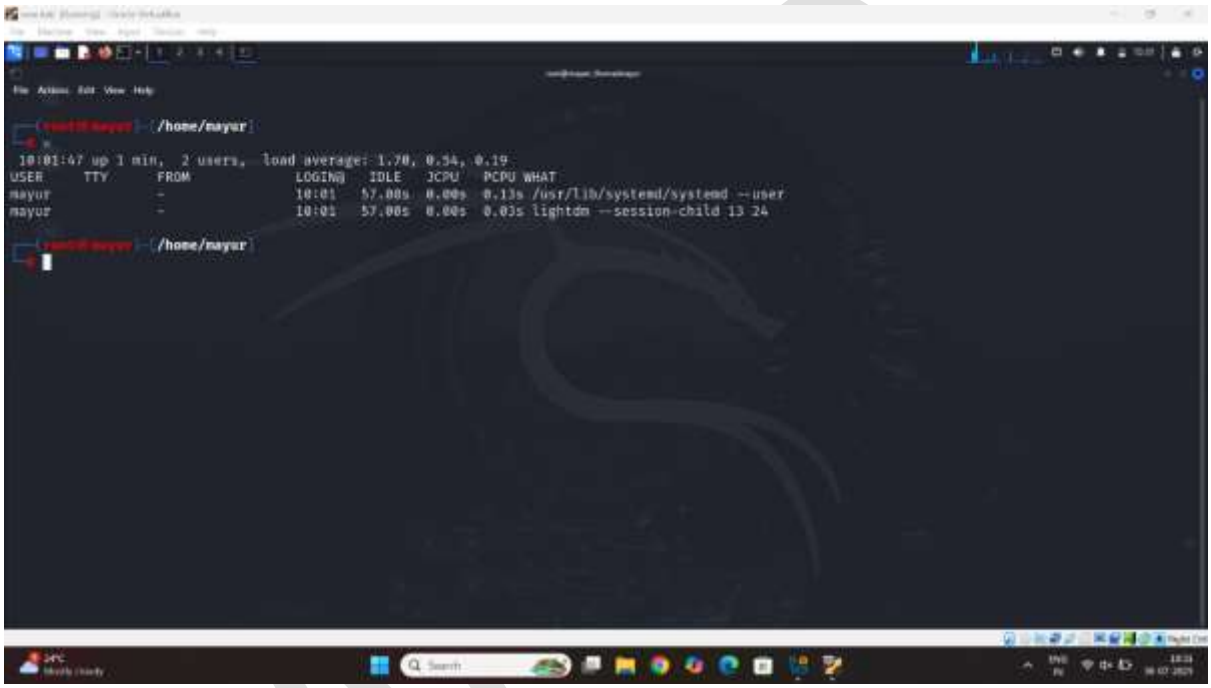
# Module 7 Linux and mac forensics

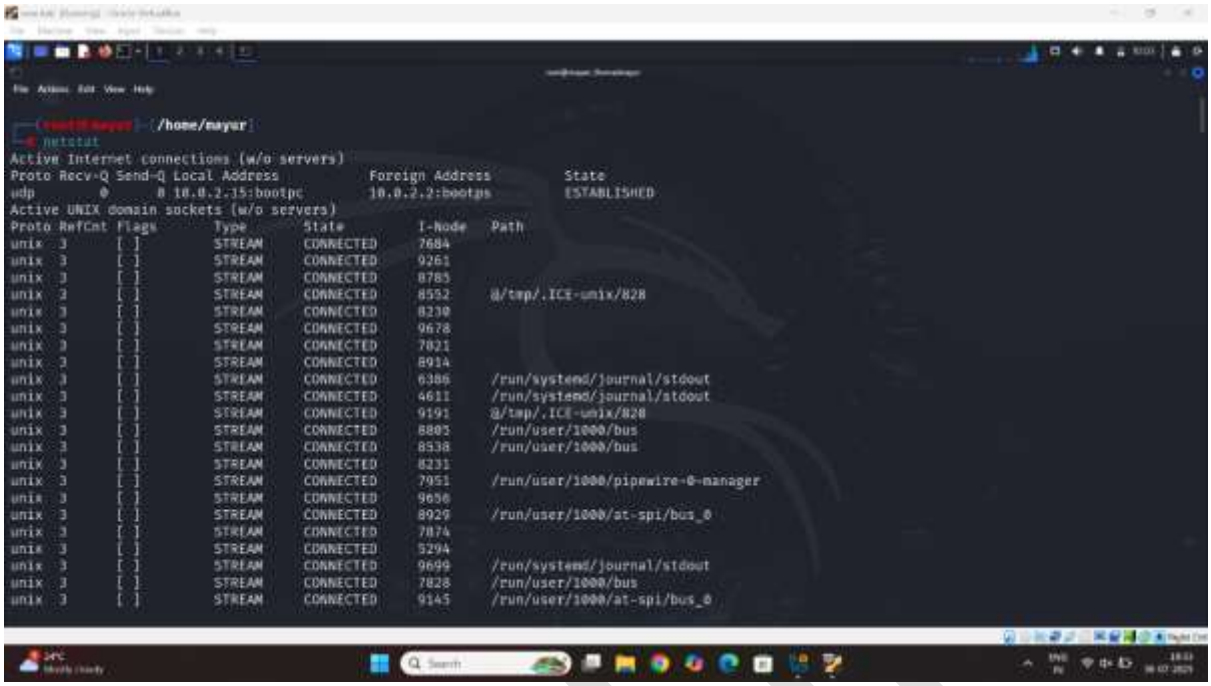
## Lab1 Acquire volatile data in Linux system

Step1 on the kali Linux machine

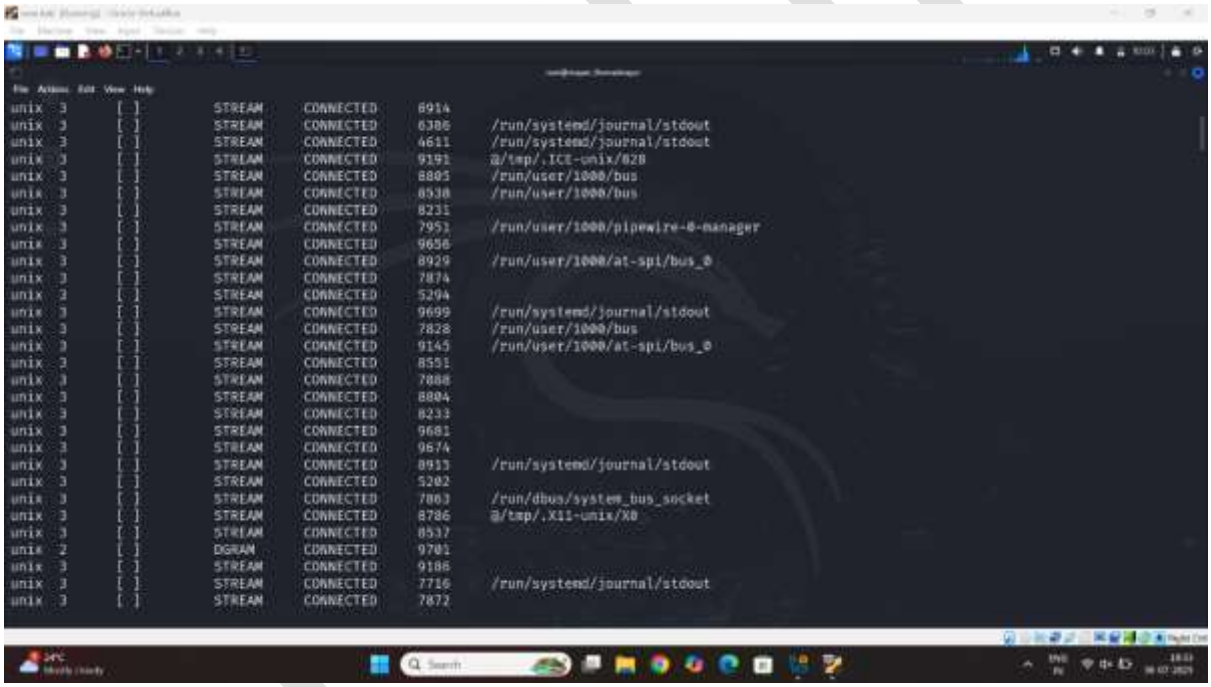
Command : W /this command are show total time of on machine




