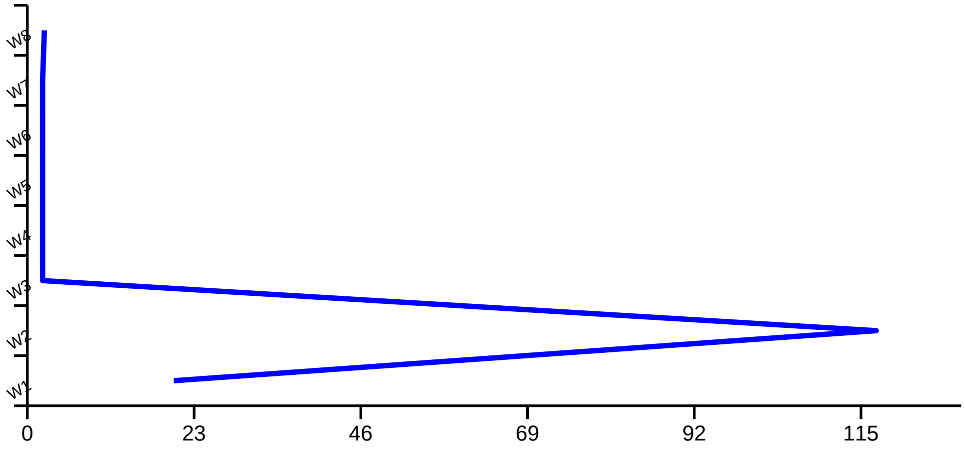
Z-Shark Network Analysis Report

1. Executive Summary

Metric	Value
File Analyzed	perfect_test_v2
Analysis Start Time	2026-01-01 18:10:57
Analysis End Time	2026-01-01 18:12:24
Total Duration	86.51 seconds
Total Packets	1,480
Total Bytes	0.08 MB
Incidents Detected	4

2. Packet Rate Over Time (PPS)



3. Network Flow Statistics

Top 5 Source IPs

Source IP	Packets	Bytes
10.0.0.5	1,000	52.73 KB
192.168.1.70	149	7.86 KB
10.0.0.7	120	6.33 KB

192.168.1.100	101	6.95 KB

Top 5 Destination Ports

Dest Port	Packets	Bytes
80	1,001	52.79 KB
443	120	6.33 KB
53	102	7.00 KB
1	1	0.05 KB
2	1	0.05 KB

4. Detected Incidents

Time	Severity	Label	Model	Justification
18:11:22	**HIGH**	High Volume Anomaly (DDoS Suspect)	DDoSDetector	PPS Z-score 291.74 exceeds threshold. Spike: 117.1 PPS (Avg: 18.7)
18:11:22	**HIGH**	Port Scan Suspect (Stateful)	PortScanDetector	Source IP 192.168.1.70 accessed 149 unique ports over time.
18:11:22	**HIGH**	ARP Spoofing Detected (MAC Conflict)	ARPSpoofDetector	IP 192.168.1.1 changed MAC from 00:11:22:33:44:55 to ff:ee:dd:cc:bb:aa.
18:11:22	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'zq8v2p9w4b1n6m3x5r7t9y2u4i6o8p0a1s2d3f4g5h6j7k8l.com' (Label: zq8v2p9w4b1n6m3x5r7t9y2u4i6o8p0a1s2d3f4g5h6j7k8l) has high entropy (4.94).

5. Mitigation Recommendations

- Isolate the source IP addresses identified in HIGH severity incidents immediately.
- Review firewall and IDS/IPS logs for correlation with the detected events.
- Implement rate-limiting policies on network devices to mitigate future volumetric attacks (e.g., DDoS).
- Update network device firmware and security patches.
- Conduct a full forensic analysis on any hosts identified in ARP Spoofing incidents.