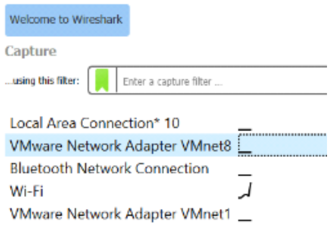
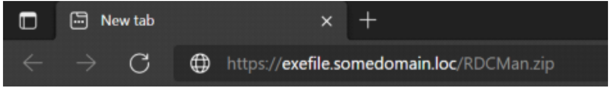
Windows Trace File

Sunday, 23 January 2022 14:53

Starting a new WireShark trace on my VMNet network interface:

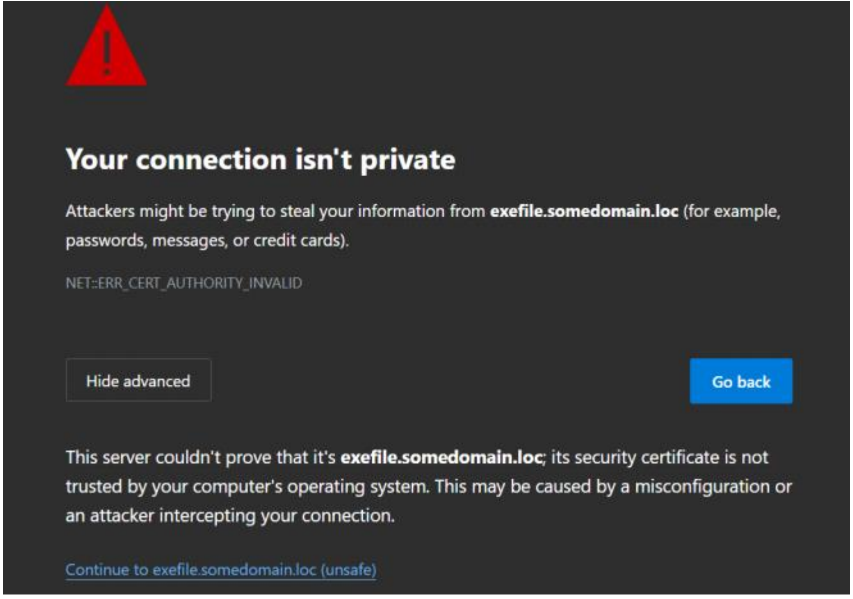

Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
Local Area Connection* 10
VMware Network Adapter VMnet8
Bluetooth Network Connection
Wi-Fi
VMware Network Adapter VMnet1

Browsing to the ZIP file



https://exefile.somedomain.loc/RDCMan.zip

Accepting the untrusted certificate:



Your connection isn't private

Attackers might be trying to steal your information from **exefile.somedomain.loc** (for example, passwords, messages, or credit cards).

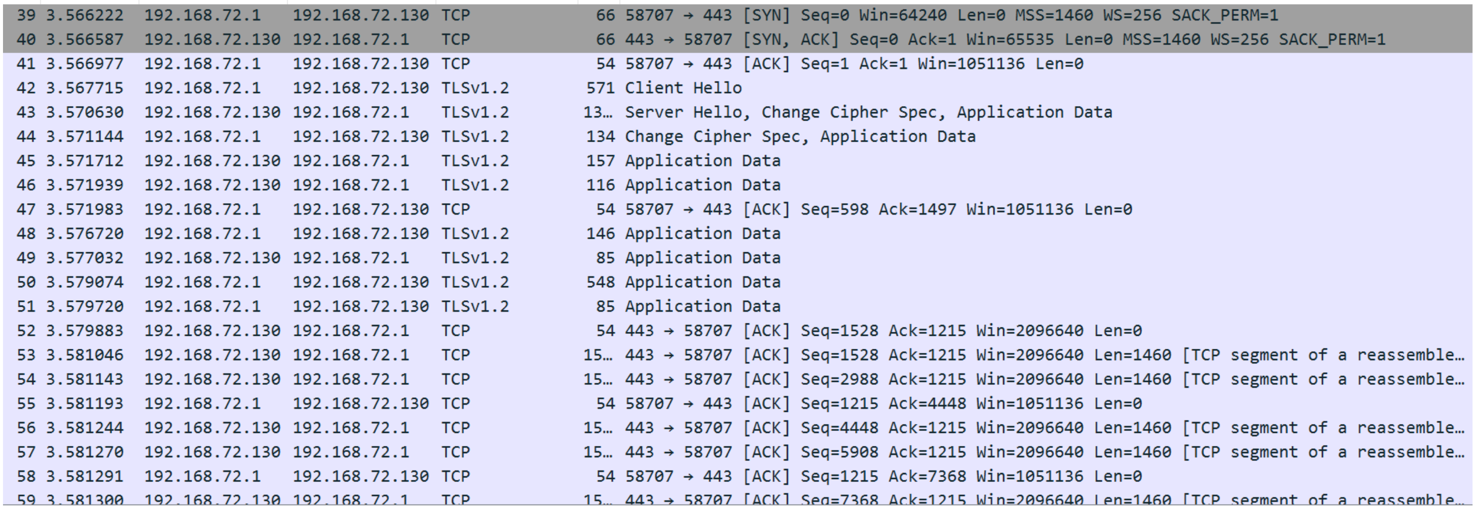
NET::ERR_CERT_AUTHORITY_INVALID

This server couldn't prove that it's **exefile.somedomain.loc**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Continue to exefile.somedomain.loc (unsafe)

