



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

## **Ingeniería en Sistemas Computacionales**

**Materia:** Fundamentos de Telecomunicaciones

**Tema:** Laboratorio N#40 Wireshark

**Alumno:** Vargas Rodríguez Javier Jesús

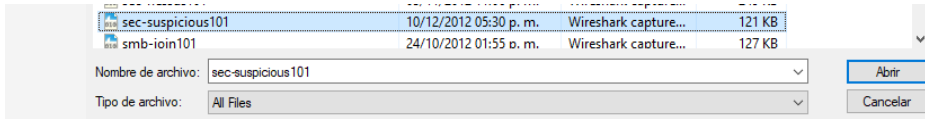
**Maestro:** Ismael Jiménez Sánchez

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

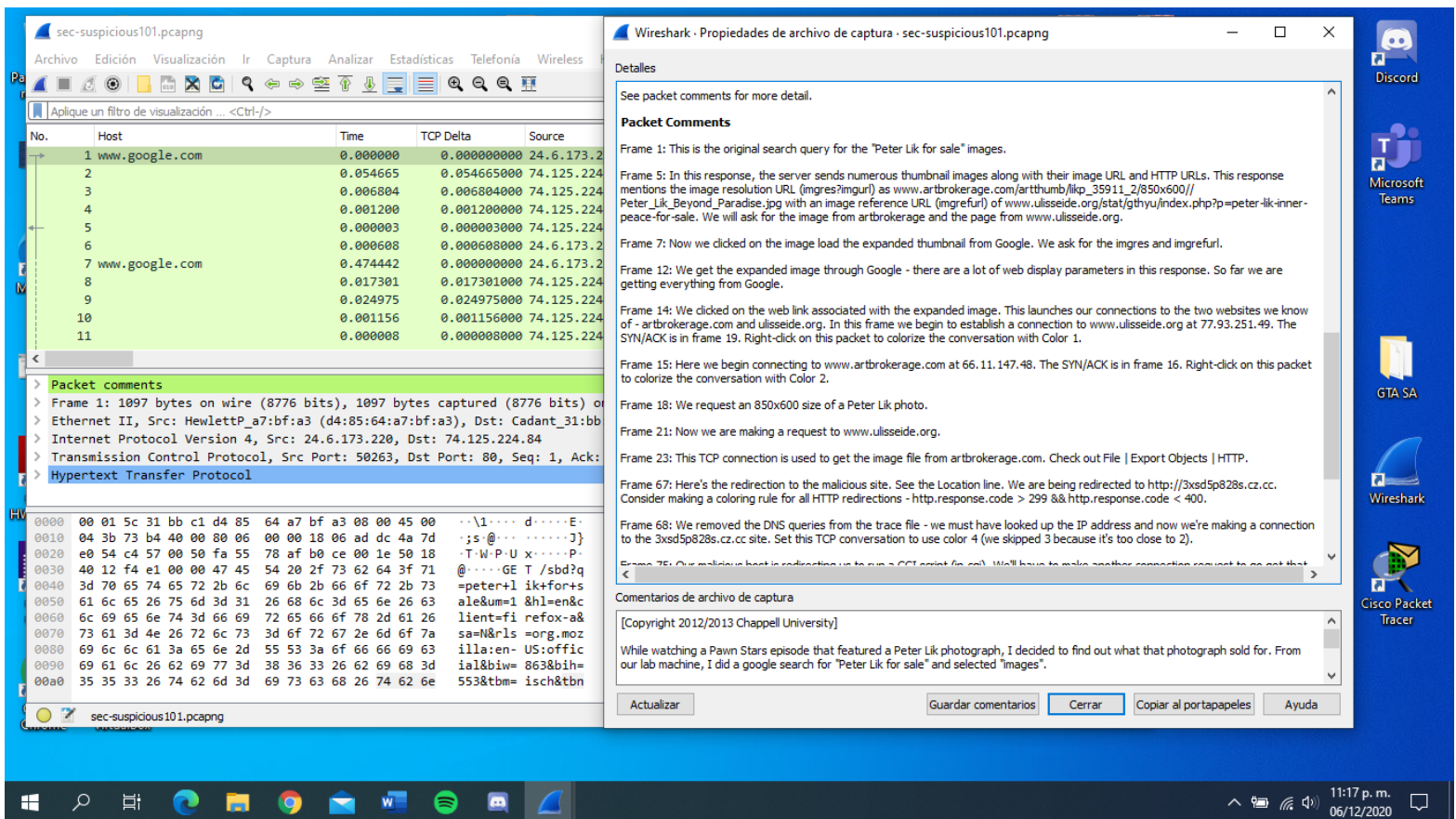
Horario: 5:00 pm – 6:00 pm

## Laboratio N#40 – Leer notas de analisis en un archivo de seguimiento de redireccionamiento malicioso.

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



### Paso 2 – Hacer clic en el botón Anotación en la barra de estado para abrir la ventana Propiedades del archivo de captura. Lea la sección de comentarios de archivos de captura.



