

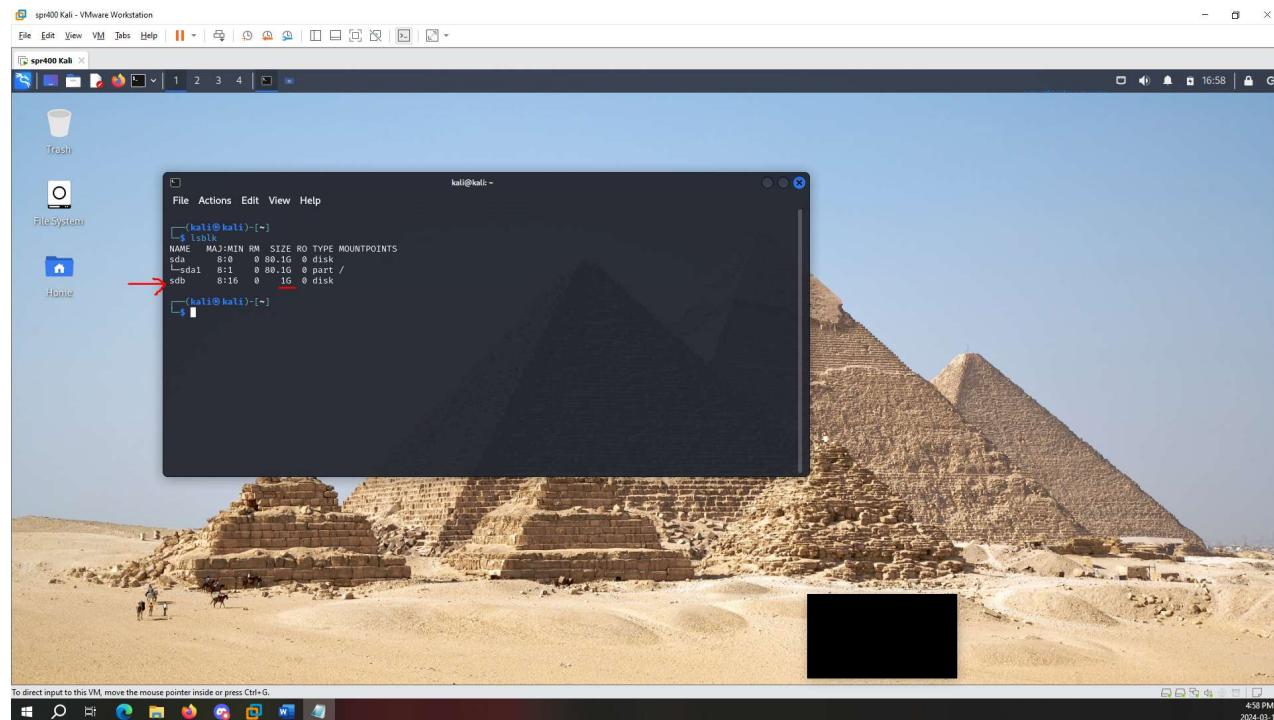
Name: Abdulfatah Abdillahi

File Carving

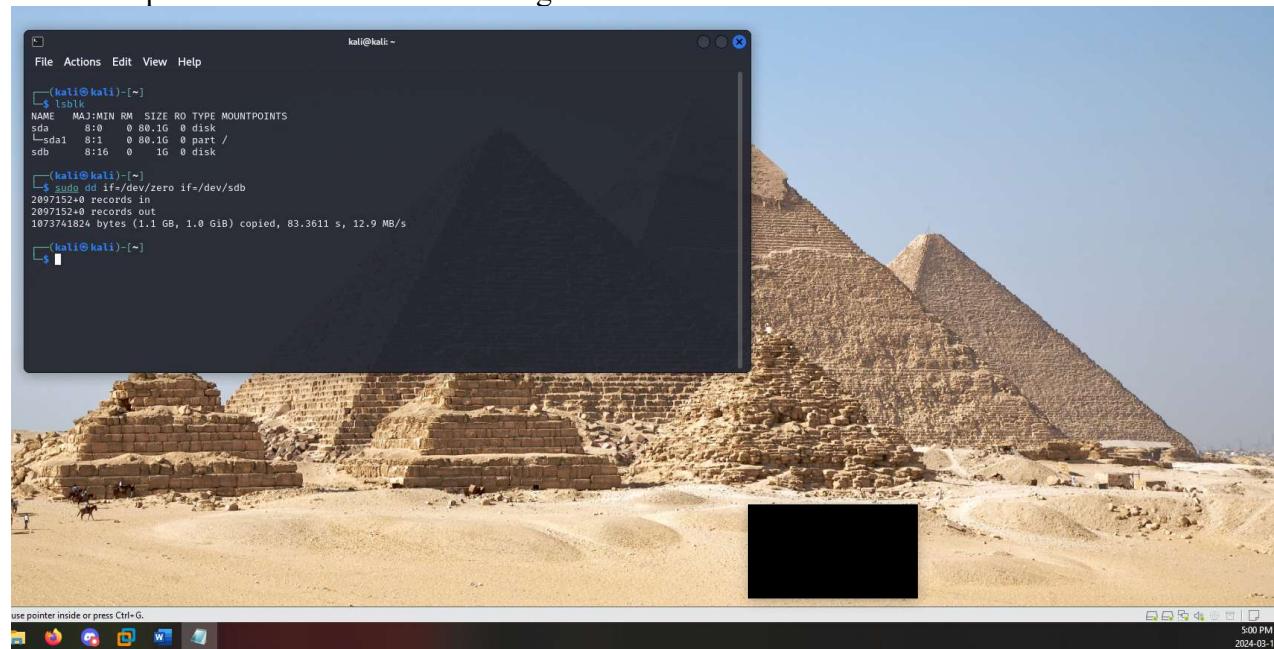
Part 1 – Carving an un-fragmented JPEG File

- Use a small size USB or virtual storage.

