

Secure Communications

Week 11

Tunnelling and Web Security (Part 2)

Sections

C. OpenSSL

C.1 `openssl s_client -connect www.live.com:443`

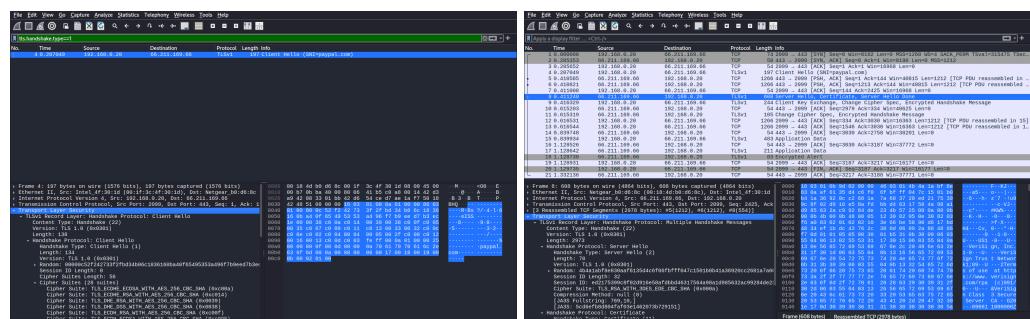
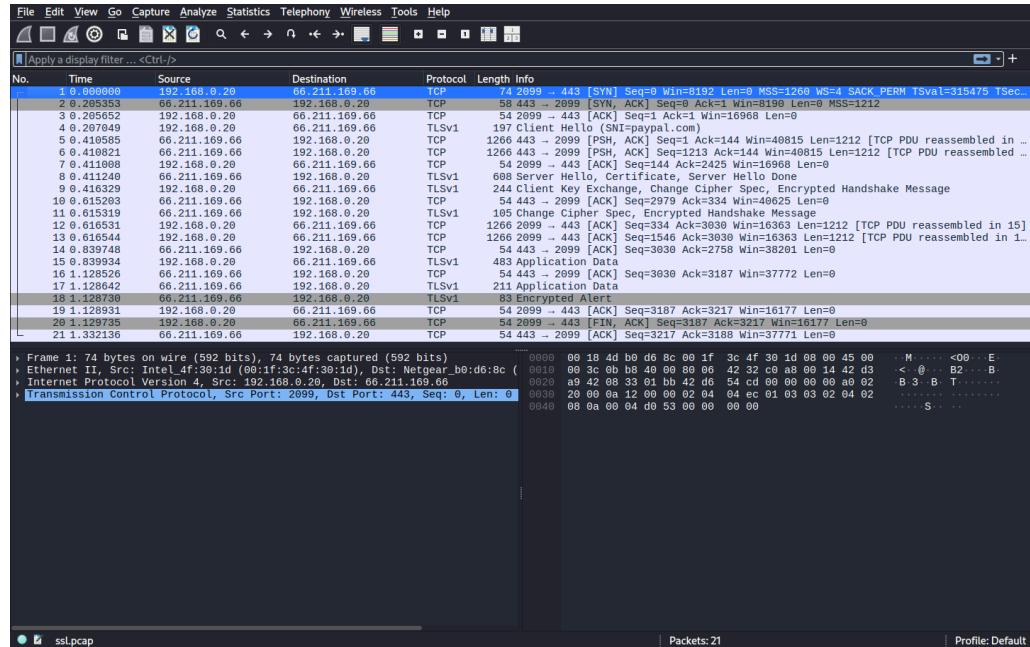


Which SSL/TLS method has been used:	TLSv1.3
Which method is used on the encryption key on the certificate, and what is the size of the public key?	RSA, 2048-bit
Which is the handshaking method that has been used to create the encryption key?	ECDH (secp521r1), 521 bits
Which TLS version is used for the tunnel?	TLSv1.3
Which symmetric encryption method is used for the tunnel:	AES-256-GCM (TLS_AES_256_GCM_SHA384)
Which hashing method is used for the tunnel:	SHA-384 (TLS_AES_256_GCM_SHA384)
What is the length of the symmetric encryption key:	256-bit
Who has signed the certificate:	DigiCert Cloud Services CA-1

