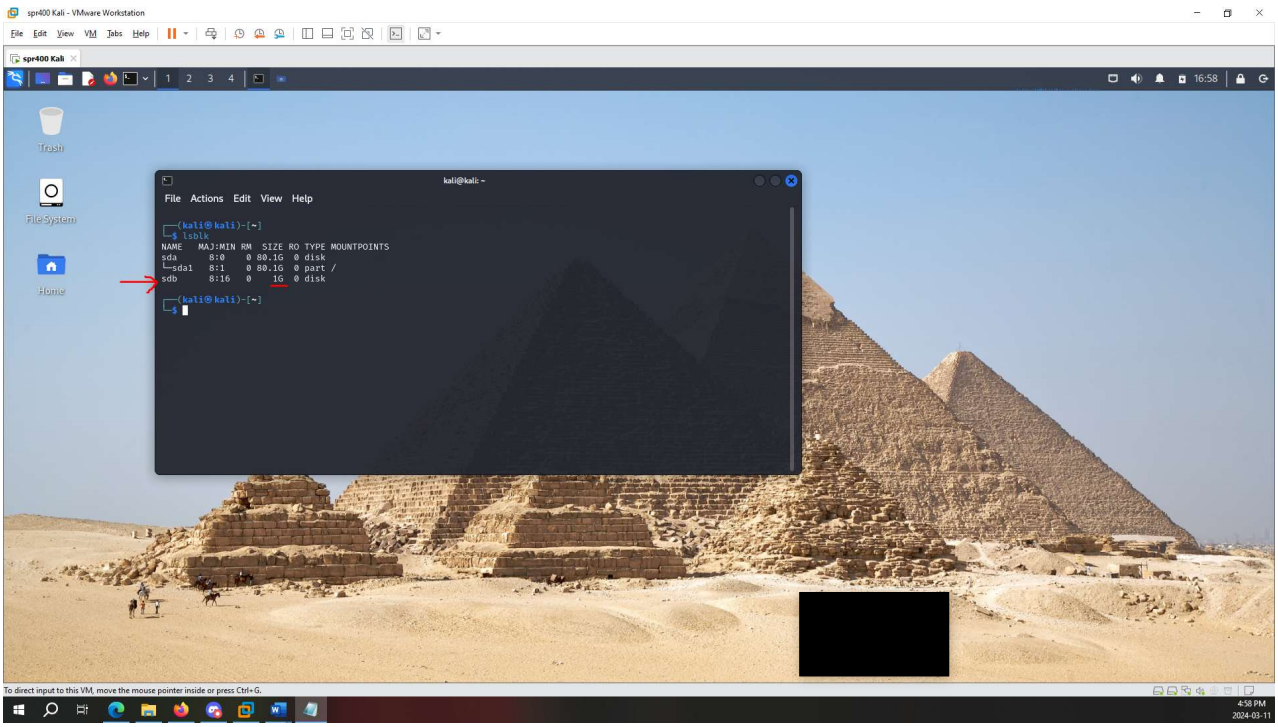
Name: **Abdulfatah Abdillahi**

File Carving

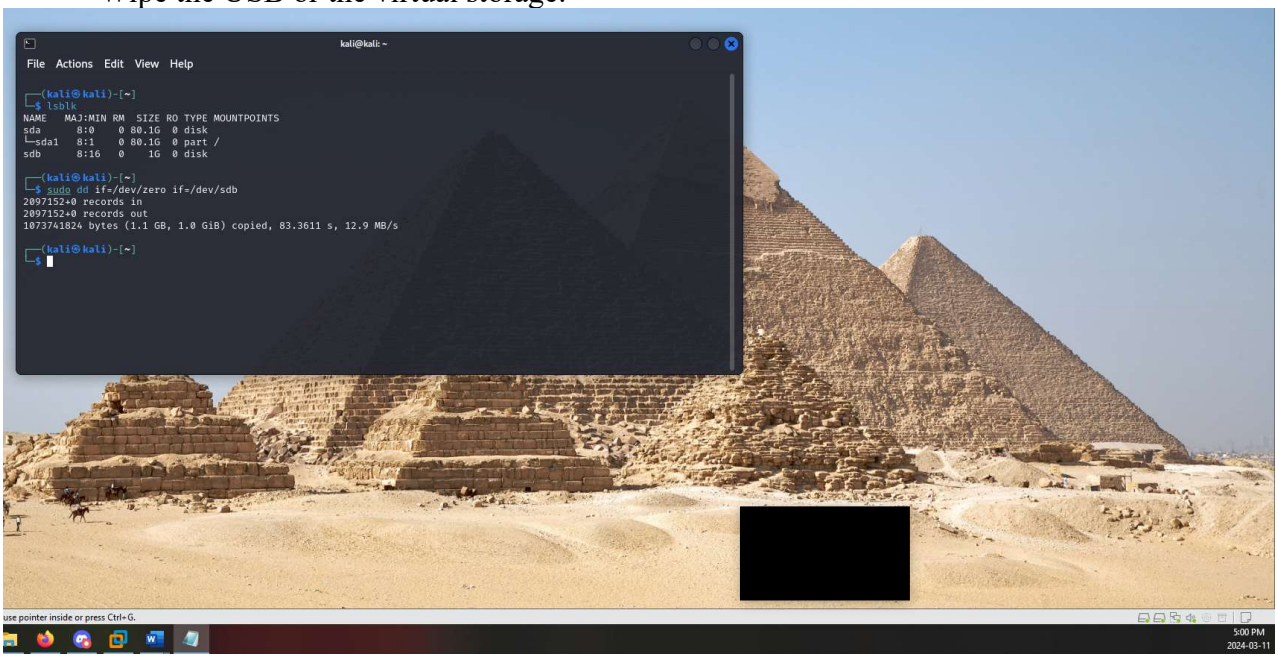
Part 1 – Carving an un-fragmented JPEG File

- Use a small size USB or virtual storage.

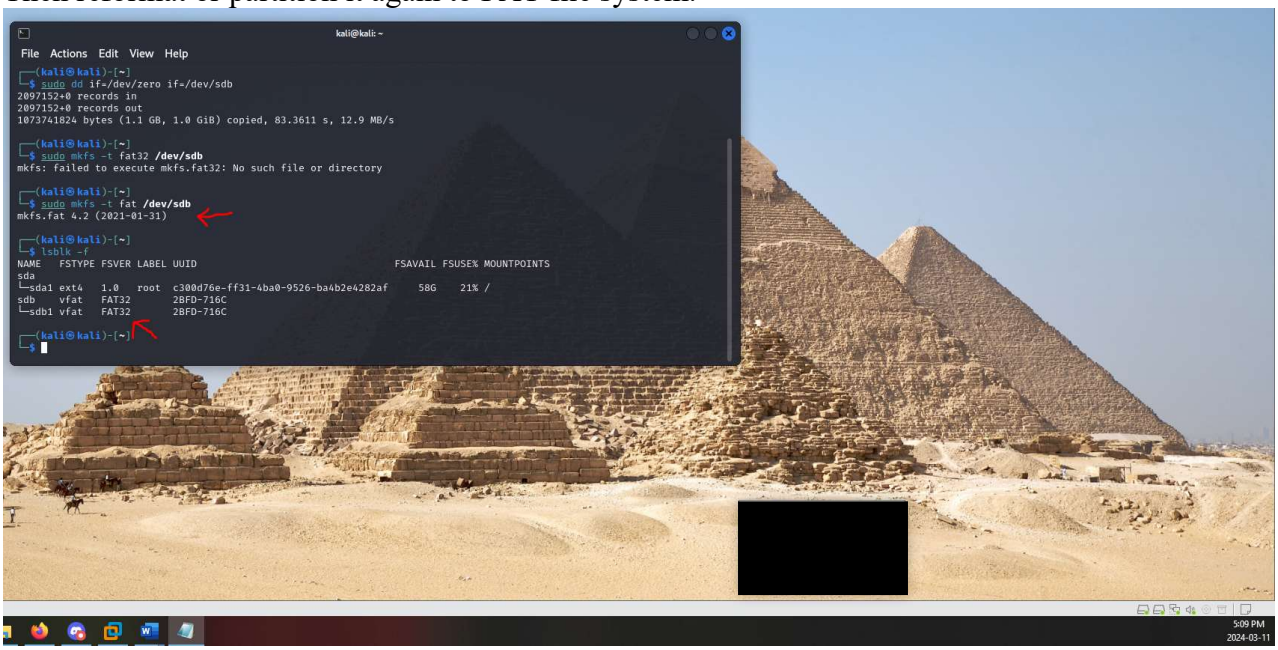
Here you can see my small 500 MB USB



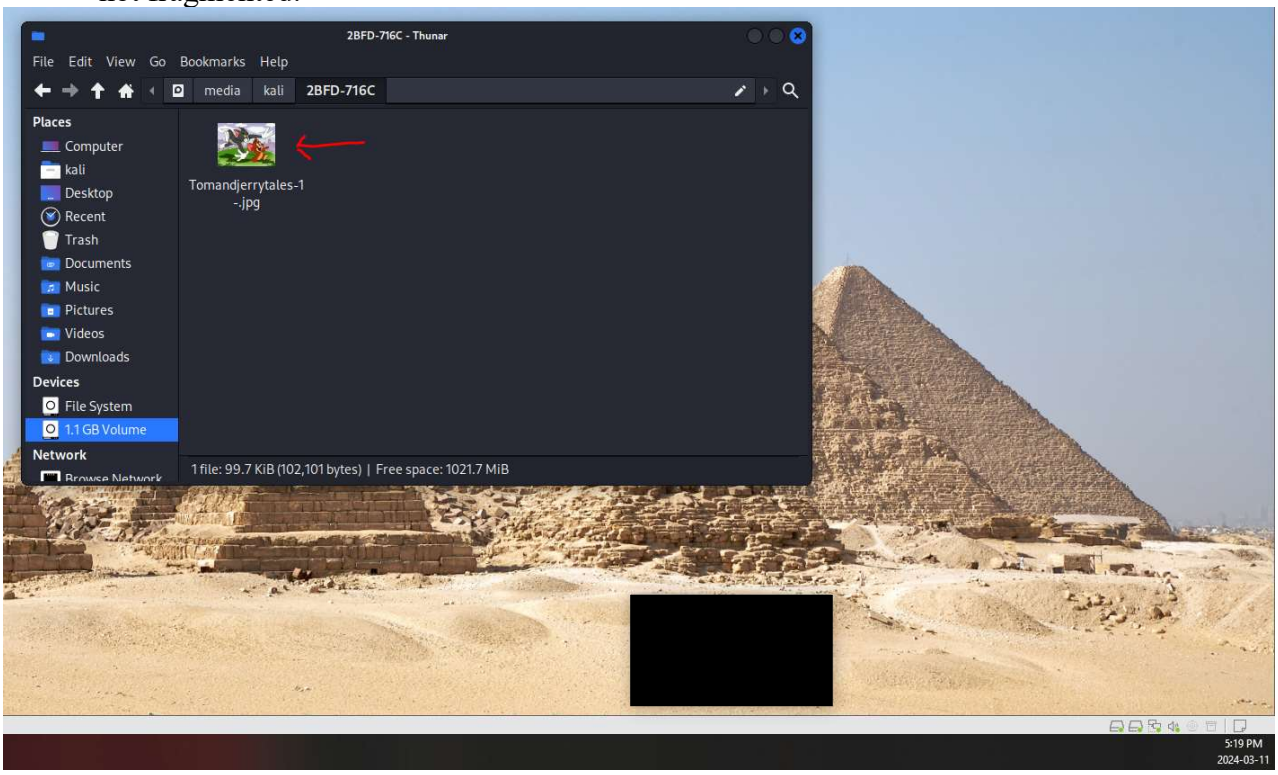
- Wipe the USB or the virtual storage.



