**DIGITAL FORENSICS LAB**

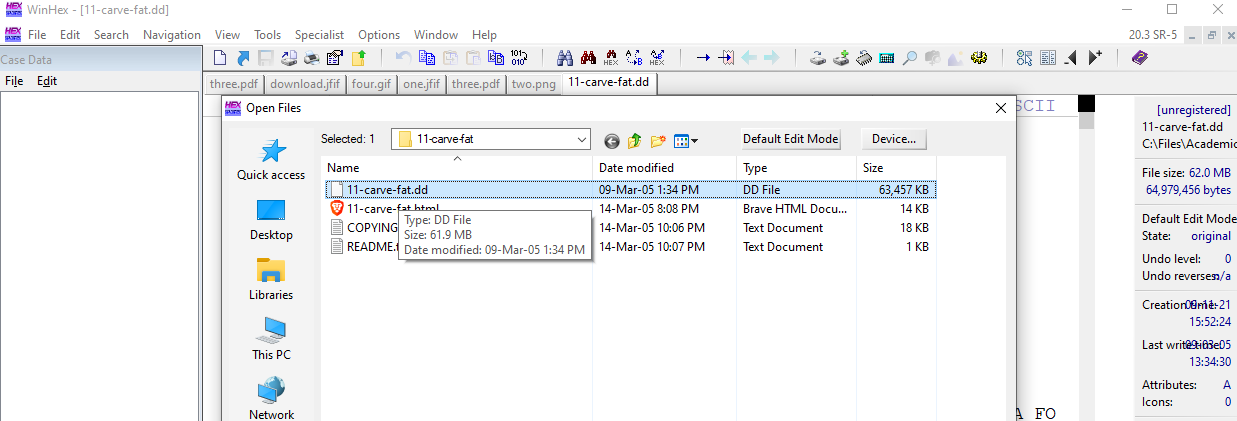
|  |  |
| --- | --- |
| Exercise 11 | |
| Name | S Shyam Sundaram |
| Registration Number | 19BCE1560 |
| Slot | L39+L40 |
| Faculty | Dr. Seshu Babu Pulagara |
| Date | 9th November, 2021 |

**AIM**

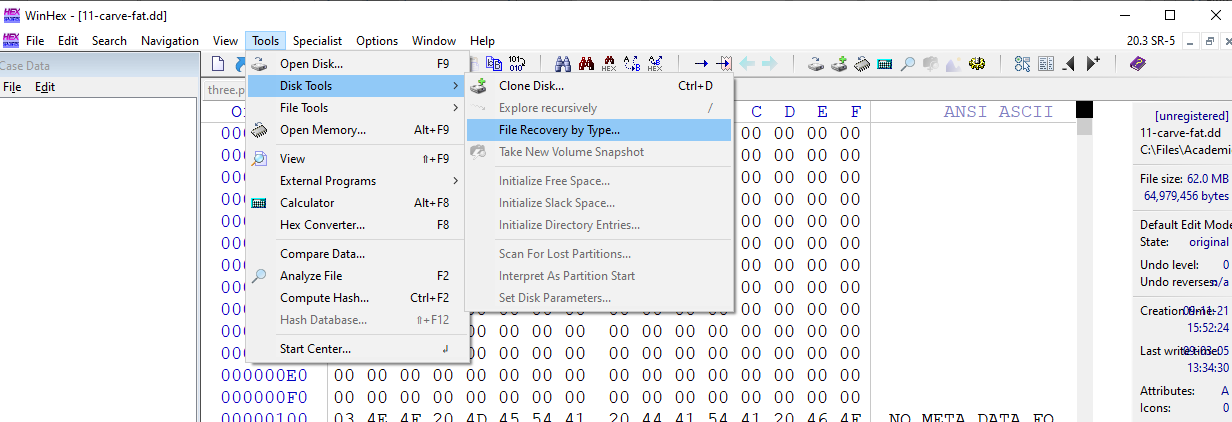
Performing Data/File carving on a couple disk images