D. Examining traces

B.1 <http://asecuritysite.com/log/ssl.zip>

Download the following file, and examine the trace with Wireshark



Client IP address and TCP port:	IP: 192.168.0.20 Port: 2099
Web server IP address and TCP port:	IP: 66.211.169.66 Port: 443
Determine one of the symmetric key encryption methods, the key exchange, and the hashing methods that the client wants to use (Hint: look at the 'Client Hello' packet)"	AES_256_CBC SHA Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
Which SSL/TLS method has been used:	TLS 1.0
Which encryption method is used for the tunnel:	3DES_EDE_CBC Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
Which hashing method is used for the tunnel:	SHA Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x000a)

What is the length of the encryption key:

168-bit

B.2 <http://asecuritysite.com/log/https.zip>

Download the following file, and examine the trace with Wireshark

The Wireshark interface displays two traces. The top trace shows the initial SSL/TLS handshake (Frames 1-21), which includes the Client Hello, Server Hello, and Certificate exchange messages. The bottom trace shows the subsequent session (Frames 28-39), where the client sends an encrypted message (Frame 39) and the server responds with an encrypted message (Frame 38). The frames are color-coded by protocol type, with TCP frames in blue and SSL/TLS frames in green.

Client IP address and TCP port:	IP: 172.16.121.155 Port: 3923
Web server IP address and TCP port:	IP: 87.106.189.123 Port: 443
Which SSL/TLS method has been used:	TLS 1.2
Which encryption method is used for the tunnel:	AES_256_CBC Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
Which hashing method is used for the tunnel:	SHA Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
What is the length of the encryption key:	256-bit

B.3 <http://asecuritysite.com/log/heart.zip>

Download the following file, and examine the trace with Wireshark

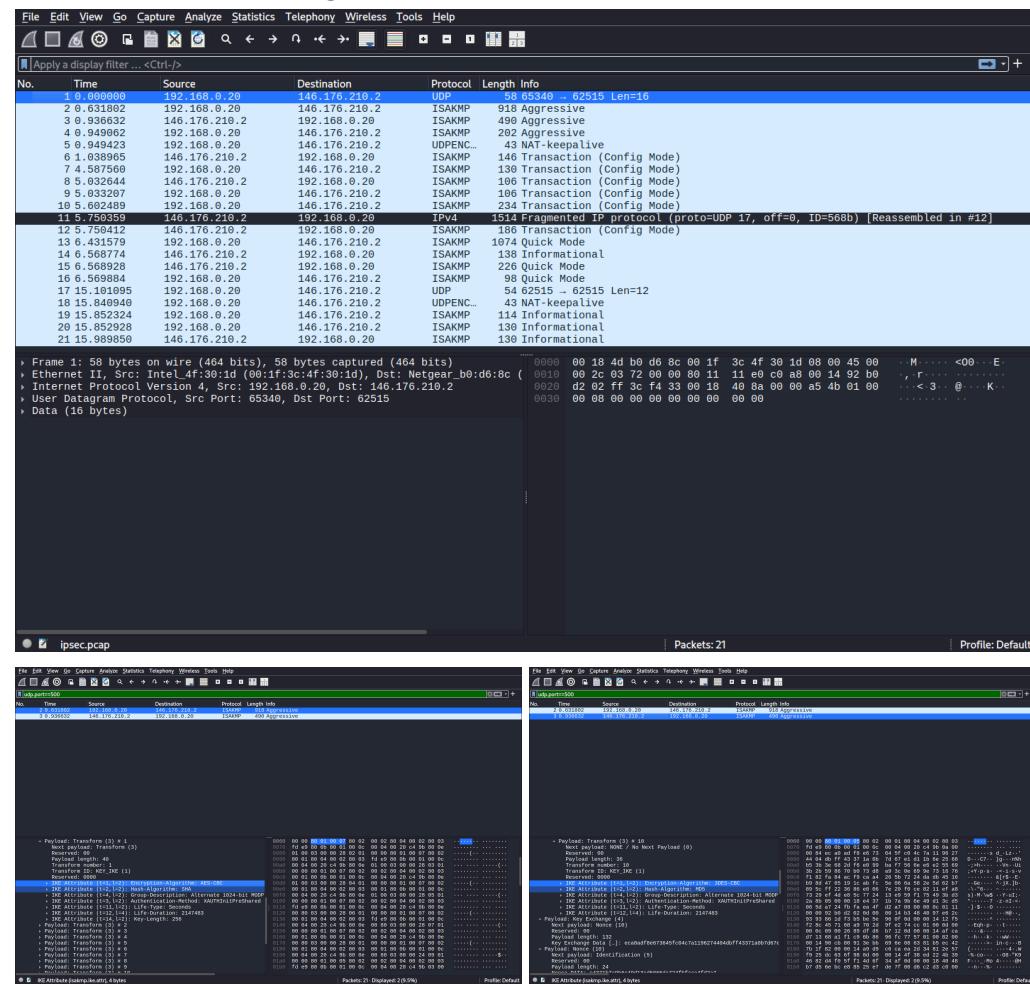
The figure consists of three vertically stacked screenshots of the Wireshark application interface. Each screenshot shows a list of network frames with detailed information about their source, destination, protocol, length, and content.

