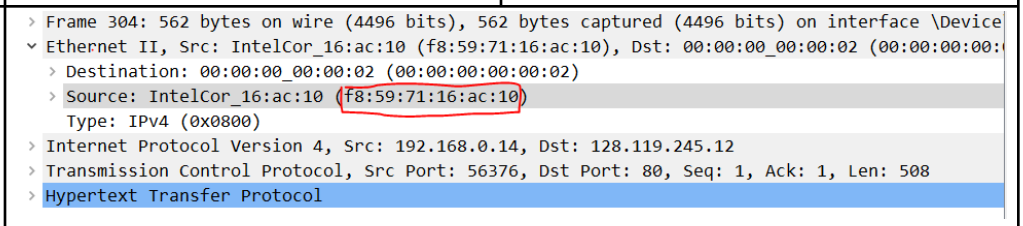
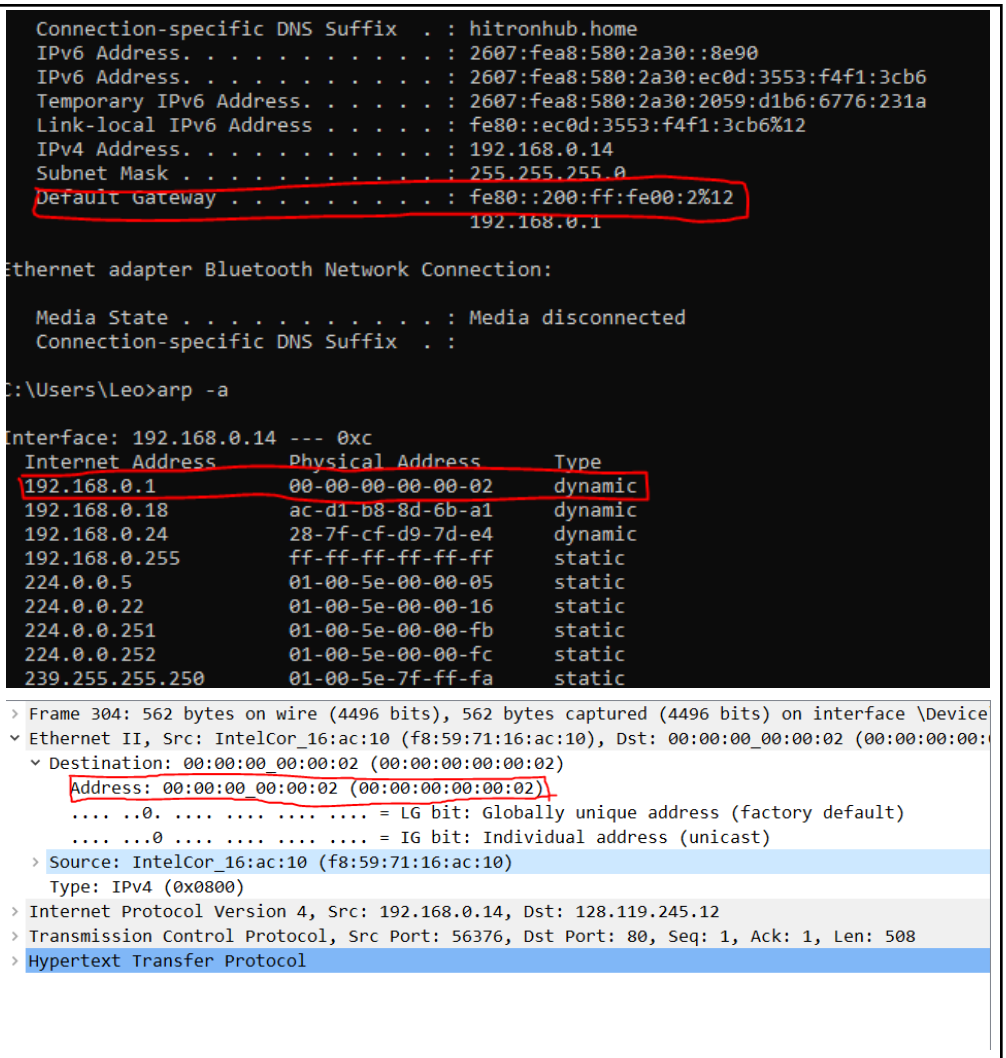
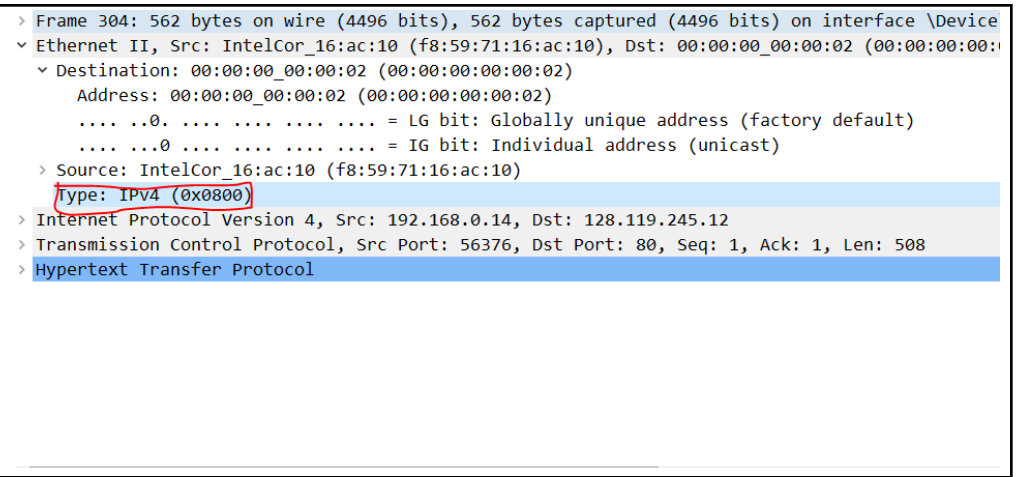
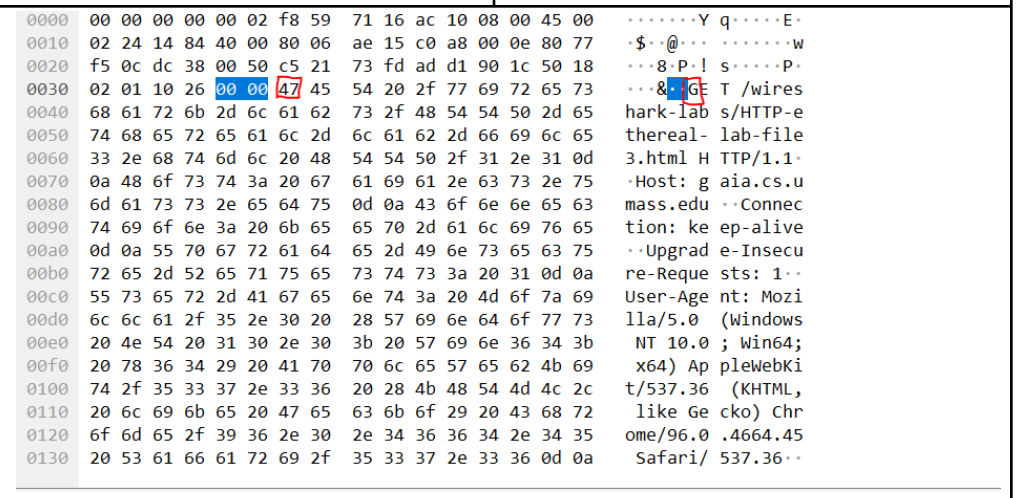
Wireshark Lab 5: Ethernet and ARP

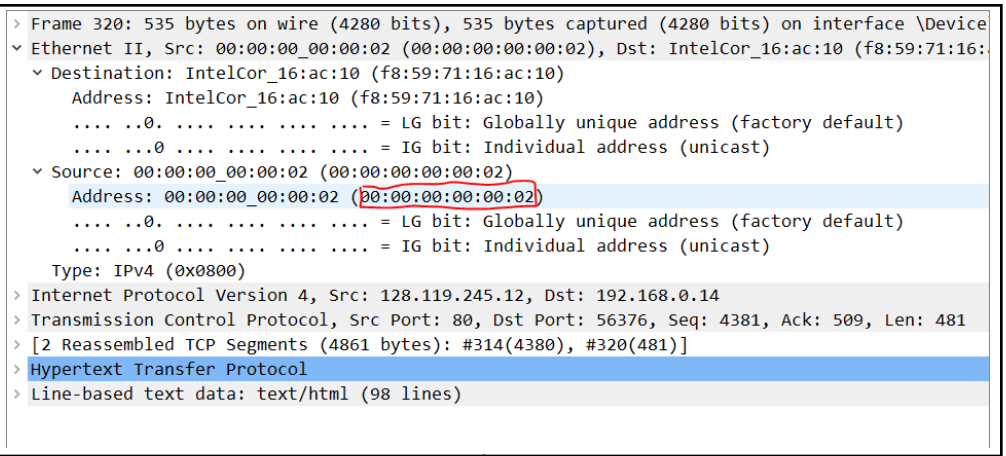
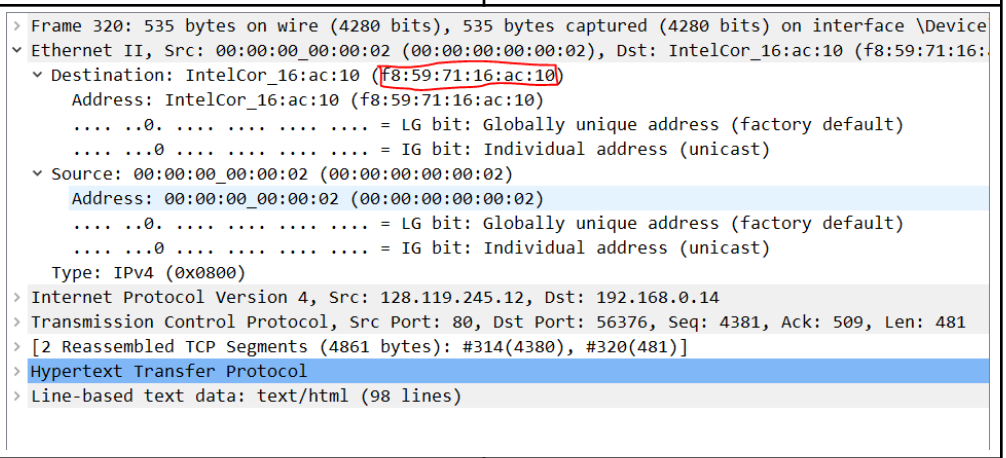
Group Details:
Leo Hanxu 1006045067
Shaoyang Zhang 1005751660

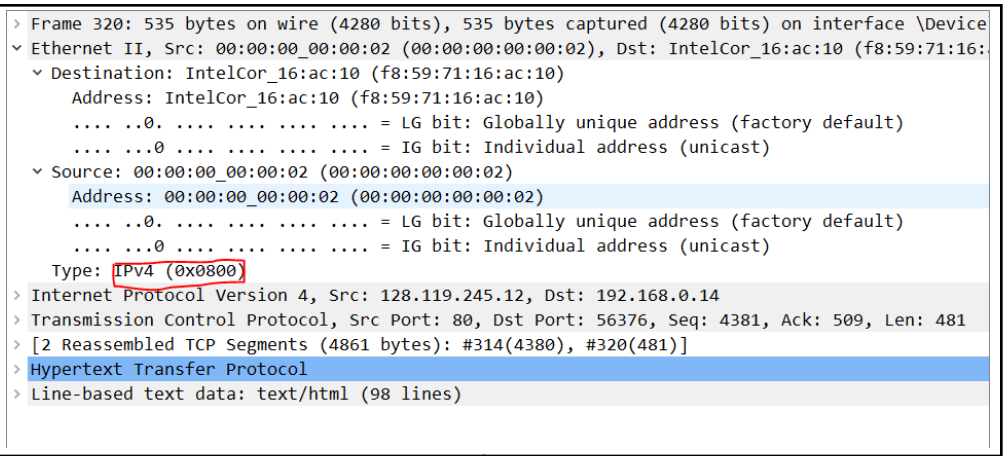
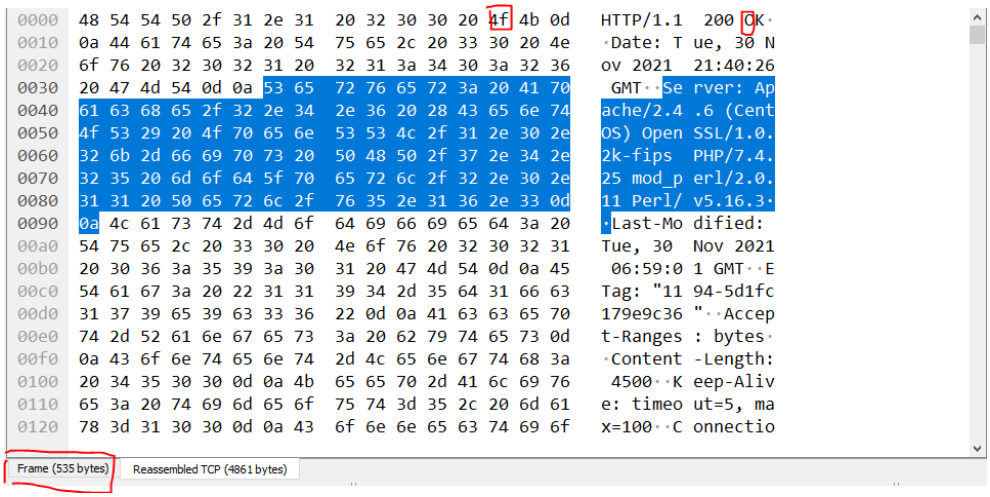
