**Batch:** *A-4* **Experiment Number:** *3*

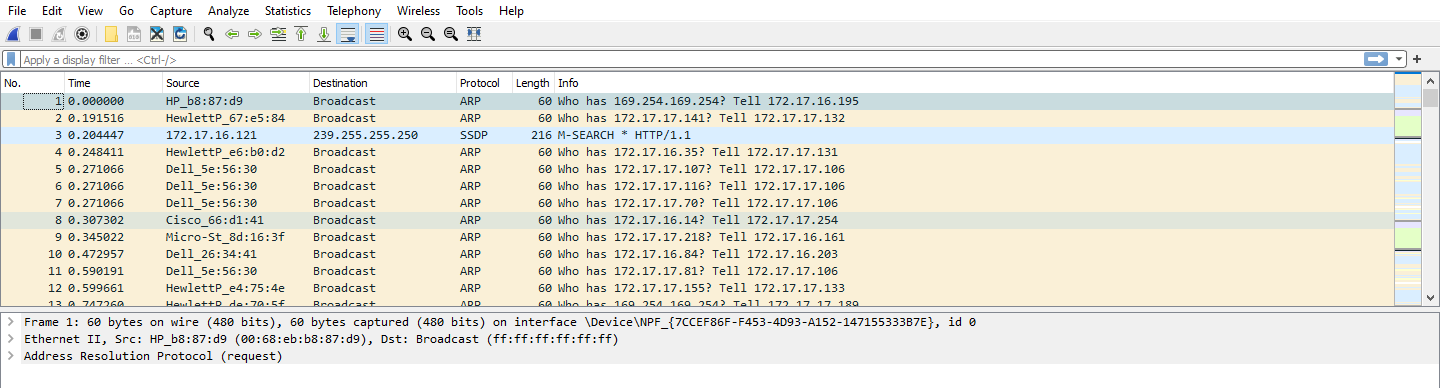
**Roll Number:** *16010422211*  **Name:** *Chetana Kulkarni*

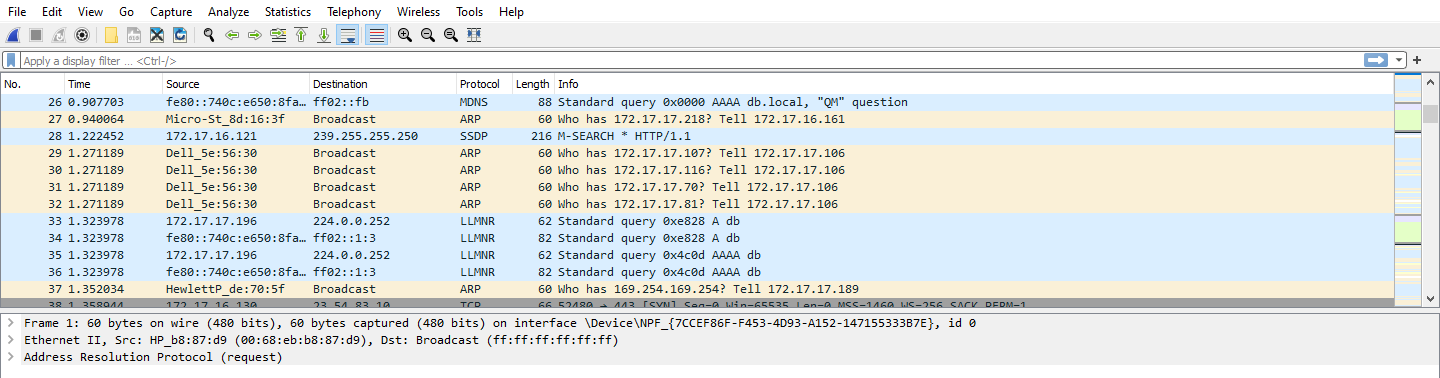
**Aim of the Experiment: To explore application layer protocols with packet analysis using Wireshark.**

