

Ejercicio1

No.	Time	Source	Destination	Protocol	Length Info
1	0.000000	192.168.1.3	192.168.1.8	TCP	78 49859 → 7777 [SYN, ECN, CWR] Seq=0 Win=65535 Len=460 Mss=1460 Snd=1369115968 TSecr=0 SACK_PERM
2	0.000000	192.168.1.8	192.168.1.3	TCP	66 49859 → 49859 [ACK] Seq=1 Win=131744 Len=0 Tsva1=369115982 Tsecr=154522618 Tsecr=369115968 wS=128
3	0.002756	192.168.1.3	192.168.1.8	TCP	66 49859 → 7777 [ACK] Seq=1 Win=131744 Len=0 Tsva1=369115982 Tsecr=154522618
4	0.002758	192.168.1.3	192.168.1.8	TCP	81 49859 → 7777 [PSH, ACK] Seq=1 Ack=1 Win=131744 Len=15 Tsva1=369115982 Tsecr=154522618
5	0.002758	192.168.1.3	192.168.1.8	TCP	66 7777 → 49859 [ACK] Seq=1 Ack=16 Win=29056 Len=0 Tsva1=154522618 Tsecr=369115982
6	0.002763	192.168.1.3	192.168.1.8	TCP	66 49859 → 7777 [FIN, ACK] Seq=16 Ack=1 Win=131744 Len=0 Tsva1=369115982 Tsecr=154522618
7	0.002763	192.168.1.3	192.168.1.8	TCP	66 7777 → 49859 [FIN, ACK] Seq=17 Ack=17 Win=29056 Len=0 Tsva1=154522618 Tsecr=369115982
8	0.008038	192.168.1.3	192.168.1.8	TCP	66 49859 → 7777 [ACK] Seq=17 Ack=2 Win=131744 Len=0 Tsva1=369115985 Tsecr=154522618

