Network Lab: Assignment #2

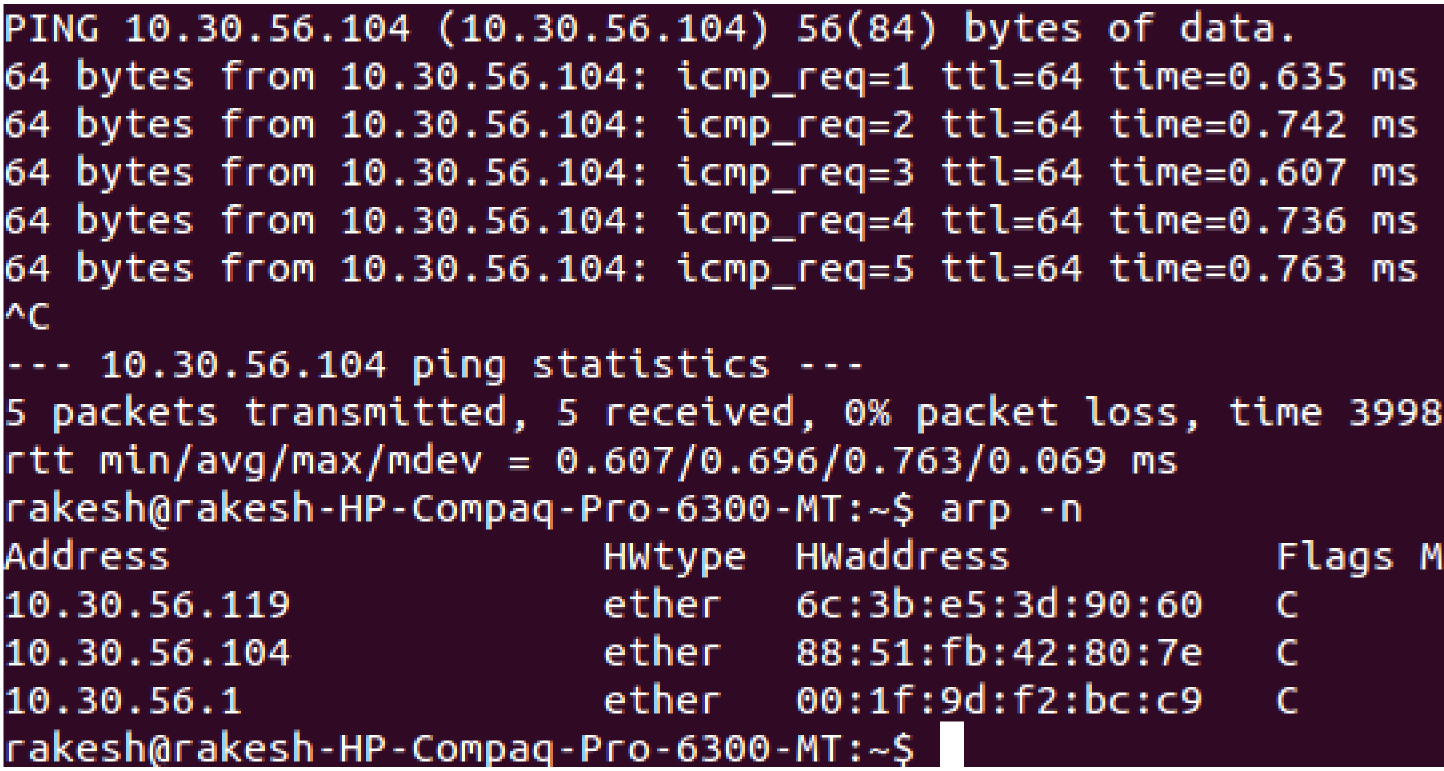
Rakesh K T

Contents

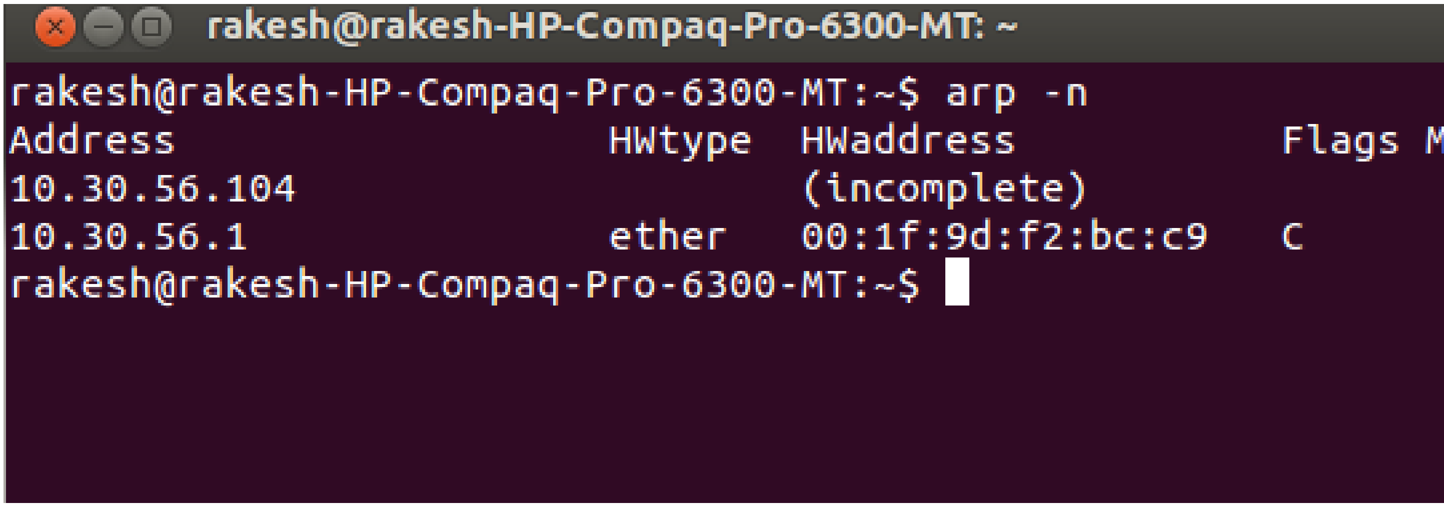
Problem 1

1.Install wireshark .Ping an IP address and sniff packets using wireshark. Make sure to empty the arp table before pinging and save the file.

Commands:
$ arp -n ——To display the arp table.
$ arp -a -d IP address ——To remove the IP address from arp table.

