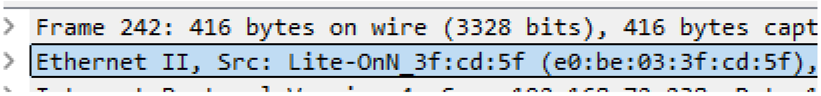
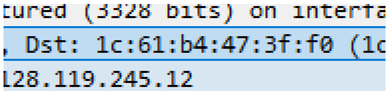
1. **What is the 48-bit Ethernet address of your computer?**



```
> Frame 242: 416 bytes on wire (3328 bits), 416 bytes capt
> Ethernet II, Src: Lite-OnN_3f:cd:5f (e0:be:03:3f:cd:5f),
```

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?**

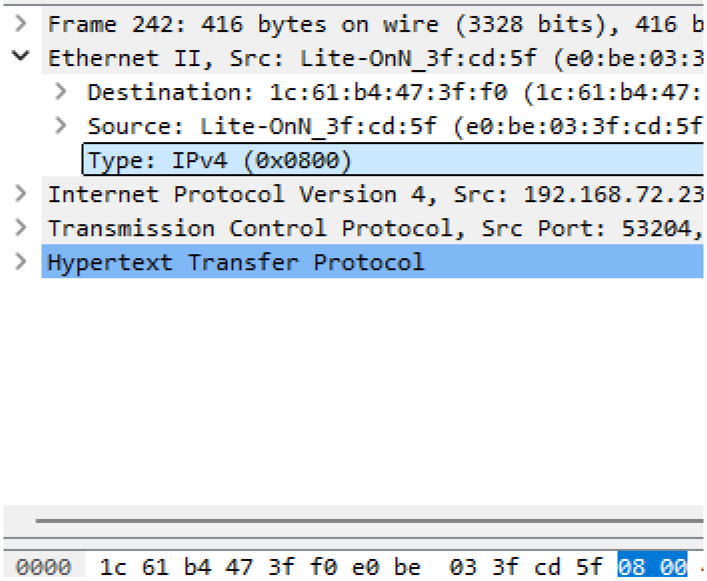
   Destination:



```
tured (3328 bits) on interfa
, Dst: 1c:61:b4:47:3f:f0 (1c
128.119.245.12
```

   It's the address of my 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?**



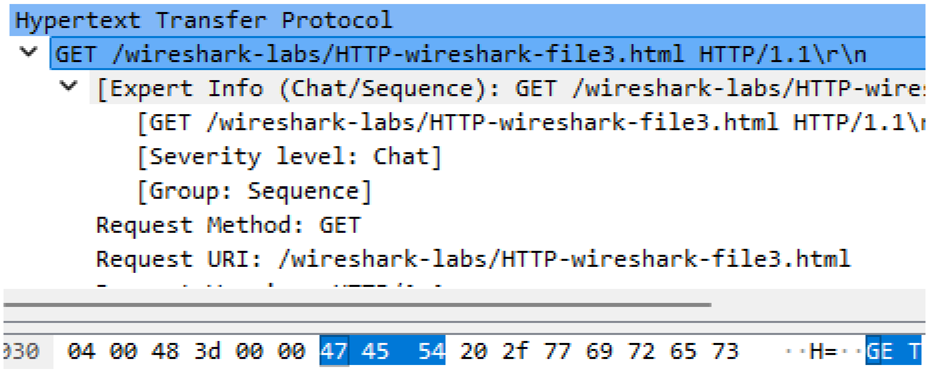
```
>  Frame 242: 416 bytes on wire (3328 bits), 416 b
v  Ethernet II, Src: Lite-OnN_3f:cd:5f (e0:be:03:3
     > Destination: 1c:61:b4:47:3f:f0 (1c:61:b4:47:
     > Source: Lite-OnN_3f:cd:5f (e0:be:03:3f:cd:5f
       Type: IPv4 (0x0800)
>  Internet Protocol Version 4, Src: 192.168.72.23
>  Transmission Control Protocol, Src Port: 53204,
>  Hypertext Transfer Protocol
```

```
0000  1c 61 b4 47 3f f0 e0 be  03 3f cd 5f 08 00 ·
```

   Two-byte frame type is 08 00, it's the 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.



