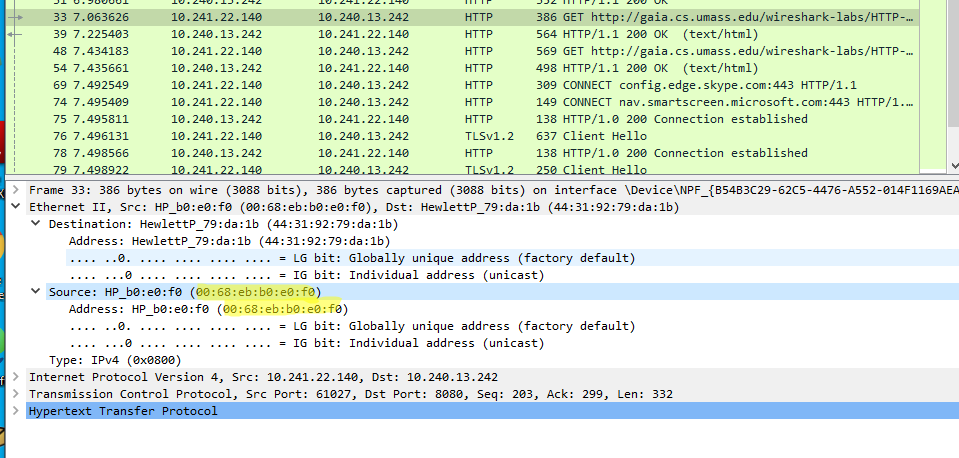
.**Lab Work:**

**Capturing and analyzing Ethernet frame**

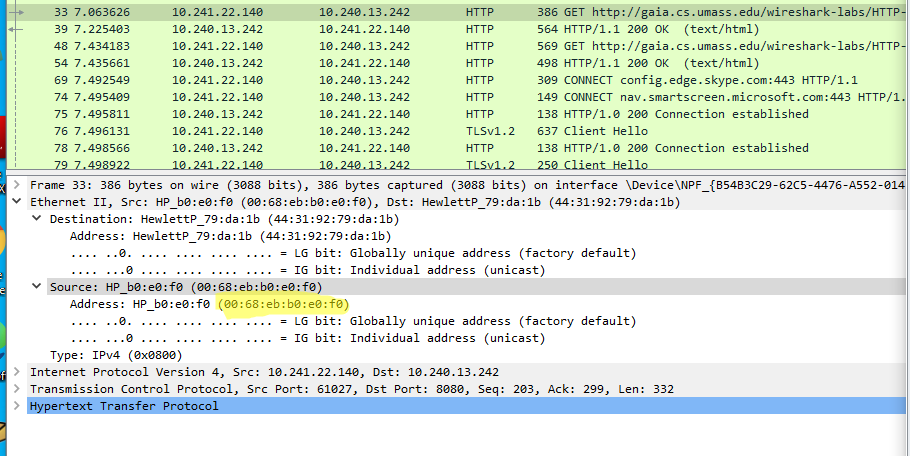
* Clear your browser cache.
* Enter the following URL into your browser  
   <http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html>  
  your browser should display the rather lengthy US Bill of Rights.
* Stop Wireshark packet capture.
* Find HTTP GET message and the HTTP OK message and record the packet numbers on a sheet for your reference.
* Select the Ethernet frame containing the HTTP GET message.

Answer the following questions based on the contents of the Ethernet frame containing the **HTTP GET** message:

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

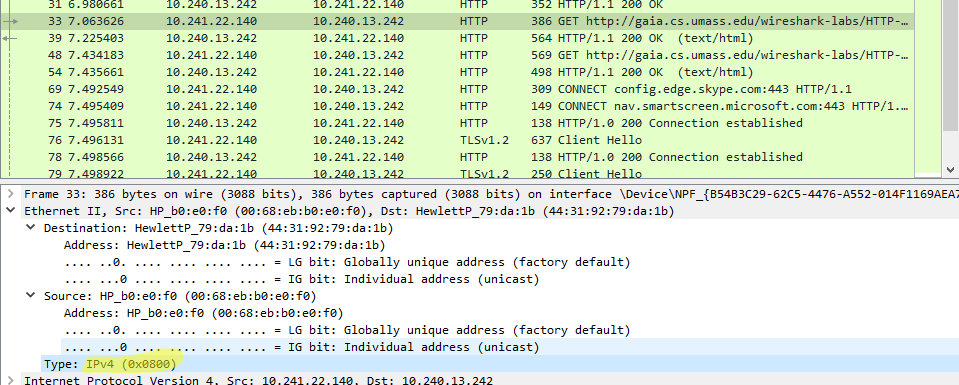


1. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is no). What device has this as its Ethernet address?



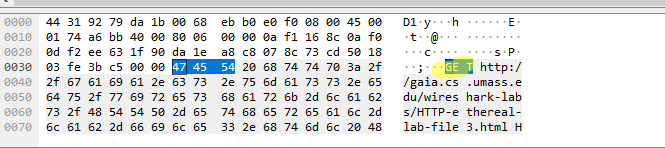
1. Give the hexadecimal value for the Frame type field. What upper layer protocol does this value corresponds to?

IPv4 (0x0800)



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

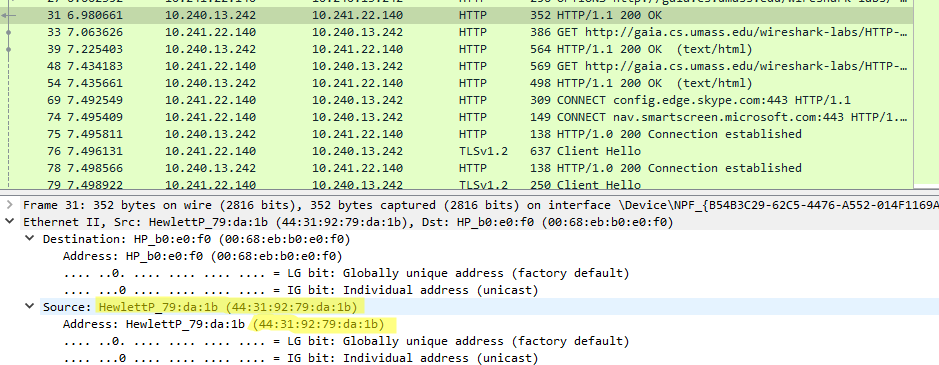
There is a 54 byte before the GET



Answer the following questions based on the contents of the Ethernet frame containing the HTTP response (OK) message:

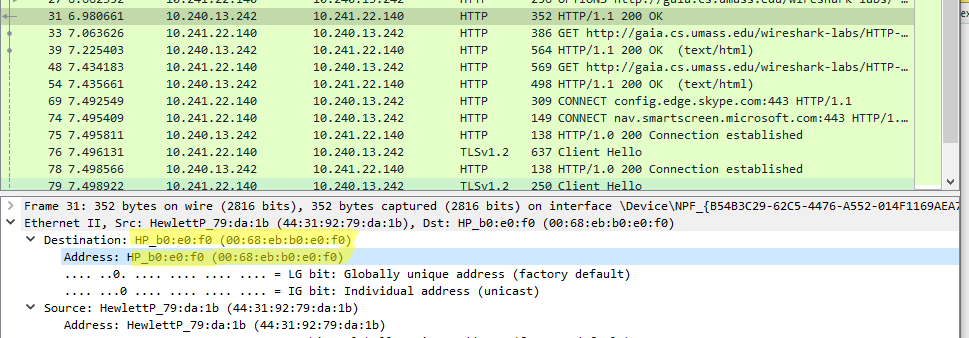
1. What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is no). What device has this as its Ethernet address?

No, the address is of gaia,cs,umass.edu



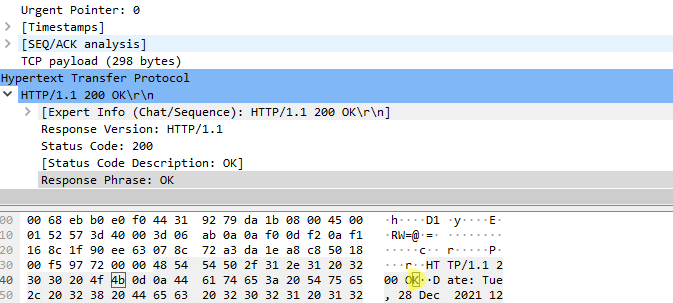
1. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?