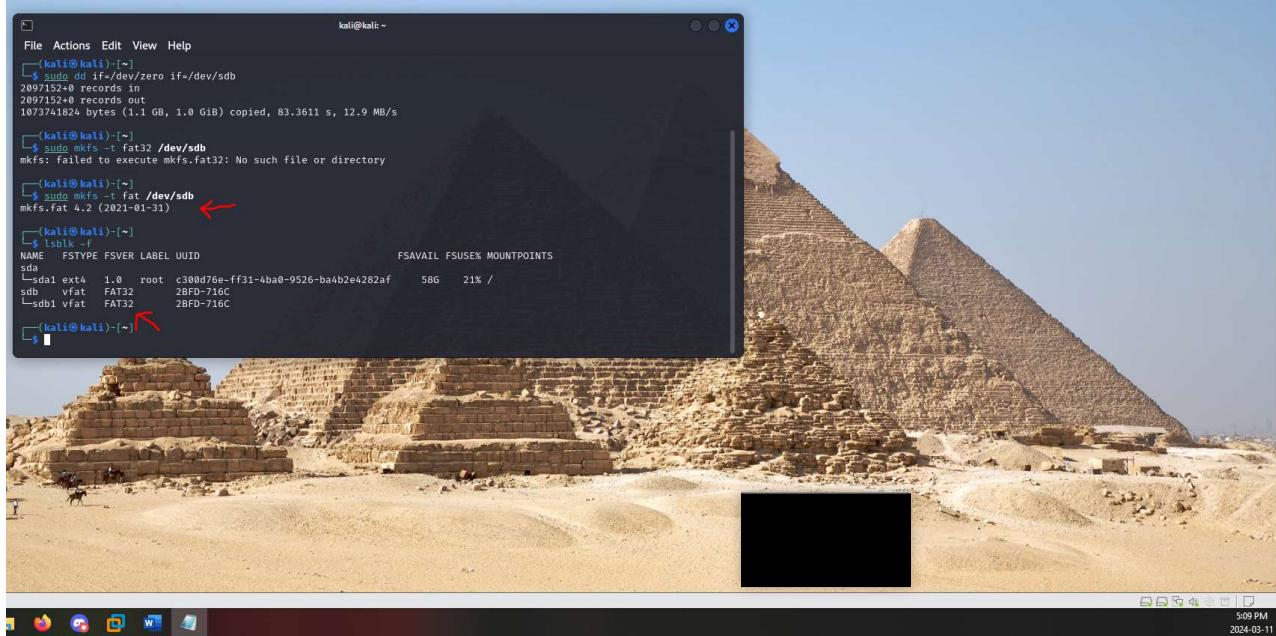
Here you can see my small 500 MB USB



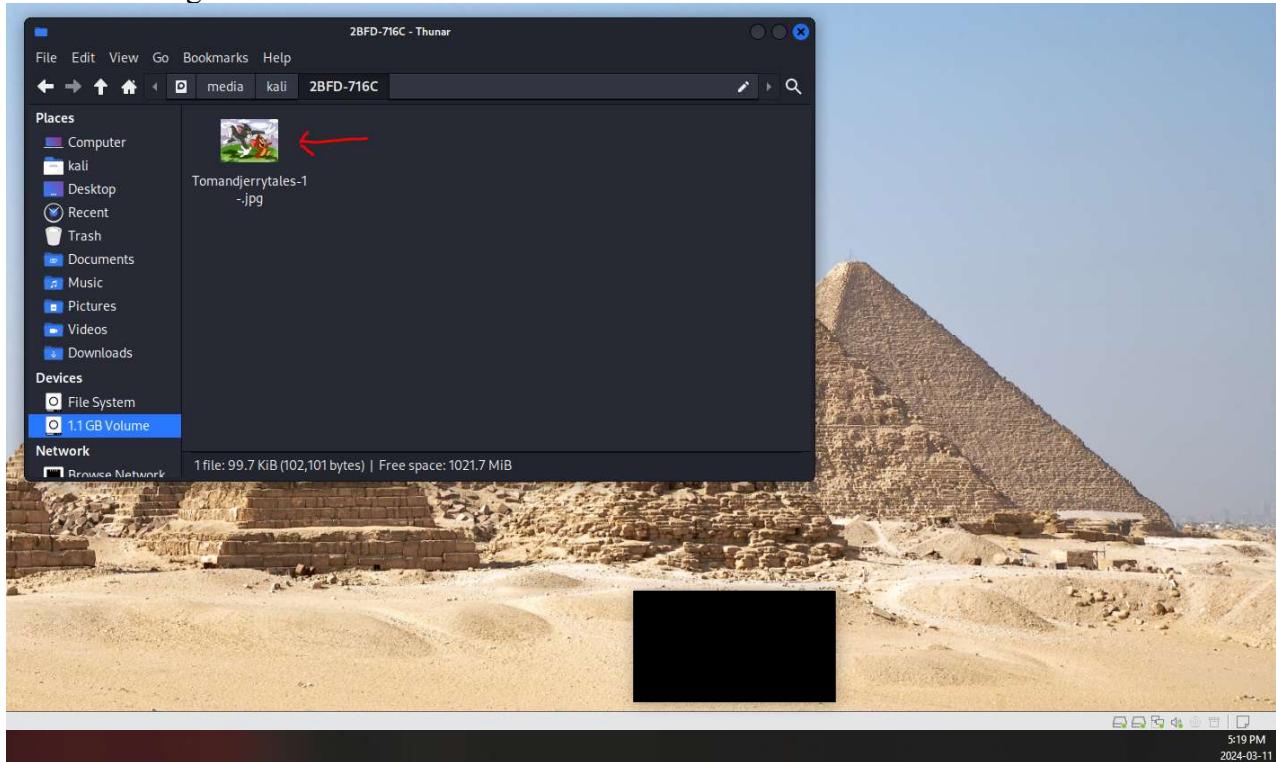
- Wipe the USB or the virtual storage.



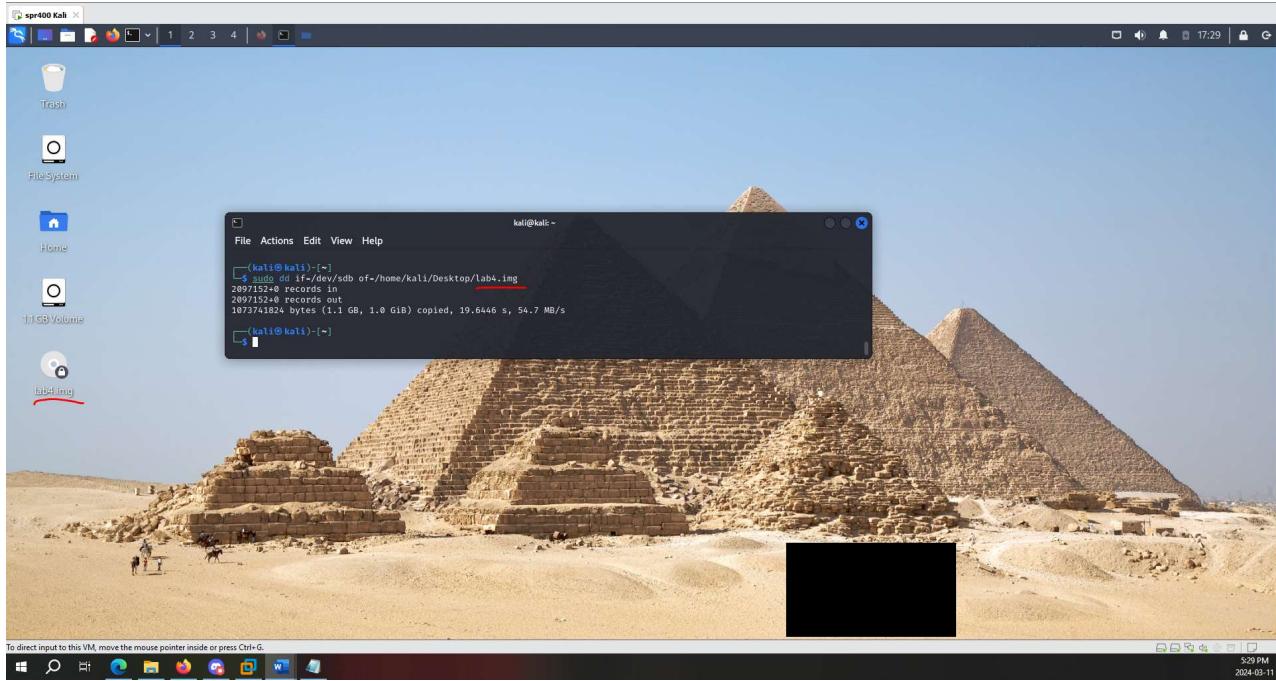
Then reformat or partition it again to FAT file system.



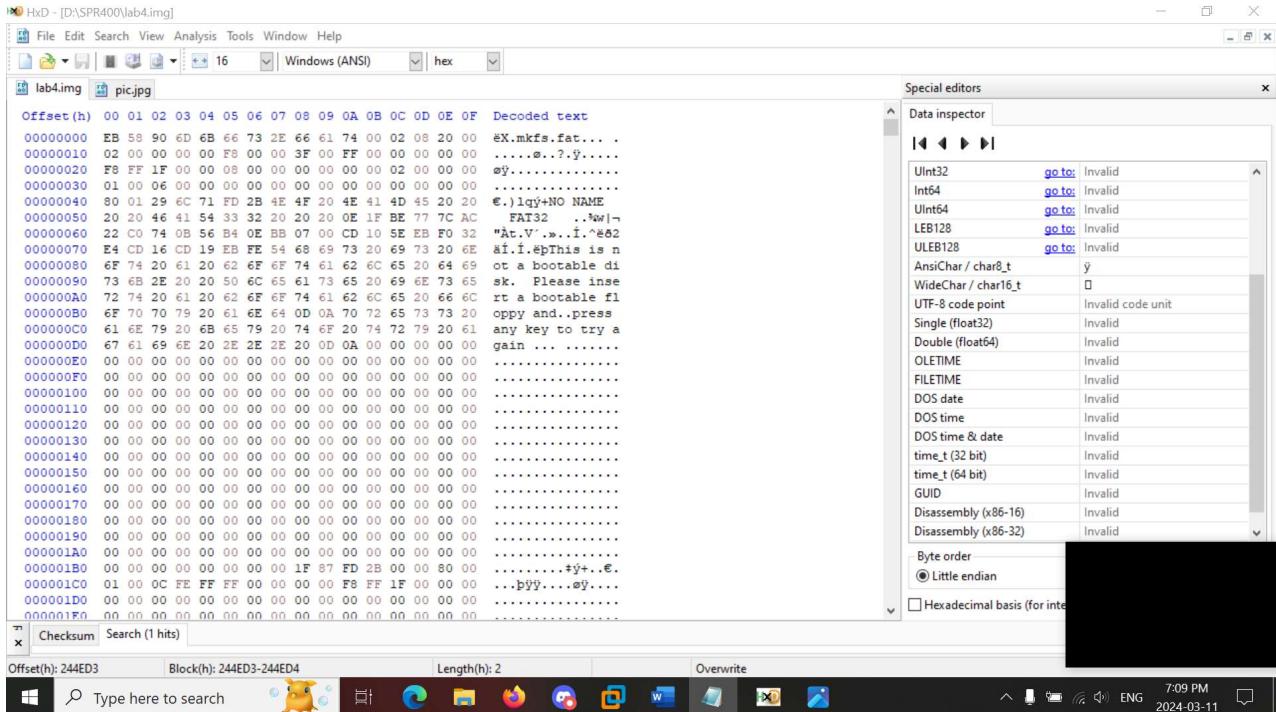
- Save only one JPEG file on the USB. So, your storage media has only one file in it and it is not fragmented.



- Connect the USB and start taking the image.

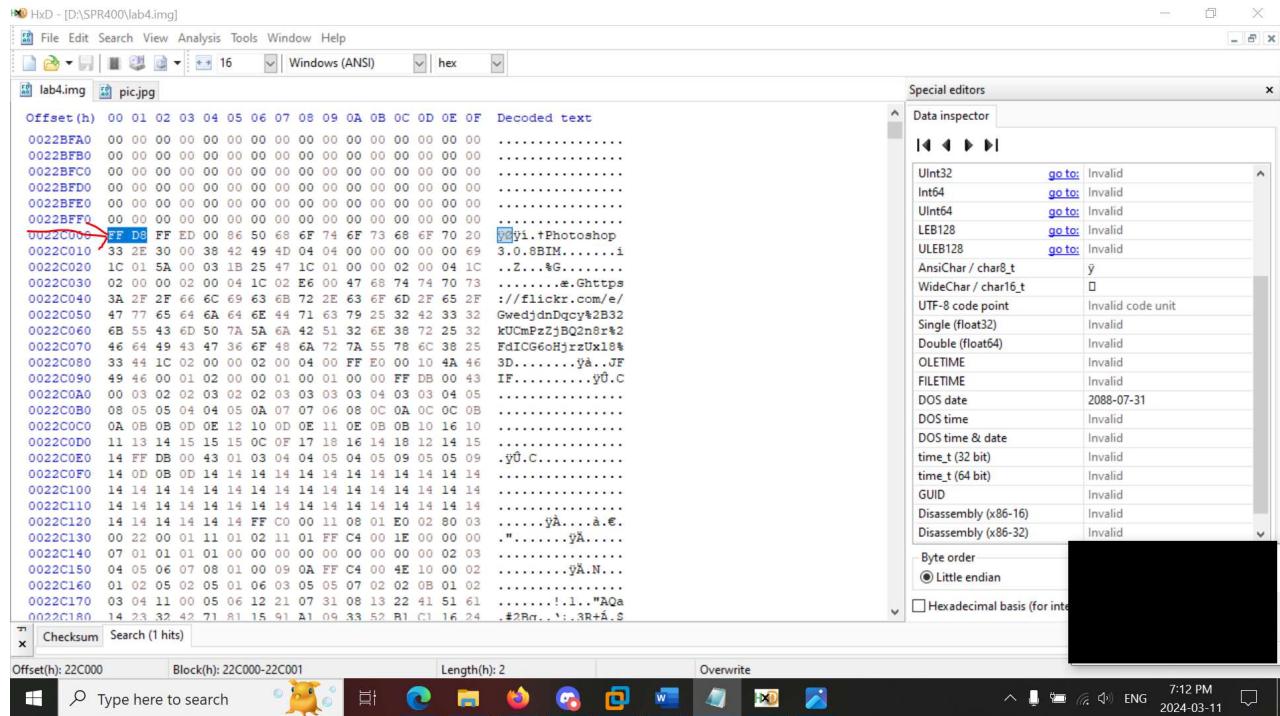


- Open the USB or virtual storage image in any hex editor.

