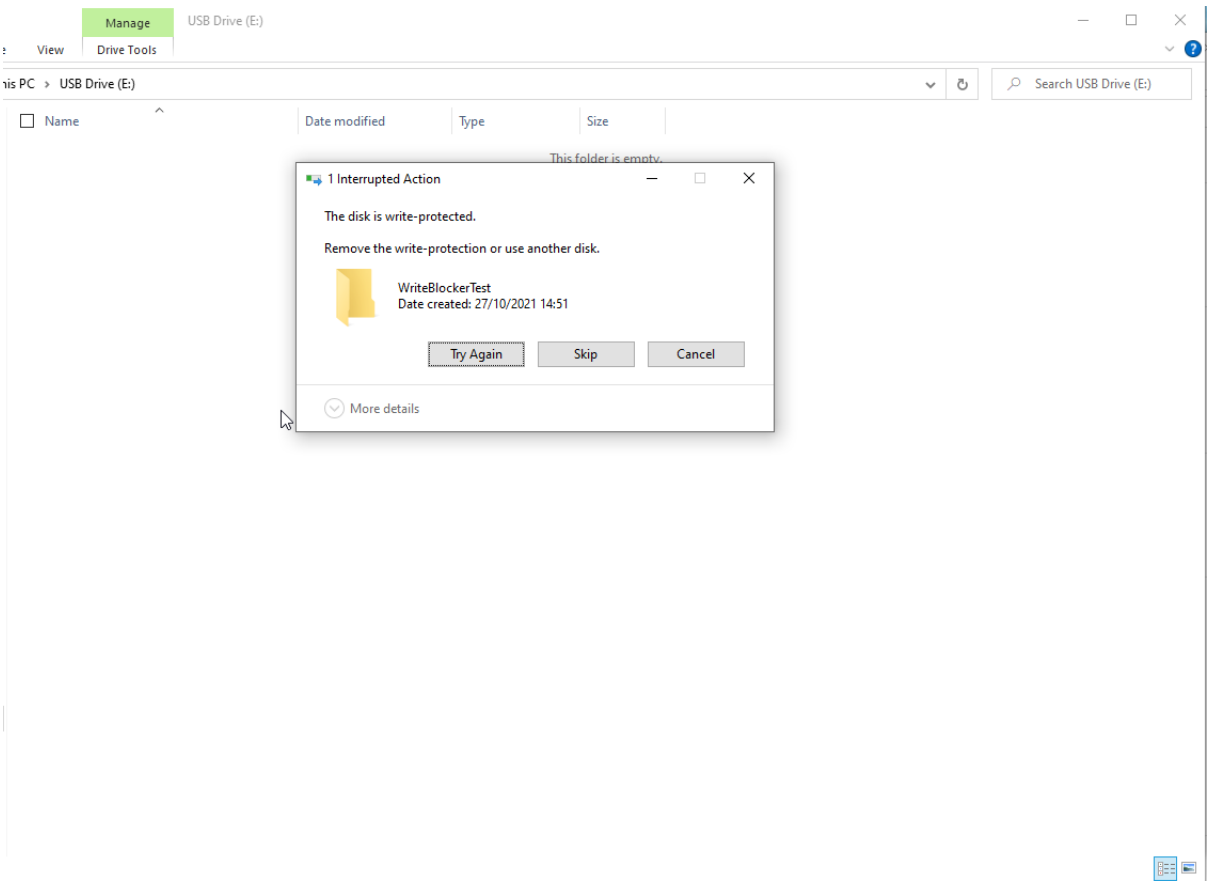
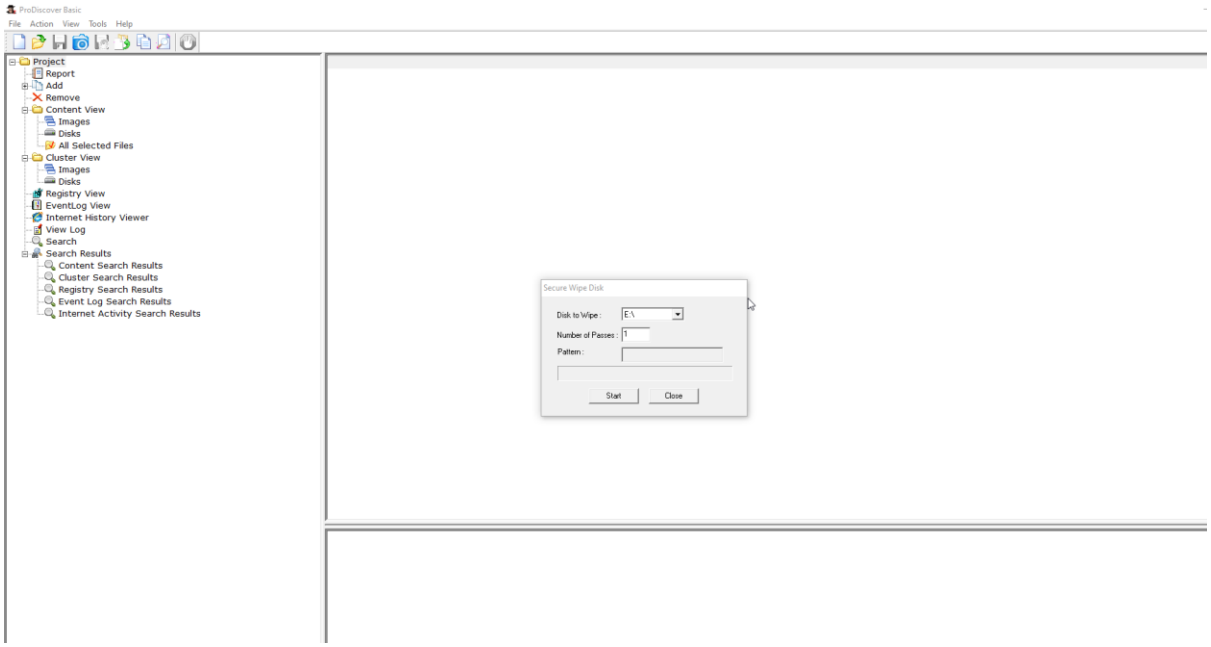
LAB REPORT

