INSTITUTO TECNOLOGICO DE CANCUN

Nombre De La Materia: Fundamentos De Telecomunicaciones

Nombre De La Unidad: Sistemas de comunicación

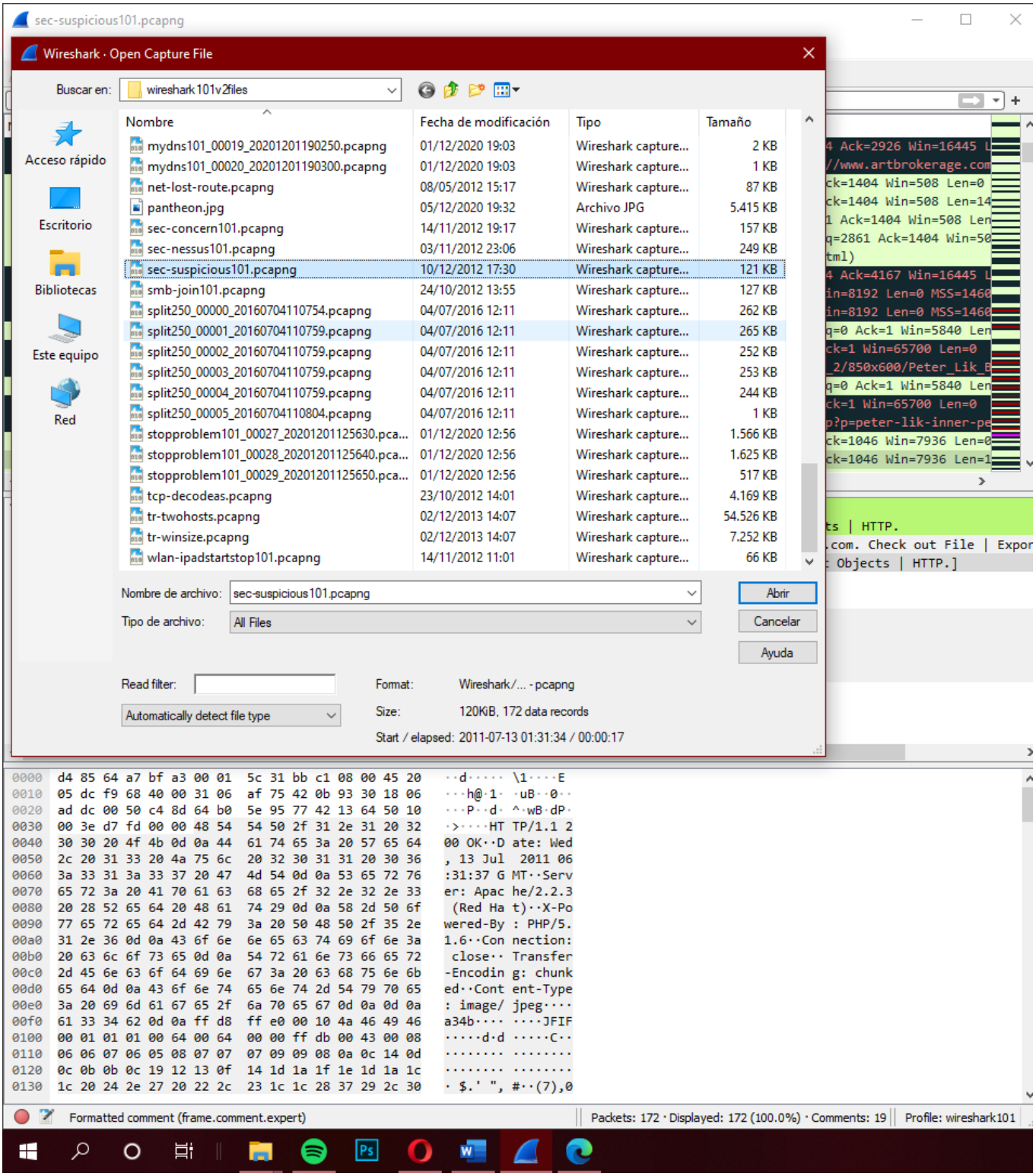
N.º De Actividad: Laboratorio 41

Nombre Del Alumno: Vazquez Canto Andres Omar

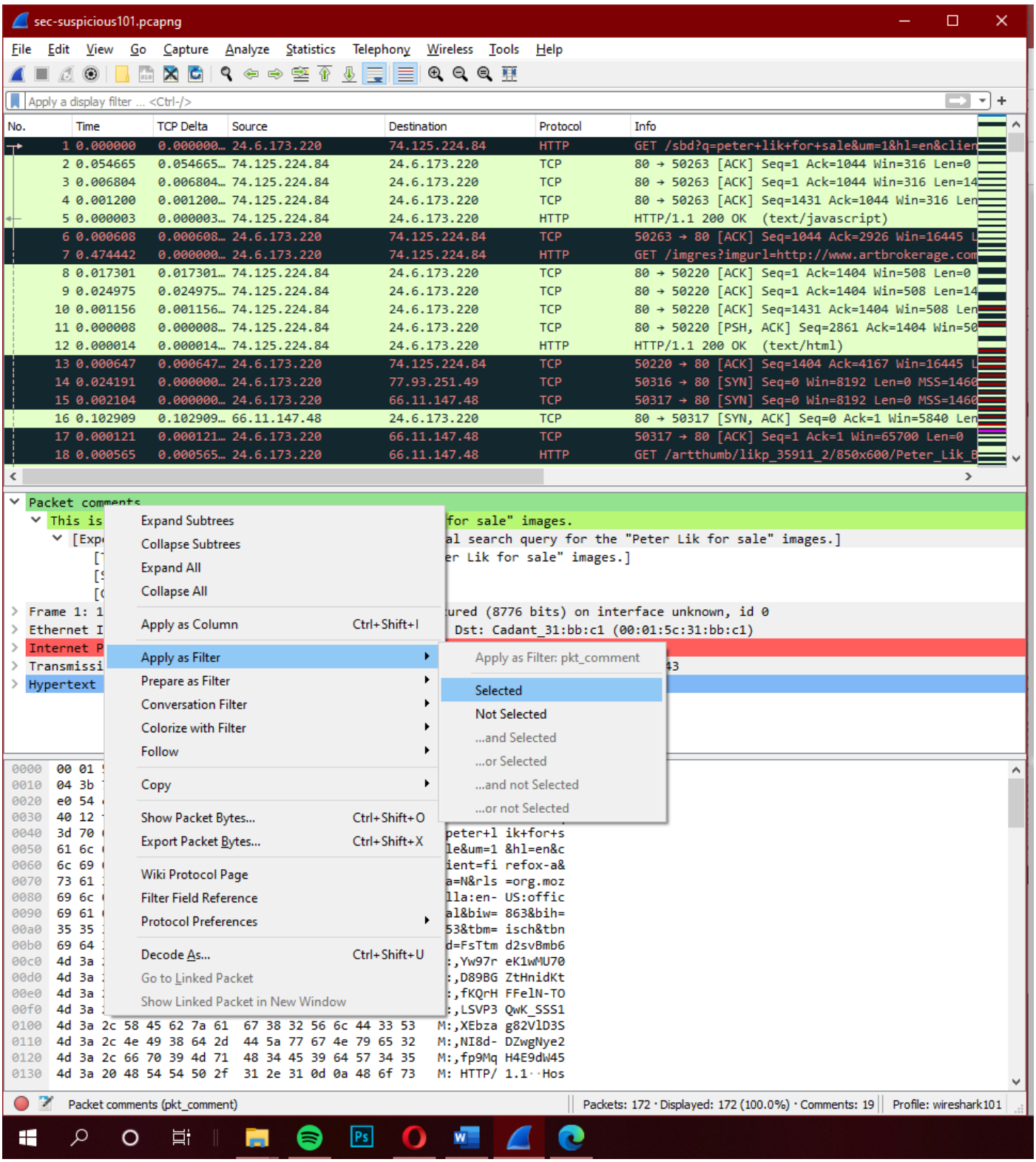
