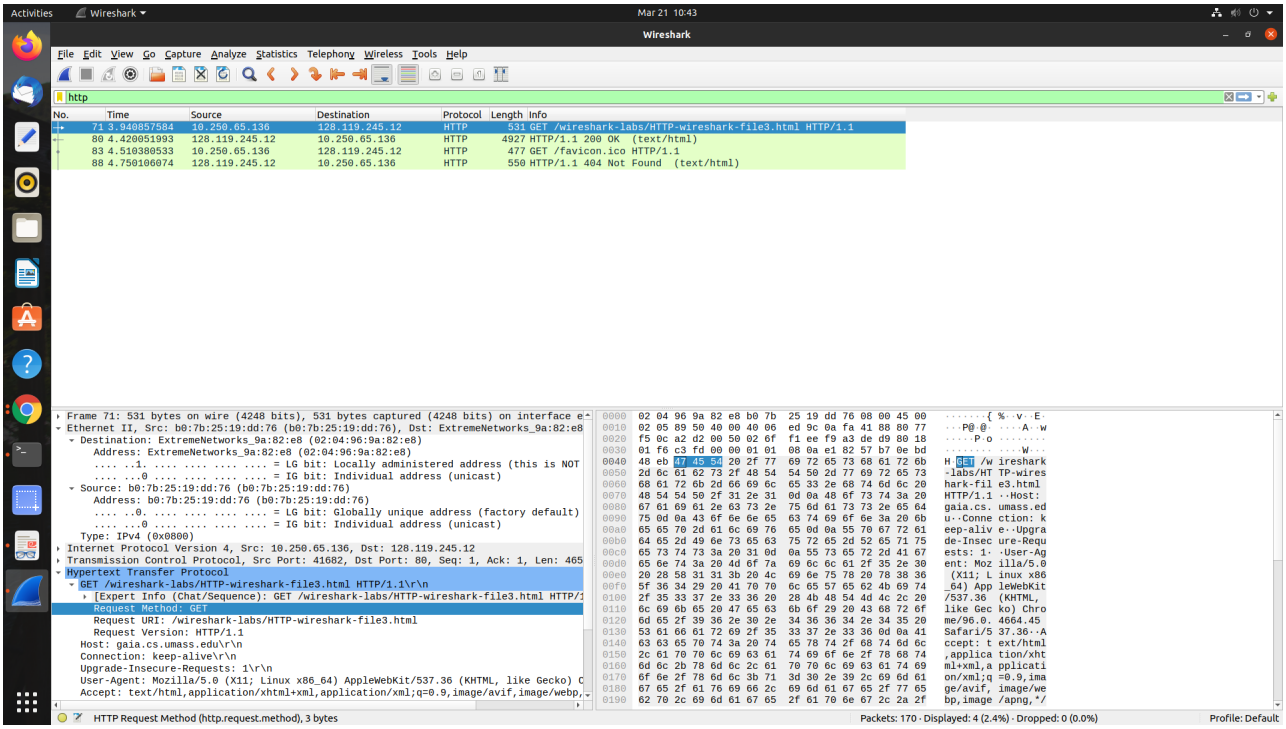
CS315 : Computer Networks Lab

Assignment 11

Sourabh Bhosale (200010004)

March 21, 2023

1 Part-1: Capturing and analyzing Ethernet frames



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

Ethernet address of my computer: b0:7b:25:19:dd:76

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?

