Wireshark Network Traffic Analysis Report

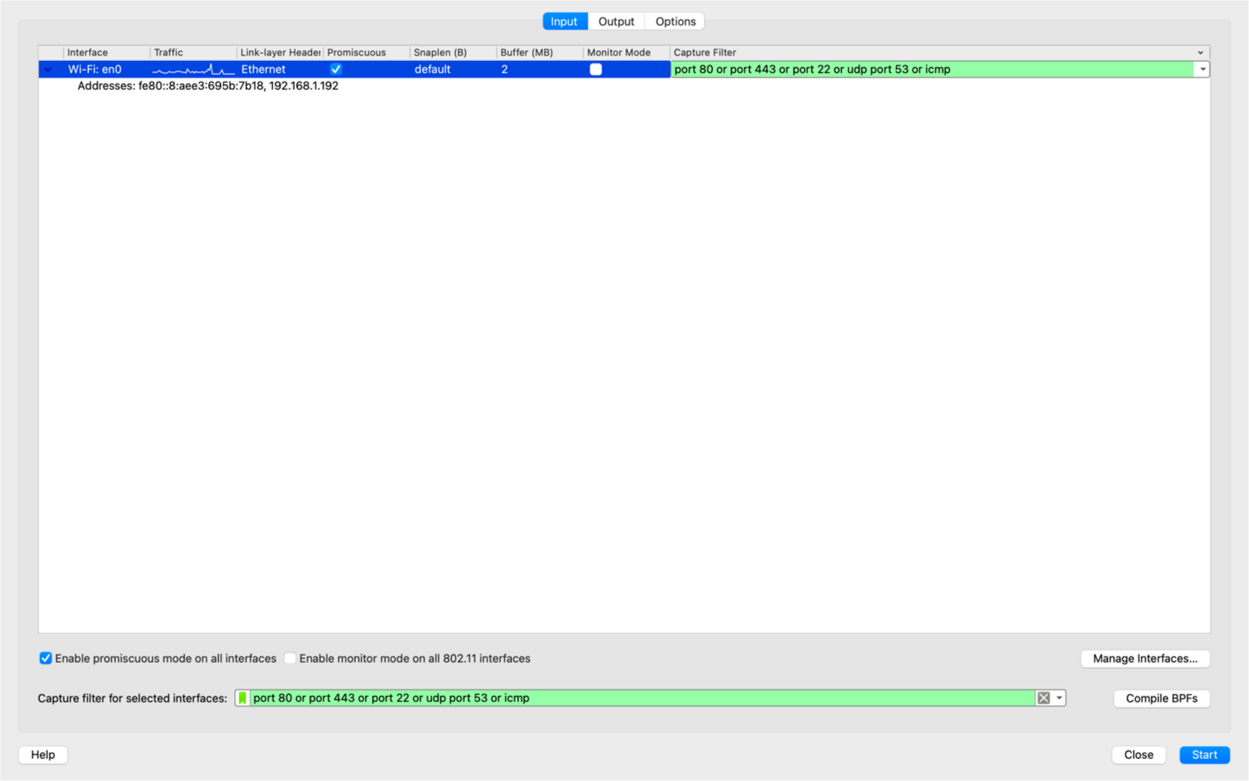
Prepared by: Iftekharul Islam
Date: 02/08/2025
Purpose: Network Security Analysis

This report analyzes captured network traffic using Wireshark to identify security risks. The analysis covers:

- Unencrypted HTTP traffic
- DNS queries to third-party servers
- Protocol hierarchy breakdown
- Potential security vulnerabilities

Setup

- **Capture Interface:** Wi-Fi (en0)
- **Applied Capture Filter:** port 80 or port 443 or port 22 or udp port 53 or icmp
- **Number of Packets Captured:** 24,484
- **File Name:** network_capture.pcapng



Interface	Traffic	Link-layer Header	Promiscuous	Snaplen (B)	Buffer (MB)	Monitor Mode	Capture Filter
Wi-Fi: en0		Ethernet	☑	default	2	□	port 80 or port 443 or port 22 or udp port 53 or icmp