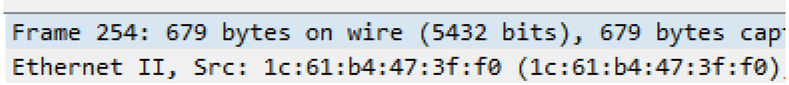
```
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wire
      [GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /wireshark-labs/HTTP-wireshark-file3.html

030  04 00 48 3d 00 00 47 45 54 20 2f 77 69 72 65 73   ··H=··GE T
```

G is equal to 47

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

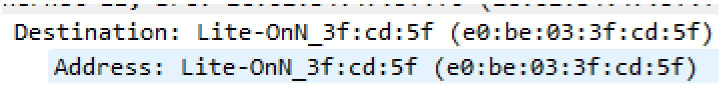
5. **What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is *no*). What device has this as its Ethernet address?**



```
Frame 254: 679 bytes on wire (5432 bits), 679 bytes cap
Ethernet II, Src: 1c:61:b4:47:3f:f0 (1c:61:b4:47:3f:f0)
```

The device is my router

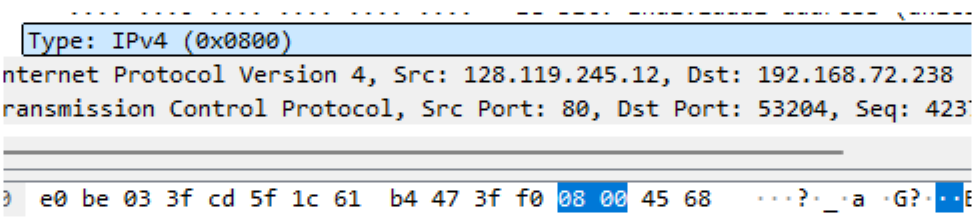
6. **What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?**



```
Destination: Lite-OnN_3f:cd:5f (e0:be:03:3f:cd:5f)
   Address: Lite-OnN_3f:cd:5f (e0:be:03:3f:cd:5f)
```

Yes it's my computer's address

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

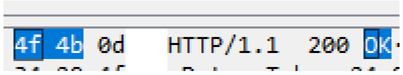


```
Type: IPv4 (0x0800)
nternet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.72.238
ransmission Control Protocol, Src Port: 80, Dst Port: 53204, Seq: 423

0  e0 be 03 3f cd 5f 1c 61  b4 47 3f f0 08 00 45 68   ···?·_·a ·G?···E
```

The upper layer is IP layer

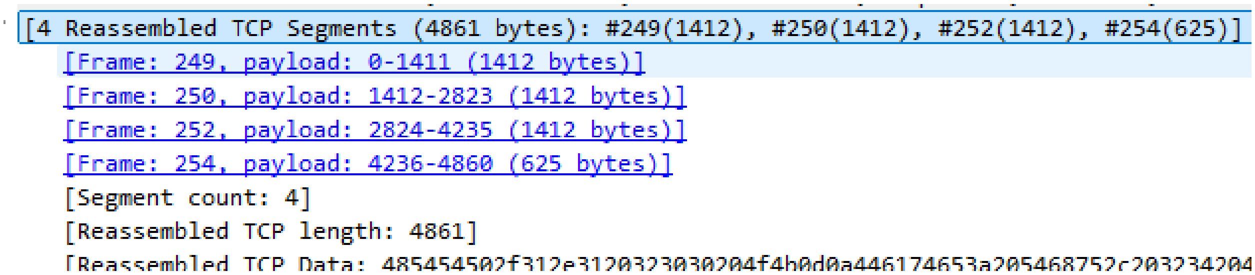
8. **How many bytes from the very start of the Ethernet frame does the ASCII “O” in “OK” (i.e., the HTTP response code) appear in the Ethernet frame? Do not count any preamble bits in your count, i.e., assume that the Ethernet frame begins with the Ethernet frame's destination address.**



```
4f 4b 0d   HTTP/1.1  200 OK·
```

