z5147986
Lab7

Question marked with (*) must be submitted

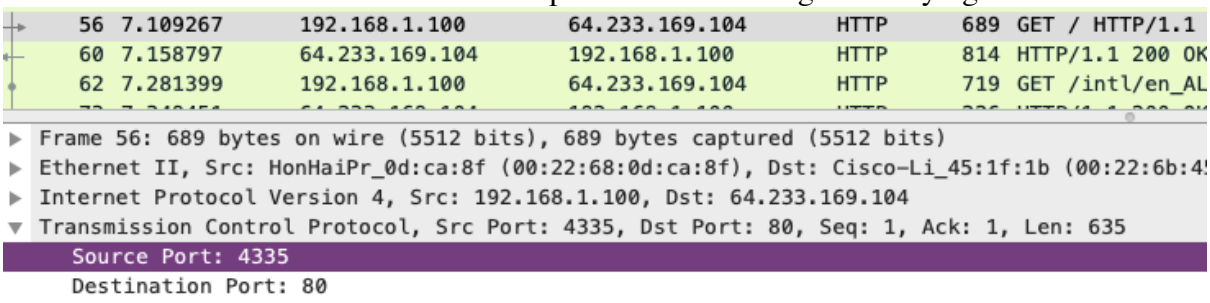
1.1

What is the IP address of the client?

192.168.1.100

***1.2**

Consider now the HTTP GET sent from the client to the Google server (whose IP address is IP address 64.233.169.104) at time 7.109267. What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET?

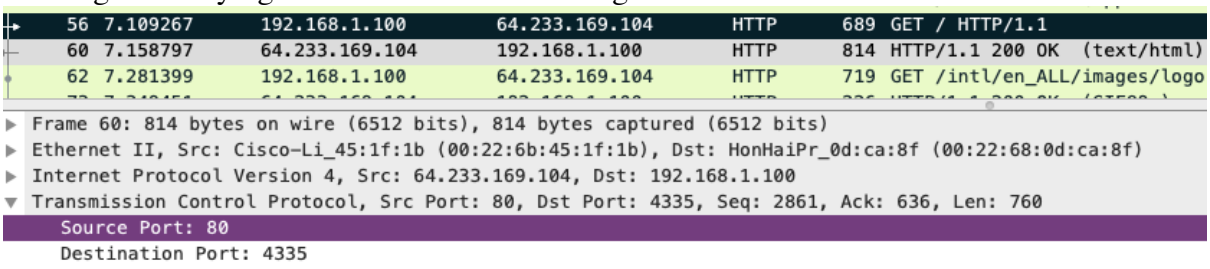


Source IP : TCP port → 192.168.1.100 : 4335

Destination IP : TCP port → 64.233.169.104 : 80

***1.3**

At what time is the corresponding 200 OK HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message?



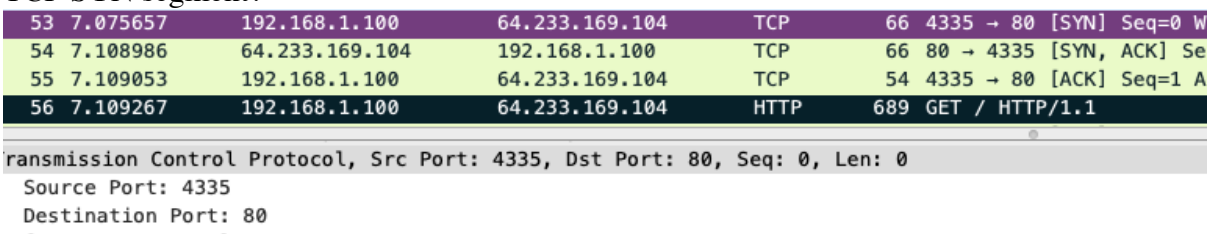
Time → 7.158797

Source IP : TCP port → 64.233.169.104 : 80

Destination IP : TCP port → 192.168.1.100 : 4335

1.4

Recall that before a GET command can be sent to an HTTP server, TCP must first set up a connection using the three-way SYN/ACK handshake. At what time is the client-to-server TCP SYN segment sent that sets up the connection used by the GET sent at time 7.109267? What are the source and destination IP addresses and source and destination ports for the TCP SYN segment?



