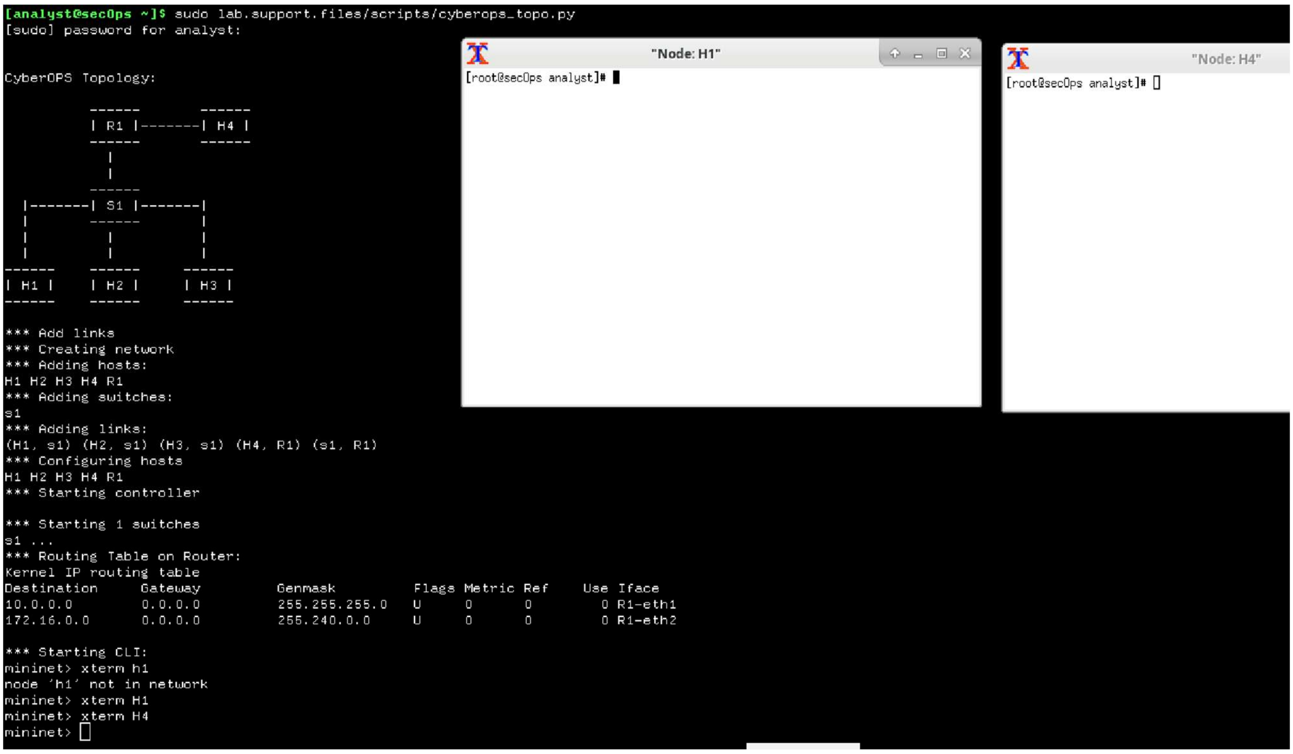
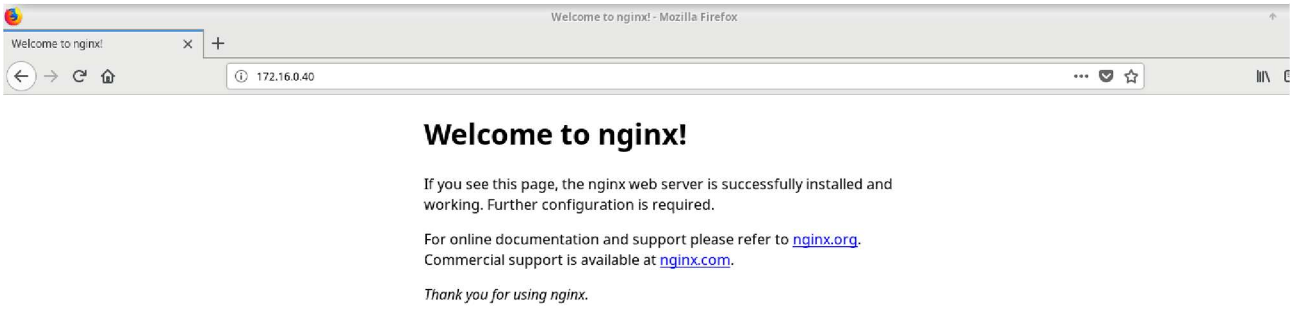
Parte 1) Avviamo la workstation e lanciamo i comandi come da guida:



```
[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
node 'h1' not in network
mininet> xterm H1
mininet> xterm H4
mininet> 
```

```
[root@secOps analyst]# 
```

```
[root@secOps analyst]# 
```

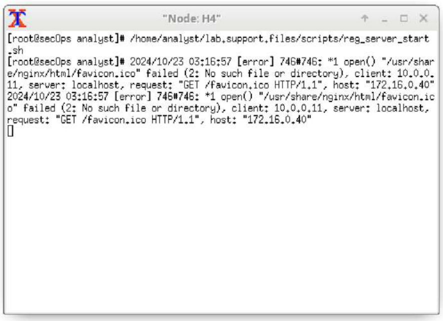


Welcome to nginx!

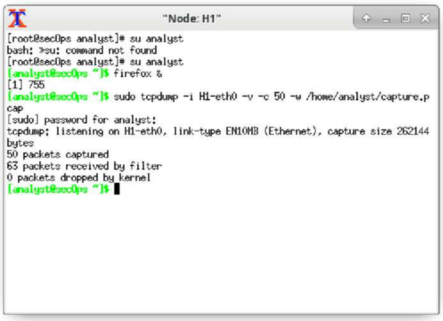
If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

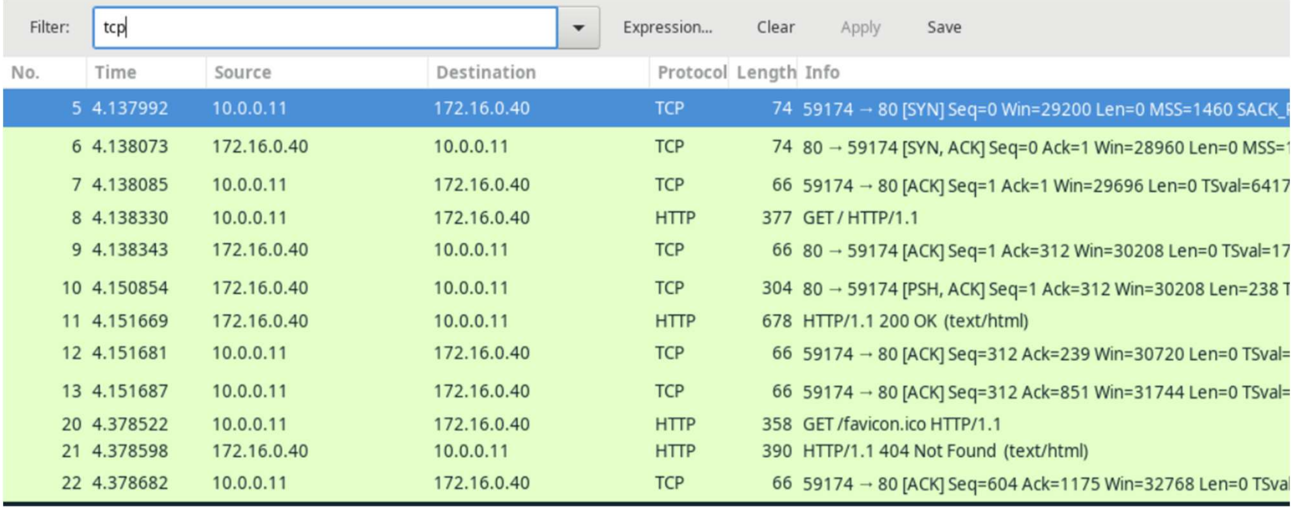


```
[root@secOps analyst]# /home/analyst/lab.support.files/scripts/reg_server_start
.sh
[root@secOps analyst]# 2024/10/23 03:16:57 [error] 746#746: *1 open() "/usr/shar
e/nginx/html/favicon.ico" failed (2: No such file or directory), client: 10.0.0.
11, server: localhost, request: "GET /favicon.ico HTTP/1.1", host: "172.16.0.40"
2024/10/23 03:16:57 [error] 746#746: *1 open() "/usr/share/nginx/html/favicon.ic
o" failed (2: No such file or directory), client: 10.0.0.11, server: localhost,
request: "GET /favicon.ico HTTP/1.1", host: "172.16.0.40"
```

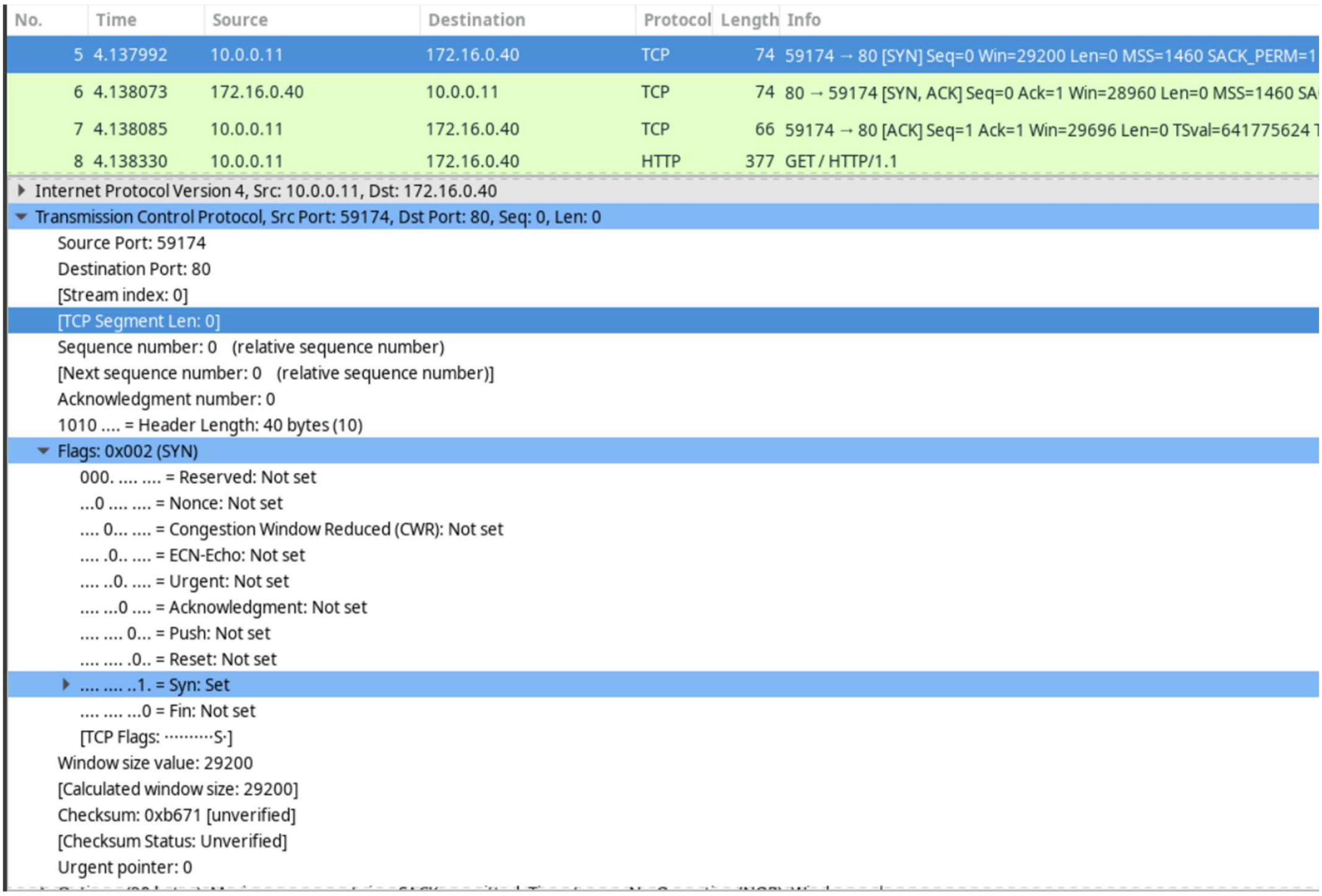


```
[root@secOps analyst]# su analyst
bash: »su: command not found
[root@secOps analyst]# su analyst
[analyst@secOps ~]$ firefox &
[1] 755
[analyst@secOps ~]$ sudo tcpdump -i H1-eth0 -v -c 50 -w /home/analyst/capture.p
cap
[sudo] password for analyst:
tcpdump: listening on H1-eth0, link-type EN10MB (Ethernet), capture size 262144
bytes
50 packets captured
63 packets received by filter
0 packets dropped by kernel
[analyst@secOps ~]$ 
```