Mark:

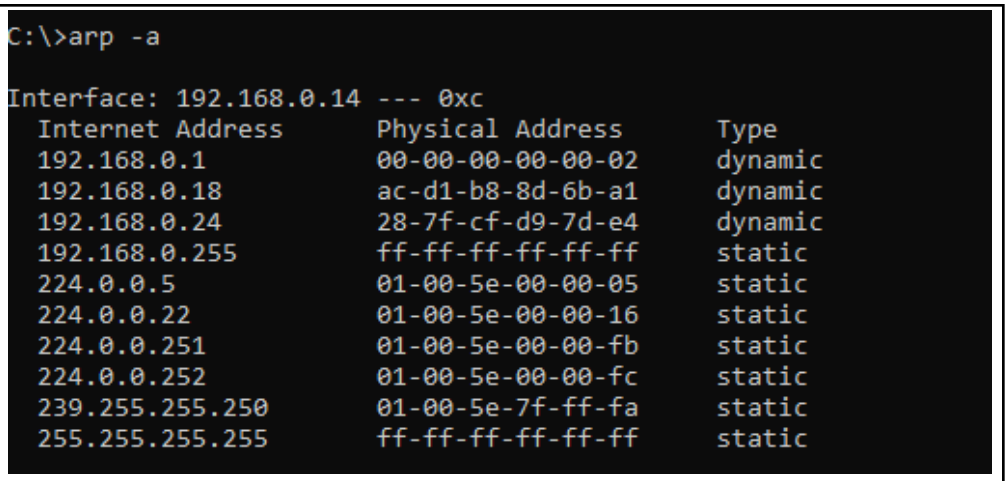
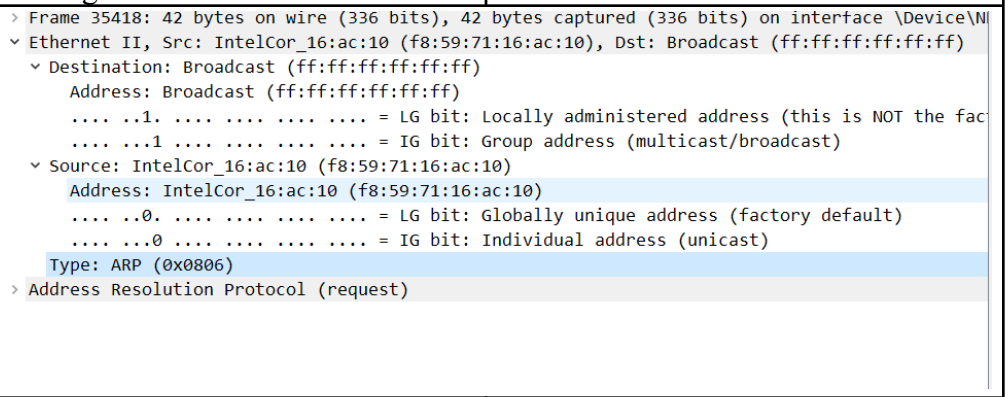
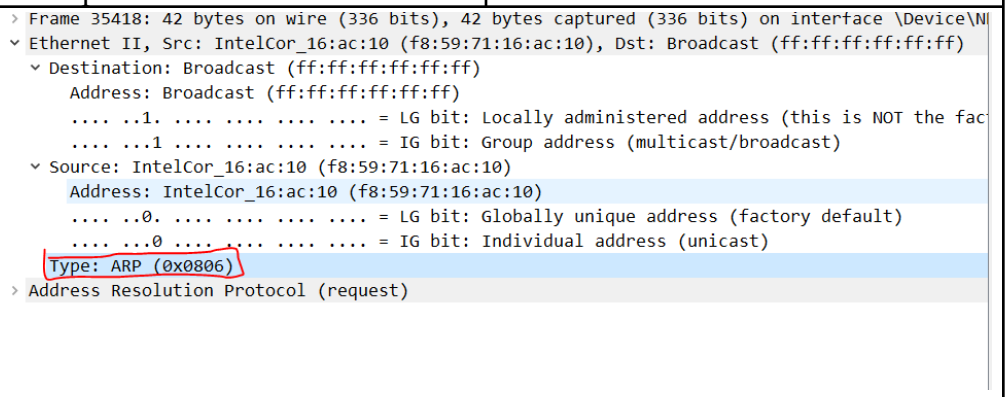
	Question	Answer
1	What is the 48-bit Ethernet address of your computer?	f8:59:71:16:ac:10
Annotated Screenshot (if needed)		
2	What is the 48-bit destination address in the Ethernet frame? What device has this as its Ethernet address?	