

California State University, Monterey Bay

Week 8 – Lab 8

Group 10

Clarence Mitchell

CST311

Introduction to Computer Networks

SUMMER 2015

Instructor: Dr. Anand Seetharam

Questions and Answers

The following are the list of questions and related answers for this lab.

The screenshot shows a Wireshark capture of an HTTP GET request. The packet list pane shows a list of packets, with packet 38 selected. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol. The packet bytes pane shows the raw data of the packet.

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
37	2015-06-16 21:42:05.052006000	10.32.89.164	128.119.245.12	TCP	54	55960->80 [ACK] Seq=1 Ack=1 win=262144 Len=0
38	2015-06-16 21:42:05.052463000	10.32.89.164	128.119.245.12	HTTP	373	GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
39	2015-06-16 21:42:05.053373000	128.119.245.12	10.32.89.164	TCP	66	80->55959 [SYN, ACK] Seq=0 Ack=1 win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=128
40	2015-06-16 21:42:05.053490000	10.32.89.164	128.119.245.12	TCP	54	55959->80 [ACK] Seq=1 Ack=1 win=262144 Len=0
41	2015-06-16 21:42:05.054584000	10.32.89.164	38.113.165.116	TCP	66	55961->443 [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
42	2015-06-16 21:42:05.147770000	38.113.165.116	10.32.89.164	TCP	66	443->55961 [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MSS=1460 WS=64 SACK_PERM=1
43	2015-06-16 21:42:05.147770000	10.32.89.164	38.113.165.116	TCP	54	55961->443 [ACK] Seq=1 Ack=1 win=65536 Len=0
44	2015-06-16 21:42:05.149029000	10.32.89.164	38.113.165.116	SSL	432	Continuation Data
45	2015-06-16 21:42:05.149247000	128.119.245.12	10.32.89.164	TCP	60	80->55960 [ACK] Seq=1 Ack=320 win=15744 Len=0
46	2015-06-16 21:42:05.149637000	128.119.245.12	10.32.89.164	TCP	1514	[TCP segment of a reassembled PDU]
47	2015-06-16 21:42:05.149704000	128.119.245.12	10.32.89.164	TCP	1514	[TCP segment of a reassembled PDU]
48	2015-06-16 21:42:05.149777000	10.32.89.164	128.119.245.12	TCP	54	55960->80 [ACK] Seq=320 Ack=1461 win=262144 Len=0
49	2015-06-16 21:42:05.149971000	10.32.89.164	128.119.245.12	TCP	54	55960->80 [ACK] Seq=320 Ack=2921 win=262144 Len=0
50	2015-06-16 21:42:05.150599000	128.119.245.12	10.32.89.164	TCP	1514	[TCP segment of a reassembled PDU]
51	2015-06-16 21:42:05.150687000	128.119.245.12	10.32.89.164	HTTP	537	HTTP/1.1 200 OK (text/html)
52	2015-06-16 21:42:05.150731000	10.32.89.164	128.119.245.12	TCP	54	55960->80 [ACK] Seq=320 Ack=4381 win=262144 Len=0
53	2015-06-16 21:42:05.150949000	10.32.89.164	128.119.245.12	TCP	54	55960->80 [ACK] Seq=320 Ack=4864 win=261632 Len=0
54	2015-06-16 21:42:05.230171000	10.32.89.164	128.119.245.12	TCP	66	55962->80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1

Frame 38: 373 bytes on wire (2984 bits), 373 bytes captured (2984 bits) on interface 0

Ethernet II, Src: HonHaiPr_62:0a:cb (ac:d1:b8:62:0a:cb), Dst: AsustekC_92:e5:90 (e0:3f:49:92:e5:90)

Internet Protocol Version 4, Src: 10.32.89.164 (10.32.89.164), Dst: 128.119.245.12 (128.119.245.12)

Transmission Control Protocol, Src Port: 55960 (55960), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 319

Hypertext Transfer Protocol

GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1\r\n

[Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1\r\n]

Request Method: GET

Request URI: /wireshark-labs/HTTP-ethereal-lab-file3.html

Request Version: HTTP/1.1

Accept: text/html, application/xhtml+xml, */*\r\n

Accept-Language: en-US,en;q=0.5\r\n

User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; Touch; rv:11.0) like Gecko\r\n

Accept-Encoding: gzip, deflate\r\n

Host: gaia.cs.umass.edu\r\n

DNT: 1\r\n

Connection: Keep-Alive\r\n

\r\n

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html]

[HTTP request 1/1]

[Response in frame 51]

0000 e0 3f 49 92 e5 90 ac d1 b8 62 0a cb 08 00 45 b8 .?I.... .b....E.

