Report Laboratorio – Cisco CyberOps Giorno 2

Obiettivi

Questo laboratorio ha come obiettivo l'analisi del funzionamento dell'handshake TCP a tre vie e della terminazione della connessione, utilizzando strumenti di cattura e analisi del traffico come Wireshark e tcpdump. Inoltre, si è osservata la presenza di protocolli di supporto (ARP, DNS, ICMP) che completano lo scenario.

Scenario

Il laboratorio prevede un client H1 che si collega al server H4 tramite il browser Firefox. Il server web è attivo sulla porta 80 (HTTP). La cattura del traffico è stata effettuata con tcpdump e successivamente analizzata in Wireshark.

Apertura della Connessione TCP (Handshake a 3 vie)

Durante l'handshake TCP sono stati osservati tre pacchetti fondamentali:

1. SYN – Inviato dal client (porta effimera 40856) al server (porta 80).

2. SYN-ACK – Risposta del server verso il client.

3. ACK – Conferma del client. La connessione è stabilita.

Chiusura della Connessione TCP (4-way termination)

La terminazione della connessione avviene in quattro fasi ordinate:
1. FIN, ACK dal client al server.
2. ACK di risposta dal server.
3. FIN, ACK dal server al client.
4. ACK finale dal client.

Protocolli di Supporto

Oltre ai pacchetti TCP, nella cattura sono stati osservati anche:
- ARP (risoluzione IP-MAC)
- DNS (richieste e risposte verso 8.8.8.8)
- ICMP (messaggi di errore e diagnostica)

Uso di tcpdump

È stato utilizzato tcpdump con l'opzione -r per leggere i pacchetti dal file di cattura.
Comando utilizzato:
tcpdump -r /home/analyst/capture.pcap tcp -c 3

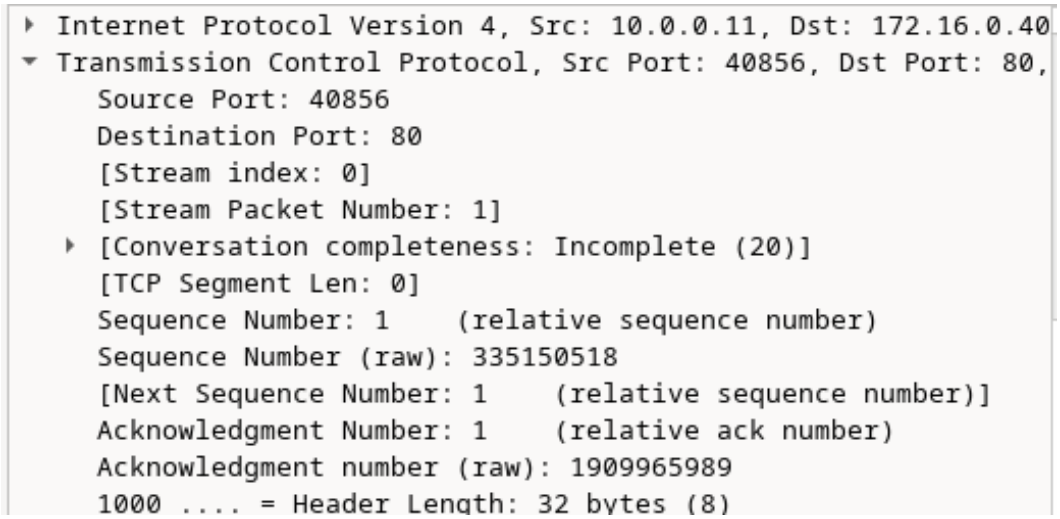
Domande e Risposte

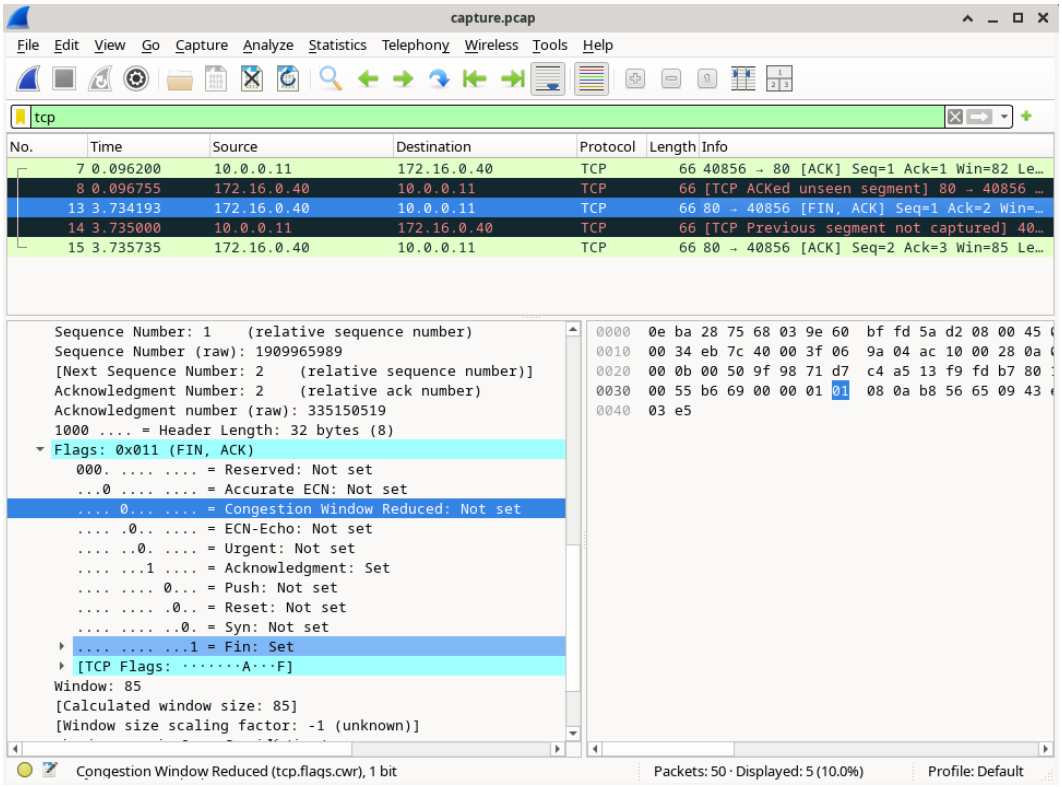
1. Porta sorgente del primo pacchetto: 40856 (effimera).
2. Porta destinazione: 80 (HTTP, well-known).
3. Flag impostato nel primo pacchetto: SYN.
4. Numero di sequenza relativo del primo pacchetto: 0.
5. Flag del secondo pacchetto: SYN, ACK.
6. Seq/Ack del secondo pacchetto: Seq=0, Ack=1.
7. Flag del terzo pacchetto: ACK.
8. Seq/Ack del terzo pacchetto: Seq=1, Ack=1.
9. Cosa fa l'opzione -r di tcpdump? Legge pacchetti da file .pcap.
10. Tre filtri utili in Wireshark: tcp.port==80, icmp, ip.addr==10.0.0.11.

