ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC BÁCH KHOA
KHOA KHOA HỌC VÀ KỸ THUẬT MÁY TÍNH

MẠNG MÁY TÍNH THỰC HÀNH - CO3094

Báo cáo:

Lab 6

Giảng viên hướng dẫn: Vũ Thành Tài

Sinh viên: Lê Đức Cường

MSSV: 2210423

Thành phố Hồ Chí Minh, tháng 4 năm 2025

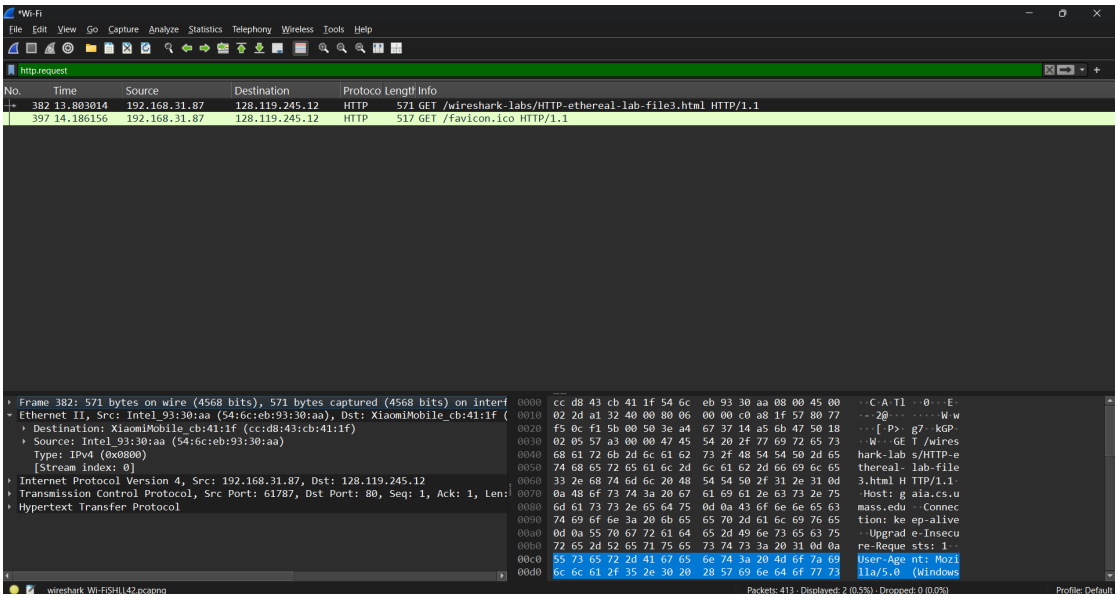
Mục lục

1 Question 1

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

ANS:

The 48-bit Ethernet address (MAC address) of my computer is: 54:6c:eb:93:30:aa



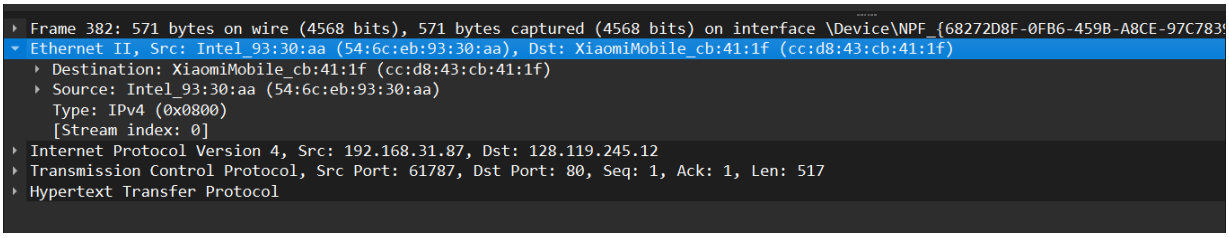
2 Question 2

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 468-469 in the text and make sure you understand the answer here.]

