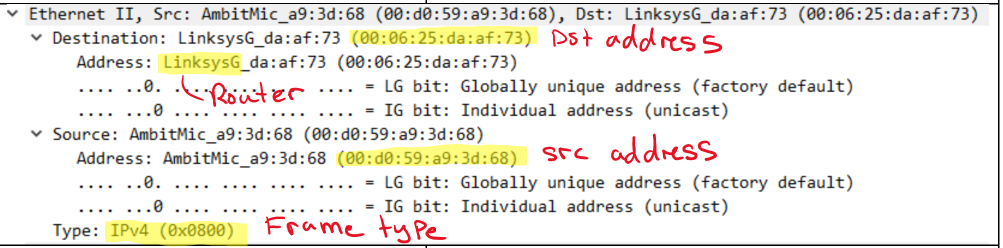
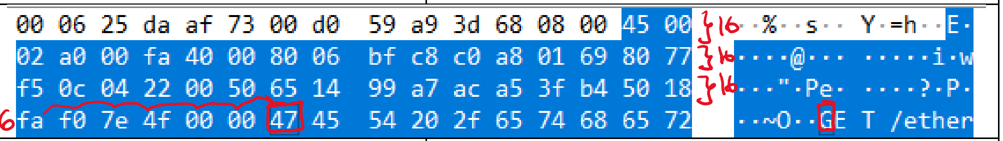
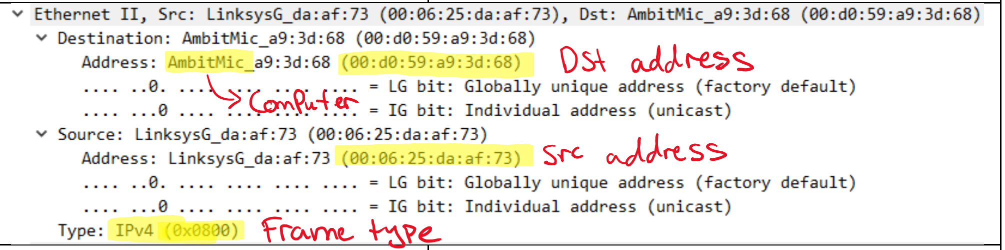
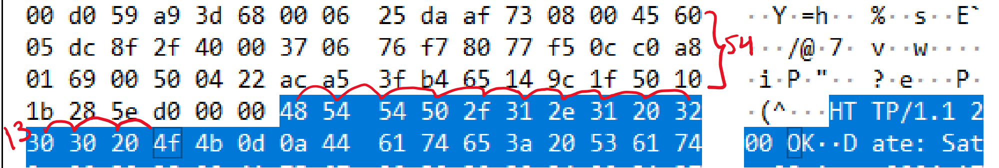
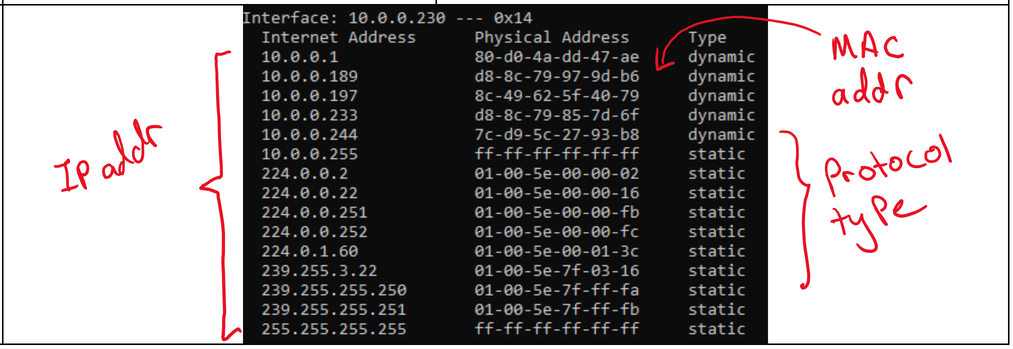
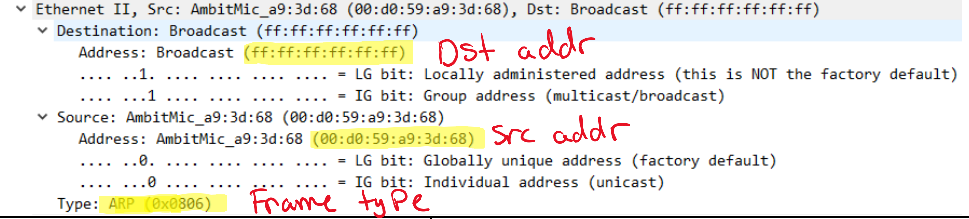
Wireshark Lab 5: Ethernet and ARP

