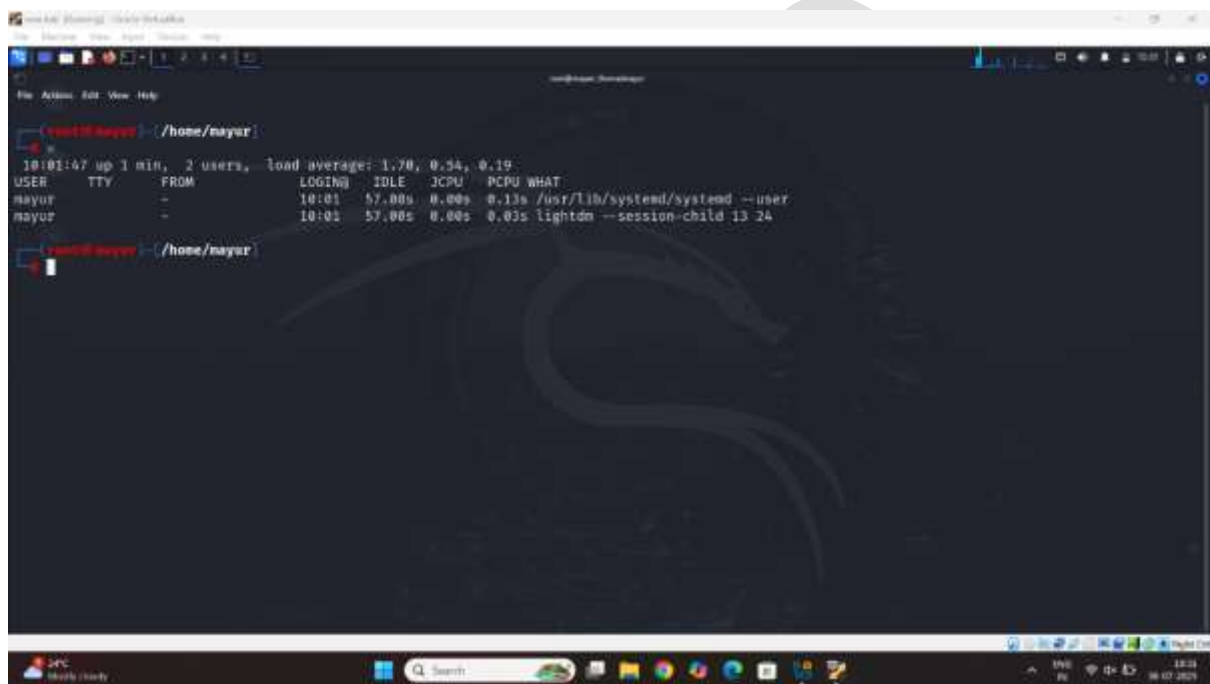


## Module 7 Linux and mac forensics

### Lab1 Acquire volatile data in Linux system

Step1 on the kali Linux machine

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



The screenshot shows a terminal window on a Kali Linux machine. The user is logged in as 'mayur' at the prompt. The command 'w' has been executed, displaying system status and user activity. The output includes the current time (10:01:47), system uptime (up 1 min), number of users (2), and load averages (1.70, 0.34, 0.19). A table follows, listing users, their TTYs, login times, idle times, JCPU, PCPU, and the command they are running. Two users, 'mayur', are shown, both running 'lightdm --session-child 13 24'.

```
w
10:01:47 up 1 min, 2 users, load average: 1.70, 0.34, 0.19
USER      TTY      FROM              LOGIN@   IDLE   JCPU   PCPU   WHAT
mayur     -        -                 10:01    57.00s 0.00s  0.13s  /usr/lib/systemd/systemd --user
mayur     -        -                 10:01    57.00s 0.00s  0.03s  lightdm --session-child 13 24
```

Step2 netstat/this command show network statitics

```

root@kali:~# ss -ttns
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 0.0.0.0:bootpc          0.0.0.0:bootpc          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    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    8803      /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

```

```

root@kali:~# ss -ttns
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    8803      /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    8913      /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    9188
unix  3      [ ]       STREAM     CONNECTED    7716      /run/systemd/journal/stdout
unix  3      [ ]       STREAM     CONNECTED    7872

```

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

```

root@kali:~# 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
qtr                 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_intel8*0         49152 1
snd_ac97_codec       196800 1 snd_intel8*0
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_intel8*0,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_intel8*0,snd_timer,snd_ac97_codec,snd_pcm
soundcore            16384 1 snd
vboxguest            53248 6 vboxsf

```

```

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              489600 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             311776 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          368448 0
crypto_sind          16384 1 aesni_intel
cryptd               28672 2 crypto_sind,ghash_clmulni_intel

```

## Step4 lsmod /this command are show list of module

```

root@kali:~# 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                  48960  2
qrtr                   57344  4
vboxsf                 49152  0
sunrpc                 880640  1
hifmat_misc            28672  1
intel_rapl_msr         20480  0
intel_rapl_common      36864  1 intel_rapl_msr
intel_uncore_frequency_common 16384  0
snd_intel8*0            49152  1
snd_ac97_codec         190800  1 snd_intel8*0
intel_pmc_core          114688  0
intel_vsec             20480  1 intel_pmc_core
ac97_bus               12288  1 snd_ac97_codec
pwt_telemetry          16384  1 intel_pmc_core
snd_pcm                192512  2 snd_intel8*0,snd_ac97_codec
pwt_class              12288  1 pwt_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_intel8*0,snd_timer,snd_ac97_codec,snd_pcm
soundcore              16384  1 snd
vboxguest              53248  6 vboxsf

root@kali:~# lsmod
Module                  Size  Used by
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                 489600  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                311776  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                   177024  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_sind             16384  1 aesni_intel
cryptd                  28672  2 crypto_sind,ghash_clmulni_intel

```

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

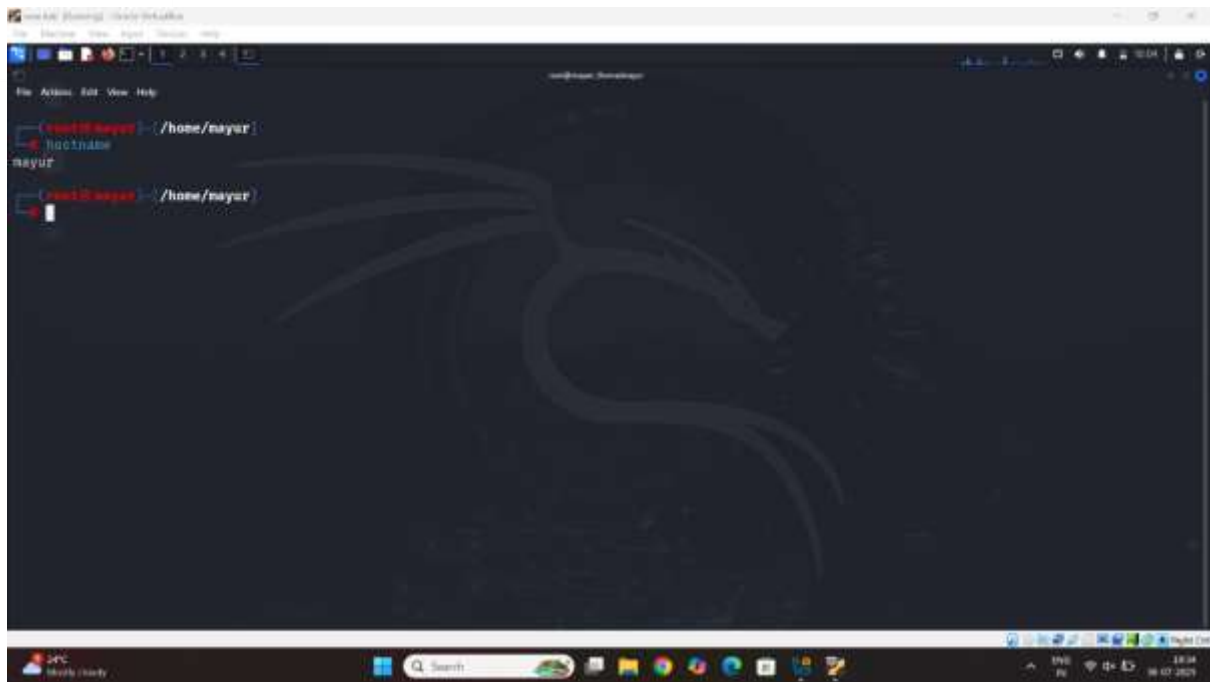
```

root@kali: ~# ps aux
USER          PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.0  22460 14212 ?        Ss   10:00   0:01 /sbin/init splash
root           2  0.0  0.0      0   0 ?        Ss   10:00   0:00 [kthreadd]
root           3  0.0  0.0      0   0 ?        Ss   10:00   0:00 [pool_workqueue_release]
root           4  0.0  0.0      0   0 ?        I<   10:00   0:00 [kworker/R-rcu_g]
root           5  0.0  0.0      0   0 ?        I<   10:00   0:00 [kworker/R-rcu_p]
root           6  0.0  0.0      0   0 ?        I<   10:00   0:00 [kworker/R-slab_]
root           7  0.0  0.0      0   0 ?        I<   10:00   0:00 [kworker/R-netns]
root           8  0.0  0.0      0   0 ?        I   10:00   0:00 [kworker/R:0-ata_sff]
root           9  0.2  0.0      0   0 ?        I   10:00   0:00 [kworker/R:1-ata_sff]
root          10  0.0  0.0      0   0 ?        I<   10:00   0:00 [kworker/R:0H-khlockd]
root          11  0.0  0.0      0   0 ?        I   10:00   0:00 [kworker/u2:0-events_unbound]
root          12  0.0  0.0      0   0 ?        I<   10:00   0:00 [kworker/R-mm_p]
root          13  0.0  0.0      0   0 ?        I   10:00   0:00 [rcu_tasks_kthread]
root          14  0.0  0.0      0   0 ?        I   10:00   0:00 [rcu_tasks_rude_kthread]
root          15  0.0  0.0      0   0 ?        I   10:00   0:00 [rcu_tasks_trace_kthread]
root          16  0.1  0.0      0   0 ?        S   10:00   0:00 [ksoftirqd/0]
root          17  0.1  0.0      0   0 ?        I   10:00   0:00 [rcu_preempt]
root          18  0.0  0.0      0   0 ?        S   10:00   0:00 [migration/0]
root          19  0.0  0.0      0   0 ?        S   10:00   0:00 [idle_inject/0]
root          20  0.0  0.0      0   0 ?        S   10:00   0:00 [cpuhp/0]
root          22  0.0  0.0      0   0 ?        S   10:00   0:00 [kdevtmpfs]
root          23  0.0  0.0      0   0 ?        I<   10:00   0:00 [kworker/R-inet_]
root          24  1.0  0.0      0   0 ?        I   10:00   0:02 [kworker/u2:1-events_unbound]
root          25  0.0  0.0      0   0 ?        S   10:00   0:00 [kauditd]
root          26  0.0  0.0      0   0 ?        S   10:00   0:00 [khungtaskd]
root          27  0.0  0.0      0   0 ?        S   10:00   0:00 [oom_reaper]

root@kali: ~# ps aux
USER          PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root          191  0.0  0.0      0   0 ?        I   10:00   0:00 [kworker/R:4-events]
root          192  0.3  0.0      0   0 ?        I<   10:00   0:00 [kworker/R:2H-khlockd]
