

INSTITUTO TECNOLÓGICO DE CANCUN



Nombre De La Materia: Fundamentos De Telecomunicaciones

Nombre De La Unidad: Sistemas de comunicación

N.º De Actividad: Laboratorio

Nombre Del Alumno: Vazquez Canto Andres Omar

N.º De Control: 17530439

Lab21- Filter to Locate a Set of Key Words in a Trace File

The image shows the 'Wireshark - Open Capture File' dialog box. The 'Buscar en:' field is set to 'wireshark101v2files'. The file list contains various .pcapng files. 'http-pictures101.pcapng' is selected. The 'Nombre de archivo:' field is 'http-pictures101.pcapng' and 'Tipo de archivo:' is 'All Files'. The 'Read filter:' is 'Automatically detect file type' and 'Format:' is 'Wireshark/... - pcapng'. The 'Size:' is '3752 KiB, 3823 data records' and 'Start / elapsed:' is '2012-11-02 16:42:50 / 00:01:18'.

Nombre	Fecha de modificación	Tipo	Tamaño
http-jezebel101.pcapng	05/11/2012 20:08	Wireshark capture...	8.204 KB
http-misctrffic101.pcapng	05/11/2012 23:24	Wireshark capture...	892 KB
http-nonstandard101.pcapng	29/10/2012 22:42	Wireshark capture...	685 KB
http-openoffice101a.pcapng	23/10/2012 18:27	Wireshark capture...	90 KB
http-openoffice101b.pcapng	23/10/2012 18:32	Wireshark capture...	19.049 KB
http-pcapnet101.pcapng	24/10/2012 15:05	Wireshark capture...	358 KB
http-pictures101.pcapng	02/11/2012 15:45	Wireshark capture...	3.753 KB
http-sfgate101.pcapng	02/11/2012 11:23	Wireshark capture...	9.225 KB
http-slow101.pcapng	17/11/2012 0:31	Wireshark capture...	1.292 KB
http-wincap101.cap	25/10/2012 22:49	Wireshark capture...	166 KB
http-wiresharkdownload101.pcapng	30/10/2012 0:25	Wireshark capture...	20.714 KB
mybackground101.pcapng	22/10/2012 19:04	Wireshark capture...	73 KB
mydns101_00001_20201201185955.pcapng	01/12/2020 18:59	Wireshark capture...	1 KB
mydns101_00001_20201201190340.pcapng	01/12/2020 19:06	Wireshark capture...	40 KB
mydns101_00002_20201201190000.pcapng	01/12/2020 19:00	Wireshark capture...	5 KB
mydns101_00003_20201201190010.pcapng	01/12/2020 19:00	Wireshark capture...	2 KB
mydns101_00004_20201201190020.pcapng	01/12/2020 19:00	Wireshark capture...	5 KB
mydns101_00005_20201201190030.pcapng	01/12/2020 19:00	Wireshark capture...	1 KB
mydns101_00006_20201201190040.pcapng	01/12/2020 19:00	Wireshark capture...	2 KB
mydns101_00007_20201201190050.pcapng	01/12/2020 19:00	Wireshark capture...	2 KB
mydns101_00008_20201201190100.pcapng	01/12/2020 19:01	Wireshark capture...	1 KB

Sequence number (raw): 3699381746
[Next sequence number: 356 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Acknowledgment number (raw): 13800358
0101 = Header Length: 20 bytes (5)
> Flags: 0x018 (PSH, ACK)
Window size value: 35040
[Calculated window size: 35040]
[Window size scaling factor: -1 (unknown)]
Checksum: 0xce35 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0

0020 4e b9 41 0b 00 50 dc 80 15 f2 00 d2 93 a6 50 18 N·A·P· ·····P·
0030 88 e0 ce 35 00 00 47 45 54 20 2f 66 69 6c 65 2d ···5·GE T /file-
0040 76 69 65 77 2f 61 76 61 74 61 72 2f 69 64 2f 31 view/ava tar/id/1
0050 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a HTTP/1.1 ·Host:
0060 20 69 2e 69 73 74 6f 63 6b 69 6d 67 2e 63 6f 6d i.istoc king.com
0070 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f ·User-A gent: Mo

Flags (12 bits) (tcp.flags), 2 byte(s) | Packets: 3823 · Displayed: 3823 (100.0%) | Profile: wireshark101

Paso 2:

The image shows a Wireshark packet capture window titled "http-pictures101.pcapng". The filter bar at the top contains the text "frame contains 'sombrero'". The packet list pane shows a single packet, No. 1563, at time 0.000000, with a source of 24.6.173.220 and a destination of 184.28.78.185. The protocol is HTTP, and the info field shows a GET request for "/file_thumbview_approve/1626884/1/stock-photo-16268884-baby-boy-wearing-sombrero.jpg".

The packet details pane shows the following information:

- Frame 1563: 472 bytes on wire (3776 bits), 472 bytes captured (3776 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300...}
- 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: 16652, Dst Port: 80, Seq: 9981, Ack: 245610, Len: 418
 - Source Port: 16652
 - Destination Port: 80
 - [Stream index: 2]
 - [TCP Segment Len: 418]
 - Sequence number: 9981 (relative sequence number)
 - Sequence number (raw): 1052593534
 - [Next sequence number: 10399 (relative sequence number)]
 - Acknowledgment number: 245610 (relative ack number)
 - Acknowledgment number (raw): 2417661067
 - 0101 = Header Length: 20 bytes (5)

The packet bytes pane shows the raw data of the HTTP request, including the GET method, the request URI, and the Host header.

Bytes 58-142: Request URI (http.request.uri) | Packets: 3823 · Displayed: 1 (0.0%) | Profile: wireshark101

Paso 3:

The image shows a Wireshark network traffic capture of an HTTP GET request. The top pane shows the packet list with three entries, all of which are GET requests for stock photos. The middle pane shows the packet details for the selected packet (Frame 3418), which is an HTTP GET request. The bottom pane shows the raw packet data in hexadecimal and ASCII. The ASCII data shows the request line: GET /file_thumbview_approve/21968700/1/stock-photo-21968700-real-babies-baby-boy-dressed-in-american-football-costume.jpg HTTP/1.1. The request includes a Host header (i.istockimg.com) and a User-Agent header (Mozilla/5.0 (Windows NT 6.1; WOW64; ...)).

http-pictures101.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

frame matches "(?i)(sombra|football)"

Info

GET /file_thumbview_approve/16268884/1/stock-photo-16268884-baby-boy-wearing-sombrero.jpg HTTP/1.1

GET /file_thumbview_approve/21968700/1/stock-photo-21968700-real-babies-baby-boy-dressed-in-american-football-costume.jpg HTTP/1.1

GET /file_thumbview_approve/21968700/2/stock-photo-21968700-real-babies-baby-boy-dressed-in-american-football-costume.jpg HTTP/1.1

< >

> Frame 3418: 504 bytes on wire (4032 bits), 504 bytes captured (4032 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300} ^

> 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: 16652, Dst Port: 80, Seq: 21219, Ack: 540491, Len: 450

Source Port: 16652

Destination Port: 80

[Stream index: 2]

[TCP Segment Len: 450]

Sequence number: 21219 (relative sequence number)

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)

< >

0020 4e b9 41 0c 00 50 3e bd 79 64 90 1f 14 6c 50 18 N·A·P>· yd···lP·

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-american-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;

Flags (12 bits) (tcp.flags), 2 byte(s) | Packets: 3823 · Displayed: 3 (0.1%) | Profile: wireshark101