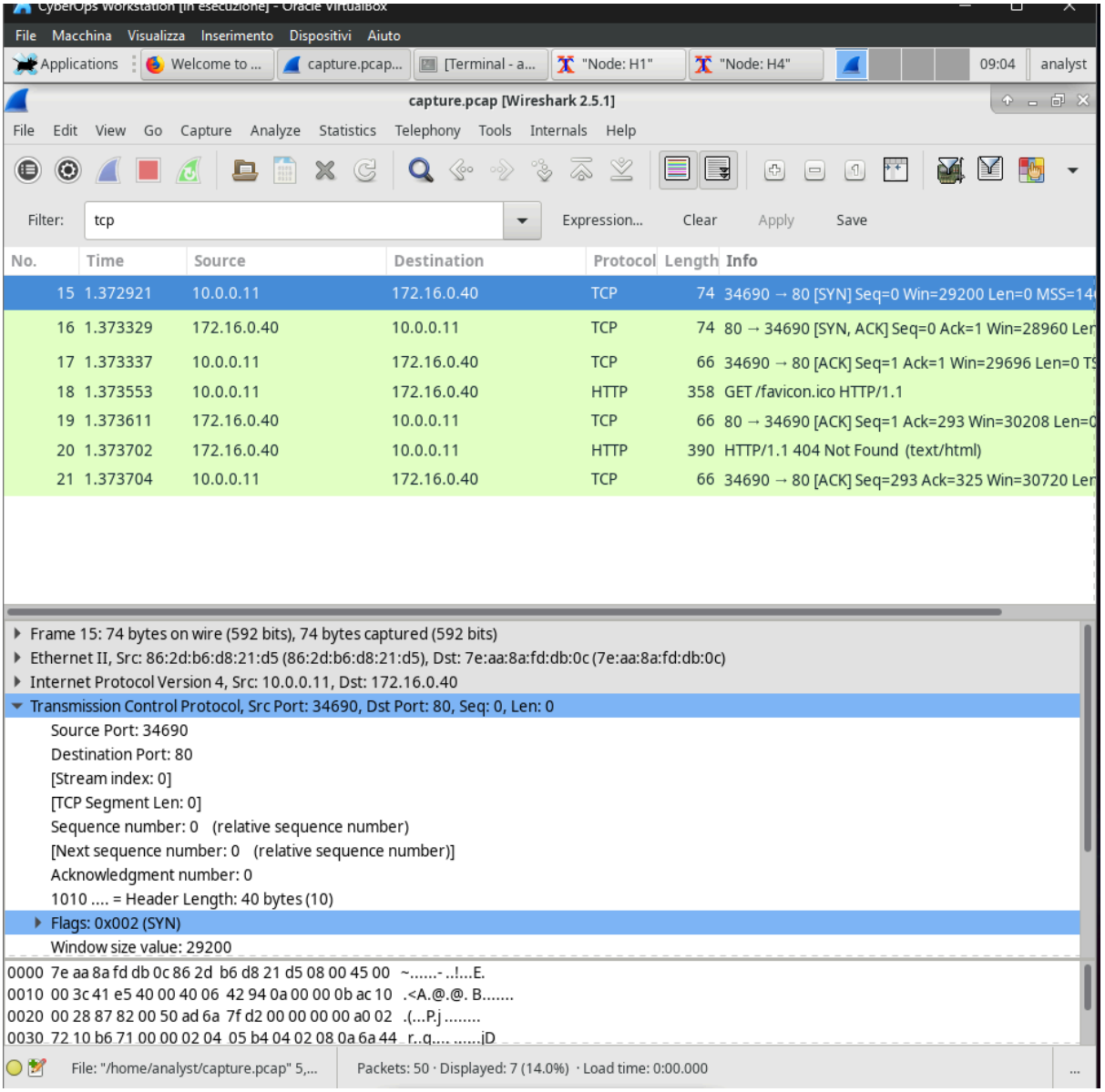
Laboratori giorno 2 – Cisco CyberOps



Qual è il numero di porta di origine TCP?
34690

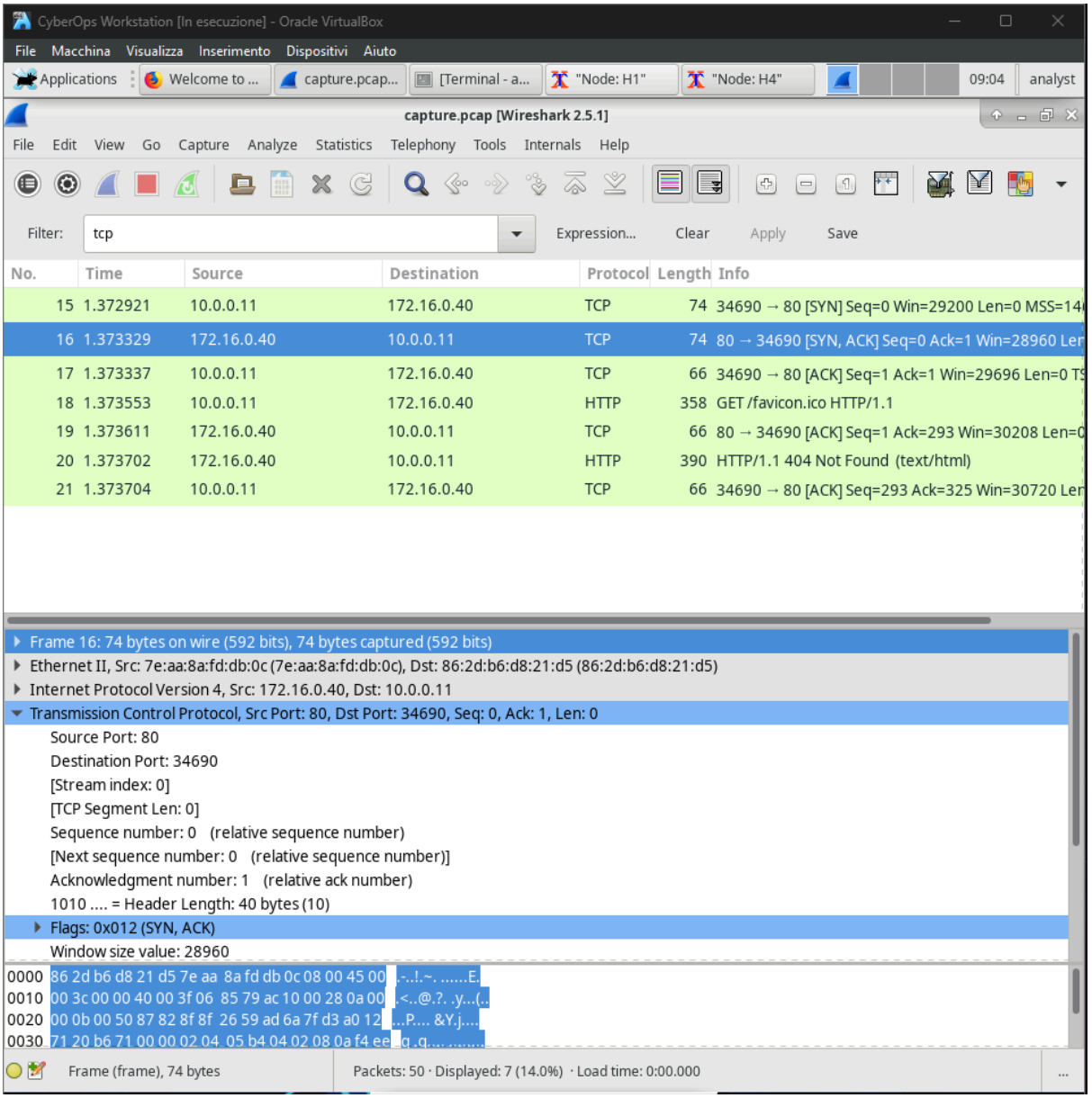
Come classificheresti il porting di origine?
Dinamico o privato

Qual è il numero di porta di destinazione TCP?
Porta 80

Come classificheresti il porto di destinazione?
Noto, registrato (protocollo HTTP o web)

