Wireshark Network Traffic Analysis Report

1. **Capture Overview**

- **File Name**: wireshark packet capture.pcap
- **Duration**: ~1 minute
- **Interface**: [Wifi]
- **Traffic Source**: the network activity captured in the file 1234.pcap, focusing on protocol usage, IP communication patterns, and notable DNS resolutions. The capture includes encrypted traffic (TLSv1.2 and QUIC), TCP handshakes, and DNS queries primarily involving GitHub and Google services.

Protocol	Description	Count	Notes
TLSv1.2	Encrypted application data	High	Dominant protocol in both captures
TCP	Transport layer acknowledgments	Moderate	Used for TLS sessions and hadnshakes
QUIC	UDP-based encrypted transport protocol	Few	Used for GitHub-related traffic
DNS	Domain name resolution	Few	Queries for www.google.com and github.com

2. IP Communication Summary

- IPv6 Traffic

- **Source/Destination Pairs**:
  - 2405:200:1630:a04::1 ↔ 2409:40c4:211f:d674::
  - 2409:40c4:211f:d674:: ↔ 64:ff9b::23c9:5274, 64:ff9b::c7e8:655b, 64:ff9b::11496:b1ae
- **Purpose**: TLSv1.2 encrypted communication, likely HTTPS sessions.

- IPv4 Traffic

- **Source/Destination**:
  - 10.253.209.169 ↔ 10.253.209.10
- **Purpose**: DNS queries and responses for www.google.com

3. TLSv1.2 Activity

- **Application Data Packets**: Numerous exchanges between IPv6 endpoints.
- **Session Characteristics**:
  - Repeated bidirectional TLS application data.
  - TCP ACK packets interspersed, confirming reliable delivery.
- **Likely Use Case**: Secure web browsing or API communication.

Query Type	Domain	Response IP(s)
A	www.google.com	142.250.182.228
AAAA	www.google.com	2404:6800:4002:805::2004
A/AAAA	Github.com	Multiple IPv6 and IPv4 addresses

 Observation: DNS queries precede TLS sessions, indicating hostname resolution before secure communication.

5. QUIC Protocol Insight

- **QUIC Packets**: Observed in GitHub-related traffic.
- **Transport**: UDP-based, used for faster encrypted communication.
- **Implication**: GitHub services may be leveraging QUIC for performance.

6. Notable Patterns

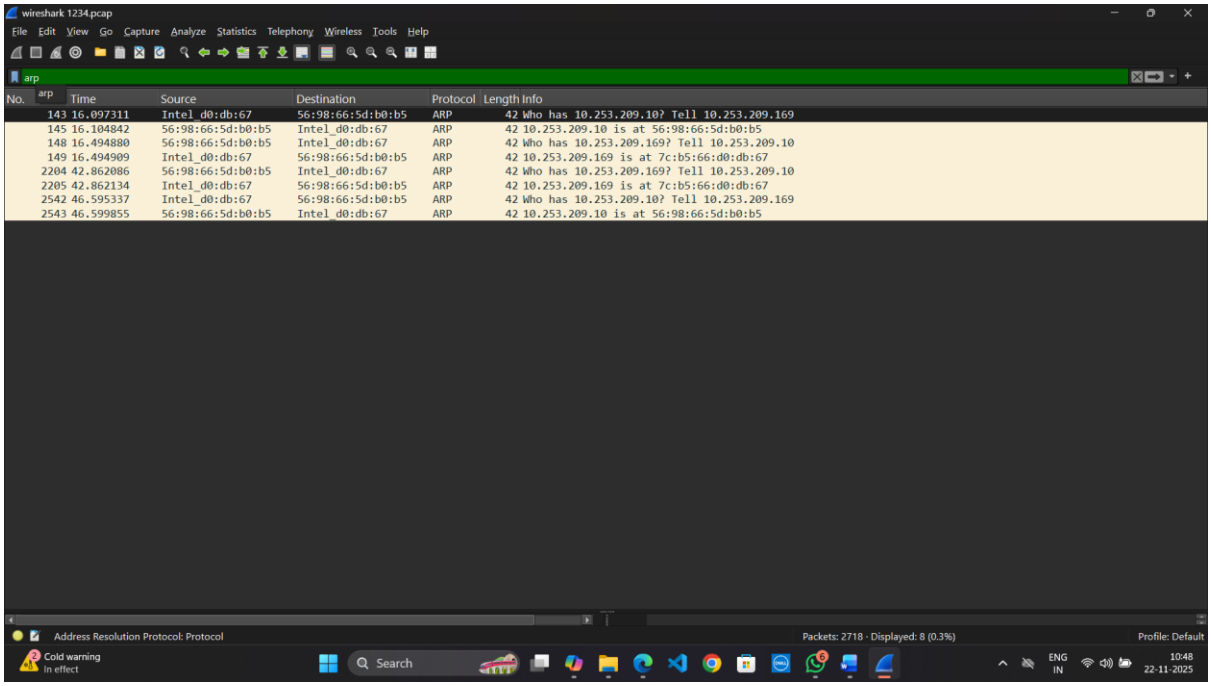
- **Repeated TLS exchanges**: Suggest persistent secure sessions.
- **Multiple destination IPs**: Indicates CDN or load-balanced architecture.
- **DNS-to-TLS flow**: Typical of HTTPS browsing behavior.

