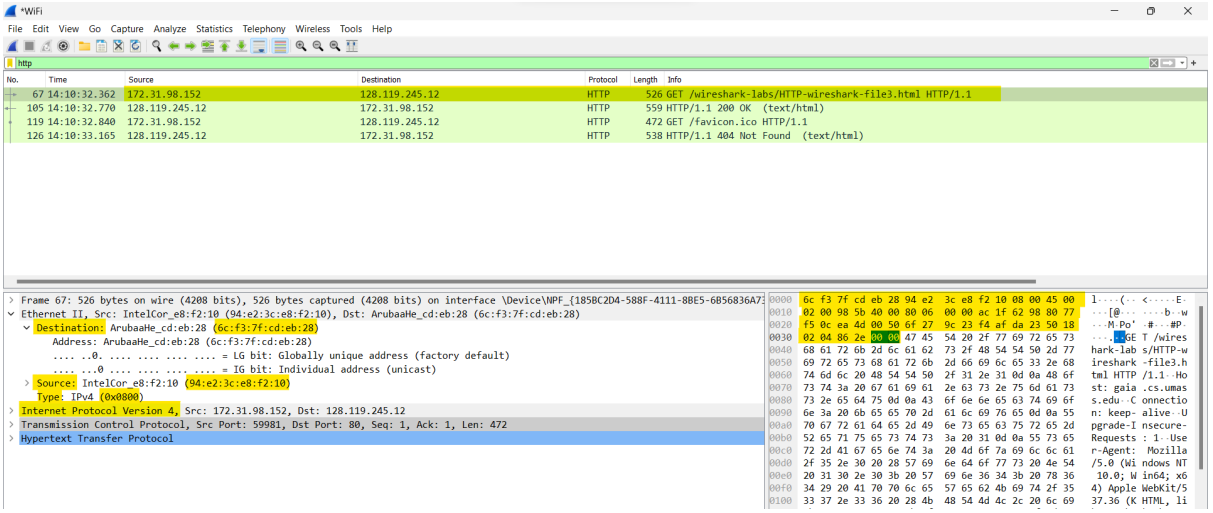
Lab 06_ETHERNET & ARP

I. Capturing and analyzing Ethernet frames

ETHERNET

- **HTTP GET request**



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

   Ethernet address of my computer (Src): 94:e2:3c:e8:f2:10

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? [Note: this is an important question, and one that students sometimes get wrong. Re-read pages 483-484 in the text and make sure you understand the answer here.]**

   Destination address in the Ethernet frame: 6c:f3:7f:cd:eb:28

   This address is not the ethernet address of gaia.cs.umass.edu

   It is the Ethernet address of **the router** to which my computer is connected.

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?**

   Type: IP (0x0800).

   This corresponds to IP protocol.

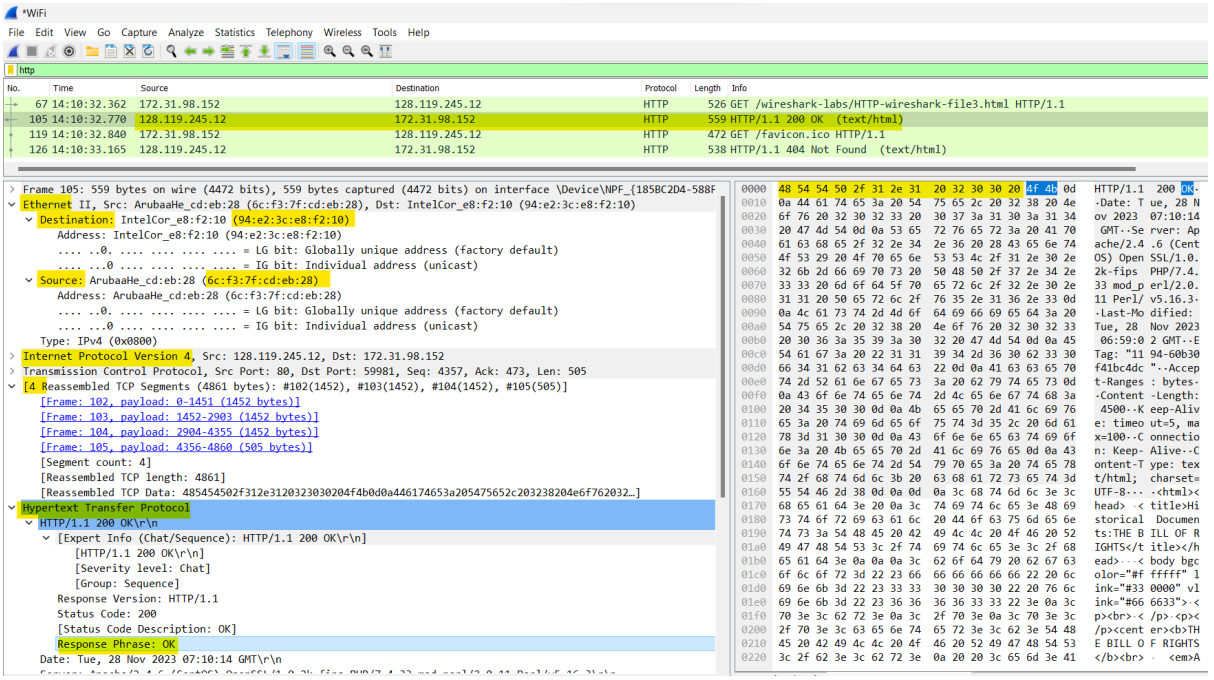
4. **How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame? Do not count any preamble bits in your count, i.e., assume that the Ethernet frame begins with the Ethernet frame's destination address.**

