NETWORK LAB

LAB ASSIGNMENT for Week # 3

Usirikayala Likhith

20223295, D2

IP

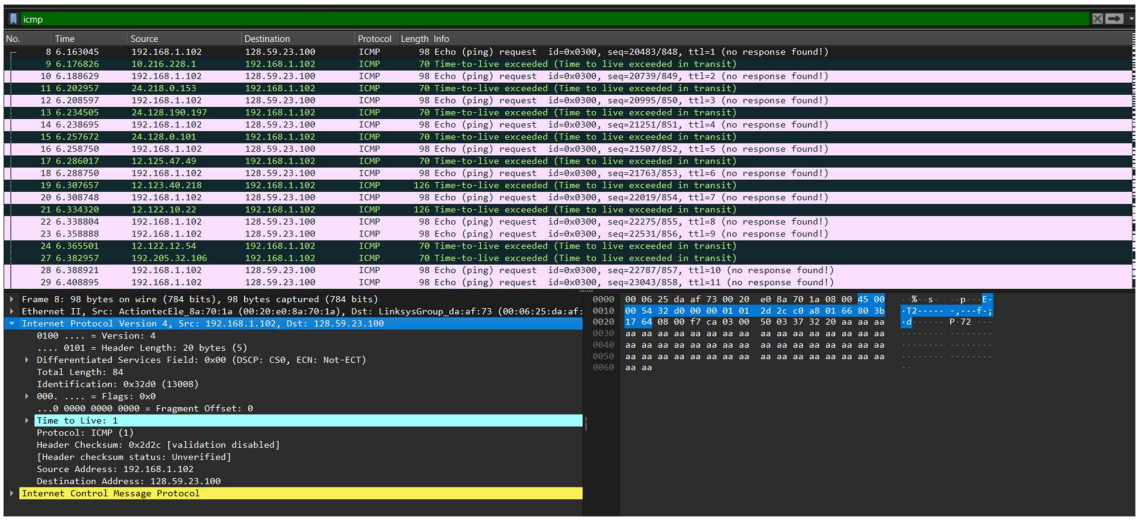
I. Simple IP Trace

Note: Answer the following questions using the ip-ethereal-trace-1 packet trace to answer the questions

below

1. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?

ANS:



The ip address of my computer is 192.168.1.102

2. Within the IP packet header, what is the value in the upper layer protocol field?

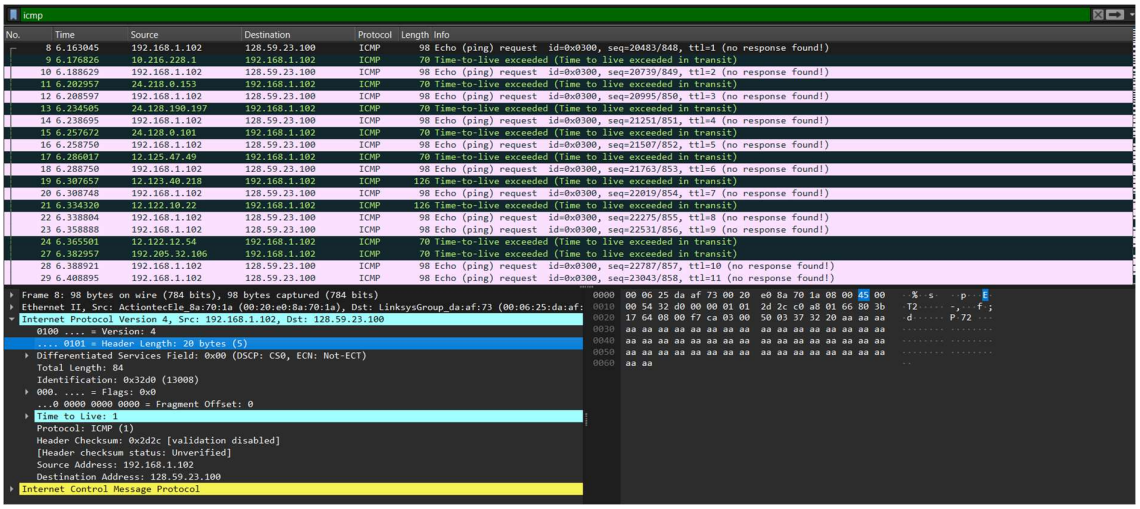
The Upper Layer protocol field is ICMP.

3. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.

