**Network Traffic Analysis Using Wireshark and Zeek**Project Report  
Submitted By: Mohd Abdus Samad

Under the Guidance of: MR. Nikhil Pandey  
Course: Cyber Security

Institution: United College Of Engineering and Research, Prayagraj  
Date: 02/08/2025

***Abstract***

This project explores the analysis of network traffic using two powerful open-source tools: **Wireshark** and **Zeek**. Wireshark enables deep packet inspection and real-time visualization of network flows, while Zeek offers scalable, event-driven monitoring and detailed log generation. The report examines methods of capturing, filtering, and analyzing packet-level and log-level data to detect anomalies, security threats, and performance bottlenecks.

Combining both tools enables robust visibility into network behavior, enhances the ability to detect intrusions, and supports forensic investigation. The integration of real-time packet capture and Zeek log analysis showcases an effective strategy for proactive network monitoring and threat detection.

***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

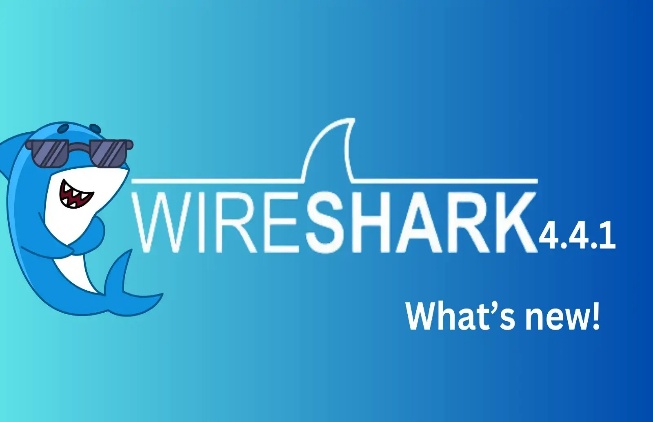
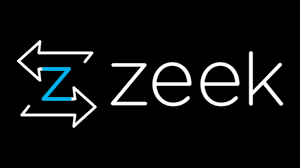
***List of Figures and Tables***

* **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

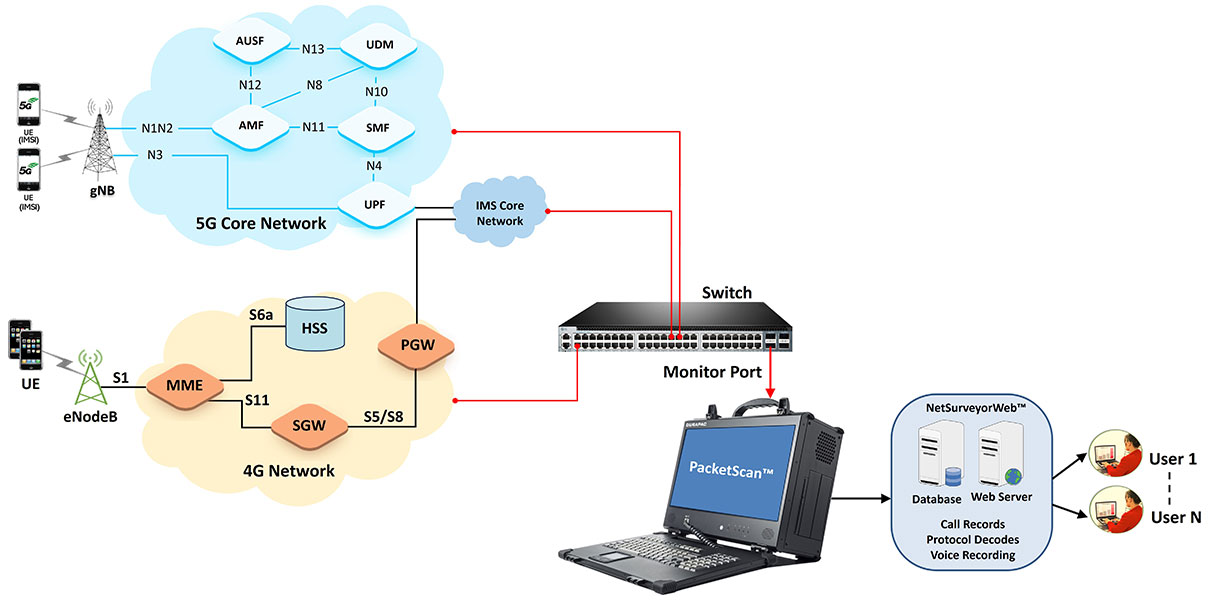
***1. Introduction***

Modern computer networks are increasingly exposed to sophisticated cyber threats and performance challenges. Network Traffic Analysis (NTA) refers to the systematic monitoring and inspection of network data to ensure performance, reliability, and security. Wireshark and Zeek are among the most widely used tools by network engineers and cybersecurity professionals. This project investigates the synergistic use of both tools for efficient anomaly detection, malware tracing, and traffic behavior monitoring in real-time and offline scenarios.

