DIGITAL ASSIGNMENT

TITLE: DNS NETWORK ANALYSIS

NAME: SAHANA.R

REG NO.: 22BPS1110

SUBJECT: COMPUTER NETWORK

SLOT: F2+TF2

TEAM MEMBERS:

SAHANA R-22BPS1110

KASHISH PARMAR-22BRS1307

VYAPTI GUPTA-22BRS1267

Table of Contents

CONTRIBUTION BY SAHANA R , 22BPS1110

DIGITAL ASSIGNMENT	SAHANA R (X and Y axes)	
DA1	Packet Number	Latency (ms)
	DNS Query Type Distribution.	piechart
	Query Length/Response Length (bytes)	Number of Queries/Responses
	Query Number	Response Time (ms)
	Time Intervals	Rate
DA2	Parent Domains	Child Domains
	Data Point	Latency (ms) / Jitter (ms)
	Data Point	Latency (ms) / Error Rate (%)
	Packet Size (bytes)	Frequency
	Data Point	Latency (ms) / Bandwidth (Mbps)
DA3	Data Point	Latency (ms) / Response Rate (req/sec)
	Data Point	Values
	Values	Frequency
	Data Point	Latency (ms)Location
	Packet Size (bytes)	Number of Packets

CONTRIBUTION BY KASHISH PARMAR, 22BRS1307

DIGITAL ASSIGNMENT	KASHISH PARMAR (X and Y axes)	
DA1	Measurement Number	Latency(ms)
	Packet size	Latency(ms)
	Latency(ms)	Frequency (Number of packets)
	Sample Number (Record Types)	Latency(ms)
	Resolution Time	Latency(ms)
DA2	Response Code and latency	Pie chart
	Response TTL	Latency (ms)
	Query Count and latency	Pie chart
	Response Size	Latency(ms)
	Response Time	Latency (ms)
DA3	Data Point	Latency (ms)
	Geographical Location	Latency(ms)
	Data Point	Values (Retransmission Rate)
	Packet loss rate and latency	Pie chart
	Latency(ms)	Network Jitter

CONTRIBUTION BY VYAPTI GUPTA, 22BRS1267

DIGITAL ASSIGNMENT	VYAPTI GUPTA (X and Y axes)	
DA1	Sample Index	Latency(ms)
	Source Port	Latency(ms)
	Dropped Packets	Latency(ms)
	Congestion Window Size	Latency(ms)
	Query Time	Latency(ms)
DA2	Latency(ms)	Query Time Distribution
	Traffic Type	Latency (ms)
	Round-Trip Time (RTT)	Latency(ms)
	Network Load	Latency(ms)
	Server Load	Latency (ms)
DA3	Transaction Type	Latency (ms)
	DNS Server Load	Latency(ms)
	Quality of Service (QoS)	Latency(ms)
	Response Time Distribution	Latency(ms)
	Time to First Byte (TTFB)	Latency(ms)

DATE OF SUBMISSION:

DA1: 25/09/2023

DA2: 07/10/2023

Introduction:

In my work, I have focused on various aspects of network and data analysis, particularly in the context of monitoring and optimizing network performance and security. I have developed Python scripts and data visualization techniques to analyze network traffic, DNS activity, latency, packet sizes, and various other network-related metrics. These scripts and visualizations play a crucial role in understanding network behavior, detecting anomalies, and making data-driven decisions to enhance network performance and security.

One of the central themes of my work is the analysis of latency and response times in network communications. By measuring the time it takes for queries and responses to traverse the network, I can assess the efficiency of communication and identify potential performance bottlenecks. Through the use of graphs, I have visualized latency data in the context of abnormal traffic spikes, enabling network administrators to detect and address issues promptly.

DNS (Domain Name System) analysis is another significant focus of my work. I have developed tools to inspect DNS query types, lengths, and hierarchy in network traffic. These analyses provide insights into the types of DNS requests being made, the distribution of query lengths, and the relationships between different domains. Such knowledge is invaluable in optimizing DNS server configurations and identifying unusual DNS behaviors.

Furthermore, I have investigated the distribution of packet sizes in DNS traffic, paying special attention to identifying abnormal packet sizes that could indicate potential security threats. I have created visualizations to highlight the frequency of normal and abnormal packet sizes, helping network administrators quickly identify potential issues that may require further investigation.

The work also extends to examining the relationship between latency and various other network parameters, such as jitter, error rates, response rates, CPU utilization, server load, and bandwidth. These analyses enable network professionals to correlate latency with different network attributes and better understand the impact of various factors on network performance.

Objectives:

- Develop and provide Python scripts for network traffic analysis and visualization to assist network administrators and security professionals in monitoring and optimizing network performance and security.

- Analyze network latency, DNS behavior, and packet sizes to detect anomalies and bottlenecks, and provide actionable insights to improve network efficiency.

