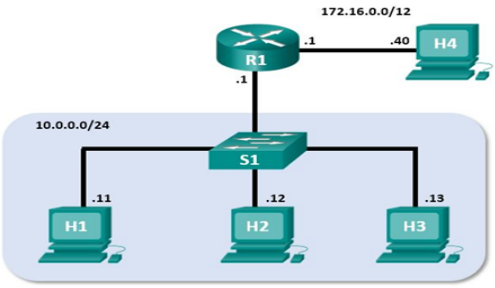
ESERCIZIO W11L2

Usare Wireshark per Osservare l'Handshake a 3 Vie TCP

Topologia Mininet



Risorse Richieste: Macchina virtuale CyberOps Workstation

Obiettivi

- **Parte 1: Preparare gli Host per Catturare il Traffico**
- **Parte 2: Analizzare i Pacchetti usando Wireshark**
- **Parte 3: Visualizzare i Pacchetti usando tcpdump**

Contesto / Scenario

In questo laboratorio, userai Wireshark per catturare ed esaminare i pacchetti generati tra il browser del PC che utilizza il protocollo HTTP (HyperText Transfer Protocol) e un server web, come www.google.com. Quando un'applicazione, come HTTP o FTP (File Transfer Protocol), si avvia per la prima volta su un host, TCP utilizza l'handshake a tre vie per stabilire una sessione TCP affidabile tra i due host. Ad esempio, quando un PC utilizza un browser web per navigare in internet, viene avviato un handshake a tre vie e viene stabilita una sessione tra l'host del PC e il server web. Un PC può avere più sessioni TCP attive simultaneamente con vari siti web.

3

ISTRUZIONI

Parte 1: Preparare gli Host per Catturare il Traffico

a. Avviare la VM CyberOps. Accedere con nome utente analyst e password cyberops.

b. Avviare Mininet.

```
[analyst@secOps ~]$ sudo lab.support.files/scripts/cyberops_topo.py
```

c. Avviare gli host H1 e H4 in Mininet.

```
*** Starting CLI:
    mininet> xterm H1
    mininet> xterm H4
```

d. Avviare il server web su H4.

```
[root@secOps analyst]# /home/analyst/lab.support.files/scripts/reg_server_start.sh
```

4

e. Per motivi di sicurezza, non è possibile eseguire Firefox dall'account utente root. Sull'host H1, usare il comando `su` (switch user) per passare dall'utente root all'account utente analyst:

```
[root@secOps analyst]# su analyst
```

f. Avviare il browser web su H1. Ci vorrà qualche momento.

```
[analyst@secOps ~]$ firefox &
```

g. Dopo l'apertura della finestra di Firefox, avviare una sessione `tcpdump` nel terminale Node: H1 e inviare l'output a un file chiamato capture.pcap. Con l'opzione `-v`, è possibile osservare l'avanzamento. Questa cattura si fermerà dopo aver catturato 50 pacchetti, poiché è configurata con l'opzione `-c 50`.

```
[analyst@secOps ~]$ sudo tcpdump -i H1-eth0 -v -c 50 -w /home/analyst/capture.pcap
```

h. Dopo l'avvio di `tcpdump`, navigare rapidamente a 172.16.0.40 nel browser web Firefox.

5

Parte 2: Analizzare i Pacchetti usando Wireshark

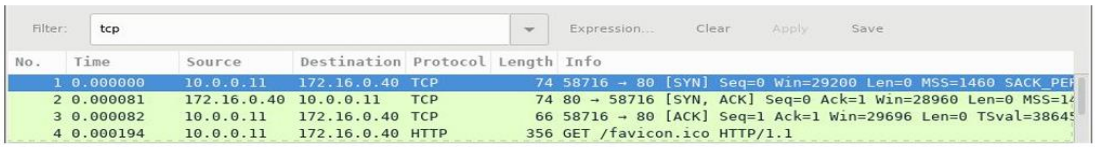
Passo 1: Applicare un filtro alla cattura salvata.

a. Premere INVIO per vedere il prompt. Avviare Wireshark su Node: H1. Fare clic su OK quando viene richiesto l'avviso riguardante l'esecuzione di Wireshark come superutente.

```
[analyst@secOps ~]$ wireshark-gtk &
```

b. In Wireshark, fare clic su File > Open. Selezionare il file pcap salvato situato in /home/analyst/capture.pcap.

c. Applicare un filtro tcp alla cattura. In questo esempio, i primi 3 frame rappresentano il traffico di interesse.

