

Họ và tên: Trần Trí Dũng

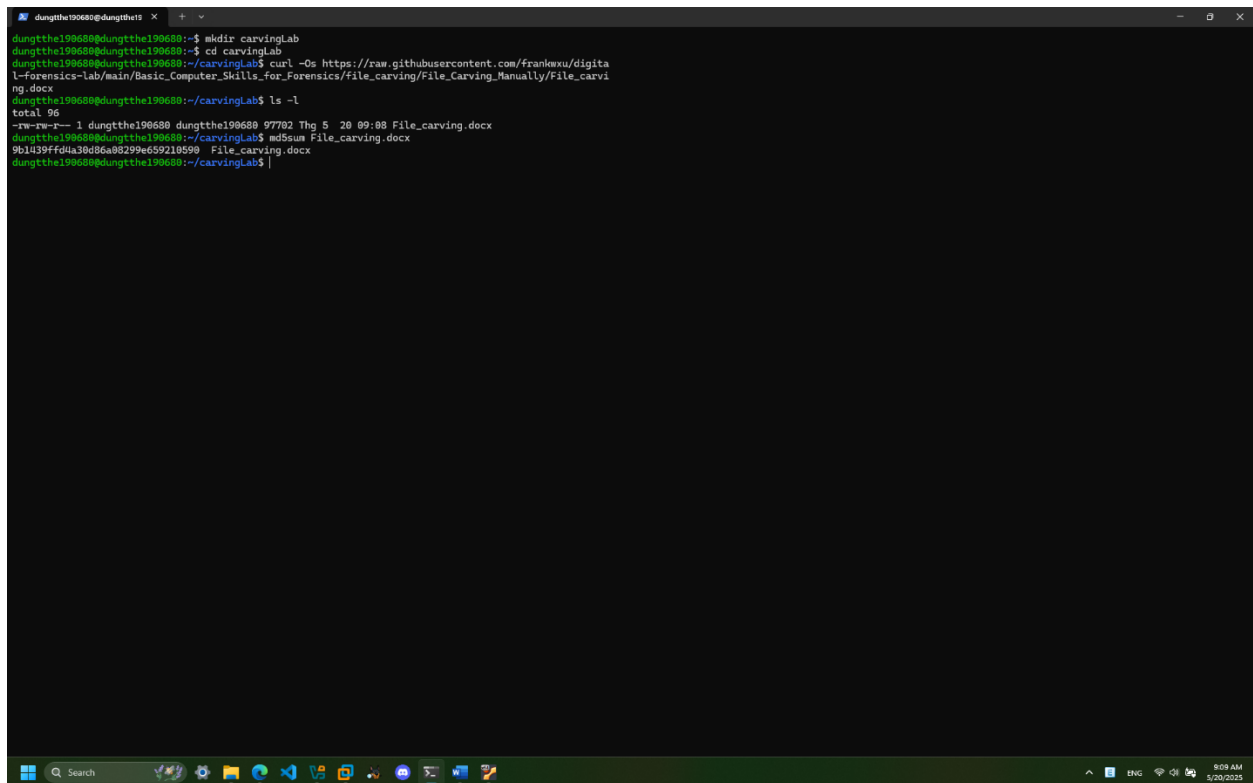
Mã số sinh viên: HE190680

Lớp: IA1901

Lab 2: Data Carving

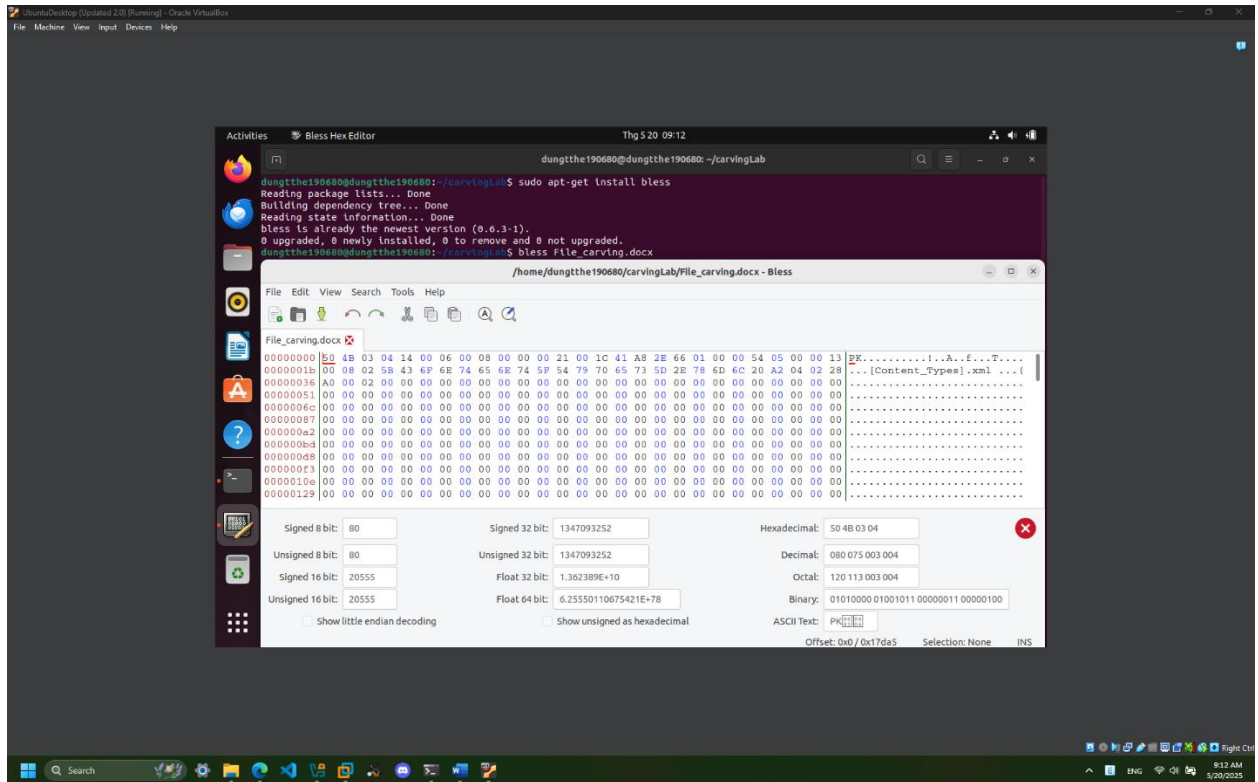
1. Extracting images from a corrupted Word document

