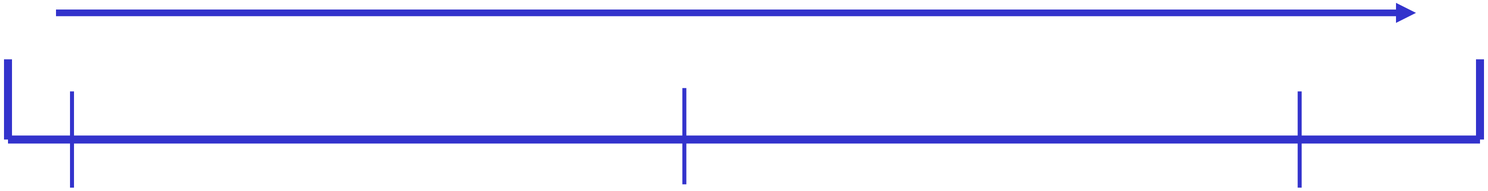
Introduction to Computer Forensics and Security

6G7Z1009

The Forensic Computing Process / Incident Response Strategy

Process



Identification & Preservation of evidence

Analysis of evidence

Documentation & Presentation of evidence

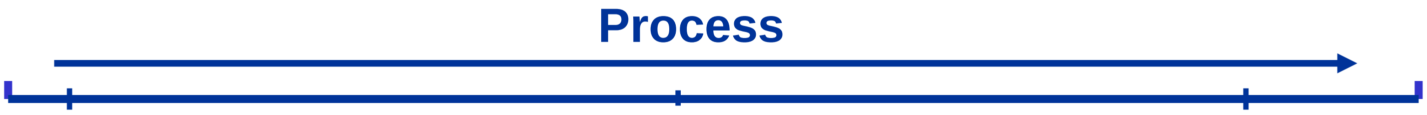
Identification & Preservation

Analysis

Documentation & Presentation

Identification of Evidence

- Can be called search and seizure, in which a trained officer will be used to do the this job. At Scene:
  - Secure the scene physically and electronically
  - Disconnect external data communications
  - Decide whether to switch off or leave alone



Process

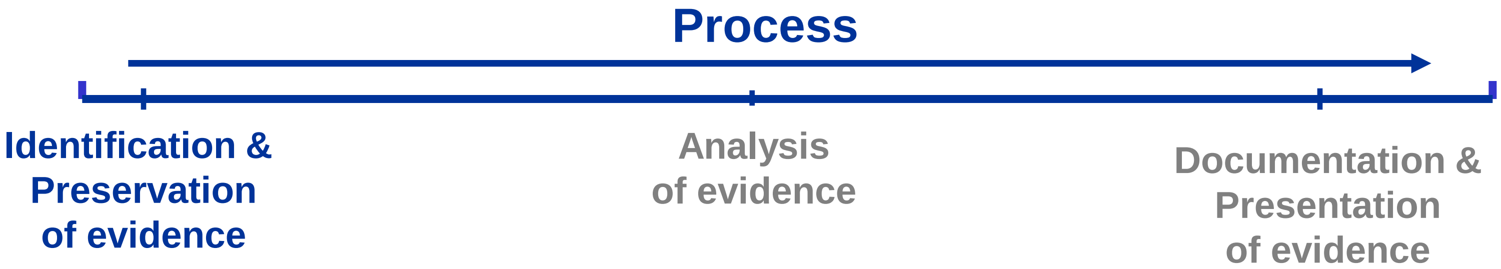
Identification & Preservation of evidence

Analysis of evidence

Documentation & Presentation of evidence

Identification of Evidence

- Can include any form of electronic data or devices such as:
  - Files
  - Emails
  - Internet activities
  - PCs, Laptops, Hard Drives, & Flash Memories.
  - Mobile phones, PDAs, & Digital Cameras.