0010 01 67 59 45 40 00 80 06 c6 4b 0a 20 59 a4 80 77 .gye@... .K. Y..w

0020 f5 0c da 98 00 50 08 ac 39 b9 c9 d3 61 29 50 18P... 9...a)P.

0030 04 00 df 15 00 00 47 45 54 20 2f 77 69 72 65 73GE T /wires

0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 50 2d 65 hark-lab s/HTTP-e

0050 74 68 65 72 65 61 6c 20 4d 6c 61 62 2d 66 69 6c 65 thermal-lab-file

0060 3 26 68 74 6d 6c 20 4d 6c 61 62 2d 66 69 6c 65 3.html H TTP/1.1

0070 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 .Accept: text/ht

0080 6d 6c 2c 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f ml, appl ication/

Frame (frame), 373 bytes Packets: 202 - Displayed: 202 (100.0%) - Dropped: 0 (0.0%) Profile: Default

The screenshot shows a Wireshark capture of an IP packet. The packet list pane shows a list of packets, with packet 38 selected. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol. The packet bytes pane shows the raw data of the packet.

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
38	2015-06-16 21:42:05.052463000	HonHaiPr_62:0a:cb	AsustekC_92:e5:90	IP	373	IP
39	2015-06-16 21:42:05.053373000	AsustekC_92:e5:90	HonHaiPr_62:0a:cb	IP	66	IP
40	2015-06-16 21:42:05.053490000	HonHaiPr_62:0a:cb	AsustekC_92:e5:90	IP	54	IP
41	2015-06-16 21:42:05.054584000	HonHaiPr_62:0a:cb	AsustekC_92:e5:90	IP	66	IP
42	2015-06-16 21:42:05.147770000	AsustekC_92:e5:90	HonHaiPr_62:0a:cb	IP	66	IP
43	2015-06-16 21:42:05.147770000	HonHaiPr_62:0a:cb	AsustekC_92:e5:90	IP	54	IP
44	2015-06-16 21:42:05.149029000	HonHaiPr_62:0a:cb	AsustekC_92:e5:90	IP	432	IP
45	2015-06-16 21:42:05.149247000	AsustekC_92:e5:90	HonHaiPr_62:0a:cb	IP	60	IP
46	2015-06-16 21:42:05.149637000	AsustekC_92:e5:90	HonHaiPr_62:0a:cb	IP	1514	IP
47	2015-06-16 21:42:05.149704000	AsustekC_92:e5:90	HonHaiPr_62:0a:cb	IP	1514	IP
48	2015-06-16 21:42:05.149777000	HonHaiPr_62:0a:cb	AsustekC_92:e5:90	IP	54	IP
49	2015-06-16 21:42:05.149971000	HonHaiPr_62:0a:cb	AsustekC_92:e5:90	IP	54	IP
50	2015-06-16 21:42:05.150599000	AsustekC_92:e5:90	HonHaiPr_62:0a:cb	IP	1514	IP
51	2015-06-16 21:42:05.150687000	AsustekC_92:e5:90	HonHaiPr_62:0a:cb	IP	537	IP
52	2015-06-16 21:42:05.150731000	HonHaiPr_62:0a:cb	AsustekC_92:e5:90	IP	54	IP
53	2015-06-16 21:42:05.150949000	HonHaiPr_62:0a:cb	AsustekC_92:e5:90	IP	54	IP
54	2015-06-16 21:42:05.230171000	HonHaiPr_62:0a:cb	AsustekC_92:e5:90	IP	66	IP
55	2015-06-16 21:42:05.230172000	HonHaiPr_62:0a:cb	AsustekC_92:e5:90	IP	66	IP

Frame 38: 373 bytes on wire (2984 bits), 373 bytes captured (2984 bits) on interface 0

Ethernet II, Src: HonHaiPr_62:0a:cb (ac:d1:b8:62:0a:cb), Dst: AsustekC_92:e5:90 (e0:3f:49:92:e5:90)

Destination: AsustekC_92:e5:90 (e0:3f:49:92:e5:90)

Address: AsustekC_92:e5:90 (e0:3f:49:92:e5:90)

... 0. ... = LG bit: Globally unique address (factory default)

... 0 ... = IG bit: Individual address (unicast)

Source: HonHaiPr_62:0a:cb (ac:d1:b8:62:0a:cb)

Address: HonHaiPr_62:0a:cb (ac:d1:b8:62:0a:cb)

... 0. ... = LG bit: Globally unique address (factory default)

... 0 ... = IG bit: Individual address (unicast)

Type: IP (0x0800)

Data (359 bytes)

0000 e0 3f 49 92 e5 90 ac d1 b8 62 0a cb 08 00 45 b8 .?I.... .b....E.

