

INSTITUTO TECNOLÓGICO DE CANCUN



Nombre De La Materia: Fundamentos De Telecomunicaciones

Nombre De La Unidad: Sistemas de comunicación

N.º De Actividad: Laboratorio 22

Nombre Del Alumno: Vazquez Canto Andres Omar

N.º De Control: 17530439

Lab22- Filter with Wildcards between Words

Paso 1:

The image shows the Wireshark 'Open Capture File' dialog box. The 'Buscar en:' field is set to 'wireshark101v2files'. The file list shows various capture files, with 'http-pictures101.pcapng' selected. The file details section shows the following information:

Nombre de archivo: http-pictures101.pcapng
Tipo de archivo: All Files
Read filter:
Format: Wireshark/... - pcapng
Size: 3752 KiB, 3823 data records
Start / elapsed: 2012-11-02 16:42:50 / 00:01:18

The packet list shows the following details:

Sequence number (raw): 1052604772
[Next sequence number: 21669 (relative sequence number)]
Acknowledgment number: 540491 (relative ack number)
Acknowledgment number (raw): 2417955948
0101 = Header Length: 20 bytes (5)

The packet data shows the following hex and ASCII values:

0020 4e b9 41 0c 00 50 3e bd 79 64 90 1f 14 6c 50 18 N·A·P>· yd··1P·
0030 40 29 ce 94 00 00 47 45 54 20 2f 66 69 6c 65 5f @)···GE T /file_
0040 74 68 75 6d 62 76 69 65 77 5f 61 70 70 72 6f 76 thumbvie w_approv
0050 65 2f 32 31 39 36 38 37 30 30 2f 31 2f 73 74 6f e/219687 00/1/sto
0060 63 6b 2d 70 68 6f 74 6f 2d 32 31 39 36 38 37 30 ck-photo -2196870
0070 30 2d 72 65 61 6c 2d 62 61 62 69 65 73 2d 62 61 0-real-b abies-ba
0080 62 79 2d 62 6f 79 2d 64 72 65 73 73 65 64 2d 69 by-boy-d ressed-i
0090 6e 2d 61 6d 65 72 69 63 61 6e 2d 66 6f 6f 74 62 n-america an-footb
00a0 61 6c 6c 2d 63 6f 73 74 75 6d 65 2e 6a 70 67 20 all-cost ume.jpg
00b0 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 HTTP/1.1 ·Host:
00c0 69 2e 69 73 74 6f 63 6b 69 6d 67 2e 63 6f 6d 0d i.istock img.com·
00d0 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a ·User-Ag ent: Moz
00e0 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 illa/5.0 (Window
00f0 73 20 4e 54 20 36 2e 31 3b 20 57 4f 57 36 34 3b s NT 6.1 ; WOW64;

The status bar at the bottom shows: Flags (12 bits) (tcp.flags), 2 byte(s) | Packets: 3823 · Displayed: 3 (0.1%) | Profile: wireshark101

Paso 2:

The image shows a Wireshark window titled "http-pictures101.pcapng". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture, and analysis. A filter bar at the top displays the filter "http.request.uri matches 'baby.{1,3}smiling'", which has resulted in two packets being displayed in the packet list.

No.	Time	TCP Delta	Source	Destination	Protocol	Info
427	0.000000	0.000529000	24.6.173.220	184.28.78.185	HTTP	GET /file_thumbview_approve/16072653/1/stock-
749	3.539544	0.148145000	24.6.173.220	184.28.78.185	HTTP	GET /file_thumbview_approve/16072653/2/stock-

The packet details pane is currently empty. The status bar at the bottom indicates "Packets: 3823 · Displayed: 2 (0.1%)" and "Profile: wireshark101". The Windows taskbar at the very bottom shows icons for the Start menu, search, task view, File Explorer, Spotify, Photoshop, a red application, a blue application, a 3D application, and Word.

Paso 3:

The image shows a Wireshark packet capture analysis of a file named `http-pictures101.pcapng`. The filter bar at the top is set to `http.request.uri matches "baby.{1,20}smiling"`. The packet list shows three HTTP GET requests from source IP 24.6.173.220 to destination IP 184.28.78.185. The selected packet is packet 404, which is an HTTP GET request for `/file_thumbview_approve/10195917/1/stock-video-10195917-baby-on-belly-smiling.jpg`. The packet details pane shows the following information:

- Frame 404: 468 bytes on wire (3744 bits), 468 bytes captured (3744 bits) on interface `\Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A}`
- Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
- Internet Protocol Version 4, Src: 24.6.173.220, Dst: 184.28.78.185
- Transmission Control Protocol, Src Port: 16650, Dst Port: 80, Seq: 1242, Ack: 35551, Len: 414
 - Source Port: 16650
 - Destination Port: 80
 - [Stream index: 5]
 - [TCP Segment Len: 414]
 - Sequence number: 1242 (relative sequence number)
 - Sequence number (raw): 1993311422
 - [Next sequence number: 1656 (relative sequence number)]
 - Acknowledgment number: 35551 (relative ack number)
 - Acknowledgment number (raw): 2438933624
 - 0101 = Header Length: 20 bytes (5)

The packet bytes pane shows the raw data of the HTTP request, including the GET method, the full URL, and the User-Agent string: `Mozilla/5.0 (Windows NT 6.1; WOW64; rv:16.0) Gecko/20100101 Firefox/16.0`.