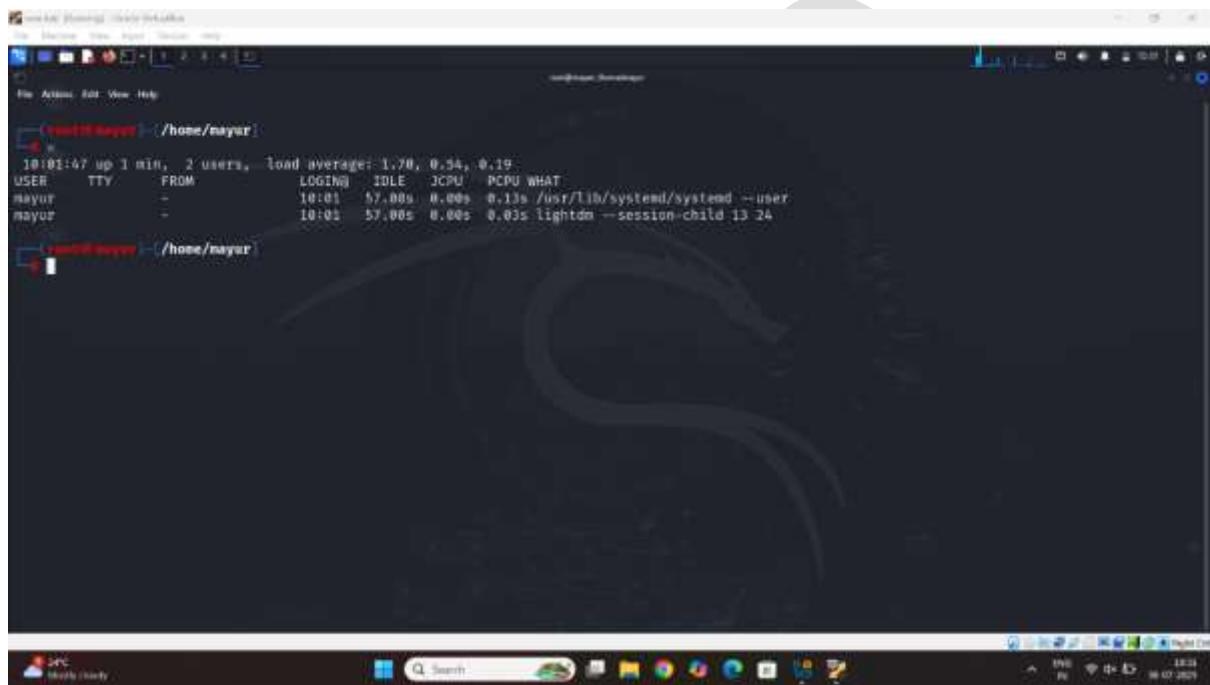


Module 7 Linux and mac forensics

Lab1 Acquire volatile data in Linux system

Step1 on the kali Linux machine

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



```
root@kali:~# w
 10:01:47 up 1 min,  2 users,  load average: 1.70, 0.54, 0.19
USER   TTY      FROM          LOGIN@    IDLE   JCPU   PCPU WHAT
maylor      -          10:01   57.00s  0.00s  0.13s /usr/lib/systemd/systemd --user
maylor      -          10:01   57.00s  0.00s  0.03s lightdm --session-child 13 24
```

Step2 netstat/this command show network statitics

```
(vagrant@kali: ~) /home/mayer
[vagrant@kali: ~] - netstat
Active Internet connections (w/o servers)
Proto Recv-Q Local Address           Foreign Address         State
udp        0      192.168.2.35:bootpc    192.168.2.2: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  3      [ ]        STREAM    CONNECTED  8552  @/tmp/.ICE-unix/828
unix  3      [ ]        STREAM    CONNECTED  8239
unix  3      [ ]        STREAM    CONNECTED  9678
unix  3      [ ]        STREAM    CONNECTED  7821
unix  3      [ ]        STREAM    CONNECTED  8934
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  8938  /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
[vagrant@kali: ~] - netstat
Active Internet connections (w/o servers)
Proto Recv-Q Local Address           Foreign Address         State
unix  3      [ ]        STREAM    CONNECTED  8934
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  8938  /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  8884
unix  3      [ ]        STREAM    CONNECTED  8233
unix  3      [ ]        STREAM    CONNECTED  9681
unix  3      [ ]        STREAM    CONNECTED  9874
unix  3      [ ]        STREAM    CONNECTED  8933  /run/systemd/journal/stdout
unix  3      [ ]        STREAM    CONNECTED  5282
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  3      [ ]        DGRAM   CONNECTED  9781
unix  3      [ ]        STREAM    CONNECTED  9186
unix  3      [ ]        STREAM    CONNECTED  7718  /run/systemd/journal/stdout
unix  3      [ ]        STREAM    CONNECTED  7872
```

Step3 lsof /this command show list open file of machine

```

lsof
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           48960  2
qrtr            57344  4
vboxsf           49352  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   196688  1 snd_intel8x0
intel_pmc_core   114688  0
intel_vsec        20480  1 intel_pmc_core
ac97_bus         12288  1 snd_ac97_codec
pm_telemetry     16384  1 intel_pmc_core
snd_pcm          192512  2 snd_intel8x0,snd_ac97_codec
pm_class          12288  1 pm_telemetry
rapl             20480  0
joydev            24576  0
snd_timer         53248  3 snd_seq,snd_hrtimer,snd_pcm
snd              155648  18 snd_seq,snd_seq_device,snd_intel8x0,snd_timer,snd_ac97_codec,snd_pcm
soundcore         16384  1 snd
vboxguest         53248  6 vboxsf

