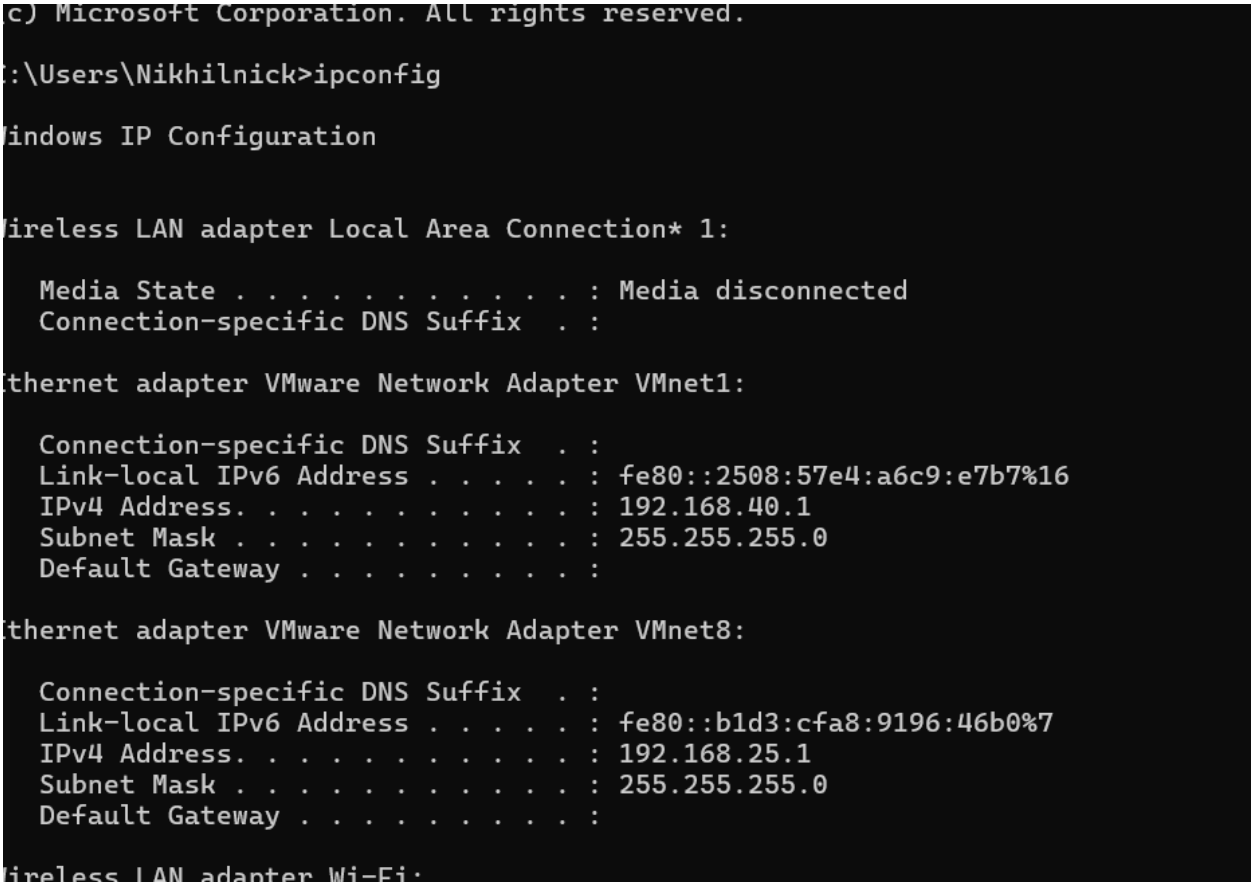
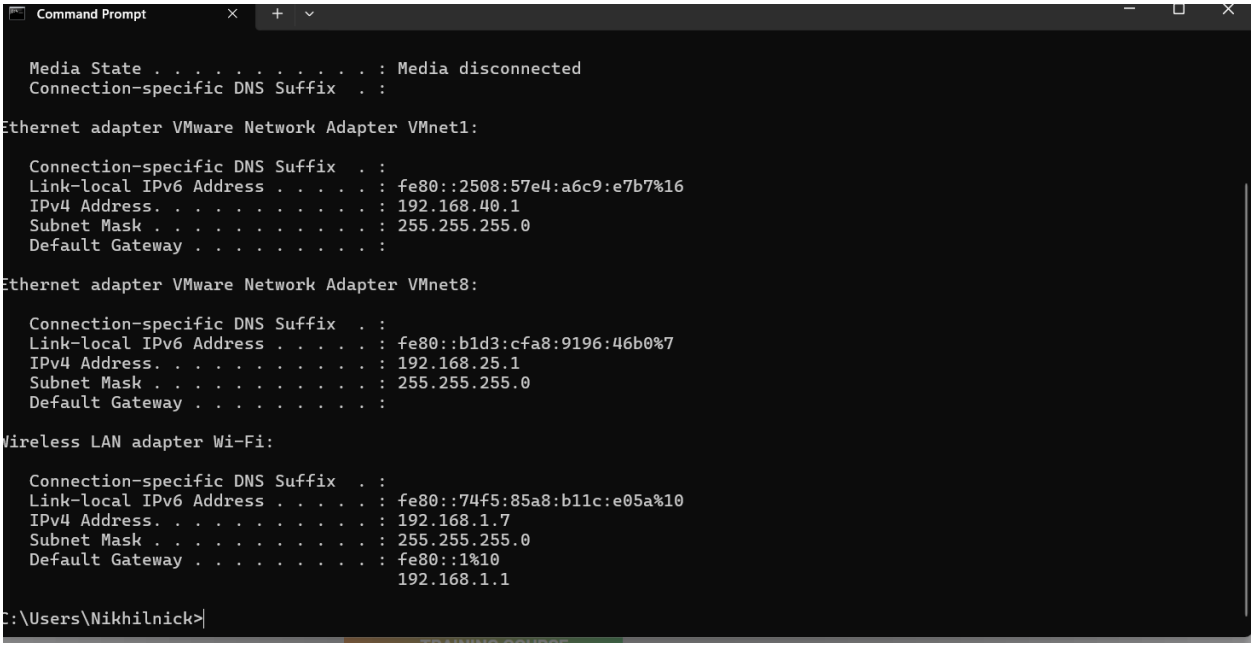
ASSIGNMENT-3

INFORMATION GATHERING ON WEBSITES USING KALI LINUX

In this assignment we need to gather information on websites. Here are few steps and task we have performed to reach goal.

