PacketReporter

Customer: netwho

Segment: Backbone

Notes: Demo Capture

Table of Contents

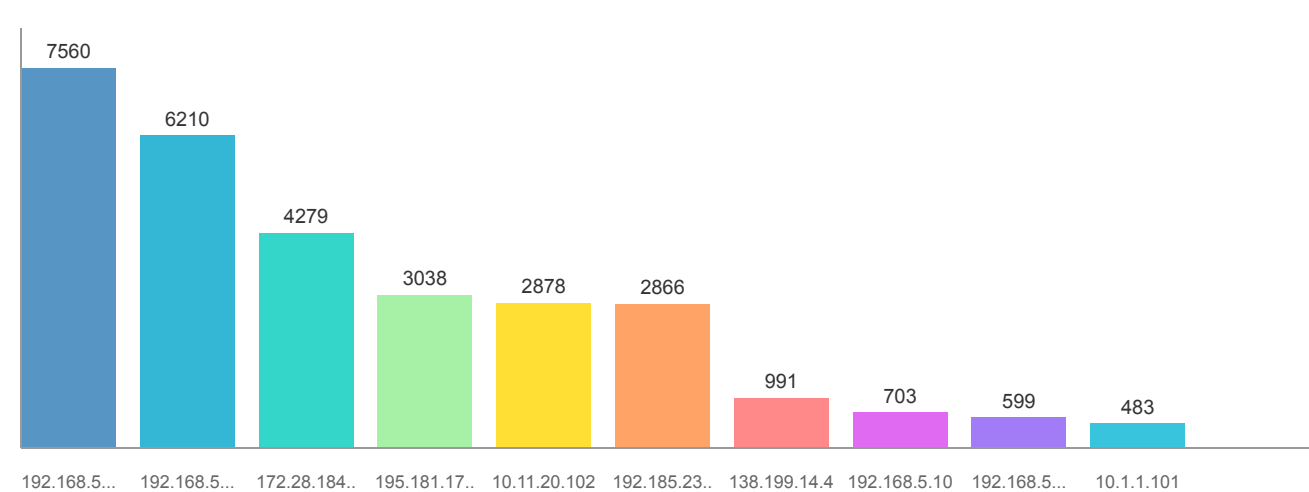# PacketReporter - Detailed Network Analysis Report

Generated: 2025-10-31 09:47:34
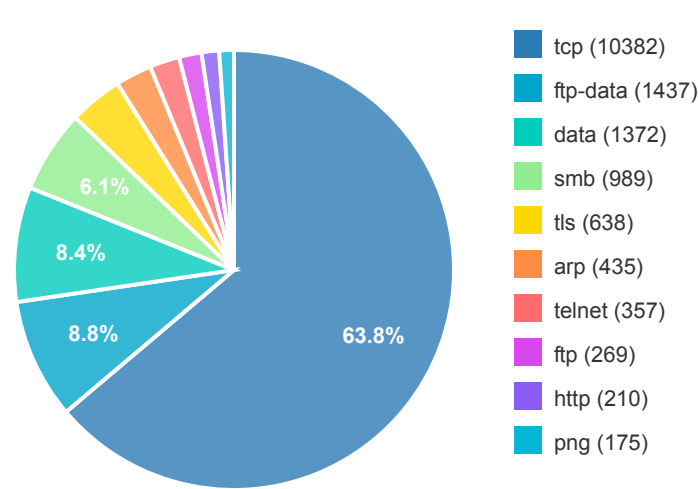
1. Summary

