Digital Forensics

File System Forensics Masterclass

Fraser Brown

Heriot-Watt University

March 2, 2018

Outline

1. Overview
2. What is Digital Forensics?
3. Why File System Analysis?
4. Forensic Process
    - Digital Crime Scene Investigation Process Overview
    - PICL Guidelines
    - Analysis Types
5. Evidence Acquisition/Imaging
    - Write Blockers
    - Imaging Challenges
    - Image Types
6. File Systems
    - File System Aspects/Categories
7. File System Analysis Techniques
8. The Sleuth Kit (TSK)
    - TSK Layers
9. Research
10. Additional Resources
11. Careers

What is Digital Forensics

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

The artefacts we will be dealing with in the lab are files and file systems.

Why File System Analysis? I

- There are many different forms of digital forensic analysis:
  - Network Analysis,
  - Live memory (RAM) Analysis,
  - File system analysis,
  - Database Analysis,
  - Application/OS Analysis
- File system analysis allows:
  - Introduction to a new field using a common ground
  - Insight into how OS files relate to memory and what creation and deletion features actual do

Why File System Analysis? II

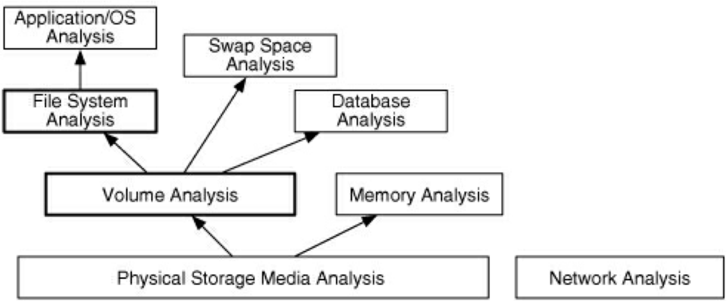

Figure: Layers of Analysis

Forensic Process

Digital forensics results can be used in a court of law therefore accuracy, integrity and an unbiased approach towards evidence is required.
As a result similar approaches to evidence handling and procedure from traditional forms of forensics are utilised.

Scientific Method

Defining a hypothesis based on evidence then proceeding search for evidence which disproves our hypothesis.

Digital Forensic Investigation

"A digital forensic investigation is a process that uses science and technology to analyse digital objects and that develops and tests theories, which can be entered into a court of law, to answer questions about events that occurred. In other words, a digital forensic investigation is a more restricted form of digital investigation." - Brian Carrier

Digital Crime Scene Investigation Process Overview

There are three major areas in digital crime scene investigations:

- System Preservation
- Evidence Searching
- Event Reconstruction

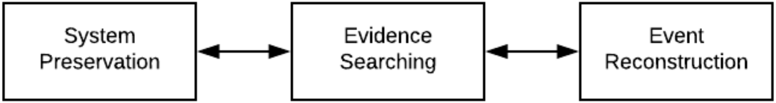

Figure: Diagram of Digital Forensics Investigation Phases

PICL Guidelines

While each forensic investigator/team may have their own procedures and work flow the PICL guidelines below provide a good staring structure:

- Preservation: Preservation of the system being investigated.
- Isolation: Keeping analysis environment is separate from both the suspect data and the outside world.
- Correlation: Correlate data with other independent sources. Reduces risk of forged data.
- Logging: Log/document your actions. This helps identify what searches you have not yet conducted and what your results were.

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

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.

What are File Systems?

File System:

File systems manage how data is stored and retrieved in a computer system. They consist of structural and user data which can be organised and understood by users and computers.

File System Aspects/Categories

Each files system contains elements from each of the following categores:

- File System:
  Contains file system structure overview and where to find other structures and important data. (fsstat)
- Content:
  Contains data relating to actual file contents, these are usual organised into containers called data units (block/cluster).
- Meta data:
  Data that describes files such as access times, file size, users.
- File Name:
  Contains the data that assigns a name to a file, is used by users instead of a metadata address.
- Application:
  Special features/additional functionality such as quota data or journalling.

File System Analysis Techniques

There are many different techniques and theory for the aforementioned categories. In the respect of time and cope of the lecture I will only cover the ones that are relevant to the lab materials.

Acquisition and Analysis Tools

Digital Forensic Research

Additional Resources

Careers