Find the ip address of windows machine. For finding ip address go to command prompt type ipconfig and we can see the ip address.

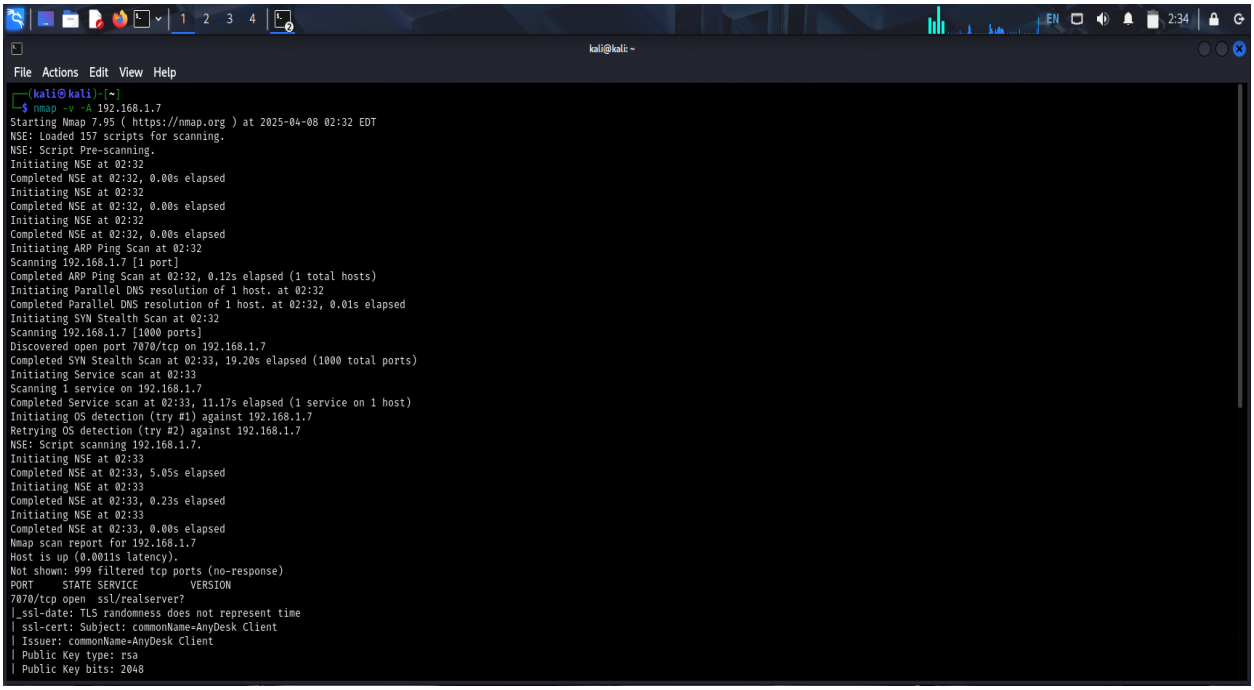


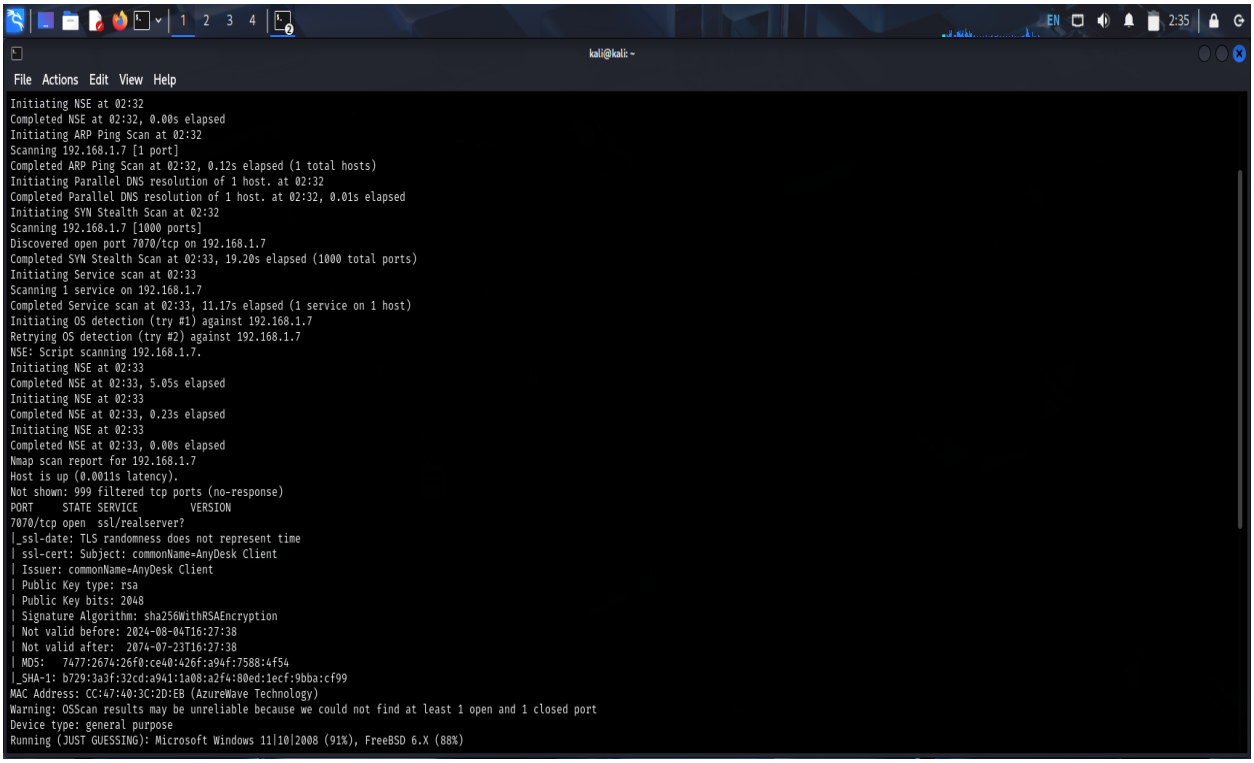


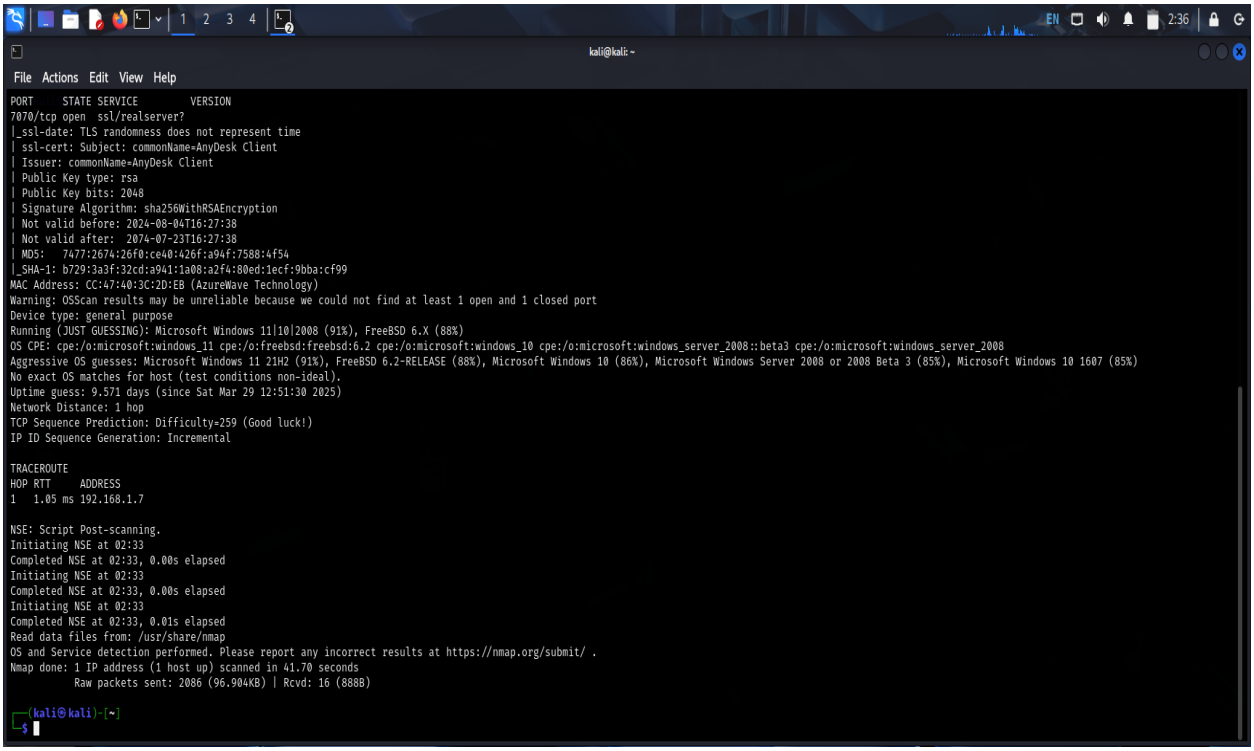
After getting the ip address use the command nmap for gathering information such as os details, ports, service details

Sudo nmap -v -A 192.168.1.7

Here -A gives all the os details, ports, service details .

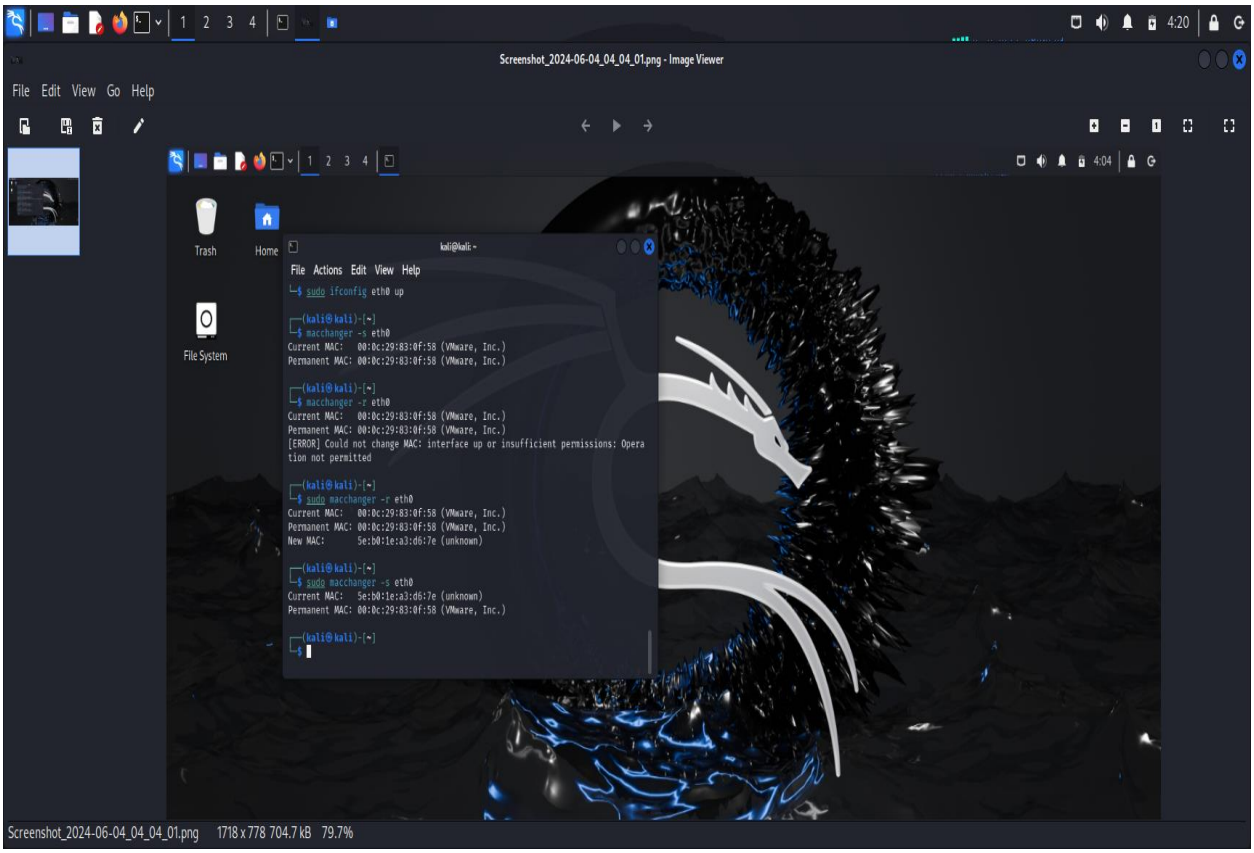



kali@kali: ~
File Actions Edit View Help
Initiating NSE at 02:32
Completed NSE at 02:32, 0.00s elapsed
Initiating ARP Ping Scan at 02:32
Scanning 192.168.1.7 [1 port]
Completed ARP Ping Scan at 02:32, 0.12s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:32
Completed Parallel DNS resolution of 1 host. at 02:32, 0.01s elapsed
Initiating SYN Stealth Scan at 02:32
Scanning 192.168.1.7 [1000 ports]
Discovered open port 7070/tcp on 192.168.1.7
Completed SYN Stealth Scan at 02:33, 19.20s elapsed (1000 total ports)
Initiating Service scan at 02:33
Scanning 1 service on 192.168.1.7
Completed Service scan at 02:33, 11.17s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 192.168.1.7
Retrying OS detection (try #2) against 192.168.1.7
NSE: Script scanning 192.168.1.7.
Initiating NSE at 02:33
Completed NSE at 02:33, 5.05s elapsed
Initiating NSE at 02:33
Completed NSE at 02:33, 0.23s elapsed
Initiating NSE at 02:33
Completed NSE at 02:33, 0.00s elapsed
Nmap scan report for 192.168.1.7
Host is up (0.0011s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
7070/tcp open ssl/realserver?
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=AnyDesk Client
| Issuer: commonName=AnyDesk Client
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-08-04T16:27:38
| Not valid after: 2074-07-23T16:27:38
| MD5: 7477:2674:26f0:ce40:426f:a94f:7588:4f54
|_SHA-1: b729:3a3f:32cd:a941:1a08:a2f4:80ed:1ecf:9bba:cf99
MAC Address: CC:47:40:3C:2D:EB (AzureWave Technology)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 11|10|2008 (91%), FreeBSD 6.X (88%)


kali@kali: ~
File Actions Edit View Help
PORT STATE SERVICE VERSION
7070/tcp open ssl/realserver?
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=AnyDesk Client
| Issuer: commonName=AnyDesk Client
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-08-04T16:27:38
| Not valid after: 2074-07-23T16:27:38
| MD5: 7477:2674:26f0:ce40:426f:a94f:7588:4f54
|_SHA-1: b729:3a3f:32cd:a941:1a08:a2f4:80ed:1ecf:9bba:cf99
MAC Address: CC:47:40:3C:2D:EB (AzureWave Technology)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 11|10|2008 (91%), FreeBSD 6.X (88%)
OS CPE: cpe:/o:microsoft:windows_11 cpe:/o:freebsd:freebsd:6.2 cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_server_2008::beta3 cpe:/o:microsoft:windows_server_2008
Aggressive OS guesses: Microsoft Windows 11 21H2 (91%), FreeBSD 6.2-RELEASE (88%), Microsoft Windows 10 (86%), Microsoft Windows Server 2008 or 2008 Beta 3 (85%), Microsoft Windows 10 1607 (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 9.571 days (since Sat Mar 29 12:51:30 2025)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: Incremental
TRACEROUTE
HOP RTT ADDRESS
1 1.05 ms 192.168.1.7
NSE: Script Post-scanning.
Initiating NSE at 02:33
Completed NSE at 02:33, 0.00s elapsed
Initiating NSE at 02:33
Completed NSE at 02:33, 0.00s elapsed
Initiating NSE at 02:33
Completed NSE at 02:33, 0.01s elapsed
Read data files from: /usr/share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 41.70 seconds
Raw packets sent: 2086 (96.904KB) | Rcvd: 16 (888B)
(kali㉿kali)-[~]
$

TASK 2

In this task we need to change the mac address to any random address ,for that we can use the command macchanger -r eth0 for random mac address.



