

Justin Phillips

cs372 2020

lab5

Answer the following questions, based on the contents of the Ethernet frame containing the HTTP GET message. Whenever possible, when answering a question you should include a screenshot of the packet(s) within the trace that you used to answer the question asked. Make sure to include in the screenshot ALL and ONLY the minimum amount of packet detail that you need to answer the question.

1. What is the 48-bit Ethernet address of your computer?

Source: IntelCor_07:2f:8d (e4:a7:a0:07:2f:8d)

1-lab4.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
218	12:04:06.094046	72.21.91.29	10.0.0.118	OCSP	853	Response
231	12:04:06.130279	192.124.249.23	10.0.0.118	OCSP	1006	Response
378	12:04:06.394911	10.0.0.118	72.21.91.29	OCSP	443	Request
427	12:04:06.424558	72.21.91.29	10.0.0.118	OCSP	853	Response
535	12:04:06.620978	10.0.0.118	128.119.245.12	HTTP	443	GET /wireshark-labs/HTTP-ethereal-lab-file3
570	12:04:06.680637	10.0.0.118	72.21.91.29	OCSP	443	Request
586	12:04:06.700527	72.21.91.29	10.0.0.118	OCSP	853	Response
587	12:04:06.702544	10.0.0.118	72.21.91.29	OCSP	443	Request
600	12:04:06.730709	72.21.91.29	10.0.0.118	OCSP	853	Response

> Frame 535: 443 bytes on wire (3544 bits), 443 bytes captured (3544 bits) on interface \Device\NPF_{9FB385DA-C0...}

▼ Ethernet II, Src: IntelCor_07:2f:8d (e4:a7:a0:07:2f:8d), Dst: Technico_e7:bb:82 (3c:b7:4b:e7:bb:82)

- > Destination: Technico_e7:bb:82 (3c:b7:4b:e7:bb:82)
- > Source: IntelCor_07:2f:8d (e4:a7:a0:07:2f:8d)
- Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 10.0.0.118, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 38224, Dst Port: 80, Seq: 1, Ack: 1, Len: 389

> Hypertext Transfer Protocol

0000	3c b7 4b e7 bb 82 e4 a7 a0 07 2f 8d 08 00 45 00	<.K.../...E-
0010	01 ad c7 d4 40 00 40 06 f1 7c 0a 00 00 76 80 77	...@.@- ...v.w
0020	f5 0c 95 50 00 50 10 52 fd 32 24 c3 da 46 50 18	...P.P.R -2\$.FP-
0030	02 01 96 96 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 54 50 2d 65	hark-lab s/HTTP-e
0050	74 68 65 72 65 61 6c 2d 6c 61 62 2d 66 69 6c 65	thereal- lab-file
0060	33 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d	3.html H TTP/1.1-
0070	0a 48 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75	-Host: g aia.cs.u
0080	6d 61 73 73 2e 65 64 75 0d 0a 55 73 65 72 2d 41	mass.edu --User-A
0090	67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e	gent: Mo zilla/5.
00a0	30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 31 30	0 (Windo ws NT 10
00b0	2e 30 3b 20 57 69 6e 36 34 3b 20 78 36 34 3b 20	.0; Win6 4; x64;
00c0	72 76 3a 37 39 2e 30 29 20 47 65 63 6b 6f 2f 32	rv:79.0) Gecko/2
00d0	30 31 30 30 31 30 31 20 46 69 72 65 66 6f 78 2f	0100101 Firefox/
00e0	37 39 2e 30 0d 0a 41 63 63 65 70 74 3a 20 74 65	79.0--Ac cept: te
00f0	78 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74	xt/html, applicat

Source Hardware Address (eth.src), 6 bytes

2. 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.]

Destination: Technico_e7:bb:82 (3c:b7:4b:e7:bb:82)(screen shot is in 1)

this is the address of my router

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

Type: IPv4 (0x0800)(as seen in 1) the upper layer protocol that this corresponds to is IP protocol as payload

