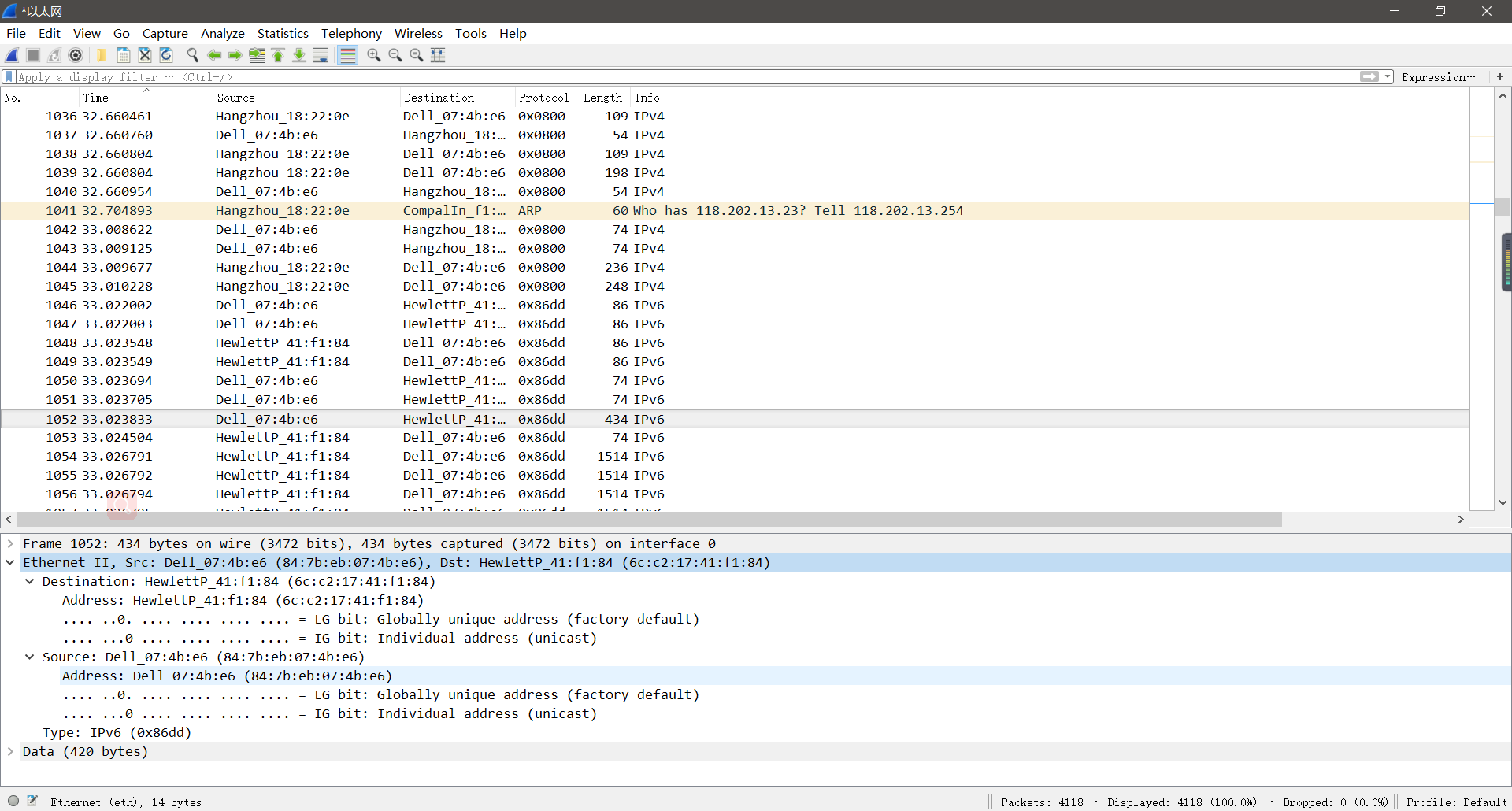
Lab03-Ethernet and ARP Lab

*1.0 Capturing and analyzing Ethernet frames*

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



A: I know my computer’s name is DELL, so from the picture, I get the 48-bit Ethernet address of my computer is **84:7b:eb:07:4b:e6**.

