

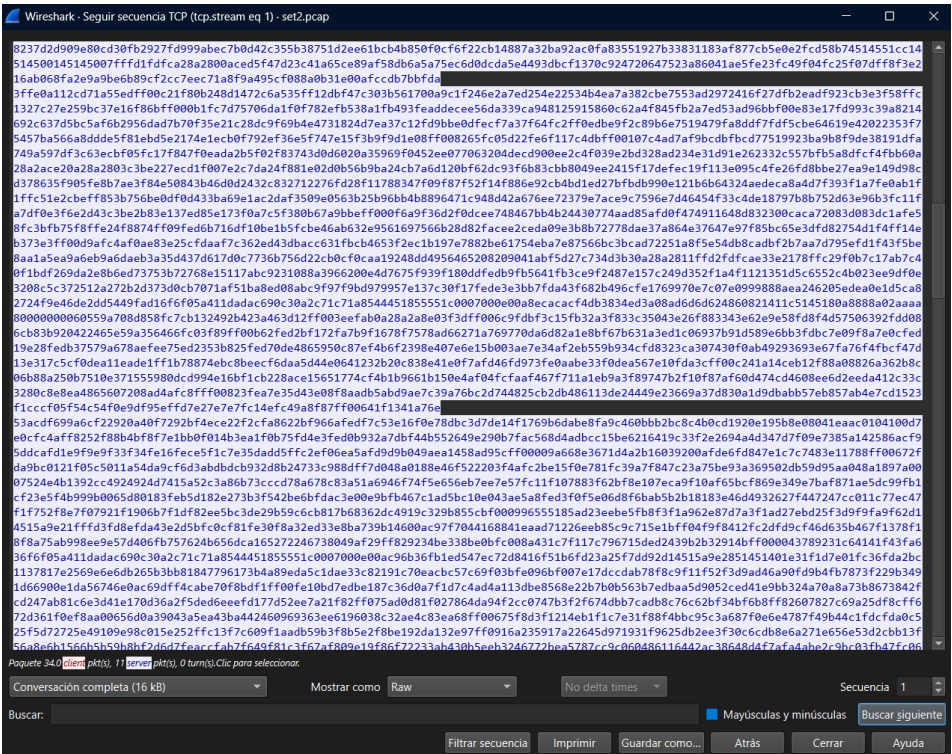
Ejercicio1

set1.pcap						
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda						
Aplique un filtro de visualización ... <Ctrl />						
No.	Time	Source	Destination	Protocol	Length Info	
1	0.000000	192.168.1.3	192.168.1.8	TCP	74	49859 → 7777 [SYN, ACK, ECE] Seq=0 Win=0 Len=0 MSS=460 W=0 Len=0 TSval=369115982 TSecr=0 SACK_PERM
2	0.000318	192.168.1.8	192.168.1.3	TCP	74	7777 → 49859 [SYN, ACK, ECE] Seq=0 Ack=1 Win=28960 Len=0 MSS=460 SACK_PERM TSval=154522618 TSecr=369115982 WS=128
3	0.002276	192.168.1.3	192.168.1.8	TCP	66	49859 → 7777 [ACK] Seq=1 Ack=1 Win=131744 Len=0 TSval=369115982 TSecr=154522618
4	0.002278	192.168.1.3	192.168.1.8	TCP	81	49859 → 7777 [PSH, ACK] Seq=1 Ack=1 Win=131744 Len=15 TSval=369115982 TSecr=154522618
5	0.002412	192.168.1.8	192.168.1.3	TCP	66	7777 → 49859 [ACK] Seq=1 Ack=16 Win=29056 Len=0 TSval=154522618 TSecr=369115982
6	0.002643	192.168.1.3	192.168.1.8	TCP	66	49859 → 7777 [FIN, ACK] Seq=16 Ack=1 Win=131744 Len=0 TSval=369115982 TSecr=154522618
7	0.002731	192.168.1.8	192.168.1.3	TCP	66	7777 → 49859 [FIN, ACK] Seq=1 Ack=17 Win=29056 Len=0 TSval=154522618 TSecr=369115982
8	0.000038	192.168.1.3	192.168.1.8	TCP	66	49859 → 7777 [ACK] Seq=17 Ack=2 Win=131744 Len=0 TSval=369115985 TSecr=154522618

