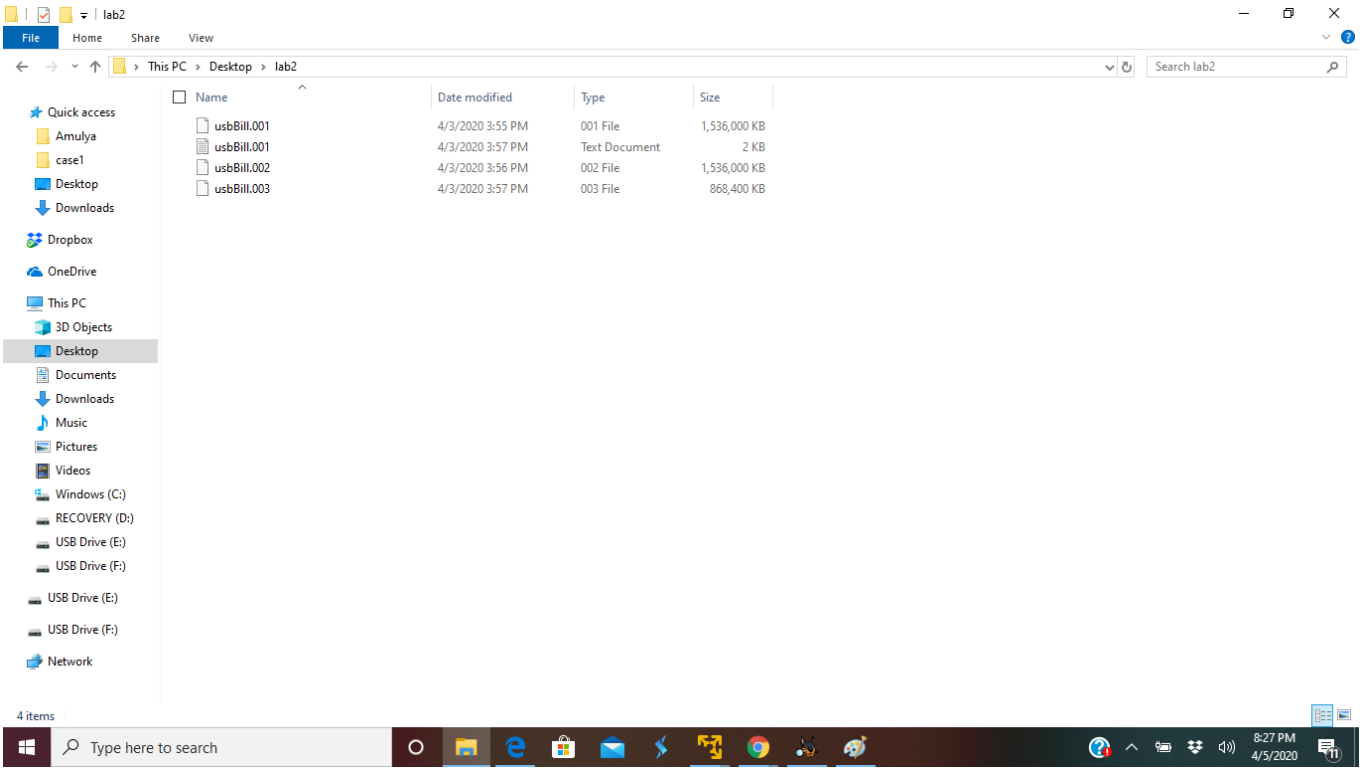
Lab 2

Name : Jaya Sahithi Aravapalli.

Task 9 Answer the Question

1)

