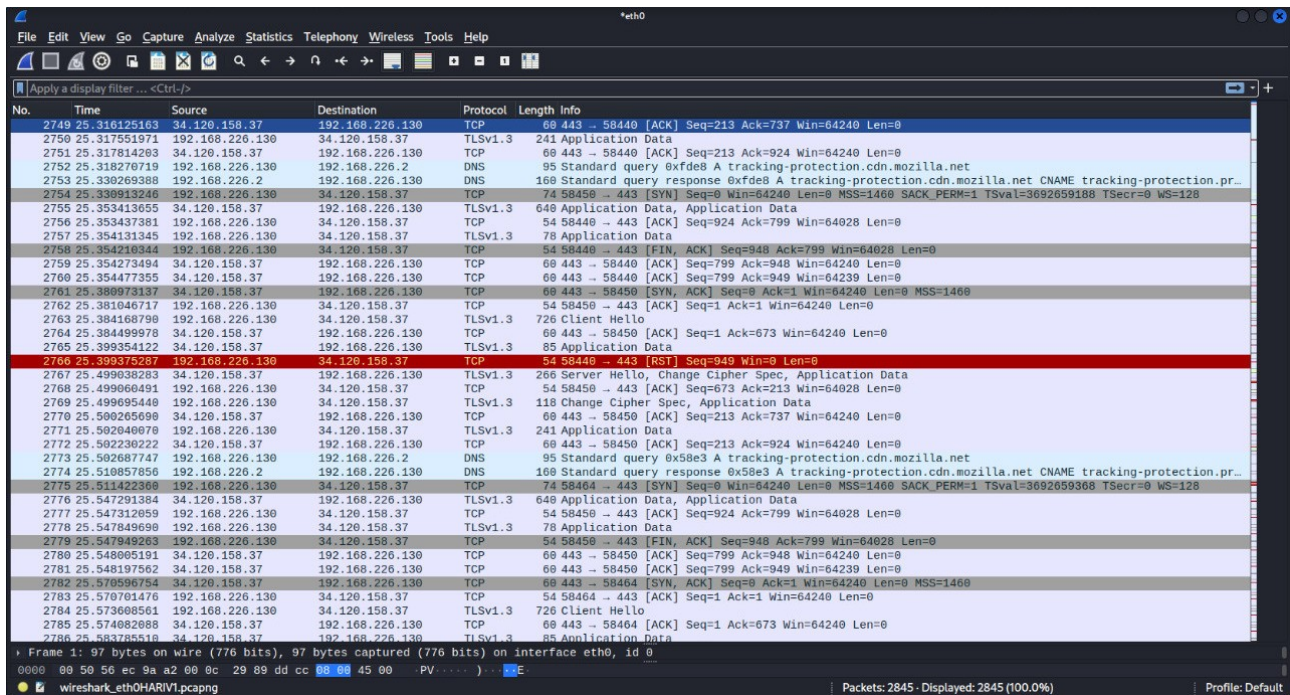
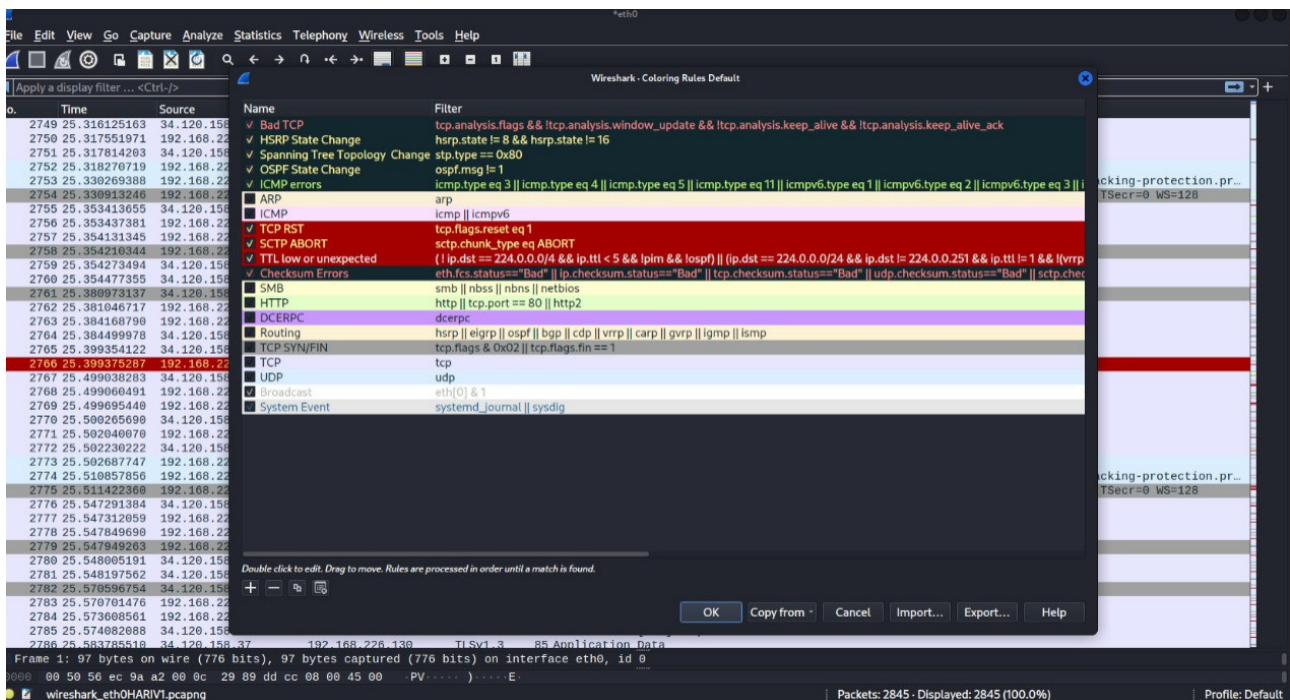