Yes it’s the address of my computer



1. How many bytes from the very start of the Ethernet frame does the ASCII “O” in “OK” appear in the Ethernet frame?

There are 67 byte before the OK



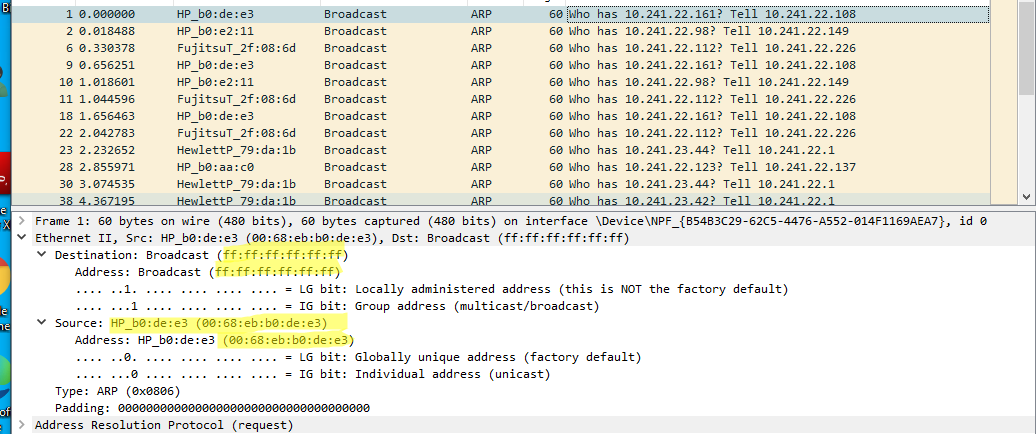
**Capturing and analyzing an ARP traffic**

* Use the same trace of the previous part. Enter **arp** in the filter field.
* Find any ARP request message and its corresponding response message.

Answer the following questions:

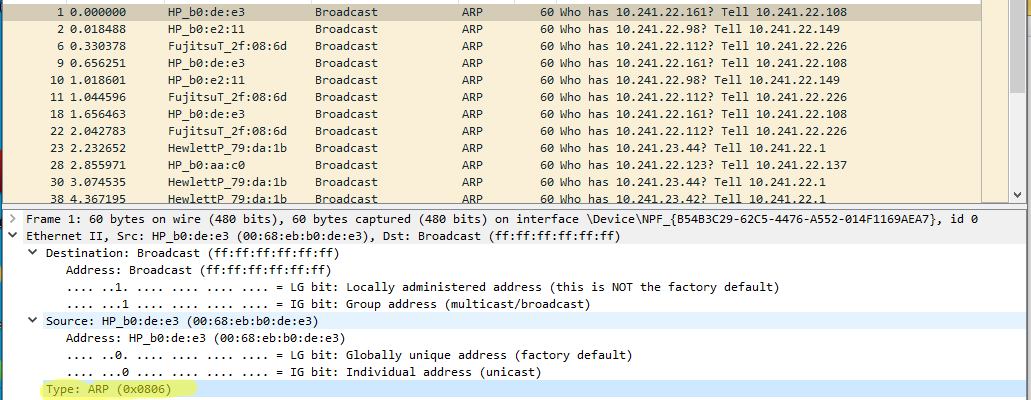
1. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?

