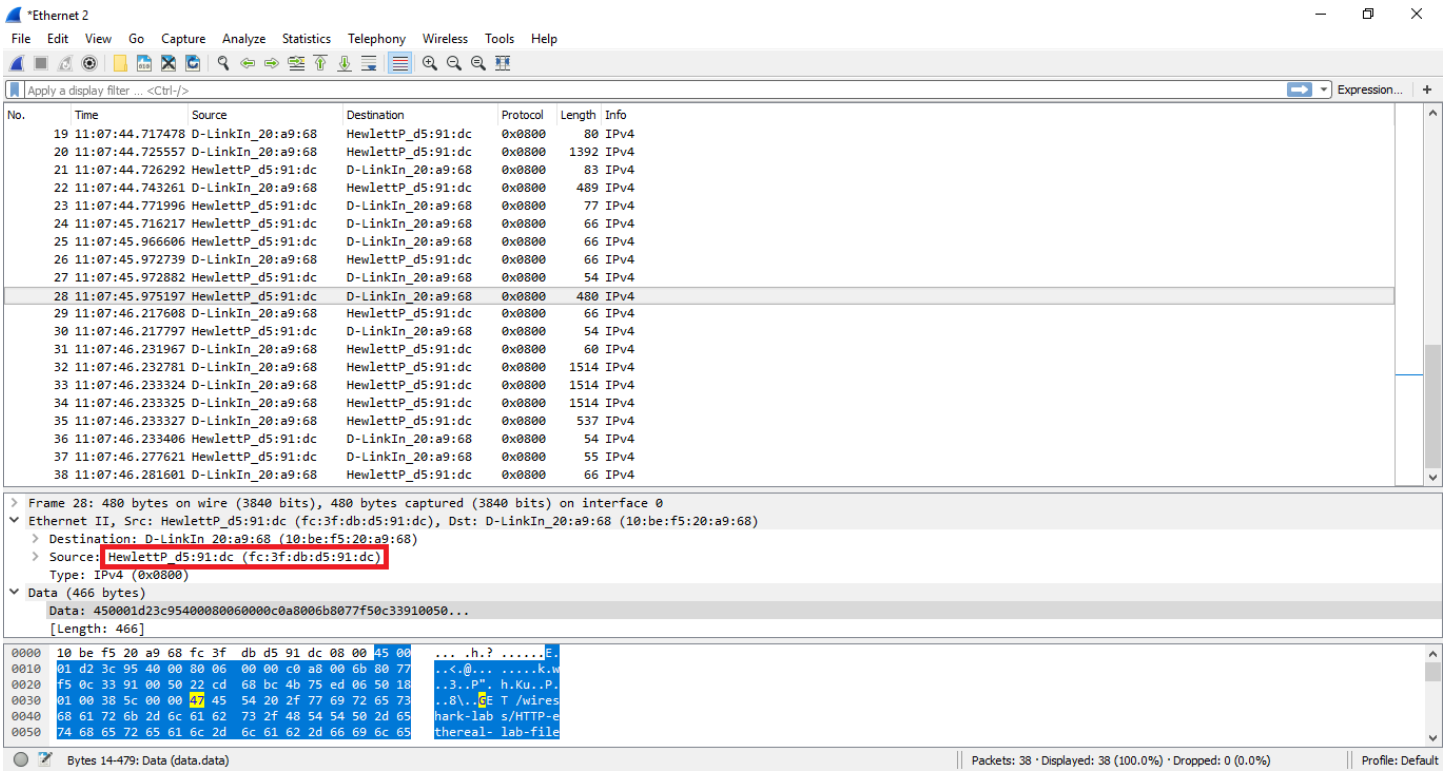
Jessica Spokoyny
Dec 3, 2016
CS 372 – Lab 5

Lab 5

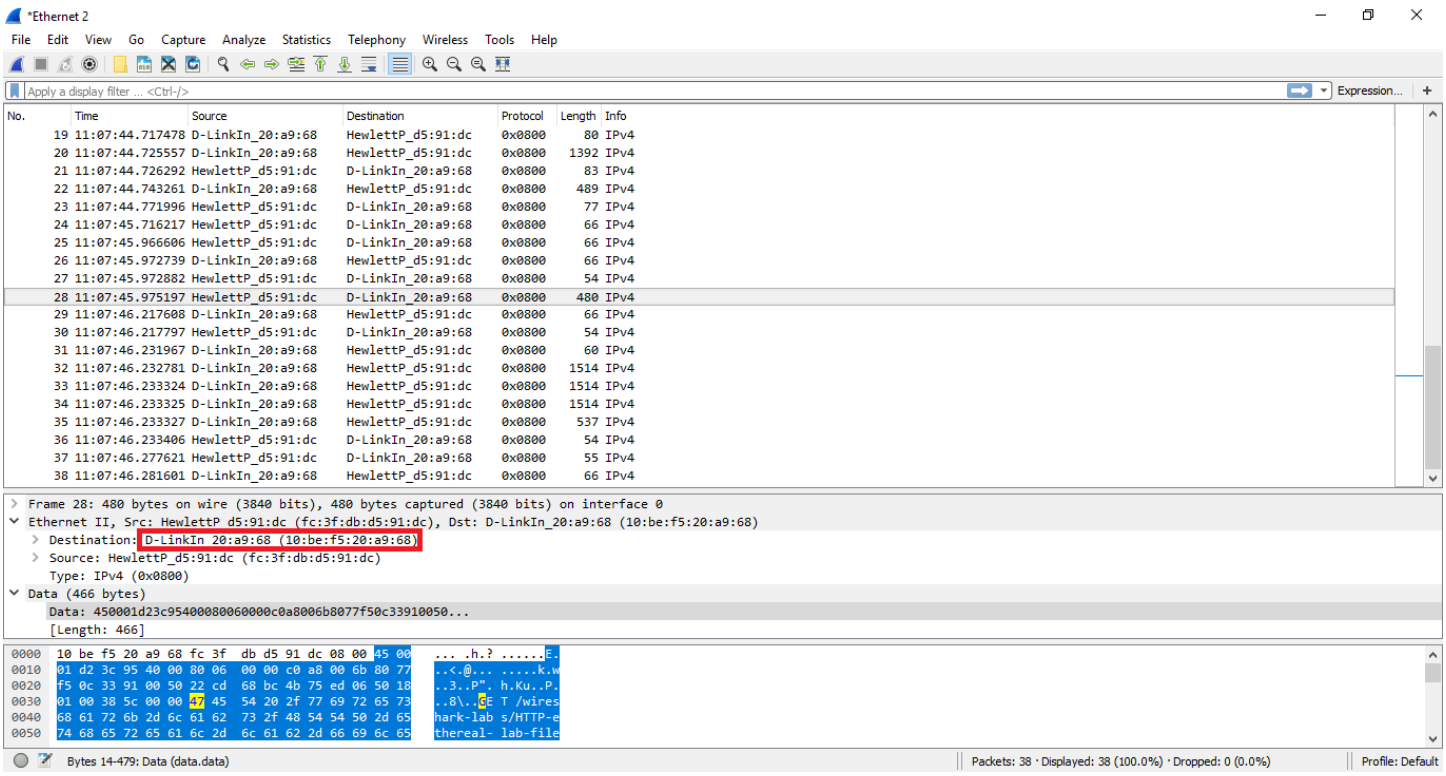
1. **What is the 48-bit Ethernet address of your computer?**

The 48-bit Ethernet address of my computer is fc:3f:db:d5:91:dc



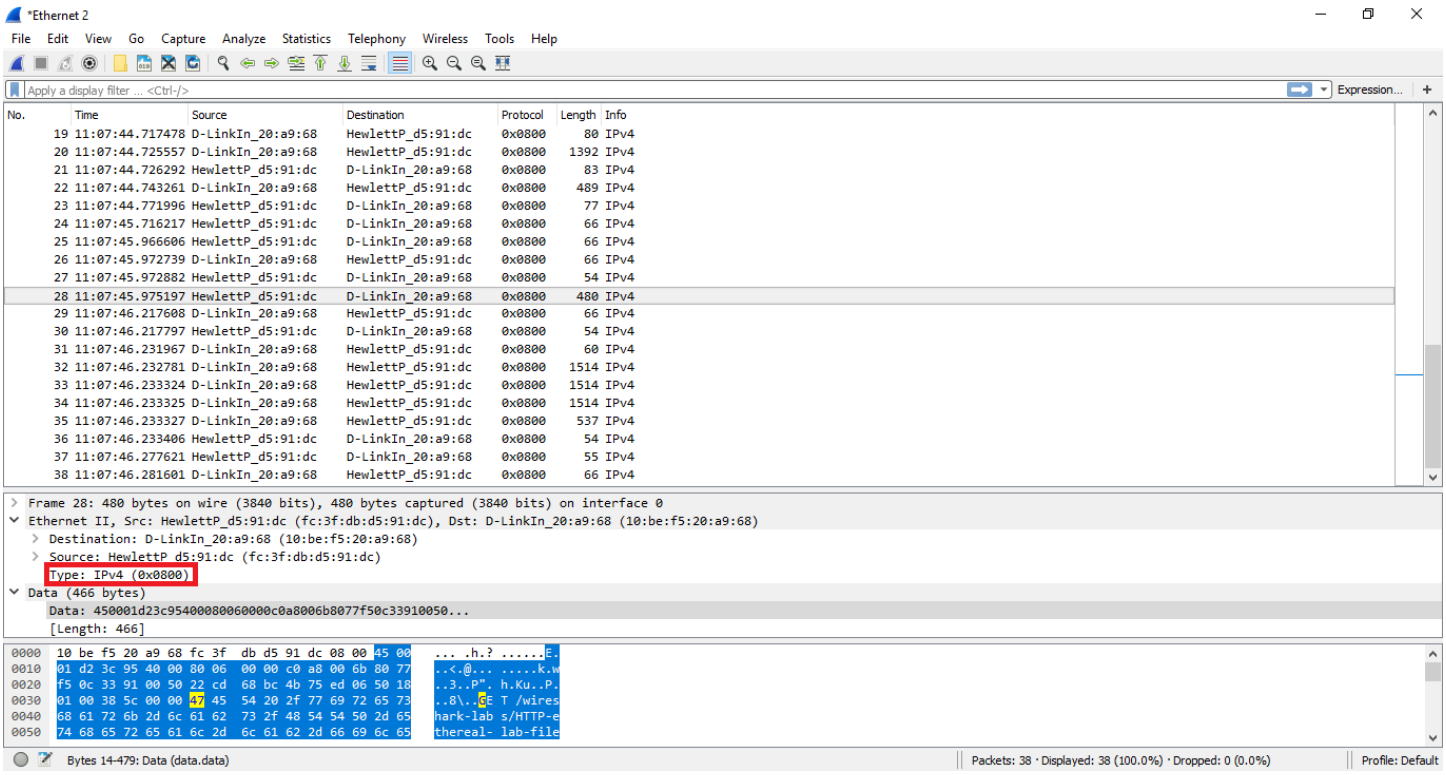
2. **What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is *no*). What device has this as its Ethernet address? [Note: this is an important question, and one that students sometimes get wrong. Re-read pages 468-469 in the text and make sure you understand the answer here.]**

The 48-bit destination address in the Ethernet frame is 10:be:f5:20:a9:68
This is not the Ethernet address of gaia.cs.umass.edu. It is the Ethernet address of my D-Link router.



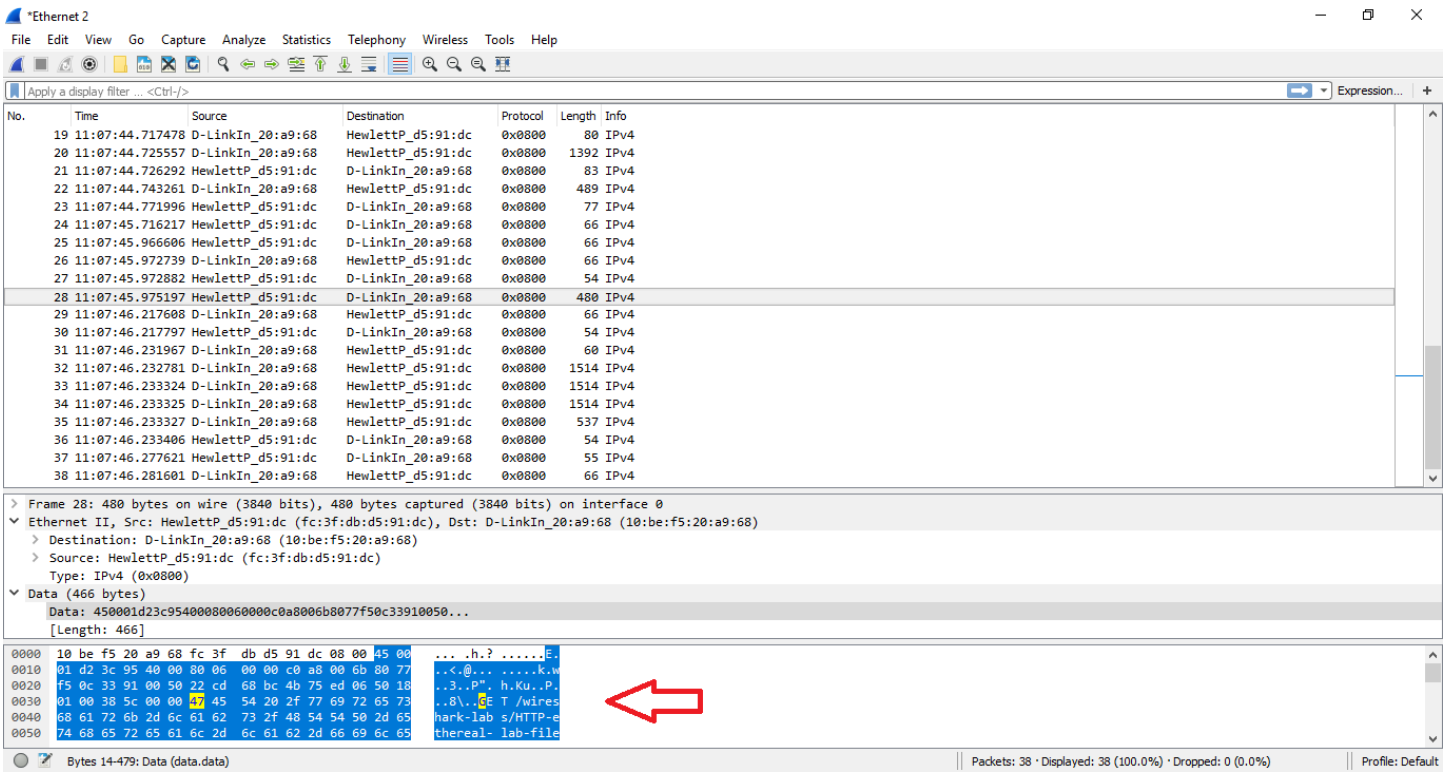
3. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

The hexadecimal value for the two-byte Frame type field is 0x0800. This corresponds to the IPv4 upper layer protocol.



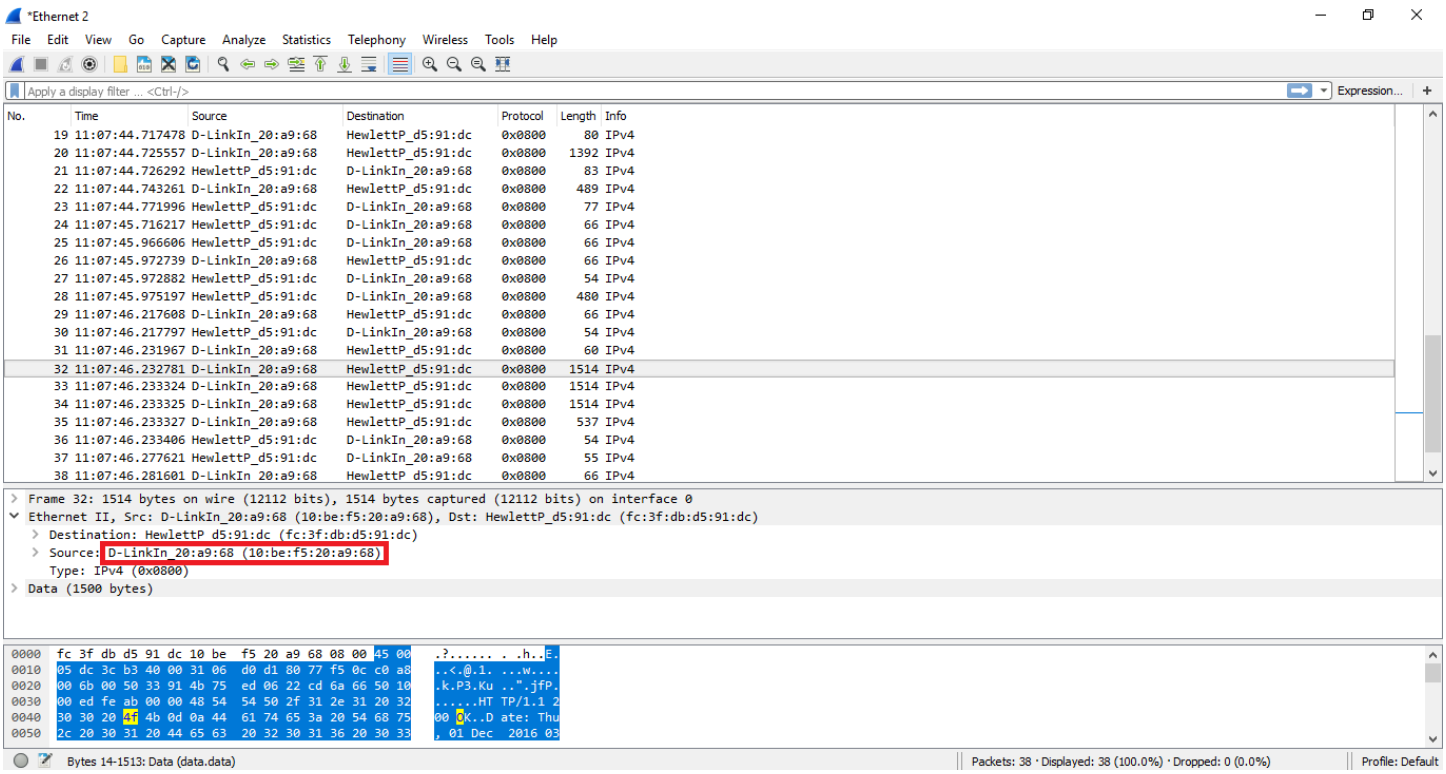
4. How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame?