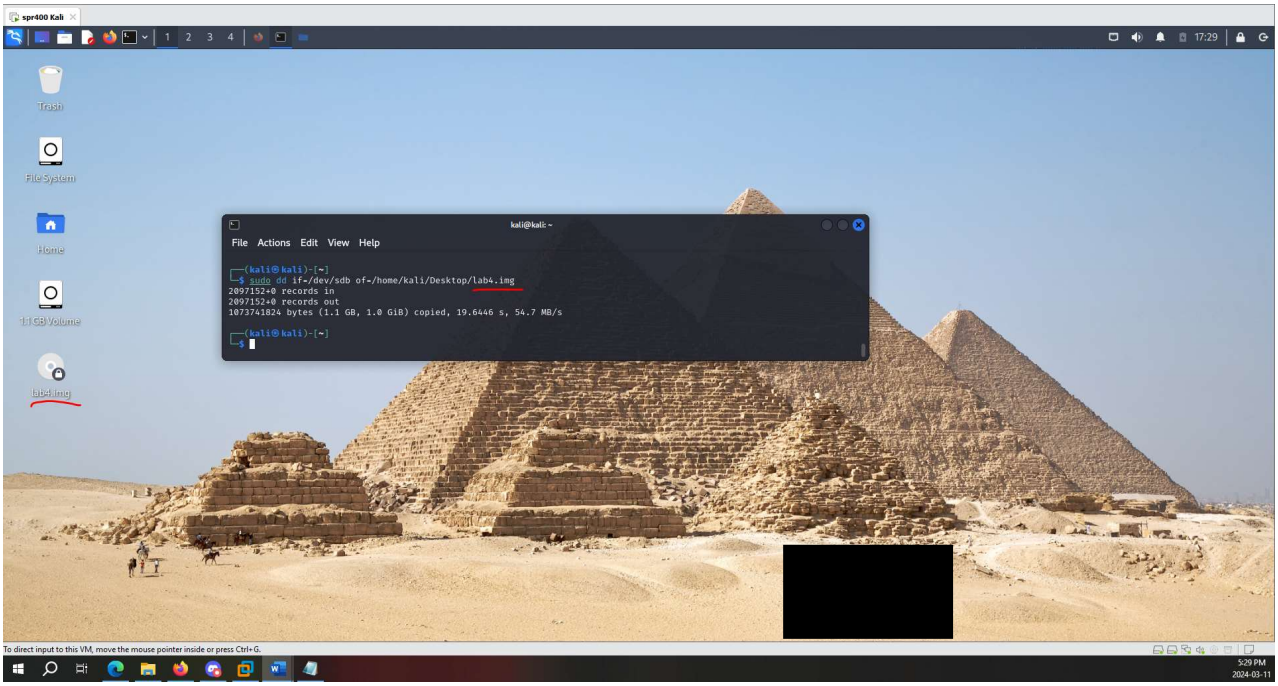
Then reformat or partition it again to FAT file system.



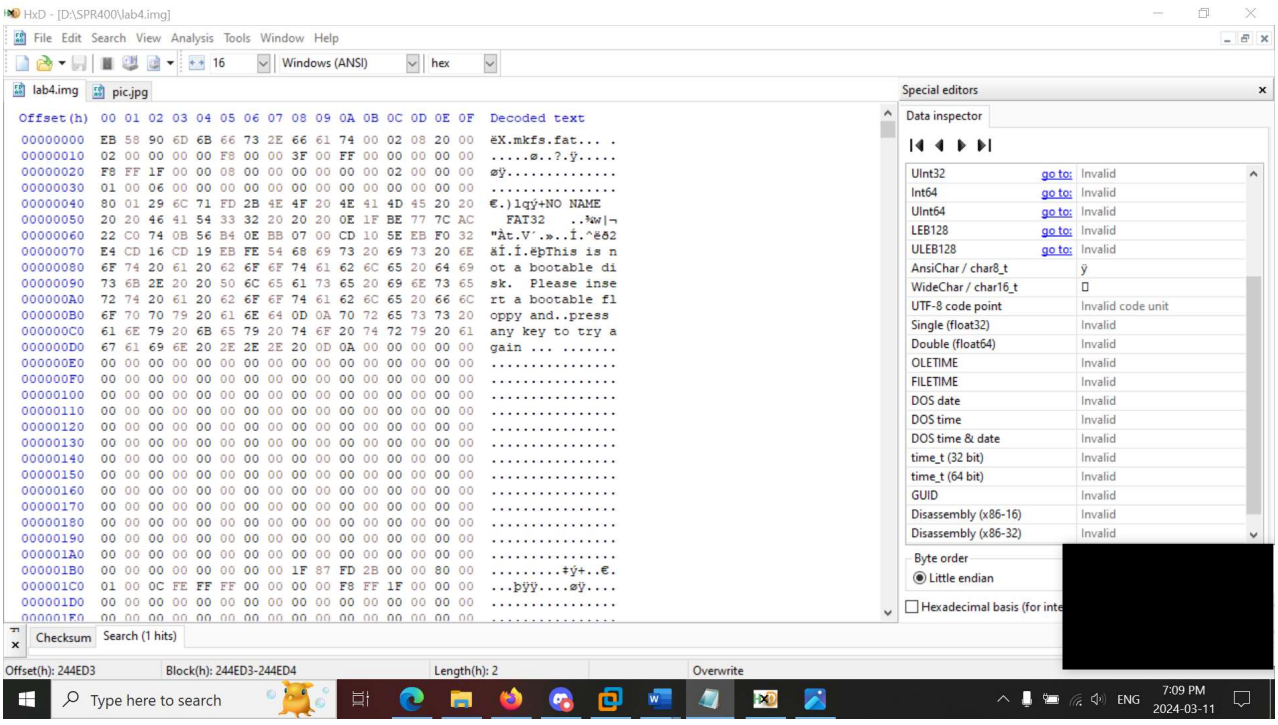
- Save only one JPEG file on the USB. So, your storage media has only one file in it and it is not fragmented.



- Connect the USB and start taking the image.

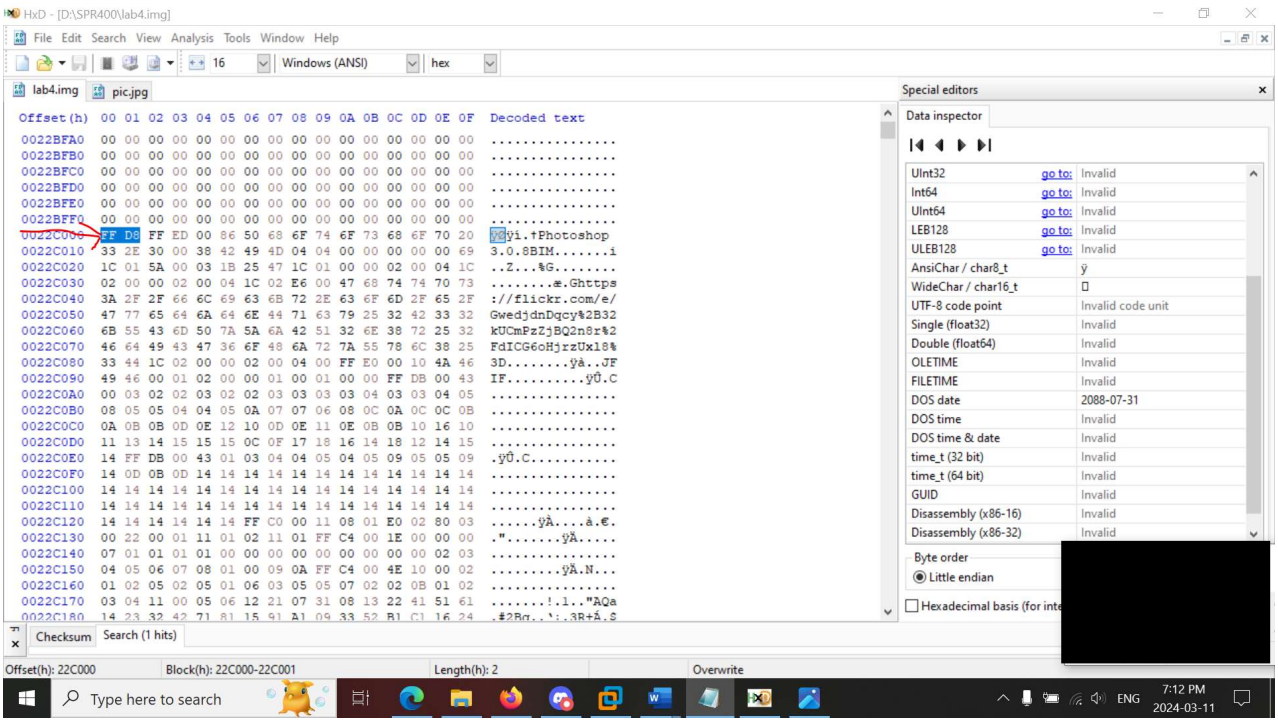


- Open the USB or virtual storage image in any **hex editor**.