TASK 3

We need to enumerate all the ports in window machine for this go to command prompt type netsat -an it will display all the information.

```
C:\Users\Nikhilnick>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:902            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7070           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49671          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49672          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49673          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49674          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49675          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:24830        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:36393        127.0.0.1:65001        ESTABLISHED
  TCP    127.0.0.1:36394        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:40172        127.0.0.1:40173        ESTABLISHED
  TCP    127.0.0.1:40173        127.0.0.1:40172        ESTABLISHED
  TCP    127.0.0.1:65001        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:65001        127.0.0.1:36393        ESTABLISHED
```

```
TCP    192.168.1.7:139        0.0.0.0:0              LISTENING
TCP    192.168.1.7:2325       104.18.63.125:443      CLOSE_WAIT
TCP    192.168.1.7:2346       104.18.63.125:443      CLOSE_WAIT
TCP    192.168.1.7:2496       104.18.32.47:443       ESTABLISHED
TCP    192.168.1.7:2498       172.64.155.209:443     ESTABLISHED
TCP    192.168.1.7:2504       51.8.64.151:443        CLOSE_WAIT
TCP    192.168.1.7:2505       51.8.64.151:443        CLOSE_WAIT
TCP    192.168.1.7:36551      23.58.31.18:80         CLOSE_WAIT
TCP    192.168.1.7:36951      148.113.16.13:443      ESTABLISHED
TCP    192.168.1.7:36985      74.125.24.188:5228     ESTABLISHED
TCP    192.168.1.7:49469      4.213.25.240:443       ESTABLISHED
TCP    192.168.25.1:139       0.0.0.0:0              LISTENING
TCP    192.168.40.1:139       0.0.0.0:0              LISTENING
TCP    [::]:135               [::]:0                 LISTENING
TCP    [::]:445               [::]:0                 LISTENING
TCP    [::]:7070              [::]:0                 LISTENING
TCP    [::]:49664             [::]:0                 LISTENING
TCP    [::]:49665             [::]:0                 LISTENING
TCP    [::]:49666             [::]:0                 LISTENING
TCP    [::]:49667             [::]:0                 LISTENING
TCP    [::]:49668             [::]:0                 LISTENING
TCP    [::]:49675             [::]:0                 LISTENING
TCP    [::1]:37013            [::1]:37014            ESTABLISHED
TCP    [::1]:37014            [::1]:37013            ESTABLISHED
UDP    0.0.0.0:123            *:*
UDP    0.0.0.0:5050           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5353           *:*
```

```
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5355           *:*
UDP    0.0.0.0:50001          *:*
UDP    0.0.0.0:51479          *:*
UDP    0.0.0.0:52470          *:*
UDP    0.0.0.0:53568          *:*
UDP    0.0.0.0:53915          *:*
UDP    0.0.0.0:55972          184.26.54.155:443
UDP    0.0.0.0:62505          *:*
UDP    0.0.0.0:63899          8.8.8.8:443
UDP    127.0.0.1:1900         *:*
UDP    127.0.0.1:10110        *:*
UDP    127.0.0.1:49223        *:*
UDP    127.0.0.1:50701        *:*
UDP    127.0.0.1:54241        127.0.0.1:54241
UDP    192.168.1.7:137        *:*
UDP    192.168.1.7:138        *:*
UDP    192.168.1.7:1900       *:*
UDP    192.168.1.7:5353       *:*
UDP    192.168.1.7:50700      *:*
UDP    192.168.25.1:137       *:*
```

```
UDP    192.168.40.1:50698     *:*
UDP    [::]:123               *:*
UDP    [::]:5353              *:*
UDP    [::]:5353              *:*
UDP    [::]:5353              *:*
UDP    [::]:5353              *:*
UDP    [::]:5353              *:*
UDP    [::]:5353              *:*
UDP    [::]:5353              *:*
UDP    [::]:5355              *:*
UDP    [::]:51479             *:*
UDP    [::]:52470             *:*
UDP    [::]:53568             *:*
UDP    [::]:62506             *:*
UDP    [::1]:1900             *:*
UDP    [::1]:5353             *:*
UDP    [::1]:50697            *:*
UDP    [fe80::2508:57e4:a6c9:e7b7%16]:1900  *:*
UDP    [fe80::2508:57e4:a6c9:e7b7%16]:50694  *:*
UDP    [fe80::74f5:85a8:b11c:e05a%10]:1900  *:*
UDP    [fe80::74f5:85a8:b11c:e05a%10]:50696  *:*
UDP    [fe80::b1d3:cfa8:9196:46b0%7]:1900  *:*
UDP    [fe80::b1d3:cfa8:9196:46b0%7]:50695  *:*
```