Ejercicio2

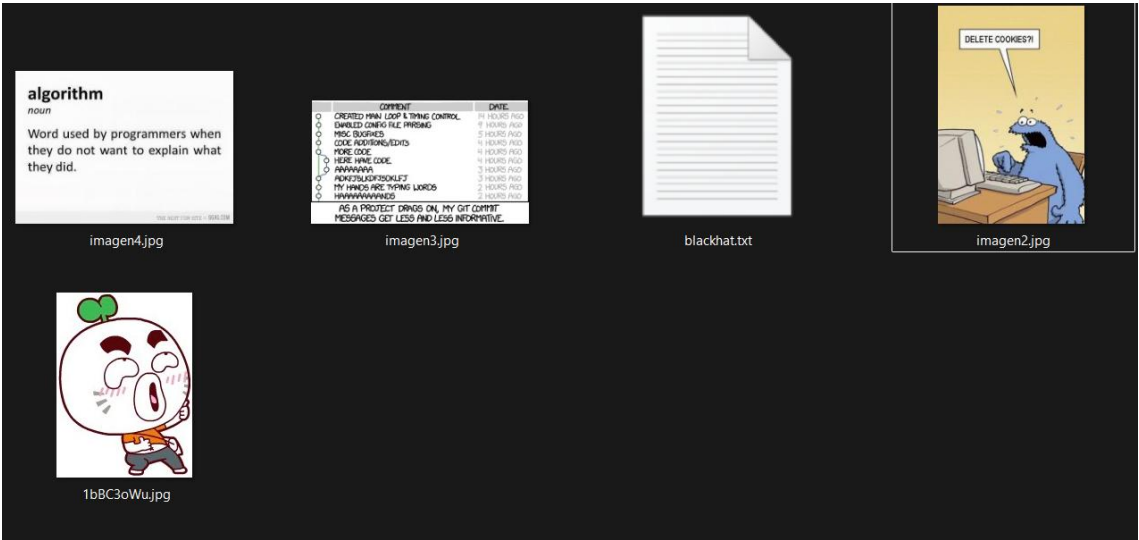
No.	Time	Source	Destination	Protocol	Length Info	
4	0.003381	192.168.1.8	192.168.1.228	FTP	91	Response: 220 Teh Shrieking Shack
6	2.374242	192.168.1.228	192.168.1.8	FTP	81	Request: USER woodworm
8	2.374374	192.168.1.8	192.168.1.228	FTP	100	Response: 331 Please specify the password.
10	5.854089	192.168.1.228	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	5.875831	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	13.365397	192.168.1.228	192.168.1.8	FTP	74	Request: TYPE I
17	13.365463	192.168.1.8	192.168.1.228	FTP	97	Response: 200 Switching to Binary mode.
19	13.365954	192.168.1.228	192.168.1.8	FTP	93	Request: PORT 192,168,1,228,195,60
20	13.366919	192.168.1.8	192.168.1.228	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 1bBC3oMu.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	90	Response: 226 Transfer complete.
53	21.652859	192.168.1.228	192.168.1.8	FTP	93	Request: PORT 192,168,1,228,195,61
54	21.652953	192.168.1.8	192.168.1.228	FTP	117	Response: 200 PORT command successful. Consider using PASV.
56	21.653405	192.168.1.228	192.168.1.8	FTP	85	Request: STOR b516898D.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	90	Response: 226 Transfer complete.
159	31.420060	192.168.1.228	192.168.1.8	FTP	93	Request: PORT 192,168,1,228,195,62
160	31.420153	192.168.1.8	192.168.1.228	FTP	117	Response: 200 PORT command successful. Consider using PASV.
162	31.420562	192.168.1.228	192.168.1.8	FTP	90	Request: STOR geer-blackhat-boiii14.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	90	Response: 226 Transfer complete.
261	42.315258	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	42.315740	192.168.1.228	192.168.1.8	FTP	85	Request: STOR x66oyPjk.jpg
268	42.316221	192.168.1.8	192.168.1.228	FTP	88	Response: 150 Ok to send data.
436	42.319428	192.168.1.8	192.168.1.228	FTP	90	Response: 226 Transfer complete.
438	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	49.695290	192.168.1.228	192.168.1.8	FTP	85	Request: STOR xcfgNgY3.jpg
445	49.695760	192.168.1.8	192.168.1.228	FTP	88	Response: 150 Ok to send data.
474	49.696450	192.168.1.8	192.168.1.228	FTP	50	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	80	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

