

# Secure Communications

## Week 11

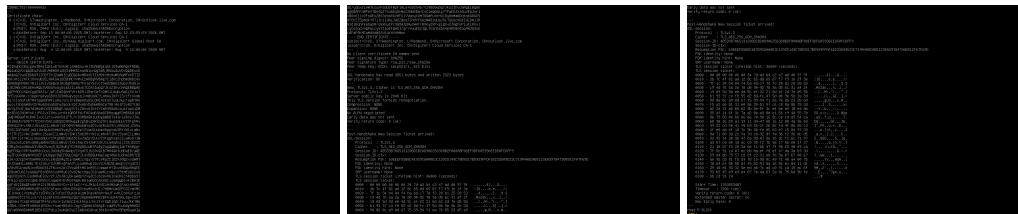
### Tunnelling and Web Security (Part 2)

---

#### 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**

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.20	66.211.169.66	TCP	74	2099 → 443 [SYN] Seq=0 Win=0 Len=0 MSS=1269 WS=4 SACK_PERM TSval=315475 Tsec=0
2	0.205353	66.211.169.66	192.168.0.20	TCP	58	443 → 2099 [SYN, ACK] Seq=0 Ack=1 Win=8196 Len=0 MSS=1212
3	0.205652	192.168.0.20	66.211.169.66	TCP	54	2099 → 443 [ACK] Seq=141 Win=16968 Len=0
4	0.207649	192.168.0.20	66.211.169.66	TLSv1	197	Client Hello (SN=paypal.com)
5	0.410595	66.211.169.66	192.168.0.20	TCP	1266	443 → 2099 [PSH, ACK] Seq=141 Ack=144 Win=40815 Len=1212 [TCP PDU reassembled in ...]
6	0.410821	192.168.0.20	66.211.169.66	TCP	1266	443 → 2099 [PSH, ACK] Seq=1213 Ack=144 Win=40815 Len=1212 [TCP PDU reassembled in ...]
7	0.411088	192.168.0.20	66.211.169.66	TCP	54	2099 → 443 [ACK] Seq=144 Ack=2425 Win=16968 Len=0
8	0.411240	66.211.169.66	192.168.0.20	TLSv1	608	Server Hello, Certificate, Server Hello Done
9	0.416329	192.168.0.20	66.211.169.66	TLSv1	244	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
10	0.615203	66.211.169.66	192.168.0.20	TCP	54	443 → 2099 [ACK] Seq=2975 Ack=334 Win=40825 Len=0
11	0.615319	192.168.0.20	66.211.169.66	TCP	195	Change Cipher Spec, Encrypted Handshake Message
12	0.615631	192.168.0.20	66.211.169.66	TCP	1266	2099 → 443 [ACK] Seq=334 Ack=3038 Win=16363 Len=1212 [TCP PDU reassembled in 15]
13	0.616544	192.168.0.20	66.211.169.66	TCP	1266	2099 → 443 [ACK] Seq=1546 Ack=3838 Win=16363 Len=1212 [TCP PDU reassembled in 15]
14	0.839748	66.211.169.66	192.168.0.20	TCP	54	443 → 2099 [ACK] Seq=3038 Ack=2758 Win=38261 Len=0
15	0.839934	192.168.0.20	66.211.169.66	TLSv1	483	Application Data
16	1.128526	66.211.169.66	192.168.0.20	TCP	54	443 → 2099 [ACK] Seq=3038 Ack=3187 Win=37772 Len=0
17	1.128642	66.211.169.66	192.168.0.20	TLSv1	211	Application Data
18	1.128730	66.211.169.66	192.168.0.20	TLSv1	83	Encrypted Alert
19	1.128931	192.168.0.20	66.211.169.66	TCP	54	2099 → 443 [ACK] Seq=3187 Ack=3217 Win=16177 Len=0
20	1.129735	192.168.0.20	66.211.169.66	TCP	54	2099 → 443 [FIN, ACK] Seq=3187 Ack=3217 Win=16177 Len=0
21	1.332136	66.211.169.66	192.168.0.20	TCP	54	443 → 2099 [ACK] Seq=3217 Ack=3188 Win=37771 Len=0