ANS:

The 48-bit destination address in the Ethernet frame is: cc:d8:43:cb:41:1f.

This is not the Ethernet address of gaia.cs.umass.edu. It is the MAC address of the default gateway/router in the local network. Since Ethernet is a link-layer protocol, it only works within the local network. To reach gaia.cs.umass.edu (which is outside the local network), the frame is first sent to the router, which then forwards the IP packet over the Internet.



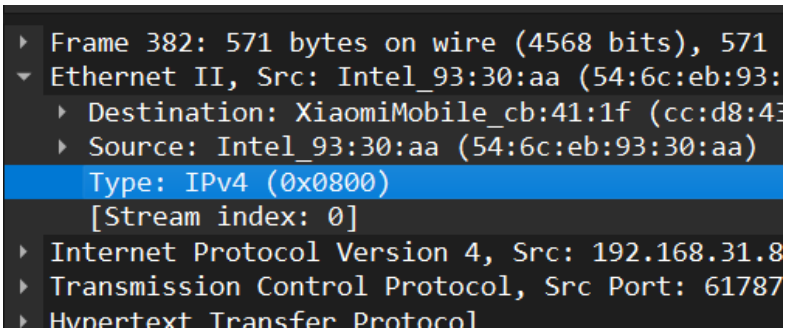
3 Question 3

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

ANS:

The two-byte Frame Type field has the hexadecimal value: 0x0800

This corresponds to the Internet Protocol version 4 (IPv4) at the upper layer.



4 Question 4

How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame?

ANS:

The ASCII character "G" in "GET" appears at byte 54 from the start of the Ethernet frame. This is determined by examining the raw bytes in the Packet Bytes pane of Wireshark, where the value 47 (ASCII for "G") is located at the 55th position, starting from byte 0.

```
cc d8 43 cb 41 1f 54 6c  eb 93 30 aa 08 00 45 00   ··C·A·Tl ··0···E·
02 2d a1 32 40 00 80 06  00 00 c0 a8 1f 57 80 77   ·-·2@··· ·····W·w
f5 0c f1 5b 00 50 3e a4  67 37 14 a5 6b 47 50 18   ···[·P>· g7··kGP·
02 05 57 a3 00 00 47 45  54 20 2f 77 69 72 65 73   ··W···GE T /wires
68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 65   hark-lab s/HTTP-e
74 68 65 72 65 61 6c 2d  6c 61 62 2d 66 69 6c 65   thereal- lab-file
33 2e 68 74 6d 6c 20 48  54 54 50 2f 31 2e 31 0d   3.html H TTP/1.1·
0a 48 6f 73 74 3a 20 67  61 69 61 2e 63 73 2e 75   ·Host: g aia.cs.u
6d 61 73 73 2e 65 64 75  0d 0a 43 6f 6e 6e 65 63   mass.edu ··Connec
74 69 6f 6e 3a 20 6b 65  65 70 2d 61 6c 69 76 65   tion: ke ep-alive
0d 0a 55 70 67 72 61 64  65 2d 49 6e 73 65 63 75   ··Upgrad e-Insecu
72 65 2d 52 65 71 75 65  73 74 73 3a 20 31 0d 0a   re-Reque sts: 1··
55 73 65 72 2d 41 67 65  6e 74 3a 20 4d 6f 7a 69   User-Age nt: Mozi
6c 6c 61 2f 35 2e 30 20  28 57 69 6e 64 6f 77 73   lla/5.0  (Windows
20 4e 54 20 31 30 2e 30  3b 20 57 69 6e 36 34 3b   NT 10.0 ; Win64;
```

5 Question 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?

ANS:

The Ethernet source address is the same as the MAC address of my computer, which is 54:6c:eb:93:30:aa. This means that the HTTP GET request was sent directly from my computer without passing through any intermediate device like a router or proxy. Therefore, the device with this Ethernet address is my own computer

