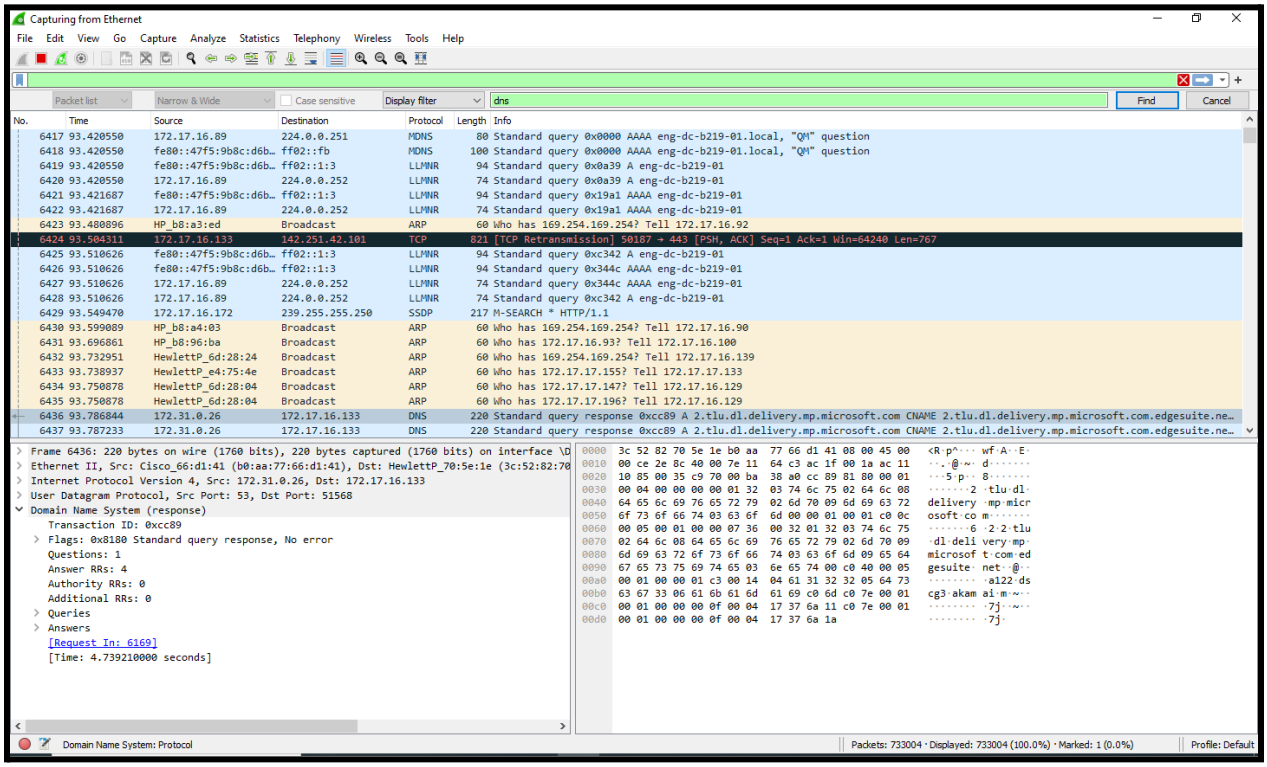
Batch: B3 **Experiment Number: 3**

Roll Number: 16010422185 **Name: Pratham Panchal**

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

Program/ Steps:

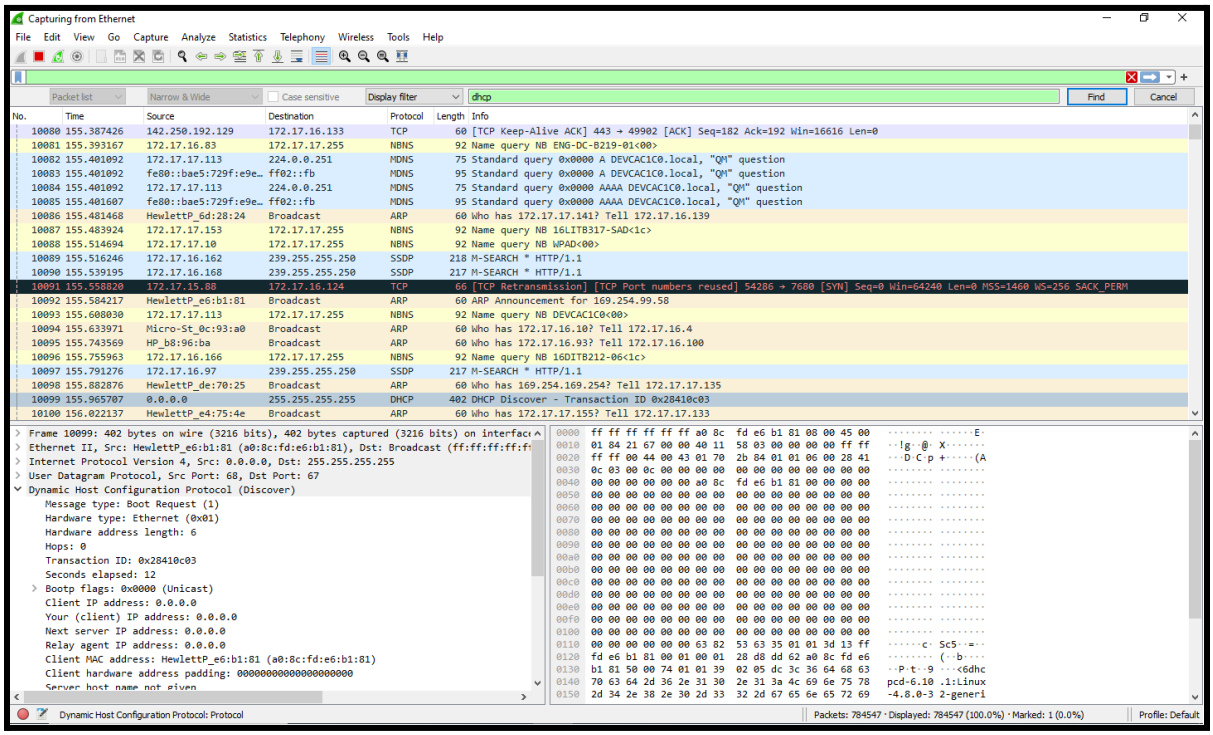
1) **DNS :**



Structure:

Transaction ID: 0xcc89	Flags : 0x8180
Questions : 1	Answers RRs :4
Authority RRs :0	Additional RRs :0
Queries : 2.tlu.dl.delivery.mp.microsoft.com	
Answers : 2.tlu.dl.delivery.mp.microsoft.com	

2) DHCP :



Structure:

Message Type : Boot request(1)	htype : Ethernet	hlen : 6	hops : 0
Transaction ID : 0x28410c03			
Seconds : 12		Flags 0x0000	
Client IP Address : 0.0.0.0			
Your IP Address : 0.0.0.0			
Server IP Address : 0.0.0.0			
Gateway IP Address : 0.0.0.0			
Client MAC Address : a0:8c:fd:e6:b1:81			
Server Name : not given			
Boot File Name : not given			
Options : DHCP message type		Magic cookies : DHCP	

Post Lab Question-Answers:

1) **What is the difference between Wireshark software and NMAP software?**

-

Gerne of comparison	Nmap	Wireshark
Purpose of use	Nmap is primarily chosen for the use case of network scanners. Network scanner enables information regarding groups, shares, services, usernames of the computers in the network to be fetched and saved for future processing.	Wireshark falls into the category of packet scanner. The objective is similar to network sniffing where network traffic that is a part of the entire larger network of the system is intercepted and logged for future processing.
Features	Nmap comprises various features very different from that of Wireshark in order to fulfill the task of network scanning. Some of the features include host discovery, scanning of ports, detecting versions of the applications, fingerprinting of TCP/IP stack, and scriptable interaction.	Wireshark makes sure it encompasses the required features in order to fulfill the task of packet scanning. These features include capturing packets of the different protocols, parsing, and displaying the fields from the capture only on the types of network that pcap supports.

Made available by	Nmap is made available by insecure.org.	Wireshark is made available by wireshark.org.
Written in	Nmap is written in languages like C, C++, Python, Lua although it is a cross-platform tool	Wireshark is written only in C and C++ although it being a cross-platform tool.
Return type	Since Nmap is a targeted scanning, Nmap will return only the details from the scanned network. For example, details of only the IP the network is connected to.	Wireshark is mostly generic scanning and hence returns details of every request that is made in the network.
Allows to learn	Nmap allows applications to learn about the other computers that are available on the network.	Wireshark allows an application to learn what is being sent or receive on one's computer.

2) At which of the OSI layer Wireshark runs?

-It runs at the Data link layer.

3) Just write down the names of the softwares which have similar functionality as Wireshark. (open source or proprietary)

-1. tcpdump

2. Tshark

3. Colasoft Capsa

4. Microsoft Message Analyzer

5. NetworkMiner

Outcomes:

CO2. Enumerate the layers of the OSI model and TCP/IP model, their functions and Protocols.

Conclusion (based on the Results and outcomes achieved):

We learnt how to analyze packets of different protocols using wireshark software.

Grade: AA / AB / BB / BC / CC / CD /DD

Signature of faculty in-charge with date

References:

Books/ Journals/ Websites:

- **Behrouz A Forouzan, "Data Communication and networking", Tata McGraw hill, India, 4 th Edition**
- **http://www.wireshark.org**
- **Wireshark user manual.**