

Donald's Investigation

31/01/2022 - Shivangi is asked by Robert to investigate allegations on Donald about downloading's non-work related files to his external drive - authorize to seize or view entire computer if necessary.

Seized Donald's drive from work station.

7/02/2022 - Attached the disk to forensics workstation Ubuntu 20.04 for imaging

Identified suspected drive as sdb on forensic station, size is 102MiB, 2 partitions found each approximately half the drive. One FAT (sdb1) and one NTFS (sdb2).

Verified the presence of disk

- shivangi@ubuntu:~\$ lshw -class disk -businfo:

Bus info	Device	Class	Description
scsi@32:0.0.0	/dev/sda	disk	21GB VMware Virtual S
scsi@32:0.1.0	/dev/sdb	disk	106MB VMware Virtual S
scsi@3:0.0.0	/dev/cdrom	disk	VMware SATA CD01
	/dev/cdrom	disk	

Details about the disk

- shivangi@ubuntu:~\$ fdisk -l /dev/sdb:

Disk /dev/sdb: 102 MiB, 106954752 bytes, 208896 sectors

Disk model: VMware Virtual S

Units: sectors of 1 * 512 = 512 bytes

Sector size (logical/physical): 512 bytes / 512 bytes

I/O size (minimum/optimal): 512 bytes / 512 bytes

Disklabel type: dos

Disk identifier: 0x536b9e19

Device	Boot	Start	End	Sectors	Size	Id	Type
--------	------	-------	-----	---------	------	----	------

/dev/sdb1	128	102527	102400	50M	c	W95
-----------	-----	--------	--------	-----	---	-----

FAT32 (LBA)

/dev/sdb2	102528	202879	100352	49M	7	
-----------	--------	--------	--------	-----	---	--

HPFS/NTFS/exFAT

Extra space is noted at the end of the drive as well as starting of reserved space.

For next imaging step to perform and store, moving to the donalds investigation file.

- shivangi@ubuntu:~\$ cd Documents/Donald-investigation/

The whole disk and the partitions are captured and compressed.

whole disk:

- shivangi@ubuntu:~/Documents/Donald-investigation\$ dd if=/dev/sdb bs=1M | gzip > wholedrive.dd.gz
102+0 records in
102+0 records out
106954752 bytes (107 MB, 102 MiB) copied, 10.0557 s, 10.6 MB/s

part 1:

- shivangi@ubuntu:~/Documents/Donald-investigation\$ dd if=/dev/sdb1 bs=1M | gzip > part1.dd.gz
50+0 records in
50+0 records out
52428800 bytes (52 MB, 50 MiB) copied, 4.6425 s, 11.3 MB/s

part 2:

- shivangi@ubuntu:~/Documents/Donald-investigation\$ dd if=/dev/sdb2 bs=1M | gzip > part2.dd.gz
49+0 records in
49+0 records out
51380224 bytes (51 MB, 49 MiB) copied, 5.08609 s, 10.1 MB/s

The images created are hashed

- shivangi@ubuntu:~/Documents/Donald-investigation\$dc3dd if=/dev/sdb hash=md5 hash=sha1 hash=sha256 hash=sha512 hlog=wholedrive.hlog | gzip > wholedrive.dc3dd.gz

dc3dd 7.2.646 started at 2022-02-07 16:34:49 -0800

compiled options:

command line: dc3dd if=/dev/sdb hash=md5 hash=sha1 hash=sha256 hash=sha512 hlog=wholedrive.hlog

device size: 208896 sectors (probed), 106,954,752 bytes

sector size: 512 bytes (probed)

106954752 bytes (102 M) copied (100%), 32 s, 3.2 M/s

input results for device `/dev/sdb':

208896 sectors in

0 bad sectors replaced by zeros

fe366ed45fc565669f6727e2730212 (md5)

ba70db0473d92560f7bb4d3ae3ec2f3c544516de (sha1)

6f8f847371b02a6be7ef4346770c94f660003684fe8ab7b24b66cc0c2467c17a (sha256)

b8ab8a17e03c1c864a27b724acache80fd5bc69c732cf3d5ea6770294662b79afa550783912d8d1e90cf7b0fed30fd0310d2b9f099e4b77d34ca3b640fce368f (sha512)

output results for file `stdout':

208896 sectors out

dc3dd completed at 2022-02-07 16:35:21 -0800

The ownership of the whole disk hash log file is changed.