N.º De Control: 17530439

Lab41- Export Malicious Redirection Packet Comments

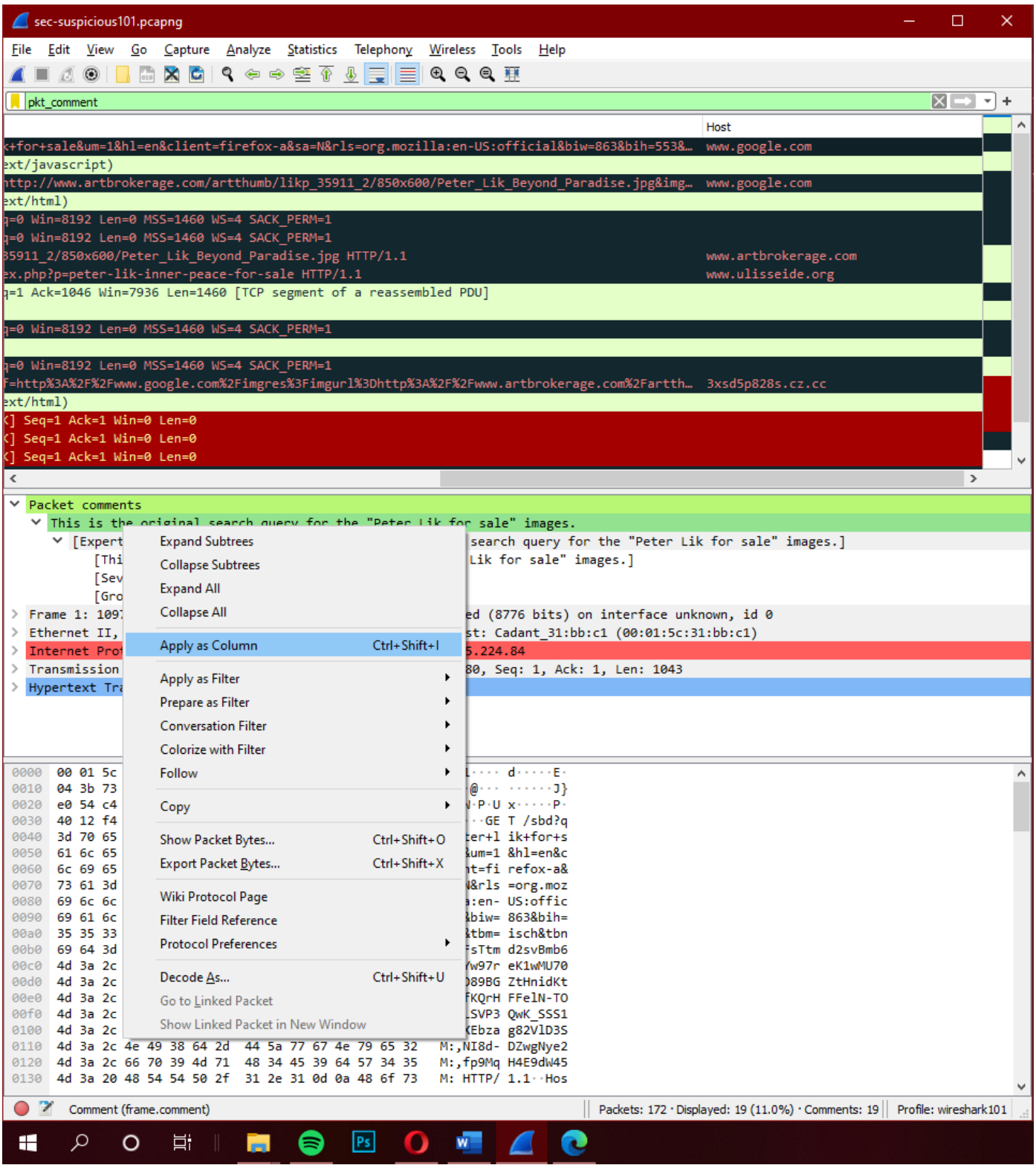
Paso 1:



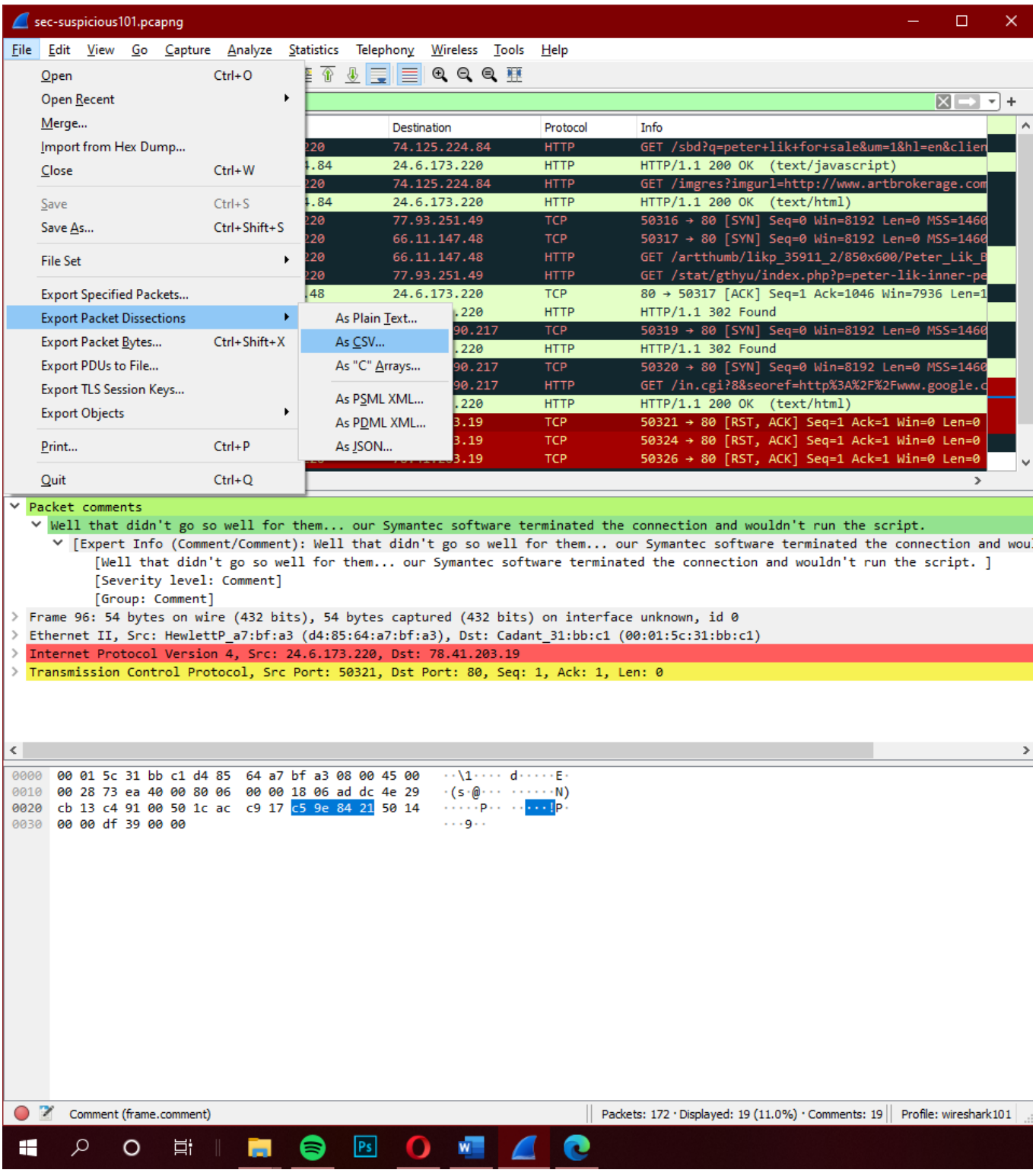
Paso 2:

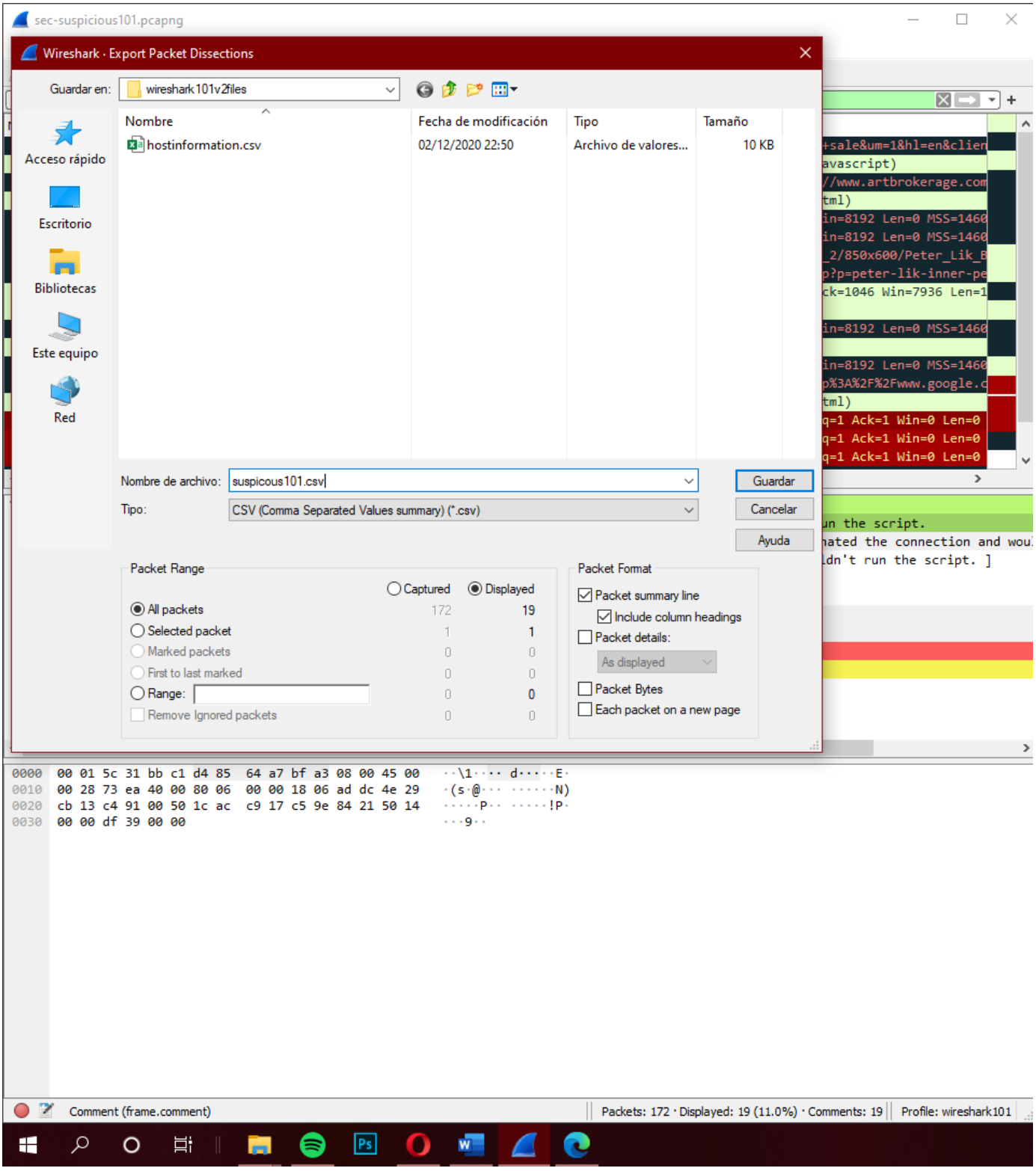

sec-suspicious101.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time TCP Delta Source Destination Protocol Info
1 0.000000 0.000000… 24.6.173.220 74.125.224.84 HTTP GET /sbd?q=peter+lik+for+sale&um=1&hl=en&clien
2 0.054665 0.054665… 74.125.224.84 24.6.173.220 TCP 80 → 50263 [ACK] Seq=1 Ack=1044 Win=316 Len=0
3 0.006804 0.006804… 74.125.224.84 24.6.173.220 TCP 80 → 50263 [ACK] Seq=1 Ack=1044 Win=316 Len=14
4 0.001200 0.001200… 74.125.224.84 24.6.173.220 TCP 80 → 50263 [ACK] Seq=1431 Ack=1044 Win=316 Len
5 0.000003 0.000003… 74.125.224.84 24.6.173.220 HTTP HTTP/1.1 200 OK (text/javascript)
6 0.000608 0.000608… 24.6.173.220 74.125.224.84 TCP 50263 → 80 [ACK] Seq=1044 Ack=2926 Win=16445 L
7 0.474442 0.000000… 24.6.173.220 74.125.224.84 HTTP GET /imgres?imgurl=http://www.artbrokerage.com
8 0.017301 0.017301… 74.125.224.84 24.6.173.220 TCP 80 → 50220 [ACK] Seq=1 Ack=1404 Win=508 Len=0
9 0.024975 0.024975… 74.125.224.84 24.6.173.220 TCP 80 → 50220 [ACK] Seq=1 Ack=1404 Win=508 Len=14
10 0.001156 0.001156… 74.125.224.84 24.6.173.220 TCP 80 → 50220 [ACK] Seq=1431 Ack=1404 Win=508 Len
11 0.000008 0.000008… 74.125.224.84 24.6.173.220 TCP 80 → 50220 [PSH, ACK] Seq=2861 Ack=1404 Win=50
12 0.000014 0.000014… 74.125.224.84 24.6.173.220 HTTP HTTP/1.1 200 OK (text/html)
13 0.000647 0.000647… 24.6.173.220 74.125.224.84 TCP 50220 → 80 [ACK] Seq=1404 Ack=4167 Win=16445 L
14 0.024191 0.000000… 24.6.173.220 77.93.251.49 TCP 50316 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
15 0.002104 0.000000… 24.6.173.220 66.11.147.48 TCP 50317 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
16 0.102909 0.102909… 66.11.147.48 24.6.173.220 TCP 80 → 50317 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len
17 0.000121 0.000121… 24.6.173.220 66.11.147.48 TCP 50317 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
18 0.000565 0.000565… 24.6.173.220 66.11.147.48 HTTP GET /artthumb/likp_35911_2/850x600/Peter_Lik_B
Packet comments
Frame 1: 1
Ethernet I
Internet P
Transmissi
Hypertext
Expand Subtrees
Collapse Subtrees
Expand All
Collapse All
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes... Ctrl+Shift+O
Export Packet Bytes... Ctrl+Shift+X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As... Ctrl+Shift+U
Go to Linked Packet
Show Linked Packet in New Window
Apply as Filter: pkt_comment
Selected
Not Selected
...and Selected
...or Selected
...and not Selected
...or not Selected
Packet comments (pkt_comment)
Packets: 172 · Displayed: 172 (100.0%) · Comments: 19
Profile: wireshark101

