Visualizzazione di pacchetti scambiati con Wireshark

Utilizziamo il sito www.old-unisannio.it (non più online) per visualizzare i pacchetti; questo perchè il sito nella sua vecchia versione ascolta sulla singola porta 80.

Se avviamo wireshark in ascolto sulla rete wifi, con il filtro `tcp port 80`, otteniamo la cattura dei pacchetti:

Segmento SYN

L'attivazione della connessinoe è data dai segmenti SYN e ACK: infatti il segmento SYN inviato dalla porta 59105, numero di porta aperto dal browser verso il numero di porta 80 verso la macchina remota. E' un **segmento di controllo** inviato dal client verso il server con un numero di sequenza posto a 0.

Tramite wireshark è possibile anche vedere la grandezza della finestra

Questo significa che il mittente può inviare fino a 64240 byte, corrispondente alla memoria disponibile nel buffer del ricevente. Non è però detto che inviando più di 64240 byte quelli in eccesso vengano scartati; questo perchè nel frattempo il buffer in ricezione potrebbe liberarsi.

Possiamo inoltre vedere come siano presenti delle opzioni all'interno dell'intestazione:

da queste informazioni estrapoliamo la grandezza massima di un segmento, ovvero 1460 bytes; questo ci dice che le nostre informazioni verranno incapsulate all'interno di segmenti con un'area dati al più di 1460 byte.
Tra le opzioni troviamo anche SACK (selective acknowledgement), opzione che ci permette di abilitare la modalità di riscontro selettivo come variante del protocollo TCP.

Segmento SYN ACK

Possiamo osservare anche il segmento SYN ACK:

Questo segmento viene inviato dal server verso il client per accettare la richiesta di connessione e promuovere la connessione client-server.

Infine si chiude la 3-Way Handshake con il segmento di riscontro:

Notiamo anche che il browser apre due connesisoni: una dalla porta 59105 ed una da 59106; i browser moderni attivano due connessioni per migliorare l'efficienza. Inoltre, se un'ulteriore connessione servirà successivamente, la connessione è già pronta all'uso.