- shivangi@ubuntu:~/Documents/Donald-investigation\$ sudo chown shivangi wholedrive.hlog

shivangi@ubuntu:~/Documents/Donald-investigation\$ ls -l

total 26204

```
-rw-rw-r-- 1 shivangi shivangi 2136 Feb  7 20:42 activities.txt
-rw-rw-r-- 1 shivangi shivangi 4392281 Feb  7 16:26 part1.dd.gz
-rw-rw-r-- 1 shivangi shivangi 4543381 Feb  7 16:26 part2.dd.gz
-rw-rw-r-- 1 shivangi shivangi 8939694 Feb  7 16:35 wholedrive.dc3dd.gz
-rw-rw-r-- 1 shivangi shivangi 8939694 Feb  7 16:22 wholedrive.dd.gz
-rw-r--r-- 1 shivangi root      597 Feb  7 16:35 wholedrive.hlog
```

Generated sha256 hash for the whole drive image file.

- shivangi@ubuntu:~/Documents/Donald-investigation\$ gunzip < wholedrive.dd.gz|sha256sum > wholedrive.sha256

Finding image of Clint Eastwood in Donald's drive.

8/02/2022 The files are moved to a Windows 10 desktop for further investigation with the software

The wholedrive.dc3dd.gz decompressed on the windows desktop before inserting into Autopsy.

The following image of Clint Eastwood was found under the name whoisit3.jpg



The following is the report generated by Autopsy.

Windows-10-200495670-1032 - VMware Workstation

File Edit View VM Tabs Help

Autopsy Forensic Report for case: X

File | C:/Users/shiva/Documents/Donalds-investigation/Donalds_investigation/Reports/D...

Report Navigation

- Case Summary
- Tagged Files (1)
- Tagged Images (1)
- Tagged Results (0)

Autopsy Forensic Report

HTML Report Generated on 2022/02/08 14:41:55

Case: Donalds_investigation
Number of data sources in case: 1

Image Information:

wholedrive.dc3dd

Timezone: America/Los_Angeles
Path: C:/Users/shiva/Documents/Donalds-investigation/wholedrive.dc3dd/wholedrive.dc3dd

Software Information:

Autopsy Version:	4.19.3
Android Analyzer Module:	4.19.3
Android Analyzer (aLEAPP) Module:	4.19.3
Central Repository Module:	4.19.3

Activate Windows
Go to Settings to activate Windows.

Type here to search

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Windows-10-200495670-1032 - VMware Workstation

File Edit View VM Tabs Help

Autopsy Forensic Report for case: X

File | C:/Users/shiva/Documents/Donalds-investigation/Donalds_investigation/Reports/D...

Report Navigation

- Case Summary
- Tagged Files (1)
- Tagged Images (1)
- Tagged Results (0)

Data Source Integrity Module:	4.19.3
Email Parser Module:	4.19.3
Embedded File Extractor Module:	4.19.3
Encryption Detection Module:	4.19.3
Extension Mismatch Detector Module:	4.19.3
File Type Identification Module:	4.19.3
GPX Parser Module:	1.2
Hash Lookup Module:	4.19.3
Interesting Files Identifier Module:	4.19.3
Keyword Search Module:	4.19.3
PhotoRec Carver Module:	7.0
Picture Analyzer Module:	4.19.3
Plaso Module:	4.19.3
Recent Activity Module:	4.19.3
Virtual Machine Extractor Module:	4.19.3
YARA Analyzer Module:	4.19.3
iOS Analyzer (iLEAPP) Module:	4.19.3