7. Security and Performance Observations

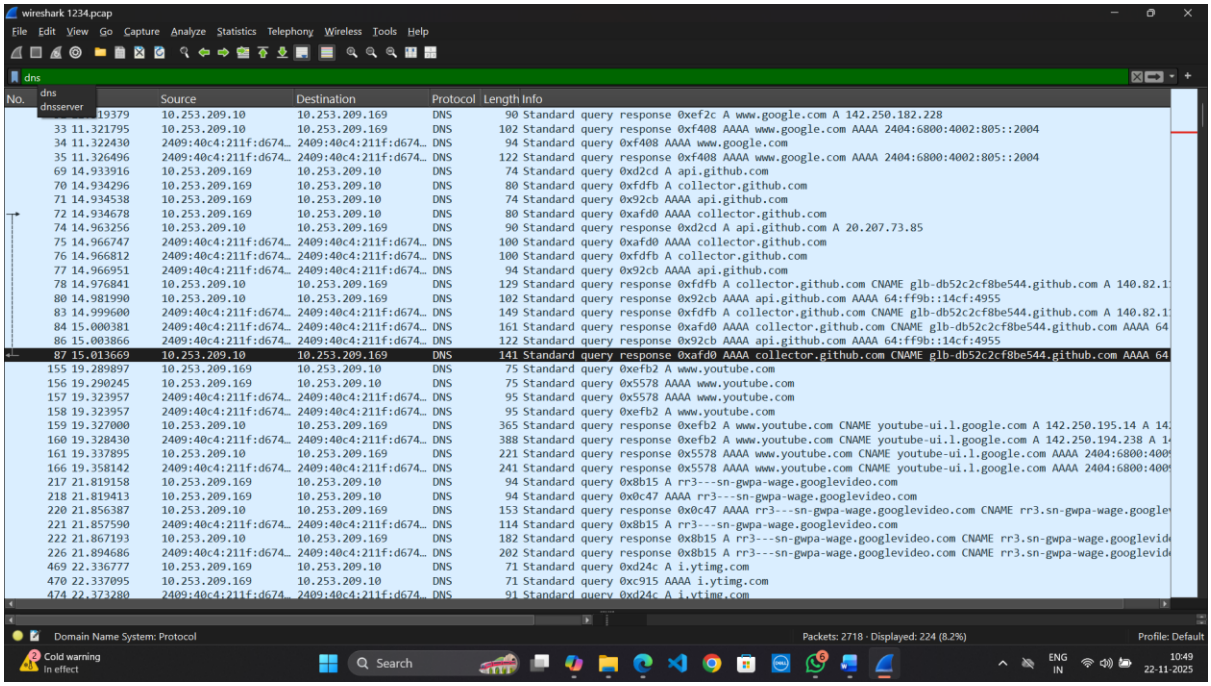
- ✅ **Encryption**: TLSv1.2 and QUIC ensure confidentiality.
- ✅ **IPv6 Usage**: Modern addressing, possibly mobile or cloud-based endpoints.
- ⚠️ **No anomalies detected**: No malformed packets, retransmissions, or alerts.

