**Batch: B-1 Experiment Number: 3 - Application layer protocols.**

**Roll Number: 16010422234 Name: Chandana Ramesh Galgali**

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

**Program/ Steps:**

1. Start the machine as an administrator.

2. Start the internet.

3. Go to the official website of Wireshark. (www.wireshark.org) and download the old

stable version of Wireshark for 32 bit windows operating system.

4. After successful installation you will get the blue icon of Wireshark on the desktop.

5. Click on the icon and start the software.

6. Choose an interface and start capturing the packets.

7. Study the packet details of any one application layer protocols.

8. Understand color code in detail.

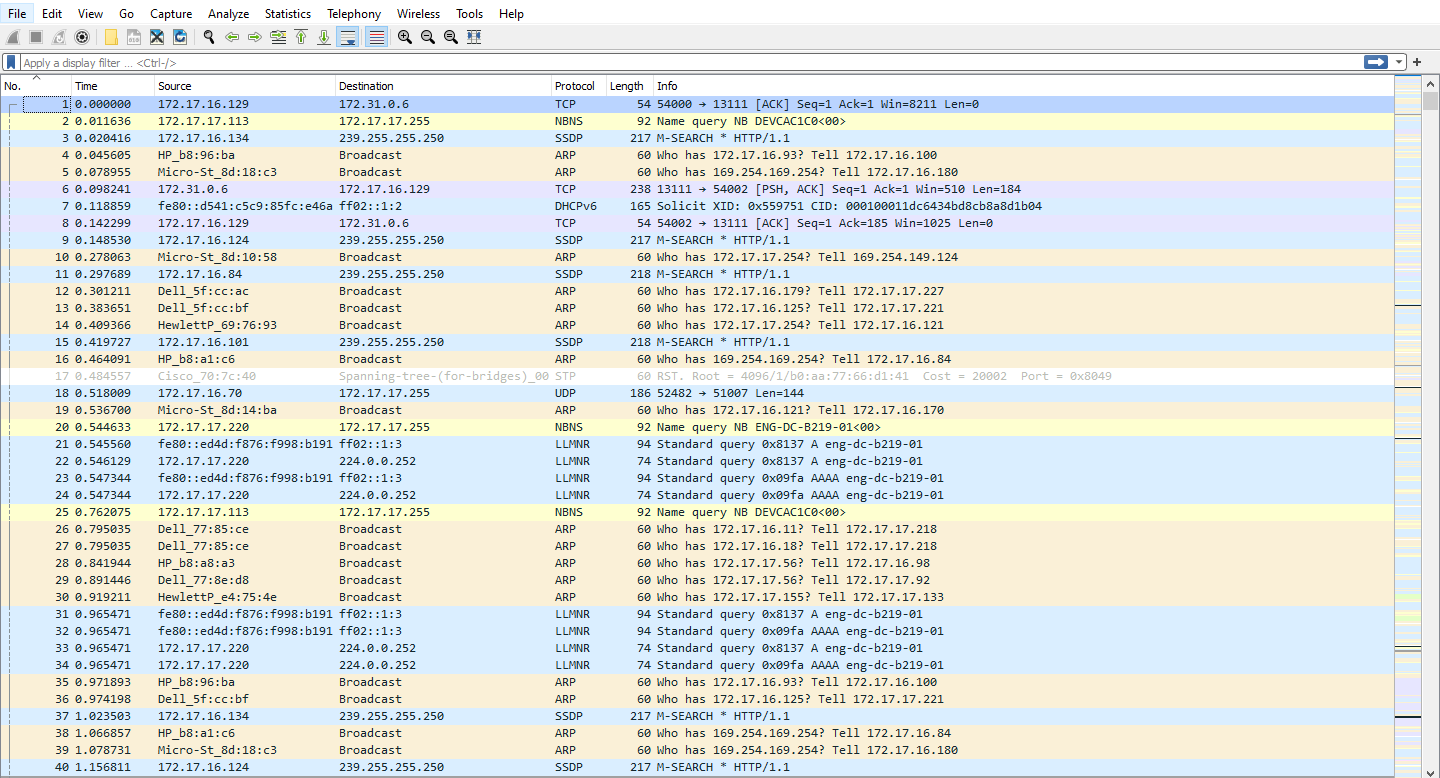
9. Perform the statistics for captured application layer protocol packets. (Every student

should perform for different protocols.)

