CS447 Lab Assignment 3

Decoding Ethernet Frames

Rajnish Kumar [CIN: 304470392]
Gaurav Prajapati [CIN: 304470132]
Manan Patel [CIN: 304373828]

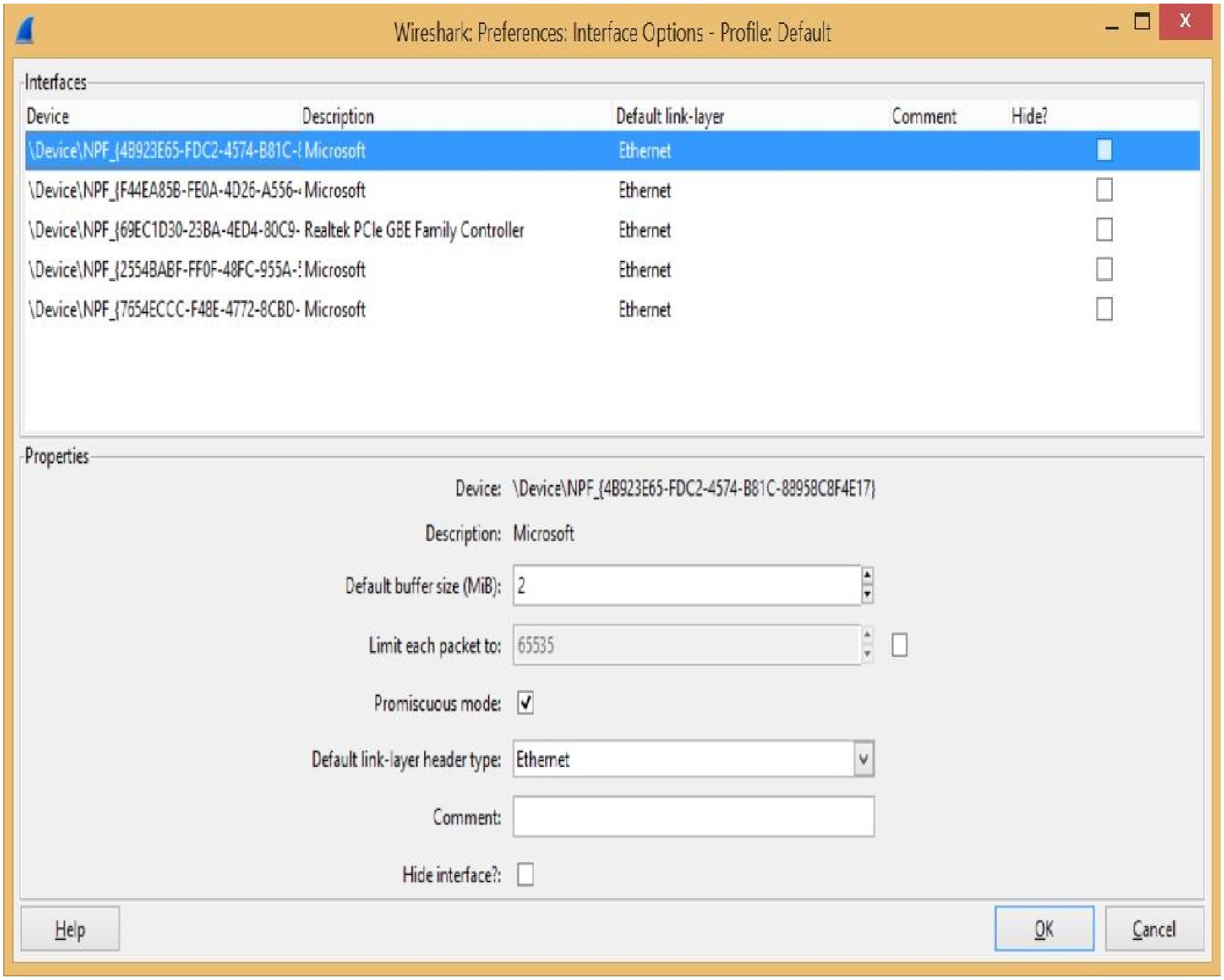
Date: 07/15/2015 Group# 11

"I hear and I forget; I see and I remember; I do and I understand"

Go to web site http://www.wireshark.org and download a copy of the packet capture (sniffer) and analyzer for your VM instance of Windows operating system.

1. Turn on your sniffer in promiscuous mode and begin capturing all network traffic.

⇨ Screen shot <promiscuous mode>



Wireshark: Preferences: Interface Options - Profile: Default
Interfaces

Device	Description	Default link-layer	Comment	Hide?
\Device\NPF_{4B923E65-FDC2-4574-B81C-{	Microsoft	Ethernet		□
\Device\NPF_{F44EA85B-FE0A-4D26-A556-·	Microsoft	Ethernet		□
\Device\NPF_{69EC1D30-23BA-4ED4-80C9-	Realtek PCIe GBE Family Controller	Ethernet		□
\Device\NPF_{2554BABF-FF0F-48FC-955A-!	Microsoft	Ethernet		□
\Device\NPF_{7654ECCC-F48E-4772-8CBD-	Microsoft	Ethernet		□

Device: \Device\NPF_{4B923E65-FDC2-4574-B81C-88958C8F4E17}

Description: Microsoft

Default buffer size (MiB): 2

Limit each packet to: 65535 □

Promiscuous mode: ☑

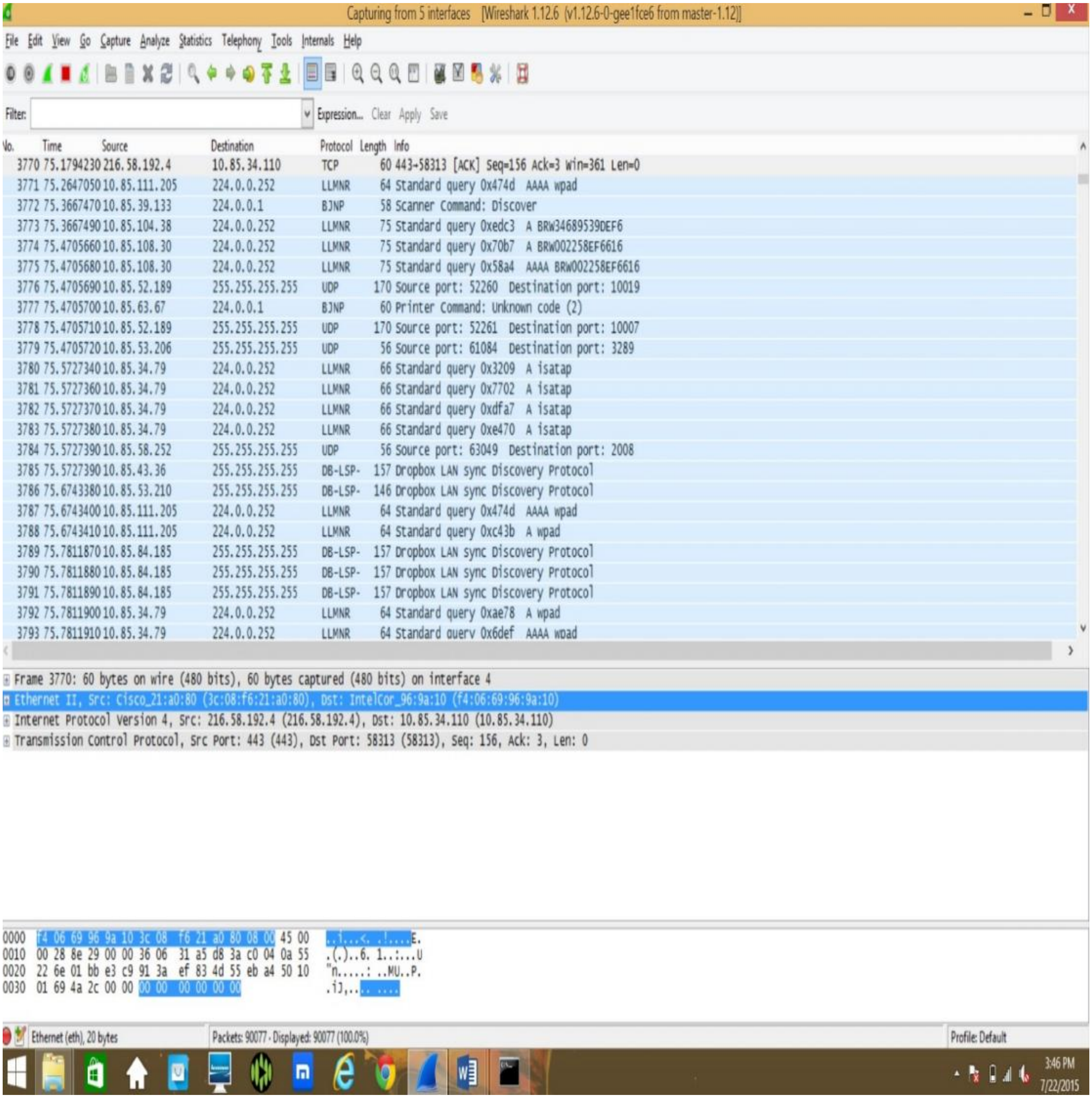
Default link-layer header type: Ethernet

Comment:

Hide interface?: □

a. What is the destination Ethernet address of broadcast traffic? Submit screenshot with this value circled.

Ans: f4:06:69:96:9a:10


Capturing from 5 interfaces [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
Profile: Default
3:46 PM
7/22/2015

```
No.  Time       Source         Destination      Protocol Length Info
3770 75.1794230 216.58.192.4   10.85.34.110     TCP       60 443→58313 [ACK] Seq=156 Ack=3 Win=361 Len=0
3771 75.2647050 10.85.111.205  224.0.0.252      LLMNR     64 Standard query 0x474d  AAAA wpad
3772 75.3667470 10.85.39.133   224.0.0.1        BJNP      58 Scanner Command: Discover
3773 75.3667490 10.85.104.38   224.0.0.252      LLMNR     75 Standard query 0xedc3  A BRW34689539DEF6
3774 75.4705660 10.85.108.30   224.0.0.252      LLMNR     75 Standard query 0x70b7  A BRW002258EF6616
3775 75.4705680 10.85.108.30   224.0.0.252      LLMNR     75 Standard query 0x58a4  AAAA BRW002258EF6616
3776 75.4705690 10.85.52.189   255.255.255.255  UDP      170 Source port: 52260  Destination port: 10019
3777 75.4705700 10.85.63.67    224.0.0.1        BJNP      60 Printer Command: Unknown code (2)
3778 75.4705710 10.85.52.189   255.255.255.255  UDP      170 Source port: 52261  Destination port: 10007
3779 75.4705720 10.85.53.206   255.255.255.255  UDP       56 Source port: 61084  Destination port: 3289
3780 75.5727340 10.85.34.79    224.0.0.252      LLMNR     66 Standard query 0x3209  A isatap
3781 75.5727360 10.85.34.79    224.0.0.252      LLMNR     66 Standard query 0x7702  A isatap
3782 75.5727370 10.85.34.79    224.0.0.252      LLMNR     66 Standard query 0xdfa7  A isatap
3783 75.5727380 10.85.34.79    224.0.0.252      LLMNR     66 Standard query 0xe470  A isatap
3784 75.5727390 10.85.58.252   255.255.255.255  UDP       56 Source port: 63049  Destination port: 2008
3785 75.5727390 10.85.43.36    255.255.255.255  DB-LSP-  157 Dropbox LAN sync Discovery Protocol
3786 75.6743380 10.85.53.210   255.255.255.255  DB-LSP-  146 Dropbox LAN sync Discovery Protocol
3787 75.6743400 10.85.111.205  224.0.0.252      LLMNR     64 Standard query 0x474d  AAAA wpad
3788 75.6743410 10.85.111.205  224.0.0.252      LLMNR     64 Standard query 0xc43b  A wpad
3789 75.7811870 10.85.84.185   255.255.255.255  DB-LSP-  157 Dropbox LAN sync Discovery Protocol
3790 75.7811880 10.85.84.185   255.255.255.255  DB-LSP-  157 Dropbox LAN sync Discovery Protocol
3791 75.7811890 10.85.84.185   255.255.255.255  DB-LSP-  157 Dropbox LAN sync Discovery Protocol
3792 75.7811900 10.85.34.79    224.0.0.252      LLMNR     64 Standard query 0xae78  A wpad
3793 75.7811910 10.85.34.79    224.0.0.252      LLMNR     64 Standard query 0x6def  AAAA wpad
```

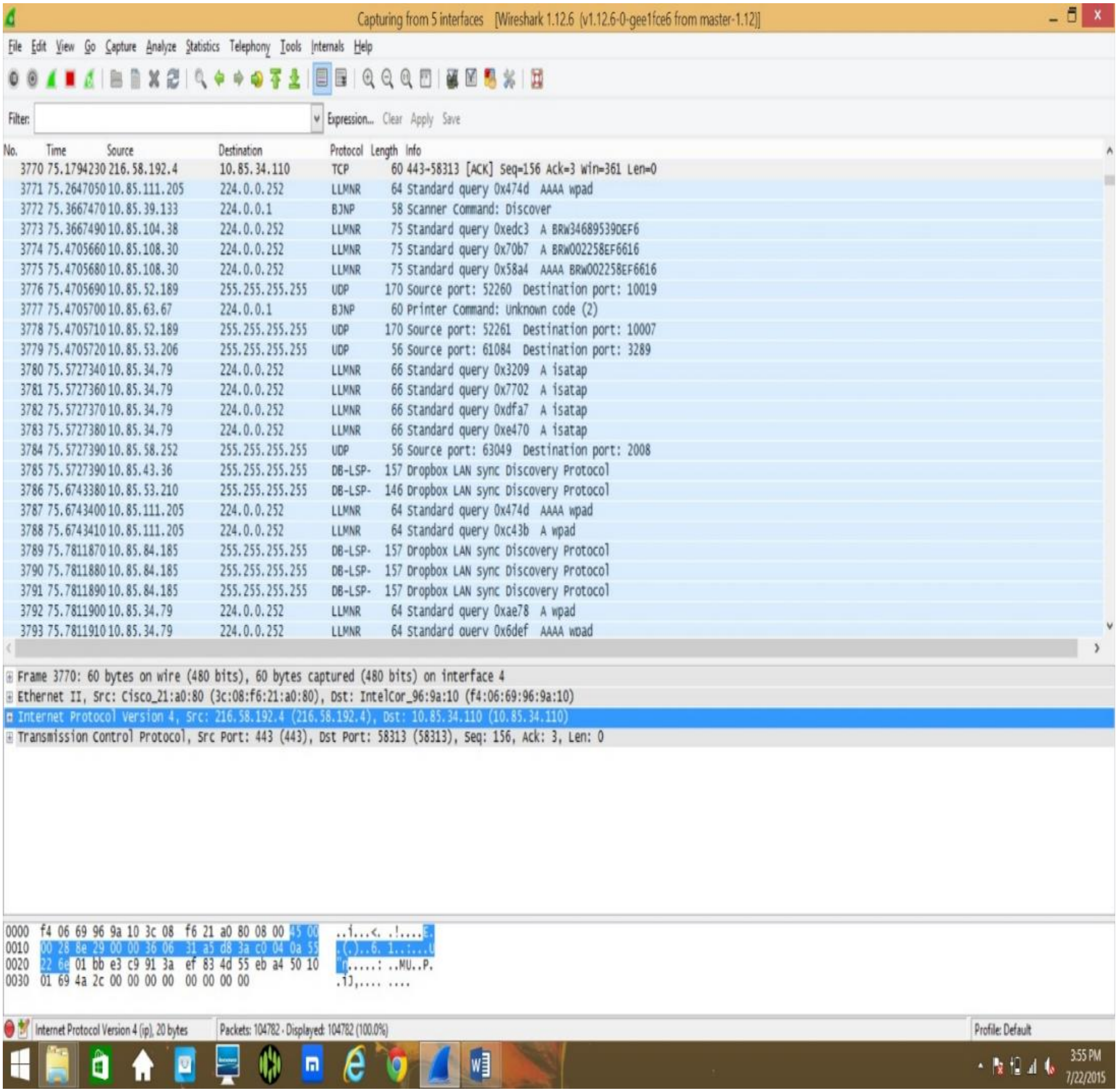
```
⊞ Frame 3770: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 4
⊞ Ethernet II, Src: Cisco_21:a0:80 (3c:08:f6:21:a0:80), Dst: IntelCor_96:9a:10 (f4:06:69:96:9a:10)
⊞ Internet Protocol Version 4, Src: 216.58.192.4 (216.58.192.4), Dst: 10.85.34.110 (10.85.34.110)
⊞ Transmission Control Protocol, Src Port: 443 (443), Dst Port: 58313 (58313), Seq: 156, Ack: 3, Len: 0
```

```
0000  f4 06 69 96 9a 10 3c 08  f6 21 a0 80 08 00 45 00   ..i...<. .!....E.
0010  00 28 8e 29 00 00 36 06  31 a5 d8 3a c0 04 0a 55   .(.)..6. 1..:...U
0020  22 6e 01 bb e3 c9 91 3a  ef 83 4d 55 eb a4 50 10   "n.....: ..MU..P.
0030  01 69 4a 2c 00 00 00 00  00 00 00 00               .iJ,.... ....
```

Ethernet (eth), 20 bytes | Packets: 90077 · Displayed: 90077 (100.0%)

b. What is the destination IP address of broadcast traffic? Submit screenshot with this value circled.

