

WIRESHARK ASSIGNMENT

Computer Networks

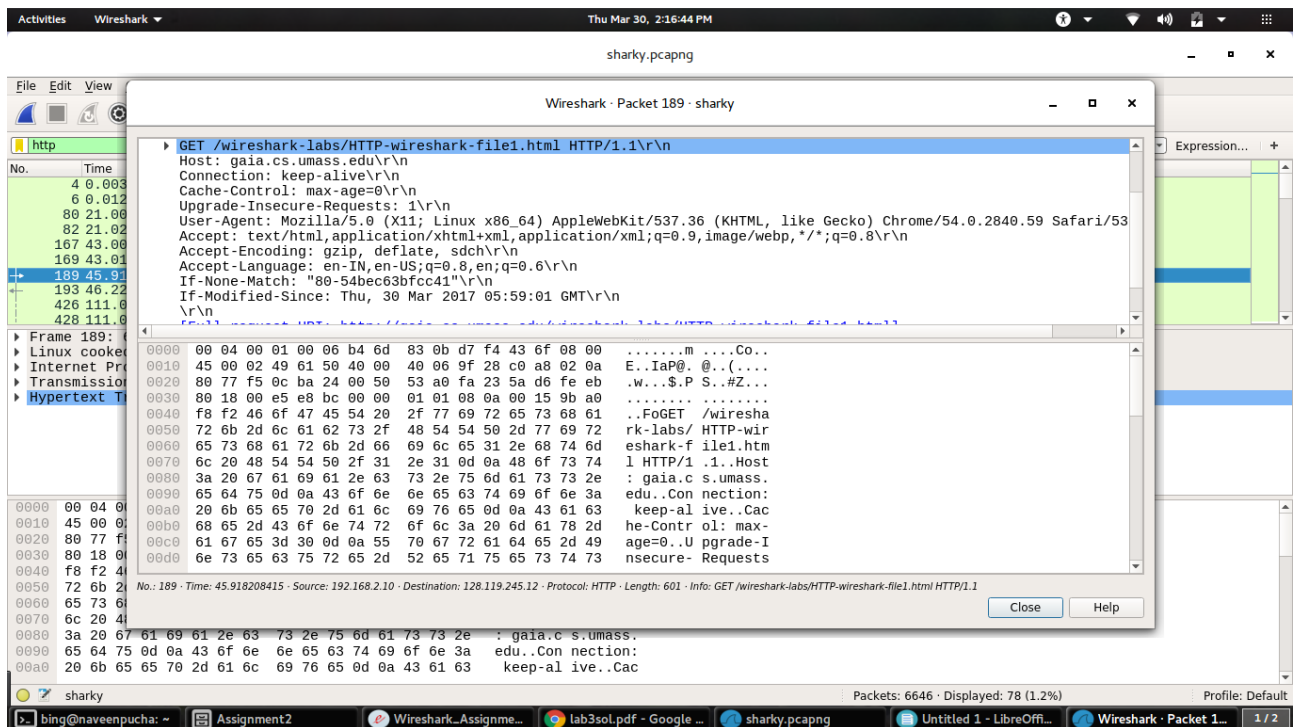
Sai Naveen Pucha

201502013

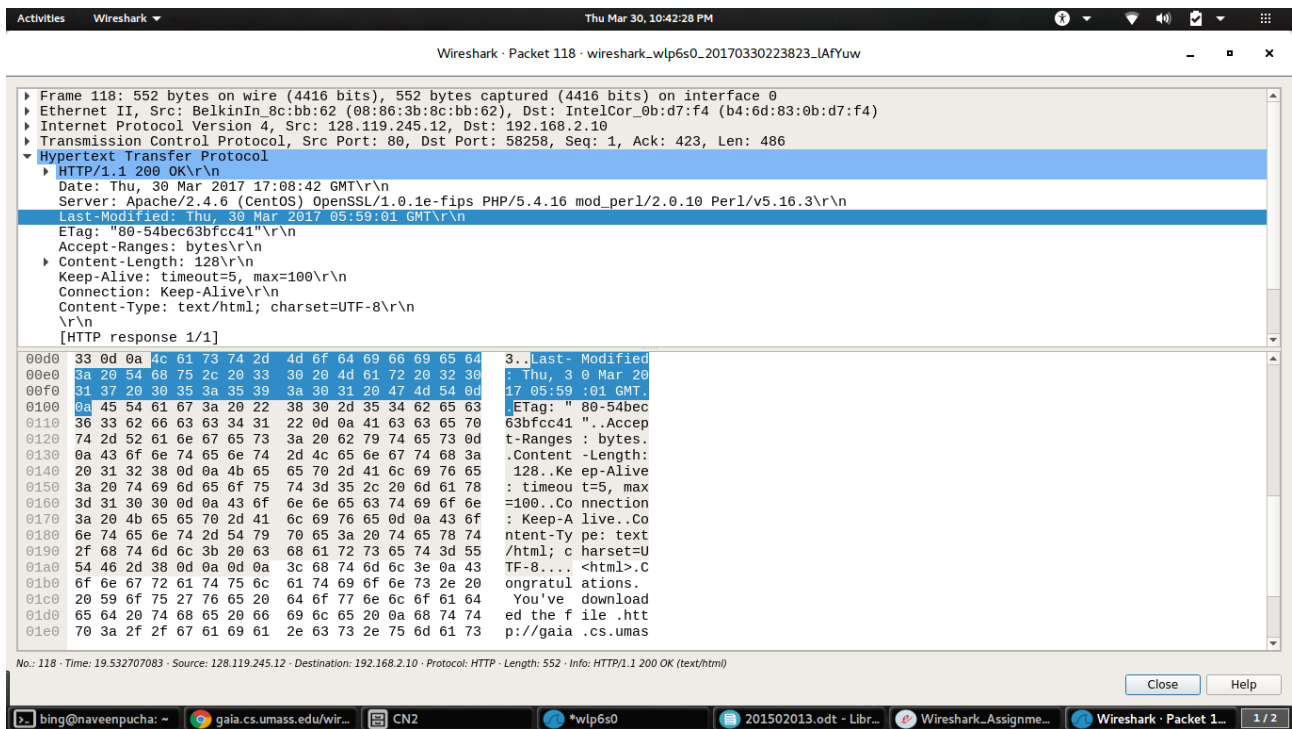
PART 1

A

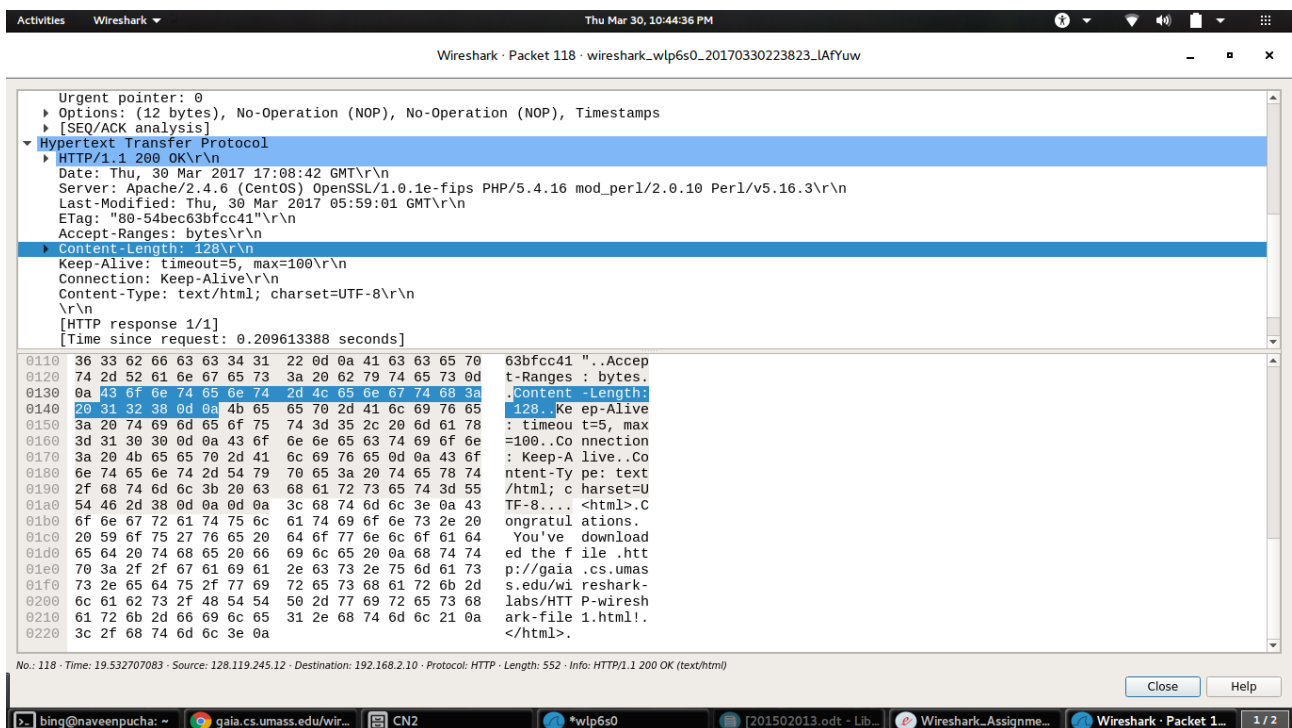
- 1) My browser is running http version 1.1. My server is running http 1.1 .
Accept-Language : en-IN, en-US; q=0.8,en; q=0.6\r\n



