# Wireshark Capture Analysis Summary

## 1. Overview

This document summarizes the findings from a network capture analyzed using Wireshark on Kali Linux. The analysis focused on identifying various network protocols, key communication endpoints, and notable HTTP and DNS activities.

## 2. Protocol Summary

|  |  |
| --- | --- |
| **Protocol** | **Packet Count** |
| UDP | 7932 |
| QUIC | 2122 |
| TCP | 1477 |
| TLSv1.3 | 1222 |
| DNS | 106 |
| TLSv1.2 | 27 |
| ICMP | 26 |
| ARP | 16 |
| HTTP | 8 |
| MDNS | 2 |
| AJP13 | 2 |

## 3. HTTP Requests

Several HTTP GET requests were identified from host 192.168.1.6 to edgedl.me.gvt1.com, which appears to be a Google-related content delivery server (used for Chrome updates or background downloads). Example requests include:

|  |  |  |  |
| --- | --- | --- | --- |
| **Frame No.** | **Source IP** | **Host** | **Request URI** |
| 11380 | 192.168.1.6 | edgedl.me.gvt1.com | /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/... |
| 11631 | 192.168.1.6 | edgedl.me.gvt1.com | /edgedl/diffgen-puffin/ggkkehgbnfjpeggfpleeakpidbkibbmn/... |
| 11660 | 192.168.1.6 | edgedl.me.gvt1.com | /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/... |
| 11856 | 192.168.1.6 | edgedl.me.gvt1.com | /edgedl/diffgen-puffin/hfnkpimlhhgieaddgfemjhofmfblmnib/... |

## 4. Top IPv4 Conversations

The top communication pairs show frequent connections between the local host (192.168.1.6) and multiple Google servers, indicating browsing or background synchronization activity.

|  |  |  |
| --- | --- | --- |
| **Source <-> Destination** | **Frames** | **Total Data Transferred** |
| 192.168.1.6 <-> 142.251.220.110 | 4462 | 4.63 MB |
| 151.101.38.251 <-> 192.168.1.6 | 2656 | 2.81 MB |
| 192.168.1.6 <-> 142.251.223.229 | 2033 | 4.22 MB |
| 192.168.1.6 <-> 142.250.205.36 | 1150 | 1.00 MB |

## 5. DNS and WHOIS Queries

The DNS analysis revealed multiple lookups for 'google.com' and reverse DNS entries, along with WHOIS queries to 'whois.domaintools.com'. These queries suggest either background application lookups or routine browsing activity.

## 6. Conclusion

The Wireshark capture demonstrated active network communication from the host 192.168.1.6 to multiple Google servers using QUIC, TLS, and TCP. The main protocols observed include UDP, QUIC, TCP, and TLSv1.3, indicating modern encrypted traffic patterns. Minimal HTTP traffic and occasional DNS, ARP, and ICMP packets were also detected. Overall, the traffic appears to represent normal background operations such as updates, browser synchronization, and DNS resolution.