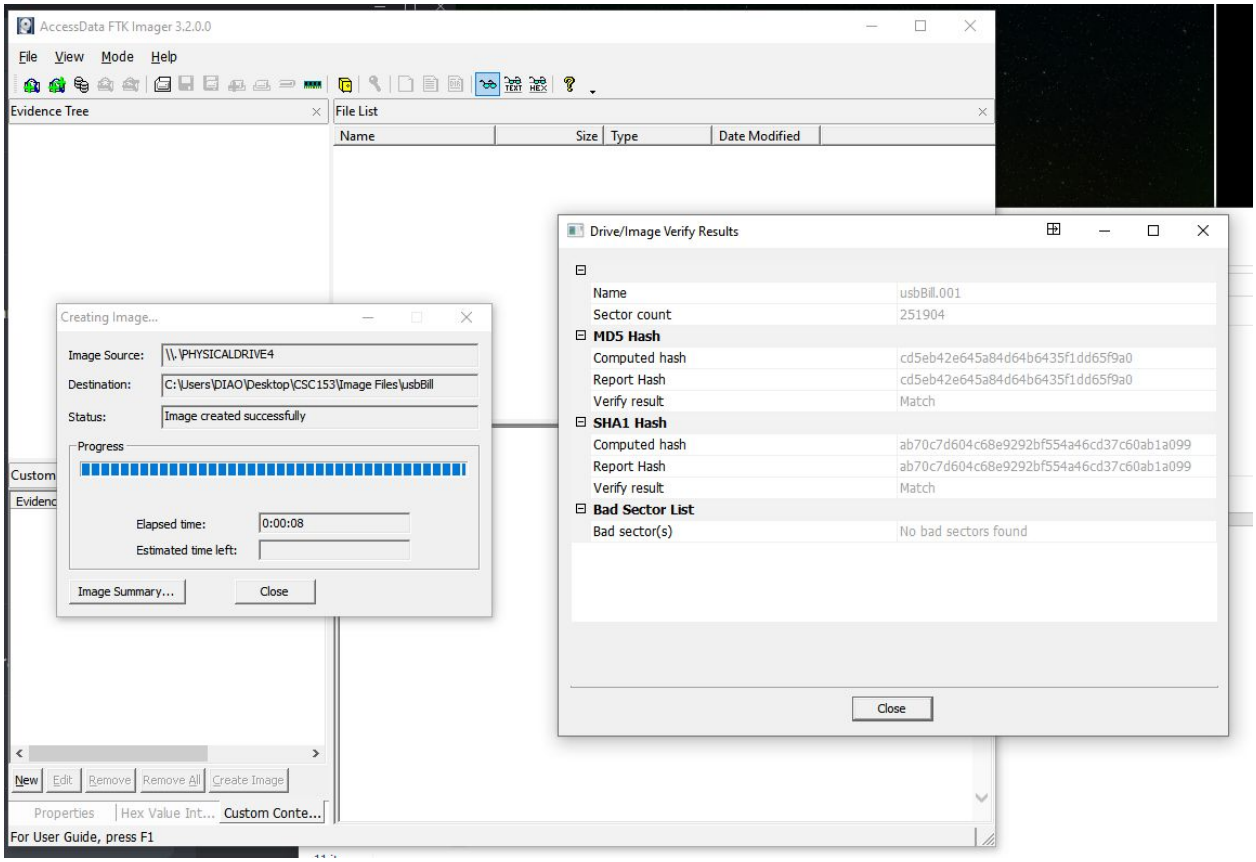
Rongguang Ou
CSC 153 - LAB 2 Report
10/28/19

Report Overview:

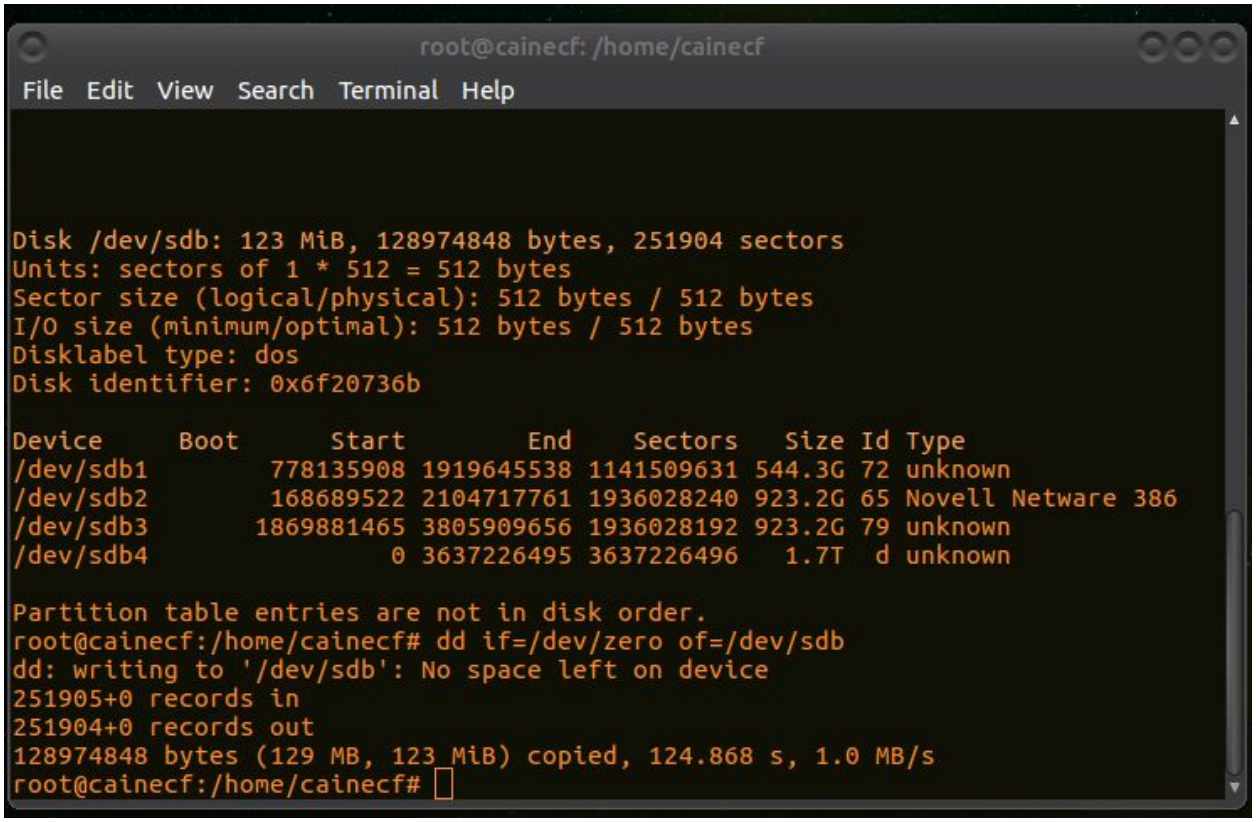
First step I did to investigate is I used FTK Imager to perform data acquisition of the suspect drive and saved the image as a .dd file. I then perform two more data acquisition with linux dd and dcfldd to gather the image of the suspect drive also calculates and verified the hash of the src drive before and after data acquisition, and verified the image's hash matches the src drive hash. I then proceed to use Autospy to load the image I have acquired from previously to see what Autospy can uncover for me. I discovered there is a office file namely "test.docx". I was able to view the content of this document. I also did a keyword search for the word "Warranties" and found that it is in the document named "test.docx". There were no other files uncovered because "test.docx". Same steps were performed for suspect drive number two(zero'd one). However, this time no files were uncovered.

Task 3:
Create Image of the suspect drive

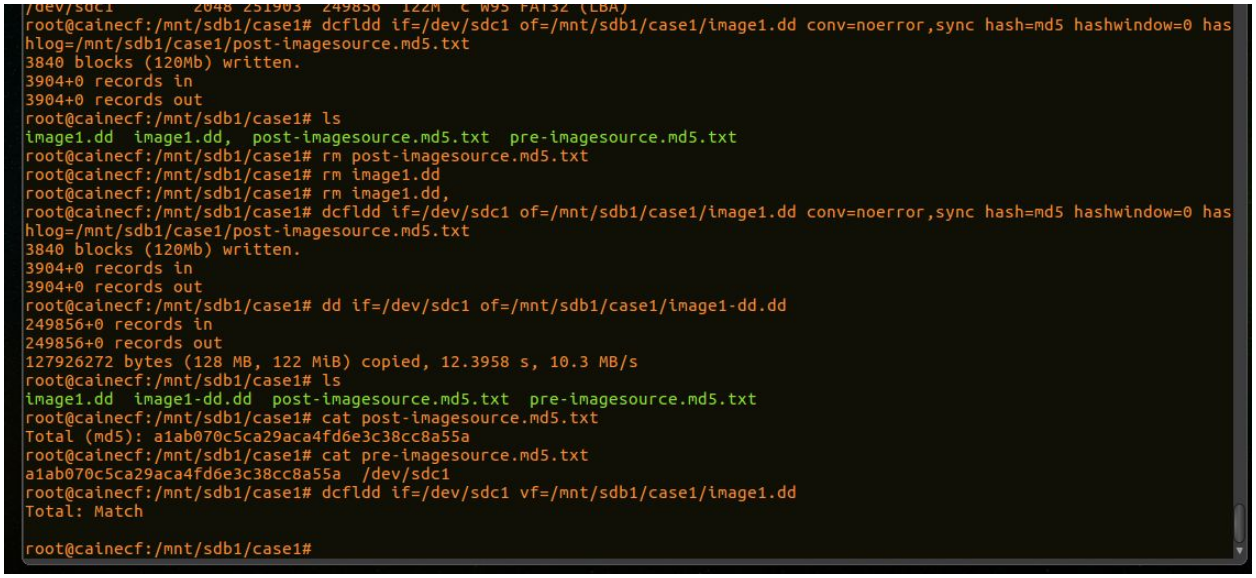


Task 4:

Zero out target drive

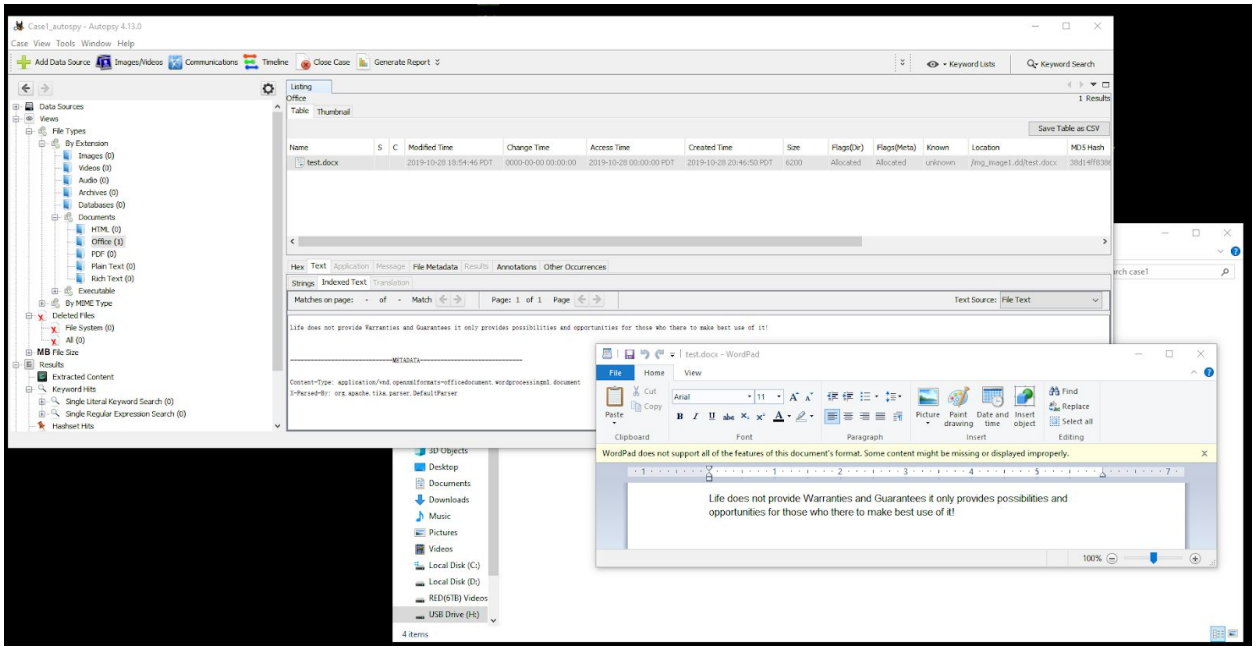


Acquire image using both dcfldd and dd and verified hash after creating image



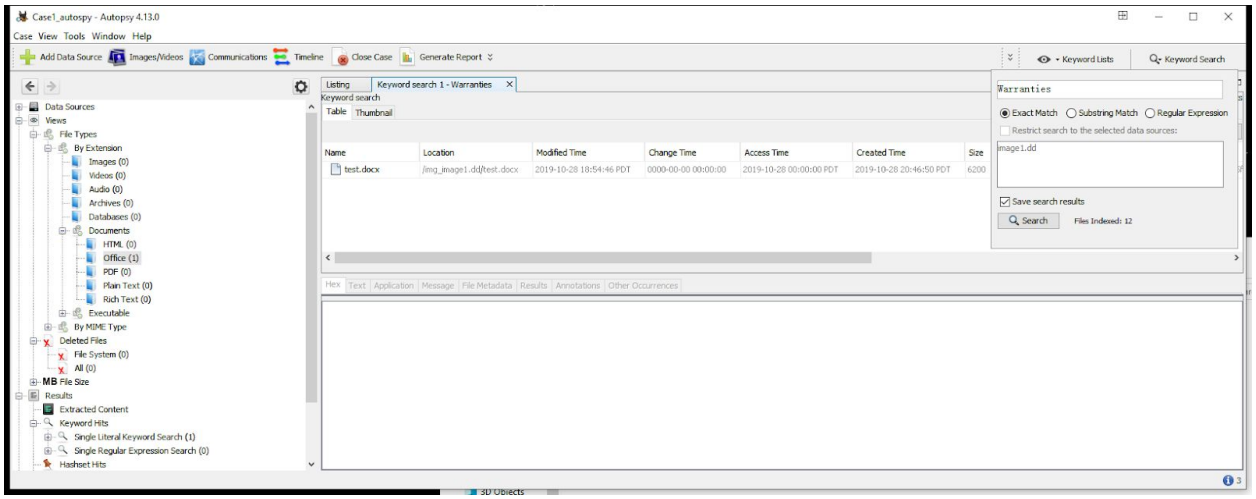
Task 5:

Used autospy to locate any file recovered. In this case, retrieved a test.docx document and was able to open it to see the content.



