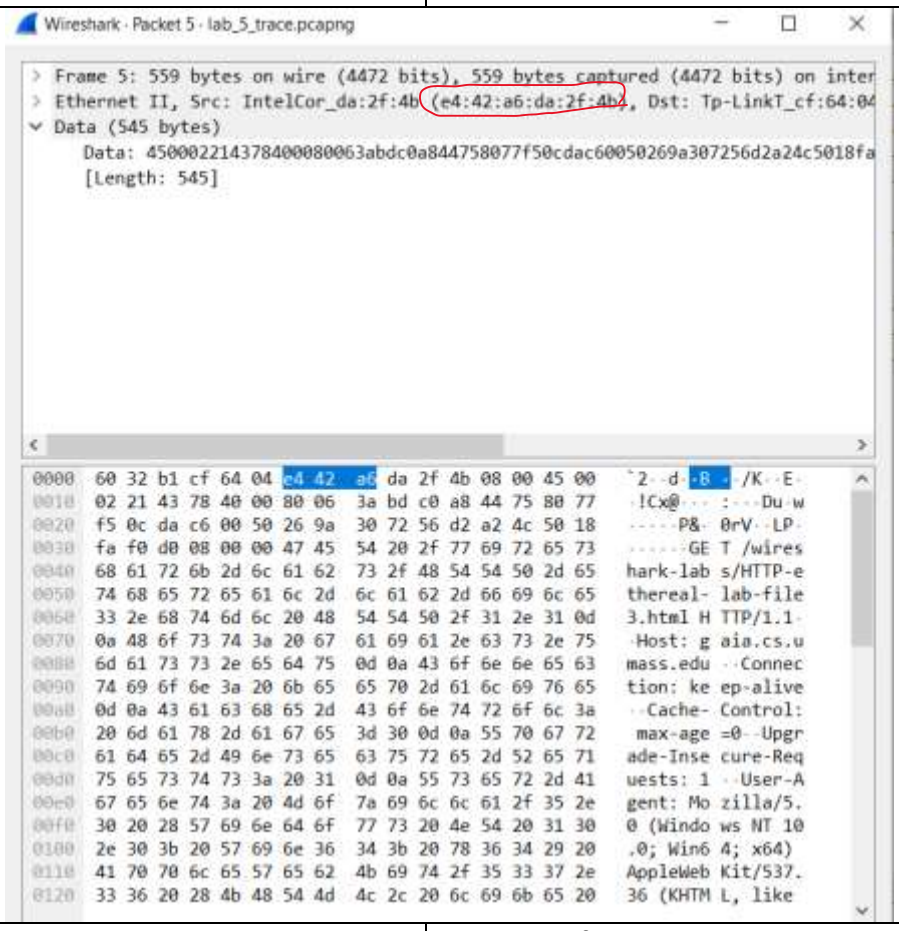
Wireshark Lab 5: Ethernet and ARP

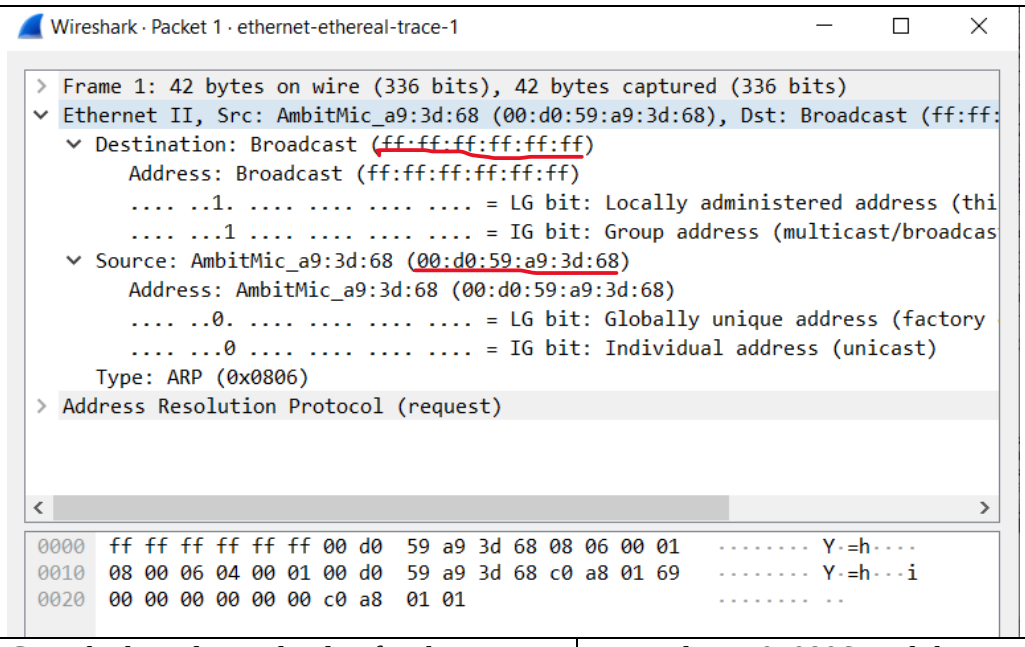
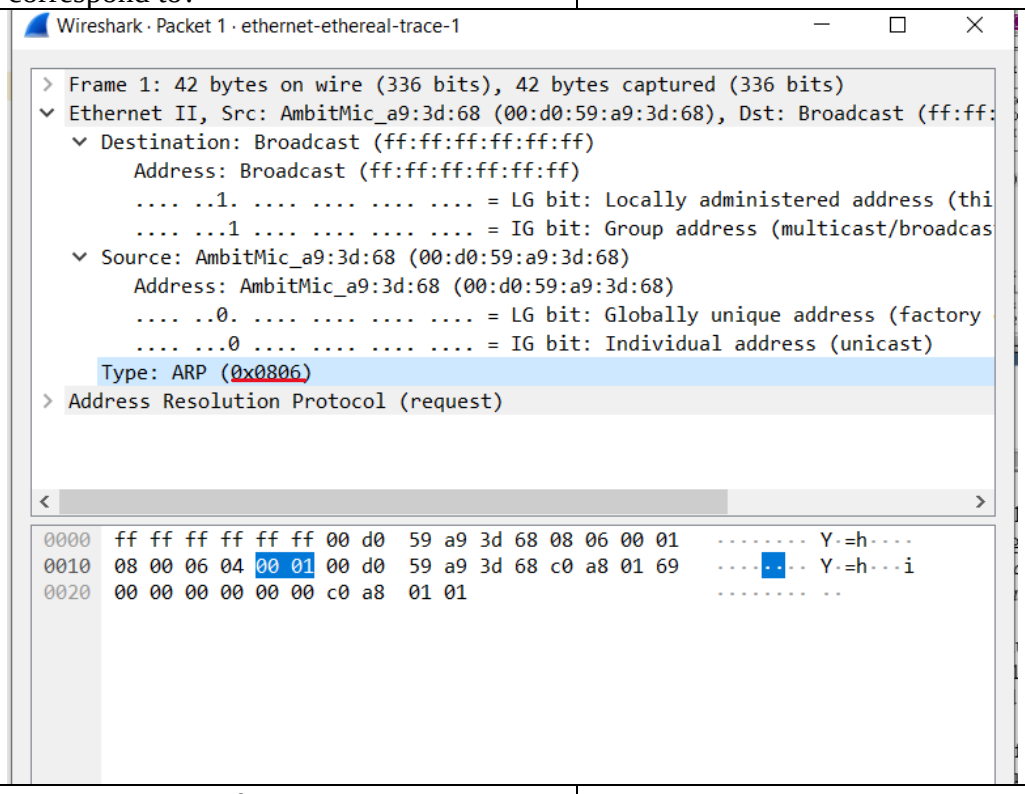
Group Details:
Muhammad Zaheer Hashmi – 1004299056
