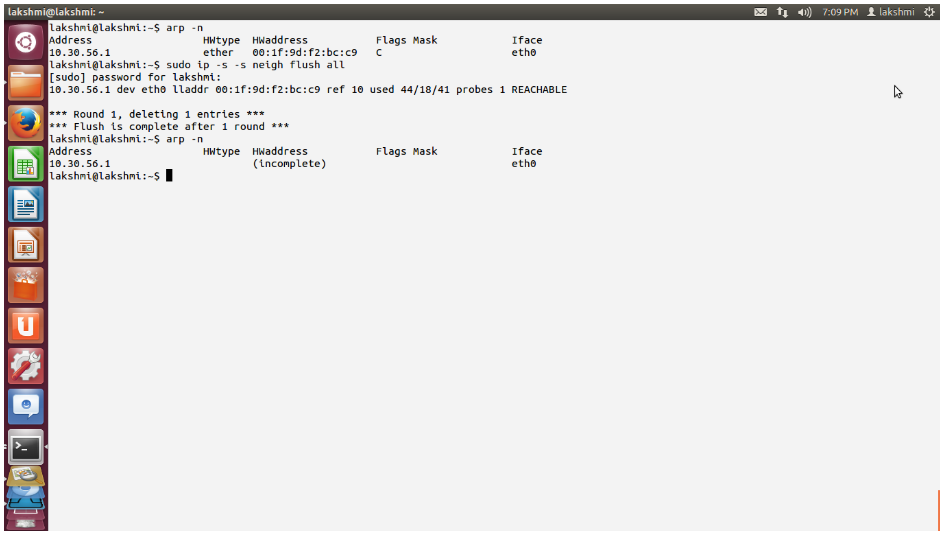
CS620:Advanced Computer Networks : Assignment 2

Lakshmi Devi K

Contents

Problem 1

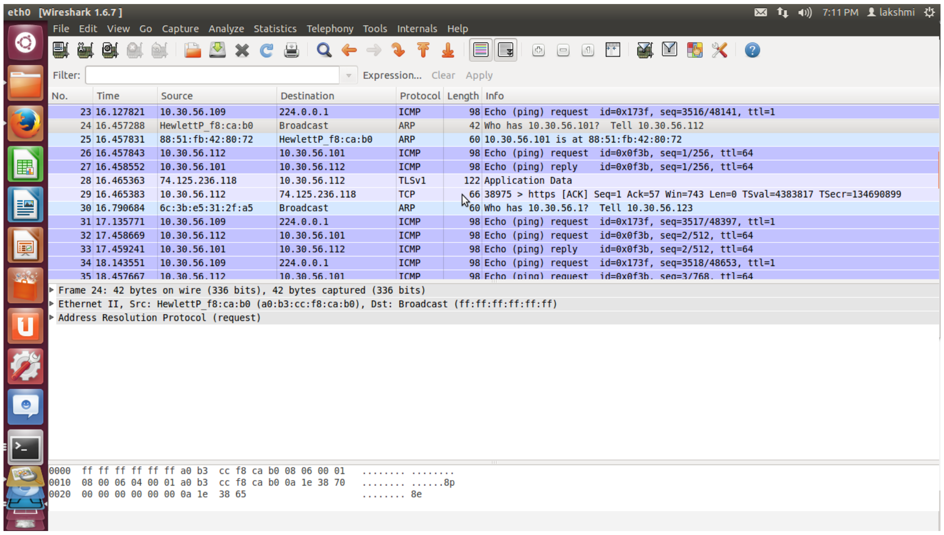
Ping a local ip address and analyse the sniffer capture using wireshark.
Steps: 1)Clear the arp table



```
lakshmi@lakshmi:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.30.56.1               ether   00:1f:9d:f2:bc:c9   C                     eth0
lakshmi@lakshmi:~$ sudo ip -s -s neigh flush all
[sudo] password for lakshmi:
10.30.56.1 dev eth0 lladdr 00:1f:9d:f2:bc:c9 ref 10 used 44/18/41 probes 1 REACHABLE

*** Round 1, deleting 1 entries ***
*** Flush is complete after 1 round ***
lakshmi@lakshmi:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.30.56.1                       (incomplete)                              eth0
lakshmi@lakshmi:~$ 
```

