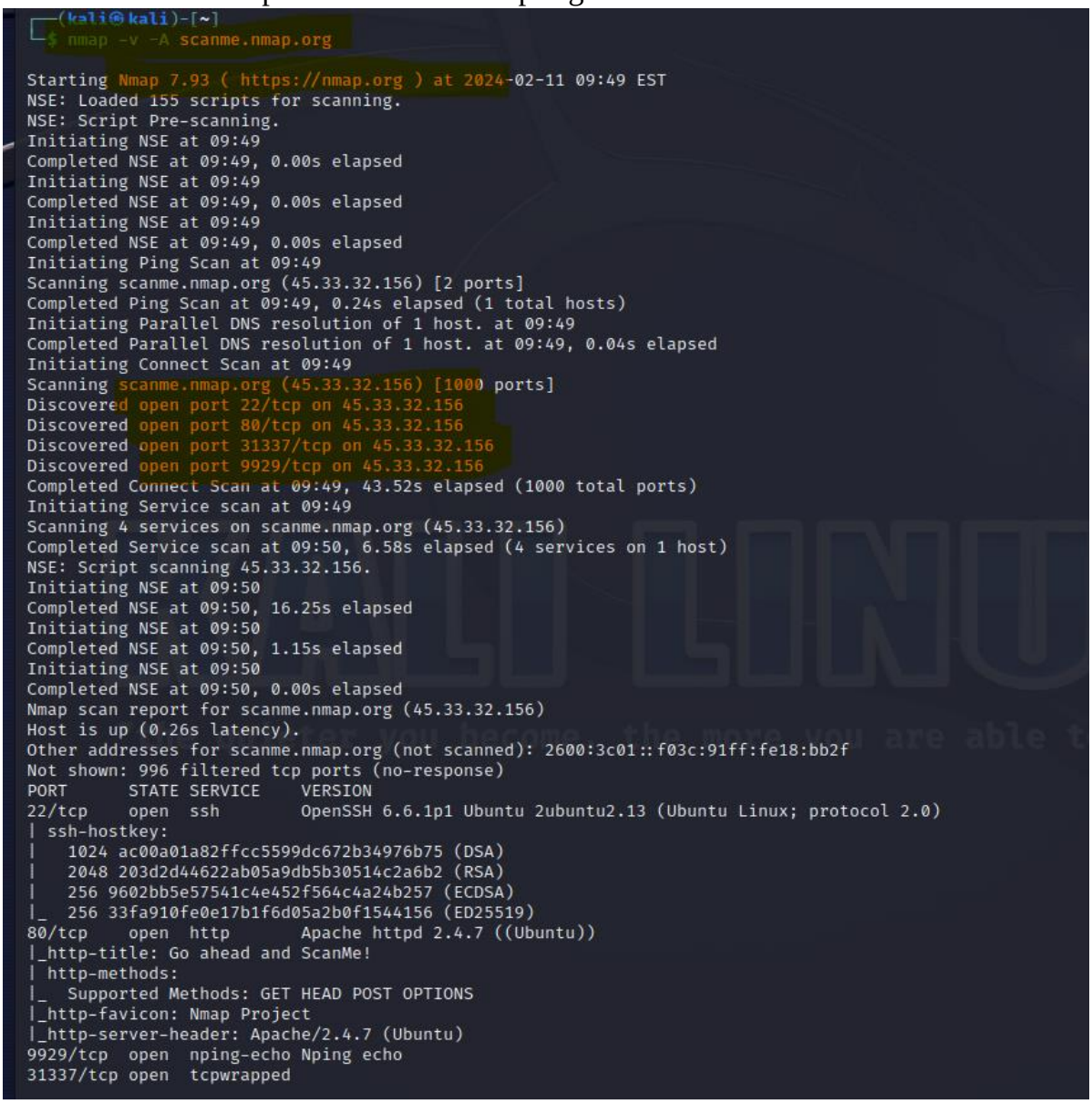
Network Security

Roll: MC233104
Name: Saif Md. Zulker Nein Chowdhury
Mobile: 01672947867
Email: julker@gmail.com

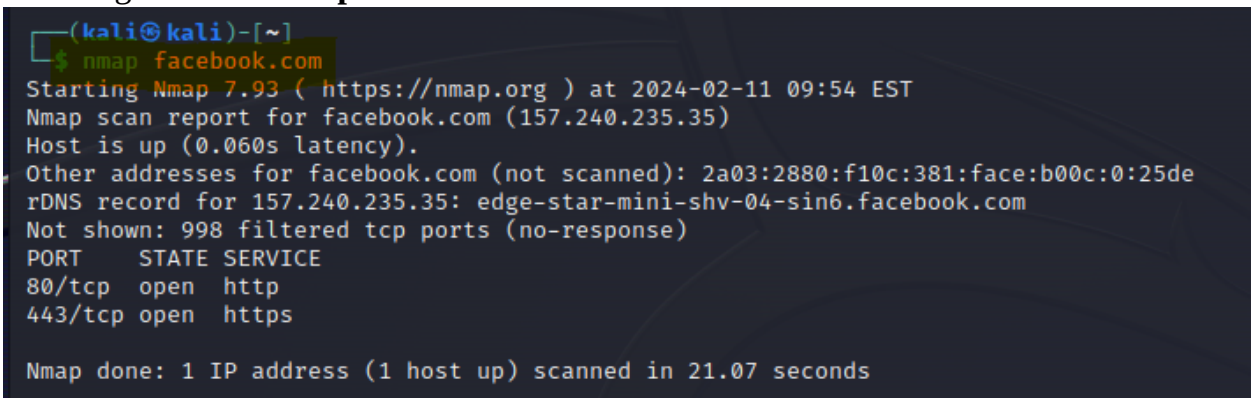
Exercise 1: Nmap Practice

In the following exercise, I have used these commands.

