

INSTITUTO TECNOLÓGICO DE CANCUN



Nombre De La Materia: Fundamentos De Telecomunicaciones

Nombre De La Unidad: Sistemas de comunicación

N.º De Actividad: Laboratorio 33

Nombre Del Alumno: Vazquez Canto Andres Omar

N.º De Control: 17530439

Lab33- Detect Suspicious Protocols or Applications

Paso 1:

The screenshot shows the 'Wireshark - Open Capture File' dialog box. The search path is 'wireshark101v2files'. The file list contains various .pcapng files and a .csv file. 'general101c.pcapng' is selected, with a tooltip showing its type as 'Wireshark capture file' and size as '448 KB'. The file details at the bottom show 'Nombre de archivo: general101c.pcapng', 'Tipo de archivo: All Files', 'Read filter: Automatically detect file type', 'Format: Wireshark/... - pcapng', 'Size: 448KB, 727 data records', and 'Start / elapsed: 2012-08-31 16:16:42 / 00:34:35'. The background shows a Wireshark packet capture of an HTTP request.

Nombre	Fecha de modificación	Tipo	Tamaño
dns-nmap101.pcapng	30/10/2012 15:10	Wireshark capture...	8 KB
exportexe.pcapng	02/12/2020 22:28	Wireshark capture...	537 KB
filterexpressions101.txt	19/11/2012 21:22	Documento de te...	1 KB
ftp-bounce.pcapng	09/05/2012 14:39	Wireshark capture...	51 KB
ftp-clientside101.pcapng	03/11/2012 18:55	Wireshark capture...	5.999 KB
ftp-crack101.pcapng	03/11/2012 19:35	Wireshark capture...	1.906 KB
ftp-download101.pcapng	21/10/2012 12:14	Wireshark capture...	24.344 KB
ftp-passwords101.pcapng	14/07/2016 22:17	Wireshark capture...	1.200 KB
general101.pcapng	25/10/2012 23:55	Wireshark capture...	92 KB
general101b.pcapng	02/11/2012 15:13	Wireshark capture...	182 KB
general101c.pcapng	06/11/2012 13:38	Wireshark capture...	449 KB
general101d.pcapng	06/11/2012 15:47	Wireshark capture...	34.807 KB
gen-startupchatty101.p		Wireshark capture...	3.240 KB
hostinformation.csv		Archivo de valores...	10 KB
http-au101b.pcapng	23/10/2012 17:09	Wireshark capture...	747 KB
http-browse101.pcapng	20/10/2012 17:50	Wireshark capture...	1.719 KB
http-browse101b.pcapng	08/11/2012 14:55	Wireshark capture...	119 KB
http-browse101c.pcapng	04/11/2012 20:31	Wireshark capture...	838 KB
http-browse101d.pcapng	04/11/2012 20:31	Wireshark capture...	838 KB
http-chappellu101.pcapng	24/10/2012 16:10	Wireshark capture...	948 KB
http-chappellu101b.pcapng	24/01/2013 18:41	Wireshark capture...	615 KB