Process
Identification & Preservation of evidence
Analysis of evidence
Documentation & Presentation of evidence

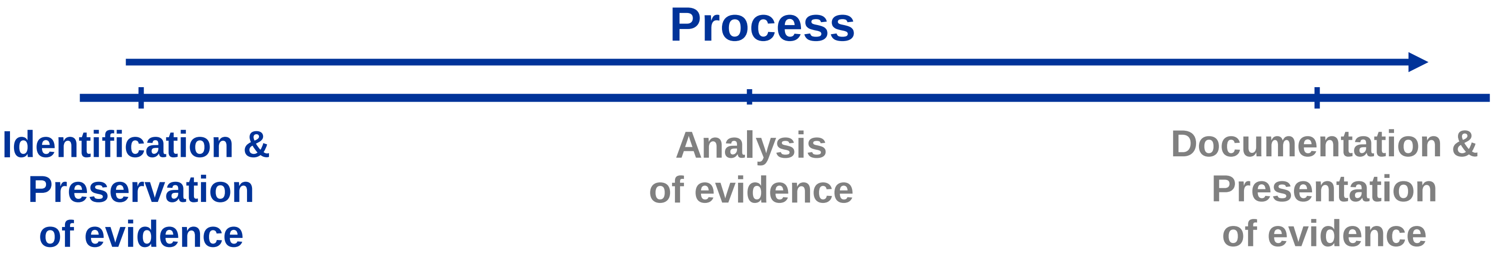
Preservation of Evidence

- Take all necessary measures to avoid altering or damaging the evidence
  - ➢ Package with care.
  - ➢ Transport to evidence locker if possible.

- Produce an exact copy of the hard disk (an “image”)

Hard disk Packaging

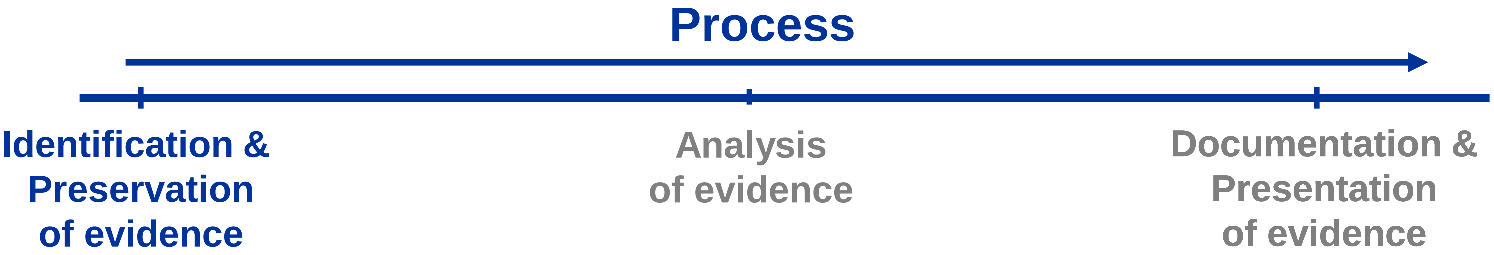
Drivelock write blocker



Process
Identification & Preservation of evidence
Analysis of evidence
Documentation & Presentation of evidence

Preservation of Evidence

- Record
  - Details of exhibit numbers/bag seal numbers
  - Details of system/media
  - Damage found
  - Other property found
  - Photograph of system (optional)
  - Comparison of system date/time with actual date/time.



Process

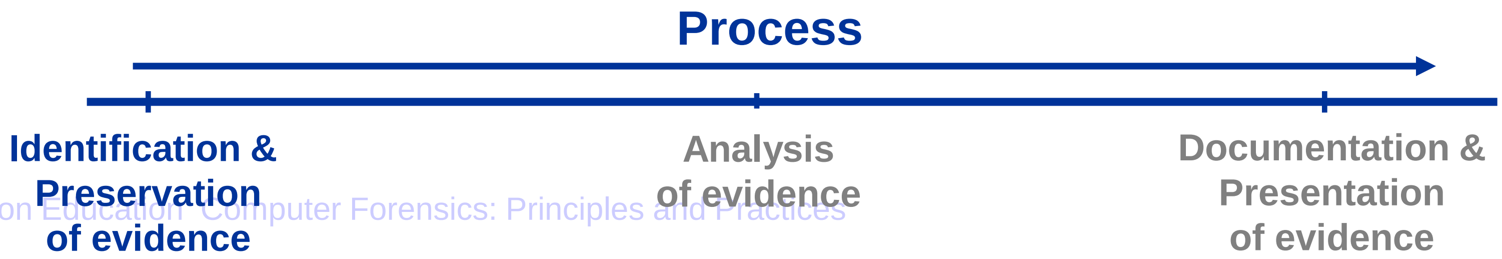
Identification & Preservation of evidence

