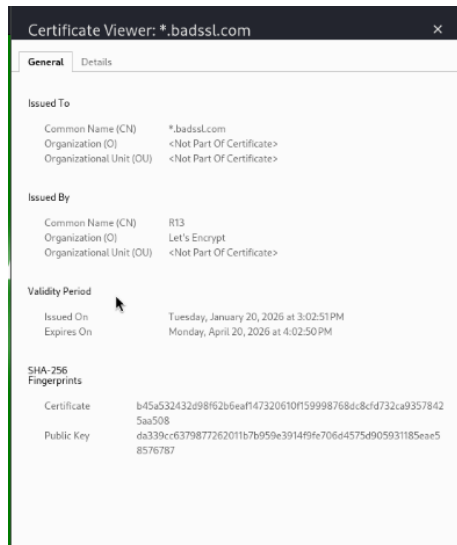


# Connor Schuler

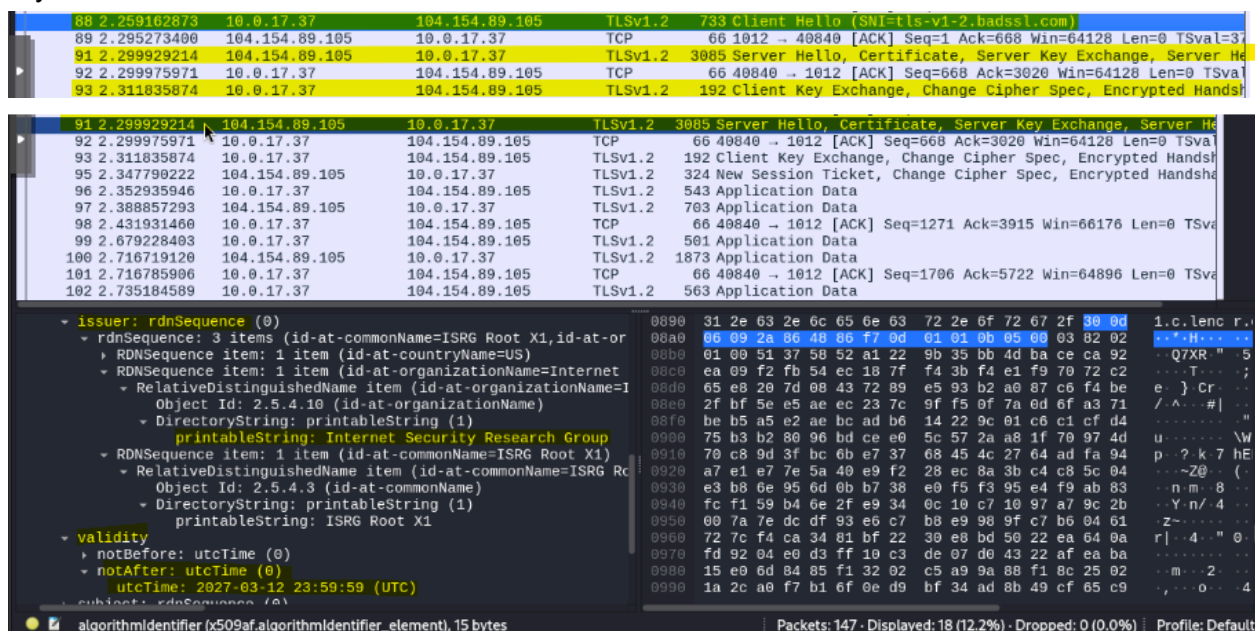
## SEC-260-02

### STR2026

**Deliverable 1:** Image shows the issuer, common name (aka server certificate was assigned to), its validity period, and the public key.



**Deliverable 2:** Images show the 3 packet TLS handshake, a Client Hello (SYN), Server Hello (SYN/ACK), and Key Exchange (ACK). They also show the relevant certificate information: issuer, common name (aka server certificate was assigned to), its validity period, and the public key.



91	2.299929214	104.154.89.105	10.0.17.37	TLSv1.2	3085 Server Hello, Certificate, Server Key Exchange, Server H
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	2.388857293	104.154.89.105	10.0.17.37	TLSv1.2	703 Application Data
98	2.431931460	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	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 TSva
102	2.735184589	10.0.17.37	104.154.89.105	TLSv1.2	563 Application Data

<ul style="list-style-type: none"> <li>signedCertificate <ul style="list-style-type: none"> <li>version: v3 (2)</li> <li>serialNumber: 0x5a00f212d8d4b480f3924157ea298305</li> <li>signature (sha256WithRSAEncryption)</li> <li>issuer: rdnSequence (0)</li> <li>validity <ul style="list-style-type: none"> <li>notBefore: utcTime (0)</li> <li>notAfter: utcTime (0)</li> <li>utcTime: 2027-03-12 23:59:59 (UTC)</li> </ul> </li> <li>subject: rdnSequence (0)</li> <li>subjectPublicKeyInfo <ul style="list-style-type: none"> <li>algorithm (rsaEncryption)</li> <li>subjectPublicKey [...] <ul style="list-style-type: none"> <li>modulus: 0x00a567708dd0568164151761cdb906d4ad19908c2650379816639254dbd9cc840593ecd3ec081ba06</li> <li>publicExponent: 65537</li> </ul> </li> </ul> </li> </ul> </li> </ul>
---