Task 6:

Keyword search for “Warranties” was able to find doc that contains this keyword.



Task 7 : zeroing out suspect drive before repeating task 4-6

```
Disk /dev/sdc: 123 MiB, 128974848 bytes, 251904 sectors
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: 0x4be940e9

Device     Boot Start    End Sectors  Size Id Type
/dev/sdc1        2048 251903  249856  122M  c W95 FAT32 (LBA)
root@cainecf:/mnt/sdb1# dd if=/dev/zero of=/dev/sdc1
dd: writing to '/dev/sdc1': No space left on device
249857+0 records in
249856+0 records out
127926272 bytes (128 MB, 122 MiB) copied, 117.086 s, 1.1 MB/s
root@cainecf:/mnt/sdb1#
```

Reformat zero'd suspect drive to fat 32

```
root@cainecf:/mnt/sdb1# mkfs.msdos -vF32 /dev/sdc1
mkfs.fat 3.0.28 (2015-05-16)
/dev/sdc1 has 4 heads and 62 sectors per track,
hidden sectors 0x0800;
logical sector size is 512,
using 0xf8 media descriptor, with 249856 sectors;
drive number 0x80;
filesystem has 2 32-bit FATs and 1 sector per cluster.
FAT size is 1922 sectors, and provides 245980 clusters.
There are 32 reserved sectors.
Volume ID is e7ee2e8a, no volume label.
root@cainecf:/mnt/sdb1#
```

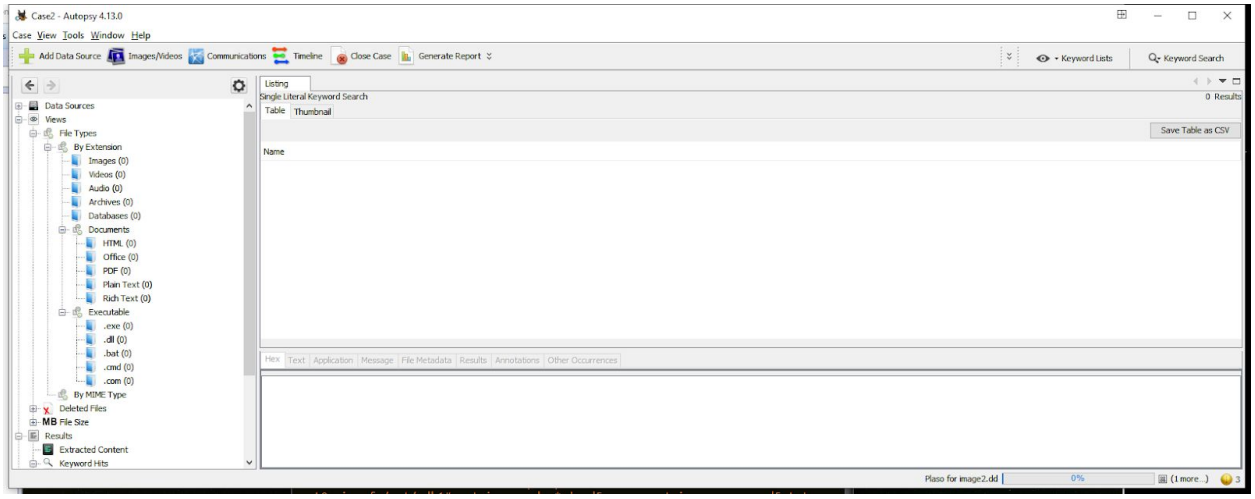
Acquire image using dclfdd and dd for the suspect drive

```
Try 'dcfldd --help' for more information.
root@cainecf:/mnt/sdb1# dcfldd if=/dev/sdc1 of=/mnt/sdb1/case2/image2.dd conv=no
error,sync hash=md5 hashwindow=0 hashlog=/mnt/sdb1/case2/post-imagesource.md5.tx
t
3840 blocks (120Mb) written.
3904+0 records in
3904+0 records out
root@cainecf:/mnt/sdb1# dd if=/dev/sdc1 of=/mnt/sdb1/case2/image2.dd.dd
249856+0 records in
249856+0 records out
127926272 bytes (128 MB, 122 MiB) copied, 11.4774 s, 11.1 MB/s
root@cainecf:/mnt/sdb1#
```

Verified the hash still the same

```
root@cainecf:/mnt/sdb1# dcfldd if=/dev/sdc1 vf=/mnt/sdb1/case2/image2.dd
Total: Match
```