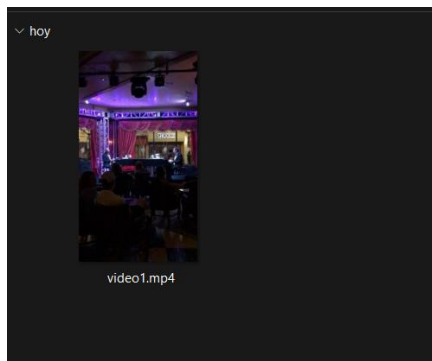
No.	Time	Source	Destination	Protocol	Length	Info
4	0.005125	192.168.1.220	192.168.1.20	TCP	1060	51063 → 7777 [PSH, ACK] Seq=1025 Ack=1 Win=131712 Len=1024 TSval=932937927 TSecr=1926733056
6	0.005265	192.168.1.220	192.168.1.20	TCP	1514	51063 → 7777 [ACK] Seq=1025 Ack=1 Win=131712 Len=1448 TSval=932937927 TSecr=1926733056
8	0.005312	192.168.1.220	192.168.1.20	TCP	666	51063 → 7777 [PSH, ACK] Seq=2473 Ack=1 Win=131712 Len=600 TSval=932937927 TSecr=1926733056
10	0.006262	192.168.1.220	192.168.1.20	TCP	1514	51063 → 7777 [ACK] Seq=3073 Ack=1 Win=131712 Len=1448 TSval=932937927 TSecr=1926733056
12	0.006332	192.168.1.220	192.168.1.20	TCP	666	51063 → 7777 [PSH, ACK] Seq=4521 Ack=1 Win=131712 Len=600 TSval=932937927 TSecr=1926733056
14	0.006563	192.168.1.220	192.168.1.20	TCP	1514	51063 → 7777 [ACK] Seq=5121 Ack=1 Win=131712 Len=1448 TSval=932937927 TSecr=1926733056
16	0.006704	192.168.1.220	192.168.1.20	TCP	666	51063 → 7777 [PSH, ACK] Seq=5569 Ack=1 Win=131712 Len=600 TSval=932937927 TSecr=1926733056
18	0.006731	192.168.1.220	192.168.1.20	TCP	1514	51063 → 7777 [ACK] Seq=7169 Ack=1 Win=131712 Len=1448 TSval=932937927 TSecr=1926733056
20	0.006755	192.168.1.220	192.168.1.20	TCP	666	51063 → 7777 [PSH, ACK] Seq=8617 Ack=1 Win=131712 Len=600 TSval=932937927 TSecr=1926733056
22	0.006795	192.168.1.220	192.168.1.20	TCP	1514	51063 → 7777 [ACK] Seq=9017 Ack=1 Win=131712 Len=1448 TSval=932937927 TSecr=1926733056
24	0.006831	192.168.1.220	192.168.1.20	TCP	666	51063 → 7777 [PSH, ACK] Seq=10665 Ack=1 Win=131712 Len=600 TSval=932937927 TSecr=1926733056
26	0.009129	192.168.1.220	192.168.1.20	TCP	1514	51063 → 7777 [ACK] Seq=11265 Ack=1 Win=131712 Len=1448 TSval=932937931 TSecr=1926733061
28	0.009157	192.168.1.220	192.168.1.20	TCP	1514	51063 → 7777 [ACK] Seq=12713 Ack=1 Win=131712 Len=1448 TSval=932937931 TSecr=1926733061
30	0.009568	192.168.1.220	192.168.1.20	TCP	1514	51063 → 7777 [ACK] Seq=14161 Ack=1 Win=131712 Len=1448 TSval=932937931 TSecr=1926733061
32	0.010003	192.168.1.220	192.168.1.20	TCP	1514	51063 → 7777 [ACK] Seq=15609 Ack=1 Win=131712 Len=1448 TSval=932937931 TSecr=1926733061
34	0.010010	192.168.1.220	192.168.1.20	TCP	1514	51063 → 7777 [ACK] Seq=17057 Ack=1 Win=131712 Len=1448 TSval=932937931 TSecr=1926733062
36	0.010018	192.168.1.220	192.168.1.20	TCP	1514	51063 → 7777 [ACK] Seq=18505 Ack=1 Win=131712 Len=1448 TSval=932937931 TSecr=1926733062
37	0.011893	192.168.1.220	192.168.1.20	TCP	1514	51063 → 7777 [ACK] Seq=19953 Ack=1 Win=131712 Len=1448 TSval=932937932 TSecr=1926733062
39	0.011931	192.168.1.220	192.168.1.20	TCP	1514	51063 → 7777 [ACK] Seq=21401 Ack=1 Win=131712 Len=1448 TSval=932937932 TSecr=1926733063
