**Network Traffic Analysis Using Wireshark and Zeek**Project Report  
Submitted By: Piyush Srivastava

Under the Guidance of: MR. Ayush Kumar

Course: Cyber Security

Institution: United College Of Engineering and Research, Prayagraj  
Date: 31/07/2025

****

***Abstract***

This project explores the analysis of network traffic using two leading open-source tools: **Wireshark** and **Zeek**. Wireshark offers deep packet inspection and visualization, while Zeek excels in scalable network monitoring through event-driven logs. The report delves into capturing, filtering, and interpreting packet data to identify anomalies, malicious activities, and performance bottlenecks. The project demonstrates how combining these tools enhances visibility into network behaviour, aids in intrusion detection, and supports forensic investigations. Real-time packet captures and Zeek logs offer practical insight into the effectiveness of proactive network monitoring strategies

***Table of Contents***

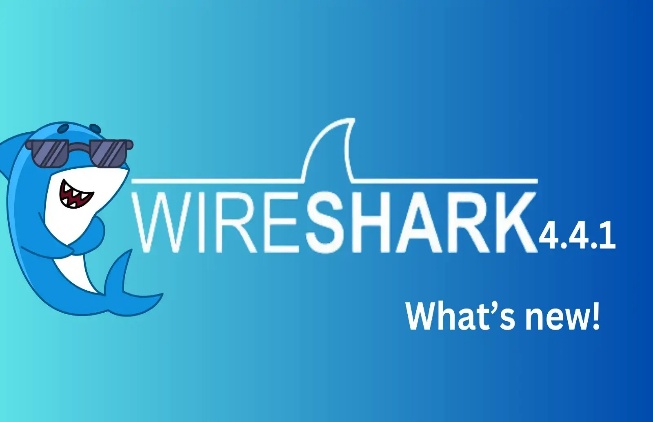
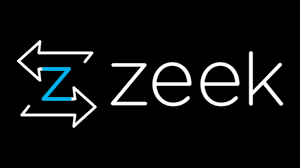
1. List of Figures and Tables
2. Introduction
3. Literature Review
4. Methodology/Approach
5. Results and Discussion
6. Conclusion
7. Recommendations
8. References

***List of Figures and Tables***

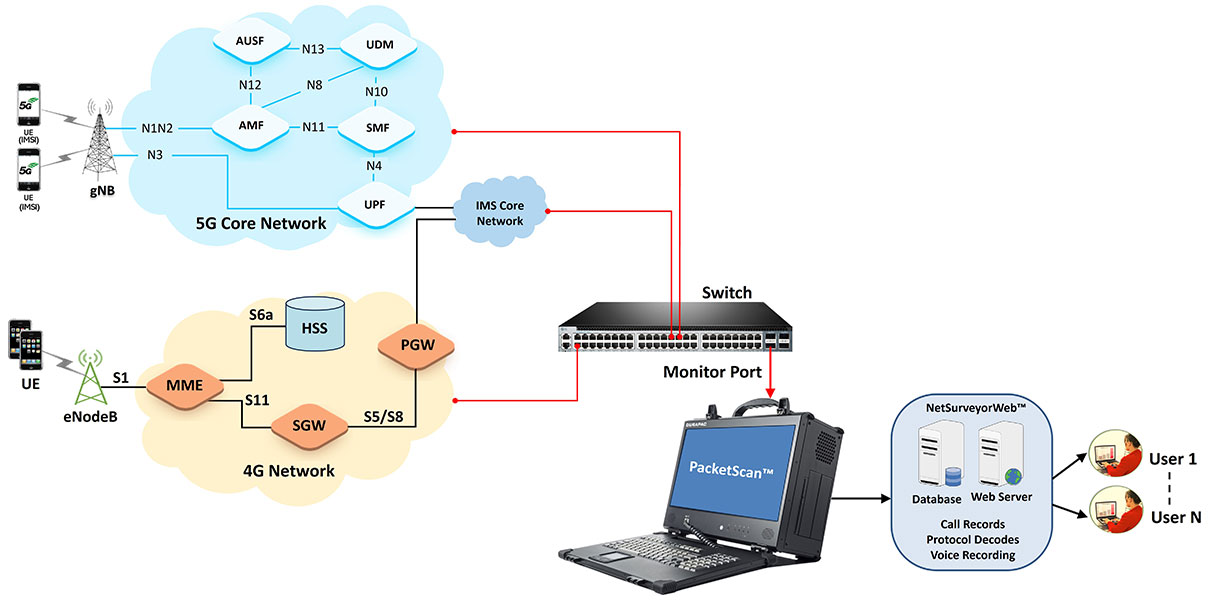
* **Figure 1**: Wireshark User Interface
* **Figure 2**: Packet Capture Example in Wireshark
* **Figure 3**: Zeek Log Files Overview
* **Figure 4**: Protocol Hierarchy in Wireshark
* **Table 1**: Feature Comparison: Wireshark vs Zeek
* **Table 2:**Captured Packet Types During Analysis

***1. Introduction***

Modern networks are prone to sophisticated threats and performance issues. Network Traffic Analysis (NTA) involves monitoring, capturing, and interpreting traffic to ensure performance, reliability, and security. Tools like **Wireshark** and **Zeek** are essential for network administrators and security professionals. This report investigates how these tools can be used collaboratively to detect anomalies and identify malicious patterns.