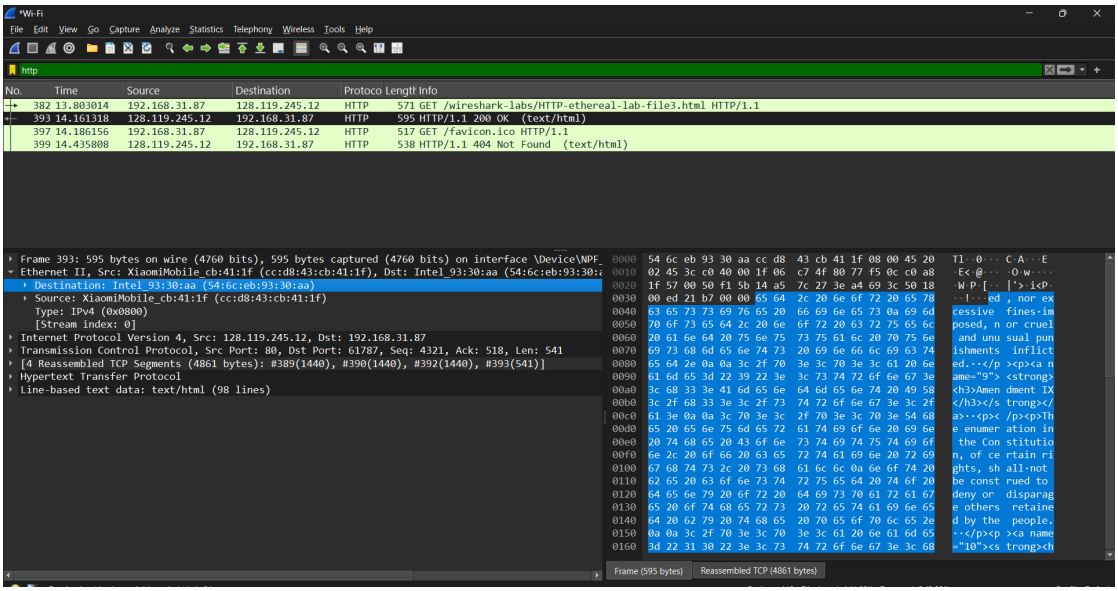
```
▸ Frame 382: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface \Device\NPF_
▾ Ethernet II, Src: Intel_93:30:aa (54:6c:eb:93:30:aa), Dst: XiaomiMobile_cb:41:1f (cc:d8:43:cb:41:1
  ▸ Destination: XiaomiMobile_cb:41:1f (cc:d8:43:cb:41:1f)
  ▸ Source: Intel_93:30:aa (54:6c:eb:93:30:aa)
    Type: IPv4 (0x0800)
    [Stream index: 0]
▸ Internet Protocol Version 4, Src: 192.168.31.87, Dst: 128.119.245.12
▸ Transmission Control Protocol, Src Port: 61787, Dst Port: 80, Seq: 1, Ack: 1, Len: 517
▸ Hypertext Transfer Protocol
```

6 Question 6

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

ANS:

The destination address in the Ethernet frame is 54:6c:eb:93:30:aa. Yes, this is the Ethernet (MAC) address of my computer. The HTTP response is being sent back from the router (or gateway) to my computer, so the destination MAC must match my device's MAC address. Ethernet only works within the local network, so the frame is addressed directly to the receiving machine's MAC address.



7 Question 7

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

ANS:

The hexadecimal value of the two-byte Frame Type field is 0x0800. This indicates that the Ethernet frame carries an IPv4 packet as its payload.

