

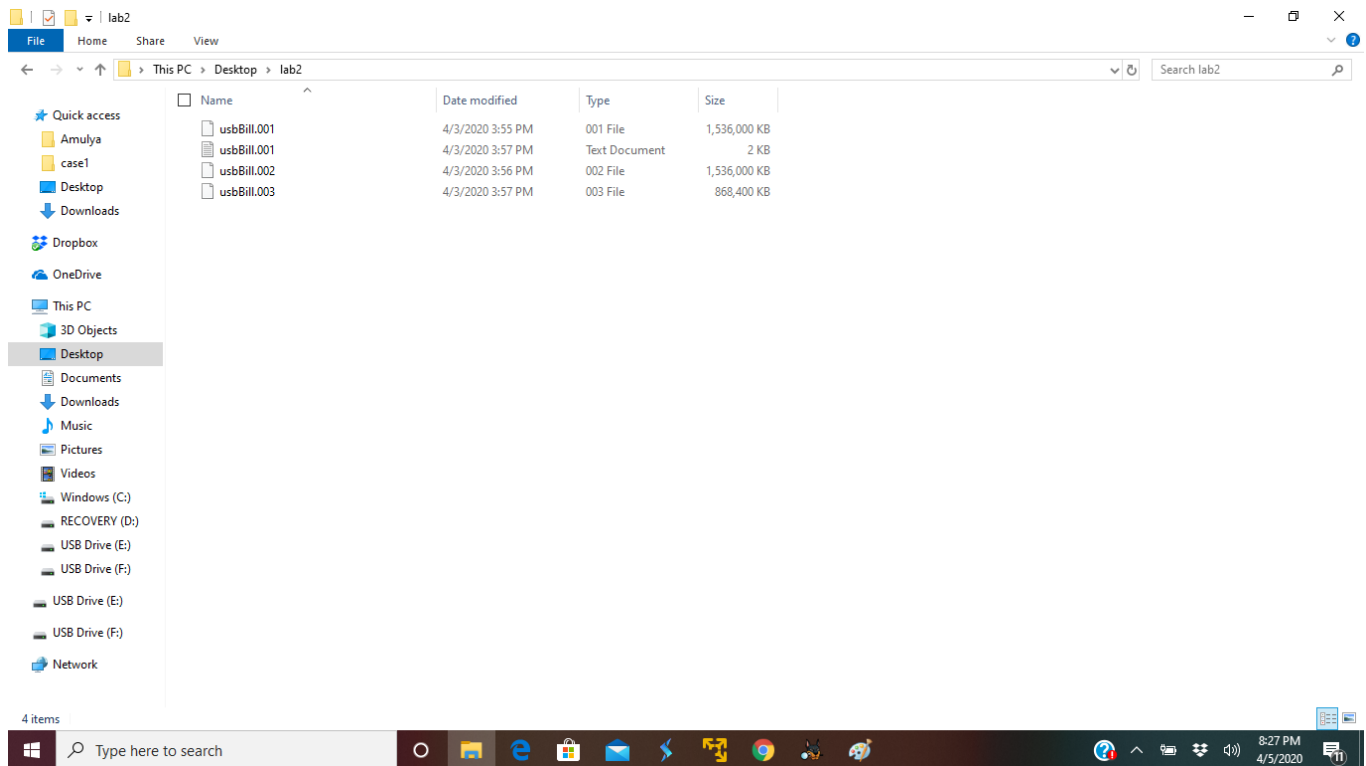
Lab 2

Name : Jaya Sahithi Aravapalli.

Task 9 Answer the Question

1)