40	0.011936	192.168.1.220	192.168.1.20	TCP	1514	51063 → 7777 [ACK] Seq=22849 Ack=1 Win=131712 Len=1448 TSval=932937932 TSecr=1926733063
41	0.011948	192.168.1.220	192.168.1.20	TCP	1514	51063 → 7777 [ACK] Seq=24297 Ack=1 Win=131712 Len=1448 TSval=932937932 TSecr=1926733063
42	0.011950	192.168.1.220	192.168.1.20	TCP	1514	51063 → 7777 [ACK] Seq=25745 Ack=1 Win=131712 Len=1448 TSval=932937932 TSecr=1926733063
43	0.011957	192.168.1.220	192.168.1.20	TCP	1514	51063 → 7777 [ACK] Seq=27193 Ack=1 Win=131712 Len=1448 TSval=932937932 TSecr=1926733063
45	0.012067	192.168.1.220	192.168.1.20	TCP	1514	51063 → 7777 [ACK] Seq=28641 Ack=1 Win=131712 Len=1448 TSval=932937932 TSecr=1926733063
46	0.012074	192.168.1.220	192.168.1.20	TCP	1514	51063 → 7777 [ACK] Seq=30089 Ack=1 Win=131712 Len=1448 TSval=932937932 TSecr=1926733063
47	0.012076	192.168.1.220	192.168.1.20	TCP	1514	51063 → 7777 [ACK] Seq=31537 Ack=1 Win=131712 Len=1448 TSval=932937932 TSecr=1926733063
49	0.015133	192.168.1.220	192.168.1.20	TCP	1514	51063 → 7777 [ACK] Seq=32985 Ack=1 Win=131712 Len=1448 TSval=932937933 TSecr=1926733065
50	0.015160	192.168.1.220	192.168.1.20	TCP	1514	51063 → 7777 [ACK] Seq=34433 Ack=1 Win=131712 Len=1448 TSval=932937933 TSecr=1926733065
51	0.015191	192.168.1.220	192.168.1.20	TCP	1514	51063 → 7777 [ACK] Seq=35881 Ack=1 Win=131712 Len=1448 TSval=932937933 TSecr=1926733065
52	0.015198	192.168.1.220	192.168.1.20	TCP	1514	51063 → 7777 [ACK] Seq=37329 Ack=1 Win=131712 Len=1448 TSval=932937933 TSecr=1926733065
53	0.015212	192.168.1.220	192.168.1.20	TCP	1514	51063 → 7777 [ACK] Seq=38777 Ack=1 Win=131712 Len=1448 TSval=932937934 TSecr=1926733066
54	0.015218	192.168.1.220	192.168.1.20	TCP	1514	51063 → 7777 [ACK] Seq=40225 Ack=1 Win=131712 Len=1448 TSval=932937934 TSecr=1926733066
55	0.015231	192.168.1.220	192.168.1.20	TCP	1514	51063 → 7777 [ACK] Seq=41673 Ack=1 Win=131712 Len=1448 TSval=932937934 TSecr=1926733066
56	0.015247	192.168.1.220	192.168.1.20	TCP	1514	51063 → 7777 [ACK] Seq=43121 Ack=1 Win=131712 Len=1448 TSval=932937934 TSecr=1926733066
57	0.015314	192.168.1.220	192.168.1.20	TCP	1514	51063 → 7777 [ACK] Seq=44569 Ack=1 Win=131712 Len=1448 TSval=932937934 TSecr=1926733066
58	0.015345	192.168.1.220	192.168.1.20	TCP	1514	51063 → 7777 [ACK] Seq=46017 Ack=1 Win=131712 Len=1448 TSval=932937934 TSecr=1926733066
60	0.016086	192.168.1.220	192.168.1.20	TCP	1514	51063 → 7777 [ACK] Seq=47465 Ack=1 Win=131712 Len=1448 TSval=932937934 TSecr=1926733068
62	0.016839	192.168.1.220	192.168.1.20	TCP	1514	51063 → 7777 [ACK] Seq=48913 Ack=1 Win=131712 Len=1448 TSval=932937934 TSecr=1926733068
64	0.016873	192.168.1.220	192.168.1.20	TCP	1514	51063 → 7777 [ACK] Seq=50361 Ack=1 Win=131712 Len=1448 TSval=932937934 TSecr=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).

