

**Department of Computer Science and Engineering**  
**International Islamic University Chittagong**

**M.Sc in Computer Science and Engineering**



**Assignment 2**

**Packet Sniffing using Wireshark**  
**Subject: Network Security**  
**Course Code: CSE6251**

submitted to

**Mohammad Zainal Abedin**  
**Assistant Professor**

by

**Redoan Ahmed (MC223107)**

# 1. Introduction:

This report presents the findings of a network security assignment focusing on packet sniffing using Wireshark. Packet sniffing is a technique used to capture and analyze network traffic for various purposes, including network troubleshooting, security analysis, and monitoring. Wireshark is a popular and powerful network protocol analyzer that allows for detailed inspection of network packets.

# 2. Methodology:

The assignment involved capturing and analyzing network traffic using Wireshark. The following steps were followed to conduct the packet sniffing:

1. Installation of Wireshark: Wireshark was installed on a Windows machine, which serves as the platform for capturing and analyzing network packets.

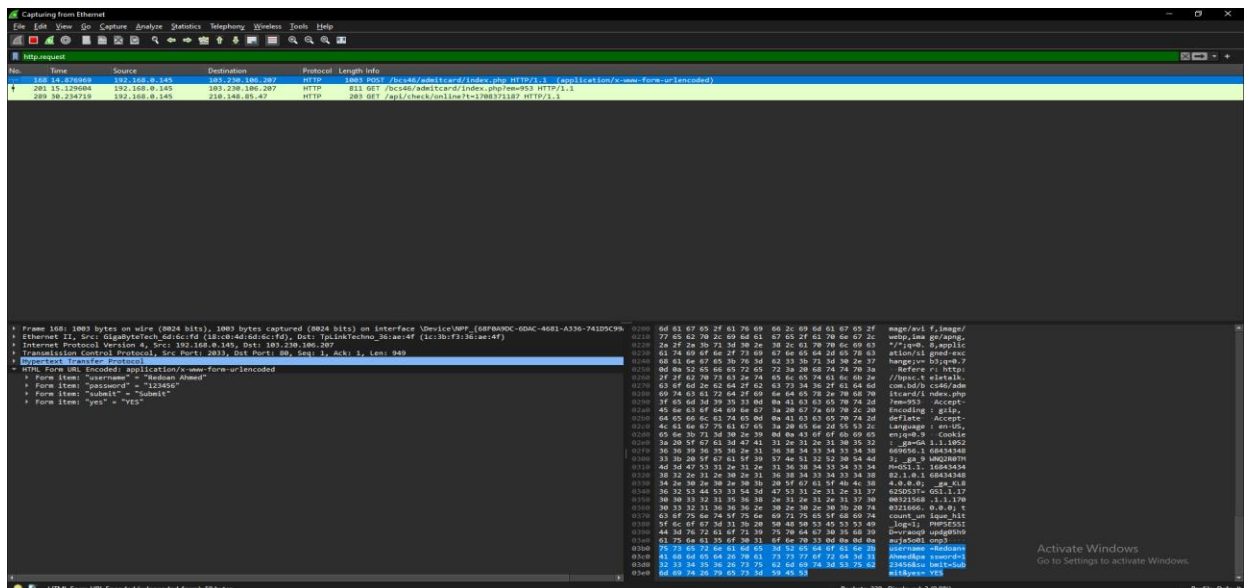
2. Packet Capture: Wireshark was launched, and packet capture was initiated on the network interface connected to the target network segment.

3. Filtering: Filters were applied to capture specific types of traffic, such as HTTP, HTTPS, DNS, or TCP/UDP traffic.

4. Analysis: Captured packets were analyzed to identify potential security issues, anomalies, or suspicious activities.

5. Documentation: Detailed notes were taken during the analysis process, documenting any noteworthy findings, including source and destination IP addresses, protocols used, and any potential security implications.

# 3. Practical:



## **4. Findings:**

The packet sniffing analysis revealed several noteworthy findings:

**HTTP Traffic:** A significant amount of HTTP traffic was observed, including web browsing activities and communication with various web servers.

**HTTPS Traffic:** Encrypted HTTPS traffic was also captured, indicating secure communication between clients and servers.

**DNS Queries:** DNS queries were captured, revealing the domain names being accessed by the network users.

**TCP/UDP Traffic:** Various TCP and UDP traffic were observed, including communication with different services and protocols.

## **5. Recommendations:**

Based on the findings, the following recommendations are proposed to enhance network security:

**Encryption:** Encourage the use of encryption protocols such as HTTPS to secure sensitive data transmitted over the network.

**Traffic Monitoring:** Implement continuous network traffic monitoring to detect and respond to potential security threats in real-time.

**User Awareness:** Provide security awareness training to users to educate them about the risks associated with unencrypted network traffic and potential security threats.

**Network Segmentation:** Implement network segmentation to isolate critical systems and sensitive data from potential attackers.

## **6. Conclusion:**

In conclusion, the packet sniffing analysis using Wireshark has provided valuable insights into the network traffic patterns and potential security risks. By capturing and analyzing network packets, security professionals can better understand the network environment and take appropriate measures to enhance security.