

**Experiment No.:10**

| **TITLE: Study of Packet Analyzer tool: Wireshark** |
| --- |

**AIM:** To study and analyse various Protocols using Packet Analyzer tool: Wireshark

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Expected Outcome of Experiment:**

**CO:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Books/ Journals/ Websites referred:**

1. A. S. Tanenbaum, “Computer Networks”, Pearson Education, Fourth Edition
2. B. A. Forouzan, “Data Communications and Networking”, TMH, Fourth Edition

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Pre Lab/ Prior Concepts:**

IPv4 Addressing, Subnetting, Link State Protocol, Router configuration Commands

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**New Concepts to be learned: Packet Analyzer tool: Wireshark**.

**THEORY:**

**Wireshark is an open-source packet analyzer widely used in education, network analysis, software development, protocol development, and network troubleshooting. Often referred to as a sniffer, network protocol analyzer, or simply a network analyzer, Wireshark enables users to capture and filter packets to meet specific requirements, aiding in various networking tasks. Network security engineers use it frequently to investigate security issues. As a free tool, it captures incoming and outgoing data, often being described as a free packet-sniffing application. Wireshark operates the network card in a "promiscuous" mode, allowing it to accept and capture all incoming packets.**

**Uses of Wireshark**

**Network security engineers use it to analyze and address security issues.**

**It enables users to view all traffic passing through a network.**

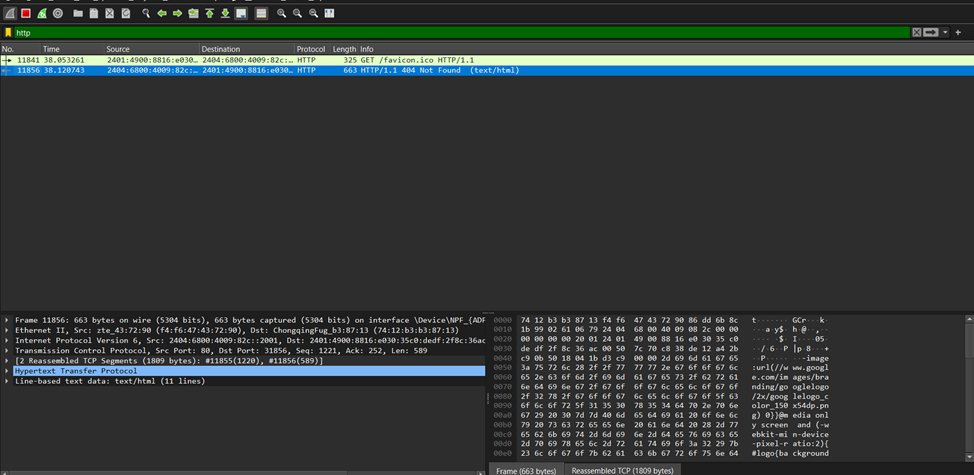
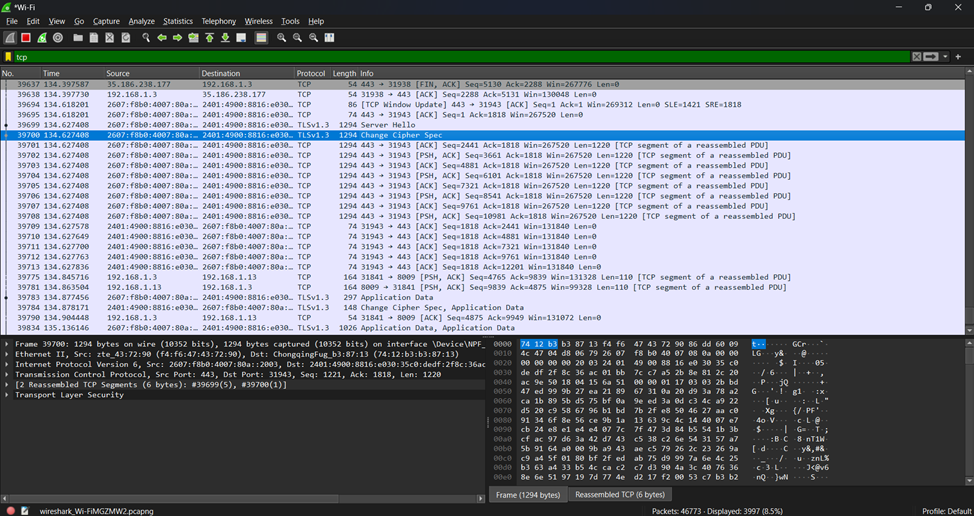
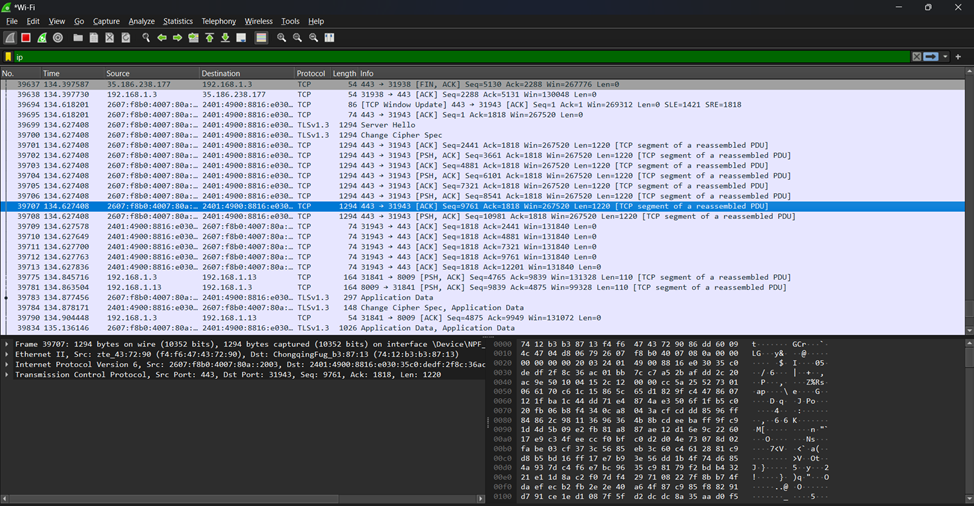
**Network engineers rely on it to troubleshoot and resolve network problems.**