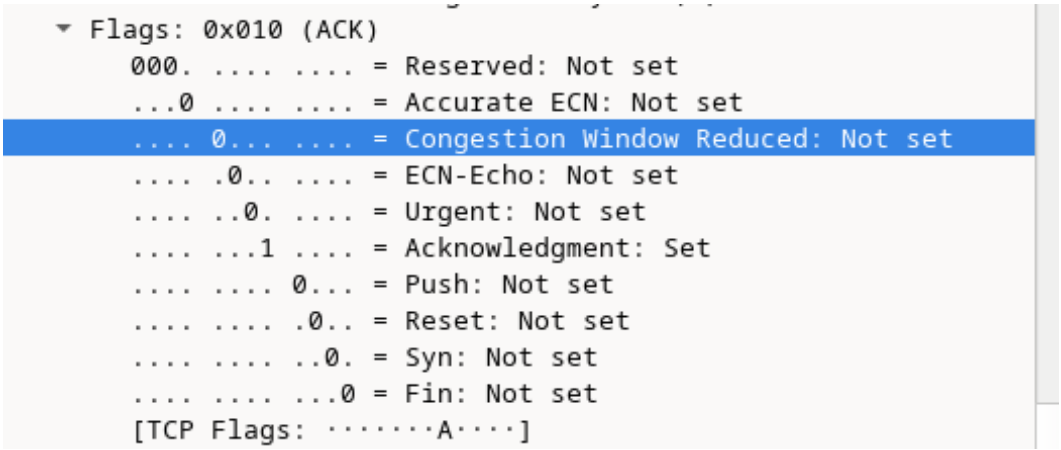
Conclusioni

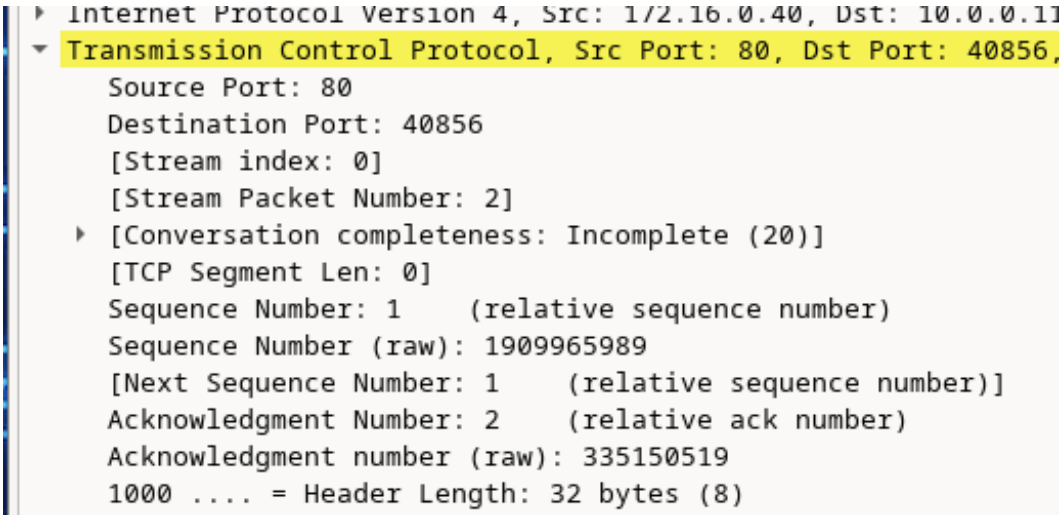
L'esercizio ha permesso di comprendere in dettaglio il funzionamento dell'handshake TCP, la terminazione della connessione e l'utilizzo di strumenti fondamentali come Wireshark e tcpdump. Queste conoscenze sono applicabili in contesti di sicurezza informatica e troubleshooting di rete.

