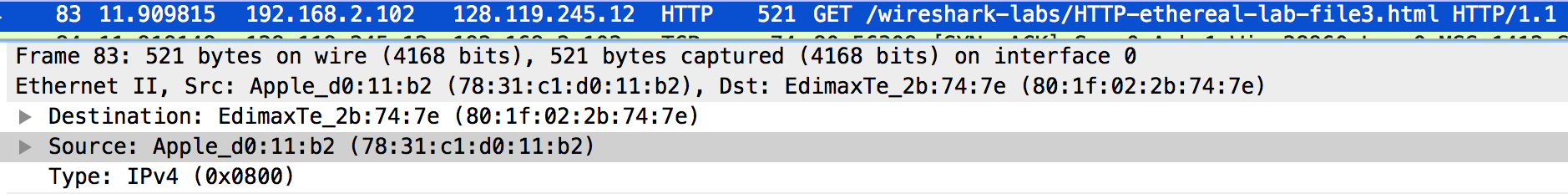
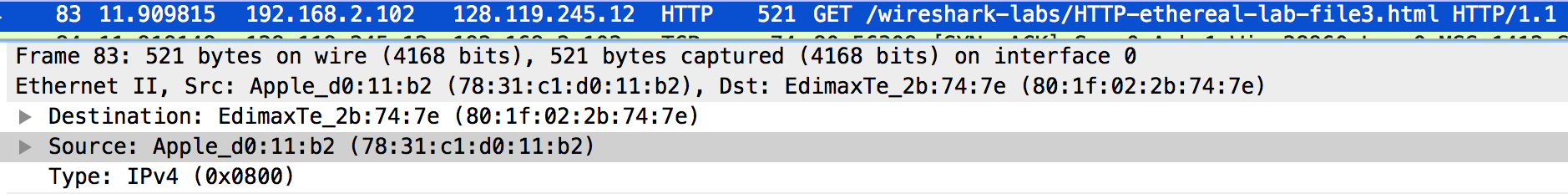
**Wireshark Ethernet and ARP**

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

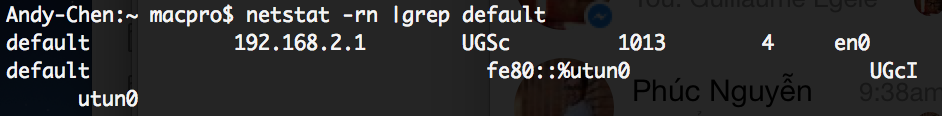
****

My computer MAC address: 78:31:c1:d0:11:b2

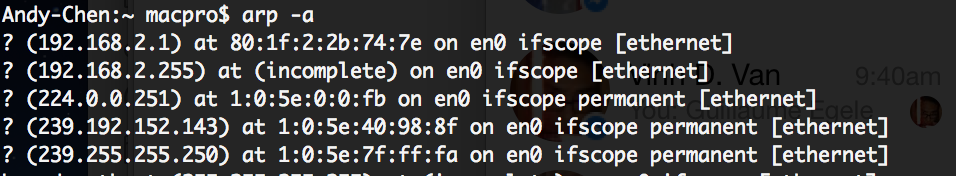
1. **What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is no). What device has this as its Ethernet address? [Note: this is an important question, and one that students sometimes get wrong. Re-read pages 468-469 in the text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

****

The MAC address of the destination in the Ethernet frame: 80:1f:02:2b:74:7e



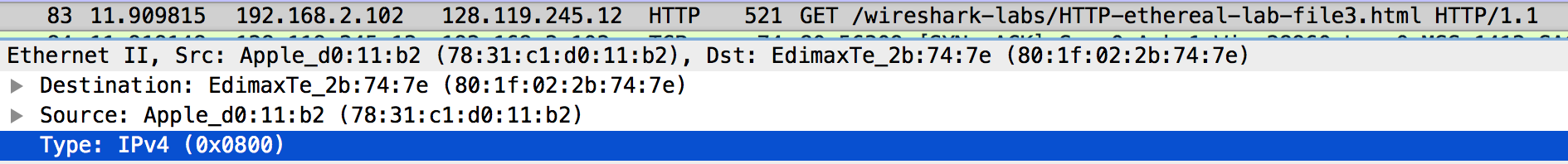
My connected router’s IP address is 192.168.2.1



The MAC address of my connected router (192.168.2.1) is 80:1f:2:2b:74:7e

* The MAC address of the destination in the Ethernet frame is also the MAC address of my connected router.

