

Lab 2: Ethernet and ARPA

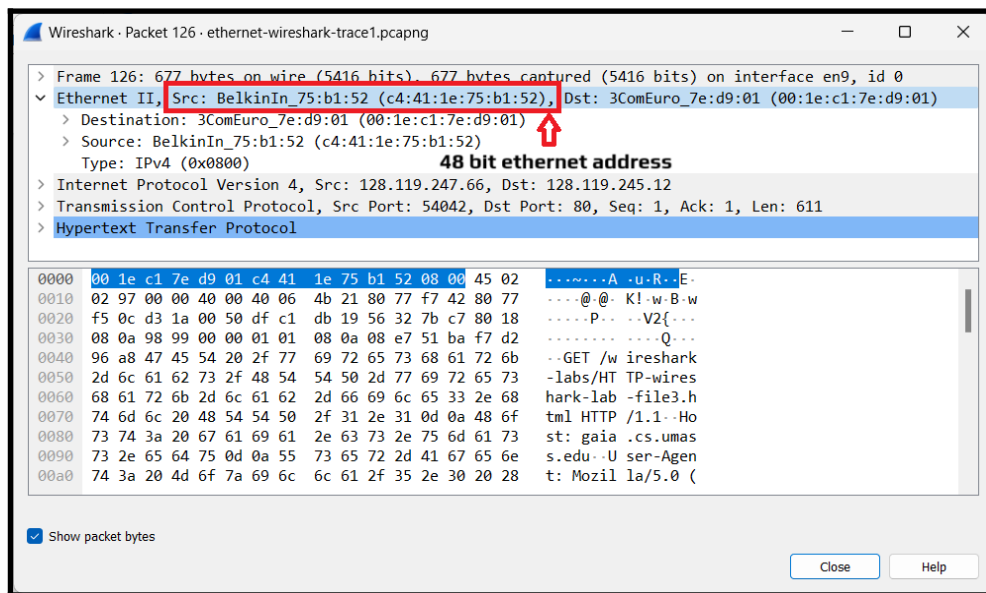
University of Windsor
Department of Electrical and Computer Engineering
ELEC 8560 – Computer Networks
Semester: Fall 2023

Student Name: Amey Mahendra Thakur

Student number: 110107589

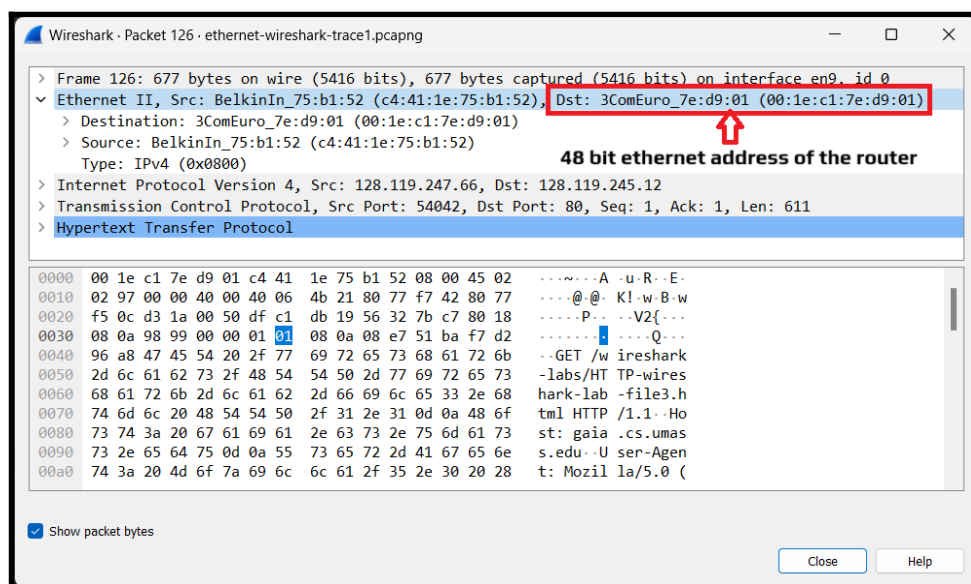
Answers: You need to use full SS, not partial for 1, 2, 5 and 6.

1. The 48-bit Ethernet address of the computer used to capture packet in wireshark using given zip file is **c4:41:1e:75:b1:52**.