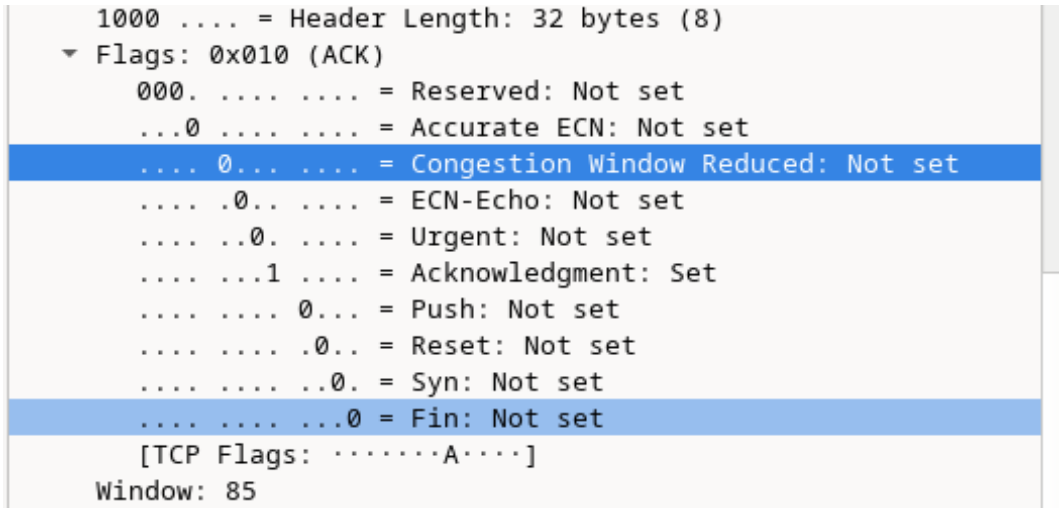
Screenshot del Laboratorio

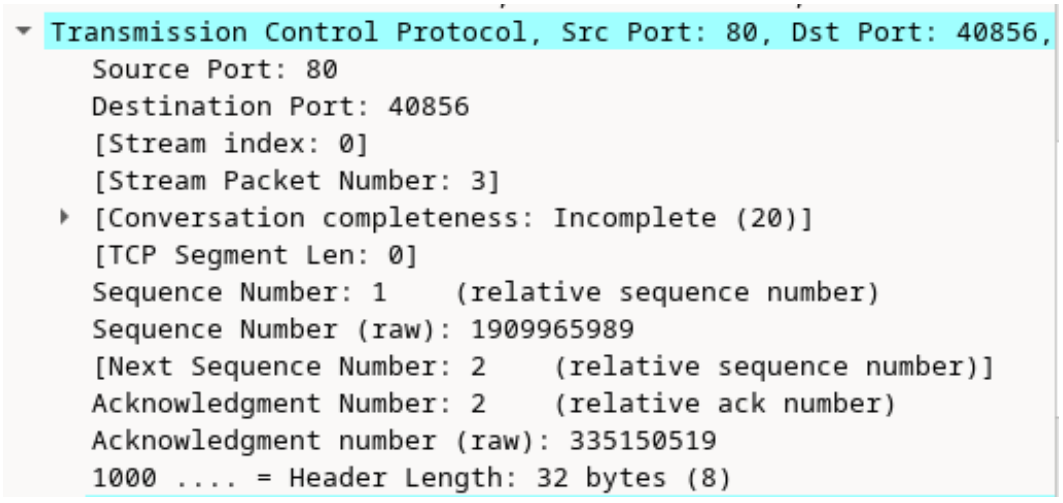


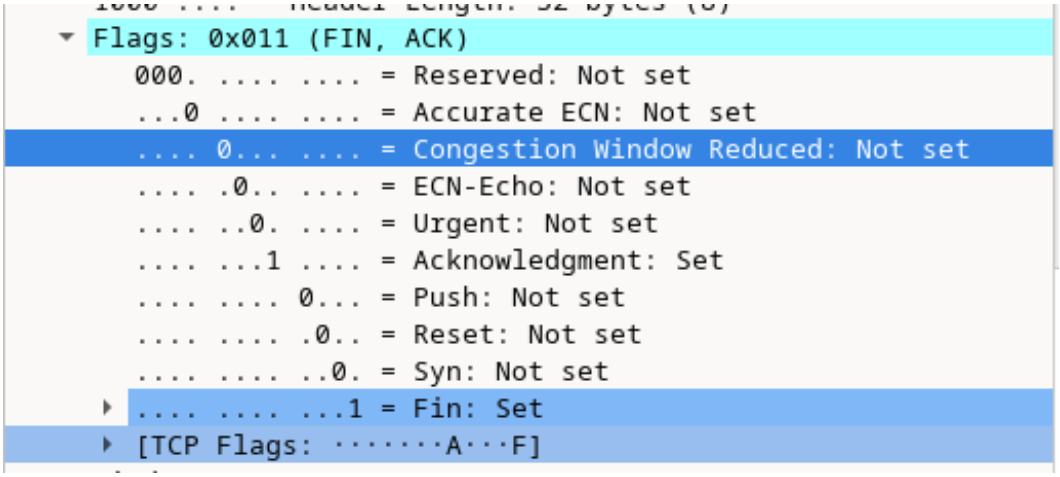

capture.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
7 0.096200 10.0.0.11 172.16.0.40 TCP 66 40856 → 80 [ACK] Seq=1 Ack=1 Win=82 Le…
8 0.096755 172.16.0.40 10.0.0.11 TCP 66 [TCP ACKed unseen segment] 80 → 40856 …
13 3.734193 172.16.0.40 10.0.0.11 TCP 66 80 → 40856 [FIN, ACK] Seq=1 Ack=2 Win=…
14 3.735000 10.0.0.11 172.16.0.40 TCP 66 [TCP Previous segment not captured] 40…
15 3.735735 172.16.0.40 10.0.0.11 TCP 66 80 → 40856 [ACK] Seq=2 Ack=3 Win=85 Le…
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 1909965989
[Next Sequence Number: 2 (relative sequence number)]
Acknowledgment Number: 2 (relative ack number)
Acknowledgment number (raw): 335150519
1000 .... = Header Length: 32 bytes (8)
Flags: 0x011 (FIN, ACK)
000. .... = Reserved: Not set
...0 .... = Accurate ECN: Not set
.... 0... .... = Congestion Window Reduced: 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
....1 = Fin: Set
[TCP Flags: ·····A···F]
Window: 85
[Calculated window size: 85]
[Window size scaling factor: -1 (unknown)]
0000 0e ba 28 75 68 03 9e 60 bf fd 5a d2 08 00 45
0010 00 34 eb 7c 40 00 3f 06 9a 04 ac 10 00 28 0a
0020 00 0b 00 50 9f 98 71 d7 c4 a5 13 f9 fd b7 80
0030 00 55 b6 69 00 00 01 01 08 0a b8 56 65 09 43
0040 03 e5
Congestion Window Reduced (tcp.flags.cwr), 1 bit
Packets: 50 · Displayed: 5 (10.0%)
Profile: Default


