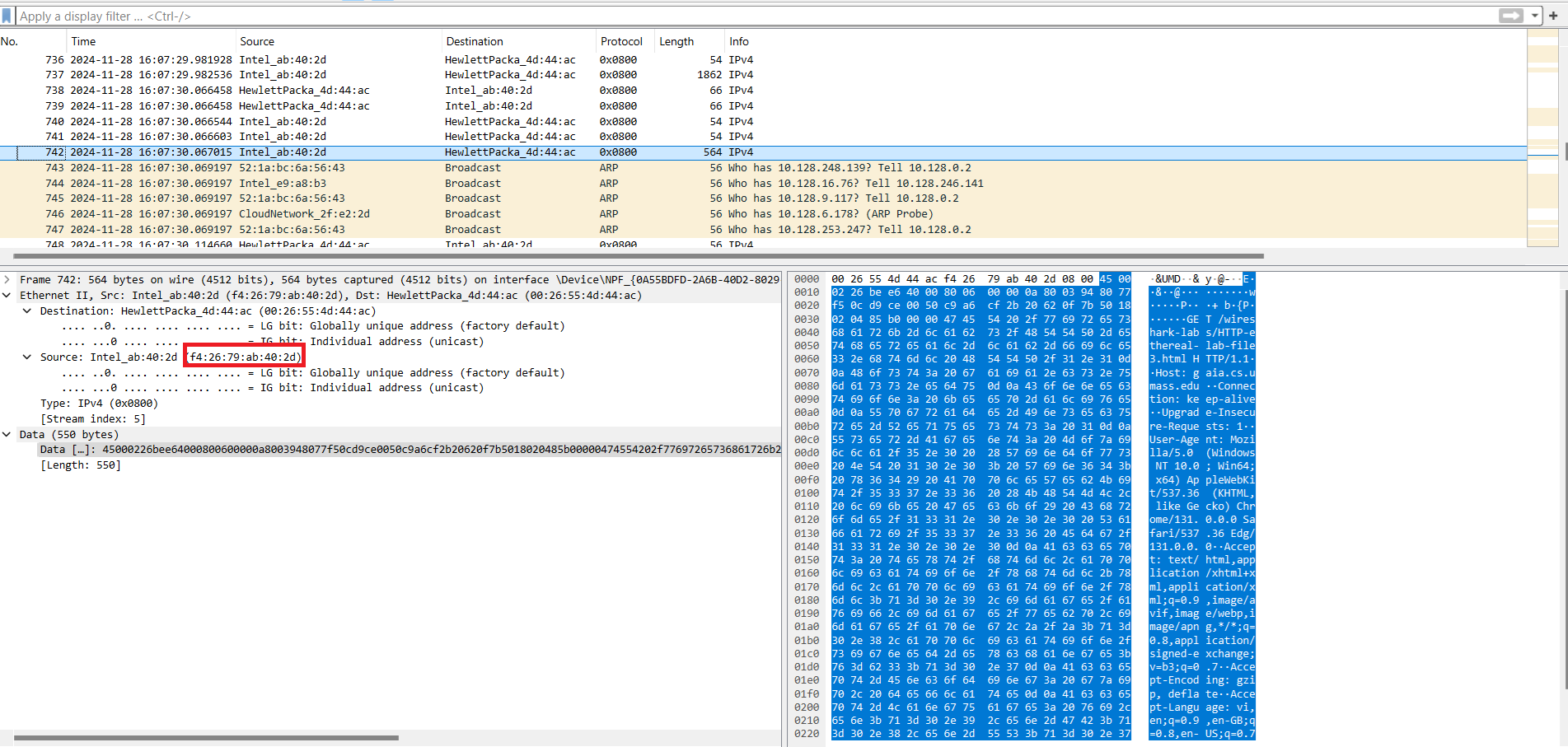
2252720\_Võ Trúc Sơn\_lab7\_Ethernet&ARP

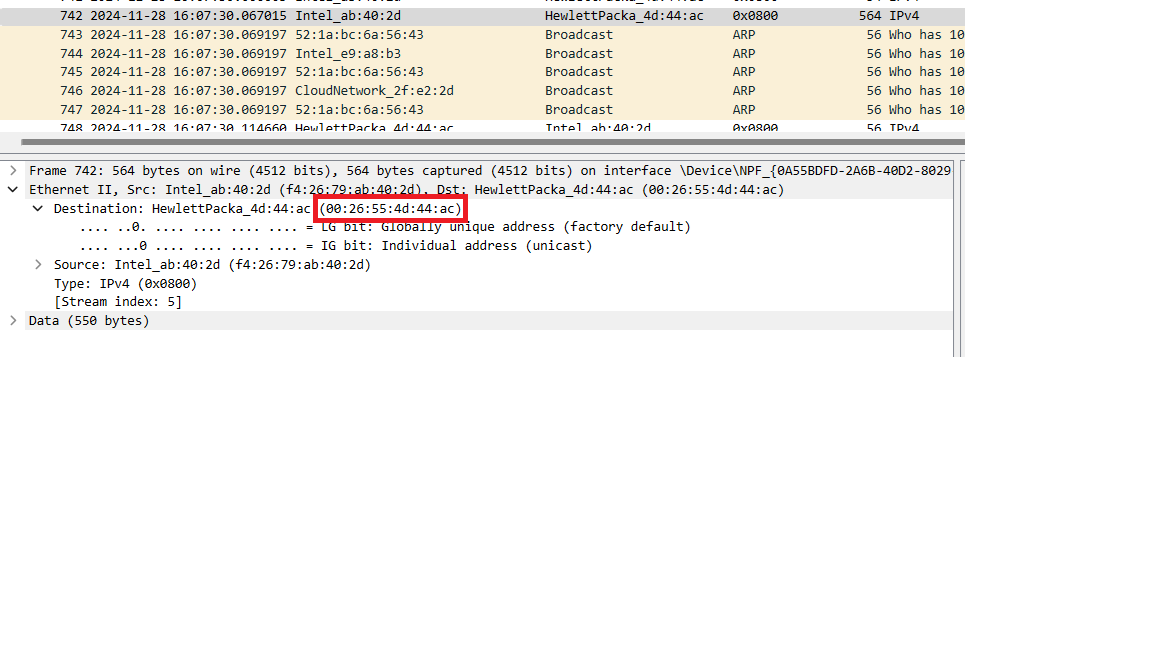
*1. What is the 48-bit Ethernet address of your computer?*

