

# CISCO Cyber ops 2

## Obiettivi del laboratorio:

1. Preparare gli host per catturare il traffico.
2. Analizzare i pacchetti utilizzando Wireshark.
3. Visualizzare i pacchetti utilizzando tcpdump.

## Parte 1: Preparare gli host per catturare il traffico

1. **Avviare la VM CyberOps**
  - Accesso effettuato con l'utente analyst e password cyberops.
2. **Avvio di Mininet**
  - Comando eseguito:
  - `sudo lab.support.files/scripts/cyberops_topo.py`
3. **Avviare gli host H1 e H4 in Mininet**
  - Comandi eseguiti nella CLI di Mininet:
  - `xterm H1`
  - `xterm H4`
4. **Avvio del server web su H4**
  - Comando eseguito:
  - `/home/analyst/lab.support.files/scripts/reg_server_start.sh`
5. **Passare dall'utente root all'utente analyst su H1**
  - Comando eseguito:
  - `su analyst`
6. **Avviare Firefox su H1**
  - Comando eseguito:
  - `firefox &`
7. **Catturare il traffico con tcpdump**
  - Comando eseguito su H1:
  - `sudo tcpdump -i H1-eth0 -v -c 50 -w /home/analyst/capture.pcap`
  - Durante la cattura, si è acceduto all'indirizzo 172.16.0.40 tramite Firefox su H1.

## Parte 2: Analizzare i pacchetti utilizzando Wireshark

1. **Avvio di Wireshark su H1**
  - Comando eseguito:
  - `wireshark &`
2. **Apertura del file pcap**
  - Percorso del file: `/home/analyst/capture.pcap`.
  - File aperto tramite **File > Open** in Wireshark.
3. **Applicazione di un filtro TCP**
  - Filtro applicato:
  - `tcp`

#### 4. Esame dei pacchetti (stretta di mano TCP a tre vie)

- **Frame 1:** Inizio della stretta di mano (SYN inviato).
  - Porta sorgente: **34020** (dinamico/privato).
  - Porta destinazione: **80** (noto, HTTP).
  - Flag impostato: **SYN**.
  - Numero di sequenza relativo: **0**.

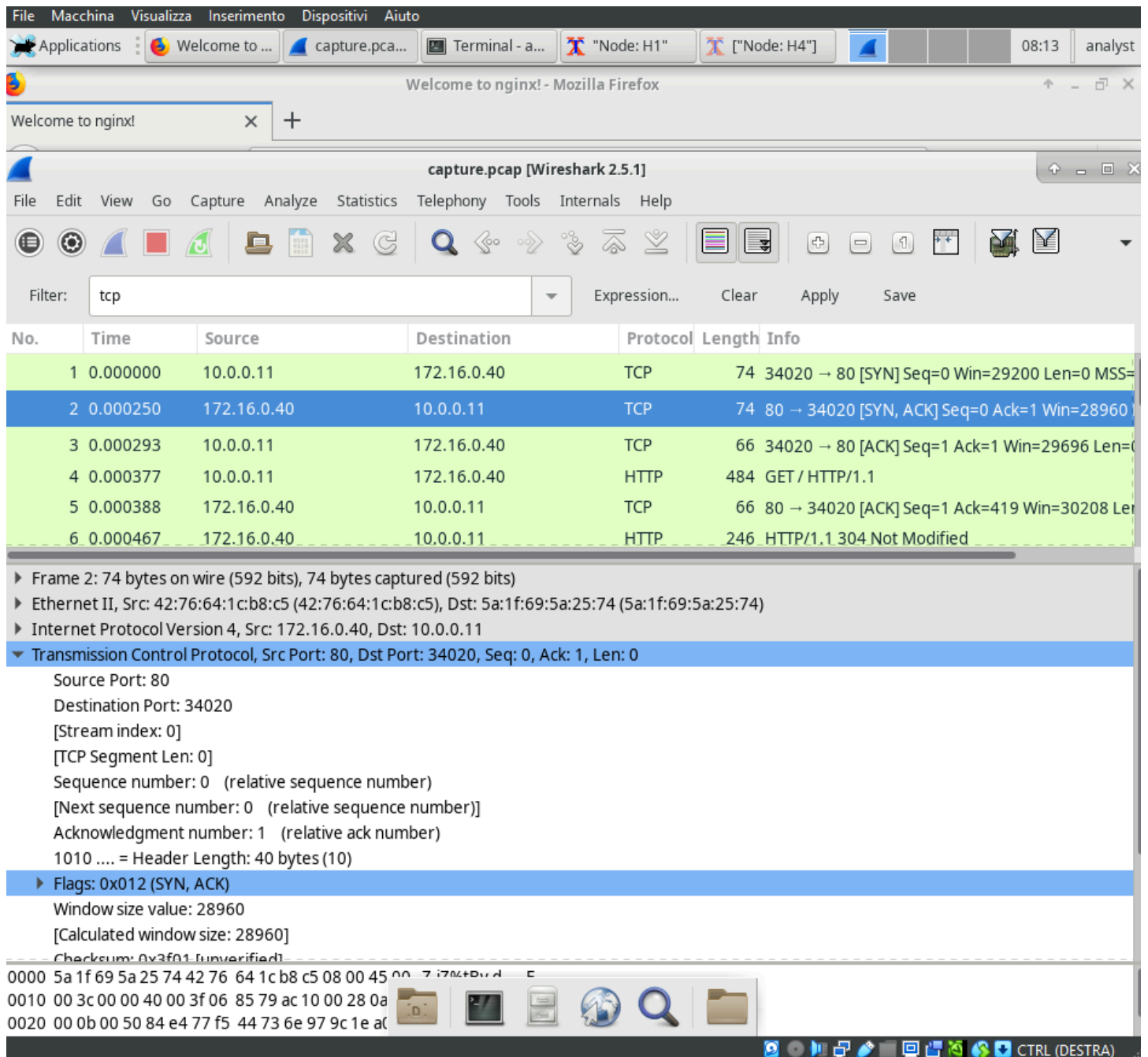
The screenshot shows the Wireshark 2.5.1 interface. The packet list at the top shows the following frames:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.11	172.16.0.40	TCP	74	34020 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=
2	0.000250	172.16.0.40	10.0.0.11	TCP	74	80 → 34020 [SYN, ACK] Seq=0 Ack=1 Win=28960
3	0.000293	10.0.0.11	172.16.0.40	TCP	66	34020 → 80 [ACK] Seq=1 Ack=1 Win=29696 Len=0
4	0.000377	10.0.0.11	172.16.0.40	HTTP	484	GET / HTTP/1.1
5	0.000388	172.16.0.40	10.0.0.11	TCP	66	80 → 34020 [ACK] Seq=1 Ack=419 Win=30208 Len
6	0.000467	172.16.0.40	10.0.0.11	HTTP	246	HTTP/1.1 304 Not Modified

