NETWORK TRAFFIC ANALYSIS

Forensic Investigation Report

Case ID:	CASE-20260113-141721
Analyst:	Emrys
Evidence File:	2022-MTA-workshop-Win11-host.pcap
Report Generated:	2026-01-13T14:17:23

■ CONFIDENTIAL - FOR AUTHORIZED PERSONNEL ONLY ■

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: 2026-01-13T14:17:21.302130

Complete IP Address Inventory

Source IP Addresses

No source IPs found.

Destination IP Addresses

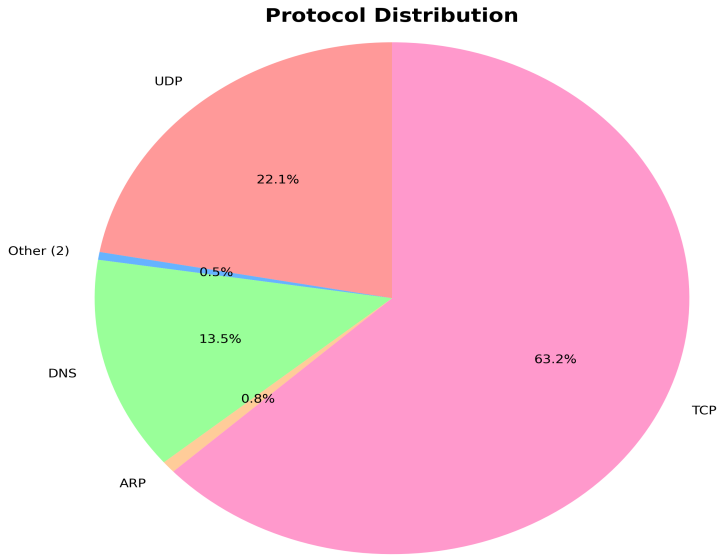
No destination IPs found.

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



Suspicious Activity Analysis

✓ No suspicious activity detected.

CHAIN OF CUSTODY (CoC) FORM

Case Information

Case Title:	CASE-20260113-141721
Analyst:	Emrys
Case Description:	N/A
Date Started:	2026-01-13

Evidence Details

Evidence Type:	PCAP Network Capture File
File Name:	2022-MTA-workshop-Win11-host.pcap
File Size:	3,335,701 bytes
Evidence Source:	Digital Network Traffic Capture
Original Hash (SHA256):	`42bda89f0ecdc1fd1a49ea02b766199ff508e489746afceb6719544670655351`
Original Hash (MD5):	`b132bc2118f0af23cb9880854b3b0634`
Acquisition Date/Time:	2026-01-13T14:17:21

Storage & Integrity Information

Storage Location:	Local Evidence Repository
Backup Location:	Secure Backup System
Access Restriction:	Authorized Personnel Only
Final Hash Verification:	
Hash BEFORE Analysis:	`42bda89f0ecdc1fd1a49ea02b766199ff508e489746afceb6719544670655351`
Hash AFTER Analysis:	`42bda89f0ecdc1fd1a49ea02b766199ff508e489746afceb6719544670655351`
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	2026-01-13T14:17:21	Emrys	Evidence Acquired	PCAP file loaded for analysis.	Yes	✓
2	2026-01-13T14:17:21	Emrys	Hash Calculated	SHA256 and MD5 hashes generate	Yes	✓
3	2026-01-13T14:17:22	Emrys	Analysis Started	Loaded 5110 packets for analysis	Yes	✓

Certification

Name	Signature	Date
Emrys		2026-01-13