

Lab Assignment: Introduction to Wireshark

Objective:

The objective of this lab assignment is to introduce students to Wireshark, a widely used network protocol analyzer, and familiarise them with its basic functionalities. By completing this assignment, students will gain hands-on experience in capturing and analysing network traffic.

Requirements:

- Computer with Wireshark installed (Download Wireshark from: <https://www.wireshark.org/download.html>)
- Access to a network (Wi-Fi or Ethernet)

Tasks:

Task 1: Installing Wireshark

- Download Wireshark from the provided link.
- Follow the installation instructions for your operating system.
- Ensure Wireshark is installed correctly by launching the application.

Task 2: Capturing Network Traffic

- Launch Wireshark.
- Select the network interface through which you want to capture traffic (e.g., Wi-Fi, Ethernet).
- Click on the green 'Start' button to begin capturing traffic.
- Perform various activities such as visiting websites, sending/receiving emails, or using applications that require network connectivity.
- After capturing traffic for a sufficient amount of time (at least 1 minute), click on the red 'Stop' button to stop capturing.

Task 3: Analysing Captured Traffic

- Explore the captured packets in Wireshark.
- Identify different protocols used in the captured traffic (e.g., HTTP, TCP, UDP).
- Filter the captured packets based on specific protocols or criteria (e.g., HTTP traffic only, packets from a specific IP address).
- Analyse the contents of selected packets to understand the communication between devices.

- Take note of any suspicious or interesting findings during the analysis.

Task 4: Exporting Captured Data

- Export captured packets to a file for further analysis or sharing.
- Choose an appropriate file format for export (e.g., .pcap, .csv).
- Save the exported file to a location of your choice.

Task 5: Documentation and Reflection

- Document your observations and findings during the packet capture and analysis process.
- Reflect on the importance of network protocol analysis and the potential real-world applications of Wireshark.
- Discuss any challenges encountered during the assignment and how you overcame them.