UMGC Lab

Name: Pelumi Johnson
Date: January 13, 2026
Course: CMIT 436 | Cloud Security
Institution: University of Maryland Global Campus (UMGC)
Lab Title: Capturing Network Traffic Using Wireshark

Objective

The objective of this lab was to demonstrate how to use Wireshark, a network protocol analyzer, to capture live network traffic and save the captured packets for further analysis. This lab introduced foundational packet capture concepts and provided exposure to observing real-time network communications within a virtual environment.

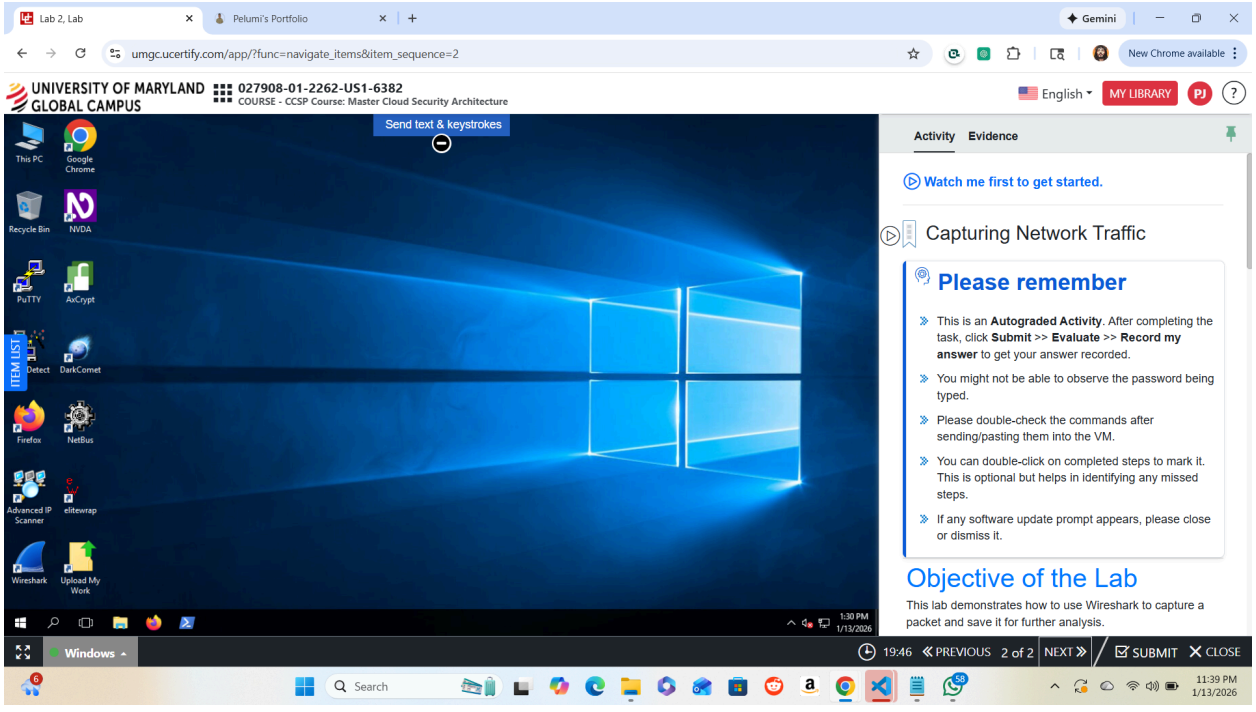
Lab Environment

- Operating System: Windows (Virtual Lab Environment)
- Network Analysis Tool: Wireshark
- Network Interface Used: Ethernet0
- Traffic Generation Tool: Google Chrome

