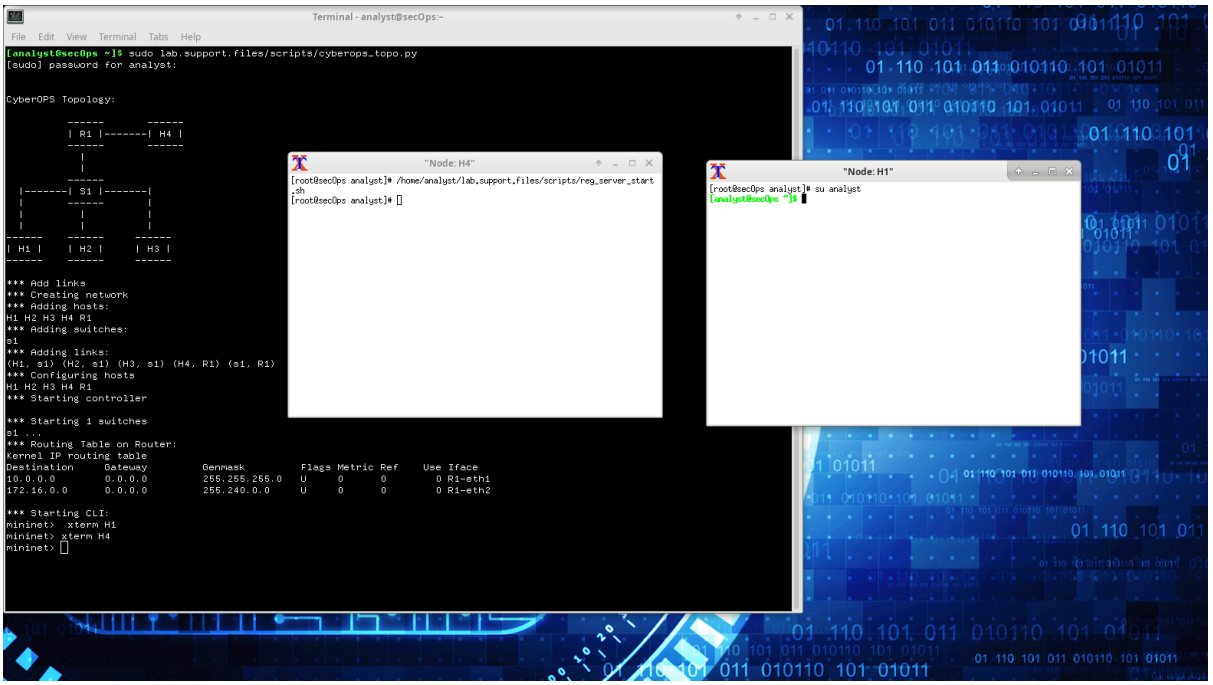
S10L3



Come primo step apriamo il terminale e apriamo mininet

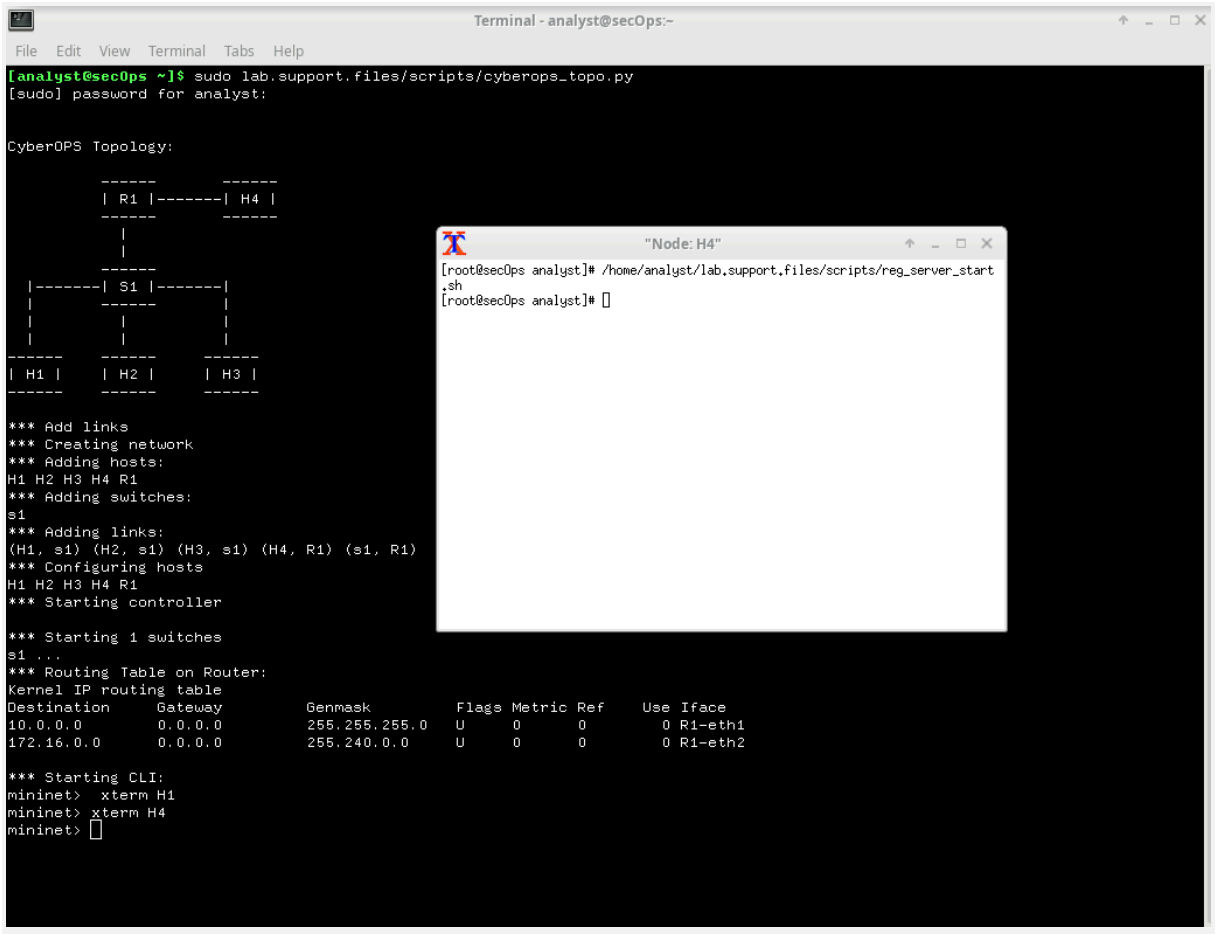
Mininet è una piattaforma software per la simulazione di reti che permette di creare e testare reti di computer virtuali (simulazioni di reti) in un ambiente controllato e isolato. È molto utilizzata per sviluppare, testare e prototipare protocolli di rete, topologie e sistemi di gestione delle reti.

Mininet crea una rete virtuale composta da host, switch e router, simulando il comportamento di una rete reale. Le risorse di rete, come la banda, la latenza e la capacità di buffering, possono essere configurate per rispecchiare le condizioni di rete di interesse. Inoltre, Mininet è particolarmente utile in contesti di ricerca e sviluppo di software per reti, in particolare per le reti SDN (Software-Defined Networking), poiché consente di emulare e sperimentare facilmente configurazioni avanzate senza necessità di hardware fisico costoso.

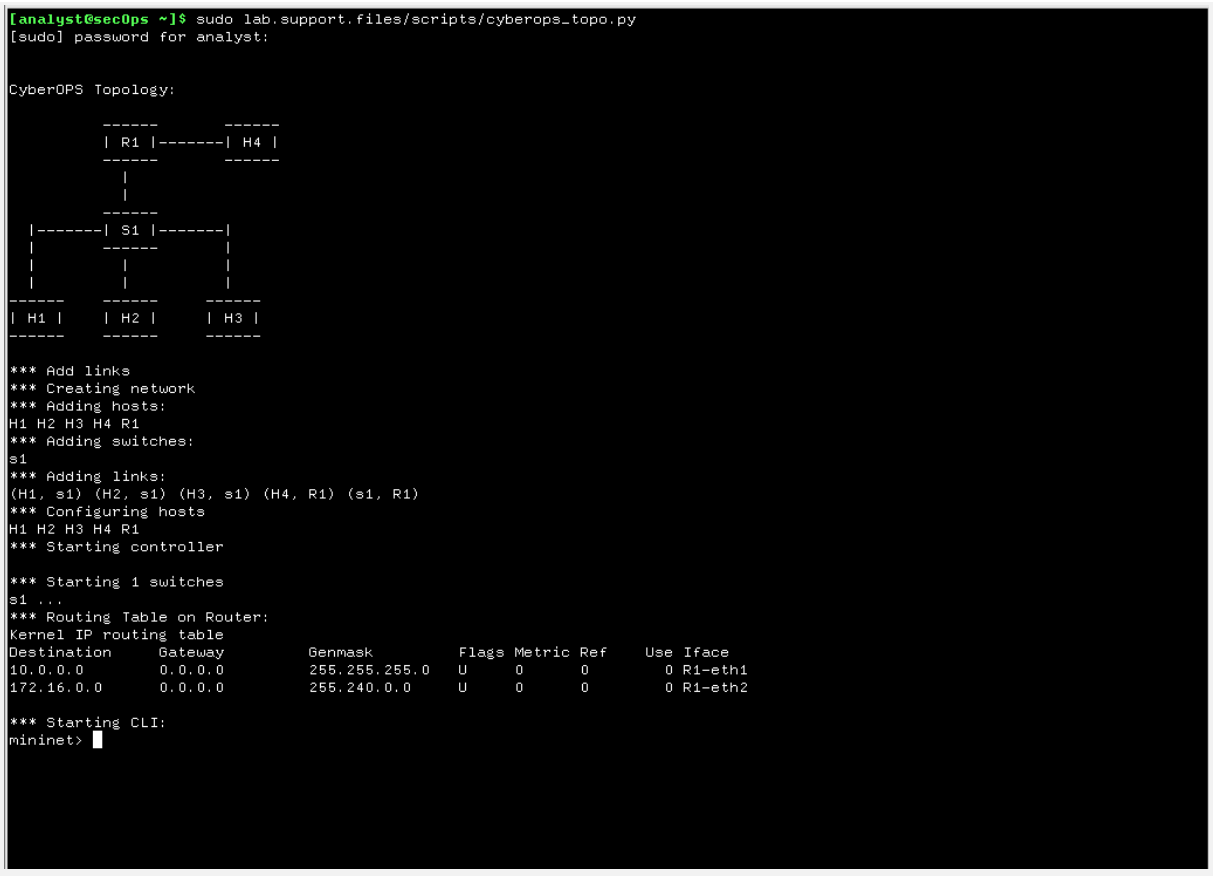
diamo lo start a H1 E H4

```
mininet> xterm H1
```