Wireshark · Propiedades de archivo de captura · sec-suspicious101.pcapng

Detalles

See packet comments for more detail.

**Packet Comments**

Frame 1: This is the original search query for the "Peter Lik for sale" images.

Frame 5: In this response, the server sends numerous thumbnail images along with their image URL and HTTP URLs. This response mentions the image resolution URL (imgres?imgurl) as [www.artbrokerage.com/artthumb/ikp\\_35911\\_2/850x600//Peter\\_Lik\\_Beyond\\_Paradise.jpg](http://www.artbrokerage.com/artthumb/ikp_35911_2/850x600//Peter_Lik_Beyond_Paradise.jpg) with an image reference URL (imgrefurl) of [www.ulisseide.org/stat/gthyu/index.php?p=peter-lik-inner-peace-for-sale](http://www.ulisseide.org/stat/gthyu/index.php?p=peter-lik-inner-peace-for-sale). We will ask for the image from artbrokerage and the page from www.ulisseide.org.

Frame 7: Now we clicked on the image load the expanded thumbnail from Google. We ask for the imgres and imgrefurl.

Frame 12: We get the expanded image through Google - there are a lot of web display parameters in this response. So far we are getting everything from Google.

Frame 14: We clicked on the web link associated with the expanded image. This launches our connections to the two websites we know of - artbrokerage.com and ulisseide.org. In this frame we begin to establish a connection to [www.ulisseide.org](http://www.ulisseide.org) at 77.93.251.49. The SYN/ACK is in frame 19. Right-click on this packet to colorize the conversation with Color 1.

Frame 15: Here we begin connecting to [www.artbrokerage.com](http://www.artbrokerage.com) at 66.11.147.48. The SYN/ACK is in frame 16. Right-click on this packet to colorize the conversation with Color 2.

Frame 18: We request an 850x600 size of a Peter Lik photo.

Frame 21: Now we are making a request to [www.ulisseide.org](http://www.ulisseide.org).

Frame 23: This TCP connection is used to get the image file from artbrokerage.com. Check out File | Export Objects | HTTP.

Frame 67: Here's the redirection to the malicious site. See the Location line. We are being redirected to <http://3xsd5p828s.cz.cc>. Consider making a coloring rule for all HTTP redirections - `http.response.code > 299 && http.response.code < 400`.

Frame 68: We removed the DNS queries from the trace file - we must have looked up the IP address and now we're making a connection to the [3xsd5p828s.cz.cc](http://3xsd5p828s.cz.cc) site. Set this TCP conversation to use color 4 (we skipped 3 because it's too close to 2).

Frame 75: Our malicious host is redirecting us to run a CGI script (in .cc). We'll have to make another connection request to go get that.

**Comentarios de archivo de captura**

[Copyright 2012/2013 Chappell University]

While watching a Pawn Stars episode that featured a Peter Lik photograph, I decided to find out what that photograph sold for. From our lab machine, I did a google search for "Peter Lik for sale" and selected "images".

Actualizar Guardar comentarios Cerrar Copiar al portapapeles Ayuda

Paso 3 – Hacemos clic en el botón de información de experto y expandimos la sección de comentarios para leerlos.

The screenshot shows the Wireshark interface with a packet capture of 'sec-suspicious101.pcapng'. The main pane displays a list of packets, with packet 1 selected. The 'Information specialized' window is open, showing a list of packet comments. The comments are as follows:

Gravedad	Resumen	Grupo	Protocolo
Warning	Connection reset (RST)	Sequence	TCP
Note	This frame is a (suspected) retransmission	Sequence	TCP
Chat	Connection finish (FIN)	Sequence	TCP
Chat	Connection establish acknowledge (SYN+ACK): server por...	Sequence	TCP
Chat	Connection establish request (SYN): server port 80	Sequence	TCP
Chat	GET /sbd?q=peter+lik+for+sale&um=1&hl=en&client=fir...	Sequence	HTTP
Comment	Packet comments listed below.	Comment	Frame
	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

Paso 4 – Haga clic en cualquiera de los comentarios para saltar a ese paquete del archivo en seguimiento.

The screenshot shows the Wireshark interface with a packet capture of 'sec-suspicious101.pcapng'. The main pane displays a list of packets, with packet 79 selected. The 'Information specialized' window is open, showing a list of packet comments. The comments are as follows:

Paquete	Resumen	Grupo	Protocolo
Warning	Connection reset (RST)	Sequence	TCP
Note	This frame is a (suspected) retransmission	Sequence	TCP
Chat	Connection finish (FIN)	Sequence	TCP
Chat	Connection establish acknowledge (SYN+ACK): server por...	Sequence	TCP
Chat	Connection establish request (SYN): server port 80	Sequence	TCP
Chat	GET /sbd?q=peter+lik+for+sale&um=1&hl=en&client=fir...	Sequence	HTTP
Comment	Packet comments listed below.	Comment	Frame
	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