.

***Packet Scan***



***2. Literature Review***

Wireshark and Zeek have been featured prominently in both academic and industry studies.

- Wireshark is renowned for its ability to perform detailed protocol analysis at the packet level.

-Zeek (formerly Bro) is well-suited for policy-based traffic monitoring and log generation.

Studies suggest that using Wireshark for packet-level inspection and Zeek for behavioral analysis results in better detection of security threats. Zeek's scripting capabilities also enable custom detection logic tailored to specific environments.



***3. Methodology/Approach***

**Tools Used:**

* **Wireshark**: For live packet capture,filtering,and inspection.
* **Zeek**: For log-based network behavior analysis using scripts.

Procedure:

1. A test virtual network was set up to simulate various traffic patterns.

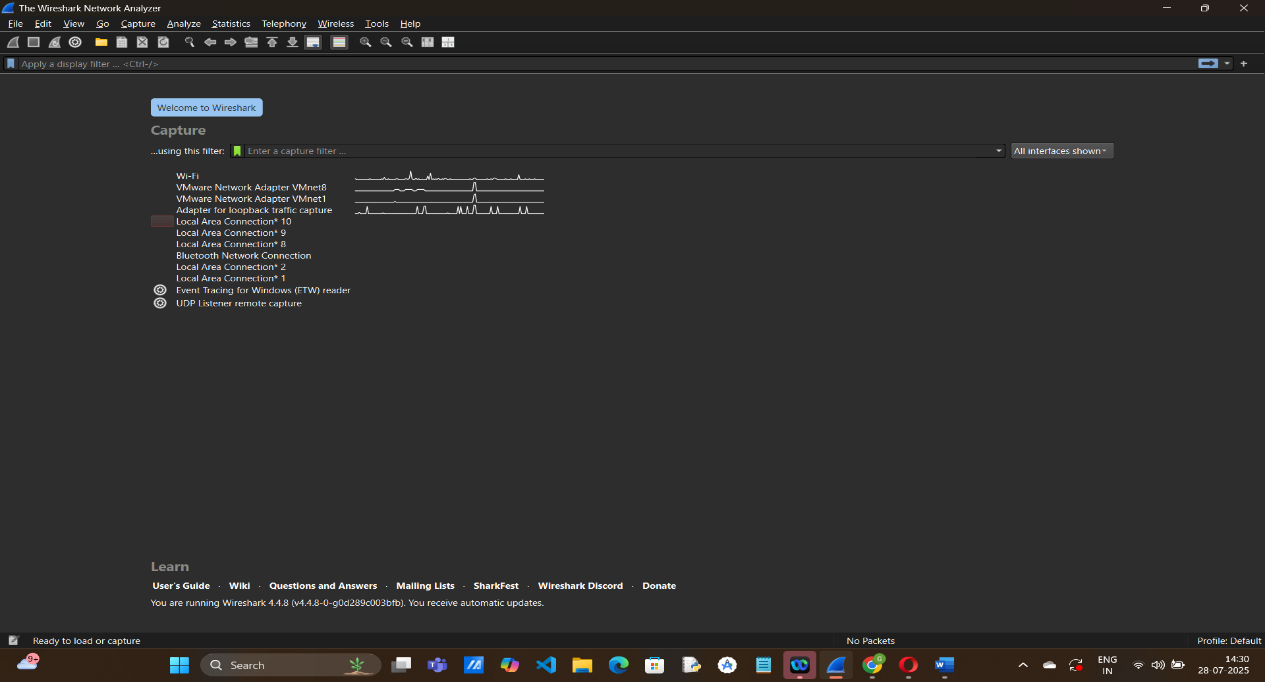
2. Network traffic was captured using Wireshark and stored as .pcap files.

