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.

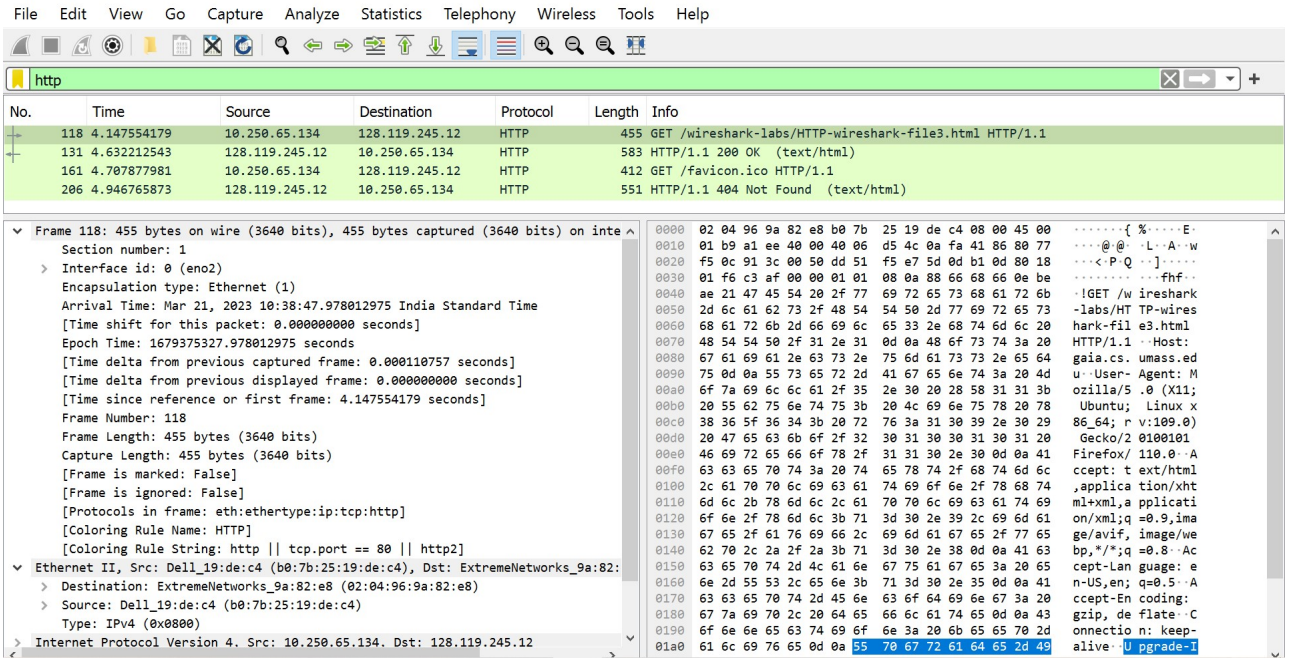

Figure 1: Packet Trace observed

(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 ndexing, then it is `Byte 66` .

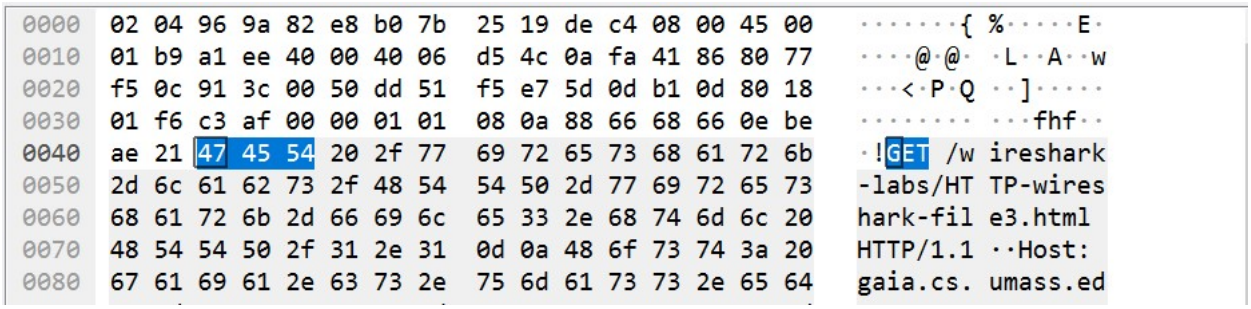

Figure 2: ASCII 'G'