Step2 netstat/this command show network statitics

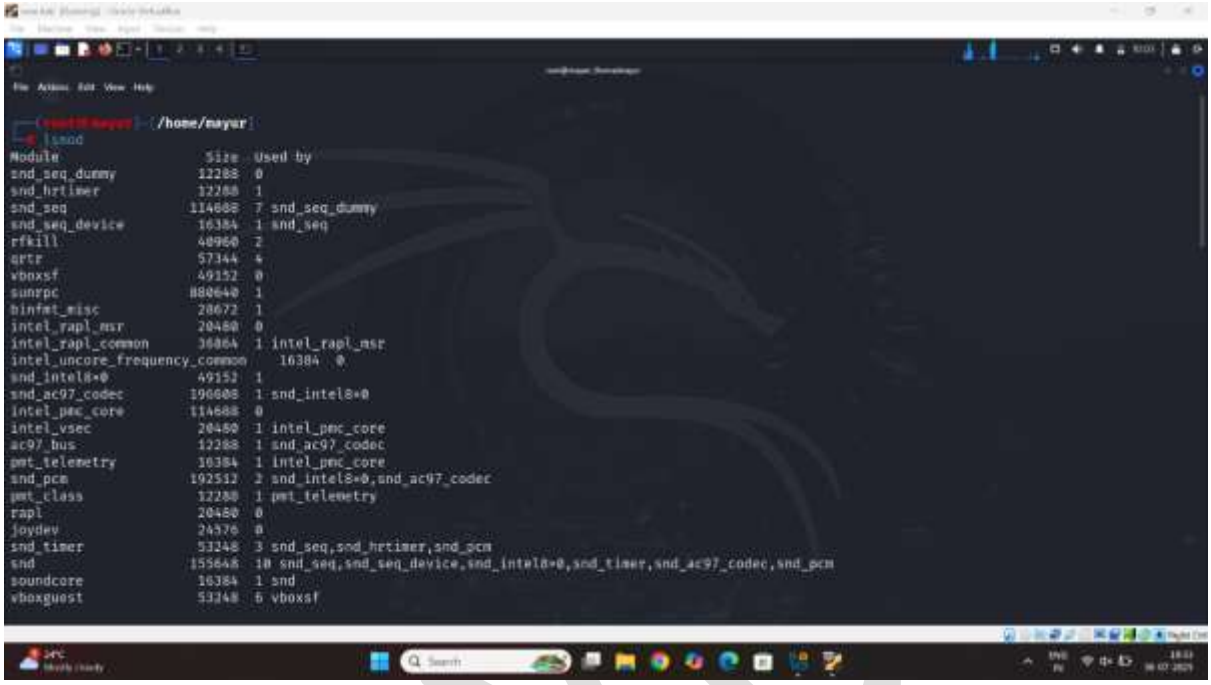


```
File  Actions  Edit  View  Help

┌──(root㉿kali)-[/home/mayur]
└─# netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      8 10.0.2.15:bootpc        10.0.2.2:bootps         ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  3      [ ]         STREAM     CONNECTED     7684
unix  3      [ ]         STREAM     CONNECTED     9261
unix  3      [ ]         STREAM     CONNECTED     8785
unix  2      [ ]         STREAM     CONNECTED     8552     @/tmp/.ICE-unix/828
unix  3      [ ]         STREAM     CONNECTED     8230
unix  3      [ ]         STREAM     CONNECTED     9678
unix  3      [ ]         STREAM     CONNECTED     7021
unix  3      [ ]         STREAM     CONNECTED     8914
unix  3      [ ]         STREAM     CONNECTED     6386     /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     4611     /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     9191     @/tmp/.ICE-unix/828
unix  3      [ ]         STREAM     CONNECTED     8805     /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     8538     /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     8231
unix  3      [ ]         STREAM     CONNECTED     7951     /run/user/1000/pipewire-0-manager
unix  3      [ ]         STREAM     CONNECTED     9656
unix  3      [ ]         STREAM     CONNECTED     8929     /run/user/1000/at-spi/bus_0
unix  3      [ ]         STREAM     CONNECTED     7874
unix  3      [ ]         STREAM     CONNECTED     5294
unix  3      [ ]         STREAM     CONNECTED     9699     /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     7828     /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     9145     /run/user/1000/at-spi/bus_0
```

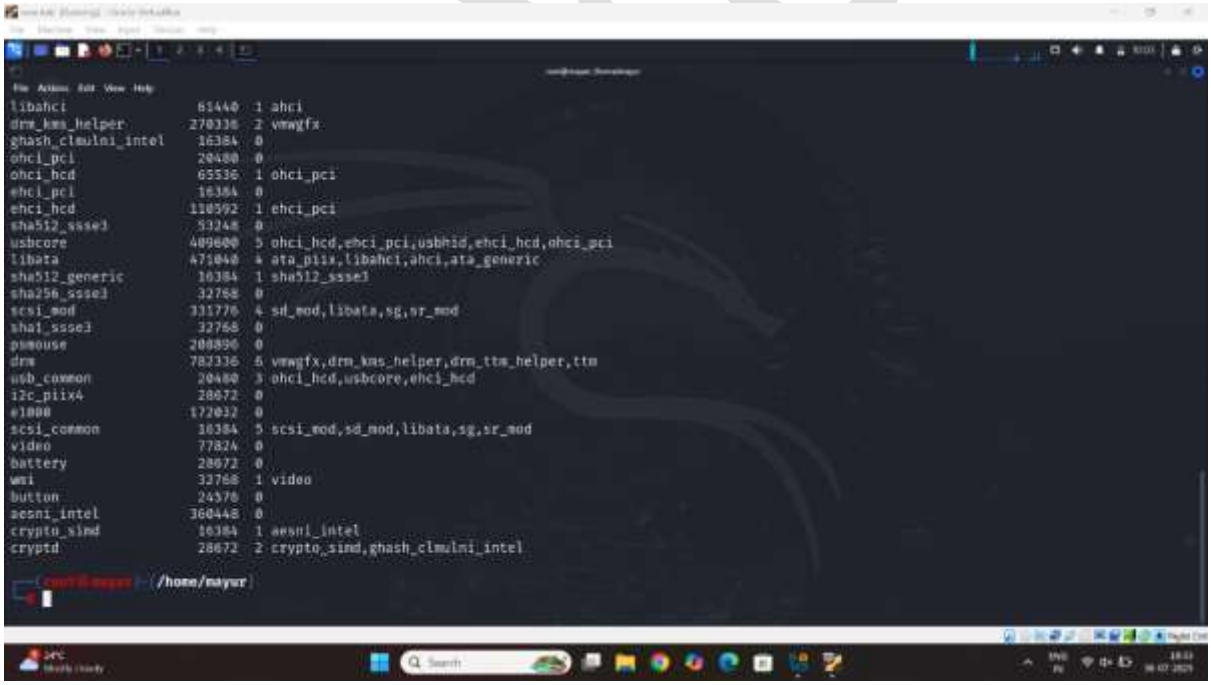


```
File  Actions  Edit  View  Help
unix  3      [ ]         STREAM     CONNECTED     8914
unix  3      [ ]         STREAM     CONNECTED     6386     /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     4611     /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     9191     @/tmp/.ICE-unix/828
unix  3      [ ]         STREAM     CONNECTED     8805     /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     8538     /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     8231
unix  3      [ ]         STREAM     CONNECTED     7951     /run/user/1000/pipewire-0-manager
unix  3      [ ]         STREAM     CONNECTED     9656
unix  3      [ ]         STREAM     CONNECTED     8929     /run/user/1000/at-spi/bus_0
unix  3      [ ]         STREAM     CONNECTED     7874
unix  3      [ ]         STREAM     CONNECTED     5294
unix  3      [ ]         STREAM     CONNECTED     9699     /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     7828     /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     9145     /run/user/1000/at-spi/bus_0
unix  3      [ ]         STREAM     CONNECTED     8551
unix  3      [ ]         STREAM     CONNECTED     7888
unix  3      [ ]         STREAM     CONNECTED     8804
unix  3      [ ]         STREAM     CONNECTED     8233
unix  3      [ ]         STREAM     CONNECTED     9681
unix  3      [ ]         STREAM     CONNECTED     9674
unix  3      [ ]         STREAM     CONNECTED     8933     /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     5202
unix  3      [ ]         STREAM     CONNECTED     7863     /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     8786     @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     8537
unix  2      [ ]         DGRAM      CONNECTED     9701
unix  3      [ ]         STREAM     CONNECTED     9186
unix  3      [ ]         STREAM     CONNECTED     7716     /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     7872
```

