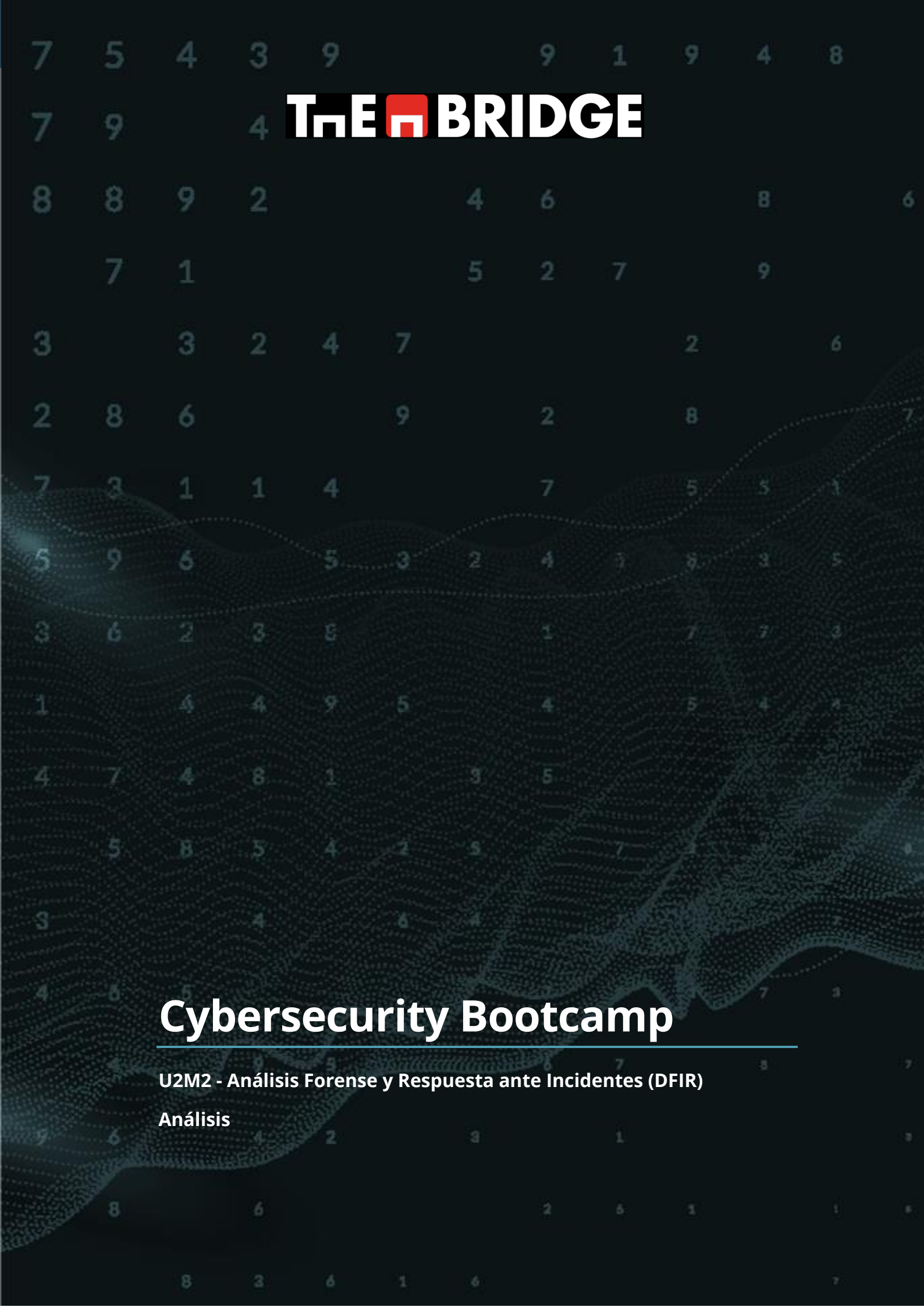


Cybersecurity Bootcamp

U2M2 - Análisis Forense y Respuesta ante Incidentes (DFIR)

Análisis

Índice

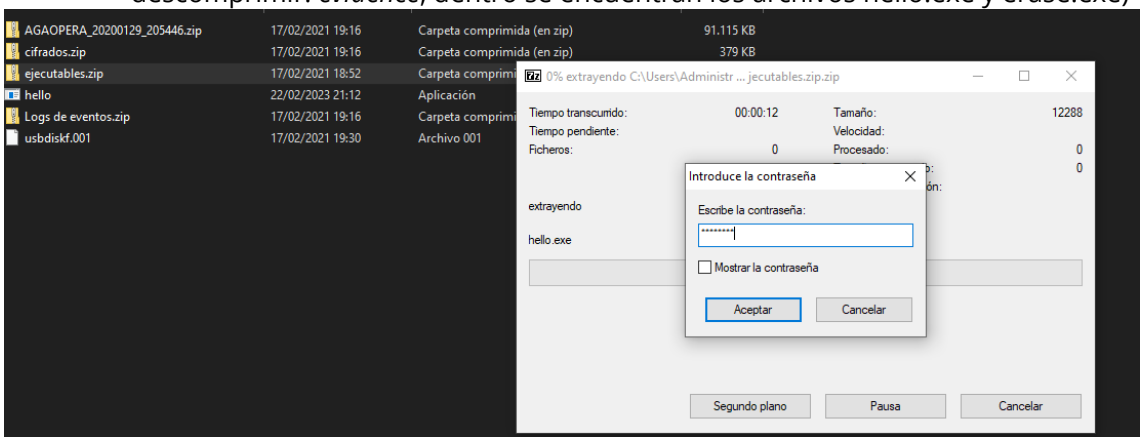
Análisis

Nota: para la realización de los ejercicios que se indican a continuación es necesario disponer de la máquina virtual "Windows 10 Forense.ova" compartida en el repositorio de máquinas virtuales de classroom.

Recuerda que puedes adaptar el tamaño de recursos de la memoria RAM del host que quieres asignarle a la máquina (6GB por defecto).

3.1. Extrae las firmas hash de los siguientes ficheros

- Ficheros necesarios para el ejercicio: ejecutables.zip (contraseña para descomprimir: *evidence*, dentro se encuentran los archivos hello.exe y erase.exe)



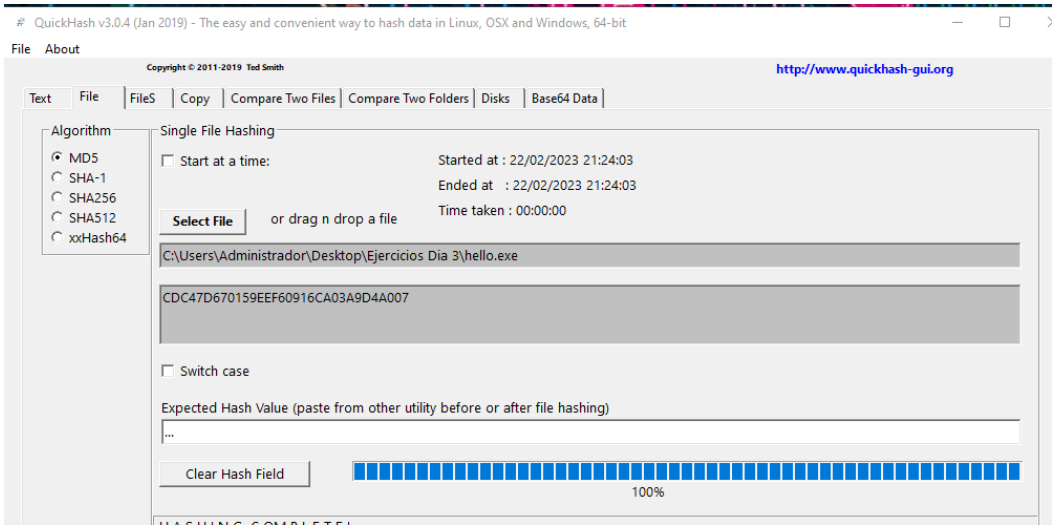
- Primero, ejecuta ambos ficheros (no hay riesgo de compromiso de ningún tipo, y no son necesarios privilegios de administración para su ejecución).

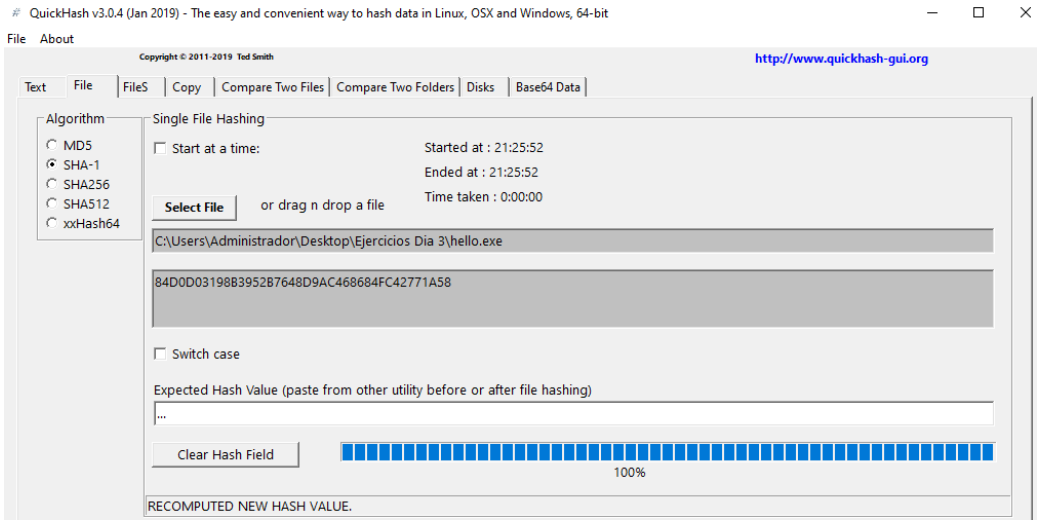
- ¿Son ambos archivos el mismo fichero?

Ambos archivos comparten el mismo MD5 pero el SHA1 es diferente por lo que hay indicios de que el archivo ha sido modificado y el primero hello.exe seria el limpio e erase.exe seria el modificado y aparentemente un archivo malicioso.

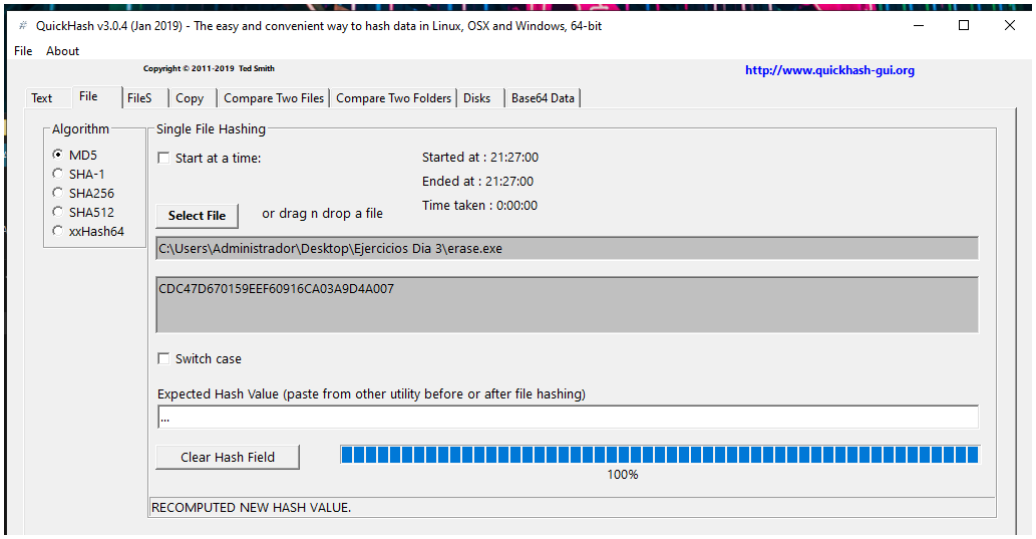
- Calcula las firmas hash MD5 y SHA1 para ambos ficheros.