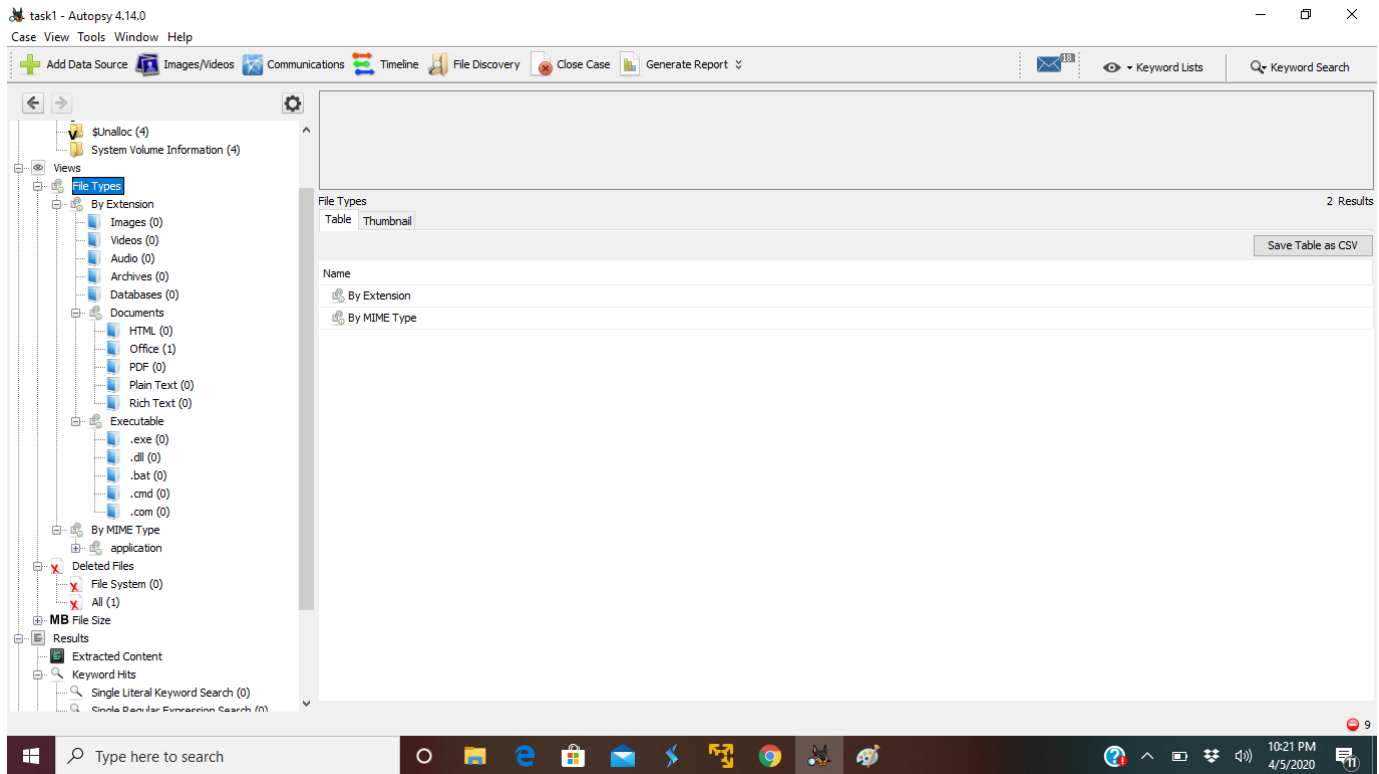
The extension is .001



2)

