Digital Forensics

File System Forensics Masterclass

Fraser Brown

Heriot-Watt University

February 21, 2018

Outline

Digital Forensics Background

Digital Forensics:

"Computer [Digital] Forensics is the practice of determining the past actions that have taken place on a computer system using forensic techniques and understanding artefacts." - David Cowen

Artefact:

"An Artefact is a reproducible file, setting or system change that occurs every time an application or operating system performs a specific action" - David Cowen

Analysis Types

Live Analysis:

"A live analysis occurs when you use the operating system or other resources of the system being investigated to find evidence." - Brian Carrier

Dead Analysis:

"A dead analysis occurs when you are running trusted applications in a trusted operating system to find evidence." - Brian Carrier

Why File System Forensics?

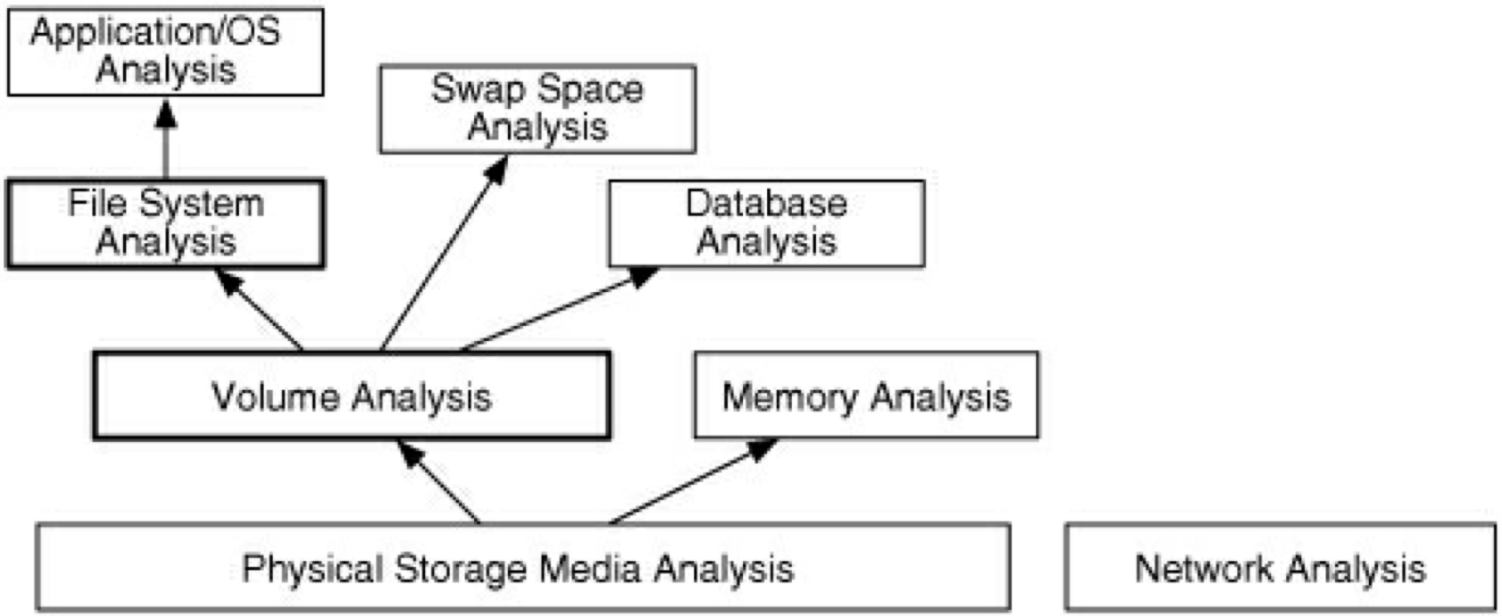

Figure: Layers of Analysis

Forensic Process

Evidence Acquisition/Imaging

- In order to perform analysis on digital artefacts a forensic duplicate of the media must be created.
- Forensic Duplicates are *bit-for-bit* copies of the original disk and can encompass the full disk or a single partition.
- This process is known as imaging or acquisition.
- Contents of a disk are always changing therefore *Write Blockers* are used to preserve the disk state.
- Hash functions such as SHA-256, SHA-1, MD5 are used to verify the image against the original artefact.

Write Blockers

Write Blockers

Are hardware or software devices that allow gathering of information without damaging the disk contents by blocking write commands but allowing read commands.

- Write Blockers are customisable:
  - Blocking of all or specific commands.
  - Can control the read and write speed.
- Write Blockers come in two forms:
  - *Native*: Same interface for input and output e.g. IDE-to-IDE
  - *Tailgate*: uses different interfaces for input and output e.g. firewire/USB-to-SATA

Imaging Challenges with Solid State Drives (SSD)

While an SSD can be imaged with the same tools as a traditional hard disk drive (HDD), there are technology specific issues that cause problems for forensic investigators.

- *Program-Erase cycles*
  - Sequence of events that result in data being written to a solid state flash memory cell, then erased and rewritten (e.g flash memory USB sticks).
  - These P/E cycles result in a small amount of physical damage to the medium, which can result in bad sectors.
- *Wear Levelling*
  - prolongs the life of solid state/flash memory
  - Distributes rewrites evenly across the medium, so no single block dies prematurely.
- These two technologies due to the evolution of memory results in unallocated space being overwritten earlier than it would on a HDD. This could overwrite valuable hidden information by accident

Image Types

- Raw Format (`.dd .raw .img`)
  - only contain data from the original artifact
  - meta data is no included however can be generated into a separate file by tools.
  - Tools: `dd`, `dcfldd`, `dd_rescue`, `rdd`, `df3dd`, `guymager`
- EnCase Evidence Format (Expert Witness `.E01`)
  - Expert Witness images use headers and footers to hold metadata about the image.
  - metatdata can include: drive type, source disk OS, timestamps, hashes, CRCs over blocks.

Memory

File System

Acquisition and Analysis Tools

Digital Forensic Research

Additional Resources

Careers