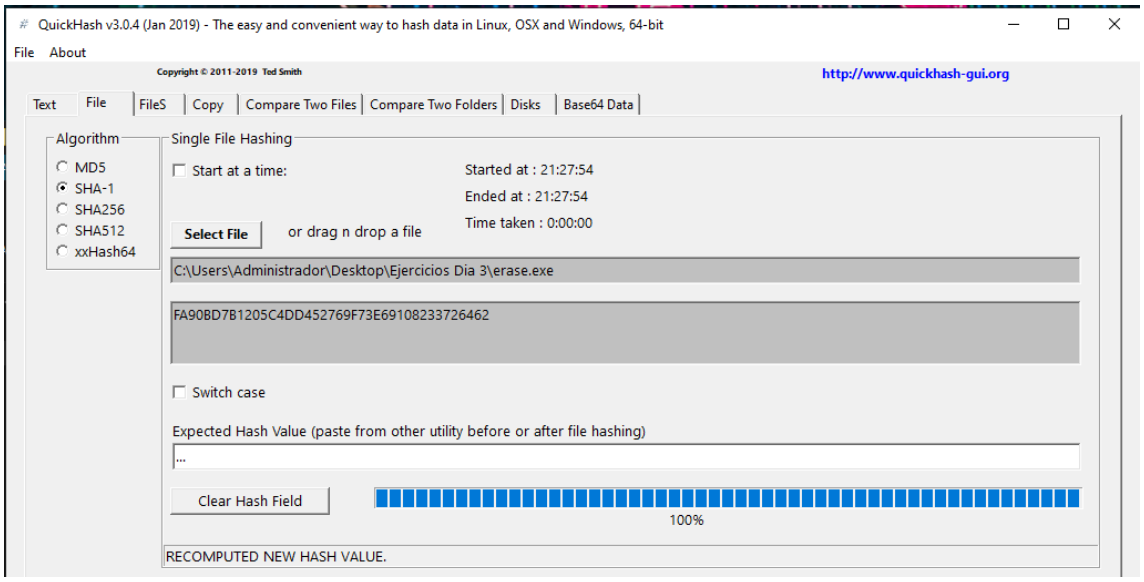
hello.exe





Erase.exe





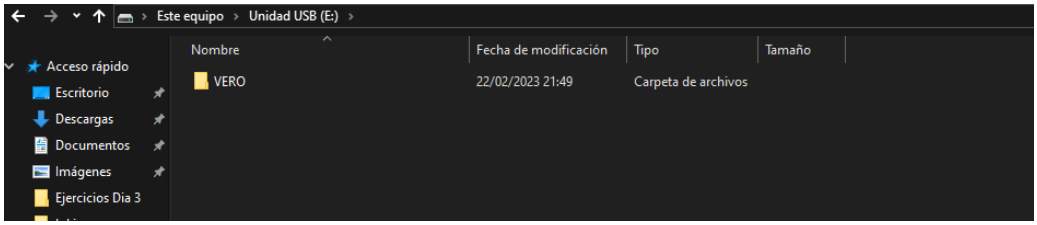
- ¿Qué conclusiones puedes extraer?

Luego de calcular los hashes de ambos archivos que parecen ser distintos, se detecto que hello.exe y erase.exe poseen el mismo hash MD5, el cual es un hash de autenticación, esto no es algo normal ya que cada archivo debería tener un hash distinto, no podrían compartirlo, esto significa que se ha producido una COLISION MD5 en el que de manera accidental o malintencionada se envió un archivo malicioso aparentemente erase.exe con el mismo hash que un archivo limpio hello.exe. puede que si esto fue malintencionado el atacante haya enviado el archivo que parece limpio para que sea ejecutado, ya que el hash MD5 sirve como cifrado de autenticación.

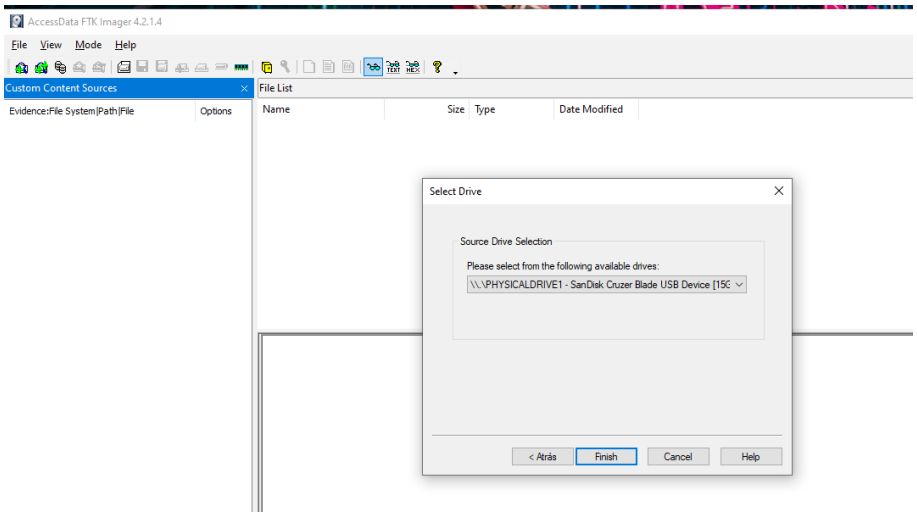
Fichero	MD5	SHA1
hello.exe	CDC47D670159EEF60916CA03A9D4A007	84D0D03198B3952B7648D9AC468684FC42771A58
erase.exe	CDC47D670159EEF60916CA03A9D4A007	FA90BD7B1205C4DD452769F73E69108233726462

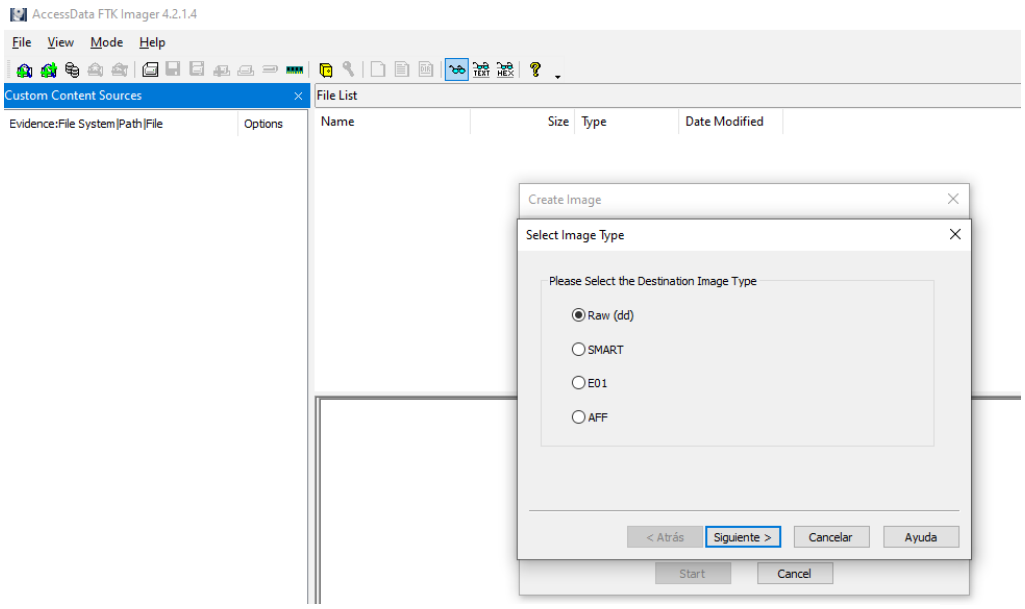
3.2. Realiza una imagen forense de un dispositivo externo y extrae ficheros de dicha imagen.

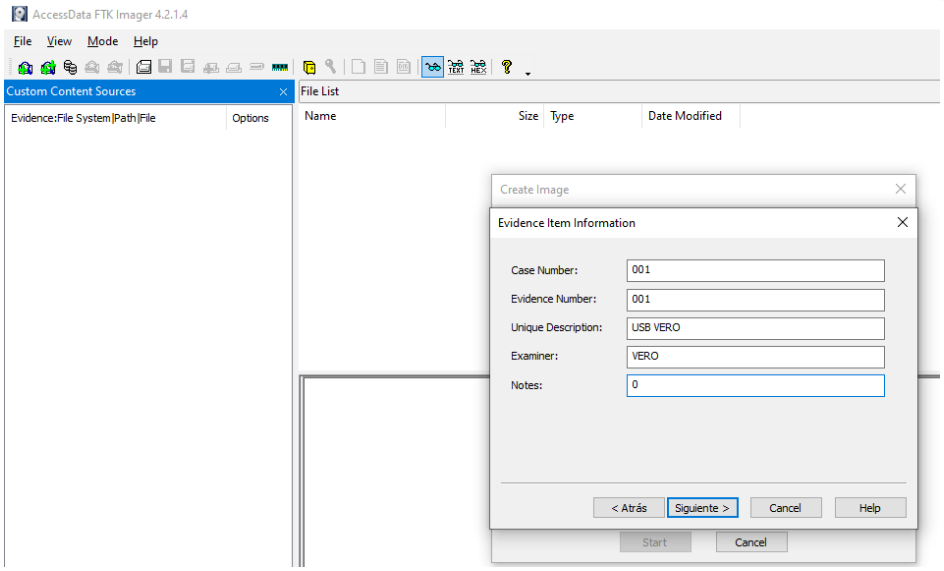
- Guía necesaria para el ejercicio:
- http://www.reydes.com/d/?q=Crear_la_Imagen_Forense_desde_una_Unidad_utilizando_FTK_Imager
- Para ello, primero debes conectar la unidad USB al ordenador y copiar algún documento en la misma (un fichero ofimático, un archivo de texto y una imagen, por ejemplo).

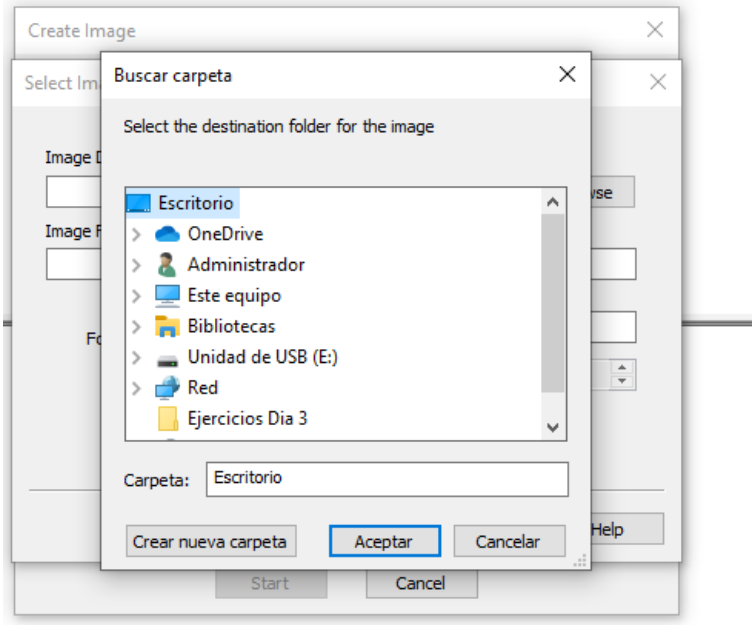


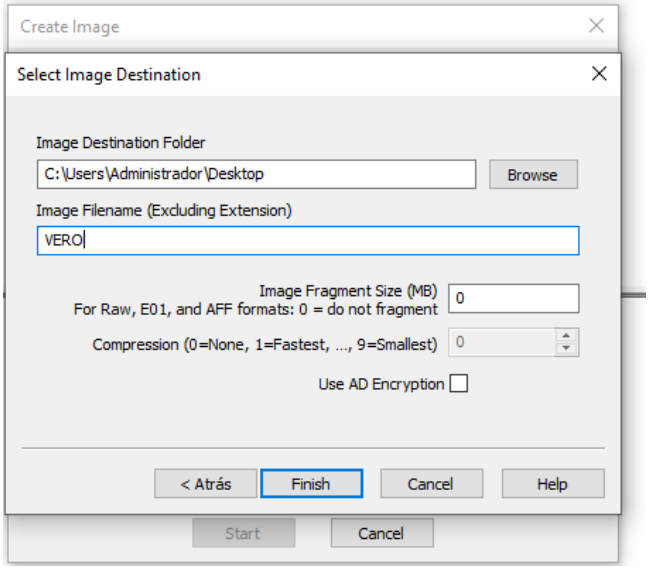
- Realiza una imagen forense completa de la unidad USB con la herramienta FTK Imager siguiendo las instrucciones que encontrarás en el manual.

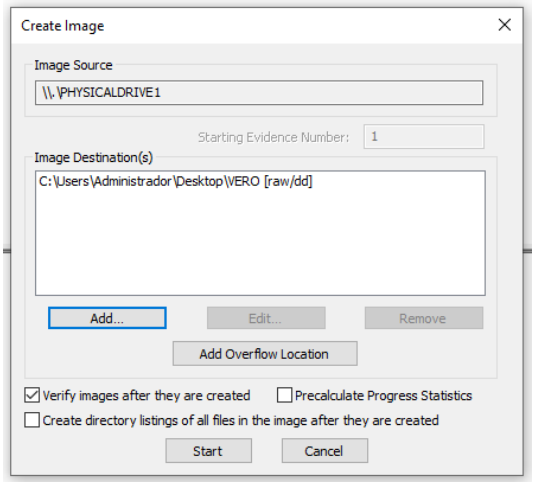

AccessData FTK Imager 4.2.1.4
File View Mode Help
Custom Content Sources
Evidence:File System|Path|File
Options
File List
Name
Size
Type
Date Modified
Select Drive
Source Drive Selection
Please select from the following available drives:
\\.\PHYSICALDRIVE1 - SanDisk Cruzer Blade USB Device [15
< Atrás
Finish
Cancel
Help

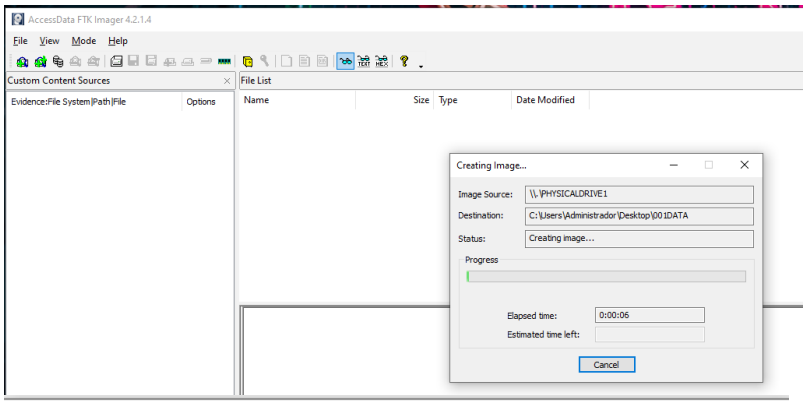

AccessData FTK Imager 4.2.1.4
File View Mode Help
Custom Content Sources
Evidence:File System|Path|File
Options
File List
Name
Size
Type
Date Modified
Create Image
Select Image Type
Please Select the Destination Image Type
Raw (dd)
SMART
E01
AFF
< Atrás
Siguiente >
Cancelar
Ayuda
Start
Cancel

