Esercitazione 7 - TLS/SSL

*tasto destro su "**tls-trace.pcap**" —> **open with wireshark** —> "tcp.stream eq 0"*

*aprire messaggio **Client Hello**:*

- *ogni record TLS inizia con: **content type**, **version** e **length**;*
- ***random bytes**: è la nonce casuale;*
- ***cipher suites**: quelle supportate sono **18**;*

*Aprire messaggio **Server Hello:***

- *nel campo **cipher suite** è contenuta la suite scelta dal server fra le **18** supportate dal client;*
- *dato che la **session id length** è zero, non c'è una **session id***
- *il nome della Certificate Authority è contenuto nel frame 31 e non nel messaggio di **Server Hello**.*

*Al frame 33 si trova il messaggio di **SSL Key Exchange**:*

*possiamo notare che contiene la chiave pubblica **ECDH** del Client che viene usata per scambiare le chiavi **ECDH** insieme alla **chiave pubblica del server** e alla **chiave privata del Client**. (Nb **ECDH** è EC Diffie Hellmann).*

*Abbiamo anche i messaggi **Change Cipher Spec** e **Encrypted Key Exchange** (sono equivalenti ai **finished message**):*

- *il contenuto aggiuntivo per questa connessione, ovvero il **new session ticket**, si ha nel **frame 35**.*
- *il vantaggio che si ha nell'usare **ECDHE** consiste nel fatto che è più veloce di **DHE** ed offre maggiore segretezza.*
- *l'algoritmo usato per cifrare i messaggi TLS è **AES_128_GCM**.*