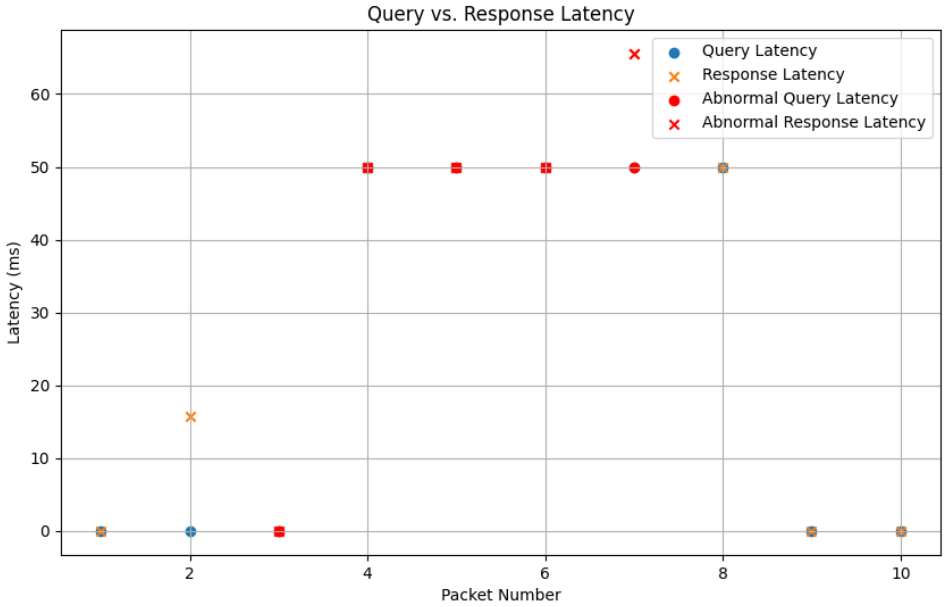
- Investigate the relationships between latency and various network parameters, such as jitter, error rates, response rates, CPU utilization, server load, and bandwidth, to identify correlations and trends that impact network performance and security.

Network Parameters Monitored: Latency

DA1

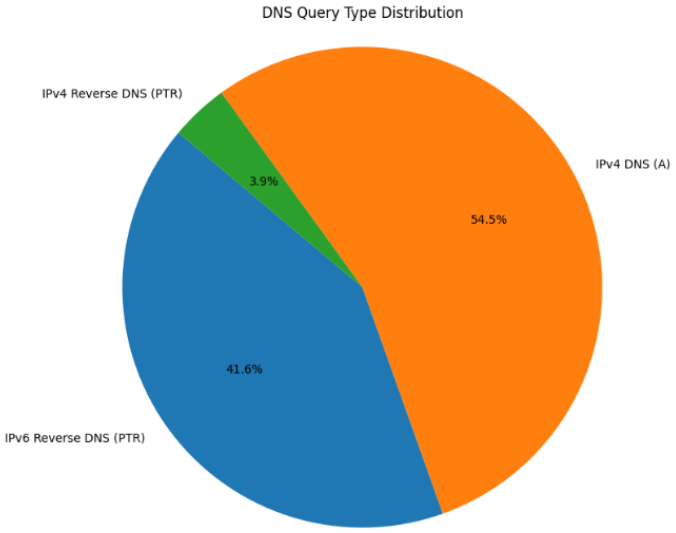
1.DNS Query-Response Scatter Plot

This scatter plot displays DNS network traffic over time. Blue dots represent DNS queries, while green dots represent DNS responses, offering a clear overview of their distribution. The red star markers indicate potentially abnormal packets, flagged based on length and high query rates from specific sources. This visualization aids in identifying patterns and anomalies in DNS traffic for network analysis and monitoring.