***Packet Scan***



***2. Literature Review***

Wireshark and Zeek have been extensively used in academic and industry research. Studies highlight Wireshark’s capability in protocol-level inspection, while Zeek (formerly Bro) is recognized for real-time intrusion detection and traffic logging. Research suggests that combining packet-based (Wireshark) and log-based (Zeek) tools can enhance NTA efficiency. Academic papers also emphasize Zeek's extensibility via custom scripts.



***3. Methodology/Approach***

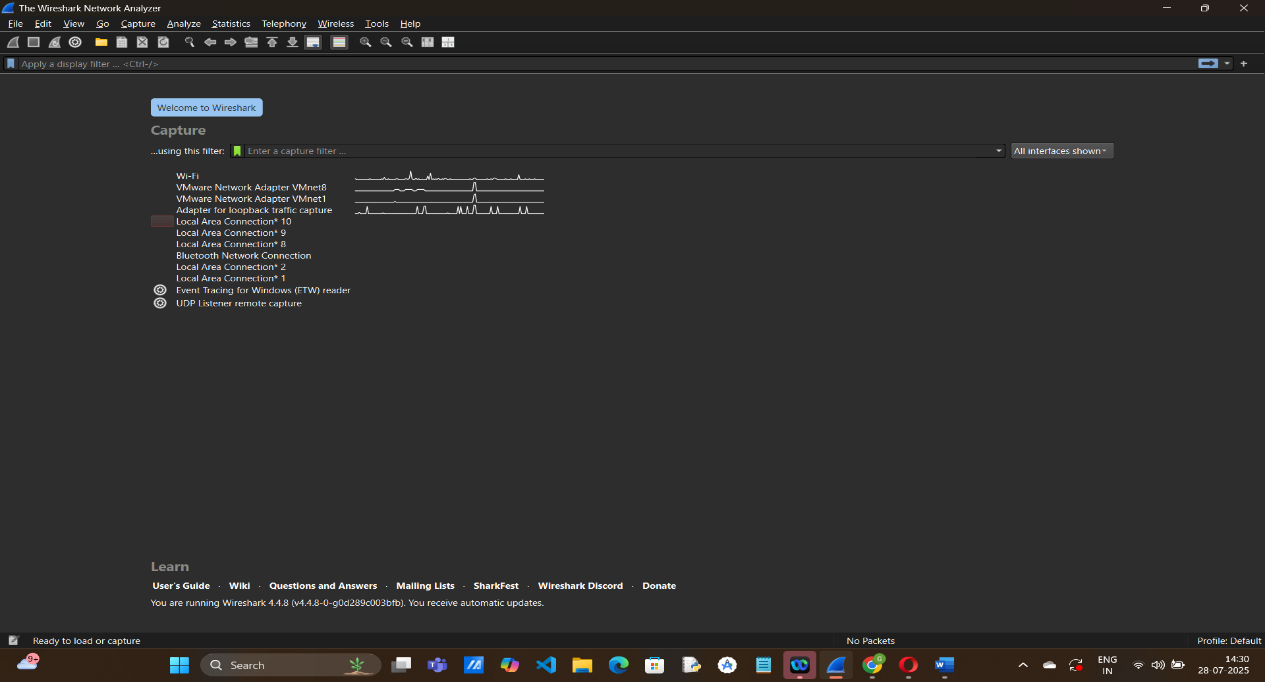
