Lab 2: Live Recovery

CNIT42000-001

Ethan Hammond

Prof. Tahir Khan

Date Submitted: 2/2/23

Date Due: 2/2/23

Table of Contents

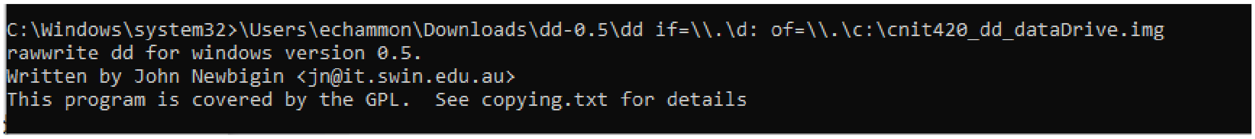
Abstract

During the investigation, a USB drive was acquired and were given to the CNIT 420 lab at Purdue and were asked to complete several tasks with the drive. First, the drive was converted to a RAW dd format with Windows PowerShell, and the hash of the file was examined. The drive was then put in an E01 format with AccessData FTK with no compression, and the hash was compared to the RAW hash. The E01 image was put into Autopsy to examine the files and metadata to find out the most relevant information about the files on the drive. The goal of the laboratory exercise was to compare and contrast the different conversion methods as well as what information can be extracted with Autopsy and what to do with the information after it has been examined.

Report

Task 1:

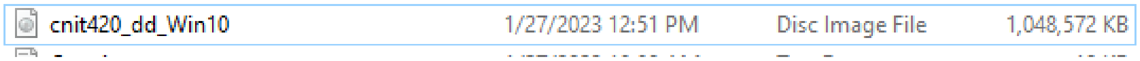
Most investigations of digital media is first copied from the direct source onto the computer of the forensic investigator. In this case, the suspect USB needed to be transferred onto the lab computer. This was done through the dd tool found in Purdue RTFM. The drive was made into an image file by use of the dd tool shown in Figure 1 below in Windows PowerShell.



```
C:\Windows\system32>\Users\echammon\Downloads\dd-0.5\dd if=\\.\d: of=\\.\c:\cnit420_dd_dataDrive.img
rawwrite dd for windows version 0.5.
Written by John Newbigin <jn@it.swin.edu.au>
This program is covered by the GPL.  See copying.txt for details
```

Figure 1: Copying of the files from the USB drive (D:\) to the image file on the computer's C:\ drive.

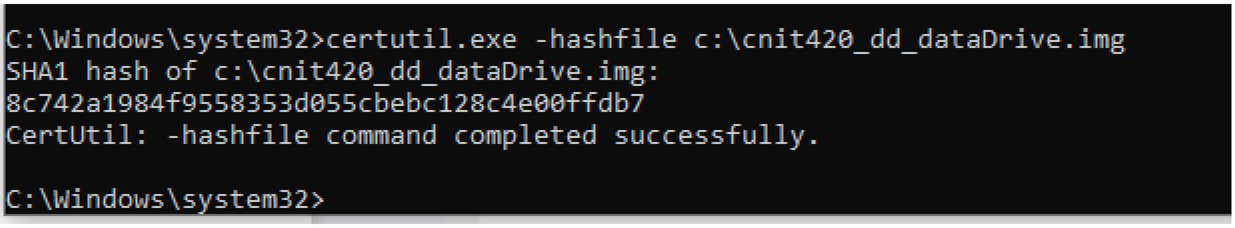
As the 'of=' field was set to 'c:\cnit420_dd_Win10.img', the image file that was created was put into the base C:\ drive on the machine with the correct name of the file. The created file can be seen in Figure 2 below.



```
cnit420_dd_Win10          1/27/2023 12:51 PM     Disc Image File     1,048,572 KB
```

Figure 2: New img named "cnit420_dd_Win10.img" on the C:\ drive.

The next step after copying a user's drive to the forensic lab computer is to compute a hash function of a file so that it is able to be proven that there were no modifications to the data, as the hashes will be the exact same if no changes have been made to either image or drive. The MD5 hash of the image can be seen in Figure 3 below.