The ASCII “G” in “GET” appears 54 bytes from the very start of the Ethernet frame.



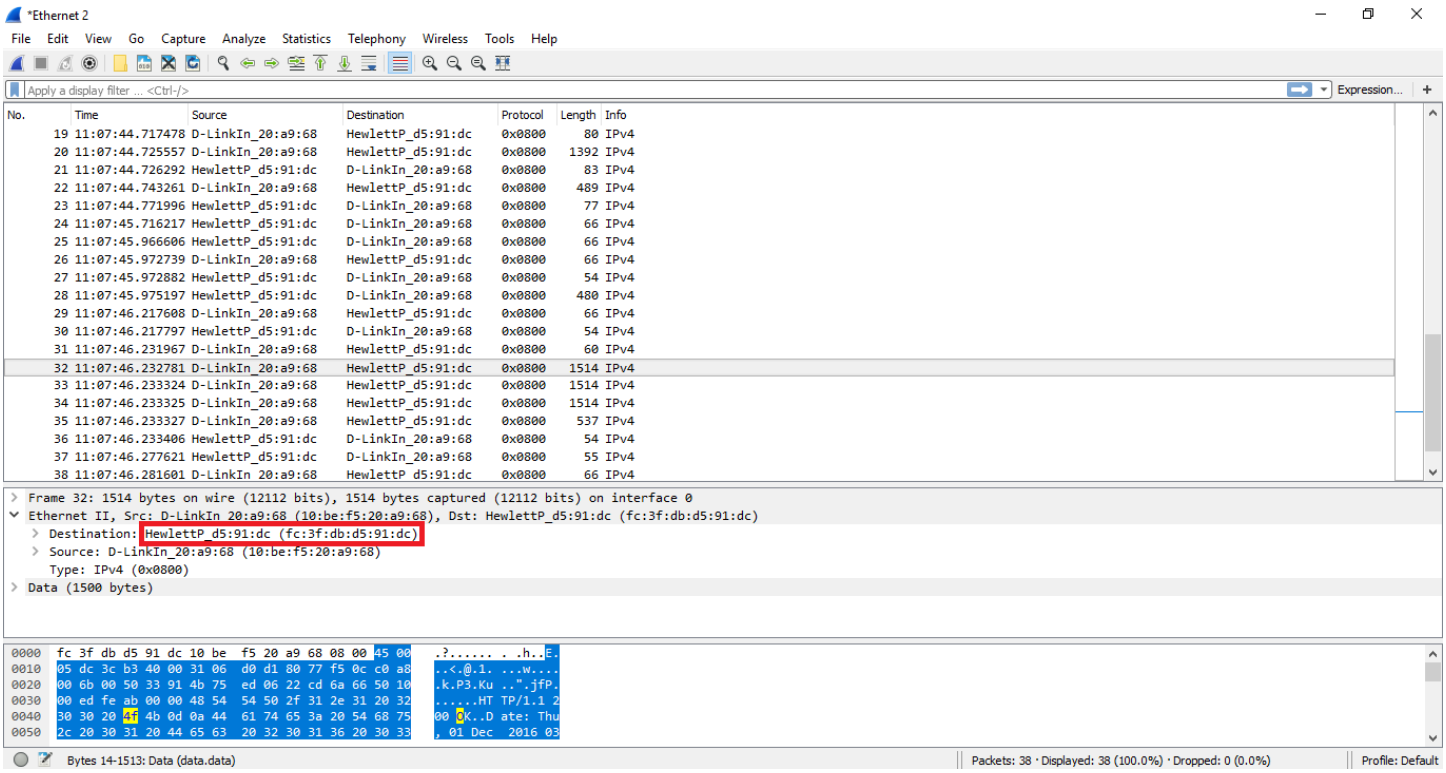
5. **What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is *no*). What device has this as its Ethernet address?**

The value of the Ethernet source address is 10:be:f5:20:a9:68
This is neither the address of my computer nor is it the address of gaia.cs.umass.edu. This is the Ethernet address of my D-Link router.



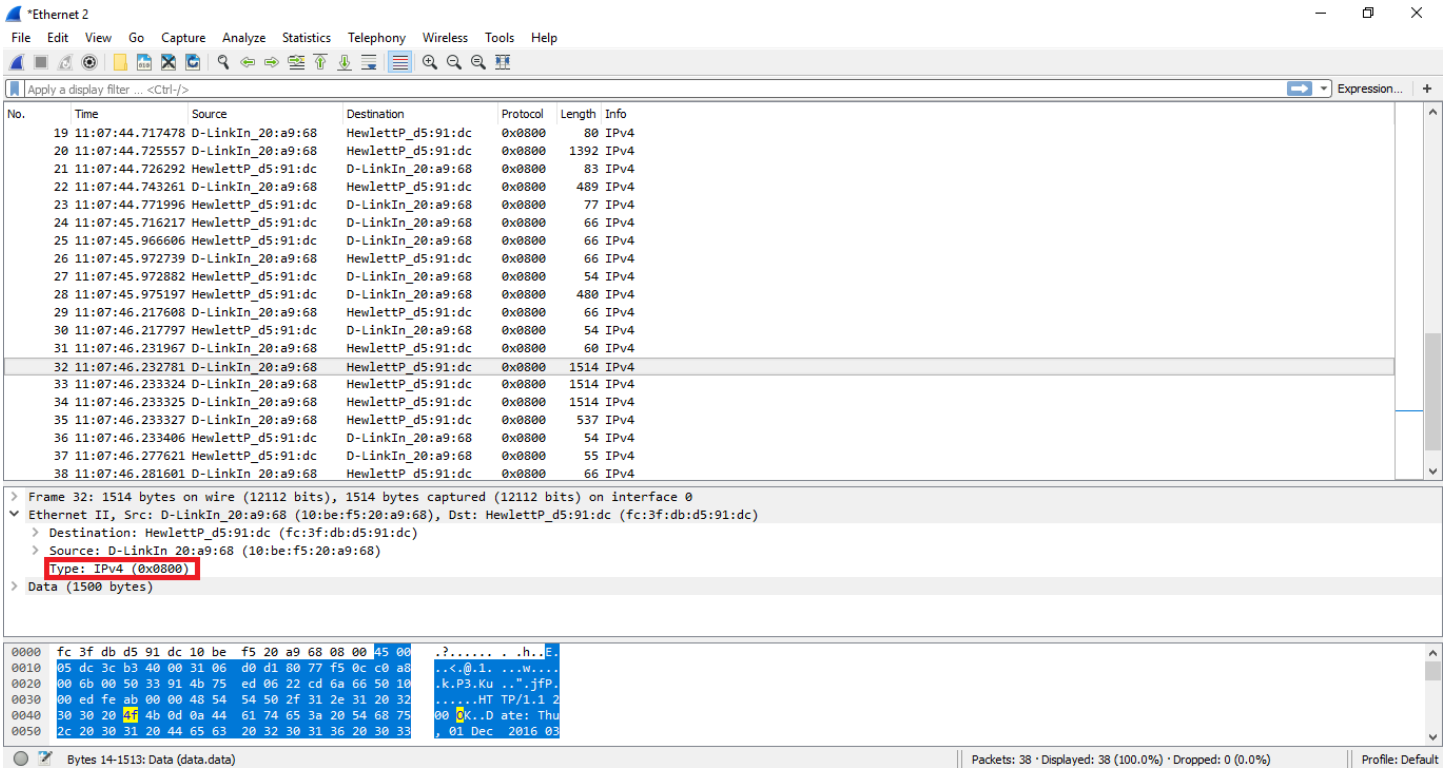
6. **What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?**

The destination address in the Ethernet frame is fc:3f:db:d5:91:dc and is the Ethernet address of my computer.



