

Instituto Tecnológico de Cancún

Ingeniería en Sistemas Computacionales

Fundamentos de Telecomunicaciones

**Lab20 - Locate TCP Connection Attempts
to a Client**

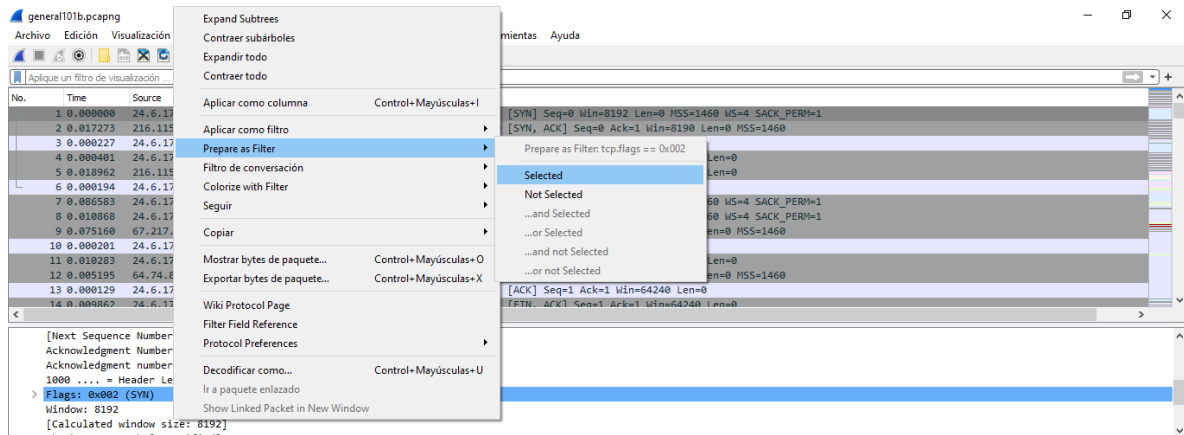
Docente: Ing. Ismael Jiménez Sánchez

Alumno: Uc Uc César Enrique

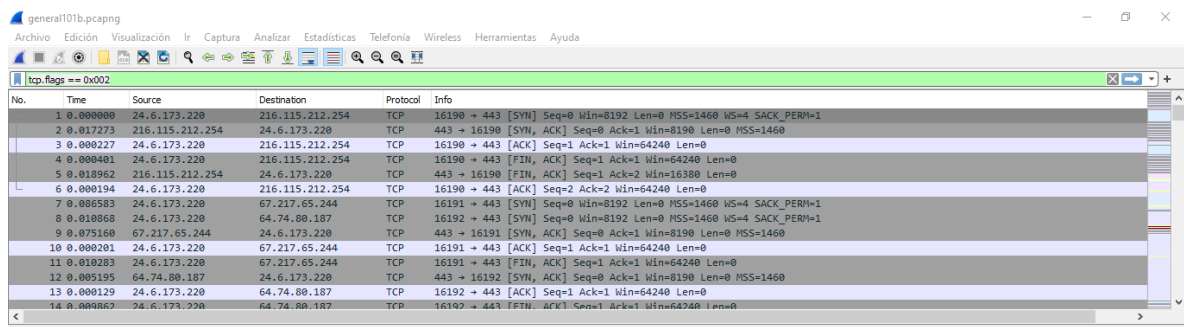
Lab20 - Locate TCP Connection Attempts to a Client

1 Abrimos el archivo general101b.pcapng

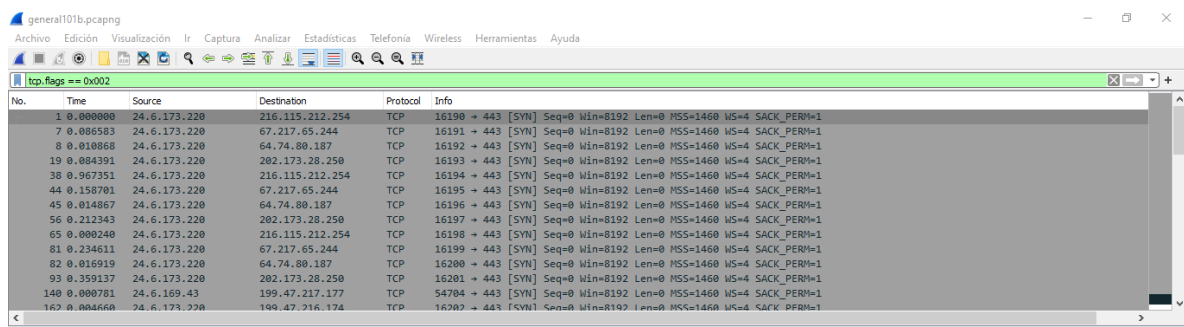
2 En el panel de detalles en el paquete 1 hacemos click derecho en Flags>Prepare as Filter>Selected