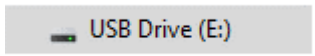
Part A: Write Blocker, Wiping and Cleaning, Formatting

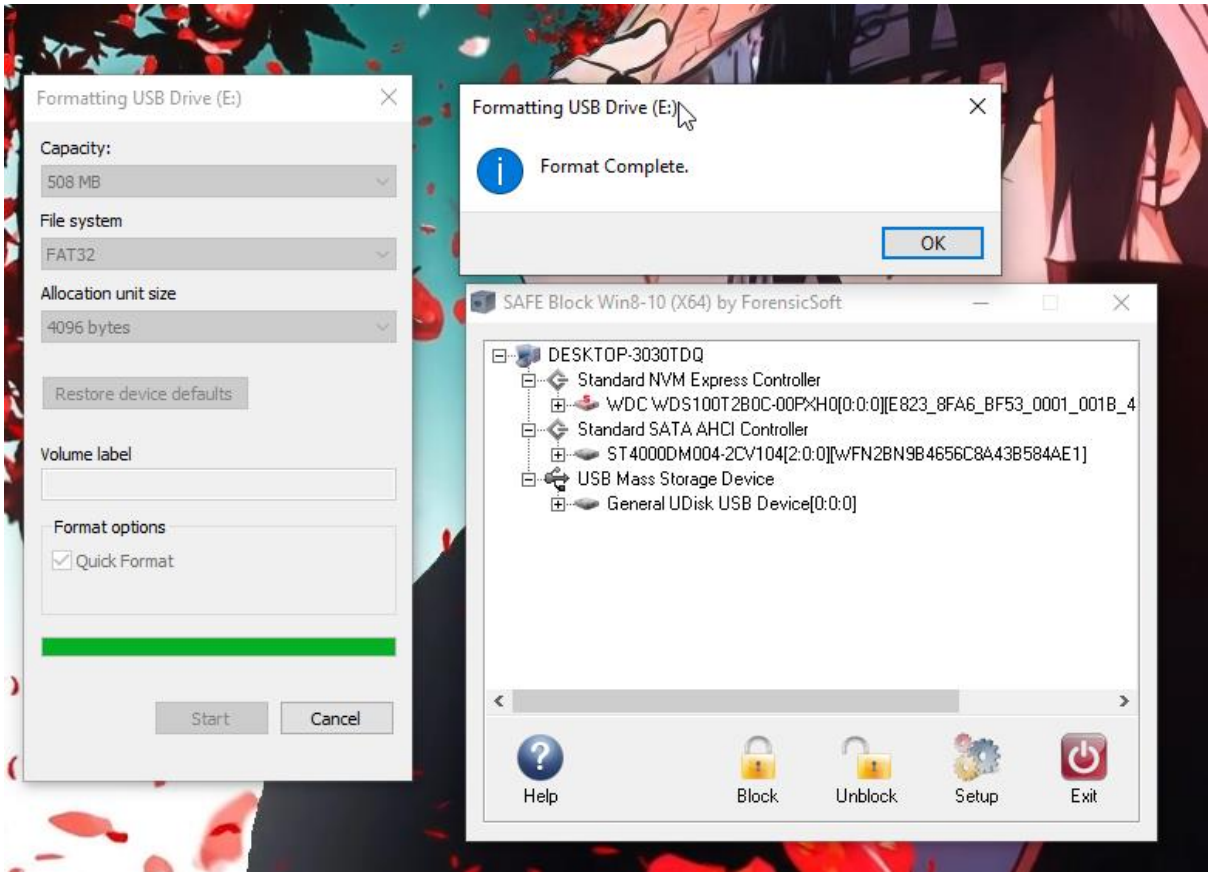
In starting Part A download and installed a write blocker to my computer, I decided to use SafeBlock which was provided to me via blackboard and installed it on my forensic workstation (My Computer).

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.