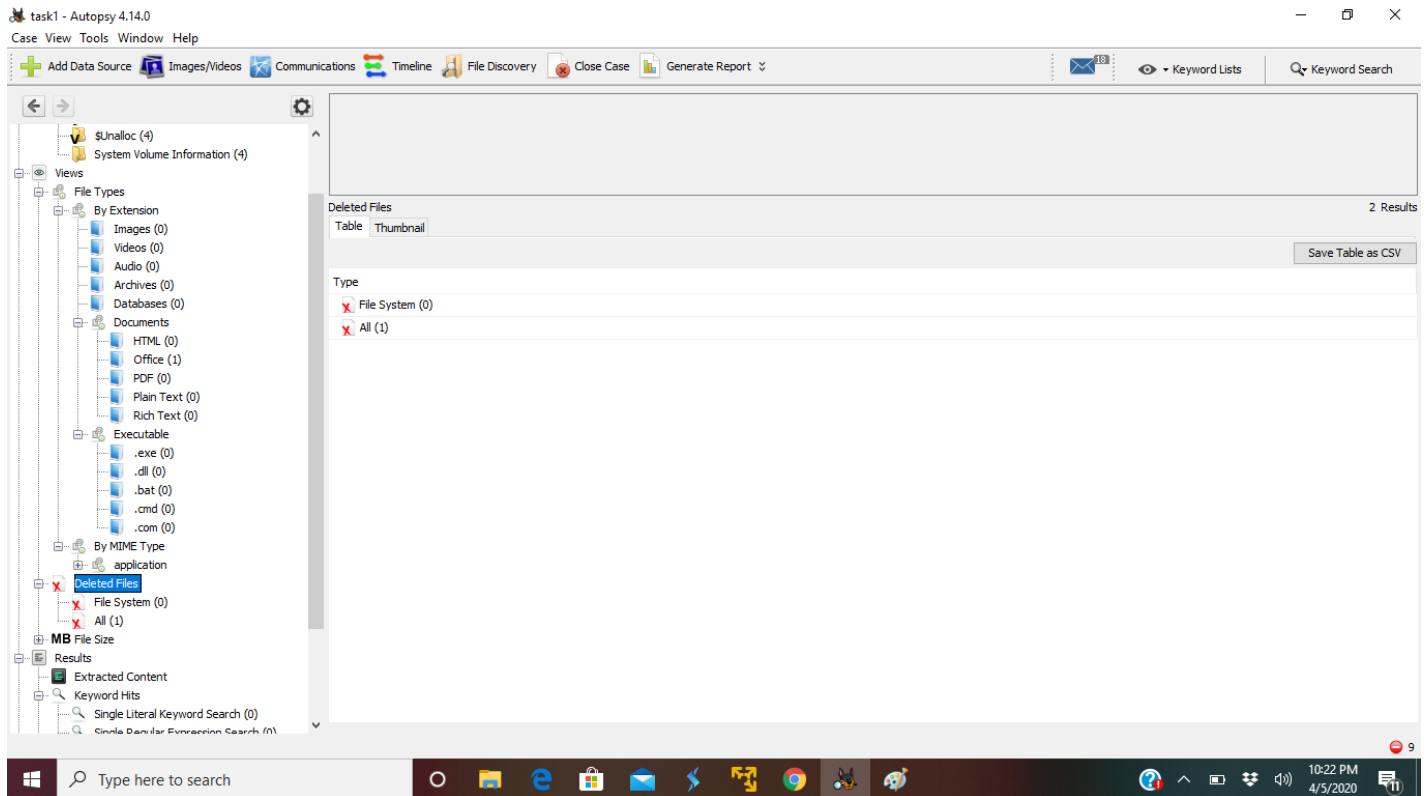
There is only one file because it's a new pen drive.

