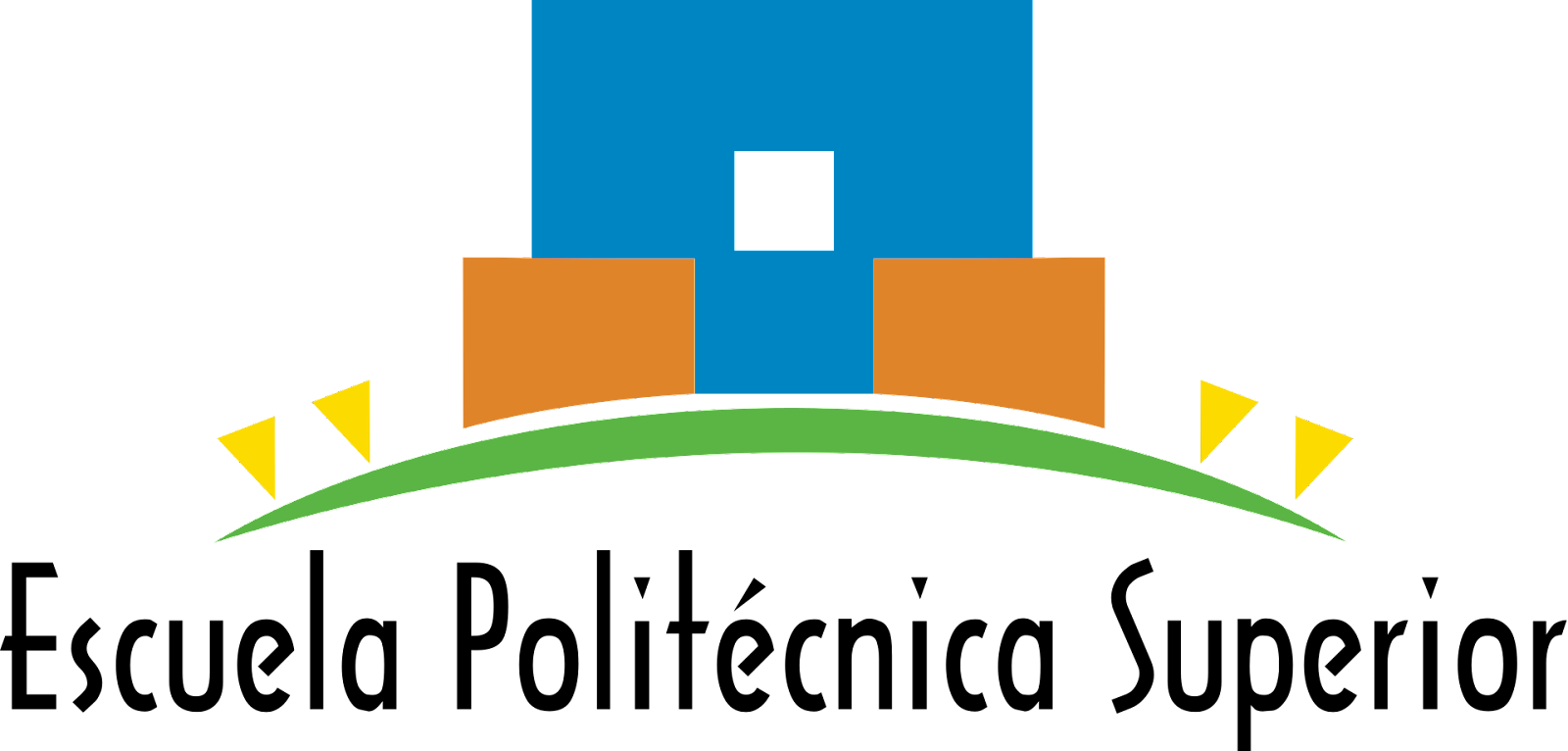
**UNIVERSIDAD AUTÓNOMA DE MADRID**



**Prácticas Ciberseguridad**

**Práctica 2 - Auditoria e Informática Forense**

Miguel Ibáñez González

Oscar Navalon Navarro

09/04/2024

Grupo: 2462

Pareja: 05

## **ÍNDICE**

[1. Clonado 3](#_1a0lu4avpu2)

[2. Obtención de información volátil 3](#_a7cxec4yphbq)

[2.1 RAM: 3](#_k2g911uvjksw)

[2.2. Conexiones de red: 3](#_8tuyarcbq8ez)

[3. Artefactos forenses 4](#_33f3nas88m5)

[3.1 Actividad de Usuario 4](#_q9cccu9gxu41)

[3.2 Archivos borrados 5](#_oapiq2j9gdtt)

[3.3 Contraseñas 6](#_oybi8q5220eh)

[3.4 Archivos que no coinciden 6](#_9imd5b45q8oj)

[3.5 Shadow Copy 7](#_5u0msi8r56g)

[4. Análisis Forense Server\_Disk1.e01 8](#_ud4hzsq8zy56)

[4.1 Bulk extractor 8](#_tc34e970rdh8)

[4.2 OSForensics 10](#_qeabyhhrf0vf)

[5. Responder Preguntas 16](#_hgcfr4nl9zml)

[6.Reflexión 16](#_khbrlv1tbey0)

## 

## 

## 

## 

## 

## 

## 

## **1. Clonado**

1. Instalación de Kali Linux en VMware para realizar la copia dentro de la máquina virtual.
2. Una vez obtenida la imagen. Hemos realizado una clonado bit a bit con el comando dc3dd if=Server\_Disk1.e01 hash=sha256 of=Copia.e01
3. Una vez realizada esta copia se debe asegurar la integridad completa de los datos de la copia. Esto lo hacemos con una simple asignación del hash md5 con el comando: md5sum <archivo.e01>.
4. Comprobamos que el hash asignado a cada una de las copias coinciden, de esta manera podemos asegurar que no ha habido cambios a nivel de bit en la copia.
5. Una vez realizada la copia, la sacamos a Windows para realizar un análisis forense con OSForensics.

## **2. Obtención de información volátil**

## **2.1 RAM:**

Al ser una imagen post-mortem, no es posible obtener un volcado de la memoria ram.

## **2.2. Conexiones de red:**

Con ayuda de Bulk-extractor vamos a ver las conexiones de red que más tarde analizaremos.

## **3. Artefactos forenses**

## **3.1 Actividad de Usuario**

El artefacto forense Actividad de usuario de

OSForensics se utiliza para investigar la

actividad del usuario en un sistema. Los

resultados de este artefacto nos pueden

ayudar a encontrar datos útiles para un

análisis forense, algunos de estos resultados

son:

1. Historial de navegación: muestra los sitios web visitados por un usuario, las fechas y horas de acceso, así como las cookies y otros datos relacionados con la actividad en línea.
2. Historial de archivos: rastrear los archivos abiertos, modificados o eliminados por un usuario.
3. Actividad de aplicaciones: muestra la actividad de las aplicaciones utilizadas por un usuario, incluyendo los programas abiertos, cerrados, instalados o desinstalados.
4. Actividad de correo electrónico: proporciona detalles sobre los correos electrónicos enviados, recibidos o eliminados por un usuario.
5. Historial de inicio de sesión: muestra los intentos de inicio de sesión en el sistema, incluyendo información sobre quién intentó acceder al sistema, cuándo y si tuvieron éxito o no.
6. Actividad de red: muestra la actividad de red, incluyendo conexiones entrantes y salientes, lo que puede ayudar a determinar si el usuario ha estado comunicándose con otros sistemas o servicios en línea.