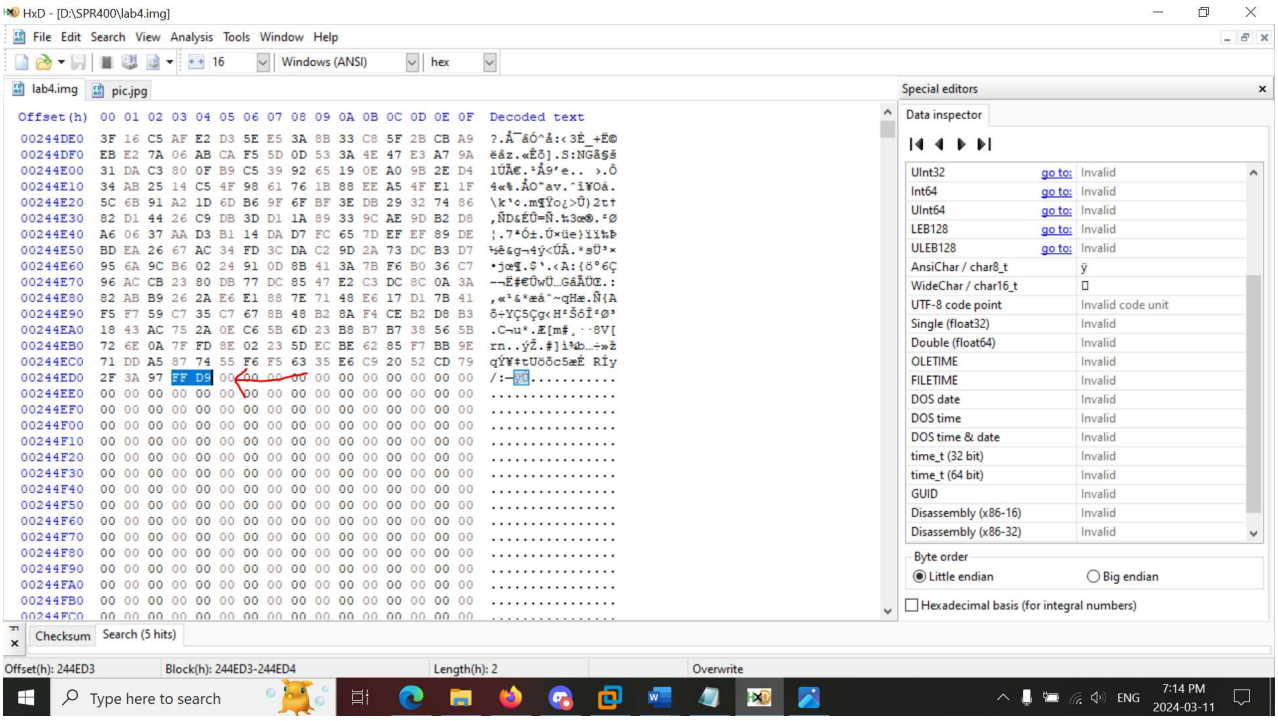


- Recover the file Header-Footer carving strategy.

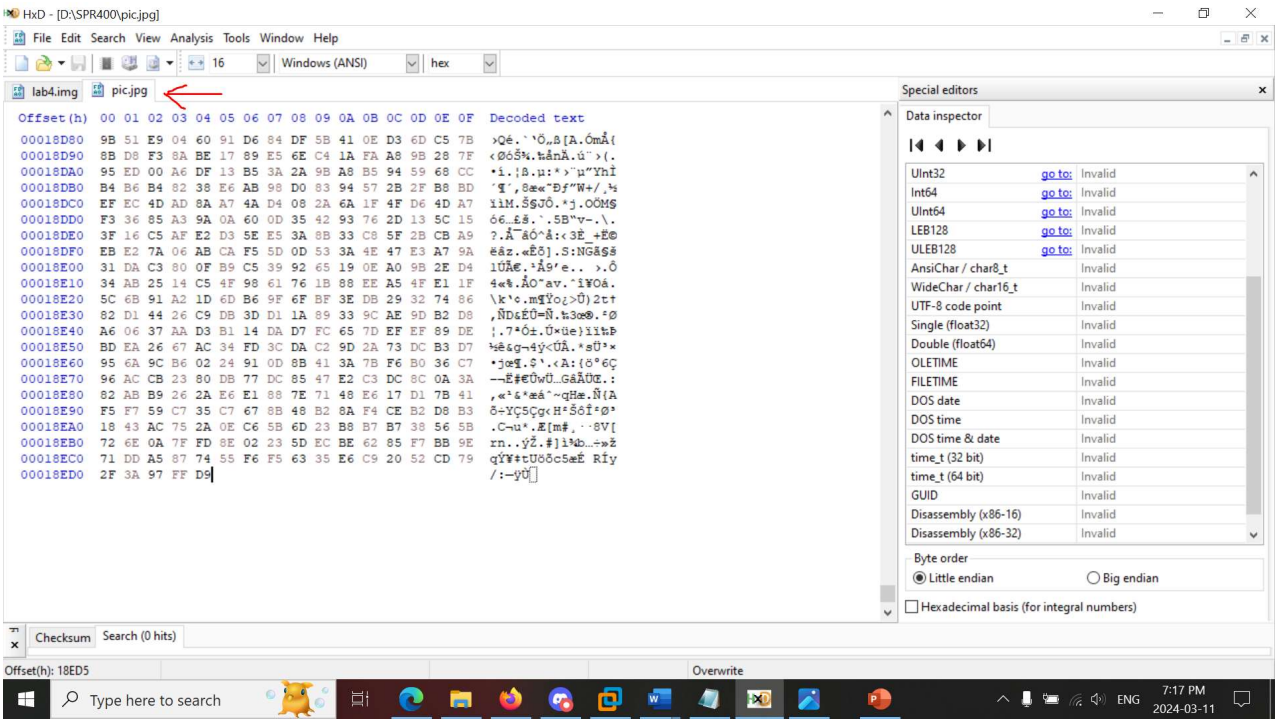
Header: FFD8 and



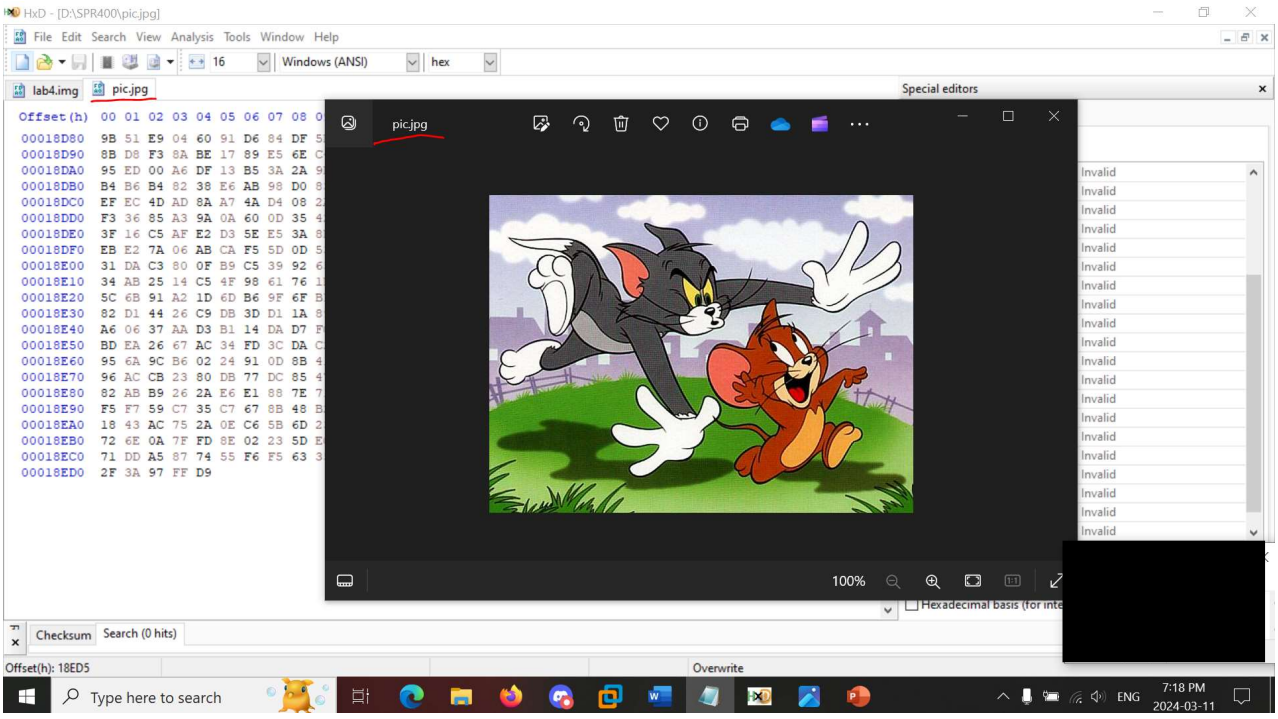
Footer: FFD9



Copying the contents of the image into a new file to save as jpg:

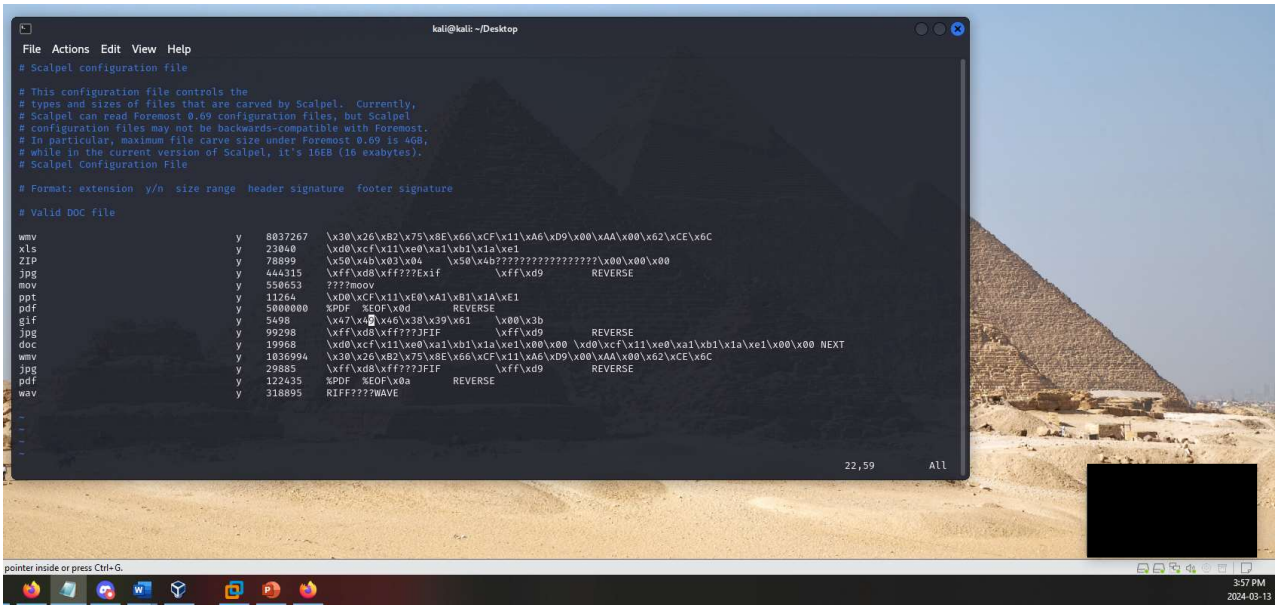


Opening the image (pic.jpg)

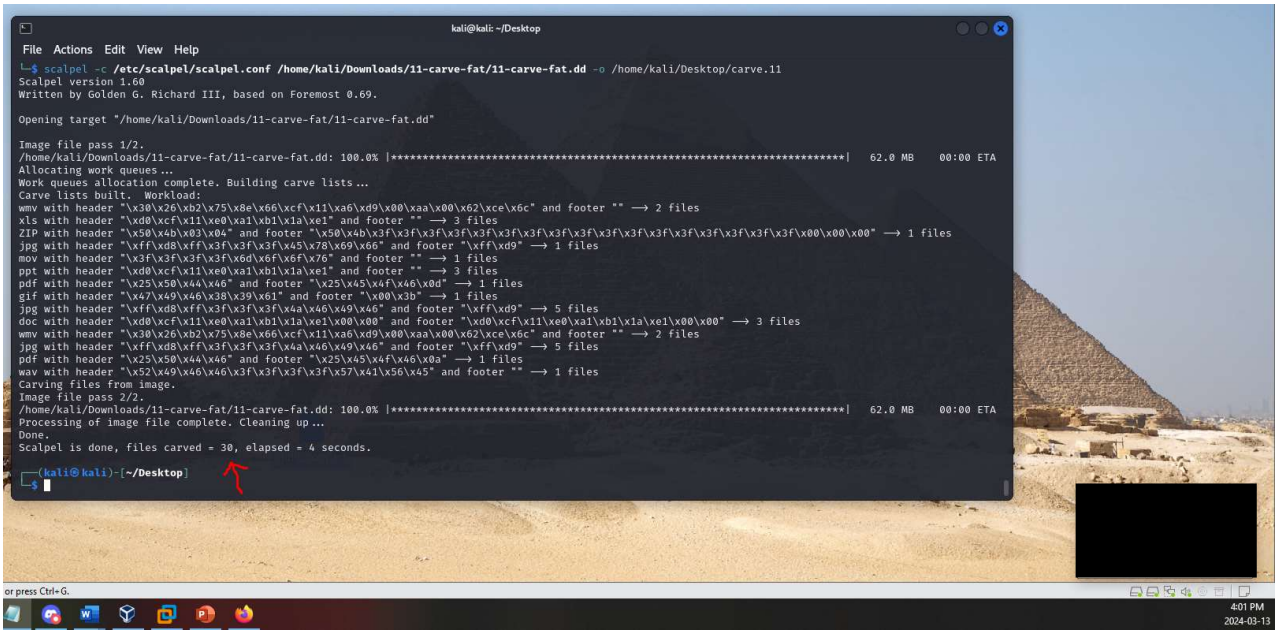


Part 2 -Scalpel

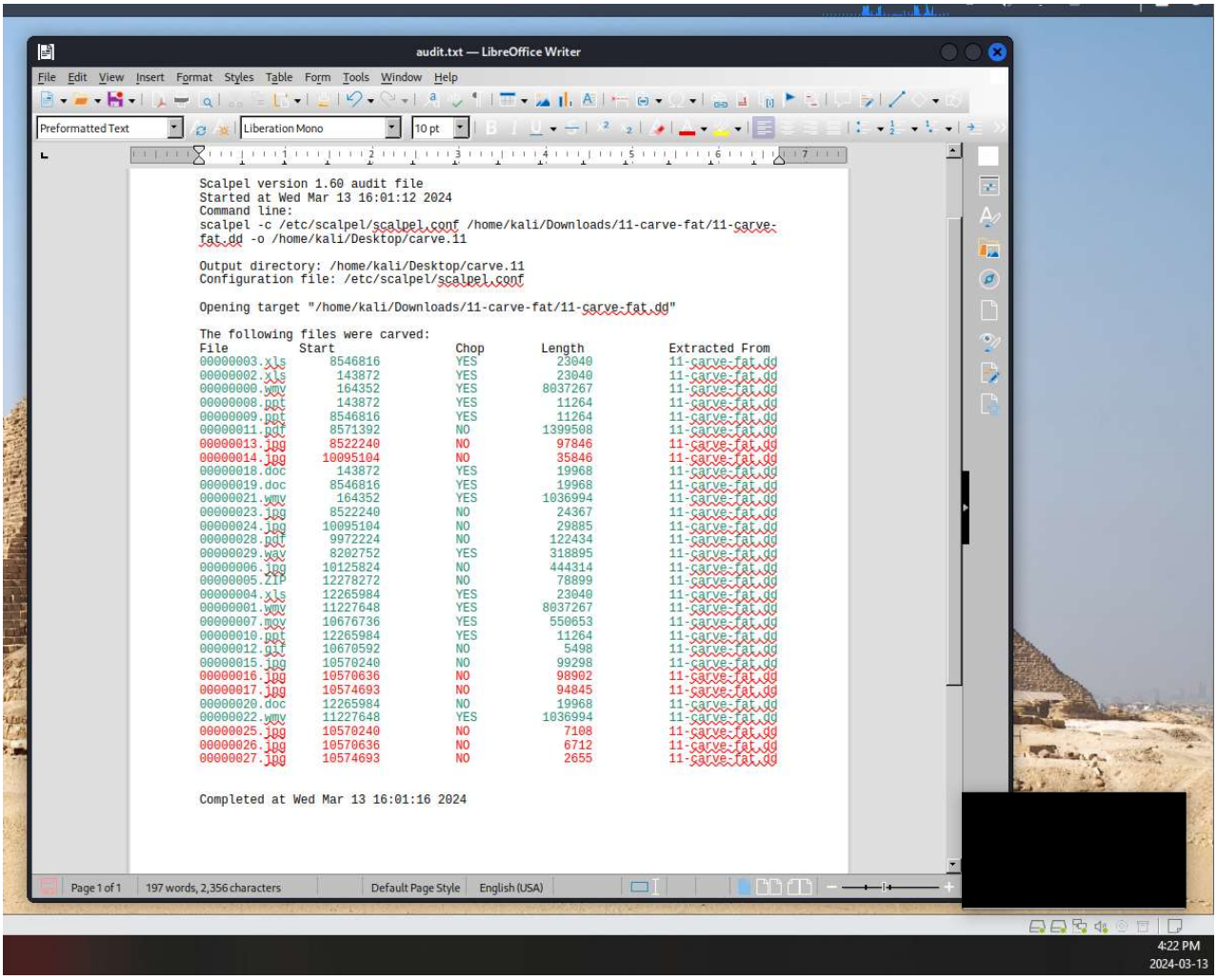
After installing Scalpel, I will carve test image 11 found at http://dftt.sourceforce.net/
I will do this by modifying the configuration file. This is the modified configuration file I used for Scalpel.



I ran the command *scalpel -c /etc/scalpel/scalpel.conf /home/kali/Downloads/11-carve-fat/11-carve-fat.dd -o /home/kali/Desktop/carve.11* and received the below output which tells me that carve was successful and I have 30 files carved.



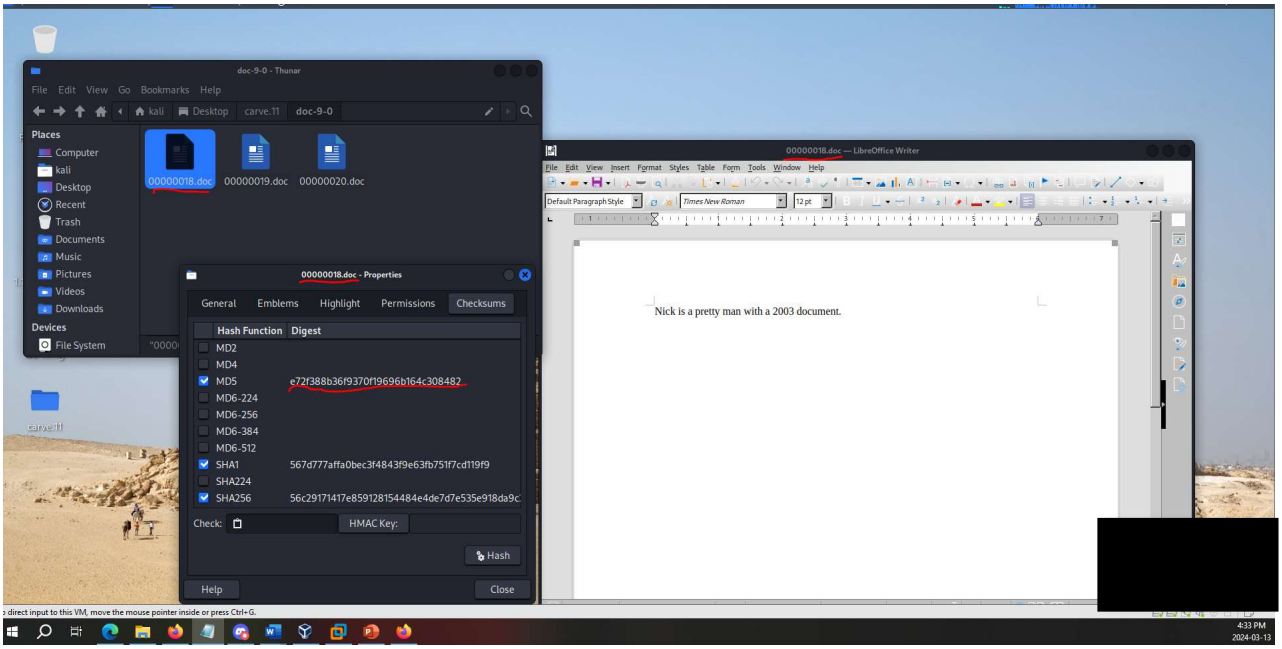
The below screenshot shows the audit.txt file of the carved files. The entries highlighted in green are one of the 15 files listed that I managed to recover. The entries highlighted in red are not one of the 15 files (i.e false positive). It is worth noting that some of the images are duplicates which is why we ensured to document the correct files along with their corresponding hashes.



