

CS315: Lab Assignment 11

B Siddharth Prabhu
200010003@iitdh.ac.in

21 March 2023

1 Answers to Part 1: Capture and Analysis of Ethernet Frames

On clearing the browser cache and subsequently accessing the required webpage, the packet trace observed is pictured in Figure (1). In the below figure, the details of the first HTTP Request packet are shown.

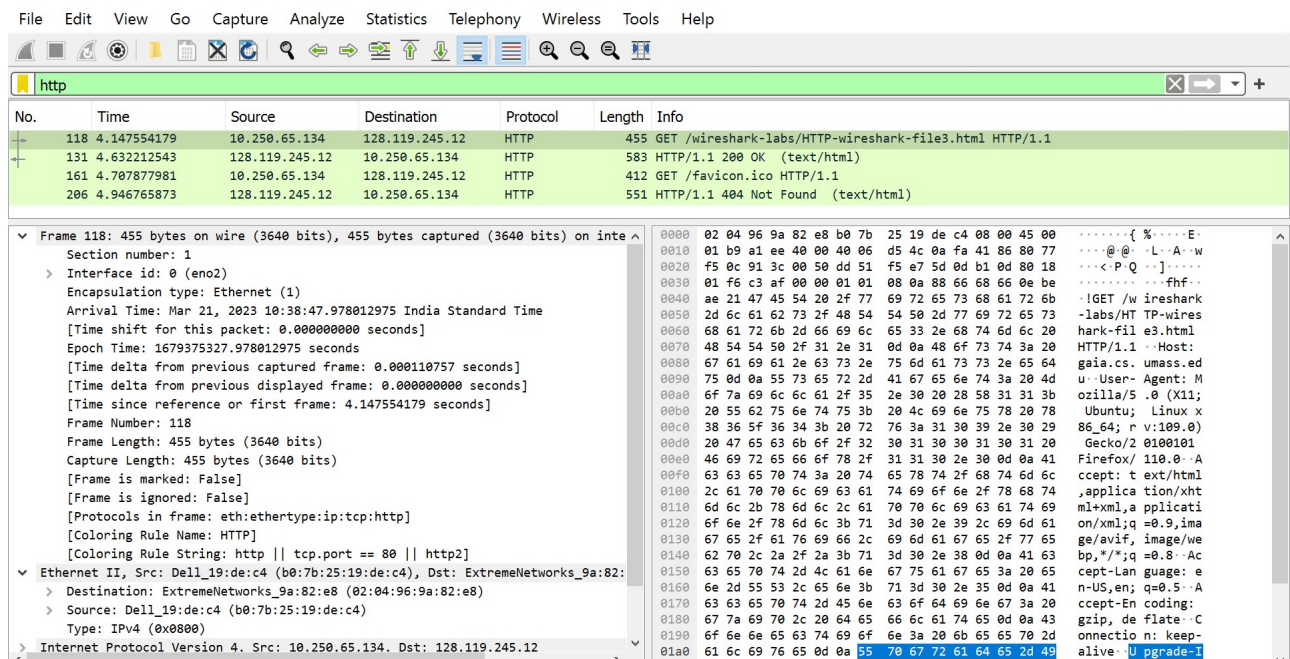


Figure 1: Packet Trace observed

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

The 48-bit Ethernet address of my computer is `b0:7b:25:19:de:c4` .

(2) What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of `gaia.cs.umass.edu`? What device has this as its Ethernet address?

The 48-bit destination address in the Ethernet frame is `02:04:96:9a:82:e8` . This is not the Ethernet address of `gaia.cs.umass.edu`; it is the Ethernet address of the interface of our next-hop router, that is in the lab.

(3) What is the hexadecimal value for the two-byte Frame type field in the Ethernet frame carrying the HTTP GET request? What upper layer protocol does this correspond to?

The hexadecimal value for the two-byte Frame type field in the Ethernet frame is `0x0800` in the Ethernet frame carrying the HTTP GET request. This corresponds to the `IPv4` (Internet Protocol Version 4) Network Layer Protocol.

(4) How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame?

The ASCII “G” in “GET” appears at the `67th Byte`, as seen in Figure (2). If we go by zero-based indexing, then it is `Byte 66`.