Ans: 10.85.34.110


Capturing from 5 interfaces [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
3:55 PM
7/22/2015

```
No.   Time      Source        Destination     Protocol Length Info
 3770 75.1794230 216.58.192.4  10.85.34.110    TCP       60 443→58313 [ACK] Seq=156 Ack=3 Win=361 Len=0
 3771 75.2647050 10.85.111.205 224.0.0.252     LLMNR     64 Standard query 0x474d  AAAA wpad
 3772 75.3667470 10.85.39.133  224.0.0.1       BJNP      58 Scanner Command: Discover
 3773 75.3667490 10.85.104.38  224.0.0.252     LLMNR     75 Standard query 0xedc3  A BRW34689539DEF6
 3774 75.4705660 10.85.108.30  224.0.0.252     LLMNR     75 Standard query 0x70b7  A BRW002258EF6616
 3775 75.4705680 10.85.108.30  224.0.0.252     LLMNR     75 Standard query 0x58a4  AAAA BRW002258EF6616
 3776 75.4705690 10.85.52.189  255.255.255.255 UDP      170 Source port: 52260  Destination port: 10019
 3777 75.4705700 10.85.63.67   224.0.0.1       BJNP      60 Printer Command: Unknown code (2)
 3778 75.4705710 10.85.52.189  255.255.255.255 UDP      170 Source port: 52261  Destination port: 10007
 3779 75.4705720 10.85.53.206  255.255.255.255 UDP       56 Source port: 61084  Destination port: 3289
 3780 75.5727340 10.85.34.79   224.0.0.252     LLMNR     66 Standard query 0x3209  A isatap
 3781 75.5727360 10.85.34.79   224.0.0.252     LLMNR     66 Standard query 0x7702  A isatap
 3782 75.5727370 10.85.34.79   224.0.0.252     LLMNR     66 Standard query 0xdfa7  A isatap
 3783 75.5727380 10.85.34.79   224.0.0.252     LLMNR     66 Standard query 0xe470  A isatap
 3784 75.5727390 10.85.58.252  255.255.255.255 UDP       56 Source port: 63049  Destination port: 2008
 3785 75.5727390 10.85.43.36   255.255.255.255 DB-LSP-  157 Dropbox LAN sync Discovery Protocol
 3786 75.6743380 10.85.53.210  255.255.255.255 DB-LSP-  146 Dropbox LAN sync Discovery Protocol
 3787 75.6743400 10.85.111.205 224.0.0.252     LLMNR     64 Standard query 0x474d  AAAA wpad
 3788 75.6743410 10.85.111.205 224.0.0.252     LLMNR     64 Standard query 0xc43b  A wpad
 3789 75.7811870 10.85.84.185  255.255.255.255 DB-LSP-  157 Dropbox LAN sync Discovery Protocol
 3790 75.7811880 10.85.84.185  255.255.255.255 DB-LSP-  157 Dropbox LAN sync Discovery Protocol
 3791 75.7811890 10.85.84.185  255.255.255.255 DB-LSP-  157 Dropbox LAN sync Discovery Protocol
 3792 75.7811900 10.85.34.79   224.0.0.252     LLMNR     64 Standard query 0xae78  A wpad
 3793 75.7811910 10.85.34.79   224.0.0.252     LLMNR     64 Standard querv 0x6def  AAAA wpad
```

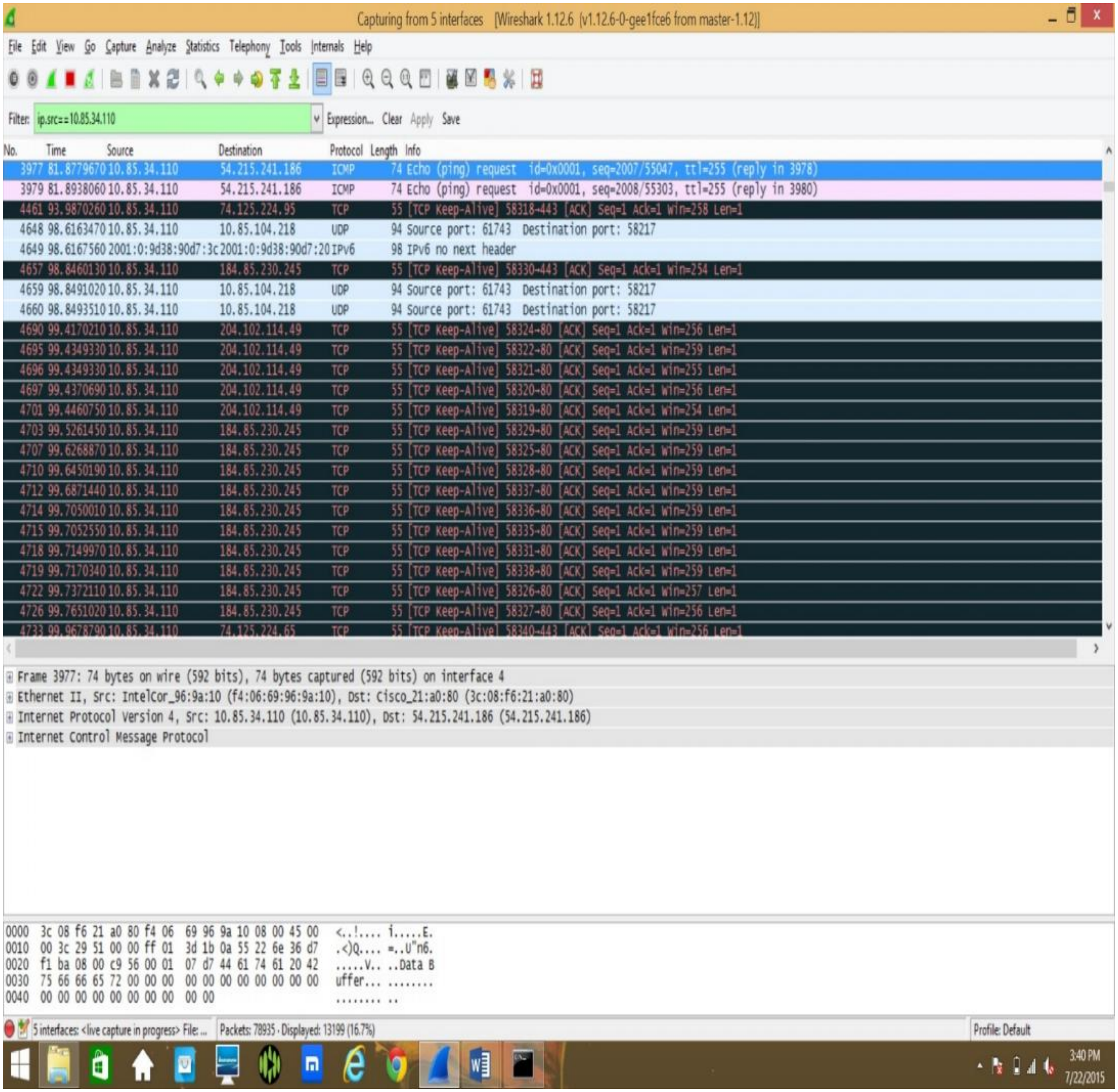
```
⊞ Frame 3770: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 4
⊞ Ethernet II, Src: Cisco_21:a0:80 (3c:08:f6:21:a0:80), Dst: IntelCor_96:9a:10 (f4:06:69:96:9a:10)
⊞ Internet Protocol Version 4, Src: 216.58.192.4 (216.58.192.4), Dst: 10.85.34.110 (10.85.34.110)
⊞ Transmission Control Protocol, Src Port: 443 (443), Dst Port: 58313 (58313), Seq: 156, Ack: 3, Len: 0
```

```
0000  f4 06 69 96 9a 10 3c 08  f6 21 a0 80 08 00 45 00   ..i...<. .!....E.
0010  00 28 8e 29 00 00 36 06  31 a5 d8 3a c0 04 0a 55   .(.)..6. 1..:...U
0020  22 6e 01 bb e3 c9 91 3a  ef 83 4d 55 eb a4 50 10   "n.....: ..MU..P.
0030  01 69 4a 2c 00 00 00 00  00 00 00 00               .iJ,.... ....
```

Internet Protocol Version 4 (ip), 20 bytes | Packets: 104782 · Displayed: 104782 (100.0%) | Profile: Default

c. What filtering rule can you use on your sniffer so that it will display only Ethernet frames that contain your computer’s IP address? Submit a screenshot with this filter in effect.

Ans: ip.src==10.85.34.110


Capturing from 5 interfaces [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save
Profile: Default
3:40 PM
7/22/2015

Filter: ip.src==10.85.34.110

```
No.  Time       Source                   Destination              Protocol Length Info
3977 81.8779670 10.85.34.110             54.215.241.186           ICMP     74 Echo (ping) request  id=0x0001, seq=2007/55047, ttl=255 (reply in 3978)
3979 81.8938060 10.85.34.110             54.215.241.186           ICMP     74 Echo (ping) request  id=0x0001, seq=2008/55303, ttl=255 (reply in 3980)
4461 93.9870260 10.85.34.110             74.125.224.95            TCP      55 [TCP Keep-Alive] 58318→443 [ACK] Seq=1 Ack=1 Win=258 Len=1
4648 98.6163470 10.85.34.110             10.85.104.218            UDP      94 Source port: 61743  Destination port: 58217
4649 98.6167560 2001:0:9d38:90d7:3c      2001:0:9d38:90d7:20      IPv6     98 IPv6 no next header
4657 98.8460130 10.85.34.110             184.85.230.245           TCP      55 [TCP Keep-Alive] 58330→443 [ACK] Seq=1 Ack=1 Win=254 Len=1
4659 98.8491020 10.85.34.110             10.85.104.218            UDP      94 Source port: 61743  Destination port: 58217
4660 98.8493510 10.85.34.110             10.85.104.218            UDP      94 Source port: 61743  Destination port: 58217
4690 99.4170210 10.85.34.110             204.102.114.49           TCP      55 [TCP Keep-Alive] 58324→80 [ACK] Seq=1 Ack=1 Win=256 Len=1
4695 99.4349330 10.85.34.110             204.102.114.49           TCP      55 [TCP Keep-Alive] 58322→80 [ACK] Seq=1 Ack=1 Win=259 Len=1
4696 99.4349330 10.85.34.110             204.102.114.49           TCP      55 [TCP Keep-Alive] 58321→80 [ACK] Seq=1 Ack=1 Win=255 Len=1
4697 99.4370690 10.85.34.110             204.102.114.49           TCP      55 [TCP Keep-Alive] 58320→80 [ACK] Seq=1 Ack=1 Win=256 Len=1
4701 99.4460750 10.85.34.110             204.102.114.49           TCP      55 [TCP Keep-Alive] 58319→80 [ACK] Seq=1 Ack=1 Win=254 Len=1
4703 99.5261450 10.85.34.110             184.85.230.245           TCP      55 [TCP Keep-Alive] 58329→80 [ACK] Seq=1 Ack=1 Win=259 Len=1
4707 99.6268870 10.85.34.110             184.85.230.245           TCP      55 [TCP Keep-Alive] 58325→80 [ACK] Seq=1 Ack=1 Win=259 Len=1
4710 99.6450190 10.85.34.110             184.85.230.245           TCP      55 [TCP Keep-Alive] 58328→80 [ACK] Seq=1 Ack=1 Win=259 Len=1
4712 99.6871440 10.85.34.110             184.85.230.245           TCP      55 [TCP Keep-Alive] 58337→80 [ACK] Seq=1 Ack=1 Win=259 Len=1
4714 99.7050010 10.85.34.110             184.85.230.245           TCP      55 [TCP Keep-Alive] 58336→80 [ACK] Seq=1 Ack=1 Win=259 Len=1
4715 99.7052550 10.85.34.110             184.85.230.245           TCP      55 [TCP Keep-Alive] 58335→80 [ACK] Seq=1 Ack=1 Win=259 Len=1
4718 99.7149970 10.85.34.110             184.85.230.245           TCP      55 [TCP Keep-Alive] 58331→80 [ACK] Seq=1 Ack=1 Win=259 Len=1
4719 99.7170340 10.85.34.110             184.85.230.245           TCP      55 [TCP Keep-Alive] 58338→80 [ACK] Seq=1 Ack=1 Win=259 Len=1
4722 99.7372110 10.85.34.110             184.85.230.245           TCP      55 [TCP Keep-Alive] 58326→80 [ACK] Seq=1 Ack=1 Win=257 Len=1
4726 99.7651020 10.85.34.110             184.85.230.245           TCP      55 [TCP Keep-Alive] 58327→80 [ACK] Seq=1 Ack=1 Win=256 Len=1
4733 99.9678790 10.85.34.110             74.125.224.65            TCP      55 [TCP Keep-Alive] 58340→443 [ACK] Seq=1 Ack=1 Win=256 Len=1
```

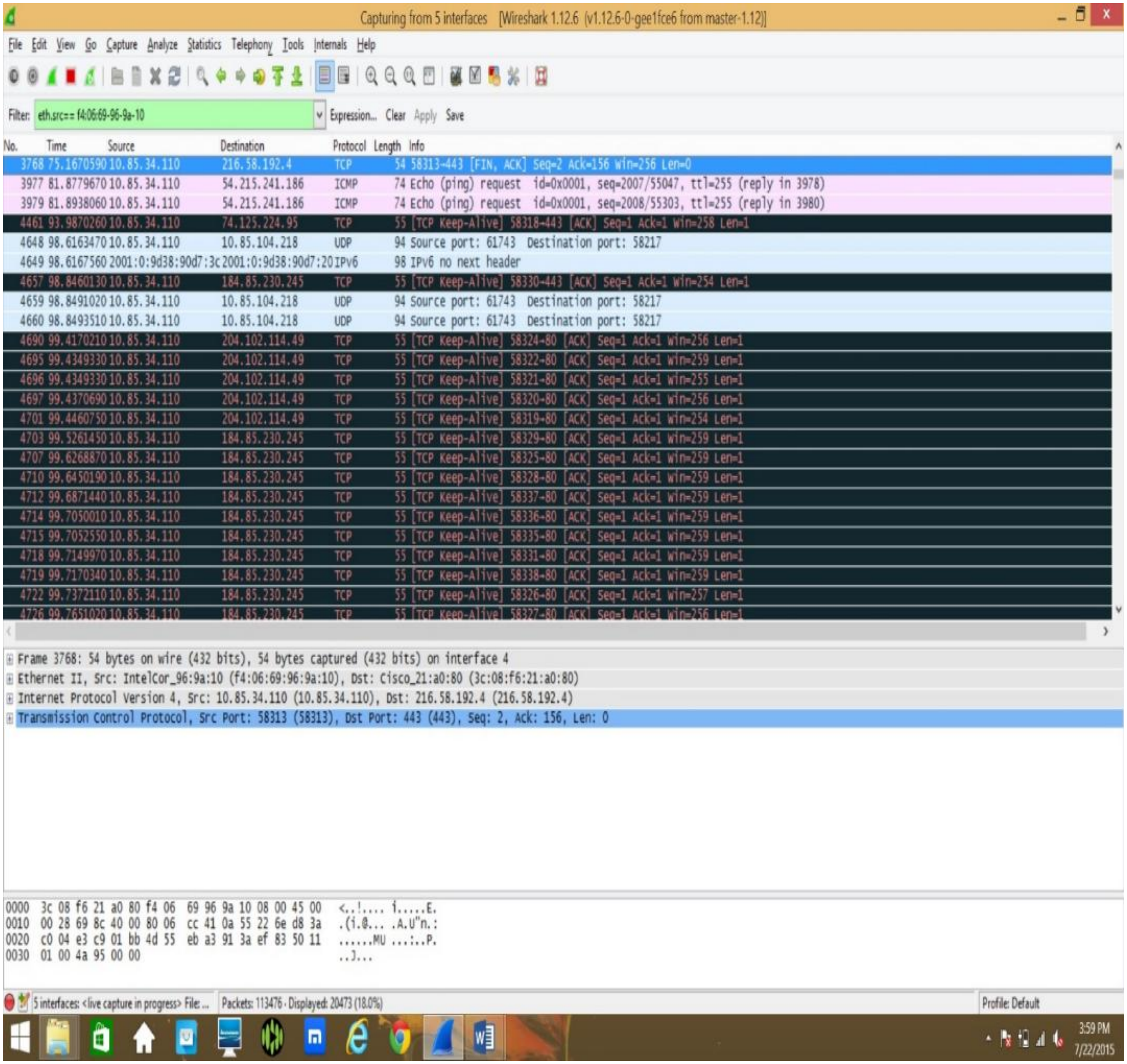
```
⊞ Frame 3977: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 4
⊞ Ethernet II, Src: IntelCor_96:9a:10 (f4:06:69:96:9a:10), Dst: Cisco_21:a0:80 (3c:08:f6:21:a0:80)
⊞ Internet Protocol Version 4, Src: 10.85.34.110 (10.85.34.110), Dst: 54.215.241.186 (54.215.241.186)
⊞ Internet Control Message Protocol
```

```
0000  3c 08 f6 21 a0 80 f4 06  69 96 9a 10 08 00 45 00   <..!.... i.....E.
0010  00 3c 29 51 00 00 ff 01  3d 1b 0a 55 22 6e 36 d7   .<)Q.... =..U"n6.
0020  f1 ba 08 00 c9 56 00 01  07 d7 44 61 74 61 20 42   .....V.. ..Data B
0030  75 66 66 65 72 00 00 00  00 00 00 00 00 00 00 00   uffer... ........
0040  00 00 00 00 00 00 00 00  00 00                     ........ ..
```

5 interfaces: <live capture in progress> File: ... Packets: 78935 · Displayed: 13199 (16.7%)

d. What filtering rule can you use on your sniffer so that it will display only Ethernet frames that contain your computer’s Ethernet address in the Ethernet frame header? Submit a screenshot with this filter in effect.