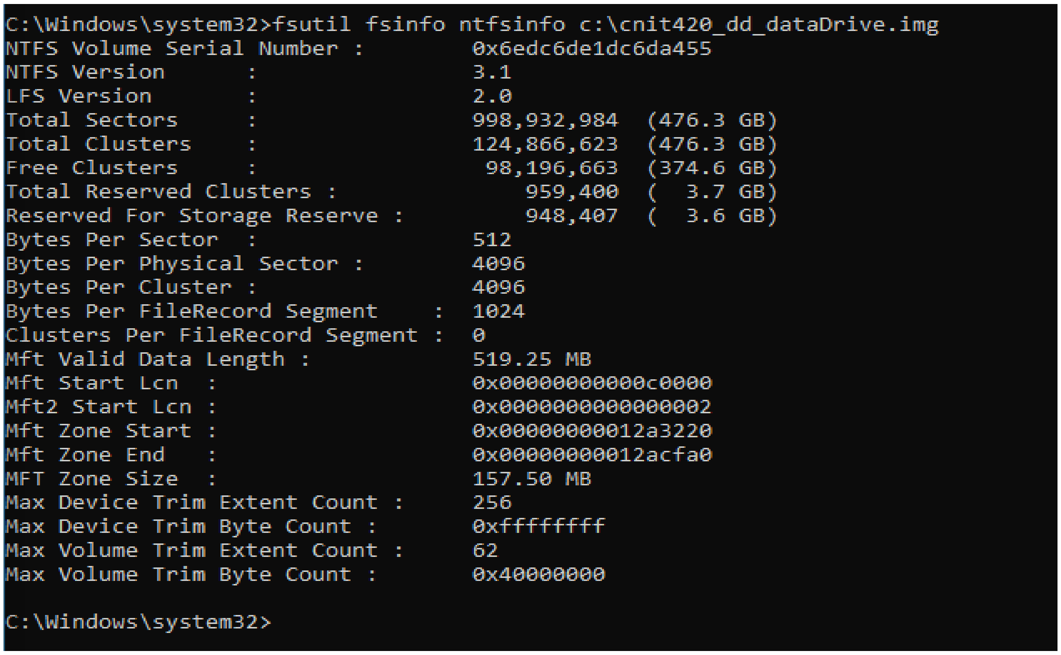


```
C:\Windows\system32>certutil.exe -hashfile c:\cnit420_dd_dataDrive.img
SHA1 hash of c:\cnit420_dd_dataDrive.img:
8c742a1984f9558353d055cbebc128c4e00ffdb7
CertUtil: -hashfile command completed successfully.

C:\Windows\system32>
```

Figure 3: Hashing the new created image file with certutil.exe utility built into cmd.exe.

In the dd.exe utility, the ‘in’ refers to the file input. In this case, the file being inputted is the USB drive that we are turning into an image file. The ‘out’ keyword refers to the file being outputted including the file name and extension as well as the path that the user would like to send the dd image file to. The block size of the image can be found in Windows PowerShell using *fsutil* shown in Figure 4 below. The block size is shown below in the ‘Total Clusters’, being 476.3GB in size.



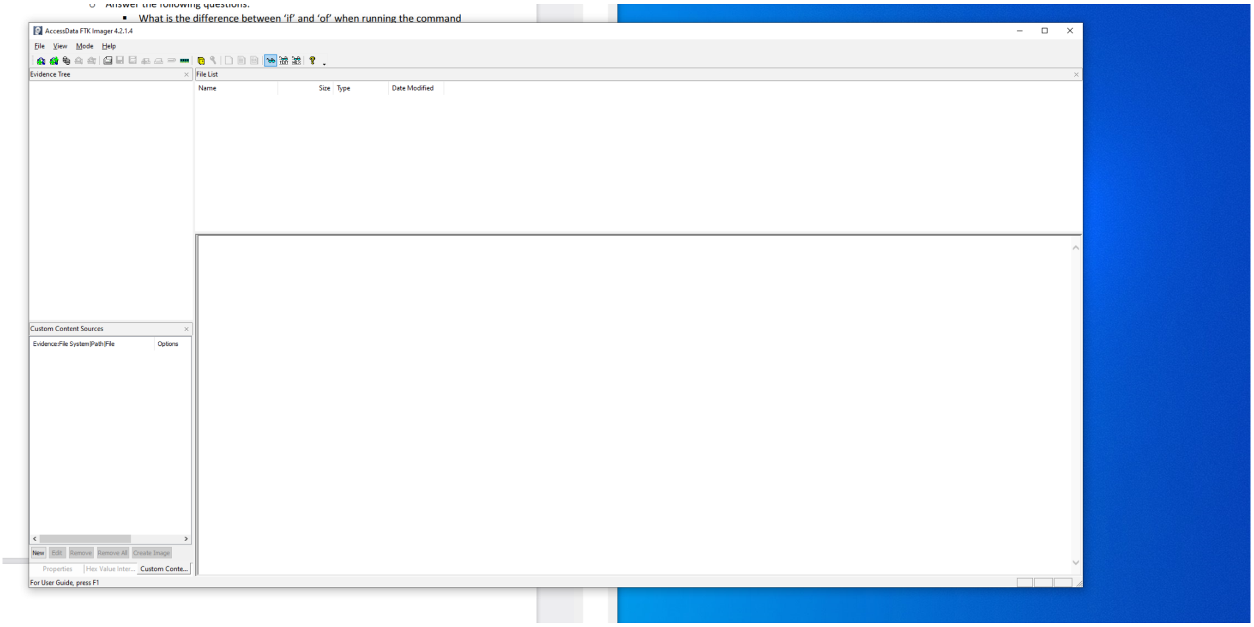
```
C:\Windows\system32>fsutil fsinfo ntfsinfo c:\cnit420_dd_dataDrive.img
NTFS Volume Serial Number :        0x6edc6de1dc6da455
NTFS Version      :                3.1
LFS Version       :                2.0
Total Sectors     :                998,932,984  (476.3 GB)
Total Clusters    :                124,866,623  (476.3 GB)
Free Clusters     :                 98,196,663  (374.6 GB)
Total Reserved Clusters :              959,400  (  3.7 GB)
Reserved For Storage Reserve :         948,407  (  3.6 GB)
Bytes Per Sector  :                512
Bytes Per Physical Sector :        4096
Bytes Per Cluster :                4096
Bytes Per FileRecord Segment    :  1024
Clusters Per FileRecord Segment :  0
Mft Valid Data Length :            519.25 MB
Mft Start Lcn  :                   0x00000000000c0000
Mft2 Start Lcn :                   0x0000000000000002
Mft Zone Start :                   0x00000000012a3220
Mft Zone End   :                   0x00000000012acfa0
MFT Zone Size  :                   157.50 MB
Max Device Trim Extent Count :     256
Max Device Trim Byte Count :       0xffffffff
Max Volume Trim Extent Count :     62
Max Volume Trim Byte Count :       0x40000000

C:\Windows\system32>
```

Figure 4: Block size shown with the fsutil utility from a Windows command prompt in administrator mode.

Task 2:

To create an image using FTK imager, the very first thing that needs to be accomplished is the installation of the imaging software. The installation of AccessData FTK onto the Windows 10 Lab machine can be seen in Figure 5 below.