## **3.2 Archivos borrados**

Este artefacto forense sirve para obtener información

sobre los archivos eliminados, sus nombres, rutas,

tamaños, fechas de eliminación, su contenido y

metadatos asociados. Algunos ejemplos:

1. Nombre de archivo: Puede mostrar los nombres de

los archivos que han sido eliminados.

1. Ruta de archivo: Además del nombre del archivo,

OSForensics puede mostrar la ruta completa del

archivo en el sistema de archivos.

1. Tamaño del archivo: Puede mostrar el tamaño de

los archivos borrados.

1. Fecha y hora de eliminación: La herramienta puede

recuperar la fecha y hora en que se eliminó cada

archivo. Esto puede ayudar a establecer cuándo se

realizaron las eliminaciones y si coinciden con

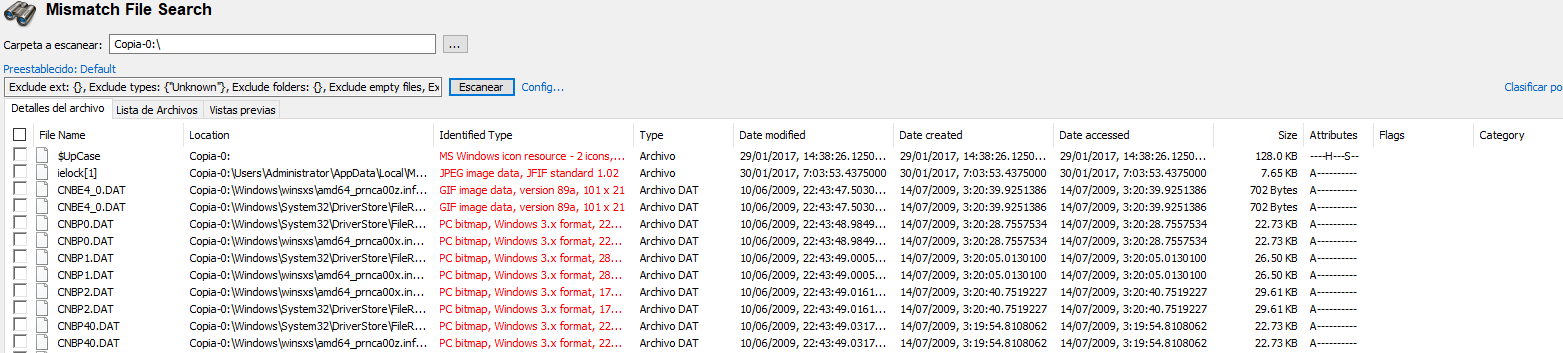
eventos relevantes en la investigación.

## **3.3 Contraseñas**

El artefacto forense se centra en recuperar, analizar y entender las contraseñas utilizadas en un sistema informático. Este artefacto se puede usar para:

1. Identificar patrones de seguridad débiles o fuertes: analizar las contraseñas puede revelar si los usuarios han utilizado contraseñas fuertes o débiles.
2. Acceso a cuentas y datos protegidos: el análisis de contraseñas puede ayudar a acceder a cuentas protegidas, esto puede ser muy importante en una investigación forense.
3. Reconstruir actividades del usuario: las contraseñas pueden proporcionar pistas sobre la actividad del usuario, como la frecuencia con la que cambian las contraseñas, si comparten contraseñas entre cuentas, y si utilizan contraseñas comunes o específicas en diferentes servicios.
4. Identificar posibles amenazas internas: Puede ayudar a identificar posibles amenazas internas, como el uso indebido de privilegios de usuario, la compartición de contraseñas entre empleados o el acceso no autorizado a datos sensibles.

## **3.4 Archivos que no coinciden**



Los "archivos que no coinciden" son archivos duplicados o versiones diferentes del mismo archivo encontrados en un sistema o dispositivo. Este artefacto forense puede ser útil por varias razones:

1. Identificación de duplicados: ayuda a identificar archivos duplicados en un sistema.
2. Determinación de versiones anteriores o modificadas: ayuda a encontrar múltiples versiones de un mismo archivo.
3. Reconstrucción de actividades del usuario: rastrea la actividad del usuario.
4. Identificación de posibles archivos ocultos o cifrados: descubre archivos ocultos o cifrados.

## **3.5 Shadow Copy**

Shadow Copy es una característica de los sistemas operativos Windows que permite realizar copias instantáneas de los datos almacenados en un volumen en un momento específico en el tiempo. La función de Shadow Copy tiene varios usos:

1. Recuperación de datos: permite la recuperación de archivos y carpetas que hayan sido eliminados o modificados accidentalmente.
2. Copias de seguridad sin interrupciones: puede utilizarse para realizar copias de seguridad de archivos abiertos y en uso sin detener los servicios o aplicaciones que los utilizan.
3. Análisis forense: puede examinar las instantáneas para analizar el estado del sistema en un momento específico en el pasado.
4. Auditoría y cumplimiento: puede utilizarse para realizar auditorías de cambios en archivos y carpetas.
5. Protección contra ransomware: las copias instantáneas de volumen pueden proporcionar una capa adicional de protección contra el ransomware.

