Network Traffic Analysis Report

Satvik-2301mc37

Friday 17th October, 2025

1 Introduction

This report summarizes the findings from a network traffic analysis conducted on packet capture files. The objective of this analysis was to identify the most active protocols, detect any suspicious or unusual traffic, and gain key insights into the network communication patterns. The following sections detail the observations made from the provided screenshots of the packet analysis.

2 Most Active Protocols

Based on the analysis of the provided packet captures, several protocols showed significant activity. The following were the most prominent:

- **Domain Name System (DNS):** As seen in 'Screenshot from 2025-10-17 14-35-00.png', the DNS protocol was highly active. The capture shows numerous standard queries and responses between the source '10.21.17.102' and the DNS server '8.8.8.8'. These requests were for various domains, including 'www.typing.com', 'static.cloudflareinsights.com', 'fonts.googleapis.com', 'fonts.gstatic.com', and 'www.googletagmanager.com'.
- **Internet Control Message Protocol (ICMP):** The screenshot 'Screenshot from 2025-10-17 14-34-37.png' indicates a significant amount of ICMP traffic. Specifically, there are numerous "Echo (ping) request" and "Echo (ping) reply" packets between '10.21.17.102' and '8.8.8.8'. This suggests a continuous ping operation was active during the capture.
- **Hypertext Transfer Protocol (HTTP):** 'Screenshot from 2025-10-17 14-34-01.png' and 'Screenshot from 2025-10-17 14-53-09.png' show activity for the HTTP protocol. The traffic consists of 'GET' requests from '10.21.17.102' to '146.190.62.39'. The 'tshark' command output in the latter screenshot reveals that the host being accessed is 'httpforever.com'.
- **Transport Layer Security (TLS) and Transmission Control Protocol (TCP):** The capture in 'Screenshot from 2025-10-17 14-42-25.png' displays TLSv1.2 and TLSv1.3 traffic, which runs over TCP. This indicates secure web traffic. The details show a 'Client Hello', 'Server Hello', and 'Application Data' being exchanged between '10.21.17.102' and various destination IPs like '104.18.20.55', '142.250.192.98', and '185.199.108.133'.

3 Detailed Packet Analysis

As required by Task 3, a detailed analysis of one sample packet for ICMP, HTTP, and DNS protocols was conducted. The key details are summarized in the table below. The information is based on the data visible in the provided screenshots.

Protocol	Source IP	Destination IP	TTL	Packet Length	Flags
ICMP	10.21.17.102	8.8.8.8	64	98 bytes	
HTTP	10.21.17.102	146.190.62.39	64	527 bytes	PSH, ACK
DNS	10.21.17.102	8.8.8.8	64	85 bytes	Standard query

Table 1: Detailed Packet Information for Selected Protocols.

How to Check Flags in Wireshark

The flags for a given packet can be found in the "Packet Details" pane in Wireshark (the middle pane). You need to expand the appropriate protocol layer to see the flags field.

- **For ICMP:** The relevant flag (DF) is in the IP header. Expand the "Internet Protocol Version 4" layer and you will see a "Flags" field.
- **For HTTP:** Since HTTP runs over TCP, the flags are part of the TCP header. Expand the "Transmission Control Protocol" layer to see the "Flags" field, which will show if flags like PSH (Push) and ACK (Acknowledgment) are set.
- **For DNS:** DNS has its own flags within its protocol header. Expand the "Domain Name System" layer and look for the "Flags" field. This will show details like the "Recursion Desired" (RD) bit.

4 Suspicious or Unusual Traffic

While most of the traffic appears to be standard for web browsing and network diagnostics, a few patterns could be considered for closer inspection:

- **Continuous ICMP Pinging:** The large and continuous volume of ICMP echo requests and replies to '8.8.8.8' (Google's public DNS server) is noteworthy. While this is often used for network connectivity checks, a prolonged and uninterrupted ping could be indicative of a monitoring script or, in some contexts, could be used for network reconnaissance or covert channels.
- **Repeated HTTP Requests to httpforever.com:** The name of the domain 'httpforever.com' and the repeated 'GET' requests to it are unusual. This site may be designed to keep an HTTP connection open indefinitely, which could be used for testing purposes, but could also be a feature of certain types of malware or adware that need to maintain a connection to a command and control server. The repetition of these requests warrants further investigation into the nature of this domain.

5 Key Insights about Network Communication

The captured traffic provides a clear picture of the network communication patterns originating from the host '10.21.17.102':

- **Standard Web Browsing Activity:** The sequence of DNS queries followed by TCP/TLS connections to the resolved IP addresses is indicative of normal web browsing. For example, the DNS queries for Google Fonts and other domains are followed by secure connections, which is typical for modern websites that load resources from various sources.
- **Network Diagnostics:** The ICMP traffic to a reliable public server like '8.8.8.8' is a common method for checking internet connectivity. The consistency of this traffic suggests an automated process is likely at play.
- **Correlation between Protocols:** There is a clear correlation between the different protocols. DNS queries are made to resolve domain names, and shortly after, TCP and HTTP/TLS connections are established to the IP addresses returned by the DNS server. This demonstrates the foundational role of DNS in enabling almost all other network communications over the internet.

6 Conclusion

The network traffic analysis reveals a host engaged in what appears to be regular web browsing, evidenced by the numerous DNS lookups and subsequent HTTP/TLS connections. Alongside this, a continuous ICMP ping to a public DNS server suggests an active network monitoring or diagnostic tool. The repeated HTTP requests to 'httpforever.com' stand out as unusual and may require further investigation to rule out any malicious activity. Overall, the captured data provides valuable insights into the host's network behavior and highlights the interconnectedness of various protocols in day-to-day internet usage.