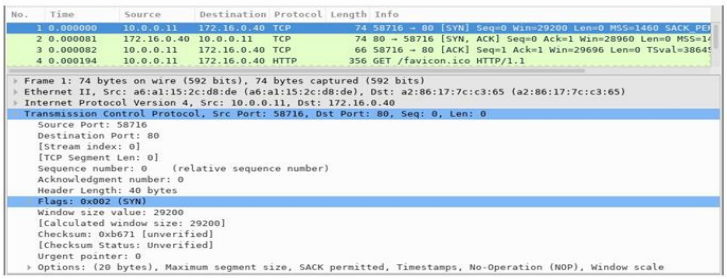


Passo 2: Esaminare le informazioni all'interno dei pacchetti, inclusi indirizzi IP, numeri di porta TCP e flag di controllo TCP.

a. In questo esempio, il frame 1 è l'inizio dell'handshake a tre vie tra il PC e il server su H4. Nel riquadro dell'elenco dei pacchetti (sezione superiore della finestra principale), selezionare il primo pacchetto, se necessario.

b. Fare clic sulla freccia a sinistra del Transmission Control Protocol nel riquadro dei dettagli del pacchetto per espanderlo ed esaminare le informazioni TCP. Localizzare le informazioni sulla porta di origine e destinazione.

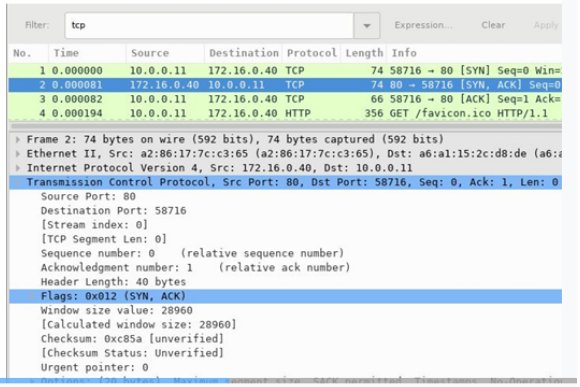
c. Fare clic sulla freccia a sinistra dei Flags. Un valore di 1 significa che il flag è impostato. Localizzare il flag impostato in questo pacchetto.



Nota: Potrebbe essere necessario regolare le dimensioni delle finestre superiore e centrale all'interno di Wireshark per visualizzare le informazioni necessarie.

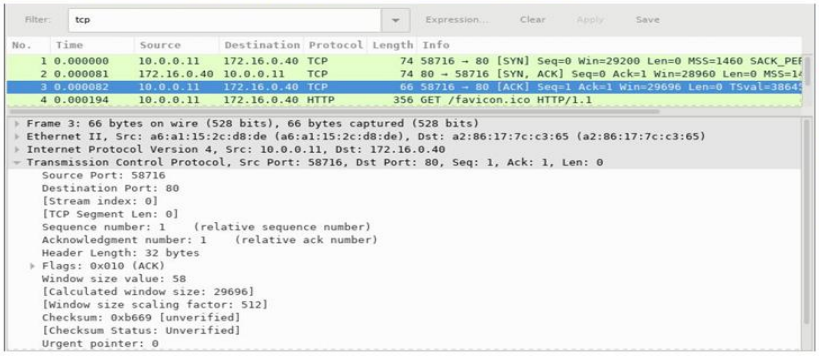
- **Qual è il numero di porta TCP di origine?**
- **Come classificheresti la porta di origine?**
- **Qual è il numero di porta TCP di destinazione?**
- **Come classificheresti la porta di destinazione?**
- **Quale flag è impostato?**
- **A quale valore è impostato il numero di sequenza relativo?**

d. Selezionare il pacchetto successivo nell'handshake a tre vie. In questo esempio, è il frame 2. Questa è la risposta del server web alla richiesta iniziale di avviare una sessione.