## 

## **4. Análisis Forense Server\_Disk1.e01**

## **4.1 Bulk extractor**

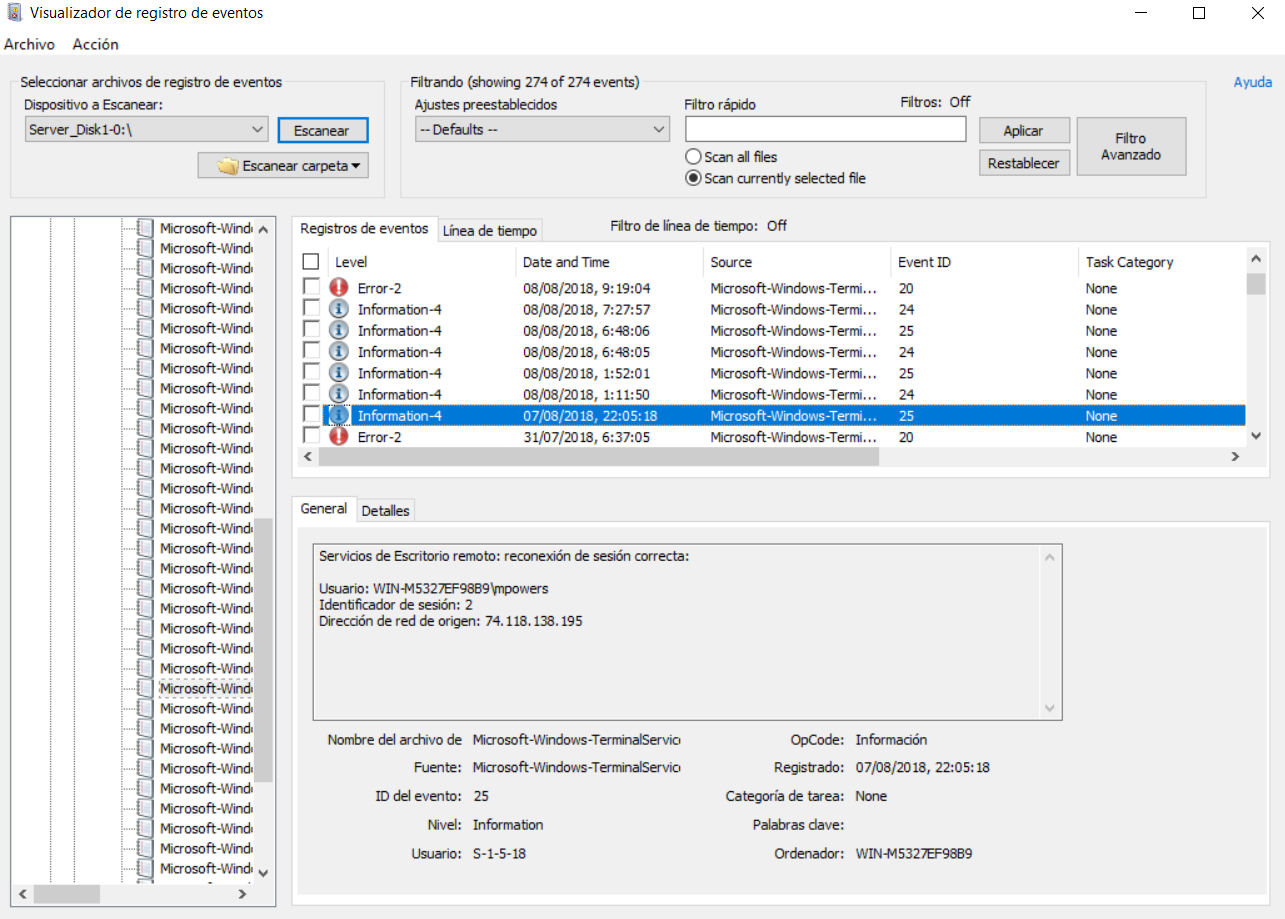
Comando: bulk\_extractor -o <folder> <image>:

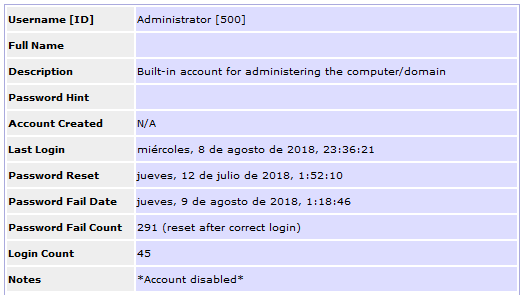
* Incunplimientos de las politica de uso de no descargar, instalar y ejecutar programas no destinados al desempeño de las tareas asignadas a los empleados/as:
  + **domain.txt:** 
    - www.cooctdlfast.com lgame.exe[http://www.cooctdlfast.com/download.php?\220\002](http://www.cooctdlfast.com/download.php?%5C220%5C002)
    - gamestoredownload.download \370;0\021\335-\254aThttp://gamestoredownload.download/ws-word2017pa.d
    - www.wikitweak.com ular\000\001\000,\001<http://www.wikitweak.com/downloads/pp.ex>
    - gameplaylabs.com .com\000\001\0005\001<http://gameplaylabs.com/download/?dl=cr>
    - download.pplive.com \000\000\000\000\000\000\000\000\000<http://download.pplive.com/pptv(pplive)_fo>
  + **url\_facebook-address.txt:**
    - ://[www.facebook.com/dasun.tharanga.142](http://www.facebook.com/dasun.tharanga.142)
  + **url\_histogram.txt:**
    - <https://www.drwebhk.com/en/virus_techinfo/Trojan.DownLoader9.50268.html>
    - http://apps\_holdem-poker.66ghz.com
    - http://apps\_holdem-poker.66ghz.com/privacypolicy/
    - [http://www.LuckyAcePoker.com/install.images4us.com/setups/pacificpoker.com/affiliatenetworks.aspcasinonet\_](http://www.luckyacepoker.com/install.images4us.com/setups/pacificpoker.com/affiliatenetworks.aspcasinonet_)
    - [http://datingfavorite.nethttp://datingvirtual.netS1](about:blank)
    - <http://quierovivirsano.com.co/wp-admin/chulo/quote/index.html>
    - <http://www.kjdhendieldiouyu.com/cfdata.ima?ccode=%s&cfdatacc=%s&gmt=%dasdfjkluiop.comsweepstakess.comhotxxxtv.comfreeporntoday.netfreepornnow.netporn1.orgvirgins>
    - <https://www.drwebhk.com/en/virus_techinfo/Trojan.DownLoader9.50268.html>
  + **url.txt:**
    - https://www.drwebhk.com/en/virus\_techinfo/Trojan.DownLoader9.50268.html of a <a href=\134"https://www.drwebhk.com/en/virus\_techinfo/Trojan.DownLoader9.50268.html\134">Trojan softwa
  + **url\_searches.txt**
    - search?q=download+fortnite
    - search?q=download+youtube
    - search?q=download+youtube+videos

