Universiti Malaysia PAHANG

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).

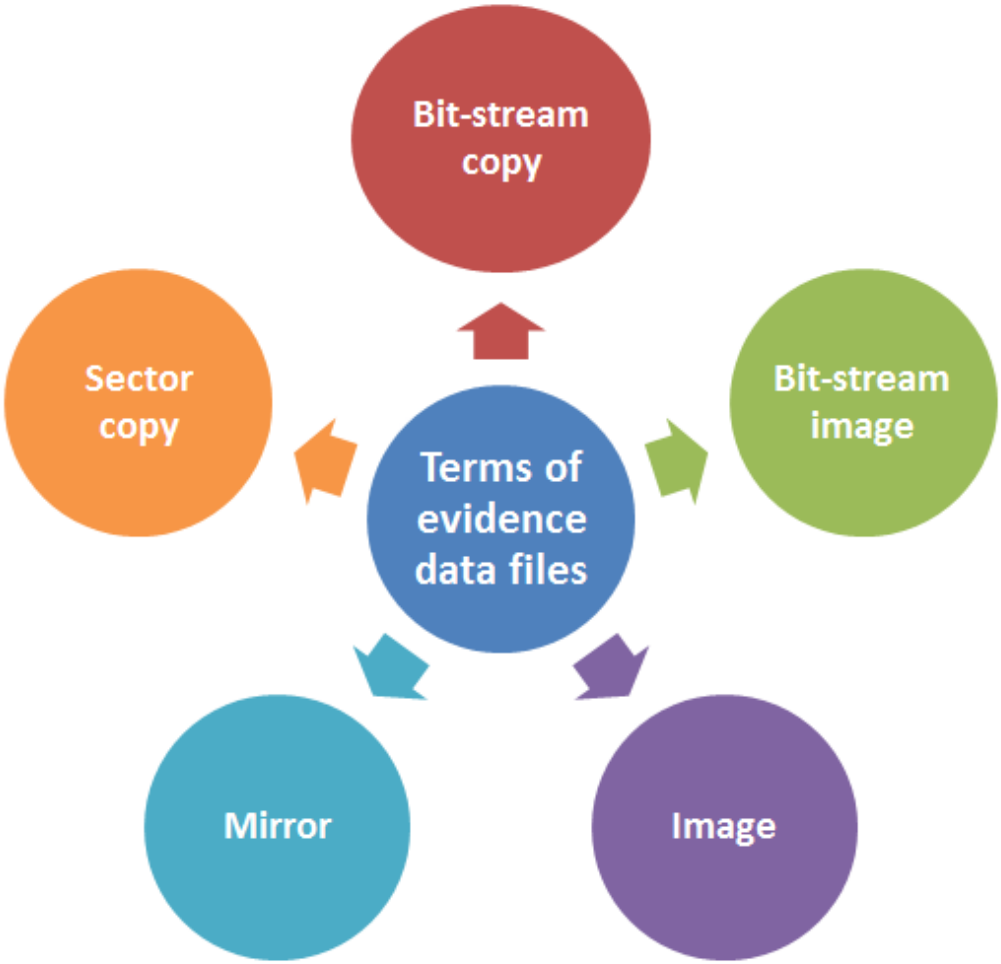
Understanding Storage Formats for Digital Evidence

- Acquisition method types:
  - Static acquisition
    - Standard method.
    - Copying data from a powered-off computer.
    - Data is not altered during acquisition process, thus it cab be repeated.
  - Live acquisition
    - Data is copied from a running system.
    - Preferred method especially for encrypted hard disk .
    - It alters data, so it can be repeated.
    - It is important to collect RAM data.

