



- 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 bytes)

## • HTTP response message

The image shows a Wireshark packet capture of an HTTP response. The packet list at the top shows a GET request for a file. The packet details pane shows the Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol layers. The packet bytes pane shows the raw data of the packet.

**Packet List:**

| No. | Time         | Source         | Destination    | Protocol | Length | Info   |
|-----|--------------|----------------|----------------|----------|--------|--|
| 67  | 14:10:32.362 | 172.31.98.152  | 128.119.245.12 | HTTP     | 526    | GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1 |
| 105 | 14:10:32.770 | 128.119.245.12 | 172.31.98.152  | HTTP     | 559    | HTTP/1.1 200 OK (text/html)                            |
| 110 | 14:10:32.840 | 172.31.98.152  | 128.119.245.12 | HTTP     | 472    | GET /favicon.ico HTTP/1.1                              |
| 126 | 14:10:33.165 | 128.119.245.12 | 172.31.98.152  | HTTP     | 538    | HTTP/1.1 404 Not Found (text/html)                     |

**Packet Details:**

- Ethernet II**, Src: ArubaaHe\_cd:eb:28 (6c:f3:7f:cd:eb:28), Dst: IntelCor\_e8:f2:10 (94:e2:3c:e8:f2:10)
  - Destination: IntelCor\_e8:f2:10 (94:e2:3c:e8:f2:10)
  - Source: ArubaaHe\_cd:eb:28 (6c:f3:7f:cd:eb:28)
  - Type: IPv4 (0x0800)
- Internet Protocol Version 4**, Src: 128.119.245.12, Dst: 172.31.98.152
- Transmission Control Protocol**, Src Port: 80, Dst Port: 59981, Seq: 4357, Ack: 473, Len: 505
- Hypertext Transfer Protocol**, HTTP/1.1 200 OK
  - Response Version: HTTP/1.1
  - Status Code: 200
  - Status Code Description: OK
  - Response Phrase: OK

**Packet Bytes:**

```

0000  48 54 54 50 2f 31 2e 31 20 32 30 30 20 2f 4b 0d  HTTP/1.1 200 OK
0010  0a 44 61 74 65 3a 20 54 75 65 2c 20 32 38 20 4e  -Date: Tue, 28 Nov 2023 07:10:14
0020  6f 76 20 32 30 32 33 20 30 37 3a 31 30 3a 31 34  ov 2023 07:10:14
0030  20 47 4d 54 0d 0a 53 65 72 76 65 72 3e 20 41 70  GMT-Sever: Ap
0040  61 63 68 65 2f 32 2e 34 2e 36 20 28 43 65 6e 74  ache/2.4.6 (Cent
0050  4f 53 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 30 2e  OS) Open SSL/1.0.
