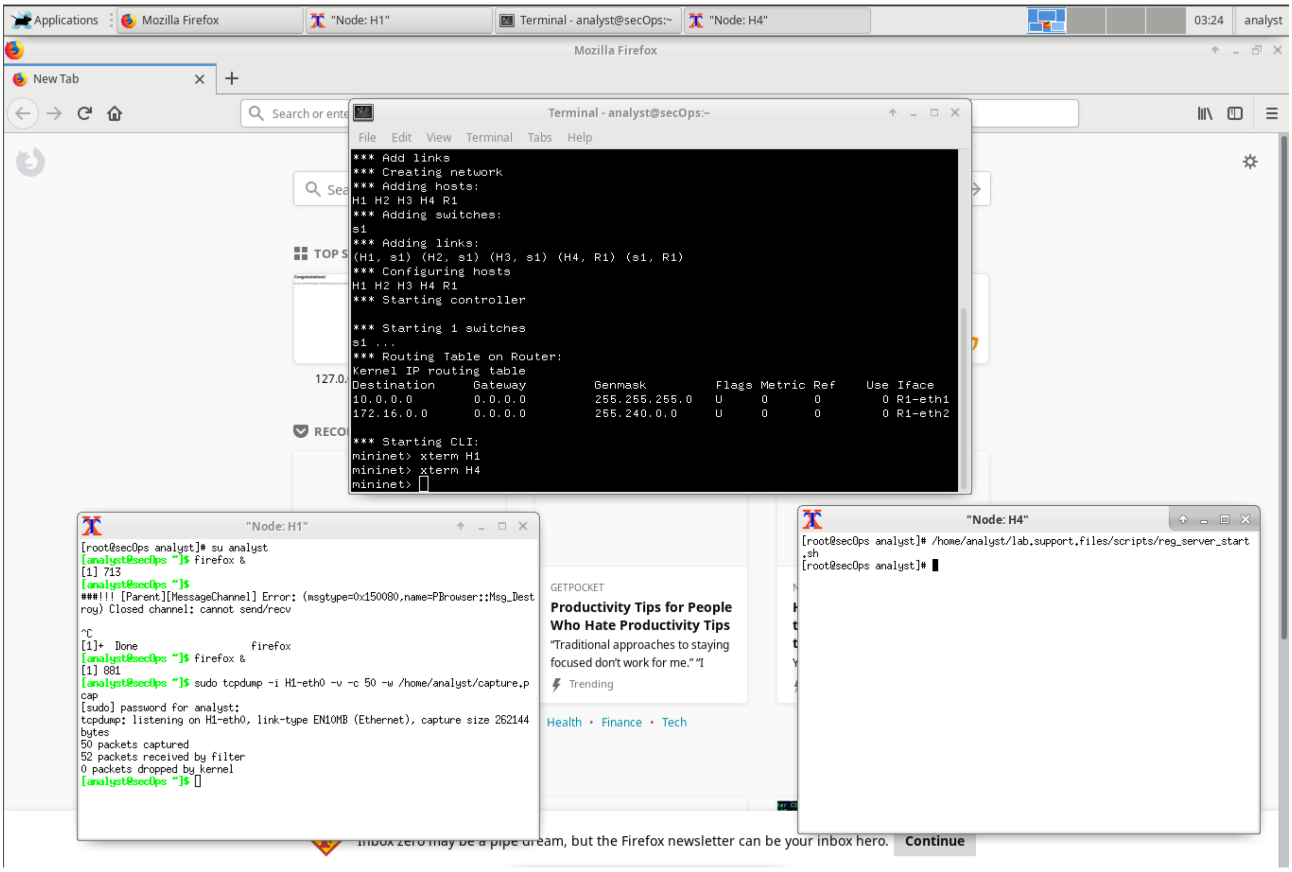
THREE-WAY HANDSHAKE CAPTURE

Prepare the Hosts



Applications
Mozilla Firefox
"Node: H1"
Terminal - analyst@secOps:~
"Node: H4"
03:24
analyst
New Tab
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
GETPOCKET
Productivity Tips for People Who Hate Productivity Tips
"Traditional approaches to staying focused don't work for me." "I
Trending
Health • Finance • Tech
Inbox zero may be a pipe dream, but the Firefox newsletter can be your inbox hero.
Continue

```
*** 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: H1"

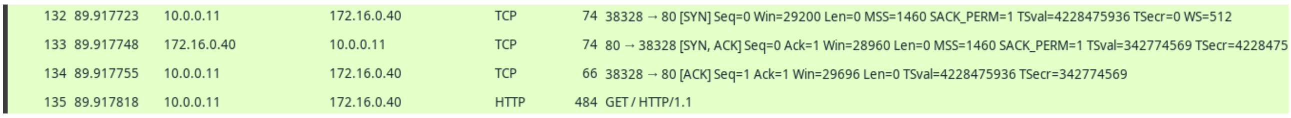
```
[root@secOps analyst]# su analyst
[analyst@secOps ~]$ firefox &
[1] 713
[analyst@secOps ~]$
###!!! [Parent][MessageChannel] Error: (msgtype=0x150080,name=PBrowser::Msg_Dest
roy) Closed channel: cannot send/recv