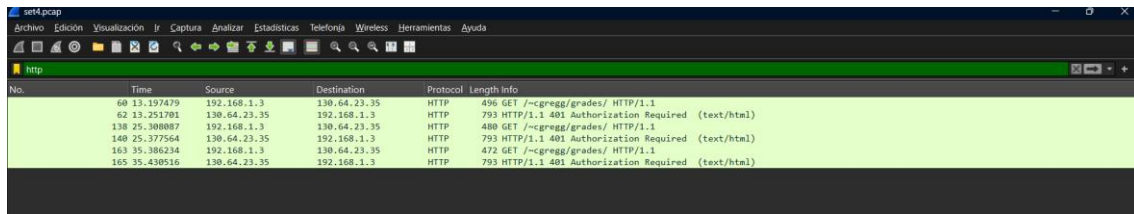
```
0000001466747970717420200000000717420200000008776964650239392e6d64617400d0400700da9bcc3ebf58d9a8cd1c172ffeb2b8e95abaebf67f4c5ce8d3ee43
af02e8f00813fe647fe0fc27fe0fb7fd490806c7e6ad544e6008347818fd23d6ee80fb7dd04e74e6cc1c192b2c74613096cf0783fac5be0b2a01c91dd790033ce60edfb0
3b7f3c424e765cf7119fac79df47349fe03b8fea9bfff3bb38ec40021c7fcea4f5ba427cdfcb84ab2493f96cb5cd1409cbd35b1a6ab525f685f79aec0a0c2ae22424b2ae46
8f203802a65e413cd14c9f4177a3123a300a6b4ca89fa5391a00fb4f183517b6b8456a5d920d5df211e1d0e0f4842db158a0eb70529e96fef8d90bc4c7222cbbf0e31a3
0f2dbbf1d38237e1a3a3061e92bb1e0c9c011cd72cf4982b31144240bfe8c4f3b7456ee889134974b94d6442d4d0b49dc4757ff358b078d1fb19efa6da83abfe7520093d
62c8ff7ef65c2a35cb0da342c62d98d24d63a00db472b1363fb2be9ba22583838dc70044fc9142a3bed319b6b24923b40143a141dc2f48924d854032e4163eef93542a
149e21db54bcfd22d74484432a8017668bc56628b51d2e8ccfc5dde569bc241c39d8e15c8538b166e52c98ecb39d30608551bb98c0ce53c896a98290320445db66f8e2f
7efa142c6b2a1264d789a3830ef666216a1f98868f77bba4ba58450d8cc81048ba15e207d1526b5aa0d4270af31136565c090fa305b704a4cea175d00bcb033470a15ac
```

