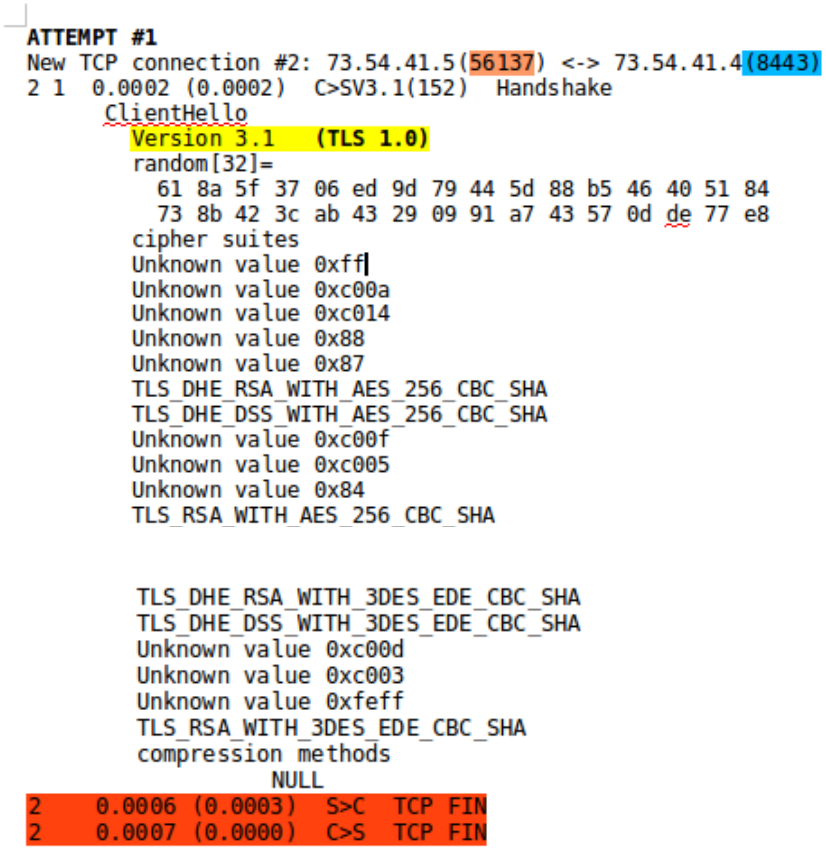
1. PDF of POODLEAttack output, marked up as outlined in Step 12:
    a. For the lab turn-in, open the attacker dump with LibreOffice Writer and label the following information in the text:
        i. Highlight the port(s) our firefox session(s) are running on with orange. (10 points)
        ii. Highlight the port the attack proxy is running on with blue. (10 points)
        iii. Highlight the port the target webserver is running on with green. (10 points)
    b. For the **attacker packet dump**
        i. Label the first attempt (**Attempt #1 Client**) of the client to connect to the web server (which is really the attacker's IP), using version 3.1 and where the attempt fails (10 points)
        ii. Label version 3.1 as **TLS 1.0**. (10 points)
        iii. Highlight the portion in Attempt #1 that shows the connection being terminated (this is the proxy denying the use of version 3.1 with a FIN) with red. (5 points)



```
ATTEMPT #1
New TCP connection #2: 73.54.41.5(56137) <-> 73.54.41.4(8443)
2 1   0.0002 (0.0002)  C>SV3.1(152)  Handshake
      ClientHello
        Version 3.1   (TLS 1.0)
        random[32]=
          61 8a 5f 37 06 ed 9d 79 44 5d 88 b5 46 40 51 84
          73 8b 42 3c ab 43 29 09 91 a7 43 57 0d de 77 e8
        cipher suites
        Unknown value 0xff
        Unknown value 0xc00a
        Unknown value 0xc014
        Unknown value 0x88
        Unknown value 0x87
        TLS_DHE_RSA_WITH_AES_256_CBC_SHA
        TLS_DHE_DSS_WITH_AES_256_CBC_SHA
        Unknown value 0xc00f
        Unknown value 0xc005
        Unknown value 0x84
        TLS_RSA_WITH_AES_256_CBC_SHA


        TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
        TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
        Unknown value 0xc00d
        Unknown value 0xc003
        Unknown value 0xfeff
        TLS_RSA_WITH_3DES_EDE_CBC_SHA
        compression methods
                  NULL
2     0.0006 (0.0003)  S>C  TCP FIN
2     0.0007 (0.0000)  C>S  TCP FIN
```

iv. Label the second attempt (**Attempt #2 Client**) by the client to connect to the web server, using version 3.0. Label this as **SSL 3.0**.
(10 points)

```
ATTEMPT #2
New TCP connection #3: 73.54.41.5(56138) <-> 73.54.41.4(8443)
3 1  0.0001 (0.0001)  C>SV3.0(83)  Handshake
       ClientHello
          Version 3.0    (SSL v3)
          random[32]=
            61 8a 5f 37 58 79 1c 33 18 e3 c8 25 1d 6c f5 a8
            53 17 0c c6 84 19 ec da d9 f3 18 d6 cb b8 fc 50
          cipher suites
          Unknown value 0xff
          Unknown value 0x88
          Unknown value 0x87
          SSL_DHE_RSA_WITH_AES_256_CBC_SHA
          SSL_DHE_DSS_WITH_AES_256_CBC_SHA
          Unknown value 0x84
          SSL_RSA_WITH_AES_256_CBC_SHA
          Unknown value 0x45
          Unknown value 0x44
          SSL_DHE_RSA_WITH_AES_128_CBC_SHA
          SSL_DHE_DSS_WITH_AES_128_CBC_SHA
          Unknown value 0x96
          Unknown value 0x41
          SSL_RSA_WITH_AES_128_CBC_SHA
          SSL_RSA_WITH_RC4_128_SHA
          SSL_RSA_WITH_RC4_128_MD5
          SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
          SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
          Unknown value 0xfeff
          SSL_RSA_WITH_3DES_EDE_CBC_SHA
          compression methods
                    NULL
```

v. Label where the attacker makes a request to the ssl server on behalf of the client (**Attacker to Vulnerable Server**)
(10 points)

vi. Identify whether the request is for **TLS or SSL**. Explain why it is the version it is in your lab report.
(5 points)

The attacker intercepted the transmission and requested the server to use v3 instead of TLS 1.0.

```
ATTACKER to VULN SERVER
New TCP connection #4: 73.54.41.4(48934) <-> 73.54.41.3(4433)
4 1  0.0001 (0.0001)  C>SV3.0(83)  Handshake
      ClientHello
        Version 3.0  (SSL v3)
        random[32]=
          61 8a 5f 37 58 79 1c 33 18 e3 c8 25 1d 6c f5 a8
          53 17 0c c6 84 19 ec da d9 f3 18 d6 cb b8 fc 50
        cipher suites
        Unknown value 0xff
        Unknown value 0x88
        Unknown value 0x87
        SSL_DHE_RSA_WITH_AES_256_CBC_SHA
        SSL_DHE_DSS_WITH_AES_256_CBC_SHA
        Unknown value 0x84
        SSL_RSA_WITH_AES_256_CBC_SHA
        Unknown value 0x45
        Unknown value 0x44
        SSL_DHE_RSA_WITH_AES_128_CBC_SHA
        SSL_DHE_DSS_WITH_AES_128_CBC_SHA
        Unknown value 0x96
        Unknown value 0x41
        SSL_RSA_WITH_AES_128_CBC_SHA
        SSL_RSA_WITH_RC4_128_SHA
        SSL_RSA_WITH_RC4_128_MD5
        SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
        SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
        Unknown value 0xfeff
        SSL_RSA_WITH_3DES_EDE_CBC_SHA
        compression methods
                  NULL
```

vii. Find the change cipher suite (**Change Cipher Suite**)which then signals the transmission of application data (**Application Data**) color with pink. (10 points)

```
7 4  0.0013 (0.0000)  S>CV3.0(4)  Handshake
      ServerHelloDone
7 5  0.0019 (0.0005)  C>SV3.0(260)  Handshake
      ClientKeyExchange
7 6  0.0019 (0.0000)  C>SV3.0(1)  ChangeCipherSpec
7 7  0.0019 (0.0000)  C>SV3.0(64)  Handshake
8 5  0.0015 (0.0006)  C>SV3.0(260)  Handshake
      ClientKeyExchange
6 6  0.0384 (0.0361)  C>SV3.0(1)  ChangeCipherSpec
6 7  0.0384 (0.0000)  C>SV3.0(64)  Handshake
6 8  0.0385 (0.0001)  S>CV3.0(1)  ChangeCipherSpec
6 9  0.0385 (0.0000)  S>CV3.0(64)  Handshake
5 8  0.0432 (0.0363)  S>CV3.0(1)  ChangeCipherSpec
8 6  0.0391 (0.0376)  C>SV3.0(1)  ChangeCipherSpec
8 7  0.0391 (0.0000)  C>SV3.0(64)  Handshake
8 8  0.0393 (0.0001)  S>CV3.0(1)  ChangeCipherSpec
8 9  0.0393 (0.0000)  S>CV3.0(64)  Handshake
7 8  0.0398 (0.0378)  S>CV3.0(1)  ChangeCipherSpec
5 9  0.0815 (0.0382)  S>CV3.0(64)  Handshake
7 9  0.0779 (0.0381)  S>CV3.0(64)  Handshake
7 10 0.0782 (0.0002)  C>SV3.0(32)  application_data
7 11 0.0782 (0.0000)  C>SV3.0(320)  application_data
8 10 0.0778 (0.0385)  C>SV3.0(32)  application_data
8 11 0.1151 (0.0372)  C>SV3.0(320)  application_data
5 10 5.0866 (5.0051)  C>SV3.0(32)  Alert
5    5.0867 (0.0000)  C>S  TCP FIN
6 10 5.0821 (5.0436)  C>SV3.0(32)  Alert
6    5.0823 (0.0001)  C>S  TCP FIN
5    5.0870 (0.0002)  S>C  TCP FIN
6 11 5.0832 (0.0009)  S>CV3.0(32)  Alert
8 12 5.0566 (4.9414)  S>CV3.0(32)  application_data
8 13 5.0566 (0.0000)  S>CV3.0(208)  application_data
7 12 5.0570 (4.9788)  S>CV3.0(32)  application_data
7 13 5.0940 (0.0369)  S>CV3.0(208)  application_data
8 14 5.0950 (0.0384)  S>CV3.0(32)  Alert
7 14 5.0955 (0.0015)  S>CV3.0(32)  Alert
```

c. Leaked information file with the cookie highlighted in purple (a screenshot is also acceptable.)
(10 points)