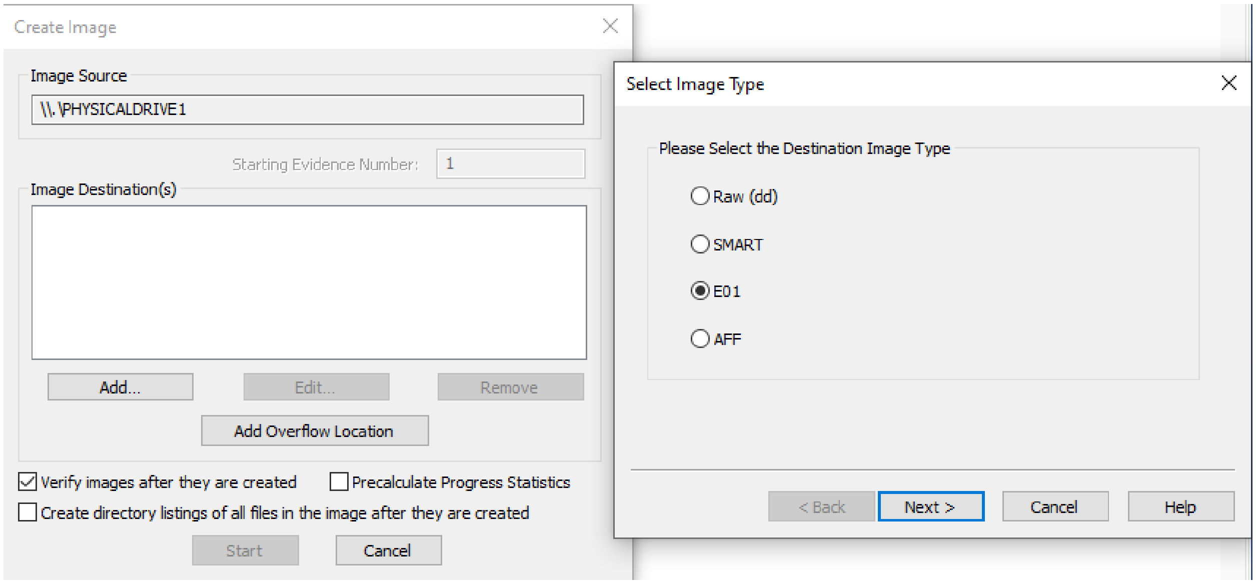


Answer the following questions.

- What is the difference between ‘if’ and ‘of’ when running the command

Figure 5: Installation of AccessData FTK on the Windows lab computer.

Once the imaging software had been installed, it was then necessary to choose the source media, being the suspect flash drive, and choose an image type to be converted to. In this case, the E01 destination image type was to be selected, and can be seen in Figure 6 below.



Create Image

Image Source

\\.\PHYSICALDRIVE1

Starting Evidence Number: 1

Image Destination(s)

☑ Verify images after they are created ☐ Precalculate Progress Statistics

☐ Create directory listings of all files in the image after they are created

Select Image Type

Please Select the Destination Image Type

○ Raw (dd)

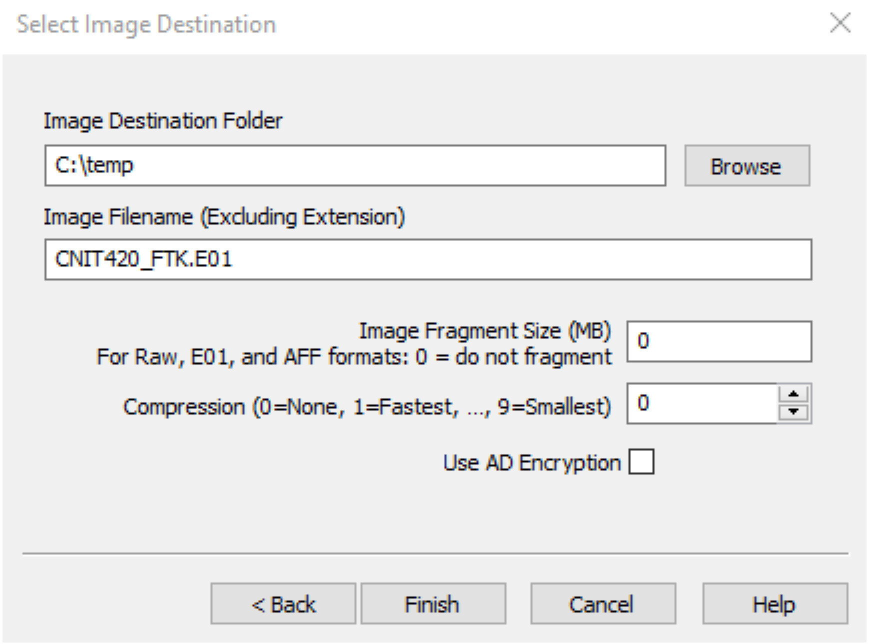
○ SMART

● E01

○ AFF

Figure 6: Adding of the USB drive to AccessData FTX and selection of E01 File type to be converted into.