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on eth0

Ethernet II, Src: Intel47:30:1d (00:1f:3c:4f:30:1d), Dst: Netgear\_b0:d6:8c (08:00:27:00:d6:8c)

Internet Protocol Version 4, Src: 192.168.0.20, Dst: 66.211.169.66

Transmission Control Protocol, Src Port: 2099, Dst Port: 443, Seq: 0, Len: 0

ssl.pcap
Packets: 21
Profile: Default

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.20	66.211.169.66	TCP	74	2099 → 443 [SYN] Seq=0 Win=0 Len=0 MSS=1269 WS=4 SACK_PERM TSval=315475 Tsec=0
2	0.205353	66.211.169.66	192.168.0.20	TCP	58	443 → 2099 [SYN, ACK] Seq=0 Ack=1 Win=8196 Len=0 MSS=1212
3	0.205652	192.168.0.20	66.211.169.66	TCP	54	2099 → 443 [ACK] Seq=141 Win=16968 Len=0
4	0.207649	192.168.0.20	66.211.169.66	TLSv1	197	Client Hello (SN=paypal.com)
5	0.410595	66.211.169.66	192.168.0.20	TCP	1266	443 → 2099 [PSH, ACK] Seq=141 Ack=144 Win=40815 Len=1212 [TCP PDU reassembled in ...]
6	0.410821	192.168.0.20	66.211.169.66	TCP	1266	443 → 2099 [PSH, ACK] Seq=1213 Ack=144 Win=40815 Len=1212 [TCP PDU reassembled in ...]
7	0.411088	192.168.0.20	66.211.169.66	TCP	54	2099 → 443 [ACK] Seq=144 Ack=2425 Win=16968 Len=0
8	0.411240	66.211.169.66	192.168.0.20	TLSv1	608	Server Hello, Certificate, Server Hello Done
9	0.416329	192.168.0.20	66.211.169.66	TLSv1	244	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
10	0.615203	66.211.169.66	192.168.0.20			