0000	02 04 96 9a 82 e8 b0 7b 25 19 de c4 08 00 45 00{ %.....E.
0010	01 b9 a1 ee 40 00 40 06 d5 4c 0a fa 41 86 80 77@.@. .L. .A..w
0020	f5 0c 91 3c 00 50 dd 51 f5 e7 5d 0d b1 0d 80 18	...<.P.Q ..].....
0030	01 f6 c3 af 00 00 01 01 08 0a 88 66 68 66 0e befhf..
0040	ae 21 47 45 54 20 2f 77 69 72 65 73 68 61 72 6b	..!GET /w ireshark
0050	2d 6c 61 62 73 2f 48 54 54 50 2d 77 69 72 65 73	-labs/HT TP-wires
0060	68 61 72 6b 2d 66 69 6c 65 33 2e 68 74 6d 6c 20	hark-fil e3.html
0070	48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20	HTTP/1.1 ..Host:
0080	67 61 69 61 2e 63 73 2e 75 6d 61 73 73 2e 65 64	gaia.cs. umass.ed

Figure 2: ASCII ‘G’

Next, we look at the Ethernet frame containing the first byte of the HTTP response message. The figure below contains details of the same.

The image shows a Wireshark capture of an HTTP response. The packet list shows frame 131 (583 bytes) as an HTTP 200 OK response. The packet details pane shows the following structure:

- Ethernet II, Src: ExtremeNetworks_9a:82:e8 (02:04:96:9a:82:e8), Dst: Dell_19:de:c4 (b0:7b:25:19:de:c4)
 - Destination: Dell_19:de:c4 (b0:7b:25:19:de:c4)
 - Source: ExtremeNetworks_9a:82:e8 (02:04:96:9a:82:e8)
 - Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.250.65.134
- Transmission Control Protocol, Src Port: 80, Dst Port: 37180, Seq: 4345, Ack: 390, Len: 5

The packet bytes pane shows the raw data of the frame, starting with the Ethernet header (02 04 96 9a 82 e8 b0 7b) and the IP header (25 19 de c4 08 00 45 00). The ASCII representation of the data is also shown on the right, starting with the GET request line.

Figure 3: Packet Details

(5) What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu. What device has this as its Ethernet address?

The Ethernet source address is `02:04:96:9a:82:e8` . This is not the Ethernet address of `gaia.cs.umass.edu`; it is the Ethernet address of the interface of our next-hop router, that is in the lab.

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

The destination address in the Ethernet frame is `b0:7b:25:19:de:c4` . Yes, this is the Ethernet address of my computer.

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

The hexadecimal value for the two-byte Frame type field in the Ethernet frame is `0x0800` in the Ethernet frame carrying the HTTP GET request. This corresponds to the `IPv4` (Internet Protocol Version 4) Network Layer Protocol.

(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” in “OK” appears at the `80th Byte` from the start of the frame, as seen in Figure (4) below. If we go by zero-based ndexing, then it is `Byte 79` .

0000	b0 7b 25 19 de c4 02 04 96 9a 82 e8 08 00 45 00	·{%. E·
0010	05 dc 1f 2d 40 00 3f 06 54 eb 80 77 f5 0c 0a fa	· · · -@·?· T·w· · ·
0020	41 86 00 50 91 3c 5d 0d b1 0d dd 51 f7 6c 80 18	A· ·P·<]· · ·Q·1· ·
0030	00 7a 10 d1 00 00 01 01 08 0a 0e be ae 52 88 66	·z· · · · · · · · ·R·f
0040	68 66 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f	hfHTTP/1 .1 200 0
0050	4b 0d 0a 44 61 74 65 3a 20 54 75 65 2c 20 32 31	K· ·Date: Tue, 21
0060	20 4d 61 72 20 32 30 32 33 20 30 35 3a 30 38 3a	Mar 202 3 05:08:
0070	34 38 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20	48 GMT· · Server:

Figure 4: ASCII ‘O’

