Joseph Shaffer

Shaffer.567

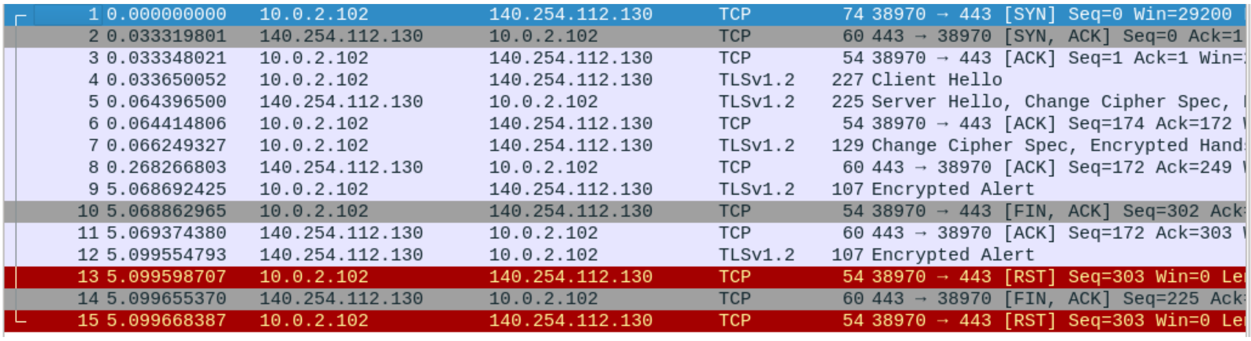
CSE 5473

Lab 4

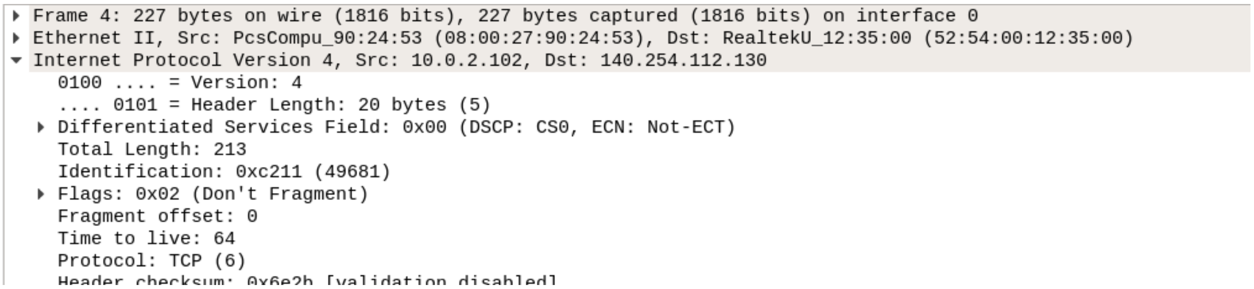
2. Understand SSL/TLS handshake (3%+ 0.5% extra credit)

(1) (1%) Show the differences between RSA-based key exchange and DH-based key exchange. Hint: In the firefox browser installed in your VM, install “toggle cipher suite” add-on. To analyze RSA-based key exchange: only enable cipher suites with “rsa-xxx”, then visit www.osu.edu. Similarly, to test DH-based key exchange, only enable cipher suites with “dhexxx”, then visit www.netaddress.com.

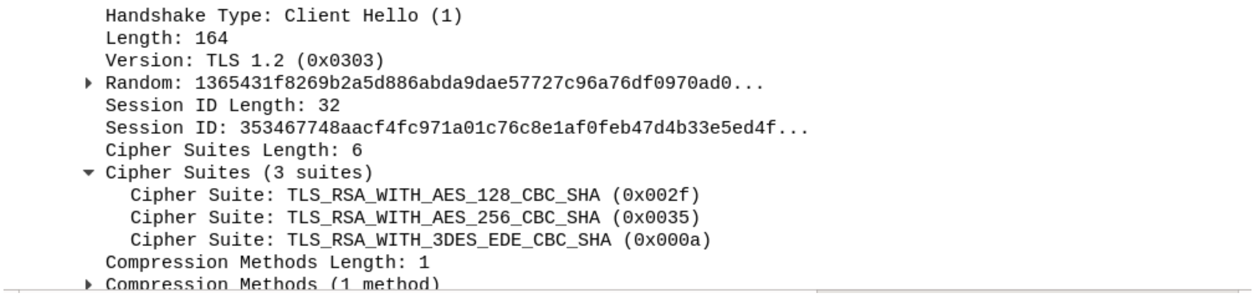
www.osu.edu:



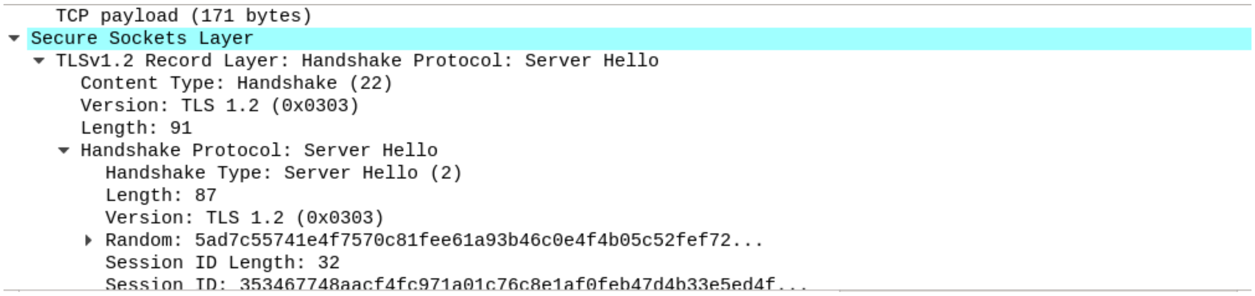
```
  1 0.000000000   10.0.2.102       140.254.112.130   TCP        74 38970 → 443 [SYN] Seq=0 Win=29200
  2 0.033319801   140.254.112.130  10.0.2.102        TCP        60 443 → 38970 [SYN, ACK] Seq=0 Ack=1
  3 0.033348021   10.0.2.102       140.254.112.130   TCP        54 38970 → 443 [ACK] Seq=1 Ack=1 Win=
  4 0.033650052   10.0.2.102       140.254.112.130   TLSv1.2   227 Client Hello
  5 0.064396500   140.254.112.130  10.0.2.102        TLSv1.2   225 Server Hello, Change Cipher Spec,
  6 0.064414806   10.0.2.102       140.254.112.130   TCP        54 38970 → 443 [ACK] Seq=174 Ack=172
  7 0.066249327   10.0.2.102       140.254.112.130   TLSv1.2   129 Change Cipher Spec, Encrypted Hand
  8 0.268266803   140.254.112.130  10.0.2.102        TCP        60 443 → 38970 [ACK] Seq=172 Ack=249
  9 5.068692425   10.0.2.102       140.254.112.130   TLSv1.2   107 Encrypted Alert
 10 5.068862965   10.0.2.102       140.254.112.130   TCP        54 38970 → 443 [FIN, ACK] Seq=302 Ack
 11 5.069374380   140.254.112.130  10.0.2.102        TCP        60 443 → 38970 [ACK] Seq=172 Ack=303
 12 5.099554793   140.254.112.130  10.0.2.102        TLSv1.2   107 Encrypted Alert
 13 5.099598707   10.0.2.102       140.254.112.130   TCP        54 38970 → 443 [RST] Seq=303 Win=0 Le
 14 5.099655370   140.254.112.130  10.0.2.102        TCP        60 443 → 38970 [FIN, ACK] Seq=225 Ack
 15 5.099668387   10.0.2.102       140.254.112.130   TCP        54 38970 → 443 [RST] Seq=303 Win=0 Le
```



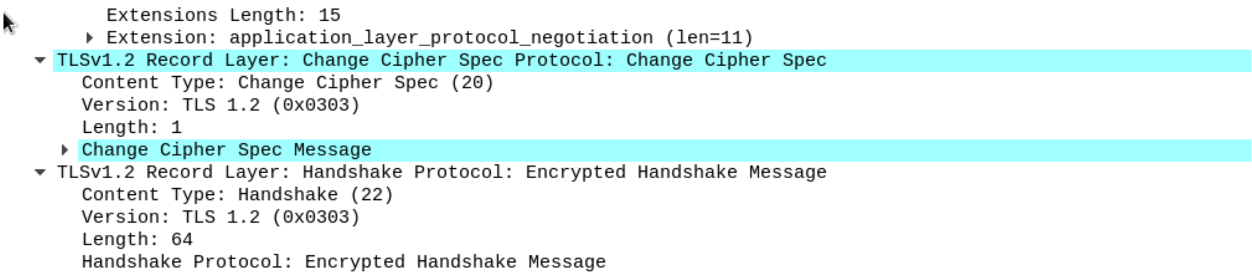
```
▸ Frame 4: 227 bytes on wire (1816 bits), 227 bytes captured (1816 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_90:24:53 (08:00:27:90:24:53), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
▾ Internet Protocol Version 4, Src: 10.0.2.102, Dst: 140.254.112.130
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 213
    Identification: 0xc211 (49681)
  ▸ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0x6e2b [validation disabled]
```



```
        Handshake Type: Client Hello (1)
        Length: 164
        Version: TLS 1.2 (0x0303)
      ▸ Random: 1365431f8269b2a5d886abda9dae57727c96a76df0970ad0...
        Session ID Length: 32
        Session ID: 353467748aacf4fc971a01c76c8e1af0feb47d4b33e5ed4f...
        Cipher Suites Length: 6
      ▾ Cipher Suites (3 suites)
          Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
          Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
          Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
        Compression Methods Length: 1
      ▸ Compression Methods (1 method)
```

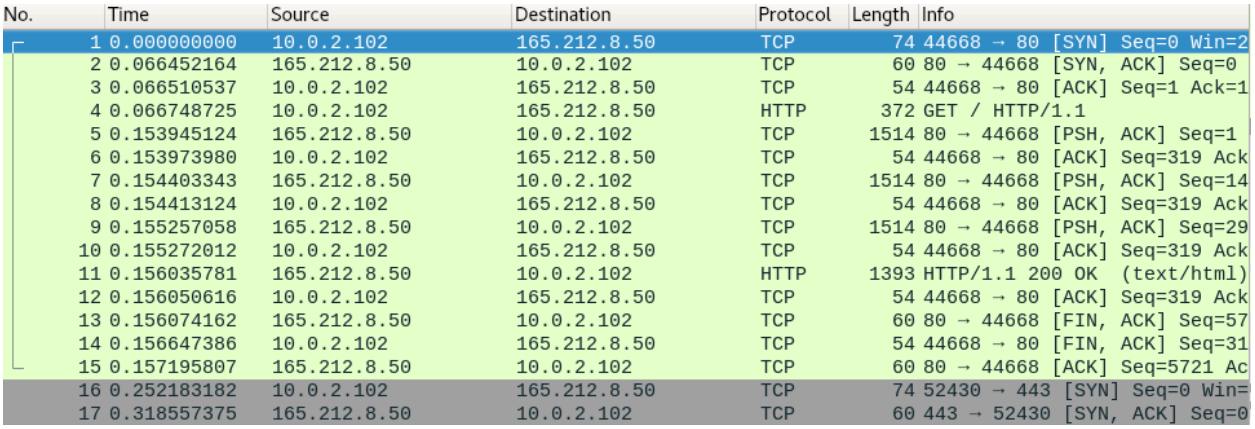


```
    TCP payload (171 bytes)
▾ Secure Sockets Layer
  ▾ TLSv1.2 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 91
    ▾ Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 87
        Version: TLS 1.2 (0x0303)
      ▸ Random: 5ad7c55741e4f7570c81fee61a93b46c0e4f4b05c52fef72...
        Session ID Length: 32
        Session ID: 353467748aacf4fc971a01c76c8e1af0feb47d4b33e5ed4f...
```

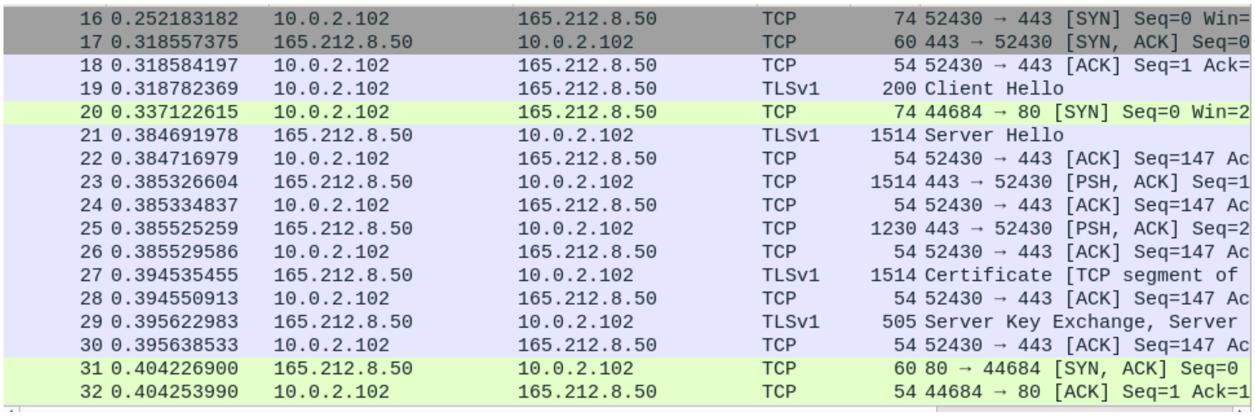


```
        Extensions Length: 15
      ▸ Extension: application_layer_protocol_negotiation (len=11)
  ▾ TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      Content Type: Change Cipher Spec (20)
      Version: TLS 1.2 (0x0303)
      Length: 1
    ▸ Change Cipher Spec Message
  ▾ TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 64
      Handshake Protocol: Encrypted Handshake Message
```

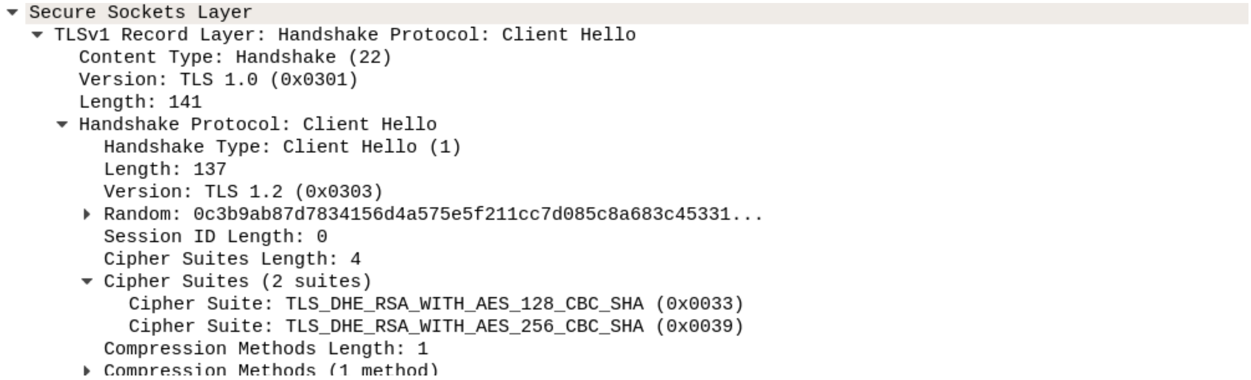
www.netaddress.com:



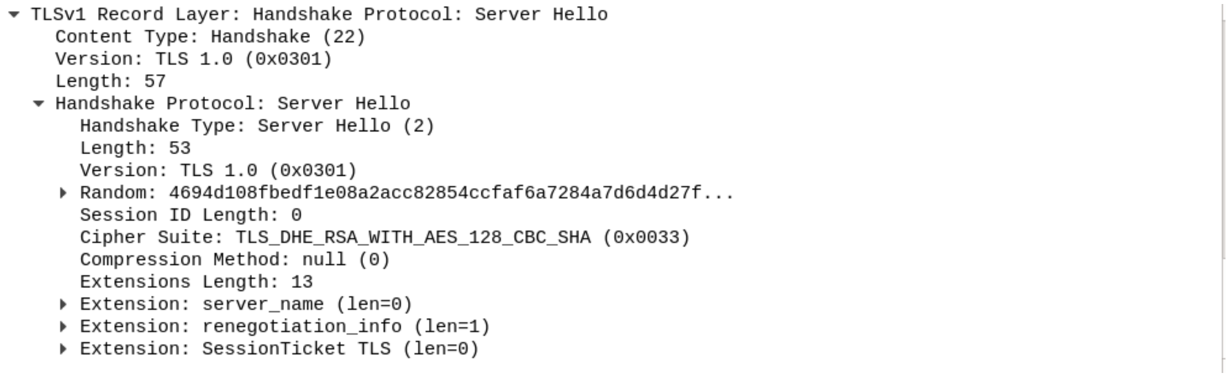
```
No.   Time         Source         Destination    Protocol Length Info
    1 0.000000000  10.0.2.102     165.212.8.50   TCP        74 44668 → 80 [SYN] Seq=0 Win=2
    2 0.066452164  165.212.8.50   10.0.2.102     TCP        60 80 → 44668 [SYN, ACK] Seq=0
    3 0.066510537  10.0.2.102     165.212.8.50   TCP        54 44668 → 80 [ACK] Seq=1 Ack=1
    4 0.066748725  10.0.2.102     165.212.8.50   HTTP      372 GET / HTTP/1.1
    5 0.153945124  165.212.8.50   10.0.2.102     TCP      1514 80 → 44668 [PSH, ACK] Seq=1
    6 0.153973980  10.0.2.102     165.212.8.50   TCP        54 44668 → 80 [ACK] Seq=319 Ack
    7 0.154403343  165.212.8.50   10.0.2.102     TCP      1514 80 → 44668 [PSH, ACK] Seq=14
    8 0.154413124  10.0.2.102     165.212.8.50   TCP        54 44668 → 80 [ACK] Seq=319 Ack
    9 0.155257058  165.212.8.50   10.0.2.102     TCP      1514 80 → 44668 [PSH, ACK] Seq=29
   10 0.155272012  10.0.2.102     165.212.8.50   TCP        54 44668 → 80 [ACK] Seq=319 Ack
   11 0.156035781  165.212.8.50   10.0.2.102     HTTP     1393 HTTP/1.1 200 OK  (text/html)
   12 0.156050616  10.0.2.102     165.212.8.50   TCP        54 44668 → 80 [ACK] Seq=319 Ack
   13 0.156074162  165.212.8.50   10.0.2.102     TCP        60 80 → 44668 [FIN, ACK] Seq=57
   14 0.156647386  10.0.2.102     165.212.8.50   TCP        54 44668 → 80 [FIN, ACK] Seq=31
   15 0.157195807  165.212.8.50   10.0.2.102     TCP        60 80 → 44668 [ACK] Seq=5721 Ac
   16 0.252183182  10.0.2.102     165.212.8.50   TCP        74 52430 → 443 [SYN] Seq=0 Win=
   17 0.318557375  165.212.8.50   10.0.2.102     TCP        60 443 → 52430 [SYN, ACK] Seq=0
```