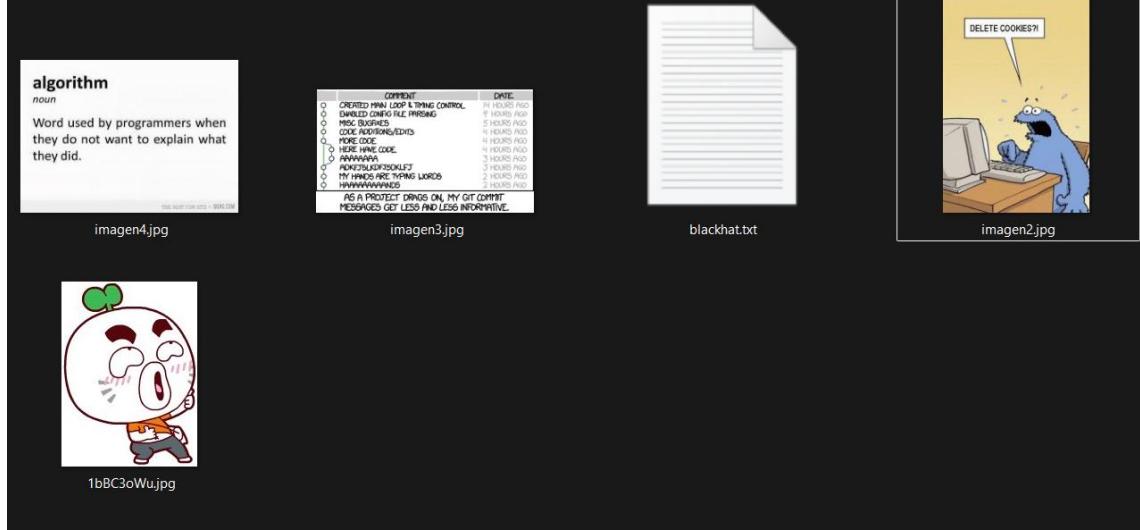
Ejercicio2

No.	Time	Source	Destination	Protocol	Length Info
4	0.003381	192.168.1.8	192.168.1.228	FTP	91 Response: 220 Teh Shrieking Shack
6	0.003381	192.168.1.228	192.168.1.8	FTP	80 Request: 220 192.168.1.228
8	0.2.374374	192.168.1.8	192.168.1.228	FTP	100 Response: 331 Please specify the password.
10	5.854089	192.168.1.228	192.168.1.8	FTP	82 Request: PASS BabyShark
11	5.875157	192.168.1.8	192.168.1.228	FTP	89 Response: 230 Login successful.
13	5.875833	192.168.1.228	192.168.1.8	FTP	72 Request: SYST
14	5.875853	192.168.1.8	192.168.1.228	FTP	85 Response: 215 UNIX Type: L8
16	13.36618	192.168.1.228	192.168.1.8	FTP	74 Request: PWD
17	13.36618	192.168.1.228	192.168.1.8	FTP	93 Response: 200 Switching to Binary mode.
19	13.365453	192.168.1.228	192.168.1.8	FTP	93 Request: PORT 192.168.1.228,195,60
20	13.366019	192.168.1.228	192.168.1.8	FTP	117 Response: 200 PORT command successful. Consider using PASV.
22	13.366418	192.168.1.228	192.168.1.8	FTP	85 Request: STOR 1bBC0JwU.jpg
26	13.368125	192.168.1.8	192.168.1.228	FTP	88 Response: 150 Ok to send data.
51	14.372129	192.168.1.8	192.168.1.228	FTP	99 Response: 226 Transfer complete.
52	14.372129	192.168.1.228	192.168.1.8	FTP	93 Request: PORT 192.168.1.228,195,61
54	21.652953	192.168.1.9	192.168.1.228	FTP	117 Response: 200 PORT command successful. Consider using PASV.
56	21.653495	192.168.1.228	192.168.1.8	FTP	85 Request: STOR b5f6B980.jpg
60	21.653853	192.168.1.8	192.168.1.228	FTP	88 Response: 150 Ok to send data.
157	21.656342	192.168.1.8	192.168.1.228	FTP	99 Response: 226 Transfer complete.
159	31.420066	192.168.1.228	192.168.1.8	FTP	93 Request: PORT 192.168.1.228,195,62
160	31.420066	192.168.1.8	192.168.1.228	FTP	117 Response: 200 PORT command successful. Consider using PASV.
162	31.420062	192.168.1.228	192.168.1.8	FTP	98 Request: STOR gear-blackhat-dotline14.txt
166	31.421033	192.168.1.8	192.168.1.228	FTP	88 Response: 150 Ok to send data.
259	31.423289	192.168.1.8	192.168.1.228	FTP	98 Response: 226 Transfer complete.
261	42.315252	192.168.1.228	192.168.1.8	FTP	93 Request: PORT 192.168.1.228,195,63
262	42.315353	192.168.1.8	192.168.1.228	FTP	117 Response: 200 PORT command successful. Consider using PASV.
264	42.315748	192.168.1.228	192.168.1.8	FTP	85 Request: STOR x6GoyPx.jpg
268	42.315748	192.168.1.8	192.168.1.228	FTP	88 Response: 150 Ok to send data.
286	42.319428	192.168.1.8	192.168.1.228	FTP	98 Response: 226 Transfer complete.
348	49.694544	192.168.1.228	192.168.1.8	FTP	93 Request: PORT 192.168.1.228,195,64
439	49.694640	192.168.1.8	192.168.1.228	FTP	117 Response: 200 PORT command successful. Consider using PASV.
441	49.695298	192.168.1.228	192.168.1.8	FTP	85 Request: STOR xcfgHgY3.jpg
445	49.695766	192.168.1.8	192.168.1.228	FTP	88 Response: 150 Ok to send data.
474	49.696858	192.168.1.8	192.168.1.228	FTP	99 Response: 226 Transfer complete.
476	52.930134	192.168.1.228	192.168.1.8	FTP	72 Request: QUIT
477	52.930203	192.168.1.8	192.168.1.228	FTP	88 Response: 221 Goodbye.

Se puede observar algunos uploads en líneas que usan el comando STOR seguido del nombre del archivo.

Hemos dado a seguir y que nos lo muestre en formato RAW.

Tras eso hay que guardar como y lo guardamos en su respectivos formatos.