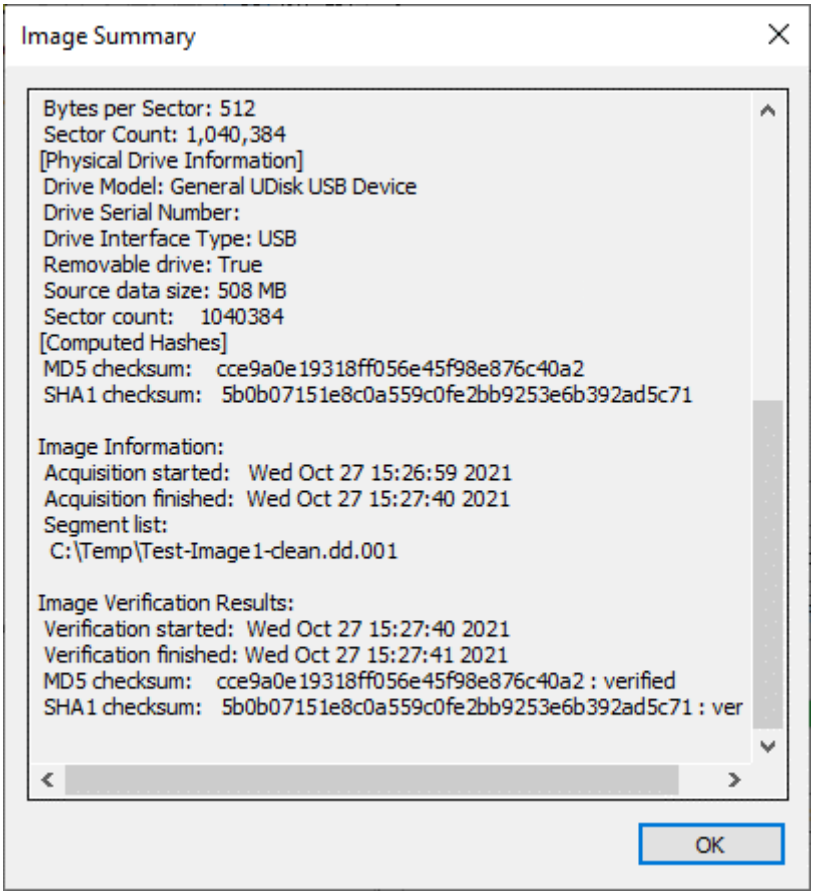

ProDiscover Basic
File Action View Tools Help
Project
Report
Add
Remove
Content View
Images
Disks
All Selected Files
Cluster View
Images
Disks
Registry View
EventLog View
Internet History Viewer
View Log
Search
Search Results
Content Search Results
Cluster Search Results
Registry Search Results
Event Log Search Results
Internet Activity Search Results
Secure Wipe Disk
Disk to Wipe :
E:\
Number of Passes :
1
Pattern :
Start
Close


USB Drive (E:)


Formatting USB Drive (E:)
Capacity:
508 MB
File system
FAT32
Allocation unit size
4096 bytes
Restore device defaults
Volume label
Format options
Quick Format
Start
Cancel
Formatting USB Drive (E:)
Format Complete.
OK
SAFE Block Win8-10 (X64) by ForensicSoft
DESKTOP-3030TDQ
Standard NVM Express Controller
WDC WDS100T2B0C-00PXH0[0:0:0][E823_8FA6_BF53_0001_001B_4
Standard SATA AHCI Controller
ST4000DM004-2CV104[2:0:0][WFN2BN9B4656C8A43B584AE1]
USB Mass Storage Device
General UDisk USB Device[0:0:0]
Help
Block
Unblock
Setup
Exit

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.



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.

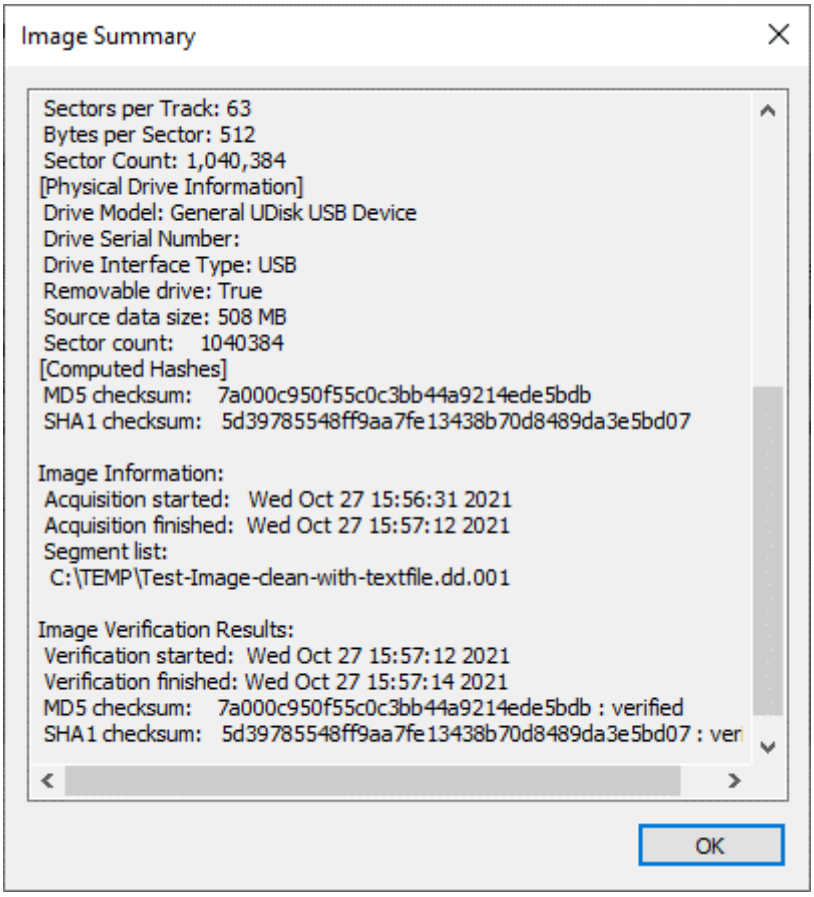
Can enable/disable Synchronized Template Results Scrolling.

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.

