Cryptography

> DAT159

By Sondre Gjellestad and Arne Molland

Task 1

After setting up the certificate, the connection works.

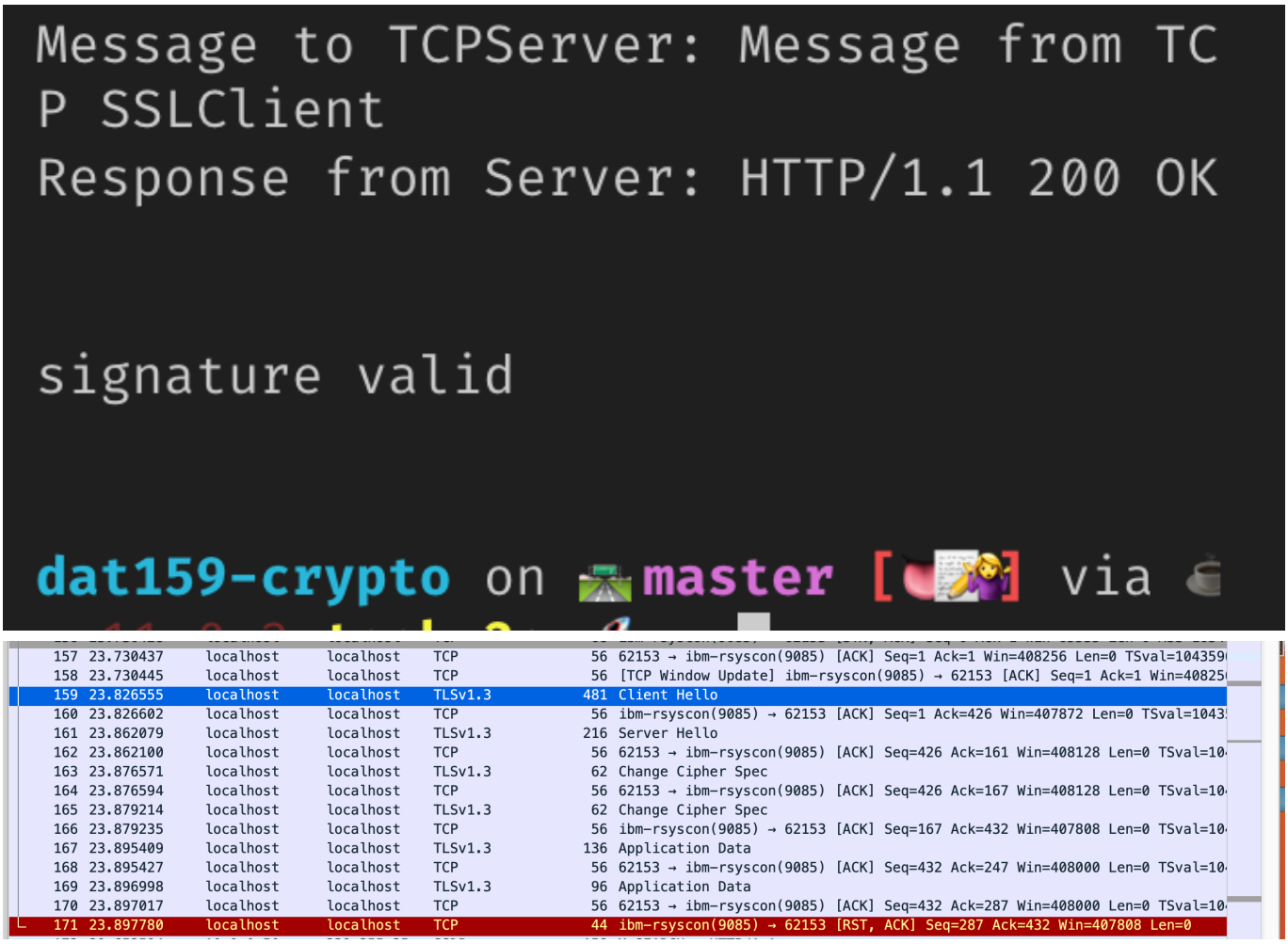
```
Message to TCPServer: Message from TCP SSLClient
Response from Server: HTTP/1.1 200 OK
```

```
Run | Debug
public static void main(String[] args) throws InvalidKeyException, NoSuchAlgorithmExce
        NoSuchPaddingException, UnrecoverableKeyException, KeyStoreException {
    // Set the truststore dynamically using the system property

    System.setProperty("javax.net.ssl.trustStore", "keys/tcp_truststore");
    System.setProperty("javax.net.ssl.trustStorePassword", "abcdef");

    String message = "Message from TCP SSLClient";
    TCPClientSSLRSA c = new TCPClientSSLRSA(ServerConfig.SERVER, ServerConfig.PORT);
    c.clientProcess(message);
}
```

```
3972 99.315022    localhost    localhost    TLSv1.3      481 Client Hello
3973 99.315047    localhost    localhost    TCP           56 ibm-rsyscon(9085) → 53127 [ACK] Seq=1 Ack=426 Win=407872 Len=0 TSval=114092558
3974 99.370974    localhost    localhost    TLSv1.3      216 Server Hello
