Logbook & Assignment Questions

Part A:

Provide a description of the function of the boot sector:

The function of the boot sector is to start the boot process in order to load an operating system, the boot sector exists on the hard drive where the operating system windows/Linux/Mac is installed. Once a computer is launched the bios looks for clues on how to boot up the OS, in doing so the first place the bios will check is the boot sector and each drive has one boot sector, the bios checks the boot sector and finds which drive holds the OS.

Provide a description of the function of the FAT:

A file allocation table aka FAT is a table that an operating system maintains on a hard disk that provides a map of the clusters which is the basic units of logical storage on a hard disk that a file has been stored in. The OS creates a FAT entry for the new file that records where each cluster is created and their order. When you read a file, the OS assembles the file from clusters and places it as an entire file where you want to read it.

Part B:

A. Image Name: Test-Image1-clean.dd.001

B. Hash Value:

MD5: cce9a0e19318ff056e45f98e876c40a2

SHA1: 5b0b07151e8c0a559c0fe2bb9253e6b392ad5c71

C. Storage Location: C:\Temp\Test-Image1-clean.dd

What is the FAT32 File System and why is it important for Pen Drives?

FAT32 is a disk format used to organise the files that are on a disk drive. The disk drive is sorted into different sections called sectors and a File Allocation table (FAT) is created at the beginning of the drive so that information in the file can bee found by the computer. 32 refers to the number of bits that the system uses to store these addresses. FAT32 is important for its usefulness, there’s a good reason it’s lasted so long and is still used in this modern decade. FAT32 is important due to its compatibility with a huge variety of devices such as smartphones, tablets, computers, digital cameras, gaming consoles, surveillance cameras, etc etc.

Part D:

A. Image Name: Test-Image-clean-with-textfile.dd.001

B. Hash Value:

MD5: 7a000c950f55c0c3bb44a9214ede5bdb

SHA1: 5d39785548ff9aa7fe13438b70d8489da3e5bd07

C. Storage Location: C:\Temp\Test-Image-clean-with-textfile.dd.001

For my observation of the files and their comparison I don’t feel like there’s a major difference between the 2 cleaned disk images beside the fact that one has a text file embodied in it as I found and presented below.

Graphical user interface

Description automatically generated

A picture containing text

Description automatically generated

Graphical user interface

Description automatically generated with medium confidence

Part E:

Open <http://www.tavi.co.uk/phobos/fat.html> and <https://www.pjrc.com/tech/8051/ide/fat32.html> and summarise what it says about the FAT:

The FAT file system is heavily based on the file map model in terms of its on-disk layout, it is a simple robust file system. There are 3 variants of the FAT file System, a 12-bit, 16 bit and 32-bit version.

Here’s a basic layout:

Table

Description automatically generated

The FAT file system contains several important data areas which help to describe the rest of the file system, to understand how a disk is laid out, it is necessary to understand the boot block.

Here’s a boot block chart:

Text

Description automatically generated with medium confidence

The FAT occupies one or more blocks immediately following the boot block, part of its last block will remain unused, if there is a second FAT, this immediately follows the first block, but starting in a new block, this is repeated in any further FATS. On a hard drive there is usually only one FAT, a floppy disk can have several FATs. If a FAT is unreadable, files cannot be accessed, and another version/copy of the FAT must be used.

In the case of the 16-bit FAT file system, each entry in the FAT is two bytes in length (i.e. 16 bits). The disk data area is divided into clusters, which are the same thing as allocation units, but numbered differently (instead of being numbered from the start of the disk, they are numbered from the start of the disk data area). So, the cluster number is the allocation unit number, minus a constant value which is the size of the areas in between the start of the disk and the start of the data area.