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



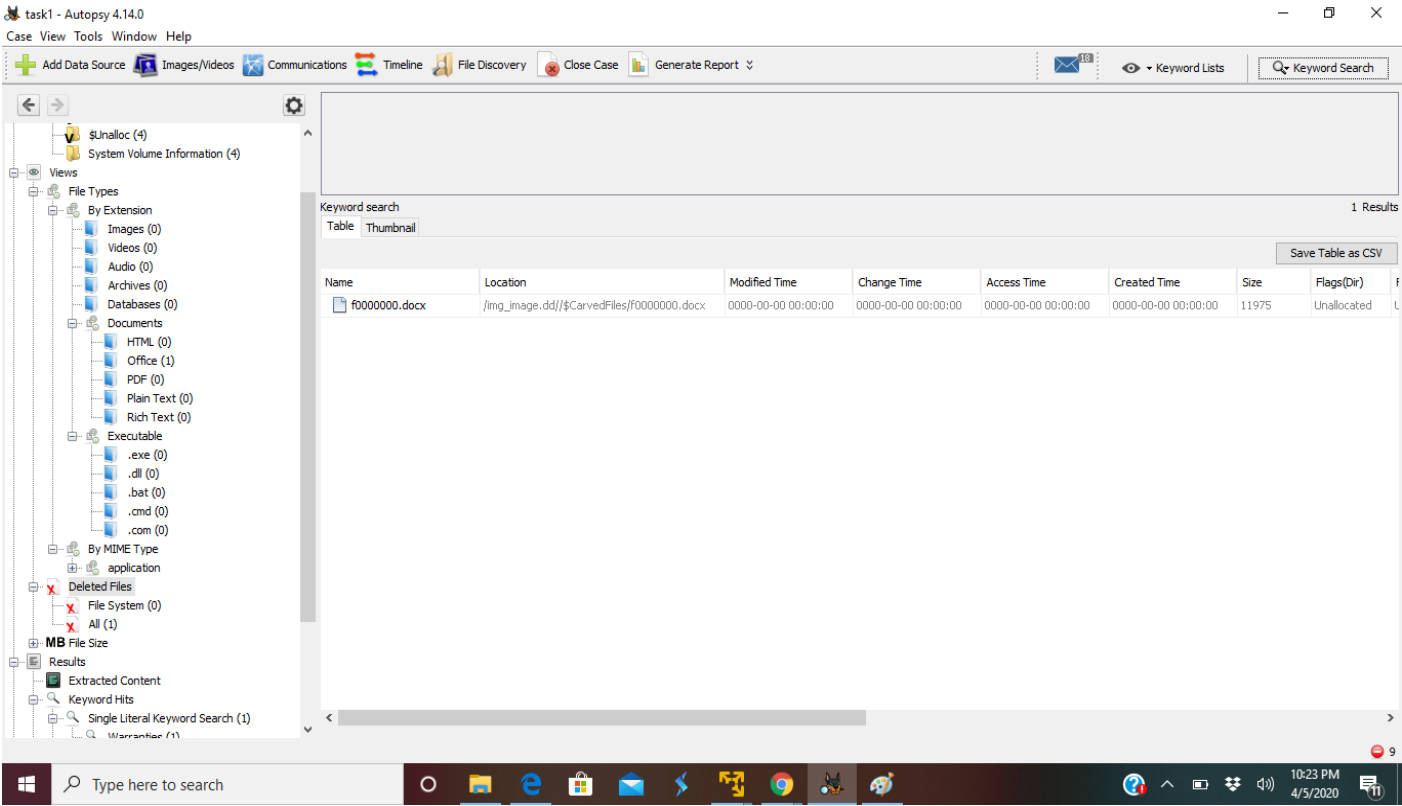
3)

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.

Case2 - Autopsy 4.14.0

Case View Tools Window Help

+ Add Data Source Images/Videos Communications Timeline File Discovery Close Case

Keyword Lists Keyword Search

Listing Data Sources 1 Results

Table Thumbnail Save Table as CSV

Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID
image1.dd	Image	1992294400	512	America/Los_Angeles	0871a612-b314-4e1f-8008-07544572f57