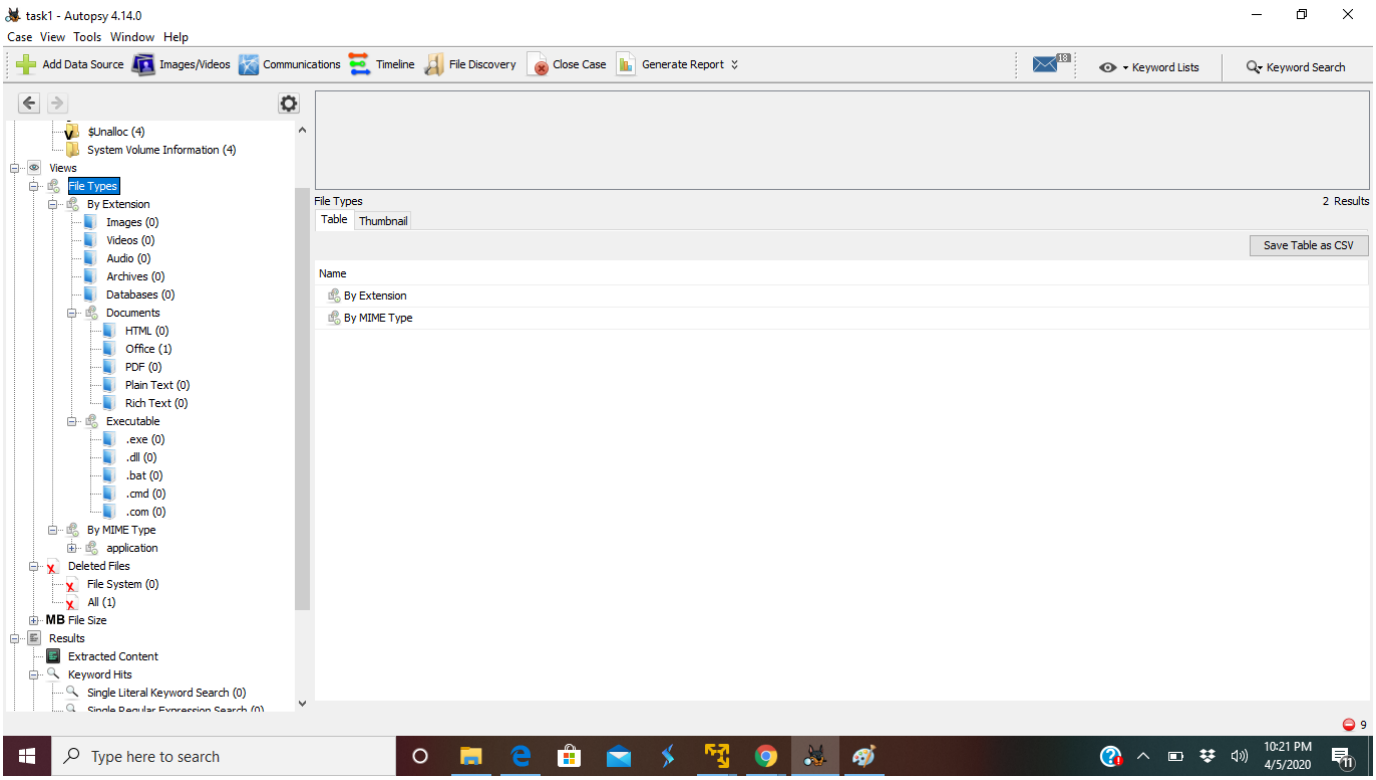
The extension is .001



2)

