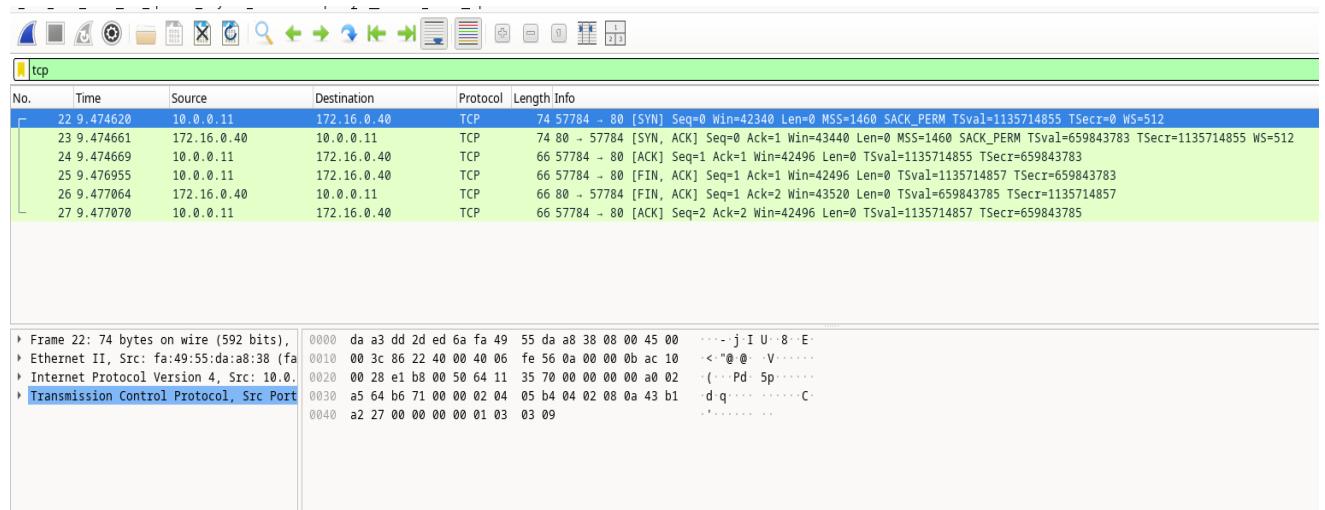


# Wireshark per osservare il 3-Way-Handshake TCP

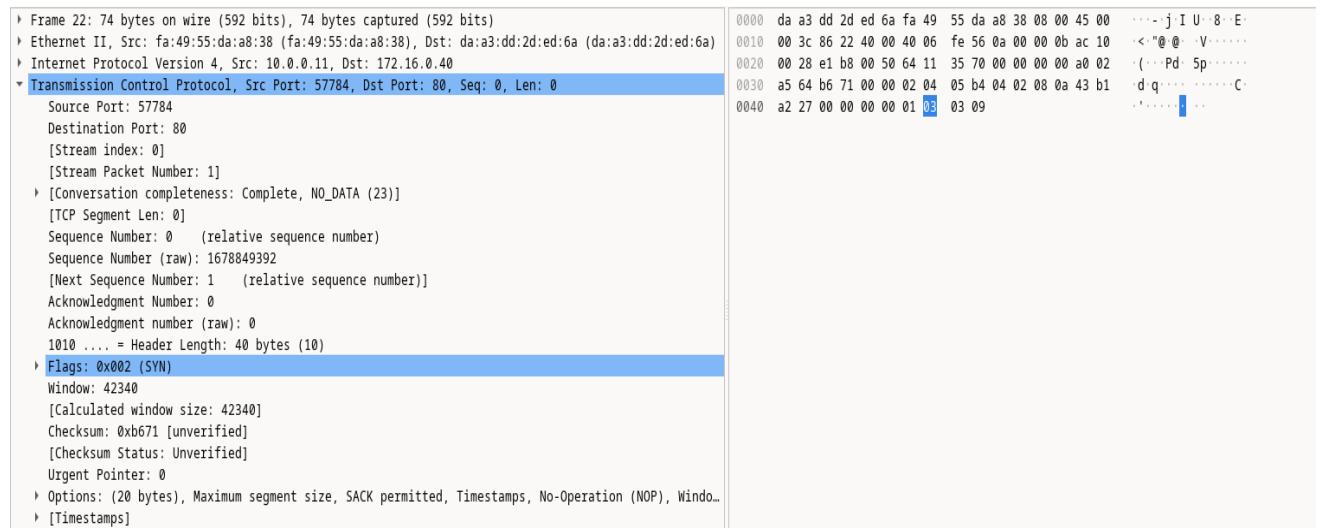
## Executive Summary

Il presente report analizza le fasi della procedura di **3-way handshake**, documentate attraverso l'utilizzo del software **Wireshark**

## Fase1 – Analisi primo pacchetto (SYN)



\*Fig.1 Risultato filtro tcp



\*Fig.2 Analisi primo pacchetto

**1)Qual è il numero di porta TCP di origine?:** 57784

**2)Come classificheresti la porta di origine?:** porta dinamica

**3)Qual è il numero di porta TCP di destinazione?:** 80

**4)Come classificheresti la porta di destinazione?:** porta servizio HTTP  
(HyperTextTransferProtocol)

**5)Quale flag è impostato?:** Syn

**6)A quale valore è impostato il numero di sequenza relativo?:** 0

---

## Fase2 – Analisi secondo pacchetto (SYN – ACK)

```
[TCP Segment Len: 0]
Sequence Number: 0      (relative sequence number)
Sequence Number (raw): 2786280250