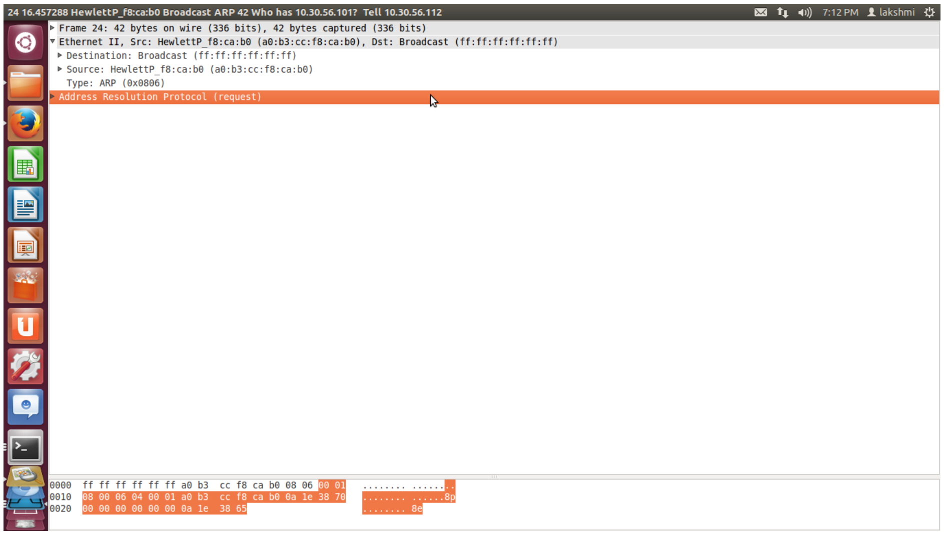
2)start the wireshark sniffer analyser by typing the command sudo wireshark in the terminal. 3)start the capture session 4)Open the terminal and type the command ping 10.30.56.107(any local ip address) 5)check the arp table in the wildshark.



No.	Time	Source	Destination	Protocol	Length	Info
23	16.127821	10.30.56.109	224.0.0.1	ICMP	98	Echo (ping) request id=0x173f, seq=3516/48141, ttl=1
24	16.457288	HewlettP_f8:ca:b0	Broadcast	ARP	42	Who has 10.30.56.101? Tell 10.30.56.112
25	16.457831	88:51:fb:42:80:72	HewlettP_f8:ca:b0	ARP	60	10.30.56.101 is at 88:51:fb:42:80:72
26	16.457843	10.30.56.112	10.30.56.101	ICMP	98	Echo (ping) request id=0x0f3b, seq=1/256, ttl=64
27	16.458552	10.30.56.101	10.30.56.112	ICMP	98	Echo (ping) reply id=0x0f3b, seq=1/256, ttl=64
28	16.465363	74.125.236.118	10.30.56.112	TLSv1	122	Application Data
29	16.465383	10.30.56.112	74.125.236.118	TCP	66	38975 > https [ACK] Seq=1 Ack=57 Win=743 Len=0 TSval=4383817 TSecr=134690899
30	16.790684	6c:3b:e5:31:2f:a5	Broadcast	ARP	60	Who has 10.30.56.1? Tell 10.30.56.123
31	17.135771	10.30.56.109	224.0.0.1	ICMP	98	Echo (ping) request id=0x173f, seq=3517/48397, ttl=1
32	17.458669	10.30.56.112	10.30.56.101	ICMP	98	Echo (ping) request id=0x0f3b, seq=2/512, ttl=64
33	17.459241	10.30.56.101	10.30.56.112	ICMP	98	Echo (ping) reply id=0x0f3b, seq=2/512, ttl=64
34	18.143551	10.30.56.109	224.0.0.1	ICMP	98	Echo (ping) request id=0x173f, seq=3518/48653, ttl=1
35	18.457667	10.30.56.112	10.30.56.101	ICMP	98	Echo (ping) request id=0x0f3b, seq=3/768, ttl=64

```
▸ Frame 24: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
▸ Ethernet II, Src: HewlettP_f8:ca:b0 (a0:b3:cc:f8:ca:b0), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff a0 b3  cc f8 ca b0 08 06 00 01   ........ ........
0010  08 00 06 04 00 01 a0 b3  cc f8 ca b0 0a 1e 38 70   ........ ......8p
0020  00 00 00 00 00 00 0a 1e  38 65                     ........ 8e
```