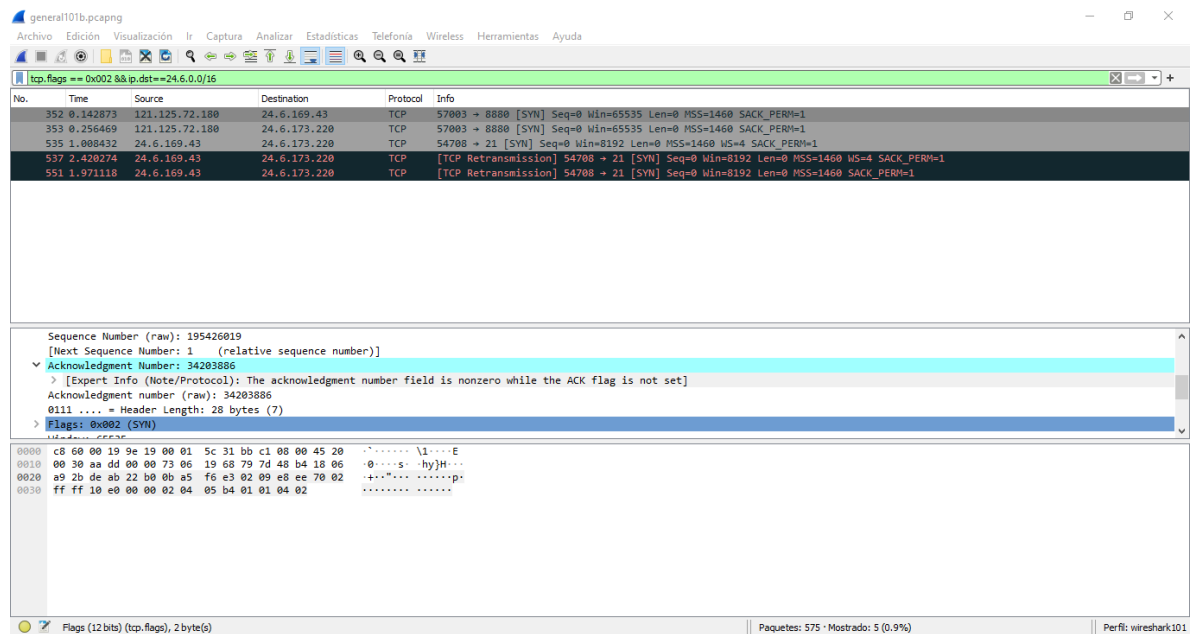
Deberá aparecer tcp.flags == 0x002



3 Aplicamos el tcp.flags == 0x002



Le agregamos && ip.dst==24.6.0.0/16 y lo aplicamos



Wireshark interface showing a packet capture with the filter `tcp.flags == 0x002 && ip.dst == 24.6.0.0/16`. The packet list shows several TCP packets, including a SYN packet and a retransmission. The packet details pane shows the structure of a TCP packet, including the sequence number, acknowledgment number, and flags.

No.	Time	Source	Destination	Protocol	Info
352	0.142873	121.125.72.180	24.6.169.43	TCP	57003 → 8880 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
353	0.256469	121.125.72.180	24.6.173.220	TCP	57003 → 8880 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
535	1.000432	24.6.169.43	24.6.173.220	TCP	54708 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 MS=4 SACK_PERM=1
537	2.430274	24.6.169.43	24.6.173.220	TCP	[TCP Retransmission] 54708 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 MS=4 SACK_PERM=1
551	1.971118	24.6.169.43	24.6.173.220	TCP	[TCP Retransmission] 54708 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1

Sequence Number (raw): 195426019
[Next Sequence Number: 1 (relative sequence number)]
✓ Acknowledgment Number: 34203886
> [Expert Info (Note/Protocol): The acknowledgment number field is nonzero while the ACK flag is not set]
Acknowledgment number (raw): 34203886
0111 = Header Length: 28 bytes (7)
> Flags: 0x002 (SYN)

0000 c8 60 00 19 9e 19 00 01 5c 31 bb c1 08 00 45 20 \1....E
0010 00 30 aa dd 00 00 73 06 19 68 79 7d 48 b4 18 06s..hy]H..
0020 a9 2b de ab 22 b0 0b a5 f6 e3 02 09 e8 ee 70 02p.....
0030 ff ff 10 e0 00 00 02 04 05 b4 01 01 04 02

Flags (12 bits) (tcp.flags), 2 byte(s) | Paquetes: 575 · Mostrado: 5 (0.9%) | Perfil: wireshark101

Deberá solo aparecer 5 paquetes mostrados

Paquetes: 575 · Mostrado: 5 (0.9%)