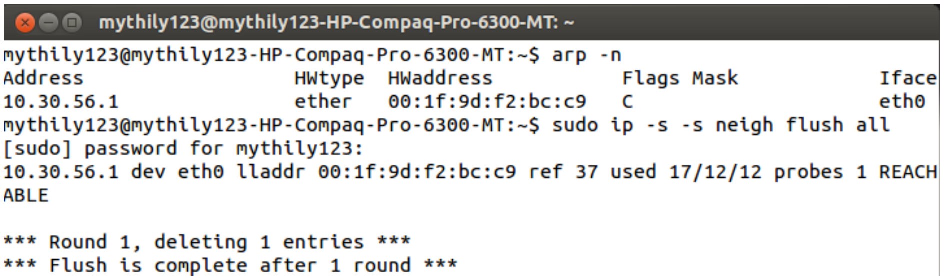
Advanced Networks Lab: Assignment #2

A Ganga Mythily

Contents

Problem 1

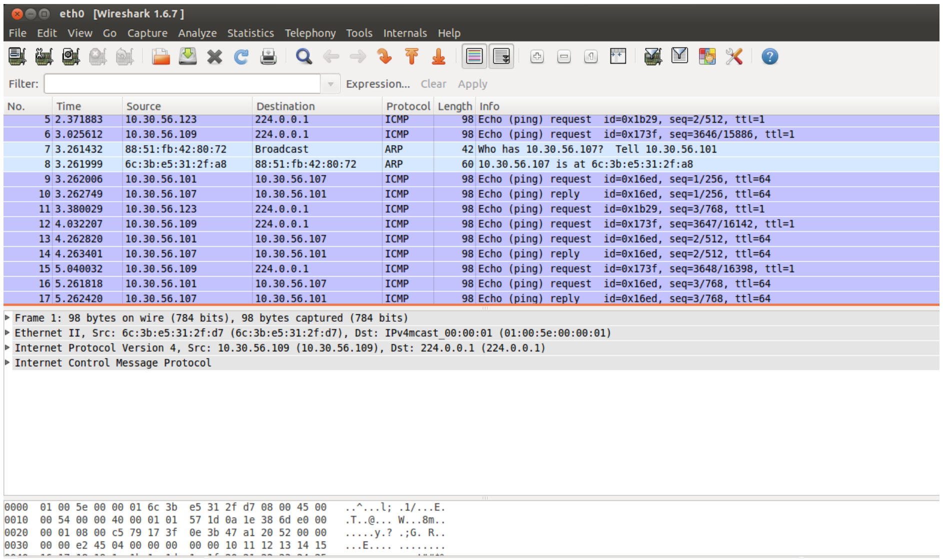
Ping another IP address
Steps: 1)List arp cache using arp -n 2)Clear cache using sudo ip -s -s neigh flushall 3)Open wireshark using sudo wireshark. 4)Start to capture packets 5)Ping any id address(say 101.30.56.107) 6)Analyse it.



```
mythily123@mythily123-HP-Compaq-Pro-6300-MT:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.30.56.1               ether   00:1f:9d:f2:bc:c9   C                     eth0
mythily123@mythily123-HP-Compaq-Pro-6300-MT:~$ sudo ip -s -s neigh flush all
[sudo] password for mythily123:
10.30.56.1 dev eth0 lladdr 00:1f:9d:f2:bc:c9 ref 37 used 17/12/12 probes 1 REACH
ABLE

*** Round 1, deleting 1 entries ***
*** Flush is complete after 1 round ***
```