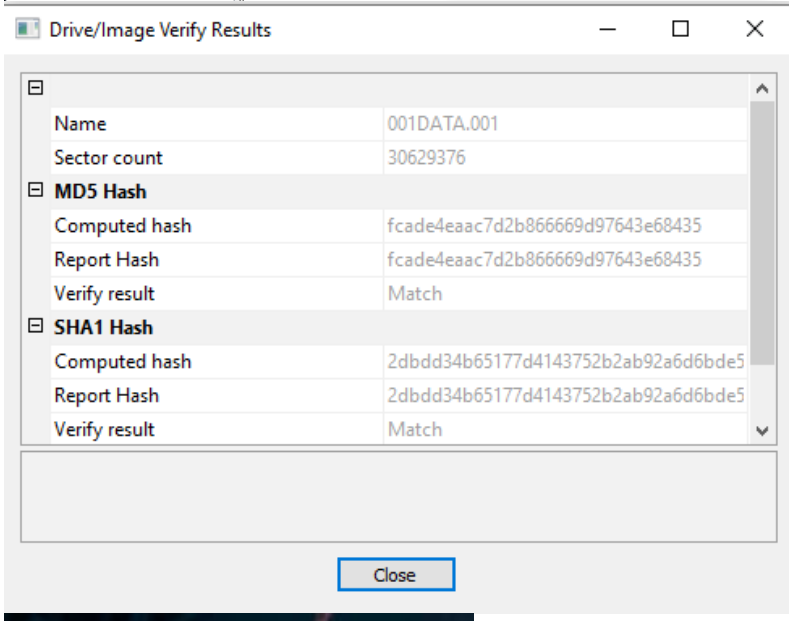

AccessData FTK Imager 4.2.1.4
File View Mode Help
Custom Content Sources
Evidence:File System|Path|File
Options
File List
Name
Size
Type
Date Modified
Create Image
Evidence Item Information
Case Number:
001
Evidence Number:
001
Unique Description:
USB VERO
Examiner:
VERO
Notes:
0
< Atrás
Siguiente >
Cancel
Help
Start
Cancel

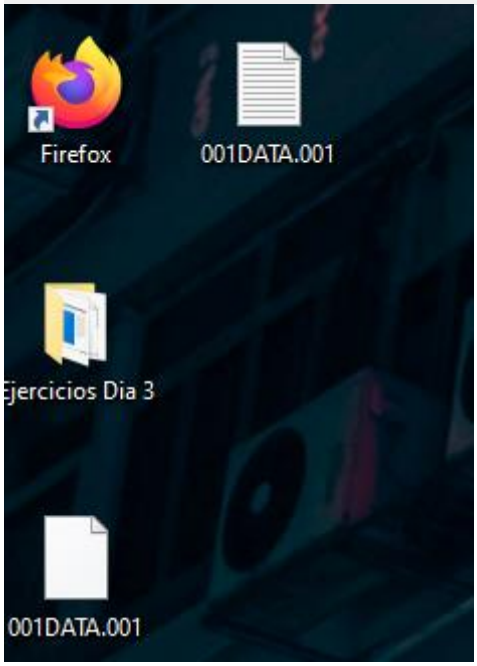

Create Image
Buscar carpeta
Select the destination folder for the image
Escritorio
OneDrive
Administrador
Este equipo
Bibliotecas
Unidad de USB (E:)
Red
Ejercicios Dia 3
Carpeta:
Escritorio
Crear nueva carpeta
Aceptar
Cancelar
Start
Cancel


Create Image
Select Image Destination
Image Destination Folder
C:\Users\Administrador\Desktop
Browse
Image Filename (Excluding Extension)
VERO
Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment
0
Compression (0=None, 1=Fastest, ..., 9=Smallest)
0
Use AD Encryption
< Atrás
Finish
Cancel
Help
Start
Cancel

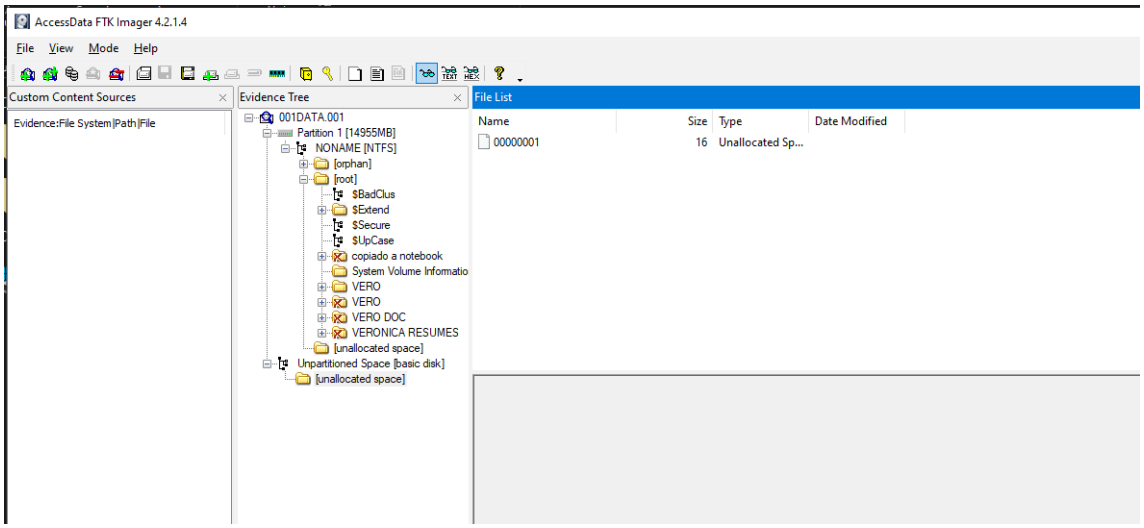

Create Image
Image Source
\\.\PHYSICALDRIVE1
Starting Evidence Number:
1
Image Destination(s)
C:\Users\Administrador\Desktop\VERO [raw/dd]
Add...
Edit...
Remove
Add Overflow Location
Verify images after they are created
Precalculate Progress Statistics
Create directory listings of all files in the image after they are created
Start
Cancel





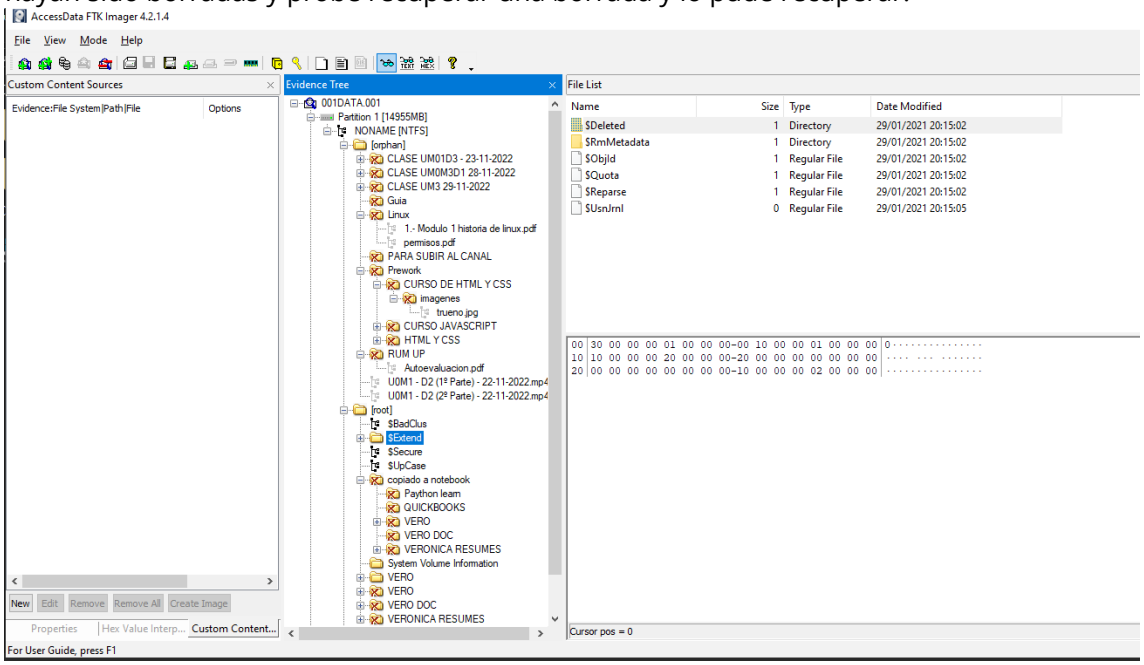


- Una vez generada la imagen, móntala con la herramienta FTK Imager y navega por el árbol de directorios del dispositivo.



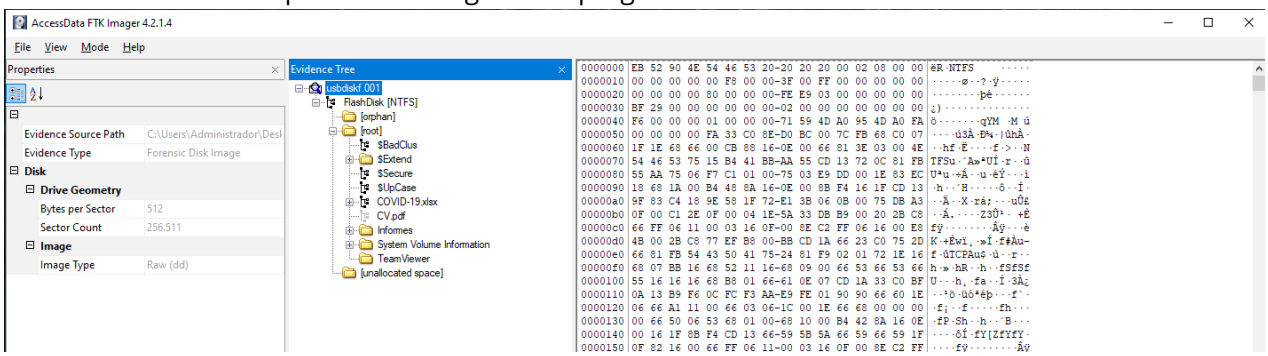
- ¿Puedes encontrar algún fichero borrado con anterioridad de la memoria USB pero cuyo contenido aún sea recuperable?

Antes de montar el USB en la maquina para probarlo copie varias carpetas y archivos y luego los borre, como se puede ver en la imagen de abajo, todas aparecen en el árbol aunque hayan sido borradas y probe recuperar una borrada y lo pude recuperar.



3.3. Realiza una imagen forense de un dispositivo externo y extrae ficheros de dicha imagen.

- Ficheros necesarios para el ejercicio: usbdiskf.001
- Según nos ha informado el cliente, la secretaria del CEO de la clínica privada Saludhealth ha encontrado esta mañana a primera hora un dispositivo USB desconocido por completo para ella conectado a su PC de sobremesa al ir a conectar un disco duro para extraer información relevante y relacionada con el presente caso de coronavirus que está afectando a nivel mundial.
- Debido a que durante los últimos meses han estado recibiendo amenazas anónimas vía email, que sospechan que puedan ser de un exempleado descontento, nos han solicitado realizar un análisis de dicho dispositivo USB a fin de identificar si han sufrido un incidente de seguridad.
- A partir de la imagen forense realizada sobre el dispositivo USB, analízalo para tratar de responder a las siguientes preguntas:

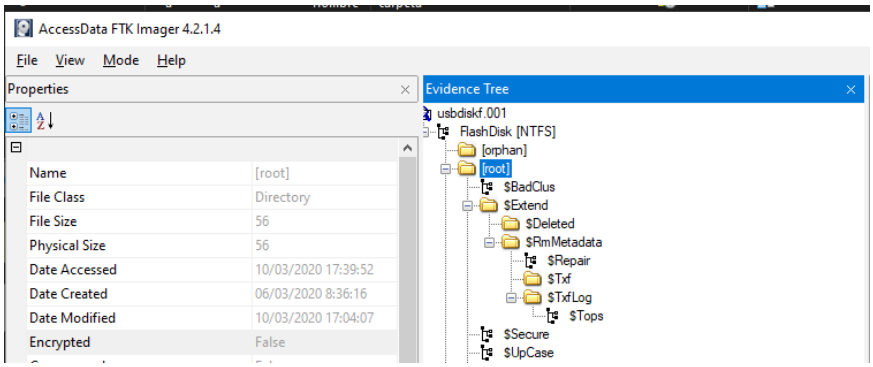


- ¿Cuál es el nombre asignado al dispositivo USB por su dueño real?

El nombre del USB es flashdisk, halle datos como el owner name: Administrators, del grupo administradores, algunos directorios son accesibles a todos y modificables por todos.

- ¿En qué momento se modificó el contenido del USB por última vez?

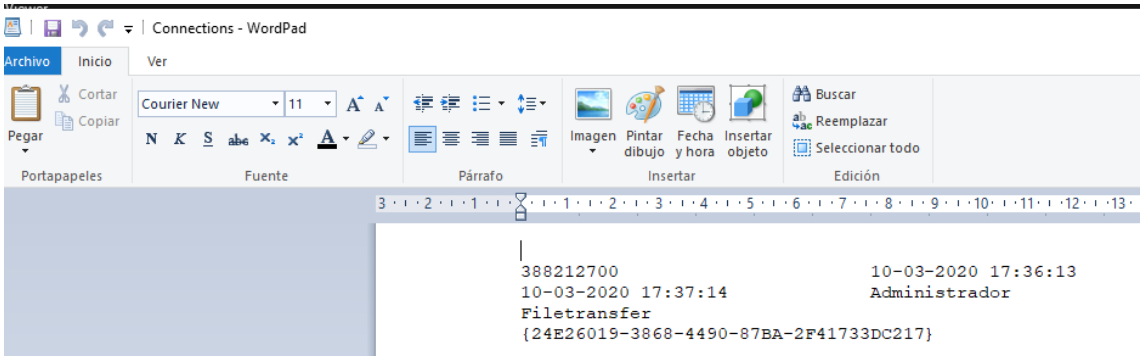
Aparentemente la última vez que el contenido del USB fue modificado fue el 10/03/2020



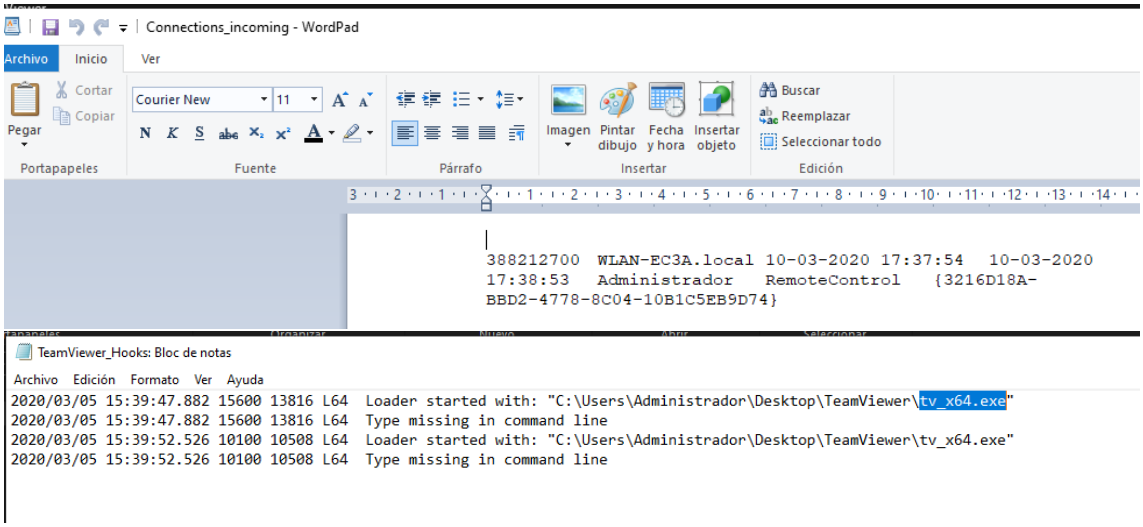
- ¿Observas indicios de que se haya podido producir un potencial incidente de seguridad?

Hay algunas señales de modificación de directorios y archivos en un mismo dia 06/03/2020
La mayoría de los directorios fueron modificados en la fecha mencionada, además dentro de las carpetas analizadas había una de teamviewer dentro de la cual se puede ver

información de transferencia de archivos justamente el 10/03/2020 ultimo dia de acceso al USB

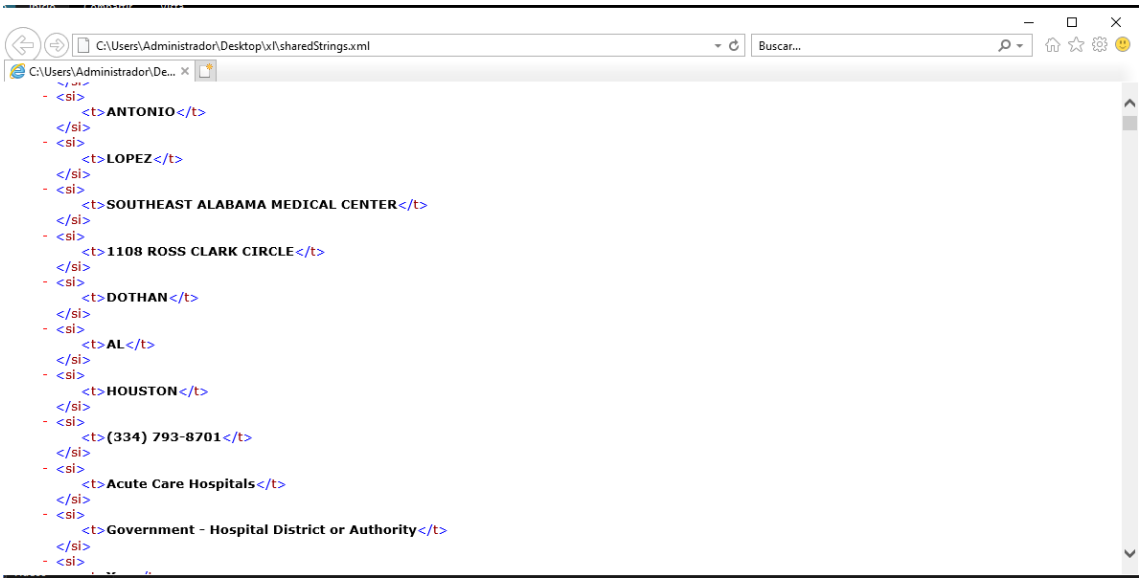


Tambien un control remoto ese mismo dia y a la misma hora, por lo que podemos deducir que la persona en cuestión estaba teniendo acceso remoto a una maquina ese ultimo dia de modificación.



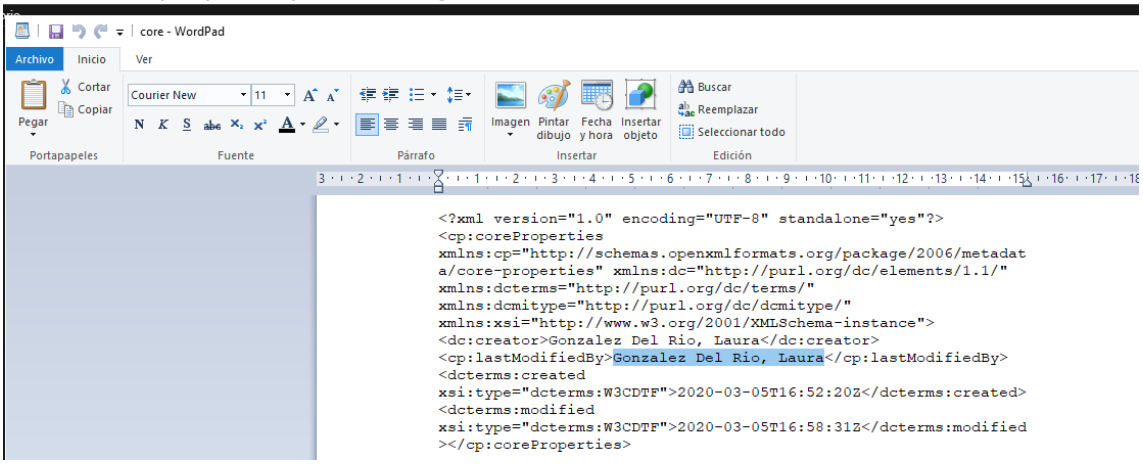
Tambien se hallo un archivo ejecutable tv_x64.exe, desconocido para mi hasta ahora, investigando de que se trata descubri información de que podría tratarse de un malware, esto es necesario investigar ya que algunas veces este archivo ejecutable es un camuflaje de algún virus, tv_x64.exe no es un archivo básico de Windows. El proceso no tiene ninguna ventana visible. El archivo tiene una firma digital. El archivo tv_x64.exe es un archivo con la firma de Verisign. Tv_x64.exe es capaz de manipular otros programas. Entonces la evaluación técnica de seguridad es 29% peligrosa.

Tambien se hallaron informaciones confidenciales como datos completos de paciente, nombres, ID, lugar de residencia, teléfono, lugares de consulta y datos que pueden ser propagados en sitios como la Deepweb, lo cual podría llegar a ser peligroso tanto para la compañía como las personas cuyos datos están expuestos.



También se hallaron dos informes de auditoría de dos empresas distintas REPSOL SA y RENFE-operadora, considerados confidenciales ya que en los documentos se hallan datos de balances y estados del negocio asi como la opinión de los auditores externos, esto podría manipularse o divulgarse y resultar en el perjuicio de las compañías cuyos datos están expuestos.

Una ultima acotación que podría resultar interesante es que hallamos un nombre que parece haber creado y modificado archivos, no esta demás realizar una investigación acerca de esto aunque pueda parecer insignificante.



Se hallaron mas datos pero considerados irrelevantes al caso por ahora.

- En caso afirmativo, ¿podrías indicar si resulta necesario notificar el incidente y ante qué organismos?

Se recomienda notificar sobre los datos relevantes a las compañías mencionadas arriba, cuyos datos están expuestos, además de realizar una investigación acerca del poseedor de este dispositivo, por otro lado también notificar ante organismos de seguridad una posible fuga de datos, teniendo en cuenta que se realizaron transferencias de archivos a través de teamviewer, esto podría afectar la privacidad de los pacientes de la clínica en cuestión, estas instituciones son autoridades de control, como ser la Agencia de Protección de datos de España.

- ¿Puedes identificar alguna información adicional del presunto dueño del USB (nombre, aficiones, etc.)?

Dentro de los documentos hallados se encontró un Curriculum que podría ser del presunto dueño del USB, Se trata de Manolo Ruiz, un producto owner, especializado en SCRUM, es de Madrid, en el documento consta el barrio en el que reside y posee dos perros, además de sus gustos por el deporte, estos datos podría ayudar a identificar si se trata del dueño del USB o la relación que podría tener con el mismo.

3.4. Identifica empleando fuentes públicas y las muestras de archivos proporcionadas, qué tipo de familia de *ransomware* ha cifrado los siguientes archivos.

- Ficheros necesarios para el ejercicio: cifrados.zip
- ¿Qué indicadores se emplean para identificar la familia de *ransomware*?

El principal indicador que se toma en primer lugar es identificar la extensión del archivo e investigarlo.

1- banner_image.png.GeekFam@tutanota.com.zeoticus
2- CV Teresa Martinez.PDF.08pw4ghz
3- Garden.jpg.WNCRY
4- Objeto social.pdf.id[125DFD2B-2686].[CYBERTRUCK2048@protonmail.com].Devos

Muestra descifrable?	Familia	Extensión	¿Es
1-Zeoticus, este virus es una peligrosa infección de ransomware que proviene de la familia de virus Zeoticus Ransomware y su objetivo principal es ingresar a su sistema informático junto con el cifrado de archivos en él. Cualquiera que sea la situación con Zeoticus virus ransomware, es un criptovirus que utiliza el algoritmo AES en todos sus archivos importantes que utiliza. Este virus es descifrable.			
2-.pdf es una infección de tipo ransomware que pertenece a la familia de ransomware Dharma. Como ocurre con casi todas las infecciones de esta familia, Tras introducirse en el sistema, .pdf encripta la mayor parte de los archivos almacenados, de ahí que se vuelvan inutilizables. Asimismo, .pdf cambia el nombre de cada archivo añadiendo el ID único de víctima, el correo electrónico del desarrollador y la extensión, . Sepa qué ".pdf" como extensión es un formato completamente auténtico de Portable Document Format (PDF), por tanto, en los archivos cifrados se verá probablemente el icono PDF. Sin embargo, no deje engañarse por ello, los archivos están cifrados. Los archivos se cifran en RSA y son descifrables.			
3-WannaCry Ransomware es un virus destructivo de cifrado de archivos que pertenece a la familia Jigsaw Ransomware. Al igual que otras amenazas de malware de la misma categoría, también encripta los archivos esenciales de los usuarios y luego les exige una suma de rescate por el software de descifrado. Este peligroso cripto virus utiliza una criptografía sólida para bloquear sus archivos y documentos vitales y agrega la extensión «.WNCRY» con cada uno de ellos como sufijo. Después de eso, abrir los datos comprometidos será imposible para usted a menos que use la herramienta de descifrado que solo puede obtenerse de los atacantes, se concluye que el rasomware es descifrable.			

4-Devos es parte de la familia de ransomware Phobos. Como la mayoría de los programas de este tipo, Devos bloquea el acceso a los archivos cifrándolos, cambia sus nombres de archivo y proporciona a las víctimas instrucciones sobre cómo recuperar sus archivos. Este ransomware cambia el nombre de todos los archivos encriptados agregando la identificación de la víctima, la dirección de correo electrónico del desarrollador y agregando la extensión ".Devos" a sus nombres de archivo. Por ejemplo, cambia el nombre de "1.jpg" a "1.jpg.id[1E857D00-2654].[qq1935@mail.fr].Devos", y así sucesivamente. Proporciona a las víctimas dos notas de rescate: una en una ventana emergente (archivo "info.hta") y otra en un archivo de texto llamado "info.txt". Desafortunadamente, no hay herramientas gratuitas que puedan descifrar archivos cifrados por este ransomware, al menos no por el momento. Es común que los ciberdelincuentes que diseñaron un ransomware en particular sean los únicos que pueden ayudar a las víctimas a descifrar sus datos. Sin embargo, también es común que no envíen una herramienta de descifrado y/o clave incluso después de un pago, por lo que se concluye que el ransomware es descifrable.

3.5. Trata de identificar en los siguientes logs de eventos de Windows actividad maliciosa o ilegítima.

- Ficheros necesarios para el ejercicio: Logs de eventos.zip
- El log Security registra actividad relacionada con la seguridad del equipo como pueden ser eventos de intentos de inicio de sesión[2], inicios exitosos, modificaciones de permisos de usuarios, creación de nuevos usuarios, etc.

[2] Para más información sobre eventos de acceso: https://ponderthebits.com/2018/02/windows-rdp- related-event-logs-identification-tracking-and-investigation/

- ¿Qué identificador de evento corresponde con inicios de sesión exitosos?

El id 4624 es el que recoge un intento exitoso de inicio de sesión en un equipo.

¿Qué información de interés recoge este tipo de eventos?

La información importante que se puede derivar del Evento 4624 incluye:

Tipo de inicio de sesión: Este campo revela el tipo de inicio de sesión que se produjo. En otras palabras, señala cómo inició sesión el usuario. Hay un total de nueve tipos distintos de inicio de sesión; los más comunes son: tipo de inicio de sesión 2 (interactivo) y tipo de inicio de sesión 3 (red). Cualquier tipo de inicio de sesión distinto a 5 (que denota un inicio de servicio) es una señal de alarma.

Nuevo inicio de sesión: Esta sección revela el Nombre de la cuenta del usuario para quien se ha creado el nuevo inicio de sesión y la ID de inicio de sesión, un valor hexadecimal que ayuda a correlacionar este evento con otros.

Tipo de inicio de sesión	Descripción
2	**Inicio de sesión interactivo** Ocurre cuando un usuario inicia sesión con el teclado y pantalla locales del equipo.
3	**Inicio de sesión de red**
4	**Inicio de sesión por lote**
5	**Inicio de sesión de servicios**
7	**Inicio de sesión de desbloqueo**
8	**Inicio de sesión de NetworkClearText**
9	**Inicio de sesión de NewCredentials**
10	**Inicio de sesión de RemoteInteractive**
11	**Inicio de sesión de CachedInteractive**

La sección Sujeto revela la cuenta en el sistema local (no el usuario) que solicitó el inicio de sesión.

La sección Nivel de suplantación revela la medida en que un proceso en la sesión de inicio de sesión puede suplantar a un cliente. Los niveles de suplantación determinan las operaciones que un servidor puede realizar en el contexto del cliente.

La sección Información del proceso revela detalles sobre el procedimiento que intentó el inicio de sesión.

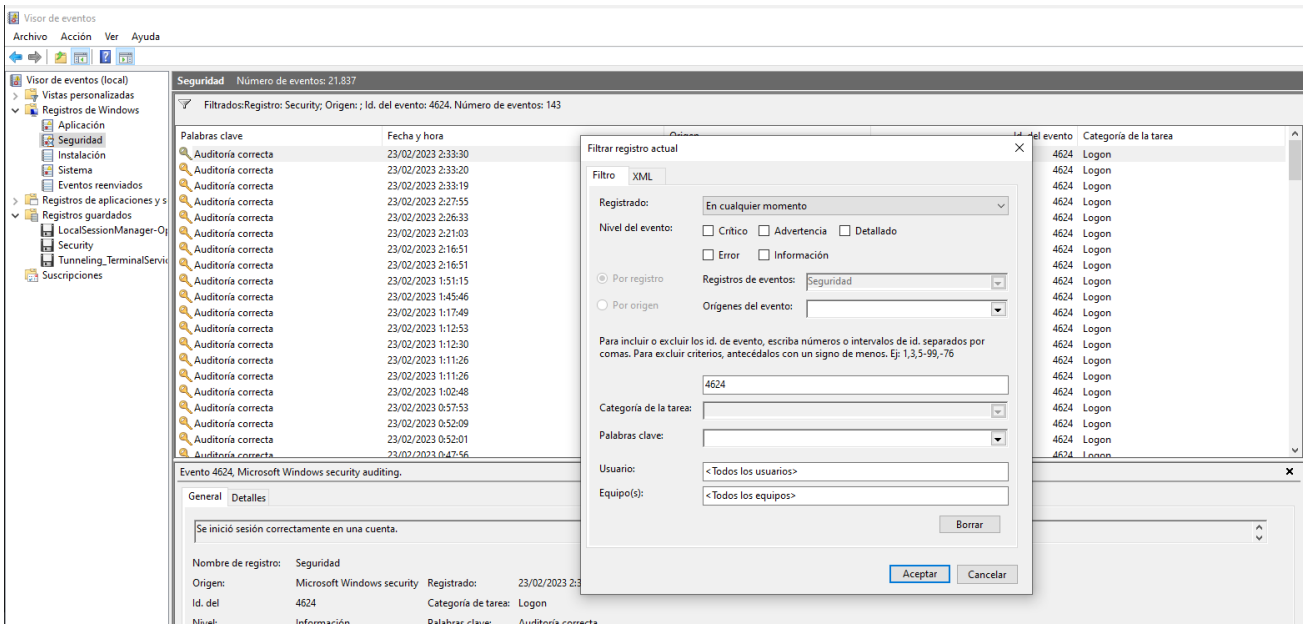
La sección Información de red revela dónde estaba el usuario cuando inició sesión. Si esta acción se comenzó desde el mismo equipo, la información estará en blanco o reflejará el nombre de la estación de trabajo en el equipo local y la dirección de la red fuente.

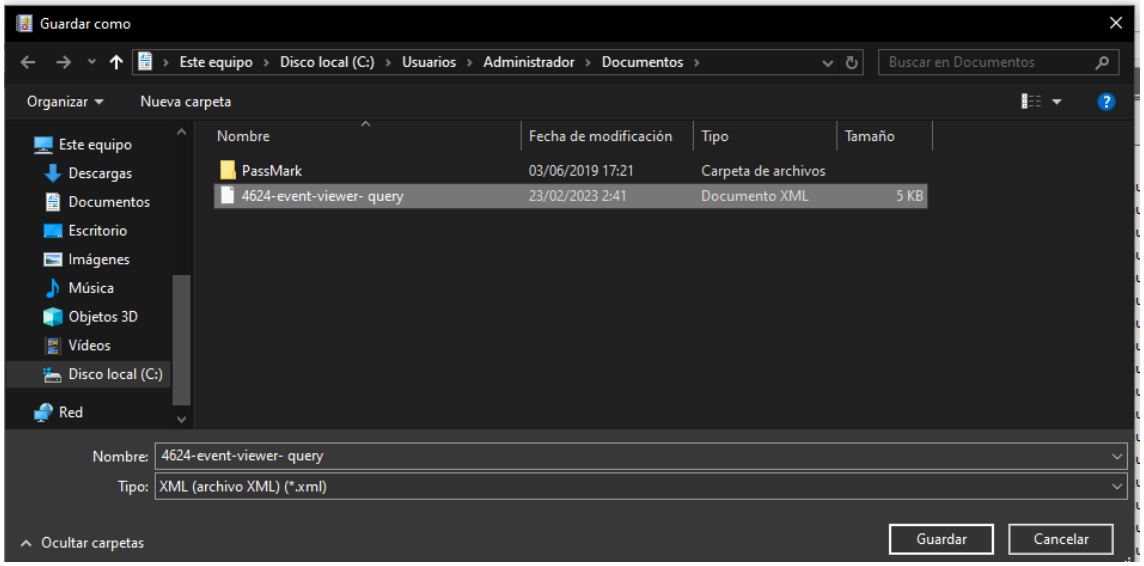
La Información de autenticación revela detalles sobre el paquete de autenticación utilizado para el inicio de sesión.

- Por su parte, el log System recoge los eventos registrados en el equipo relacionados propiamente con el sistema operativo o aplicaciones nativas de Windows.
    - ¿Qué identificador de evento corresponde con el borrado de logs EVTX?

El identificador de borrado de logs es el 1102

- Mediante la herramienta Event Viewer nativa de Windows, podemos abrir y filtrar los logs de eventos de nuestro propio equipo, como logs que importemos de otros equipos Windows.
- Event Viewer permite además realizar filtrados por ciertos campos y un detalle de filtrado más detallado haciendo uso de etiquetas XML.
    - Guarda desde Event Viewer un archivo xml con todos los eventos de inicio de sesión exitosos en un archivo con el nombre 4624-event-viewer-query.xml





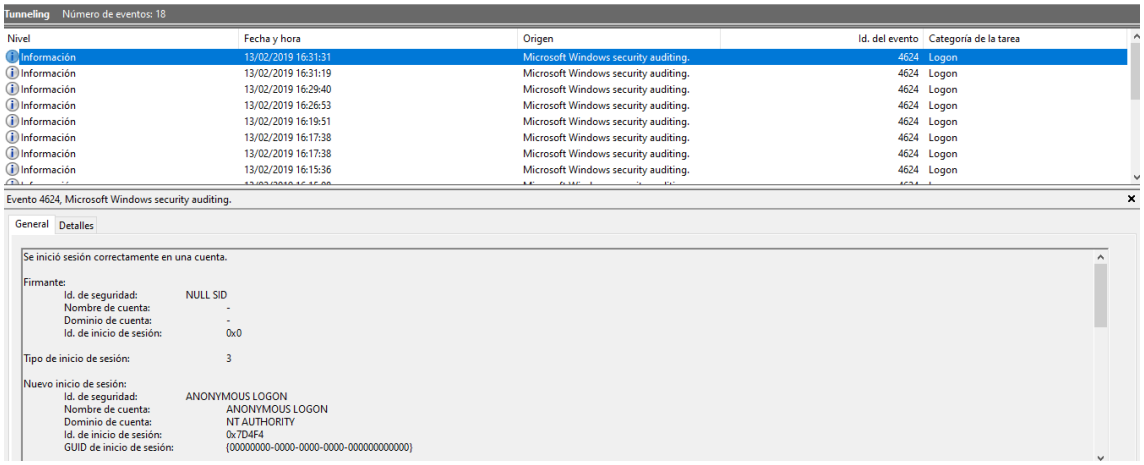

```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
- <Events>
  - <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
    - <System>
      <Provider Guid="{54849625-5478-4994-a5ba-3e3b0328c30d}" Name="Microsoft-Windows-Security-Auditing"/>
      <EventID>4624</EventID>
      <Version>2</Version>
      <Level>0</Level>
      <Task>12544</Task>
      <Opcode>0</Opcode>
      <Keywords>0x8020000000000000</Keywords>
      <TimeCreated SystemTime="2023-02-23T01:33:30.695034700Z"/>
      <EventRecordID>75453</EventRecordID>
      <Correlation ActivityID="{0fec1257-46e5-0000-dc12-ec0fe546d901}"/>
      <Execution ThreadID="7728" ProcessID="628"/>
      <Channel>Security</Channel>
      <Computer>DESKTOP-60G0MD5</Computer>
      <Security/>
    </System>
```

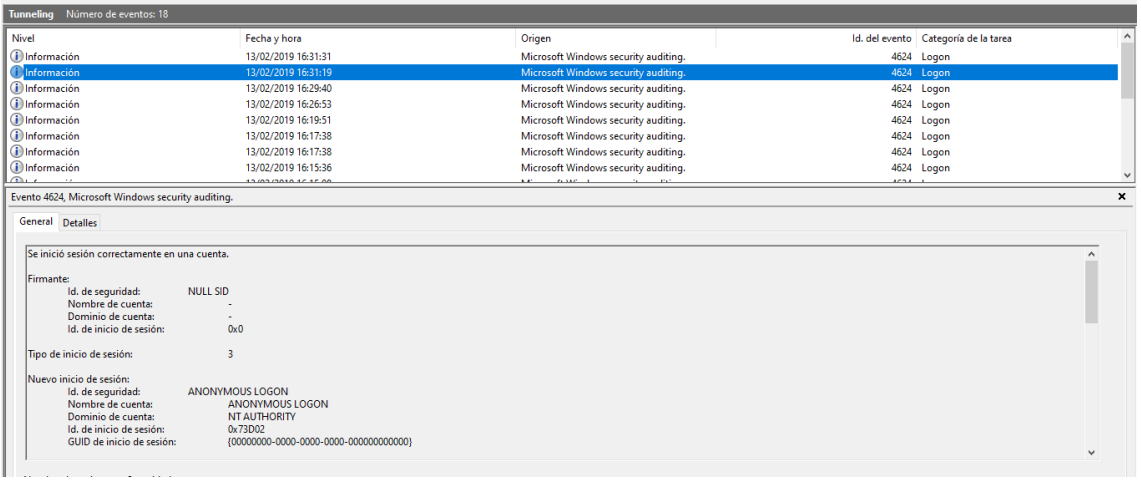
- Para los siguientes archivos EVTX que registran eventos de Windows, identifica qué acciones maliciosas han quedado registradas en cada uno de ellos y completa la información de la tabla:

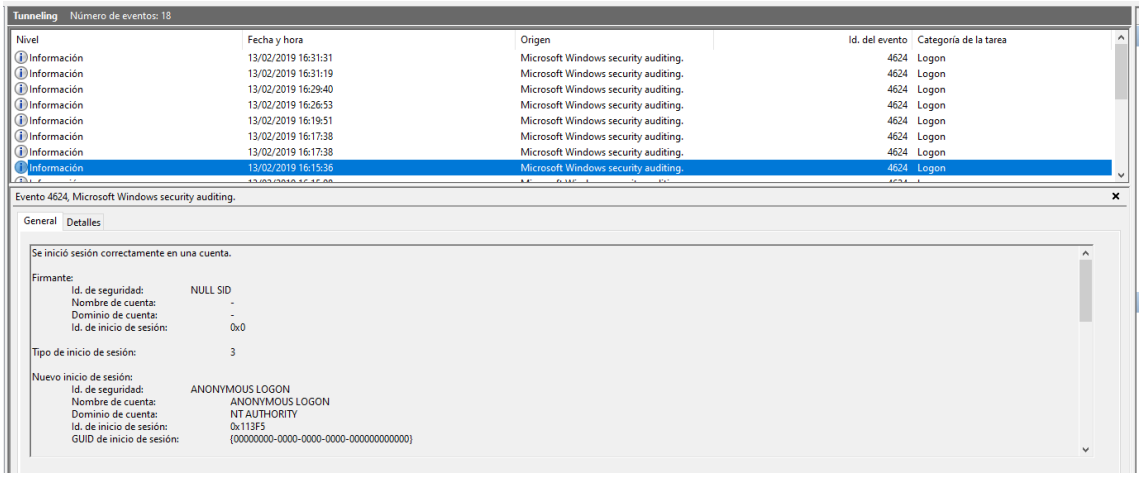
Log Destacada	Event ID	Fecha y Hora	Actividad Maliciosa
Tunneling.evtx	4624	13-02-2019 16:29:40	-Conexión RDP a través de túnel SSH inverso e inicio de sesión y movimientos laterales

Tunneling_Terminal - Services-RemoteControl.evtx	1149	13-02-2019 18:51:19	Autenticación de usuario
Security.evtx	1102 5156 4663	20-03-2019 0:35:07 20-03-2019 0:35:08 20-03-2019 0:35:14 y 0:35.15	Se borraron registros se permitió una conexión se intento tener acceso a un objeto
Security_Share.evtx	5145 5145	18-03-2019 15:23:27-26 18-03-2019 15:23:24	Se compartio archivo sospechoso Se compartio archivo Sospechoso, tener en cuenta que puede tratarse de una acción de defensa por parte de la organización
LocalSessionManager - Operational.evtx	21 22 40	21-01-2019 13:47 21-01-2019 21-01-2019	Inicio de session remota de una IP externa, luego recibe una shell y se desconecta al instante, esto sucede en bucle y las IP tanto de Administrador como de Olivia como de Yolanda van cambiando muestro pantallazo abajo para el caso de Yolanda, esto puede ser una actividad sospechosa. Tambien se dan unos errores cuyo ID es el 59 pero investigando pude notar que suele ser un evento normal que da error.

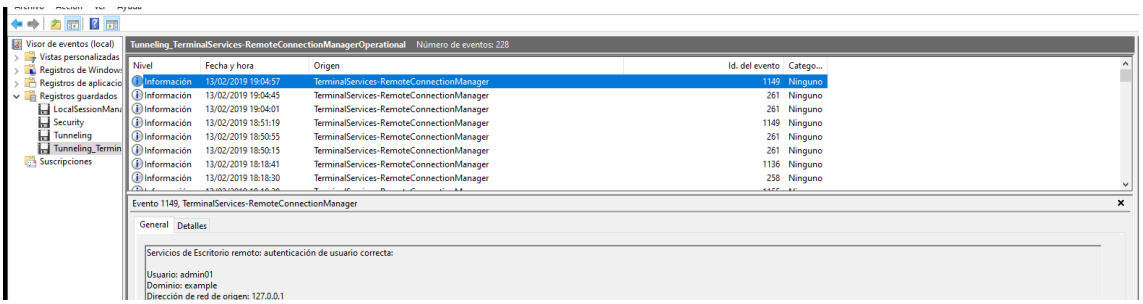
Tunneling.evtx

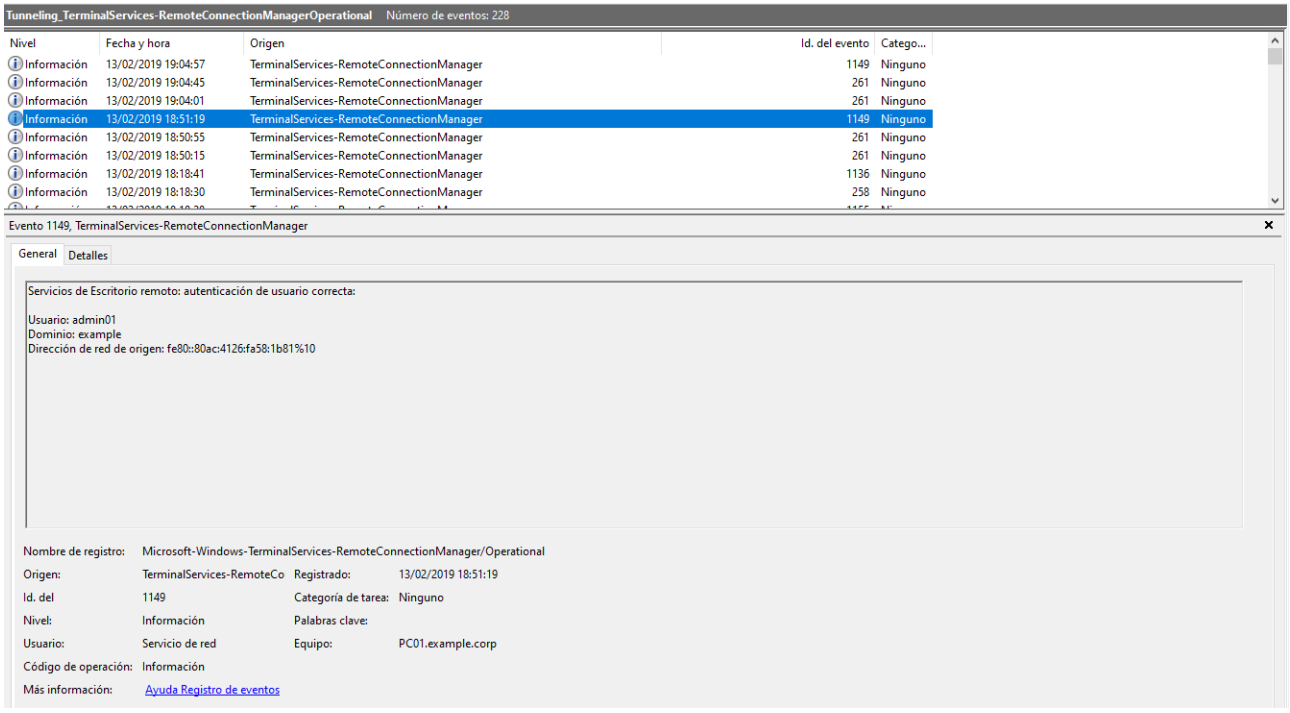






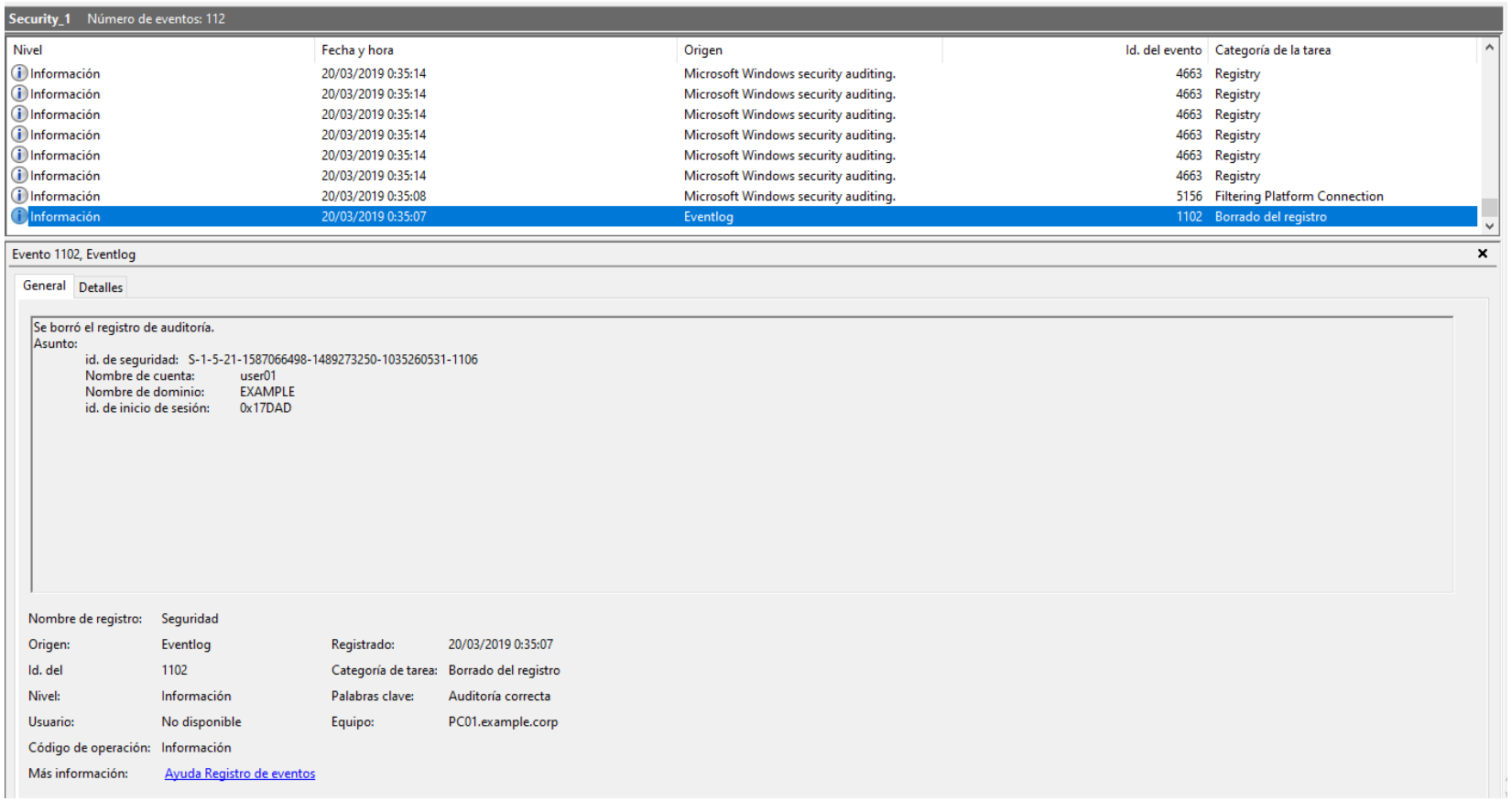
Tunneling_Terminal- Services- RemoteControl.evtx



