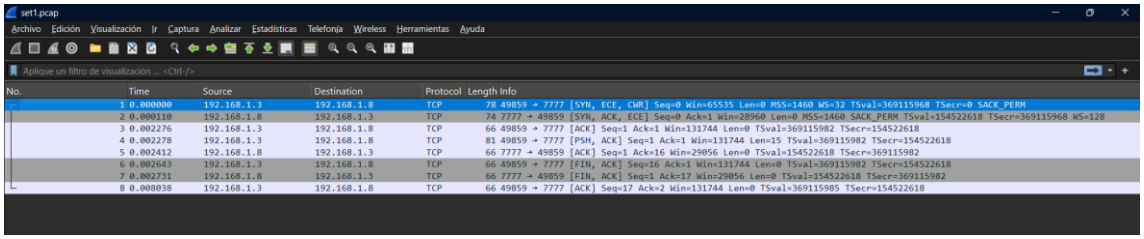
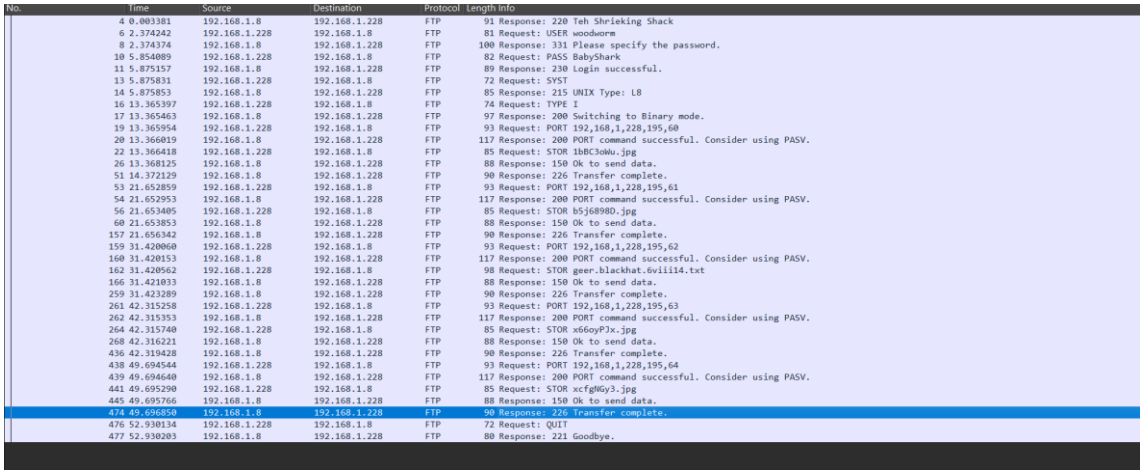
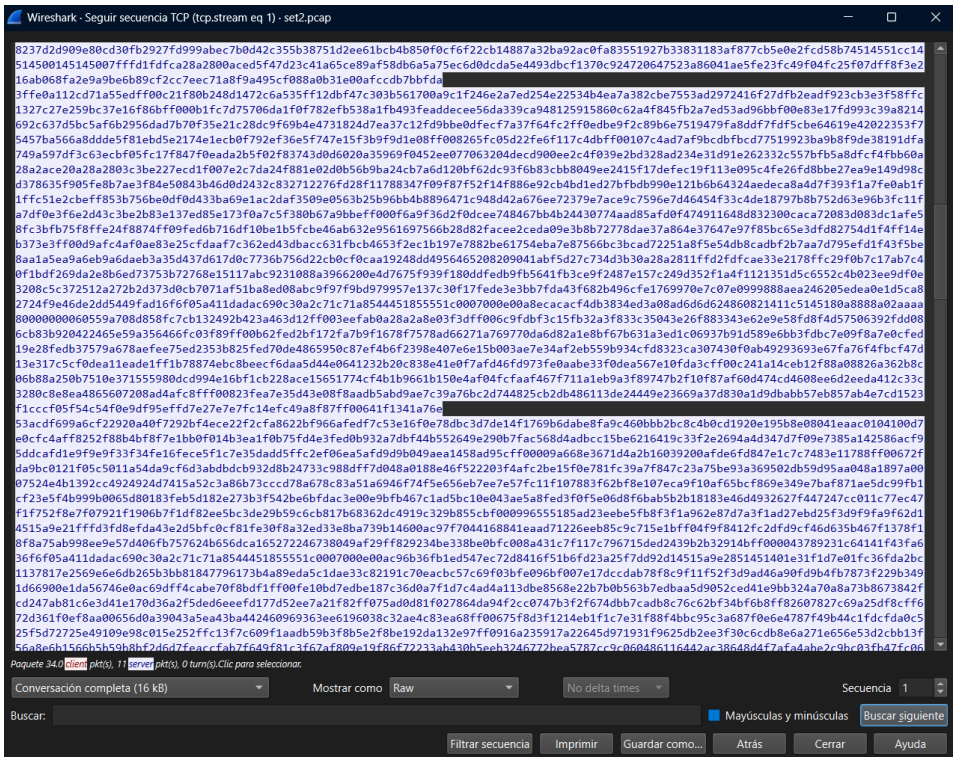
Ejercicio1