Ingest History:

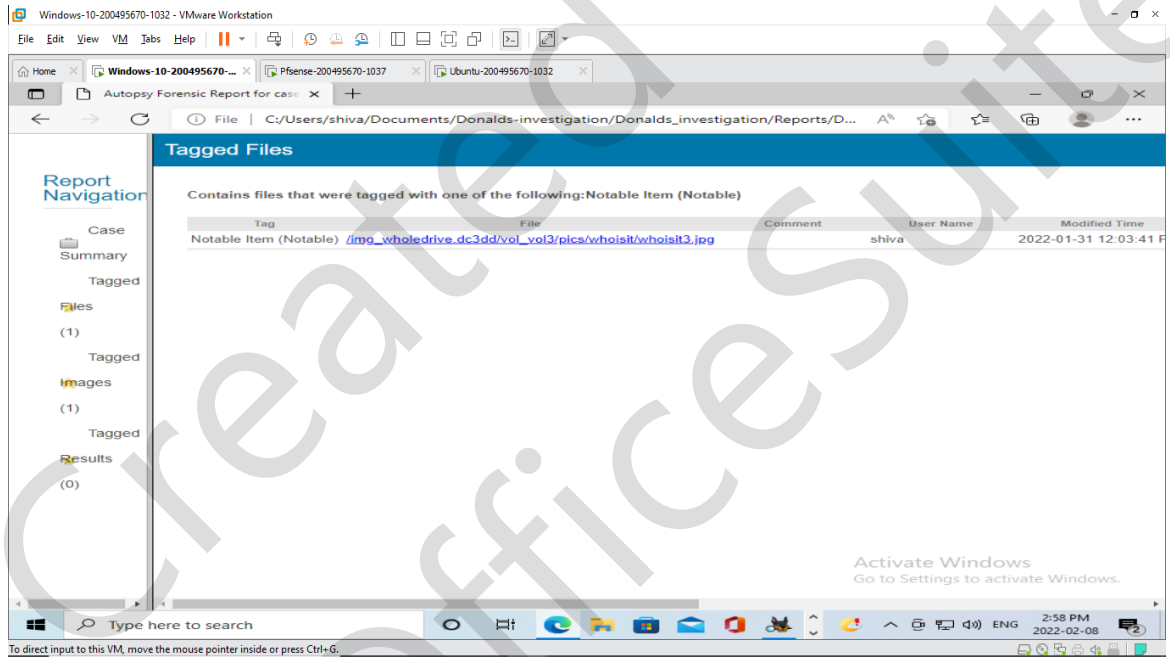
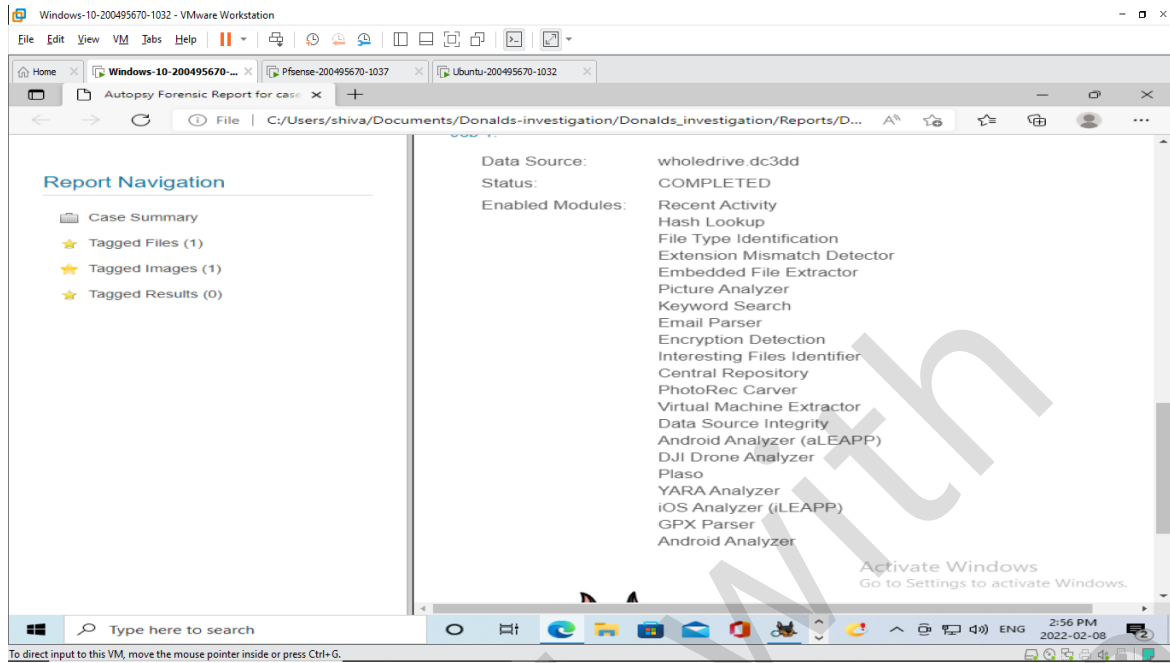
Job 1:

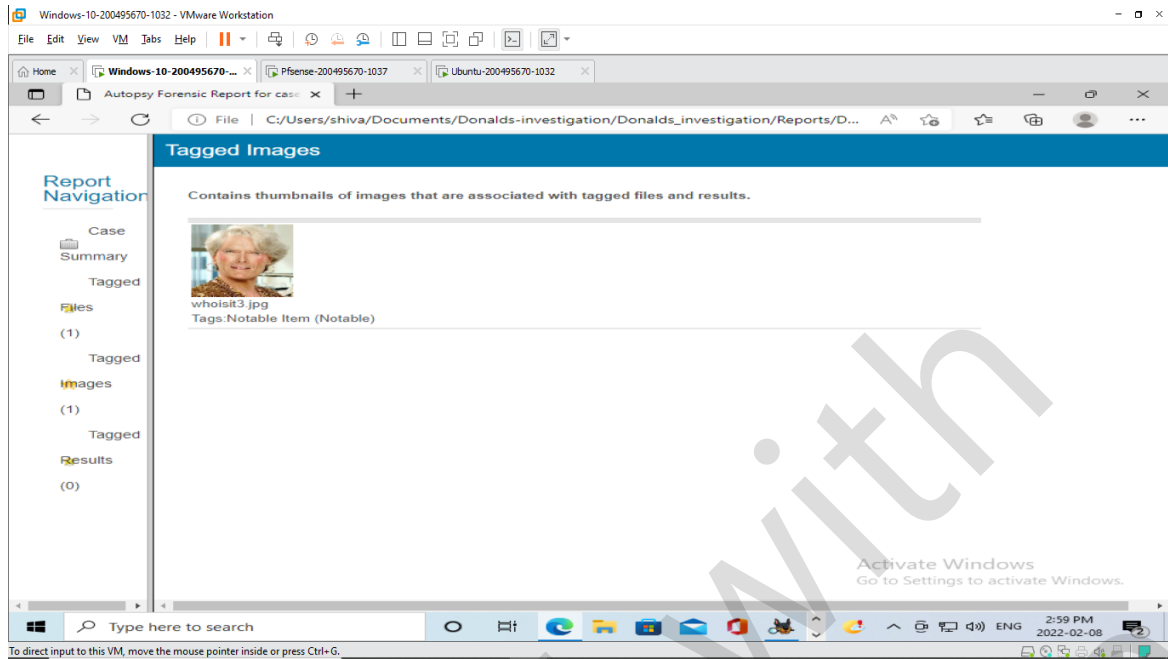
Data Source:	wholedrive.dc3dd
Status:	COMPLETED

Activate Windows
Go to Settings to activate Windows.

