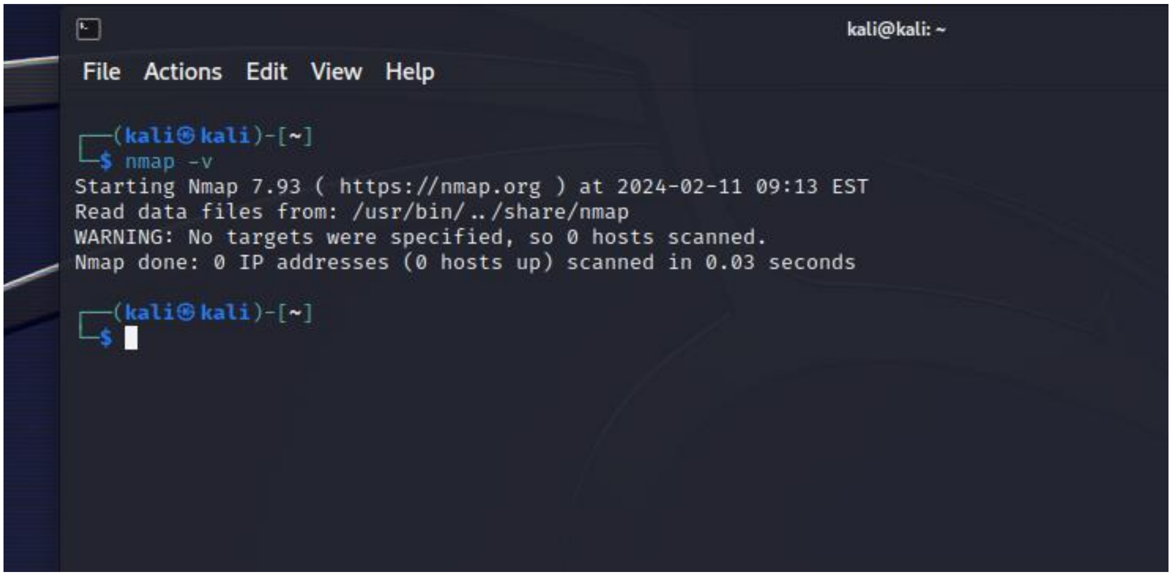
Network Security

Roll: MC233102
Name: Anwar Hussain
Mobile: 01750010980
Email: palash.cuet@gmail.com

Exercise 1: Nmap Exploration with Kali Linux

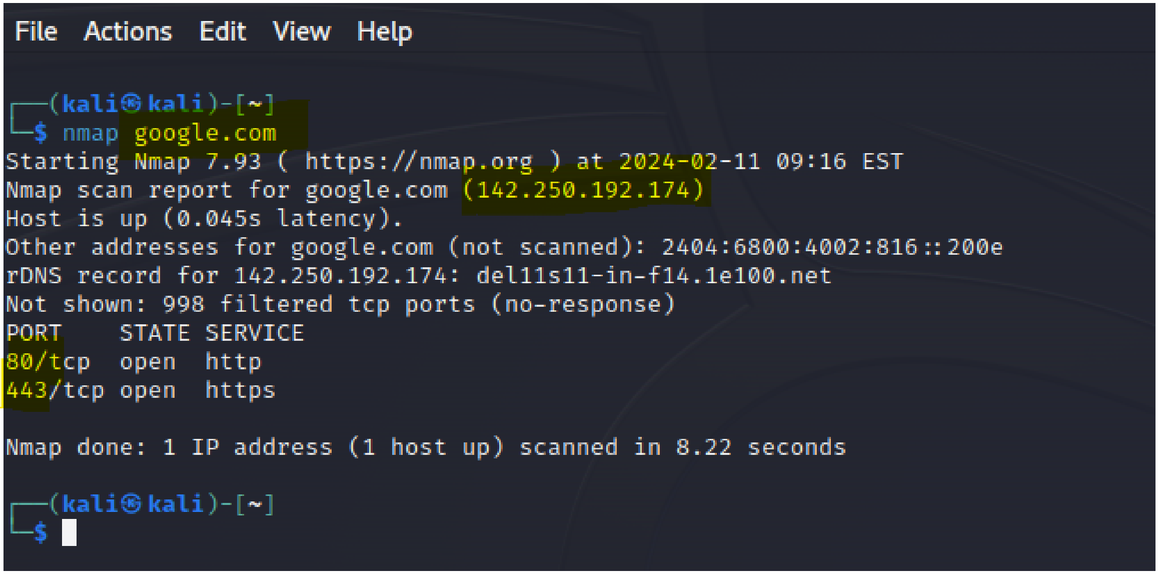
In the following exercise, I have used these commands.