Step 1:

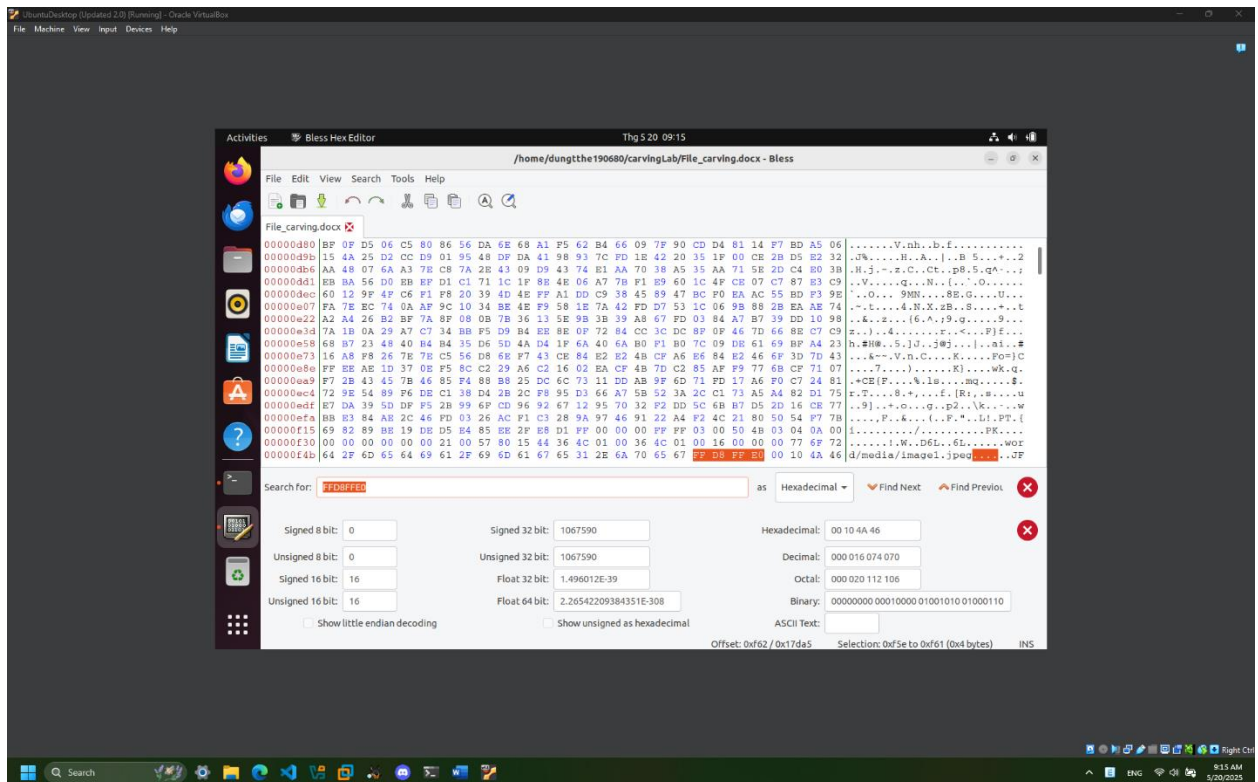


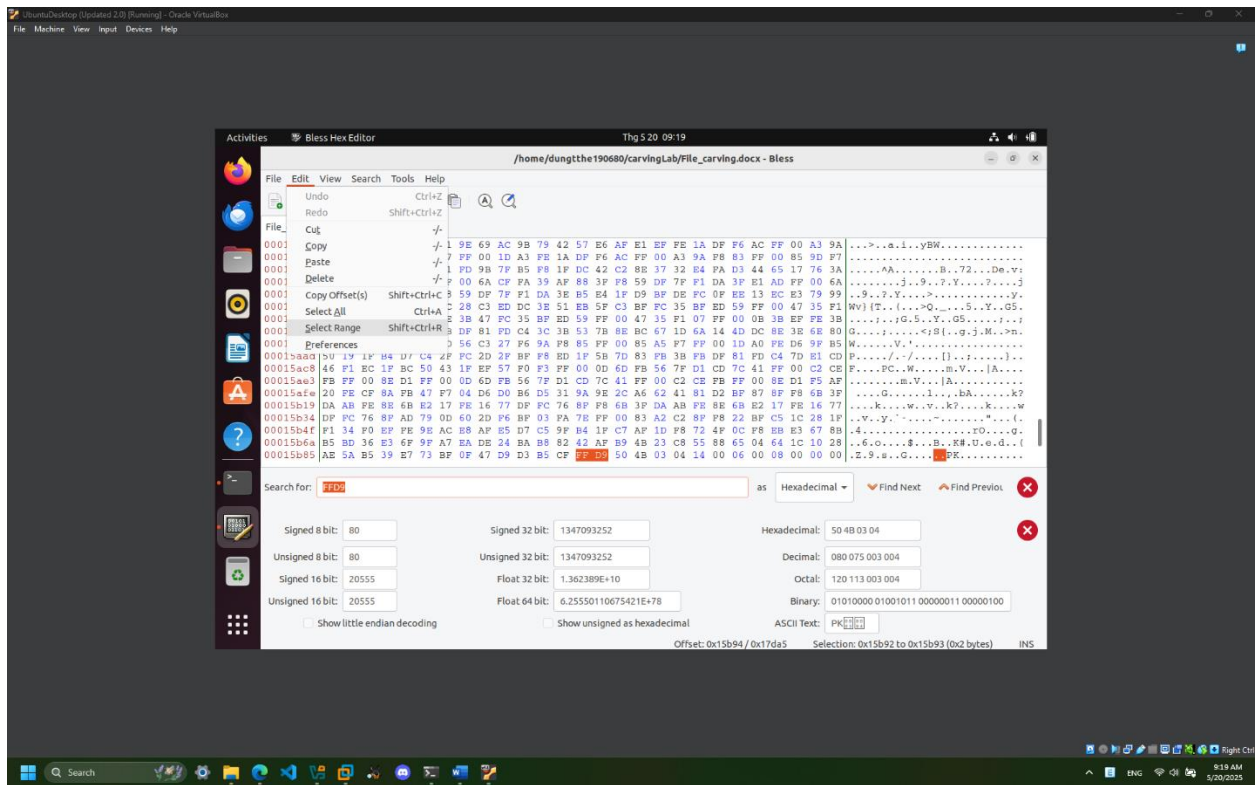
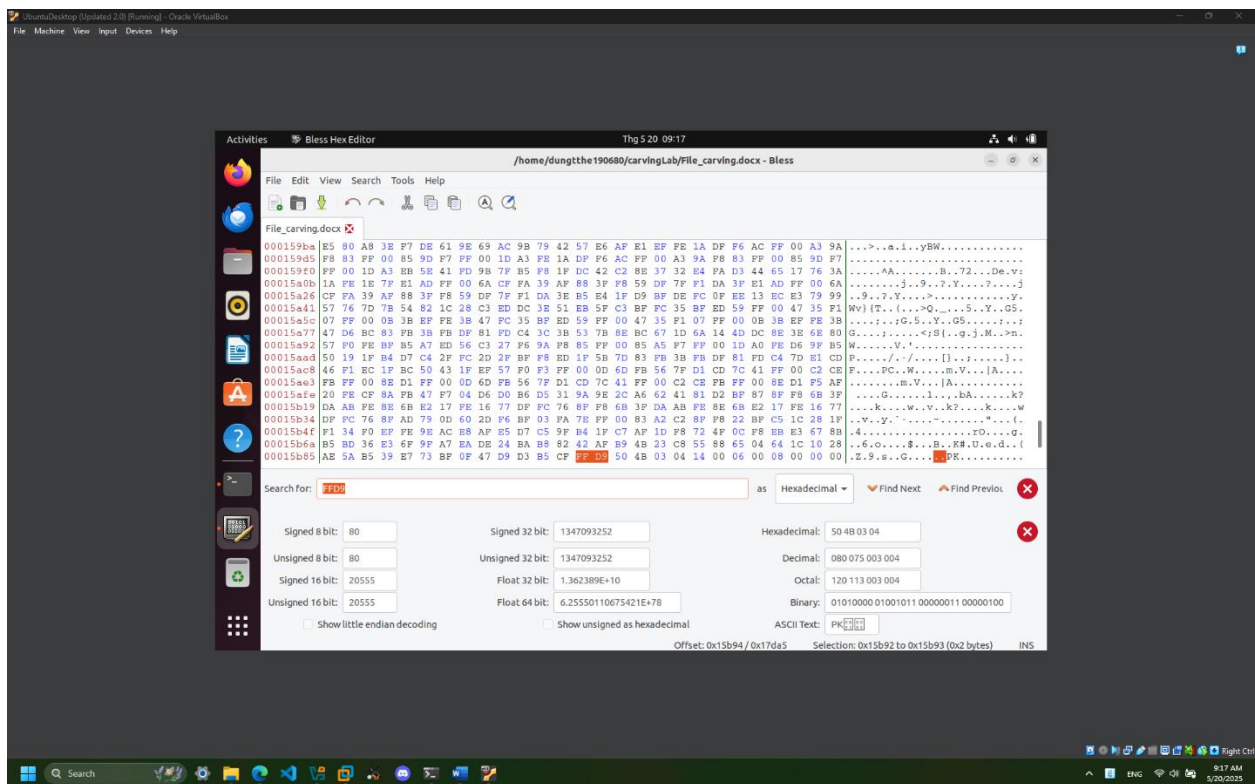
```
dungtthe190680@dungtthe190680:~$ mkdir carvingLab
dungtthe190680@dungtthe190680:~$ cd carvingLab
dungtthe190680@dungtthe190680:~/carvingLab$ curl -Os https://raw.githubusercontent.com/frankexu/digital-forensics-lab/main/Basic_Computer_Skills_for_Forensics/file_carving/File_Carving_Manually/File_carving.docx
