Project Report

Title: HTTP is not secure because it sends data in plain text, making it easy to intercept. HTTPS encrypts data for safety. Using Wireshark, we can capture HTTP traffic and see how sensitive information, like passwords, can be stolen.

**Course:** CEH Class

**Student Name:** Laxman

**Objective**

HTTP transmits data in plain text, making it vulnerable to attacks like network sniffing. In contrast, HTTPS encrypts data for security. Using Wireshark, a powerful packet analysis tool, we can capture and analyses HTTP traffic to demonstrate how credentials and sensitive information can be exposed, highlighting the importance of secure connections.

**Configuration Details**

**Machine (Kali Linux):**

**• Operating System:** Kali Linux

**• RAM:** 4 GB

**• Processors:** 4

**• Storage:** 30 GB

**• Network Adapter:** NAT

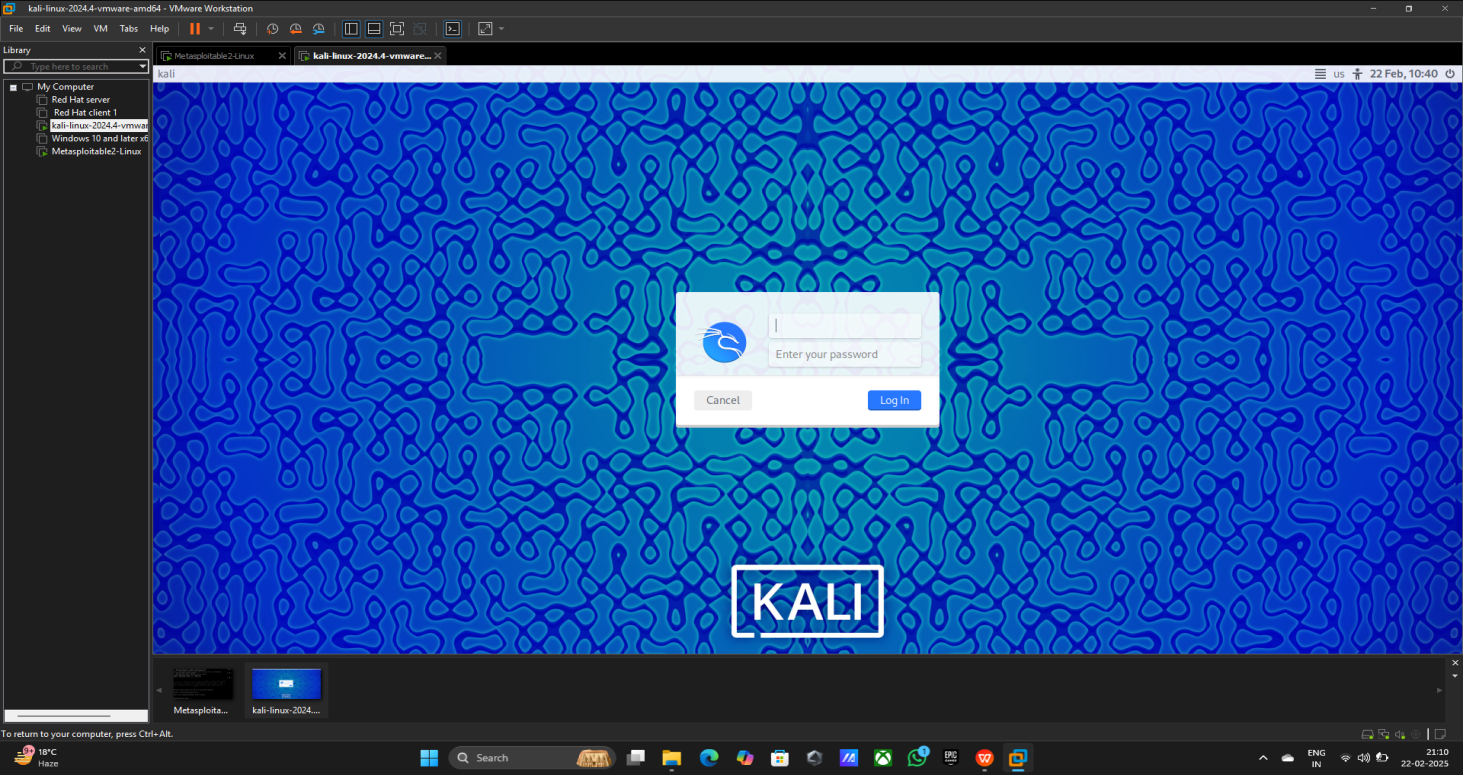