1. Version Check: nmap -v

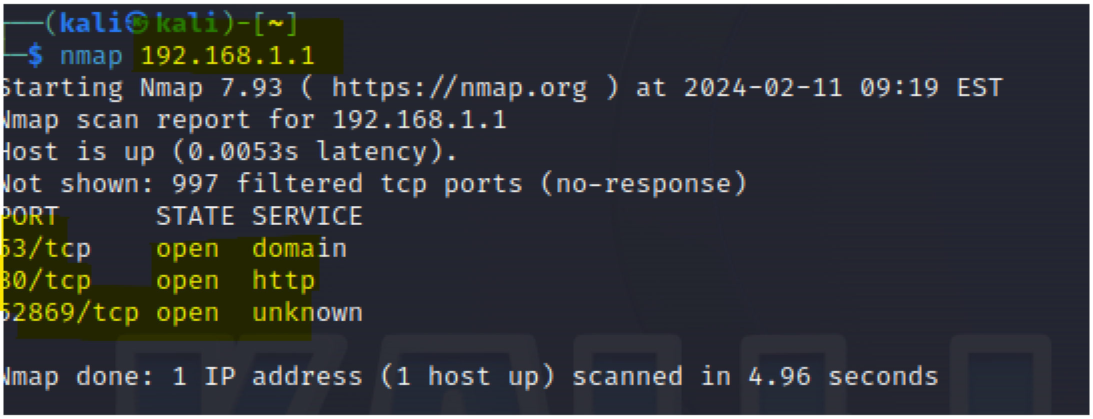


```
┌──(kali㉿kali)-[~]
└─$ nmap -v
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-11 09:13 EST
Read data files from: /usr/bin/../share/nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.03 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

2. Scanning Website and IP: **nmap google.com / nmap 192.168.1.1**

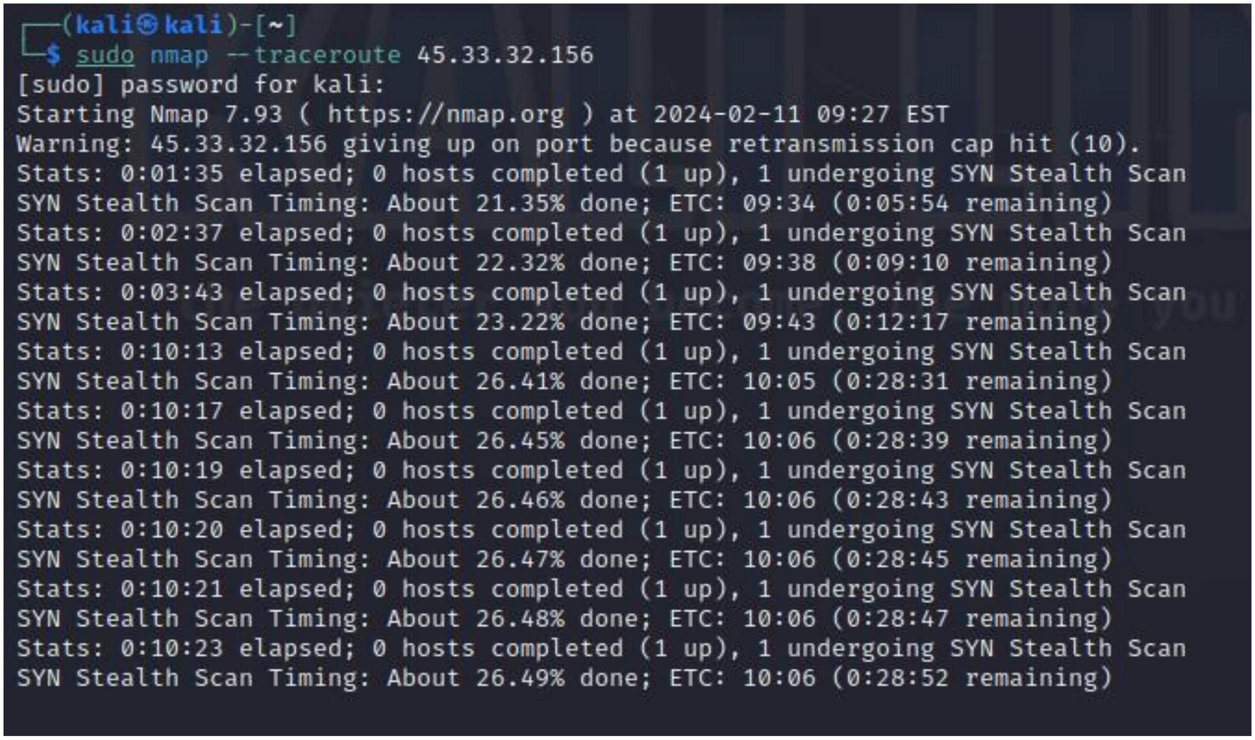


```
┌──(kali㉿kali)-[~]
└─$ nmap google.com
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-11 09:16 EST
Nmap scan report for google.com (142.250.192.174)
Host is up (0.045s latency).