Addresses: fe80::8:aee3:695b:7b18, 192.168.1.192

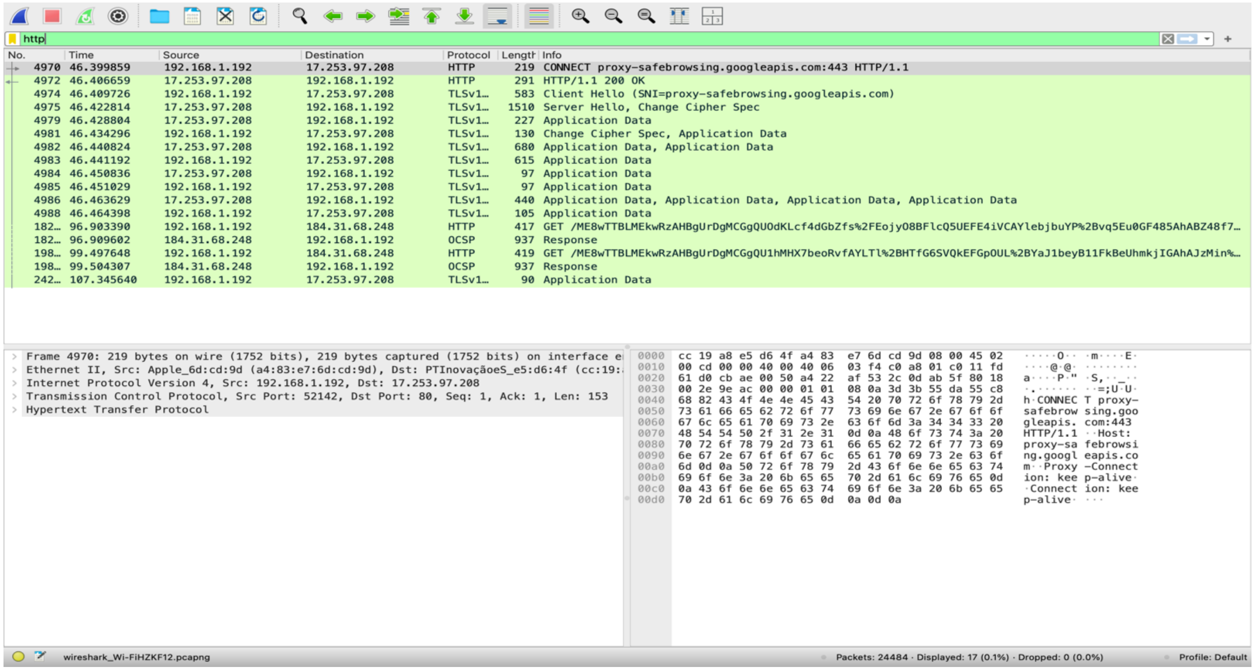
☑ Enable promiscuous mode on all interfaces □ Enable monitor mode on all 802.11 interfaces

Capture filter for selected interfaces: port 80 or port 443 or port 22 or udp port 53 or icmp

Findings

Unencrypted HTTP Traffic

- **Filter Used:** HTTP
- **Observation:** Some HTTP requests were detected.
- **Security Risk:** Unencrypted HTTP traffic exposes data, making it vulnerable to sniffing.
- **Recommendation:** Enforce HTTPS everywhere.