Lab Handout – 1

Ans 1 :-



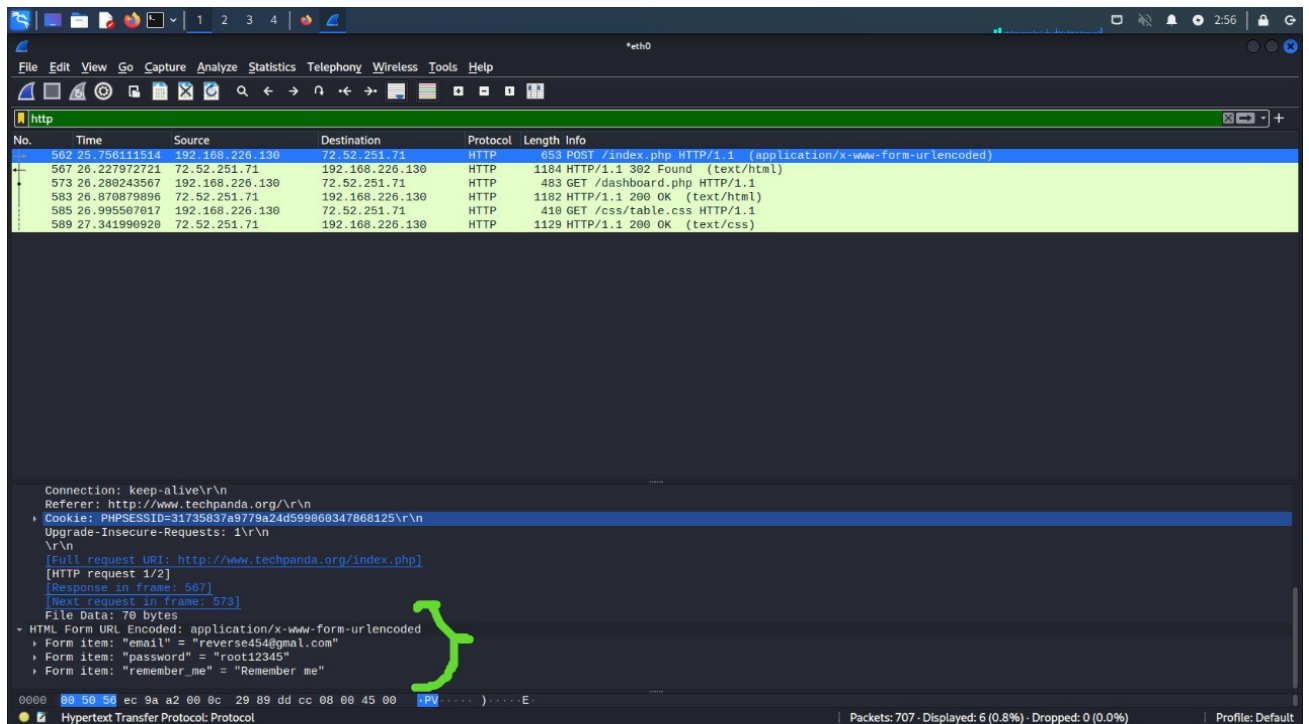
Ans 2 :-



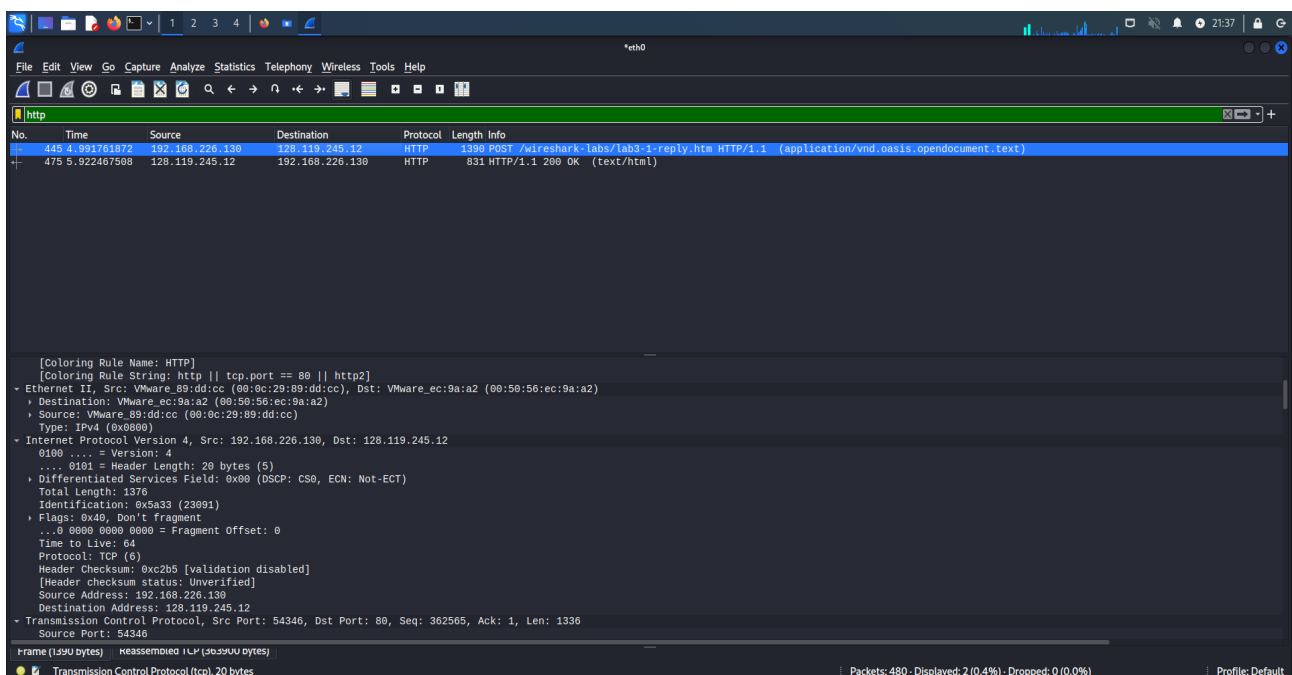
Ans 3 :- Change the filter to **ip.addr == <destination>**, where <destination> is the destination address of the HTTP packet.

Ans 4 :- DNS uses TCP for Zone transfer and UDP for name, and queries either regular (primary) or reverse. UDP can be used to exchange small information whereas TCP must be used to exchange information larger than 512 bytes.

Ans 5 :- Http Password Sniffing through Wireshark on [TechPanda](http://www.techpanda.org) website.