**• IP Address:** 192.168.44.129

**• Username:** Kali

**Steps Performed**

**Step 1: Setup the Virtual Machines**

**• Evidence**

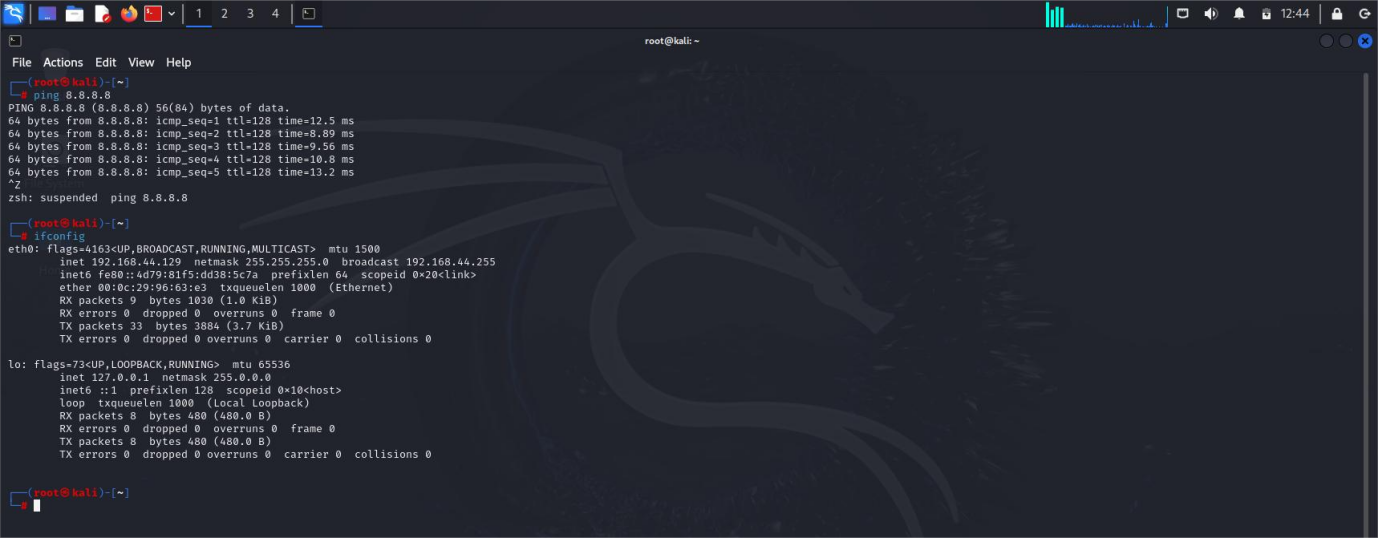
****

**Step 2: Pinging with the google**

**Command Using:** 1) ping 8.8.8.8

1. Press Ctrl+Z
2. ifconfig

**• Evidence**

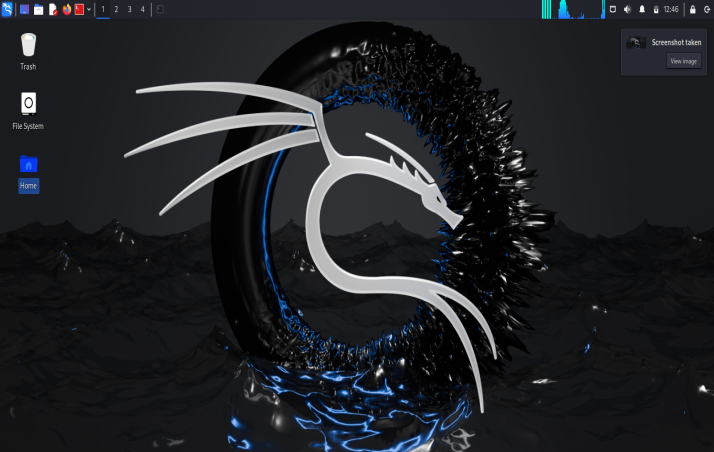


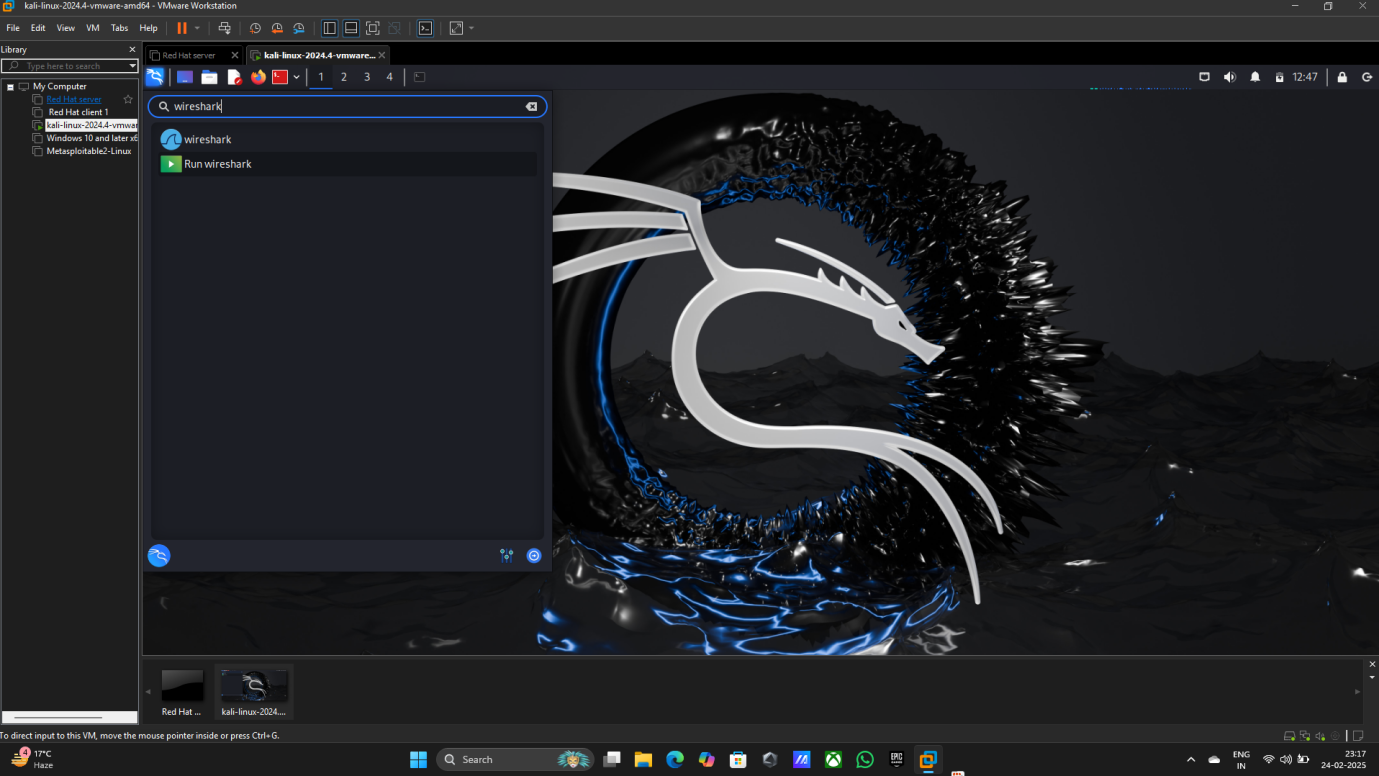