0010 01 67 59 45 40 00 80 06 c6 4b 0a 20 59 a4 80 77 .gye@... .K. Y..w

0020 f5 0c da 98 00 50 08 ac 39 b9 c9 d3 61 29 50 18P... 9...a)P.

0030 04 00 df 15 00 00 47 45 54 20 2f 77 69 72 65 73GE T /wires

0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 50 2d 65 hark-lab s/HTTP-e

0050 74 68 65 72 65 61 6c 20 4d 6c 61 62 2d 66 69 6c 65 thermal-lab-file

0060 3 26 68 74 6d 6c 20 4d 6c 61 62 2d 66 69 6c 65 3.html H TTP/1.1

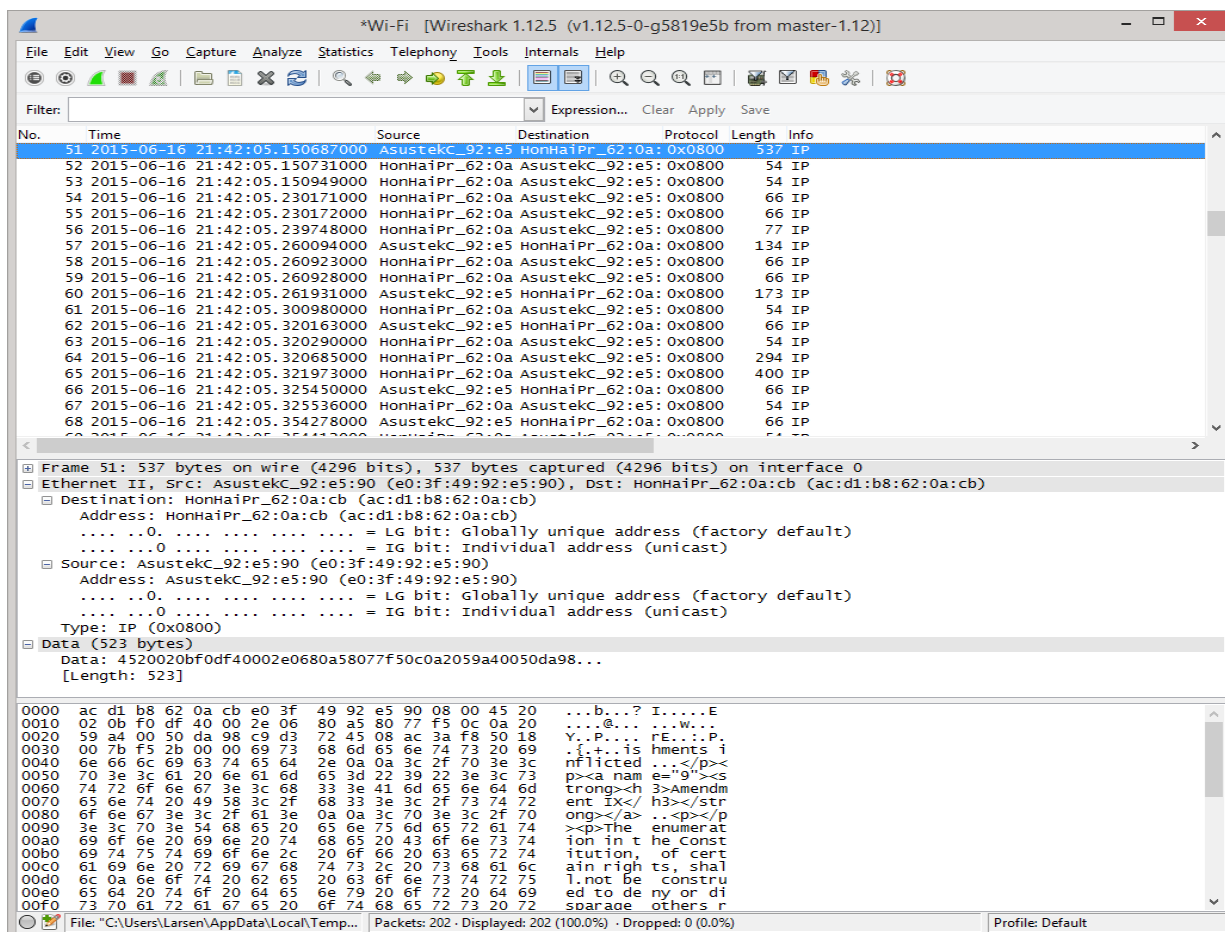
0070 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 .Accept: text/ht

