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.

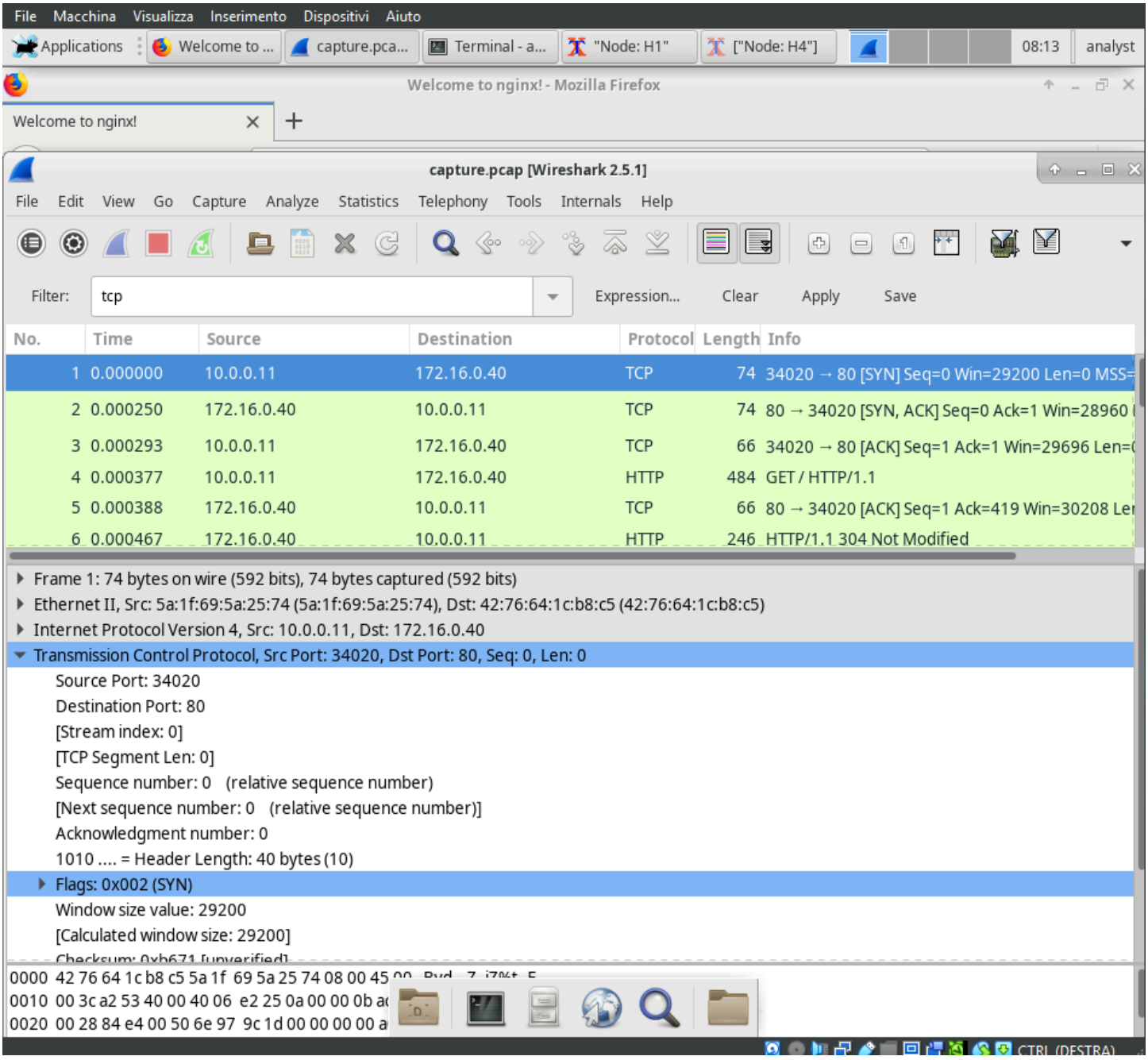
Parte 1: Preparare gli host per catturare il traffico

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.

