

INSTITUTO TECNOLÓGICO 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:

The screenshot shows the Wireshark 'Open Capture File' dialog box. The search path is 'wireshark101v2files'. The file list contains various .pcapng files. The file 'general101b.pcapng' is selected, and a tooltip shows its details: 'Tipo: Wireshark capture file', 'Tamaño: 181 KB', and 'Fecha de modificación: 02/11/2012 15:13'. The 'Nombre de archivo' field is 'general101b.pcapng' and the 'Tipo de archivo' is 'All Files'. The 'Read filter' is empty, and the 'Format' is 'Wireshark/... - pcapng'. The 'Size' is '181 KiB, 575 data records' and the 'Start / elapsed' time is '2012-11-02 16:06:00 / 00:02:14'. The 'Abrir' button is highlighted.

Below the dialog, the packet list shows the first few packets of the capture. The first packet is a TCP Reset (RST) from 192.168.1.1 to 192.168.1.100, port 80. The second packet is a TCP Reset (RST) from 192.168.1.1 to 192.168.1.100, port 80. The third packet is a TCP Reset (RST) from 192.168.1.1 to 192.168.1.100, port 80. The fourth packet is a TCP Reset (RST) from 192.168.1.1 to 192.168.1.100, port 80. The fifth packet is a TCP Reset (RST) from 192.168.1.1 to 192.168.1.100, port 80. The sixth packet is a TCP Reset (RST) from 192.168.1.1 to 192.168.1.100, port 80. The seventh packet is a TCP Reset (RST) from 192.168.1.1 to 192.168.1.100, port 80. The eighth packet is a TCP Reset (RST) from 192.168.1.1 to 192.168.1.100, port 80. The ninth packet is a TCP Reset (RST) from 192.168.1.1 to 192.168.1.100, port 80. The tenth packet is a TCP Reset (RST) from 192.168.1.1 to 192.168.1.100, port 80.

No.	Time	Source	Destination	Protocol	Length	Info
0000	0.000000	192.168.1.1	192.168.1.100	TCP	60	80 → 80 [RST] Seq=0 Win=0 Len=0
0010	0.000000	192.168.1.1	192.168.1.100	TCP	60	80 → 80 [RST] Seq=0 Win=0 Len=0
0020	0.000000	192.168.1.1	192.168.1.100	TCP	60	80 → 80 [RST] Seq=0 Win=0 Len=0
0030	0.000000	192.168.1.1	192.168.1.100	TCP	60	80 → 80 [RST] Seq=0 Win=0 Len=0
0040	0.000000	192.168.1.1	192.168.1.100	TCP	60	80 → 80 [RST] Seq=0 Win=0 Len=0

The status bar at the bottom shows 'Packets: 3290 · Displayed: 3290 (100.0%)' and 'Profile: wireshark101'.

Paso 2:

The image shows the Wireshark network protocol analyzer interface. The main packet list pane displays a list of captured packets. A filter is applied to the list: `tcp.flags==0x0002`. The selected packet (No. 363) is a TCP segment with flags 0x0002 (SYN). A context menu is open over this packet, showing various actions. The 'Prepare as Filter' option is selected, and a sub-menu is open showing the filter expression `tcp.flags == 0x002`.

Packet List:

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	54704 → 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=0
353	0.256469				TCP	57003 → 8880 [SYN] Seq=0 Win=65535 Len=0
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

Packet Details:

- Frame 1: 66 bytes on wire (528 bits) capture length 66 bytes
- Ethernet II, Src: Hewlett-Packard (08:00:00:08:00:08), Dst: Intel (08:00:00:08:00:08)
- Internet Protocol Version 4, Src: 24.6.173.220, Dst: 216.115.212.254
- Transmission Control Protocol, Seq=16190, Win=8192, Len=0, Flags=0x0002 (SYN)
- Flags: 0x0002 (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

Packet Bytes:

```
0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00  ..\1... d....E-
0010 00 34 01 c0 40 00 80 06 00 00 18 06 ad dc d8 73  .4..@.....s
0020 d4 fe 3f 3e 01 bb f2 95 45 53 00 00 00 00 80 02  .?>.... ES....
0030 20 00 73 7b 00 00 02 04 05 b4 01 03 03 02 01 01  .s{.....
0040 04 02
```

Status Bar: Flags (12 bits) (tcp.flags), 2 byte(s) | Packets: 575 · Displayed: 42 (7.3%) | Profile: wireshark101

Paso 3:

The image shows a Wireshark packet capture window titled "general101b.pcapng". The filter bar at the top displays the filter `tcp.flags==0x0002 && ip.dst==24.6.0.0/16`. The packet list shows five packets, with packet 537 selected. The packet details pane shows the structure of the selected packet, and the packet bytes pane shows the raw data in hexadecimal and ASCII.

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 W
551	6.007251	6.007251000	24.6.169.43	24.6.173.220	TCP	[TCP Retransmission] 54708 → 21 [SYN] Seq=0 W

> 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
v 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 ..d...^.....E-
0010 00 34 26 0c 40 00 80 06 4d a4 18 06 a9 2b 18 06 +4&..@...M.....
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