root          193  0.0  0.0      0   0 ?        S   10:00   0:00 [irq/18-vmmgfx]
root          194  0.0  0.0      0   0 ?        I<   10:00   0:00 [kworker/R-ttn]
root          238  0.0  0.0      0   0 ?        S   10:00   0:00 [jbd2/sda1-8]
root          239  0.0  0.0      0   0 ?        I<   10:00   0:00 [kworker/R-ext4-]
root          294  0.1  0.8 41580 17928 ?        Ss   10:00   0:00 /usr/lib/systemd/systemd-journald
root          330  0.1  0.1 29712 8000 ?        Ss   10:00   0:00 /usr/lib/systemd/systemd-udevd
root          343  0.0  0.0      0   0 ?        S   10:00   0:00 [psimon]
root          440  0.1  0.3  8276 6460 ?        Ss   10:00   0:00 /usr/sbin/haveged --foreground --verbose=1
root          450  0.0  0.3 30584 6996 ?        Ss   10:00   0:00 /usr/libexec/accounts-daemon
root          459  0.1  0.2  8176 5504 ?        Ss   10:00   0:00 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --system
d-activation --syslog-only
root          463  0.1  0.4 36178 9640 ?        Ss   10:00   0:00 /usr/lib/polkit-1/polkitd --no-debug
root          464  0.0  0.0      0   0 ?        I<   10:00   0:00 [kworker/R-rpcio]
root          466  0.0  0.4 17584 8704 ?        Ss   10:00   0:00 /usr/lib/systemd/systemd-logind
root          467  0.0  0.0      0   0 ?        I<   10:00   0:00 [kworker/R-xprt]
root          473  0.0  0.1  7048 2560 ?        Ss   10:00   0:00 /usr/sbin/cron -f
root          542  0.1  0.9 33370 19912 ?        Ss   10:00   0:00 /usr/sbin/NetworkManager --no-daemon
root          559  0.0  0.5 30972 12076 ?        Ss   10:00   0:00 /usr/sbin/ModemManager
root          586  0.0  0.1 29080 3072 ?        Ss   10:00   0:00 /usr/sbin/VBoxService
root          644  0.0  0.3 38057 7272 ?        Ss   10:00   0:00 /usr/sbin/lightdm
root          660  0.0  0.1  5900 2176 tty1    Ss+  10:00   0:00 /sbin/agetty -o -p -- \u --noclear - linux
root          661  3.5  5.9 40114 120320 tty?    SsL+ 10:00   0:07 /usr/lib/xorg/Xorg :0 -seat seat0 -auth /var/run/lightdm/root/:0 -nolisten tcp vt7 -novtswitch
root          685  0.0  0.0      0   0 ?        S   10:00   0:00 [psimon]
root          711  0.0  0.1 20244 2688 ?        Ss   10:00   0:00 /usr/libexec/rthitd-daemon
root          779  0.0  0.4 23473 8152 ?        Ss   10:01   0:00 lightdm --session-child 13 24
mayur        787  0.0  0.3 21056 11904 ?        Ss   10:01   0:00 /usr/lib/systemd/systemd --user
mayur        788  0.0  0.1 20360 3516 ?        S   10:01   0:00 (sd-pam)

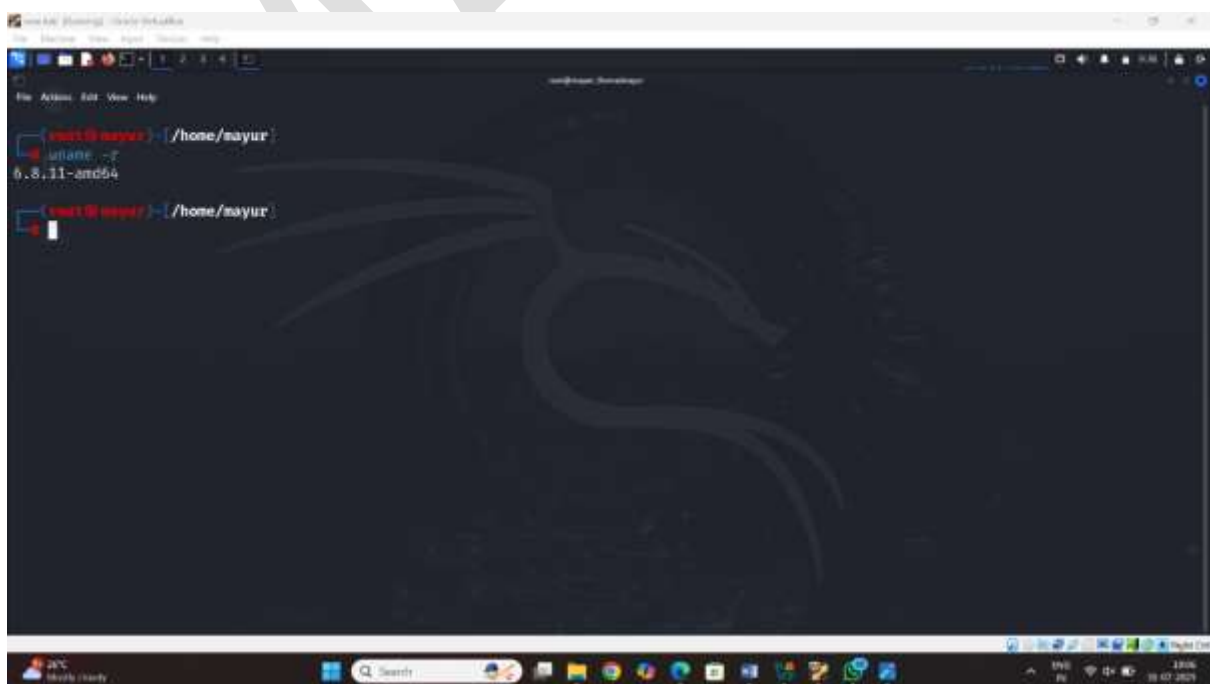
```