Flags: 0x010 (ACK)
000. .... = Reserved: Not set
...0 .... = Accurate ECN: Not set
.... 0... .... = Congestion Window Reduced: 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····]


Internet Protocol Version 4, Src: 172.16.0.40, Dst: 10.0.0.11
Transmission Control Protocol, Src Port: 80, Dst Port: 40856,
Source Port: 80
Destination Port: 40856
[Stream index: 0]
[Stream Packet Number: 2]
[Conversation completeness: Incomplete (20)]
[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 1909965989
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 2 (relative ack number)
Acknowledgment number (raw): 335150519
1000 .... = Header Length: 32 bytes (8)

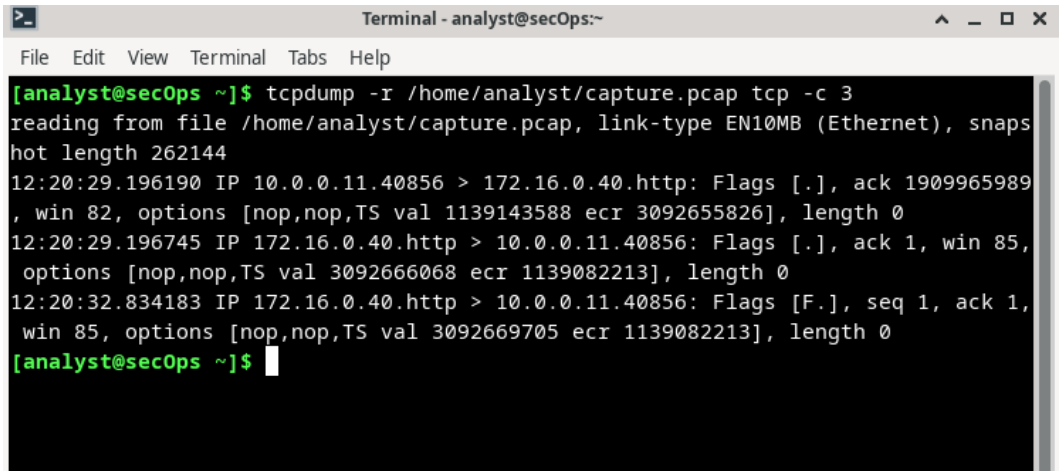

1000 .... = Header Length: 32 bytes (8)
Flags: 0x010 (ACK)
000. .... = Reserved: Not set
...0 .... = Accurate ECN: Not set
.... 0... .... = Congestion Window Reduced: Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....1 .... = Acknowledgment: Set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
....0. = Syn: Not set
....0 = Fin: Not set
[TCP Flags: ·····A····]
Window: 85


Transmission Control Protocol, Src Port: 80, Dst Port: 40856,
Source Port: 80
Destination Port: 40856
[Stream index: 0]
[Stream Packet Number: 3]
[Conversation completeness: Incomplete (20)]
[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 1909965989
[Next Sequence Number: 2 (relative sequence number)]
Acknowledgment Number: 2 (relative ack number)
Acknowledgment number (raw): 335150519
1000 .... = Header Length: 32 bytes (8)