00:00:00:00:00:02 But it is different from the actual gateway mac address as shown in the command prompt. Our guess the reason it is different is it is a different type of MAC address. This is not the Ethernet address of the destination, it is Ethernet is the gateway address which is the address of the router

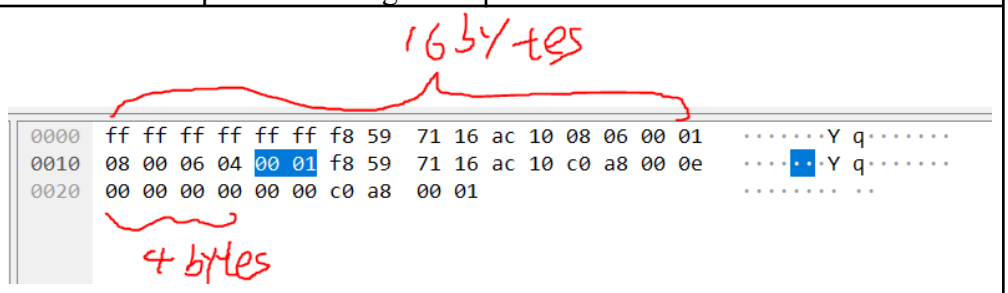
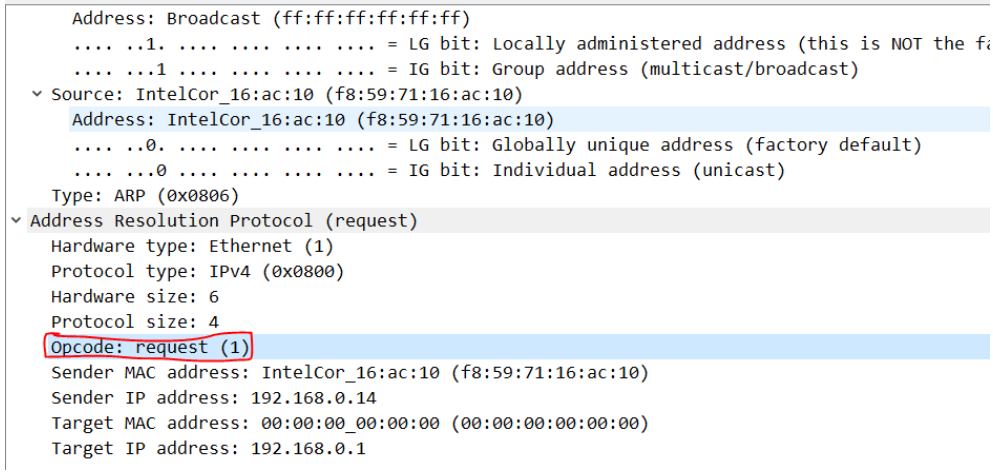
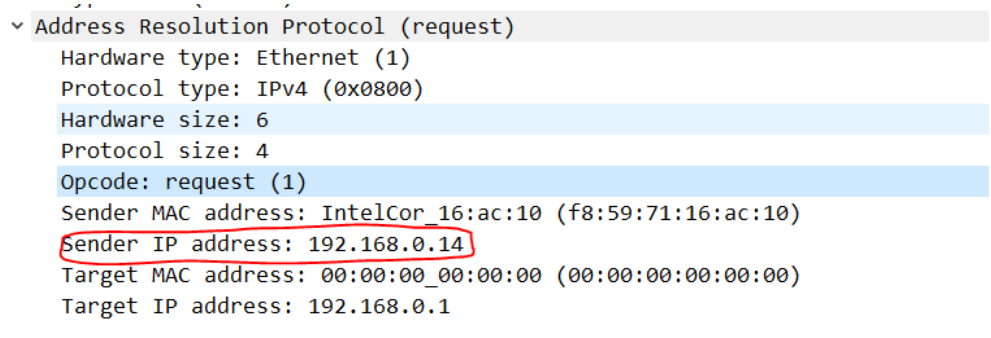
Annotated Screenshot (if needed)		
