NETWORK TRAFFIC ANALYSIS

Forensic Investigation Report

Case ID:	CASE-20260113-113037
Analyst:	Emrys
Evidence File:	2022-MTA-workshop-Win11-host.pcap
Report Generated:	2026-01-13T11:30:39

Executive Summary

Network traffic analysis was conducted on the provided PCAP file. The analysis identified 38 unique source IP addresses and 43 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	42bda89f0ecdc1fd1a49ea02b766199ff508e489746afceb6719544670655351
MD5	b132bc2118f0af23cb9880854b3b0634

File Size: 3,335,701 bytes
Verified: 2026-01-13T11:30:37.325254

Complete IP Address Inventory

Source IP Addresses

No source IPs found.

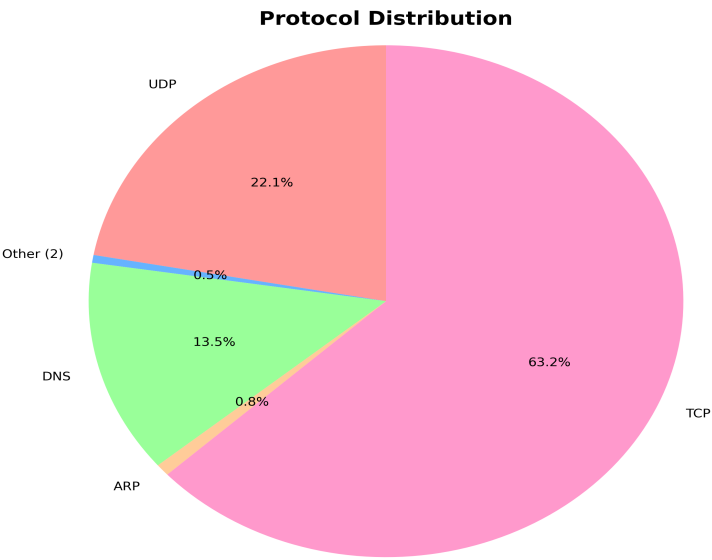## Destination IP Addresses

No destination IPs found.

Total Unique Source IPs: 38
Total Unique Destination IPs: 43

Protocol Distribution Analysis

Protocol	Packet Count	Percentage
UDP	405	22.11%
Other (2)	9	0.49%
DNS	247	13.48%
ARP	14	0.76%
TCP	1,157	63.16%

Protocol Distribution Chart

Protocol Distribution

UDP 22.1%

Other (2) 0.5%

DNS 13.5%

ARP 0.8%

TCP 63.2%

Suspicious Activity Analysis

✓ No suspicious activity detected.

Chain of Custody Documentation

#	Timestamp	Action	Analyst	Notes
1	2026-01-13T11:30:37	Evidence Acquired	Emrys	PCAP file loaded for analysis. SHA256: 4...
2	2026-01-13T11:30:37	Hash Calculated	Emrys	SHA256 and MD5 hashes generated for inte...
3	2026-01-13T11:30:38	Analysis Started	Emrys	Loaded 5110 packets for analysis