Ans: eth.src== f4:06:69-96-9a-10



Capturing from 5 interfaces [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: eth.src== f4:06:69-96-9a-10

```
No.  Time       Source                  Destination             Protocol Length Info
3768 75.1670590 10.85.34.110            216.58.192.4            TCP      54 58313→443 [FIN, ACK] Seq=2 Ack=156 Win=256 Len=0
3977 81.8779670 10.85.34.110            54.215.241.186          ICMP     74 Echo (ping) request  id=0x0001, seq=2007/55047, ttl=255 (reply in 3978)
3979 81.8938060 10.85.34.110            54.215.241.186          ICMP     74 Echo (ping) request  id=0x0001, seq=2008/55303, ttl=255 (reply in 3980)
4461 93.9870260 10.85.34.110            74.125.224.95           TCP      55 [TCP Keep-Alive] 58318→443 [ACK] Seq=1 Ack=1 Win=258 Len=1
4648 98.6163470 10.85.34.110            10.85.104.218           UDP      94 Source port: 61743  Destination port: 58217
4649 98.6167560 2001:0:9d38:90d7:3c     2001:0:9d38:90d7:20     IPv6     98 IPv6 no next header
4657 98.8460130 10.85.34.110            184.85.230.245          TCP      55 [TCP Keep-Alive] 58330→443 [ACK] Seq=1 Ack=1 Win=254 Len=1
4659 98.8491020 10.85.34.110            10.85.104.218           UDP      94 Source port: 61743  Destination port: 58217
4660 98.8493510 10.85.34.110            10.85.104.218           UDP      94 Source port: 61743  Destination port: 58217
4690 99.4170210 10.85.34.110            204.102.114.49          TCP      55 [TCP Keep-Alive] 58324→80 [ACK] Seq=1 Ack=1 Win=256 Len=1
4695 99.4349330 10.85.34.110            204.102.114.49          TCP      55 [TCP Keep-Alive] 58322→80 [ACK] Seq=1 Ack=1 Win=259 Len=1
4696 99.4349330 10.85.34.110            204.102.114.49          TCP      55 [TCP Keep-Alive] 58321→80 [ACK] Seq=1 Ack=1 Win=255 Len=1
4697 99.4370690 10.85.34.110            204.102.114.49          TCP      55 [TCP Keep-Alive] 58320→80 [ACK] Seq=1 Ack=1 Win=256 Len=1
4701 99.4460750 10.85.34.110            204.102.114.49          TCP      55 [TCP Keep-Alive] 58319→80 [ACK] Seq=1 Ack=1 Win=254 Len=1
4703 99.5261450 10.85.34.110            184.85.230.245          TCP      55 [TCP Keep-Alive] 58329→80 [ACK] Seq=1 Ack=1 Win=259 Len=1
4707 99.6268870 10.85.34.110            184.85.230.245          TCP      55 [TCP Keep-Alive] 58325→80 [ACK] Seq=1 Ack=1 Win=259 Len=1
4710 99.6450190 10.85.34.110            184.85.230.245          TCP      55 [TCP Keep-Alive] 58328→80 [ACK] Seq=1 Ack=1 Win=259 Len=1
4712 99.6871440 10.85.34.110            184.85.230.245          TCP      55 [TCP Keep-Alive] 58337→80 [ACK] Seq=1 Ack=1 Win=259 Len=1
4714 99.7050010 10.85.34.110            184.85.230.245          TCP      55 [TCP Keep-Alive] 58336→80 [ACK] Seq=1 Ack=1 Win=259 Len=1
4715 99.7052550 10.85.34.110            184.85.230.245          TCP      55 [TCP Keep-Alive] 58335→80 [ACK] Seq=1 Ack=1 Win=259 Len=1
4718 99.7149970 10.85.34.110            184.85.230.245          TCP      55 [TCP Keep-Alive] 58331→80 [ACK] Seq=1 Ack=1 Win=259 Len=1
4719 99.7170340 10.85.34.110            184.85.230.245          TCP      55 [TCP Keep-Alive] 58338→80 [ACK] Seq=1 Ack=1 Win=259 Len=1
4722 99.7372110 10.85.34.110            184.85.230.245          TCP      55 [TCP Keep-Alive] 58326→80 [ACK] Seq=1 Ack=1 Win=257 Len=1
4726 99.7651020 10.85.34.110            184.85.230.245          TCP      55 [TCP Keep-Alive] 58327→80 [ACK] Seq=1 Ack=1 Win=256 Len=1
```

```
⊞ Frame 3768: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 4
⊞ Ethernet II, Src: IntelCor_96:9a:10 (f4:06:69:96:9a:10), Dst: Cisco_21:a0:80 (3c:08:f6:21:a0:80)
⊞ Internet Protocol Version 4, Src: 10.85.34.110 (10.85.34.110), Dst: 216.58.192.4 (216.58.192.4)
⊞ Transmission Control Protocol, Src Port: 58313 (58313), Dst Port: 443 (443), Seq: 2, Ack: 156, Len: 0
```

```
0000  3c 08 f6 21 a0 80 f4 06  69 96 9a 10 08 00 45 00   <..!.... i.....E.
0010  00 28 69 8c 40 00 80 06  cc 41 0a 55 22 6e d8 3a   .(i.@... .A.U"n.:
0020  c0 04 e3 c9 01 bb 4d 55  eb a3 91 3a ef 83 50 11   ......MU ...:..P.
0030  01 00 4a 95 00 00                                  ..J...
```

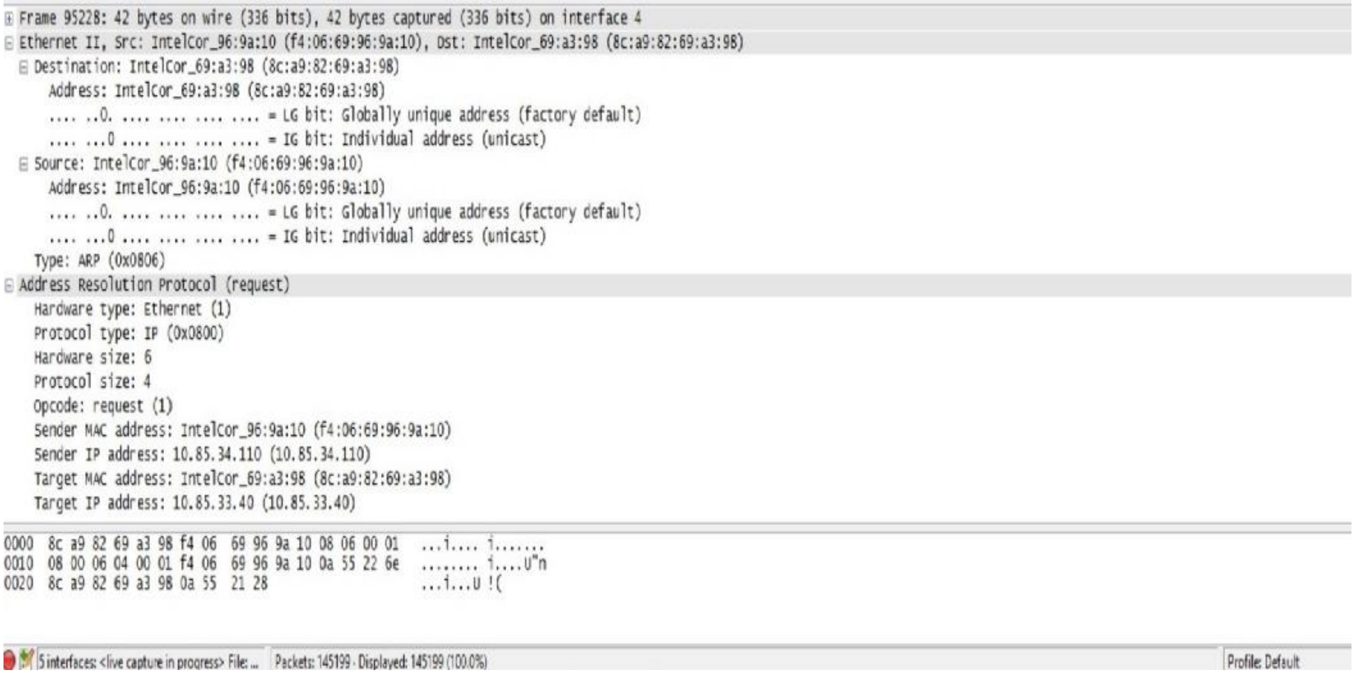
5 interfaces: <live capture in progress> File: ... Packets: 113476 · Displayed: 20473 (18.0%) Profile: Default

2. Capture and decode an **ARP request** and the corresponding **ARP reply** packet. You may need to initially clear your ARP cache (arp –d) in command prompt window (cmd.exe) before generating an ARP packet.

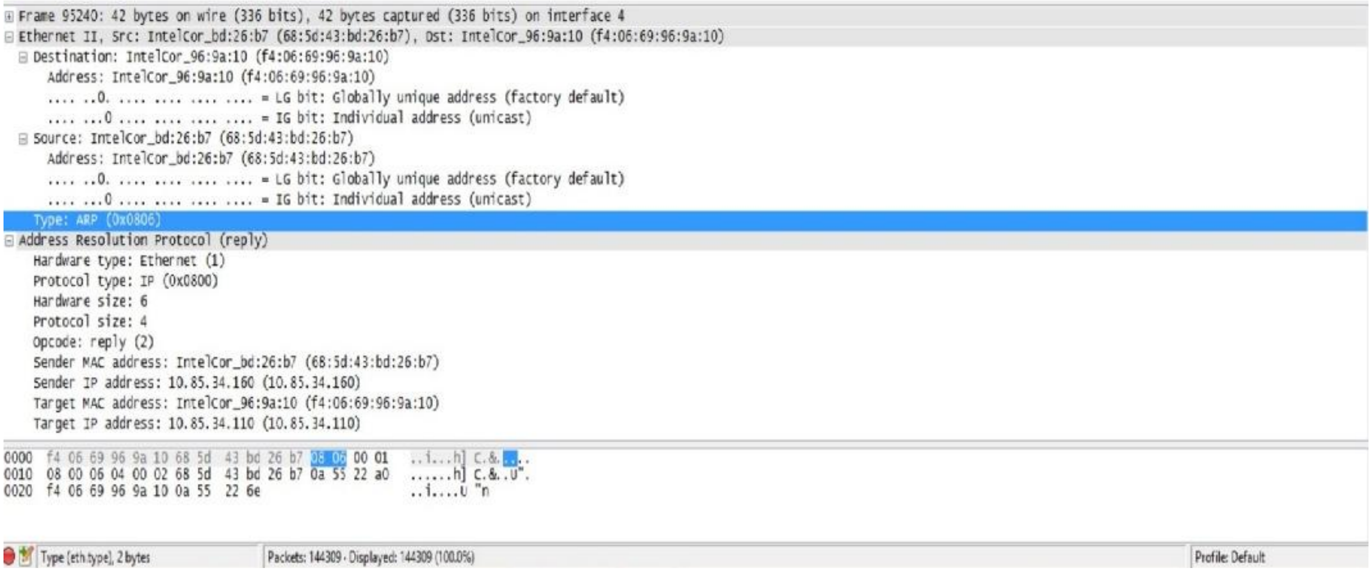
   a. What is the hexadecimal value the field in Ethernet frame header that is used to identify that the packet is an ARP packet? Submit screenshot with this value circled.

Ans:

- ARP=0X0806(TYPE:ARP)
- OPCODE :request(0X0001)
- OPCODE :reply(0X0002)



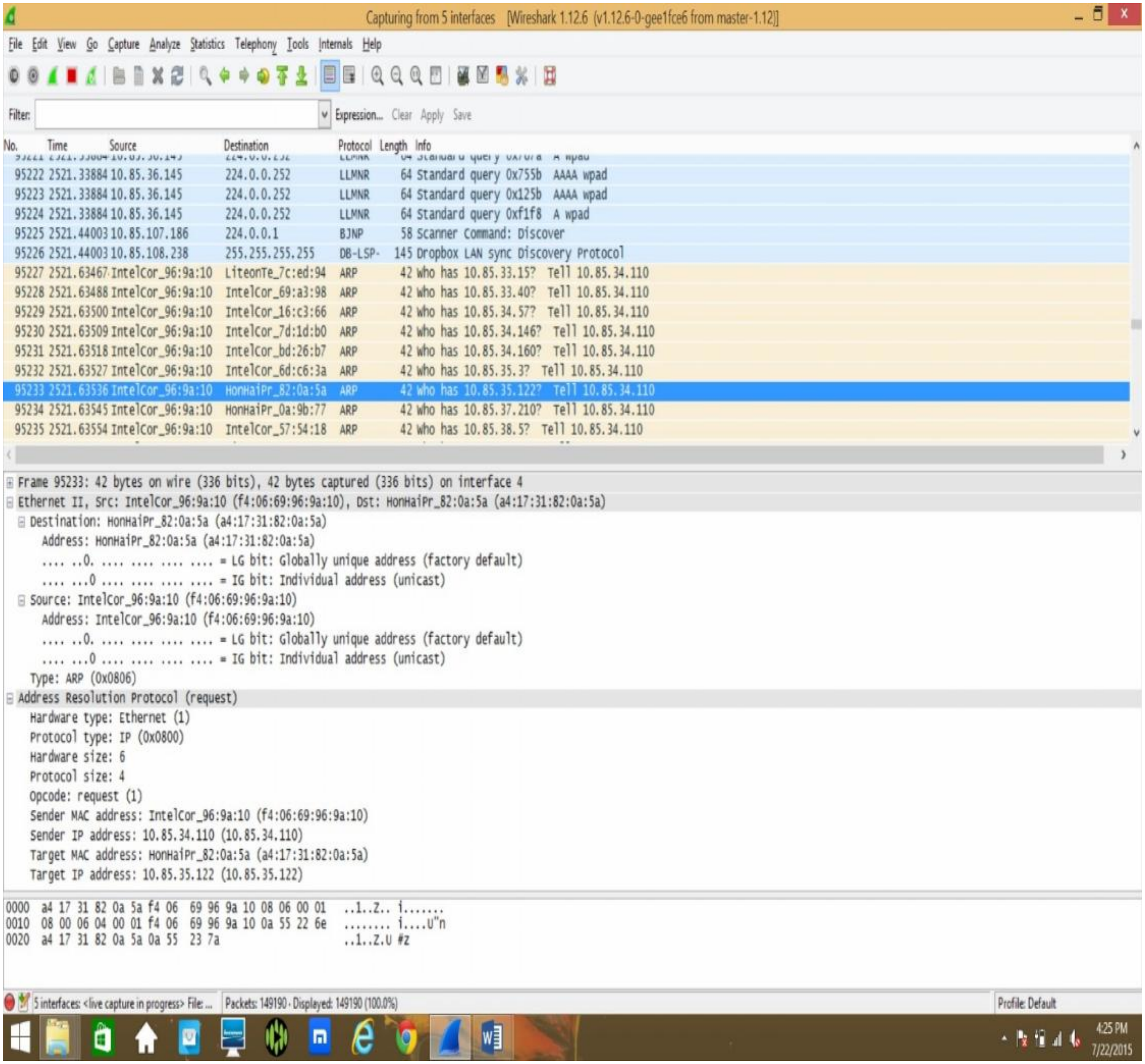
```
⊞ Frame 95228: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 4
⊟ Ethernet II, Src: IntelCor_96:9a:10 (f4:06:69:96:9a:10), Dst: IntelCor_69:a3:98 (8c:a9:82:69:a3:98)
  ⊟ Destination: IntelCor_69:a3:98 (8c:a9:82:69:a3:98)
      Address: IntelCor_69:a3:98 (8c:a9:82:69:a3:98)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ⊟ Source: IntelCor_96:9a:10 (f4:06:69:96:9a:10)
      Address: IntelCor_96:9a:10 (f4:06:69:96:9a:10)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
⊟ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: IntelCor_96:9a:10 (f4:06:69:96:9a:10)
    Sender IP address: 10.85.34.110 (10.85.34.110)
    Target MAC address: IntelCor_69:a3:98 (8c:a9:82:69:a3:98)
    Target IP address: 10.85.33.40 (10.85.33.40)

0000  8c a9 82 69 a3 98 f4 06  69 96 9a 10 08 06 00 01   ...i.... i.......
0010  08 00 06 04 00 01 f4 06  69 96 9a 10 0a 55 22 6e   ........ i....U"n
0020  8c a9 82 69 a3 98 0a 55  21 28                     ...i...U !(

5 interfaces: <live capture in progress> File: ...   Packets: 145199 · Displayed: 145199 (100.0%)   Profile: Default
```



```
⊞ Frame 95240: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 4
⊟ Ethernet II, Src: IntelCor_bd:26:b7 (68:5d:43:bd:26:b7), Dst: IntelCor_96:9a:10 (f4:06:69:96:9a:10)
  ⊟ Destination: IntelCor_96:9a:10 (f4:06:69:96:9a:10)
      Address: IntelCor_96:9a:10 (f4:06:69:96:9a:10)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ⊟ Source: IntelCor_bd:26:b7 (68:5d:43:bd:26:b7)
      Address: IntelCor_bd:26:b7 (68:5d:43:bd:26:b7)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
⊟ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: IntelCor_bd:26:b7 (68:5d:43:bd:26:b7)
    Sender IP address: 10.85.34.160 (10.85.34.160)
    Target MAC address: IntelCor_96:9a:10 (f4:06:69:96:9a:10)
    Target IP address: 10.85.34.110 (10.85.34.110)

0000  f4 06 69 96 9a 10 68 5d  43 bd 26 b7 08 06 00 01   ..i...h] C.&.....
0010  08 00 06 04 00 02 68 5d  43 bd 26 b7 0a 55 22 a0   ......h] C.&..U".
0020  f4 06 69 96 9a 10 0a 55  22 6e                     ..i....U "n

Type (eth.type), 2 bytes   Packets: 144309 · Displayed: 144309 (100.0%)   Profile: Default
```

b. Turn in screenshots which show the two types of ARP packets decoded.