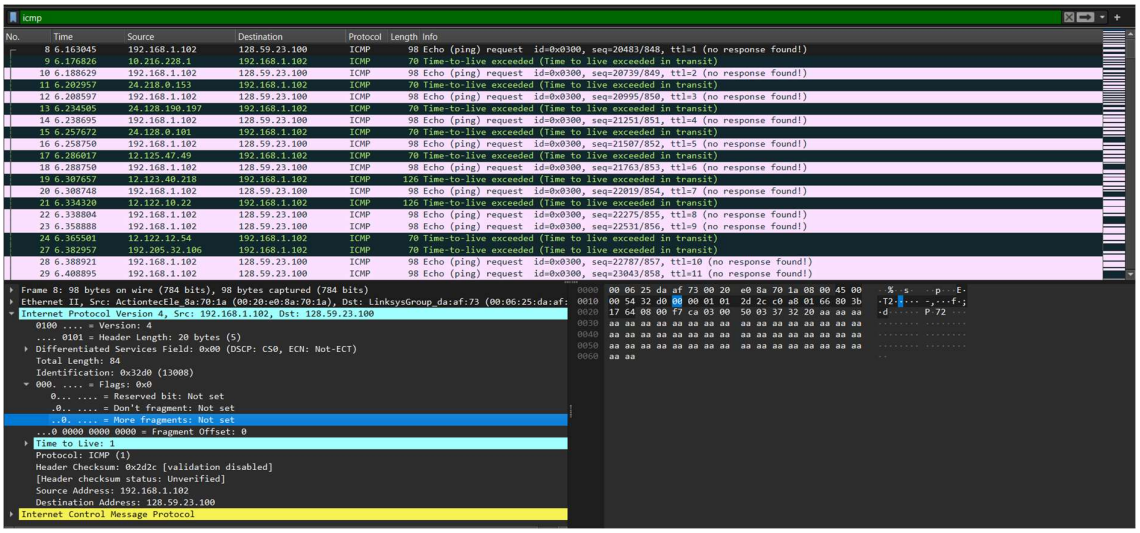
There are 20 bytes in the IP header. The packet was sending 84 bytes of data. So remaining 64 bytes are payload bytes.

Payload bytes = Total bytes-IP header bytes.

Payload bytes = 84-20 = 64 bytes.



4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.



As of now this ip datagram hasn't been fragmented as the more fragments bit in the flag is not set.

Next, sort the traced packets according to IP source address by clicking on the Source column header; a small downward pointing arrow should appear next to the word Source. If the arrow points up, click on the Source column header again. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol portion in the details of selected packet header window. In the listing of captured packets window, you should see all of the subsequent ICMP messages (perhaps with additional interspersed packets sent by other protocols running on your computer) below this first ICMP. Use the down arrow to move through the ICMP messages sent by your computer.

5. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?

The Identification Number and the header Check sum are always changing from one datagram to the next within the series of ICMP messages.

6. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?

Fields that stay constant:

Version

Length of header

Source IP

Destination IP

Upper layer protocol

Fields that must change:

The header checksum

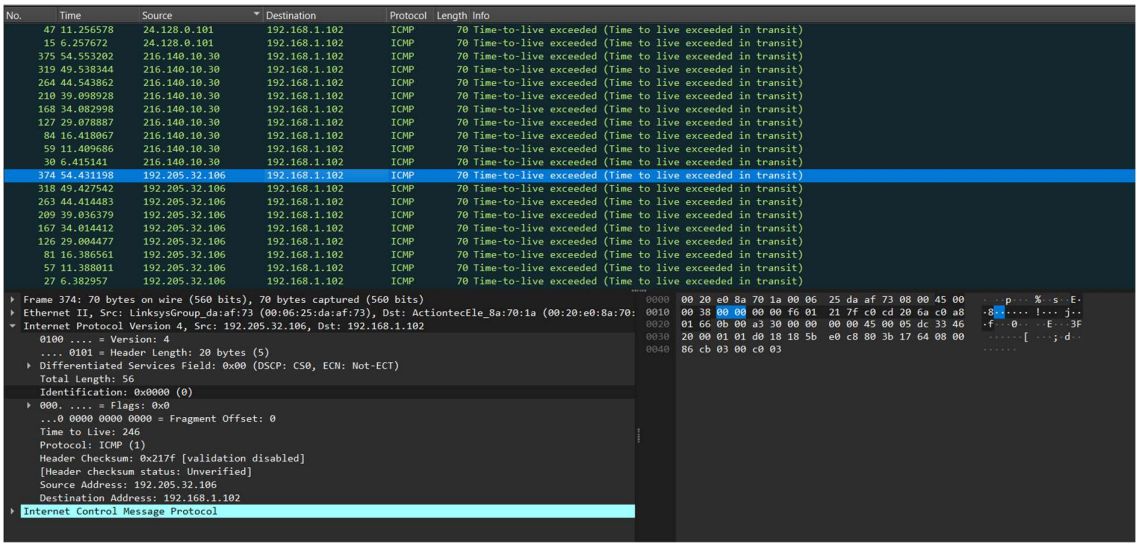
Identification

7. Describe the pattern you see in the values in the Identification field of the IP datagram

The pattern in the identification field is that the field increases by one in each packet.

Next (with the packets still sorted by source address) find the series of ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router.