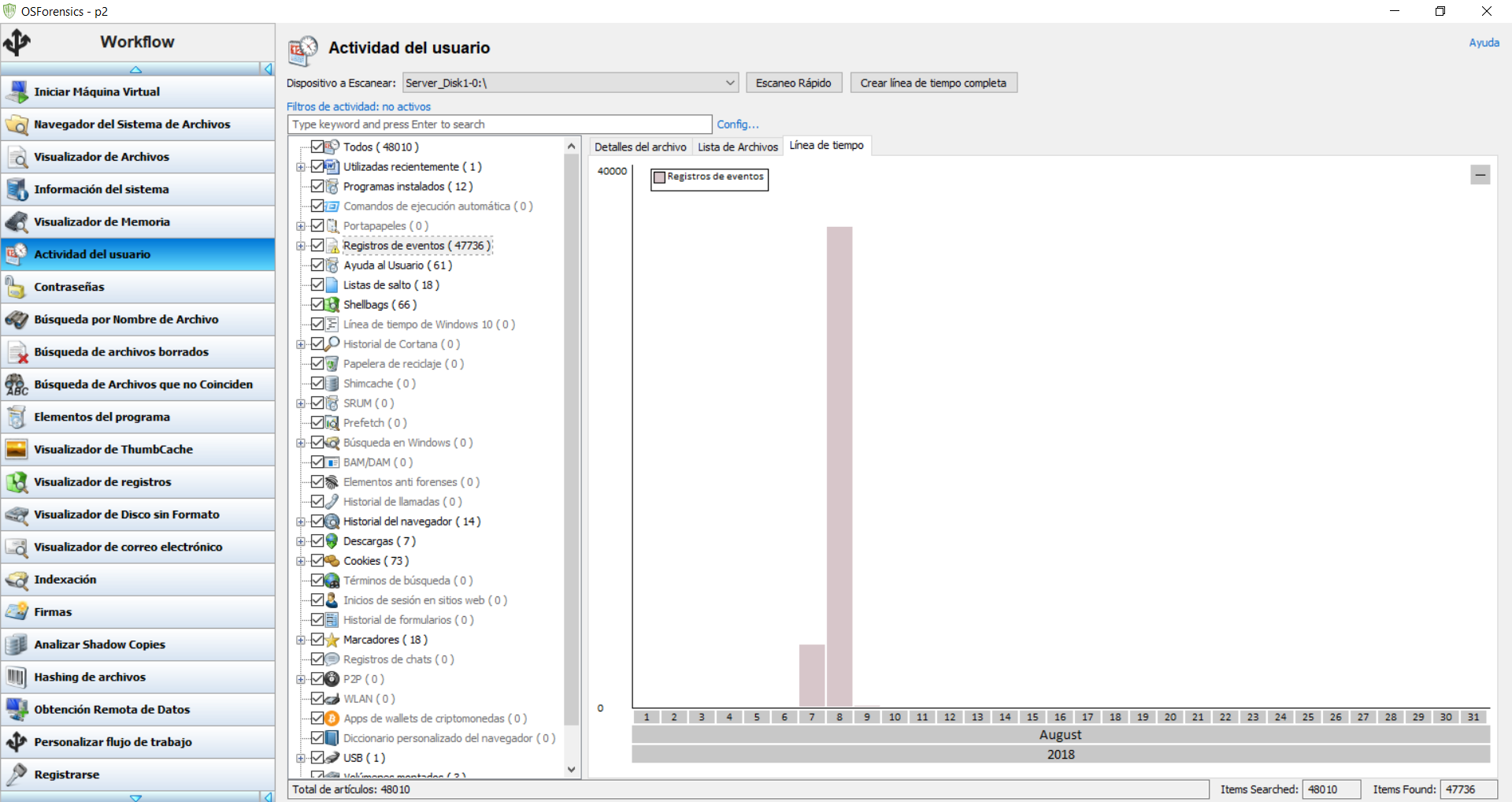
Todas las urls mencionadas anteriormente y encontradas en los ficheros que devuelve el comando comando bulk\_extractor -o, incumplen las políticas de la empresa ya que esas urls no pueden ser utilizadas en ningún caso para trabajar.

