

z5147986

Lab7

Question marked with (*) must be submitted

1.1

What is the IP address of the client?

192.168.1.100

***1.2**

Consider now the HTTP GET sent from the client to the Google server (whose IP address is IP address 64.233.169.104) at time 7.109267. What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET?

56	7.109267	192.168.1.100	64.233.169.104	HTTP	689	GET / HTTP/1.1
60	7.158797	64.233.169.104	192.168.1.100	HTTP	814	HTTP/1.1 200 OK
62	7.281399	192.168.1.100	64.233.169.104	HTTP	719	GET /intl/en_AL
▼ Frame 56: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits)						
▶ Ethernet II, Src: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f), Dst: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)						
▶ Internet Protocol Version 4, Src: 192.168.1.100, Dst: 64.233.169.104						
▼ Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635						
Source Port: 4335						
Destination Port: 80						

Source IP : TCP port → 192.168.1.100 : 4335

Destination IP : TCP port → 64.233.169.104 : 80

***1.3**

At what time is the corresponding 200 OK HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message?

56	7.109267	192.168.1.100	64.233.169.104	HTTP	689	GET / HTTP/1.1
60	7.158797	64.233.169.104	192.168.1.100	HTTP	814	HTTP/1.1 200 OK (text/html)
62	7.281399	192.168.1.100	64.233.169.104	HTTP	719	GET /intl/en_ALL/images/logo
▼ Frame 60: 814 bytes on wire (6512 bits), 814 bytes captured (6512 bits)						
▶ Ethernet II, Src: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b), Dst: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f)						
▶ Internet Protocol Version 4, Src: 64.233.169.104, Dst: 192.168.1.100						
▼ Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 2861, Ack: 636, Len: 760						
Source Port: 80						
Destination Port: 4335						

Time → 7.158797

Source IP : TCP port → 64.233.169.104 : 80

Destination IP : TCP port → 192.168.1.100 : 4335

1.4

Recall that before a GET command can be sent to an HTTP server, TCP must first set up a connection using the three-way SYN/ACK handshake. At what time is the client-to-server TCP SYN segment sent that sets up the connection used by the GET sent at time 7.109267? What are the source and destination IP addresses and source and destination ports for the TCP SYN segment?

53	7.075657	192.168.1.100	64.233.169.104	TCP	66	4335 → 80 [SYN] Seq=0 W
54	7.108986	64.233.169.104	192.168.1.100	TCP	66	80 → 4335 [SYN, ACK] Se
55	7.109053	192.168.1.100	64.233.169.104	TCP	54	4335 → 80 [ACK] Seq=1 A
56	7.109267	192.168.1.100	64.233.169.104	HTTP	689	GET / HTTP/1.1
▼ Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 0, Len: 0						
Source Port: 4335						
Destination Port: 80						

Time → 7.075657

Source IP : TCP port → 192.168.1.100 : 4335

Destination IP : TCP port → 64.233.169.104 : 80

z5147986

Lab7

1.5

What are the source and destination IP addresses and source and destination ports of the ACK sent in response to the SYN. At what time is this SYN/ACK received at the client?

54	7.108986	64.233.169.104	192.168.1.100	TCP	66	80 → 4335 [SYN, ACK]
55	7.109053	192.168.1.100	64.233.169.104	TCP	54	4335 → 80 [ACK] Seq=
56	7.109267	192.168.1.100	64.233.169.104	HTTP	689	GET / HTTP/1.1

Frame 54: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b), Dst: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f)
Internet Protocol Version 4, Src: 64.233.169.104, Dst: 192.168.1.100
Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 0, Ack: 1, Len: 0
Source Port: 80
Destination Port: 4335

Time → 7.108986

Source IP : TCP port → 64.233.169.104 : 80

Destination IP : TCP port → 192.168.1.100 : 4335

1.6

Find the HTTP GET message that was sent from the client to the Google server at time 7.102967 (where t=7.109267 is time at which this was sent as recorded in the NAT_home_side trace file). At what time does this message appear in the NAT_ISP_side trace file?

