

INSTITUTO TECNOLÓGICO DE CANCUN



Nombre De La Materia: Fundamentos De Telecomunicaciones

Nombre De La Unidad: Sistemas de comunicación

N.º De Actividad: Laboratorio 29

Nombre Del Alumno: Vazquez Canto Andres Omar

N.º De Control: 17530439

Lab29- Export a Single TCP Conversation

Paso1:

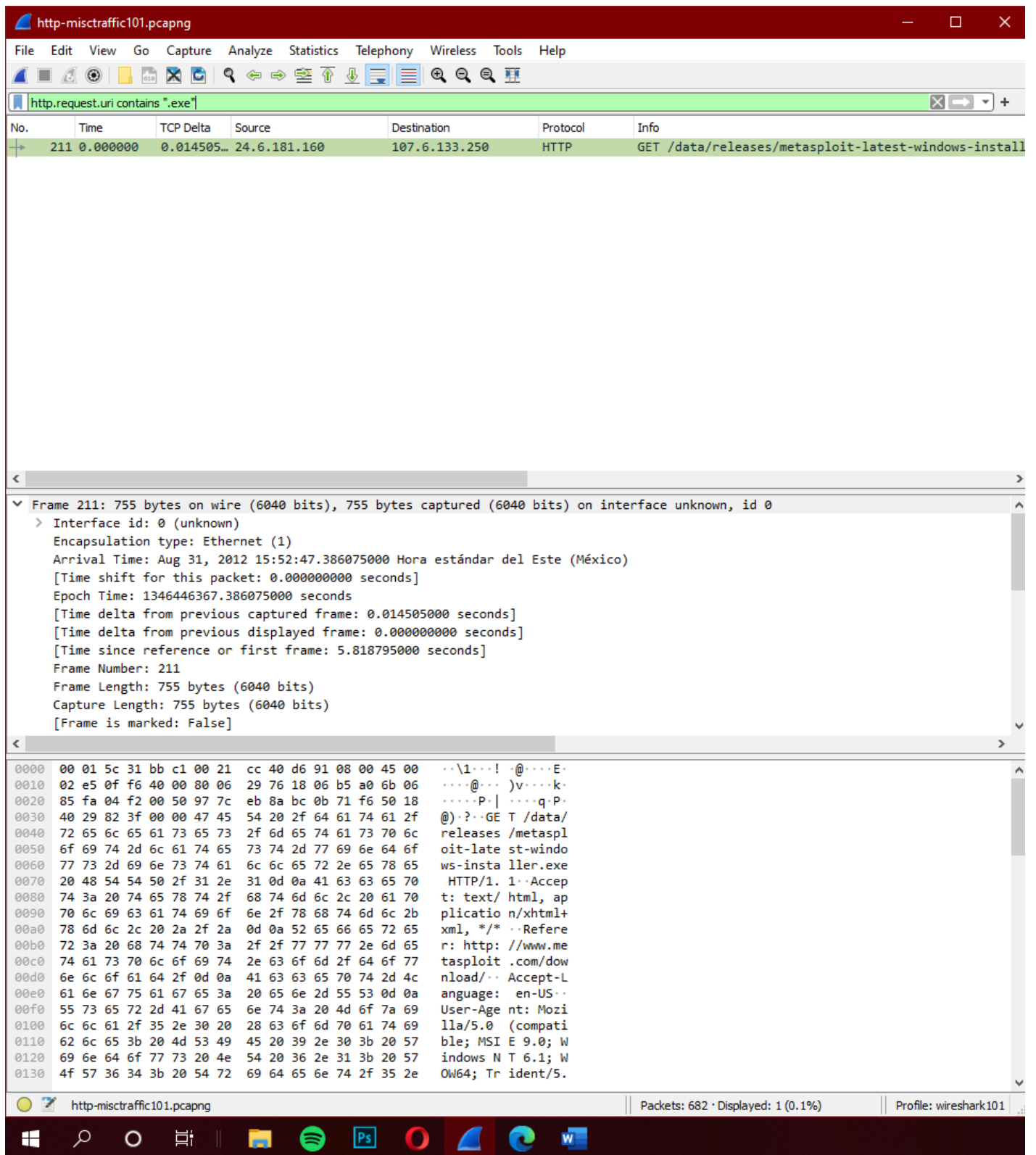
The screenshot shows the Wireshark 'Open Capture File' dialog box. The 'Buscar en:' field is set to 'wireshark101v2files'. The file list contains various .pcapng files, with 'http-misctraffic101.pcapng' selected. The 'Nombre de archivo:' field also contains 'http-misctraffic101.pcapng'. The 'Tipo de archivo:' is set to 'All Files'. The 'Read filter:' is empty, and the 'Format:' is 'Wireshark/... - pcapng'. The 'Size:' is '891KB, 682 data records'. The 'Start / elapsed:' is '2012-08-31 15:52:41 / 00:00:07'. The 'Abrir' button is highlighted.