**Tools Used:**

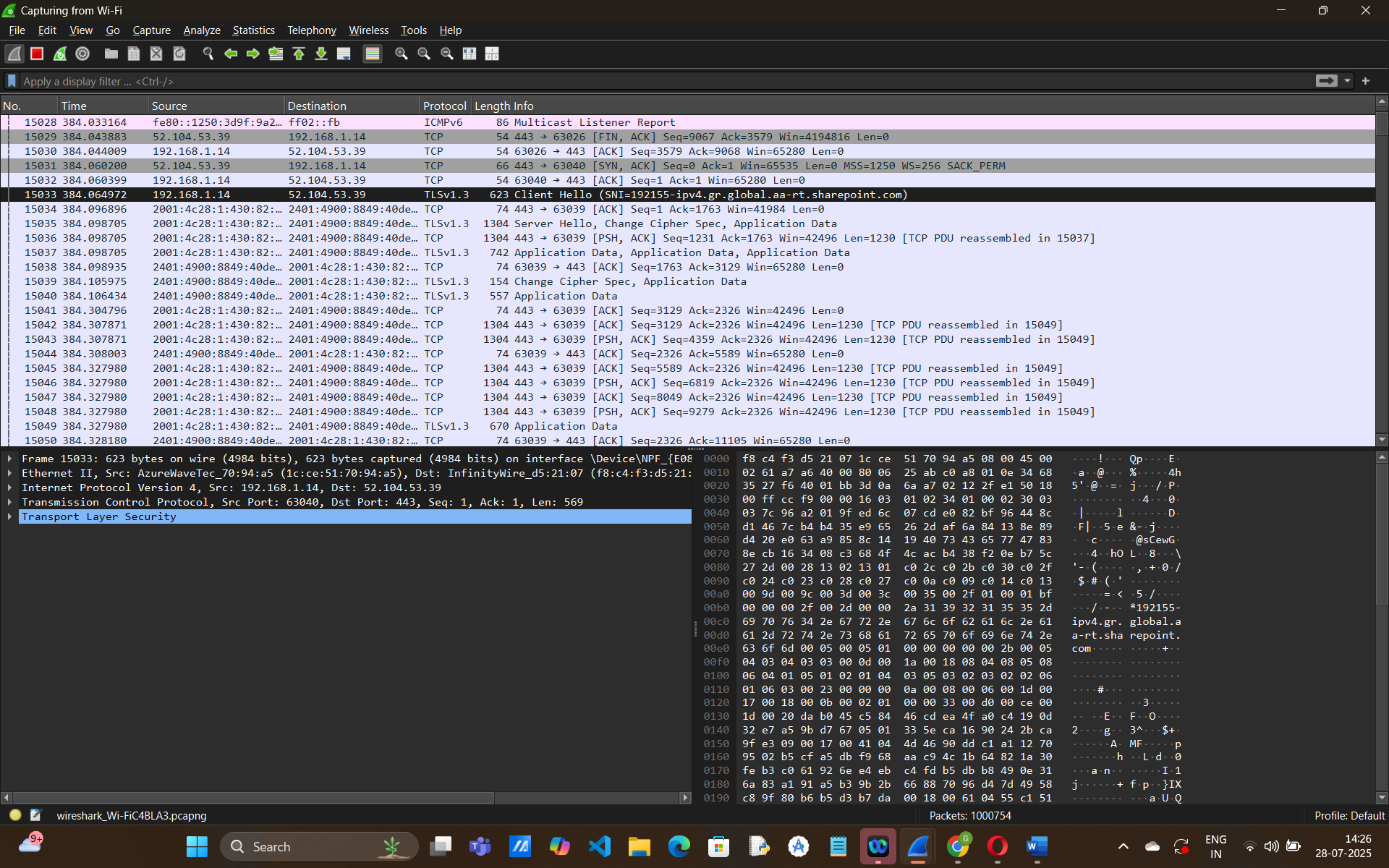
* **Wireshark**: For real-time capture and packet analysis.
* **Zeek**: For script-based logging and analysis.

**Procedure:**

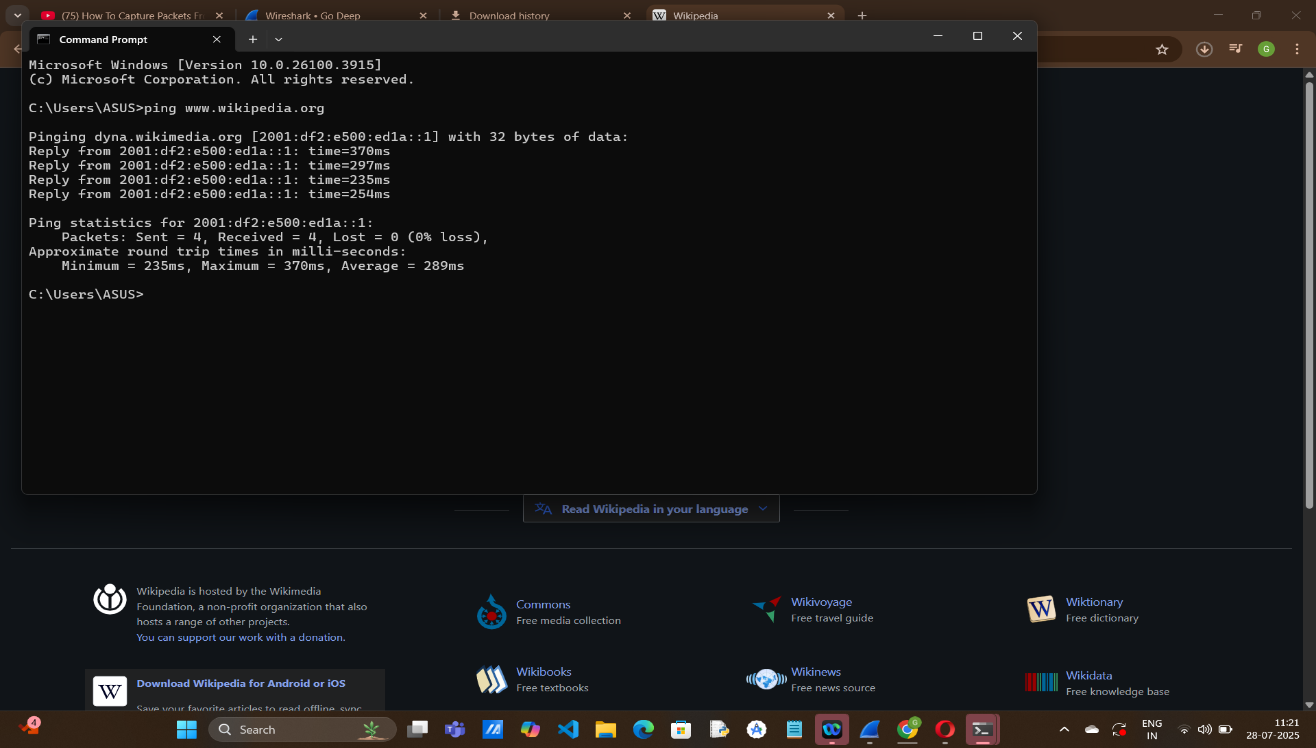
1. Setup of a test network with simulated traffic.
2. Capturing traffic using Wireshark and saving .pcap files.
3. Running Zeek on captured files to generate logs (e.g., HTTP, DNS, Conn logs).
4. Analyzing logs for anomalies like malformed packets, port scans, suspicious DNS queries.