Destination address: 02:04:96:9a:82:e8

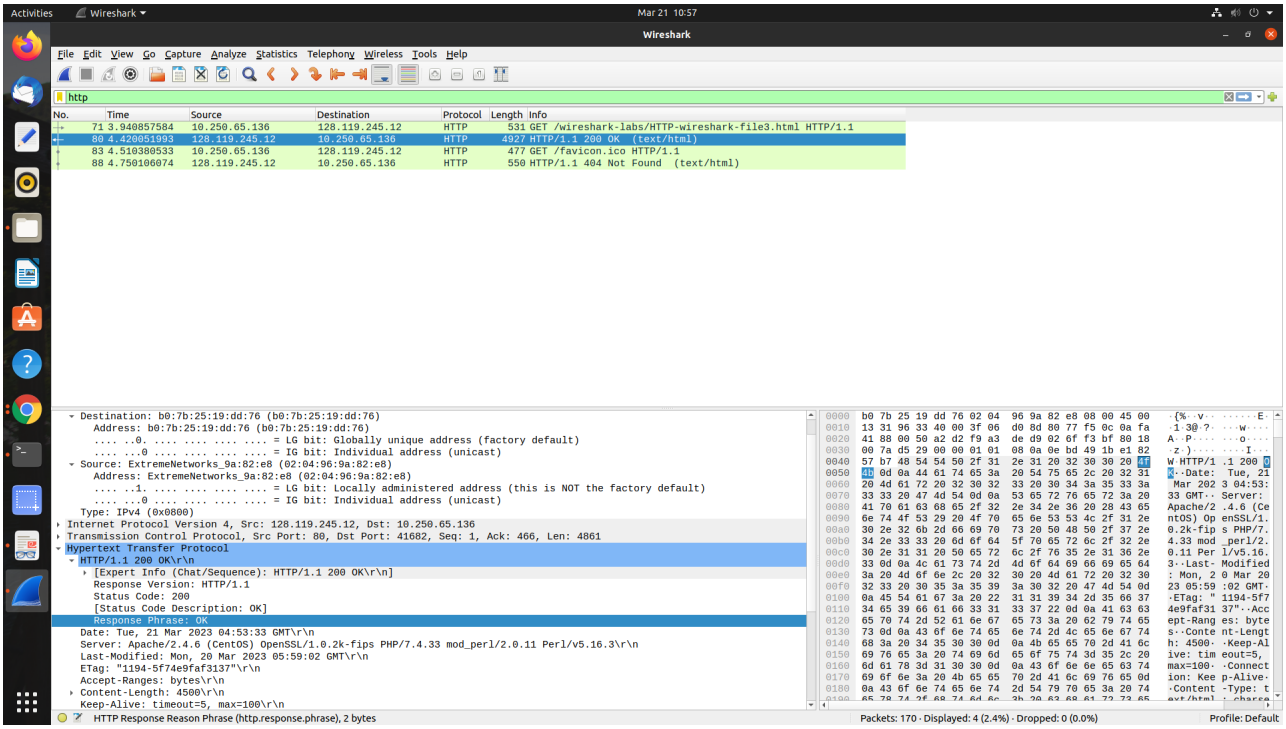
No, this address is not the Ethernet address of gaia.cs.umass.edu. It is address of my ExtremeNetworks Link router.

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?

Hexadecimal value for frame type field is Type: IPv4 (0x0800). This corresponds to IP protocol.

4. How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame? Do not count any preamble bits in your count, i.e., assume that the Ethernet frame begins with the Ethernet frame's destination address.

66 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?

Source address: 02:04:96:9a:82:e8
No, this is not the address of my computer or of gaia.cs.umass.edu. This is the address of my router.

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

Destination address: b0:7b:25:19:dd:76
This is the address of my computer.

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

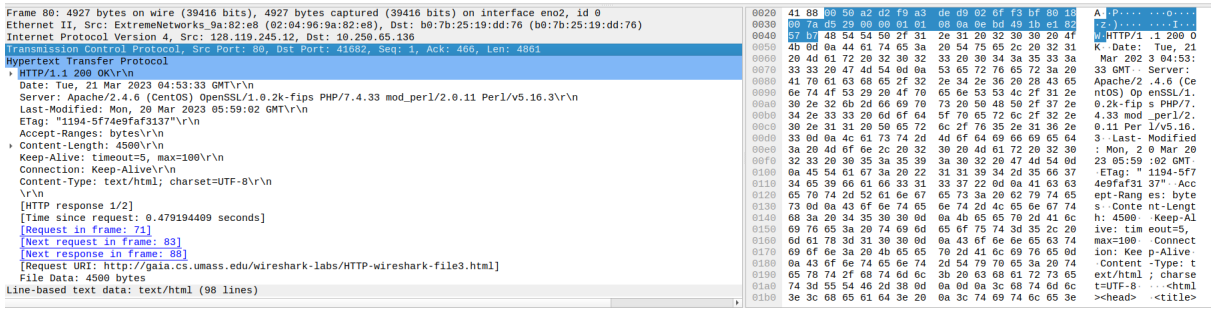
Hexadecimal value for frame type field is Type: IPv4 (0x0800). This corresponds to IP protocol.

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? Do not count any preamble bits in your count, i.e., assume that the Ethernet frame begins with the Ethernet frame's destination address.