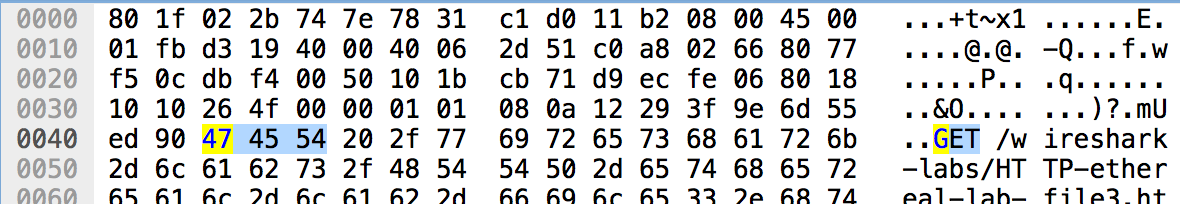
1. **Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?**



The hexadecimal value for the 2-bytes Frame type field is 0x0800

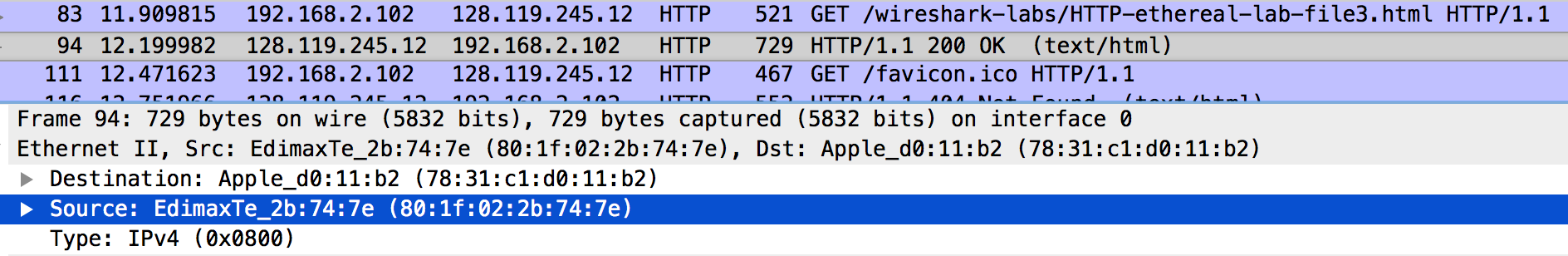
The upper layer corresponded to IPv4

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



It appears at the byte 67th from the begining the the Ethernet frame.

1. **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: 80:1f:02:2b:74:7e

It is neither the MAC address of my laptop or gaia.cs.umass.edu. It is indeed the address of my connected router as shown in question 2.

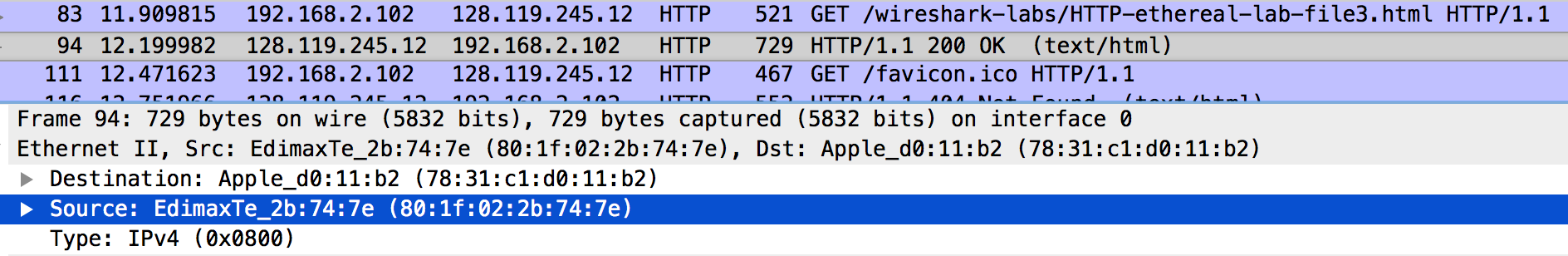
1. **What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?**

The destination address in the Ethernet frame is 78:31:c1:d0:11:b2

My computer MAC address: 78:31:c1:d0:11:b2 as shown in question 1.

