Question 3

(a) Chrome 57 connected to whisperlab.org and the server picks

TLS 1.2: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256

(b) Chrome 57 connected to whisperlab.org and the client picks

TLS 1.2: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256

(c) Android 7.0 connected to uwo.ca and the client picks

TLS 1.2: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384

(d) IE 7 / Vista connected to uwo.ca and the server picks

TLS 1.0: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA