# IBM Project

**Network Analysis Using Wireshark And Zeek**

**Submitted by:** Ashish Kumar Bind

**College:** United College of Engineering And Research

**Program:** B.Tech 1st year

**Supervisor:** Ayush Sir

**Date:** 01 August 2025

# Network Analysis Using Wireshark and Zeek

## Abstract

This project investigates network traffic analysis using Wireshark and Zeek to identify anomalies and potential security threats. The primary problem addressed is the detection of malicious activity within network communications, which is crucial for maintaining network integrity and security. Our approach utilizes Wireshark for in-depth packet analysis and Zeek for comprehensive network monitoring and event logging. Wireshark enables detailed examination of network packets, facilitating the identification of suspicious patterns and protocols. Zeek complements this by providing a broader view of network behavior, detecting anomalies based on pre-defined rules and signatures.

The key findings include the successful identification of unusual network traffic patterns indicative of potential intrusions or malware communication. By correlating Wireshark's packet-level data with Zeek's event logs, we were able to pinpoint specific hosts and protocols involved in suspicious activities. This project highlights the effectiveness of Wireshark and Zeek as essential tools for network administrators and security analysts, providing valuable insights into network behavior and enhancing overall security posture.

# Table of Content

**1.Introduction**

**2.Methodology/Approach**

**3.Results and Discussion**

**4.Conclusion**

**5.Recommendations**

**6.Refereces**

**7.Appendices**

## Introduction

In today's interconnected world, network analysis has become an indispensable component of cybersecurity and network management. It involves monitoring, inspecting, and analyzing network traffic to identify performance bottlenecks, security threats, and other anomalies. This project, "Network Analysis Using Wireshark and Zeek," delves into the practical application of these powerful tools to address specific challenges in network security and behavior analysis.

The core problem this project aims to solve is the detection and identification of unusual or malicious activities within a network. These activities can range from unauthorized access attempts and data exfiltration to malware communication and denial-of-service attacks. Early detection and effective response to these threats are critical for maintaining the confidentiality, integrity, and availability of network resources.

Wireshark and Zeek were chosen as the primary tools for this project due to their complementary capabilities in network analysis. Wireshark is a widely used network packet analyzer that allows for detailed examination of network traffic at the packet level. Its intuitive interface and powerful filtering capabilities make it ideal for dissecting protocols, inspecting packet contents, and identifying suspicious patterns. Zeek (formerly known as Bro) is a network security monitoring tool that provides a comprehensive view of network activity through event logging and analysis. It uses a signature-based approach to detect known threats and can also identify anomalous behavior based on deviations from established network baselines.

The methodology employed in this project involves capturing network traffic using appropriate methods, followed by detailed analysis using Wireshark and Zeek. Wireshark is used to examine individual packets and identify specific characteristics of network communications, while Zeek is used to generate logs and alerts based on pre-defined rules and anomaly detection algorithms. The project culminates in the presentation of key findings, including identified network anomalies, potential security threats, and insights into overall network behavior. The goal is to demonstrate how Wireshark and Zeek can be effectively utilized to enhance network security and improve network management practices.

## Methodology/Approach

### Overall Plan and Strategy

The project's methodology was structured to provide a clear and repeatable process for network analysis using Wireshark and Zeek. The initial phase involved defining the specific network scenarios to be analyzed, such as identifying suspicious connections, analyzing protocol behavior, and detecting potential security breaches. The approach emphasized a combination of signature-based detection (using Zeek's capabilities) and anomaly-based detection (leveraging both Zeek and Wireshark to identify deviations from normal network behavior). A key aspect of the strategy was to integrate the findings from both tools to gain a more comprehensive understanding of network events.

### Tools and Technologies

The primary tools employed in this project were Wireshark and Zeek.

* **Wireshark:** Wireshark is a free and open-source packet analyzer. Its core functionality lies in capturing network traffic and allowing users to inspect the data at a granular level. It supports a wide range of network protocols and provides features for filtering, sorting, and analyzing packets. Wireshark's contribution to this project includes:
  + **Packet Capture:** Capturing network traffic from various interfaces.
  + **Protocol Dissection:** Decoding and displaying the contents of network packets based on their protocol.
  + **Filtering:** Using display filters to isolate specific types of traffic for analysis (e.g., filtering by IP address, port number, or protocol).
  + **Statistical Analysis:** Generating statistics on captured traffic, such as packet counts, byte counts, and protocol distribution.
* **Zeek:** Zeek is a powerful network security monitoring tool that analyzes network traffic in real-time and generates detailed logs and alerts. Unlike traditional intrusion detection systems, Zeek focuses on understanding network behavior and providing a comprehensive view of network activity. Its key functionalities include:
  + **Network Monitoring:** Monitoring network traffic for suspicious activities.
  + **Event Logging:** Generating detailed logs of network events, such as connections, DNS queries, HTTP requests, and SSL certificates.
  + **Signature-Based Detection:** Detecting known threats based on pre-defined signatures and rules.
  + **Anomaly Detection:** Identifying unusual network behavior based on deviations from established baselines.
  + **Scripting:** Using Zeek's scripting language to customize analysis and detection capabilities.

### Step-by-Step Process

The following steps outline the process of capturing, processing, analyzing, and interpreting network traffic using Wireshark and Zeek:

1. **Setup and Configuration:**
   * **Wireshark:** Installing Wireshark on a suitable platform and configuring it to capture traffic from the desired network interface.
   * **Zeek:** Installing Zeek and configuring it to monitor the network interface. This includes setting up Zeek's logging and alert mechanisms.
2. **Data Collection:**
   * Using Wireshark to capture network traffic for a specific duration or until a specific event occurs.
   * Allowing Zeek to passively monitor network traffic and generate logs and alerts.
3. **Initial Analysis with Wireshark:**
   * Loading the captured traffic into Wireshark.
   * Applying basic filters to isolate specific types of traffic (e.g., HTTP, DNS, or SSH).
   * Examining packet details to identify potential anomalies or suspicious patterns.
4. **Analysis with Zeek:**
   * Reviewing Zeek's logs to identify suspicious connections, unusual DNS queries, or other anomalous events.
   * Using Zeek's scripting capabilities to customize analysis and detection rules.
5. **Correlation and Interpretation:**
   * Correlating Wireshark's packet-level data with Zeek's event logs to gain a more comprehensive understanding of network events.
   * Identifying potential security threats or performance bottlenecks based on the combined analysis.

For common network scenarios, the following initial analysis techniques were employed:

* **Protocol Analysis:** Using Wireshark to dissect network protocols and identify any deviations from expected behavior.
* **Identifying Suspicious Connections:** Using Zeek to identify connections to known malicious hosts or unusual port numbers.
* **Performance Monitoring:** Using Wireshark to analyze network latency and identify potential performance bottlenecks.

## Results and Discussion

This section presents the findings from our network analysis conducted using Wireshark and Zeek. We explored various network scenarios to identify anomalies, potential security threats, and overall network behavior. The analysis focused on specific case studies, each demonstrating the practical application of these tools in solving network-related problems.

### Case Study 1: Detecting a Port Scan

One common network reconnaissance technique is port scanning, where an attacker attempts to determine which ports on a target machine are open and listening. Detecting such scans is crucial for identifying potential threats early on. Using Wireshark, we captured network traffic and filtered for TCP packets with the SYN flag set, which is indicative of a connection attempt. By analyzing the source IP addresses and destination ports, we identified a host attempting to connect to a wide range of ports on a target machine within a short period. This behavior strongly suggested a port scan.

Zeek's connection logs corroborated this finding. Zeek automatically identifies and logs connection attempts, including the number of connections, bytes transferred, and duration. A high number of connection attempts from a single source to multiple destination ports within a short timeframe, as highlighted by Zeek, further confirmed the presence of a port scan. By combining Wireshark's packet-level detail with Zeek's aggregated connection data, we were able to confidently identify and characterize the port scan activity.

*[Visual Aid: A screenshot of a Wireshark capture showing a series of TCP SYN packets from a single source IP to multiple destination ports. Another screenshot of a Zeek connection log highlighting the high number of connection attempts.]*

### Case Study 2: Analyzing DNS Query Anomalies

DNS (Domain Name System) is a critical component of network communication. Analyzing DNS traffic can reveal suspicious activities such as domain generation algorithms (DGAs) used by malware to communicate with command-and-control servers. We used Wireshark to capture DNS queries and responses. We then filtered for unusually long domain names or queries to non-standard top-level domains (TLDs). Such queries can indicate that a compromised host is attempting to resolve domains generated by a DGA.