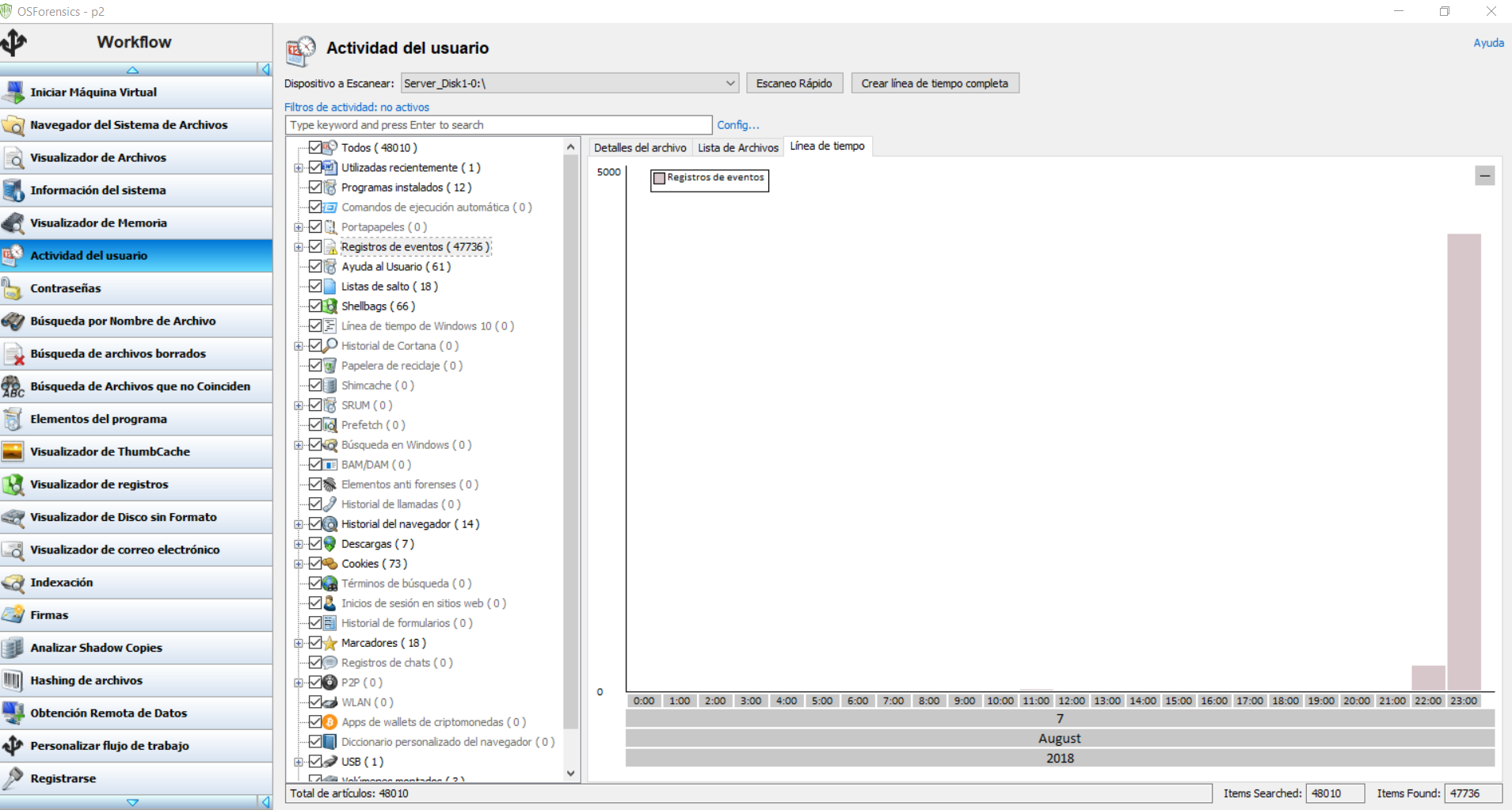
## 

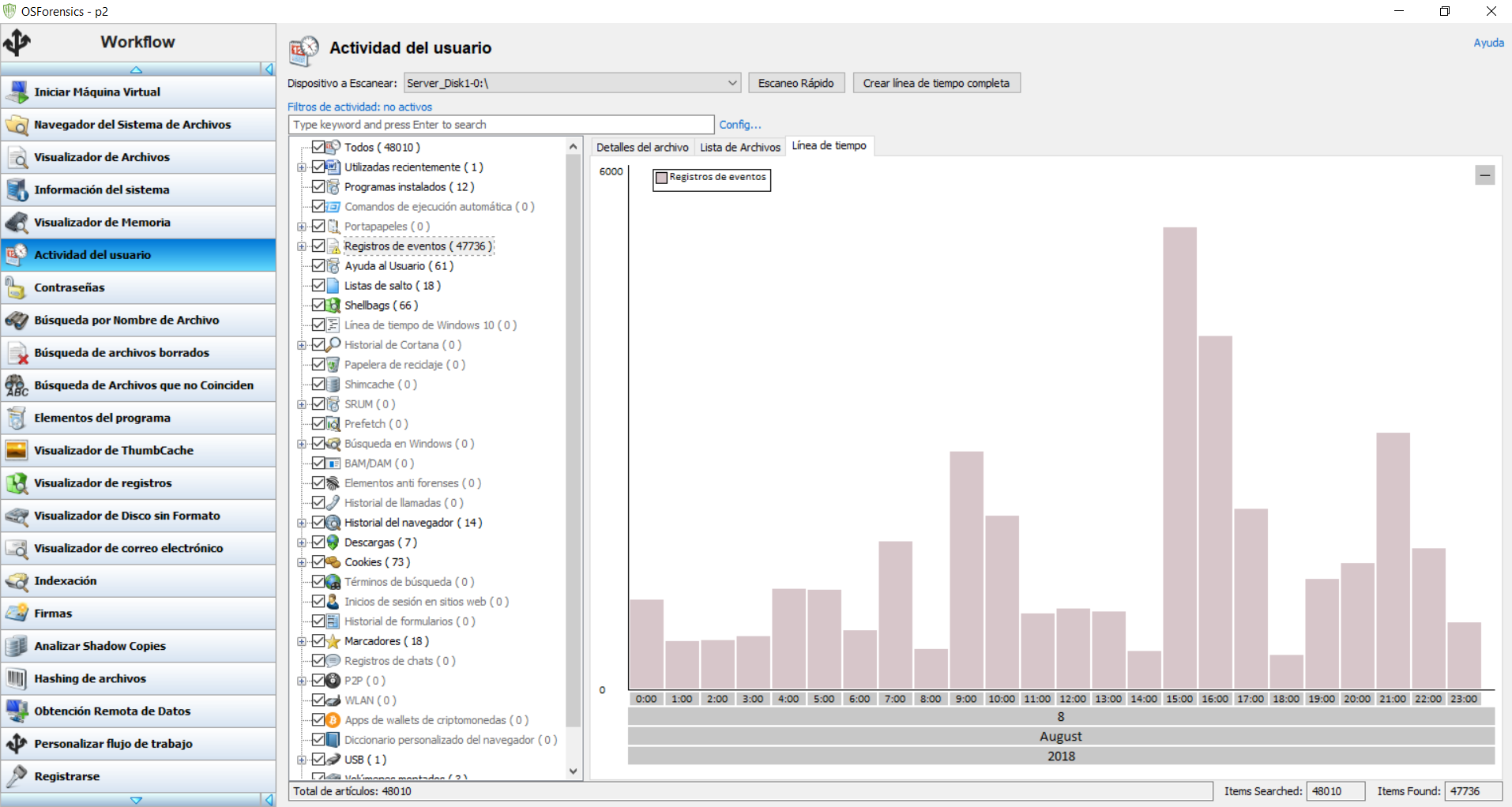
## **4.2 OSForensics**

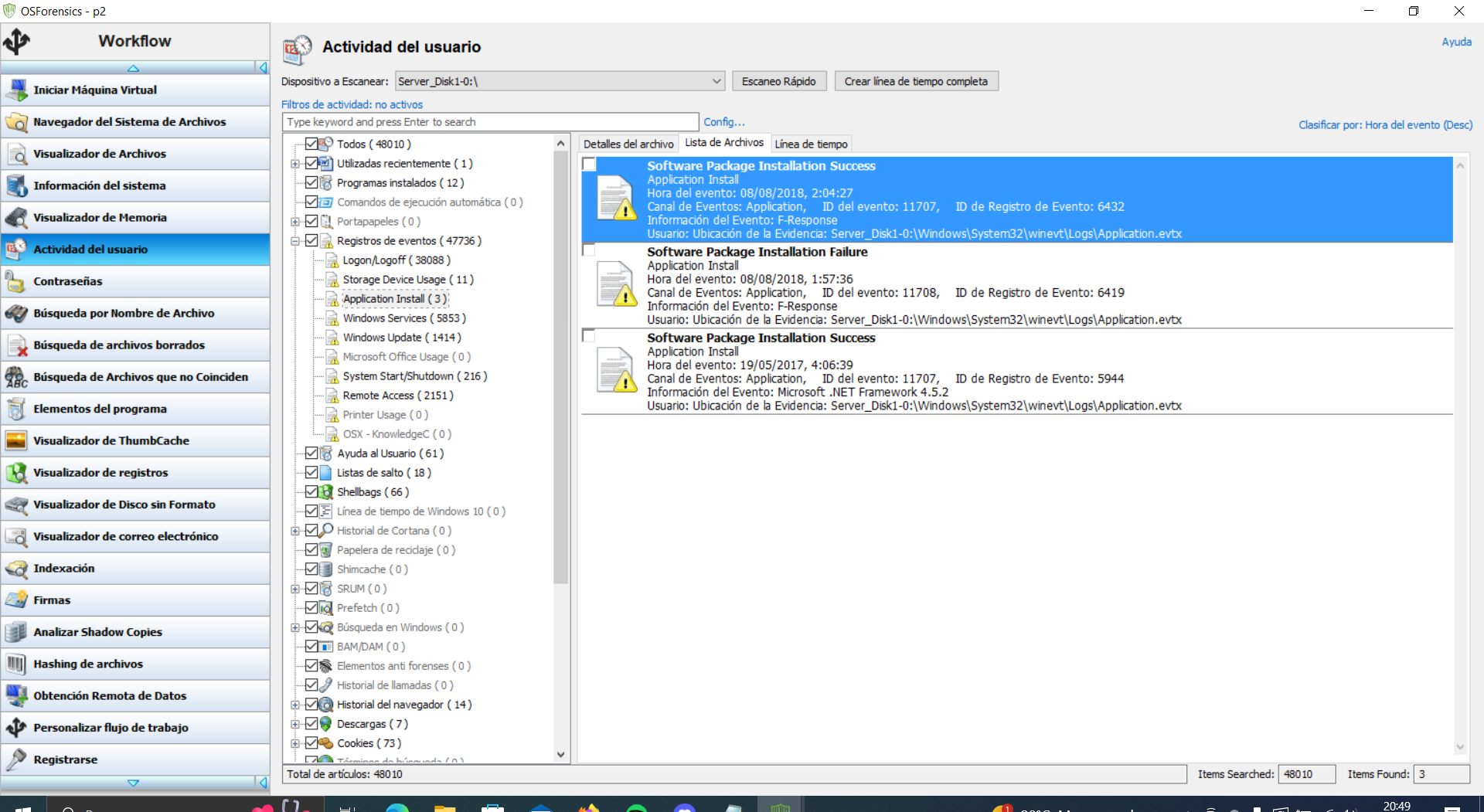
Como podemos ver en el visualizador del registro de eventos, el 7 de agosto hay muchos intentos de inicio de sesión, lo cual parece un ataque de fuerza bruta sobre la máquina de la víctima. Todo comienza a las 22:05 donde a través de la dirección de red 74.118.138.195 se conecta en remoto desde la cuenta de mpowers.

