



“Secretaría De La Educación Superior”  
“Instituto Tecnológico de Cancún”

## **Ingeniería en Sistemas Computacionales**

**Materia:** Fundamentos de Telecomunicaciones

**Tema:** Laboratorio N#41 Wireshark

**Alumno:** Vargas Rodríguez Javier Jesús

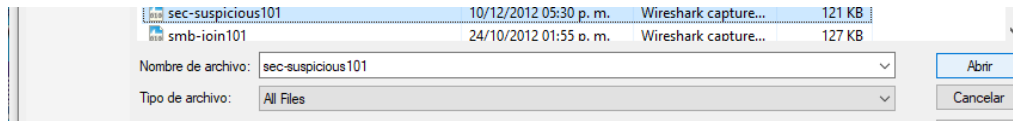
**Maestro:** Ismael Jiménez Sánchez

***Fecha De Entrega: 6/Diciembre/2020***

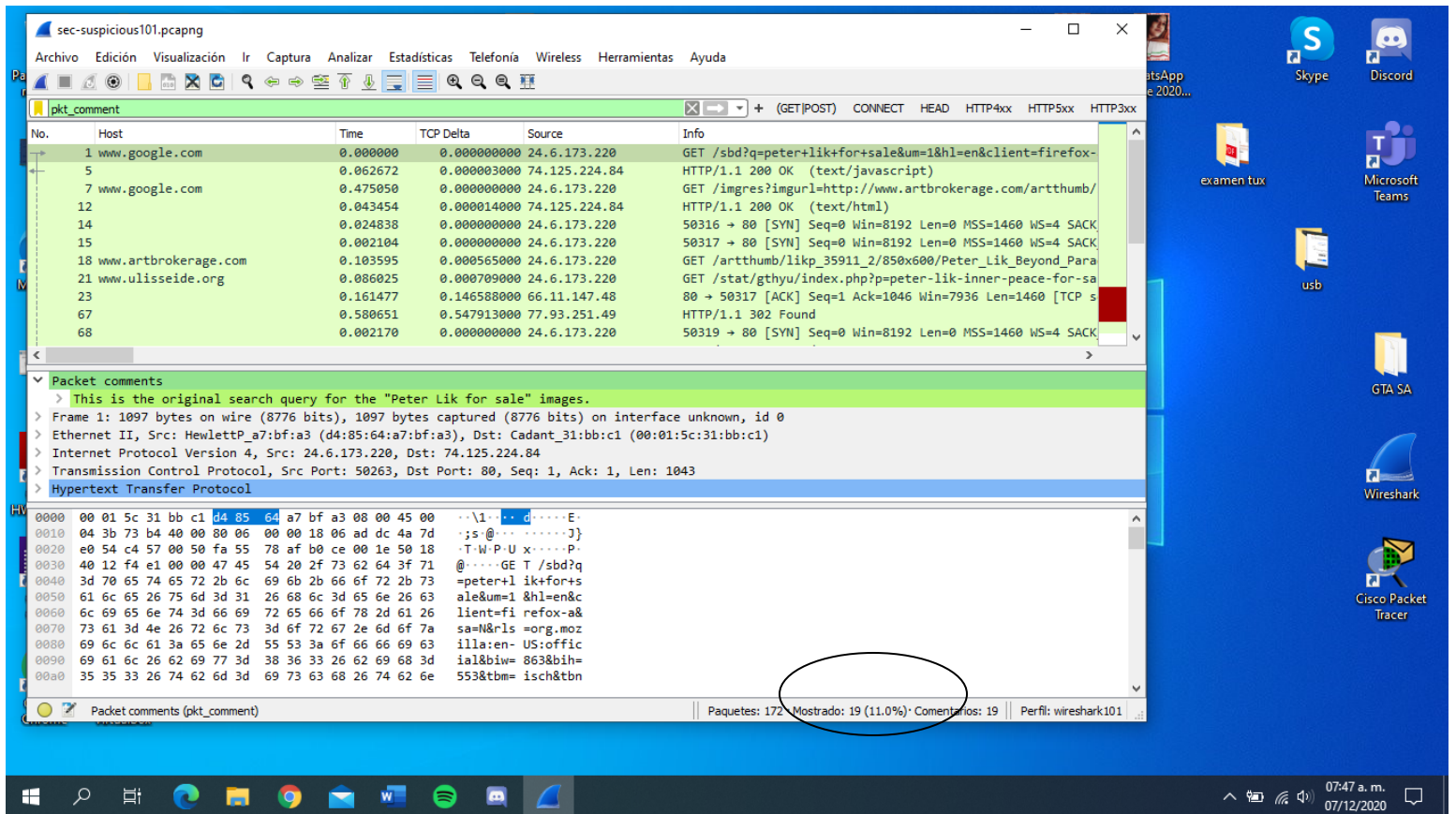
Horario: 5:00 pm – 6:00 pm

## Laboratio N#41 – Exportar comentarios de paquetes redireccionamiento malintencionado.

### Paso 1 – Abrimos sec-suspicious101.pcapng



Paso 2 – En el frame 1 hacemos clic derecho en la línea de comentarios del paquete en el área Detalles del paquete y seleccionamos aplicar como filtro | Seleccionado. Solo 19 paquetes deben de coincidir con ese filtro.