- **Quali sono i valori delle porte di origine e destinazione?**
- **Quali flag sono impostati?**
- **A quali valori sono impostati i numeri relativi di sequenza e acknowledgment?**

e. Infine, selezionare il terzo pacchetto nell'handshake a tre vie.



Esaminare il terzo e ultimo pacchetto dell'handshake.

Quale flag è impostato?

I numeri relativi di sequenza e acknowledgment sono impostati a 1 come punto di partenza. La connessione TCP è stabilita e la comunicazione tra il computer di origine e il server web può iniziare.

Parte 3: Visualizzare i pacchetti usando tcpdump

È anche possibile visualizzare il file pcap e filtrare per le informazioni desiderate.

a. Aprire una nuova finestra di terminale, inserire man tcpdump. Nota: Potrebbe essere necessario premere INVIO per vedere il prompt.

Utilizzando le pagine manuale (man pages) disponibili con il sistema operativo Linux, è possibile leggere o cercare tra le pagine manuale le opzioni per selezionare le informazioni desiderate dal file pcap.

```
[analyst@secOps ~]$ man tcpdump
  TCPDUMP(1)                General Commands Manual                TCPDUMP(1)

  NAME
         tcpdump - dump traffic on a network

  SYNOPSIS
         tcpdump [ -AbdDefhHIJKlLnNOpqStuUvxX# ] [ -B buffer_size ]
                 [ -c count ]
                 [ -C file_size ] [ -G rotate_seconds ] [ -F file ]
                 [ -i interface ] [ -j tstamp_type ] [ -m module ] [ -M secret ]
                 [ --number ] [ -Q in|out|inout ]
                 [ -r file ] [ -V 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 ]
  <output omesso>
```

Per cercare nelle pagine man, è possibile usare / (ricerca in avanti) o ? (ricerca indietro) per trovare termini specifici, n per passare alla corrispondenza successiva e q per uscire. Ad esempio, per cercare informazioni sull'opzione -r, digitare /-r. Digitare n per passare alla corrispondenza successiva.

Cosa fa l'opzione -r?

b. Nello stesso terminale, aprire il file di cattura usando il seguente comando per visualizzare i primi 3 pacchetti TCP catturati:

```
[analyst@secOps ~]$ tcpdump -r /home/analyst/capture.pcap tcp -c 3
reading from file capture.pcap, link-type EN10MB (Ethernet)
13:58:30.647462 IP 10.0.0.11.58716 > 172.16.0.40.http: Flags [S], seq 2432755549, win 29200, options [mss 1460,sackOK,TS val 3864513189 ecr 0,nop,wscale 9], length 0
13:58:30.647543 IP 172.16.0.40.http > 10.0.0.11.58716: Flags [S.], seq 1766419191, ack 2432755550, win 28960, options [mss 1460,sackOK,TS val 50557410 ecr 3864513189,nop,wscale 9], length 0
13:58:30.647544 IP 10.0.0.11.58716 > 172.16.0.40.http: Flags [.], ack 1, win 58, options [nop,nop,TS val 3864513189 ecr 50557410], length 0
```

Per visualizzare l'handshake a 3 vie, potrebbe essere necessario aumentare il numero di righe dopo l'opzione -c.

c. Navigare al terminale usato per avviare Mininet. Terminare Mininet inserendo quit nella finestra principale del terminale della VM CyberOps.

```
mininet> quit
  *** Stopping 0 controllers

  *** Stopping 2 terms
  *** Stopping 5 links
  .....
  *** Stopping 1 switches
  s1
  *** Stopping 5 hosts
  H1 H2 H3 H4 R1
  *** Done
  [analyst@secOps ~]$
```

d. Dopo aver chiuso Mininet, inserire sudo mn -c per pulire i processi avviati da Mininet. Inserire la password cyberops quando richiesto.