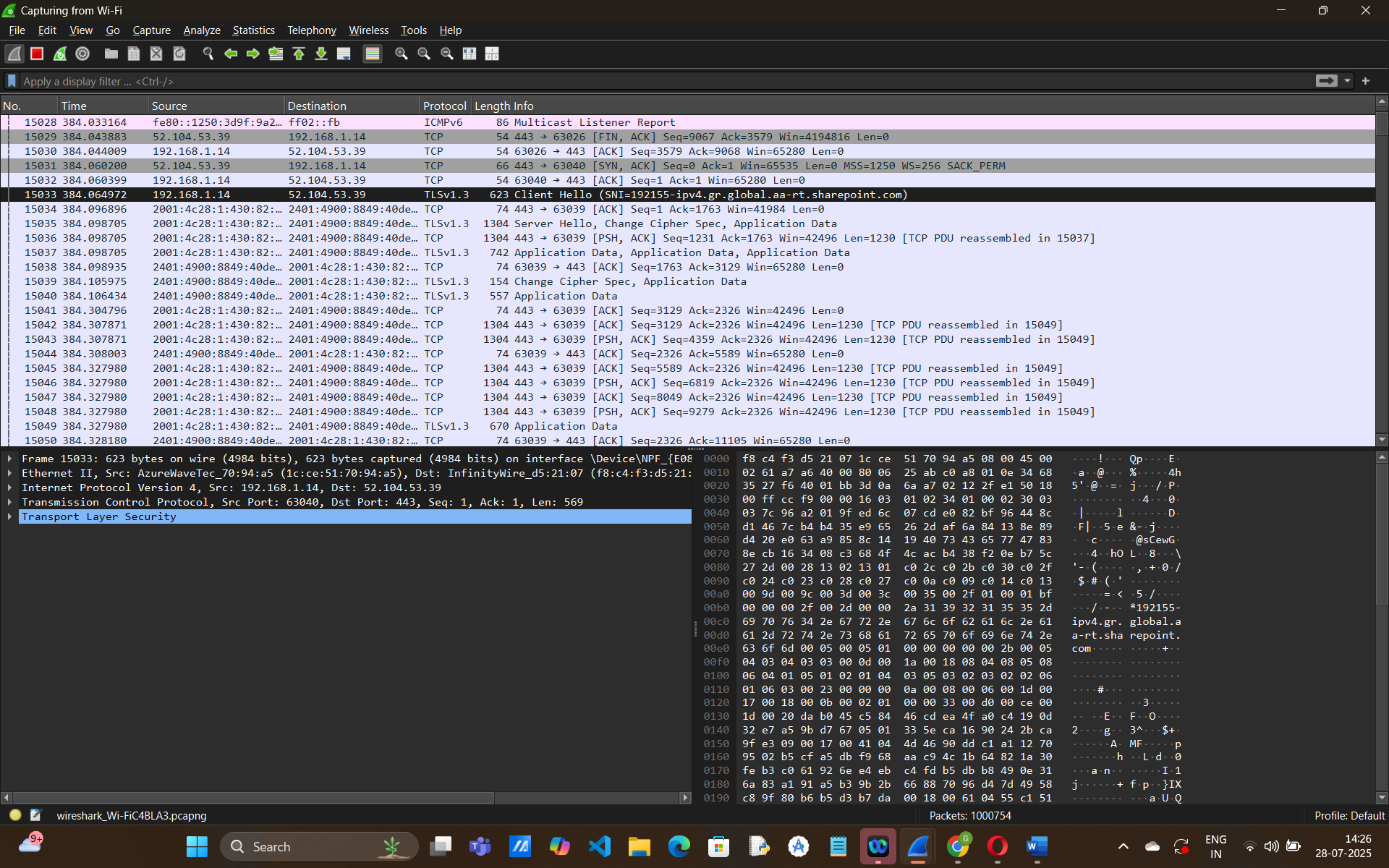
3. The .pcap files were processed through Zeek to generate logs such as conn.log, dns.log, http.log.