```

```

lsof
libahci          65440  1 ahci
dm_kms_helper   270336  2 vmmqfx
ghash_clemlmi_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    33248  0
usbcore          48960  3 ohci_hcd,ehci_pci,usbhid,ehci_hcd,ohci_pci
libata           471840  4 ata_piix,libahci,ohci,ata_generic
sha512_generic   16384  1 sha512_ssse3
sha256_ssse3    32768  0
scsi_mod         31176  4 sd_mod,libata,sg,sr_mod
sha1_ssse3       32768  0
pmevent          208896  0
drm              782336  6 vmmqfx,dm_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
acenzi_intel     360448  0
crypto_sind      16384  1 acenzi_intel
cryptd           28672  2 crypto_sind,ghash_clemlmi_intel

```

Step4 lsmod /this command are show list of module

```
(root@Mayur: ~) [ - ] lsmod
Module           Size  Used by
snd_seq_dummy    12288  0
snd_hrtimer      12288  1
snd_seq          114088  7 snd_seq_dummy
snd_seq_device   16384  1 snd_seq
rfkill          48960  2
qtr              57344  4
voxsf            49152  0
sunrpc           850640  1
binfmt_misc     28672  1
intel_rapl_nsr  20480  0
intel_rapl_common 36864  1 intel_rapl_ms
intel_uncore_frequency_common 16384  0
snd_intel8x0    49152  1
snd_ac97_codec  196088  1 snd_intel8x0
intel_pmc_core  114688  0
intel_vsec       20480  1 intel_pmc_core
ac97_bus         12288  1 snd_ac97_codec
pm_telemetry     16384  1 intel_pmc_core
snd_pcm          192532  2 snd_intel8x0,snd_ac97_codec
pm_class         12288  1 pm_telemetry
rapl             20480  0
joydev           24576  0
snd_timer        33248  3 snd_seq,snd_hrtimer,snd_pcm
snd              159648  10 snd_seq,snd_seq_device,snd_intel8x0,snd_timer,snd_ac97_codec,snd_pcm
soundcore        16384  1 snd
vboxguest        53248  6 vboxsf
```

```
(root@Mayur: ~) [ - ] lsmod
Module           Size  Used by
libahci          65440  1 ahci
dm_kms_helper   270336  2 vmmqfx
ghash_clemlini_intel 16384  0
ohci_pci         20480  0
ohci_hcd         65536  1 ohci_pci
ehci_pci         16384  0
ehci_hcd         130992  1 ehci_pci
sha512_ssse3    33248  0
usbcore          469680  5 ohci_hcd,ehci_pci,usbhid,ehci_hcd,ohcs_pci
libata           475840  4 ata_piix,libahci,ahci,ata_generic
sha512_generic  16384  1 sha512_ssse3
sha256_ssse3    32768  0
scsi_mod        131776  4 sd_mod,libata,sg,sr_mod
shai_ssse3      32768  0
pmouse          208960  0
drm              782336  5 vmmqfx,dm_kms_helper,drm_ttma_helper,tta
usb_common       10480  3 ohci_hcd,usbcore,ehci_hcd
i2c_piix4       28672  0
el000            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
acsnl_intel     360448  0
crypto_simd     16384  1 acsnl_intel
cryptd           28672  2 crypto_simd,ghash_clemlini_intel
```