**PROCESS**

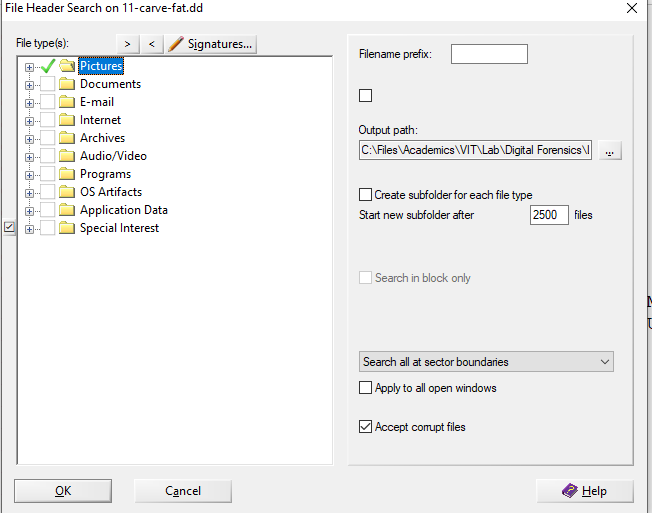
1. Open the image (the DD file) using WinHex.



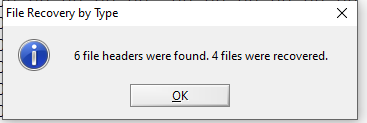
1. Next go to Tools>Disk Tools>File Recovery by Type…



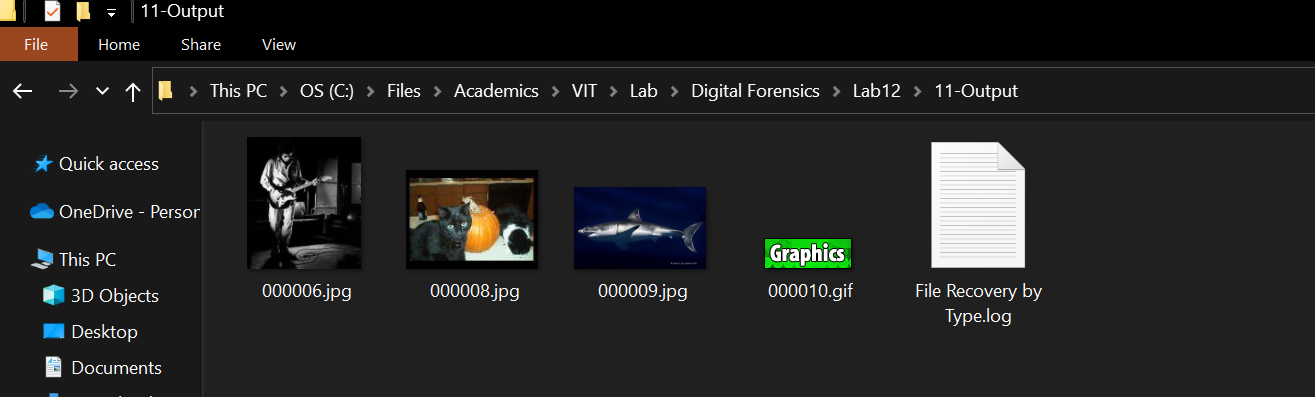
1. Select the type of files you would like to recover (like Pictures, Audio etc). We can also specify what kinds of extensions to recover by expanding each file type. Also select the Output path where the recovered files are supposed to be saved. Then click ‘OK’.