4. Logs were analyzed to detect:

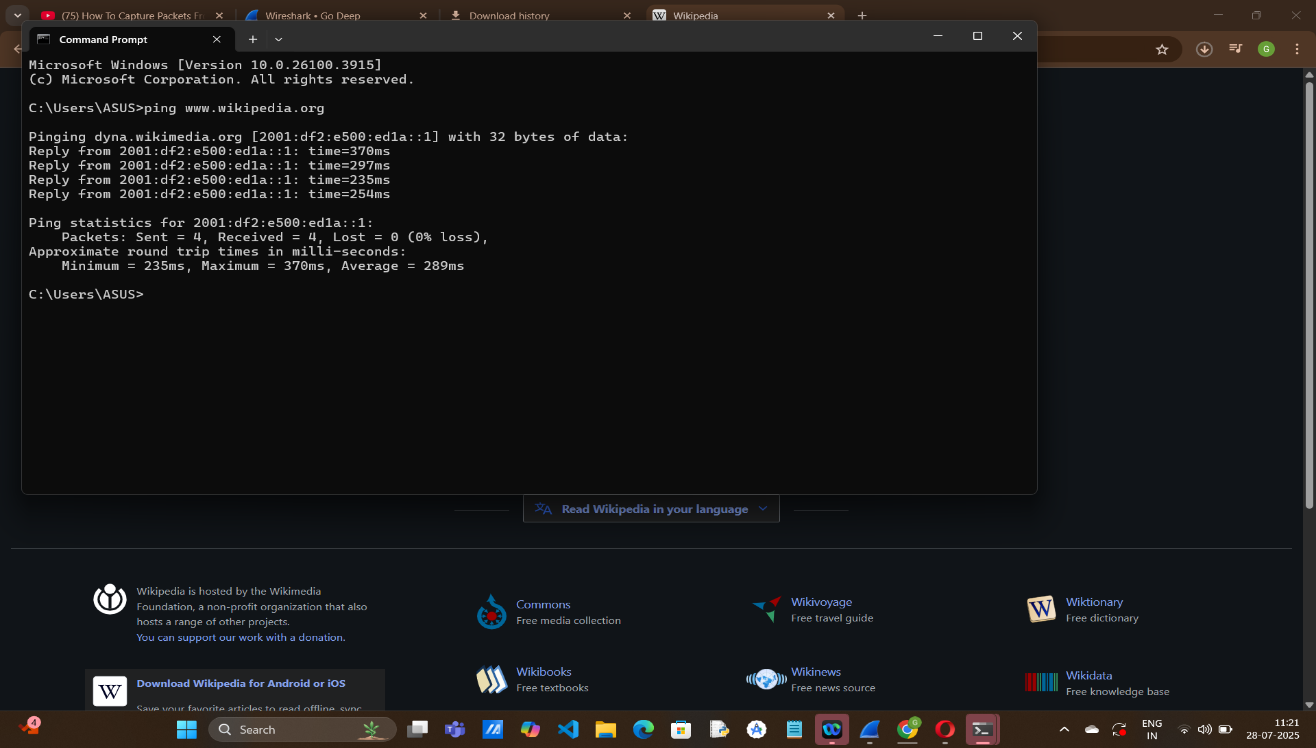
* + Malformed packets
  + DNS tunneling
  + Port scanning
  + Suspicious user-agent headers

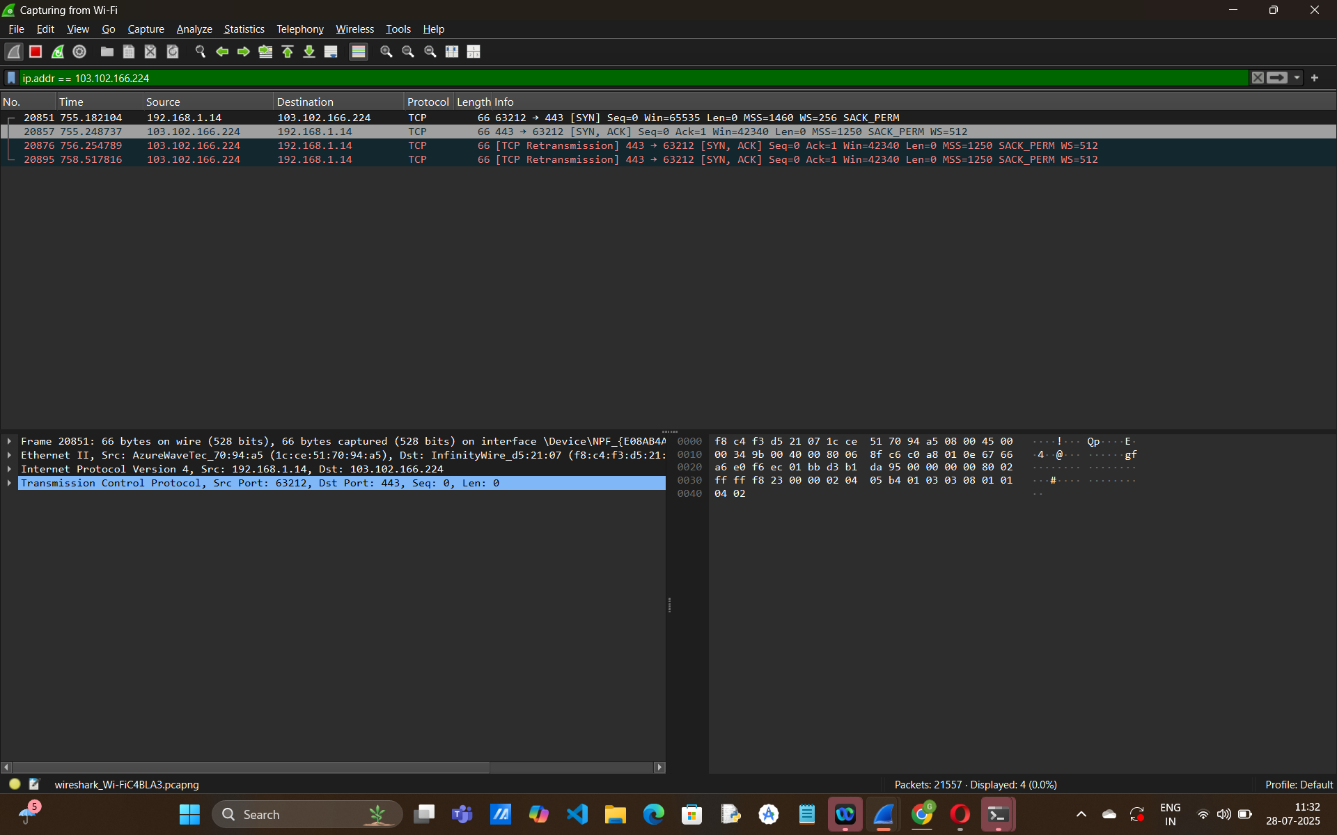
***Figure 1: Wireshark User Interface***