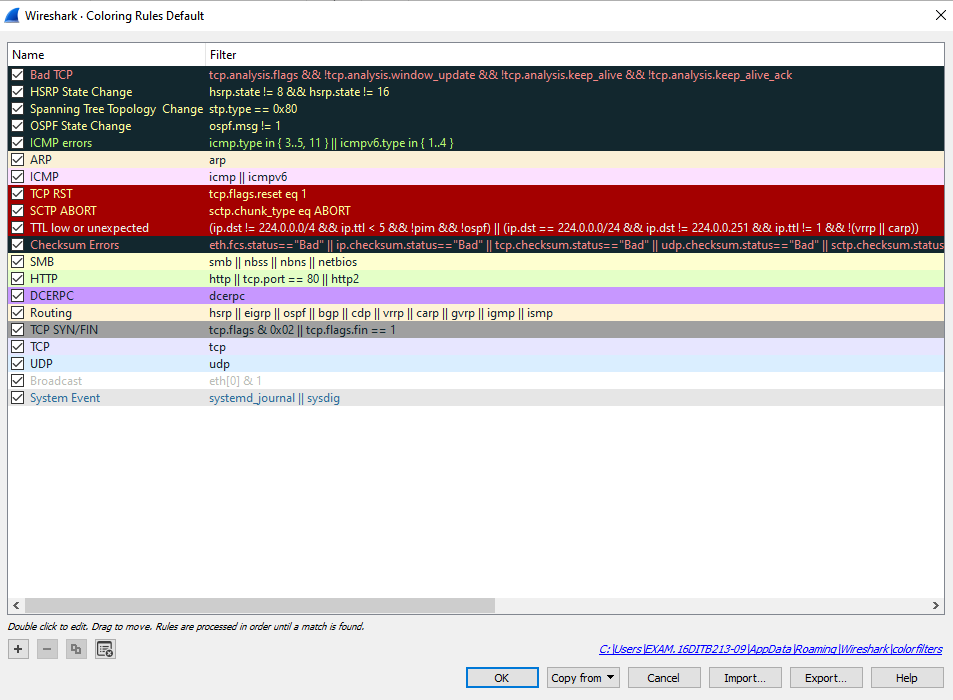
10. Show the output to the teacher and get it approved.