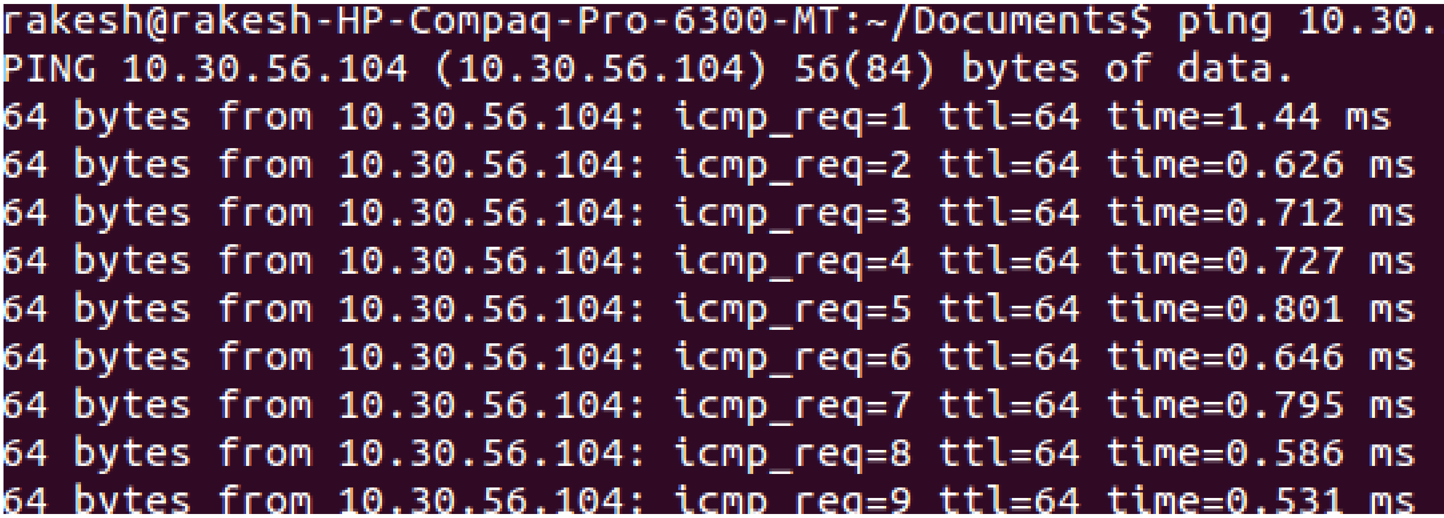


```
PING 10.30.56.104 (10.30.56.104) 56(84) bytes of data.
64 bytes from 10.30.56.104: icmp_req=1 ttl=64 time=0.635 ms
64 bytes from 10.30.56.104: icmp_req=2 ttl=64 time=0.742 ms
64 bytes from 10.30.56.104: icmp_req=3 ttl=64 time=0.607 ms
64 bytes from 10.30.56.104: icmp_req=4 ttl=64 time=0.736 ms
64 bytes from 10.30.56.104: icmp_req=5 ttl=64 time=0.763 ms
^C
--- 10.30.56.104 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3998
rtt min/avg/max/mdev = 0.607/0.696/0.763/0.069 ms
rakesh@rakesh-HP-Compaq-Pro-6300-MT:~$ arp -n