- 2) The IP address of my computer is 192.168.2.10(this is a virtual address assigned)
The IP address of the gaia.cs.umass.edu server is 128.119.245.12
- 3) 200 is the status code returned from the server to my browser
- 4) The file is last modified on Thu, 30 Mar 2017 05:59:01 GMT\r\n



5) The content length is 128 bytes

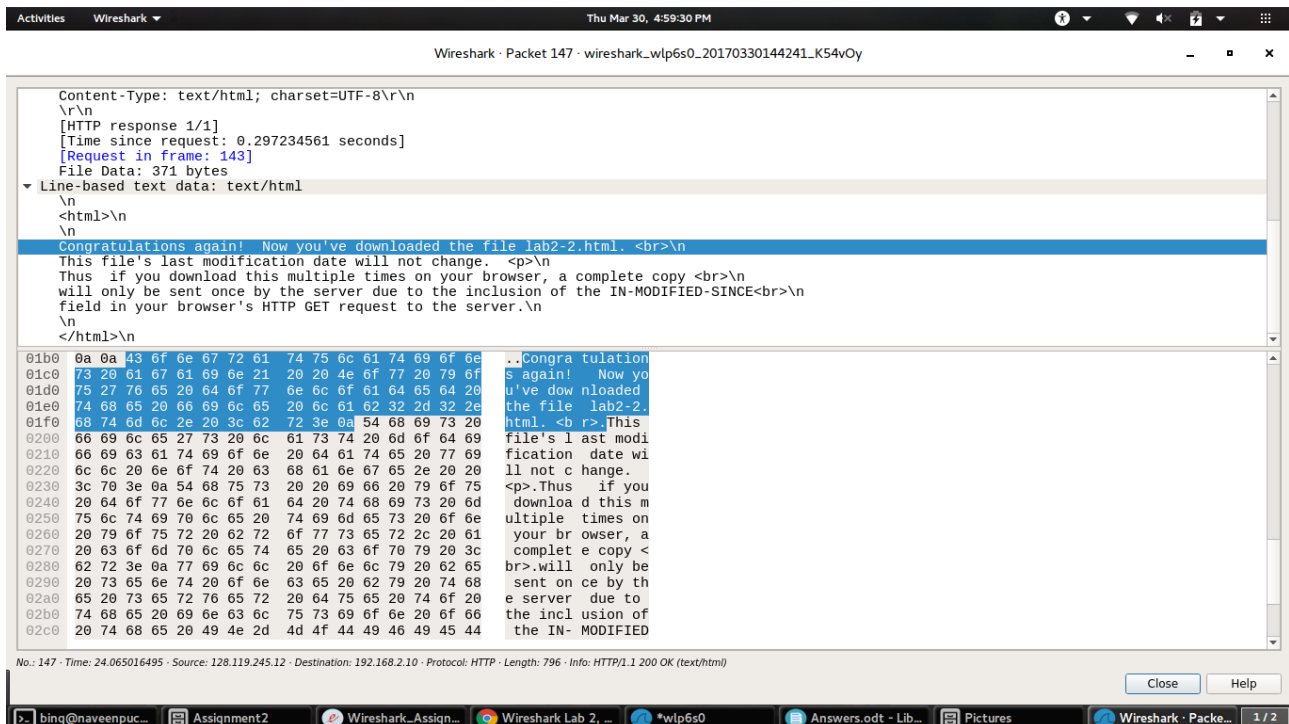


6) No, the raw data appears to match up exactly with what is shown in the packet-listing window.

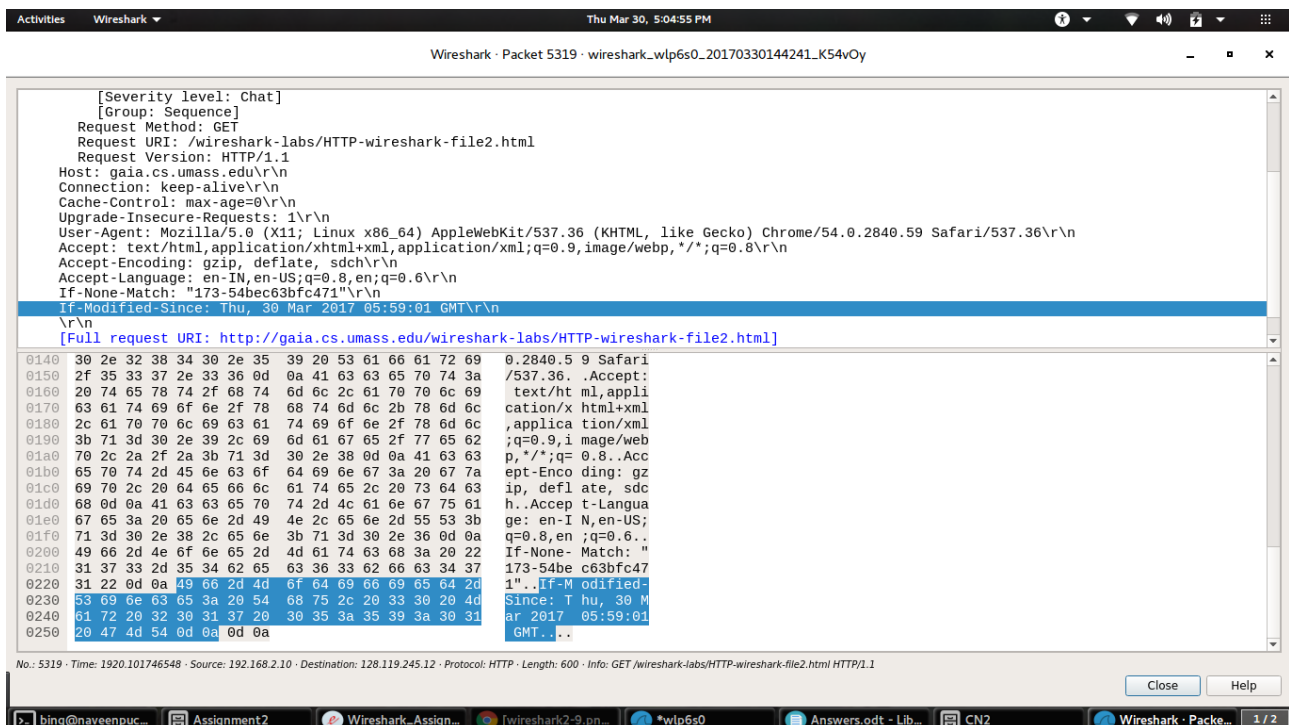
B

7) There is no IF-MODIFIED-SINCE line in the HTTP GET in the GET message.