79 bytes into the frame.

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?

Only 1 Ethernet frame carries data that is part of complete HTTP "OK 200 ..." reply message.



2 Part-2: The Address Resolution Protocol

```
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
? (10.250.65.253) at 00:04:96:9e:47:a3 [ether] on eno2
_gateway (10.250.65.250) at 02:04:96:9a:82:e8 [ether] on eno2
? (10.250.65.243) at 30:b6:2d:a7:1c:ff [ether] on eno2
user@sysad-OptiPlex-7050-1:~$
```

1. How many entries are stored in your ARP cache?

5 entries.

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

The ARP cache contains entries that map IP addresses to MAC addresses.

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

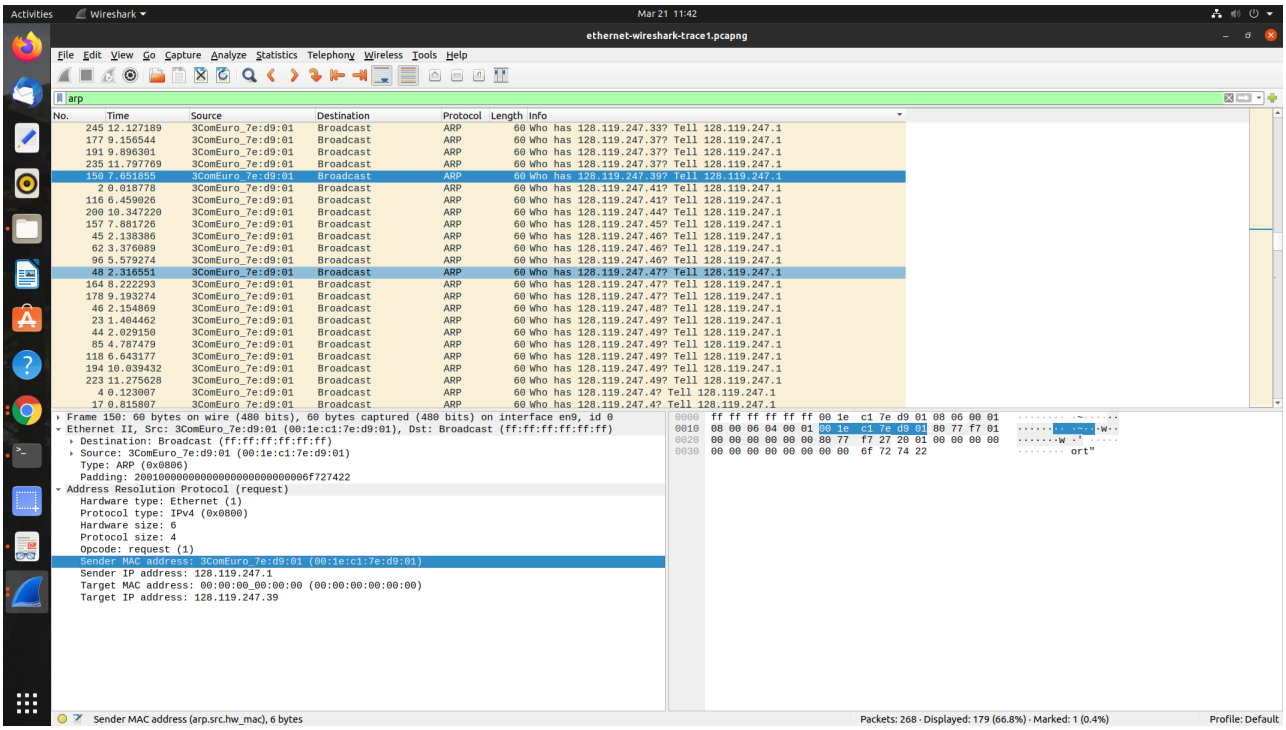
Source address: 00:1e:c1:7e:d9:01

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…)?

Destination address: Broadcast (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?

Type: ARP (oxo8o6). This corresponds to ARP protocol.



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

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

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

Opcode: 0x0001

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

Yes, Sender IP address: 128.119.247.1

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?

Target IP address: 128.119.247.39

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

Opcode: 0x0002 (request (2))

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

c4:41:1e:75:b1:52

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?

There is no reply in this trace, because we are not at the machine that sent the request. The ARP request is broadcast, but the ARP reply is sent back directly to the sender's Ethernet address.