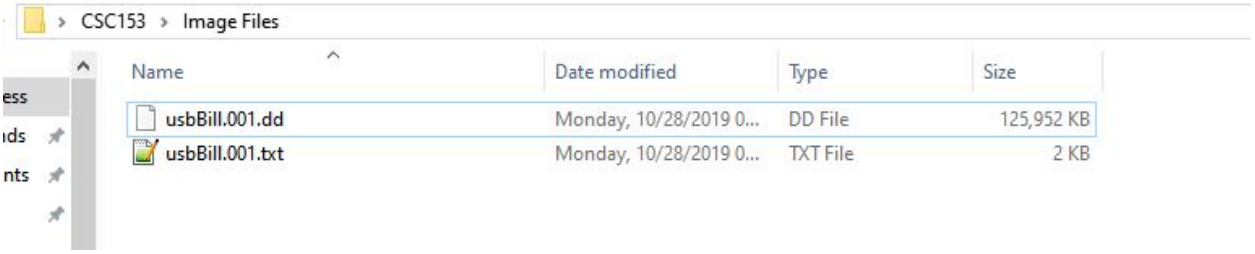
Using autospy , nothing was recovered this time. The search for keyword “Warranties” also fails.



Task 9 :

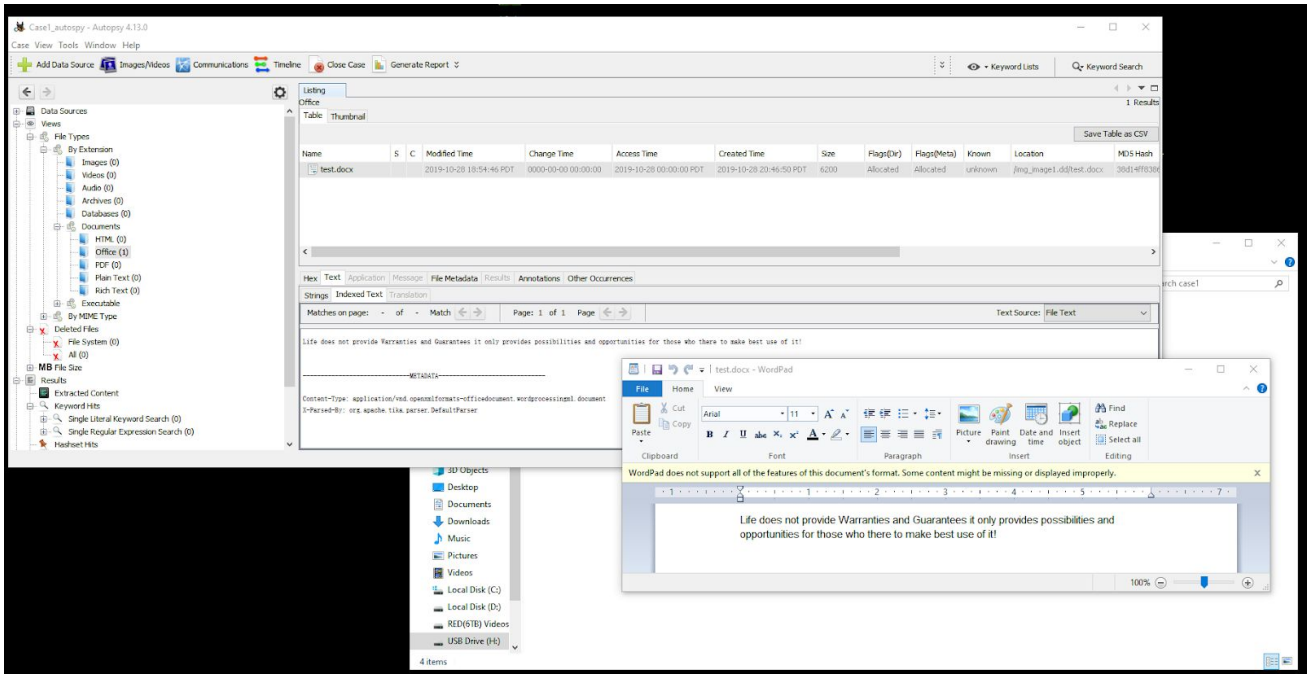
1. In Task 4, the acquired image has an extension of “.dd”. In Task 3, what is the extension for the image file?