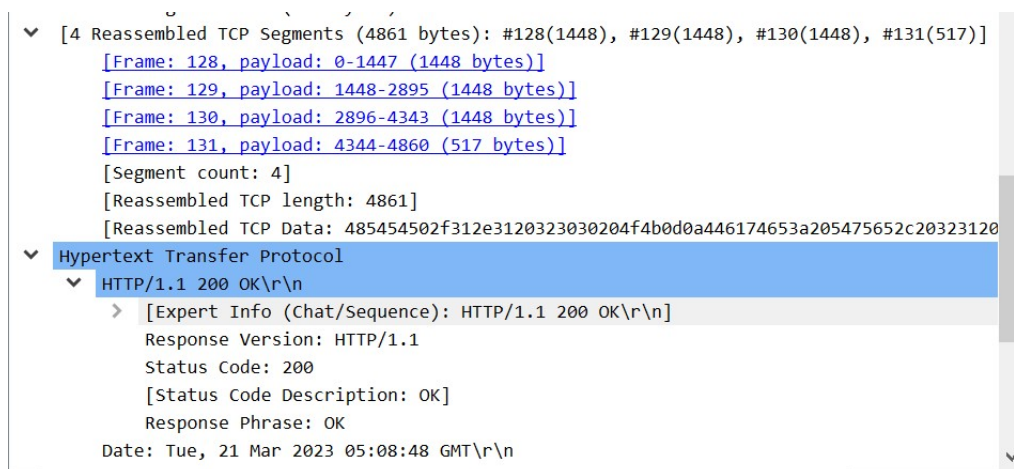


Figure 5: Ethernet frames containing HTTP OK message

(9) How many Ethernet frames (each containing an IP datagram, each containing a TCP segment) carry data that is part of the complete HTTP “OK 200 ...” reply message?

Four Ethernet Frames are observed to carry data that is part of the complete HTTP “OK 200 ...” reply message.

2 Answers to Part 2: Address Resolution Protocol

In this section, we shall observe the ARP protocol in action. Below is a screenshot of when the command `arp -a` is run in Windows Command Prompt. Following this, `arp -d -a` is run to clear the ARP cache. No output is displayed for the `-d` flag, but entries in the ARP cache will significantly reduce.

```
C:\Users\bsidd>arp -a

Interface: 10.196.9.171 --- 0x9
Internet Address      Physical Address      Type
10.196.3.250          02-04-96-9a-82-e8    dynamic
10.196.3.251          ca-f1-96-b3-5f-42    dynamic
10.196.4.27           9e-12-e3-5f-5c-f5    dynamic
10.196.5.162          fe-15-f3-10-62-6f    dynamic
10.196.5.186          6e-a3-ad-17-b5-b8    dynamic
10.196.5.197          f0-86-20-89-e1-c4    dynamic
10.196.5.228          d0-d0-03-a3-54-14    dynamic
10.196.7.36           82-81-ec-49-78-fa    dynamic
10.196.7.194          ce-e8-d6-9c-76-73    dynamic
10.196.8.35           48-46-c1-69-42-25    dynamic
10.196.8.36           34-cf-f6-8f-5f-f2    dynamic
10.196.8.223          04-6c-59-0f-8d-f9    dynamic
10.196.9.249          b8-08-cf-88-a2-cf    dynamic
10.196.10.68          44-5c-e9-e8-5a-48    dynamic
10.196.46.192         a2-22-3d-b2-a1-e7    dynamic
10.196.50.117         b4-c9-b9-b5-dd-40    dynamic
10.196.83.146         00-04-96-f6-64-a4    dynamic
10.196.99.53          70-2a-d5-f0-9e-a0    dynamic
10.196.131.133        f2-ad-d6-6f-0f-de    dynamic
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
224.0.0.253           01-00-5e-00-00-fd    static
224.0.1.187           01-00-5e-00-01-bb    static
```

Figure 6: `arp -a` on Windows

There are quite a lot of entries, so here is the ARP cache obtained on a Linux-based system.

```
user@sysad-OptiPlex-7050-1: ~
user@sysad-OptiPlex-7050-1:~$ arp -a
? (10.250.65.251) at 00:04:96:9e:78:77 [ether] on eno2
? (10.250.65.252) at 00:04:96:cc:fd:68 [ether] on eno2
_gateway (10.250.65.250) at 02:04:96:9a:82:e8 [ether] on eno2
? (10.250.65.254) at 00:04:96:9e:8b:e5 [ether] on eno2
? (10.250.65.253) at 00:04:96:9e:47:a3 [ether] on eno2
? (10.250.65.243) at 30:b6:2d:a7:1c:ff [ether] on eno2
user@sysad-OptiPlex-7050-1:~$
```

Figure 7: `arp -a` on Linux

(1) How many entries are stored in your ARP cache?