Ans:

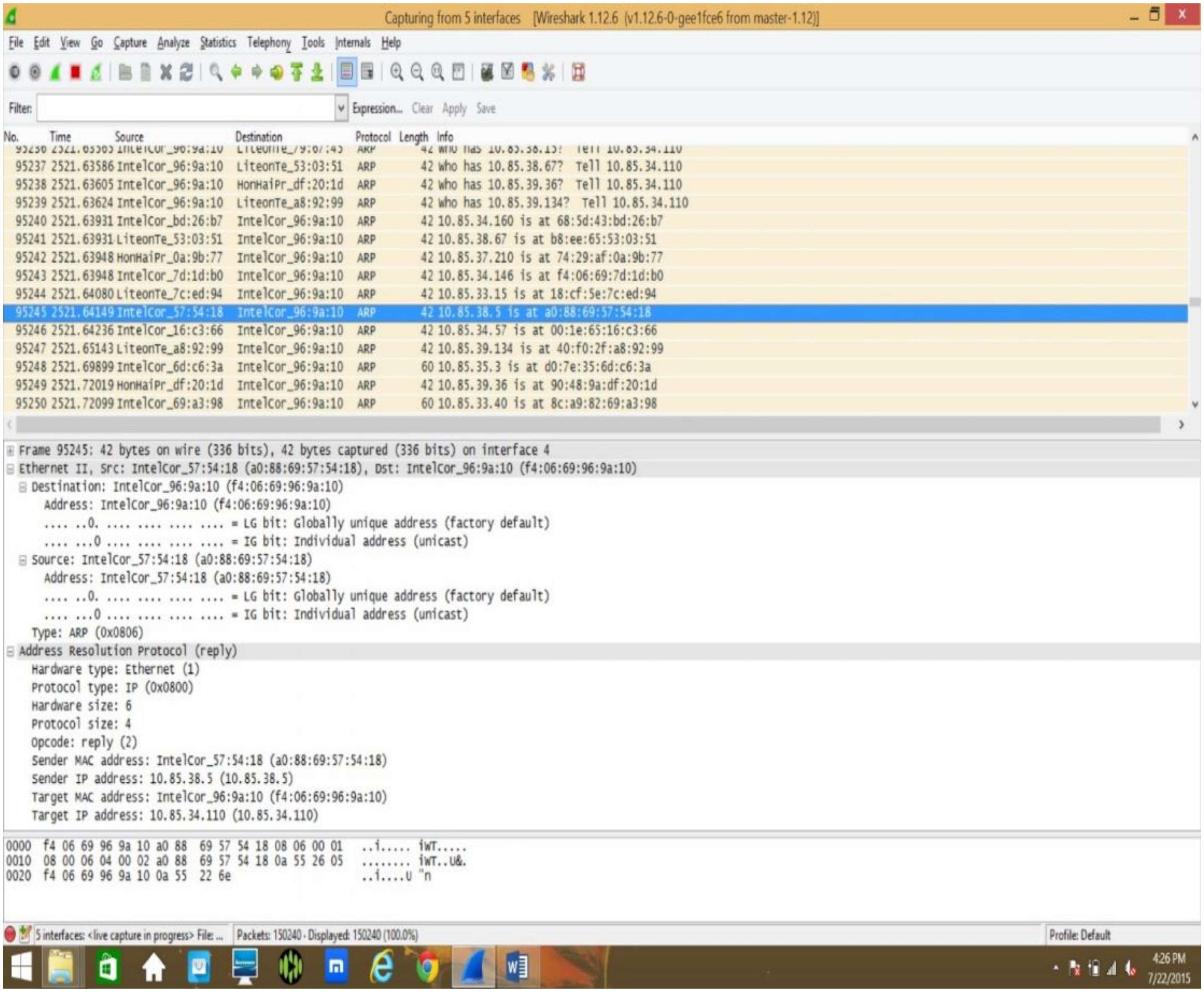

Capturing from 5 interfaces [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
Profile: Default
4:25 PM
7/22/2015

```
No.   Time        Source              Destination        Protocol Length Info
95222 2521.33884 10.85.36.145        224.0.0.252        LLMNR     64 Standard query 0x755b  AAAA wpad
95223 2521.33884 10.85.36.145        224.0.0.252        LLMNR     64 Standard query 0x125b  AAAA wpad
95224 2521.33884 10.85.36.145        224.0.0.252        LLMNR     64 Standard query 0xf1f8  A wpad
95225 2521.44003 10.85.107.186       224.0.0.1          BJNP      58 Scanner Command: Discover
95226 2521.44003 10.85.108.238       255.255.255.255    DB-LSP-  145 Dropbox LAN sync Discovery Protocol
95227 2521.63467 IntelCor_96:9a:10   LiteonTe_7c:ed:94  ARP       42 Who has 10.85.33.15?  Tell 10.85.34.110
95228 2521.63488 IntelCor_96:9a:10   IntelCor_69:a3:98  ARP       42 Who has 10.85.33.40?  Tell 10.85.34.110
95229 2521.63500 IntelCor_96:9a:10   IntelCor_16:c3:66  ARP       42 Who has 10.85.34.57?  Tell 10.85.34.110
95230 2521.63509 IntelCor_96:9a:10   IntelCor_7d:1d:b0  ARP       42 Who has 10.85.34.146?  Tell 10.85.34.110
95231 2521.63518 IntelCor_96:9a:10   IntelCor_bd:26:b7  ARP       42 Who has 10.85.34.160?  Tell 10.85.34.110
95232 2521.63527 IntelCor_96:9a:10   IntelCor_6d:c6:3a  ARP       42 Who has 10.85.35.3?  Tell 10.85.34.110
95233 2521.63536 IntelCor_96:9a:10   HonHaiPr_82:0a:5a  ARP       42 Who has 10.85.35.122?  Tell 10.85.34.110
95234 2521.63545 IntelCor_96:9a:10   HonHaiPr_0a:9b:77  ARP       42 Who has 10.85.37.210?  Tell 10.85.34.110
95235 2521.63554 IntelCor_96:9a:10   IntelCor_57:54:18  ARP       42 Who has 10.85.38.5?  Tell 10.85.34.110
```

```
⊞ Frame 95233: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 4
⊟ Ethernet II, Src: IntelCor_96:9a:10 (f4:06:69:96:9a:10), Dst: HonHaiPr_82:0a:5a (a4:17:31:82:0a:5a)
  ⊟ Destination: HonHaiPr_82:0a:5a (a4:17:31:82:0a:5a)
      Address: HonHaiPr_82:0a:5a (a4:17:31:82:0a:5a)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ⊟ Source: IntelCor_96:9a:10 (f4:06:69:96:9a:10)
      Address: IntelCor_96:9a:10 (f4:06:69:96:9a:10)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
⊟ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: IntelCor_96:9a:10 (f4:06:69:96:9a:10)
    Sender IP address: 10.85.34.110 (10.85.34.110)
    Target MAC address: HonHaiPr_82:0a:5a (a4:17:31:82:0a:5a)
    Target IP address: 10.85.35.122 (10.85.35.122)
```

```
0000  a4 17 31 82 0a 5a f4 06  69 96 9a 10 08 06 00 01   ..1..Z.. i.......
0010  08 00 06 04 00 01 f4 06  69 96 9a 10 0a 55 22 6e   ........ i....U"n
0020  a4 17 31 82 0a 5a 0a 55  23 7a                     ..1..Z.U #z
```

5 interfaces: <live capture in progress> File: ... Packets: 149190 · Displayed: 149190 (100.0%)


Capturing from 5 interfaces   [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
5 interfaces: <live capture in progress> File: ...
Packets: 150240 · Displayed: 150240 (100.0%)
Profile: Default
4:26 PM
7/22/2015

```
No.   Time       Source            Destination       Protocol Length Info
95236 2521.63565 IntelCor_96:9a:10 LiteonTe_79:67:45 ARP      42 who has 10.85.38.15?  Tell 10.85.34.110
95237 2521.63586 IntelCor_96:9a:10 LiteonTe_53:03:51 ARP      42 who has 10.85.38.67?  Tell 10.85.34.110
95238 2521.63605 IntelCor_96:9a:10 HonHaiPr_df:20:1d ARP      42 who has 10.85.39.36?  Tell 10.85.34.110
95239 2521.63624 IntelCor_96:9a:10 LiteonTe_a8:92:99 ARP      42 who has 10.85.39.134?  Tell 10.85.34.110
95240 2521.63931 IntelCor_bd:26:b7 IntelCor_96:9a:10 ARP      42 10.85.34.160 is at 68:5d:43:bd:26:b7
95241 2521.63931 LiteonTe_53:03:51 IntelCor_96:9a:10 ARP      42 10.85.38.67 is at b8:ee:65:53:03:51
95242 2521.63948 HonHaiPr_0a:9b:77 IntelCor_96:9a:10 ARP      42 10.85.37.210 is at 74:29:af:0a:9b:77
95243 2521.63948 IntelCor_7d:1d:b0 IntelCor_96:9a:10 ARP      42 10.85.34.146 is at f4:06:69:7d:1d:b0
95244 2521.64080 LiteonTe_7c:ed:94 IntelCor_96:9a:10 ARP      42 10.85.33.15 is at 18:cf:5e:7c:ed:94
95245 2521.64149 IntelCor_57:54:18 IntelCor_96:9a:10 ARP      42 10.85.38.5 is at a0:88:69:57:54:18
95246 2521.64236 IntelCor_16:c3:66 IntelCor_96:9a:10 ARP      42 10.85.34.57 is at 00:1e:65:16:c3:66
95247 2521.65143 LiteonTe_a8:92:99 IntelCor_96:9a:10 ARP      42 10.85.39.134 is at 40:f0:2f:a8:92:99
95248 2521.69899 IntelCor_6d:c6:3a IntelCor_96:9a:10 ARP      60 10.85.35.3 is at d0:7e:35:6d:c6:3a
95249 2521.72019 HonHaiPr_df:20:1d IntelCor_96:9a:10 ARP      42 10.85.39.36 is at 90:48:9a:df:20:1d
95250 2521.72099 IntelCor_69:a3:98 IntelCor_96:9a:10 ARP      60 10.85.33.40 is at 8c:a9:82:69:a3:98
```

```
⊞ Frame 95245: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 4
⊟ Ethernet II, Src: IntelCor_57:54:18 (a0:88:69:57:54:18), Dst: IntelCor_96:9a:10 (f4:06:69:96:9a:10)
  ⊟ Destination: IntelCor_96:9a:10 (f4:06:69:96:9a:10)
      Address: IntelCor_96:9a:10 (f4:06:69:96:9a:10)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ⊟ Source: IntelCor_57:54:18 (a0:88:69:57:54:18)
      Address: IntelCor_57:54:18 (a0:88:69:57:54:18)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
⊟ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: IntelCor_57:54:18 (a0:88:69:57:54:18)
    Sender IP address: 10.85.38.5 (10.85.38.5)
    Target MAC address: IntelCor_96:9a:10 (f4:06:69:96:9a:10)
    Target IP address: 10.85.34.110 (10.85.34.110)
```

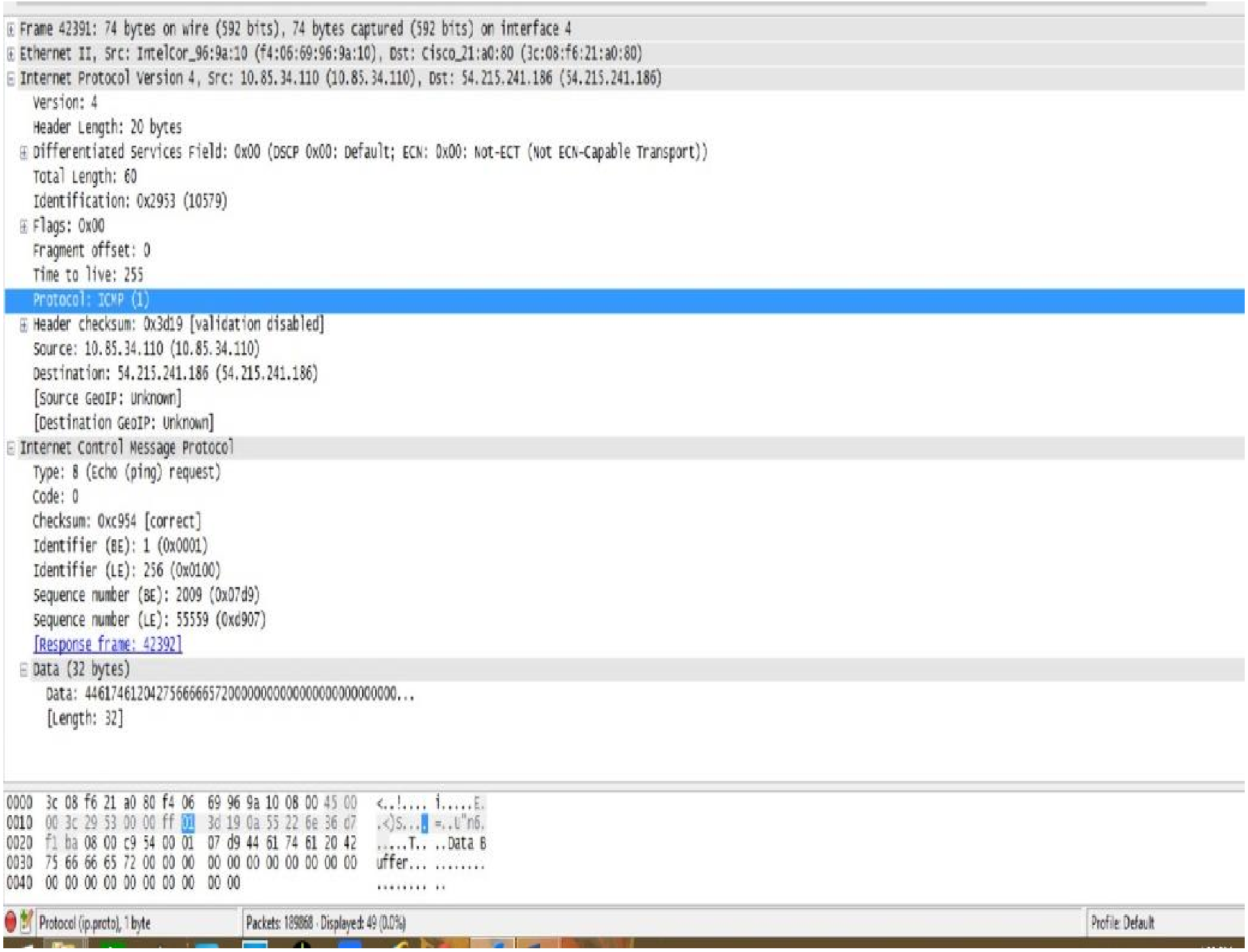
```
0000  f4 06 69 96 9a 10 a0 88  69 57 54 18 08 06 00 01   ..i..... iWT.....
0010  08 00 06 04 00 02 a0 88  69 57 54 18 0a 55 26 05   ........ iWT..U&.
0020  f4 06 69 96 9a 10 0a 55  22 6e                     ..i....U "n
```

3. Capture and decode an **ICMP echo request** and the corresponding **ICMP echo reply** packet by running the ping command.

   a. What is the decimal value of the protocol field in IP header that is used to indicate that the packet is an ICMP packet? Submit screenshot with this value circled.