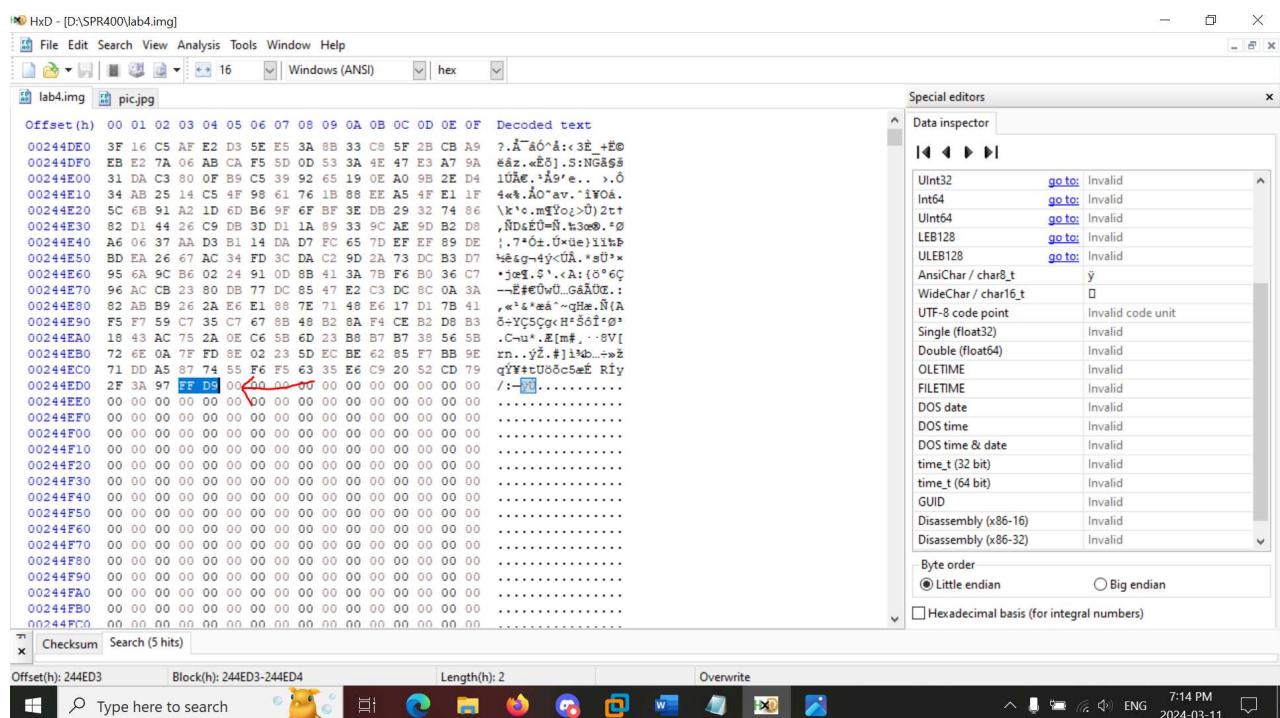


- Recover the file Header-Footer carving strategy.

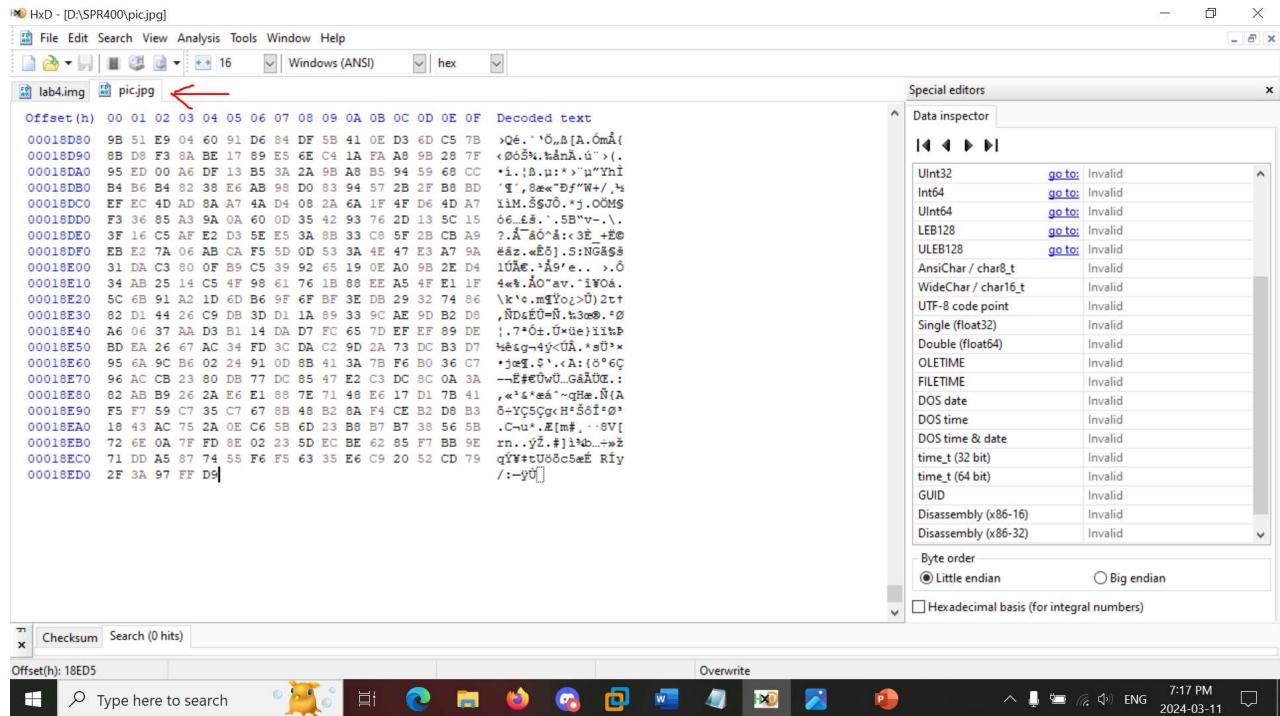
Header: FFD8 and



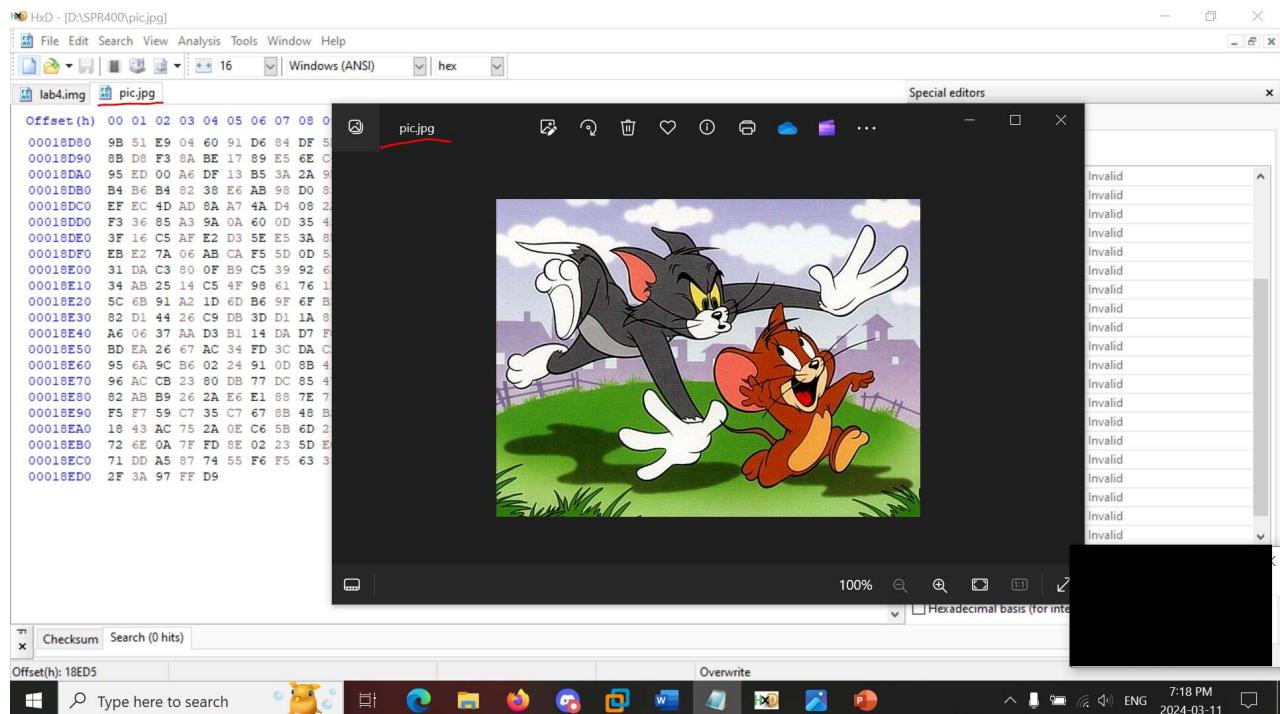
Footer: FFD9



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



Opening the image (pic.jpg)