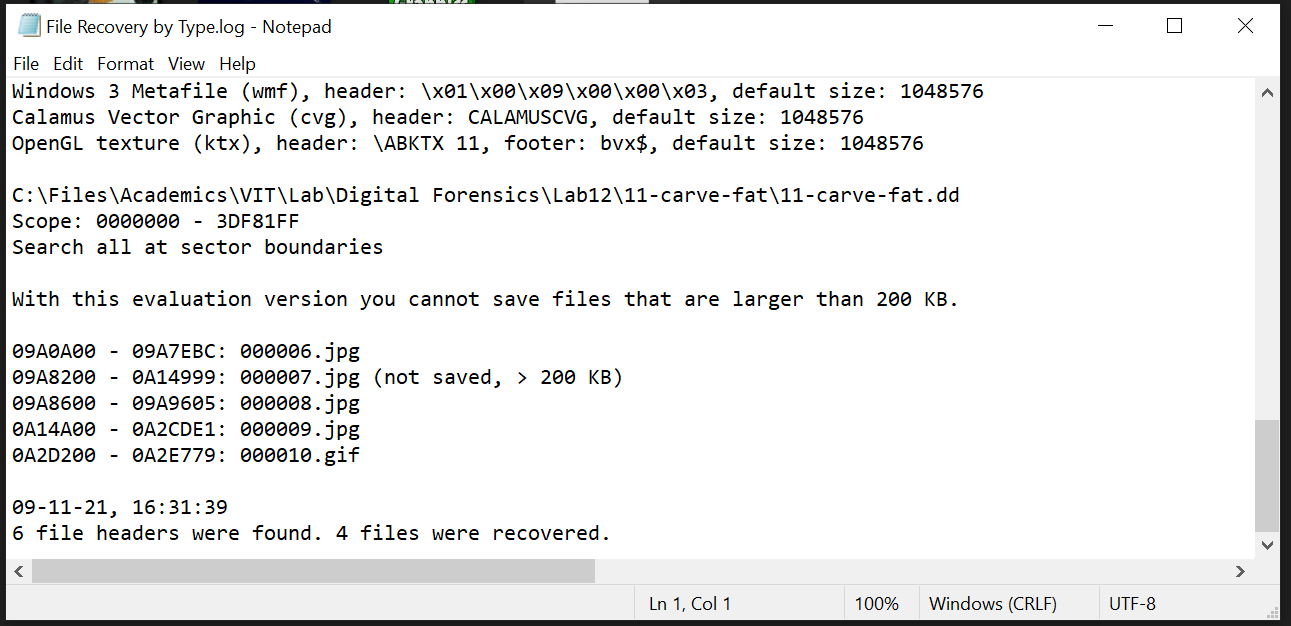
1. Upon completion, the program will display a pop-up as follows. In case of this image file, we find 6 headers out of which WinHex was able to recover 4 image files.



1. Go to the output folder and check the recovered files.



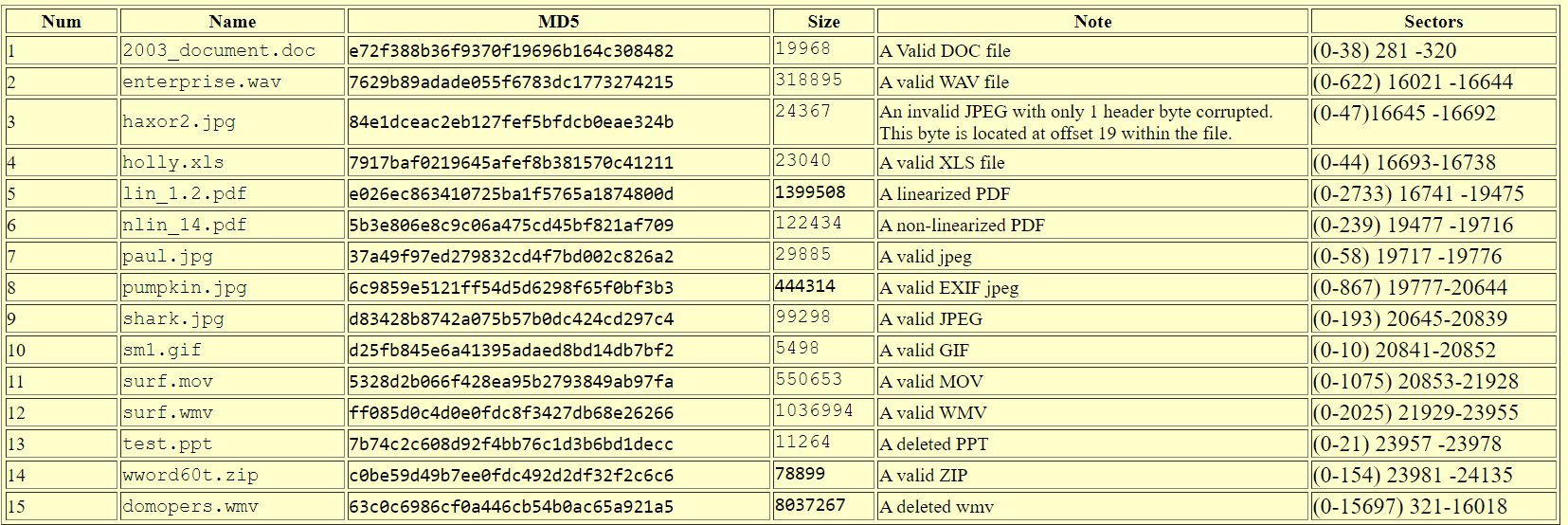
1. We can open the log file to see which files were not recovered. The current evaluation of WinHex used (trial version) does not save files bigger than 200 KB. So, one of the files could not be recovered due to licensing restriction. The log is as shown below.