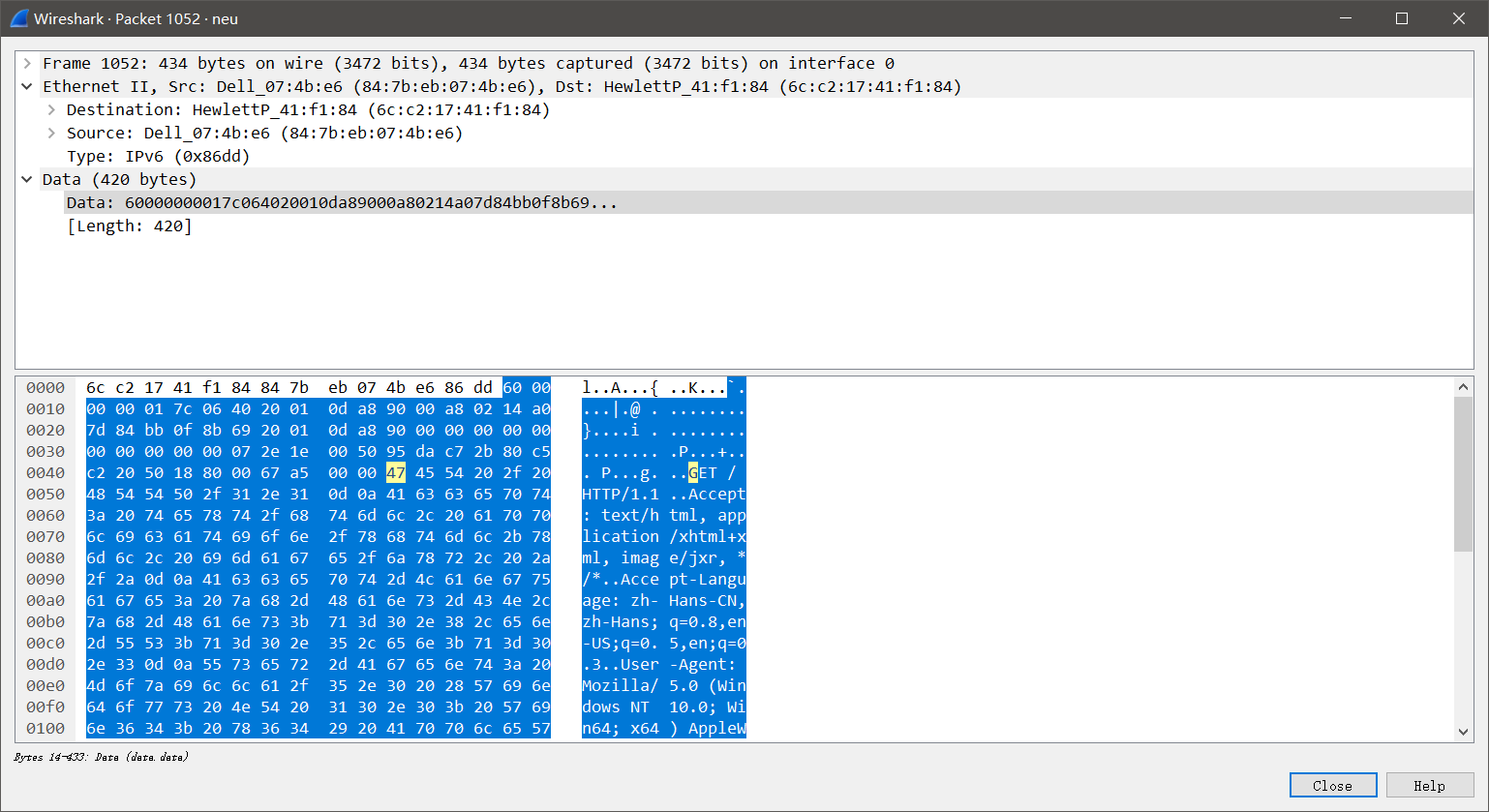
2. *Q: What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of* [*http://www.neu.edu.cn*](http://www.neu.edu.cn)*? If not, what device has this as its Ethernet address?*

A: From the wireshark, we know the address is **70:f9:6d:18:22:0e**. And it is **not** the Ethernet addr of neu website. It is the **Ethernet address of my router** (because we are using neu campus-net. So, even if it has the similar name to NEU website, it isn’t NEU website.)

