SVKM’S NMIMS University

Mukesh Patel School of Technology Management and Engineering

**PART A**

**(PART A: TO BE REFFERED BY STUDENTS)**

**Experiment No.06**

**A.1—Aim:**

Working of Wireshark application on live network.

A packet-sniffer software is normally has two components: a packet-capturer and a packet-analyzer. The packet-capturer captures a copy of all outgoing and incoming frames (at the data-link layer) and passes them to the packet-analyzer. The packet analyzer can then extract different headers and the ultimate message for analysis

**A.2--- Prerequisite:**

TCP configuration and protocols

**A.3--- Outcome:**

After successful completion of this experiment students will be able to understand the how packet travels from process to Process.

**A.4--- Task:**

■ Start up your web browser and clear the browser's cache memory

■ Open the Wireshark and start capturing. Use the filter box to capture only frames

that the source or the sink protocol is HTTP. Note that you need to type http in lowercase in the filter box and click Apply.

■ Now, go back to your browser, access one of your favorite web site.

■ Stop capturing and save the captured file.

Questions

Using the first frame with the source protocol HTTP/ TCP, answer the following question in

your lab-report sheet.

1. Is the frame an outgoing or an incoming frame?

2. What is the source IP address of the network-layer header in the frame?

3. What is the destination IP address of the network-layer header in the frame?

4. What is the total number of bytes in the whole frame?

5. What is the number of bytes in the Ethernet (data-link layer) header?

6. What is the number of bytes in the IP header?

7. What is the number of bytes in the TCP header?

8. Write about various colour coding schemes used to identify the types of traffic.

**(PART - B)**

(TO BE COMPLETED BY STUDENTS)

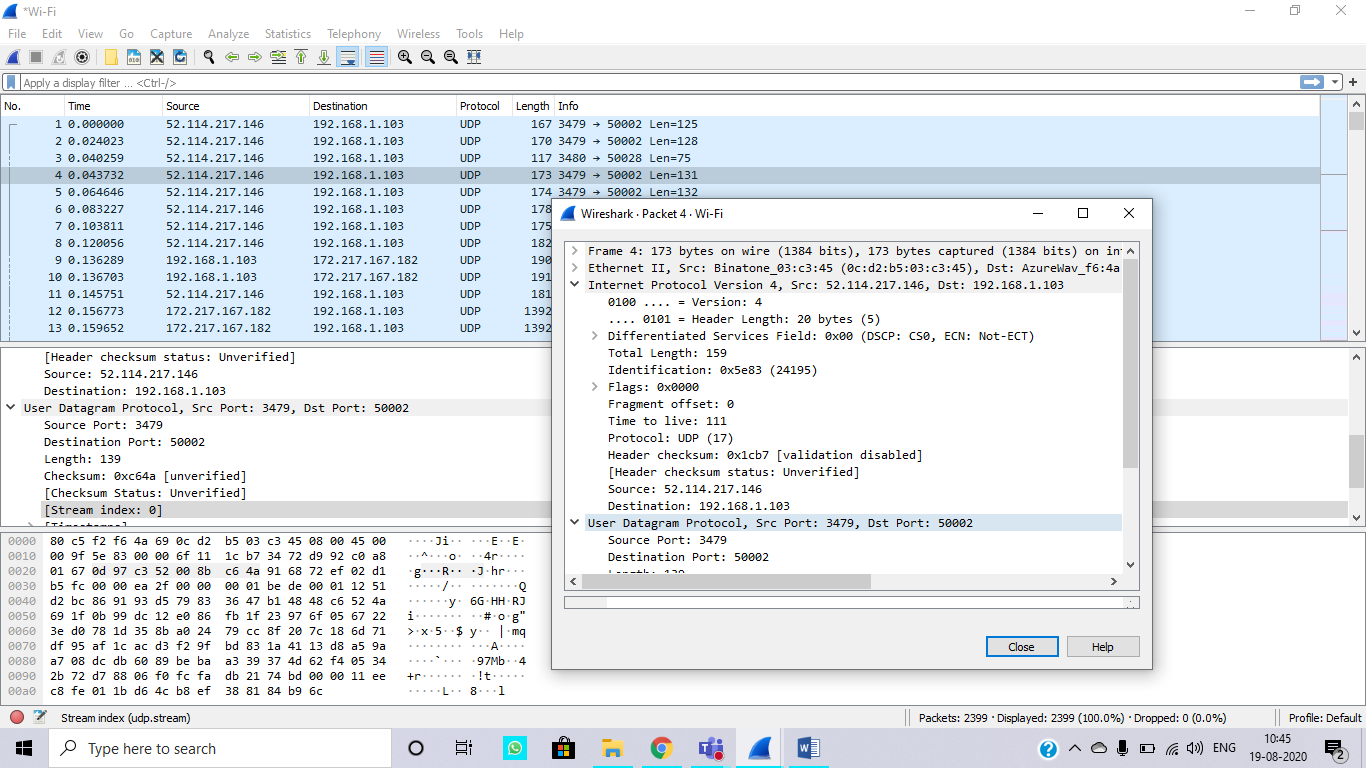
(Students must submit the soft copy as per following segments within two hours of the practical. The soft copy must be uploaded on the Blackboard or emailed to the concerned lab in charge faculties at the end of the practical in case there is no Black board access available)

