Computer Forensic & Investigation

Storage Formats for Digital Evidence

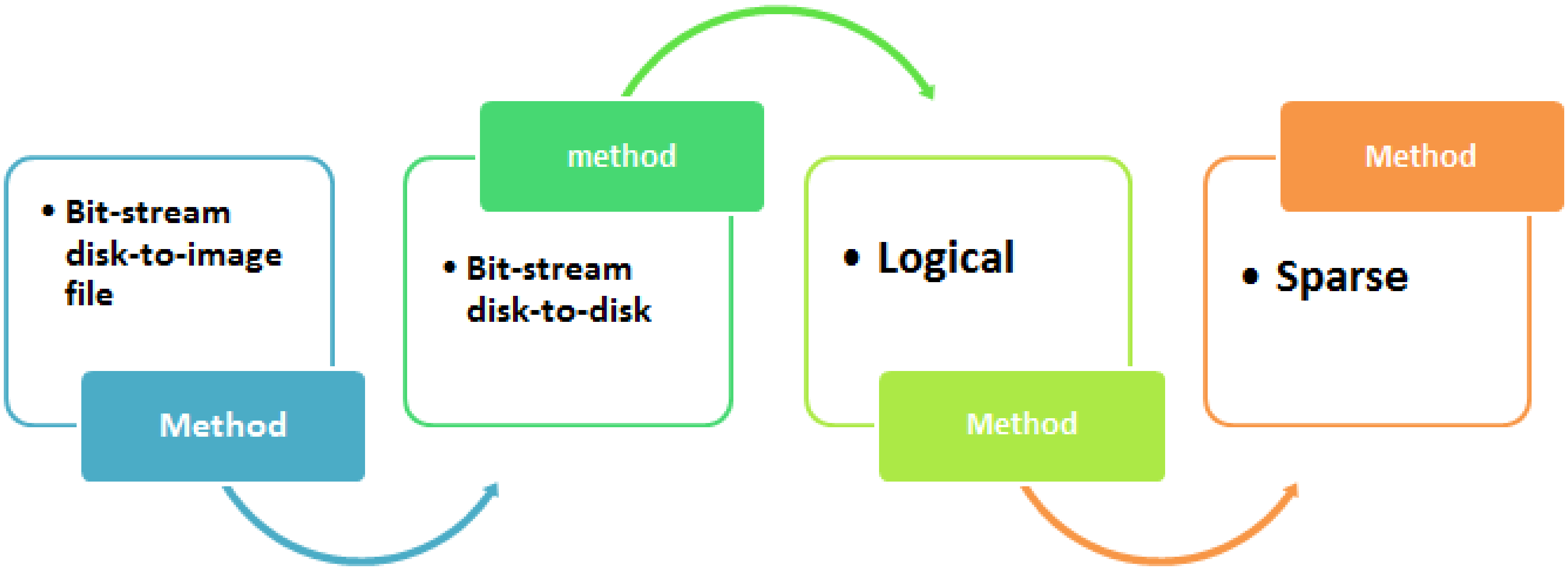
Editors
Dr. Abdulghani Ali Ahmed
Wan Nurulsafawati Wan Manan
Faculty of Computer Systems & Software Engineering
abdulghani@ump.edu.my

Source: (Nelson et al., Guide to Computer Forensics and Investigations 4th Edition, 2015).

Determining the Best Acquisition Method

- Acquisition is two types:

Static acquisitions and **live acquisitions**



Source: (Nelson et al., Guide to Computer Forensics and Investigations 4th Edition, 2015).

Bit-stream disk-to-image file

Bit-stream disk-to-image file method:

- Widely common
- It can create multiple copy
- Each Copy is a bit-for-bit duplication of the original disk.
- Tools: ProDiscover, EnCase, FTK, SMART, Sleuth Kit, X-Ways, iLook

Source: (Nelson et al., Guide to Computer Forensics and Investigations 4th Edition, 2015).

Bit-stream disk-to-disk

- Used when Bit-stream disk-to-image copy can not be used.
  - Errors due to incompatibility between Hardware and software
  - Generally it is good for older drives
- It can be used to adjusts geometry of target disk’s (cylinder, head, and track configuration) in order to match the suspect's drive
- Tools: EnCase, SafeBack (MS-DOS), Snap Copy

Source: (Nelson et al., Guide to Computer Forensics and Investigations 4th Edition, 2015).

Logical Acquisition and Sparse Acquisition

- To be used if evidence disk is big and time is inadequate.
- For logical acquisition, only particular files related to the case are captured like Outlook **.pst** or **.ost** files.
- For Sparse acquisition, some data is collected.

Source: (Nelson et al., Guide to Computer Forensics and Investigations 4th Edition, 2015).