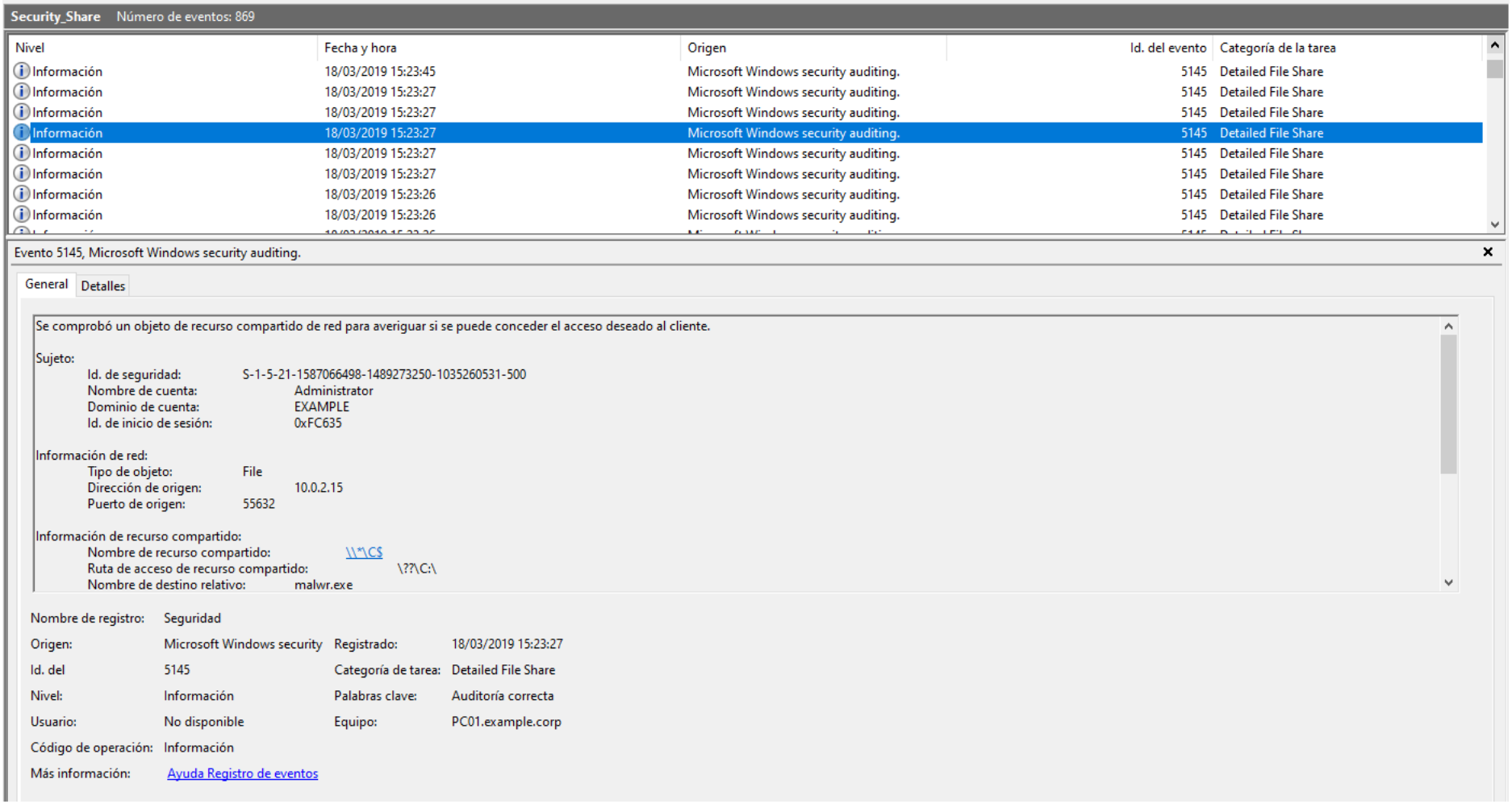


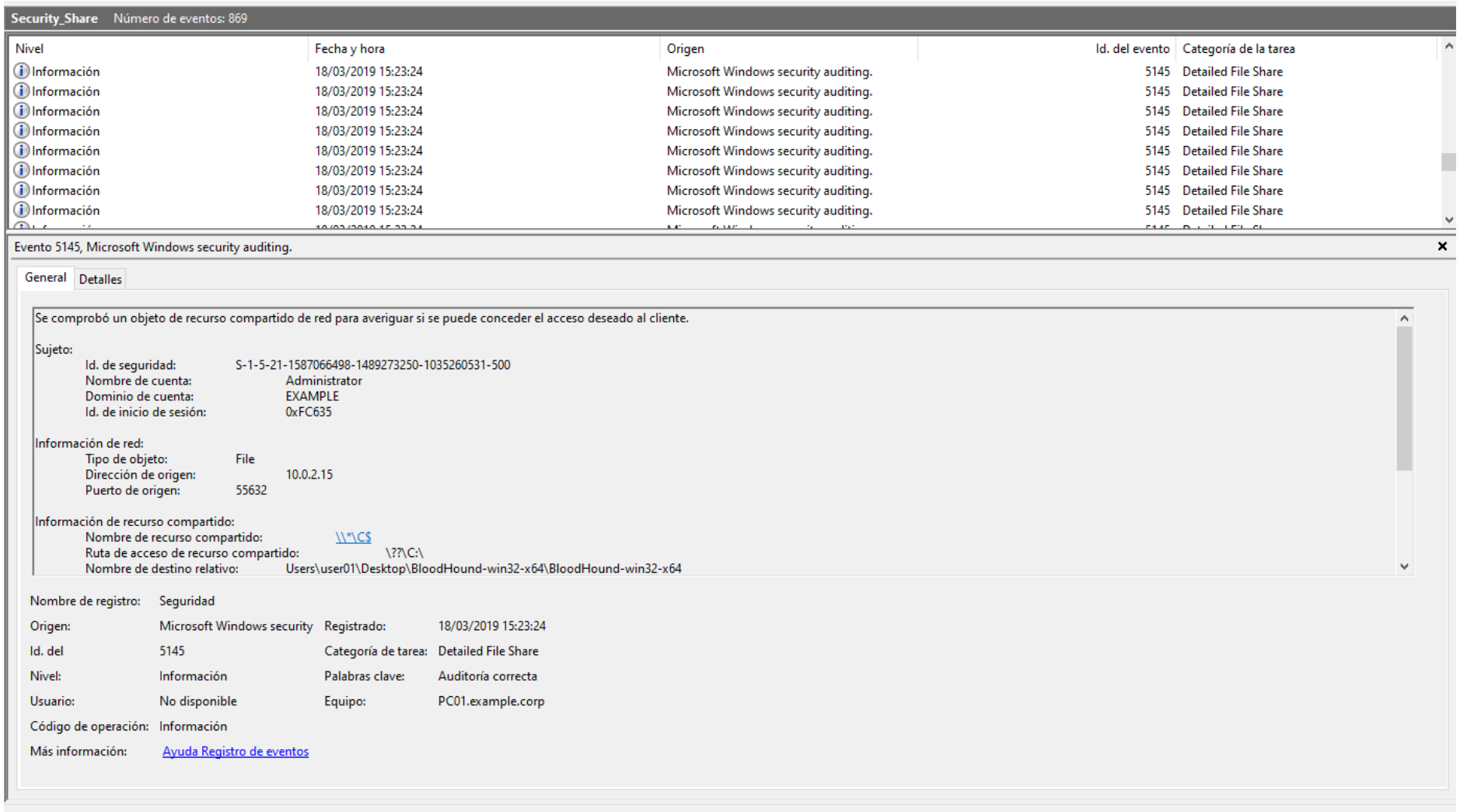
Security.evtx

Teniendo en cuenta el borrado de registro, la conexión se puede deducir que el evento 4663 podria ser malicioso ya que se intento acceder a un objeto. Además podemos fijarnos en el horario de las acciones lo cual hace mas sospechoso aun.



Security_Share.evtx



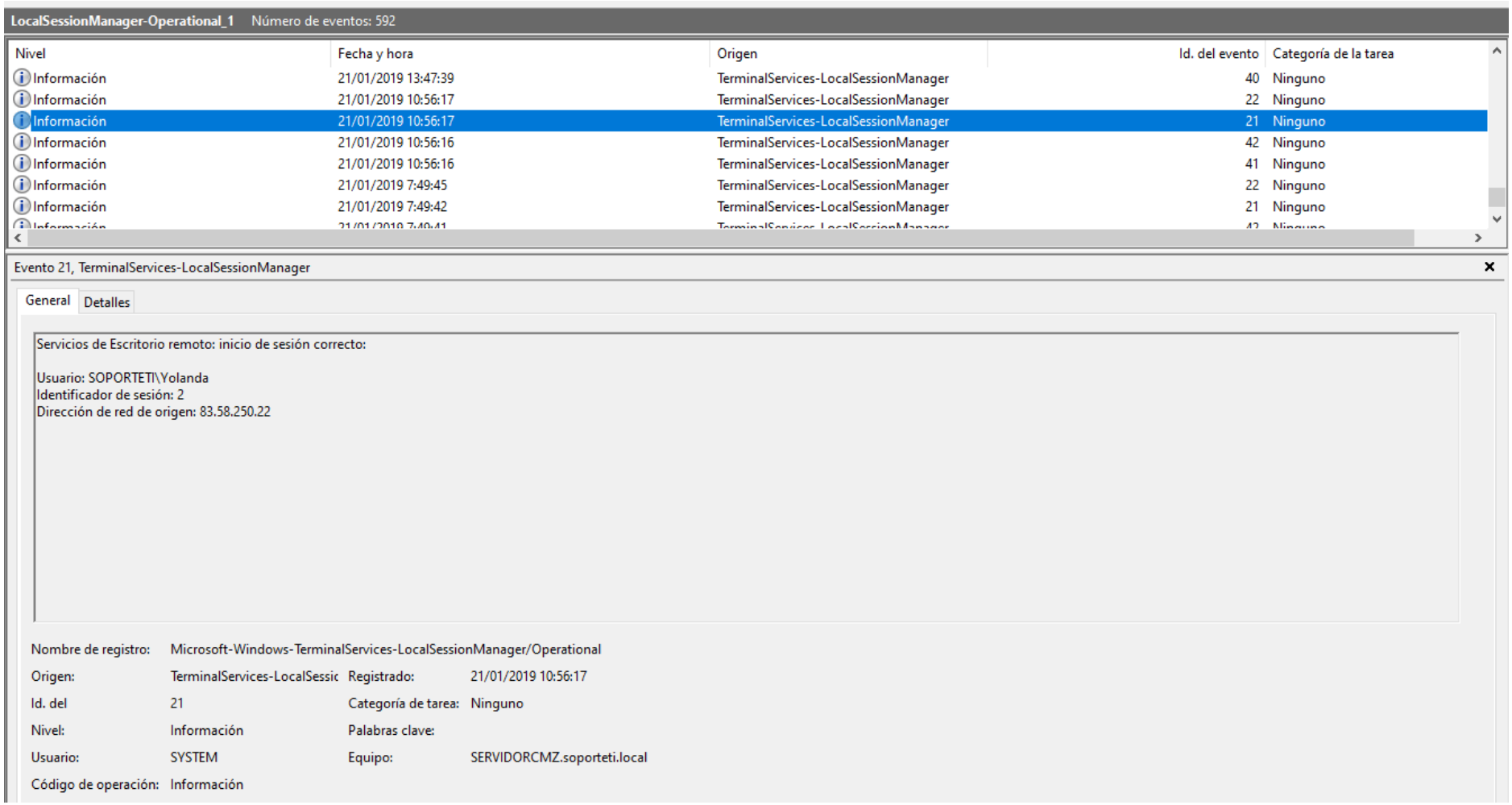


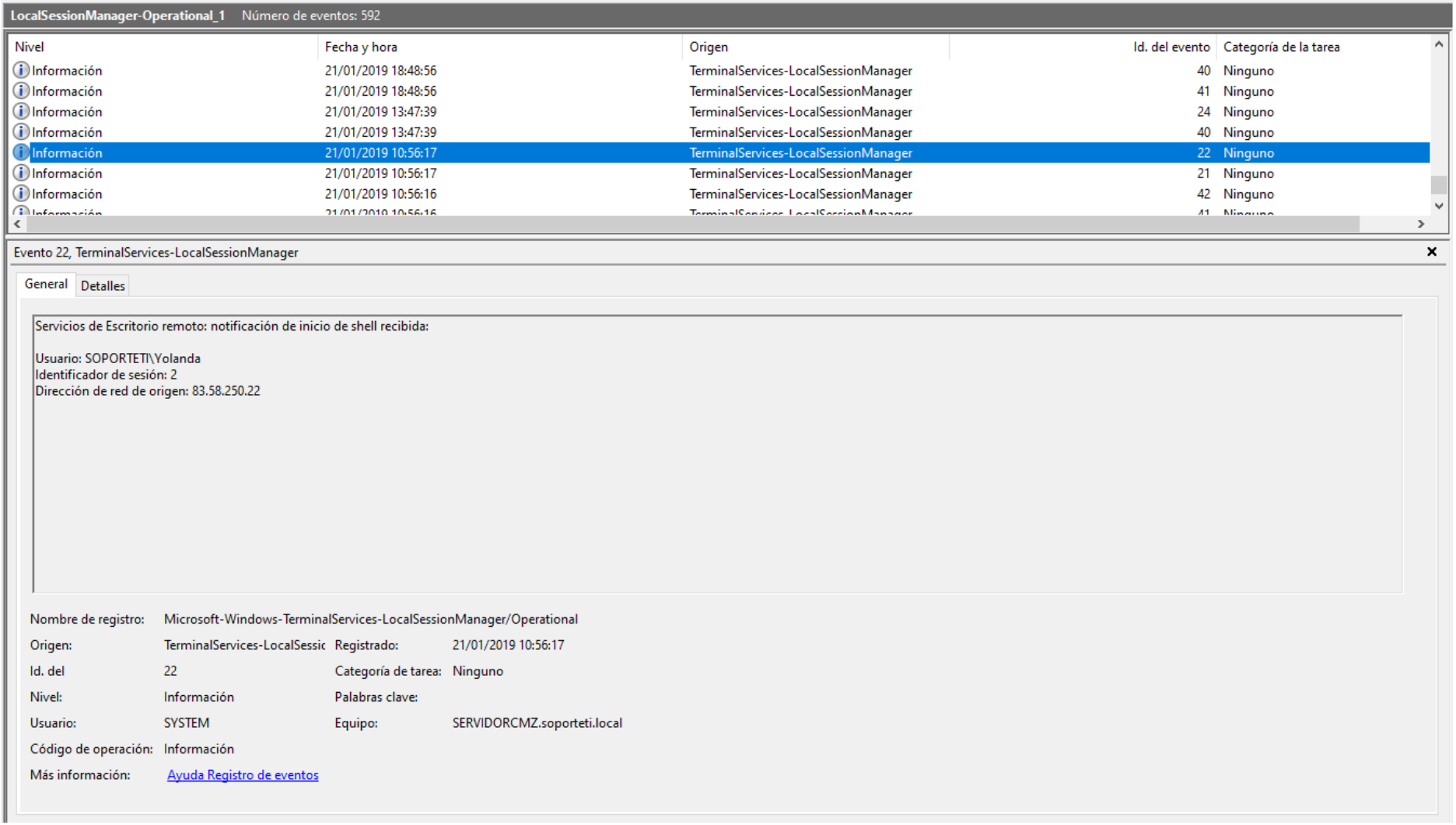
Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Información	18/03/2019 15:23:24	Microsoft Windows security auditing.	5145	Detailed File Share
Información	18/03/2019 15:23:24	Microsoft Windows security auditing.	5145	Detailed File Share
Información	18/03/2019 15:23:24	Microsoft Windows security auditing.	5145	Detailed File Share
Información	18/03/2019 15:23:24	Microsoft Windows security auditing.	5145	Detailed File Share
Información	18/03/2019 15:23:24	Microsoft Windows security auditing.	5145	Detailed File Share
Información	18/03/2019 15:23:24	Microsoft Windows security auditing.	5145	Detailed File Share
Información	18/03/2019 15:23:24	Microsoft Windows security auditing.	5145	Detailed File Share
Información	18/03/2019 15:23:24	Microsoft Windows security auditing.	5145	Detailed File Share

