Notebook

December 26, 2024

1 Wireshark Analysis

[1]:
```
import sys
sys.path.append('..')

import pandas as pd
from scripts.analyze import data_analysis
```

1.1 Retrieve the Data

Import the data using Pandas. Display the resulting DataFrame to confirm the import was successful.

[2]:
```
# Import the data
data = pd.read_csv('../data/capture.csv', on_bad_lines='skip')
data.head()
```

[2]:

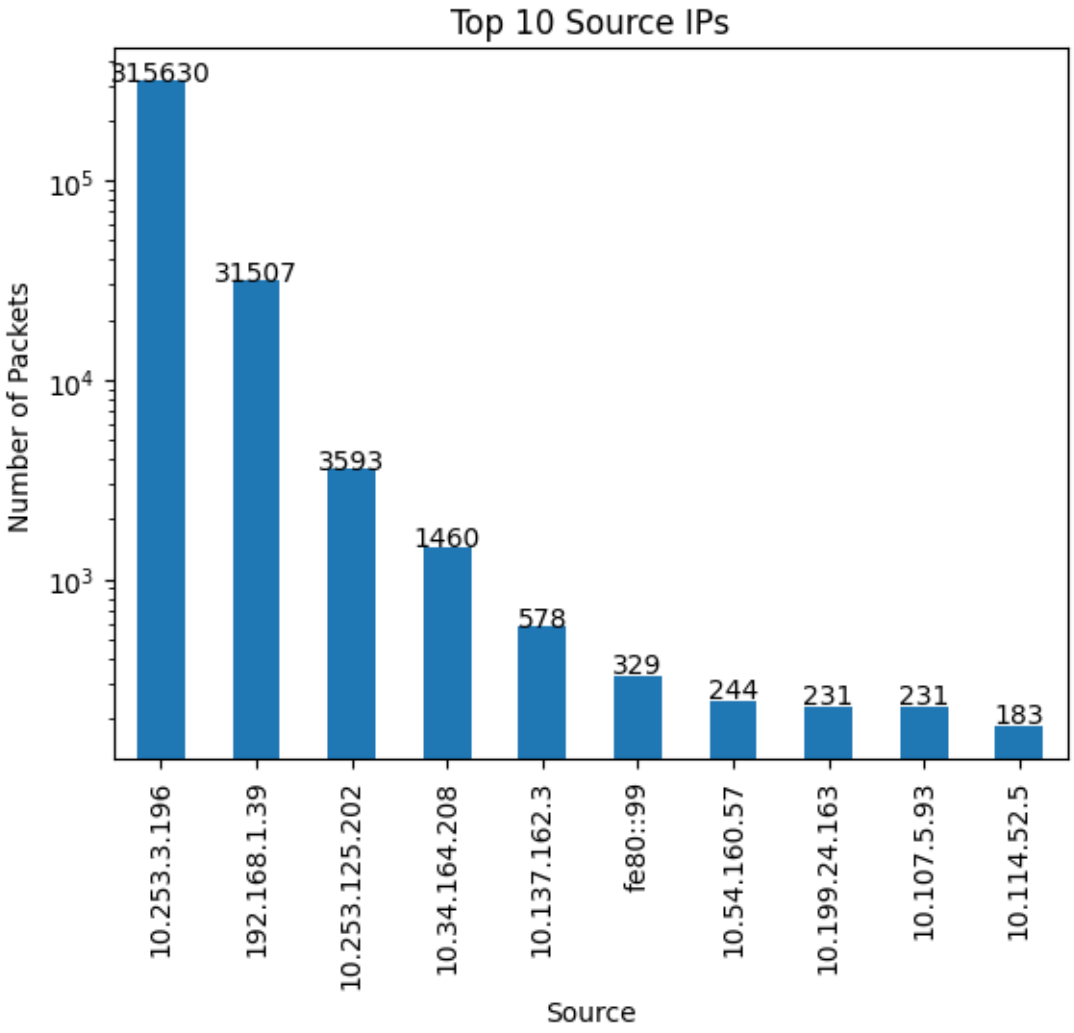
	Time	Source	Destination	Protocol	Length	Info
0	0.000000	192.168.1.39	10.248.228.70	TLSv1.2	635	Application Data
1	0.000279	192.168.1.39	10.248.228.70	TLSv1.2	165	Application Data
2	0.017569	10.248.228.70	192.168.1.39	TCP	66	443 > 58736 [ACK] Seq=1 Ack=669 Win=63 Len=0 T…
3	0.017570	10.248.228.70	192.168.1.39	TCP	1514	443 > 58736 [ACK] Seq=1 Ack=669 Win=63 Len=144…
4	0.017644	192.168.1.39	10.248.228.70	TCP	66	58736 > 443 [ACK] Seq=669 Ack=1449 Win=2025 Le…