Analysis of evidence

Documentation & Presentation of evidence

Preservation of Evidence

- Log book
  - Must be maintained
  - Must be secured
  - Must be taken to court
- Booking out
  - All property/exhibits must be booked out prior to analysis.



Process

Identification & Preservation of evidence

Analysis of evidence

Documentation & Presentation of evidence

Analysis of Evidence

- **Discovering all files** (normal files).
- **Recovering all (or as much as possible) of deleted files.**
- **Revealing the content of hidden files as well as temporary files** – ones used in both the application programs and the operating system.
- **Accessing the contents of protected and encrypted files.**

Analysis

Process

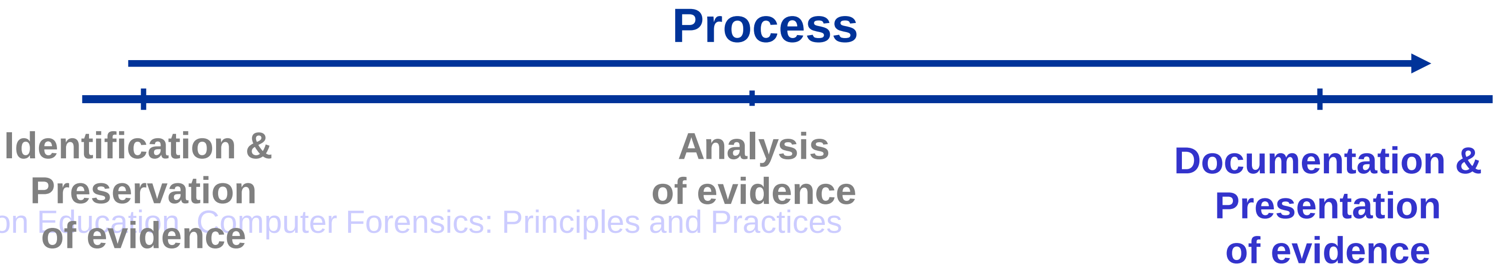
Identification & Preservation of evidence

Analysis of evidence

Documentation & Presentation of evidence

Documentation & Presentation of evidence

- A final formal report (State what you did and what you found).
- Witness statement.
- System image files.
- Extracted evidence.
- Forensic tool reports.
- Present and testify your findings.



Process

Identification & Preservation of evidence

Analysis of evidence

Documentation & Presentation of evidence

The Basic Principle

- “Evidence must not be damaged, destroyed or otherwise compromised by procedures used to investigate the computer, otherwise it may be rendered inadmissable.” (Qinetiq)

The Rules

- Maintain the integrity of the evidence.
- Do not work on the original evidence.
- Do not trust the computer system.
- Record all actions.

ACPO Principle 1

- “No action should be taken by an analyst that should change data held on a computer or other media which may subsequently be relied upon in Court.”

ACPO Principle 2

- “In exceptional circumstances where a person finds it necessary to access original data held on a target computer that person must be competent to do so and to give evidence explaining the relevance and implications of their actions.”

ACPO Principle 3

- “An audit trail or other record of all processes applied to computer-based evidence should be created and preserved. An independent third party should be able to examine these processes and achieve the same result.”

ACPO Principle 4

- “The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

Forensic Duplication - Imaging

- Normally, imaging takes place by hosting the hard disc drives in an imaging system
- Must record the media details
- Imaging should be performed in a ‘safe’ OS environment, with the devices mounted read-only.

