**AJAY KUMAR GARG ENGINEERING COLLEGE, GHAZIABAD**

**Department of Computer Science & Engineering**

****

LAB FILE

## COURSE : B.Tech (CSE)

**SEMESTER : IV**

## YEAR : 2nd Year

**SUBJECT : Cyber Security Workshop SUBJECT CODE : BCS-453**

|  |  |  |
| --- | --- | --- |
| **SUBMITTED TO:** | **SUBMITTED BY:** | **SUBMITTED TO:** |
| **Mr. Updesh Kumar** | **Name:** | **(HoD CSE)** |
| **Assistant Professor** | **Roll No:** |  |
| **CSE Department** | **Branch:** |  |
| **AKGEC, Ghaziabad** | **Section/Group:** |  |

Experiment-3

Packet Analysis using Wire shark

=====================================================================================

**Basic Packet Inspection:** Capture network traffic using Wire shark and analyze basic protocols like HTTP, DNS, and SMTP to understand how data is transmitted and received.

1. **Aim:** Study of packet sniffer tools like Wireshark.
2. **Objectives:** To observe the performance in promiscuous & non-promiscuous mode & to find the packets based on different filters.

* To understand the flow of network packets through the TCP/IP Stack
* Understand the TCP three-way handshake protocol
* To practice capturing FTP packet flow
* To analyze the FTP packet flow
* To learn how to use a network traffic capture and analysis tool, like Wireshark™

Packet Capturing (Packet Sniffing): A packet sniffer is an application which can capture and analyze network traffic which is passing through a system’s Network Interface Card (NIC). The sniffer sets the card to promiscuous mode, which means all traffic is read, whether it is addressed to that machine or not. The figure below shows an attacker sniffing packets from the network, and the Wireshark packet sniffer/analyzer (formerly known as ethereal).

1. **Outcomes:** The learner will be able to:-

* Identify different packets moving in/out of network using packet sniffer for network analysis.
* Understand professional, ethical, legal, security and social issues and responsibilities. Also will be able to analyze the local and global impact of computing on individuals, organizations, and society.
* Match the industry requirements in the domains of Database management, Programming and Networking with the required management skills.

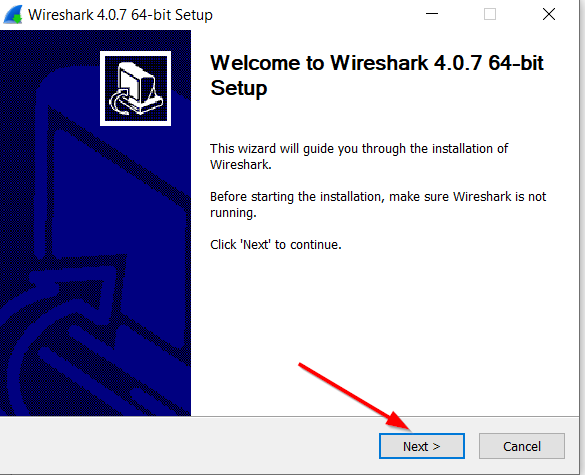
1. **Hardware / Software Required:** Wireshark, Ethereal and tcpdump.
2. **Theory:** Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and display them in human-readable format. Wireshark includes filters, color-coding and other features that let you dig deep into network traffic and inspect individual packets.
   1. **Applications:**
      * Network administrators use it to troubleshoot network problems
      * Network security engineers use it to examine security problems
      * Developers use it to debug protocol implementations
      * People use it to learn network protocol internals beside these examples can be helpful in many other situations too.
   2. **Features:** The following are some of the many features wireshark provides:
      * Available for UNIX and Windows.
      * Capture live packet data from a network interface.
      * Open files containing packet data captured with tcpdump/WinDump, Wireshark, and a number of other packet capture programs.
      * Import packets from text files containing hex dumps of packet data.
      * Display packets with very detailed protocol information.
      * Export some or all packets in a number of capture file formats.
      * Filter packets on many criteria.
      * Search for packets on many criteria.
      * Colorize packet display based on filters.
      * Create various statistics.