< -- Filtering by Protocols -- >

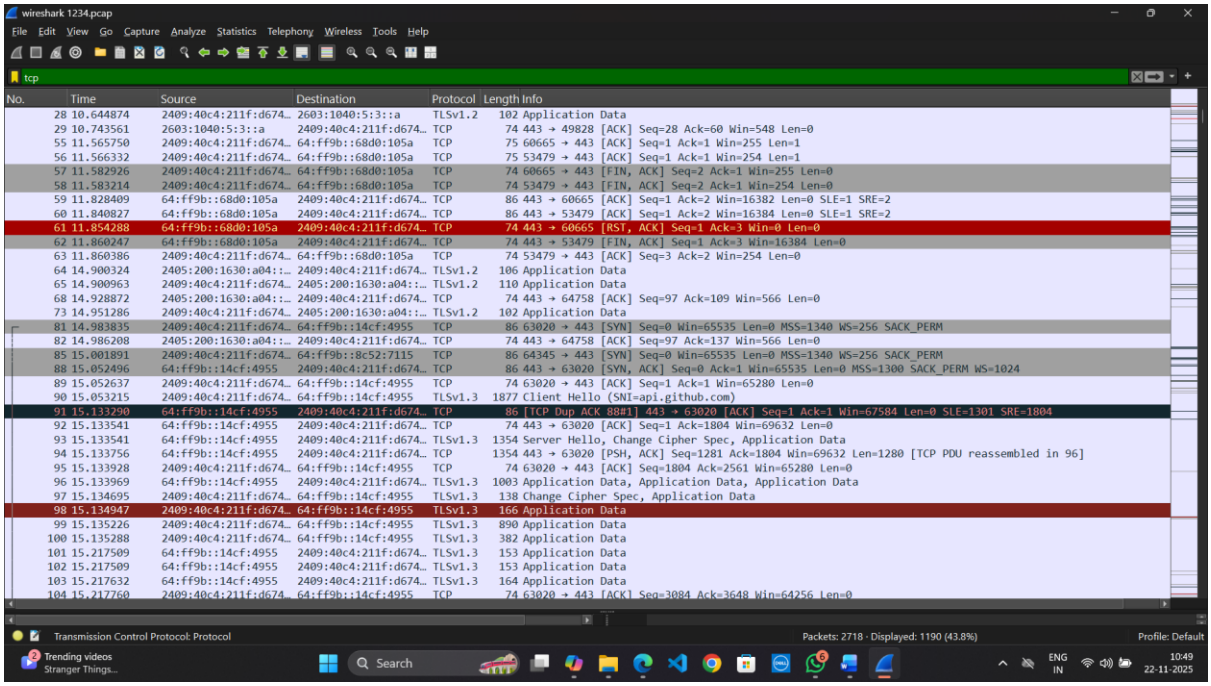
ARP--



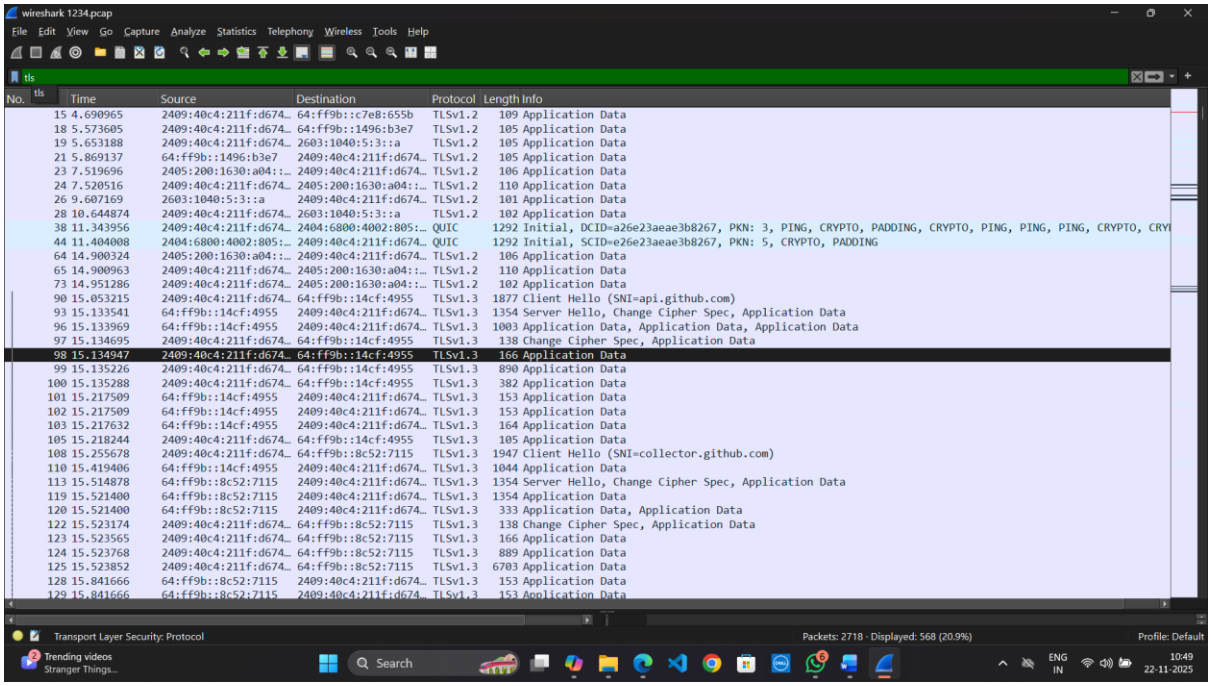
DNS—


wireshark 1234.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Source Destination Protocol Length Info
33 11.321795 10.253.209.10 10.253.209.169 DNS 102 Standard query response 0xf408 AAAA www.google.com AAAA 2404:6800:4002:805::2004
34 11.322430 2409:40c4:211f:d674… 2409:40c4:211f:d674… DNS 94 Standard query 0xf408 AAAA www.google.com
35 11.326496 2409:40c4:211f:d674… 2409:40c4:211f:d674… DNS 122 Standard query response 0xf408 AAAA www.google.com AAAA 2404:6800:4002:805::2004
69 14.933916 10.253.209.169 10.253.209.10 DNS 74 Standard query 0xd2cd A api.github.com
70 14.934296 10.253.209.169 10.253.209.10 DNS 80 Standard query 0xfdfb A collector.github.com
71 14.934538 10.253.209.169 10.253.209.10 DNS 74 Standard query 0x92cb AAAA api.github.com
72 14.934678 10.253.209.169 10.253.209.10 DNS 80 Standard query 0xafd0 AAAA collector.github.com
74 14.963256 10.253.209.10 10.253.209.169 DNS 90 Standard query response 0xd2cd A api.github.com A 20.207.73.85
75 14.966747 2409:40c4:211f:d674… 2409:40c4:211f:d674… DNS 100 Standard query 0xafd0 AAAA collector.github.com
76 14.966812 2409:40c4:211f:d674… 2409:40c4:211f:d674… DNS 100 Standard query 0xfdfb A collector.github.com
77 14.966951 2409:40c4:211f:d674… 2409:40c4:211f:d674… DNS 94 Standard query 0x92cb AAAA api.github.com
78 14.976841 10.253.209.10 10.253.209.169 DNS 129 Standard query response 0xfdfb A collector.github.com CNAME glb-db52c2cf8be544.github.com A 140.82.1