[3]:
```
data_analysis(data)
```

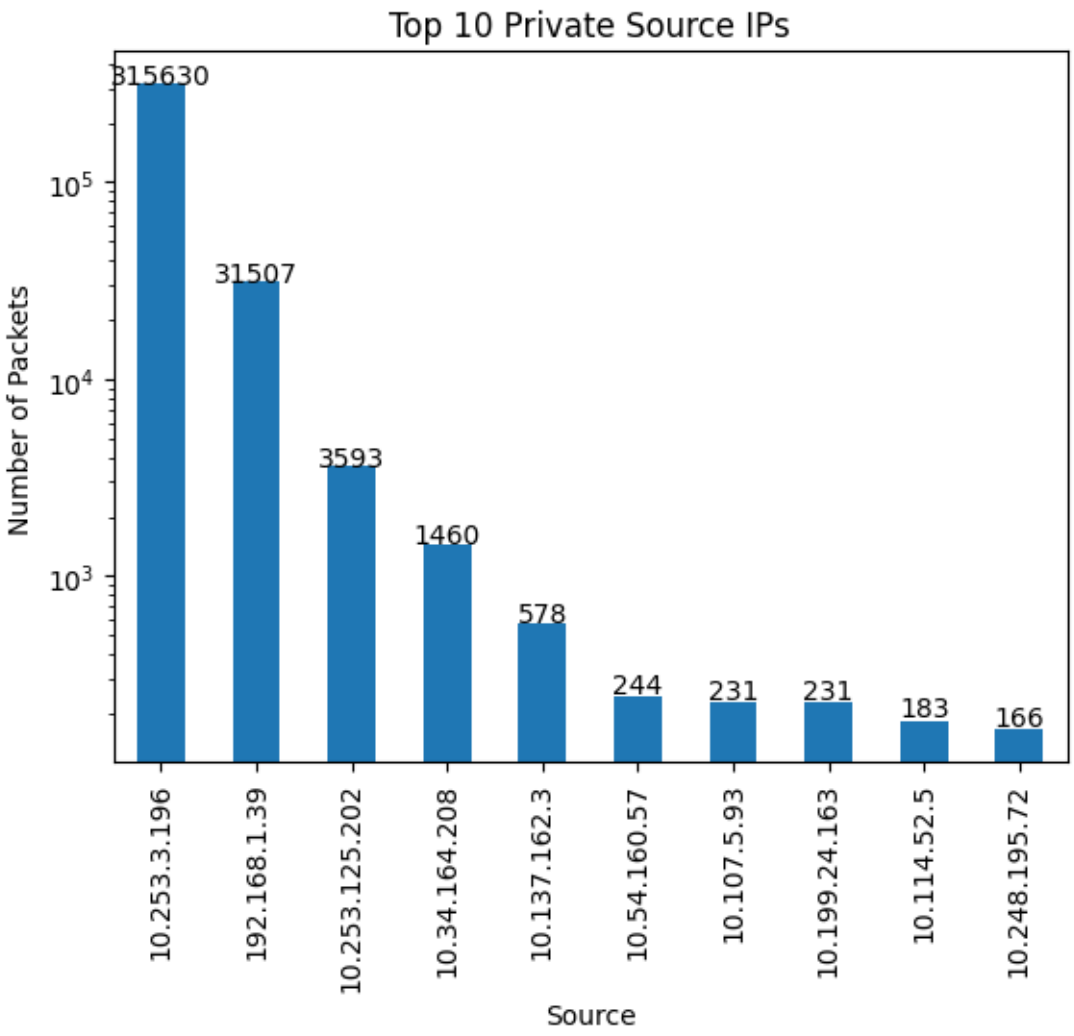
```
Data Preprocessing
========================================
There are no missing values in the dataset
The dataset has 358312 rows and 6 columns after deleting rows with missing
values
```