**Introduction to Wireshark**: Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible. You could think of a network packet analyzer as a measuring device for examining what’s happening inside a network cable, just like an electrician uses a voltmeter for examining what’s happening inside an electric cable (but at a higher level, of course) Downloading.

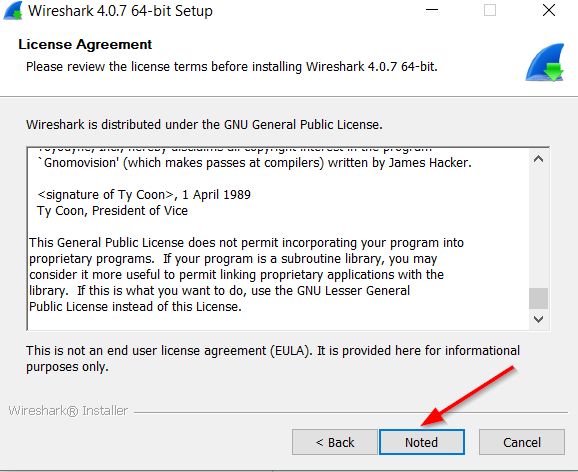
**Steps: 1**. Your first step is to head to the Wireshark download page and locate the Windows installer.

**2.** You will be presented with the Wireshark wizard to guide you through the installation. Click “Next.”

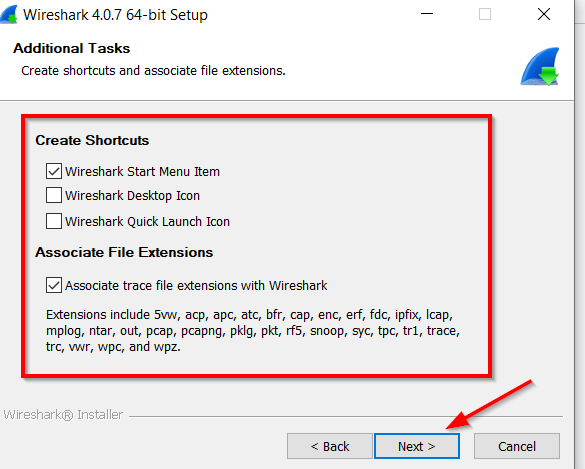
**3.** Next, you can review, agree to the license agreement, and click “Noted” to continue.



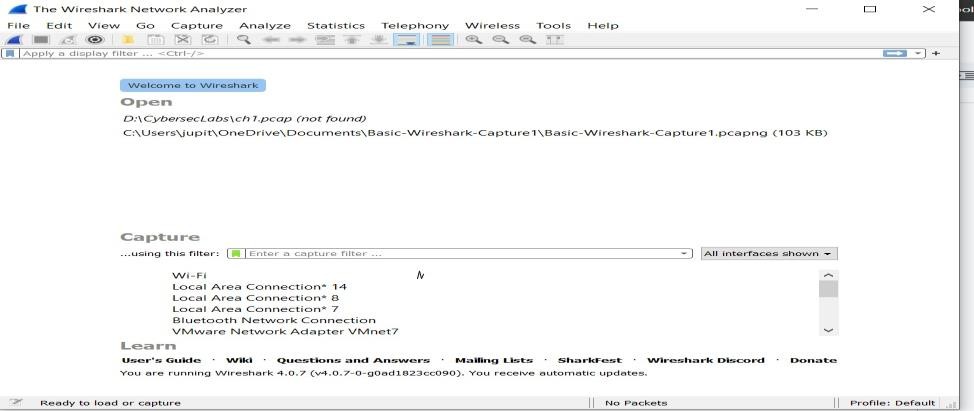
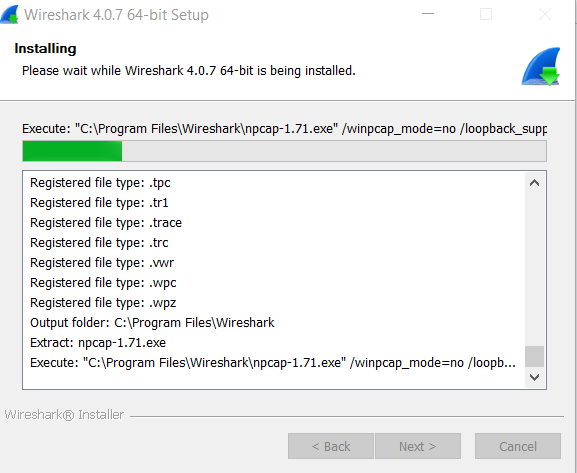
Once your file is downloaded, you can open the file from your Download folder.