Hairan Zheng - 1004957601

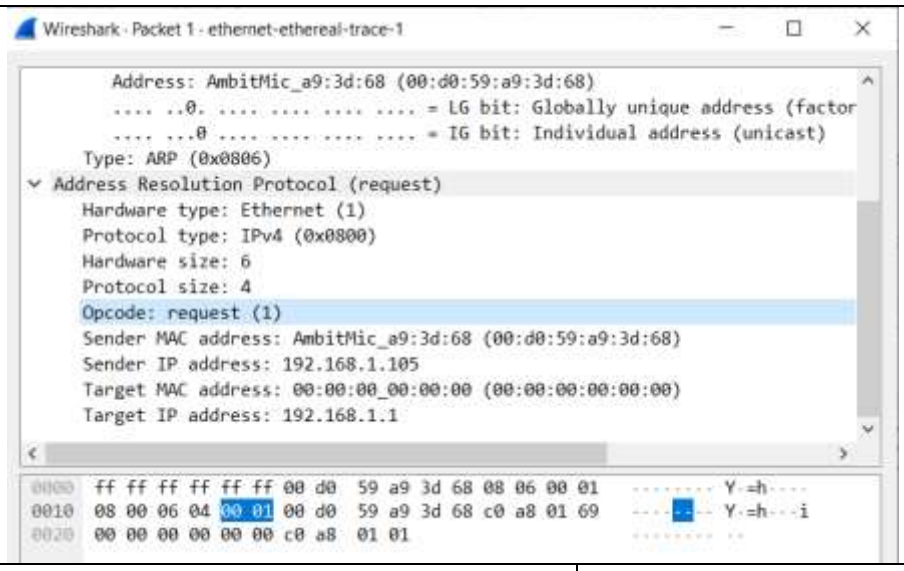
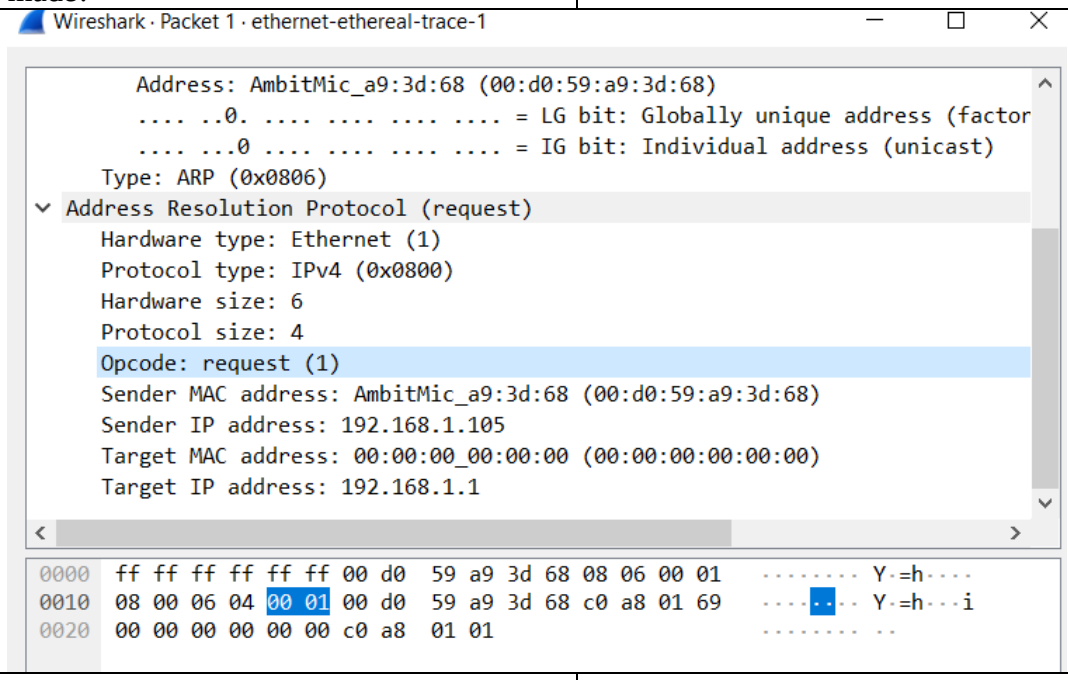
Mark:

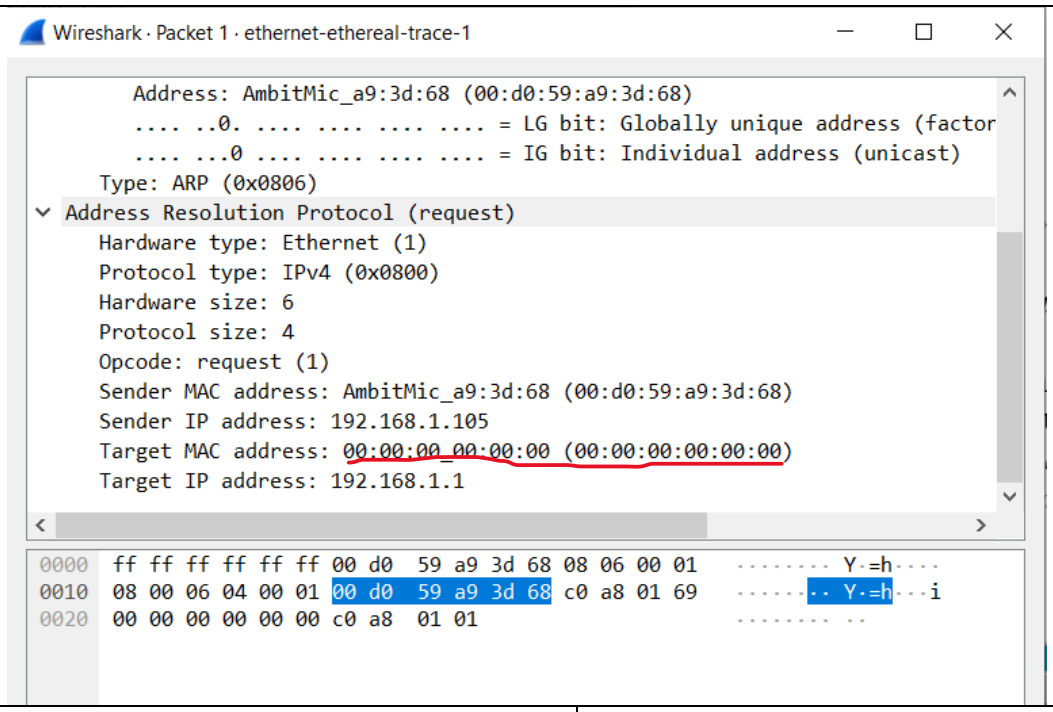
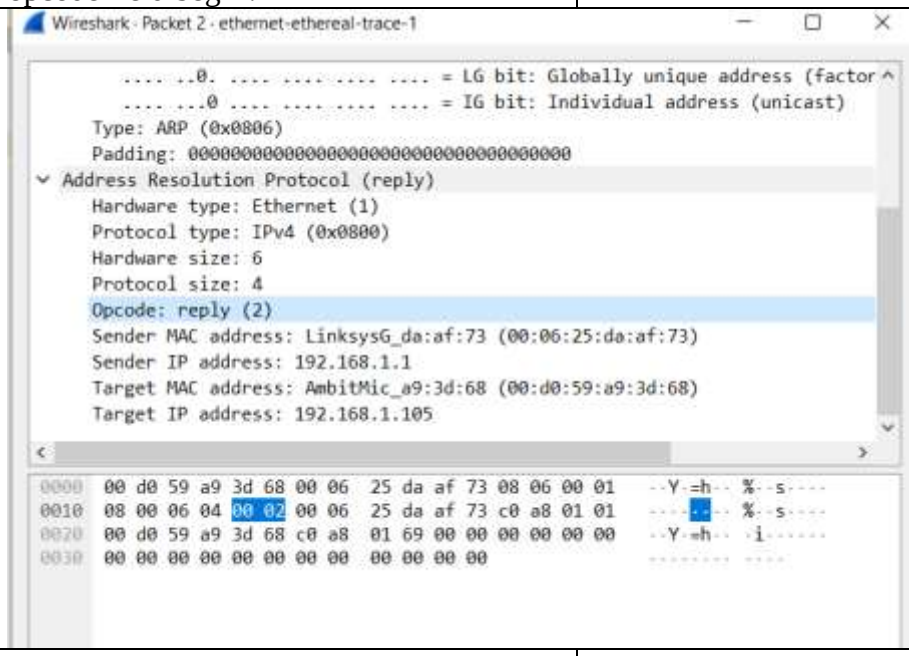
	Question	Answer