Capture Statistics

Total Packets: **16714**

Total Bytes: **11.7 MB**

Duration: **714960407.92 seconds**
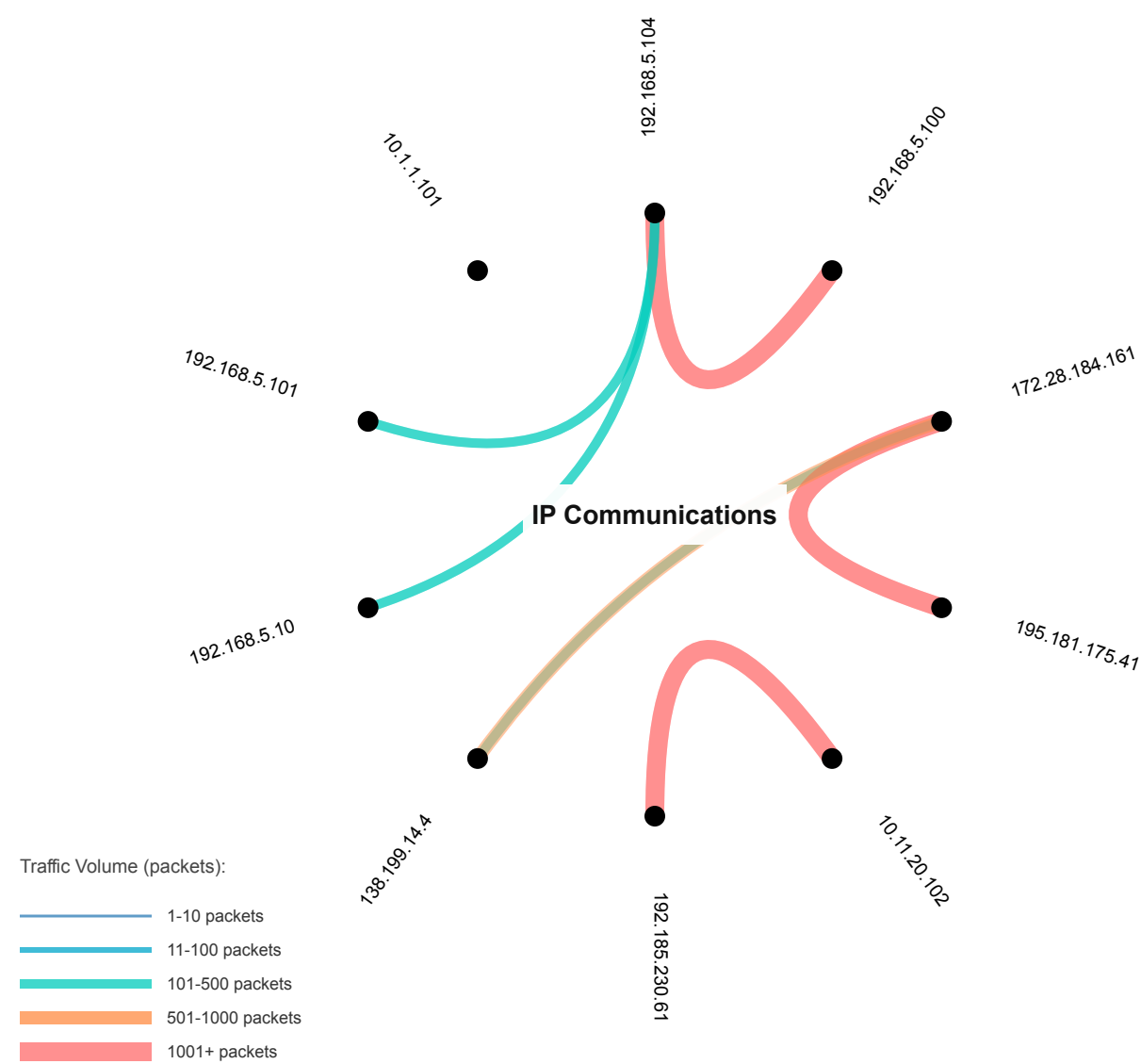
Unique IP Addresses: **10**

2. Top 10 IP Addresses
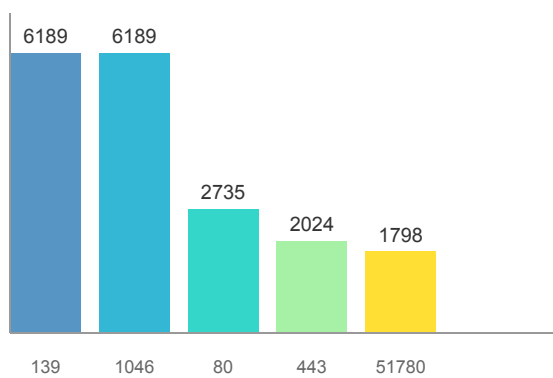

3. Top Protocols and Applications

- tcp (10382)
- ftp-data (1437)
- data (1372)
- smb (989)
- tls (638)
- arp (435)
- telnet (357)
- ftp (269)
- http (210)
- png (175)

