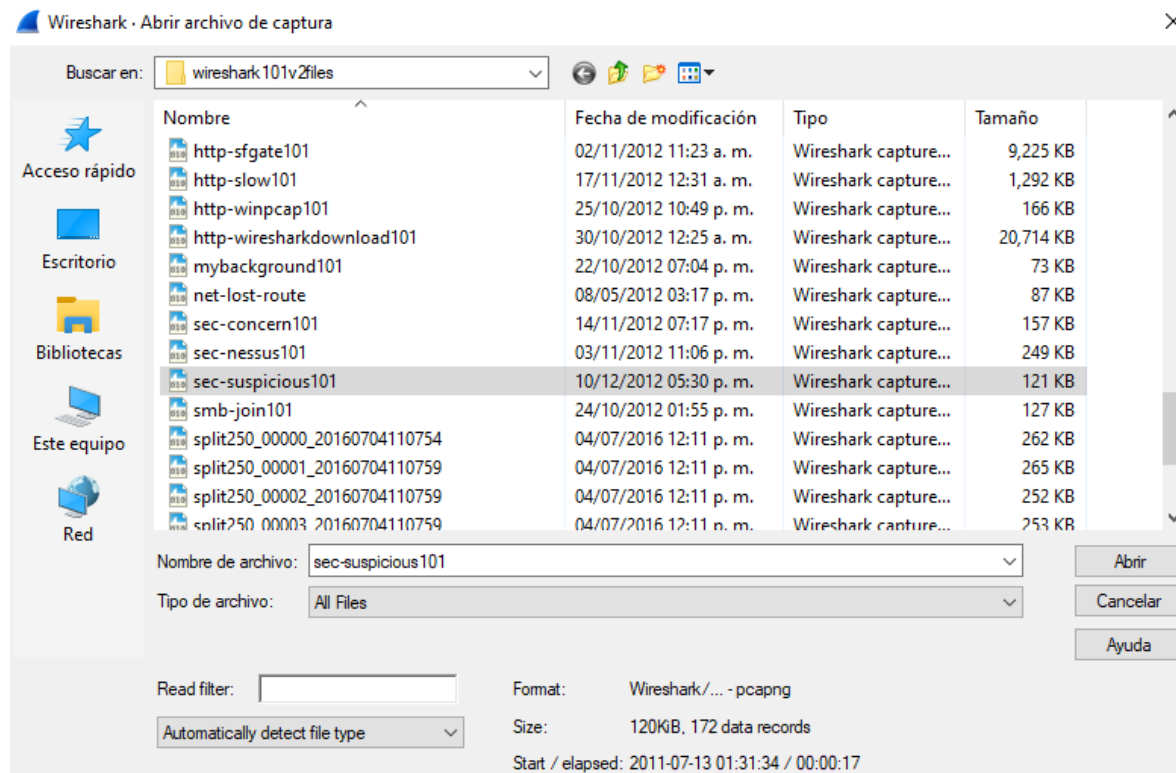
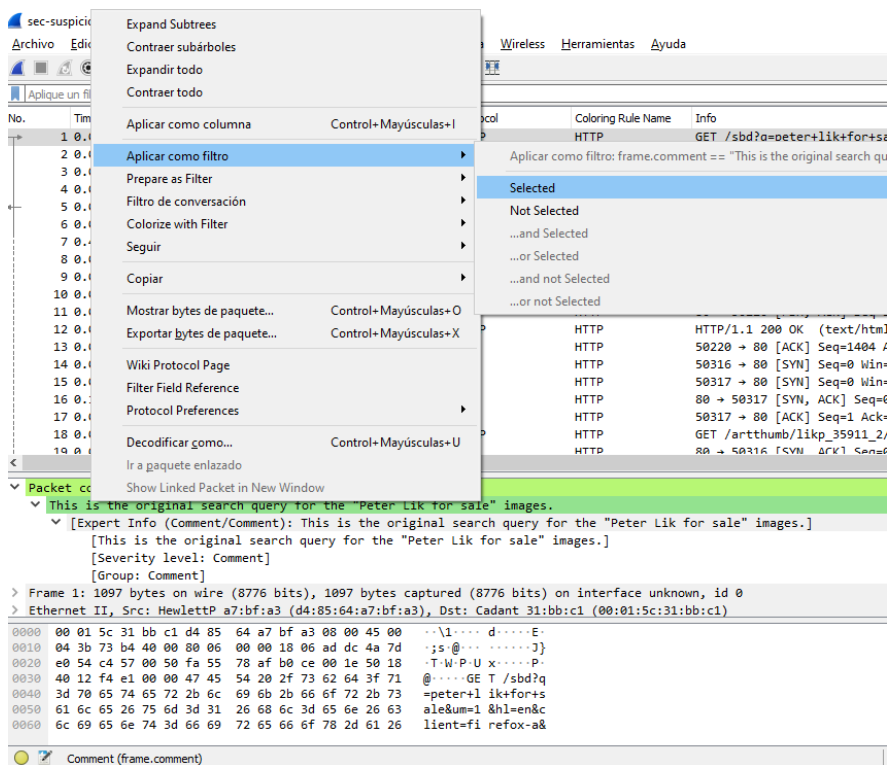


