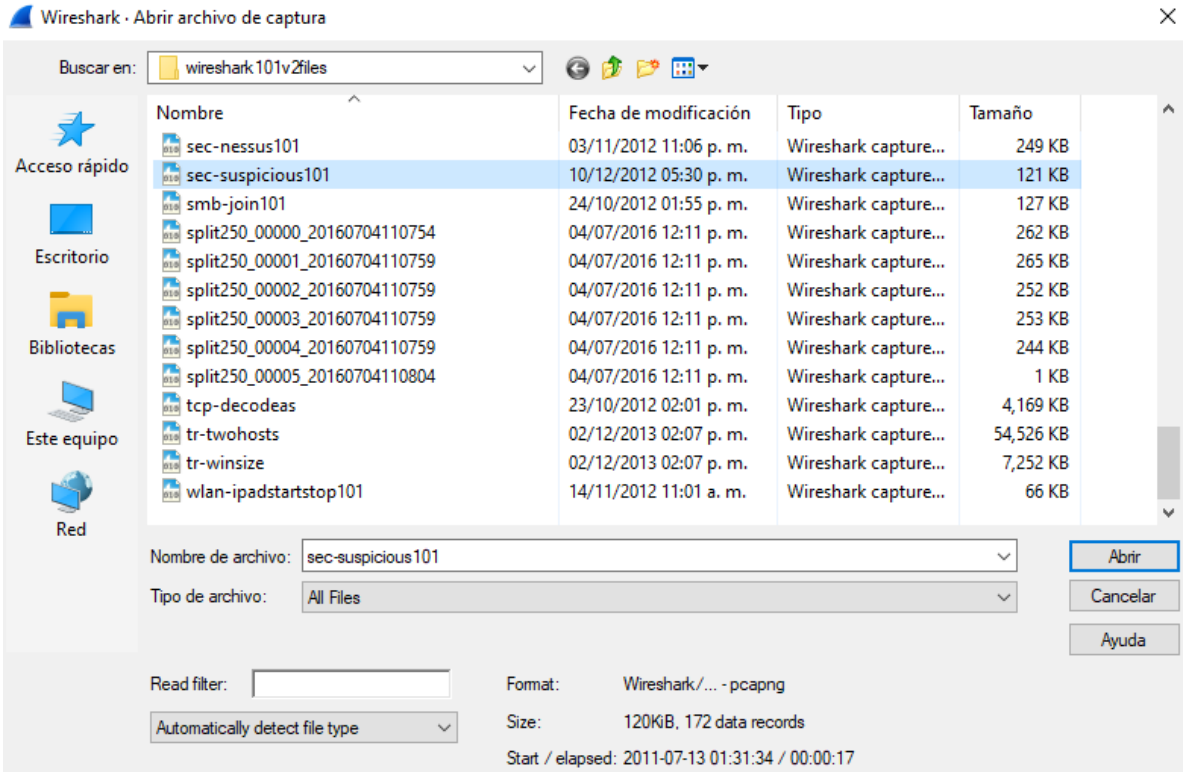
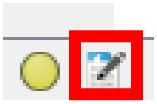
Lab 40