0080 6d 6c 2c 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f ml, appl ication/

Frame (frame), 373 bytes Packets: 202 - Displayed: 202 (100.0%) - Dropped: ... Profile: Default

1. Capturing and analyzing Ethernet frames

- What is the 48-bit Ethernet address of your computer?
 - I got the IP address **ac:d1:b8:62:0a:cb**
- What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of **gaia.cs.umass.edu**? (Hint: the answer is *no*). What device has this as its Ethernet address? [Note: this is an important question, and one that students sometimes get wrong. Re-read pages 468-469 in the text and make sure you understand the answer here.]
 - The destination address **e0:3f:49:92:e5:90** is not the Ethernet address of **gaia.cs.umass.edu**. It is the address of my **Asus router**, which is the link used to get off the subnet.
- Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?
 - The hexadecimal value is **0x0800**. This corresponds to the **IP** protocol.
- How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame?
 - It appears that the **G** in the **GET** appears **52** bits into the frame.



5. What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is no). What device has this as its Ethernet address?
 - The source address e0:3f:49:92:e5:90 is neither the Ethernet address of gaia.cs.umass.edu nor the address of my computer. It is the address of my Asus router.
6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?
 - The destination address ac:d1:b8:62:0a:cb is the address of computer.
7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?
 - The hex value for the Frame type field is 0x0800, which is IP.
8. How many bytes from the very start of the Ethernet frame does the ASCII “O” in “OK” (i.e., the HTTP response code) appear in the Ethernet frame?
 - The ASCII “O” appears to be 52 bytes from the start of the Ethernet frame..