dungtthe190680@dungtthe190680:~/carvingLab$ ls -l
total 96
-rw-rw-r-- 1 dungtthe190680 dungtthe190680 97782 Thg 5  20 09:08 File_carving.docx
dungtthe190680@dungtthe190680:~/carvingLab$ md5sum File_carving.docx
9b1d39ffdua3b8d6a8299e459210599  File_carving.docx
dungtthe190680@dungtthe190680:~/carvingLab$
```

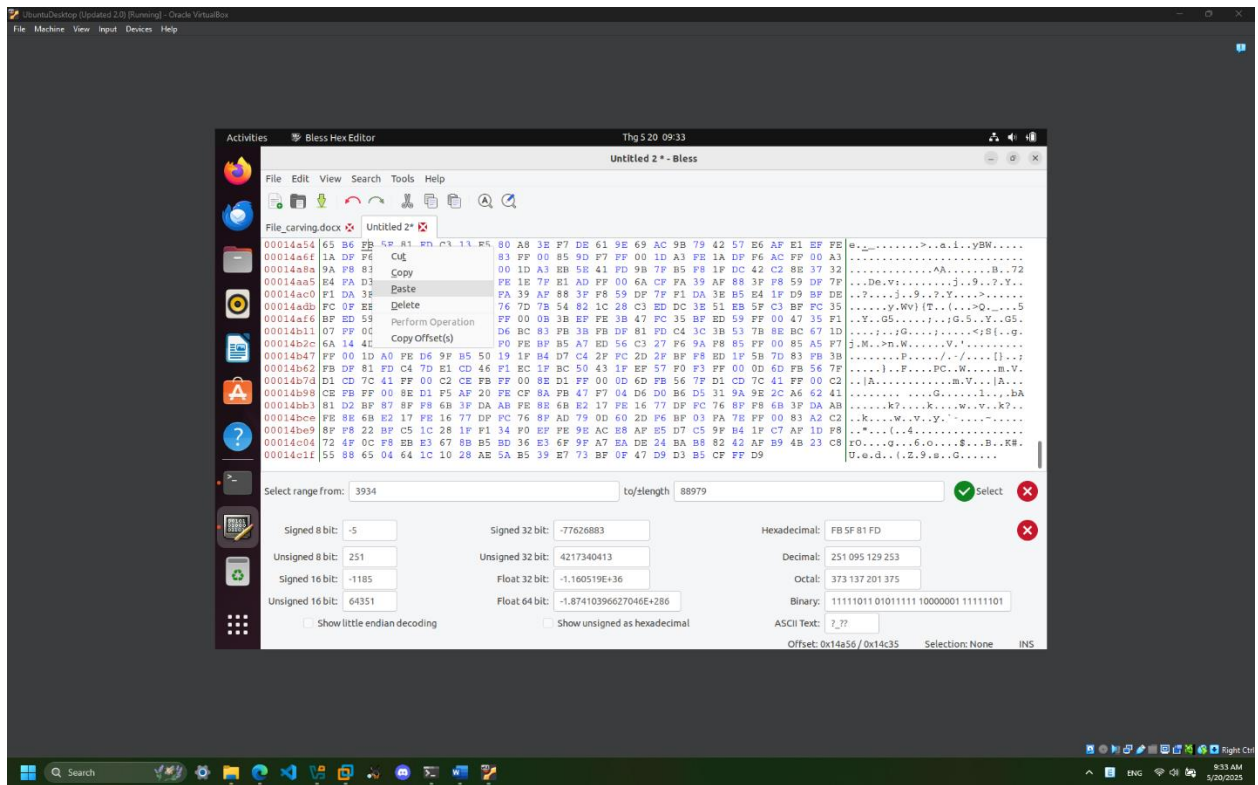
Step 2:

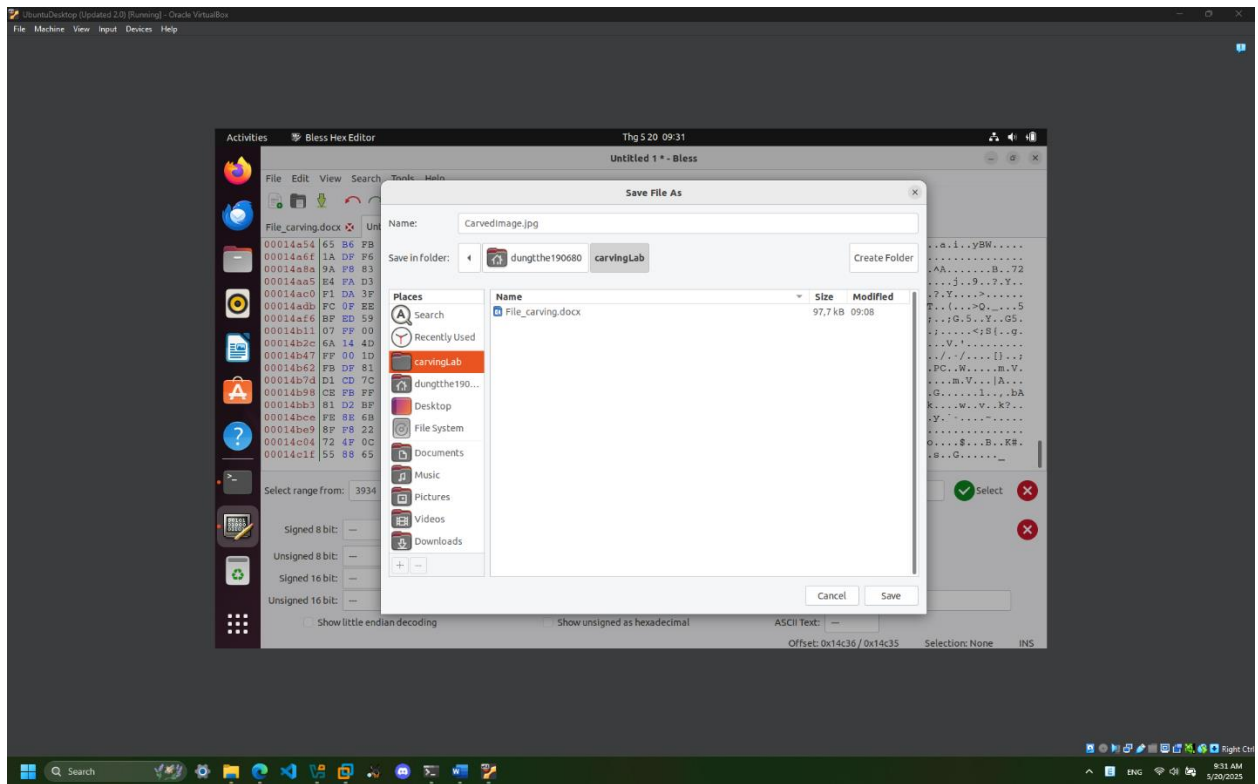


Step 3:

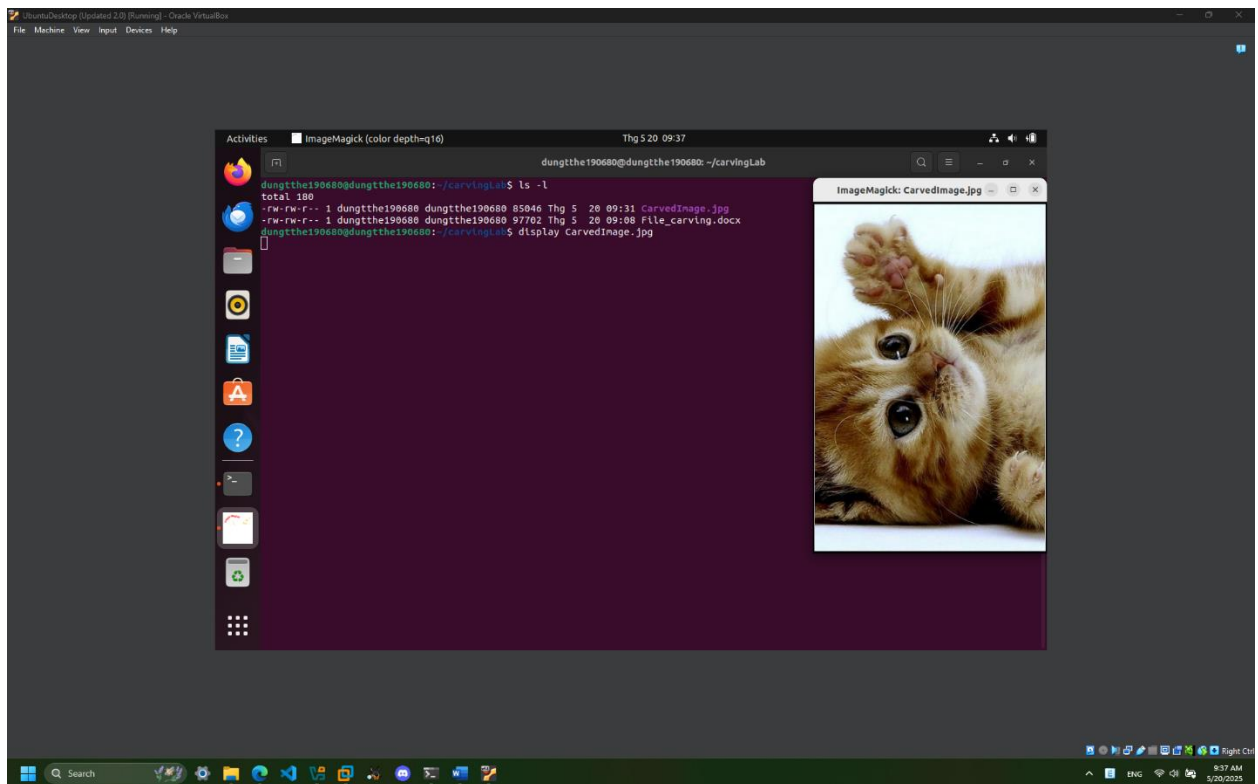








Step 4:



2. Carving/Recovering a USB image – Step 1 + 2:

```
dungthe190680@dungthe19: ~$ curl -O https://raw.githubusercontent.com/frankxuxi/digital-forensics-lab/main/Basic_Computer_Skills_for_Forensics/file_carving/usb_image/120M.7z
dungthe190680@dungthe19: ~$ ls -l 120M.7z
-rw-rw-r-- 1 dungthe190680 dungthe190680 36720470 Thg 5 20 09:47 120M.7z
dungthe190680@dungthe19: ~$ hashdeep -c md5,sha1 120M.7z
#### HASHDEEP-1.0
#### size,md5,sha1,filename
## Invoked from: /home/dungthe190680/carvingLab
## $ hashdeep -c md5,sha1 120M.7z
36720470,dfe7b5d4e54cd1bf50d5d5f47aceeb3c,2010745018afaa2da3d1c17a8eb590fca66eeef7,/home/dungthe190680/carvingLab/120M.7z
dungthe190680@dungthe19: ~$ 7z l 120M.7z
7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=non,HugeFiles=on,64 bits,12 CPUs 13th Gen Intel(R) Core(TM) i5-13400P (B06A2),ASM,AES-NI)

Scanning the drive for archives:
1 file, 36720470 bytes (36 MiB)

Listing archive: 120M.7z
--
Path = 120M.7z
Type = 7z
Physical Size = 36720470
Headers Size = 214
Method = LZMA2:24
Solid = +
Blocks = 1

Date       Time      Attr      Size  Compressed  Name
-----
2021-09-23 09:59:31 D...A      0         0  120M
2021-09-23 09:59:31 ....A 124780544 36720256 120M/usb_fat_carving.001
2021-09-23 09:59:32 ....A 1685      120M/usb_fat_carving.001.txt
--
2021-09-23 09:59:32      124782229 36720256 2 files, 1 folders
dungthe190680@dungthe19: ~$ 7z e 120M.7z
7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=non,HugeFiles=on,64 bits,12 CPUs 13th Gen Intel(R) Core(TM) i5-13400P (B06A2),ASM,AES-NI)

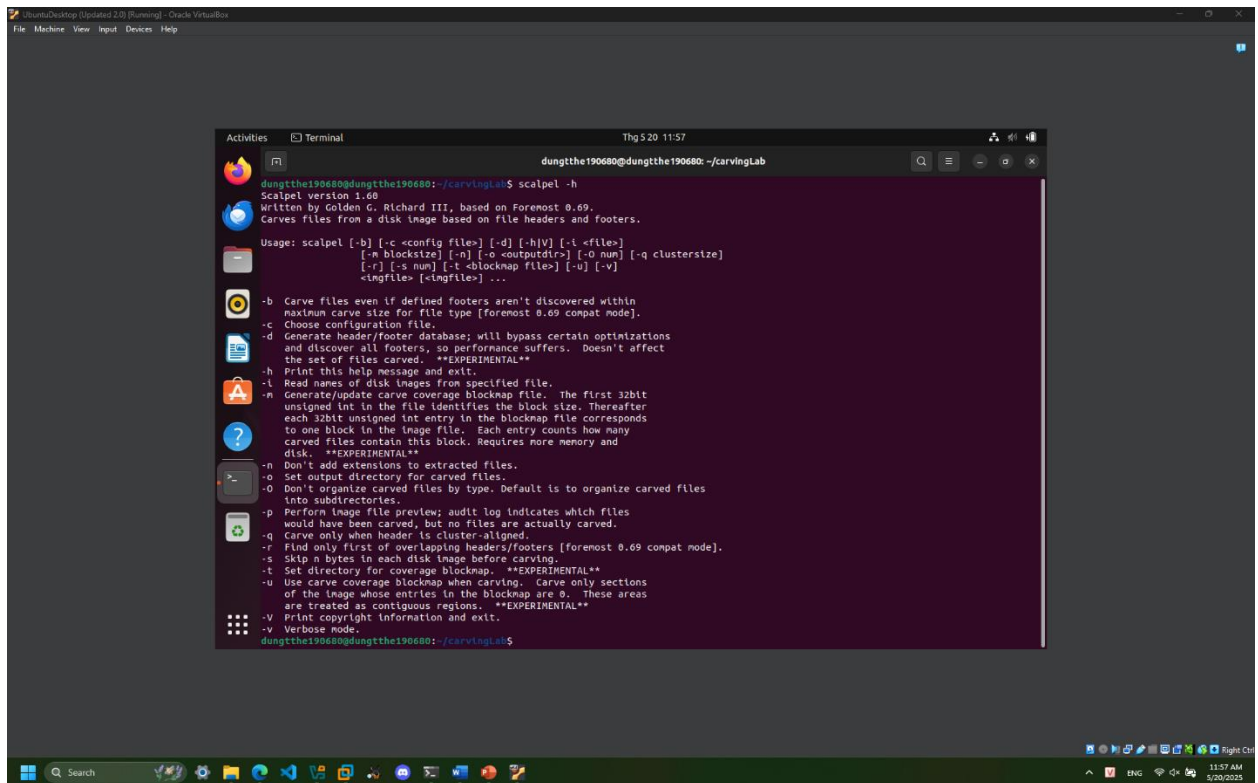
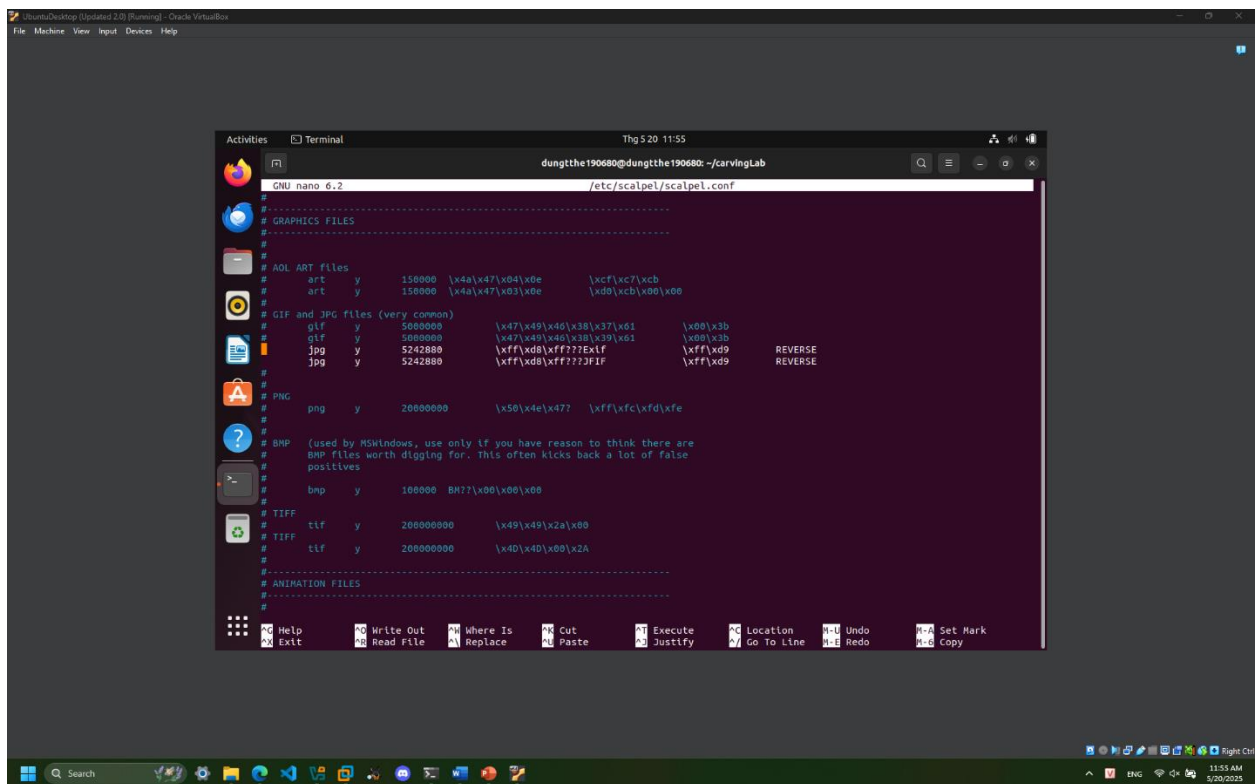
Scanning the drive for archives:
1 file, 36720470 bytes (36 MiB)

Extracting archive: 120M.7z
--
Path = 120M.7z
Type = 7z
Physical Size = 36720470
Headers Size = 214
Method = LZMA2:24
Solid = +
Blocks = 1

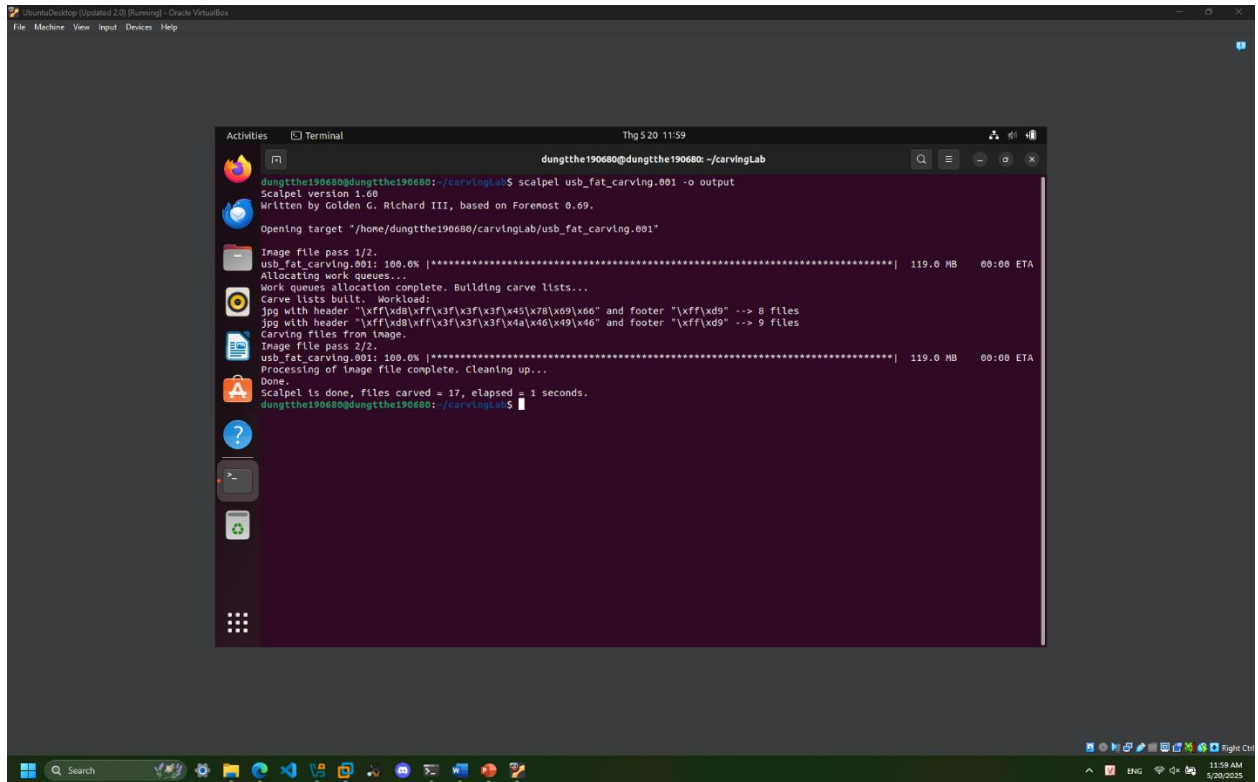
Everything is Ok

Folders: 1
Files: 2
Size:      124782229
Compressed: 36720470
dungthe190680@dungthe19: ~$ hashdeep -c md5,sha1 usb_fat_carving.001