8. What is the value in the Identification field and the TTL field?

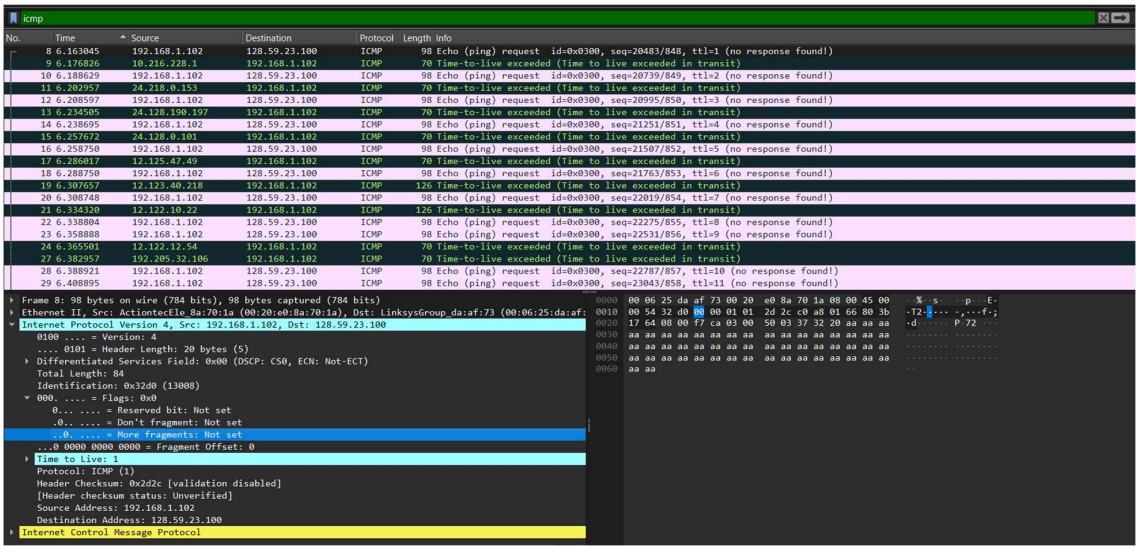


The TTL field value is 246 and the Identification field value is 0X0000(0).

II. Fragmentation

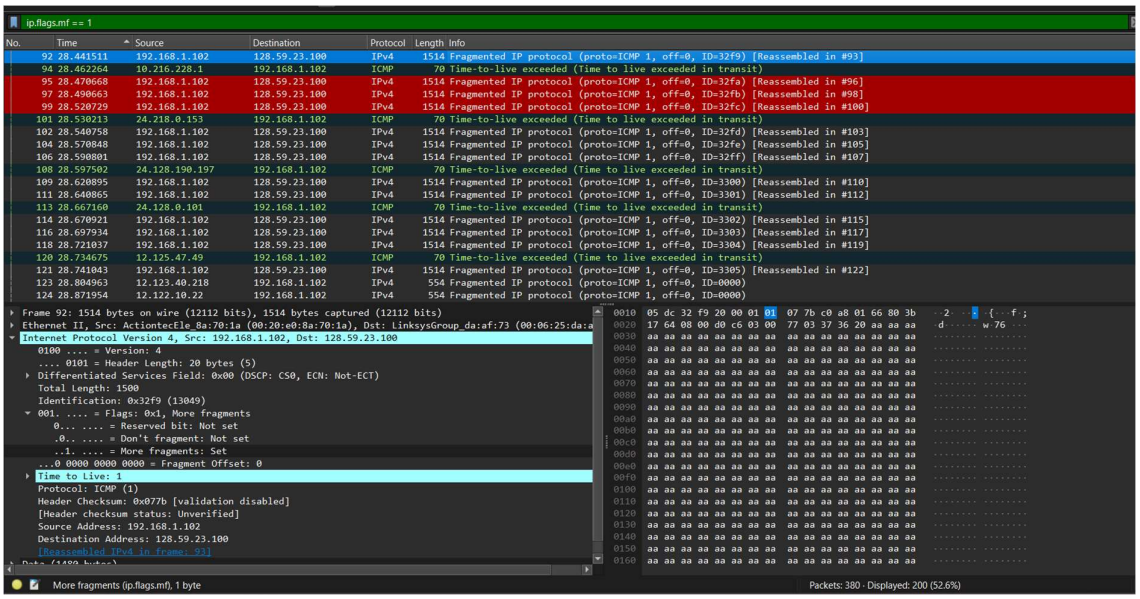
Sort the packet listing according to time again by clicking on the Time column.

9. Find the first ICMP Echo Request message that was sent by your computer. Has that message been fragmented across more than one IP datagram?