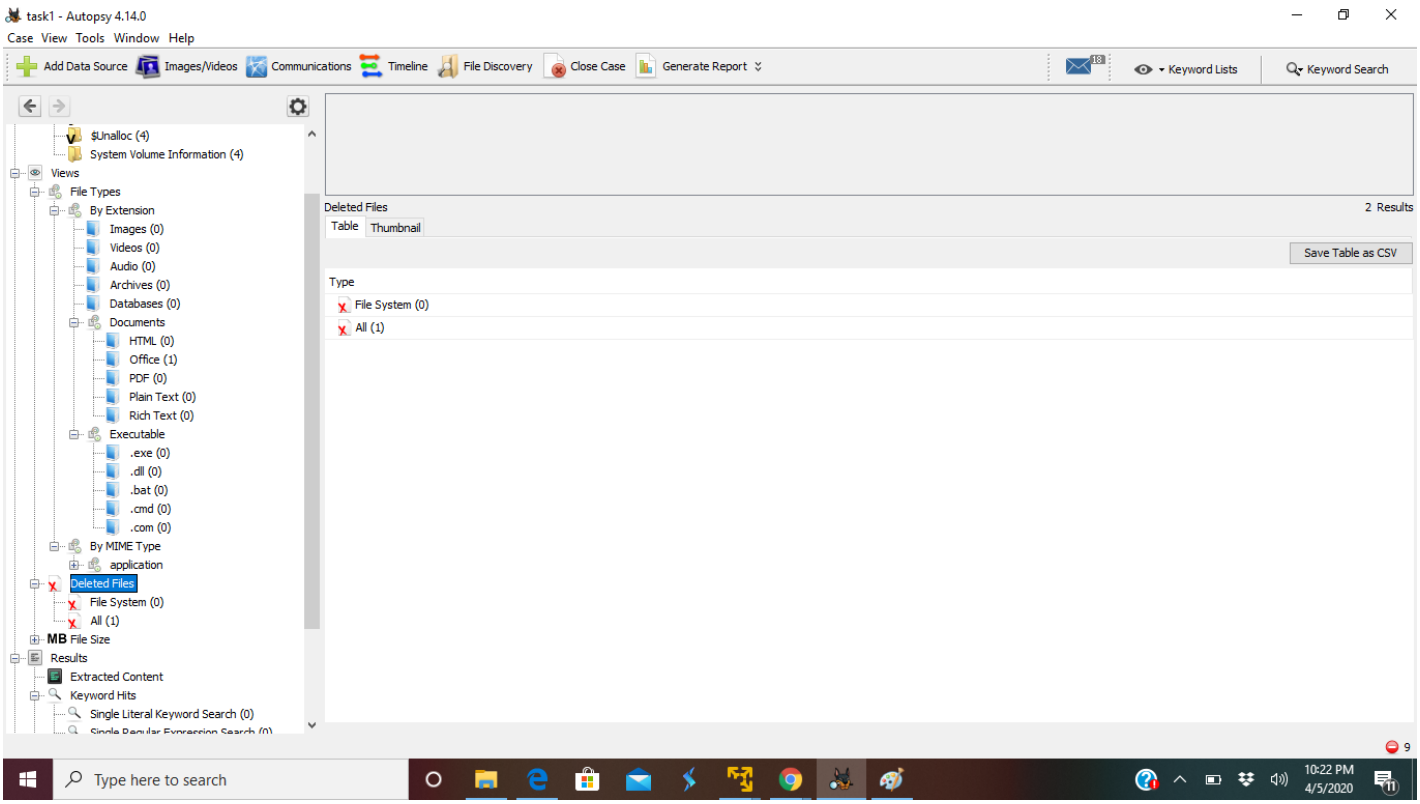
There is only one file because it’s a new pen drive.

The file I have in my USB Drive test.doc.



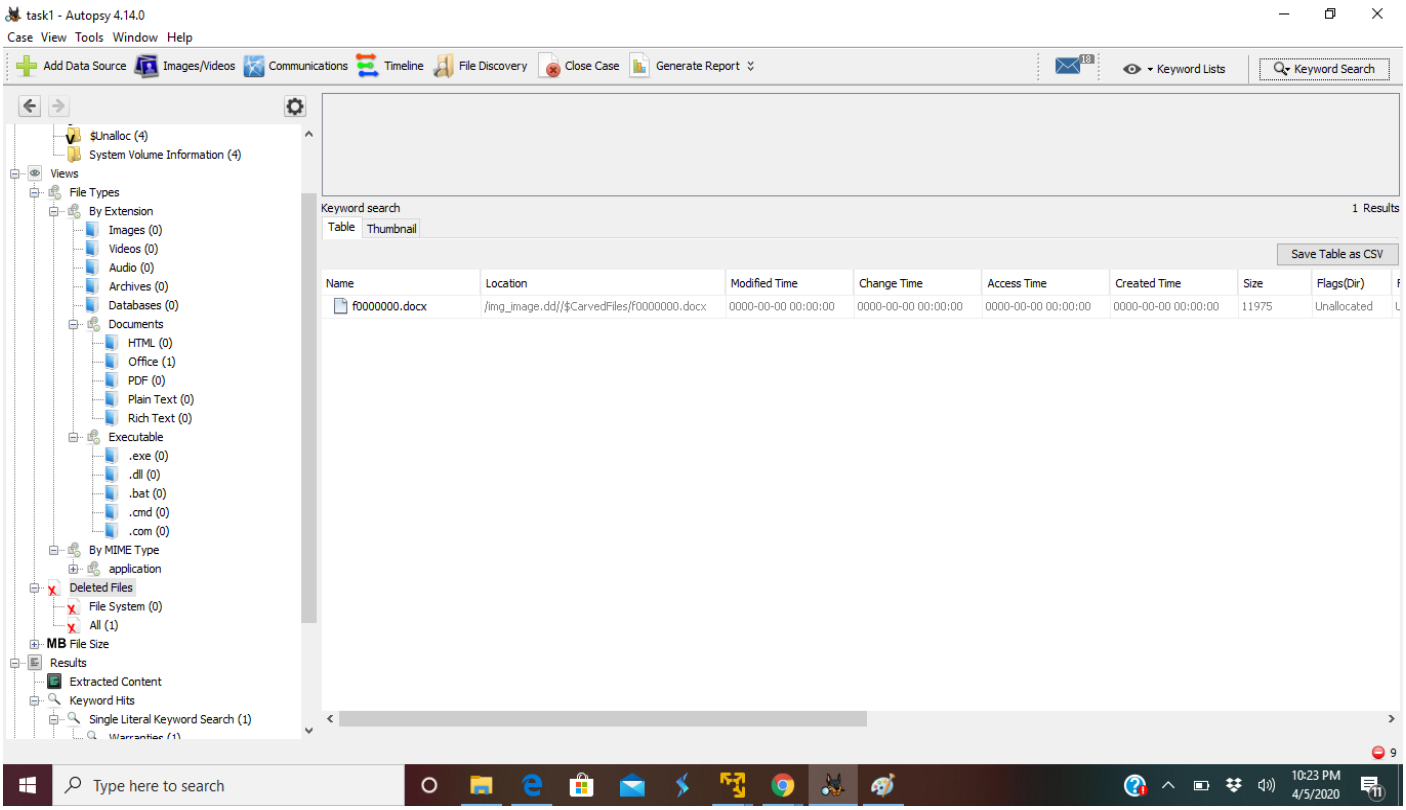
3)