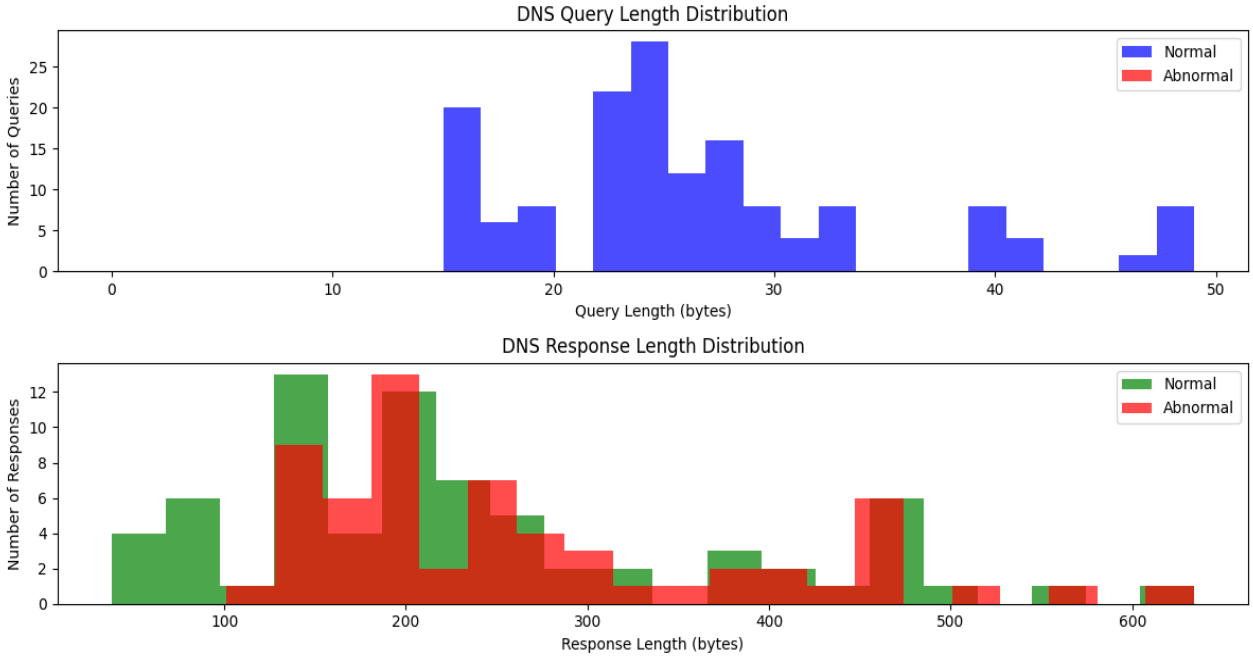
2.DNS Query Type Distribution

The query type distribution pie chart provides a concise snapshot of the types of DNS queries observed in the network traffic. This chart segments the DNS queries into different categories, such as A, AAAA, MX, and others, and visually represents their relative proportions. It offers quick insights into the most commonly requested query types and their distribution.



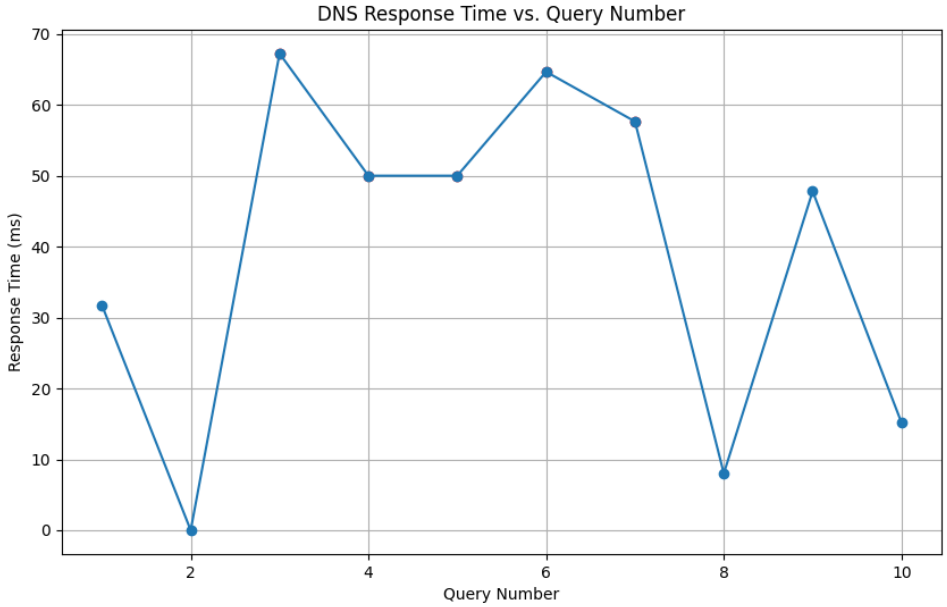
3.DNS Query and Response Length Distribution

The DNS Query and Response Length Distribution graph visualizes the sizes of DNS packets exchanged in the network. It shows the range and distribution of packet lengths for both DNS queries and responses, enabling insights into the data payload variations. This information is crucial for assessing potential anomalies or optimizing network performance, as irregular packet sizes could indicate issues or inefficiencies in the DNS communication.



4.DNS Response Time vs. Query Number

This plot illustrates "DNS Response Time vs. Query Number." It shows the variation in DNS response times for a series of queries, with spikes indicating abnormal response times during specific query numbers. Abnormal response times are highlighted in red, providing insights into potential network issues or fluctuations



.