Acquisition Methods

- Basic ways of acquiring
  - Bit-stream disk-to-image file
  - Bit-stream disk-to-disk

Acquisition Methods

- Bit-stream disk-to-image file
  - Most common method
    - Most flexible
  - Can make more than one copy
  - Direct input to EnCase, FTK, others
    - Saves time and disk resources
    - Don’t need to match disk geometry

Acquisition Methods

- Bit-stream disk-to-disk
  - Consider disk’s geometry
  - SafeBack, and Norton Ghost
    - Can adjust to different geometries
    - Must run in DOS mode

Using Windows Acquisition Tools

- Make job more convenient
  - Hot-swappable devices
  - Use USB or FireWire connections
- Drawbacks:
  - Windows can contaminate your evidence
  - Require write-blocking hardware/Software

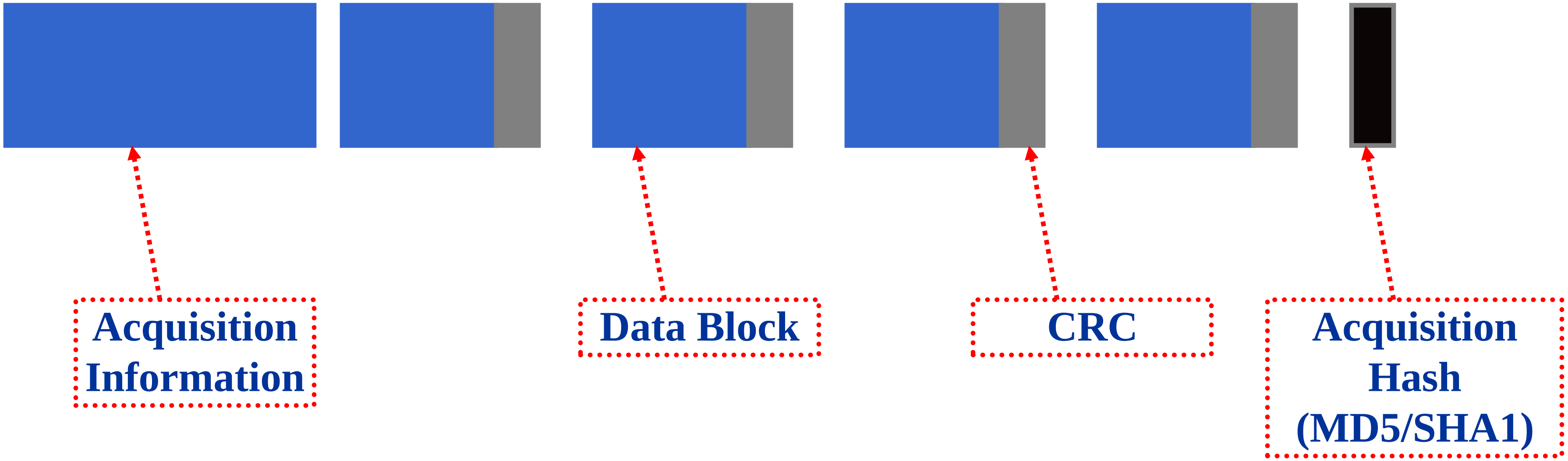
Disk Write Blockers

- Prevent data been written to the suspect drive.
- Ensure integrity of the suspect drive
- Software write blockers and hardware write blockers are available.

EnCase File Formats

- EnCase® v7 has two different formats for the evidence file: the Legacy format (.E01) and the Current format (Ex01).

EnCase Legacy Evidence File Format (.E01)



Acquisition Information

Data Block

CRC

Acquisition Hash (MD5/SHA1)

Verify the accuracy of the copy

- CRC cyclic redundancy check: computations to validate that the copy is exactly the same as original.
- Hashing is a digital fingerprint, an encryption technique referred to as cryptographic hash verification. MD5 (Message Digest 5) which is 128-bit hash value, and SHA-1 (Secure Hash Algorithm) which is This 160-bit hash value.