8 Question 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?

ANS:

The ASCII character "O" in "OK" appears at byte 66 from the start of the Ethernet frame. This position is determined by adding the sizes of the Ethernet (14 bytes), IP (20 bytes), and TCP headers (usually 20 bytes), and locating the start of the HTTP payload.

```
0010  02 45 3c c0 40 00 1f 06  c7 4f 80 77 f5 0c c0 a8  ·E<·@··· ·O·w····
0020  1f 57 00 50 f1 5b 14 a5  7c 27 3e a4 69 3c 50 18  ·W·P·[·· |'>·i<P·
0030  00 ed 21 b7 00 00 65 64  2c 20 6e 6f 72 20 65 78  ··!···ed , nor ex
0040  63 65 73 73 69 76 65 20  66 69 6e 65 73 0a 69 6d  cessive  fines·im
0050  70 6f 73 65 64 2c 20 6e  6f 72 20 63 72 75 65 6c  posed, n or cruel
0060  20 61 6e 64 20 75 6e 75  73 75 61 6c 20 70 75 6e   and unu sual pun
0070  69 73 68 6d 65 6e 74 73  20 69 6e 66 6c 69 63 74  ishments  inflict
0080  65 64 2e 0a 0a 3c 2f 70  3e 3c 70 3e 3c 61 20 6e  ed.··</p ><p><a n
0090  61 6d 65 3d 22 39 22 3e  3c 73 74 72 6f 6e 67 3e  ame="9"> <strong>
00a0  3c 68 33 3e 41 6d 65 6e  64 6d 65 6e 74 20 49 58  <h3>Amen dment IX
00b0  3c 2f 68 33 3e 3c 2f 73  74 72 6f 6e 67 3e 3c 2f  </h3></s trong></
00c0  61 3e 0a 0a 3c 70 3e 3c  2f 70 3e 3c 70 3e 54 68  a>··<p>< /p><p>Th
00d0  65 20 65 6e 75 6d 65 72  61 74 69 6f 6e 20 69 6e  e enumer ation in
00e0  20 74 68 65 20 43 6f 6e  73 74 69 74 75 74 69 6f   the Con stitutio
00f0  6e 2c 20 6f 66 20 63 65  72 74 61 69 6e 20 72 69  n, of ce rtain ri
0100  67 68 74 73 2c 20 73 68  61 6c 6c 0a 6e 6f 74 20  ghts, sh all·not
0110  62 65 20 63 6f 6e 73 74  72 75 65 64 20 74 6f 20  be const rued to
0120  64 65 6e 79 20 6f 72 20  64 69 73 70 61 72 61 67  deny or  disparag
0130  65 20 6f 74 68 65 72 73  20 72 65 74 61 69 6e 65  e others  retaine
0140  64 20 62 79 20 74 68 65  20 70 65 6f 70 6c 65 2e  d by the  people.
0150  0a 0a 3c 2f 70 3e 3c 70  3e 3c 61 20 6e 61 6d 65  ··</p><p ><a name
0160  3d 22 31 30 22 3e 3c 73  74 72 6f 6e 67 3e 3c 68  ="10"><s trong><h
0170  33 3e 41 6d 65 6e 64 6d  65 6e 74 20 58 3c 2f 68  3>Amendm ent X</h
```