3. *Q: Give the hexadecimal value for the two-byte Frame type field. What type of frame does this specify?*

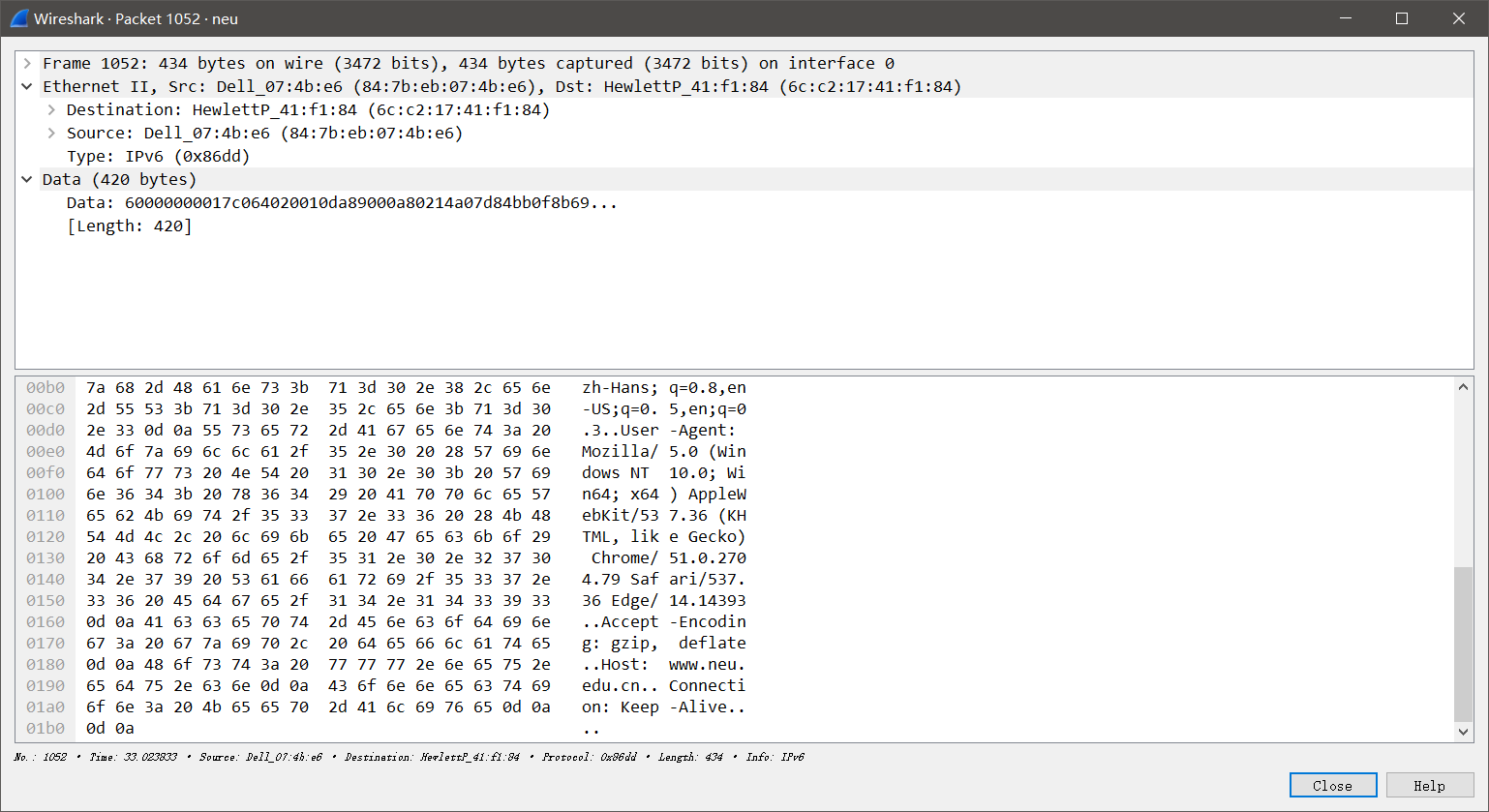
A: The hexadecimal value for the Frame type field is **0x86dd**. The type is **IPv6**.

4. *Q: How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame?*



A: The ASCII “G” appears **74** bytes from the start of the Ethernet frame. There are 14 bytes Ethernet frame, and then 40 bytes of IP header followed by 20 bytes of TCP header before the HTTP data is encountered.

5. *What is the hexadecimal value of the CRC field in this Ethernet frame?*



The hex value of the CRC field is **0d 0a 0d 0a**.

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

6. *What is the value of the Ethernet source address? Is this the address of* [*www.uiowa.edu*](http://www.uiowa.edu)*? If not, what device has this as its Ethernet address?*

The Ethernet source address is **2001:da8:9000::7**. And it is also **not** the address of uiowa net. It’s the address of **uiowa router**.

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

The destination address in the Ethernet frame is **2001:da8:9000:a802:14a0:7d84:bb0f:8b69**. And it is **not** the Ethernet address of my computer.

8. Give the hexadecimal value for the two-byte Frame type field. What type of frame does this specify?

**0x86dd.** The type is **IPv6**.

9. 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?

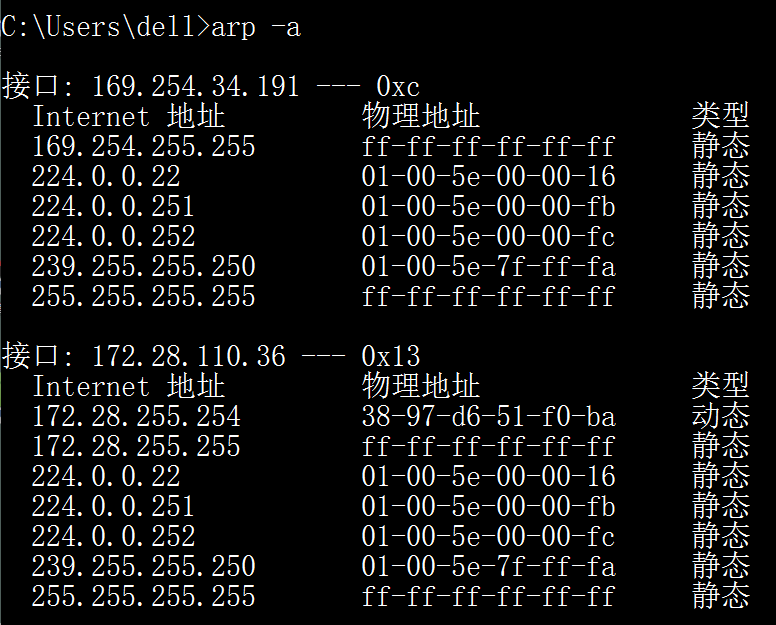
The ASCII “G” appears **74** bytes from the start of the Ethernet frame. Again, There are 14 bytes Ethernet frame, and then 40 bytes of IP header followed by 20 bytes of TCP header before the HTTP data is encountered.

10. What is the hexadecimal value of the CRC field in this Ethernet frame?

*2.0 The Address Resolution Protocol*

*2.1 ARP Caching*

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



The first column is the Internet Address Column, containing the IP address. The second column is the Physical Address Column, containing the MAC address. The last column is Type Column, indicating the protocol type.