Ejercicio3

No.	Time	Source	Destination	Protocol	Length Info
4	0.005125	192.168.1.228	192.168.1.20	TCP	1090 51063 + 7777 [PSH, ACK] Seq=1 Ack=1 Win=131712 Len=1024 TStamp=932937926 TSect=1926733056
6	0.005265	192.168.1.228	192.168.1.20	TCP	1514 51063 + 7777 [ACK] Seq=1025 Ack=1 Win=131712 Len=1448 TStamp=932937927 TSect=1926733056
8	0.005312	192.168.1.228	192.168.1.20	TCP	666 51063 + 7777 [PSH, ACK] Seq=2473 Ack=1 Win=131712 Len=608 TStamp=932937927 TSect=1926733056
10	0.006262	192.168.1.228	192.168.1.20	TCP	1514 51063 + 7777 [ACK] Seq=3073 Ack=1 Win=131712 Len=1448 TStamp=932937927 TSect=1926733056
12	0.006309	192.168.1.228	192.168.1.20	TCP	666 51063 + 7777 [ACK] Seq=3073 Ack=1 Win=131712 Len=1448 TStamp=932937927 TSect=1926733056
14	0.006663	192.168.1.228	192.168.1.20	TCP	1514 51063 + 7777 [ACK] Seq=5121 Ack=1 Win=131712 Len=1448 TStamp=92937927 TSect=1926733056
16	0.006789	192.168.1.228	192.168.1.20	TCP	666 51063 + 7777 [PSH, ACK] Seq=6569 Ack=1 Win=131712 Len=608 TStamp=932937927 TSect=1926733056
18	0.006731	192.168.1.228	192.168.1.20	TCP	1514 51063 + 7777 [ACK] Seq=7161 Ack=1 Win=131712 Len=1448 TStamp=932937927 TSect=1926733056
20	0.006755	192.168.1.228	192.168.1.20	TCP	666 51063 + 7777 [PSH, ACK] Seq=8623 Ack=1 Win=131712 Len=608 TStamp=932937927 TSect=1926733056
22	0.006795	192.168.1.228	192.168.1.20	TCP	1514 51063 + 7777 [ACK] Seq=9217 Ack=1 Win=131712 Len=1448 TStamp=932937927 TSect=1926733056
24	0.006831	192.168.1.228	192.168.1.20	TCP	666 51063 + 7777 [ACK] Seq=1025 Ack=1 Win=131712 Len=1448 TStamp=932937927 TSect=1926733056
26	0.006959	192.168.1.228	192.168.1.20	TCP	1514 51063 + 7777 [ACK] Seq=11265 Ack=1 Win=131712 Len=1448 TStamp=932937931 TSect=1926733061
28	0.009157	192.168.1.228	192.168.1.20	TCP	1514 51063 + 7777 [ACK] Seq=12113 Ack=1 Win=131712 Len=1448 TStamp=932937931 TSect=1926733061
30	0.009968	192.168.1.228	192.168.1.20	TCP	1514 51063 + 7777 [ACK] Seq=14161 Ack=1 Win=131712 Len=1448 TStamp=932937931 TSect=1926733061
32	0.010003	192.168.1.228	192.168.1.20	TCP	1514 51063 + 7777 [ACK] Seq=15609 Ack=1 Win=131712 Len=1448 TStamp=932937931 TSect=1926733061
34	0.010010	192.168.1.228	192.168.1.20	TCP	1514 51063 + 7777 [ACK] Seq=17057 Ack=1 Win=131712 Len=1448 TStamp=932937931 TSect=1926733062
36	0.010018	192.168.1.228	192.168.1.20	TCP	1514 51063 + 7777 [ACK] Seq=18512 Ack=1 Win=131712 Len=1448 TStamp=932937931 TSect=1926733062
38	0.010026	192.168.1.228	192.168.1.20	TCP	1514 51063 + 7777 [ACK] Seq=19923 Ack=1 Win=131712 Len=1448 TStamp=932937931 TSect=1926733062
39	0.011931	192.168.1.228	192.168.1.20	TCP	1514 51063 + 7777 [ACK] Seq=21401 Ack=1 Win=131712 Len=1448 TStamp=932937931 TSect=1926733063