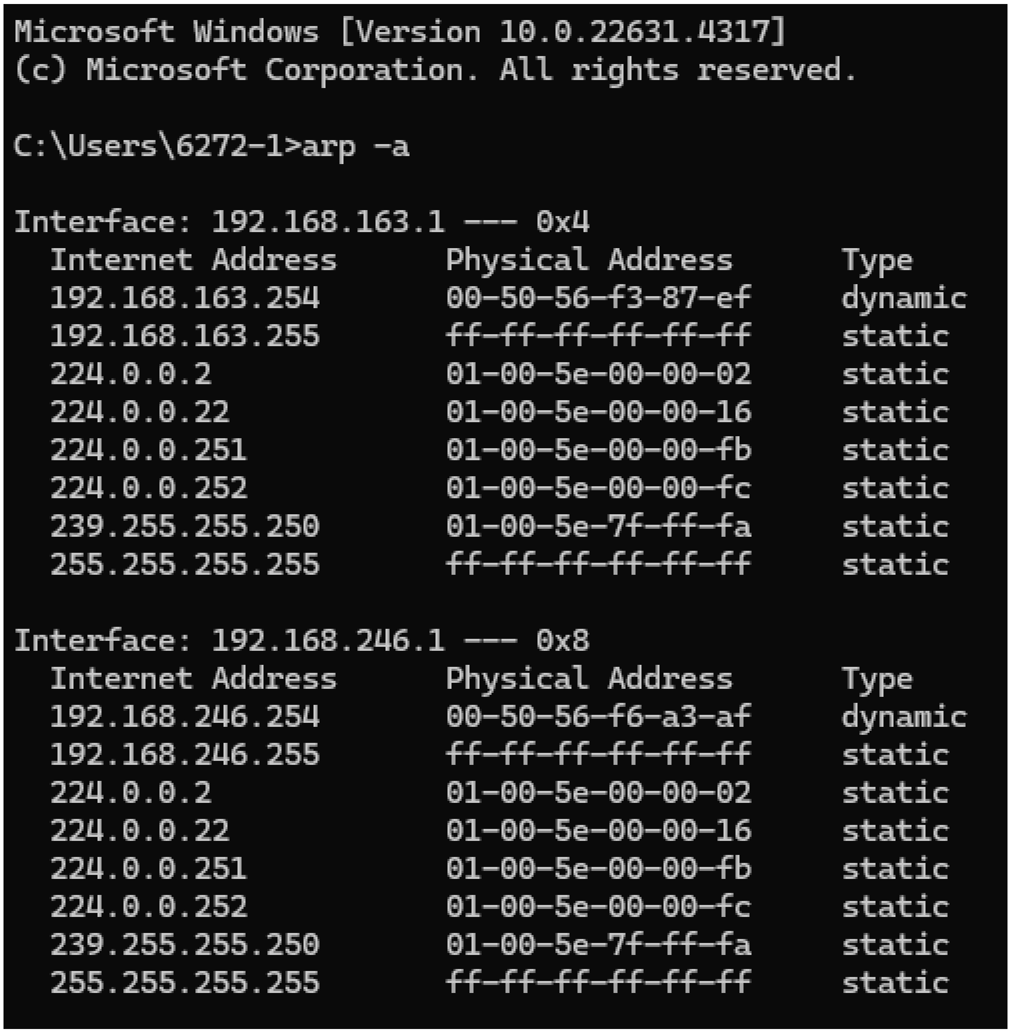
O = 4f

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?**



```
[4 Reassembled TCP Segments (4861 bytes): #249(1412), #250(1412), #252(1412), #254(625)]
    [Frame: 249, payload: 0-1411 (1412 bytes)]
    [Frame: 250, payload: 1412-2823 (1412 bytes)]
    [Frame: 252, payload: 2824-4235 (1412 bytes)]
    [Frame: 254, payload: 4236-4860 (625 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a205468752c203234204
```

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



```
Microsoft Windows [Version 10.0.22631.4317]
(c) Microsoft Corporation. All rights reserved.

C:\Users\6272-1>arp -a

Interface: 192.168.163.1 --- 0x4
  Internet Address      Physical Address      Type
  192.168.163.254       00-50-56-f3-87-ef     dynamic
  192.168.163.255       ff-ff-ff-ff-ff-ff     static
  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
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.246.1 --- 0x8
  Internet Address      Physical Address      Type
  192.168.246.254       00-50-56-f6-a3-af     dynamic
  192.168.246.255       ff-ff-ff-ff-ff-ff     static
  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
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

There are 4 different entries, Interface, Internet Address, Physical Address and Type

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

-Interface contains the network interface.
-Internet Address is IPv4 address
-Physical Address is the MAC address
-Type indicates whether the entry is dynamic or static.

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

13. 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...)?

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

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

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

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

18. ***What is the IP address of the device whose corresponding Ethernet address is being requested in the ARP request message sent by your computer?***

Now find the ARP reply message that was sent in response to the ARP request from your computer.

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

20. ***Finally (!), let's look at the answer to the ARP request message! What is the Ethernet address corresponding to the IP address that was specified in the ARP request message sent by your computer (see question 18)?***

We've looked the ARP request message sent by your computer running Wireshark, and the ARP reply sent in reply. But there are other devices in this network that are also sending ARP requests that you can find in the trace.

21. ***We've looked 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?***