1. The next screen will ask if you want to donate to the Wireshark Foundation to help support Wireshark and Sharkfest at https://wiresharkfoundation.org/. Click “Next” when finished.
2. Next, you will be asked what components you want to install. You can make your choice and then click“Next.”
3. The following screen will ask if you want to create any shortcuts and if you want to associate trace file extensions with Wireshark (recommended).



1. Now you must install Ncap (an open-source library for packet capture and network analysis). It’s a library allowing Wireshark to capture and analyze network traffic effectively. It enhances Wireshark's capabilities by providing optimized packet capture.
2. Wireshark will now begin the installation process.

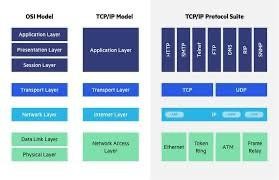
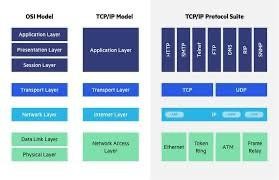


**Objective 1:** Basic Packet Inspection: Capture network traffic using Wire shark and analyze basic protocols like HTTP, DNS, and SMTP to understand how data is transmitted and received.

Tool Used: Wireshark Protocols used in different OSI Layers:

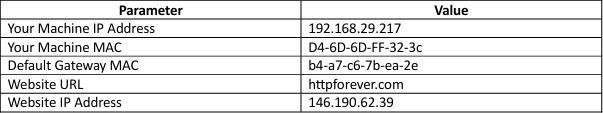
RECEIVER/SERVER

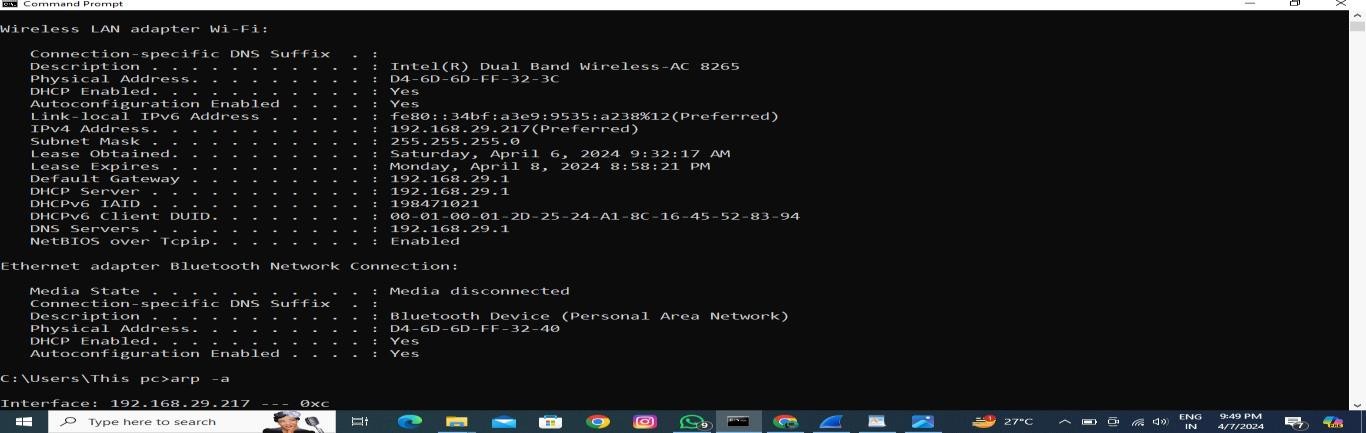
SENDER/BROWSER

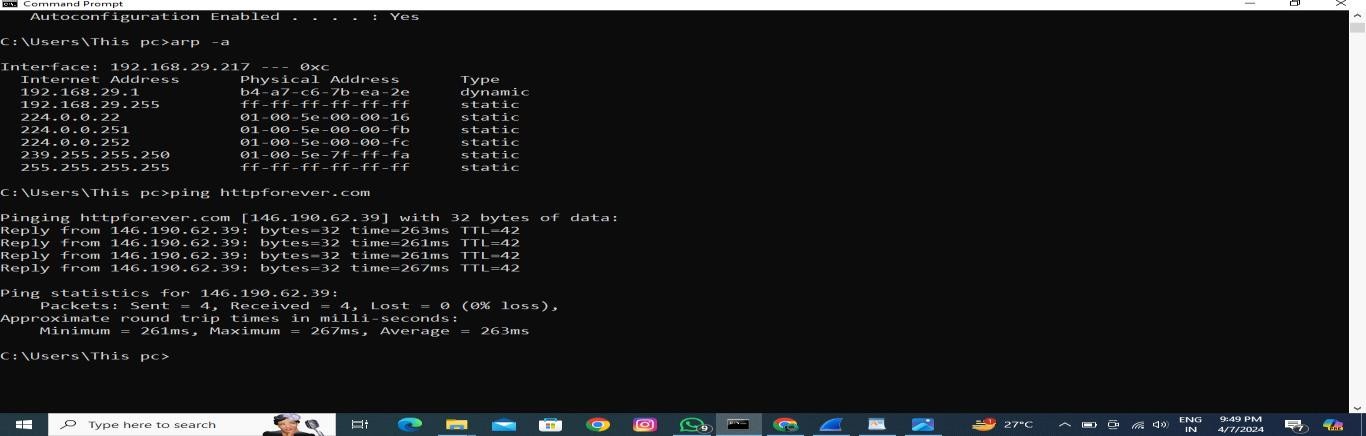
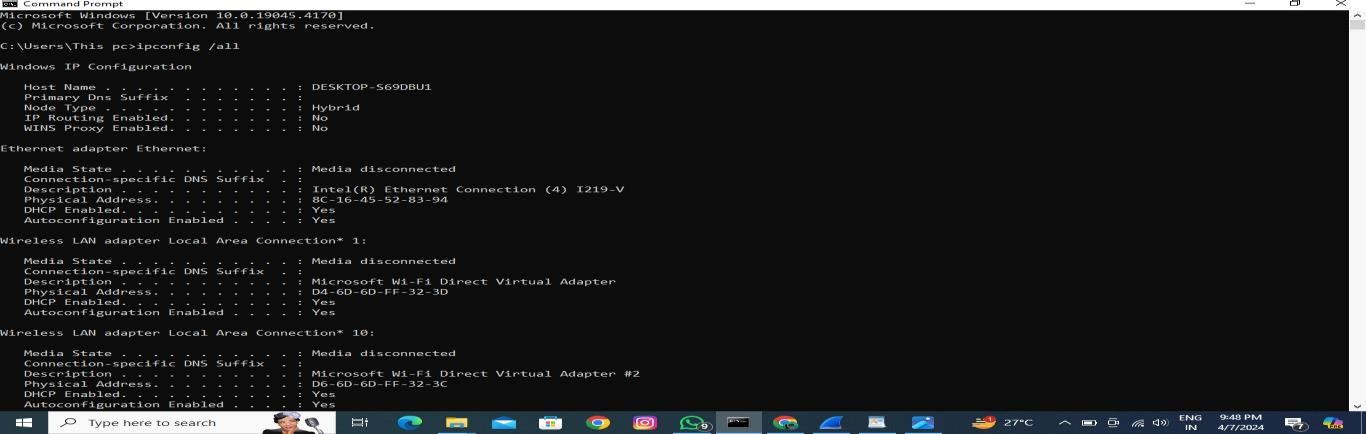