To find the routing table type route print in command prompt to get the tables.

```
C:\Users\Nikhilnick>route print
===========================================================================
Interface List
 17...ce 47 40 3c 2d ab ......Microsoft Wi-Fi Direct Virtual Adapter
  4...ce 47 40 3c 2d bb ......Microsoft Wi-Fi Direct Virtual Adapter #2
 16...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
  7...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
 10...cc 47 40 3c 2d eb ......MediaTek Wi-Fi 6 MT7921 Wireless LAN Card
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1      192.168.1.7     35
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      192.168.1.0    255.255.255.0         On-link       192.168.1.7    291
      192.168.1.7  255.255.255.255         On-link       192.168.1.7    291
    192.168.1.255  255.255.255.255         On-link       192.168.1.7    291
     192.168.25.0    255.255.255.0         On-link      192.168.25.1    291
     192.168.25.1  255.255.255.255         On-link      192.168.25.1    291
   192.168.25.255  255.255.255.255         On-link      192.168.25.1    291
     192.168.40.0    255.255.255.0         On-link      192.168.40.1    291
     192.168.40.1  255.255.255.255         On-link      192.168.40.1    291
   192.168.40.255  255.255.255.255         On-link      192.168.40.1    291
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link       192.168.1.7    291
```

```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1      192.168.1.7     35
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      192.168.1.0    255.255.255.0         On-link       192.168.1.7    291
      192.168.1.7  255.255.255.255         On-link       192.168.1.7    291
    192.168.1.255  255.255.255.255         On-link       192.168.1.7    291
     192.168.25.0    255.255.255.0         On-link      192.168.25.1    291
     192.168.25.1  255.255.255.255         On-link      192.168.25.1    291
   192.168.25.255  255.255.255.255         On-link      192.168.25.1    291
     192.168.40.0    255.255.255.0         On-link      192.168.40.1    291
     192.168.40.1  255.255.255.255         On-link      192.168.40.1    291
   192.168.40.255  255.255.255.255         On-link      192.168.40.1    291
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link       192.168.1.7    291
        224.0.0.0        240.0.0.0         On-link      192.168.25.1    291
        224.0.0.0        240.0.0.0         On-link      192.168.40.1    291
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link       192.168.1.7    291
  255.255.255.255  255.255.255.255         On-link      192.168.25.1    291
  255.255.255.255  255.255.255.255         On-link      192.168.40.1    291
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
```

