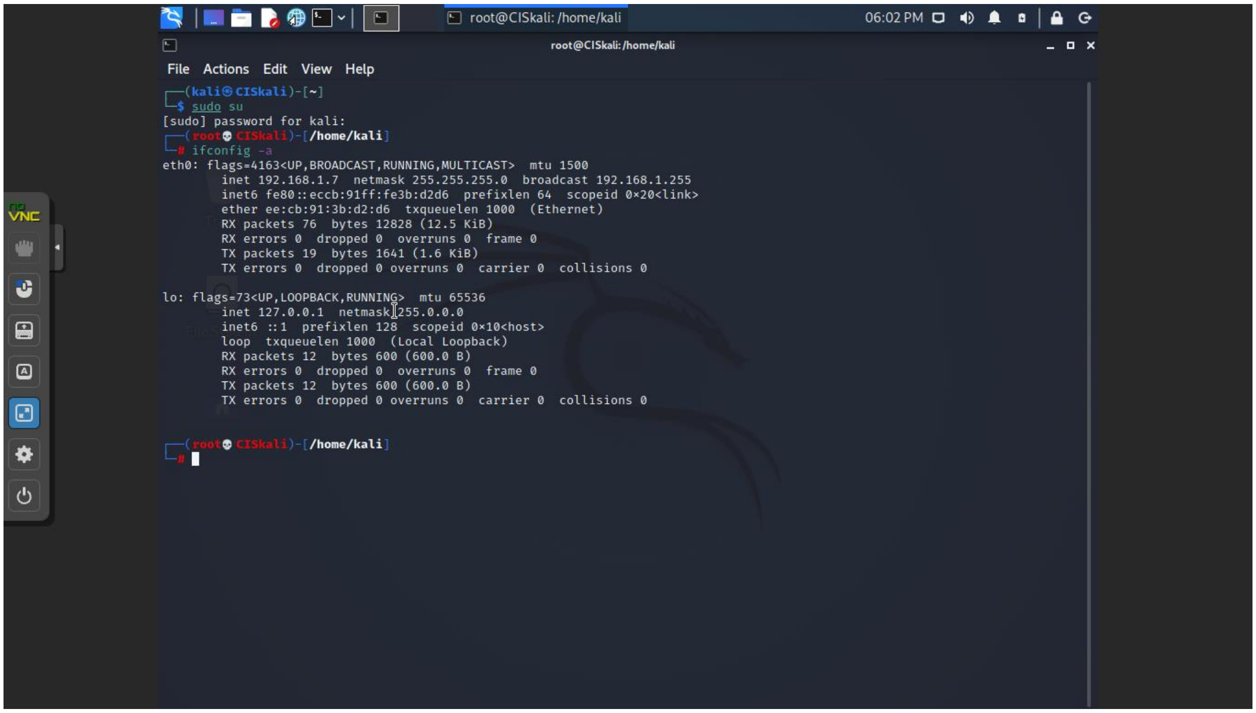
Homework 3: Packet Analysis (Part 2)

- This is an individual assignment, and worth 20 points.
- The due date is Tuesday, September 28, 2:30 (Sec 01) / 5:30 (Sec 76).
- You should not scan any live servers using Nmap or send malicious packets using hping3. If caught, you may be expelled from school (not a joke!).
- Please zoom in on the outcomes.
- Use the accompanying outcome document to report your results.
- Follow the naming convention.
- YOU ARE NOT ALLOWED TO DO THIS DURING THE CLASS.