3	Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?	0x0800 It corresponds to IPv4

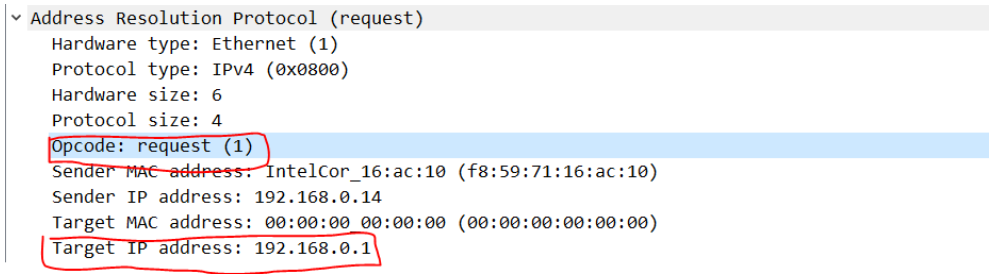
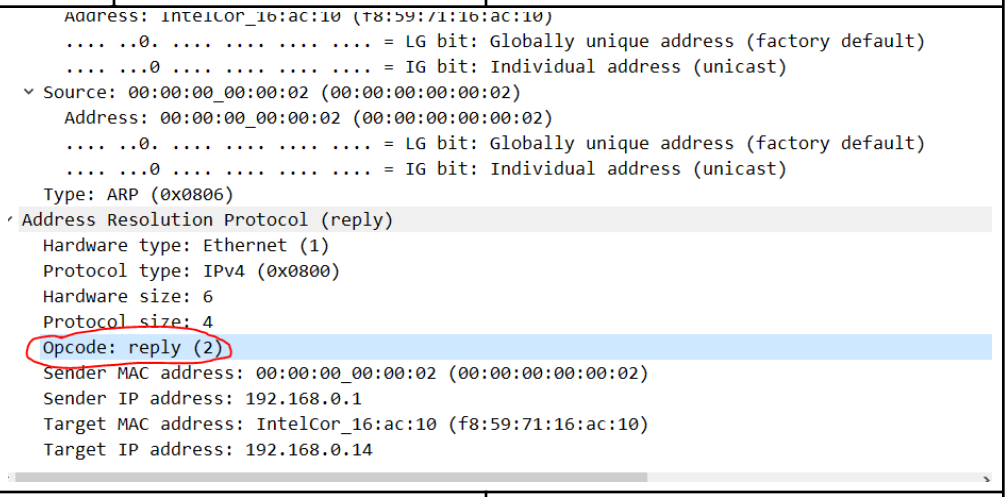
Annotated Screenshot (if needed)		
4	How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame?	54 bytesç
Annotated Screenshot (if needed)		
5	What is the value of the Ethernet source address? What device has this as its Ethernet address?	