8) The server did return the contents of the file. There is section “Line-Based Text Data” which has what the server has sent back to the browser as shown in the screenshot.

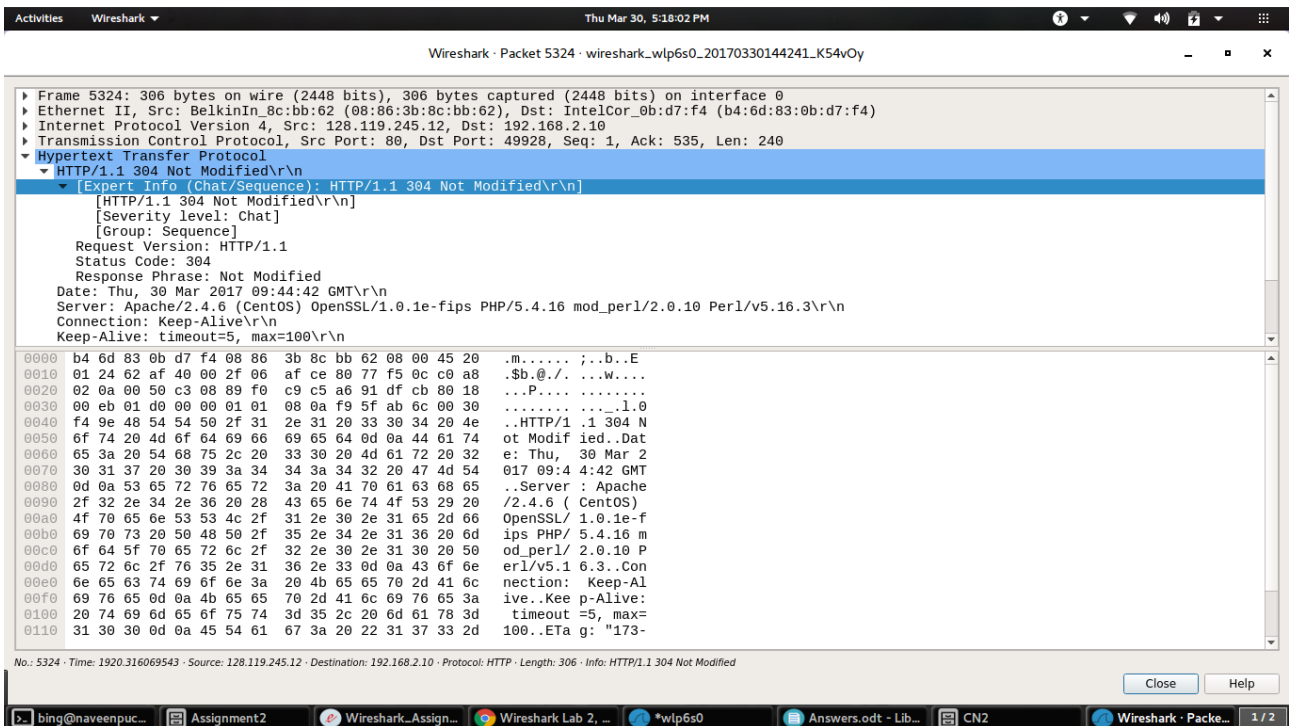


9) Yes
If-Modified-Since: Thu, 30 Mar 2017 05:59:01 GMT\r\n



10) The http status code for this is 304: Not Modified

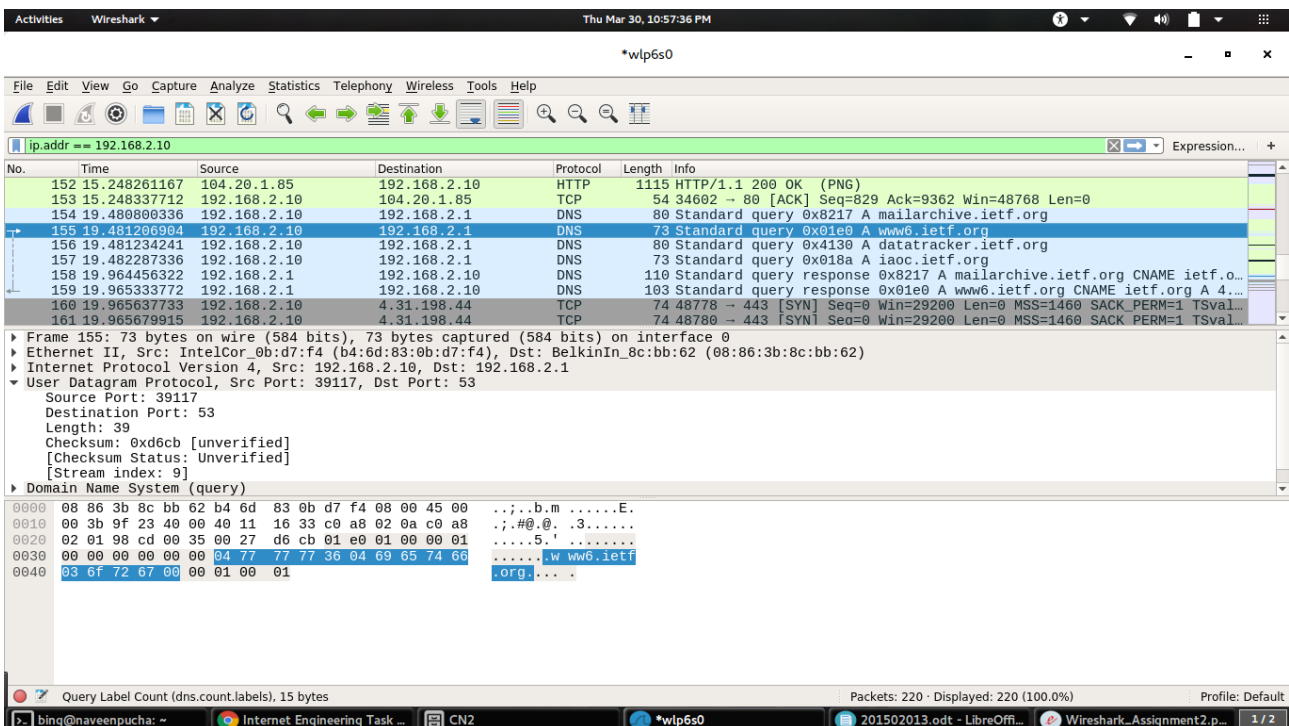
The server did not return the contents of the file because the browser simply retrieved the contents from its cache. If the file had been modified since it was last accessed, it might have returned the contents of the file. Check the below screenshot for reference.



