Lab 2: Data Carving

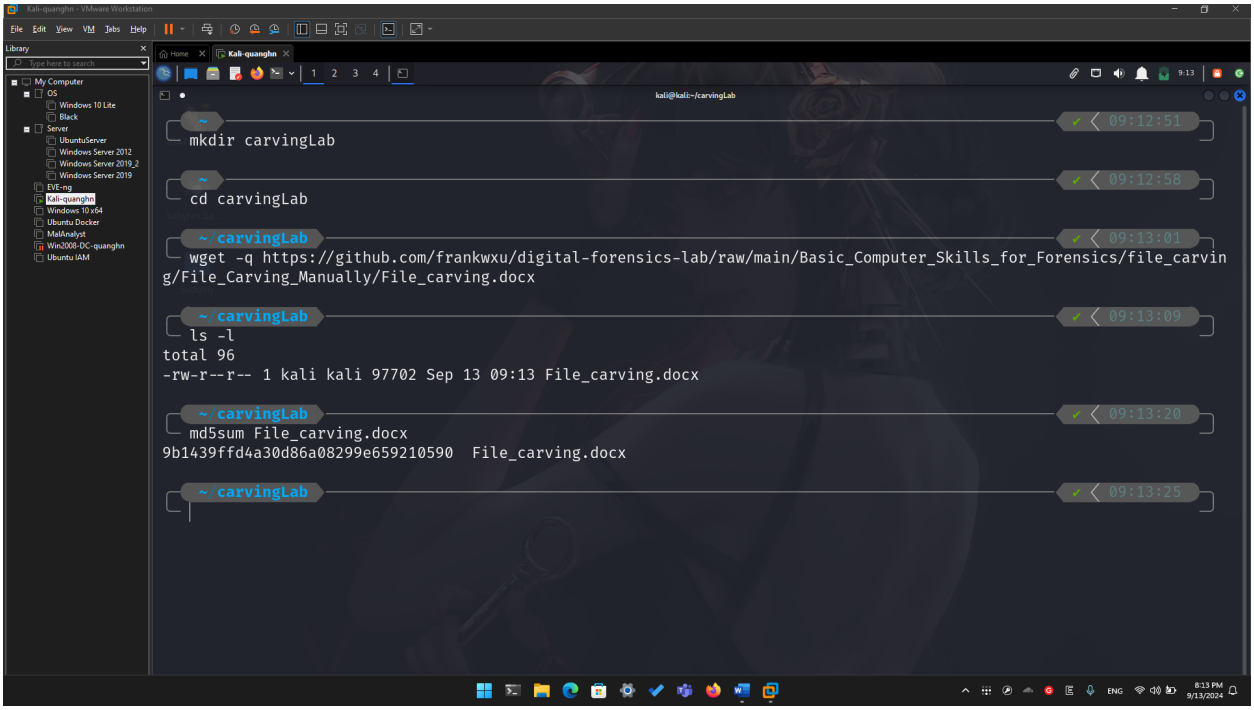
Group: CyberSec_N00b

Member:

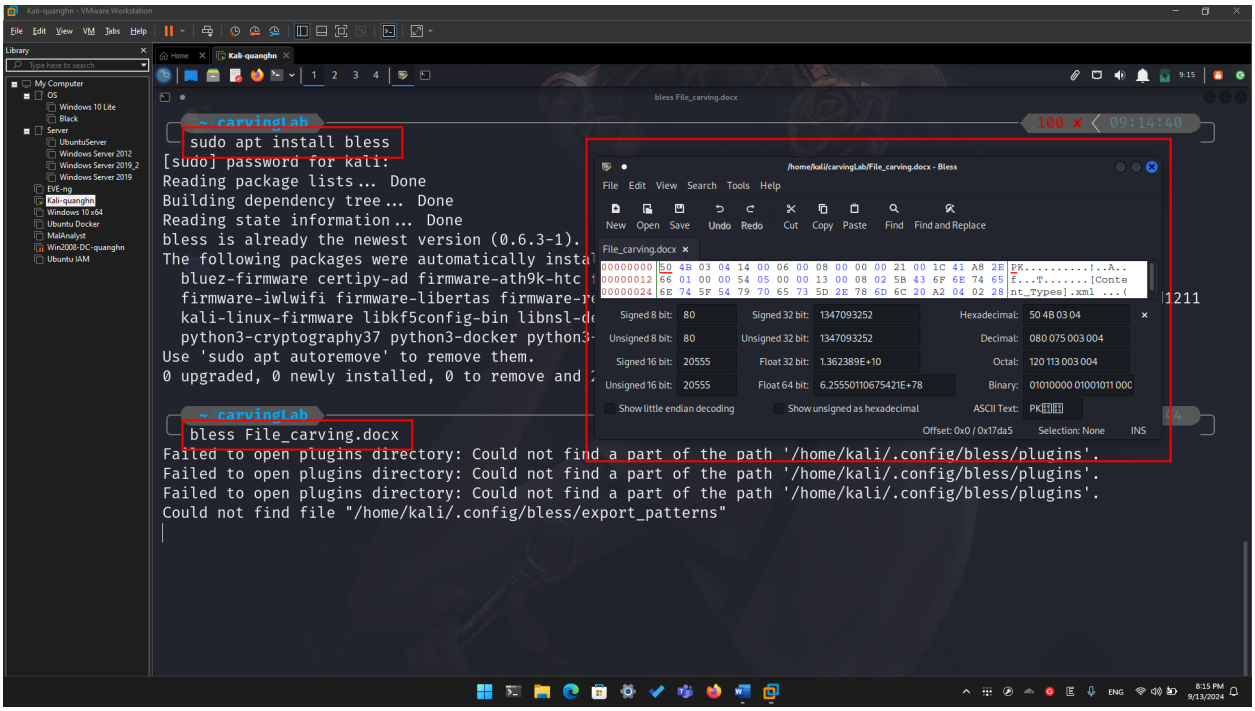
- *Huỳnh Ngọc Quang (SE181838)*
- *Hồ Tài Liên Vy Kha (SE181818)*
- *Hoàng Kim Long (DE180860)*
- *Phạm Thành Long (SE181692)*
- *Nguyễn Lê Hoàng Thông (SE182533)*

1. Extracting images from a corrupted Word document

Step 1.