[Next Sequence Number: 1      (relative sequence number)]
Acknowledgment Number: 1      (relative ack number)
Acknowledgment number (raw): 1678849393
1010 .... = Header Length: 40 bytes (10)
-> Flags: 0x012 (SYN, ACK)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Accurate ECN: Not set
    .... 0.... .... = Congestion Window Reduced: Not set
    .... .0... .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...1 .... = Acknowledgment: Set
    .... .... 0... .... = Push: Not set
    .... .... .0.. .... = Reset: Not set
-> .... .... .1. .... = Syn: Set
    .... .... .0 = Fin: Not set
    [TCP Flags: .....A..S.]
Window: 43440
[Calculated window size: 43440]
Checksum: 0xb671 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
-> Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Wind
-> [Timestamps]
```

\*Fig.2 Analisi secondo pacchetto

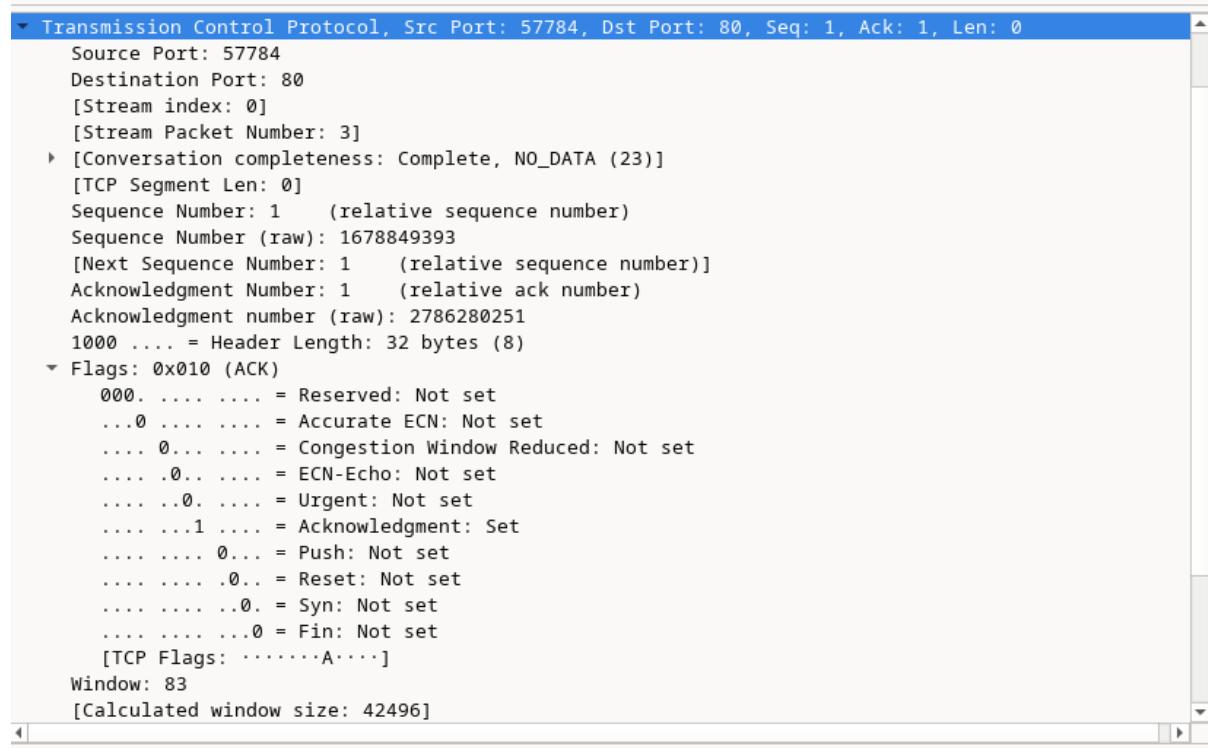
**7)Quali sono i valori delle porte di origine e destinazione? 80 (Source)  
57784 (Destination)**