Parte 2) carichiamo il file di output generato precedentemente su wireshark e applichiamo un filtro tcp:

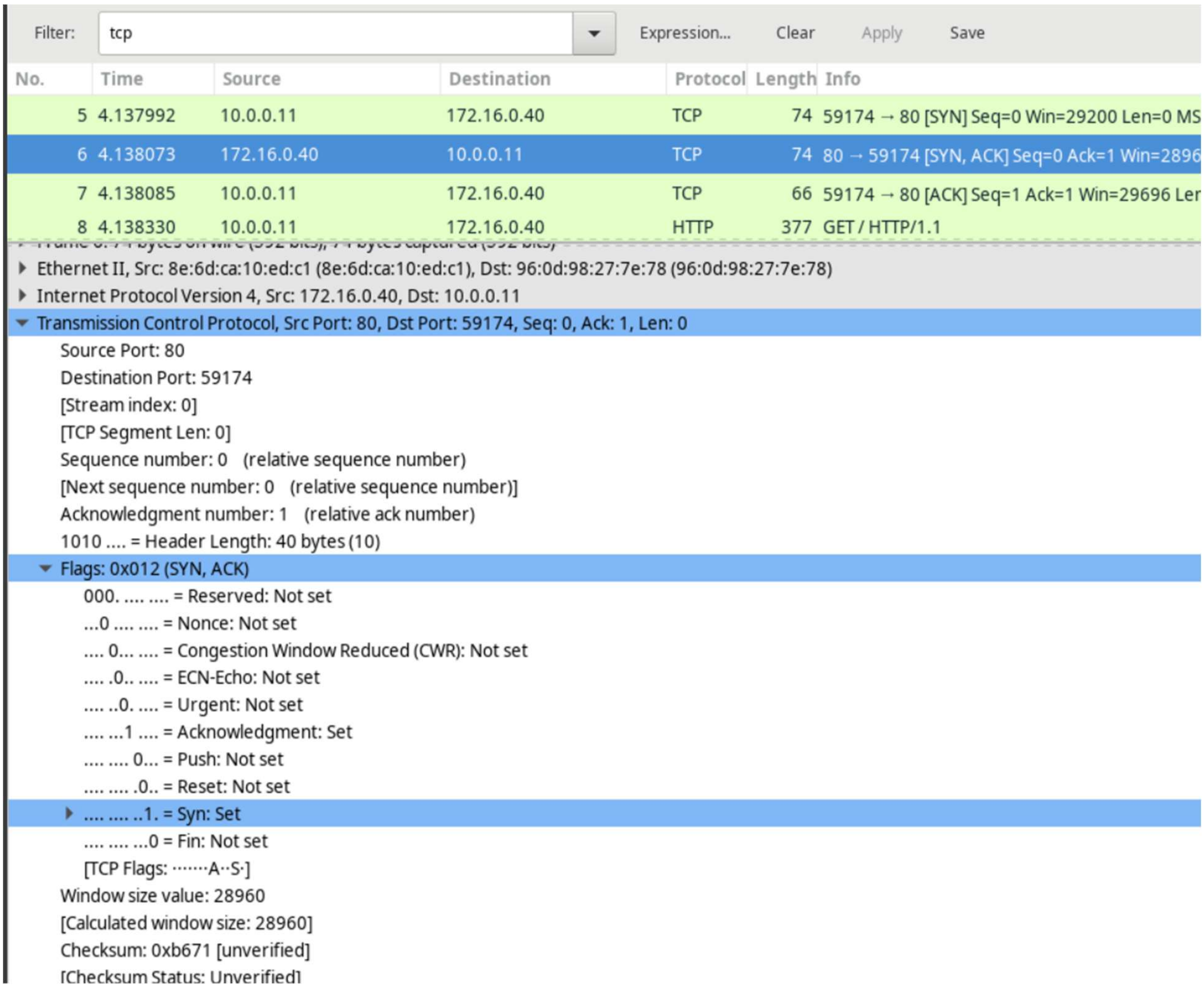


No.	Time	Source	Destination	Protocol	Length	Info
5	4.137992	10.0.0.11	172.16.0.40	TCP	74	59174 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_P
6	4.138073	172.16.0.40	10.0.0.11	TCP	74	80 → 59174 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1
7	4.138085	10.0.0.11	172.16.0.40	TCP	66	59174 → 80 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=6417
8	4.138330	10.0.0.11	172.16.0.40	HTTP	377	GET / HTTP/1.1
9	4.138343	172.16.0.40	10.0.0.11	TCP	66	80 → 59174 [ACK] Seq=1 Ack=312 Win=30208 Len=0 TSval=17
10	4.150854	172.16.0.40	10.0.0.11	TCP	304	80 → 59174 [PSH, ACK] Seq=1 Ack=312 Win=30208 Len=238 T
11	4.151669	172.16.0.40	10.0.0.11	HTTP	678	HTTP/1.1 200 OK (text/html)
12	4.151681	10.0.0.11	172.16.0.40	TCP	66	59174 → 80 [ACK] Seq=312 Ack=239 Win=30720 Len=0 TSval=
13	4.151687	10.0.0.11	172.16.0.40	TCP	66	59174 → 80 [ACK] Seq=312 Ack=851 Win=31744 Len=0 TSval=
20	4.378522	10.0.0.11	172.16.0.40	HTTP	358	GET /favicon.ico HTTP/1.1
21	4.378598	172.16.0.40	10.0.0.11	HTTP	390	HTTP/1.1 404 Not Found (text/html)
22	4.378682	10.0.0.11	172.16.0.40	TCP	66	59174 → 80 [ACK] Seq=604 Ack=1175 Win=32768 Len=0 TSval



No.	Time	Source	Destination	Protocol	Length	Info
5	4.137992	10.0.0.11	172.16.0.40	TCP	74	59174 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1
6	4.138073	172.16.0.40	10.0.0.11	TCP	74	80 → 59174 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SA
7	4.138085	10.0.0.11	172.16.0.40	TCP	66	59174 → 80 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=641775624 T
8	4.138330	10.0.0.11	172.16.0.40	HTTP	377	GET / HTTP/1.1

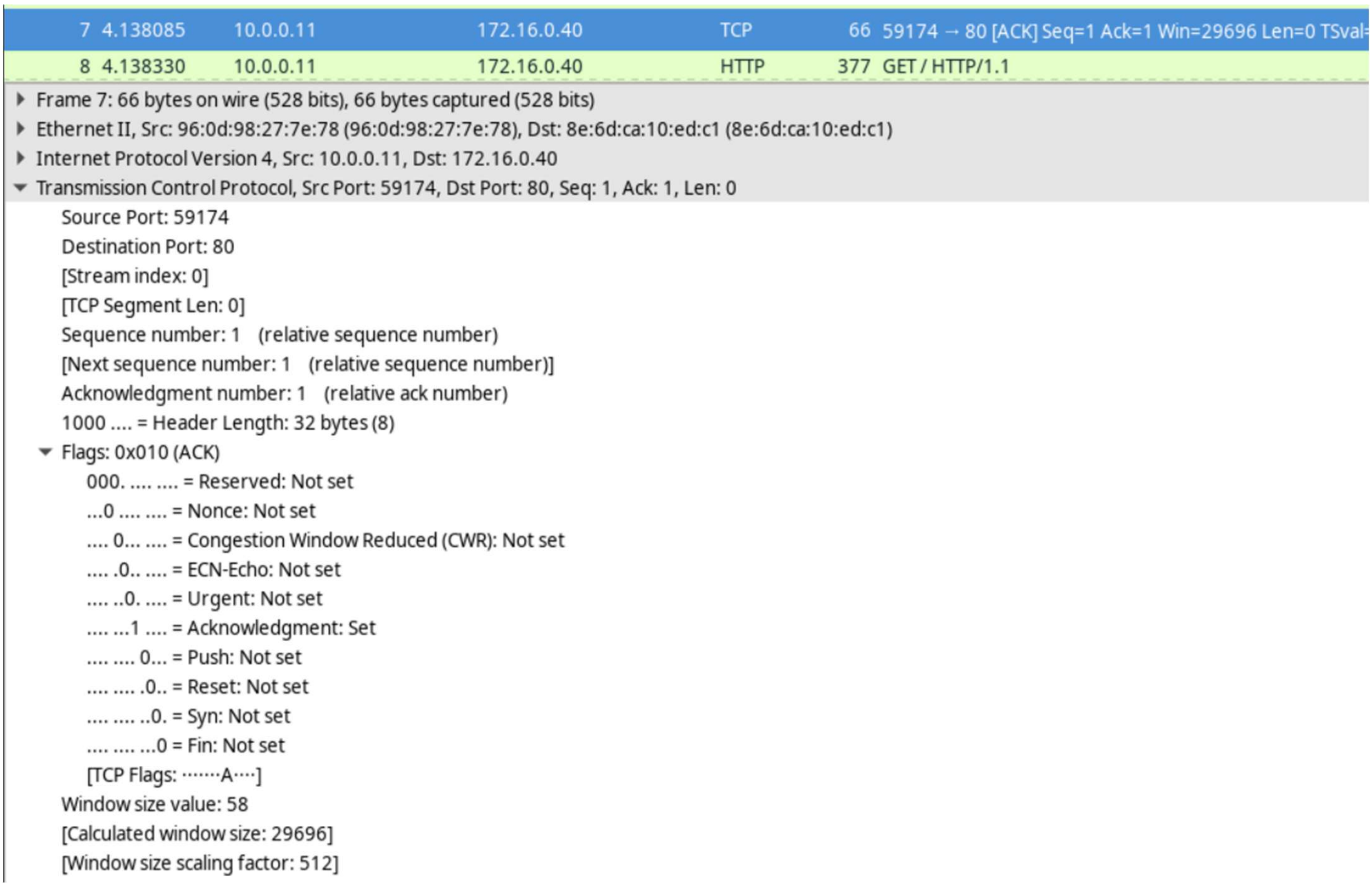
```
▸ Internet Protocol Version 4, Src: 10.0.0.11, Dst: 172.16.0.40
▾ Transmission Control Protocol, Src Port: 59174, Dst Port: 80, Seq: 0, Len: 0
      Source Port: 59174
      Destination Port: 80
      [Stream index: 0]
      [TCP Segment Len: 0]
      Sequence number: 0    (relative sequence number)
      [Next sequence number: 0    (relative sequence number)]
      Acknowledgment number: 0
      1010 .... = Header Length: 40 bytes (10)
    ▾ Flags: 0x002 (SYN)
          000. .... .... = Reserved: Not set
          ...0 .... .... = Nonce: Not set
          .... 0... .... = Congestion Window Reduced (CWR): Not set
          .... .0.. .... = ECN-Echo: Not set
          .... ..0. .... = Urgent: Not set
          .... ...0 .... = Acknowledgment: Not set
          .... .... 0... = Push: Not set
          .... .... .0.. = Reset: Not set
        ▸ .... .... ..1. = Syn: Set
          .... .... ...0 = Fin: Not set
          [TCP Flags: ··········S·]
      Window size value: 29200
      [Calculated window size: 29200]
      Checksum: 0xb671 [unverified]
      [Checksum Status: Unverified]
      Urgent pointer: 0
```