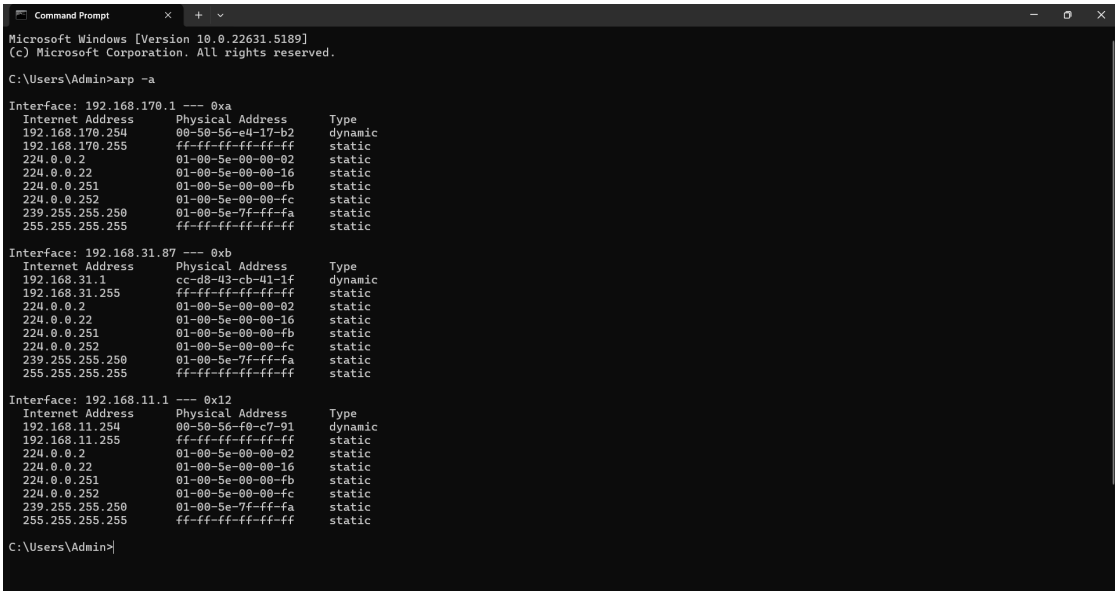
9 Question 9

Write down the contents of your computer's ARP cache. What is the meaning of each column value?

ANS: By executing the arp -a command in the Command Prompt, I obtained the ARP cache table of my computer. The result includes three columns:

- Internet Address: This is the IP address of a host or device that my computer has recently communicated with on the local network.
- Physical Address: This is the MAC (Media Access Control) address associated with the IP address.
- Type: This indicates whether the ARP entry was learned dynamically (automatically by the system) or set statically.

As shown in the screenshot below, the ARP cache contains several entries.



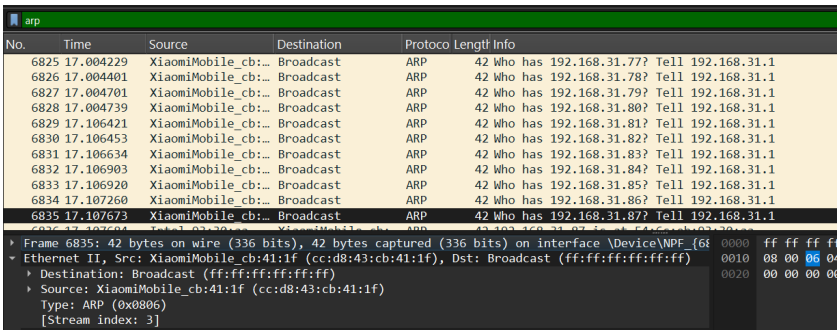
```
Command Prompt
Microsoft Windows [Version 10.0.22631.5189]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>arp -a

Interface: 192.168.170.1 --- 0xa
  Internet Address      Physical Address      Type
  192.168.170.254       00-50-56-e4-17-b2     dynamic
  192.168.170.255       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: 192.168.31.87 --- 0xb
  Internet Address      Physical Address      Type
  192.168.31.1          cc-d8-43-cb-41-1f     dynamic
  192.168.31.255        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: 192.168.11.1 --- 0x12
  Internet Address      Physical Address      Type
  192.168.11.254        00-50-56-f0-c7-91     dynamic
  192.168.11.255        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

C:\Users\Admin>
```

10 Question 10

What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?

In the ARP Request frame, the Ethernet source address is: cc:d8:43:cb:41:1f. This is the MAC address of my computer, which is sending the ARP request.

The Ethernet destination address is: ff:ff:ff:ff:ff:ff This is the broadcast address, because ARP requests are sent to all devices on the local network to find out who has the requested IP address.



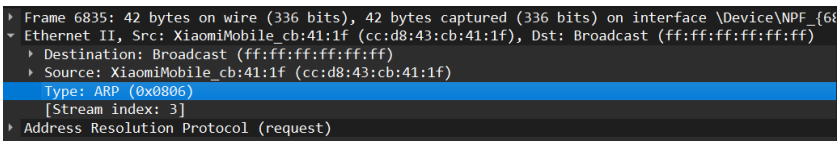
11 Question 11

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

ANS:

The hexadecimal value of the two-byte Ethernet Frame Type field is 0x0806. This value corresponds to the Address Resolution Protocol (ARP), which operates at the network layer.