**8)Quali flag sono impostati? SYN, ACK**

**9) A quali valori sono impostati i numeri relativi di sequenza e acknowledgment? (0 – SEQ) (1 - ACK)**

---

### Fase3 – Analisi terzo pacchetto (ACK)



The screenshot shows the detailed analysis of a TCP segment in Wireshark. The analysis pane displays the following information:

- Transmission Control Protocol, Src Port: 57784, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
- Source Port: 57784
- Destination Port: 80
- [Stream index: 0]
- [Stream Packet Number: 3]
- [Conversation completeness: Complete, NO\_DATA (23)]
- [TCP Segment Len: 0]
- Sequence Number: 1 (relative sequence number)
- Sequence Number (raw): 1678849393
- [Next Sequence Number: 1 (relative sequence number)]
- Acknowledgment Number: 1 (relative ack number)
- Acknowledgment number (raw): 2786280251
- 1000 .... = Header Length: 32 bytes (8)
- Flags: 0x010 (ACK)
  - 000. .... .... = Reserved: Not set
  - ...0 .... .... = Accurate ECN: Not set
  - .... 0.... .... = Congestion Window Reduced: Not set
  - .... .0.... .... = ECN-Echo: Not set
  - .... ..0.... .... = Urgent: Not set
  - .... ...1 .... = Acknowledgment: Set
  - .... .... 0.... = Push: Not set
  - .... .... .0... = Reset: Not set
  - .... .... ..0. = Syn: Not set
  - .... .... ...0 = Fin: Not set
- [TCP Flags: .....A....]
- Window: 83
- [Calculated window size: 42496]

\*Fig.3 Analisi terzo pacchetto

**10) Quale flag è impostato? ACK**

---

### Fase4 - Tcpdump

```

TCPDUMP(1)                               General Commands Manual                TCPDUMP(1)

NAME
    tcpdump - dump traffic on a network

SYNOPSIS
    tcpdump [ -AbdDefhHIJKLnNOpqStuUvxX# ] [ -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 ]

```

\*Fig.4 Lista comandi *tcpdump*

### 11)Cosa fa l'opzione -r?

L'opzione –r permette di legger pacchetti da un file di cattura.

## Altre domande

11)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. ---

- **DNS:** per filtrare solo le richieste di risoluzione dei nomi
- **ARP:** per filtrare le richieste che i dispositivi inviano per trovarsi all'interno della rete.
- **Ip.addr:** per filtrare esclusivamente il traffico relativo a uno specifico indirizzo IP.

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

- **Per la risoluzione delle prestazioni della rete**
- **Per individuare in tempo reale tentativi di intrusione o attacchi diretti ai server aziendali**
- **Per vedere codici di errore o database che non rispondono correttamente**

---

## Conclusione

Il report ha analizzato i pacchetti di un tipico **3-way handshake** tramite **Wireshark**, confermando l'efficacia di questo strumento per il monitoraggio delle reti in ambito aziendale.