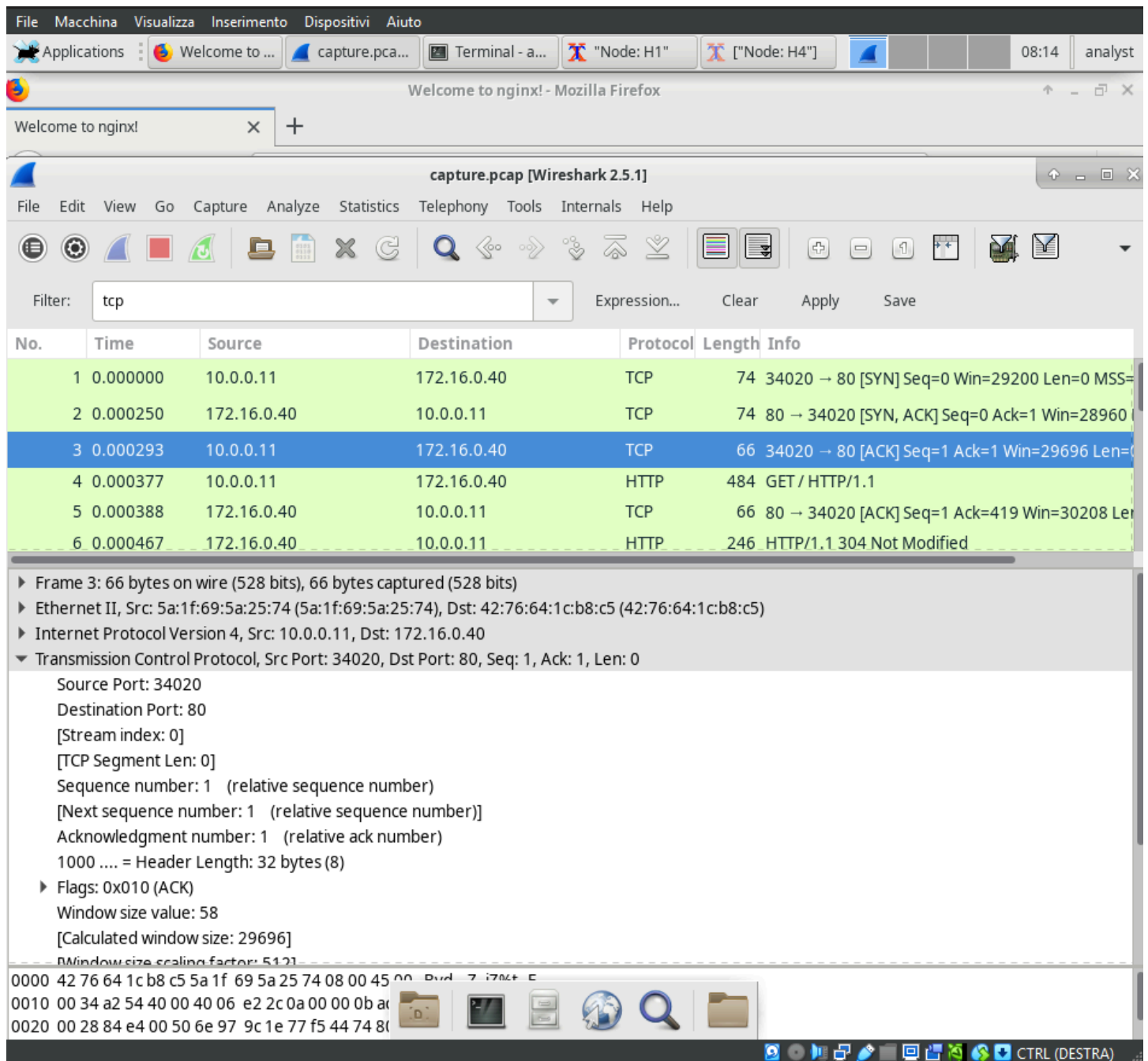
The packet details pane for Frame 1 shows the following information:

- Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
- Ethernet II, Src: 5a:1f:69:5a:25:74 (5a:1f:69:5a:25:74), Dst: 42:76:64:1c:b8:c5 (42:76:64:1c:b8:c5)
- Internet Protocol Version 4, Src: 10.0.0.11, Dst: 172.16.0.40
- Transmission Control Protocol, Src Port: 34020, Dst Port: 80, Seq: 0, Len: 0
  - Source Port: 34020
  - 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
  - [Calculated window size: 29200]
  - Checksum: 0xb671 [unverified]

- **Frame 2:** Risposta del server (SYN-ACK).
  - Porta sorgente: **80**.
  - Porta destinazione: **34020**.
  - Flag impostati: **SYN** e **ACK**.
  - Numero di sequenza relativo: **0**.
  - Numero di conferma relativo: **1**.



- **Frame 3:** Conferma del client (ACK).
  - Porta sorgente: **34020**.
  - Porta destinazione: **80**.
  - Flag impostato: **ACK**.
  - Numero di sequenza relativo: **1**.
  - Numero di conferma relativo: **1**.



## Parte 3: Visualizzare i pacchetti utilizzando tcpdump

### 1. Consultare il manuale di tcpdump

- Comando eseguito:
- `man tcpdump`
- Ricerca del flag -r:
  - Utilizzato per leggere file .pcap salvati.

### 2. Visualizzare i primi 3 pacchetti TCP catturati

- Comando eseguito:
- `tcpdump -r /home/analyst/capture.pcap tcp -c 3`
- Output:

```
Terminal - analyst@secOps:~  
File Edit View Terminal Tabs Help  
[analyst@secOps ~]$ tcpdump -r /home/analyst/capture.pcap tcp -c 3  
reading from file /home/analyst/capture.pcap, link-type EN10MB (Ethernet)  
08:07:39.743611 IP 10.0.0.11.34020 > 172.16.0.40.http: Flags [S], seq 1855429661, win 29200, options [mss 1460  
,sackOK,TS val 278521607 ecr 0,nop,wscale 9], length 0  
08:07:39.743861 IP 172.16.0.40.http > 10.0.0.11.34020: Flags [S.], seq 2012562547, ack 1855429662, win 28960,  
options [mss 1460,sackOK,TS val 2162629806 ecr 278521607,nop,wscale 9], length 0  
08:07:39.743904 IP 10.0.0.11.34020 > 172.16.0.40.http: Flags [.], ack 1, win 58, options [nop,nop,TS val 27852  
1607 ecr 2162629806], length 0  
[analyst@secOps ~]$
```

## 1. Chiusura di Mininet

- Comandi eseguiti:
- mininet> quit
- sudo mn -c

## Domande di riflessione

### 1. Tre filtri utili per un amministratore di rete:

- **TCP:** Per analizzare solo il traffico TCP.
- **IP specifico:** Per isolare il traffico verso/da un indirizzo IP.
- **HTTP:** Per analizzare richieste e risposte HTTP.

### 2. Altri utilizzi di Wireshark in una rete di produzione:

- Monitoraggio e analisi del traffico per rilevare anomalie o comportamenti sospetti.
- Analisi post-fatto di attacchi informatici.
- Identificazione di protocolli o porte non autorizzati in uso.

**Conclusioni:** Il laboratorio ha permesso di osservare il funzionamento della stretta di mano TCP a tre vie e di analizzarne i dettagli utilizzando sia Wireshark che tcpdump. Questi strumenti sono fondamentali per l'amministrazione di rete e la sicurezza informatica, fornendo una visione approfondita del traffico e delle connessioni attive.