**DDoS Attack Detection Using Network Traffic Analysis**

**1. Introduction**

This document provides an in-depth analysis of a real-world Distributed Denial-of-Service (DDoS) attack simulation, focusing on detection, analysis, and mitigation. The attack was performed using Hping3 to flood the target with SYN packets from randomized IP addresses, while Wireshark was employed to capture and analyze the resulting network traffic. The report documents the methods used, findings observed, and recommended countermeasures to mitigate similar attacks.

**2. Objective**

The primary goal of this project is to detect and analyze a SYN flood DDoS attack by capturing and inspecting network traffic. The objective is to understand the attack pattern, identify key characteristics, and suggest mitigation strategies to protect networks against similar threats.

**3. Methodology**

The detection process involved the following steps:

* **Tool Utilization:**
* Kali Linux as the attack and analysis platform.
* Wireshark for capturing and analyzing network traffic.
* Hping3 for generating SYN flood traffic.
* **Commands Used:**
* Capture command: sudo wireshark
* SYN flood generation: sudo hping3 -S --flood --rand-source -p 80 <target ip>
* **Data Capture:**
* Packet capture using Wireshark to log network traffic during the attack.
* Visualization and filtering to isolate attack patterns.

**4. Wireshark Analysis and Findings**

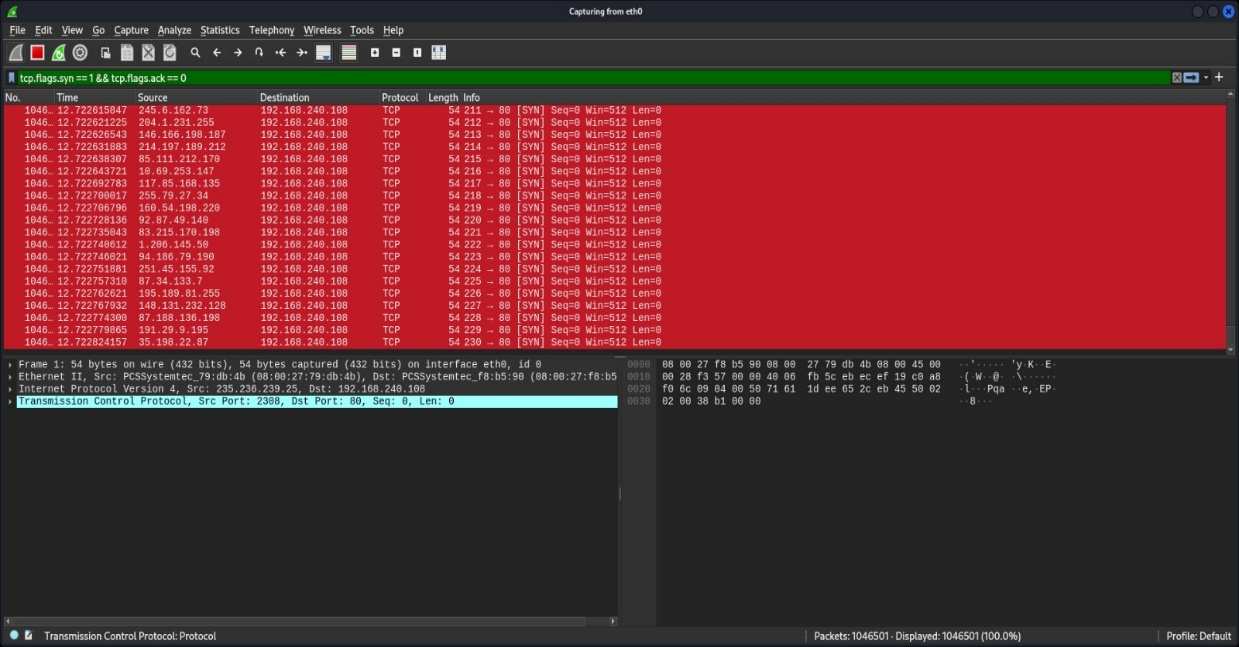
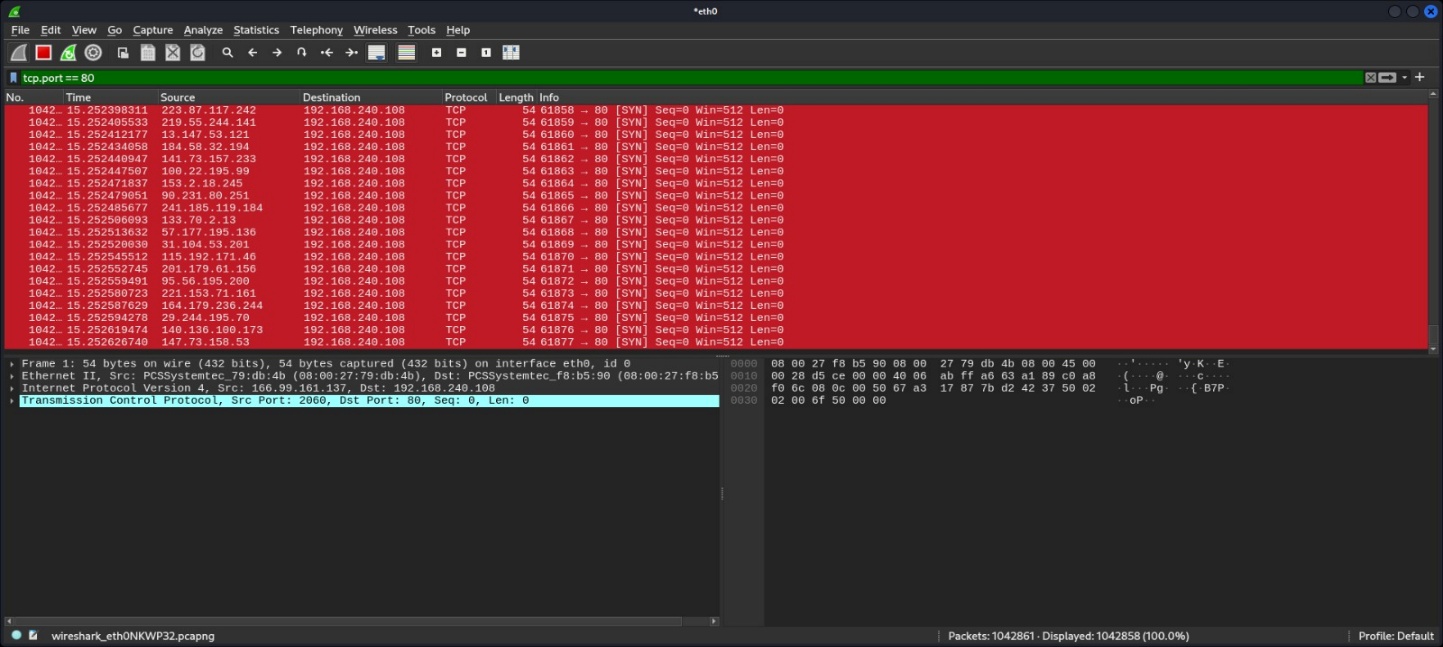
****

Fig.1 SYN Flood Attack Detection

* SYN flood DDoS attack targeting IP 192.168.240.108 detected using Wireshark with the filter tcp.flags.syn == 1 && tcp.flags.ack == 0. The attack involves thousands of SYN packets without an ACK flag, showing that the target is overwhelmed with half-open connections.

 Fig.2 SYN Flood Attack on Port 80

* TCP SYN flood traffic targeting port 80 on IP 192.168.240.108, detected using the filter tcp.port == 80 , showing incomplete handshakes.

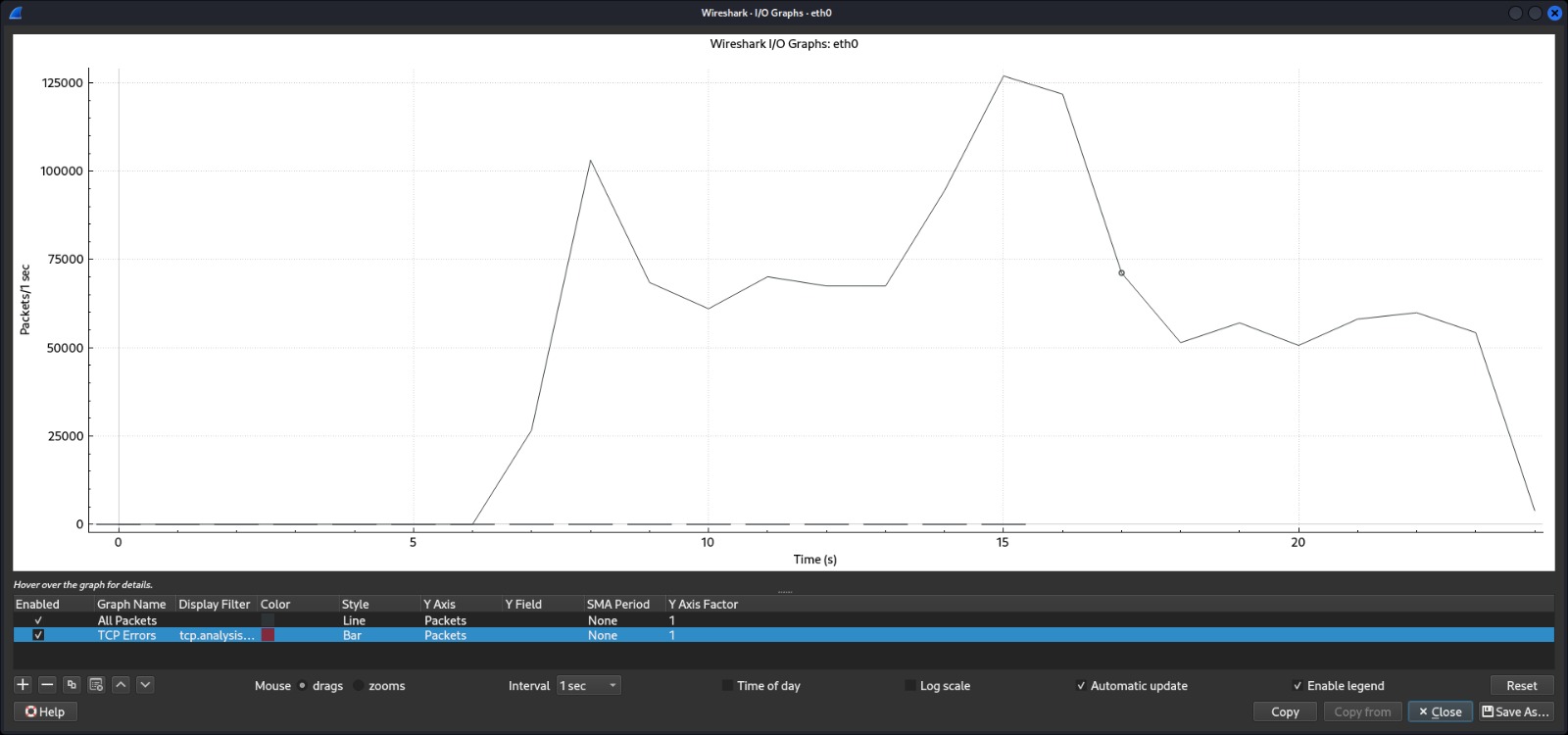


Fig.3 I/O Graph Analysis

* The I/O graph shows Steep spikes (notably at around the 5s and 15s marks) exceeding 125,000 packets per second.The sharp rise and fall patterns suggests SYN flood attack attempts.