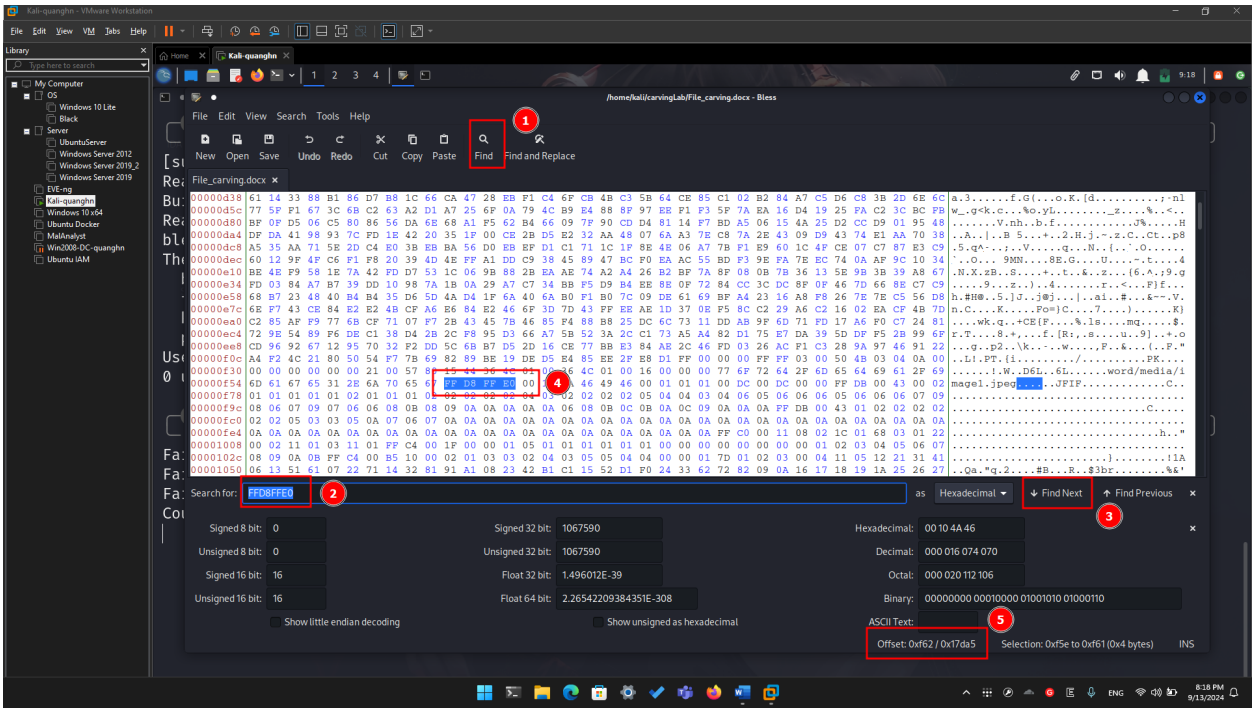


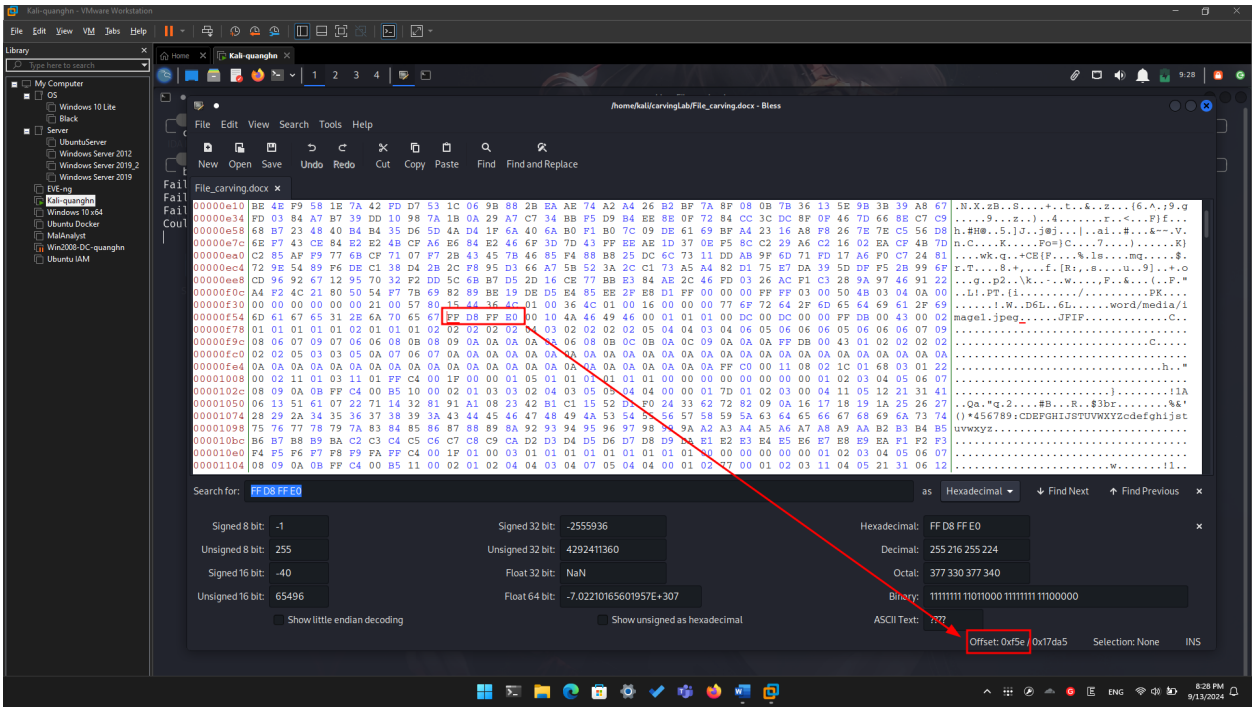
Step 2.



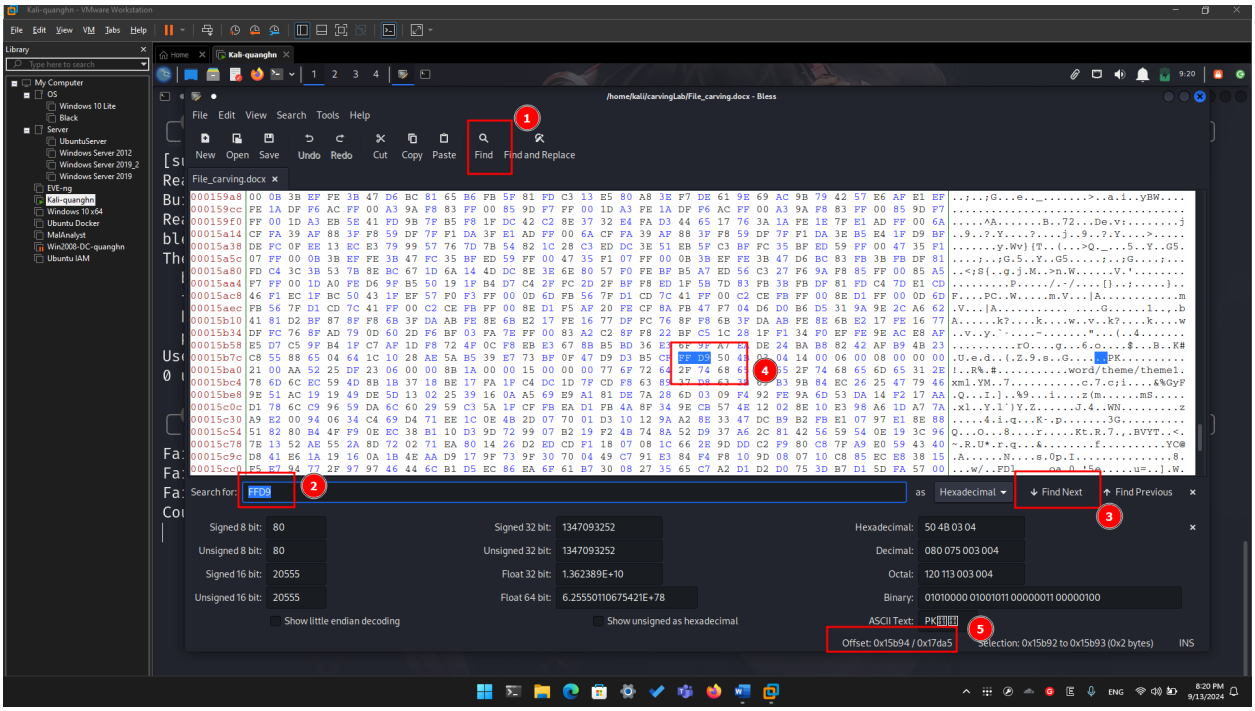
Step 3.

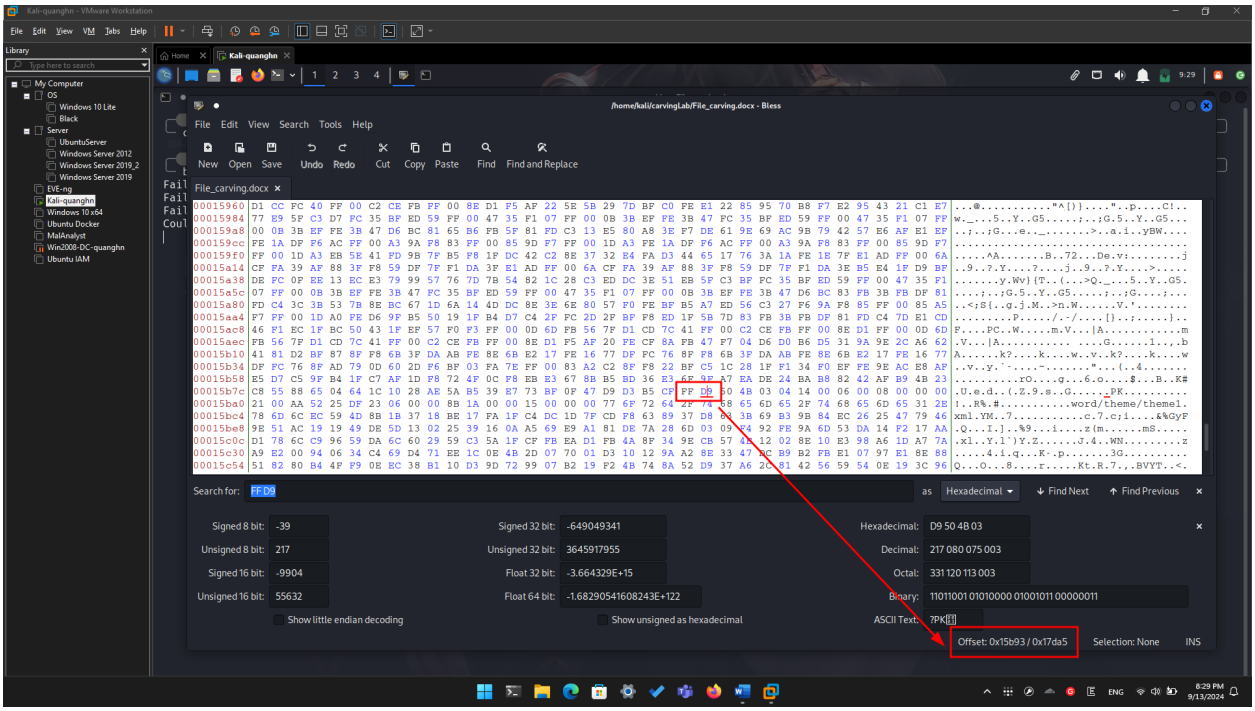
– Search file header start offset – 0F5E