00:00:00:00:00:02 same issue as question two it is the address of the router which is the gateway address

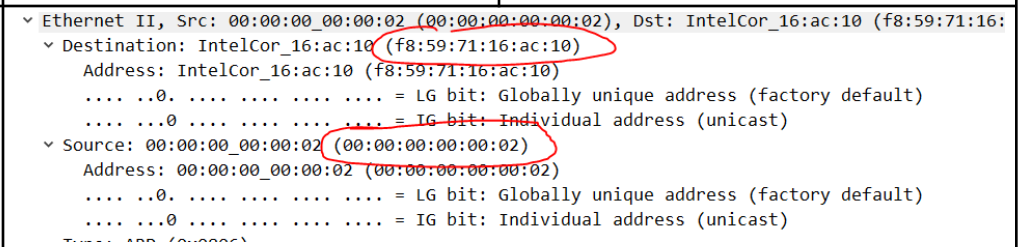
Annotated Screenshot (if needed)		
6	What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?	f8:59:71:16:ac:10 it the Ethernet address of my computer
Annotated Screenshot (if needed)		
7	Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?	0x0800 IPv4

Annotated Screenshot (if needed)		
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?	13+535 = 548 bytes
Annotated Screenshot (if needed)		
9	Write down the contents of your computer’s ARP cache. What is the meaning of each column value?	The first column and the second column correspond to the mapping between the IP address and the MAC address that is known in the local network. The third column corresponds to the type of IP address whether it is dynamic or static.