**Commands used for making Reference Table:**

* Ipconfig /all (for getting information of local host)
* arp -a (for getting MAC address of Gateway)
* ping httpforever.com for capturing http packets







1. **Steps to Analyse HTTP protocol**

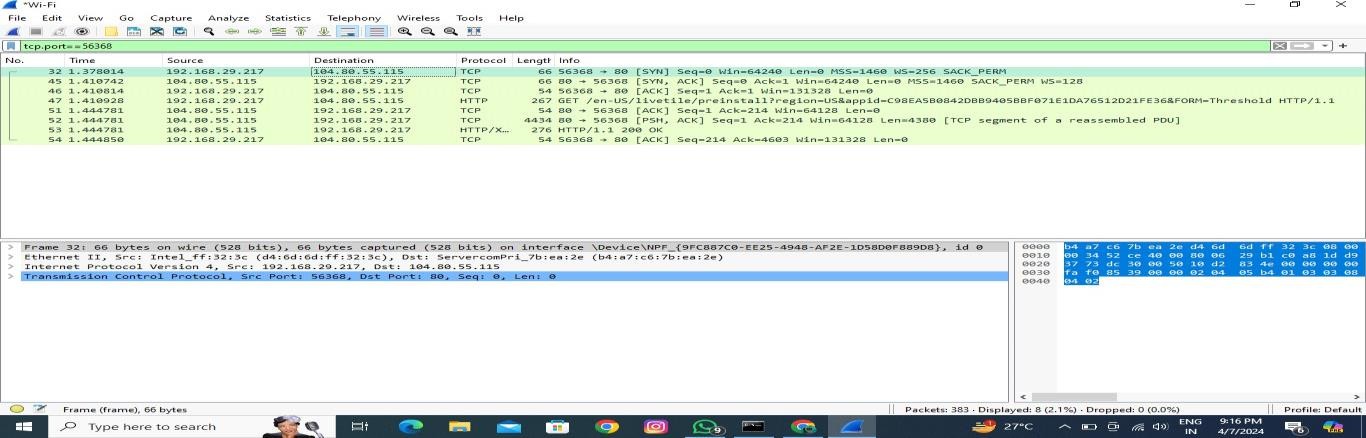
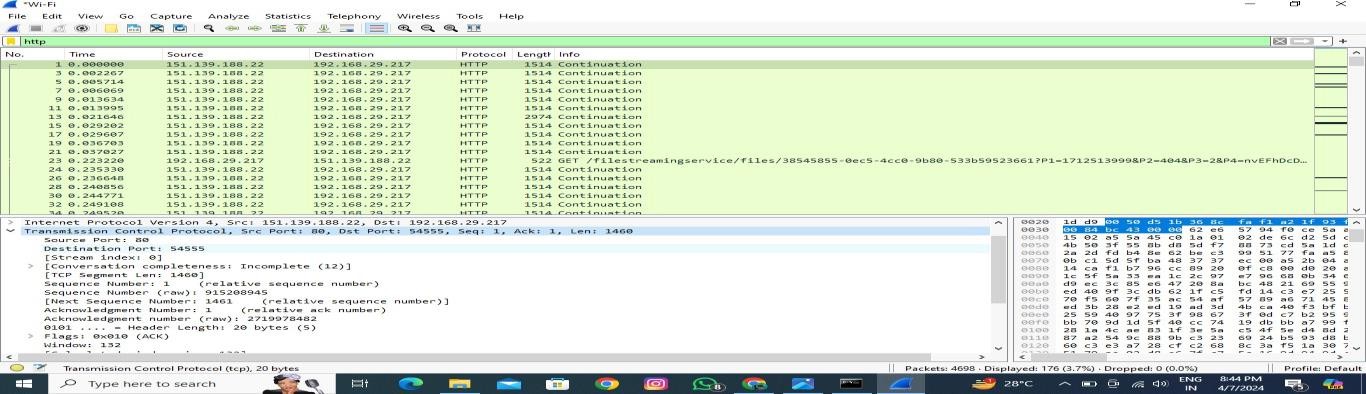
Step 1: Open ether/wifi adapter in Wireshark Step2: Apply http filter as given below:

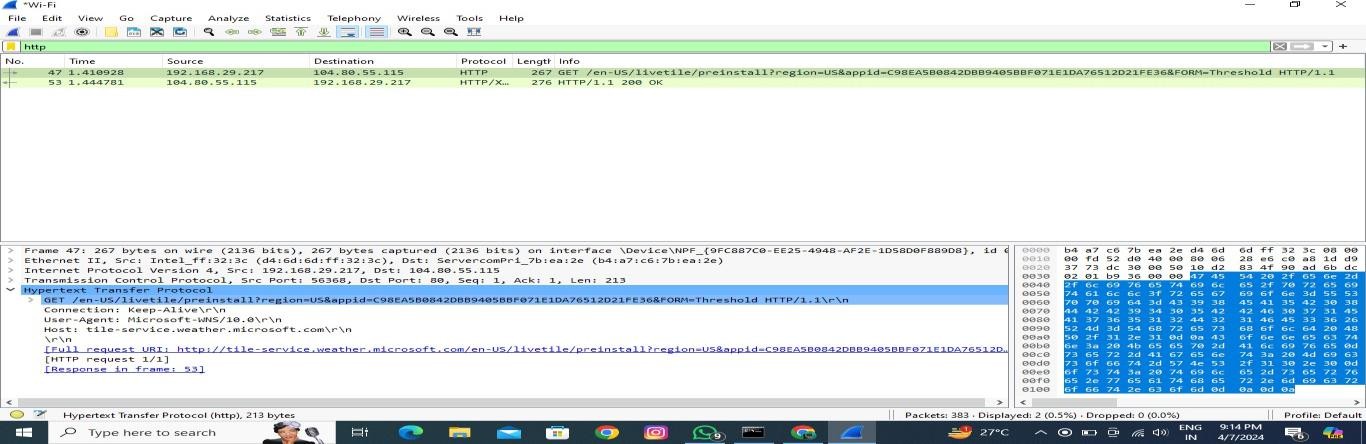
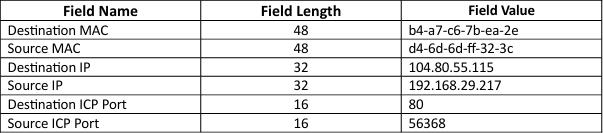
Step 3: Start Capturing

Step 4: open httpforever.com in the browser Step

5: Analyse the TCP data (source port, destination port), source Mac, Destination Mac, Source Ip etc. and compare it with the reference table

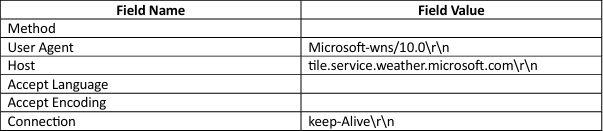
Step 6: check 3way handshaking befor establishing http connection by using the filter tcp.port==56368\*

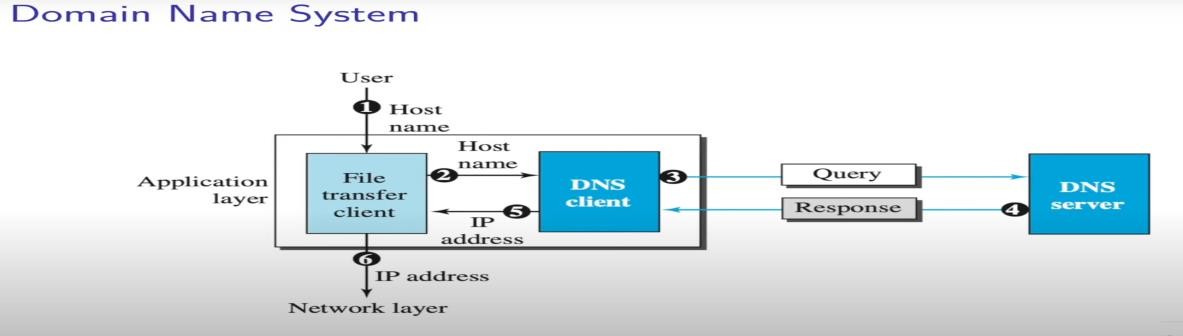




Step 7: Now finally record the data for http header in the table given ABOVE.