Procedure

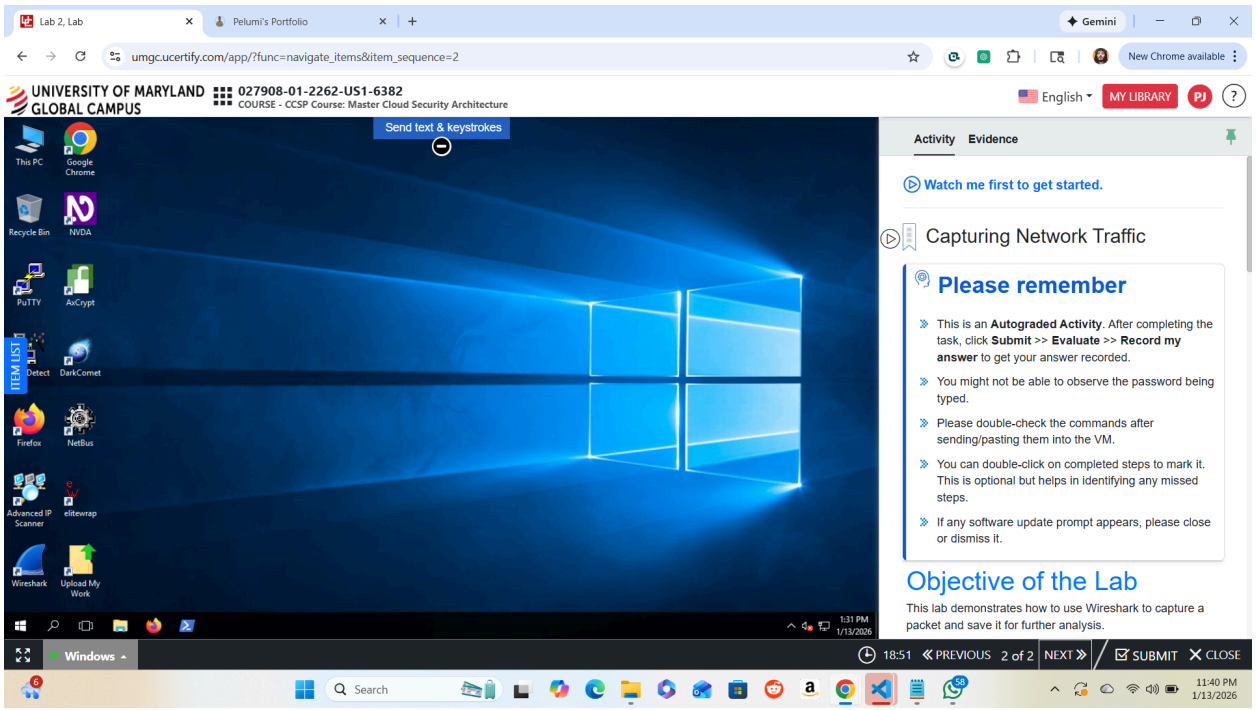
Step 1: Powering On the Virtual Machine

The virtual machine was powered on using the Windows tab and selecting the On/Connect option within the uCertify lab environment.



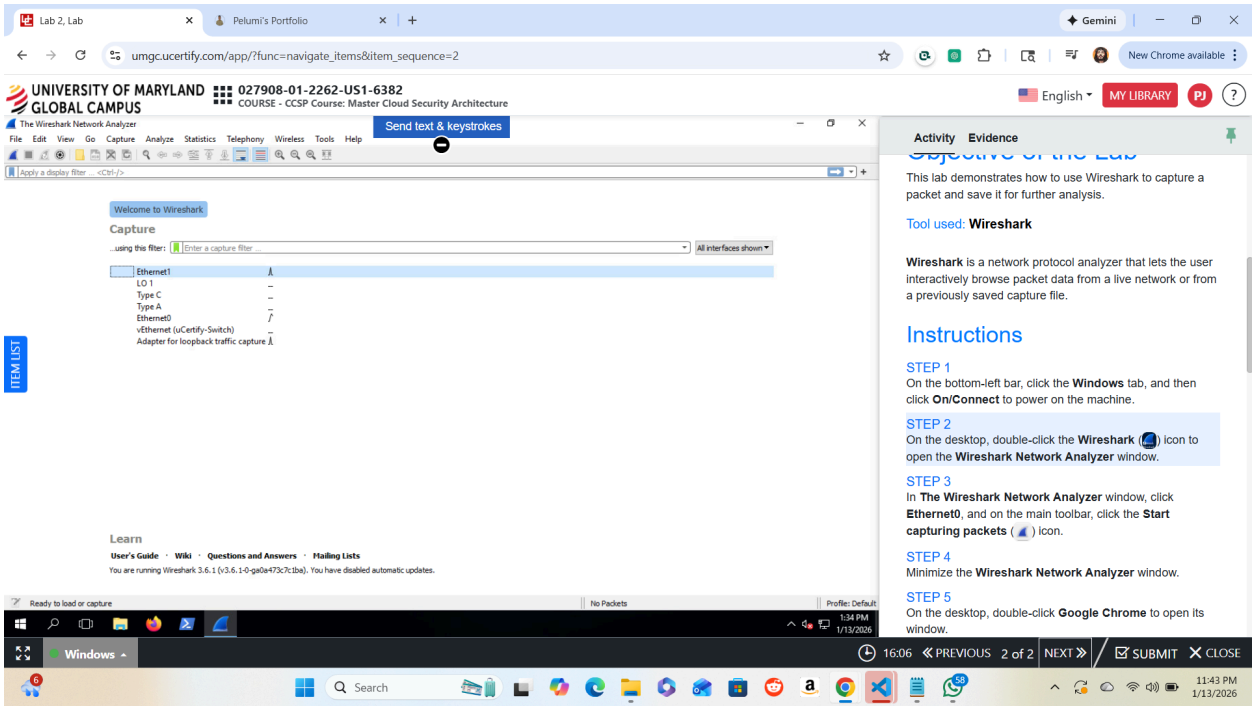
Step 2: Launching Wireshark

After the system finished loading, the Wireshark application was launched by double-clicking the Wireshark icon on the desktop. This opened the Wireshark Network Analyzer window.