The deleted file is test.doc .



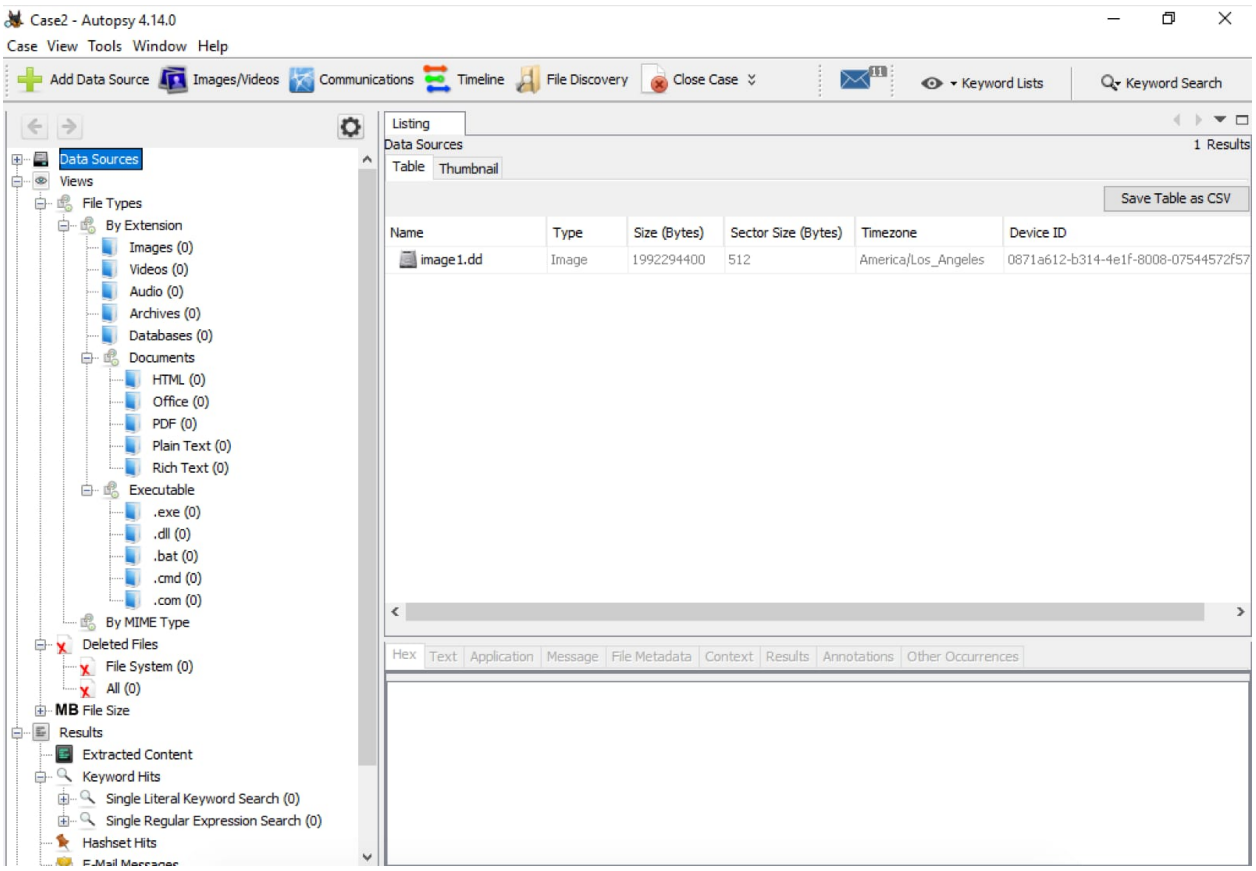
4)

