NETWORK TRAFFIC ANALYSIS

Forensic Investigation Report

Case ID:	CASE-20260113-143423
Analyst:	Emrys
Evidence File:	2014-11-16-traffic-analysis-exercise.pcap
Report Generated:	2026-01-13T14:34:25

Executive Summary

Network traffic analysis was conducted on the provided PCAP file. The analysis identified 11 unique source IP addresses and 16 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	0e3fac547536f773bf1a21180a2294a10be97e956f091d24e168f147ecf5fafd
MD5	41d34d07aa81f3cb5ee12315cc5c88a9

File Size: 2,551,397 bytes
Verified: 2026-01-13T14:34:23.981520

Complete IP Address Inventory

Source IP Addresses

No source IPs found.

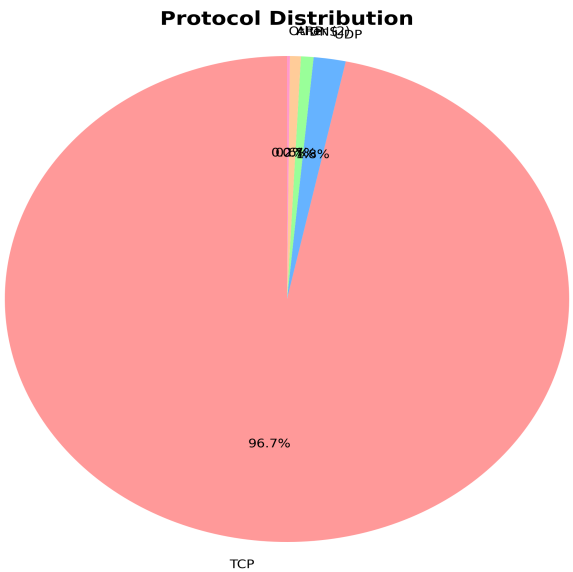## Destination IP Addresses

No destination IPs found.

Total Unique Source IPs: 11
Total Unique Destination IPs: 16

Protocol Distribution Analysis

Protocol	Packet Count	Percentage
TCP	2,951	96.66%
UDP	56	1.83%
DNS	22	0.72%
ARP	19	0.62%
Other (2)	5	0.16%

Protocol Distribution Chart

Protocol Distribution

TCP

Suspicious Activity Analysis

✓ No suspicious activity detected.

CHAIN OF CUSTODY (CoC) FORM

Case Information

Case Title:	CASE-20260113-143423
Analyst:	Emrys
Case Description:	N/A
Date Started:	2026-01-13

Evidence Details

Evidence Type:	PCAP Network Capture File
File Name:	2014-11-16-traffic-analysis-exercise.pcap
File Size:	2,551,397 bytes
Evidence Source:	Digital Network Traffic Capture
Original Hash (SHA256):	0e3fac547536f773bf1a21180a2294a10be97e956f091d24e168f147ecf5fafd
Original Hash (MD5):	41d34d07aa81f3cb5ee12315cc5c88a9
Acquisition Date/Time:	2026-01-13T14:34:23

Storage & Integrity Information

Storage Location:	Local Evidence Repository
Backup Location:	Secure Backup System
Access Restriction:	Authorized Personnel Only
Final Hash Verification:	
Hash BEFORE Analysis:	0e3fac547536f773bf1a21180a2294a10be97e956f091d24e168f147ecf5fafd
Hash AFTER Analysis:	0e3fac547536f773bf1a21180a2294a10be97e956f091d24e168f147ecf5fafd
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	2026-01-13T14:34:23	Emrys	Evidence Acquired	PCAP file loaded for analysis. SHA256: 0e3fac54753	Yes	✓
2	2026-01-13T14:34:23	Emrys	Hash Calculated	SHA256 and MD5 hashes generated for integrity veri	Yes	✓
3	2026-01-13T14:34:24	Emrys	Analysis Started	Loaded 3053 packets for analysis	Yes	✓

Certification

Name	Signature	Date
Emrys		2026-01-13