INSTITUTO TECNOLOGICO DE CANCUN

Nombre De La Materia: Fundamentos De Telecomunicaciones

Nombre De La Unidad: Sistemas de comunicación

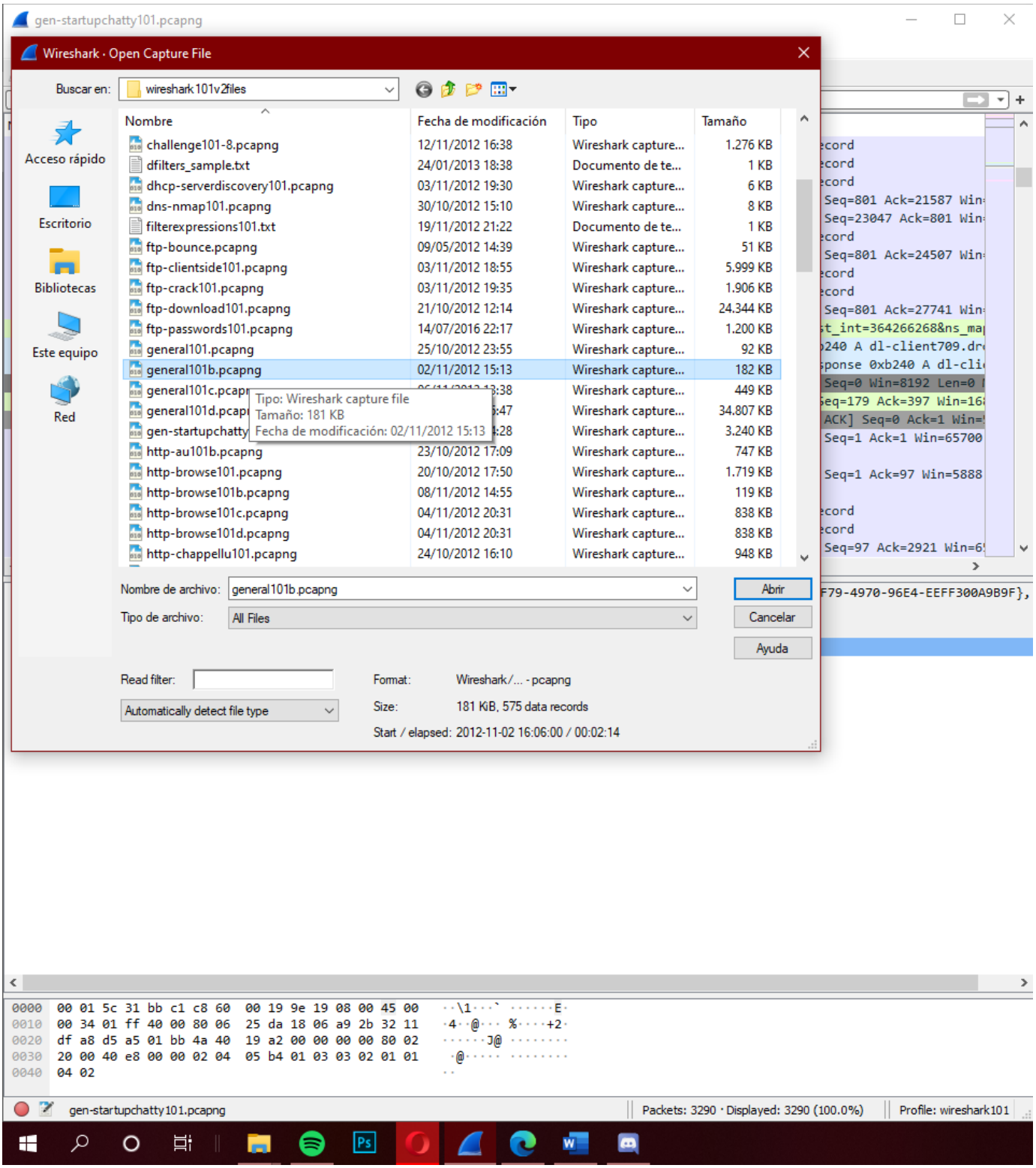
N.º De Actividad: Laboratorio 20

Nombre Del Alumno: Vazquez Canto Andres Omar

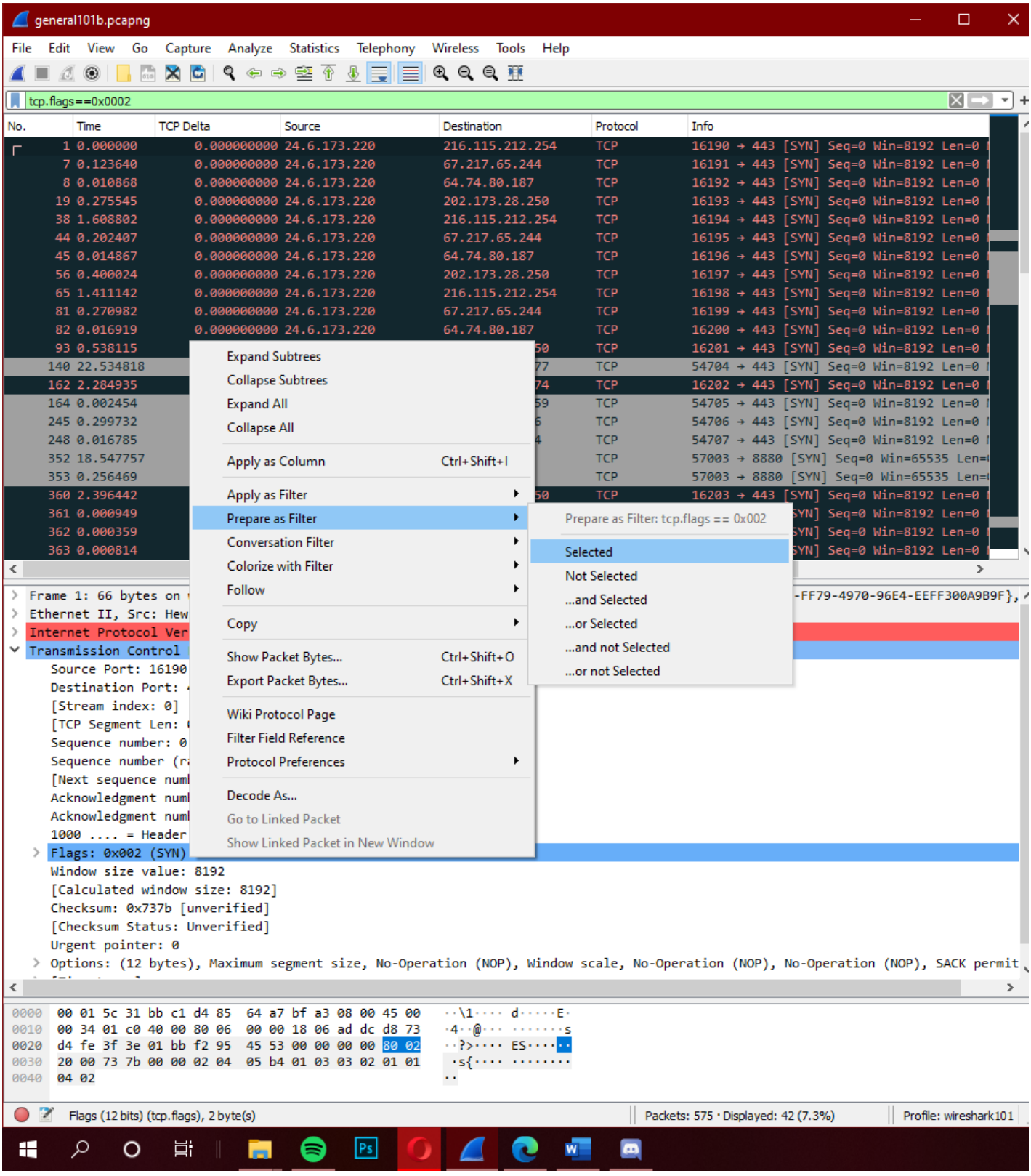