Step6 hostname/this command are use show  
hostname



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

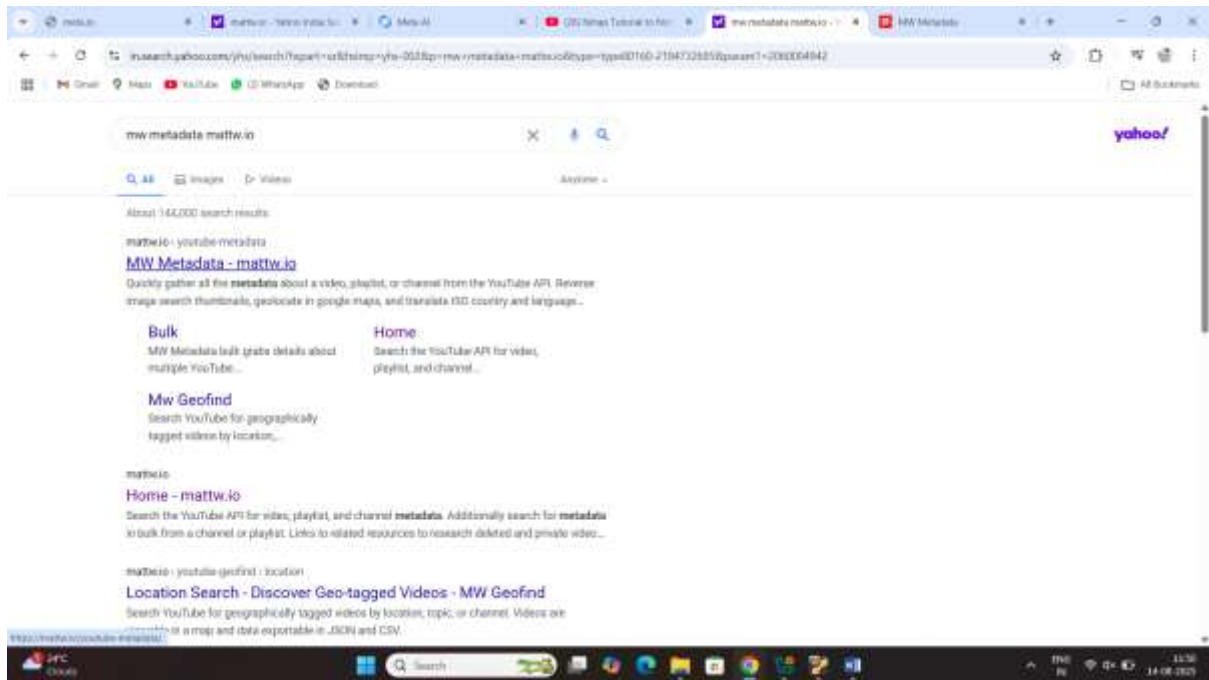
Step1 uname -r /this command are use system version  
kernel



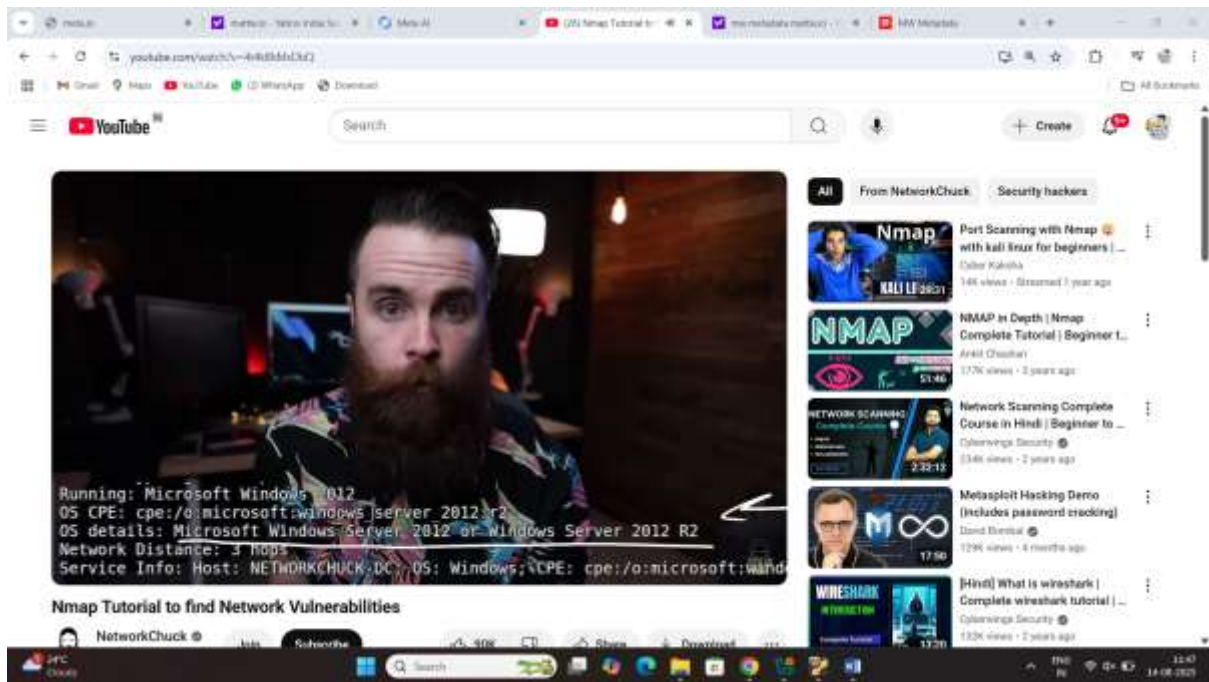


## Lab3 how to image investigation and vedio meta data analysis of image

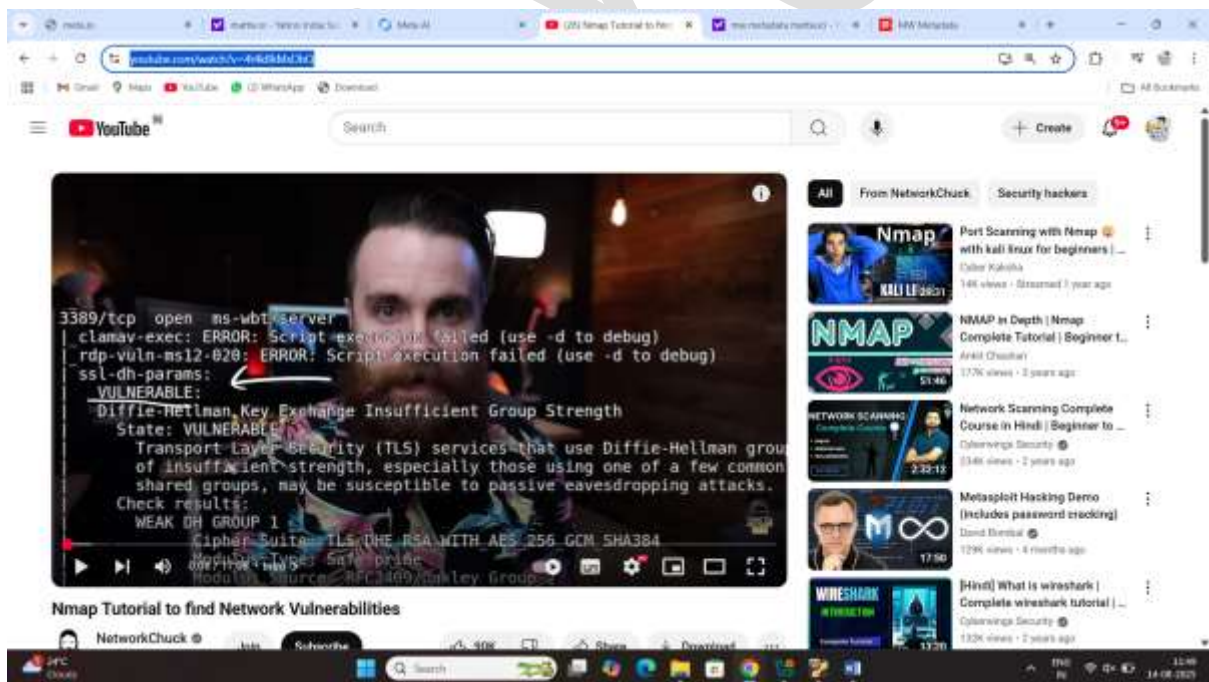
# There was website is mata.io



## Step2 Select the youtube vedio

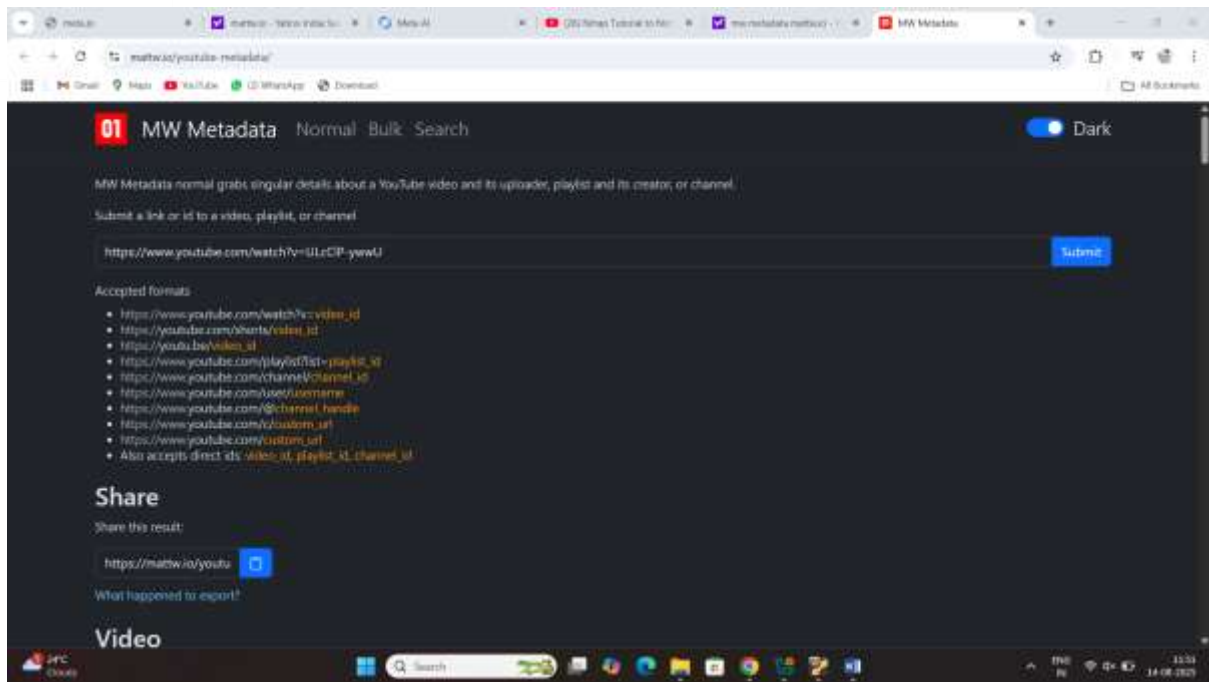


Step3 cope the url of vedio



Step4 open the website and paste the vedio url





Step5 click on the submit button  
result:

The screenshot shows a web browser window with multiple tabs. The active tab is 'mattw.in/youtu...', displaying the YouTube metadata page for a video titled 'Nmap Tutorial to find Network Vulnerabilities'.

**Video Information:**

- Video Title:** Nmap Tutorial to find Network Vulnerabilities
- Published by:** NetworkChuck
- Published on:** 19 Jul 2020 21:47:37 GMT (5 years ago) (convert)
- Tags:** ethical hacking, hacker, hacking tutorial, how to be a hacker, how to become a hacker, how to hack, information technology, kali linux, team hacking, linux tutorial, linux exam, linux aio-b54, raspberry pi, raspberry pi 3, rasp 32, how to, nmap basics, nmap full tutorial, nmap complete tutorial, nmap, network hacking, hacking network
- Category:** id is 20 which means Science & Technology
- Default language:** EN which means English
- Audio language:** EN-US which means English / United States of America (the)
- The video id is:** 49-4b8bMvD8c