   Ans: Decimal value of the protocol field in IP header:

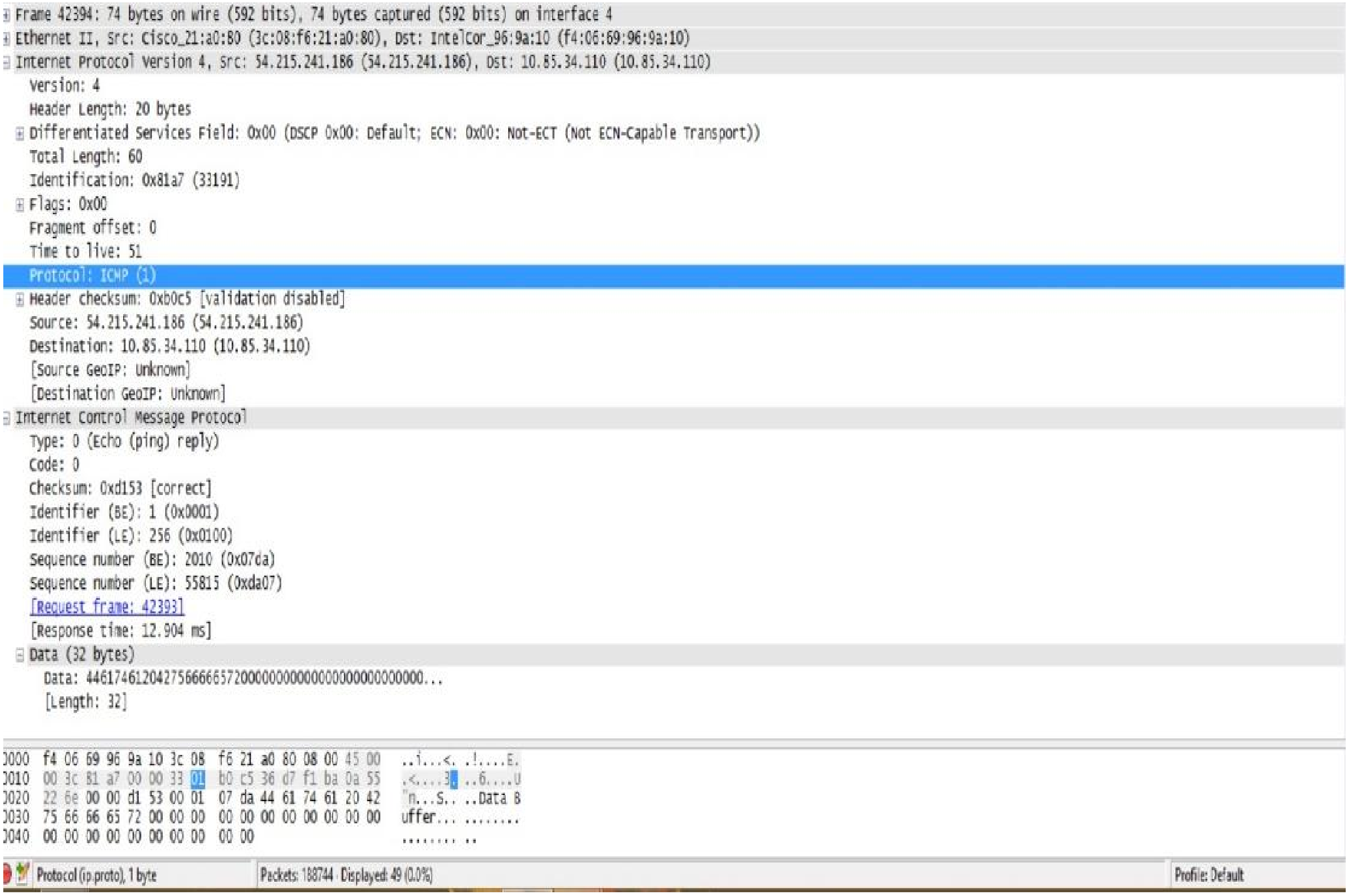
   - *For ICMP echo request:* 0x01 = = 0000 0001 = = 1



```
⊞ Frame 42391: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 4
⊞ Ethernet II, Src: IntelCor_96:9a:10 (f4:06:69:96:9a:10), Dst: Cisco_21:a0:80 (3c:08:f6:21:a0:80)
⊟ Internet Protocol Version 4, Src: 10.85.34.110 (10.85.34.110), Dst: 54.215.241.186 (54.215.241.186)
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 60
    Identification: 0x2953 (10579)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (1)
  ⊞ Header checksum: 0x3d19 [validation disabled]
    Source: 10.85.34.110 (10.85.34.110)
    Destination: 54.215.241.186 (54.215.241.186)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊟ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xc954 [correct]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 2009 (0x07d9)
    Sequence number (LE): 55559 (0xd907)
    [Response frame: 42392]
  ⊟ Data (32 bytes)
      Data: 446174612042756666657200000000000000000000000000...
      [Length: 32]

0000  3c 08 f6 21 a0 80 f4 06  69 96 9a 10 08 00 45 00   <..!.... i.....E.
0010  00 3c 29 53 00 00 ff 01  3d 19 0a 55 22 6e 36 d7   .<)S.... =..U"n6.
0020  f1 ba 08 00 c9 54 00 01  07 d9 44 61 74 61 20 42   .....T.. ..Data B
0030  75 66 66 65 72 00 00 00  00 00 00 00 00 00 00 00   uffer... ........
0040  00 00 00 00 00 00 00 00  00 00                     ........ ..
```

Protocol (ip.proto), 1 byte
Packets: 189868 · Displayed: 49 (0.0%)
Profile: Default

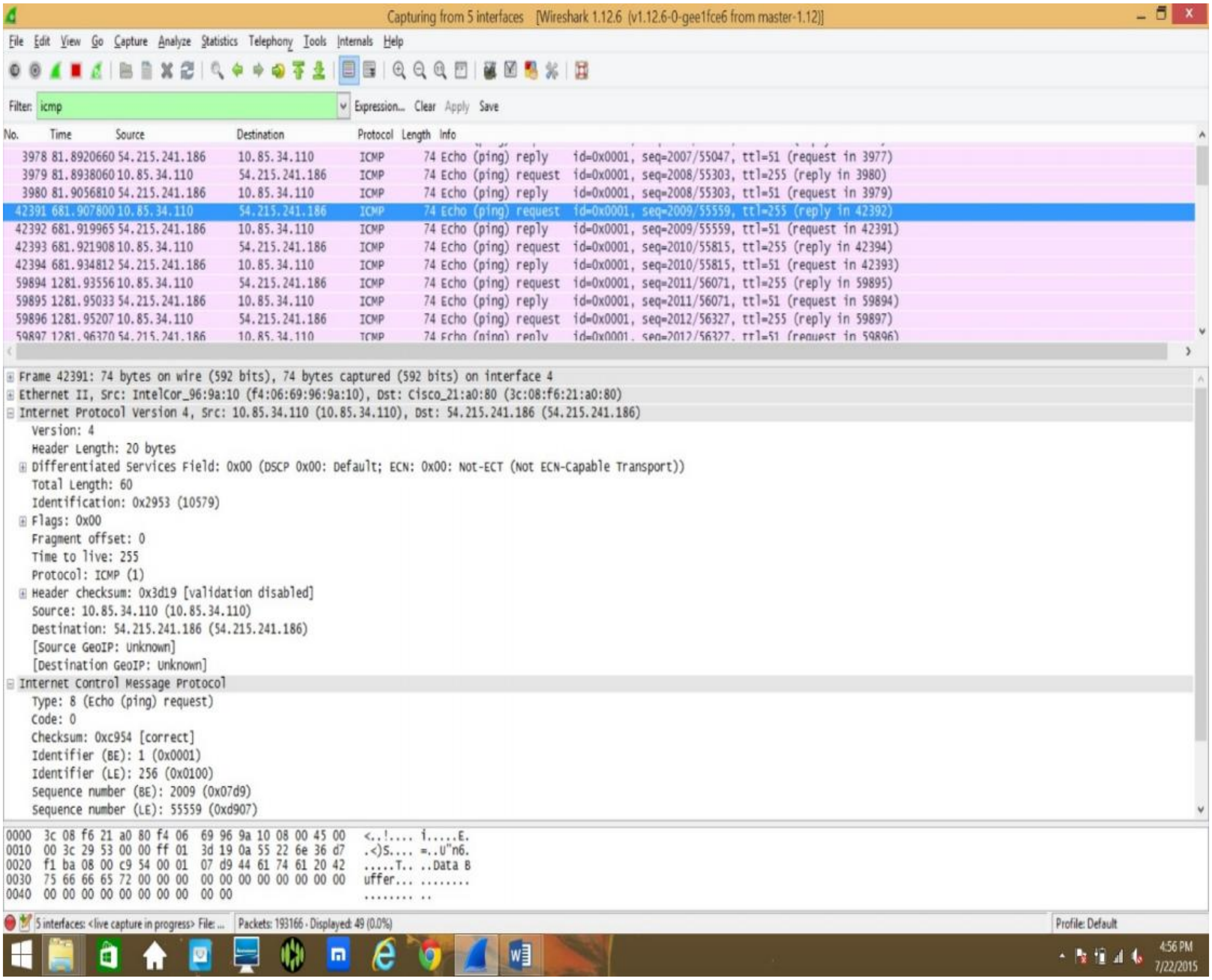
- *For ICMP echo reply: 0*x01 = = 0000 0001 = = 1



```
⊞ Frame 42394: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 4
⊞ Ethernet II, Src: Cisco_21:a0:80 (3c:08:f6:21:a0:80), Dst: IntelCor_96:9a:10 (f4:06:69:96:9a:10)
⊟ Internet Protocol Version 4, Src: 54.215.241.186 (54.215.241.186), Dst: 10.85.34.110 (10.85.34.110)
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 60
    Identification: 0x81a7 (33191)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 51
    Protocol: ICMP (1)
  ⊞ Header checksum: 0xb0c5 [validation disabled]
    Source: 54.215.241.186 (54.215.241.186)
    Destination: 10.85.34.110 (10.85.34.110)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊟ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xd153 [correct]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 2010 (0x07da)
    Sequence number (LE): 55815 (0xda07)
    [Request frame: 42393]
    [Response time: 12.904 ms]
  ⊟ Data (32 bytes)
      Data: 446174612042756666657200000000000000000000000000...
      [Length: 32]

0000  f4 06 69 96 9a 10 3c 08  f6 21 a0 80 08 00 45 00   ..i...<. .!....E.
0010  00 3c 81 a7 00 00 33 01  b0 c5 36 d7 f1 ba 0a 55   .<....3. ..6....U
0020  22 6e 00 00 d1 53 00 01  07 da 44 61 74 61 20 42   "n...S.. ..Data B
0030  75 66 66 65 72 00 00 00  00 00 00 00 00 00 00 00   uffer... ........
0040  00 00 00 00 00 00 00 00  00 00                     ........ ..

Protocol (ip.proto), 1 byte    Packets: 188744 · Displayed: 49 (0.0%)    Profile: Default
```

b. Turn in screenshots which show the two types of ICMP packets decoded.

Ans:

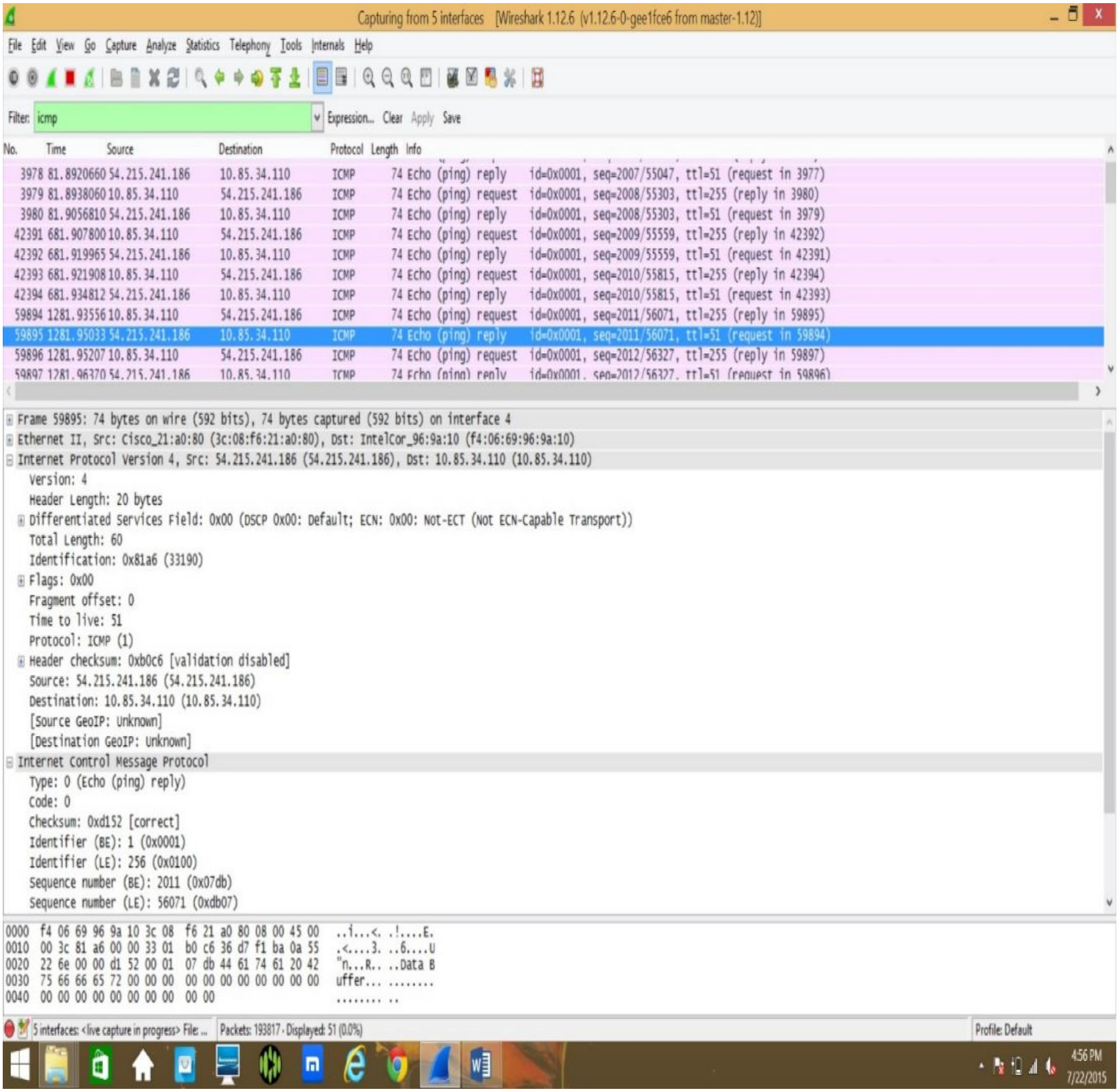

Capturing from 5 interfaces [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: icmp
Expression... Clear Apply Save

```
No.   Time        Source          Destination     Protocol Length Info
 3978 81.8920660 54.215.241.186  10.85.34.110    ICMP     74 Echo (ping) reply    id=0x0001, seq=2007/55047, ttl=51 (request in 3977)
 3979 81.8938060 10.85.34.110    54.215.241.186  ICMP     74 Echo (ping) request  id=0x0001, seq=2008/55303, ttl=255 (reply in 3980)
 3980 81.9056810 54.215.241.186  10.85.34.110    ICMP     74 Echo (ping) reply    id=0x0001, seq=2008/55303, ttl=51 (request in 3979)
42391 681.907800 10.85.34.110    54.215.241.186  ICMP     74 Echo (ping) request  id=0x0001, seq=2009/55559, ttl=255 (reply in 42392)
42392 681.919965 54.215.241.186  10.85.34.110    ICMP     74 Echo (ping) reply    id=0x0001, seq=2009/55559, ttl=51 (request in 42391)
42393 681.921908 10.85.34.110    54.215.241.186  ICMP     74 Echo (ping) request  id=0x0001, seq=2010/55815, ttl=255 (reply in 42394)
42394 681.934812 54.215.241.186  10.85.34.110    ICMP     74 Echo (ping) reply    id=0x0001, seq=2010/55815, ttl=51 (request in 42393)
59894 1281.93556 10.85.34.110    54.215.241.186  ICMP     74 Echo (ping) request  id=0x0001, seq=2011/56071, ttl=255 (reply in 59895)
59895 1281.95033 54.215.241.186  10.85.34.110    ICMP     74 Echo (ping) reply    id=0x0001, seq=2011/56071, ttl=51 (request in 59894)
59896 1281.95207 10.85.34.110    54.215.241.186  ICMP     74 Echo (ping) request  id=0x0001, seq=2012/56327, ttl=255 (reply in 59897)
59897 1281.96370 54.215.241.186  10.85.34.110    ICMP     74 Echo (ping) reply    id=0x0001, seq=2012/56327, ttl=51 (request in 59896)
```

```
⊞ Frame 42391: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 4
⊞ Ethernet II, Src: IntelCor_96:9a:10 (f4:06:69:96:9a:10), Dst: Cisco_21:a0:80 (3c:08:f6:21:a0:80)
⊟ Internet Protocol Version 4, Src: 10.85.34.110 (10.85.34.110), Dst: 54.215.241.186 (54.215.241.186)
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 60
    Identification: 0x2953 (10579)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (1)
  ⊞ Header checksum: 0x3d19 [validation disabled]
    Source: 10.85.34.110 (10.85.34.110)
    Destination: 54.215.241.186 (54.215.241.186)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊟ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xc954 [correct]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 2009 (0x07d9)
    Sequence number (LE): 55559 (0xd907)
```

```
0000  3c 08 f6 21 a0 80 f4 06  69 96 9a 10 08 00 45 00   <..!.... i.....E.
0010  00 3c 29 53 00 00 ff 01  3d 19 0a 55 22 6e 36 d7   .<)S.... =..U"n6.
0020  f1 ba 08 00 c9 54 00 01  07 d9 44 61 74 61 20 42   .....T.. ..Data B
0030  75 66 66 65 72 00 00 00  00 00 00 00 00 00 00 00   uffer... ........
0040  00 00 00 00 00 00 00 00  00 00                     ........ ..
```

5 interfaces: <live capture in progress> File: ...
Packets: 193166 · Displayed: 49 (0.0%)
Profile: Default
4:56 PM
7/22/2015