PART 2

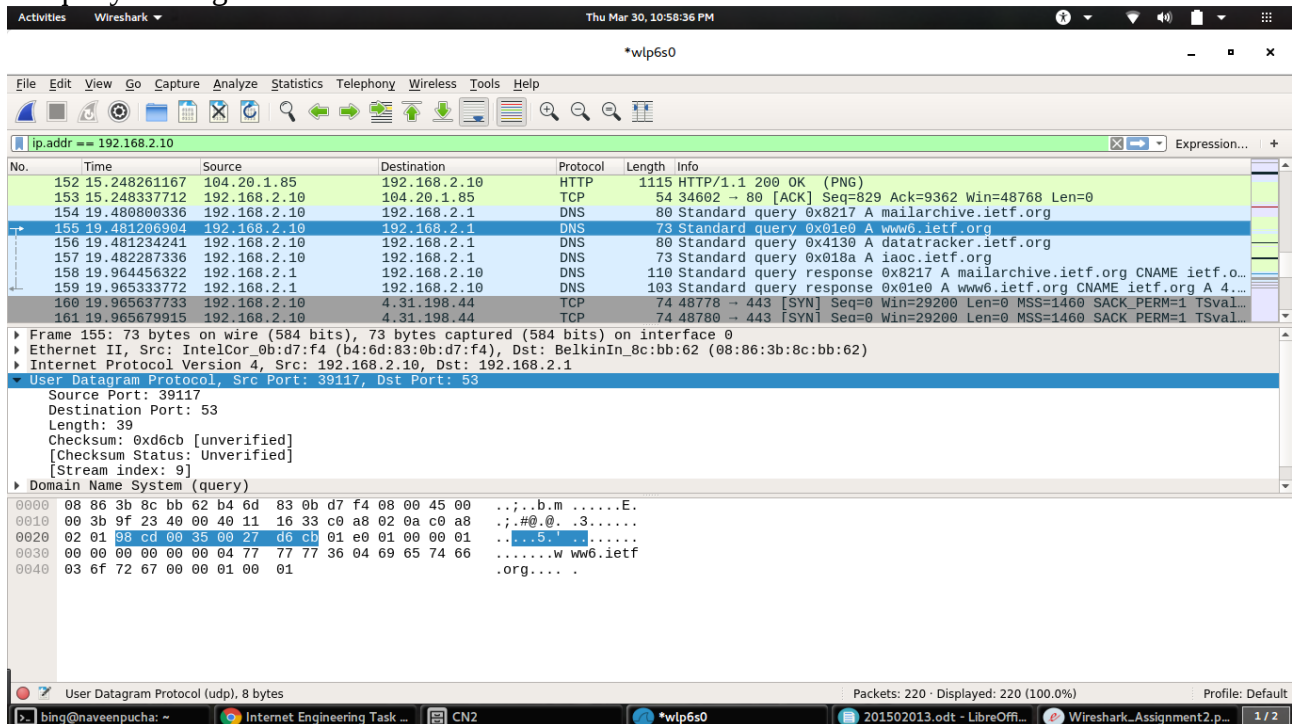
A

1) Related to the DNS query the response messages are sent over UDP

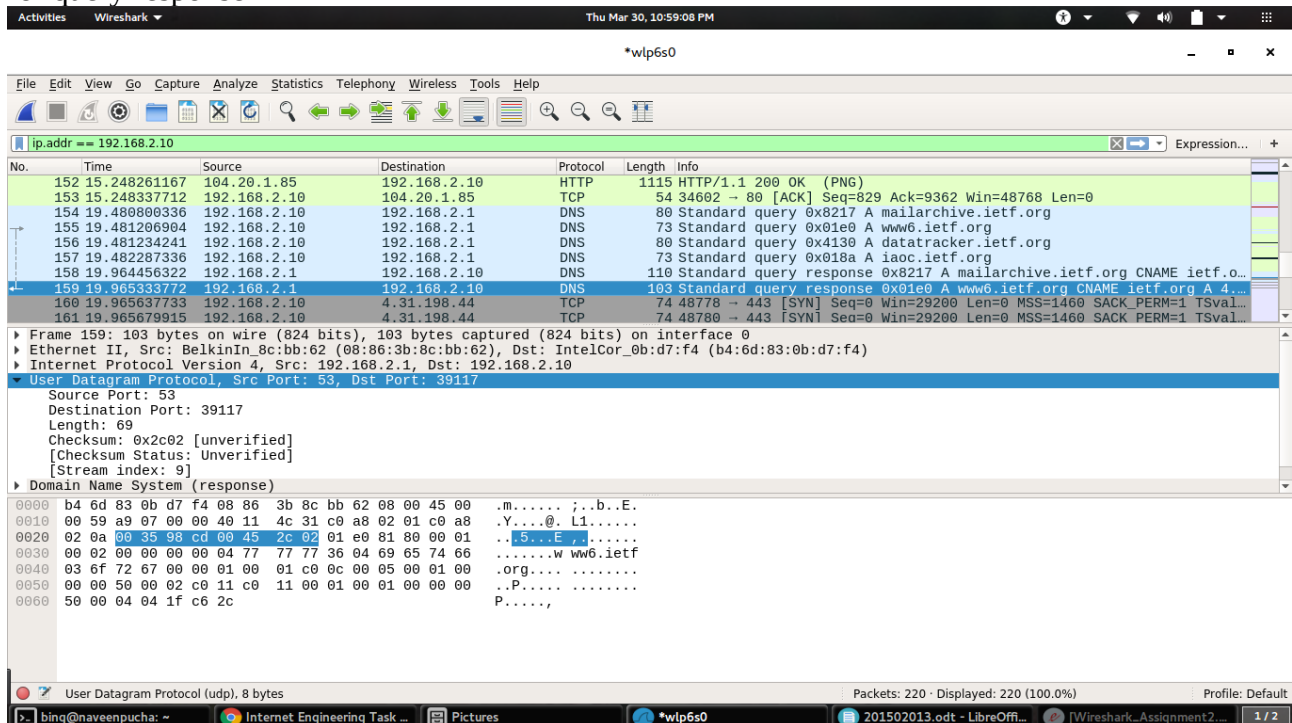


2) Destination Port : 53 for query message Source Port : 53 for query response Check below screenshots for reference.

for query message

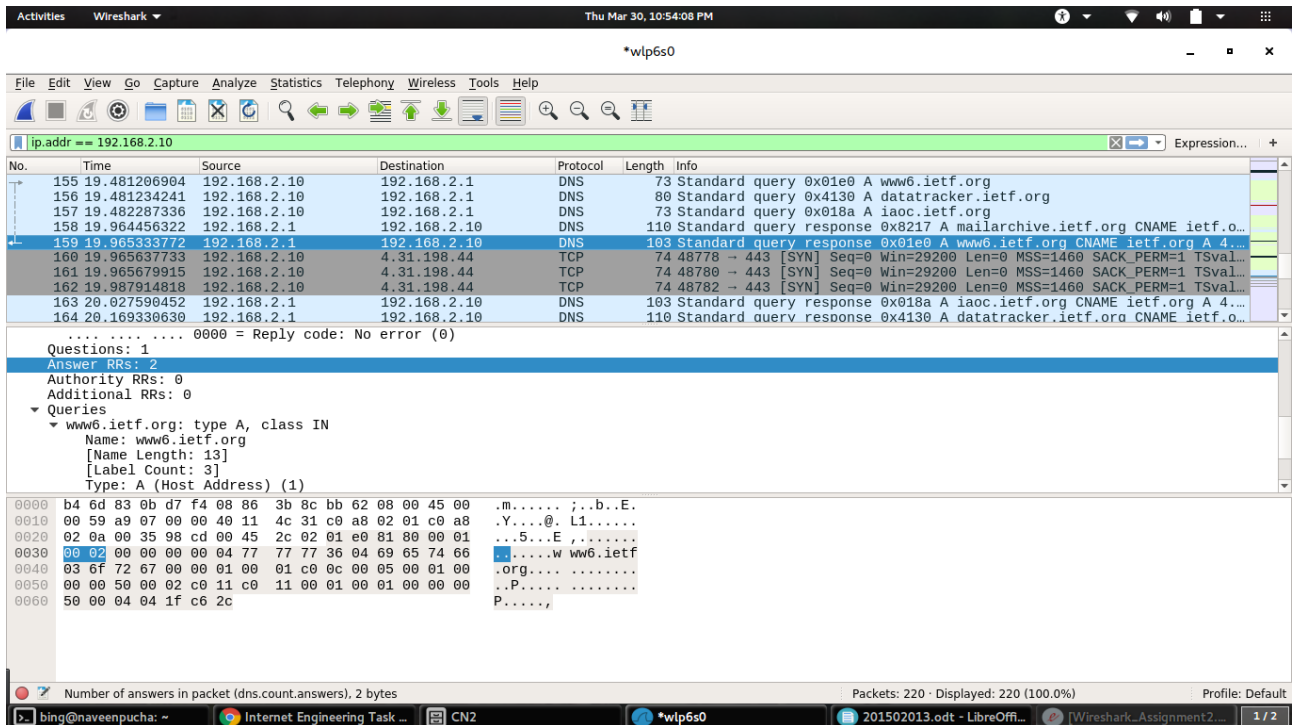


for query response



3) The IP address of the local DNS server is 192.168.2.1 and the IP address of the to which the DNS query message is sent to is also 192.168.2.1. Yes, as we can see that the IP addresses are the same. As we can see the IP address of the destination in the screenshot of the 2nd question of part 2.