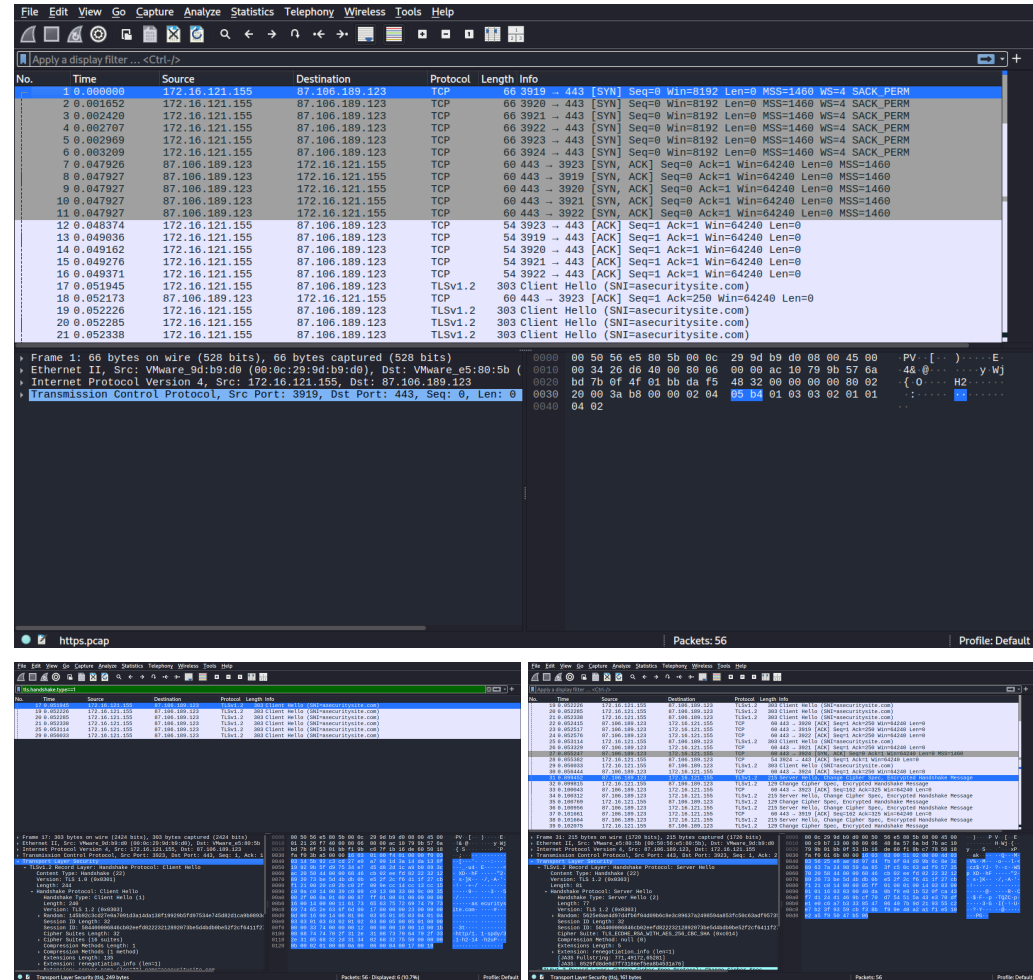
Client IP address and TCP port:	IP: 192.168.0.20   Port: 2099
Web server IP address and TCP port:	IP: 66.211.169.66   Port: 443
Determine one of the symmetric key encryption methods, the key exchange, and the hashing methods that the client wants to use (Hint: look at the 'Client Hello' packet)"	AES_256_CBC 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_3DES_EDE_CBC_SHA (0x000a)

What is the length of the encryption key:

168-bit

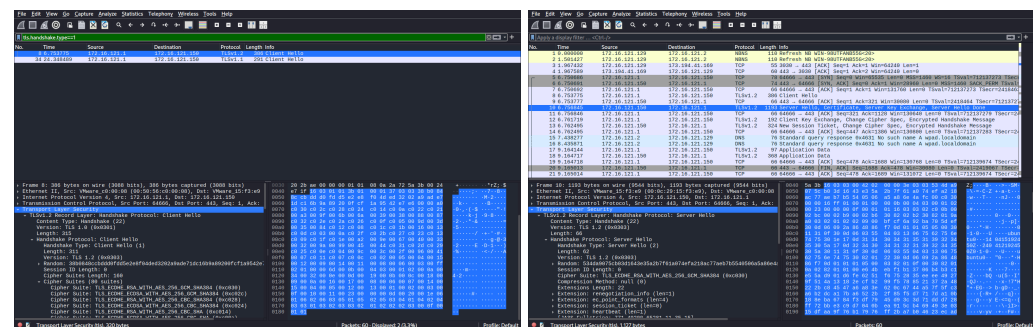
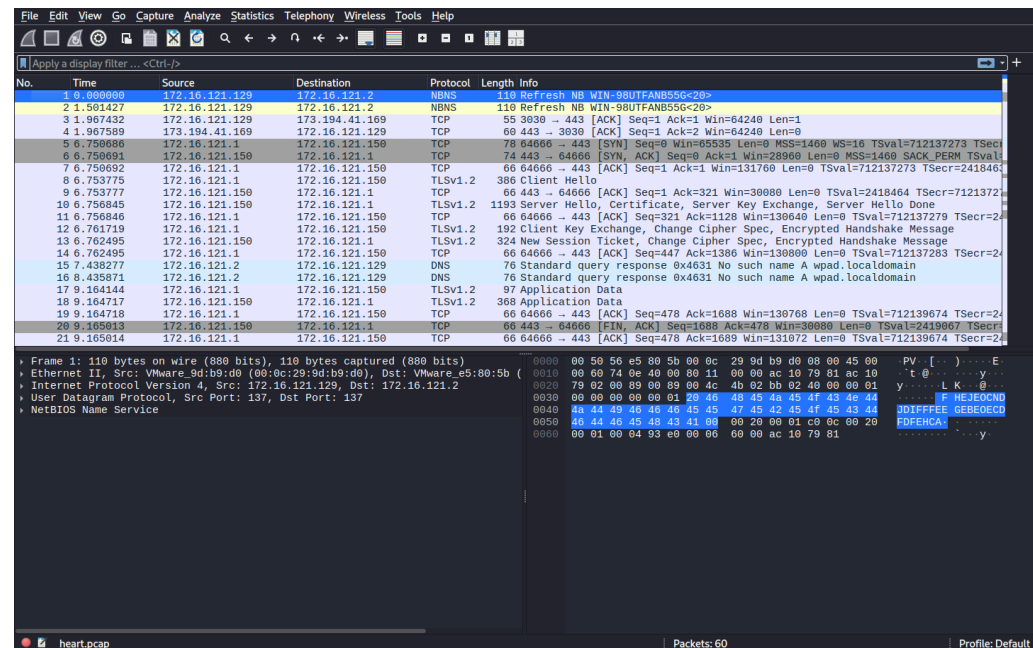
B.2 <http://asecuritysite.com/log/https.zip>