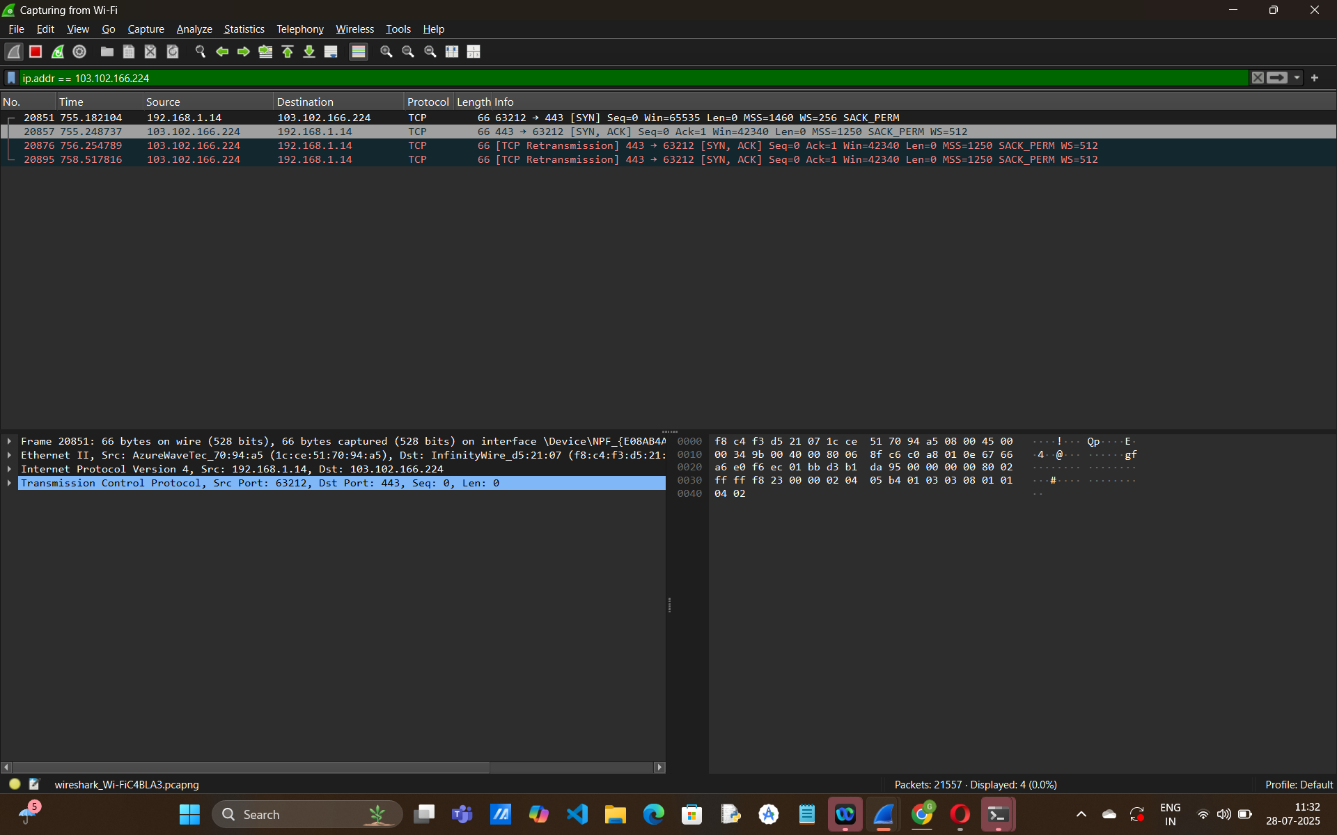
***Figure 1: Wireshark User Interface***



