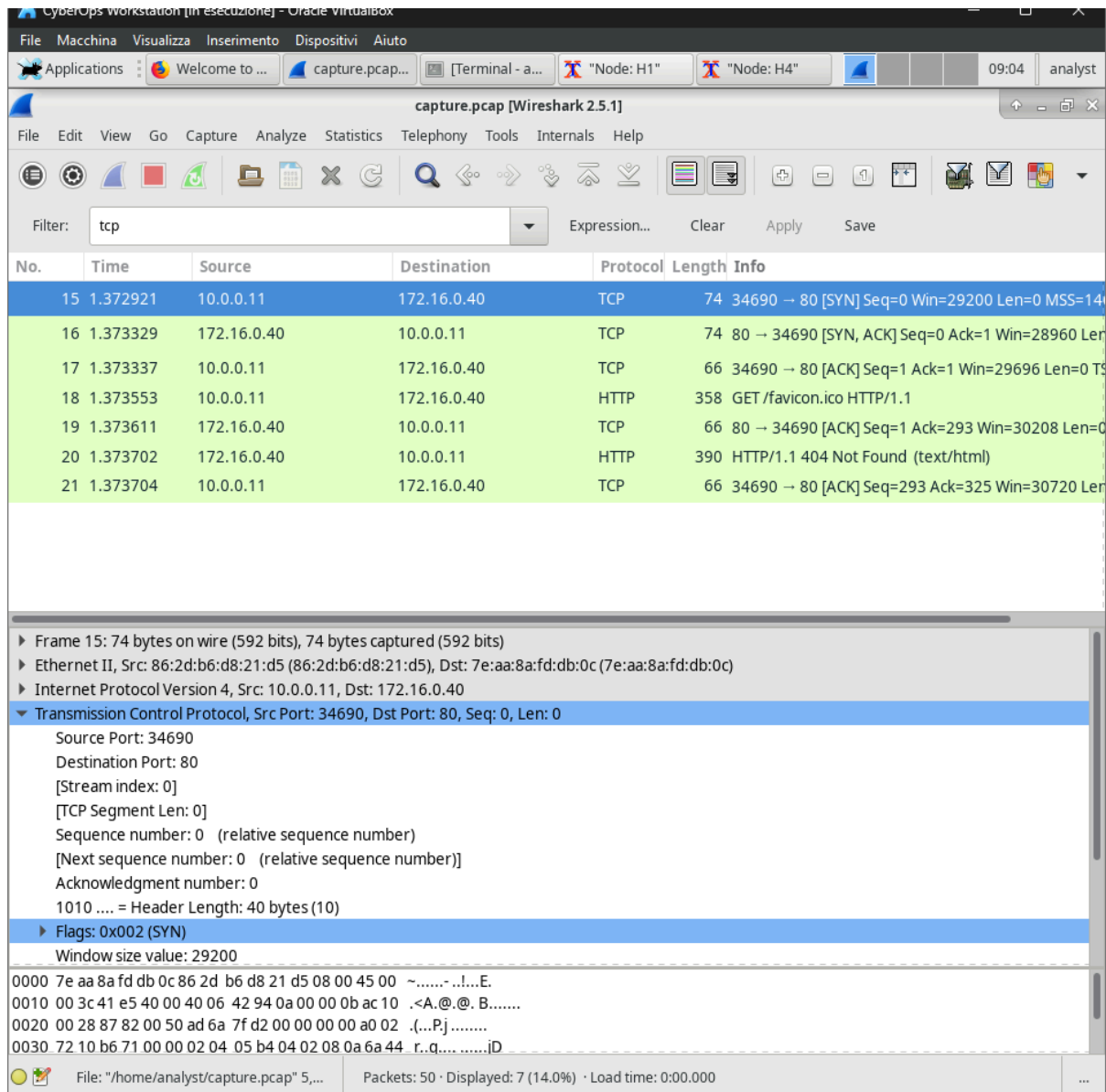


Laboratori giorno 2 – Cisco CyberOps



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?