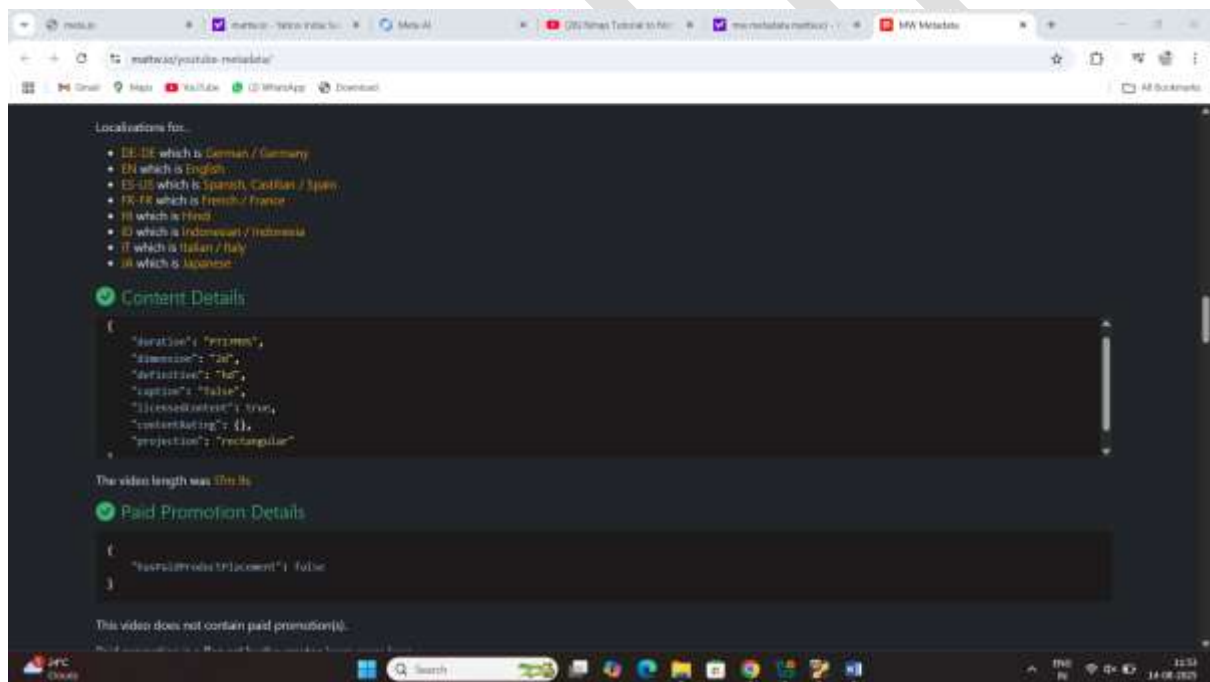
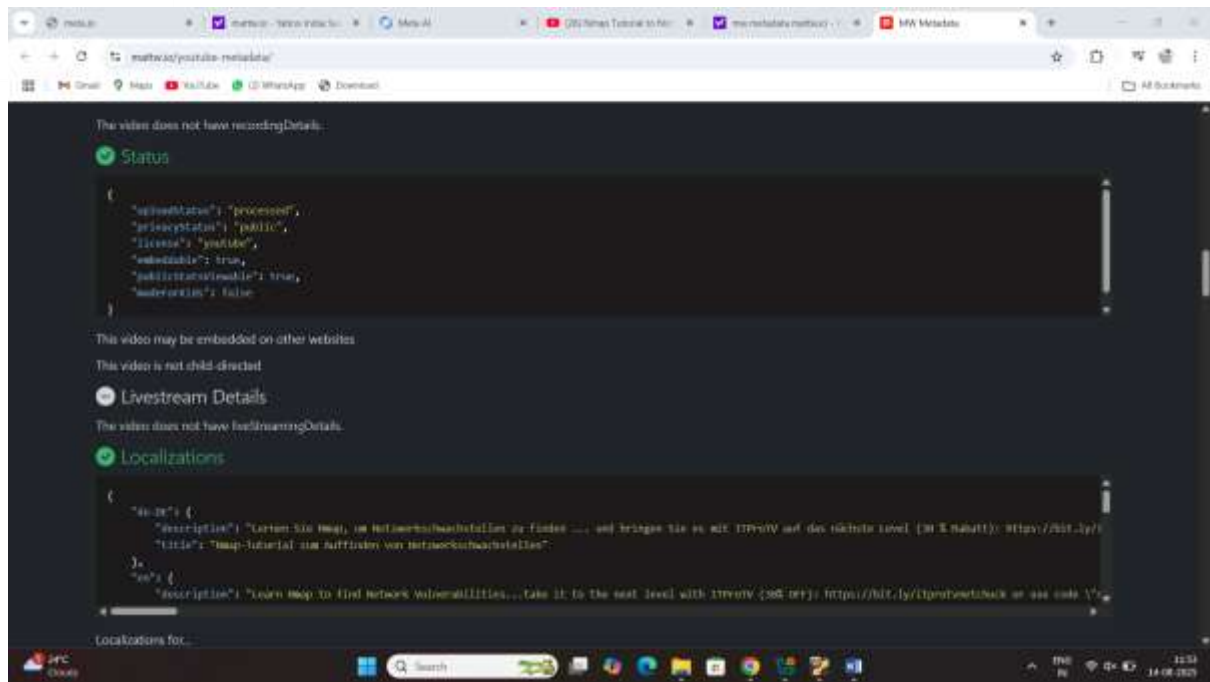
**Statistics:**

- ViewCount:** 1307223
- LikeCount:** 16016
- FavoritedCount:** 78
- CommentCount:** 2835

**Geolocation:**

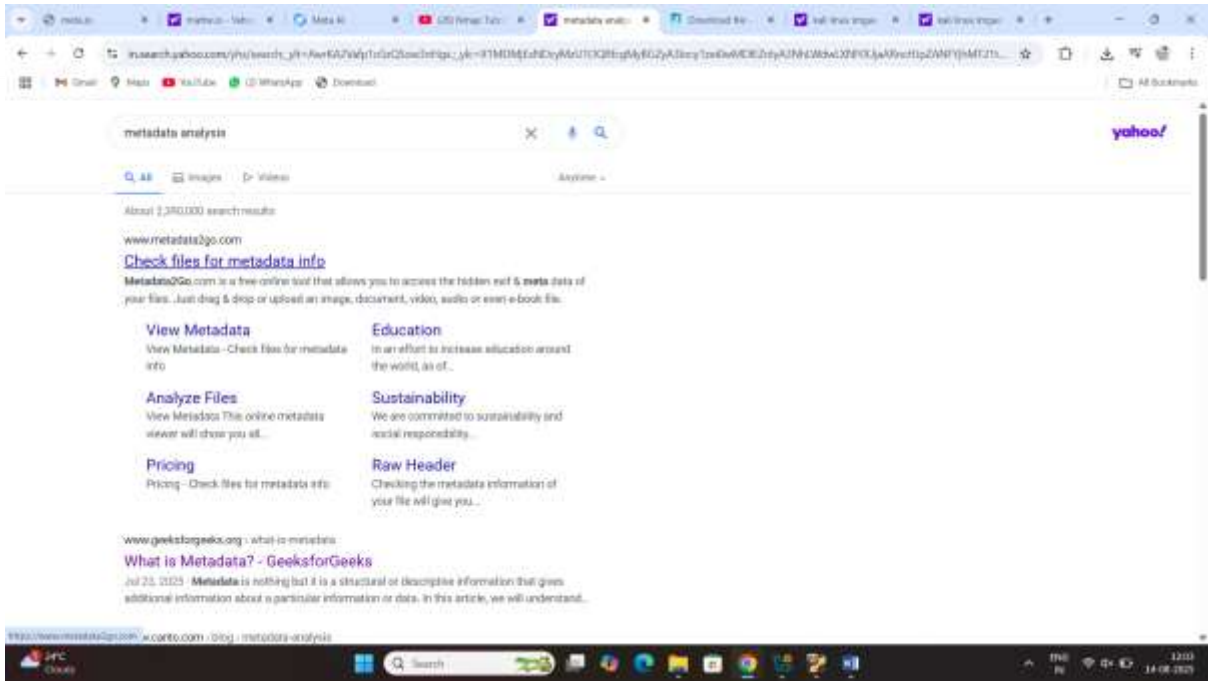
The video is no longer provides the [dislikeCount](#) since 2021-12-13 (see more here).

