

**Connor Schuler
SEC-260-02
STR2026**

Deliverable 1: Image shows the TLS/TCP 3 way handshake, a SYN, SYN/ACK, and ACK.

88.2.259162873	10.0.17.37	104.154.89.105	TLSv1.2	733 Client Hello (SNI=tls-v1-2.badssl.com)
89.2.295273400	104.154.89.105	10.0.17.37	TCP	66 1012 .. 40840 [ACK] Seq=1 Ack=668 Win=64128 Len=0 TSval=37
91.2.2999929214	104.154.89.105	10.0.17.37	TLSv1.2	3085 Server Hello, Certificate, Server Key Exchange, Server He
92.2.299975971	10.0.17.37	104.154.89.105	TCP	66 40840 .. 1012 [ACK] Seq=668 Ack=30209 Win=64128 Len=0 TSval
93.2.311835874	10.0.17.37	104.154.89.105	TLSv1.2	192 Client Key Exchange, Change Cipher Spec, Encrypted Handsh

Deliverable 2: Images shows the issuer of the Certificate, its valid-till date, and the public key for the certificate.

91 2.299979214	104.154.89.105	10.0.17.37	TLSv1.2	3005 Server Hello, Certificate, Server Key Exchange, Server He
92 2.299975971	10.0.17.37	104.154.89.105	TCP	66 40840 -> 1012 [ACK] Seq=668 Ack=3020 Win=64128 Len=0 TSva
93 2.311835874	10.0.17.37	104.154.89.105	TLSv1.2	192 Client Key Exchange, Change Cipher Spec, Encrypted Handsh
95 2.347790222	104.154.89.105	10.0.17.37	TLSv1.2	324 New Session Ticket, Change Cipher Spec, Encrypted Handsh
96 2.352935946	10.0.17.37	104.154.89.105	TLSv1.2	543 Application Data
97 2.3888578293	104.154.89.105	10.0.17.37	TLSv1.2	763 Application Data
98 2.4139131460	10.0.17.37	104.154.89.105	TCP	66 40840 -> 1012 [ACK] Seq=1271 Ack=3915 Win=66176 Len=0 TSva
99 2.679228403	10.0.17.37	104.154.89.105	TLSv1.2	561 Application Data
100 2.716719120	104.154.89.105	10.0.17.37	TLSv1.2	1873 Application Data
101 2.716785996	10.0.17.37	104.154.89.105	TCP	66 40840 -> 1012 [ACK] Seq=1706 Ack=5722 Win=64896 Len=0 TSva
102 2.735184589	10.0.17.37	104.154.89.105	TLSv1.2	563 Application Data

91.2.2999929214	104.154.89.105	10.0.17.37	TLSv1.2	3085 Server Hello, Certificate, Server Key Exchange, Server Name
92.2.299975971	10.0.17.37	104.154.89.105	TCP	66 40840 → 1012 [ACK] Seq=568 Ack=3020 Win=54128 Len=0 TSva
93.2.311835874	10.0.17.37	104.154.89.105	TLSv1.2	192 Client Key Exchange, Change Cipher Spec, Encrypted Handsh
95.2.347799222	104.154.89.105	10.0.17.37	TLSv1.2	324 New Session Ticket, Change Cipher Spec, Encrypted Handsh
96.2.352935946	10.0.17.37	104.154.89.105	TLSv1.2	543 Application Data
97.2.388857293	104.154.89.105	10.0.17.37	TLSv1.2	703 Application Data
98.2.431931466	10.0.17.37	104.154.89.105	TCP	66 40840 → 1012 [ACK] Seq=1271 Ack=3915 Win=66176 Len=0 TSva
99.2.679228403	10.0.17.37	104.154.89.105	TLSv1.2	561 Application Data
100.2.7.16719120	104.154.89.105	10.0.17.37	TLSv1.2	1873 Application Data
101.2.7.16785996	10.0.17.37	104.154.89.105	TCP	66 40840 → 1012 [ACK] Seq=1706 Ack=5722 Win=64896 Len=0 TSva
102.2.7.35184589	10.0.17.37	104.154.89.105	TLSv1.2	563 Application Data