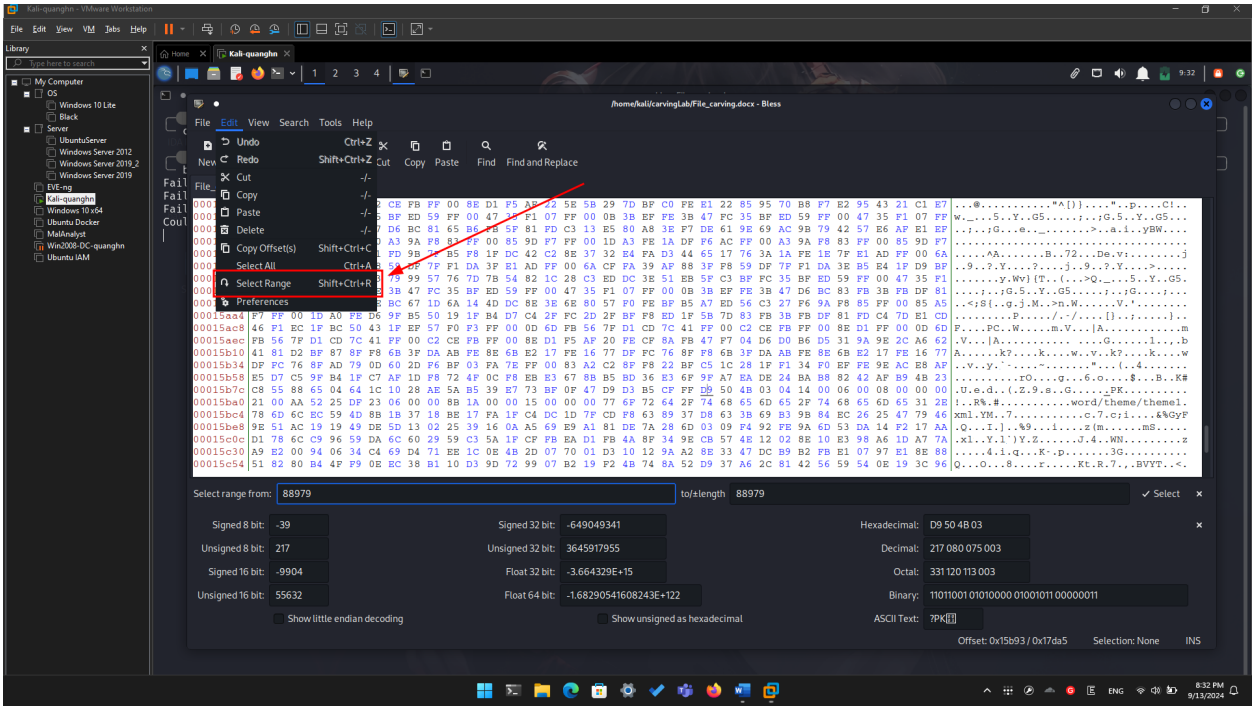
– Search file trailer ends offset – 15B93



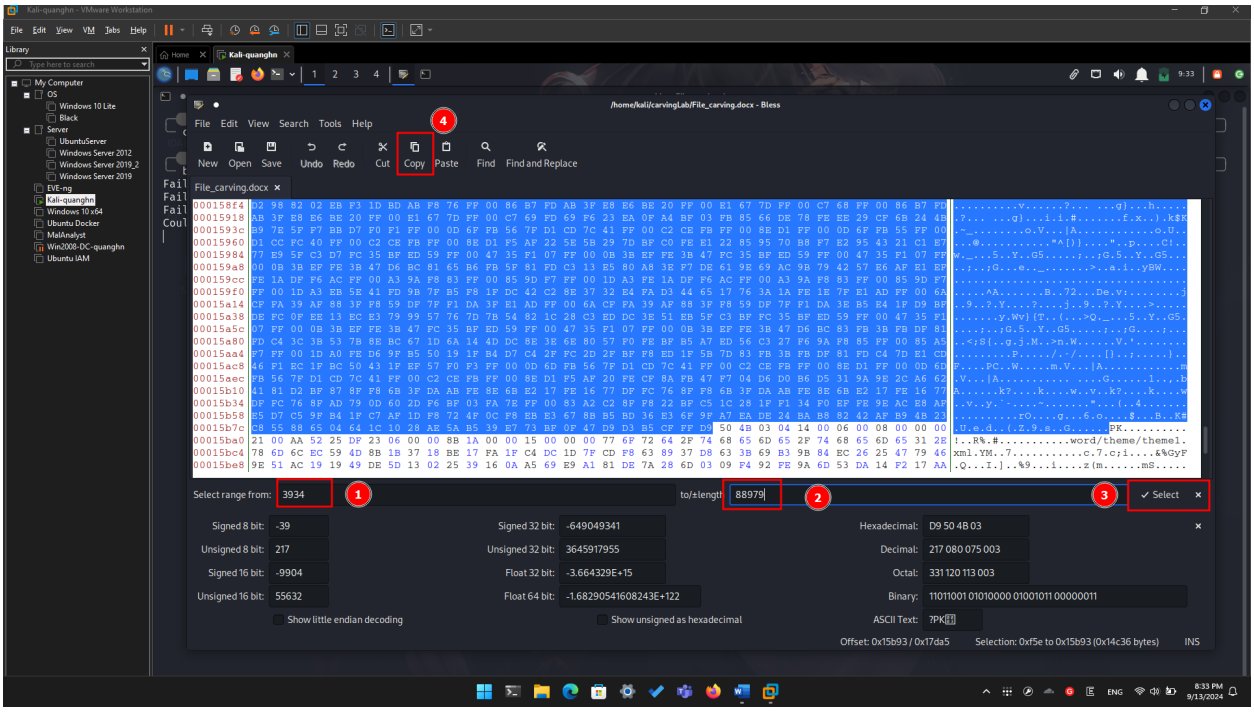


– Select hex from header to tail

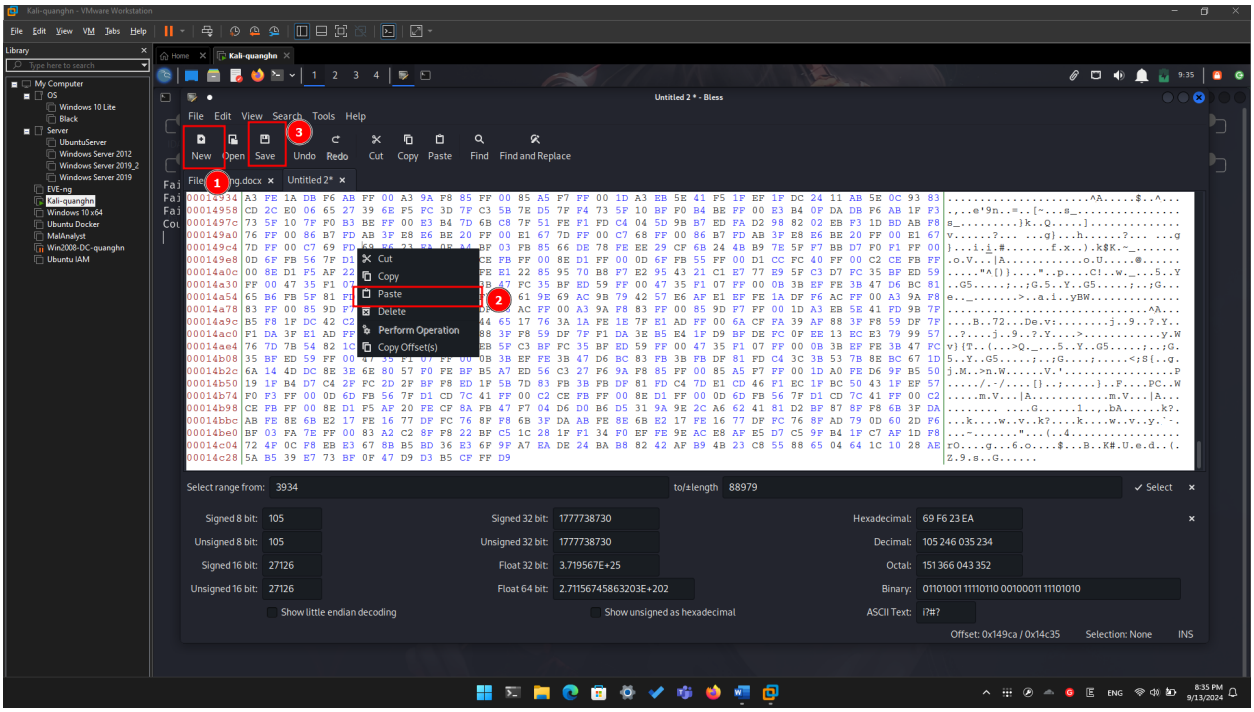
  - (0F5E)16=(3934)10
  - (15B93)16=(88979)10