Address                  HWtype  HWaddress           Flags M
10.30.56.119             ether   6c:3b:e5:3d:90:60   C
10.30.56.104             ether   88:51:fb:42:80:7e   C
10.30.56.1               ether   00:1f:9d:f2:bc:c9   C
rakesh@rakesh-HP-Compaq-Pro-6300-MT:~$
```



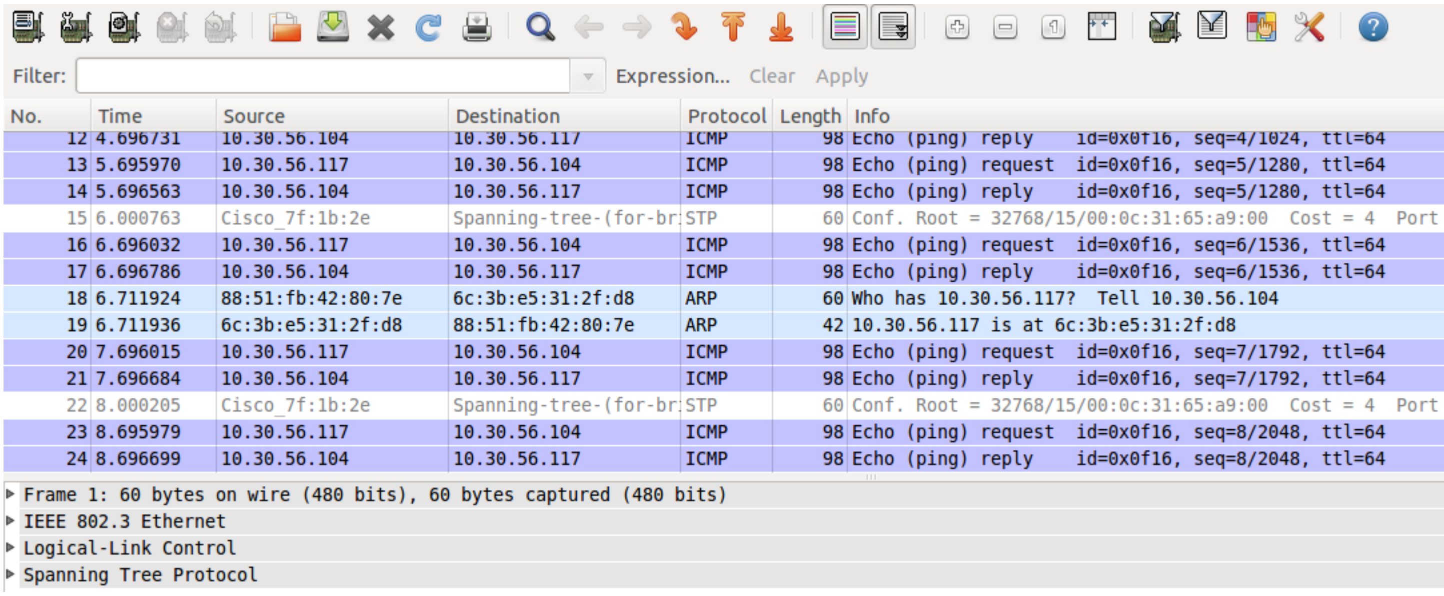
```
rakesh@rakesh-HP-Compaq-Pro-6300-MT:~$ arp -n
Address                  HWtype  HWaddress           Flags M
10.30.56.104                     (incomplete)
10.30.56.1               ether   00:1f:9d:f2:bc:c9   C
rakesh@rakesh-HP-Compaq-Pro-6300-MT:~$
```