40	0.011936	192.168.1.228	192.168.1.20	TCP	1514 51063 + 7777 [ACK] Seq=22849 Ack=1 Win=131712 Len=1448 TStamp=932937932 TSect=1926733063
41	0.011946	192.168.1.228	192.168.1.20	TCP	1514 51063 + 7777 [ACK] Seq=24297 Ack=1 Win=131712 Len=1448 TStamp=932937932 TSect=1926733063
42	0.011950	192.168.1.228	192.168.1.20	TCP	1514 51063 + 7777 [ACK] Seq=25745 Ack=1 Win=131712 Len=1448 TStamp=932937932 TSect=1926733063
43	0.011957	192.168.1.228	192.168.1.20	TCP	1514 51063 + 7777 [ACK] Seq=27193 Ack=1 Win=131712 Len=1448 TStamp=932937932 TSect=1926733063
45	0.012063	192.168.1.228	192.168.1.20	TCP	1514 51063 + 7777 [ACK] Seq=28663 Ack=1 Win=131712 Len=1448 TStamp=932937932 TSect=1926733063
47	0.012074	192.168.1.228	192.168.1.20	TCP	1514 51063 + 7777 [ACK] Seq=29889 Ack=1 Win=131712 Len=1448 TStamp=932937932 TSect=1926733063
47	0.012076	192.168.1.228	192.168.1.20	TCP	1514 51063 + 7777 [ACK] Seq=31557 Ack=1 Win=131712 Len=1448 TStamp=932937932 TSect=1926733063
49	0.015133	192.168.1.228	192.168.1.20	TCP	1514 51063 + 7777 [ACK] Seq=32985 Ack=1 Win=131712 Len=1448 TStamp=932937933 TSect=1926733065
50	0.015166	192.168.1.228	192.168.1.20	TCP	1514 51063 + 7777 [ACK] Seq=34433 Ack=1 Win=131712 Len=1448 TStamp=932937933 TSect=1926733065
51	0.015191	192.168.1.228	192.168.1.20	TCP	1514 51063 + 7777 [ACK] Seq=35881 Ack=1 Win=131712 Len=1448 TStamp=932937933 TSect=1926733065
52	0.015199	192.168.1.228	192.168.1.20	TCP	1514 51063 + 7777 [ACK] Seq=37329 Ack=1 Win=131712 Len=1448 TStamp=932937933 TSect=1926733065
53	0.015212	192.168.1.228	192.168.1.20	TCP	1514 51063 + 7777 [ACK] Seq=38977 Ack=1 Win=131712 Len=1448 TStamp=932937934 TSect=1926733066
54	0.015218	192.168.1.228	192.168.1.20	TCP	1514 51063 + 7777 [ACK] Seq=39309 Ack=1 Win=131712 Len=1448 TStamp=932937934 TSect=1926733066
55	0.015231	192.168.1.228	192.168.1.20	TCP	1514 51063 + 7777 [ACK] Seq=40809 Ack=1 Win=131712 Len=1448 TStamp=932937934 TSect=1926733066
56	0.015247	192.168.1.228	192.168.1.20	TCP	1514 51063 + 7777 [ACK] Seq=41212 Ack=1 Win=131712 Len=1448 TStamp=932937934 TSect=1926733066
57	0.015314	192.168.1.228	192.168.1.20	TCP	1514 51063 + 7777 [ACK] Seq=44569 Ack=1 Win=131712 Len=1448 TStamp=932937934 TSect=1926733066
58	0.015345	192.168.1.228	192.168.1.20	TCP	1514 51063 + 7777 [ACK] Seq=46017 Ack=1 Win=131712 Len=1448 TStamp=932937934 TSect=1926733066
60	0.016886	192.168.1.228	192.168.1.20	TCP	1514 51063 + 7777 [ACK] Seq=47465 Ack=1 Win=131712 Len=1448 TStamp=932937934 TSect=1926733068
62	0.016839	192.168.1.228	192.168.1.20	TCP	1514 51063 + 7777 [ACK] Seq=48913 Ack=1 Win=131712 Len=1448 TStamp=932937934 TSect=1926733068
64	0.016873	192.168.1.228	192.168.1.20	TCP	1514 51063 + 7777 [ACK] Seq=50361 Ack=1 Win=131712 Len=1448 TStamp=932937934 TSect=1926733068

Buscamos flujos de TCP con datos y seleccionamos los flujos que tengan el termino PSH.

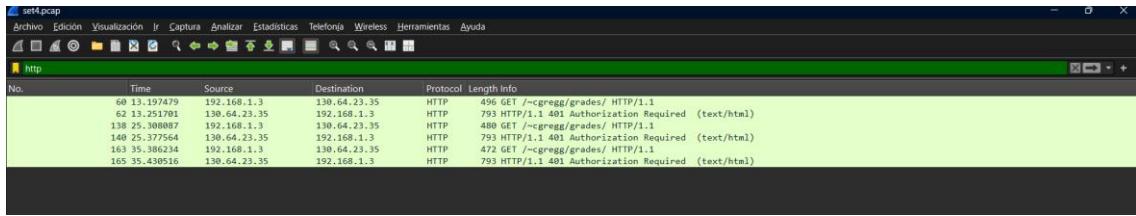
Volvemos a hacer click derecho y seguir, después de eso formato RAW y ahora nos tenemos que fijar en el inicio del flujo, dependiendo del inicio será un tipo de archivo u otro (PDF, JPG,MP4).



En nuestro caso tras buscarlo nuestro archivo es un mp4. Tras eso lo guardamos en nuestra carpeta.

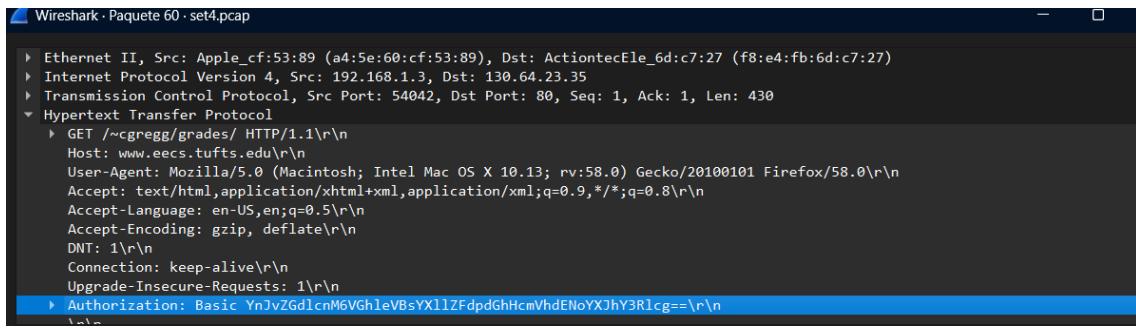
Ejercicio4

Ponemos nuestro filtro para buscar http sin seguridad:



Hemos visto varios archivos get que puede que tengan credenciales dentro de la URL.

El encabezado encontrado dentro del paquete fue el siguiente:



Authorization: Basic

YnJvZGd1cnM6VGhleVBsYXllZFdpdGhHcmVhdENoYXJhY3Rlcg==

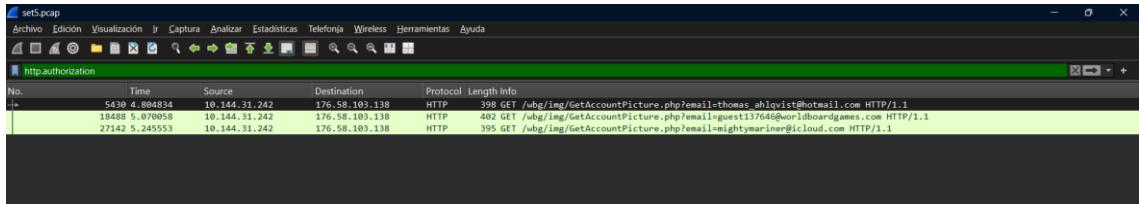
La cadena codificada en Base64 representa las credenciales utilizadas por el cliente. Tras proceder a su decodificación, el resultado obtenido fue:

- **Usuario:** brodgers
- **Contraseña:** TheyPlayedWithGreatCharacter

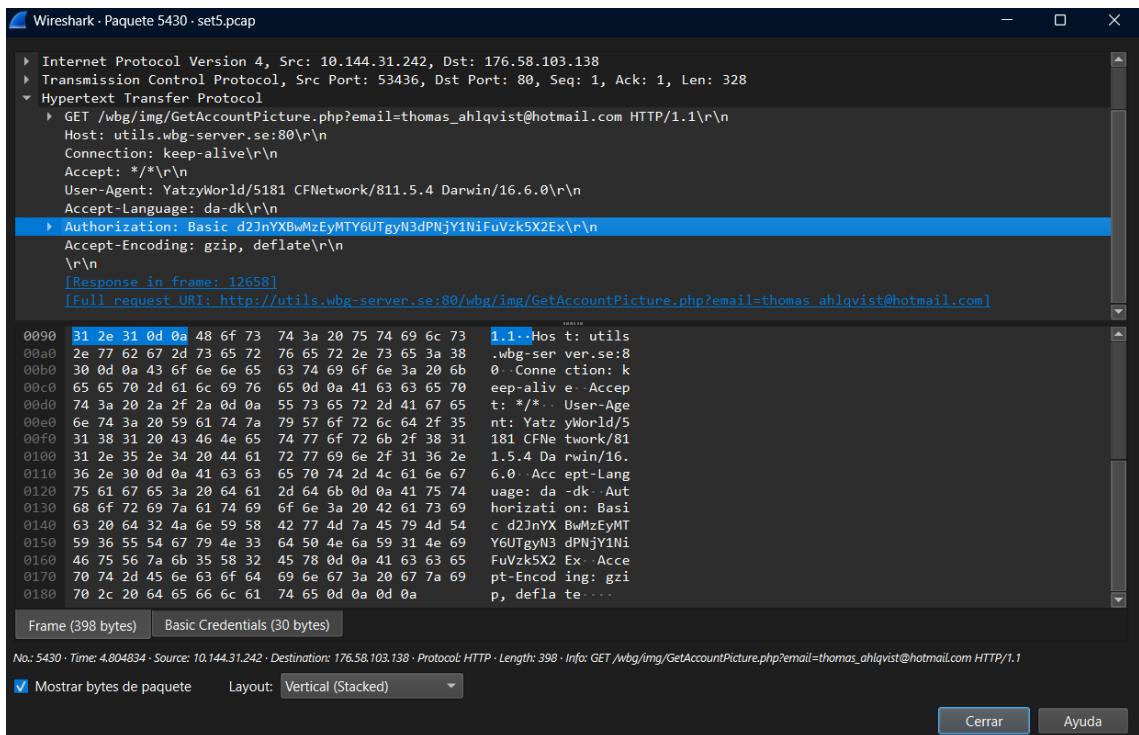
Este intercambio se realizó mediante el protocolo HTTP sin cifrar, lo cual permitió que las credenciales fueran capturadas íntegramente en texto plano dentro del tráfico interceptado.

Ejercicio5

Es como el ejercicio anterior pero ponemos un filtro algo mas restrictivo.
Http.authorization



Volvemos a ver lo mismo anteriormente:



En el primer paquete relevante identificado dentro de set5.pcap, se observó una petición HTTP de tipo GET hacia el servidor utils.wbg-server.se. La solicitud incluía un parámetro de correo electrónico (thomas_ahlqvist@hotmail.com) y contenía un encabezado de autenticación básica transmitido en texto plano debido al uso de HTTP sobre el puerto 80.

El campo capturado fue:

Authorization: Basic d2JnYXBwMzEyMTY6UTgyN3dPNjY1NiFuVzk5X2Ex

Tras la decodificación de la cadena Base64, se obtuvo el siguiente par de credenciales:

Usuario: wbgapp31216

Contraseña: Q827wO6656!nW99_a1

Esta credencial corresponde al primer usuario comprometido dentro del tráfico analizado.

En el segundo paquete HTTP identificado dentro del archivo set5.pcap, se observó otra petición GET hacia el mismo servidor utils.wbg-server.se, esta vez asociada al correo guest137646@worldboardgames.com. Nuevamente, la solicitud fue realizada mediante HTTP sin cifrado y contenía un encabezado de autenticación básica.

El campo capturado fue:

Authorization: Basic d2JnYXBwMzEyMTY6UTgyN3dPNjY1NiFuVzk5X2Ex

La decodificación de la cadena Base64 reveló las siguientes credenciales:

Usuario: wbgapp31216

Contraseña: Q827wO6656!nW99_a1

Esto confirma que la misma credencial está siendo reutilizada para múltiples accesos, un patrón común en aplicaciones que utilizan cuentas de servicio internas. Sin cifrado TLS, estas credenciales pueden ser interceptadas fácilmente y reutilizadas por un atacante.