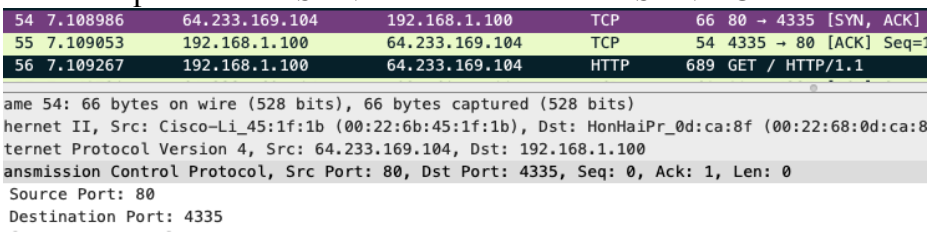
Time → 7.075657

Source IP : TCP port → 192.168.1.100 : 4335

Destination IP : TCP port → 64.233.169.104 : 80

z5147986
Lab7

1.5
What are the source and destination IP addresses and source and destination ports of the ACK sent in response to the SYN. At what time is this SYN/ACK received at the client?

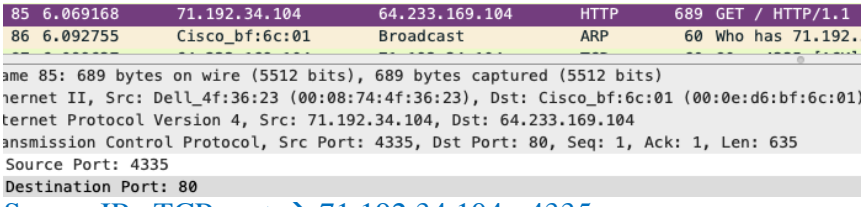


Time → 7.108986
Source IP : TCP port → 64.233.169.104 : 80
Destination IP : TCP port → 192.168.1.100 : 4335

1.6
Find the HTTP GET message that was sent from the client to the Google server at time 7.102967 (where t=7.109267 is time at which this was sent as recorded in the NAT_home_side trace file). At what time does this message appear in the NAT_ISP_side trace file?

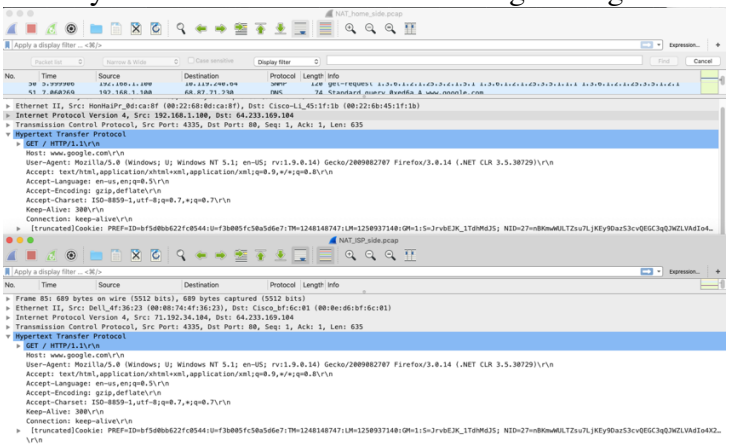
Time → 6.069168

***1.7**
What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET message (as recorded in the NAT_ISP_side trace file)? Which of these fields are the same, and which are different, than in your answer to Question 2 above?



Source IP : TCP port → 71.192.34.104 : 4335
Destination IP : TCP port → 64.233.169.104 : 80
Only the Destination IP, Destination TCP port are the same.