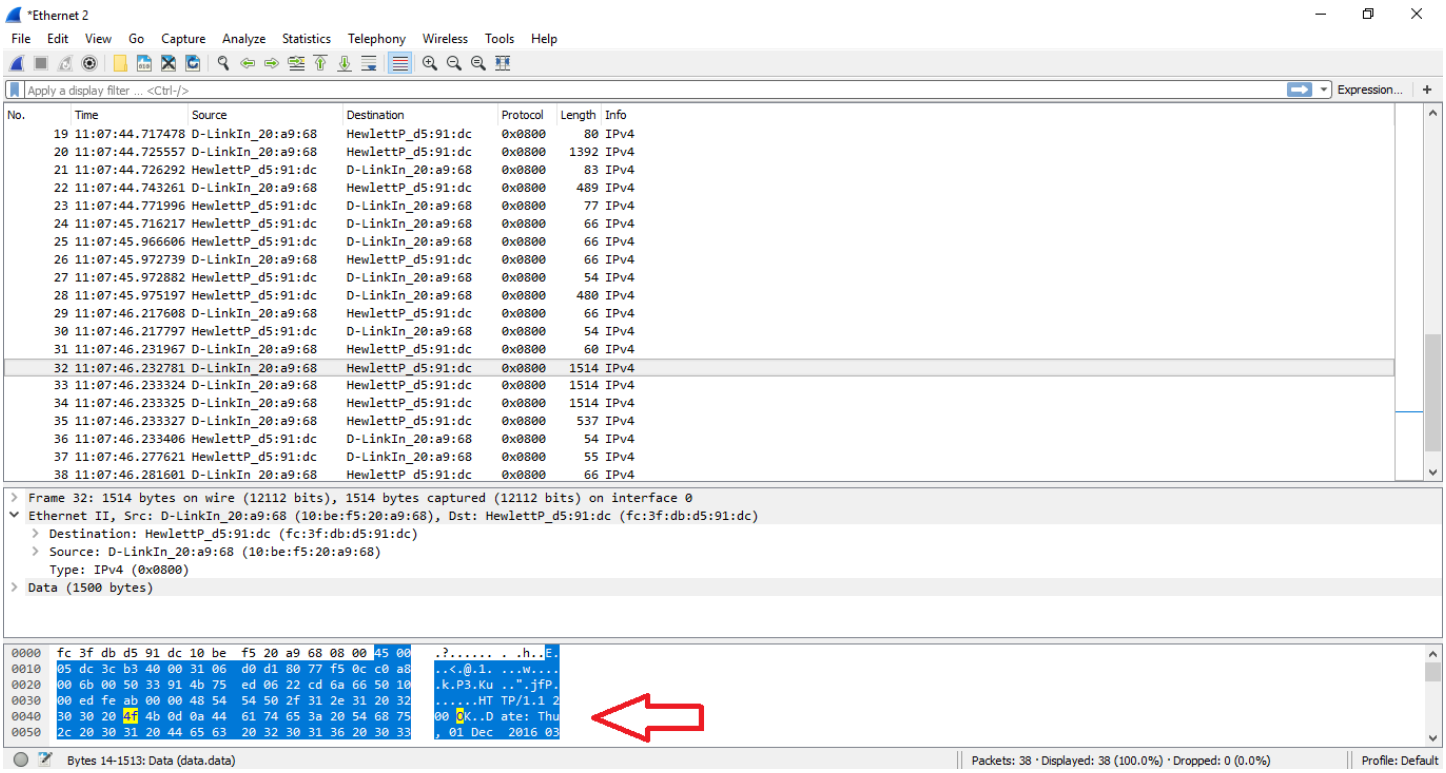
7. **Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?**

The hexadecimal value for the two-byte Frame type field is 0x0800. This corresponds to the IPv4 upper layer protocol.



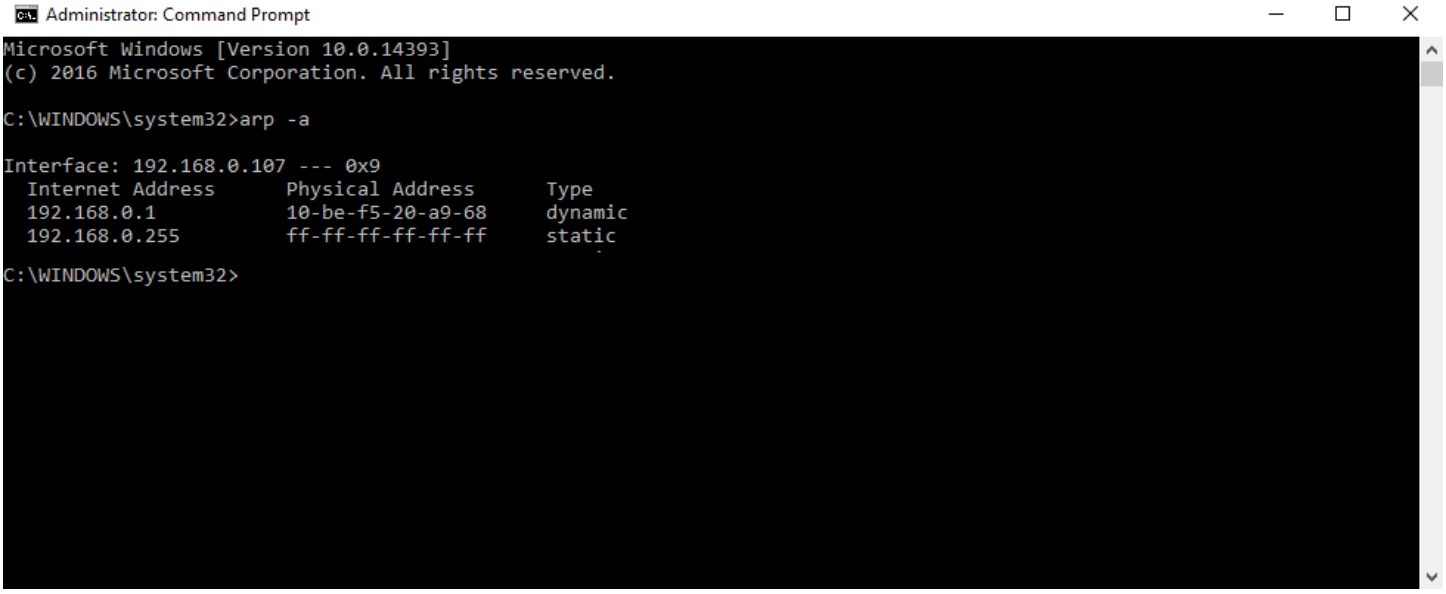
8. How many bytes from the very start of the Ethernet frame does the ASCII "O" in "OK" (i.e., the HTTP response code) appear in the Ethernet frame?

The ASCII "O" in "OK" appears 67 bytes from the very start of the Ethernet frame.



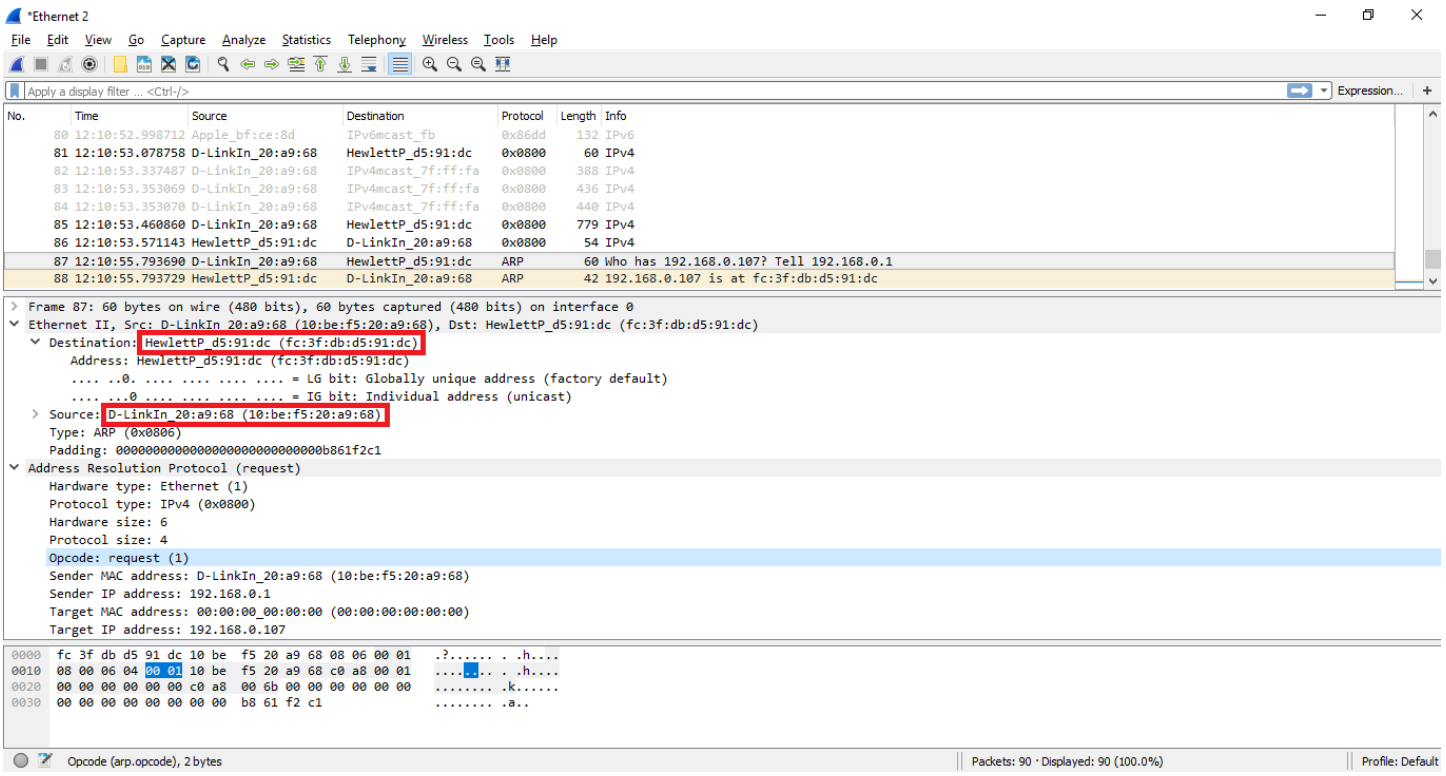
9. **Write down the contents of your computer's ARP cache. What is the meaning of each column value?**

The columns show Internet Address (IPv4), Physical Address (Ethernet), and Type (whether the IPv4 address is dynamic or static).