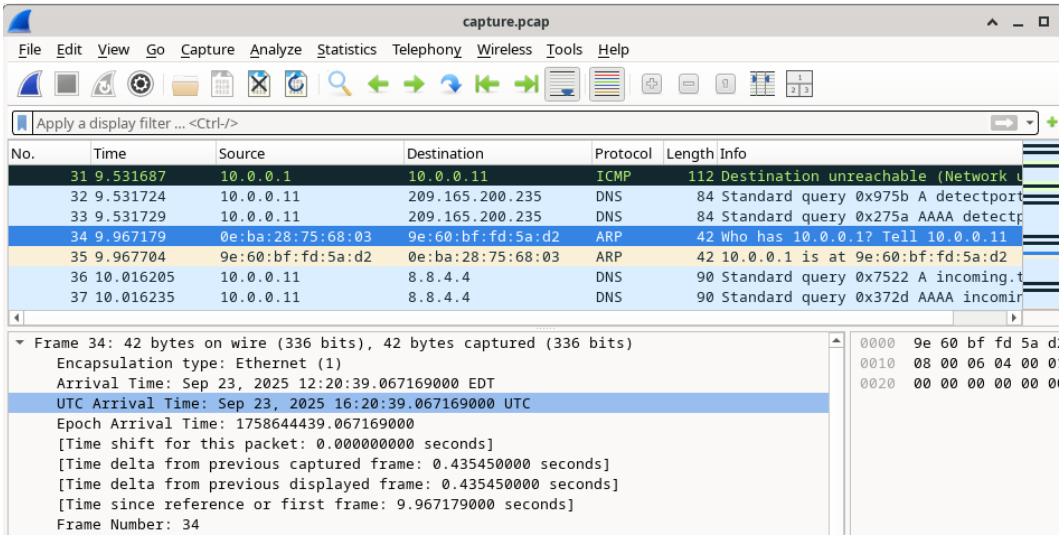


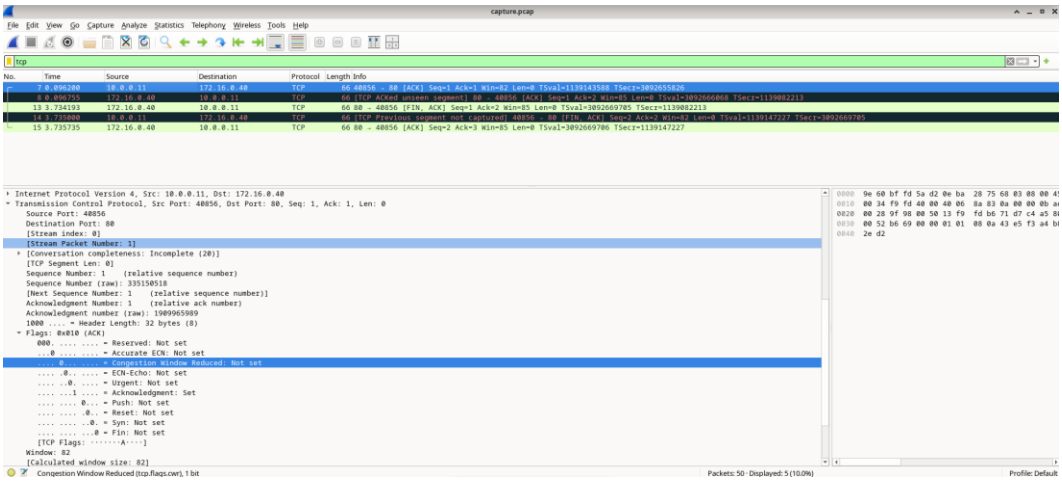

```
TCPDUMP(1)                General Commands Manual                TCPDUMP(1)

NAME
       tcpdump - dump traffic on a network

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