* It is exactly my laptop MAC address.

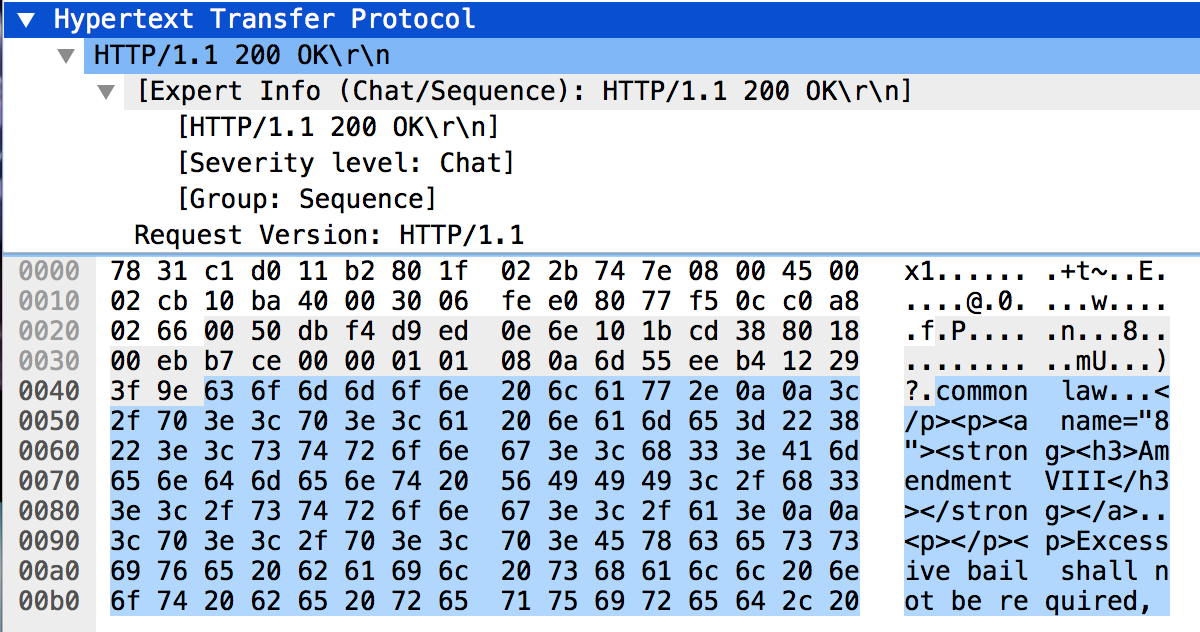
1. **Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?**