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

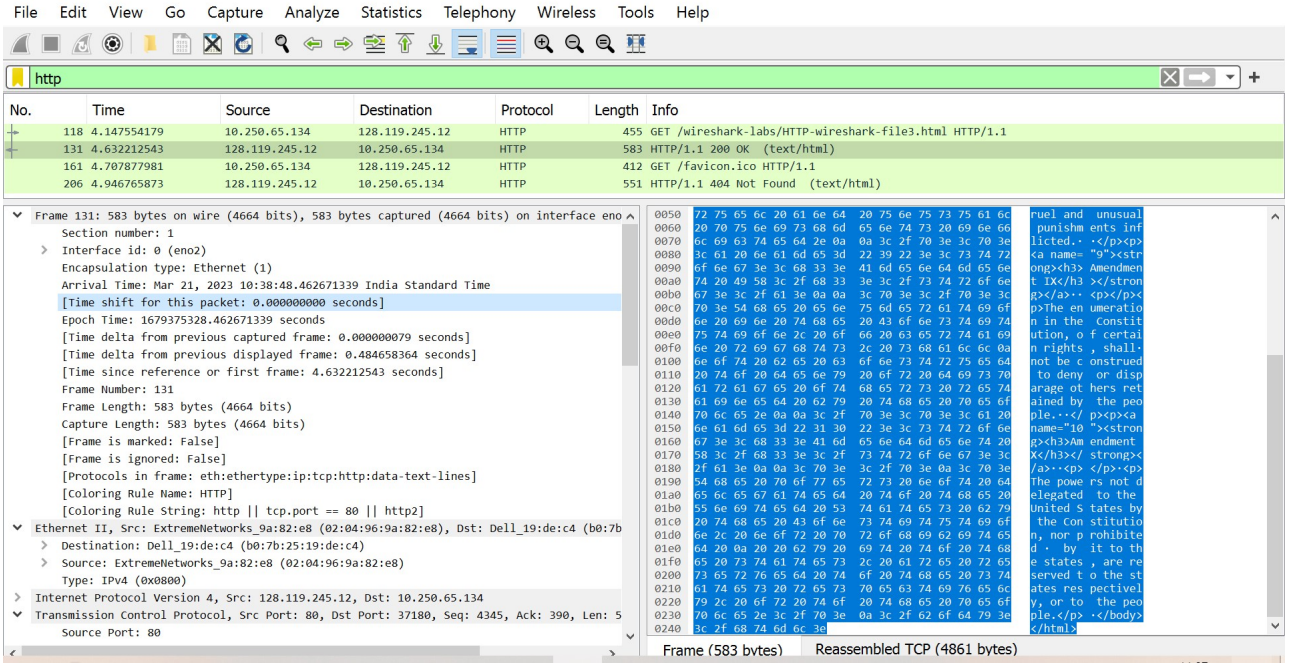

Figure 3: Packet Details

(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` .

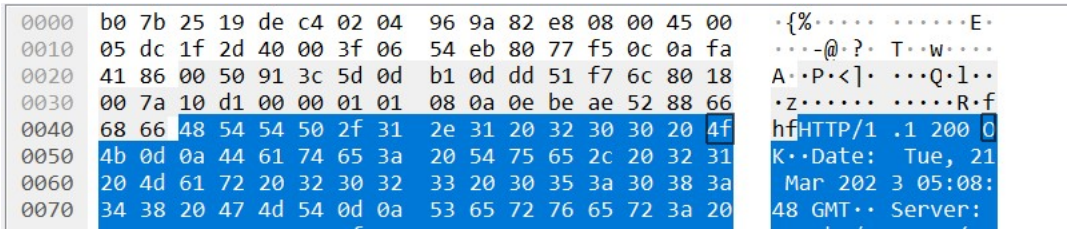

Figure 4: ASCII 'O'