1. Version Check: nmap -v -A scanme.nmap.org



2. Scanning Website: **nmap facebook.com**



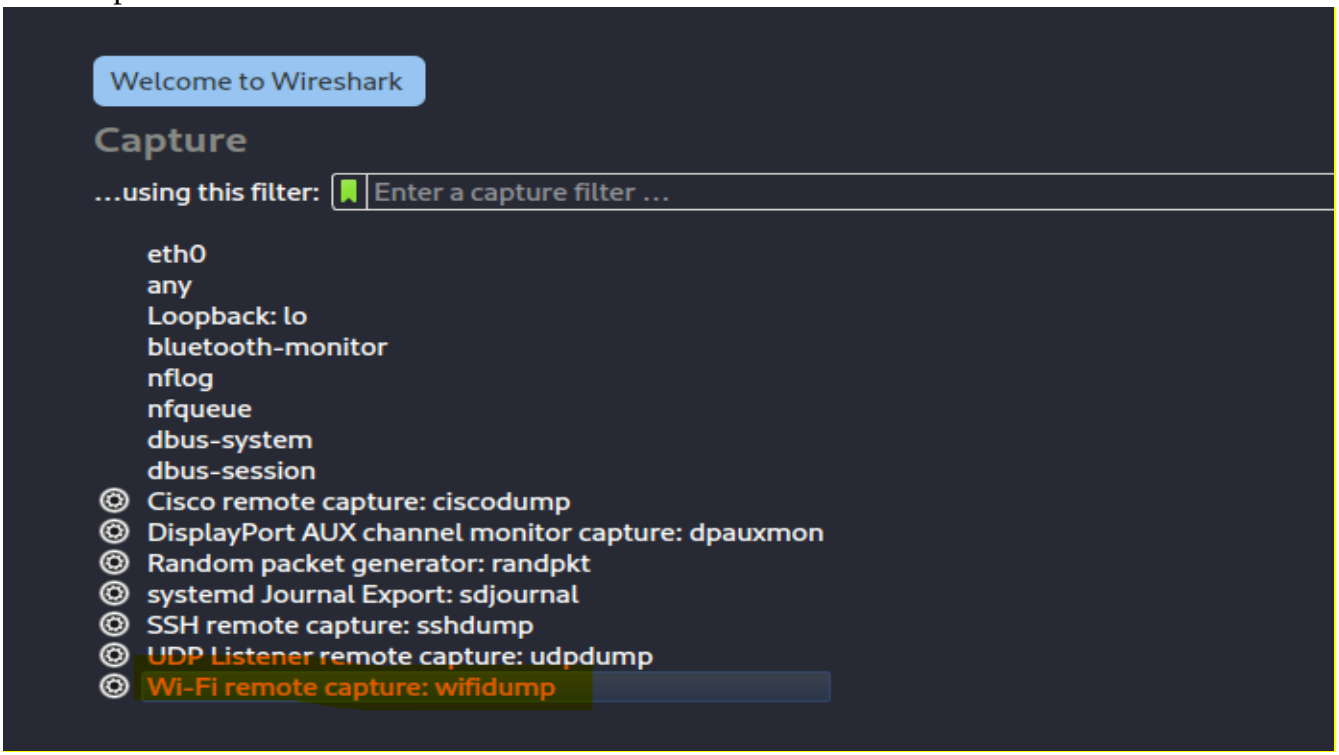
3. Host Discovery – **Traceout: sudo nmap –traceout 51.23.48.15**