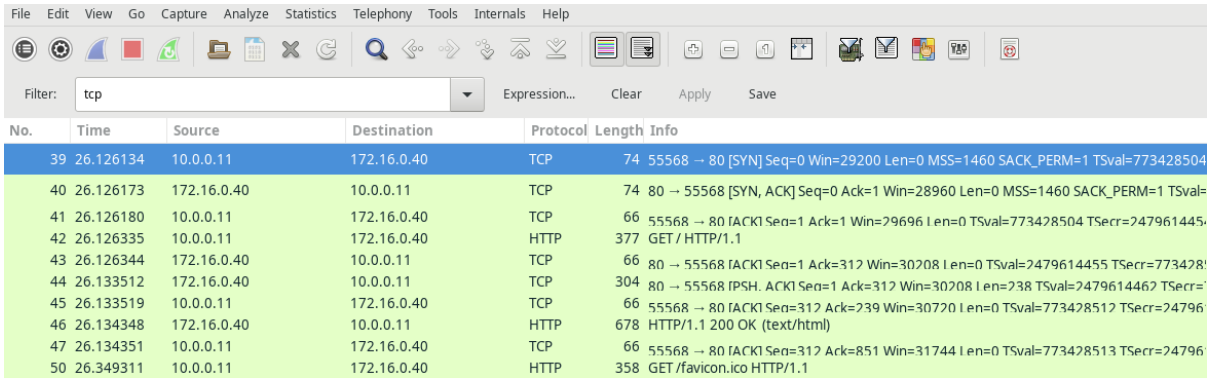
```
[analyst@secOps ~]$ sudo mn -c
 [sudo] password for analyst:
```

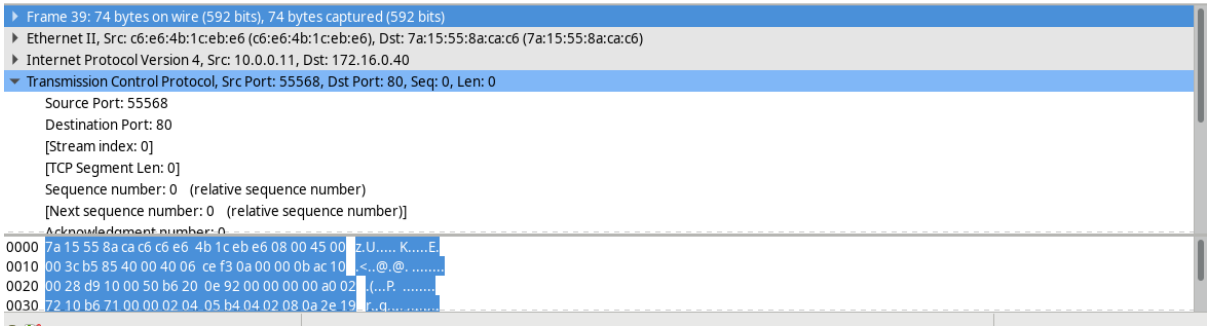
Domande di Riflessione

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.

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

Qual è il numero di porta TCP di origine? 55568





Come classificheresti la porta di origine?