85	6.069168	71.192.34.104	64.233.169.104	HTTP	689	GET / HTTP/1.1
----	----------	---------------	----------------	------	-----	----------------

Time → 6.069168

*1.7

What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET message (as recorded in the NAT_ISP_side trace file)? Which of these fields are the same, and which are different, than in your answer to Question 2 above?

85	6.069168	71.192.34.104	64.233.169.104	HTTP	689	GET / HTTP/1.1
86	6.092755	Cisco_bf:6c:01	Broadcast	ARP	60	Who has 71.192.34.104

Frame 85: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits) on interface 0
Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01)
Internet Protocol Version 4, Src: 71.192.34.104, Dst: 64.233.169.104
Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635
Hypertext Transfer Protocol
GET / HTTP/1.1
Host: www.google.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.0.14) Gecko/20090227 Firefox/3.0.14 (.NET CLR 3.5.30729)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive

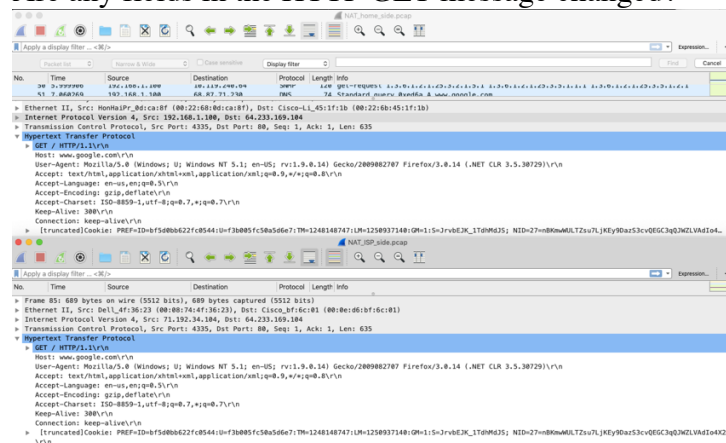
Source IP : TCP port → 71.192.34.104 : 4335

Destination IP : TCP port → 64.233.169.104 : 80

Only the Destination IP, Destination TCP port are the same.

1.8

Are any fields in the HTTP GET message changed?



All the fields are the same

z5147986

Lab7

*1.9

Which of the following fields in the IP datagram carrying the HTTP GET are changed:
Version, Header Length, Flags, Checksum. If any of these fields have changed, give a reason
(in one sentence) stating why this field needed to change.

The image shows two Wireshark packet capture windows. The top window, titled 'NAT_home_side.pcap', displays packet 56, which is an Internet Protocol Version 4 (IPv4) packet. The packet details pane shows the following fields: Version: 4, Header Length: 20 bytes (5), Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT), Total Length: 675, Identification: 0xa2ac (41644), Flags: 0x4000, Don't fragment, Time to live: 128, Protocol: TCP (6), Header checksum: 0xa94a [validation disabled], [Header checksum status: Unverified], Source: 192.168.1.100, and Destination: 64.233.169.104. The bottom window, titled 'NAT_ISP_side.pcap', displays packet 90, which is also an Internet Protocol Version 4 (IPv4) packet. The packet details pane shows the following fields: Version: 4, Header Length: 20 bytes (5), Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT), Total Length: 675, Identification: 0xa2ac (41644), Flags: 0x4000, Don't fragment, Time to live: 127, Protocol: TCP (6), Header checksum: 0x022f [validation disabled], [Header checksum status: Unverified], Source: 71.192.34.104, and Destination: 64.233.169.104.

No.	Time	Source	Destination	Protocol	Length	Info
56	0.9999900	192.168.1.100	10.119.240.04	IPv4	120	get-request 1.3.0..