Filter: tcp

```
No.  Time      Source       Destination   Protocol Length Info
  5  4.137992  10.0.0.11    172.16.0.40   TCP        74   59174 → 80 [SYN] Seq=0 Win=29200 Len=0 MS
  6  4.138073  172.16.0.40  10.0.0.11     TCP        74   80 → 59174 [SYN, ACK] Seq=0 Ack=1 Win=2896
  7  4.138085  10.0.0.11    172.16.0.40   TCP        66   59174 → 80 [ACK] Seq=1 Ack=1 Win=29696 Ler
  8  4.138330  10.0.0.11    172.16.0.40   HTTP      377   GET / HTTP/1.1
```

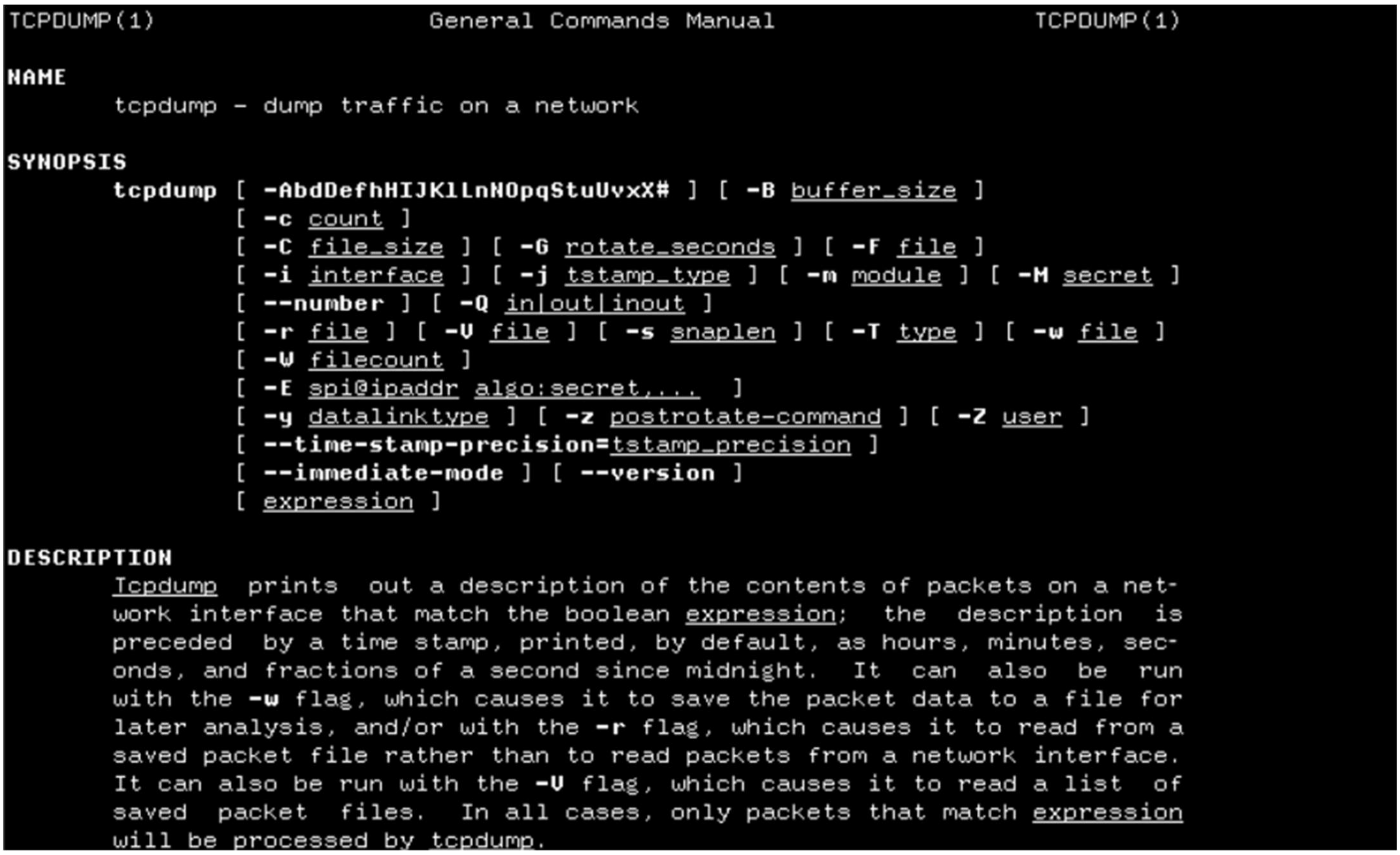
```
▸ Frame 6: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
▸ Ethernet II, Src: 8e:6d:ca:10:ed:c1 (8e:6d:ca:10:ed:c1), Dst: 96:0d:98:27:7e:78 (96:0d:98:27:7e:78)
▸ Internet Protocol Version 4, Src: 172.16.0.40, Dst: 10.0.0.11
▾ Transmission Control Protocol, Src Port: 80, Dst Port: 59174, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 59174
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    1010 .... = Header Length: 40 bytes (10)
  ▾ Flags: 0x012 (SYN, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    ▸ .... .... ..1. = Syn: Set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·······A··S·]
    Window size value: 28960
    [Calculated window size: 28960]
    Checksum: 0xb671 [unverified]
    [Checksum Status: Unverified]
```



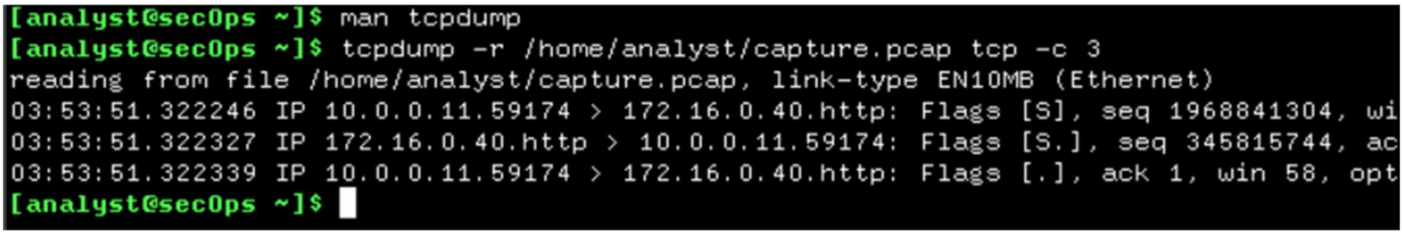
```
  7  4.138085  10.0.0.11    172.16.0.40   TCP        66   59174 → 80 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=
  8  4.138330  10.0.0.11    172.16.0.40   HTTP      377   GET / HTTP/1.1
```

```
▸ Frame 7: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
▸ Ethernet II, Src: 96:0d:98:27:7e:78 (96:0d:98:27:7e:78), Dst: 8e:6d:ca:10:ed:c1 (8e:6d:ca:10:ed:c1)
▸ Internet Protocol Version 4, Src: 10.0.0.11, Dst: 172.16.0.40
▾ Transmission Control Protocol, Src Port: 59174, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
    Source Port: 59174
    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)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·······A····]
    Window size value: 58
    [Calculated window size: 29696]
    [Window size scaling factor: 512]
```

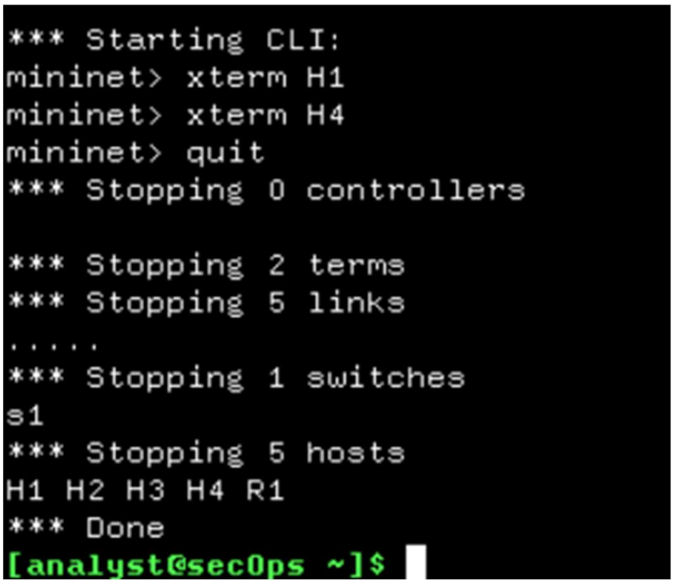
Parte 3)