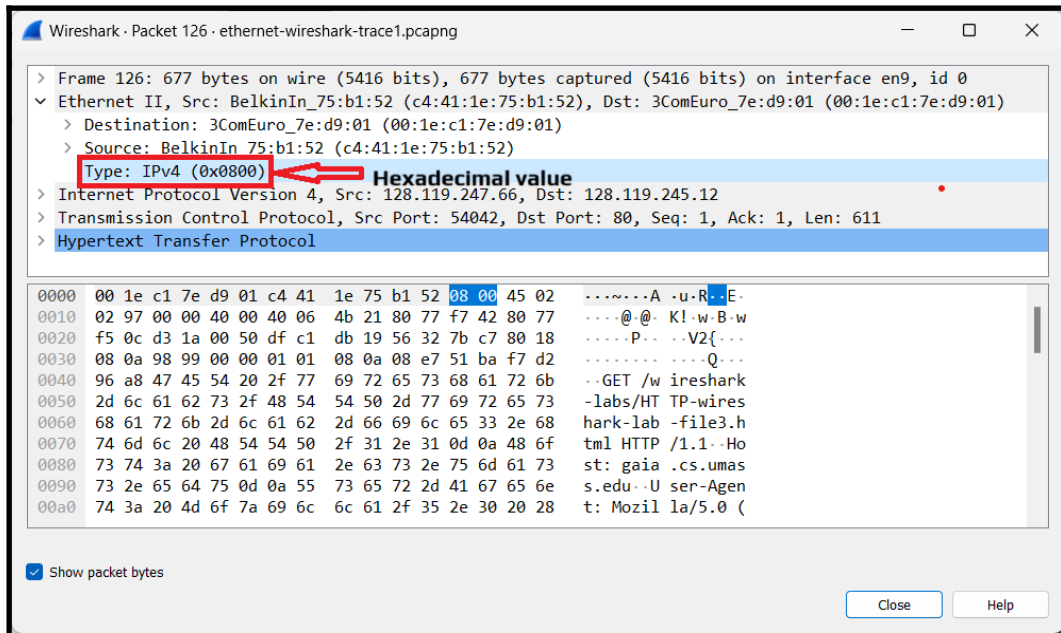


2. The 48-bit destination address in the Ethernet frame is **00:1e:c1:7e:d9:01**. This is NOT the Ethernet address of "gaia.cs.umass.edu." It is the address of my **ComEuro router**.

- 0.5



3. The hexadecimal value for the two-byte Frame type field in the Ethernet frame carrying the HTTP GET reques is **0x0800**.



4. I have 66 Bytes before the ASCII character “G” in HTTP GET

Which can be classified as:

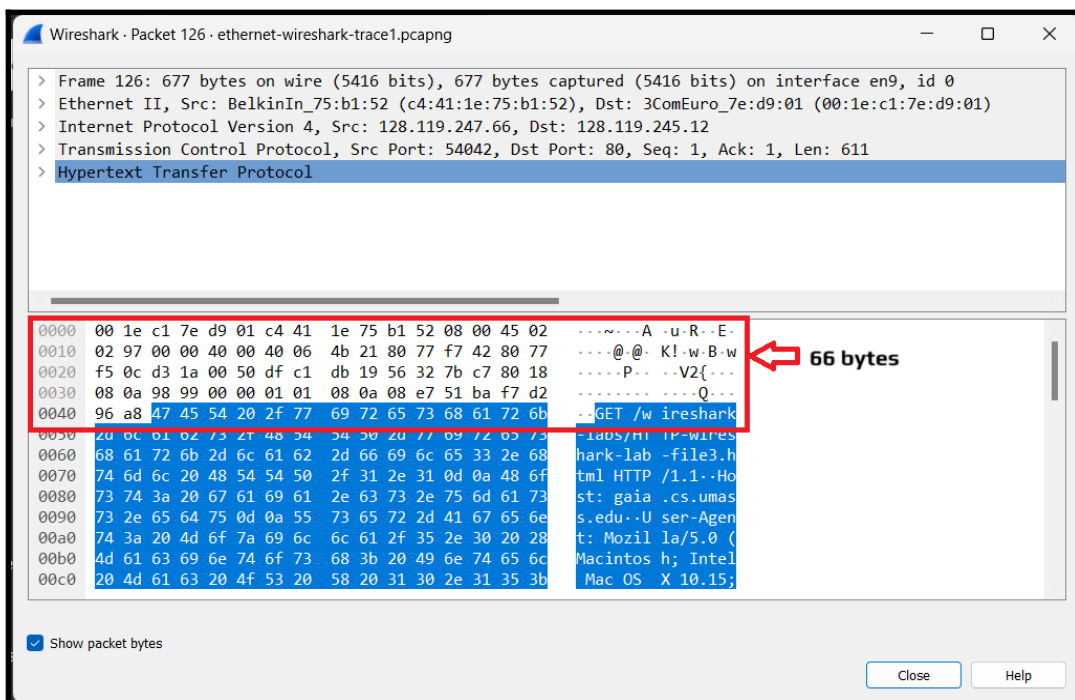
No. of bytes in Ethernet Frame: 14

No. of bytes in IP Frame: 20

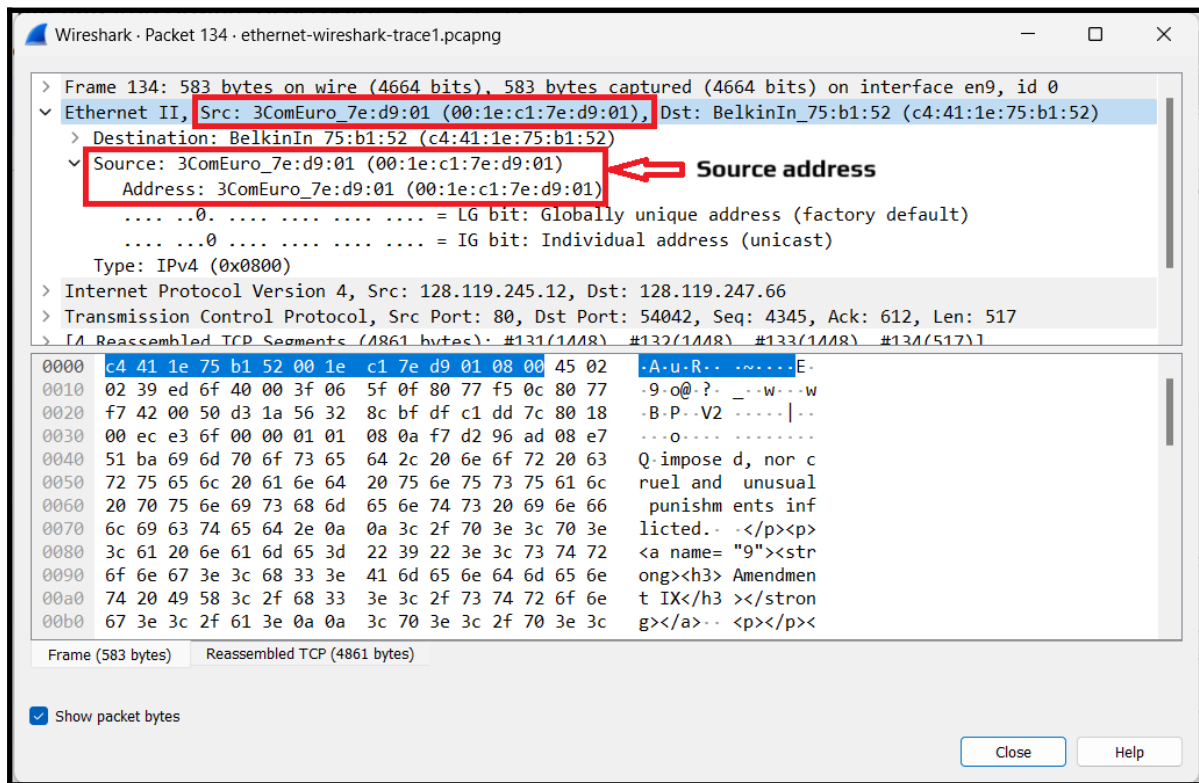
No. of bytes in TCP Frame: 32

 Total Number of Bytes before “G”: 66

After removing the 2 preamble bytes, the resulting data is : $66 - 2 = 64$.

