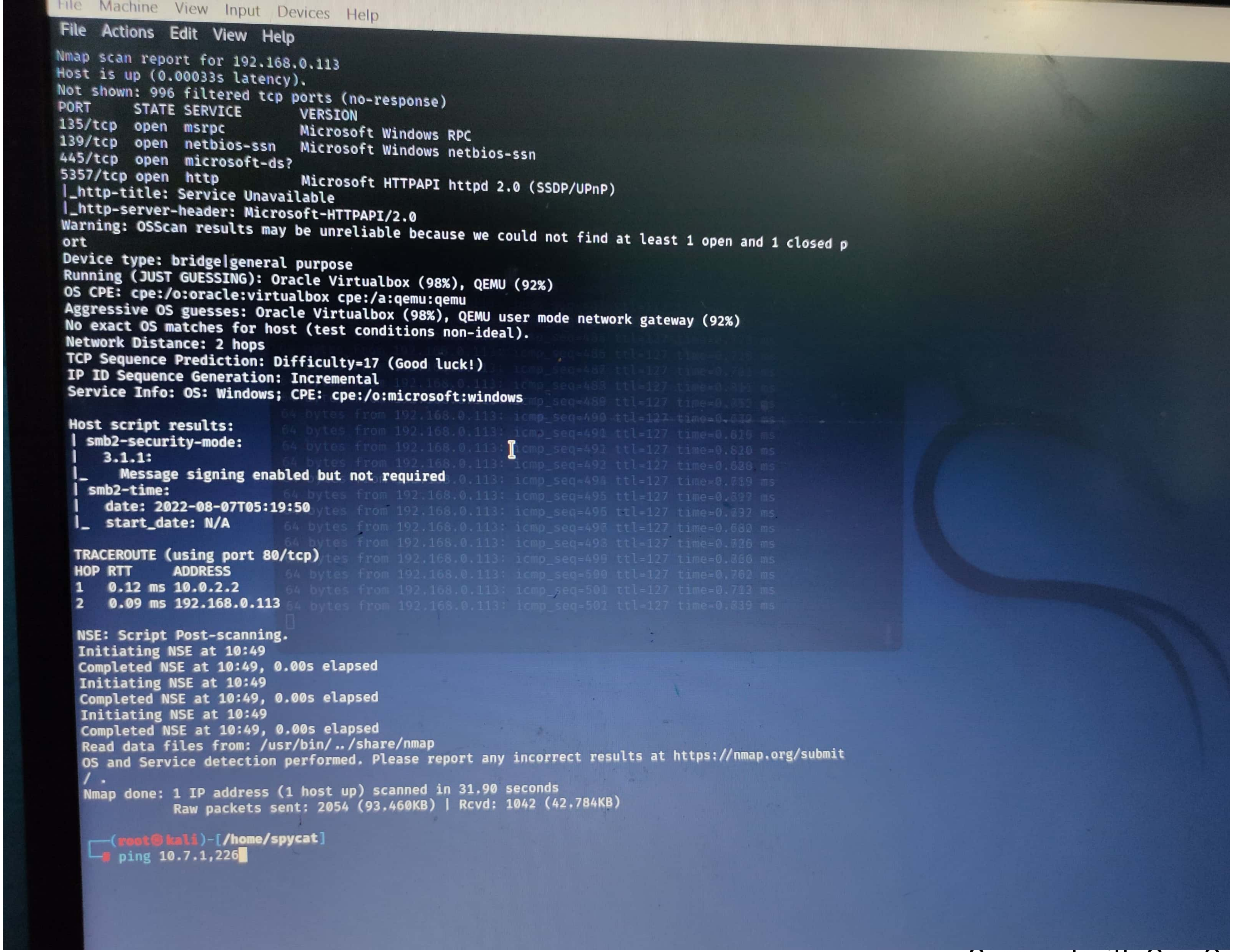
PROCEDURE FOR WIRESHARK AND NMAP TOOL

STEP 1:FIRST OPEN ROOT TERMINAL AND PERFORM TCP CONNECT (-sT) I.e, FULL OPEN SCAN BY USING NMAP .THAT IS ALL ABOUT 3 WAY HANDSHAKE FROM NETWORK TO THE WEBSERVER .