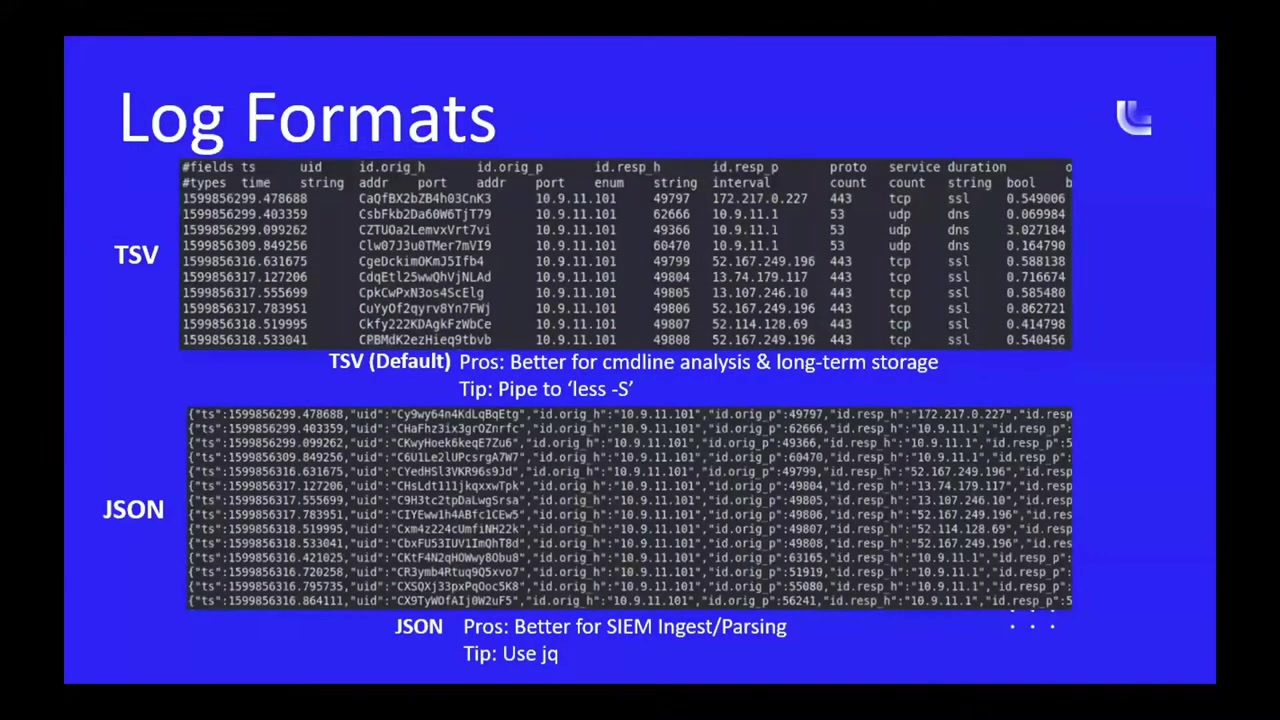


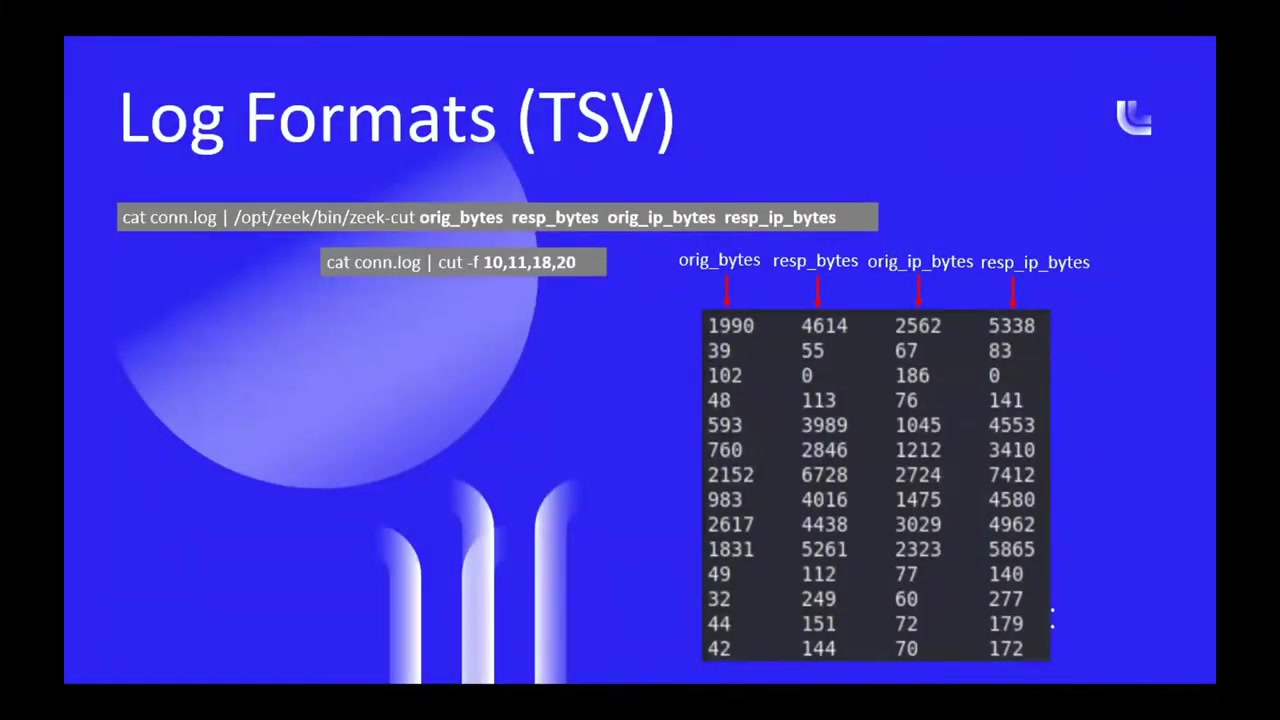
***Figure 2: Packet Capture Example in Wireshark***