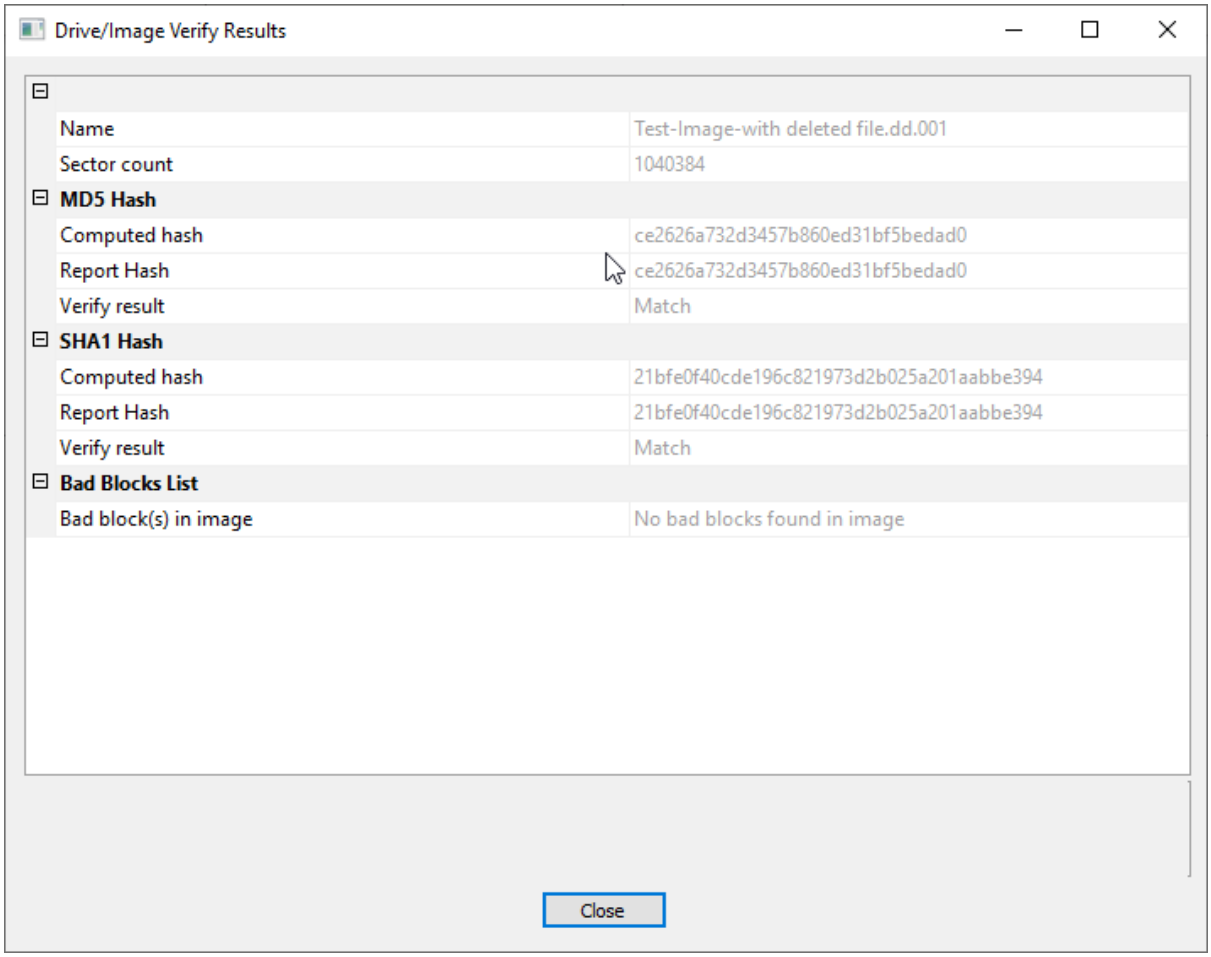
Part D: Putting a single text file on the USB and determining the differences

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.



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.


Drive/Image Verify Results
Name
Test-Image-with deleted file.dd.001
Sector count
1040384
MD5 Hash
Computed hash
ce2626a732d3457b860ed31bf5bedad0
Report Hash
ce2626a732d3457b860ed31bf5bedad0
Verify result
Match
SHA1 Hash
Computed hash
21bfe0f40cde196c821973d2b025a201aabbe394
Report Hash
21bfe0f40cde196c821973d2b025a201aabbe394
Verify result
Match
Bad Blocks List
Bad block(s) in image
No bad blocks found in image
Close