The hexadecimal value for the 2-bytes Frame type field is 0x0800

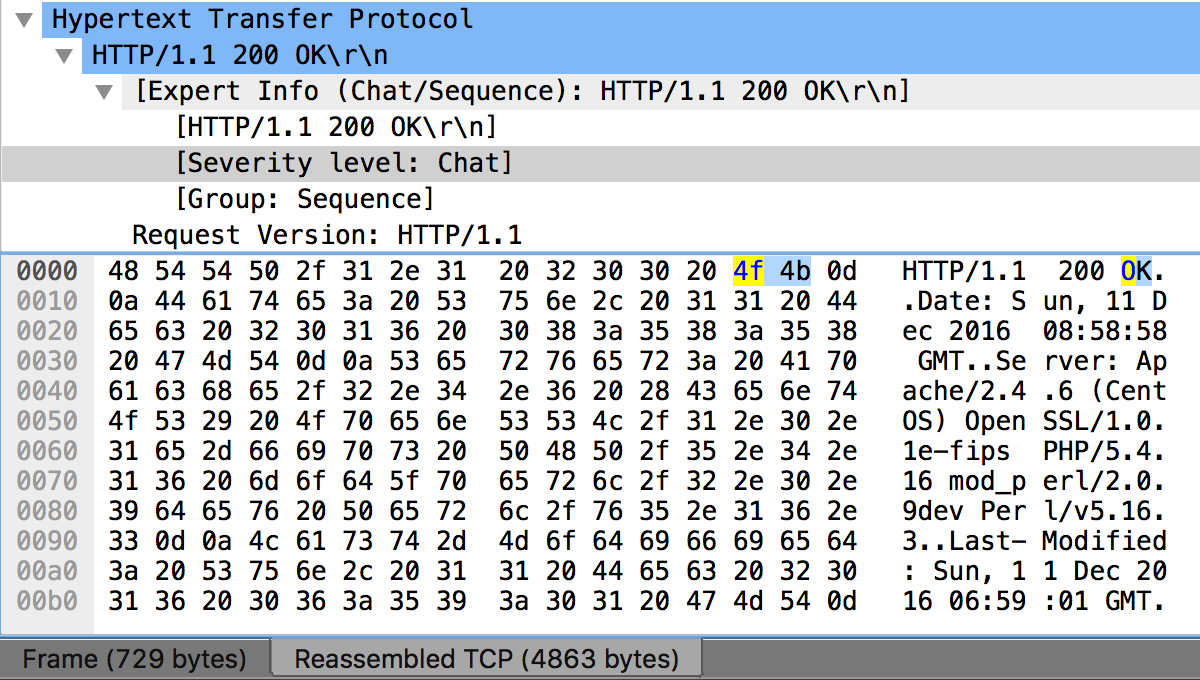
The upper layer corresponded to IPv4

1. **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?**



We know that the HTTP response code begins at the byte 67th.

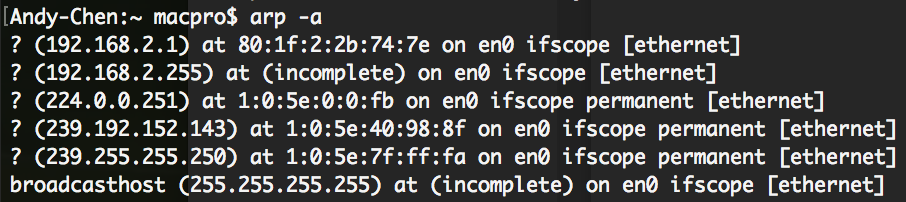
Then we reassemble the TCP, we have:



It means the character “O” of “OK” is at the 14th byte from the beginning of the HTTP response code.

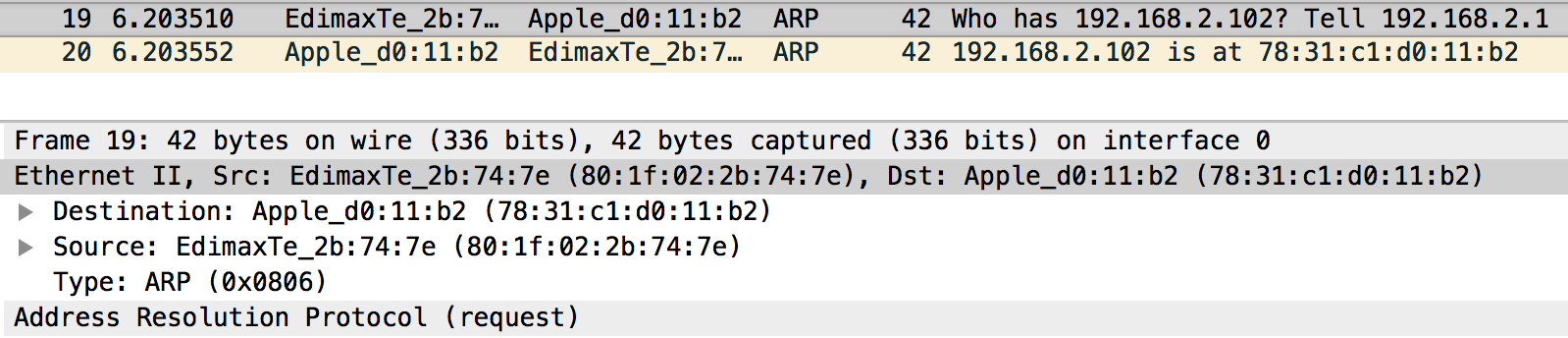
* Thus, the “O” is at the **byte 80th** (which is 14 + 66) from the beginning of the Ethernet frame.