machine.png



eth0 [Wireshark 1.6.7]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply

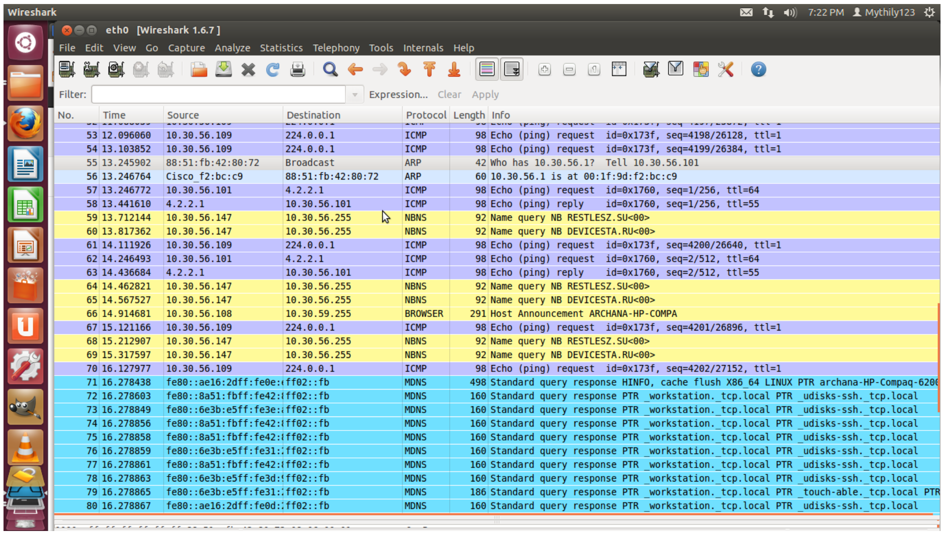
No.	Time	Source	Destination	Protocol	Length	Info
5	2.371883	10.30.56.123	224.0.0.1	ICMP	98	Echo (ping) request id=0x1b29, seq=2/512, ttl=1
6	3.025612	10.30.56.109	224.0.0.1	ICMP	98	Echo (ping) request id=0x173f, seq=3646/15886, ttl=1
7	3.261432	88:51:fb:42:80:72	Broadcast	ARP	42	Who has 10.30.56.107? Tell 10.30.56.101
8	3.261999	6c:3b:e5:31:2f:a8	88:51:fb:42:80:72	ARP	60	10.30.56.107 is at 6c:3b:e5:31:2f:a8
9	3.262006	10.30.56.101	10.30.56.107	ICMP	98	Echo (ping) request id=0x16ed, seq=1/256, ttl=64
10	3.262749	10.30.56.107	10.30.56.101	ICMP	98	Echo (ping) reply id=0x16ed, seq=1/256, ttl=64
11	3.380029	10.30.56.123	224.0.0.1	ICMP	98	Echo (ping) request id=0x1b29, seq=3/768, ttl=1
12	4.032207	10.30.56.109	224.0.0.1	ICMP	98	Echo (ping) request id=0x173f, seq=3647/16142, ttl=1
13	4.262820	10.30.56.101	10.30.56.107	ICMP	98	Echo (ping) request id=0x16ed, seq=2/512, ttl=64
14	4.263401	10.30.56.107	10.30.56.101	ICMP	98	Echo (ping) reply id=0x16ed, seq=2/512, ttl=64
15	5.040032	10.30.56.109	224.0.0.1	ICMP	98	Echo (ping) request id=0x173f, seq=3648/16398, ttl=1
16	5.261818	10.30.56.101	10.30.56.107	ICMP	98	Echo (ping) request id=0x16ed, seq=3/768, ttl=64
17	5.262420	10.30.56.107	10.30.56.101	ICMP	98	Echo (ping) reply id=0x16ed, seq=3/768, ttl=64

```
▸ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
▸ Ethernet II, Src: 6c:3b:e5:31:2f:d7 (6c:3b:e5:31:2f:d7), Dst: IPv4mcast_00:00:01 (01:00:5e:00:00:01)
▸ Internet Protocol Version 4, Src: 10.30.56.109 (10.30.56.109), Dst: 224.0.0.1 (224.0.0.1)
▸ Internet Control Message Protocol
```

```
0000  01 00 5e 00 00 01 6c 3b  e5 31 2f d7 08 00 45 00   ..^...l; .1/...E.
0010  00 54 00 00 40 00 01 01  57 1d 0a 1e 38 6d e0 00   .T..@... W...8m..
0020  00 01 08 00 c5 79 17 3f  0e 3b 47 a1 20 52 00 00   .....y.? .;G. R..
0030  00 00 e2 45 04 00 00 00  00 00 10 11 12 13 14 15   ...E.... ........
```

Problem 2

Ping google.com
Steps: 1)Clear google cache. 2)Open wireshark using sudo wireshark. 3)Start to capture packets. 4)Ping 4.2.2.1