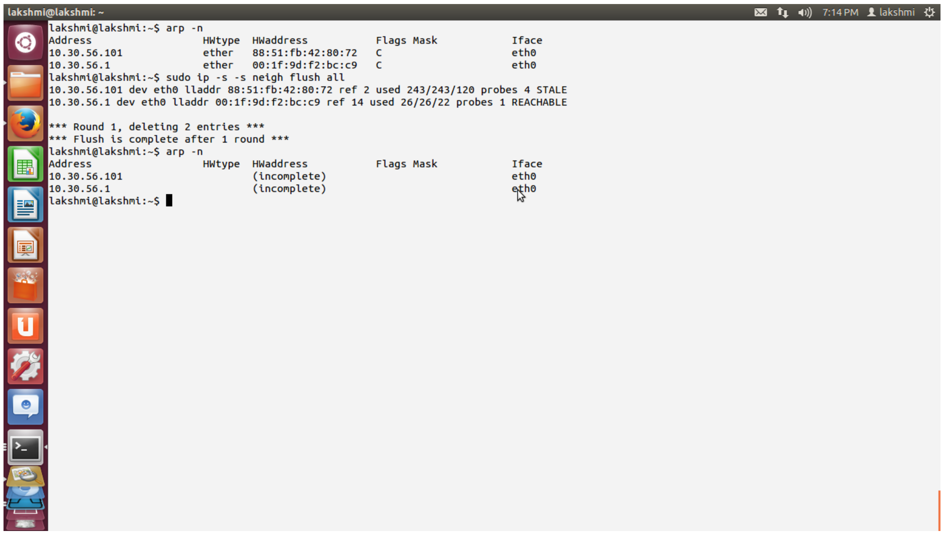


```
24 16.457288 HewlettP_f8:ca:b0 Broadcast ARP 42 Who has 10.30.56.101?  Tell 10.30.56.112
▶ Frame 24: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
▼ Ethernet II, Src: HewlettP_f8:ca:b0 (a0:b3:cc:f8:ca:b0), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▶ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▶ Source: HewlettP_f8:ca:b0 (a0:b3:cc:f8:ca:b0)
    Type: ARP (0x0806)
▶ Address Resolution Protocol (request)

0000  ff ff ff ff ff ff a0 b3  cc f8 ca b0 08 06 00 01   ........ ........
0010  08 00 06 04 00 01 a0 b3  cc f8 ca b0 0a 1e 38 70   ........ ......8p
0020  00 00 00 00 00 00 0a 1e  38 65                     ........ 8e
```