Other addresses for google.com (not scanned): 2404:6800:4002:816::200e
rDNS record for 142.250.192.174: del11s11-in-f14.1e100.net
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 8.22 seconds

┌──(kali㉿kali)-[~]
└─$ 
```



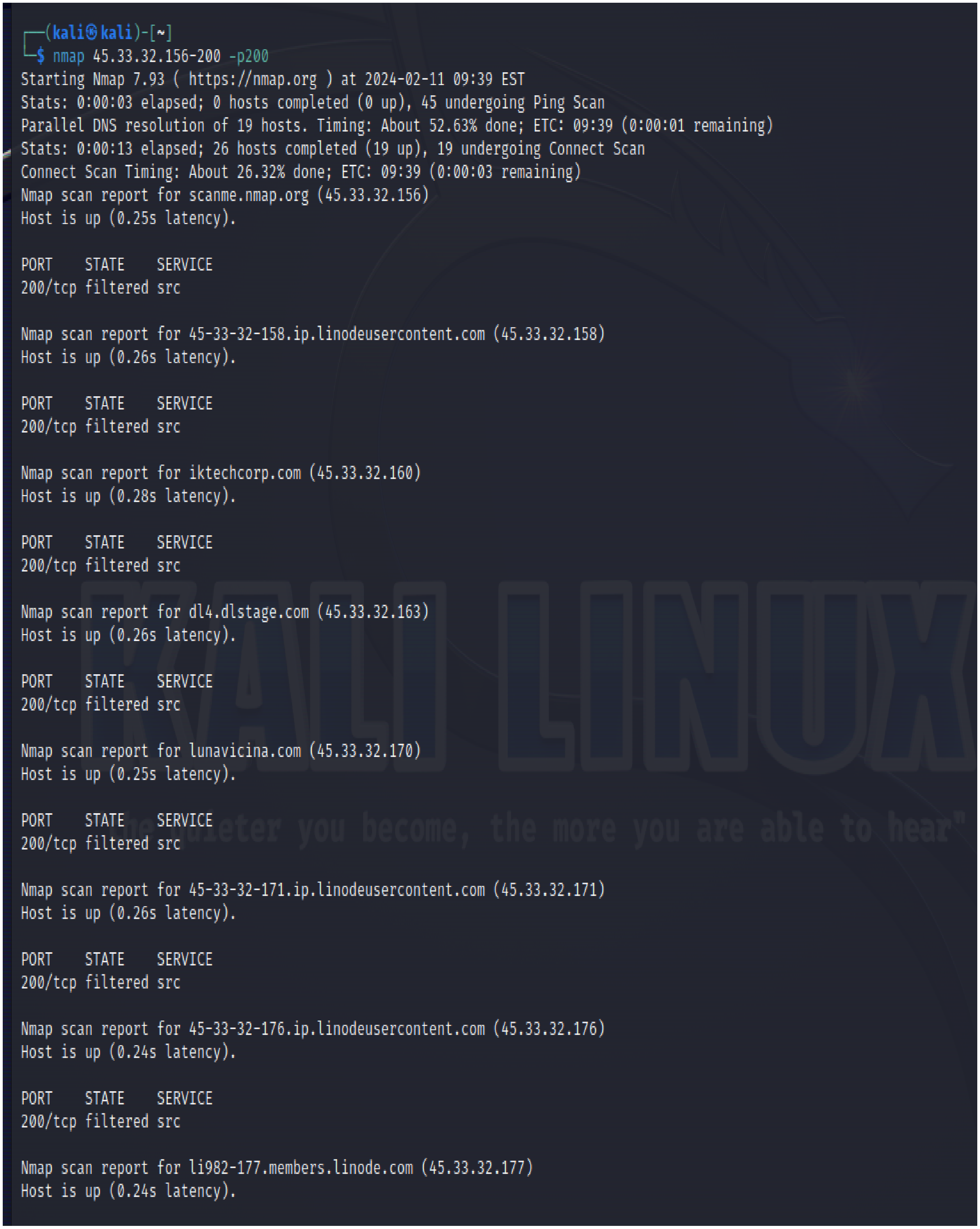
```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-11 09:19 EST
Nmap scan report for 192.168.1.1
Host is up (0.0053s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
