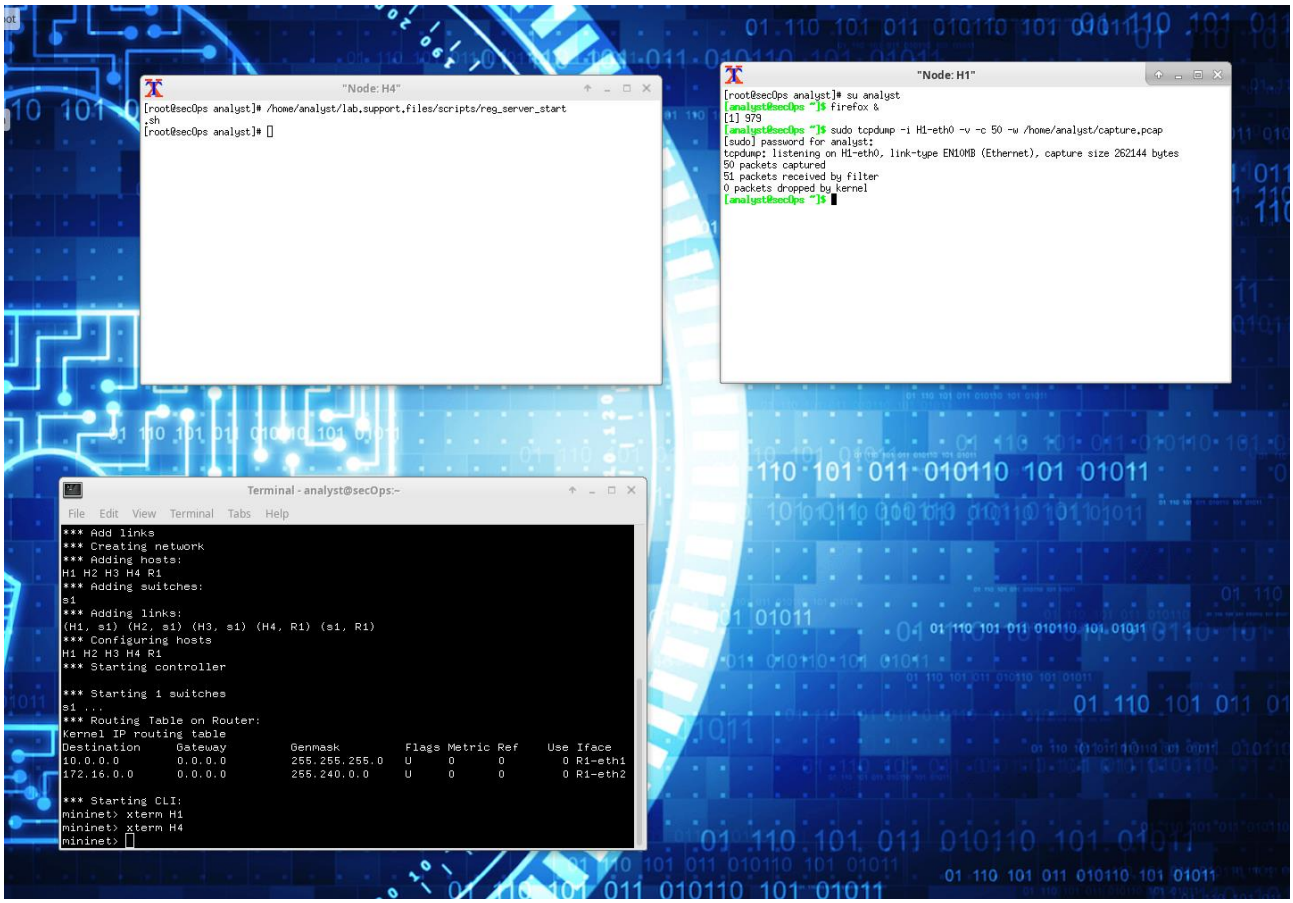
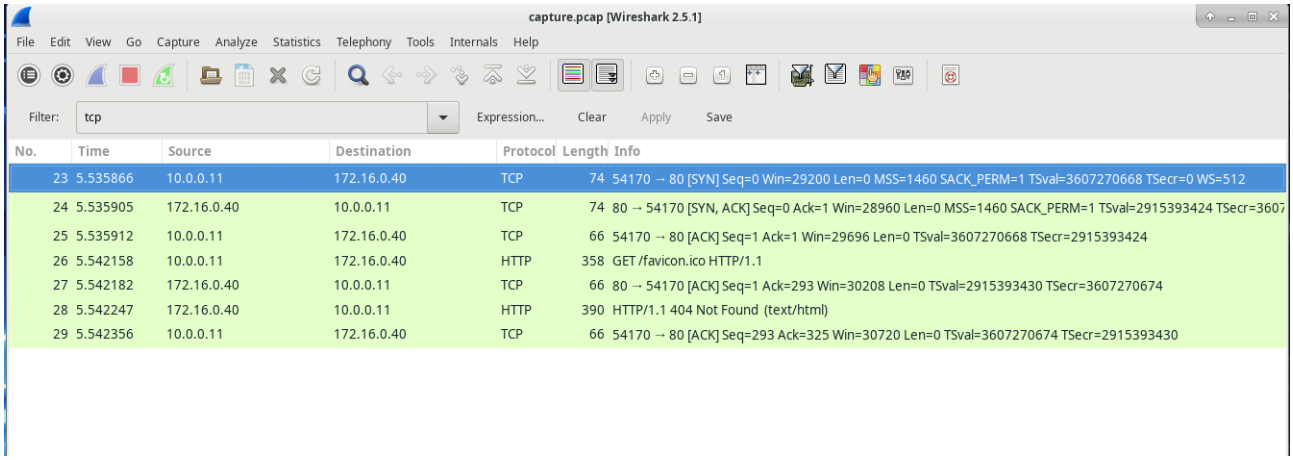
Pratica S11L3

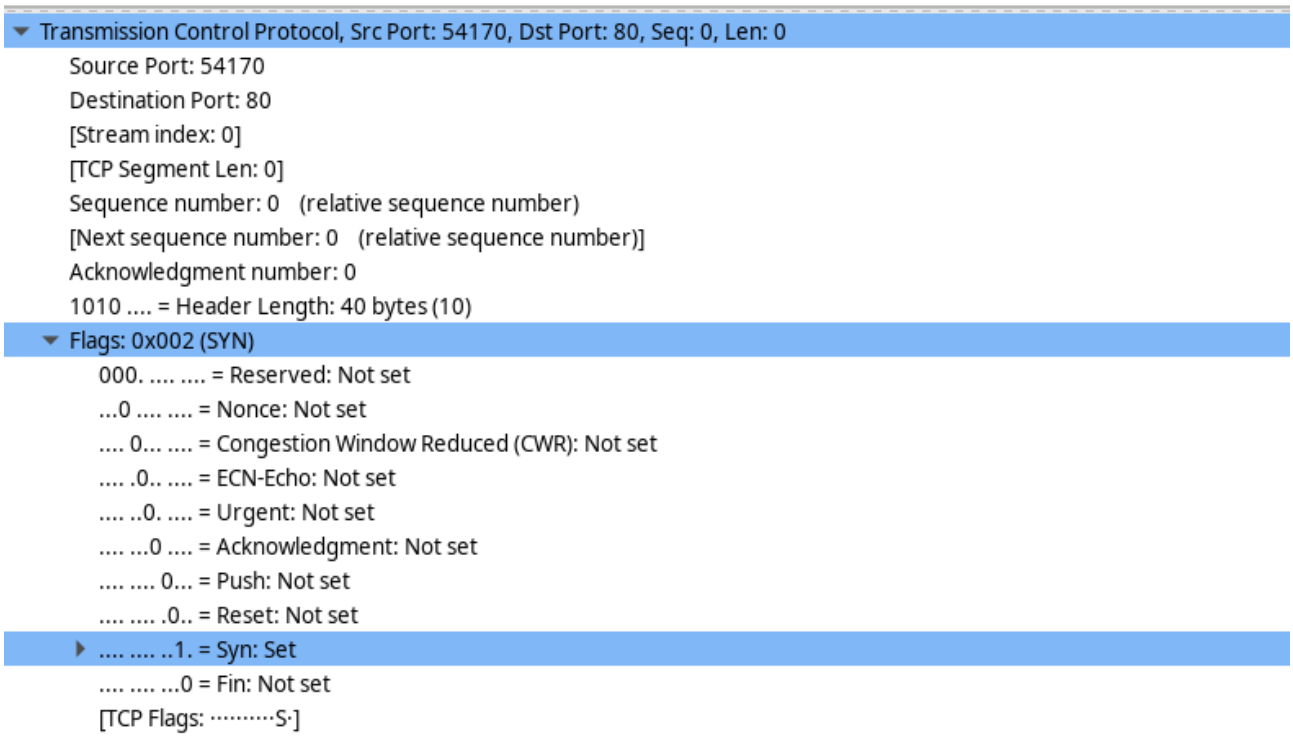
Apro la CyberOps Workstation, imposto i terminali come da guida e catturo