Digital Forensics

File System Forensics Masterclass

Fraser Brown

Heriot-Watt University

March 11, 2018

Outline

1. What is Digital Forensics?
2. Forensic Process
3. Forensic Imaging
4. File Systems
5. File System Analysis
6. Forensic Tools
7. Additional Resources
8. 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

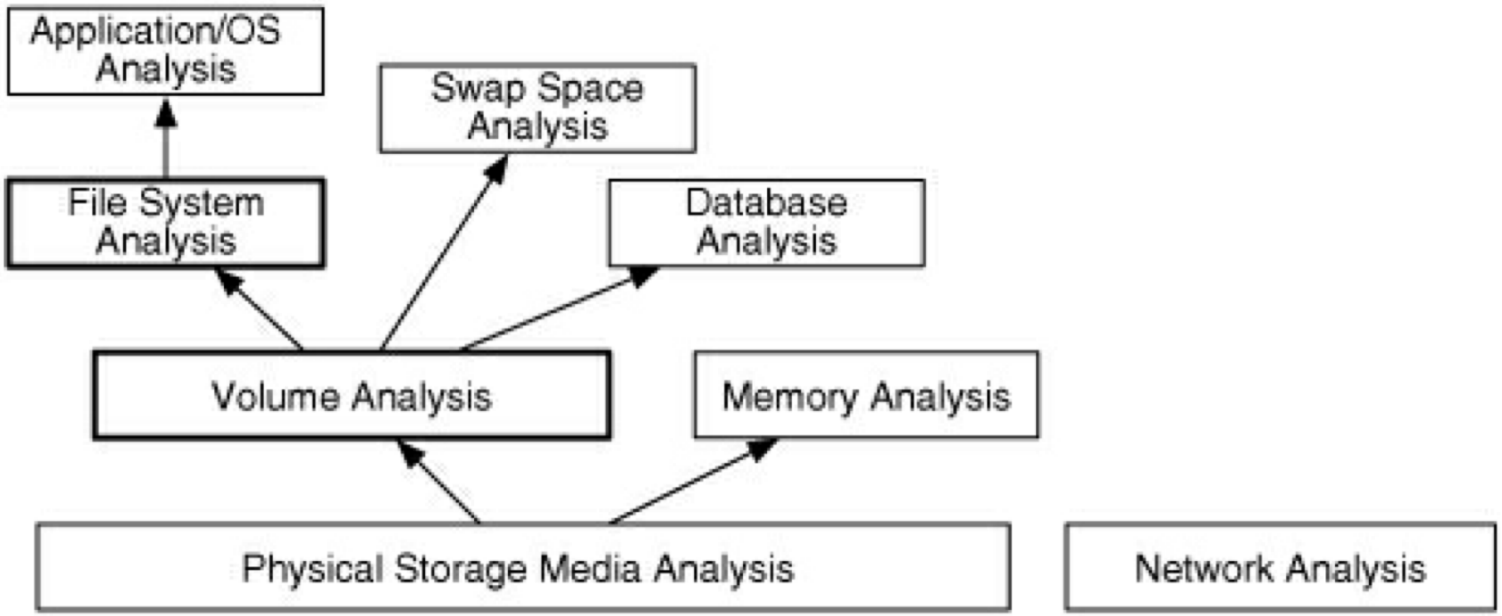


Figure: Layers of Analysis

Forensic Process

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

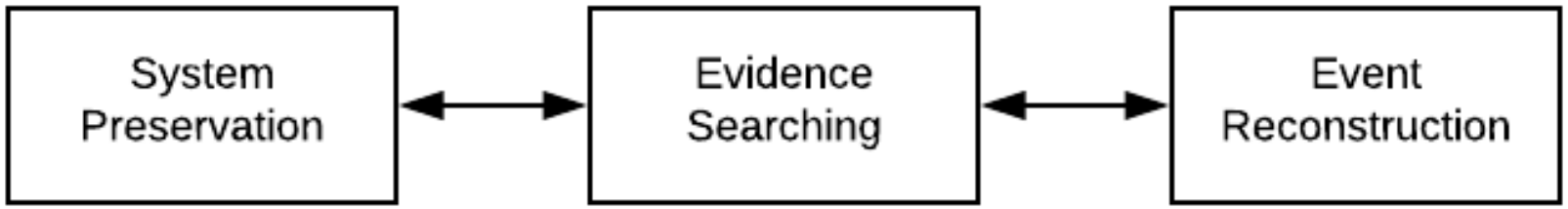


Figure: Diagram of Digital Forensics Investigation Phases

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

Forensic Imaging

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.