http

No.	Time	Source	Destination	Protocol	Length	Info
4970	46.399859	192.168.1.192	17.253.97.208	HTTP	219	CONNECT proxy-safebrowsing.googleapis.com:443 HTTP/1.1
4972	46.406659	17.253.97.208	192.168.1.192	HTTP	291	HTTP/1.1 200 OK
4974	46.409726	192.168.1.192	17.253.97.208	TLSv1…	583	Client Hello (SNI=proxy-safebrowsing.googleapis.com)
4975	46.422814	17.253.97.208	192.168.1.192	TLSv1…	1510	Server Hello, Change Cipher Spec
4979	46.428804	17.253.97.208	192.168.1.192	TLSv1…	227	Application Data
4981	46.434296	192.168.1.192	17.253.97.208	TLSv1…	130	Change Cipher Spec, Application Data
4982	46.440824	17.253.97.208	192.168.1.192	TLSv1…	680	Application Data, Application Data
4983	46.441192	192.168.1.192	17.253.97.208	TLSv1…	615	Application Data
4984	46.450836	17.253.97.208	192.168.1.192	TLSv1…	97	Application Data
4985	46.451029	192.168.1.192	17.253.97.208	TLSv1…	97	Application Data
4986	46.463629	17.253.97.208	192.168.1.192	TLSv1…	440	Application Data, Application Data, Application Data, Application Data
4988	46.464398	192.168.1.192	17.253.97.208	TLSv1…	105	Application Data
182…	96.903390	192.168.1.192	184.31.68.248	HTTP	417	GET /ME8wTTBLMEkwRzAHBgUrDgMCGgQUOdKLcf4dGbZfs%2FEojyO8BFlcQ5UEFE4iVCAYlebjbuYP%2Bvq5Eu0GF485AhABZ48f7…
182…	96.909602	184.31.68.248	192.168.1.192	OCSP	937	Response
198…	99.497648	192.168.1.192	184.31.68.248	HTTP	419	GET /ME8wTTBLMEkwRzAHBgUrDgMCGgQU1hMHX7beoRvfAYLTl%2BHTfG6SVQkEFGpOUL%2BYaJ1beyB11FkBeUhmkjIGAhAJzMin%…
198…	99.504307	184.31.68.248	192.168.1.192	OCSP	937	Response
242…	107.345640	192.168.1.192	17.253.97.208	TLSv1…	90	Application Data

```
> Frame 4970: 219 bytes on wire (1752 bits), 219 bytes captured (1752 bits) on interface e
> Ethernet II, Src: Apple_6d:cd:9d (a4:83:e7:6d:cd:9d), Dst: PTInovaçãoeS_e5:d6:4f (cc:19:
> Internet Protocol Version 4, Src: 192.168.1.192, Dst: 17.253.97.208
> Transmission Control Protocol, Src Port: 52142, Dst Port: 80, Seq: 1, Ack: 1, Len: 153
> Hypertext Transfer Protocol
```

```
0000  cc 19 a8 e5 d6 4f a4 83  e7 6d cd 9d 08 00 45 02   ·····O·· ·m····E·
0010  00 cd 00 00 40 00 40 06  03 f4 c0 a8 01 c0 11 fd   ····@·@· ········
0020  61 d0 cb ae 00 50 a4 22  af 53 2c 0d ab 5f 80 18   a····P·" ·S,··_··
0030  00 2e 9e ac 00 00 01 01  08 0a 3d 3b 55 da 55 c8   ·.······ ··=;U·U·
0040  68 82 43 4f 4e 4e 45 43  54 20 70 72 6f 78 79 2d   h·CONNEC T proxy-
0050  73 61 66 65 62 72 6f 77  73 69 6e 67 2e 67 6f 6f   safebrow sing.goo
0060  67 6c 65 61 70 69 73 2e  63 6f 6d 3a 34 34 33 20   gleapis. com:443 
0070  48 54 54 50 2f 31 2e 31  0d 0a 48 6f 73 74 3a 20   HTTP/1.1 ··Host: 
0080  70 72 6f 78 79 2d 73 61  66 65 62 72 6f 77 73 69   proxy-sa febrowsi
0090  6e 67 2e 67 6f 6f 67 6c  65 61 70 69 73 2e 63 6f   ng.googl eapis.co
00a0  6d 0d 0a 50 72 6f 78 79  2d 43 6f 6e 6e 65 63 74   m··Proxy -Connect
00b0  69 6f 6e 3a 20 6b 65 65  70 2d 61 6c 69 76 65 0d   ion: kee p-alive·
00c0  0a 43 6f 6e 6e 65 63 74  69 6f 6e 3a 20 6b 65 65   ·Connect ion: kee
00d0  70 2d 61 6c 69 76 65 0d  0a 0d 0a                  p-alive· ···
```