The screenshot shows the Wireshark interface with the file 'sec-suspicious101.pcapng' open. The packet list pane shows 172 packets, and the packet details pane shows the packet comments for the selected packet. The packet comments are filtered to show only 19 packets. The packet details show the packet comments for the selected packet.

No.	Host	Time	TCP Delta	Source	Info
1	www.google.com	0.000000	0.000000000	24.6.173.220	GET /sbd?q=peter+lik+for+sale&um=1&hl=en&client=firefox-
5		0.062672	0.000003000	74.125.224.84	HTTP/1.1 200 OK (text/javascript)
7	www.google.com	0.475050	0.000000000	24.6.173.220	GET /imgres?imgurl=http://www.artbrokerage.com/artthumb/
12		0.043454	0.000014000	74.125.224.84	HTTP/1.1 200 OK (text/html)
14		0.024838	0.000000000	24.6.173.220	50316 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK
15		0.002104	0.000000000	24.6.173.220	50317 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK
18	www.artbrokerage.com	0.103595	0.000565000	24.6.173.220	GET /artthumb/likp_35911_2/850x600/Peter_Lik_Beyond_Para
21	www.ulisseide.org	0.086025	0.000709000	24.6.173.220	GET /stat/gthyu/index.php?p=peter-lik-inner-peace-for-sa
23		0.161477	0.146588000	66.11.147.48	80 → 50317 [ACK] Seq=1 Ack=1046 Win=7936 Len=1460 [TCP s
67		0.580651	0.547913000	77.93.251.49	HTTP/1.1 302 Found
68		0.002170	0.000000000	24.6.173.220	50319 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK

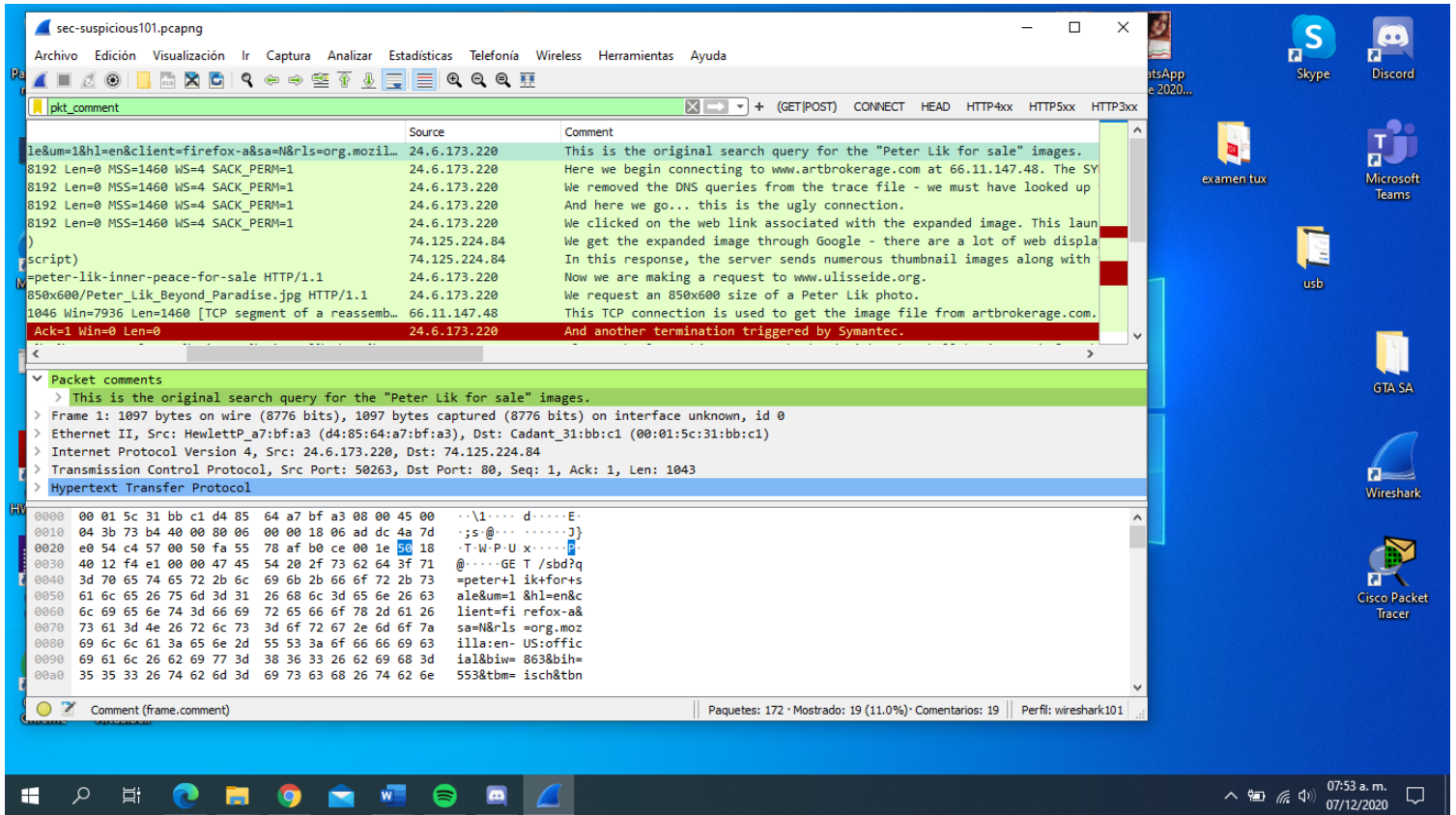
Packet comments

- > This is the original search query for the "Peter Lik for sale" images.
- > Frame 1: 1097 bytes on wire (8776 bits), 1097 bytes captured (8776 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: 74.125.224.84
- > Transmission Control Protocol, Src Port: 50263, Dst Port: 80, Seq: 1, Ack: 1, Len: 1043
- > Hypertext Transfer Protocol

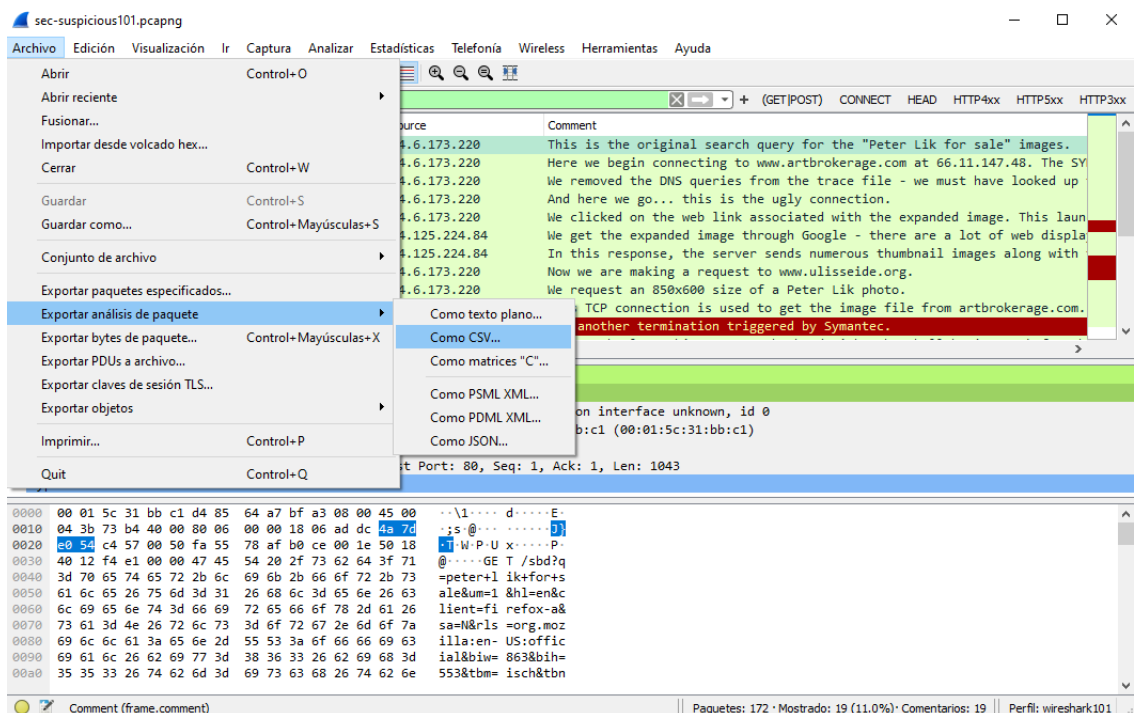
Packet comments (pkt\_comment)

