

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	2.299929214	104.154.89.105	10.0.17.37	TLSv1.2	3085 Server Hello, Certificate, Server Key Exchange, Server Hello Done
92	2.299975971	10.0.17.37	104.154.89.105	TCP	66 40840 → 1012 [ACK] Seq=668 Ack=3020 Win=64128 Len=0 TSval=37
93	2.311835874	10.0.17.37	104.154.89.105	TLSv1.2	192 Client Key Exchange, Change Cipher Spec, Encrypted Handshake

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

91	2.299929214	104.154.89.105	10.0.17.37	TLSv1.2	3085 Server Hello, Certificate, Server Key Exchange, Server Hello Done
92	2.299975971	10.0.17.37	104.154.89.105	TCP	66 40840 → 1012 [ACK] Seq=668 Ack=3020 Win=64128 Len=0 TSval=37
93	2.311835874	10.0.17.37	104.154.89.105	TLSv1.2	192 Client Key Exchange, Change Cipher Spec, Encrypted Handshake
95	2.347790222	104.154.89.105	10.0.17.37	TLSv1.2	324 New Session Ticket, Change Cipher Spec, Encrypted Handshake
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	2.431931400	10.0.17.37	104.154.89.105	TCP	66 40840 → 1012 [ACK] Seq=1271 Ack=3915 Win=66176 Len=0 TSval=37
99	2.679228403	10.0.17.37	104.154.89.105	TLSv1.2	501 Application Data
100	2.716719120	104.154.89.105	10.0.17.37	TLSv1.2	1873 Application Data
101	2.716785906	10.0.17.37	104.154.89.105	TCP	66 40840 → 1012 [ACK] Seq=1706 Ack=5722 Win=64896 Len=0 TSval=37
102	2.735184589	10.0.17.37	104.154.89.105	TLSv1.2	563 Application Data

▼ issuer: rdnSequence (0)	0890	31 2e 63 2e 6c 65 6e 63 72 2e 6f 72 67 2f 30 0d	1.c.lenc r..
▼ rdnSequence: 3 items (id-at-commonName=ISRG Root X1,id-at-or	08a0	06 09 2a 06 48 86 f7 0d 01 01 0b 05 00 03 82 02	...H... 5
▼ RDNSequence item: 1 item (id-at-countryName=US)	08b0	01 00 51 37 58 52 a1 22 9b 35 bb 4d ba ce ca 92	...Q7XR... 5
▼ RDNSequence item: 1 item (id-at-organizationName=Internet	08c0	ea 09 f2 fb 54 ec 18 7f f4 3b f4 e1 f9 70 72 c2	...T... ;
▼ RelativeDistinguishedName item (id-at-organizationName=I	08d0	65 e8 20 7d 08 43 72 89 e5 93 b2 a0 87 c6 f4 be	e...} Cr... 5
Object Id: 2.5.4.10 (id-at-organizationName)	08e0	2f bf 5e e5 ae ec 23 7c 9f f5 0f 7a 0d 6f a3 71	/...#... 5
▼ DirectoryString: printableString (1)	08f0	be b5 a5 e2 ae bc ad b6 14 22 9c 01 c6 c1 cf d4	... 5
printableString: Internet Security Research Group	0900	75 b3 b2 80 96 bd ce e0 5c 57 2a a8 1f 70 97 4d	u...VW 5
▼ RDNSequence item: 1 item (id-at-commonName=ISRG Root X1)	0910	70 c8 9d 3f bc 6b e7 37 68 45 4c 27 64 ad fa 94	p...? k 7 hE 5
▼ RelativeDistinguishedName item (id-at-commonName=ISRG Ro	0920	a7 e1 e7 7e 5a 40 e9 f2 28 ec 8a 3b c4 c8 5c 04	...~Z0... (- 5
Object Id: 2.5.4.3 (id-at-commonName)	0930	e3 b8 6e 95 6d 0b b7 38 e0 f5 f3 95 e4 f9 ab 83	...n m 8... 5
▼ DirectoryString: printableString (1)	0940	fc f1 59 b4 6e 2f e9 34 0c 19 c7 10 97 a7 9c 2b	...Y n/ 4... 5
printableString: ISRG Root X1	0950	00 7a 7e dc df 93 e6 c7 b8 e9 98 9f c7 b6 04 61	Z... 5
▼ validity	0960	72 7c f4 ca 34 81 bf 22 30 e8 bd 50 22 ea 64 0a	r...4... 0 5
▼ notBefore: utcTime (0)	0970	fd 92 04 e0 d3 ff 10 c3 de 07 06 43 22 af ea ba	...m...2... 5
▼ notAfter: utcTime (0)	0980	15 e0 6d 84 85 f1 32 02 c5 a9 9a 88 f1 8c 25 02	...m...2... 5
utcTime: 2027-03-12 23:59:59 (UTC)	0990	1a 2c a0 f7 b1 6f 0e d9 bf 34 ad 8b 49 cf 65 c9	...o... 4 5
subject: rdnSequence (0)			

▼ signedCertificate			
version: v3 (2)			
serialNumber: 0x5a00f212d8d4b480f3924157ea298305			
signature (sha256WithRSAEncryption)			
▼ issuer: rdnSequence (0)			
▼ validity			
▼ notBefore: utcTime (0)			
▼ notAfter: utcTime (0)			
utcTime: 2027-03-12 23:59:59 (UTC)			
▼ subject: rdnSequence (0)			
▼ subjectPublicKeyInfo			
algorithm (rsaEncryption)			
▼ subjectPublicKey [...]: 3082010a0202010100a567708dd0568164151761c			
modulus: 0x0a567708dd0568164151761c906d4ad19908c2650379816639254dbd9cc840593ecd3ec081ba00			
publicExponent: 65537			