N-SAM REPORT

A COMPLETE NETWORK ANALYSIS

Prepared For :

FYP Panel

Executive Summary and Analysis Parameters

Date of Report:

2024-03-28

Analysis Start Time:

2024-03-26 05:14:53.422408

Analysis End Time:

2024-03-27 05:37:23.552305

Analyzed IP:

All

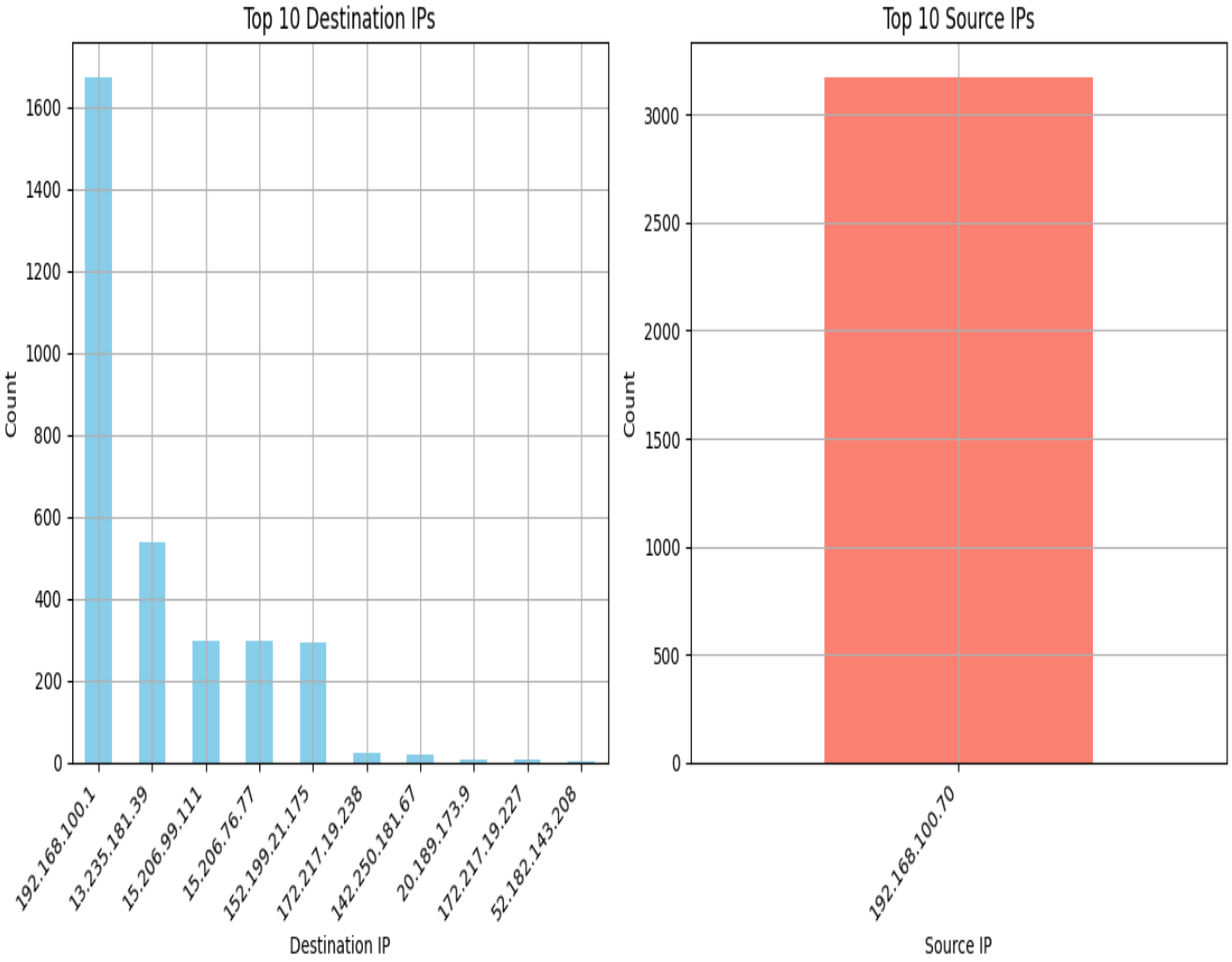
Executive Summary

This report presents an analysis of network within the specified time frame, focusing on the demanded IPs (i.e All). The analysis period spans from (2024-03-26 05:14:53.422408) to (2024-03-27 05:37:23.552305), during which various network activities were monitored and evaluated.

