COMP416 – Project 2

**PART1.A**

1. **How many TCP packets are transmitted in total while your KUSIS ID number is exchanged one by one with non-persistent connections?**

138 TCP packets are transmitted in total with non-persistent connections.

Graphical user interface, application

Description automatically generated

1. **How many cipher suites does your client support? Which frame is this information part of?**

My client supports 49 cipher suites. It can be seen by selecting any of the ‘Client Hello’ packets. The information is under the Transport Layer Security -> TLSv1.3 Record Layer: Handshake Protocol: Client Hello -> Handshake Protocol: Client Hello

**Graphical user interface, text, application

Description automatically generated**

1. **In which frame does the server provide its choice of cipher suite? Which cipher does your server choose? What is the complete name of Server-Hello packet and the possible reason for it?**

The cipher suite choice of the server is under the Transport Layer Security -> TLSv1.3 Record Layer: Handshake Protocol: Server Hello -> Handshake Protocol: Server Hello. My server chooses cipher suite: TLS\_AES\_256\_GCM\_SHA384 (0x1302).

**Table

Description automatically generated**

1. **What is the message type for (a) Client Hello (b) Server Hello? What are other message types supported through the employment of this field?**

The message type is Client Hello, and its code is (1). Message type is Server Hello, and its code is (2). These are two of the SSL handshake message types. There are other types such as Hello Request (0), Certificate (11), ServerKeyExchange (12), Certificate Request (13), ServerHelloDone (14), Certificate Verify (15), ClientKeyExchange (16), Finished (20).

**PART1.B**

1. **Report both delays for 5 different executions and present the measurements as a single graph. Briefly describe the reasons for the results you have obtained.**

Quest

PART2

PART3