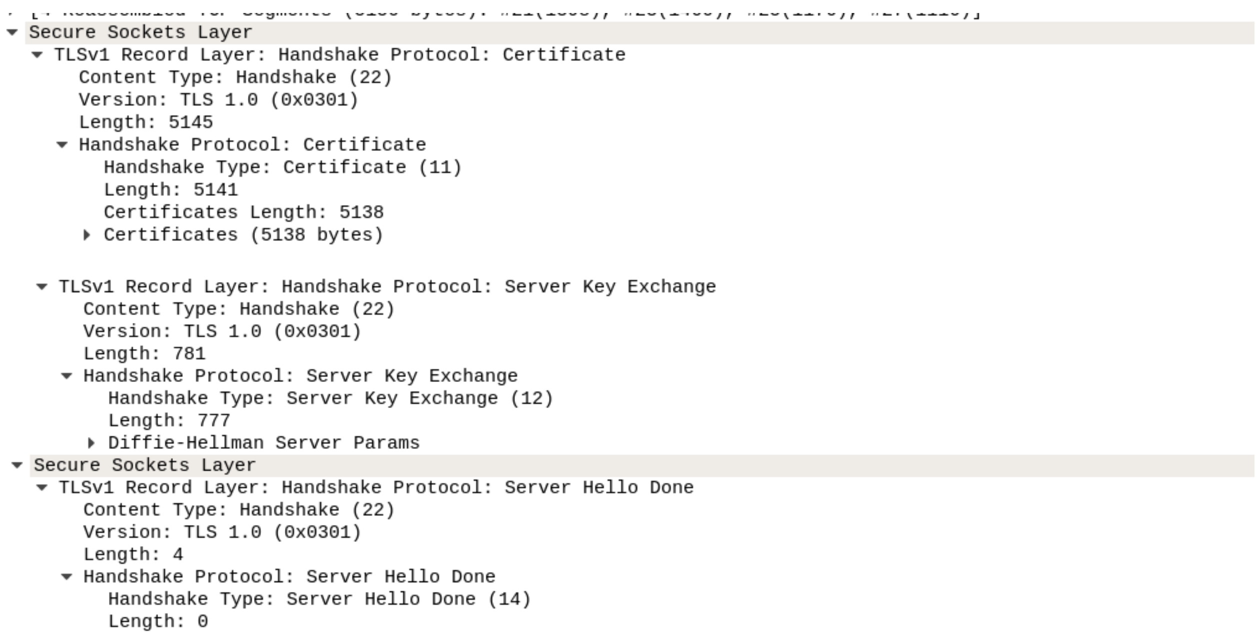
```
   16 0.252183182  10.0.2.102     165.212.8.50   TCP        74 52430 → 443 [SYN] Seq=0 Win=
   17 0.318557375  165.212.8.50   10.0.2.102     TCP        60 443 → 52430 [SYN, ACK] Seq=0
   18 0.318584197  10.0.2.102     165.212.8.50   TCP        54 52430 → 443 [ACK] Seq=1 Ack=
   19 0.318782369  10.0.2.102     165.212.8.50   TLSv1     200 Client Hello
   20 0.337122615  10.0.2.102     165.212.8.50   TCP        74 44684 → 80 [SYN] Seq=0 Win=2
   21 0.384691978  165.212.8.50   10.0.2.102     TLSv1    1514 Server Hello
   22 0.384716979  10.0.2.102     165.212.8.50   TCP        54 52430 → 443 [ACK] Seq=147 Ac
   23 0.385326604  165.212.8.50   10.0.2.102     TCP      1514 443 → 52430 [PSH, ACK] Seq=1
   24 0.385334837  10.0.2.102     165.212.8.50   TCP        54 52430 → 443 [ACK] Seq=147 Ac
   25 0.385525259  165.212.8.50   10.0.2.102     TCP      1230 443 → 52430 [PSH, ACK] Seq=2
   26 0.385529586  10.0.2.102     165.212.8.50   TCP        54 52430 → 443 [ACK] Seq=147 Ac
   27 0.394535455  165.212.8.50   10.0.2.102     TLSv1    1514 Certificate [TCP segment of
   28 0.394550913  10.0.2.102     165.212.8.50   TCP        54 52430 → 443 [ACK] Seq=147 Ac
   29 0.395622983  165.212.8.50   10.0.2.102     TLSv1     505 Server Key Exchange, Server
   30 0.395638533  10.0.2.102     165.212.8.50   TCP        54 52430 → 443 [ACK] Seq=147 Ac
   31 0.404226900  165.212.8.50   10.0.2.102     TCP        60 80 → 44684 [SYN, ACK] Seq=0
   32 0.404253990  10.0.2.102     165.212.8.50   TCP        54 44684 → 80 [ACK] Seq=1 Ack=1
```



```
▾ Secure Sockets Layer
  ▾ TLSv1 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 141
    ▾ Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 137
        Version: TLS 1.2 (0x0303)
      ▸ Random: 0c3b9ab87d7834156d4a575e5f211cc7d085c8a683c45331...
        Session ID Length: 0
        Cipher Suites Length: 4
      ▾ Cipher Suites (2 suites)
          Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
          Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
        Compression Methods Length: 1
      ▸ Compression Methods (1 method)
```



```
  ▾ TLSv1 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 57
    ▾ Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 53
        Version: TLS 1.0 (0x0301)
      ▸ Random: 4694d108fbedf1e08a2acc82854ccfaf6a7284a7d6d4d27f...
        Session ID Length: 0
        Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
        Compression Method: null (0)
        Extensions Length: 13
      ▸ Extension: server_name (len=0)
      ▸ Extension: renegotiation_info (len=1)
      ▸ Extension: SessionTicket TLS (len=0)
```



```
▾ Secure Sockets Layer
  ▾ TLSv1 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 5145
    ▾ Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 5141
        Certificates Length: 5138
      ▸ Certificates (5138 bytes)

  ▾ TLSv1 Record Layer: Handshake Protocol: Server Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 781
    ▾ Handshake Protocol: Server Key Exchange
        Handshake Type: Server Key Exchange (12)
        Length: 777
      ▸ Diffie-Hellman Server Params
▾ Secure Sockets Layer
  ▾ TLSv1 Record Layer: Handshake Protocol: Server Hello Done
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 4
    ▾ Handshake Protocol: Server Hello Done
        Handshake Type: Server Hello Done (14)
        Length: 0
```

When a TLS/SSL session starts, the server gives the client it's certificate. The key in the certificate could perform different actions depending on the key-agreement algorithm decided on by the client and the server.

The RSA algorithm is used for actual asymmetric key encryption. It generates public-private key pair and then use them for exchanging data.

For the RSA key agreement, the certificate contains the server public RSA key and the server has a private RSA key used for decryption, which is the private key. The client generates a random sequence called the pre-master secret. The client uses the public RSA key on the certificate to encrypt the pre-master secret. The server decrypts the message and gets the pre-master secret. The server and the client then perform some random mixing on the pre-master secret. The master secret is used to derive keys for symmetric encryption and MAC.

Diffie hellman is used for key exchange using the concept of primitive root and then both parties use that common key for subsequent data-exchange using symmetric key encryption.

For the Diffie-Hellman key exchange, the client must also generate a public-private DH pair used to exchange and generate the pre-master secret. A more modern approach is to use session keys in which the server certificate contains it's public key for verifying a signature algorithm that it used to sign either an RSA or DHE public key for key-agreement. Thus the server is not reusing it's key-agreement public key. This provides perfect forward secrecy. In which finding the private key of the signature algorithm the server uses to sign its key does not make all the session keys vulnerable. In addition finding a session key should allow you to obtain information that would allow you to decrypt traffic that used another session key.

(2) (1%) Show the differences between the first and second SSL connection in an SSL session.

An SSL certificate is necessary to create a SSL connection. Following this, a private key and public key are created. The next step is the submission of the certificate signing request which is a data file that contains your details and the public key. The certificate authority would then validate your details. Following authentication of the details, a SSL certificate is issued and the newly issued SSL is matched to the private key. From this point, an encrypted link is established between your website and the customer's web browser. The SSL handshake starts with a user asking their browser to make a secure connection to a website. The browser obtains the IP address of the site from a DNS server then requests a secure connection to the website. To initiate this secure connection, the browser requests that the server identifies itself by sending a copy of its SSL certificate to the browser. The browser checks the certificate to ensure that it is signed by a trusted CA, that it is valid, that it confirms to required security standards on key lengths and other items, and that the domain listed on the certificate matches that domain that was requested by the user. When the browser confirms that the website can be trusted, it creates a symmetric session key which it encrypts with the public key in the website's certificate. The session key is then sent to the web server. The web server uses its private key to decrypt the symmetric session key. The server sends back an acknowledgement that is encrypted with the session key. From now on, all data transmitted between the server and the browser is encrypted and secure.

An SSL connection is a transport that provides a suitable type of service. For SSL, such connections are peer to peer relationships that are also transient. Every connection is associated with one session.

An SSL session is an association between a client and a server. Sessions are created by the handshake protocol. Sessions define a set of cryptographic security parameters which can be shared among multiple connections. The sessions are used to avoid the expensive negotiation of new security parameters for each connection.

Between any pair of parties there may be multiple secure connections.

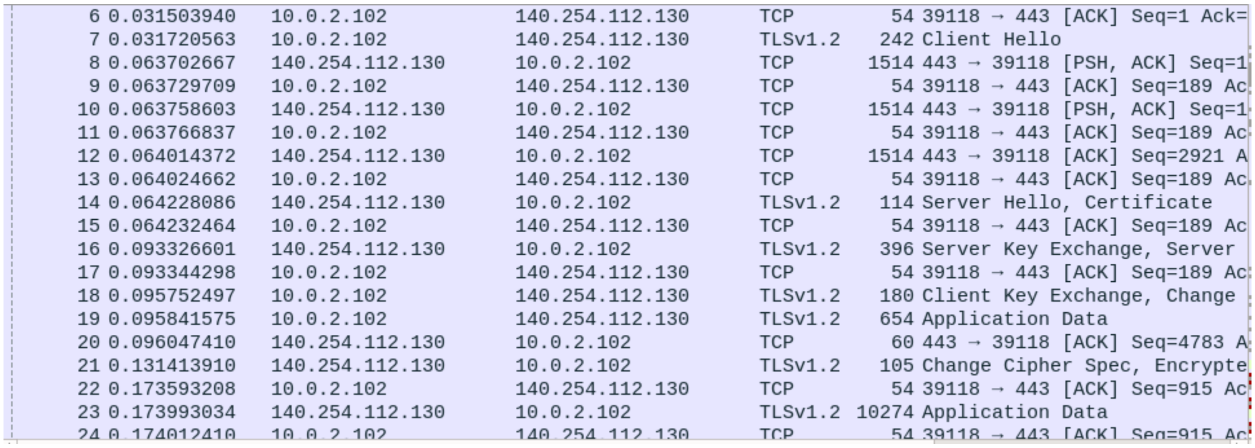
It is possible to have multiple sessions in a share single connection but not at the same time. Instead an active SSL session inside the connection can be replaced by a new session using renegotiation. Renegotiation is required if the sequence number of a TLS session would wrap. More common is a renegotiation of a session without client authentication to a session with client authentication.

On a SSL connection, a renegotiation can occur to request for new cipher suites for key materials. To renegotiate, a client will send a ClientHello over its existing SSL connection. A server will send a HelloRequest and expects client to renegotiate with a ClientHello in a very short time.

(3) (1%) Using Wireshark analysis to discuss the differences between TLS v1.0, TLS v1.1, and

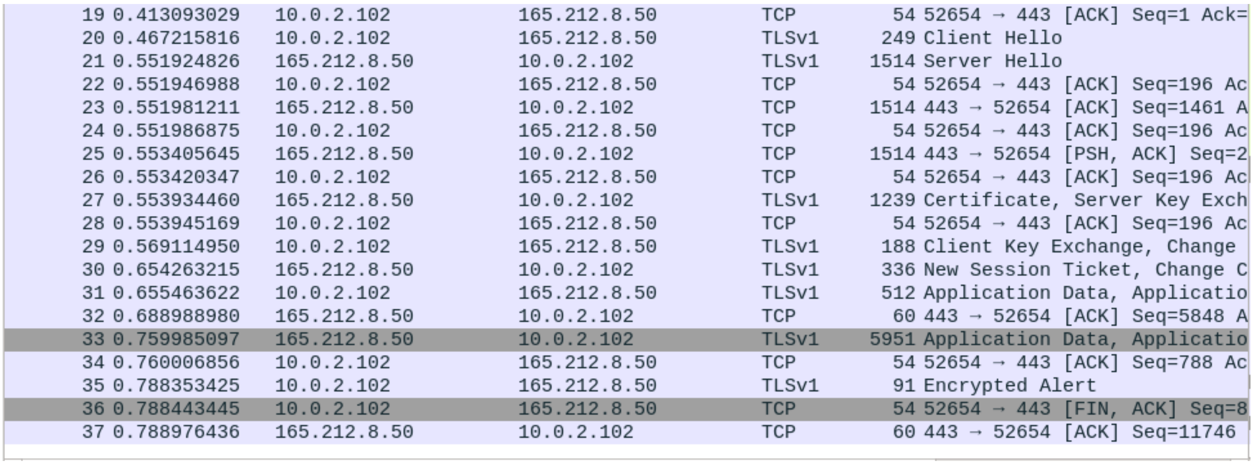
TLS v1.2.

Wireshark Analysis of www.osu.edu:



```
 6 0.031503940   10.0.2.102        140.254.112.130   TCP        54 39118 → 443 [ACK] Seq=1 Ack=
 7 0.031720563   10.0.2.102        140.254.112.130   TLSv1.2   242 Client Hello
 8 0.063702667   140.254.112.130   10.0.2.102        TCP      1514 443 → 39118 [PSH, ACK] Seq=1
 9 0.063729709   10.0.2.102        140.254.112.130   TCP        54 39118 → 443 [ACK] Seq=189 Ac
10 0.063758603   140.254.112.130   10.0.2.102        TCP      1514 443 → 39118 [PSH, ACK] Seq=1
11 0.063766837   10.0.2.102        140.254.112.130   TCP        54 39118 → 443 [ACK] Seq=189 Ac
12 0.064014372   140.254.112.130   10.0.2.102        TCP      1514 443 → 39118 [ACK] Seq=2921 A
13 0.064024662   10.0.2.102        140.254.112.130   TCP        54 39118 → 443 [ACK] Seq=189 Ac
14 0.064228086   140.254.112.130   10.0.2.102        TLSv1.2   114 Server Hello, Certificate
15 0.064232464   10.0.2.102        140.254.112.130   TCP        54 39118 → 443 [ACK] Seq=189 Ac
16 0.093326601   140.254.112.130   10.0.2.102        TLSv1.2   396 Server Key Exchange, Server
17 0.093344298   10.0.2.102        140.254.112.130   TCP        54 39118 → 443 [ACK] Seq=189 Ac
18 0.095752497   10.0.2.102        140.254.112.130   TLSv1.2   180 Client Key Exchange, Change
19 0.095841575   10.0.2.102        140.254.112.130   TLSv1.2   654 Application Data
20 0.096047410   140.254.112.130   10.0.2.102        TCP        60 443 → 39118 [ACK] Seq=4783 A
21 0.131413910   140.254.112.130   10.0.2.102        TLSv1.2   105 Change Cipher Spec, Encrypte
22 0.173593208   10.0.2.102        140.254.112.130   TCP        54 39118 → 443 [ACK] Seq=915 Ac
23 0.173993034   140.254.112.130   10.0.2.102        TLSv1.2 10274 Application Data
24 0.174012410   10.0.2.102        140.254.112.130   TCP        54 39118 → 443 [ACK] Seq=915 Ac
```

Wireshark Analysis of www.netaddress.com:



```
19 0.413093029   10.0.2.102     165.212.8.50   TCP       54 52654 → 443 [ACK] Seq=1 Ack=
20 0.467215816   10.0.2.102     165.212.8.50   TLSv1    249 Client Hello
21 0.551924826   165.212.8.50   10.0.2.102     TLSv1   1514 Server Hello
22 0.551946988   10.0.2.102     165.212.8.50   TCP       54 52654 → 443 [ACK] Seq=196 Ac
23 0.551981211   165.212.8.50   10.0.2.102     TCP     1514 443 → 52654 [ACK] Seq=1461 A
24 0.551986875   10.0.2.102     165.212.8.50   TCP       54 52654 → 443 [ACK] Seq=196 Ac
25 0.553405645   165.212.8.50   10.0.2.102     TCP     1514 443 → 52654 [PSH, ACK] Seq=2
26 0.553420347   10.0.2.102     165.212.8.50   TCP       54 52654 → 443 [ACK] Seq=196 Ac
27 0.553934460   165.212.8.50   10.0.2.102     TLSv1   1239 Certificate, Server Key Exch
28 0.553945169   10.0.2.102     165.212.8.50   TCP       54 52654 → 443 [ACK] Seq=196 Ac
29 0.569114950   10.0.2.102     165.212.8.50   TLSv1    188 Client Key Exchange, Change
30 0.654263215   165.212.8.50   10.0.2.102     TLSv1    336 New Session Ticket, Change C
31 0.655463622   10.0.2.102     165.212.8.50   TLSv1    512 Application Data, Applicatio
32 0.688988980   165.212.8.50   10.0.2.102     TCP       60 443 → 52654 [ACK] Seq=5848 A
33 0.759985097   165.212.8.50   10.0.2.102     TLSv1   5951 Application Data, Applicatio
34 0.760006856   10.0.2.102     165.212.8.50   TCP       54 52654 → 443 [ACK] Seq=788 Ac
35 0.788353425   10.0.2.102     165.212.8.50   TLSv1     91 Encrypted Alert
36 0.788443445   10.0.2.102     165.212.8.50   TCP       54 52654 → 443 [FIN, ACK] Seq=8
37 0.788976436   165.212.8.50   10.0.2.102     TCP       60 443 → 52654 [ACK] Seq=11746
```

TLS 1.0 is an upgrade from SSL 3.0, and the differences although not that dramatic are significant enough that SSL 3.0 and TLS 1.0 do not interpolate. Some of the major differences are key derivation functions are different, the MACs are different as SSL 3.0 uses a modification of an early HMAC while TLS uses HMAC, the finished messages are different, TLS has more alerts and TLS requires DSS/DH support.

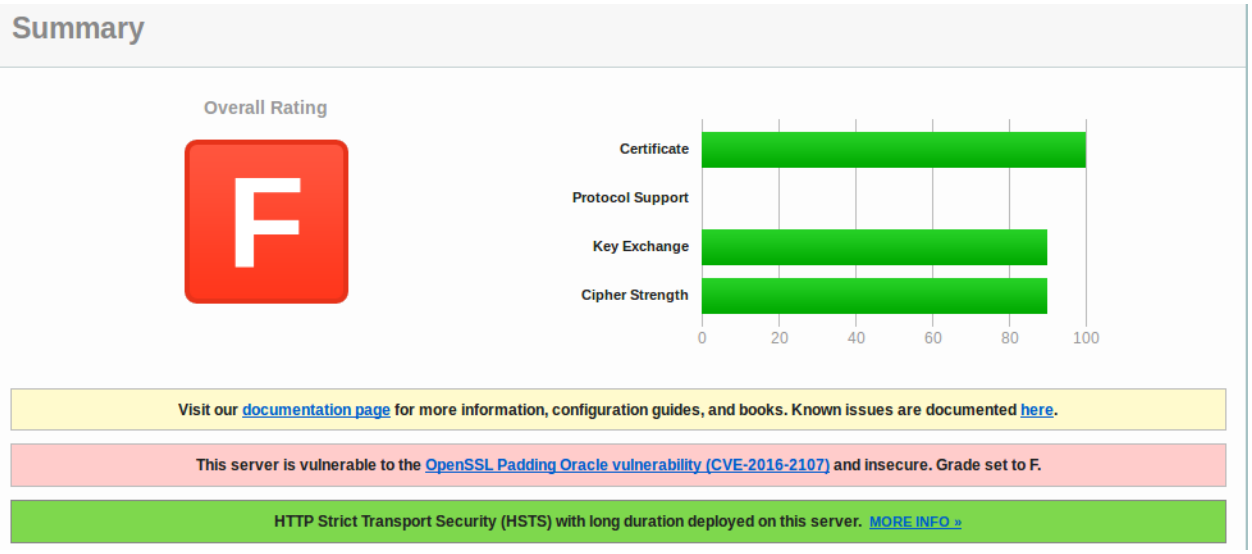
TLS 1.1 is an update to TLS 1.0. The major changes are the implicit initialization vector is replaced with an explicit IV to protect against cipher block chaining attacks, handling of padded errors is changed to use the bad_record_mac alert rather than the decryption_failed alert to protect against CBC attacks, IANA registries are defined for protocol parameters and premature closes no longer cause a session to be non-resumable.