Type here to search

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



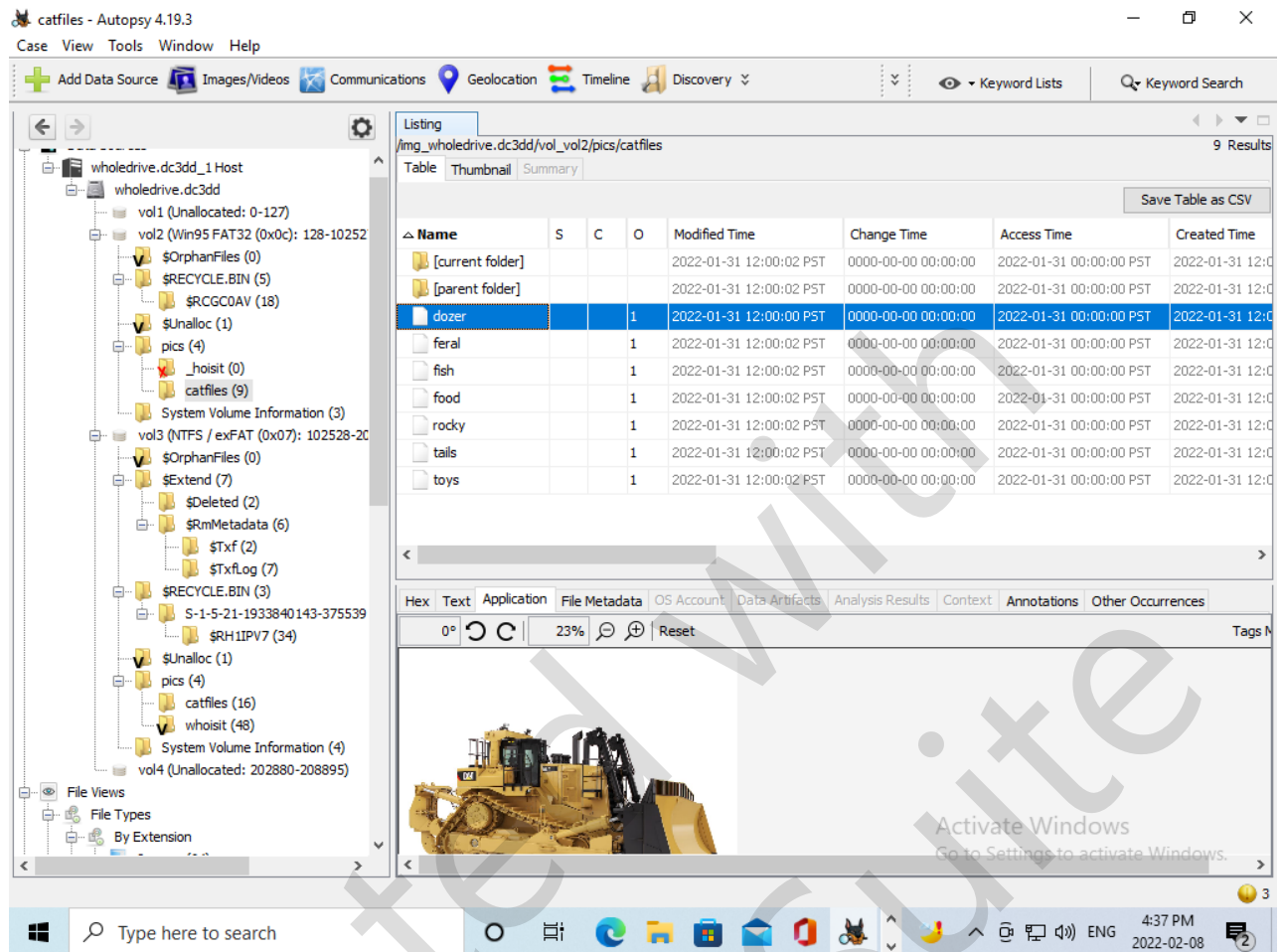


Finding Zone.identifier streams using Autopsy

8/02/2022 New case created and the image disk is uploaded to Autopsy to identify the difference between the drives.