4) There are 2 answers in the response. The answer has 1 type CNAME and 1 type A queries, containing the website name and host address respectively.



5) As shown in the above screenshot the destination address is 212.110.167.151 This is address provided by the DNS server.

6) No all the images are loaded from the website. So no additional DNS queries are necessary.

7) The destination port is 53 and the source port is 49478

Activities Wireshark Thu Mar 30, 7:21:05 PM

*wlp6s0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.2.10

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	74.125.130.188	192.168.2.10	TCP	66	5228 → 35212 [FIN, ACK] Seq=1 Ack=1 Win=332 Len=0 TSval=512610958 TSecr...
2	0.000461242	192.168.2.1	192.168.2.10	DNS	144	Standard query response 0xeb0d No such name A iibxttdhm SOA a.root-serv...
3	0.001783857	192.168.2.10	74.125.130.188	TCP	66	35212 → 5228 [ACK] Seq=1 Ack=2 Win=229 Len=0 TSval=6888054 TSecr=512610...
4	0.027749776	192.168.2.1	192.168.2.10	DNS	143	Standard query response 0x2b7d No such name A txpxvmke SOA a.root-serv...
5	2.566183880	192.168.2.10	10.4.20.204	DNS	71	Standard query 0x6234 A www.mit.edu
6	3.566184299	192.168.2.10	192.168.2.1	DNS	71	Standard query 0x46b0 A www.mit.edu
7	3.993491560	192.168.2.1	192.168.2.10	DNS	160	Standard query response 0x46b0 A www.mit.edu CNAME www.mit.edu.edgekey...
9	8.477744993	192.168.2.10	224.0.0.251	IGMPv2	46	Membership Report group 224.0.0.251

Frame 5: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0
 Ethernet II, Src: IntelCor_0b:d7:f4 (b4:6d:83:0b:d7:f4), Dst: BelkinIn_8c:bb:62 (08:86:3b:8c:bb:62)
 Internet Protocol Version 4, Src: 192.168.2.10, Dst: 10.4.20.204
 User Datagram Protocol, Src Port: 49478, Dst Port: 53
 Domain Name System (query)

```

0000  08 86 3b 8c bb 62 b4 6d 83 0b d7 f4 08 00 45 00  ...;.b.m.....E.
0010  00 39 7a c9 00 00 40 11 1e 69 c0 a8 02 0a 0a 04  .9z...@.i.....
0020  14 cc c1 46 00 35 00 25 a7 c0 62 34 01 00 00 01  ..F.5.%..b4....
0030  00 00 00 00 00 00 03 77 77 77 03 6d 69 74 03 65  .....w ww.mit.e
0040  64 75 00 00 01 00 01  du....
  
```

User Datagram Protocol (udp), 8 bytes

Packets: 9 - Displayed: 8 (88.9%) Profile: Default

bing@naveenpucha: ~ Assignment2 Wireshark_Assignme... vpn - How to discon... Answers.odt - LibreO... CN2 *wlp6s0 1/2

8) It is being sent to 192.168.2.1. Yes it is the IP address of the default local DNS server.

Activities Wireshark Thu Mar 30, 7:24:02 PM

*wlp6s0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.2.10

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	74.125.130.188	192.168.2.10	TCP	66	5228 → 35212 [FIN, ACK] Seq=1 Ack=1 Win=332 Len=0 TSval=512610958 TSecr...
2	0.000461242	192.168.2.1	192.168.2.10	DNS	144	Standard query response 0xeb0d No such name A iibxttdhm SOA a.root-serv...
3	0.001783857	192.168.2.10	74.125.130.188	TCP	66	35212 → 5228 [ACK] Seq=1 Ack=2 Win=229 Len=0 TSval=6888054 TSecr=512610...
4	0.027749776	192.168.2.1	192.168.2.10	DNS	143	Standard query response 0x2b7d No such name A txpxvmke SOA a.root-serv...
5	2.566183880	192.168.2.10	10.4.20.204	DNS	71	Standard query 0x6234 A www.mit.edu
6	3.566184299	192.168.2.10	192.168.2.1	DNS	71	Standard query 0x46b0 A www.mit.edu
7	3.993491560	192.168.2.1	192.168.2.10	DNS	160	Standard query response 0x46b0 A www.mit.edu CNAME www.mit.edu.edgekey...
9	8.477744993	192.168.2.10	224.0.0.251	IGMPv2	46	Membership Report group 224.0.0.251

Fragment offset: 0
 Time to live: 64
 Protocol: UDP (17)
 Header checksum: 0x0361 [validation disabled]
 [Header checksum status: Unverified]
 Source: 192.168.2.10
 Destination: 192.168.2.1
 [Source GeoIP: Unknown]
 [Destination GeoIP: Unknown]
 User Datagram Protocol, Src Port: 61985, Dst Port: 53
 Domain Name System (query)

```

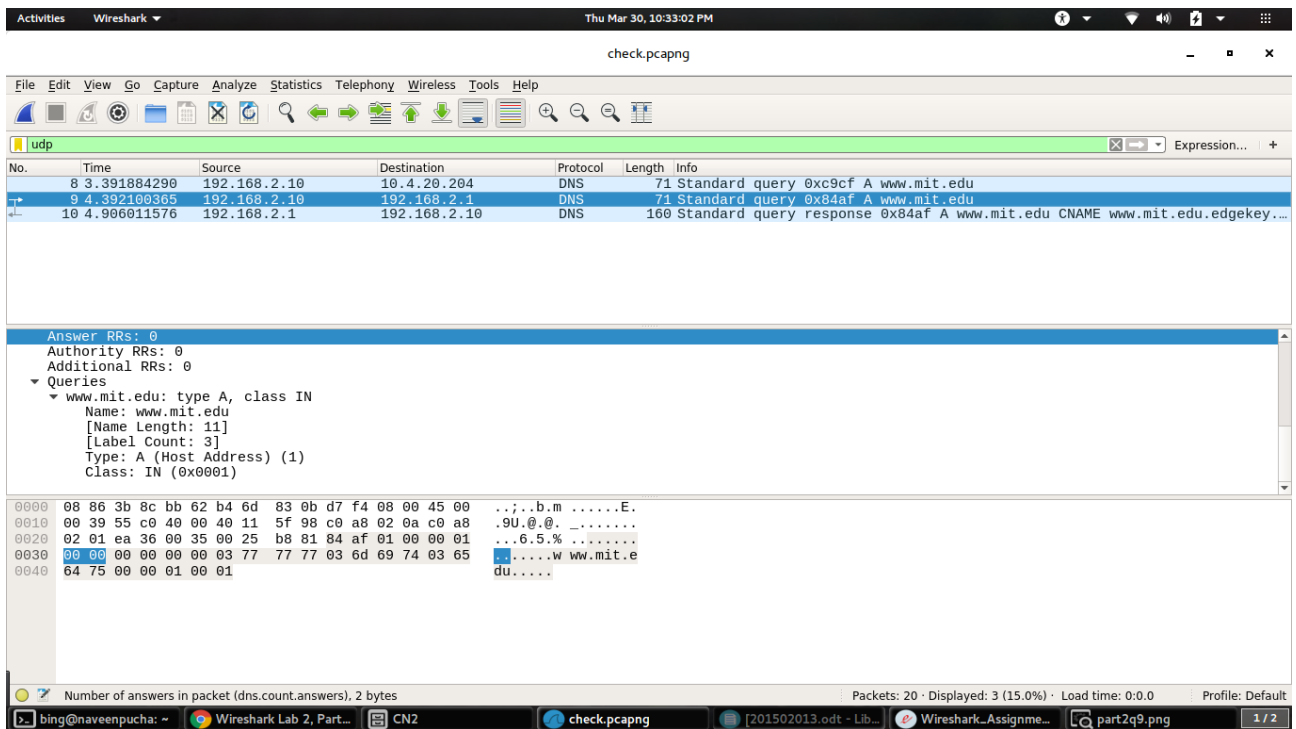
0000  08 86 3b 8c bb 62 b4 6d 83 0b d7 f4 08 00 45 00  ...;.b.m.....E.
0010  00 39 b1 f7 40 00 40 11 03 61 c0 a8 02 0a c0 a8  .9..@.a.....
0020  02 01 f2 21 00 35 00 25 ee 95 46 b0 01 00 00 01  ..!.5.%..F.....
0030  00 00 00 00 00 00 03 77 77 77 03 6d 69 74 03 65  .....w ww.mit.e
0040  64 75 00 00 01 00 01  du....
  