1	What is the 48-bit Ethernet address of your computer?	e4:42:a6:da:2f:2b
Annotated Screenshot (if needed)		
2	What is the 48-bit destination address in the Ethernet frame? What device has this as its Ethernet address?	60:32:b1:cf:64:04 Device that has this as its Ethernet address is Tp-LinkT_cf

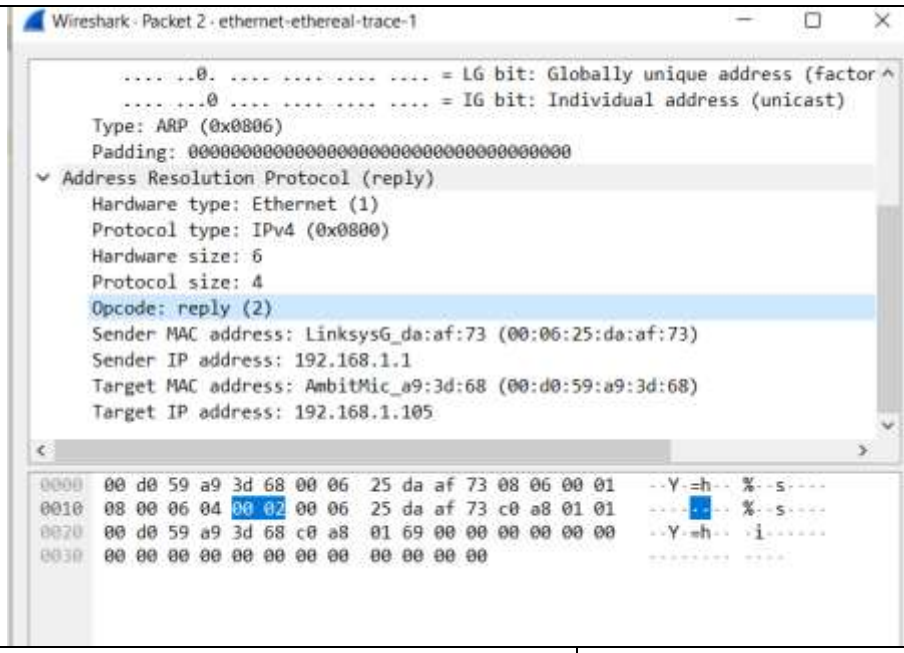
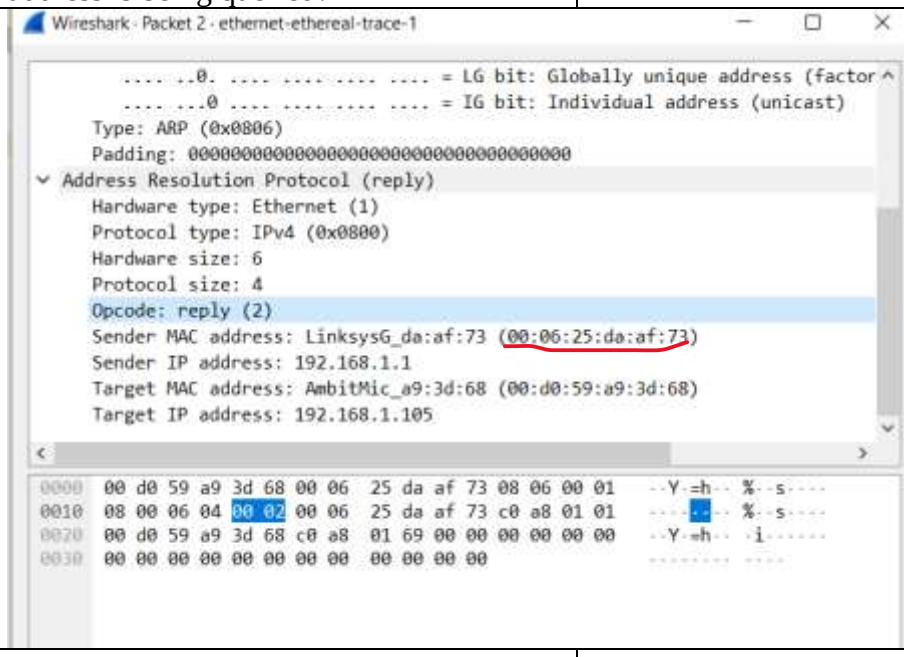
Annotated Screenshot (if needed)	Ethernet II, Src: IntelCor_da:2f:4b (e4:42:a6:da:2f:4b), Dst: Tp-LinkT_cf:64:04 Destination: Tp-LinkT_cf:64:04 (60:32:b1:cf:64:04)	
3	Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?	0x8000 is the hexadecimal value. The upper layer protocol corresponds to IP.