*2.2 Observing ARP in action*

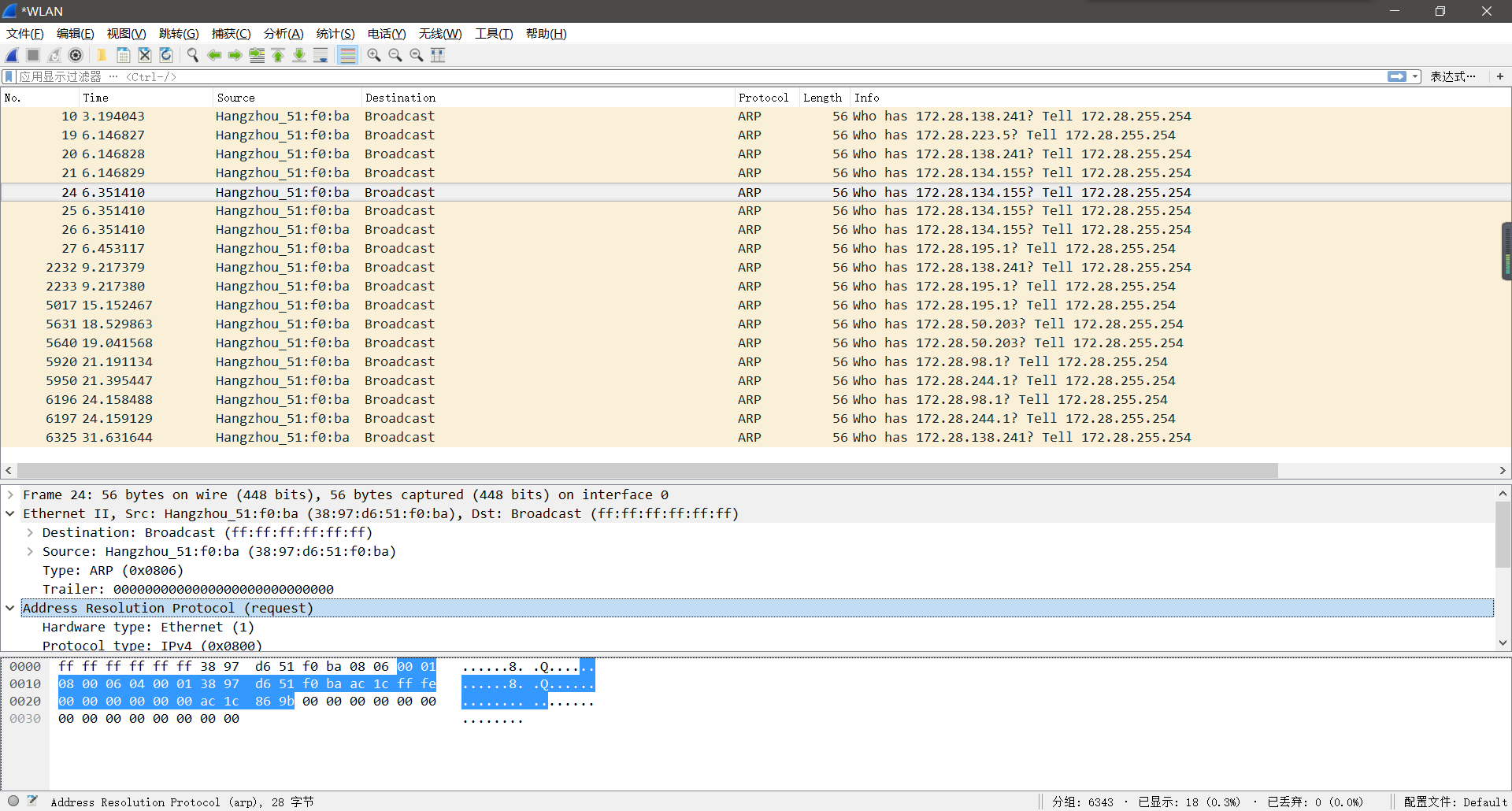
1. *What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?*

The hex value for the source address is **38:97:d6:51:f0:ba** . The hex value for the destination address is **ff:ff:ff:ff:ff:ff**, the broadcast address.