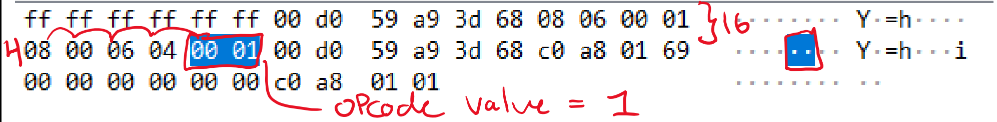
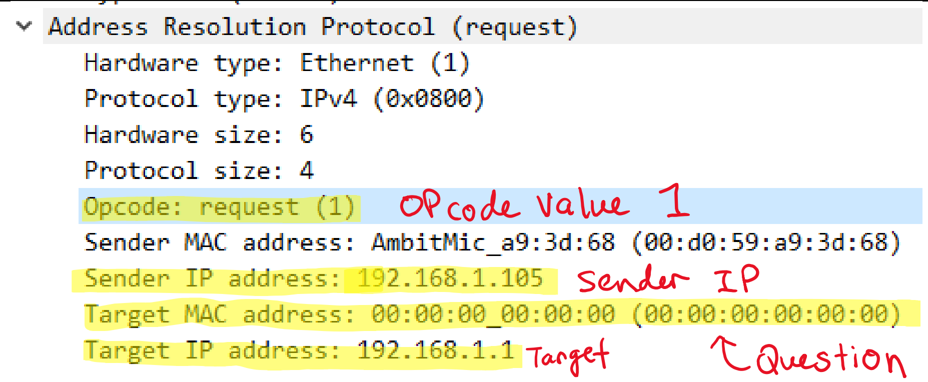
Group Details: Shayshu NR – 1005035196, Johnathan Yan - 1004745476

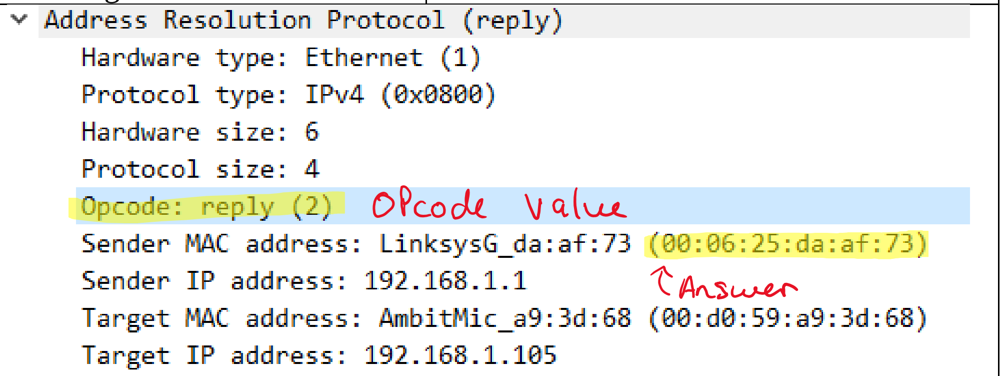
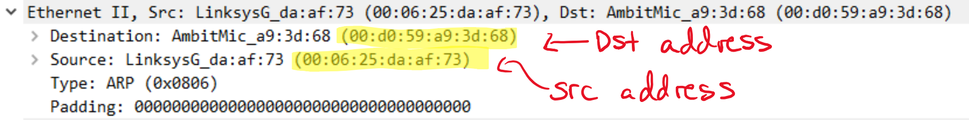
Mark:

	Question	Answer
1	What is the 48-bit Ethernet address of your computer?	The source address is 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) Address: LinksysG_da:af:73 (00:06:25:da:af:73) .... ..0. .... = LG bit: Globally unique address (factory default) ....0 .... = IG bit: Individual address (unicast) Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68) Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68) .... ..0. .... = LG bit: Globally unique address (factory default) ....0 .... = IG bit: Individual address (unicast) Type: IPv4 (0x0800) 	
2	What is the 48-bit destination address in the Ethernet frame? What device has this as its Ethernet address?	The destination address is 00:06:25:da:af:73. This is the address of a LinkSys router.
3	Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?	The frame type is 0x0800, which corresponds to the IP protocol, (in particular IPv4).
4	How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame?	The G appears 54 bytes into the frame. 14 bytes for Ethernet frame, 20 bytes for IP header, and 20 bytes for the TCP header.
Annotated Screenshot (if needed)	 00 06 25 da af 73 00 d0 59 a9 3d 68 08 00 45 00 ··%··s·· Y·=h··E· 02 a0 00 fa 40 00 80 06 bf c8 c0 a8 01 69 80 77 ····@··· ·····i·w f5 0c 04 22 00 50 65 14 99 a7 ac a5 3f b4 50 18 ···"·Pe· ····?·P· fa f0 7e 4f 00 00 47 45 54 20 2f 65 74 68 65 72 ··~O··GE T /ether 	
5	What is the value of the Ethernet source address? What device has this as its	The source address is 00:06:25:da:af:73. This is the ethernet address of the LinkSys router.