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



Ejercicio4

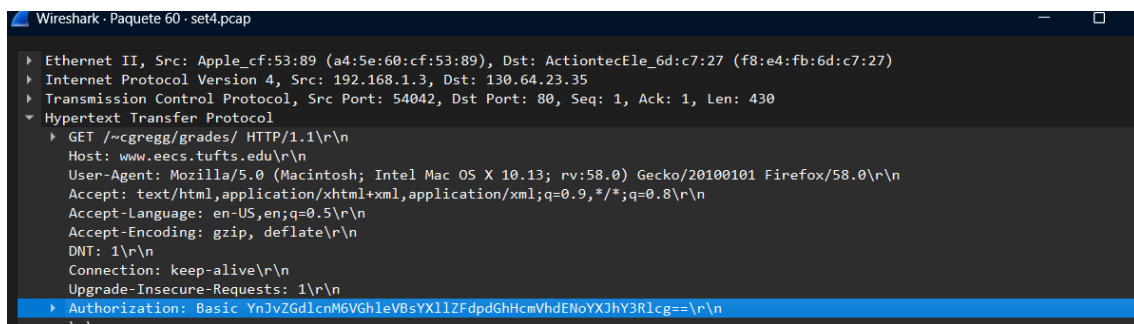
Ponemos nuestro filtro para buscar http sin seguridad:



No.	Time	Source	Destination	Protocol	Length	Info
60	13.197479	192.168.1.3	130.64.23.35	HTTP	496	GET /~cgregg/grades/ HTTP/1.1
62	13.251701	130.64.23.35	192.168.1.3	HTTP	793	HTTP/1.1 401 Authorization Required (text/html)
138	25.308087	192.168.1.3	130.64.23.35	HTTP	480	GET /~cgregg/grades/ HTTP/1.1
140	25.377564	130.64.23.35	192.168.1.3	HTTP	793	HTTP/1.1 401 Authorization Required (text/html)
163	35.386234	192.168.1.3	130.64.23.35	HTTP	472	GET /~cgregg/grades/ HTTP/1.1
165	35.430516	130.64.23.35	192.168.1.3	HTTP	793	HTTP/1.1 401 Authorization Required (text/html)

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

El encabezado encontrado dentro del paquete fue el siguiente:



```
Wireshark - Paquete 60 · set4.pcap
  ▶ Ethernet II, Src: Apple_cf:53:89 (a4:5e:60:cf:53:89), Dst: ActiontecEle_6d:c7:27 (f8:e4:fb:6d:c7:27)
  ▶ Internet Protocol Version 4, Src: 192.168.1.3, Dst: 130.64.23.35
  ▶ Transmission Control Protocol, Src Port: 54042, Dst Port: 80, Seq: 1, Ack: 1, Len: 430
  ▼ Hypertext Transfer Protocol
    ▶ GET /~cgregg/grades/ HTTP/1.1\r\n
      Host: www.eecs.tufts.edu\r\n
      User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:58.0) Gecko/20100101 Firefox/58.0\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
      Accept-Language: en-US,en;q=0.5\r\n
      Accept-Encoding: gzip, deflate\r\n
      DNT: 1\r\n
      Connection: keep-alive\r\n
      Upgrade-Insecure-Requests: 1\r\n
      ▶ Authorization: Basic YnJvZGdlcnM6VGhleVBsYXllZFdpdGhHcmVhdENoYXJhY3Rlcg==\r\n
      \r\n
```