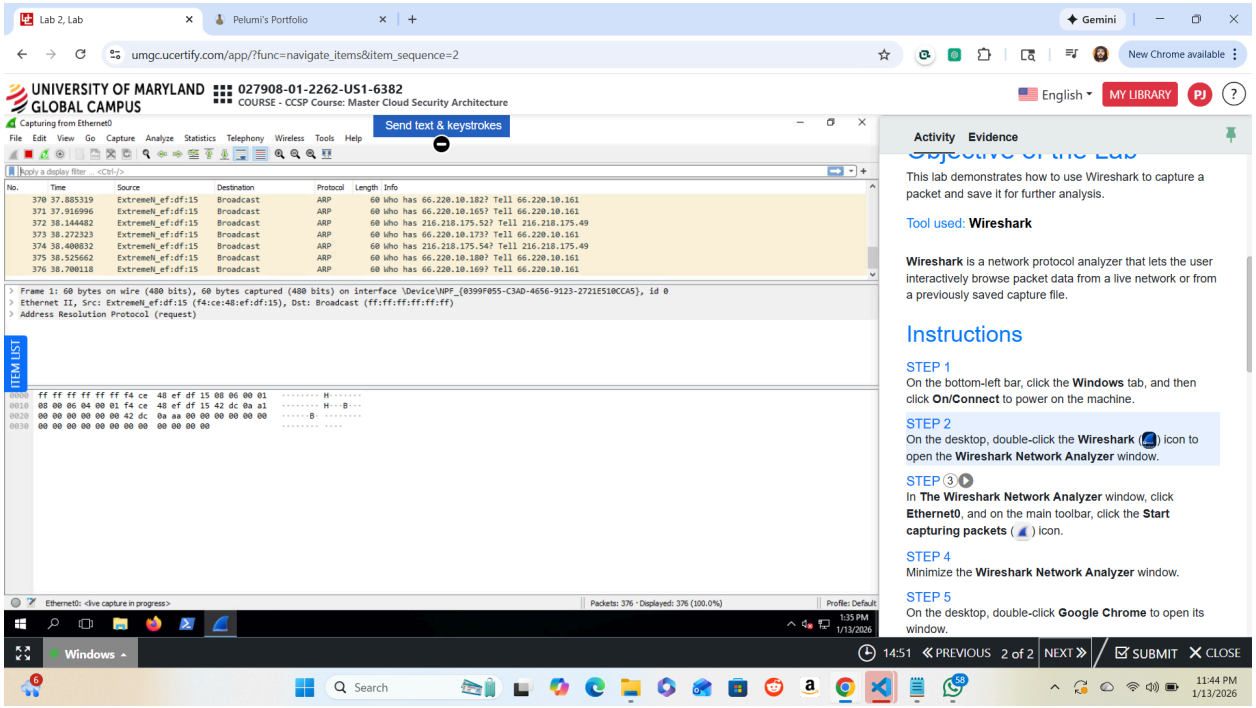
Step 3: Selecting the Network Interface

Within the Wireshark interface, the Ethernet0 network interface was selected. This interface represents the active network connection used by the virtual machine.