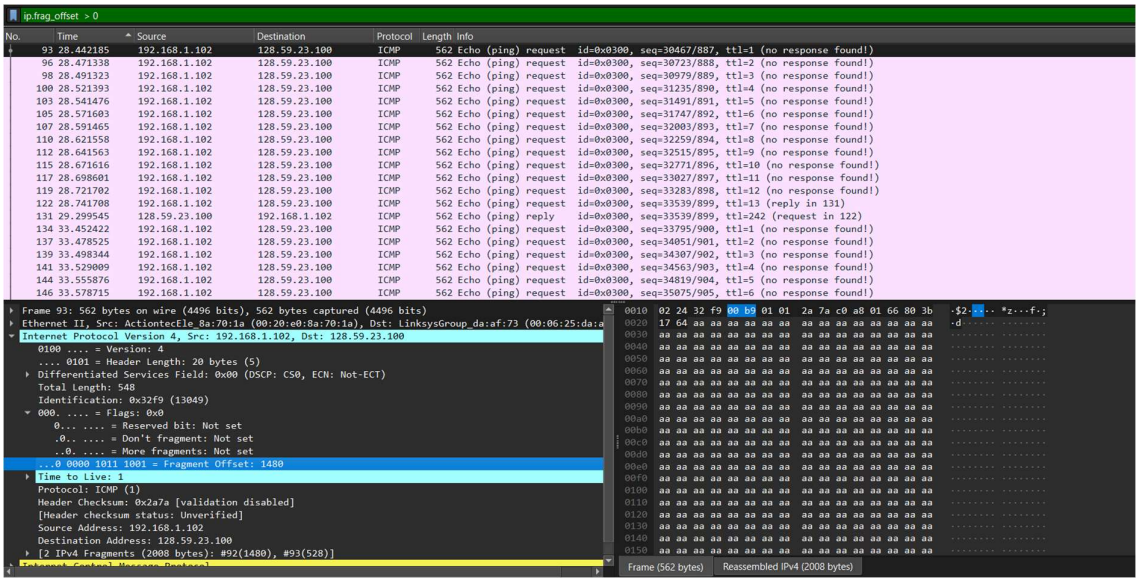
No The packet hasn't been fragmented because the more fragments bit is not set and fragment number is 0.

10. Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?



The more fragments bit is set so this packet is fragmented. The fragment offset is 0 so this the first packet of this fragment. The length of this IP datagram is 1514.

11. Print out the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are the more fragments? How can you tell?



The fragment offset is not 0. It indicates that this packet is not first fragment. There are no more fragments for this packet because the more fragment bit is not set.

12. What fields change in the IP header between the first and second fragment?

Length

Flags Set

Fragment offset

header checksum

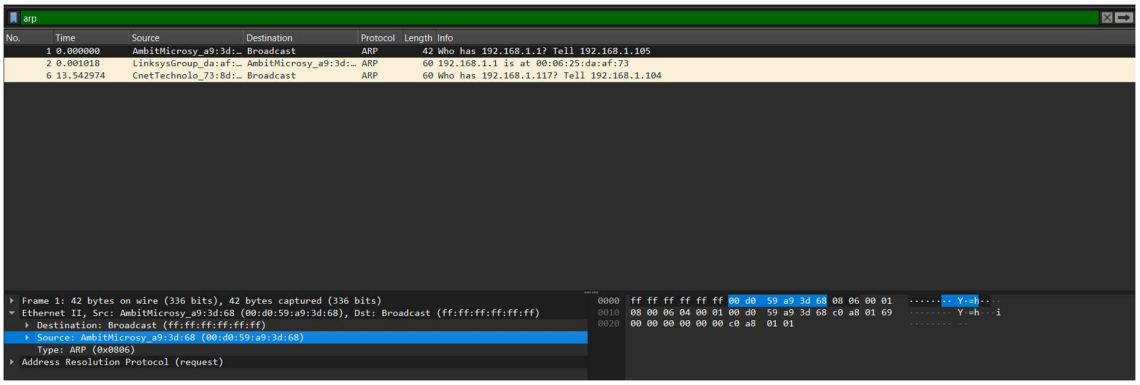
ARP

I. Capturing and analysing Ethernet frames

Note: Answer the following questions using the ethernet-ethereal-trace-1 packet trace to answer the

questions below

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

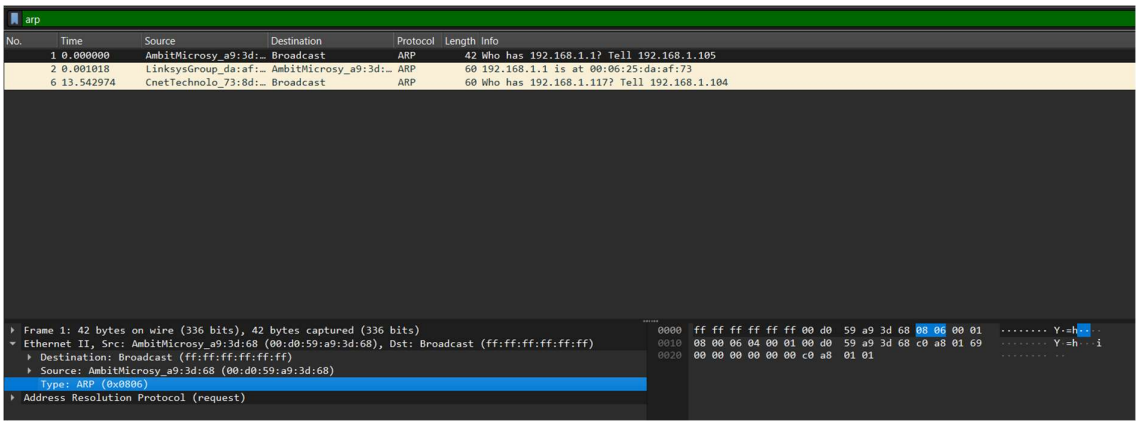


The 48 bit Ethernet address of my computer is 00:d0:59:a9:3d:68.

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.]

