rd Edition, 2015).

Planning Your Investigation (cont.)

- – Setup a workstation for forensics processes
- – Take the evidence kept in the secure container
- – Create a copy for the original evidence
- – Return the original evidence to the secure container
- – Investigate the copied evidence using proper forensics tools

Source: (Nelson et al., Guide to Computer Forensics and Investigations 3rd Edition, 2015).

Planning Your Investigation (cont.)

- Forensic investigator uses an **evidence custody form to** record all the processes which have been done on the original evidence and its copies.
- There are two types for evidence custody form:
  - **Single-evidence form**
    - Every single evidence is listing on a different form
  - **Multi-evidence form**
    - Multiple evidences listing in one form

Source: (Nelson et al., Guide to Computer Forensics and Investigations 3rd Edition, 2015).

Securing Your Evidence

To secure digital evidence, forensic investigator need to:

Use **evidence bags** to secure and catalog the evidence

Use computer safe products

– Antistatic bags. – Antistatic pads

Use well-padded containers

Use evidence tape to seal all openings

– Floppy disk or CD drives. – Power supply electrical

Source: *(Nelson et al., Guide to Computer Forensics and Investigations 3rd Edition, 2015).*

Securing Your Evidence (continued)

Record initials on a tape to prove that evidence has not been tampered or altered.

Consider computer temperature and humidity specific

Source: (Nelson et al., Guide to Computer Forensics and Investigations 3rd Edition, 2015).

Questions

?

Source: (Nelson et al., *Guide to Computer Forensics and Investigations 3rd Edition, 2015).*