Capturing from 5 interfaces [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: icmp

```
No.   Time        Source          Destination     Protocol Length Info
 3978 81.8920660  54.215.241.186  10.85.34.110    ICMP     74 Echo (ping) reply    id=0x0001, seq=2007/55047, ttl=51 (request in 3977)
 3979 81.8938060  10.85.34.110    54.215.241.186  ICMP     74 Echo (ping) request  id=0x0001, seq=2008/55303, ttl=255 (reply in 3980)
 3980 81.9056810  54.215.241.186  10.85.34.110    ICMP     74 Echo (ping) reply    id=0x0001, seq=2008/55303, ttl=51 (request in 3979)
42391 681.907800  10.85.34.110    54.215.241.186  ICMP     74 Echo (ping) request  id=0x0001, seq=2009/55559, ttl=255 (reply in 42392)
42392 681.919965  54.215.241.186  10.85.34.110    ICMP     74 Echo (ping) reply    id=0x0001, seq=2009/55559, ttl=51 (request in 42391)
42393 681.921908  10.85.34.110    54.215.241.186  ICMP     74 Echo (ping) request  id=0x0001, seq=2010/55815, ttl=255 (reply in 42394)
42394 681.934812  54.215.241.186  10.85.34.110    ICMP     74 Echo (ping) reply    id=0x0001, seq=2010/55815, ttl=51 (request in 42393)
59894 1281.93556  10.85.34.110    54.215.241.186  ICMP     74 Echo (ping) request  id=0x0001, seq=2011/56071, ttl=255 (reply in 59895)
59895 1281.95033  54.215.241.186  10.85.34.110    ICMP     74 Echo (ping) reply    id=0x0001, seq=2011/56071, ttl=51 (request in 59894)
59896 1281.95207  10.85.34.110    54.215.241.186  ICMP     74 Echo (ping) request  id=0x0001, seq=2012/56327, ttl=255 (reply in 59897)
59897 1281.96370  54.215.241.186  10.85.34.110    ICMP     74 Echo (ping) reply    id=0x0001, seq=2012/56327, ttl=51 (request in 59896)
```

```
⊞ Frame 59895: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 4
⊞ Ethernet II, Src: Cisco_21:a0:80 (3c:08:f6:21:a0:80), Dst: IntelCor_96:9a:10 (f4:06:69:96:9a:10)
⊟ Internet Protocol Version 4, Src: 54.215.241.186 (54.215.241.186), Dst: 10.85.34.110 (10.85.34.110)
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 60
    Identification: 0x81a6 (33190)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 51
    Protocol: ICMP (1)
  ⊞ Header checksum: 0xb0c6 [validation disabled]
    Source: 54.215.241.186 (54.215.241.186)
    Destination: 10.85.34.110 (10.85.34.110)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊟ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xd152 [correct]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 2011 (0x07db)
    Sequence number (LE): 56071 (0xdb07)
```

```
0000  f4 06 69 96 9a 10 3c 08  f6 21 a0 80 08 00 45 00   ..i...<. .!....E.
0010  00 3c 81 a6 00 00 33 01  b0 c6 36 d7 f1 ba 0a 55   .<....3. ..6....U
0020  22 6e 00 00 d1 52 00 01  07 db 44 61 74 61 20 42   "n...R.. ..Data B
0030  75 66 66 65 72 00 00 00  00 00 00 00 00 00 00 00   uffer... ........
0040  00 00 00 00 00 00 00 00  00 00                     ........ ..
```

5 interfaces: <live capture in progress> File: ...

Packets: 193817 · Displayed: 51 (0.0%)

Profile: Default

4. On your Windows computer, capture and decode packets generated by a tracert command from your lab computer to www.calstatela.edu.

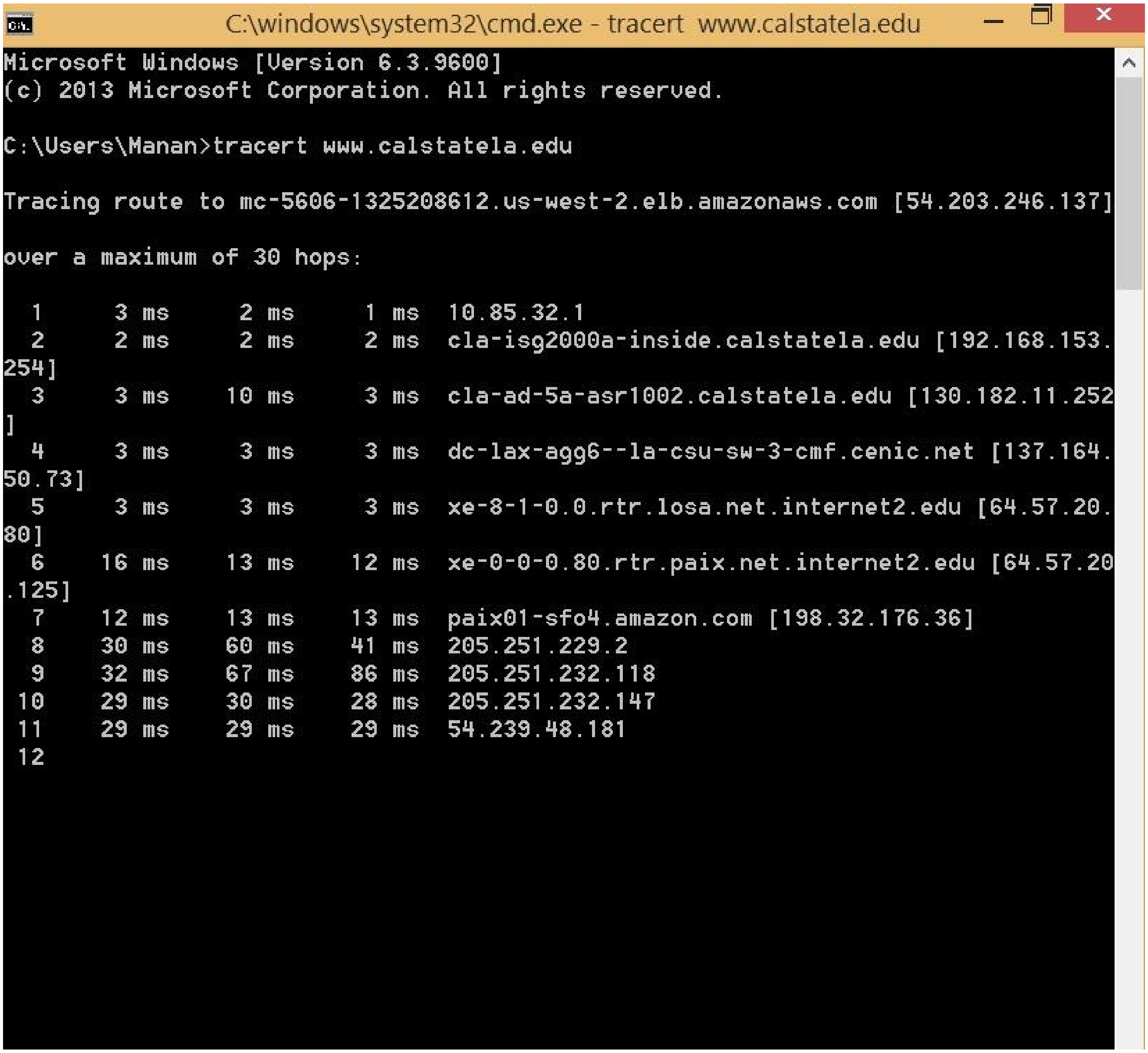
   a. What does tracert command do to its ICMP packets that will cause the routers to reply with ICMP messages?

Ans: tracert command is used to find the router level path for from our computer to a remote computer with the help of ICMP packets to reply with ICMP messages and used to increase the TTL.

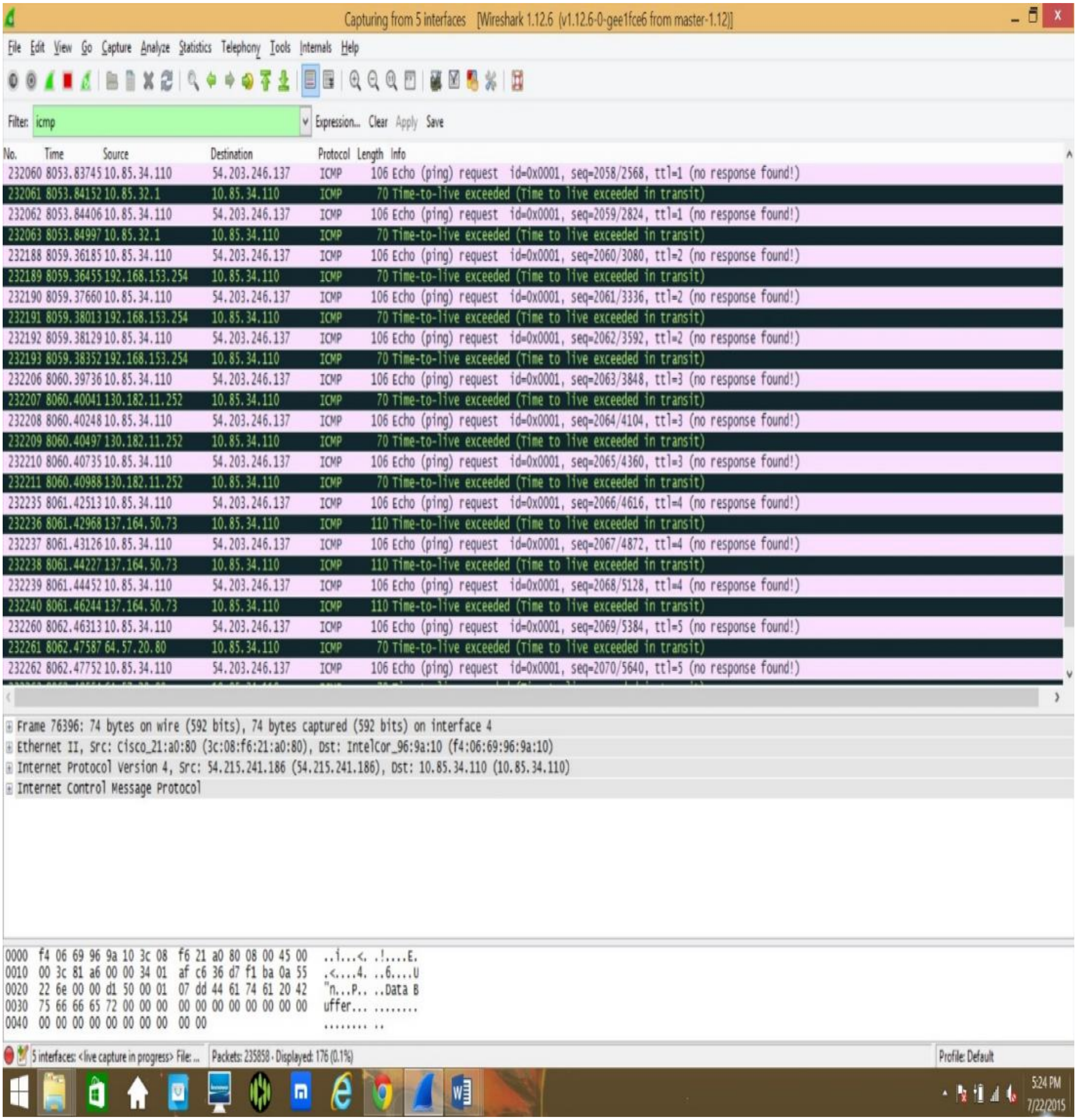
Tracert finds the path by sending echo request with a TTL of 1 and incrementing the TTL by 1 on each transmission until target host reaches the maximum hops.

   b. Turn in screenshots which show tracert packets decoded.

Ans:



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Manan>tracert www.calstatela.edu

Tracing route to mc-5606-1325208612.us-west-2.elb.amazonaws.com [54.203.246.137]

over a maximum of 30 hops:

  1     3 ms     2 ms     1 ms  10.85.32.1
  2     2 ms     2 ms     2 ms  cla-isg2000a-inside.calstatela.edu [192.168.153.
254]
  3     3 ms    10 ms     3 ms  cla-ad-5a-asr1002.calstatela.edu [130.182.11.252
]
  4     3 ms     3 ms     3 ms  dc-lax-agg6--la-csu-sw-3-cmf.cenic.net [137.164.
50.73]
  5     3 ms     3 ms     3 ms  xe-8-1-0.0.rtr.losa.net.internet2.edu [64.57.20.
80]
  6    16 ms    13 ms    12 ms  xe-0-0-0.80.rtr.paix.net.internet2.edu [64.57.20
.125]
  7    12 ms    13 ms    13 ms  paix01-sfo4.amazon.com [198.32.176.36]
  8    30 ms    60 ms    41 ms  205.251.229.2
  9    32 ms    67 ms    86 ms  205.251.232.118
 10    29 ms    30 ms    28 ms  205.251.232.147
 11    29 ms    29 ms    29 ms  54.239.48.181
 12
```


Capturing from 5 interfaces [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save
Profile: Default
5:24 PM
7/22/2015

Filter: icmp

```
No.    Time       Source           Destination     Protocol Length Info
232060 8053.83745 10.85.34.110     54.203.246.137  ICMP     106 Echo (ping) request  id=0x0001, seq=2058/2568, ttl=1 (no response found!)
232061 8053.84152 10.85.32.1       10.85.34.110    ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
232062 8053.84406 10.85.34.110     54.203.246.137  ICMP     106 Echo (ping) request  id=0x0001, seq=2059/2824, ttl=1 (no response found!)
232063 8053.84997 10.85.32.1       10.85.34.110    ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
232188 8059.36185 10.85.34.110     54.203.246.137  ICMP     106 Echo (ping) request  id=0x0001, seq=2060/3080, ttl=2 (no response found!)
232189 8059.36455 192.168.153.254  10.85.34.110    ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
232190 8059.37660 10.85.34.110     54.203.246.137  ICMP     106 Echo (ping) request  id=0x0001, seq=2061/3336, ttl=2 (no response found!)
232191 8059.38013 192.168.153.254  10.85.34.110    ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
232192 8059.38129 10.85.34.110     54.203.246.137  ICMP     106 Echo (ping) request  id=0x0001, seq=2062/3592, ttl=2 (no response found!)
232193 8059.38352 192.168.153.254  10.85.34.110    ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
232206 8060.39736 10.85.34.110     54.203.246.137  ICMP     106 Echo (ping) request  id=0x0001, seq=2063/3848, ttl=3 (no response found!)
232207 8060.40041 130.182.11.252   10.85.34.110    ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
232208 8060.40248 10.85.34.110     54.203.246.137  ICMP     106 Echo (ping) request  id=0x0001, seq=2064/4104, ttl=3 (no response found!)
232209 8060.40497 130.182.11.252   10.85.34.110    ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
232210 8060.40735 10.85.34.110     54.203.246.137  ICMP     106 Echo (ping) request  id=0x0001, seq=2065/4360, ttl=3 (no response found!)
232211 8060.40988 130.182.11.252   10.85.34.110    ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
232235 8061.42513 10.85.34.110     54.203.246.137  ICMP     106 Echo (ping) request  id=0x0001, seq=2066/4616, ttl=4 (no response found!)
232236 8061.42968 137.164.50.73    10.85.34.110    ICMP     110 Time-to-live exceeded (Time to live exceeded in transit)
232237 8061.43126 10.85.34.110     54.203.246.137  ICMP     106 Echo (ping) request  id=0x0001, seq=2067/4872, ttl=4 (no response found!)
232238 8061.44227 137.164.50.73    10.85.34.110    ICMP     110 Time-to-live exceeded (Time to live exceeded in transit)
232239 8061.44452 10.85.34.110     54.203.246.137  ICMP     106 Echo (ping) request  id=0x0001, seq=2068/5128, ttl=4 (no response found!)
232240 8061.46244 137.164.50.73    10.85.34.110    ICMP     110 Time-to-live exceeded (Time to live exceeded in transit)
232260 8062.46313 10.85.34.110     54.203.246.137  ICMP     106 Echo (ping) request  id=0x0001, seq=2069/5384, ttl=5 (no response found!)
232261 8062.47587 64.57.20.80      10.85.34.110    ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
232262 8062.47752 10.85.34.110     54.203.246.137  ICMP     106 Echo (ping) request  id=0x0001, seq=2070/5640, ttl=5 (no response found!)
```

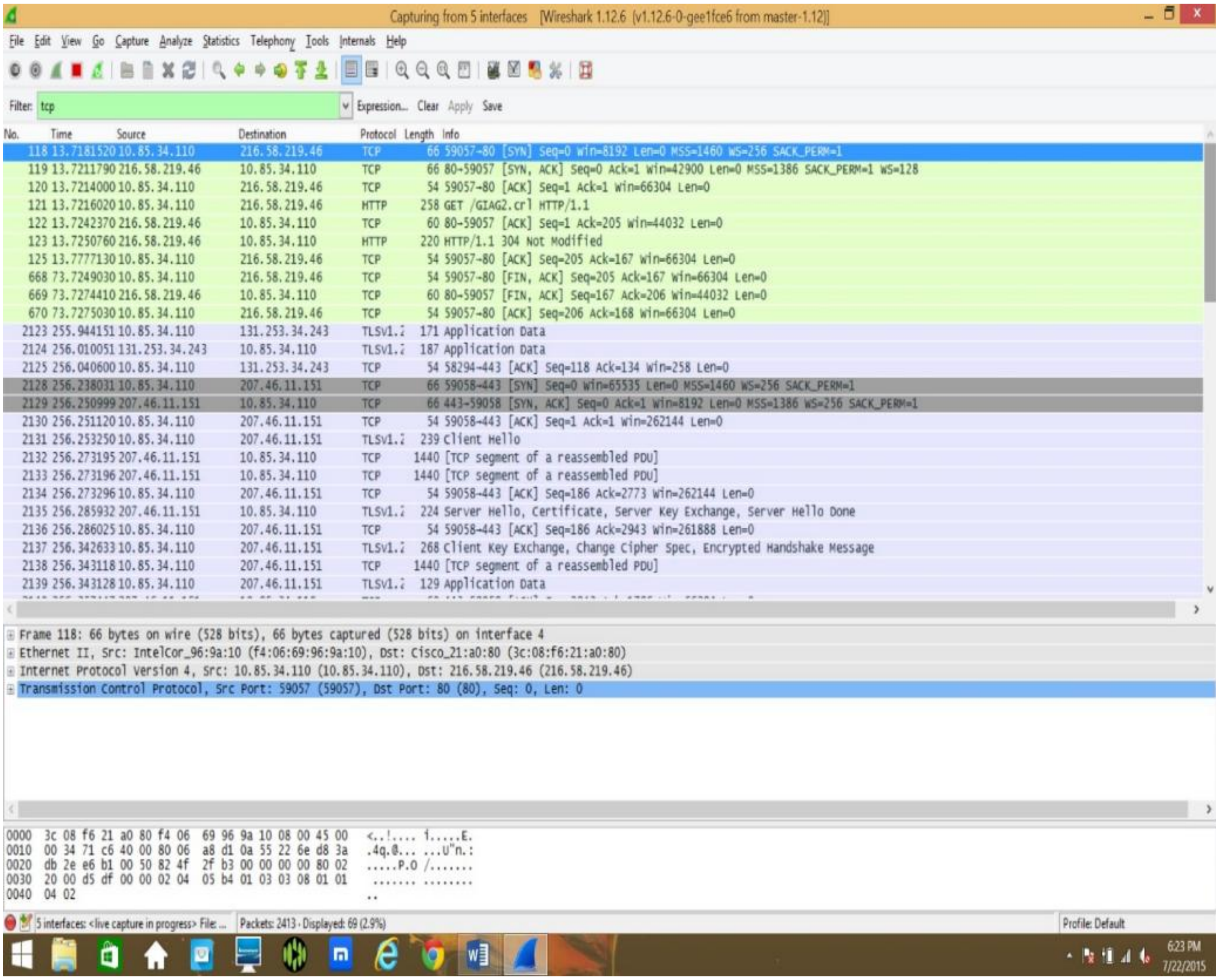
```
⊞ Frame 76396: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 4
⊞ Ethernet II, Src: Cisco_21:a0:80 (3c:08:f6:21:a0:80), Dst: IntelCor_96:9a:10 (f4:06:69:96:9a:10)
⊞ Internet Protocol Version 4, Src: 54.215.241.186 (54.215.241.186), Dst: 10.85.34.110 (10.85.34.110)
⊞ Internet Control Message Protocol
```