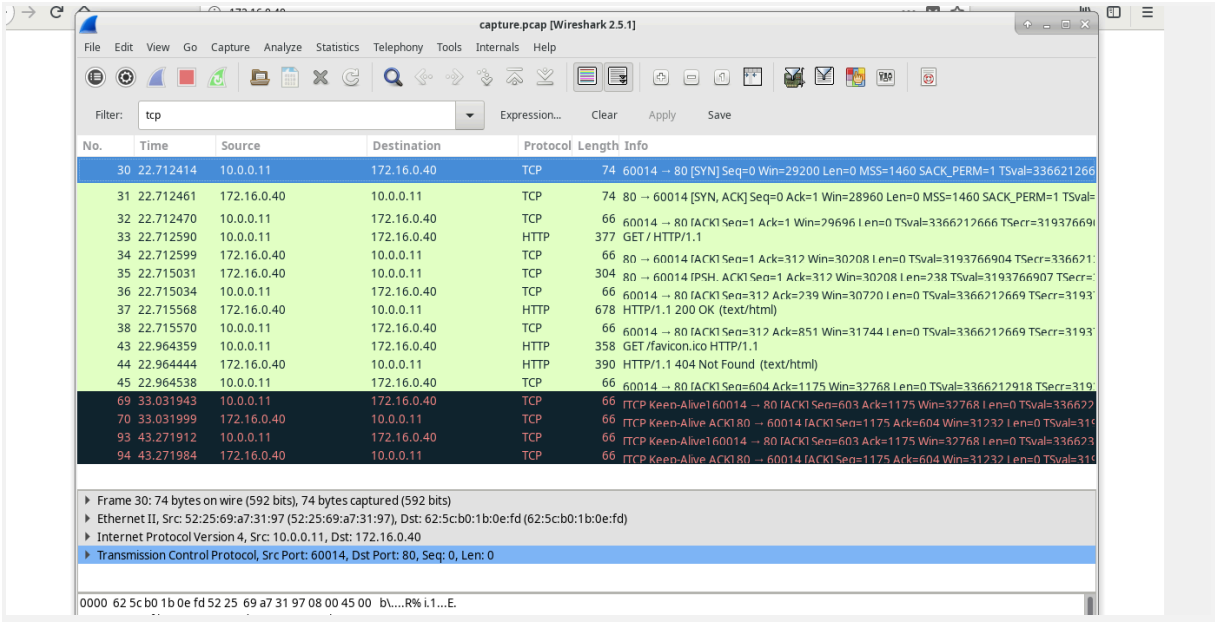
```
mininet> xterm H4
```

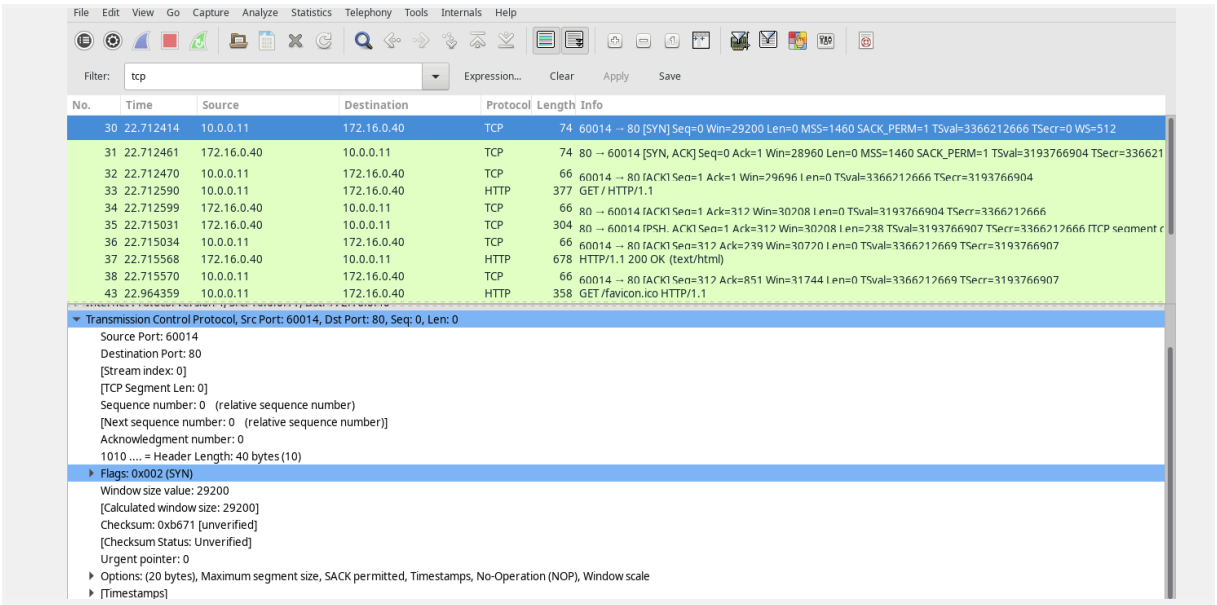

Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ sudo lab.support.files/scripts/cyberops_topo.py
[sudo] password for analyst:
CyberOPS Topology:
R1
H4
S1
H1
H2
H3
*** Add links
*** Creating network
*** Adding hosts:
H1 H2 H3 H4 R1
*** Adding switches:
s1
*** Adding links:
(H1, s1) (H2, s1) (H3, s1) (H4, R1) (s1, R1)
*** Configuring hosts
H1 H2 H3 H4 R1
*** Starting controller
*** Starting 1 switches
s1 ...
*** Routing Table on Router:
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
10.0.0.0 0.0.0.0 255.255.255.0 U 0 0 0 R1-eth1
172.16.0.0 0.0.0.0 255.240.0.0 U 0 0 0 R1-eth2
*** Starting CLI:
mininet> xterm H1
mininet> xterm H4
mininet>
"Node: H4"
[root@secOps analyst]# /home/analyst/lab.support.files/scripts/reg_server_start.sh
[root@secOps analyst]#