Extension generated by FTK imager for the image file is .dd

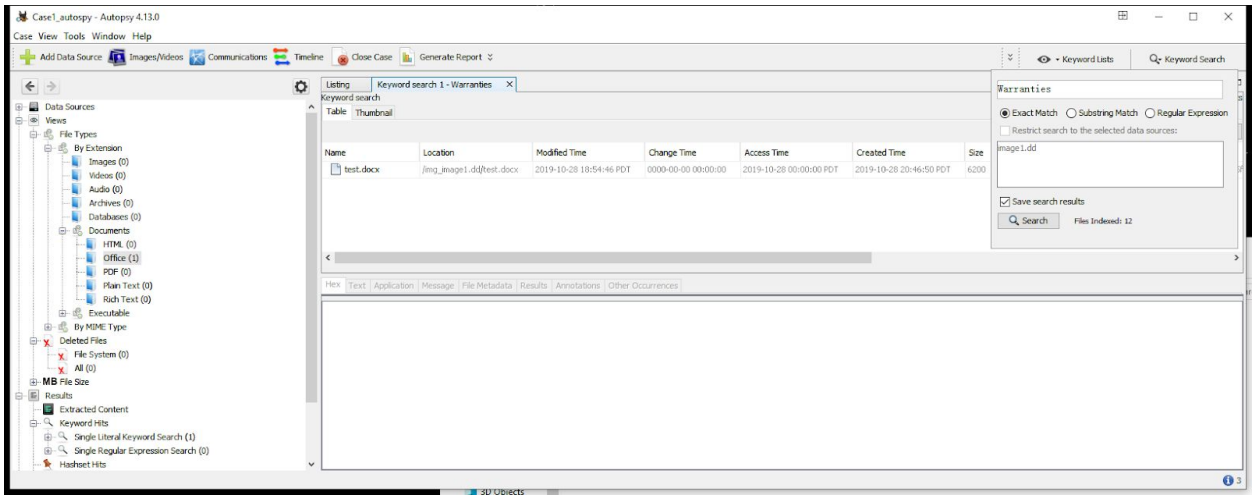


2. In Task 5, how many files are there on the USB drive? What are they? Please attach screenshots to prove your answer.

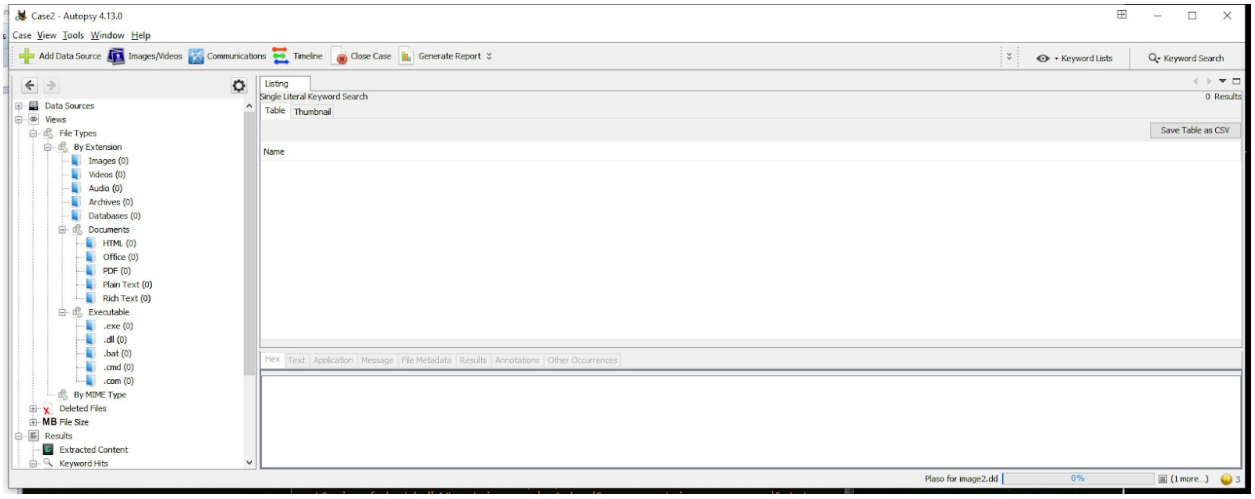
There is only one document file namely “test.docx” is recovered.



3. In Task 5, which file/files are deleted? Please attach screenshots to prove your answer.
There are no deleted files or that the software was not able to pick up any. (SEE ABOVE PICTURE)
4. In Task 6, are you able to find any hit when you search “Warranties” as the key word? In which file is the key word located? Please attach screenshots to prove your answer.
A keyword search of “Warranties” did return with result.