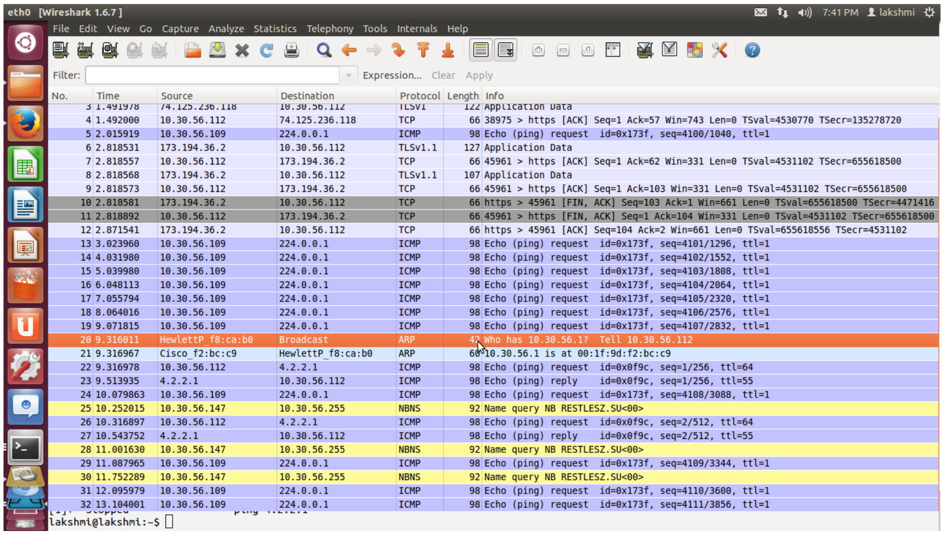
Problem 2

ping an external ip address and analyse the sniffer capture.
Steps: 1)Start the capture session in wireshark.In terminal,type ping google.com.Check the arp table .



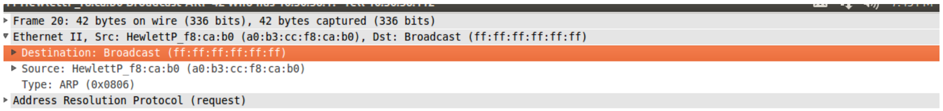
```
lakshmi@lakshmi:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.30.56.101             ether   88:51:fb:42:80:72   C                     eth0
10.30.56.1               ether   00:1f:9d:f2:bc:c9   C                     eth0
lakshmi@lakshmi:~$ sudo ip -s -s neigh flush all
10.30.56.101 dev eth0 lladdr 88:51:fb:42:80:72 ref 2 used 243/243/120 probes 4 STALE
10.30.56.1 dev eth0 lladdr 00:1f:9d:f2:bc:c9 ref 14 used 26/26/22 probes 1 REACHABLE

*** Round 1, deleting 2 entries ***
*** Flush is complete after 1 round ***
lakshmi@lakshmi:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.30.56.101                     (incomplete)                              eth0
10.30.56.1                       (incomplete)                              eth0
lakshmi@lakshmi:~$ 
```