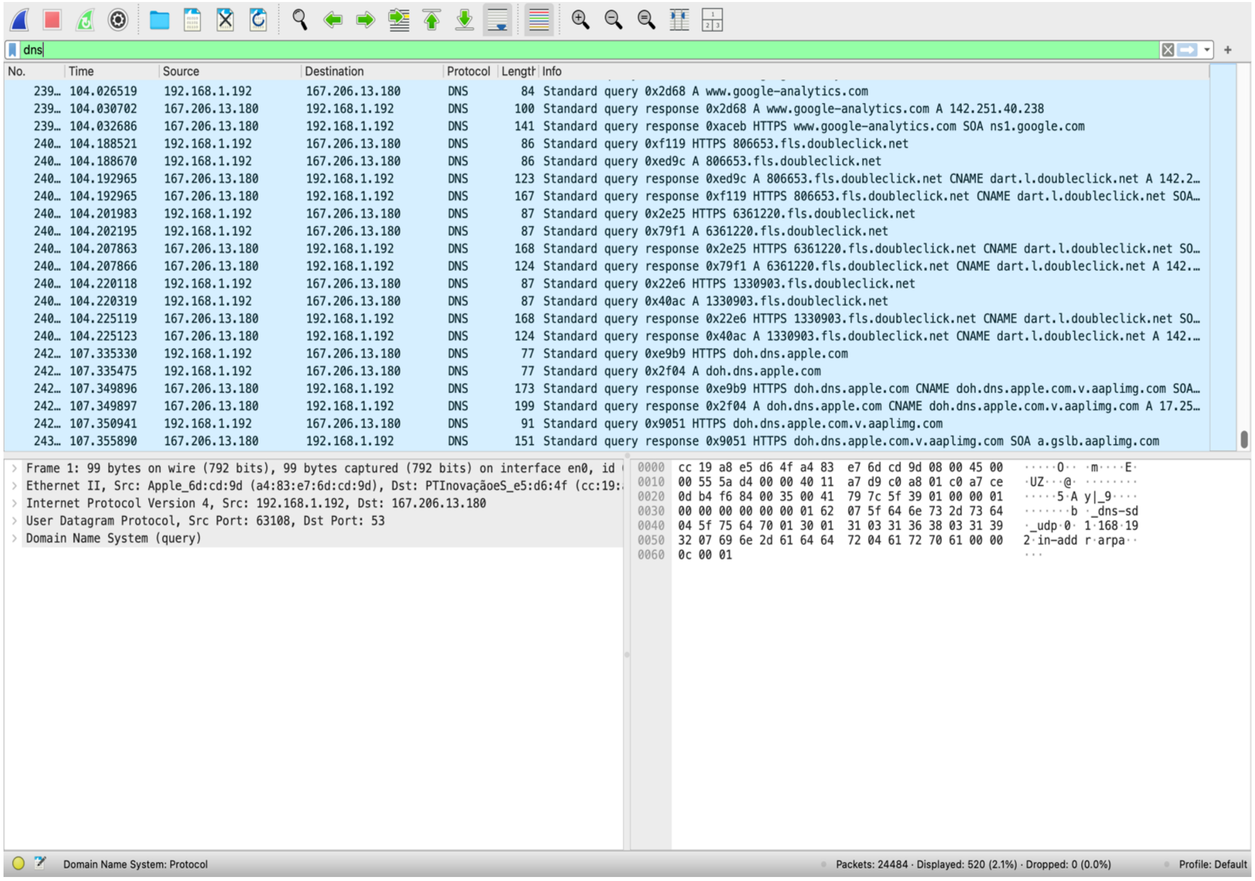
wireshark_Wi-FiHZKF12.pcapng

Packets: 24484 · Displayed: 17 (0.1%) · Dropped: 0 (0.0%)

Profile: Default

DNS Queries

- **Filter Used:** DNS
- **Observation:** The system made DNS queries to multiple domains, including:
  - google-analytics.com
  - doubleclick.net
- **Security Risk:** Potential tracking via DNS queries.
- **Recommendation:** Use secure DNS (DNS over HTTPS/DoT).