Answer: The source address is as picture follow

**

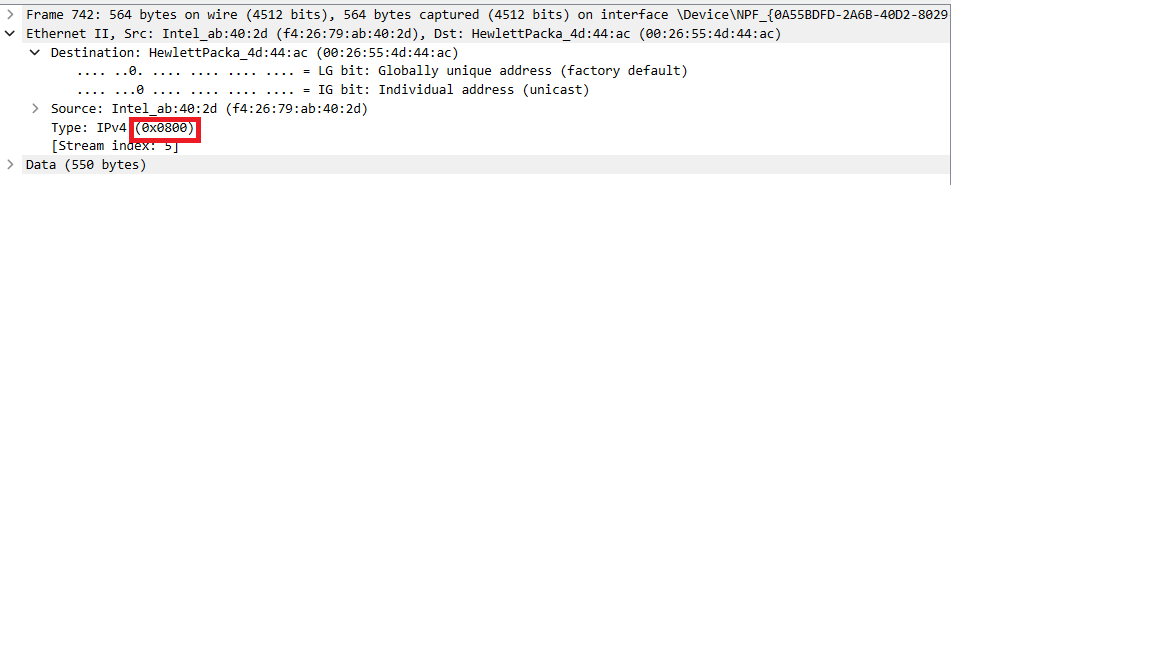
*2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is no). What device has this as its Ethernet address? [Note: this is an important question, and one that students sometimes get wrong. Re-read pages 468-469 in the text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

Answer: The destination address is in the picture as follow. This is not the address of *gaia.cs.umass.edu*. We can see in the picture that the Ethernet address is of “HewlettPacka\_4d:44:ac”.

**

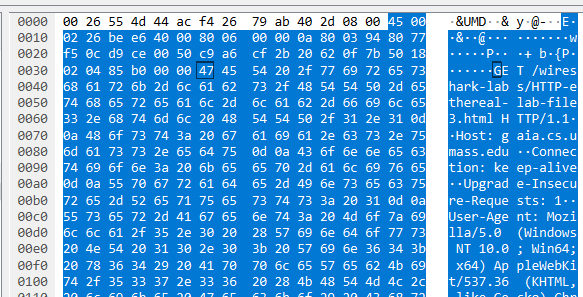
*3. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?*

Answer: The hexadecimal value is 0x0800. It is corresponded to the IPv4 protocol.