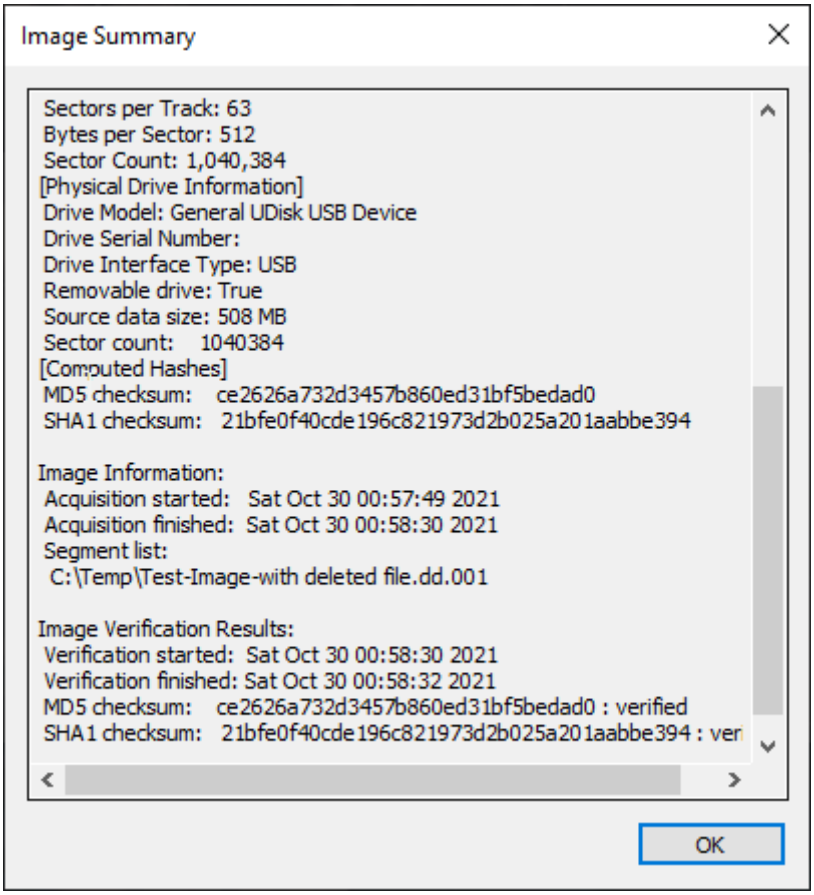


Image Summary
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 1,040,384
[Physical Drive Information]
Drive Model: General UDisk USB Device
Drive Serial Number:
Drive Interface Type: USB
Removable drive: True
Source data size: 508 MB
Sector count: 1040384
[Computed Hashes]
MD5 checksum: ce2626a732d3457b860ed31bf5bedad0
SHA1 checksum: 21bfe0f40cde196c821973d2b025a201aabbe394
Image Information:
Acquisition started: Sat Oct 30 00:57:49 2021
Acquisition finished: Sat Oct 30 00:58:30 2021
Segment list:
C:\Temp\Test-Image-with deleted file.dd.001
Image Verification Results:
Verification started: Sat Oct 30 00:58:30 2021
Verification finished: Sat Oct 30 00:58:32 2021
MD5 checksum: ce2626a732d3457b860ed31bf5bedad0 : verified
SHA1 checksum: 21bfe0f40cde196c821973d2b025a201aabbe394 : ver
OK

PART G: Directories and deletion

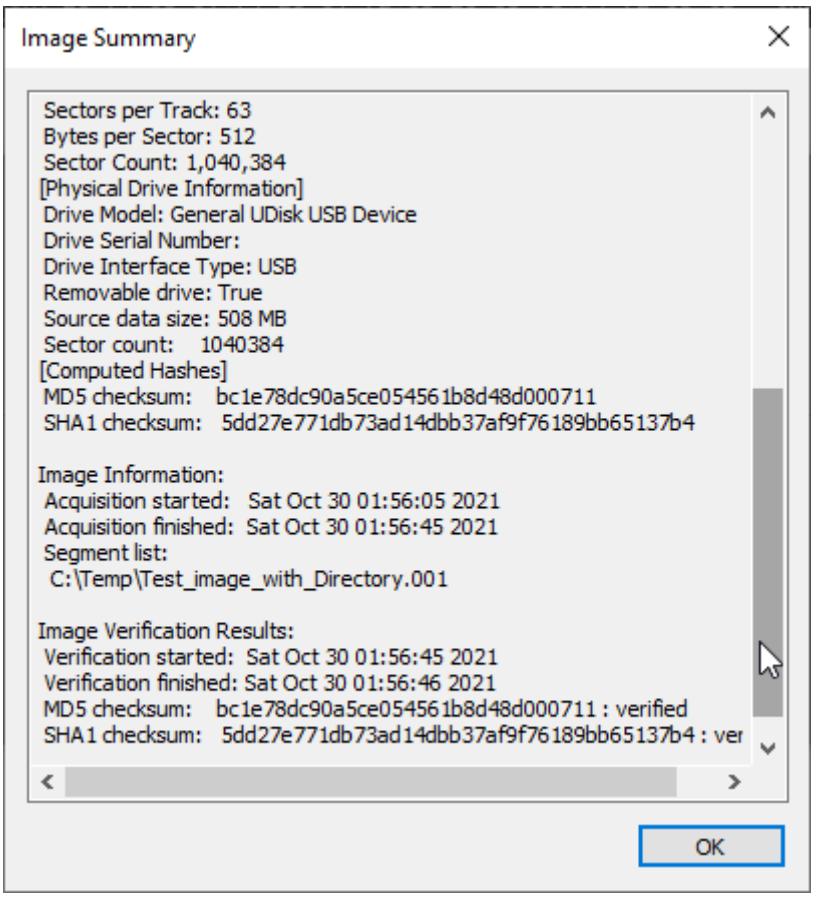
For part G I started by creating a new Directory on the USB Drive, by doing so I now have a USB with a boot sector, file system, remnants of a text file and a single directory.

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.

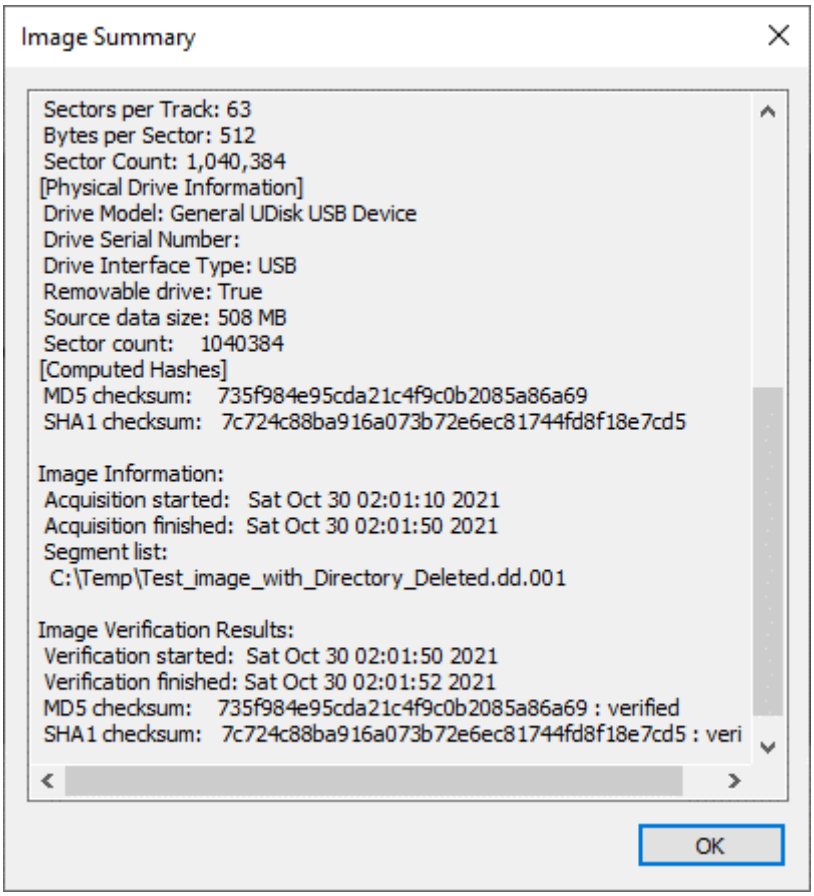
I will now use 101 Hex Editor to compare the two images and note my observations in my logbook.

