ASSIGNMENT 1

CS6503: Digital Forensics

Dr Dax Roberts

Andrew Graff
2231290

Contents

Introduction

Kia ora,

Whilst it is inevitable that we're headed to a technological driven world, we use many different digital mediums and tend to take value for what it is, and not the leaps and bounds of what could be.

Digital forensics has shifted a paradigm to an important aspect of investigation that involves analysing of digital evidence. It is the mere matter of having skills and tools to perform more than the normal expectation of an end user. What is meant by this is, the belief of deleting or formatting of data that when it is gone, it's gone.

In this assignment, we have hands-on section where we use various tools to perform some data carving, recovery and analysis. These are supported by a video of myself carrying out assignment instructions along with a power point presentation to further add for what will be observed in the 30-minute video.

The later two tasks in this assignment are a report about a New Zealand crime that involves different sources of electronic evidence and also an attribute and analysis of two common file systems.

Task 1: Forensic case study and analysis

Four main phases

1. **Preparation**
2. **Analysis 1**
3. **Analysis 2**
4. **Reflection**

Reflection

Discuss how the tools were in finding the files and data

Scalpel – It required configuration set up in nano, which meant removing hashes (aligning) these to carve data from our CSF (usb image). As this was saved, we would call this file when executing the command. The audit.txt file listed all the files carved. When performing analysis 2, we could find the same files and pdf.

Foremost – This was an easy command line input in Kali Linux terminal. It did not require configuration in nano, it recovered all the data except personal image jpg and provided a better audit.txt file with a complete listing number of files extracted and types. This audit txt file was better as it had total/summary output. When performing analysis 2, we couldn't find the doc/excel files as we did before but could find the pdf.

Autopsy - We used Windows for Autopsy GUI, and this digital forensic analysis tool had far more features and was able to find all the files and data. It required ingest analyzing times but proved effective in the end. When performing analysis 2, again we couldn't find the doc/excel files but located the deleted pdf file. The office data could have been over written when we added two folders and populated these with files and then deleting a folder. In autopsy we could see the flags, although these were not deleted.

Consider the overall ease of use of the tools

Scalpel – Abit tricky as need to set up a config file in nano and this took some time to understand as the O'Reilly Chapter 9 did not clearly instruct the alignment of the hash removal. Once this was overcome, the tool was relatively simple and easy to use. Overall ease was medium.

Foremost – the easiest tool to use of the three when doing a quick data recovery. It required one line command with a nice audit output. It only needed one command to fully extract all the data. Overall ease was easy.

Autopsy – requires some time to navigate around and familiarize with the tool. Once this was accomplished, you could find many features and capabilities when performing a digital forensic analysis. Over ease was medium.

How accurate the tools were at finding the files

Scalpel as per config set up was limited to what it could find. In the nano setup, I set it up to find word.doc and excel files however neither of these files were carved. We did find the pdfs and images. This had ok accuracy depending if search was limited to older versions (word/excel). Scalpel could find the personal storage device.jpg. Analysis 1: 4/6 found.

Foremost located all the files and organised these in their respective folders. There were extra files found which were from data from a word.doc such as png. These were the images I used in my assignment. This had ok accuracy however could not find the personal storage device.jpg file. Analysis 1: 5/6 found.

Autopsy had good accuracy, as it extracted a lot of information, a breakdown of the source device and many other alternative ways to explore the depth of the disk. It extracted images from word docs. Analysis 1: 6/6 found.

Recommendation

One tool I recommend that I used was Autopsy. It has a nice GUI offering a lot more for digital forensic analysis. A further exploration of this tool could discover more than just data carving or recovery

Anything I would have done differently would be taking time to learn and familiarize Linux commands to perform all the assignment instructions using Kali Linux only.

Task 2: Sources of electronic evidence

Find one New Zealand crime that has been reported in the news since Jan 1, 2018. Crime must have resulted in a conviction.

Grace Millane murder: Jesse Kempson guilty of attacking two more women (bbc.com)

A British graduate Grace Millane had been travelling NZ and met with a guy named Jesse Kempson through a NZ dating app. Grace was later found dead and Jesse was convicted for her murder.