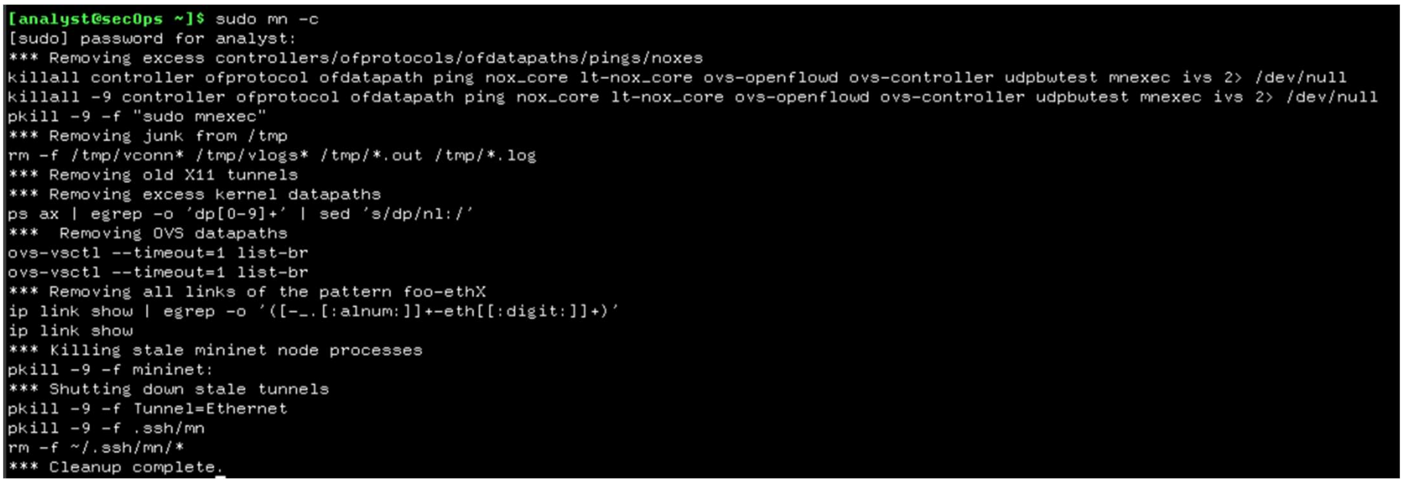
```
TCPDUMP(1)                    General Commands Manual                   TCPDUMP(1)

NAME
       tcpdump - dump traffic on a network

SYNOPSIS
       tcpdump [ -AbdDefhHIJKlLnNOpqStuUvxX# ] [ -B buffer_size ]
               [ -c count ]
               [ -C file_size ] [ -G rotate_seconds ] [ -F file ]
               [ -i interface ] [ -j tstamp_type ] [ -m module ] [ -M secret ]
               [ --number ] [ -Q in|out|inout ]
               [ -r file ] [ -V file ] [ -s snaplen ] [ -T type ] [ -w file ]
               [ -W filecount ]
               [ -E spi@ipaddr algo:secret,...  ]
               [ -y datalinktype ] [ -z postrotate-command ] [ -Z user ]
               [ --time-stamp-precision=tstamp_precision ]
               [ --immediate-mode ] [ --version ]
               [ expression ]

DESCRIPTION
       Tcpdump  prints  out a description of the contents of packets on a net-
       work interface that match the boolean expression;  the  description  is
       preceded  by a time stamp, printed, by default, as hours, minutes, sec-
       onds, and fractions of a second since midnight.  It  can  also  be  run
       with the -w flag, which causes it to save the packet data to a file for
       later analysis, and/or with the -r flag, which causes it to read from a
       saved packet file rather than to read packets from a network interface.
       It can also be run with the -V flag, which causes it to read a list  of
       saved  packet  files.  In all cases, only packets that match expression
       will be processed by tcpdump.
```



```
[analyst@secOps ~]$ man tcpdump
[analyst@secOps ~]$ tcpdump -r /home/analyst/capture.pcap tcp -c 3
reading from file /home/analyst/capture.pcap, link-type EN10MB (Ethernet)
03:53:51.322246 IP 10.0.0.11.59174 > 172.16.0.40.http: Flags [S], seq 1968841304, wi
03:53:51.322327 IP 172.16.0.40.http > 10.0.0.11.59174: Flags [S.], seq 345815744, ac
03:53:51.322339 IP 10.0.0.11.59174 > 172.16.0.40.http: Flags [.], ack 1, win 58, opt
[analyst@secOps ~]$ 
```



```
*** Starting CLI:
mininet> xterm H1
mininet> xterm H4
mininet> quit
*** Stopping 0 controllers

*** Stopping 2 terms
*** Stopping 5 links
.....
*** Stopping 1 switches
s1
*** Stopping 5 hosts
H1 H2 H3 H4 R1
*** Done
[analyst@secOps ~]$ 
```



```
[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 minimet 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.
```

BONUS)

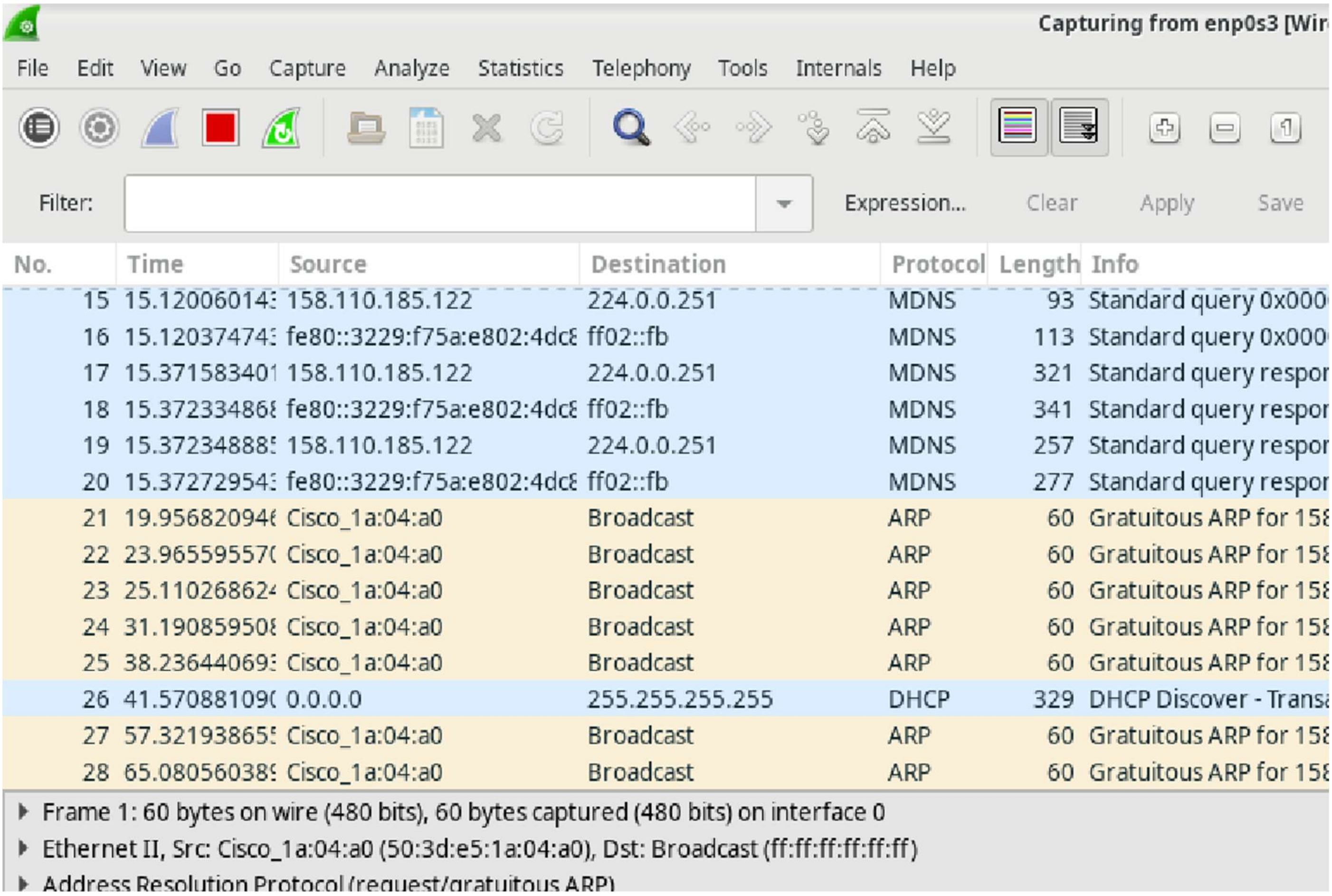
Per poter vedere l’interfaccia abbiamo dovuto usare questi comandi:

sudo chgrp wireshark /usr/bin/dumpcap

sudo chmod 750 /usr/bin/dumpcap

sudo setcap cap_net_raw,cap_net_admin=eip /usr/bin/dumpcap

sudo usermod -a -G wireshark $USER

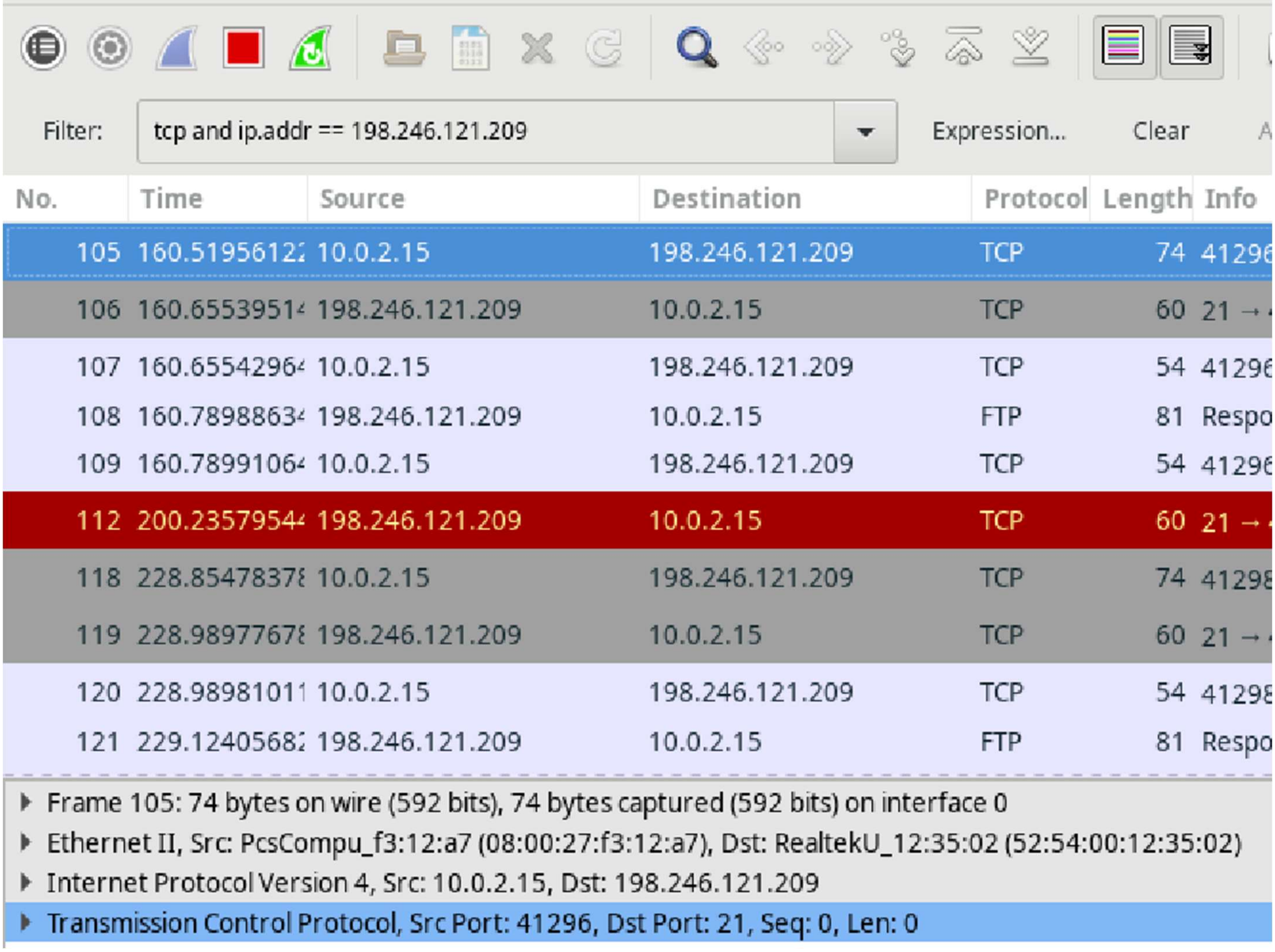


No.	Time	Source	Destination	Protocol	Length	Info
15	15.12006014:	158.110.185.122	224.0.0.251	MDNS	93	Standard query 0x000
16	15.12037474:	fe80::3229:f75a:e802:4dc8	ff02::fb	MDNS	113	Standard query 0x000
17	15.371583401	158.110.185.122	224.0.0.251	MDNS	321	Standard query respor
18	15.37233486{	fe80::3229:f75a:e802:4dc8	ff02::fb	MDNS	341	Standard query respor
19	15.37234888!	158.110.185.122	224.0.0.251	MDNS	257	Standard query respor
20	15.37272954:	fe80::3229:f75a:e802:4dc8	ff02::fb	MDNS	277	Standard query respor
21	19.95682094(	Cisco_1a:04:a0	Broadcast	ARP	60	Gratuitous ARP for 158
22	23.96559557(	Cisco_1a:04:a0	Broadcast	ARP	60	Gratuitous ARP for 158
23	25.11026862‹	Cisco_1a:04:a0	Broadcast	ARP	60	Gratuitous ARP for 158
24	31.19085950{	Cisco_1a:04:a0	Broadcast	ARP	60	Gratuitous ARP for 158
25	38.23644069:	Cisco_1a:04:a0	Broadcast	ARP	60	Gratuitous ARP for 158
26	41.57088109(	0.0.0.0	255.255.255.255	DHCP	329	DHCP Discover - Transa
27	57.32193865!	Cisco_1a:04:a0	Broadcast	ARP	60	Gratuitous ARP for 158
28	65.08056038!	Cisco_1a:04:a0	Broadcast	ARP	60	Gratuitous ARP for 158

▸ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

▸ Ethernet II, Src: Cisco_1a:04:a0 (50:3d:e5:1a:04:a0), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

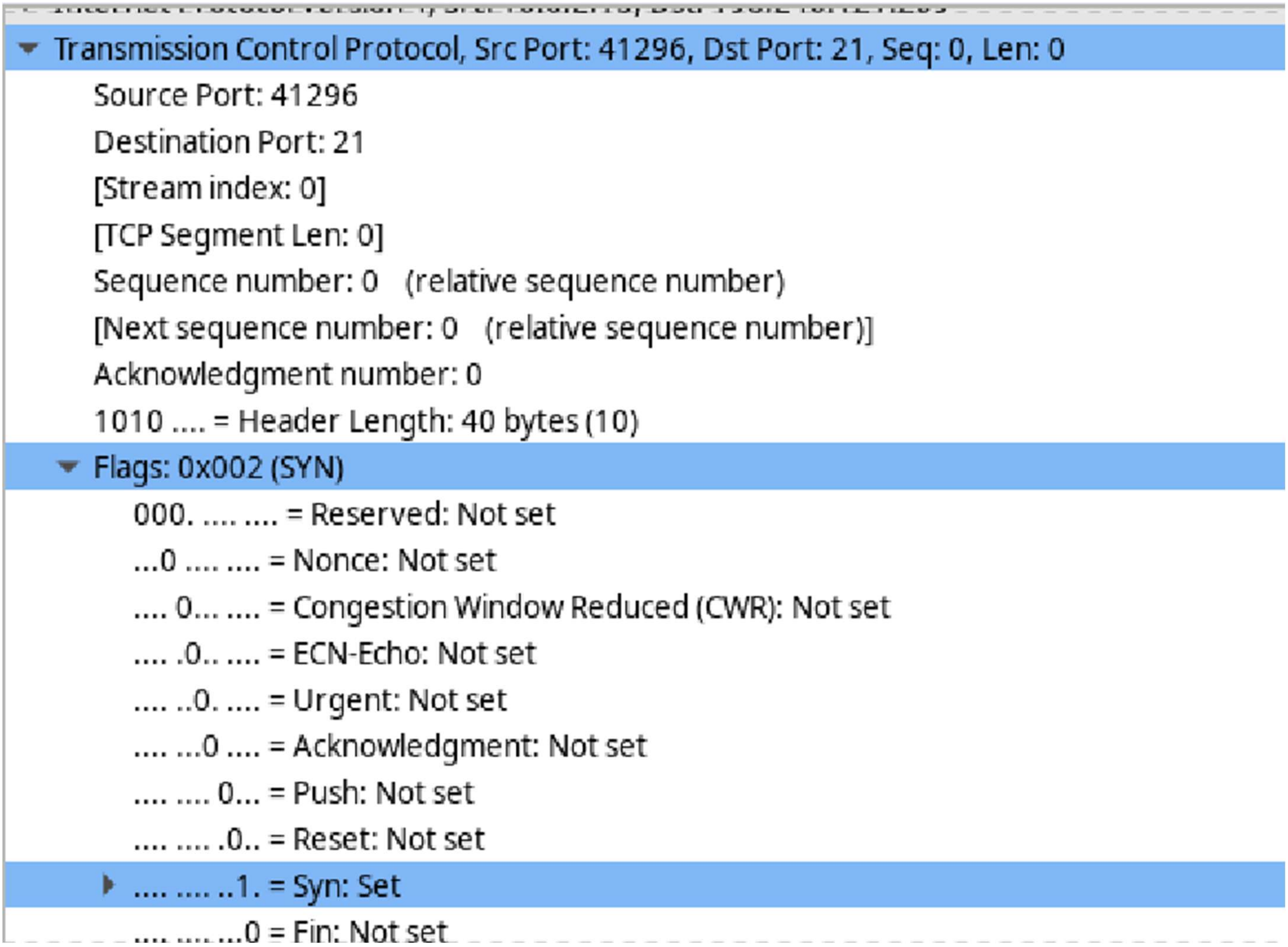
▸ Address Resolution Protocol (request/gratuitous ARP)



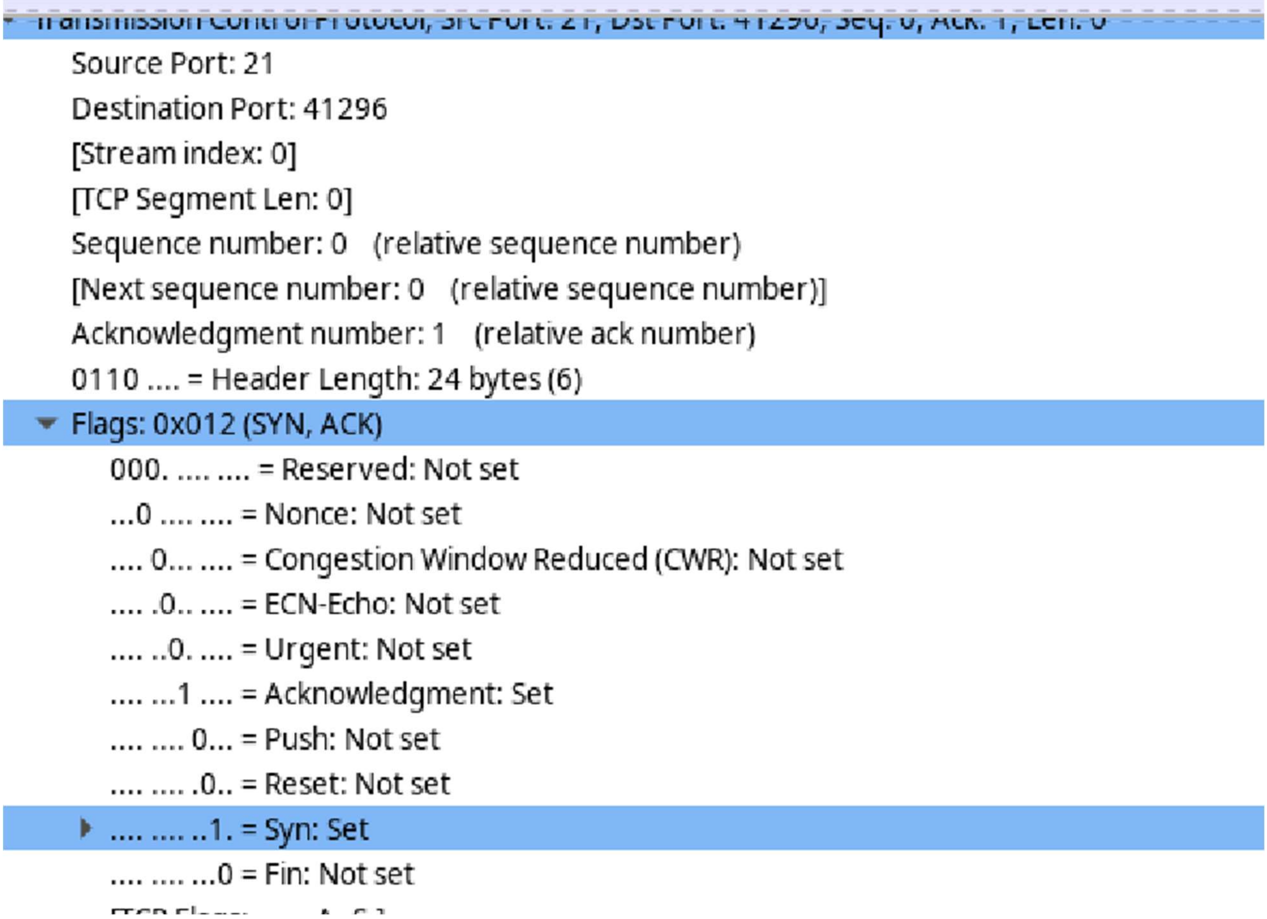
Filter: tcp and ip.addr == 198.246.121.209

No.	Time	Source	Destination	Protocol	Length	Info
105	160.5195612	10.0.2.15	198.246.121.209	TCP	74	41296
106	160.6553951	198.246.121.209	10.0.2.15	TCP	60	21 →
107	160.6554296	10.0.2.15	198.246.121.209	TCP	54	41296
108	160.7898863	198.246.121.209	10.0.2.15	FTP	81	Respo
109	160.7899106	10.0.2.15	198.246.121.209	TCP	54	41296
112	200.2357954	198.246.121.209	10.0.2.15	TCP	60	21 →
118	228.8547837	10.0.2.15	198.246.121.209	TCP	74	41298
119	228.9897767	198.246.121.209	10.0.2.15	TCP	60	21 →
120	228.9898101	10.0.2.15	198.246.121.209	TCP	54	41298
121	229.1240568	198.246.121.209	10.0.2.15	FTP	81	Respo