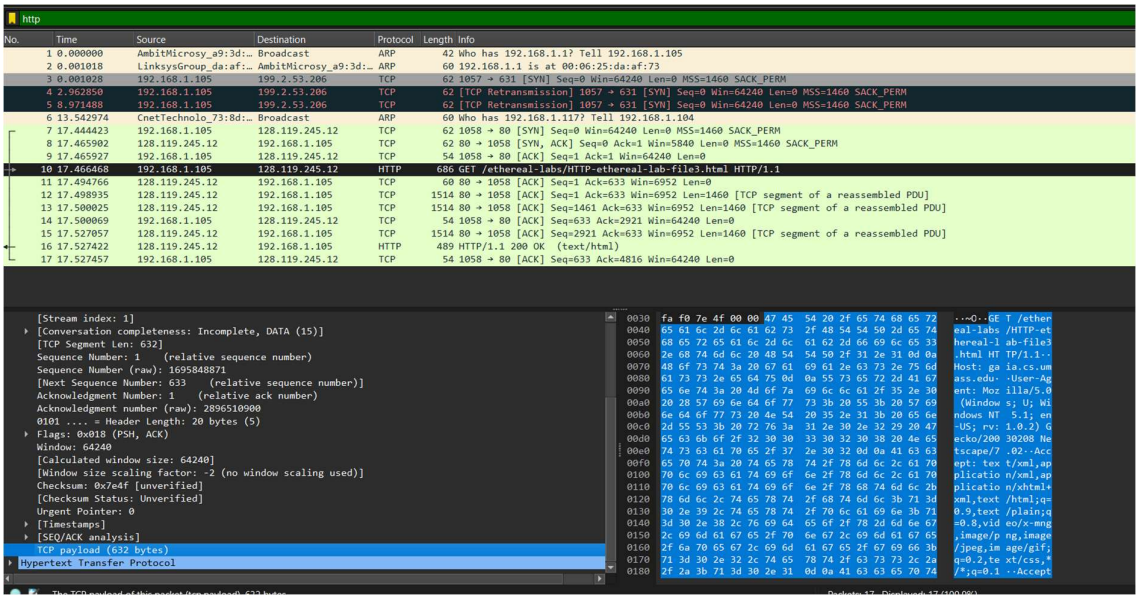
The destination address in the Ethernet frame is ff:ff:ff:ff:ff:ff. No this is not the giai.cs.umass.edu ethernet address. Broadcast MAC address.

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



0X0806 is the hexadecimal value and this correspond to ARP.

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



686 – 632 = 54 bytes.

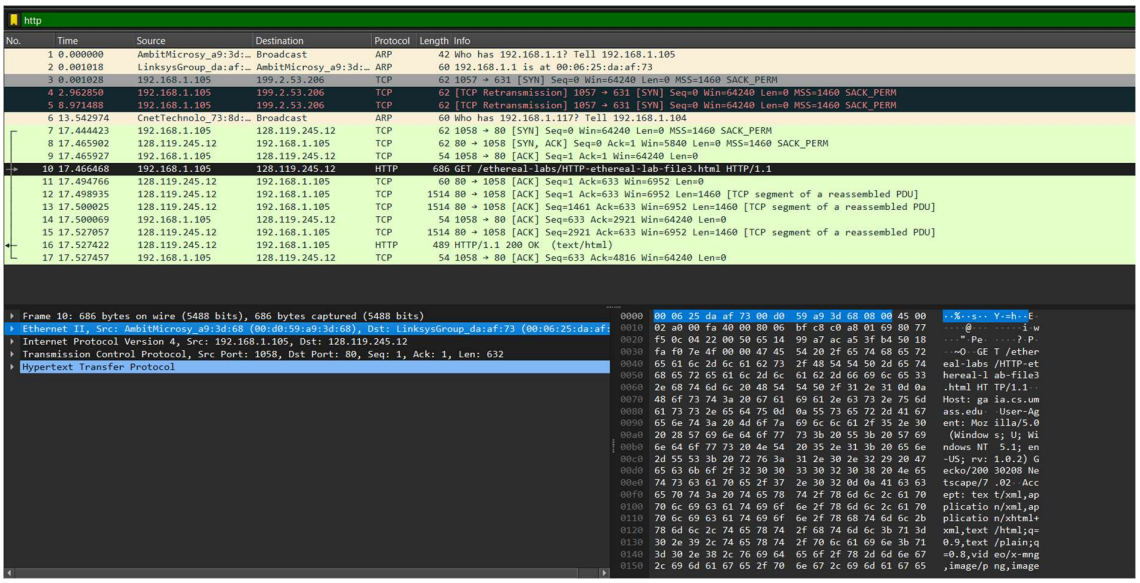
Next, answer the following questions, based on the contents of the Ethernet frame containing the first byte of the HTTP response message.

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 Ethernet Source address is 00:d0:59:a9:3d:68.

No.

Ambit Micro Systems.



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

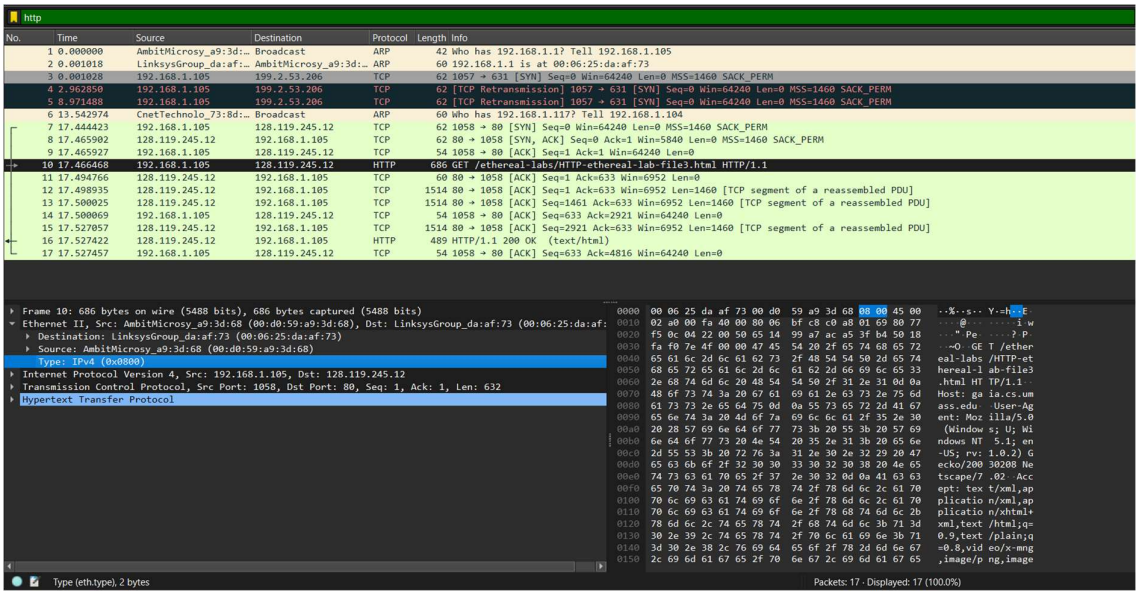
00:06:25:da:af:73.

NO

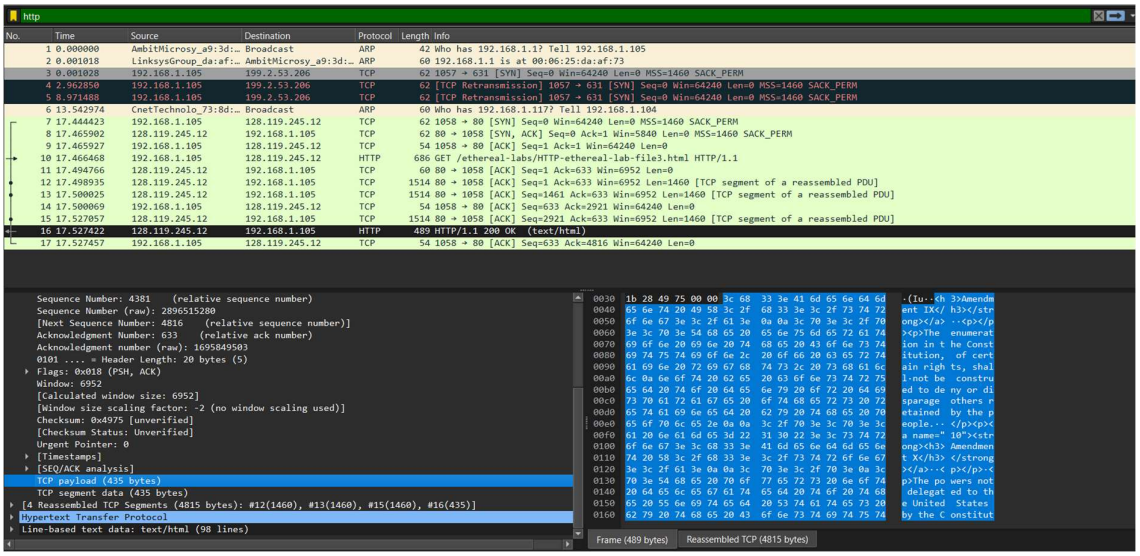
7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

0X0800

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?



489 -435 = 54 bytes.

II. The Address Resolution Protocol

The Windows arp command with no arguments will display the contents of the ARP cache on your computer. Run the arp command.

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

Internet Address: The IP address of the device in the ARP cache.

Physical Address: The MAC address corresponding to the IP address.

Type: The type of ARP entry. dynamic means the entry was learned dynamically through ARP requests. static means it was manually configured and will not change