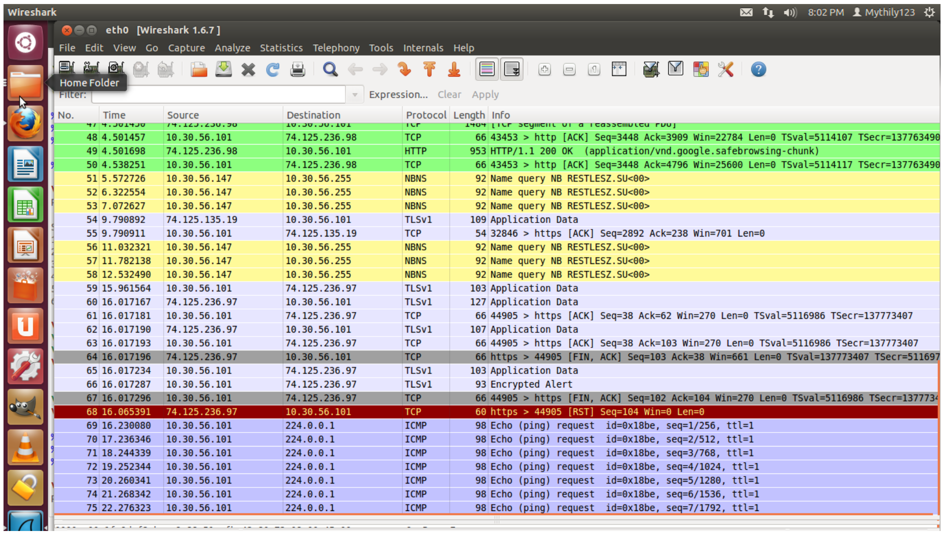
No.	Time	Source	Destination	Protocol	Length	Info
53	12.096060	10.30.56.109	224.0.0.1	ICMP	98	Echo (ping) request id=0x173f, seq=4198/26128, ttl=1
54	13.103852	10.30.56.109	224.0.0.1	ICMP	98	Echo (ping) request id=0x173f, seq=4199/26384, ttl=1
55	13.245902	88:51:fb:42:80:72	Broadcast	ARP	42	Who has 10.30.56.1? Tell 10.30.56.101
56	13.246764	Cisco_f2:bc:c9	88:51:fb:42:80:72	ARP	60	10.30.56.1 is at 00:1f:9d:f2:bc:c9
57	13.246772	10.30.56.101	4.2.2.1	ICMP	98	Echo (ping) request id=0x1760, seq=1/256, ttl=64
58	13.441610	4.2.2.1	10.30.56.101	ICMP	98	Echo (ping) reply id=0x1760, seq=1/256, ttl=55
59	13.712144	10.30.56.147	10.30.56.255	NBNS	92	Name query NB RESTLESZ.SU<00>
60	13.817362	10.30.56.147	10.30.56.255	NBNS	92	Name query NB DEVICESTA.RU<00>
61	14.111926	10.30.56.109	224.0.0.1	ICMP	98	Echo (ping) request id=0x173f, seq=4200/26640, ttl=1
62	14.246493	10.30.56.101	4.2.2.1	ICMP	98	Echo (ping) request id=0x1760, seq=2/512, ttl=64
63	14.436684	4.2.2.1	10.30.56.101	ICMP	98	Echo (ping) reply id=0x1760, seq=2/512, ttl=55
64	14.462821	10.30.56.147	10.30.56.255	NBNS	92	Name query NB RESTLESZ.SU<00>
65	14.567527	10.30.56.147	10.30.56.255	NBNS	92	Name query NB DEVICESTA.RU<00>
66	14.914681	10.30.56.108	10.30.59.255	BROWSER	291	Host Announcement ARCHANA-HP-COMPA
67	15.121166	10.30.56.109	224.0.0.1	ICMP	98	Echo (ping) request id=0x173f, seq=4201/26896, ttl=1
68	15.212907	10.30.56.147	10.30.56.255	NBNS	92	Name query NB RESTLESZ.SU<00>
69	15.317597	10.30.56.147	10.30.56.255	NBNS	92	Name query NB DEVICESTA.RU<00>
70	16.127977	10.30.56.109	224.0.0.1	ICMP	98	Echo (ping) request id=0x173f, seq=4202/27152, ttl=1
71	16.278438	fe80::ae16:2dff:fe0e:	ff02::fb	MDNS	498	Standard query response HINFO, cache flush X86_64 LINUX PTR archana-HP-Compaq-620
72	16.278603	fe80::8a51:fbff:fe42:	ff02::fb	MDNS	160	Standard query response PTR _workstation._tcp.local PTR _udisks-ssh._tcp.local
73	16.278849	fe80::6e3b:e5ff:fe3e:	ff02::fb	MDNS	160	Standard query response PTR _workstation._tcp.local PTR _udisks-ssh._tcp.local
74	16.278856	fe80::8a51:fbff:fe42:	ff02::fb	MDNS	160	Standard query response PTR _workstation._tcp.local PTR _udisks-ssh._tcp.local
75	16.278858	fe80::8a51:fbff:fe42:	ff02::fb	MDNS	160	Standard query response PTR _workstation._tcp.local PTR _udisks-ssh._tcp.local
76	16.278859	fe80::6e3b:e5ff:fe31:	ff02::fb	MDNS	160	Standard query response PTR _workstation._tcp.local PTR _udisks-ssh._tcp.local
77	16.278861	fe80::8a51:fbff:fe42:	ff02::fb	MDNS	160	Standard query response PTR _workstation._tcp.local PTR _udisks-ssh._tcp.local
78	16.278863	fe80::6e3b:e5ff:fe3d:	ff02::fb	MDNS	160	Standard query response PTR _workstation._tcp.local PTR _udisks-ssh._tcp.local
79	16.278865	fe80::6e3b:e5ff:fe31:	ff02::fb	MDNS	186	Standard query response PTR _workstation._tcp.local PTR _touch-able._tcp.local PTR
80	16.278867	fe80::ae16:2dff:fe0d:	ff02::fb	MDNS	160	Standard query response PTR _workstation._tcp.local PTR _udisks-ssh._tcp.local