80 14.981990 10.253.209.10 10.253.209.169 DNS 102 Standard query response 0x92cb AAAA api.github.com AAAA 64:ff9b::14cf:4955
83 14.999600 2409:40c4:211f:d674… 2409:40c4:211f:d674… DNS 149 Standard query response 0xfdfb A collector.github.com CNAME glb-db52c2cf8be544.github.com A 140.82.1
84 15.000381 2409:40c4:211f:d674… 2409:40c4:211f:d674… DNS 161 Standard query response 0xafd0 AAAA collector.github.com CNAME glb-db52c2cf8be544.github.com AAAA 64
86 15.003866 2409:40c4:211f:d674… 2409:40c4:211f:d674… DNS 122 Standard query response 0x92cb AAAA api.github.com AAAA 64:ff9b::14cf:4955
87 15.013669 10.253.209.10 10.253.209.169 DNS 141 Standard query response 0xafd0 AAAA collector.github.com CNAME glb-db52c2cf8be544.github.com AAAA 64
155 19.289897 10.253.209.169 10.253.209.10 DNS 75 Standard query 0xefb2 A www.youtube.com
156 19.290245 10.253.209.169 10.253.209.10 DNS 75 Standard query 0x5578 AAAA www.youtube.com
157 19.323957 2409:40c4:211f:d674… 2409:40c4:211f:d674… DNS 95 Standard query 0x5578 AAAA www.youtube.com
158 19.323957 2409:40c4:211f:d674… 2409:40c4:211f:d674… DNS 95 Standard query 0xefb2 A www.youtube.com
159 19.327000 10.253.209.10 10.253.209.169 DNS 365 Standard query response 0xefb2 A www.youtube.com CNAME youtube-ui.l.google.com A 142.250.195.14 A 14
160 19.328430 2409:40c4:211f:d674… 2409:40c4:211f:d674… DNS 388 Standard query response 0xefb2 A www.youtube.com CNAME youtube-ui.l.google.com A 142.250.194.238 A 1