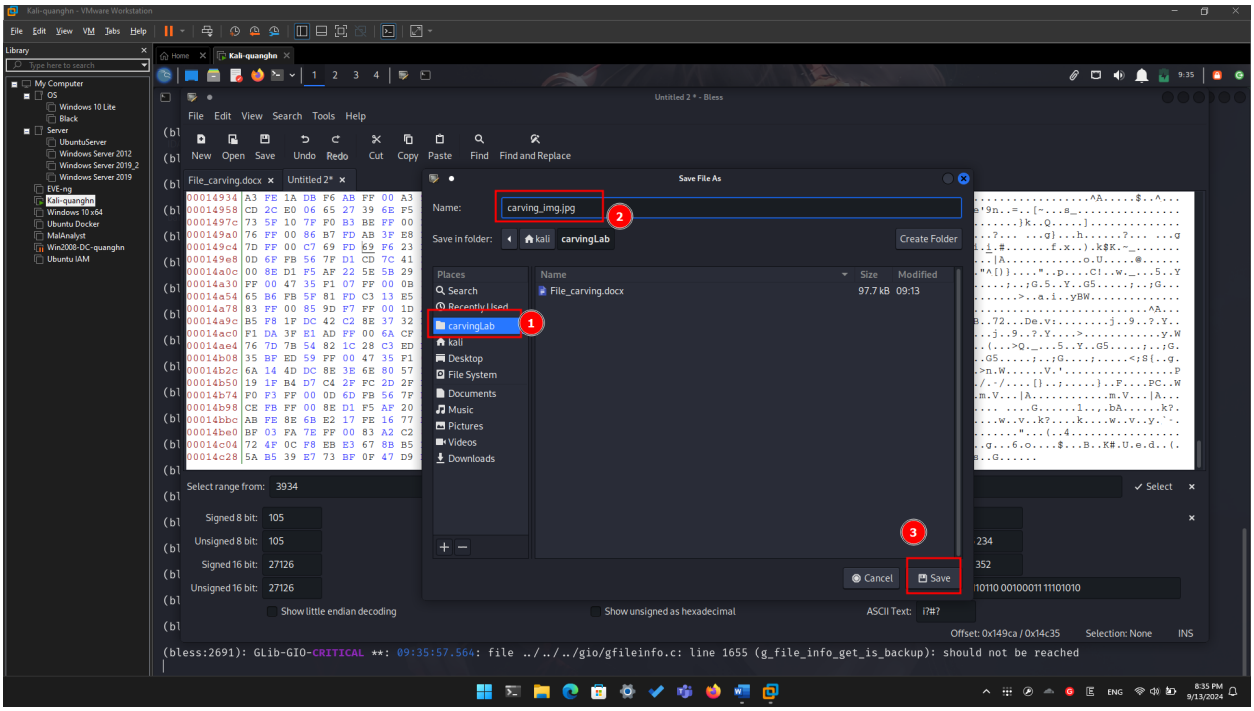
– Copy the selection



– Paste the selection

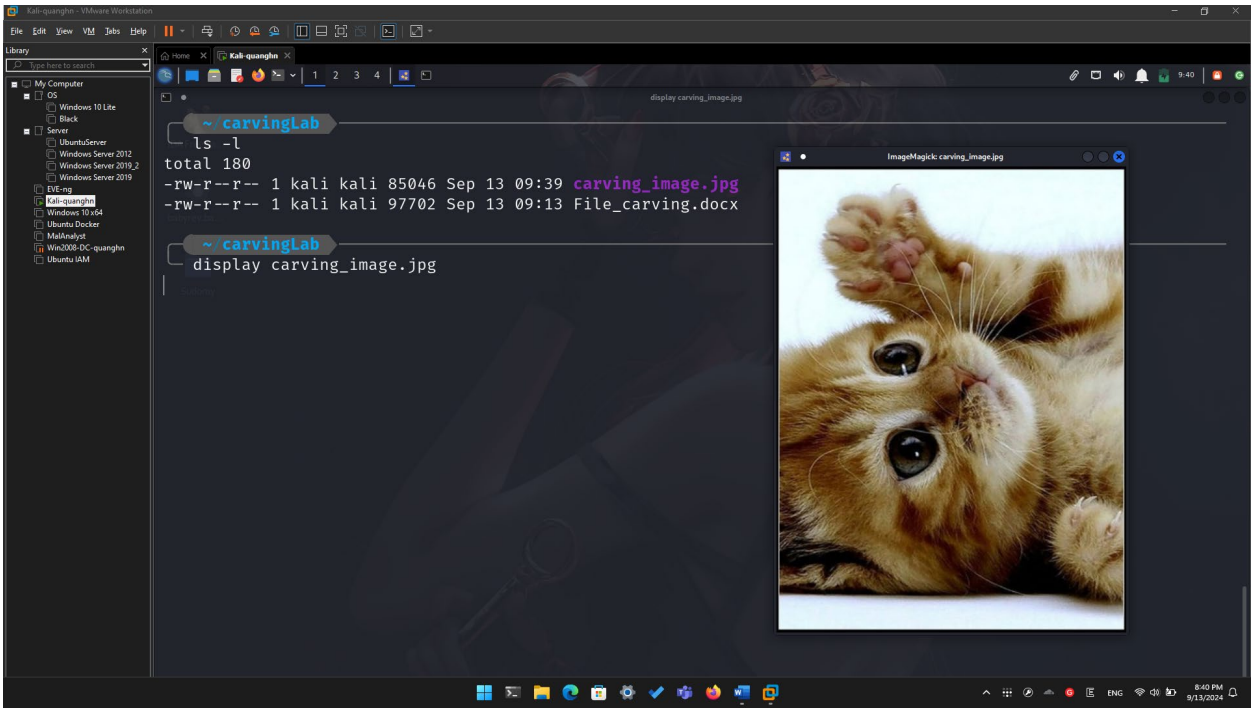


– Save the image



Step 4.

– Show the carved image

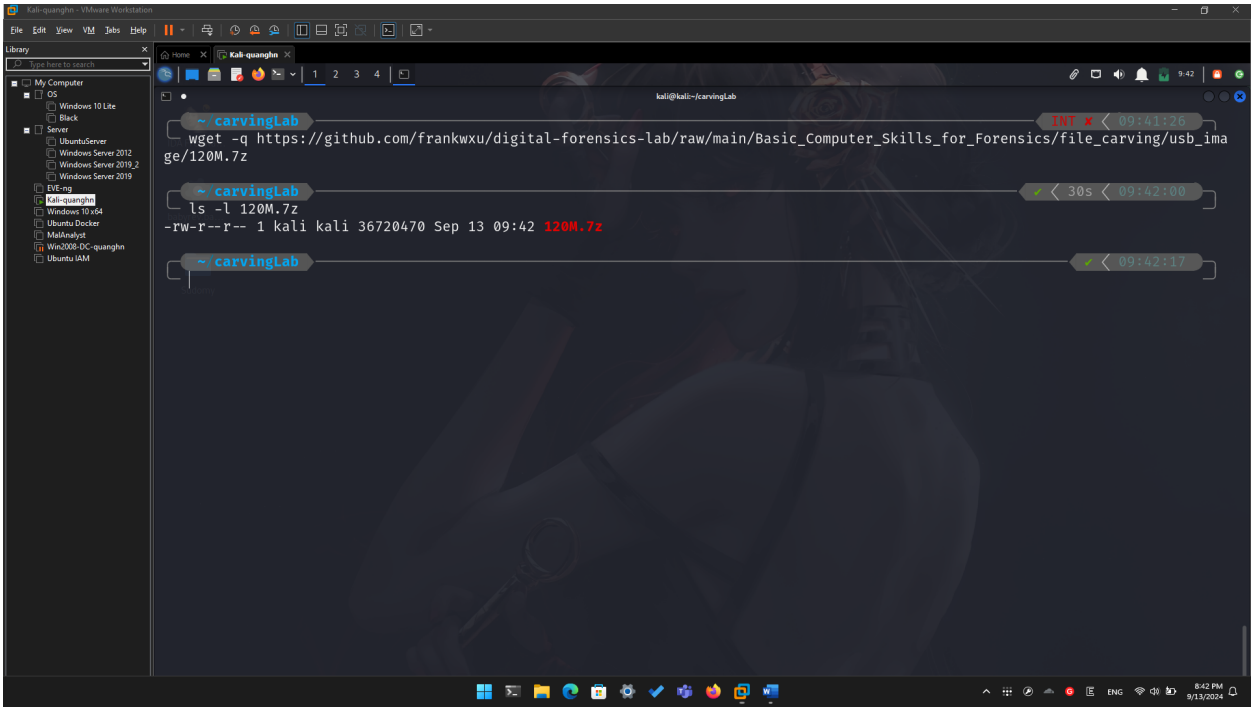


2. Carving/Recovering a USB image

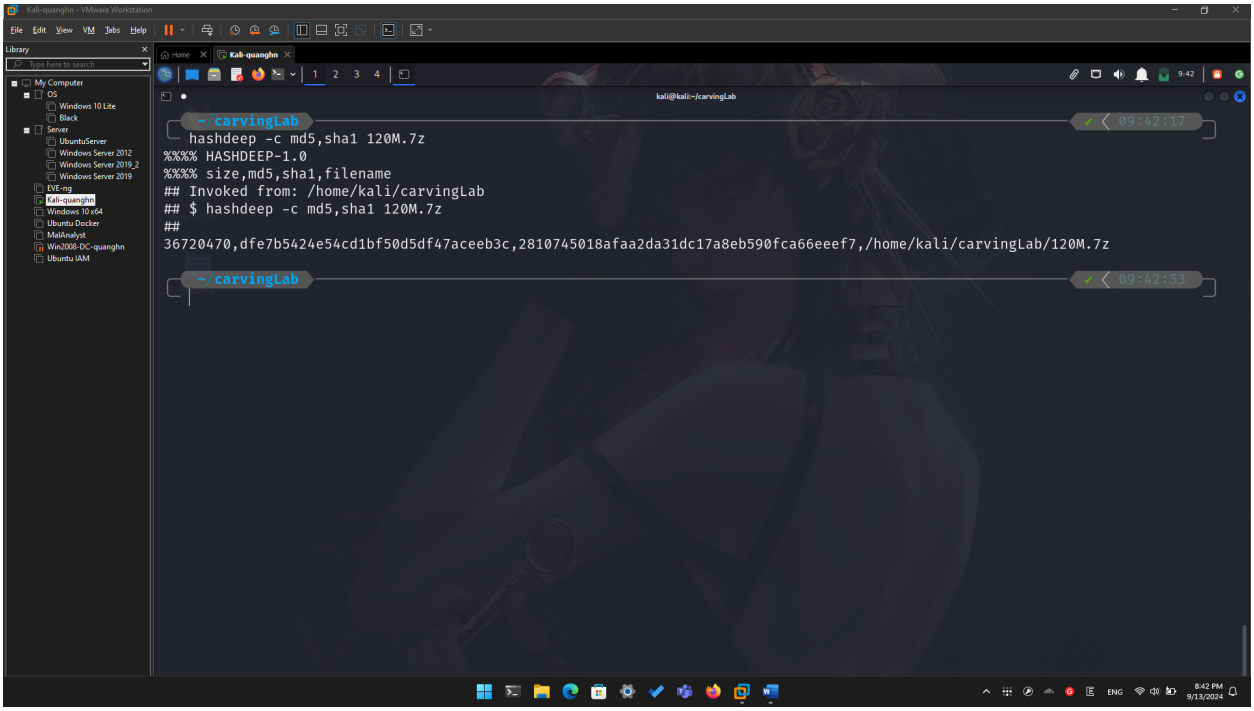
– Prepare a USB image for file carving

Step 1.