Source Analysis
==========

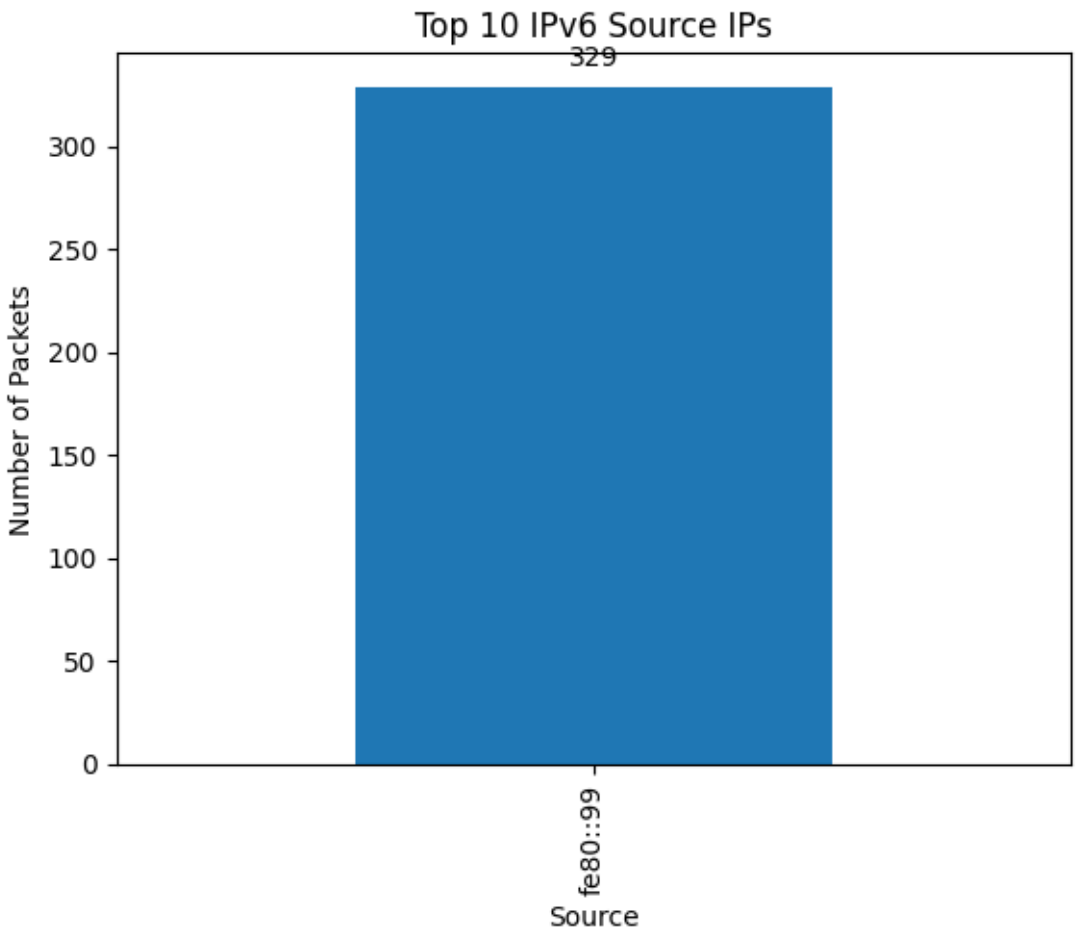
Source Analysis for All Addresses



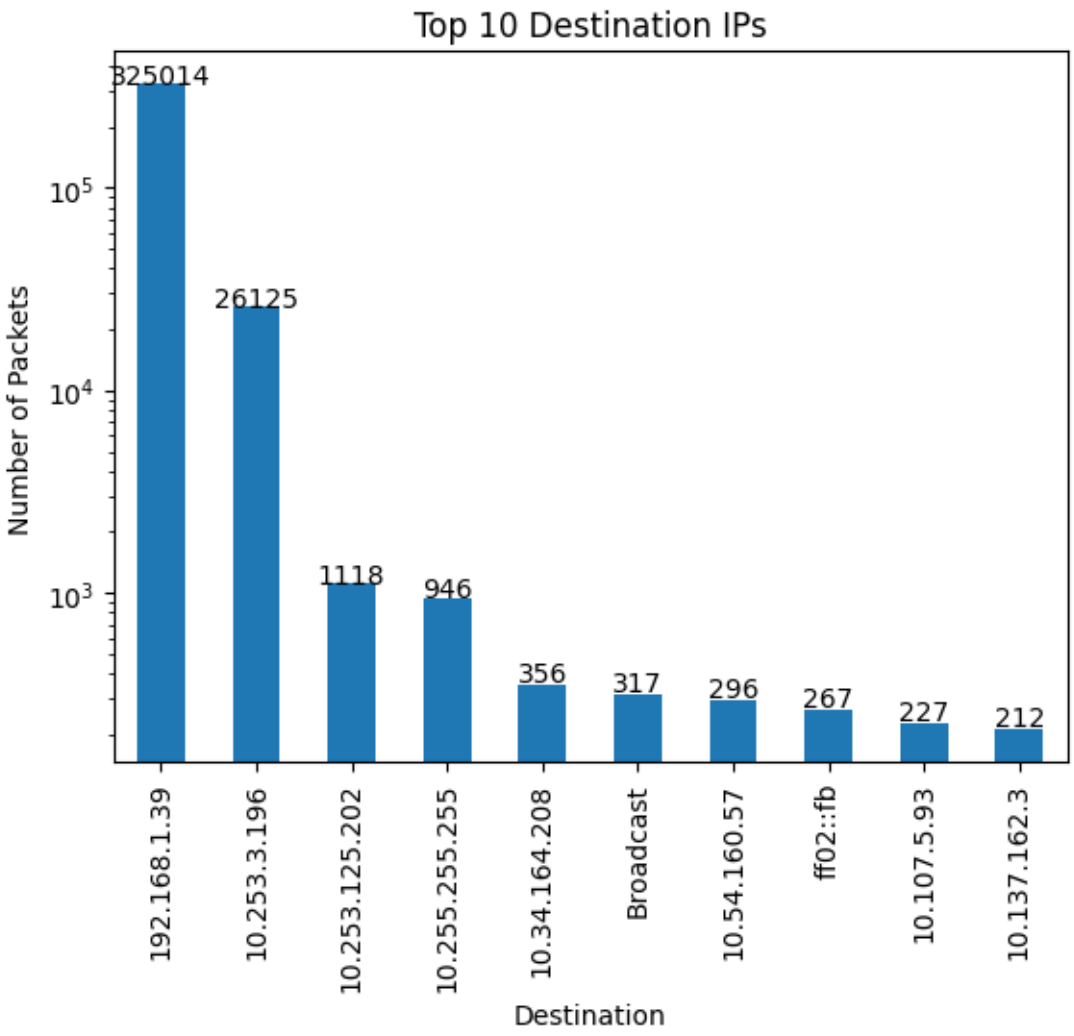
Source Analysis for Private Addresses



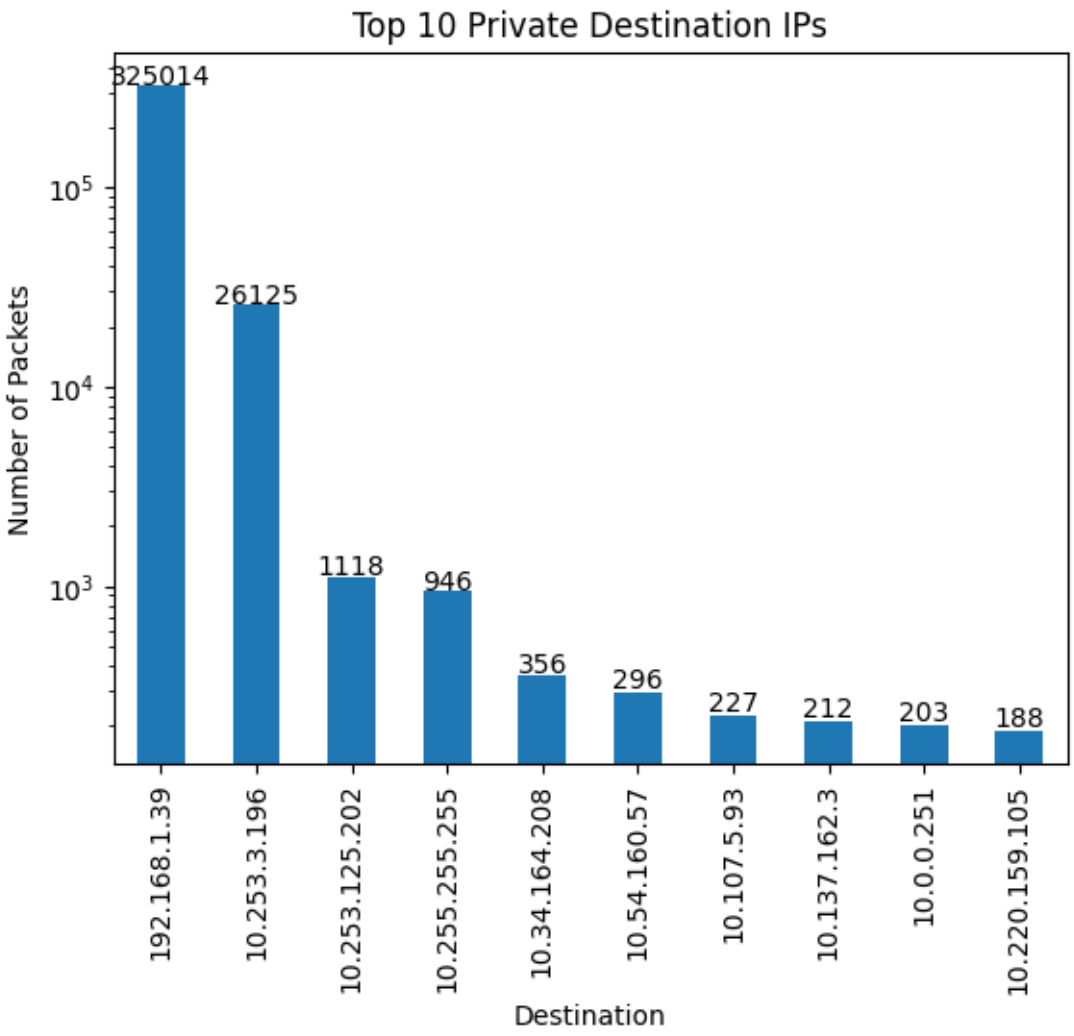

```
Source Analysis for Public Addresses
The dataset does not have Public Source IPs
Source Analysis for IPv6 Addresses
```



