



TECNOLOGICO NACIONAL DE MEXICO

INSTITUTO TECNOLÓGICO DE CANCÚN

FUNDAMENTOS DE TELECOMUNICACIONES

Ingeniería en Sistemas Computacionales

ALUMNO: OSWALDO ENRIQUE TUYUB JIMENEZ

DOCENTE: ING. ISMAEL JIMENEZ SANCHEZ

ACTIVIDAD

“LABORATORIO 41”

UNIDAD 3

1)

sec-suspicious101.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

pkt_comment

No.	Time	Source	Destination	Protocol	Comment
1	0.000000	24.6.173.220	74.125.224.84	HTTP	This is the original search query for the "Peter Lik for sale" images.
5	0.062672	74.125.224.84	24.6.173.220	HTTP	In this response, the server sends numerous thumbnail images along with their image URL and HTTP URLs. This response men
7	0.537722	24.6.173.220	74.125.224.84	HTTP	Now we clicked on the image load the expanded thumbnail from Google. We ask for the imgres and imgrefurl1.
12	0.581176	74.125.224.84	24.6.173.220	HTTP	We get the expanded image through Google - there are a lot of web display parameters in this response. So far we are get
14	0.686014	24.6.173.220	77.93.251.49	TCP	We clicked on the web link associated with the expanded image. This launches our connections to the two websites we know
15	0.688118	24.6.173.220	66.11.147.48	TCP	Here we begin connecting to www.artbrokerage.com at 66.11.147.48. The SYN/ACK is in frame 16. Right-click on this packet
18	0.711713	24.6.173.220	66.11.147.48	HTTP	We request an 850x600 size of a Peter Lik photo.
21	0.797738	24.6.173.220	77.93.251.49	HTTP	Now we are making a request to www.ulisseide.org.
23	0.850315	66.11.147.48	24.6.173.220	TCP	This TCP connection is used to get the image files from artbrokerage.com. Check out File Export Objects HTTP

Packet comments

- We request an 850x600 size of a Peter Lik photo.
 - [Expert Info (Comment/Comment): We request an 850x600 size of a Peter Lik photo.]
 - [We request an 850x600 size of a Peter Lik photo.]
 - [Severity level: Comment]
 - [Group: Comment]

> Frame 18: 1099 bytes on wire (8792 bits), 1099 bytes captured (8792 bits) on interface unknown, id 0

> 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: 66.11.147.48

> Transmission Control Protocol, Src Port: 50317, Dst Port: 80, Seq: 1, Ack: 1, Len: 1045

Source Port: 50317

0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00 ... \....d....E-
 0010 04 3d 73 c3 40 00 80 06 00 00 18 06 ad dc 42 0b ... s @....B-
 0020 93 30 c4 8d 00 50 77 42 0f 4f 64 b0 5e 95 50 18 ... 0...PwB ^Od^P-
 0030 40 29 9f 4d 00 00 47 45 54 20 2f 61 72 74 74 68 ... @)H-GE T^arth
 0040 75 6d 62 2f 6c 69 6b 70 5f 33 35 39 31 31 5f 32 ... umb/likp_35911.2
 0050 2f 38 35 30 78 36 30 30 2f 50 65 74 65 72 5f 4c ... /850x600 /Peter_L
 0060 69 6b 5f 42 65 79 6f 6e 64 5f 50 61 72 61 64 69 ... ik_Beyon d_Paradi
 0070 73 65 2e 6a 70 67 20 48 54 54 50 2f 31 2e 31 0d ... se.jpg H TTP/1.1-
 0080 0a 48 6f 73 74 3a 20 77 77 72 2e 61 72 74 62 72 ... :Host: w ww.artbr
 0090 6f 6b 65 72 61 67 65 2e 63 6f 6d 0a 55 73 65 ... okerage.com Use
 00a0 72 2d 41 67 65 6e 74 3a 20 4d 4f 7a 69 6c 6c 61 ... r-Agent: Mozilla
 00b0 2f 35 2e 30 28 57 69 6e 64 6f 77 73 3b 20 55 ... /5.0 (Windows; U
 00c0 3b 20 57 69 6e 64 6f 77 73 20 4e 54 20 36 2e 31 ... ; Window s NT 6.1
 00d0 3b 20 65 6e 2d 55 53 3b 20 72 76 3a 31 2e 39 2e ... ; en-US; rv:1.9.
 00e0 32 2e 31 38 29 20 47 65 63 6b 6f 2f 32 30 31 31 ... 2.18) Gecko/2011

Comment (frame.comment) Paquetes: 172 - Mostrado: 19 (11.0%) - Comentarios: 19 Perfi: wireshark101 12:43 p.m. 07/12/2020

2)

Lab41.pdf

Archivo | C:/Users/zorr... | 1 de 3

Step 1: Open sec-suspicious101.pcapng.

Step 2: In frame 1, right-click on the Packet comments line in the Filter | Selected. Only 19 packets should match your display.

Step 3: Now expand the Packet comments section of frame 1. Right-click with "This is the original..." and select Apply as Column.