Task 1. Identifying the IP address of Kali

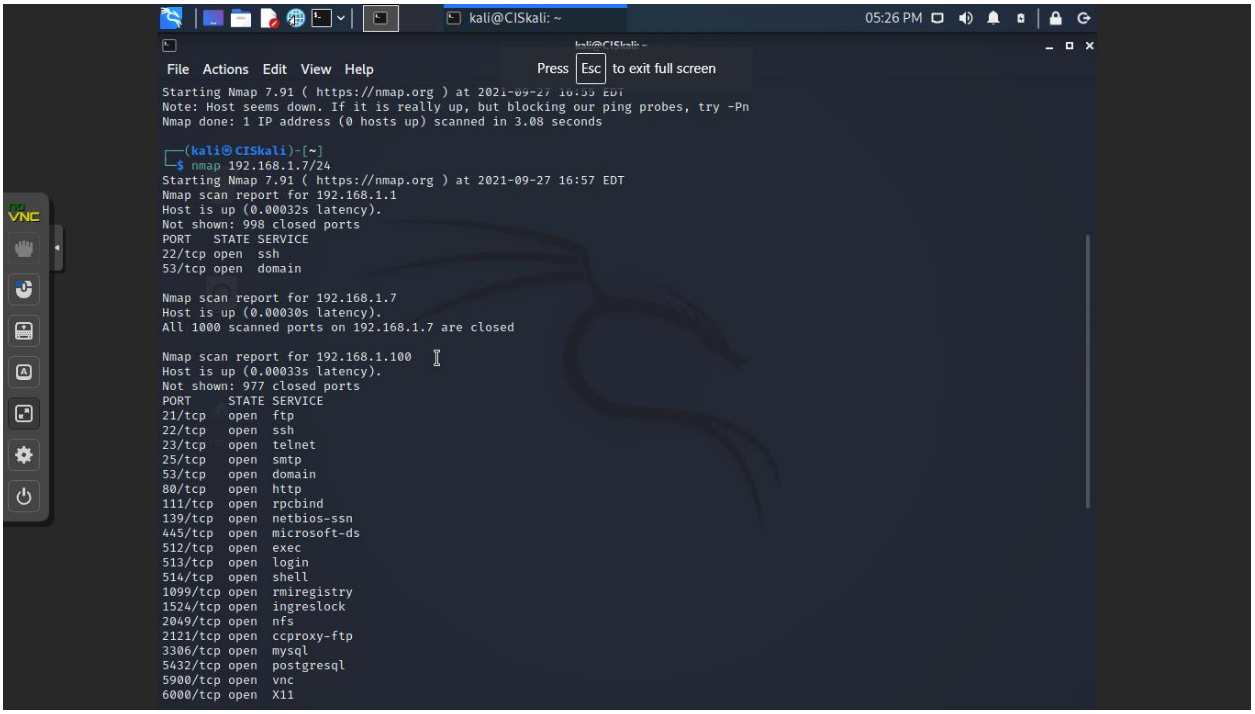
- Find the IP address and the subnet mask of **Kali**. Report the result with a screenshot.



```
┌──(kali㉿CISkali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root💀CISkali)-[/home/kali]
└─# ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.7  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::eccb:91ff:fe3b:d2d6  prefixlen 64  scopeid 0x20<link>
        ether ee:cb:91:3b:d2:d6  txqueuelen 1000  (Ethernet)
        RX packets 76  bytes 12828 (12.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 19  bytes 1641 (1.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 12  bytes 600 (600.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12  bytes 600 (600.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root💀CISkali)-[/home/kali]
└─# 
```

Task 2. Performing a Ping Sweeping

- Take a screenshot of the Nmap scan report. The screenshot should include the command you used.