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



It shows the IP address, MAC address and whether the protocol is permanent or not.

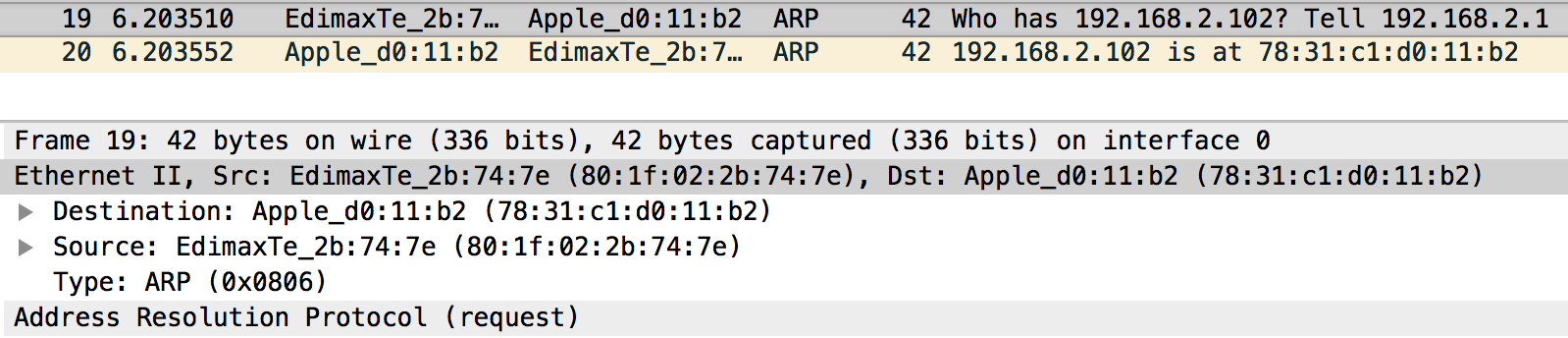
1. **What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?**



Source address: 80:1f:02:2b:74:7e

Destination address: 78:31:c1:d0:11:b2

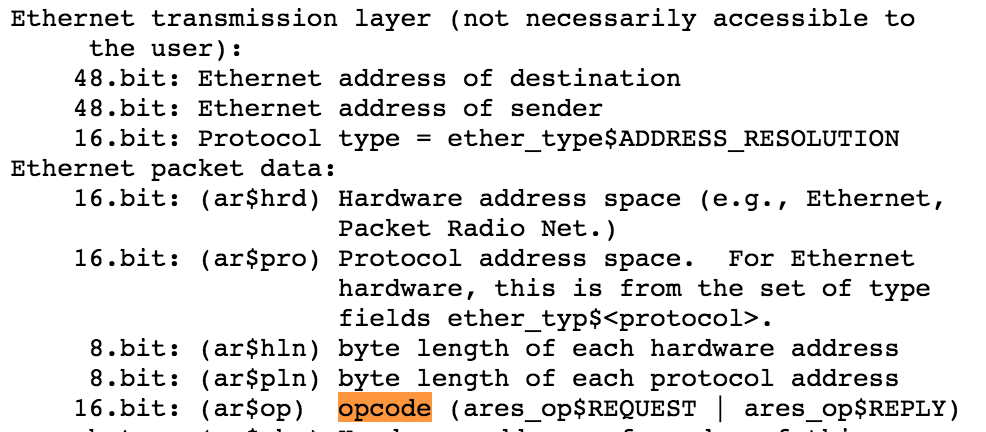
1. **Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?**