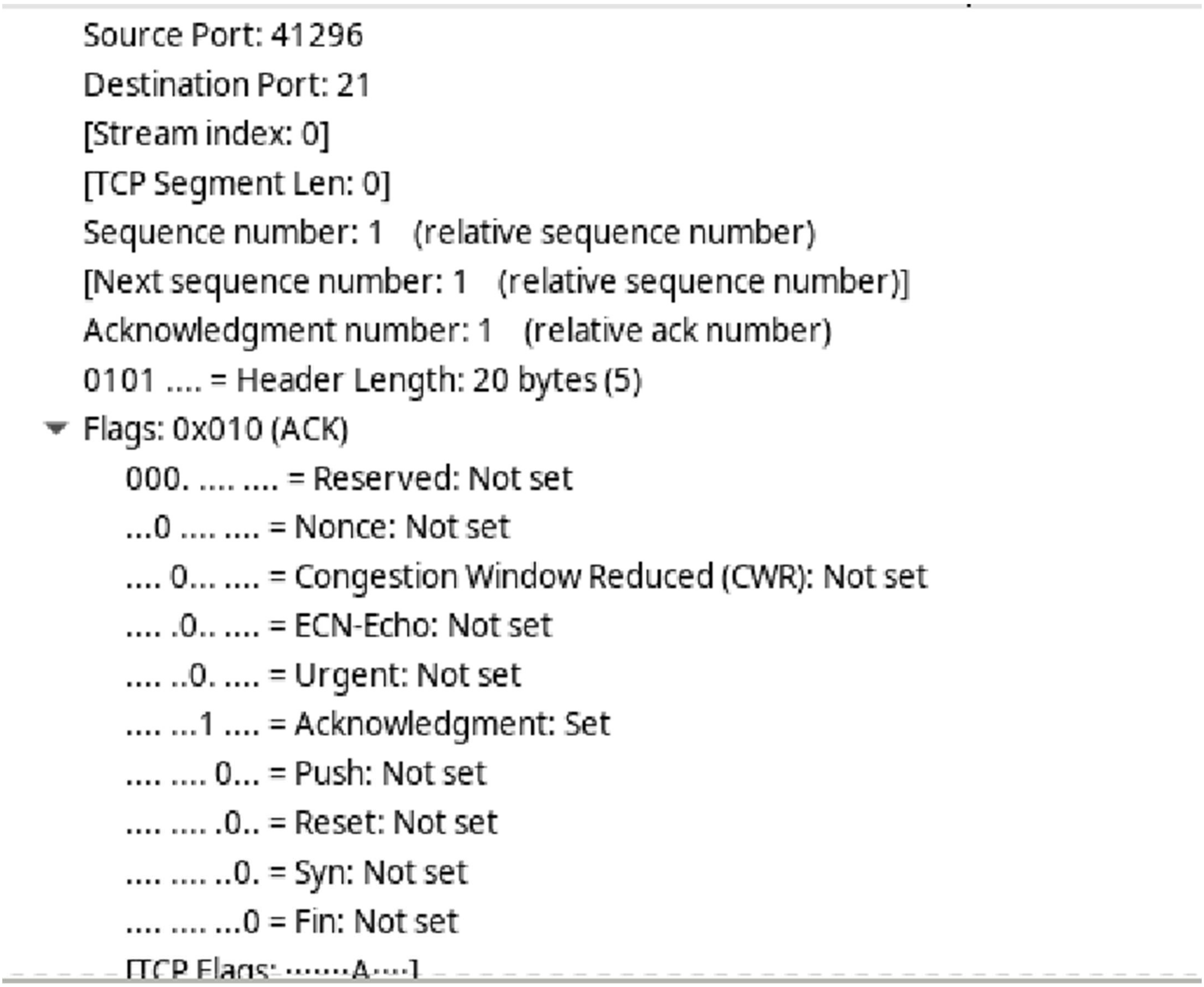
- Frame 105: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
- Ethernet II, Src: PcsCompu_f3:12:a7 (08:00:27:f3:12:a7), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
- Internet Protocol Version 4, Src: 10.0.2.15, Dst: 198.246.121.209
- Transmission Control Protocol, Src Port: 41296, Dst Port: 21, Seq: 0, Len: 0



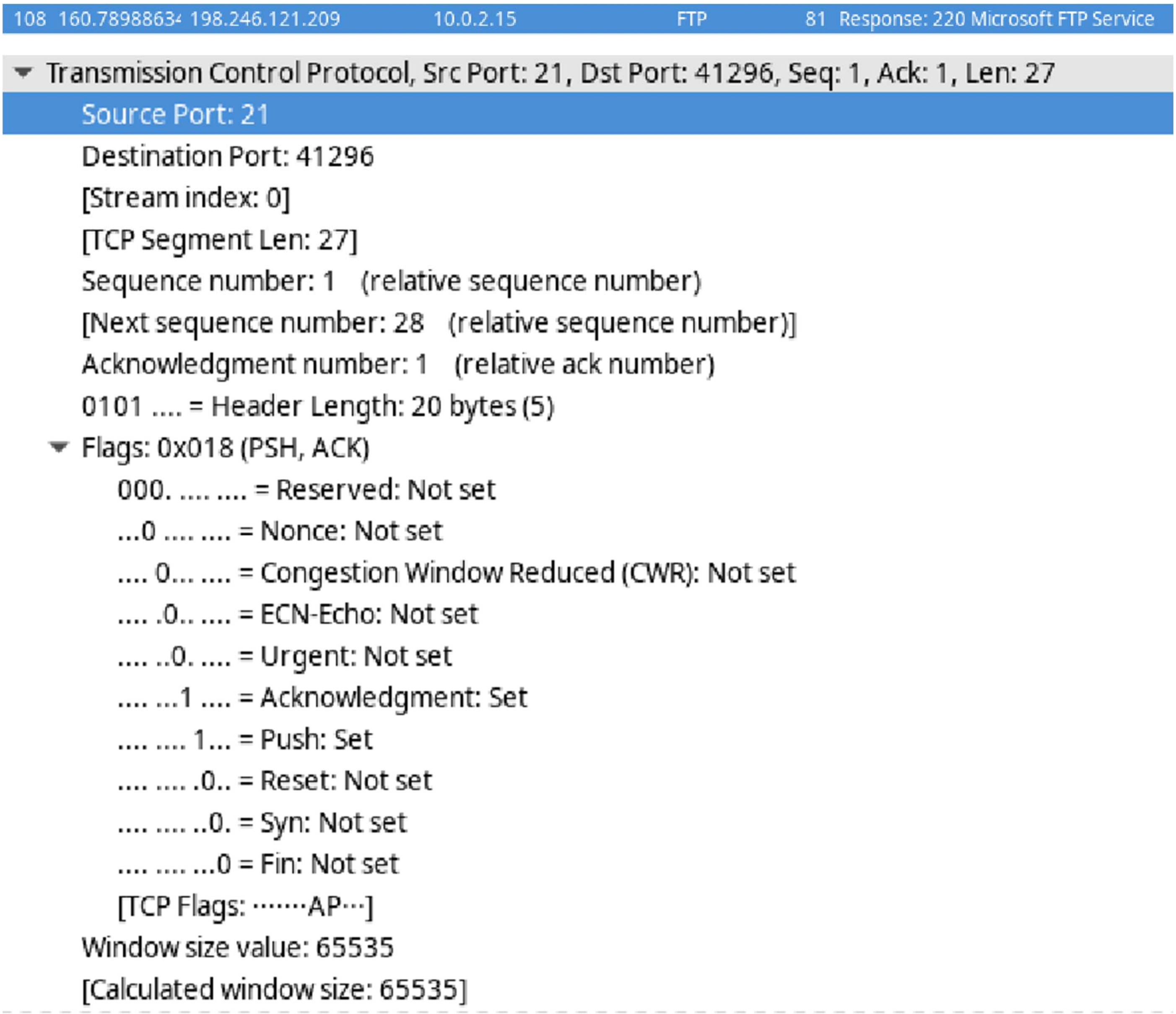
```
Transmission Control Protocol, Src Port: 41296, Dst Port: 21, Seq: 0, Len: 0
    Source Port: 41296
    Destination Port: 21
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 0
    1010 .... = Header Length: 40 bytes (10)
    Flags: 0x002 (SYN)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...0 .... = Acknowledgment: Not set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..1. = Syn: Set
        .... .... ...0 = Fin: Not set
```



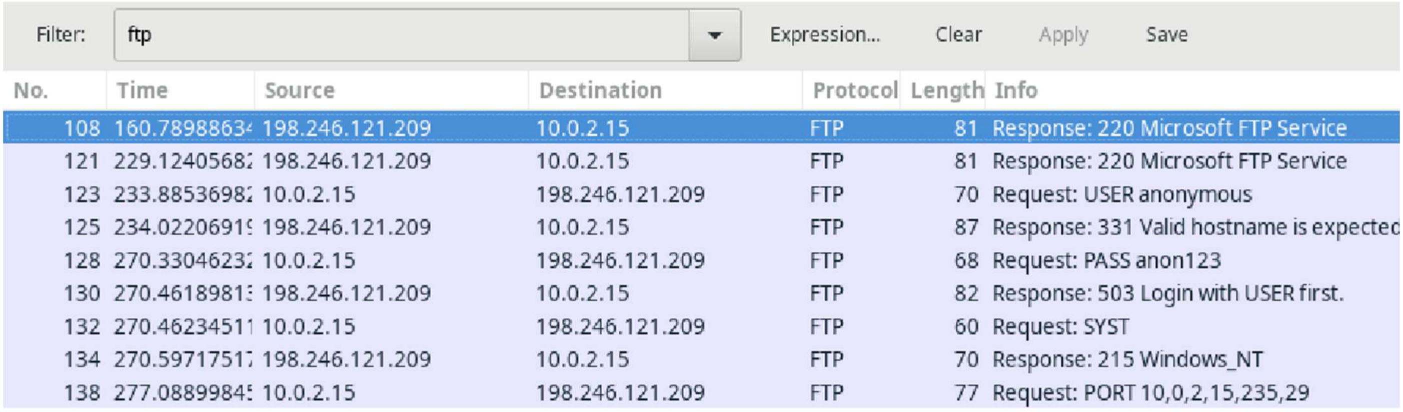
```
Transmission Control Protocol, Src Port: 21, Dst Port: 41296, Seq: 0, Ack: 1, Len: 0
    Source Port: 21
    Destination Port: 41296
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0110 .... = Header Length: 24 bytes (6)
    Flags: 0x012 (SYN, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..1. = Syn: Set
        .... .... ...0 = Fin: Not set
```



```
    Source Port: 41296
    Destination Port: 21
    [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)
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x010 (ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
        [TCP Flags: ·······A····]
```