	Ethernet address?	
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) Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68) .... ..0. .... = LG bit: Globally unique address (factory default) ....0 .... = IG bit: Individual address (unicast) Source: LinksysG_da:af:73 (00:06:25:da:af:73) Address: LinksysG_da:af:73 (00:06:25:da:af:73) .... ..0. .... = LG bit: Globally unique address (factory default) ....0 .... = IG bit: Individual address (unicast) Type: IPv4 (0x0800) 	
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. This is the ethernet address of my computer.
7	Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?	The frame type is 0x0800, which corresponds to the IP layer, in particular 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?	Again, the O appears 67 bytes into the frame. 14 bytes for the Ethernet header, 20 bytes for the IP header, and 20 bytes for the TCP header, then 14 bytes offset into the segment.
Annotated Screenshot (if needed)	 00 d0 59 a9 3d 68 00 06 25 da af 73 08 00 45 60 ··Y·=h·· %··s··E` 05 dc 8f 2f 40 00 37 06 76 f7 80 77 f5 0c c0 a8 ···/@·7· v··w···· 01 69 00 50 04 22 ac a5 3f b4 65 14 9c 1f 50 10 ·i·P·"·· ?·e···P· 1b 28 5e d0 00 00 48 54 54 50 2f 31 2e 31 20 32 ·(^···HT TP/1.1 2 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 53 61 74 00 OK··D ate: Sat 	
9	Write down the contents of your computer’s ARP cache. What is the meaning of each column value?	The first column is the IP address, the next column is the corresponding physical address (MAC address), and the last column is the type that indicates the protocol type (Static, dynamic, etc…)
Annotated Screenshot (if needed)	 Interface: 10.0.0.230 --- 0x14 Internet Address Physical Address Type 10.0.0.1 80-d0-4a-dd-47-ae dynamic 10.0.0.189 d8-8c-79-97-9d-b6 dynamic 10.0.0.197 8c-49-62-5f-40-79 dynamic 10.0.0.233 d8-8c-79-85-7d-6f dynamic 10.0.0.244 7c-d9-5c-27-93-b8 dynamic 10.0.0.255 ff-ff-ff-ff-ff-ff static 224.0.0.2 01-00-5e-00-00-02 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 224.0.1.60 01-00-5e-00-01-3c static 239.255.3.22 01-00-5e-7f-03-16 static 239.255.255.250 01-00-5e-7f-ff-fa static 239.255.255.251 01-00-5e-7f-ff-fb static 255.255.255.255 ff-ff-ff-ff-ff-ff static 	

<table>
<tr><td>10</td><td>What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?</td><td>The source address is 00:d0:58:a9:3d:68, the destination address is the broadcast address ff:ff:ff:ff:ff:ff.</td></tr>
<tr><td>Annotated Screenshot
(if needed)</td><td colspan="2">
Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), 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: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    ....0 .... = IG bit: Individual address (unicast)
  Type: ARP (0x0806)
</td></tr>
<tr><td>11</td><td>Give the hexadecimal value for the two-byte Ethernet Frame type field.

What upper layer protocol does this correspond to?</td><td>The code is 0x0806, which indicates that the layer protocol is ARP.</td></tr>
<tr><td>12.a</td><td>How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?</td><td>The opcode fields starts 20 bytes into the ARP header.</td></tr>
<tr><td>Annotated Screenshot
(if needed)</td><td colspan="2">
ff ff ff ff ff ff 00 d0 59 a9 3d 68 08 06 00 01   ········ Y·=h····
08 00 06 04 00 01 00 d0 59 a9 3d 68 c0 a8 01 69   ········ Y·=h···i
00 00 00 00 00 00 c0 a8 01 01   ········ ··
</td></tr>
<tr><td>12.b</td><td>What is the value of the opcode field within the ARP-payload part of the
Ethernet frame in which an ARP request is made?</td><td>The value is 1</td></tr>
<tr><td>Annotated Screenshot
(if needed)</td><td colspan="2">
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
</td></tr>
<tr><td>12.c</td><td>Does the ARP message contain the IP address of the sender?</td><td>Yes, in this case it’s 192.168.1.105</td></tr>
<tr><td>12.d</td><td>Where in the ARP request does the “question” appear – the Ethernet
address of the machine whose</td><td>The question is the target MAC address. So, the sender is asking for the MAC address of the device with the target IP address of 192.168.1.1.</td></tr>
</table>

	corresponding IP address is being queried?	
13.a	How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?	Same as the request, the opcode begins at byte 20.
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) Sender MAC address: LinksysG_da:af:73 (00:06:25:da:af:73) Sender IP address: 192.168.1.1 Target MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68) Target IP address: 192.168.1.105	
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
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 answer is the now filled in Sender MAC address, 00:d0:59:a9:3d:68
14	What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?	Source (Gateway): 00:06:25:da:af:73 Destination (my computer): 00:d0:59:a9:3d:68
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: ARP (0x0806) Padding: 000000000000000000000000000000000000	
15	Why is there no ARP reply (sent in response to the ARP request in packet 6) in the packet trace?	There is no reply because the packet has not reached the intended target yet. This packet shows up on wire shark because ARP requests are broadcasted to everyone, but the reply is sent directly to the sender.