^C
[1]+  Done                    firefox
[analyst@secOps ~]$ firefox &
[1] 881
[analyst@secOps ~]$ sudo tcpdump -i H1-eth0 -v -c 50 -w /home/analyst/capture.p
cap
[sudo] password for analyst:
tcpdump: listening on H1-eth0, link-type EN10MB (Ethernet), capture size 262144
bytes
50 packets captured
52 packets received by filter
0 packets dropped by kernel
[analyst@secOps ~]$
```

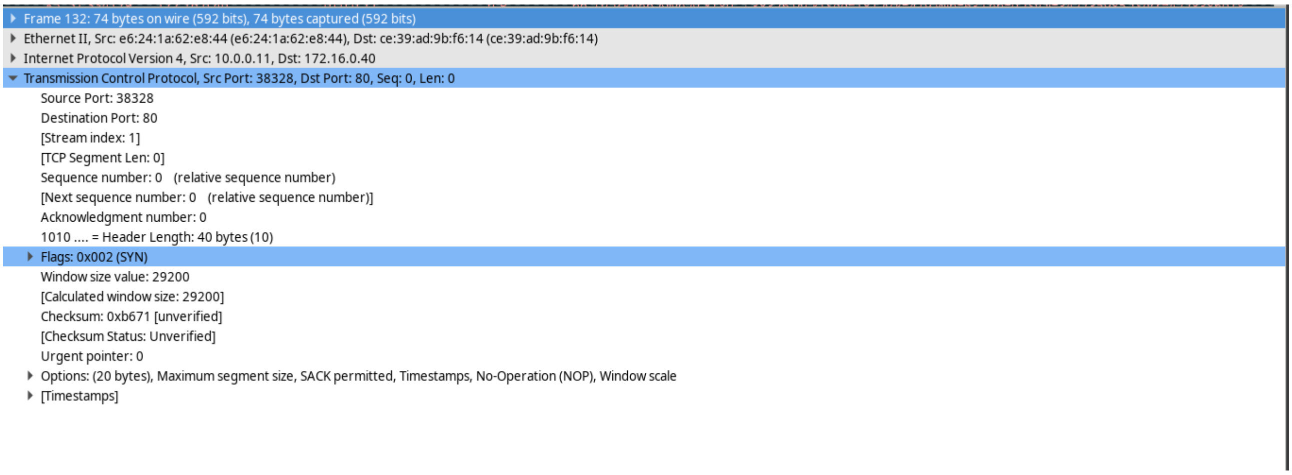
"Node: H4"

```
[root@secOps analyst]# /home/analyst/lab.support.files/scripts/reg_server_start
.sh
[root@secOps analyst]#
```

Analyze the Packets using Wireshark

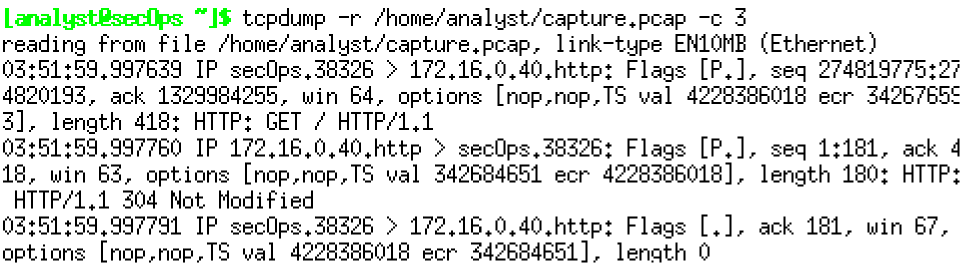