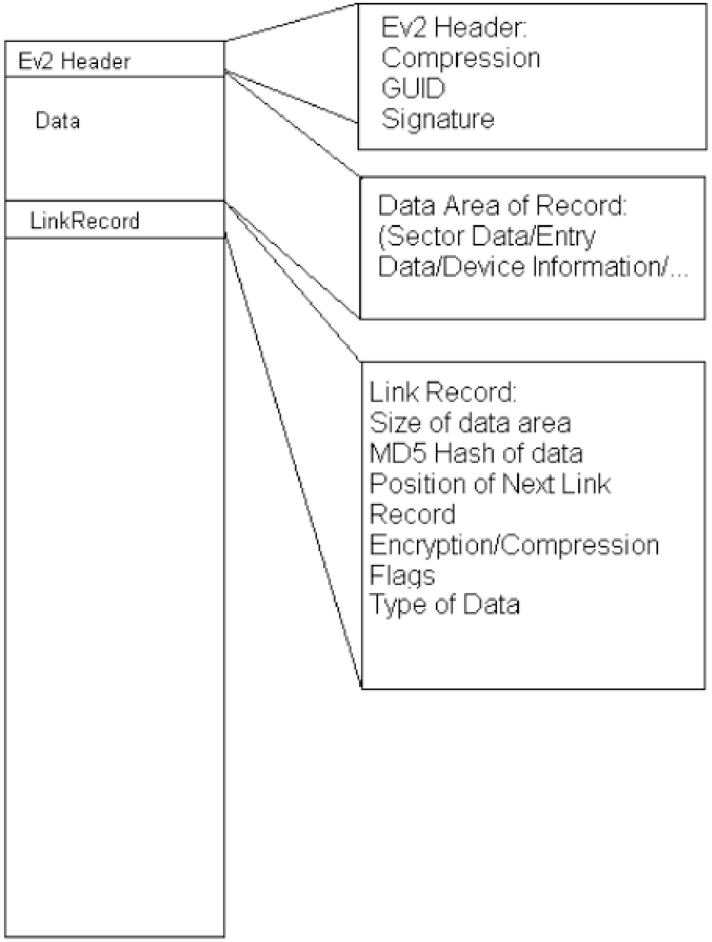
EnCase Compression

- EnCase uses an industry standard compression algorithm (Zlib) to achieve an average size reduction of 50%.

EnCase current evidence file formats .EX01

- EnCase v7 has a new evidence file (.Ex01) format, which restructured the way data is stored.
- The new format allows for encryption and supports a new compression algorithm (bzip2).
- Improved support for multi-threaded acquisitions, where sectors can be out of order.
- Efficient storage and handling of sector blocks that are filled with the same pattern (such as 00-byte fills).
- Internal improvements of the data structures