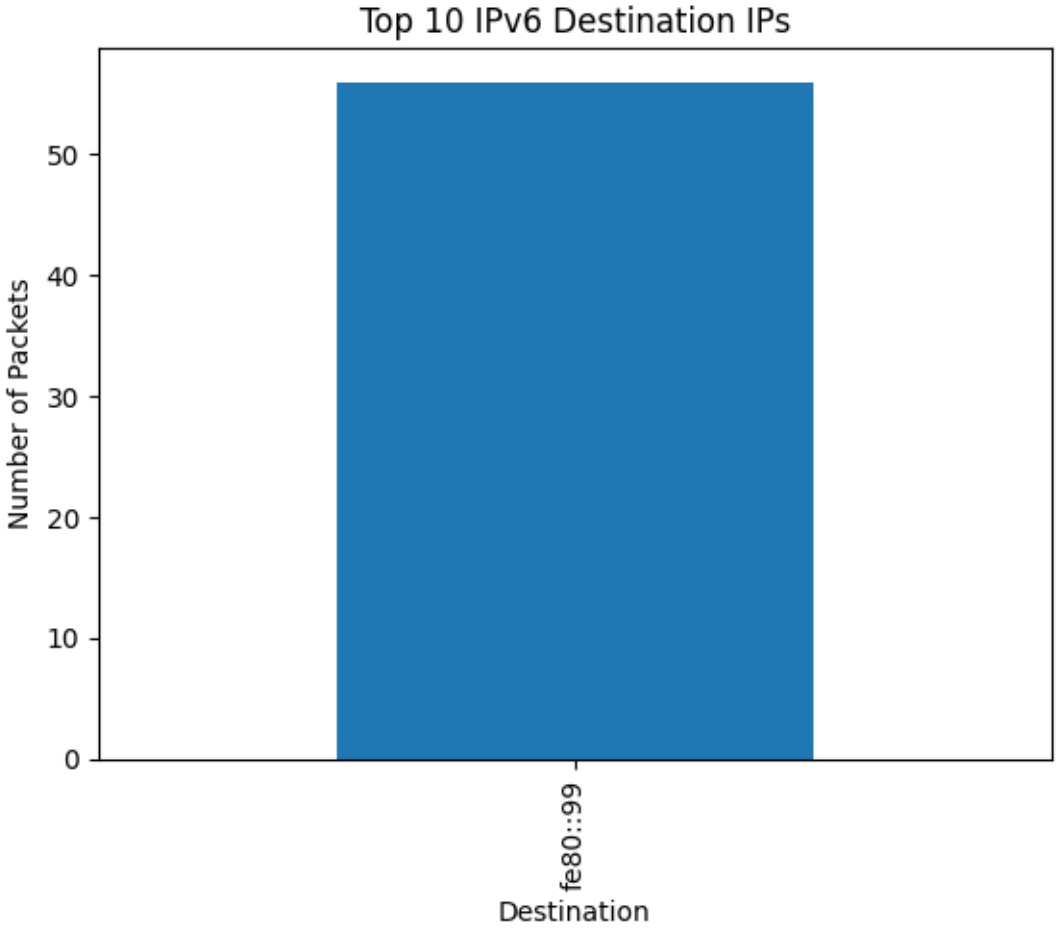

```
Destination Analysis
=====================================

Destination Analysis for All Addresses
```



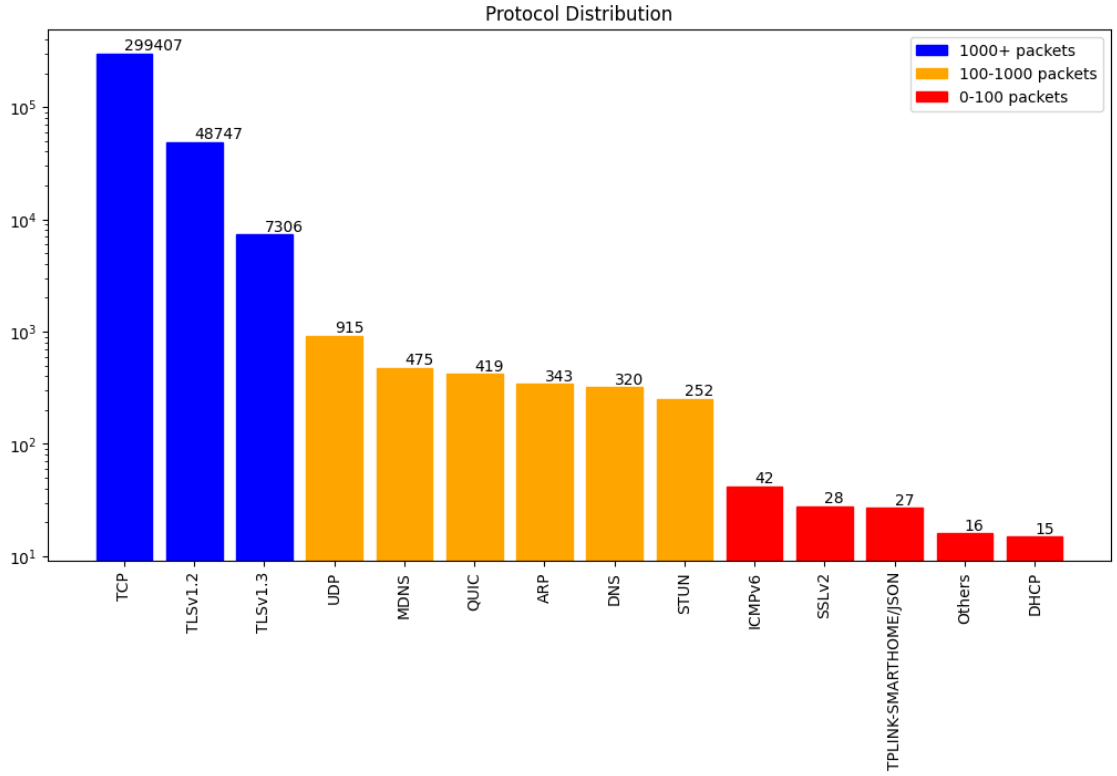
Destination Analysis for Private Addresses



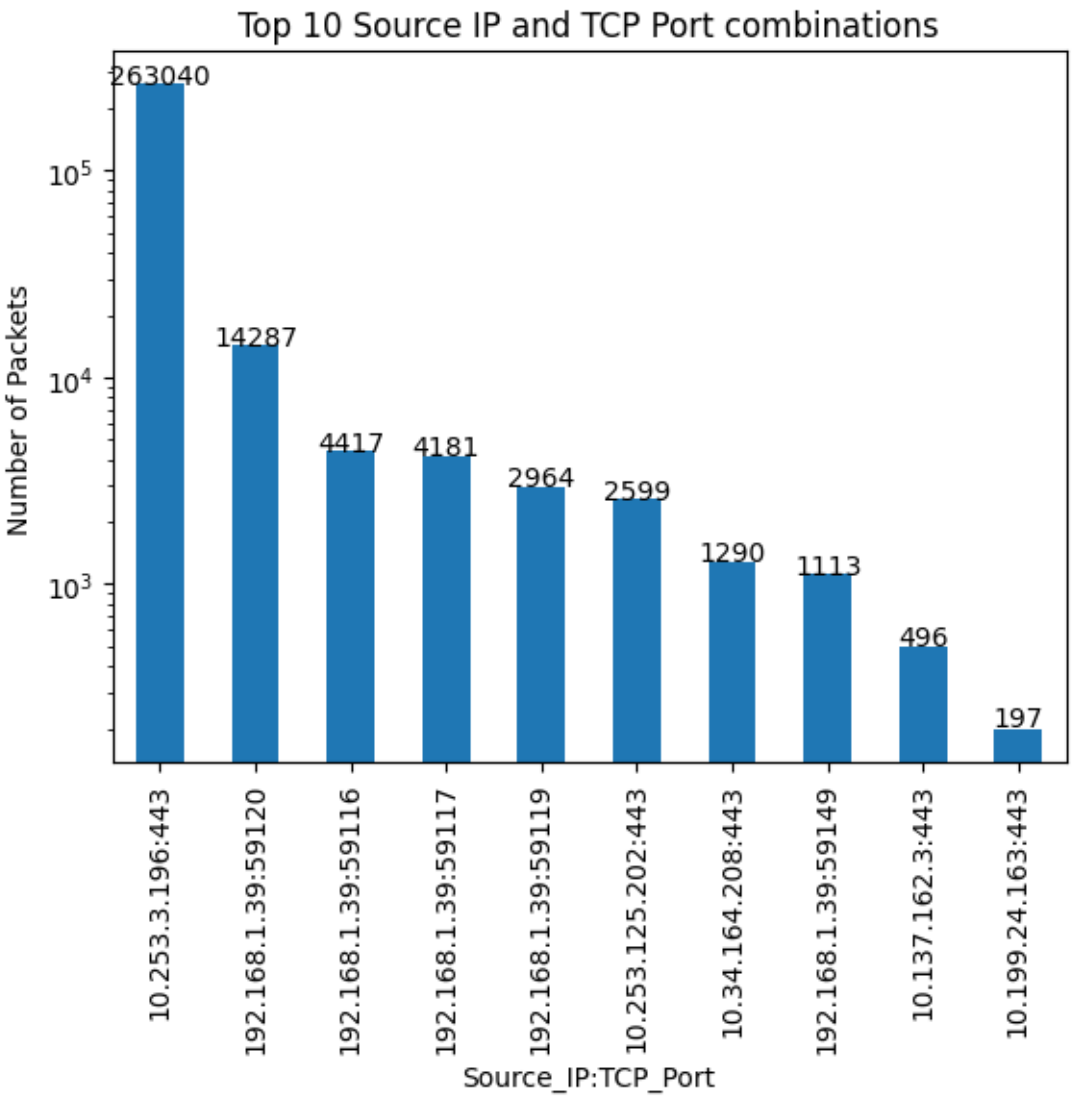

```
Destination Analysis for Public Addresses
The dataset does not have Public Destination IPs
Destination Analysis for IPv6 Addresses
```