4. How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame?

bytes 54-56 is the GET request, so 54 would be the G

1-lab4.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help



http

No.	Time	Source	Destination	Protocol	Length	Info
218	12:04:06.094046	72.21.91.29	10.0.0.118	OCSP	853	Response
231	12:04:06.130279	192.124.249.23	10.0.0.118	OCSP	1006	Response
378	12:04:06.394911	10.0.0.118	72.21.91.29	OCSP	443	Request
427	12:04:06.424558	72.21.91.29	10.0.0.118	OCSP	853	Response
535	12:04:06.620978	10.0.0.118	128.119.245.12	HTTP	443	GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
570	12:04:06.680637	10.0.0.118	72.21.91.29	OCSP	443	Request
586	12:04:06.700527	72.21.91.29	10.0.0.118	OCSP	853	Response
587	12:04:06.702544	10.0.0.118	72.21.91.29	OCSP	443	Request
600	12:04:06.730709	72.21.91.29	10.0.0.118	OCSP	853	Response

- > Frame 535: 443 bytes on wire (3544 bits), 443 bytes captured (3544 bits) on interface \Device\NPF_{9FB385DA...}
- > Ethernet II, Src: IntelCor_07:2f:8d (e4:a7:a0:07:2f:8d), Dst: Technico_e7:bb:82 (3c:b7:4b:e7:bb:82)
- > Internet Protocol Version 4, Src: 10.0.0.118, Dst: 128.119.245.12
- > Transmission Control Protocol, Src Port: 38224, Dst Port: 80, Seq: 1, Ack: 1, Len: 389

Hypertext Transfer Protocol

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

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

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:79.0) Gecko/20100101 Firefox/79.0\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n

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

Accept-Encoding: gzip, deflate\r\n

DNT: 1\r\n

Connection: keep-alive\r\n

Upgrade-Insecure-Requests: 1\r\n

\r\n

0030	02 01 96 96 00 00 47 45 54 20 2f 77 69 72 65 73GET /wires
0040	68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 65	hark-lab s/HTTP-e
0050	74 68 65 72 65 61 6c 2d 6c 61 62 2d 66 69 6c 65	thereal- lab-file
0060	33 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d	3.html H TTP/1.1.
0070	0a 48 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75	.Host: g aia.cs.u
0080	6d 61 73 73 2e 65 64 75 0d 0a 55 73 65 72 2d 41	mass.edu ..User-A
0090	67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e	gent: Mo zilla/5.
00a0	30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 31 30	0 (Windo ws NT 10
00b0	2e 30 3b 20 57 69 6e 36 34 3b 20 78 36 34 3b 20	.0; Win6 4; x64;
00c0	72 76 3a 37 39 2e 30 29 20 47 65 63 6b 6f 2f 32	rv:79.0) Gecko/2
00d0	30 31 30 30 31 30 31 20 46 69 72 65 66 6f 78 2f	0100101 Firefox/
00e0	37 39 2e 30 0d 0a 41 63 63 65 70 74 3a 20 74 65	79.0..Ac cept: te
00f0	78 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74	xt/html, applicat
0100	69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70	ion/xhtml+xml,ap
0110	70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d	plicatio n/xml;q=
0120	30 2e 39 2c 69 6d 61 67 65 2f 77 65 62 70 2c 2a	0.9,image/webp,*

HTTP Request Method (http.request.method), 3 bytes



Next, answer the following questions, based on the contents of the Ethernet frame containing the first byte of the HTTP response message.

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?

Address: Technico_e7:bb:82 (3c:b7:4b:e7:bb:82), this is address of my router

1-lab4.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
586	12:04:06.700527	72.21.91.29	10.0.0.118	OCSP	853	Response
587	12:04:06.702544	10.0.0.118	72.21.91.29	OCSP	443	Request
600	12:04:06.730709	72.21.91.29	10.0.0.118	OCSP	853	Response
605	12:04:06.730709	128.119.245.12	10.0.0.118	HTTP	534	HTTP/1.1 200 OK (text/html)
800	12:04:08.084844	10.0.0.118	128.119.245.12	HTTP	321	GET /favicon.ico HTTP/1.1
844	12:04:08.192047	128.119.245.12	10.0.0.118	HTTP	538	HTTP/1.1 404 Not Found (text/html)
1005	12:04:11.100857	10.0.0.118	13.227.77.55	OCSP	452	Request
1010	12:04:11.130535	13.227.77.55	10.0.0.118	OCSP	1060	Response
1076	12:04:12.591485	10.0.0.118	72.21.91.29	OCSP	443	Request

> Frame 605: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface \Device\NPF_{9FB385DA-CC7B-4B...}