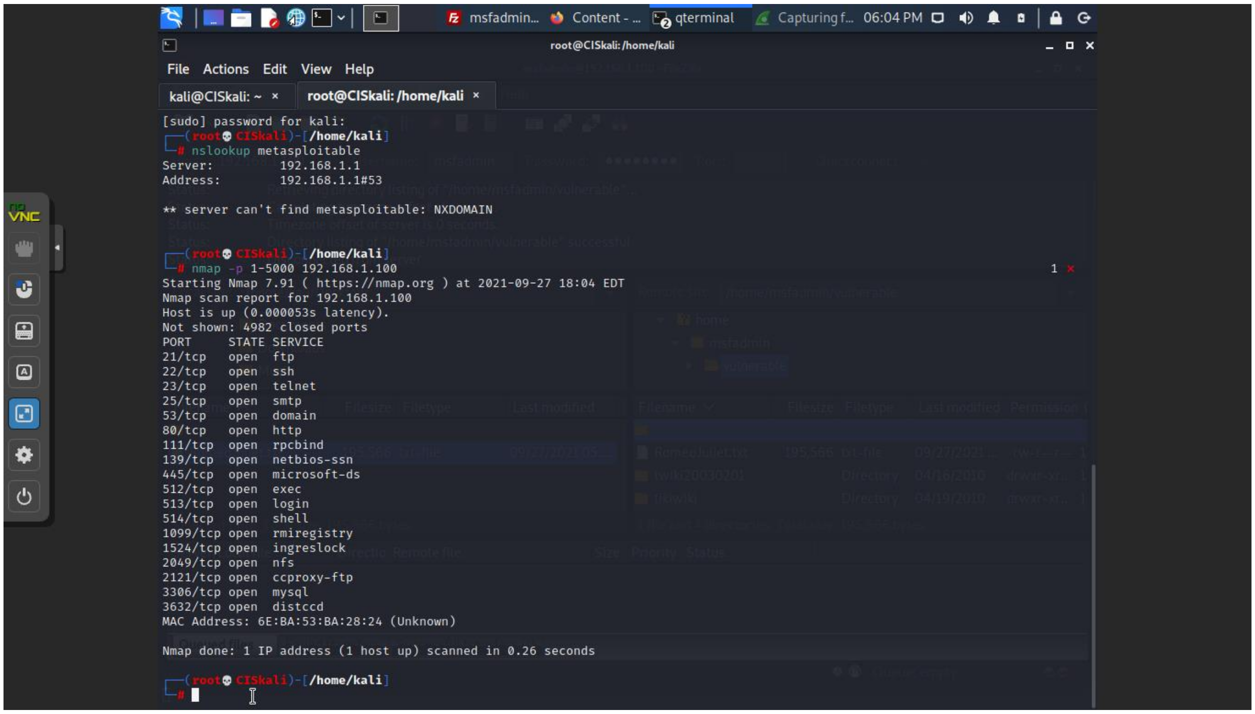


```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-27 16:55 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.08 seconds

┌──(kali㉿CISkali)-[~]
└─$ nmap 192.168.1.7/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-27 16:57 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00032s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain

Nmap scan report for 192.168.1.7
Host is up (0.00030s latency).
All 1000 scanned ports on 192.168.1.7 are closed

Nmap scan report for 192.168.1.100
Host is up (0.00033s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
```

- Report the IP address of **Metasploitable**.
  192.168.1.100

Task 3. Performing a Port Scanning

- Take a screenshot of the scan report. The screenshot must include the command you used.