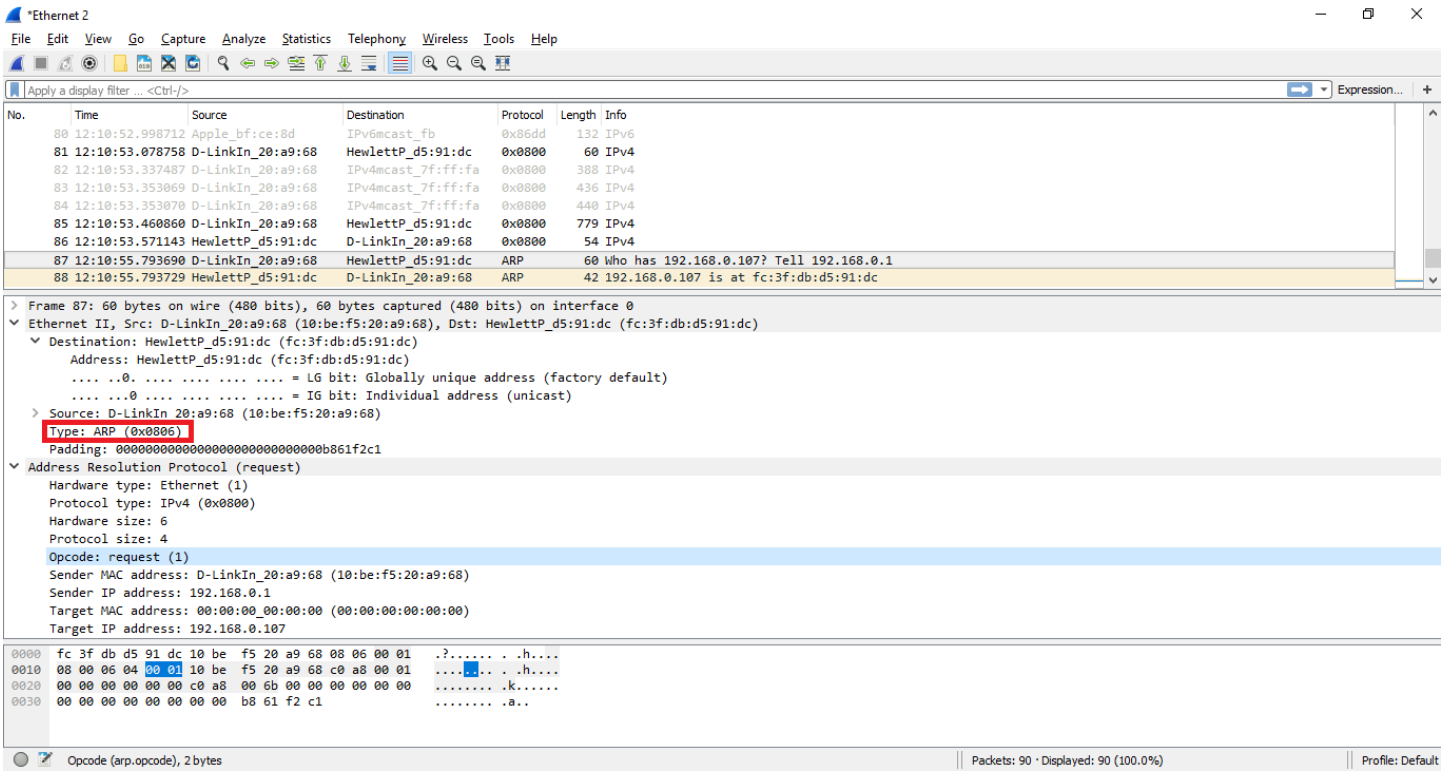
10. **What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?**

The hexadecimal value for the source addresses in the Ethernet frame containing the ARP request message is 10:be:f5:20:a9:68
The hexadecimal value for the destination addresses in the Ethernet frame containing the ARP request message is fc:3f:db:d5:91:dc



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

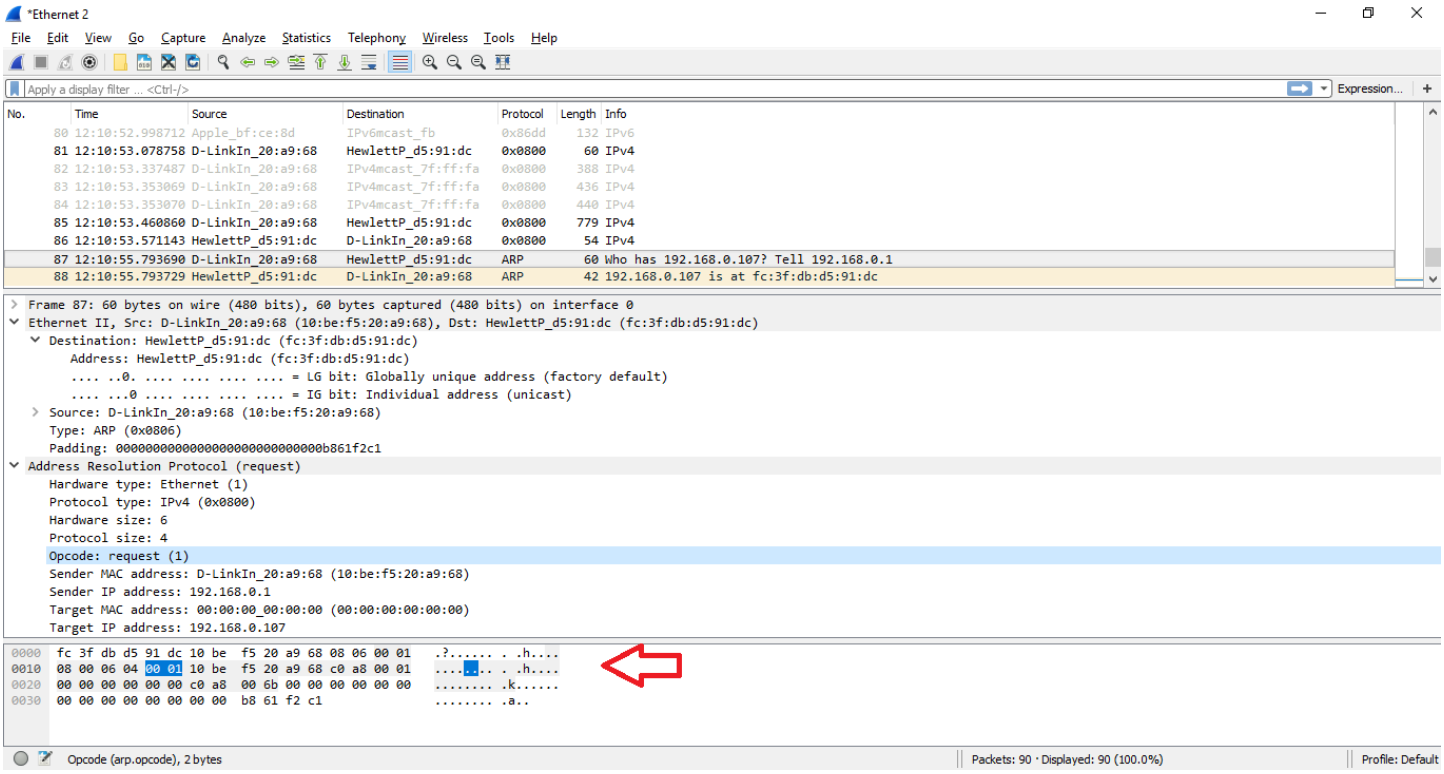
The hexadecimal value for the two-byte Ethernet Frame type field is 0x0806 which corresponds to the ARP upper level protocol.



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.