#### HASHDEEP-1.0
#### size,md5,sha1,filename
## Invoked from: /home/dungthe190680/carvingLab
## $ hashdeep -c md5,sha1 usb_fat_carving.001
##
124780544,b8a1d0b8a49f4a6667b00a3b3e85e604,bcc2d09fd49c9521ecb1739f6542c6bf327375ef,/home/dungthe190680/carvingLab/usb_fat_carving.001
dungthe190680@dungthe19: ~$ cat usb_fat_carving.001.txt | grep "checksum"
MD5 checksum: b8a1d0b8a49f4a6667b00a3b3e85e604
SHA1 checksum: bcc2d09fd49c9521ecb1739f6542c6bf327375ef
MD5 checksum: b8a1d0b8a49f4a6667b00a3b3e85e604 : verified
SHA1 checksum: bcc2d09fd49c9521ecb1739f6542c6bf327375ef : verified
dungthe190680@dungthe19: ~$ fdisk -l usb_fat_carving.001
Disk usb_fat_carving.001: 119 MiB, 124780544 bytes, 243712 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x1159a00

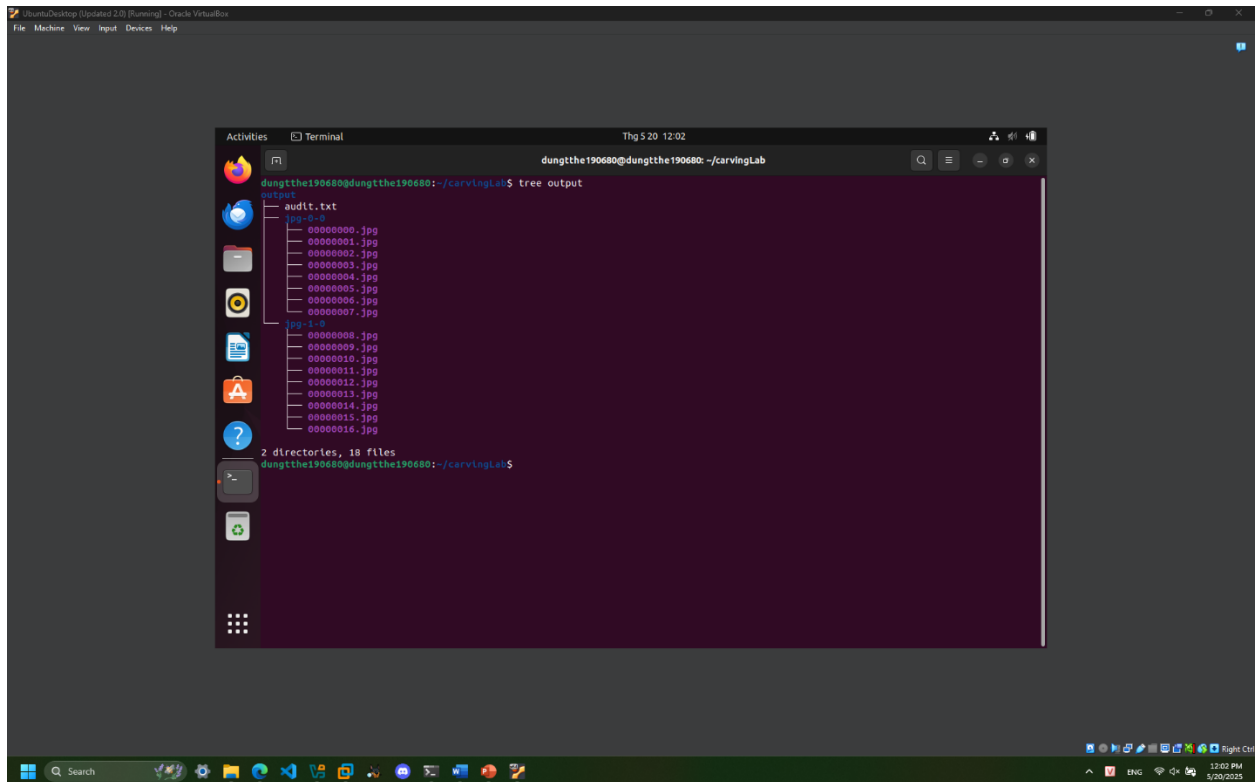
Device      Boot Start    End Sectors  Size Id Type
usb_fat_carving.001p1 * 128 243711 243584 118,9M e W95 FAT16 (LBA)
dungthe190680@dungthe19: ~$ fdisk -o 128 usb_fat_carving.001
r/r * 1: USB (Volume Label Entry)
d/d 6: System Volume Information
r/r * 7: _est
r/r 10: dropbox_device
d/d * 13: oLd_File_Carving_files
r/r * 15: B_ub_poe4.bmp
r/r * 18: B_zoom-eubie-mono.bmp
r/r * 21: BallardLab8.java
r/r * 24: brttLab19.java
r/r * 27: DO_example.doc
r/r * 30: DO_example2.doc
r/r * 33: G_BuiltForThis.gif
r/r * 36: G_zoom-sc.gif
r/r * 37: H_Form.html
r/r * 39: H_hello.html
r/r * 41: J_ub_law.jpg
r/r * 44: J_ub_night.jpg
r/r * 47: nps-2008-jean_outlook.pst
r/r * 50: P_CAS-zoom-6.png
r/r * 53: P_MSB_1_zoom.png
r/r * 57: pd_Evidence_search_techniques.pdf
r/r * 61: pd_Forensic_Report_Template.pdf
r/r * 64: pp_Number_Systems.pptx
r/r * 67: pp_one_page.pptx
r/r 69: readme.docx
r/r 70: readme.txt
r/r * 71: ttf_1.ttf
r/r * 74: T_Eubie-iphone-5-8.tiff
r/r * 78: T_youknowus-iphone-5-8.tiff
r/r * 81: W_axLoadcomplete.wav
r/r * 84: W_speaker_test_sound.wav
r/r * 86: Z_file.zip
r/r * 88: 江莎莎行程轨迹.doc
r/r * 91: nps-2008-jean_outlook.pst
v/v 3889687: $Mn
v/v 3889668: $FAT1
v/v 3889669: $FAT2
v/v 3889670: $OrphanFiles
dungthe190680@dungthe19: ~$
```