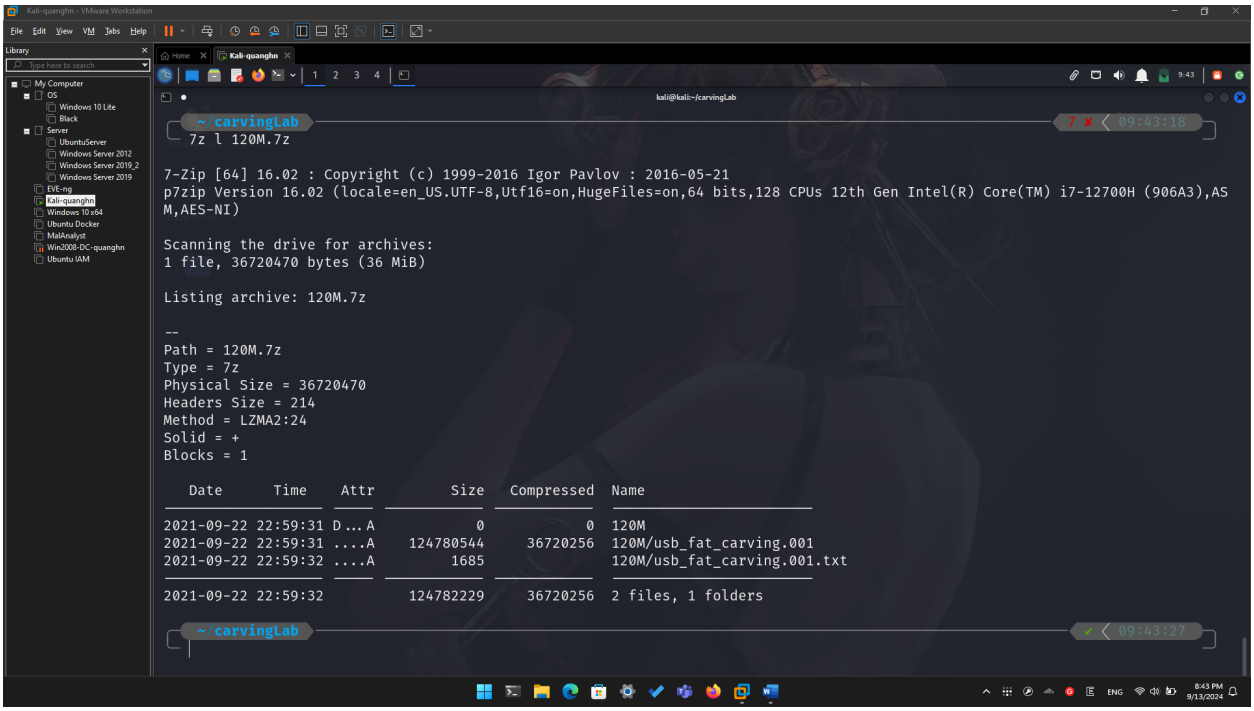
– Download the zipped USB image



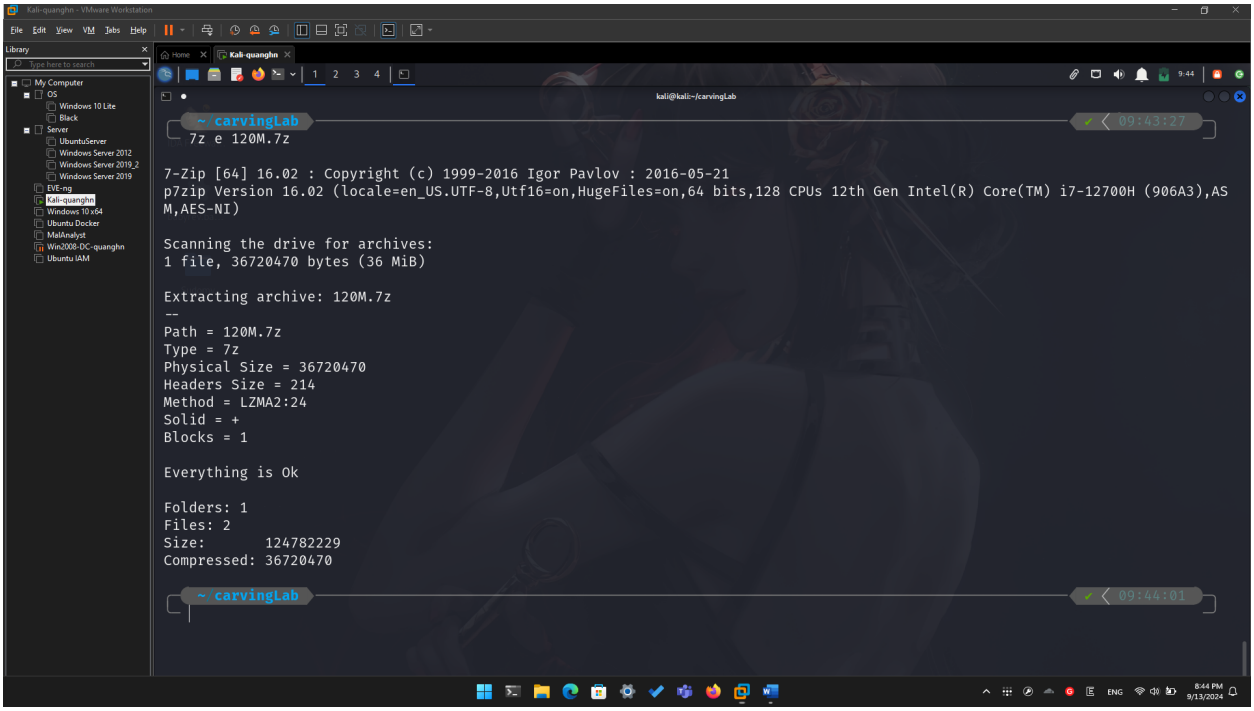
– Compute hashes



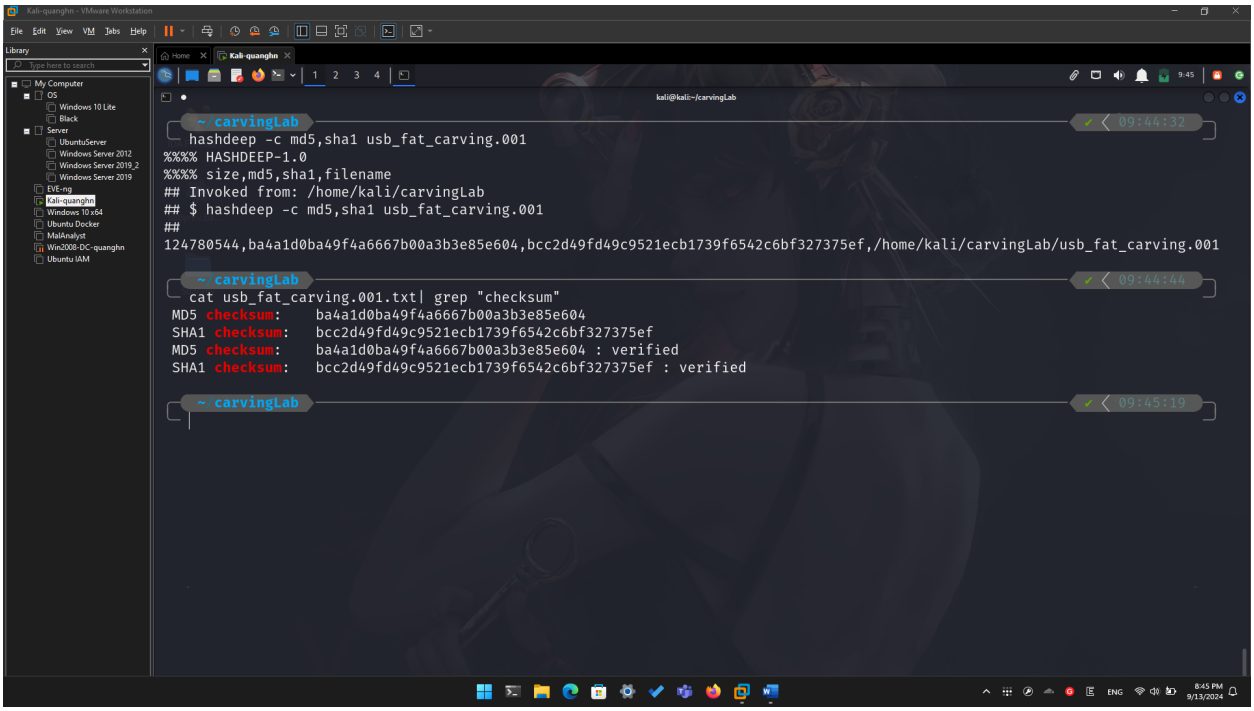
– List the content of the zipped file