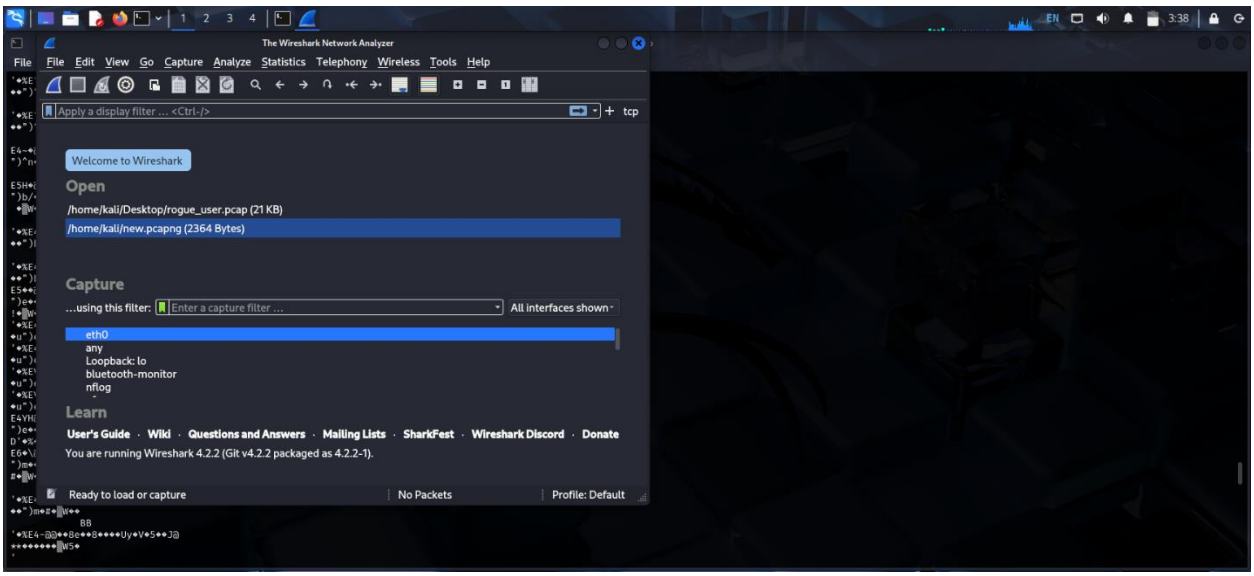
```
None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
 10    291 ::/0                     fe80::1
  1    331 ::1/128                  On-link
 10    291 fe80::/64                On-link
  7    291 fe80::/64                On-link
 16    291 fe80::/64                On-link
 16    291 fe80::2508:57e4:a6c9:e7b7/128
                                    On-link
 10    291 fe80::74f5:85a8:b11c:e05a/128
                                    On-link
  7    291 fe80::b1d3:cfa8:9196:46b0/128
                                    On-link
  1    331 ff00::/8                 On-link