dns

```
No.     Time        Source          Destination     Protocol Length Info
  239… 104.026519  192.168.1.192   167.206.13.180  DNS       84 Standard query 0x2d68 A www.google-analytics.com
  239… 104.030702  167.206.13.180  192.168.1.192   DNS      100 Standard query response 0x2d68 A www.google-analytics.com A 142.251.40.238
  239… 104.032686  167.206.13.180  192.168.1.192   DNS      141 Standard query response 0xaceb HTTPS www.google-analytics.com SOA ns1.google.com
  240… 104.188521  192.168.1.192   167.206.13.180  DNS       86 Standard query 0xf119 HTTPS 806653.fls.doubleclick.net
  240… 104.188670  192.168.1.192   167.206.13.180  DNS       86 Standard query 0xed9c A 806653.fls.doubleclick.net
  240… 104.192965  167.206.13.180  192.168.1.192   DNS      123 Standard query response 0xed9c A 806653.fls.doubleclick.net CNAME dart.l.doubleclick.net A 142.2…
  240… 104.192965  167.206.13.180  192.168.1.192   DNS      167 Standard query response 0xf119 HTTPS 806653.fls.doubleclick.net CNAME dart.l.doubleclick.net SOA…
  240… 104.201983  192.168.1.192   167.206.13.180  DNS       87 Standard query 0x2e25 HTTPS 6361220.fls.doubleclick.net
  240… 104.202195  192.168.1.192   167.206.13.180  DNS       87 Standard query 0x79f1 A 6361220.fls.doubleclick.net
  240… 104.207863  167.206.13.180  192.168.1.192   DNS      168 Standard query response 0x2e25 HTTPS 6361220.fls.doubleclick.net CNAME dart.l.doubleclick.net SO…
  240… 104.207866  167.206.13.180  192.168.1.192   DNS      124 Standard query response 0x79f1 A 6361220.fls.doubleclick.net CNAME dart.l.doubleclick.net A 142.…
  240… 104.220118  192.168.1.192   167.206.13.180  DNS       87 Standard query 0x22e6 HTTPS 1330903.fls.doubleclick.net
  240… 104.220319  192.168.1.192   167.206.13.180  DNS       87 Standard query 0x40ac A 1330903.fls.doubleclick.net
  240… 104.225119  167.206.13.180  192.168.1.192   DNS      168 Standard query response 0x22e6 HTTPS 1330903.fls.doubleclick.net CNAME dart.l.doubleclick.net SO…
  240… 104.225123  167.206.13.180  192.168.1.192   DNS      124 Standard query response 0x40ac A 1330903.fls.doubleclick.net CNAME dart.l.doubleclick.net A 142.…
  242… 107.335330  192.168.1.192   167.206.13.180  DNS       77 Standard query 0xe9b9 HTTPS doh.dns.apple.com
  242… 107.335475  192.168.1.192   167.206.13.180  DNS       77 Standard query 0x2f04 A doh.dns.apple.com
  242… 107.349896  167.206.13.180  192.168.1.192   DNS      173 Standard query response 0xe9b9 HTTPS doh.dns.apple.com CNAME doh.dns.apple.com.v.aaplimg.com SOA…
  242… 107.349897  167.206.13.180  192.168.1.192   DNS      199 Standard query response 0x2f04 A doh.dns.apple.com CNAME doh.dns.apple.com.v.aaplimg.com A 17.25…
  242… 107.350941  192.168.1.192   167.206.13.180  DNS       91 Standard query 0x9051 HTTPS doh.dns.apple.com.v.aaplimg.com
  243… 107.355890  167.206.13.180  192.168.1.192   DNS      151 Standard query response 0x9051 HTTPS doh.dns.apple.com.v.aaplimg.com SOA a.gslb.aaplimg.com
```

```
> Frame 1: 99 bytes on wire (792 bits), 99 bytes captured (792 bits) on interface en0, id
> Ethernet II, Src: Apple_6d:cd:9d (a4:83:e7:6d:cd:9d), Dst: PTInovaçãoeS_e5:d6:4f (cc:19:
> Internet Protocol Version 4, Src: 192.168.1.192, Dst: 167.206.13.180
> User Datagram Protocol, Src Port: 63108, Dst Port: 53
> Domain Name System (query)
```

```
0000  cc 19 a8 e5 d6 4f a4 83  e7 6d cd 9d 08 00 45 00   ·····O·· ·m····E·
0010  00 55 5a d4 00 00 40 11  a7 d9 c0 a8 01 c0 a7 ce   ·UZ···@· ········
0020  0d b4 f6 84 00 35 00 41  79 7c 5f 39 01 00 00 01   ·····5·A y|_9····
0030  00 00 00 00 00 00 01 62  07 5f 64 6e 73 2d 73 64   ·······b ·_dns-sd
0040  04 5f 75 64 70 01 30 01  31 03 31 36 38 03 31 39   ·_udp·0· 1·168·19
0050  32 07 69 6e 2d 61 64 64  72 04 61 72 70 61 00 00   2·in-add r·arpa··
0060  0c 00 01                                           ···
```