$ sudo wireshark ———-Open wireshark
ping IP address



```
rakesh@rakesh-HP-Compaq-Pro-6300-MT:~/Documents$ ping 10.30.
PING 10.30.56.104 (10.30.56.104) 56(84) bytes of data.
64 bytes from 10.30.56.104: icmp_req=1 ttl=64 time=1.44 ms
64 bytes from 10.30.56.104: icmp_req=2 ttl=64 time=0.626 ms
64 bytes from 10.30.56.104: icmp_req=3 ttl=64 time=0.712 ms
64 bytes from 10.30.56.104: icmp_req=4 ttl=64 time=0.727 ms
64 bytes from 10.30.56.104: icmp_req=5 ttl=64 time=0.801 ms
64 bytes from 10.30.56.104: icmp_req=6 ttl=64 time=0.646 ms
64 bytes from 10.30.56.104: icmp_req=7 ttl=64 time=0.795 ms
64 bytes from 10.30.56.104: icmp_req=8 ttl=64 time=0.586 ms
64 bytes from 10.30.56.104: icmp_req=9 ttl=64 time=0.531 ms
```

Captured packets using wireshark



No.	Time	Source	Destination	Protocol	Length	Info
12	4.696731	10.30.56.104	10.30.56.117	ICMP	98	Echo (ping) reply id=0x0f16, seq=4/1024, ttl=64
13	5.695970	10.30.56.117	10.30.56.104	ICMP	98	Echo (ping) request id=0x0f16, seq=5/1280, ttl=64
14	5.696563	10.30.56.104	10.30.56.117	ICMP	98	Echo (ping) reply id=0x0f16, seq=5/1280, ttl=64
15	6.000763	Cisco_7f:1b:2e	Spanning-tree-(for-br	STP	60	Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port
16	6.696032	10.30.56.117	10.30.56.104	ICMP	98	Echo (ping) request id=0x0f16, seq=6/1536, ttl=64
17	6.696786	10.30.56.104	10.30.56.117	ICMP	98	Echo (ping) reply id=0x0f16, seq=6/1536, ttl=64
18	6.711924	88:51:fb:42:80:7e	6c:3b:e5:31:2f:d8	ARP	60	Who has 10.30.56.117? Tell 10.30.56.104
19	6.711936	6c:3b:e5:31:2f:d8	88:51:fb:42:80:7e	ARP	42	10.30.56.117 is at 6c:3b:e5:31:2f:d8
20	7.696015	10.30.56.117	10.30.56.104	ICMP	98	Echo (ping) request id=0x0f16, seq=7/1792, ttl=64
21	7.696684	10.30.56.104	10.30.56.117	ICMP	98	Echo (ping) reply id=0x0f16, seq=7/1792, ttl=64
22	8.000205	Cisco_7f:1b:2e	Spanning-tree-(for-br	STP	60	Conf. Root = 32768/15/00:0c:31:65:a9:00 Cost = 4 Port
23	8.695979	10.30.56.117	10.30.56.104	ICMP	98	Echo (ping) request id=0x0f16, seq=8/2048, ttl=64
24	8.696699	10.30.56.104	10.30.56.117	ICMP	98	Echo (ping) reply id=0x0f16, seq=8/2048, ttl=64

```
▶ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
▶ IEEE 802.3 Ethernet
▶ Logical-Link Control
▶ Spanning Tree Protocol
```