   There are exactly 54 bytes prior to the ASCII "G" for the GET request.

   These bytes represent:

   + The ethernet frame (first 14 bytes containing destination address, source address, and frame type)
   + The IP header (20 bytes)
   + The TCP header (20 byt**es)**

- **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?**

   The Ethernet source address: 6c:f3:7f:cd:eb:28

   It is the Ethernet address of **the router** to which my computer is connected.

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: 94:e2:3c:e8:f2:10

This address is not the ethernet address of gaia.cs.umass.edu

It is the Ethernet address of **the router** to which my computer is connected.

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

   Same as before: 0x0800 corresponding to an IPv4 frame.

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.**

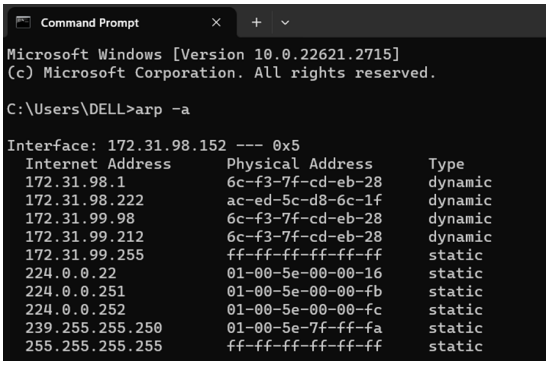
   There are 67 bytes before the "O" (or "O" appears as the 68th byte). These bytes include the ethernet frame, the IP header, the TCP header, and some HTTP preamble text.

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?**

   There are 4 Ethernet frames.