52869/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 4.96 seconds
```

3. Host Discovery – **Traceout: sudo nmap –traceout 45.33.32.156**

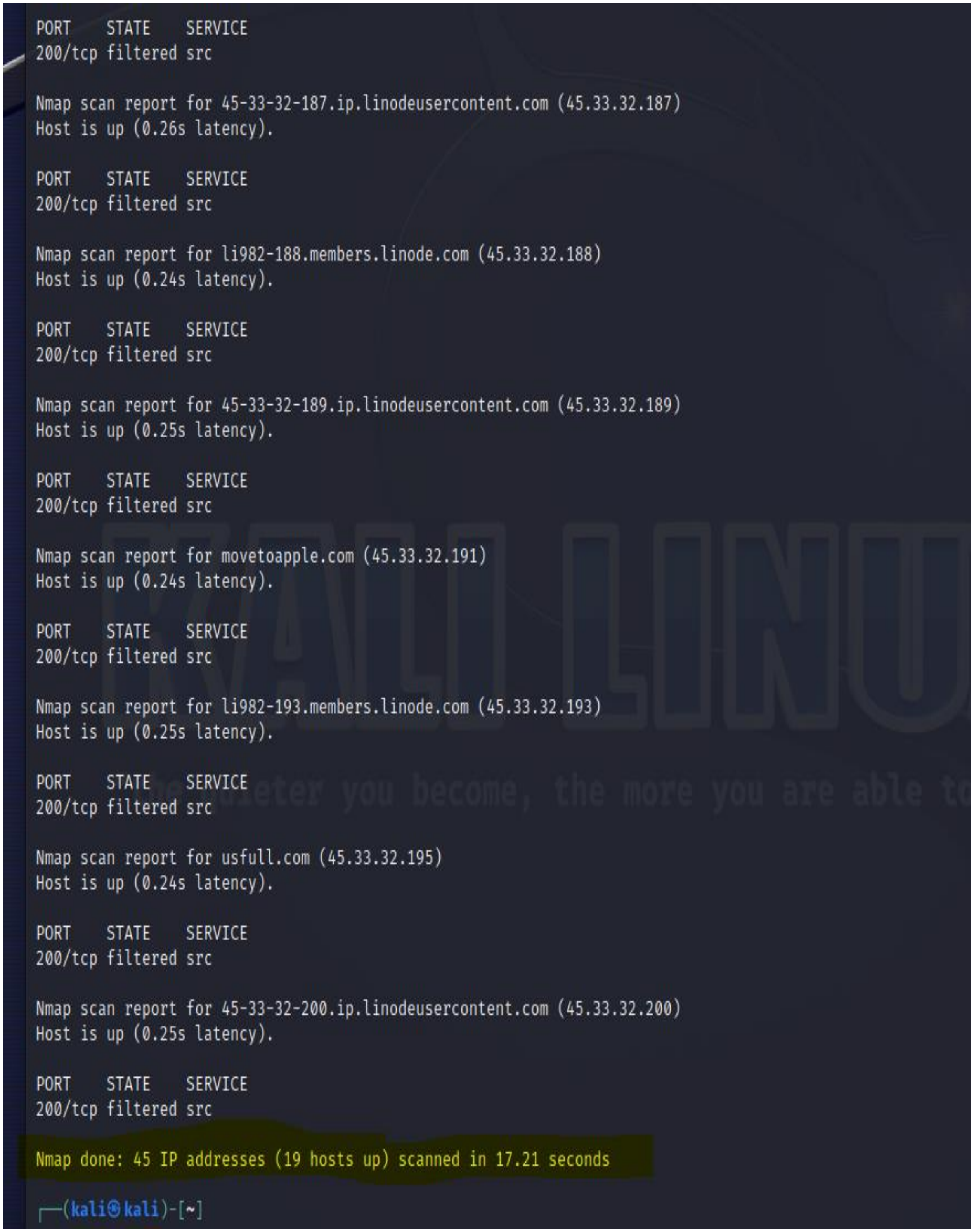


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap --traceroute 45.33.32.156
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-11 09:27 EST
Warning: 45.33.32.156 giving up on port because retransmission cap hit (10).