1.8
Are any fields in the HTTP GET message changed?

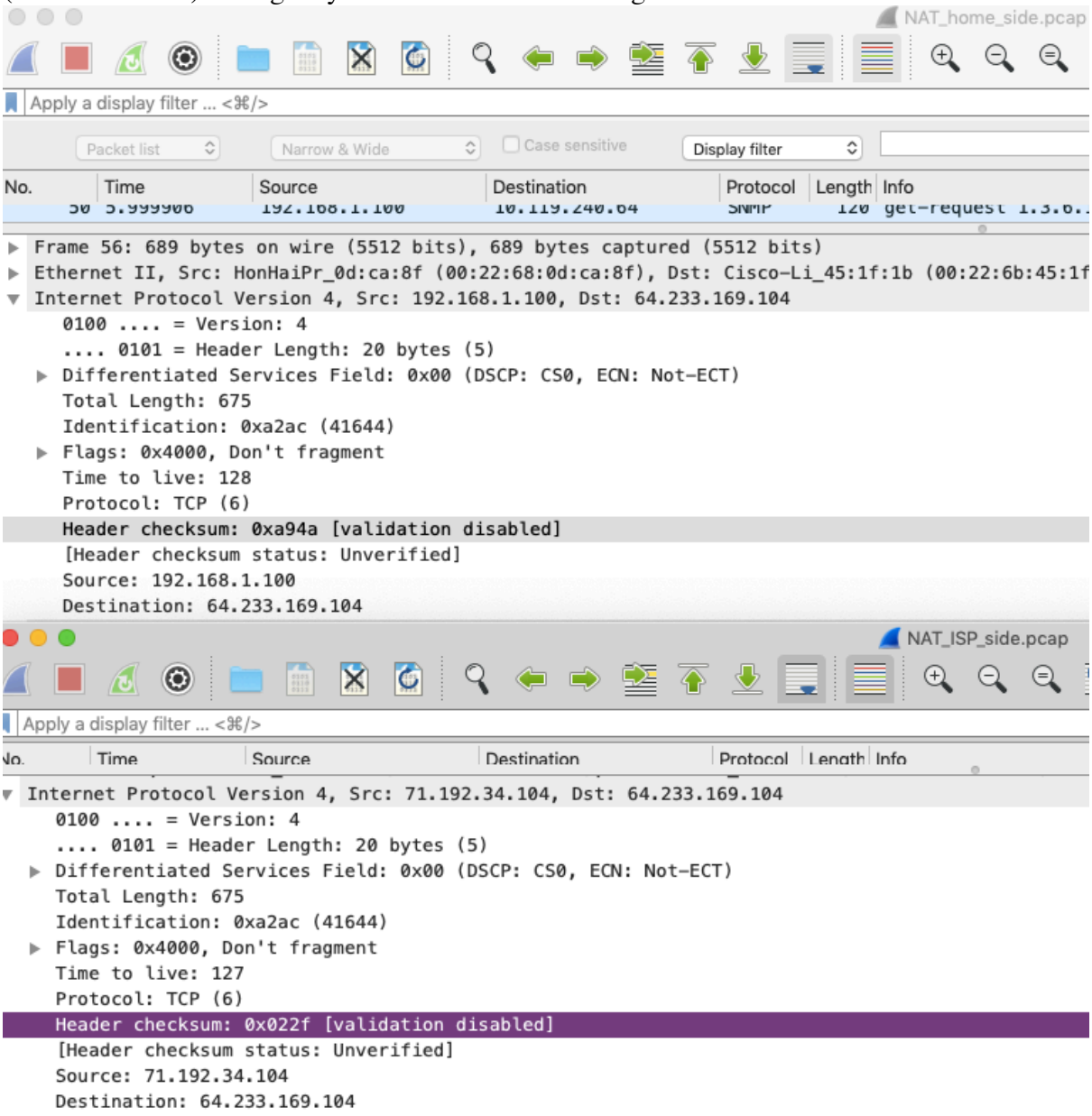


All the fields are the same

z5147986
Lab7

***1.9**

Which of the following fields in the IP datagram carrying the HTTP GET are changed: Version, Header Length, Flags, Checksum. If any of these fields have changed, give a reason (in one sentence) stating why this field needed to change.