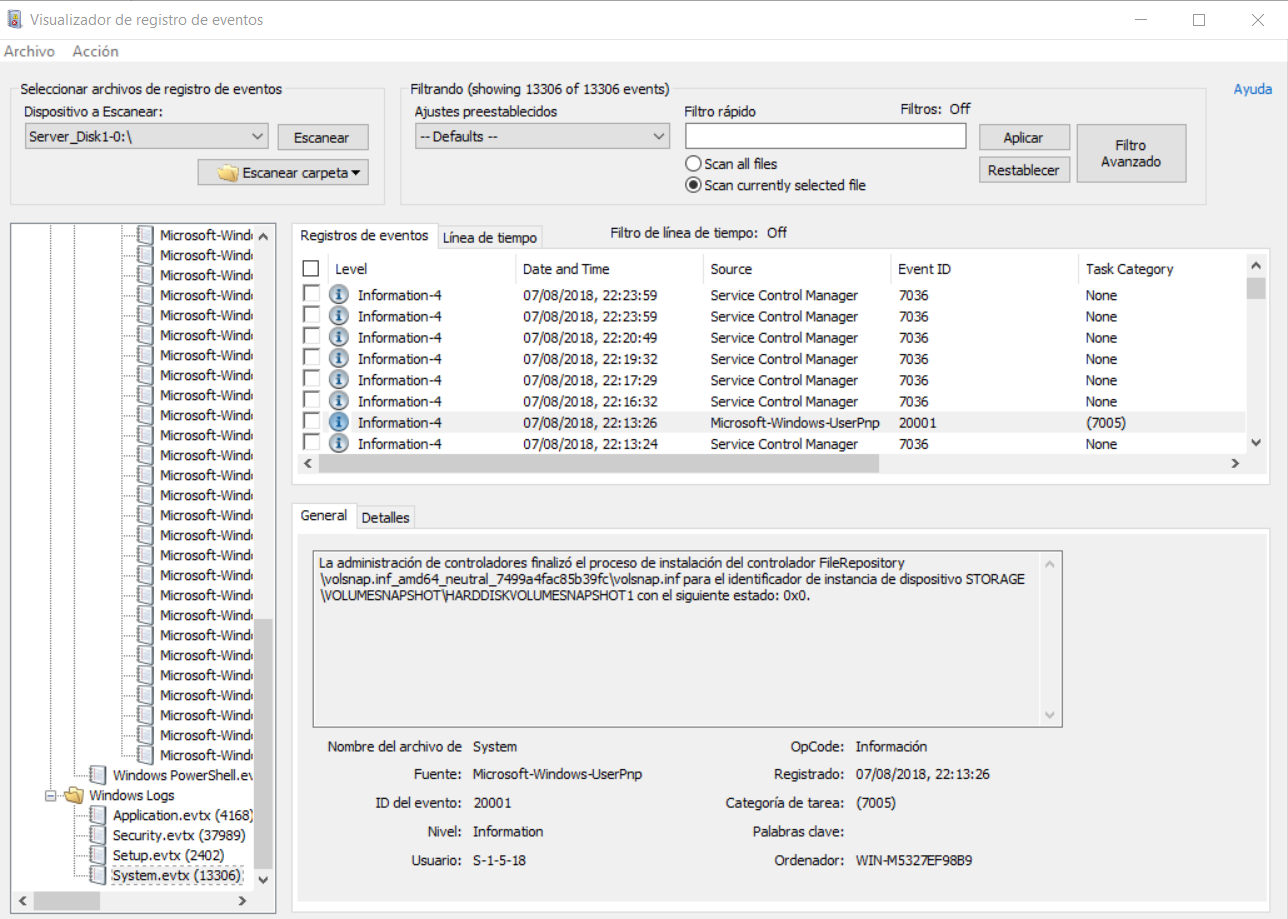
En la información del sistema podemos ver que se ha incrementado mucho el contador de logfails del 7 de ago al 9 ago

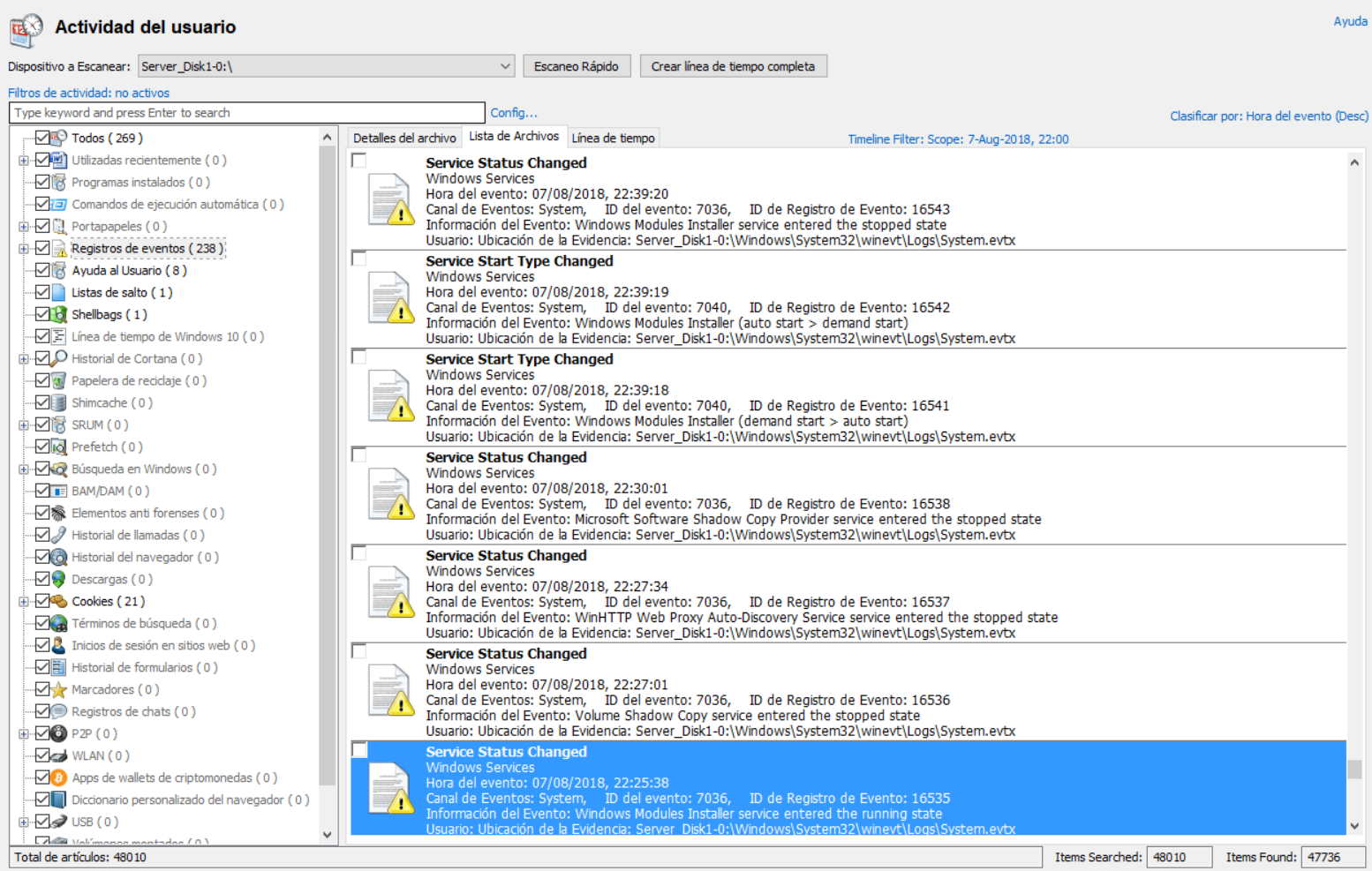
Podemos ver los días de la actividad del usuario, 7 y 8 de agosto:  