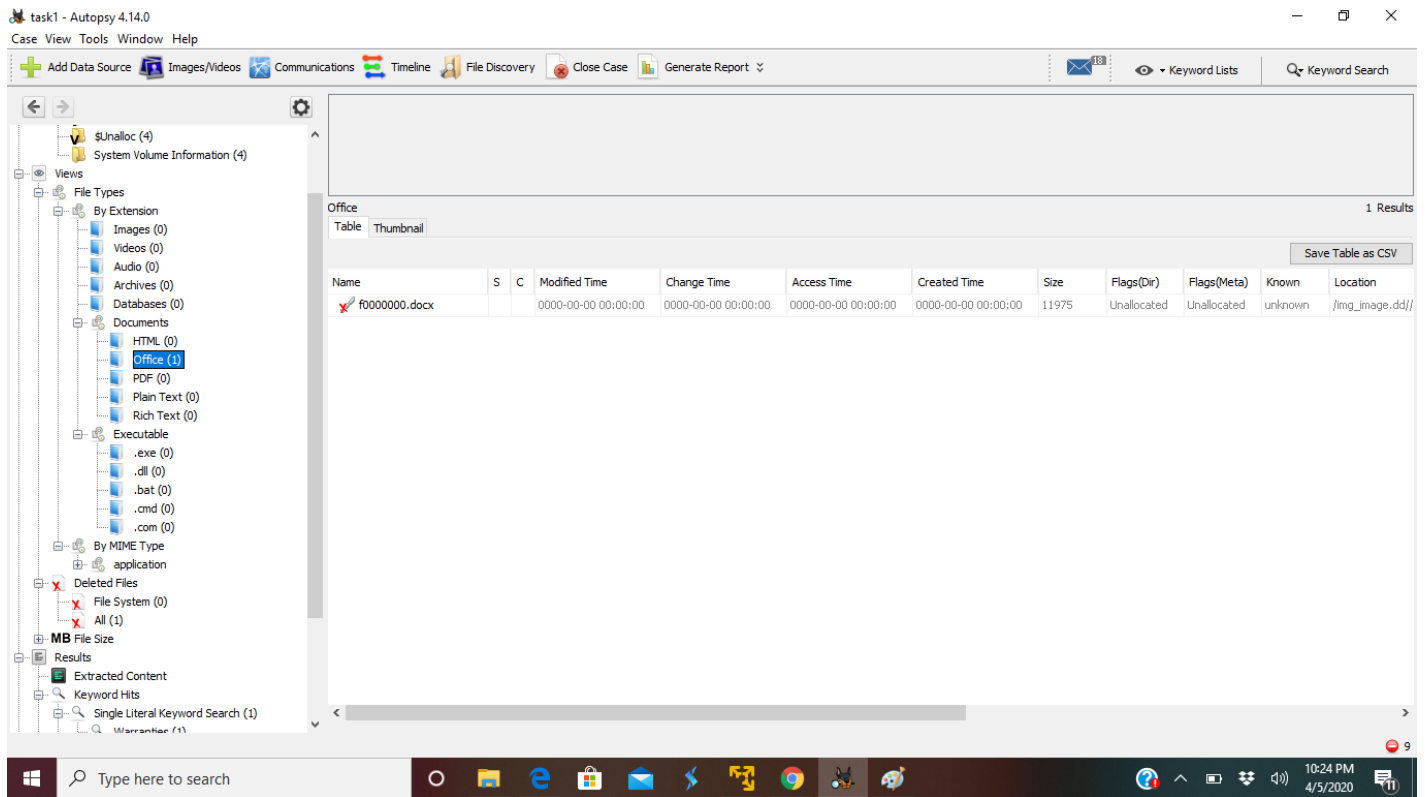
Hex Text Application Message File Metadata Context Results Annotations Other Occurrences

File Types

- By Extension
 - Images (0)
 - Videos (0)
 - Audio (0)
 - Archives (0)
 - Databases (0)
 - Documents
 - HTML (0)
 - Office (0)
 - PDF (0)
 - Plain Text (0)
 - Rich Text (0)
 - Executable
 - .exe (0)
 - .dll (0)
 - .bat (0)
 - .cmd (0)
 - .com (0)
- By MIME Type
- Deleted Files
 - File System (0)
 - All (0)
- MB File Size
- Results
 - Extracted Content
 - Keyword Hits
 - Single Literal Keyword Search (0)
 - Single Regular Expression Search (0)
 - Hashset Hits
 - E-Mail Messages

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.

Case2 - Autopsy 4.14.0

Case View Tools Window Help

+ Add Data Source Images/Videos Communications Timeline File Discovery Close Case

Keyword Lists Keyword Search

Listing Data Sources 1 Results

Table Thumbnail Save Table as CSV

Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID
image1.dd	Image	1992294400	512	America/Los_Angeles	0871a612-b314-4e1f-8008-07544572f57

Hex Text Application Message File Metadata Context Results Annotations Other Occurrences

8)

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

task1 - Autopsy 4.14.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Timeline File Discovery Close Case Generate Report

image1.dd
\$OrphanFiles (0)
\$Unalloc (4)
System Volume Information (4)

Views

File Types

- By Extension
 - Images (0)
 - Videos (0)
 - Audio (0)
 - Archives (0)
 - Databases (0)
 - Documents
 - HTML (0)
 - Office (1)
 - PDF (0)
 - Plain Text (0)
 - Rich Text (0)
 - Executable
 - .exe (0)
 - .dll (0)
 - .bat (0)
 - .cmd (0)
 - .com (0)
- By MIME Type
 - application
- Deleted Files
 - File System (0)
 - All (1)
- MB File Size
- Results
 - Extracted Content