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

Understanding Storage Formats for Digital Evidence

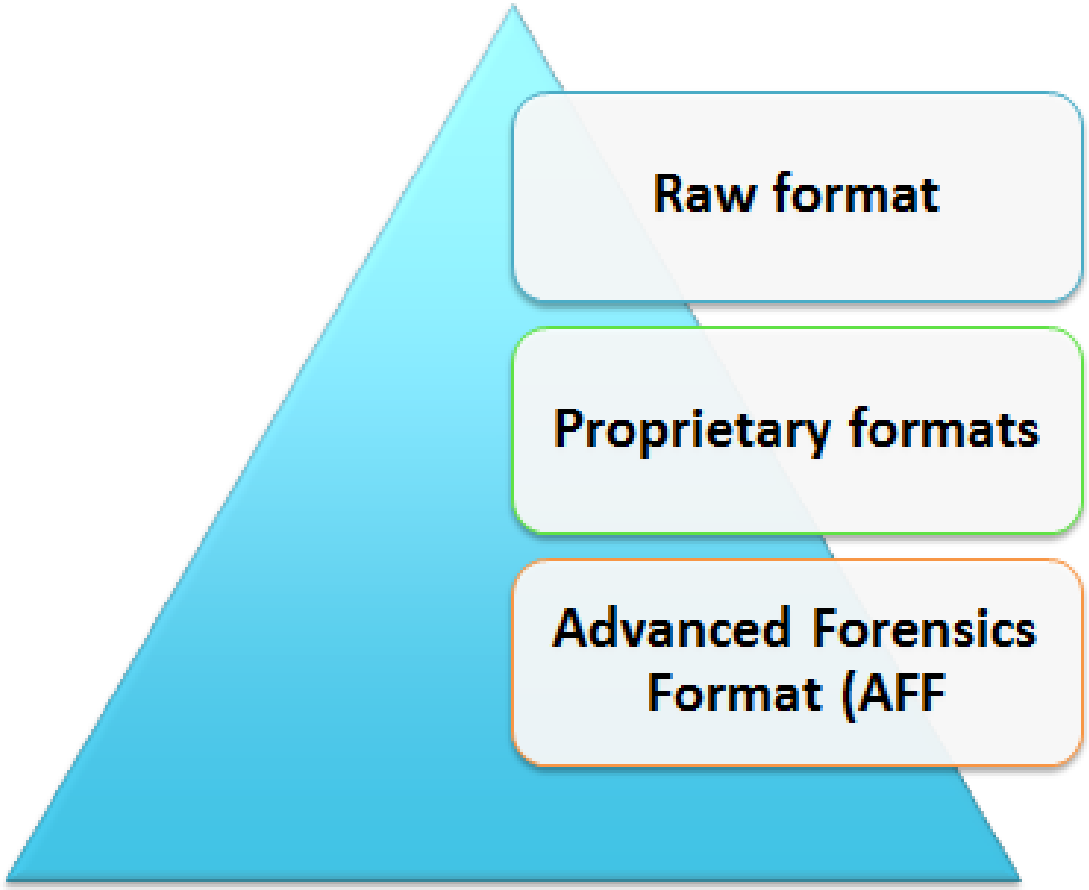
- Evidence data files terms:



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

Storage Formats for Digital Evidence

There are 3 evidence storage formats:



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

Raw Format

- This Format mostly used in Linux. Linux uses command “dd” to get Raw format.
- Drive is copied to a file using Bit-by-bit method.
- Advantages
  - Fast in transferring the data
  - Avoid minor errors of data read on source drive
  - Raw format can be read by most of digital forensics tools

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

Raw Format

- **Disadvantages**
  - Requires big storage, equals the data size on the original disk.
  - Bad sectors (Marginal) are not collected
  - Small threshold of retry once it reads on weak media spots
    - Free tools use less retries than commercial ones
  - Checking Validation is stored in isolated digest format such as MD5, SHA-1, and CRC-32.