No.	Time	Source	Destination	Protocol	Length	Info
3	1.491978	74.125.236.118	10.30.56.112	TLSv1	122	Application Data
4	1.492000	10.30.56.112	74.125.236.118	TCP	66	38975 > https [ACK] Seq=1 Ack=57 Win=743 Len=0 TSval=4530770 TSecr=135278720
5	2.015919	10.30.56.109	224.0.0.1	ICMP	98	Echo (ping) request id=0x173f, seq=4100/1040, ttl=1
6	2.818531	173.194.36.2	10.30.56.112	TLSv1.1	127	Application Data
7	2.818557	10.30.56.112	173.194.36.2	TCP	66	45961 > https [ACK] Seq=1 Ack=62 Win=331 Len=0 TSval=4531102 TSecr=655618500
8	2.818568	173.194.36.2	10.30.56.112	TLSv1.1	107	Application Data
9	2.818573	10.30.56.112	173.194.36.2	TCP	66	45961 > https [ACK] Seq=1 Ack=103 Win=331 Len=0 TSval=4531102 TSecr=655618500
10	2.818581	173.194.36.2	10.30.56.112	TCP	66	https > 45961 [FIN, ACK] Seq=103 Ack=1 Win=661 Len=0 TSval=655618500 TSecr=4471416
11	2.818892	10.30.56.112	173.194.36.2	TCP	66	45961 > https [FIN, ACK] Seq=1 Ack=104 Win=331 Len=0 TSval=4531102 TSecr=655618500
12	2.871541	173.194.36.2	10.30.56.112	TCP	66	https > 45961 [ACK] Seq=104 Ack=2 Win=661 Len=0 TSval=655618556 TSecr=4531102
13	3.023960	10.30.56.109	224.0.0.1	ICMP	98	Echo (ping) request id=0x173f, seq=4101/1296, ttl=1
14	4.031980	10.30.56.109	224.0.0.1	ICMP	98	Echo (ping) request id=0x173f, seq=4102/1552, ttl=1
15	5.039980	10.30.56.109	224.0.0.1	ICMP	98	Echo (ping) request id=0x173f, seq=4103/1808, ttl=1
16	6.048113	10.30.56.109	224.0.0.1	ICMP	98	Echo (ping) request id=0x173f, seq=4104/2064, ttl=1
17	7.055794	10.30.56.109	224.0.0.1	ICMP	98	Echo (ping) request id=0x173f, seq=4105/2320, ttl=1
18	8.064016	10.30.56.109	224.0.0.1	ICMP	98	Echo (ping) request id=0x173f, seq=4106/2576, ttl=1
19	9.071815	10.30.56.109	224.0.0.1	ICMP	98	Echo (ping) request id=0x173f, seq=4107/2832, ttl=1
20	9.316011	HewlettP_f8:ca:b0	Broadcast	ARP	42	Who has 10.30.56.1? Tell 10.30.56.112
21	9.316967	Cisco_f2:bc:c9	HewlettP_f8:ca:b0	ARP	60	10.30.56.1 is at 00:1f:9d:f2:bc:c9
22	9.316978	10.30.56.112	4.2.2.1	ICMP	98	Echo (ping) request id=0x0f9c, seq=1/256, ttl=64
23	9.513935	4.2.2.1	10.30.56.112	ICMP	98	Echo (ping) reply id=0x0f9c, seq=1/256, ttl=55
24	10.079863	10.30.56.109	224.0.0.1	ICMP	98	Echo (ping) request id=0x173f, seq=4108/3088, ttl=1
25	10.252015	10.30.56.147	10.30.56.255	NBNS	92	Name query NB RESTLESZ.SU<00>
26	10.316897	10.30.56.112	4.2.2.1	ICMP	98	Echo (ping) request id=0x0f9c, seq=2/512, ttl=64
27	10.543752	4.2.2.1	10.30.56.112	ICMP	98	Echo (ping) reply id=0x0f9c, seq=2/512, ttl=55
28	11.001630	10.30.56.147	10.30.56.255	NBNS	92	Name query NB RESTLESZ.SU<00>
29	11.087965	10.30.56.109	224.0.0.1	ICMP	98	Echo (ping) request id=0x173f, seq=4109/3344, ttl=1
30	11.752289	10.30.56.147	10.30.56.255	NBNS	92	Name query NB RESTLESZ.SU<00>
31	12.095979	10.30.56.109	224.0.0.1	ICMP	98	Echo (ping) request id=0x173f, seq=4110/3600, ttl=1
32	13.104001	10.30.56.109	224.0.0.1	ICMP	98	Echo (ping) request id=0x173f, seq=4111/3856, ttl=1