Throughout this period, a comprehensive assessment was conducted on the specified IPs. These insights serve to inform stakeholders about the current state of network security and highlight areas requiring immediate attention or further investigation.

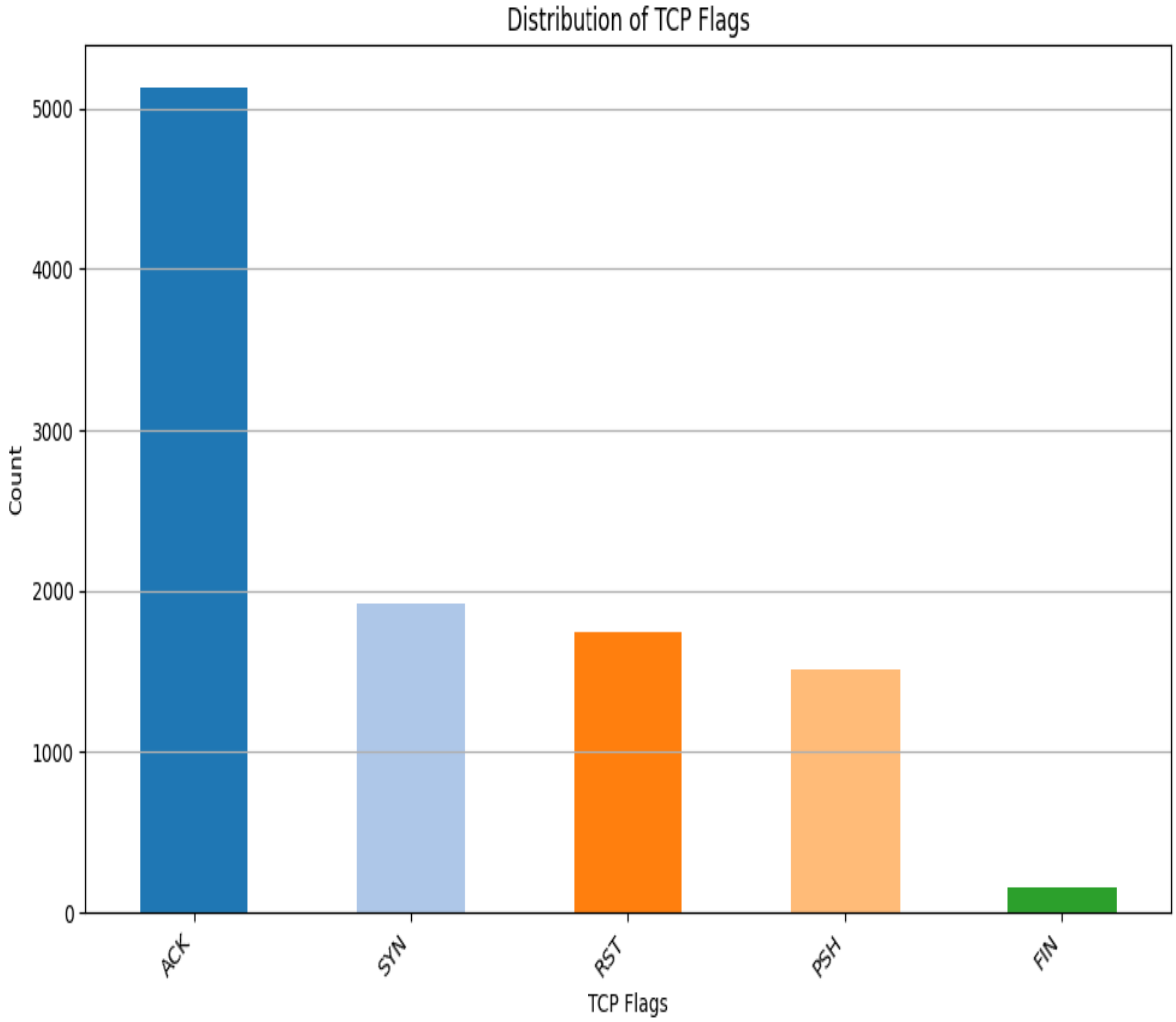
In conclusion, this report serves as a valuable resource for decision-makers, providing actionable insights and recommendations to enhance the network security posture and mitigate potential cyber risks.