TLS 1.2 is based on TLS 1.1 and contains improved flexibility. The major differences are the MD5/SHA-1 combination in the pseudorandom function was replaced with cipher-suite-specified PRFs, the MD5/SHA-1 combination in the digitally-signed element was replaced with a single hash, there was substantial cleanup to the client's and server's ability to specify which hash and signature algorithms were accepted, addition of support for authenticated encryption with additional modes, TLS extensions definition and AES cipher suites were merged in, tighter checking of Encrypted Pre Master Secret version numbers, many of the requirements were tightened, verify_data length depends on the cipher suite, and description of Bleichenbacher/Dilma attack defenses cleaned up.

3. Analyzing SSL/TLS security (2%+ 0.5% extra credit)

www.ssllabs.com provides a suite of security test of SSL/TLS implementations of a website.

Similar open-source tools are also available. Go to ssllabs.com and start an analysis of a HTTPS website, e.g., https://cse.osu.edu. Show the screenshot of the analysis results. Use the knowledge you've learned in class, make the best effort to explain the report. (This is an open-ended question. You may earn up to 0.5% extra credits by showing greater details of your analysis and understanding).



Summary

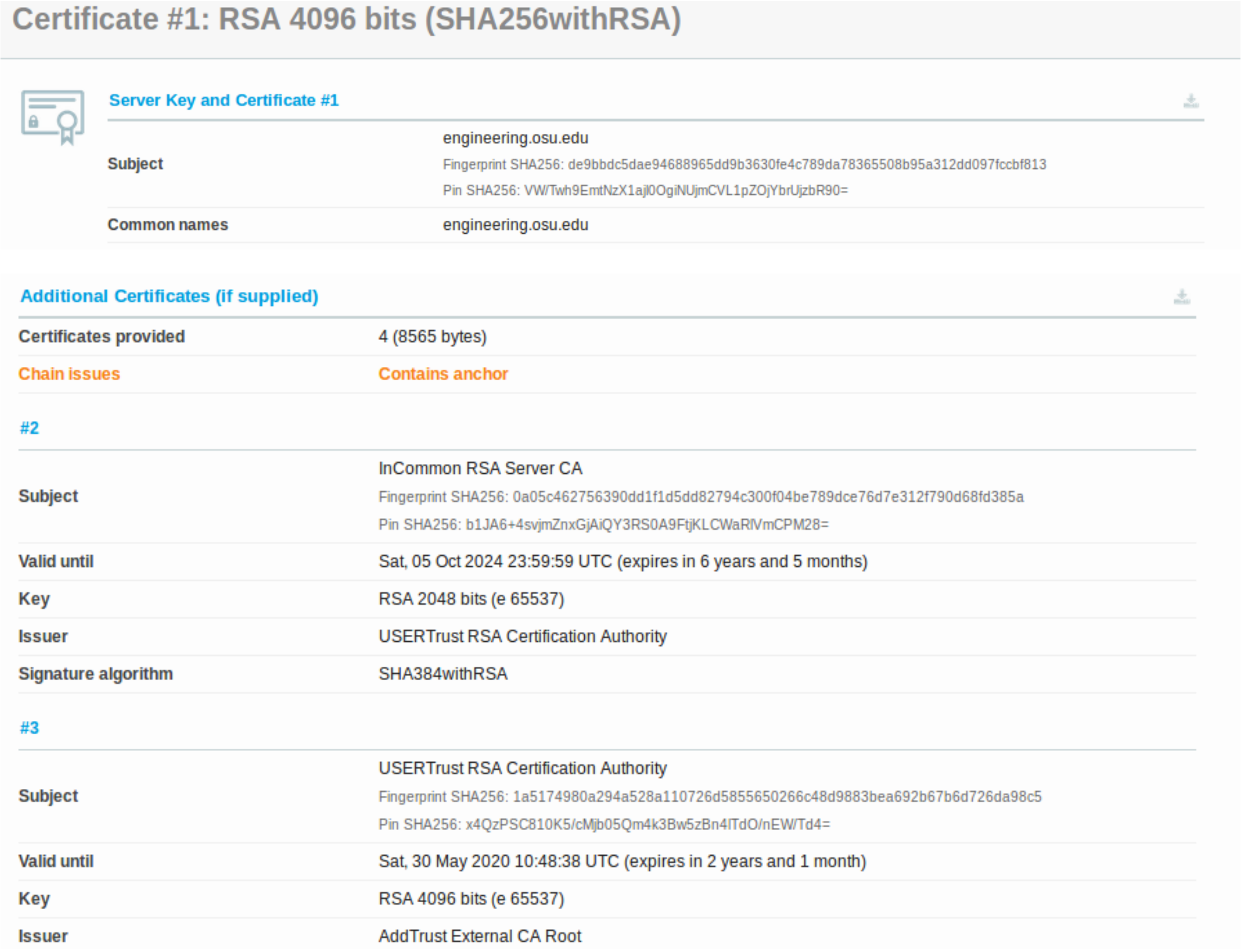
Overall Rating

F

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server is vulnerable to the OpenSSL Padding Oracle vulnerability (CVE-2016-2107) and insecure. Grade set to F.

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »



Certificate #1: RSA 4096 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	engineering.osu.edu Fingerprint SHA256: de9bbdc5dae94688965dd9b3630fe4c789da78365508b95a312dd097fccbf813 Pin SHA256: VW/Twh9EmtNzX1ajl0OgiNUjmCVL1pZOjYbrUjzbR90=
Common names	engineering.osu.edu

Additional Certificates (if supplied)

Certificates provided	4 (8565 bytes)
Chain issues	Contains anchor
#2	
Subject	InCommon RSA Server CA Fingerprint SHA256: 0a05c462756390dd1f1d5dd82794c300f04be789dce76d7e312f790d68fd385a Pin SHA256: b1JA6+4svjmZnxGjAiQY3RS0A9FtjKLCWaRlVmCPM28=
Valid until	Sat, 05 Oct 2024 23:59:59 UTC (expires in 6 years and 5 months)
Key	RSA 2048 bits (e 65537)
Issuer	USERTrust RSA Certification Authority
Signature algorithm	SHA384withRSA
#3	
Subject	USERTrust RSA Certification Authority Fingerprint SHA256: 1a5174980a294a528a110726d5855650266c48d9883bea692b67b6d726da98c5 Pin SHA256: x4QzPSC810K5/cMjb05Qm4k3Bw5zBn4lTdO/nEW/Td4=
Valid until	Sat, 30 May 2020 10:48:38 UTC (expires in 2 years and 1 month)
Key	RSA 4096 bits (e 65537)
Issuer	AddTrust External CA Root

Signature algorithm	SHA384withRSA

#3

Subject	USERTrust RSA Certification Authority Fingerprint SHA256: 1a5174980a294a528a110726d5855650266c48d9883bea692b67b6d726da98c5 Pin SHA256: x4QzPSC810K5/cMjb05Qm4k3Bw5zBn4lTdO/nEW/Td4=
Valid until	Sat, 30 May 2020 10:48:38 UTC (expires in 2 years and 1 month)
Key	RSA 4096 bits (e 65537)
Issuer	AddTrust External CA Root
Signature algorithm	SHA384withRSA

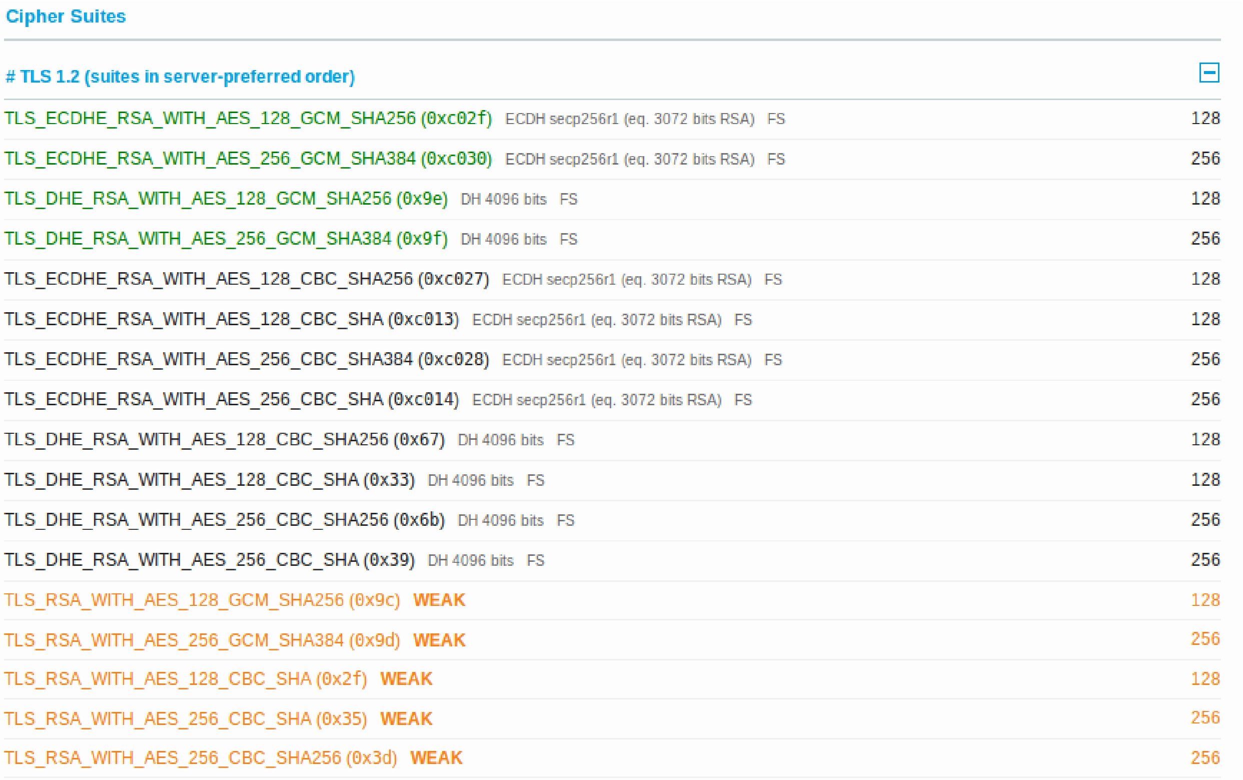
#4

Subject	AddTrust External CA Root In trust store Fingerprint SHA256: 687fa451382278fff0c8b11f8d43d576671c6eb2bceab413fb83d965d06d2ff2 Pin SHA256: lCppFqbkrlJ3EcVFAkeip0+44VaoJUymbnOaEUk7tEU=
Valid until	Sat, 30 May 2020 10:48:38 UTC (expires in 2 years and 1 month)
Key	RSA 2048 bits (e 65537)
Issuer	AddTrust External CA Root Self-signed
Signature algorithm	SHA1withRSA Weak, but no impact on root certificate

Protocols

TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No

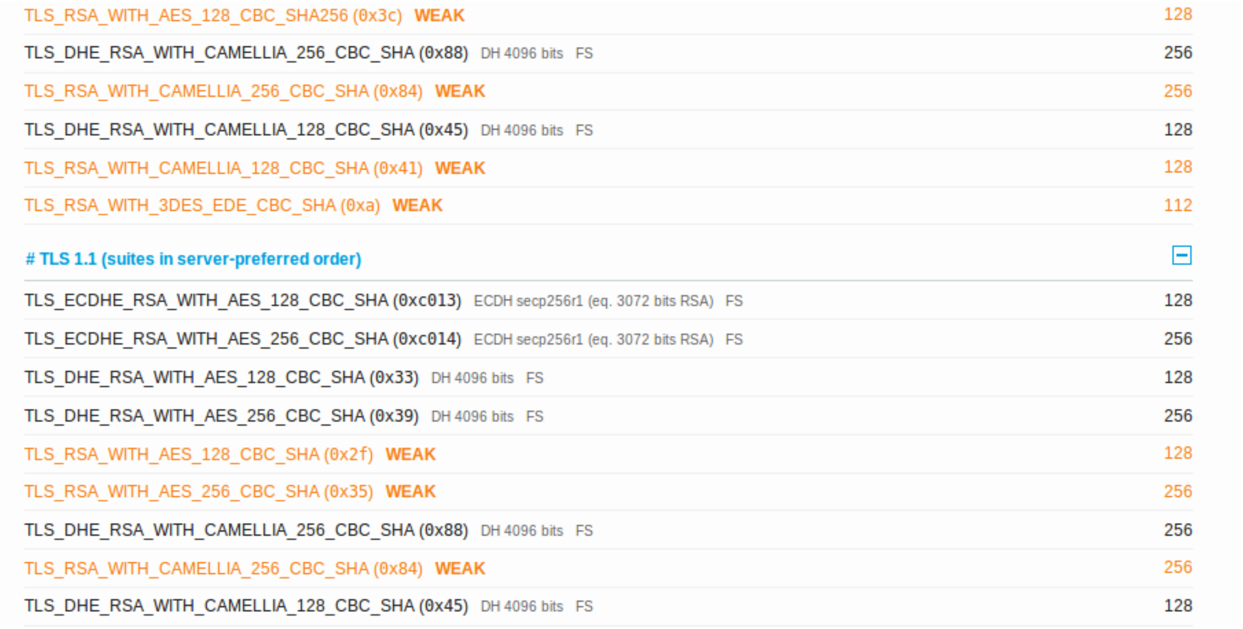
For TLS 1.3 tests, we currently support draft version 18.



Cipher Suites

TLS 1.2 (suites in server-preferred order)

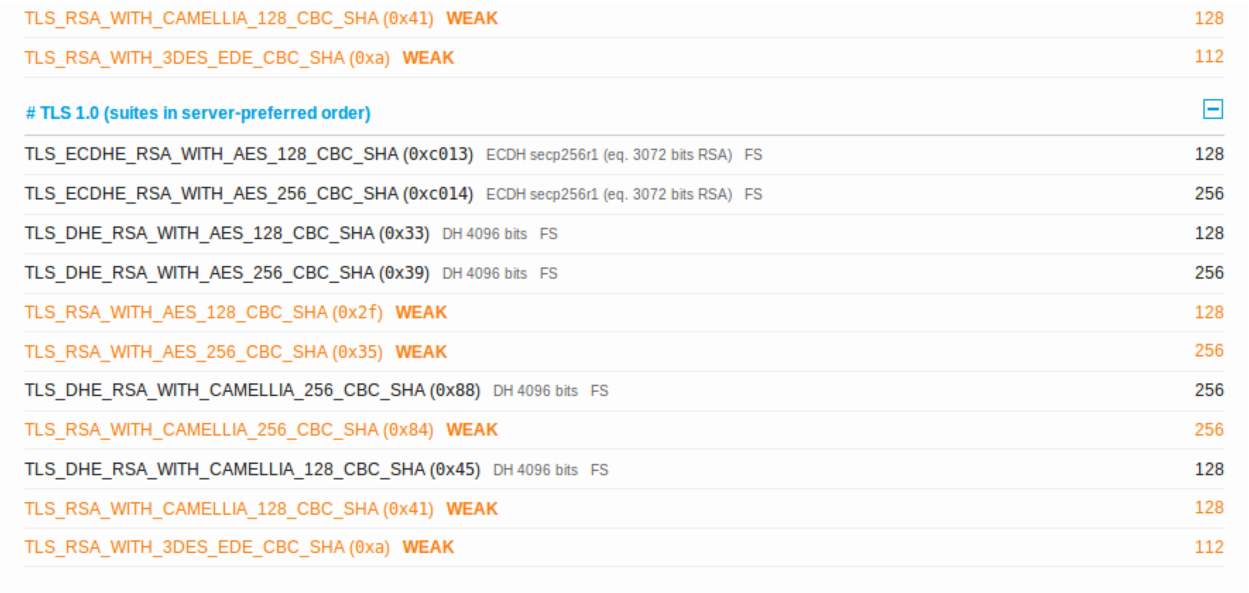
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 4096 bits FS	128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 4096 bits FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) DH 4096 bits FS	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 4096 bits FS	128
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) DH 4096 bits FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 4096 bits FS	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) **WEAK**	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) **WEAK**	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) **WEAK**	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) **WEAK**	256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) **WEAK**	256



TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) **WEAK**	128
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) DH 4096 bits FS	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84) **WEAK**	256
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45) DH 4096 bits FS	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41) **WEAK**	128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) **WEAK**	112

TLS 1.1 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 4096 bits FS	128
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 4096 bits FS	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) **WEAK**	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) **WEAK**	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) DH 4096 bits FS	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84) **WEAK**	256
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45) DH 4096 bits FS	128



TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41) WEAK	128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) WEAK	112
# TLS 1.0 (suites in server-preferred order)	⊟
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 4096 bits FS	128
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 4096 bits FS	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) DH 4096 bits FS	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84) WEAK	256
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45) DH 4096 bits FS	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41) WEAK	128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) WEAK	112

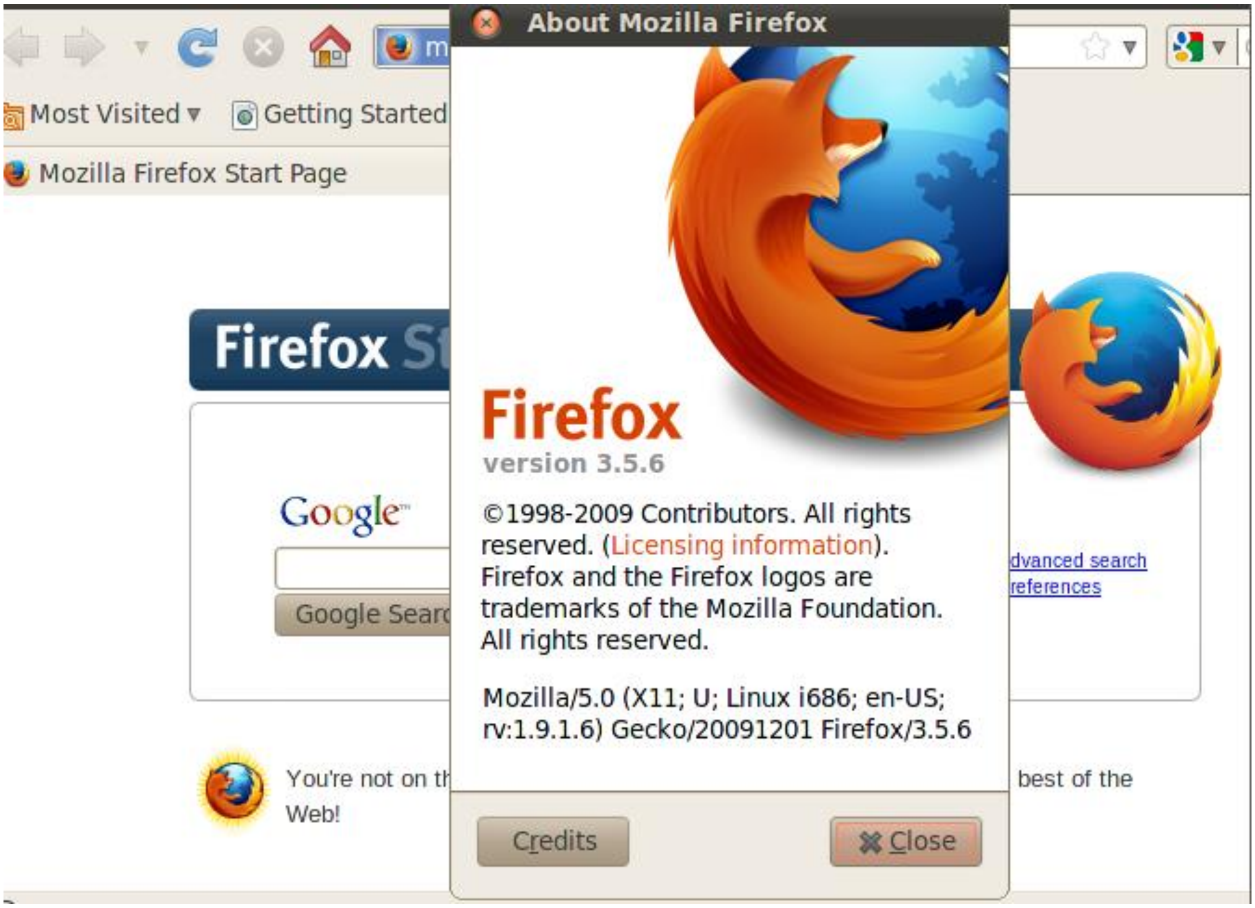
With an overall rating of an F, it is clear that https://www.cse.osu.edu is not a strongly secure website for it's SSL/TLS implementations. Most importantly, the website's server is vulnerable to the OpenSSL Padding Oracle vulnerability. The server has a certificate that is created with the signature algorithm of SHA256 with RSA and a RSA key of 4096 bits. The certificate does not have a weak key and is a trusted according to the report. The server also has 3 other certificates that have different length RSA keys and all use SHA with RSA for the signature algorithm. The protocols that the server uses is TLS 1.0, TLS 1.1, and TLS 1.2, which means that the server does not use TLS 1.3 or neither SSL 2 or SSL3. The cipher suites are all TLS with different key exchange algorithms, where the weaker cipher suites are the least preferred by the server. The website's TLS implementations are not vulnerable to a lot of attacks such as the Beast or Poodle attacks as well as supports secure renegotiation, downgrade attack prevention, forward secrecy and strict transport security. The main problem with the server's SSL/TLS implementations is that is vulnerable to the Open SSL Padding Oracle vulnerability.