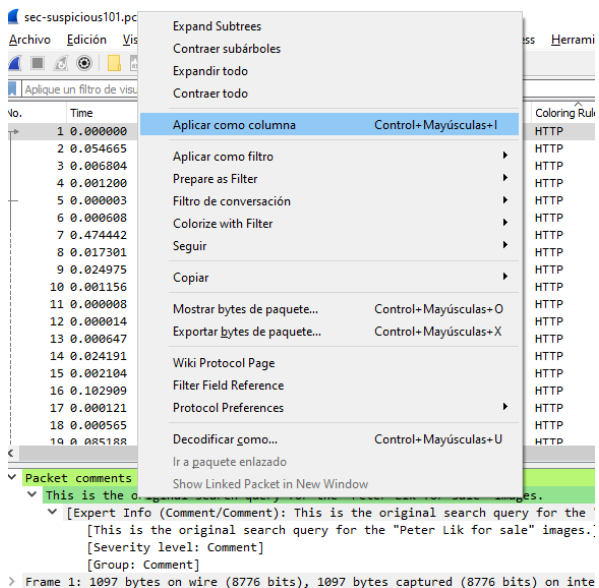
Lab 41

Abriremos el archivo suspicious101.pcapng y en el paquete 1 daremos clic derecho y en comentarios de paquete del menú seleccionar aplicar como filtro y después en selected y nos mostrará 19 paquetes

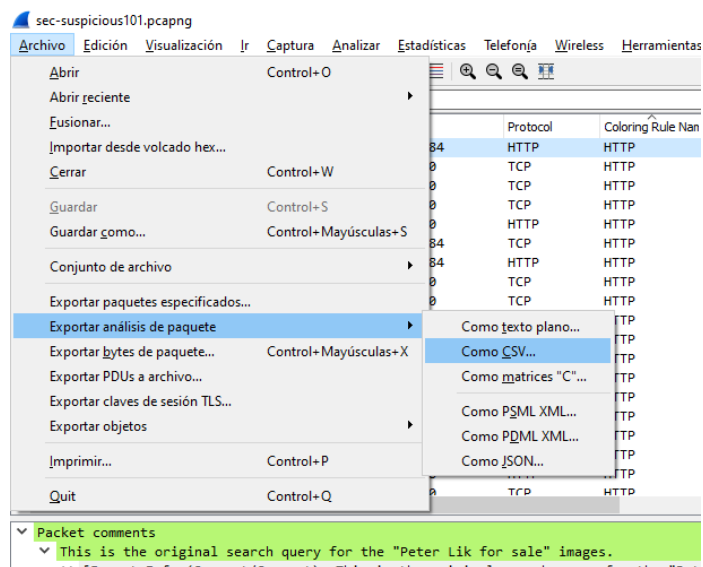




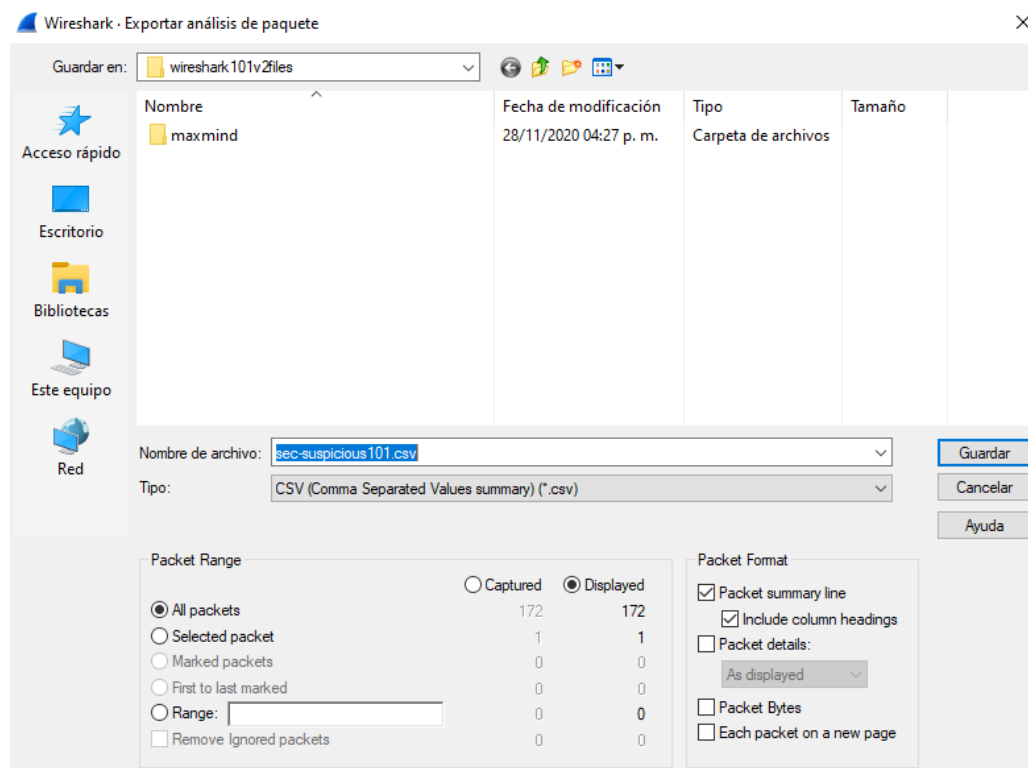
Ahora aplicaremos los comentarios como columnas, dándole clic nuevamente al primer paquete y en el submenú inferior daremos clic derecho y aplicar como columna



