# Project Report

Project Title: Network Traffic Analysis Using Wireshark and Zeek

Name: Aman Deep

Institution: United College of Engineering and Research, Prayagraj

Course: PBEL Internship in Cybersecurity by IBM

Mentor: Ayush Kumar

Date: July 30, 2025

## Abstract

This project focuses on analyzing network traffic using two powerful tools: Wireshark and Zeek. The primary aim is to detect suspicious behavior, anomalies in protocol behavior, and signs of potential intrusions in a controlled lab environment. Wireshark allows deep packet inspection, while Zeek provides higher-level traffic analysis and scripting capabilities. The goal was to capture, filter, and interpret meaningful traffic patterns and generate a report outlining any detected threats. This project enhances skills in network forensics and introduces students to real-world cybersecurity tools. Key findings include the identification of abnormal traffic patterns that could be linked to port scanning, brute-force login attempts, and unauthorized file transfers.

## Table of Contents

1. Title Page  
2. Abstract  
3. Table of Contents  
4. List of Figures and Tables  
5. Introduction  
6. Literature Review  
7. Methodology / Approach  
8. Results and Discussion  
9. Conclusion  
10. Recommendations  
11. References  
12. Appendices

## List of Figures and Tables

Figure 1: UDP Packet View in Wireshark  
Figure 2: IPv4 Header Analysis in Wireshark  
Figure 3: HTTP GET Request Inspection  
Figure 4: IPv6 HTTP Traffic Analysis

## Introduction

Network traffic analysis is a fundamental component in cybersecurity operations, allowing analysts to monitor, inspect, and investigate network activities. The project aims to explore the use of Wireshark and Zeek for analyzing network traffic. These tools help identify malicious behavior, detect vulnerabilities, and understand typical vs. anomalous patterns. The motivation behind this project is to build foundational knowledge of traffic analysis using open-source tools widely used in the industry.

## Literature Review

Wireshark, formerly known as Ethereal, is an open-source packet analyzer used for network troubleshooting and analysis. Zeek, formerly known as Bro, operates at a higher level, converting network packets into events and logs. Studies and cybersecurity case reports highlight these tools as critical in both academic research and professional incident response. Literature emphasizes Zeek's scalability and scripting flexibility, while Wireshark’s strength lies in visualizing raw packet data.

## Methodology / Approach

Approach:  
- Set up a virtual lab environment using Kali Linux and Ubuntu as the victim machine.  
- Simulated normal and suspicious traffic using tools like hping3, Nmap, and Netcat.  
  
Tools & Technologies:  
- Wireshark (packet-level inspection)  
- Zeek (log-based analysis)  
- VirtualBox (virtual network environment)  
  
Steps:  
1. Captured traffic using Wireshark.  
2. Saved PCAP files for analysis.  
3. Deployed Zeek to process captured traffic.  
4. Analyzed Zeek logs: conn.log, dns.log, http.log, etc.  
5. Interpreted logs and matched them against known threat patterns.