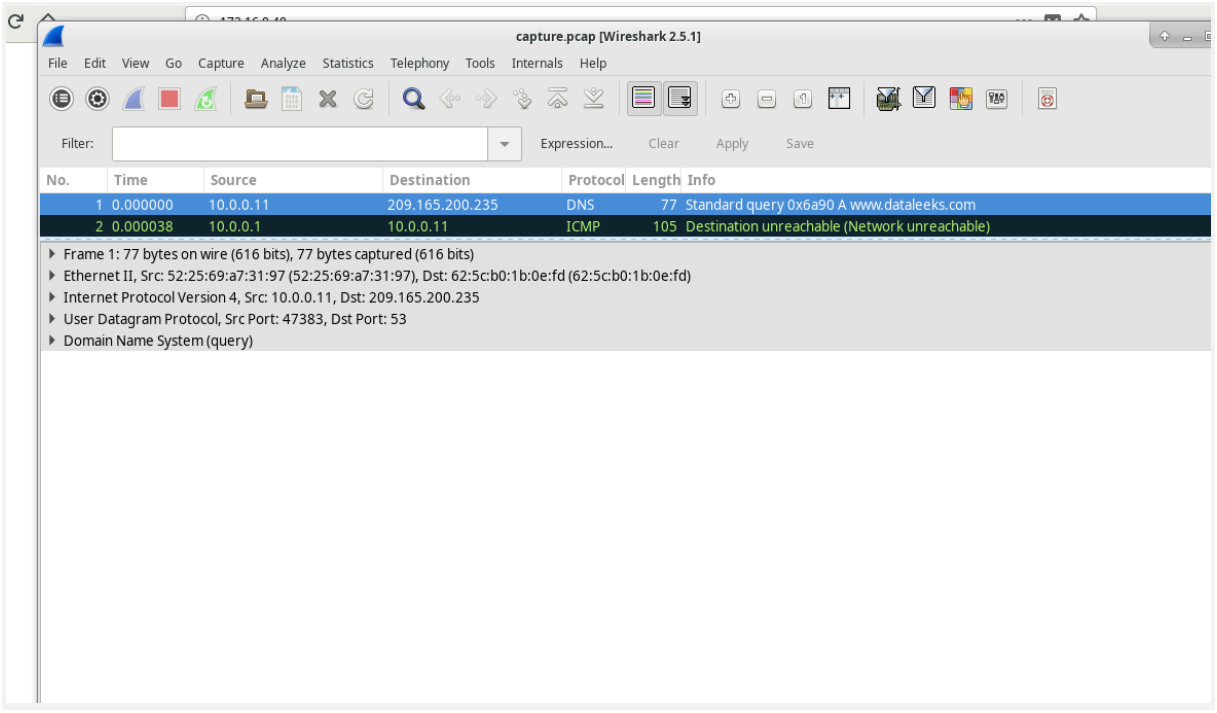
STARTIAMO IL WEB SERVER

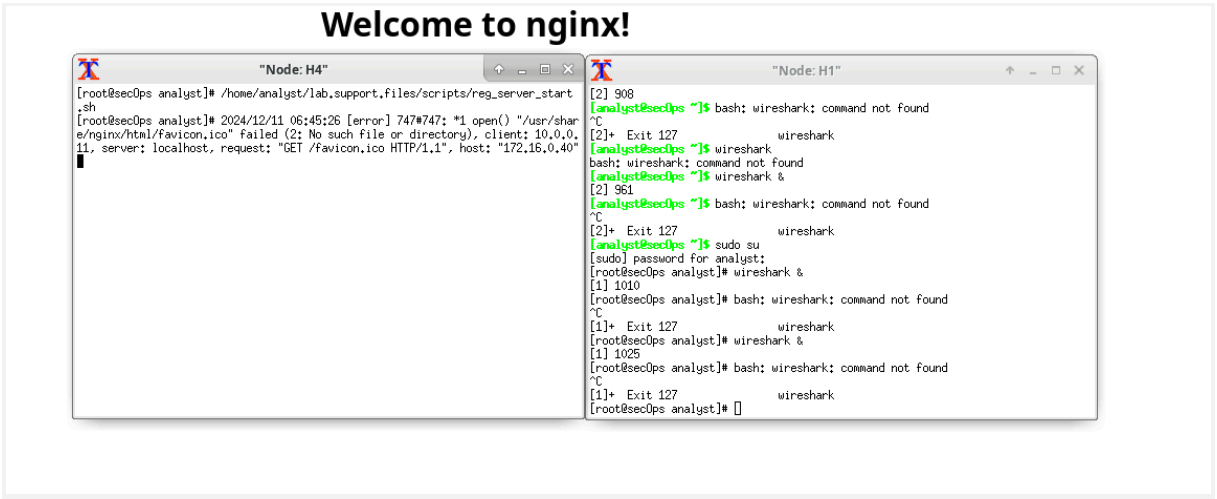


PARTE 2 CATTURA CON WIRESHARK


capture.pcap [Wireshark 2.5.1]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: tcp
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
30 22.712414 10.0.0.11 172.16.0.40 TCP 74 60014 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3366212666
31 22.712461 172.16.0.40 10.0.0.11 TCP 74 80 → 60014 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=
32 22.712470 10.0.0.11 172.16.0.40 TCP 66
33 22.712590 10.0.0.11 172.16.0.40 HTTP 377 GET / HTTP/1.1
34 22.712599 172.16.0.40 10.0.0.11 TCP 66
35 22.715031 172.16.0.40 10.0.0.11 TCP 304
36 22.715034 10.0.0.11 172.16.0.40 TCP 66
37 22.715568 172.16.0.40 10.0.0.11 HTTP 678 HTTP/1.1 200 OK (text/html)
38 22.715570 10.0.0.11 172.16.0.40 TCP 66
43 22.964359 10.0.0.11 172.16.0.40 HTTP 358 GET /favicon.ico HTTP/1.1
44 22.964444 172.16.0.40 10.0.0.11 HTTP 390 HTTP/1.1 404 Not Found (text/html)
45 22.964538 10.0.0.11 172.16.0.40 TCP 66
69 33.031943 10.0.0.11 172.16.0.40 TCP 66
70 33.031999 172.16.0.40 10.0.0.11 TCP 66
93 43.271912 10.0.0.11 172.16.0.40 TCP 66
94 43.271984 172.16.0.40 10.0.0.11 TCP 66
Frame 30: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: 52:25:69:a7:31:97 (52:25:69:a7:31:97), Dst: 62:5c:b0:1b:0e:fd (62:5c:b0:1b:0e:fd)
Internet Protocol Version 4, Src: 10.0.0.11, Dst: 172.16.0.40
Transmission Control Protocol, Src Port: 60014, Dst Port: 80, Seq: 0, Len: 0