# Step3 lsof /this command show list open file of machine

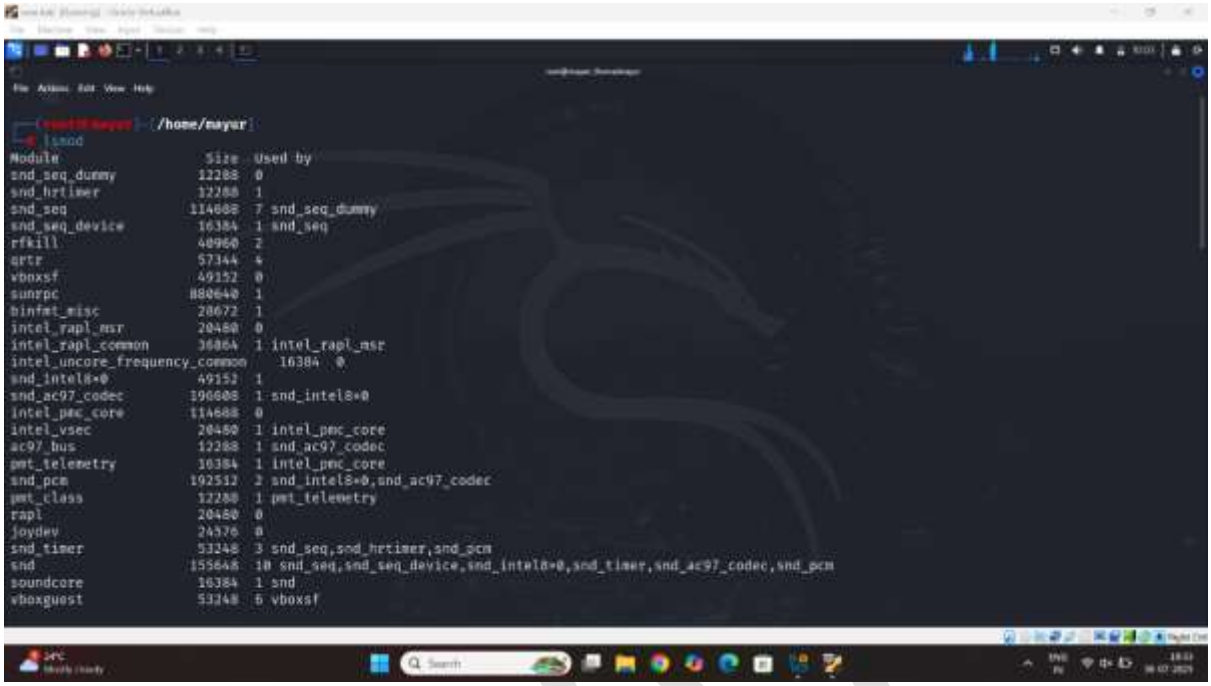


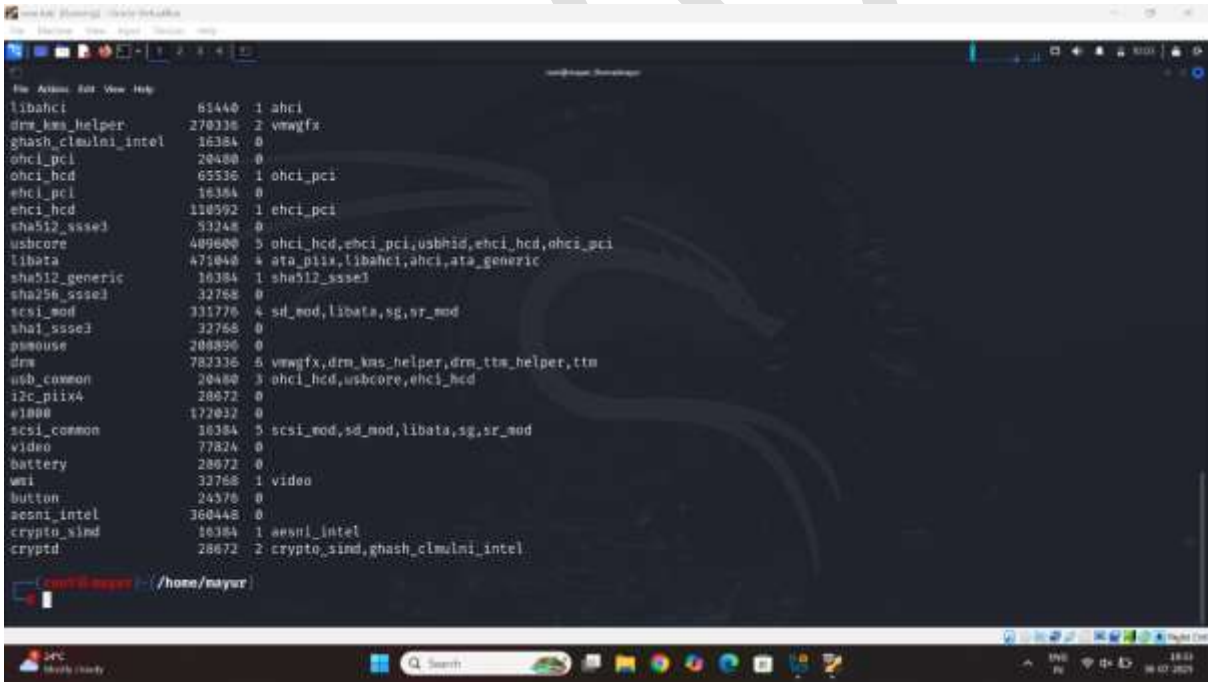
```
File  Actions  Edit  View  Help

┌──(root㉿kali)-[/home/mayur]
└─# lsmod
Module                  Size  Used by
snd_seq_dummy          12288  0
snd_hrtimer            12288  1
snd_seq               114688  7 snd_seq_dummy
snd_seq_device         16384  1 snd_seq
rfkill                 40960  2
qrtr                   57344  4
vboxsf                 49152  0
sunrpc                880640  1
binfmt_misc            28672  1
intel_rapl_msr         20480  0
intel_rapl_common      36864  1 intel_rapl_msr
intel_uncore_frequency_common    16384  0
snd_intel8x0           49152  1
snd_ac97_codec        196608  1 snd_intel8x0
intel_pmc_core        114688  0
intel_vsec             20480  1 intel_pmc_core
ac97_bus               12288  1 snd_ac97_codec
pmt_telemetry          16384  1 intel_pmc_core
snd_pcm               192512  2 snd_intel8x0,snd_ac97_codec
pmt_class              12288  1 pmt_telemetry
rapl                   20480  0
joydev                 24576  0
snd_timer              53248  3 snd_seq,snd_hrtimer,snd_pcm
snd                   155648  10 snd_seq,snd_seq_device,snd_intel8x0,snd_timer,snd_ac97_codec,snd_pcm
soundcore              16384  1 snd
vboxguest              53248  6 vboxsf
```



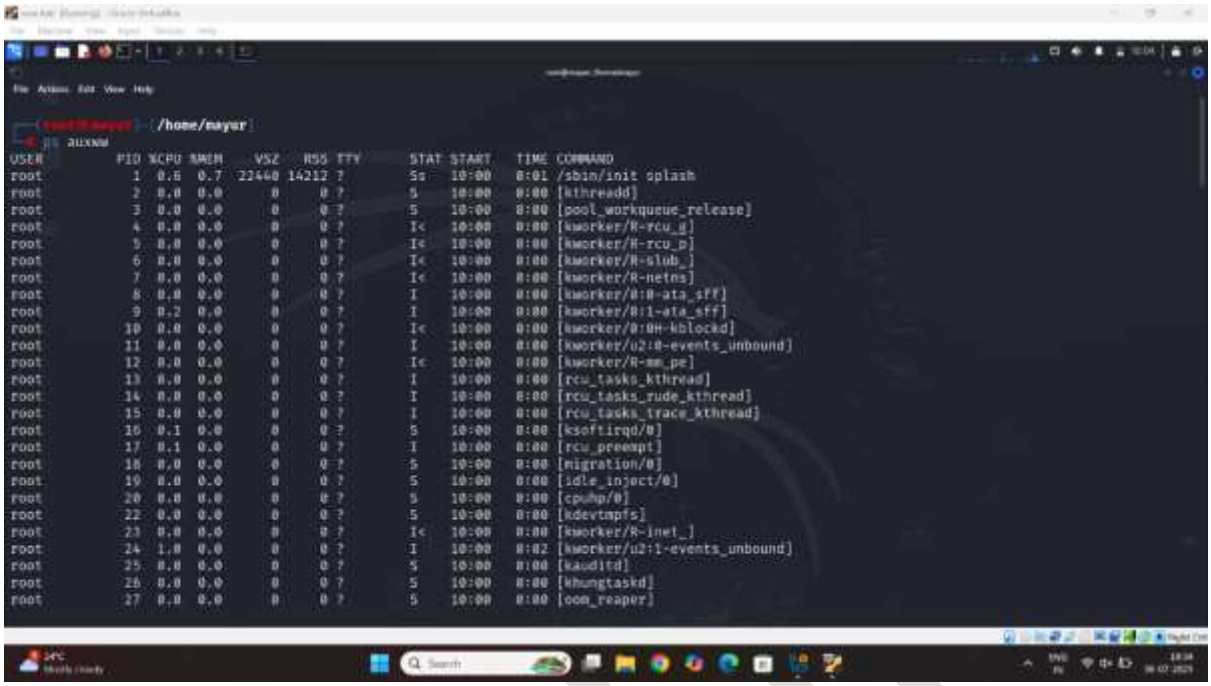
```
File  Actions  Edit  View  Help
libahci                61440  1 ahci
drm_kms_helper        270336  2 vmwgfx
ghash_clmulni_intel    16384  0
ohci_pci               20480  0
ohci_hcd               65536  1 ohci_pci
ehci_pci               16384  0
ehci_hcd              110592  1 ehci_pci
sha512_ssse3           53248  0
usbcore               409600  5 ohci_hcd,ehci_pci,usbhid,ehci_hcd,ohci_pci
libata                471040  4 ata_piix,libahci,ahci,ata_generic
sha512_generic         16384  1 sha512_ssse3
sha256_ssse3           32768  0
scsi_mod              331776  4 sd_mod,libata,sg,sr_mod
sha1_ssse3             32768  0
psmouse               208896  0
drm                   782336  5 vmwgfx,drm_kms_helper,drm_ttm_helper,ttm
usb_common             20480  3 ohci_hcd,usbcore,ehci_hcd
i2c_piix4              28672  0
e1000                 172032  0
scsi_common            16384  5 scsi_mod,sd_mod,libata,sg,sr_mod
video                  77824  0
battery                28672  0
wmi                    32768  1 video
button                 24576  0
aesni_intel           360448  0
crypto_simd            16384  1 aesni_intel
cryptd                 28672  2 crypto_simd,ghash_clmulni_intel

┌──(root㉿kali)-[/home/mayur]
└─#
```