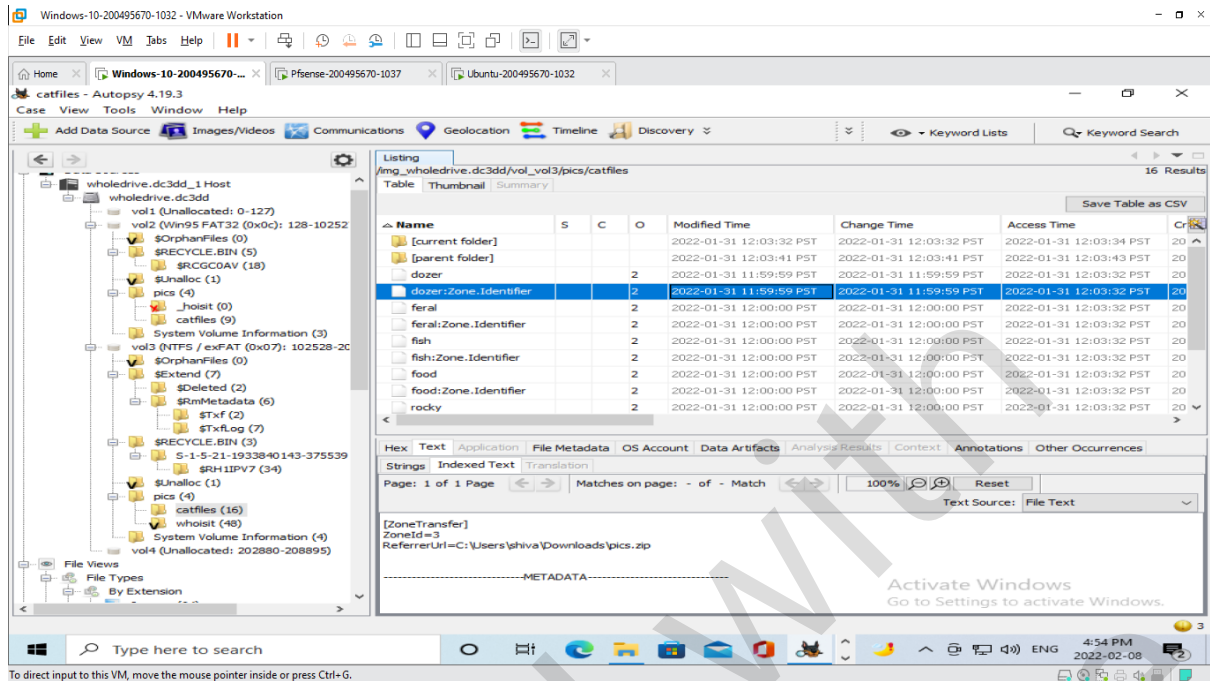
C drive is named as Volume 2 and D drive is named as Volume 3.

On collapsing the Volume 2(C drive) and navigating to catfiles folder, there are 9 files present that are of various images, parent folder and current folder .



On collapsing Volume 3(D drive) and navigating to catfiles folder, 16 files are present. These extra files have the images name along with .Zone.Identifiers.

There are 7 image files and their .zone.identifier files along with parent folder and current folder files.



Zone identifier files are generally created by the Microsoft OS when a file is downloaded for security purposes. These files get deleted when the files are deleted. This indicates that the images in Volume 2(C drive) were deleted, hence the less file count compared to Volume 3(D drive).