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

Proprietary Formats

- Features offered
  - Compressing image files or not is an optional.
  - Image file may be devided into many segmented files
    - Integrity of data is checked for every segment

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

Proprietary Formats

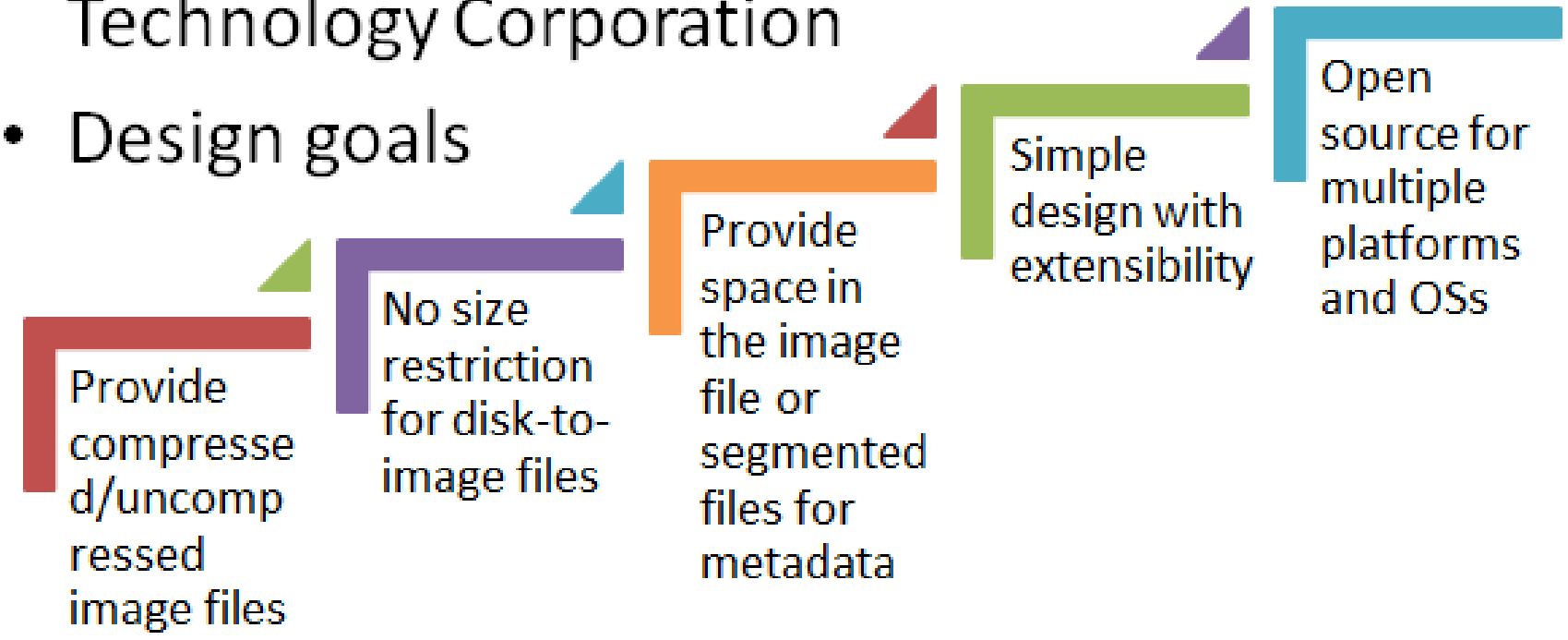
- Disadvantages
  - Sharing image file among several tools is not possible.
  - Has a file shortcoming for any segmented size
    - Typical size of segmented file is 650 MB or 2 GB
- Expert Witness format: unofficial standard
  - FTK, EnCase, X-Ways Forensics, and SMART used EW format
  - Able to generate compressed or uncompressed files.

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

Advanced Forensics Format

– Has several file extensions as **.E01**, **.E02**, **.E03**,

- Introduced by Dr. Simson L. Garfinkel of Basis Technology Corporation
- Design goals



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

Advanced Forensics Format (cont.)

- **“.afd”** is file extensions for segmented image files
- “**.afm”** is file extension for metadata of Advanced Forensics Format (AFF)
- The Advanced Forensics Format is open source

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).