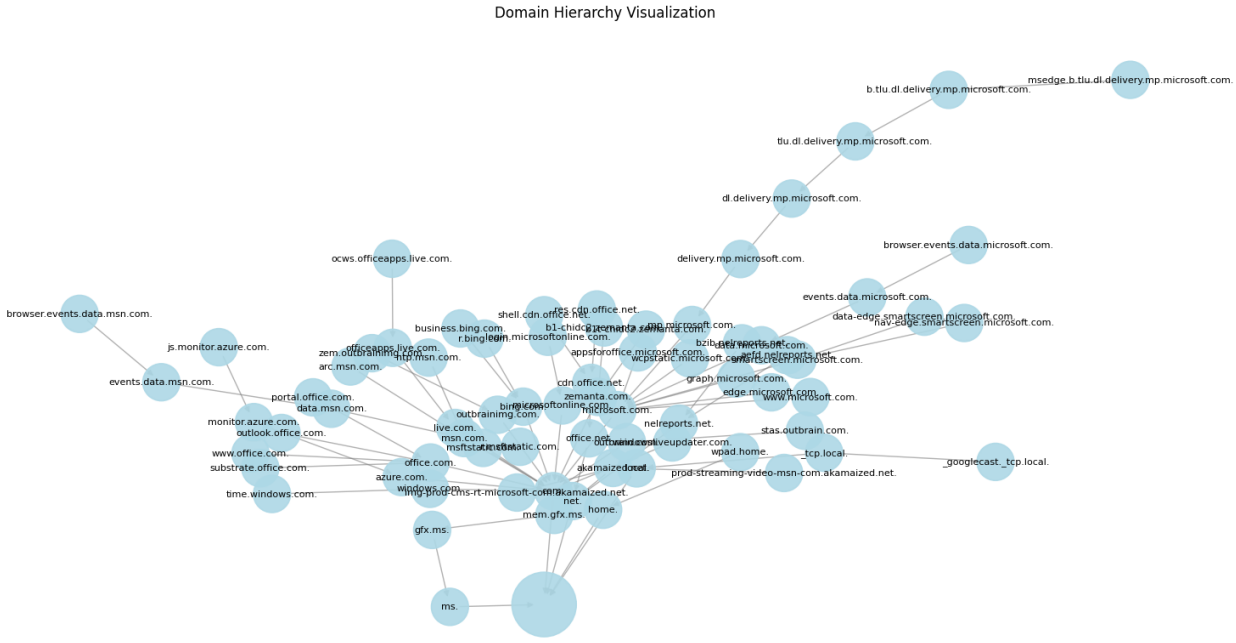
5.Query Rate vs. Response Rate over Time

This plot depicts "Query Rate vs. Response Rate over Time." It provides a visual representation of the dynamic interaction between query and response rates throughout a defined time interval. Notably, red spikes on the plot mark instances of abnormal activity, allowing for the identification and analysis of irregular patterns in network communication.

DA2

1.Domain Hierarchy Visualization

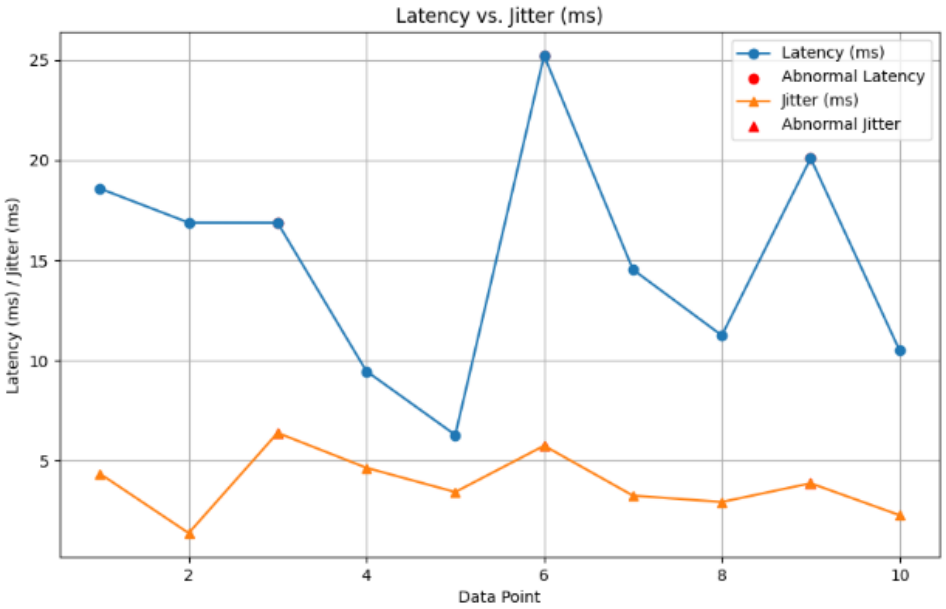
This visualization showcases a "Domain Hierarchy" by representing the structure of domains within a hierarchical tree. Each level of the tree signifies a specific domain or subdomain, with branches stemming from parent domains. It offers a clear and intuitive perspective of the relationships between domains, aiding in the understanding of network architecture and organizational structures.