Paquetes: 172 Mostrado: 19 (11.0%) Comentarios: 19 Perfil: wireshark101

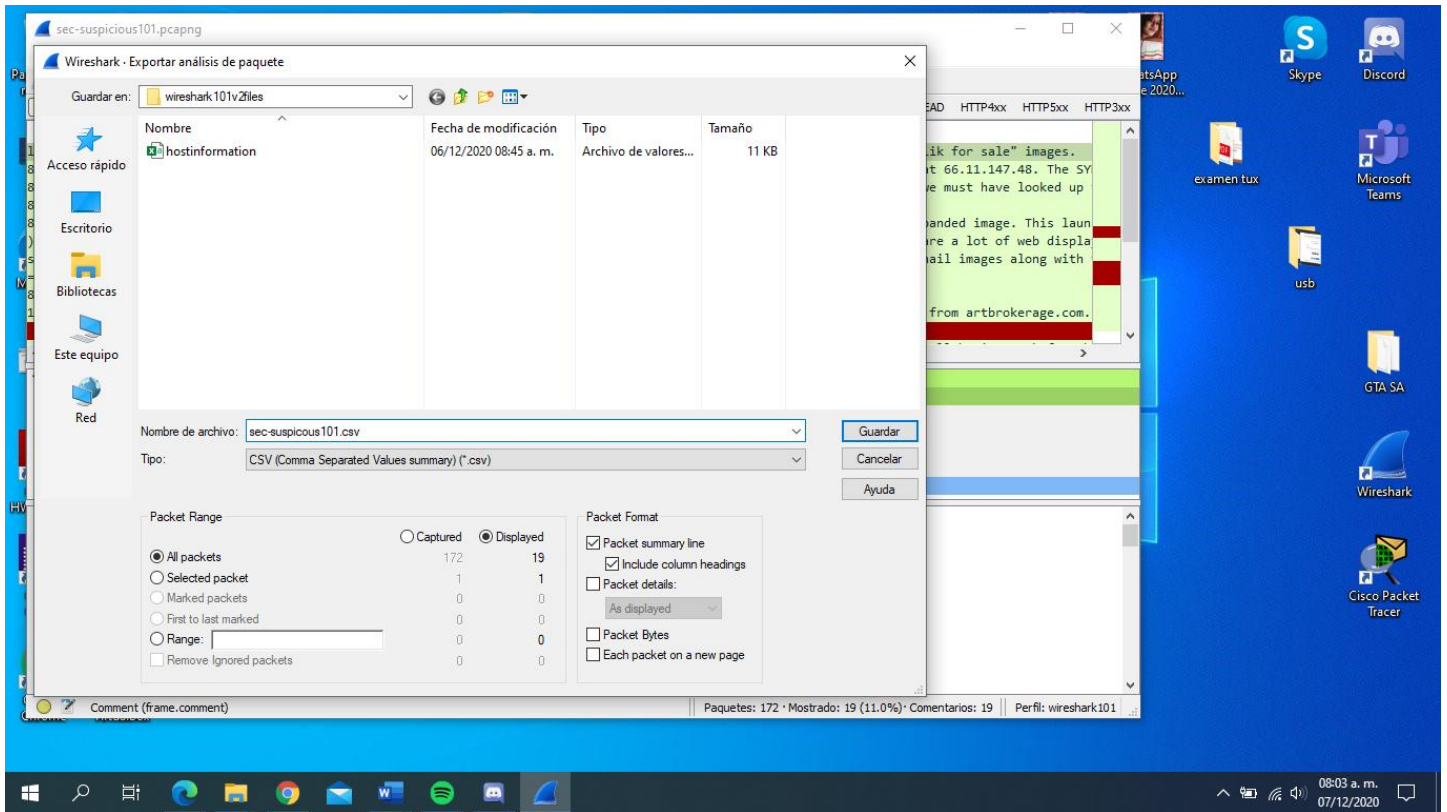
Paso 3 – Ahora expandimos la sección de comentarios de paquetes del Frame 1. Haga clic derecho en el comentario que dice “Este es el original” ... y lo seleccionamos aplicar como columna.



Paso 4 – Seleccione Archivo | Direcciones de paquetes expuestas | Como CSV.



Paso 5 – Navegamos hasta el directorio donde deseemos guardar el archivo de texto y le asignamos un nombre sec-suspicious101.csv.



Paso 6 – Abrimos nuestro archivo csv en una hoja de cálculo para revisar la información exportada.

sec-suspicious101 - Excel

JAVIER JESUS VARGAS RODRIGUEZ

ArchivosInicioInsertarDisposición de páginaFórmulasDatosRevisarVistaAyuda¿Qué desea hacer?