10 most active IP addresses



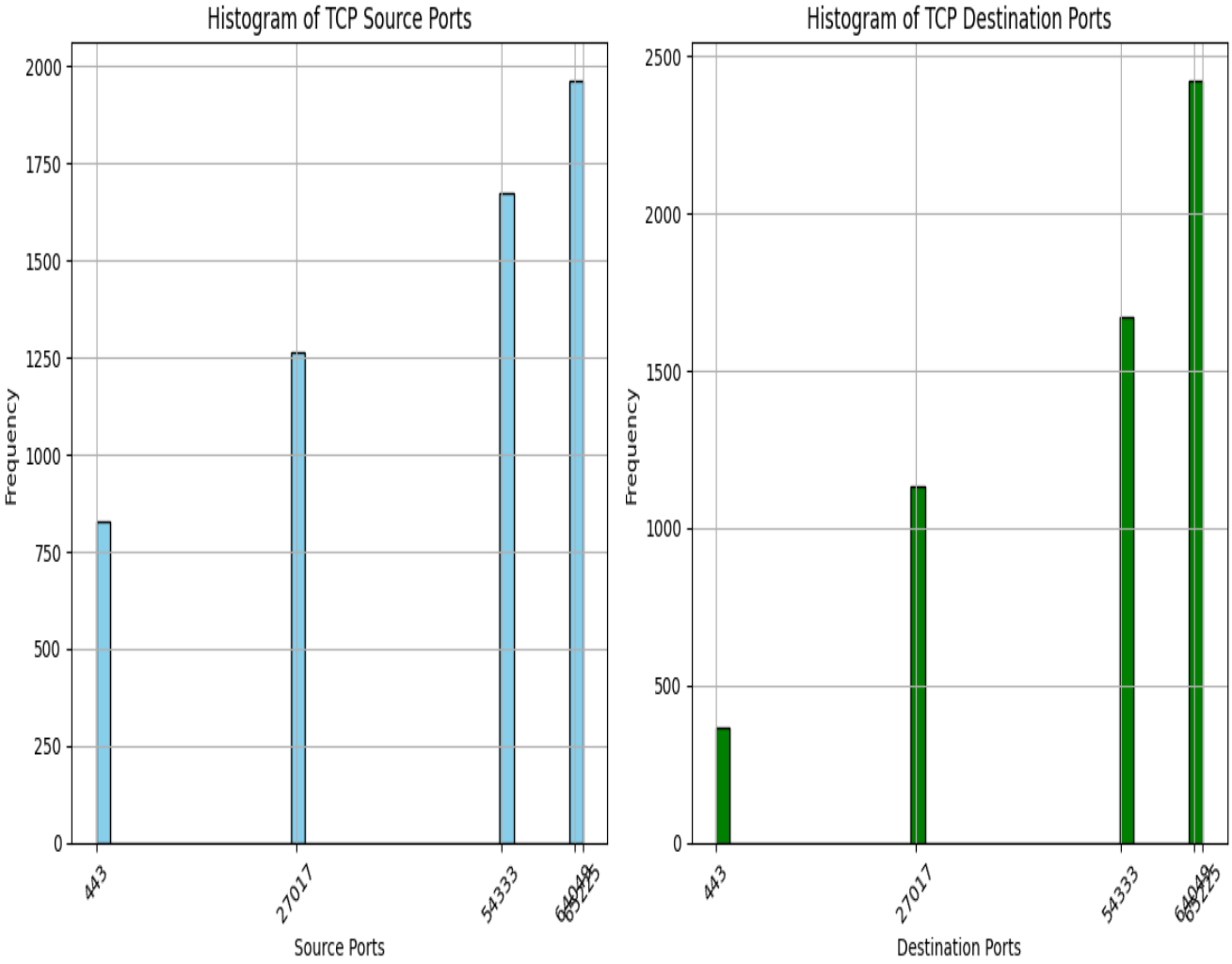
Identifying the top 10 IPs involves determining the IP addresses that are most frequently involved in network communication. These IPs may represent hosts that are generating significant amounts of traffic, communicating with a large number of other hosts, or exhibiting suspicious behavior that warrants further investigation.