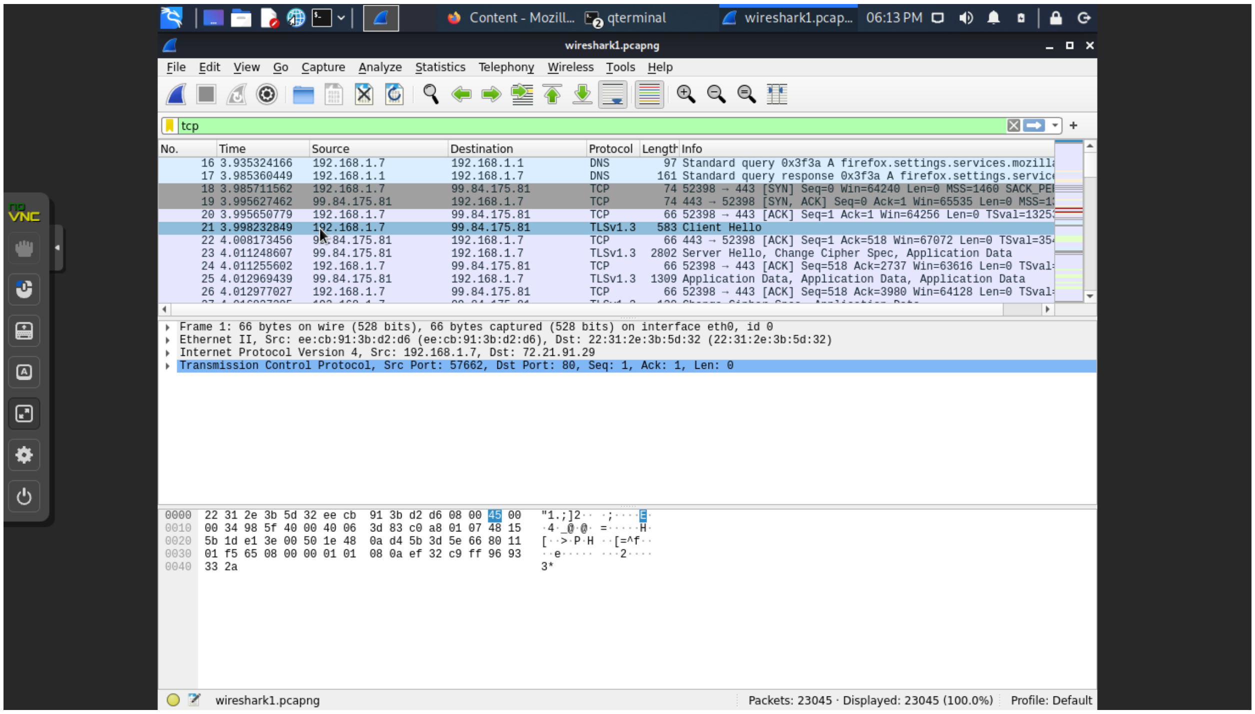


```
[sudo] password for kali:
┌──(root💀CISkali)-[/home/kali]
└─# nslookup metasploitable
Server:         192.168.1.1
Address:        192.168.1.1#53

** server can't find metasploitable: NXDOMAIN


┌──(root💀CISkali)-[/home/kali]
└─# nmap -p 1-5000 192.168.1.100                                    1 ×
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-27 18:04 EDT
Nmap scan report for 192.168.1.100
Host is up (0.000053s latency).
Not shown: 4982 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
3632/tcp open  distccd
MAC Address: 6E:BA:53:BA:28:24 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds

┌──(root💀CISkali)-[/home/kali]
└─# 
```

Task 4. Analyzing FTP Signatures

- Task

1) Identify the TCP packets used for the initial three-way handshake for the connection to Metasploitable. Take a screenshot of those TCP packets. Those packets are placed right before the first ftp packet.