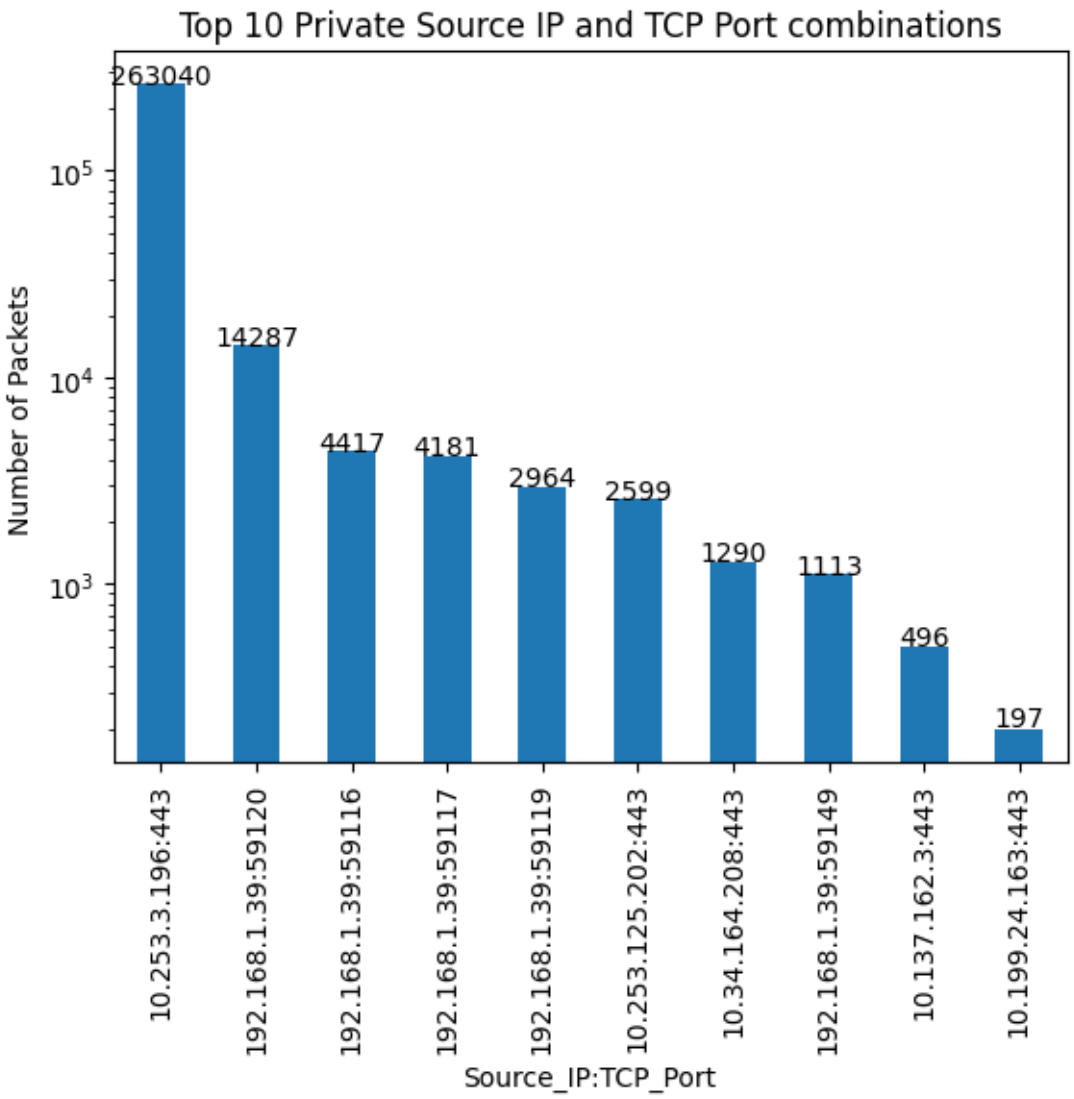


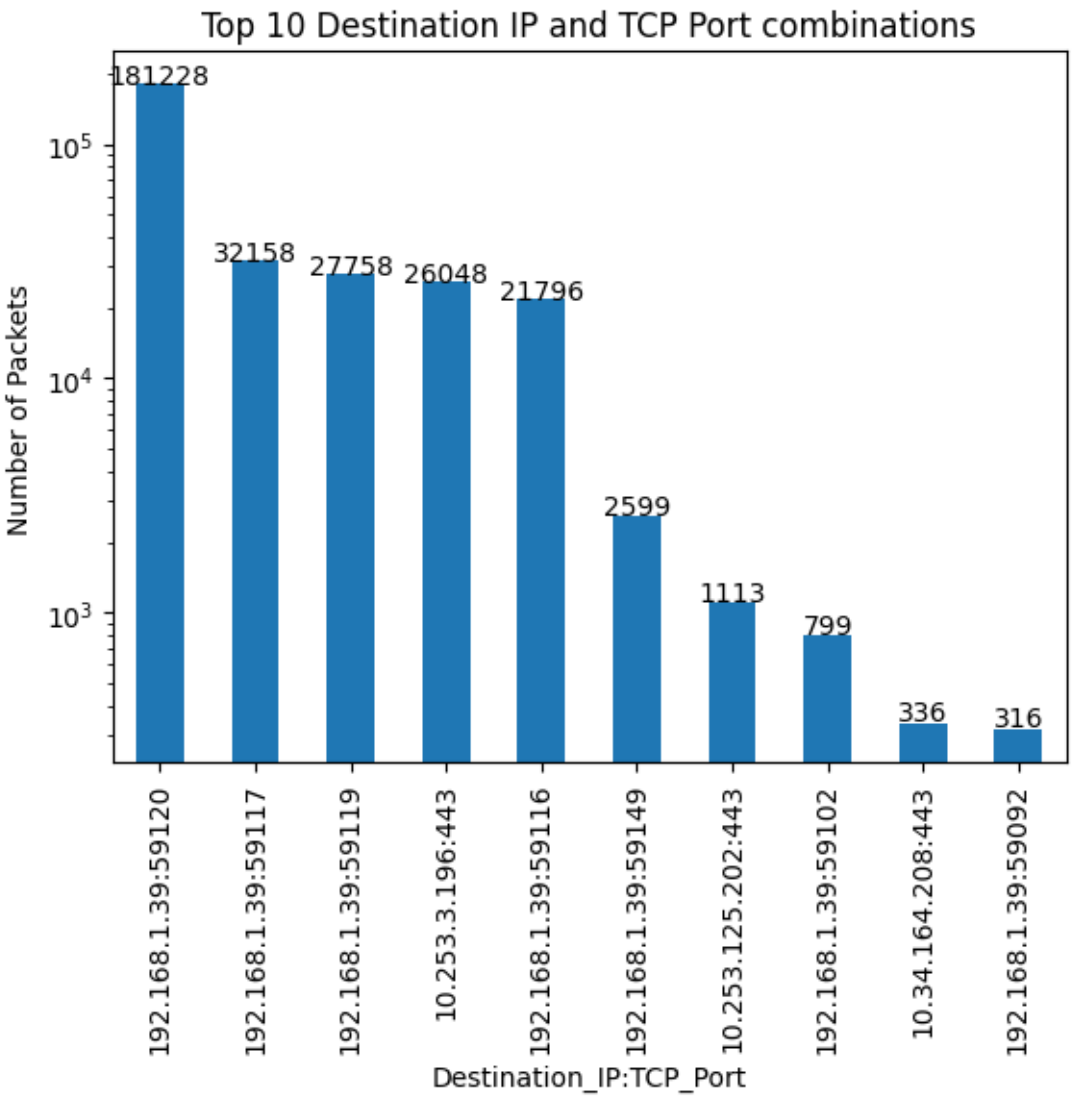

```
Protocol Analysis
========================================
```