Ejercicio2

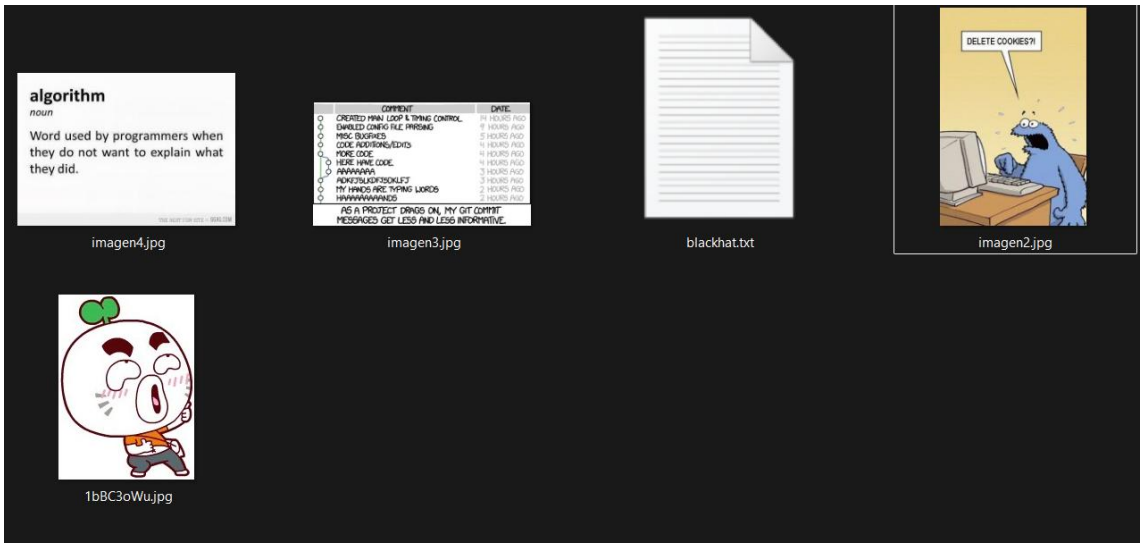


Se puede observar algunos uploads en líneas que usan el comando STOR seguido del nombre del archivo.