**Step 3: Open the kali home**

**Command Using:** Search Wireshark in search bar

**• Evidence**

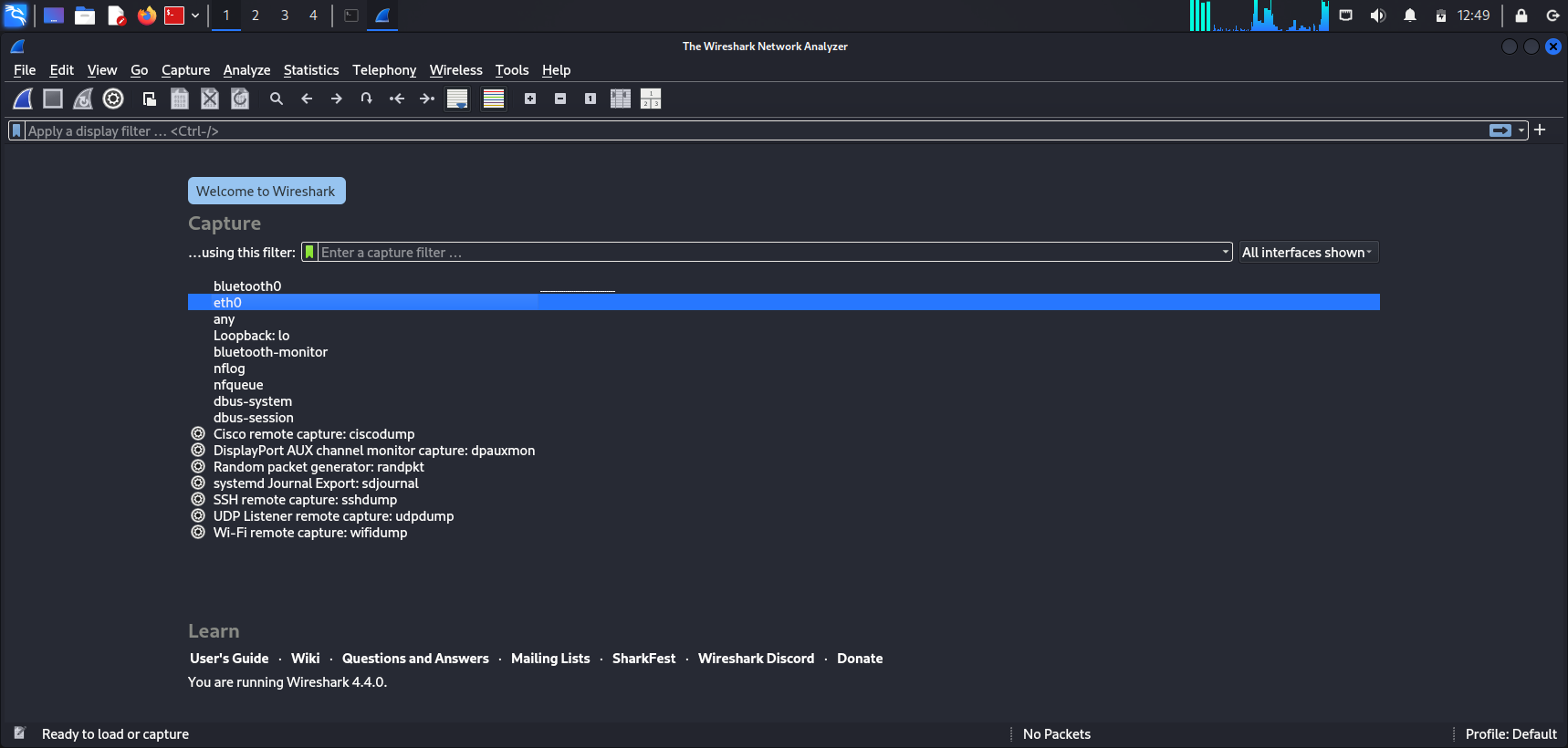
**> Click on appliction icon**

****

****

**> You see defaut page of wireshark**

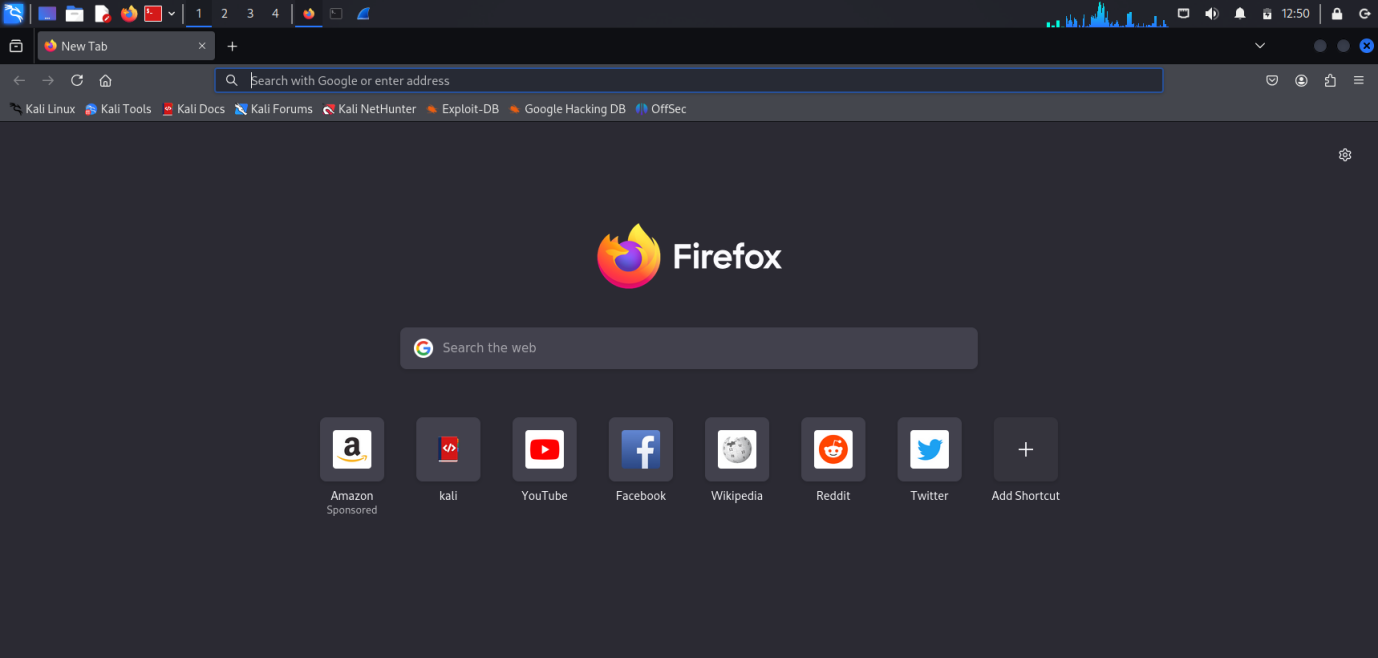
**• Evidence**

****

**Step 4: Open the Firefox**

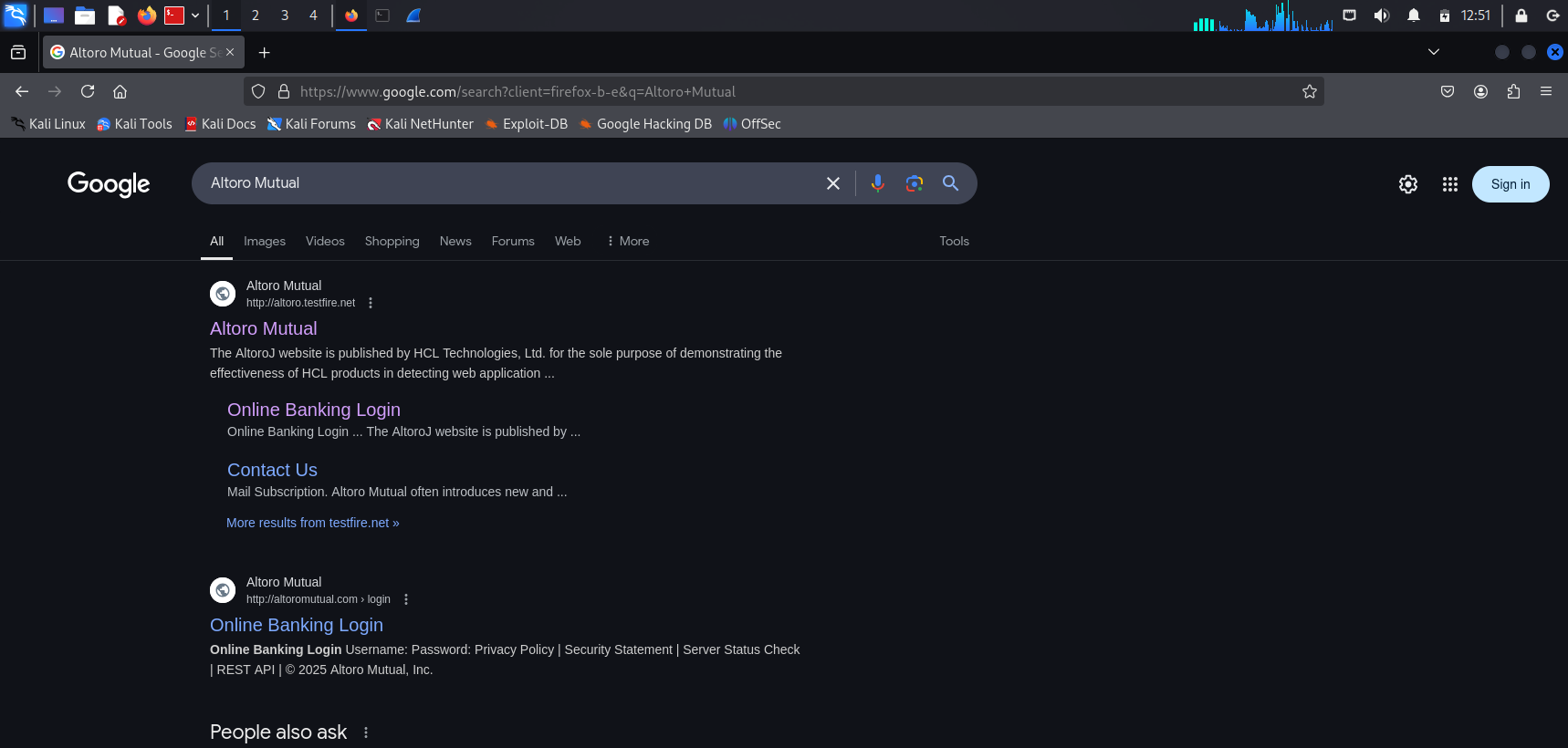
**Command Using:** Search AltoroMutusl

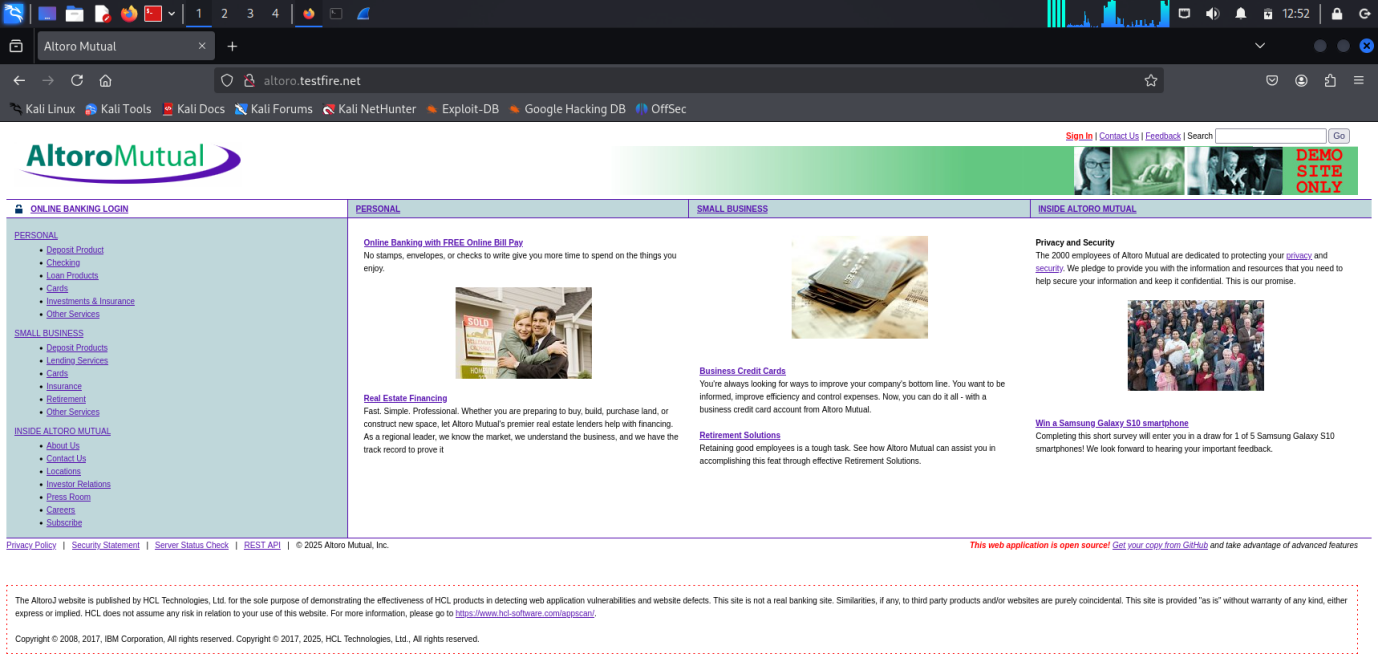
