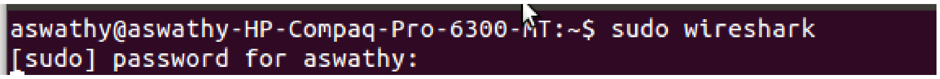
Networking Lab: Assignment #2

Aswathy Mohan S

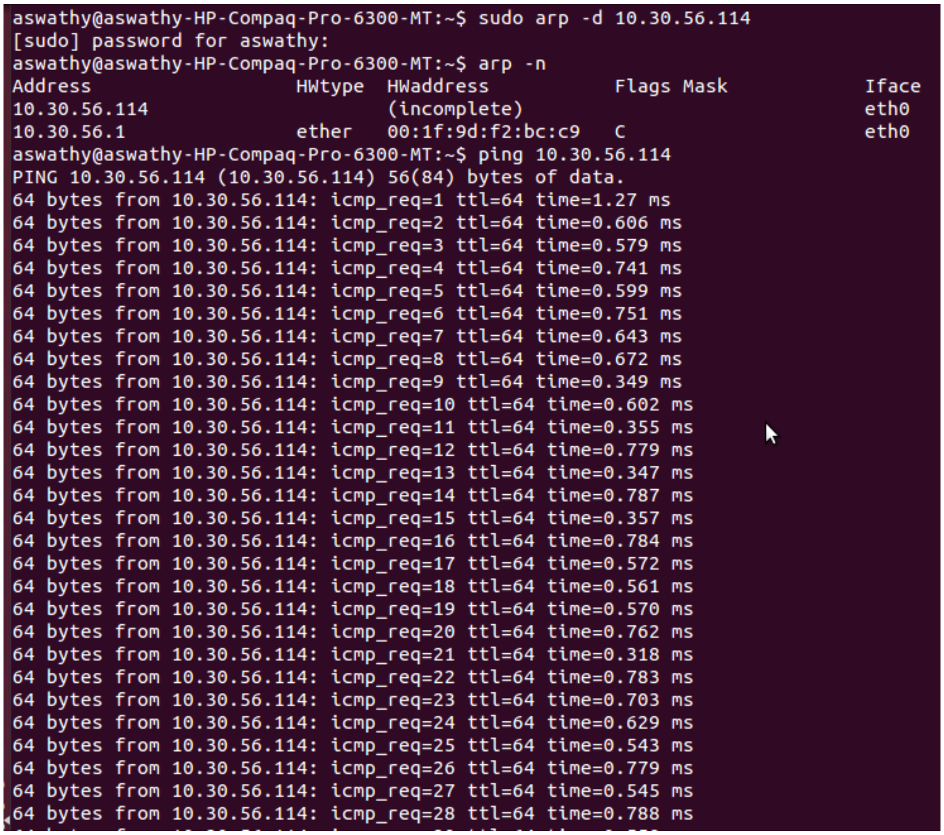
Contents

Problem 1

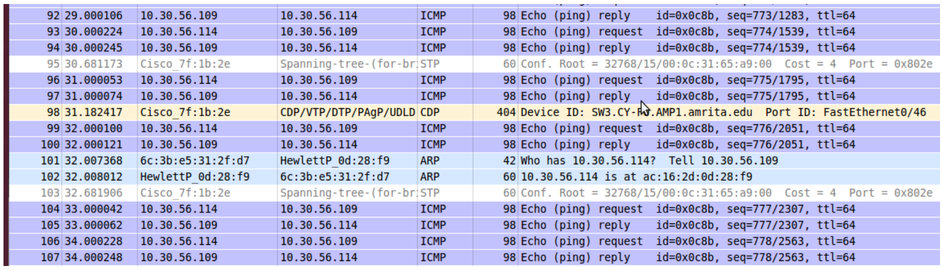
Ping another IP address and do sniffer capture using wireshark
Answer: Wireshark is a free and opensource packet analyzer. Deleted hardware address of 10.30.56.114 from arp table using sudo arp -d 10.30.56.114 and then listed the details in the arp table using arp -n.
sudo wireshark
sudo arp -d 10.30.56.114
arp -n
ping 10.30.56.114



```
aswathy@aswathy-HP-Compaq-Pro-6300-MT:~$ sudo wireshark
[sudo] password for aswathy:
```