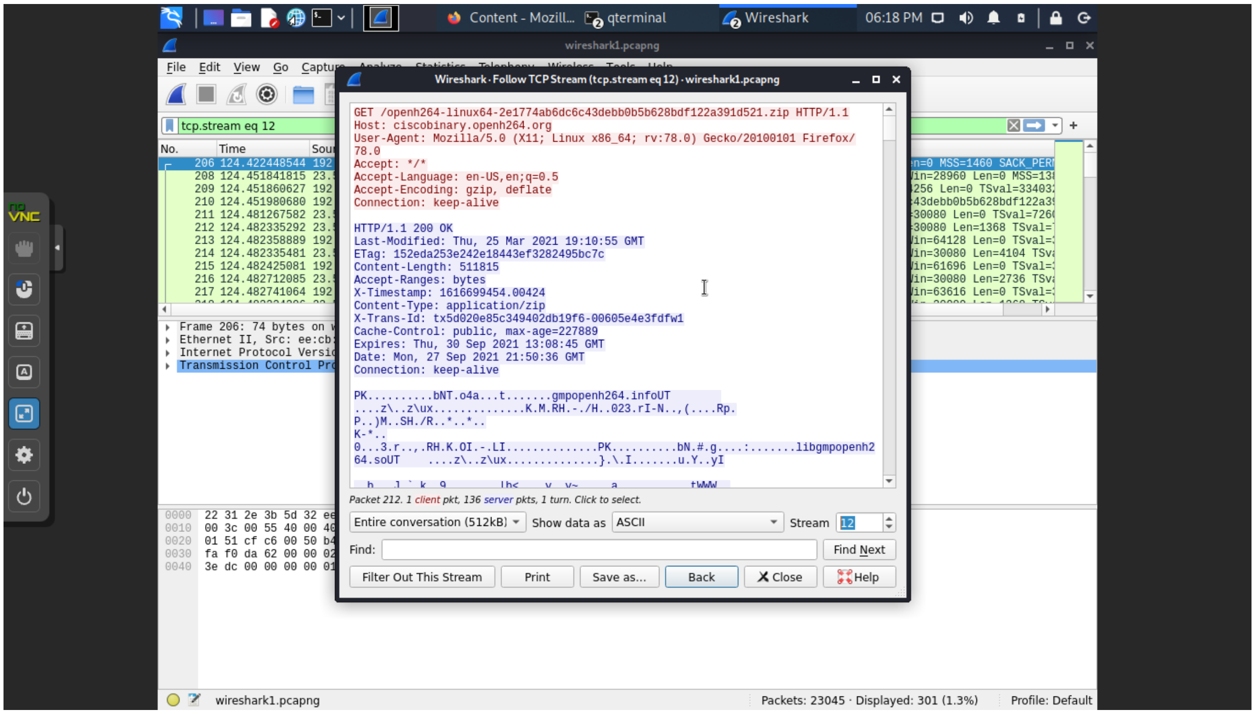
wireshark1.pcapng

Filter: tcp

```
No.  Time         Source         Destination    Protocol Length Info
  16 3.935324166  192.168.1.7    192.168.1.1    DNS        97 Standard query 0x3f3a A firefox.settings.services.mozilla
  17 3.985360449  192.168.1.1    192.168.1.7    DNS       161 Standard query response 0x3f3a A firefox.settings.service
  18 3.985711562  192.168.1.7    99.84.175.81   TCP        74 52398 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PE
  19 3.995627462  99.84.175.81   192.168.1.7    TCP        74 443 → 52398 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1
  20 3.995650779  192.168.1.7    99.84.175.81   TCP        66 52398 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1325
  21 3.998232849  192.168.1.7    99.84.175.81   TLSv1.3   583 Client Hello
  22 4.008173456  99.84.175.81   192.168.1.7    TCP        66 443 → 52398 [ACK] Seq=1 Ack=518 Win=67072 Len=0 TSval=35
  23 4.011248607  99.84.175.81   192.168.1.7    TLSv1.3  2802 Server Hello, Change Cipher Spec, Application Data
  24 4.011255602  192.168.1.7    99.84.175.81   TCP        66 52398 → 443 [ACK] Seq=518 Ack=2737 Win=63616 Len=0 TSval=
  25 4.012969439  99.84.175.81   192.168.1.7    TLSv1.3  1309 Application Data, Application Data, Application Data
  26 4.012977027  192.168.1.7    99.84.175.81   TCP        66 52398 → 443 [ACK] Seq=518 Ack=3980 Win=64128 Len=0 TSval=

▸ Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0
▸ Ethernet II, Src: ee:cb:91:3b:d2:d6 (ee:cb:91:3b:d2:d6), Dst: 22:31:2e:3b:5d:32 (22:31:2e:3b:5d:32)
▸ Internet Protocol Version 4, Src: 192.168.1.7, Dst: 72.21.91.29
▸ Transmission Control Protocol, Src Port: 57662, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

0000  22 31 2e 3b 5d 32 ee cb  91 3b d2 d6 08 00 45 00   "1.;]2·· ·;····E·
0010  00 34 98 5f 40 00 40 06  3d 83 c0 a8 01 07 48 15   ·4·_@·@· =·····H·
0020  5b 1d e1 3e 00 50 1e 48  0a d4 5b 3d 5e 66 80 11   [··>·P·H ··[=^f··
0030  01 f5 65 08 00 00 01 01  08 0a ef 32 c9 ff 96 93   ··e····· ···2····
0040  33 2a                                              3*
```

wireshark1.pcapng   Packets: 23045 · Displayed: 23045 (100.0%)   Profile: Default

2) Identify the TCP stream used for the authentication of the client to the FTP server. Take a screenshot of the content of the TCP stream. For this, go to Analyze > Follow > TCP Stream and locate the TCP stream.