0060  32 6b 2d 66 69 70 73 20 50 48 50 2f 37 2e 34 2e  2k-fips PHP/7.4.
0070  33 33 20 6d 6f 64 5f 70 65 72 6c 2f 32 2e 30 2e  33 mod_p erl/2.0.
0080  31 31 20 50 65 72 6c 2f 76 35 2e 31 36 2e 33 0d  11 Perl/ v5.16.3.
0090  0a 4c 61 73 74 2d 4d 6f 64 69 66 69 65 64 3a 20  -Last-Modified:
00a0  54 75 65 2c 20 32 38 20 4e 6f 76 20 32 30 32 33  Tue, 28 Nov 2023
00b0  20 30 36 3a 35 39 3a 30 32 20 47 4d 54 0d 0a 45  06:59:02 GMT-E
00c0  54 61 67 3a 20 22 31 31 39 34 2d 36 30 62 33 30  Tag: "11 94-60b30
00d0  66 34 31 62 63 34 64 63 22 0d 0a 41 63 63 65 70  f41bc4dc "...Accep
00e0  74 2d 52 61 6e 67 65 73 3a 20 62 79 74 65 73 0d  t-Ranges : bytes-
00f0  0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a  -Content -Length:
0100  20 34 35 30 30 0d 0a 4b 65 65 70 2d 41 6c 69 67  4500-K eep-Alive
0110  65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c 20 6d 61  e: timeo ut=5, na
0120  78 3d 31 30 30 0d 0a 43 6f 6e 6e 65 63 74 69 6f  x=100-C onnectio
0130  6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 43  n: Keep- Alive-C
0140  6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78  ontent-T ype: tex
0150  74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 0d  t/html; charset=
0160  55 54 46 2d 38 0d 0a 0d 0a 3c 68 74 6d 6c 3e 3c  UTF-8... <html>
0170  68 65 61 64 3e 20 0a 3c 74 69 74 6c 65 3e 48 69  head> < title>Hi
0180  73 74 6f 72 69 63 61 6c 20 44 6f 63 75 6d 65 6e  storical Documen
0190  74 73 3a 54 48 45 20 42 49 4c 20 4f 46 46 20 52  ts:THE B ILL OF R
01a0  49 47 48 54 53 3c 2f 74 69 74 6c 65 3e 3c 2f 68  IGHTS</t itle></h
01b0  65 61 64 3e 0a 0a 3c 62 6f 64 79 20 62 67 63  ead>...< body bgc
01c0  6f 6c 6f 72 3d 22 33 66 66 66 66 66 66 22 0c 6c  olor="#f fffff" l
01d0  69 6e 6b 3d 22 33 33 30 30 30 22 20 76 6c 3c  ink="#33 0000" v1
01e0  69 6e 6b 3d 22 33 36 36 36 33 33 22 3e 0a 3c  ink="#66 6633"><
01f0  70 3e 3c 62 72 3e 0a 3c 2f 70 3e 0a 3c 70 3e 3c  p>ebr>...</p><p>
0200  2f 70 3e 3c 63 65 6e 74 65 72 3e 3c 62 3e 54 48  /p><cent er>b>TH
0210  45 20 42 49 4c 20 4f 46 20 52 49 47 48 54 53  E BILL O F RIGHTS
0220  3c 2f 62 3e 3c 62 72 3e 0a 20 20 3c 65 6d 3e 41  <b>ebr>... <em>A