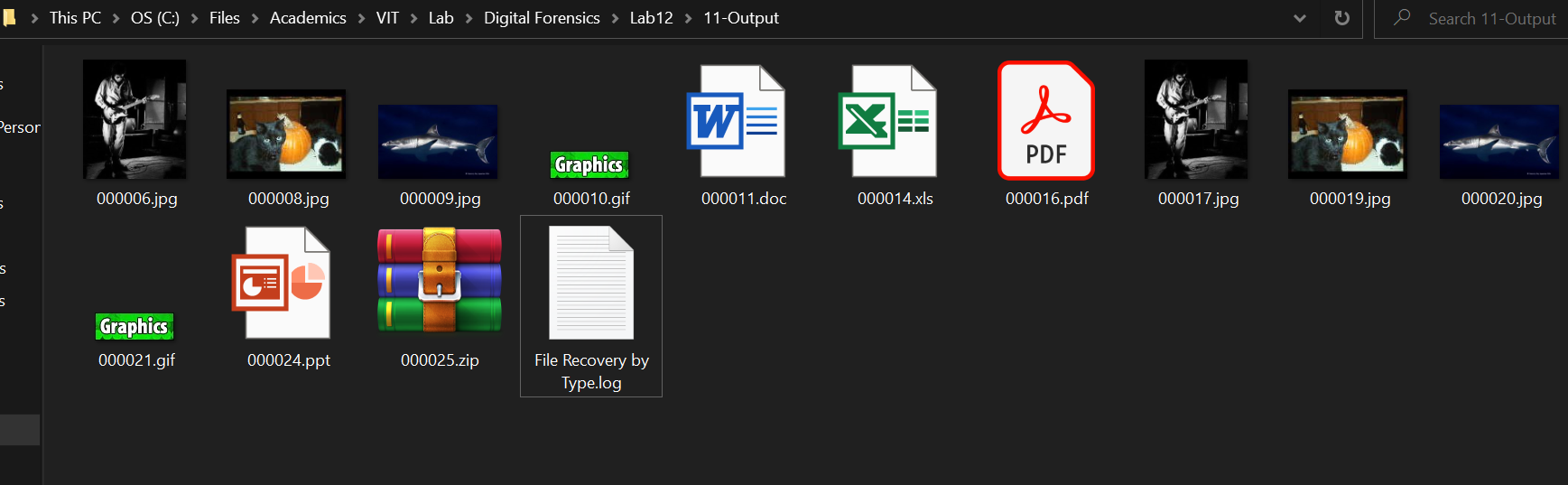
**OBSERVATIONS**

**Image 1 – Image of a FAT disk**

The image used here is that of a FAT disk. It had the following list of files which were then deleted:

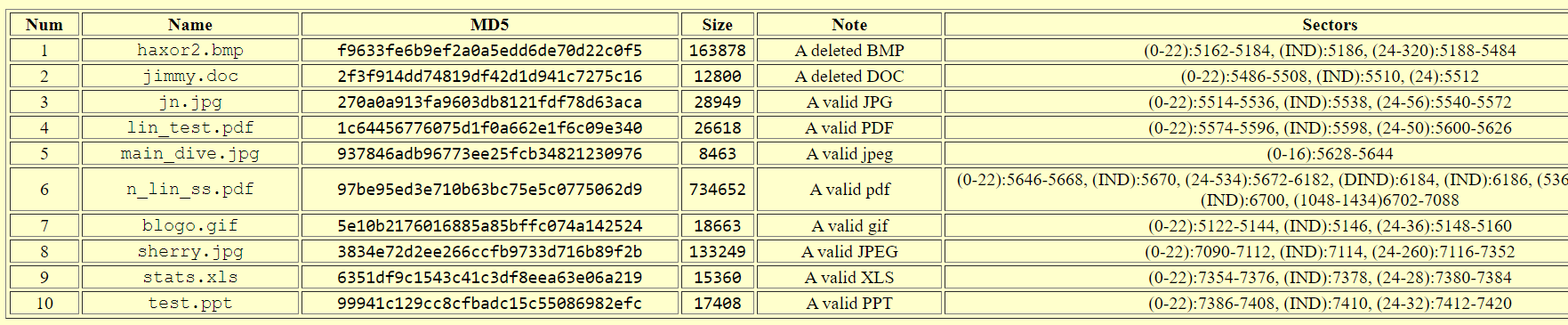


Using WinHex, we try and recover the deleted files by following the process above.



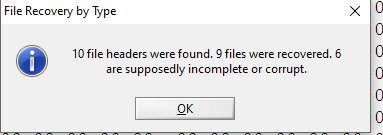
**Image 2 – Image of a EXT2 disk**

The image used here is that of a EXT2 disk. It had the following list of files which were then deleted:

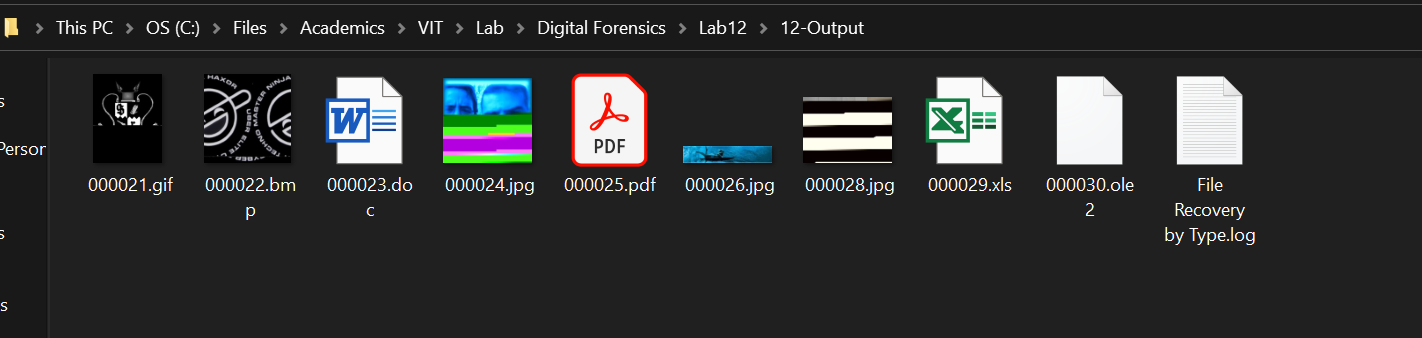


Using WinHex, we try and recover the deleted files by following the process above.

Deleted files which were supported by WinHex could be recovered. However, due to the limits the lack of licensing poses, we extract only files that are smaller than 200 KB. Out of the 10 files detected, 9 were recovered. 6 of them appear to be incomplete or corrupt according to WinHex.



All files recovered from the second image are the following:



**CONCLUSION**

The deleted files were recovered using file/data carving with the aid of WinHex.