Version → same
Header Length → same
Flags → same
Header Checksum → different
IP Header Checksum is recalculated every time the IP header (source IP) is changed

1.10

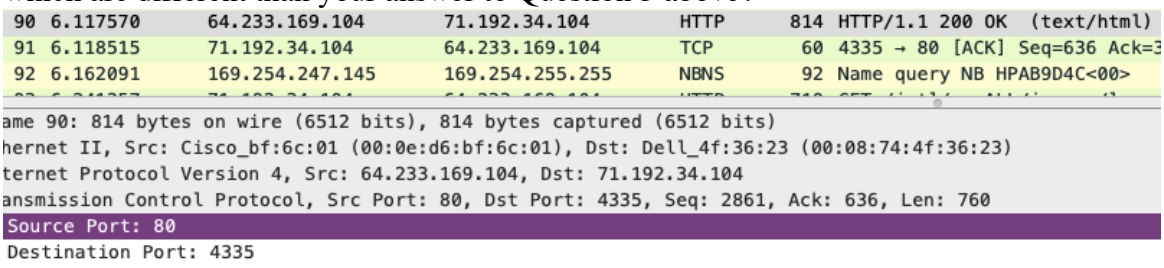
In the NAT_ISP_side trace file, at what time is the first 200 OK HTTP message received from the Google server?

Time → 6.117570

z5147986
Lab7

***1.11**

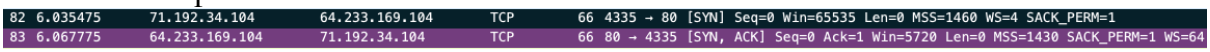
What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message? Which of these fields are the same, and which are different than your answer to Question 3 above?



Source IP : TCP port → 64.233.169.104 : 80
Destination IP : TCP port → 71.192.34.104 : 4335
Only the Destination IP, Destination TCP port are different

1.12

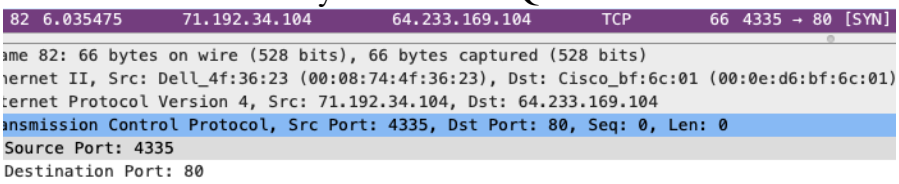
In the NAT_ISP_side trace file, at what time were the client-to-server TCP SYN segment and the server-to-client TCP SYN/ACK segment corresponding to the segments in Question 4 and 5 above captured?



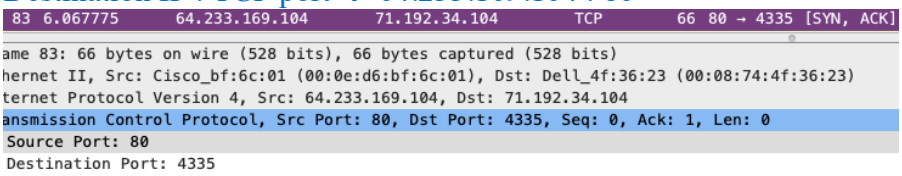
Client-to-server TCP SYN time → 6.035475
Server-to-client TCP SYN/ACK → 6.067775

***1.13**

What are the source and destination IP addresses and source and destination ports for these two segments (TCP SYN and TCP SYN/ACK)? Which of these fields are the same, and which are different than your answer to Question 4 and 5 above?



TCP SYN
Source IP : TCP port → 71.192.34.104 : 4335
Destination IP : TCP port → 64.233.169.104 : 80



TCP SYN/ACK
Source IP : TCP port → 64.233.169.104 : 80
Destination IP : TCP port → 71.192.34.104 : 4335

The Destination IP : TCP port (TCP SYN) and Source IP : TCP port (TCP SYN/ACK) for ISP are the **same** as the Destination IP : TCP port (TCP SYN) and Source IP : TCP port (TCP SYN/ACK) for Home.

