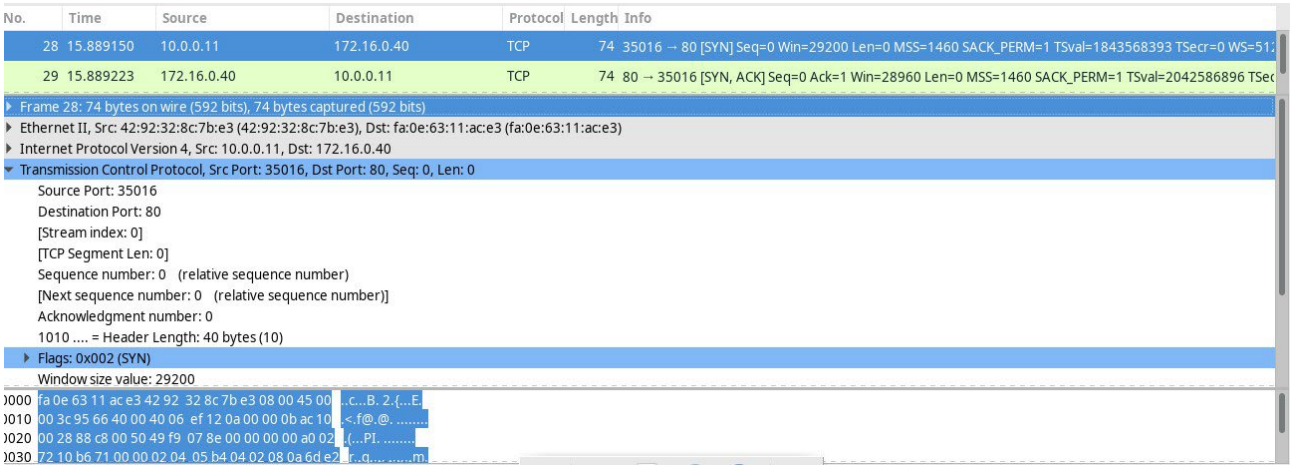
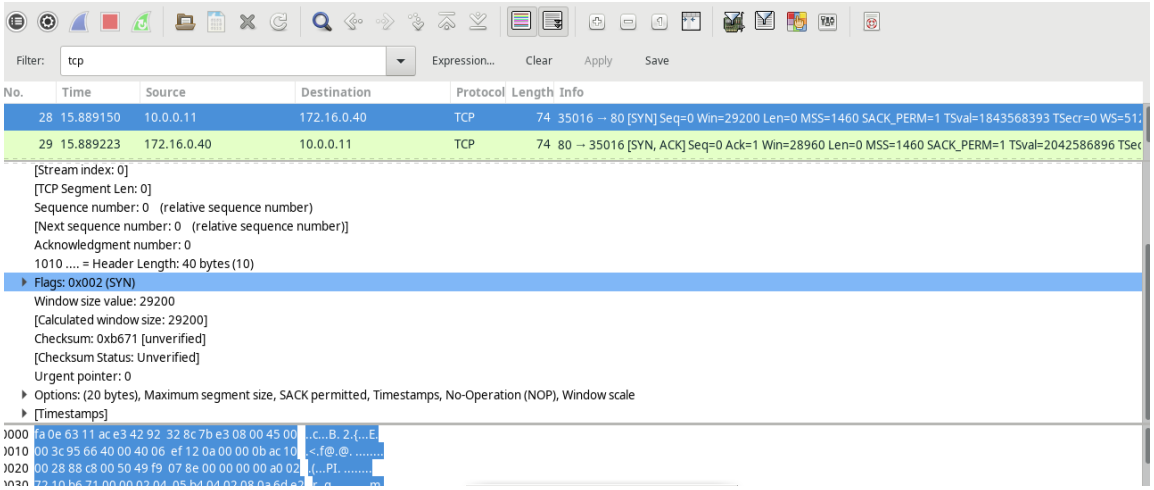




Domande:

- **Qual è il numero di porta TCP di origine?**

35016

- **Come classificheresti la porta di origine?**

Porta effimera (dynamically assigned dal client)