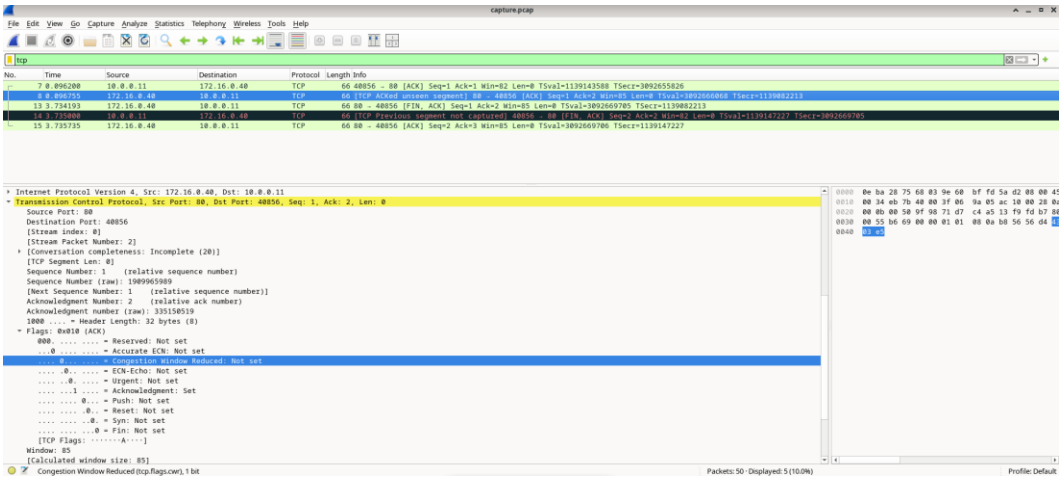
```
   -r file
          Read packets from file (which was created with the -w  option  or
          by  other tools that write pcap or pcapng files).  Standard input
          is used if file is ``-''.
```

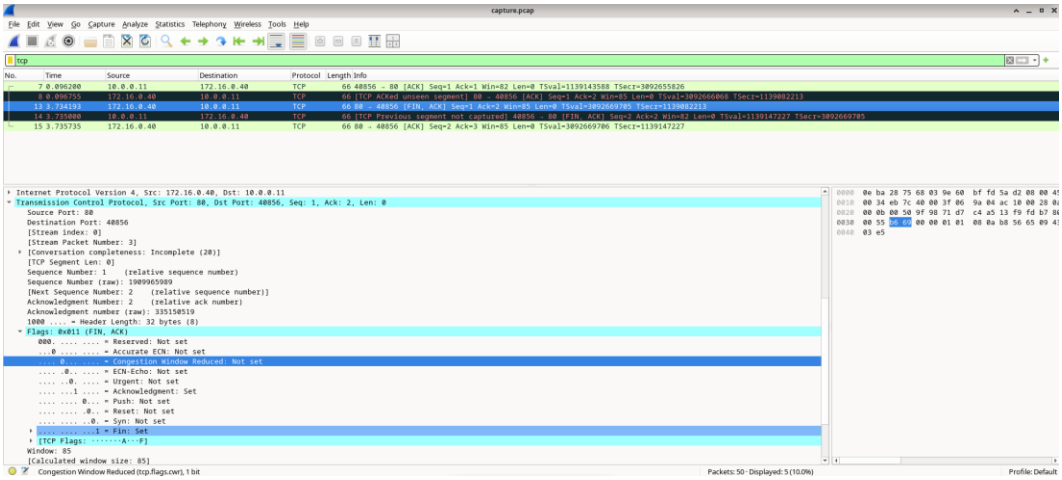