**

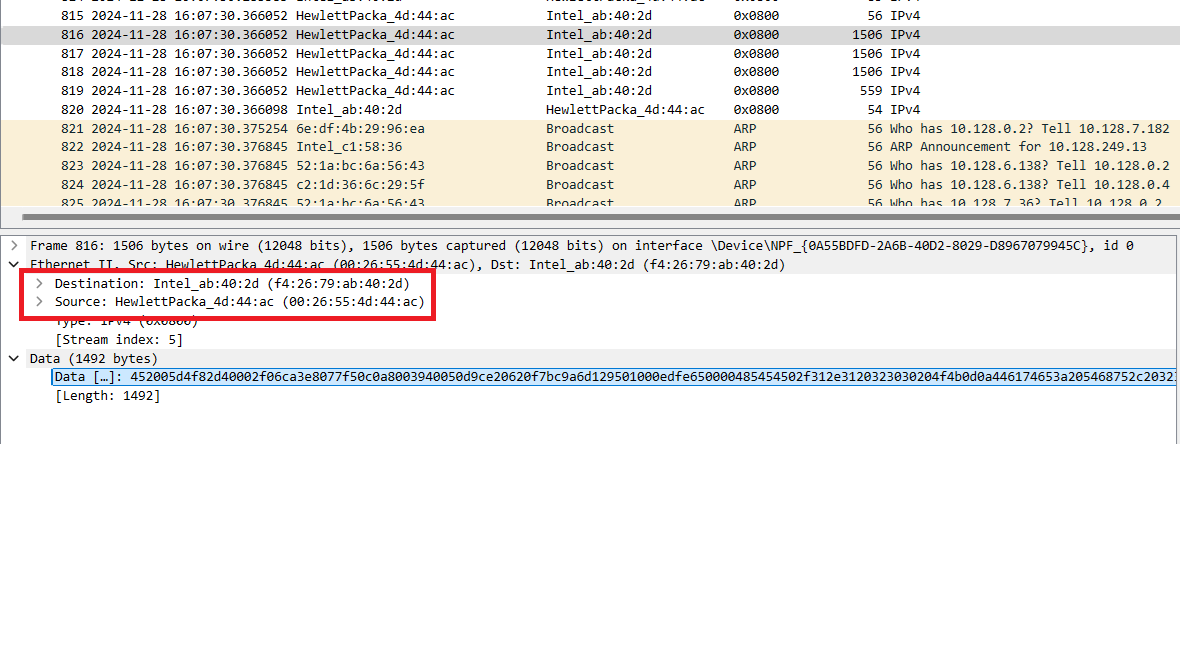
*4. How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame?*

Answer: Calculation: 54 bytes

**

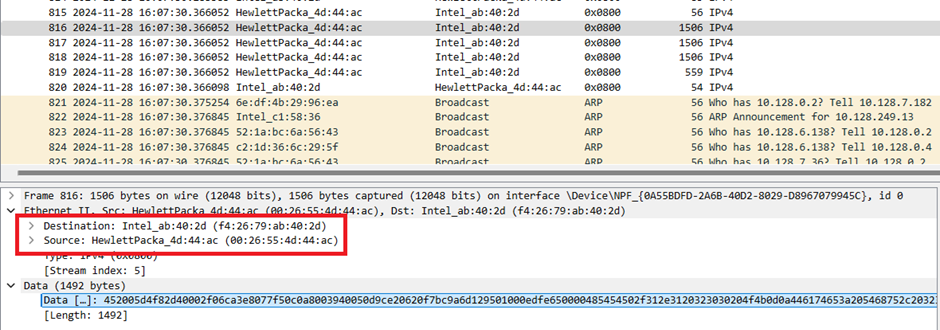
*5. What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is no). What device has this as its Ethernet address?*

Answer: You can see the source address as follow. It probably not the address of my computer or *gaia.cs.umass.edu* but it is from HewlettPacka\_4d:44:ac

**

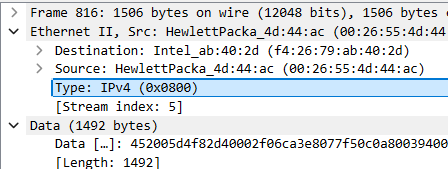
*6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?*

Answer: You can see the destination address as follow. This is the Ethernet address of my computer.

**

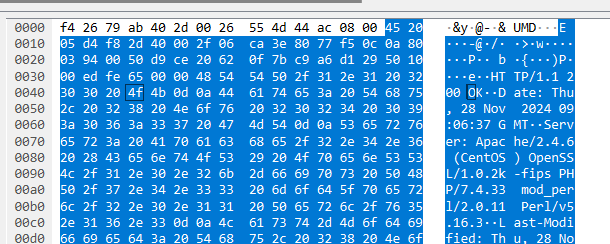
*7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?*

Answer: This is the hexadecimal value, correspond to Ipv4.

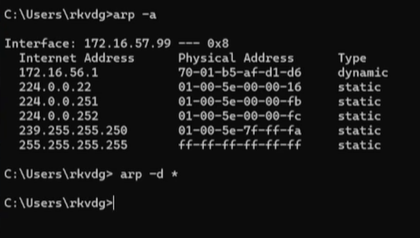
**

*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?*

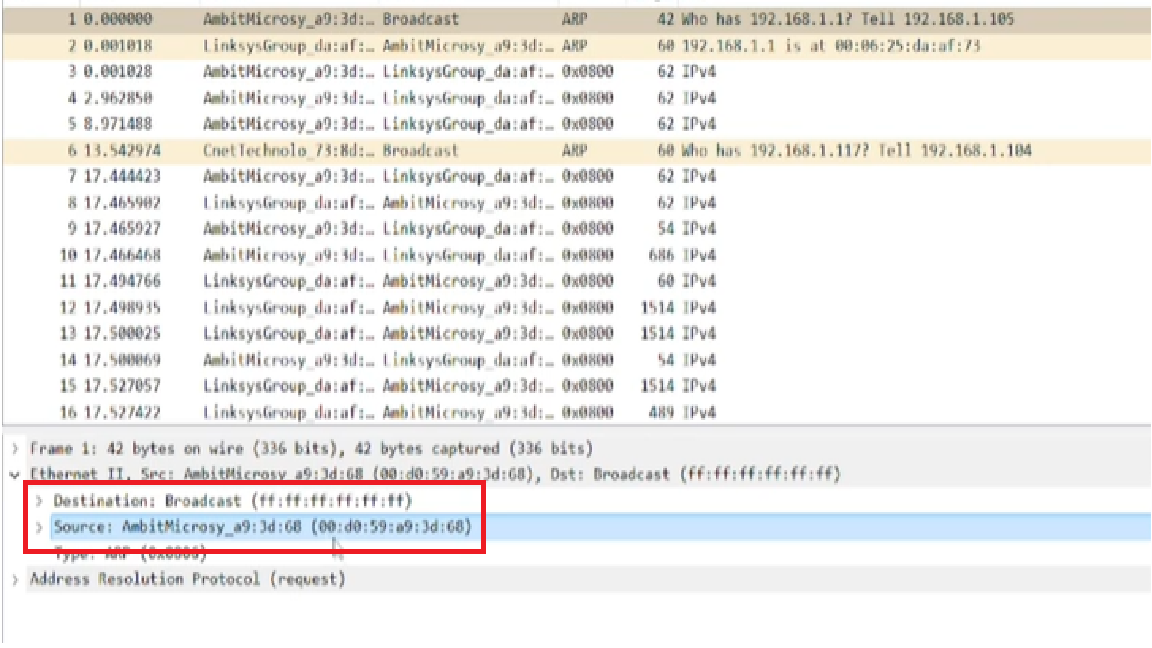
Answer: it’s 54 bytes.