il traffico di rete in un file .pcap



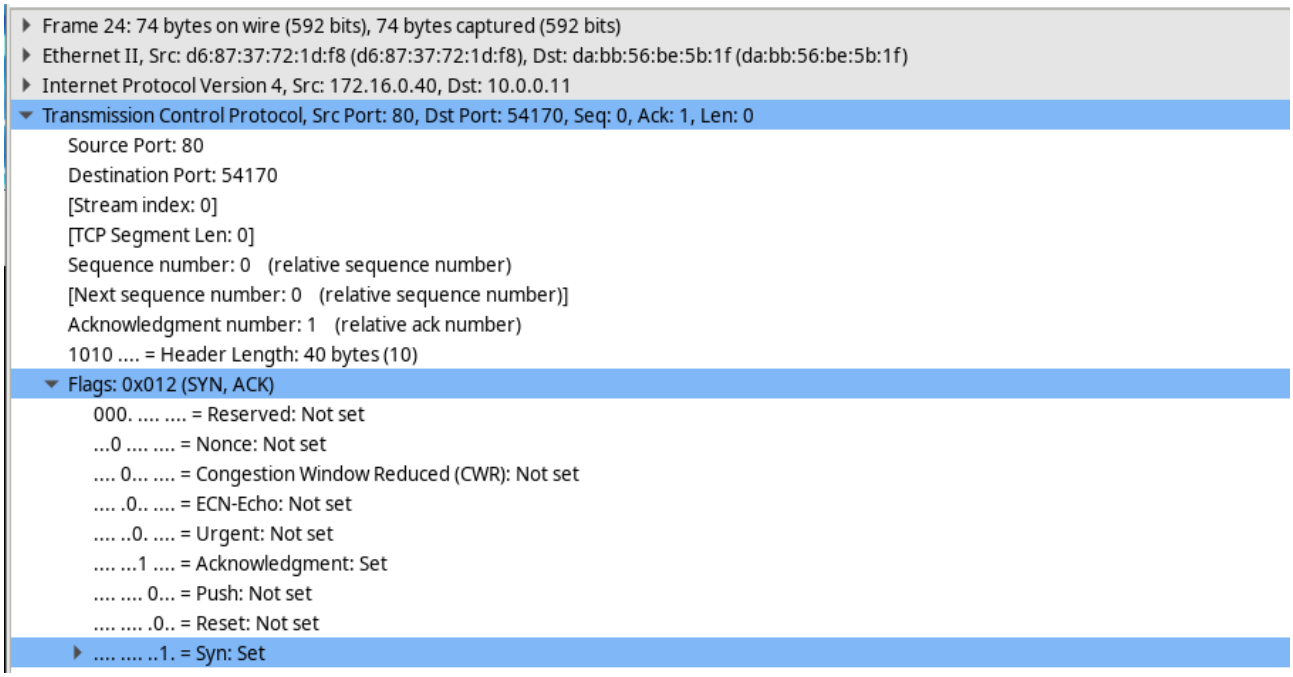
Apro il file .pcap con wireshark ed imposto il filtro su TCP



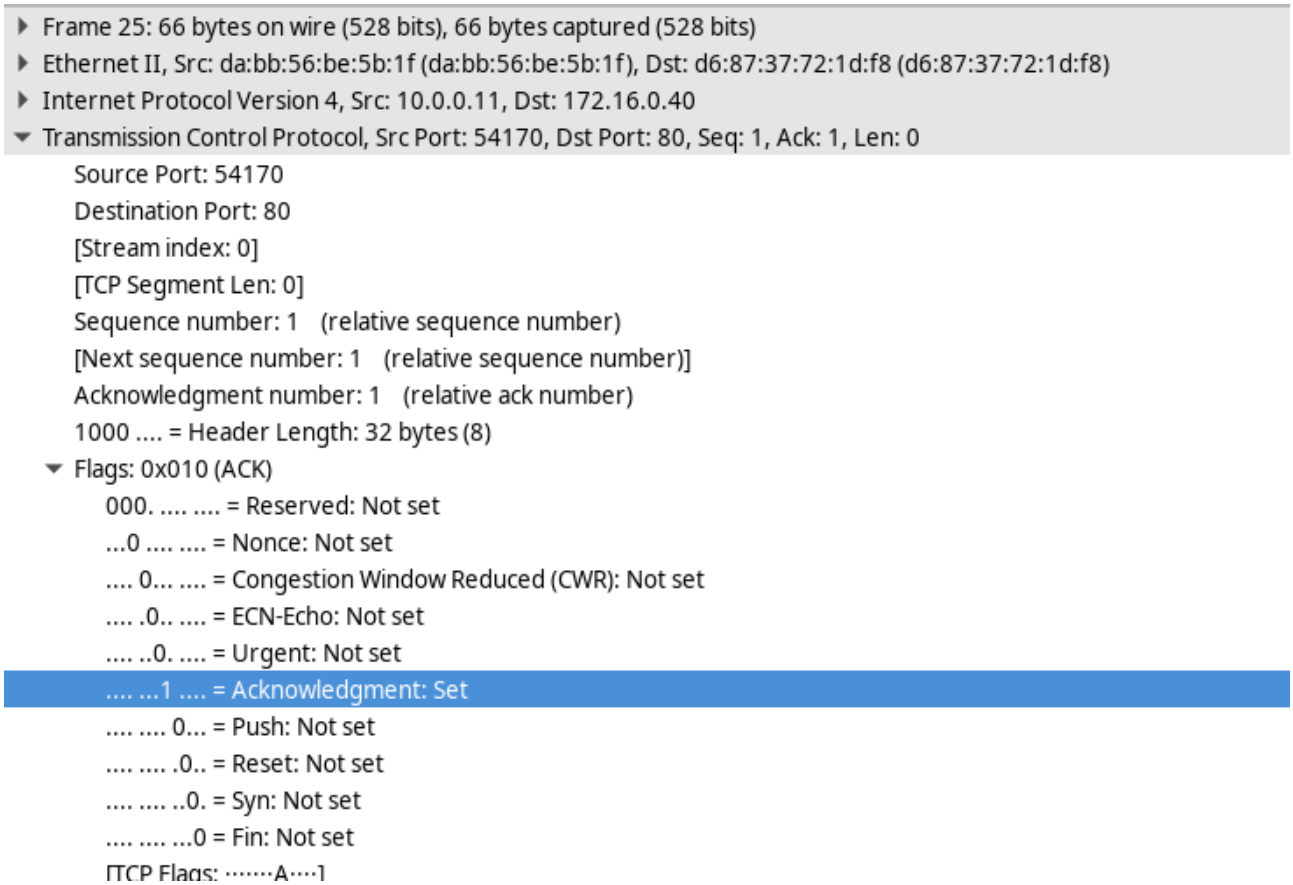
Analizzo il primo pacchetto che corrisponde all'inizio del three-way handshake, vedo che la connessione parte dalla porta 54170 con destinazione porta 80, è attiva la flag SYN



Analizzo il secondo pacchetto e vedo che c'è la risposta del server con un pacchetto SYN,ACK



Per chiudere il trhee-way handshake analizzo il terzo pacchetto e vedo la flag ACK attiva



Da terminale con tcpdump posso analizzare il file non avendo a disposizione wireshark