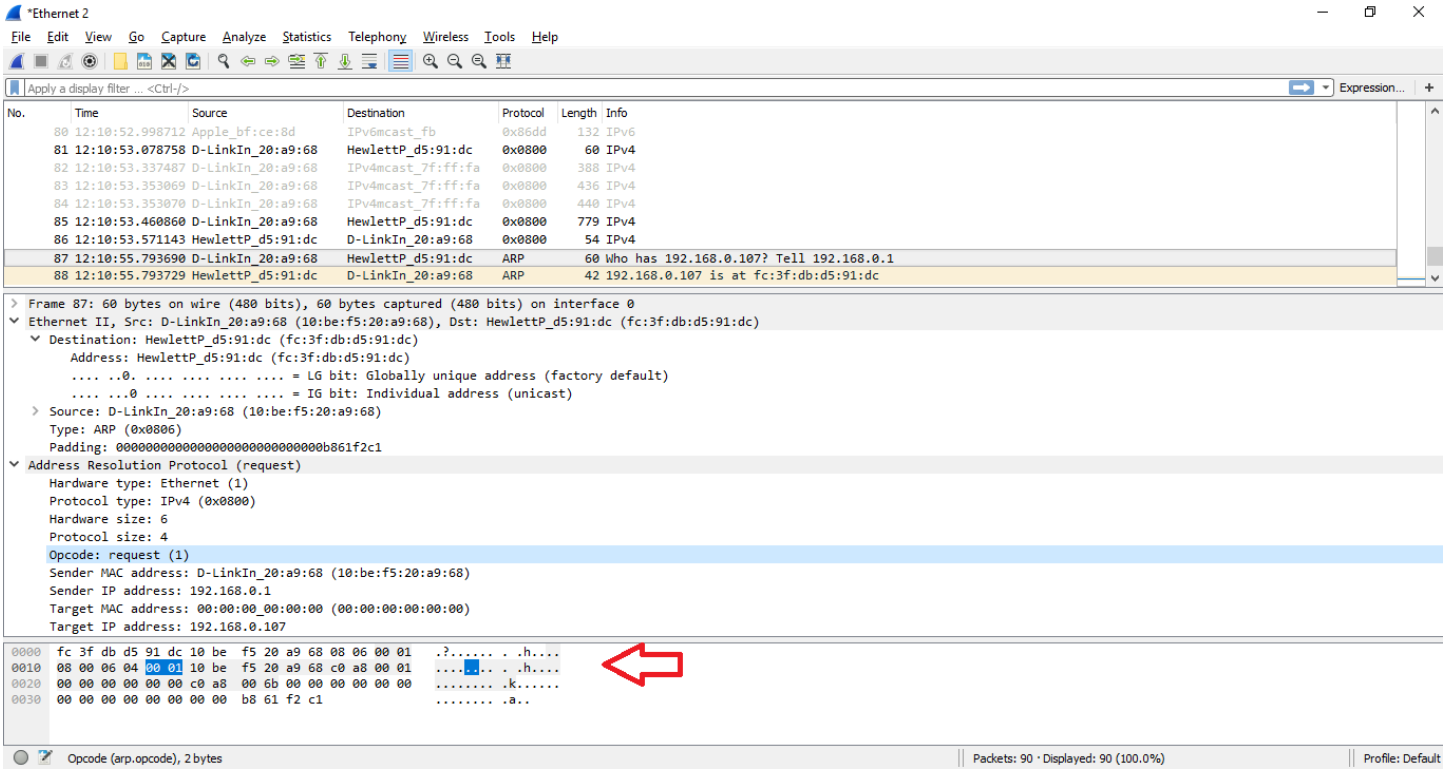
    a) How many bytes from the very beginning of the Ethernet frame does the ARP *opcode* field begin?

The ARP *opcode* field begins 20 bytes from the very beginning of the Ethernet frame.



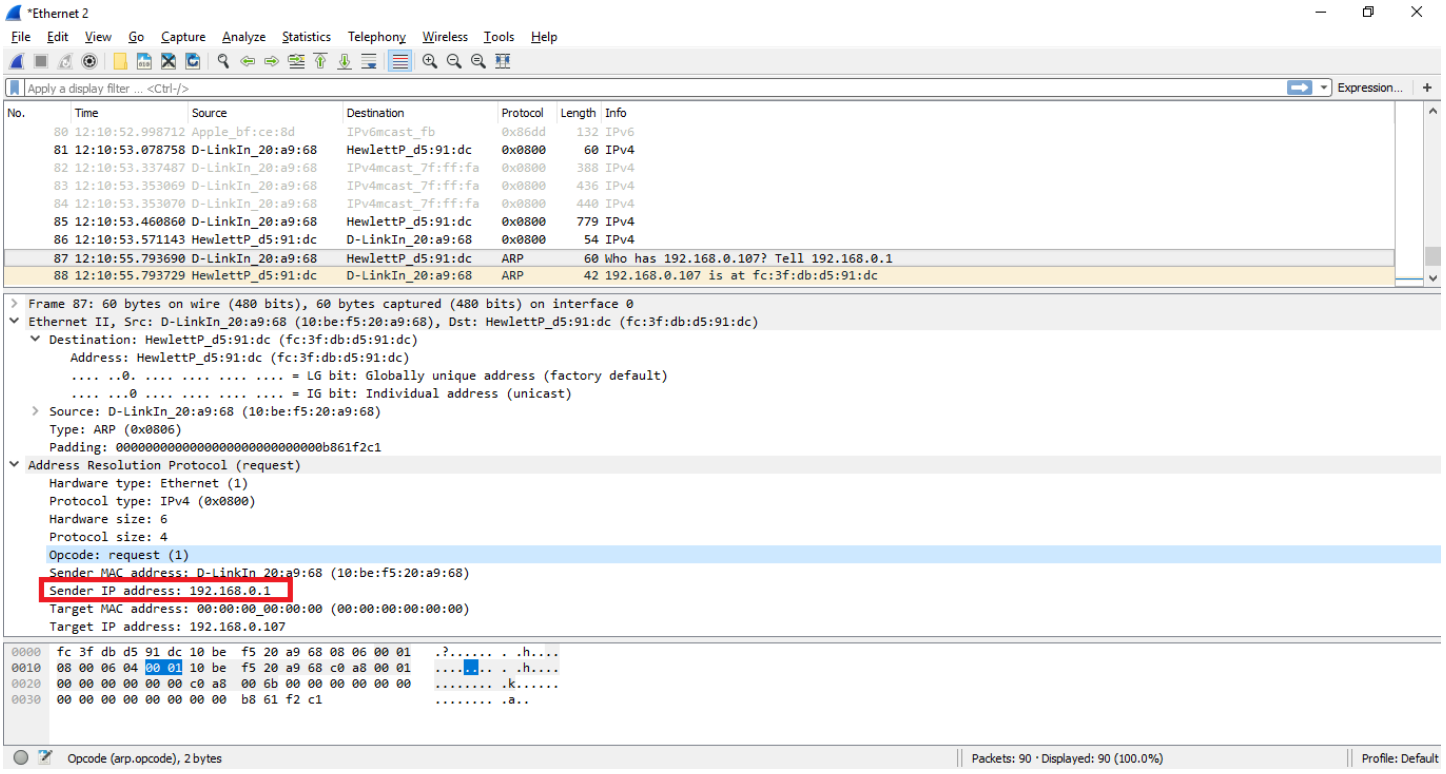
    b) What is the value of the *opcode* field within the ARP-payload part of the Ethernet frame in which an ARP request is made?

The value of the *opcode* field within the ARP-payload part of the Ethernet frame is 0x0001 (request).