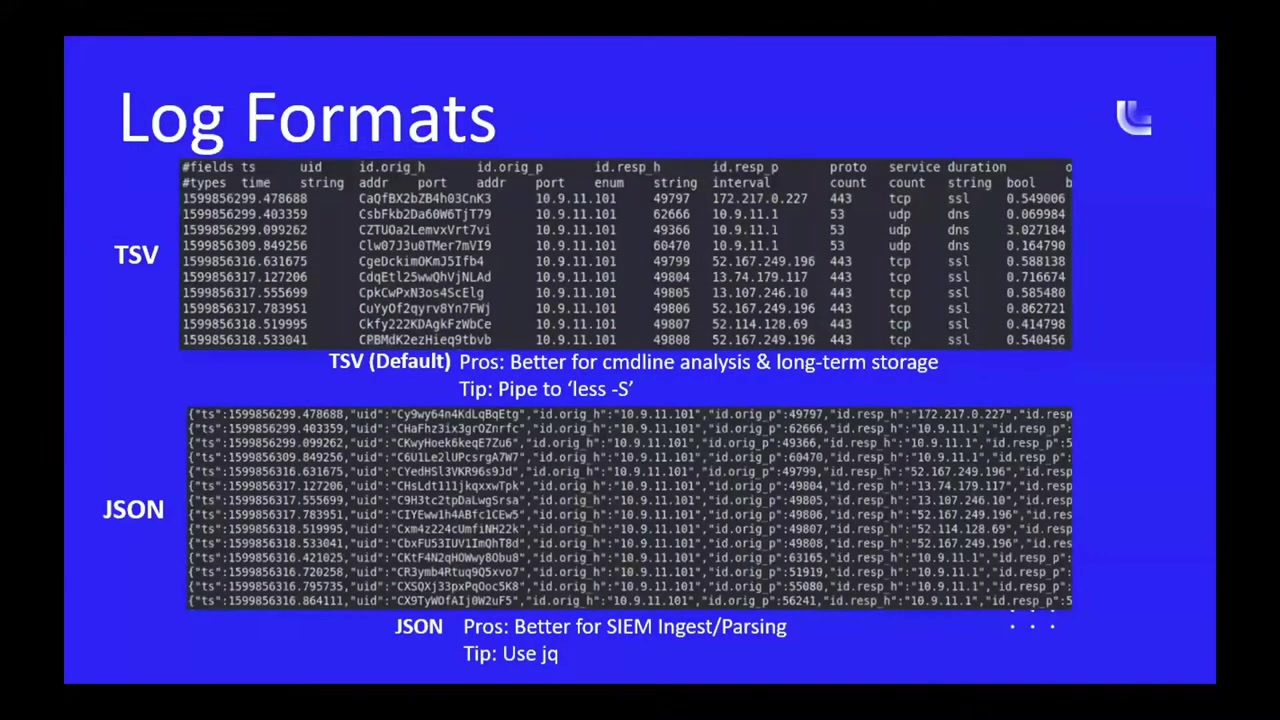


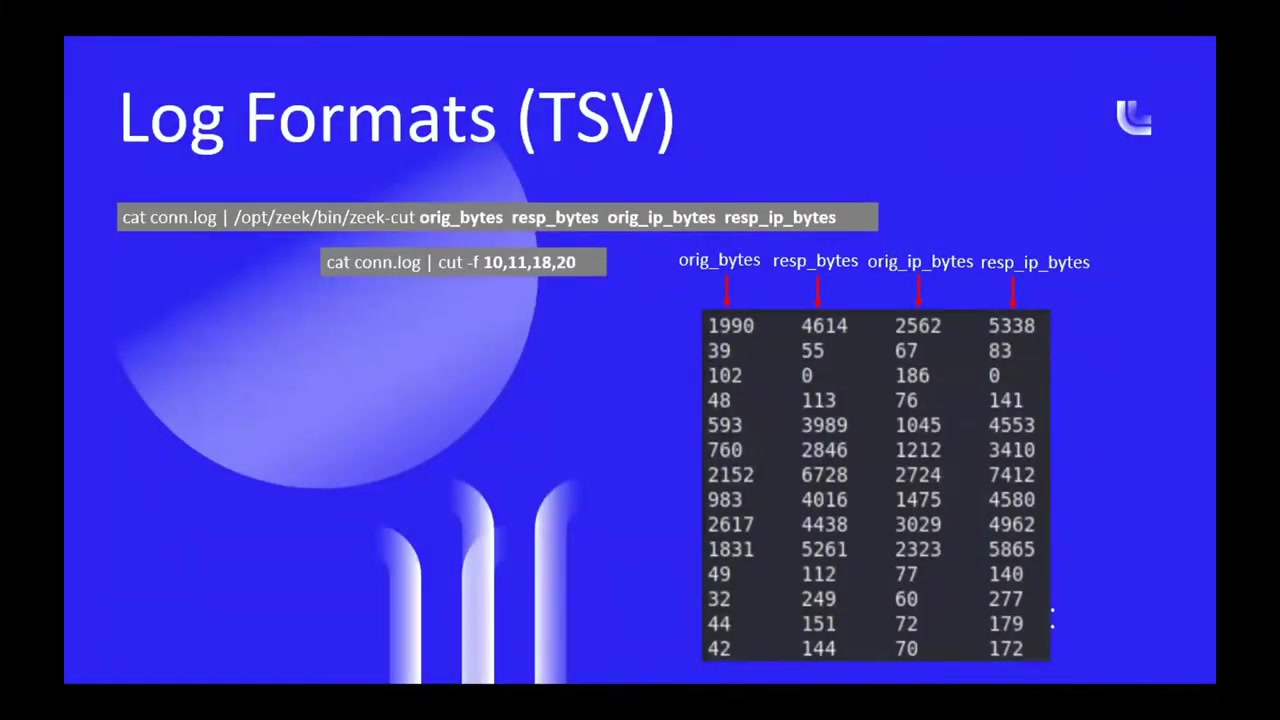
***Figure 2: Packet Capture Example in Wireshark***