EnCase current evidence file formats .EX01 and .LX01



Ev2 Header

Data

LinkRecord

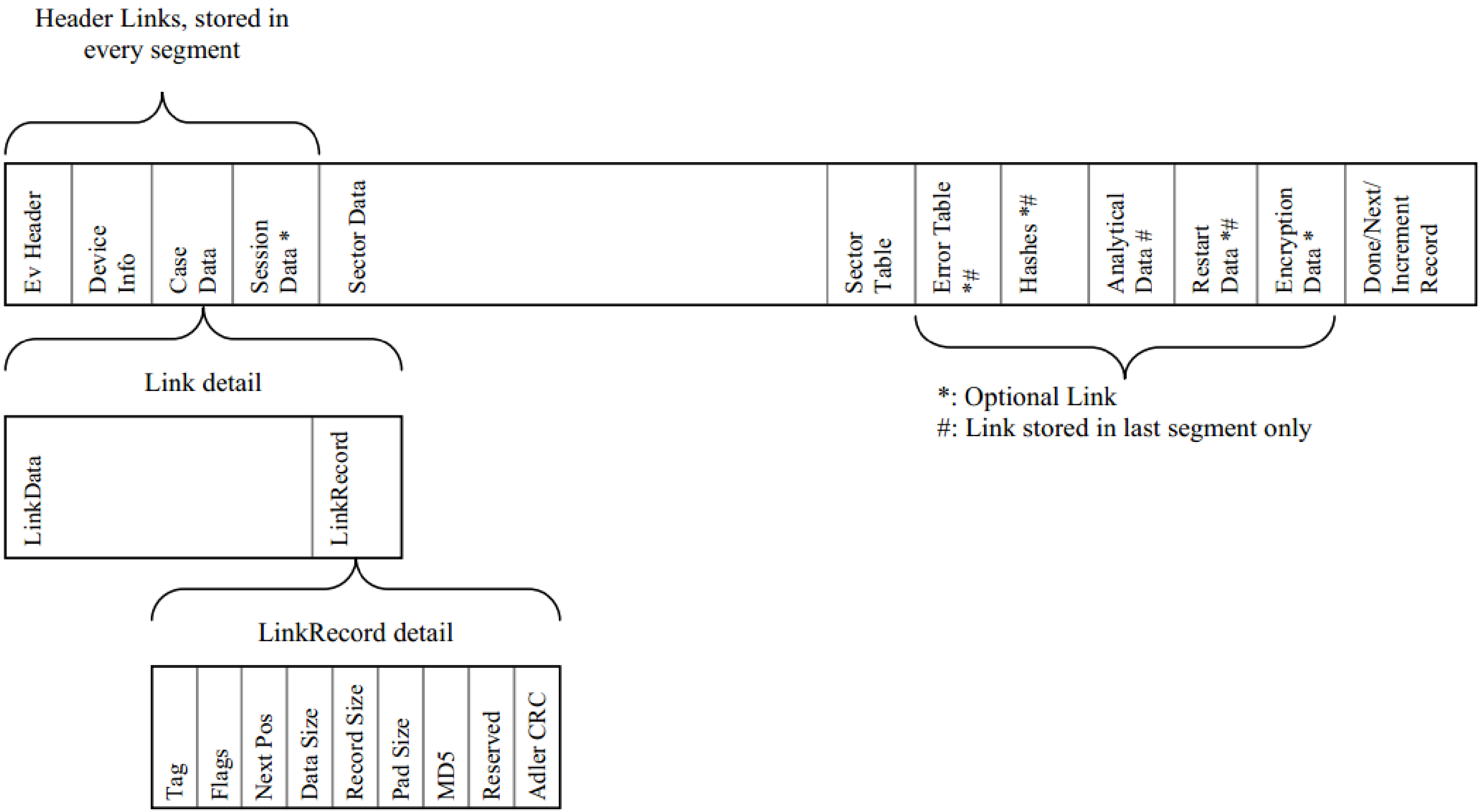
Ev2 Header:
Compression
GUID
Signature

Data Area of Record:
(Sector Data/Entry
Data/Device Information/...

Link Record:
Size of data area
MD5 Hash of data
Position of Next Link
Record
Encryption/Compression
Flags
Type of Data

Evidence File Segment Layout

Evidence File Segment Layout



Header Links, stored in every segment

Ev Header | Device Info | Case Data | Session Data * | Sector Data | Sector Table | Error Table *# | Hashes *# | Analytical Data # | Restart Data *# | Encryption Data * | Done/Next/ Increment Record

Link detail

LinkData | LinkRecord

LinkRecord detail

Tag | Flags | Next Pos | Data Size | Record Size | Pad Size | MD5 | Reserved | Adler CRC

*: Optional Link
#: Link stored in last segment only

Summary

- Make the forensic computing process your main incident response strategy.
- Apply ACPO principles
- Data acquisition methods:
  - Bit-stream disk-to-image file
  - Bit-stream disk-to-disk
- Be careful when using tools
- Windows data acquisition tools
  - Easy to use
  - Can modify data!
- Encase, FTK Imager, DD

Questions?

m.owda@mmu.ac.uk

References

- ACPO Guidelines, Good Practice Guide for Computer-Based Electronic Evidence, www.7safe.com.
- Access Data FTK Imager, www.accessdata.com
- EnCase 7 Computer Forensics Academic Program
- *M. Hatzesberger,* How to Forensically Acquire Data Using Software and Hardware Write-block Solutions**.**