File Systems

What are File Systems? I

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.

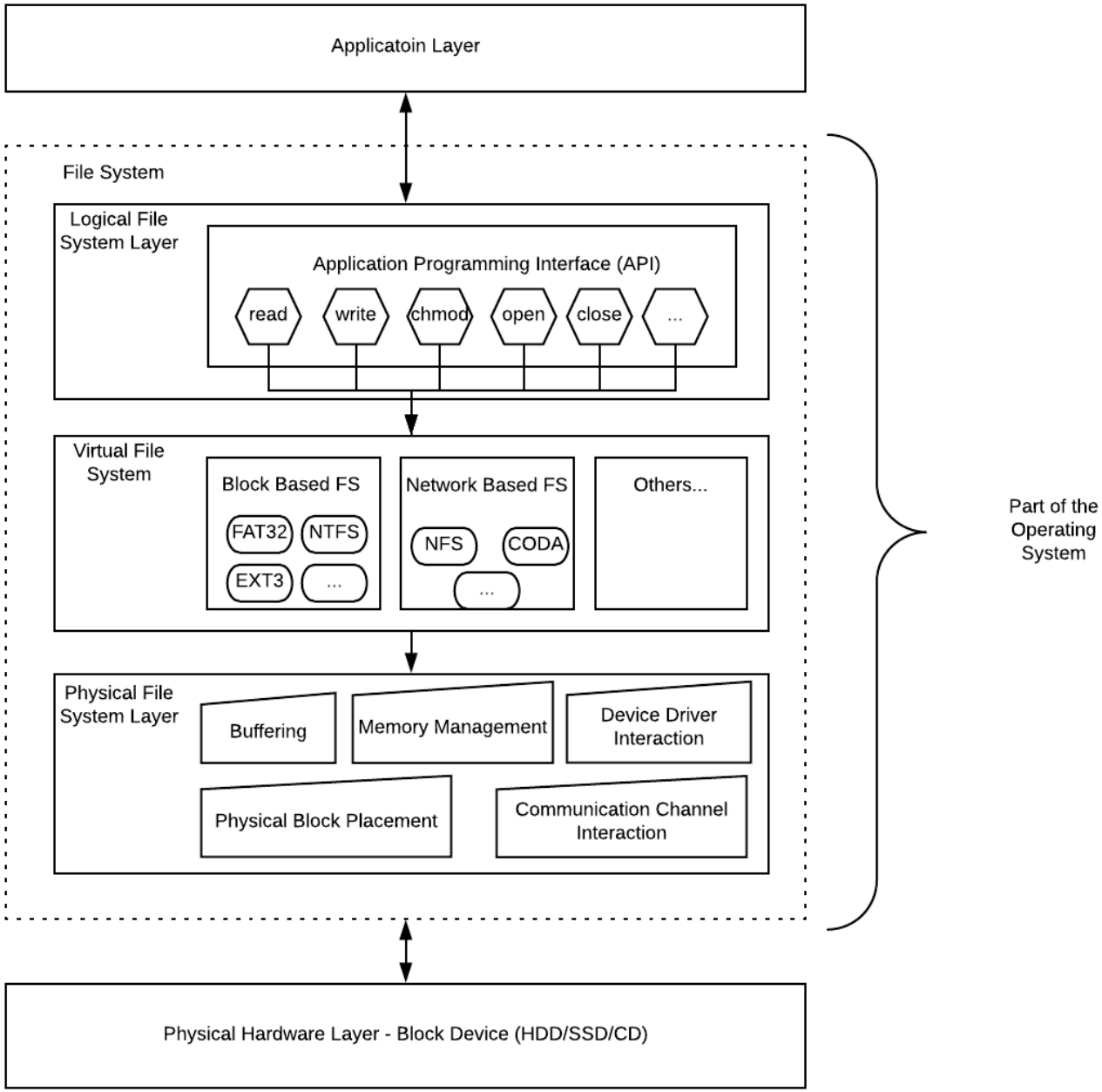
- File system architectures (FAT32, Ext3 etc.) provide different methods of tracking data on physical media each has their own data structures, look up tables and allocation methods.
- Modern operating systems contain support for many different file systems providing an interface with physical storage.

