Universiti Malaysia PAHANG
Engineering • Technology • Creativity

Computer Forensic & Investigation

Understanding Computer Investigations

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

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

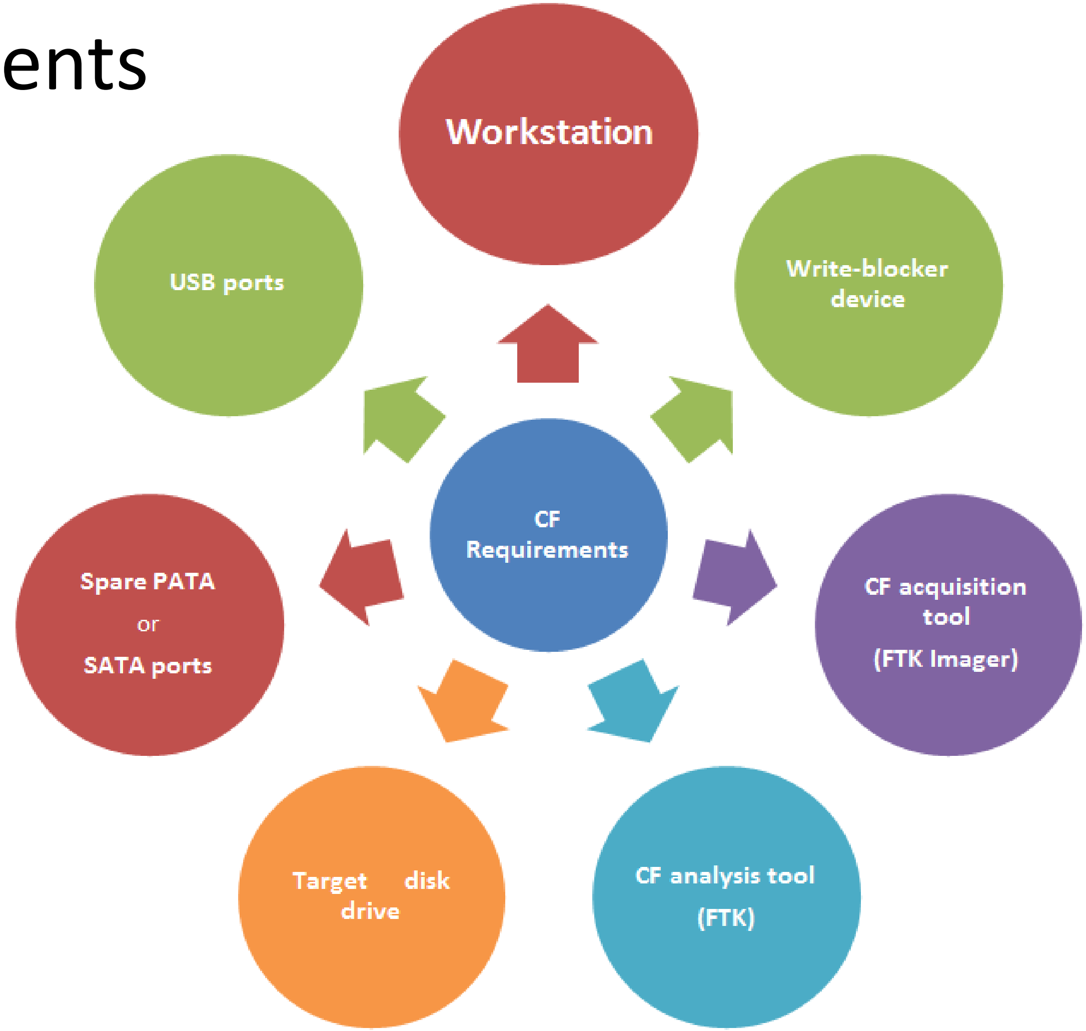
Understanding Data Recovery Workstations and Software

- Forensic Investigation is typically done on a forensics lab (or data-recovery lab)
- Data-recovery lab is related to digital forensics lab but not same.
- Computer forensics workstation
  - PC properly configured
  - Installed with forensics software
- To prevent evidence altering use :
  - forensics boot floppy disk/cd
  - Write-blocker devices