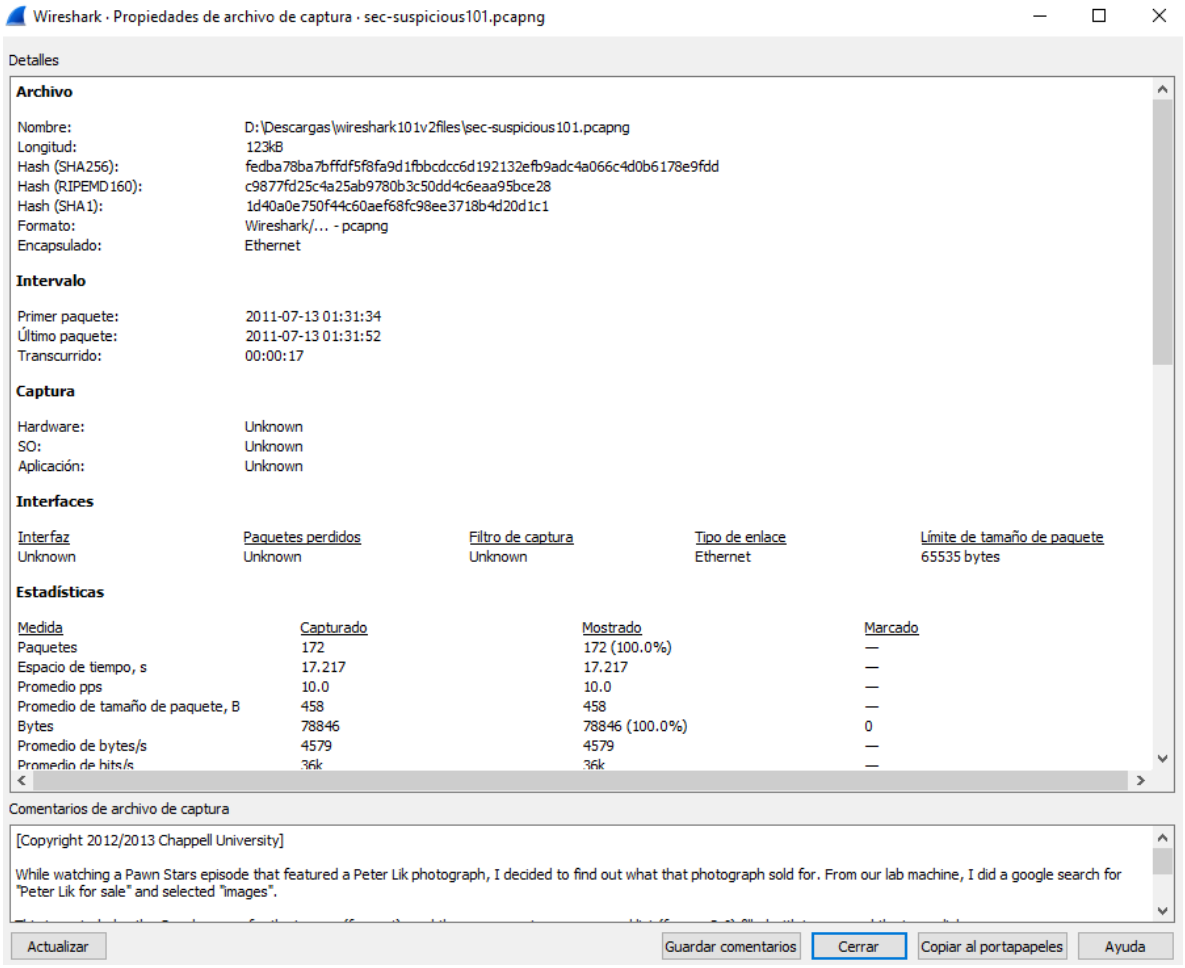
Abriremos el archivo sec-suspicious101.pcapng