In this case, the Ethernet frame is carrying an ARP request or reply message.



12 Question 12

Download the ARP specification from ftp://ftp.rfc-editor.org/in-notes/std/std37.txt. A readable, detailed discussion of ARP is also at http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html.

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

b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?

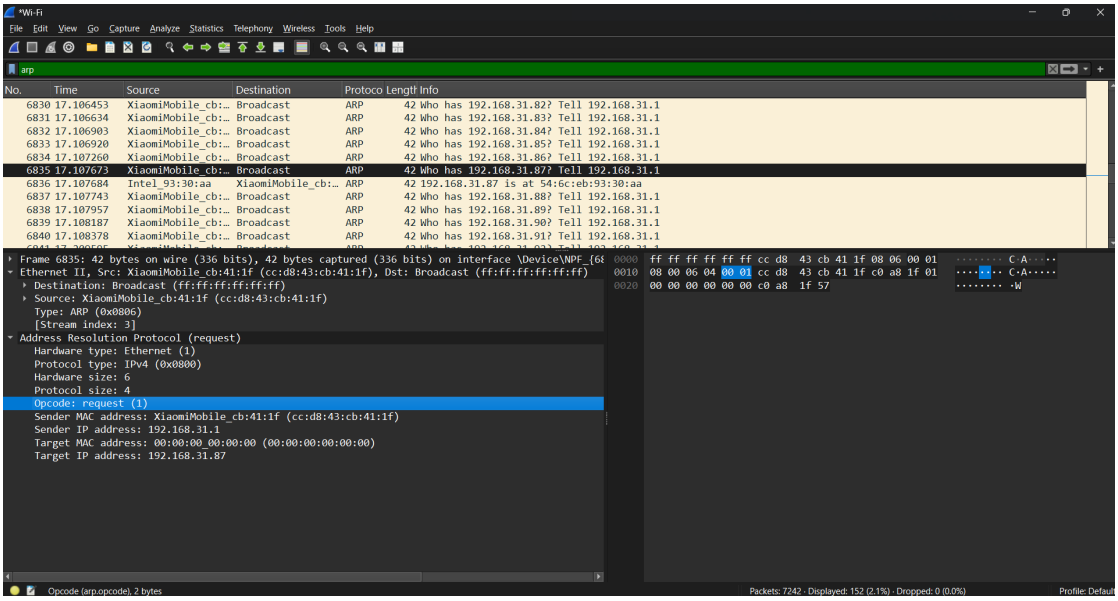
c) Does the ARP message contain the IP address of the sender?

d) Where in the ARP request does the "question" appear – the Ethernet address of the machine whose corresponding IP address is being queried?

ANS:

a)

The ARP Opcode field begins at byte 20 from the start of the Ethernet frame. This includes 14 bytes of Ethernet header plus the first 6 bytes of the ARP header.



b)

The value of the Opcode field is 0x0001, which indicates an ARP Request.

c)

Yes, the ARP message contains the IP address of the sender. It appears in the Sender IP address field, which tells other devices who is asking.

```
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: XiaomiMobile_cb:41:1f (cc:d8:43:cb:41:1f)
Sender IP address: 192.168.31.1
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.31.87
```

d)

In the ARP request message, the "question" is expressed by setting the Target MAC address to 00:00:00:00:00:00, which indicates that the sender does not yet know the MAC address of the device it is trying to reach.

The Target IP address field is set to 192.168.31.87, meaning that the sender is querying:

"Who has IP address 192.168.31.87? Tell me your MAC address."

This combination of unknown MAC (all zeros) and known IP in the ARP request allows devices on the local network to check if the target IP matches theirs and, if so, respond with their MAC address.

