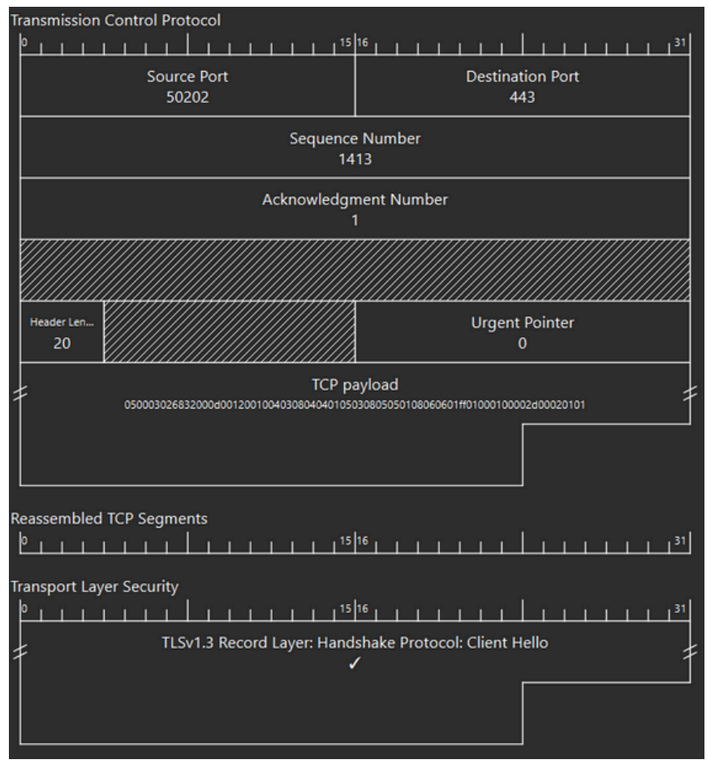
```
▼ Certificate […]: 308207c6308205aea00302010202133300003a1474c989eeb85788200
  ▼ signedCertificate
      version: v3 (2)
      serialNumber: 0x33000003a1474c989eeb8578820000000003a1
    ▼ signature (sha256WithRSAEncryption)
        Algorithm Id: 1.2.840.113549.1.1.11 (sha256WithRSAEncryption)
    ▼ issuer: rdnSequence (0)
```

```
▼ validity
  ▼ notBefore: utcTime (0)
      utcTime: 2025-05-17 02:31:11 (UTC)
  ▼ notAfter: utcTime (0)
      utcTime: 2026-05-17 02:31:11 (UTC)
```

```
▼ Extension: signature_algorithms (len=18)
    Type: signature_algorithms (13)
    Length: 18
    Signature Hash Algorithms Length: 16
  ▼ Signature Hash Algorithms (8 algorithms)
    ▼ Signature Algorithm: ecdsa_secp256r1_sha256 (0x0403)
        Signature Hash Algorithm Hash: SHA256 (4)
        Signature Hash Algorithm Signature: ECDSA (3)
    ▼ Signature Algorithm: rsa_pss_rsae_sha256 (0x0804)
        Signature Hash Algorithm Hash: Unknown (8)
        Signature Hash Algorithm Signature: Unknown (4)
    ▼ Signature Algorithm: rsa_pkcs1_sha256 (0x0401)
        Signature Hash Algorithm Hash: SHA256 (4)
        Signature Hash Algorithm Signature: RSA (1)
    ▼ Signature Algorithm: ecdsa_secp384r1_sha384 (0x0503)
        Signature Hash Algorithm Hash: SHA384 (5)
        Signature Hash Algorithm Signature: ECDSA (3)
    ▼ Signature Algorithm: rsa_pss_rsae_sha384 (0x0805)
        Signature Hash Algorithm Hash: Unknown (8)
        Signature Hash Algorithm Signature: Unknown (5)
    ▼ Signature Algorithm: rsa_pkcs1_sha384 (0x0501)
        Signature Hash Algorithm Hash: SHA384 (5)
        Signature Hash Algorithm Signature: RSA (1)
    ▼ Signature Algorithm: rsa_pss_rsae_sha512 (0x0806)
        Signature Hash Algorithm Hash: Unknown (8)
        Signature Hash Algorithm Signature: Unknown (6)
    ▼ Signature Algorithm: rsa_pkcs1_sha512 (0x0601)
        Signature Hash Algorithm Hash: SHA512 (6)
        Signature Hash Algorithm Signature: RSA (1)
```

```
▼ Cipher Suites (16 suites)
    Cipher Suite: Reserved (GREASE) (0x0a0a)
    Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
    Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
    Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
    Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
    Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
    Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
    Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
    Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
  Compression Methods Length: 1
```




```
▼ Version: TLS 1.2 (0x0303)
  ▼ [Expert Info (Chat/Deprecated): This legacy_version field MUST be ignored. Tl
      [This legacy_version field MUST be ignored. The supported_versions extensi
      [Severity level: Chat]
      [Group: Deprecated]
  Random: bf06347c748b540421b4328646659f9036d21c8f7d6a554f9158a422d73c925e
  Session ID Length: 32
  Session ID: 6f876a59015919abeda97ab6bc5c84109e016db54855c3cb24610bfb9eda7d38
  Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
  Compression Method: null (0)
  Extensions Length: 1134
```

