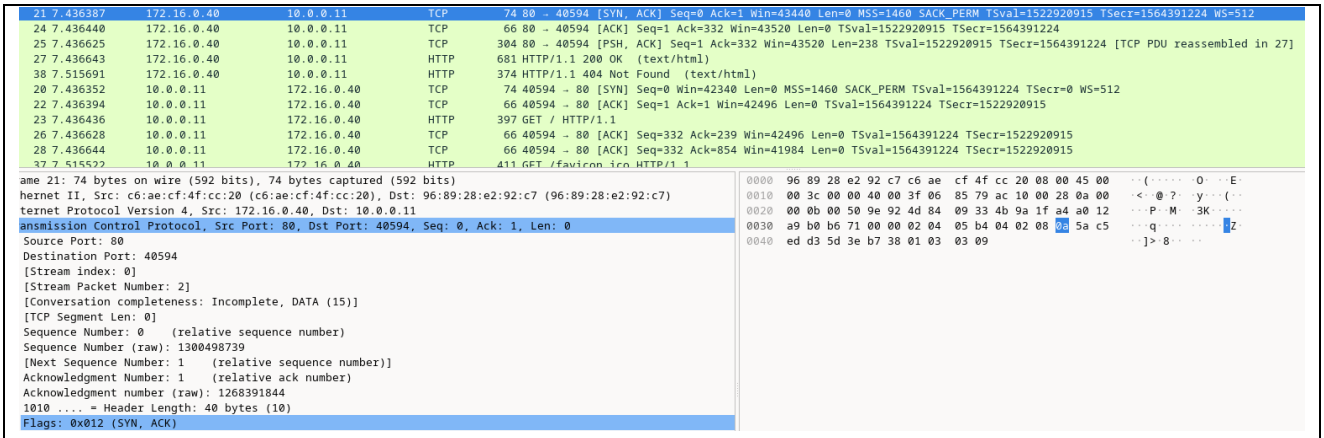
S11L2

UNIT 3

Marco Falchi



Qual è il numero di porta TCP di origine?

Il numero di porta TCP di origine è 40594

Come classificheresti la porta di origine?

La porta di origine, 40594, è una porta effimera (o dinamica). Le porte effimere sono utilizzate dai sistemi operativi client per connessioni stabilite in uscita.

Non sono porte "ben note" (come la 80 per HTTP o la 443 per HTTPS), né porte registrate (quelle assegnate a servizi specifici ma non comunemente usate).

Qual è il numero di porta TCP di destinazione?

Il numero di porta TCP di destinazione è 80 quindi su un servizio http

Come classificheresti la porta di destinazione?

La porta di destinazione è la 80 che è una porta nota (well-known port).

Quale flag è impostato?

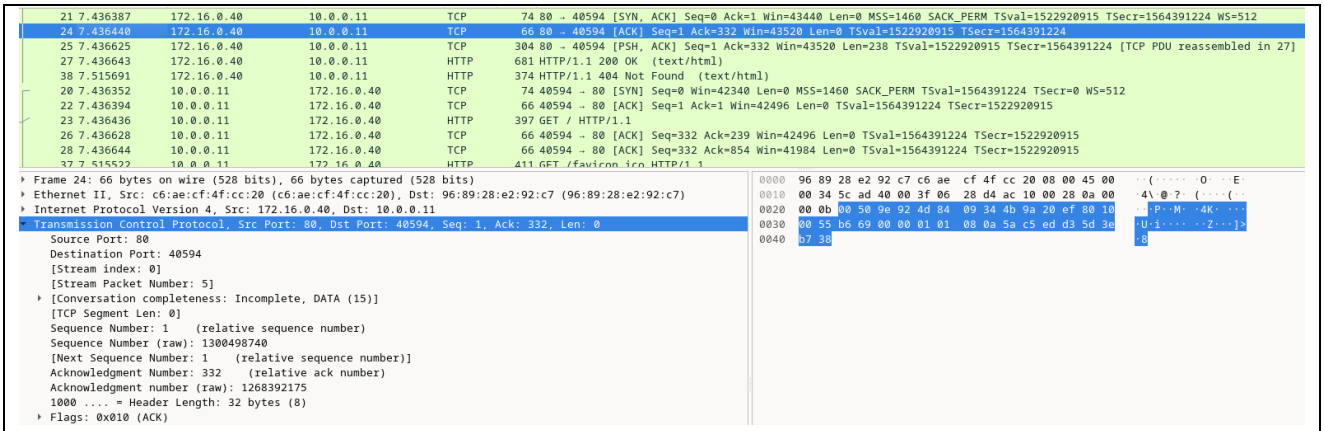
Il flag SYN (Synchronize) è impostato.

Questo indica che il pacchetto fa parte della prima fase di un **three-way handshake** per stabilire una connessione TCP.

A quale valore è impostato il numero di sequenza relativo?

Il numero di sequenza relativo è impostato a 0.

Un numero di sequenza relativo di 0 è tipico del primo pacchetto di una sessione TCP, come in questo caso, dove il flag SYN è impostato.



Quali sono i valori delle porte di origine e destinazione?

I valori delle porte sono invertiti rispetto al primo pacchetto:

Porta di origine: 80 (quella del server web)

Porta di destinazione: 40594 (la porta effimera del client che ha avviato la connessione)

Quali flag sono impostati?