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:



With Deleted Directory:



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.

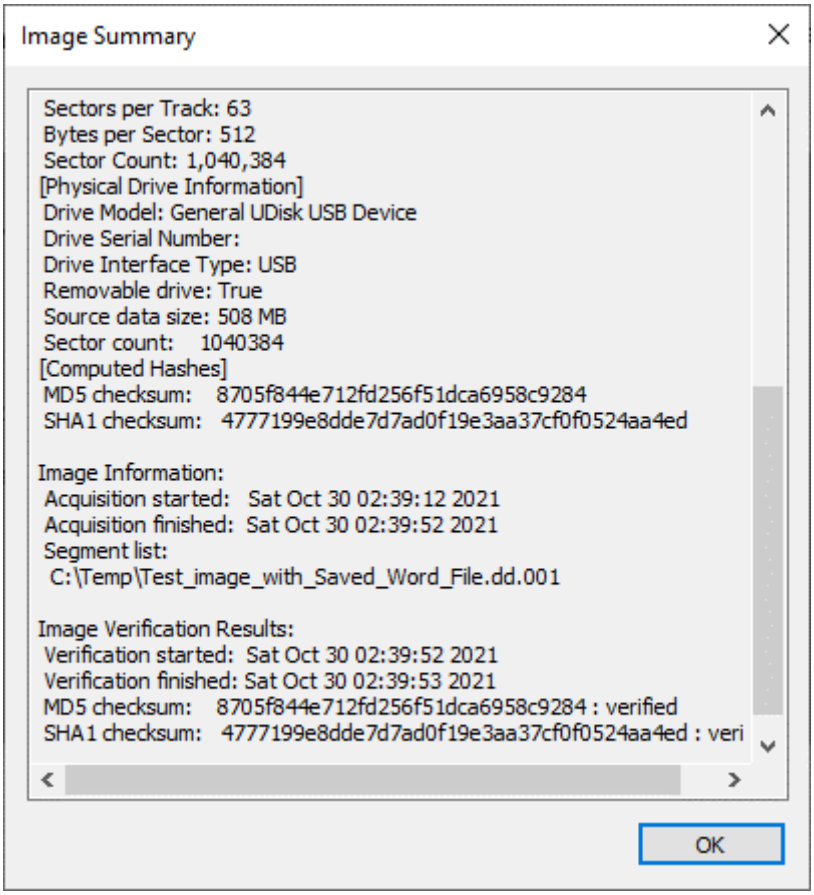
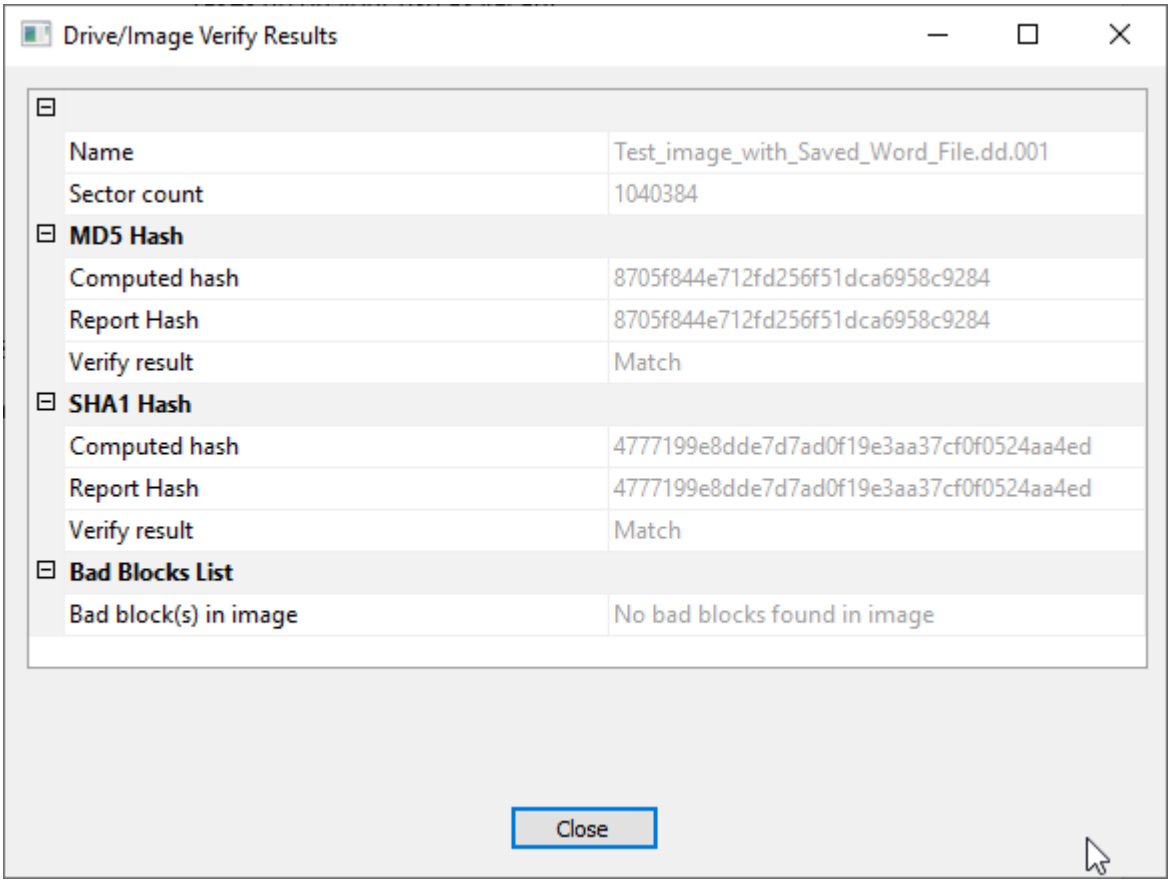