tls

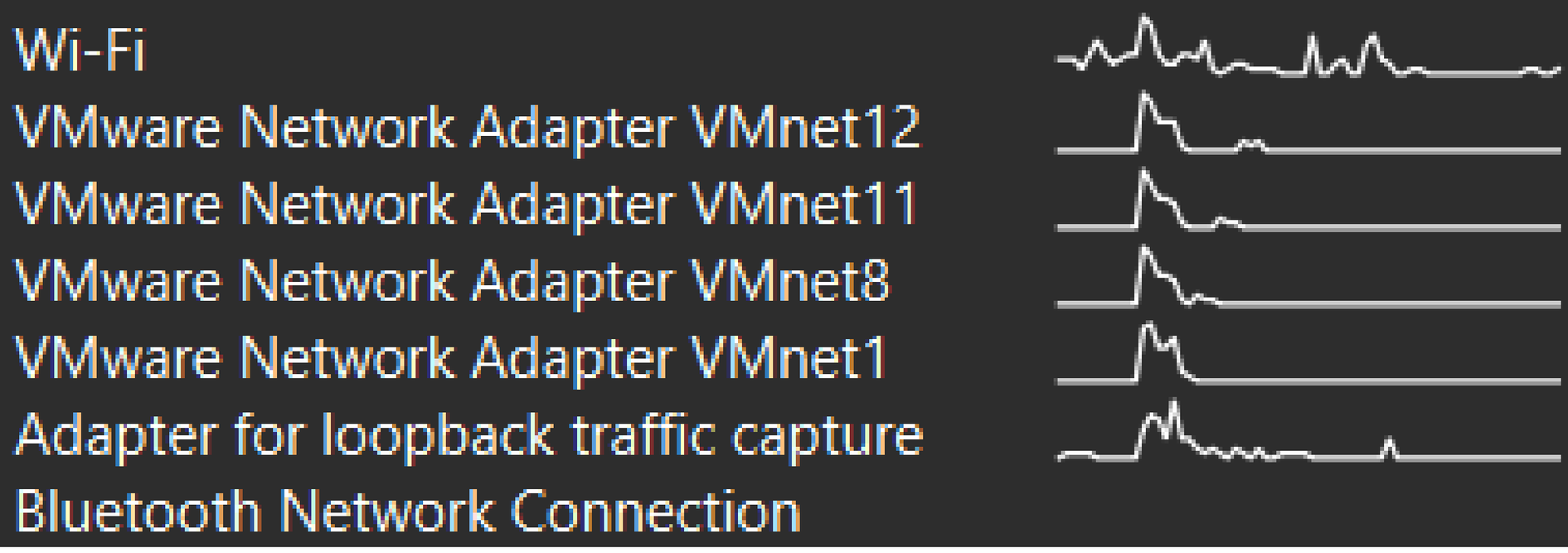
	Time	Source	Destination	Protocol	Length	Info
7830	68.697284	192.168.1.5	52.11.244.75	TLSv1.3	151	Application Data
7831	68.697419	192.168.1.5	52.11.244.75	TLSv1.3	897	Application Data
7834	69.084363	52.11.244.75	192.168.1.5	TLSv1.3	653	Application Data
7835	69.084363	52.11.244.75	192.168.1.5	TLSv1.3	85	Application Data
7837	69.086123	192.168.1.5	54.214.39.173	TLSv1.3	144	Application Data
7838	69.086180	192.168.1.5	54.214.39.173	TLSv1.3	908	Application Data
7841	69.427147	192.168.1.5	15.197.167.90	TLSv1.3	600	Application Data
7844	69.427320	192.168.1.5	15.197.167.90	TLSv1.3	849	Application Data
7846	69.430267	54.214.39.173	192.168.1.5	TLSv1.3	172	Application Data
7859	69.476202	15.197.167.90	192.168.1.5	TLSv1.3	89	Application Data
7865	69.506383	192.168.1.5	172.217.24.67	TLSv1.3	405	Client Hello (SNI=update.googleapis.com)
7866	69.506577	192.168.1.5	15.197.167.90	TLSv1.3	89	Application Data
7868	69.529731	172.217.24.67	192.168.1.5	TLSv1.3	1466	Server Hello, Change Cipher Spec

