

| No. | Time | Source | Destination | Protocol | Length | Info |
|--|---|-------------|-------------|----------|--------|--|
| 28 | 15.889150 | 10.0.0.11 | 172.16.0.40 | TCP | 74 | 35016 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1843568393 TSecr=0 WS=512 |
| 29 | 15.889223 | 172.16.0.40 | 10.0.0.11 | TCP | 74 | 80 → 35016 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=2042586896 TSecr=1843568393 |
| ▶ Frame 28: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0 ▶ Ethernet II, Src: 42:92:32:8c:7b:e3 (42:92:32:8c:7b:e3), Dst: fa:0e:63:11:ac:e3 (fa:0e:63:11:ac:e3) ▶ Internet Protocol Version 4, Src: 10.0.0.11, Dst: 172.16.0.40 ▶ Transmission Control Protocol, Src Port: 35016, Dst Port: 80, Seq: 0, Len: 0 | | | | | | |
| Source Port: 35016 Destination Port: 80 [Stream index: 0] [TCP Segment Len: 0] Sequence number: 0 (relative sequence number) [Next sequence number: 0 (relative sequence number)] Acknowledgment number: 0 1010 = Header Length: 40 bytes (10) | | | | | | |
| ▶ Flags: 0x002 (SYN) Window size value: 29200 | | | | | | |
| 0000 | fa 0e 63 11 ac e3 42 92 32 8c 7b e3 08 00 45 00 ...C...B. 2 {...E | | | | | |
| 0010 | 00 3c 95 66 40 00 40 06 ef 12 0a 00 00 0b ac 10 ...<.f@.@..... | | | | | |
| 0020 | 00 28 88 c8 00 50 49 f9 07 8e 00 00 00 00 a0 02 {...PI. | | | | | |
| 0030 | 72 10 b6 71 00 00 02 04 05 b4 04 02 08 0a 6d e2 ...q.....m | | | | | |

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|-------------|-------------|----------|--------|--|
| 28 | 15.889150 | 10.0.0.11 | 172.16.0.40 | TCP | 74 | 35016 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1843568393 TSecr=0 WS=512 |
| 29 | 15.889223 | 172.16.0.40 | 10.0.0.11 | TCP | 74 | 80 → 35016 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=2042586896 TSecr=1843568393 |
| [Stream index: 0] [TCP Segment Len: 0] Sequence number: 0 (relative sequence number) [Next sequence number: 0 (relative sequence number)] Acknowledgment number: 0 1010 = Header Length: 40 bytes (10) | | | | | | |
| ▶ Flags: 0x002 (SYN) Window size value: 29200 [Calculated window size: 29200] Checksum: 0xb671 [unverified] [Checksum Status: Unverified] Urgent pointer: 0 Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale ▶ [Timestamps] | | | | | | |
| 0000 | fa 0e 63 11 ac e3 42 92 32 8c 7b e3 08 00 45 00 ...C...B. 2 {...E | | | | | |
| 0010 | 00 3c 95 66 40 00 40 06 ef 12 0a 00 00 0b ac 10 ...<.f@.@..... | | | | | |
| 0020 | 00 28 88 c8 00 50 49 f9 07 8e 00 00 00 00 a0 02 {...PI. | | | | | |
| 0030 | 72 10 b6 71 00 00 02 04 05 b4 04 02 08 0a 6d e2 ...q.....m | | | | | |