Quale flag (o bandiere) è impostato?
Flag SYN

Su cosa è impostato il numero di sequenza relativo?
0

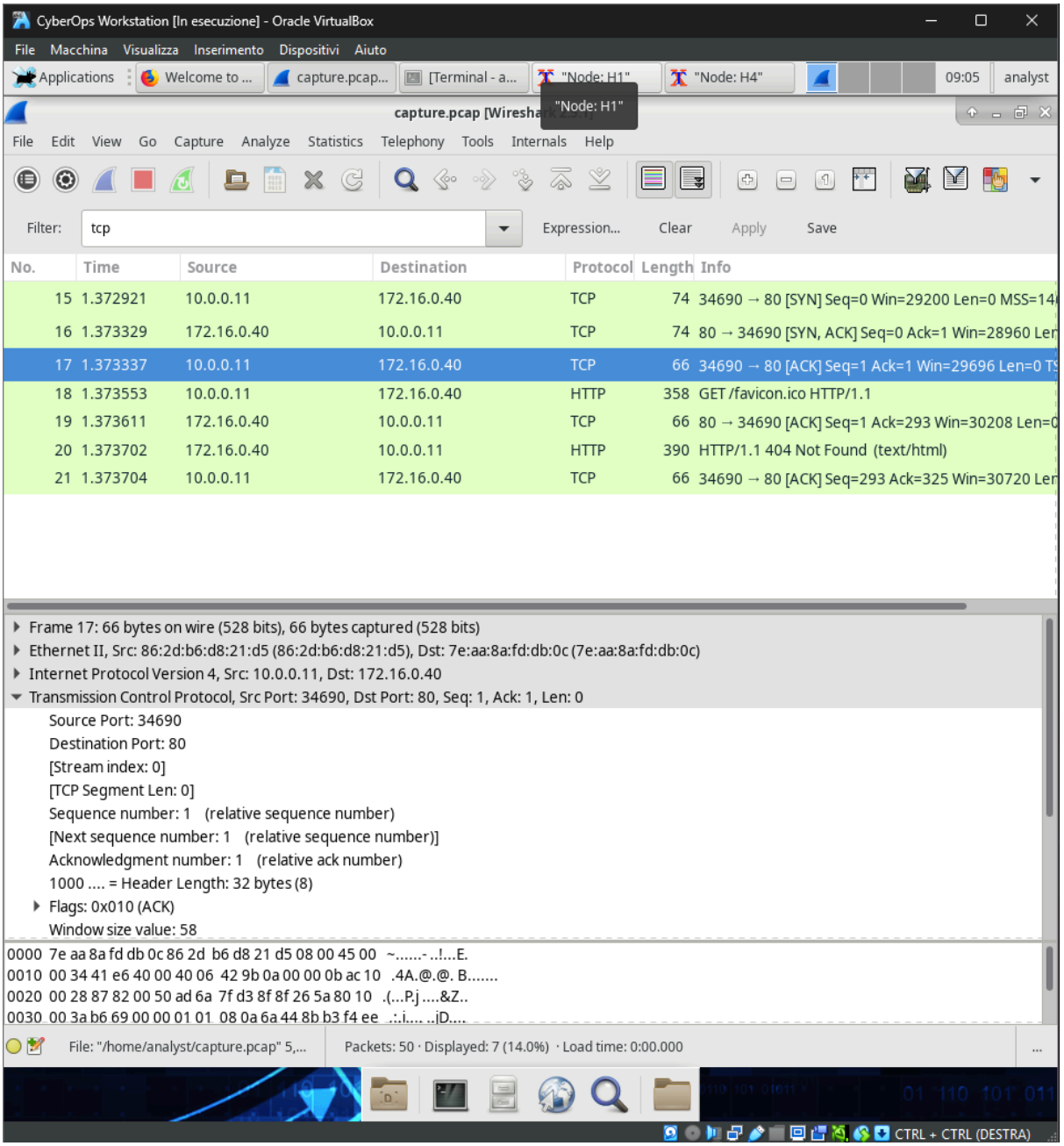


Quali sono i valori delle porte di origine e di destinazione?
La porta di origine è ora 80 e la porta di destinazione è ora 34690

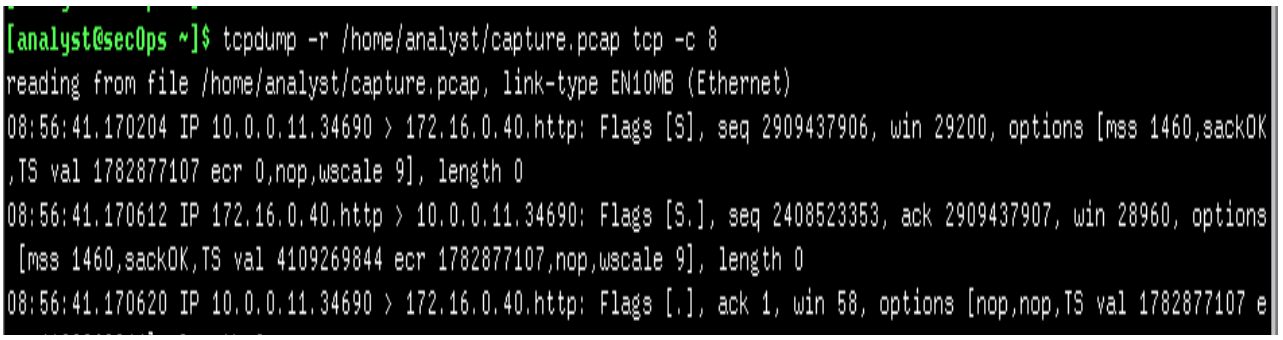
Quali flag sono impostati?
Il flag di riconoscimento (ACK) e il flag Syn (SYN)

Su cosa sono impostati i numeri di sequenza e di riconoscimento relativi?

Il numero di sequenza relativo è 0 e il numero di riconoscimento relativo è 1.



Quale flag (o bandiere) è impostato?
Flag di riconoscimento (ACK)



L'opzione -r consente di leggere il pacchetto dal file che è stato salvato utilizzando l'opzione -w con tcpdump o altri strumenti che scrivono file pcap o pcap-ng, come Wireshark.