4. SSL/TLS attacks (5%)

Take a screenshot to show the installed version of your firefox. Take screenshots to show the

inter-VM communication and you can visit a webpage (e.g., http://www.facebook.com from

your firefox browser. (1%)



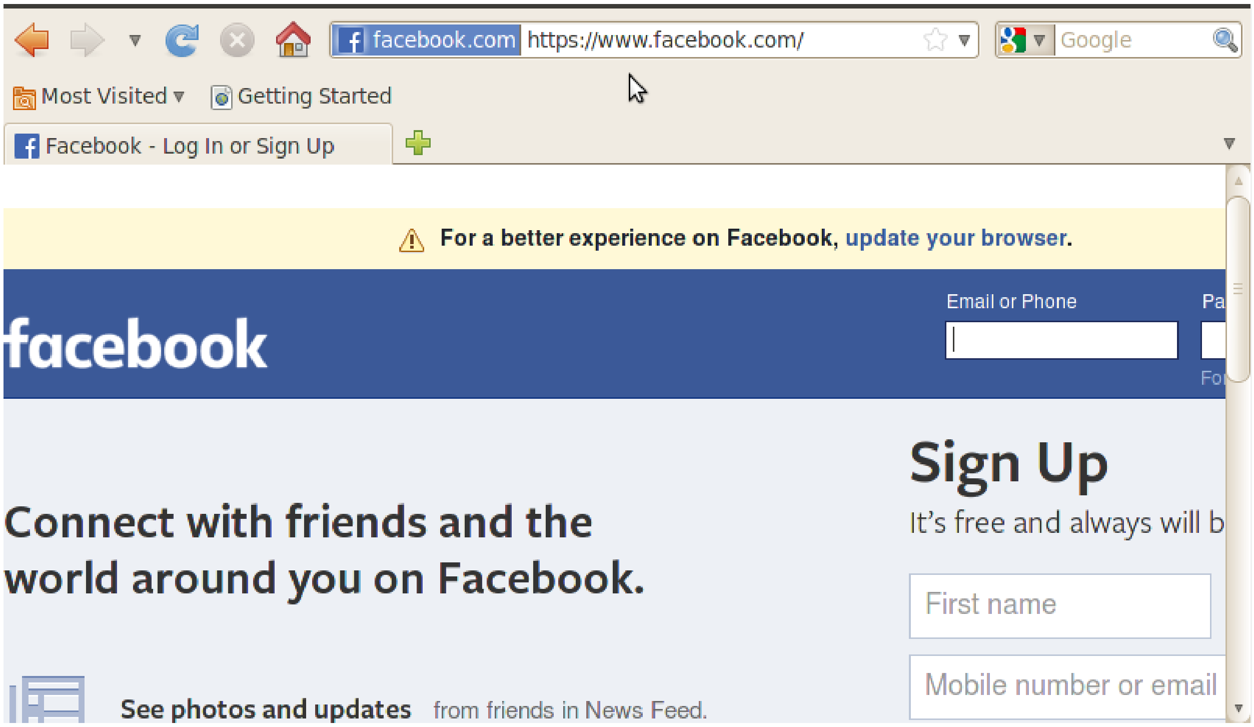
Firefox

version 3.5.6

©1998-2009 Contributors. All rights reserved. (Licensing information). Firefox and the Firefox logos are trademarks of the Mozilla Foundation. All rights reserved.

Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.1.6) Gecko/20091201 Firefox/3.5.6

You're not on th best of the Web!



https://www.facebook.com/

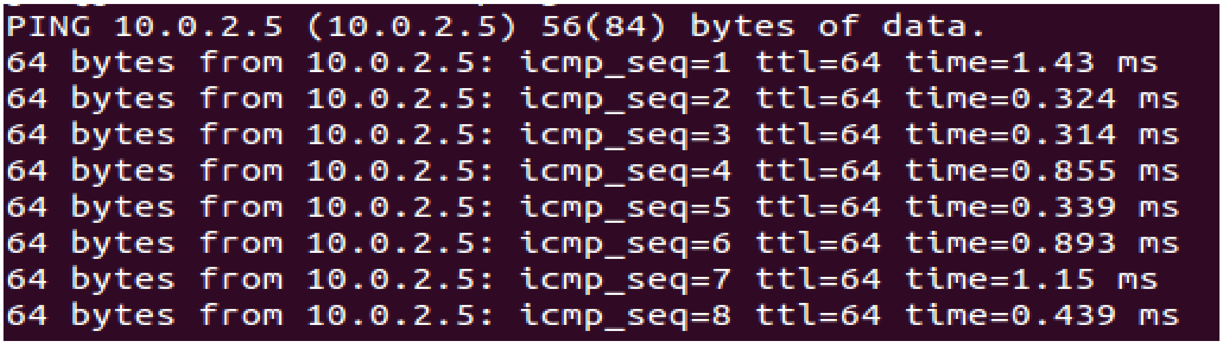
⚠ For a better experience on Facebook, update your browser.

Sign Up

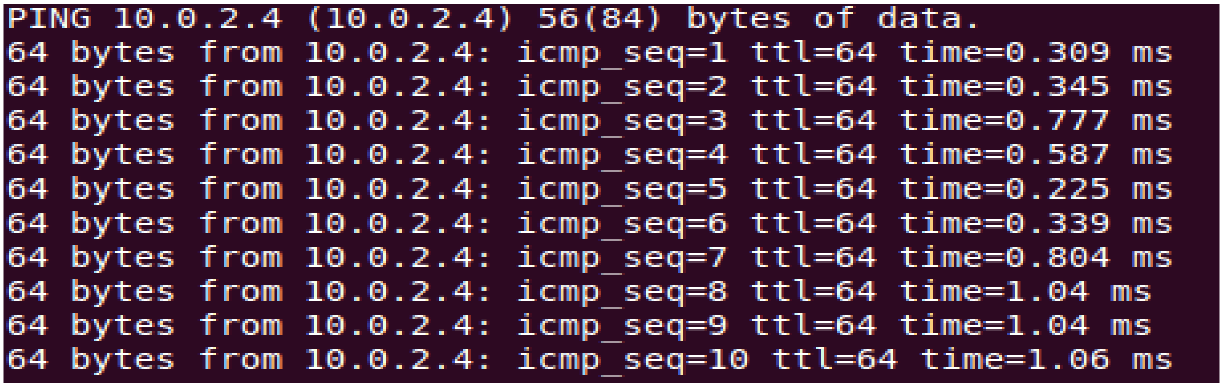
It's free and always will b

Connect with friends and the world around you on Facebook.

See photos and updates from friends in News Feed.



```
PING 10.0.2.5 (10.0.2.5) 56(84) bytes of data.
64 bytes from 10.0.2.5: icmp_seq=1 ttl=64 time=1.43 ms
64 bytes from 10.0.2.5: icmp_seq=2 ttl=64 time=0.324 ms
64 bytes from 10.0.2.5: icmp_seq=3 ttl=64 time=0.314 ms
64 bytes from 10.0.2.5: icmp_seq=4 ttl=64 time=0.855 ms
64 bytes from 10.0.2.5: icmp_seq=5 ttl=64 time=0.339 ms
64 bytes from 10.0.2.5: icmp_seq=6 ttl=64 time=0.893 ms
64 bytes from 10.0.2.5: icmp_seq=7 ttl=64 time=1.15 ms
64 bytes from 10.0.2.5: icmp_seq=8 ttl=64 time=0.439 ms
```

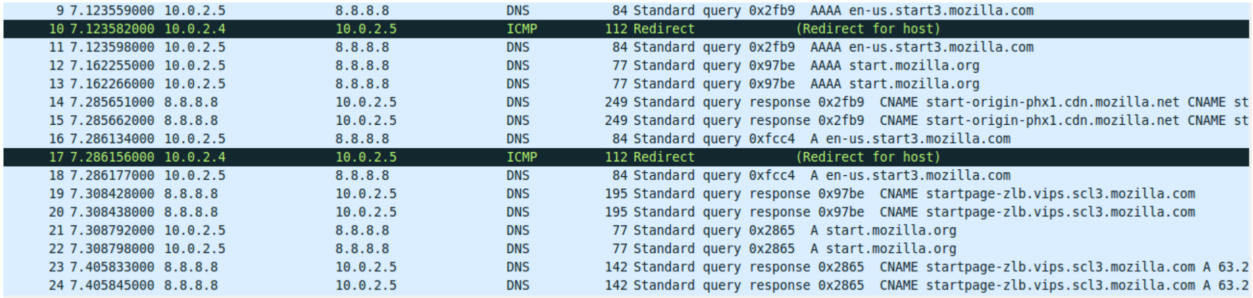


```
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=0.309 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=0.345 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=0.777 ms
64 bytes from 10.0.2.4: icmp_seq=4 ttl=64 time=0.587 ms
64 bytes from 10.0.2.4: icmp_seq=5 ttl=64 time=0.225 ms
64 bytes from 10.0.2.4: icmp_seq=6 ttl=64 time=0.339 ms
64 bytes from 10.0.2.4: icmp_seq=7 ttl=64 time=0.804 ms
64 bytes from 10.0.2.4: icmp_seq=8 ttl=64 time=1.04 ms
64 bytes from 10.0.2.4: icmp_seq=9 ttl=64 time=1.04 ms
64 bytes from 10.0.2.4: icmp_seq=10 ttl=64 time=1.06 ms
```

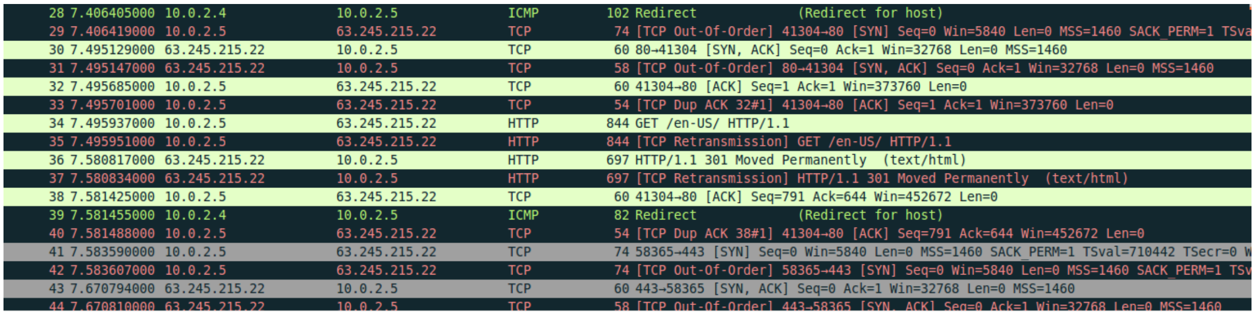
4.2 (2%) Downgrade HTTPS to HTTP using sslstrip

Step 4: In the Victim VM, in the firefox browser, visit facebook.com. Now both webpages should be automatically directed to HTTPS links: https://www.facebook.com.

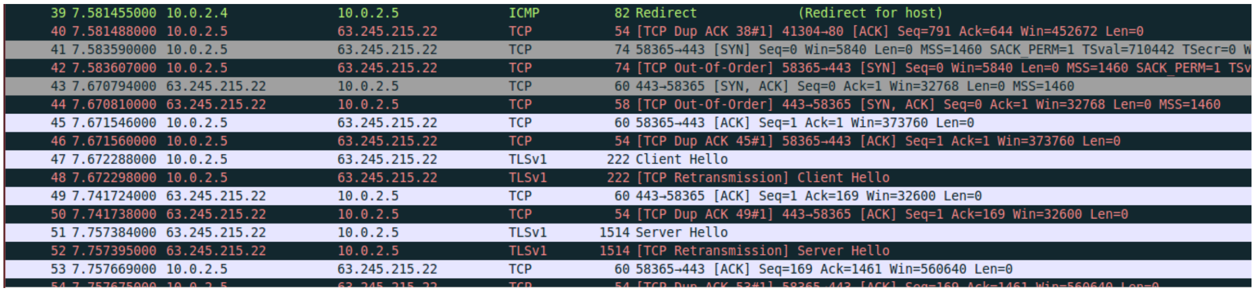
Step 5: In the "secure sign-in" box, enter a (fake) online ID and passcode, and click on the "sign in" button.



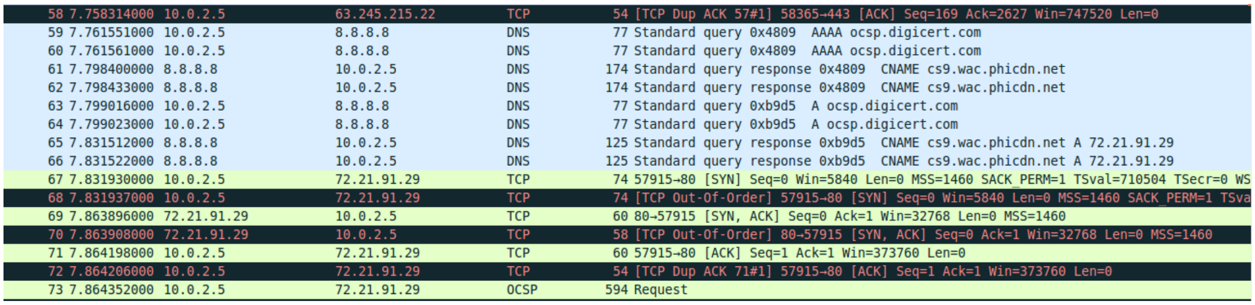
```
  9 7.123559000 10.0.2.5        8.8.8.8         DNS     84 Standard query 0x2fb9  AAAA en-us.start3.mozilla.com
 10 7.123582000 10.0.2.4        10.0.2.5        ICMP   112 Redirect              (Redirect for host)
 11 7.123598000 10.0.2.5        8.8.8.8         DNS     84 Standard query 0x2fb9  AAAA en-us.start3.mozilla.com
 12 7.162255000 10.0.2.5        8.8.8.8         DNS     77 Standard query 0x97be  AAAA start.mozilla.org
 13 7.162266000 10.0.2.5        8.8.8.8         DNS     77 Standard query 0x97be  AAAA start.mozilla.org
 14 7.285651000 8.8.8.8         10.0.2.5        DNS    249 Standard query response 0x2fb9  CNAME start-origin-phx1.cdn.mozilla.net CNAME st
 15 7.285662000 8.8.8.8         10.0.2.5        DNS    249 Standard query response 0x2fb9  CNAME start-origin-phx1.cdn.mozilla.net CNAME st
 16 7.286134000 10.0.2.5        8.8.8.8         DNS     84 Standard query 0xfcc4  A en-us.start3.mozilla.com
 17 7.286156000 10.0.2.4        10.0.2.5        ICMP   112 Redirect              (Redirect for host)
 18 7.286177000 10.0.2.5        8.8.8.8         DNS     84 Standard query 0xfcc4  A en-us.start3.mozilla.com
 19 7.308428000 8.8.8.8         10.0.2.5        DNS    195 Standard query response 0x97be  CNAME startpage-zlb.vips.scl3.mozilla.com
 20 7.308438000 8.8.8.8         10.0.2.5        DNS    195 Standard query response 0x97be  CNAME startpage-zlb.vips.scl3.mozilla.com
 21 7.308792000 10.0.2.5        8.8.8.8         DNS     77 Standard query 0x2865  A start.mozilla.org
 22 7.308798000 10.0.2.5        8.8.8.8         DNS     77 Standard query 0x2865  A start.mozilla.org
 23 7.405833000 8.8.8.8         10.0.2.5        DNS    142 Standard query response 0x2865  CNAME startpage-zlb.vips.scl3.mozilla.com A 63.2
 24 7.405845000 8.8.8.8         10.0.2.5        DNS    142 Standard query response 0x2865  CNAME startpage-zlb.vips.scl3.mozilla.com A 63.2
```



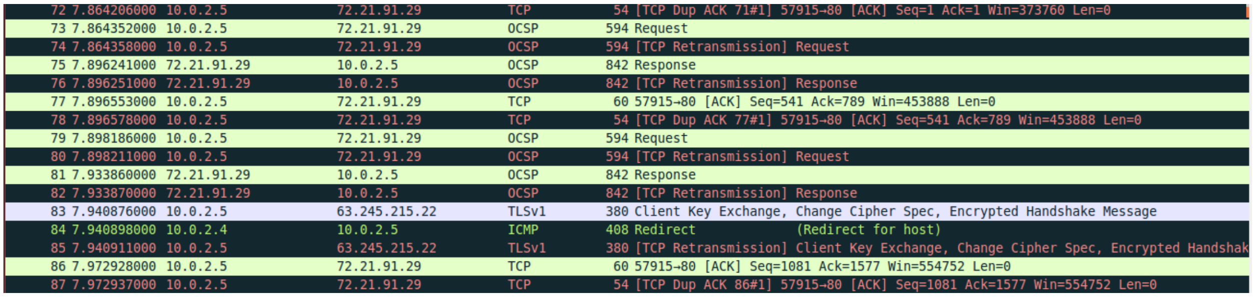
```
28 7.406405000  10.0.2.4          10.0.2.5          ICMP       102 Redirect              (Redirect for host)
29 7.406419000  10.0.2.5          63.245.215.22     TCP         74 [TCP Out-Of-Order] 41304→80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSva
30 7.495129000  63.245.215.22     10.0.2.5          TCP         60 80→41304 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
31 7.495147000  63.245.215.22     10.0.2.5          TCP         58 [TCP Out-Of-Order] 80→41304 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
32 7.495685000  10.0.2.5          63.245.215.22     TCP         60 41304→80 [ACK] Seq=1 Ack=1 Win=373760 Len=0
33 7.495701000  10.0.2.5          63.245.215.22     TCP         54 [TCP Dup ACK 32#1] 41304→80 [ACK] Seq=1 Ack=1 Win=373760 Len=0
34 7.495937000  10.0.2.5          63.245.215.22     HTTP       844 GET /en-US/ HTTP/1.1
35 7.495951000  10.0.2.5          63.245.215.22     HTTP       844 [TCP Retransmission] GET /en-US/ HTTP/1.1
36 7.580817000  63.245.215.22     10.0.2.5          HTTP       697 HTTP/1.1 301 Moved Permanently  (text/html)
37 7.580834000  63.245.215.22     10.0.2.5          HTTP       697 [TCP Retransmission] HTTP/1.1 301 Moved Permanently  (text/html)
38 7.581425000  10.0.2.5          63.245.215.22     TCP         60 41304→80 [ACK] Seq=791 Ack=644 Win=452672 Len=0
39 7.581455000  10.0.2.4          10.0.2.5          ICMP        82 Redirect              (Redirect for host)
40 7.581488000  10.0.2.5          63.245.215.22     TCP         54 [TCP Dup ACK 38#1] 41304→80 [ACK] Seq=791 Ack=644 Win=452672 Len=0
41 7.583590000  10.0.2.5          63.245.215.22     TCP         74 58365→443 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=710442 TSecr=0 W
42 7.583607000  10.0.2.5          63.245.215.22     TCP         74 [TCP Out-Of-Order] 58365→443 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSv
43 7.670794000  63.245.215.22     10.0.2.5          TCP         60 443→58365 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
44 7.670810000  63.245.215.22     10.0.2.5          TCP         58 [TCP Out-Of-Order] 443→58365 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
```