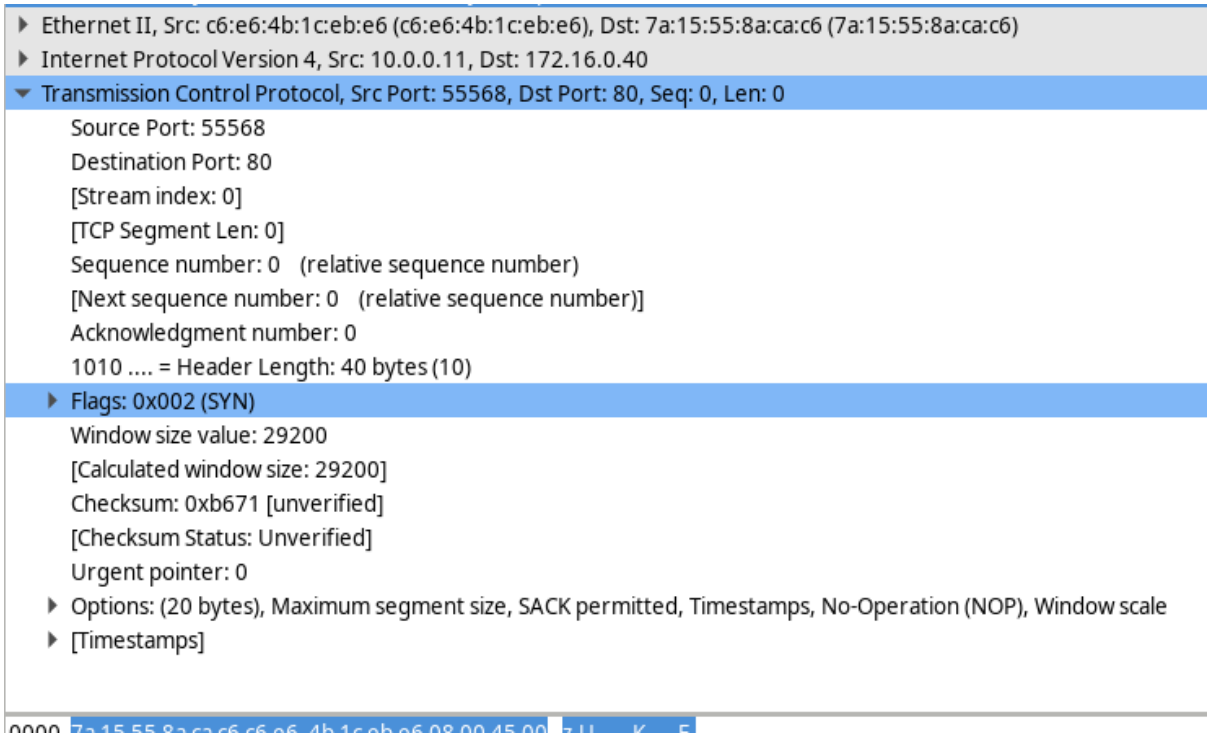
- Le porte **effimere(49152-65535)** vengono usate dai client quando avviano una connessione verso un server (es. navigazione web, SSH, ecc.).
- **Non sono legate a servizi specifici**, quindi per sapere con certezza cosa sta usando la porta 55568, bisogna **analizzare il traffico di rete** o **verificare i processi in esecuzione**.

Qual è il numero di porta TCP di destinazione? 80

Come classificheresti la porta di destinazione?

- Porta well known
- La porta **80/TCP** è usata dai server web per gestire richieste HTTP.
- È la porta predefinita per la **navigazione web senza cifratura** (HTTP), a differenza della porta **443**, che è usata per HTTPS (HTTP su TLS/SSL).
- Quando digiti un indirizzo come `http://example.com`, il browser comunica con il server sulla porta 80.