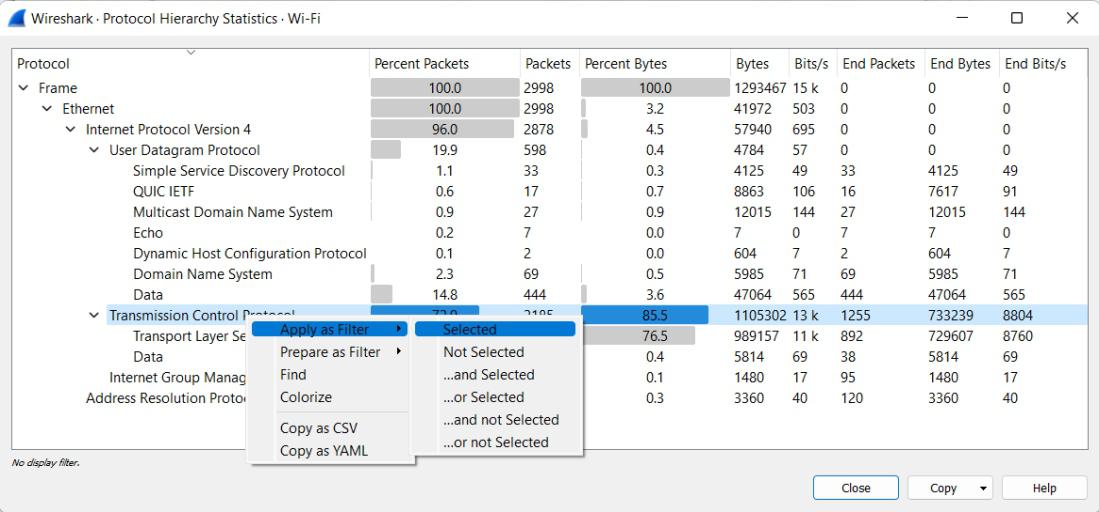


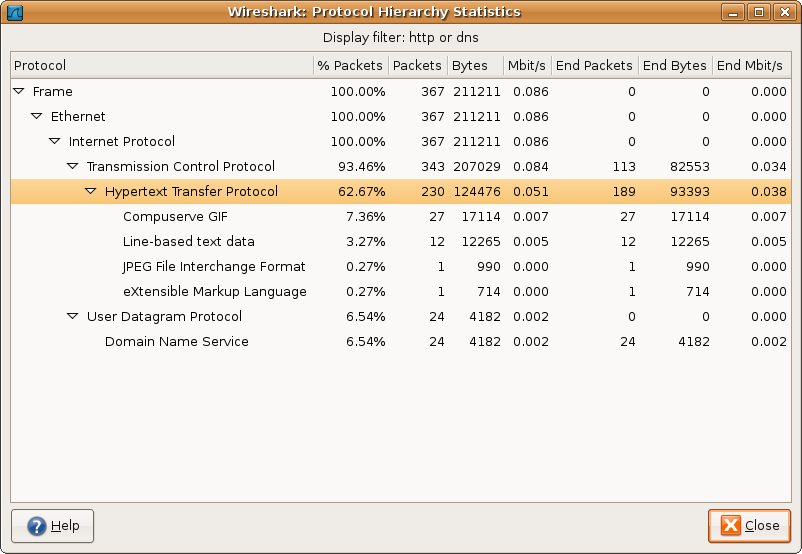
***Figure 3: Zeek Log Files Overview***





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

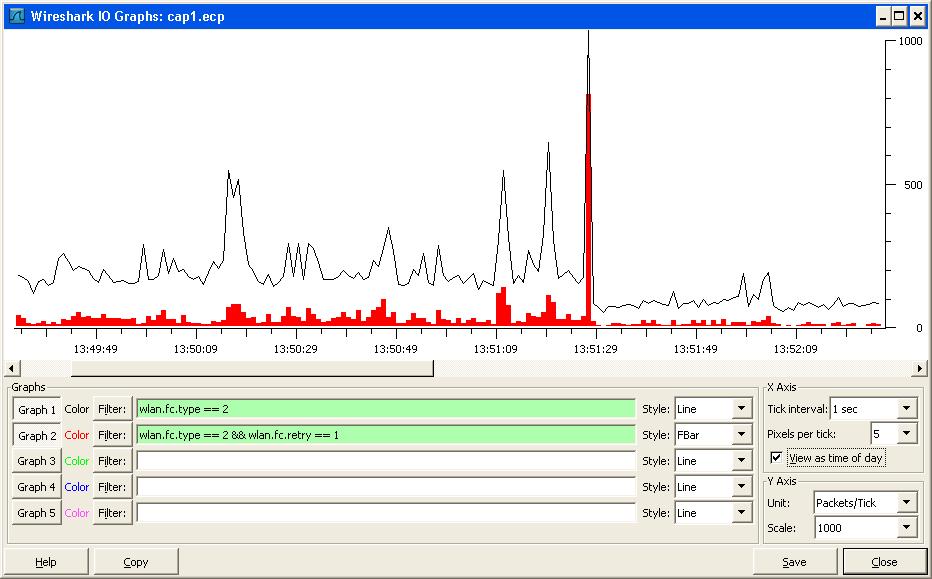




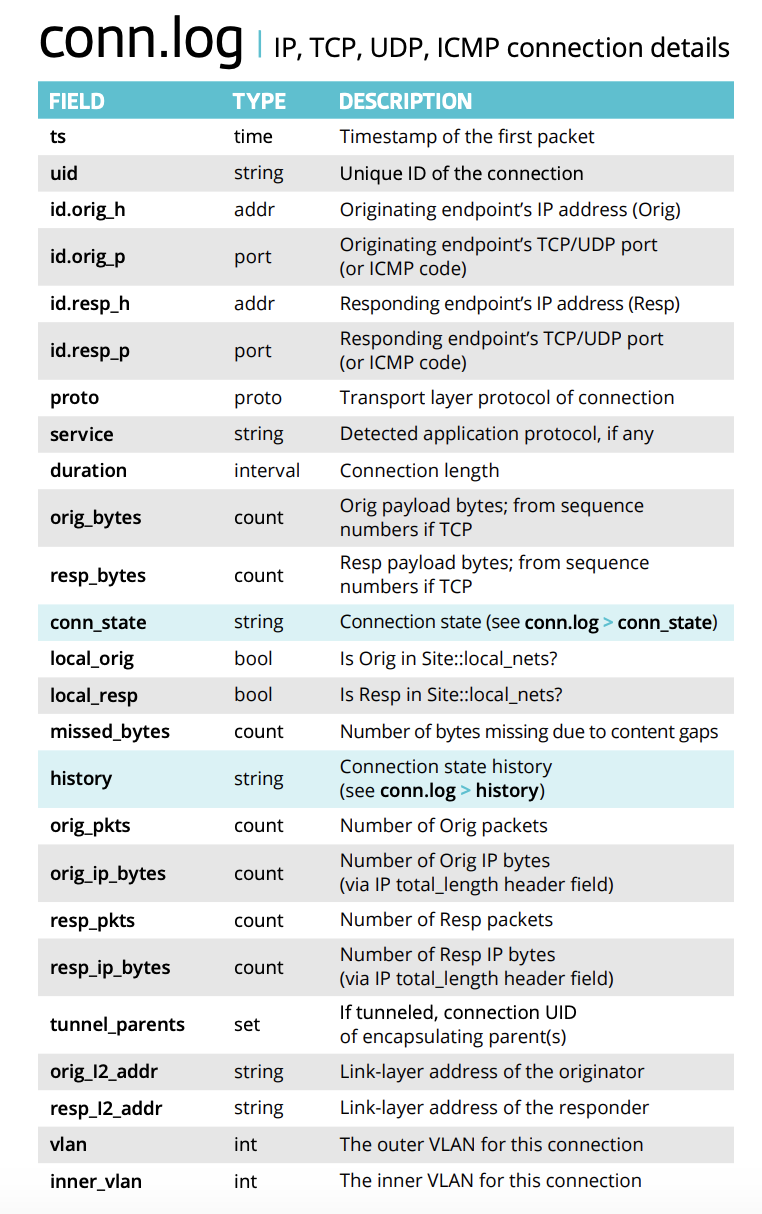
***4. Results and Discussion***

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% |