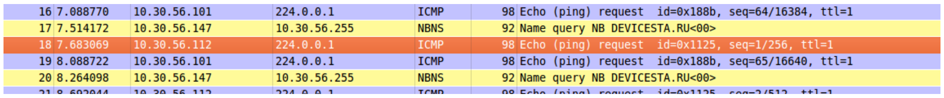
```
lakshmi@lakshmi:~$ 
```



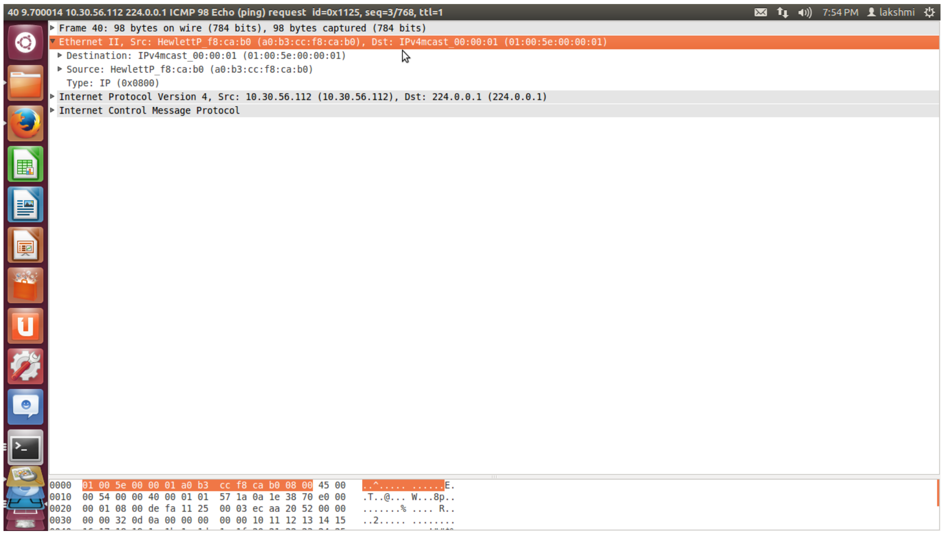
```
▸ Frame 20: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
▾ Ethernet II, Src: HewlettP_f8:ca:b0 (a0:b3:cc:f8:ca:b0), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Source: HewlettP_f8:ca:b0 (a0:b3:cc:f8:ca:b0)
    Type: ARP (0x0806)
▸ Address Resolution Protocol (request)
```

Problem 3

ping an multicast group and analyse the sniffer capture.
Steps: 1)Start the capture session in wireshark.In terminal,type ping 224.0.0.1.Check the arp table .



```
16 7.088770   10.30.56.101   224.0.0.1      ICMP   98 Echo (ping) request  id=0x188b, seq=64/16384, ttl=1
17 7.514172   10.30.56.147   10.30.56.255   NBNS   92 Name query NB DEVICESTA.RU<00>
18 7.683069   10.30.56.112   224.0.0.1      ICMP   98 Echo (ping) request  id=0x1125, seq=1/256, ttl=1
19 8.088722   10.30.56.101   224.0.0.1      ICMP   98 Echo (ping) request  id=0x188b, seq=65/16640, ttl=1
20 8.264098   10.30.56.147   10.30.56.255   NBNS   92 Name query NB DEVICESTA.RU<00>
21 8.692044   10.30.56.112   224.0.0.1      ICMP   98 Echo (ping) request  id=0x1125, seq=2/512, ttl=1
```



40 9.700014 10.30.56.112 224.0.0.1 ICMP 98 Echo (ping) request id=0x1125, seq=3/768, ttl=1

```
▶ Frame 40: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
▼ Ethernet II, Src: HewlettP_f8:ca:b0 (a0:b3:cc:f8:ca:b0), Dst: IPv4mcast_00:00:01 (01:00:5e:00:00:01)
  ▶ Destination: IPv4mcast_00:00:01 (01:00:5e:00:00:01)
  ▶ Source: HewlettP_f8:ca:b0 (a0:b3:cc:f8:ca:b0)
    Type: IP (0x0800)
▶ Internet Protocol Version 4, Src: 10.30.56.112 (10.30.56.112), Dst: 224.0.0.1 (224.0.0.1)
▶ Internet Control Message Protocol
```

```
0000  01 00 5e 00 00 01 a0 b3  cc f8 ca b0 08 00 45 00   ..^..... ......E.
0010  00 54 00 00 40 00 01 01  57 1a 0a 1e 38 70 e0 00   .T..@... W...8p..
0020  00 01 08 00 de fa 11 25  00 03 ec aa 20 52 00 00   .......% .... R..
0030  00 00 32 0d 0a 00 00 00  00 00 10 11 12 13 14 15   ..2..... ........
```