Step5 ps auxww /this command are checking process all details

```

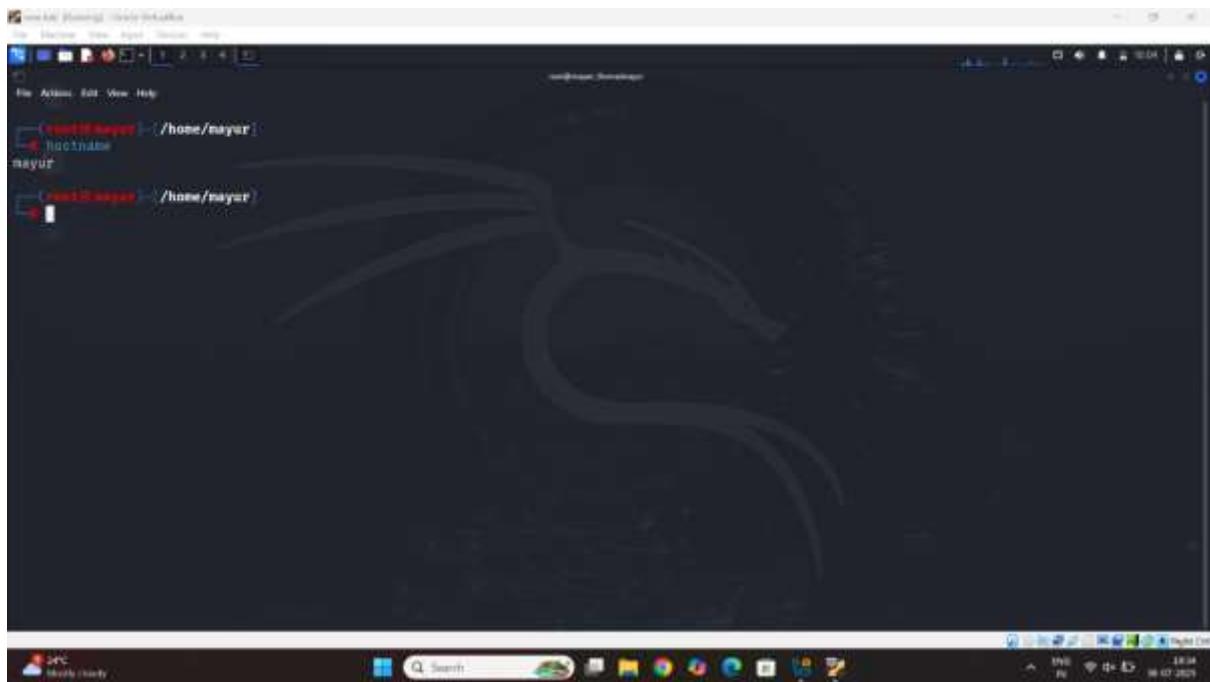
top - 10:00:00 up 1 day, 1 min, 0 users, load average: 0.00, 0.00, 0.00
Tasks: 210 total, 0 running, 210 sleeping, 0 stopped, 0 zombie
CPU states: 0.6% user, 0.7% nice, 22.4% sys, 76.7% idle
Memory: 194M total, 188M used, 6M free, 0K shmem
Swap: 0K total, 0K used, 0K free, 0K reserved, 0K available

PID USER      CPU %  VSZ   RSS TTY      STAT START  TIME COMMAND
  1 root      0.6  0.7 22440 14212 ?    S  10:00  0:01 /sbin/init splash
  2 root      0.0  0.0     0  0 ?    S  10:00  0:00 [kthreadd]
  3 root      0.0  0.0     0  0 ?    S  10:00  0:00 [pool_workqueue_release]
  4 root      0.0  0.0     0  0 ?    I< 10:00  0:00 [kworker/R-rcu_g]
  5 root      0.0  0.0     0  0 ?    I< 10:00  0:00 [kworker/R-rcu_p]
  6 root      0.0  0.0     0  0 ?    I< 10:00  0:00 [kworker/H-slab_]
  7 root      0.0  0.0     0  0 ?    I< 10:00  0:00 [kworker/H-nets_]
  8 root      0.0  0.0     0  0 ?    I< 10:00  0:00 [kworker/H-ata_sff]
  9 root      0.2  0.0     0  0 ?    I< 10:00  0:00 [kworker/B1-ata_sff]
 10 root      0.0  0.0     0  0 ?    I< 10:00  0:00 [kworker/B1H-kblockd]
 11 root      0.0  0.0     0  0 ?    I< 10:00  0:00 [kworker/u2:0-events_unbound]
 12 root      0.0  0.0     0  0 ?    I< 10:00  0:00 [kworker/H-mm_pel]
 13 root      0.0  0.0     0  0 ?    I< 10:00  0:00 [rcu_tasks_kthread]
 14 root      0.0  0.0     0  0 ?    I< 10:00  0:00 [rcu_tasks_rude_kthread]
 15 root      0.0  0.0     0  0 ?    I< 10:00  0:00 [rcu_tasks_trace_kthread]
 16 root      0.1  0.0     0  0 ?    S  10:00  0:00 [ksoftirqd/0]
 17 root      0.1  0.0     0  0 ?    I< 10:00  0:00 [rcu_preempt]
 18 root      0.0  0.0     0  0 ?    S  10:00  0:00 [migration/0]
 19 root      0.0  0.0     0  0 ?    S  10:00  0:00 [idle_inject/0]
 20 root      0.0  0.0     0  0 ?    S  10:00  0:00 [cpuhp/0]
 21 root      0.0  0.0     0  0 ?    S  10:00  0:00 [kdevtmpfs]
 22 root      0.0  0.0     0  0 ?    I< 10:00  0:00 [kworker/H-inet_]
 23 root      1.0  0.0     0  0 ?    I< 10:00  0:02 [kworker/u2:1-events_unbound]
 24 root      0.0  0.0     0  0 ?    S  10:00  0:00 [kauuidd]
 25 root      0.0  0.0     0  0 ?    S  10:00  0:00 [khungtaskd]
 26 root      0.0  0.0     0  0 ?    S  10:00  0:00 [oom_reaper]
 27 root      0.0  0.0     0  0 ?    S  10:00  0:00 [oom_reaper]

  191 root      0.0  0.0     0  0 ?    I  10:00  0:00 [kworker/B4-events]
 192 root      0.1  0.0     0  0 ?    I< 10:00  0:00 [kworker/B2H-kblockd]
 193 root      0.0  0.0     0  0 ?    S  10:00  0:00 [irq/18-vmwgfx]
 194 root      0.0  0.0     0  0 ?    I< 10:00  0:00 [kworker/H-itm]
 238 root      0.0  0.0     0  0 ?    S  10:00  0:00 [jbd2/sdal-8]
 239 root      0.0  0.0     0  0 ?    I< 10:00  0:00 [kworker/H-ext4-]
 294  0.1  0.6 41580 17928 ?    Ss 10:00  0:00 /usr/lib/systemd/systemd-journal
 336  0.1  0.1 29712 8880 ?    Ss 10:00  0:00 /usr/lib/systemd/systemd-udevd
 343  0.0  0.0     0  0 ?    S  10:00  0:00 [psimon]
 440  0.1  0.3 8176 6460 ?    Ss 10:00  0:00 /usr/sbin/Naevged --Foreground --verbose-i
 458  0.0  0.3 308846 6996 ?    Ssl 10:00  0:00 /usr/libexec/accounts-daemon
 message+ 459  0.1  0.2 8176 5584 ?    Ss 10:00  0:00 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
 polkitd  463  0.1  0.4 381784 9640 ?    Ssl 10:00  0:00 /usr/lib/polkit-1/polkitd --no-debug
 464  0.0  0.0     0  0 ?    I< 10:00  0:00 [kworker/H-rpcio]
 466  0.0  0.4 17584 8784 ?    Ss 10:00  0:00 /usr/lib/systemd/systemd-logind
 467  0.0  0.0     0  0 ?    I< 10:00  0:00 [kworker/H-xprt]
 473  0.0  0.1 7648 2568 ?    Ss 10:00  0:00 /usr/sbin/cron -f
 542  0.1  0.0 333788 19912 ?    Ssl 10:00  0:00 /usr/sbin/NetworkManager --no-daemon
 559  0.0  0.5 389724 12076 ?    Ssl 10:00  0:00 /usr/sbin/ModemManager
 585  0.0  0.1 298888 3872 ?    Ssl 10:00  0:00 /usr/sbin/VBoxService
 644  0.0  0.3 380576 7272 ?    Ssl 10:00  0:00 /usr/sbin/lightdm
 660  0.0  0.1 5980 2176 ttys1  Ss+ 10:00  0:00 /sbin/agetty -p - \u -noclear - linux
 661  0.5  0.9 401144 120328 ttys1  Ssl+ 10:00  0:07 /usr/lib/xorg/xorg :0 -seat seat0 -auth /var/run/lightdm/root/:0 -nolisten tcp vt7 -novtswitch
 685  0.0  0.0     0  0 ?    S  10:00  0:00 [psimon]
 rtkit  711  0.0  0.1 28244 2888 ?    Ssl 10:00  0:00 /usr/libexec/rtkit-daemon
 779  0.0  0.4 234736 8152 ?    Sl 10:01  0:00 lightdm --session-child 13 24
 mayer  787  0.0  0.3 21056 11904 ?    Ss 10:01  0:00 /usr/lib/systemd/systemd --user
 mayer  788  0.0  0.1 20368 3516 ?    S  10:01  0:00 (sd-pam)

