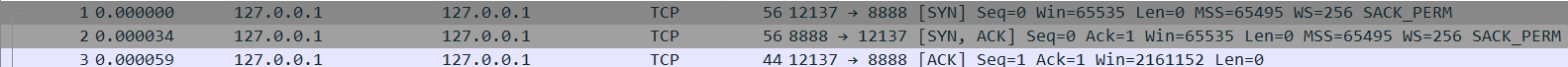
**學號：D1166506**

**姓名：周嘉禾**

一張含有 文字, 電子產品, 螢幕擷取畫面, 陳列 的圖片

自動產生的描述

1. 前三個封包是TCP的三向交握

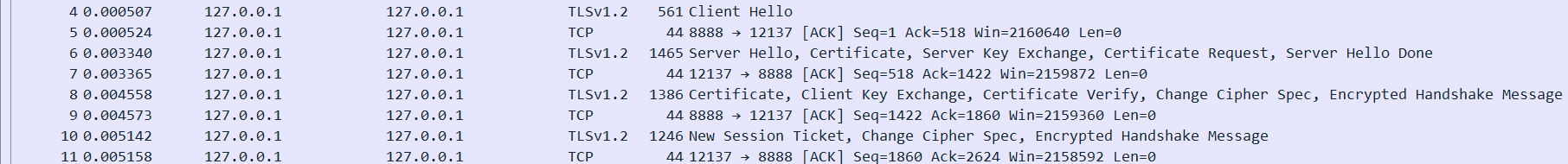


1. 第5~11個封包會交換SSL(TLSv1.2) 的資訊
   1. 第4個封包是從Client端發送的，以Client Hello作為開頭，並包含多個SSL通訊可用的參數與資訊，像是TLS Version, Random Number, Session ID, Cipher Suites, Compression Methods, Extensions (Optional)等
   2. 第6個封包是從Server端發送的，以 Server Hello作為開頭，並交換 Certificate, Server Key Exchange, Certificate Request等資訊，並以Server Hello Done作為結尾
   3. 第8個封包是從Client端發送的，包含Certificate, Client Key Exchange, Certificate Verify

同時，在這個封包中交換Change Cipher Spec, Encrypted Handshake Message等資訊

* 1. 第10個封包是從Server端發送的，包含New Session Ticket, Change Cipher Spec, Encrypted Handshake Message等資訊

值得注意的是，這個交握過程的每次封包發送，必回傳一個ACK封包，而且不是以SSL加密



1. 第12~21個封包是Client/Server的通訊過程，以SSL加密，並且每次傳送封包都有一個以TCP回傳的ACK Flag

一張含有 文字, 字型, 螢幕擷取畫面 的圖片

自動產生的描述

1. 第22~25個封包是Client/Server連線關閉的四向交握，以TCP進行通訊，沒有使用SSL加密