The Source IP: TCP port (TCP SYN) and Destination IP : TCP port (TCP SYN/ACK) for ISP are **different** from the Source IP : TCP port (TCP SYN) and Destination IP : TCP port (TCP SYN/ACK) for Home.

z5147986
Lab7

***1.14**

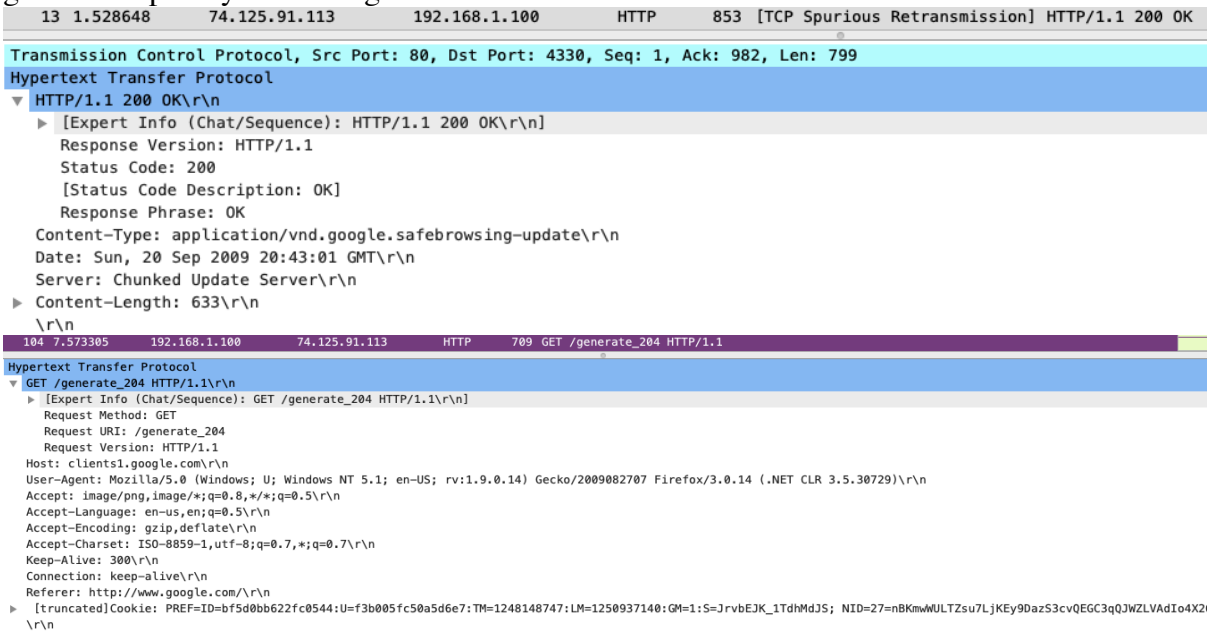
The discussion on NAT in the Week 7 lecture slide No 80 shows the NAT translation table used by a NAT router. Using your answers to the questions above, fill in the NAT translation table entries for the HTTP connection considered in the questions above.

WAN side addr → 71.192.34.104, 4335
LAN side addr → 192.168.1.100, 4335

Steps	Source	Destination
1. host sends	192.168.1.100, 4335	64.233.169.104, 80
2. NAT router changes	71.192.34.104, 4335	64.233.169.104, 80
3. Reply arrives	64.233.169.104, 80	71.192.34.104, 4335
4. NAT router changes	64.233.169.104, 80	192.168.1.100, 4335

1.15

The trace files investigated above have additional connections to Google servers above and beyond the HTTP GET, 200 OK request/response studied above. For example, in the NAT_home_side trace file, consider the client-to-server GET at time 1.572315, and the GET at time 7.573305. Research the use of these two HTTP messages and safe browsing in general. Explain your findings in a concise manner.

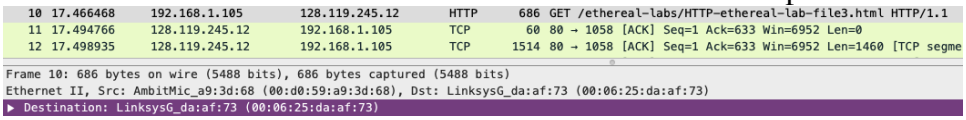


Google safe browsing is a blacklist service that provides list of URLs for web resources that contain malware or phishing content.