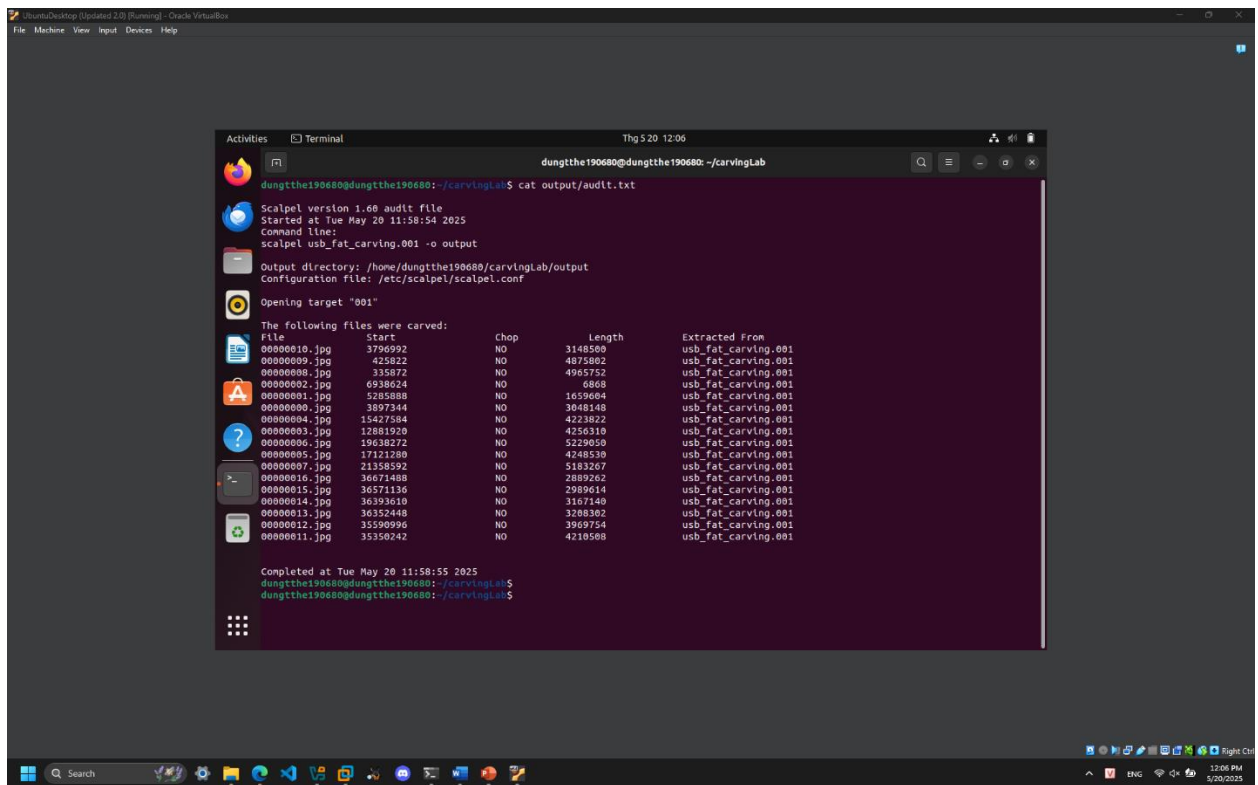
Step 3:



```
dungtthe190680@dungtthe190680: ~/carvingLab
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.
Opening target "/home/dungtthe190680/carvingLab/usb_fat_carving.001"
Image file pass 1/2.
usb_fat_carving.001: 100.0% |*****| 119.0 MB 00:00 ETA
Allocating work queues...
Work queues allocation complete. Building carve lists...
Carve lists built. Workload:
jpg with header "\xff\xd8\xff\x3f\x3f\x45\x78\x09\x00" and footer "\xff\xd9" --> 8 files
jpg with header "\xff\xd8\xff\x3f\x3f\x4a\x40\x49\x40" and footer "\xff\xd9" --> 9 files
Carving files from image.
Image file pass 2/2.
usb_fat_carving.001: 100.0% |*****| 119.0 MB 00:00 ETA
Processing of image file complete. Cleaning up...
Done.
Scalpel is done, files carved = 17, elapsed = 1 seconds.
dungtthe190680@dungtthe190680: ~/carvingLab$
```



```
dungtthe190680@dungtthe190680: ~/carvingLab
tree output
.
├── audit.txt
├── output
│   ├── jpg-0-0
│   │   ├── 00000000.jpg
│   │   ├── 00000001.jpg
│   │   ├── 00000002.jpg
│   │   ├── 00000003.jpg
│   │   ├── 00000004.jpg
│   │   ├── 00000005.jpg
│   │   ├── 00000006.jpg
│   │   └── 00000007.jpg
│   ├── jpg-1-0
│   │   ├── 00000008.jpg
│   │   ├── 00000009.jpg
│   │   ├── 00000010.jpg
│   │   ├── 00000011.jpg
│   │   ├── 00000012.jpg
│   │   ├── 00000013.jpg
│   │   ├── 00000014.jpg
│   │   ├── 00000015.jpg
│   │   └── 00000016.jpg
└── 2 directories, 18 files
dungtthe190680@dungtthe190680: ~/carvingLab$
```

Step 4:

