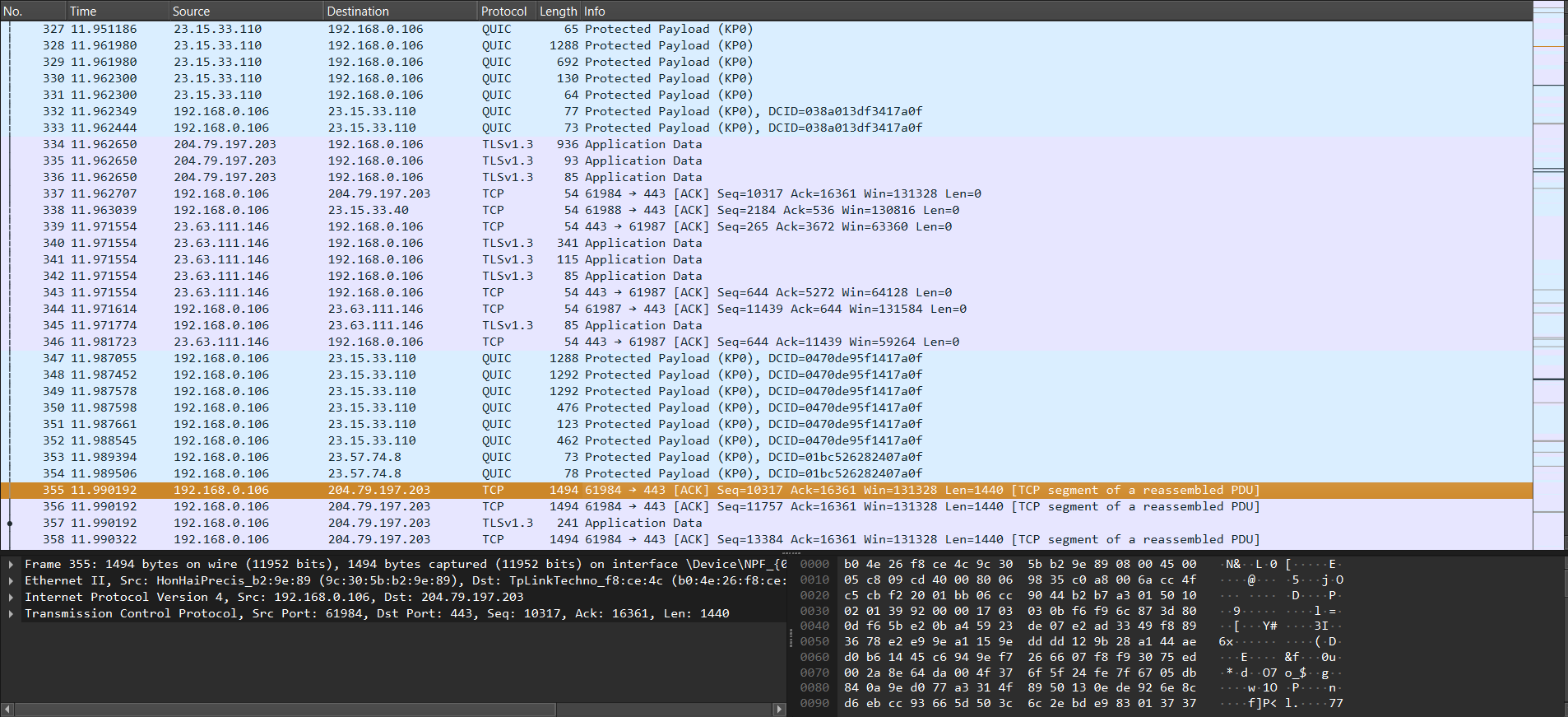
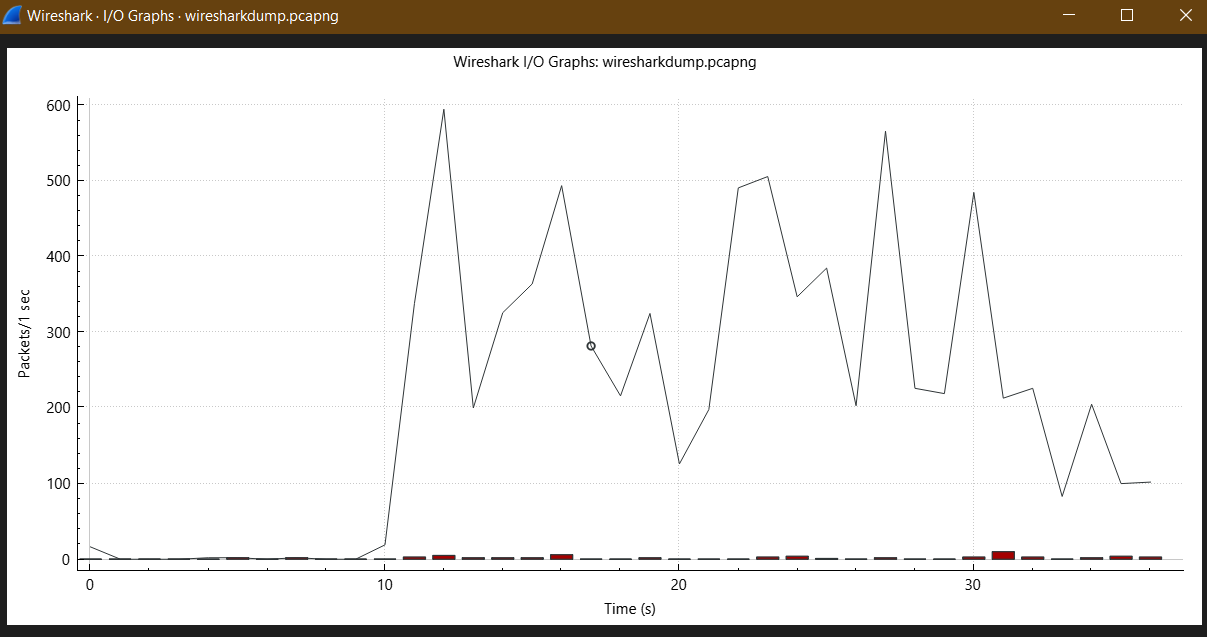
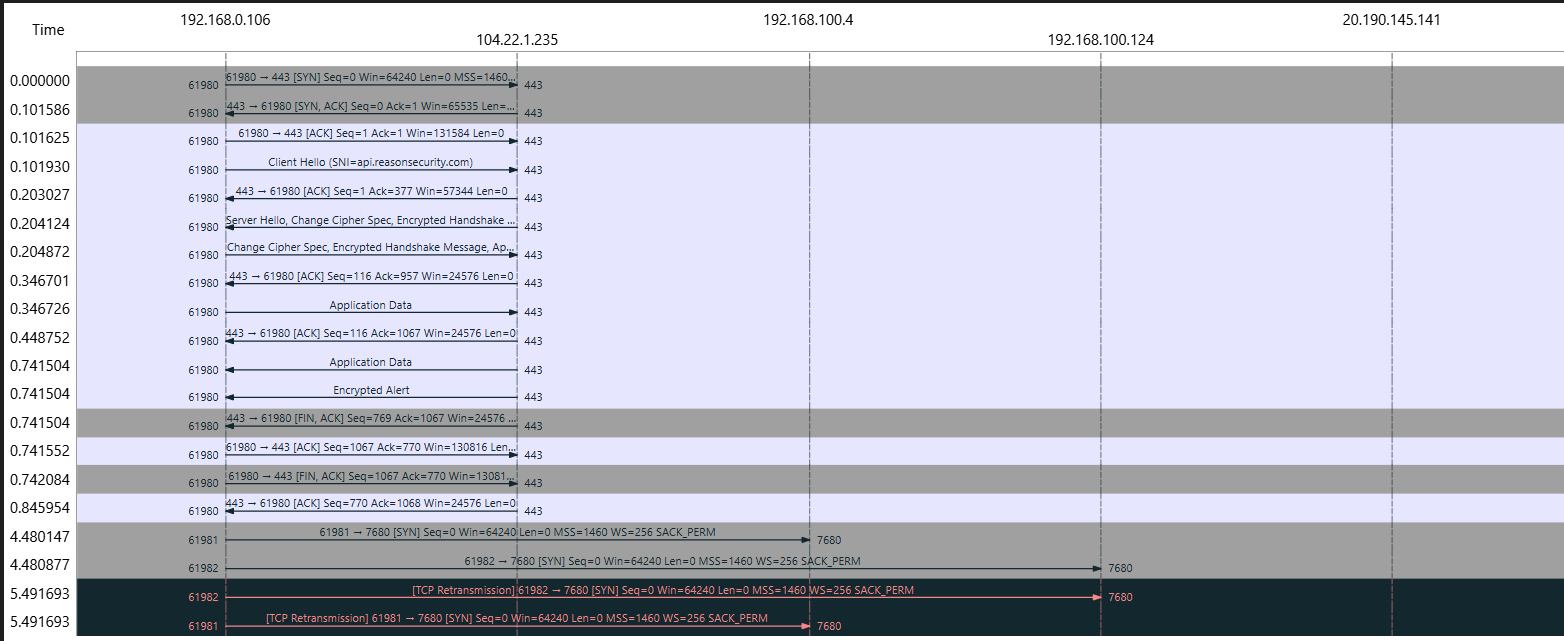
Task 3: Wireshark Analysis and Firewall

Analysis of provided Wireshark Dump

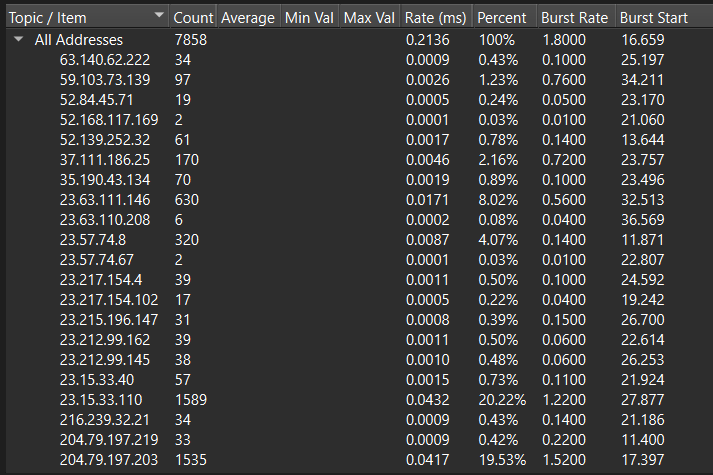
Following is the Wireshark dump  


Graphical Representation  


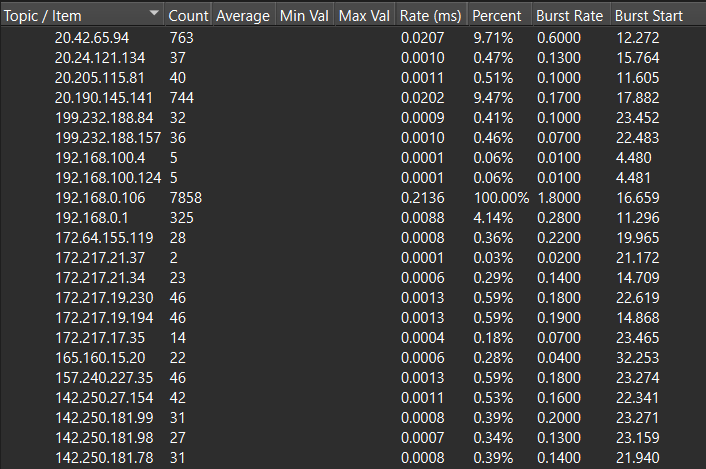
The following graph shows the flow of packets between endpoints over time. This time is from 0-30 seconds. The following graph shows a transfer of 600 packets from 0-10 seconds. However, from 10-20 second there is a difference in flow of packets. The graph helps in visualization of sequence of packets, which is a representation of various IP addresses. Moreover, it helps in the identification of sequences and unusual patterns

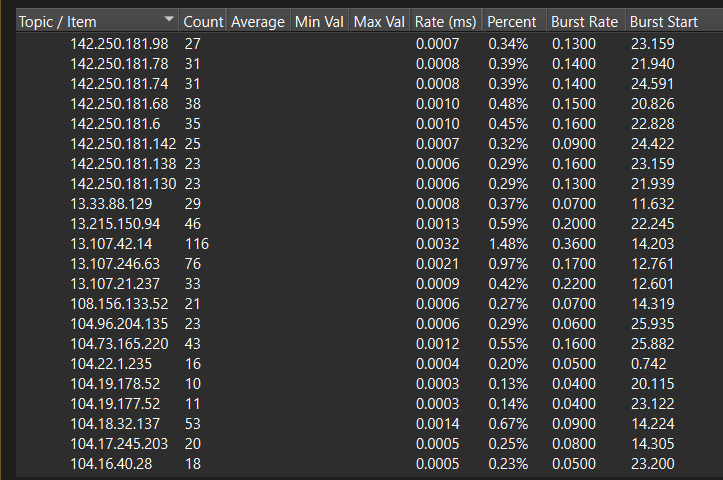
Wireshark Flow Graph  


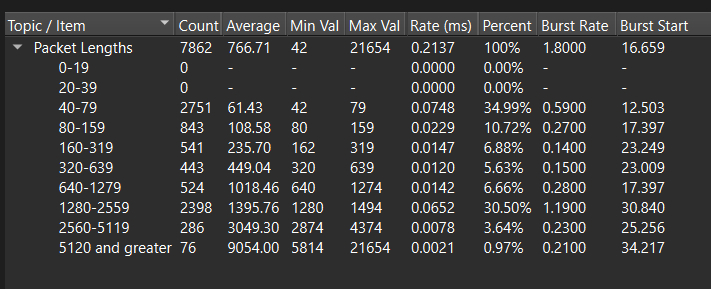
Following is the number of addresses in Wireshark Dump. There is a total number of 443 addresses in 104.22.1.235, which is under 192.168.0.106.



There is a total number of 7858 addresses, out of which, there is a total number of 34 addresses of 63.140.62.222. There are 97 addresses of 59.103.73.139. The least number of addresses is 2 for 23.57.74.67 and 52.168.117.169.





Following is the length of packets. In case of packet lengths 0-19, there is a count of 0. In context of 40-79 there is a total count of 2751.   


Following are the firewall rules

* Firewall Rules and Descriptions

General Rules

1. Default Deny All:

- Rule: `DROP all`

- Description: Deny all incoming traffic by default to minimize exposure.

2. Allow Established Connections:

- Rule: `PERMIT established`

- Description: Allow established and related traffic to maintain ongoing connections.

Specific Rules Based on Analysis

1. Permit Essential Services:

- HTTP:

- Rule: `PERMIT tcp any any eq 80`

- Description: Allow HTTP traffic.

- HTTPS:

- Rule: `PERMIT tcp any any eq 443`

- Description: Allow HTTPS traffic.

- DNS:

- Rule: `PERMIT udp any any eq 53`

- Description: Allow DNS traffic.

2. Drop Malicious or Unnecessary Ports:

- NetBIOS and SMB:

- Rule: `DROP tcp any any eq 135`

- Rule: `DROP tcp any any eq 139`

- Rule: `DROP tcp any any eq 445`

- Description: Block commonly exploited ports.

3. Restrict High-Risk Ports:

- Rule: `DROP tcp any any range 1024 65535`

- Description: Block high-numbered ports to prevent unauthorized access.

4. Log Suspicious Traffic:

- Large Packets:

-Rule: `LOG ip any any gt 1500`

- Description: Log packets larger than 1500 bytes for further analysis.

5. Permit Internal Traffic:

- Rule: ‘PERMIT ip 192.168.0.0 0.0.255.255`

- Description: Allow all internal network traffic within the organization's IP range.