After the image source and destination file type were selected, it was necessary to choose a filename, a file destination area, image fragment size, as well as a compression amount. For this lab, it was specified not to use any fragmenting size or compression amount. The specific selections can be seen below in Figure 7.



Select Image Destination

Image Destination Folder

C:\temp

Image Filename (Excluding Extension)

CNIT420_FTK.E01

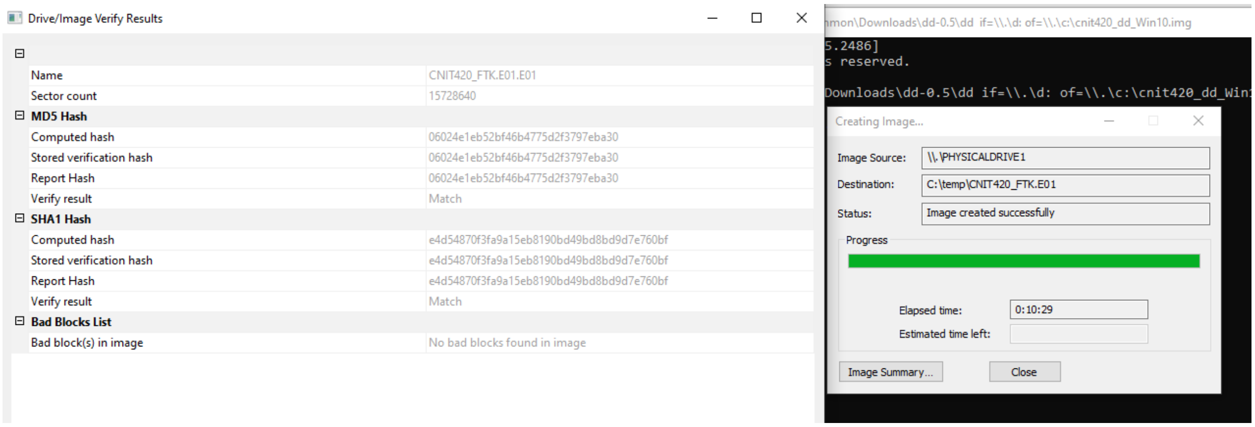
Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment: 0

Compression (0=None, 1=Fastest, ..., 9=Smallest): 0

Use AD Encryption □

Figure 7: Image destination settings with no fragmentation or compression.

Once the media was launched and the conversion started, a progress bar appeared and took about six minutes to complete the conversion. After it was converted, a verification summary results tab was provided including sector count and hash details. As shown in Figure 8 below, the new hash can be seen.



Drive/Image Verify Results

Name	CNIT420_FTK.E01.E01
Sector count	15728640
MD5 Hash	
Computed hash	06024e1eb52bf46b4775d2f3797eba30
Stored verification hash	06024e1eb52bf46b4775d2f3797eba30
Report Hash	06024e1eb52bf46b4775d2f3797eba30
Verify result	Match
SHA1 Hash	
Computed hash	e4d54870f3fa9a15eb8190bd49bd8bd9d7e760bf
Stored verification hash	e4d54870f3fa9a15eb8190bd49bd8bd9d7e760bf
Report Hash	e4d54870f3fa9a15eb8190bd49bd8bd9d7e760bf
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

```
mon\Downloads\dd-0.5\dd  if=\\.\d: of=\\.\c:\cnit420_dd_Win10.img
5.2486]
s reserved.

Downloads\dd-0.5\dd if=\\.\d: of=\\.\c:\cnit420_dd_Win
```

Creating Image...

Image Source: \\.\PHYSICALDRIVE1

Destination: C:\temp\CNIT420_FTK.E01

Status: Image created successfully

Progress

Elapsed time: 0:10:29

Estimated time left:

Figure 8: Finished creation of “CNIT420_FTK.E01” image in the C:\Temp file on the lab computer and the results and hash of the new file.