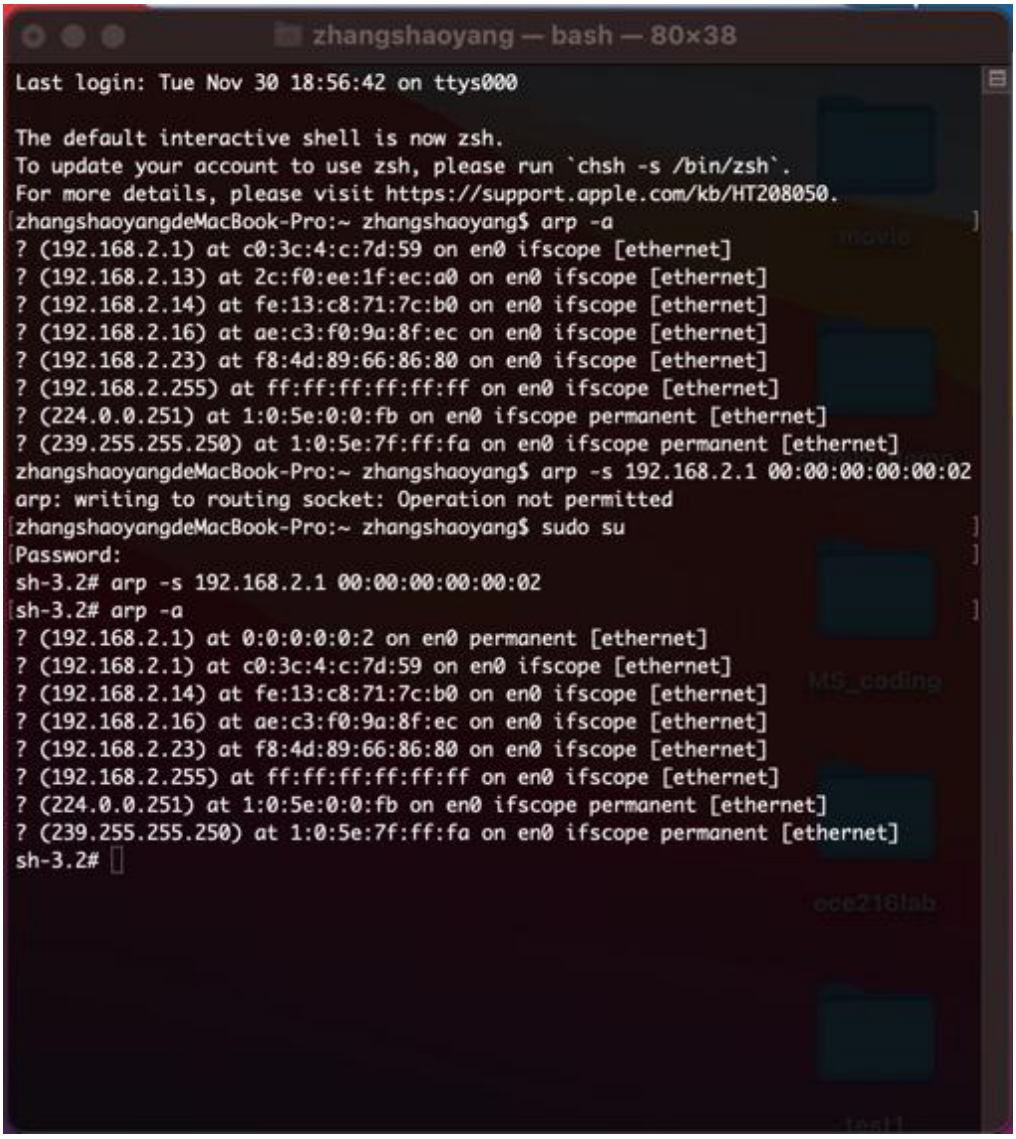
Annotated Screenshot (if needed)		
10	What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?	Destination: ff:ff:ff:ff:ff:ff Source: f8:59:71:16:ac:10
Annotated Screenshot (if needed)		
11	Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?	0x0806, it corresponds to ARP
Annotated Screenshot (if needed)		

12.a	How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?	Excluding the preamble part of the header, it ARP opcode start at 21 byte
Annotated Screenshot (if needed)		
12.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 is 1
Annotated Screenshot (if needed)		
12.c	Does the ARP message contain the IP address of the sender?	Yes
Annotated Screenshot (if needed)		
12.d	Where in the ARP request does the “question” appear – the Ethernet address of the machine whose corresponding IP address is being	The opcode field is 1 meaning this is the request message. It is asking who has the IP address (shown in the target IP address) 192.168.0.1. If you

	queried?	are that address, respond to the device which has IP address 192.168.0.14(which shown in the send ip address field)
Annotated Screenshot (if needed)		
13.a	How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?	Excluding the preamble part of the header, it ARP opcode start at 21 byte
Annotated Screenshot (if needed)	same as 12 a	
13.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?	The value is 2 which is a reply message
Annotated Screenshot (if needed)		
13.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?	It is answering to the device that has IP address 192.168.0.14 that it has the IP address 192.168.0.1, and also answering that its MAC address is 00:00:00:00:00:02 (appear in sender MAC address field).
Annotated Screenshot (if needed)		
14	What are the hexadecimal values for the source and destination	Destination: f8:59:71:16:ac:10 Source: 00:00:00:00:00:02

	addresses in the Ethernet frame containing the ARP reply message?	
Annotated Screenshot (if needed)		