The hexadecimal value: 0x0806

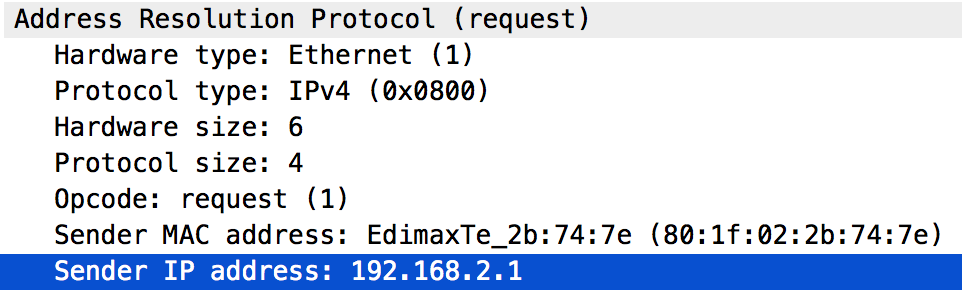
It corresponds to ARP protocol

1. **Download the ARP specification from** [**ftp://ftp.rfc-editor.org/in-notes/std/std37.txt**](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**](http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html)**.**
   1. **How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?**



The ARP opcode field begins at byte 21th from the very beginning of the Ethernet frame (The photo is taken from the std37.txt file).

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

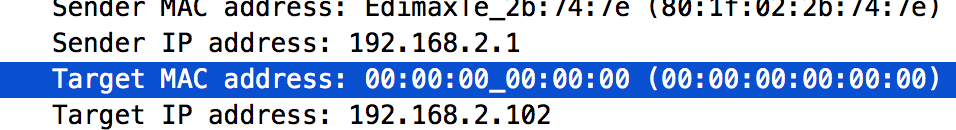


The value for opcode field within the ARP-payload of the request is 1, for request.

* 1. **Does the ARP message contain the IP address of the sender?**

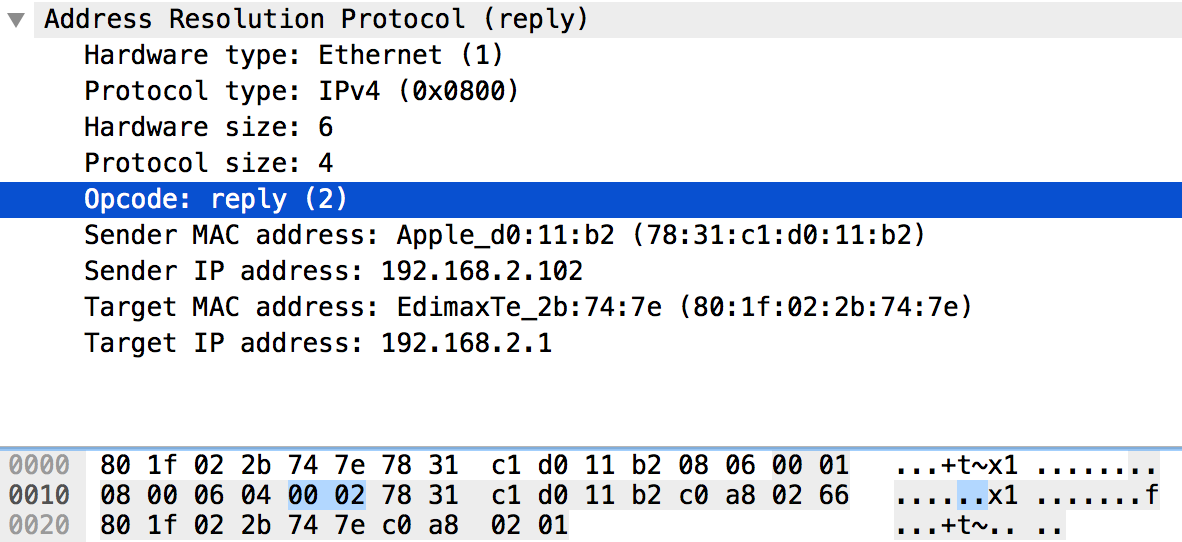
Yes, it does.

* 1. **Where in the ARP request does the “question” appear – the Ethernet address of the machine whose corresponding IP address is being queried?**



“Target MAC address” is set to 00:00:00:00:00:00 to question the machine whose corresponding IP address (192.168.2.102) is being queried.