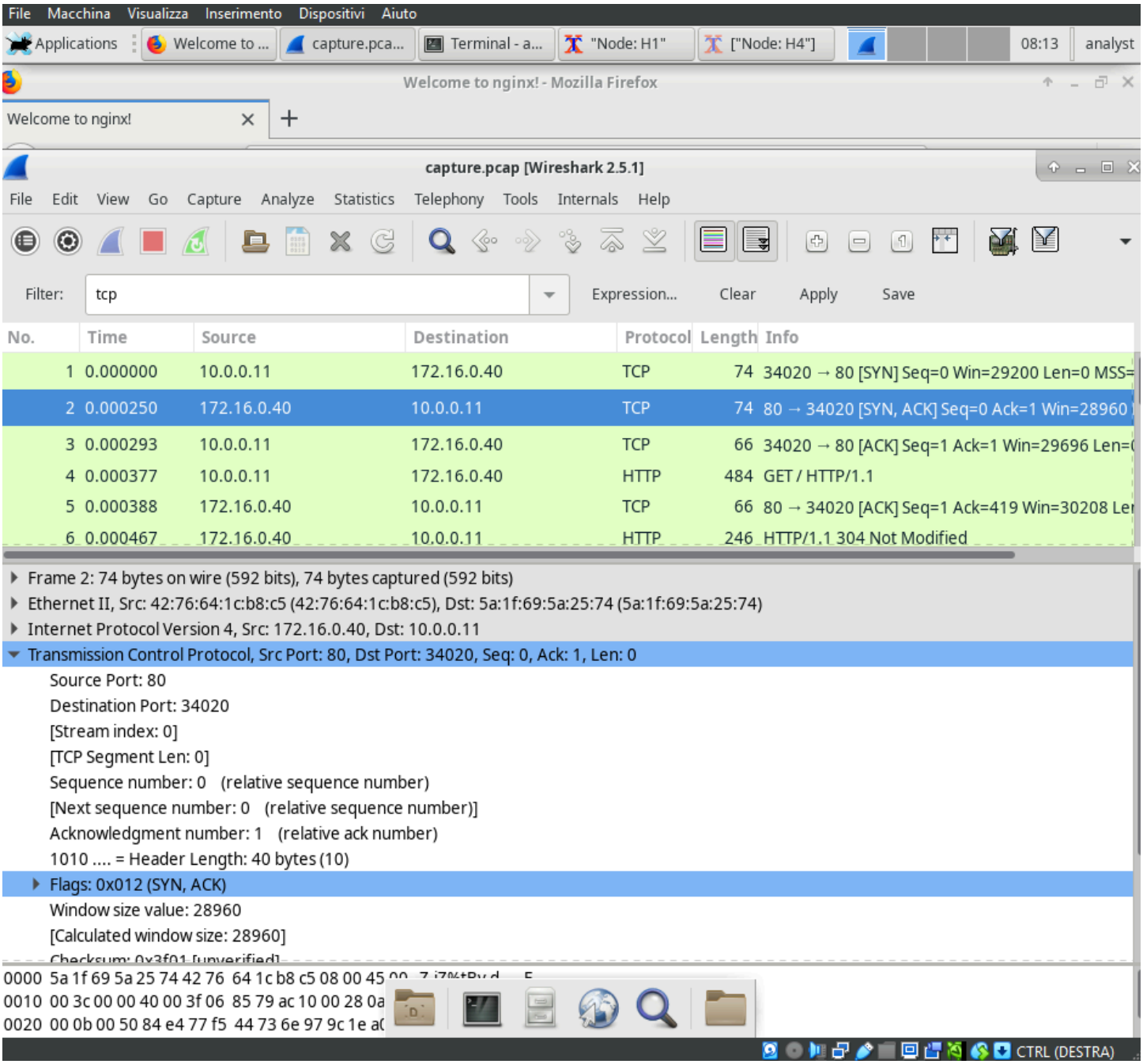
Parte 2: Analizzare i pacchetti utilizzando Wireshark

