



NETWORK TRAFFIC ANALYSIS

Forensic Investigation Report

Case ID:	CASE-20260113-144649
Analyst:	Emrys
Evidence File:	evidence01.pcap
Report Generated:	2026-01-13T14:46:50

■ CONFIDENTIAL - FOR AUTHORIZED PERSONNEL ONLY ■

Executive Summary

Network traffic analysis was conducted on the provided PCAP file. The analysis identified 11 unique source IP addresses and 13 unique destination IP addresses. No significant suspicious activity was detected during the analysis.

Evidence Integrity Verification

✓ Evidence Hash Verified

Hash Algorithm	Hash Value
SHA-256	8b997bb2d221d538174f89796b6434e853d2ed19bd5da5f15bec9bd7bc485650
MD5	d187d77e18c84f6d72f5845edca833f5

File Size: 70,957 bytes

Verified: 2026-01-13T14:46:49.607881

Complete IP Address Inventory

Source IP Addresses

#	Source IP Address	Packet Count
1	192.168.1.159	59
2	192.168.1.158	38
3	205.188.13.12	31
4	192.168.1.157	28
5	64.12.25.91	24
6	64.12.24.50	20
7	192.168.1.2	7
8	64.236.68.246	5
9	192.168.1.10	4
10	192.168.1.30	3

Destination IP Addresses

#	Destination IP Address	Packet Count
1	192.168.1.159	76
2	192.168.1.255	39
3	192.168.1.158	30
4	64.12.24.50	20
5	64.12.25.91	16
6	205.188.13.12	16
7	192.168.1.2	5
8	64.236.68.246	5
9	192.168.1.30	4
10	192.168.1.157	4

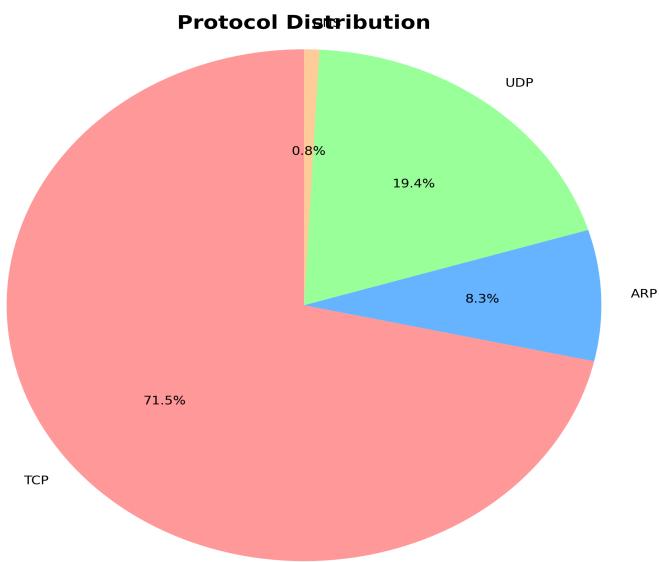
Total Unique Source IPs: 11

Total Unique Destination IPs: 13

Protocol Distribution Analysis

Protocol	Packet Count	Percentage
TCP	173	71.49%
ARP	20	8.26%
UDP	47	19.42%
DNS	2	0.83%

Protocol Distribution Chart



Suspicious Activity Analysis

✓ No suspicious activity detected.

CHAIN OF CUSTODY (CoC) FORM

Case Information

Case Title:	CASE-20260113-144649
Analyst:	Emrys
Case Description:	N/A
Date Started:	2026-01-13

Evidence Details

Evidence Type:	PCAP Network Capture File
File Name:	evidence01.pcap
File Size:	70,957 bytes
Evidence Source:	Digital Network Traffic Capture
Original Hash (SHA256):	8b997bb2d221d538174f89796b6434e853d2ed19bd5da5f15bec9bd7bc485650
Original Hash (MD5):	d187d77e18c84f6d72f5845edca833f5
Acquisition Date/Time:	2026-01-13T14:46:49

Storage & Integrity Information

Storage Location:	Local Evidence Repository
Backup Location:	Secure Backup System
Access Restriction:	Authorized Personnel Only
Final Hash Verification:	
Hash BEFORE Analysis:	8b997bb2d221d538174f89796b6434e853d2ed19bd5da5f15bec9bd7bc485650
Hash AFTER Analysis:	8b997bb2d221d538174f89796b6434e853d2ed19bd5da5f15bec9bd7bc485650
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	2026-01-13T14:46:49	Emrys	Evidence Acquired	PCAP file loaded for analysis. SHA256: 8b997bb2d22	Yes	✓
2	2026-01-13T14:46:49	Emrys	Hash Calculated	SHA256 and MD5 hashes generated for integrity veri	Yes	✓
3	2026-01-13T14:46:49	Emrys	Analysis Started	Loaded 240 packets for analysis	Yes	✓

Certification

Name	Signature	Date
Emrys		2026-01-13

--- End of Report ---

Generated by Network Traffic Analyzer | CASE-20260113-144649