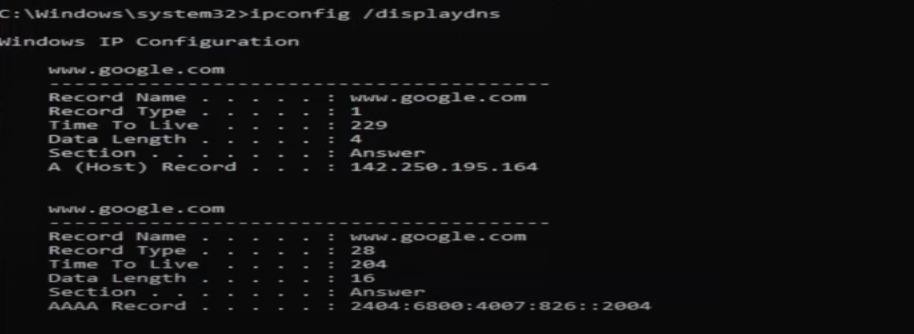
1. **Steps to analyse DNS protocol**

****

DNS:

**Command for cmd:**

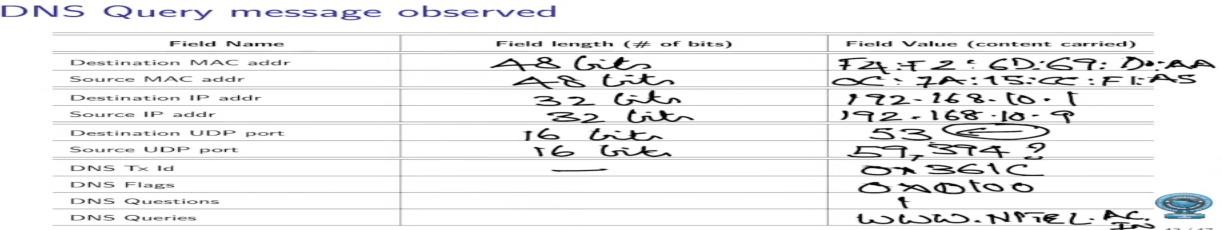
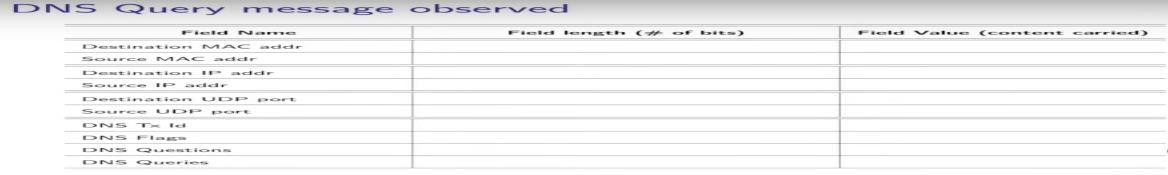
ipconfig /displaydns ipconfig /flushdns



**DNS observation Step:**

1: Start capturing via Wireshark Step

2: ping nptel.ac.in (command prompt) Step 3: Apply dns protocol filter in wireshark Step 4: Observe the data in the given table:

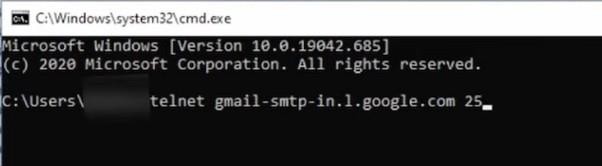


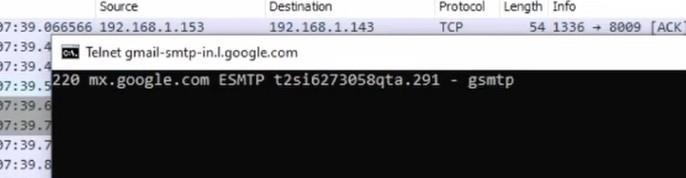
**Step to analyse SMTP protocol**

**Step 1: Start capturing via Wireshark**

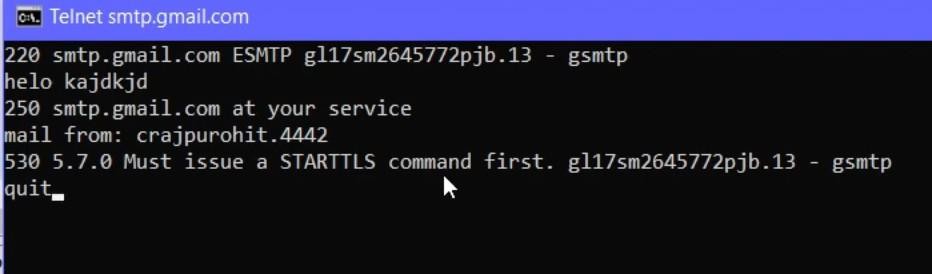
**Step 2: Enable the telnet feature by usin windows feature service Step 3: telnet gmail-smtp-in.l.google.com 25 (command prompt)**

Helo sahil

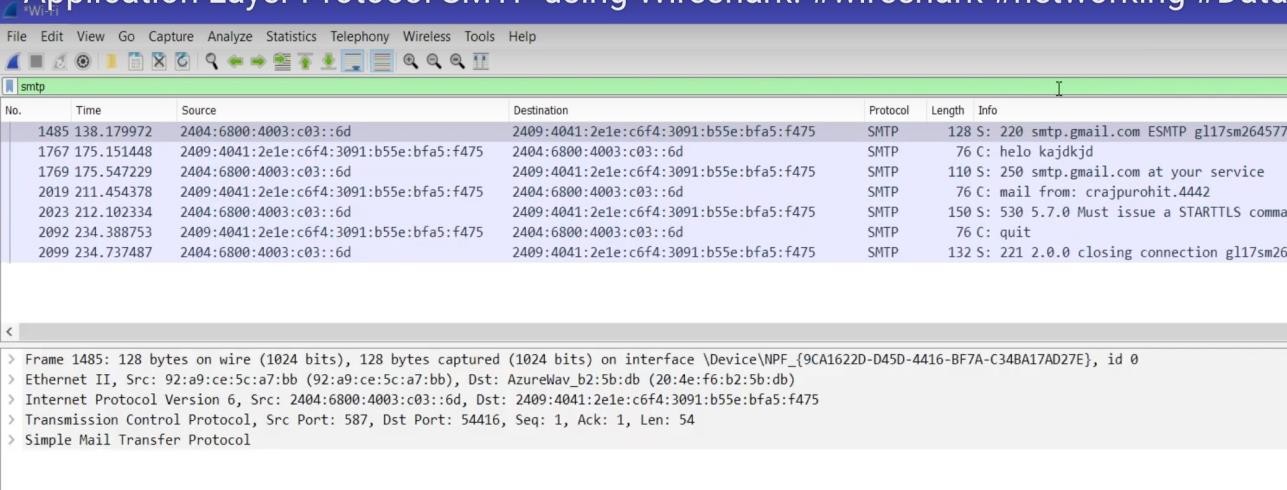




Commands to use:



**Step 3: Apply smtp protocol filter in Wireshark Step 4: Observe the data in SMTP:**



**Note:** Wireshark is an extremely powerful tool, and this tutorial is just scratching the surface of what you can do with it. Professionals use it to debug network protocol implementations, examine security problems and inspect network protocol internals.

**Conclusion:** In this experiment we analyze various packet sniffing tools that monitor network traffic transmitted between legitimate users or in the network. The packet sniffer is network monitoring tool. It is opted for network monitoring, traffic analysis, troubleshooting, Packet grapping, message, protocol analysis, penetration testing and many other purposes.

**RESULT:** This experiment successfully executed using Wireshark.