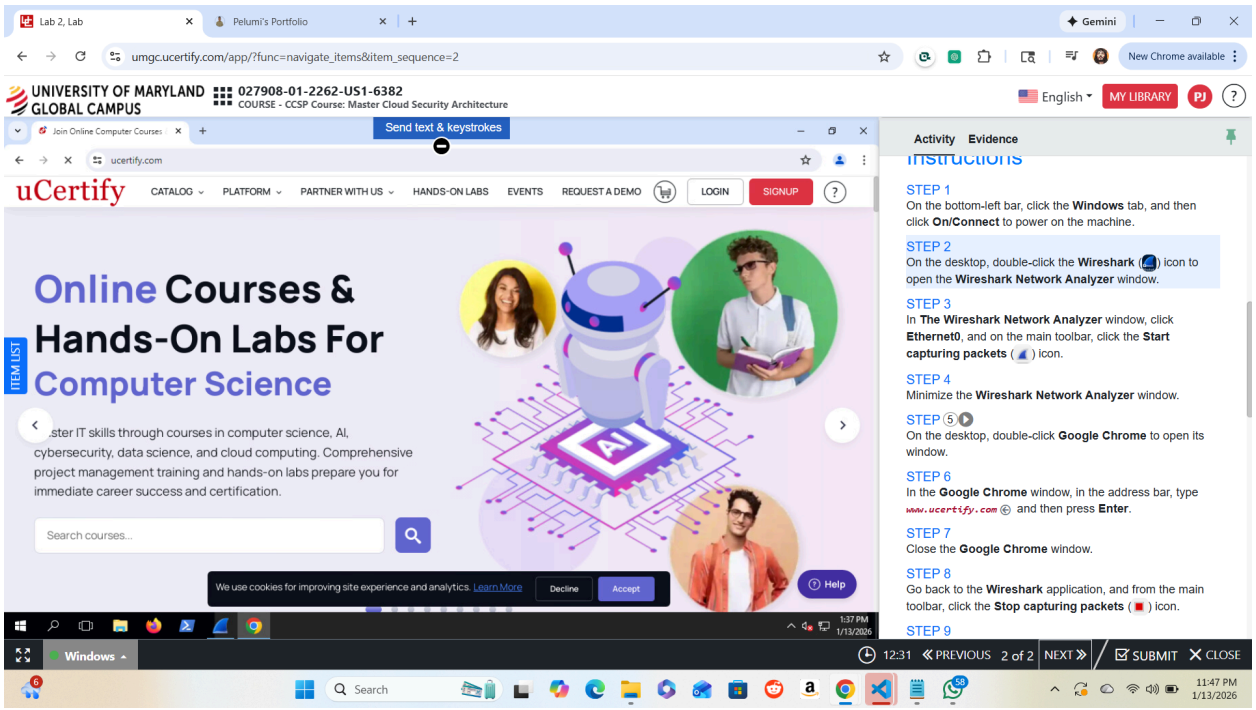
Step 4: Starting Packet Capture

Packet capture was initiated by clicking the Start Capturing Packets button on the Wireshark toolbar. Wireshark immediately began collecting live network traffic.