## Screenshots (Methodology)

Figure 1: UDP Packet View in Wireshark

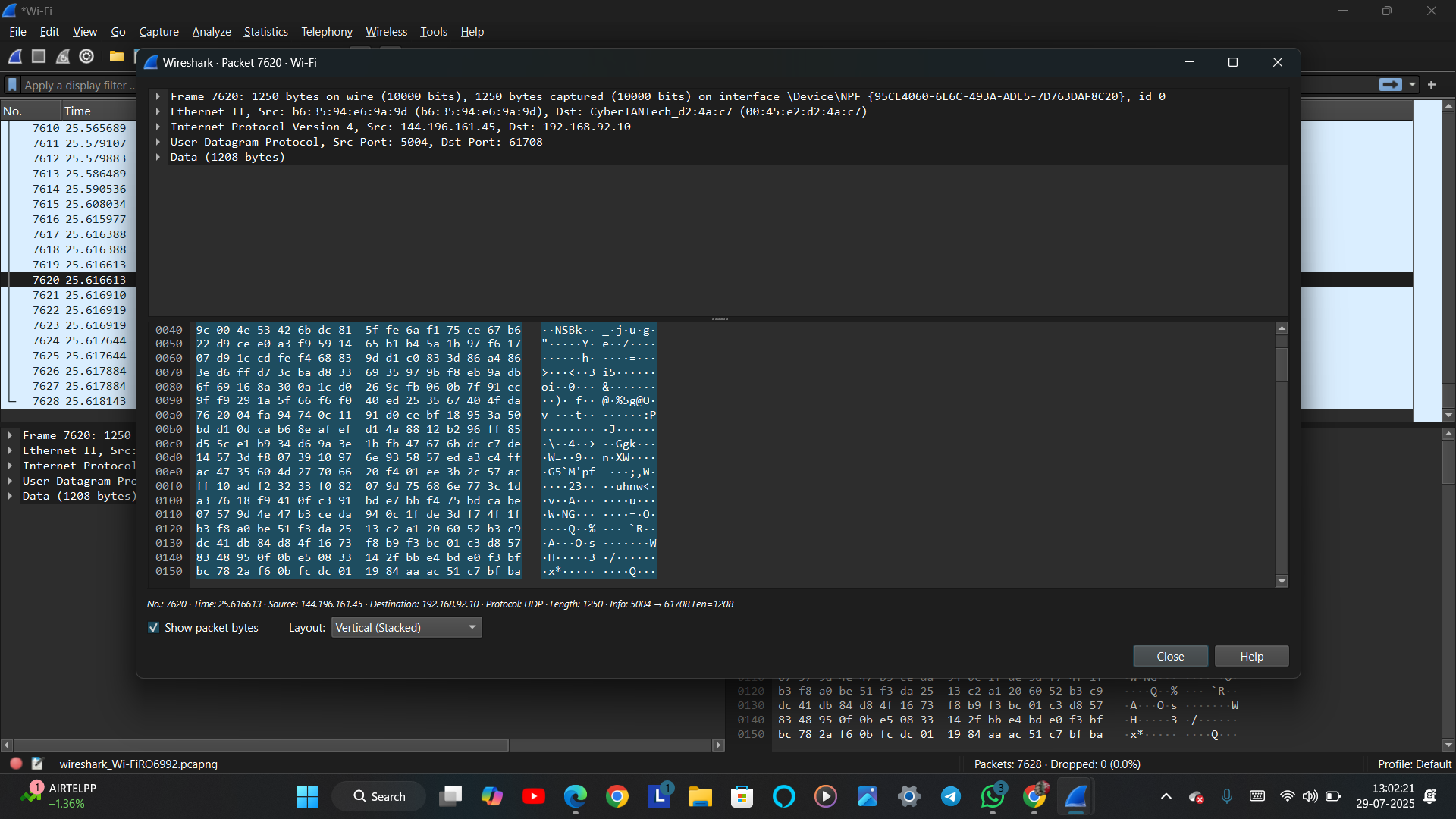
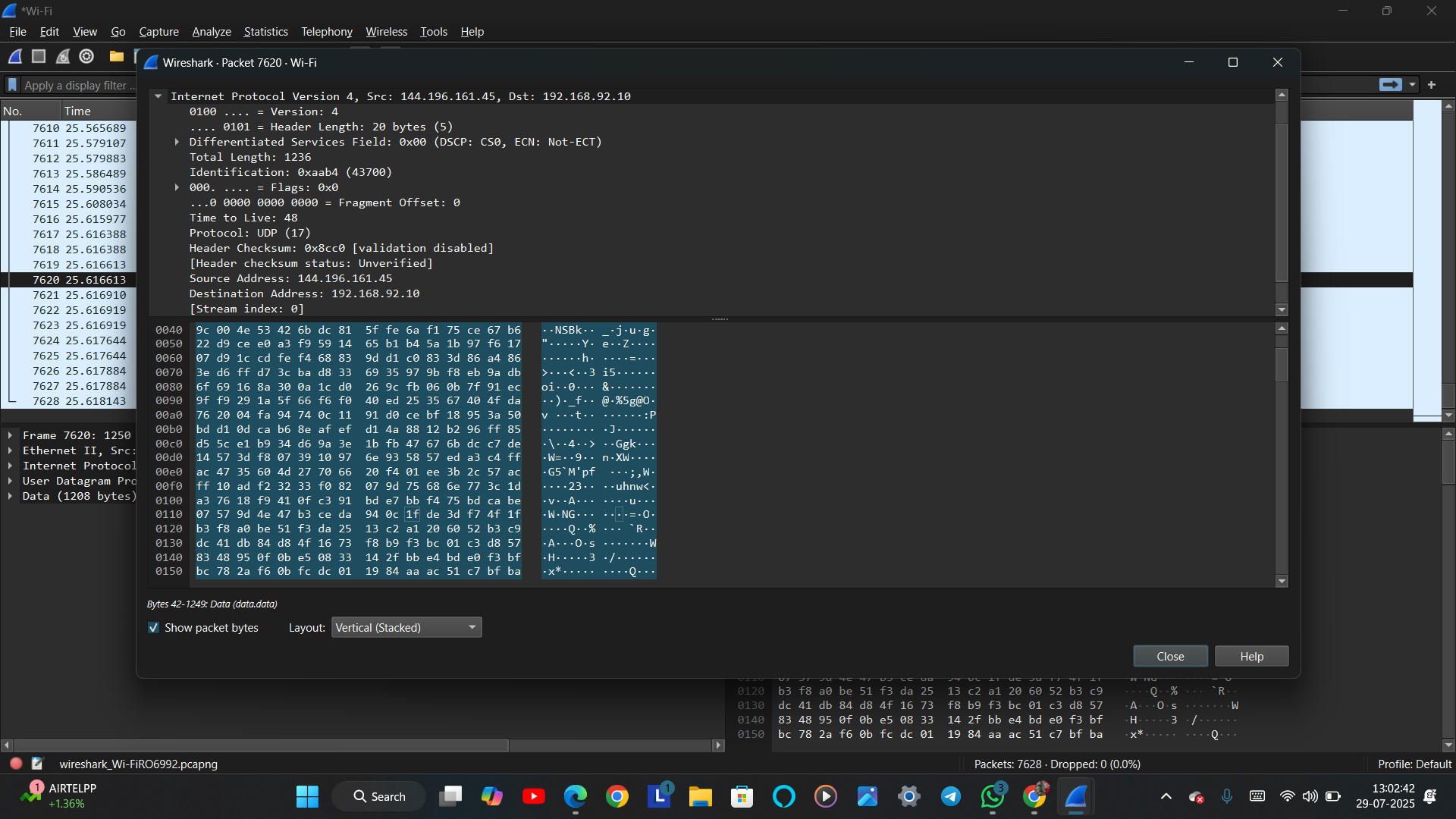