```

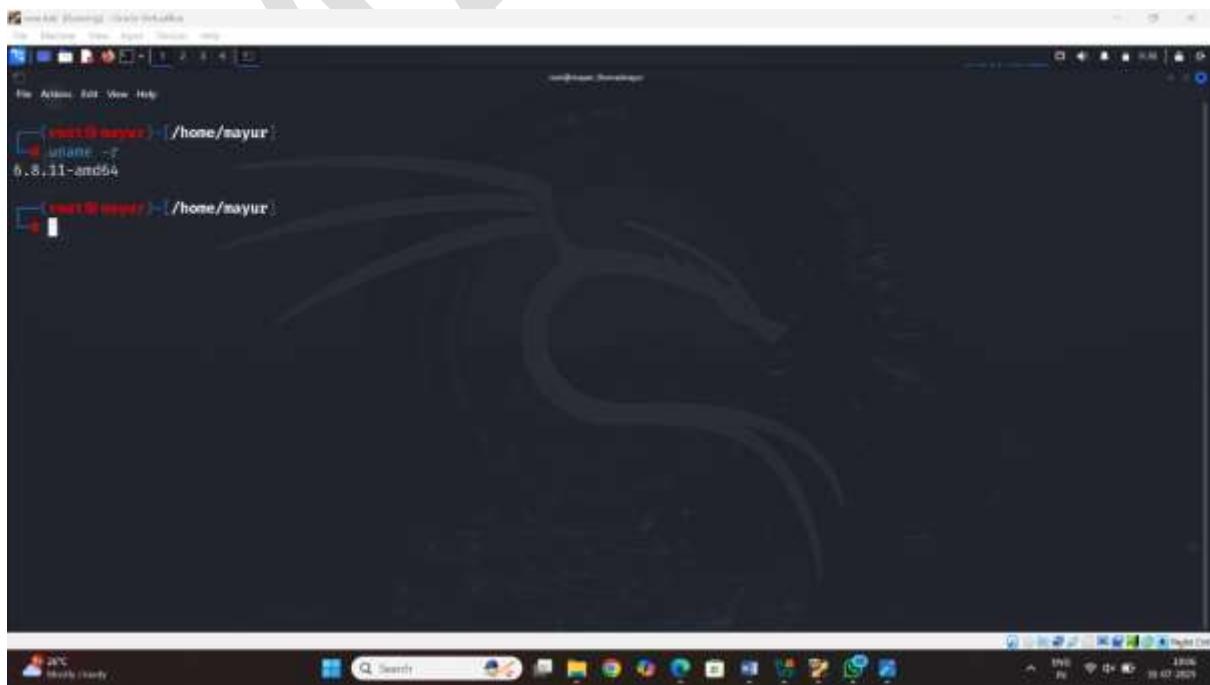
Step6 hostname/this command are use show hostname



```
root@Mayur:~# cat /etc/hostname
Mayur
root@Mayur:~#
```

