Network Traffic Analysis and Firewall Configuration Report

Sanush Kannamkulangara Sanoj, GH1030311

July 3, 2025

Executive Summary

This study examines anomalous external network activity that was captured using Wireshark. Along with a set of suggested firewall rules (DROP/PERMIT) to reduce recognized risks and stop additional suspicious activity, this report also offers a descriptive and visual description of the network behavior.The primary observation involved DNS traffic from an internal client (192.168.88.61) to an external NTP server (`time.nist.gov`), consistently receiving DNS query refusals from the internal DNS resolver (192.168.88.1). Repeated failures may indicate either misconfiguration or a sign of illicit activities like malware beaconing or DNS tunneling, even if the behavior may be normal.

Methodology

- A PCAP file was extracted from 4SICS and was analysed in Wireshark.
- The file was exported as a CSV log and parsed for DNS query patterns.
- I focused on source/destination IPs, protocols, ports, and responses.
- Application-layer protocols (DNS), endpoints, and packet details were recorded.

Technical Analysis

OSI Layer Breakdown

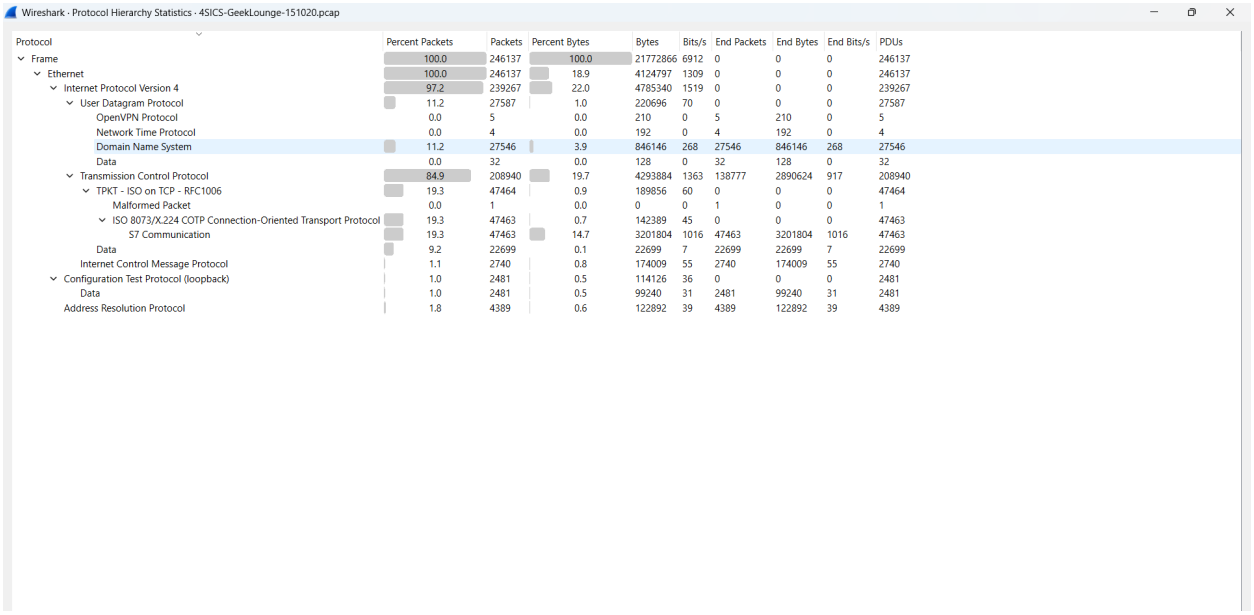
- **Layer 3 (Network Layer)**: IPv4 communication between 192.168.88.61 and 192.168.88.1
- **Layer 4 (Transport Layer)**: UDP (port 53) used for DNS
- **Layer 7 (Application Layer)**: DNS queries to `time.nist.gov`, responses were marked as refuse

Security Implications

- Repeatedly rejected queries could be a sign of intentional blocking or policy misconfiguration.
- From the observation, continuous outbound DNS requests be a sign of DNS tunneling or malware activity.
- Time synchronization might require NTP requests, which should be specifically filtered.