Lab Manual – 3



Ans 1 :- Source Address: 192.168.226.130, Source Port: 54346

Ans 2 :- Destination Address: 128.119.245.12, Destination Port: 80

Image for Question 3,4,5,6

Wireshark capture of a TCP handshake. The packet list shows frames 1, 2, 3, and 4. The packet details for frame 4 show the TCP header flags and sequence numbers.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.226.130	128.119.245.12	TCP	74	54346 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3933648989 TSecr=0 WS=128
2	0.251123322	192.168.226.130	128.119.245.12	TCP	74	54360 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3933649240 TSecr=0 WS=128
3	0.366199341	128.119.245.12	192.168.226.130	TCP	60	80 → 54346 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
4	0.366234423	192.168.226.130	128.119.245.12	TCP	54	54346 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0

Packet details for frame 4:

```

Acknowledgment number (raw): 0
1010 .... = Header Length: 40 bytes (10)
- Flags: 0x002 (SYN)
  000. .... = Reserved: Not set
  ...0 .... = Nonce: Not set
  ....0 .... = Congestion Window Reduced (CWR): Not set
  ....0 .... = ECN-Echo: Not set
  ....0 .... = Urgent: Not set
  ....0 .... = Acknowledgment: Not set
  ....0 .... = Push: Not set
  ....0 .... = Reset: Not set
  ....1 .... = Syn: Set
  - [Expert Info (Chat/Sequence): Connection establish request (SYN): server port 80]
    [Connection establish request (SYN): server port 80]
    [Severity level: Chat]
    [Group: Sequence]
  ....0 .... = Fin: Not set
  [TCP Flags: .....S.]
  Window: 64240
  [Calculated window size: 64240]
  Checksum: 0x18de [unverified]
  [Checksum Status: Unverified]
  ....
  0020 f5 0c d4 4a 80 50 44 75 05 3e 00 00 00 00 a0 02 ...J...ou >.....
  Destination Port (tcp.dstport), 2 bytes
  
```

Segment 1- 4 are used for the connection between client and the given website to complete the handshake. Total 4 segments were used.

[SEQ/ACK analysis] in TCP Header Flags segment identifies TCP segment as handshaking segments

[This is an ACK to the segment in frame: 1]

[The RTT to ACK the segment was: 0.366199341 seconds]

[iRTT: 0.366234423 seconds]

Ans 4:- TCP first six data carrying segments are :- 5,6,10,14,15,16.

Wireshark capture of an HTTP POST request and response. The packet list shows frames 445 and 475. The packet details for frame 445 show the HTTP request and the packet details for frame 475 show the HTTP response.

No.	Time	Source	Destination	Protocol	Length	Info
445	4.991761872	192.168.226.130	128.119.245.12	HTTP	1390	POST /wreshark-labs/lab3-1-reply.htm HTTP/1.1 (application/vnd.oasis.opendocument.text)
475	5.922467508	128.119.245.12	192.168.226.130	HTTP	831	HTTP/1.1 200 OK (text/html)

Packet details for frame 445:

```

Source Address: 192.168.226.130
Destination Address: 128.119.245.12
- Transmission Control Protocol, Src Port: 54346, Dst Port: 80, Seq: 362565, Ack: 1, Len: 1336
  Source Port: 54346
  Destination Port: 80
  [Stream index: 0]
  [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 1336]
  Sequence Number: 362565 (relative sequence number)
  Sequence Number (raw): 1148882307
  [Next Sequence Number: 363901 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 133014359
  0101 .... = Header Length: 20 bytes (5)
  - Flags: 0x018 (PSH, ACK)
    000. .... = Reserved: Not set
    ...0 .... = Nonce: Not set
    ....0 .... = Congestion Window Reduced (CWR): Not set
    ....0 .... = ECN-Echo: Not set
    ....0 .... = Urgent: Not set
    ....1 .... = Acknowledgment: Set
    ....1 .... = Push: Set
  Frame (1390 bytes) reassembled 1 TCP segment(s)
  Hypertext Transfer Protocol: Protocol
  
```

And the http POST data carrying TCP segment is 445.