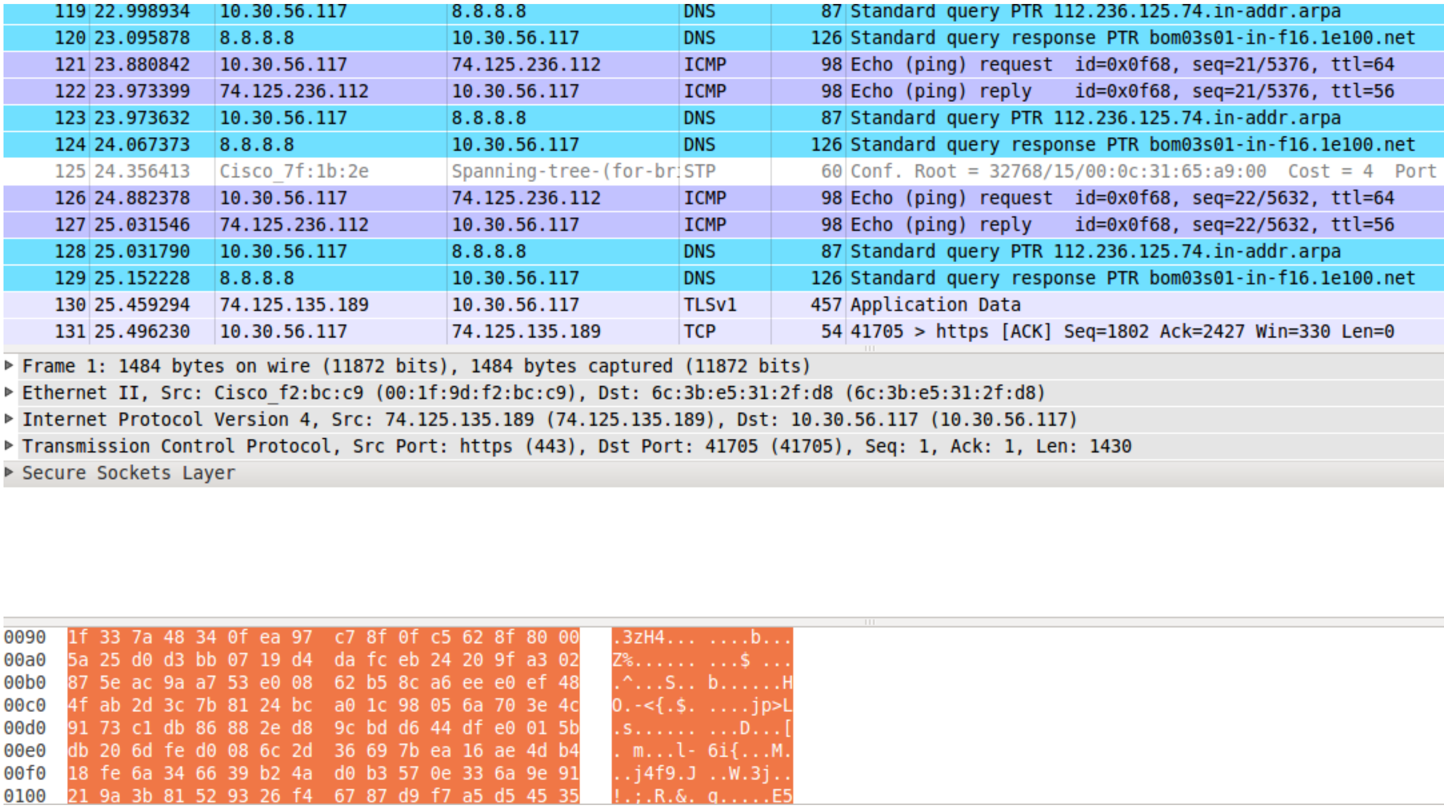
Problem 2

2.Using sniffer capture analyse the output and save the file when pinging www.google.com

Launch wireshark and capture data.