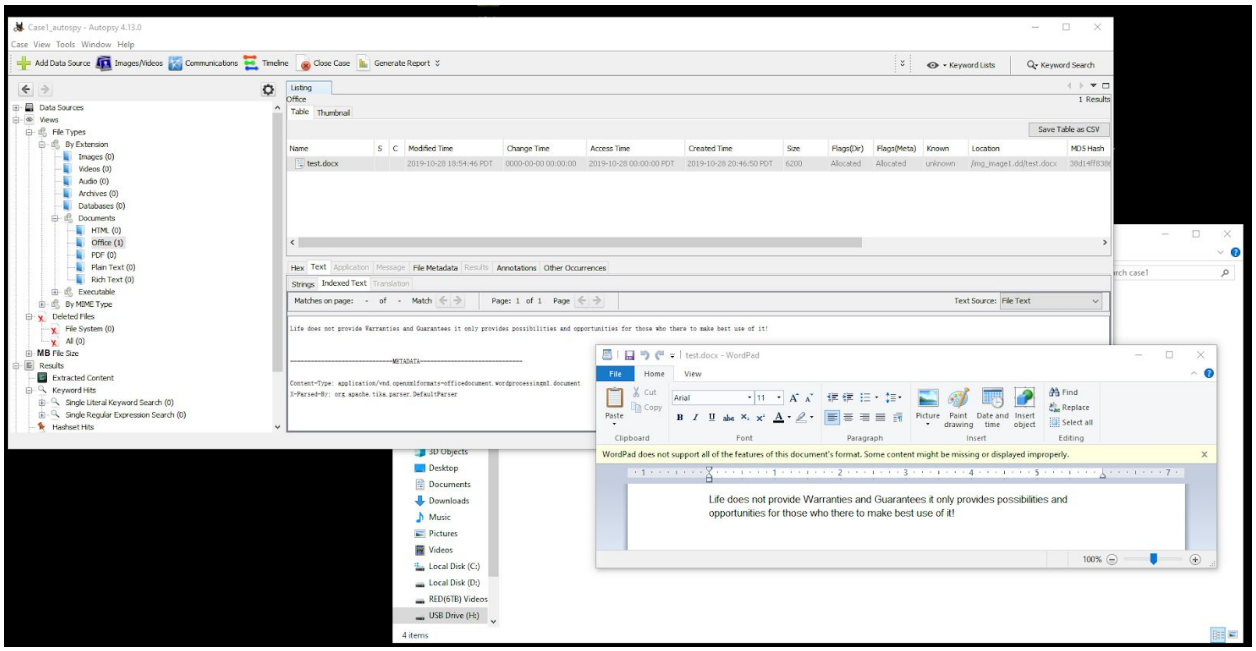


5. In Task 8, how many files are there on the USB drive? What are they? Please attach screenshots to prove your answer.
The zero’d USB drive contains no files.



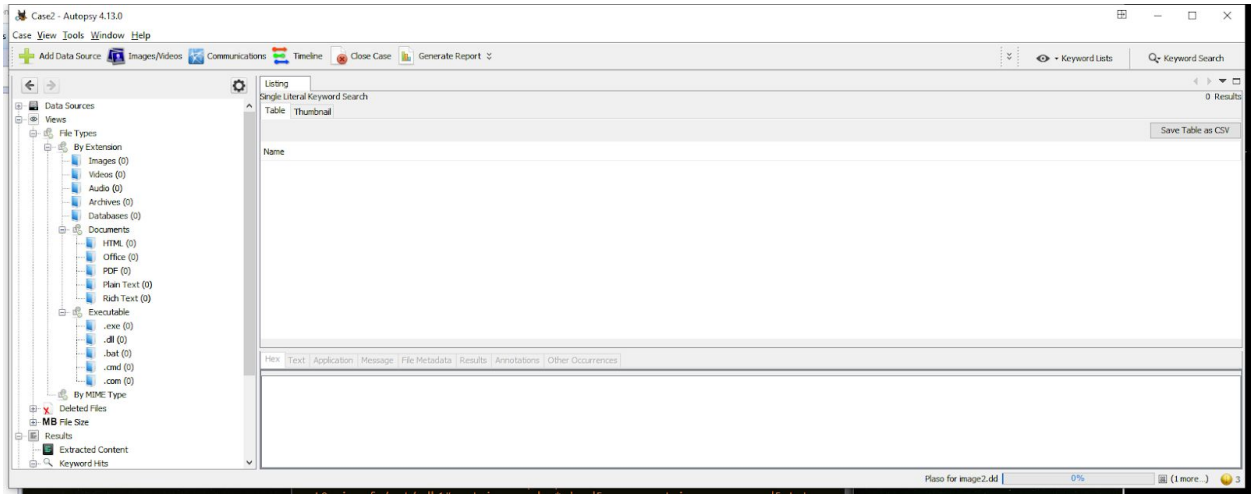
6. In Task 2, you performed a “disk format” operation towards the USB drive. Did this operation completely erase the “test.doc” (or “test.docx”) file in the USB drive? How do you know? Please provide a screenshot to prove your answer.

Perform a disk format operation did not completely erase test.doc. It is only appear to be erased. Autospy was able to recover this file.



7. In Task 7, you performed a “zero out” operation towards the USB drive. Did this operation completely erase the “test.doc” (or “test.docx”) file in the USB drive? How do you know? Please provide a screenshot to prove your answer.