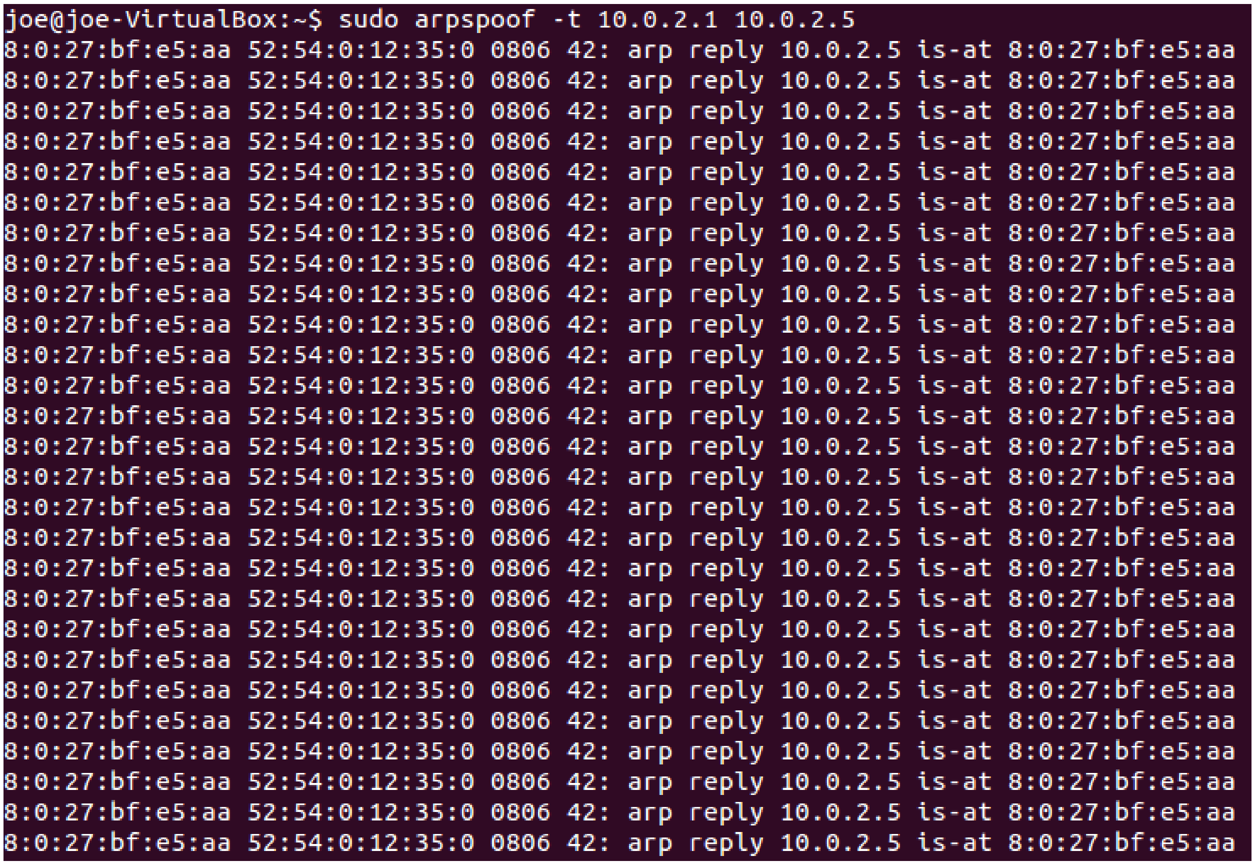
```
39 7.581455000  10.0.2.4          10.0.2.5          ICMP        82 Redirect              (Redirect for host)
40 7.581488000  10.0.2.5          63.245.215.22     TCP         54 [TCP Dup ACK 38#1] 41304→80 [ACK] Seq=791 Ack=644 Win=452672 Len=0
41 7.583590000  10.0.2.5          63.245.215.22     TCP         74 58365→443 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=710442 TSecr=0 W
42 7.583607000  10.0.2.5          63.245.215.22     TCP         74 [TCP Out-Of-Order] 58365→443 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSv
43 7.670794000  63.245.215.22     10.0.2.5          TCP         60 443→58365 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
44 7.670810000  63.245.215.22     10.0.2.5          TCP         58 [TCP Out-Of-Order] 443→58365 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
45 7.671546000  10.0.2.5          63.245.215.22     TCP         60 58365→443 [ACK] Seq=1 Ack=1 Win=373760 Len=0
46 7.671560000  10.0.2.5          63.245.215.22     TCP         54 [TCP Dup ACK 45#1] 58365→443 [ACK] Seq=1 Ack=1 Win=373760 Len=0
47 7.672288000  10.0.2.5          63.245.215.22     TLSv1      222 Client Hello
48 7.672298000  10.0.2.5          63.245.215.22     TLSv1      222 [TCP Retransmission] Client Hello
49 7.741724000  63.245.215.22     10.0.2.5          TCP         60 443→58365 [ACK] Seq=1 Ack=169 Win=32600 Len=0
50 7.741738000  63.245.215.22     10.0.2.5          TCP         54 [TCP Dup ACK 49#1] 443→58365 [ACK] Seq=1 Ack=169 Win=32600 Len=0
51 7.757384000  63.245.215.22     10.0.2.5          TLSv1     1514 Server Hello
52 7.757395000  63.245.215.22     10.0.2.5          TLSv1     1514 [TCP Retransmission] Server Hello
53 7.757669000  10.0.2.5          63.245.215.22     TCP         60 58365→443 [ACK] Seq=169 Ack=1461 Win=560640 Len=0
54 7.757675000  10.0.2.5          63.245.215.22     TCP         54 [TCP Dup ACK 53#1] 58365→443 [ACK] Seq=169 Ack=1461 Win=560640 Len=0
```



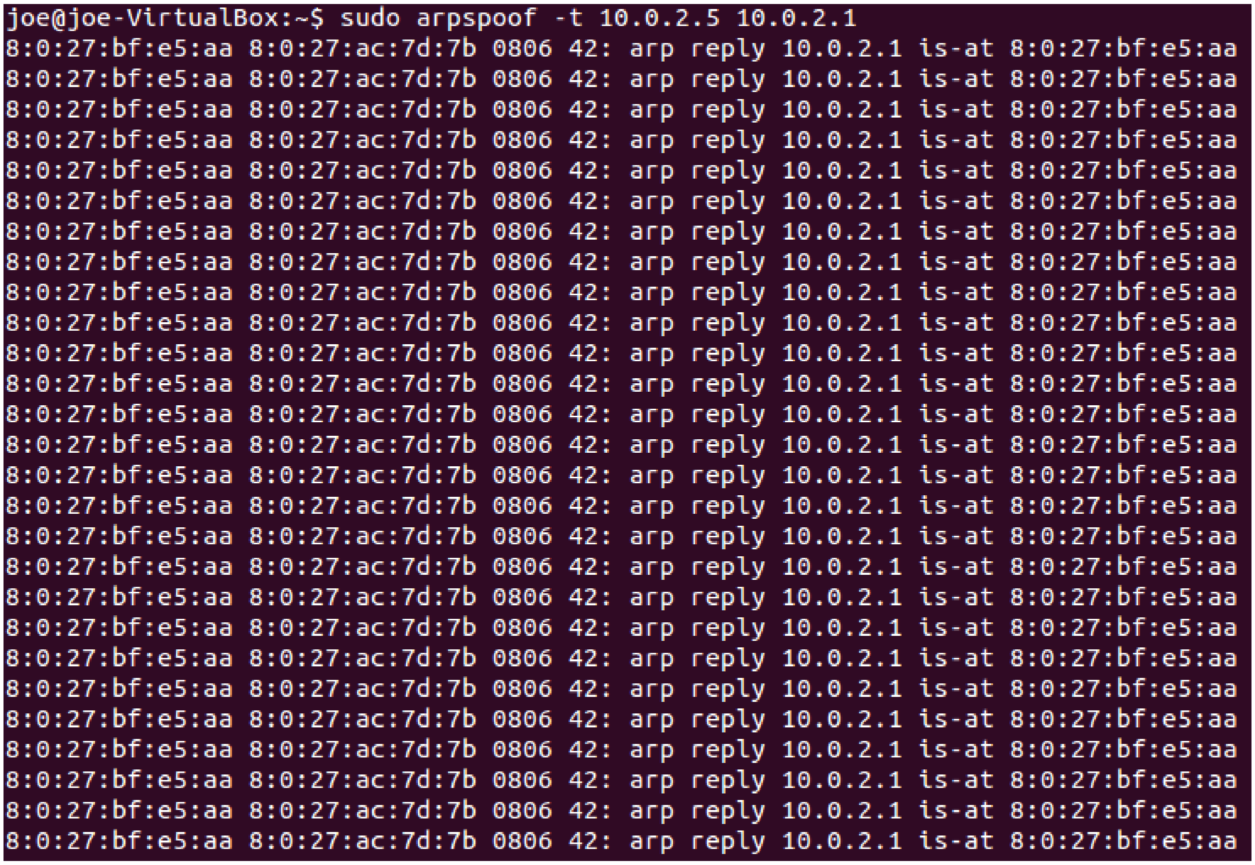
```
58 7.758314000  10.0.2.5          63.245.215.22     TCP         54 [TCP Dup ACK 57#1] 58365→443 [ACK] Seq=169 Ack=2627 Win=747520 Len=0
59 7.761551000  10.0.2.5          8.8.8.8           DNS         77 Standard query 0x4809  AAAA ocsp.digicert.com
60 7.761561000  10.0.2.5          8.8.8.8           DNS         77 Standard query 0x4809  AAAA ocsp.digicert.com
61 7.798400000  8.8.8.8           10.0.2.5          DNS        174 Standard query response 0x4809  CNAME cs9.wac.phicdn.net
62 7.798433000  8.8.8.8           10.0.2.5          DNS        174 Standard query response 0x4809  CNAME cs9.wac.phicdn.net
63 7.799016000  10.0.2.5          8.8.8.8           DNS         77 Standard query 0xb9d5  A ocsp.digicert.com
64 7.799023000  10.0.2.5          8.8.8.8           DNS         77 Standard query 0xb9d5  A ocsp.digicert.com
65 7.831512000  8.8.8.8           10.0.2.5          DNS        125 Standard query response 0xb9d5  CNAME cs9.wac.phicdn.net A 72.21.91.29
66 7.831522000  8.8.8.8           10.0.2.5          DNS        125 Standard query response 0xb9d5  CNAME cs9.wac.phicdn.net A 72.21.91.29
67 7.831930000  10.0.2.5          72.21.91.29       TCP         74 57915→80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=710504 TSecr=0 WS
68 7.831937000  10.0.2.5          72.21.91.29       TCP         74 [TCP Out-Of-Order] 57915→80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSva
69 7.863896000  72.21.91.29       10.0.2.5          TCP         60 80→57915 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
70 7.863908000  72.21.91.29       10.0.2.5          TCP         58 [TCP Out-Of-Order] 80→57915 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
71 7.864198000  10.0.2.5          72.21.91.29       TCP         60 57915→80 [ACK] Seq=1 Ack=1 Win=373760 Len=0
72 7.864206000  10.0.2.5          72.21.91.29       TCP         54 [TCP Dup ACK 71#1] 57915→80 [ACK] Seq=1 Ack=1 Win=373760 Len=0
73 7.864352000  10.0.2.5          72.21.91.29       OCSP       594 Request
```



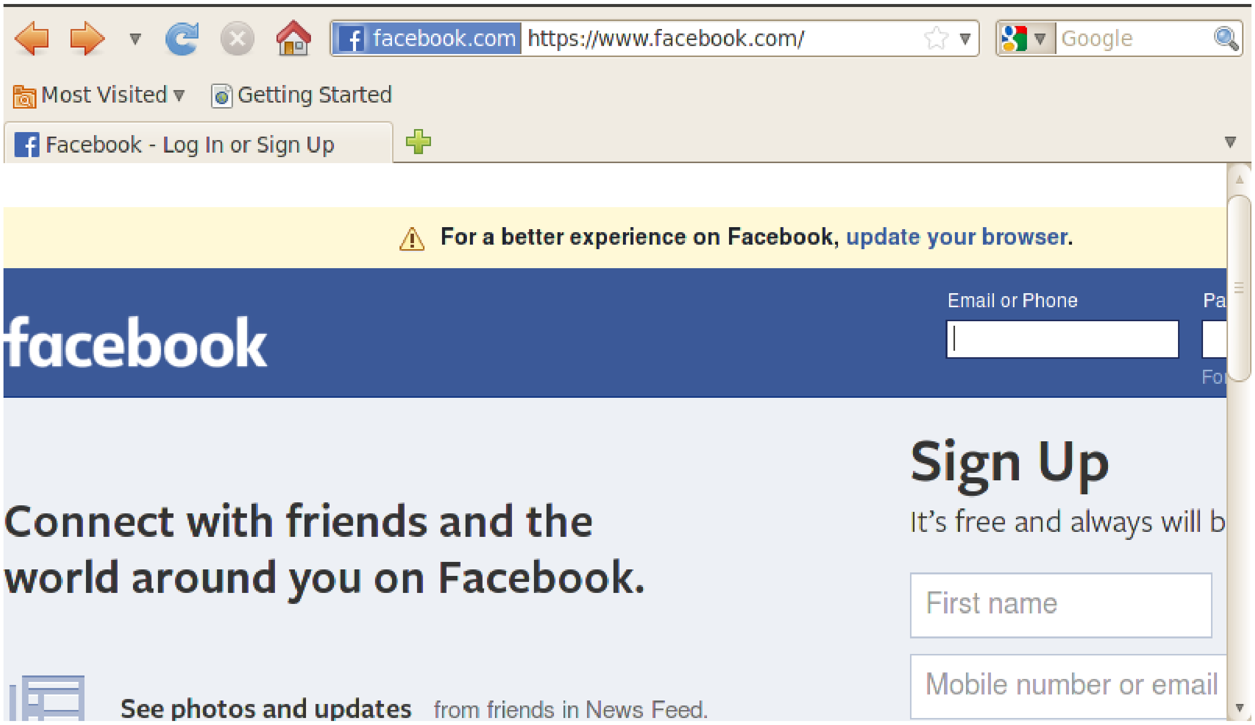
```
72 7.864206000  10.0.2.5          72.21.91.29       TCP         54 [TCP Dup ACK 71#1] 57915→80 [ACK] Seq=1 Ack=1 Win=373760 Len=0
73 7.864352000  10.0.2.5          72.21.91.29       OCSP       594 Request
74 7.864358000  10.0.2.5          72.21.91.29       OCSP       594 [TCP Retransmission] Request
75 7.896241000  72.21.91.29       10.0.2.5          OCSP       842 Response
76 7.896251000  72.21.91.29       10.0.2.5          OCSP       842 [TCP Retransmission] Response
77 7.896553000  10.0.2.5          72.21.91.29       TCP         60 57915→80 [ACK] Seq=541 Ack=789 Win=453888 Len=0
78 7.896578000  10.0.2.5          72.21.91.29       TCP         54 [TCP Dup ACK 77#1] 57915→80 [ACK] Seq=541 Ack=789 Win=453888 Len=0
79 7.898186000  10.0.2.5          72.21.91.29       OCSP       594 Request
80 7.898211000  10.0.2.5          72.21.91.29       OCSP       594 [TCP Retransmission] Request
81 7.933860000  72.21.91.29       10.0.2.5          OCSP       842 Response
82 7.933870000  72.21.91.29       10.0.2.5          OCSP       842 [TCP Retransmission] Response
83 7.940876000  10.0.2.5          63.245.215.22     TLSv1      380 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
84 7.940898000  10.0.2.4          10.0.2.5          ICMP       408 Redirect              (Redirect for host)
85 7.940911000  10.0.2.5          63.245.215.22     TLSv1      380 [TCP Retransmission] Client Key Exchange, Change Cipher Spec, Encrypted Handshak
86 7.972928000  10.0.2.5          72.21.91.29       TCP         60 57915→80 [ACK] Seq=1081 Ack=1577 Win=554752 Len=0
87 7.972937000  10.0.2.5          72.21.91.29       TCP         54 [TCP Dup ACK 86#1] 57915→80 [ACK] Seq=1081 Ack=1577 Win=554752 Len=0
```



```
joe@joe-VirtualBox:~$ sudo arpspoof -t 10.0.2.1 10.0.2.5
8:0:27:bf:e5:aa 52:54:0:12:35:0 0806 42: arp reply 10.0.2.5 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 52:54:0:12:35:0 0806 42: arp reply 10.0.2.5 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 52:54:0:12:35:0 0806 42: arp reply 10.0.2.5 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 52:54:0:12:35:0 0806 42: arp reply 10.0.2.5 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 52:54:0:12:35:0 0806 42: arp reply 10.0.2.5 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 52:54:0:12:35:0 0806 42: arp reply 10.0.2.5 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 52:54:0:12:35:0 0806 42: arp reply 10.0.2.5 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 52:54:0:12:35:0 0806 42: arp reply 10.0.2.5 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 52:54:0:12:35:0 0806 42: arp reply 10.0.2.5 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 52:54:0:12:35:0 0806 42: arp reply 10.0.2.5 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 52:54:0:12:35:0 0806 42: arp reply 10.0.2.5 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 52:54:0:12:35:0 0806 42: arp reply 10.0.2.5 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 52:54:0:12:35:0 0806 42: arp reply 10.0.2.5 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 52:54:0:12:35:0 0806 42: arp reply 10.0.2.5 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 52:54:0:12:35:0 0806 42: arp reply 10.0.2.5 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 52:54:0:12:35:0 0806 42: arp reply 10.0.2.5 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 52:54:0:12:35:0 0806 42: arp reply 10.0.2.5 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 52:54:0:12:35:0 0806 42: arp reply 10.0.2.5 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 52:54:0:12:35:0 0806 42: arp reply 10.0.2.5 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 52:54:0:12:35:0 0806 42: arp reply 10.0.2.5 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 52:54:0:12:35:0 0806 42: arp reply 10.0.2.5 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 52:54:0:12:35:0 0806 42: arp reply 10.0.2.5 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 52:54:0:12:35:0 0806 42: arp reply 10.0.2.5 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 52:54:0:12:35:0 0806 42: arp reply 10.0.2.5 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 52:54:0:12:35:0 0806 42: arp reply 10.0.2.5 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 52:54:0:12:35:0 0806 42: arp reply 10.0.2.5 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 52:54:0:12:35:0 0806 42: arp reply 10.0.2.5 is-at 8:0:27:bf:e5:aa
```



```
joe@joe-VirtualBox:~$ sudo arpspoof -t 10.0.2.5 10.0.2.1
8:0:27:bf:e5:aa 8:0:27:ac:7d:7b 0806 42: arp reply 10.0.2.1 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 8:0:27:ac:7d:7b 0806 42: arp reply 10.0.2.1 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 8:0:27:ac:7d:7b 0806 42: arp reply 10.0.2.1 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 8:0:27:ac:7d:7b 0806 42: arp reply 10.0.2.1 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 8:0:27:ac:7d:7b 0806 42: arp reply 10.0.2.1 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 8:0:27:ac:7d:7b 0806 42: arp reply 10.0.2.1 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 8:0:27:ac:7d:7b 0806 42: arp reply 10.0.2.1 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 8:0:27:ac:7d:7b 0806 42: arp reply 10.0.2.1 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 8:0:27:ac:7d:7b 0806 42: arp reply 10.0.2.1 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 8:0:27:ac:7d:7b 0806 42: arp reply 10.0.2.1 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 8:0:27:ac:7d:7b 0806 42: arp reply 10.0.2.1 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 8:0:27:ac:7d:7b 0806 42: arp reply 10.0.2.1 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 8:0:27:ac:7d:7b 0806 42: arp reply 10.0.2.1 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 8:0:27:ac:7d:7b 0806 42: arp reply 10.0.2.1 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 8:0:27:ac:7d:7b 0806 42: arp reply 10.0.2.1 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 8:0:27:ac:7d:7b 0806 42: arp reply 10.0.2.1 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 8:0:27:ac:7d:7b 0806 42: arp reply 10.0.2.1 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 8:0:27:ac:7d:7b 0806 42: arp reply 10.0.2.1 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 8:0:27:ac:7d:7b 0806 42: arp reply 10.0.2.1 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 8:0:27:ac:7d:7b 0806 42: arp reply 10.0.2.1 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 8:0:27:ac:7d:7b 0806 42: arp reply 10.0.2.1 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 8:0:27:ac:7d:7b 0806 42: arp reply 10.0.2.1 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 8:0:27:ac:7d:7b 0806 42: arp reply 10.0.2.1 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 8:0:27:ac:7d:7b 0806 42: arp reply 10.0.2.1 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 8:0:27:ac:7d:7b 0806 42: arp reply 10.0.2.1 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 8:0:27:ac:7d:7b 0806 42: arp reply 10.0.2.1 is-at 8:0:27:bf:e5:aa
8:0:27:bf:e5:aa 8:0:27:ac:7d:7b 0806 42: arp reply 10.0.2.1 is-at 8:0:27:bf:e5:aa
```



For a better experience on Facebook, update your browser.