Annotated Screenshot (if needed)	5 0.086457 IntelCor_da:2f:4b Tp-LinkT_cf:64:04 0x0800 559 IPv4	
4	How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame?	14 Bytes of Ethernet Frame data, followed by 20 bytes of IP headers and 20 bytes of TCP (Transport) headers before we can access The G in the http (Application) headers, which is 54 bytes from the start of the Ethernet frame.
Annotated Screenshot (if needed)	 **Data Encapsulation.**	
5	What is the value of the Ethernet source address? What device has this as its Ethernet address?	60:32:b1:cf:64:04 Tp-LinkT_cf has this as its Ethernet Address.
Annotated Screenshot (if needed)	Source: Tp-LinkT_cf:64:04 (60:32:b1:cf:64:04) Address: Tp-LinkT_cf:64:04 (60:32:b1:cf:64:04)	
6	What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?	e4:42:a6:da:2f:4b This is the Ethernet address of my computer.
Annotated Screenshot (if needed)	Destination: IntelCor_da:2f:4b (e4:42:a6:da:2f:4b) Address: IntelCor_da:2f:4b (e4:42:a6:da:2f:4b)	
7	Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?	0x0800 This value corresponds to IP.

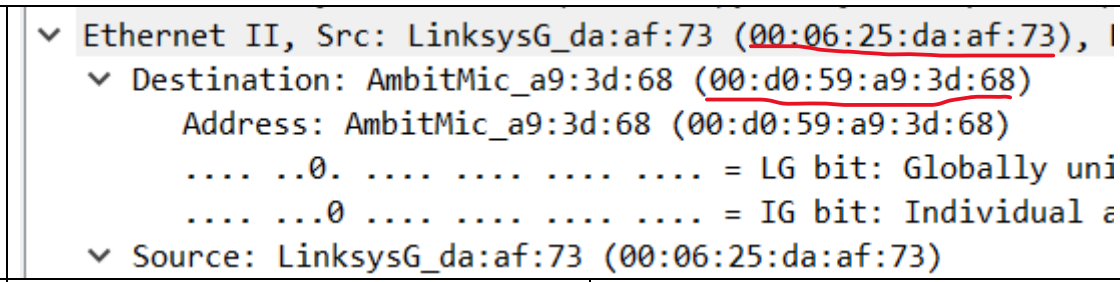
Annotated Screenshot (if needed)	12 0.179349 Tp-LinkT_cf:64:04 IntelCor_da:2f:4b 0x0800 535 IPv4	
8	How many bytes from the very start of the Ethernet frame does the ASCII “O” in “OK” (i.e., the HTTP response code) appear in the Ethernet frame?	HTTP Ok isn’t shown in the Ethernet frame.