161 19.337895 10.253.209.10 10.253.209.169 DNS 221 Standard query response 0x5578 AAAA www.youtube.com CNAME youtube-ui.l.google.com AAAA 2404:6800:400
166 19.358142 2409:40c4:211f:d674… 2409:40c4:211f:d674… DNS 241 Standard query response 0x5578 AAAA www.youtube.com CNAME youtube-ui.l.google.com AAAA 2404:6800:400
217 21.819158 10.253.209.169 10.253.209.10 DNS 94 Standard query 0x8b15 A rr3---sn-gwpa-wage.googlevideo.com
218 21.819413 10.253.209.169 10.253.209.10 DNS 94 Standard query 0x0c47 AAAA rr3---sn-gwpa-wage.googlevideo.com
220 21.856387 10.253.209.10 10.253.209.169 DNS 153 Standard query response 0x0c47 AAAA rr3---sn-gwpa-wage.googlevideo.com CNAME rr3.sn-gwpa-wage.google
221 21.857590 2409:40c4:211f:d674… 2409:40c4:211f:d674… DNS 114 Standard query 0x8b15 A rr3---sn-gwpa-wage.googlevideo.com
222 21.867193 10.253.209.10 10.253.209.169 DNS 182 Standard query response 0x8b15 A rr3---sn-gwpa-wage.googlevideo.com CNAME rr3.sn-gwpa-wage.googlevid
226 21.894686 2409:40c4:211f:d674… 2409:40c4:211f:d674… DNS 202 Standard query response 0x8b15 A rr3---sn-gwpa-wage.googlevideo.com CNAME rr3.sn-gwpa-wage.googlevid
469 22.336777 10.253.209.169 10.253.209.10 DNS 71 Standard query 0xd24c A i.ytimg.com
470 22.337095 10.253.209.169 10.253.209.10 DNS 71 Standard query 0xc915 AAAA i.ytimg.com
474 22.373280 2409:40c4:211f:d674… 2409:40c4:211f:d674… DNS 91 Standard query 0xd24c A i.ytimg.com
Domain Name System: Protocol
Packets: 2718 · Displayed: 224 (8.2%)
Profile: Default
Cold warning
In effect
Search
ENG
IN
10:49
22-11-2025