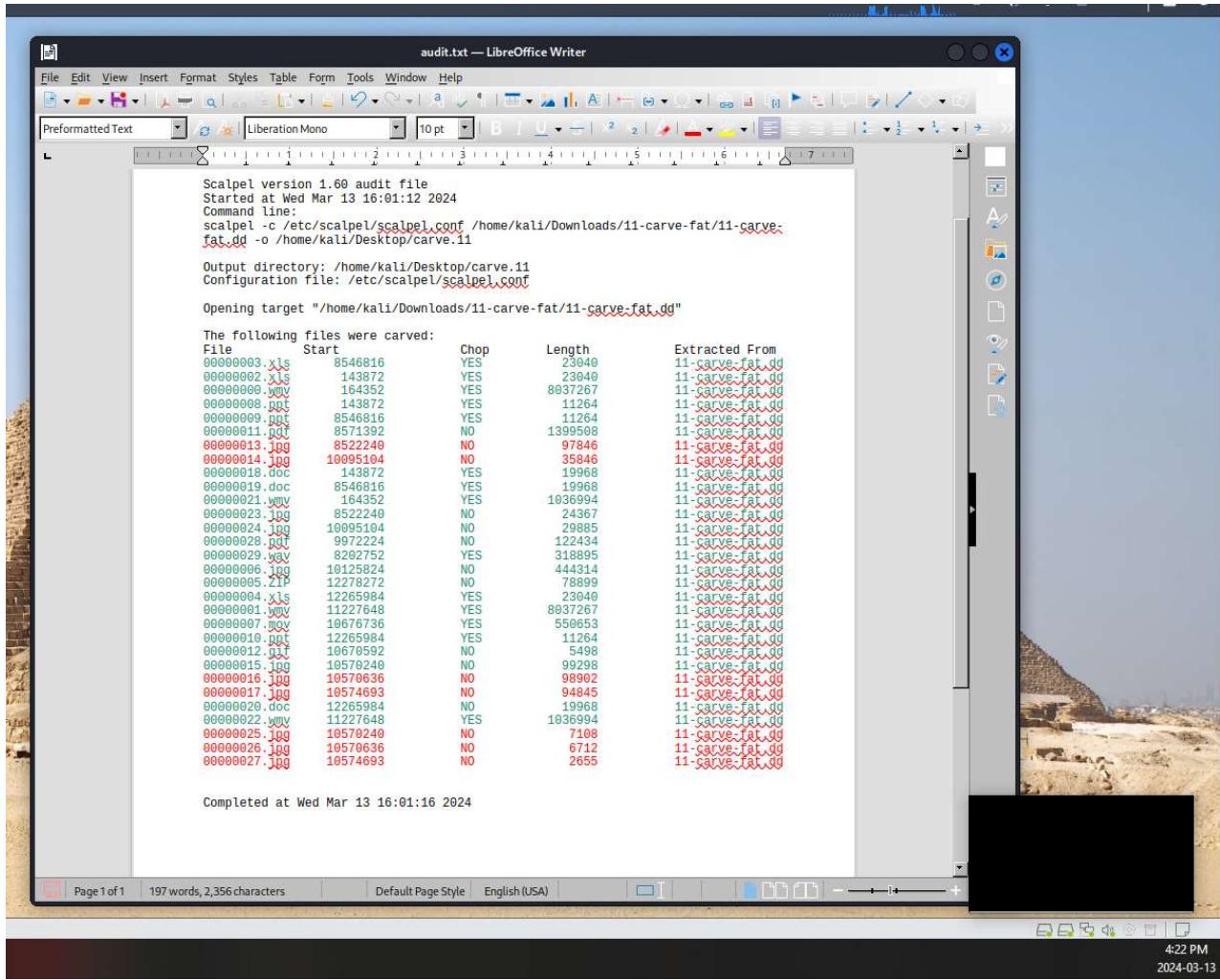


Part 2 -Scalpel

After installing Scalpel, I will carve test image 11 found at <http://dftt.sourceforge.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.



Scalpel version 1.60 audit file
Started at Wed Mar 13 16:01:12 2024
Command line:
scalpel -c /etc/scalpel.conf /home/kali/Downloads/11-carve-fat/11-carve-
fat.dd -o /home/kali/Desktop/carve.11
Output directory: /home/kali/Desktop/carve.11
Configuration file: /etc/scalpel/scalpel.conf
Opening target "/home/kali/Downloads/11-carve-fat/11-carve-fat.dd"
The following files were carved:

File	Start	Chop	Length	Extracted From
00000003.xls	8546816	YES	23040	11-carve-fat.dd
00000002.xls	143872	YES	23040	11-carve-fat.dd
00000009.wmv	164352	YES	8037267	11-carve-fat.dd
00000008.ppt	143872	YES	11264	11-carve-fat.dd
00000009.ppt	8546816	YES	11264	11-carve-fat.dd
00000011.ppt	8571392	NO	1399508	11-carve-fat.dd
00000013.jpg	8522248	NO	97846	11-carve-fat.dd
00000014.jpg	10095104	NO	35846	11-carve-fat.dd
00000018.doc	143872	YES	19968	11-carve-fat.dd
00000019.doc	8546816	YES	19968	11-carve-fat.dd
00000021.wmv	164352	YES	1036994	11-carve-fat.dd
00000023.jpg	8522248	NO	24367	11-carve-fat.dd
00000024.jpg	10095104	NO	29885	11-carve-fat.dd
00000028.xlsx	9972224	NO	122434	11-carve-fat.dd
00000029.wmv	8202752	YES	318895	11-carve-fat.dd
00000006.jpg	10125824	NO	444314	11-carve-fat.dd
00000005.zip	12278272	NO	78899	11-carve-fat.dd
00000004.xls	12265984	YES	23040	11-carve-fat.dd
00000001.wmv	11227648	YES	8037267	11-carve-fat.dd
00000007.wmv	10676736	YES	550653	11-carve-fat.dd
00000010.xls	12265984	YES	11264	11-carve-fat.dd
00000012.xlsx	10678592	NO	5498	11-carve-fat.dd
00000015.jpg	10578248	NO	99298	11-carve-fat.dd
00000016.jpg	10570636	NO	98902	11-carve-fat.dd
00000017.jpg	10574693	NO	94845	11-carve-fat.dd
00000029.doc	12265984	NO	19968	11-carve-fat.dd
00000022.wmv	11227648	YES	1036994	11-carve-fat.dd
00000025.jpg	10576240	NO	7108	11-carve-fat.dd
00000026.jpg	10570636	NO	6712	11-carve-fat.dd
00000027.jpg	10574693	NO	2655	11-carve-fat.dd

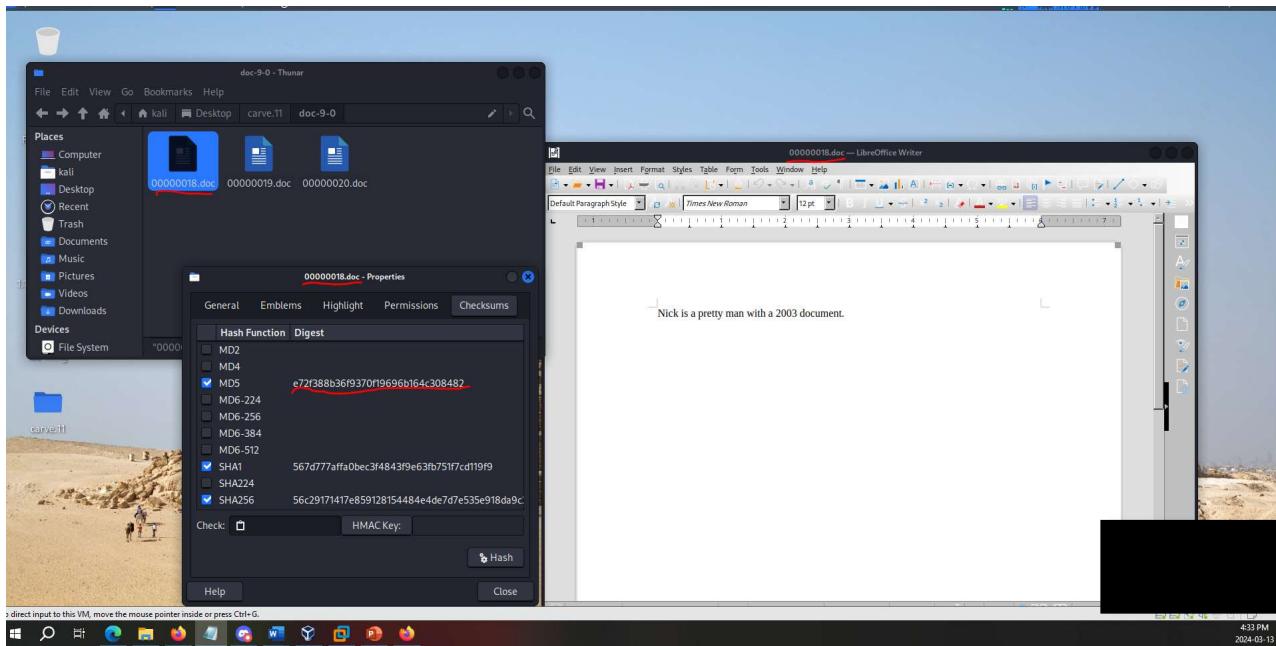
Completed at Wed Mar 13 16:01:16 2024

Page 1 of 1 | 197 words, 2,356 characters | Default Page Style | English (USA) | | 4:22 PM | 2024-03-13