TCP Flag Distribution Across Network



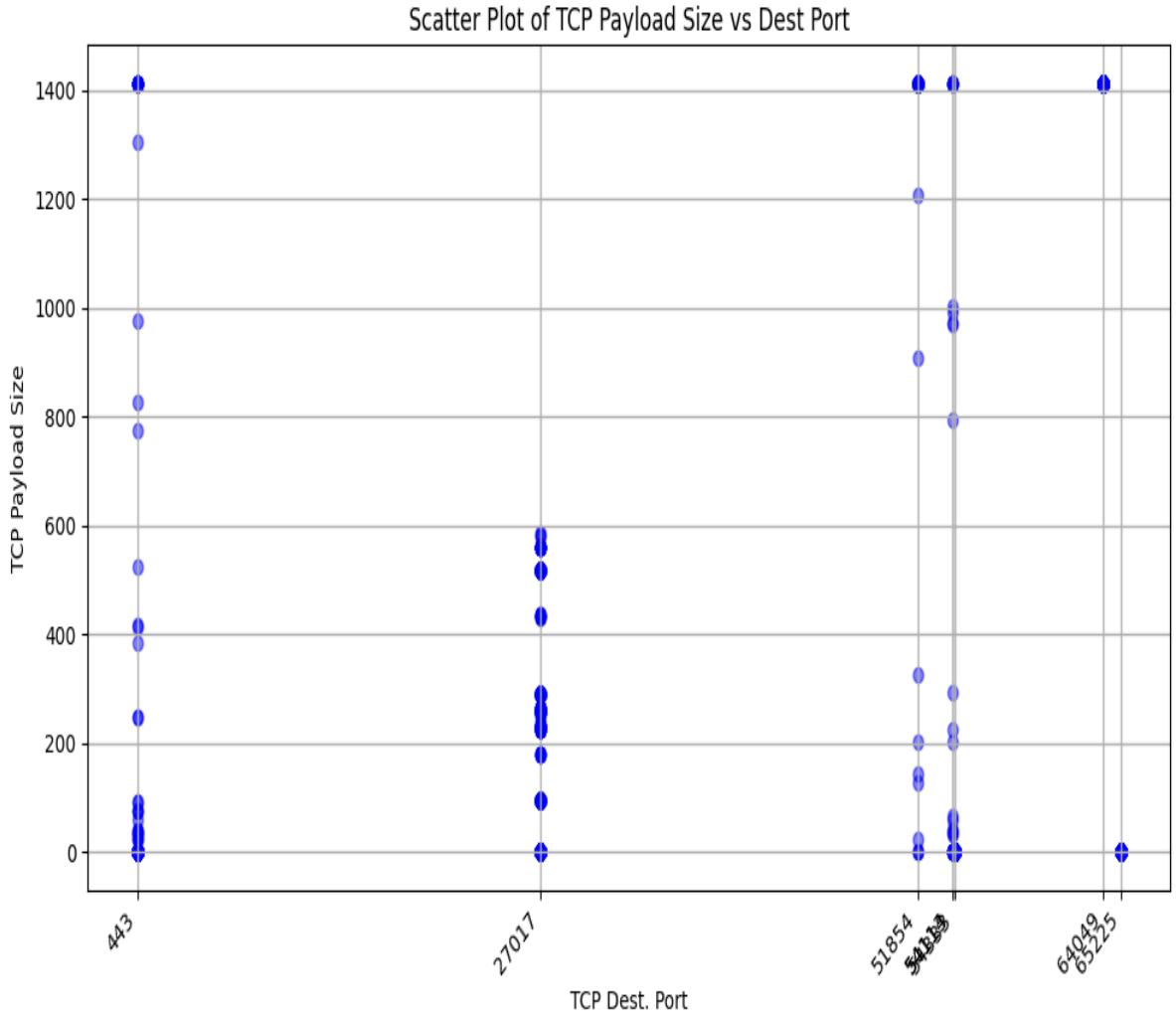
TCP flags represent control bits within the TCP header that control the state of a TCP connection. They include flags such as SYN (synchronize), ACK (acknowledge), FIN (finish), RST (reset), and others. Analyzing TCP flags provides insights into the nature of network traffic, including whether connections are being established, data is being acknowledged, or connections are being terminated abruptly.