Each of **two pieces** of evidence

Describe what the electronic evidence is

- Mobile evidence
- CCTV evidence

Describe what made the evidence relevant to the case

- Mobile evidence belonging to Jesse Kempson contained explicit photos, screenshots of Ms Millanes Instagram profile and search history of pornography and "Waitakere Ranges" and "Hottest fire".

  This is relevant to the case as it indicates Jesse was in communication with Grace after connecting via Tinder dating application and most importantly the two searches were locations of where the shovel was purchased.

- CCTV footage showed Jesse Kempson purchasing a suitcase that was involved with the transport and burial of Millanes body. Another CCTV footage from the CityLife Hotel shows Grace Millane exiting a lift with Jesse Kempson.

  This is relevant to the case because the CCTV evidence footage obtains a clear visual of the suitcase that was directly involved (matches) containing Ms Millanes body. The other footage shows the two together just hours before Grace's body was found.

Describe one potential challenges with the collection of that evidence

- Potential challenges with the collection of Mobile evidence would be by passing biometrics or security locking of the phone. Any possible encryption software used to encrypt data can pose potential challenges. The collection of search engine data and accessing gallery to obtain the photo evidence can be complex.

- Potential challenges with the collection of CCTV footage are the hours of footage to examine and search through carefully and find the time period related to the events. Accessing CCTV data and making sure the visual files have been saved and stored to

memory for collection. If the storage was full, it would be difficult to collect any footage of the subject.

Describe one potential challenge with the analysis of that evidence

- Potential challenges with the analysis of mobile evidence could be the type of system running on the mobile phone and ensuring adequate software or tools
  are available to operate analysis with the mobile data. Processes are involved in the capturing of the mobile and finding ways to access the phone without tampering any data.

- Potential challenges with the analysis of CCTV footage could be the quality of the visuals observed. If the quality or angle of the camera is not clear this may well be a constraint to obtaining a clear evidence and information leading events. Another potential challenge is any encryption software that could be a barrier to accessing footage required for analysis. May be a situation where the owner of the software is not present or able to be present to access any footage if protected. Legality issues could mean delays which leaves a time of possible tampering.

Task 3: Attributes & analysis of common file systems

Netlab 5: Filesystem Analysis

Briefly describe the lab, include how many filesystems analysis is achieved

This lab is about file systems and the understanding of the most common file systems. Files systems are standards for organizing data on storage devices (Hard Drive, SSD etc). We come across different types of file systems most commonly during the formatting of a drive (deleting all the data). Selecting either as an example **NTFS** or **exFAT**.

In the lab we identify different file systems using hex editors to review three formatted evidence files (FEF). We read the data (bits) that is contained in a partition table by opening the disk image and changing the offset base to decimal. We learn about what volume serial numbers are, how to decode them and creation dates and times.

"Computers use particular kinds of file systems to store and organize data on media, such as hard drive or flash drive, or the CDs, DVDs, and BDs in an optical drive", (Fisher, 2023).

We identify and analyse three different file system data for **FAT, NTFS** and **exFAT**. These three different file systems contain a physical location of data on the device. **FAT** stands for File Allocation Table, **NTFS** stands for New Technology File System and **exFAT** stands for Extensible File Allocation Table.

It is learned the partitions determine how much data you can access, and file systems determine how that data is handled. As you can see in the table below is a structure of the MBR is 512 bits (sector size/hard disks/floppy disks) contain three sections "Bootstrap Code Area, Partition Table and Boot Record signature.

