

**Instituto Tecnológico de Cancún**

**Ingeniería en Sistemas Computacionales**

**Fundamentos de Telecomunicaciones**

**Lab40 - Read Analysis Notes in a  
Malicious Redirection Trace File**

**Docente: Ing. Ismael Jiménez Sánchez**

**Alumno: Uc Uc César Enrique**

## Lab40 - Read Analysis Notes in a Malicious Redirection Trace File

### 1 Abrir el documento sec.suspicious101.pcapng

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

The image shows the Wireshark interface with the 'Propiedades de archivo de captura' (Capture File Properties) window open. The 'Detalles' (Details) pane shows the following statistics:

Medida	Capturado	Mostrado	Marcado
Paquetes	172	172 (100.0%)	—
Espacio de tiempo, s	17.217	17.217	—
Promedio pps	10.0	10.0	—
Promedio de tamaño de paquete, B	458	458	—
Bytes	78846	78846 (100.0%)	0
Promedio de bytes/s	4579	4579	—
Promedio de bits/s	36k	36k	—

The 'Section Comment' pane contains the following text:

[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".

This trace includes the Google query for the images (frame 1), and the responses in a compressed list (frames 2-6) filled with images and the image links.

I clicked on one image which was linked to artbrokerage.com and ulisseide.org (frame 7).

See packet comments for more detail.

The 'Packet Comments' pane shows the following 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/likp\_35911\_2/850x600/Peter\_Lik\_Beyond\_Paradise.jpg with an image reference URL (imgrefurl) of www.ulisseide.org/stat/ghyui/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 the frame we begin to establish a connection to www.ulisseide.org at 77.93.251.49. The SYN/ACK is in frame 15. Right-click on this packet to colorize the conversation with Color 1.

Frame 15: 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 to colorize the conversation with Color 2.

The 'Comentarios de archivo de captura' (Capture File Comments) pane shows the following comment:

[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".

### 3 Le damos click en el botón de Expert Information y expandimos Comments y podemos observar los diferentes comentarios que contiene los paquetes en el archivo.

The image shows the Wireshark interface with the 'Información especializada' (Expert Information) window open. The 'Comentarios' (Comments) pane shows the following comments:

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

5 In this response, the server sends numerous thumbnail images...

7 Now we clicked on the image load the expanded thumbnail...

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.

14 We clicked on the web link associated with the expanded image...

15 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 to colorize the conversation with Color 2.

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

21 Now we are making a request to www.ulisseide.org.

23 This TCP connection is used to get the image file from artb...

67 Here's the redirection to the malicious site. See the Location...

68 We removed the DNS queries from the trace file - we must...

75 Our malicious host is redirecting us to run a CGI script (in...

79 And here we go... this is the ugly connection.

84 Please oh please hit us over the head with a baseball bat! ...

87 They're dropping a cookie on our drive and giving us a link...

96 Well that didn't go so well for them... our Symantec softwa...

104 And another termination triggered by Symantec.

117 Yes, Symantec is screaming with messages on our system...

159 We're just returning to Google after a little sidetrack to the ...

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

The screenshot displays the Wireshark interface with two main windows. The left window, titled 'sec-suspicious101.pcapng', shows a list of network packets. The right window, titled 'Wireshark - Información especializada - sec-suspicious101.pcapng', provides a detailed view of the selected packet (Frame 23).

**Packet List (Left Window):**

No.	Time	Source	Destination
11	0.000008	74.125.224.84	24.6.173.220
12	0.000014	74.125.224.84	24.6.173.220
13	0.000647	24.6.173.220	74.125.224.84
14	0.002191	24.6.173.220	77.93.251.49
15	0.002104	24.6.173.220	66.11.147.48
16	0.102909	66.11.147.48	24.6.173.220
17	0.000121	24.6.173.220	66.11.147.48
18	0.000565	24.6.173.220	66.11.147.48
19	0.005108	77.93.251.49	24.6.173.220
20	0.000128	24.6.173.220	77.93.251.49
21	0.000709	24.6.173.220	77.93.251.49
22	0.014889	66.11.147.48	24.6.173.220
23	0.146588	66.11.147.48	24.6.173.220
24	0.000001	66.11.147.48	24.6.173.220

**Packet Details (Right Window):**

The right window shows the details of Frame 23, which is a TCP connection. The 'Packet comments' section is expanded, showing a comment that reads: 'This TCP connection is used to get the image file from a...'. The comment is highlighted in blue, and a blue arrow points from it to the packet list, indicating that clicking on the comment will navigate to the corresponding packet.

**Packet Comments (Right Window):**

Comentario	Paquete
This is the original search query for the "Peter Lik for sale" l...	1
In this response, the server sends numerous thumbnail im...	5
Now we clicked on the image load the expanded thumbna...	7
We get the expanded image through Google - there are a l...	12
We clicked on the web link associated with the expanded l...	14
Here we begin connecting to www.artbrokerage.com at 66...	15
We request an 850x600 size of a Peter Lik photo.	18
Now we are making a request to www.ulisseide.org.	21
This TCP connection is used to get the image file from artb...	23
Here's the redirection to the malicious site. See the Locatio...	67
We removed the DNS queries from the trace file - we must...	68
Our malicious host is redirecting us to run a CGI script (in...	75
And here we go... this is the ugly connection.	79
Please oh please hit us over the head with a baseball bat! ...	84
They're dropping a cookie on our drive and giving us a link...	87
Well that didn't go so well for them... our Symantec softwa...	96
And another termination triggered by Symantec.	104
Yes, Symantec is screaming with messages on our system...	117
We're just returning to Google after a little sidetrack to the...	159