**

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

**

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

**

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

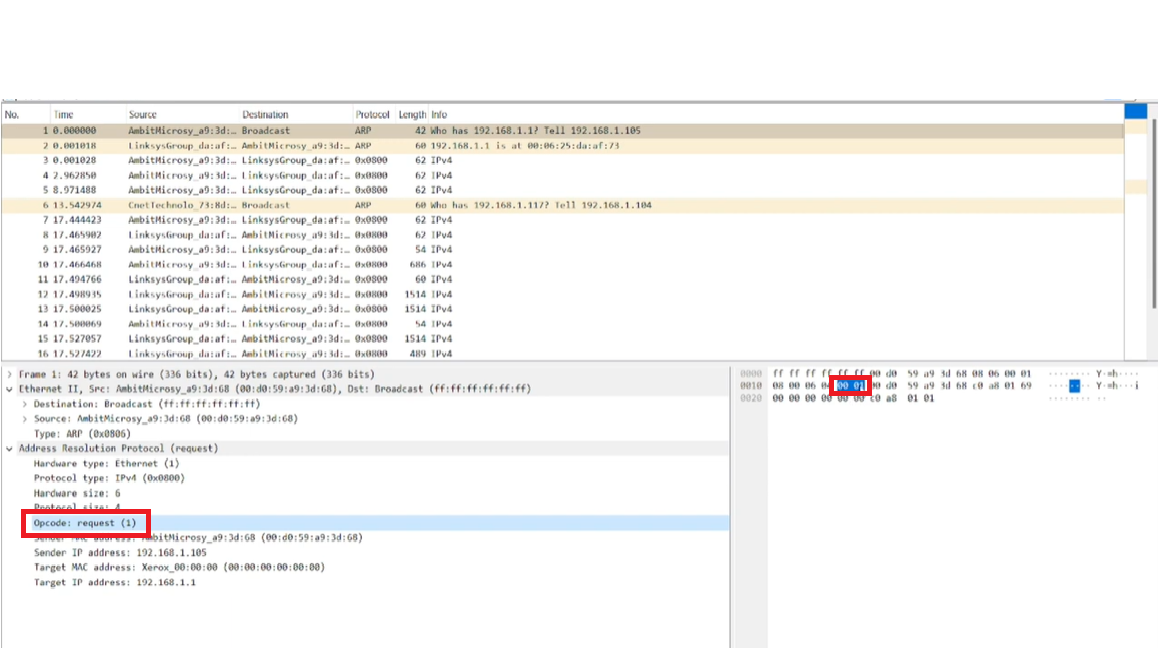
**

*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.*

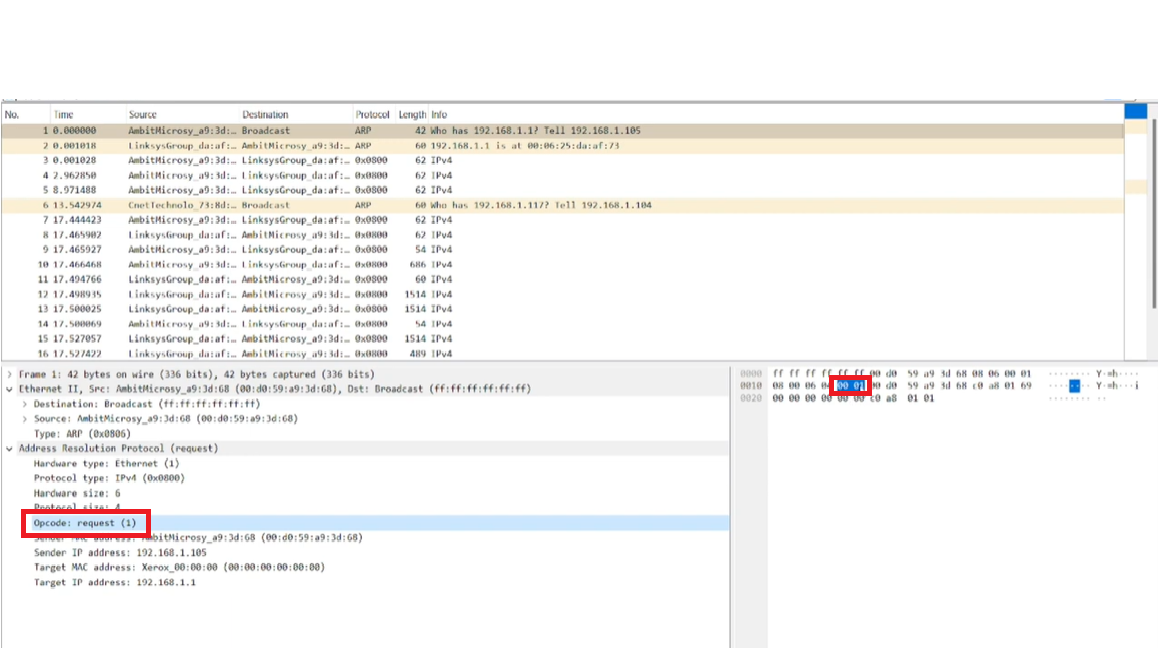
*a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?*