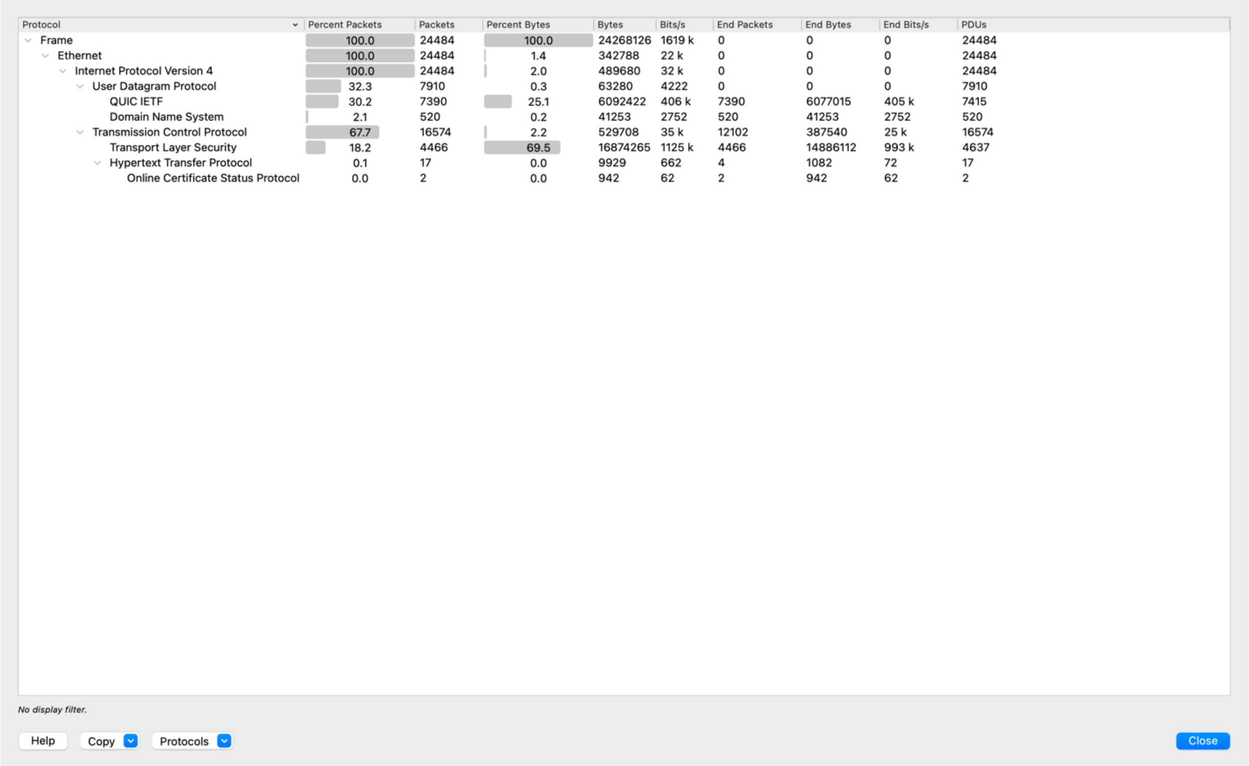
Domain Name System: Protocol

Packets: 24484 · Displayed: 520 (2.1%) · Dropped: 0 (0.0%)

Profile: Default

Protocol Hierarchy Analysis

- **Statistics:**
  - TCP (67.7%)
  - QUIC (30.2%)
  - DNS (2.1%)
- **Observation:** High QUIC traffic, indicating encrypted communications.
- **Security Concern:** QUIC can bypass traditional network monitoring.
- **Recommendation:** Ensure TLS/SSL decryption policies are enforced.



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	24484	100.0	24268126	1619 k	0	0	0	24484
Ethernet	100.0	24484	1.4	342788	22 k	0	0	0	24484
Internet Protocol Version 4	100.0	24484	2.0	489680	32 k	0	0	0	24484
User Datagram Protocol	32.3	7910	0.3	63280	4222	0	0	0	7910
QUIC IETF	30.2	7390	25.1	6092422	406 k	7390	6077015	405 k	7415
Domain Name System	2.1	520	0.2	41253	2752	520	41253	2752	520
Transmission Control Protocol	67.7	16574	2.2	529708	35 k	12102	387540	25 k	16574
Transport Layer Security	18.2	4466	69.5	16874265	1125 k	4466	14886112	993 k	4637
Hypertext Transfer Protocol	0.1	17	0.0	9929	662	4	1082	72	17
Online Certificate Status Protocol	0.0	2	0.0	942	62	2	942	62	2

No display filter.

Security Recommendations

1. **Enable HTTPS Everywhere** – Prevent unencrypted data transmission.
2. **Use Secure DNS (DoH/DoT)** – Encrypt DNS queries to avoid tracking.
3. **Monitor QUIC Traffic** – Ensure security policies cover encrypted traffic.
4. **Implement a VPN** – Encrypt all traffic to prevent sniffing.

Future Steps

- Automating packet analysis using Python scripts.
- Integrating with a SIEM tool like Splunk for real-time monitoring.
- Conducting threat intelligence on network anomalies.

This network traffic analysis highlights key security risks, including unencrypted HTTP traffic and DNS tracking. Implementing secure communication protocols and encryption is necessary to enhance cybersecurity.