TCP Top 5 Port Usage



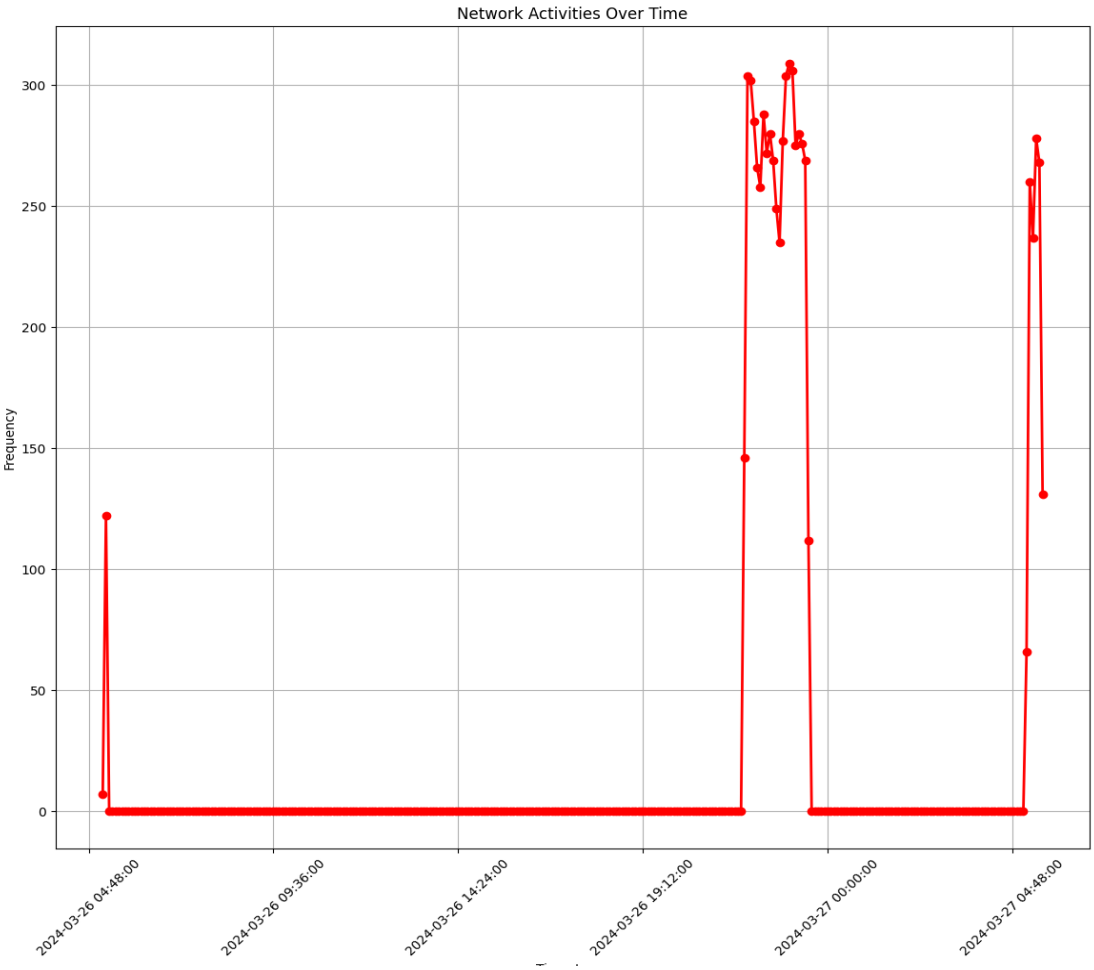
TCP ports are numerical identifiers associated with endpoints in a network communication. The source port is the port number used by the originating device, while the destination port is the port number used by the receiving device. Analyzing TCP destination and source ports helps identify the services and applications being used, as different services typically use specific port numbers.