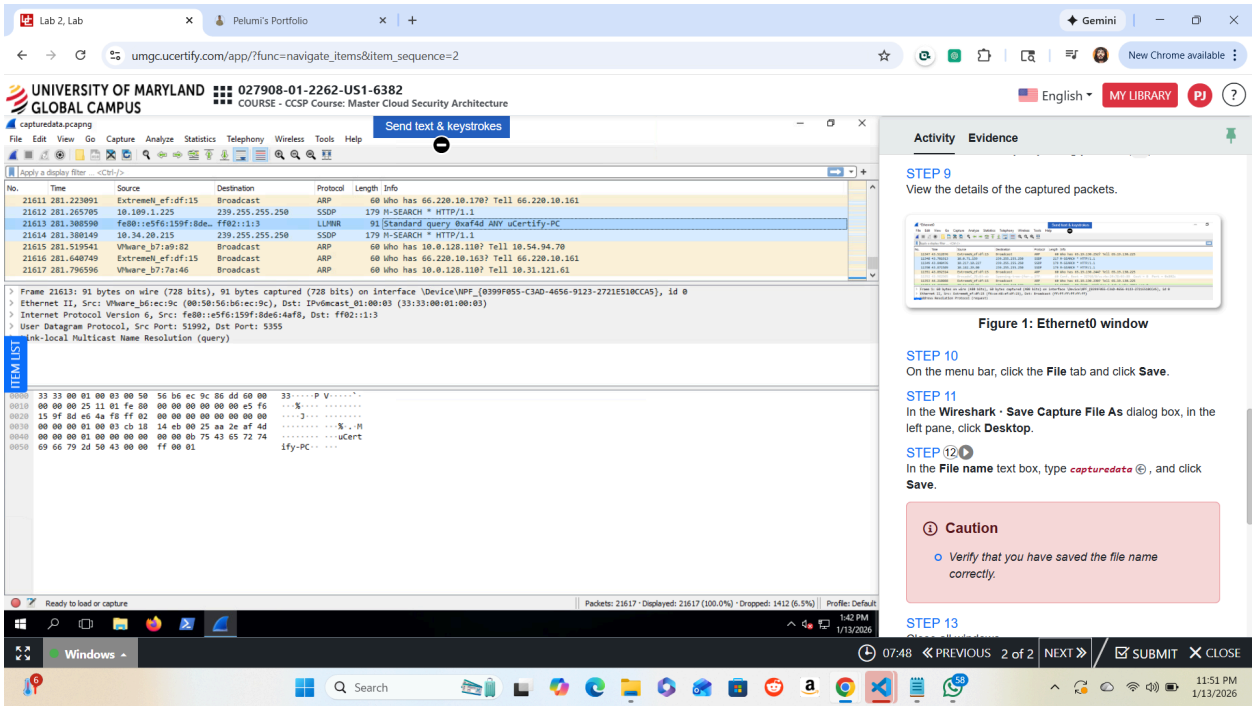
Step 5: Generating Network Traffic

To generate network activity, Google Chrome was opened and the website www.ucertify.com was accessed. This action produced various types of network traffic, including DNS requests and web communication packets.



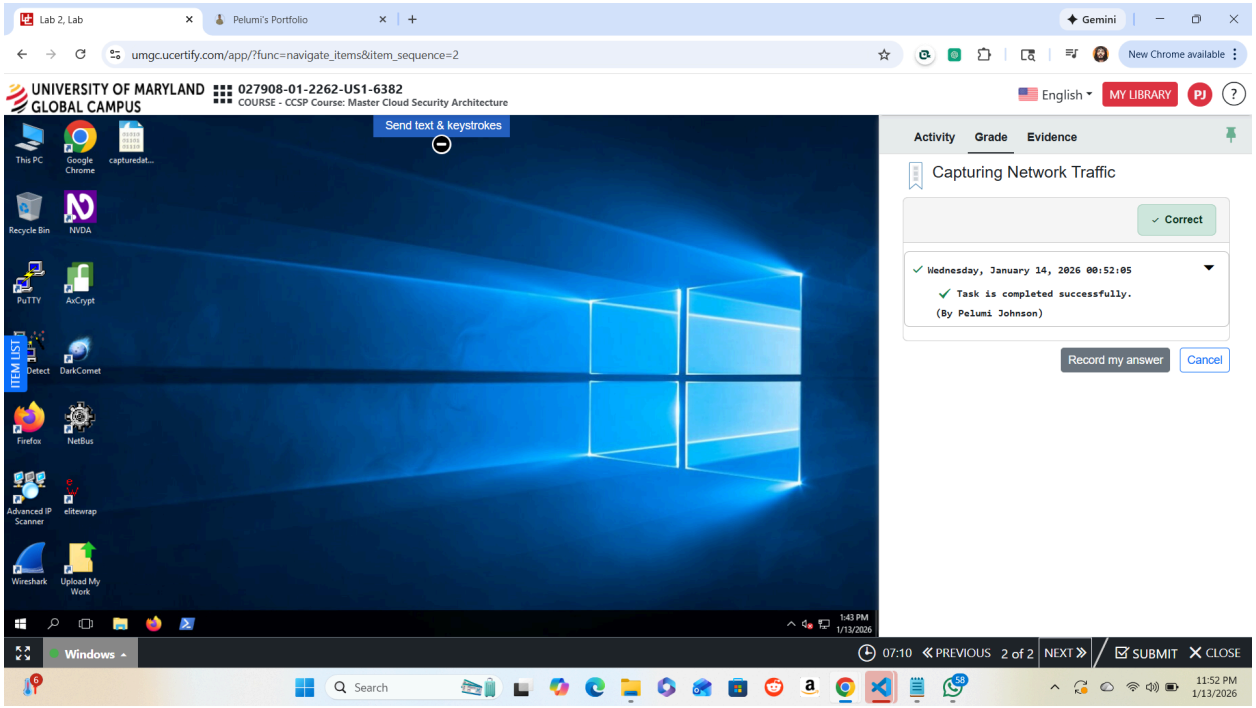
Step 6: Stopping the Packet Capture

After sufficient traffic was captured, the Wireshark window was returned to focus, and the Stop Capturing Packets button was selected to end the capture session.



Step 7: Viewing Captured Packets

The captured packets were reviewed within the Wireshark interface. Multiple protocol types were observed, including ARP, SSDP, LLMNR, and IPv6 traffic, demonstrating typical background and broadcast network activity.



Results

The lab successfully demonstrated live packet capture using Wireshark. Network traffic was captured, reviewed, and saved correctly. Multiple protocols were visible in the capture, confirming that normal system and browser activity generates continuous network communication. The task was completed successfully and marked as correct within the uCertify platform.

Conclusion

This lab provided practical experience with Wireshark and reinforced core networking and cybersecurity concepts related to traffic capture and analysis. Packet capture is a foundational skill for cybersecurity professionals, supporting activities such as troubleshooting, monitoring, and incident investigation. The lab illustrated how everyday user actions translate into observable network traffic.