When I searched the key wound I found it in the file f0000000.docx.



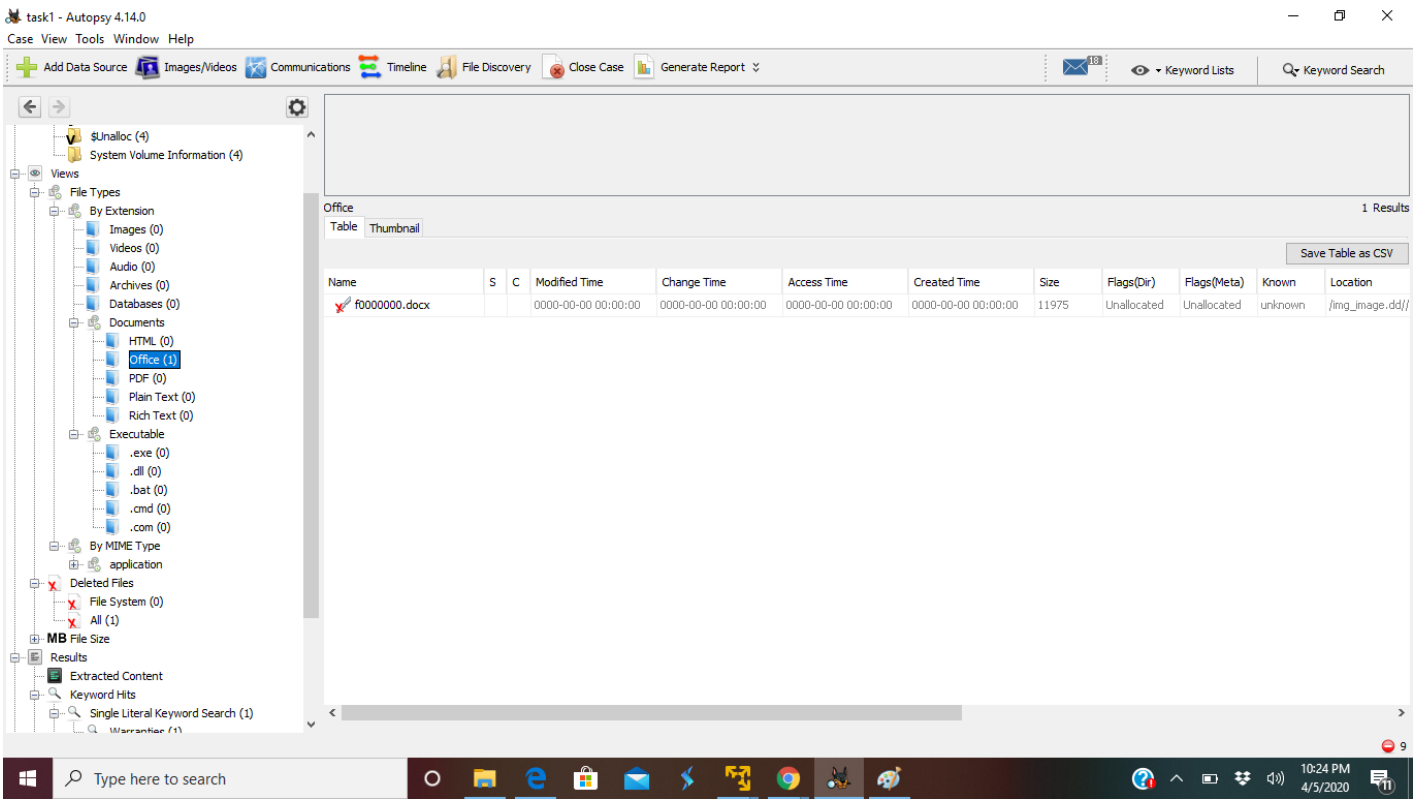
5)

There are no files after zero out.