0000 62 5c b0 1b 0e fd 52 25 69 a7 31 97 08 00 45 00 b\....R% i.1...E.


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: tcp
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
30 22.712414 10.0.0.11 172.16.0.40 TCP 74 60014 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3366212666 TSecr=0 WS=512
31 22.712461 172.16.0.40 10.0.0.11 TCP 74 80 → 60014 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=3193766904 TSecr=336621
32 22.712470 10.0.0.11 172.16.0.40 TCP 66 60014 → 80 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=3366212666 TSecr=3193766904
33 22.712590 10.0.0.11 172.16.0.40 HTTP 377 GET / HTTP/1.1
34 22.712599 172.16.0.40 10.0.0.11 TCP 66 80 → 60014 [ACK] Seq=1 Ack=312 Win=30208 Len=0 TSval=3193766904 TSecr=3366212666
35 22.715031 172.16.0.40 10.0.0.11 TCP 304 80 → 60014 [PSH, ACK] Seq=1 Ack=312 Win=30208 Len=238 TSval=3193766907 TSecr=3366212666 [TCP segment
36 22.715034 10.0.0.11 172.16.0.40 TCP 66 60014 → 80 [ACK] Seq=312 Ack=239 Win=30720 Len=0 TSval=3366212669 TSecr=3193766907
37 22.715568 172.16.0.40 10.0.0.11 HTTP 678 HTTP/1.1 200 OK (text/html)
38 22.715570 10.0.0.11 172.16.0.40 TCP 66 60014 → 80 [ACK] Seq=312 Ack=851 Win=31744 Len=0 TSval=3366212669 TSecr=3193766907
43 22.964359 10.0.0.11 172.16.0.40 HTTP 358 GET /favicon.ico HTTP/1.1
Transmission Control Protocol, Src Port: 60014, Dst Port: 80, Seq: 0, Len: 0
Source Port: 60014
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]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
[Timestamps]





ANALIZZIAMO LA 3 WAY HANDSHAKE