Sign Up

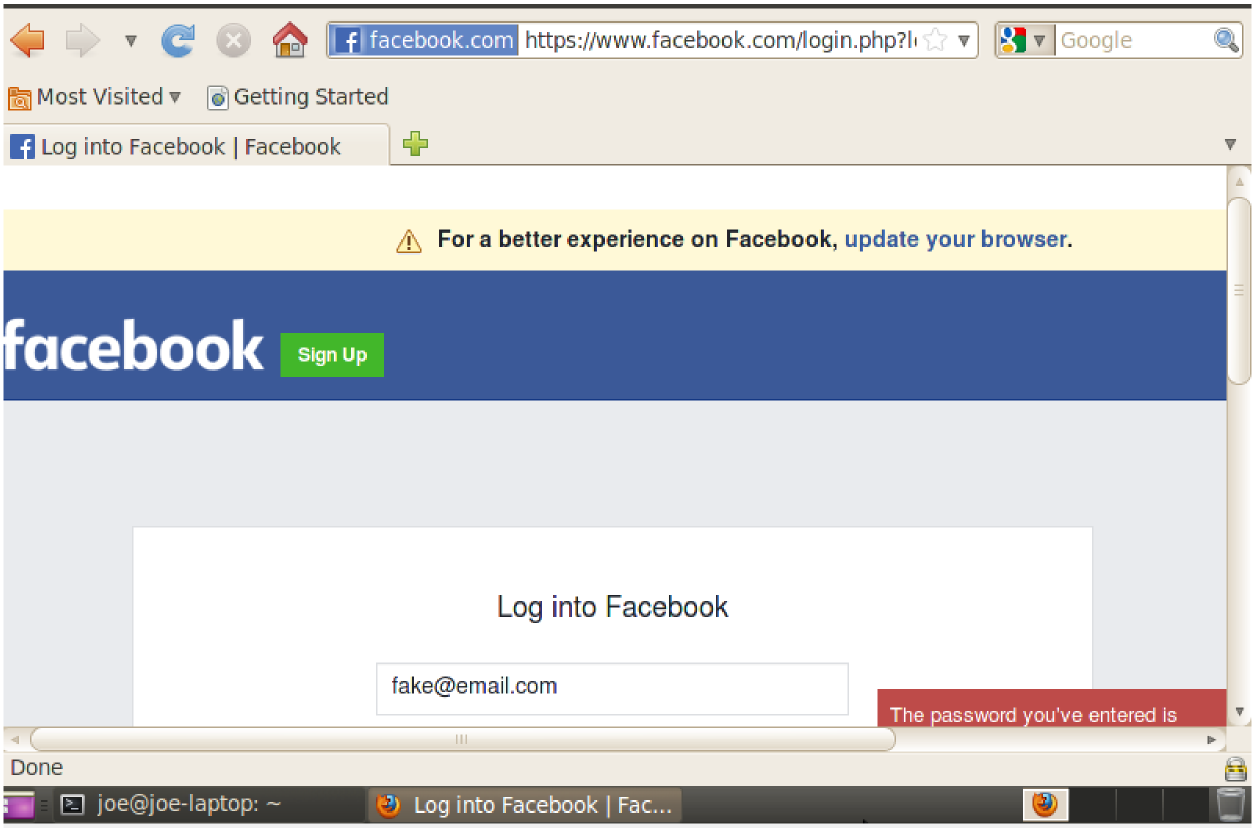
It's free and always will b

Connect with friends and the world around you on Facebook.

First name

Mobile number or email

See photos and updates from friends in News Feed.



https://www.facebook.com/login.php?l

For a better experience on Facebook, update your browser.

Log into Facebook

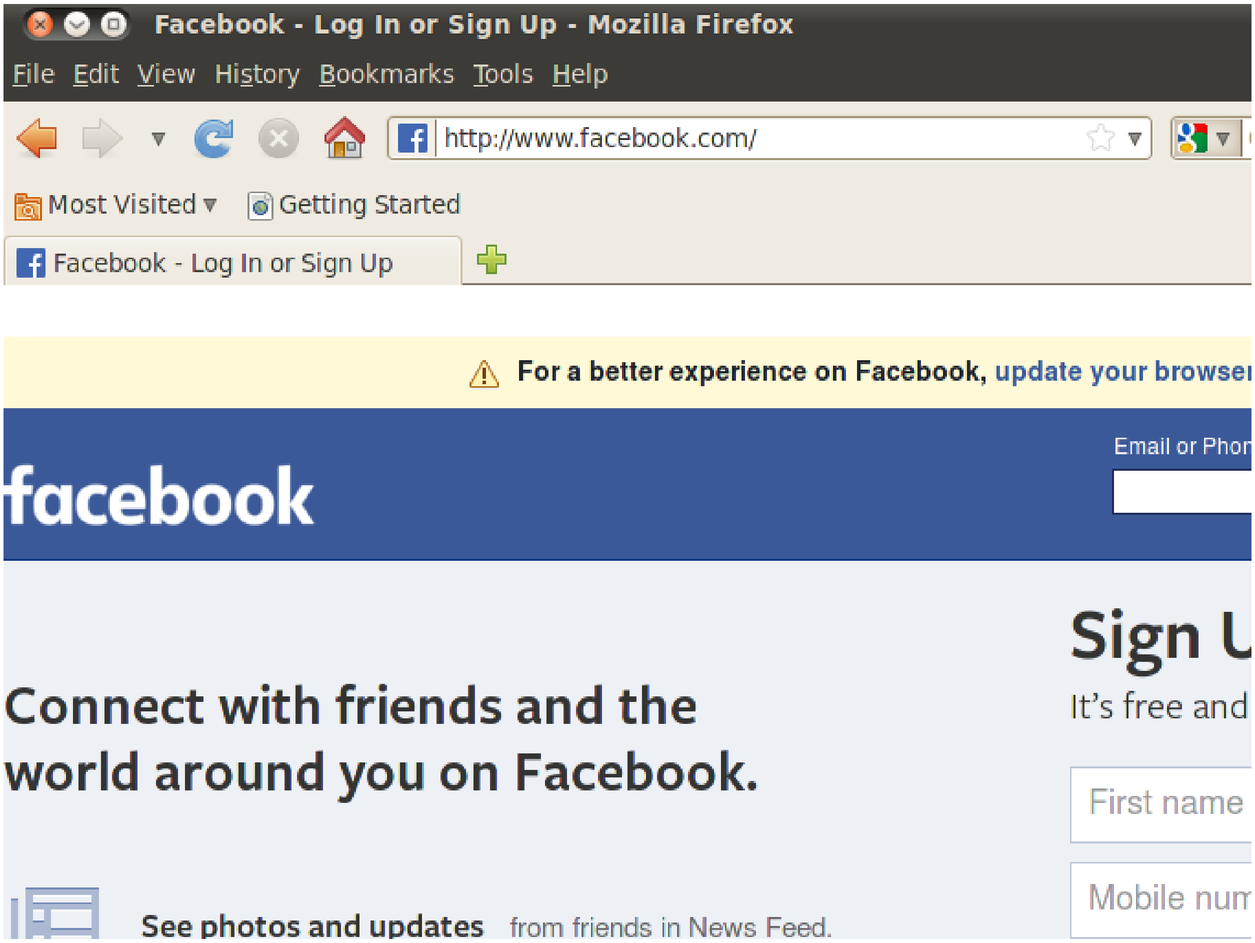
fake@email.com

The password you've entered is

Step 9: Run sslstrip:

Step 10: In the Victim VM, in the firefox browser, visit facebook.com. (Tips: it should not redirect to HTTPS this time, instead you should be visiting http://www.facebook.com)

Step 11: In the “secure sign-in” box, enter a (fake) online ID and passcode, and click on the “sign in” button.



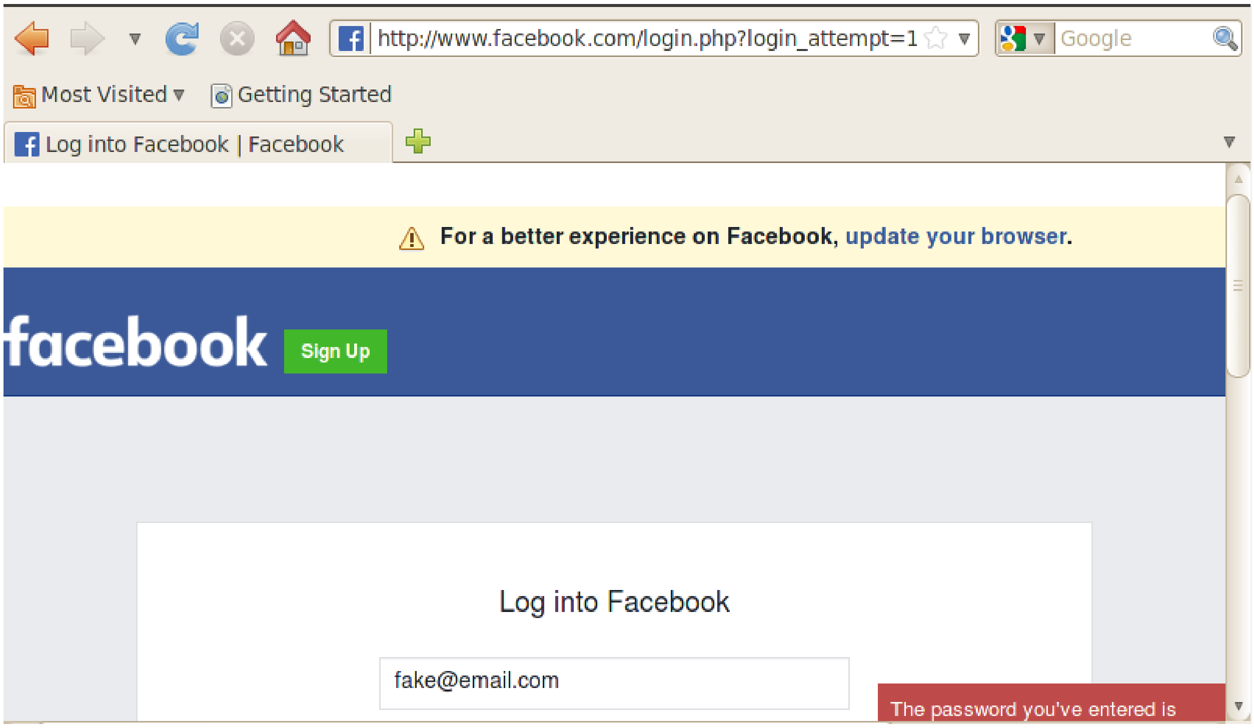
Facebook - Log In or Sign Up - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.facebook.com/
Most Visited
Getting Started
Facebook - Log In or Sign Up

For a better experience on Facebook, update your browser

Connect with friends and the world around you on Facebook.

See photos and updates from friends in News Feed.

Sign U
It's free and
First name
Mobile num

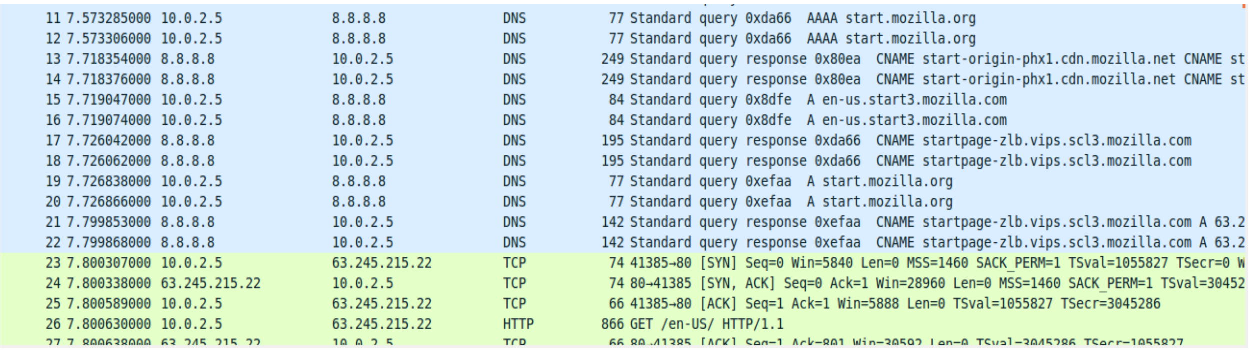

http://www.facebook.com/login.php?login_attempt=1
Google
Most Visited
Getting Started
Log into Facebook | Facebook
facebook
Sign Up

For a better experience on Facebook, update your browser.

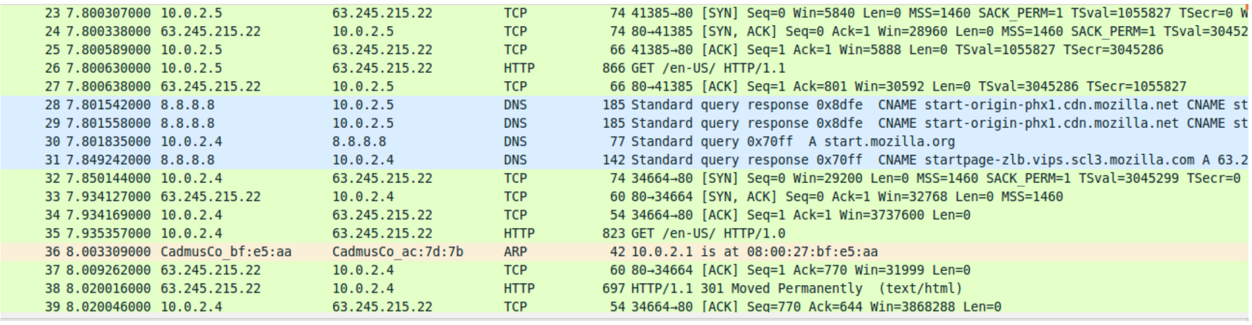
Log into Facebook

fake@email.com

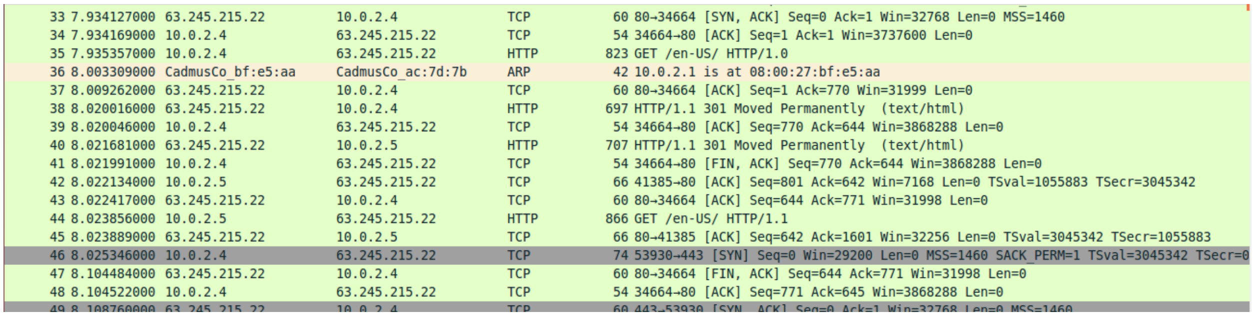
The password you've entered is



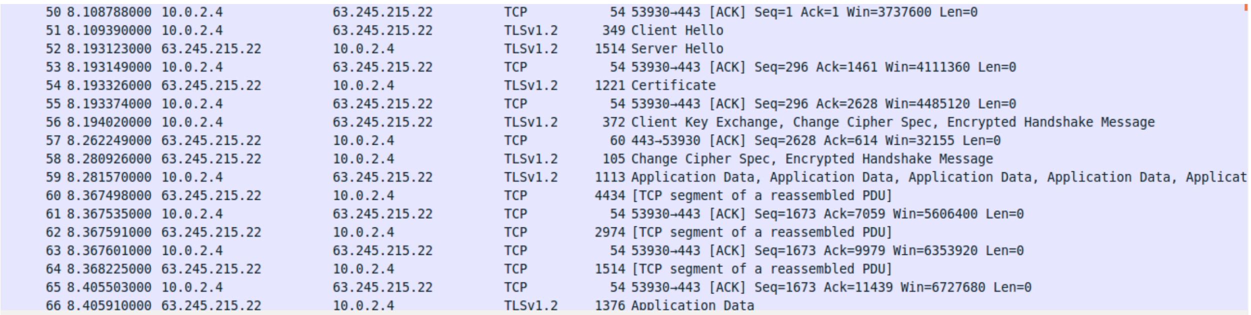
```
    11 7.573285000 10.0.2.5         8.8.8.8          DNS      77 Standard query 0xda66  AAAA start.mozilla.org
    12 7.573306000 10.0.2.5         8.8.8.8          DNS      77 Standard query 0xda66  AAAA start.mozilla.org
    13 7.718354000 8.8.8.8          10.0.2.5         DNS     249 Standard query response 0x80ea  CNAME start-origin-phx1.cdn.mozilla.net CNAME st
    14 7.718376000 8.8.8.8          10.0.2.5         DNS     249 Standard query response 0x80ea  CNAME start-origin-phx1.cdn.mozilla.net CNAME st
    15 7.719047000 10.0.2.5         8.8.8.8          DNS      84 Standard query 0x8dfe  A en-us.start3.mozilla.com
    16 7.719074000 10.0.2.5         8.8.8.8          DNS      84 Standard query 0x8dfe  A en-us.start3.mozilla.com
    17 7.726042000 8.8.8.8          10.0.2.5         DNS     195 Standard query response 0xda66  CNAME startpage-zlb.vips.scl3.mozilla.com
    18 7.726062000 8.8.8.8          10.0.2.5         DNS     195 Standard query response 0xda66  CNAME startpage-zlb.vips.scl3.mozilla.com
    19 7.726838000 10.0.2.5         8.8.8.8          DNS      77 Standard query 0xefaa  A start.mozilla.org
    20 7.726866000 10.0.2.5         8.8.8.8          DNS      77 Standard query 0xefaa  A start.mozilla.org
    21 7.799853000 8.8.8.8          10.0.2.5         DNS     142 Standard query response 0xefaa  CNAME startpage-zlb.vips.scl3.mozilla.com A 63.2
    22 7.799868000 8.8.8.8          10.0.2.5         DNS     142 Standard query response 0xefaa  CNAME startpage-zlb.vips.scl3.mozilla.com A 63.2
    23 7.800307000 10.0.2.5         63.245.215.22    TCP      74 41385→80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=1055827 TSecr=0 W
    24 7.800338000 63.245.215.22    10.0.2.5         TCP      74 80→41385 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=30452
    25 7.800589000 10.0.2.5         63.245.215.22    TCP      66 41385→80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=1055827 TSecr=3045286
    26 7.800630000 10.0.2.5         63.245.215.22    HTTP    866 GET /en-US/ HTTP/1.1
    27 7.800638000 63.245.215.22    10.0.2.5         TCP      66 80→41385 [ACK] Seq=1 Ack=801 Win=30592 Len=0 TSval=3045286 TSecr=1055827
```