According to stackoverflow it returns generate_204 if WLAN is open, no response if closed or blocked if redirect to captive portal (A **captive portal** is a Web page that the user of a public-access **network** is obliged to view and interact with before access is granted) is present and based on the http status 204 No Content is not the same since there is no Etag header in the response

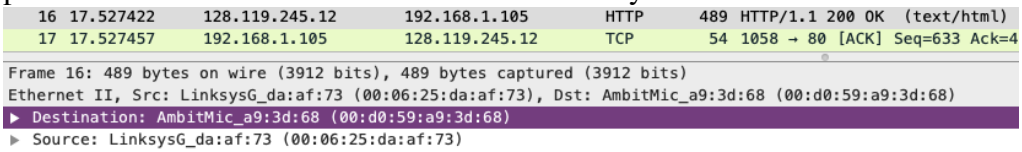
z5147986
Lab7

2.1
What is the 48-bit Ethernet address of the source host of this packet?



00:06:25:da:af:73

***2.2**
What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? If not, then which device has this address? (Note: this is an important question, and one that students sometimes get wrong. You may want to refer back to relevant parts of the text and lecture notes and make sure you understand the answer here.)



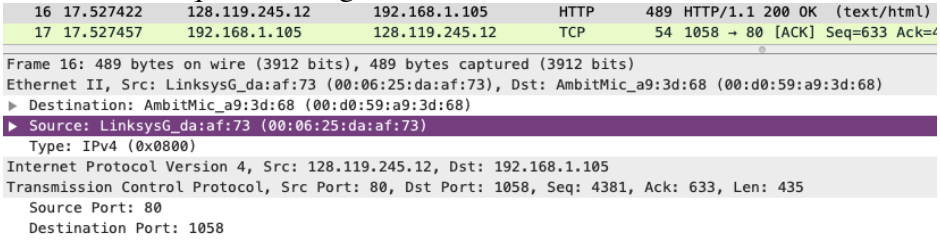
00:d0:59:a9:3d:68
No it does not.
This is the MAC address to the switch in the subnet

2.3
Give the hexadecimal value for the two-byte Frame type field.
0x0800 IP(v4)

***2.4**
How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame? Note that when you examine the Data portion of this frame, it actually consists of both the Ethernet frame headers as well as the payload (i.e. bottom window in Wireshark shows the entire 686 byte frame that is captured). Of the bytes preceding the G, the first few bytes are the Ethernet frame header. Does this include the preamble bytes, or are those bytes omitted from the capture? Given this, how many bytes of frame header are present? What are the remainder of the bytes before the G?

0x37, 3 * 16 + 7 = 55 bytes away from the start of the Ethernet frame
Preamble bytes not included.
686 - 672 = 14 bytes
Bytes before G = 55 – 14 = 41 bytes

***2.5**
What is the value of the Ethernet source address? Is this the address of the host that sent the GET HTTP request, or of gaia.cs.umass.edu? If not then which device has this address?



00:06:25:da:af:73
The address above is not the address of the host and not gaia.cs.umass.edu.
It is a MAC address belong to the switch in the subnet