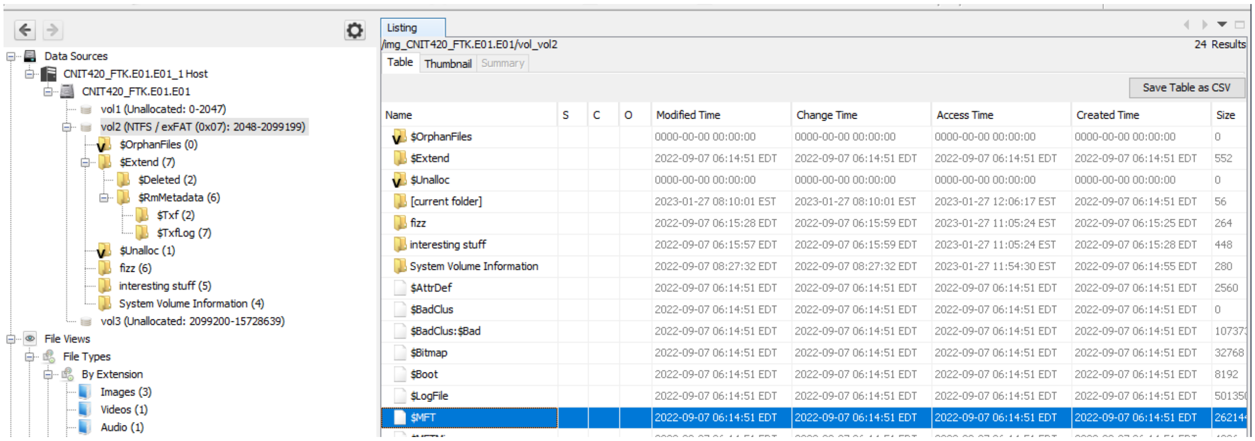
The hash value created here by the same drive was given a different hash than the image created in Task 1 because there was a different method of converting the media into an image. The different methods and softwares use different encryption methods. This makes it critical to use the same methods and software when copying a suspect drive in cyber forensics.

Image Type	Summary
RAW	Most common, do not contain headers or metadata. Pads all memory ranges that were skipped. Fast, most tools can use RAW format.
E01	Encase file format. Compresses the image file, and contains a lot of data including date/time of acquisition as well as information about the investigator.
SMART	Designed for Linux OS, uses efficient compression.
AFF	Advanced Forensics Format. Available to compress or uncompress. Open source, and provides extra space for metadata.

Figure 9: Differences between RAW dd, E01, SMART, and AFF image formats. Information taken from Professor Khan’s Brightspace Slides.

Task 3:

After the drive had been converted into an E01 image, it was necessary to inspect all aspects of the drive in Autopsy. The Master File Table was sought to be found because it contains valuable information about all files on the drive. The MFT can be seen in Figure 10 off of the suspect's image.



- Data Sources
  - CNIT420_FTK.E01.E01_1 Host
    - CNIT420_FTK.E01.E01
      - vol1 (Unallocated: 0-2047)
      - vol2 (NTFS / exFAT (0x07): 2048-2099199)
        - $OrphanFiles (0)
        - $Extend (7)
          - $Deleted (2)
          - $RmMetadata (6)
            - $Txf (2)
            - $TxfLog (7)
        - $Unalloc (1)
        - fizz (6)
        - interesting stuff (5)
        - System Volume Information (4)
      - vol3 (Unallocated: 2099200-15728639)
- File Views
  - File Types
    - By Extension
      - Images (3)
      - Videos (1)
      - Audio (1)

