TECNOLÓGICO NACIONAL DE MÉXICO

INSTITUTO TECNOLOGICO DE CANCUN

SISTEMAS COMPUTACIONALES

MATERIA: Fundamentos de Telecomunicaciones

PROFESOR: ING. ISMAEL JIMÉNEZ SÁNCHEZ

LABORATORIO: 40

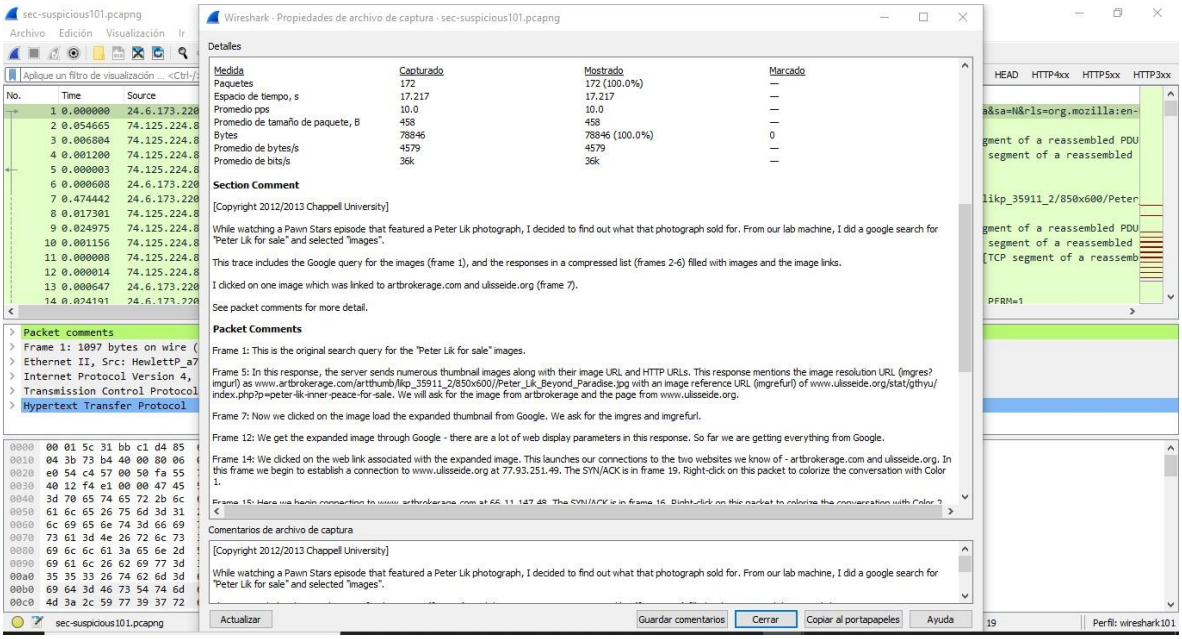
Alumno:

SARRAGOT PASTRANA WILIAM ADRIEN

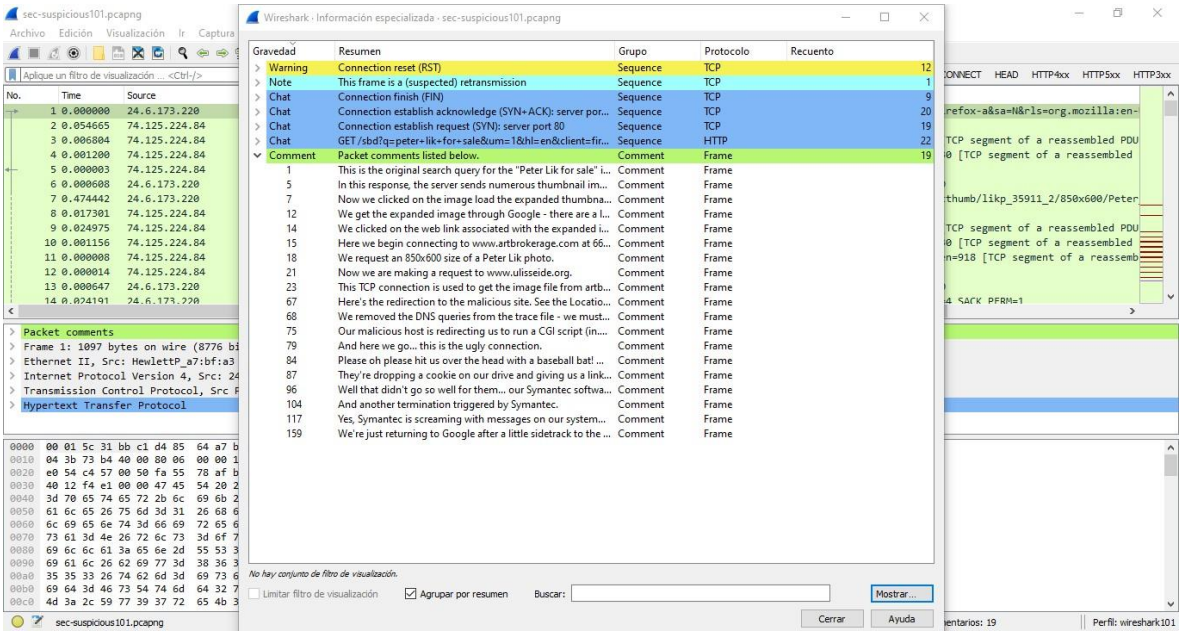
LAB40 - READ ANALYSIS NOTES IN A MALICIOUS REDIRECTION TRACE FILE 1

Paso 1: Abrir el documento sec.suspicous101.pcapng

Paso 2 : Le damos click en el botón de Annotation y saldrán las propiedades del archivo.



