LAB REPORT

# Part A: Write Blocker, Wiping and Cleaning, Formatting

In starting Part A download and installed a write blocker to my computer, I decided to use SafeBlock which was provided to me via blackboard and installed it on my forensic workstation (My Computer).

After that I installed my trusty USB as seen below and attempted to save a file to the USB key. The file was successfully interrupted by the write-blocker and the file was not transferred. Next, I disabled the write blocker and installed the disk wiping software ProDiscover and wiped the USB drive. The usb drive was already previously formatted to FAT32 but I did it again just in case and I now have a clean and formatted drive with only a FAT32 Boot Sector, and a FAT file system installed.

Graphical user interface, application, Word

Description automatically generated

Graphical user interface

Description automatically generated with medium confidence

Graphical user interface, text, application, chat or text message

Description automatically generated

# Part B: Forensic Imaging

For part B I started with requesting and installing the software FTK Imager and using it to take a forensic image of the USB drive. I saved the image to C:\TEMP\Test-Image1-clean.dd and took note off the 2 hash values associated with the image (As seen below and in my other document linked in this folder). I now have an image of a clean USB key.

Graphical user interface, text, application

Description automatically generated

# Part C: Research 1 – Comparing image files

Access the Compare Files tool by clicking the Tools -> Compare Files menu option.

The Comparison tool supports two different algorithms: Binary and Byte by Byte.

Two options exist for running comparisons in the Options box.

Can enable/disable Synchronized Template Results Scrolling.

To compare two blocks of data in the same file, set the file name for File A and File B to be the same file name.

The Output Window will appear after a comparison is run. This window displays a list of all matches and differences, plus a graphical representation of how the files match.

# Part D: Putting a single text file on the USB and determining the differences

For part D I started with the software FTK Imager and using it to take a forensic image of the USB drive with the text file. I saved the image to C:\TEMP\Test-Image1-clean.dd and took note off the 2 hash values associated with the image (As seen below and in my other document linked in this folder). I now have an image of a USB key with a Text file inside of it. I will now use 101 Hex Editor to compare the two images and try and locate the body of the text file in the image and note my observations in my logbook.

Graphical user interface, text

Description automatically generated

# PART F: Consequences of file deletion

For part D I started with the software FTK Imager and using it to take a forensic image of the USB drive with the text file. I saved the image to C:\TEMP\ Test-Image-with deleted file.dd and took note off the 2 hash values associated with the image (As seen below and in my other document linked in this folder). I now have an image of a USB key with a deleted Text file inside of it. I will now use 101 Hex Editor to compare the two images and try and locate the body of the text file in the image and note my observations in my logbook, see what happens when a text file is deleted and still see if the text from the text file is still visible on the image.

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text

Description automatically generated

# PART G: Directories and deletion

For part G I started by creating a new Directory on the USB Drive, by doing so I now have a USB with a boot sector, file system, remnants of a text file and a single directory.

Next, I opened the software FTK Imager and using it to take a forensic image of the USB drive. I saved the image to C:\TEMP\Test\_image\_with\_Directory and took note off the 2 hash values associated with the image (As seen below and in my other document linked in this folder). I now have an image of a USB key with a boot sector, file system, remnants of a text file and a single directory.

I will now use 101 Hex Editor to compare the two images and note my observations in my logbook.

Following my previous steps, I then deleted the directory on the USB Drive and now have a USB with a boot sector, file system, remnants of a text file and remnants of a single directory. Repeating the last steps, I will take another forensic image and note the new hash value and compare the two images, this one and the previous one using 101 hex editor.

**With Directory:**

Graphical user interface, text

Description automatically generated

**With Deleted Directory:**

Graphical user interface, text

Description automatically generated

# PART H: describing files using Hex Offsets (Memory and Sector Number)

For part G I started by copying a new image on the USB Drive, by doing so I now have a USB with a new image called “test\_jpeg.jpeg”

Next, I opened the software FTK Imager and using it to take a forensic image of the USB drive. I saved the image to C:\TEMP\Test\_image\_with\_Saved\_Word\_File and took note off the 2 hash values associated with the image (As seen below and in my other document linked in this folder). I now have an image of a USB key with a jpeg image.

I will now use 101 Hex Editor to compare the two images and note my observations in my logbook.

Graphical user interface, text

Description automatically generated

Graphical user interface, text, application

Description automatically generated

# Part I: Forensic Investigation and Application of Parts A – H

For Part I, I started with wiping the USB Pen drive and formatting with FAT32. I then copied the evidence file (Terry’s USB Drive) to the USB Pen drive.

Next, I opened the software FTK Imager and using it to take a forensic image of the USB drive. I saved the image and checked the hash values of the original evidence drive to check if it matches the image I’ve just taken.

Using OSForensics and 101 hex editor I attempted to locate and analyze evidence. I created a folder on my drive and called it “Investigation of Terry” next I created a case in OSForensics and filled in the remaining details.

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text

Description automatically generated