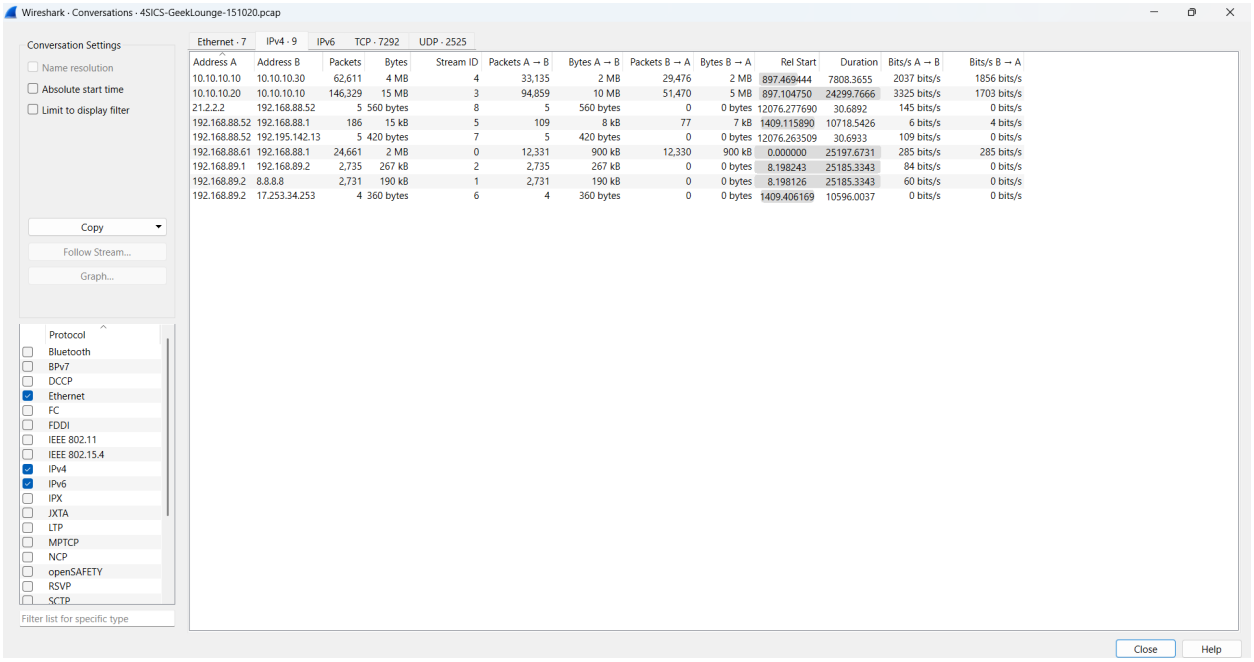
Visual Representations

Protocol Hierarchy

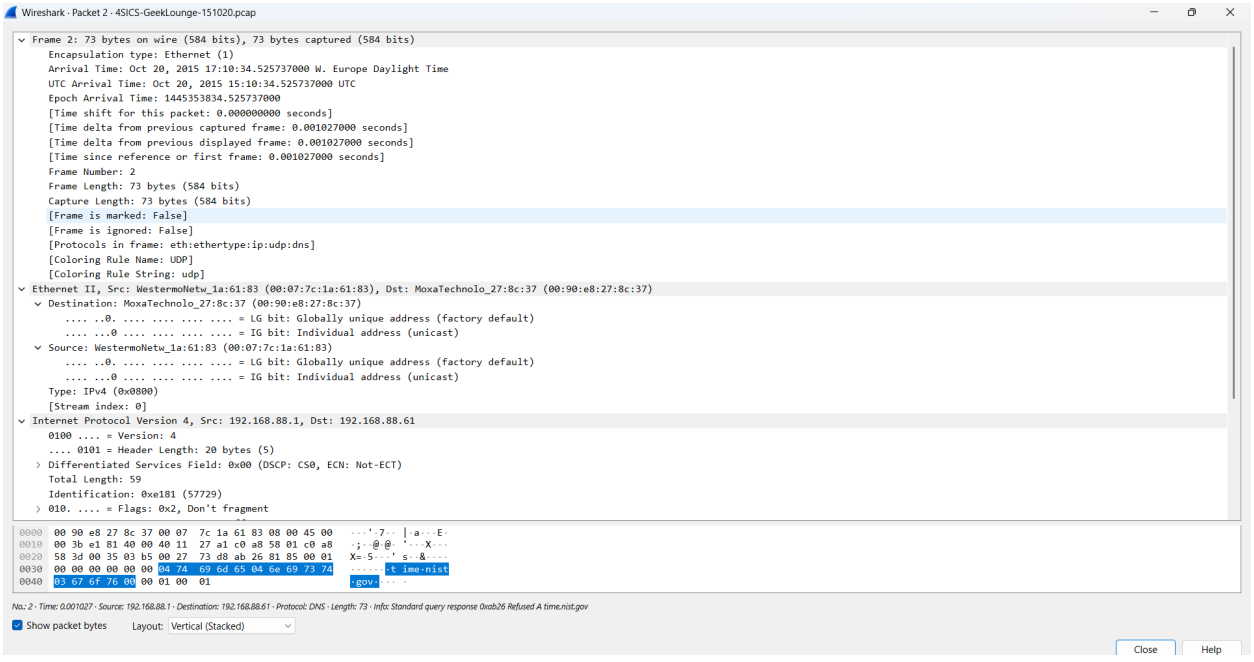


Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	246137	100.0	21772866	6912	0	0	0	246137
Ethernet	100.0	246137	18.9	4124797	1309	0	0	0	246137
Internet Protocol Version 4	97.2	239267	22.0	4785340	1519	0	0	0	239267
User Datagram Protocol	11.2	27587	1.0	220696	70	0	0	0	27587
OpenVPN Protocol	0.0	5	0.0	210	0	5	210	0	5
Network Time Protocol	0.0	4	0.0	192	0	4	192	0	4
Domain Name System	11.2	27546	3.9	846146	268	27546	846146	268	27546
Data	0.0	32	0.0	128	0	32	128	0	32
Transmission Control Protocol	84.9	208940	19.7	4293884	1363	138777	2890624	917	208940
TPKT - ISO on TCP - RFC1006	19.3	47464	0.9	189856	60	0	0	0	47464
Malformed Packet	0.0	1	0.0	0	0	1	0	0	1
ISO 8073/X.224 COTP Connection-Oriented Transport Protocol	19.3	47463	0.7	142389	45	0	0	0	47463
S7 Communication	19.3	47463	14.7	3201804	1016	47463	3201804	1016	47463
Data	9.2	22699	0.1	22699	7	22699	22699	7	22699
Internet Control Message Protocol	1.1	2740	0.8	174009	55	2740	174009	55	2740
Configuration Test Protocol (loopback)	1.0	2481	0.5	114126	36	0	0	0	2481
Data	1.0	2481	0.5	99240	31	2481	99240	31	2481
Address Resolution Protocol	1.8	4389	0.6	122892	39	4389	122892	39	4389

IPv4 Conversations



DNS Packet Details



Firewall Rules