Download the following file, and examine the trace with Wireshark



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

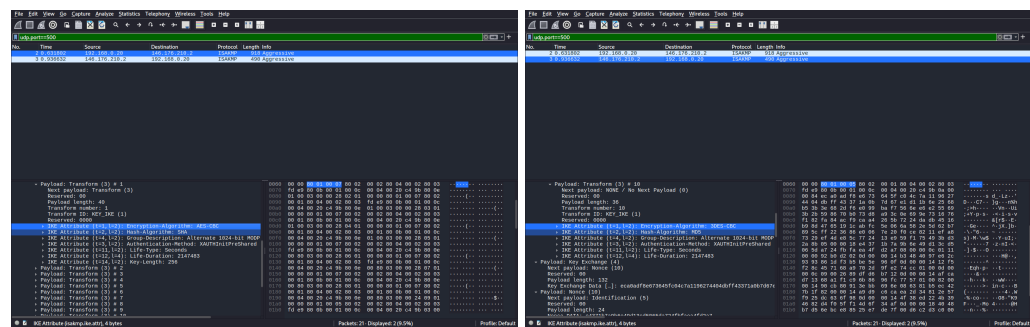
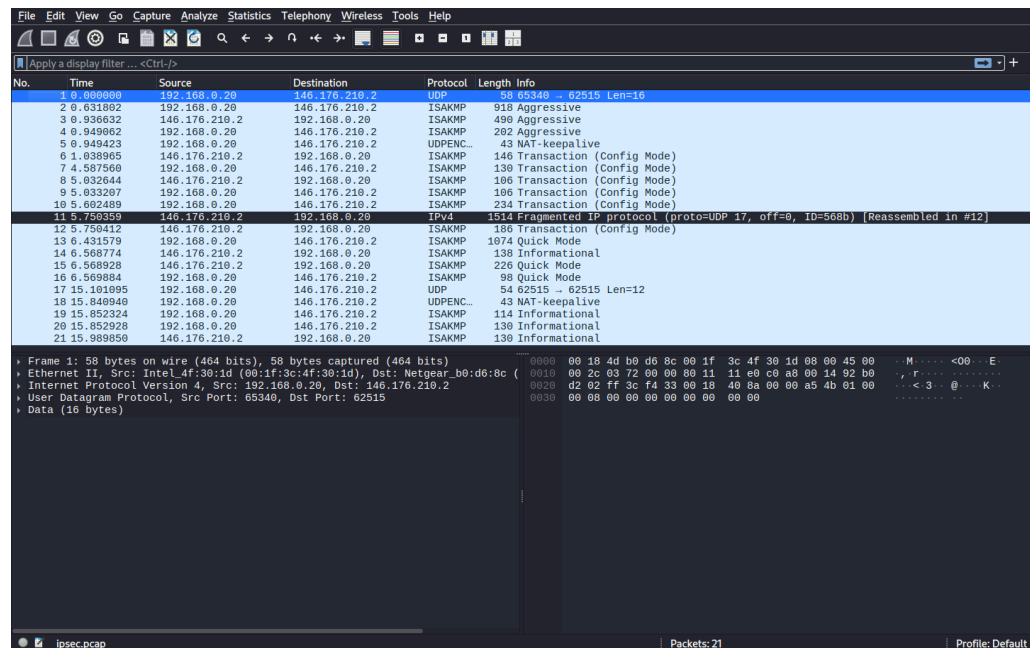
Download the following file, and examine the trace with Wireshark