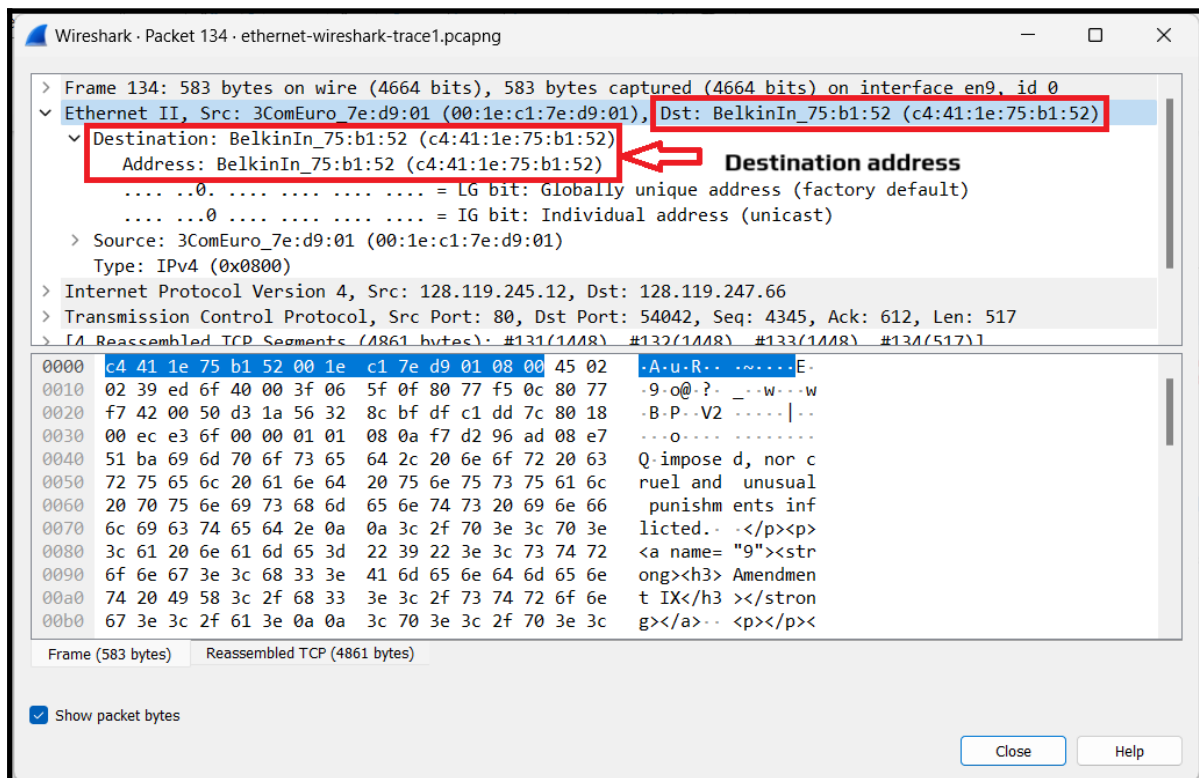


5. The source address **00:1e:c1:7e:d9:01** is neither the Ethernet address of “gaia.cs.umass.edu” nor the address of my computer. It is the address of **ComEuro router**.

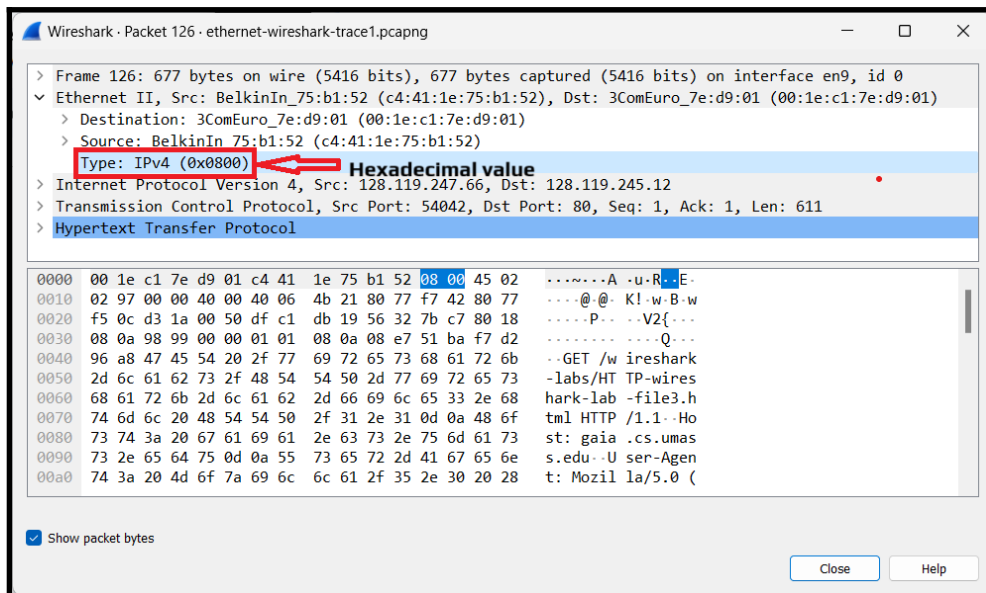


- 0.5

6. The destination address **c4:41:1e:75:b1:52** is the address of my computer.



7. The hex value for the Frame type field is **0x0800**. (Note - same as question 3)



8. I have 54 Bytes before the HTTP OK response and in HTTP OK response and I have 13 Bytes before ASCII character “O” in HTTP frame.