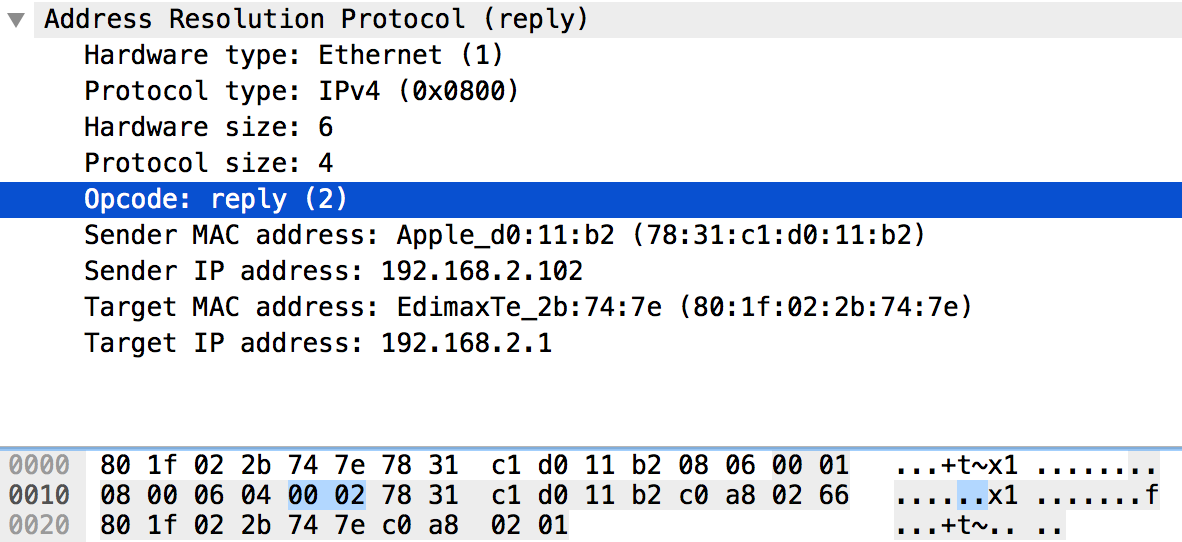
1. **Now find the ARP reply that was sent in response to the ARP request.**
   1. **How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?**



The ARP opcode field begins at byte 21th from the very beginning of the Ethernet frame

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

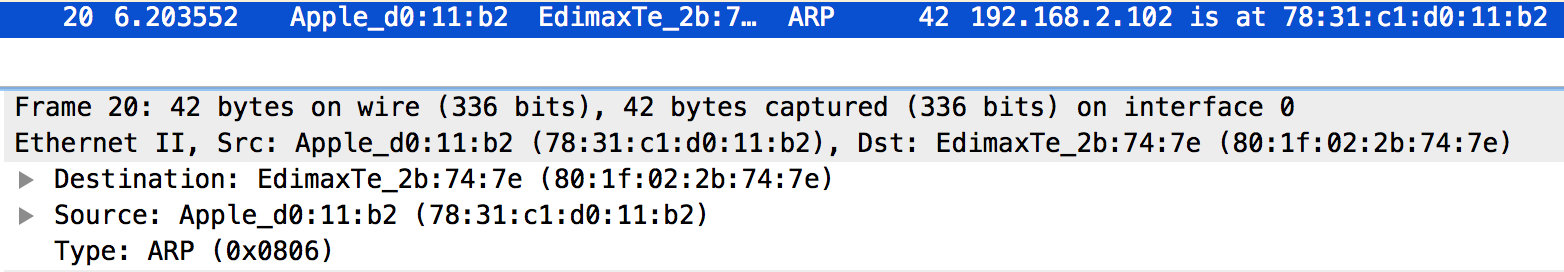
The value for opcode field within the ARP-payload part of Ethernet frame in which an ARP response is 2.

* 1. **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 request ARP questions the MAC address for IP address 192.168.2.102

* + - The “answer” is at the Sender MAC address.

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



Source address: 78:31:c1:d0:11:b2

Destination address: 80:1f:02:2b:74:7e

1. **Open the ethernet-ethereal-trace-1 trace file in** [**http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip**](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?**

Because the ARP request message is a Broadcast message, means every host in the same network can receive this message (it does not know which is the computer), thus we (the one in the same network) also receive it. However, the ARP response message is unicast to the one who sent the request message, thus we cannot see the response message for the ARP request message in line 6 (we are not this host).