Answer: it is 20 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?*

Answer: That is 00 01. It is a request

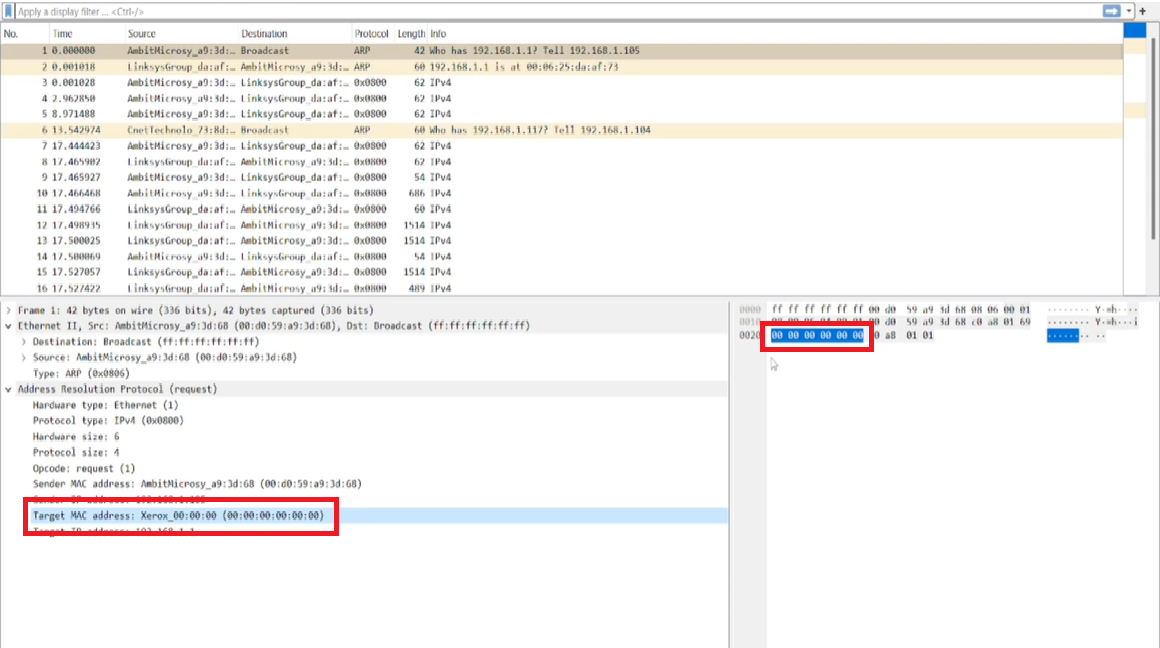


*c) Does the ARP message contain the IP address of the sender?*

Answer: Yes, you can see the source which is my computer IP address.

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

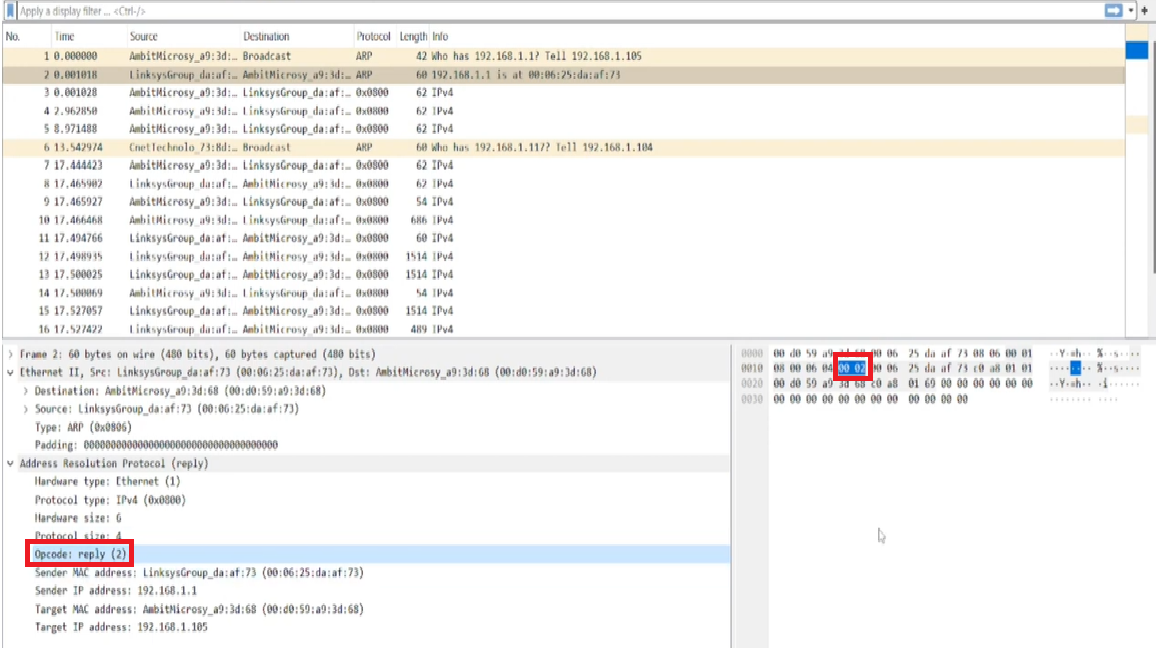
Answer: We can conclude that ARP packet structure conclude many fields and the ARP hardware address is specifically where the ARP request indicates the ethernet address that correspond to the IP address being queried. This field is basically of 6 bytes and is used to specify the hardware address of the target machine for which the ARP request is seeking to resolve the corresponding IP address.