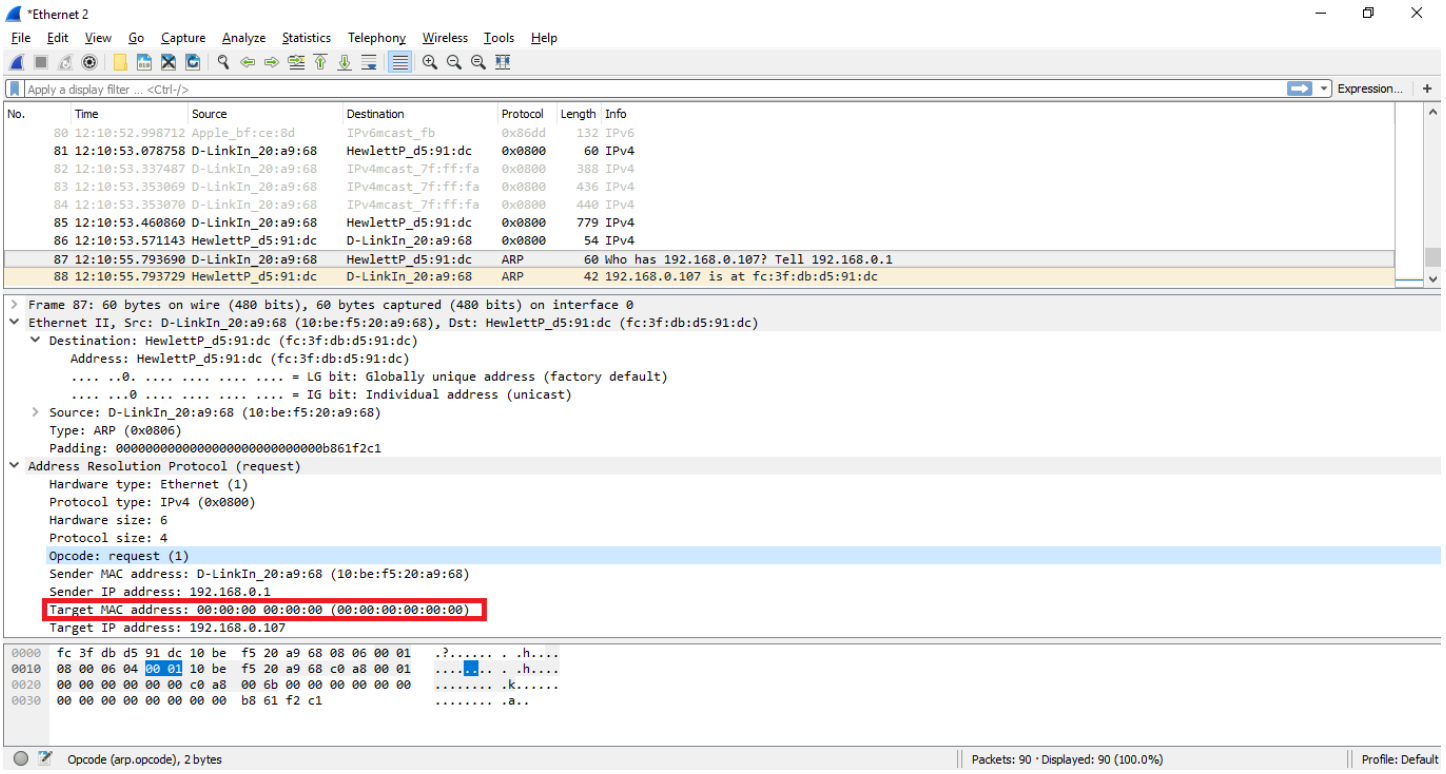
c) **Does the ARP message contain the IP address of the sender?**

Yes, the ARP message contains the IP address of the sender.



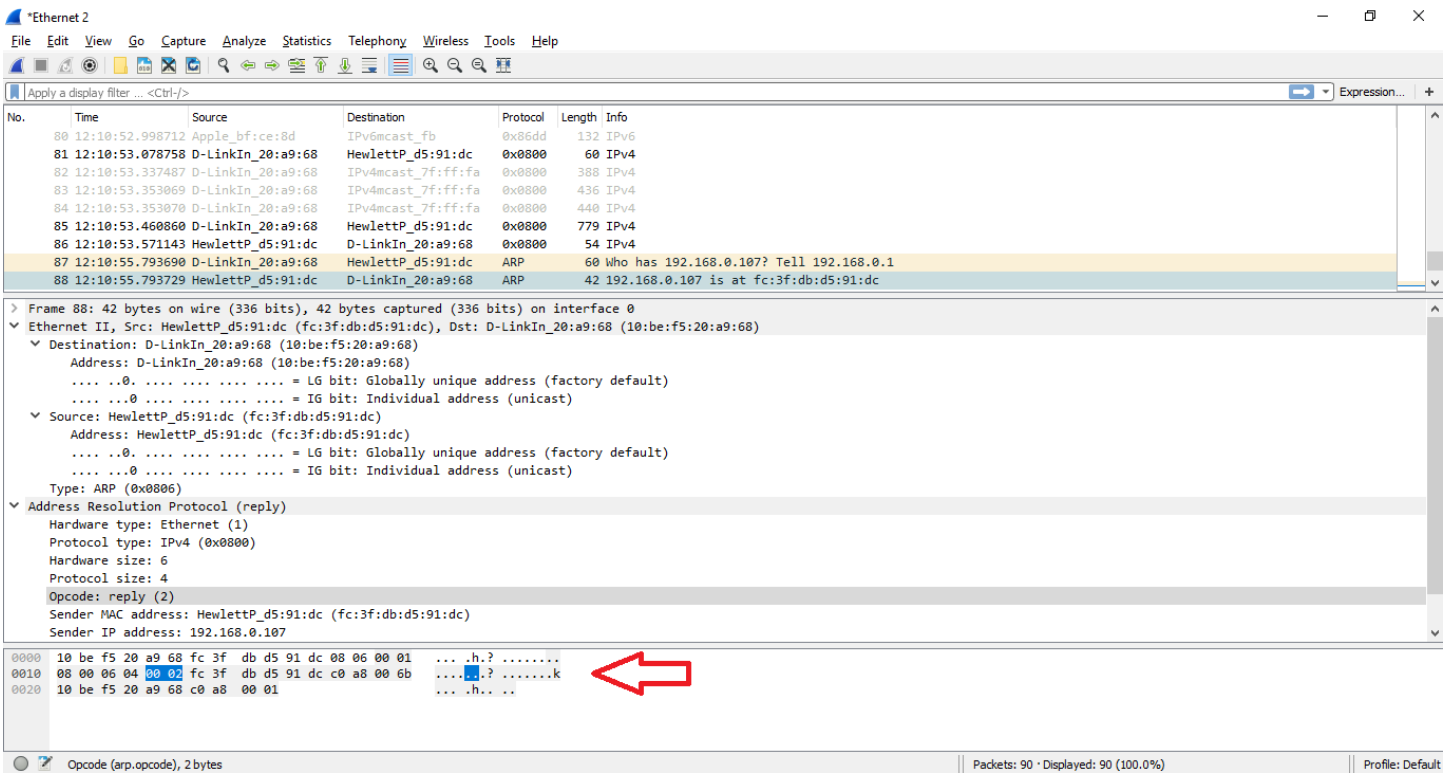
d) **Where in the ARP request does the "question" appear – the Ethernet address of the machine whose corresponding IP address is being queried?**

The *Target MAC address* field is set to 00:00:00:00:00:00 to question the machine whose corresponding IP address is being queried.



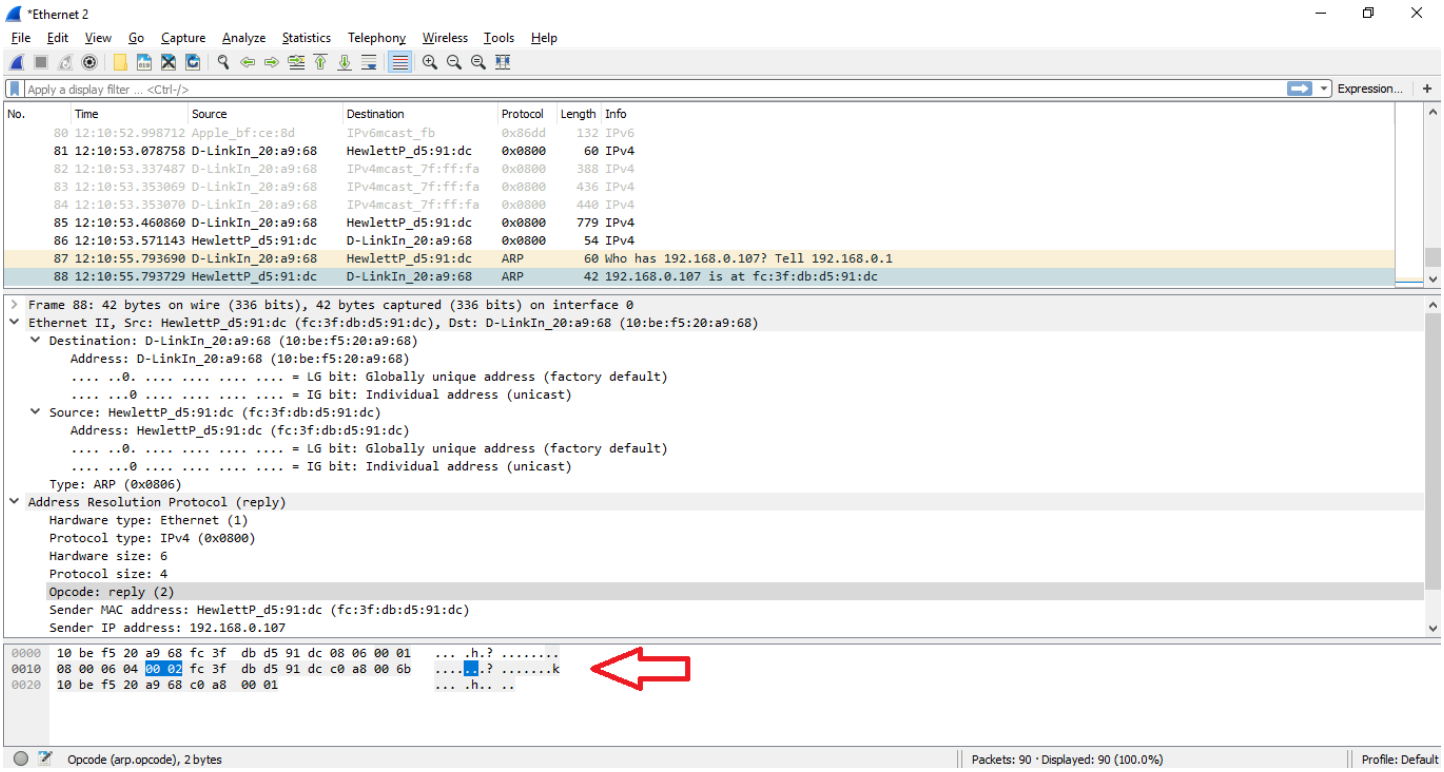
13. Now find the ARP reply that was sent in response to the ARP request.
    a) **How many bytes from the very beginning of the Ethernet frame does the ARP *opcode* field begin?**

The ARP *opcode* field begins 20 bytes from the very beginning of the Ethernet frame.



