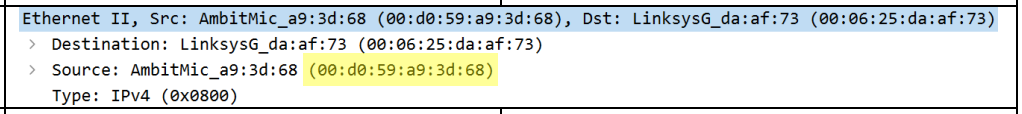
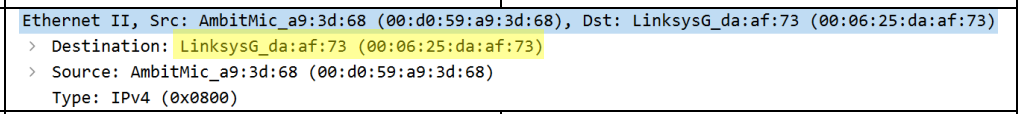
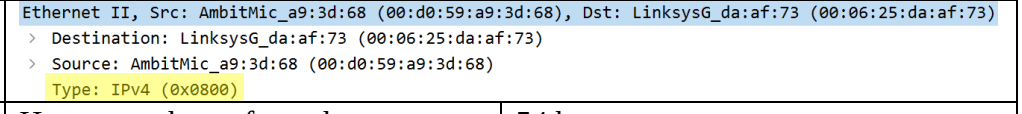
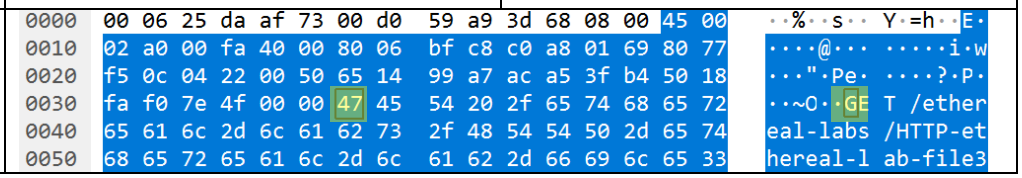
Wireshark Lab 5: Ethernet and ARP

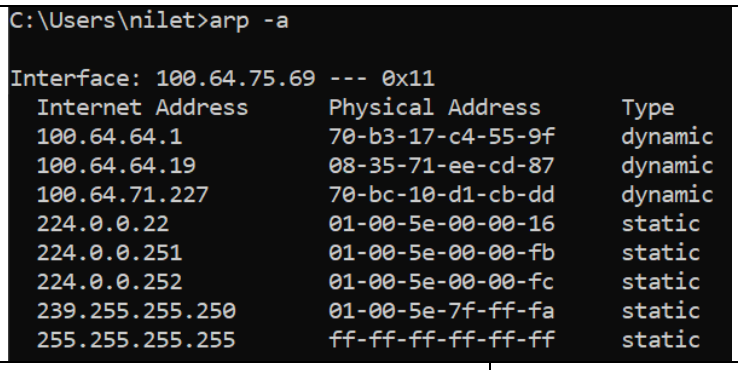
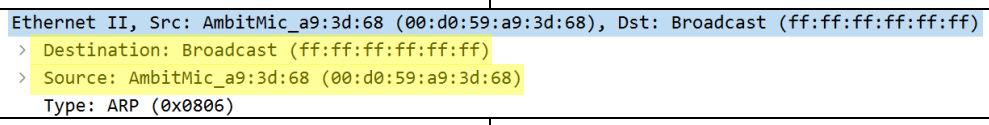
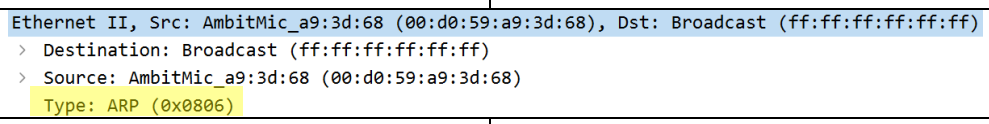
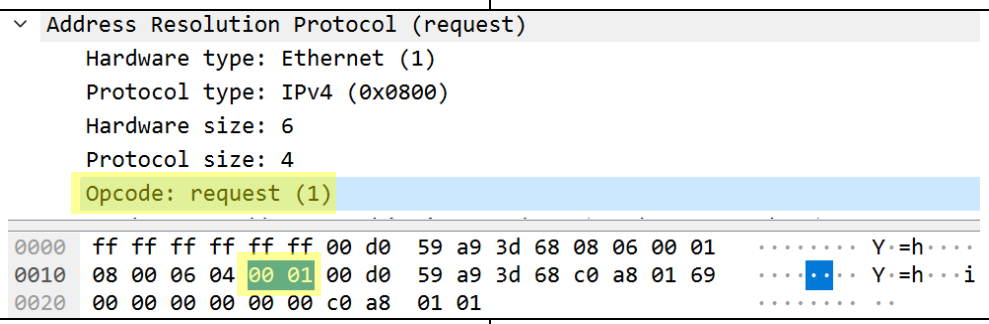
Group Details:

Leting Ni	1006255446
Yuhe Chen	1005689480

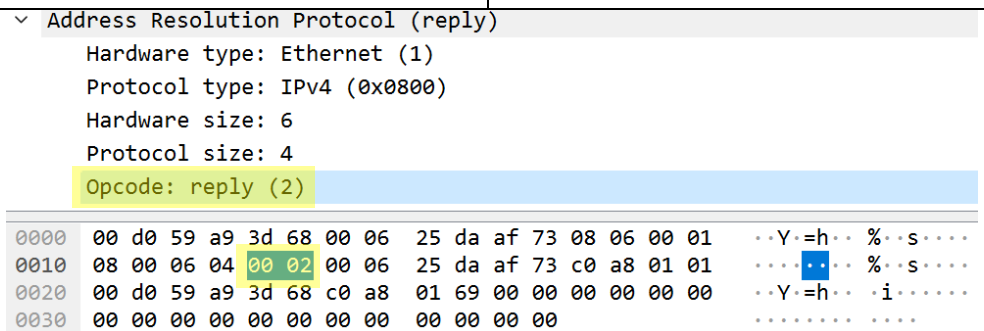
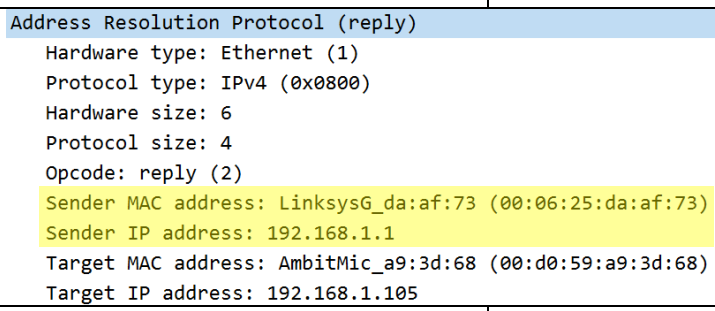
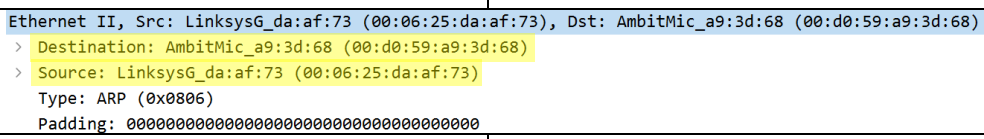
Mark:

	Question	Answer
1	What is the 48-bit Ethernet address of your computer?	00:d0:59:a9:3d:68
Annotated Screenshot (if needed)	 Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysG_da:af:73 (00:06:25:da:af:73) › Destination: LinksysG_da:af:73 (00:06:25:da:af:73) › Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68) Type: IPv4 (0x0800)	
2	What is the 48-bit destination address in the Ethernet frame? What device has this as its Ethernet address?	00:06:25:da:af:73 It is the address of my Linksys router (gateway to get off my subnet).
Annotated Screenshot (if needed)	 Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysG_da:af:73 (00:06:25:da:af:73) › Destination: LinksysG_da:af:73 (00:06:25:da:af:73) › Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68) Type: IPv4 (0x0800)	
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)	 Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysG_da:af:73 (00:06:25:da:af:73) › Destination: LinksysG_da:af:73 (00:06:25:da:af:73) › Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68) Type: IPv4 (0x0800)	
4	How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame?	54 bytes
Annotated Screenshot (if needed)	 0000 00 06 25 da af 73 00 d0 59 a9 3d 68 08 00 45 00 ··%··s·· Y·=h··E· 0010 02 a0 00 fa 40 00 80 06 bf c8 c0 a8 01 69 80 77 ····@··· ·····i·w 0020 f5 0c 04 22 00 50 65 14 99 a7 ac a5 3f b4 50 18 ···"·Pe· ····?·P· 0030 fa f0 7e 4f 00 00 47 45 54 20 2f 65 74 68 65 72 ··~O··GE T /ether 0040 65 61 6c 2d 6c 61 62 73 2f 48 54 54 50 2d 65 74 eal-labs /HTTP-et 0050 68 65 72 65 61 6c 2d 6c 61 62 2d 66 69 6c 65 33 hereal-l ab-file3	