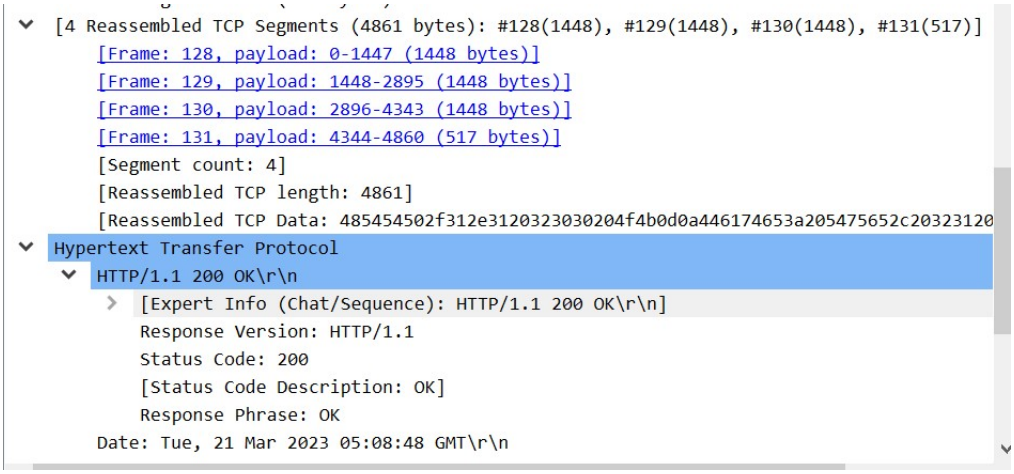

Figure 5: Ethernet frames containing HTTP OK message

(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.