▼ Ethernet II, Src: Technico_e7:bb:82 (3c:b7:4b:e7:bb:82), Dst: IntelCor_07:2f:8d (e4:a7:a0:07:2f:8d)

- ▼ Destination: IntelCor_07:2f:8d (e4:a7:a0:07:2f:8d)
Address: IntelCor_07:2f:8d (e4:a7:a0:07:2f:8d)
.... 0. = LG bit: Globally unique address (factory default)
.... 0. = IG bit: Individual address (unicast)
- ▼ Source: Technico_e7:bb:82 (3c:b7:4b:e7:bb:82)
Address: Technico_e7:bb:82 (3c:b7:4b:e7:bb:82)
.... 0. = LG bit: Globally unique address (factory default)
.... 0. = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.118

> Transmission Control Protocol, Src Port: 80, Dst Port: 38224, Seq: 4381, Ack: 390, Len: 480

> [4 Reassembled TCP Segments (4860 bytes): #602(1460), #603(1460), #604(1460), #605(480)]

> Hypertext Transfer Protocol

Offset	Hex	ASCII
0000	e4 a7 a0 07 2f 8d 3c b7 4b e7 bb 82 08 00 45 00/.<. K...E.
0010	02 08 a5 00 40 00 21 06 32 f6 80 77 f5 0c 0a 00@!- 2..w....
0020	00 76 00 50 95 50 24 c3 eb 62 10 52 fe b7 50 18	..v.P.P\$. .b.R..P.
0030	00 ed 97 82 00 00 6d 65 6e 74 73 20 69 6e 66 6cme nts infl
0040	69 63 74 65 64 2e 0a 0a 3c 2f 70 3e 3c 70 3e 3c	icted... </p><p><
0050	61 20 6e 61 6d 65 3d 22 39 22 3e 3c 73 74 72 6f	a name=" 9"><stro
0060	6e 67 3e 3c 68 33 3e 41 6d 65 6e 64 6d 65 6e 74	ng><h3>A mendment
0070	20 49 58 3c 2f 68 33 3e 3c 2f 73 74 72 6f 6e 67	IX</h3> </strong
0080	3e 3c 2f 61 3e 0a 0a 3c 70 3e 3c 2f 70 3e 3c 70	>...< p></p><p
0090	3e 54 68 65 20 65 6e 75 6d 65 72 61 74 69 6f 6e	>The enu meration
00a0	20 69 6e 20 74 68 65 20 43 6f 6e 73 74 69 74 75	in the Constitu
00b0	74 69 6f 6e 2c 20 6f 66 20 63 65 72 74 61 69 6e	tion, of certain
00c0	20 72 69 67 68 74 73 2c 20 73 68 61 6c 6c 0a 6e	rights, shall.n
00d0	6f 74 20 62 65 20 63 6f 6e 73 74 72 75 65 64 20	ot be co nstrued

Frame (534 bytes) Reassembled TCP (4860 bytes)

Source or Destination Hardware Address (eth.addr), 6 bytes

Type here to search

6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?

Destination: IntelCor_07:2f:8d (e4:a7:a0:07:2f:8d)(from above) this is my pc

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

(0x0800) the upper layer protocol that this corresponds to is IP protocol(valie is in the screen shot above)

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?

at the bottom of the screen shot it shows that after byte 13 the "O" appears in the frame

1-lab4.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help



No.	Time	Source	Destination	Protocol	Length	Info
586	12:04:06.700527	72.21.91.29	10.0.0.118	OCSP	853	Response
587	12:04:06.702544	10.0.0.118	72.21.91.29	OCSP	443	Request
600	12:04:06.730709	72.21.91.29	10.0.0.118	OCSP	853	Response
605	12:04:06.730709	128.119.245.12	10.0.0.118	HTTP	534	HTTP/1.1 200 OK (text/html)
800	12:04:08.084844	10.0.0.118	128.119.245.12	HTTP	321	GET /favicon.ico HTTP/1.1
844	12:04:08.192047	128.119.245.12	10.0.0.118	HTTP	538	HTTP/1.1 404 Not Found (text/html)
1005	12:04:11.100857	10.0.0.118	13.227.77.55	OCSP	452	Request
1010	12:04:11.130535	13.227.77.55	10.0.0.118	OCSP	1060	Response
1076	12:04:12.591485	10.0.0.118	72.21.91.29	OCSP	443	Request

```

.....0..... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.118
> Transmission Control Protocol, Src Port: 80, Dst Port: 38224, Seq: 4381, Ack: 390, Len: 480
> [4 Reassembled TCP Segments (4860 bytes): #602(1460), #603(1460), #604(1460), #605(480)]
▼ Hypertext Transfer Protocol
  ▼ HTTP/1.1 200 OK\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
      Date: Fri, 31 Jul 2020 19:04:06 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.7 mod_perl/2.0.11 Perl/v5.16.3\r\n
      Last-Modified: Fri, 31 Jul 2020 05:59:02 GMT\r\n