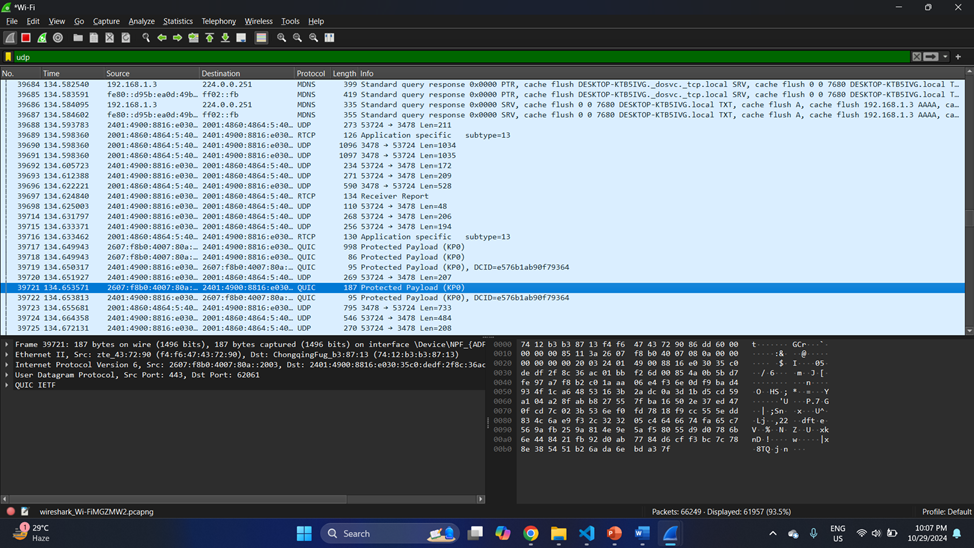
**It is helpful for diagnosing latency issues and identifying malicious activities on the network.**

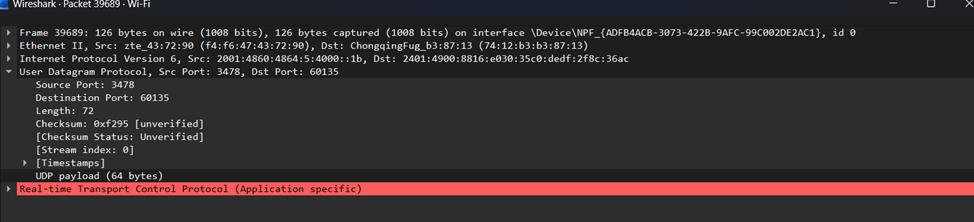
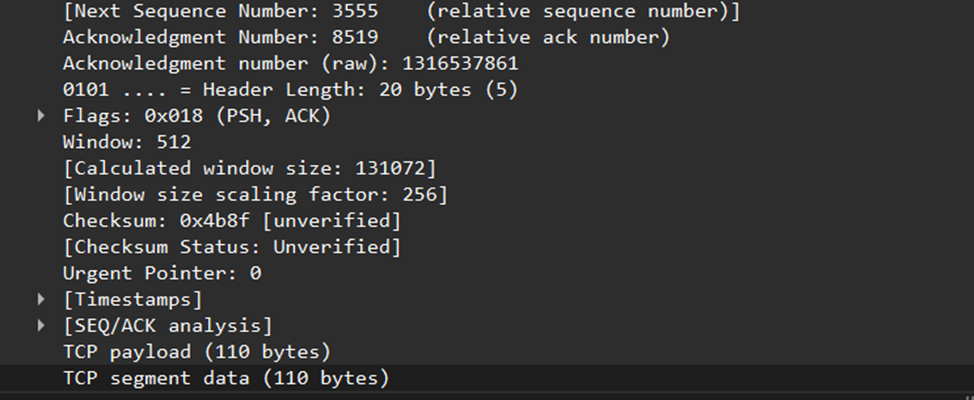
**Wireshark can analyze and identify dropped packets.**

**It reveals how devices such as laptops, smartphones, desktops, switches, and routers communicate within a local network or globally.**

**IMPLEMENTATION:**

**  
  
  
  
  
  
  
**

****

**  
**

**CONCLUSION:**

Learned Packet Analyzer tool:WireShark.

**Date: 30/10/24 Signature of faculty in-charge**