**• Evidence**

****

**> Pree on the first Link.**

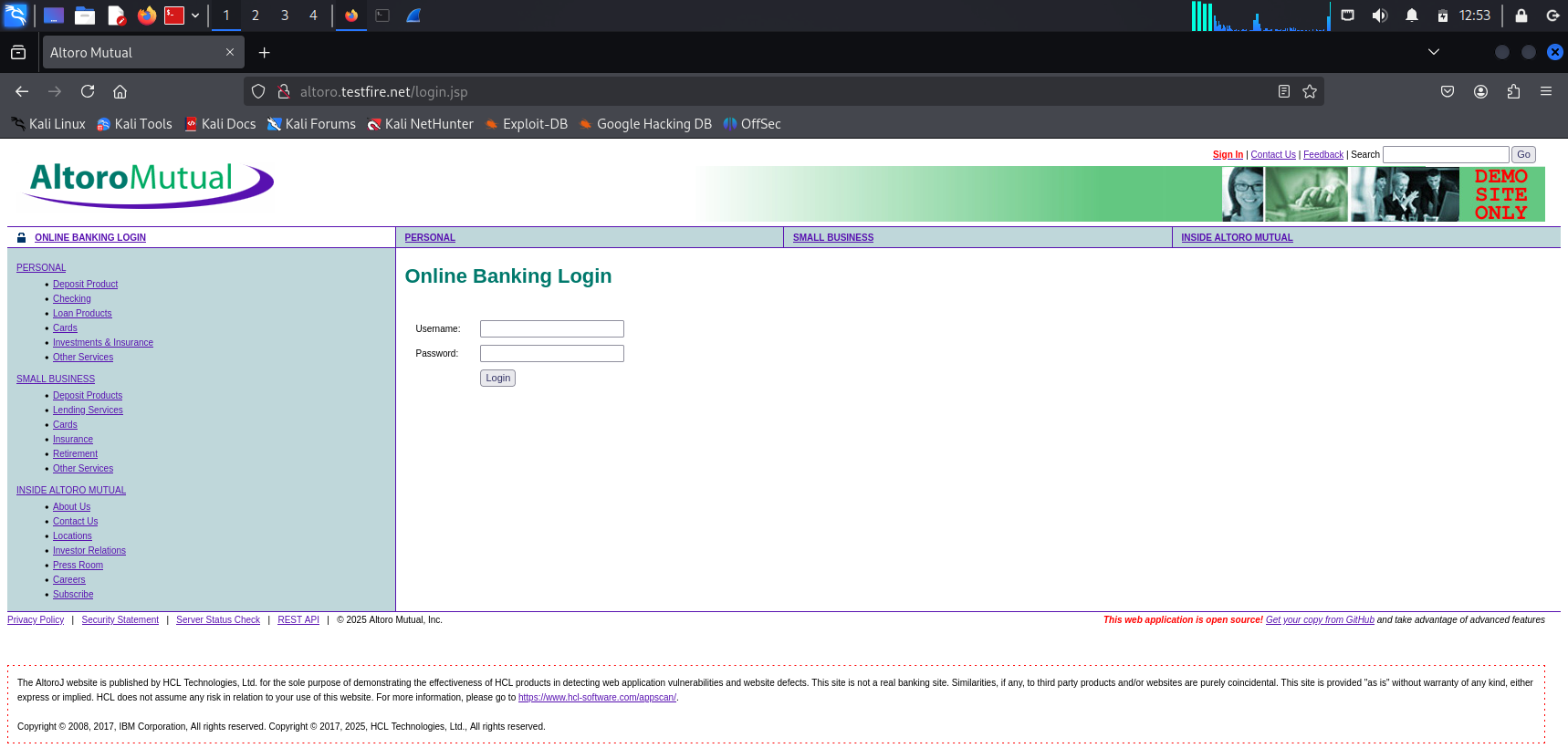
**• Evidence**

****



**>** Click on the Sign in button.

**• Evidence**



**Step 5: Open the Wireshark and AltoroMutual**

**Command Using: Type UserName:** Laxman

**Type password:** 123456

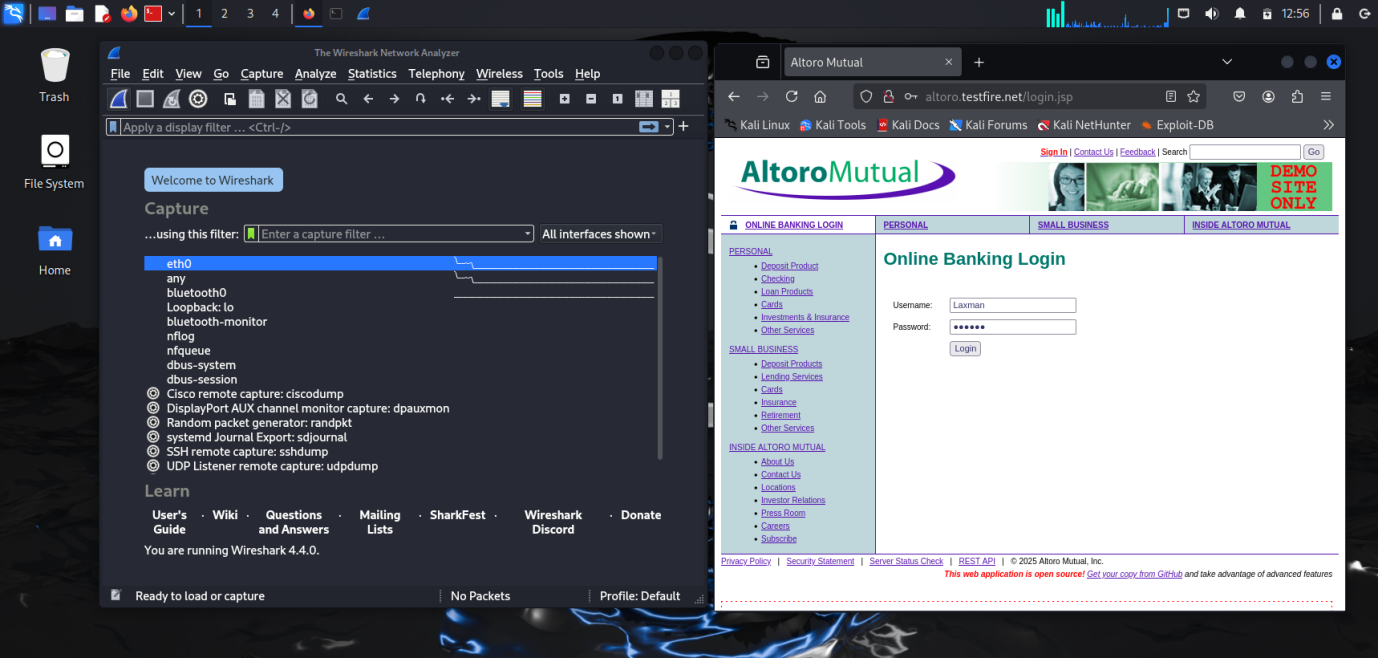
**Some important steps:-**

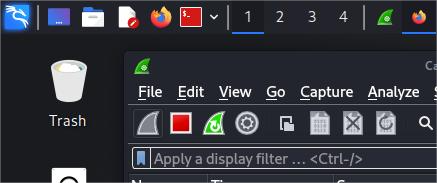
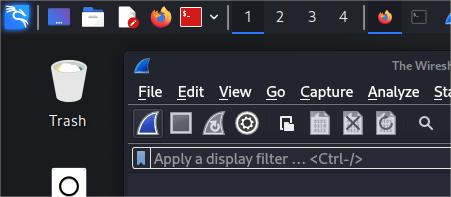
**>** Press on the start capturing packets.