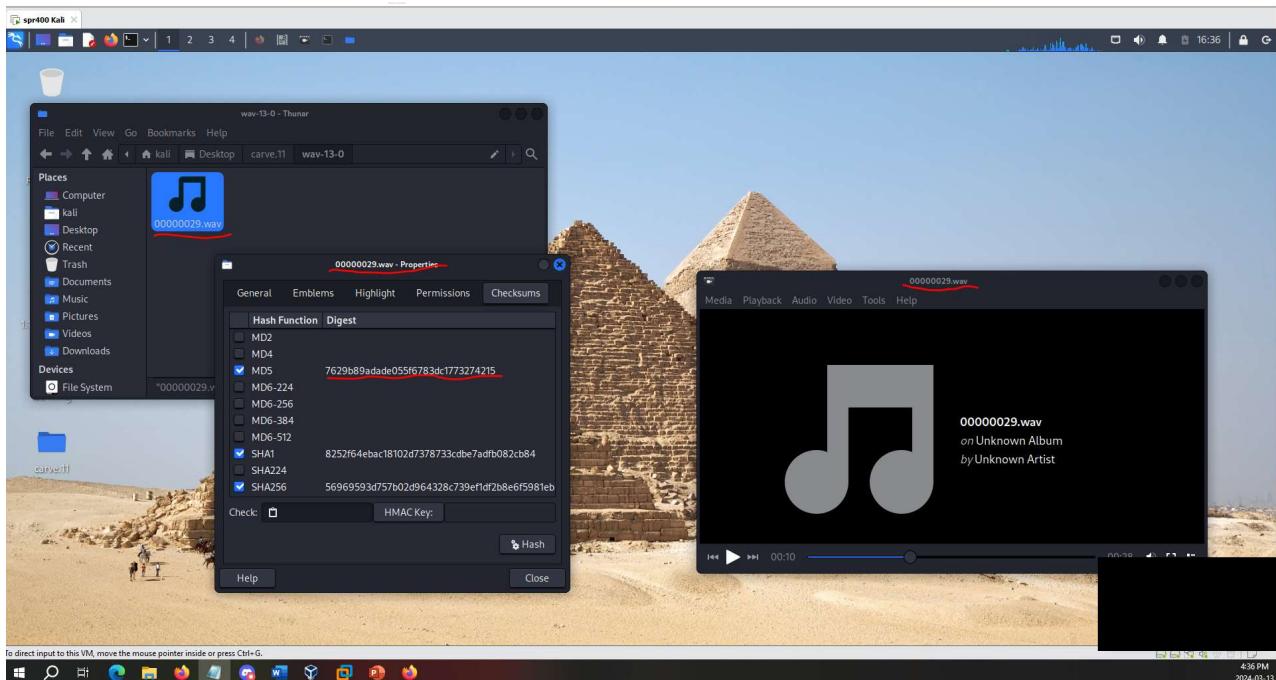
Files Recovered

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

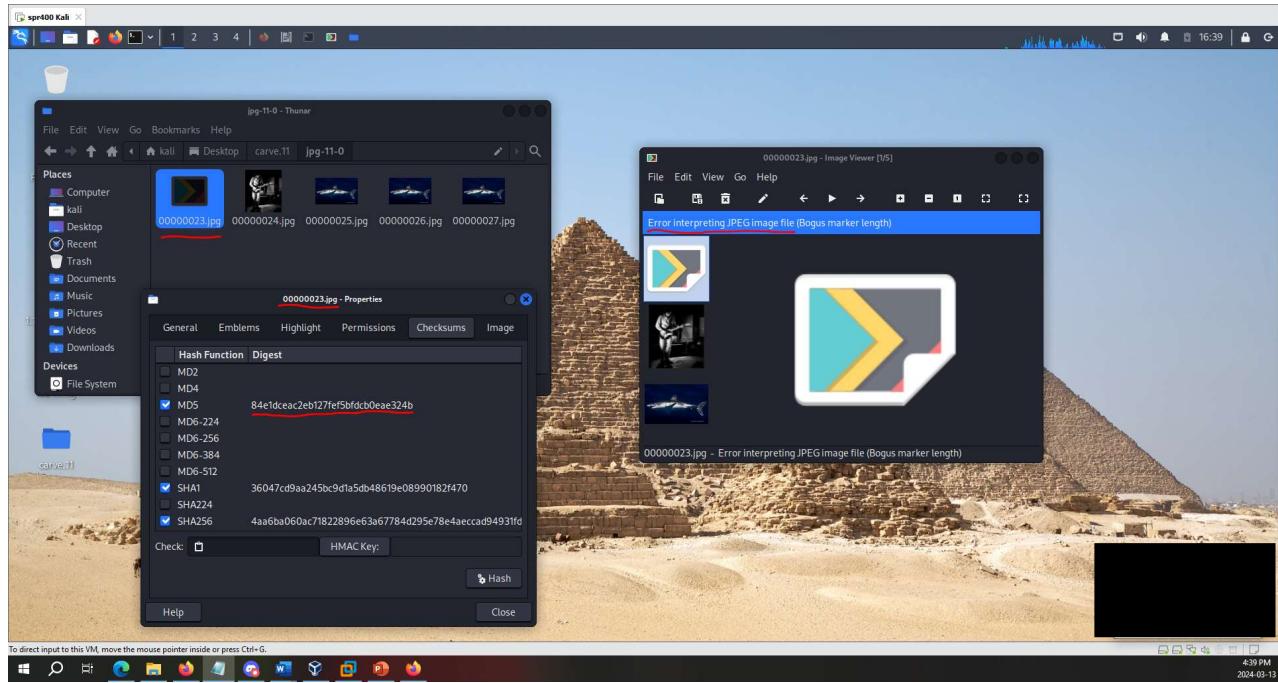
2003_document.doc



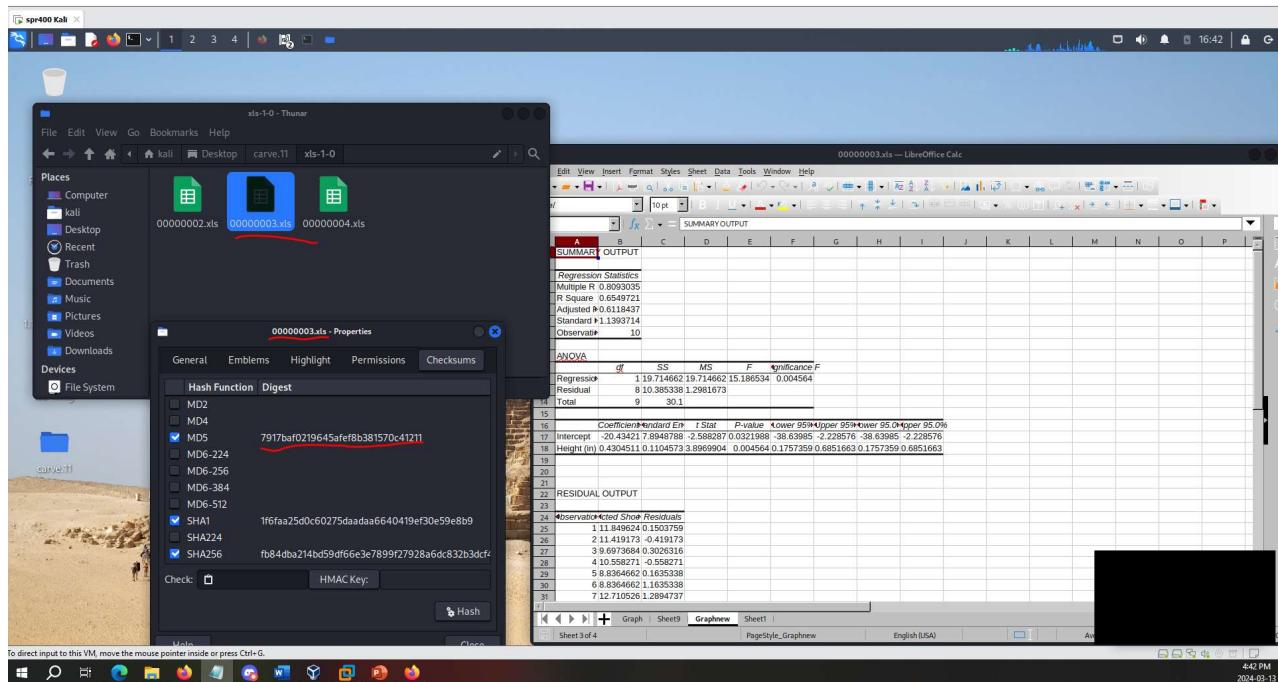
enterprise.wav



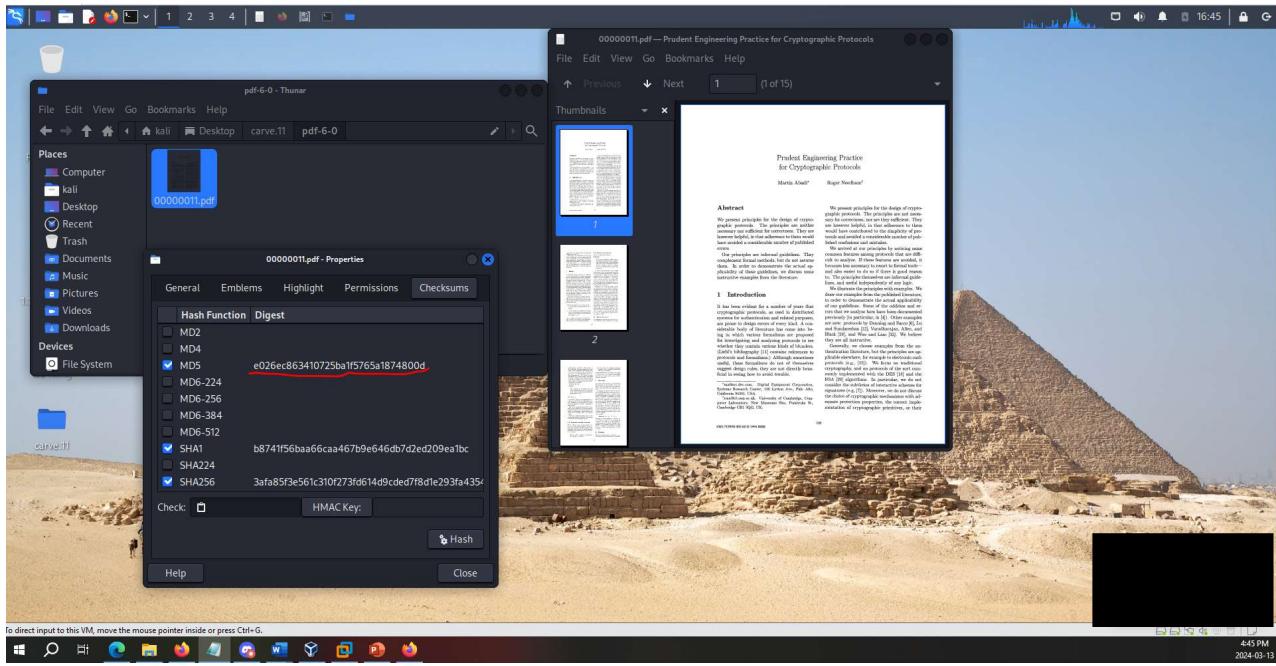
haxor2.jpg (invalid JPEG)