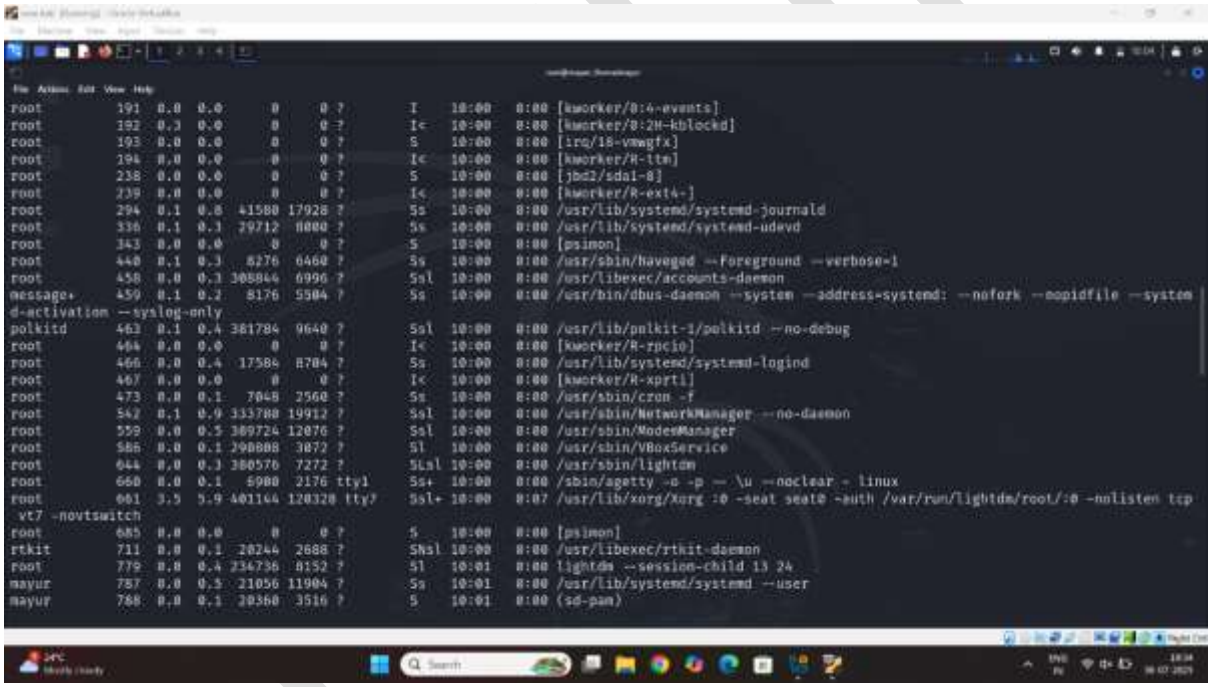
# Step4 lsmod /this command are show list of module