Image Summary
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 1,040,384
[Physical Drive Information]
Drive Model: General UDisk USB Device
Drive Serial Number:
Drive Interface Type: USB
Removable drive: True
Source data size: 508 MB
Sector count: 1040384
[Computed Hashes]
MD5 checksum: 8705f844e712fd256f51dca6958c9284
SHA1 checksum: 4777199e8dde7d7ad0f19e3aa37cf0f0524aa4ed
Image Information:
Acquisition started: Sat Oct 30 02:39:12 2021
Acquisition finished: Sat Oct 30 02:39:52 2021
Segment list:
C:\Temp\Test_image_with_Saved_Word_File.dd.001
Image Verification Results:
Verification started: Sat Oct 30 02:39:52 2021
Verification finished: Sat Oct 30 02:39:53 2021
MD5 checksum: 8705f844e712fd256f51dca6958c9284 : verified
SHA1 checksum: 4777199e8dde7d7ad0f19e3aa37cf0f0524aa4ed : veri
OK

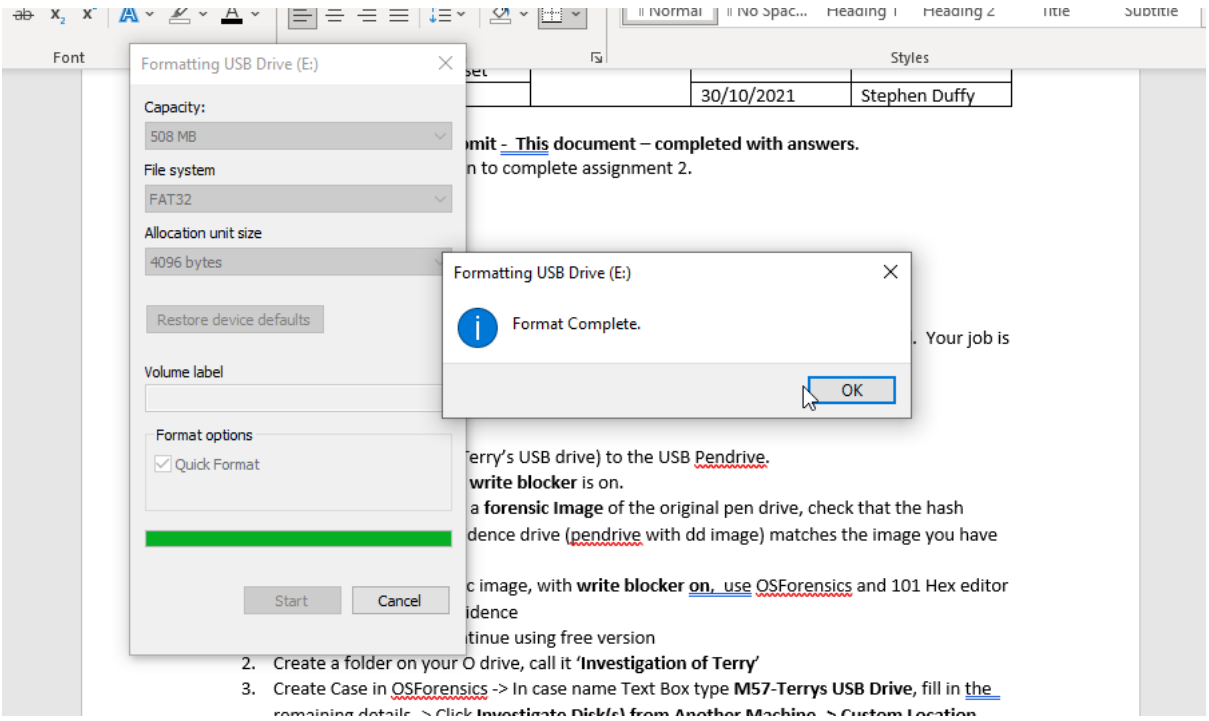

Drive/Image Verify Results
Name
Test_image_with_Saved_Word_File.dd.001
Sector count
1040384
MD5 Hash
Computed hash
8705f844e712fd256f51dca6958c9284
Report Hash
8705f844e712fd256f51dca6958c9284
Verify result
Match
SHA1 Hash
Computed hash
4777199e8dde7d7ad0f19e3aa37cf0f0524aa4ed
Report Hash
4777199e8dde7d7ad0f19e3aa37cf0f0524aa4ed
Verify result
Match
Bad Blocks List
Bad block(s) in image
No bad blocks found in image
Close