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 Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
Which hashing method is used for the tunnel:	SHA384 Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
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:

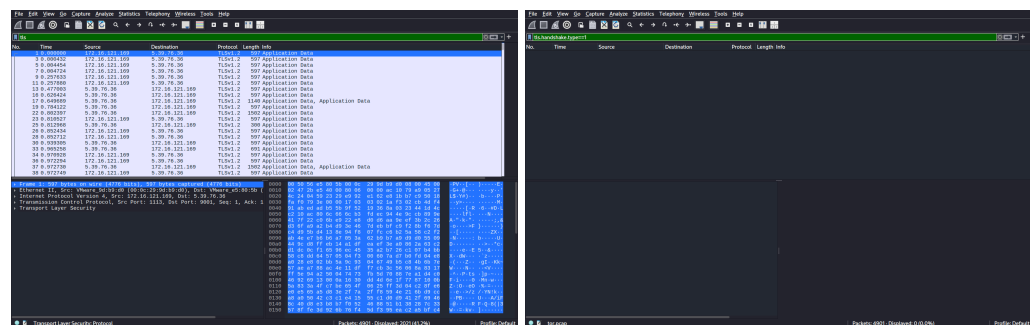
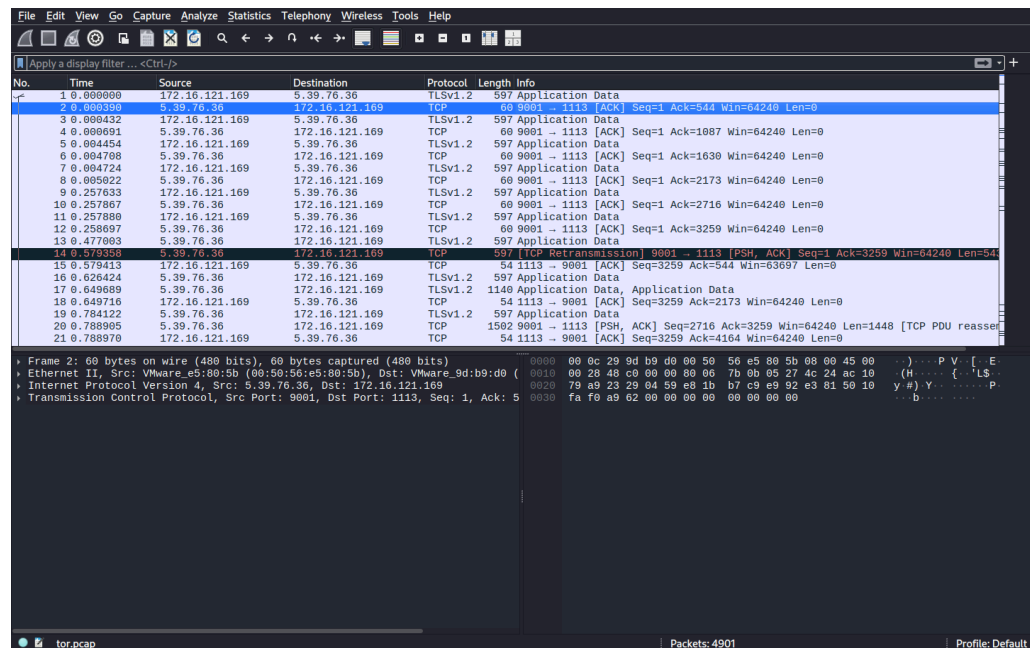
AES-CBC  
SHA