```
0000  f4 06 69 96 9a 10 3c 08  f6 21 a0 80 08 00 45 00   ..i...<. .!....E.
0010  00 3c 81 a6 00 00 34 01  af c6 36 d7 f1 ba 0a 55   .<....4. ..6....U
0020  22 6e 00 00 d1 50 00 01  07 dd 44 61 74 61 20 42   "n...P.. ..Data B
0030  75 66 66 65 72 00 00 00  00 00 00 00 00 00 00 00   uffer... ........
0040  00 00 00 00 00 00 00 00  00 00                     ........ ..
```

```
5 interfaces: <live capture in progress> File: ...   Packets: 235858 · Displayed: 176 (0.1%)
```

5.

6. Capture and decode packets associated with a http session. Provide screenshots to support your answer.



Capturing from 5 interfaces [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: tcp
Expression... Clear Apply Save
5 interfaces: <live capture in progress> File: ...
Packets: 2413 · Displayed: 69 (2.9%)
Profile: Default
6:23 PM
7/22/2015

```
No.  Time        Source          Destination      Protocol Length Info
 118 13.7181520 10.85.34.110    216.58.219.46    TCP        66 59057→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
 119 13.7211790 216.58.219.46   10.85.34.110     TCP        66 80→59057 [SYN, ACK] Seq=0 Ack=1 Win=42900 Len=0 MSS=1386 SACK_PERM=1 WS=128
 120 13.7214000 10.85.34.110    216.58.219.46    TCP        54 59057→80 [ACK] Seq=1 Ack=1 Win=66304 Len=0
 121 13.7216020 10.85.34.110    216.58.219.46    HTTP      258 GET /GIAG2.crl HTTP/1.1
 122 13.7242370 216.58.219.46   10.85.34.110     TCP        60 80→59057 [ACK] Seq=1 Ack=205 Win=44032 Len=0
 123 13.7250760 216.58.219.46   10.85.34.110     HTTP      220 HTTP/1.1 304 Not Modified
 125 13.7777130 10.85.34.110    216.58.219.46    TCP        54 59057→80 [ACK] Seq=205 Ack=167 Win=66304 Len=0
 668 73.7249030 10.85.34.110    216.58.219.46    TCP        54 59057→80 [FIN, ACK] Seq=205 Ack=167 Win=66304 Len=0
 669 73.7274410 216.58.219.46   10.85.34.110     TCP        60 80→59057 [FIN, ACK] Seq=167 Ack=206 Win=44032 Len=0
 670 73.7275030 10.85.34.110    216.58.219.46    TCP        54 59057→80 [ACK] Seq=206 Ack=168 Win=66304 Len=0
2123 255.944151 10.85.34.110    131.253.34.243   TLSv1.2   171 Application Data
2124 256.010051 131.253.34.243  10.85.34.110     TLSv1.2   187 Application Data
2125 256.040600 10.85.34.110    131.253.34.243   TCP        54 58294→443 [ACK] Seq=118 Ack=134 Win=258 Len=0
2128 256.238031 10.85.34.110    207.46.11.151    TCP        66 59058→443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
2129 256.250999 207.46.11.151   10.85.34.110     TCP        66 443→59058 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1386 WS=256 SACK_PERM=1
2130 256.251120 10.85.34.110    207.46.11.151    TCP        54 59058→443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
2131 256.253250 10.85.34.110    207.46.11.151    TLSv1.2   239 Client Hello
2132 256.273195 207.46.11.151   10.85.34.110     TCP      1440 [TCP segment of a reassembled PDU]
2133 256.273196 207.46.11.151   10.85.34.110     TCP      1440 [TCP segment of a reassembled PDU]
2134 256.273296 10.85.34.110    207.46.11.151    TCP        54 59058→443 [ACK] Seq=186 Ack=2773 Win=262144 Len=0
2135 256.285932 207.46.11.151   10.85.34.110     TLSv1.2   224 Server Hello, Certificate, Server Key Exchange, Server Hello Done
2136 256.286025 10.85.34.110    207.46.11.151    TCP        54 59058→443 [ACK] Seq=186 Ack=2943 Win=261888 Len=0
2137 256.342633 10.85.34.110    207.46.11.151    TLSv1.2   268 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2138 256.343118 10.85.34.110    207.46.11.151    TCP      1440 [TCP segment of a reassembled PDU]
2139 256.343128 10.85.34.110    207.46.11.151    TLSv1.2   129 Application Data
```

```
⊞ Frame 118: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 4
⊞ Ethernet II, Src: IntelCor_96:9a:10 (f4:06:69:96:9a:10), Dst: Cisco_21:a0:80 (3c:08:f6:21:a0:80)
⊞ Internet Protocol Version 4, Src: 10.85.34.110 (10.85.34.110), Dst: 216.58.219.46 (216.58.219.46)
⊞ Transmission Control Protocol, Src Port: 59057 (59057), Dst Port: 80 (80), Seq: 0, Len: 0
```

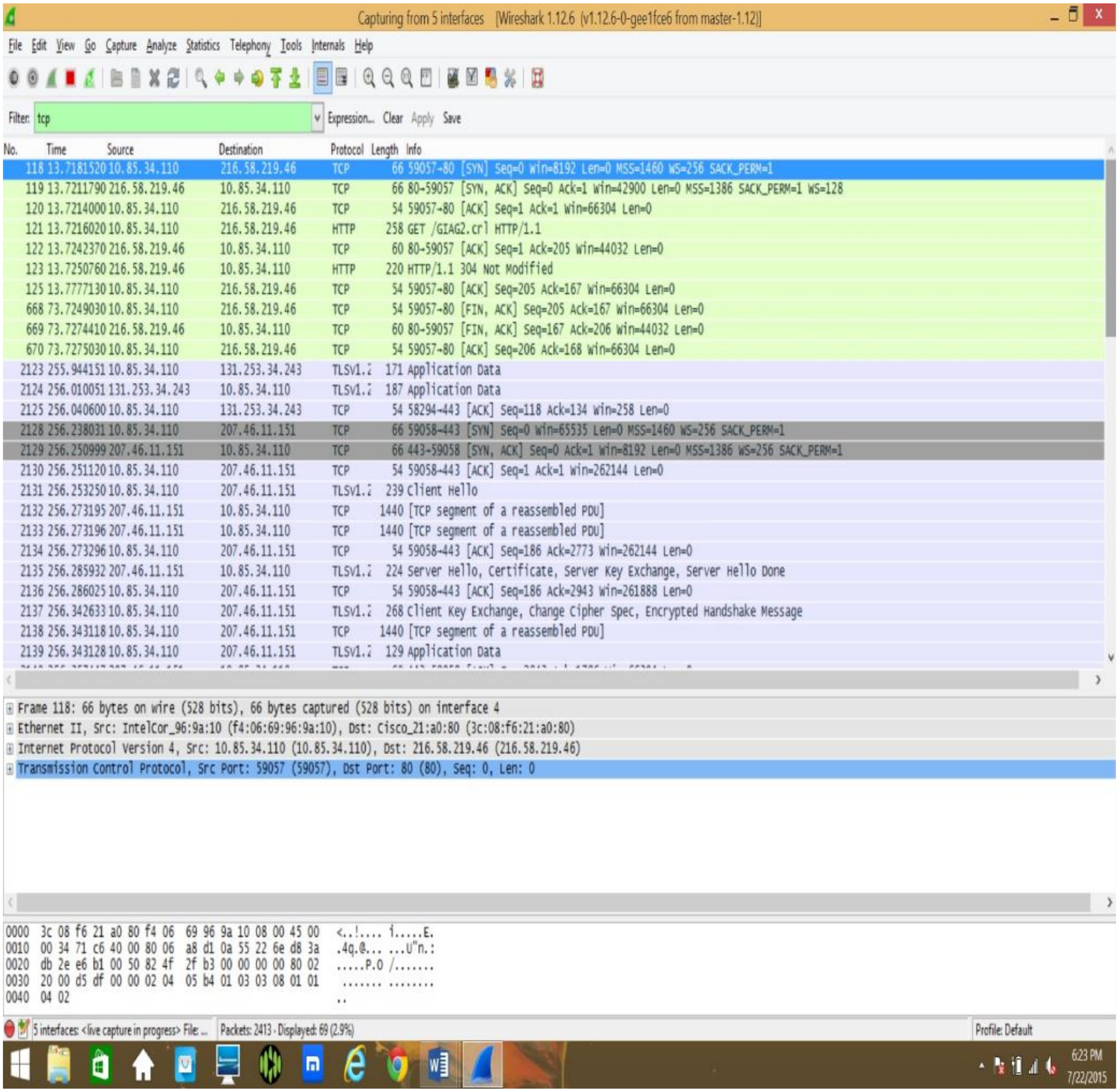
```
0000  3c 08 f6 21 a0 80 f4 06  69 96 9a 10 08 00 45 00   <..!.... i.....E.
0010  00 34 71 c6 40 00 80 06  a8 d1 0a 55 22 6e d8 3a   .4q.@... ...U"n.:
0020  db 2e e6 b1 00 50 82 4f  2f b3 00 00 00 00 80 02   .....P.O /.......
0030  20 00 d5 df 00 00 02 04  05 b4 01 03 03 08 01 01    ....... ........
0040  04 02                                              ..
```

a. Circle and Identify the packets on a screenshot that comprise the 3-way handshake used during startup of the TCP connection. What TCP flags were set to 1 during the 3-way handshake?

Ans: These are the 3-way handsake which is:

- SYN
- ACK
- SYN, ACK

⇨ tcp.flags.SYN==1



Capturing from 5 interfaces [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save
Profile: Default
6:23 PM
7/22/2015

Filter: tcp

```
No.     Time        Source          Destination     Protocol Length Info
    118 13.7181520 10.85.34.110    216.58.219.46   TCP        66 59057→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
    119 13.7211790 216.58.219.46   10.85.34.110    TCP        66 80→59057 [SYN, ACK] Seq=0 Ack=1 Win=42900 Len=0 MSS=1386 SACK_PERM=1 WS=128
    120 13.7214000 10.85.34.110    216.58.219.46   TCP        54 59057→80 [ACK] Seq=1 Ack=1 Win=66304 Len=0
    121 13.7216020 10.85.34.110    216.58.219.46   HTTP      258 GET /GIAG2.crl HTTP/1.1
    122 13.7242370 216.58.219.46   10.85.34.110    TCP        60 80→59057 [ACK] Seq=1 Ack=205 Win=44032 Len=0
    123 13.7250760 216.58.219.46   10.85.34.110    HTTP      220 HTTP/1.1 304 Not Modified
    125 13.7777130 10.85.34.110    216.58.219.46   TCP        54 59057→80 [ACK] Seq=205 Ack=167 Win=66304 Len=0
    668 73.7249030 10.85.34.110    216.58.219.46   TCP        54 59057→80 [FIN, ACK] Seq=205 Ack=167 Win=66304 Len=0
    669 73.7274410 216.58.219.46   10.85.34.110    TCP        60 80→59057 [FIN, ACK] Seq=167 Ack=206 Win=44032 Len=0
    670 73.7275030 10.85.34.110    216.58.219.46   TCP        54 59057→80 [ACK] Seq=206 Ack=168 Win=66304 Len=0
   2123 255.944151 10.85.34.110    131.253.34.243  TLSv1.2   171 Application Data
   2124 256.010051 131.253.34.243  10.85.34.110    TLSv1.2   187 Application Data
   2125 256.040600 10.85.34.110    131.253.34.243  TCP        54 58294→443 [ACK] Seq=118 Ack=134 Win=258 Len=0
   2128 256.238031 10.85.34.110    207.46.11.151   TCP        66 59058→443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
   2129 256.250999 207.46.11.151   10.85.34.110    TCP        66 443→59058 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1386 WS=256 SACK_PERM=1
   2130 256.251120 10.85.34.110    207.46.11.151   TCP        54 59058→443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
   2131 256.253250 10.85.34.110    207.46.11.151   TLSv1.2   239 Client Hello
   2132 256.273195 207.46.11.151   10.85.34.110    TCP      1440 [TCP segment of a reassembled PDU]
   2133 256.273196 207.46.11.151   10.85.34.110    TCP      1440 [TCP segment of a reassembled PDU]
   2134 256.273296 10.85.34.110    207.46.11.151   TCP        54 59058→443 [ACK] Seq=186 Ack=2773 Win=262144 Len=0
   2135 256.285932 207.46.11.151   10.85.34.110    TLSv1.2   224 Server Hello, Certificate, Server Key Exchange, Server Hello Done
   2136 256.286025 10.85.34.110    207.46.11.151   TCP        54 59058→443 [ACK] Seq=186 Ack=2943 Win=261888 Len=0
   2137 256.342633 10.85.34.110    207.46.11.151   TLSv1.2   268 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
   2138 256.343118 10.85.34.110    207.46.11.151   TCP      1440 [TCP segment of a reassembled PDU]
   2139 256.343128 10.85.34.110    207.46.11.151   TLSv1.2   129 Application Data
```

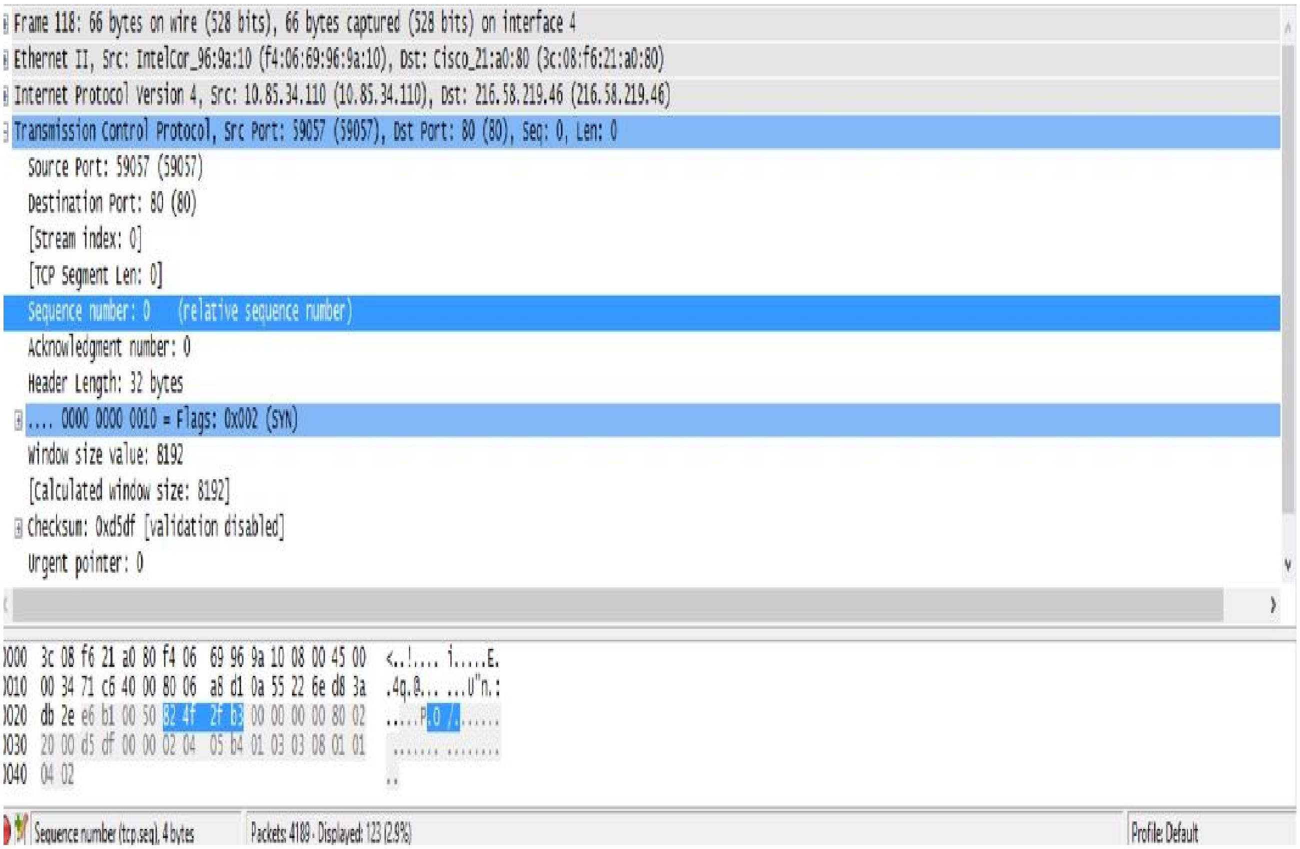
```
⊞ Frame 118: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 4
⊞ Ethernet II, Src: IntelCor_96:9a:10 (f4:06:69:96:9a:10), Dst: Cisco_21:a0:80 (3c:08:f6:21:a0:80)
⊞ Internet Protocol Version 4, Src: 10.85.34.110 (10.85.34.110), Dst: 216.58.219.46 (216.58.219.46)
⊞ Transmission Control Protocol, Src Port: 59057 (59057), Dst Port: 80 (80), Seq: 0, Len: 0
```