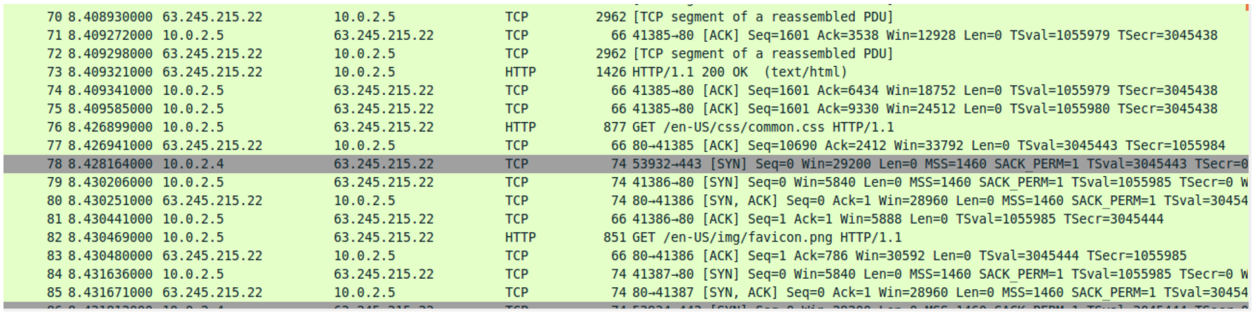
```
    23 7.800307000 10.0.2.5         63.245.215.22    TCP      74 41385→80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=1055827 TSecr=0 W
    24 7.800338000 63.245.215.22    10.0.2.5         TCP      74 80→41385 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=30452
    25 7.800589000 10.0.2.5         63.245.215.22    TCP      66 41385→80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=1055827 TSecr=3045286
    26 7.800630000 10.0.2.5         63.245.215.22    HTTP    866 GET /en-US/ HTTP/1.1
    27 7.800638000 63.245.215.22    10.0.2.5         TCP      66 80→41385 [ACK] Seq=1 Ack=801 Win=30592 Len=0 TSval=3045286 TSecr=1055827
    28 7.801542000 8.8.8.8          10.0.2.5         DNS     185 Standard query response 0x8dfe  CNAME start-origin-phx1.cdn.mozilla.net CNAME st
    29 7.801558000 8.8.8.8          10.0.2.5         DNS     185 Standard query response 0x8dfe  CNAME start-origin-phx1.cdn.mozilla.net CNAME st
    30 7.801835000 10.0.2.4         8.8.8.8          DNS      77 Standard query 0x70ff  A start.mozilla.org
    31 7.849242000 8.8.8.8          10.0.2.4         DNS     142 Standard query response 0x70ff  CNAME startpage-zlb.vips.scl3.mozilla.com A 63.2
    32 7.850144000 10.0.2.4         63.245.215.22    TCP      74 34664→80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3045299 TSecr=0
    33 7.934127000 63.245.215.22    10.0.2.4         TCP      60 80→34664 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
    34 7.934169000 10.0.2.4         63.245.215.22    TCP      54 34664→80 [ACK] Seq=1 Ack=1 Win=3737600 Len=0
    35 7.935357000 10.0.2.4         63.245.215.22    HTTP    823 GET /en-US/ HTTP/1.0
    36 8.003309000 CadmusCo_bf:e5:aa CadmusCo_ac:7d:7b ARP    42 10.0.2.1 is at 08:00:27:bf:e5:aa
    37 8.009262000 63.245.215.22    10.0.2.4         TCP      60 80→34664 [ACK] Seq=1 Ack=770 Win=31999 Len=0
    38 8.020016000 63.245.215.22    10.0.2.4         HTTP    697 HTTP/1.1 301 Moved Permanently  (text/html)
    39 8.020046000 10.0.2.4         63.245.215.22    TCP      54 34664→80 [ACK] Seq=770 Ack=644 Win=3868288 Len=0
```



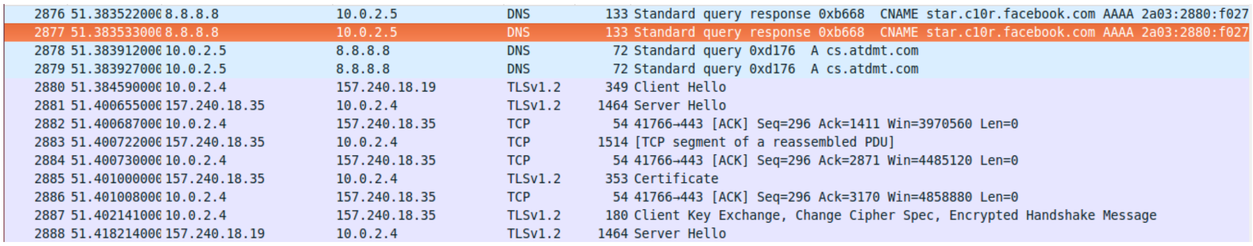
```
33 7.934127000 63.245.215.22      10.0.2.4           TCP        60 80→34664 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
34 7.934169000 10.0.2.4           63.245.215.22      TCP        54 34664→80 [ACK] Seq=1 Ack=1 Win=3737600 Len=0
35 7.935357000 10.0.2.4           63.245.215.22      HTTP      823 GET /en-US/ HTTP/1.0
36 8.003309000 CadmusCo_bf:e5:aa  CadmusCo_ac:7d:7b  ARP        42 10.0.2.1 is at 08:00:27:bf:e5:aa
37 8.009262000 63.245.215.22      10.0.2.4           TCP        60 80→34664 [ACK] Seq=1 Ack=770 Win=31999 Len=0
38 8.020016000 63.245.215.22      10.0.2.4           HTTP      697 HTTP/1.1 301 Moved Permanently  (text/html)
39 8.020046000 10.0.2.4           63.245.215.22      TCP        54 34664→80 [ACK] Seq=770 Ack=644 Win=3868288 Len=0
40 8.021681000 63.245.215.22      10.0.2.5           HTTP      707 HTTP/1.1 301 Moved Permanently  (text/html)
41 8.021991000 10.0.2.4           63.245.215.22      TCP        54 34664→80 [FIN, ACK] Seq=770 Ack=644 Win=3868288 Len=0
42 8.022134000 10.0.2.5           63.245.215.22      TCP        66 41385→80 [ACK] Seq=801 Ack=642 Win=7168 Len=0 TSval=1055883 TSecr=3045342
43 8.022417000 63.245.215.22      10.0.2.4           TCP        60 80→34664 [ACK] Seq=644 Ack=771 Win=31998 Len=0
44 8.023856000 10.0.2.5           63.245.215.22      HTTP      866 GET /en-US/ HTTP/1.1
45 8.023889000 63.245.215.22      10.0.2.5           TCP        66 80→41385 [ACK] Seq=642 Ack=1601 Win=32256 Len=0 TSval=3045342 TSecr=1055883
46 8.025346000 10.0.2.4           63.245.215.22      TCP        74 53930→443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3045342 TSecr=0
47 8.104484000 63.245.215.22      10.0.2.4           TCP        60 80→34664 [FIN, ACK] Seq=644 Ack=771 Win=31998 Len=0
48 8.104522000 10.0.2.4           63.245.215.22      TCP        54 34664→80 [ACK] Seq=771 Ack=645 Win=3868288 Len=0
49 8.108760000 63.245.215.22      10.0.2.4           TCP        60 443→53930 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
```



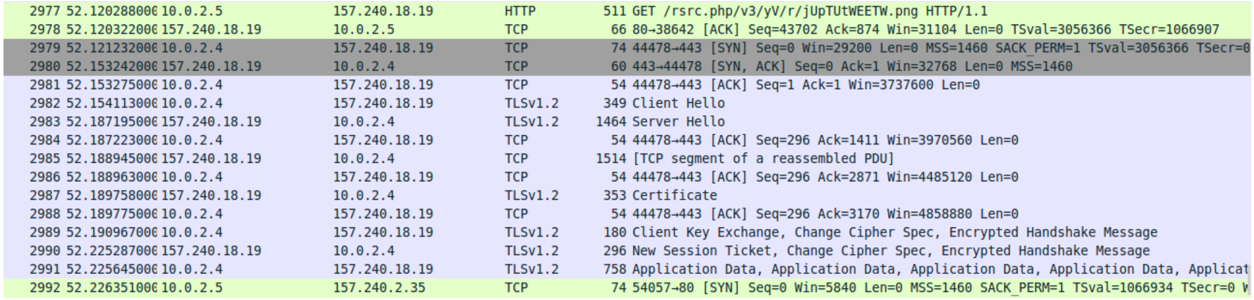
```
50 8.108788000 10.0.2.4           63.245.215.22      TCP        54 53930→443 [ACK] Seq=1 Ack=1 Win=3737600 Len=0
51 8.109390000 10.0.2.4           63.245.215.22      TLSv1.2   349 Client Hello
52 8.193123000 63.245.215.22      10.0.2.4           TLSv1.2  1514 Server Hello
53 8.193149000 10.0.2.4           63.245.215.22      TCP        54 53930→443 [ACK] Seq=296 Ack=1461 Win=4111360 Len=0
54 8.193326000 63.245.215.22      10.0.2.4           TLSv1.2  1221 Certificate
55 8.193374000 10.0.2.4           63.245.215.22      TCP        54 53930→443 [ACK] Seq=296 Ack=2628 Win=4485120 Len=0
56 8.194020000 10.0.2.4           63.245.215.22      TLSv1.2   372 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
57 8.262249000 63.245.215.22      10.0.2.4           TCP        60 443→53930 [ACK] Seq=2628 Ack=614 Win=32155 Len=0
58 8.280926000 63.245.215.22      10.0.2.4           TLSv1.2   105 Change Cipher Spec, Encrypted Handshake Message
59 8.281570000 10.0.2.4           63.245.215.22      TLSv1.2  1113 Application Data, Application Data, Application Data, Application Data, Applicat
60 8.367498000 63.245.215.22      10.0.2.4           TCP      4434 [TCP segment of a reassembled PDU]
61 8.367535000 10.0.2.4           63.245.215.22      TCP        54 53930→443 [ACK] Seq=1673 Ack=7059 Win=5606400 Len=0
62 8.367591000 63.245.215.22      10.0.2.4           TCP      2974 [TCP segment of a reassembled PDU]
63 8.367601000 10.0.2.4           63.245.215.22      TCP        54 53930→443 [ACK] Seq=1673 Ack=9979 Win=6353920 Len=0
64 8.368225000 63.245.215.22      10.0.2.4           TCP      1514 [TCP segment of a reassembled PDU]
65 8.405503000 10.0.2.4           63.245.215.22      TCP        54 53930→443 [ACK] Seq=1673 Ack=11439 Win=6727680 Len=0
66 8.405910000 63.245.215.22      10.0.2.4           TLSv1.2  1376 Application Data
```



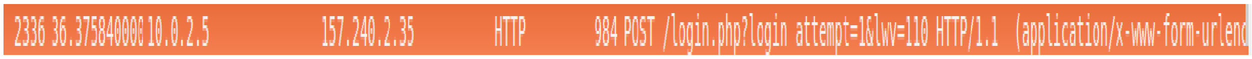
```
70 8.408930000 63.245.215.22      10.0.2.5           TCP      2962 [TCP segment of a reassembled PDU]
71 8.409272000 10.0.2.5           63.245.215.22      TCP        66 41385→80 [ACK] Seq=1601 Ack=3538 Win=12928 Len=0 TSval=1055979 TSecr=3045438
72 8.409298000 63.245.215.22      10.0.2.5           TCP      2962 [TCP segment of a reassembled PDU]
73 8.409321000 63.245.215.22      10.0.2.5           HTTP     1426 HTTP/1.1 200 OK  (text/html)
74 8.409341000 10.0.2.5           63.245.215.22      TCP        66 41385→80 [ACK] Seq=1601 Ack=6434 Win=18752 Len=0 TSval=1055979 TSecr=3045438
75 8.409585000 10.0.2.5           63.245.215.22      TCP        66 41385→80 [ACK] Seq=1601 Ack=9330 Win=24512 Len=0 TSval=1055980 TSecr=3045438
76 8.426899000 10.0.2.5           63.245.215.22      HTTP      877 GET /en-US/css/common.css HTTP/1.1
77 8.426941000 63.245.215.22      10.0.2.5           TCP        66 80→41385 [ACK] Seq=10690 Ack=2412 Win=33792 Len=0 TSval=3045443 TSecr=1055984
78 8.428164000 10.0.2.4           63.245.215.22      TCP        74 53932→443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3045443 TSecr=0
79 8.430206000 10.0.2.5           63.245.215.22      TCP        74 41386→80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=1055985 TSecr=0 W
80 8.430251000 63.245.215.22      10.0.2.5           TCP        74 80→41386 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=30454
81 8.430441000 10.0.2.5           63.245.215.22      TCP        66 41386→80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=1055985 TSecr=3045444
82 8.430469000 10.0.2.5           63.245.215.22      HTTP      851 GET /en-US/img/favicon.png HTTP/1.1
83 8.430480000 63.245.215.22      10.0.2.5           TCP        66 80→41386 [ACK] Seq=1 Ack=786 Win=30592 Len=0 TSval=3045444 TSecr=1055985
84 8.431636000 10.0.2.5           63.245.215.22      TCP        74 41387→80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=1055985 TSecr=0 W
85 8.431671000 63.245.215.22      10.0.2.5           TCP        74 80→41387 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=30454
```



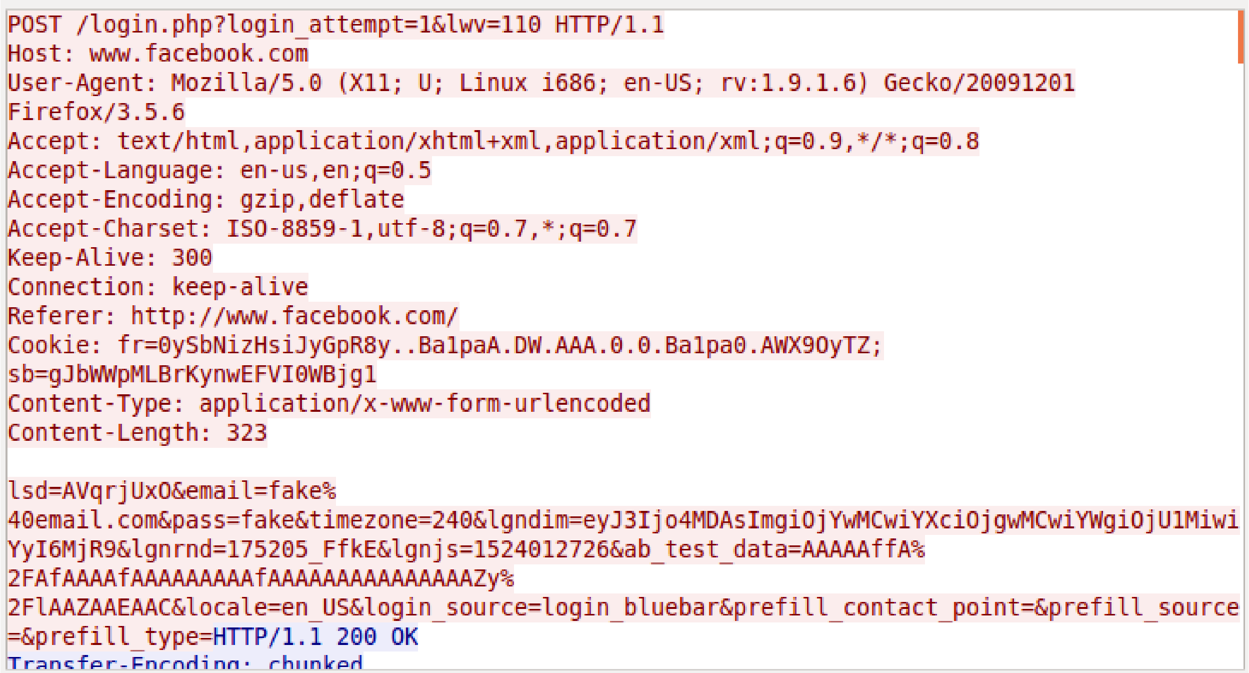
```
2876 51.38352200 8.8.8.8            10.0.2.5           DNS       133 Standard query response 0xb668  CNAME star.c10r.facebook.com AAAA 2a03:2880:f027
2877 51.38353300 8.8.8.8            10.0.2.5           DNS       133 Standard query response 0xb668  CNAME star.c10r.facebook.com AAAA 2a03:2880:f027
2878 51.38391200 10.0.2.5           8.8.8.8            DNS        72 Standard query 0xd176  A cs.atdmt.com
2879 51.38392700 10.0.2.5           8.8.8.8            DNS        72 Standard query 0xd176  A cs.atdmt.com
2880 51.38459000 10.0.2.4           157.240.18.19      TLSv1.2   349 Client Hello
2881 51.40065500 157.240.18.35      10.0.2.4           TLSv1.2  1464 Server Hello
2882 51.40068700 10.0.2.4           157.240.18.35      TCP        54 41766→443 [ACK] Seq=296 Ack=1411 Win=3970560 Len=0
2883 51.40072200 157.240.18.35      10.0.2.4           TCP      1514 [TCP segment of a reassembled PDU]
2884 51.40073000 10.0.2.4           157.240.18.35      TCP        54 41766→443 [ACK] Seq=296 Ack=2871 Win=4485120 Len=0
2885 51.40100000 157.240.18.35      10.0.2.4           TLSv1.2   353 Certificate
2886 51.40100800 10.0.2.4           157.240.18.35      TCP        54 41766→443 [ACK] Seq=296 Ack=3170 Win=4858880 Len=0
2887 51.40214100 10.0.2.4           157.240.18.35      TLSv1.2   180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2888 51.41821400 157.240.18.19      10.0.2.4           TLSv1.2  1464 Server Hello
```



```
2977 52.12028800( 10.0.2.5        157.240.18.19   HTTP      511 GET /rsrc.php/v3/yV/r/jUpTUtWEETW.png HTTP/1.1
2978 52.12032200( 157.240.18.19   10.0.2.5        TCP        66 80→38642 [ACK] Seq=43702 Ack=874 Win=31104 Len=0 TSval=3056366 TSecr=1066907
2979 52.12123200( 10.0.2.4        157.240.18.19   TCP        74 44478→443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3056366 TSecr=0
2980 52.15324200( 157.240.18.19   10.0.2.4        TCP        60 443→44478 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
2981 52.15327500( 10.0.2.4        157.240.18.19   TCP        54 44478→443 [ACK] Seq=1 Ack=1 Win=3737600 Len=0
2982 52.15411300( 10.0.2.4        157.240.18.19   TLSv1.2   349 Client Hello
2983 52.18719500( 157.240.18.19   10.0.2.4        TLSv1.2  1464 Server Hello
2984 52.18722300( 10.0.2.4        157.240.18.19   TCP        54 44478→443 [ACK] Seq=296 Ack=1411 Win=3970560 Len=0
2985 52.18894500( 157.240.18.19   10.0.2.4        TCP      1514 [TCP segment of a reassembled PDU]
2986 52.18896300( 10.0.2.4        157.240.18.19   TCP        54 44478→443 [ACK] Seq=296 Ack=2871 Win=4485120 Len=0
2987 52.18975800( 157.240.18.19   10.0.2.4        TLSv1.2   353 Certificate
2988 52.18977500( 10.0.2.4        157.240.18.19   TCP        54 44478→443 [ACK] Seq=296 Ack=3170 Win=4858880 Len=0
2989 52.19096700( 10.0.2.4        157.240.18.19   TLSv1.2   180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2990 52.22528700( 157.240.18.19   10.0.2.4        TLSv1.2   296 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
2991 52.22564500( 10.0.2.4        157.240.18.19   TLSv1.2   758 Application Data, Application Data, Application Data, Application Data, Applicat
2992 52.22635100( 10.0.2.5        157.240.2.35    TCP        74 54057→80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=1066934 TSecr=0 W
```