Which can be classified as:

No. of bytes in Ethernet Frame: 14

No. of bytes in IP Frame: 20

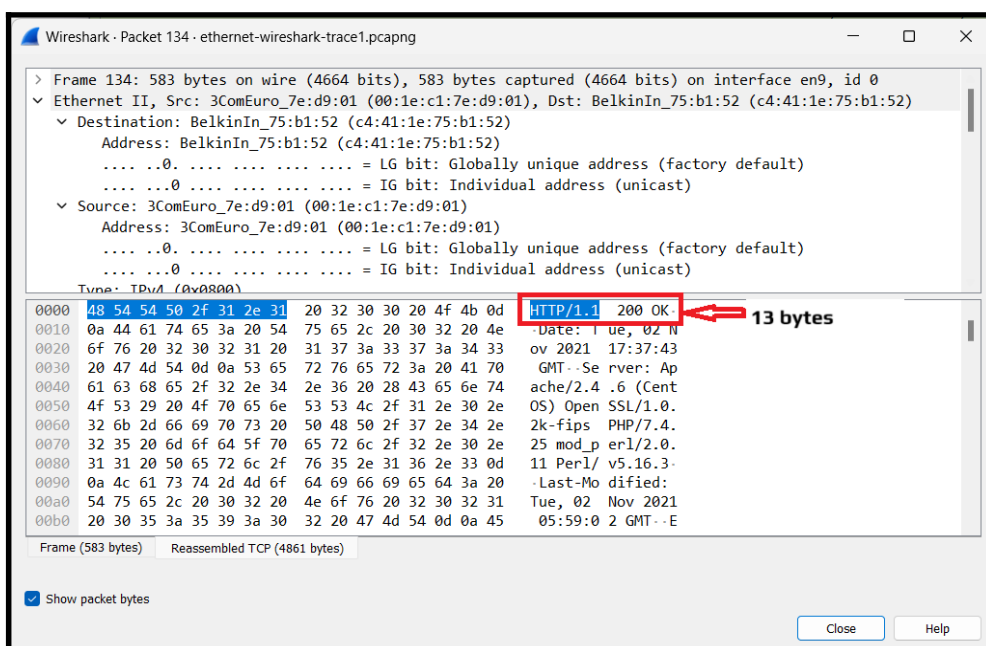
No. of bytes in TCP Frame: 32

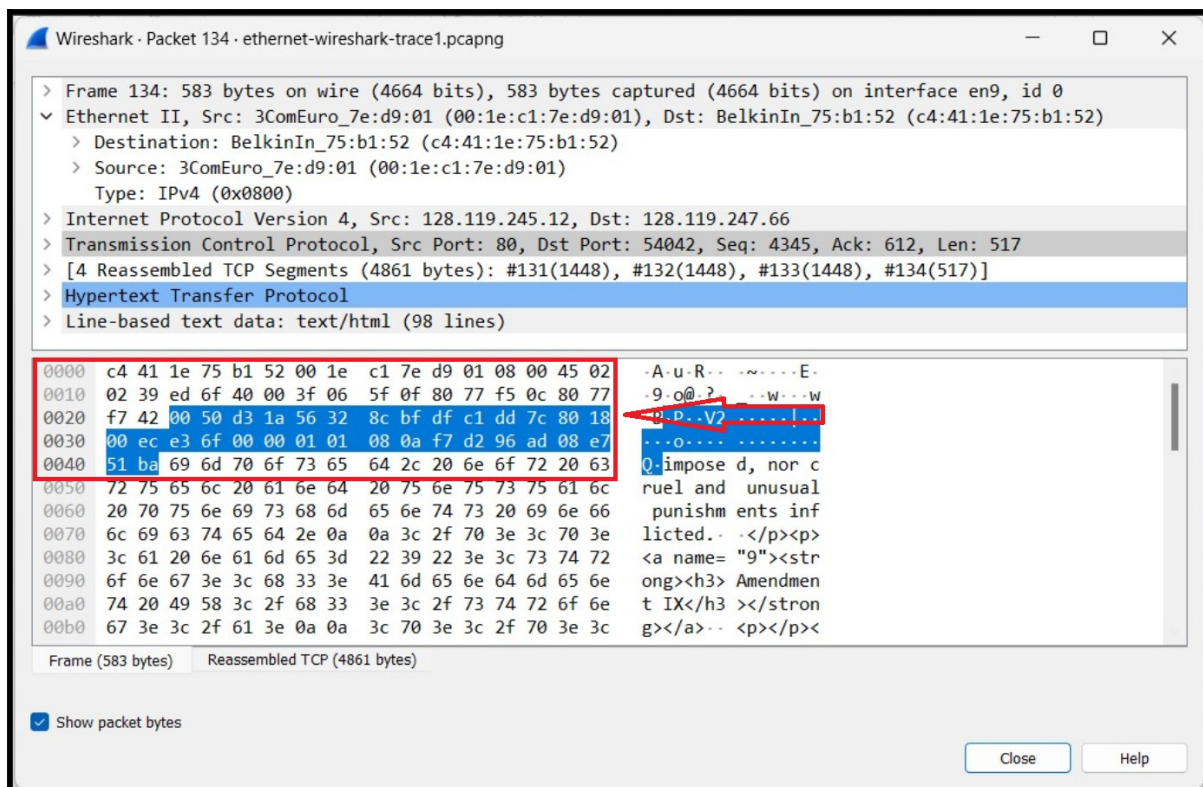
Total No. of Bytes before HTTP OK : 66

No. of Bytes before “O” in the response: 13

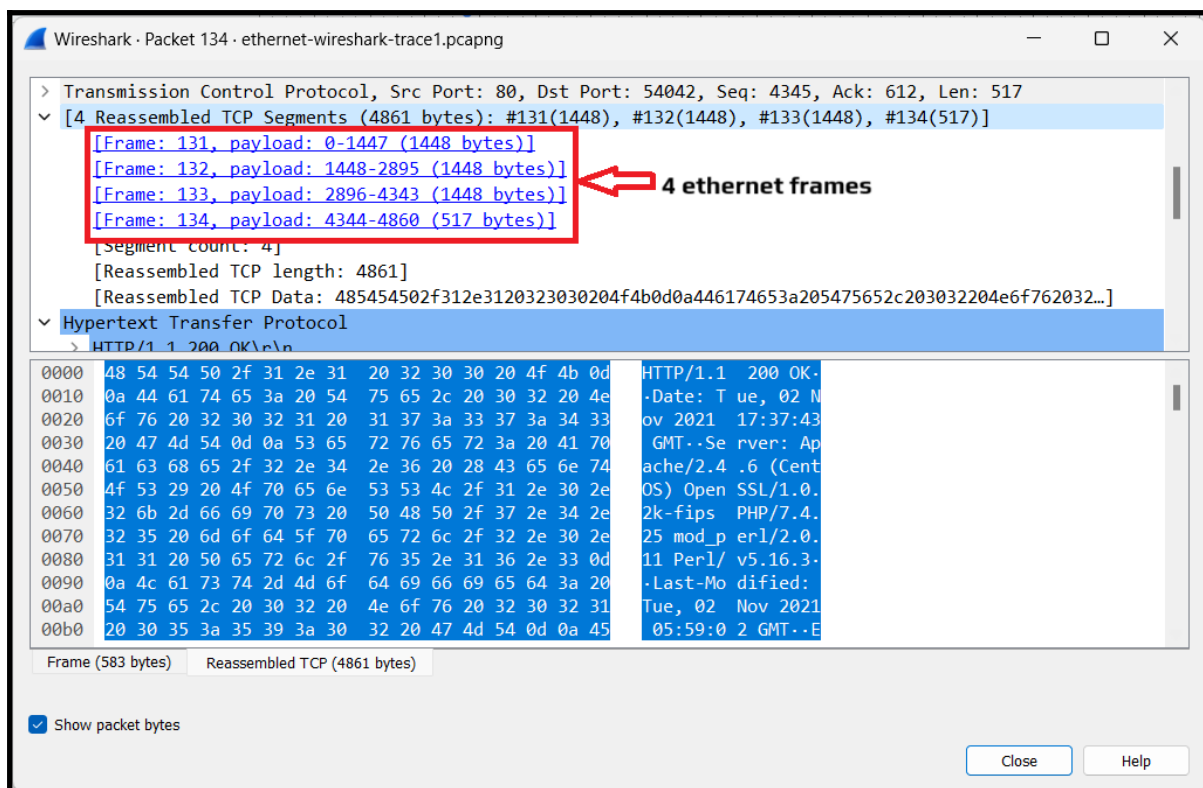
Total No. of Bytes before ASCII “O” : 79

After removing the 2 preamble bytes, the resulting data is: $79 - 2 = 77$ bytes.

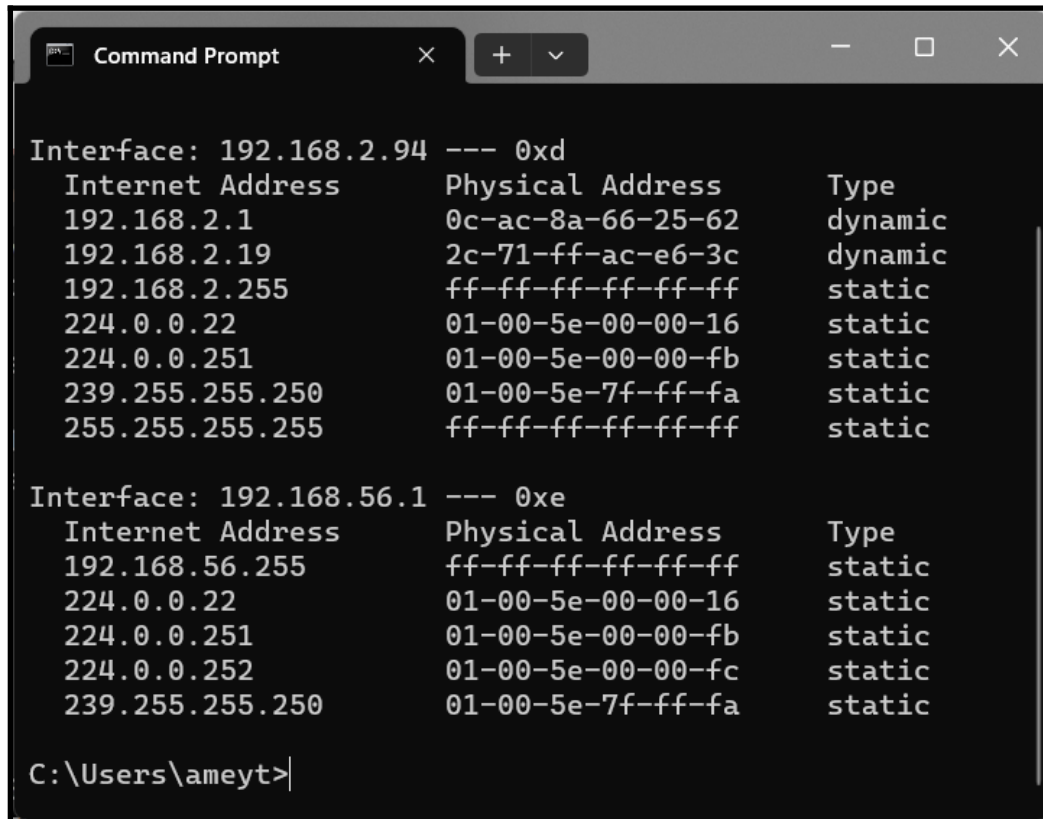




9. **4 Ethernet frames** (each containing an IP datagram, each containing a TCP segment) carry data that is part of the complete HTTP "OK 200 ..." reply message.



10. There are **2 interfaces** in ARP cache, where first interface had **7 entries** and second interface had **5 entries**.



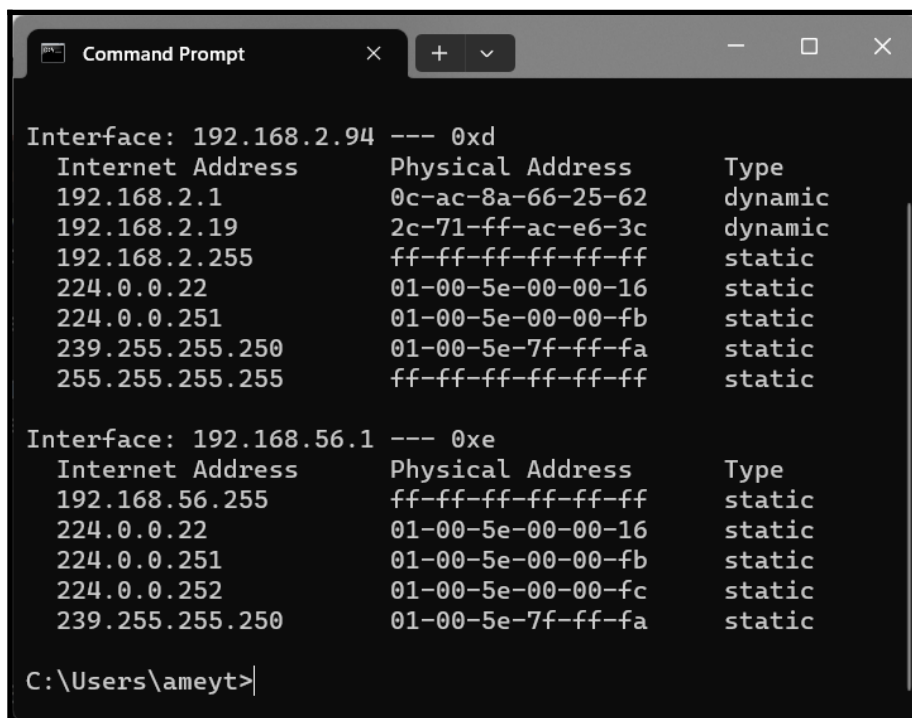
```
Command Prompt

Interface: 192.168.2.94 --- 0xd
Internet Address      Physical Address      Type
192.168.2.1          0c-ac-8a-66-25-62    dynamic
192.168.2.19         2c-71-ff-ac-e6-3c    dynamic
192.168.2.255        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
239.255.255.250      01-00-5e-7f-ff-fa    static
255.255.255.255      ff-ff-ff-ff-ff-ff    static

Interface: 192.168.56.1 --- 0xe
Internet Address      Physical Address      Type
192.168.56.255       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

C:\Users\ameyt>
```