4. IP Communication Matrix (Top 10 Hosts)

10.1.1.101

192.168.5.104

192.168.5.100

192.168.5.101

172.28.184.161

IP Communications

192.168.5.10

195.181.175.41

138.199.14.4

10.11.20.102

192.185.230.61

Traffic Volume (packets):

— 1-10 packets
— 11-100 packets
— 101-500 packets
— 501-1000 packets
— 1001+ packets

5. Port Analysis

5.1 Top 5 TCP Ports

Port	Count
139	6189
1046	6189
80	2735
443	2024
51780	1798

5.2 Top 5 UDP Ports

Port	Count
1065	691
64093	691
64663	597
1132	597
53	91
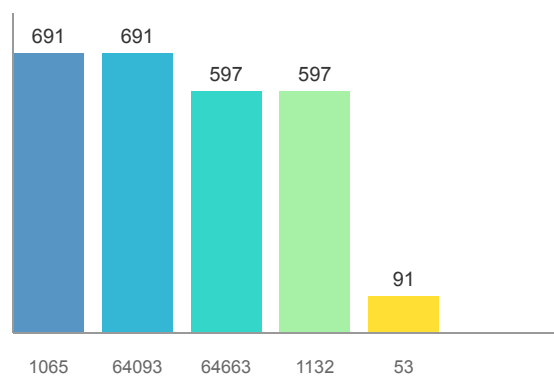
6. DNS Analysis

6.1 Top 10 DNS Queries

#	Domain	Queries
1	www.google-analytics.com	8
2	1906714720.rsc.cdn77.org	8
3	www.http2demo.io	8
4	www.facebook.com	8
5	1153288396.rsc.cdn77.org	8
6	www.googleadservices.com	8
7	connect.facebook.net	8
8	ocsp.digicert.com	4
9	www2.x3x4.su	4
10	safebrowsing.googleapis.com	4

6.2 DNS Record Types Distribution

- A (52)
- AAAA (28)
- TXT (3)
- MX (2)
- Type 65 (2)

59.8%

32.2%
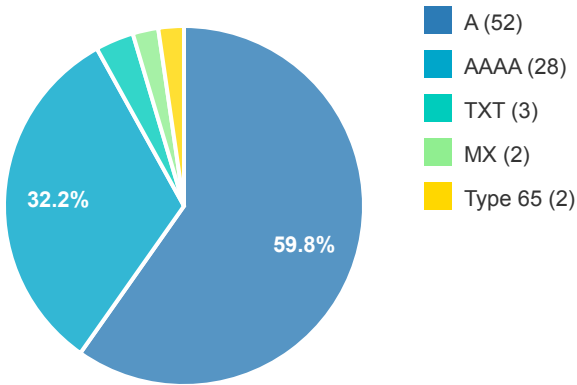
7. TLS/SSL Analysis

7.1 TLS/SSL Version Distribution

TLS 1.2	621
TLS 1.0	19

7.2 Top 10 TLS Server Names (SNI)

#	Server Name	Connections
1	ms.netwho.lan	3
2	xencloudmail-my.sharepoint.com	2
3	connect.facebook.net	2
4	1906714720.rsc.cdn77.org	2
5	www.facebook.com	2
6	safebrowsing.googleapis.com	1
7	n/a	n/a
8	n/a	n/a
9	n/a	n/a
10	n/a	n/a

7.3 Top 10 Certificate Common Names

#	Common Name	Count
1	GeoTrust Inc.	2
2	*.sharepoint.com	2
3	n/a	n/a
4	n/a	n/a
5	n/a	n/a
6	n/a	n/a
7	n/a	n/a
8	n/a	n/a
9	n/a	n/a
10	n/a	n/a

Total TLS Connections: **12**

8. HTTP Analysis

8.1 Top 10 HTTP User-Agents

#	User-Agent	Requests
1	Mozilla/5.0 (X11; Linux x86_64;..	192
2	Mozilla/4.0 (compatible; MSIE 6..	19
3	cpuminer 2.2.3	18
4	IP retriever	1
5	n/a	n/a
6	n/a	n/a
7	n/a	n/a
8	n/a	n/a
9	n/a	n/a
10	n/a	n/a

8.2 Top 10 HTTP Hosts

#	Host	Requests
1	1153288396.rsc.cdn77.org	172
2	www2.x3x4.su:666	18
3	www.http2demo.io	17
4	10.1.1.1	10
5	239.255.255.250:1900	6
6	opera3-servedby.advertising.com	2
7	opera1-servedby.advertising.com	2
8	opera4-servedby.advertising.com	2
9	opera2-servedby.advertising.com	2
10	ins1.opera.com	1

8.3 HTTP Status Codes

Status	Count
200	214
301	1

9. MAC Layer Analysis

9.2 Frame Size Distribution
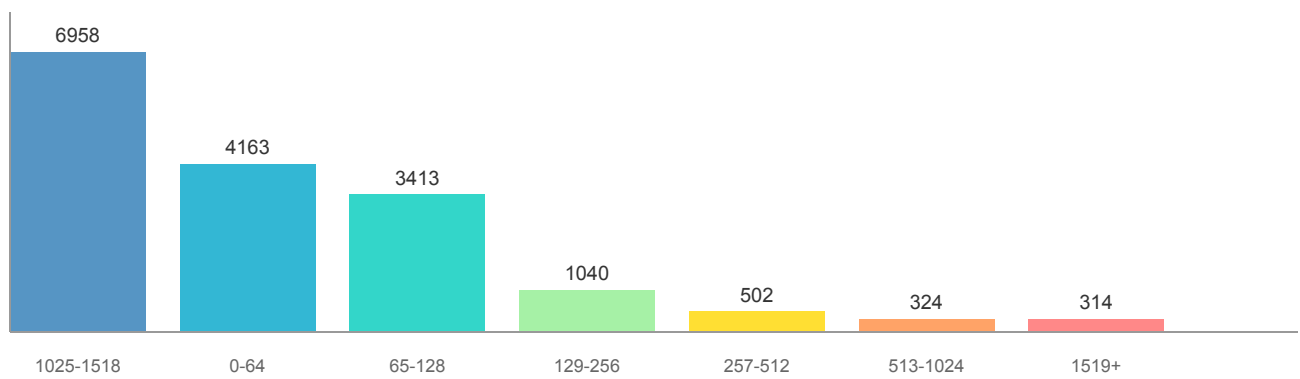
9.3 Top 10 MAC Vendors

#	Vendor	Packets
1	PCPartner_2c:d0:5c	4646
2	eacAUTOMATIO_2b:dc:85	2433
3	WesternDigit_5e:c2:c8	2242
4	6a:40:2c:73:0f:d4	1855
5	Netgear_b6:93:f1	1734
6	HewlettPacka_1c:47:ae	1144
7	Domotz_b:44:f3	392
8	PCPartner_31:0c:a6	376
9	Netgear_98:2a:12	295
10	SMCNetworks_22:5a:03	206