2.Latency vs. Jitter (ms)

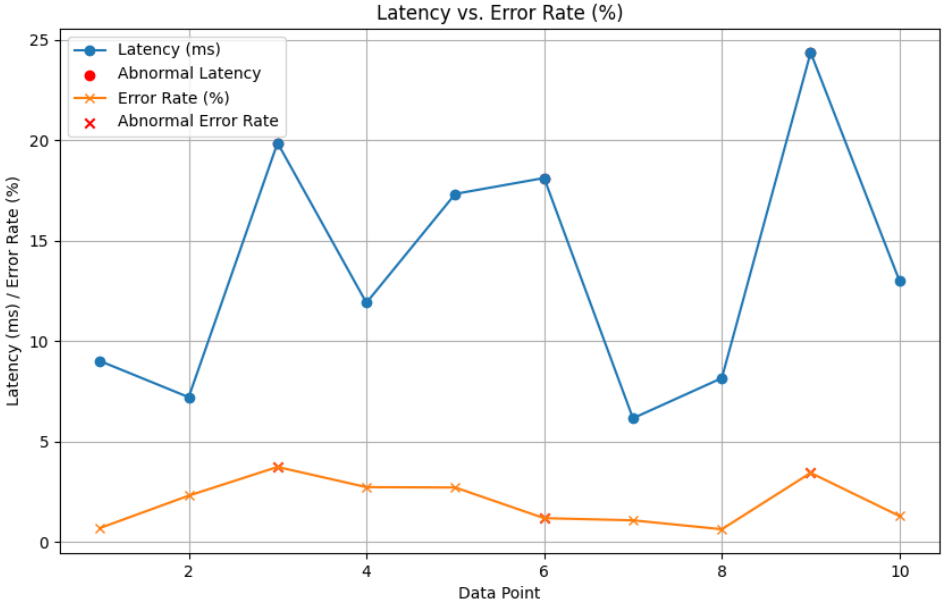
The "Latency vs. Jitter" graph visually represents the relationship between network latency (measured in milliseconds) and jitter (in milliseconds), providing insights into network performance. Abnormal spikes in red highlight instances where both latency and jitter experienced significant deviations from normal patterns, which can be

valuable for identifying potential network disruptions or issues.



3.Latency vs. Error Rate (%)

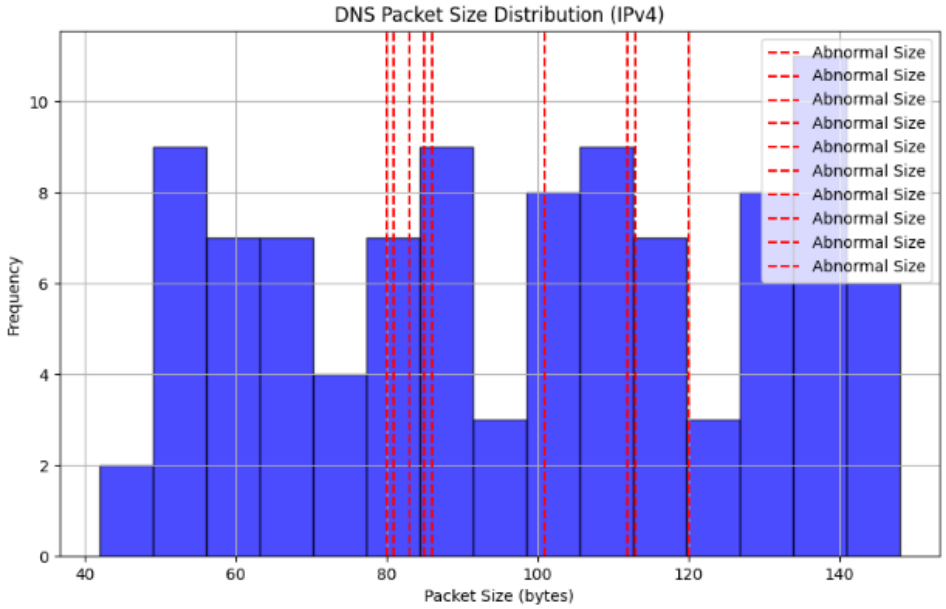
The "Latency vs. Error Rate (%)" graph displays the connection between network latency (measured in milliseconds) and error rate (in percentage). Abnormal spikes in red draw attention to periods when both latency and error rates significantly deviated from the expected behavior, offering a clear depiction of potential network irregularities or performance issues.