Command:Ping www.google.com

Captured packets using wireshark



```
119 22.998934 10.30.56.117     8.8.8.8                DNS    87 Standard query PTR 112.236.125.74.in-addr.arpa
120 23.095878 8.8.8.8          10.30.56.117           DNS   126 Standard query response PTR bom03s01-in-f16.1e100.net
121 23.880842 10.30.56.117     74.125.236.112         ICMP   98 Echo (ping) request  id=0x0f68, seq=21/5376, ttl=64
122 23.973399 74.125.236.112   10.30.56.117           ICMP   98 Echo (ping) reply    id=0x0f68, seq=21/5376, ttl=56
123 23.973632 10.30.56.117     8.8.8.8                DNS    87 Standard query PTR 112.236.125.74.in-addr.arpa
124 24.067373 8.8.8.8          10.30.56.117           DNS   126 Standard query response PTR bom03s01-in-f16.1e100.net
125 24.356413 Cisco_7f:1b:2e   Spanning-tree-(for-br: STP    60 Conf. Root = 32768/15/00:0c:31:65:a9:00  Cost = 4  Port
126 24.882378 10.30.56.117     74.125.236.112         ICMP   98 Echo (ping) request  id=0x0f68, seq=22/5632, ttl=64
127 25.031546 74.125.236.112   10.30.56.117           ICMP   98 Echo (ping) reply    id=0x0f68, seq=22/5632, ttl=56
128 25.031790 10.30.56.117     8.8.8.8                DNS    87 Standard query PTR 112.236.125.74.in-addr.arpa
129 25.152228 8.8.8.8          10.30.56.117           DNS   126 Standard query response PTR bom03s01-in-f16.1e100.net
130 25.459294 74.125.135.189   10.30.56.117           TLSv1 457 Application Data
131 25.496230 10.30.56.117     74.125.135.189         TCP    54 41705 > https [ACK] Seq=1802 Ack=2427 Win=330 Len=0
```

```
▶ Frame 1: 1484 bytes on wire (11872 bits), 1484 bytes captured (11872 bits)
▶ Ethernet II, Src: Cisco_f2:bc:c9 (00:1f:9d:f2:bc:c9), Dst: 6c:3b:e5:31:2f:d8 (6c:3b:e5:31:2f:d8)
▶ Internet Protocol Version 4, Src: 74.125.135.189 (74.125.135.189), Dst: 10.30.56.117 (10.30.56.117)
▶ Transmission Control Protocol, Src Port: https (443), Dst Port: 41705 (41705), Seq: 1, Ack: 1, Len: 1430
▶ Secure Sockets Layer
```

```
0090  1f 33 7a 48 34 0f ea 97  c7 8f 0f c5 62 8f 80 00   .3zH4... ....b...
00a0  5a 25 d0 d3 bb 07 19 d4  da fc eb 24 20 9f a3 02   Z%...... ...$ ...
00b0  87 5e ac 9a a7 53 e0 08  62 b5 8c a6 ee e0 ef 48   .^...S.. b......H
00c0  4f ab 2d 3c 7b 81 24 bc  a0 1c 98 05 6a 70 3e 4c   O.-<{.$. ....jp>L
00d0  91 73 c1 db 86 88 2e d8  9c bd d6 44 df e0 01 5b   .s...... ...D...[
00e0  db 20 6d fe d0 08 6c 2d  36 69 7b ea 16 ae 4d b4   . m...l- 6i{...M.
00f0  18 fe 6a 34 66 39 b2 4a  d0 b3 57 0e 33 6a 9e 91   ..j4f9.J ..W.3j..
0100  21 9a 3b 81 52 93 26 f4  67 87 d9 f7 a5 d5 45 35   !.;.R.&. g.....E5
```