Rule #	Action	Source IP	Destination IP	Protocol	Port	Description

1	PERMIT	192.168.88.61	Any	UDP	53	Allow DNS queries from internal client
2	DROP	Any	192.168.88.61	Any	Any	Block unsolicited inbound traffic to client
3	PERMIT	192.168.88.61	time.nist.gov	UDP	123	Allow NTP sync if required
4	DROP	192.168.88.61	Any External IP	UDP/TCP	!53,!123	Block all other outbound connections except DNS/NTP
5	DROP	Any	Any	Any	Any	Default deny-all fallback rule

Recommendations

- To investigate DNS server configuration on 192.168.88.1.
- Allow outbound NTP to known servers only (e.g., `time.nist.gov`).
- Blocking all other unknown external outbound connections.
- Monitoring client 192.168.88.61 for DNS queries.
- check firewall logs for unusual patterns once in a while.

GitHub Repository

The full project, including the PCAP file, CSV export, screenshots, and report source code, is available on GitHub:

- **Repository:** https://github.com/Sann7x/Wiresharkdumpanalysis

References and Sources

1. Pcap file source – `https://www.netresec.com/?page=PCAP4SICS`

Conclusion

The number and consistency of rejected responses may warrant additional research, even though the observed DNS behavior might be acceptable. To improve internal network security, firewall rules have been established to impose stricter outbound controls and permit only necessary traffic.