Paso 3:

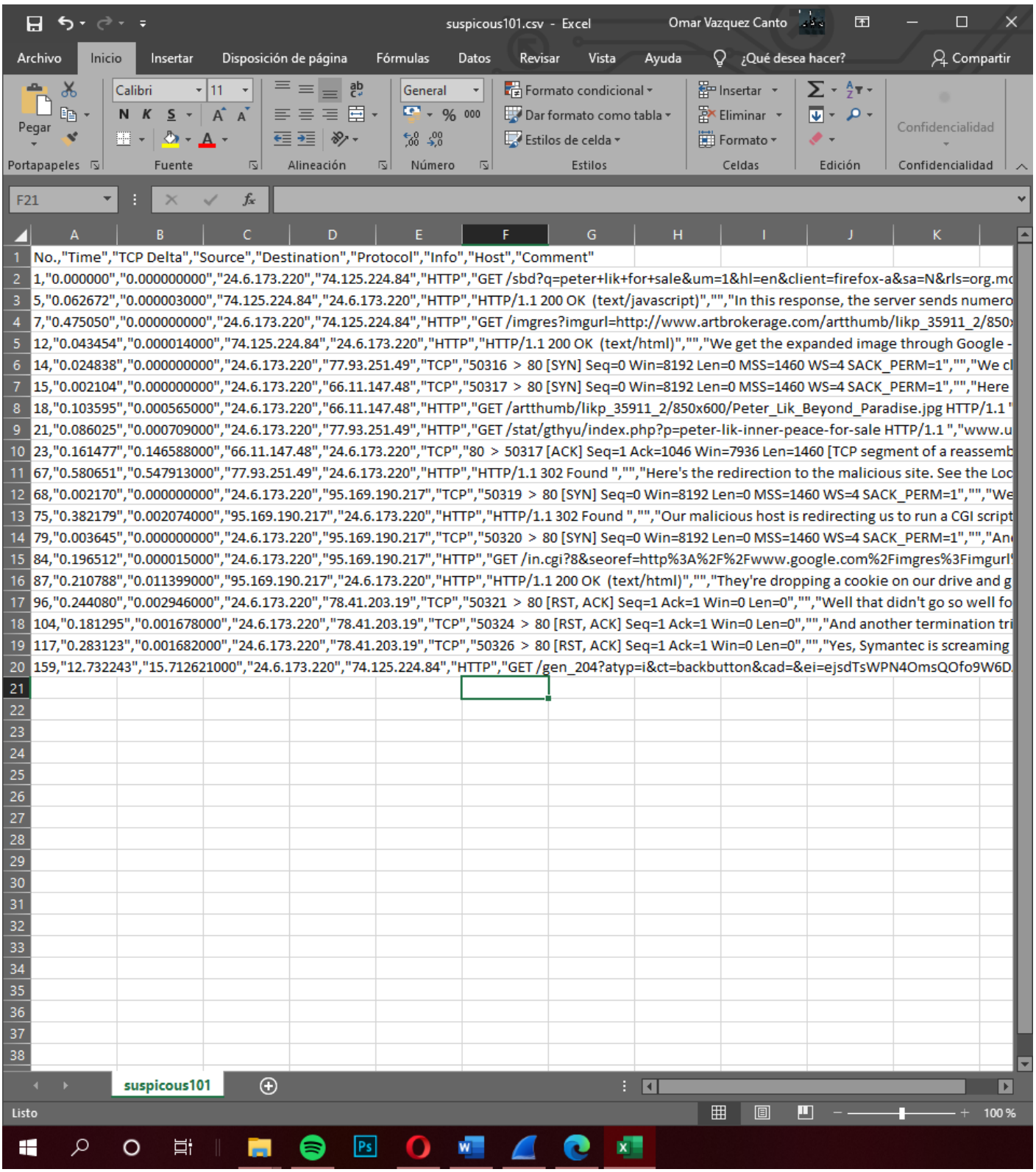

sec-suspicious101.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
pkt_comment
Host
www.google.com
www.google.com
www.artbrokerage.com
www.ulisseide.org
3xsd5p828s.cz.cc
Packet comments
Expand Subtrees
Collapse Subtrees
Expand All
Collapse All
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes... Ctrl+Shift+O
Export Packet Bytes... Ctrl+Shift+X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As... Ctrl+Shift+U
Go to Linked Packet
Show Linked Packet in New Window
Comment (frame.comment)
Packets: 172 · Displayed: 19 (11.0%) · Comments: 19
Profile: wireshark101

Paso 4 y 5:


sec-suspicious101.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Open Ctrl+O
Open Recent
Merge...
Import from Hex Dump...
Close Ctrl+W
Save Ctrl+S
Save As... Ctrl+Shift+S
File Set
Export Specified Packets...
Export Packet Dissections
Export Packet Bytes... Ctrl+Shift+X
Export PDUs to File...
Export TLS Session Keys...
Export Objects
Print... Ctrl+P
Quit Ctrl+Q
As Plain Text...
As CSV...
As "C" Arrays...
As PSML XML...
As PDML XML...
As JSON...
Destination Protocol Info
74.125.224.84 HTTP GET /sbd?q=peter+lik+for+sale&um=1&hl=en&clien
24.6.173.220 HTTP HTTP/1.1 200 OK (text/javascript)
74.125.224.84 HTTP GET /imgres?imgurl=http://www.artbrokerage.com
24.6.173.220 HTTP HTTP/1.1 200 OK (text/html)
77.93.251.49 TCP 50316 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
66.11.147.48 TCP 50317 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
66.11.147.48 HTTP GET /artthumb/likp_35911_2/850x600/Peter_Lik_B
77.93.251.49 HTTP GET /stat/gthyu/index.php?p=peter-lik-inner-pe
24.6.173.220 TCP 80 → 50317 [ACK] Seq=1 Ack=1046 Win=7936 Len=1
HTTP HTTP/1.1 302 Found
TCP 50319 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
HTTP HTTP/1.1 302 Found
TCP 50320 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