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

| | | | | | | |
|---|-----------|-------------|-----------|-----|----|---|
| 29 | 15.889223 | 172.16.0.40 | 10.0.0.11 | TCP | 74 | 80 → 35016 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=2042586896 TSecr=0 |
| ▶ Frame 29: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) ▶ Ethernet II, Src: fa:0e:63:11:ac:e3 (fa:0e:63:11:ac:e3), Dst: 42:92:32:8c:7b:e3 (42:92:32:8c:7b:e3) ▶ Internet Protocol Version 4, Src: 172.16.0.40, Dst: 10.0.0.11 ▼ Transmission Control Protocol, Src Port: 80, Dst Port: 35016, Seq: 0, Ack: 1, Len: 0 | | | | | | |
| Source Port: 80 Destination Port: 35016 [Stream index: 0] [TCP Segment Len: 0] Sequence number: 0 (relative sequence number) [Next sequence number: 0 (relative sequence number)] Acknowledgment number: 1 (relative ack number) 1010 = Header Length: 40 bytes (10) | | | | | | |
| ▶ Flags: 0x012 (SYN, ACK) Window size value: 28960 [Calculated window size: 28960] Checksum: 0xb671 [unverified] [Checksum Status: Unverified] Urgent pointer: 0 ▶ Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale ▶ [SEQ/ACK analysis] ▶ [Timestamps] | | | | | | |

| | | | | | | |
|--|-----------|-------------|-----------|-----|----|---|
| 29 | 15.889223 | 172.16.0.40 | 10.0.0.11 | TCP | 74 | 80 → 35016 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=2042586896 TSecr=0 |
| [TCP Segment Len: 0] Sequence number: 0 (relative sequence number) [Next sequence number: 0 (relative sequence number)] Acknowledgment number: 1 (relative ack number) 1010 = Header Length: 40 bytes (10) | | | | | | |
| ▶ Flags: 0x012 (SYN, ACK) Window size value: 28960 [Calculated window size: 28960] Checksum: 0xb671 [unverified] [Checksum Status: Unverified] Urgent pointer: 0 ▶ Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale ▶ [SEQ/ACK analysis] ▶ [Timestamps] | | | | | | |

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**

| | | | | | | |
|---|-----------|-----------|-------------|-----|----|--|
| 30 | 15.889238 | 10.0.0.11 | 172.16.0.40 | TCP | 66 | 35016 → 80 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=1843568393 TSecr=2042586896 |
| ▶ Ethernet II, Src: 42:92:32:8c:7d:e3 (42:92:32:8c:7d:e3), Dst: fa:0e:03:11:aces (fa:0e:03:11:aces) | | | | | | |
| ▶ Internet Protocol Version 4, Src: 10.0.0.11, Dst: 172.16.0.40 | | | | | | |
| ▼ Transmission Control Protocol, Src Port: 35016, Dst Port: 80, Seq: 1, Ack: 1, Len: 0 | | | | | | |
| Source Port: 35016 | | | | | | |
| Destination Port: 80 | | | | | | |
| [Stream index: 0] | | | | | | |
| [TCP Segment Len: 0] | | | | | | |
| Sequence number: 1 (relative sequence number) | | | | | | |
| [Next sequence number: 1 (relative sequence number)] | | | | | | |
| Acknowledgment number: 1 (relative ack number) | | | | | | |
| 1000 = Header Length: 32 bytes (8) | | | | | | |
| ▶ Flags: 0x010 (ACK) | | | | | | |
| Window size value: 58 | | | | | | |

- Quale flag è impostato?

ACK

```
[ -r file ] [ -U file ] [ -s snaplen ] [ -T type ] [ -w file ]
[ -W filecount ]
[ -E spi@ipaddr algo:secret,... ]
[ -y datalinktype ] [ -z postrotate-command ] [ -Z user ]
[ --time-stamp-precision=tstamp_precision ]
[ --immediate-mode ] [ --version ]
[ expression ]
```

DESCRIPTION

`Tcpdump` prints out a description of the contents of packets on a network interface that match the boolean expression; the description is preceded by a time stamp, printed, by default, as hours, minutes, seconds, and fractions of a second since midnight. It can also be run with the `-w` flag, which causes it to save the packet data to a file for later analysis, and/or with the `-r` flag, which causes it to read from a saved packet file rather than to read packets from a network interface. It can also be run with the `-U` flag, which causes it to read a list of

- 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 Wireshark 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.