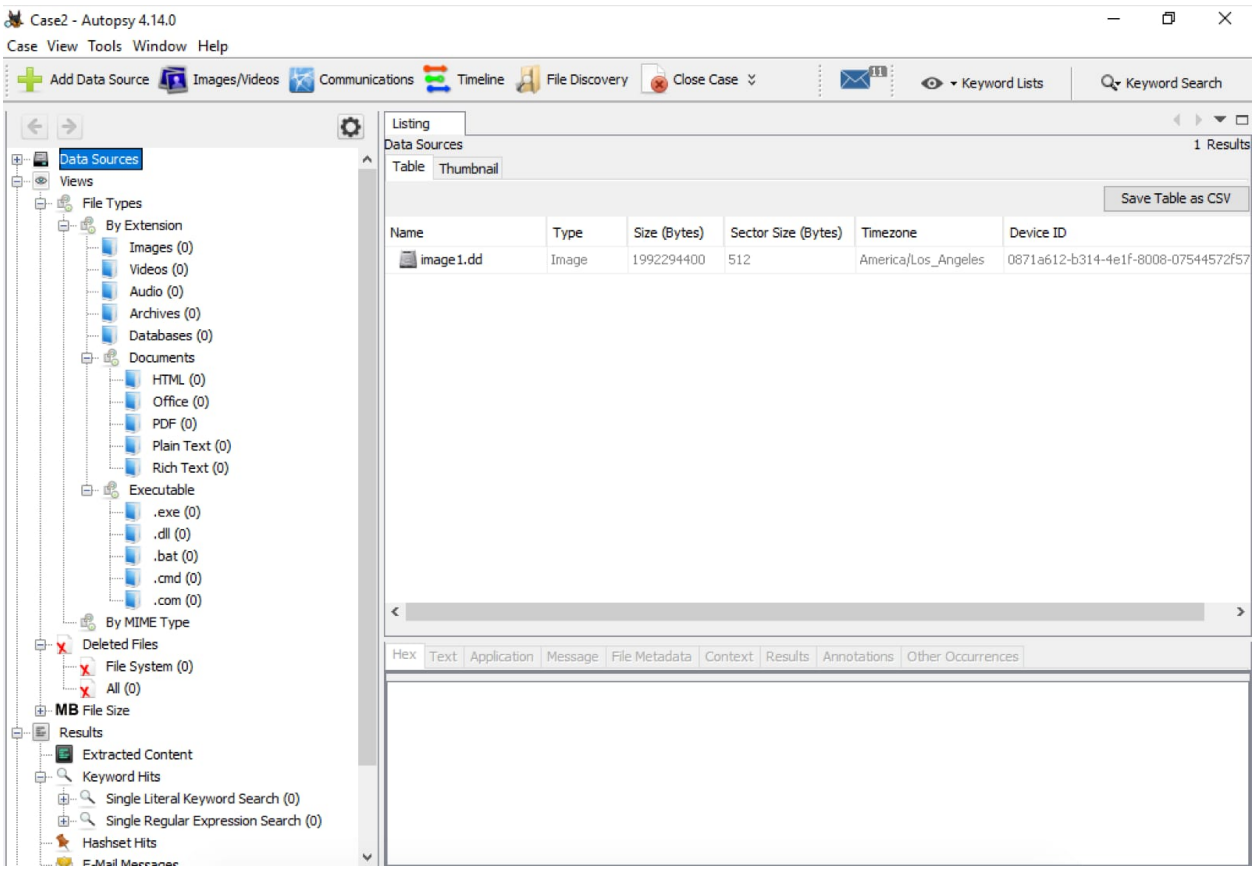
6)

This task does not completely erase the USB drive. It still shows the file in deleted files.