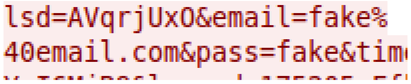


```
2336 36.37584000( 10.0.2.5        157.240.2.35    HTTP      984 POST /login.php?login attempt=1&lwv=110 HTTP/1.1  (application/x-www-form-urlenc
```



```
POST /login.php?login_attempt=1&lwv=110 HTTP/1.1
Host: www.facebook.com
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.1.6) Gecko/20091201
Firefox/3.5.6
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.facebook.com/
Cookie: fr=0ySbNizHsiJyGpR8y..Ba1paA.DW.AAA.0.0.Ba1pa0.AWX9OyTZ;
sb=gJbWWpMLBrKynwEFVI0WBjg1
Content-Type: application/x-www-form-urlencoded
Content-Length: 323

lsd=AVqrjUxO&email=fake%
40email.com&pass=fake&timezone=240&lgndim=eyJ3Ijo4MDAsImgiOjYwMCwiYXciOjgwMCwiYWgiOjU1Miwi
YyI6MjR9&lgnrnd=175205_FfkE&lgnjs=1524012726&ab_test_data=AAAAAffA%
2FAfAAAAfAAAAAAAAAAfAAAAAAAAAAAAAAAZy%
2FlAAZAAEAAC&locale=en_US&login_source=login_bluebar&prefill_contact_point=&prefill_source
=&prefill_type=HTTP/1.1 200 OK
Transfer-Encoding: chunked
```

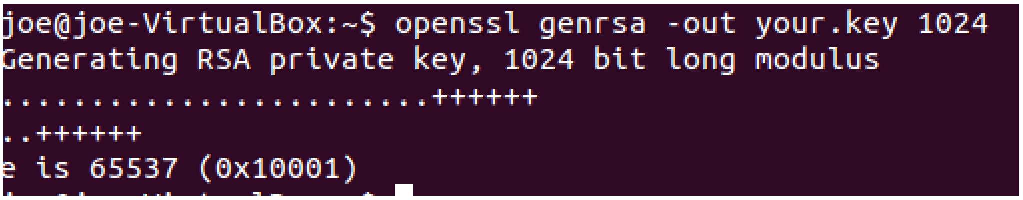


```
lsd=AVqrjUxO&email=fake%
40email.com&pass=fake&tim
```

It can clearly be seen from the screen shots above that by inspecting a HTTP packet, the email and password for the facebook login can be determined. In this situation the email used was fake@email.com and the password was fake, which can both be seen in the screenshots above.

4.3 (2%) Replacing SSL certificates using sslsniff

(1) Create your private key:

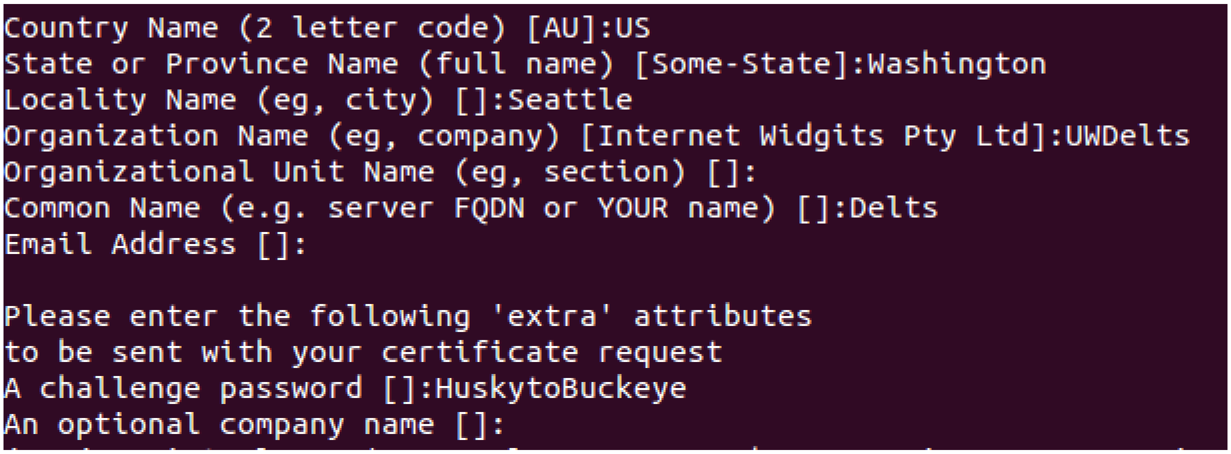


```
joe@joe-VirtualBox:~$ openssl genrsa -out your.key 1024
Generating RSA private key, 1024 bit long modulus
.........................++++++
..++++++
e is 65537 (0x10001)
```

(2) Create a CSR:

You will be prompt to create a certificate that you will use to fool the user. This is your opportunity to be creative:

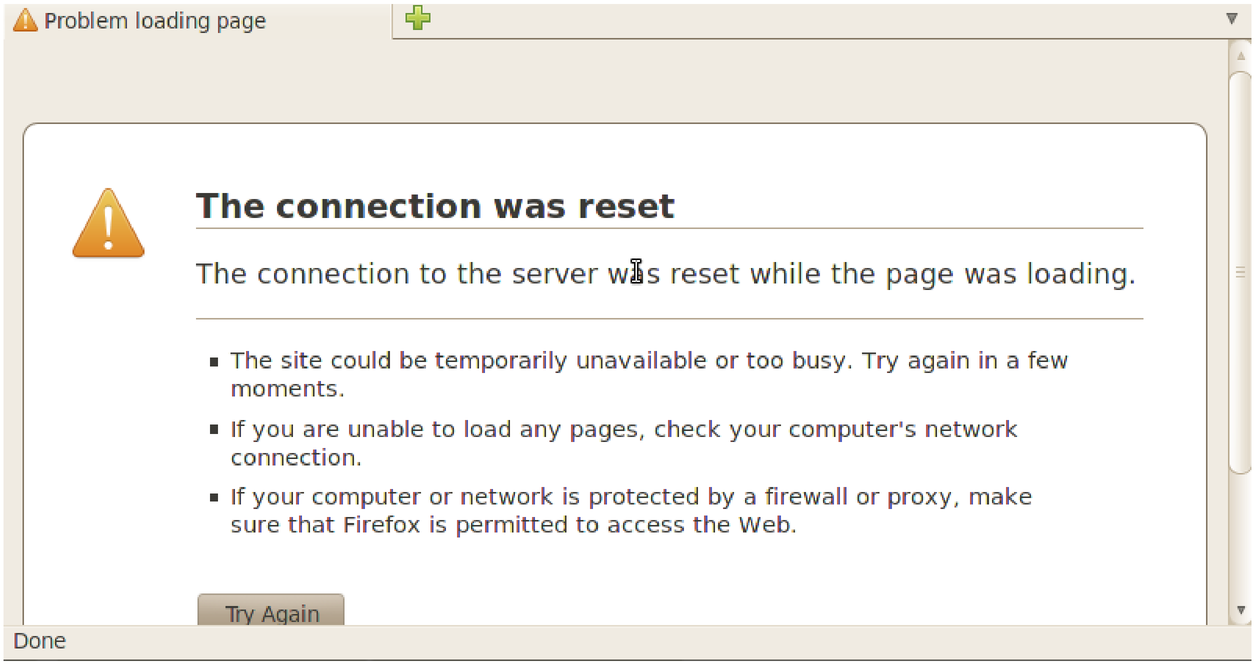
(3) Create your self-signed certificate:



```
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Washington
Locality Name (eg, city) []:Seattle
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UWDelts
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:Delts
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:HuskytoBuckeye
An optional company name []:
```

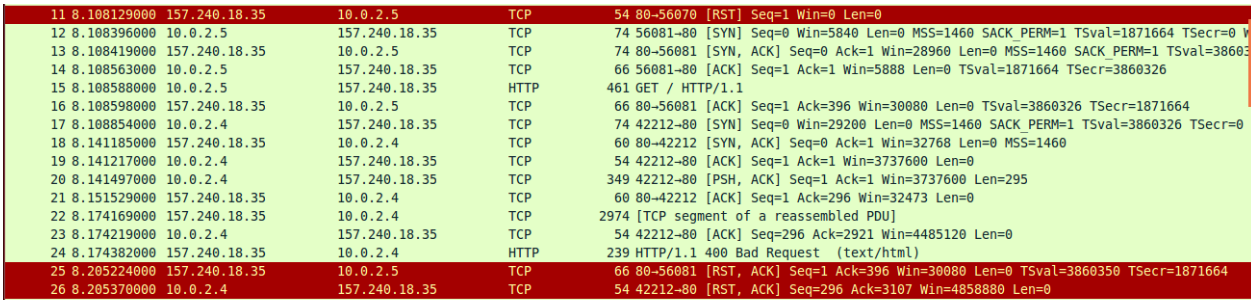
Step 7: In Victim VM, open the browser (firefox 3.5.6) and visit https://www.facebook.com. If the attack is successful, the browser will inform you that the certificate CA is not trusted.



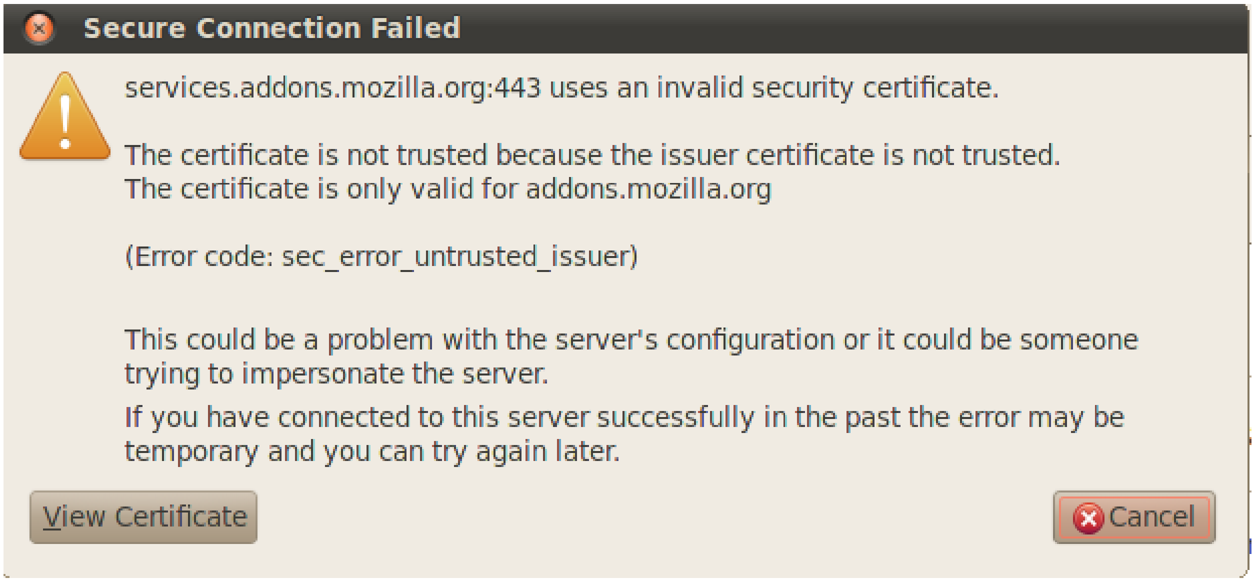
The connection was reset

The connection to the server was reset while the page was loading.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.



```
     11 8.108129000 157.240.18.35        10.0.2.5             TCP        54 80→56070 [RST] Seq=1 Win=0 Len=0
     12 8.108396000 10.0.2.5             157.240.18.35        TCP        74 56081→80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=1871664 TSecr=0 W
     13 8.108419000 157.240.18.35        10.0.2.5             TCP        74 80→56081 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=38603
     14 8.108563000 10.0.2.5             157.240.18.35        TCP        66 56081→80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=1871664 TSecr=3860326
     15 8.108588000 10.0.2.5             157.240.18.35        HTTP      461 GET / HTTP/1.1
     16 8.108598000 157.240.18.35        10.0.2.5             TCP        66 80→56081 [ACK] Seq=1 Ack=396 Win=30080 Len=0 TSval=3860326 TSecr=1871664
     17 8.108854000 10.0.2.4             157.240.18.35        TCP        74 42212→80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3860326 TSecr=0
     18 8.141185000 157.240.18.35        10.0.2.4             TCP        60 80→42212 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
     19 8.141217000 10.0.2.4             157.240.18.35        TCP        54 42212→80 [ACK] Seq=1 Ack=1 Win=3737600 Len=0
     20 8.141497000 10.0.2.4             157.240.18.35        TCP       349 42212→80 [PSH, ACK] Seq=1 Ack=1 Win=3737600 Len=295
     21 8.151529000 157.240.18.35        10.0.2.4             TCP        60 80→42212 [ACK] Seq=1 Ack=296 Win=32473 Len=0
     22 8.174169000 157.240.18.35        10.0.2.4             TCP      2974 [TCP segment of a reassembled PDU]
     23 8.174219000 10.0.2.4             157.240.18.35        TCP        54 42212→80 [ACK] Seq=296 Ack=2921 Win=4485120 Len=0
     24 8.174382000 157.240.18.35        10.0.2.4             HTTP      239 HTTP/1.1 400 Bad Request  (text/html)
     25 8.205224000 157.240.18.35        10.0.2.5             TCP        66 80→56081 [RST, ACK] Seq=1 Ack=396 Win=30080 Len=0 TSval=3860350 TSecr=1871664
     26 8.205370000 10.0.2.4             157.240.18.35        TCP        54 42212→80 [RST, ACK] Seq=296 Ack=3107 Win=4858880 Len=0
```



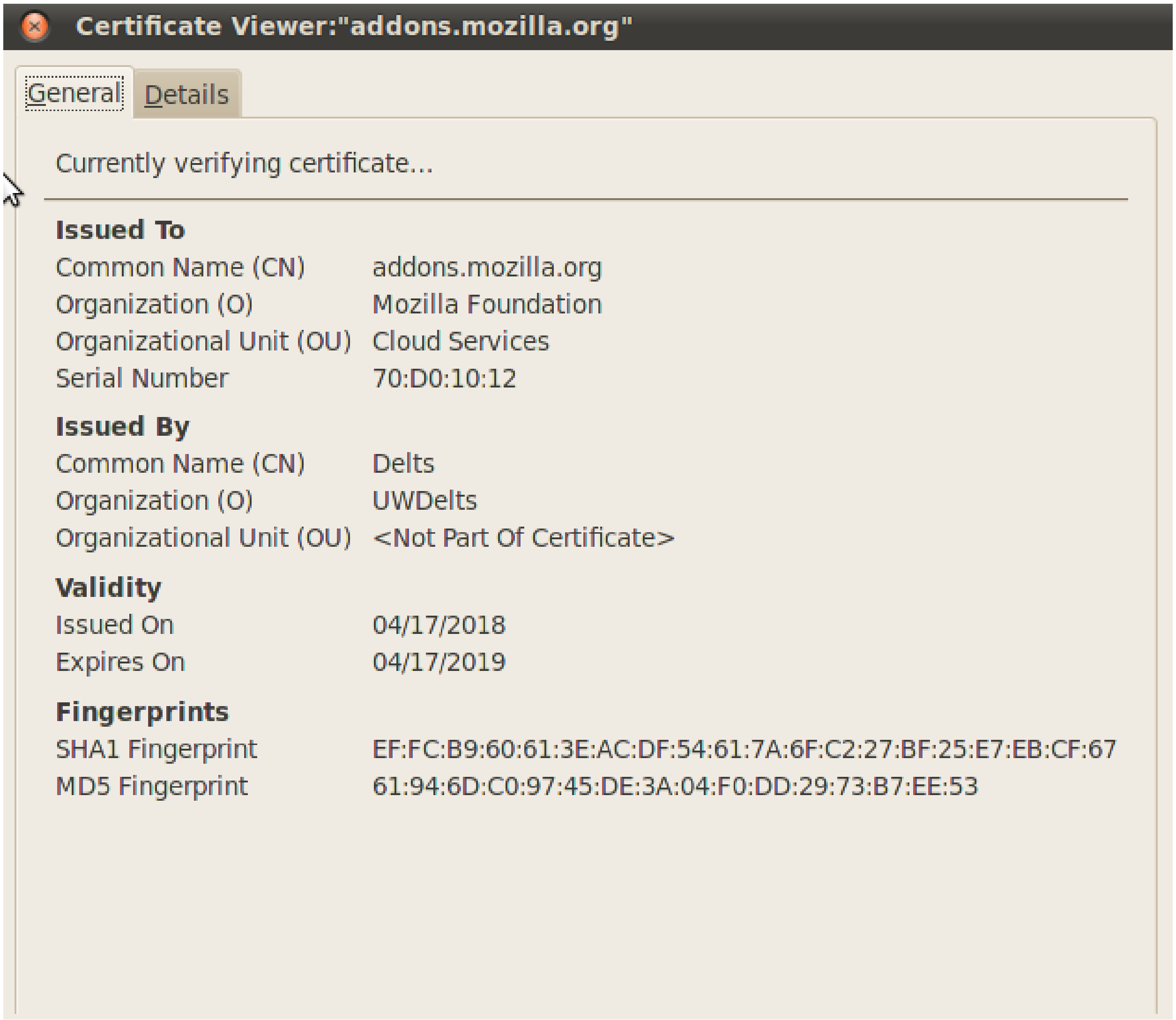
services.addons.mozilla.org:443 uses an invalid security certificate.

The certificate is not trusted because the issuer certificate is not trusted.
The certificate is only valid for addons.mozilla.org

(Error code: sec_error_untrusted_issuer)

This could be a problem with the server's configuration or it could be someone trying to impersonate the server.

If you have connected to this server successfully in the past the error may be temporary and you can try again later.



Certificate Viewer:"addons.mozilla.org"

Currently verifying certificate...

Issued To

Common Name (CN)	addons.mozilla.org
Organization (O)	Mozilla Foundation
Organizational Unit (OU)	Cloud Services
Serial Number	70:D0:10:12

Issued By

Common Name (CN)	Delts
Organization (O)	UWDelts
Organizational Unit (OU)	<Not Part Of Certificate>

Validity

Issued On	04/17/2018
Expires On	04/17/2019

Fingerprints

SHA1 Fingerprint	EF:FC:B9:60:61:3E:AC:DF:54:61:7A:6F:C2:27:BF:25:E7:EB:CF:67
MD5 Fingerprint	61:94:6D:C0:97:45:DE:3A:04:F0:DD:29:73:B7:EE:53

The screen shots show that the browser says that certificate is not trusted and the details of the certificate are what I created.