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



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>

### A Web cryptography assessment

The Sslabs tool (<https://sslabs.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>B rating</b>	<b>B rating</b>	<b>A rating</b>
The digital certificate key size and type?	<b>EC 256 bits SHA256withECDSA</b>	<b>RSA 2048 bits SHA256withRSA</b>	<b>RSA 2048 bits SHA256withRSA</b>
Does the name of the site match the name on the server?	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>
Who is the signer of the digital certificate?	<b>Let's Encrypt</b>	<b>Let's Encrypt</b>	<b>DigiCert Global G2</b>
The expiry date on the digital certificate?	<b>Mon, 19 Jan 2020 08:53:28 UTC</b>	<b>Sat, 24 Jan 2020 09:44:47 UTC</b>	<b>Fri, 24 Jul 2020 23:30:50 UTC</b>
What is the hashing method on the certificate?	<b>SHA256withECDSA</b>	<b>SHA256withRSA</b>	<b>SHA256withRSA</b>
If it uses RSA keys, what is the e value that is used in the encryption (M <sup>e</sup> mod N)?	<b>1</b>	<b>65537</b>	<b>65537</b>
Determine a weak cipher suite used and explain why it might be weak?	<b>Protocol Support: TLS 1.0 and TLS 1.1</b>	<b>Protocol Support: TLS 1.0 and TLS 1.1</b>	<b>All good</b>
Is SSL v2 supported?	<b>No</b>	<b>No</b>	<b>No</b>
If SSL v2 was supported, what problems might there be with the site (this will require some research)?	<b>No</b>	<b>No</b>	<b>No</b>
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?	<b>Supports: TLS 1.0 and TLS 1.1</b> Older devices or software may fail to connect	<b>Supports: TLS 1.0 and TLS 1.1</b> Older devices or software may fail to connect	<b>Not Supported: TLS 1.0 and TLS 1.1</b>
Is the site vulnerable to Heartbleed?	<b>No</b>	<b>No</b>	<b>No</b>
Is the site vulnerable to DROWN?	<b>No</b>	<b>No</b>	<b>No</b>
Is the site vulnerable to BREAST?	<b>No</b>	<b>No</b>	<b>No</b>
Is the site vulnerable to POODLE?	<b>No</b>	<b>No</b>	<b>No</b>

1

Research questions:

What does TLS, ECDHE, RSA, WITH, AES, 256, CBC, SHA384 identify?  
It is the ECDHE (Elliptic Curve Diffie-Hellman Ephemeral) key exchange, ECDHE (Elliptic Curve Diffie-Hellman Ephemeral) authentication, RSA encryption, AES-256 in CBC mode, and SHA384 / HMAC: SHA-384.

If a site gets a 'T' grade, what is the problem?  
Trust issues (T): If sslabs don't trust a certificate (and there aren't any other security issues), it assigns it a 'T' grade (for "Trust").