Stats: 0:01:35 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 21.35% done; ETC: 09:34 (0:05:54 remaining)
Stats: 0:02:37 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 22.32% done; ETC: 09:38 (0:09:10 remaining)
Stats: 0:03:43 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 23.22% done; ETC: 09:43 (0:12:17 remaining)
Stats: 0:10:13 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 26.41% done; ETC: 10:05 (0:28:31 remaining)
Stats: 0:10:17 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 26.45% done; ETC: 10:06 (0:28:39 remaining)
Stats: 0:10:19 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 26.46% done; ETC: 10:06 (0:28:43 remaining)
Stats: 0:10:20 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 26.47% done; ETC: 10:06 (0:28:45 remaining)
Stats: 0:10:21 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 26.48% done; ETC: 10:06 (0:28:47 remaining)
Stats: 0:10:23 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 26.49% done; ETC: 10:06 (0:28:52 remaining)
```

4. Port Specification: **nmap 45.33.32.156-200 -p200**

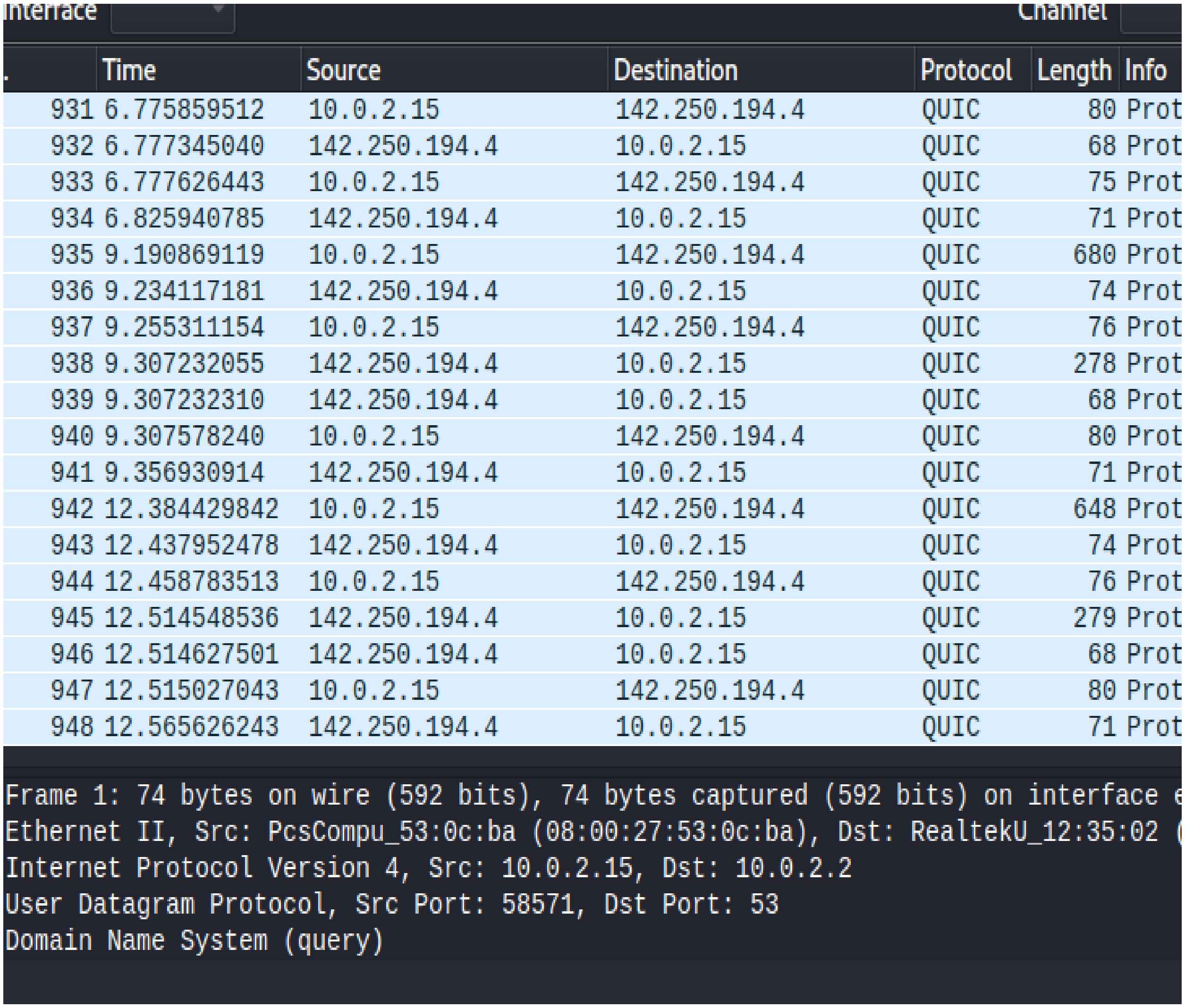


```
┌──(kali㉿kali)-[~]
└─$ nmap 45.33.32.156-200 -p200
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-11 09:39 EST
Stats: 0:00:03 elapsed; 0 hosts completed (0 up), 45 undergoing Ping Scan
Parallel DNS resolution of 19 hosts. Timing: About 52.63% done; ETC: 09:39 (0:00:01 remaining)
Stats: 0:00:13 elapsed; 26 hosts completed (19 up), 19 undergoing Connect Scan
Connect Scan Timing: About 26.32% done; ETC: 09:39 (0:00:03 remaining)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).

PORT    STATE    SERVICE
200/tcp filtered src

Nmap scan report for 45-33-32-158.ip.linodeusercontent.com (45.33.32.158)
Host is up (0.26s latency).