- **Qual è il numero di porta TCP di destinazione?**

80

- **Come classificheresti la porta di destinazione?**

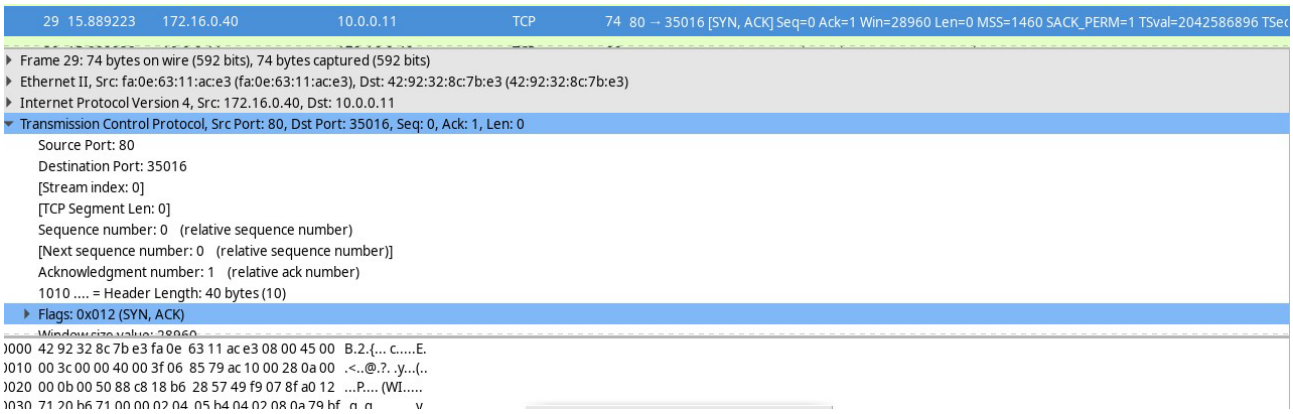
HTTP Server

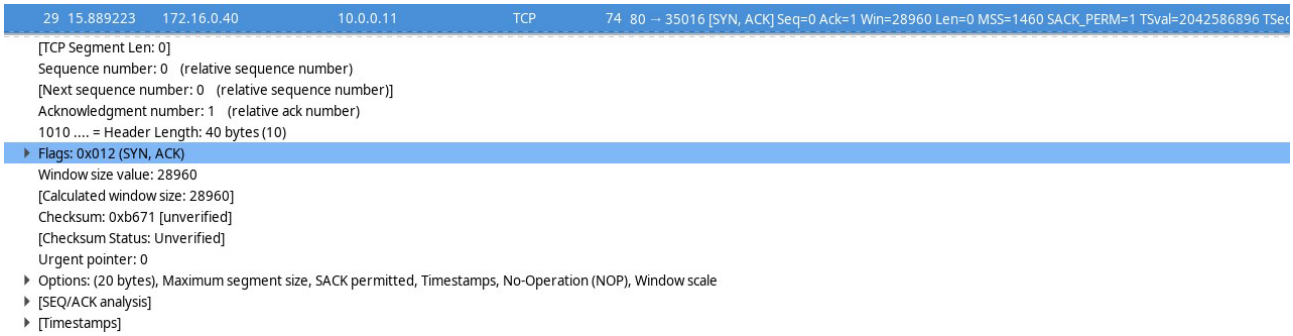
- **Quale flag è impostato?**

SYN

- **A quale valore è impostato il numero di sequenza relativo?**

0





Domande:

- **Quali sono i valori delle porte di origine e destinazione?**

Porta di origine: **80** (HTTP)

Porta di destinazione **35016** → porta effimera (client)