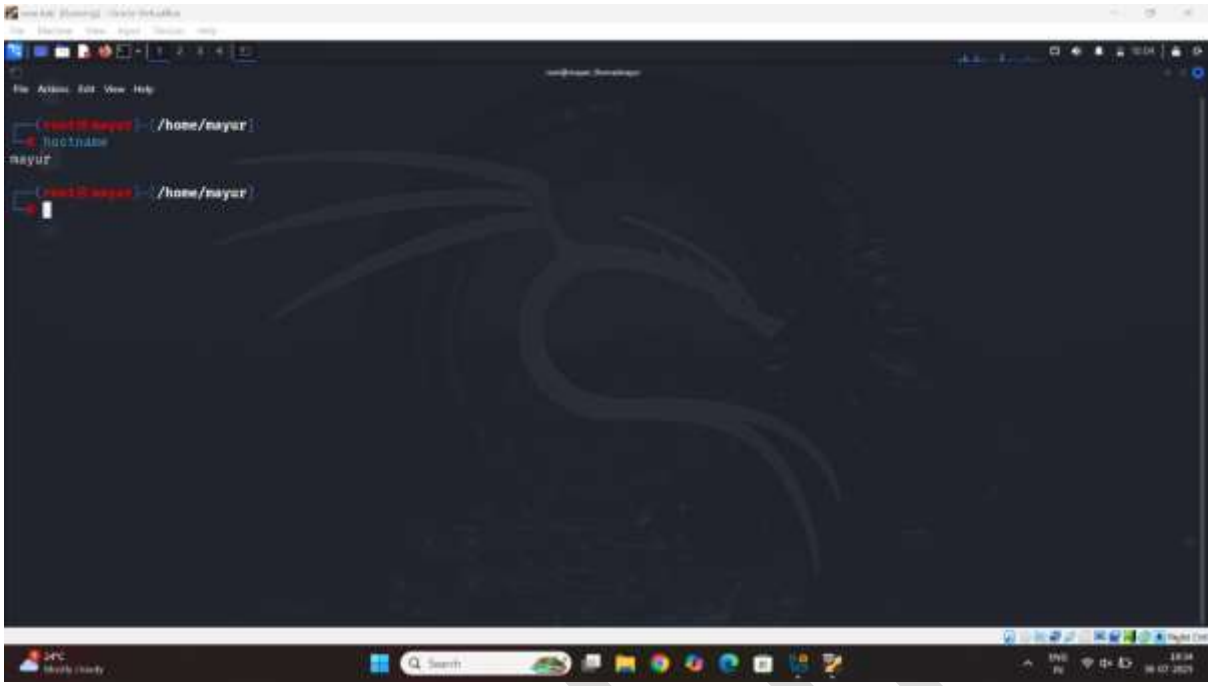




# Step5 ps auxww /this command are checking process all details



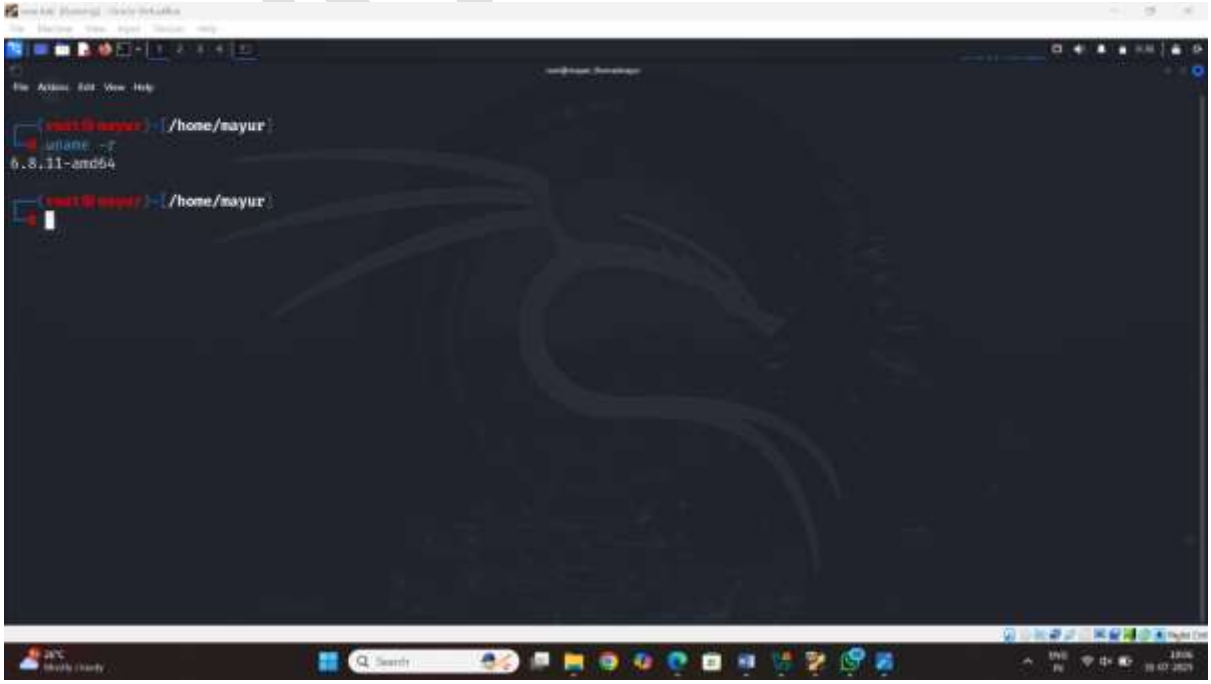




Step6 hostname/this command are use show hostname



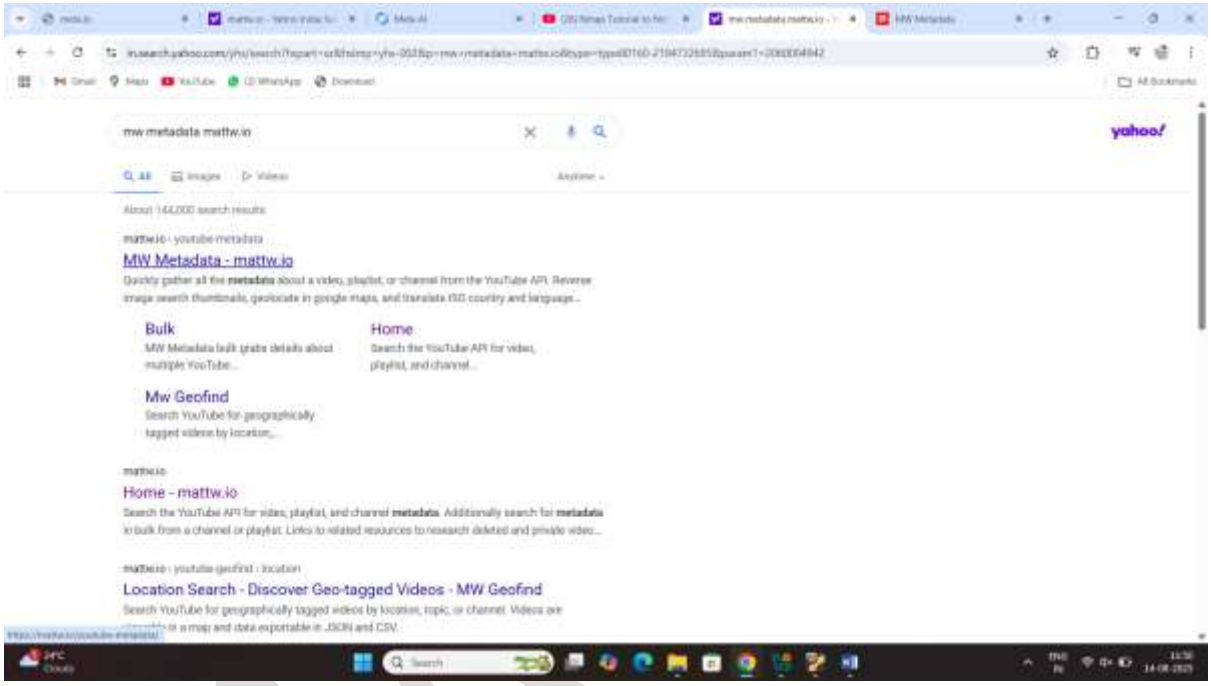

## Lab2 acquire non volatile data in Linux system / hardisk

Step1 uname –r /this command are use system version kernel

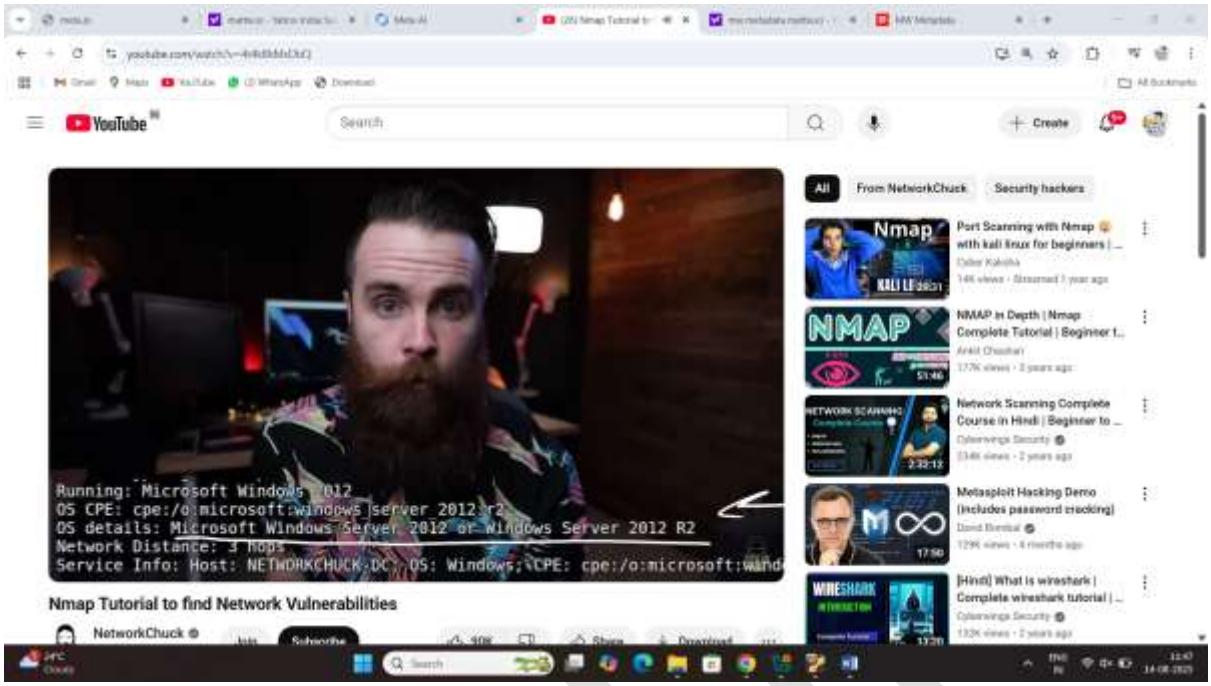


# Lab3 how to image investigation and vedio meta data analysis of image

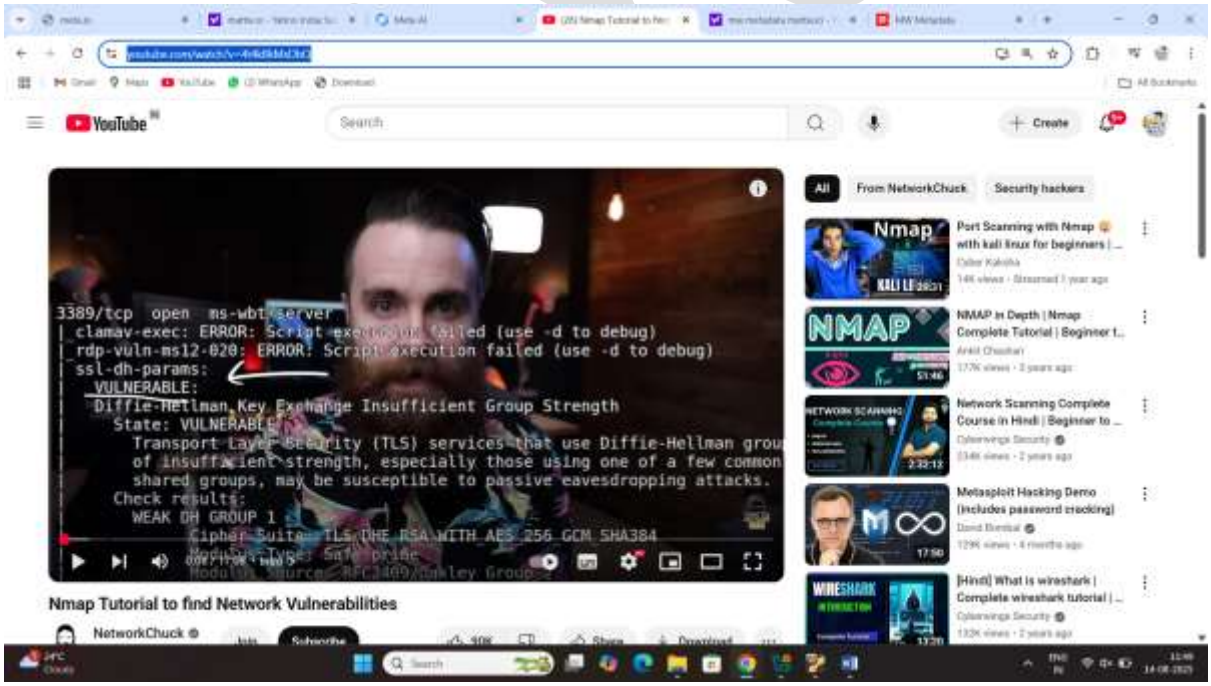
## There was website is mata.io



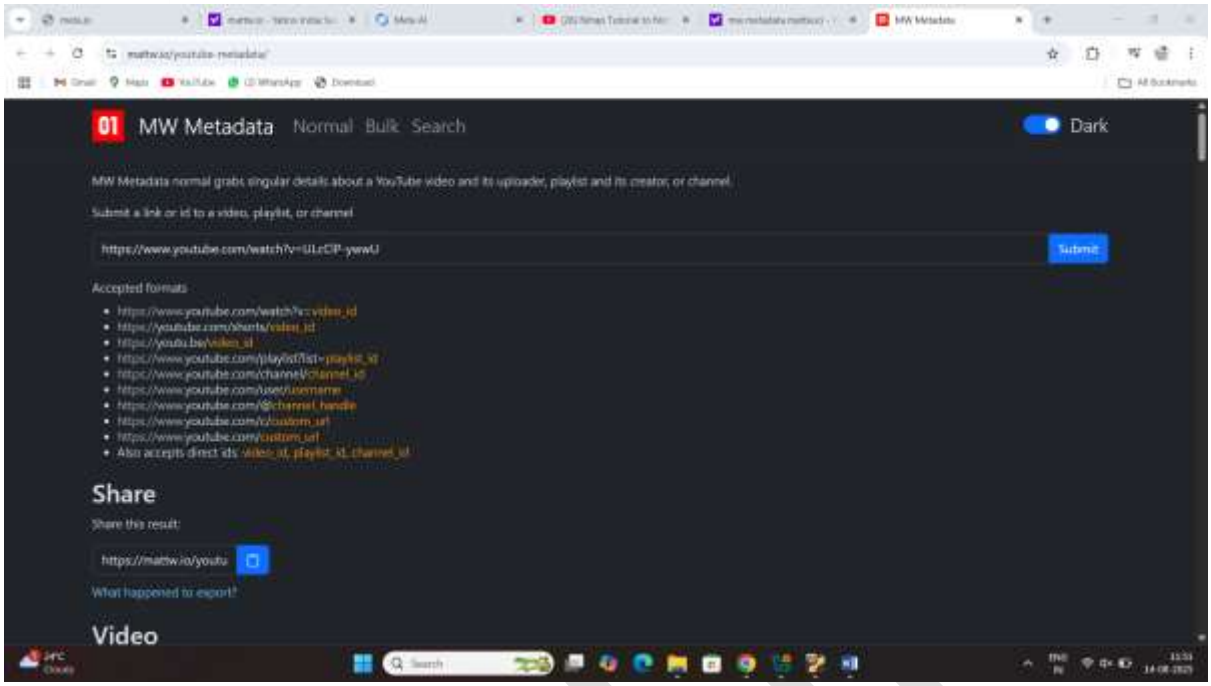