- Screenshot 1:** Shows a list of frames from a PCAP file named "heart.pcap". The frames include various protocols like NBNS, TCP, TLSv1.2, and DNS. A specific frame (Frame 1) is highlighted, showing its details: Source 172.16.121.129, Destination 172.16.121.2, Protocol NBNS, Length 110, and Info: "110 Refresh NB WIN-98UTFAN855G<20>". Below the frame list, a detailed hex dump and ASCII dump are provided for Frame 1.
- Screenshot 2:** Shows a list of frames from the same "heart.pcap" file. It highlights a different frame (Frame 2) which is a TCP segment. The details show Source 172.16.121.2, Destination 172.16.121.150, Protocol TCP, Length 443, and Info: "443 [ACK] Seq=1 Ack=1 Win=64240 Len=0". Below the frame list, a detailed hex dump and ASCII dump are provided for Frame 2.
- Screenshot 3:** Shows a list of frames from the same "heart.pcap" file. It highlights a different frame (Frame 3) which is a TCP segment. The details show Source 172.16.121.150, Destination 172.16.121.2, Protocol TCP, Length 443, and Info: "443 [ACK] Seq=1 Ack=2 Win=64240 Len=0". Below the frame list, a detailed hex dump and ASCII dump are provided for Frame 3.

Client IP address and TCP port:	IP: 172.16.121.1 Port: 64666
Web server IP address and TCP port:	IP: 172.16.121.150 Port: 443
Which SSL/TLS method has been used:	TLS 1.2
Which encryption method is used for the tunnel:	AES_256_GCM
Which hashing method is used for the tunnel:	SHA384
What is the length of the encryption key:	256-bit

B.4 <http://asecuritysite.com/log/ipsec.zip>

Download the following file, and examine the trace with Wireshark



Which is the IP address of the client and of the server:

Client: 192.168.0.20
Server: 146.176.210.2

Which packet number identifies the start of the VPN connection (Hint: look for UDP Port 500):

2

Determine one of the encryption and the hashing methods that the client wants to use:

AES-CBC
SHA

Now determine the encryption and hashing methods that are agreed in the ISAKMP:

3DES-CBC
MD5

B.5 <http://asecuritysite.com/log/tor.zip>

Download the following file, and examine the trace with Wireshark

The top Wireshark window displays a list of 4901 captured packets. The bottom window shows two panes of packet details for the same file. The left pane shows the initial TLS handshake, and the right pane shows the continuation of the session.

Which TCP port does the client use to send to?	9001
What is the IP address of the Tor node that the client connects to?	IP: 172.16.121.169 Port: 1113
What is strange about the packet size?	Tor traffic often uses fixed-size “cells” (512 bytes) – strange to see identical-length packets.
Is SSL/TLS used for the connection?	No, tor is not using TLS for that hop. I wasn't be able to find any tls handshakes (but found some packets)
Can you trace any content in the conversation?	Because Tor encrypts its application data heavily, you typically cannot read the content of the conversation in Wireshark.
Can you determine the Web site that is being connected to?	No, because the Tor node decrypts data at exit and then sends the request to the destination – the original site name is not visible in the TLS handshake.

Lab 5: Tunnelling and Web Security

Objective: In this lab we will investigate the usage of SSL/TLS and VPN tunnels.