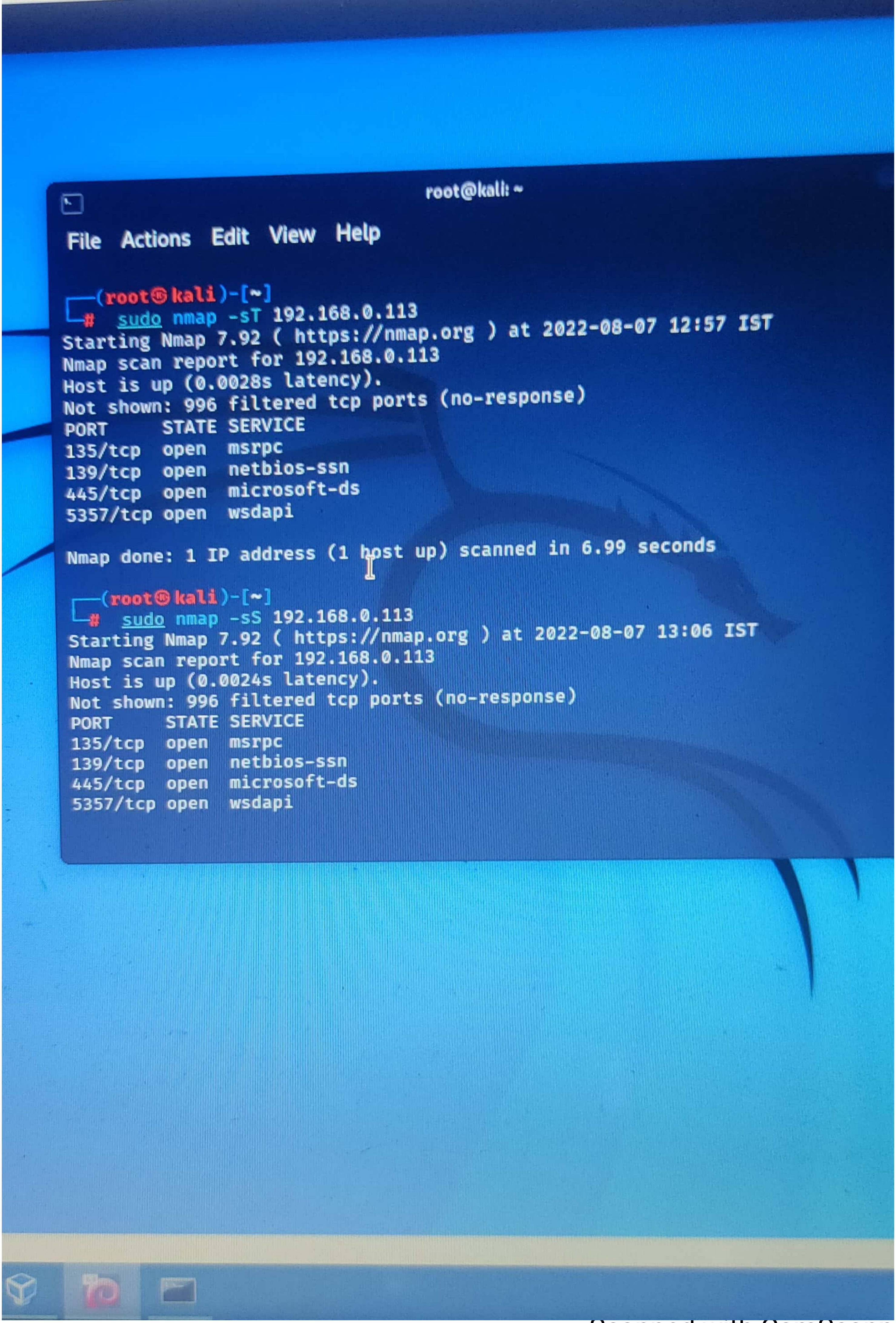
STEP 2: THEN YOU HAVE TO PERFORM NETWORK SCAN BY USING STEALTHY(-sS) I.e, syn scan (half open scan) from nmap to the ip .

STEP 3: THEN YOU HAVE TO OPEN WIRESHARK IN ONE PAGE AND SELECT ETH0 AND PERFORM –sS ,-st ,AGGRESIVE SCAN (-A) IN ROOT TERMINAL IN KALI LINUX .

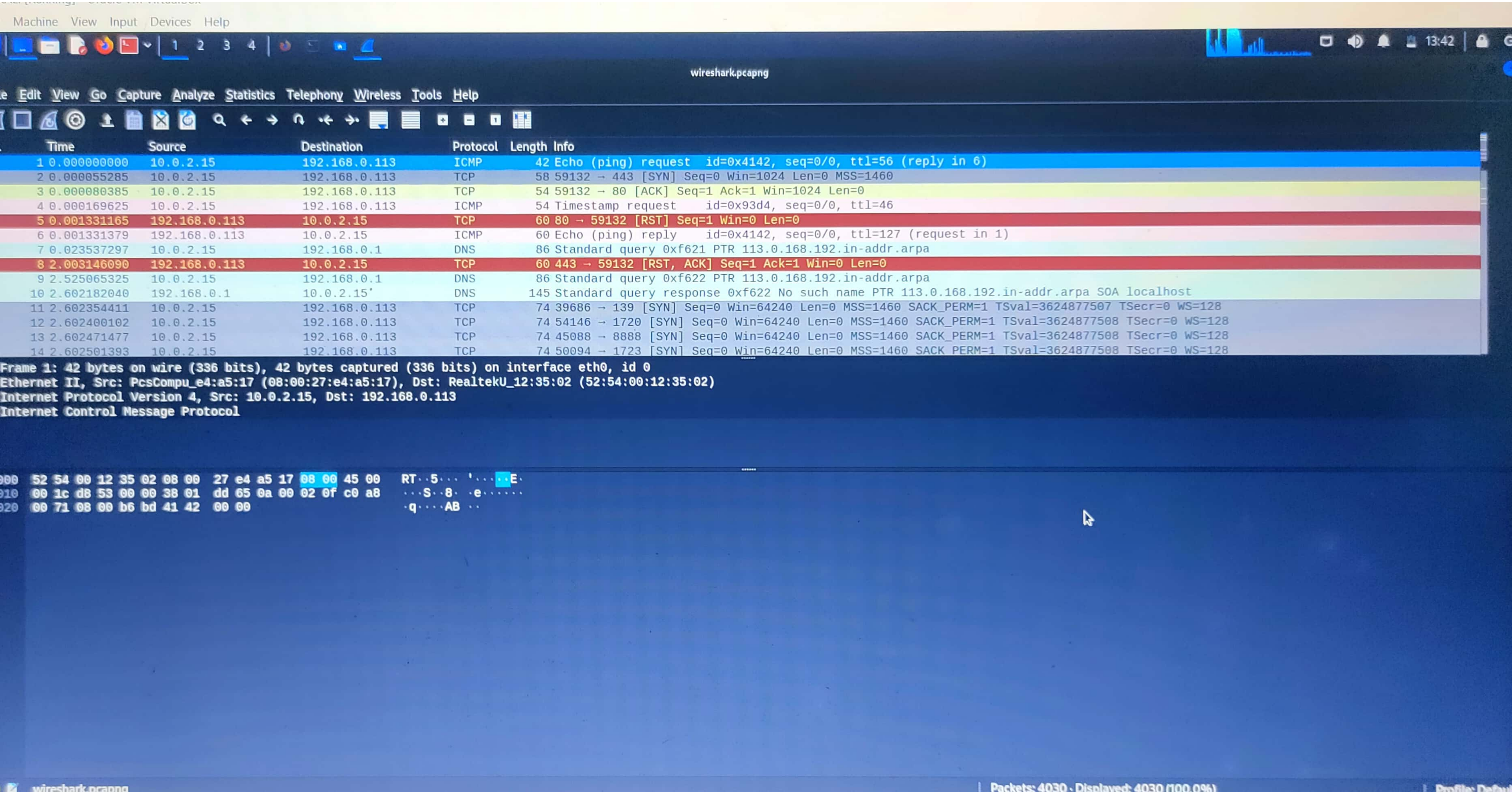
STEP 4: BY THIS YOU GET THE DECRYPT DATA FROM WIRESHARK TOOL HOW THEY TALK FROM SOURCE IP TO DESTINATION IP .


File Machine View Input Devices Help
File Actions Edit View Help

```
Nmap scan report for 192.168.0.113
Host is up (0.00033s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
5357/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed p
ort
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (92%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network gateway (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=17 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2022-08-07T05:19:50
|_  start_date: N/A

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.12 ms 10.0.2.2
2   0.09 ms 192.168.0.113

NSE: Script Post-scanning.
Initiating NSE at 10:49
Completed NSE at 10:49, 0.00s elapsed
Initiating NSE at 10:49
Completed NSE at 10:49, 0.00s elapsed
Initiating NSE at 10:49
Completed NSE at 10:49, 0.00s elapsed
Read data files from: /usr/bin/../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 31.90 seconds
           Raw packets sent: 2054 (93.460KB) | Rcvd: 1042 (42.784KB)

┌──(root㉿kali)-[/home/spycat]
└─# ping 10.7.1,226
```



```
┌──(root㉿kali)-[~]
└─# sudo nmap -sT 192.168.0.113
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-07 12:57 IST
Nmap scan report for 192.168.0.113
Host is up (0.0028s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 6.99 seconds

┌──(root㉿kali)-[~]
└─# sudo nmap -sS 192.168.0.113
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-07 13:06 IST
Nmap scan report for 192.168.0.113
Host is up (0.0024s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
```