Six Entries are observed to be stored in the ARP cache shown in Figure (7).

(2) What is contained in each displayed entry of the ARP cache?

Each of the entries contains the IP address, MAC address pairs of devices in the network. It also has the connection type, shown as [ether] for the entries in the figure.

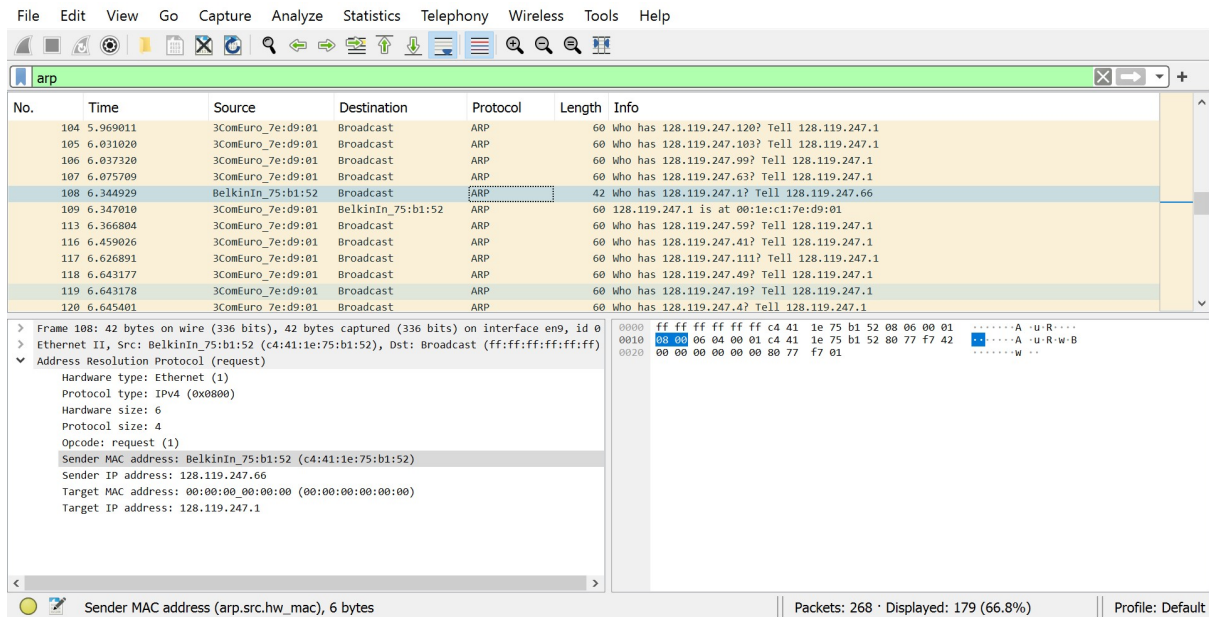


Figure 8: Packet Trace observed

We shall now focus on the packet trace given, `ethernet-wireshark-trace1.pcapng`, which is shown in Figure (8) above.

(3) What is the hexadecimal value of the source address in the Ethernet frame containing the ARP request message sent out by your computer?

The hexadecimal value of the source address in the Ethernet frame containing the ARP request message is `c4:41:1e:75:b1:52`.

(4) What is the hexadecimal value of the destination addresses in the Ethernet frame containing the ARP request message sent out by your computer? And what device (if any) corresponds to that address (e.g., client, server, router, switch or otherwise...)?

The hexadecimal value of the destination addresses in the Ethernet frame containing the ARP request message is `ff:ff:ff:ff:ff:ff`. This is a broadcast address, which corresponds to all devices on the network.

(5) What is the hexadecimal value for the two-byte Ethernet Frame type field? What upper layer protocol does this correspond to?

The hexadecimal value for the two-byte Ethernet Frame type field, as seen in Figure (8) is observed to be `0x0806`. This corresponds to Address Resolution Protocol (ARP).

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

The ARP opcode begins at the 21st byte from the start of the frame, as seen in Figure (4). If we go by zero-based indexing, then it is Byte 20 .