HTTP GET /in.cgi?8&seoref=http%3A%2F%2Fwww.google.c
HTTP HTTP/1.1 200 OK (text/html)
TCP 50321 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
TCP 50324 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
TCP 50326 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
Packet comments
Well that didn't go so well for them... our Symantec software terminated the connection and wouldn't run the script.
[Expert Info (Comment/Comment): Well that didn't go so well for them... our Symantec software terminated the connection and wou
[Well that didn't go so well for them... our Symantec software terminated the connection and wouldn't run the script.]
[Severity level: Comment]
[Group: Comment]
Frame 96: 54 bytes on wire (432 bits), 54 bytes captured (432 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: 78.41.203.19
Transmission Control Protocol, Src Port: 50321, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00
0010 00 28 73 ea 40 00 80 06 00 00 18 06 ad dc 4e 29
0020 cb 13 c4 91 00 50 1c ac c9 17 c5 9e 84 21 50 14
0030 00 00 df 39 00 00
Comment (frame.comment)
Packets: 172 · Displayed: 19 (11.0%) · Comments: 19
Profile: wireshark101


sec-suspicious101.pcapng
Wireshark · Export Packet Dissections
Guardar en:
wireshark101v2files
Acceso rápido
Escritorio
Bibliotecas
Este equipo
Red
Nombre
Fecha de modificación
Tipo
Tamaño
hostinformation.csv
02/12/2020 22:50
Archivo de valores...
10 KB
Nombre de archivo:
suspicous101.csv
Tipo:
CSV (Comma Separated Values summary) (*.csv)
Guardar
Cancelar
Ayuda
Packet Range
Captured
Displayed
All packets
172
19
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
0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00
0010 00 28 73 ea 40 00 80 06 00 00 18 06 ad dc 4e 29
0020 cb 13 c4 91 00 50 1c ac c9 17 c5 9e 84 21 50 14
0030 00 00 df 39 00 00
Comment (frame.comment)
Packets: 172 · Displayed: 19 (11.0%) · Comments: 19
Profile: wireshark101