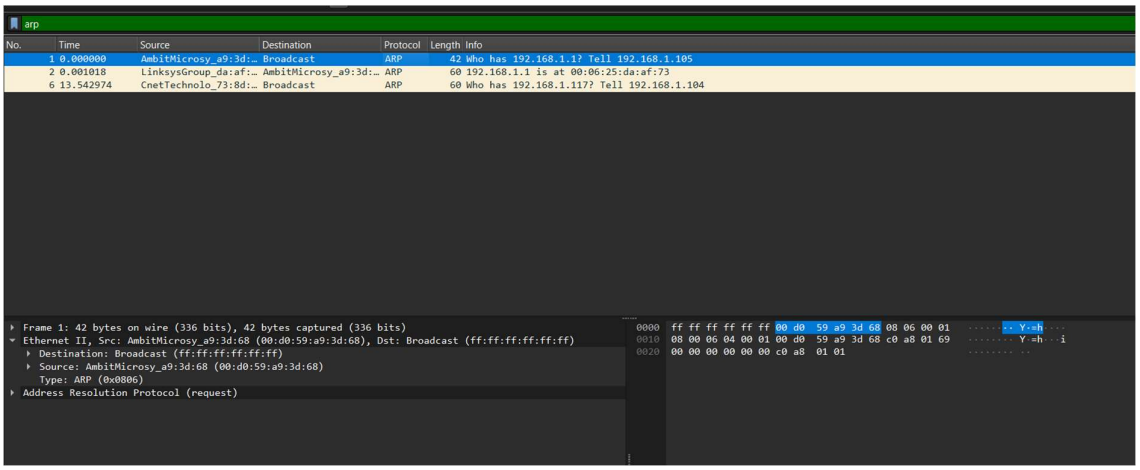
```
C:\Users\91934>arp -a

Interface: 192.168.56.1 --- 0xf
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 172.29.45.68 --- 0x14
  Internet Address      Physical Address      Type
  172.29.32.1           00-1b-90-95-b0-00     dynamic
  172.29.63.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

.

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



Source : 00:d0:59:a9:3d:68.

Destination : ff:ff:ff:ff:ff:ff

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

0X0806. This Corresponds to ARP.

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?

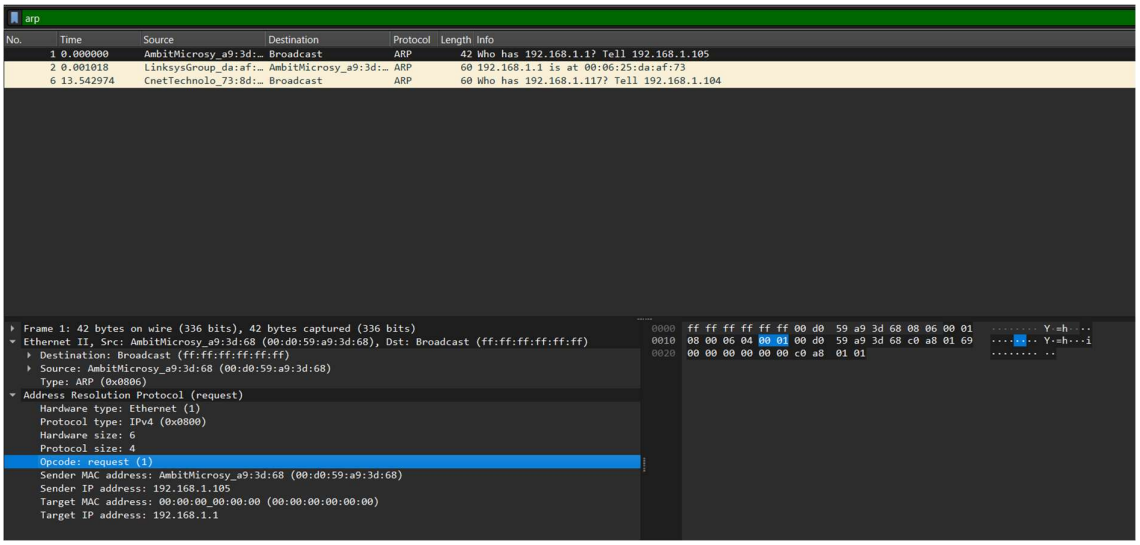
20 bytes.

6 for each source address and destination address and 2 for protocol type and 6 for arp header.

A total of 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?

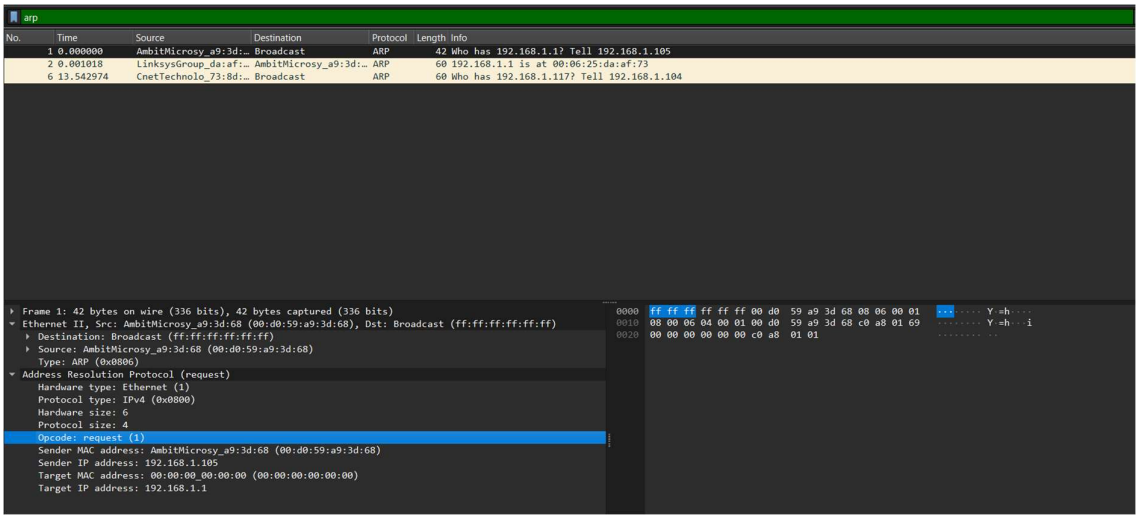
The value of opcode request is 1.



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

Yes it 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?