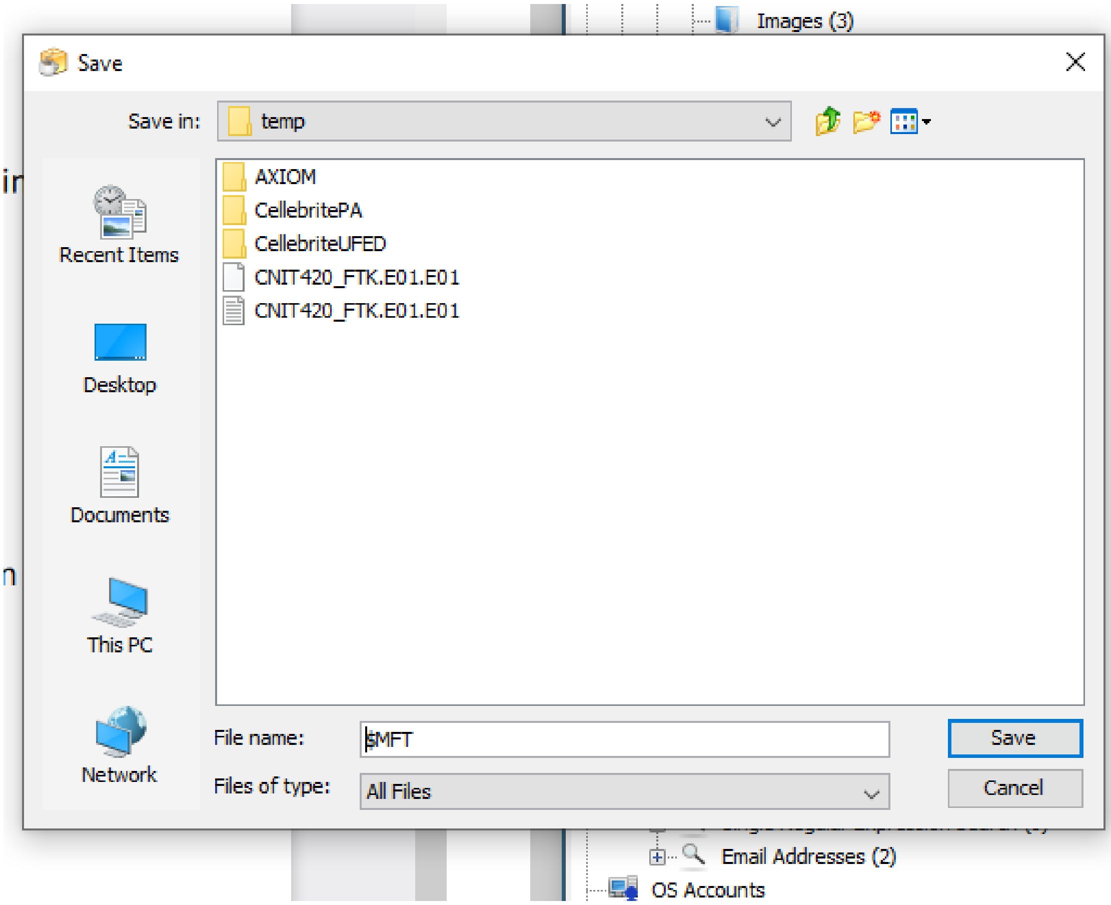
/img_CNIT420_FTK.E01.E01/vol_vol2

24 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
$OrphanFiles				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
$Extend				2022-09-07 06:14:51 EDT	2022-09-07 06:14:51 EDT	2022-09-07 06:14:51 EDT	2022-09-07 06:14:51 EDT	552
$Unalloc				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
[current folder]				2023-01-27 08:10:01 EST	2023-01-27 08:10:01 EST	2023-01-27 12:06:17 EST	2022-09-07 06:14:51 EDT	56
fizz				2022-09-07 06:15:28 EDT	2022-09-07 06:15:59 EDT	2023-01-27 11:05:24 EST	2022-09-07 06:15:25 EDT	264
interesting stuff				2022-09-07 06:15:57 EDT	2022-09-07 06:15:59 EDT	2023-01-27 11:05:24 EST	2022-09-07 06:15:28 EDT	448
System Volume Information				2022-09-07 08:27:32 EDT	2022-09-07 08:27:32 EDT	2023-01-27 11:54:30 EST	2022-09-07 06:14:55 EDT	280
$AttrDef				2022-09-07 06:14:51 EDT	2022-09-07 06:14:51 EDT	2022-09-07 06:14:51 EDT	2022-09-07 06:14:51 EDT	2560
$BadClus				2022-09-07 06:14:51 EDT	2022-09-07 06:14:51 EDT	2022-09-07 06:14:51 EDT	2022-09-07 06:14:51 EDT	0
$BadClus:$Bad				2022-09-07 06:14:51 EDT	2022-09-07 06:14:51 EDT	2022-09-07 06:14:51 EDT	2022-09-07 06:14:51 EDT	10737
$Bitmap				2022-09-07 06:14:51 EDT	2022-09-07 06:14:51 EDT	2022-09-07 06:14:51 EDT	2022-09-07 06:14:51 EDT	32768
$Boot				2022-09-07 06:14:51 EDT	2022-09-07 06:14:51 EDT	2022-09-07 06:14:51 EDT	2022-09-07 06:14:51 EDT	8192
$LogFile				2022-09-07 06:14:51 EDT	2022-09-07 06:14:51 EDT	2022-09-07 06:14:51 EDT	2022-09-07 06:14:51 EDT	50135
$MFT				2022-09-07 06:14:51 EDT	2022-09-07 06:14:51 EDT	2022-09-07 06:14:51 EDT	2022-09-07 06:14:51 EDT	26214

Figure 10: Master File table found in Vol2.

To secure the evidence in this scenario, the MFT was saved to the C:\temp on the lab computer that was used to inspect the image. This way, if the E01 image was damaged or something happened to it, the MFT could be used to determine what files are on the drive and where they are located. The exporting of the MFT can be seen in Figure 11 below.



Save in: temp

AXIOM
CellebritePA
CellebriteUFED
CNIT420_FTK.E01.E01
CNIT420_FTK.E01.E01

File name: $MFT
Files of type: All Files

Figure 11: Exporting the MFT onto the hard drive of the lab computer.