Figure 2: IPv4 Header Analysis in Wireshark



## Results and Discussion

Findings:  
- Unusual TCP SYN floods detected.  
- DNS tunneling patterns observed.  
- HTTP requests with embedded base64 payloads identified.  
  
Discussion:  
These findings suggest attempts at reconnaissance and potential command-and-control traffic. Wireshark provided low-level visibility, while Zeek’s logs helped correlate events over time.  
  
Challenges Faced:  
- Filtering out normal traffic from large PCAP files.  
- Understanding Zeek script outputs.  
- Time synchronization issues across VMs.

Figure 3: HTTP GET Request Inspection

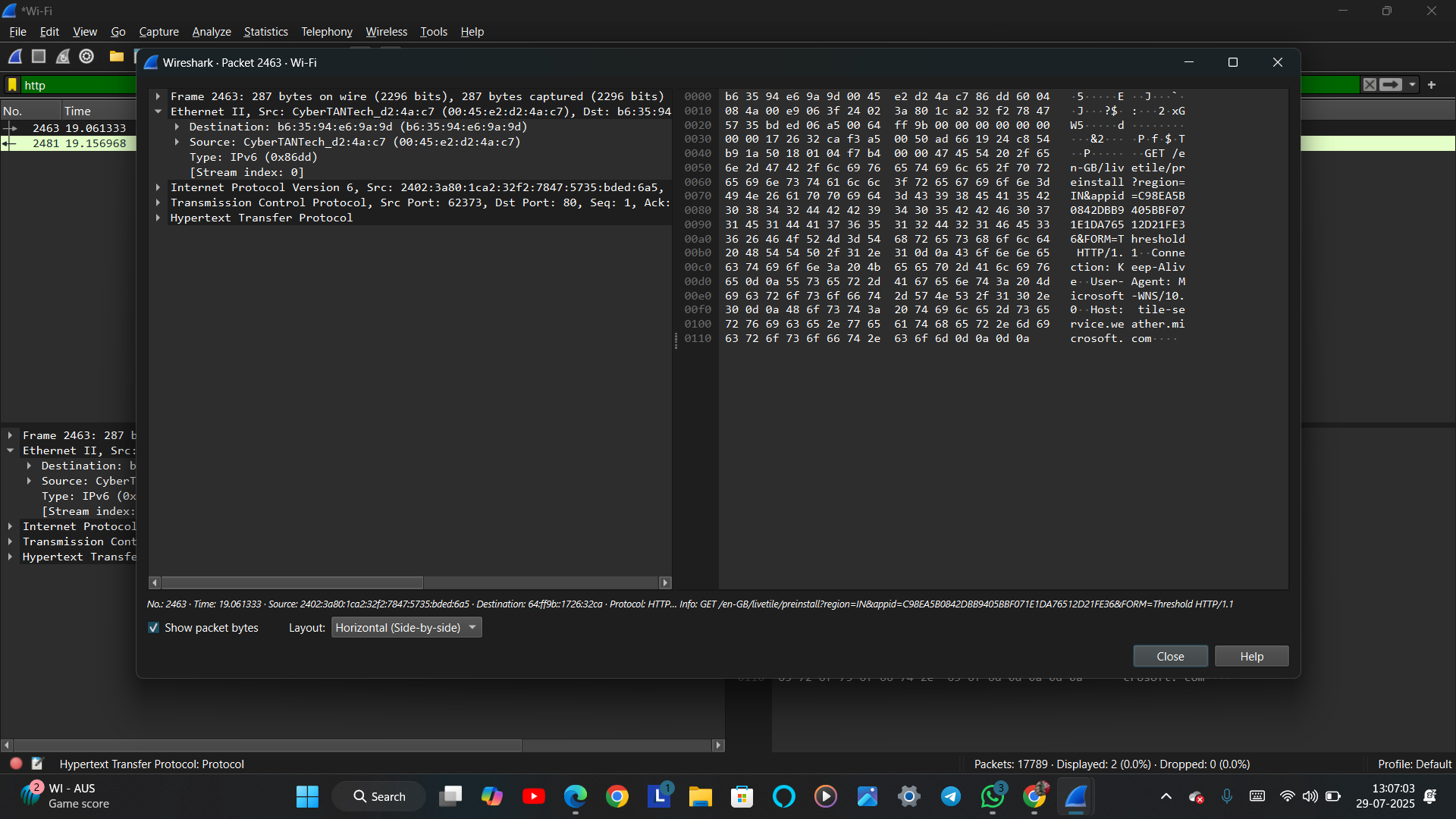
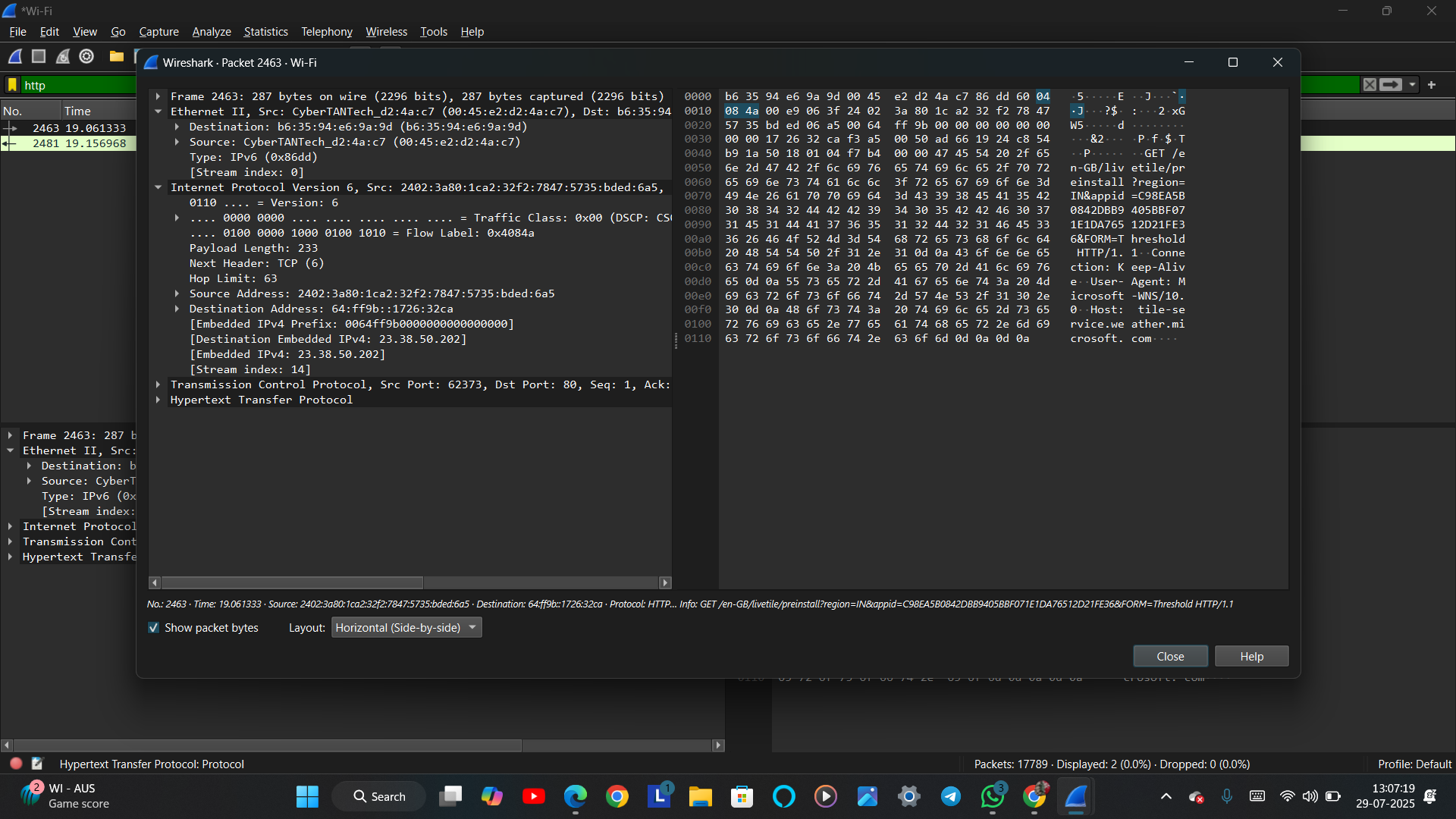


Figure 4: IPv6 HTTP Traffic Analysis



## Conclusion

The project successfully demonstrated basic network traffic analysis skills using Wireshark and Zeek. Suspicious traffic patterns such as SYN floods and encoded payloads were detected, proving the effectiveness of the methodology. The project enhanced both theoretical understanding and practical skills in cybersecurity.  
  
Future Work:  
- Automating traffic analysis using Python scripting.  
- Integrating ELK Stack for real-time dashboards.  
- Simulating more advanced attack scenarios (e.g., MITM, malware beaconing).

## Recommendations

- Regularly capture and analyze internal network traffic for proactive threat detection.  
- Train teams to interpret Zeek logs for early warning signs.  
- Combine Wireshark with IDS tools like Snort for layered security.

## References

1. Wireshark Official Documentation – https://www.wireshark.org/docs/  
2. Zeek Network Security Monitor – https://zeek.org/  
3. Nmap Network Mapper – https://nmap.org/  
4. Practical Packet Analysis by Chris Sanders

## Appendices

- Appendix A: Sample conn.log Output from Zeek  
- Appendix B: Screenshot of TCP Stream in Wireshark  
- Appendix C: List of Simulated Attacks