2. The Address Resolution Protocol

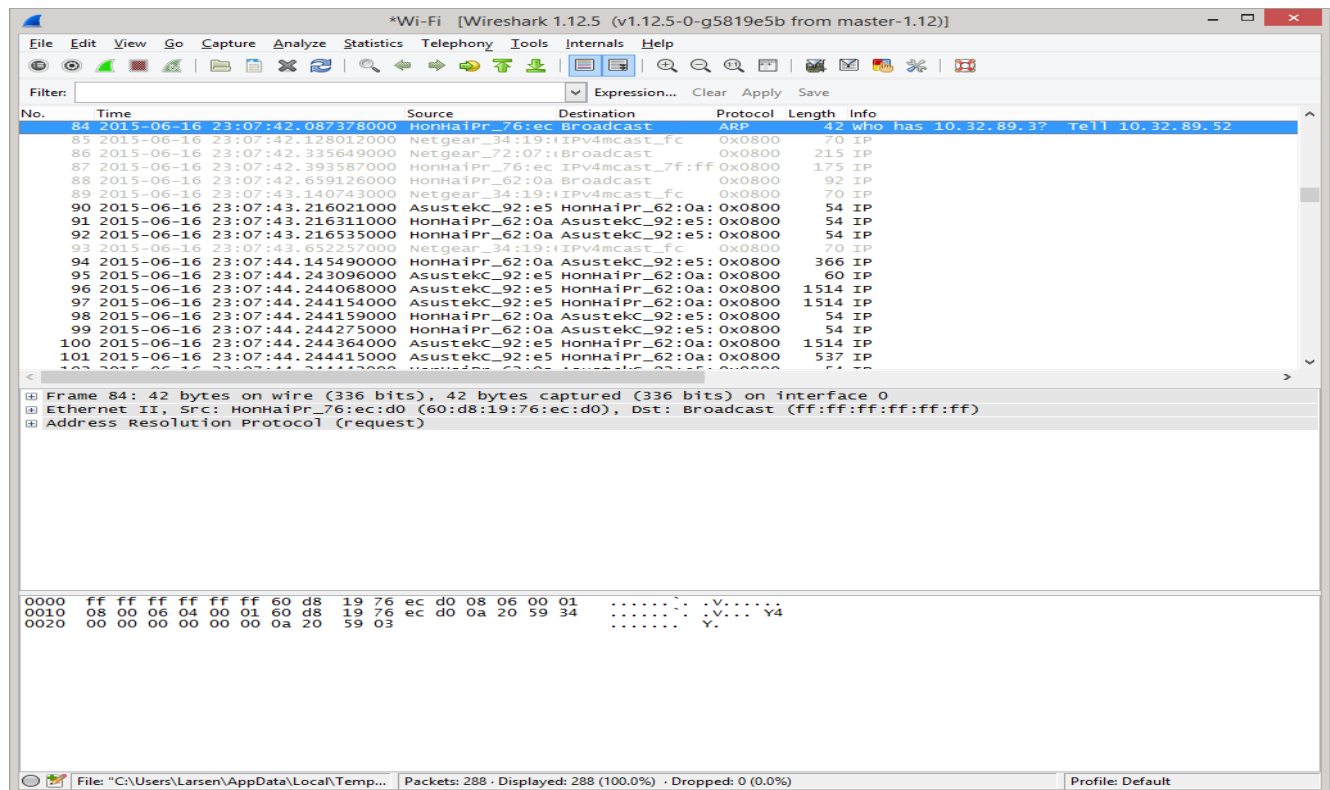
```

C:\Windows\system32>arp -a

Interface: 10.32.89.164 --- 0x5
Internet Address      Physical Address      Type
10.32.89.3            e0-3f-49-92-e5-90    dynamic
10.32.89.12           28-c6-8e-72-07-d7    dynamic
10.32.89.13           1c-7e-e5-de-de-78    dynamic
10.32.89.14           1c-7e-e5-de-de-6c    dynamic
10.32.89.21           28-c6-8e-34-19-6b    dynamic
10.32.89.30           00-1b-a9-a6-9d-c1    dynamic
10.32.89.31           1c-7e-e5-de-de-78    dynamic
10.32.89.39           00-1f-e1-05-c6-dc    dynamic
10.32.89.52           60-d8-19-76-ec-d0    dynamic
10.32.89.162          9c-d6-43-93-7b-8f    dynamic
10.32.89.240          60-45-bd-de-91-88    dynamic
10.32.89.255          ff-ff-ff-ff-ff-ff    static
224.0.0.2             01-00-5e-00-00-02    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static

C:\Windows\system32>
  
```

9. Write down the contents of your computer’s ARP cache. What is the meaning of each column value?
 - This command is windows 8.1 requires the “-a” option.
 - The first column is the internet address of the computer then its physical address and finally what type it is and it is dynamic.



10. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?

- The source address is (60:d8:19:76:ec:d0)
- The Destination address is (ff:ff:ff:ff:ff:ff)

11. Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?

- The hex value for the two byte Ethernet frame is ARP (0x0806), the corresponding upper layer protocol is ARP.

12. Download the ARP specification from <http://ftp.rfc-editor.org/in-notes/std/std37.txt>. A readable, detailed discussion of ARP is also at

<http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html>

a) How many bytes from the very beginning of the Ethernet frame does the ARP *opcode* field begin?

- The ARP opcode field begins 20 bytes from the very beginning of the Ethernet frame.

b) What is the value of the *opcode* field within the ARP-payload part of the Ethernet frame in which an ARP request is made?