```

User Datagram Protocol (udp), 8 bytes

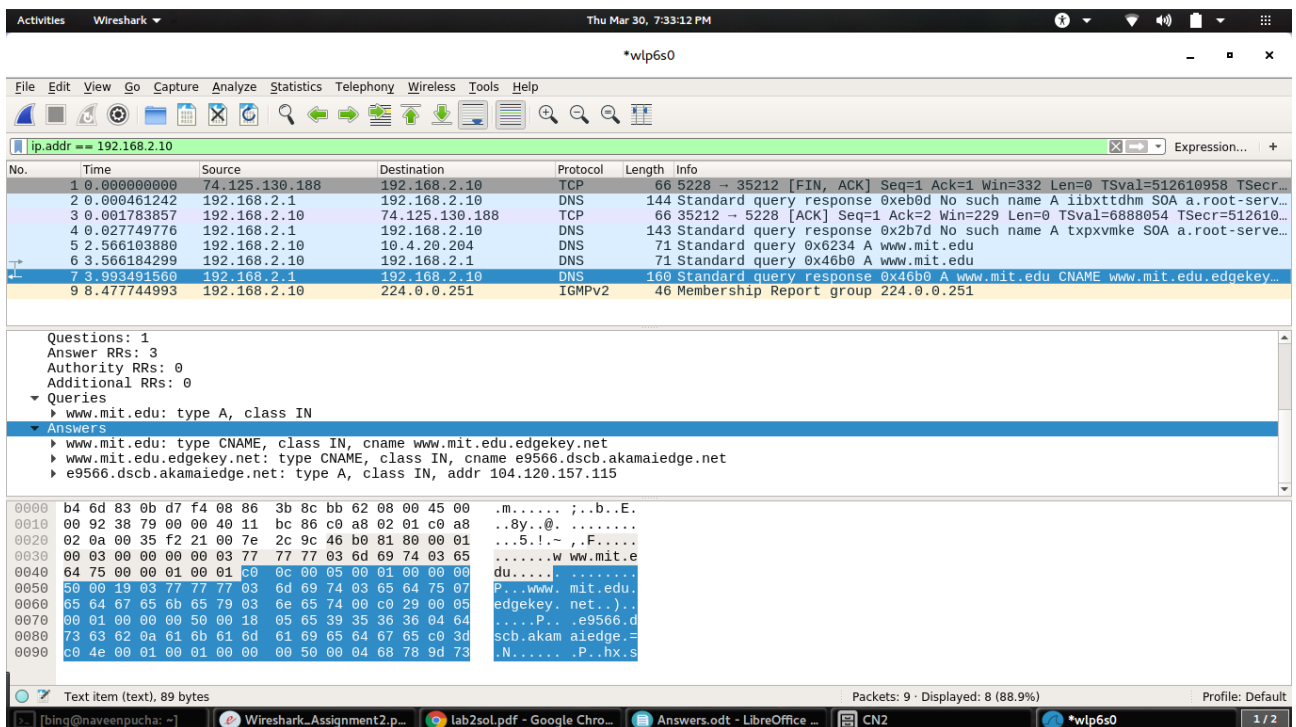
Packets: 9 - Displayed: 8 (88.9%) Profile: Default

bing@naveenpucha: ~ Assignment2 Wireshark_Assignme... [lab2sol.pdf - Google... Answers.odt - LibreO... CN2 *wlp6s0 1/2

9) It is a Type A query. Yes the query contains answers.



10) There are “Three” answers provided. Two answers are of type CNAME and one is a host address.



PART 3

1) The source IP address is 192.168.1.102 using port 1161

The screenshot shows a Wireshark capture of a TCP connection. The packet list shows a sequence of packets: 198 (ACK), 199 (POST), 200 (ACK), 201 (ACK), 202 (ACK), 203 (HTTP OK), 206 (ACK), and 213 (SYN). The packet details pane for packet 199 shows the following information:

- Frame 199: 104 bytes on wire (832 bits), 104 bytes captured (832 bits)
- Ethernet II, Src: PremaxPe_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
- Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 164041, Ack: 1, Len: 50
- Source Port: 1161
- Destination Port: 80
- [Stream index: 0]
- [TCP Segment Len: 50]
- Sequence number: 164041 (relative sequence number)

The packet bytes pane shows the raw data of the packet, including the Ethernet II header, IP header, and TCP header. The TCP header shows the source port 1161, destination port 80, sequence number 164041, and acknowledgment number 1.

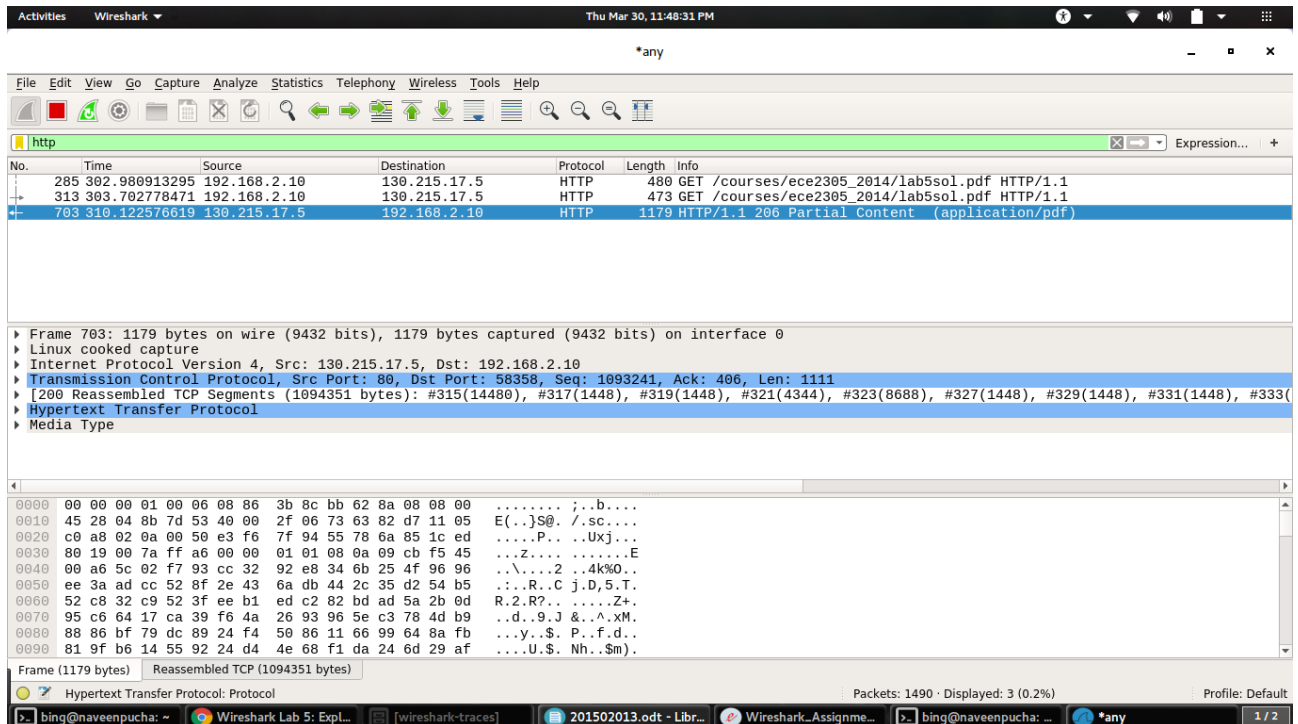
2) The destination IP address is 128.119.245.12 using port 80