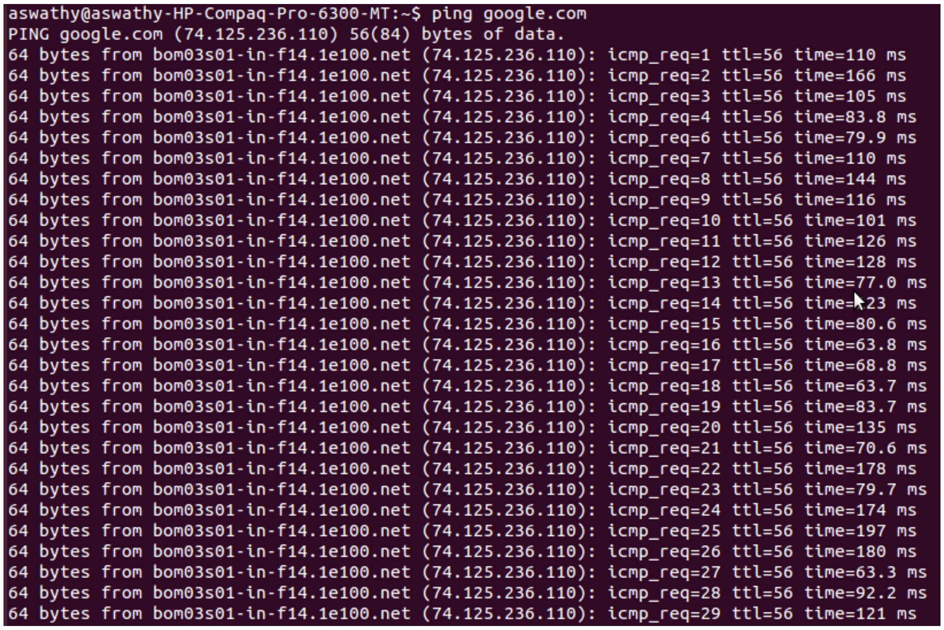
```
aswathy@aswathy-HP-Compaq-Pro-6300-MT:~$ sudo arp -d 10.30.56.114
[sudo] password for aswathy:
aswathy@aswathy-HP-Compaq-Pro-6300-MT:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.30.56.114                     (incomplete)                              eth0
10.30.56.1               ether   00:1f:9d:f2:bc:c9   C                     eth0
aswathy@aswathy-HP-Compaq-Pro-6300-MT:~$ ping 10.30.56.114
PING 10.30.56.114 (10.30.56.114) 56(84) bytes of data.
64 bytes from 10.30.56.114: icmp_req=1 ttl=64 time=1.27 ms
64 bytes from 10.30.56.114: icmp_req=2 ttl=64 time=0.606 ms
64 bytes from 10.30.56.114: icmp_req=3 ttl=64 time=0.579 ms
64 bytes from 10.30.56.114: icmp_req=4 ttl=64 time=0.741 ms
64 bytes from 10.30.56.114: icmp_req=5 ttl=64 time=0.599 ms
64 bytes from 10.30.56.114: icmp_req=6 ttl=64 time=0.751 ms
64 bytes from 10.30.56.114: icmp_req=7 ttl=64 time=0.643 ms
64 bytes from 10.30.56.114: icmp_req=8 ttl=64 time=0.672 ms
64 bytes from 10.30.56.114: icmp_req=9 ttl=64 time=0.349 ms
64 bytes from 10.30.56.114: icmp_req=10 ttl=64 time=0.602 ms
64 bytes from 10.30.56.114: icmp_req=11 ttl=64 time=0.355 ms
64 bytes from 10.30.56.114: icmp_req=12 ttl=64 time=0.779 ms
64 bytes from 10.30.56.114: icmp_req=13 ttl=64 time=0.347 ms
64 bytes from 10.30.56.114: icmp_req=14 ttl=64 time=0.787 ms
64 bytes from 10.30.56.114: icmp_req=15 ttl=64 time=0.357 ms
64 bytes from 10.30.56.114: icmp_req=16 ttl=64 time=0.784 ms
64 bytes from 10.30.56.114: icmp_req=17 ttl=64 time=0.572 ms
64 bytes from 10.30.56.114: icmp_req=18 ttl=64 time=0.561 ms
64 bytes from 10.30.56.114: icmp_req=19 ttl=64 time=0.570 ms
64 bytes from 10.30.56.114: icmp_req=20 ttl=64 time=0.762 ms
64 bytes from 10.30.56.114: icmp_req=21 ttl=64 time=0.318 ms
64 bytes from 10.30.56.114: icmp_req=22 ttl=64 time=0.783 ms
64 bytes from 10.30.56.114: icmp_req=23 ttl=64 time=0.703 ms
64 bytes from 10.30.56.114: icmp_req=24 ttl=64 time=0.629 ms
64 bytes from 10.30.56.114: icmp_req=25 ttl=64 time=0.543 ms
64 bytes from 10.30.56.114: icmp_req=26 ttl=64 time=0.779 ms
64 bytes from 10.30.56.114: icmp_req=27 ttl=64 time=0.545 ms
64 bytes from 10.30.56.114: icmp_req=28 ttl=64 time=0.788 ms
```