Después daremos clic en archivo, exportar análisis de paquete y después en como CSV



Y exportaremos el archivo con el nombre suspicious101.csv y con las siguientes características



Después abriremos el archivo recién creado y en el archivo CSV y podrá visualizar sus paquetes, inclusive con las columnas ocultas

	A	B	C	D	E	F	G	H	I	J
1	No.	Time	Source	Destination	Protocol	Coloring Rule	Packet contents	Comment	Info	
2	1	0	24.6.173.220	74.125.224.8	HTTP	HTTP	à\234\223	This is the original search query for the "Peter Lik for sale" images.	GET /sbd?q=peterHi	
3	5	0.000003	74.125.224.8	24.6.173.220	HTTP	HTTP	à\234\223	In this response, the server sends numerous thumbnail images along with their image URL and HTTP UI	80 > 50263 [ACK] Se	
4	7	0.474442	24.6.173.220	74.125.224.8	HTTP	HTTP	à\234\223	Now we clicked on the image load the expanded thumbnail from Google. We ask for the imgres and in	80 > 50263 [ACK] Se	
5	12	0.000014	74.125.224.8	24.6.173.220	HTTP	HTTP	à\234\223	We get the expanded image through Google - there are a lot of web display parameters in this respons	80 > 50263 [ACK] Se	
6	14	0.024191	24.6.173.220	77.93.251.49	TCP	HTTP	à\234\223	We clicked on the web link associated with the expanded image. This launches our connections to the	HTTP/1.1 200 OK (te	
7	15	0.002104	24.6.173.220	66.11.147.48	TCP	HTTP	à\234\223	Here we begin connecting to www.artbrokerage.com at 66.11.147.48. The SYN/ACK is in frame 16. Right	50263 > 80 [ACK] Se	
8	18	0.000565	24.6.173.220	66.11.147.48	HTTP	HTTP	à\234\223	We request an 850x600 size of a Peter Lik photo.	GET /imgres?imgurl	
9	21	0.000709	24.6.173.220	77.93.251.49	HTTP	HTTP	à\234\223	Now we are making a request to www.ulisseide.org.	80 > 50220 [ACK] Se	
10	23	0.146588	66.11.147.48	24.6.173.220	TCP	HTTP	à\234\223	This TCP connection is used to get the image file from artbrokerage.com. Check out File Export Objec	80 > 50220 [ACK] Se	
11	67	0.048584	77.93.251.49	24.6.173.220	HTTP	HTTP	à\234\223	Here's the redirection to the malicious site. See the Location line. We are being redirected to http://3x	80 > 50220 [ACK] Se	
12	68	0.00217	24.6.173.220	95.169.190.2	TCP	HTTP	à\234\223	We removed the DNS queries from the trace file - we must have looked up the IP address and now we	80 > 50220 [PSH, AC	
13	75	0.002074	95.169.190.2	24.6.173.220	HTTP	HTTP	à\234\223	Our malicious host is redirecting us to run a CGI script (in.cgi). We'll have to make another connection	HTTP/1.1 200 OK (te	
14	79	0.002733	24.6.173.220	95.169.190.2	TCP	HTTP	à\234\223	And here we go... this is the ugly connection.	50220 > 80 [ACK] Se	
15	84	0.000015	24.6.173.220	95.169.190.2	HTTP	HTTP	à\234\223	Please oh please hit us over the head with a baseball bat! We ask for the malicious in.cgi script now.	D 50316 > 80 [SYN] Se	
16	87	0.011399	95.169.190.2	24.6.173.220	HTTP	HTTP	à\234\223	They're dropping a cookie on our drive and giving us a link to a .info site in a script.	50317 > 80 [SYN] Se	
17	96	0.002946	24.6.173.220	78.41.203.19	TCP	TCP RST	à\234\223	Well that didn't go so well for them... our Symantec software terminated the connection and wouldn't	80 > 50317 [SYN, AC	
18	104	0.001678	24.6.173.220	78.41.203.19	TCP	TCP RST	à\234\223	And another termination triggered by Symantec.	50317 > 80 [ACK] Se	
19	117	0.001682	24.6.173.220	78.41.203.19	TCP	TCP RST	à\234\223	Yes, Symantec is screaming with messages on our system...	GET /artthumb/likp	
20	159	0.327815	24.6.173.220	74.125.224.8	HTTP	HTTP	à\234\223	We're just returning to Google after a little sidetrack to the dark side...	80 > 50316 [SYN, AC	
21										

Volver a wireshark y darle clic al botón borrar para eliminar el filtro de pantalla, y eliminar la columna