The image shows a Wireshark packet capture of a TCP stream. The packet list on the left shows several segments, with packet 5 (0.367149168) selected. The packet details pane on the right shows the structure of the selected packet, including the TCP header and the payload (reassembly data). The packet bytes pane at the bottom shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.226.130	128.119.245.12	TCP	74	54360 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3933648989 TSecr=0 WS=128
2	0.251123322	192.168.226.130	128.119.245.12	TCP	74	54360 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3933649240 TSecr=0 WS=128
3	0.366199341	128.119.245.12	192.168.226.130	TCP	60	80 → 54360 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
4	0.366234423	192.168.226.130	128.119.245.12	TCP	54	54360 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
5	0.367149168	192.168.226.130	128.119.245.12	TCP	2974	54360 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=2920 [TCP segment of a reassembled PDU]
6	0.367336960	192.168.226.130	128.119.245.12	TCP	2974	54360 → 80 [PSH, ACK] Seq=2921 Ack=1 Win=64240 Len=2920 [TCP segment of a reassembled PDU]
7	0.367694770	128.119.245.12	192.168.226.130	TCP	60	80 → 54360 [ACK] Seq=1 Ack=1461 Win=64240 Len=0
8	0.367695071	128.119.245.12	192.168.226.130	TCP	60	80 → 54360 [ACK] Seq=1 Ack=2921 Win=64240 Len=0
9	0.367751573	128.119.245.12	192.168.226.130	TCP	60	80 → 54360 [ACK] Seq=1 Ack=4381 Win=64240 Len=0
10	0.367769700	192.168.226.130	128.119.245.12	TCP	2974	54360 → 80 [PSH, ACK] Seq=5841 Ack=1 Win=64240 Len=2920 [TCP segment of a reassembled PDU]
11	0.371803683	128.119.245.12	192.168.226.130	TCP	60	80 → 54360 [ACK] Seq=1 Ack=5841 Win=64240 Len=0
12	0.371804930	128.119.245.12	192.168.226.130	TCP	60	80 → 54360 [ACK] Seq=1 Ack=7301 Win=64240 Len=0
13	0.371804996	128.119.245.12	192.168.226.130	TCP	60	80 → 54360 [ACK] Seq=1 Ack=8761 Win=64240 Len=0
14	0.371821586	192.168.226.130	128.119.245.12	TCP	2974	54360 → 80 [PSH, ACK] Seq=8761 Ack=1 Win=64240 Len=2920 [TCP segment of a reassembled PDU]
15	0.371894266	192.168.226.130	128.119.245.12	TCP	2974	54360 → 80 [PSH, ACK] Seq=11681 Ack=1 Win=64240 Len=2920 [TCP segment of a reassembled PDU]
16	0.371962148	192.168.226.130	128.119.245.12	TCP	2974	54360 → 80 [PSH, ACK] Seq=14601 Ack=1 Win=64240 Len=2920 [TCP segment of a reassembled PDU]

Details of selected packet (5):

- ...1... = Acknowledgment: Set
- ...0... = Reset: Not set
- ...0... = Syn: Not set
- ...0... = Fin: Not set
- [TCP Flags:AP...]
- Window: 64240
- [Calculated window size: 64240]
- [Window size scaling factor: -2 (no window scaling used)]
- Checksum: 0x2492 [Unverified]
- [Checksum Status: Unverified]
- Urgent Pointer: 0
- Time stamps
 - [Time since first frame in this TCP stream: 0.367149168 seconds]
 - [Time since previous frame in this TCP stream: 0.000914745 seconds]
- SEQ/ACK analysis
 - [RTT: 0.366234423 seconds]
 - [Bytes in flight: 2920]
 - [Bytes sent since last PSH flag: 2920]
 - TCP payload (2920 bytes)
 - [Reassembled PDU in frame: 445]
 - TCP segment data (2920 bytes)

Packet bytes: f5 0c d4 4a 08 58 44 75 05 3f 4f 74 2f 57 50 16 ... J-PDU -?0t/WP

From the Above Diagram :-

TCP Segment 5:- TCP segment data (2920 bytes)

TCP Segment 6:- TCP segment data (2920 bytes)

TCP Segment 10:- segment data (2920 bytes)

TCP Segment 14:- segment data (2920 bytes)

TCP Segment 15:- segment data (2920 bytes)

TCP Segment 16:- segment data (2920 bytes)

TCP Segment 445 (HTTP Post) :- TCP segment data (1336 bytes)