Step2 Select the youtube vedio




Step3 cope the url of vedio

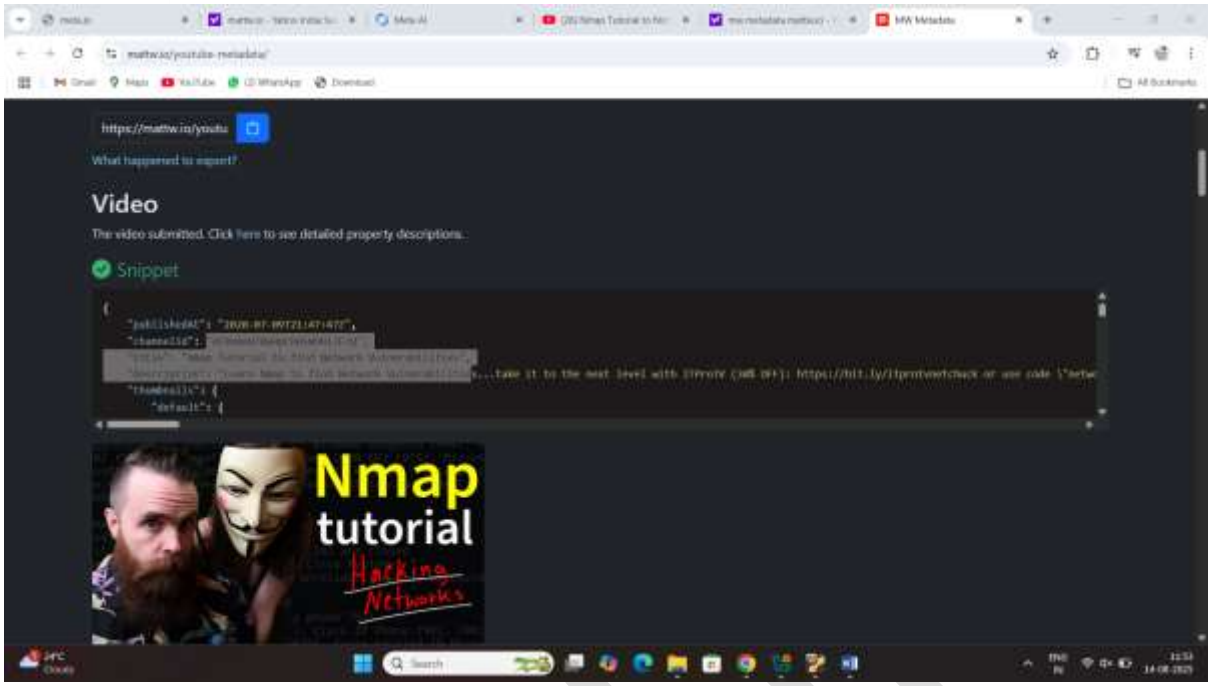


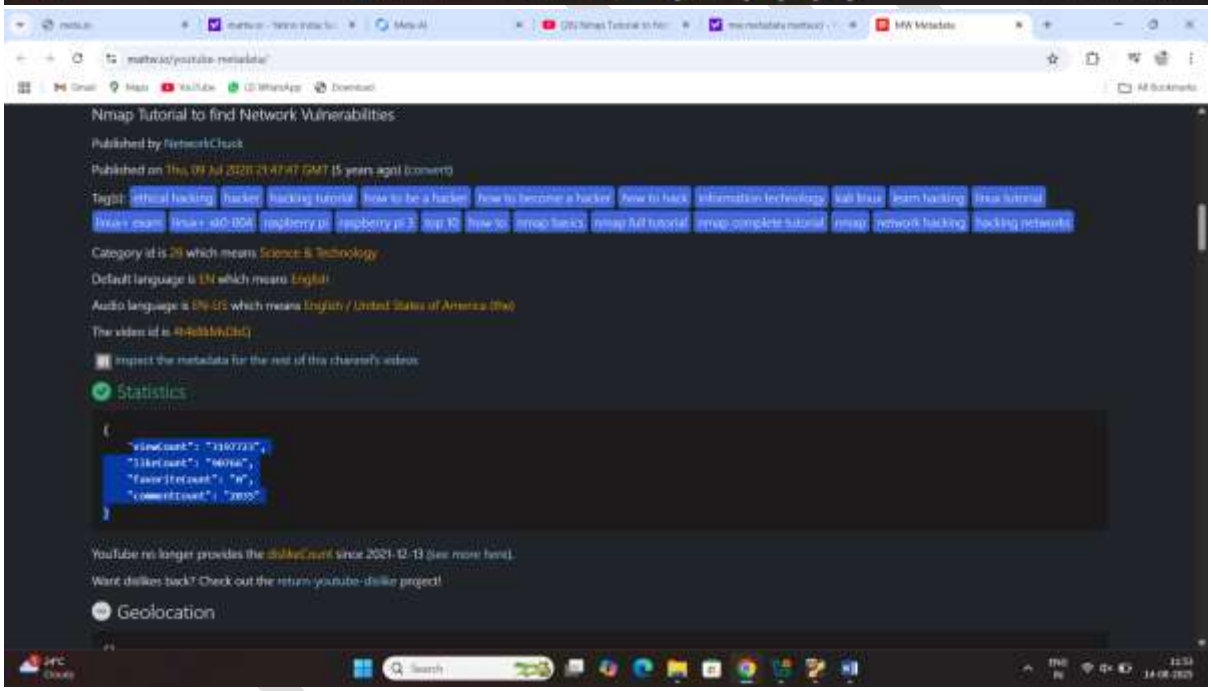

Step4 open the website and paste the vedio url

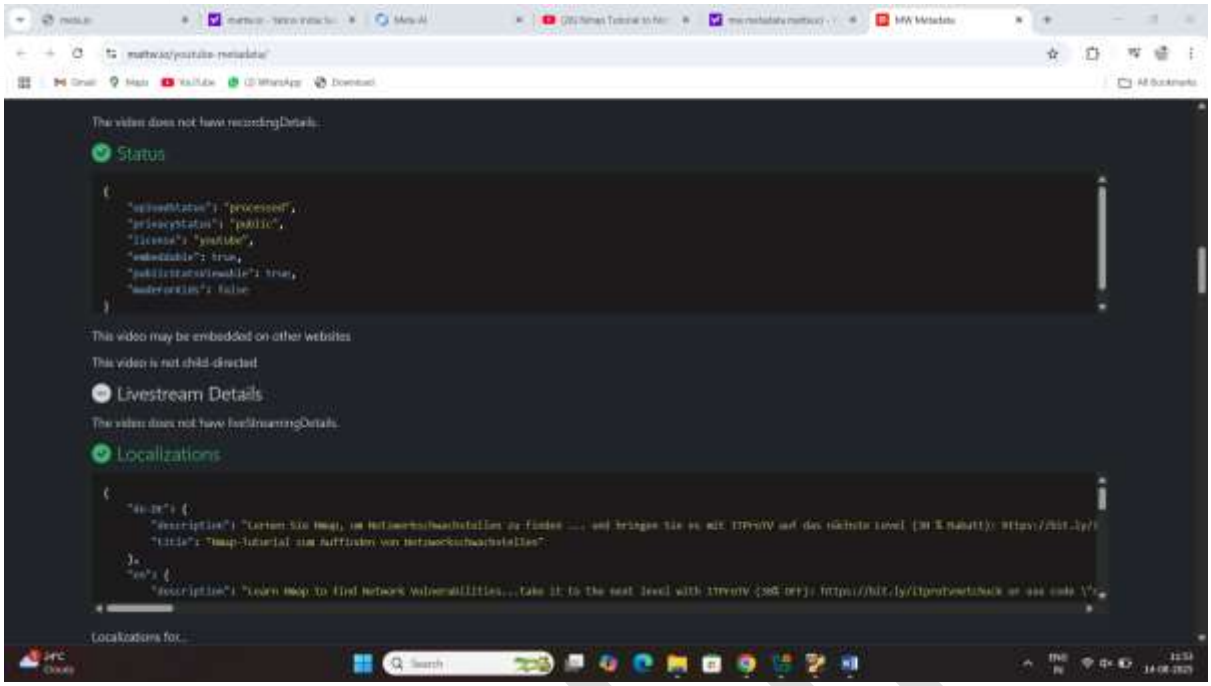


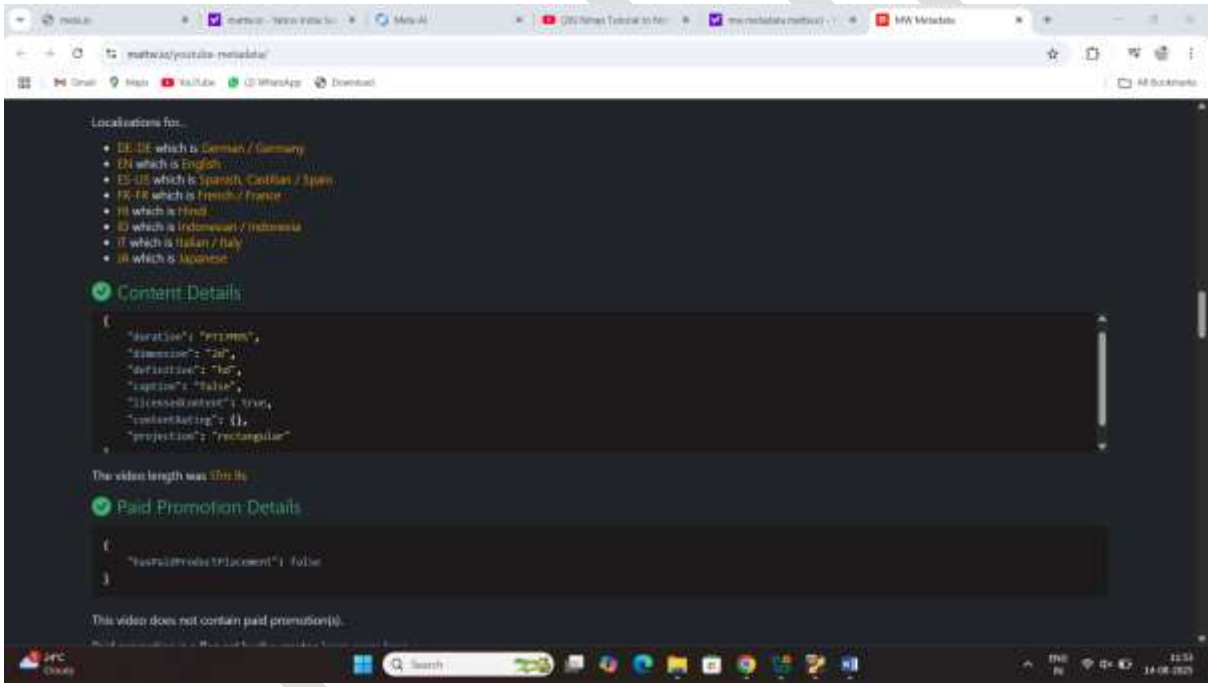

Step5 clcik on the submite button

result:


https://mattw.io/youtu
What happened to export?
Video
The video submitted. Click here to see detailed property descriptions.
Snippet
Nmap
tutorial
Hacking
Networks

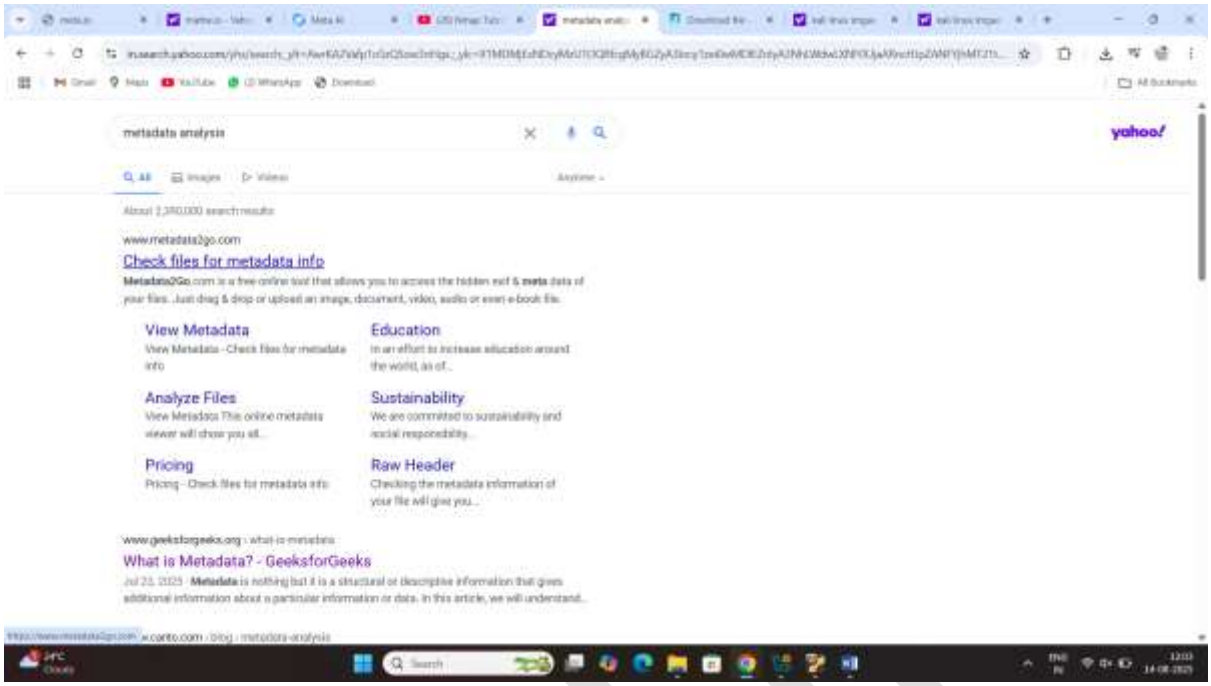

Nmap Tutorial to find Network Vulnerabilities
Published by NetworkChuck
Tags: ethical hacking hacker hacking tutorial how to be a hacker how to become a hacker how to hack information technology kali linux learn hacking linux tutorial
Category id is 28 which means Science & Technology
Default language is EN which means English
Audio language is EN-US which means English / United States of America (the)
Inspect the metadata for the rest of this channel's videos
Statistics
YouTube no longer provides the dislikeCount since 2021-12-13 (see more here).
Want dislikes back? Check out the return-youtube-dislike project!
Geolocation