No.	Time	Source	Destination	Protocol	Length	Info
7973	69.882395	54.214.39.173	192.168.1.5	TCP	54	443 → 50198 [FIN, ACK] Seq=4378 Ack=10218 Win=99328 Len=0
7974	69.882473	192.168.1.5	54.214.39.173	TCP	54	50198 → 443 [RST, ACK] Seq=10218 Ack=4378 Win=0 Len=0
7975	69.884599	54.214.39.173	192.168.1.5	TLSv1.3	78	Application Data
7976	69.884599	54.214.39.173	192.168.1.5	TCP	54	443 → 50199 [FIN, ACK] Seq=3431 Ack=1892 Win=45056 Len=0
7977	69.884649	192.168.1.5	54.214.39.173	TCP	54	50199 → 443 [RST, ACK] Seq=1892 Ack=3431 Win=0 Len=0
7978	69.977551	192.168.1.5	104.26.13.218	TCP	54	[TCP Retransmission] 50159 → 443 [FIN, ACK] Seq=1787 Ack=3790 Win=64768 Len=
7979	69.983044	104.18.0.51	192.168.1.5	TCP	66	[TCP Previous segment not captured] 443 → 50163 [ACK] Seq=9123 Ack=9101 Win=
7980	70.055631	104.26.13.218	192.168.1.5	TCP	54	443 → 50184 [FIN, ACK] Seq=4585 Ack=2404 Win=131072 Len=0
7981	70.055710	192.168.1.5	104.26.13.218	TCP	54	50184 → 443 [ACK] Seq=2404 Ack=4586 Win=64000 Len=0
7982	70.057526	192.168.1.5	104.26.13.218	TCP	54	[TCP Retransmission] 50158 → 443 [FIN, ACK] Seq=2327 Ack=16103 Win=65280 Len
7983	70.058026	104.18.0.51	192.168.1.5	TCP	54	443 → 50183 [FIN, ACK] Seq=39708 Ack=3502 Win=131072 Len=0
7984	70.058060	192.168.1.5	104.18.0.51	TCP	54	50183 → 443 [ACK] Seq=3502 Ack=39709 Win=65280 Len=0
7985	70.094762	104.26.13.218	192.168.1.5	TCP	66	[TCP Previous segment not captured] 443 → 50159 [ACK] Seq=3791 Ack=1788 Win=
7986	70.113342	104.18.0.51	192.168.1.5	TCP	54	[TCP Out-Of-Order] 443 → 50163 [FIN, ACK] Seq=9122 Ack=9101 Win=131072 Len=0
7987	70.113406	192.168.1.5	104.18.0.51	TCP	54	50163 → 443 [ACK] Seq=9101 Ack=9123 Win=64512 Len=0
7988	70.129177	104.26.13.218	192.168.1.5	TCP	54	443 → 50158 [FIN, ACK] Seq=16103 Ack=2328 Win=139264 Len=0
7989	70.129298	192.168.1.5	104.26.13.218	TCP	54	50158 → 443 [ACK] Seq=2328 Ack=16104 Win=65280 Len=0
7990	70.217614	192.168.1.5	104.26.13.218	TCP	54	[TCP Retransmission] 50182 → 443 [FIN, ACK] Seq=2090 Ack=1888 Win=65280 Len=
7991	70.722018	104.26.13.218	192.168.1.5	TCP	54	443 → 50182 [FIN, ACK] Seq=1888 Ack=2091 Win=139264 Len=0
7992	70.722018	104.26.13.218	192.168.1.5	TCP	54	[TCP Retransmission] 443 → 50159 [FIN, ACK] Seq=3790 Ack=1788 Win=131072 Len
7993	70.722180	192.168.1.5	104.26.13.218	TCP	54	50182 → 443 [ACK] Seq=2091 Ack=1889 Win=65280 Len=0
7994	70.722349	192.168.1.5	104.26.13.218	TCP	54	50159 → 443 [ACK] Seq=1788 Ack=3791 Win=64768 Len=0

Welcome to Wireshark

Capture

...using this filter: Enter a capture filter ...



No.	Time	Source	Destination	Protocol	Length	Info
7857	69.471015	192.168.1.5	54.214.39.173	TCP	54	50198 → 443 [ACK] Seq=10217 Ack=4354 Win=64256 Len=0
7858	69.471595	192.168.1.1	192.168.1.5	DNS	97	Standard query response 0xc482 A update.googleapis.com A 172.217.24.67
7859	69.476202	15.197.167.90	192.168.1.5	TLSv1.3	89	Application Data
7860	69.487029	192.168.1.5	172.217.24.67	TCP	66	50202 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
7861	69.498305	192.168.1.5	142.250.193.138	QUIC	74	Protected Payload (KP0), DCID=e0d458e63a366b8d
7862	69.505047	172.217.24.67	192.168.1.5	TCP	66	443 → 50202 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
7863	69.505205	192.168.1.5	172.217.24.67	TCP	54	50202 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
7864	69.506383	192.168.1.5	172.217.24.67	TCP	1466	50202 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=1412 [TCP PDU reassembled in 7865]
7865	69.506383	192.168.1.5	172.217.24.67	TLSv1.3	405	Client Hello (SNI=update.googleapis.com)
7866	69.506577	192.168.1.5	15.197.167.90	TLSv1.3	89	Application Data
7867	69.525281	172.217.24.67	192.168.1.5	TCP	54	443 → 50202 [ACK] Seq=1 Ack=1764 Win=268032 Len=0
7868	69.529731	172.217.24.67	192.168.1.5	TLSv1.3	1466	Server Hello, Change Cipher Spec