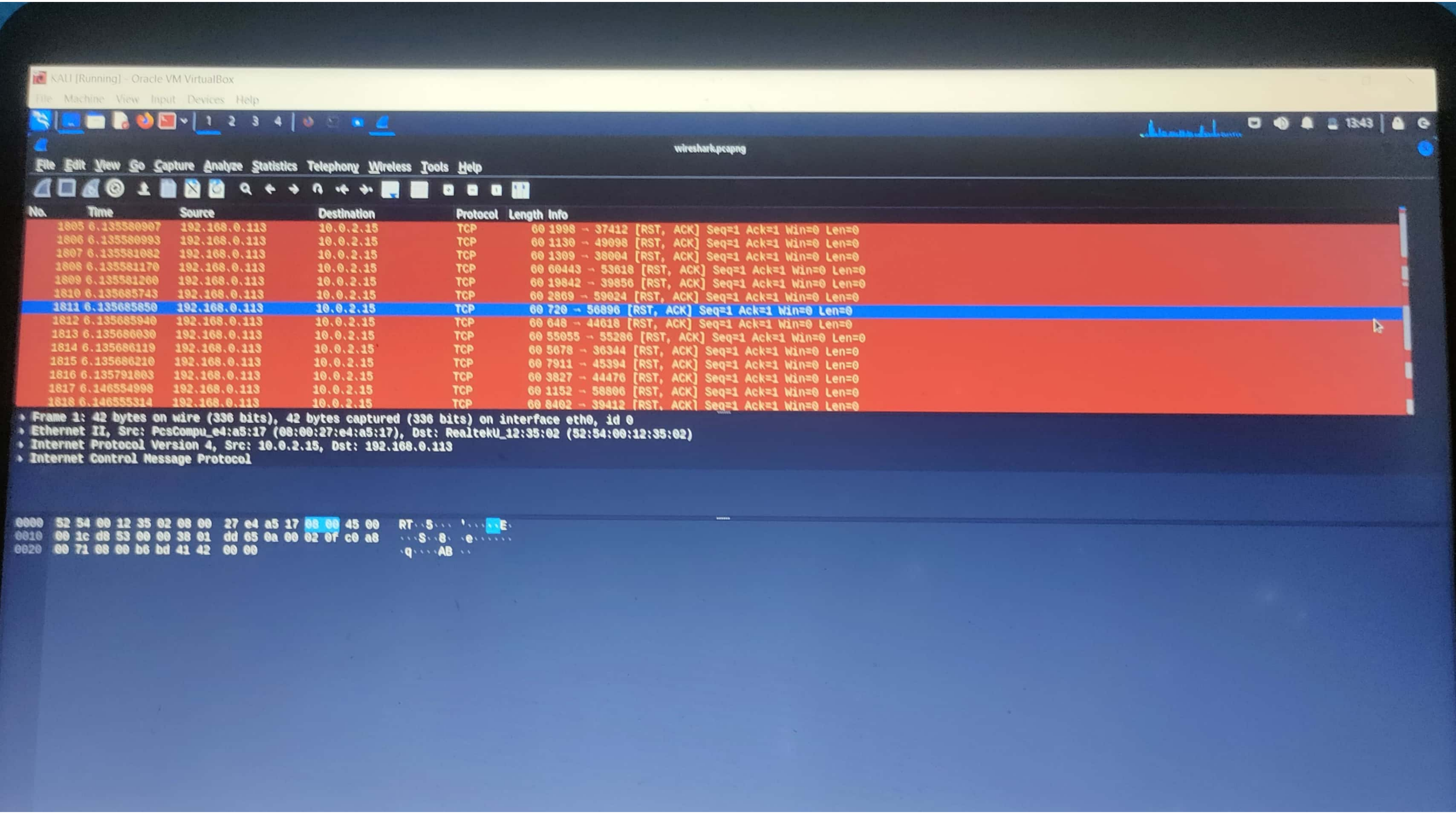
Machine View Input Devices Help
1 2 3 4
13:42
wireshark.pcapng
le Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
    Time          Source          Destination     Protocol  Length Info
  1 0.000000000   10.0.2.15       192.168.0.113   ICMP        42 Echo (ping) request  id=0x4142, seq=0/0, ttl=56 (reply in 6)
  2 0.000055285   10.0.2.15       192.168.0.113   TCP         58 59132 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  3 0.000080385   10.0.2.15       192.168.0.113   TCP         54 59132 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
  4 0.000169625   10.0.2.15       192.168.0.113   ICMP        54 Timestamp request    id=0x93d4, seq=0/0, ttl=46
  5 0.001331165   192.168.0.113   10.0.2.15       TCP         60 80 → 59132 [RST] Seq=1 Win=0 Len=0
  6 0.001331379   192.168.0.113   10.0.2.15       ICMP        60 Echo (ping) reply    id=0x4142, seq=0/0, ttl=127 (request in 1)
  7 0.023537297   10.0.2.15       192.168.0.1     DNS         86 Standard query 0xf621 PTR 113.0.168.192.in-addr.arpa
  8 2.003146090   192.168.0.113   10.0.2.15       TCP         60 443 → 59132 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  9 2.525065325   10.0.2.15       192.168.0.1     DNS         86 Standard query 0xf622 PTR 113.0.168.192.in-addr.arpa
 10 2.602182040   192.168.0.1     10.0.2.15       DNS        145 Standard query response 0xf622 No such name PTR 113.0.168.192.in-addr.arpa SOA localhost
 11 2.602354411   10.0.2.15       192.168.0.113   TCP         74 39686 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3624877507 TSecr=0 WS=128
 12 2.602400102   10.0.2.15       192.168.0.113   TCP         74 54146 → 1720 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3624877508 TSecr=0 WS=128
 13 2.602471477   10.0.2.15       192.168.0.113   TCP         74 45088 → 8888 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3624877508 TSecr=0 WS=128
 14 2.602501393   10.0.2.15       192.168.0.113   TCP         74 50094 → 1723 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3624877508 TSecr=0 WS=128
```

```
Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_e4:a5:17 (08:00:27:e4:a5:17), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.0.113
Internet Control Message Protocol
```

