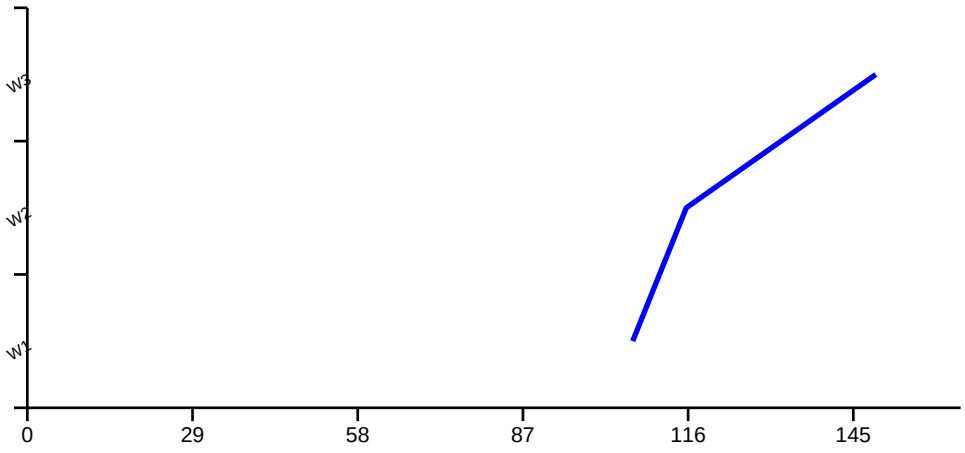
Z-Shark Network Analysis Report

1. Executive Summary

Metric	Value
File Analyzed	http-flood
Analysis Start Time	2018-08-02 07:30:52
Analysis End Time	2018-08-02 07:31:14
Total Duration	22.06 seconds
Total Packets	2,431
Total Bytes	0.91 MB
Incidents Detected	7

2. Packet Rate Over Time (PPS)



3. Network Flow Statistics

Top 5 Source IPs

Source IP	Packets	Bytes
10.0.0.2	1,429	136.64 KB
10.128.0.2	1,002	791.86 KB

Z-Shark Network Analysis Report

Top 5 Destination Ports

Dest Port	Packets	Bytes
80	1,429	136.64 KB
37361	7	7.08 KB
37368	7	7.08 KB
37369	7	7.08 KB
37362	6	7.02 KB

4. Detected Incidents

Time	Severity	Label	Model	Justification
07:31:02	HIGH	High Volume Anomaly (DDoS Suspect)	DDoSDetector	PPS Z-score 96.26 exceeds threshold 5.00.
07:31:02	HIGH	Source IP Entropy Collapse (DDoS Suspect)	DDoSDetector	Source IP entropy dropped to 0.98, 80.5% below mean 5.00.
07:31:02	HIGH	Port Scan Suspect	PortScanDetector	Source IP 10.128.0.2 accessed 89 unique ports with 437 packets.
07:31:12	HIGH	Source IP Entropy Collapse (DDoS Suspect)	DDoSDetector	Source IP entropy dropped to 0.98, 76.7% below mean 4.20.
07:31:12	HIGH	Port Scan Suspect	PortScanDetector	Source IP 10.128.0.2 accessed 100 unique ports with 470 packets.
07:31:14	HIGH	Source IP Entropy Collapse (DDoS Suspect)	DDoSDetector	Source IP entropy dropped to 0.98, 71.2% below mean 3.39.
07:31:14	MEDIUM	Port Scan Suspect	PortScanDetector	Source IP 10.128.0.2 accessed 20 unique ports with 95 packets.

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.