11. What is contained in each displayed entry of the ARP cache
- There are three columns with values representing the IP address, Physical Address and the Type of address.



```
Command Prompt

Interface: 192.168.2.94 --- 0xd
Internet Address      Physical Address      Type
192.168.2.1          0c-ac-8a-66-25-62    dynamic
192.168.2.19         2c-71-ff-ac-e6-3c    dynamic
192.168.2.255        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
239.255.255.250      01-00-5e-7f-ff-fa    static
255.255.255.255      ff-ff-ff-ff-ff-ff    static

Interface: 192.168.56.1 --- 0xe
Internet Address      Physical Address      Type
192.168.56.255       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

C:\Users\ameyt>
```

Wrong packet selected for 12 and 13. The packet should be related to ARP request from your computer

12. The hexadecimal value of the source address in the Ethernet frame containing the ARP request message sent out by your computer is **00:1e:c1:7e:d9:01**.

ethernet-wireshark-trace1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp

No.	Time	Source	Destination	Protocol	Length	Info
78	13:37:40.514667	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.83? Tell 128.119.247.1
79	13:37:40.524072	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.85? Tell 128.119.247.1
80	13:37:40.659004	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.30? Tell 128.119.247.1
81	13:37:40.674701	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.2? Tell 128.119.247.1
82	13:37:40.739039	Apple_ac:ad:e1	Broadcast	ARP	60	Who has 169.254.1.0? Tell 128.119.247.79
83	13:37:41.148087	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.9? Tell 128.119.247.1
84	13:37:41.152168	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.4? Tell 128.119.247.1
85	13:37:41.234063	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.49? Tell 128.119.247.1
86	13:37:41.243049	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.72? Tell 128.119.247.1
87	13:37:41.360820	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.19? Tell 128.119.247.1
88	13:37:41.479737	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.119? Tell 128.119.247.1

> Frame 5: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface en9, id 0

> Ethernet II, Src: 3ComEuro_7e:d9:01 (00:1e:c1:7e:d9:01), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

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

> Source: 3ComEuro_7e:d9:01 (00:1e:c1:7e:d9:01)

> Type: ARP (0x0806)

> Trailer: c2cf0000000000000000000000000000

> Address Resolution Protocol (request)

0000 ff ff ff ff ff ff 00 1e c1 7e d9

0010 08 00 06 04 00 01 00 1e c1 7e d9

0020 00 00 00 00 00 00 80 77 f7 34 c2

0030 00 00 00 00 00 00 00 00 00 00

- 1

13. The hexadecimal value of the destination addresses in the Ethernet frame containing the ARP request message sent out by your computer **ff:ff:ff:ff:ff:ff** and there is no device.

ethernet-wireshark-trace1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp

No.	Time	Source	Destination	Protocol	Length	Info
78	13:37:40.514667	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.83? Tell 128.119.247.1
79	13:37:40.524072	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.85? Tell 128.119.247.1
80	13:37:40.659004	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.30? Tell 128.119.247.1
81	13:37:40.674701	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.2? Tell 128.119.247.1
82	13:37:40.739039	Apple_ac:ad:e1	Broadcast	ARP	60	Who has 169.254.1.0? Tell 128.119.247.79
83	13:37:41.148087	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.9? Tell 128.119.247.1
84	13:37:41.152168	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.4? Tell 128.119.247.1
85	13:37:41.234063	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.49? Tell 128.119.247.1
86	13:37:41.243049	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.72? Tell 128.119.247.1
87	13:37:41.360820	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.19? Tell 128.119.247.1
88	13:37:41.479737	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.119? Tell 128.119.247.1

> Frame 5: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface en9, id 0

> Ethernet II, Src: 3ComEuro_7e:d9:01 (00:1e:c1:7e:d9:01), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

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

> Source: 3ComEuro_7e:d9:01 (00:1e:c1:7e:d9:01)

> Type: ARP (0x0806)

> Trailer: c2cf0000000000000000000000000000

> Address Resolution Protocol (request)

0000 ff ff ff ff ff ff 00 1e c1 7e d9

0010 08 00 06 04 00 01 00 1e c1 7e d9

0020 00 00 00 00 00 00 80 77 f7 34 c2

0030 00 00 00 00 00 00 00 00 00 00

- 1

14. The hexadecimal value for the two-byte Ethernet Frame type field is **0x0806**. It corresponds to ARP protocol.