```

```

0000 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d HTTP/1.1 200 OK
0010 0a 44 61 74 65 3a 20 46 72 69 2c 20 33 31 20 4a .Date: Fri, 31 J
0020 75 6c 20 32 30 32 30 20 31 39 3a 30 34 3a 30 36 ul 2020 19:04:06
0030 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41 70 GMT..Se rver: Ap
0040 61 63 68 65 2f 32 2e 34 2e 36 20 28 43 65 6e 74 ache/2.4 .6 (Cent
0050 4f 53 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 30 2e OS) Open SSL/1.0.
0060 32 6b 2d 66 69 70 73 20 50 48 50 2f 37 2e 34 2e 2k-fips PHP/7.4.
0070 37 20 6d 6f 64 5f 70 65 72 6c 2f 32 2e 30 2e 31 7 mod_pe rl/2.0.1
0080 31 20 50 65 72 6c 2f 76 35 2e 31 36 2e 33 0d 0a 1 Perl/v 5.16.3..
0090 4c 61 73 74 2d 4d 6f 64 69 66 69 65 64 3a 20 46 Last-Mod ified: F
00a0 72 69 2c 20 33 31 20 4a 75 6c 20 32 30 32 30 20 ri, 31 J ul 2020
00b0 30 35 3a 35 39 3a 30 32 20 47 4d 54 0d 0a 45 54 05:59:02 GMT..ET
00c0 61 67 3a 20 22 31 31 39 34 2d 35 61 62 62 36 37 ag: "119 4-5abb67
00d0 63 35 37 34 61 61 64 22 0d 0a 41 63 63 65 70 74 c574aad" ..Accept

```

Frame (534 bytes) Reassembled TCP (4860 bytes)

Bytes 13-14: Response Phrase (http.response.phrase)



9. Write down the contents of your computer's ARP cache. What is the meaning of each column value?

the value of each column is as follows the internet address is the address of Ip address of each device,
The physical address is the MAC address of each device and the type is the protocol of each device

Command Prompt

inet_addr Specifies an internet address.
-N if_addr Displays the ARP entries for the network interface specified by if_addr.
-d Deletes the host specified by inet_addr. inet_addr may be wildcarded with * to delete all hosts.
-s Adds the host and associates the Internet address inet_addr with the Physical address eth_addr. The Physical address is given as 6 hexadecimal bytes separated by hyphens. The entry is permanent.
eth_addr Specifies a physical address.
if_addr If present, this specifies the Internet address of the interface whose address translation table should be modified. If not present, the first applicable interface will be used.

Example:

```
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Adds a static entry.  
> arp -a .... Displays the arp table.
```