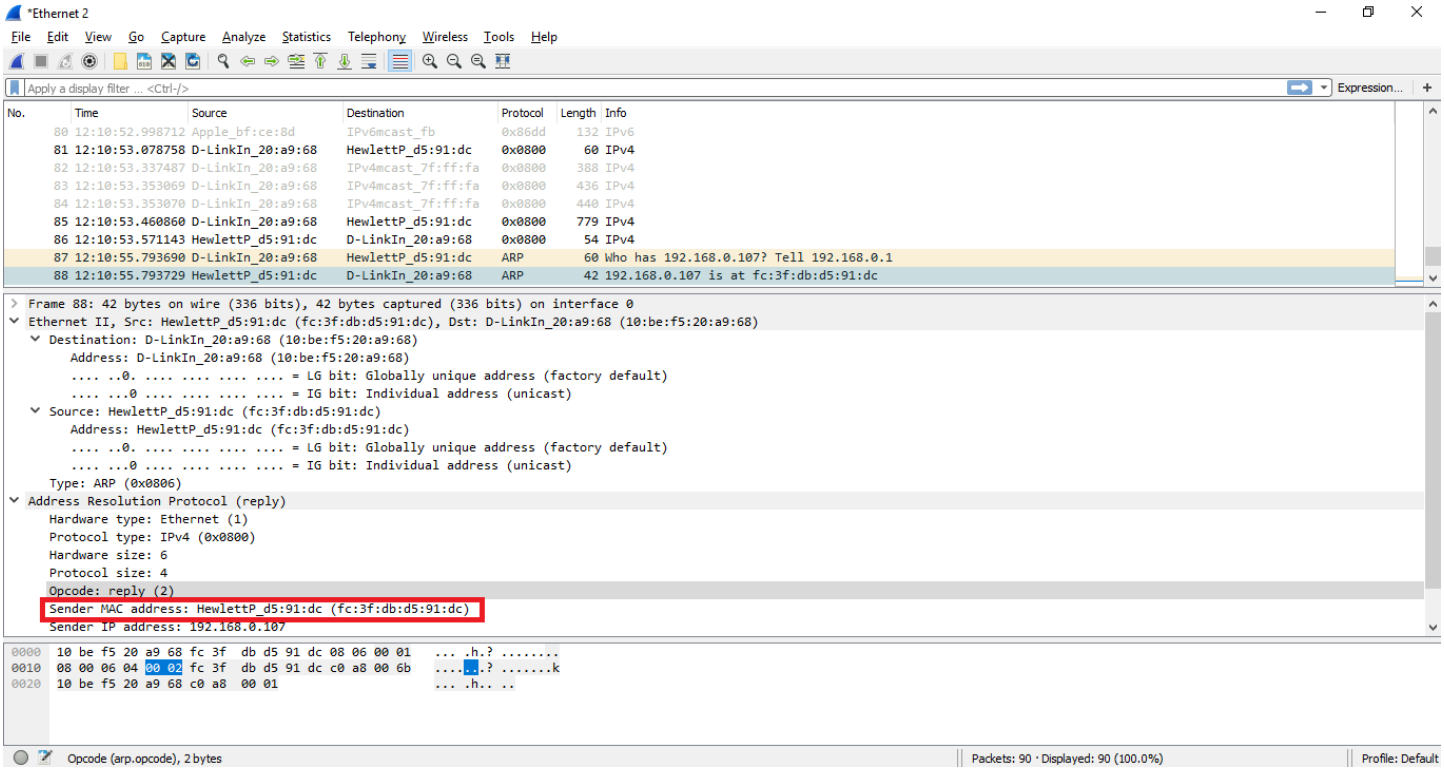
b) What is the value of the *opcode* field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

The value of the *opcode* field within the ARP-payload part of the Ethernet frame is 0x0002 (reply).



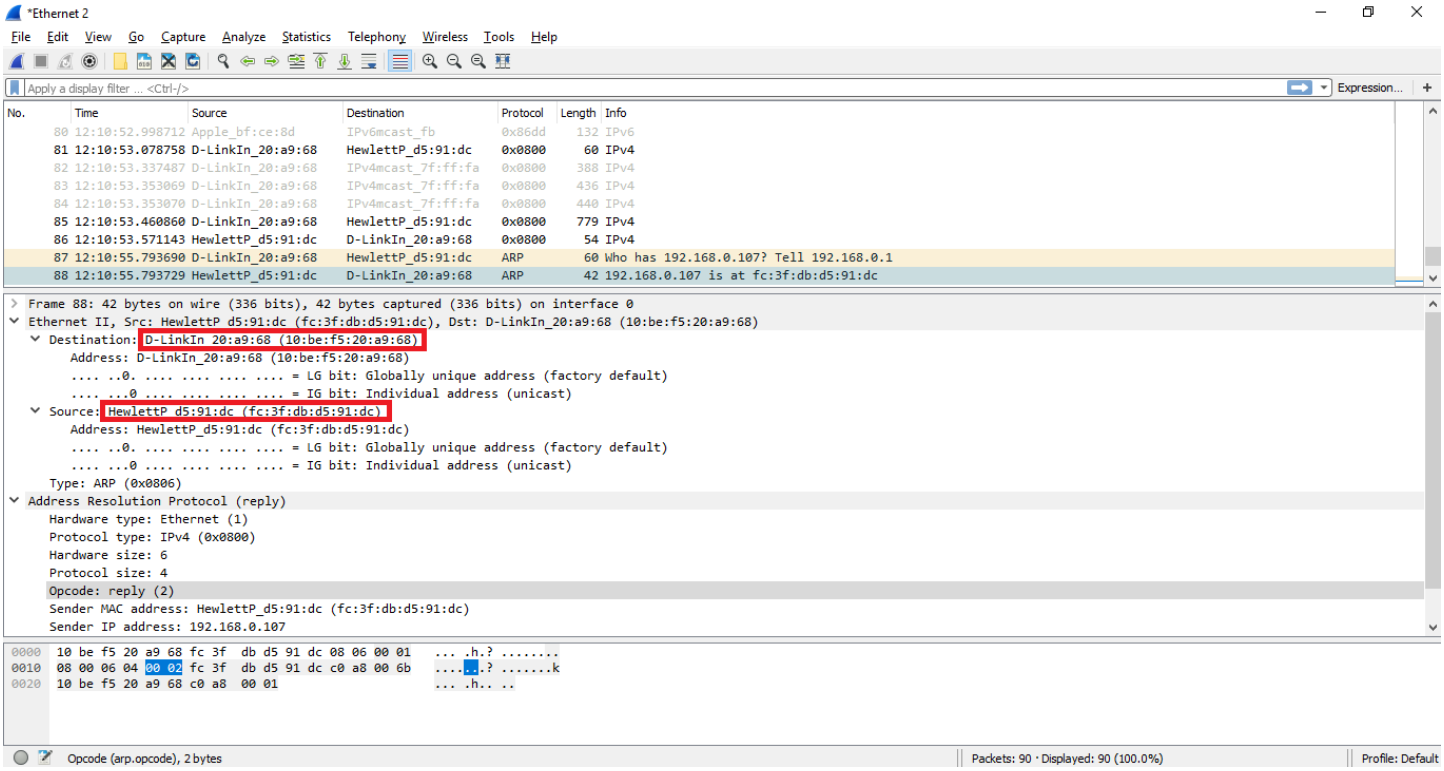
c) Where in the ARP message does the "answer" to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?

The answer to the earlier ARP request appears in the *Sender MAC address* field which contains the corresponding IP address that is being queried.



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

The hexadecimal value for the source addresses in the Ethernet frame containing the ARP reply message is fc:3f:db:d5:91:dc
The hexadecimal value for the destination addresses in the Ethernet frame containing the ARP reply message is 10:be:f5:20:a9:68



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?

There is no ARP reply sent in response to the ARP request in packet 6 in the packet trace because we are not the ones sending the request, and thus will not receive a reply. In the request sent in packet 1, 'our computer' is AmbitMic_a9:3d:68 and the request specifies that the response should be sent back to us – so we receive it. However, in packet 6, the sender is Telebit_73:8d:ce (not us) and they will receive the response directly.

Extra Credit

EX-1. 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?

EX-2. 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.