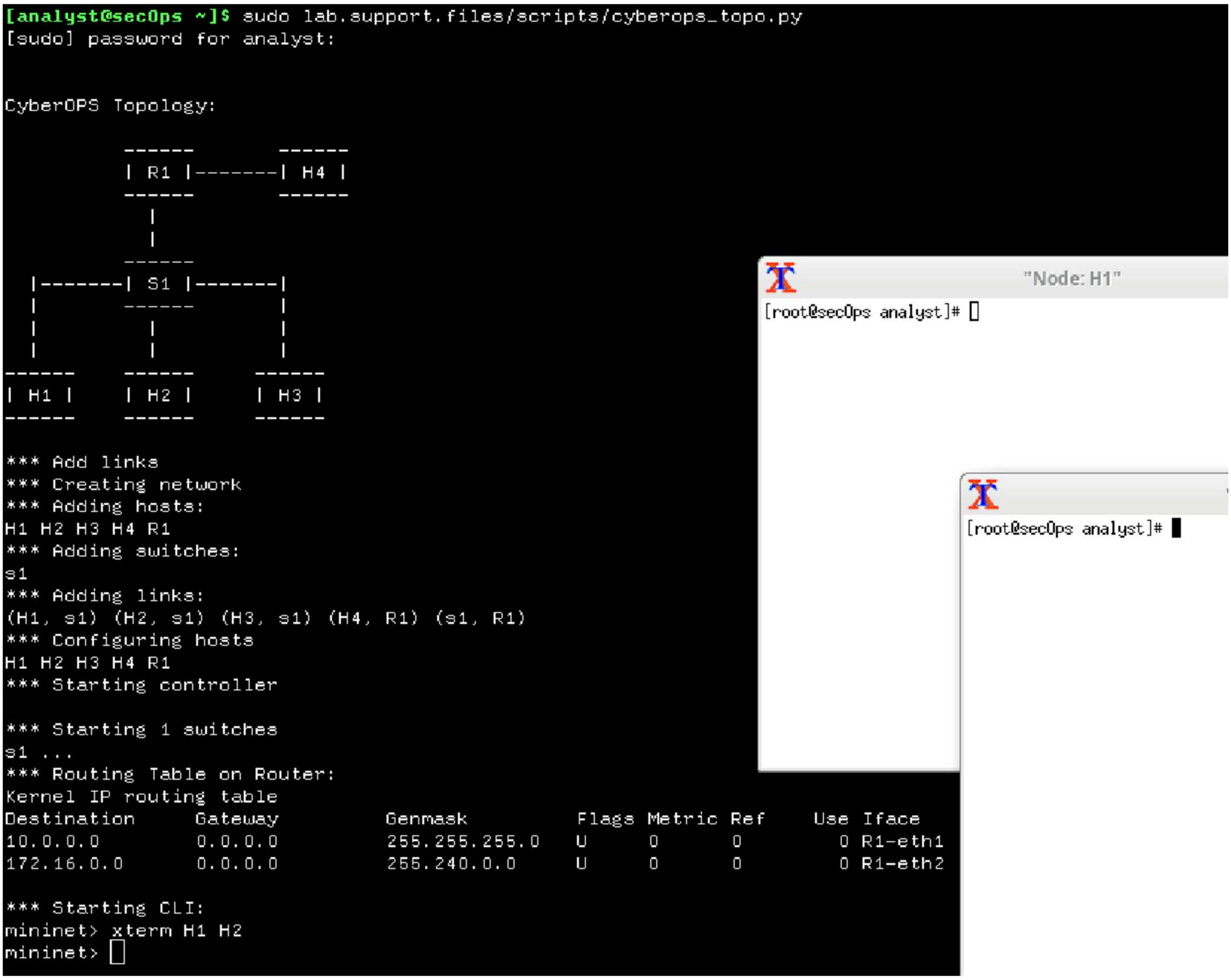


```
108  160.7898863⁴ 198.246.121.209        10.0.2.15        FTP        81  Response: 220 Microsoft FTP Service

▼ Transmission Control Protocol, Src Port: 21, Dst Port: 41296, Seq: 1, Ack: 1, Len: 27
      Source Port: 21
      Destination Port: 41296
      [Stream index: 0]
      [TCP Segment Len: 27]
      Sequence number: 1    (relative sequence number)
      [Next sequence number: 28    (relative sequence number)]
      Acknowledgment number: 1    (relative ack number)
      0101 .... = Header Length: 20 bytes (5)
    ▼ Flags: 0x018 (PSH, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 1... = Push: Set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
        [TCP Flags: ·······AP···]
      Window size value: 65535
      [Calculated window size: 65535]
```



```
Filter: ftp

No.   Time          Source            Destination       Protocol Length Info
  108 160.7898863⁴  198.246.121.209   10.0.2.15         FTP         81  Response: 220 Microsoft FTP Service
  121 229.1240568²  198.246.121.209   10.0.2.15         FTP         81  Response: 220 Microsoft FTP Service
  123 233.8853698²  10.0.2.15         198.246.121.209   FTP         70  Request: USER anonymous
  125 234.0220691⁹  198.246.121.209   10.0.2.15         FTP         87  Response: 331 Valid hostname is expected
  128 270.3304623²  10.0.2.15         198.246.121.209   FTP         68  Request: PASS anon123
  130 270.4618981³  198.246.121.209   10.0.2.15         FTP         82  Response: 503 Login with USER first.
  132 270.4623451¹  10.0.2.15         198.246.121.209   FTP         60  Request: SYST
  134 270.5971751⁷  198.246.121.209   10.0.2.15         FTP         70  Response: 215 Windows_NT
  138 277.0889984⁵  10.0.2.15         198.246.121.209   FTP         77  Request: PORT 10,0,2,15,235,29
```

PARTE 2)

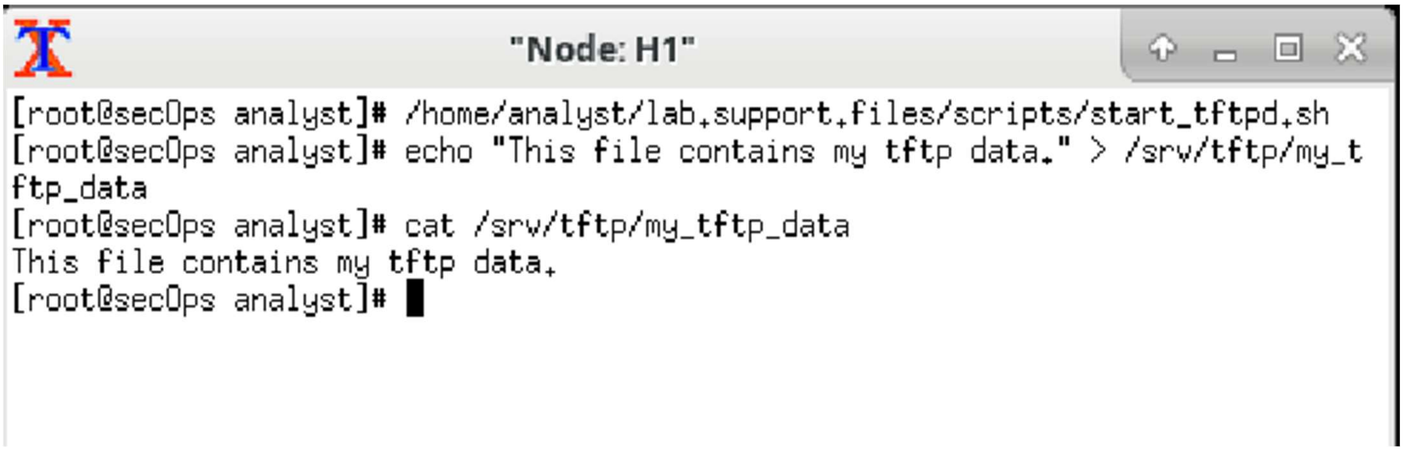


```
[analyst@secOps ~]$ sudo lab.support.files/scripts/cyberops_topo.py
[sudo] password for analyst:


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 H2
mininet> 
```

"Node: H1"

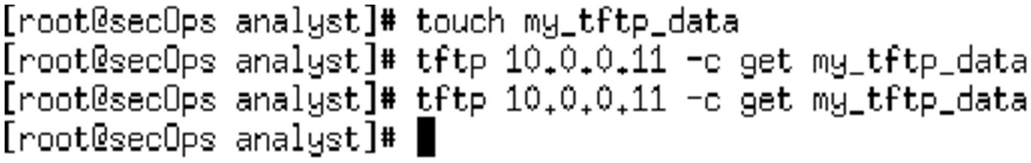
```
[root@secOps analyst]# 
```

```
[root@secOps analyst]# 
```

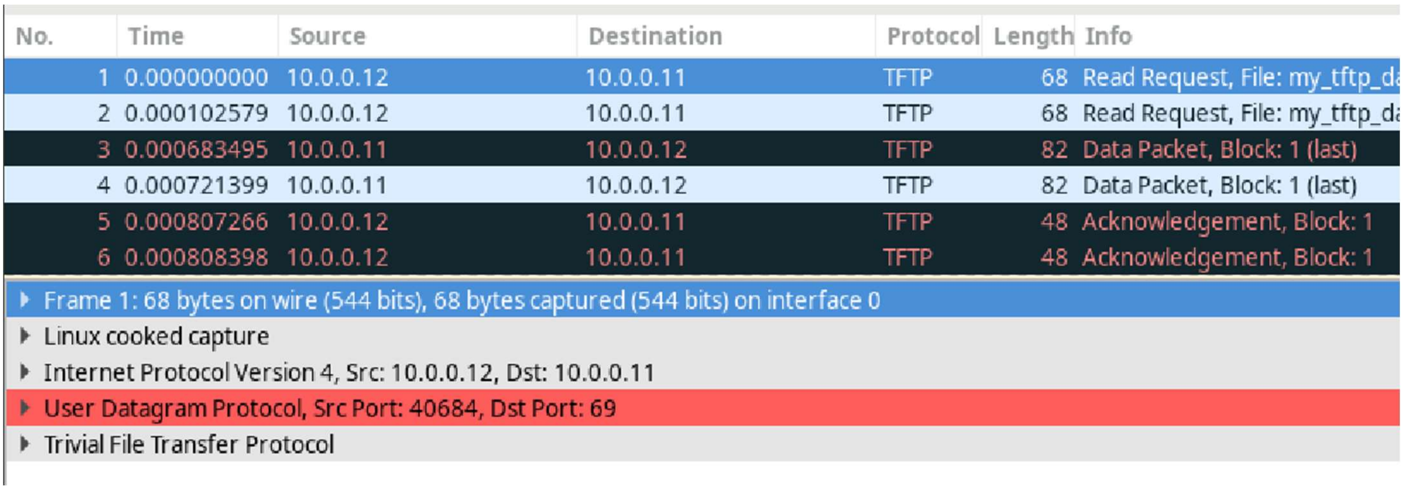


"Node: H1"

```
[root@secOps analyst]# /home/analyst/lab.support.files/scripts/start_tftpd.sh
[root@secOps analyst]# echo "This file contains my tftp data." > /srv/tftp/my_t
ftp_data
[root@secOps analyst]# cat /srv/tftp/my_tftp_data
This file contains my tftp data.
[root@secOps analyst]# 
```