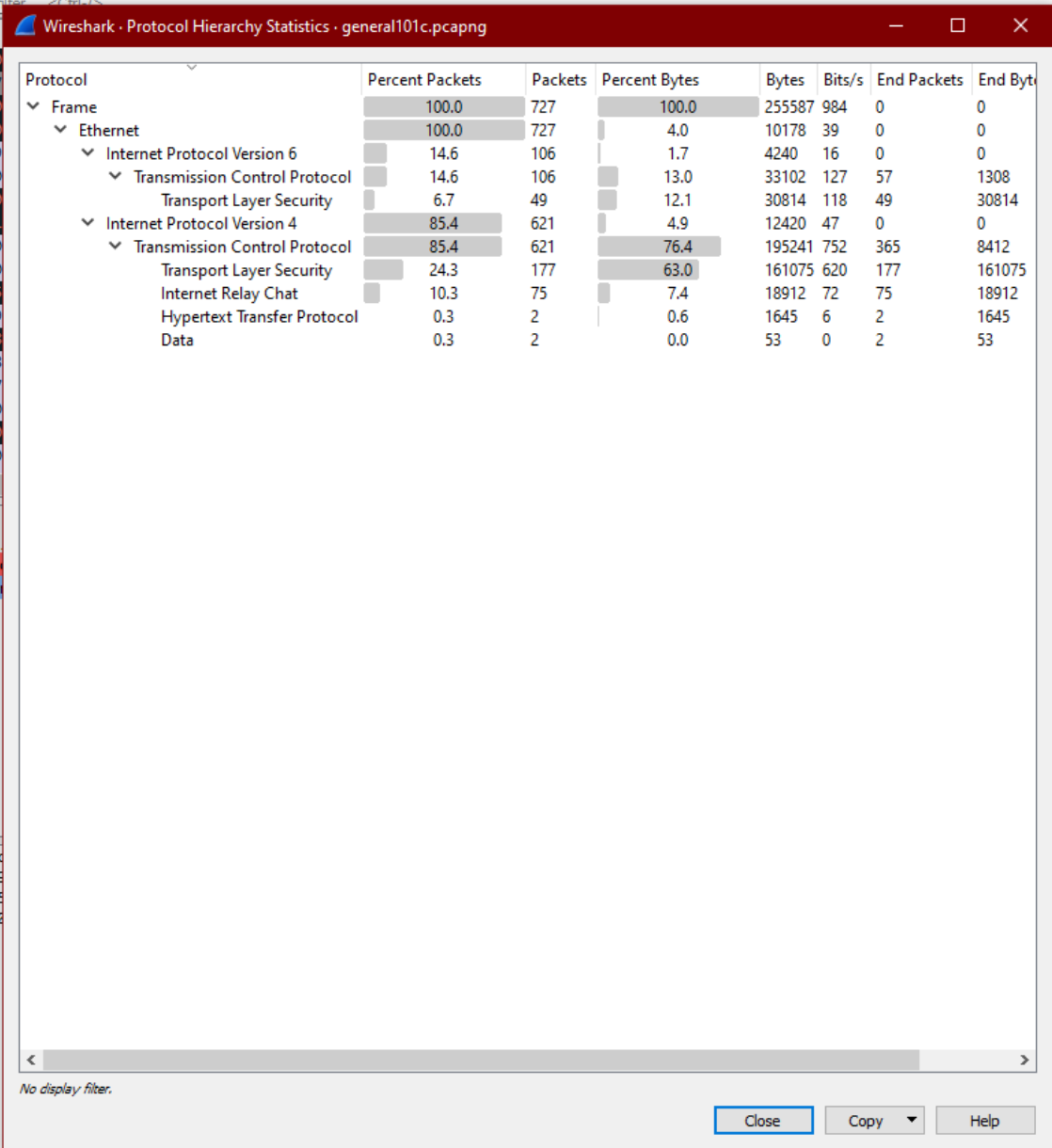
Nombre de archivo: general101c.pcapng
Tipo de archivo: All Files
Read filter: Automatically detect file type
Format: Wireshark/... - pcapng
Size: 448KB, 727 data records
Start / elapsed: 2012-08-31 16:16:42 / 00:34:35

Abrir
Cancelar
Ayuda

0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00 ..\1... d...E.
0010 00 34 1a f2 40 00 80 06 00 00 18 06 ad dc ad c2 .4..@.....
0020 4f 79 f0 9e 00 50 24 6b 15 b2 00 00 00 80 02 Oy...P\$k.....
0030 20 00 c3 44 00 00 02 04 05 b4 01 03 03 02 01 01 ..D.....
0040 04 02 ..

http-browse101c.pcapng | Packets: 1668 · Displayed: 1668 (100.0%) | Profile: wireshark101

Paso 2:



The image shows the Wireshark Protocol Hierarchy Statistics window for the file general101c.pcapng. The window displays a tree view of protocols and a table of statistics.

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes
Frame	100.0	727	100.0	255587	984	0	0
Ethernet	100.0	727	4.0	10178	39	0	0
Internet Protocol Version 6	14.6	106	1.7	4240	16	0	0
Transmission Control Protocol	14.6	106	13.0	33102	127	57	1308
Transport Layer Security	6.7	49	12.1	30814	118	49	30814
Internet Protocol Version 4	85.4	621	4.9	12420	47	0	0
Transmission Control Protocol	85.4	621	76.4	195241	752	365	8412
Transport Layer Security	24.3	177	63.0	161075	620	177	161075
Internet Relay Chat	10.3	75	7.4	18912	72	75	18912
Hypertext Transfer Protocol	0.3	2	0.6	1645	6	2	1645
Data	0.3	2	0.0	53	0	2	53

The background shows the main Wireshark interface with a packet list on the left and a packet details pane on the right. The status bar at the bottom indicates "Packets: 727 · Displayed: 727 (100.0%)" and "Profile: wireshark101".

Paso 3:

The image shows a Wireshark capture of IRC traffic. The main packet list displays several messages between 24.6.173.220 and 67.220.66.111. The 'Protocol Hierarchy Statistics' window is open, showing the breakdown of the captured data by protocol.

Wireshark - Protocol Hierarchy Statistics - general101c.pcapng

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes
Frame	100.0	727	100.0	255587	984	0	0
Ethernet	100.0	727	4.0	10178	39	0	0
Internet Protocol Version 6	14.6	106	1.7	4240	16	0	0
Transmission Control Protocol	14.6	106	13.0	33102	127	57	1308
Transport Layer Security	6.7	49	12.1	30814	118	49	30814
Internet Protocol Version 4	85.4	621	4.9	12420	47	0	0
Transmission Control Protocol	85.4	621	76.4	195241	752	365	8412
Transport Layer Security	24.3	177	63.0	161075	620	177	161075
Internet Relay Chat	10.3	75	7.4	18912	72	75	18912
Hypertext Transfer Protocol	0.3	2	0.6	1645	6	2	1645
Data	0.3	2	0.0	53	0	2	53

Profile: wireshark101