TCP --


wireshark 1234.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
28 10.644874 2409:40c4:211f:d674… 2603:1040:5:3::a TLSv1.2 102 Application Data
29 10.743561 2603:1040:5:3::a 2409:40c4:211f:d674… TCP 74 443 → 49828 [ACK] Seq=28 Ack=60 Win=548 Len=0
55 11.565750 2409:40c4:211f:d674… 64:ff9b::68d0:105a TCP 75 60665 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
56 11.566332 2409:40c4:211f:d674… 64:ff9b::68d0:105a TCP 75 53479 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1
57 11.582926 2409:40c4:211f:d674… 64:ff9b::68d0:105a TCP 74 60665 → 443 [FIN, ACK] Seq=2 Ack=1 Win=255 Len=0
58 11.583214 2409:40c4:211f:d674… 64:ff9b::68d0:105a TCP 74 53479 → 443 [FIN, ACK] Seq=2 Ack=1 Win=254 Len=0
59 11.828409 64:ff9b::68d0:105a 2409:40c4:211f:d674… TCP 86 443 → 60665 [ACK] Seq=1 Ack=2 Win=16382 Len=0 SLE=1 SRE=2
60 11.840827 64:ff9b::68d0:105a 2409:40c4:211f:d674… TCP 86 443 → 53479 [ACK] Seq=1 Ack=2 Win=16384 Len=0 SLE=1 SRE=2
61 11.854288 64:ff9b::68d0:105a 2409:40c4:211f:d674… TCP 74 443 → 60665 [RST, ACK] Seq=1 Ack=3 Win=0 Len=0
62 11.860247 64:ff9b::68d0:105a 2409:40c4:211f:d674… TCP 74 443 → 53479 [FIN, ACK] Seq=1 Ack=3 Win=16384 Len=0
63 11.860386 2409:40c4:211f:d674… 64:ff9b::68d0:105a TCP 74 53479 → 443 [ACK] Seq=3 Ack=2 Win=254 Len=0
64 14.900324 2405:200:1630:a04::… 2409:40c4:211f:d674… TLSv1.2 106 Application Data
65 14.900963 2409:40c4:211f:d674… 2405:200:1630:a04::… TLSv1.2 110 Application Data
68 14.928872 2405:200:1630:a04::… 2409:40c4:211f:d674… TCP 74 443 → 64758 [ACK] Seq=97 Ack=109 Win=566 Len=0
73 14.951286 2409:40c4:211f:d674… 2405:200:1630:a04::… TLSv1.2 102 Application Data
81 14.983835 2409:40c4:211f:d674… 64:ff9b::14cf:4955 TCP 86 63020 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1340 WS=256 SACK_PERM
82 14.986208 2405:200:1630:a04::… 2409:40c4:211f:d674… TCP 74 443 → 64758 [ACK] Seq=97 Ack=137 Win=566 Len=0
85 15.001891 2409:40c4:211f:d674… 64:ff9b::8c52:7115 TCP 86 64345 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1340 WS=256 SACK_PERM