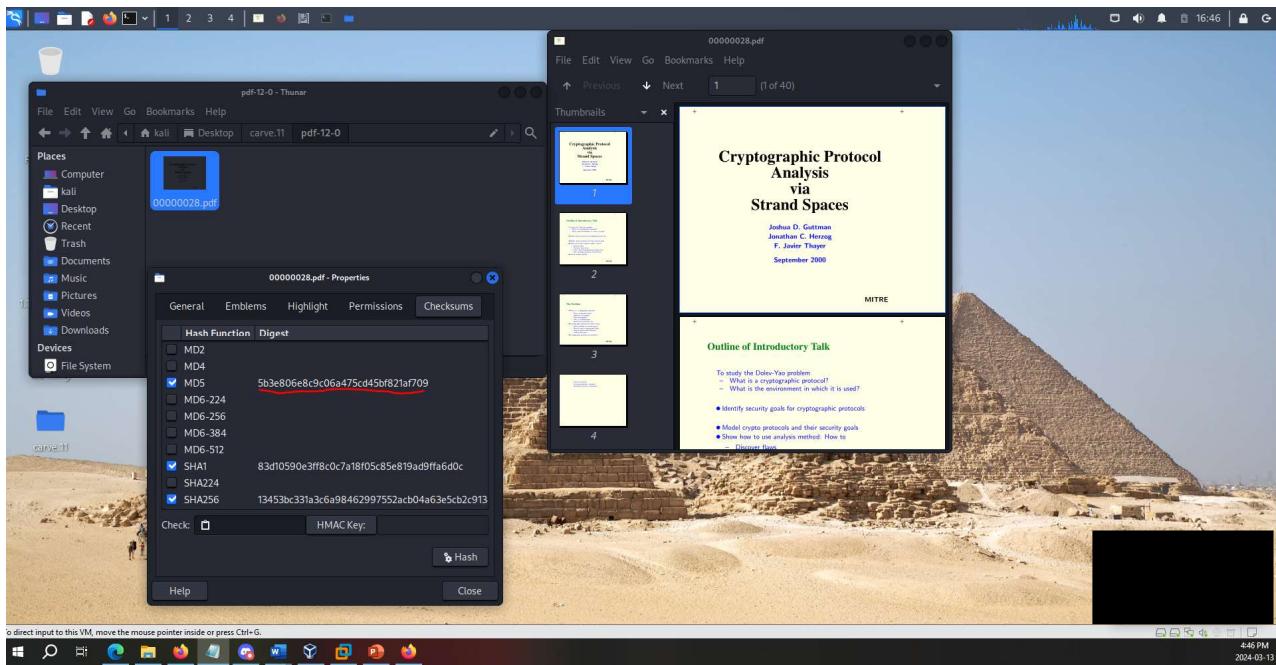
holly.xls



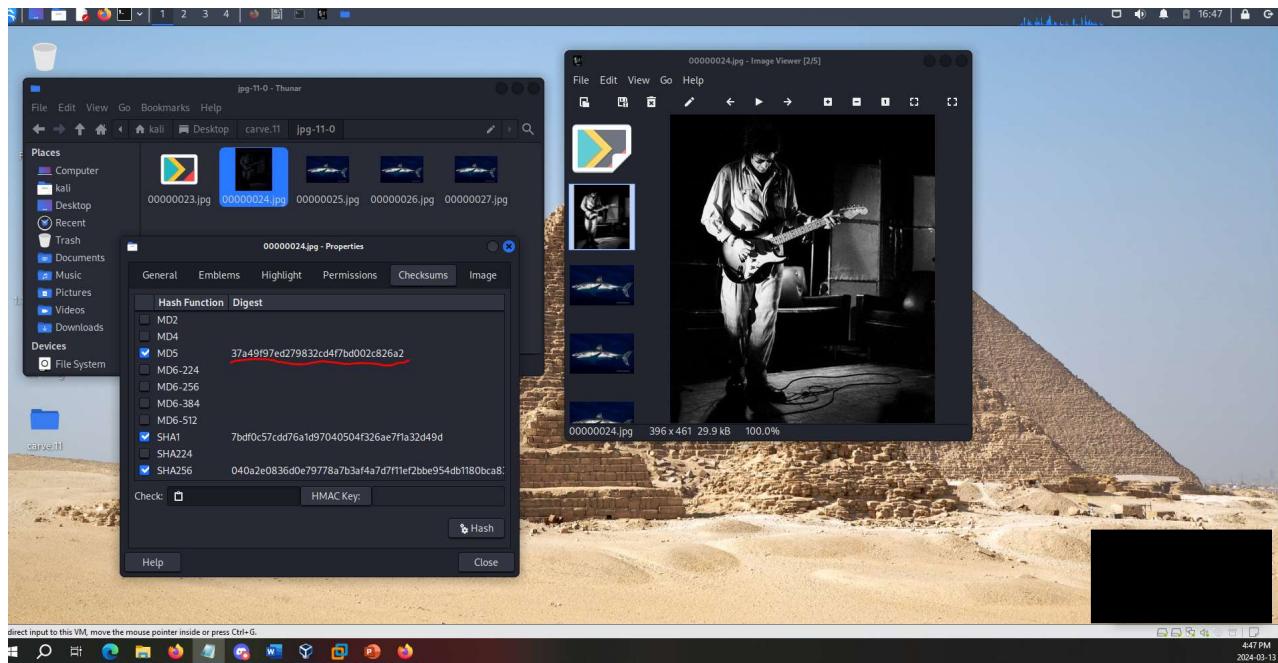
lin_1.2.pdf



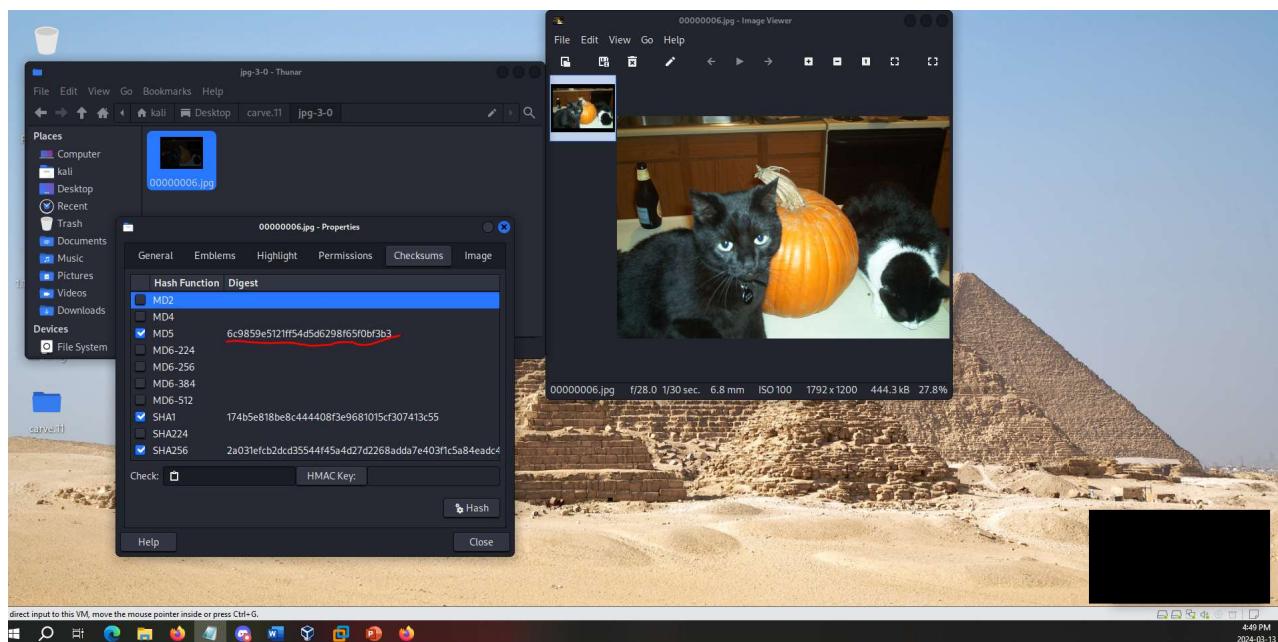
nlin_14.pdf



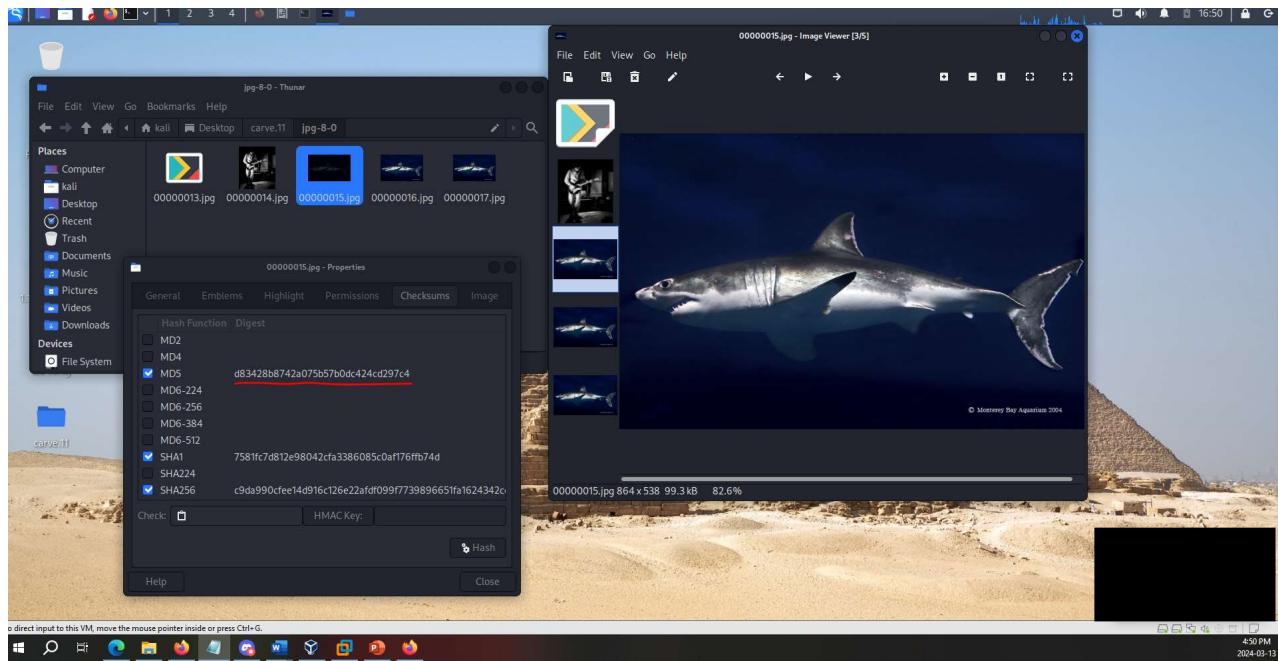
paul.jpg