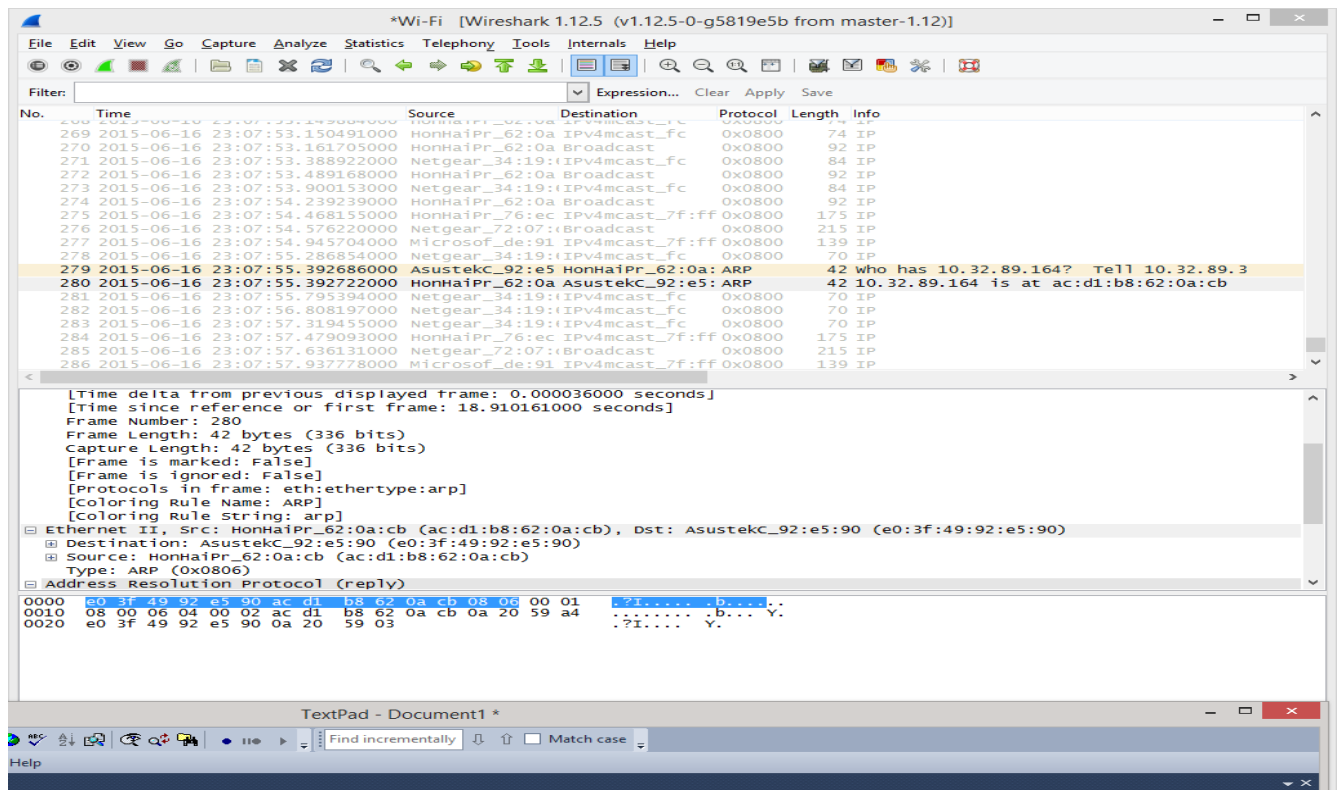
- The hex value for opcode field within the ARP-payload of the request is 0x0001, for request.

c) Does the ARP message contain the IP address of the sender? Where in the ARP request does the “question” appear – the Ethernet address of the machine whose corresponding IP address is being queried?

- Yes, the ARP message containing the IP address 10.32.89.164 for the sender. The field “Target MAC address” is set to 00:00:00:00:00:00 to question the machine whose corresponding IP address (10.32.89.3) is being queried.

13. Now find the ARP reply that was sent in response to the ARP request.

- How many bytes from the very beginning of the Ethernet frame does the ARP *opcode* field begin?
 - The ARP opcode field begins 20 bytes from the very beginning of the Ethernet frame.
- What is the value of the *opcode* field within the ARP-payload part of the Ethernet frame in which an ARP response is made?
 - The hex value for opcode field within the ARP-payload of the request is 0x0001, for request.
- Where in the ARP message does the “answer” to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?
 - ARP request appears in the “Sender MAC address” field, which contains the Ethernet address ac:d1:b8:62:0a:cb for the sender with IP address 10.32.89.3.



14. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?

- The hex value for the source address is ac:d1:b8:62:0a:cb and for the destination is e0:3f:49:92:e5:90

15. Open the *ethernet-ethereal-trace-1* trace file in <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip>. The first and second ARP packets in this trace correspond to an ARP request sent by the computer running Wireshark, and the ARP reply sent to the computer running Wireshark by the computer with the ARP-requested Ethernet address. But there is yet another computer on this network, as indicated by packet 6 – another ARP request. Why is there no ARP reply (sent in response to the ARP request in packet 6) in the packet trace?
- There is no reply in this trace, that we can see because we are not the machine that sent the original request. We can see the reply to "our" ARP request because it is sent directly to us.