**

*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?*

Answer: it is 20 bytes

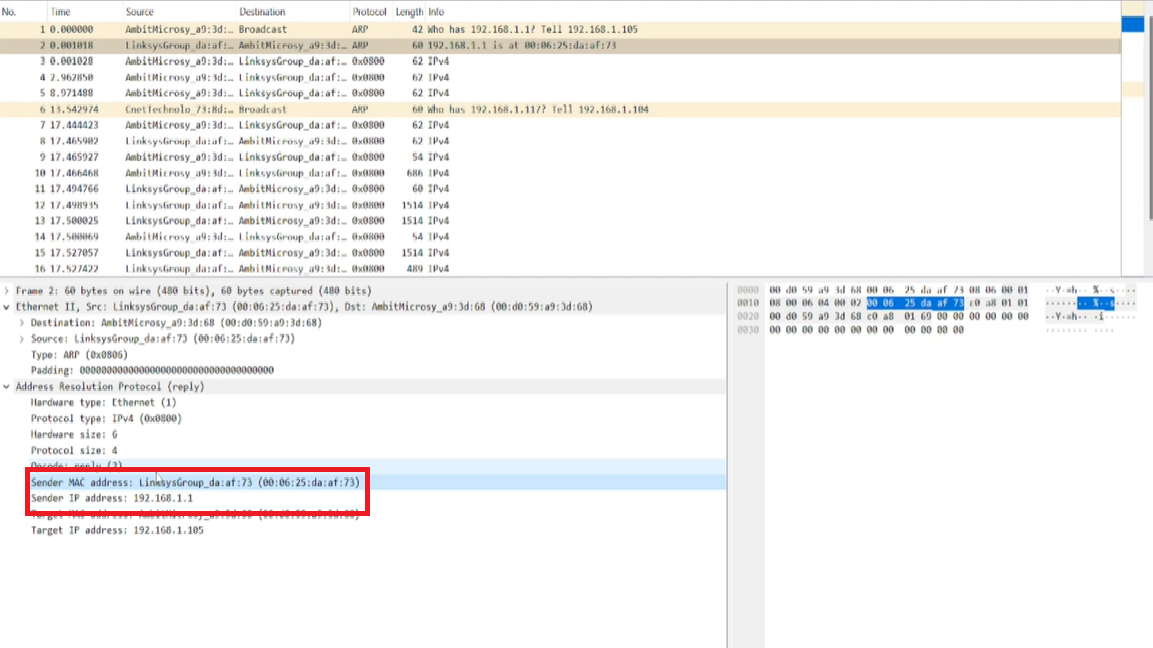
**

*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?*

Answer: The opcode value is 00 02.

*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?*

Answer: the answer is as follow.



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

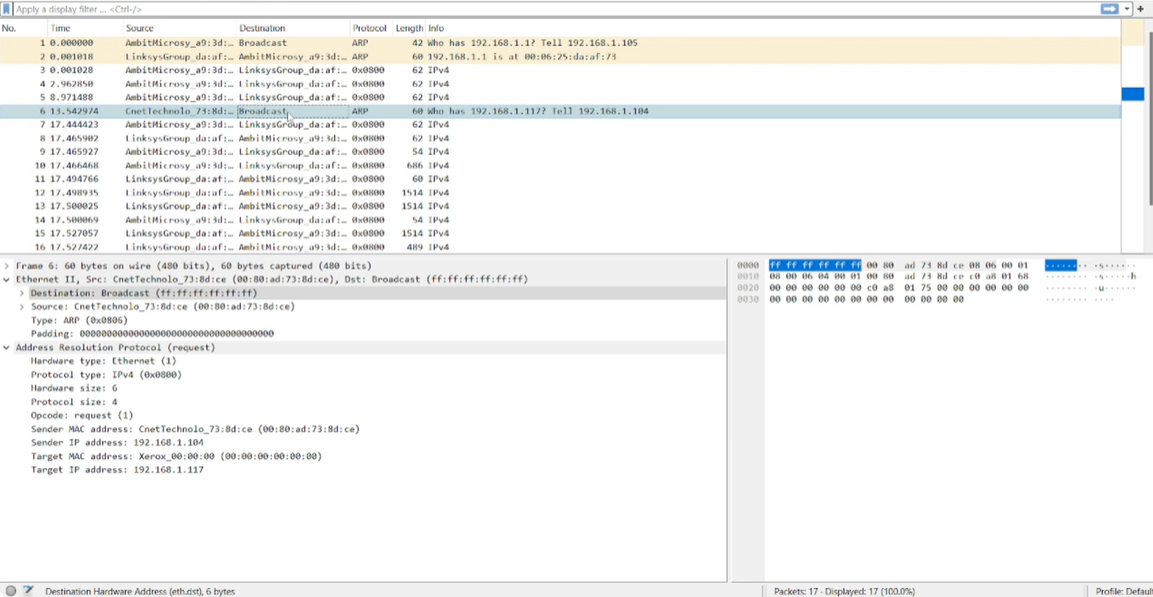
Answer: the answer is as follow.