My source addresses is 00:68:eb:b0:de:e3

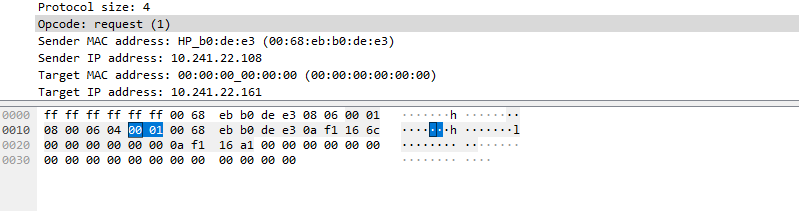
destination addresses is ff:ff:ff:ff:ff:ff:

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

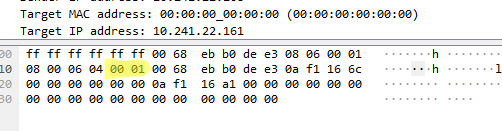
ARP 0x0806



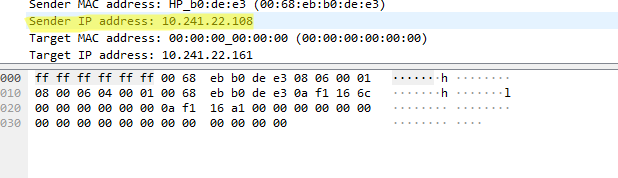
1. How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

There is 20 byte before it.  


1. What is the value of the opcode field?  
   x0001

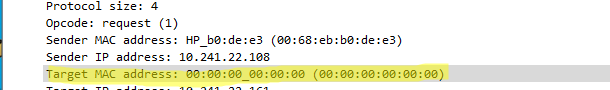


1. Does the ARP request message contain the IP address of the sender?

Yes, it does  


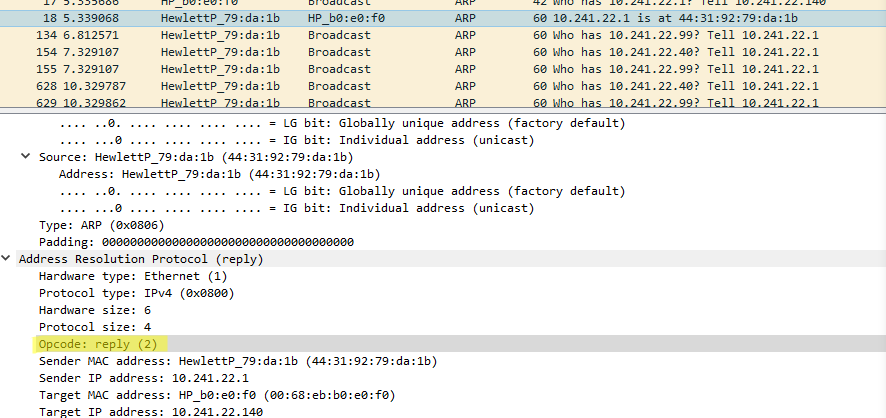
1. Where in the ARP request does the “question” appear – the Ethernet address of the machine whose corresponding IP address is being queried?

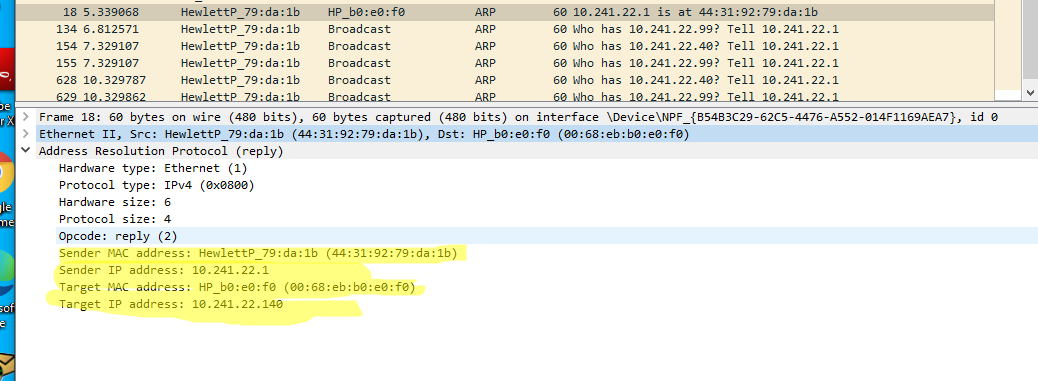
It use MAC address of the target



1. For the ARP reply message what is the value of the opcode field?

Replay (2)



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