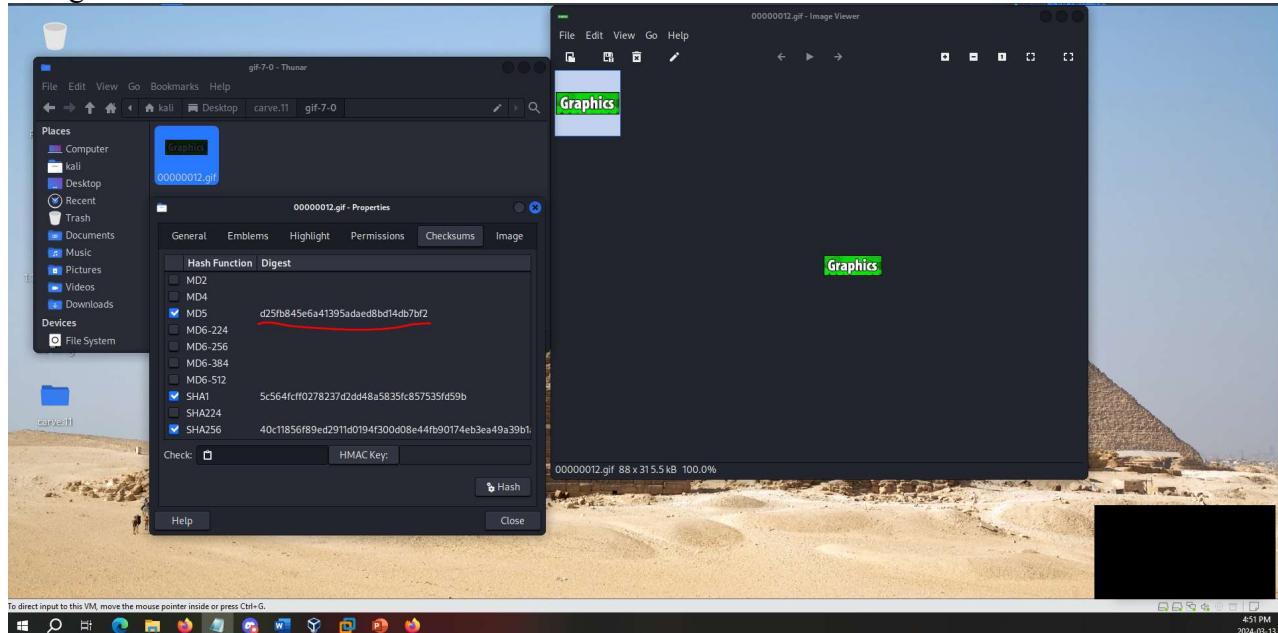
pumpkin.jpg



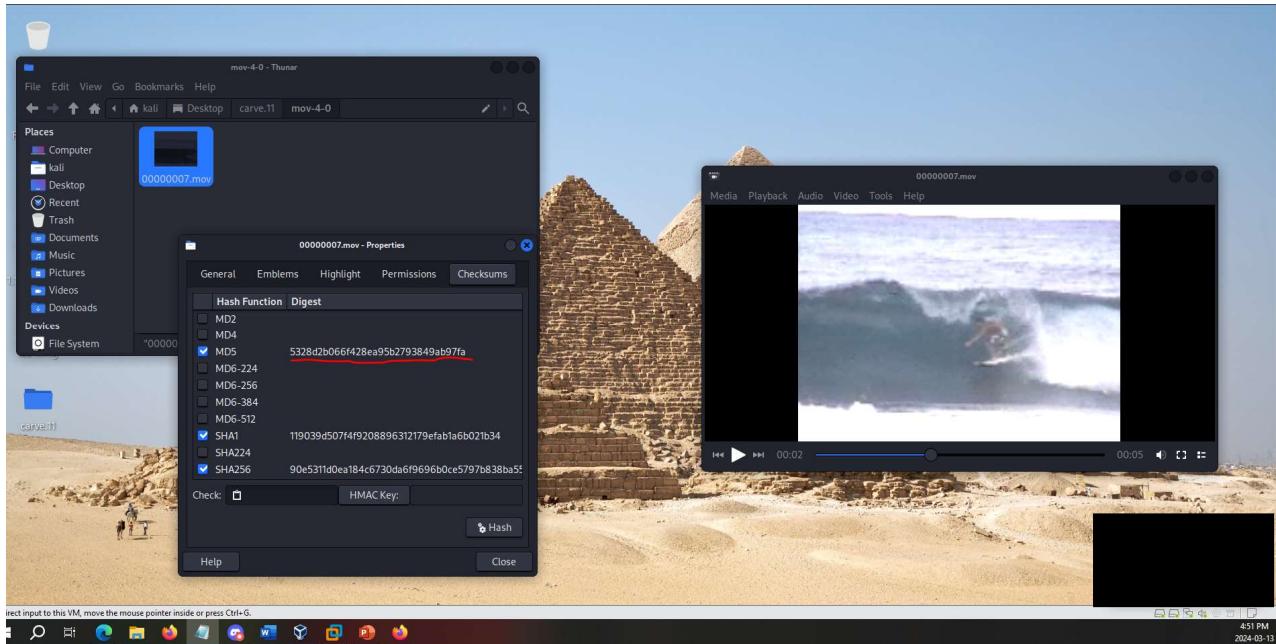
shark.jpg



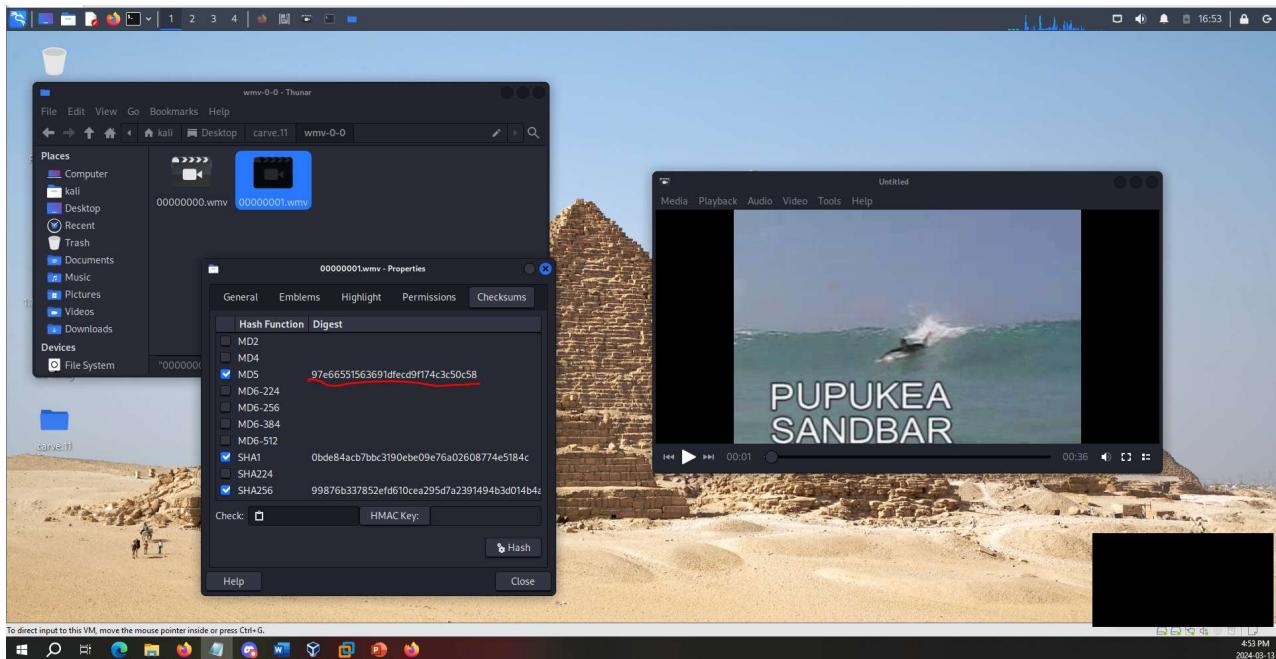
sm1.gif



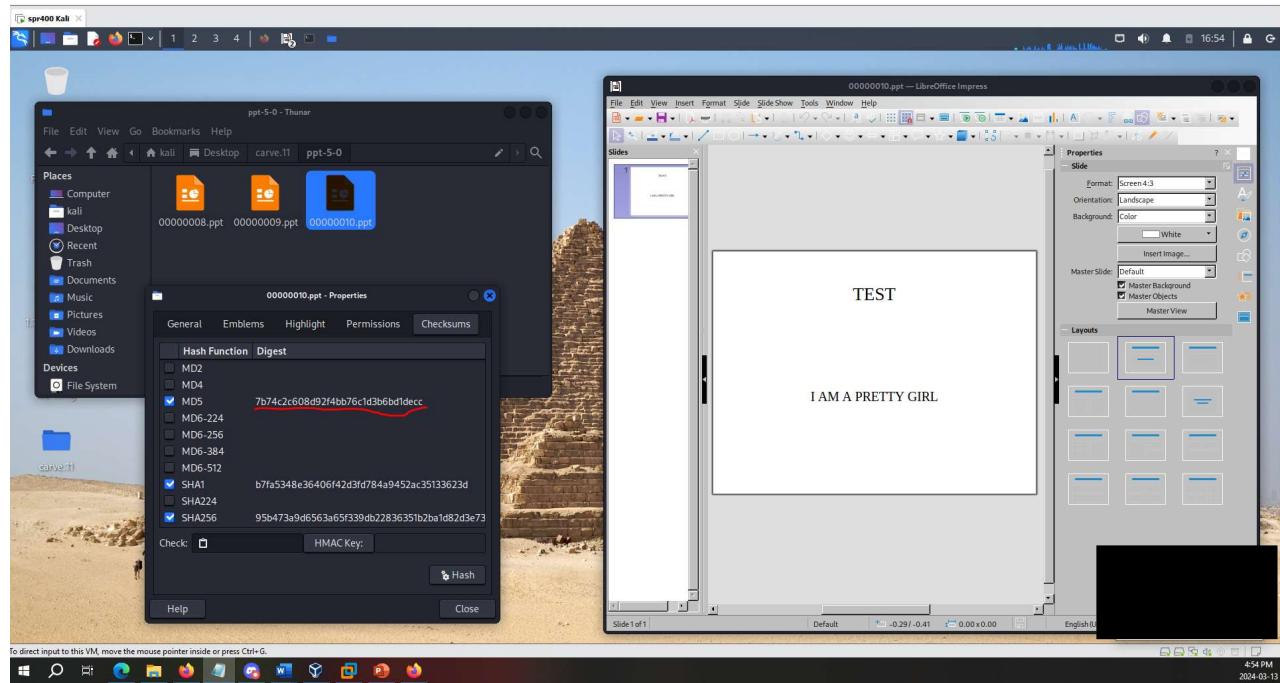
surf.mov