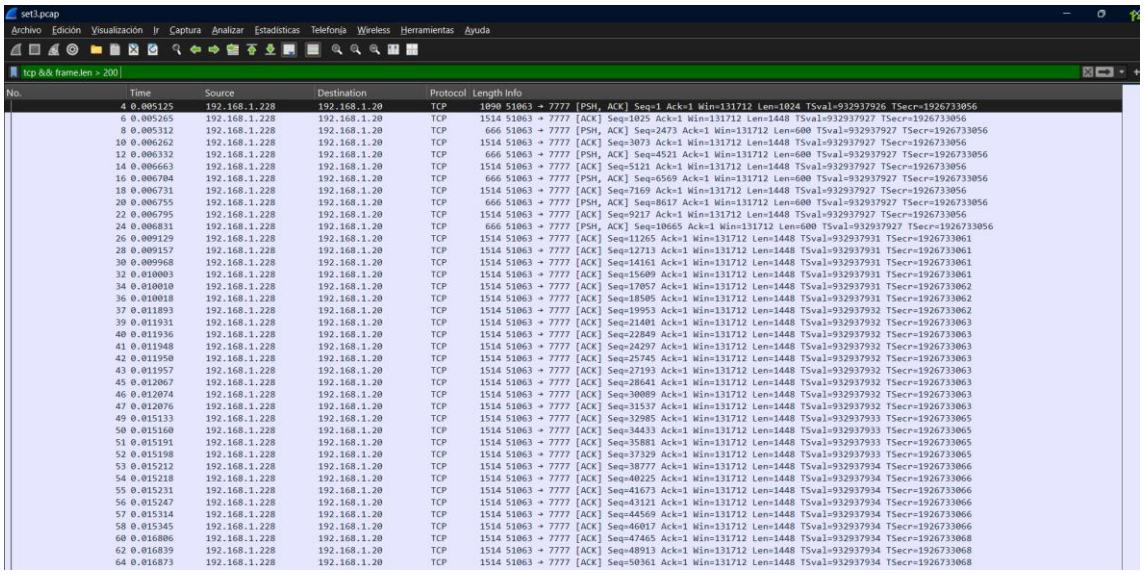


Hemos dado a seguir y que nos lo muestre en formato RAW.

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

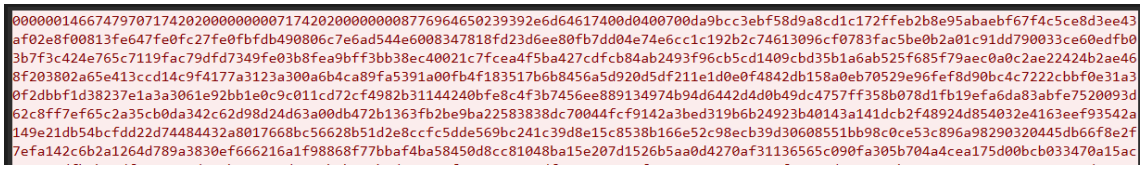


Ejercicio3

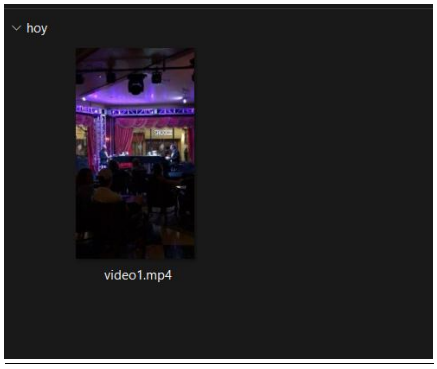


Buscamos flujos de TCP con datos y seleccionamos los flujos que tengan el termino PSH.

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).

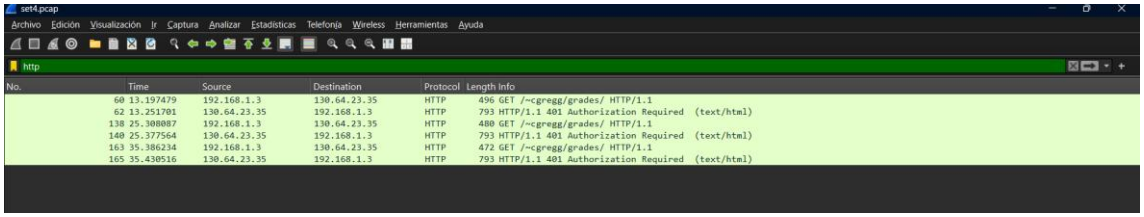


En nuestro caso tras buscarlo nuestro archivo es un mp4. Tras eso lo guardamos en nuestra carpeta.



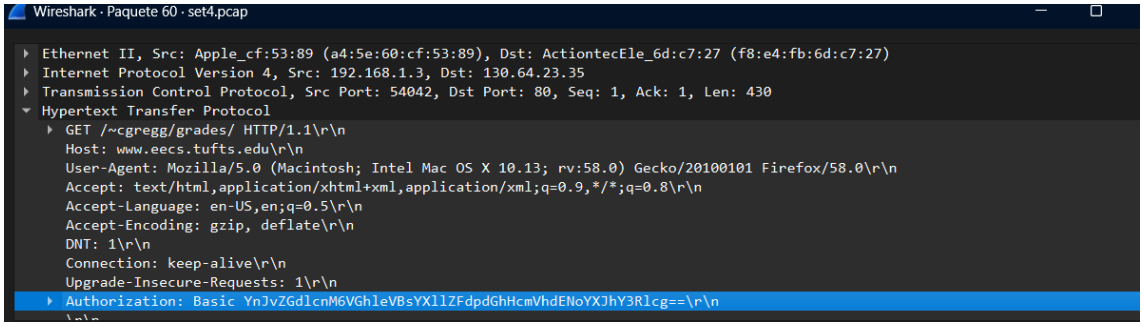
Ejercicio4

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 YnJvZGdlcnM6VGhleVBsYXllZFdpdGhHcmVhdENoYXJhY3Rlcg==

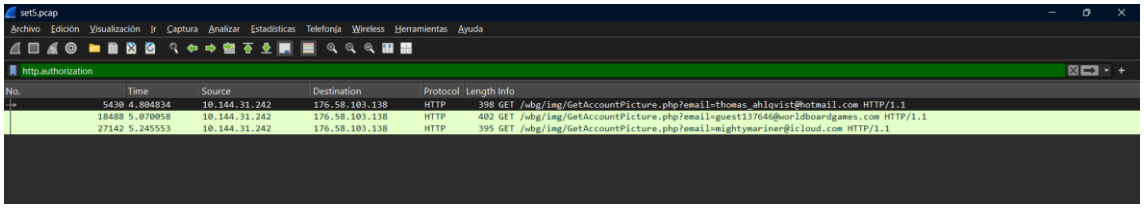
La cadena codificada en Base64 representa las credenciales utilizadas por el cliente. Tras proceder a su decodificación, el resultado obtenido fue:

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

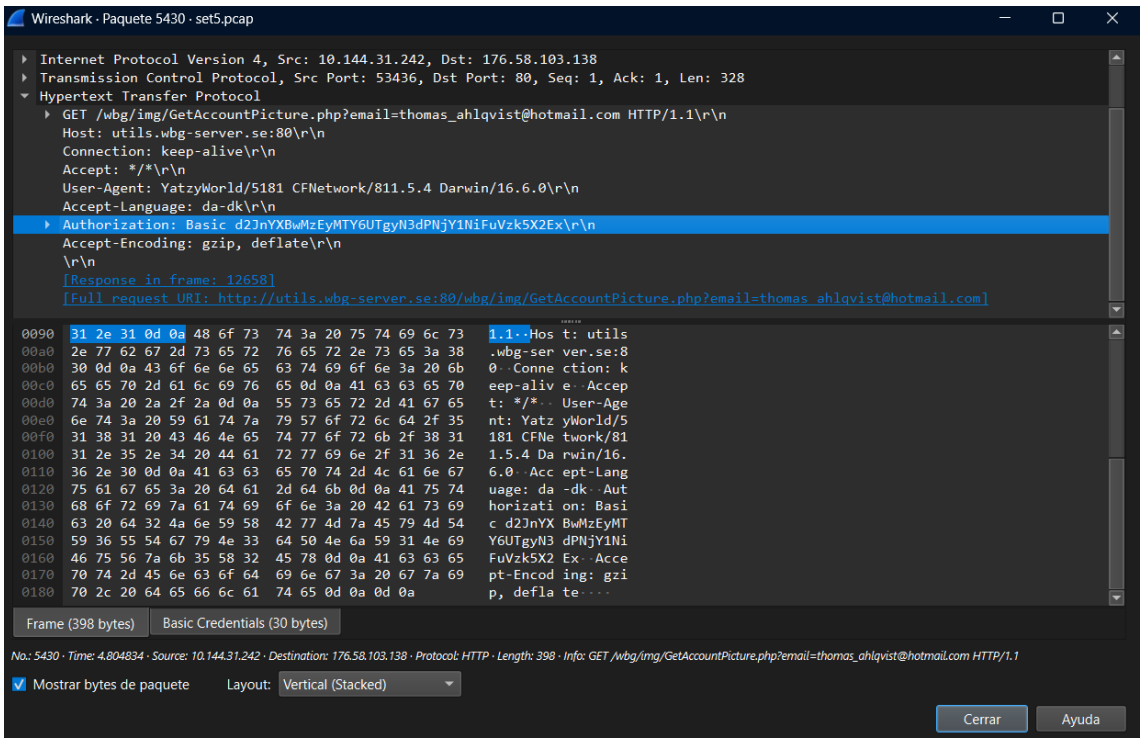
Este intercambio se realizó mediante el protocolo HTTP sin cifrar, lo cual permitió que las credenciales fueran capturadas íntegramente en texto plano dentro del tráfico interceptado.