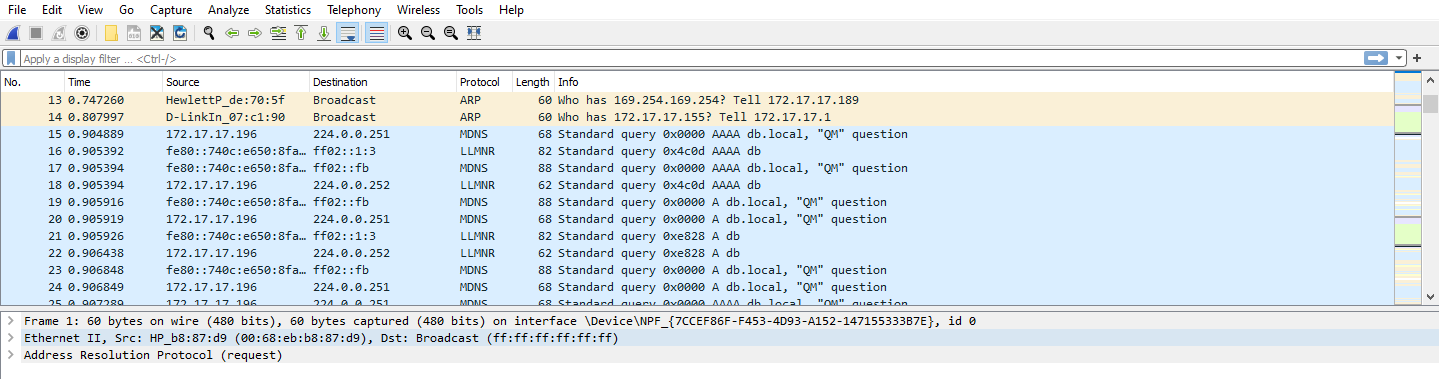
**Program Code:**

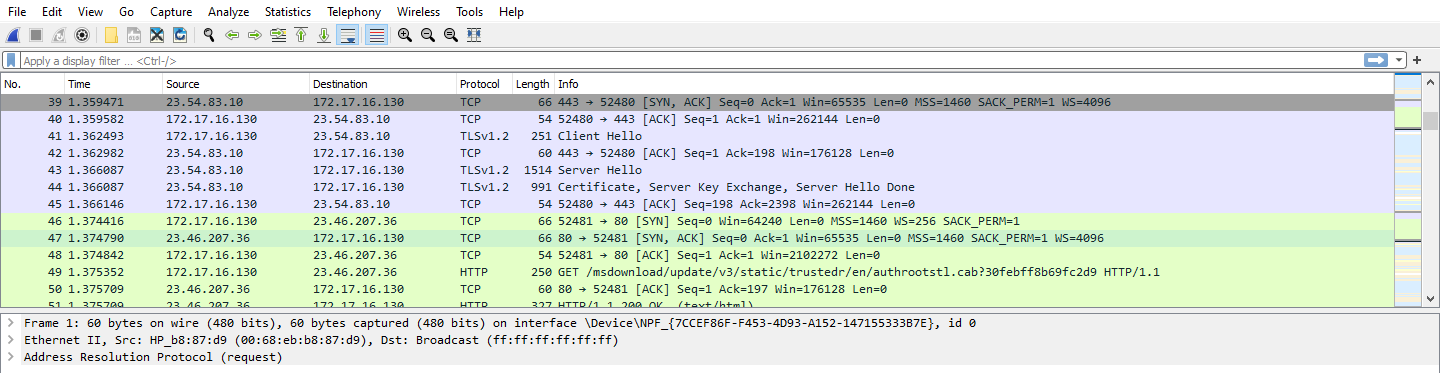
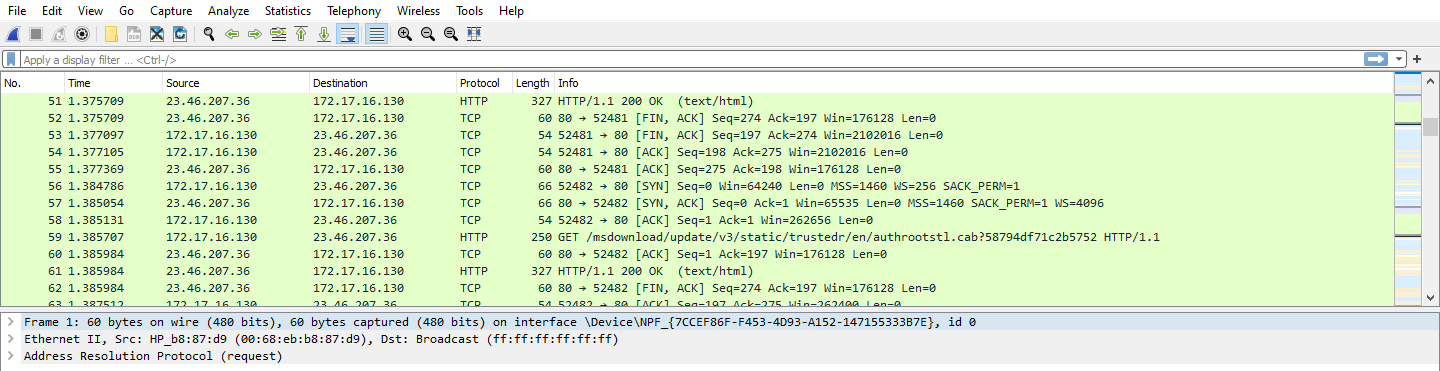
**Output/Result:**