Frame 56: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits)

Ethernet II, Src: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f), Dst: Cisco-Li_45:1f:1b (00:22:6b:45:1f)

Internet Protocol Version 4, Src: 192.168.1.100, Dst: 64.233.169.104

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 675
- Identification: 0xa2ac (41644)
- Flags: 0x4000, Don't fragment
- Time to live: 128
- Protocol: TCP (6)
- Header checksum: 0xa94a [validation disabled]
- [Header checksum status: Unverified]
- Source: 192.168.1.100
- Destination: 64.233.169.104

No.	Time	Source	Destination	Protocol	Length	Info
90	6.117570	71.192.34.104	64.233.169.104	HTTP	814	HTTP/1.1 200 OK (text/html)

Version → same

Header Length → same

Flags → same

Header Checksum → different

IP Header Checksum is recalculated every time the IP header (source IP) is changed

1.10

In the NAT_ISP_side trace file, at what time is the first 200 OK HTTP message received from the Google server?

90 6.117570 64.233.169.104 71.192.34.104 HTTP 814 HTTP/1.1 200 OK (text/html)

Time → 6.117570

z5147986

Lab7

*1.11

What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message? Which of these fields are the same, and which are different than your answer to Question 3 above?

90	6.117570	64.233.169.104	71.192.34.104	HTTP	814	HTTP/1.1 200 OK (text/html)
91	6.118515	71.192.34.104	64.233.169.104	TCP	60	4335 → 80 [ACK] Seq=636 Ack=3
92	6.162091	169.254.247.145	169.254.255.255	NBNS	92	Name query NB HPAB9D4C<00>
93	6.044557	71.192.34.104	64.233.169.104	TCP	66	80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM=1 WS=64

Frame 90: 814 bytes on wire (6512 bits), 814 bytes captured (6512 bits) on interface 0
Ethernet II, Src: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
Internet Protocol Version 4, Src: 64.233.169.104, Dst: 71.192.34.104
Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 2861, Ack: 636, Len: 760
Source Port: 80
Destination Port: 4335

Source IP : TCP port → 64.233.169.104 : 80

Destination IP : TCP port → 71.192.34.104 : 4335

Only the Destination IP, Destination TCP port are different

1.12

In the NAT_ISP_side trace file, at what time were the client-to-server TCP SYN segment and the server-to-client TCP SYN/ACK segment corresponding to the segments in Question 4 and 5 above captured?

82	6.035475	71.192.34.104	64.233.169.104	TCP	66	4335 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK_PERM=1
83	6.067775	64.233.169.104	71.192.34.104	TCP	66	80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM=1 WS=64

Client-to-server TCP SYN time → 6.035475

Server-to-client TCP SYN/ACK → 6.067775

*1.13

What are the source and destination IP addresses and source and destination ports for these two segments (TCP SYN and TCP SYN/ACK)? Which of these fields are the same, and which are different than your answer to Question 4 and 5 above?

82	6.035475	71.192.34.104	64.233.169.104	TCP	66	4335 → 80 [SYN]
----	----------	---------------	----------------	-----	----	-----------------

Frame 82: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01)
Internet Protocol Version 4, Src: 71.192.34.104, Dst: 64.233.169.104
Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 0, Len: 0
Source Port: 4335
Destination Port: 80

TCP SYN

Source IP : TCP port → 71.192.34.104 : 4335

Destination IP : TCP port → 64.233.169.104 : 80

83	6.067775	64.233.169.104	71.192.34.104	TCP	66	80 → 4335 [SYN, ACK]
----	----------	----------------	---------------	-----	----	----------------------

Frame 83: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
Internet Protocol Version 4, Src: 64.233.169.104, Dst: 71.192.34.104
Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 0, Ack: 1, Len: 0
Source Port: 80
Destination Port: 4335

TCP SYN/ACK

Source IP : TCP port → 64.233.169.104 : 80

Destination IP : TCP port → 71.192.34.104 : 4335

The Destination IP : TCP port (TCP SYN) and Source IP : TCP port (TCP SYN/ACK) for ISP are the **same** as the Destination IP : TCP port (TCP SYN) and Source IP : TCP port (TCP SYN/ACK) for Home.