Paso 6:


suspicous101.csv - Excel
Omar Vazquez Canto
Archivo
Inicio
Insertar
Disposición de página
Fórmulas
Datos
Revisar
Vista
Ayuda
¿Qué desea hacer?
Compartir
Pegar
Calibri
11
General
Formato condicional
Dar formato como tabla
Estilos de celda
Insertar
Eliminar
Formato
Confidencialidad
Portapapeles
Fuente
Alineación
Número
Estilos
Celdas
Edición
Confidencialidad
F21
No.,"Time","TCP Delta","Source","Destination","Protocol","Info","Host","Comment"
1,"0.000000","0.000000000","24.6.173.220","74.125.224.84","HTTP","GET /sbd?q=peter+lik+for+sale&um=1&hl=en&client=firefox-a&sa=N&rls=org.mo
5,"0.062672","0.000003000","74.125.224.84","24.6.173.220","HTTP","HTTP/1.1 200 OK (text/javascript)","","In this response, the server sends numero
7,"0.475050","0.000000000","24.6.173.220","74.125.224.84","HTTP","GET /imgres?imgurl=http://www.artbrokerage.com/artthumb/likp_35911_2/850
12,"0.043454","0.000014000","74.125.224.84","24.6.173.220","HTTP","HTTP/1.1 200 OK (text/html)","","We get the expanded image through Google -
14,"0.024838","0.000000000","24.6.173.220","77.93.251.49","TCP","50316 > 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1","","We cl
15,"0.002104","0.000000000","24.6.173.220","66.11.147.48","TCP","50317 > 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1","","Here
18,"0.103595","0.000565000","24.6.173.220","66.11.147.48","HTTP","GET /artthumb/likp_35911_2/850x600/Peter_Lik_Beyond_Paradise.jpg HTTP/1.1 "
21,"0.086025","0.000709000","24.6.173.220","77.93.251.49","HTTP","GET /stat/gthyu/index.php?p=peter-lik-inner-peace-for-sale HTTP/1.1 ","www.u
23,"0.161477","0.146588000","66.11.147.48","24.6.173.220","TCP","80 > 50317 [ACK] Seq=1 Ack=1046 Win=7936 Len=1460 [TCP segment of a reassemb
67,"0.580651","0.547913000","77.93.251.49","24.6.173.220","HTTP","HTTP/1.1 302 Found ","","Here's the redirection to the malicious site. See the Loc
68,"0.002170","0.000000000","24.6.173.220","95.169.190.217","TCP","50319 > 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1","","We
75,"0.382179","0.002074000","95.169.190.217","24.6.173.220","HTTP","HTTP/1.1 302 Found ","","Our malicious host is redirecting us to run a CGI script
79,"0.003645","0.000000000","24.6.173.220","95.169.190.217","TCP","50320 > 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1","","An
84,"0.196512","0.000015000","24.6.173.220","95.169.190.217","HTTP","GET /in.cgi?8&seoref=http%3A%2F%2Fwww.google.com%2Fimgres%3Fimgurl
87,"0.210788","0.011399000","95.169.190.217","24.6.173.220","HTTP","HTTP/1.1 200 OK (text/html)","","They're dropping a cookie on our drive and g
96,"0.244080","0.002946000","24.6.173.220","78.41.203.19","TCP","50321 > 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0","","Well that didn't go so well fo
104,"0.181295","0.001678000","24.6.173.220","78.41.203.19","TCP","50324 > 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0","","And another termination tri
117,"0.283123","0.001682000","24.6.173.220","78.41.203.19","TCP","50326 > 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0","","Yes, Symantec is screaming
159,"12.732243","15.712621000","24.6.173.220","74.125.224.84","HTTP","GET /gen_204?atyp=i&ct=backbutton&cad=&ei=ejsdTsWPN4OmsQOfo9W6D
suspicous101
Listo
100 %