C:\>windows\system32\arp -a

```
Interface: 172.20.10.4 --- 0xe
Internet Address      Physical Address      Type
172.20.10.1           82-0c-67-47-93-64     dynamic
172.20.10.15          ff-ff-ff-ff-ff-ff     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:\>

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

Destination: Broadcast (ff:ff:ff:ff:ff:ff)

Address: Broadcast (ff:ff:ff:ff:ff:ff)

Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)

Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)

Wireshark · Packet 1 · ethernet-ethereal-trace-1

> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
▼ Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 ▼ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
 Address: Broadcast (ff:ff:ff:ff:ff:ff)
 1. = LG bit: Locally administered address (this is NOT the factory default)
 1 = IG bit: Group address (multicast/broadcast)
 ▼ Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
 Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
 0. = LG bit: Globally unique address (factory default)
 0 = IG bit: Individual address (unicast)
 Type: ARP (0x0806)
> Address Resolution Protocol (request)

0000	ff ff ff ff ff ff 00 d0 59 a9 3d 68 08 06 00 01 Y.=h....
0010	08 00 06 04 00 01 00 d0 59 a9 3d 68 c0 a8 01 69 Y.=h...i
0020	00 00 00 00 00 00 c0 a8 01 01

Windows taskbar: Type here to search, icons for Edge, Firefox, File Explorer, Shopping, Word, Excel, and Wireshark.

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

Type: ARP (0x0806)(in screen shot above), and the protocol is ARP

12. Download the ARP specification from <ftp://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>.

ethernet-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	10:19:20.157130	AmbitMic_a9:3d:68	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.105
2	10:19:20.158148	LinksysG_da:af:73	AmbitMic_a9:3d:68	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
3	10:19:20.158158	192.168.1.105	199.2.53.206	TCP	62	1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
4	10:19:23.119980	192.168.1.105	199.2.53.206	TCP	62	[TCP Retransmission] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
5	10:19:29.128618	192.168.1.105	199.2.53.206	TCP	62	[TCP Retransmission] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
6	10:19:33.700104	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
7	10:19:37.601553	192.168.1.105	128.119.245.12	TCP	62	1058 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
8	10:19:37.623032	128.119.245.12	192.168.1.105	TCP	62	80 → 1058 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
9	10:19:37.623057	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0

> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)

▼ Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

- > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
- > Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
- Type: ARP (0x0806)

▼ Address Resolution Protocol (request)

- Hardware type: Ethernet (1)
- Protocol type: IPv4 (0x0800)
- Hardware size: 6
- Protocol size: 4
- Opcode: request (1)
- Sender MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
- Sender IP address: 192.168.1.105
- Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
- Target IP address: 192.168.1.1

```
0000  ff ff ff ff ff ff 00 d0 59 a9 3d 68 08 06 00 01  .... Y.=h...
0010  08 00 06 04 00 01 00 d0 59 a9 3d 68 c0 a8 01 69  .... Y.=h...i
0020  00 00 00 00 00 00 c0 a8 01 01  ....
```

Opcode (arp.opcode), 2 bytes

Type here to search

a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin? bytes 20-21

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?

0001

c) Does the ARP message contain the IP address of the sender?

Sender IP address: 192.168.1.105

d) Where in the ARP request does the “question” appear – the Ethernet address of the machine whose corresponding IP address is being queried?

who has 192.168.1.1? it appears in the Target IP address: 192.168.1.1 which is the router

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



c) 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?

192.168.1.1 is at 00:06:25:da:af:73 appears in Sender MAC address: LinksysG_da:af:73
(00:06:25:da:af:73) Sender IP address: 192.168.1.1 this is the router

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

Destination: Broadcast (ff:ff:ff:ff:ff:ff)

Address: Broadcast (ff:ff:ff:ff:ff:ff)

Source: CnetTech_73:8d:ce (00:80:ad:73:8d:ce)

Address: CnetTech_73:8d:ce (00:80:ad:73:8d:ce)

ethernet-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp

No.	Time	Source	Destination	Protoc	Lengt	Info
1	10:19:20.157130	AmbitMic_a9:3d:68	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.105
2	10:19:20.158148	LinksysG_da:af:73	AmbitMic_a9:3d...	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
6	10:19:33.700104	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104

> Frame 6: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)

▼ Ethernet II, Src: CnetTech_73:8d:ce (00:80:ad:73:8d:ce), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

- ▼ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
 - Address: Broadcast (ff:ff:ff:ff:ff:ff)
 - 1. = LG bit: Locally administered address (this is NOT the factory default)
 - 1 = IG bit: Group address (multicast/broadcast)
- ▼ Source: CnetTech_73:8d:ce (00:80:ad:73:8d:ce)
 - Address: CnetTech_73:8d:ce (00:80:ad:73:8d:ce)
 - 0. = LG bit: Globally unique address (factory default)
 - 0 = IG bit: Individual address (unicast)
 - Type: ARP (0x0806)
 - Padding: 00000000000000000000000000000000

> Address Resolution Protocol (request)

```

0000  ff ff ff ff ff ff 00 80  ad 73 8d ce 08 06 00 01  .....s...
0010  08 00 06 04 00 01 00 80  ad 73 8d ce c0 a8 01 68  .....s...h
0020  00 00 00 00 00 00 c0 a8  01 75 00 00 00 00 00  .....u....
0030  00 00 00 00 00 00 00 00  00 00 00 00  .....
  
```

Sender IP address (arp.src.proto_ipv4), 4 bytes

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?

We can only see the reply from our own pc because it was sent directly to the pc