[YouTube Demo: https://youtu.be/ASCDJq4Wy9Y](https://youtu.be/ASCDJq4Wy9Y)

A Web cryptography assessment

The SSLabs tool (<https://ssllabs.com>) can be used to assess the security of the cryptography used on a Web site. Pick three of your favourite sites to scan. Now perform a test on them, and determine:

Site	Site 1:	Site 2:	Site 3:
What grade does the site get?	B rating	B rating	A rating
The digital certificate key size and type?	EC 256 bits SHA256withECDSA	RSA 2048 bits SHA256withRSA	RSA 2048 bits SHA256withRSA
Does the name of the site match the name on the server?	Yes	Yes	Yes
Who is the signer of the digital certificate?	W2	W3	AlphaCert Global S2 TLS RSA SHA256 2028 CA1
The expiry date on the digital certificate?	Sat, 19 Jan 2026 09:33:58 UTC	Sat, 24 Jan 2026 18:44:47 UTC	Fri, 24 Jul 2026 23:59:58 UTC
What is the hashing method on the certificate?	SHA256withECDSA	SHA256withRSA	SHA256withRSA
If it uses RSA keys, what is the e value that is used in the encryption (M ^e mod N)?	65537	65537	65537
Determine a weak cipher suite used and example why it might be weak?	Protocol Support: TLS 1.0 and TLS 1.1	Protocol Support: TLS 1.0 and TLS 1.1	All good
Is SSL v2 supported?	No	No	No
If SSL v2 was supported, what problems might there be with the site (this will require some research)?			
Outline the usage of TLS 1.0/1.1 and 1.2, and identify a problem if one of these TLS versions were not supported?	Supports: TLS 1.0 and TLS 1.1 Older devices or software may fail to connect	Supports: TLS 1.0 and TLS 1.1 Older devices or software may fail to connect	Not supported: TLS 1.0 and TLS 1.1
Is the site vulnerable to Heartbleed? Is the site vulnerable to DROWN? Is the site vulnerable to BEAST? Is the site vulnerable to POODLE?	No Not mitigated server-side No	No Not mitigated server-side No	No Not mitigated server-side No

1

Research questions:

What does TLS_ECDHE_RSA_WITH_AES_256_CCM_SHA384 identify?

It is the cipher suite used in a TLS connection.
- Key exchange: ECDHE (Elliptic-Curve Diffie-Hellman Ephemeral)
- Encryption: AES-256 in CCM mode
- Hashing / HMAC: SHA-384

If a site gets a 'T' grade, what is the problem? It assigns it a 'T' grade (for "trust").

If the site was susceptible to Poodle, what is the vulnerability?

PooleD is an attack on SSL 3.0's padding (and occasionally TLS padding).
- An attacker can decrypt cookies or session data by exploiting CBC padding.

Can you find a site which gets an "A-"? What features does a site need to get an "A+" grade?

I didn't find any "A+" grade website
To get an "A+" grade on SSLabs is to install a valid SSL certificate with CA bundle and configure HSTS in .htaccess.

A.2 We will now create a Python program which calls up the SSLabs assessment. First create a CSV file (sites.csv) with your sites in it. The format is Name of site, URL:

web,site
Cloudflare,www.cloudflare.com
BBC,bbc.co.uk

Next enter the following code and run it:

```
# Code from https://github.com/trrulli/ssllabs/blob/master/ssllabscanner.py
import requests
import time
import sys
import logging

API = 'https://api.ssllabs.com/api/v2/'

def requestAPI(path, payload={}):
    """
    This is a helper method that takes the path to the relevant
    API call, a user-defined payload and requests the
    data/server test from Qualys' SSL Labs.
    Returns JSON formatted data.
    """
    url = API + path

    try:
        response = requests.get(url, params=payload)
        except requests.exception.RequestException:
            logging.error('Request failed.')
            sys.exit(1)

        data = response.json()
        return data

def resultsFromCache(host, publish='off', startNew='off', fromCache='on',
all='done'):
    """
    Analyze
    payload = {
        'host': host,
        'publish': publish,
        'startNew': startNew,
        'all': all,
        'ignoreMismatch': ignoreMismatch
    }
    results = requestAPI(path, payload)
    payload.pop('startNew')
    while results['status'] != 'READY' and results['status'] != 'ERROR':
        time.sleep(30)
        results = requestAPI(path, payload)
    return results
```

