TECNOLOGICO NACIONAL DE MEXICO

INSTITUTO TECNOLÓGICO DE CANCÚN

FUNDAMENTOS DE TELECOMUNICACIONES

Ingeniería en Sistemas Computacionales

ALUMNO: OSWALDO ENRIQUE TUYUB JIMENEZ

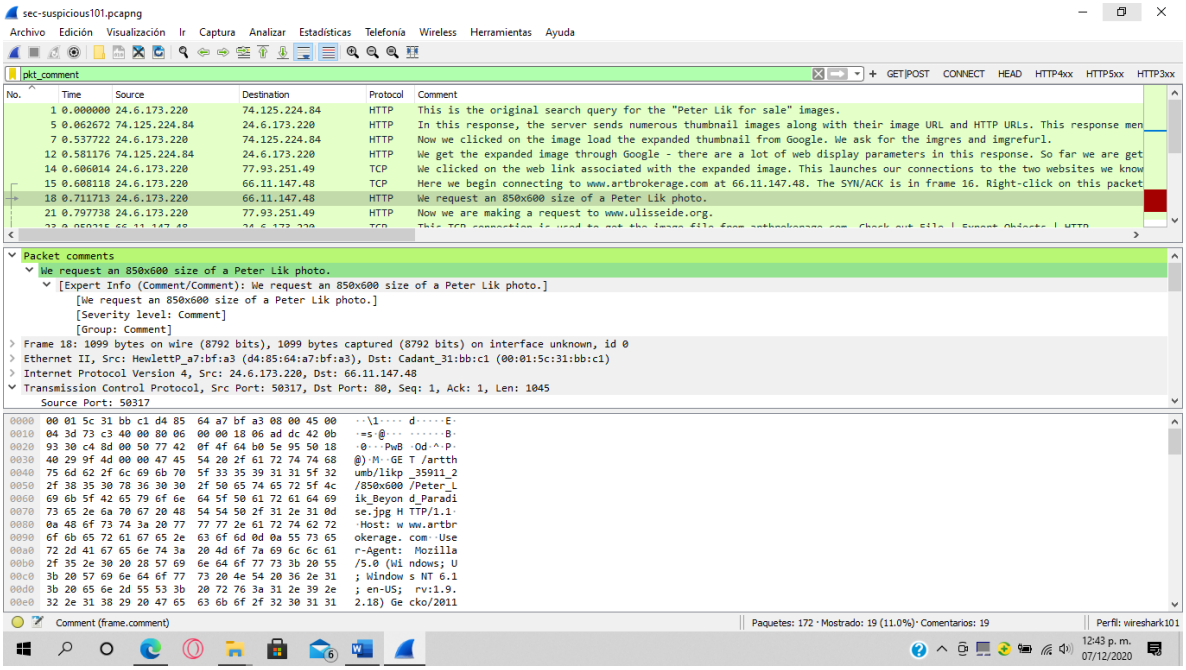
DOCENTE: ING. ISMAEL JIMENEZ SANCHEZ

ACTIVIDAD

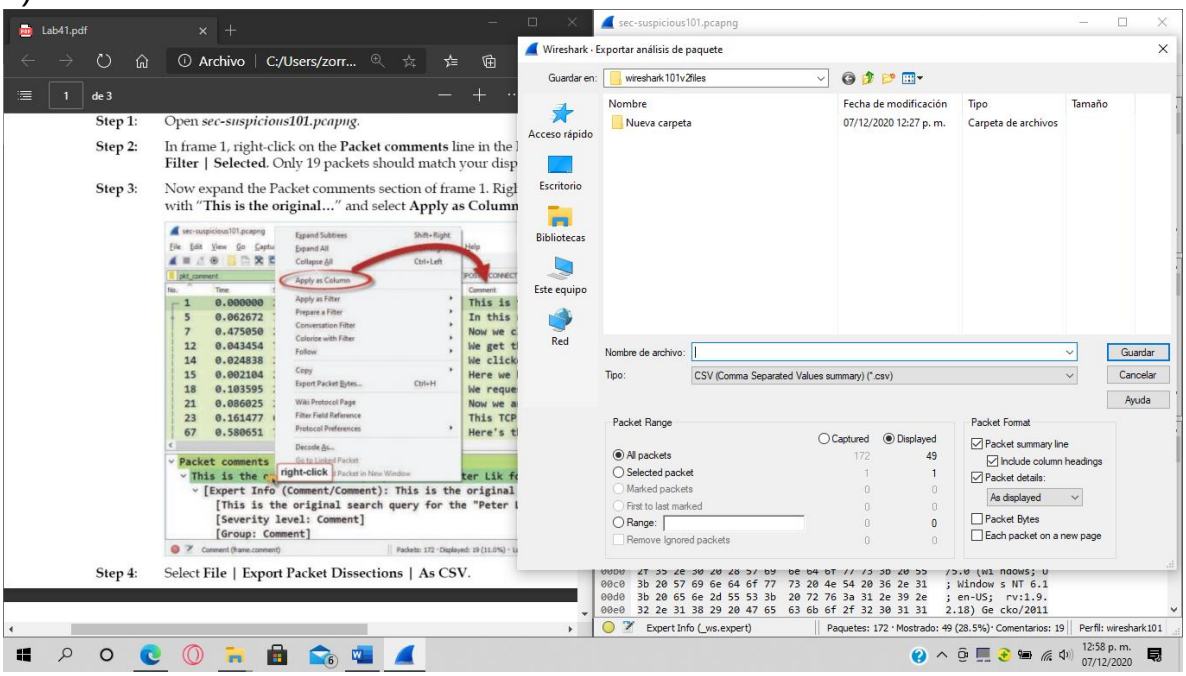
“LABORATORIO 41”