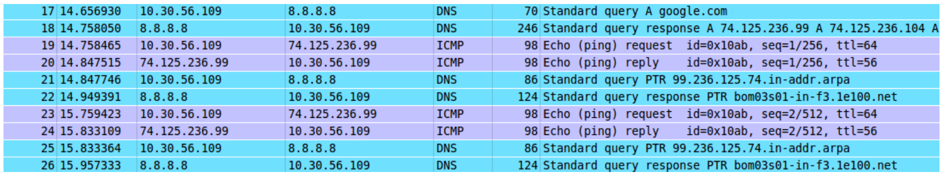
```
 92 29.000106 10.30.56.109       10.30.56.114          ICMP   98 Echo (ping) reply    id=0x0c8b, seq=773/1283, ttl=64
 93 30.000224 10.30.56.114       10.30.56.109          ICMP   98 Echo (ping) request  id=0x0c8b, seq=774/1539, ttl=64
 94 30.000245 10.30.56.109       10.30.56.114          ICMP   98 Echo (ping) reply    id=0x0c8b, seq=774/1539, ttl=64
 95 30.681173 Cisco_7f:1b:2e     Spanning-tree-(for-br STP    60 Conf. Root = 32768/15/00:0c:31:65:a9:00  Cost = 4  Port = 0x802e
 96 31.000053 10.30.56.114       10.30.56.109          ICMP   98 Echo (ping) request  id=0x0c8b, seq=775/1795, ttl=64
 97 31.000074 10.30.56.109       10.30.56.114          ICMP   98 Echo (ping) reply    id=0x0c8b, seq=775/1795, ttl=64
 98 31.182417 Cisco_7f:1b:2e     CDP/VTP/DTP/PAgP/UDLD CDP   404 Device ID: SW3.CY-AV.AMP1.amrita.edu  Port ID: FastEthernet0/46
 99 32.000100 10.30.56.114       10.30.56.109          ICMP   98 Echo (ping) request  id=0x0c8b, seq=776/2051, ttl=64
100 32.000121 10.30.56.109       10.30.56.114          ICMP   98 Echo (ping) reply    id=0x0c8b, seq=776/2051, ttl=64
101 32.007368 6c:3b:e5:31:2f:d7  HewlettP_0d:28:f9     ARP    42 Who has 10.30.56.114?  Tell 10.30.56.109
102 32.008012 HewlettP_0d:28:f9  6c:3b:e5:31:2f:d7     ARP    60 10.30.56.114 is at ac:16:2d:0d:28:f9
103 32.681906 Cisco_7f:1b:2e     Spanning-tree-(for-br STP    60 Conf. Root = 32768/15/00:0c:31:65:a9:00  Cost = 4  Port = 0x802e
104 33.000042 10.30.56.114       10.30.56.109          ICMP   98 Echo (ping) request  id=0x0c8b, seq=777/2307, ttl=64
105 33.000062 10.30.56.109       10.30.56.114          ICMP   98 Echo (ping) reply    id=0x0c8b, seq=777/2307, ttl=64
106 34.000228 10.30.56.114       10.30.56.109          ICMP   98 Echo (ping) request  id=0x0c8b, seq=778/2563, ttl=64
107 34.000248 10.30.56.109       10.30.56.114          ICMP   98 Echo (ping) reply    id=0x0c8b, seq=778/2563, ttl=64
```