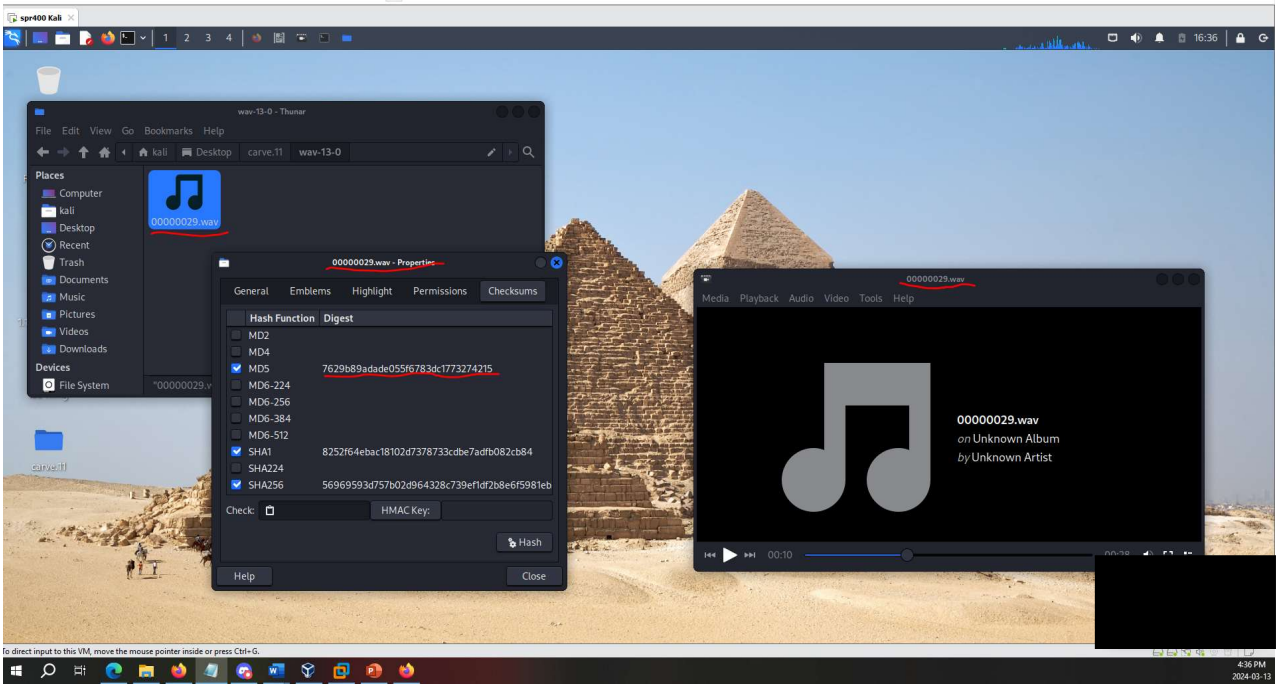
Files Recovered

Each file in the image has a corresponding MD5 hash. I ensured to include the matching hashes in the screenshot as well.