PORT    STATE    SERVICE
200/tcp filtered src

Nmap scan report for iktechcorp.com (45.33.32.160)
Host is up (0.28s latency).

PORT    STATE    SERVICE
200/tcp filtered src

Nmap scan report for dl4.dlstage.com (45.33.32.163)
Host is up (0.26s latency).

PORT    STATE    SERVICE
200/tcp filtered src

Nmap scan report for lunavicina.com (45.33.32.170)
Host is up (0.25s latency).

PORT    STATE    SERVICE
200/tcp filtered src

Nmap scan report for 45-33-32-171.ip.linodeusercontent.com (45.33.32.171)
Host is up (0.26s latency).

PORT    STATE    SERVICE
200/tcp filtered src

Nmap scan report for 45-33-32-176.ip.linodeusercontent.com (45.33.32.176)
Host is up (0.24s latency).

PORT    STATE    SERVICE
200/tcp filtered src

Nmap scan report for li982-177.members.linode.com (45.33.32.177)
Host is up (0.24s latency).
```



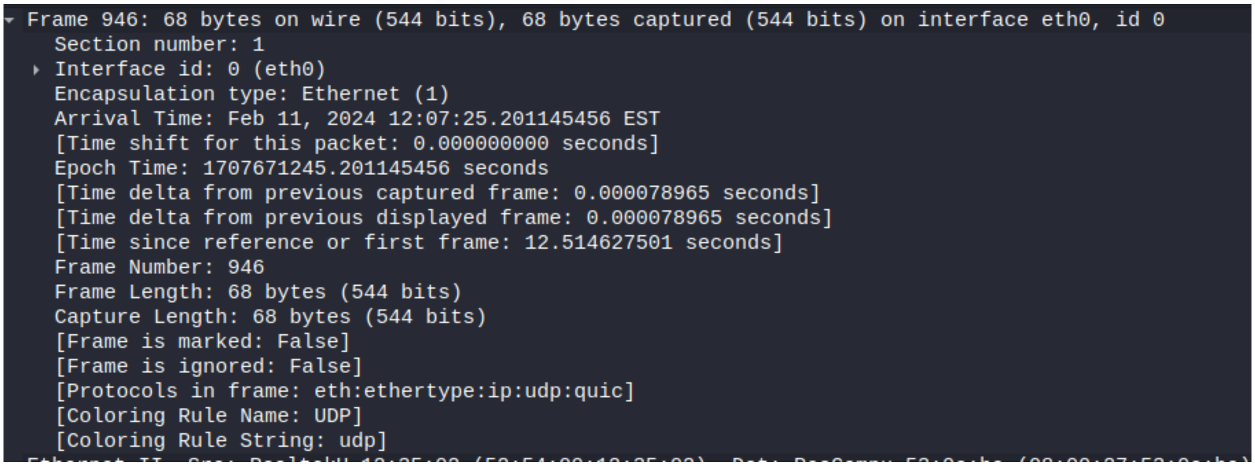
```
PORT    STATE    SERVICE
200/tcp filtered src

Nmap scan report for 45-33-32-187.ip.linodeusercontent.com (45.33.32.187)
Host is up (0.26s latency).

PORT    STATE    SERVICE
200/tcp filtered src

Nmap scan report for li982-188.members.linode.com (45.33.32.188)
Host is up (0.24s latency).

PORT    STATE    SERVICE
200/tcp filtered src

Nmap scan report for 45-33-32-189.ip.linodeusercontent.com (45.33.32.189)
Host is up (0.25s latency).

PORT    STATE    SERVICE
200/tcp filtered src

Nmap scan report for movetoapple.com (45.33.32.191)
Host is up (0.24s latency).

PORT    STATE    SERVICE
200/tcp filtered src

Nmap scan report for li982-193.members.linode.com (45.33.32.193)
Host is up (0.25s latency).

PORT    STATE    SERVICE
200/tcp filtered src

Nmap scan report for usfull.com (45.33.32.195)
Host is up (0.24s latency).

PORT    STATE    SERVICE
200/tcp filtered src

Nmap scan report for 45-33-32-200.ip.linodeusercontent.com (45.33.32.200)
Host is up (0.25s latency).