```
000  52 54 00 12 35 02 08 00  27 e4 a5 17 08 00 45 00   RT··5···  '·····E·
010  00 1c d8 53 00 00 38 01  dd 65 0a 00 02 0f c0 a8   ···S··8·  ·e······
020  00 71 08 00 b6 bd 41 42  00 00                     ·q····AB  ··
```

wireshark.pcapng | Packets: 4030 · Displayed: 4030 (100.0%) | Profile: Default

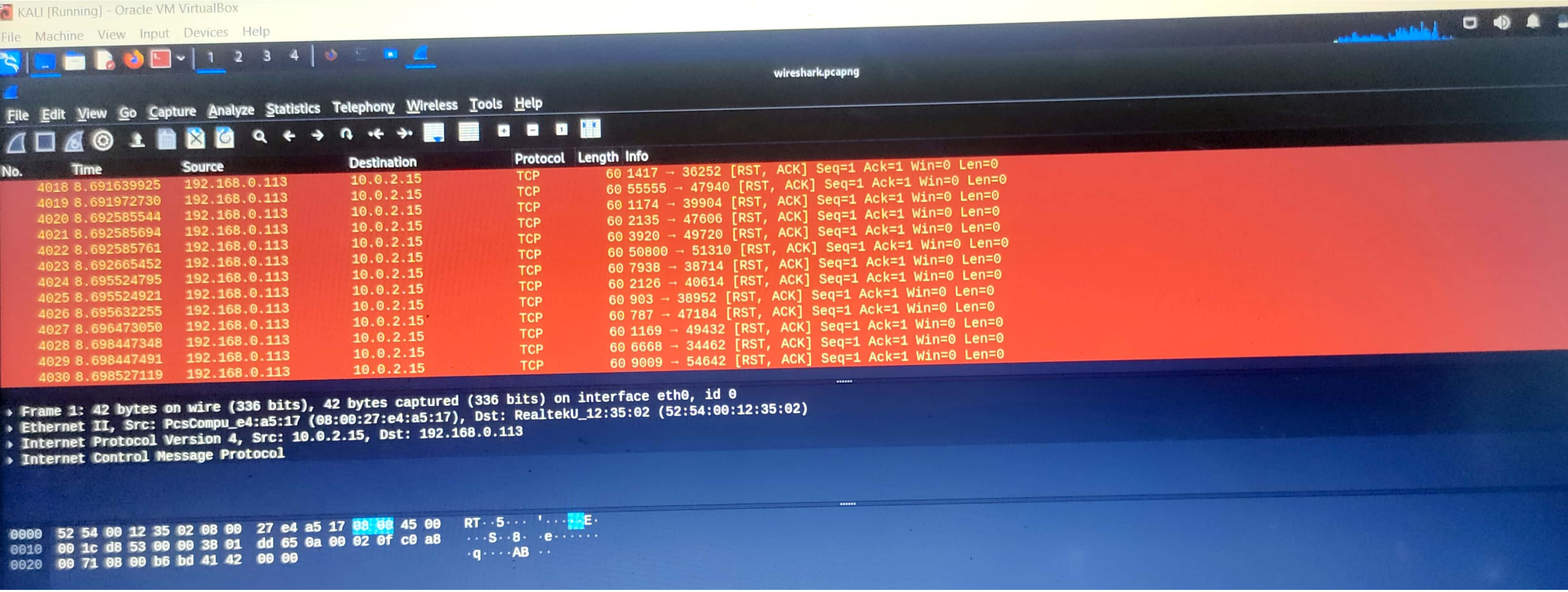


KALI [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
13:43
wireshark.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No.	Time	Source	Destination	Protocol	Length	Info
1805	6.135580907	192.168.0.113	10.0.2.15	TCP	60	1998 → 37412 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1806	6.135580993	192.168.0.113	10.0.2.15	TCP	60	1130 → 49098 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1807	6.135581082	192.168.0.113	10.0.2.15	TCP	60	1309 → 38004 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1808	6.135581170	192.168.0.113	10.0.2.15	TCP	60	60443 → 53618 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1809	6.135581260	192.168.0.113	10.0.2.15	TCP	60	19842 → 39856 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1810	6.135685743	192.168.0.113	10.0.2.15	TCP	60	2869 → 59024 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1811	6.135685850	192.168.0.113	10.0.2.15	TCP	60	720 → 56896 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1812	6.135685940	192.168.0.113	10.0.2.15	TCP	60	648 → 44618 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1813	6.135686030	192.168.0.113	10.0.2.15	TCP	60	55055 → 55286 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1814	6.135686119	192.168.0.113	10.0.2.15	TCP	60	5678 → 36344 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1815	6.135686210	192.168.0.113	10.0.2.15	TCP	60	7911 → 45394 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1816	6.135791803	192.168.0.113	10.0.2.15	TCP	60	3827 → 44476 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1817	6.146554998	192.168.0.113	10.0.2.15	TCP	60	1152 → 58806 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1818	6.146555314	192.168.0.113	10.0.2.15	TCP	60	8402 → 39412 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

```
▸ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
▸ Ethernet II, Src: PcsCompu_e4:a5:17 (08:00:27:e4:a5:17), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.0.113
▸ Internet Control Message Protocol
```

```
0000  52 54 00 12 35 02 08 00  27 e4 a5 17 08 00 45 00   RT··5···'·····E·
0010  00 1c d8 53 00 00 38 01  dd 65 0a 00 02 0f c0 a8   ···S··8··e······
0020  00 71 08 00 b6 bd 41 42  00 00                     ·q····AB··
```



KALI [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
wireshark.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
No.   Time          Source          Destination   Protocol  Length Info
 4018 8.691639925   192.168.0.113   10.0.2.15     TCP       60 1417 → 36252 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 4019 8.691972730   192.168.0.113   10.0.2.15     TCP       60 55555 → 47940 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 4020 8.692585544   192.168.0.113   10.0.2.15     TCP       60 1174 → 39904 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 4021 8.692585694   192.168.0.113   10.0.2.15     TCP       60 2135 → 47606 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 4022 8.692585761   192.168.0.113   10.0.2.15     TCP       60 3920 → 49720 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 4023 8.692665452   192.168.0.113   10.0.2.15     TCP       60 50800 → 51310 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 4024 8.695524795   192.168.0.113   10.0.2.15     TCP       60 7938 → 38714 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 4025 8.695524921   192.168.0.113   10.0.2.15     TCP       60 2126 → 40614 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 4026 8.695632255   192.168.0.113   10.0.2.15     TCP       60 903 → 38952 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 4027 8.696473050   192.168.0.113   10.0.2.15     TCP       60 787 → 47184 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 4028 8.698447348   192.168.0.113   10.0.2.15     TCP       60 1169 → 49432 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 4029 8.698447491   192.168.0.113   10.0.2.15     TCP       60 6668 → 34462 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 4030 8.698527119   192.168.0.113   10.0.2.15     TCP       60 9009 → 54642 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

```
› Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
› Ethernet II, Src: PcsCompu_e4:a5:17 (08:00:27:e4:a5:17), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
› Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.0.113
› Internet Control Message Protocol
```