Wireshark · Follow TCP Stream (tcp.stream eq 12) · wireshark1.pcapng

Filter: tcp.stream eq 12

```
GET /openh264-linux64-2e1774ab6dc6c43debb0b5b628bdf122a391d521.zip HTTP/1.1
Host: ciscobinary.openh264.org
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/
78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive

HTTP/1.1 200 OK
Last-Modified: Thu, 25 Mar 2021 19:10:55 GMT
ETag: 152eda253e242e18443ef3282495bc7c
Content-Length: 511815
Accept-Ranges: bytes
X-Timestamp: 1616699454.00424
Content-Type: application/zip
X-Trans-Id: tx5d020e85c349402db19f6-00605e4e3fdfw1
Cache-Control: public, max-age=227889
Expires: Thu, 30 Sep 2021 13:08:45 GMT
Date: Mon, 27 Sep 2021 21:50:36 GMT
Connection: keep-alive

PK..........bNT.o4a...t.......gmpopenh264.infoUT
....z\..z\ux.............K.M.RH.-./H..023.rI-N..,(....Rp.
P..)M..SH./R..*..*..
K-*..
0...3.r..,.RH.K.OI.-.LI.............PK..........bN.#.g....:.......libgmpopenh2
64.soUT    ....z\..z\ux.............}.\.I.......u.Y..yI
```

Packet 212. 1 client pkt, 136 server pkts, 1 turn. Click to select.

Entire conversation (512kB)   Show data as: ASCII   Stream: 12

Find:

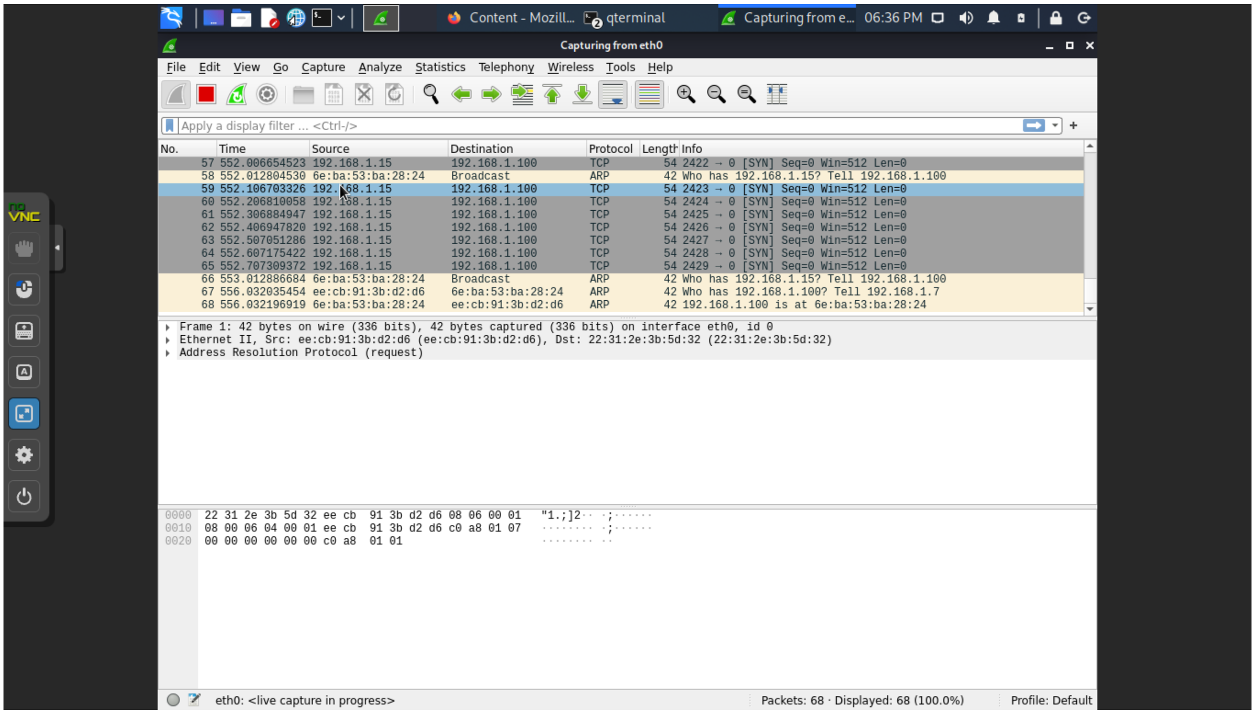
wireshark1.pcapng   Packets: 23045 · Displayed: 301 (1.3%)   Profile: Default