What are File Systems? II

File systems are made up of 2/3 layers:

1. **Logical Layer**: Provides a user application level API for commands such as read, write and chmod etc.
2. **Virtual Layer***optional*: Allows access to multiple physical file systems e.g. block based: FAT32, NTFS or network based: NFS
3. **Physical Layer**: Interacts with hardware, performing block and memory management and interacting with device drivers etc.

What are File Systems? III



File Systems Terminology

- **Sector**:
  Smallest addressable section of memory, which holds static amount of data (512/2048/4096-bytes)
- **INode**:
  Data structure in a file system that contains meta data (a.k.a Meta Data Pointers/Structures)
- **Data Unit**:
  Standard sized container for storing *content* data,which consists of multiple **sectors**. Different file systems have different names for these data units e.g. (Cluster or Block).

File System Aspects/Categories

Each file system contains elements from the following categories:

- **File System**:
  Contains file system structure overview and where to find other structures and important data.
- **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 meta data address.
- **Application**:
  Special features/additional functionality such as quota data or journalling.

File System Categories Interaction

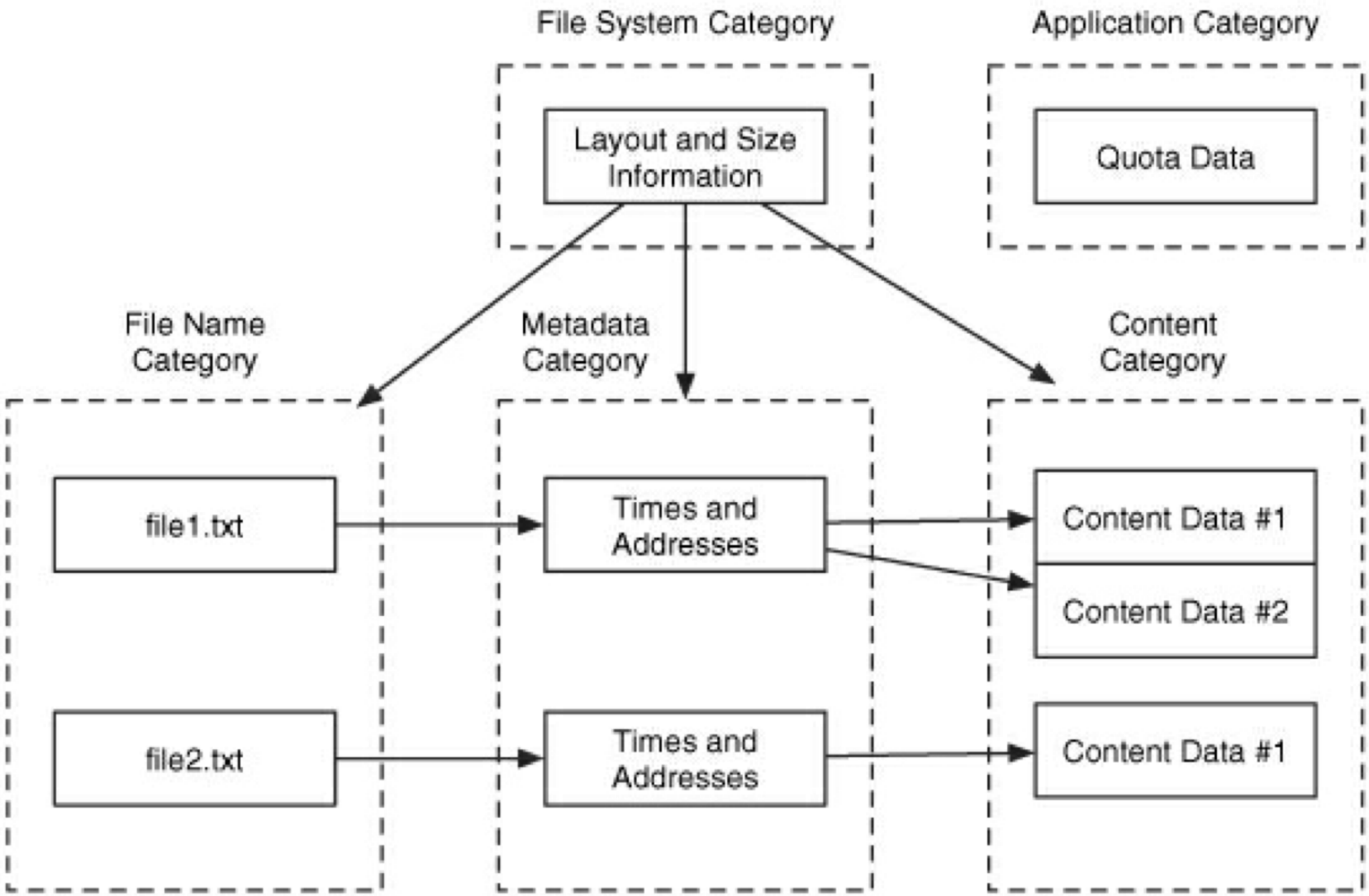


Figure: File System Categories Interaction

File System Categories By Example

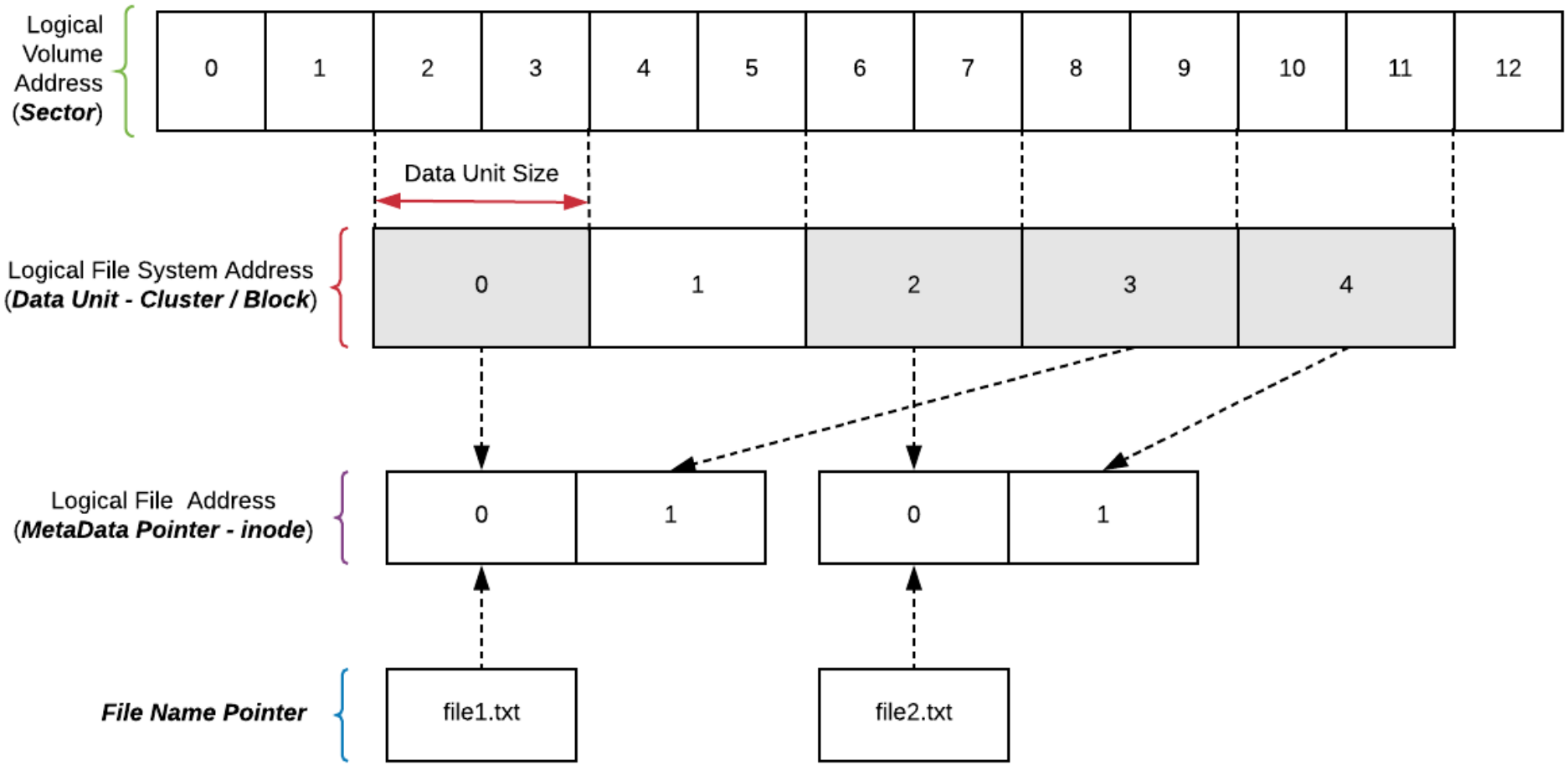


Figure: File System Example

File System Architectures

There are numerous file system architectures available, some are operating system specific others are designed to be more universal.
Examples include:

- FAT - File Allocation Table (FAT8/16/32) - Commonly found on Removable Media
- NTFS - New Technology File System - Default For Windows
- Ext - Extended File System (Ext2/3/4) - Default for Linux

We will focus on FAT32 in this lecture due to the lab being structured around applying forensic techniques on removable media.

File Allocation Table 32 - FAT32

There are

File System Analysis

File System Analysis Techniques

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

Forensic Tools

(Used in Accompanying Lab)

Guymager - Forensic Imaging

Guymager

Guymager is a GUI based forensic imaging tool, that allows for the creation of various image types such as Raw (dd) and EnCase (E01).

