

# 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

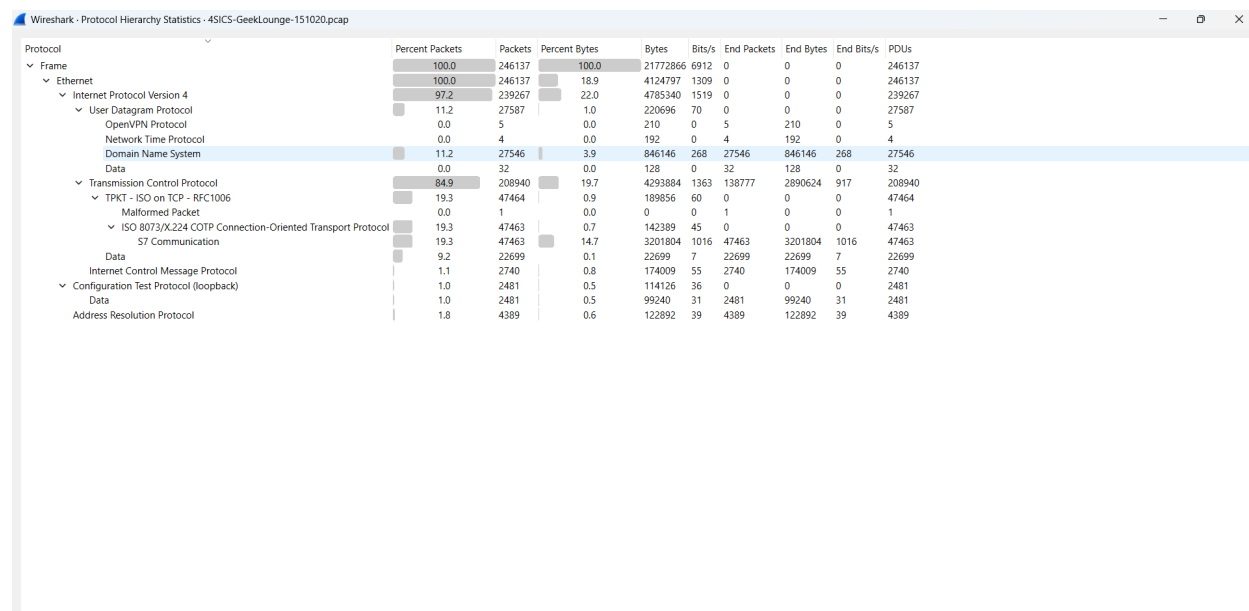
- **Layer 3 (Network Layer):** IPv4 communication between 192.168.88.61 and 192.168.88.1
- **Layer 4 (Transport Layer):** UDP (port 53) used for DNS
- **Layer 7 (Application Layer):** DNS queries to `time.nist.gov`, responses were marked as refuse

## 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



## IPv4 Conversations

Wireshark - Conversations - 45ICS-GeekLounge-151020.pcap

Conversation Settings

- ☐ Name resolution
- ☐ Absolute start time
- ☐ Limit to display filter

Copy

Follow Stream...

Graph...

Protocol

- ☐ Bluetooth
- ☐ BPV7
- ☐ DCCP
- ☒ Ethernet
- ☐ FC
- ☐ FDDI
- ☐ IEEE 802.11
- ☐ IEEE 802.15.4
- ☒ IPv4
- ☒ IPv6
- ☐ IPX
- ☐ JXTA
- ☐ LTP
- ☐ MPTCP
- ☐ NCP
- ☐ openSAFETY
- ☐ RSVP
- ☐ SCTP

Filter list for specific type

Ethernet - 7	IPv4 - 9	IPv6	TCP - 7292	UDP - 2525								
Address A	Address B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
10.10.10.10	10.10.10.30	62,611	4 MB	4	33,135	2 MB	29,476	2 MB	897.469444	7808.3655	2037 bits/s	1856 bits/s
10.10.10.20	10.10.10.10	146,329	15 MB	3	94,859	10 MB	51,470	5 MB	897.104750	24299.7666	3325 bits/s	1703 bits/s
212.2.2	192.168.88.52	5	560 bytes	8	5	560 bytes	0	0 bytes	12076.277690	30.6892	145 bits/s	0 bits/s
192.168.88.52	192.168.88.1	186	15 kB	5	109	8 kB	77	7 kB	1409.115890	10718.5426	6 bits/s	4 bits/s
192.168.88.52	192.195.142.13	5	420 bytes	7	5	420 bytes	0	0 bytes	12076.263509	30.6933	109 bits/s	0 bits/s
192.168.88.61	192.168.88.1	24,661	2 MB	0	12,331	900 kB	12,330	900 kB	0.000000	25197.6731	285 bits/s	285 bits/s
192.168.89.1	192.168.89.2	2,735	267 kB	2	2,735	267 kB	0	0 bytes	8.198243	25185.3343	84 bits/s	0 bits/s
192.168.89.2	8.8.8.8	2,731	190 kB	1	2,731	190 kB	0	0 bytes	8.198126	25185.3343	60 bits/s	0 bits/s
192.168.89.2	17.253.34.253	4	360 bytes	6	4	360 bytes	0	0 bytes	1409.406169	10596.0037	0 bits/s	0 bits/s

Close Help

## DNS Packet Details

Wireshark - Packet 2 - 45ICS-GeekLounge-151020.pcap

Frame 2: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)

Encapsulation type: Ethernet (1)

Arrival Time: Oct 20, 2015 17:10:34.525737000 W. Europe Daylight Time

UTC Arrival Time: Oct 20, 2015 15:10:34.525737000 UTC

Epoch Arrival Time: 1445353834.525737000

[Time shift for this packet: 0.000000000 seconds]

[Time delta from previous captured frame: 0.001027000 seconds]

[Time delta from previous displayed frame: 0.001027000 seconds]

[Time since reference or first frame: 0.001027000 seconds]

Frame Number: 2

Frame Length: 73 bytes (584 bits)

Capture Length: 73 bytes (584 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:udp:dns]

[Coloring Rule Name: UDP]

[Coloring Rule String: udp]

Ethernet II, Src: WesternoNetw\_1a:61:83 (00:07:7c:1a:61:83), Dst: MoxaTechnolo\_27:8c:37 (00:90:e8:27:8c:37)

Destination: MoxaTechnolo\_27:8c:37 (00:90:e8:27:8c:37)

.....0 ..... = IG bit: Globally unique address (factory default)

.....0 ..... = IG bit: Individual address (unicast)

Source: WesternoNetw\_1a:61:83 (00:07:7c:1a:61:83)

.....0 ..... = IG bit: Globally unique address (factory default)

.....0 ..... = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

[Stream index: 0]

Internet Protocol Version 4, Src: 192.168.88.1, Dst: 192.168.88.61

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 59

Identification: 0xe181 (57729)

> 010. .... = Flags: 0x2, Don't fragment

0000 00 90 e8 27 8c 37 00 07 7c 1a 61 83 08 00 45 00 ...7... |a...E

0010 00 3b e1 81 40 00 40 11 27 a1 c0 a8 58 01 c0 a8 ...@...X...

0020 58 3d 00 35 03 b5 00 27 73 d8 ab 26 81 85 00 01 X=5...s&

0030 00 00 00 00 00 04 74 69 6d 65 04 60 69 73 74 .....t.me.nist

0040 03 67 6f 76 00 00 01 00 01 gov...

No. 2 - Time: 0.001027 - Source: 192.168.88.1 - Destination: 192.168.88.61 - Protocol: DNS - Length: 73 - Info: Standard query response 0xaab26 Refused A time.nist.gov

Show packet bytes Layout: Vertical (Stacked)

Close Help

## 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.