Problem 2

ping google.com and do sniffer capture using wireshark
ping google.com



```
aswathy@aswathy-HP-Compaq-Pro-6300-MT:~$ ping google.com
PING google.com (74.125.236.110) 56(84) bytes of data.
64 bytes from bom03s01-in-f14.1e100.net (74.125.236.110): icmp_req=1 ttl=56 time=110 ms
64 bytes from bom03s01-in-f14.1e100.net (74.125.236.110): icmp_req=2 ttl=56 time=166 ms
64 bytes from bom03s01-in-f14.1e100.net (74.125.236.110): icmp_req=3 ttl=56 time=105 ms
64 bytes from bom03s01-in-f14.1e100.net (74.125.236.110): icmp_req=4 ttl=56 time=83.8 ms
64 bytes from bom03s01-in-f14.1e100.net (74.125.236.110): icmp_req=6 ttl=56 time=79.9 ms
64 bytes from bom03s01-in-f14.1e100.net (74.125.236.110): icmp_req=7 ttl=56 time=110 ms
64 bytes from bom03s01-in-f14.1e100.net (74.125.236.110): icmp_req=8 ttl=56 time=144 ms
64 bytes from bom03s01-in-f14.1e100.net (74.125.236.110): icmp_req=9 ttl=56 time=116 ms
64 bytes from bom03s01-in-f14.1e100.net (74.125.236.110): icmp_req=10 ttl=56 time=101 ms
64 bytes from bom03s01-in-f14.1e100.net (74.125.236.110): icmp_req=11 ttl=56 time=126 ms
64 bytes from bom03s01-in-f14.1e100.net (74.125.236.110): icmp_req=12 ttl=56 time=128 ms
64 bytes from bom03s01-in-f14.1e100.net (74.125.236.110): icmp_req=13 ttl=56 time=77.0 ms
64 bytes from bom03s01-in-f14.1e100.net (74.125.236.110): icmp_req=14 ttl=56 time=123 ms
64 bytes from bom03s01-in-f14.1e100.net (74.125.236.110): icmp_req=15 ttl=56 time=80.6 ms
64 bytes from bom03s01-in-f14.1e100.net (74.125.236.110): icmp_req=16 ttl=56 time=63.8 ms
64 bytes from bom03s01-in-f14.1e100.net (74.125.236.110): icmp_req=17 ttl=56 time=68.8 ms
64 bytes from bom03s01-in-f14.1e100.net (74.125.236.110): icmp_req=18 ttl=56 time=63.7 ms
64 bytes from bom03s01-in-f14.1e100.net (74.125.236.110): icmp_req=19 ttl=56 time=83.7 ms
64 bytes from bom03s01-in-f14.1e100.net (74.125.236.110): icmp_req=20 ttl=56 time=135 ms
64 bytes from bom03s01-in-f14.1e100.net (74.125.236.110): icmp_req=21 ttl=56 time=70.6 ms
64 bytes from bom03s01-in-f14.1e100.net (74.125.236.110): icmp_req=22 ttl=56 time=178 ms
64 bytes from bom03s01-in-f14.1e100.net (74.125.236.110): icmp_req=23 ttl=56 time=79.7 ms
64 bytes from bom03s01-in-f14.1e100.net (74.125.236.110): icmp_req=24 ttl=56 time=174 ms
64 bytes from bom03s01-in-f14.1e100.net (74.125.236.110): icmp_req=25 ttl=56 time=197 ms
64 bytes from bom03s01-in-f14.1e100.net (74.125.236.110): icmp_req=26 ttl=56 time=180 ms
64 bytes from bom03s01-in-f14.1e100.net (74.125.236.110): icmp_req=27 ttl=56 time=63.3 ms
64 bytes from bom03s01-in-f14.1e100.net (74.125.236.110): icmp_req=28 ttl=56 time=92.2 ms
64 bytes from bom03s01-in-f14.1e100.net (74.125.236.110): icmp_req=29 ttl=56 time=121 ms
```



17	14.656930	10.30.56.109	8.8.8.8	DNS	70	Standard query A google.com
18	14.758050	8.8.8.8	10.30.56.109	DNS	246	Standard query response A 74.125.236.99 A 74.125.236.104 A
19	14.758465	10.30.56.109	74.125.236.99	ICMP	98	Echo (ping) request id=0x10ab, seq=1/256, ttl=64
20	14.847515	74.125.236.99	10.30.56.109	ICMP	98	Echo (ping) reply id=0x10ab, seq=1/256, ttl=56
21	14.847746	10.30.56.109	8.8.8.8	DNS	86	Standard query PTR 99.236.125.74.in-addr.arpa
22	14.949391	8.8.8.8	10.30.56.109	DNS	124	Standard query response PTR bom03s01-in-f3.1e100.net
23	15.759423	10.30.56.109	74.125.236.99	ICMP	98	Echo (ping) request id=0x10ab, seq=2/512, ttl=64
24	15.833109	74.125.236.99	10.30.56.109	ICMP	98	Echo (ping) reply id=0x10ab, seq=2/512, ttl=56
25	15.833364	10.30.56.109	8.8.8.8	DNS	86	Standard query PTR 99.236.125.74.in-addr.arpa
26	15.957333	8.8.8.8	10.30.56.109	DNS	124	Standard query response PTR bom03s01-in-f3.1e100.net