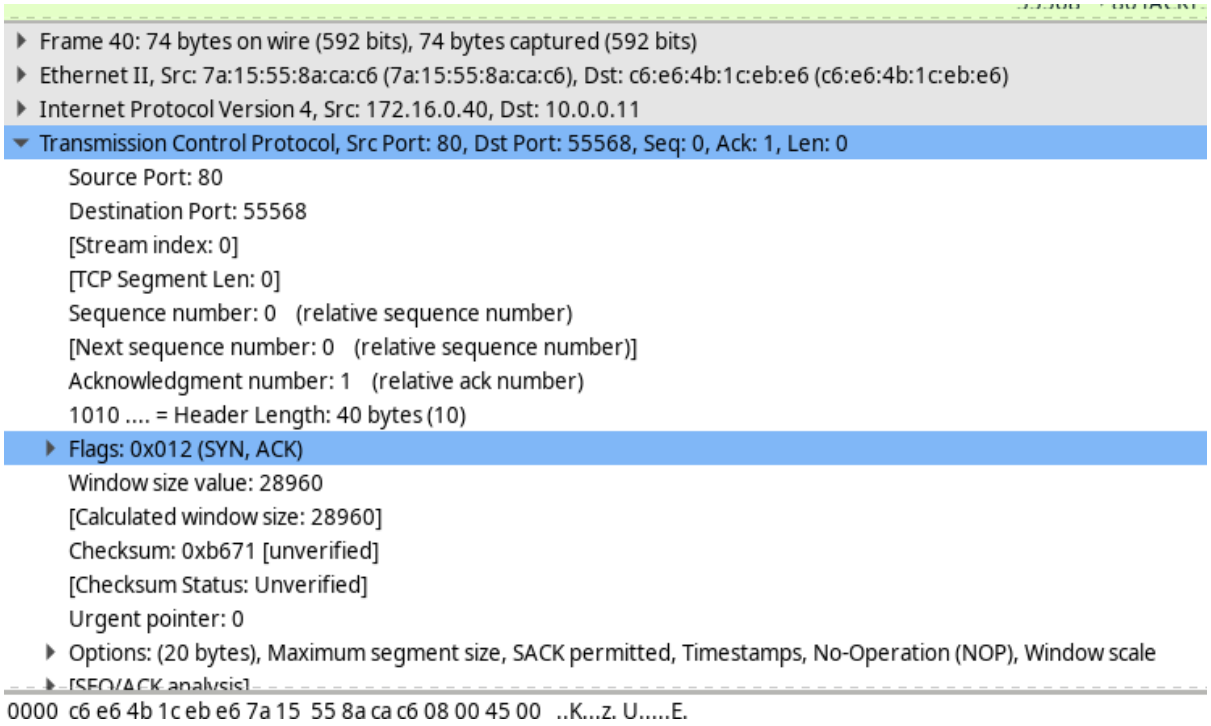
Quale flag è impostato? 0x002 (SYN)



A quale valore è impostato il numero di sequenza relativo? 0

Quali sono i valori delle porte di origine e destinazione?