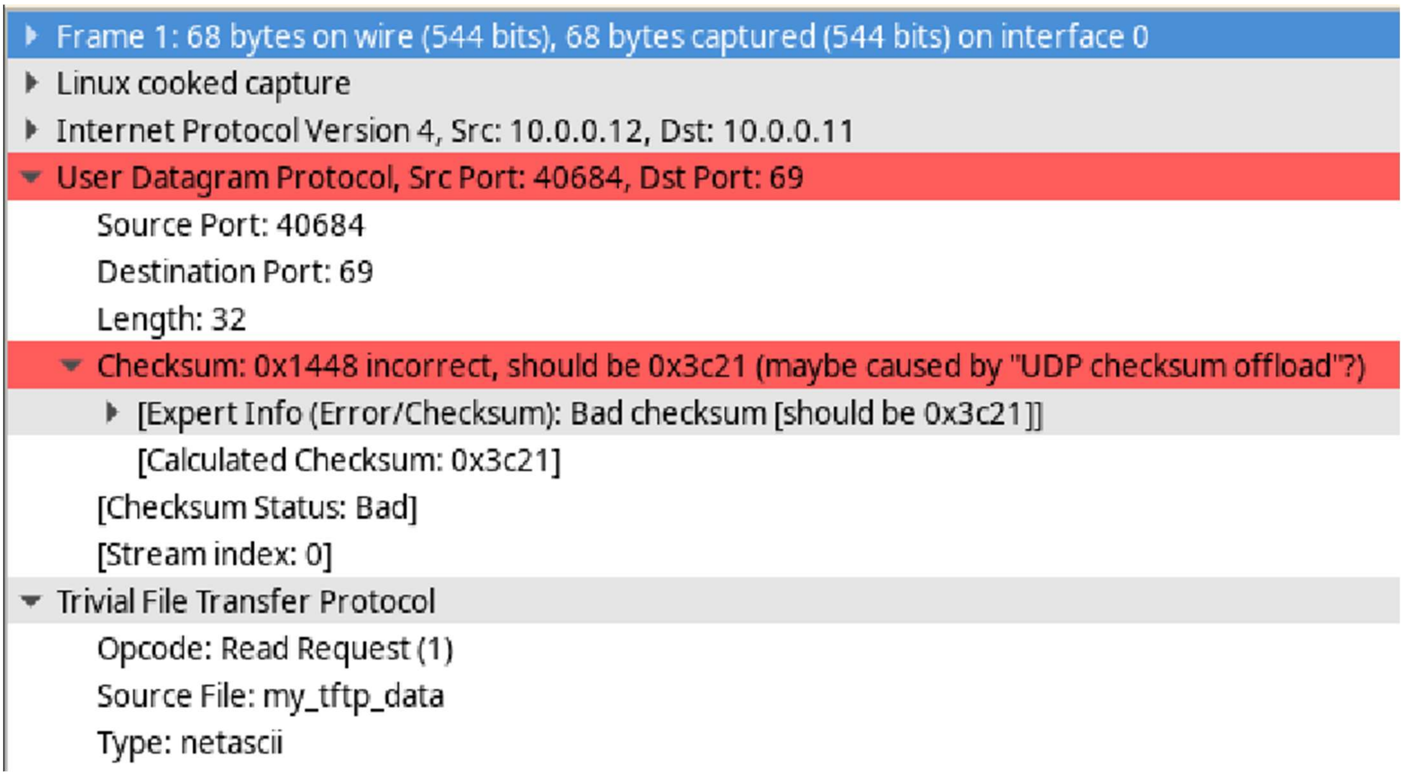


```
[root@secOps analyst]# touch my_tftp_data
[root@secOps analyst]# tftp 10.0.0.11 -c get my_tftp_data
[root@secOps analyst]# tftp 10.0.0.11 -c get my_tftp_data
[root@secOps analyst]# 
```

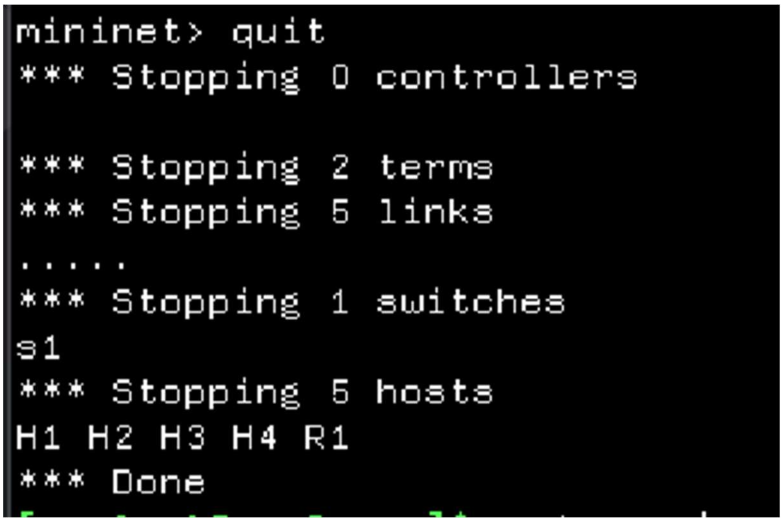


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.0.12	10.0.0.11	TFTP	68	Read Request, File: my_tftp_da
2	0.000102579	10.0.0.12	10.0.0.11	TFTP	68	Read Request, File: my_tftp_da
3	0.000683495	10.0.0.11	10.0.0.12	TFTP	82	Data Packet, Block: 1 (last)
4	0.000721399	10.0.0.11	10.0.0.12	TFTP	82	Data Packet, Block: 1 (last)
5	0.000807266	10.0.0.12	10.0.0.11	TFTP	48	Acknowledgement, Block: 1
6	0.000808398	10.0.0.12	10.0.0.11	TFTP	48	Acknowledgement, Block: 1

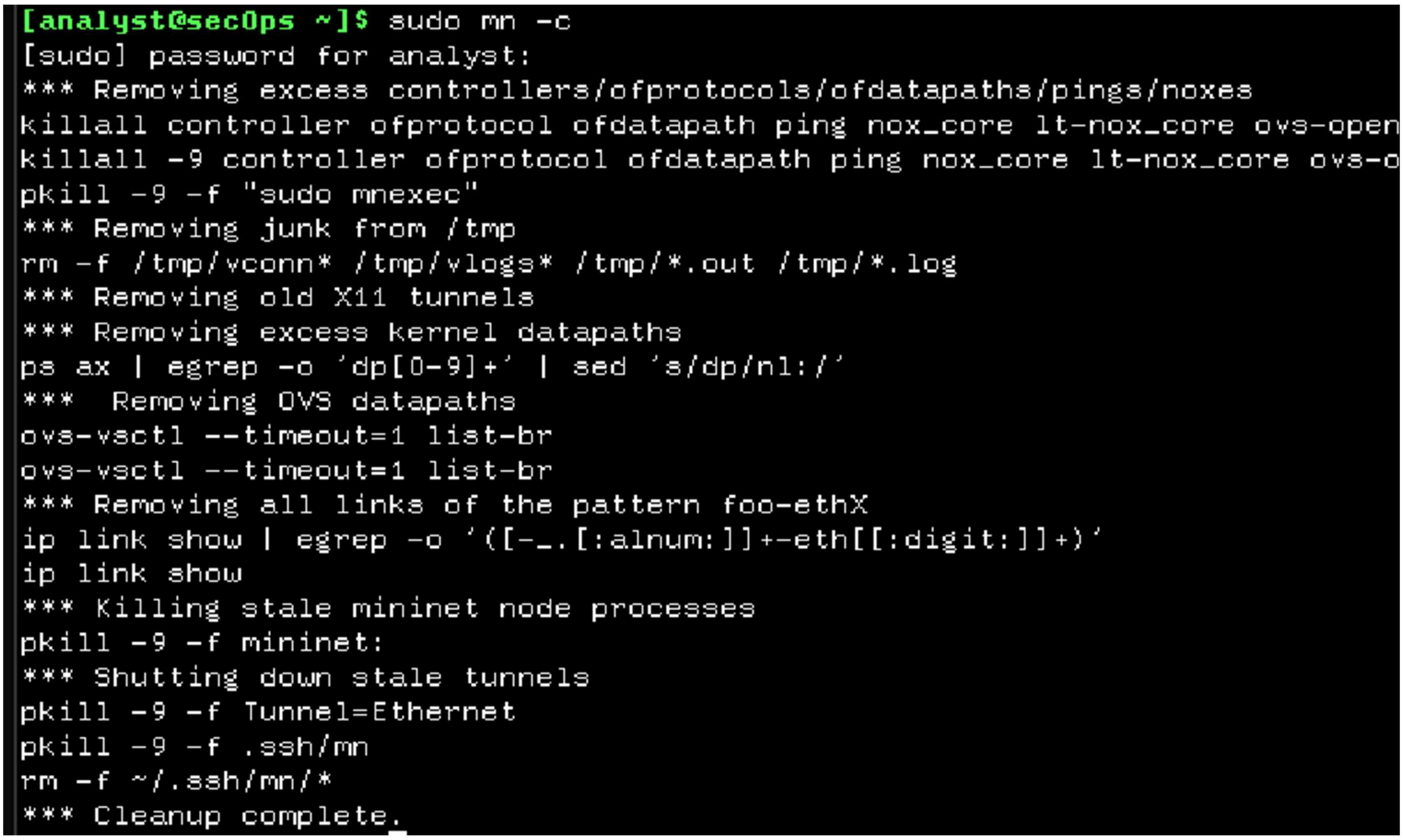
```
▸ Frame 1: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 10.0.0.12, Dst: 10.0.0.11
▸ User Datagram Protocol, Src Port: 40684, Dst Port: 69
▸ Trivial File Transfer Protocol
```



```
▸ Frame 1: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 10.0.0.12, Dst: 10.0.0.11
▾ User Datagram Protocol, Src Port: 40684, Dst Port: 69
    Source Port: 40684
    Destination Port: 69
    Length: 32
  ▾ Checksum: 0x1448 incorrect, should be 0x3c21 (maybe caused by "UDP checksum offload"?)
    ▸ [Expert Info (Error/Checksum): Bad checksum [should be 0x3c21]]
      [Calculated Checksum: 0x3c21]
    [Checksum Status: Bad]
    [Stream index: 0]
▾ Trivial File Transfer Protocol
    Opcode: Read Request (1)
    Source File: my_tftp_data
    Type: netascii
```



```
mininet> quit
*** Stopping 0 controllers

*** Stopping 2 terms
*** Stopping 5 links
.....
*** Stopping 1 switches
s1
*** Stopping 5 hosts
H1 H2 H3 H4 R1
*** Done
```



```
[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-open
killall -9 controller ofprotocol ofdatapath ping nox_core lt-nox_core ovs-o
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.
```