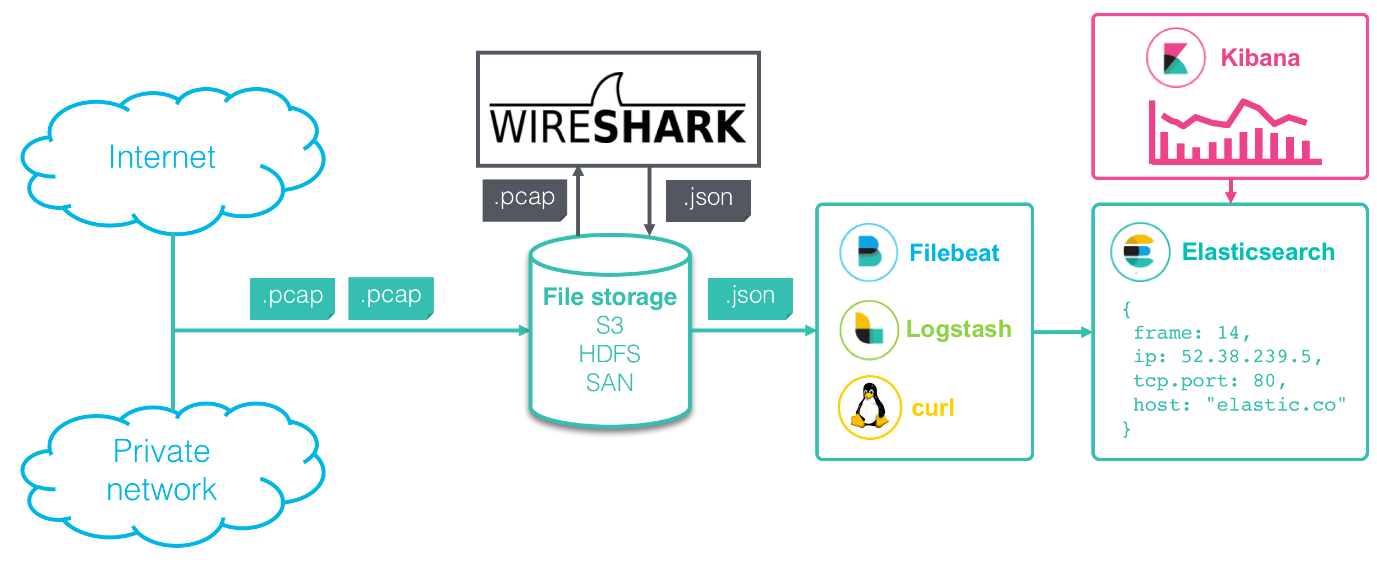
***5. Conclusion***

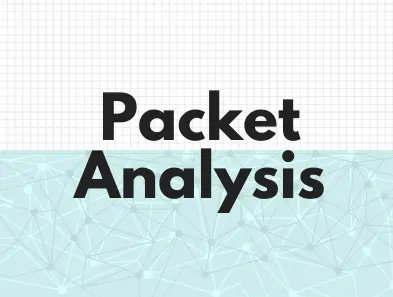
The combined use of wireshark and Zeek provides a robust framework for understanding and securing network environments.

-Wireshark provides packets-level visibility for real-time investigation.

-Zeek offers behavioral monitoring,historical analysis,and scripting flexibility.

Together,they empower cybersecurity analysts to proactively detect,investigate,and respond to threats with greatern confidence.Their open source nature makes them suitable for both educational and enterprise environments.





***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