killian Halpin

Assignment 1  20093283

File system forensics

Contents

[File Creation: 2](#_Toc87966394)

[The Deletion Process: 3](#_Toc87966395)

[Duplicate: 4](#_Toc87966396)

[Data Structures: 4](#_Toc87966397)

[Directory Entry: 5](#_Toc87966398)

[File Recovery: 5](#_Toc87966399)

# File Creation:

When a file is being created we read the boot sector from 0 and locate the FAT structures, data area and root directory. If we are saving into a directory that already exists we go through each directory entry and look until we find the one we are looking for. We read the contents of the of the directories starting cluster and process each one until we find one which is unallocated. When the available entry is found we set the status by writing what we want to call the file, the size and current time are also written. Clusters are also allocated so the FAT structures are searched and a cluster is set used by setting the file to EOF. If the file is over 4,100 bytes a second cluster will be needed. The next available cluster is allocated.

Diagram

Description automatically generated

# The Deletion Process:

In the deletion of files once you press the delete button the file is just moved to another location the recycle bin, the contents of the file are kept completely intact. When you delete the file from the recycle bin this in turn removes the file name from the folder. However the space on the disk where the file previously was is not changed and would still hold the information the data is just not linked to the file name. The space on the disk is then marked as free and other files can be written to that space and eventually the data would be overwritten. There are tools that can be used if you wish to stop the data from ever being recovered but it is a slow process and can damage the disk.

Diagram

Description automatically generated

# Duplicate:

First I downloaded the file from the assignment brief on moodle. I then made a forensic copy of the file to work off using the dd command as to not damage anything on the original file. After doing this I checked the hash values to make sure they matched the originals. I also used write blockers while doing this. This stops any unwanted material being wrote to the disk.

Text

Description automatically generated with medium confidence

# Data Structures:

Once that was done I ran the fsstat and fls command on the image. From the information received from running them commands I was able to draw the map.

Letter

Description automatically generated

# Directory Entry:

The directory entry has the starting cluster of the file and the FAT is used to find the remaining clusters in the file. The non-zero entry contains the address of the next cluster in the file. To find this next cluster you just look at the clusters in the FAT and decide if it’s the last cluster in the file or if there is another one. Using the FAT to locate clusters is like a treasure hunt, you are given clues about the first location where you then find clues to the second location. This is repeated until the final site is found.

For example if we had a file in clusters 40, 41 and 45 and we wanted to see the contents of this file we would look at the starting cluster and should have a value of 40. The size of the file would show that more than one cluster is needed for this. The entry also contains 41 this is the second cluster in the file. There is one more cluster needed and we examine the file to find the value of 45 which should have the end of file marker EOF as it is the last cluster in the file. These sequences are called a cluster chain.

Diagram

Description automatically generated

# File Recovery:

After this I put the image of the disk into autopsy. Autopsy is a forensic tool used to see files and images on the disk and also allows you to recover deleted content on the disk. I found an image of a map where the drop will take place. The image was named ‘handoff’ this can be assumed to be the handoff location.

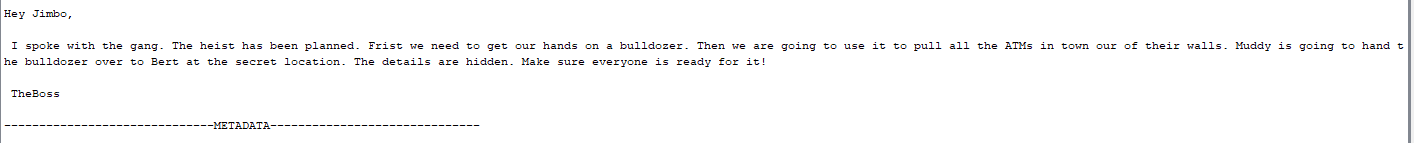
Diagram

Description automatically generated

There was also a file which stated the drop would take place the 16th of November at 10pm. The image and file were found in folder 3 a zip folder. Which was deleted.

Text

Description automatically generated with medium confidence

Also I found plans to have a robbery of all the ATMs in Waterford city. There was a file called ‘Masterplan.txt found in a folder. They plan to get a bulldozer to pull all the ATMs out of the wall, they have it all planned out the bulldozer will be delivered to a secret location. All other information about the heist is hidden and will have to be found. They also plan to escape up the river by boat.

A picture containing table

Description automatically generated

Map

Description automatically generated

I then ran the fls-r command to see the contents of the files on the drive. The I ran the istat command to see where the files started and finished. I then cut TheMasterPlan.txt file out using the dd command and found a link to where they bought the bulldozer for the robberies. I also checked for hidden passwords but there were none on this site.

Graphical user interface

Description automatically generated with low confidence

Text

Description automatically generated

I then ran the istat commands on all the files that came up and cut the files out using dd and got the same results as I found on autopsy. As the zip folders wouldn’t open normally for me I tried using 7zip and they opened. I found the handoff png and the text file in the folder2.zip.

Graphical user interface, application

Description automatically generated

Text

Description automatically generated

I copied out the folder 4 and first viewed it in an hex editor and then saved it in txt format as I found there was a text file there also. I found a link to w3 schools not sure if this means anything or not. I did the same process for folder1.

Text

Description automatically generated

Text

Description automatically generated