80 origine, 55568 destinazione

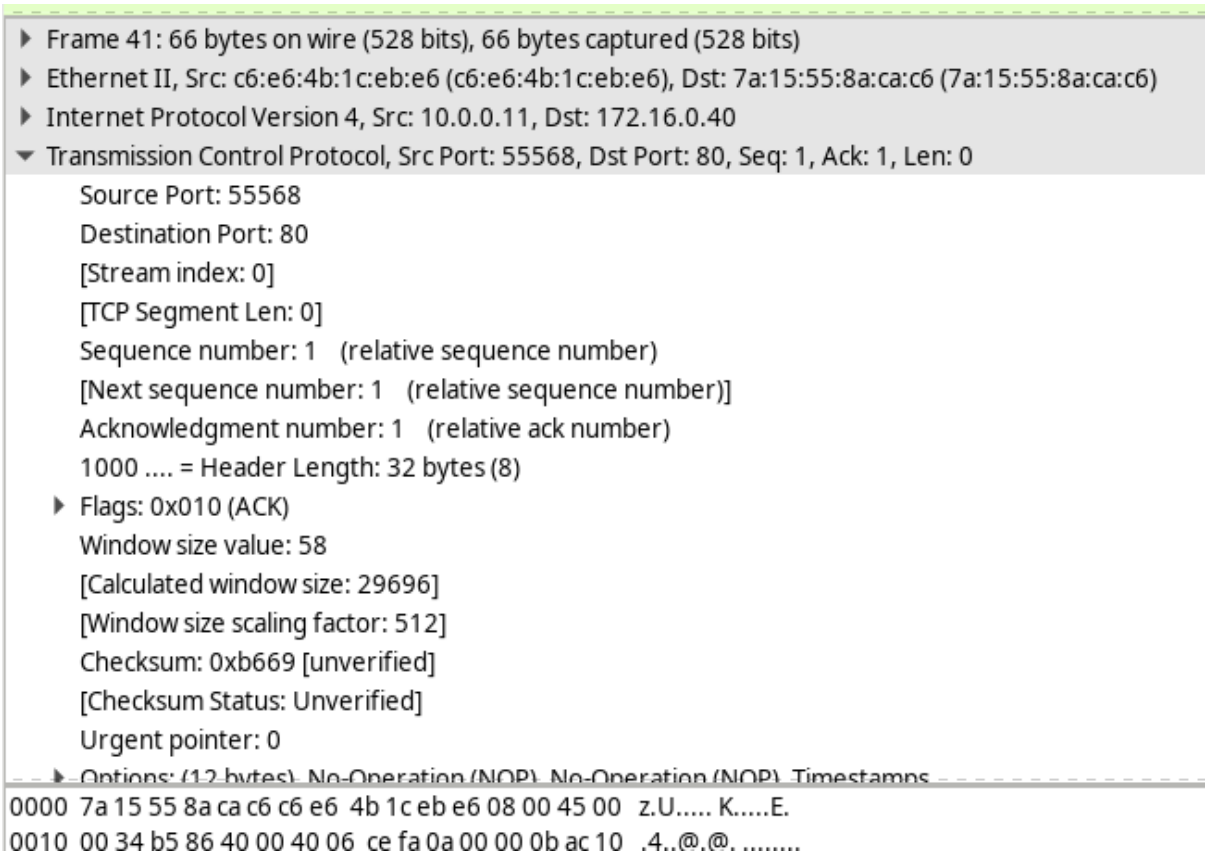


Quali flag sono impostati? 0x012 (SYN ACK)

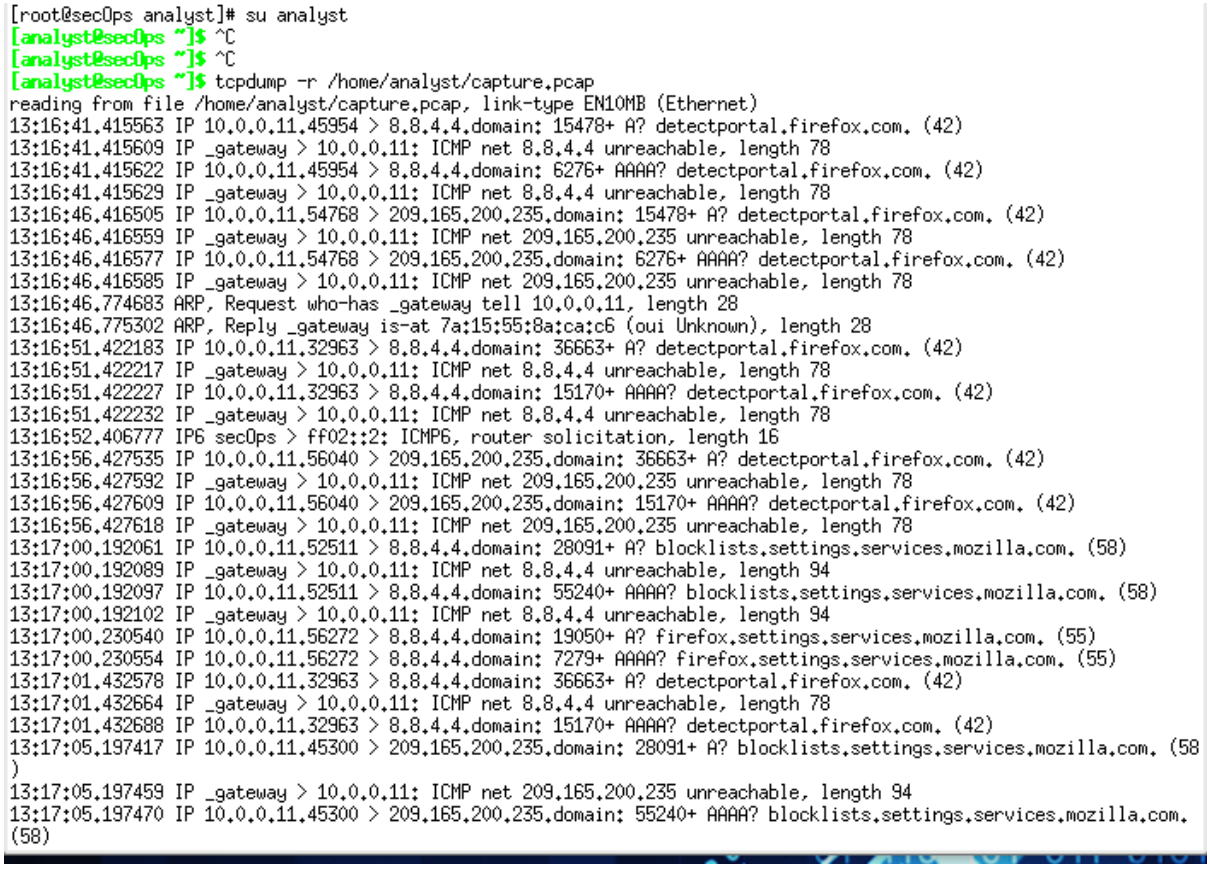
A quali valori sono impostati i numeri relativi di sequenza e acknowledgment?