Problem 3

Ping 224.0.0.1(multicast)

Steps: 1)Clear google cache. 2)Open wireshark using sudo wireshark. 3)Start to capture packets. 4)Ping 224.0.0.1

MAC address of multicast:01:00:5e:00:00:01 MAC address of broadcast:ff:ff:ff:ff:ff:ff



No.	Time	Source	Destination	Protocol	Length	Info
47	4.501450	74.125.236.98	10.30.56.101	TCP	1484	[TCP segment of a reassembled PDU]
48	4.501457	10.30.56.101	74.125.236.98	TCP	66	43453 > http [ACK] Seq=3448 Ack=3909 Win=22784 Len=0 TSval=5114107 TSecr=137763490
49	4.501698	74.125.236.98	10.30.56.101	HTTP	953	HTTP/1.1 200 OK (application/vnd.google.safebrowsing-chunk)
50	4.538251	10.30.56.101	74.125.236.98	TCP	66	43453 > http [ACK] Seq=3448 Ack=4796 Win=25600 Len=0 TSval=5114117 TSecr=137763490
51	5.572726	10.30.56.147	10.30.56.255	NBNS	92	Name query NB RESTLESZ.SU<00>
52	6.322554	10.30.56.147	10.30.56.255	NBNS	92	Name query NB RESTLESZ.SU<00>
53	7.072627	10.30.56.147	10.30.56.255	NBNS	92	Name query NB RESTLESZ.SU<00>
54	9.790892	74.125.135.19	10.30.56.101	TLSv1	109	Application Data
55	9.790911	10.30.56.101	74.125.135.19	TCP	54	32846 > https [ACK] Seq=2892 Ack=238 Win=701 Len=0
56	11.032321	10.30.56.147	10.30.56.255	NBNS	92	Name query NB RESTLESZ.SU<00>
57	11.782138	10.30.56.147	10.30.56.255	NBNS	92	Name query NB RESTLESZ.SU<00>
58	12.532490	10.30.56.147	10.30.56.255	NBNS	92	Name query NB RESTLESZ.SU<00>
59	15.961564	10.30.56.101	74.125.236.97	TLSv1	103	Application Data
60	16.017167	74.125.236.97	10.30.56.101	TLSv1	127	Application Data
61	16.017181	10.30.56.101	74.125.236.97	TCP	66	44905 > https [ACK] Seq=38 Ack=62 Win=270 Len=0 TSval=5116986 TSecr=137773407
62	16.017190	74.125.236.97	10.30.56.101	TLSv1	107	Application Data
63	16.017193	10.30.56.101	74.125.236.97	TCP	66	44905 > https [ACK] Seq=38 Ack=103 Win=270 Len=0 TSval=5116986 TSecr=137773407
64	16.017196	74.125.236.97	10.30.56.101	TCP	66	https > 44905 [FIN, ACK] Seq=103 Ack=38 Win=661 Len=0 TSval=137773407 TSecr=511697
65	16.017234	10.30.56.101	74.125.236.97	TLSv1	103	Application Data
66	16.017287	10.30.56.101	74.125.236.97	TLSv1	93	Encrypted Alert
67	16.017296	10.30.56.101	74.125.236.97	TCP	66	44905 > https [FIN, ACK] Seq=102 Ack=104 Win=270 Len=0 TSval=5116986 TSecr=137773
68	16.065391	74.125.236.97	10.30.56.101	TCP	60	https > 44905 [RST] Seq=104 Win=0 Len=0
69	16.230080	10.30.56.101	224.0.0.1	ICMP	98	Echo (ping) request id=0x18be, seq=1/256, ttl=1
70	17.236346	10.30.56.101	224.0.0.1	ICMP	98	Echo (ping) request id=0x18be, seq=2/512, ttl=1
71	18.244339	10.30.56.101	224.0.0.1	ICMP	98	Echo (ping) request id=0x18be, seq=3/768, ttl=1
72	19.252344	10.30.56.101	224.0.0.1	ICMP	98	Echo (ping) request id=0x18be, seq=4/1024, ttl=1
73	20.260341	10.30.56.101	224.0.0.1	ICMP	98	Echo (ping) request id=0x18be, seq=5/1280, ttl=1
74	21.268342	10.30.56.101	224.0.0.1	ICMP	98	Echo (ping) request id=0x18be, seq=6/1536, ttl=1
75	22.276323	10.30.56.101	224.0.0.1	ICMP	98	Echo (ping) request id=0x18be, seq=7/1792, ttl=1