TCP Payload Size variation wrt to Destination Port



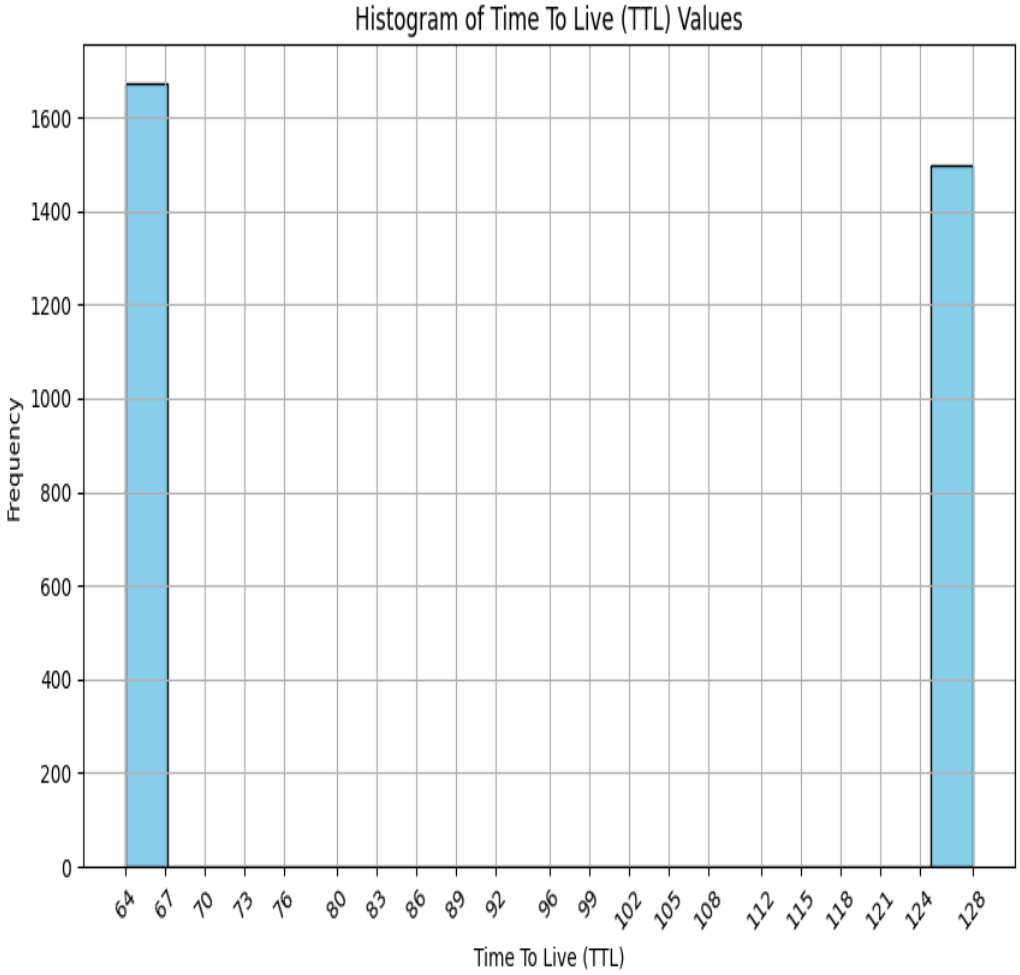
This comparison examines the size of TCP payloads in relation to the source ports from which the traffic originates. Understanding the relationship between payload size and source port can reveal patterns in network communication. For example, certain types of traffic may exhibit larger payloads or originate from specific source ports associated with particular services or applications.

Network Activities Over Time



This analysis provides a temporal view of network activities, showing how traffic patterns evolve over time. By monitoring network activities over time, security teams can detect anomalies, identify periods of high or low network utilization, and correlate events with specific time frames to understand network behavior comprehensively.

Histogram of Time To Live (TTL) Values



Time To Live (TTL) is a value in IP packet headers that determines the maximum number of hops (routers) a packet can traverse before being discarded. A histogram of TTL values provides insights into the network topology and routing characteristics. Analyzing TTL values can help identify misconfigurations, anomalies in routing paths, or potentially malicious traffic attempting to obfuscate its origin.

Source IP wrt Payload Analysis

Source IPs and total payload sent:

192.168.100.70: 166.58 MB

Dest IP wrt Payload Analysis

Destination IPs and total payload received:

192.168.100.1: 0 Bytes