Zeek's DNS logs provided additional context. Zeek logs all DNS queries and responses, including the domain name, query type, and response code. By analyzing these logs, we identified queries for domains that were unusually long and had no legitimate purpose. This analysis, combined with the Wireshark capture, allowed us to identify potential malware communication attempts.

*[Visual Aid: A screenshot of a Wireshark capture showing DNS queries with unusually long domain names. A Zeek DNS log highlighting the frequency and characteristics of these anomalous DNS queries.]*

### Case Study 3: Identifying a Potential Malware Beacon

Malware often uses beaconing techniques to periodically communicate with its command-and-control (C2) server. This communication can be identified by analyzing network traffic patterns. We used Wireshark to look for periodic HTTP or HTTPS requests from a specific host to a remote server. The consistency in timing and the nature of the requests raised suspicion.

Zeek's HTTP logs further aided this investigation. Zeek logs all HTTP requests, including the URI, user-agent, and referrer. By correlating the Wireshark capture with Zeek's HTTP logs, we confirmed the periodic nature of the requests and identified the user-agent string being used. Unusual user-agent strings or requests to suspicious URLs strengthened the suspicion of a malware beacon. Further investigation of the host revealed the presence of malware.

*[Visual Aid: A screenshot of a Wireshark capture showing periodic HTTP requests. A Zeek HTTP log highlighting the user-agent string and the consistency of the requests.]*

### Challenges Encountered

Several challenges were encountered during the analysis process. One significant challenge was dealing with large volumes of network traffic, which made it difficult to isolate specific events of interest. Effective filtering and careful analysis were necessary to overcome this issue. Another challenge was the presence of encrypted traffic (HTTPS), which limited the ability to inspect the contents of the packets directly. However, even with encryption, metadata such as TLS certificate information and connection patterns could still provide valuable insights. Additionally, complex protocol interactions required a deep understanding of network protocols and their expected behavior.

## Conclusion

This project successfully demonstrated the effectiveness of network analysis using Wireshark and Zeek to identify anomalies and potential security threats. By combining Wireshark's detailed packet analysis with Zeek's comprehensive network monitoring capabilities, we were able to gain valuable insights into network behavior and detect suspicious activities. The initial problem of identifying malicious activity within network communications was addressed through a systematic approach of data capture, analysis, and correlation.

Key insights gained include a deeper understanding of network protocols, traffic patterns, and the techniques used by attackers to compromise network security. We learned how to effectively use Wireshark's filtering and dissection capabilities to analyze network packets and identify suspicious patterns. Additionally, we gained proficiency in using Zeek to generate detailed logs and alerts, enabling us to detect anomalies and potential security breaches. The practical scenarios explored, such as detecting port scans, analyzing DNS query anomalies, and identifying malware beacons, showcased the versatility and power of these tools in real-world network environments.

For future work, several enhancements could be undertaken to further improve the project. Integrating Wireshark and Zeek with other security tools, such as intrusion detection systems (IDS) and security information and event management (SIEM) platforms, would allow for more comprehensive threat detection and response. Analyzing different types of network attacks, such as distributed denial-of-service (DDoS) attacks or advanced persistent threats (APTs), would provide valuable insights into emerging threats and attack techniques. Finally, scaling the analysis to larger networks and cloud environments would present new challenges and opportunities for optimizing network security monitoring.

## Recommendations

Based on our findings, we recommend the following:

* **Continuous Monitoring with Zeek:** Deploy Zeek for 24/7 network monitoring to establish a baseline of normal behavior and detect anomalies in real-time. Customize Zeek scripts to focus on specific threats relevant to your network environment.
* **Efficient Packet Capture with Wireshark:** Use capture filters in Wireshark to reduce the volume of captured data, focusing on specific protocols or IP ranges of interest. This improves analysis efficiency.
* **SOC Integration:** Integrate network analysis findings from Wireshark and Zeek into your Security Operations Center (SOC) workflow. Use alerts from Zeek to trigger investigations with Wireshark for in-depth packet analysis.

## References

List all academic papers, books, websites, and software documentation referenced throughout this report. Ensure proper citation formatting (e.g., IEEE or APA style).

## Appendices

This section contains supplementary materials that support the findings presented in the main report. Examples include full Zeek logs for specific events, detailed Wireshark filter syntax used, or raw PCAP file summaries. These materials provide additional depth for interested readers.