/img_image1.dd/\$Unalloc 4 Results

Table Thumbnail

Save Table as CSV

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Kno
Unalloc_15_1082146816_2155888640			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1073741824	Unallocated	Unallocated	unkr
Unalloc_15_2155888640_3229630464			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1073741824	Unallocated	Unallocated	unkr
Unalloc_15_3229630464_4034936832			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	805306368	Unallocated	Unallocated	unkr
Unalloc_15_8404992_1082146816			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1073741824	Unallocated	Unallocated	unkr

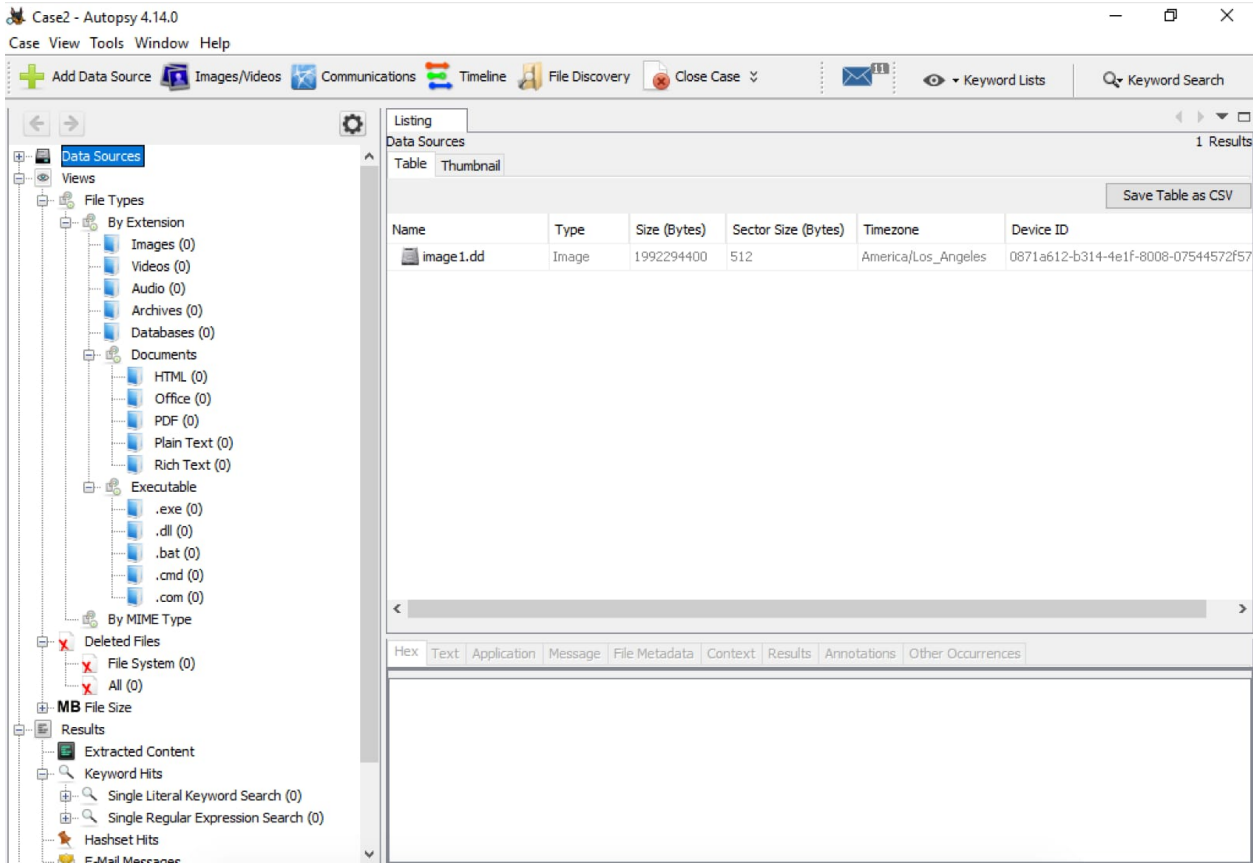
9

Type here to search

10:25 PM 4/5/2020

9)

I couldn't find any file after zero out.



10)

After performing 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 keyword 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.