Lab2 acquire non volatile data in Linux system / hardisk

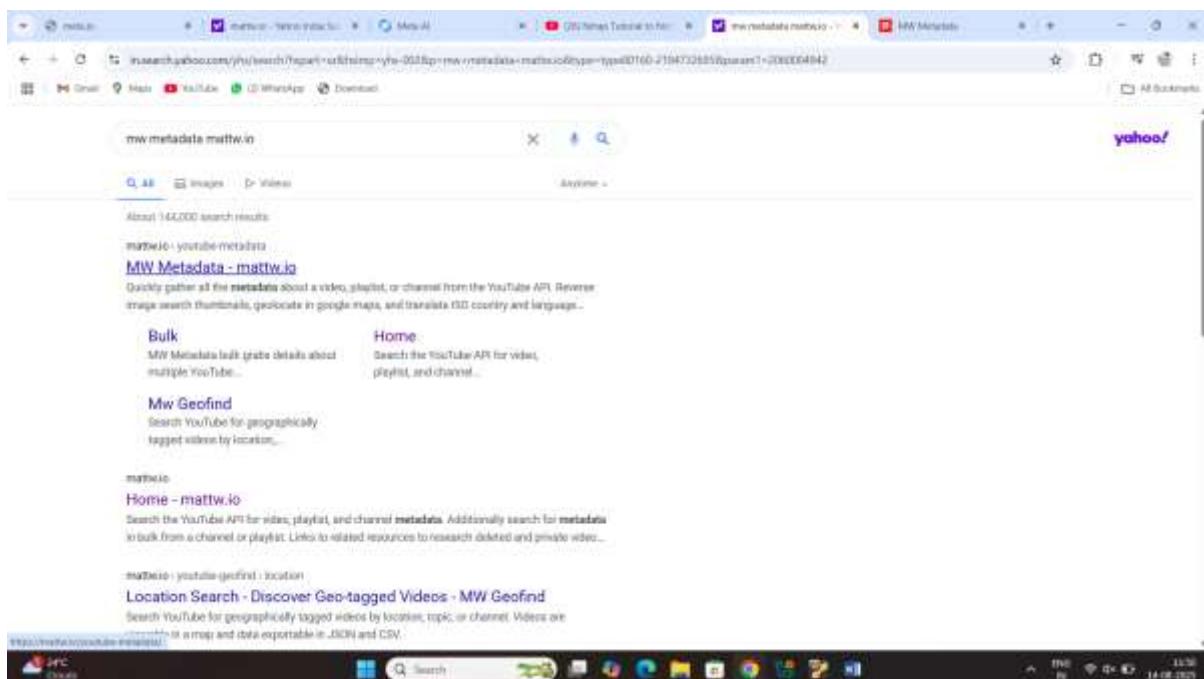
Step1 uname -r /this command are use system version kernel



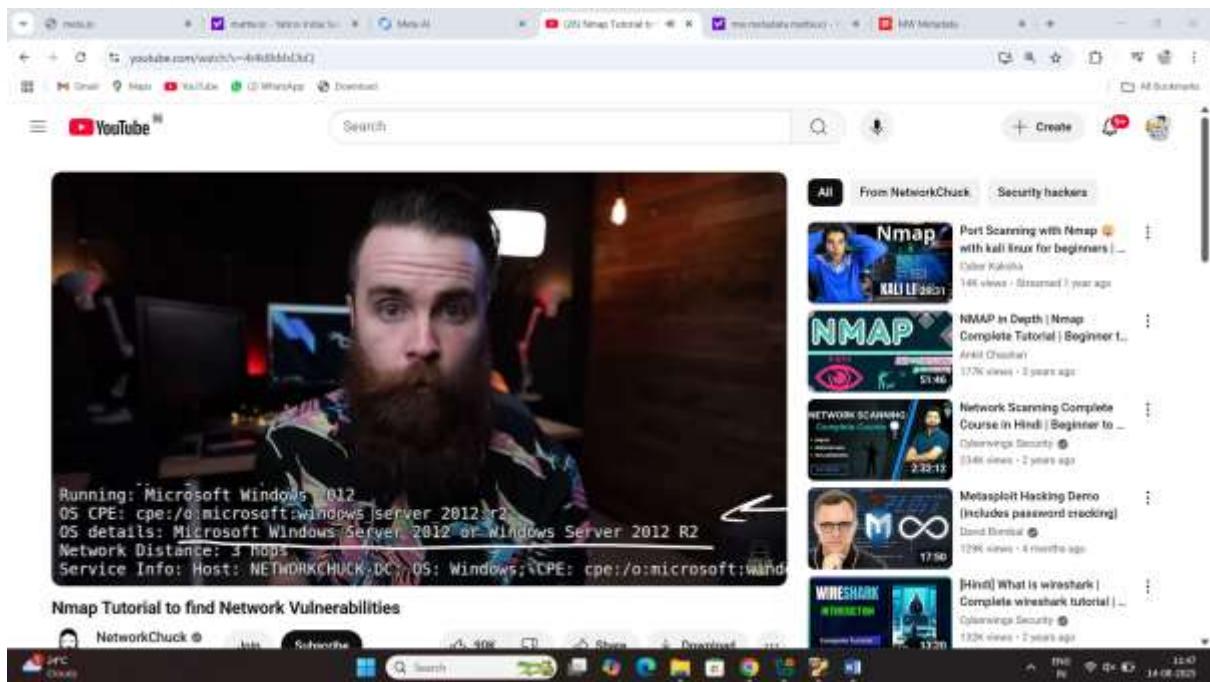
```
root@Mayur:~# uname -r
4.8.11-ard64
root@Mayur:~#
```