The Source IP: TCP port (TCP SYN) and Destination IP : TCP port (TCP SYN/ACK) for ISP are **different** from the Source IP : TCP port (TCP SYN) and Destination IP : TCP port (TCP SYN/ACK) for Home.

z5147986

Lab7

*1.14

The discussion on NAT in the Week 7 lecture slide No 80 shows the NAT translation table used by a NAT router. Using your answers to the questions above, fill in the NAT translation table entries for the HTTP connection considered in the questions above.

WAN side addr → 71.192.34.104, 4335

LAN side addr → 192.168.1.100, 4335

Steps	Source	Destination
1. host sends	192.168.1.100, 4335	64.233.169.104, 80
2. NAT router changes	71.192.34.104, 4335	64.233.169.104, 80
3. Reply arrives	64.233.169.104, 80	71.192.34.104, 4335
4. NAT router changes	64.233.169.104, 80	192.168.1.100, 4335

1.15

The trace files investigated above have additional connections to Google servers above and beyond the HTTP GET, 200 OK request/response studied above. For example, in the NAT_home_side trace file, consider the client-to-server GET at time 1.572315, and the GET at time 7.573305. Research the use of these two HTTP messages and safe browsing in general. Explain your findings in a concise manner.

13	1.528648	74.125.91.113	192.168.1.100	HTTP	853	[TCP Spurious Retransmission] HTTP/1.1 200 OK
Transmission Control Protocol, Src Port: 80, Dst Port: 4330, Seq: 1, Ack: 982, Len: 799						
Hypertext Transfer Protocol						
HTTP/1.1 200 OK\r\n						
[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]						
Response Version: HTTP/1.1						
Status Code: 200						
[Status Code Description: OK]						
Response Phrase: OK						
Content-Type: application/vnd.google.safebrowsing-update\r\n						
Date: Sun, 20 Sep 2009 20:43:01 GMT\r\n						
Server: Chunked Update Server\r\n						
Content-Length: 633\r\n						
\r\n						
104	7.573305	192.168.1.100	74.125.91.113	HTTP	709	GET /generate_204 HTTP/1.1
Hypertext Transfer Protocol						
GET /generate_204 HTTP/1.1\r\n						
[Expert Info (Chat/Sequence): GET /generate_204 HTTP/1.1\r\n]						
Request Method: GET						
Request URI: /generate_204						
Request Version: HTTP/1.1						
Host: clients1.google.com\r\n						
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.0.14) Gecko/2009082707 Firefox/3.0.14 (.NET CLR 3.5.30729)\r\n						
Accept: image/png,image/*;q=0.8,*/*;q=0.5\r\n						
Accept-Language: en-us,en;q=0.5\r\n						
Accept-Encoding: gzip,deflate\r\n						
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n						
Keep-Alive: 300\r\n						
Connection: keep-alive\r\n						
Referer: http://www.google.com/\r\n						
[truncated]Cookie: PREF=ID=bfd5d0bb622fc0544;U=f3b005fc50a5d6e7;TM=1248148747;LM=1250937140;GM=1;S=jrvbEJK_1TdHmDJS;NID=27=nBkmwWULTZsu7LjKEy9DazS3cvQEGC3qQJWZLVadIo4X2;\r\n						

Google safe browsing is a blacklist service that provides list of URLs for web resources that contain malware or phishing content.

According to [stackoverflow](#) it returns generate_204 if WLAN is open, no response if closed or blocked if redirect to captive portal (A **captive portal** is a Web page that the user of a public-access **network** is obliged to view and interact with before access is granted) is present and based on the [http status](#) 204 No Content is not the same since there is no Etag header in the response

z5147986

Lab7

2.1

What is the 48-bit Ethernet address of the source host of this packet?

10	17.466468	192.168.1.105	128.119.245.12	HTTP	686	GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
11	17.494766	128.119.245.12	192.168.1.105	TCP	60	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0
12	17.498935	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=1460 [TCP segment]

Frame 10: 686 bytes on wire (5488 bits), 686 bytes captured (5488 bits)
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)

00:06:25:da:af:73

*2.2

What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? If not, then which device has this address? (Note: this is an important question, and one that students sometimes get wrong. You may want to refer back to relevant parts of the text and lecture notes and make sure you understand the answer here.)

16	17.527422	128.119.245.12	192.168.1.105	HTTP	489	HTTP/1.1 200 OK (text/html)
17	17.527457	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=633 Ack=4

Frame 16: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
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)

00:d0:59:a9:3d:68

No it does not.

This is the MAC address to the switch in the subnet

2.3

Give the hexadecimal value for the two-byte Frame type field.

0x0800 IP(v4)

*2.4

How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame? Note that when you examine the Data portion of this frame, it actually consists of both the Ethernet frame headers as well as the payload (i.e. bottom window in Wireshark shows the entire 686 byte frame that is captured). Of the bytes preceding the G, the first few bytes are the Ethernet frame header. Does this include the preamble bytes, or are those bytes omitted from the capture? Given this, how many bytes of frame header are present? What are the remainder of the bytes before the G?

0030	fa f0 7e 4f 00 00	47 45 54 20 2f 65 74 68 65 72	...0...GET /ether
------	-------------------	-------------------------------	-------------------

0x37, $3 * 16 + 7 = 55$ bytes away from the start of the Ethernet frame

Preamble bytes not included.

$686 - 672 = 14$ bytes

Bytes before G = $55 - 14 = 41$ bytes

*2.5

What is the value of the Ethernet source address? Is this the address of the host that sent the GET HTTP request, or of gaia.cs.umass.edu? If not then which device has this address?

16	17.527422	128.119.245.12	192.168.1.105	HTTP	489	HTTP/1.1 200 OK (text/html)
17	17.527457	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=633 Ack=4

Frame 16: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
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)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.105
Transmission Control Protocol, Src Port: 80, Dst Port: 1058, Seq: 4381, Ack: 633, Len: 435
Source Port: 80
Destination Port: 1058

00:06:25:da:af:73

The address above is not the address of the host and not gaia.cs.umass.edu.
It is a MAC address belong to the switch in the subnet

z5147986

Lab7

2.6

What is the destination address in the Ethernet frame? Is this the Ethernet address of the source host that sent the earlier GET HTTP request?

00:d0:59:a9:3d:68

Yes

2.7

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?

0x07, 7 bytes

z5147986

Lab7

*3.1

What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message? Is there something special about the destination address?

1	0.000000	AmbitMic_a9:3d:68	Broadcast	ARP
Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0 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)				
Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)				
2	0.001018	LinksysG_da:af:73	AmbitMic_a9:3d:68	ARP
Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0 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)				

No.	Source	Destination
1	00:d0:59:a9:3d:68	ff:ff:ff:ff:ff:ff
2	00:06:25:da:af:73	00:d0:59:a9:3d:68

3.2

Give the hexadecimal value for the two-byte Ethernet Frame type field.

0x0806, ARP

3.3

How many bytes from the very beginning of the Ethernet frame does the ARP *opcode* field begin?

? I don't get this ?

3.4

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 of opcode field → request (1)

3.5

Does the ARP request message contain the IP address of the sender?

Yes

*3.6

Where in the ARP request does the “question” (IP address for which the mapping is being requested) appear?

Target IP address → 192.168.1.1

3.7

How many bytes from the very beginning of the Ethernet frame does the ARP *opcode* field begin?

? I don't get this ?

z5147986

Lab7

***3.8**

What is the value of the *opcode* field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

Value of opcode field → reply (2)

***3.9**

Where in the ARP message does the “answer” to the earlier ARP request appear – the Ethernet address of the machine whose corresponding IP address is being queried?

Target IP address → 192.168.1.105

***3.10**

What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?

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																	
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	00	00	00	00
Target MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)																	
Target IP address: 192.168.1.105																	
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	00	00	00	00

Source → 00:06:25:da:af:73

Destination → 00:d0:59:a9:3d:68