

## 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.

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

Detalles

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	—

**Section 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".

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.

**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/likp\_35911\_2/850x600/Peter\_Lik\_Beyond\_Paradise.jpg with an image reference URL (imgrefurl) of www.ulisseide.org/stat/gthyu/index.php?ip=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 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 at 65.11.147.48. The SYN/ACK is in frame 16. Right-click on this packet to colorize the conversation with Color 2.

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".

## 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.

Wireshark - Información especializada - sec-suspicious101.pcapng

Gravedad	Resumen	Grupo	Protocolo	Recuento
Warning	Connection reset (RST)	Sequence	TCP	12
Note	This frame is a (suspected) retransmission	Sequence	TCP	1
Chat	Connection finish (FIN)	Sequence	TCP	9
Chat	Connection establish acknowledgement (SYN+ACK): server port...	Sequence	TCP	20
Chat	Connection establish request (SYN): server port 80	Sequence	TCP	19
Chat	GET /sbd?ip=peter+lik+for+sale&um=1&hl=en&client=fin...	Sequence	HTTP	22
Comment	Packet comments listed below.	Comment	Frame	19

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

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

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

12 We get the expanded image through Google - there are a l...

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

15 Here we begin connecting to www.artbrokerage.com at 66...

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 Locatio...

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 ...

No hay conjunto de filtro de visualización.

☐ Limitar filtro de visualización ☒ Agrupar por resumen Buscar:

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

The screenshot shows the Wireshark interface with the following components:

- Packet List Pane:** Displays a list of captured packets. Packet 23 is highlighted in blue, indicating it is selected. The packet is a TCP connection reset (RST) from 74.125.224.84 to 24.6.173.220.
- Packet Details Pane:** Shows the details of the selected packet (Frame 23). It includes a comment that reads: "This TCP connection is used to get the image file from artb...". A blue arrow points from this comment to packet 23 in the packet list pane.
- Packet Bytes Pane:** Displays the raw bytes of the selected packet in hexadecimal and ASCII format.
- Packet Comments Pane:** A pane on the right side of the interface that lists all comments for the selected packet. It shows a list of comments, including the one selected in the packet details pane.

The interface also includes a menu bar (Archivo, Edición, Visualización, Ir, Captura, Analizar, Estadísticas, Tele) and a toolbar with various icons for file operations, capture, and analysis.