Ans 5:- Time relative to the first Frame in the TCP Stream i.e, 0.000000sec

TCP Segment 5:- Sent : 0.367149168 seconds , received : 0.368063913 seconds

TCP Segment 6:- Sent :0.367336960 seconds , received : 0.367769700 seconds

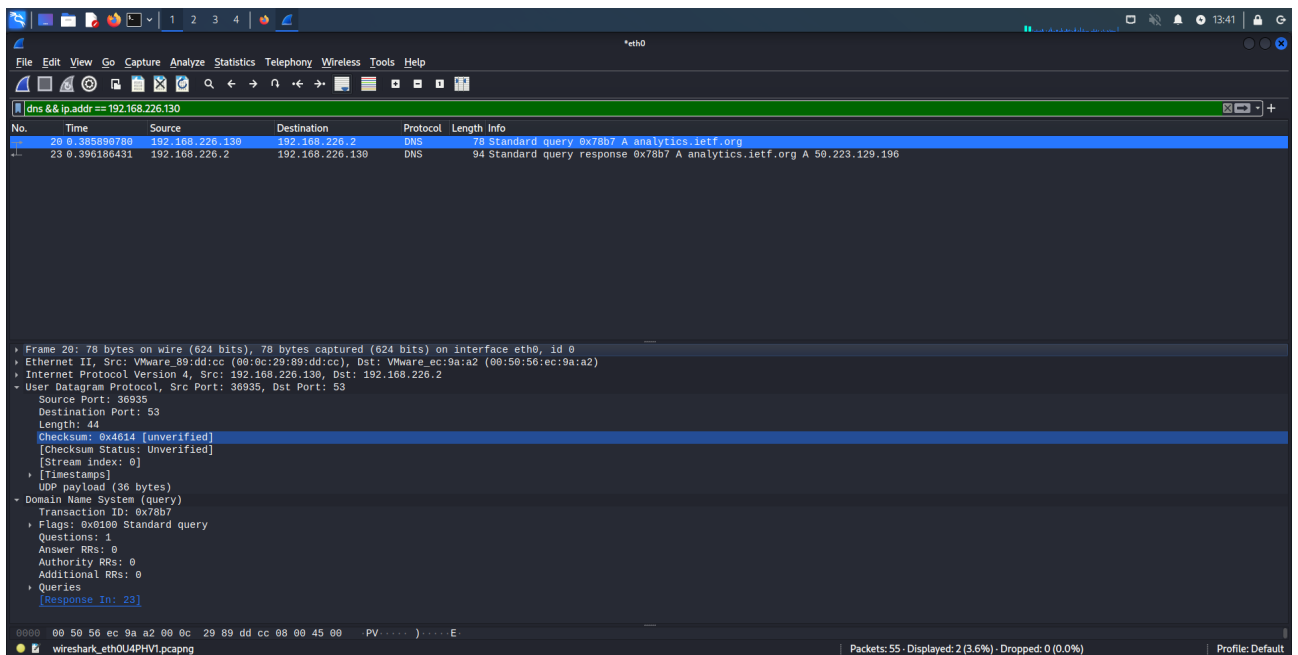
TCP Segment 10:- Sent : 0.367769700 seconds, received : 0.371821586 seconds

TCP Segment 14:- Sent : 0.371821586 seconds, received : 0.371894266 seconds

TCP Segment 15:- Sent :0.371894266 seconds , received : 0.371962148 seconds

TCP Segment 16:- Sent :0.371962148 seconds , received : 0.371966148 seconds

Lab Manual – 4



Ans 1 :- From the above diagram we can see that the response message is transported using UDP(User Datagram Packet).We can only tell that the reason being data sent over UDP so that the data can be transferred Quickly and there is no such data where the lost of data can be a problem.

Ans 2:- Destination port : 53

Ans 3:- Source Port: 36935

Ans 4:- Destination IP address : 192.168.226.2 Yes they are same.

Ans 5:- analytics.ietf.org: type A, class IN, this data is present under “Domain Name System(Query)” Section under “Queries” .

Ans 6:- Under Domain Name System (response) are the Answers is Present, and 1 Answer is present and it's Highlighted below:-

Transaction ID: 0x78b7

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 1

Authority RRs: 0

Additional RRs: 0

Queries

analytics.ietf.org: type A, class IN

Answers

analytics.ietf.org: type A, class IN, addr 50.223.129.196

Name: analytics.ietf.org

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 5 (5 seconds)