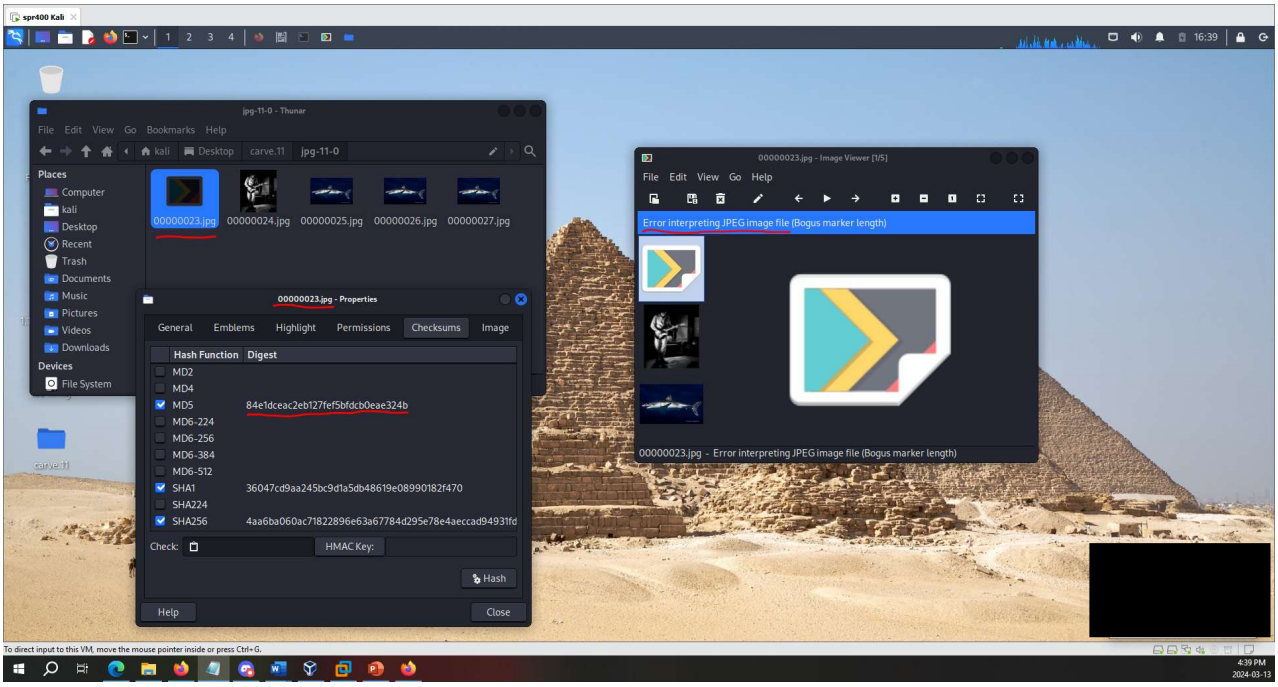
2003_document.doc



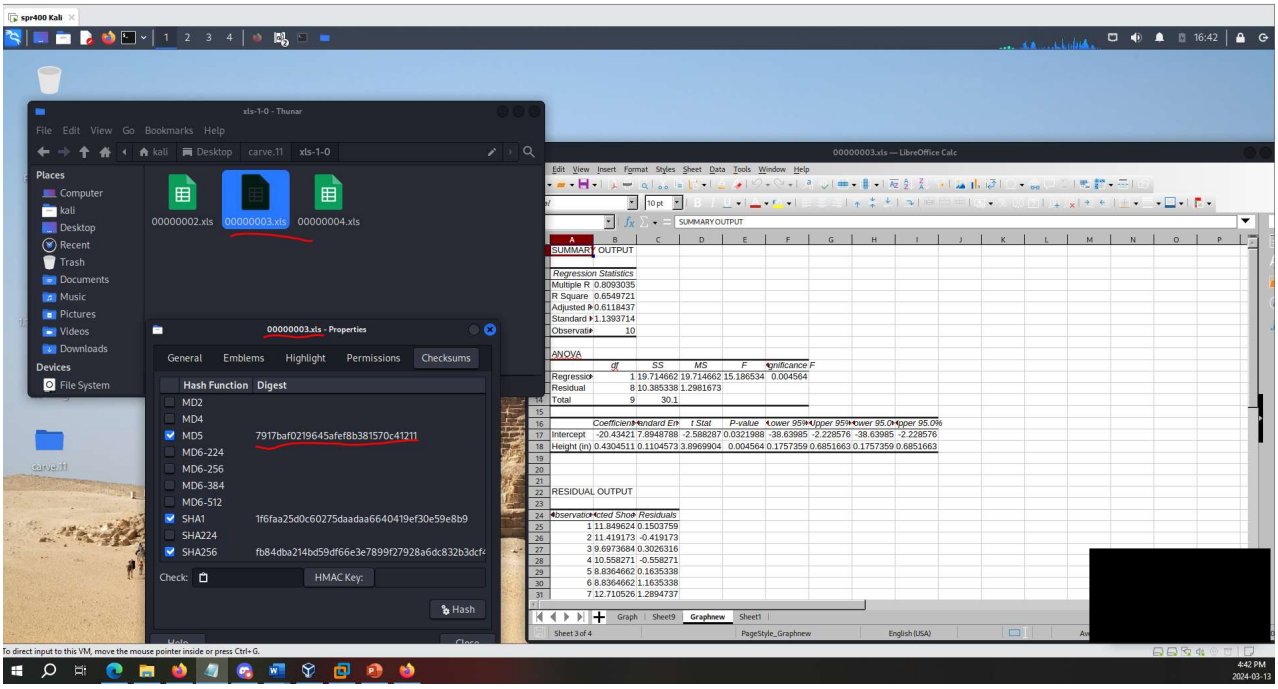
enterprise.wav



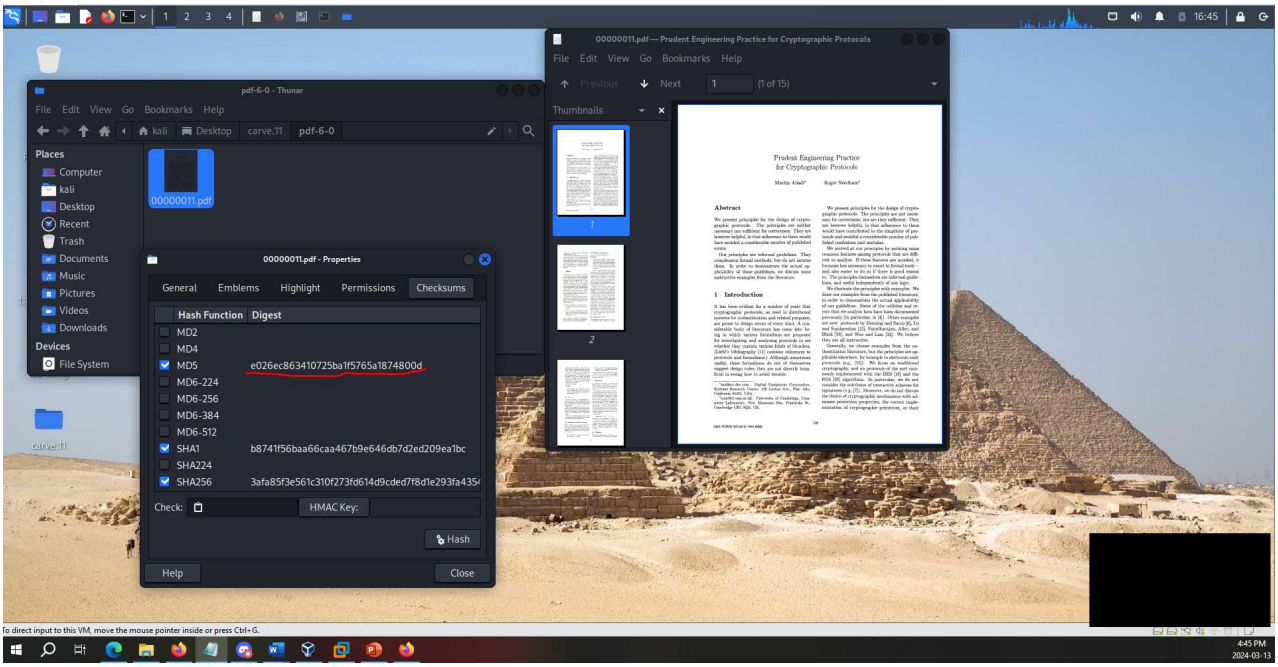
haxor2.jpg (invalid JPEG)



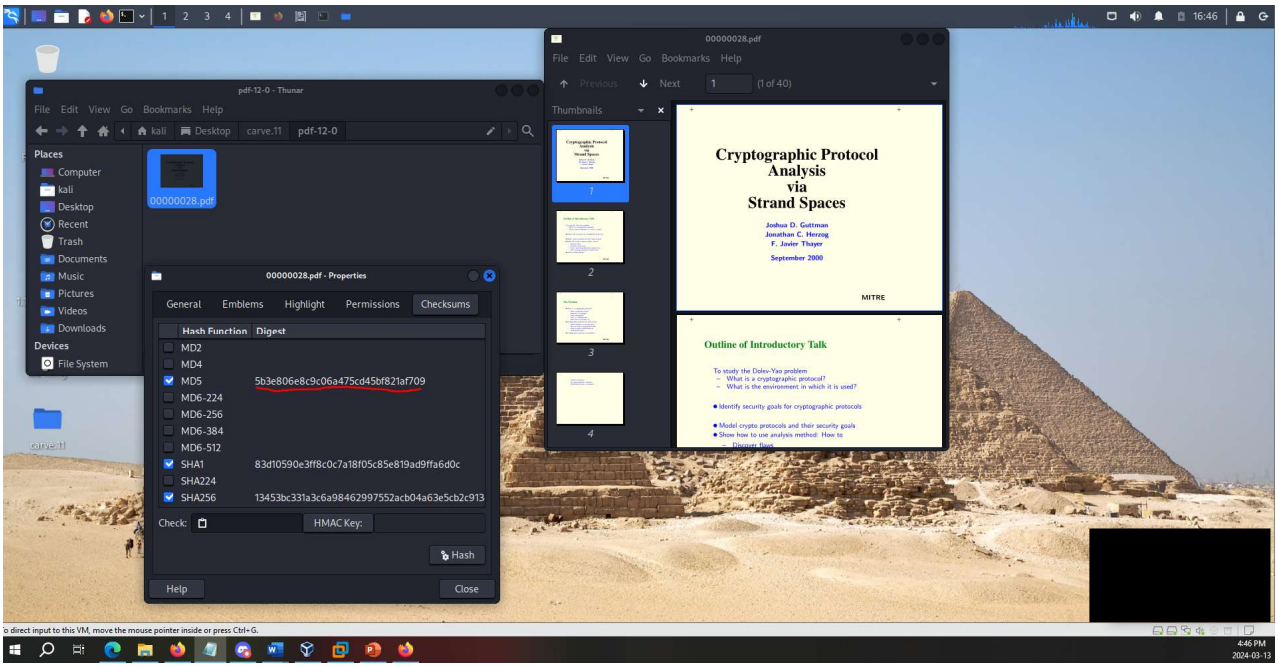
holly.xls



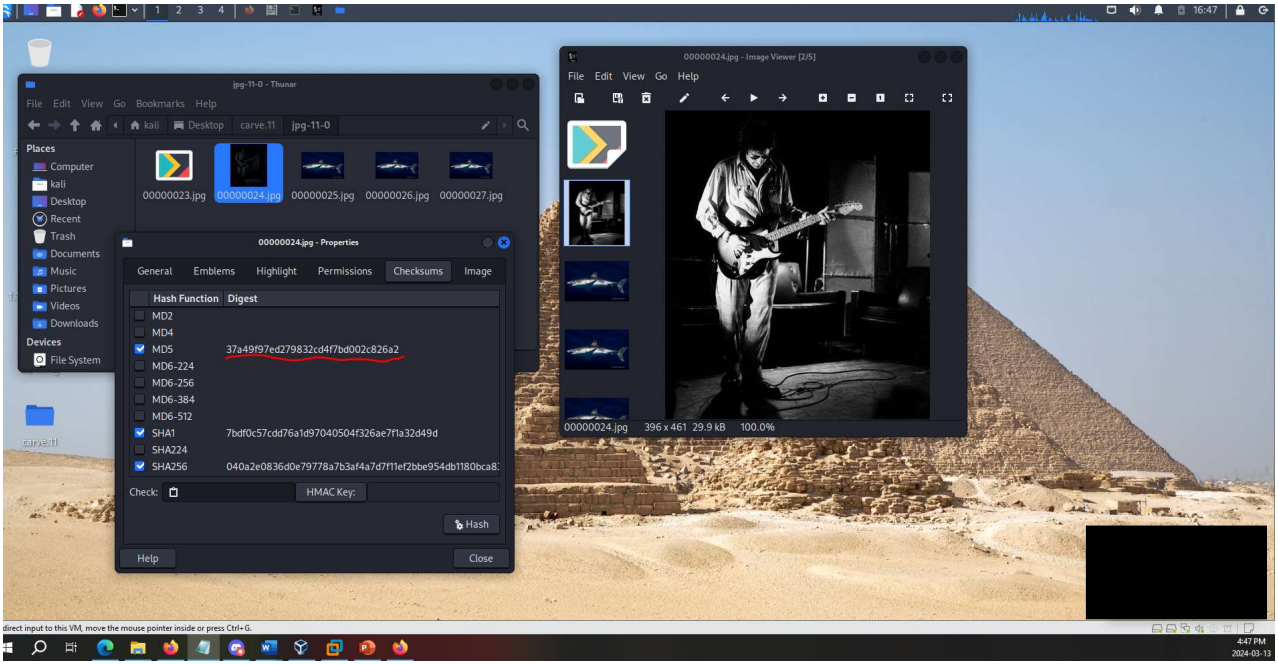
lin_1.2.pdf



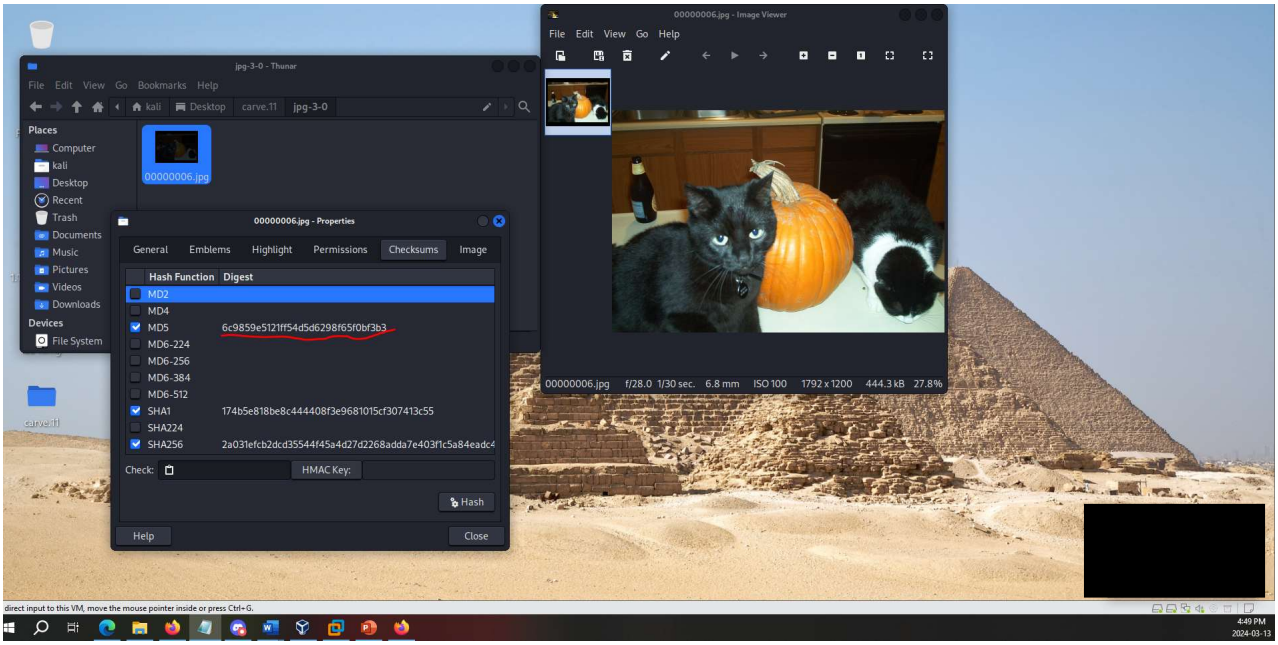
nlin_14.pdf



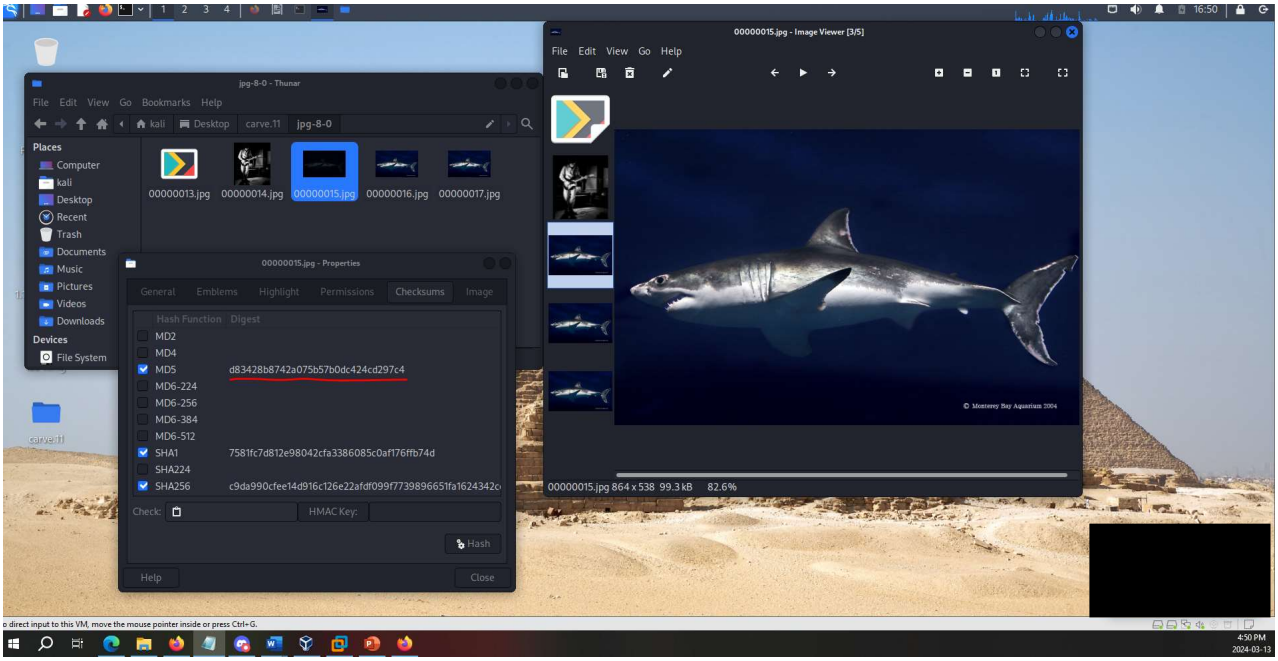
paul.jpg



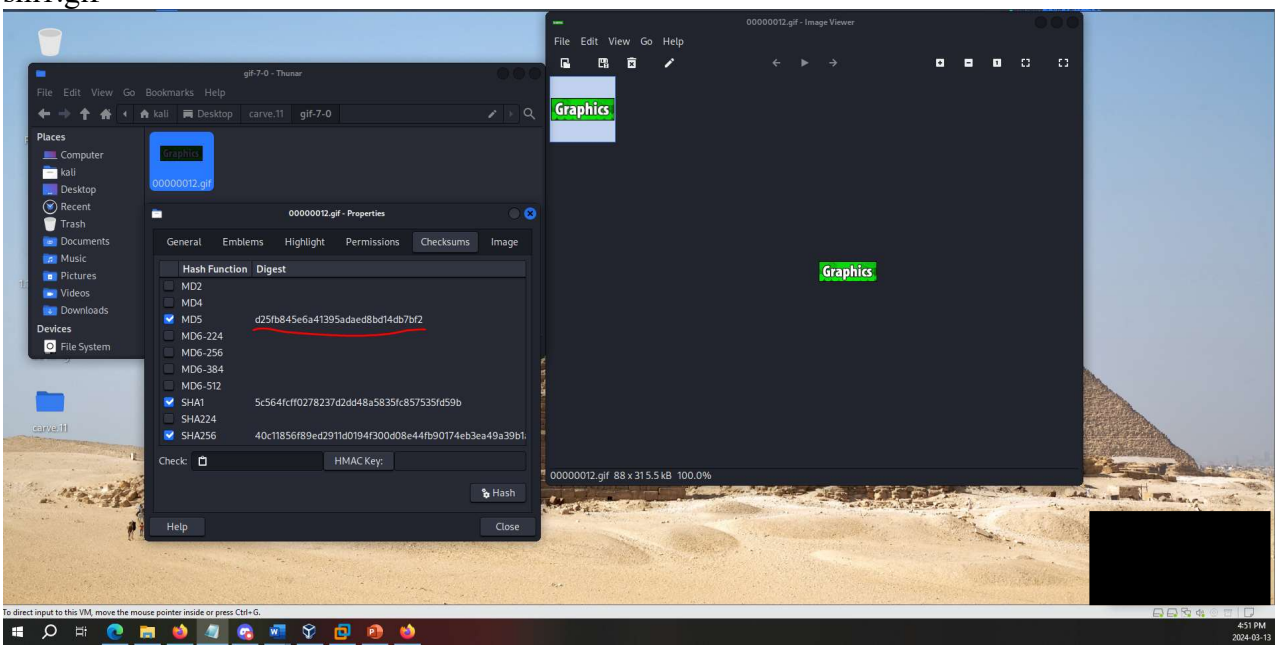
pumpkin.jpg



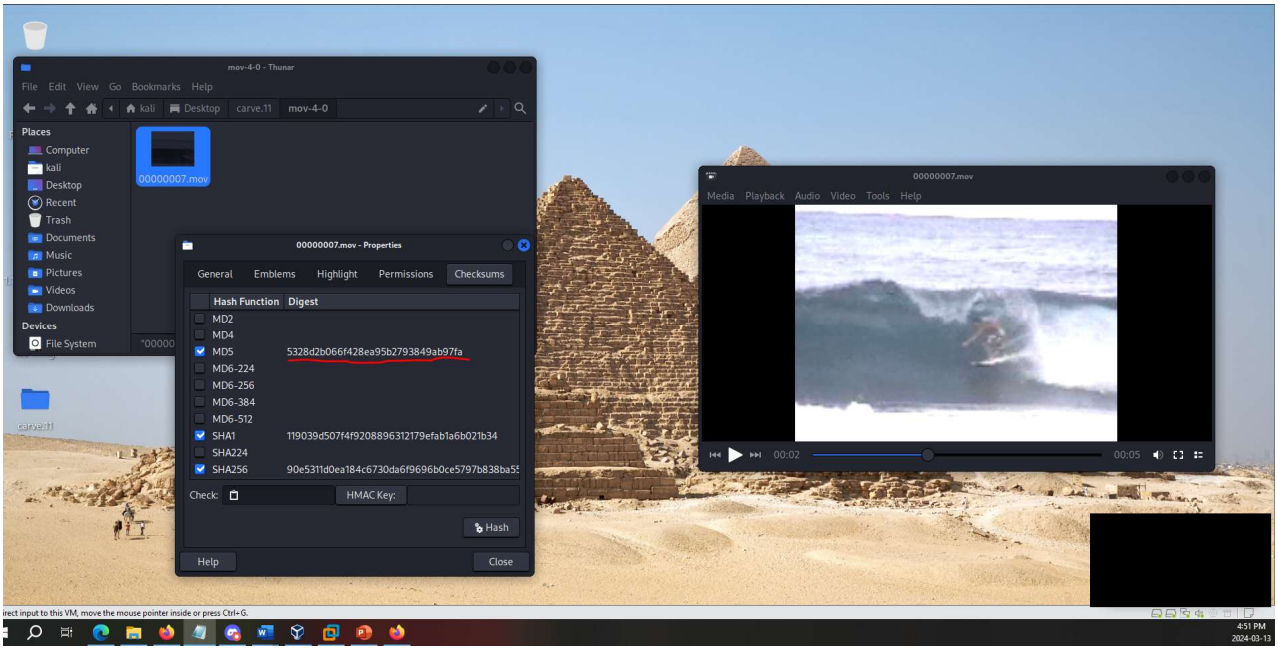
shark.jpg



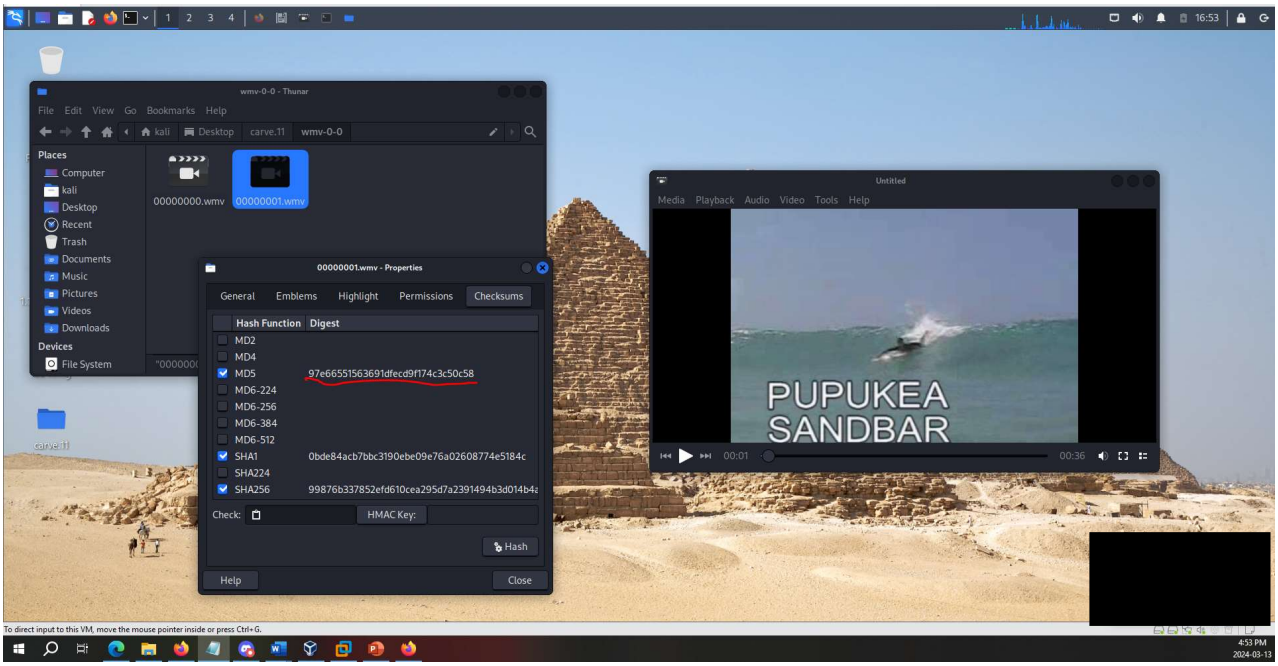
sm1.gif



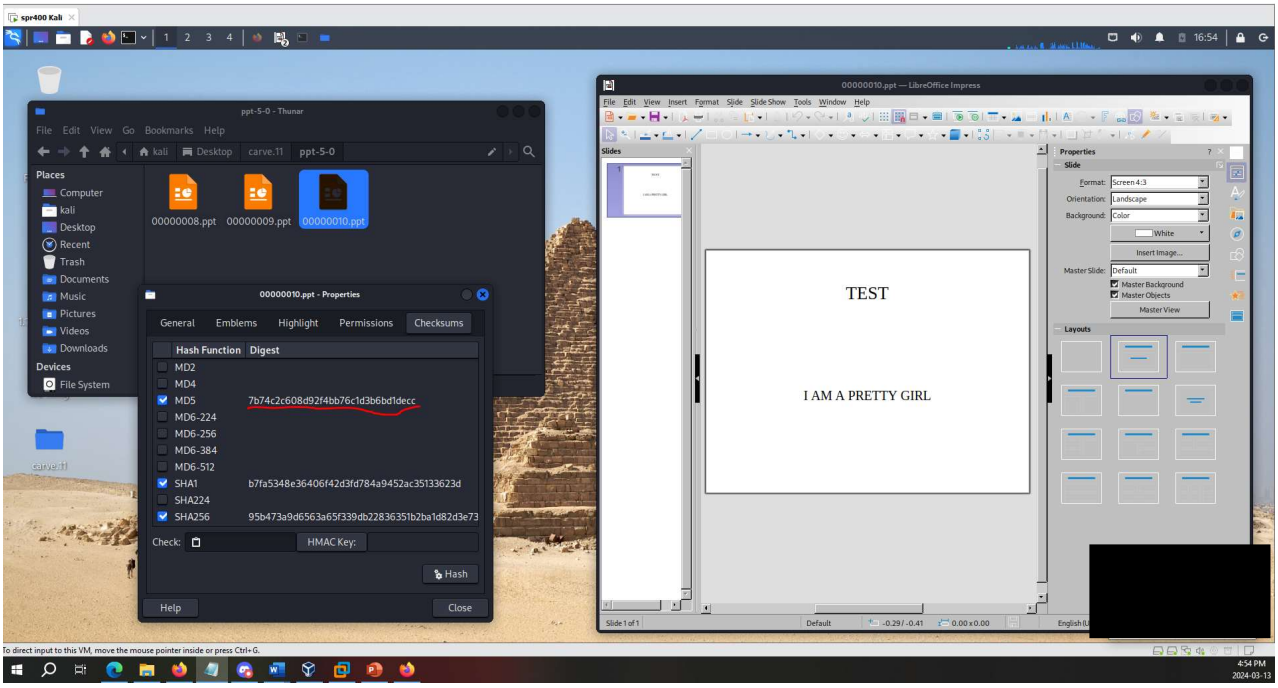
surf.mov



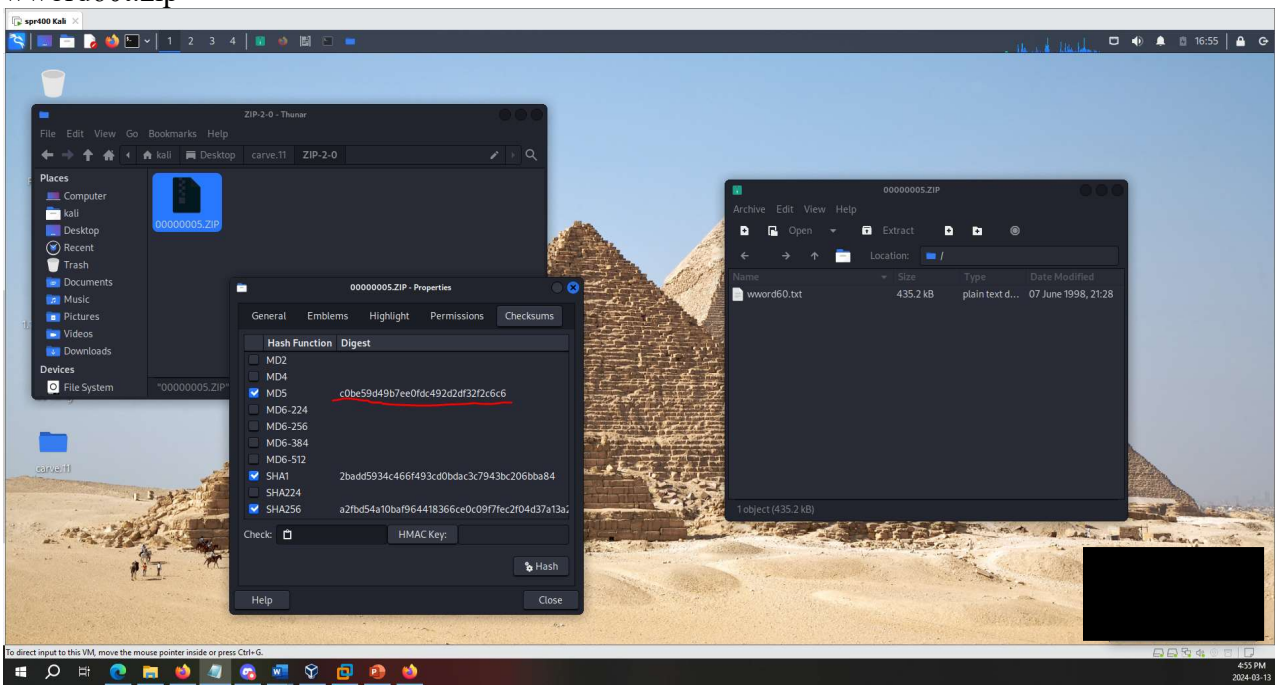
surf.wmv



test.ppt



wword60t.zip



domopers.wmv