The screenshot shows a Wireshark capture of a TCP connection. The packet list shows a sequence of packets: 198 (ACK), 199 (POST), 200 (ACK), 201 (ACK), 202 (ACK), 203 (HTTP OK), 206 (ACK), and 213 (SYN). The packet details pane for packet 199 shows the following information:

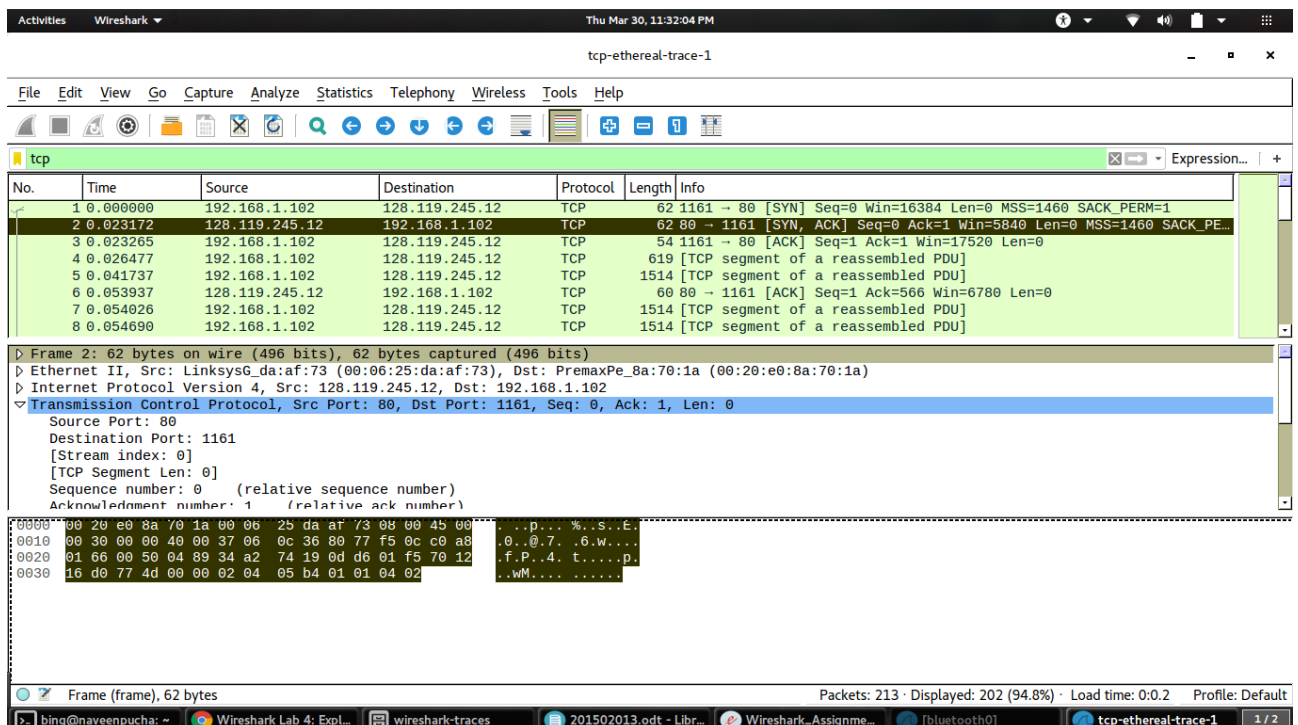
- Frame 199: 104 bytes on wire (832 bits), 104 bytes captured (832 bits)
- Ethernet II, Src: PremaxPe_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
- Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 164041, Ack: 1, Len: 50
- Source Port: 1161
- Destination Port: 80
- [Stream index: 0]
- [TCP Segment Len: 50]
- Sequence number: 164041 (relative sequence number)

The packet bytes pane shows the raw data of the packet, including the Ethernet II header, IP header, and TCP header. The TCP header shows the source port 1161, destination port 80, sequence number 164041, and acknowledgment number 1.

3) The source IP address is 130.215.17.5 using port 80



4) The sequence number of the segment which will be used to initiate the TCP connection is 0. That is Seq=0. This contains a SYN flag which identifies the segment as a SYN segment.



5) The sequence number of the TCP segment containing the HTTP post command is 164041

Activities Wireshark Thu Mar 30, 11:33:00 PM

tcp-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
198	5.297257	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=159389 Win=62780 Len=0
199	5.297341	192.168.1.102	128.119.245.12	HTTP	184	POST /ethereal-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
200	5.389471	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=162309 Win=62780 Len=0
201	5.447887	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=164041 Win=62780 Len=0
202	5.455830	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=164091 Win=62780 Len=0
203	5.461175	128.119.245.12	192.168.1.102	HTTP	784	HTTP/1.1 200 OK (text/html)
206	5.651141	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=164091 Ack=731 Win=16790 Len=0
213	7.595557	192.168.1.102	199.2.53.206	TCP	62	1162 → 631 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1

[Stream index: 0]
[TCP Segment Len: 50]
Sequence number: 164041 (relative sequence number)
[Next sequence number: 164091 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Header Length: 20 bytes
Flags: 0x018 (PSH, ACK)
Window size value: 17520
[Calculated window size: 17520]

0000 00 06 25 0a a1 73 00 20 80 8a 70 1a 08 00 45 00 ...S...P...E
0010 00 5a 1e 9a 40 00 00 06 a4 71 c0 a8 01 66 80 77 .Z..@...q...f.w
0020 f5 0c 04 89 00 50 0d d8 82 bd 34 a2 74 1a 50 18P...4.t.P
0030 44 70 9f 0f 00 00 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d Dp.....
0040 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d
0050 2d 2d 2d 2d 2d 32 36 35 30 30 31 39 31 36 39 31 -----265 00191691
0060 35 37 32 34 2d 2d 0d 0a 5724---

Frame (104 bytes) Reassembled TCP (164090 bytes)

Sequence number (tcp.seq), 4 bytes

Packets: 213 · Displayed: 202 (94.8%) · Load time: 0:0.2 Profile: Default

bing@naveenpucha: ~ Wireshark Lab 4: Expl... CN2 201502013.odt - Libr... Wireshark_Assigne... [bluetooth0] tcp-ethereal-trace-1 1/2

PART 4

1) There are 4 fields in the header. These are the Source Port, Destination Port, Length and Checksum

Activities Wireshark Thu Mar 30, 9:20:20 PM

*wlp6s0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp

No.	Time	Source	Destination	Protocol	Length	Info
8	3.391884290	192.168.2.10	10.4.20.204	DNS	71	Standard query 0xc9cf A www.mit.edu
9	4.392100365	192.168.2.10	192.168.2.1	DNS	71	Standard query 0x84af A www.mit.edu
10	4.906011576	192.168.2.1	192.168.2.10	DNS	160	Standard query response 0x84af A www.mit.edu CNAME www.mit.edu.edgekey...

Frame 8: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0
Ethernet II, Src: IntelCor_0b:d7:f4 (b4:6d:83:0b:d7:f4), Dst: BelkinIn_8c:bb:62 (08:86:3b:8c:bb:62)
Internet Protocol Version 4, Src: 192.168.2.10, Dst: 10.4.20.204
User Datagram Protocol, Src Port: 58496, Dst Port: 53
Source Port: 58496
Destination Port: 53
Length: 37
Checksum: 0x1cf1 [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
Domain Name System (query)
0000 08 86 3b 8c bb 62 b4 6d 83 0b d7 f4 08 00 45 00 ...;..b.m.....E.
0010 00 39 f8 1c 00 00 40 11 a1 15 c0 a8 02 0a 8a 04 .9....@.....
0020 14 cc 04 00 00 35 00 25 1c f1 c9 cf 01 00 00 01 ..5.%.....
0030 00 00 00 00 00 00 03 77 77 77 03 6d 69 74 03 65w ww.mit.e
0040 64 75 00 00 01 00 01 du....