If the site was susceptible to Poodle, what is the vulnerability?  
Poodle is an attack on SSL 3.0 padding (and occasionally TLS padding). SSLv3 is enabled, and 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/Tru113/ssl-labs/blob/master/ssl-labsscanner.py  
import requests  
import time  
import sys  
import logging  
API = 'https://api.ssl-labs.com/api/v2/'  
  
def requestAPI(path, payload={}):  
    '''This is a helper method that takes the path to the relevant  
    API call and the 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.exceptions.RequestException:  
        logging.exception('Request failed.')  
        sys.exit(1)  
    data = response.json()  
    return data  
  
def resultsFromCache(host, publish='off', startNew='off', fromCache='on',  
all='done'):  
    path = 'analyze'  
    payload = {'host': host,  
               'publish': publish,  
               'startNew': startNew,  
               'fromCache': fromCache,  
               'all': all}
```

2

```
'startNew': startNew,  
'fromCache': fromCache,  
'all': all  
}  
data = requestAPI(path, payload)  
return data  
  
def newScan(host, publish='off', startNew='on', all='done',  
ignoreMismatch='on'):  
    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")  
        print row['web']
```

Note that it can 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:

```
Technical Details  
Certificate Issued: TLS, AES, 128, GCM, SHA256, 128 bit keys, TLS 1.2  
The cipher suite is affected by experimental attacks to the underlying random number generation.  
The cipher suite is affected by experimental attacks to the underlying random number generation.  
The cipher suite is affected by experimental attacks to the underlying random number generation.
```

Site name: **bbc.co.uk** Site rating: **Grade: 'B'**

Other significant details:

```
Technical Details  
Certificate Issued: TLS, AES, 128, GCM, SHA256, 128 bit keys, TLS 1.2  
The cipher suite is affected by experimental attacks to the underlying random number generation.  
The cipher suite is affected by experimental attacks to the underlying random number generation.  
The cipher suite is affected by experimental attacks to the underlying random number generation.
```

3

### B Viewing details

No	Description	Result
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 <b>Google.com</b> .  Stop Wireshark and identify some of your connection details:	Your IP address and TCP port: <b>IP: 10.0.2.15   Port: 52674</b>  Google's Web server IP address and TCP port: <b>IP: 209.85.203.94   Port: 443</b>  Which SSL/TLS version is used: <b>TLS 1.2</b>  By examining the Wireshark trace, which encryption method is used for the tunnel (hint: look in the 'Server Hello' response): <b>TLS_AES_128_GCM_SHA256 (0x1301)</b>  By examining the Wireshark trace, which hashing method is used for the tunnel (hint: look in the 'Server Hello' response): <b>SHA256 (0x1404)</b>  By examining the Wireshark trace, what is the length of the encryption key (hint: look in the 'Server Hello' response): <b>128</b>  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. <b>Yes</b>
B.2	Run Wireshark and capture traffic from your main network connection. Start a Web browser and go to <b>https://twitter.com</b> .  Stop Wireshark and identify some of your connection details:	Your IP address and TCP port: <b>IP: 10.0.2.15   Port: 60394</b>  Twitter's Web server IP address and TCP port: <b>IP: 54.237.156.18   Port: 443</b>  Which SSL/TLS version is used: <b>TLS 1.2</b>  By examining the Wireshark trace, which encryption method is used for the tunnel: <b>TLS_AES_256_GCM_SHA384 (0x1303)</b>

4

		<p>By examining the Wireshark trace, which hash method is used for the tunnel: <b>SHA384 (H1181)</b></p> <p>By examining the Wireshark trace, what is the length of the encryption key: <b>256</b></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? <b>Yes</b></p>
--	--	---

## C OpenSSL

No	Description	Result
C.1	On your VM instance (or your desktop), make a connection to the <b>www.live.com</b> Web site:  <b>openssl s_client -connect www.live.com:443</b>	<p>Which SSL/TLS method has been used: <b>TLSv1.2</b></p> <p>Which method is used on the encryption key on the certificate, and what is the size of the public key? <b>ECDSA (secp256r1), 521 bits</b></p> <p>Which is the handshaking method that has been used to create the encryption key? <b>ECDH (secp256r1), 521 bits</b></p> <p>Which TLS version is used for the tunnel? <b>TLSv1.2</b></p> <p>Which symmetric encryption method is used for the tunnel: <b>AES-256-GCM</b></p> <p>Which hashing method is used for the tunnel: <b>SHA-384</b></p> <p>What is the length of the symmetric encryption key: <b>256-bits</b></p> <p>Who has signed the certificate: <b>DigiCert Cloud Services CA-1</b></p>

5

--	--	--

## D Examining traces

No	Description	Result
D.1	Download the following file, and examine the trace with Wireshark:  <b>http://asecuritysite.com/log/ssl.zip</b>	<p>Client IP address and TCP port: <b>IP: 172.16.0.20   Port: 2899</b></p> <p>Web server IP address and TCP port: <b>IP: 44.211.109.66   Port: 443</b></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)? <b>AES-256-GCM SHA</b></p> <p>Which SSL/TLS method has been used: <b>TLS 1.2</b></p> <p>Which encryption method is used for the tunnel: <b>AES-256-GCM</b></p> <p>Which hashing method is used for the tunnel: <b>SHA</b></p> <p>What is the length of the encryption key: <b>256-bits</b></p>
D.2	Download the following file, and examine the trace with Wireshark:  <b>http://asecuritysite.com/log/https.zip</b>	<p>Client IP address and TCP port: <b>IP: 172.16.121.155   Port: 3923</b></p> <p>Web server IP address and TCP port: <b>IP: 47.146.189.123   Port: 443</b></p> <p>Which SSL/TLS method has been used: <b>TLS 1.2</b></p> <p>Which encryption method is used for the tunnel: <b>AES-256-GCM</b></p> <p>Which hashing method is used for the tunnel: <b>SHA</b></p> <p>What is the length of the encryption key: <b>256-bits</b></p>
D.3	Download the following file, and examine the trace with Wireshark:  <b>http://asecuritysite.com/log/heart.zip</b>	<p>Client IP address and TCP port: <b>IP: 172.16.121.15   Port: 64668</b></p> <p>Web server IP address and TCP port: <b>IP: 172.16.121.158   Port: 443</b></p> <p>Which SSL/TLS method has been used: <b>TLS 1.2</b></p>

6

		<p>Which encryption method is used for the tunnel: <b>AES-256-GCM</b></p> <p>Which hashing method is used for the tunnel: <b>SHA384</b></p> <p>What is the length of the encryption key: <b>256-bits</b></p>
D.4	Download the following file, and examine the trace with Wireshark:  <b>http://asecuritysite.com/log/ipsec.zip</b>	<p>Which is the IP address of the client and of the server: Client: <b>192.168.0.20</b> Server: <b>146.176.218.2</b></p> <p>Which packet number identifies the start of the VPN connection (Hint: look for UDP Port 500): <b>1</b></p> <p>Determine one of the encryption and the hashing methods that the client wants to use: <b>AES-GCM SHA</b></p> <p>Now determine the encryption and hashing methods that are agreed in the ISAKMP: <b>AES-256-GCM SHA</b></p>
	Download the following file, and examine the trace with Wireshark:  <b>http://asecuritysite.com/log/tor.zip</b>	<p>Which TCP port does the client use to send to? <b>9001</b></p> <p>What is the IP address of the Tor node that the client connects to? <b>IP: 172.16.121.109   Port: 1112</b></p> <p>What is strange about the packet size? <b>The size of the packet is 100 bytes, which is the size of the Tor node's public key.</b></p> <p>Is SSL/TLS used for the connection? <b>No, the connection is not encrypted.</b></p> <p>Can you trace any content in the conversation? <b>No, the connection is not encrypted.</b></p> <p>Can you determine the Web site that is being connected to? <b>No, the connection is not encrypted.</b></p>

## What I should have learnt from this lab?

The key things learnt:

- How to perform a cryptography assessment on a Web site (using sslslabs) 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