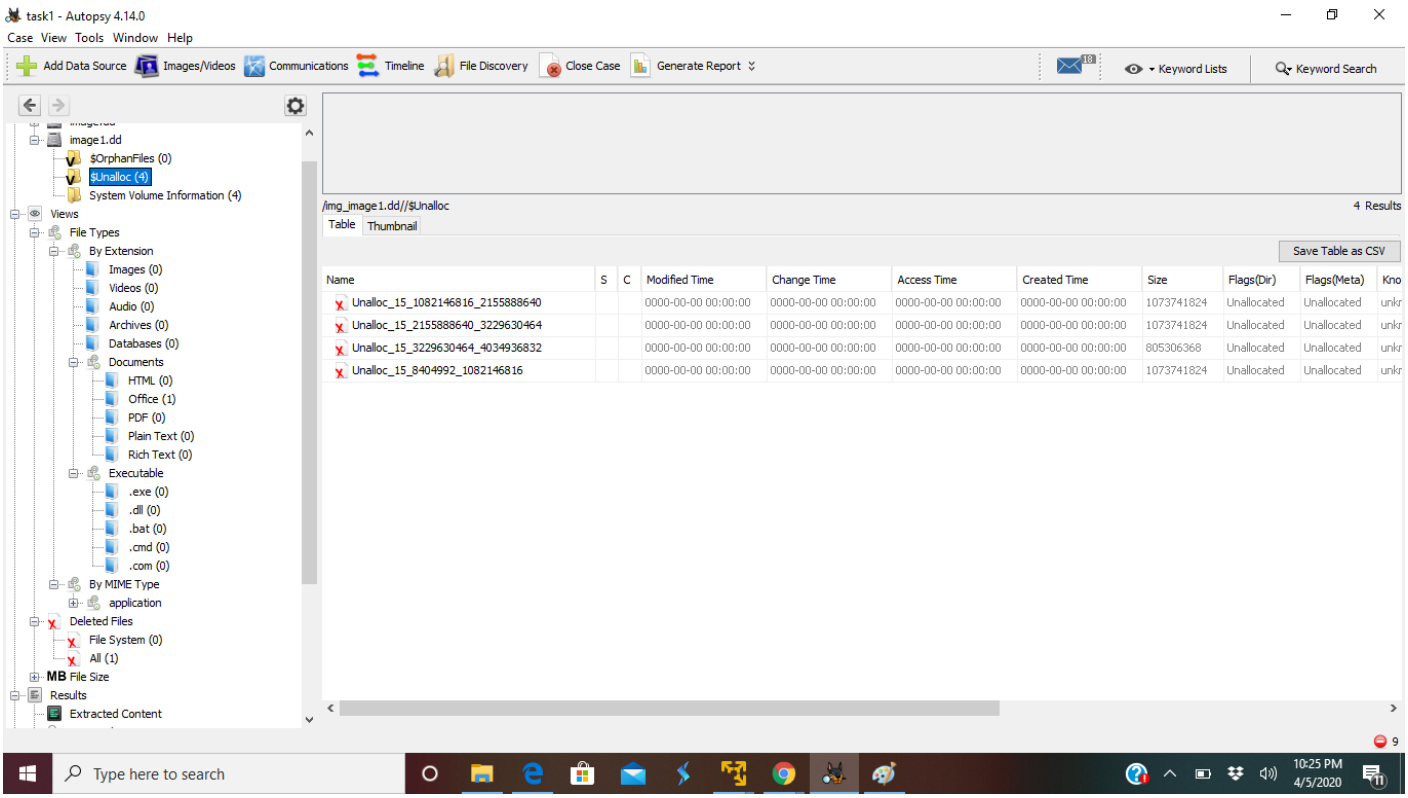
7)

Yes, this task has completely erased test.doc. The provided screenshot below proves this.