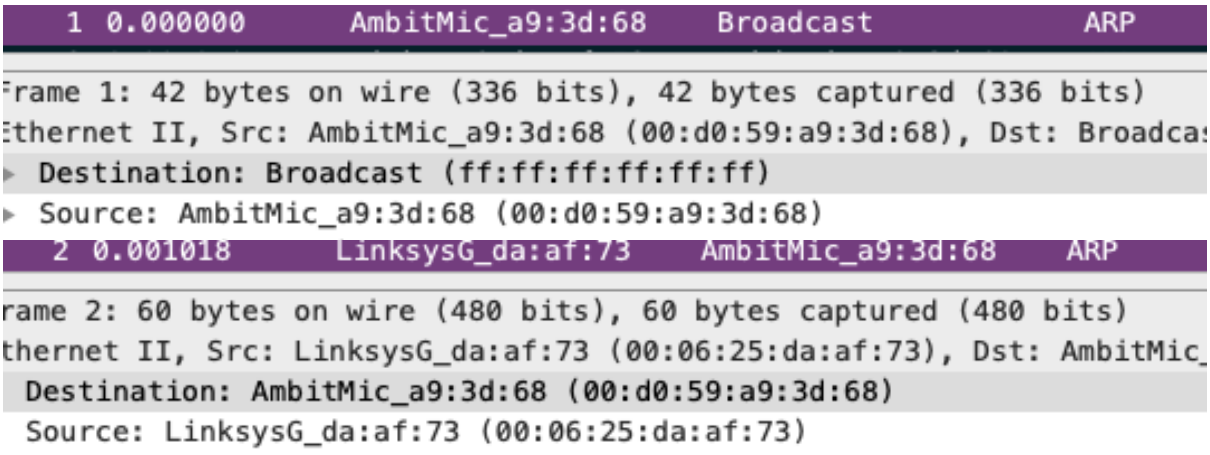
z5147986
Lab7

2.6
What is the destination address in the Ethernet frame? Is this the Ethernet address of the source host that sent the earlier GET HTTP request?
00:d0:59:a9:3d:68
Yes

2.7
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?
0x07, 7 bytes

z5147986
Lab7

***3.1**
What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message? Is there something special about the destination address?



No.	Source	Destination
1	00:d0:59:a9:3d:68	ff:ff:ff:ff:ff:ff
2	00:06:25:da:af:73	00:d0:59:a9:3d:68

3.2
Give the hexadecimal value for the two-byte Ethernet Frame type field.
0x0806, ARP

3.3
How many bytes from the very beginning of the Ethernet frame does the ARP *opcode* field begin?
? I don't get this ?

3.4
What is the value of the *opcode* field within the ARP-payload part of the Ethernet frame in which an ARP request is made?
Value of opcode field → request (1)

3.5
Does the ARP request message contain the IP address of the sender?
Yes

***3.6**
Where in the ARP request does the "question" (IP address for which the mapping is being requested) appear?
Target IP address → 192.168.1.1

3.7
How many bytes from the very beginning of the Ethernet frame does the ARP *opcode* field begin?
? I don't get this ?

z5147986
Lab7

***3.8**

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

Value of opcode field → reply (2)

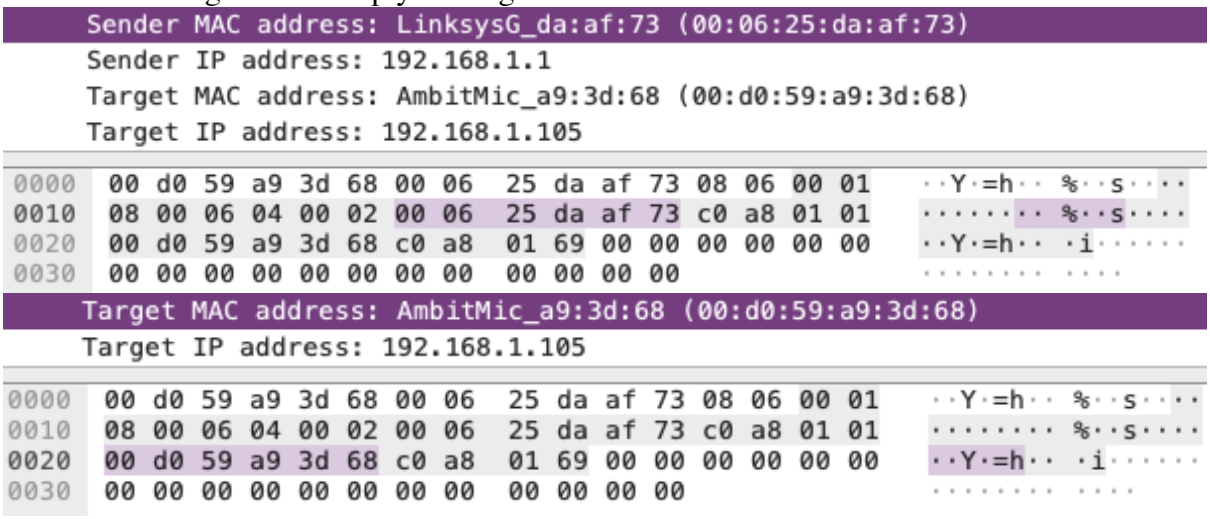
***3.9**

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

Target IP address → 192.168.1.105

***3.10**

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



Source → 00:06:25:da:af:73

Destination → 00:d0:59:a9:3d:68