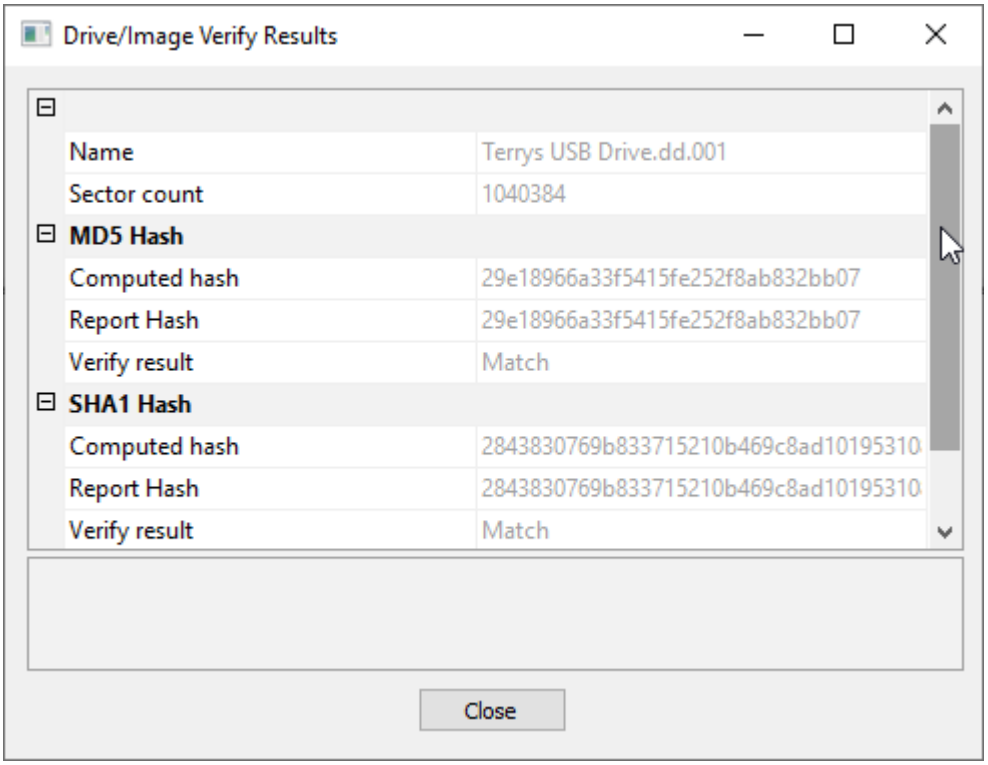
Part I: Forensic Investigation and Application of Parts A – H

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.




Drive/Image Verify Results
Name
Terrys USB Drive.dd.001
Sector count
1040384
MD5 Hash
Computed hash
29e18966a33f5415fe252f8ab832bb07
Report Hash
29e18966a33f5415fe252f8ab832bb07
Verify result
Match
SHA1 Hash
Computed hash
2843830769b833715210b469c8ad10195310
Report Hash
2843830769b833715210b469c8ad10195310
Verify result
Match
Close

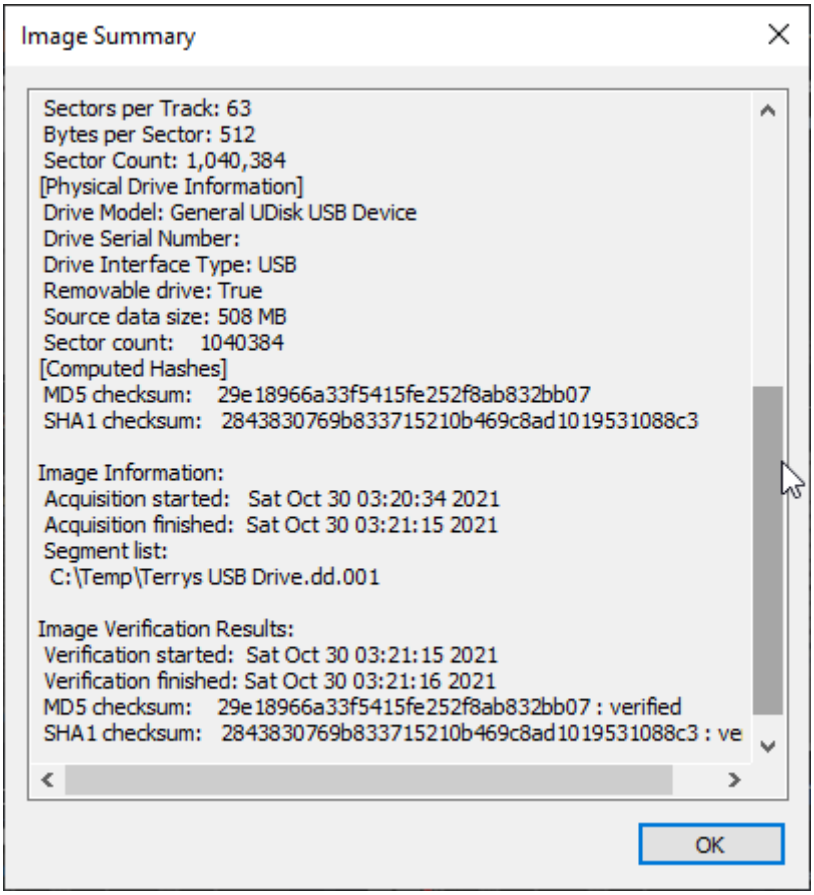


Image Summary
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 1,040,384
[Physical Drive Information]
Drive Model: General UDisk USB Device
Drive Serial Number:
Drive Interface Type: USB
Removable drive: True
Source data size: 508 MB
Sector count: 1040384
[Computed Hashes]
MD5 checksum: 29e18966a33f5415fe252f8ab832bb07
SHA1 checksum: 2843830769b833715210b469c8ad1019531088c3
Image Information:
Acquisition started: Sat Oct 30 03:20:34 2021
Acquisition finished: Sat Oct 30 03:21:15 2021
Segment list:
C:\Temp\Terrys USB Drive.dd.001
Image Verification Results:
Verification started: Sat Oct 30 03:21:15 2021
Verification finished: Sat Oct 30 03:21:16 2021
MD5 checksum: 29e18966a33f5415fe252f8ab832bb07 : verified
SHA1 checksum: 2843830769b833715210b469c8ad1019531088c3 : ve
OK