There is only one entry in the FAT for every cluster aka data area block on the disk. Every N relates to a cluster N. Clusters 0 and 1 don’t exist and those FAT entries are special. The Last cluster of a file has the value 0xffff in its FAT entry to indicate that there are no more clusters

# FAT32 STRUCTURE PROVIDED BELOW

# 

Part F:

A. Image Name: Test-Image-with deleted file.dd.001

B. Hash Value:

MD5: ce2626a732d3457b860ed31bf5bedad0

SHA1: 21bfe0f40cde196c821973d2b025a201aabbe394

C. Storage Location: C:\TEMP\Test-Image-with deleted file.dd

Graphical user interface

Description automatically generated with low confidence

What happens when a file is deleted?

The MD5 sum has changed and is different to the original MD5 sum and the text remains from the deleted text file from the other image.

Can you still ‘see’ the text of the text file (are the contents of the text file still visible on the image?). Yes/no

Yes, the text of the text file is still visible on the image.

Text

Description automatically generated

Part G:

A. Image Name: Test\_image\_with\_Directory.dd.001

B. Hash Value:

MD5: ce2626a732d3457b860ed31bf5bedad0

SHA1: 5dd27e771db73ad14dbb37af9f76189bb65137b4

C. Storage Location: C:\TEMP\Test\_image\_with\_Directory.dd

Part 2:

A. Image Name: Test\_image\_with\_Directory\_Deleted.dd.001

B. Hash Value:

MD5: 735f984e95cda21c4f9c0b2085a86a69

SHA1: 7c724c88ba916a073b72e6ec81744fd8f18e7cd5

C. Storage Location: C:\TEMP\ Test\_image\_with\_Directory\_Deleted.dd

A screenshot of a computer

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated with medium confidence

What happens when a Directory is deleted?

The folder/Directory isn’t completely gone it just leaves an earmark of the space the file takes up on your usb as vacant.

Part H:

A. Image Name: Test\_image\_with\_Saved\_Word\_File.dd.001

B. Hash Value:

MD5: 8705f844e712fd256f51dca6958c9284

SHA1: 4777199e8dde7d7ad0f19e3aa37cf0f0524aa4ed

C. Storage Location: C:\TEMP\ Test\_image\_with\_Saved\_Word\_File.dd

Find the start and end magic numbers associated with a jpeg file.

Start: FF D8

End: FF D9

Using the start magic number, find the beginning of the jpeg File

A screenshot of a computer

Description automatically generated with medium confidence

Using the End magic number, find the end of the jpeg image file.

A screenshot of a computer

Description automatically generated with medium confidence

What is the sector number and the memory offset to the start of the JPEG file? Log the information in the following table:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Starting Sector | Ending Sector | Observed data | Date and Time | Signature |
| 403B0Ah | 46AB0Ah |  | 30/10/2021 | Stephen Duffy |
| Starting Offset | Ending Offset | 30/10/2021 | Stephen Duffy |
| 0xFFD8 | 0xFFD9 | 30/10/2021 | Stephen Duffy |

Part I:

Graphical user interface, text, application, email

Description automatically generated

(Sorry if any of Terry’s Evidence pictures are blurry they were all really bad quality for me)

Has Terry sent any emails? Document the emails.

Terry has not sent any emails that we can find but there is images of him sending/receiving emails.

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Has he been using zip files? Document the Zip files (file size, ownership, metadata)

He had not been using any Zip Files from what I have found

Graphical user interface, text, application

Description automatically generated

Are there any Office or Open Office documents? Document the evidence.

There was no office or open office documents on the evidence drive

Graphical user interface, text, application

Description automatically generated

Are there any images that showing any illicit business? Document thoroughly.

Graphical user interface, text, application, email

Description automatically generated

Using Keylogger:

Graphical user interface, text, application

Description automatically generated

Graphical user interface

Description automatically generated

Graphical user interface

Description automatically generated

Graphical user interface

Description automatically generated

Graphical user interface, timeline

Description automatically generated

Graphical user interface, application

Description automatically generated

Graphical user interface, PowerPoint

Description automatically generated