## Second method image investigation

## There was website meta data analysis

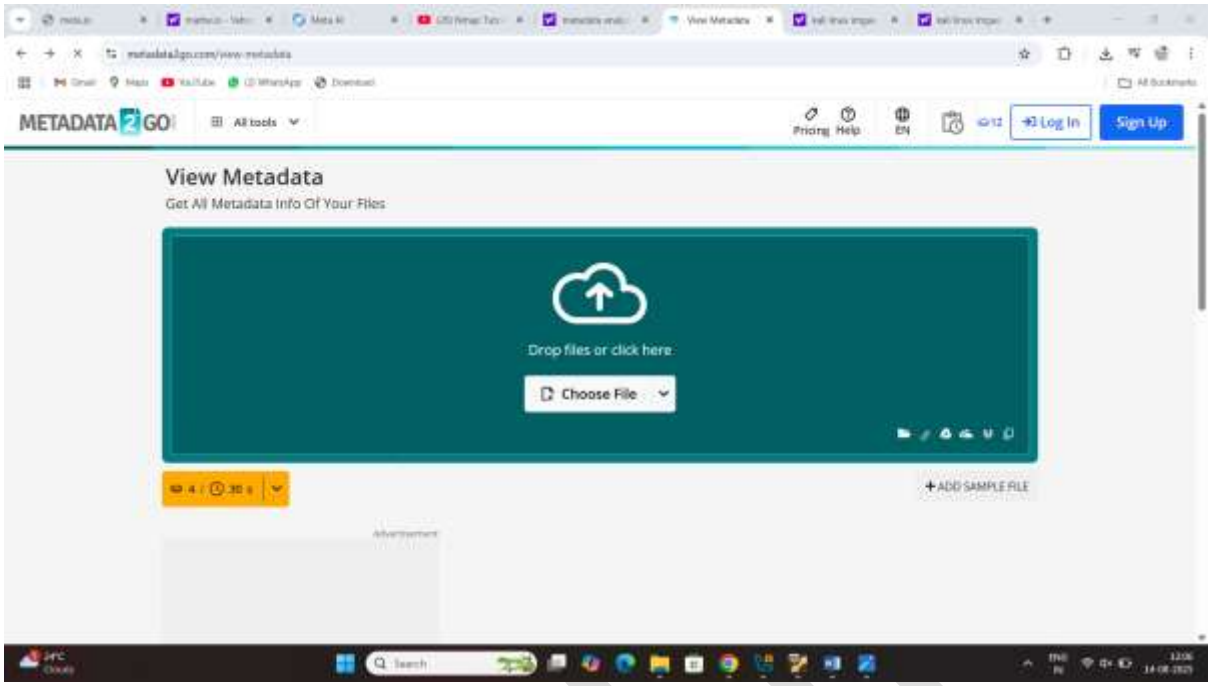



Step2 open the image

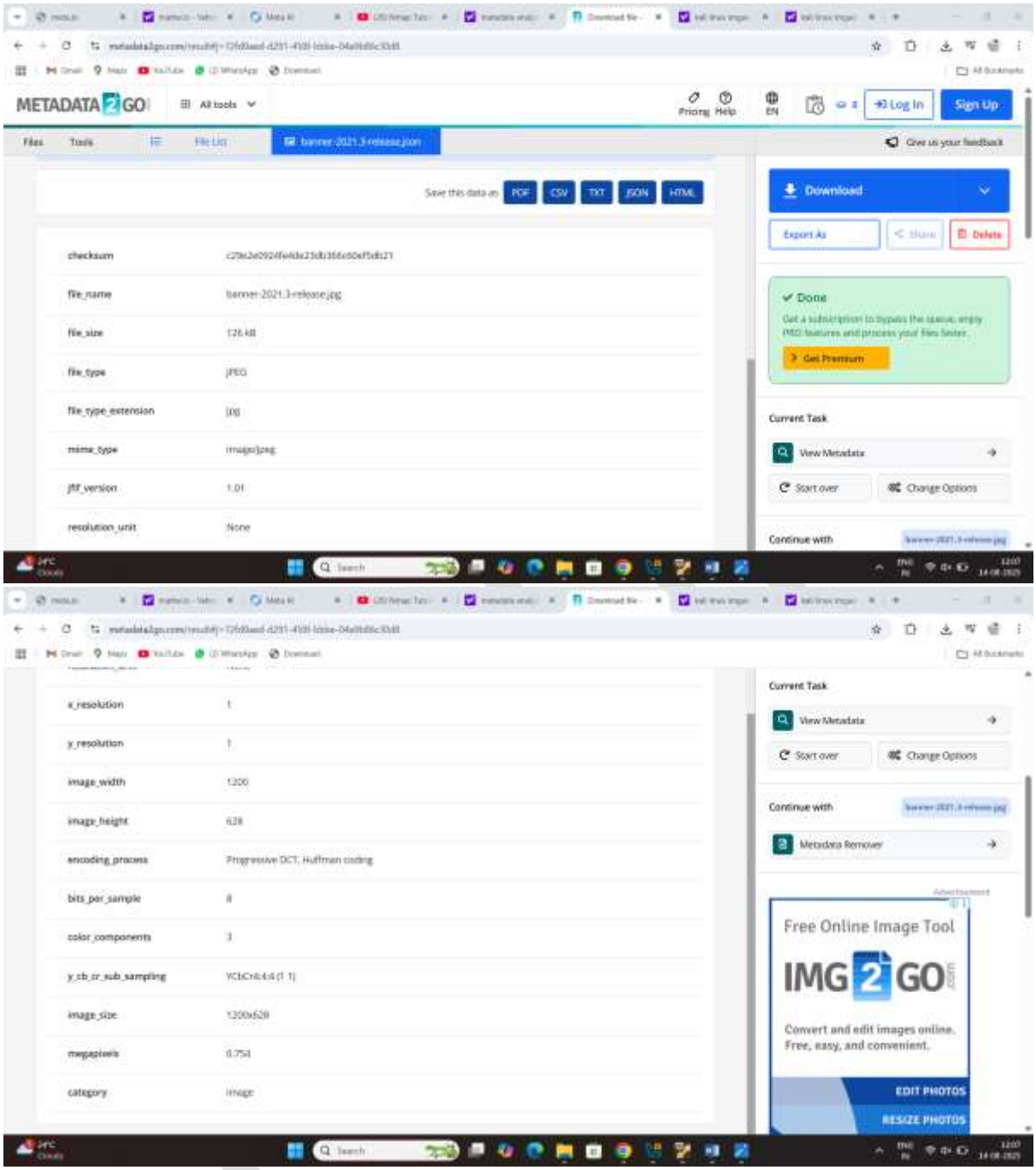
Step3 select the image of investigation

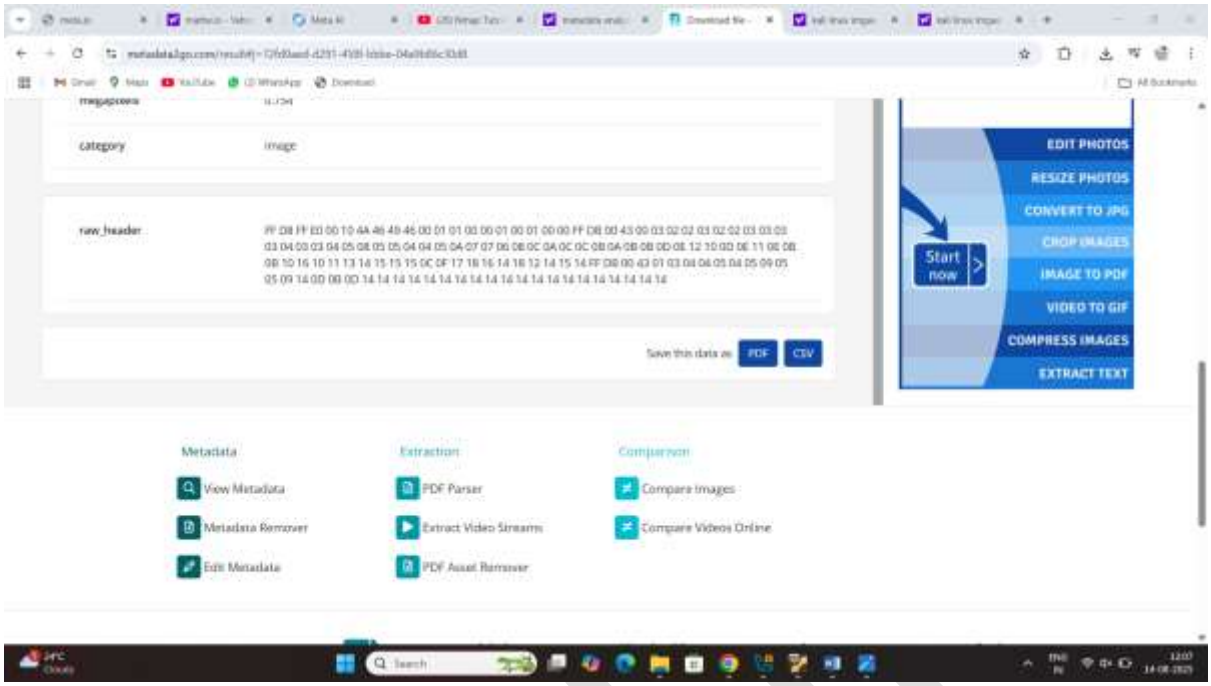

I am select this kali linux image

Step4 open the website click on  option choice




## Result:


METADATA2GO
All tools
Pricing
Help
EN
Log In
Sign Up
Files
Tools
File List
banner-2021.3-release.json
Give us your feedback
Save this data as
PDF
CSV
TXT
JSON
HTML
checksum
file_name
banner-2021.3-release.jpg
file_size
126 kB
file_type
JPEG
file_type_extension
jpg
mime_type
image/jpeg
jfif_version
1.01
resolution_unit
None
Download
Export As
Share
Delete
Done
Get a subscription to bypass the queue, enjoy PRO features and process your files faster.
Get Premium
Current Task
View Metadata
Start over
Change Options
Continue with
x_resolution
1
y_resolution
1
image_width
1200
image_height
628
encoding_process
Progressive DCT, Huffman coding
bits_per_sample
8
color_components
3
y_cb_cr_sub_sampling
YCbCr4:4:4 (1 1)
image_size
1200x628
megapixels
0.754
category
image
Metadata Remover
Advertisement
Free Online Image Tool
IMG 2 GO
Convert and edit images online. Free, easy, and convenient.
EDIT PHOTOS
RESIZE PHOTOS


category
image
raw_header
Save this data as
PDF
CSV
EDIT PHOTOS
RESIZE PHOTOS
CONVERT TO JPG
CROP IMAGES
IMAGE TO PDF
VIDEO TO GIF
COMPRESS IMAGES
EXTRACT TEXT
Start now
Metadata
View Metadata
Metadata Remover
Edit Metadata
Extraction
PDF Parser
Extract Video Streams
PDF Asset Remover
Comparison
Compare Images
Compare Videos Online