Christopher Bazyani

Practical Cyber Security

Unit 4

Packet Sniffing – SSL

**Opening the SSL Trace**

Opening the SSL pcap file supplied

Text

Description automatically generated with low confidence

**Inspecting the SSL Trace**

Entering and applying a display filter of “ssl”.

A picture containing application

Description automatically generated

Selecting the number 12 SSL packet and viewing its application data protocol



Text

Description automatically generated

**The SSL Handshake**

Selecting packet 4, which is a TLS Client Hello message



Text

Description automatically generated

Selecting packet 6, which is a TLS Server Hello message



The session ID sent by the server is 32 bytes long. This identifier allows later resumption of the session with an abbreviated handshake when both the client and server indicate the same value.

Text

Description automatically generated

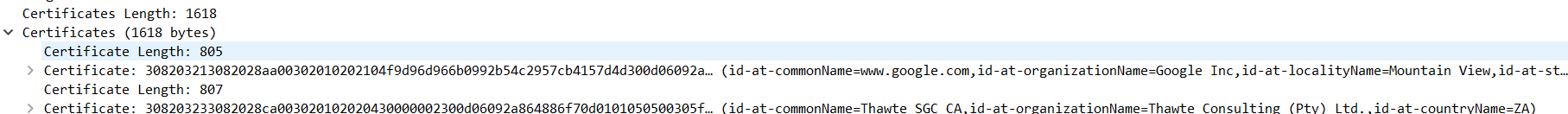
The Cipher method chosen by the Server is TLS\_RSA\_WITH\_RC4\_128\_SHA (0x0005). The Client will list the different cipher methods it supports, and the Server will pick one of these methods to use.

**Certification Message**

Finding and inspecting the details of the Certificate message including expanding the Handshake

protocol block within the TLS Record. Packet number 7





**Client Key Exchange and Change Cipher Messages**

Finding and inspecting the details of the Client Key Exchange and Change Cipher messages for packet 9



Text, letter

Description automatically generated

**Alert Message**

Lastly, we find and inspect the details of an Alert message at the end of the trace using packet 42.



Text

Description automatically generated