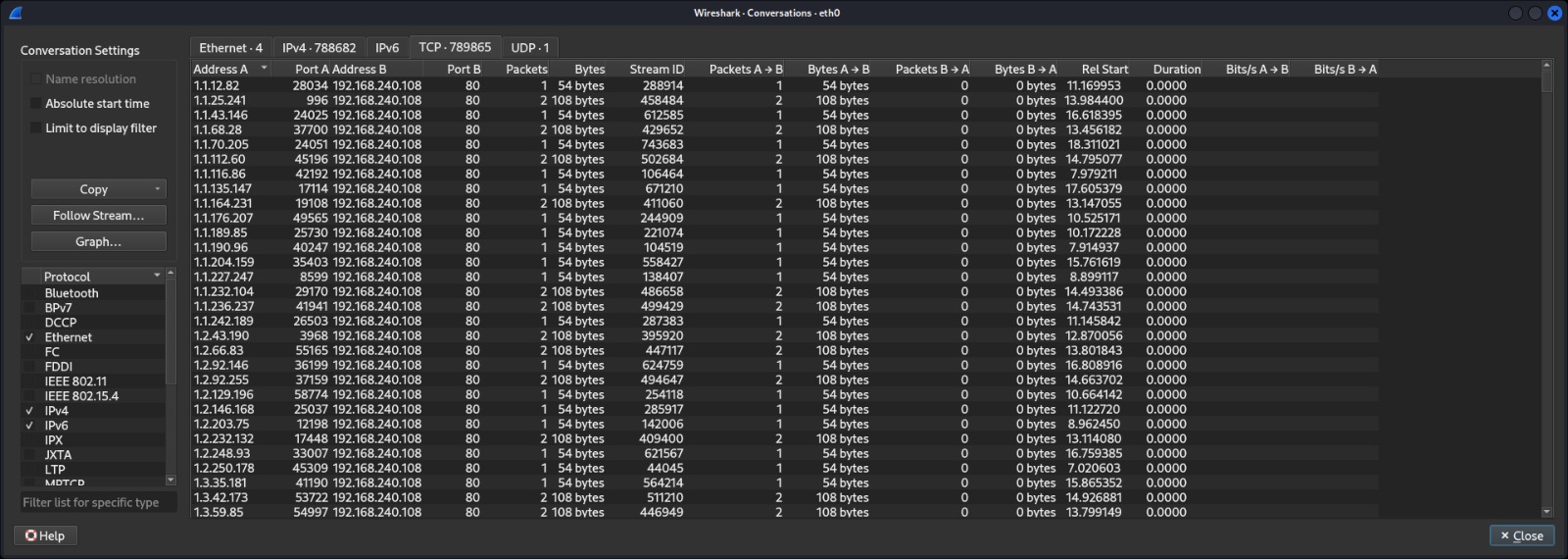


Fig.4 TCP Conversation Statistics

* Multiple IP addresses sending SYN packets to the target IP (192.168.240.108) on port 80, each with minimal byte size (54 or 108 bytes) and zero response bytes indicating a SYN flood DDoS attack.

* **Key findings:**
* High volume of repetitive requests originating from multiple IP addresses.
* Significant surges in network traffic over a short duration.
* Massive number of TCP conversations targeting port 80.
* Minimal data exchange (54 or 108 bytes) per conversation.
* Zero response from the target server

**5. Impact of the Attack**

* **Service Disruption:** The Windows 10 target system may experience slowdowns or become unresponsive.
* **Network Congestion:** The excessive packet volume can degrade overall network performance.
* **Resource Exhaustion:** A prolonged attack can consume bandwidth, CPU, and memory resources.

**6. Recommendations for Mitigation**

* **Implement Rate Limiting:** Restrict excessive incoming traffic from single sources.
* **Use Firewalls & IDS:** Deploy an **Intrusion Detection System (IDS)** to monitor and block suspicious traffic.
* **Enable SYN Cookies:** Protect against **SYN Flood attacks** by enabling SYN cookies on the target machine.
* **Monitor Network Logs:** Continuously analyze traffic patterns for early threat detection.

**7. Conclusion**

* This Wireshark analysis successfully **detected a potential DDoS attack** by analyzing traffic patterns and identifying key indicators like **traffic spikes and TCP errors**. Proactive measures, such as rate limiting and firewall configurations, are essential to mitigate the impact of such attacks.