II. The Address Resolution Protocol

- **ARP Caching**



```
Command Prompt
Microsoft Windows [Version 10.0.22621.2715]
(c) Microsoft Corporation. All rights reserved.

C:\Users\DELL>arp -a

Interface: 172.31.98.152 --- 0x5
  Internet Address      Physical Address      Type
  172.31.98.1           6c-f3-7f-cd-eb-28     dynamic
  172.31.98.222         ac-ed-5c-d8-6c-1f     dynamic
  172.31.99.98          6c-f3-7f-cd-eb-28     dynamic
  172.31.99.212         6c-f3-7f-cd-eb-28     dynamic
  172.31.99.255         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
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

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

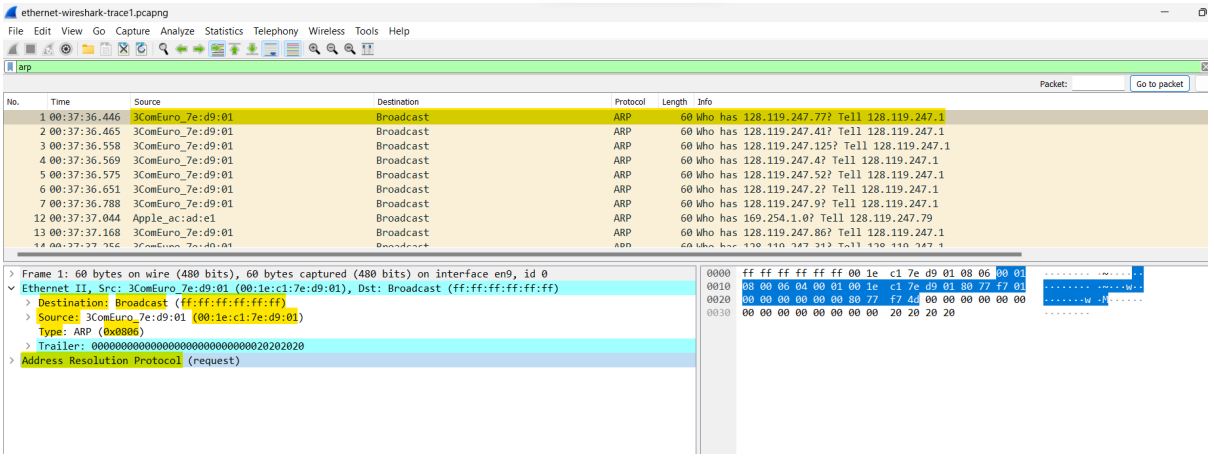
    10 entries.

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

    The Internet Address column contains 3 columns representing:

+ the IP Address at the network layer.
+ the MAC Address to physically communicate with the hardware that is located at that IP address.
+ the type indicates the protocol type whether or not it is changing (dynamic) or static.

- **Observing ARP in action**



12. 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 for the source address is 00:1e:c1:7e:d9:01.

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...)?

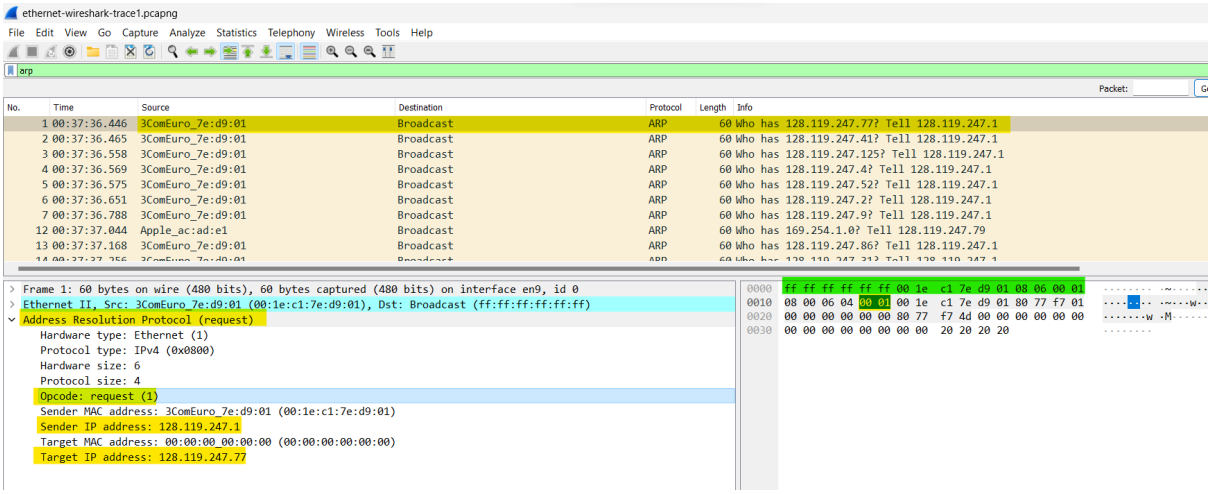
The hexadecimal value for the destination address is ff:ff:ff:ff:ff:ff.

The source address is the Ethernet address of my computer and the destination address is broadcast.

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

The type value is 0x0806 which corresponds to ARP.

- **ARP request message sent by your computer**



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

    The ARP opcode field begins 6 bytes (48 bits) from the beginning of the ARP frame. Since the Ethernet frame (consisting of 6-byte source and 6-byte destination MAC addresses, as well as 2-byte Frame type) is 14 bytes long, the opcode appears 20 bytes from the start of the packet.

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

    The opcode is 01.

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

    Yes.

    The IP address of the sender: 128.119.247.1

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?**

    Target IP address: 128.119.247.9

- **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?**

    The opcode is 02.

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)?**

    Sender MAC address.

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?**

    Because this host computer is not the router that maintains the ARP table (ip address of the computer and arp request do not match) and therefore does not give the sender an answer (the computer will not receive the request). Only the router running the network will respond to the ARP request.

EX-2. What is the default amount of time that an entry remains in your ARP cache before being removed?

→ depending on the operating system