Compressing Disk Images

- Data Compression is two types: Lossless and Lossy.
- Using a lossless compressing, a disk image can be compressed by 50% or more.
- However, ZIP files which are already compressed, will not be compressed much more
- The compressed image can be verified using MD5 or SHA-1 hash algorithms.

Source: (Nelson et al., Guide to Computer Forensics and Investigations 4th Edition, 2015).

Tape Backup

- In case of large drive, tape backup system can be a possible alternative.
- Volume of acquired data is unlimited. Number of tapes is also unlimited.
- Tape disadvantage is time. it’s slow

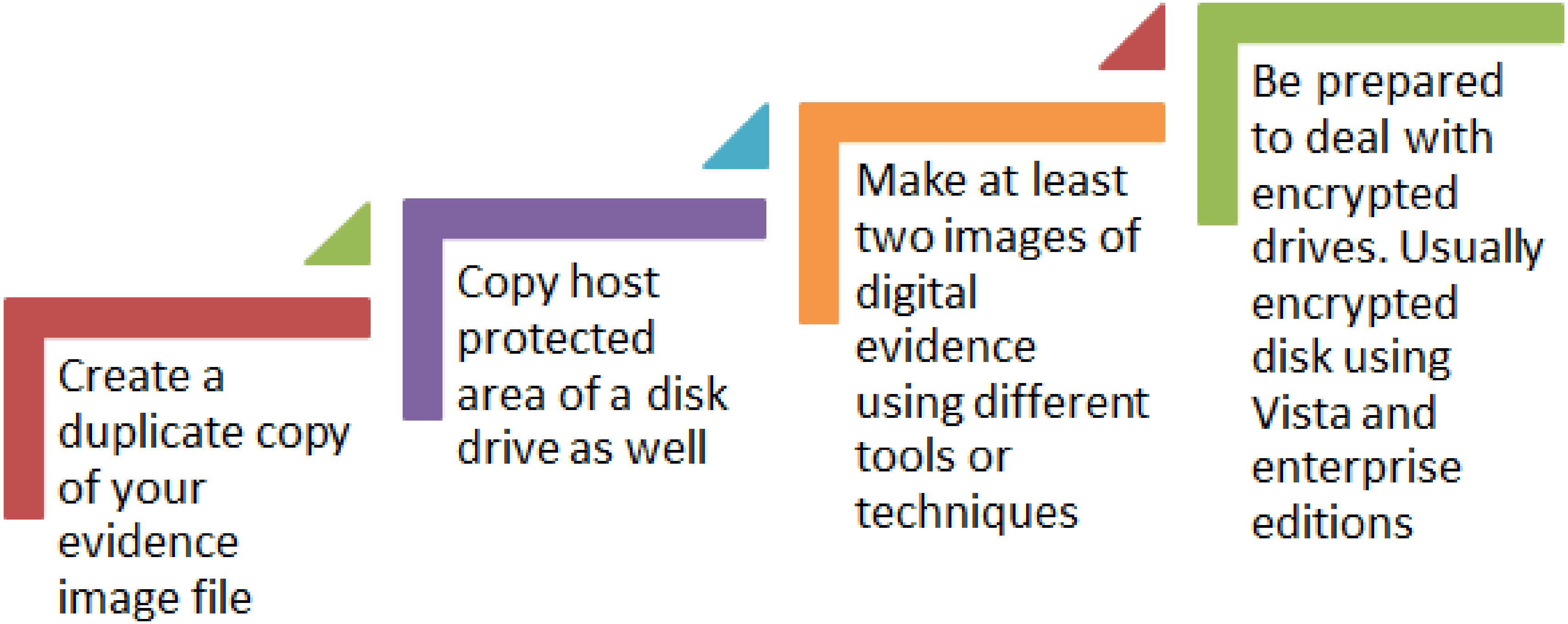
Source: (Nelson et al., Guide to Computer Forensics and Investigations 4th Edition, 2015).

Returning Evidence Drives

- In civil litigation, after imaging the original disk, a discovery order may ask forensic investigator to give it back.
- In case retaining the disk is impossible, investigator should make sure that a proper kind of copy (logical or bitstream) is made.
  - Client attorney or supervisor should know what is required to achieve the investigation process.

Source: (Nelson et al., Guide to Computer Forensics and Investigations 4th Edition, 2015).

Contingency Planning for Image Acquisitions



Create a duplicate copy of your evidence image file

Copy host protected area of a disk drive as well

Make at least two images of digital evidence using different tools or techniques

Be prepared to deal with encrypted drives. Usually encrypted disk using Vista and enterprise editions

Source: (Nelson et al., Guide to Computer Forensics and Investigations 4th Edition, 2015).