Authorization: Basic

YnJvZGdlcnM6VGhleVBsYXllZFdpdGhHcmVhdENoYXJhY3Rlcg==

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

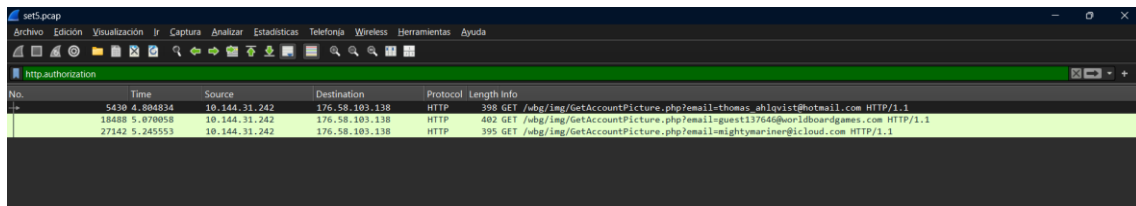
- **Usuario:** brodgers
- **Contraseña:** TheyPlayedWithGreatCharacter

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.

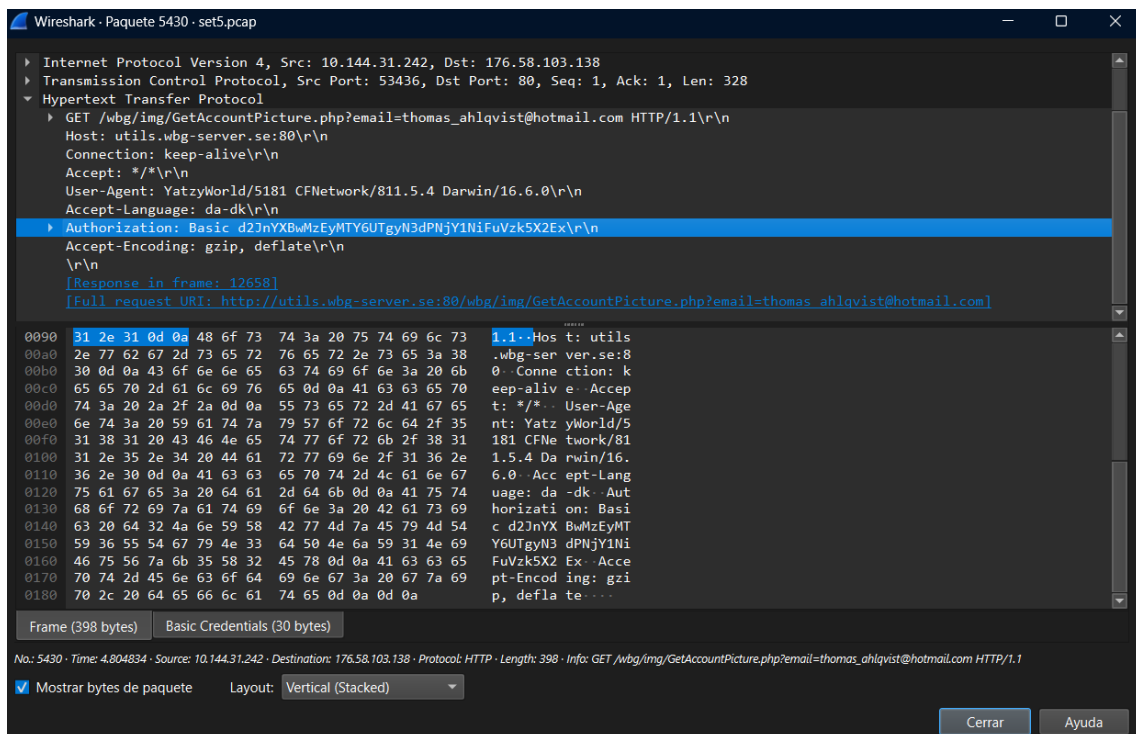
Ejercicio5

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

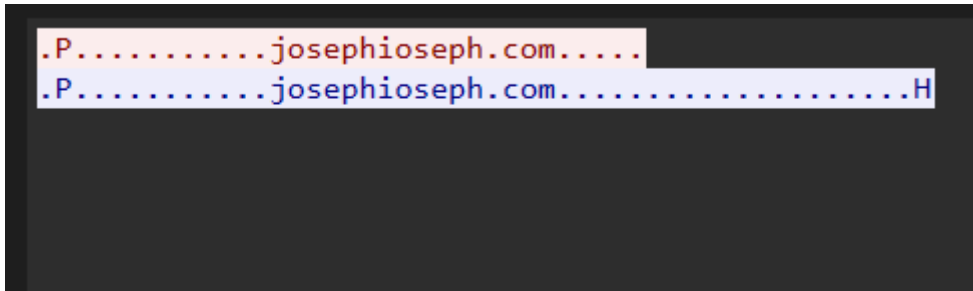
set6.pcap						
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda						
Filter: dns & smtp & tcp.port == 25						
No.	Time	Source	Destination	Protocol	Length Info	
1	0.000000	10.11.16.1	10.11.16.1	DNS	76	Standard query 0x9850 A josephioseph.com
2	1.982426	10.11.16.1	10.11.16.101	DNS	92	Standard query response 0x9850 A josephioseph.com A 192.185.16.72
6	2.345133	10.11.16.101	192.185.16.72	HTTP	370	GET /timaya/htadrills.hta HTTP/1.1
8	2.355154	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 0x0533 A josephioseph.com
11	13.344120	10.11.16.1	10.11.16.101	DNS	92	Standard query response 0x0533 A josephioseph.com A 192.185.16.72
15	13.498485	10.11.16.101	192.185.16.72	HTTP	137	GET /timaya/drills.exe HTTP/1.1
630	31.090772	10.11.16.101	10.11.16.1	DNS	91	Standard query 0xb3a A myapplicationsdownload.download
631	33.076209	10.11.16.1	10.11.16.101	DNS	187	Standard query response 0xb3a 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	33.447284	209.182.213.90	10.11.16.101	HTTP	193	HTTP/1.1 404 Not Found (text/html)
643	41.520966	10.11.16.101	10.11.16.1	DNS	91	Standard query 0xe88b A myapplicationsdownload.download
644	43.520959	10.11.16.1	10.11.16.101	DNS	187	Standard query response 0xe88b A myapplicationsdownload.download A 209.182.213.90