PORT    STATE    SERVICE
200/tcp filtered src

Nmap done: 45 IP addresses (19 hosts up) scanned in 17.21 seconds

┌──(kali㉿kali)-[~]
```

Exercise 2: Wireshark Exploration with Kali Linux

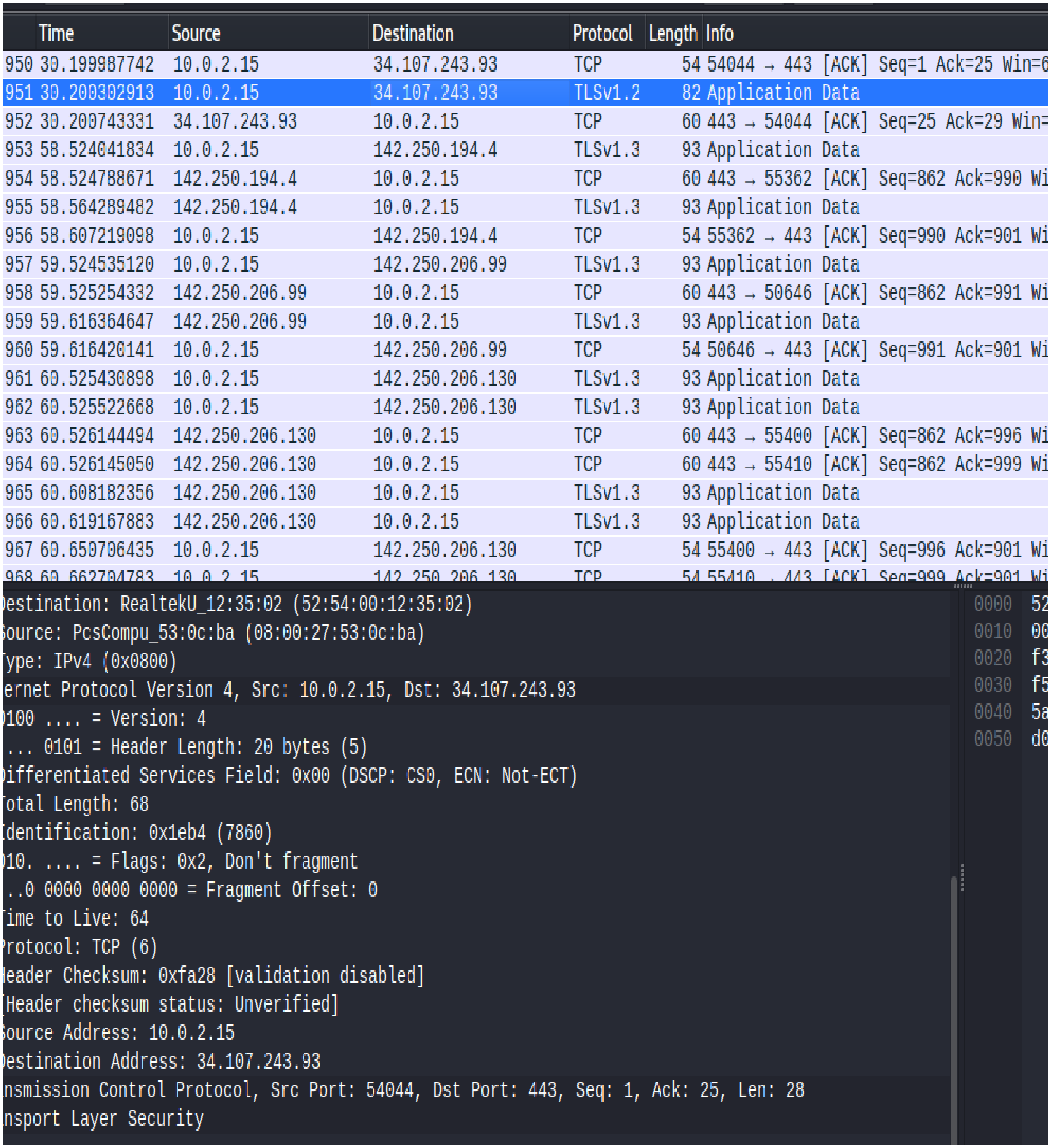


.	Time	Source	Destination	Protocol	Length	Info
931	6.775859512	10.0.2.15	142.250.194.4	QUIC	80	Prot
932	6.777345040	142.250.194.4	10.0.2.15	QUIC	68	Prot
933	6.777626443	10.0.2.15	142.250.194.4	QUIC	75	Prot
934	6.825940785	142.250.194.4	10.0.2.15	QUIC	71	Prot
935	9.190869119	10.0.2.15	142.250.194.4	QUIC	680	Prot
936	9.234117181	142.250.194.4	10.0.2.15	QUIC	74	Prot
937	9.255311154	10.0.2.15	142.250.194.4	QUIC	76	Prot
938	9.307232055	142.250.194.4	10.0.2.15	QUIC	278	Prot
939	9.307232310	142.250.194.4	10.0.2.15	QUIC	68	Prot
940	9.307578240	10.0.2.15	142.250.194.4	QUIC	80	Prot
941	9.356930914	142.250.194.4	10.0.2.15	QUIC	71	Prot
942	12.384429842	10.0.2.15	142.250.194.4	QUIC	648	Prot
943	12.437952478	142.250.194.4	10.0.2.15	QUIC	74	Prot
944	12.458783513	10.0.2.15	142.250.194.4	QUIC	76	Prot
945	12.514548536	142.250.194.4	10.0.2.15	QUIC	279	Prot
946	12.514627501	142.250.194.4	10.0.2.15	QUIC	68	Prot
947	12.515027043	10.0.2.15	142.250.194.4	QUIC	80	Prot
948	12.565626243	142.250.194.4	10.0.2.15	QUIC	71	Prot

```
Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface e
Ethernet II, Src: PcsCompu_53:0c:ba (08:00:27:53:0c:ba), Dst: RealtekU_12:35:02 (
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.2
User Datagram Protocol, Src Port: 58571, Dst Port: 53
Domain Name System (query)
```



```
▾ Frame 946: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface eth0, id 0
    Section number: 1
  ▸ Interface id: 0 (eth0)
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb 11, 2024 12:07:25.201145456 EST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1707671245.201145456 seconds
    [Time delta from previous captured frame: 0.000078965 seconds]
    [Time delta from previous displayed frame: 0.000078965 seconds]
    [Time since reference or first frame: 12.514627501 seconds]
    Frame Number: 946
    Frame Length: 68 bytes (544 bits)
    Capture Length: 68 bytes (544 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:quic]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
```



	Time	Source	Destination	Protocol	Length	Info
