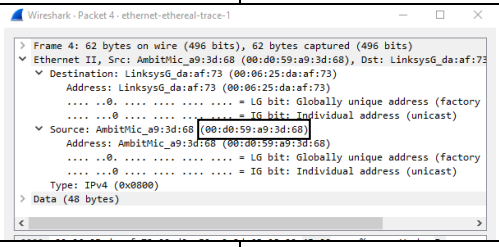
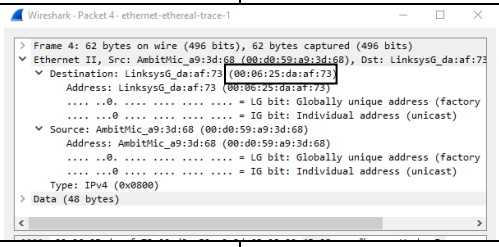
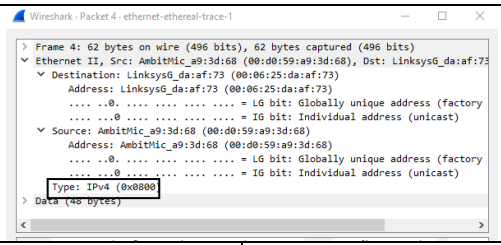
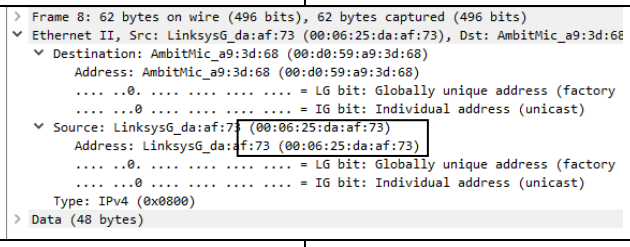
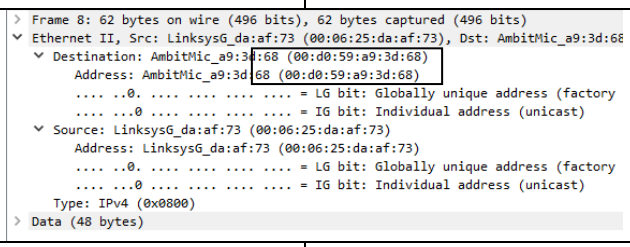
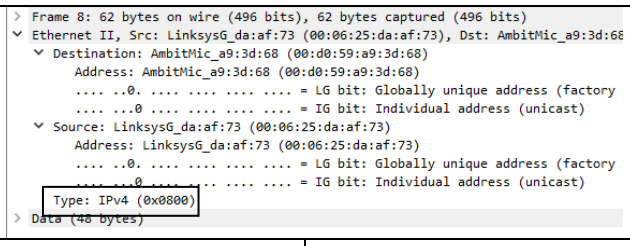
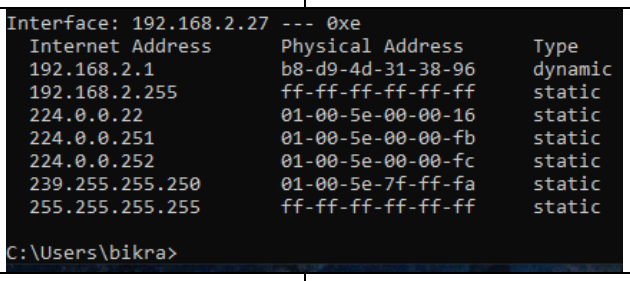
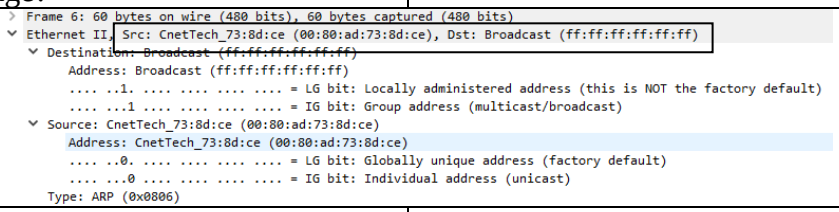
Wireshark Lab 5: Ethernet and ARP

Group Details: Bikramjit Narwal (1005242300), Chao Glen Xu (1004274634)

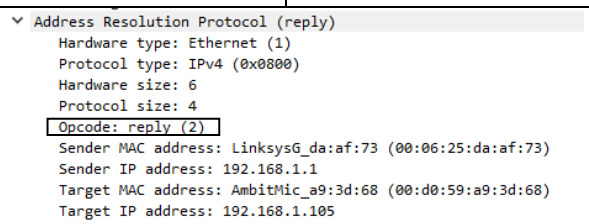
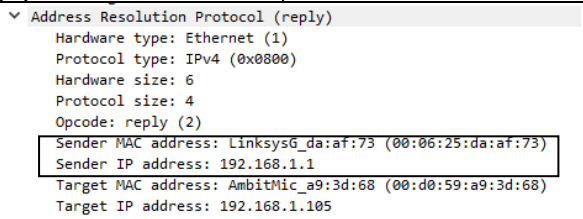
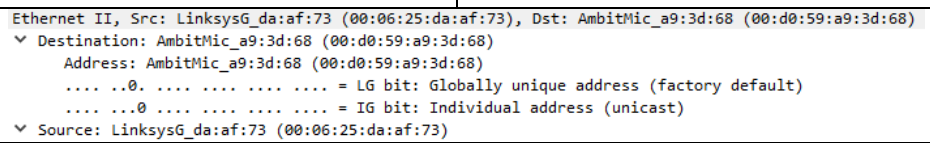
Mark:

	Question	Answer
1	What is the 48-bit Ethernet address of your computer?	00:d0:59:a9:3d:68
Annotated Screenshot (if needed)		
2	What is the 48-bit destination address in the Ethernet frame? What device has this as its Ethernet address?	00:09:25:da:af:73
Annotated Screenshot (if needed)		
3	Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?	The hexadecimal value for the two-byte Frame type field is 0x0800. It corresponds to Internet Protocol version 4.

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?	After 432 bits (54 bytes) the G in get appears.
Annotated Screenshot (if needed)		
5	What is the value of the Ethernet source address? What device has this as its Ethernet address?	The value of the Ethernet source address is 00:06:25:da:af:73. The device that has this as its Ethernet address is my router.
Annotated Screenshot (if needed)		
6	What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?	The destination address is 00:d0:59:a9:3d:68. It is the 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?	The hexadecimal value for the two-byte Frame type field is 0x0800. It corresponds to Internet Protocol version 4.

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?	It appears after 52 bytes from the start of the Ethernet frame.
Annotated Screenshot (if needed)		
9	Write down the contents of your computer's ARP cache. What is the meaning of each column value?	The meaning of each column: Internet Address column contains the IP address, the Physical Address contains the MAC address, and the type indicates the protocol type.
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?	Source: 00:80:ad:73:8d:ce Destination: ff:ff:ff:ff:ff:ff
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?	The hexadecimal value for the two-byte Ethernet Frame type field is 0x0806. Refers to ADP.

Annotated Screenshot (if needed)	Frame 6: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) Ethernet II, Src: CnetTech_73:8d:ce (00:80:ad:73:8d:ce), Dst: Broadcast (ff:ff:ff:ff:ff:ff) Destination: Broadcast (ff:ff:ff:ff:ff:ff) Address: Broadcast (ff:ff:ff:ff:ff:ff) .... ..1. .... = LG bit: Locally administered address (this is NOT the factory default) ....1 .... = IG bit: Group address (multicast/broadcast) Source: CnetTech_73:8d:ce (00:80:ad:73:8d:ce) Address: CnetTech_73:8d:ce (00:80:ad:73:8d:ce) .... ..0. .... = LG bit: Globally unique address (factory default) ....0 .... = IG bit: Individual address (unicast) Type: ARP (0x0806)	
12.a	How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?	20 bytes from the very beginning of the Ethernet frame.
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 of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made is 1.
Annotated Screenshot (if needed)	Address Resolution Protocol (request) Hardware type: Ethernet (1) Protocol type: IPv4 (0x0800) Hardware size: 6 Protocol size: 4 Opcode: request (1) Sender MAC address: CnetTech_73:8d:ce (00:80:ad:73:8d:ce) Sender IP address: 192.168.1.104 Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00) Target IP address: 192.168.1.117	
12.c	Does the ARP message contain the IP address of the sender?	192.168.1.104
Annotated Screenshot (if needed)	Address Resolution Protocol (request) Hardware type: Ethernet (1) Protocol type: IPv4 (0x0800) Hardware size: 6 Protocol size: 4 Opcode: request (1) Sender MAC address: CnetTech_73:8d:ce (00:80:ad:73:8d:ce) Sender IP address: 192.168.1.104 Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00) Target IP address: 192.168.1.117	
12.d	Where in the ARP request does the "question" appear – the Ethernet address of the machine whose corresponding IP address is being queried?	The field "Target Mac Address" is 00:00:00:00:00:00 to question the machine whose corresponding IP address is being queried.
Annotated Screenshot (if needed)	Address Resolution Protocol (request) Hardware type: Ethernet (1) Protocol type: IPv4 (0x0800) Hardware size: 6 Protocol size: 4 Opcode: request (1) Sender MAC address: CnetTech_73:8d:ce (00:80:ad:73:8d:ce) Sender IP address: 192.168.1.104 Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00) Target IP address: 192.168.1.117	
13.a	How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?	20 bytes from the very beginning of the Ethernet frame.
Annotated		

Screenshot (if needed)		
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?	It is 2.
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?	192.168.1.1
Annotated Screenshot (if needed)		
14	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
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?	Why is there no ARP reply (sent in response to the ARP request in packet 6) in the packet trace because we are not in the machine that sent the request. In addition, the ARP request is broadcast. It's also known that the ARP reply is sent back straight to the senders (source's) Ethernet address.
Annotated Screenshot (if needed)		