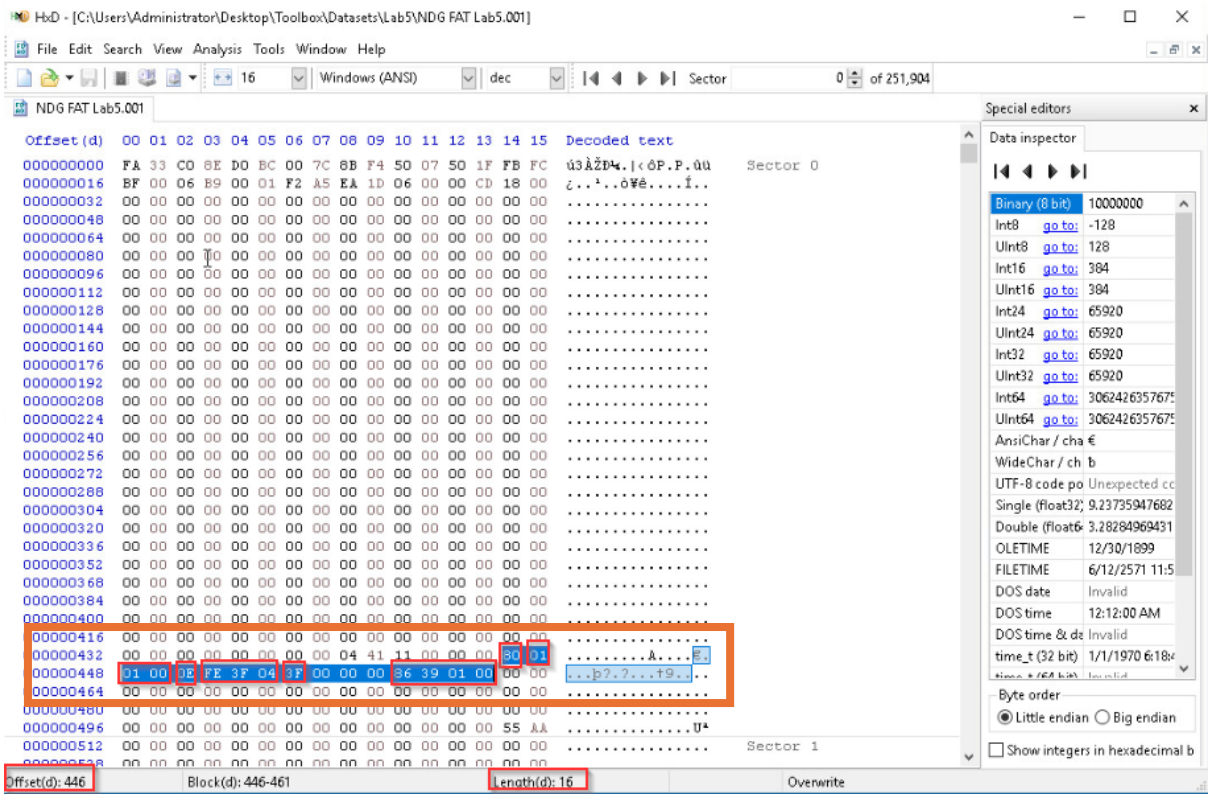
Structure of a generic MBR			
Offsets within sector		Length (in Bytes)	Description
Decimal	Hexadecimal		
000 - 445	000 – 1BD	446	Bootstrap Code Area
446 - 509	1BE – 1FD	64	Partition Table
510 - 512	1FE – 1FF	2	Boot Record Signature

"An MBR is a kind of boot sector stored on the storage device that contains the necessary code to start the boot (loading) process" (Fisher, 2023).

- The partition table is located at decimal offset 446-509 (as per Master Boot Record) MBR.
- Each partition table entry is 16 bytes long.

- Each drive can have 4 or 3 primary partition and 1 extended partition.
- Each partition table is 64 bytes long (446-509 bytes).
- So, storing 4 entries as each entry 16 bytes long.

Below is a **screenshot** of **offset 446** highlighting 16 bytes and the red squares indicate the grouping of bytes/values this is relevant to the lab because we have opened the **HxD tool**, opened the formatted evidence file and converted the data to decimal then used the search "**go to**" to locate **offset 446** to for the partition table.



These **"16 bytes"** highlighted can be divided into **6 sections** for getting information about the partition which is relevant to file system analysis. We have explained this in detail below.

0x 80 (1 byte) this indicates if partition is active or not.