```
132  89.917723   10.0.0.11     172.16.0.40   TCP    74  38328 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=4228475936 TSecr=0 WS=512
133  89.917748   172.16.0.40   10.0.0.11     TCP    74  80 → 38328 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=342774569 TSecr=4228475
134  89.917755   10.0.0.11     172.16.0.40   TCP    66  38328 → 80 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=4228475936 TSecr=342774569
135  89.917818   10.0.0.11     172.16.0.40   HTTP  484  GET / HTTP/1.1
```

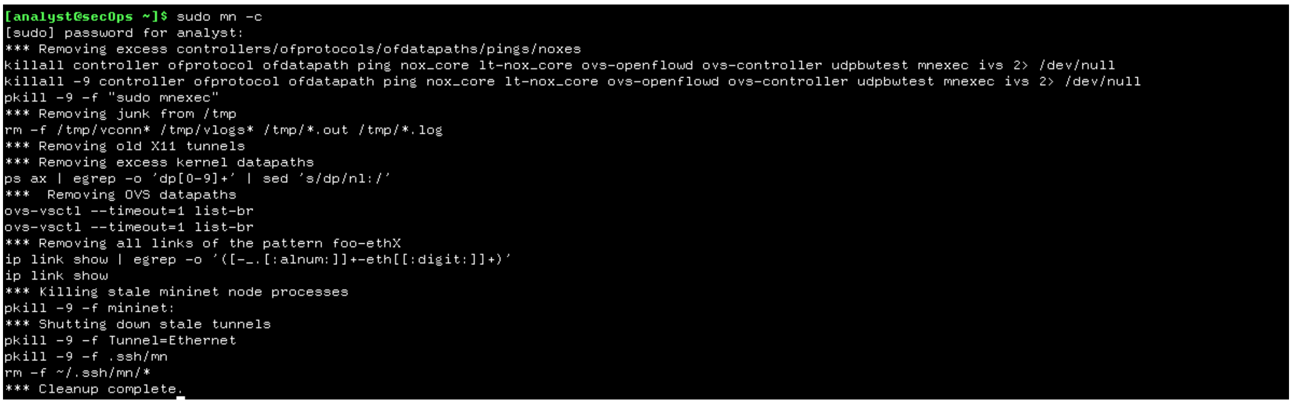


```
Frame 132: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: e6:24:1a:62:e8:44 (e6:24:1a:62:e8:44), Dst: ce:39:ad:9b:f6:14 (ce:39:ad:9b:f6:14)
Internet Protocol Version 4, Src: 10.0.0.11, Dst: 172.16.0.40
Transmission Control Protocol, Src Port: 38328, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 38328
    Destination Port: 80
    [Stream index: 1]
    [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]
```

View the packets using tcpdump



```
[analyst@secOps ~]$ tcpdump -r /home/analyst/capture.pcap -c 3
reading from file /home/analyst/capture.pcap, link-type EN10MB (Ethernet)
03:51:59.997639 IP secOps.38326 > 172.16.0.40.http: Flags [P.], seq 274819775:27
4820193, ack 1329984255, win 64, options [nop,nop,TS val 4228386018 ecr 34267659
3], length 418: HTTP: GET / HTTP/1.1
03:51:59.997760 IP 172.16.0.40.http > secOps.38326: Flags [P.], seq 1:181, ack 4
18, win 63, options [nop,nop,TS val 342684651 ecr 4228386018], length 180: HTTP:
 HTTP/1.1 304 Not Modified
03:51:59.997791 IP secOps.38326 > 172.16.0.40.http: Flags [.], ack 181, win 67,
options [nop,nop,TS val 4228386018 ecr 342684651], length 0
```



```
[analyst@secOps ~]$ sudo mn -c
[sudo] password for analyst:
*** Removing excess controllers/ofprotocols/ofdatapaths/pings/noxes
killall controller ofprotocol ofdatapath ping nox_core lt-nox_core ovs-openflowd ovs-controller udpbwtest mnexec ivs 2> /dev/null
killall -9 controller ofprotocol ofdatapath ping nox_core lt-nox_core ovs-openflowd ovs-controller udpbwtest mnexec ivs 2> /dev/null
pkill -9 -f "sudo mnexec"
*** Removing junk from /tmp
rm -f /tmp/vconn* /tmp/vlogs* /tmp/*.out /tmp/*.log
*** Removing old X11 tunnels
*** Removing excess kernel datapaths
ps ax | egrep -o 'dp[0-9]+' | sed 's/dp/nl:/'
***  Removing OVS datapaths
ovs-vsctl --timeout=1 list-br
ovs-vsctl --timeout=1 list-br
*** Removing all links of the pattern foo-ethX
ip link show | egrep -o '([-_.[:alnum:]]+-eth[[:digit:]]+)'
ip link show
*** Killing stale mininet node processes
pkill -9 -f mininet:
*** Shutting down stale tunnels
pkill -9 -f Tunnel=Ethernet
pkill -9 -f .ssh/mn
rm -f ~/.ssh/mn/*
*** Cleanup complete.
```