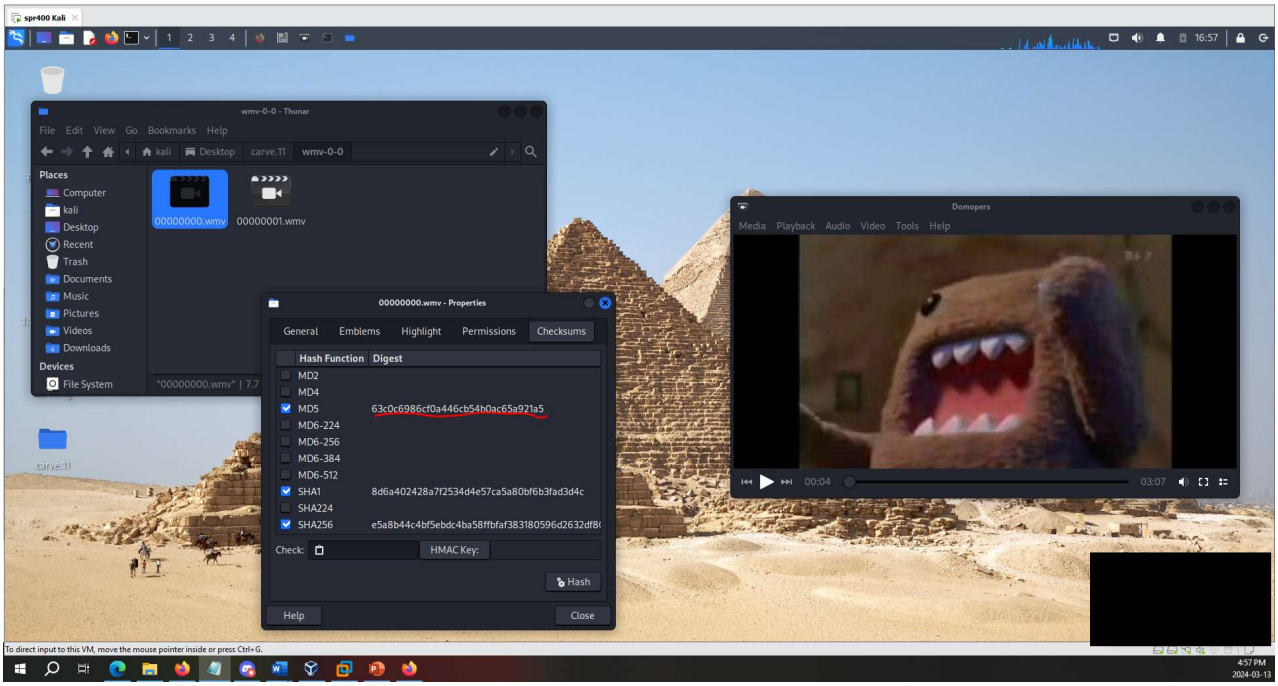


Table listing the recovered/not recovered files.

Order	File Name	Recovered (Y/N)	If not recovered, explain!
1	2003_document.doc	Y	
2	enterprise.wav	Y	
3	haxor2.jpg	N	The header of the image was corrupted and since scalpel relies on the header and footer for recovery it didn't work.
4	holly.xls	Y	
5	lin_1.2.pdf	Y	
6	nlin_14.pdf	Y	
7	paul.jpg	Y	
8	pumpkin.jpg	Y	
9	shark.jpg	Y	
10	sm1.gif	Y	
11	surf.mov	Y	
12	surf.wmv	Y	
13	test.ppt	Y	
14	wword60t.zip	Y	
15	domopers.wmv	Y	