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

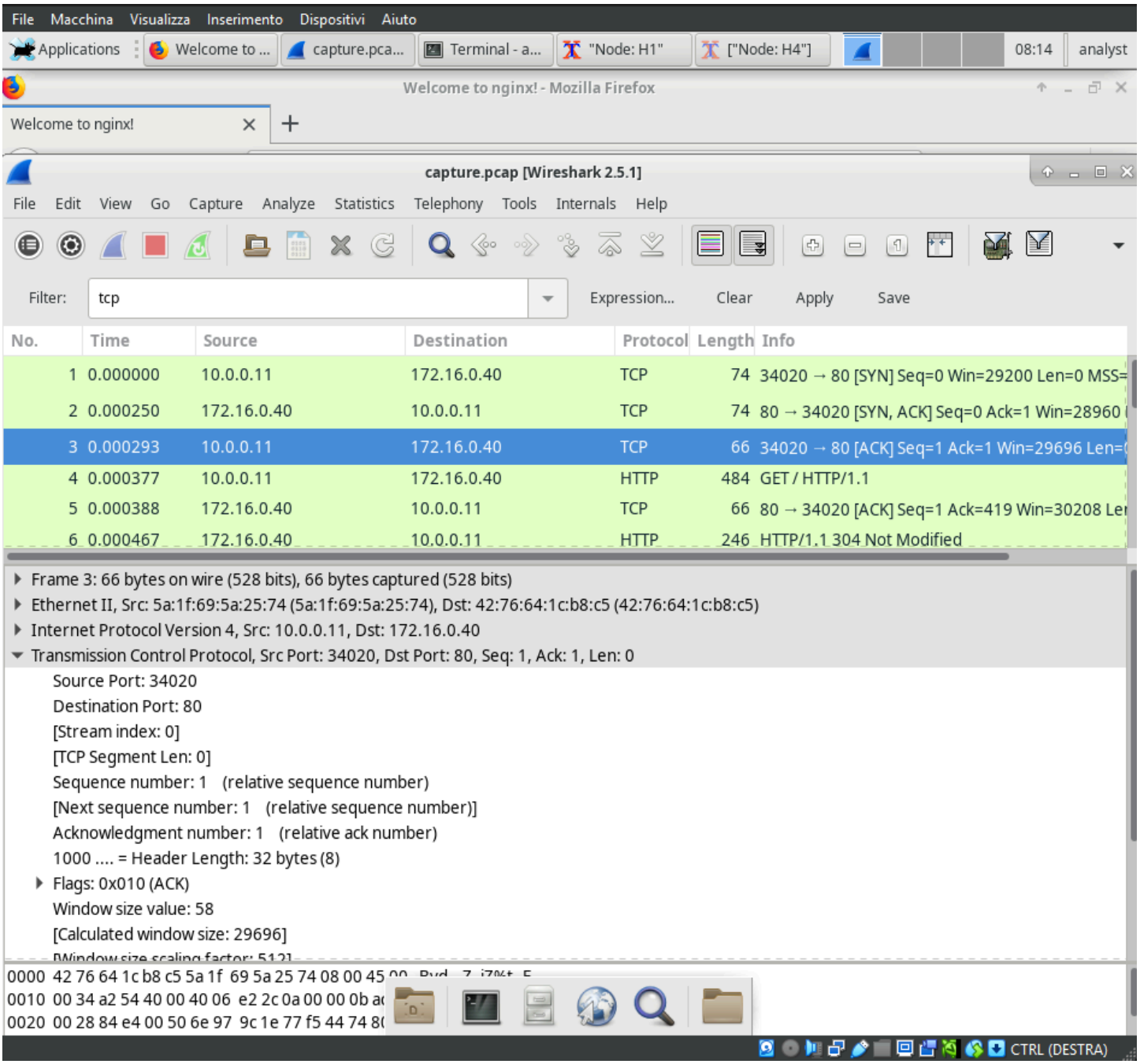
4. **Esame dei pacchetti (stretta di mano TCP a tre vie)**
   - **Frame 1**: Inizio della stretta di mano (SYN inviato).
     - Porta sorgente: **34020** (dinamico/privato).
     - Porta destinazione: **80** (noto, HTTP).
     - Flag impostato: **SYN**.
     - Numero di sequenza relativo: **0**.



   - **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**.

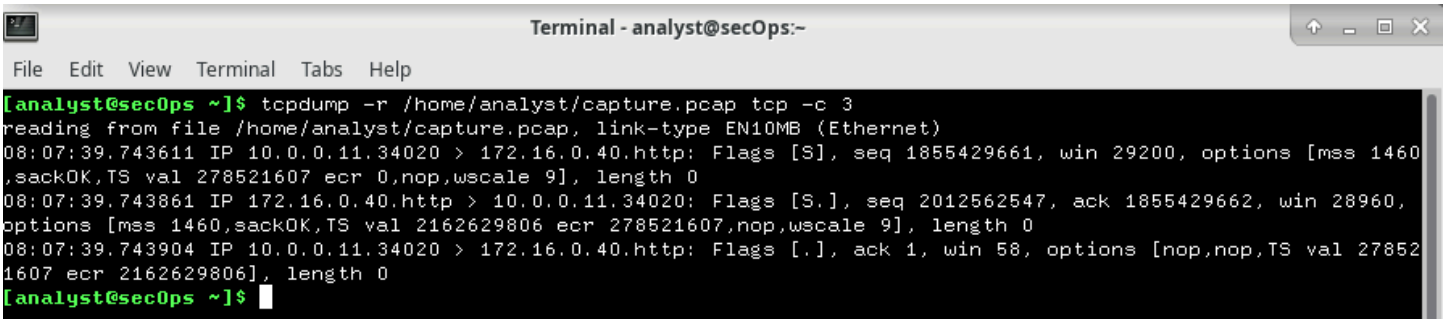


- **Frame 3**: Conferma del client (ACK).
  - Porta sorgente: **34020**.
  - Porta destinazione: **80**.
  - Flag impostato: **ACK**.
  - Numero di sequenza relativo: **1**.
  - Numero di conferma relativo: **1**.



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:



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.