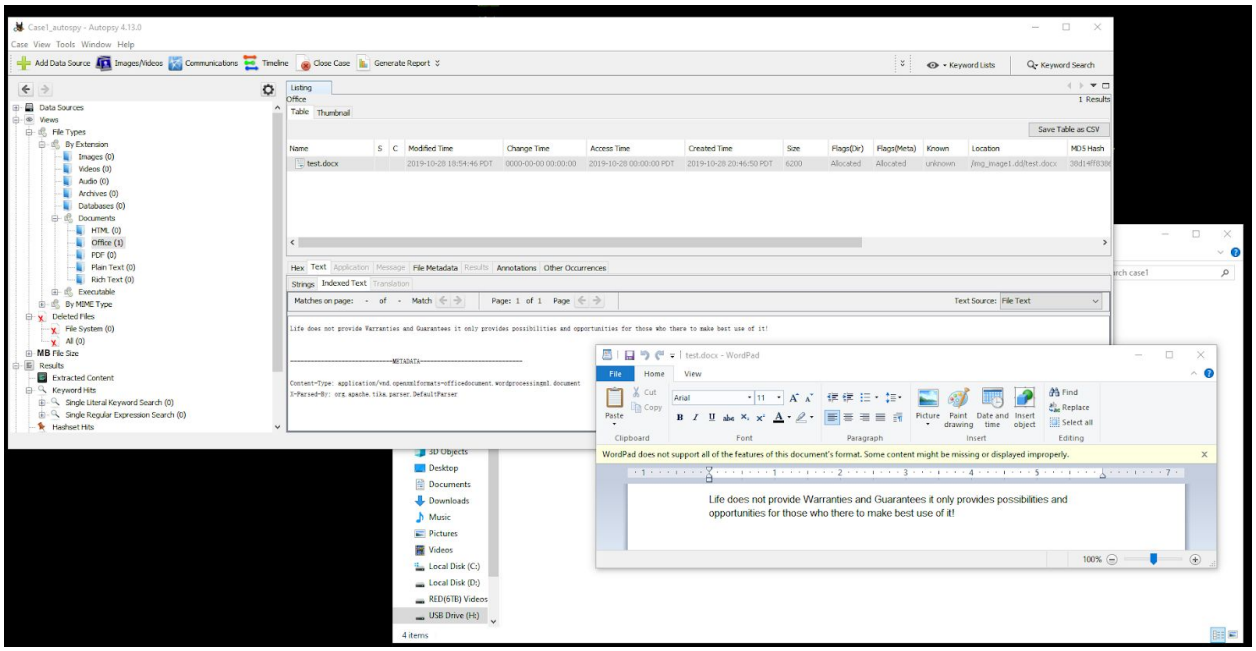
Zero out operation completely erase test.docx because it writing zero bit by bit to the entire drive and so any unallocated area would have been wiped. In this case even autospy should not able to recover this file.



8. Did have any surprise in Task 5? Did you see any other files other than “test.doc” or “test.docx”?

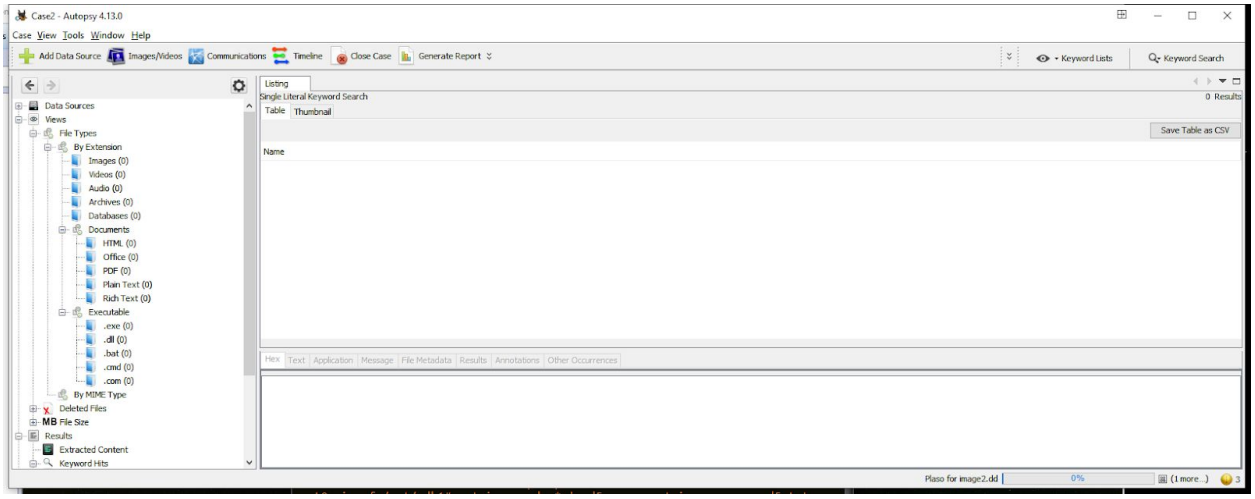
Please provide a screenshot to prove your answer.

I am not surprised to see test.docx appear again due to knowing what happened behind the scenes. There are no other files other than “test.docx”.



9. In Task 8, did you see any other files other than “test.doc” or “test.docx”? Please provide a screenshot to prove your answer.

I do not see any files for the zero’d drive. This is also expected that it will truly wipe out everything.



10. To summarize the questions above, what are the difference between disk formatting in Windows and the zero-out operation?

Disk formatting does not completely erase data stored on the drive. Zero-out operation will completely wipe out the entire drive leaving no way to recover it back.