As the laboratory was done with a flash drive that was only given out during the two-hour lab period, time ran out and the address of the file IMG_0301.JPEG was not able to be inspected long enough to find the street address that it was taken on. However, if the drive was able to be reacquired, then the investigators would make sure to check the EXIF checkbox when uploading the data source to Autopsy. Then, the file would be opened, and viewed the EXIF metadata to find the street address that the photo was taken in.

Conclusion

As digital forensic investigators, it is important to know the different types of imaging sources and conversion methods, how to use them, and what each data type offers. When copying a drive over from a suspect, it can be useful to know what is needed off of the drive, and which method to use to copy over the data to a .img file. It is also vitally important for digital forensic analysts to know how to compare the hashes of files and be able to use those values to prove that the file is reliable and the integrity of the data is still in-tact. Lastly, digital forensic investigators need to know how to use different data source methods to find out every bit of relevant information that they can. Information like where a photo was taken can be of use to a criminal or civil investigation or defense. Different ways data can be stored, converted, hashed, and what information is available on files are all pieces of a cyber forensic analyst’s job in providing as much relevant information as possible off of a provided datasource.

References

Basis Tech (2022). Autopsy Digital Forensics. https://www.autopsy.com/download/

Bytes, Alex, et al. “Get Windows NTFS Block Size.” *ByteSizedAlex*, 22 Mar. 2019, https://www.bytesizedalex.com/get-windows-ntfs-block-size/.

Lab Report Template. Login - Purdue University system. (n.d.). Retrieved January 20, 2023, from https://purdue.brightspace.com/d2l/le/content/702085/viewContent/12038644/View

“Lab 2 Instruction Manual.” Login - Purdue University System, https://purdue.brightspace.com/d2l/le/content/702085/viewContent/12038647/View.

Redirecting. (n.d.). Retrieved February 2, 2023, from https://answers.microsoft.com/en-us/windows/forum/all/how-to-determine-file-system-block-size/8d9b441d-4ea1-44b9-bbad-2e79a0479359

Time Chart

Task Number	Time Taken
Task 1	1 Hour
Task 2	30 Minutes
Task 3	30 Minutes
Report Writing	2 Hours
Total	4 Hours