– Extract the content of the zipped file

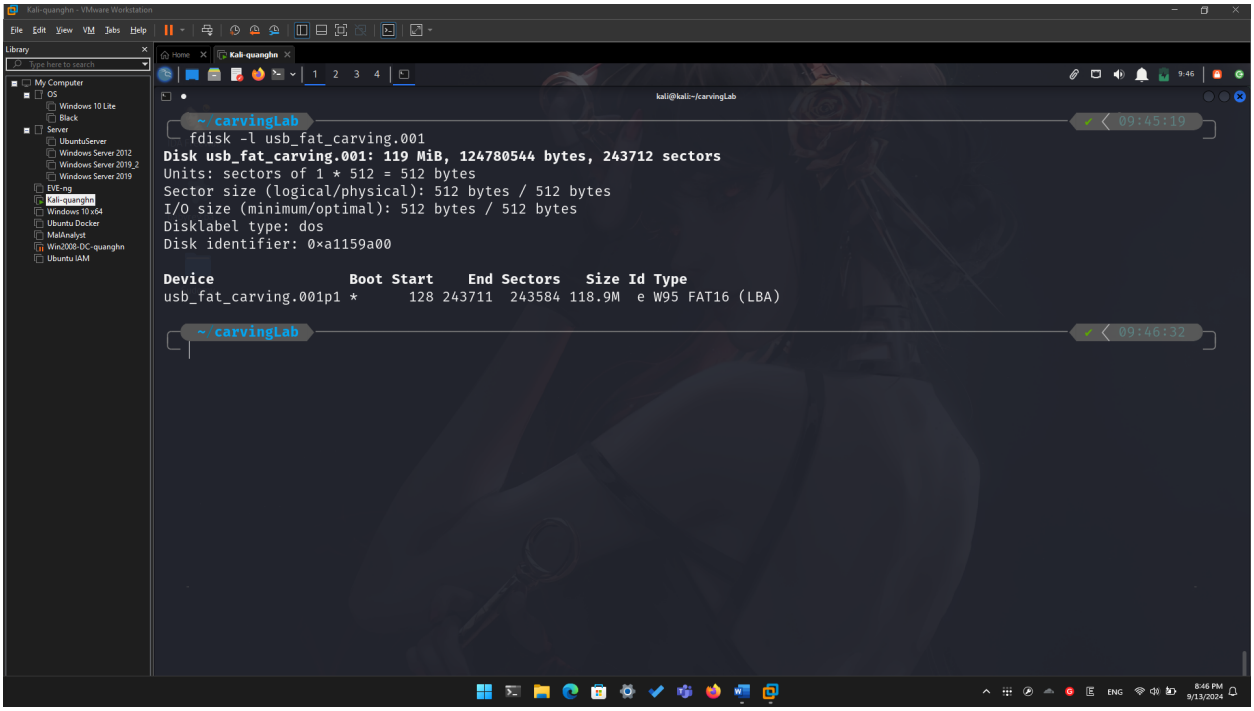


– Verify the hashes

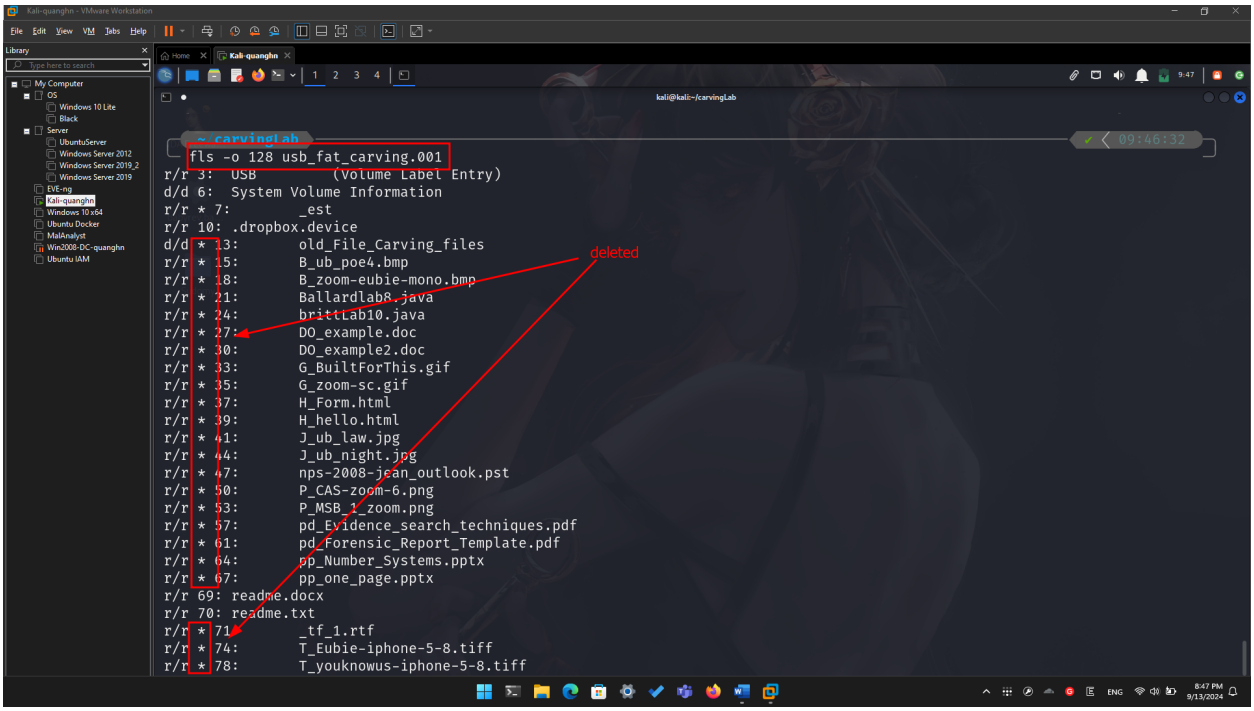


Step 2.

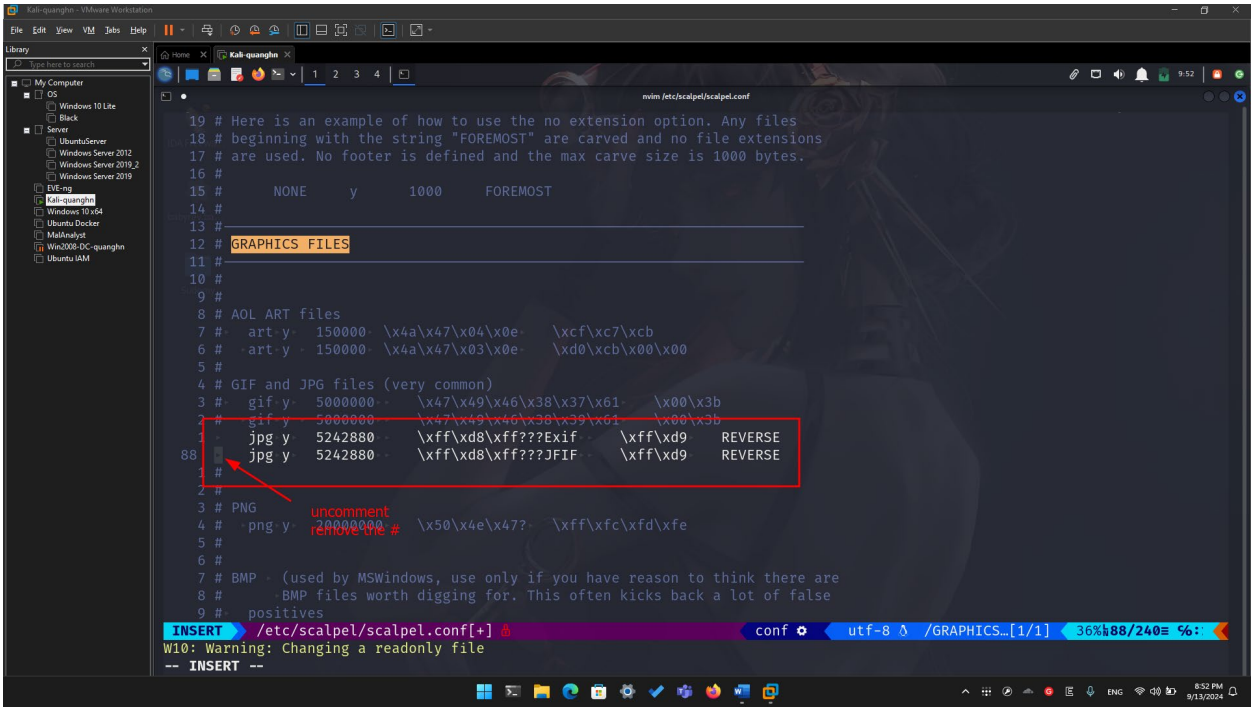
- Exam the content of the USB
- Display partitions