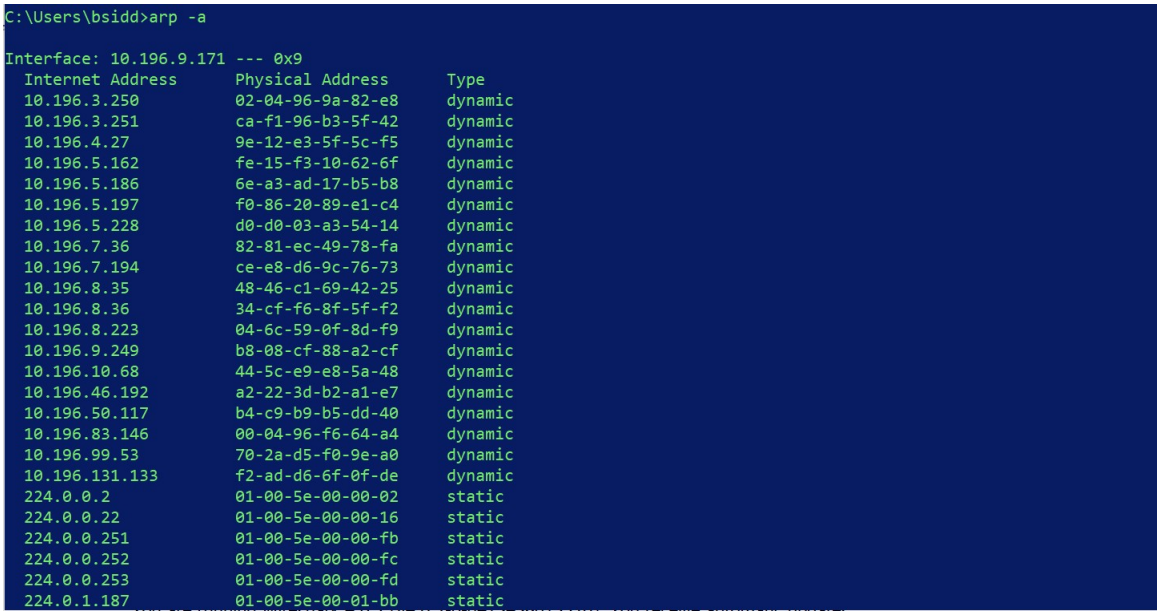

Figure 6: `arp -a` on Windows

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

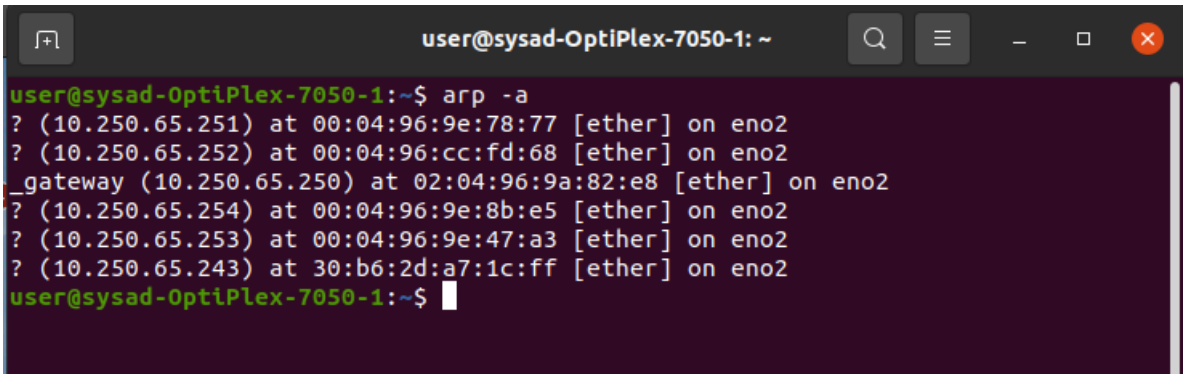

Figure 7: `arp -a` on Linux

(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.

