



# NETWORK TRAFFIC ANALYSIS

Forensic Investigation Report

Case ID:	CASE-20260113-145739
Analyst:	Emrys
Evidence File:	amp.TCP.reflection.SYNACK.pcap
Report Generated:	2026-01-13T14:57:41

■ CONFIDENTIAL - FOR AUTHORIZED PERSONNEL ONLY ■

# 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) Detailed findings are documented in the full report.

## Evidence Integrity Verification

✓ Evidence Hash Verified

Hash Algorithm	Hash Value
SHA-256	9339d7bc9d78e04a189b027890355d0b3c2687a720c32606acfa31d5325cd87e
MD5	16356bde9ddeddc6f6f82de24944807b

**File Size:** 643,499 bytes  
**Verified:** 2026-01-13T14:57:39.083633

# 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

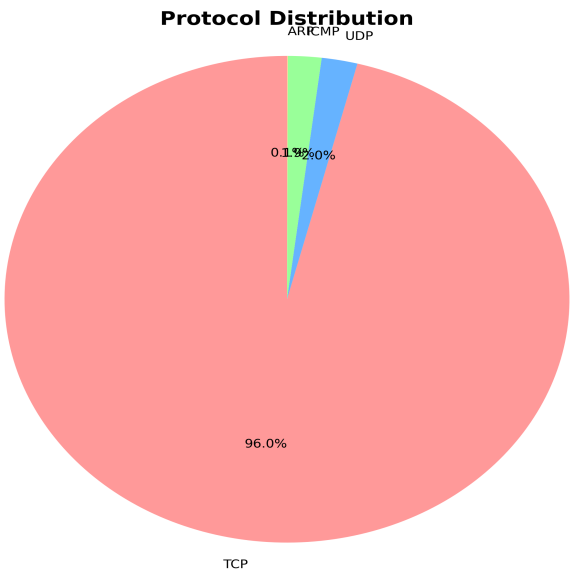
**Total Unique Source IPs: 7055**

**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

✓ No suspicious activity detected.

# CHAIN OF CUSTODY (CoC) FORM

## Case Information

Case Title:	CASE-20260113-145739
Analyst:	Emrys
Case Description:	N/A
Date Started:	2026-01-13

## 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):	16356bde9ddeddcf6f82de24944807b
Acquisition Date/Time:	2026-01-13T14:57:39

## 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	2026-01-13T14:57:39	Emrys	Evidence Acquired	PCAP file loaded for analysis. SHA256: 9339d7bc9d7	Yes	✓
2	2026-01-13T14:57:39	Emrys	Hash Calculated	SHA256 and MD5 hashes generated for integrity veri	Yes	✓
3	2026-01-13T14:57:40	Emrys	Analysis Started	Loaded 8000 packets for analysis	Yes	✓

## Certification

Name	Signature	Date
Emrys		2026-01-13

--- End of Report ---

Generated by Network Traffic Analyzer | CASE-20260113-145739