Trace File

192.168.72.1 - Client
192.168.72.130 - Server



```
 39 3.566222  192.168.72.1   192.168.72.130 TCP         66 58707 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 40 3.566587  192.168.72.130 192.168.72.1   TCP         66 443 → 58707 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
 41 3.566977  192.168.72.1   192.168.72.130 TCP         54 58707 → 443 [ACK] Seq=1 Ack=1 Win=1051136 Len=0
 42 3.567715  192.168.72.1   192.168.72.130 TLSv1.2    571 Client Hello
 43 3.570630  192.168.72.130 192.168.72.1   TLSv1.2    13… Server Hello, Change Cipher Spec, Application Data
 44 3.571144  192.168.72.1   192.168.72.130 TLSv1.2    134 Change Cipher Spec, Application Data
 45 3.571712  192.168.72.130 192.168.72.1   TLSv1.2    157 Application Data
 46 3.571939  192.168.72.130 192.168.72.1   TLSv1.2    116 Application Data
 47 3.571983  192.168.72.1   192.168.72.130 TCP         54 58707 → 443 [ACK] Seq=598 Ack=1497 Win=1051136 Len=0
 48 3.576720  192.168.72.1   192.168.72.130 TLSv1.2    146 Application Data
 49 3.577032  192.168.72.130 192.168.72.1   TLSv1.2     85 Application Data
 50 3.579074  192.168.72.1   192.168.72.130 TLSv1.2    548 Application Data
 51 3.579720  192.168.72.1   192.168.72.130 TLSv1.2     85 Application Data
 52 3.579883  192.168.72.130 192.168.72.1   TCP         54 443 → 58707 [ACK] Seq=1528 Ack=1215 Win=2096640 Len=0
 53 3.581046  192.168.72.130 192.168.72.1   TCP        15… 443 → 58707 [ACK] Seq=1528 Ack=1215 Win=2096640 Len=1460 [TCP segment of a reassemble…
 54 3.581143  192.168.72.130 192.168.72.1   TCP        15… 443 → 58707 [ACK] Seq=2988 Ack=1215 Win=2096640 Len=1460 [TCP segment of a reassemble…
 55 3.581193  192.168.72.1   192.168.72.130 TCP         54 58707 → 443 [ACK] Seq=1215 Ack=4448 Win=1051136 Len=0
 56 3.581244  192.168.72.130 192.168.72.1   TCP        15… 443 → 58707 [ACK] Seq=4448 Ack=1215 Win=2096640 Len=1460 [TCP segment of a reassemble…
 57 3.581270  192.168.72.130 192.168.72.1   TCP        15… 443 → 58707 [ACK] Seq=5908 Ack=1215 Win=2096640 Len=1460 [TCP segment of a reassemble…
 58 3.581291  192.168.72.1   192.168.72.130 TCP         54 58707 → 443 [ACK] Seq=1215 Ack=7368 Win=1051136 Len=0
 59 3.581300  192.168.72.130 192.168.72.1   TCP        15… 443 → 58707 [ACK] Seq=7368 Ack=1215 Win=2096640 Len=1460 [TCP segment of a reassemble…
```

★ **39-41 TCP Handshake**
Client sends a request to start a TCP Session.
Server responds with a SYN,ACK, client sends back an ACK - session is good to go.
Client and server established a TCP three way handshake.

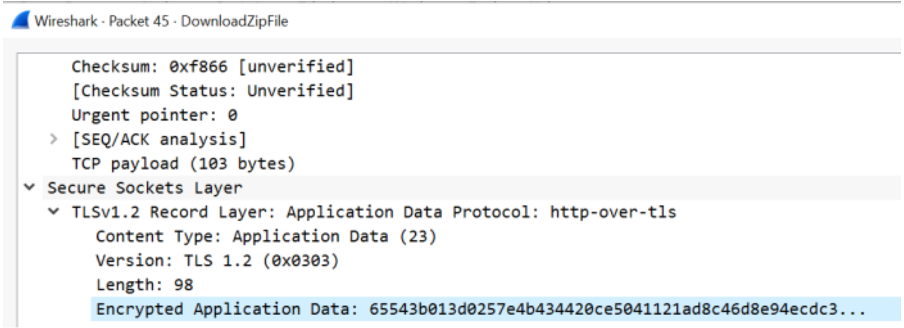
★ **42-44 TLS Handshake**
42 - Client sends a SSL\TLS1.2 Client Hello to start a the SSL\TLS1.2 handshake,
And presents the server with the cypher suites, and all other TLS information

43 - server sends back a Server Hello message, and presents the client with the server certificate, the

selected cypher suite, and other information.

44 - the client sends back a "change cypher spec" (after the server has sent one), indicates that it will switch to encrypted communication from now on

45 - information payload in the packet is encrypted:



```
      Checksum: 0xf866 [unverified]
      [Checksum Status: Unverified]
      Urgent pointer: 0
    > [SEQ/ACK analysis]
      TCP payload (103 bytes)
  ˅ Secure Sockets Layer
    ˅ TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
        Content Type: Application Data (23)
        Version: TLS 1.2 (0x0303)
        Length: 98
        Encrypted Application Data: 65543b013d0257e4b434420ce5041121ad8c46d8e94ecdc3...
```

TCP Session for file download is starting