	GET (frame)	Email	Respuesta en frame	Código HTTP	Observación del body
5430		thomas_ahlqvist@hotmail.com	12658	200 OK	Imagen de usuario
18488		guest137646@worldboardgames.com	25576	200 OK	Imagen de usuario
27142		mightymariner@icloud.com	67519	200 OK	Imagen de usuario

Ejercicio 6

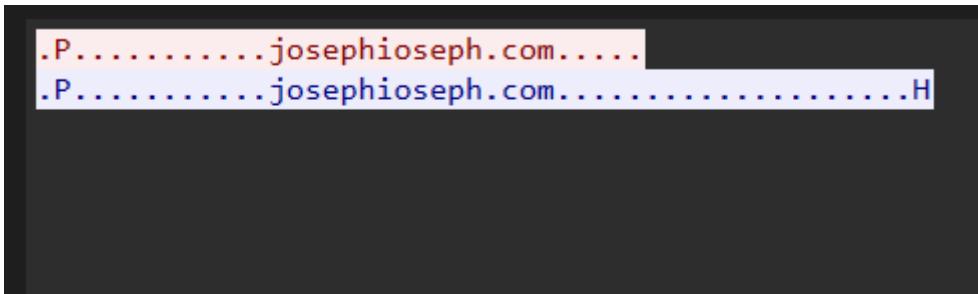
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.11.16.101	10.11.16.1	DNS	70	Standard query 0x0050 A josephioseph.com
2	0.092426	10.11.16.101	10.11.16.101	DNS	92	Standard query response 0x0050 A josephioseph.com A 192.185.16.72
6	2.145133	10.11.16.101	192.185.16.72	HTTP	370	GET /imaya/htadills.htm HTTP/1.1
8	2.335154	192.185.16.72	10.11.16.101	HTTP	1257	HTTP/1.1 200 OK (text/plain)
10	11.364652	10.11.16.101	10.11.16.1	DNS	76	Standard query 0x0033 A josephioseph.com
11	13.344120	10.11.16.1	10.11.16.101	DNS	92	Standard query response 0x0033 A josephioseph.com A 192.185.16.72
15	13.498485	10.11.16.101	192.185.16.72	HTTP	137	GET /imaya/drills.exe HTTP/1.1
630	31.090772	10.11.16.101	10.11.16.1	DNS	91	Standard query 0xbab3 A myapplicationsdownload.download
631	31.100000	10.11.16.101	10.11.16.101	DNS	108	Standard query response 0xbab3 A myapplicationsdownload.download A 209.182.213.90
637	33.197679	10.11.16.101	209.182.213.90	HTTP	258	POST /animationsetup1/animation1kc/fre.php HTTP/1.0
639	33.447229	209.182.213.90	10.11.16.101	HTTP	192	HTTP/1.1 404 Not Found (text/html)
643	41.529968	10.11.16.101	10.11.16.1	DNS	91	Standard query 0xe8bb A myapplicationsdownload.download
644	43.520559	10.11.16.1	10.11.16.101	DNS	107	Standard query response 0xe8bb A myapplicationsdownload.download A 209.182.213.90
650	43.638229	10.11.16.101	209.182.213.90	HTTP	259	POST /animationsetup1/animation1kc/fre.php HTTP/1.0
656	43.652909	10.11.16.101	10.11.16.1	DNS	192	Standard query response 0xe8bb A myapplicationsdownload.download
656	52.016242	10.11.16.101	10.11.16.1	DNS	91	Standard query 0x1idd A myapplicationsdownload.download
657	54.007916	10.11.16.101	10.11.16.1	DNS	107	Standard query response 0x1idd A myapplicationsdownload.download A 209.182.213.90
663	54.128797	10.11.16.101	209.182.213.90	HTTP	231	POST /animationsetup1/animation1kc/fre.php HTTP/1.0
665	54.371424	209.182.213.90	10.11.16.101	HTTP	191	HTTP/1.1 200 OK (text/html)
673	122.445210	10.11.16.101	10.11.16.1	DNS	91	Standard query 0x4359 A myapplicationsdownload.download
674	122.445210	10.11.16.101	10.11.16.1	DNS	107	Standard query response 0x4359 A myapplicationsdownload.download A 209.182.213.90
680	124.489147	10.11.16.101	209.182.213.90	HTTP	231	POST /animationsetup1/animation1kc/fre.php HTTP/1.0
682	124.489573	209.182.213.90	10.11.16.101	HTTP	193	HTTP/1.1 200 OK (text/html)
686	192.270896	10.11.16.101	10.11.16.1	DNS	91	Standard query 0x6e22 A myapplicationsdownload.download
687	194.941833	10.11.16.1	10.11.16.101	DNS	107	Standard query response 0x6e22 A myapplicationsdownload.download A 209.182.213.90
693	195.065942	10.11.16.101	209.182.213.90	HTTP	231	POST /animationsetup1/animation1kc/fre.php HTTP/1.0
695	195.388015	209.182.213.90	10.11.16.101	HTTP	191	HTTP/1.1 200 OK (text/html)
699	261.144001	10.11.16.101	10.11.16.1	DNS	91	Standard query 0x3914 A myapplicationsdownload.download
700	265.459880	10.11.16.1	10.11.16.101	DNS	107	Standard query response 0x3914 A myapplicationsdownload.download A 209.182.213.90
706	265.581010	10.11.16.101	209.182.213.90	HTTP	231	POST /animationsetup1/animation1kc/fre.php HTTP/1.0
708	265.581881	209.182.213.90	10.11.16.101	HTTP	193	HTTP/1.1 200 OK (text/html)
712	333.882949	10.11.16.101	10.11.16.1	DNS	91	Standard query 0x8628 A myapplicationsdownload.download
713	335.862771	10.11.16.101	10.11.16.101	DNS	107	Standard query response 0x8628 A myapplicationsdownload.download A 209.182.213.90
719	335.978508	10.11.16.101	209.182.213.90	HTTP	231	POST /animationsetup1/animation1kc/fre.php HTTP/1.0
720	335.978508	209.182.213.90	10.11.16.101	HTTP	60	HTTP/1.1 200 OK (text/html)
726	404.273104	10.11.16.101	10.11.16.1	DNS	91	Standard query 0x7456 A myapplicationsdownload.download
727	406.536313	10.11.16.101	10.11.16.101	DNS	107	Standard query response 0x7456 A myapplicationsdownload.download A 209.182.213.90
733	406.669323	10.11.16.101	209.182.213.90	HTTP	231	POST /animationsetup1/animation1kc/fre.php HTTP/1.0
735	406.924913	209.182.213.90	10.11.16.101	HTTP	193	HTTP/1.1 200 OK (text/html)