0 = not bootable or 80 = bootable. It is 80 so we know it is a bootable partition

After the 80 are (3 bytes). This represents the starting sector of partition stored as the Cylinder Head Sector (CHS) and in little endian (least significant byte first) so;

0x 01 01 00 is **0x 00 01 01**

"If we know the number of cylinders, heads, and sectors we calculate the capacity of a hard disk drive. Cylinder number x head number x sector number x 512 bytes", (Linda, 2020).

The 5th byte (1 byte) represents the type of file system that is on this partition.

0x 0E 0E represents a FAT file system. “0E = VFAT logical-block-addressable VFAT”, (Datarecovery.com, 2014).

The next 3 bytes represent the ending sector of the partition also stored in (CHS) value and little endian (so we know the ending of the sector is at 0x 04 3F FE

0x FE 3F 04 is **0x 04 3F FE**

The next 4 values include the starting sector of the file system in hexadecimal.

0x 3F 00 00 00 is **0x 00 00 00 3F**

Again, it is stored in little endian, so the value is 0x00 00 00 3F or 0x 3F (converted to decimal is 63). Therefore, the starting sector of this (FAT) file system is **sector 63**.

The last 4 values represent the number of sectors in the partition also stored in little endian.

0x 86 39 01 00 is **0x 00 01 39 86**

Using the hex tool, we can highlight these numbers to get the value in decimal. The conversion to decimal is 80262 sectors. So, a way to get the partition size is multiplying the number of sectors by the size of each sector.

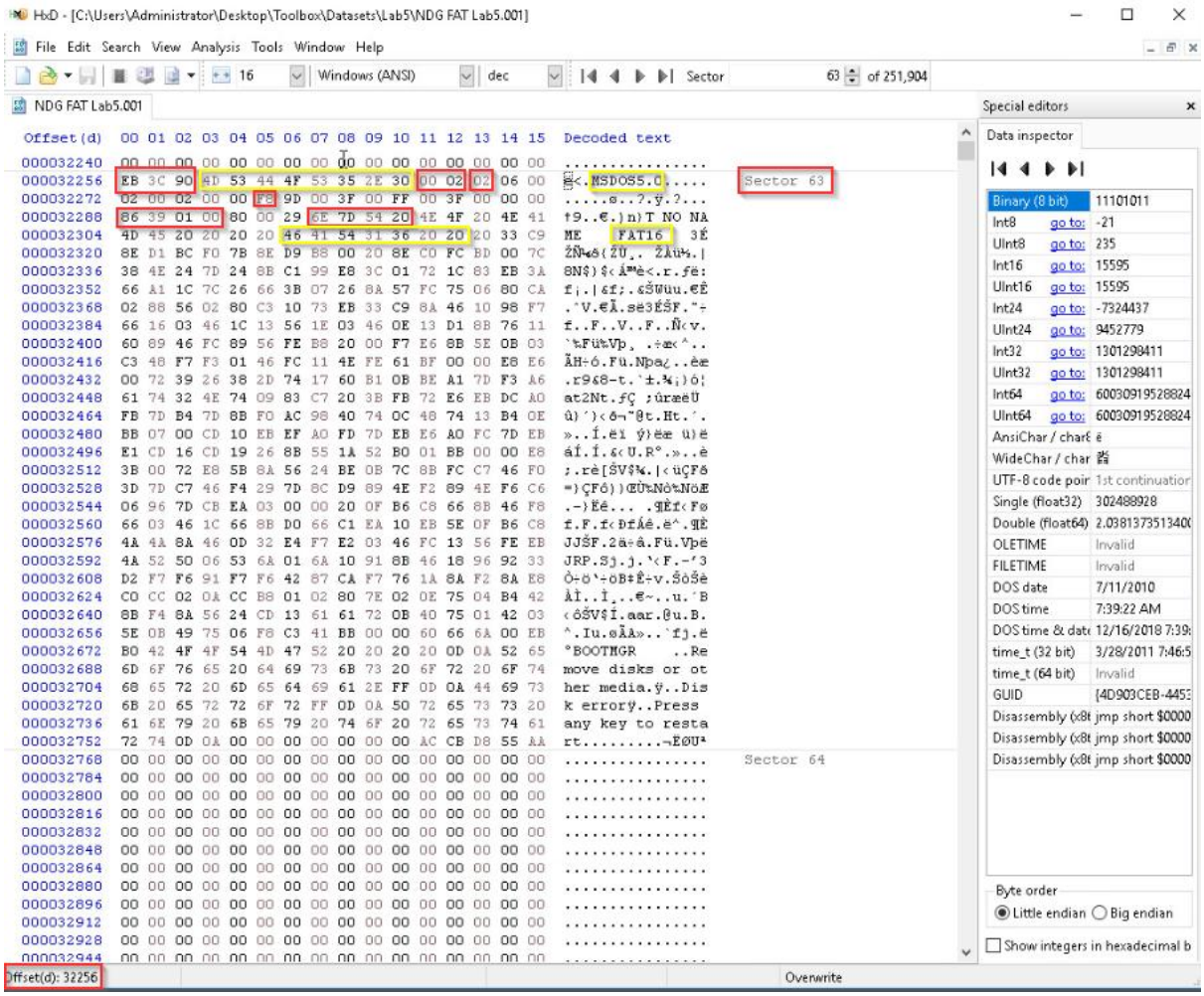
Therefore 80262 x 512 = 40094144 bytes this is approximately 40mb.