N.º De Control: 17530439

Lab20- Locate TCP Connection Attempts to a Client

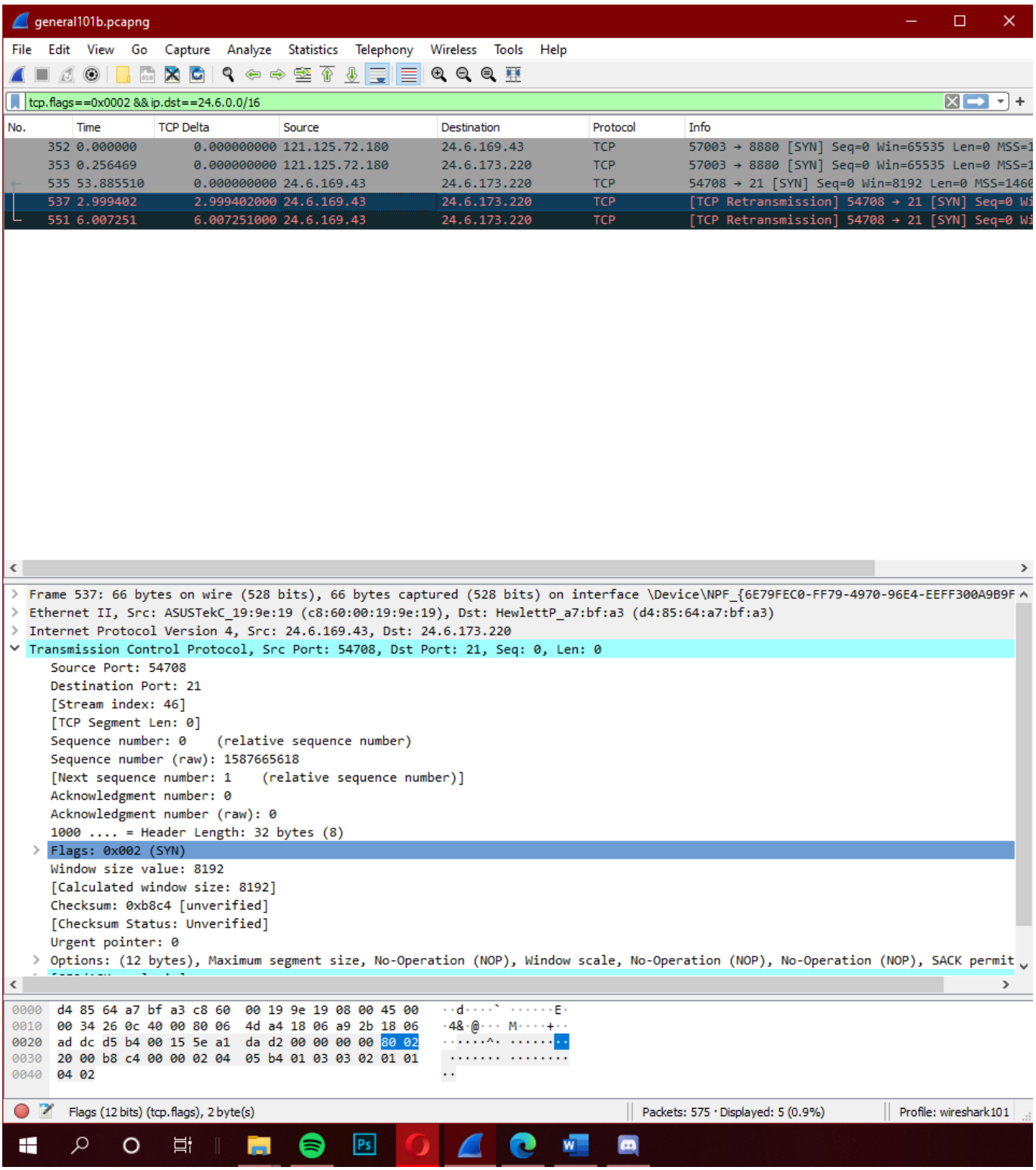
Paso 1:



Paso 2:


general101b.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.flags==0x0002
No. Time TCP Delta Source Destination Protocol Info
1 0.000000 0.000000000 24.6.173.220 216.115.212.254 TCP 16190 → 443 [SYN] Seq=0 Win=8192 Len=0
7 0.123640 0.000000000 24.6.173.220 67.217.65.244 TCP 16191 → 443 [SYN] Seq=0 Win=8192 Len=0
8 0.010868 0.000000000 24.6.173.220 64.74.80.187 TCP 16192 → 443 [SYN] Seq=0 Win=8192 Len=0
19 0.275545 0.000000000 24.6.173.220 202.173.28.250 TCP 16193 → 443 [SYN] Seq=0 Win=8192 Len=0
38 1.608802 0.000000000 24.6.173.220 216.115.212.254 TCP 16194 → 443 [SYN] Seq=0 Win=8192 Len=0
44 0.202407 0.000000000 24.6.173.220 67.217.65.244 TCP 16195 → 443 [SYN] Seq=0 Win=8192 Len=0
45 0.014867 0.000000000 24.6.173.220 64.74.80.187 TCP 16196 → 443 [SYN] Seq=0 Win=8192 Len=0
56 0.400024 0.000000000 24.6.173.220 202.173.28.250 TCP 16197 → 443 [SYN] Seq=0 Win=8192 Len=0
65 1.411142 0.000000000 24.6.173.220 216.115.212.254 TCP 16198 → 443 [SYN] Seq=0 Win=8192 Len=0
81 0.270982 0.000000000 24.6.173.220 67.217.65.244 TCP 16199 → 443 [SYN] Seq=0 Win=8192 Len=0
82 0.016919 0.000000000 24.6.173.220 64.74.80.187 TCP 16200 → 443 [SYN] Seq=0 Win=8192 Len=0
93 0.538115 TCP 16201 → 443 [SYN] Seq=0 Win=8192 Len=0
140 22.534818 TCP 54704 → 443 [SYN] Seq=0 Win=8192 Len=0
162 2.284935 TCP 16202 → 443 [SYN] Seq=0 Win=8192 Len=0
164 0.002454 TCP 54705 → 443 [SYN] Seq=0 Win=8192 Len=0
245 0.299732 TCP 54706 → 443 [SYN] Seq=0 Win=8192 Len=0
248 0.016785 TCP 54707 → 443 [SYN] Seq=0 Win=8192 Len=0
352 18.547757 TCP 57003 → 8880 [SYN] Seq=0 Win=65535 Len=
353 0.256469 TCP 57003 → 8880 [SYN] Seq=0 Win=65535 Len=
360 2.396442 TCP 16203 → 443 [SYN] Seq=0 Win=8192 Len=0
361 0.000949 TCP 16203 → 443 [SYN] Seq=0 Win=8192 Len=0
362 0.000359 TCP 16203 → 443 [SYN] Seq=0 Win=8192 Len=0
363 0.000814 TCP 16203 → 443 [SYN] Seq=0 Win=8192 Len=0
Expand Subtrees
Collapse Subtrees
Expand All
Collapse All
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes... Ctrl+Shift+O
Export Packet Bytes... Ctrl+Shift+X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As...
Go to Linked Packet
Show Linked Packet in New Window
Prepare as Filter: tcp.flags == 0x002
Selected
Not Selected
...and Selected
...or Selected
...and not Selected
...or not Selected
Frame 1: 66 bytes on
Ethernet II, Src: Hew
Internet Protocol Ver
Transmission Control
Source Port: 16190
Destination Port:
[Stream index: 0]
[TCP Segment Len:
Sequence number: 0
Sequence number (r
[Next sequence numl
Acknowledgment numl
Acknowledgment numl
1000 .... = Header
Flags: 0x002 (SYN)
Window size value: 8192
[Calculated window size: 8192]
Checksum: 0x737b [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permit
0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00
0010 00 34 01 c0 40 00 80 06 00 00 18 06 ad dc d8 73
0020 d4 fe 3f 3e 01 bb f2 95 45 53 00 00 00 00 80 02
0030 20 00 73 7b 00 00 02 04 05 b4 01 03 03 02 01 01
0040 04 02
Flags (12 bits) (tcp.flags), 2 byte(s)
Packets: 575 · Displayed: 42 (7.3%)
Profile: wireshark101

Paso 3:


general101b.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.flags==0x0002 && ip.dst==24.6.0.0/16
No. Time TCP Delta Source Destination Protocol Info
352 0.000000 0.000000000 121.125.72.180 24.6.169.43 TCP 57003 → 8880 [SYN] Seq=0 Win=65535 Len=0 MSS=1
353 0.256469 0.000000000 121.125.72.180 24.6.173.220 TCP 57003 → 8880 [SYN] Seq=0 Win=65535 Len=0 MSS=1
535 53.885510 0.000000000 24.6.169.43 24.6.173.220 TCP 54708 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
537 2.999402 2.999402000 24.6.169.43 24.6.173.220 TCP [TCP Retransmission] 54708 → 21 [SYN] Seq=0 Wi
551 6.007251 6.007251000 24.6.169.43 24.6.173.220 TCP [TCP Retransmission] 54708 → 21 [SYN] Seq=0 Wi
Frame 537: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A9B9F
Ethernet II, Src: ASUSTekC_19:9e:19 (c8:60:00:19:9e:19), Dst: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3)
Internet Protocol Version 4, Src: 24.6.169.43, Dst: 24.6.173.220
Transmission Control Protocol, Src Port: 54708, Dst Port: 21, Seq: 0, Len: 0
Source Port: 54708
Destination Port: 21
[Stream index: 46]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
Sequence number (raw): 1587665618
[Next sequence number: 1 (relative sequence number)]
Acknowledgment number: 0
Acknowledgment number (raw): 0
1000 .... = Header Length: 32 bytes (8)
Flags: 0x002 (SYN)
Window size value: 8192
[Calculated window size: 8192]
Checksum: 0xb8c4 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permit
0000 d4 85 64 a7 bf a3 c8 60 00 19 9e 19 08 00 45 00
0010 00 34 26 0c 40 00 80 06 4d a4 18 06 a9 2b 18 06
0020 ad dc d5 b4 00 15 5e a1 da d2 00 00 00 00 80 02
0030 20 00 b8 c4 00 00 02 04 05 b4 01 03 03 02 01 01
0040 04 02
Flags (12 bits) (tcp.flags), 2 byte(s)
Packets: 575 · Displayed: 5 (0.9%)
Profile: wireshark101