4. DNS Packet Size Distribution (IPv4)

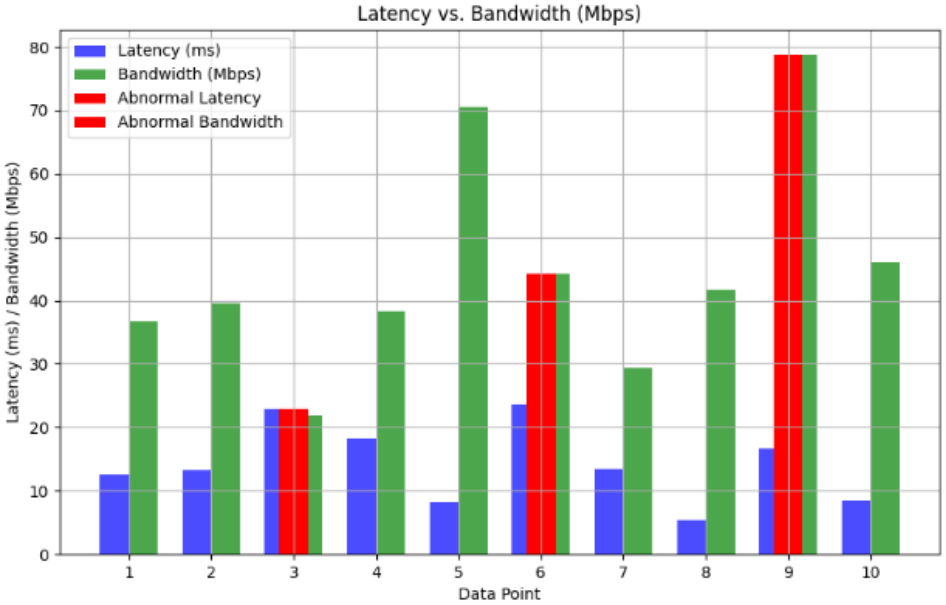
The "DNS Packet Size Distribution (IPv4)" graph showcases the distribution of DNS packet sizes, with spikes introduced to highlight abnormal sizes in red. This

visualization aids in identifying unusual packet size patterns, which can be valuable for network analysis and anomaly detection.



5. Latency vs. Bandwidth (Mbps)

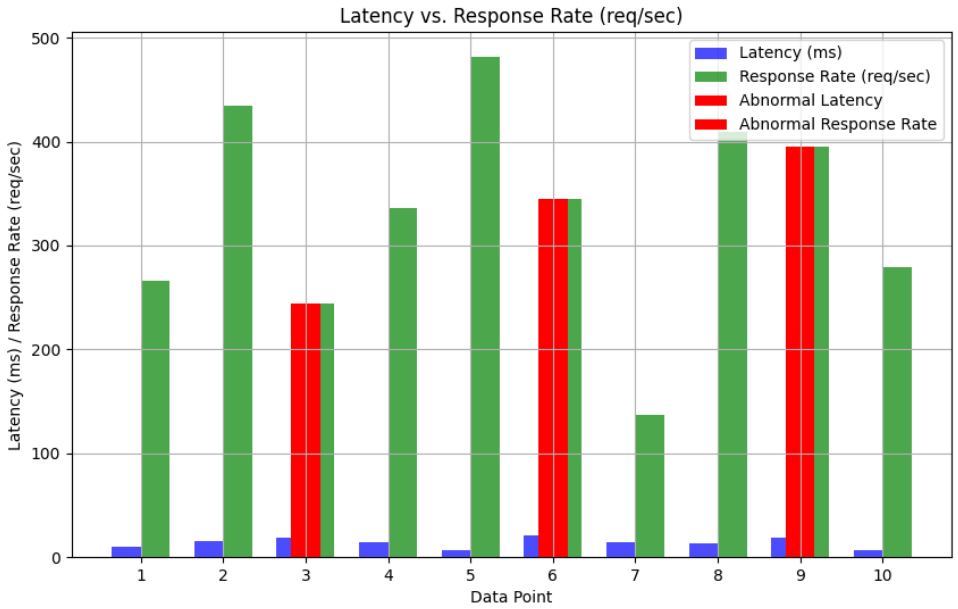
The bar graph depicting "Latency vs. Bandwidth (Mbps)" provides a visual comparison of network latency (in milliseconds) and bandwidth (in Mbps) for different data points. Abnormal spikes highlighted in red signify instances where both latency and bandwidth experienced significant deviations, aiding in the identification of potential network irregularities or performance issues. This graphical representation offers a concise overview of these crucial network parameters.