88 15.052496 64:ff9b::14cf:4955 2409:40c4:211f:d674… TCP 86 443 → 63020 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1300 SACK_PERM WS=1024
89 15.052637 2409:40c4:211f:d674… 64:ff9b::14cf:4955 TCP 74 63020 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
90 15.053215 2409:40c4:211f:d674… 64:ff9b::14cf:4955 TLSv1.3 1877 Client Hello (SNI=api.github.com)
91 15.133290 64:ff9b::14cf:4955 2409:40c4:211f:d674… TCP 86 [TCP Dup ACK 88#1] 443 → 63020 [ACK] Seq=1 Ack=1 Win=67584 Len=0 SLE=1301 SRE=1804
92 15.133541 64:ff9b::14cf:4955 2409:40c4:211f:d674… TCP 74 443 → 63020 [ACK] Seq=1 Ack=1804 Win=69632 Len=0
93 15.133541 64:ff9b::14cf:4955 2409:40c4:211f:d674… TLSv1.3 1354 Server Hello, Change Cipher Spec, Application Data
94 15.133756 64:ff9b::14cf:4955 2409:40c4:211f:d674… TCP 1354 443 → 63020 [PSH, ACK] Seq=1281 Ack=1804 Win=69632 Len=1280 [TCP PDU reassembled in 96]
95 15.133928 2409:40c4:211f:d674… 64:ff9b::14cf:4955 TCP 74 63020 → 443 [ACK] Seq=1804 Ack=2561 Win=65280 Len=0
96 15.133969 64:ff9b::14cf:4955 2409:40c4:211f:d674… TLSv1.3 1003 Application Data, Application Data, Application Data
97 15.134695 2409:40c4:211f:d674… 64:ff9b::14cf:4955 TLSv1.3 138 Change Cipher Spec, Application Data
98 15.134947 2409:40c4:211f:d674… 64:ff9b::14cf:4955 TLSv1.3 166 Application Data
99 15.135226 2409:40c4:211f:d674… 64:ff9b::14cf:4955 TLSv1.3 890 Application Data
100 15.135288 2409:40c4:211f:d674… 64:ff9b::14cf:4955 TLSv1.3 382 Application Data
101 15.217509 64:ff9b::14cf:4955 2409:40c4:211f:d674… TLSv1.3 153 Application Data
102 15.217509 64:ff9b::14cf:4955 2409:40c4:211f:d674… TLSv1.3 153 Application Data
103 15.217632 64:ff9b::14cf:4955 2409:40c4:211f:d674… TLSv1.3 164 Application Data
104 15.217760 2409:40c4:211f:d674… 64:ff9b::14cf:4955 TCP 74 63020 → 443 [ACK] Seq=3084 Ack=3648 Win=64256 Len=0
Transmission Control Protocol: Protocol
Packets: 2718 · Displayed: 1190 (43.8%)
Profile: Default
Trending videos
Stranger Things...
Search
ENG
IN
10:49
22-11-2025