13 Question 13

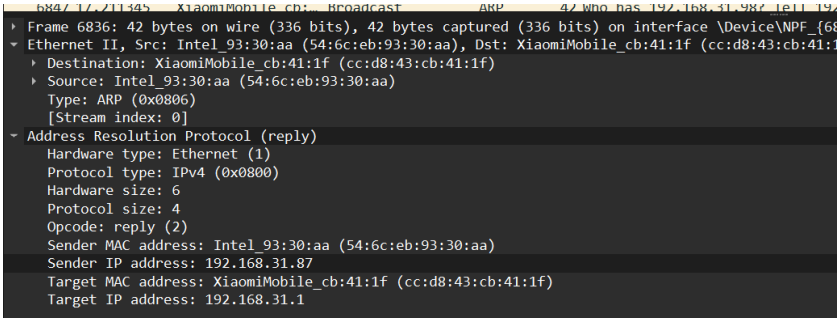
Now find the ARP reply that was sent in response to the ARP request.

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

b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

c) Where in the ARP message does the "answer" to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?

ANS:



a)

The opcode field is part of the ARP header. The Ethernet header is 14 bytes long, and the opcode field is the 7th and 8th bytes of the ARP header (which starts right after Ethernet). So, the opcode field begins at byte 20 from the start of the Ethernet frame.

b)

In your screenshot, it's labeled as: Opcode: reply (2). The value is 0x0002, which corresponds to an ARP Reply.

c)

The answer is in the fields:

Sender MAC address: 54:6c:eb:93:30:aa

Sender IP address: 192.168.31.87

14 Question 14

What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?

ANS:

In the ARP reply, the source MAC address is 54:6c:eb:93:30:aa and the destination MAC address is cc:d8:43:cb:41:1f. This indicates that the device with MAC 54:6c:eb:93:30:aa is replying to the device with MAC cc:d8:43:cb:41:1f, providing its hardware address in response to an earlier ARP request.

15 Question 15

Open the ethernet-ethereal-trace-1 trace file in http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip. The first and second ARP packets in this trace correspond to an ARP request sent by the computer running Wireshark, and the ARP reply sent to the computer running Wireshark by the computer with the ARP-requested Ethernet address. But there is yet another computer on this network, as indicated by packet 6 – another ARP request. Why is there no ARP reply (sent in response to the ARP request in packet 6) in the packet trace?

ANS:

The ARP request is sent as a broadcast to all devices on the local network because the sender does not know the receiver's MAC address.

The ARP reply is sent as a unicast directly to the sender's MAC address, since it was included in the original request.

16 Extra Credit - Ex1

The arp command: arp -s InetAddr EtherAddr allows you to manually add an entry to the ARP cache that resolves the IP address InetAddr to the physical address EtherAddr. What would happen if, when you manually added an entry, you entered the correct IP address, but the wrong Ethernet address for that remote interface?

ANS:

If a manual ARP entry is added with the correct IP address but an incorrect Ethernet (MAC) address, several problems may occur:

Misrouted packets: Data will be sent to the wrong device on the network.

No response: The intended recipient will never receive the packets, leading to failed communication.

Security risks: Sensitive data could be unintentionally sent to an unauthorized or unintended device.

Troubleshooting difficulties: Network issues may arise that are hard to trace, since the ARP entry appears valid but points to the wrong physical destination.

17 Extra Credit - Ex2

What is the default amount of time that an entry remains in your ARP cache before being removed. You can determine this empirically (by monitoring the cache contents) or by looking this up in your operation system documentation. Indicate how/where you determined this value.

ANS:

In Windows, the default ARP cache timeout is typically 2 minutes (120 seconds) for unused entries. However, if the entry is being actively used, it may remain in the cache for up to 10 minutes. In Linux, the default timeout is usually around 60 seconds. This information was determined by monitoring the ARP cache over time using the arp -a command in Windows and reviewing documentation for Linux networking behavior.s