Sono impostati due flag:

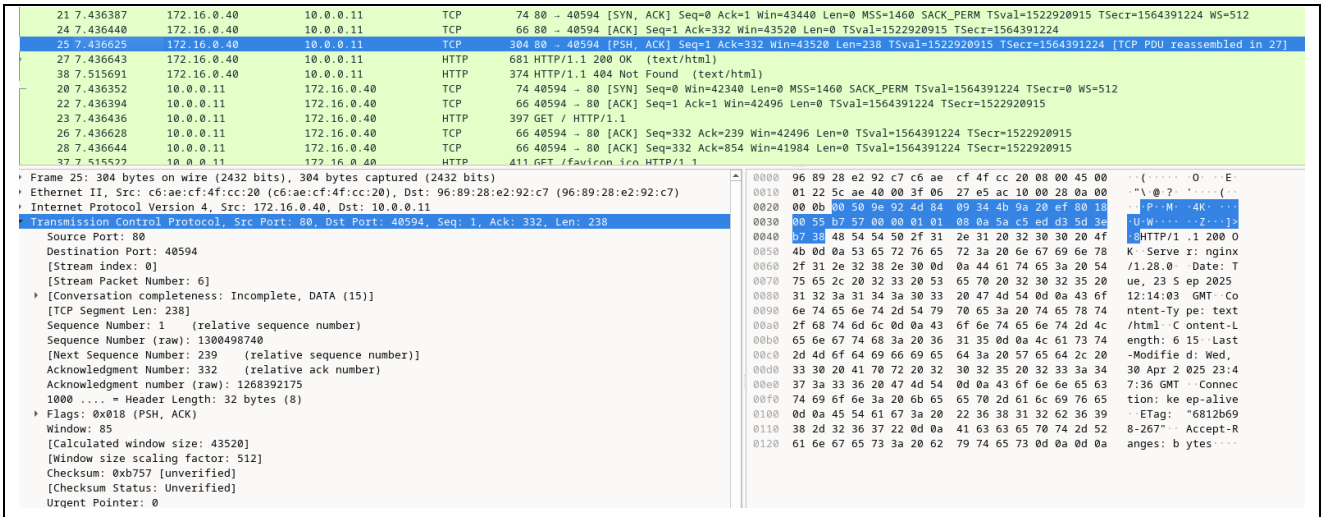
SYN (Synchronize): per sincronizzare i numeri di sequenza.

ACK (Acknowledgment): per confermare di aver ricevuto il primo pacchetto SYN del client.

A quali valori sono impostati i numeri relativi di sequenza acknowledgment?

Numero di sequenza relativo: 0. Questo valore è impostato a 0 per la prima volta che il server invia un pacchetto SYN.

Numero di acknowledgment relativo: 1. Questo valore indica che il server sta confermando la ricezione del pacchetto precedente del client e si aspetta il prossimo pacchetto con un numero di sequenza pari a 1.



Quale flag è impostato?

Il flag **ACK** (Acknowledgment) è impostato.

L'impostazione di questo flag conferma che il client ha ricevuto il pacchetto precedente del server (il SYN-ACK) e che la connessione è stata stabilita con successo, pronta per lo scambio di dati.

```
tcpdump [ -AbdDefhHIJKlLnNOpqStuUvxX# ] [ -B buffer_size ]
        [ -c count ] [ --count ] [ -C file_size ]
        [ -E spi@ipaddr algo:secret,...  ]
        [ -F file ] [ -G rotate_seconds ] [ -i interface ]
        [ --immediate-mode ] [ -j tstamp_type ] [ -m module ]
        [ -M secret ] [ --number ] [ --print ] [ -Q in|out|inout ]
        [ -r file ] [ -s snaplen ] [ -T type ] [ --version ]
        [ -V file ] [ -w file ] [ -W filecount ] [ -y datalinktype ]
        [ -z postrotate-command ] [ -Z user ]
        [ --time-stamp-precision=tstamp_precision ]
        [ --micro ] [ --nano ]
        [ expression ]
```

Cosa fa l'opzione -r?

-r è utilizzata per leggere i pacchetti da un file.

Ci sono centinaia di filtri disponibili in Wireshark. Una rete di grandi dimensioni potrebbe avere numerosi filtri e molti tipi diversi di traffico. Elenca tre filtri che potrebbero essere utili a un amministratore di rete.

(ricerca per la risposta svolta tramite ai)

tcp.flags.syn == 1 and tcp.flags.ack == 0: Questo filtro permette di visualizzare i pacchetti TCP con il solo flag SYN impostato. È uno strumento per identificare scansioni di porte o tentativi di connessione non riusciti, che potrebbero indicare attività di ricognizione o attacchi.

http.request.method == "POST": Se un amministratore ha bisogno di analizzare il traffico legato all'invio di dati come moduli web questo filtro mostra solo le richieste HTTP di tipo POST, rendendo più semplice il debugging delle applicazioni web.

icmp.type == 8: Questo filtro isola specificamente i messaggi di richiesta Echo (echo request) detti anche ping . Può essere utilizzato per monitorare la latenza e la raggiungibilità degli host, o per analizzare il traffico di diagnostica

In quali altri modi di Wireshark potrebbe essere utilizzato in una rete di produzione?

S**icurezza e analisi forense:** Gli amministratori possono catturare il traffico per rilevare attività malevole, come tentativi di esfiltrazione di dati, comunicazioni con server di comando e controllo (C2) o l'uso di protocolli non autorizzati.

Debug di applicazioni: Gli sviluppatori e gli ingegneri di sistema lo utilizzano per esaminare i dettagli a livello di pacchetto delle comunicazioni tra applicazioni. Permette di verificare che le chiamate API, i protocolli personalizzati e le risposte del server funzionino correttamente, facilitando la diagnosi di errori in ambienti complessi.

Analisi delle prestazioni: Wireshark può essere utilizzato per individuare i colli di bottiglia della rete. Analizzando i pacchetti, si possono identificare problemi come elevata latenza, pacchetti persi (mostrati come retransmissions) e problemi di congestione, permettendo di ottimizzare il flusso dei dati.