2. *Give the hexadecimal value for the two-byte Ethernet Frame type field. What type of frame does this specify?*

**0x0800**

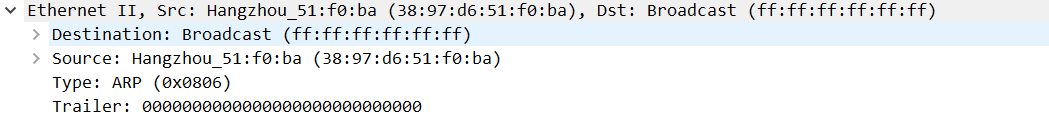
3. Request a webpage from <http://www.neu.edu.cn>



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

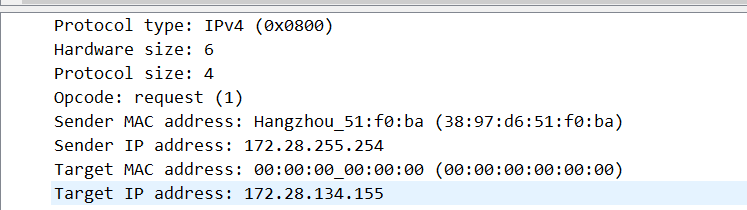
**14** bytes.

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?*



**0x0806**

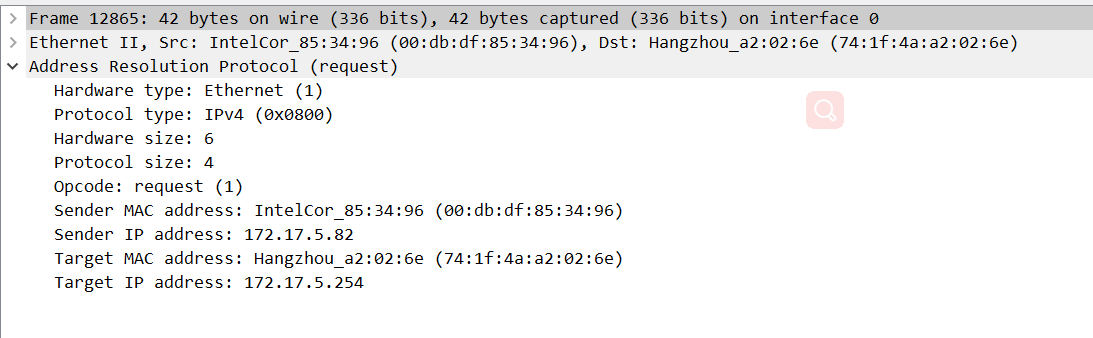
c. Does the ARP message contain the IP address of the sender?



**Yes**.

d. *Where in the ARP request does the “question” appear –i.e. the IP address of the machine whose corresponding Ethernet address is being sought?*





The answer to the earlier ARP request appears in the “**Sender MAC address**” field, which contains the Ethernet address **00:db:df:85:34:96** of the sender with IP address **172.17.5.82**.

4. *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?*

**14** bytes.

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?*

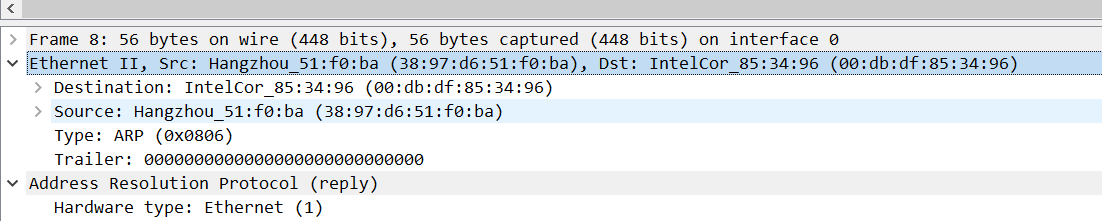
**0x0800**

c. *Where in the ARP message does the “answer” to the earlier ARP request appear – i.e. the Ethernet address of the machine with the IP address specified in the ARP request?*



The answer to the earlier ARP request appears in the “**Sender MAC address**” field, which contains the Ethernet address **74:1f:4a:a2:02:6e** for the sender with IP address **172.17.5.82**.

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



The source address is **38:97:d6:51:f0:ba**, and the destination address is **00:db:df:85:34:96**.

6. *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). Indicate how you determined this value.*

The default time to keep the ARP table entry is 20 mins. For every 20mins the ARP table will be refreshed. Because, The neighboring device can be out of the network so the ARP table should be updated according to the network states. When the table gets refreshed the content will get erased.