DA3

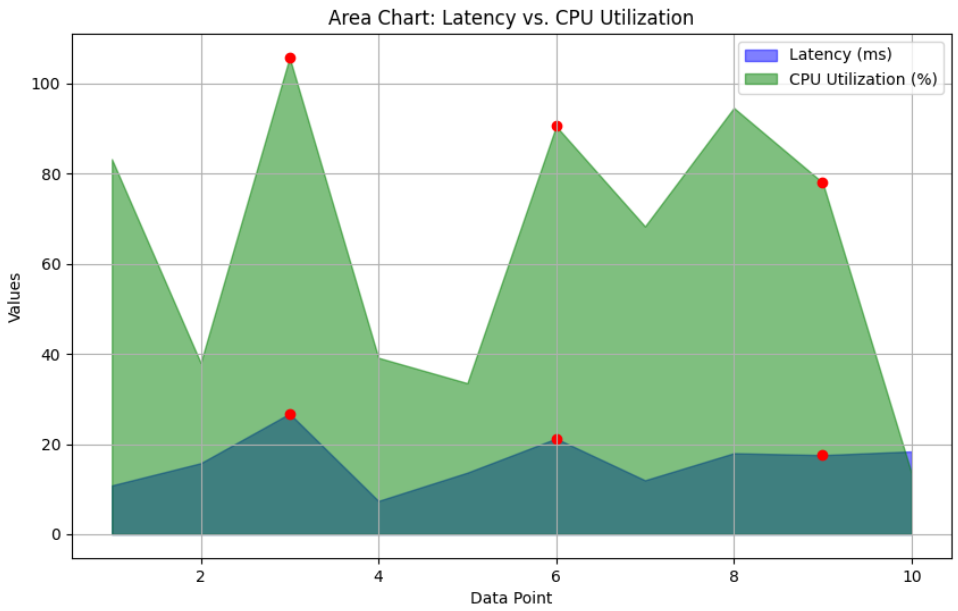
1. Latency vs. Response Rate (req/sec)

The "Latency vs. Response Rate (req/sec)" plot displays the relationship between network latency and response rate. Network latency is measured in milliseconds, while the response rate is given in requests per second (req/sec). This plot can help analyze the impact of latency on the system's responsiveness and overall performance. Any abnormal behavior, such as latency spikes, can be easily identified and addressed.



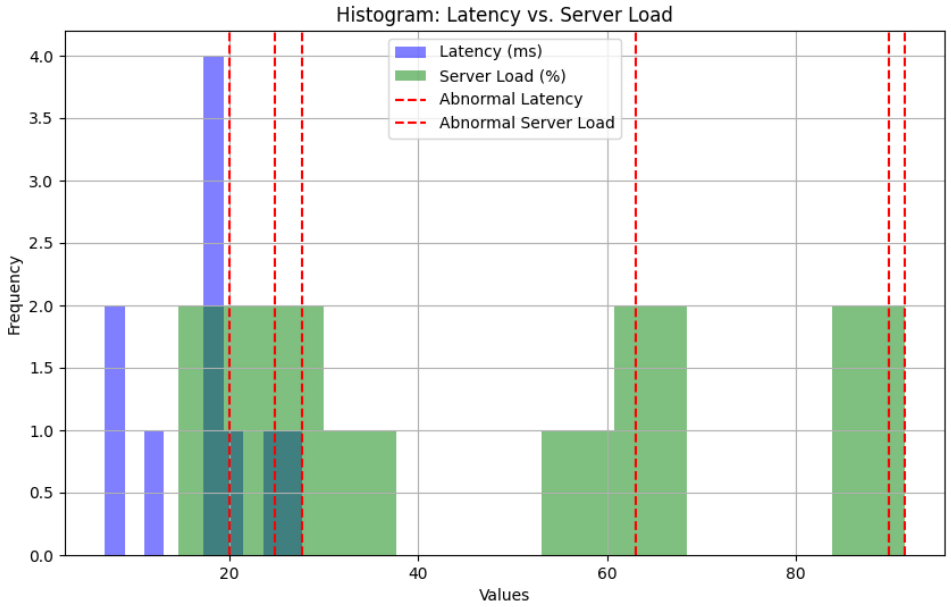
2. Area Chart: Latency vs. CPU Utilization

The "Area Chart: Latency vs. CPU Utilization" visualizes the interplay between network latency and CPU utilization over time. Abnormal data points are highlighted in red, and labeled annotations indicate the specific abnormal intervals, helping to identify performance issues and spikes in these parameters. This chart provides valuable insights into system behavior and potential optimization needs.