950	30.199987742	10.0.2.15	34.107.243.93	TCP	54	54044 → 443 [ACK] Seq=1 Ack=25 Win=6
951	30.200302913	10.0.2.15	34.107.243.93	TLSv1.2	82	Application Data
952	30.200743331	34.107.243.93	10.0.2.15	TCP	60	443 → 54044 [ACK] Seq=25 Ack=29 Win=
953	58.524041834	10.0.2.15	142.250.194.4	TLSv1.3	93	Application Data
954	58.524788671	142.250.194.4	10.0.2.15	TCP	60	443 → 55362 [ACK] Seq=862 Ack=990 Wi
955	58.564289482	142.250.194.4	10.0.2.15	TLSv1.3	93	Application Data
956	58.607219098	10.0.2.15	142.250.194.4	TCP	54	55362 → 443 [ACK] Seq=990 Ack=901 Wi
957	59.524535120	10.0.2.15	142.250.206.99	TLSv1.3	93	Application Data
958	59.525254332	142.250.206.99	10.0.2.15	TCP	60	443 → 50646 [ACK] Seq=862 Ack=991 Wi
959	59.616364647	142.250.206.99	10.0.2.15	TLSv1.3	93	Application Data
960	59.616420141	10.0.2.15	142.250.206.99	TCP	54	50646 → 443 [ACK] Seq=991 Ack=901 Wi
961	60.525430898	10.0.2.15	142.250.206.130	TLSv1.3	93	Application Data
962	60.525522668	10.0.2.15	142.250.206.130	TLSv1.3	93	Application Data
963	60.526144494	142.250.206.130	10.0.2.15	TCP	60	443 → 55400 [ACK] Seq=862 Ack=996 Wi
964	60.526145050	142.250.206.130	10.0.2.15	TCP	60	443 → 55410 [ACK] Seq=862 Ack=999 Wi
965	60.608182356	142.250.206.130	10.0.2.15	TLSv1.3	93	Application Data
966	60.619167883	142.250.206.130	10.0.2.15	TLSv1.3	93	Application Data
967	60.650706435	10.0.2.15	142.250.206.130	TCP	54	55400 → 443 [ACK] Seq=996 Ack=901 Wi
968	60.662704783	10.0.2.15	142.250.206.130	TCP	54	55410 → 443 [ACK] Seq=999 Ack=901 Wi

```
estination: RealtekU_12:35:02 (52:54:00:12:35:02)
ource: PcsCompu_53:0c:ba (08:00:27:53:0c:ba)
ype: IPv4 (0x0800)
ernet Protocol Version 4, Src: 10.0.2.15, Dst: 34.107.243.93
100 .... = Version: 4
... 0101 = Header Length: 20 bytes (5)
ifferentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
otal Length: 68
dentification: 0x1eb4 (7860)
10. .... = Flags: 0x2, Don't fragment
..0 0000 0000 0000 = Fragment Offset: 0
ime to Live: 64
rotocol: TCP (6)
eader Checksum: 0xfa28 [validation disabled]
[Header checksum status: Unverified]
ource Address: 10.0.2.15
estination Address: 34.107.243.93
nsmission Control Protocol, Src Port: 54044, Dst Port: 443, Seq: 1, Ack: 25, Len: 28
nsport Layer Security
```

```
0000  52
0010  00
0020  f3
0030  f5
0040  5a
0050  d0
```