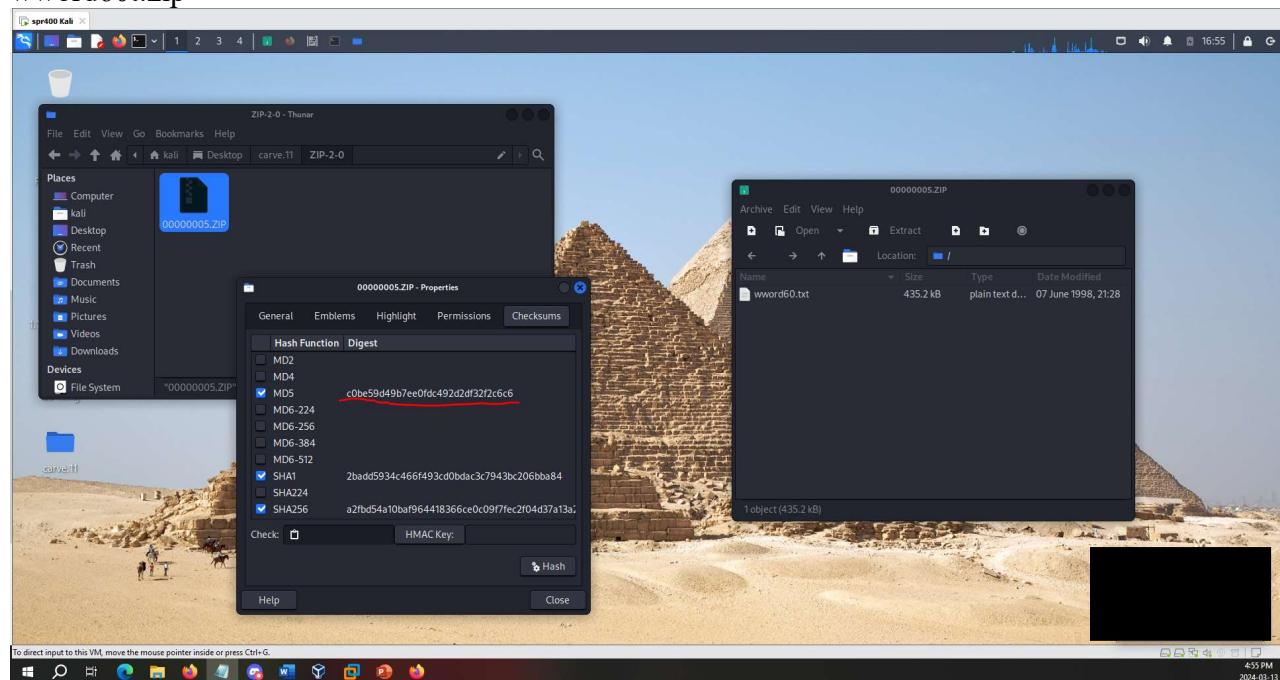
surf.wmv



test.ppt



wword60t.zip



domopers.wmv

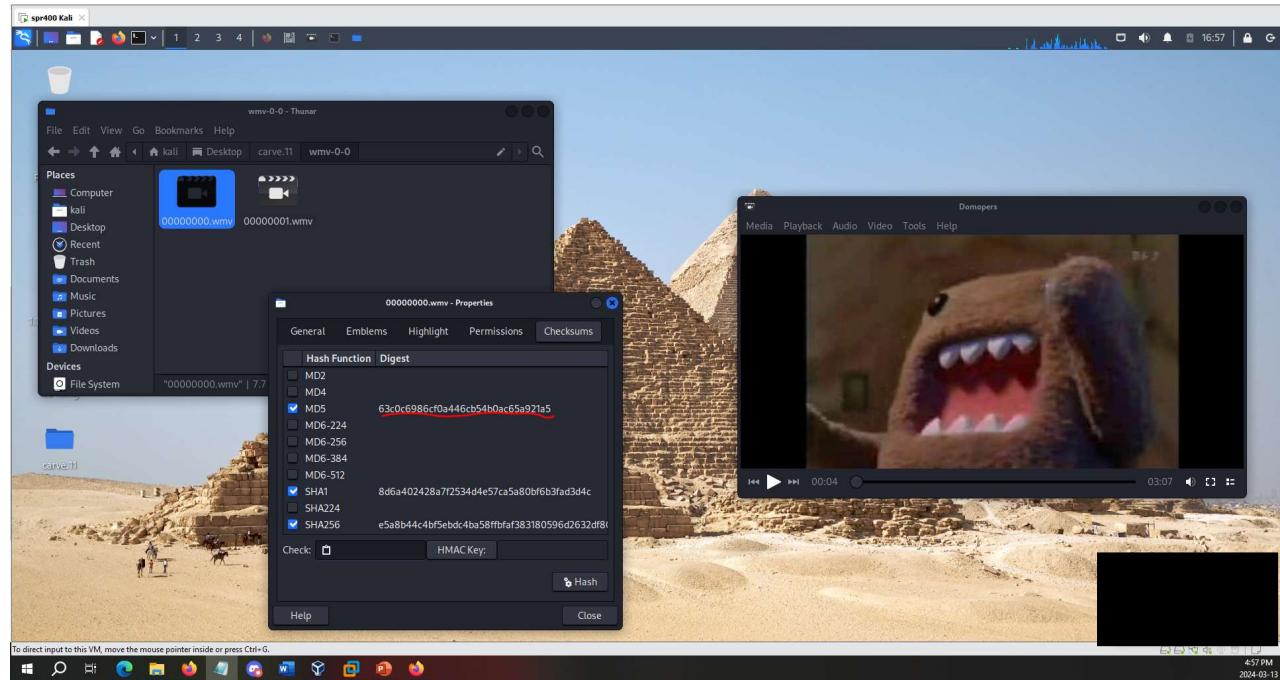


Table listing the recovered/not recovered files.

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	