Data length: 4

Address: 50.223.129.196

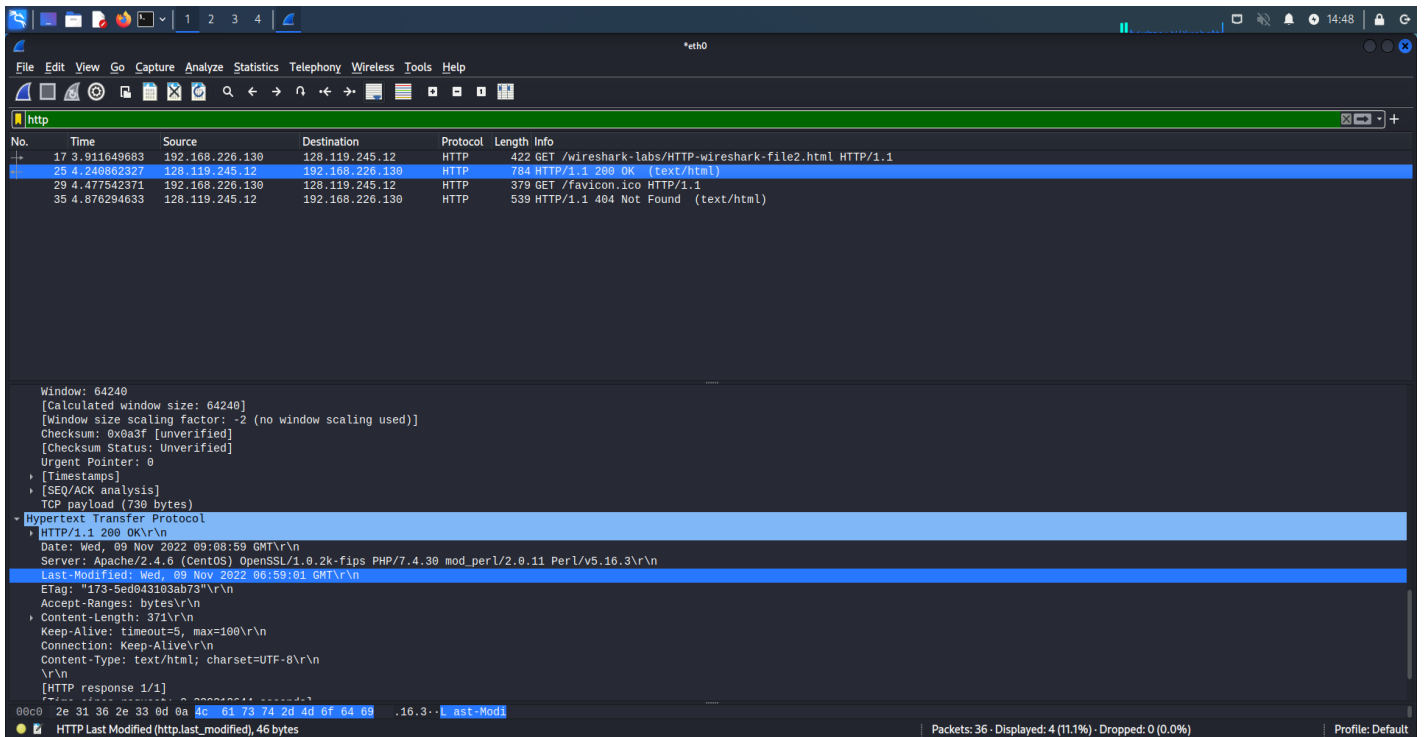
[Request In: 20]

[Time: 0.010295651 seconds]

Ans 7:- No, because that Image requested is present on that server only.

LAB MANUAL – 2

All answers will be answered Using Below Screenshot :-



Ans 1,3:- From the Above Image we can see, “Last-Modified-Since” is present in response of HTTP in “200 Ok” status message, and there was no IF_MODIFIED_SINCE in HTTP GET response and the content is :
“Last-Modified: Wed, 09 Nov 2022 06:59:01 GMT\r\n”.

Ans 2:- The content was provided under “Line based text data” header in HTTP 200 Ok (text/html) packet as highlighted below :-

Line-based text data: text/html (10 lines)

```
\n
<html>\n
\n
Congratu
This file's
Thus if y
will only l
field in yo
\n
</html>\n
```

**Congratulations again! Now you've downloaded the file lab2-2.html.
\n**
This file's last modification date will not change. <p>\n
**Thus if you download this multiple times on your browser, a complete copy
\n**
**will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE
\n**
field in your browser's HTTP GET request to the server.\n

Ans 4:- In the second GET request there was not status code and phrase and content of the message was also not explicitly returned from the server.

LAST PAGE Q/A

Ans 1:- One HTTP GET request were present. And was sent to 118.215.154.3 IP address. And the response code was 388 that tell it was internally redirected to this address 142.250.182.3 Request address.

Ans 2:- The web browser has downloaded the image serially, can be verified by analysing timestamp of response from the server.

Ans 1 :- From the Above Image we can see the response message is transported using UDP(User Datagram packet).