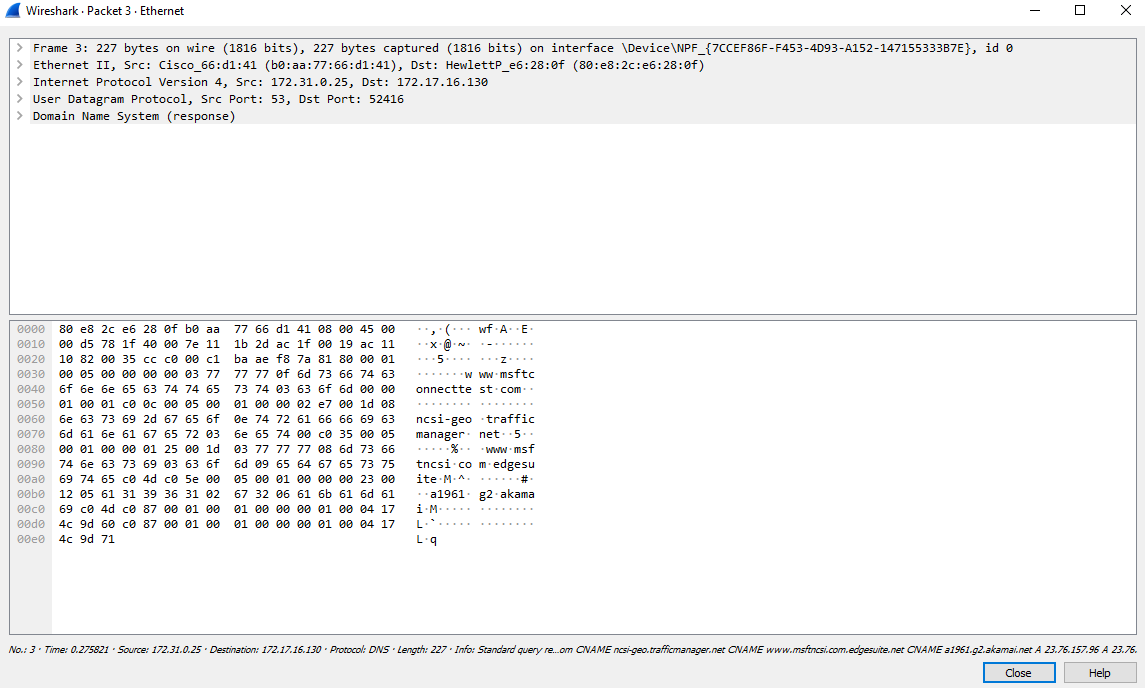
1. *Capture a packet.*

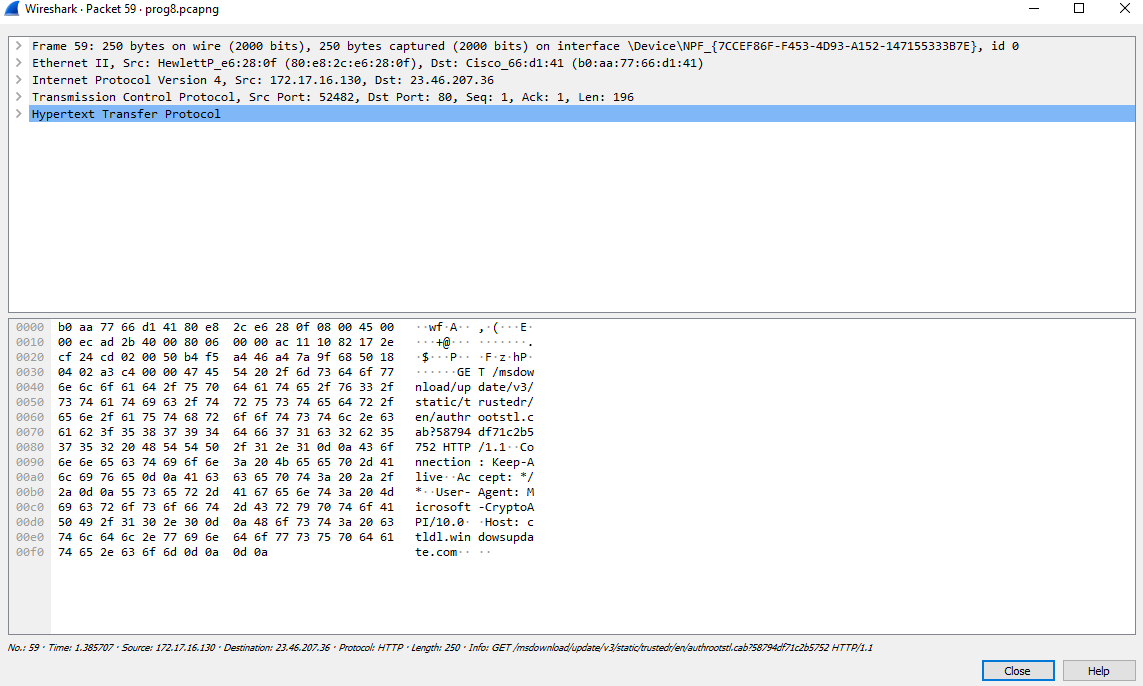




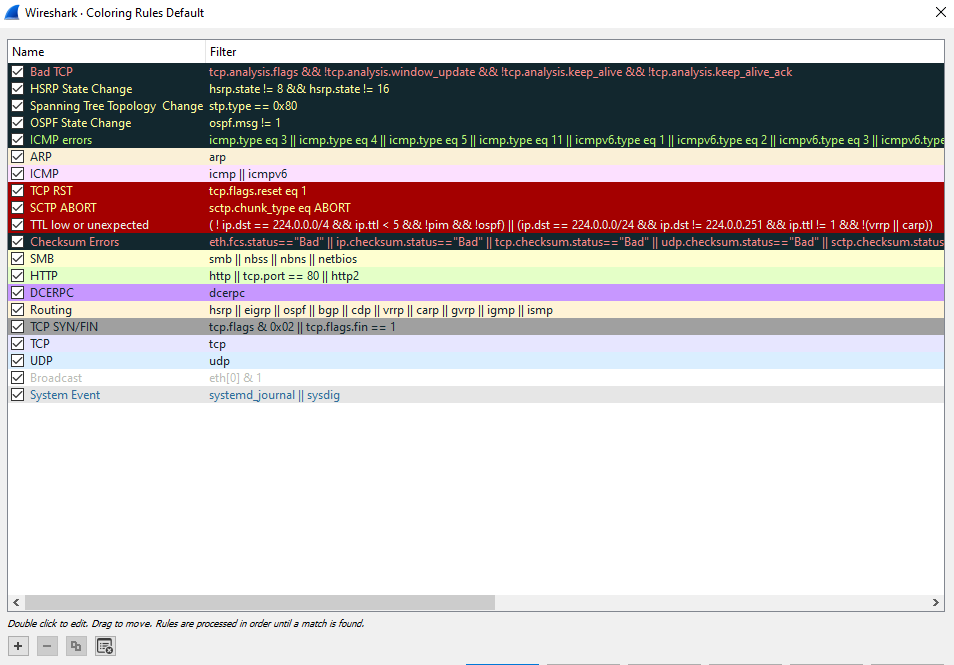


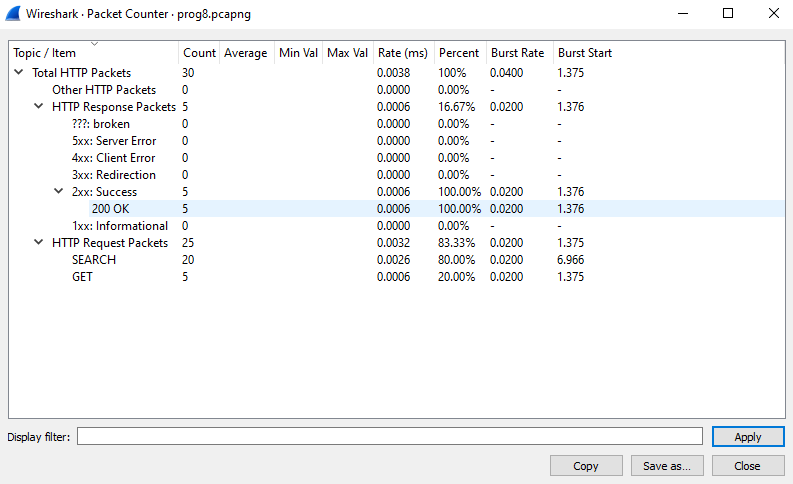
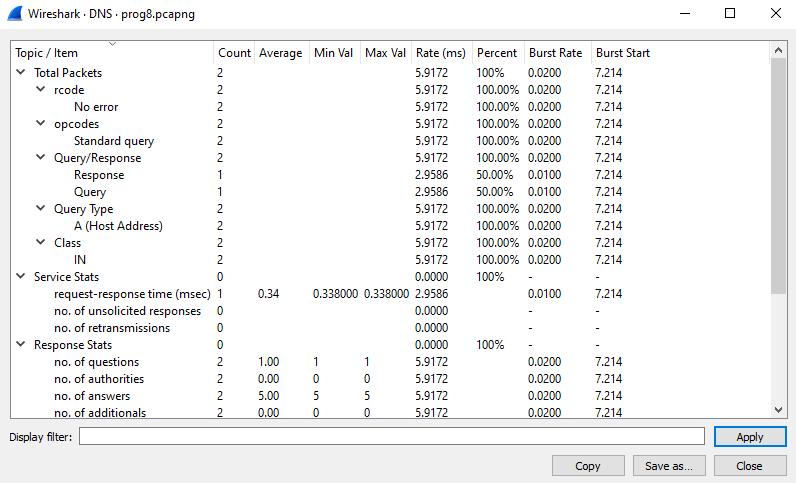




1. *Color coding of different protocols.*



1. *Statistics for the application layer protocol you have chosen.*

**Post Lab Question-Answers:**

*1***)** *Wireshark is a packet analyzer used for network troubleshooting, capturing, and analyzing packets. NMAP is a network scanner for discovering hosts and services on a network , aiding security assessments.*

*2) Wireshark primarily operates at the OSI model’s Data link layer (layer 2) and Network Layer (layer 3), analyzing and capturing network packets to provide detailed insights into network traffic.*

*3) tcpdump*

*Tshark(Command-line version of Wireshark)*

*Microsoft Message Analyzer*

*Fiddler*

**Outcomes:** *CO2: Enumerate the layers of the OSI model and TCP/IP model, their functions and protocols.*

**Conclusions:** *Learnt how to use Wireshark software for capturing packets and captured few of the protocols from the application layer like HTTP & DNS.*

**References:** *Wireshark User Manual*

[*https://www.wireshark.org*](https://www.wireshark.org)

*Behrouz Forouzan “Data Communication & Networking”, Tata McGrawhill, India 4th Edition*