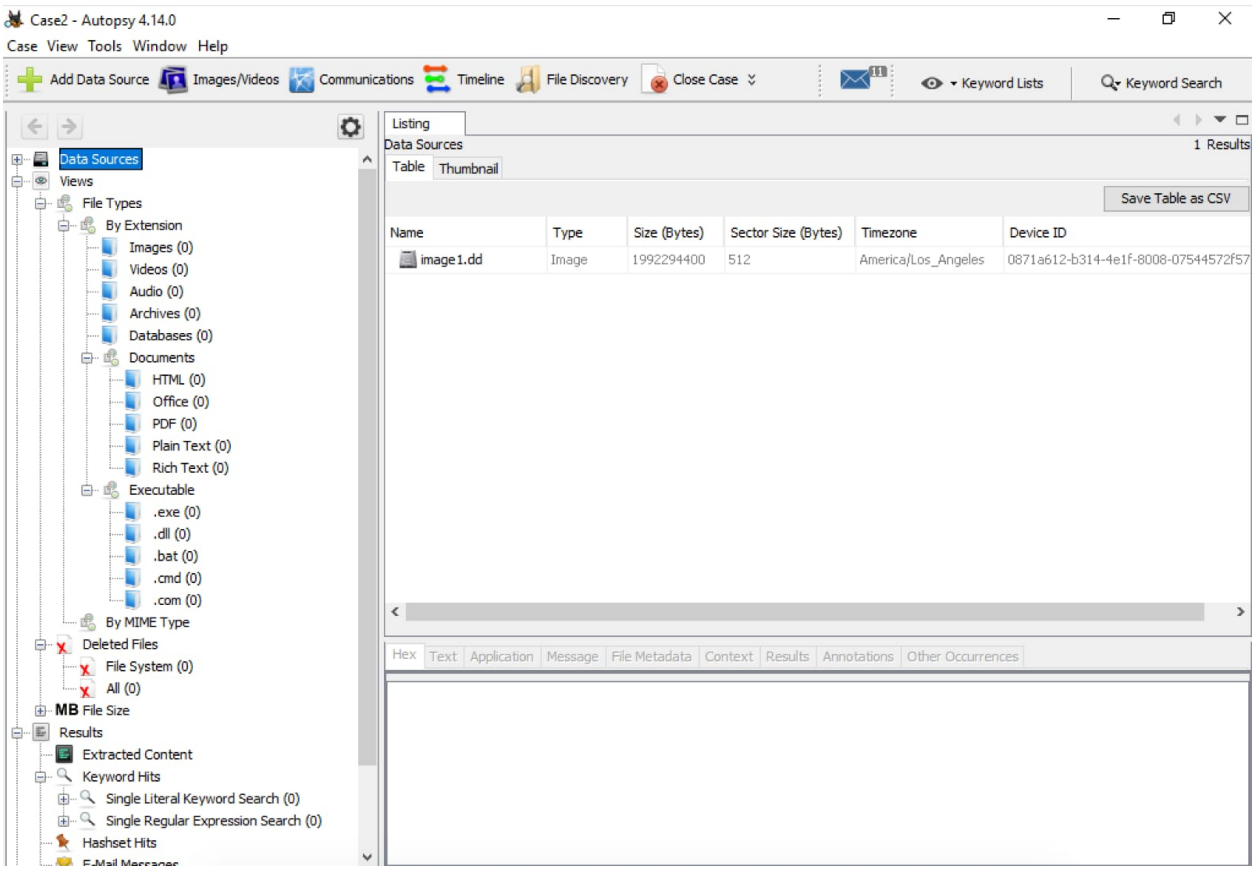
8)

I was surprised to find few unallocated files in the new pen drive.



9)

I couldn’t find any file after zero out.



10)

After preforming the disk format the USB drive is not completely erased and we can find the files in deleted files.

But after performing the zero out all the files in USB drive are completely erased.

Forensic Report

- At first I have downloaded and installed FTK imager and Autopsy windows version.
- Then, I have taken 2 USB drives of size 4 GB and 8 GB. I made the 4Gb memory pen drive as my suspect drive and the 8GB one as my target drive. And created a test.doc file with text "Life does not provide Warranties and Guarantees it only provides possibilities and opportunities for those who there to make best use of it!"
- Later I have performed a disk format for the USB drive.
- In task 3 with the image I have performed a data acquisition by using FTK Imager.
- In task 4 I have performed a data acquisition in CAINE virtual machine.
- After finishing the data acquisition in task 4 I got a image.dd file my USB drive.

- In task 5 I have analyzed the acquired data by using Autopsy.
- I have created my first case and then added my source data which is the image.dd.
- Then I could see all the files including deleted files present in my USB drive.
- I have performed a dirty word search by taking warranties as my keywork and searched it.
- Then I could see a file where the keyword is present.
- At last I have performed zero out on my USB drive.