```
File  Edit  View  Terminal  Tabs  Help
[analyst@secOps ~]$ tcpdump -r /home/analyst/capture.pcap tcp -c 3
reading from file /home/analyst/capture.pcap, link-type EN10MB (Ethernet), snapshot length 262144
12:20:29.196190 IP 10.0.0.11.40856 > 172.16.0.40.http: Flags [.], ack 1909965989, win 82, options [nop,nop,TS val 1139143588 ecr 3092655826], length 0
12:20:29.196745 IP 172.16.0.40.http > 10.0.0.11.40856: Flags [.], ack 1, win 85, options [nop,nop,TS val 3092666068 ecr 1139082213], length 0
12:20:32.834183 IP 172.16.0.40.http > 10.0.0.11.40856: Flags [F.], seq 1, ack 1, win 85, options [nop,nop,TS val 3092669705 ecr 1139082213], 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 ovs-testcontroller udpbwtest mnexec ivs ryu-manager  2> /dev/null
killall -9 controller ofprotocol ofdatapath ping nox_core lt-nox_core ovs-openflowd ovs-controller ovs-testcontroller udpbwtest mnexec ivs ryu-manager  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:/'
egrep: warning: egrep is obsolescent; using grep -E
***  Removing OVS datapaths
ovs-vsctl --timeout=1 list-br
ovs-vsctl --if-exists del-br s1
ovs-vsctl --timeout=1 list-br
*** Removing all links of the pattern foo-ethX
ip link show | egrep -o '([-_.[:alnum:]]+-eth[[:digit:]]+)'
egrep: warning: egrep is obsolescent; using grep -E
( ip link del s1-eth2;ip link del s1-eth3;ip link del s1-eth4;ip link del s1-eth1 ) 2> /dev/null
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.
[analyst@secOps ~]$
```






capture.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
7 0.096200 10.0.0.11 172.16.0.40 TCP 66 40856 → 80 [ACK] Seq=1 Ack=1 Win=82 Len=0 TSval=1139143588 TSecr=3092655826
8 0.096755 172.16.0.40 10.0.0.11 TCP 66 [TCP ACKed unseen segment] 80 → 40856 [ACK] Seq=1 Ack=2 Win=85 Len=0 TSval=3092660068 TSecr=1139082213
13 3.734193 172.16.0.40 10.0.0.11 TCP 66 80 → 40856 [FIN, ACK] Seq=1 Ack=2 Win=85 Len=0 TSval=3092669705 TSecr=1139082213
14 3.735080 10.0.0.11 172.16.0.40 TCP 66 [TCP Previous segment not captured] 40856 → 80 [FIN, ACK] Seq=2 Ack=2 Win=82 Len=0 TSval=1139147227 TSecr=3092669705
15 3.735735 172.16.0.40 10.0.0.11 TCP 66 80 → 40856 [ACK] Seq=2 Ack=3 Win=85 Len=0 TSval=3092669706 TSecr=1139147227
Internet Protocol Version 4, Src: 172.16.0.40, Dst: 10.0.0.11
Transmission Control Protocol, Src Port: 80, Dst Port: 40856, Seq: 1, Ack: 2, Len: 0
Source Port: 80
Destination Port: 40856
[Stream index: 0]
[Stream Packet Number: 2]
[Conversation completeness: Incomplete (20)]
[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 1909965989
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 2 (relative ack number)
Acknowledgment number (raw): 335150519
1000 .... = Header Length: 32 bytes (8)
Flags: 0x010 (ACK)
000. .... = Reserved: Not set
...0 .... = Accurate ECN: Not set
.... 0... .... = Congestion Window Reduced: 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: 85
[Calculated window size: 85]
Congestion Window Reduced (tcp.flags.cwr), 1 bit
Packets: 50 · Displayed: 5 (10.0%)
Profile: Default


capture.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
7 0.096200 10.0.0.11 172.16.0.40 TCP 66 40856 → 80 [ACK] Seq=1 Ack=1 Win=82 Len=0 TSval=1139143588 TSecr=3092655826
8 0.096755 172.16.0.40 10.0.0.11 TCP 66 [TCP ACKed unseen segment] 80 → 40856 [ACK] Seq=1 Ack=2 Win=85 Len=0 TSval=3092660068 TSecr=1139082213
13 3.734193 172.16.0.40 10.0.0.11 TCP 66 80 → 40856 [FIN, ACK] Seq=1 Ack=2 Win=85 Len=0 TSval=3092669705 TSecr=1139082213
14 3.735080 10.0.0.11 172.16.0.40 TCP 66 [TCP Previous segment not captured] 40856 → 80 [FIN, ACK] Seq=2 Ack=2 Win=82 Len=0 TSval=1139147227 TSecr=3092669705
15 3.735735 172.16.0.40 10.0.0.11 TCP 66 80 → 40856 [ACK] Seq=2 Ack=3 Win=85 Len=0 TSval=3092669706 TSecr=1139147227
Internet Protocol Version 4, Src: 172.16.0.40, Dst: 10.0.0.11
Transmission Control Protocol, Src Port: 80, Dst Port: 40856, Seq: 1, Ack: 2, Len: 0
Source Port: 80
Destination Port: 40856
[Stream index: 0]
[Stream Packet Number: 3]
[Conversation completeness: Incomplete (20)]
[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 1909965989
[Next Sequence Number: 2 (relative sequence number)]
Acknowledgment Number: 2 (relative ack number)
Acknowledgment number (raw): 335150519
1000 .... = Header Length: 32 bytes (8)
Flags: 0x011 (FIN, ACK)
000. .... = Reserved: Not set
...0 .... = Accurate ECN: Not set
.... 0... .... = Congestion Window Reduced: 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
....1 = Fin: Set
[TCP Flags: ·····A···F]
Window: 85
[Calculated window size: 85]
Congestion Window Reduced (tcp.flags.cwr), 1 bit
Packets: 50 · Displayed: 5 (10.0%)
Profile: Default