TSLv1.2 –


wireshark 1234.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tls
No. Time Source Destination Protocol Length Info
15 4.690965 2409:40c4:211f:d674… 64:ff9b::c7e8:655b TLSv1.2 109 Application Data
18 5.573605 2409:40c4:211f:d674… 64:ff9b::1496:b3e7 TLSv1.2 105 Application Data
19 5.653188 2409:40c4:211f:d674… 2603:1040:5:3::a TLSv1.2 105 Application Data
21 5.869137 64:ff9b::1496:b3e7 2409:40c4:211f:d674… TLSv1.2 105 Application Data
23 7.519696 2405:200:1630:a04::… 2409:40c4:211f:d674… TLSv1.2 106 Application Data
24 7.520516 2409:40c4:211f:d674… 2405:200:1630:a04::… TLSv1.2 110 Application Data
26 9.607169 2603:1040:5:3::a 2409:40c4:211f:d674… TLSv1.2 101 Application Data
28 10.644874 2409:40c4:211f:d674… 2603:1040:5:3::a TLSv1.2 102 Application Data
38 11.343956 2409:40c4:211f:d674… 2404:6800:4002:805:… QUIC 1292 Initial, DCID=a26e23aeae3b8267, PKN: 3, PING, CRYPTO, PADDING, CRYPTO, PING, PING, PING, CRYPTO, CRY
44 11.404008 2404:6800:4002:805:… 2409:40c4:211f:d674… QUIC 1292 Initial, SCID=e26e23aeae3b8267, PKN: 5, CRYPTO, PADDING
64 14.900324 2405:200:1630:a04::… 2409:40c4:211f:d674… TLSv1.2 106 Application Data
65 14.900963 2409:40c4:211f:d674… 2405:200:1630:a04::… TLSv1.2 110 Application Data
73 14.951286 2409:40c4:211f:d674… 2405:200:1630:a04::… TLSv1.2 102 Application Data
90 15.053215 2409:40c4:211f:d674… 64:ff9b::14cf:4955 TLSv1.3 1877 Client Hello (SNI=api.github.com)
93 15.133541 64:ff9b::14cf:4955 2409:40c4:211f:d674… TLSv1.3 1354 Server Hello, Change Cipher Spec, Application Data
96 15.133969 64:ff9b::14cf:4955 2409:40c4:211f:d674… TLSv1.3 1003 Application Data, Application Data, Application Data
97 15.134695 2409:40c4:211f:d674… 64:ff9b::14cf:4955 TLSv1.3 138 Change Cipher Spec, Application Data
98 15.134947 2409:40c4:211f:d674… 64:ff9b::14cf:4955 TLSv1.3 166 Application Data
99 15.135226 2409:40c4:211f:d674… 64:ff9b::14cf:4955 TLSv1.3 890 Application Data
100 15.135288 2409:40c4:211f:d674… 64:ff9b::14cf:4955 TLSv1.3 382 Application Data
101 15.217509 64:ff9b::14cf:4955 2409:40c4:211f:d674… TLSv1.3 153 Application Data
102 15.217509 64:ff9b::14cf:4955 2409:40c4:211f:d674… TLSv1.3 153 Application Data
103 15.217632 64:ff9b::14cf:4955 2409:40c4:211f:d674… TLSv1.3 164 Application Data
105 15.218244 2409:40c4:211f:d674… 64:ff9b::14cf:4955 TLSv1.3 105 Application Data
108 15.255678 2409:40c4:211f:d674… 64:ff9b::8c52:7115 TLSv1.3 1947 Client Hello (SNI=collector.github.com)
110 15.419406 64:ff9b::14cf:4955 2409:40c4:211f:d674… TLSv1.3 1044 Application Data
113 15.514878 64:ff9b::8c52:7115 2409:40c4:211f:d674… TLSv1.3 1354 Server Hello, Change Cipher Spec, Application Data
119 15.521400 64:ff9b::8c52:7115 2409:40c4:211f:d674… TLSv1.3 1354 Application Data
120 15.521400 64:ff9b::8c52:7115 2409:40c4:211f:d674… TLSv1.3 333 Application Data, Application Data
122 15.523174 2409:40c4:211f:d674… 64:ff9b::8c52:7115 TLSv1.3 138 Change Cipher Spec, Application Data
123 15.523565 2409:40c4:211f:d674… 64:ff9b::8c52:7115 TLSv1.3 166 Application Data
124 15.523768 2409:40c4:211f:d674… 64:ff9b::8c52:7115 TLSv1.3 889 Application Data
125 15.523852 2409:40c4:211f:d674… 64:ff9b::8c52:7115 TLSv1.3 6703 Application Data
128 15.841666 64:ff9b::8c52:7115 2409:40c4:211f:d674… TLSv1.3 153 Application Data
129 15.841666 64:ff9b::8c52:7115 2409:40c4:211f:d674… TLSv1.3 153 Application Data
Transport Layer Security: Protocol
Packets: 2718 · Displayed: 568 (20.9%)
Profile: Default
Trending videos
Stranger Things...
Search
ENG
IN
10:49
22-11-2025