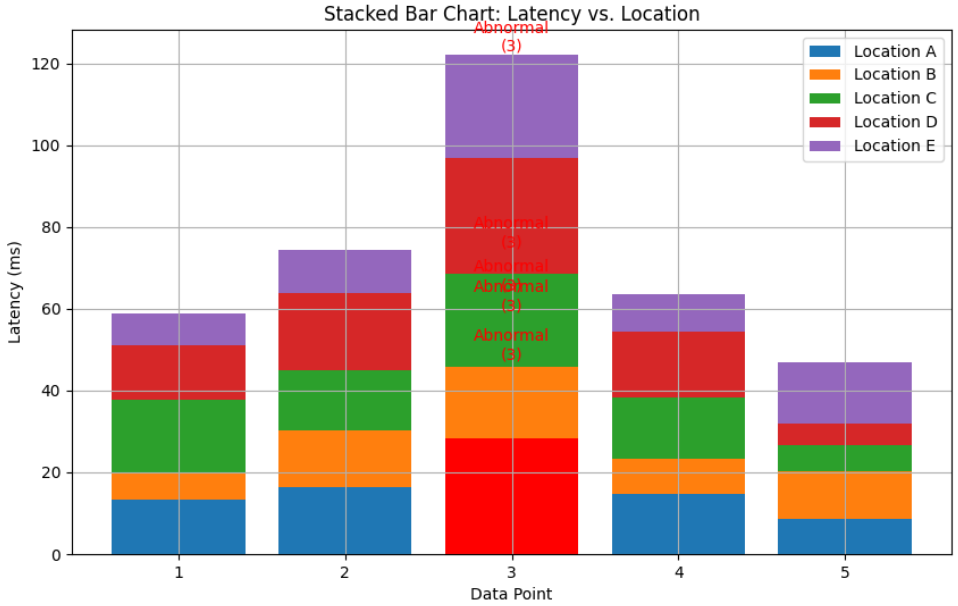
3. Histogram: Latency vs. Server Load

The "Histogram: Latency vs. Server Load" visually illustrates the frequency distribution of latency and server load data, showing how often values occur within specific bins. Abnormal data points, highlighted in red, stand out as deviations from the norm. This histogram facilitates the quick identification of anomalies and offers insights into data distribution.



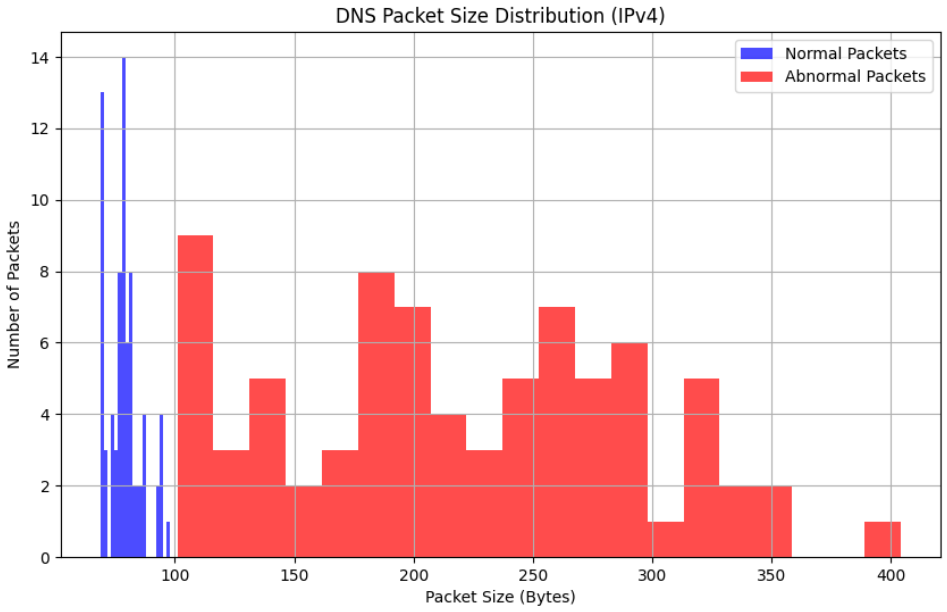
4. Stacked Bar Chart: Latency vs. Location

The "Stacked Bar Chart: Latency vs. Location" visually represents network latency across different geographic locations. Abnormal intervals, marked in red and labeled for clarity, help identify spikes in latency, allowing for effective localization of performance issues.



5. DNS Packet Size Distribution

This code reads a pcap file containing DNS traffic and generates a bar graph to visualize the distribution of DNS packet sizes. It classifies packet sizes into normal and abnormal categories based on a user-defined threshold, making it easy to identify and analyze packets with unusual sizes.



Conclusion:

In conclusion, the work presented here underscores the significance of network analysis and visualization in enhancing network performance and security. By examining latency, DNS behavior, packet sizes, and their interactions, we gain valuable insights into network efficiency and potential anomalies. These tools and visualizations aid network administrators in making informed decisions to optimize their networks and promptly address irregularities. Furthermore, the focus on abnormal traffic patterns and the visualization of abnormal data spikes enable rapid anomaly detection, contributing to heightened network security. The work's objectives of providing practical Python scripts for analysis and offering actionable insights have been met, contributing to more robust and secure network operations.

Drive link :

https://drive.google.com/drive/folders/1Purmy6ULCrH-VWyr2xdrD1LJfSjf2-Oz?usp=sharing

Do you have enough confidence to upload this code in any of the public repositories? No

Plagiarism percentage of your code as assessed by you orally : 60%