**

*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?*

Answer: the destination is broadcast so it don’t know who has the IP to reply



2252720\_Võ Trúc Sơn\_lab8

1. What are the SSIDs of the two access points that are issuing most of the beacon  
   frames in this trace?

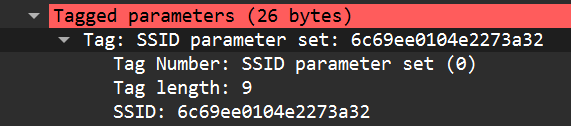
* Beacon frames are the special files that contain the information of the appearance of the Internet such as SSID, security and other things
* SSIDs is the name of the Internet
* From:





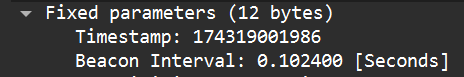
* From:



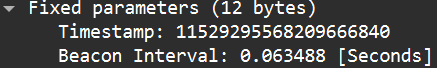


1. What are the intervals of time between the transmissions of the beacon frames the  
   *linksys\_ses\_24086* access point? From the *30 Munroe St*. access point? (Hint: this  
   interval of time is contained in the beacon frame itself)

* From 30 Munroe St:



* From linksys\_ses\_24086:



1. What (in hexadecimal notation) is the source MAC address on the beacon frame  
   from *30 Munroe St*? Recall from Figure 7.13 in the text that the source,  
   destination, and BSS are three addresses used in an 802.11 frame. For a detailed  
   discussion of the 802.11 frame structure, see section 7 in the IEEE 802.11  
   standards document (cited above).

* MAC address is below:



1. What (in hexadecimal notation) is the destination MAC address on the beacon  
   frame from *30 Munroe St*??

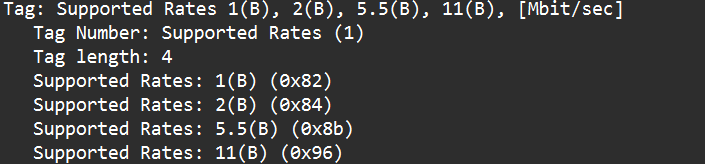


1. What (in hexadecimal notation) is the MAC BSS id on the beacon frame from *30  
   Munroe St*?

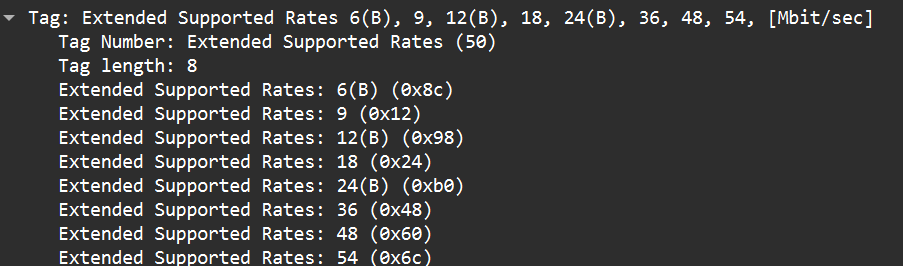


1. The beacon frames from the *30 Munroe St* access point advertise that the access  
   point can support four data rates and eight additional “extended supported rates.”  
   What are these rates?

* “Support rate”: usually is the standard rate that each AP supports



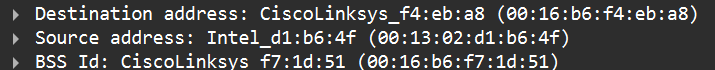
* “Extended supported rates”: is the higher rate that the AP can run if it is supported.



1. Find the 802.11 frame containing the SYN TCP segment for this first TCP session  
   (that downloads alice.txt). What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the wireless host (give  
   the hexadecimal representation of the MAC address for the host)? To the access  
   point? To the first-hop router? What is the IP address of the wireless host  
   sending this TCP segment? What is the destination IP address? Does this  
   destination IP address correspond to the host, access point, first-hop router, or  
   some other network-attached device? Explain



* Three 3 MAC addresses are:



* The MAC address of wireless host is Source address.
* The MAC address of access point is BSSID
* The MAC address of first-hop router is Destination address
* IP address of wireless host:



* Destination IP address: 128.119.245.12
* This destination IP address is involving to the host which contains the information of the text, it is not an address of other devices listed.

1. Find the 802.11 frame containing the SYNACK segment for this TCP session. What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the host? To the access point? To the first-hop router? Does the sender MAC address in the frame correspond to the IP address of the device that sent the TCP segment encapsulated within this datagram? (Hint: review Figure 6.19 in the text if you are unsure of how to answer this question, or the corresponding part of the previous question. It’s particularly important that you understand this).



* Three 3 MAC addresses are:



* The MAC address of wireless host is Source address.
* The MAC address of access point is BSSID
* The MAC address of first-hop router is Destination address
* IP address of wireless host:



* Destination IP address: 192.168.1.109
* No, if there is the AP taking the role of intermediate the MAC address will be of the AP, but the destination IP address is from the host

1. What two actions are taken (i.e., frames are sent) by the host in the trace just after  
   *t=49*, to end the association with the *30 Munroe St* AP that was initially in place  
   when trace collection began? (Hint: one is an IP-layer action, and one is an  
   802.11-layer action). Looking at the 802.11 specification, is there another frame  
   that you might have expected to see, but don’t see here?