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

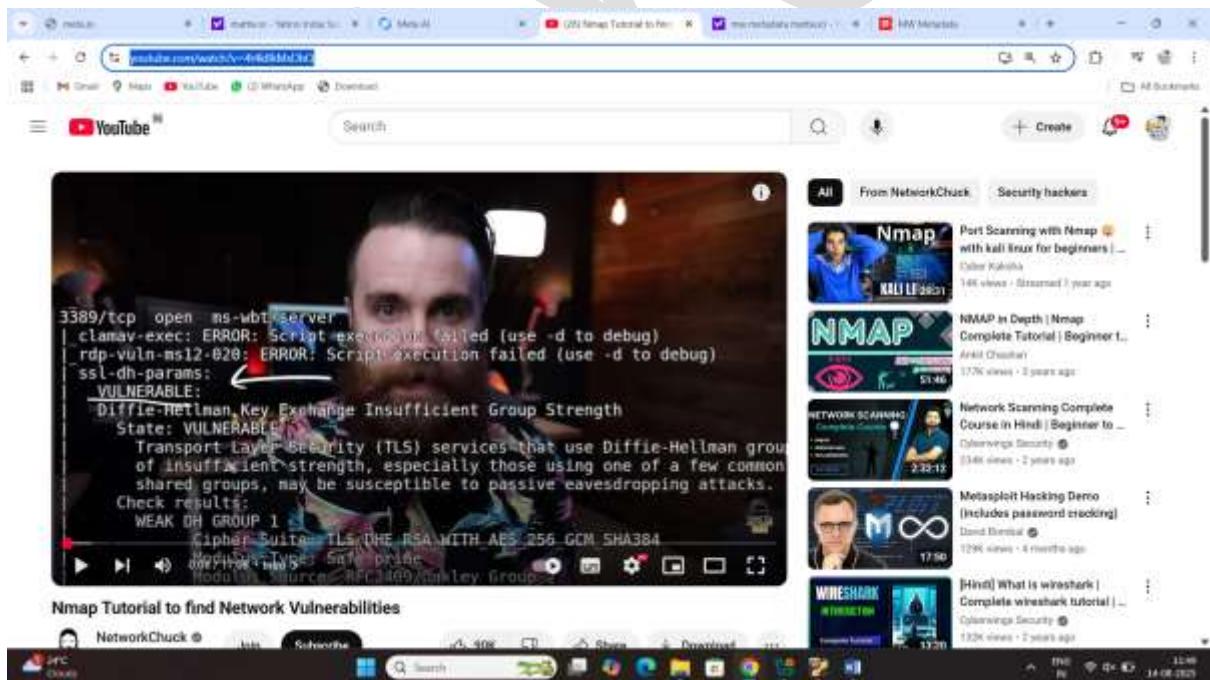
There was website is mata.io



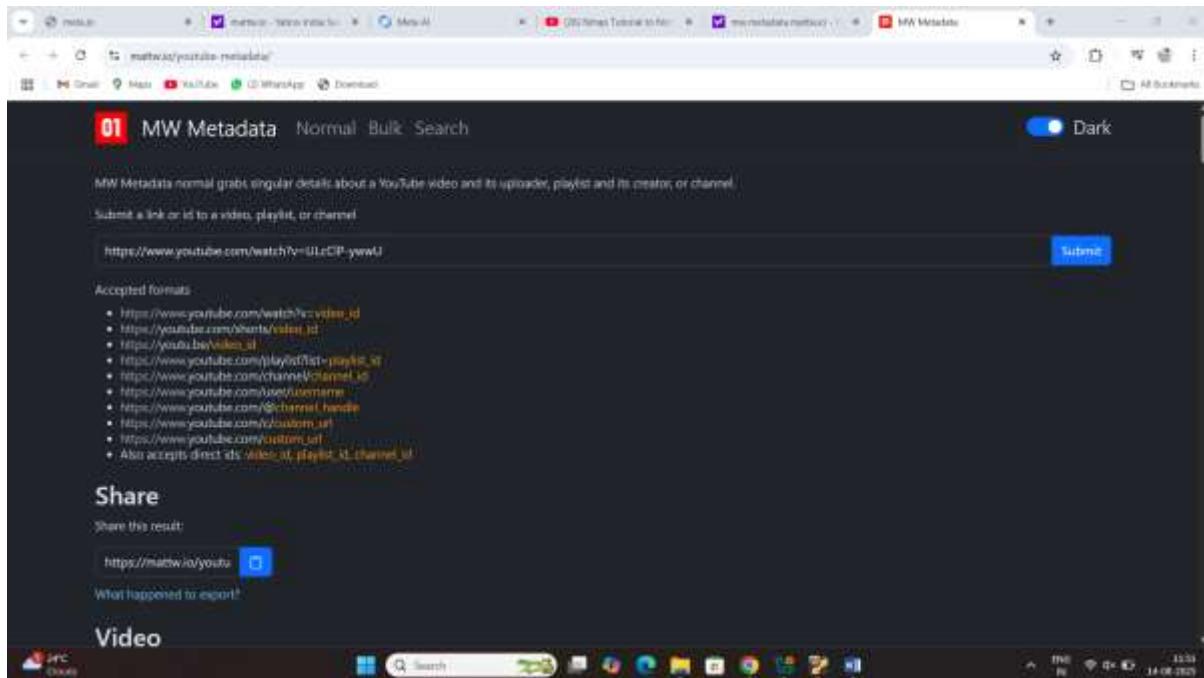
Step2 Select the youtube vedio



Step3 cope the url of vedio

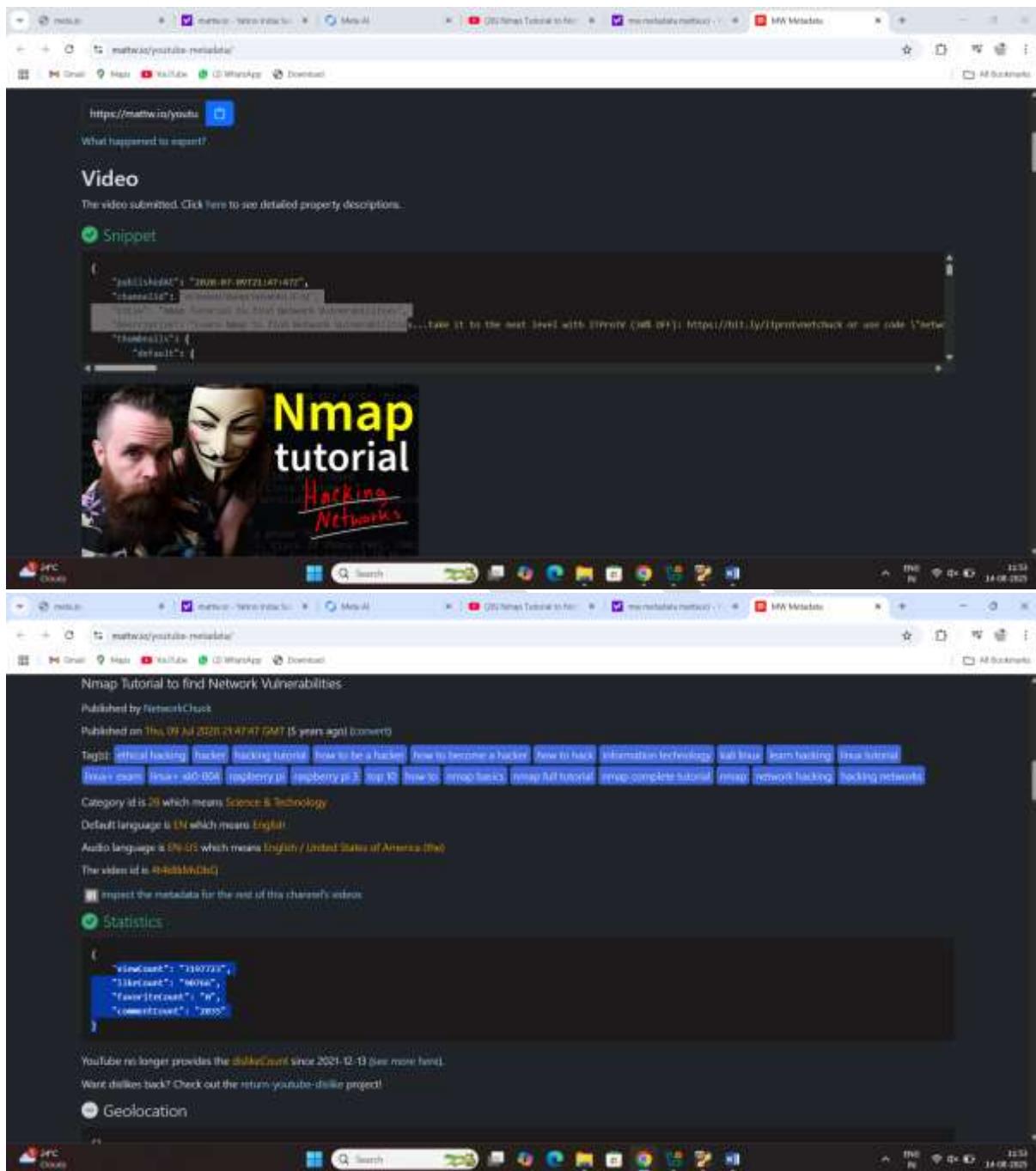


Step4 open the website and paste the vedio url



Step5 click on the submit button

result:



The video does not have recording details.

Status

```
{
  "status": "processed",
  "privacyStatus": "public",
  "license": "youtube",
  "embeddable": true,
  "publicizable": true,
  "muted": false
}
```

This video may be embedded on other websites.

This video is not child-directed.

Livestream Details

The video does not have livestreamingDetails.

Localizations

```
{
  "de_DE": {
    "description": "Dort sind Map, die Netzwerkschachtaufgaben zu finden ... und bringen sie es wie Lernaktiv auf das nächste Level (siehe Bildschirm): https://bit.ly/2kzJyfj"
  },
  "en": {
    "description": "Learn how to find Network Minigames... take it to the next level with Lernaktiv (siehe Bildschirm): https://bit.ly/2kzJyfj or see code X"
  }
}
```

Localizations for...

Localizations for...

- DE-DE which is German / Germany
- EN which is English
- ES-ES which is Spanish / Castilian / Spain
- FR-FR which is French / France
- IT-IT which is Hindi
- ID-ID which is Indonesian / Indonesia
- IT-IT which is Italian / Italy
- JA-JA which is Japanese

Content Details

```
{
  "duration": "PT2M3S",
  "dimension": "2D",
  "definition": "720p",
  "caption": "false",
  "licensedContent": true,
  "contentRating": 0,
  "projection": "rectangular"
}
```

The video length was 2m 3s.