10. IP Layer Analysis

10.1 TTL Distribution

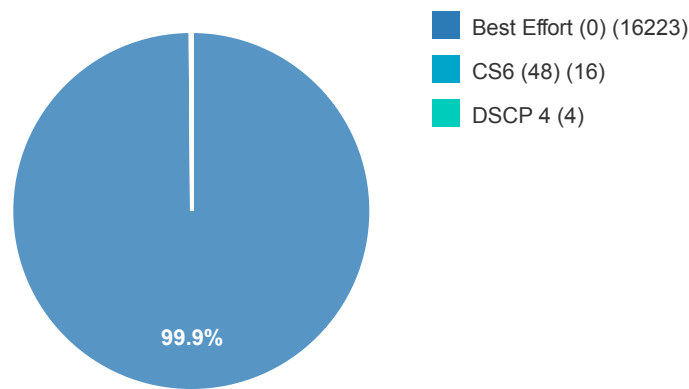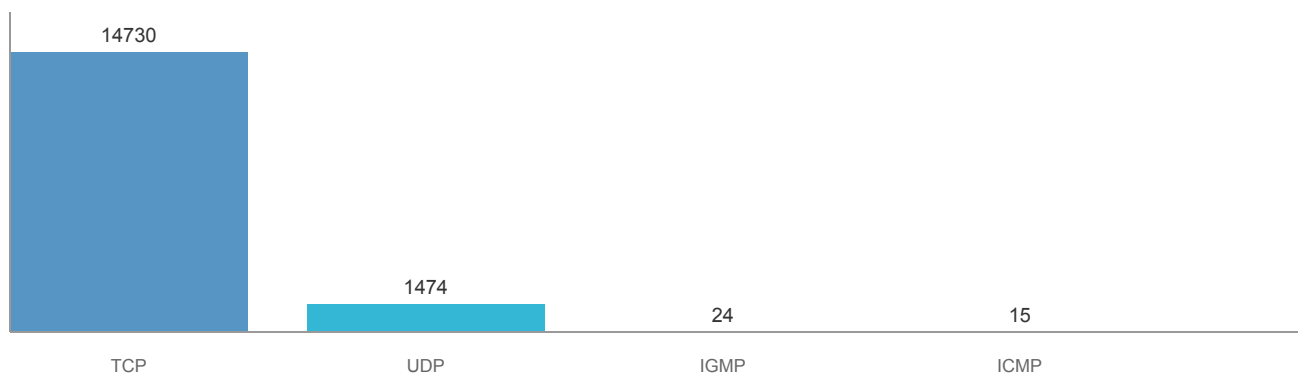| 97-128 | 33-64 | 0-32 | 65-96 | 225-255 |
| 8722 | 7214 | 251 | 51 | 5 |
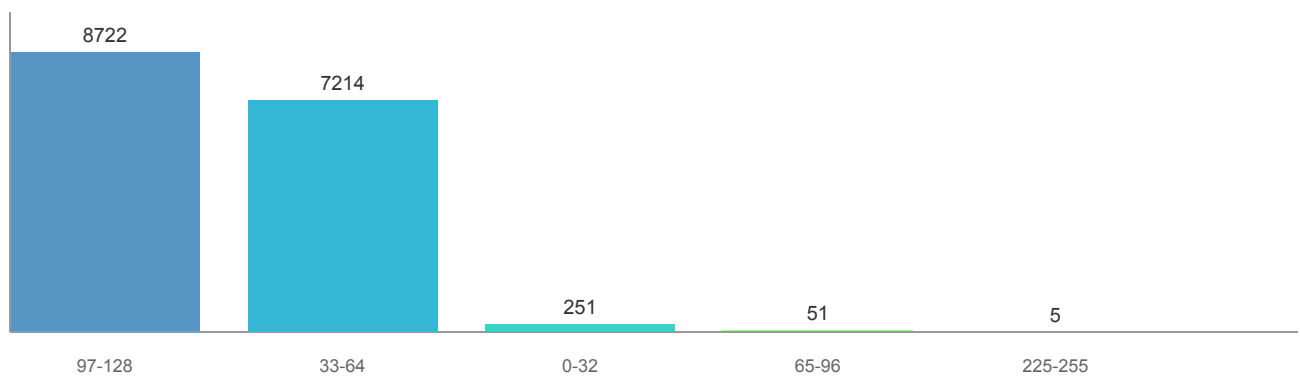
10.2 IP Fragmentation