Below the dialog, the packet list shows the first few packets of the capture:

No.	Time	Source	Destination	Protocol	Length	Info
0000	0.000000	192.168.1.101	192.168.1.1	ICMP	28	Echo (ping) request
0010	0.000000	192.168.1.1	192.168.1.101	ICMP	28	Echo (ping) reply
0020	0.000000	192.168.1.101	192.168.1.1	ICMP	28	Echo (ping) request
0030	0.000000	192.168.1.1	192.168.1.101	ICMP	28	Echo (ping) reply

The status bar at the bottom shows 'net-lost-route.pcapng', 'Packets: 159 · Displayed: 159 (100.0%)', and 'Profile: wireshark101'.

Paso2:



The image shows a Wireshark window titled "http-misctraffic101.pcapng". The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, navigation, and analysis. The filter bar at the top shows the filter "http.request.uri contains '.exe'".

No.	Time	TCP Delta	Source	Destination	Protocol	Info
211	0.000000	0.014505...	24.6.181.160	107.6.133.250	HTTP	GET /data/releases/metasploit-latest-windows-install.exe

Below the packet list, the packet details pane shows the structure of Frame 211:

- Frame 211: 755 bytes on wire (6040 bits), 755 bytes captured (6040 bits) on interface unknown, id 0
 - Interface id: 0 (unknown)
 - Encapsulation type: Ethernet (1)
 - Arrival Time: Aug 31, 2012 15:52:47.386075000 Hora estándar del Este (México)
 - [Time shift for this packet: 0.000000000 seconds]
 - Epoch Time: 1346446367.386075000 seconds
 - [Time delta from previous captured frame: 0.014505000 seconds]
 - [Time delta from previous displayed frame: 0.000000000 seconds]
 - [Time since reference or first frame: 5.818795000 seconds]
 - Frame Number: 211
 - Frame Length: 755 bytes (6040 bits)
 - Capture Length: 755 bytes (6040 bits)
 - [Frame is marked: False]

The packet bytes pane shows the raw data in hexadecimal and ASCII. The ASCII portion of the packet is a GET request for the Metasploit installer:

```
GET /data/releases/metasploit-latest-windows-installer.exe HTTP/1.1
Host: www.metasploit.com/download
Accept: text/html,application/xhtml+xml,*/*
Referer: http://www.metasploit.com/download
Accept-Language: en-US
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
```

The status bar at the bottom indicates "Packets: 682 · Displayed: 1 (0.1%)" and "Profile: wireshark101".

Paso 3:

The image shows the Wireshark network protocol analyzer interface. The main display area shows packet 211, which is an HTTP GET request. The packet list pane on the left shows the packet details, and the packet bytes pane at the bottom shows the raw data. A context menu is open over the TCP layer of the packet, showing various actions like 'Mark/Unmark Packet', 'Ignore/Unignore Packet', 'Set/Unset Time Reference', 'Time Shift...', 'Packet Comment...', 'Edit Resolved Name', 'Apply as Filter', 'Prepare as Filter', 'Conversation Filter', 'Colorize Conversation', 'SCTP', 'Follow', 'Copy', 'Protocol Preferences', 'Decode As...', and 'Show Packet in New Window'. The 'Conversation Filter' option is highlighted, and a sub-menu is open showing a list of network protocols: CIP Connection, Ethernet, F5 TCP, F5 UDP, F5 IP, IEEE 802.15.4, IPv4, IPv6, TCP (highlighted), UDP, ZigBee Network Layer, PN-IO AR, PN-IO AR (with data), and PN-CBA.