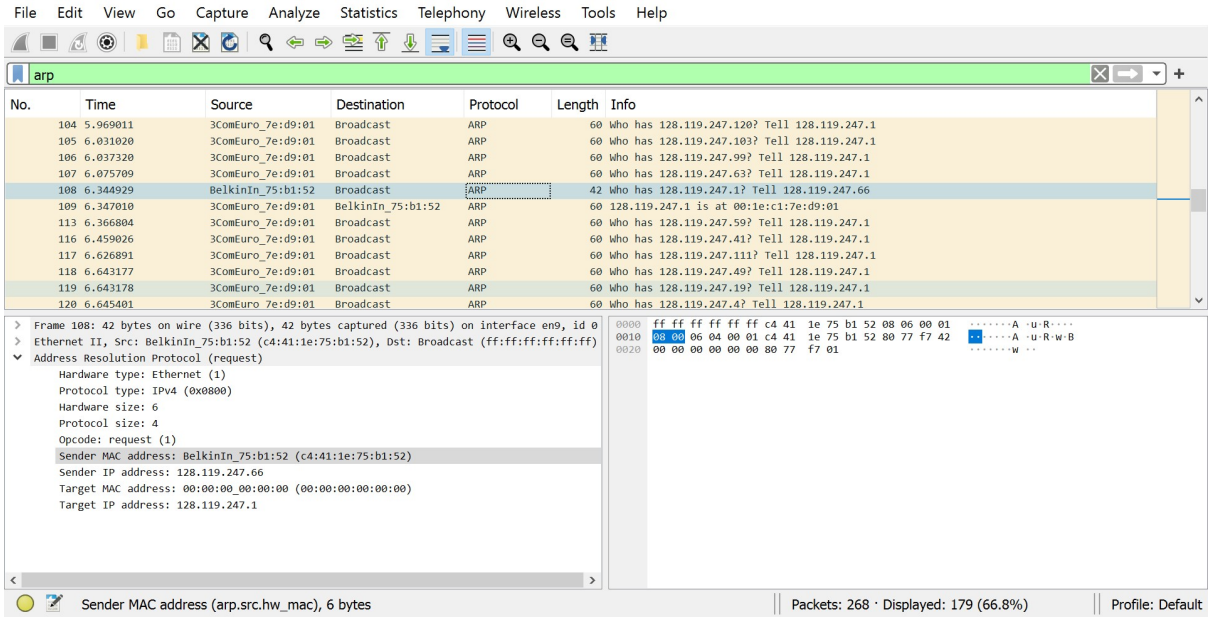

Figure 8: Packet Trace observed

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 ndexing, then it is `Byte 20` .

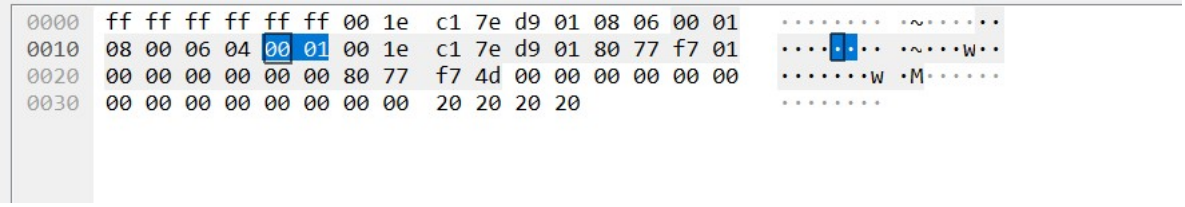

Figure 9: ARP Opcode

(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.

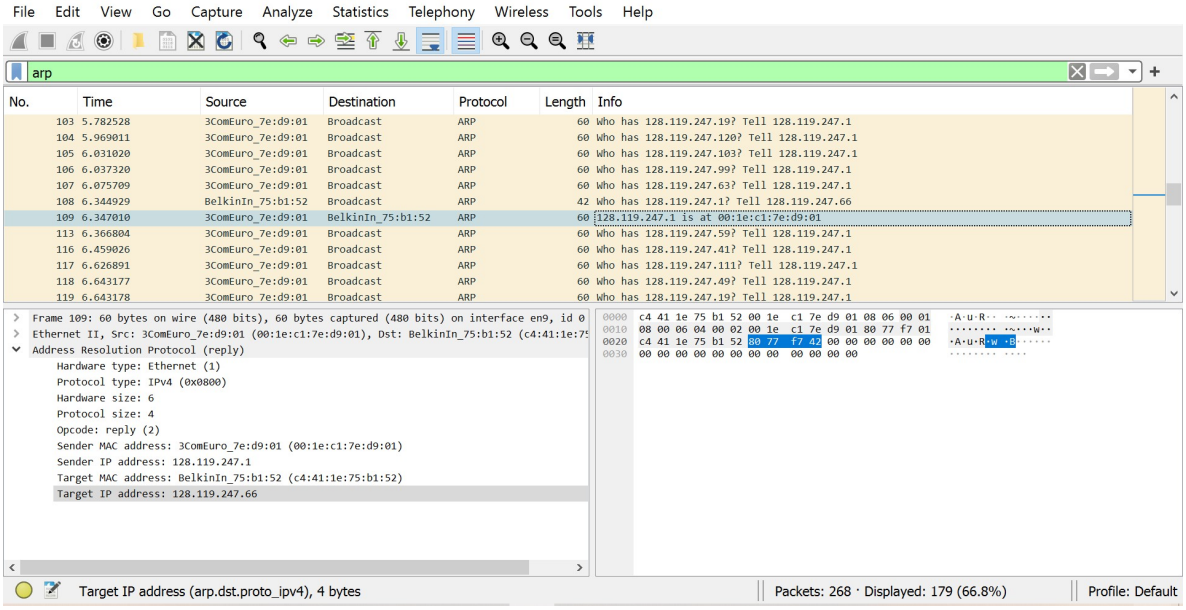

Figure 10: ARP Reply

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.