Practical-8

AIM: Capturing and analyzing network protocol traffic at different layers of protocol stack.

Tools required:

1. Desktop computer
2. Wireshark

Submission: Written file submission is expected.
Rubrics: Nicely drafted document with clarity in answers leads to full marks. Otherwise, submission carries proportional marks. Same day submission will be evaluated from 10 marks otherwise submission will be evaluated from 7 marks.

Understanding Require

- IP Address
- URL
- Finding IP address from URL
- Finding location from IP Address

Exercise 1 : Refer to the given wireshark video and write down the steps you have gone through and also conclude what you have understood from the video. (Write in your own words.)

.

Video : TCP Reassembly Setting

Steps:

Conclusion :

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.

Exercise 2 : Refer to the given wireshark video and write down the steps you have gone through and also conclude what you have understood from the video. (Write in your own words.)

.

Video : Use Regex to Filter for a Group of Phrases

Steps:

Conclusion :

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.

Exercise 3 : Refer to the given wireshark video and write down the steps you have gone through and also conclude what you have understood from the video. (Write in your own words.)

.

Video : Graph HTTP Response Times

Steps:

Conclusion :

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.

Exercise 4 : Refer to the given wireshark video and write down the steps you have gone through and also conclude what you have understood from the video. (Write in your own words.)

.

Video : Finding Suspicious Traffic in Protocol Hierarchy

Steps:

Conclusion :

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.

Exercise 5 : Refer to the given wireshark video and write down the steps you have gone through and also conclude what you have understood from the video. (Write in your own words.)

.

Video : Find TCP Problems Fast with a BadTCP Button

Steps:

Conclusion :

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.

Exercise 6: Refer to the given wireshark video and write down the steps you have gone through and also conclude what you have understood from the video. (Write in your own words.)

.

Video : Identify Separate TCP Conversations with TCP Stream Index

Steps:

Conclusion :

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.

Exercise 7: Refer to the given wireshark video and write down the steps you have gone through and also conclude what you have understood from the video. (Write in your own words.)

.

Video : Add an httphost Column

Steps:

Conclusion :

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.

Exercise 8: Refer to the given wireshark video and write down the steps you have gone through and also conclude what you have understood from the video. (Write in your own words.)

.

Video : Filter to Determine TCP Round Trip Times and Capabilities

Steps:

Conclusion :

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.

Exercise 9: Refer to the given wireshark video and write down the steps you have gone through and also conclude what you have understood from the video. (Write in your own words.)

.

Video : Correlate TCP Problems to IO Drops

Steps:

Conclusion :

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.

Exercise 10: Refer to the given wireshark video and write down the steps you have gone through and also conclude what you have understood from the video. (Write in your own words.)

.

Video : Find Delays with TCP Calculate Conversation Timestamps

Steps:

Conclusion :

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.

Exercise 11: Refer to the given wireshark video and write down the steps you have gone through and also conclude what you have understood from the video. (Write in your own words.)

.

Video : Find TCP Connections with Limited Options

Steps:

Conclusion :

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.