```
0000  3c 08 f6 21 a0 80 f4 06  69 96 9a 10 08 00 45 00   <..!.... i.....E.
0010  00 34 71 c6 40 00 80 06  a8 d1 0a 55 22 6e d8 3a   .4q.@... ...U"n.:
0020  db 2e e6 b1 00 50 82 4f  2f b3 00 00 00 00 80 02   .....P.O /.......
0030  20 00 d5 df 00 00 02 04  05 b4 01 03 03 08 01 01    ....... ........
0040  04 02                                              ..
```

5 interfaces: <live capture in progress> File: ... Packets: 2413 · Displayed: 69 (2.9%)

b. What were the absolute and relative values of the initial sequence numbers used by the http client and server? Submit screenshots with these values circled.

Ans:



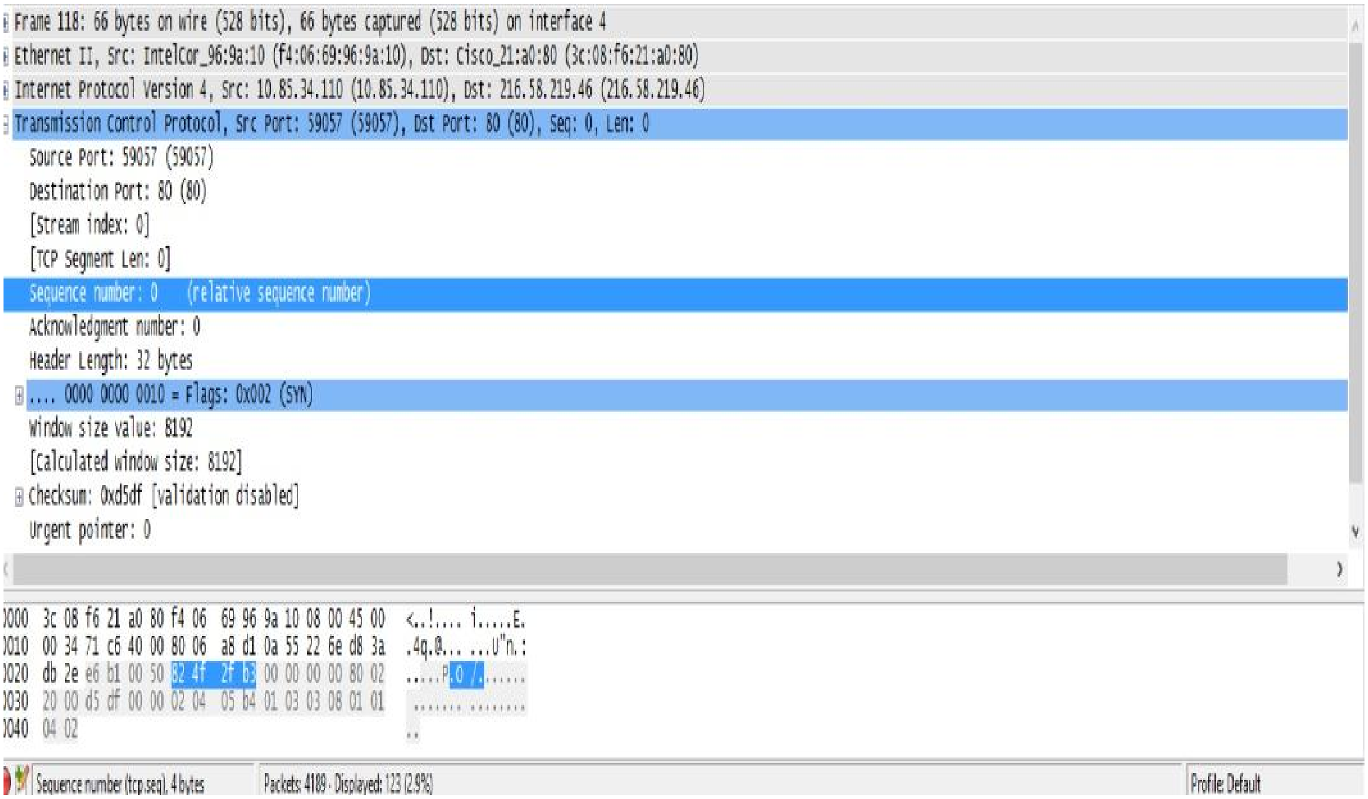
```
Frame 118: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 4
Ethernet II, Src: IntelCor_96:9a:10 (f4:06:69:96:9a:10), Dst: Cisco_21:a0:80 (3c:08:f6:21:a0:80)
Internet Protocol Version 4, Src: 10.85.34.110 (10.85.34.110), Dst: 216.58.219.46 (216.58.219.46)
Transmission Control Protocol, Src Port: 59057 (59057), Dst Port: 80 (80), Seq: 0, Len: 0
  Source Port: 59057 (59057)
  Destination Port: 80 (80)
  [Stream index: 0]
  [TCP Segment Len: 0]
  Sequence number: 0    (relative sequence number)
  Acknowledgment number: 0
  Header Length: 32 bytes
  .... 0000 0000 0010 = Flags: 0x002 (SYN)
  Window size value: 8192
  [Calculated window size: 8192]
  Checksum: 0xd5df [validation disabled]
  Urgent pointer: 0

0000  3c 08 f6 21 a0 80 f4 06  69 96 9a 10 08 00 45 00   <..!.... i.....E.
0010  00 34 71 c6 40 00 80 06  a8 d1 0a 55 22 6e d8 3a   .4q.@... ...U"n.:
0020  db 2e e6 b1 00 50 82 4f  2f b3 00 00 00 00 80 02   .....P.O /.......
0030  20 00 d5 df 00 00 02 04  05 b4 01 03 03 08 01 01    ....... ........
0040  04 02                                              ..

Sequence number (tcp.seq), 4 bytes    Packets: 4189 · Displayed: 123 (2.9%)    Profile: Default
```

Initial sequence number is :: 0

Absolute sequence number is :: 82 4f 2f b3

c. What tcp port numbers did the web client and server use? Submit screenshot with these values circled.

Ans:

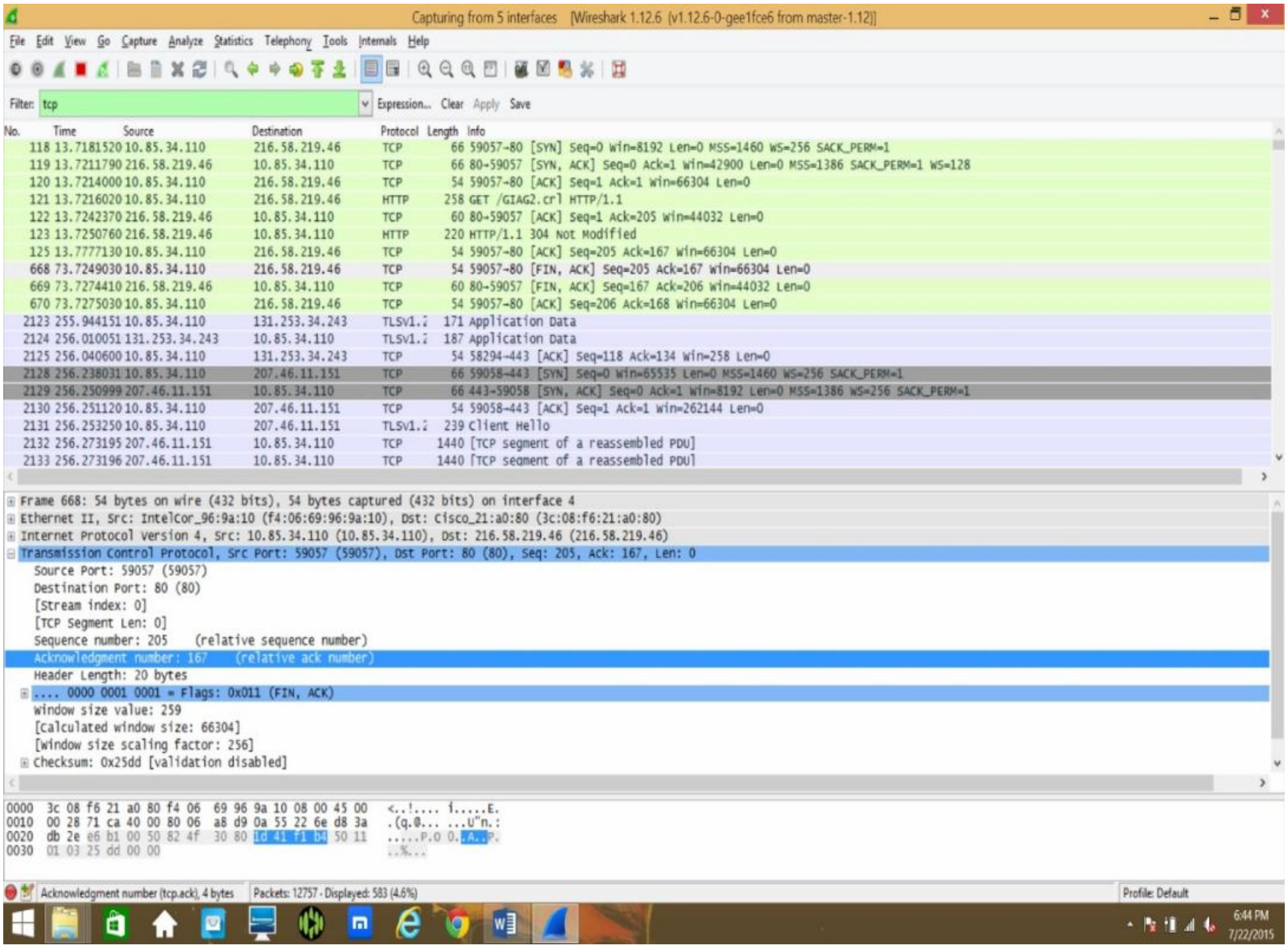


```
Frame 118: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 4
Ethernet II, Src: IntelCor_96:9a:10 (f4:06:69:96:9a:10), Dst: Cisco_21:a0:80 (3c:08:f6:21:a0:80)
Internet Protocol Version 4, Src: 10.85.34.110 (10.85.34.110), Dst: 216.58.219.46 (216.58.219.46)
Transmission Control Protocol, Src Port: 59057 (59057), Dst Port: 80 (80), Seq: 0, Len: 0
  Source Port: 59057 (59057)
  Destination Port: 80 (80)
  [Stream index: 0]
  [TCP Segment Len: 0]
  Sequence number: 0    (relative sequence number)
  Acknowledgment number: 0
  Header Length: 32 bytes
  .... 0000 0000 0010 = Flags: 0x002 (SYN)
  Window size value: 8192
  [Calculated window size: 8192]
  Checksum: 0xd5df [validation disabled]
  Urgent pointer: 0

000  3c 08 f6 21 a0 80 f4 06  69 96 9a 10 08 00 45 00   <..!.... i.....E.
010  00 34 71 c6 40 00 80 06  a8 d1 0a 55 22 6e d8 3a   .4q.@... ...U"n.:
020  db 2e e6 b1 00 50 82 4f  2f b3 00 00 00 00 80 02   .....P.O /.......
030  20 00 d5 df 00 00 02 04  05 b4 01 03 03 08 01 01    ....... ........
040  04 02                                              ..

Sequence number (tcp.seq), 4 bytes    Packets: 4189 · Displayed: 123 (2.9%)    Profile: Default
```

Web Client TCP Port No.: 59057
Server TCP Port No.: 80

d. What were the absolute and relative values of the final acknowledgement numbers sent by the http client and server? Submit screenshots with these values circled.

Ans:


Capturing from 5 interfaces [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save
Profile: Default
6:44 PM
7/22/2015

Filter: tcp

```
No.  Time        Source          Destination     Protocol Length Info
 118 13.7181520  10.85.34.110    216.58.219.46   TCP        66 59057→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
 119 13.7211790  216.58.219.46   10.85.34.110    TCP        66 80→59057 [SYN, ACK] Seq=0 Ack=1 Win=42900 Len=0 MSS=1386 SACK_PERM=1 WS=128
 120 13.7214000  10.85.34.110    216.58.219.46   TCP        54 59057→80 [ACK] Seq=1 Ack=1 Win=66304 Len=0
 121 13.7216020  10.85.34.110    216.58.219.46   HTTP      258 GET /GIAG2.crl HTTP/1.1
 122 13.7242370  216.58.219.46   10.85.34.110    TCP        60 80→59057 [ACK] Seq=1 Ack=205 Win=44032 Len=0
 123 13.7250760  216.58.219.46   10.85.34.110    HTTP      220 HTTP/1.1 304 Not Modified
 125 13.7777130  10.85.34.110    216.58.219.46   TCP        54 59057→80 [ACK] Seq=205 Ack=167 Win=66304 Len=0
 668 73.7249030  10.85.34.110    216.58.219.46   TCP        54 59057→80 [FIN, ACK] Seq=205 Ack=167 Win=66304 Len=0
 669 73.7274410  216.58.219.46   10.85.34.110    TCP        60 80→59057 [FIN, ACK] Seq=167 Ack=206 Win=44032 Len=0
 670 73.7275030  10.85.34.110    216.58.219.46   TCP        54 59057→80 [ACK] Seq=206 Ack=168 Win=66304 Len=0
2123 255.944151  10.85.34.110    131.253.34.243  TLSv1.:   171 Application Data
2124 256.010051  131.253.34.243  10.85.34.110    TLSv1.:   187 Application Data
2125 256.040600  10.85.34.110    131.253.34.243  TCP        54 58294→443 [ACK] Seq=118 Ack=134 Win=258 Len=0
2128 256.238031  10.85.34.110    207.46.11.151   TCP        66 59058→443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
2129 256.250999  207.46.11.151   10.85.34.110    TCP        66 443→59058 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1386 WS=256 SACK_PERM=1
2130 256.251120  10.85.34.110    207.46.11.151   TCP        54 59058→443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
2131 256.253250  10.85.34.110    207.46.11.151   TLSv1.:   239 Client Hello
2132 256.273195  207.46.11.151   10.85.34.110    TCP      1440 [TCP segment of a reassembled PDU]
2133 256.273196  207.46.11.151   10.85.34.110    TCP      1440 [TCP segment of a reassembled PDU]
```

```
⊞ Frame 668: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 4
⊞ Ethernet II, Src: IntelCor_96:9a:10 (f4:06:69:96:9a:10), Dst: Cisco_21:a0:80 (3c:08:f6:21:a0:80)
⊞ Internet Protocol Version 4, Src: 10.85.34.110 (10.85.34.110), Dst: 216.58.219.46 (216.58.219.46)
⊟ Transmission Control Protocol, Src Port: 59057 (59057), Dst Port: 80 (80), Seq: 205, Ack: 167, Len: 0
    Source Port: 59057 (59057)
    Destination Port: 80 (80)
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 205    (relative sequence number)
    Acknowledgment number: 167    (relative ack number)
    Header Length: 20 bytes
  ⊞ .... 0000 0001 0001 = Flags: 0x011 (FIN, ACK)
    Window size value: 259
    [Calculated window size: 66304]
    [Window size scaling factor: 256]
  ⊞ Checksum: 0x25dd [validation disabled]
```

```
0000  3c 08 f6 21 a0 80 f4 06  69 96 9a 10 08 00 45 00   <..!.... i.....E.
0010  00 28 71 ca 40 00 80 06  a8 d9 0a 55 22 6e d8 3a   .(q.@... ...U"n.:
0020  db 2e e6 b1 00 50 82 4f  30 80 1d 41 f1 b4 50 11   .....P.O 0..A..P.
0030  01 03 25 dd 00 00                                  ..%...
```

Acknowledgment number (tcp.ack), 4 bytes | Packets: 12757 · Displayed: 583 (4.6%)

Relative acknowledgement number: 167

Absolute acknowledgement number: 1d 41 f1 b4