3975 99.371001    localhost    localhost    TCP           56 53127 → ibm-rsyscon(9085) [ACK] Seq=426 Ack=161 Win=408128 Len=0 TSval=1140925
3976 99.384994    localhost    localhost    TLSv1.3       62 Change Cipher Spec
3977 99.385018    localhost    localhost    TCP           56 53127 → ibm-rsyscon(9085) [ACK] Seq=426 Ack=167 Win=408128 Len=0 TSval=1140925
3978 99.387538    localhost    localhost    TLSv1.3       62 Change Cipher Spec
3979 99.387555    localhost    localhost    TCP           56 ibm-rsyscon(9085) → 53127 [ACK] Seq=167 Ack=432 Win=407808 Len=0 TSval=1140925
3980 99.400944    localhost    localhost    TLSv1.3      136 Application Data
3981 99.400962    localhost    localhost    TCP           56 53127 → ibm-rsyscon(9085) [ACK] Seq=432 Ack=247 Win=408000 Len=0 TSval=1140925
3982 99.403963    localhost    localhost    TLSv1.3     1004 Application Data
3983 99.403978    localhost    localhost    TCP           56 53127 → ibm-rsyscon(9085) [ACK] Seq=432 Ack=1195 Win=407104 Len=0 TSval=114092
3984 99.464908    localhost    localhost    TLSv1.3      358 Application Data
3985 99.464934    localhost    localhost    TCP           56 53127 → ibm-rsyscon(9085) [ACK] Seq=432 Ack=1497 Win=406784 Len=0 TSval=114092
```