0 1

Quale flag è impostato (terzo pacchetto)? 0x010 (ACK)



Cosa fa l opzione –r?



Legge i pacchetti da un **file pcap** (anziché dalla rete in tempo reale).

- Quando usi `-r`, **tcpdump non ascolta la rete**, ma apre un file `.pcap` già esistente (registrato ad esempio con `tcpdump -w` o con Wireshark/tshark).
- Viene spesso usata per analizzare pacchetti dopo averli catturati.

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.

- Filtro per un protocollo specifico

  Per visualizzare solo il traffico HTTP: `http`
  Utile per: monitorare il traffico web in chiaro, identificare richieste sospette, troubleshooting di applicazioni web.

- **Filtro per indirizzo IP specifico**

  Per visualizzare solo il traffico da o verso un IP (esempio: 192.168.1.10):
  ip.addr == 192.168.1.10
  Utile per: isolare il traffico di un singolo host (es. un server, un PC compromesso, un dispositivo IoT).

- Filtro per una porta specifica

  Per monitorare il traffico sulla porta HTTPS (443):

tcp.port == 443
Utile per: verificare se il traffico cifrato funziona correttamente, controllare il volume di traffico TLS/SSL.

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

Wireshark, in una **rete di produzione**, è uno strumento potentissimo — non solo per "sniffare pacchetti", ma anche per diagnosticare, ottimizzare e proteggere la rete.

Ecco alcuni **usi concreti** che un amministratore di rete o un analista può fare in produzione:

Risoluzione dei problemi (troubleshooting)

- Diagnosi di problemi di connettività (perché un client non riesce a raggiungere un server?).
- Identificazione di latenze elevate (ping elevati, handshake lenti).
- Analisi di problemi DNS (DNS lento o risposte errate).
- Verifica di problemi di handshake TLS/SSL.

Analisi delle prestazioni della rete

- Misurazione del throughput effettivo tra client e server.
- Rilevamento di collo di bottiglia in alcune tratte della rete.
- Controllo di retrasmissioni TCP (segno di problemi fisici o saturazione della banda).

Monitoraggio della sicurezza

- Identificazione di traffico sospetto (esfiltrazione dati, scansioni di rete).
- Cattura e analisi di tentativi di attacco (esempio: exploit HTTP, attacchi ARP spoofing, anomalie DNS).
- Analisi forense post-incident response (cosa ha fatto un malware? quali connessioni ha aperto?).
- Controllo della compliance (è presente traffico non cifrato su servizi che dovrebbero essere cifrati?).

Documentazione e analisi storica

- Generazione di report dettagliati sul traffico di rete.
- Cattura di sessioni specifiche per audit o per verificare il rispetto delle policy aziendali.

Supporto allo sviluppo

- Analisi e debug di applicazioni in sviluppo che comunicano sulla rete.

- Verifica della correttezza dei protocolli implementati.
- Misurazione dei tempi di risposta applicativi.