Step 4: Select File | Export Packet Dissections | As CSV.

sec-suspicious101.pcapng

Wireshark - Exportar análisis de paquete

Guardar en: wreshark101vZfiles

Nombre: Fecha de modificación: 07/12/2020 12:27 p.m. Tipo: Carpeta de archivos Tamaño:

Acceso rápido: Nueva carpeta

Escritorio

Bibliotecas

Este equipo

Red

Nombre de archivo: Tipo: CSV (Comma Separated Values summary) (*.csv)

Packet Range: ☒ All packets 172 ☐ Captured 49 ☐ Selected packet 1 ☐ Marked packets 0 ☐ First to last marked 0 ☐ Range: 0 ☐ Remove ignored packets 0

Packet Format: ☒ Packet summary line ☒ Include column headings ☒ Packet details: As displayed ☐ Packet Bytes ☐ Each packet on a new page

Guardar Cancelar Ayuda

0000 2f 35 2e 30 28 57 69 6e 64 6f 77 73 20 4e 54 20 36 2e 31 ... /5.0 (Windows; U
 0010 00c0 3b 20 57 69 6e 64 6f 77 73 20 4e 54 20 36 2e 31 ... ; Window s NT 6.1
 0020 00d0 3b 20 65 6e 2d 55 53 3b 20 72 76 3a 31 2e 39 2e ... ; en-US; rv:1.9.
 0030 00e0 32 2e 31 38 29 20 47 65 63 6b 6f 2f 32 30 31 31 ... 2.18) Gecko/2011

Expert Info (exp.expert) Paquetes: 172 - Mostrado: 49 (28.5%) - Comentarios: 19 Perfi: wireshark101 12:58 p.m. 07/12/2020

3)

suspicious101 - Excel

Oswaldo Enrique Tuyub Jimenez

¿Qué desea hacer?

Archivo Inicio Insertar Disposición de página Fórmulas Datos Revisar Vista Ayuda

Formato condicional Dar formato como tabla Estilos de celda

Insertar Eliminar Formato

Ordenar y filtrar Buscar y seleccionar

Confidencialidad

Portapapeles Fuente Alineación Número

No.	Time	Source	Destination	Protocol	Comment	Info
15	0.608118	24.6.173.220	66.11.147.48	TCP	Here we beg	50317 > 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
16	0.711027	66.11.147.48	24.6.173.220	TCP		80 > 50317 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
17	0.711148	24.6.173.220	66.11.147.48	TCP		50317 > 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
18	0.711713	24.6.173.220	66.11.147.48	HTTP	We request	GET /artthumb/likp_35911_2/850x600/Peter_Lik_Beyond_Paradise.jpg HTTP/1.1
22	0.812627	66.11.147.48	24.6.173.220	TCP		80 > 50317 [ACK] Seq=1 Ack=1046 Win=7936 Len=0
23	0.959215	66.11.147.48	24.6.173.220	TCP	This TCP con	80 > 50317 [ACK] Seq=1 Ack=1046 Win=7936 Len=1460 [TCP segment of a reassembled PDU]
24	0.960196	66.11.147.48	24.6.173.220	TCP		80 > 50317 [ACK] Seq=1461 Ack=1046 Win=7936 Len=1460 [TCP segment of a reassembled PDU]
25	0.960308	24.6.173.220	66.11.147.48	TCP		50317 > 80 [ACK] Seq=1046 Ack=2921 Win=65700 Len=0
27	1.061108	66.11.147.48	24.6.173.220	TCP		80 > 50317 [ACK] Seq=2921 Ack=1046 Win=7936 Len=1460 [TCP segment of a reassembled PDU]
28	1.062024	66.11.147.48	24.6.173.220	TCP		80 > 50317 [ACK] Seq=4381 Ack=1046 Win=7936 Len=1460 [TCP segment of a reassembled PDU]
29	1.062035	66.11.147.48	24.6.173.220	TCP		80 > 50317 [ACK] Seq=5841 Ack=1046 Win=7936 Len=1460 [TCP segment of a reassembled PDU]
30	1.062215	24.6.173.220	66.11.147.48	TCP		50317 > 80 [ACK] Seq=1046 Ack=7301 Win=65700 Len=0
31	1.163737	66.11.147.48	24.6.173.220	TCP		80 > 50317 [ACK] Seq=7301 Ack=1046 Win=7936 Len=1460 [TCP segment of a reassembled PDU]
32	1.164689	66.11.147.48	24.6.173.220	TCP		80 > 50317 [ACK] Seq=8761 Ack=1046 Win=7936 Len=1460 [TCP segment of a reassembled PDU]
33	1.164838	24.6.173.220	66.11.147.48	TCP		50317 > 80 [ACK] Seq=1046 Ack=10221 Win=65700 Len=0
34	1.165679	66.11.147.48	24.6.173.220	TCP		80 > 50317 [ACK] Seq=10221 Ack=1046 Win=7936 Len=1460 [TCP segment of a reassembled PDU]
35	1.165683	66.11.147.48	24.6.173.220	TCP		80 > 50317 [ACK] Seq=11681 Ack=1046 Win=7936 Len=1460 [TCP segment of a reassembled PDU]
36	1.16586	24.6.173.220	66.11.147.48	TCP		50317 > 80 [ACK] Seq=1046 Ack=13141 Win=65700 Len=0
37	1.266689	66.11.147.48	24.6.173.220	TCP		80 > 50317 [ACK] Seq=13141 Ack=1046 Win=7936 Len=1460 [TCP segment of a reassembled PDU]
38	1.267598	66.11.147.48	24.6.173.220	TCP		80 > 50317 [ACK] Seq=14601 Ack=1046 Win=7936 Len=1460 [TCP segment of a reassembled PDU]
39	1.267698	24.6.173.220	66.11.147.48	TCP		50317 > 80 [ACK] Seq=1046 Ack=16061 Win=65700 Len=0
40	1.26851	66.11.147.48	24.6.173.220	TCP		80 > 50317 [ACK] Seq=16061 Ack=1046 Win=7936 Len=1460 [TCP segment of a reassembled PDU]

suspicious101

01:00 p. m. 07/12/2020