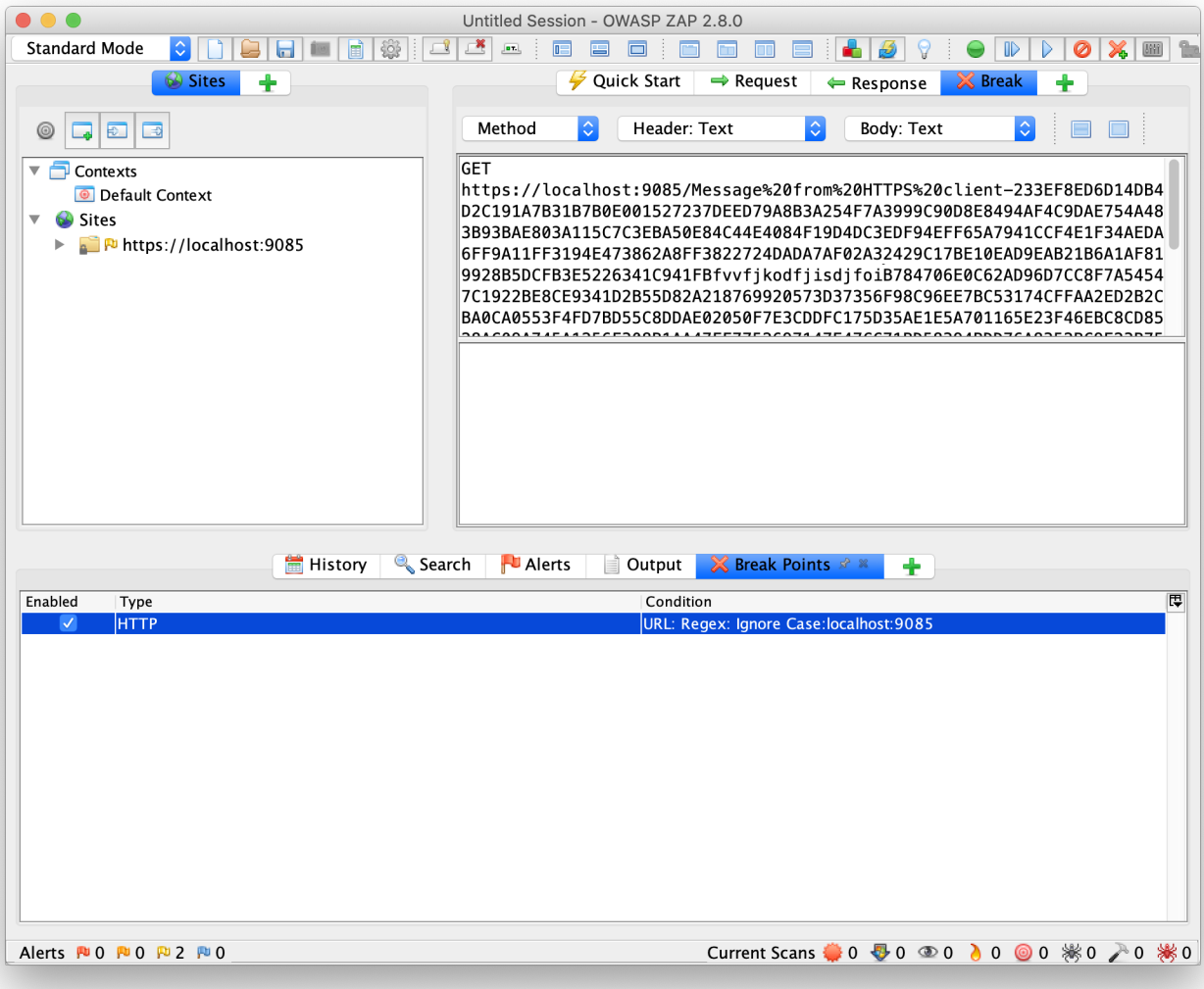
Task 3

Here is the result in WireShark.



Task 4 | Tamper with the Message (Integrity)

After setting up the proxy certificates, we've set a breakpoint like this:



After tampering with the message this is the result.

```
java.io.IOException: Server returned
HTTP response code: 502 for URL: http
s://localhost:9085/Message from HTTPS
 client-233EF8ED6D14DB4D2C191A7B31B7B
0E001527237DEED79A8B3A254F7A3999C90D8
E8494AF4C9DAE754A483B93BAE803A115C7C3
EBA50E84C44E4084F19D4DC3EDF94EFF65A79
41CCF4E1F34AEDA6FF9A11FF3194E473862A8
FF3822724DADA7AF02A32429C17BE10EAD9EA
B21B6A1AF819928B5DCFB3E5226341C941FBB
784706E0C62AD96D7CC8F7A54547C1922BE8C
E9341D2B55D82A2187699205 73D37356F98C9
6EE7BC53174CFFAA2ED2B2CBA0CA0553F4FD7
BD55C8DDAE02050F7E3CDDFC175D35AE1E5A7
01165E23F46EBC8CD8528AC09A745A1256F30
8B1AA47FF7752697147E47CC71BD58394BDD7
6A8352BC9E23B75EBD46CB3837213CC3B11A4
F5
```

Question

Can we impersonate HttpsClientProxySSLRSA in this setup? If so, we would need it's private key in order to sign messages correctly.