**Output/Result:**

**1. Capturing a packet.**

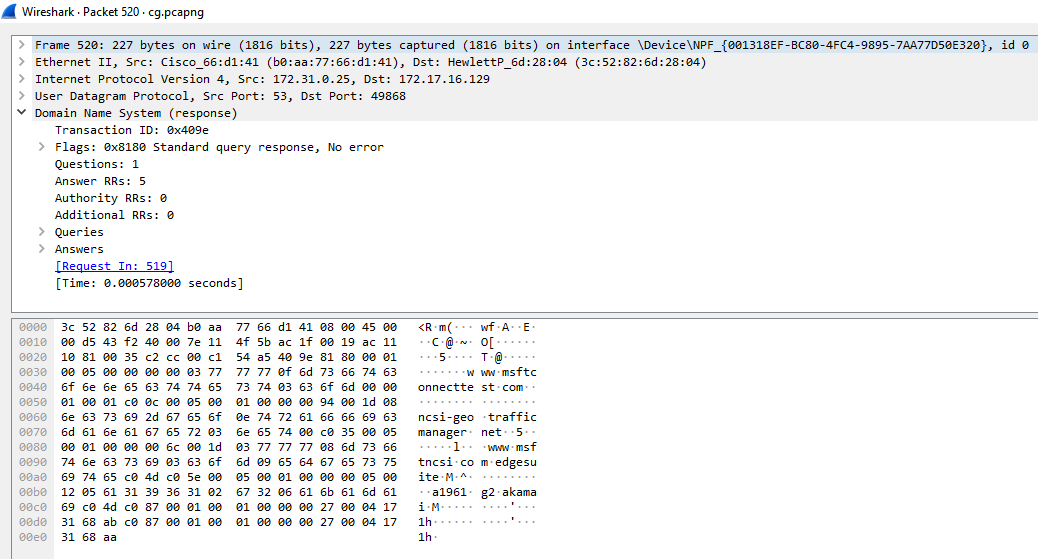
****

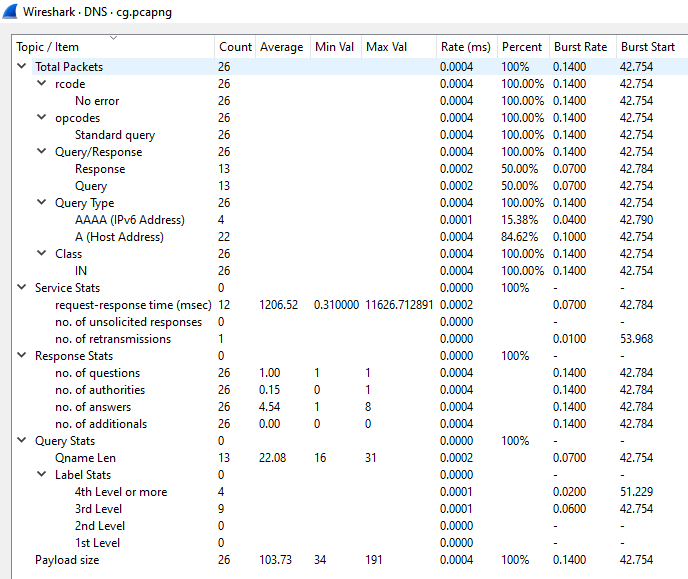
**2. Color coding of different protocols.**

****

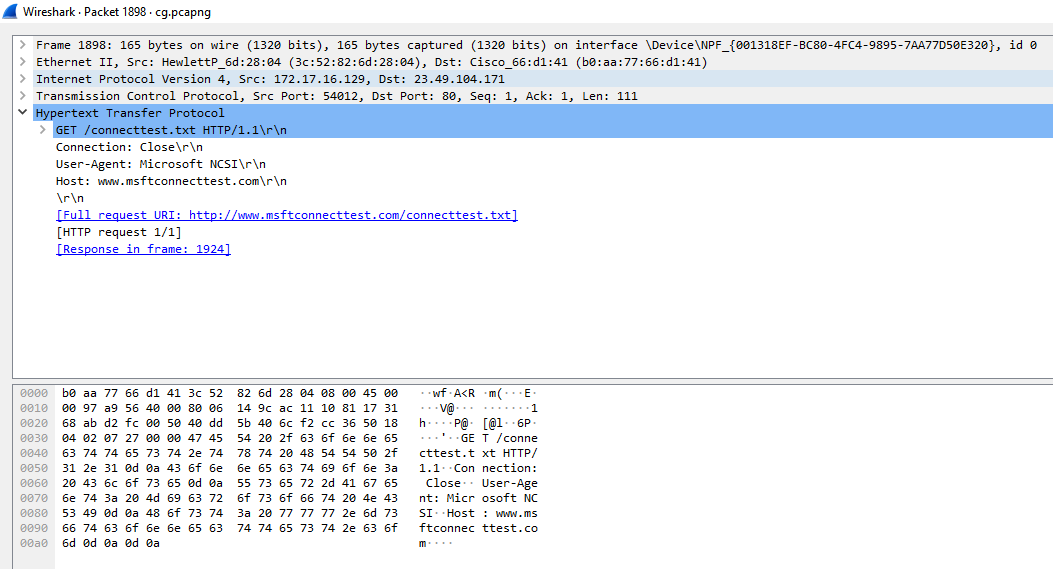
**3. Statistics for the application layer protocol you have chosen.**

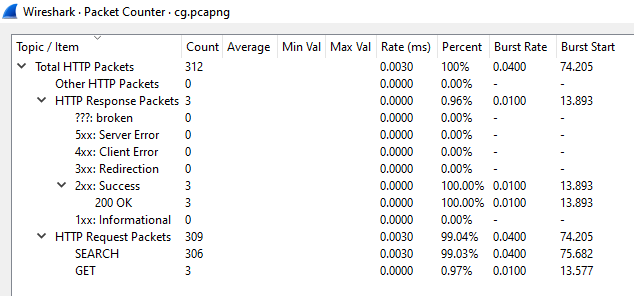
**DNS:**

****

****

**HTTP:**

****

****

**Post Lab Question-Answers:**

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

**Ans:** Wireshark and Nmap are both popular network analysis tools, but they serve different purposes and have distinct features. Here's a breakdown of the key differences between the two:

1. Functionality:
   * Wireshark: Wireshark is a network protocol analyzer that captures and analyzes network traffic in real-time. It allows you to inspect packets at a granular level, providing detailed information about network protocols, packet headers, and payload contents. Wireshark is primarily used for network troubleshooting, protocol analysis, and security auditing.
   * Nmap: Nmap (Network Mapper) is a network scanning tool used for host discovery, port scanning, and service enumeration. It helps identify open ports, detect operating systems, and gather information about network services running on target systems. Nmap is commonly used for network reconnaissance, vulnerability assessment, and penetration testing.
2. Scope:
   * Wireshark: Wireshark focuses on capturing and analyzing network traffic on a specific network interface or network segment. It provides a comprehensive view of the network communication between devices, allowing you to inspect individual packets and analyze network behavior.
   * Nmap: Nmap is designed for scanning and mapping networks to identify hosts, open ports, and services. It can scan large networks or specific IP ranges to discover active hosts and gather information about their network services.
3. User Interface:
   * Wireshark: Wireshark provides a graphical user interface (GUI) that allows users to interactively capture, filter, and analyze network traffic. It offers powerful filtering capabilities, customizable displays, and various analysis tools to dissect captured packets.
   * Nmap: Nmap primarily operates from the command-line interface (CLI), although there are graphical frontends available. It provides a wide range of command-line options and scripting capabilities, making it highly flexible and suitable for automation and scripting purposes.
4. Use Cases:
   * Wireshark: Wireshark is commonly used by network administrators, security analysts, and developers for troubleshooting network issues, analyzing network protocols, and investigating security incidents. It helps in diagnosing network performance problems, identifying malicious activities, and understanding network behavior.
   * Nmap: Nmap is widely used by network administrators, security professionals, and ethical hackers for network exploration, vulnerability scanning, and penetration testing. It helps in identifying open ports, assessing network security, and discovering potential vulnerabilities in systems.

In summary, Wireshark is primarily used for capturing and analyzing network traffic, while Nmap focuses on network scanning and host discovery. Both tools have their own strengths and are often used together to gain a comprehensive understanding of network behavior and security.

**2. At which of the OSI layer Wireshark runs?**

**Ans:** Wireshark operates at the lowest three layers of the OSI (Open Systems Interconnection) model, namely the Physical layer, Data Link layer, and Network layer.

1. Physical Layer: Wireshark can capture and analyze raw network traffic at the physical layer, including bits and electrical signals transmitted over the network medium. However, it is important to note that Wireshark typically captures data after it has been converted into a more readable format by the network interface card (NIC).
2. Data Link Layer: Wireshark can dissect and interpret data link layer protocols such as Ethernet, Wi-Fi (802.11), and others. It can analyze the frames exchanged between devices on a local network, including MAC addresses, frame types, and error detection.
3. Network Layer: Wireshark can capture and analyze network layer protocols such as IP (Internet Protocol), ICMP (Internet Control Message Protocol), and routing protocols like OSPF (Open Shortest Path First). It can provide insights into IP addressing, routing information, and network behavior.

While Wireshark primarily focuses on these lower layers, it also has the capability to analyze higher-layer protocols such as TCP (Transmission Control Protocol), UDP (User Datagram Protocol), HTTP (Hypertext Transfer Protocol), and many others. This allows for comprehensive analysis of network traffic across multiple layers of the OSI model.

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

**Ans:**

1. tcpdump: tcpdump is a command-line packet analyzer that captures and analyzes network traffic. It is available for various operating systems, including Linux, macOS, and Windows.
2. Microsoft Network Monitor: Microsoft Network Monitor is a proprietary packet analyzer developed by Microsoft. It allows for capturing and analyzing network traffic on Windows-based systems.
3. Tshark: Tshark is a command-line tool that is part of the Wireshark suite. It provides similar functionality to Wireshark but operates in a terminal environment, making it suitable for scripting and automation.
4. Colasoft Capsa: Capsa is a proprietary network analyzer that offers real-time packet capturing and analysis. It provides a graphical user interface and is available for Windows operating systems.
5. NetworkMiner: NetworkMiner is an open-source network forensic analysis tool that captures and parses network traffic. It focuses on extracting files, emails, and other artifacts from captured packets.
6. EtherApe: EtherApe is an open-source graphical network monitor that visualizes network activity in real-time. It provides a visual representation of network traffic flows and can be used for basic packet analysis.
7. PRTG Network Monitor: PRTG is a proprietary network monitoring tool that includes packet sniffing capabilities. It allows for capturing and analyzing network traffic, along with monitoring various network parameters.

**Outcomes:**

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

**Conclusion (based on the Results and outcomes achieved):**

The experiment successfully explored application layer protocols using packet analysis with Wireshark. The insights gained from this analysis can contribute to network troubleshooting, performance optimization, and security enhancement.

**References:**

**Books/ Journals/ Websites:**

1. Behrouz A Forouzan, Data Communication and Networking, Tata Mc Graw hill, India, 4th Edition
2. A. S. Tanenbaum, ”Computer Networks”, 4th edition, Prentice Hall
3. Behrouz A Forouzan, Data Communication and Networking, Tata Mc Graw hill, India, 4th Edition
4. A. S. Tanenbaum, ”Computer Networks”, 4th edition, Prentice Hall