http-misctraffic101.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request.uri contains ".exe"

No.	Time	TCP Delta	Source	Destination	Protocol	Info
211	0.000000	0.014505...	24.6.181.160	192.168.1.100	TCP	65535 → 80 [RST] Seq=3123456789 Win=0 Len=0

Frame 211: 755 bytes on wire (6040 bits), 755 bytes captured (6040 bits) on interface 0 (unknown)

Interface id: 0 (unknown)

Encapsulation type: Ethernet (1)

Arrival Time: Aug 31, 2012 15:52:47.386075000

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1346446367.386075000 seconds

[Time delta from previous captured frame: 0.014505000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 5.818795000 seconds]

Frame Number: 211

Frame Length: 755 bytes (6040 bits)

Capture Length: 755 bytes (6040 bits)

[Frame is marked: False]

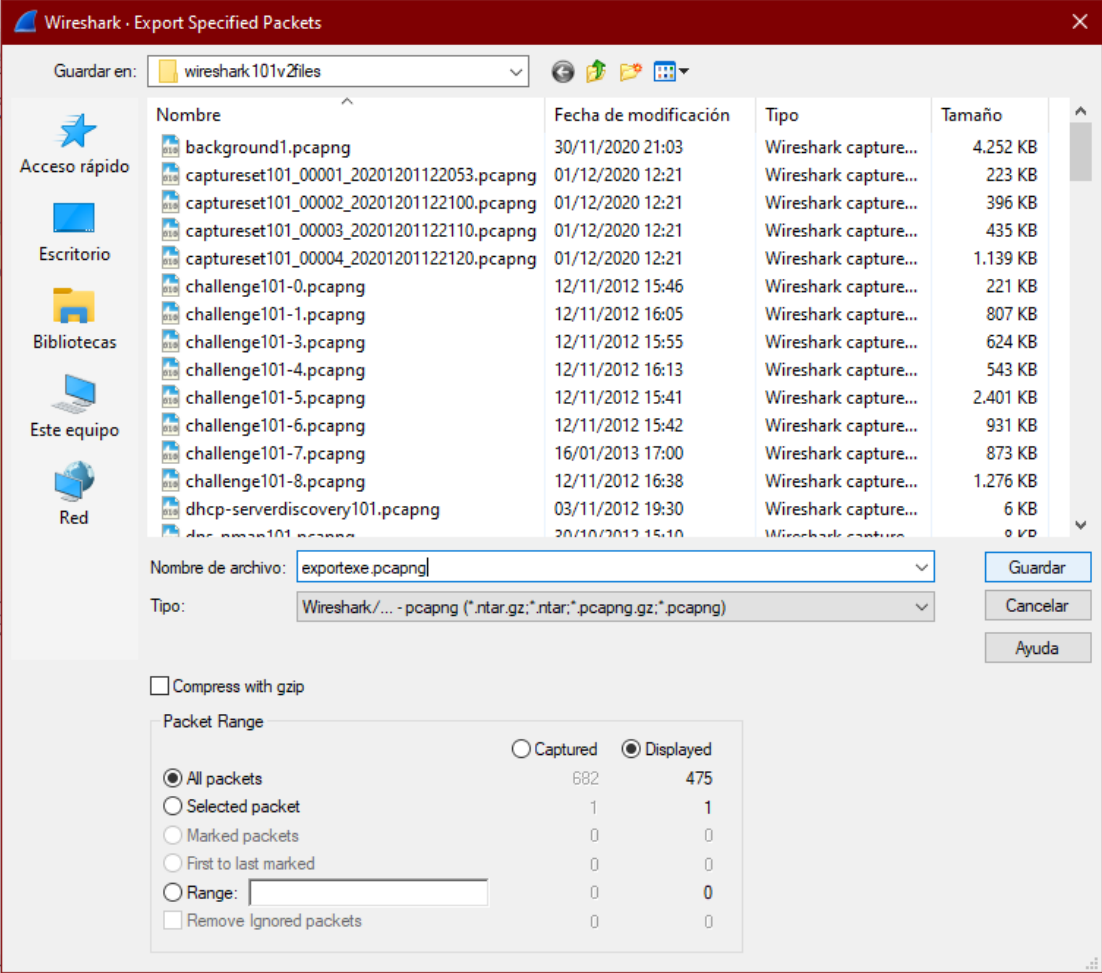
0000 00 01 5c 31 bb c1 00 21 cc 40 d6 91 08 00 45 00 ..\1...! @...E.
0010 02 e5 0f f6 40 00 80 06 29 76 18 06 b5 a0 b6 06@...)v...k.
0020 85 fa 04 f2 00 50 97 7c eb 8a bc 0b 71 f6 50 18P..|q.P.
0030 40 29 82 3f 00 00 47 45 54 20 2f 64 61 74 61 2f @).?...GE T /data/
0040 72 65 6c 65 61 73 65 73 2f 6d 65 74 61 73 70 6c releases /metaspl
0050 6f 69 74 2d 6c 61 74 65 73 74 2d 77 69 6e 64 6f oit-late st-windo
0060 77 73 2d 69 6e 73 74 61 6c 6c 65 72 2e 65 78 65 ws-insta ller.exe
0070 20 48 54 54 50 2f 31 2e 31 0d 0a 41 63 63 65 70 HTTP/1.1..Accep