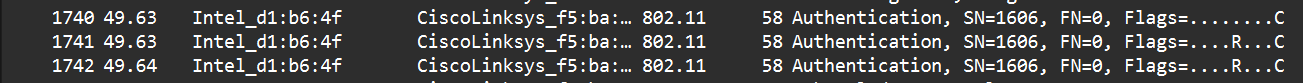
* These two frames are:

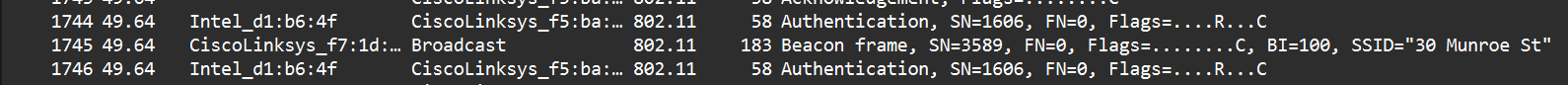




* I am waiting for the frame disassociation, but in this case because the host or the AP chooses the way that disconnects directly and fast, so they choose the frame “de-authentication” instead of “disassociation”

1. Examine the trace file and look for AUTHENICATION frames sent from the host to an AP and vice versa. How many AUTHENTICATION messages are sent from the wireless host to the linksys\_ses\_24086 AP (which has a MAC address of Cisco\_Li\_f5:ba:bb) starting at around t=49 ?







* There are 6

1. Does the host want the authentication to require a key or be open?



* It requires open

1. Do you see a reply AUTHENTICATION from the linksys\_ses\_24086 AP in the trace?

* No, I do not

1. Now let’s consider what happens as the host gives up trying to associate with the  
   *linksys\_ses\_24086* AP and now tries to associate with the *30 Munroe St* AP. Look  
   for AUTHENICATION frames sent from the host to and AP and vice versa. At  
   what times are there an AUTHENTICATION frame from the host to the *30  
   Munroe St.* AP, and when is there a reply AUTHENTICATION sent from that AP  
   to the host in reply? (Note that you can use the filter expression “wlan.fc.subtype  
   == 11and wlan.fc.type == 0 and wlan.addr == IntelCor\_d1:b6:4f” to display only  
   the AUTHENTICATION frames in this trace for this wireless host.)

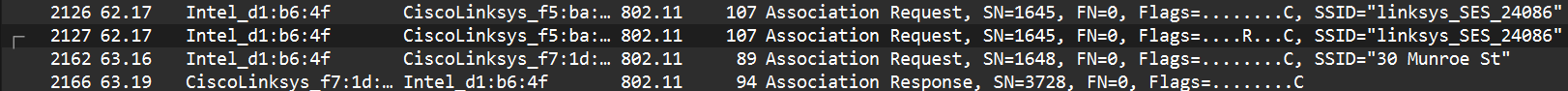
* Time sending AUTHENTICATION: 49.64



* Time receiving AUTHENTICATION: 63.16



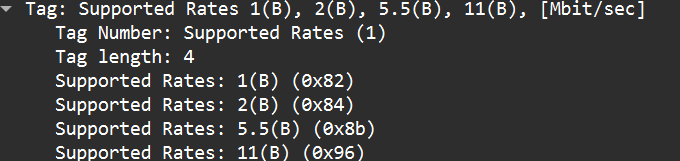
1. An ASSOCIATE REQUEST from host to AP, and a corresponding ASSOCIATE RESPONSE frame from AP to host are used for the host to associated with an AP. At what time is there an ASSOCIATE REQUEST from host to the 30 Munroe St AP? When is the corresponding ASSOCIATE REPLY sent? (Note that you can use the filter expression “wlan.fc.subtype < 2 and wlan.fc.type == 0 and wlan.addr == IntelCor\_d1:b6:4f” to display only the ASSOCIATE REQUEST and ASSOCIATE RESPONSE frames for this trace.)



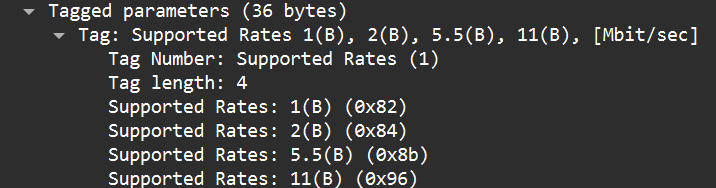
* Time sending ASSOCIATE REQUEST: 62.17
* Time receiving ASSOCIATE REPLY: 63.19

1. What transmission rates is the host willing to use? The AP? To answer this  
   question, you will need to look into the parameters fields of the 802.11 wireless  
   LAN management frame

* From the host:

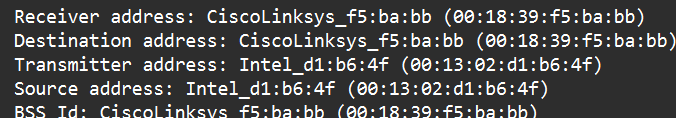


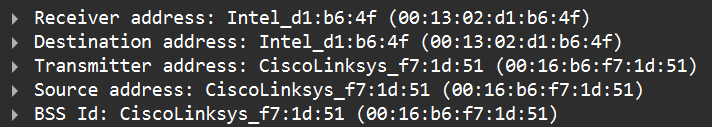
* The AP:



1. What are the sender, receiver and BSS ID MAC addresses in these frames? What  
   is the purpose of these two types of frames? (To answer this last question, you’ll  
   need to dig into the online references cited earlier in this lab).

* Sender, Receiver and BSS ID MAC addresses:





* The associative frame used to create the connection.
* Beacon frame used to announce the availability of the Internet and information for host to decide to connect