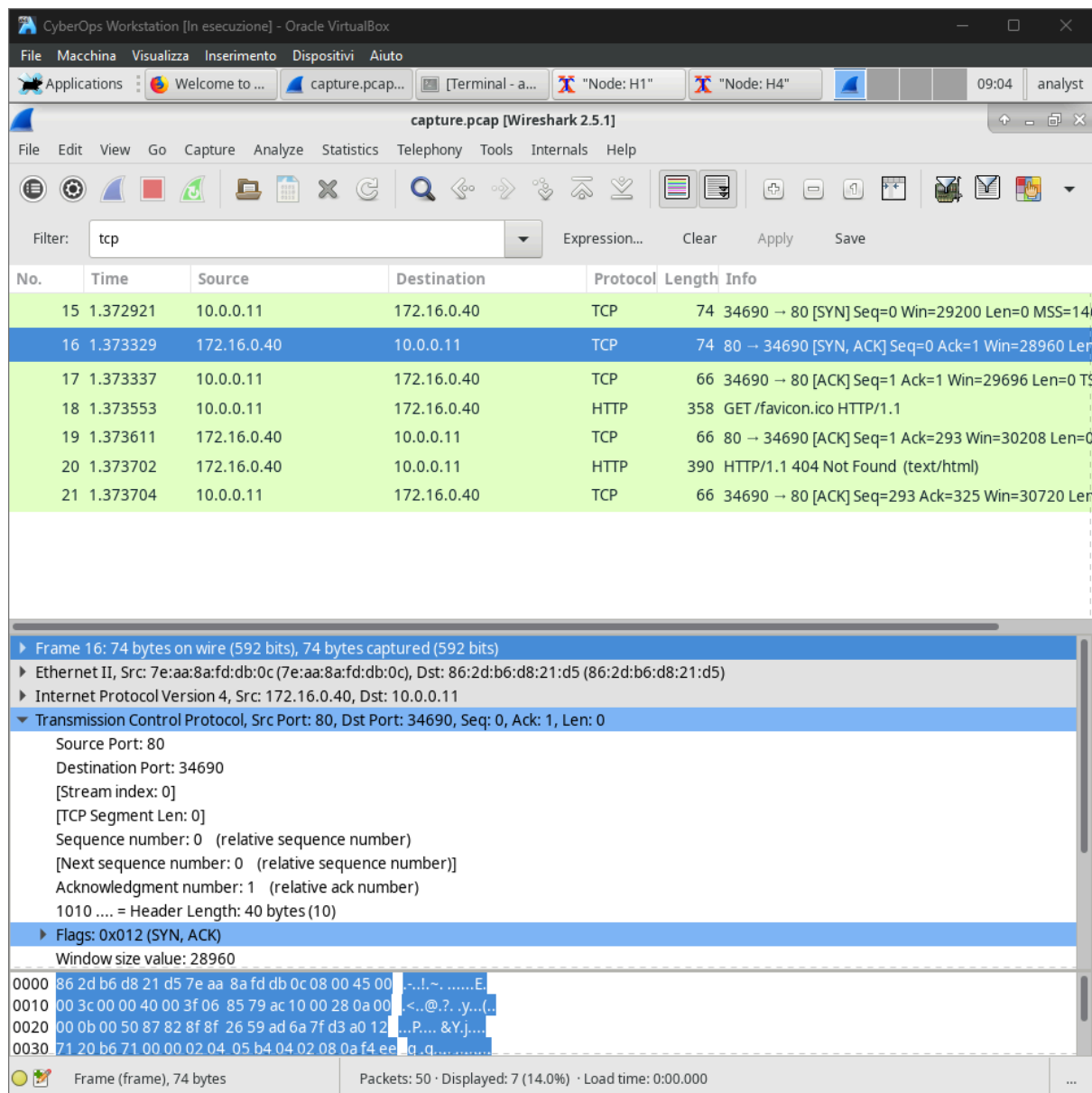
Noto, registrato (protocollo HTTP o web)

Quale flag (o bandiera) 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.

The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Macchina, Visualizza, Inserimento, Dispositivi, and Aiuto. The toolbar contains various icons for file operations, capture, analysis, and display. The main display area is divided into three panes: the packet list, packet details, and packet bytes.

The packet list pane shows a list of captured packets. The selected packet is number 17, a TCP segment from 10.0.0.11 to 172.16.0.40, port 34690 to 80, with sequence number 1 and acknowledgment number 1. The packet details pane shows the structure of the packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
15	1.372921	10.0.0.11	172.16.0.40	TCP	74	34690 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=14
16	1.373329	172.16.0.40	10.0.0.11	TCP	74	80 → 34690 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0
17	1.373337	10.0.0.11	172.16.0.40	TCP	66	34690 → 80 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TS
18	1.373553	10.0.0.11	172.16.0.40	HTTP	358	GET /favicon.ico HTTP/1.1
19	1.373611	172.16.0.40	10.0.0.11	TCP	66	80 → 34690 [ACK] Seq=1 Ack=293 Win=30208 Len=0
20	1.373702	172.16.0.40	10.0.0.11	HTTP	390	HTTP/1.1 404 Not Found (text/html)
21	1.373704	10.0.0.11	172.16.0.40	TCP	66	34690 → 80 [ACK] Seq=293 Ack=325 Win=30720 Len=0

Frame 17: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: 86:2d:b6:d8:21:d5 (86:2d:b6:d8:21:d5), Dst: 7e:aa:8a:fd:db:0c (7e:aa:8a:fd:db:0c)
Internet Protocol Version 4, Src: 10.0.0.11, Dst: 172.16.0.40
Transmission Control Protocol, Src Port: 34690, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
Source Port: 34690
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 1 (relative sequence number)
[Next sequence number: 1 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
1000 = Header Length: 32 bytes (8)
Flags: 0x010 (ACK)
Window size value: 58
0000 7e aa 8a fd db 0c 86 2d b6 d8 21 d5 08 00 45 00 ~.....-!...E.
0010 00 34 41 e6 40 00 40 06 42 9b 0a 00 00 0b ac 10 .4A.@.@. B.....
0020 00 28 87 82 00 50 ad 6a 7f d3 8f 8f 26 5a 80 10 .(...P.j....&Z..
0030 00 3a b6 69 00 00 01 01 08 0a 6a 44 8b b3 f4 ee ..!.....;iD....

Quale flag (o bandiera) è impostato?

Flag di riconoscimento (ACK)

```
[analyst@secOps ~]$ tcpdump -r /home/analyst/capture.pcap tcp -c 8
reading from file /home/analyst/capture.pcap, link-type EN10MB (Ethernet)
08:56:41.170204 IP 10.0.0.11.34690 > 172.16.0.40.http: Flags [S], seq 2909437906, win 29200, options [mss 1460,sackOK
,TS val 1782877107 ecr 0,nop,wscale 9], length 0
08:56:41.170612 IP 172.16.0.40.http > 10.0.0.11.34690: Flags [S.], seq 2408523353, ack 2909437907, win 28960, options
 [mss 1460,sackOK,TS val 4109269844 ecr 1782877107,nop,wscale 9], length 0
08:56:41.170620 IP 10.0.0.11.34690 > 172.16.0.40.http: Flags [.], ack 1, win 58, options [nop,nop,TS val 1782877107 e
```

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.