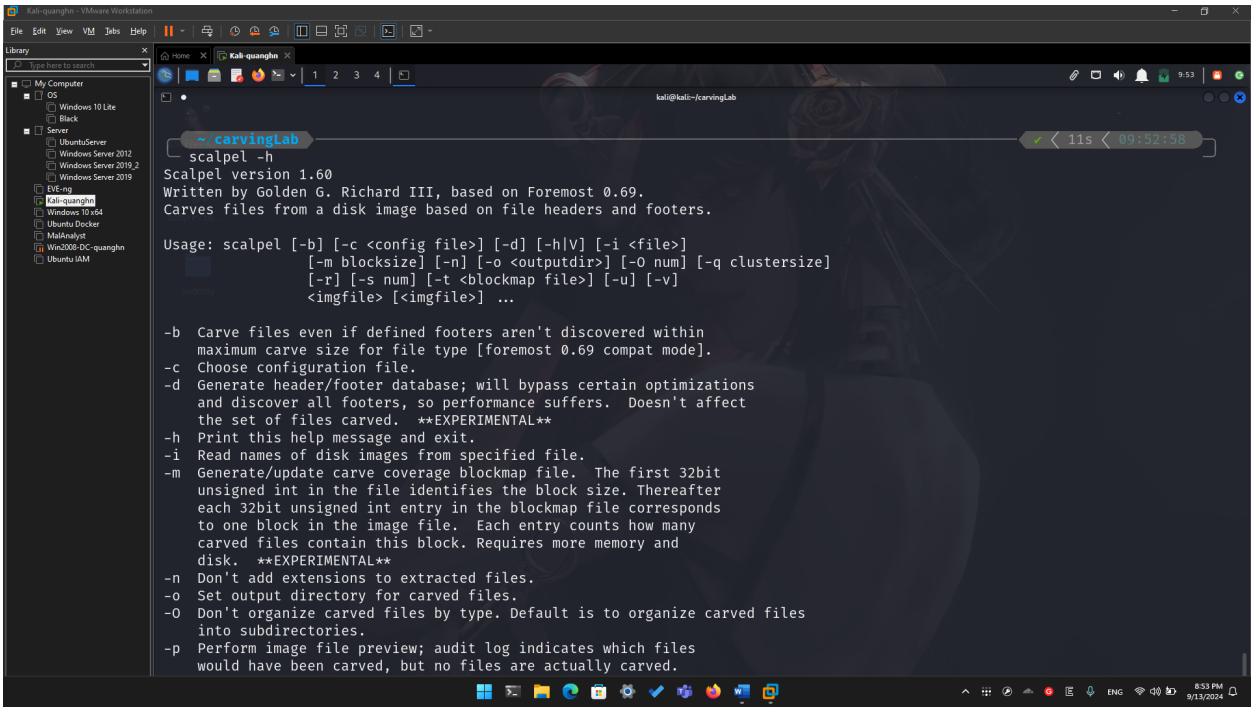
- Find deleted files



– Decide which file types need to carve

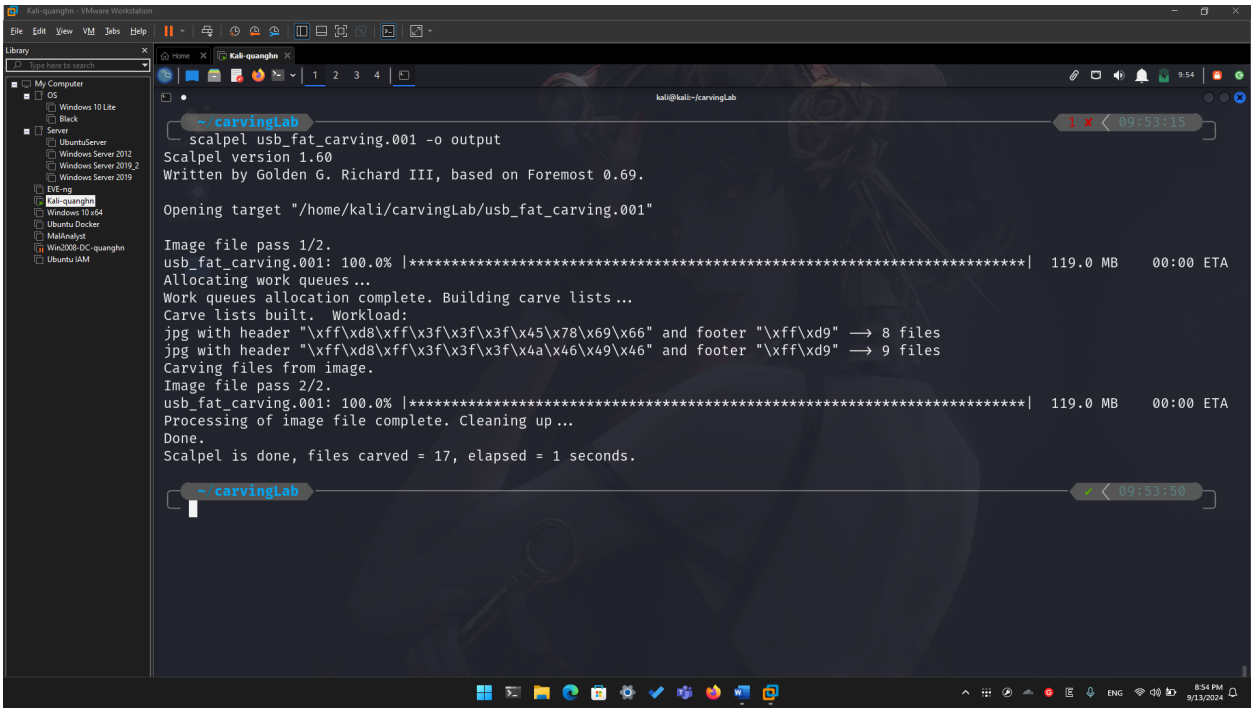


– Save it and quit!
– Show help

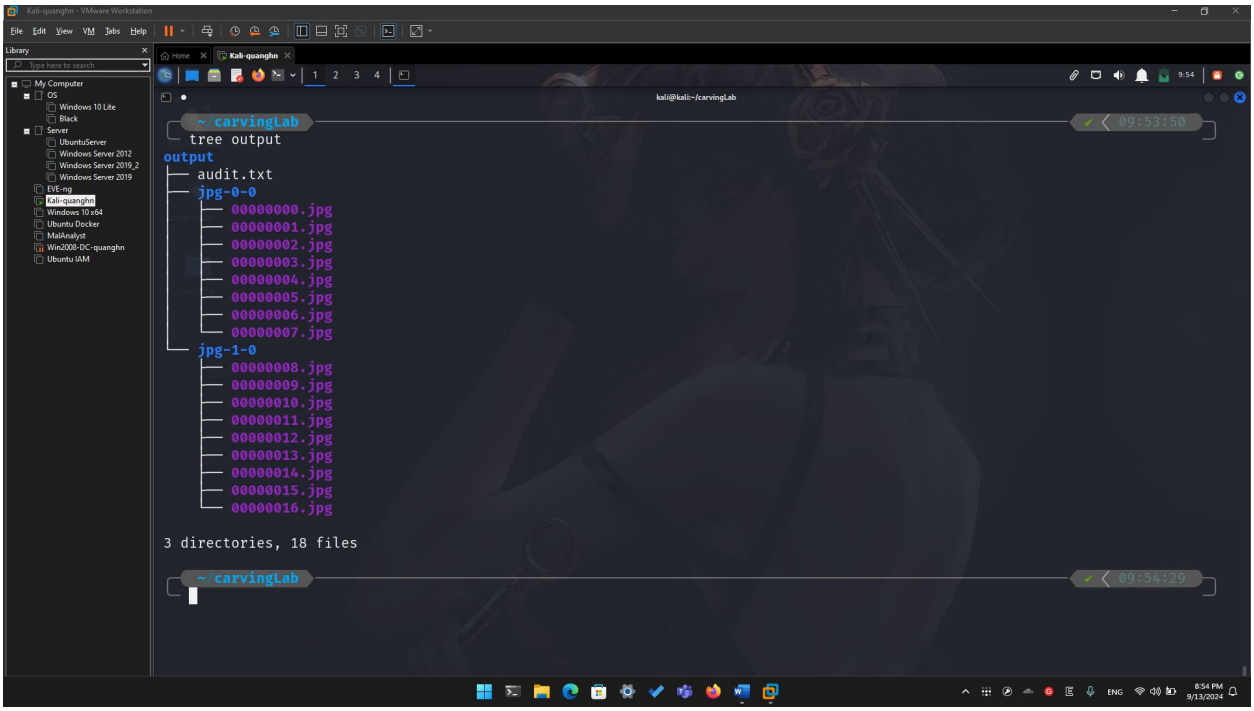


Step 3.