650	43.638729	10.11.16.101	209.182.213.90	HTTP	258	POST /animationsetup1/animation1kc/fre.php HTTP/1.0
652	43.952255	209.182.213.90	10.11.16.101	HTTP	193	HTTP/1.1 404 Not Found (text/html)
656	52.016242	10.11.16.101	10.11.16.1	DNS	91	Standard query 0x1dd A myapplicationsdownload.download
657	54.007916	10.11.16.1	10.11.16.101	DNS	187	Standard query response 0x1dd A myapplicationsdownload.download A 209.182.213.90
663	54.128707	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	193	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	124.416215	10.11.16.1	10.11.16.101	DNS	187	Standard query response 0x4359 A myapplicationsdownload.download A 209.182.213.90
680	124.600147	10.11.16.101	209.182.213.90	HTTP	231	POST /animationsetup1/animation1kc/fre.php HTTP/1.0
682	124.905703	209.182.213.90	10.11.16.101	HTTP	193	HTTP/1.1 200 OK (text/html)
686	192.970006	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	187	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	193	HTTP/1.1 200 OK (text/html)
699	263.462284	10.11.16.101	10.11.16.1	DNS	91	Standard query 0x391c A myapplicationsdownload.download
700	265.459988	10.11.16.1	10.11.16.101	DNS	187	Standard query response 0x391c 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	265.818881	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 0x6f58 A myapplicationsdownload.download
713	335.862771	10.11.16.1	10.11.16.101	DNS	187	Standard query response 0x6f58 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
724	336.219822	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 0x7d56 A myapplicationsdownload.download
727	406.536313	10.11.16.1	10.11.16.101	DNS	187	Standard query response 0x7d56 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.