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

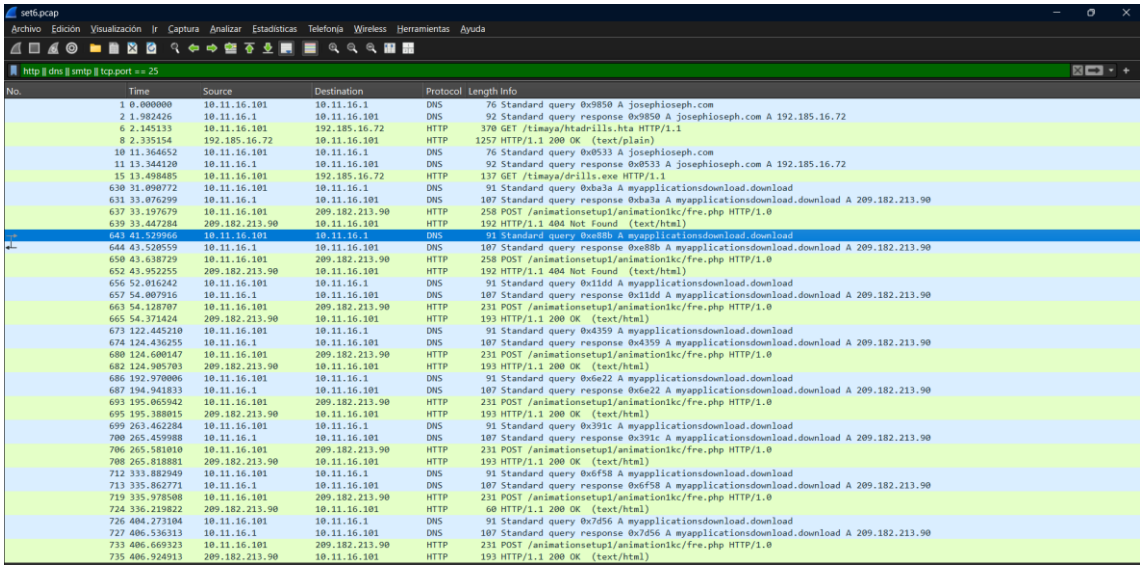
La decodificación de la cadena Base64 reveló las siguientes credenciales:

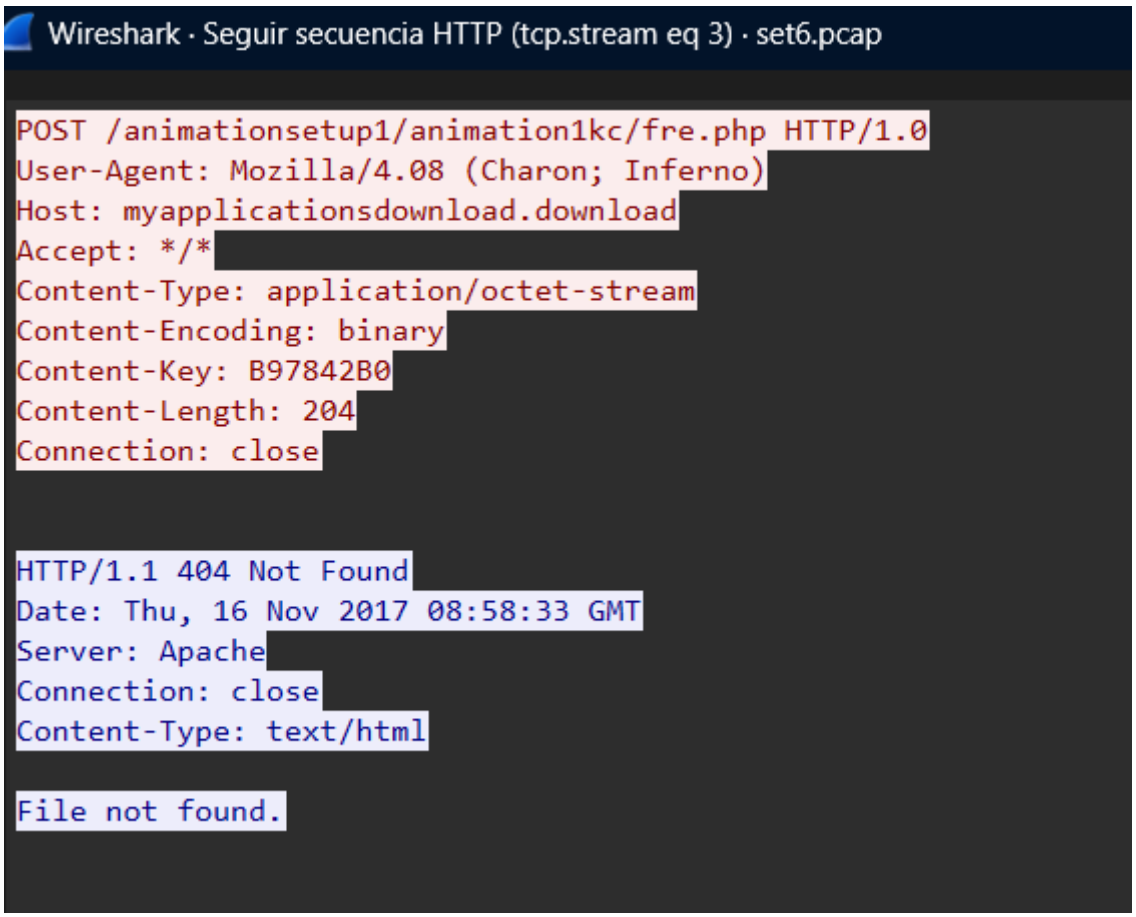
Usuario: wbgapp31216
Contraseña: Q827wO6656!nW99_a1

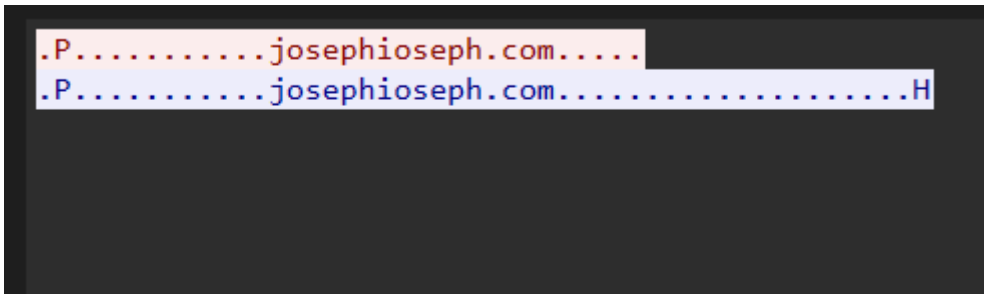
Esto confirma que la misma credencial está siendo reutilizada para múltiples accesos, un patrón común en aplicaciones que utilizan cuentas de servicio internas. Sin cifrado TLS, estas credenciales pueden ser interceptadas fácilmente y reutilizadas por un atacante.

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
http || dns || smtp || tcp.port == 25
No. Time Source Destination Protocol Length Info
1 0.000000 10.11.16.101 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 2.145133 10.11.16.101 192.185.16.72 HTTP 370 GET /timaya/htadrills.hta 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 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 0xba3a A myapplicationsdownload.download
631 33.076299 10.11.16.1 10.11.16.101 DNS 107 Standard query response 0xba3a 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 192 HTTP/1.1 404 Not Found (text/html)
643 41.529966 10.11.16.101 10.11.16.1 DNS 91 Standard query 0xe88b A myapplicationsdownload.download
644 43.520559 10.11.16.1 10.11.16.101 DNS 107 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 192 HTTP/1.1 404 Not Found (text/html)
656 52.016242 10.11.16.101 10.11.16.1 DNS 91 Standard query 0x11dd A myapplicationsdownload.download
657 54.007916 10.11.16.1 10.11.16.101 DNS 107 Standard query response 0x11dd 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
674 124.436255 10.11.16.1 10.11.16.101 DNS 107 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 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 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 107 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 107 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 107 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.