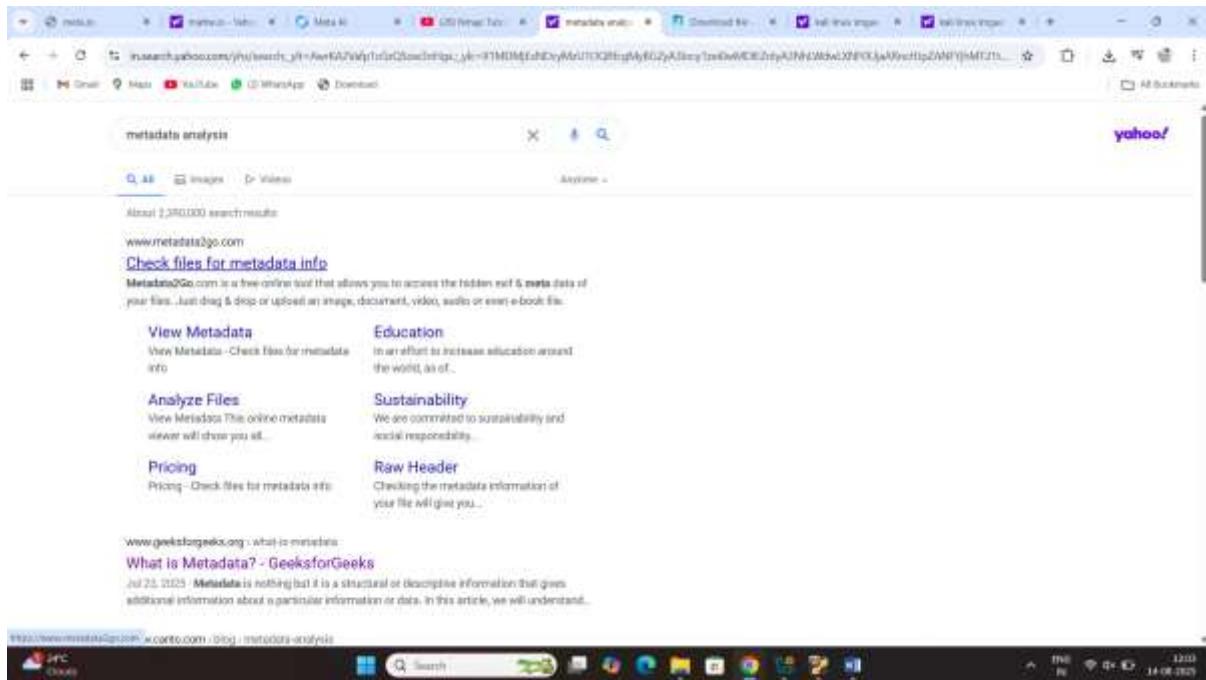
Paid Promotion Details

```
{
  "isPromotional": false
}
```

This video does not contain paid promotion(s).

Second method image investigation

There was website meta data analysis



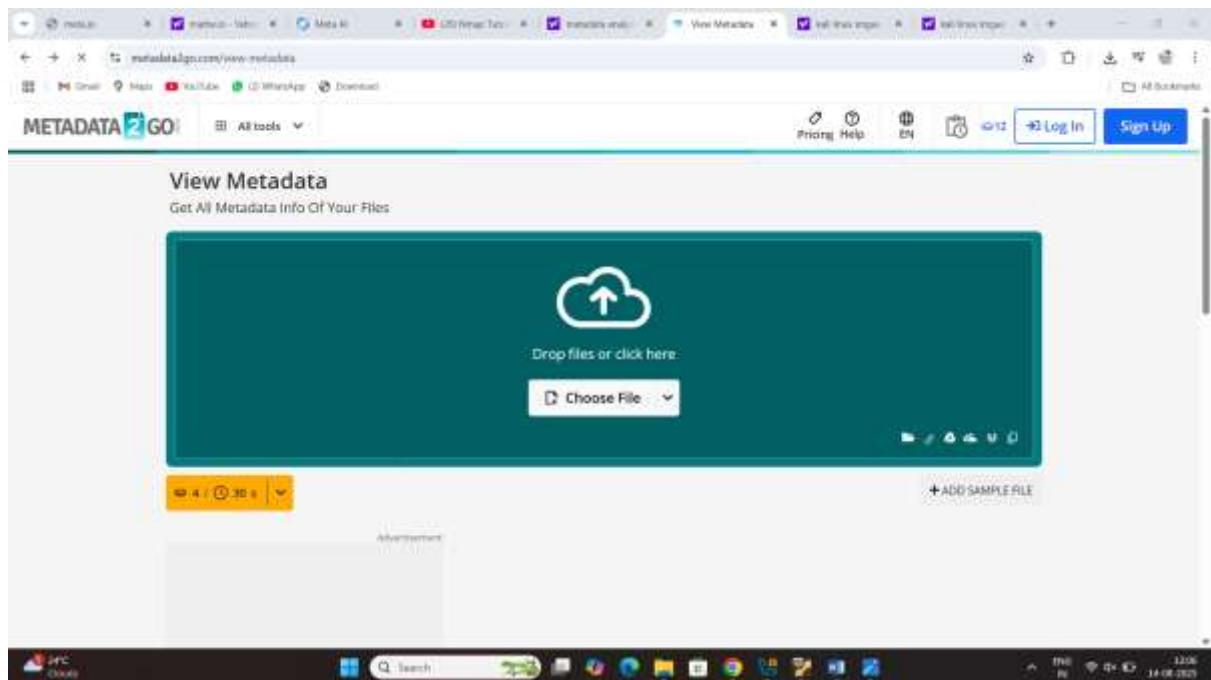
Step2 open the image

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

File List

banner-2021.3-relayage.jpg

Save this data as: PDF CSV TXT JSON HTML

checksum	c2fb2e0924fe0d21d8366e50cf5d121
file_name	banner-2021.3-relayage.jpg
file_size	126 kB
file_type	JPEG
file_type_extension	.jpg
mime_type	image/jpeg
jpeg_version	1.01
resolution_unit	None

Download

Export All Share Delete

✓ Done
Get a subscriber to update the issue, enjoy IM2G features and process your files faster.
Get Premium

Current Task: View Metadata

Start over Change Options

Continue with: banner-2021.3-relayage.jpg

METADATA2GO

All tools

File List

banner-2021.3-relayage.jpg

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: 0.054

category: image

Current Task: View Metadata

Start over Change Options

Continue with: banner-2021.3-relayage.jpg

Metadata Remover

Free Online Image Tool

IMG2GO.com

Convert and edit images online. Free, easy, and convenient.

EDIT PHOTOS RESIZE PHOTOS