0080 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 20 61 70 t: text/ html, ap
0090 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b plicatio n/xhtml+
00a0 78 6d 6c 2c 20 2a 2f 2a 0d 0a 52 65 66 65 72 65 xml, /* ..Refere
00b0 72 3a 20 68 74 74 70 3a 2f 2f 77 77 77 2e 6d 65 r: http: //www.me
00c0 74 61 73 70 6c 6f 69 74 2e 63 6f 6d 2f 64 6f 77 tasplot .com/dow
00d0 6e 6c 6f 61 64 2f 0d 0a 41 63 63 65 70 74 2d 4c nload/.. Accept-L
00e0 61 6e 67 75 61 67 65 3a 20 65 6e 2d 55 53 0d 0a anguage: en-US..
00f0 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 User-Age nt: Mozi
0100 6c 6c 61 2f 35 2e 30 20 28 63 6f 6d 70 61 74 69 lla/5.0 (compati
0110 62 6c 65 3b 20 4d 53 49 45 20 39 2e 30 3b 20 57 ble; MSI E 9.0; W
0120 69 6e 64 6f 77 73 20 4e 54 20 36 2e 31 3b 20 57 indows N T 6.1; W
0130 4f 57 36 34 3b 20 54 72 69 64 65 6e 74 2f 35 2e OW64; Tr ident/5.

http-misctraffic101.pcapng

Packets: 682 · Displayed: 1 (0.1%)

Profile: wireshark101

Paso 4:



The image shows the 'Wireshark - Export Specified Packets' dialog box. The 'Guardar en:' field is set to 'wireshark101v2files'. The 'Nombre de archivo:' field is 'exportexe.pcapng'. The 'Tipo:' is 'Wireshark/... - pcapng (*.ntar.gz;*.ntar;*.pcapng.gz;*.pcapng)'. The 'Compress with gzip' checkbox is unchecked. The 'Packet Range' section shows 'All packets' selected, with 682 captured and 475 displayed packets. The 'Guardar' button is highlighted.