Fragmented Packets: **19**

Fragmentation Rate: **0.12%**
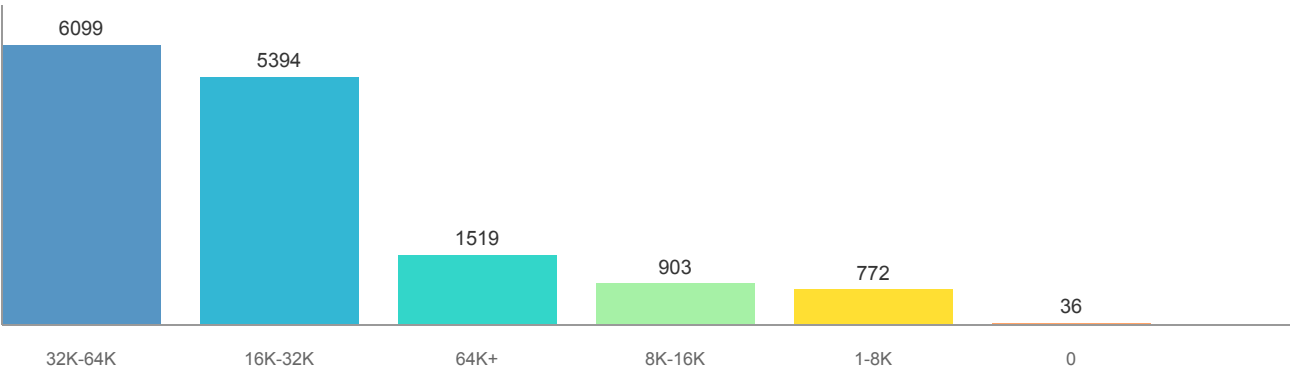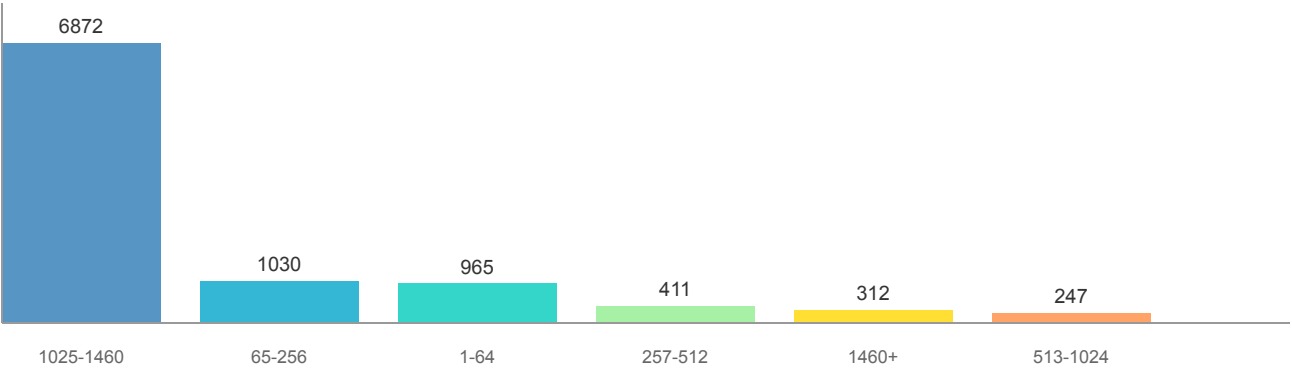
10.3 DSCP (Differentiated Services) Distribution

- Best Effort (0) (16223)
- CS6 (48) (16)
- DSCP 4 (4)

99.9%

10.4 IP Protocol Distribution

| TCP | UDP | IGMP | ICMP |
| 14730 | 1474 | 24 | 15 |

11. TCP Analysis

11.1 TCP Window Size Distribution

Category	Value
32K-64K	6099
16K-32K	5394
64K+	1519
8K-16K	903
1-8K	772
0	36

11.2 TCP Segment Size Distribution

Category	Value
1025-1460	6872
65-256	1030
1-64	965
257-512	411
1460+	312
513-1024	247

11.3 TCP Round-Trip Time Distribution

Category	Value
<1ms	3222
10-50ms	1934
1-10ms	517
100-500ms	238
50-100ms	190
500ms+	61