2

```
'startNew': startNew,
'fromCache': fromCache,
'all': all
}
data = requestAPI(path, payload)
return data

def newScan(host, publish='off', startNew='on', all='done',
ignoreMismatch=False):
    path = 'analyze'
    payload = {
        'host': host,
        'publish': publish,
        'startNew': startNew,
        'all': all,
        'ignoreMismatch': ignoreMismatch
    }
    results = requestAPI(path, payload)
    payload.pop('startNew')
    while results['status'] != 'READY' and results['status'] != 'ERROR':
        time.sleep(30)
        results = requestAPI(path, payload)
    return results

import csv
with open('sites.csv') as csvfile:
    reader = csv.DictReader(csvfile)
    for row in reader:
        url = row['site'].strip()
        a = newScan(url)
        with open('out3.txt', 'a') as myfile:
            myfile.write(str(row['web'])+"\n"+str(a)+"\n\n")
```

Note that it will take a few minutes to perform a single scan. By reading the out3.txt file, outline your findings:

Site name: www.cloudflare.com	Site rating: grade: 'B'
Other significant details:	<pre>[{"name": "Cloudflare", "value": "Cloudflare is a Content Delivery Network (CDN) that provides fast delivery of static and dynamic content over a global network of data centers."}, {"name": "Protocol", "value": "Protocol: TLS 1.3"}, {"name": "Cipher Suite", "value": "Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CCM_SHA384 (6x1391)"}, {"name": "Key Exchange", "value": "Key Exchange: ECDHE (Elliptic-Curve Diffie-Hellman Ephemeral)"}, {"name": "Encryption", "value": "Encryption: AES-256 in CCM mode"}, {"name": "Hashing / HMAC", "value": "Hashing / HMAC: SHA-384"}]</pre>
Site name: bbc.co.uk	Site rating: grade: 'B'
Other significant details:	<pre>[{"name": "BBC", "value": "BBC is a British public service broadcaster that provides news, current affairs, entertainment, and educational programs in various formats."}, {"name": "Protocol", "value": "Protocol: TLS 1.3"}, {"name": "Cipher Suite", "value": "Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CCM_SHA384 (6x1391)"}, {"name": "Key Exchange", "value": "Key Exchange: ECDHE (Elliptic-Curve Diffie-Hellman Ephemeral)"}, {"name": "Encryption", "value": "Encryption: AES-256 in CCM mode"}, {"name": "Hashing / HMAC", "value": "Hashing / HMAC: SHA-384"}]</pre>

3

B Viewing details

No Description

B.1 On your VM instance (or your desktop), run Wireshark and capture traffic from your main network connection. Start a Web browser and go to Google.com.

Your IP address and TCP port:
IP: 192.168.2.15 | Port: 56724
Google's Web server IP address and TCP port:
IP: 89.89.232.34 | Port: 443

Which SSL/TLS version is used: **TLS 1.3**

By examining the Wireshark trace, which encryption method is used for the tunnel (hint: look in the 'Server Hello' response):
TLS_AES_256_GCM_SHA384 (8x1391)

By examining the Wireshark trace, which hashing method is used for the tunnel (hint: look in the 'Server Hello' response):
SHA-384

Using Firefox, and examining the connection details from the site (click on green padlock), can you verify the TLS version, the symmetric key encryption method, the handshaking method and the hashing method used within the tunnel? A sample is shown below. **Yes**

B.2 Run Wireshark and capture traffic from your main network connection. Start a Web browser and go to [https://twitter.com](http://twitter.com).