Wireshark - Seguir secuencia HTTP (tcp.stream eq 3) · set6.pcap

```
POST /animationsetup1/animation1kc/fre.php HTTP/1.0
User-Agent: Mozilla/4.08 (Charon; Inferno)
Host: myapplicationsdownload.download
Accept: */*
Content-Type: application/octet-stream
Content-Encoding: binary
Content-Key: B97842B0
Content-Length: 204
Connection: close

HTTP/1.1 404 Not Found
Date: Thu, 16 Nov 2017 08:58:33 GMT
Server: Apache
Connection: close
Content-Type: text/html

File not found.
```



El análisis de la captura set6.pcap reveló tráfico malicioso típico de malspam y malware. Se identificaron intentos de comunicación HTTP sospechosos, incluyendo un POST binario hacia myapplicationsdownload.download con ruta /animationsetup1/animation1kc/fre.php y un User-Agent inusual (Mozilla/4.08 (Charon; Inferno)), además de dominios incrustados como josephioseph.com, que actúan como indicadores de compromiso (IoCs). Aunque algunos recursos devolvieron 404 Not Found, la actividad evidencia intención de descarga de payloads y posible beaconing a servidores de comando y control. Este tráfico demuestra cómo malware intenta distribuirse y comunicarse de forma encubierta, y subraya la importancia de documentar dominios, rutas y patrones HTTP para la detección y mitigación de amenazas sin ejecutar archivos peligrosos.