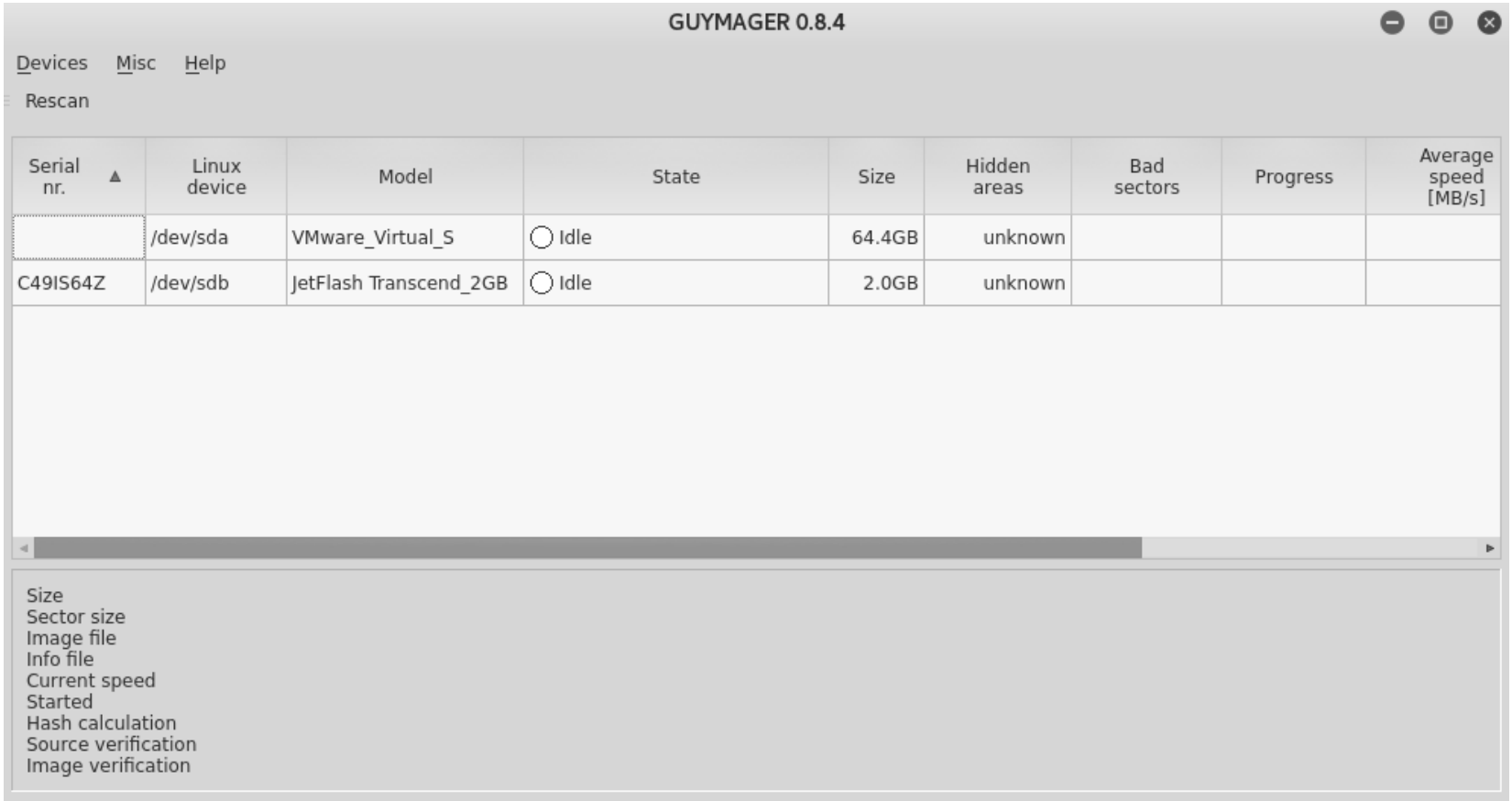


Figure: *guymager gui window example*

Foremost - Data Carving

Foremost

Foremost is a command line tool that utilises data carving techniques to recover files.

- **Data Carving** is a process where files are recovered from a disk image based on common information such as file headers, footers and data structures.
- Performing data carving for large forensic images can be rather tedious if done by hand, tools such as **Foremost** have been developed to help digital forensic investigators automating this process.

The Sleuth Kit (TSK)[1]

The Sleuth Kit (TSK)

The Sleuth Kit is a series of command line tools that allow users to inspect and analyse disk images and the file systems therein.

- The tools provided in TSK are divided into the 5 file system categories discussed previously, file system, content (data unit), meta data, file name.
- Due to the wide variety of tools within TSK I will discuss those of which we will use in the accompanying lab.
- Other features of TSK can befound in the tool overview: `http://wiki.sleuthkit.org/index.php?title=TSK_Tool_Overview`

[1] http://www.sleuthkit.org/

TSK - File System Layer Tools

- **fsstat**: shows file system details and statistics including layout, sizes and labels

TSK - File Name Tools

Allow for processing of file name structures.

- **ffind**: finds allocated and unallocated file names that point to a given meta data structure
- **fls** lists allocated and deleted file names in a directory

TSK - Meta Data Layer Tools

- **icat**: Extracts the data units of a file, which is specified by its meta data address.
- **ifind**: Finds the meta data structure that has a given file name pointing to it or the meta data structure that points to a given data unit.
- **ils**: Lists the meta data structures and their contents in a pipe delimited format.
- **istat**: Displays the statistics and details about a given meta data structure in an easy to read format.

TSK - Data Unit Tools

These file system tools process the data units where file content is stored.

- **blkcat**: Extracts the contents of a given data unit.
- **blkls**: Lists the details about data units and can extract the unallocated space of the file system.
- **blkstat**: Displays the statistics about a given data unit in an easy to read format.
- **blkcalc**: Calculates where data in the unallocated space image (from blkls) exists in the original image. This is used when evidence is found in unallocated space.

TSK - Volume System Tools

These tools take a disk (or other media) image as input and analyse its partition structures.

- **mmls**: Displays the layout of a disk, including the unallocated spaces.
- **mmstat**: Display details about a volume system (typically only the type).
- **mmcat**: Extracts the contents of a specific volume to STDOUT.

Additional Resources

Careers