```

- 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.

- 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.**

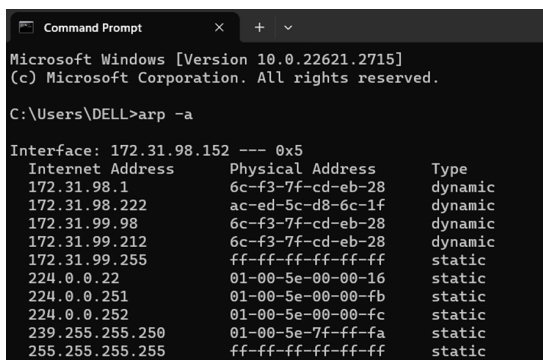
There are 67 bytes before the “O” (or “O” appears as the 68th byte). These bytes include the ethernet frame, the IP header, the TCP header, and some HTTP preamble text.

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**



```
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?**

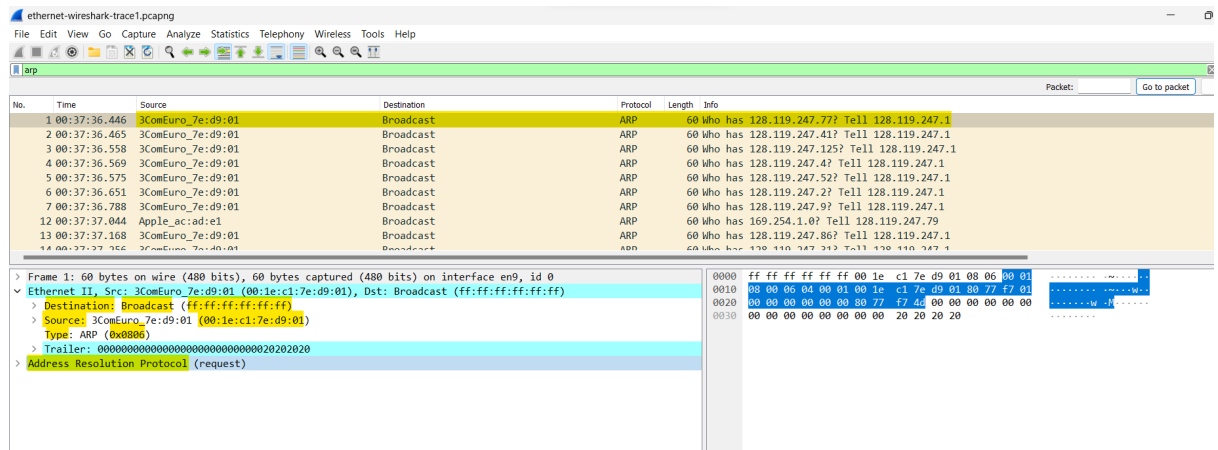
10 entries.

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**

| No. | Time         | Source            | Destination | Protocol | Length | Info  |
|-----|--------------|-------------------|-------------|----------|--------|---|
| 1   | 00:37:36.446 | 3ComEuro_7e:d9:01 | Broadcast   | ARP      | 60     | Who has 128.119.247.77? Tell 128.119.247.1  |
| 2   | 00:37:36.465 | 3ComEuro_7e:d9:01 | Broadcast   | ARP      | 60     | Who has 128.119.247.41? Tell 128.119.247.1  |
| 3   | 00:37:36.558 | 3ComEuro_7e:d9:01 | Broadcast   | ARP      | 60     | Who has 128.119.247.125? Tell 128.119.247.1 |
| 4   | 00:37:36.569 | 3ComEuro_7e:d9:01 | Broadcast   | ARP      | 60     | Who has 128.119.247.4? Tell 128.119.247.1   |
| 5   | 00:37:36.575 | 3ComEuro_7e:d9:01 | Broadcast   | ARP      | 60     | Who has 128.119.247.52? Tell 128.119.247.1  |
| 6   | 00:37:36.651 | 3ComEuro_7e:d9:01 | Broadcast   | ARP      | 60     | Who has 128.119.247.2? Tell 128.119.247.1   |
| 7   | 00:37:36.788 | 3ComEuro_7e:d9:01 | Broadcast   | ARP      | 60     | Who has 128.119.247.9? Tell 128.119.247.1   |
| 12  | 00:37:37.044 | Apple_ac:ade1     | Broadcast   | ARP      | 60     | Who has 169.254.1.0? Tell 128.119.247.9     |
| 13  | 00:37:37.168 | 3ComEuro_7e:d9:01 | Broadcast   | ARP      | 60     | Who has 128.119.247.86? Tell 128.119.247.1  |
| 14  | 00:37:37.168 | 3ComEuro_7e:d9:01 | Broadcast   | ARP      | 60     | Who has 128.119.247.312? Tell 128.119.247.1 |

| Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface en9, id 0   |  | 0000 | ff ff ff ff ff ff 00 01 c1 7e d9 01 00 06 00 00 |
|---|--|------|---|
| Ethernet II, Src: 3ComEuro_7e:d9:01 (00:1e:c1:7e:d9:01), Dst: Broadcast (ff:ff:ff:ff:ff:ff) |  | 0010 | 08 00 06 04 00 01 00 1e c1 7e d9 01 80 7f f7 01 |
| Address Resolution Protocol (request)   |  | 0020 | 00 00 00 00 00 00 80 7f f7 4d 00 00 00 00 00 00 |
| Hardware type: Ethernet (1)   |  | 0030 | 00 00 00 00 00 00 00 00 20 20 20 20             |
| Protocol type: IPv4 (0x0800)  |  |      |   |
| Hardware size: 6  |  |      |   |
| Protocol size: 4  |  |      |   |
| Opcode: request (1)   |  |      |   |
| Sender MAC address: 3ComEuro_7e:d9:01 (00:1e:c1:7e:d9:01)                                   |  |      |   |
| Sender IP address: 128.119.247.1  |  |      |   |
| Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)                                   |  |      |   |
| Target IP address: 128.119.247.77   |  |      |   |

# 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