5	What is the value of the Ethernet source address? What device has this as its Ethernet address?	00:06:25:da:af:73 It is the address of my Linksys router (gateway to get onto my subnet).
Annotated Screenshot (if needed)	Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68) › Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68) › Source: LinksysG_da:af:73 (00:06:25:da:af:73) Type: IPv4 (0x0800)	
6	What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?	00:d0:59:a9:3d:68 Yes, it is the Ethernet address of my computer.
Annotated Screenshot (if needed)	Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68) › Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68) › Source: LinksysG_da:af:73 (00:06:25:da:af:73) Type: IPv4 (0x0800)	
7	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)	Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68) › Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68) › Source: LinksysG_da:af:73 (00:06:25:da:af:73) Type: IPv4 (0x0800)	
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?	67 bytes
Annotated Screenshot (if needed)	0000 00 d0 59 a9 3d 68 00 06 25 da af 73 08 00 45 60 ··Y·=h·· %··s··E` 0010 05 dc 8f 2f 40 00 37 06 76 f7 80 77 f5 0c c0 a8 ···/@·7· v··w···· 0020 01 69 00 50 04 22 ac a5 3f b4 65 14 9c 1f 50 10 ·i·P·"·· ?·e···P· 0030 1b 28 5e d0 00 00 48 54 54 50 2f 31 2e 31 20 32 ·(^···HT TP/1.1 2 0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 53 61 74 00 OK··D ate: Sat 0050 2c 20 32 38 20 41 75 67 20 32 30 30 34 20 31 37 , 28 Aug 2004 17 0060 3a 31 39 3a 33 37 20 47 4d 54 0d 0a 53 65 72 76 :19:37 G MT··Serv	
9	Write down the contents of your computer's ARP cache. What is the meaning of each column value?	Contents: see screenshot below. Internet Address: IP address Physical Address: MAC address Type: 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:d0:59:a9:3d:68 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?	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?	20 bytes
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?	0x0001

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) 0000 ff ff ff ff ff ff 00 d0 59 a9 3d 68 08 06 00 01 ····· Y·=h···· 0010 08 00 06 04 00 01 00 d0 59 a9 3d 68 c0 a8 01 69 ····· Y·=h···i 0020 00 00 00 00 00 00 c0 a8 01 01 ····· ··	
12.c	Does the ARP message contain the IP address of the sender?	Yes. 192.168.1.105
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: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68) Sender IP address: 192.168.1.105 Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00) Target IP address: 192.168.1.1	
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 Target MAC address is set to 00:00:00:00:00:00. This will query the machine whose corresponding IP address is 192.168.1.1.
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: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68) Sender IP address: 192.168.1.105 Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00) Target IP address: 192.168.1.1	
13.a	How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?	20 bytes
Annotated Screenshot (if needed)	Address Resolution Protocol (reply) Hardware type: Ethernet (1) Protocol type: IPv4 (0x0800) Hardware size: 6 Protocol size: 4 Opcode: reply (2) 0000 00 d0 59 a9 3d 68 00 06 25 da af 73 08 06 00 01 ··Y·=h·· %··s···· 0010 08 00 06 04 00 02 00 06 25 da af 73 c0 a8 01 01 ····· %··s···· 0020 00 d0 59 a9 3d 68 c0 a8 01 69 00 00 00 00 00 00 ··Y·=h·· ·i····· 0030 00 00 00 00 00 00 00 00 00 00 00 00 ····· ····	

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?	0x0002
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?	The Sender MAC address 00:06:25:da:af:73 and the Sender IP address 192.168.1.1 is the answer to the earlier ARP request.
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?	The ARP request is broadcast, but the ARP reply is not broadcast and sent directly to the computer that sent the request. Therefore, we cannot see the ARP reply in this trace.
Annotated Screenshot (if needed)		