The last 2 bytes at the end of the MBR is the Boot Record Signature (510-511). The partition entries are 55 AA

0x 55 AA

The partition table indicates the starting sector of the **FAT file system** is **sector 63**. To get the offset we: **63 x 512** (each sector size) so offset begins at **32256** and ends at **32767** (adding 511).

Below is a screenshot that indicates we have located **sector 63** and can see the corresponding decoded text on the right pane from the values in the left. This is relevant to the lab as we learn to read these data as explained further in the report.



The **VBR (Volume boot record)** is what is highlighted above where we can locate certain artifacts. The artifacts here contain **jump instructions** (instructing the computer to skip a few non-executable bytes, **OEM ID** (name of the file system in text), **number of bytes per sector** (converting hex to dec), **number of sectors per cluster**.

Media type such as **USB drive or hard disk** etc (offset 32277 as per table), **total number of sectors** in 4 bytes (offset 32288 as per table), **volume serial number** in 4 bytes (offset 32295) and **file system** type (offset 32310) in 8 bytes.

A table can be used (depending on file system type example **FAT, NTFS or exFAT**) to find more offset numbers and getting names and descriptions from the physical disk data which gives us information and better reading of the file that is relevant to the analysis part for file systems.

Discuss if you would recommend this lab to other students with consideration to File System Analysis

I would probably less likely recommend this lab to other students with consideration to file system analysis simply because of the complexity involved with the presentation and documentation of this Netlab (many words).

The lab itself could have been broken down into simpler sections with a perhaps a more engaging direction for identifying file system data.

Personally, I did need to do some research on the terminologies to get a conceptual understanding of what file analysis is, how data is stored on a drive (reading this) and determining its structure.

Theoretical

Source **two resources** (books, blogs, or videos) that describe or provide specific labs on the topic of **"Filesystem Analysis"** for Windows and Linux Operating Systems.

Video on Windows OS Filesystem Analysis:

Provide adequate information about the **source** of information including why the source should be **considered reliable**

"FAT32 vs exFAT vs NTFS – Windows File Systems" by PowerCert Animated Videos (Video)

A YouTube video about Windows File Systems is created by PowerCert Animated Videos. This YouTube channel has content all focussed on IT indicating positive reviews from a large following subscription. This particular video is based on the different file system types and given the positive following and feedback from the comments this source should be considered reliable.

Discuss the particular **relevance** of the lab (including briefly some steps or elements of the lab) how appropriate it is for L6 students studying Digital Forensics

The relevance of the lab mirrors closely to what was observed during the practical Netlab Lab 5 File system analysis. It breaks down the different file systems in an easy understandable way through visuals and simple language. The YouTube video explains what would happen without a file system, and what happens when using a file system and the different types.