|  |  |
| --- | --- |
| Roll. No.: N049 | Name: Tarun Tanmay |
| Sem/Year : 5/ third year | Batch: B3 |
| Date of Experiment : 19-08-2020 | Date of Submission: |
| Grade -- |  |

**B.1: Code of performed experiment**

(Students are expected to write the code of performed experiment)

FRAME CONSIDERED:



1. Incoming Packet

2. 52.114.217.146

3. 192.168.1.103

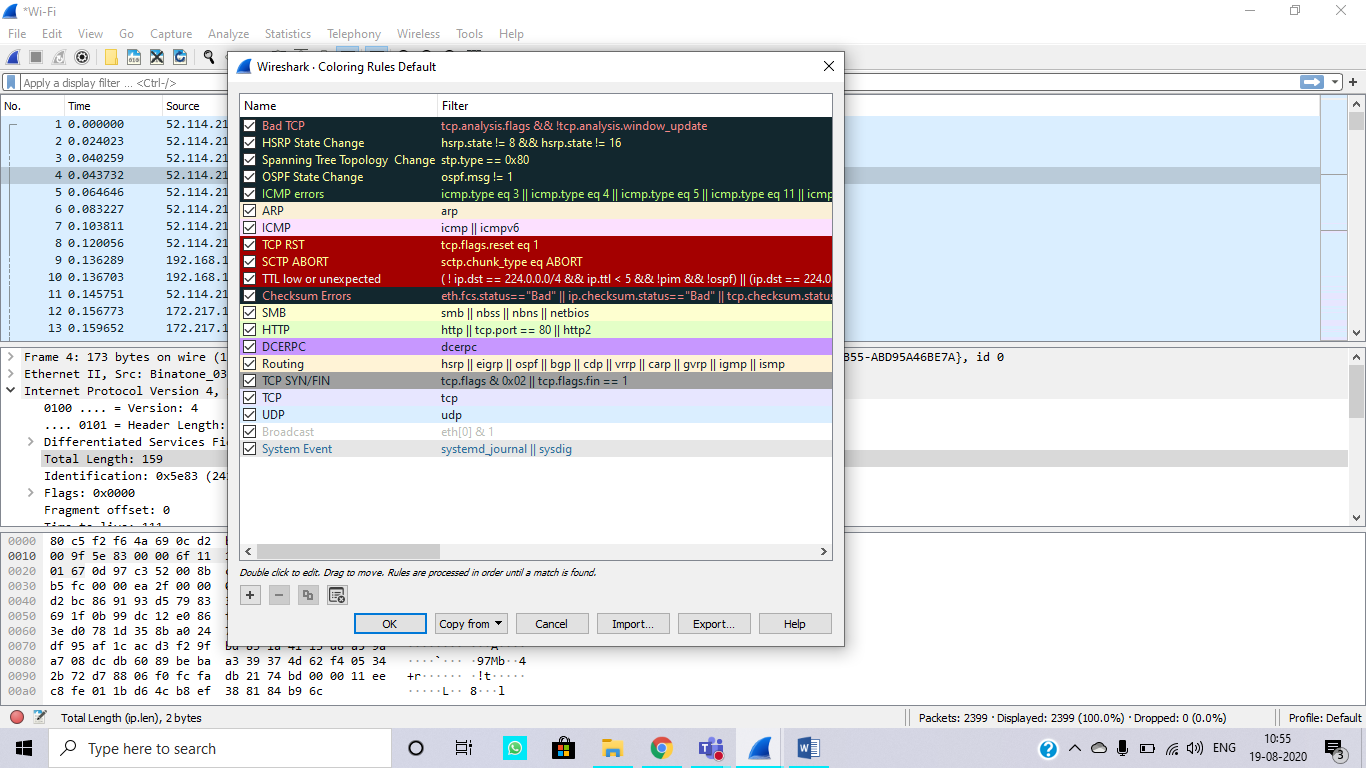
4. 173 Bytes

5. 14 bytes

6. 20 bytes (header) + 159 Bytes

7. 20 bytes (header) +700 Bytes

8.



**B.2: Observations and Learning’s:**

In this experiment, we learnt how packets are sent between IP address. We also saw about the information contained in the packets.

**B.3: Conclusion:**

We conclude that we could successfully retrieve information regarding the packets. We could figure out information like: IP header, TCP header, total number of bytes in a certain frame etc.