3) After examining the TCP stream in 2) above, discuss security implications of the file transfer.

Lack of encryption

Task 5. SYN Flooding Attack

1) Report your Wireshark capture in a screenshot that displays the source and destination IPs and [SYN].



Capturing from eth0

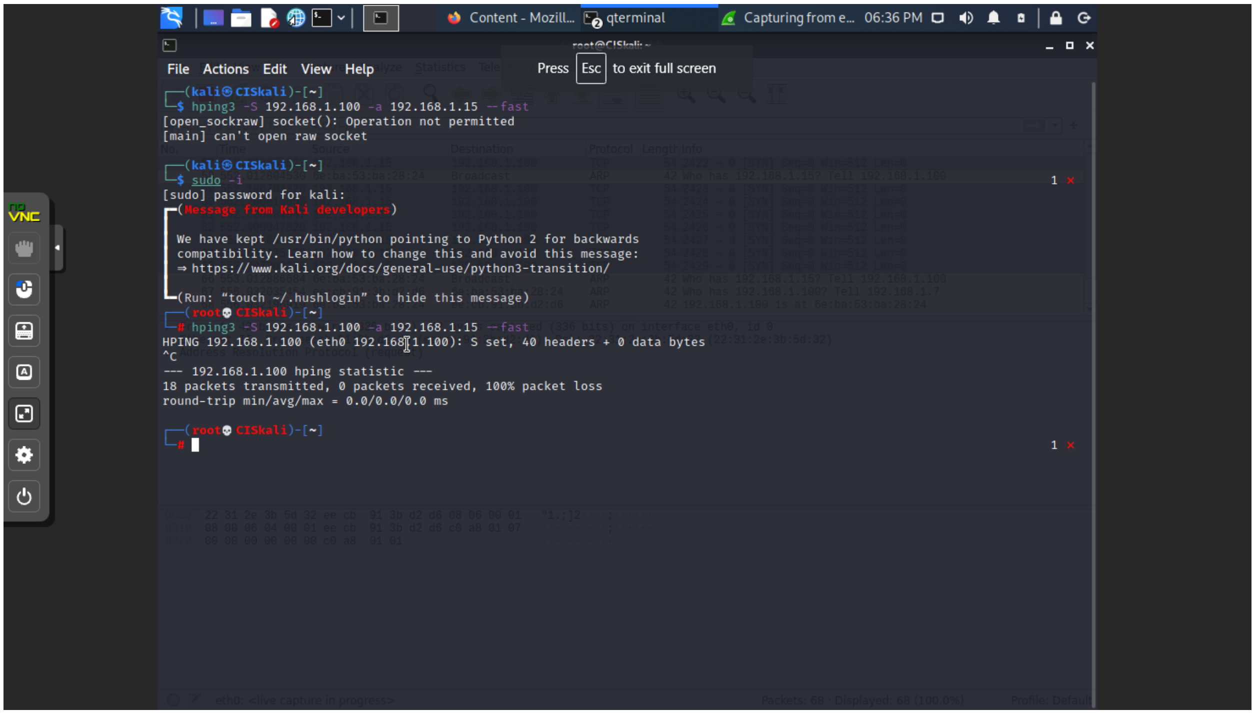
No.	Time	Source	Destination	Protocol	Length	Info
57	552.006654523	192.168.1.15	192.168.1.100	TCP	54	2422 → 0 [SYN] Seq=0 Win=512 Len=0
58	552.012804530	6e:ba:53:ba:28:24	Broadcast	ARP	42	Who has 192.168.1.15? Tell 192.168.1.100
59	552.106703326	192.168.1.15	192.168.1.100	TCP	54	2423 → 0 [SYN] Seq=0 Win=512 Len=0
60	552.206810058	192.168.1.15	192.168.1.100	TCP	54	2424 → 0 [SYN] Seq=0 Win=512 Len=0
61	552.306884947	192.168.1.15	192.168.1.100	TCP	54	2425 → 0 [SYN] Seq=0 Win=512 Len=0
62	552.406947820	192.168.1.15	192.168.1.100	TCP	54	2426 → 0 [SYN] Seq=0 Win=512 Len=0
63	552.507051286	192.168.1.15	192.168.1.100	TCP	54	2427 → 0 [SYN] Seq=0 Win=512 Len=0
64	552.607175422	192.168.1.15	192.168.1.100	TCP	54	2428 → 0 [SYN] Seq=0 Win=512 Len=0
65	552.707309372	192.168.1.15	192.168.1.100	TCP	54	2429 → 0 [SYN] Seq=0 Win=512 Len=0
66	553.012886684	6e:ba:53:ba:28:24	Broadcast	ARP	42	Who has 192.168.1.15? Tell 192.168.1.100
67	556.032035454	ee:cb:91:3b:d2:d6	6e:ba:53:ba:28:24	ARP	42	Who has 192.168.1.100? Tell 192.168.1.7
68	556.032196919	6e:ba:53:ba:28:24	ee:cb:91:3b:d2:d6	ARP	42	192.168.1.100 is at 6e:ba:53:ba:28:24

