

QUESITI 10.6.26

38	11.852310	10.0.0.11	172.16.0.40	TCP	74	52614 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=31837814 TSecr=0 WS=512
39	11.852342	172.16.0.40	10.0.0.11	TCP	74	80 → 52614 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=3506017726 TSecr=31837814 WS=512
40	11.852349	10.0.0.11	172.16.0.40	TCP	66	52614 → 80 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=31837814 TSecr=3506017726
41	11.852420	10.0.0.11	172.16.0.40	HTTP	377	GET / HTTP/1.1

Source Port: 52614
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)
000. = Reserved: Not set
...0 = Nonce: Not set
.... 0... = Congestion Window Reduced (CWR): Not set
.... .0. = ECN-Echo: Not set
.....0. = Urgent: Not set
.....0 = Acknowledgment: Not set
..... 0... = Push: Not set
..... .0.. = Reset: Not set
▼ 1. = Syn: Set
► [Expert Info (Chat/Sequence): Connection establish request (SYN): server port 80]
..... 0.. = Fin: Not set

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

La porta TCP di origine è la 52614.

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

I numeri di porta dell'intervallo 49152-65535 appartengono a porte private o dinamiche e non sono utilizzati da una applicazione in particolare.

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

La porta di destinazione è la 80.

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

Generalmente la porta 80 appartiene all'HTTP.

- **Quale flag è impostato?**

E' impostato il flag SYN.

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

Il valore del numero di sequenza relativo è impostato a 0.

38	11.852310	10.0.0.11	172.16.0.40	TCP	74	52614 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=31837814 TSecr=0 WS=512
39	11.852342	172.16.0.40	10.0.0.11	TCP	74	80 → 52614 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=3506017726 TSecr=31837814 WS=512
40	11.852349	10.0.0.11	172.16.0.40	TCP	66	52614 → 80 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=31837814 TSecr=3506017726
41	11.852420	10.0.0.11	172.16.0.40	HTTP	377	GET / HTTP/1.1

Transmission Control Protocol, Src Port: 80, Dst Port: 52614, Seq: 0, Ack: 1, Len: 0
Source Port: 80
Destination Port: 52614
[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)
000. = Reserved: Not set
...0 = Nonce: Not set
.... 0... = Congestion Window Reduced (CWR): 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

• Quali sono i valori delle porte di origine e destinazione?

La porta di origine ha come valore 80 mentre quella di destinazione 52614

• Quali flag sono impostati?

E' impostato il flag "Acknowledge" e il flag "SYN".

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

Il numero di sequenza relativo è impostato a 0. Mentre il numero di sequenza relativo dell'acknowledge è impostato a 1.

38	11.852310	10.0.0.11	172.16.0.40	TCP	74	52614 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=31837814 TSecr=0 WS=512
39	11.852342	172.16.0.40	10.0.0.11	TCP	74	80 → 52614 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=3506017726 TSecr=31837814 WS=512
40	11.852349	10.0.0.11	172.16.0.40	TCP	66	52614 → 80 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=31837814 TSecr=3506017726
41	11.852420	10.0.0.11	172.16.0.40	HTTP	377	GET / HTTP/1.1

[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)
000. = Reserved: Not set
...0 = Nonce: Not set
.... 0... = Congestion Window Reduced (CWR): 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....]

• Quale flag è impostato?

E' impostato il flag acknowledge.

1. 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.

A seguire tre filtri che potrebbero essere particolarmente utili per un amministratore di rete in Wireshark:

1) ip.addr == X.X.X.X: Questo filtro consente a un amministratore di isolare tutto il traffico da o verso un indirizzo IP specifico. È utile per:

- Risolvere problemi di connettività per un host particolare;
- Monitorare l'attività di un server o una workstation specifici;
- Indagare su traffico sospetto proveniente da o destinato a un indirizzo IP noto;
- Sostituire X.X.X.X con l'indirizzo IP effettivo.

2) tcp.port == YYYY o udp.port == YYYY: Questi filtri consentono ad un amministratore di concentrarsi sul traffico relativo a una porta TCP o UDP specifica. Questo è utile per:

- Analizzare il traffico specifico dell'applicazione (es. tcp.port == 80 per HTTP, tcp.port == 443 per HTTPS, udp.port == 53 per DNS);
- Identificare se un servizio è in ascolto o risponde sulla sua porta prevista;
- Risolvere problemi di regole del firewall che potrebbero bloccare servizi specifici;
- Sostituire YYYY con il numero di porta effettivo.

3) http o dns o smb (o qualsiasi altro filtro di protocollo comune): Wireshark dispone di una vasta gamma di filtri per protocolli di alto livello. Concentrarsi su un protocollo specifico aiuta gli amministratori a:

- Analizzare il comportamento di una particolare applicazione o servizio;
- Risolvere problemi relativi a un protocollo specifico (es. caricamento lento delle pagine web usando http, problemi di risoluzione DNS usando dns);
- Ottenere informazioni sui modelli di comunicazione di diversi servizi di rete

Questi filtri sono spesso combinati con altri filtri (es. http and ip.addr == 192.168.1.100).

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

Wireshark in produzione serve principalmente per risolvere problemi di rete (performance, connettività), rafforzare la sicurezza (individuare attacchi, attività anomale) e per analisi forensi post-incidente, fornendo una visione dettagliata del traffico a livello di pacchetto. In sintesi, Wireshark offre una visibilità profonda a livello di pacchetto, rendendolo uno strumento versatile per mantenere la rete performante, stabile e sicura.