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

Setting Up your Computer for Computer Forensics

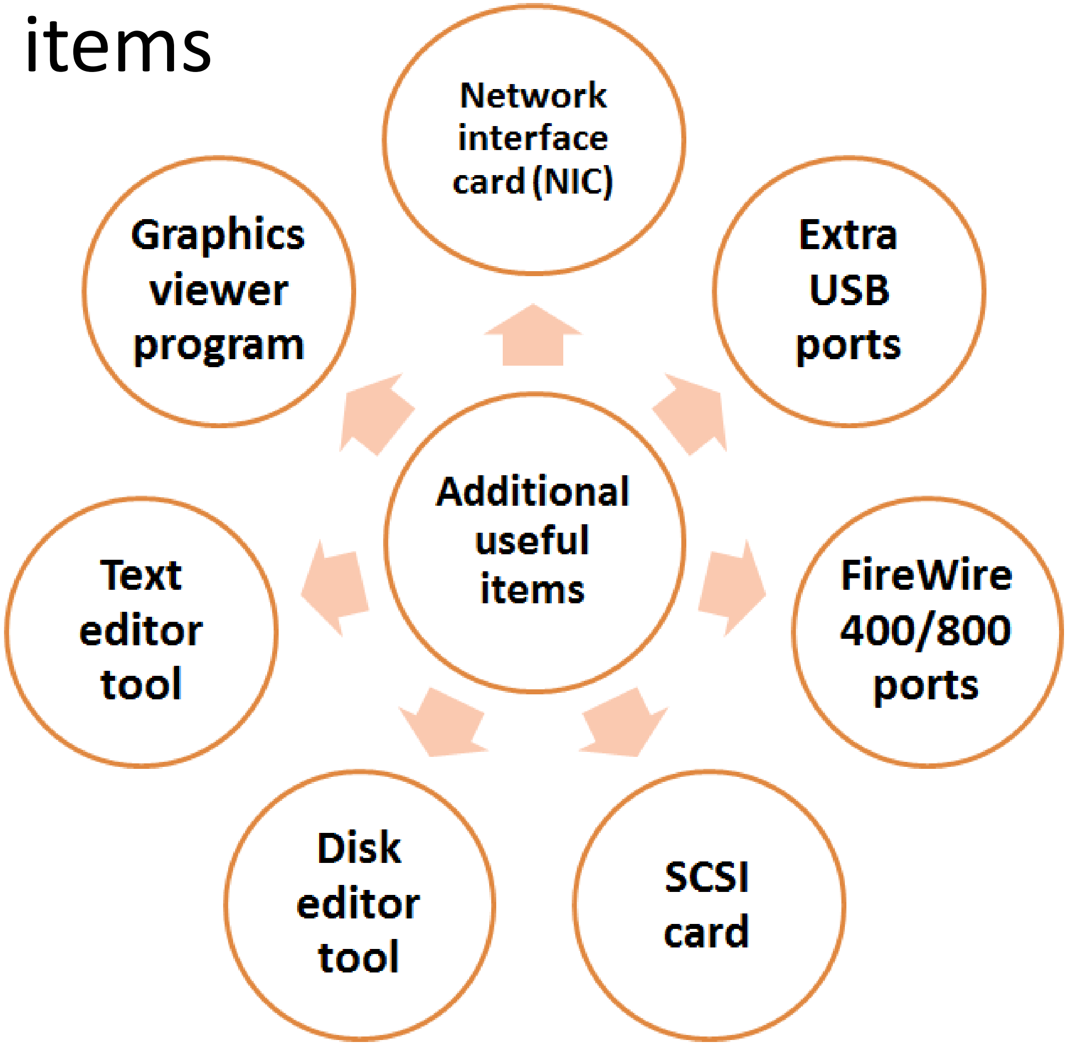
- Main requirements



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

Setting Up your Computer for Computer Forensics (continued)

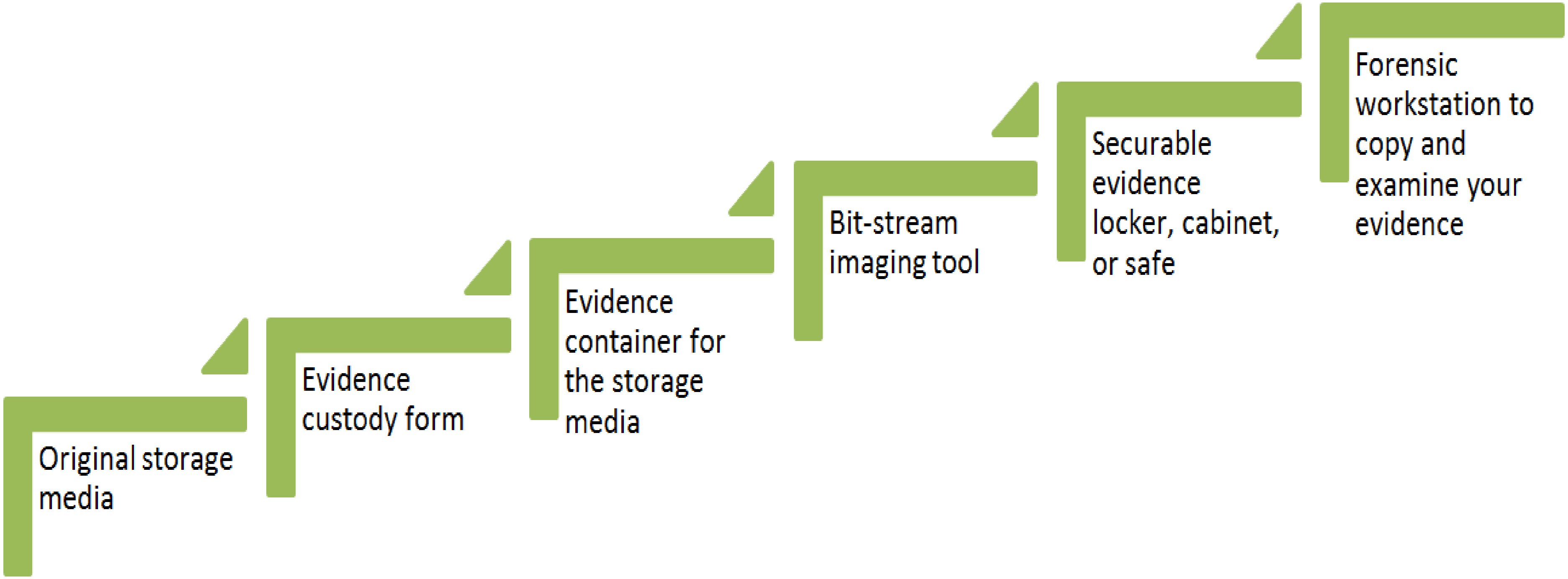
Additional useful items



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

Conducting an Investigation

- Collect resources determined in the investigation plan
- Requirements:



Original storage media

Evidence custody form

Evidence container for the storage media

Bit-stream imaging tool

Securable evidence locker, cabinet, or safe

Forensic workstation to copy and examine your evidence

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

Gathering the Evidence

- Protect evidence against damaging or altering
- Through:
  - Interview with IT manager
  - Complete form of the evidence, get signature of the IT manager
  - Follow all steps as stated in your planning Investigation

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

Understanding Bit-Stream Copies

- **Bit-stream copy**
  - Copy of the original storage medium Bit-by-bit
  - Exacting the created copy.
  - Created copy of the original storage medium is not similar to a simple backup copy because:

(1). Backup software only copies known files (active data)

(2). Backup software cannot copy deleted files, e-mail messages or recover file fragments

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

Understanding Bit-stream Copies (cont.)

- **Bit-stream image**
  - Known as forensic copy.
  - The bit-stream copy of all data existing on a disk or partition is copied to a file.
- Create a copy of an image file to the target, which should resemble the original disk manufacturer in terms of size and model.

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

Acquiring an Image of Evidence Media

- First rule of digital forensics investigation
  - Original evidence must be preserved first
- Analysis process is performed only on a created copy of the evidence being investigated

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

Completing the Case

- Final report is needed to complete the investigation case.
  - Describe what you did and what you found
- Attach report produced by forensic tool to record steps and activities of investigation process.

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

Completing the Case

- **Repeatable findings**
- Repeat the steps and obtain the same result, utilizing another forensic tools .
- Utilize a template of forensic report if needed.
- A typical forensic report contains only conclusive evidence
- The results of the investigation should indicate whether the suspect is innocent or guilty of committing the crime.