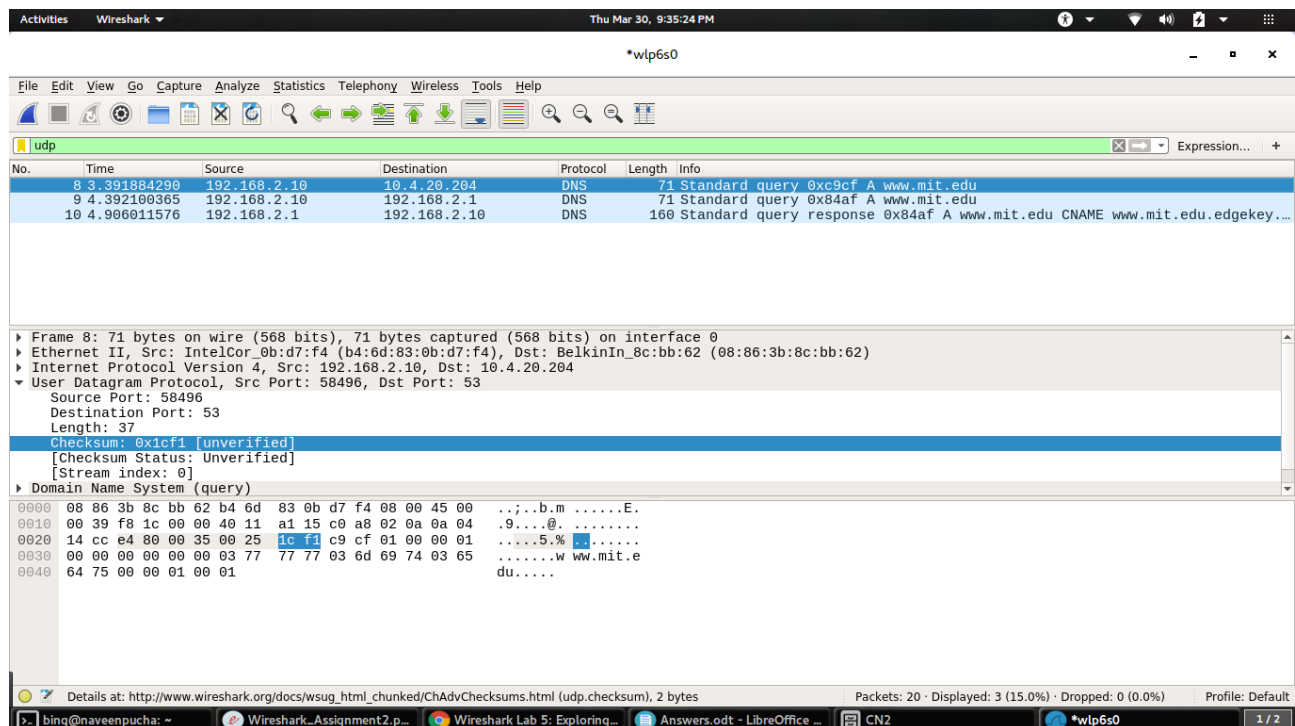
User Datagram Protocol (udp), 8 bytes

Packets: 20 · Displayed: 3 (15.0%) · Dropped: 0 (0.0%) Profile: Default

bing@naveenpucha: ~ Wireshark_Assignment2.p... Wireshark Lab 5: Exploring... Answers.odt - LibreOffice ... Home *wlp6s0 1/2

2) In the above case the length is 37. It's the count of the bytes that were captured for that particular frame, it'll match the number of bytes of raw data in the bottom section of the wireshark window.

3) The each of the UDP header files is 2 bytes long as shown below.



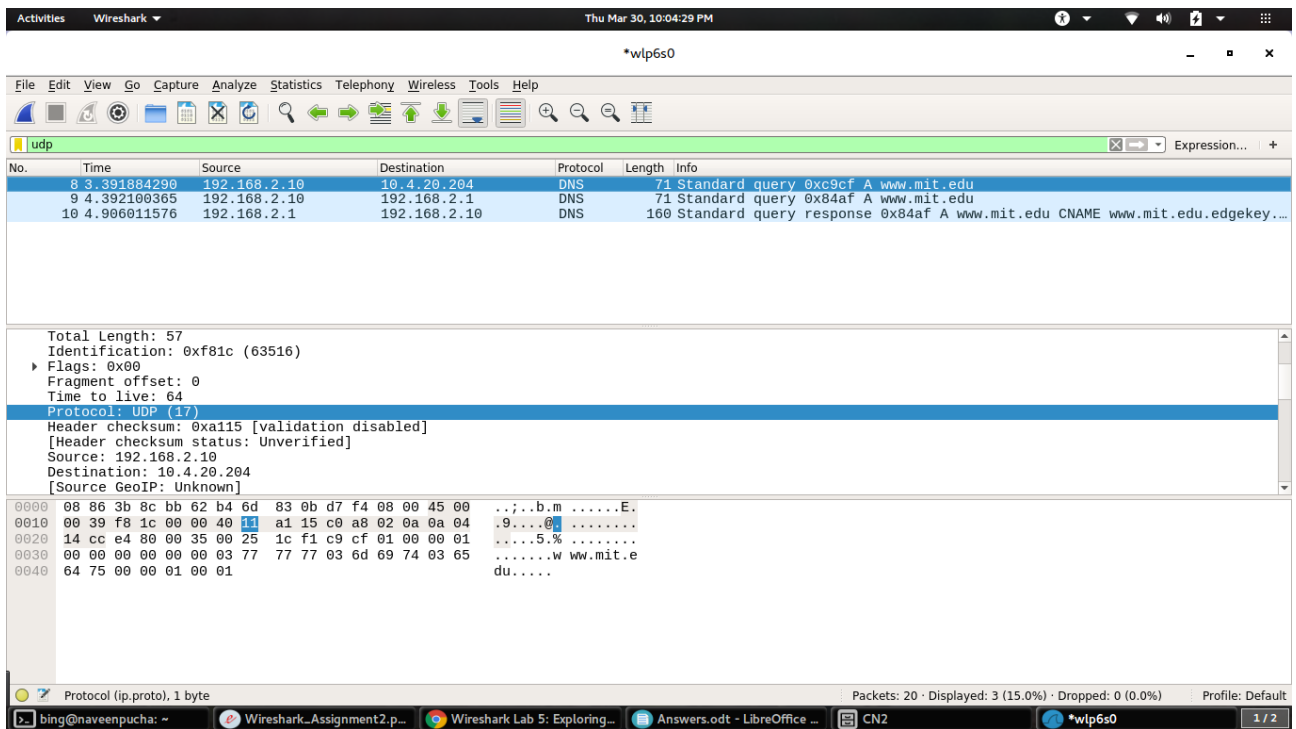
The maximum number of bytes that can be the payload is 2^{16} – the bytes already being used by the header file

There are 4 header files, and each has 2 bytes , so in total there will be 8 header bytes.

Therefore the answer for this will be $65535 - 8 = 65527$.

Largest possible is 65535

4) The protocol number for UDP is 17 in decimal and in hexadecimal notation it is 0x11.



5) It is a 16-bit field of one's complement of one's complement sum of a psuedo UDP header + UDP datagram.

The Psuedo UDP header consists of 5 fields,

Source address: 32 bits / 4 bytes, taken from IP header.

Destination address : 32 bits / 4 bytes, taken from IP header.

Reserved : 8 bits / 1 byte, set to all 0's in the beginning.

Protocol : 8 bits / 1 byte, taken from IP header.

Length : because UDP header has a length field that indicates the length of the entire datagram, including UDP header and data, the value from UDP header used.

This UDP checksum is optional. If it's not computed, it is set to all 0's.