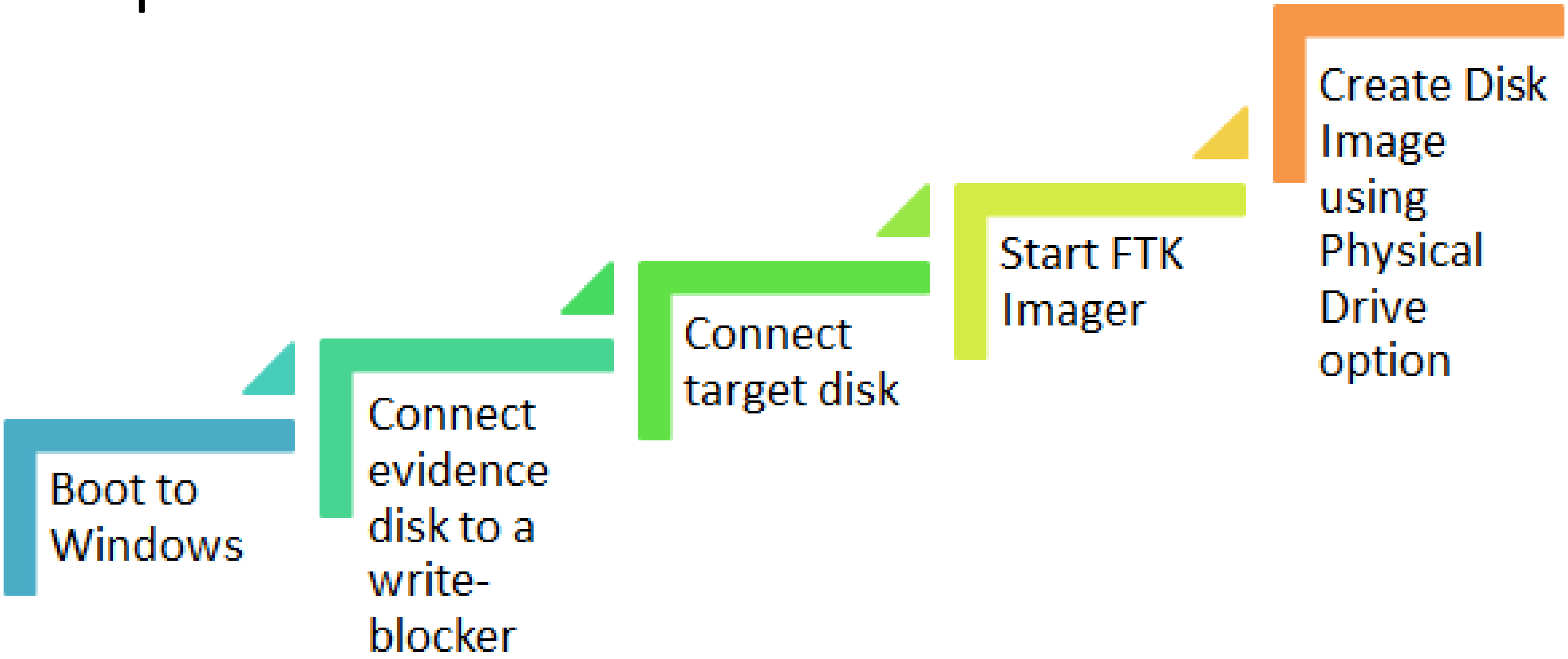
Encrypted Hard Drives

- To acquire data of encrypted drive,
- Need for Windows BitLocker OR TrueCrypt
- Data in a decrypted drive can be captured using a live acquisition.
- If can not, the encryption key or passphrase should be optioned.

Source: (Nelson et al., Guide to Computer Forensics and Investigations 4th Edition, 2015).

Capturing an Image with AccessData FTK Imager (continued)

Steps:



1. Boot to Windows
2. Connect evidence disk to a write-blocker
3. Connect target disk
4. Start FTK Imager
5. Create Disk Image using Physical Drive option

Source: *(Nelson et al., Guide to Computer Forensics and Investigations 4th Edition, 2015).*

Using Remote Network Acquisition Tools

- Using remote acquisition, data in a suspect computer can be remotely captured using network connection.
- Limitations:
  - – In case of LAN, slow data transfer and conflicts in routing table.
  - – Permissions required to access secure subnets
  - – Errors and delay are possible to occur in case of huge traffic.
  - – AntiVirus system may block remote access tool.

Source: (Nelson et al., Guide to Computer Forensics and Investigations 4th Edition, 2015).

Questions

?

Source: (Nelson et al., Guide to Computer Forensics and Investigations 4th Edition, 2015).