Nombre	Fecha de modificación	Tipo	Tamaño
background1.pcapng	30/11/2020 21:03	Wireshark capture...	4,252 KB
captureset101_00001_20201201122053.pcapng	01/12/2020 12:21	Wireshark capture...	223 KB
captureset101_00002_20201201122100.pcapng	01/12/2020 12:21	Wireshark capture...	396 KB
captureset101_00003_20201201122110.pcapng	01/12/2020 12:21	Wireshark capture...	435 KB
captureset101_00004_20201201122120.pcapng	01/12/2020 12:21	Wireshark capture...	1,139 KB
challenge101-0.pcapng	12/11/2012 15:46	Wireshark capture...	221 KB
challenge101-1.pcapng	12/11/2012 16:05	Wireshark capture...	807 KB
challenge101-3.pcapng	12/11/2012 15:55	Wireshark capture...	624 KB
challenge101-4.pcapng	12/11/2012 16:13	Wireshark capture...	543 KB
challenge101-5.pcapng	12/11/2012 15:41	Wireshark capture...	2,401 KB
challenge101-6.pcapng	12/11/2012 15:42	Wireshark capture...	931 KB
challenge101-7.pcapng	16/01/2013 17:00	Wireshark capture...	873 KB
challenge101-8.pcapng	12/11/2012 16:38	Wireshark capture...	1,276 KB
dhcp-serverdiscovery101.pcapng	03/11/2012 19:30	Wireshark capture...	6 KB
des-vmx101.pcapng	20/10/2012 15:10	Wireshark capture...	0 KB

Nombre de archivo: exportexe.pcapng

Tipo: Wireshark/... - pcapng (*.ntar.gz;*.ntar;*.pcapng.gz;*.pcapng)

☐ Compress with gzip

Packet Range

☒ All packets 682 475

☐ Selected packet 1 1

☐ Marked packets 0 0

☐ First to last marked 0 0

☐ Range: 0 0

☐ Remove Ignored packets 0 0

Guardar

Cancelar

Ayuda

0000 00 01 5c 31 bb c1 00 21 cc 40 d6 91 08 00 45 00 ..\1...! .@...E.
0010 02 e5 0f f6 40 00 80 06 29 76 18 06 b5 a0 6b 06@...)v...k.
0020 85 fa 04 f2 00 50 97 7c eb 8a bc 0b 71 f6 50 18P..|q.P.
0030 40 29 82 3f 00 00 47 45 54 20 2f 64 61 74 61 2f @)??...GE T /data/
0040 72 65 6c 65 61 73 65 73 2f 6d 65 74 61 73 70 6c releases /metaspl
0050 6f 69 74 2d 6c 61 74 65 73 74 2d 77 69 6e 64 6f oit-late st-windo
0060 77 73 2d 69 6e 73 74 61 6c 6c 65 72 2e 65 78 65 ws-insta ller.exe
0070 20 48 54 54 50 2f 31 2e 31 0d 0a 41 63 63 65 70 HTTP/1. 1..Accep
0080 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 20 61 70 t: text/ html, ap
0090 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b plicatio n/xhtml+
00a0 78 6d 6c 2c 20 2a 2f 2a 0d 0a 52 65 66 65 72 65 xml, */* ..Refere
00b0 72 3a 20 68 74 74 70 3a 2f 2f 77 77 77 2e 6d 65 r: http: //www.me
00c0 74 61 73 70 6c 6f 69 74 2e 63 6f 6d 2f 64 6f 77 tasexploit .com/dow
00d0 6e 6c 6f 61 64 2f 0d 0a 41 63 63 65 70 74 2d 4c nload/.. Accept-L
00e0 61 6e 67 75 61 67 65 3a 20 65 6e 2d 55 53 0d 0a anguage: en-US..
00f0 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 User-Age nt: Mozi
0100 6c 6c 61 2f 35 2e 30 20 28 63 6f 6d 70 61 74 69 lla/5.0 (compati
0110 62 6c 65 3b 20 4d 53 49 45 20 39 2e 30 3b 20 57 ble; MSI E 9.0; W
0120 69 6e 64 6f 77 73 20 4e 54 20 36 2e 31 3b 20 57 indows N T 6.1; W
0130 4f 57 36 34 3b 20 54 72 69 64 65 6e 74 2f 35 2e OW64; Tr ident/5.

http-misctraffic101.pcapng

Packets: 682 · Displayed: 475 (69.6%)

Profile: wireshark101