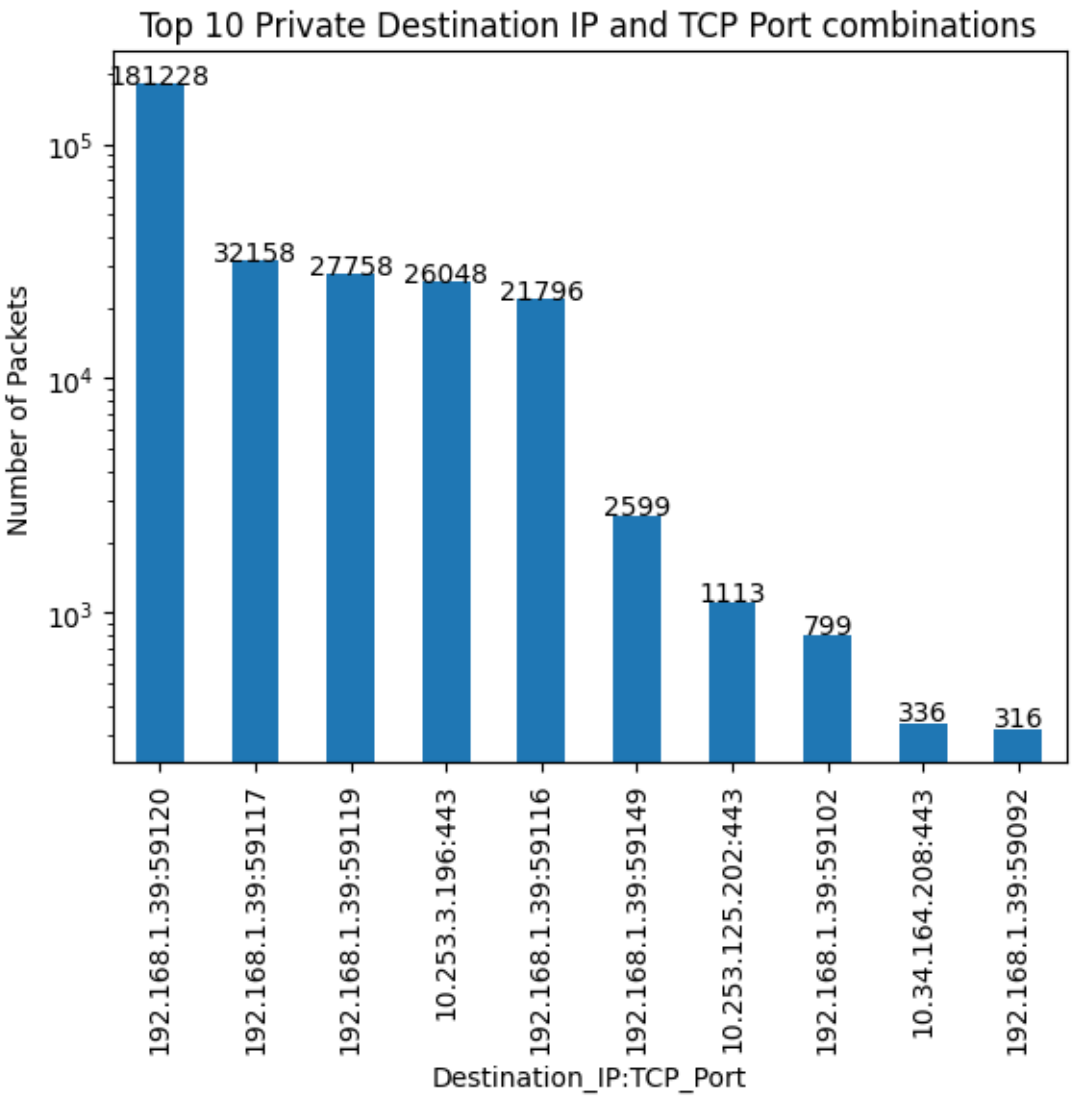


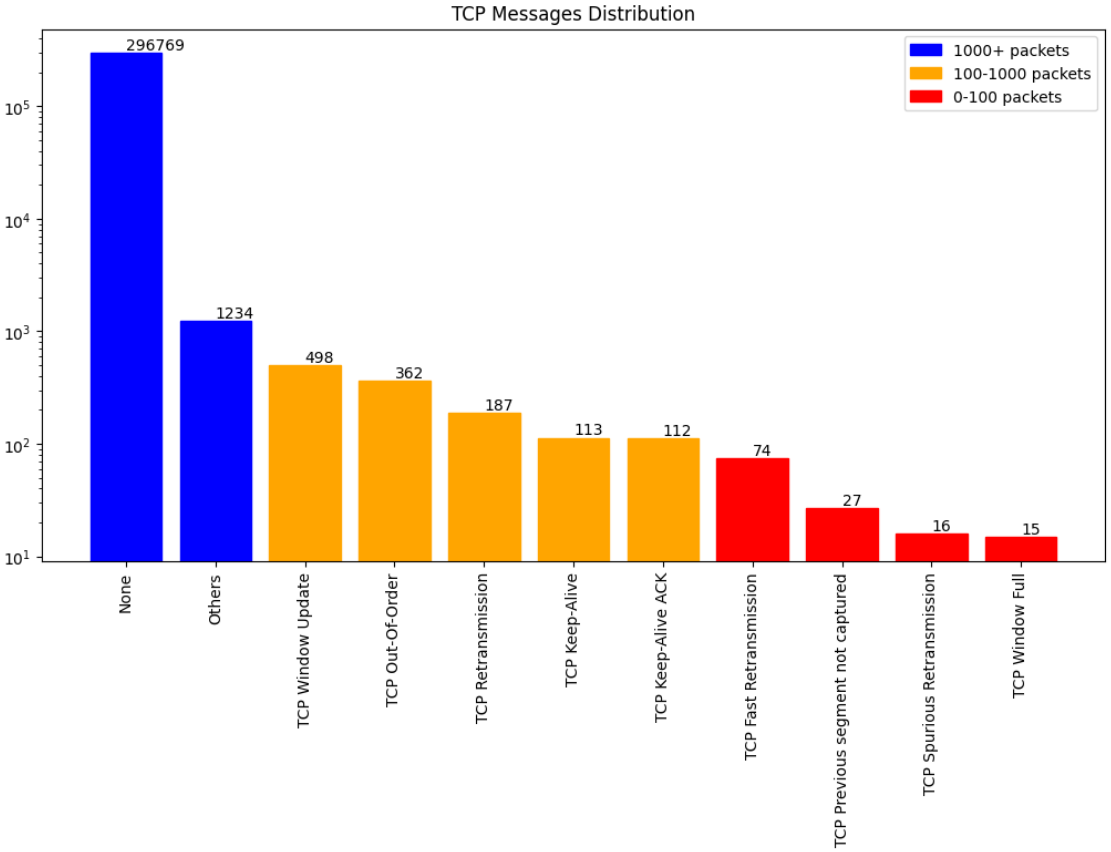
TCP Analysis
==========

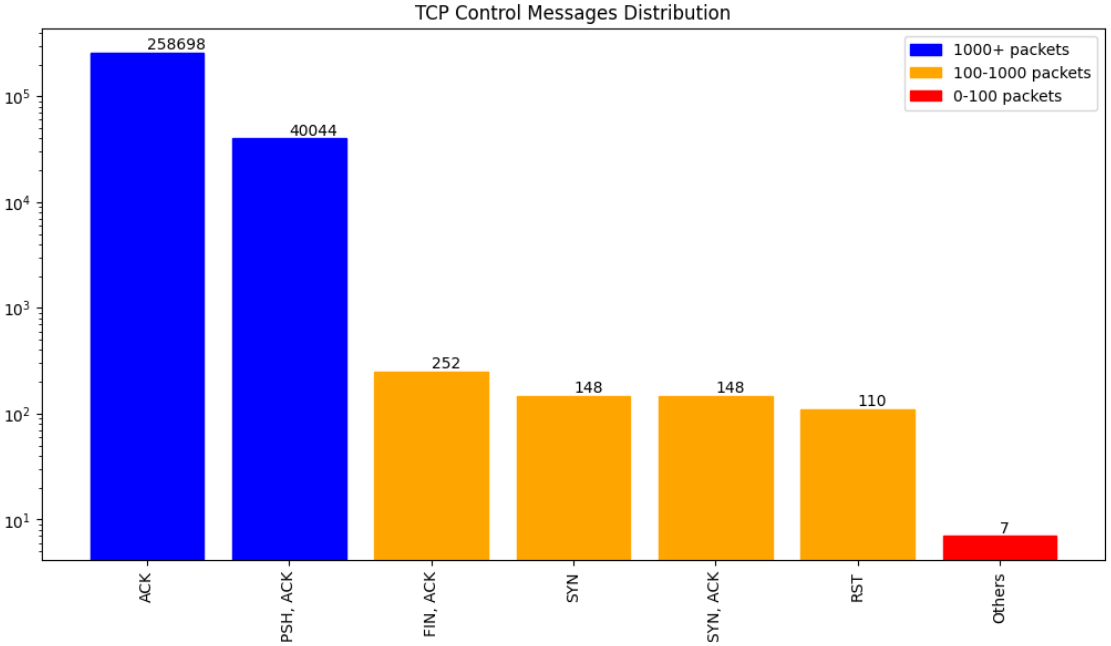

Top 10 Source IP and TCP Port combinations
Number of Packets
10^5
10^4
10^3
263040
14287
4417
4181
2964
2599
1290
1113
496
197
10.253.3.196:443
192.168.1.39:59120
192.168.1.39:59116
192.168.1.39:59117
192.168.1.39:59119
10.253.125.202:443
10.34.164.208:443
192.168.1.39:59149
10.137.162.3:443
10.199.24.163:443
Source_IP:TCP_Port


Top 10 Private Source IP and TCP Port combinations
Number of Packets
10^5
10^4
10^3
263040
14287
4417
4181
2964
2599
1290
1113
496
197
10.253.3.196:443
192.168.1.39:59120
192.168.1.39:59116
192.168.1.39:59117
192.168.1.39:59119
10.253.125.202:443
10.34.164.208:443
192.168.1.39:59149
10.137.162.3:443
10.199.24.163:443
Source_IP:TCP_Port


Top 10 Destination IP and TCP Port combinations
Number of Packets
10^5
10^4
10^3
181228
32158
27758
26048
21796
2599
1113
799
336
316
192.168.1.39:59120
192.168.1.39:59117
192.168.1.39:59119
10.253.3.196:443
192.168.1.39:59116
192.168.1.39:59149
10.253.125.202:443
192.168.1.39:59102
10.34.164.208:443
192.168.1.39:59092
Destination_IP:TCP_Port


Top 10 Private Destination IP and TCP Port combinations
Number of Packets
10^5
10^4
10^3
181228
32158
27758
26048
21796
2599
1113
799
336
316
192.168.1.39:59120
192.168.1.39:59117
192.168.1.39:59119
10.253.3.196:443
192.168.1.39:59116
192.168.1.39:59149
10.253.125.202:443
192.168.1.39:59102
10.34.164.208:443
192.168.1.39:59092
Destination_IP:TCP_Port


TCP Messages Distribution
1000+ packets
100-1000 packets
0-100 packets
296769
1234
498
362
187
113
112
74
27
16
15
None
Others
TCP Window Update
TCP Out-Of-Order
TCP Retransmission
TCP Keep-Alive
TCP Keep-Alive ACK
TCP Fast Retransmission
TCP Previous segment not captured
TCP Spurious Retransmission
TCP Window Full


TCP Control Messages Distribution
1000+ packets
100-1000 packets
0-100 packets
258698
40044
252
148
148
110
7
ACK
PSH, ACK
FIN, ACK
SYN
SYN, ACK
RST
Others

ARP Analysis
==========

IP and MAC Address Mapping

IP Address	MAC Address
192.168.1.122	Vendor_41:9e:78
192.168.1.32	Vendor_37:ab:0a
192.168.1.46	Vendor_57:20:fb
192.168.1.29	Vendor_49:00:87
192.168.1.23	Vendor_c2:50:1d
192.168.1.21	Vendor_48:56:64
192.168.1.39	Vendor_00:0a:98
192.168.1.34	Vendor_37:2b:6b
192.168.1.43	Vendor_77:dd:c1
192.168.1.1	Vendor_00:cd:18
192.168.1.113	Vendor_a9:d5:b2

Summary
==========

Summary
Description
*********Data Preprocessing*********
No missing values in the dataset
Total number of rows after deleting rows with missing values: 358312
********Source Analysis for Public IPs********
The dataset does not have Public Source IPs
***********Top Source IP Analysis***********
Top Source IP: 10.253.3.196
Total number of packets sent: 315630.