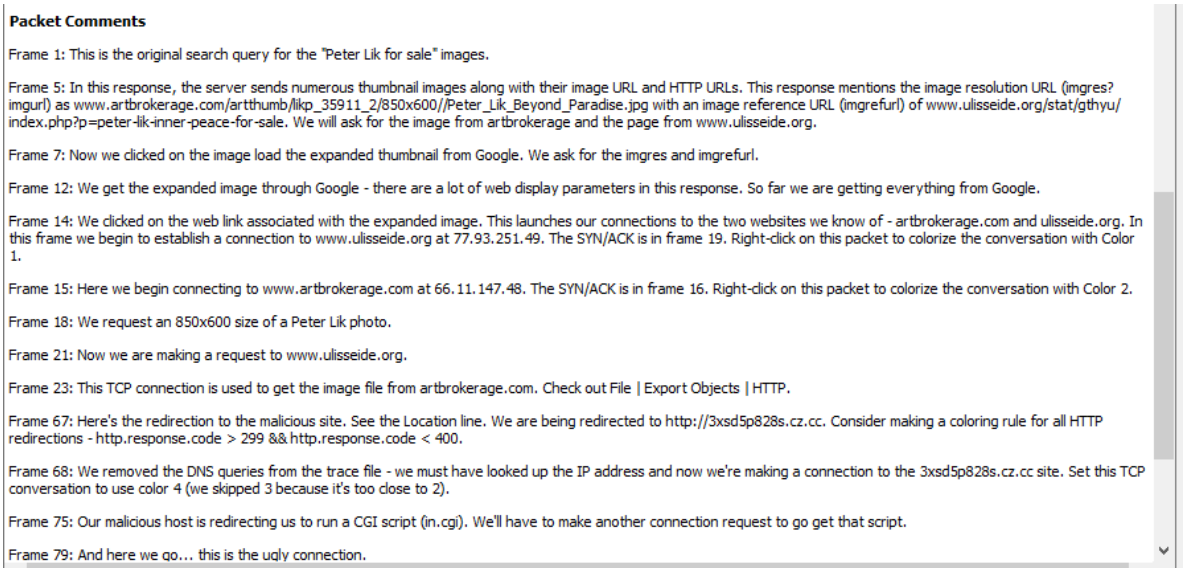
Daremos clic al botón de anotaciones



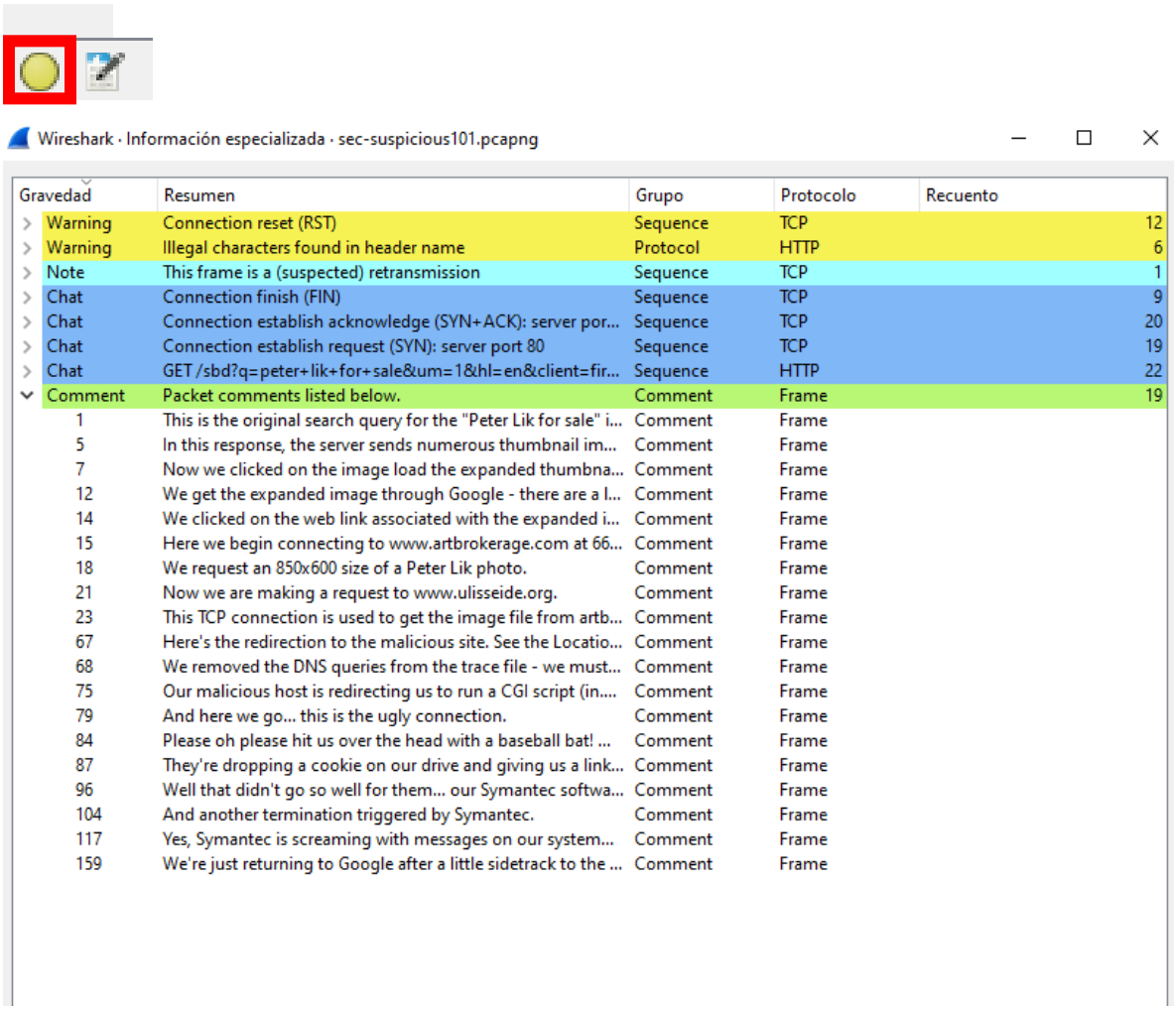
Y nos saldrá una ventana de propiedades del archivo



Navegaremos hasta encontrar la sección de packet comments y cerraremos la ventana



Después le daremos clic al botón de expert information y expandiremos la sección de comment para poder leer los comments individualmente en los paquetes de este archivo de seguimiento



Gravedad	Resumen	Grupo	Protocolo	Recuento
Warning	Connection reset (RST)	Sequence	TCP	12
Warning	Illegal characters found in header name	Protocol	HTTP	6
Note	This frame is a (suspected) retransmission	Sequence	TCP	1
Chat	Connection finish (FIN)	Sequence	TCP	9
Chat	Connection establish acknowledge (SYN+ACK): server por...	Sequence	TCP	20
Chat	Connection establish request (SYN): server port 80	Sequence	TCP	19
Chat	GET /sbd?q=peter+lik+for+sale&um=1&hl=en&client=fir...	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...	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	

Le daremos clic a cualquier comentario para saltar a ese paquete en el archivo de seguimiento. Podremos ver cuando una redirección envía al usuario a un sitio malicioso.