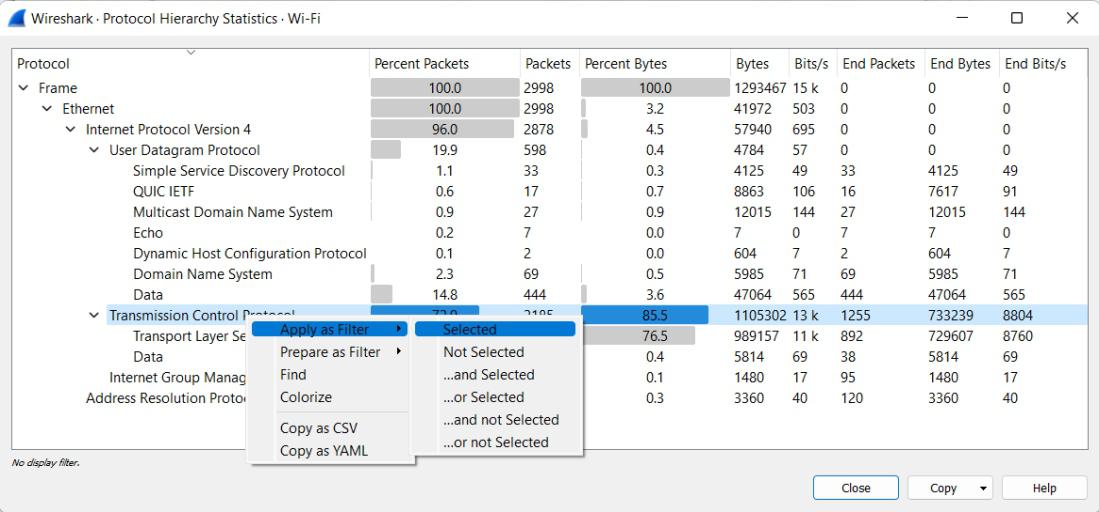


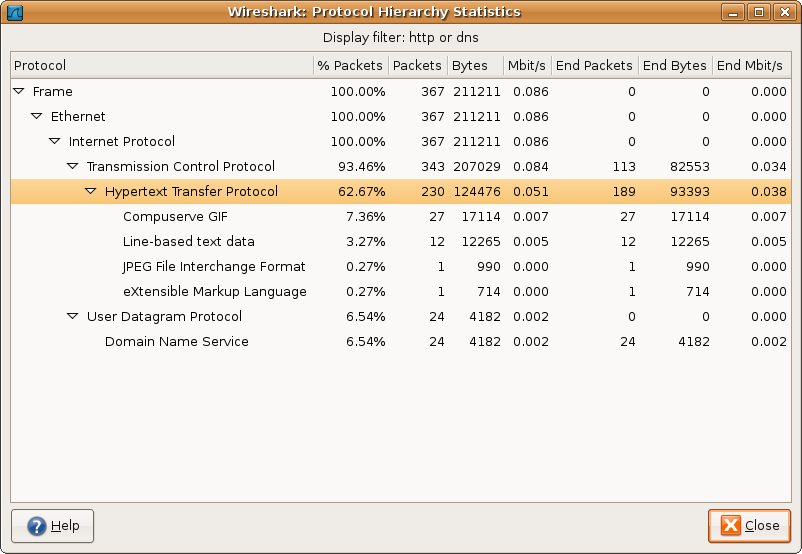
***Figure 3: Zeek Log Files Overview***





***Figure 4: Protocol Hierarchy in Wireshark***

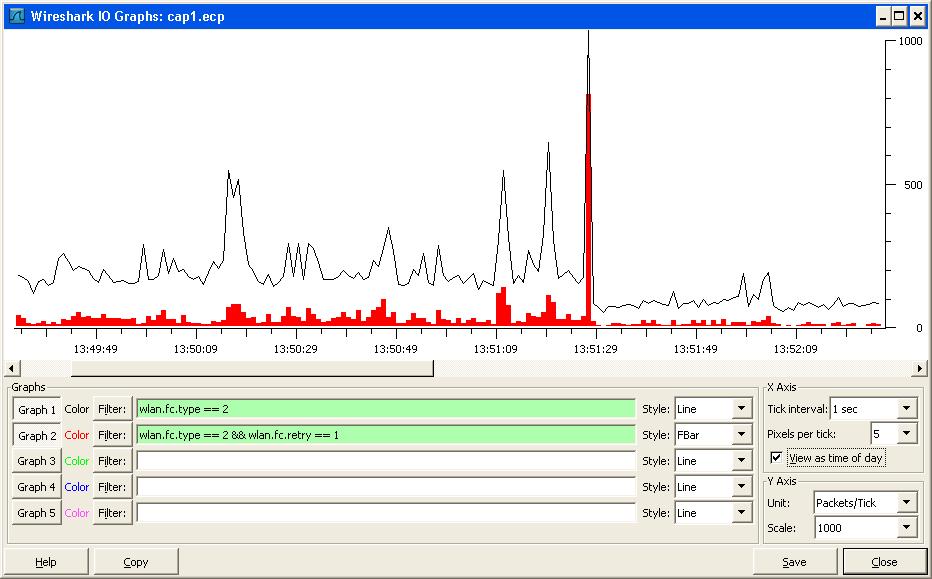




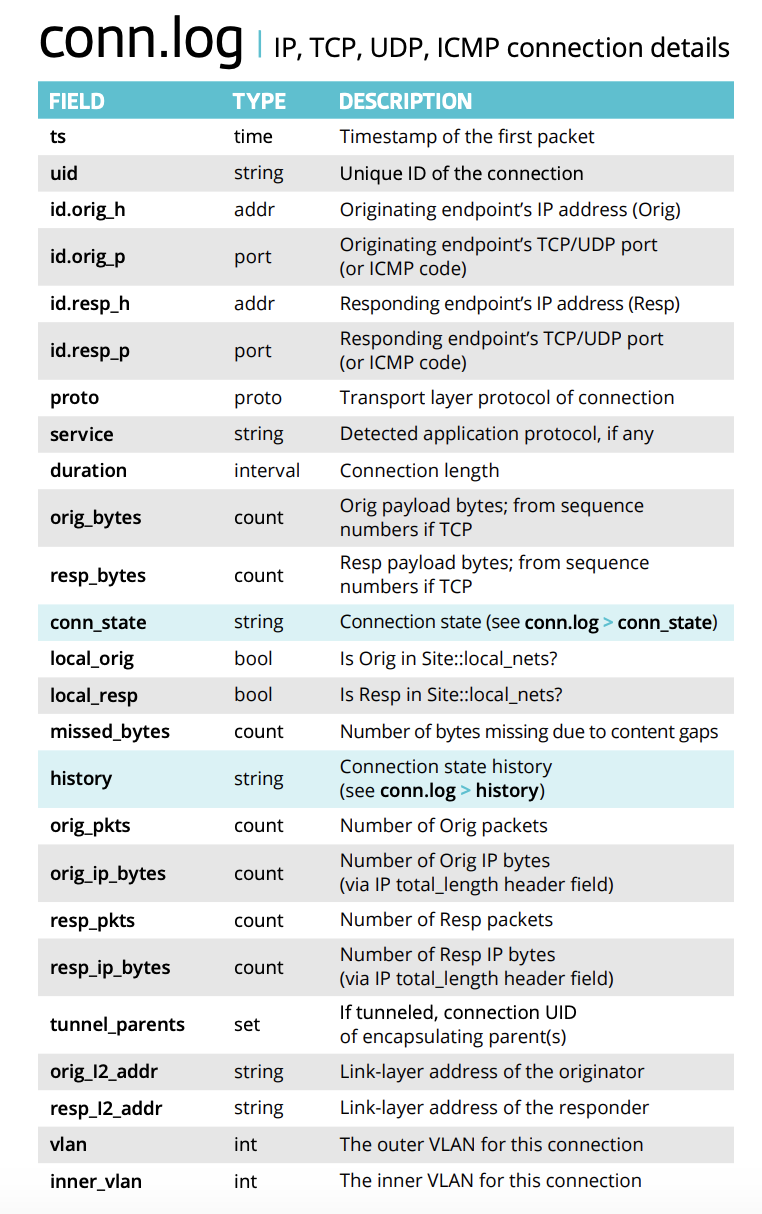
***4. Results and Discussion***

Wireshark helped in identifying protocols used (TCP, UDP, HTTP, DNS), revealing spikes in traffic and retransmissions. Zeek's logs showed:

* Suspicious DNS requests (e.g., unusual domains).
* High number of failed connection attempts (potential port scans).
* HTTP log entries with suspicious User-Agents.
* ***Graph of traffic volume over time in Wireshark.***