 10    291 ff00::/8                 On-link
  7    291 ff00::/8                 On-link
 16    291 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

Task 4

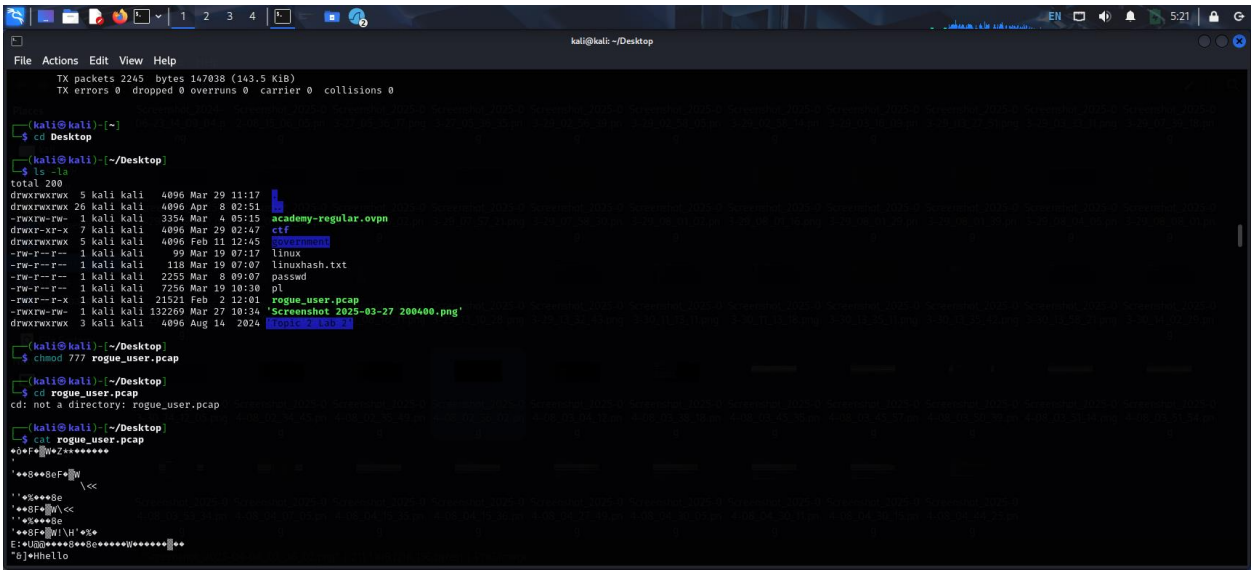
We need to have oracle virtualbox vmware .

Download oracle virtualbox vmware and go to settings click on network then change the network to bridge network which keeps windows and kali machine in same local network.

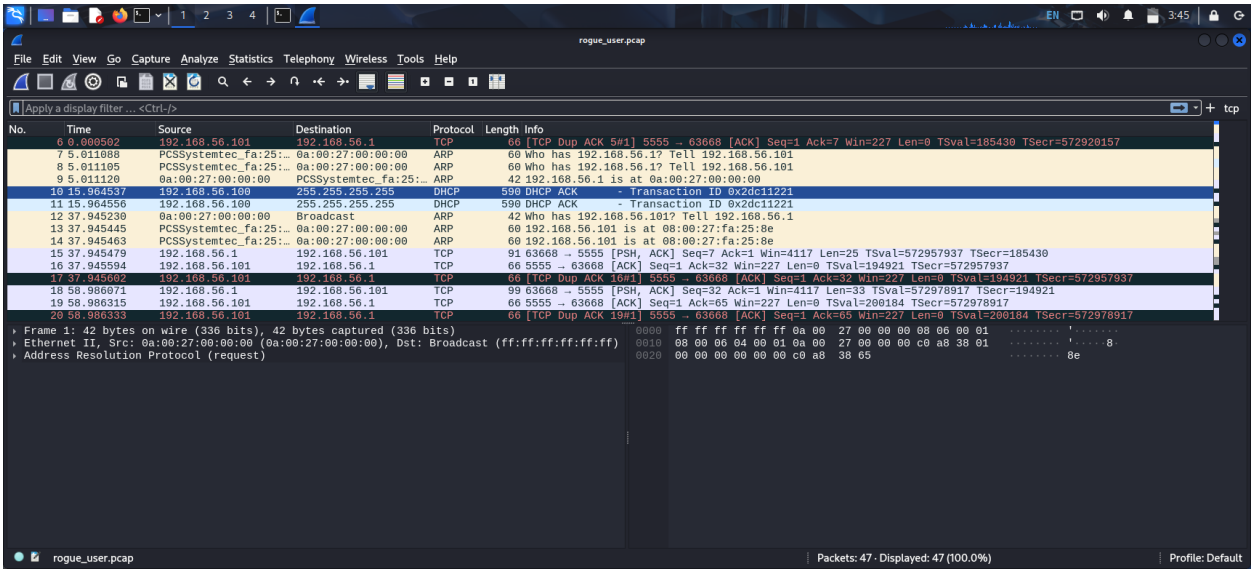
Next step is to type wireshark in kali linux and click on eth0

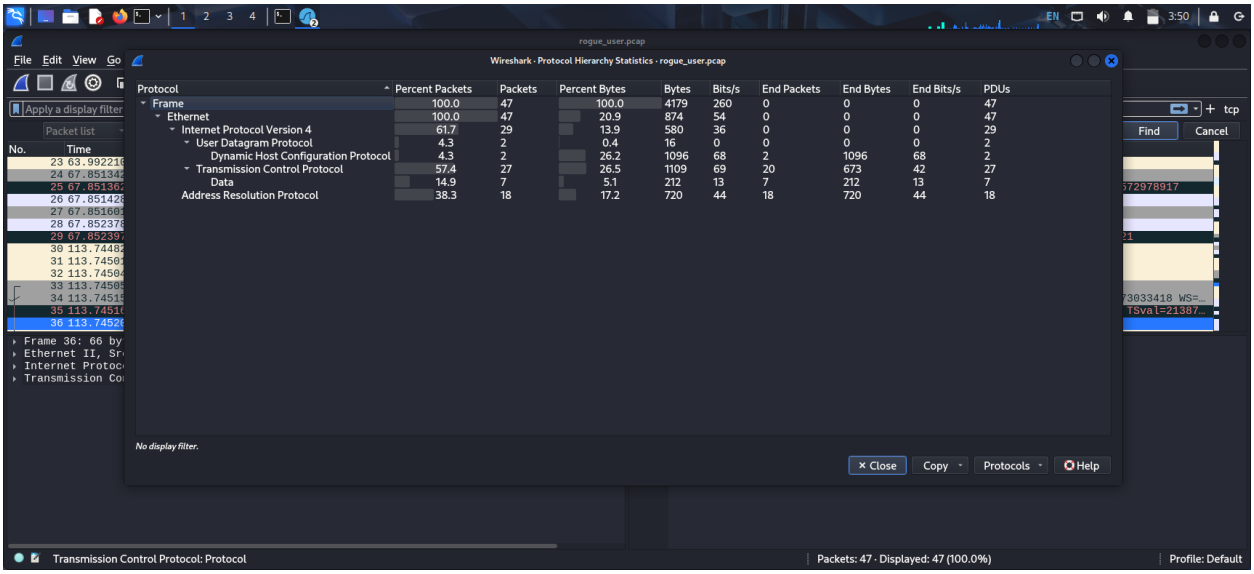