15	Why is there no ARP reply (sent in response to the ARP request in packet 6) in the packet trace?	It does not respond because its IP address is not 192.168.1.117
Annotated Screenshot (if needed)		

EX1:
if not using root access, the writing to routing socket operation is not permitted, but if using root access the operation can be done manually. However, usually after 20 minutes the table will refresh so the incorrect entry will be discarded.


zhangshaoyang — bash — 80×38
Last login: Tue Nov 30 18:56:42 on ttys000
The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
zhangshaoyangdeMacBook-Pro:~ zhangshaoyang$ arp -a
? (192.168.2.1) at c0:3c:4:c:7d:59 on en0 ifscope [ethernet]
? (192.168.2.13) at 2c:f0:ee:1f:ec:a0 on en0 ifscope [ethernet]
? (192.168.2.14) at fe:13:c8:71:7c:b0 on en0 ifscope [ethernet]
? (192.168.2.16) at ae:c3:f0:9a:8f:ec on en0 ifscope [ethernet]
? (192.168.2.23) at f8:4d:89:66:86:80 on en0 ifscope [ethernet]
? (192.168.2.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
? (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
? (239.255.255.250) at 1:0:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
zhangshaoyangdeMacBook-Pro:~ zhangshaoyang$ arp -s 192.168.2.1 00:00:00:00:00:02
arp: writing to routing socket: Operation not permitted
zhangshaoyangdeMacBook-Pro:~ zhangshaoyang$ sudo su
Password:
sh-3.2# arp -s 192.168.2.1 00:00:00:00:00:02
sh-3.2# arp -a
? (192.168.2.1) at 0:0:0:0:0:2 on en0 permanent [ethernet]
? (192.168.2.1) at c0:3c:4:c:7d:59 on en0 ifscope [ethernet]
? (192.168.2.14) at fe:13:c8:71:7c:b0 on en0 ifscope [ethernet]
? (192.168.2.16) at ae:c3:f0:9a:8f:ec on en0 ifscope [ethernet]
? (192.168.2.23) at f8:4d:89:66:86:80 on en0 ifscope [ethernet]
? (192.168.2.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
? (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
? (239.255.255.250) at 1:0:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
sh-3.2#

EX2:
through experimenting on Mac the default timeout is 20 minutes