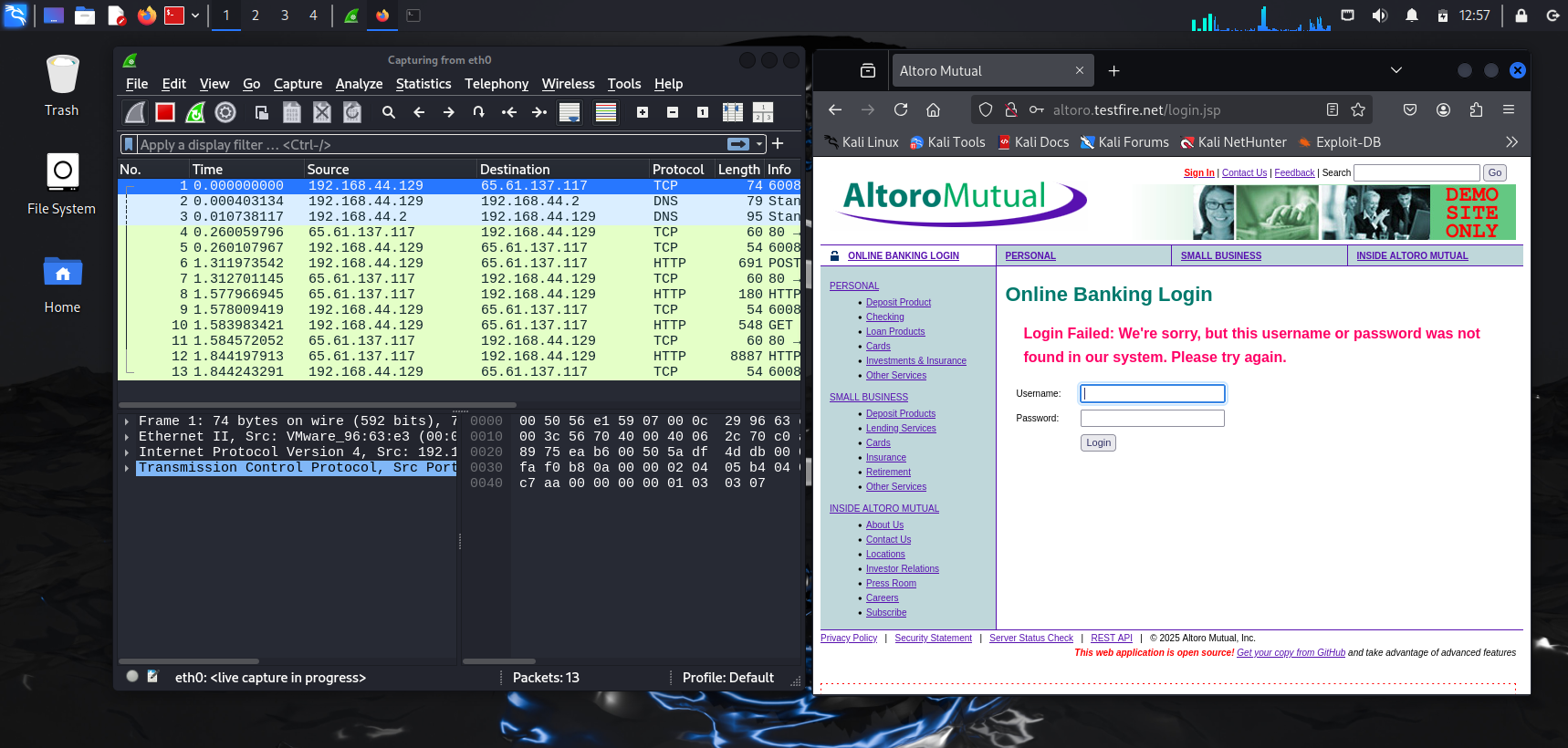
**>** Press on the Login button.

