SSD lab 03

1. Configure the Apache tomcat Web server to support HTTPS.

Step 1 - Install Java

```
sudo apt update
```

```
sudo apt install default − jdk
```

Step 2 - Generating a keystore

```
sudo keytool − genkey − alias tomcat − keyalg RSA − keystore /keystore.jks − keysize 2048
```

Step 3 - Install tomcat server

```
sudo apt − get install tomcat9
```

Step 4 - Configure Tomcat for HTTPS

```
<Connector port="8443"
        protocol="org.apache.coyote.http11.Http11NioProtocol"
        maxThreads="150"
        SSLEnabled="true"
        scheme="https"
        secure="true"
        clientAuth="false"
        sslProtocol="TLS"
        keystoreFile="/path/to/your/keystore.jks"
        keystorePass="your-keystore-password"
/>
```

Step 5 - Restart tomcat server

```
sudo systemctl restart tomcat9
```

2. Log the SSL handshake messages to a log file. Extract the TLS related messages from the log file and copy it to a separate text file.

Step 1 - Locate the catalina.sh file in tomcat bin directory

Step 2 - Enable SSL Handshake Debugging

```
JAVA_OPTS = "$JAVA_OPTS − Djavax.net.debug = ssl:handshake"
```

Step 3 - Restart Tomcat

```
sudo systemctl restart tomcat9
```

Step 4 - Extract TLS Messages

```
grep "handshake" /path/to/tomcat/logs/catalina.out > tls_handshake_messages.txt
```