Annotated Screenshot (if needed)	0000 e4 42 a0 da 2f 4b 60 32 b1 cf 64 04 08 00 45 00 ·B··/K`2··d··E· 0010 02 09 e9 88 40 00 31 06 e3 c4 80 77 f5 0c c0 a8 ····@·1·····w···· 0020 44 75 00 50 da c6 56 d2 b3 68 26 9a 32 6b 50 18 Du·P··V··h&·2kP· 0030 75 40 64 d1 00 00 68 6d 65 6e 74 73 20 69 6e 66 u@d···hm ents inf 0040 6c 69 63 74 65 64 2e 0a 0a 3c 2f 70 3e 3c 70 3e licted.·· 0050 3c 61 20 6e 61 6d 65 3d 22 39 22 3e 3c 73 74 72 <str 0060 6f 6e 67 3e 3c 68 33 3e 41 6d 65 6e 64 6d 65 6e ong><h3> Amendmen 0070 74 20 49 58 3c 2f 68 33 3e 3c 2f 73 74 72 6f 6e t IX</h3 ></stron 0080 67 3e 3c 2f 61 3e 0a 0a 3c 70 3e 3c 2f 70 3e 3c g>·· < 0090 70 3e 54 68 65 20 65 6e 75 6d 65 72 61 74 69 6f p>The en umeratio 00a0 6e 20 69 6e 20 74 68 65 20 43 6f 6e 73 74 69 74 n in the Constit 00b0 75 74 69 6f 6e 2c 20 6f 66 20 63 65 72 74 61 69 ution, o f certai 00c0 6e 20 72 69 67 68 74 73 2c 20 73 68 61 6c 6c 0a n rights , shall· 00d0 6e 6f 74 20 62 65 20 63 6f 6e 73 74 72 75 65 64 not be c onstrued 00e0 20 74 6f 20 64 65 6e 79 20 6f 72 20 64 69 73 70 to deny or disp 00f0 61 72 61 67 65 20 6f 74 68 65 72 73 20 72 65 74 arage ot hers ret 0100 61 69 6e 65 64 20 62 79 20 74 68 65 20 70 65 6f ained by the peo 0110 70 6c 65 2e 0a 0a 3c 2f 70 3e 3c 70 3e 3c 61 20 ple.··</ p> <a 0120 6e 61 6d 65 3d 22 31 30 22 3e 3c 73 74 72 6f 6e name="10 "><stron	
9	Write down the contents of your computer’s ARP cache. What is the meaning of each column value?	Internet address contains IP column. Physical address contains MAC address. Type indicates protocol type.
Annotated Screenshot (if needed)	Interface: 169.254.55.71 --- 0x6 Internet Address Physical Address Type 169.254.255.255 ff-ff-ff-ff-ff-ff 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	
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?	Hex value is 0x0806, and this 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?	Value is 0x0001
Annotated Screenshot (if needed)		
12.c	Does the ARP message contain the IP address of the sender?	Yes. 192.168.1.105 is our SENDER.
Annotated Screenshot (if needed)	42 Who has 192.168.1.1? Tell 192.168.1.105	
12.d	Where in the ARP request does the "question" appear – the Ethernet address of the machine whose corresponding IP address is being queried?	Ethernet address of target, or the IP address being queried, is set to 0

Annotated Screenshot (if needed)		
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)		
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?	We can find the answer in Sender MAC address, which is 00:06:25:da:af:73
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?	Src: 00:06:25:da:af:73 Dest: 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?	There's no reply because our machine running Wireshark did not send the ARP request in packet 6, thus the reply would not come back to us, but go to the machine that made the request.
Annotated Screenshot (if needed)		

EX-1

```
C:\WINDOWS\system32>arp -s 169.254.255.255 234r
ARP: bad argument: 234r
```

To get a correct InetAddr, I used command arp -a to get all IP to Ethernet mappings and deleted a IP-to-Ethernet mapping. Then I tried to add the mapping back with an invalid Ethernet address, and the result is a bad argument message shown in the command line.

EX-2

```
C:\WINDOWS\system32>netsh interface ipv4 show interfaces

Idx     Met         MTU          State                Name
---  ----------  ----------  ------------  ---------------------------
  9          35        1500  disconnected  VPN - VPN Client
 20          35        1500  connected     Wi-Fi
  1          75  4294967295  connected     Loopback Pseudo-Interface 1
 11          25        1500  disconnected  Local Area Connection* 1
 21          25        1500  disconnected  Local Area Connection* 2
  6          25        1500  connected     Npcap Loopback Adapter


C:\WINDOWS\system32>netsh interface ipv4 show interface 20

Interface Wi-Fi Parameters
----------------------------------------------
IfLuid                             : wireless_32768
IfIndex                            : 20
State                              : connected
Metric                             : 35
Link MTU                           : 1500 bytes
Reachable Time                     : 39000 ms
```

I can find my network interface information through cmd using the above commands and find out that has a reachable time of 39s. In other words, an entry remains in my ARP cache for 39 seconds before being removed.