Now download the file rogue_user.pcap file to desktop and copy it to kali linux change the permissions to acess the files if needed.

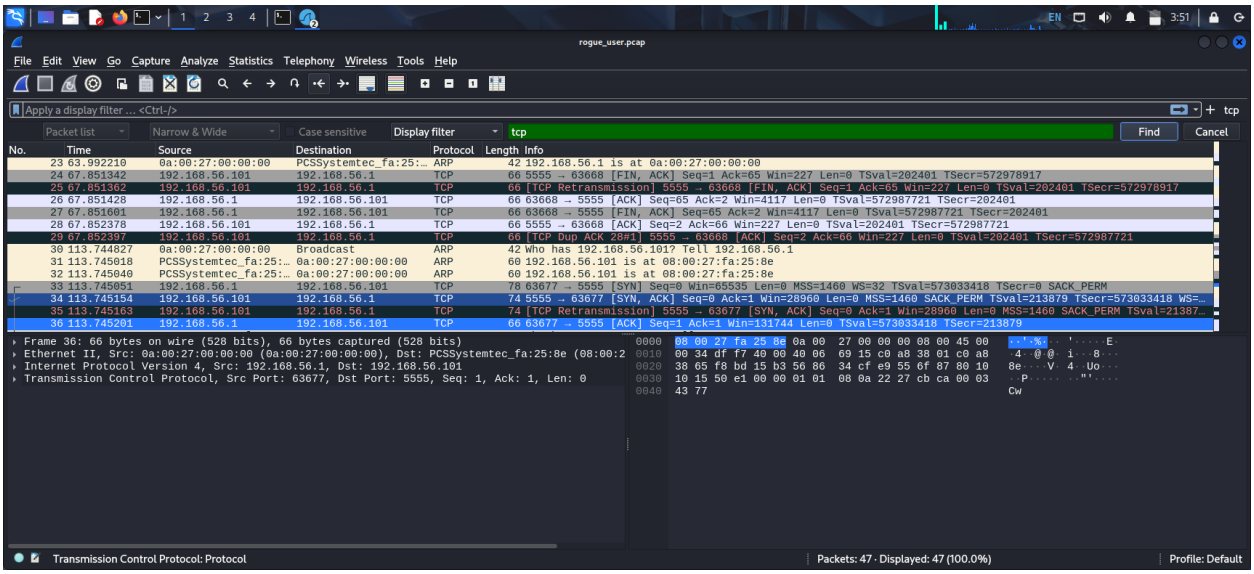


Open the file in wireshark and find the all the main protocols which are present like tcp, upd ,telnet etc.



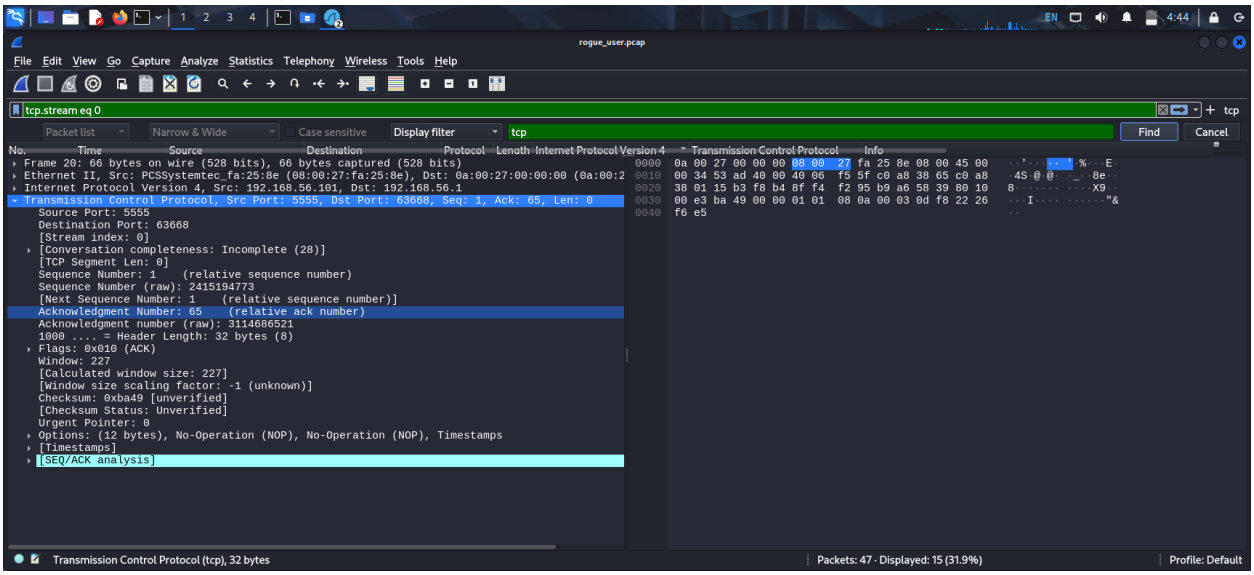


We can find tcp protocol to display column tap on any of the packets of tcp and you will find the option add to column click it.



We can details like segment, acknowledgment ,destination port ,source port etc details at the

bottom of the pane.



We have achieved all the information .