***Sample Zeek dns.log and conn.log***



***Table 1: Comparison of Wireshark and Zeek***

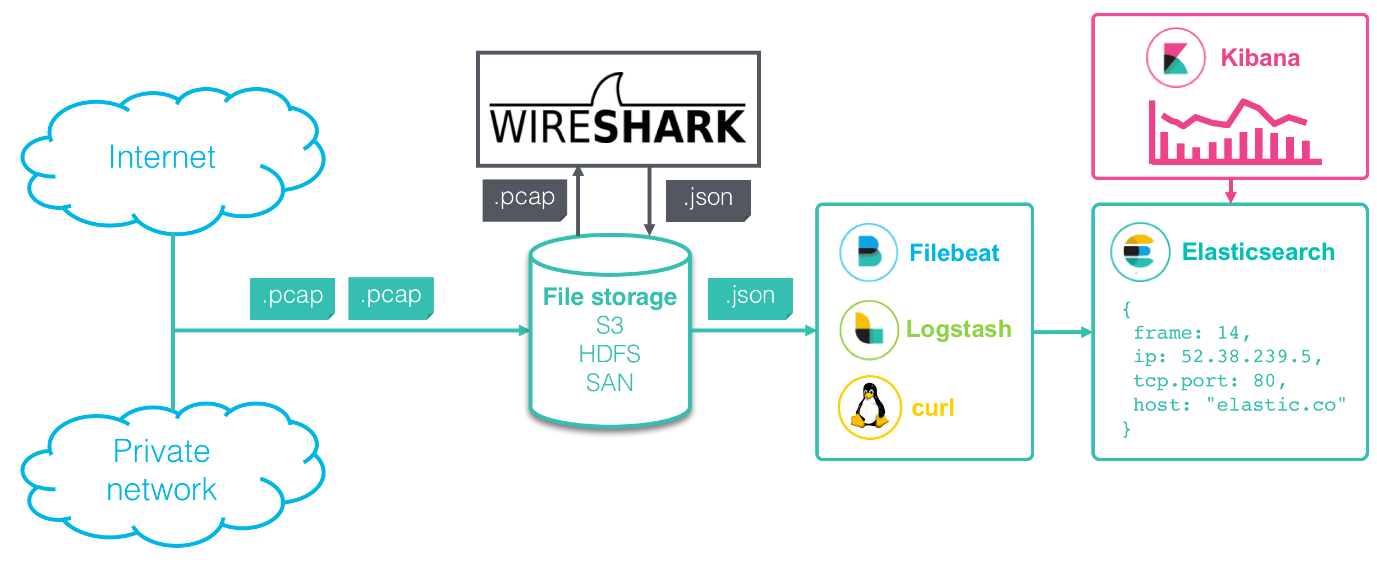
| ***Feature*** | ***Wireshark*** | ***Zeek*** |
| --- | --- | --- |
| Capture Method | Packet-based | Event-based |
| Visualization | GUI | Text Logs |
| Real-time Analysis | Yes | Yes |
| Intrusion Detection | Limited | Extensive via scripts |
| Ease of Use | Moderate | Advanced (scripting) |

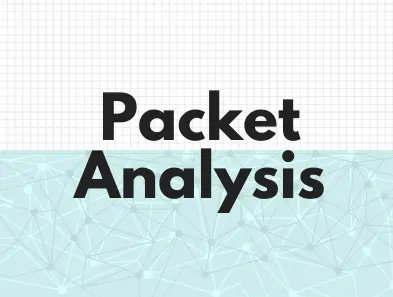
***Table 2: Captured Packet Types During Analysis***

| ***Protocol*** | ***Description*** | ***Number of Packets*** | ***Percentage (%)*** |
| --- | --- | --- | --- |
| TCP | Transmission Control Protocol | 5,462 | 45.8% |
| UDP | User Datagram Protocol | 3,210 | 26.9% |
| HTTP | Hypertext Transfer Protocol | 1,120 | 9.4% |
| DNS | Domain Name System | 980 | 8.2% |
| ARP | Address Resolution Protocol | 540 | 4.5% |
| ICMP | Internet Control Message Protocol | 310 | 2.6% |
| TLS/SSL | Encrypted Web Traffic | 289 | 2.4% |

***5. Conclusion***

The integration of Wireshark and Zeek creates a comprehensive network analysis system. Wireshark provides deep packet visibility, while Zeek offers behavioral insights. The tools together reveal both real-time and historic anomalies, enhancing network situational awareness. Their open-source nature makes them accessible for educational and professional use.





***6. Recommendations***

* Use Wireshark for training and protocol understanding.
* Deploy Zeek for ongoing network monitoring.
* Regularly update Zeek detection scripts.
* Use automation tools like **Logstash** or **ELK** stack to visualize Zeek data.
* Set alerts for anomaly thresholds in Zeek logs.

***7. References***

1. Wireshark User Guide – https://www.wireshark.org/docs/
2. Zeek Documentation – https://docs.zeek.org/
3. Paxson, V. "Bro: A System for Detecting Network Intruders in Real-Time" (1999).
4. Scapy Python Library – https://scapy.net/
5. Mahajan, R. et al. "Controlling High Bandwidth Aggregates in the Network." SIGCOMM, 2001.

***8. Appendices***

**Appendix A:** Sample Wireshark .pcap file summary  
**Appendix B:** Sample Zeek script for detecting large downloads  
**Appendix C:** Configuration of test virtual network