**>** Press on the stop capturing packets.

**• Evidence**





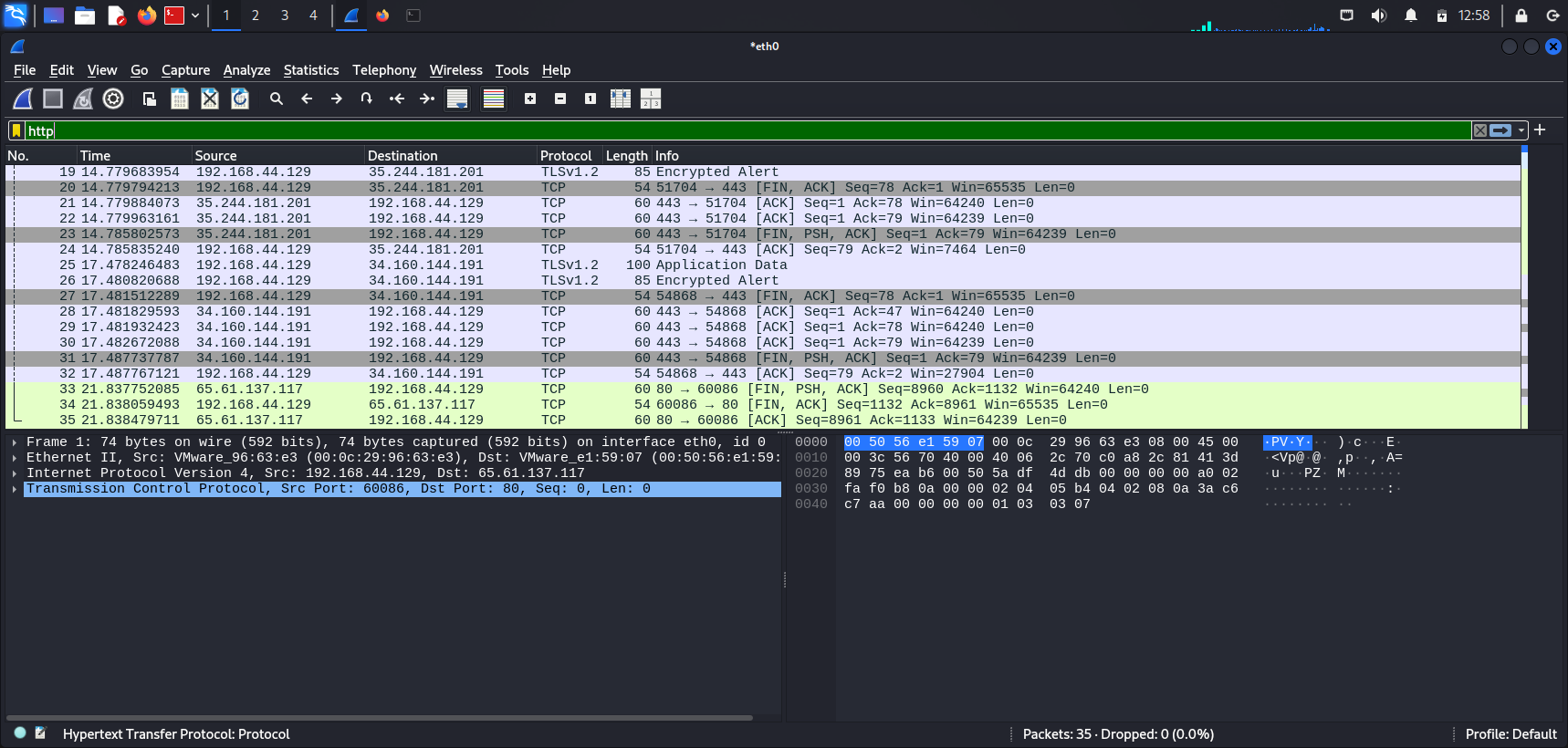


**>** After Press of Login interface you see some details on the wireshark.

**>** On the search bar type http and search.

**>** Some http port details showing you.

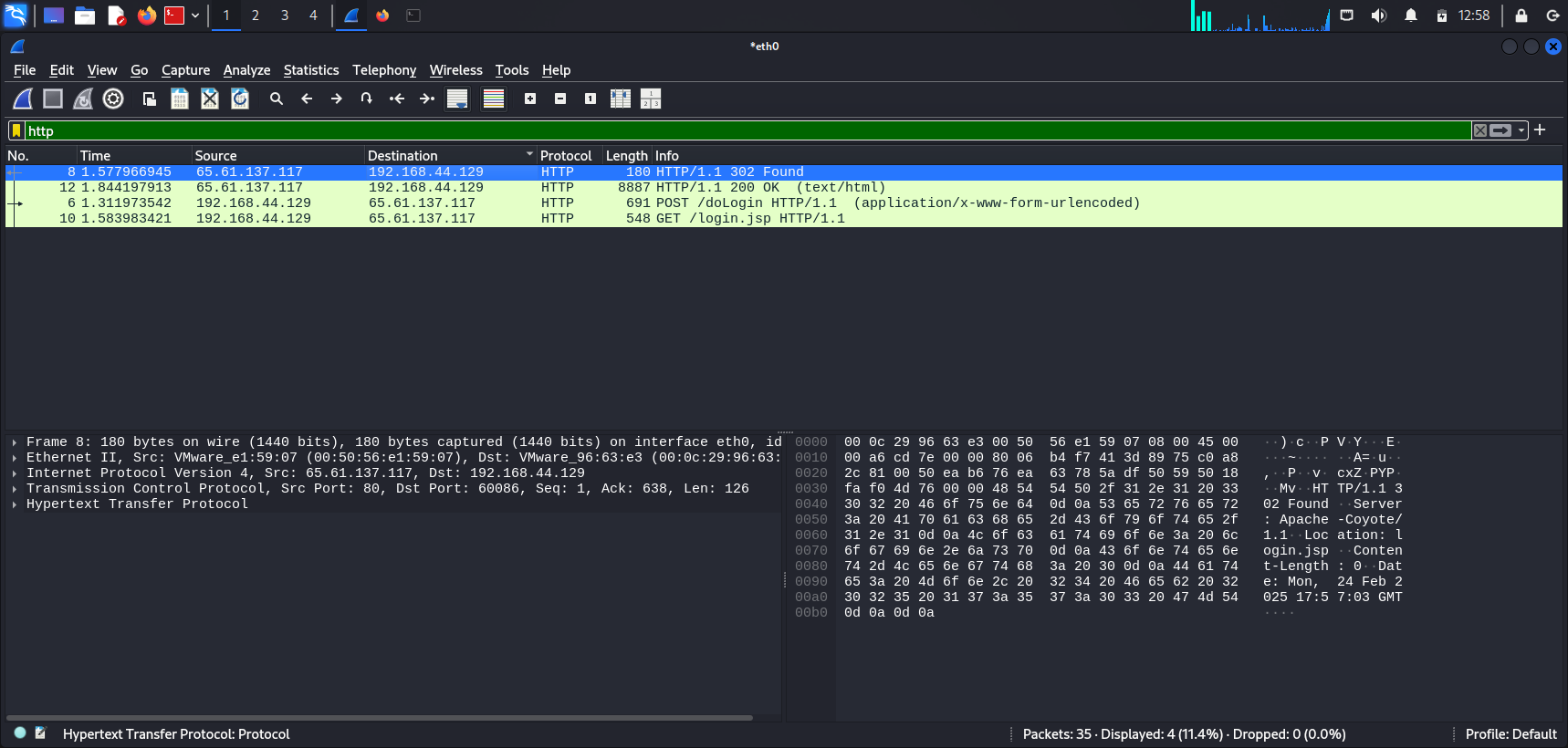
**• Evidence**



**>** Find the http port there is your info stolen.

**>** Press on the 180 HTTP/1.1 302 Found.

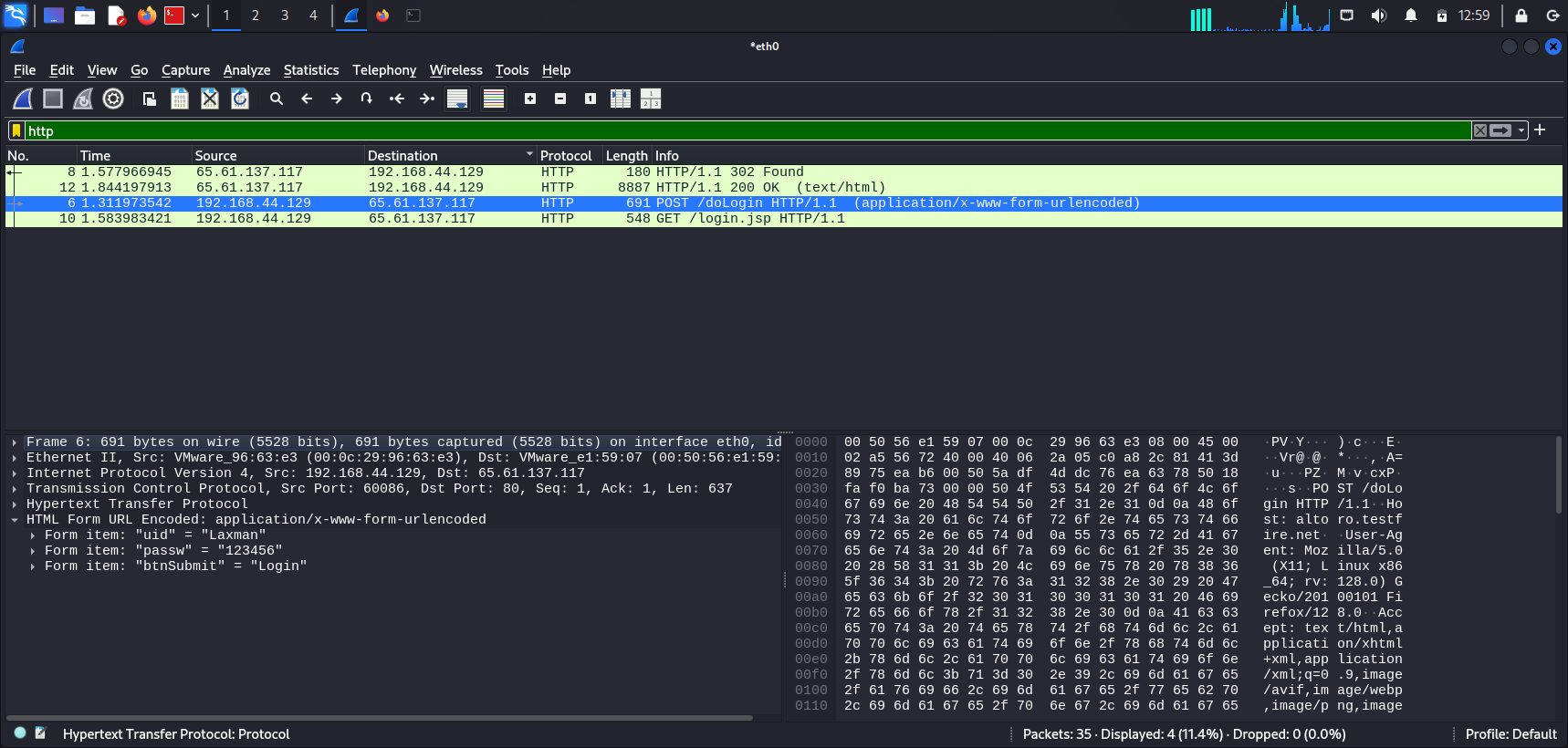
**• Evidence**



**>** Pree on the Hypertext Transfer Protocoal.

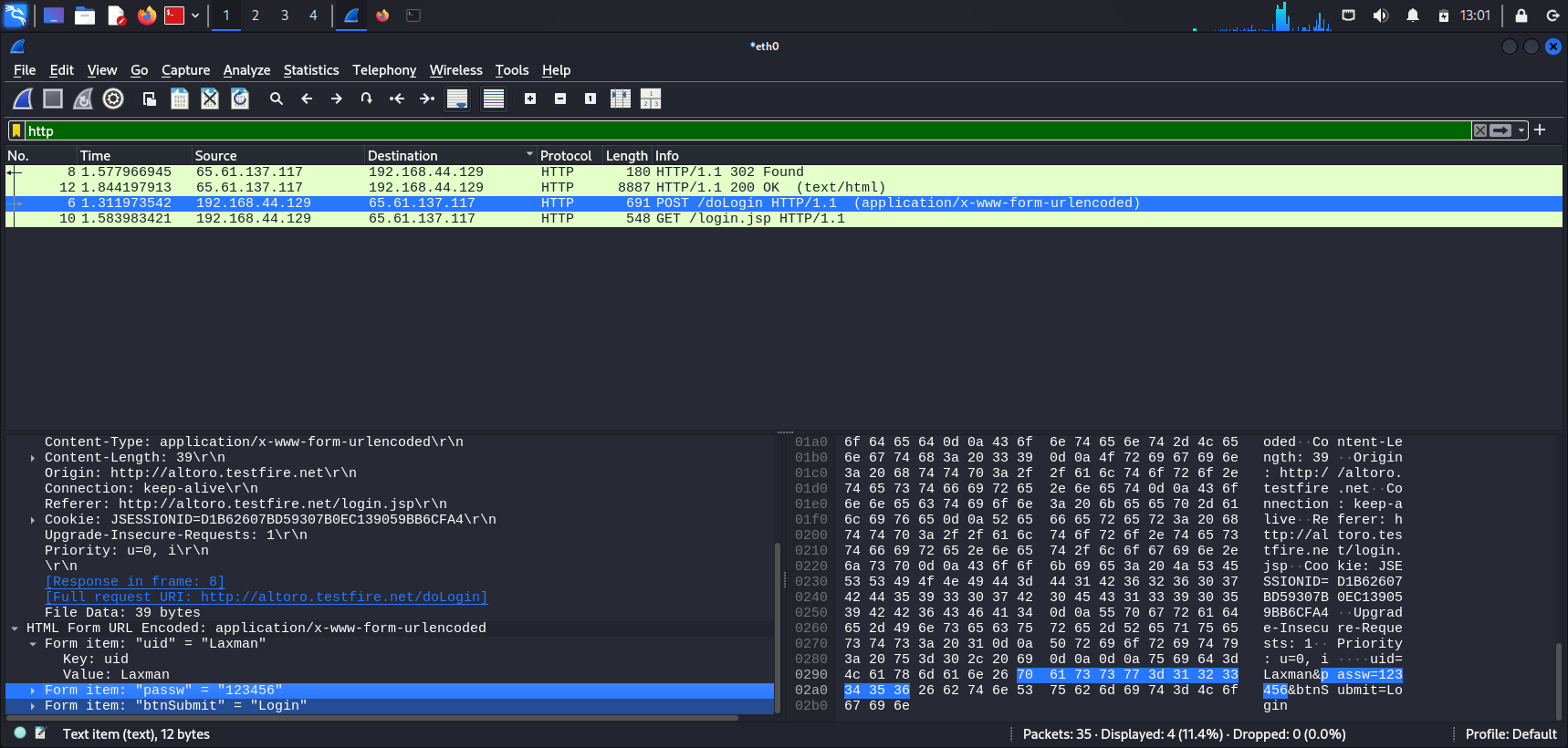
**>** You see your username and password stolen.

**• Evidence**



**>** Left and Right side your username and password showing.

**• Evidence**



**Wireshark Captures the Data:**

1. **Promiscuous/Monitor Mode –** Wireshark puts the Network Interface Card (NIC) into promiscuous mode (on wired networks) or monitor mode (on wireless networks), allowing it to capture all packets on the network.
2. **Real-Time Packet Capture –** Wireshark captures the login request as it travels to the server.

**3. Packet Analysis –** The intercepted packet is broken down into readable layers based on the TCP/IP or OSI model, allowing us to extract sensitive data like usernames and passwords.

**>** This works only if the login page uses HTTP, as HTTPS encrypts the data. However, HTTPS can sometimes be downgraded or bypassed in specific scenarios.

**Conclusion**

This assignment demonstrated the insecurity of HTTP websites and how login credentials can be intercepted using Wireshark. Since HTTP transmits data in plain text, any login request sent over an unsecured connection can be easily captured.

By enabling promiscuous mode (wired) or monitor mode (wireless), Wireshark captures network packets in real-time and breaks them down into Ethernet, IP, TCP, and HTTP layers for analysis. Filtering for HTTP traffic allows us to locate POST requests, where login details appear in plaintext.

This experiment highlights the importance of using HTTPS, which encrypts transmitted data and prevents credential leaks. Understanding this vulnerability reinforces why modern websites prioritize HTTPS for secure communication.