Paso 3: Pasamos a darle click en el botón de Expert Information y expandimos Comments y podemos observar los diferentes comentarios que contiene los paquetes en el archivo.


sec-suspicious101.pcapng
Archivo Edición Visualización Ir Captura
Aplique un filtro de visualización ... <Ctrl-/>
No. Time Source
1 0.000000 24.6.173.220
2 0.054665 74.125.224.84
3 0.006804 74.125.224.84
4 0.001200 74.125.224.84
5 0.000003 74.125.224.84
6 0.000608 24.6.173.220
7 0.474442 24.6.173.220
8 0.017301 74.125.224.84
9 0.024975 74.125.224.84
10 0.001156 74.125.224.84
11 0.000008 74.125.224.84
12 0.000014 74.125.224.84
13 0.000647 24.6.173.220
14 0.024191 24.6.173.220
Packet comments
Frame 1: 1097 bytes on wire (8776 bi
Ethernet II, Src: HewlettP_a7:bf:a3
Internet Protocol Version 4, Src: 24
Transmission Control Protocol, Src P
Hypertext Transfer Protocol
0000 00 01 5c 31 bb c1 d4 85 64 a7 b
0010 04 3b 73 b4 40 00 80 06 00 00 1
0020 e0 54 c4 57 00 50 fa 55 78 af b
0030 40 12 f4 e1 00 00 47 45 54 20 2
0040 3d 70 65 74 65 72 2b 6c 69 6b 2
0050 61 6c 65 26 75 6d 3d 31 26 68 6
0060 6c 69 65 6e 74 3d 66 69 72 65 6
0070 73 61 3d 4e 26 72 6c 73 3d 6f 7
0080 69 6c 6c 61 3a 65 6e 2d 55 53 3
0090 69 61 6c 26 62 69 77 3d 38 36 3
00a0 35 35 33 26 74 62 6d 3d 69 73 6
00b0 69 64 3d 46 73 54 74 6d 64 32 7
00c0 4d 3a 2c 59 77 39 37 72 65 4b 3
sec-suspicious101.pcapng
Wireshark · Información especializada · sec-suspicious101.pcapng
Gravedad Resumen Grupo Protocolo Recuento
Warning Connection reset (RST) Sequence TCP 12
Note This frame is a (suspected) retransmission Sequence TCP 1
Chat Connection finish (FIN) Sequence TCP 9
Chat Connection establish acknowledge (SYN+ACK): server por... Sequence TCP 20
Chat Connection establish request (SYN): server port 80 Sequence TCP 19
Chat GET /sbd?q=peter+lik+for+sale&um=1&hl=en&client=fir... Sequence HTTP 22
Comment Packet comments listed below. Comment Frame 19
1 This is the original search query for the "Peter Lik for sale" i... Comment Frame
5 In this response, the server sends numerous thumbnail im... Comment Frame
7 Now we clicked on the image load the expanded thumbna... Comment Frame
12 We get the expanded image through Google - there are a l... Comment Frame
14 We clicked on the web link associated with the expanded i... Comment Frame
15 Here we begin connecting to www.artbrokerage.com at 66... Comment Frame
18 We request an 850x600 size of a Peter Lik photo. Comment Frame
21 Now we are making a request to www.ulisseide.org. Comment Frame
23 This TCP connection is used to get the image file from artb... Comment Frame
67 Here's the redirection to the malicious site. See the Locatio... Comment Frame
68 We removed the DNS queries from the trace file - we must... Comment Frame
75 Our malicious host is redirecting us to run a CGI script (in.... Comment Frame
79 And here we go... this is the ugly connection. Comment Frame
84 Please oh please hit us over the head with a baseball bat! ... Comment Frame
87 They're dropping a cookie on our drive and giving us a link... Comment Frame
96 Well that didn't go so well for them... our Symantec softwa... Comment Frame
104 And another termination triggered by Symantec. Comment Frame
117 Yes, Symantec is screaming with messages on our system... Comment Frame
159 We're just returning to Google after a little sidetrack to the ... Comment Frame
No hay conjunto de filtro de visualización.
Limitar filtro de visualización
Agrupar por resumen
Buscar:
Mostrar...
Cerrar
Ayuda
CONNECT HEAD HTTP4xx HTTP5xx HTTP3xx
refox-a&sa=N&rls=org.mozilla:en-
TCP segment of a reassembled PDU
0 [TCP segment of a reassembled
thumb/likp_35911_2/850x600/Peter
TCP segment of a reassembled PDU
0 [TCP segment of a reassembled
n=918 [TCP segment of a reassemb
4 SACK_PERM=1
entarios: 19
Perfil: wireshark101

Paso 4 : Le damos click a cualquier comentario y nos dirigirá al paquete en el que esta