NETWORK TRAFFIC ANALYSIS

Forensic Investigation Report

Case ID:	CASE-20260117-150836
Analyst:	Emrya
Evidence File:	amp.TCP.reflection.SYNACK.pcap
Report Generated:	2026-01-17T15:08:39

Executive Summary

Network traffic analysis was conducted on the provided PCAP file. The analysis identified 7055 unique source IP addresses and 1 unique destination IP addresses. ■ SUSPICIOUS ACTIVITY DETECTED: - 2 DDoS attack indicator(s) - 2 UDP flood attack(s) Detailed findings are documented in the full report.

Evidence Integrity Verification

✓ Evidence Hash Verified

Hash Algorithm	Hash Value
SHA-256	`9339d7bc9d78e04a189b027890355d0b3c2687a720c32606acfa31d5325cd87e`
MD5	`16356bde9ddeddccf6f82de24944807b`

File Size: 643,499 bytes
Verified: 2026-01-17T15:08:36.388097

Complete IP Address Inventory

Source IP Addresses

#	Source IP Address	Packet Count
1	172.99.233.20	93
2	216.223.207.13	78
3	104.252.89.100	4
4	142.252.108.143	3
5	107.164.191.88	3
6	107.186.51.40	3
7	172.252.86.79	3
8	104.252.165.232	3
9	172.120.244.120	3
10	107.187.47.12	3

Destination IP Addresses

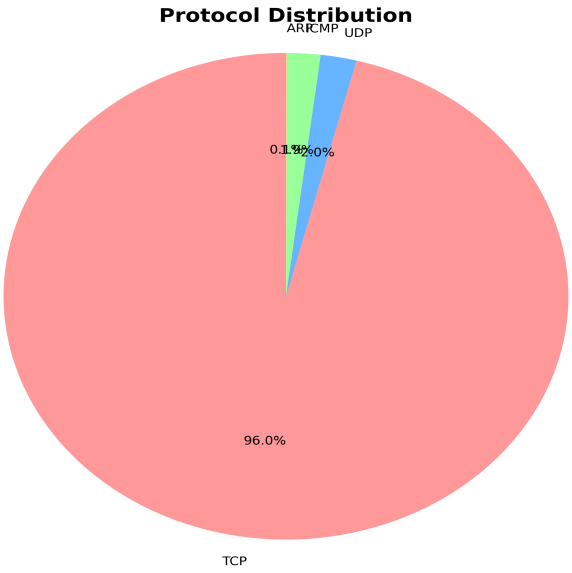
#	Destination IP Address	Packet Count
1	10.10.10.10	7996

Total Unique Source IPs: 7055
Total Unique Destination IPs: 1

Protocol Distribution Analysis

Protocol	Packet Count	Percentage
TCP	7,679	95.99%
UDP	164	2.05%
ICMP	153	1.91%
ARP	4	0.05%

Protocol Distribution Chart



Suspicious Activity Analysis

■ CRITICAL: DDoS Attack Indicators Detected

Pattern: High Packet Rate
Indication: Volumetric DDoS Attack
Severity: CRITICAL
Packet Rate: 54,492.53 packets/sec
Total Packets: 8,000
Duration: 0.15 seconds

Pattern: Distributed Attack
Indication: DDoS Attack (Multiple Sources)
Severity: CRITICAL
Target IP: 10.10.10.10
Unique Attackers: 7,055
Total Packets: 7,996

■ UDP Flood Attacks Detected

Source IP	UDP Packets	Severity
216.223.207.13	73	MEDIUM
172.99.233.20	74	MEDIUM

CHAIN OF CUSTODY (CoC) FORM

Case Information

Case Title:	CASE-20260117-150836
Analyst:	Emrya
Case Description:	N/A
Date Started:	2026-01-17

Evidence Details

Evidence Type:	PCAP Network Capture File
File Name:	amp.TCP.reflection.SYNACK.pcap
File Size:	643,499 bytes
Evidence Source:	Digital Network Traffic Capture
Original Hash (SHA256):	`9339d7bc9d78e04a189b027890355d0b3c2687a720c32606acfa31d5325cd87e`
Original Hash (MD5):	`16356bde9ddeddccf6f82de24944807b`
Acquisition Date/Time:	2026-01-17T15:08:36

Storage & Integrity Information

Storage Location:	Local Evidence Repository
Backup Location:	Secure Backup System
Access Restriction:	Authorized Personnel Only
Final Hash Verification:	
Hash BEFORE Analysis:	`9339d7bc9d78e04a189b027890355d0b3c2687a720c32606acfa31d5325cd87e`
Hash AFTER Analysis:	`9339d7bc9d78e04a189b027890355d0b3c2687a720c32606acfa31d5325cd87e`
Integrity Status:	**MATCHED ✓**

Declaration:
I/We declare that the evidence was handled ethically and professionally. All procedures followed proper chain of custody protocols. Hash verification confirms evidence integrity has been maintained throughout the analysis.

Handling Log

No.	Date/Time	Handler Name	Action Taken	Purpose	Hash (Yes/No)	Verified
1	2026-01-17T15:08:36	Emrya	Evidence Acquired	PCAP file loaded for analysis. SHA256: 9339d7bc9d7	Yes	✓
2	2026-01-17T15:08:36	Emrya	Hash Calculated	SHA256 and MD5 hashes generated for integrity veri	Yes	✓
3	2026-01-17T15:08:37	Emrya	Analysis Started	Loaded 8000 packets for analysis	Yes	✓

Certification

Name	Signature	Date
Emrya		2026-01-17