In the info we can see a query.

In the ARP section you can see the details about the query that has been asked.

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?

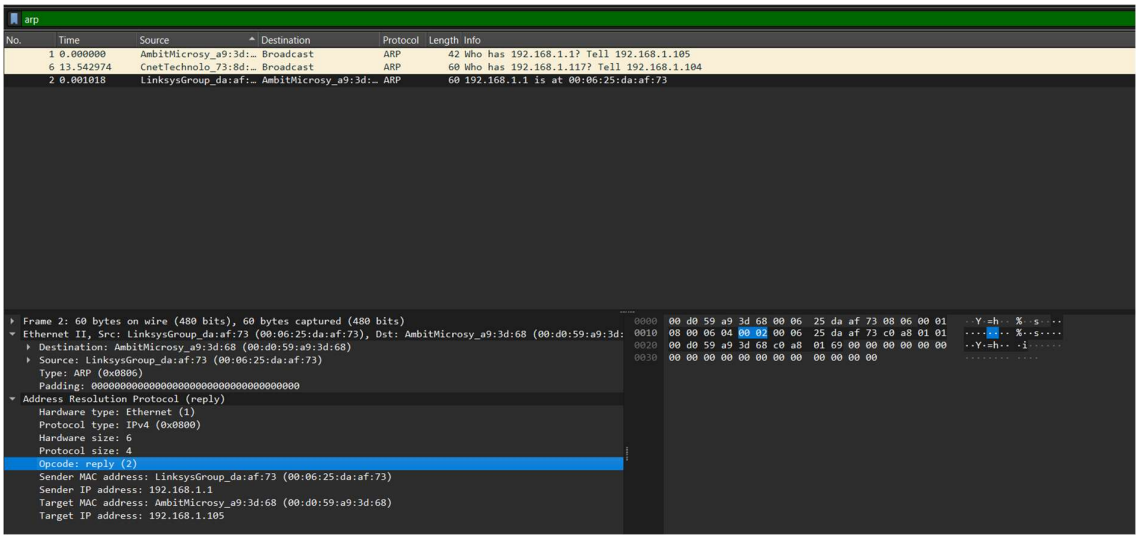
20 bytes.

6 for each source address and destination address and 2 for protocol type and 6 for arp header.

A total of 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?

0X002 for response



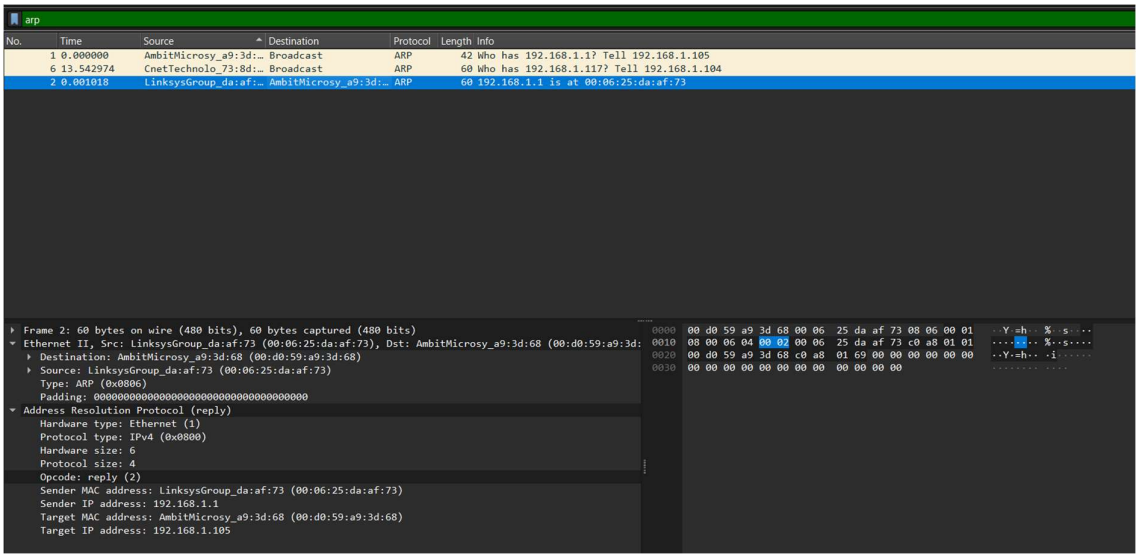
c. Where in the ARP message does the answer to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?

The answer appears on Sender MAC address field.

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

Source address: 00:06:25:da:af:73

Destination address: 00:30:59:a9:3d:68



15. 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 ARPrequested 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?

The ARP request might be targeting an IP address that does not exist on the local network. If no device is using the IP address in question, no ARP reply will be generated