```
0000  52 54 00 12 35 02 08 00  27 e4 a5 17 08 00 45 00   RT··5···  '·····E·
0010  00 1c d8 53 00 00 38 01  dd 65 0a 00 02 0f c0 a8   ···S··8·  ·e······
0020  00 71 08 00 b6 bd 41 42  00 00                     ·q····AB  ··
```

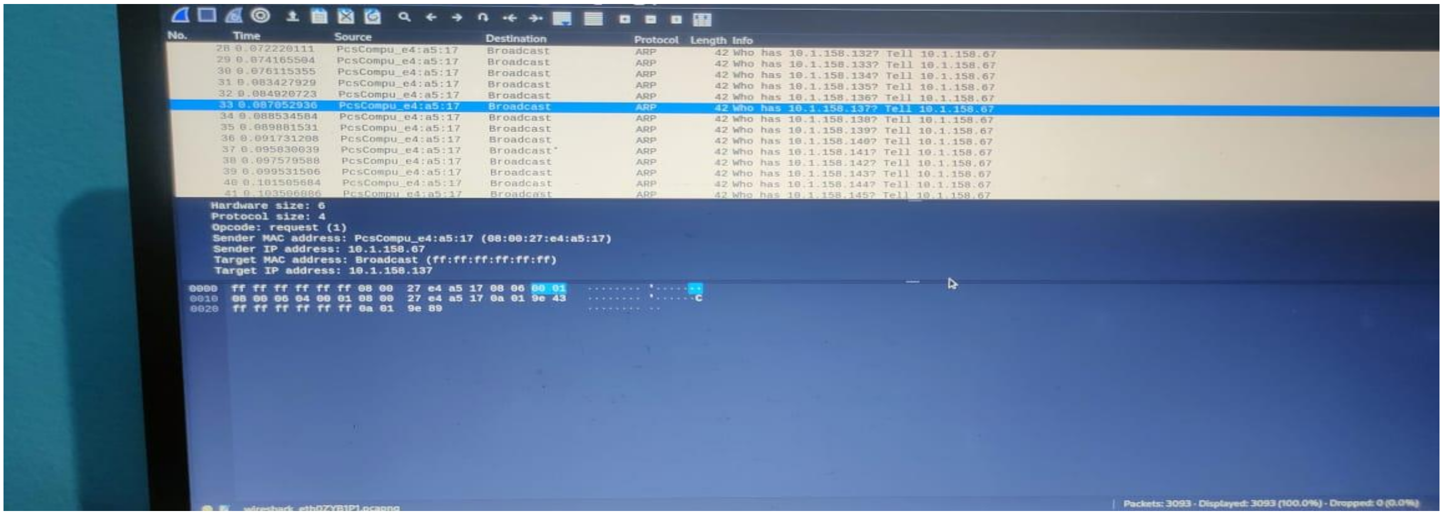
BETTERCAP AND WIRESHARK

STEP 1: FIRSTLY , OPEN THE KALI LINUX .

STEP 2: SECONDLY ,OPEN THREE ROOT TERMINAL .ONE FOR WINDOWS TO TELL THAT I AM YOUR ROUTER , SECOND IS FOR NETDISCOVER SHOWS THAT WHAT ARE THE DEVICES CONNECTED AND WHAT IS MY GATEWAY ADDTRESS AND THIRD IS ROUTER THAT I AM TAKING YOUR ADDRESS TO PERFORM SPOOFING .

STEP 3: THEN OPEN THE WIRESHARK AND RUN THE COMMAND IN THE TWO TERMINAL USING ARPSPOOF.RUN THE COMMAND ONE BY ONE BY ONE AT THE SAME TIME.

STEP 4: THEN GETTING DETAILS FROM WIRESHARK I.e., ANALYZING THE TRAFFIC USING WIRESHARK AND ALL REQUEST HAS BENN SHOWN ON WIRESHARK.



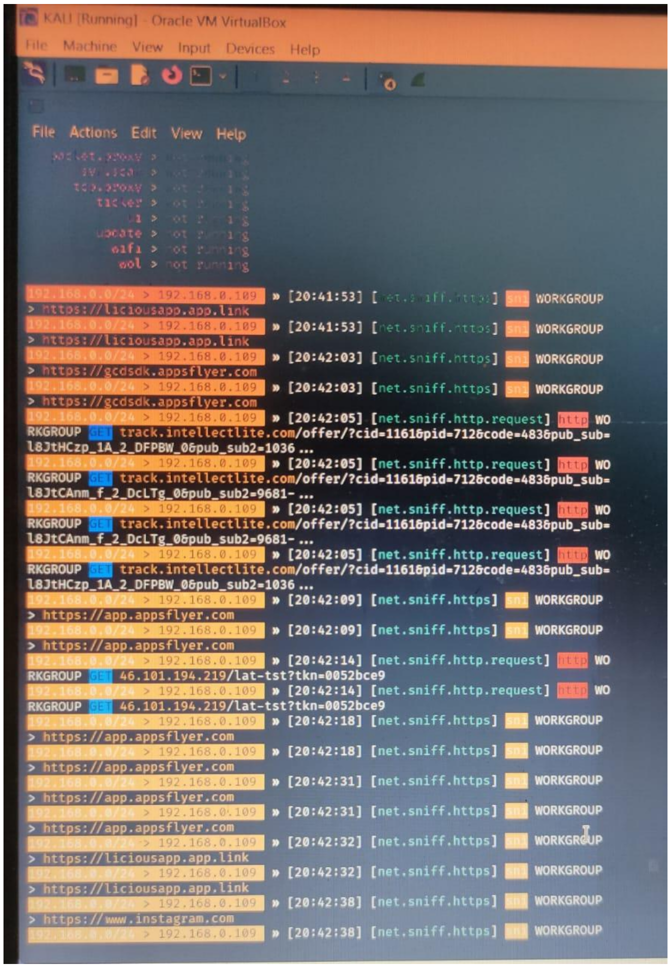
```
No.  Time           Source                 Destination   Protocol  Length  Info
28   0.072220111    PcsCompu_e4:a5:17      Broadcast     ARP       42      Who has 10.1.158.132? Tell 10.1.158.67
29   0.074165504    PcsCompu_e4:a5:17      Broadcast     ARP       42      Who has 10.1.158.133? Tell 10.1.158.67
30   0.076115355    PcsCompu_e4:a5:17      Broadcast     ARP       42      Who has 10.1.158.134? Tell 10.1.158.67
31   0.083427929    PcsCompu_e4:a5:17      Broadcast     ARP       42      Who has 10.1.158.135? Tell 10.1.158.67
32   0.084920723    PcsCompu_e4:a5:17      Broadcast     ARP       42      Who has 10.1.158.136? Tell 10.1.158.67
33   0.087052936    PcsCompu_e4:a5:17      Broadcast     ARP       42      Who has 10.1.158.137? Tell 10.1.158.67
34   0.088534584    PcsCompu_e4:a5:17      Broadcast     ARP       42      Who has 10.1.158.138? Tell 10.1.158.67
35   0.089881531    PcsCompu_e4:a5:17      Broadcast     ARP       42      Who has 10.1.158.139? Tell 10.1.158.67
36   0.091731208    PcsCompu_e4:a5:17      Broadcast     ARP       42      Who has 10.1.158.140? Tell 10.1.158.67
37   0.095830039    PcsCompu_e4:a5:17      Broadcast     ARP       42      Who has 10.1.158.141? Tell 10.1.158.67
38   0.097579588    PcsCompu_e4:a5:17      Broadcast     ARP       42      Who has 10.1.158.142? Tell 10.1.158.67
39   0.099531506    PcsCompu_e4:a5:17      Broadcast     ARP       42      Who has 10.1.158.143? Tell 10.1.158.67
40   0.101585684    PcsCompu_e4:a5:17      Broadcast     ARP       42      Who has 10.1.158.144? Tell 10.1.158.67
41   0.103506886    PcsCompu_e4:a5:17      Broadcast     ARP       42      Who has 10.1.158.145? Tell 10.1.158.67