Your IP address and TCP port:
IP: 192.168.2.15 | Port: 68098

Twitter's Web server IP address and TCP port:
IP: 13.247.136.18 | Port: 443

Which SSL/TLS version is used: **TLS 1.3**

By examining the Wireshark trace, which encryption method is used for the tunnel:
TLS_AES_256_GCM_SHA384 (6x1391)

4

		<p>By examining the Wireshark trace, which hash method is used for the tunnel: TLS_AES_256_GCM_SHA384 (TLSv1.3)</p> <p>By examining the Wireshark trace, what is the length of the encryption key: 256</p> <p>Using Firefox, and examining the connection details from the site (click on green padlock), can you verify the TLS version, the symmetric key encryption method, the handshaking method and the hashing method used within the tunnel? no</p>
--	--	--

C OpenSSL

No	Description	Result
C.1	On your VM instance (or your desktop), make a connection to the www.live.com Web site: openssl s_client -connect www.live.com:443	<p>Which SSL/TLS method has been used: TLSv1.3</p> <p>Which method is used on the encryption key on the certificate, and what is the size of the public key?: RSA_2048</p> <p>Which is the handshaking method that has been used to create the encryption key?: ECDH (secp521r1), 521 bits</p> <p>Which TLS version is used for the tunnel?: TLSv1.3</p> <p>Which symmetric encryption method is used for the tunnel: AES_256_GCM</p> <p>Which hashing method is used for the tunnel: SHA-384</p> <p>What is the length of the symmetric encryption key: 256</p> <p>Who has signed the certificate: DigiCert Close Services CA</p>

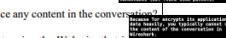
5

--	--	--

D Examining traces

No	Description	Result
D.1	Download the following file, and examine the trace with Wireshark: http://asecuritysite.com/log/ssl1.zip	<p>Client IP address and TCP port: IP: 192.168.8.28 Port: 2099</p> <p>Web server IP address and TCP port: IP: 46.211.169.66 Port: 443</p> <p>Determine one of the symmetric key encryption methods, the key exchange, and the hashing methods that the client wants to use (Hint: look at the 'Client Hello' packet) AES_256_CBC_SHA</p> <p>Which SSL/TLS method has been used: TLS 1.0</p> <p>Which encryption method is used for the tunnel: AES_256_CBC</p> <p>Which hashing method is used for the tunnel: SHA</p> <p>What is the length of the encryption key: 192-256</p>
D.2	Download the following file, and examine the trace with Wireshark: http://asecuritysite.com/log/https.zip	<p>Client IP address and TCP port: IP: 172.16.121.355 Port: 3923</p> <p>Web server IP address and TCP port: IP: 87.146.169.123 Port: 443</p> <p>Which SSL/TLS method has been used: TLS 1.2</p> <p>Which encryption method is used for the tunnel: AES_256_CBC</p> <p>Which hashing method is used for the tunnel: SHA</p> <p>What is the length of the encryption key: 256-384</p>
D.3	Download the following file, and examine the trace with Wireshark: http://asecuritysite.com/log/heart.zip	<p>Client IP address and TCP port: IP: 172.16.121.1 Port: 64666</p> <p>Web server IP address and TCP port: IP: 172.16.121.158 Port: 443</p> <p>Which SSL/TLS method has been used: TLS 1.3</p>

6

		<p>Which encryption method is used for the tunnel: AES_256_GCM</p> <p>Which hashing method is used for the tunnel: SHA384</p> <p>What is the length of the encryption key: 256-384</p>
D.4	Download the following file, and examine the trace with Wireshark: http://asecuritysite.com/log/pssec.zip	<p>Which is the IP address of the client and of the server: Client: 192.168.8.28 Server: 146.178.210.9</p> <p>Which packet number identifies the start of the VPN connection (Hint: look for UDP Port 500): 8</p> <p>Determine one of the encryption and the hashing methods that the client wants to use: AES-CBC SHA</p> <p>Now determine the encryption and hashing methods that are agreed in the ISAKMP: AES-CBC SHA</p>
	Download the following file, and examine the trace with Wireshark: http://asecuritysite.com/log/tor.zip	<p>Which TCP port does the client use to send to?: 443</p> <p>What is the IP address of the Tor node that the client connects to?: IP: 172.19.121.69 Port: 1111</p> <p>What is strange about the packet size?: </p> <p>Is SSL/TLS used for the connection?: No, tor is not using TLS for that key.</p> <p>Can you trace any content in the conversation?: </p> <p>Can you determine the Web site that is being connected to?: </p>

What I should have learnt from this lab?

The key things learnt:

- How do perform a cryptography assessment on a Web site (using sslabs) and in how to spot weaknesses.

7

- Able to interpret an SSL/TLS session, and identify the important elements of the Client Hello, and the Server Hello.

8