Want dislikes back? Check out the [return youtube-dislike](#) project!



**Second method image investigation**

**There was website meta data analysis**



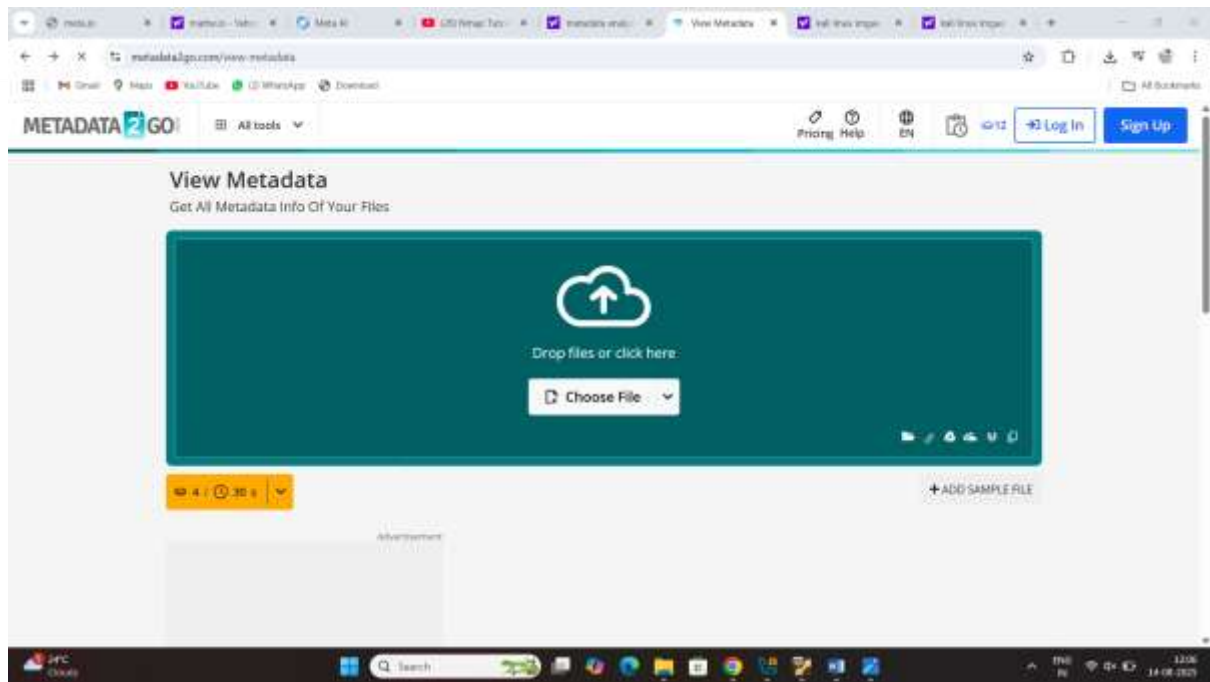
## Step2 open the image

### Step3 select the image of investigation



I am select this kali linux image

Step4 open the website click on option choice



**Result:**



The screenshot displays the Metadata2Go web interface. The browser address bar shows the URL: `metadata2go.com/result?c=76f6baed-d251-4f08-b08e-04a9b66c93d8`. The page title is "METADATA2GO". The main content area shows the file "Banner-2021.3-release.jpg" with its metadata.

**File Metadata:**

checksum	c278e2e2924f6d8a23db36e60ef5dd27
file_name	Banner-2021.3-release.jpg
file_size	126 KB
file_type	JPEG
file_type_extension	.jpg
mime_type	image/jpeg
jif_version	1.01
resolution_unit	None

**Image Metadata:**

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

The right sidebar contains a "Download" button, an "Export As" dropdown, and a "Delete" button. Below these is a "Done" message: "Get a subscription to bypass the status, enjoy PRO features, and process your files faster." with a "Get Premium" button. The "Current Task" section shows "View Metadata" and "Sort over" buttons. The "Continue with" section shows "Banner-2021.3-release.jpg" and a "Metadata Remover" button. An advertisement for "Free Online Image Tool IMG2GO" is visible at the bottom right.