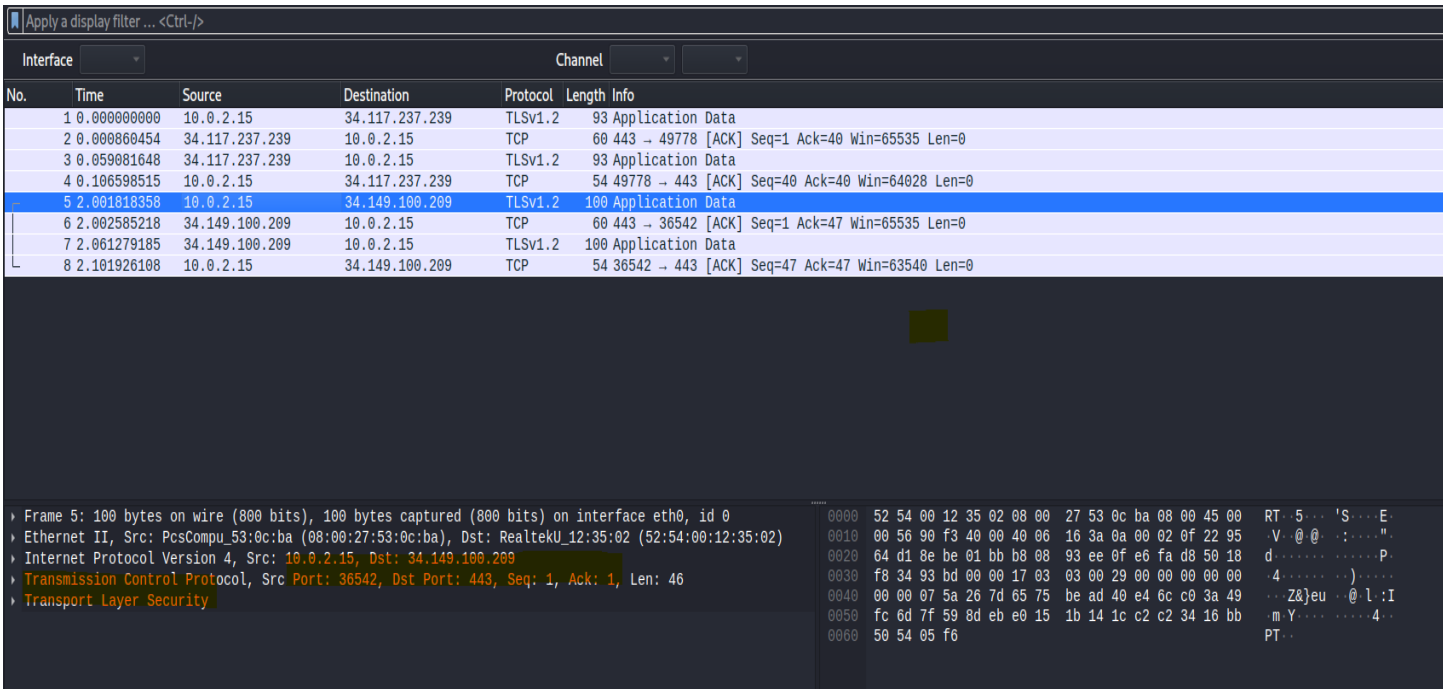
4. Port Specification: **nmap 51.23.48.15 -p443**

```
┌──(kali㉿kali)-[~]
└─$ nmap 51.23.48.15 -p300
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-11 09:59 EST
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 3.06 seconds

┌──(kali㉿kali)-[~]
└─$ nmap 51.23.48.15 -p80
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-11 09:59 EST
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 3.04 seconds

┌──(kali㉿kali)-[~]
└─$ nmap 51.23.48.15 -p80 -Pn
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-11 09:59 EST
Nmap scan report for 51.23.48.15
Host is up.

PORT   STATE    SERVICE
80/tcp filtered http

Nmap done: 1 IP address (1 host up) scanned in 2.11 seconds

┌──(kali㉿kali)-[~]
└─$
```

Exercise 2: Wireshirk Practice

Wifi Capture:




Apply a display filter ... <Ctrl-/>
Interface
Channel
No. Time Source Destination Protocol Length Info
1 0.000000000 10.0.2.15 34.117.237.239 TLSv1.2 93 Application Data
2 0.000860454 34.117.237.239 10.0.2.15 TCP 60 443 → 49778 [ACK] Seq=1 Ack=40 Win=65535 Len=0
3 0.059081648 34.117.237.239 10.0.2.15 TLSv1.2 93 Application Data
4 0.106598515 10.0.2.15 34.117.237.239 TCP 54 49778 → 443 [ACK] Seq=40 Ack=40 Win=64028 Len=0
5 2.001818358 10.0.2.15 34.149.100.209 TLSv1.2 100 Application Data
6 2.002585218 34.149.100.209 10.0.2.15 TCP 60 443 → 36542 [ACK] Seq=1 Ack=47 Win=65535 Len=0
7 2.061279185 34.149.100.209 10.0.2.15 TLSv1.2 100 Application Data
8 2.101926108 10.0.2.15 34.149.100.209 TCP 54 36542 → 443 [ACK] Seq=47 Ack=47 Win=63540 Len=0
Frame 5: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_53:0c:ba (08:00:27:53:0c:ba), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 34.149.100.209
Transmission Control Protocol, Src Port: 36542, Dst Port: 443, Seq: 1, Ack: 1, Len: 46
Transport Layer Security
0000 52 54 00 12 35 02 08 00 27 53 0c ba 08 00 45 00
0010 00 56 90 f3 40 00 40 06 16 3a 0a 00 02 0f 22 95
0020 64 d1 8e be 01 bb b8 08 93 ee 0f e6 fa d8 50 18
0030 f8 34 93 bd 00 00 17 03 03 00 29 00 00 00 00 00
0040 00 00 07 5a 26 7d 65 75 be ad 40 e4 6c c0 3a 49
0050 fc 6d 7f 59 8d eb e0 15 1b 14 1c c2 c2 34 16 bb
0060 50 54 05 f6