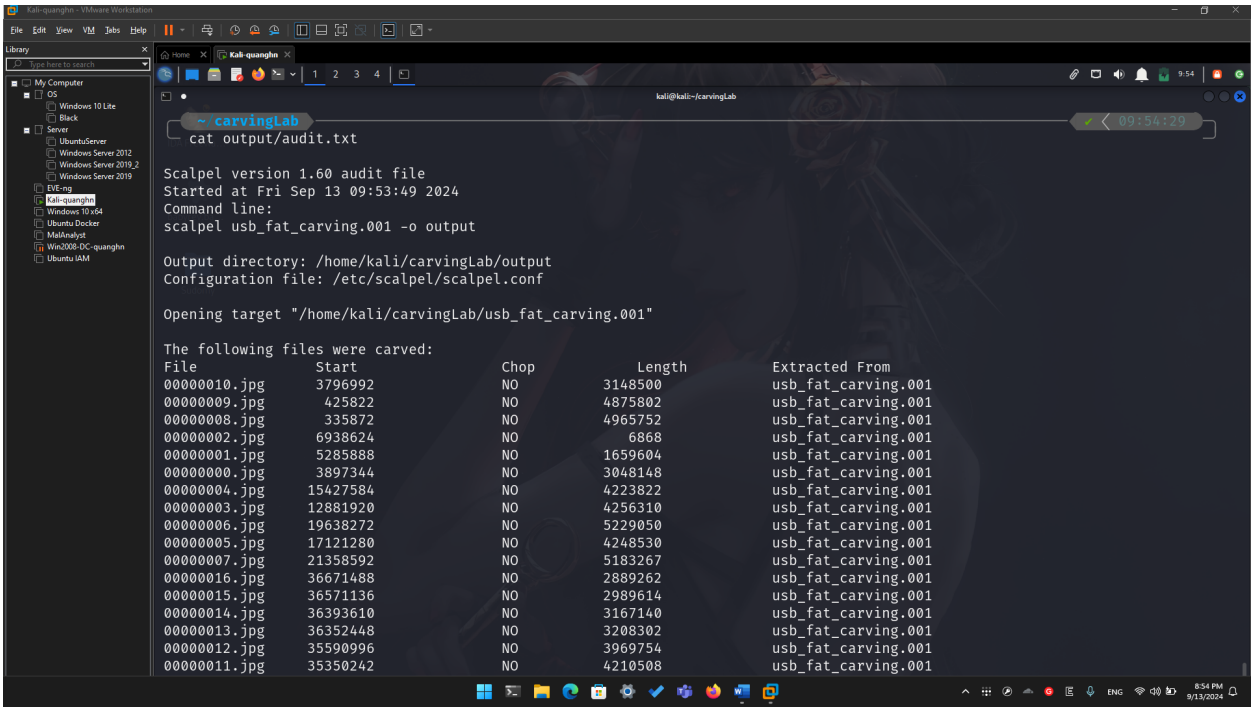
– Carving the USB image



– Show carved files

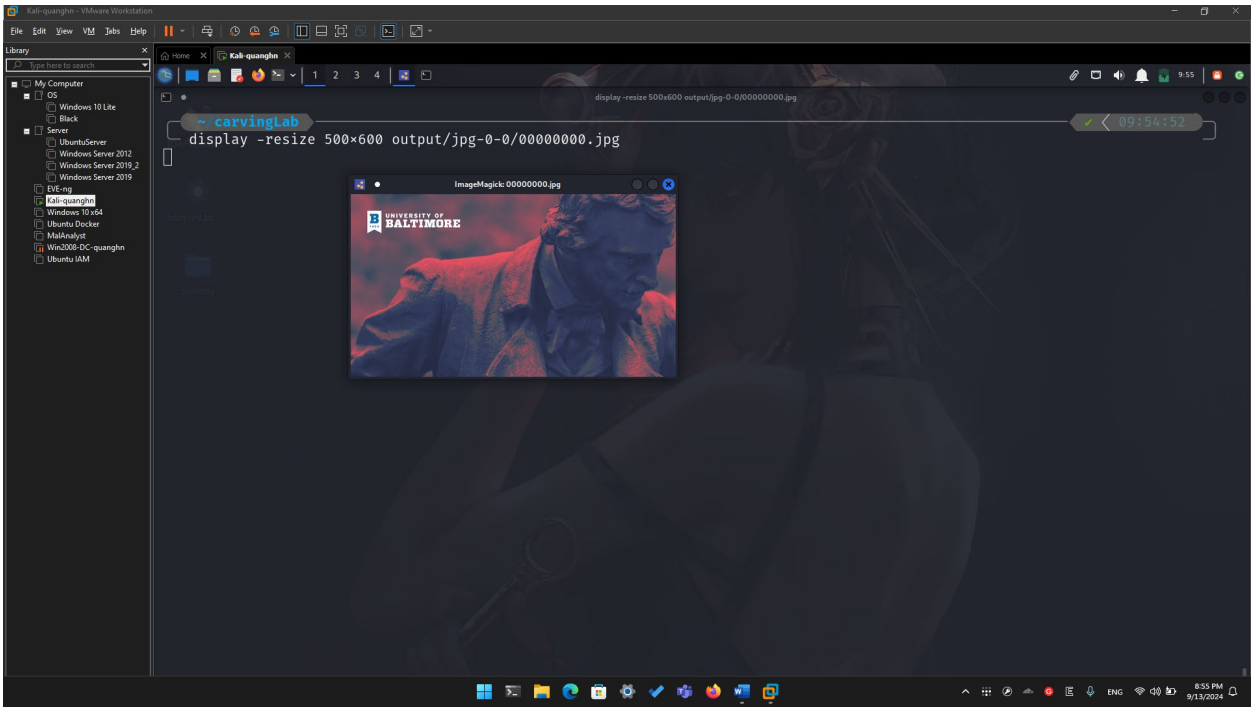


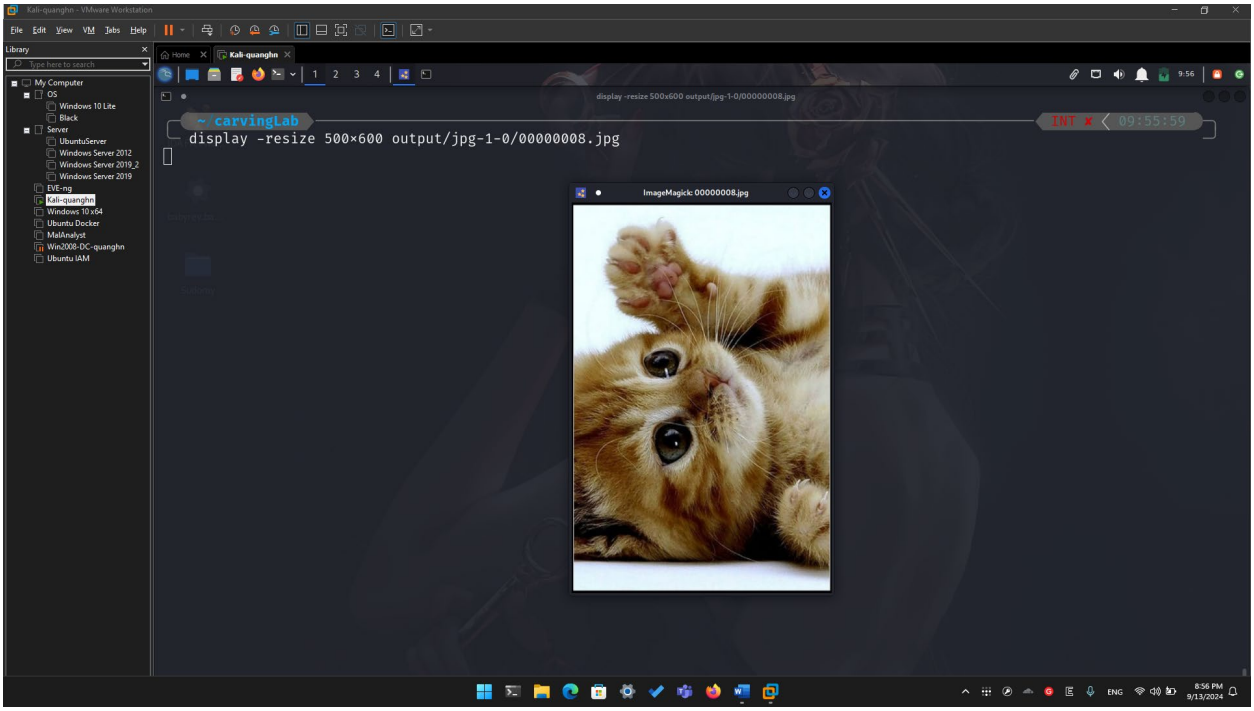
– Show audit log



Step 4.

– Display two carved jpg image


Kali-quanghn - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
OS
Windows 10 Lite
Black
Server
UbuntuServer
Windows Server 2012
Windows Server 2019_2
Windows Server 2019
EVE-ng
Kali-quanghn
Windows 10 x64
Ubuntu Docker
MalAnalyst
Win2008-DC-quanghn
Ubuntu IAM
Home
Kali-quanghn
1 2 3 4
9:55
display -resize 500x600 output/jpg-0-0/00000000.jpg
~/carvingLab
09:54:52
display -resize 500×600 output/jpg-0-0/00000000.jpg
ImageMagick: 00000000.jpg
UNIVERSITY OF BALTIMORE
ENG
8:55 PM
9/13/2024


Kali-quanghn - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
OS
Windows 10 Lite
Black
Server
UbuntuServer
Windows Server 2012
Windows Server 2019_2
Windows Server 2019
EVE-ng
Kali-quanghn
Windows 10 x64
Ubuntu Docker
MalAnalyst
Win2008-DC-quanghn
Ubuntu IAM
Home
Kali-quanghn
1 2 3 4
9:56
display -resize 500x600 output/jpg-1-0/00000008.jpg
~/carvingLab
INT x
09:55:59
display -resize 500×600 output/jpg-1-0/00000008.jpg
ImageMagick: 00000008.jpg
ENG
8:56 PM
9/13/2024