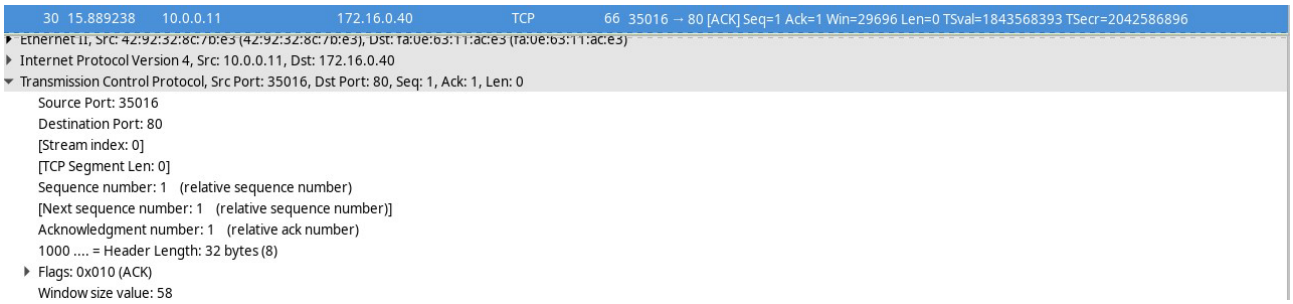
- **Quali flag sono impostati?**

SYN + ACK

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

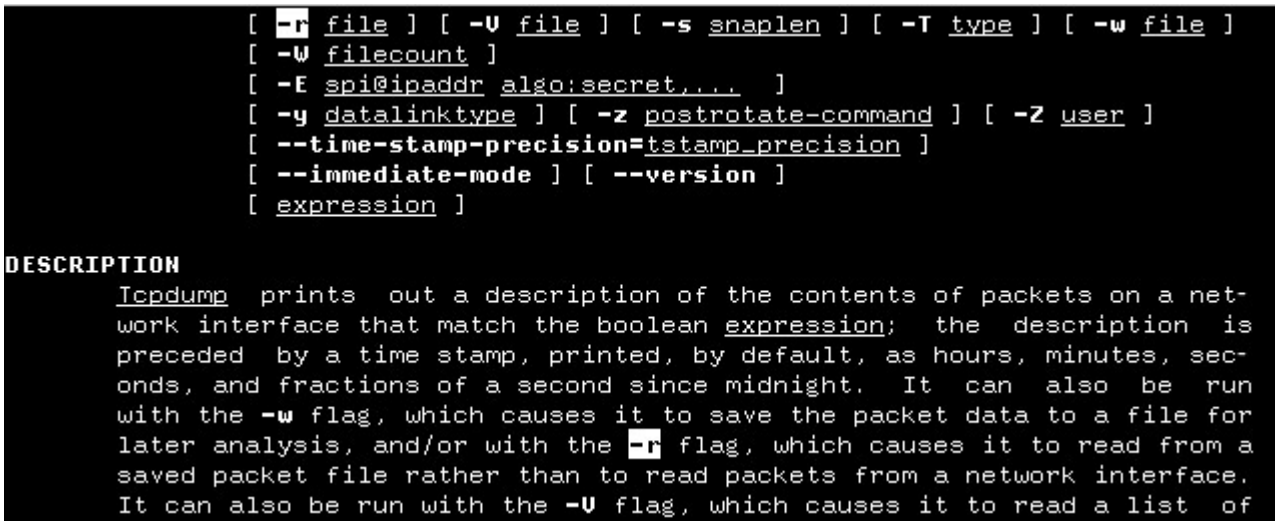
Relative Sequence Number: 0

Relative Acknowledgment Number: 1



- **Quale flag è impostato?**

ACK



- **Cosa fa l'opzione -r?**

L'opzione -r <file> in tcpdump serve a leggere i pacchetti da un file pcap invece che in tempo reale da un'interfaccia di rete.

- **Elencare tre filtri Wireshark che potrebbero essere utili a un amministratore di rete**

- ip.addr==indirizzo_ip, si possono visualizzare tutti i pacchetti che riguardano quel determinato indirizzo IP (sia come sorgente che come destinazione).
- tcp.port==numero_porta o udp.port==numero_porta, si possono visualizzare le comunicazioni che utilizzano una porta specifica.
- arp per isolare il traffico ARP e diagnosticare problemi di indirizzamento MAC/IP

- **In quali altri modi Wiresharl potrebbe essere utilizzato in una rete di produzione?**

    - Debug di applicazioni: Analizzare la comunicazione tra applicazioni e sistemi per risolvere problemi di performance o di funzionamento.
    - Rilevamento di attività sospette: Identificare traffico non autorizzato, attacchi di tipo DDoS o malware.
    - Identificazione di bottleneck: Individuare i punti critici della rete che causano rallentamenti o interruzioni.
    - Integrato in ambienti di controllo (usando dump su file o interfacce virtuali) per avere alert automatici su pattern di traffico anomalo.

    - Rilevare attività sospette (es. scanning di porte, attacchi ARP spoofing, tentativi di exploit), estrarre file trasferiti, o ricostruire sessioni dopo un incidente.