Percentage of packets sent by the top Source IP: 88.09%.
Destination Analysis for Public Addresses
The dataset does not have Public Destination IPs
***********Top Destination IP Analysis***********
Top Destination IP: 192.168.1.39
Total number of packets received: 325014.
Percentage of packets received by the top Destination IP: 90.71%.
*********TCP Analysis********
*********TCP Control Message Analysis*********

```
| TCP RST Analysis                                                          |
| Total TCP RST control messages: 110 out of 299407 total TCP control       |
| messages                                                                  |
| Percentage of TCP RST control messages: 0.04%                             |
| Percentage of TCP RST control messages: 0.04% (Low)                       |
|                                                                           |
| TCP SYN Analysis                                                          |
| Total TCP SYN control messages: 148 out of 299407 total TCP control       |
| messages                                                                  |
| Percentage of TCP SYN control messages: 0.05% (Low)                       |
| Total TCP SYN/ACK control messages: 148 out of 299407 total TCP           |
| control messages                                                          |
| Percentage of TCP SYN/ACK control messages: 0.05% (Low)                   |
| Percentage of TCP SYN and SYN/ACK control messages are equal,             |
| indicating a healthy environment.                                         |
+---------------------------------------------------------------------------+
```

Warnings

```
=======================================
+-------------------------------------------------------------------------------+
|                                  Warnings                                     |
+-----+----------------+--------------------------+---------------------------+
| No. | Category       | Description              | Recommendation            |
+-----+----------------+--------------------------+---------------------------+
| 1   | Source IP      | 10.253.3.196 sent more   | Investigate - potential   |
|     |                | than 50% of the total    | malware or DDoS attack    |
|     |                | packets.                 |                           |
| 2   | Destination IP | 192.168.1.39 received    | Investigate - potential   |
|     |                | more than 50% of the     | malware or DDoS attack    |
|     |                | total packets.           |                           |
+-----+----------------+--------------------------+---------------------------+
```

The graphs/plots have been saved in the ../results/plots/1226241136