    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: PcsCompu_e4:a5:17 (08:00:27:e4:a5:17)
    Sender IP address: 10.1.158.67
    Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
    Target IP address: 10.1.158.137

0000  ff ff ff ff ff ff 08 00  27 e4 a5 17 08 06 00 01   ........ '.......
0010  08 00 06 04 00 01 08 00  27 e4 a5 17 0a 01 9e 43   ........ '......C
0020  ff ff ff ff ff ff 0a 01  9e 89                     ........ ..

wireshark_eth0ZYB1P1.pcapng          Packets: 3093 · Displayed: 3093 (100.0%) · Dropped: 0 (0.0%)
```

STEP 4: IF YOU TERMINATE THE TERMINAL THE WIRESHARK STOPS .SO WE USING BETTERCAP .

STEP 5: SO, IN BETTERCAP WE BASICALLY ACCESS DATA OF THE TARGET MACHINE . WHEN WE OPEN THE OPEN THE BETTERCAP WE HAVE TO WRITE THE COMMAND I.e, bettercap –iface eth0 AND WE GET THE LIST OF COMMAND BY WRITING HELP AND GET THE MODULES WHICH YOU HAVE TO OPEN .

STEP 6: MODULES ARE net.probe , any.proxy ,net.spoof ,net.recon ,arp.spoof ,net.sniff ,WHICH TYPE OF DATA ACCESS FROM THE TARGET MACHINE YOU HAVE TO JUST ON THAT MODULE BY WRITING THAT MODULE SPACE ON AND YOU GET THE ACCESS THE DATA.

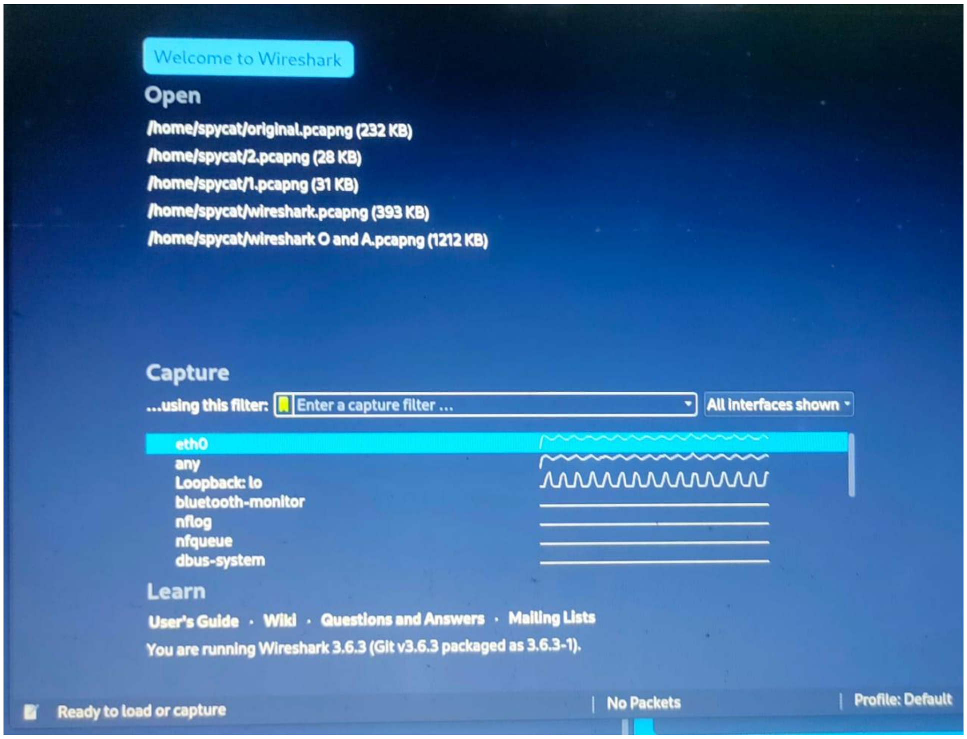
STEP 7: AS TARGET MACHINE OPEN ANY SERVER OR ANY TYPE OF DATA ALL THE INFORMATION SHOWING IN THE BETTERCAP TOOL TERMINAL.


KALI [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help