0000	ff	ff	ff	ff	ff	ff	00	1e	c1	7e	d9	01	08	06	00	01~.....
0010	08	00	06	04	00	01	00	1e	c1	7e	d9	01	80	77	f7	01[0001]....W..
0020	00	00	00	00	00	00	80	77	f7	4d	00	00	00	00	00	00W..M.....
0030	00	00	00	00	00	00	00	00	20	20	20	20				

Figure 9: ARP Opcode

(7) What is the value of the opcode field within the ARP request message sent by your computer?

The value of the opcode field within the ARP request message is 1 (Hex: 0x0001). This refers to ARP Request.

(8) Does the ARP request message contain the IP address of the sender? If the answer is yes, what is that value?

Yes, the ARP request message contains the IP address of the sender. That value is 128.119.247.1 , as seen in Figure (8).

(9) What is the IP address of the device whose corresponding Ethernet address is being requested in the ARP request message sent by your computer?

The IP address of the device whose corresponding Ethernet address is being requested in the ARP request message is 128.119.247.77 . It is observed in the Target IP address field.

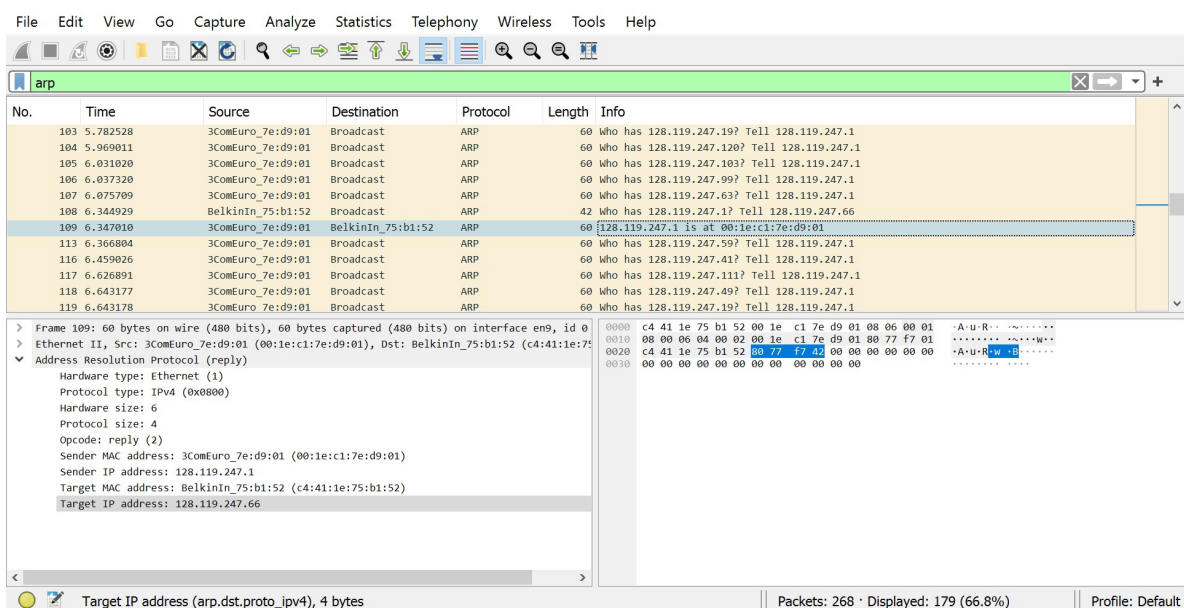


Figure 10: ARP Reply

Let's look at the ARP reply message, and answer some questions regarding the same. The screenshot of the packet details is shown in Figure (10).

(10) What is the value of the opcode field within the ARP reply message received by your computer?

The value of the opcode field within the ARP reply message is **2** (Hex: 0x0002). This refers to ARP Reply.

(11) What is the Ethernet address corresponding to the IP address that was specified in the ARP request message sent by your computer?

The Ethernet address corresponding to the IP address that was specified in the ARP request message is **00:1e:c1:7e:d9:01**.

(12) We've looked at the ARP request message sent by your computer running Wireshark, and the ARP reply message sent in response. But there are other devices in this network that are also sending ARP request messages that you can find in the trace. Why are there no ARP replies in your trace that are sent in response to these other ARP request messages?

The ARP Request is broadcast, but the ARP Responses are not broadcast. So, there are no ARP replies in your trace that are sent in response to the other ARP request messages.