It explains the **FAT32** systems and it's compatibility with limitations of file size. So using a hard drive with a **FAT32** file system could not store a file over 4gb (file size limit 4gb) or max partition size of 2TB.

Next file system is **exFAT**, (created as an upgrade to FAT32) supports unlimited file size and partition size. This is most commonly used on removable storage such as flash drives or external hard drives/SSD.

Lastly is **NTFS** (default file system for Windows system) with more features such as security (permission controls), encryption etc. This is the most commonly used file system for Windows.

Blog on Linux Filesystem Analysis:

Provide adequate information about the **source** of information including why the source should be **considered reliable** (1 mark)

"7 ways to Determine the File System Type in Linux (Ext2, Ext3 or Ext4)" by Aaron Kili (Blog)

The source of this information is found on the TecMint website which offers range of different Linux services and information. The blog is about the determining the file system type in Linux. It is supported by screenshots of the Linux system and definitions of what is a file system. It shows commands and output of the Linux commands that are entered to retrieve information. The author of the blog has written many other articles and is an upcoming Linux Sysadmin which is why this source should be considered reliable.

Discuss the particular **relevance** of the lab (including briefly some steps or elements of the lab) how appropriate it is for L6 students studying Digital Forensics

The particular relevance of the blog is the different Linux file system types explored in this blog. The title 7 ways to determine the file system type in Linux gives us information about how the data is handled and data structures within the operating system. In the practical we use GUI interface application in Windows to analyse different file system types from formatted evidence files. In a Linux OS environment, a variety of commands is used to identify Linux file system type. The types of file systems that can be seen from the output of these commands are **Ext2, Ext3 or Ext4.**

Ext2 (second extended) file system that can contain a single file size of up to 2TB and depending on **block** size, it can hold a file system up to 32TB. "Data on disks are usually accessed in blocks rather than bytes" (Bashorun, 2020).

Ext3 (third extended) file system with an added feature of journalling where changes can be tracked and improves file reliability and file system conversion (Ext2 to Ext3).

Ext4 (fourth extended) file system that is also supported by Windows OS. Added features delayed allocation and defragmentation (rearranging data for efficient storage and access).

This blog has a series of commands that can be entered to get file system information. Instead of FEF we are getting information of the OS in this lab.

The different commands are **df** (file system disk space usage) and using **-T** for a particular disk partition, **fsck** command to repair Linux file systems or print file system type on specified disk partitions, **lsblk -f** command prints file system type on the partitions. Another command useful is the **file -sL** command. This command identifies the file type, and **-s** enables reading of block or character files and **L** for symlinks (location).

This is relevant to file system analysis because we can see the different types and how this is displayed. This is appropriate for L6 Digital forensics students as they will be able to see the difference between a Windows and Linux operating systems and how the data is handled. The analysis here is how to gather information of the file system types and understanding the different file types.

References

(Bashorun, 2020) Bashorun, E. 2020, Mar 20. *A Deep-dive into the Linux Filesystem | Part 1.* Medium. A Deep-dive into the Linux Filesystem | Part 1 | by Emmanuel Bashorun | Medium

(Datareovery.com, 2014). Datarecovery.com, 2014, Jun 23. *Hexadecimal Flags for Partition Type.* Hexadecimal Flags for Partition Type - Datarecovery.com

(Fisher, 2012). Fisher, Tim. 2023, 28 Aug. *What Exactly Is a File System?*. Lifewire. What Is a File System and What Are the Different Kinds? (lifewire.com)

(Fisher, 2023). Fisher, Tim. 2023, Jan 10. *What Does Booting Mean?*. Lifewire. What Does It Mean to 'Boot' a Computer? (lifewire.com)

(Kili, 2023). Kili, A. 2023, July 13. *7 Ways to Determine the File System Type in Linux (Ext2, Ext3 or Ext4).* TechMint. 7 Ways to Determine the File System Type in Linux (Ext2, Ext3 or Ext4) (tecmint.com)

(Linda, 2020). Linda, 2020, Nov 25. *What Is Cylinder-head-sector?*. MiniTool. [Disk Basic Knowledge] What Is Cylinder-head-sector? - MiniTool Partition Wizard