```
packet.proxy > not running
    syn.scan > not running
   tcp.proxy > not running
      ticker > not running
          ui > not running
      update > not running
        wifi > not running
         wol > not running

192.168.0.0/24 > 192.168.0.109  » [20:41:53] [net.sniff.https] sni WORKGROUP
> https://liciousapp.app.link
192.168.0.0/24 > 192.168.0.109  » [20:41:53] [net.sniff.https] sni WORKGROUP
> https://liciousapp.app.link
192.168.0.0/24 > 192.168.0.109  » [20:42:03] [net.sniff.https] sni WORKGROUP
> https://gcdsdk.appsflyer.com
192.168.0.0/24 > 192.168.0.109  » [20:42:03] [net.sniff.https] sni WORKGROUP
> https://gcdsdk.appsflyer.com
192.168.0.0/24 > 192.168.0.109  » [20:42:05] [net.sniff.http.request] http WO
RKGROUP GET track.intellectlite.com/offer/?cid=1161&pid=712&code=483&pub_sub=
l8JtHCzp_1A_2_DFPBW_0&pub_sub2=1036 ...
192.168.0.0/24 > 192.168.0.109  » [20:42:05] [net.sniff.http.request] http WO
RKGROUP GET track.intellectlite.com/offer/?cid=1161&pid=712&code=483&pub_sub=
l8JtCAnm_f_2_DcLTg_0&pub_sub2=9681- ...
192.168.0.0/24 > 192.168.0.109  » [20:42:05] [net.sniff.http.request] http WO
RKGROUP GET track.intellectlite.com/offer/?cid=1161&pid=712&code=483&pub_sub=
l8JtCAnm_f_2_DcLTg_0&pub_sub2=9681- ...
192.168.0.0/24 > 192.168.0.109  » [20:42:05] [net.sniff.http.request] http WO
RKGROUP GET track.intellectlite.com/offer/?cid=1161&pid=712&code=483&pub_sub=
l8JtHCzp_1A_2_DFPBW_0&pub_sub2=1036 ...
192.168.0.0/24 > 192.168.0.109  » [20:42:09] [net.sniff.https] sni WORKGROUP
> https://app.appsflyer.com
192.168.0.0/24 > 192.168.0.109  » [20:42:09] [net.sniff.https] sni WORKGROUP
> https://app.appsflyer.com
192.168.0.0/24 > 192.168.0.109  » [20:42:14] [net.sniff.http.request] http WO
RKGROUP GET 46.101.194.219/lat-tst?tkn=0052bce9
192.168.0.0/24 > 192.168.0.109  » [20:42:14] [net.sniff.http.request] http WO
RKGROUP GET 46.101.194.219/lat-tst?tkn=0052bce9
192.168.0.0/24 > 192.168.0.109  » [20:42:18] [net.sniff.https] sni WORKGROUP
> https://app.appsflyer.com
192.168.0.0/24 > 192.168.0.109  » [20:42:18] [net.sniff.https] sni WORKGROUP
> https://app.appsflyer.com
192.168.0.0/24 > 192.168.0.109  » [20:42:31] [net.sniff.https] sni WORKGROUP
> https://app.appsflyer.com
192.168.0.0/24 > 192.168.0.109  » [20:42:31] [net.sniff.https] sni WORKGROUP
> https://app.appsflyer.com
192.168.0.0/24 > 192.168.0.109  » [20:42:32] [net.sniff.https] sni WORKGROUP
> https://liciousapp.app.link
192.168.0.0/24 > 192.168.0.109  » [20:42:32] [net.sniff.https] sni WORKGROUP
> https://liciousapp.app.link
192.168.0.0/24 > 192.168.0.109  » [20:42:38] [net.sniff.https] sni WORKGROUP
> https://www.instagram.com
192.168.0.0/24 > 192.168.0.109  » [20:42:38] [net.sniff.https] sni WORKGROUP
```

STEP 7 : MAN IN THE MIDDLE ATTACK PERFORMING WELL OR NOT IS SHOWED ON WIRESHARK BY SHOWING US ON GRAPH OF ETH0 ,ANY

AND LOOPBACK:LO.



Welcome to Wireshark

Open

/home/spycat/original.pcapng (232 KB)
/home/spycat/2.pcapng (28 KB)
/home/spycat/1.pcapng (31 KB)
/home/spycat/wireshark.pcapng (393 KB)
/home/spycat/wireshark O and A.pcapng (1212 KB)

Capture

...using this filter: Enter a capture filter ... All interfaces shown

eth0
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 3.6.3 (Git v3.6.3 packaged as 3.6.3-1).

Ready to load or capture | No Packets | Profile: Default

TEAM :

1.Joel Jiju Varghese

2.Yaddlapalli Avinash

3.Sanskar Singh Rajput

4.Harsh Raj

5.Somya Rajak