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

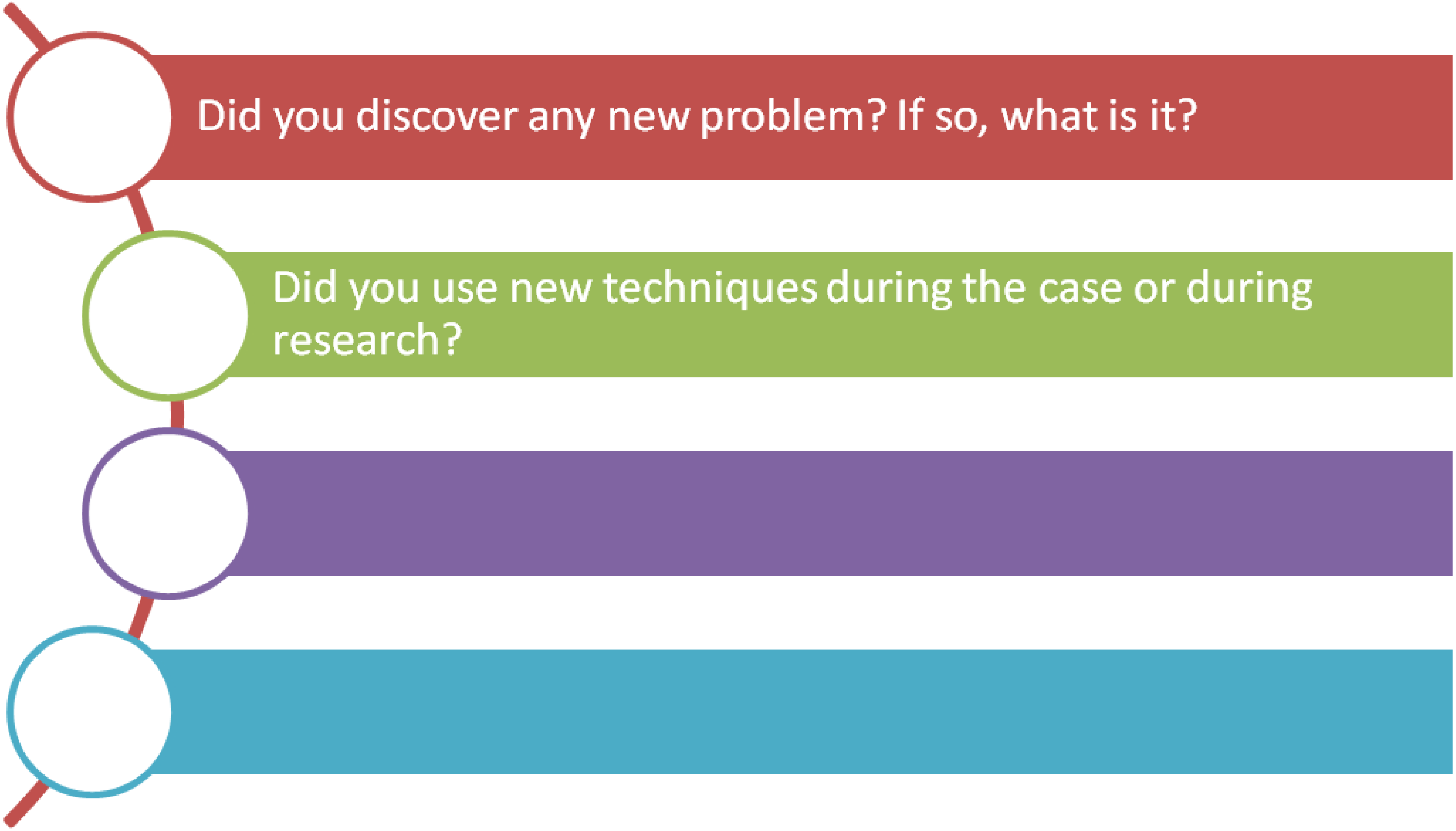
Critiquing the Case

Get answers for the following questions:

- How could you improve your performance in the case?
- Did you expect the results you found? Did the case develop in ways you did not expect?
- Was the documentation as thorough as it could have been?
- What feedback has been received from the requesting source?

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

Critiquing the Case (cont.)



Did you discover any new problem? If so, what is it?

Did you use new techniques during the case or during research?

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).