Portapapeles

Calibri11A<sup>+</sup>

General

Formato condicionalDar formato como tablaEstilos de celda

InsertarEliminarFormatoCeldas

Ordenar y filtrarEdición

Confidencialidad

Fuente

Alineación

Número

POSIBLE PÉRDIDA DE DATOS

Algunas características del libro se pueden perder si lo guarda como CSV (delimitado por comas). Para conservar estas características, guárdelo como archivo de Excel.

No mostrar de nuevoGuardar como...

A1

No.

A	B	C	D	E	F	G	H	
No.	Host	Info	Source	Comment	Destination	Protocol	Protocols in frame	
1	www.google.com	GET /sbd?q=peter+lik+for+sale&um=1&hl=en&client=firefox-a&	24.6.173.220	This is the original search query for the "Peter Lik for s	74.125.224.8	HTTP	eth:ethertype:ip:	
2	5	HTTP/1.1 200 OK (text/javascript)	74.125.224.8	In this response, the server sends numerous thumbna	24.6.173.220	HTTP	eth:ethertype:ip:	
3	7	www.google.com	GET /imgres?imgurl=http://www.artbrokerage.com/artthumb/li	24.6.173.220	Now we clicked on the image load the expanded thun	74.125.224.8	HTTP	eth:ethertype:ip:
4	12	HTTP/1.1 200 OK (text/html)	74.125.224.8	We get the expanded image through Google - there ar	24.6.173.220	HTTP	eth:ethertype:ip:	
5	14	50316 > 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_	24.6.173.220	We clicked on the web link associated with the expan	77.93.251.49	TCP	eth:ethertype:ip:	
6	15	50317 > 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_	24.6.173.220	Here we begin connecting to www.artbrokerage.com	66.11.147.48	TCP	eth:ethertype:ip:	
7	18	www.artbrokerage.com	GET /artthumb/likp_35911_2/850x600/Peter_Lik_Beyond_Paradi	24.6.173.220	We request an 850x600 size of a Peter Lik photo.	66.11.147.48	HTTP	eth:ethertype:ip:
8	21	www.ulisseide.org	GET /stat/gthyu/index.php?p=peter-lik-inner-peace-for-sale HT	24.6.173.220	Now we are making a request to www.ulisseide.org.	77.93.251.49	HTTP	eth:ethertype:ip:
9	23	80 > 50317 [ACK] Seq=1 Ack=1046 Win=7936 Len=1460 [TCP segm	66.11.147.48	This TCP connection is used to get the image file from	24.6.173.220	TCP	eth:ethertype:ip:	
10	67	HTTP/1.1 302 Found	77.93.251.49	Here's the redirection to the malicious site. See the Lc	24.6.173.220	HTTP	eth:ethertype:ip:	
11	68	50319 > 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_	24.6.173.220	We removed the DNS queries from the trace file - we	95.169.190.2	TCP	eth:ethertype:ip:	
12	75	HTTP/1.1 302 Found	95.169.190.2	Our malicious host is redirecting us to run a CGI script	24.6.173.220	HTTP	eth:ethertype:ip:	
13	79	50320 > 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_	24.6.173.220	And here we go... this is the ugly connection.	95.169.190.2	TCP	eth:ethertype:ip:	
14	84	3xsd5p828s.cz.cc	GET /in.cgi?8&seoref=http%3A%2Fwww.google.com%2Fimg	24.6.173.220	Please oh please hit us over the head with a baseball	195.169.190.2	HTTP	eth:ethertype:ip:
15	87	HTTP/1.1 200 OK (text/html)	95.169.190.2	They're dropping a cookie on our drive and giving us a	24.6.173.220	HTTP	eth:ethertype:ip:	
16	96	50321 > 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	24.6.173.220	Well that didn't go so well for them... our Symantec sc	78.41.203.19	TCP	eth:ethertype:ip:	
17	104	50324 > 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	24.6.173.220	And another termination triggered by Symantec.	78.41.203.19	TCP	eth:ethertype:ip:	
18	117	50326 > 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	24.6.173.220	Yes, Symantec is screaming with messages on our syst	78.41.203.19	TCP	eth:ethertype:ip:	
19	159	www.google.com	GET /gen_204?atyp=i&ct=backbutton&cad=&ei=jsdTsWPN4Om	24.6.173.220	We're just returning to Google after a little sidetrack t	74.125.224.8	HTTP	eth:ethertype:ip:
20								
21								

sec-suspicious101

100%

08:05 a.m.

07/12/2020