Y las horas de los dos días:  


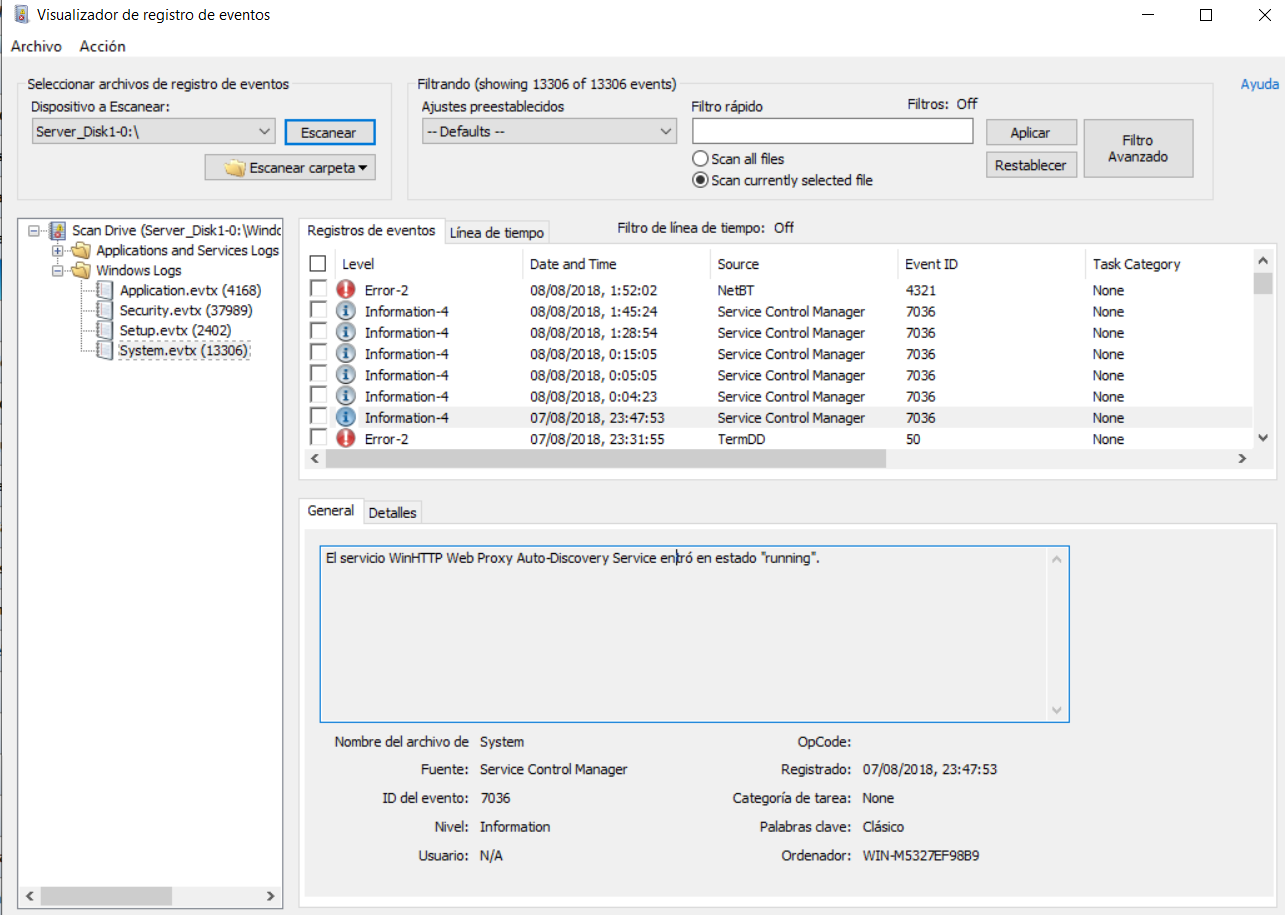


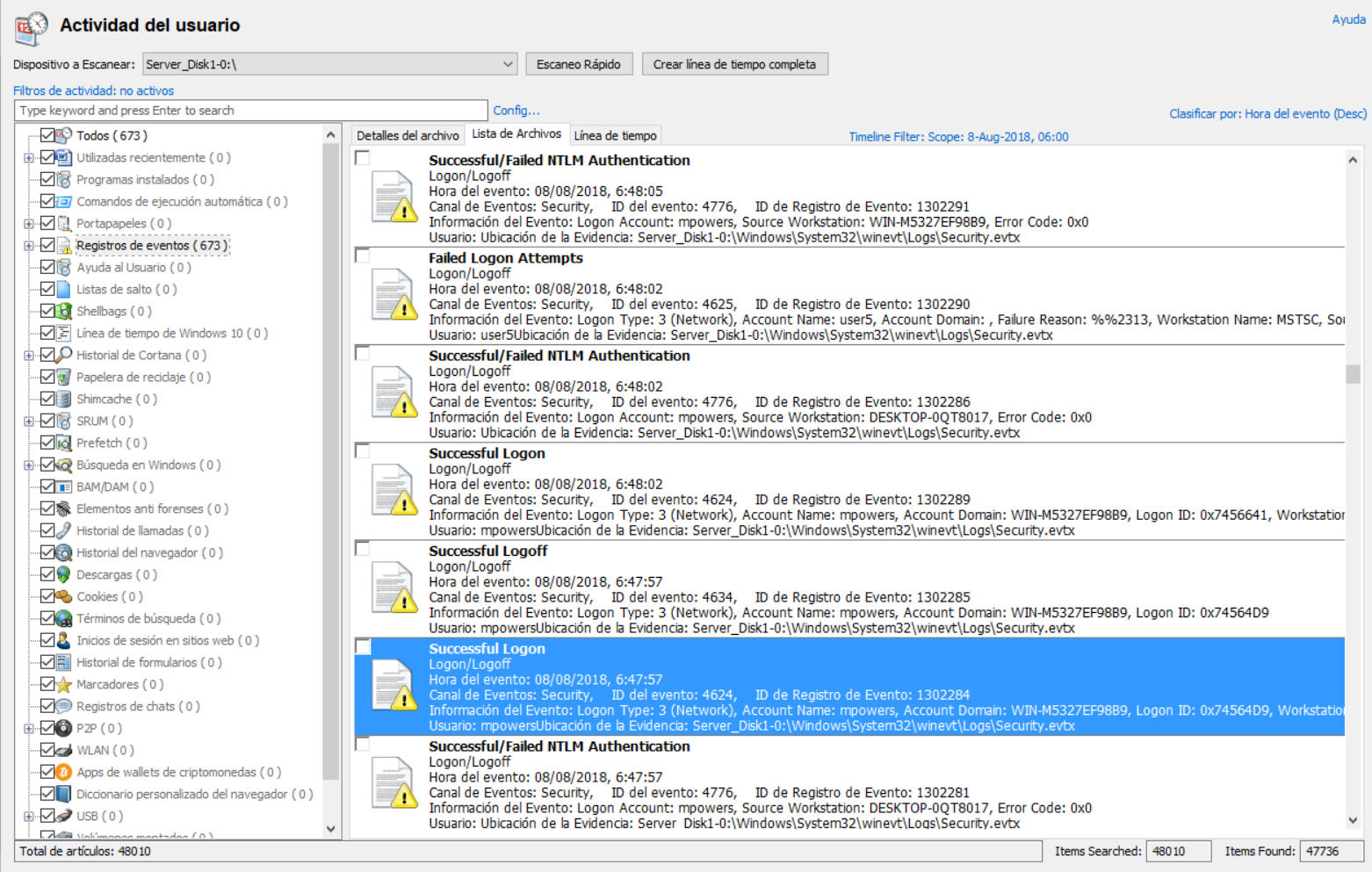
Instalaciones de los paquetes durante las horas de la madrugada de 8 de agosto:

Podemos observar cómo instala un FileRepository desde una snapshot de un disco duro:

Tras esta instalación se empiezan a cambiar los status de determinados sistemas de windows como el errorReporting o la copia automática del shadow. Todo parece indicar que están preparando la máquina para un ataque:

Es a partir de las 22:42 que empiezan los intentos de inicio de sesión, lo cual parece un ataque de fuerza bruta contra el inicio de sesión de la máquina.



El ataque continúa hasta las 6:47:57, donde se consigue hacer logon y logout seguidamente con la cuenta de powers

El atacante consigue escalar de privilegios a través de la cuenta mpowers, a las 6:48:05 se asignaron privilegios especiales a un nuevo inicio de sesión.

Sujeto:

Id. de seguridad: S-1-5-21-1223297778-3299746493-1462173606-1000

Nombre de cuenta: mpowers

Dominio de cuenta: WIN-M5327EF98B9

Id. de inicio de sesión: 0x74564D9

Privilegios: SeSecurityPrivilege

SeBackupPrivilege

SeRestorePrivilege

SeTakeOwnershipPrivilege

SeDebugPrivilege

SeSystemEnvironmentPrivilege

SeLoadDriverPrivilege

SeImpersonatePrivilege

A las 7:27:57 se desconecta el remote desktop otra vez:

Servicios de Escritorio remoto: sesión desconectada:

Usuario: WIN-M5327EF98B9\mpowers

Identificador de sesión: 2

Dirección de red de origen:

A las 7:37 El servicio WinHTTP Web Proxy Auto-Discovery Service entró en estado "stopped" Y a las 7:56:15 vuelve a conectarse desde otra ip.

Tipo de inicio de sesión: 3

Nuevo inicio de sesión:

Id. de seguridad: S-1-5-7

Nombre de cuenta: ANONYMOUS LOGON

Dominio de cuenta: WIN-M5327EF98B9

Id. de inicio de sesión: 0x74C7B06

GUID de inicio de sesión: {00000000-0000-0000-0000-000000000000}

Información de proceso:

Id. de proceso: 0x0

Nombre de proceso: -

Información de red:

Nombre de estación de trabajo:

Dirección de red de origen: 148.153.25.26

Puerto de origen: 63882

Información de autenticación detallada:

Proceso de inicio de sesión: NtLmSsp

Paquete de autenticación: NTLM

Servicios transitados: -

Nombre de paquete (solo NTLM): NTLM V1

Longitud de clave: 0

Se hacen más inicios de sesion con otras ips: 35.154.234.199, 186.155.112.4

## **5. Responder Preguntas**

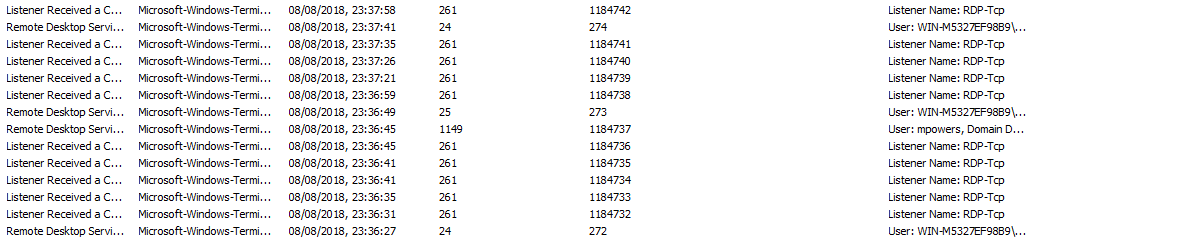
¿Se han utilizado programas no permitidos por las políticas de la empresa?

Si que se han utilizado programas no permitidos, con el comando bulk\_extractor -o <folder> <image>, en la sección 4.1, se pueden ver todas las descargas instalaciones y ejecuciones de programas que no pueden ser usados por las políticas de privacidad de la empresa.

¿Se han realizado conexiones remotas fuera del horario laboral por parte de la empresa?

Si se han realizado conexiones fuera del horario, como se señala en la sección 4.2, el 8 de agosto se realizan muchas conexiones fuera del horario.

Todas estas conexiones se pueden ver en el OSForensics, con el artefacto forense actividad de usuario, en registro de eventos->accesos remotos, aquí hay alguno ejemplos:



¿Ha incumplido el empleado las normas internas de la empresa?

Si ha incumplido las normas de la empresa, como se ha mencionado anteriormente el usuario mpowers se conecta fuera del horario y realiza búsquedas en páginas no destinadas a uso laboral..

## **6.Reflexión**

Durante el análisis forense realizado se han podido identificar varias actividades que indican posibles violaciones de las políticas de la empresa por parte de los empleados. Como el uso de programas no permitidos y las conexiones remotas fuera del horario laboral, lo cual puede representar un riesgo significativo para la seguridad y la integridad de los sistemas de la empresa, así como para la confidencialidad de la información. Al realizar este analisis nos encontramos con una serie de problemas:

Al principio uno de los problemas que tuvimos fue el espacio necesario para realizar un buen analista del disco, ya que por ejemplo el comando scalpel, devuelve una salida de 100GB, por lo que aprendimos que para realizar un análisis forense hay que tener espacio suficiente, para solucionarlo creamos una carpeta compartida dentro de la máquina virtual de kali linux.

Otra de los problemas que tuvimos es el aprender a donde mirar dentro de las herramientas que se nos proporcionan para realizar el análisis, ya que por ejemplo build extractor devuelve muchos ficheros con información, entre todos esos ficheros filtramos los importantes, donde podemos encontrar indicios de de incumplimiento de alguna política, pero los ficheros eran muy grandes por lo que usamos comandos como grep, para buscar palabras que nos ayuden a encontrar estos incumplimientos, como puede ser la palabra download para encontrar las descargas realizadas por los trabajadores de la empresa.