```
Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
Ethernet II, Src: ee:cb:91:3b:d2:d6 (ee:cb:91:3b:d2:d6), Dst: 22:31:2e:3b:5d:32 (22:31:2e:3b:5d:32)
Address Resolution Protocol (request)
```

```
0000  22 31 2e 3b 5d 32 ee cb  91 3b d2 d6 08 06 00 01   "1.;]2·· ·;······
0010  08 00 06 04 00 01 ee cb  91 3b d2 d6 c0 a8 01 07   ········ ·;······
0020  00 00 00 00 00 00 c0 a8  01 01                     ········ ··
```

eth0: <live capture in progress>   Packets: 68 · Displayed: 68 (100.0%)   Profile: Default

2) Also, take a screenshot that shows the command you used.



```
┌──(kali㉿CISkali)-[~]
└─$ hping3 -S 192.168.1.100 -a 192.168.1.15 --fast
[open_sockraw] socket(): Operation not permitted
[main] can't open raw socket

┌──(kali㉿CISkali)-[~]
└─$ sudo -i
[sudo] password for kali:
┏━(Message from Kali developers)
┃
┃ We have kept /usr/bin/python pointing to Python 2 for backwards
┃ compatibility. Learn how to change this and avoid this message:
┃ ⇒ https://www.kali.org/docs/general-use/python3-transition/
┃
┗━(Run: “touch ~/.hushlogin” to hide this message)
┌──(root💀CISkali)-[~]
└─# hping3 -S 192.168.1.100 -a 192.168.1.15 --fast
HPING 192.168.1.100 (eth0 192.168.1.100): S set, 40 headers + 0 data bytes
^C
--- 192.168.1.100 hping statistic ---
18 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

┌──(root💀CISkali)-[~]
└─# 
```