UNIDAD 3

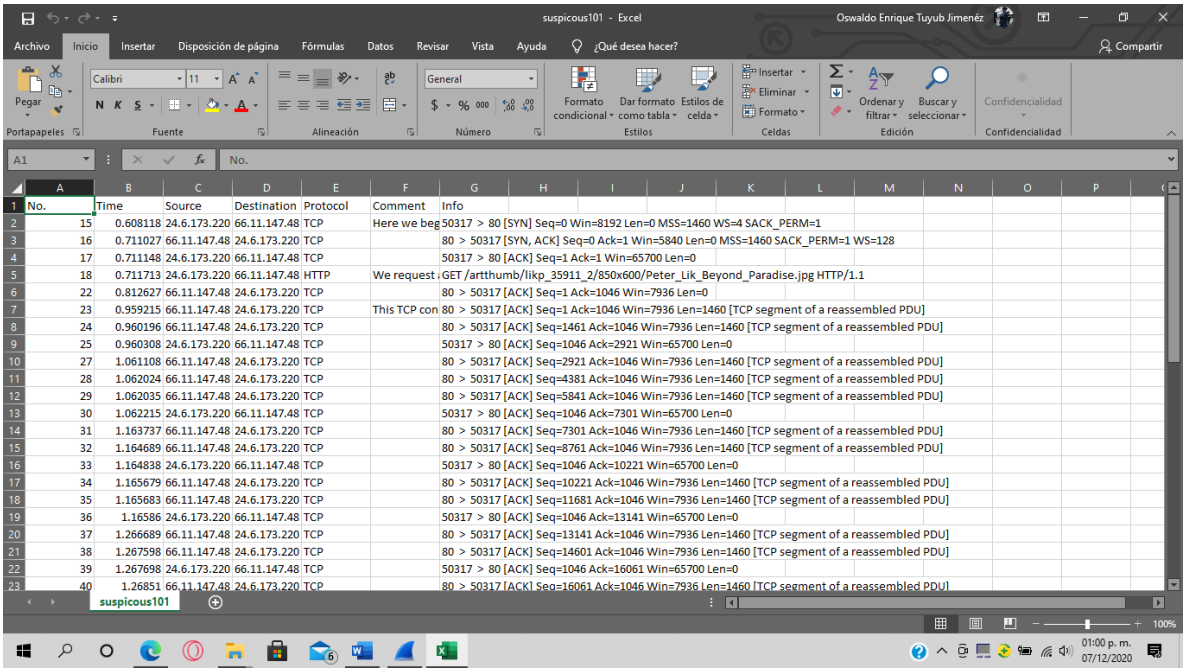
1)


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 imgrefurl.
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 0.606014 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 0.608118 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.uliseside.org.
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
Comment (frame.comment)
Paquetes: 172 · Mostrado: 19 (11.0%) · Comentarios: 19
Perfil: 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 disp
Step 3: Now expand the Packet comments section of frame 1. Rig
with "This is the original..." and select Apply as Column
right-click
Step 4: Select File | Export Packet Dissections | As CSV.
sec-suspicious101.pcapng
Wireshark · Exportar análisis de paquete
Guardar en: wireshark101v2files
Acceso rápido
Escritorio
Bibliotecas
Este equipo
Red
Nombre
Nueva carpeta
Fecha de modificación
07/12/2020 12:27 p. m.
Tipo
Carpeta de archivos
Tamaño
Nombre de archivo:
Tipo: CSV (Comma Separated Values summary) (*.csv)
Guardar
Cancelar
Ayuda
Packet Range
Captured
Displayed
All packets 172 49
Selected packet 1 1
Marked packets 0 0
First to last marked 0 0
Range: 0 0
Remove Ignored packets 0 0
Packet Format
Packet summary line
Include column headings
Packet details:
As displayed
Packet Bytes
Each packet on a new page
Expert Info (_ws.expert)
Paquetes: 172 · Mostrado: 49 (28.5%) · Comentarios: 19
Perfil: wireshark101
12:58 p. m.
07/12/2020

3)




| 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] |