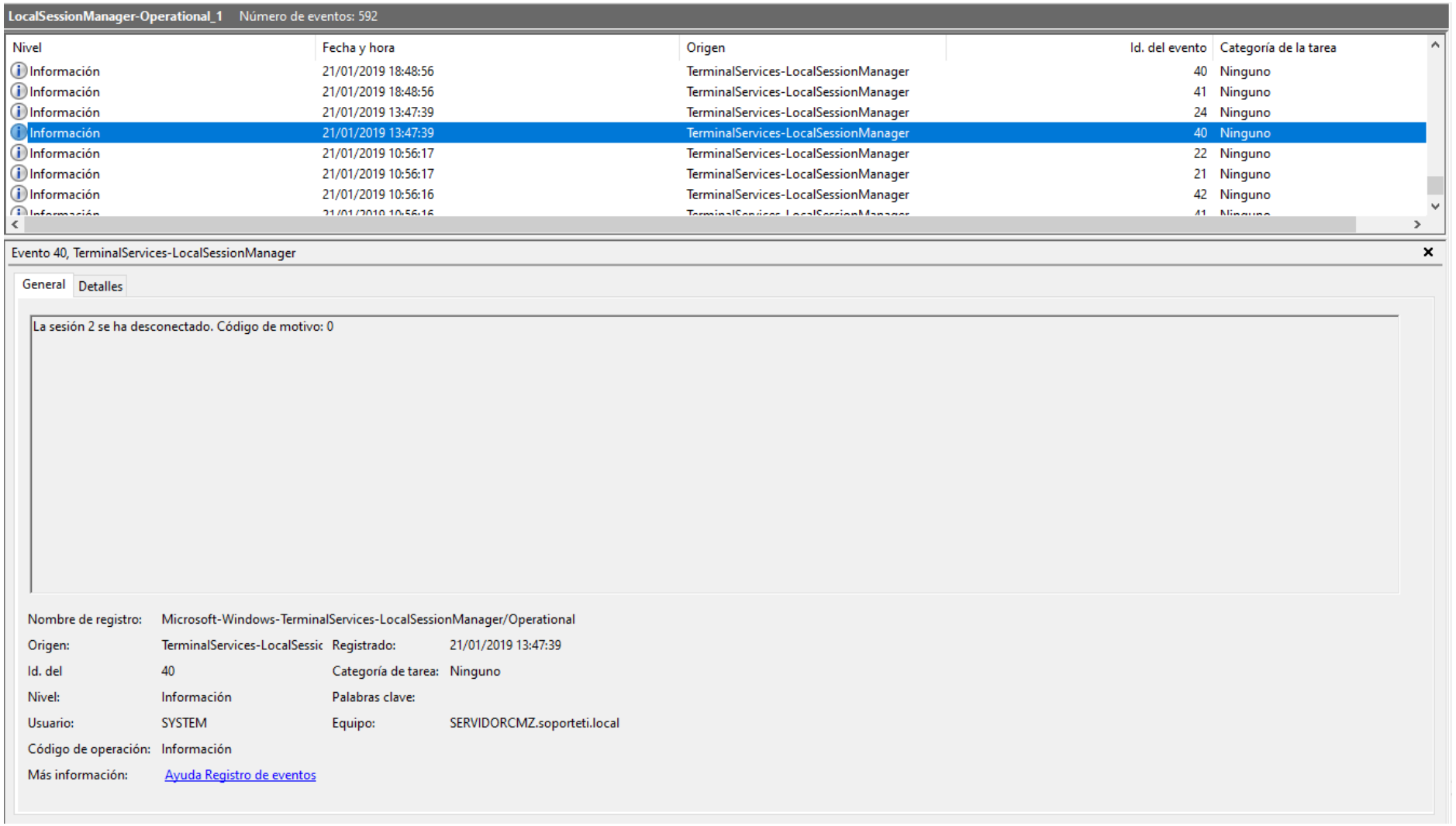
```
Se comprobó un objeto de recurso compartido de red para averiguar si se puede conceder el acceso deseado al cliente.

Sujeto:
          Id. de seguridad:          S-1-5-21-1587066498-1489273250-1035260531-500
          Nombre de cuenta:                    Administrator
          Dominio de cuenta:                   EXAMPLE
          Id. de inicio de sesión:             0xFC635

Información de red:
          Tipo de objeto:            File
          Dirección de origen:                 10.0.2.15
          Puerto de origen:          55632

Información de recurso compartido:
          Nombre de recurso compartido:                  \\*\C$
          Ruta de acceso de recurso compartido:                    \??\C:\
          Nombre de destino relativo:          Users\user01\Desktop\BloodHound-win32-x64\BloodHound-win32-x64
```

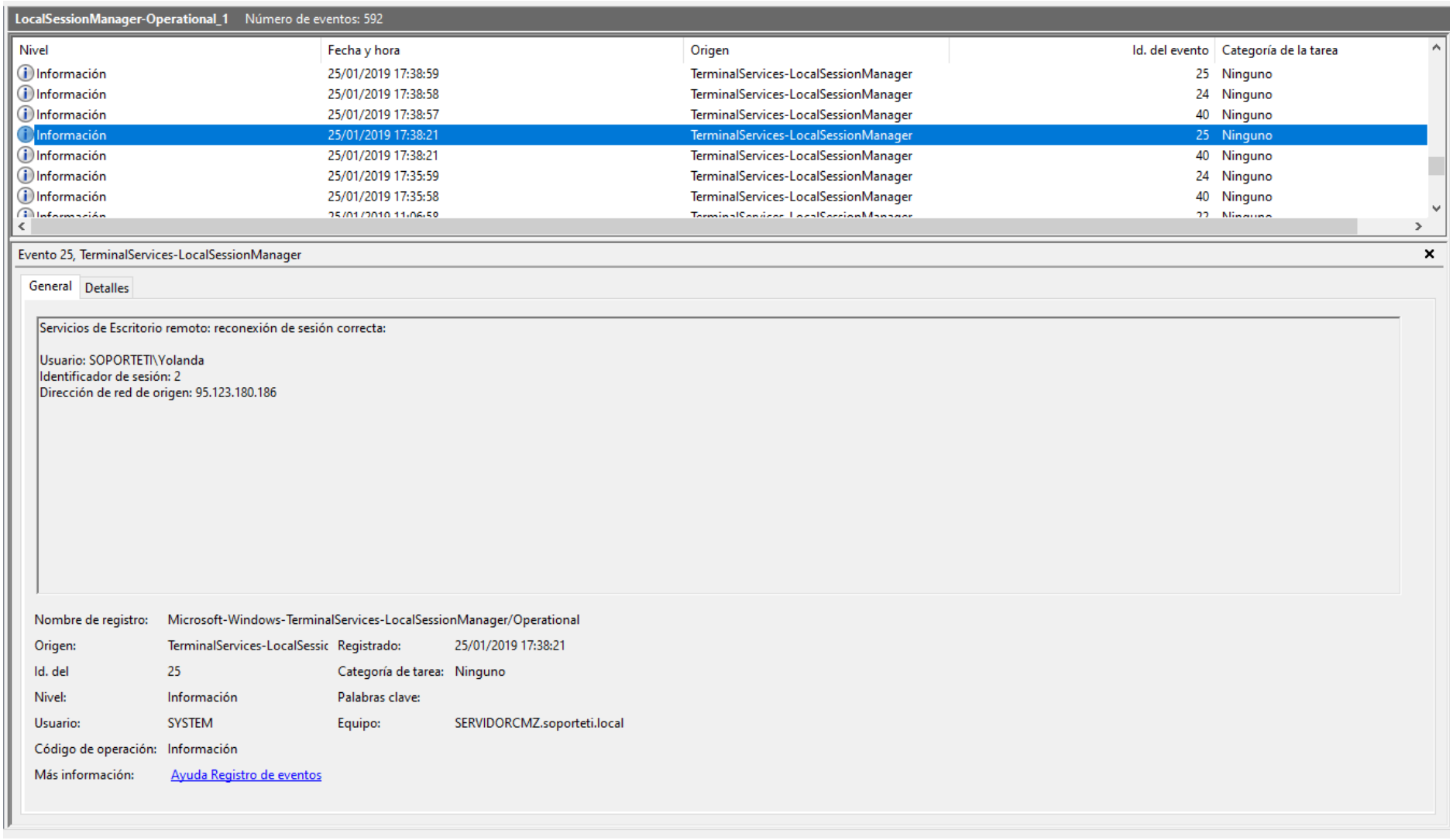
Nombre de registro:	Seguridad		
Origen:	Microsoft Windows security	Registrado:	18/03/2019 15:23:24
Id. del	5145	Categoría de tarea:	Detailed File Share
Nivel:	Información	Palabras clave:	Auditoría correcta
Usuario:	No disponible	Equipo:	PC01.example.corp
Código de operación:	Información		
Más información:	Ayuda Registro de eventos		

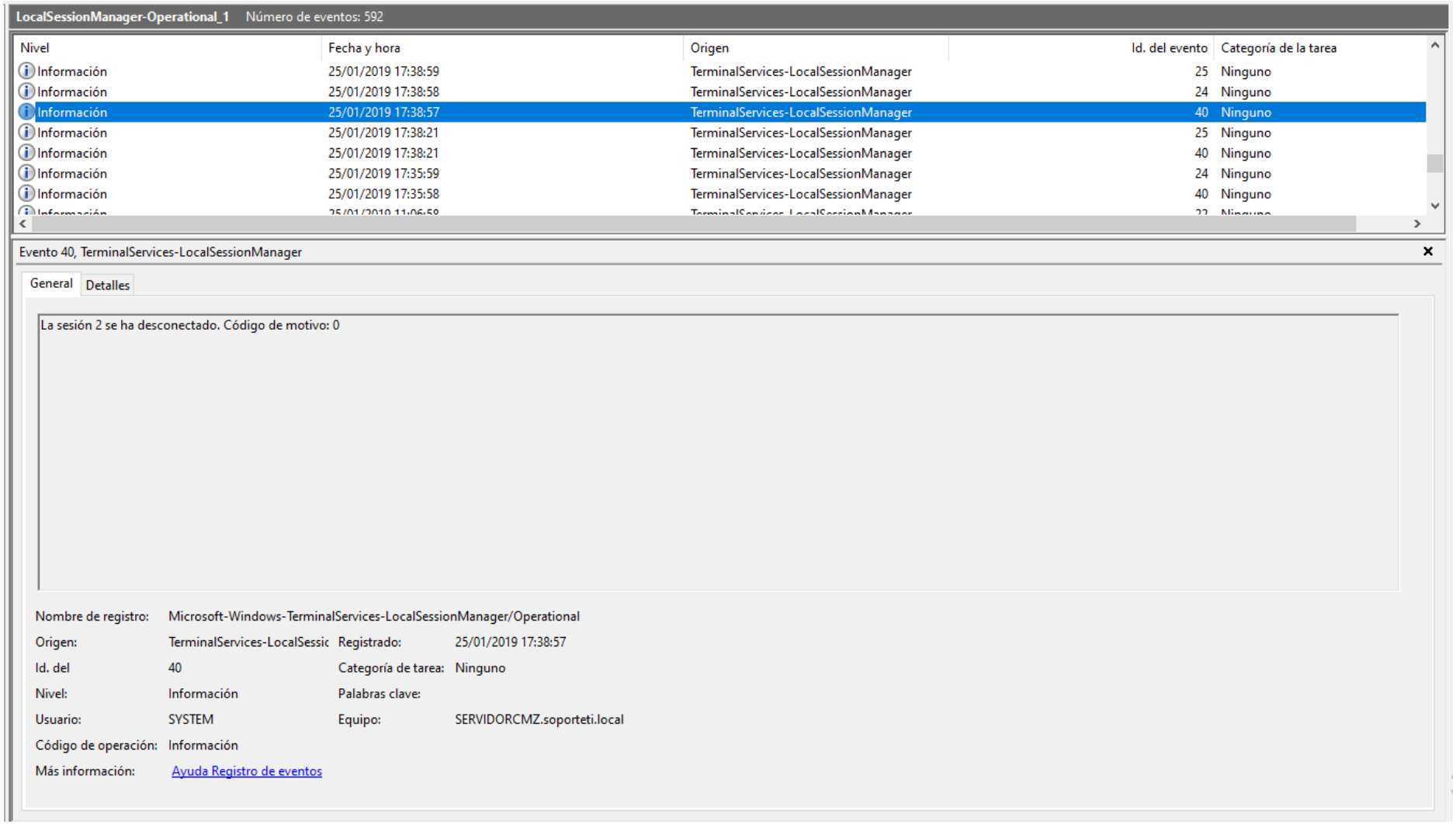
LocalSessionManager - Operational.evtx

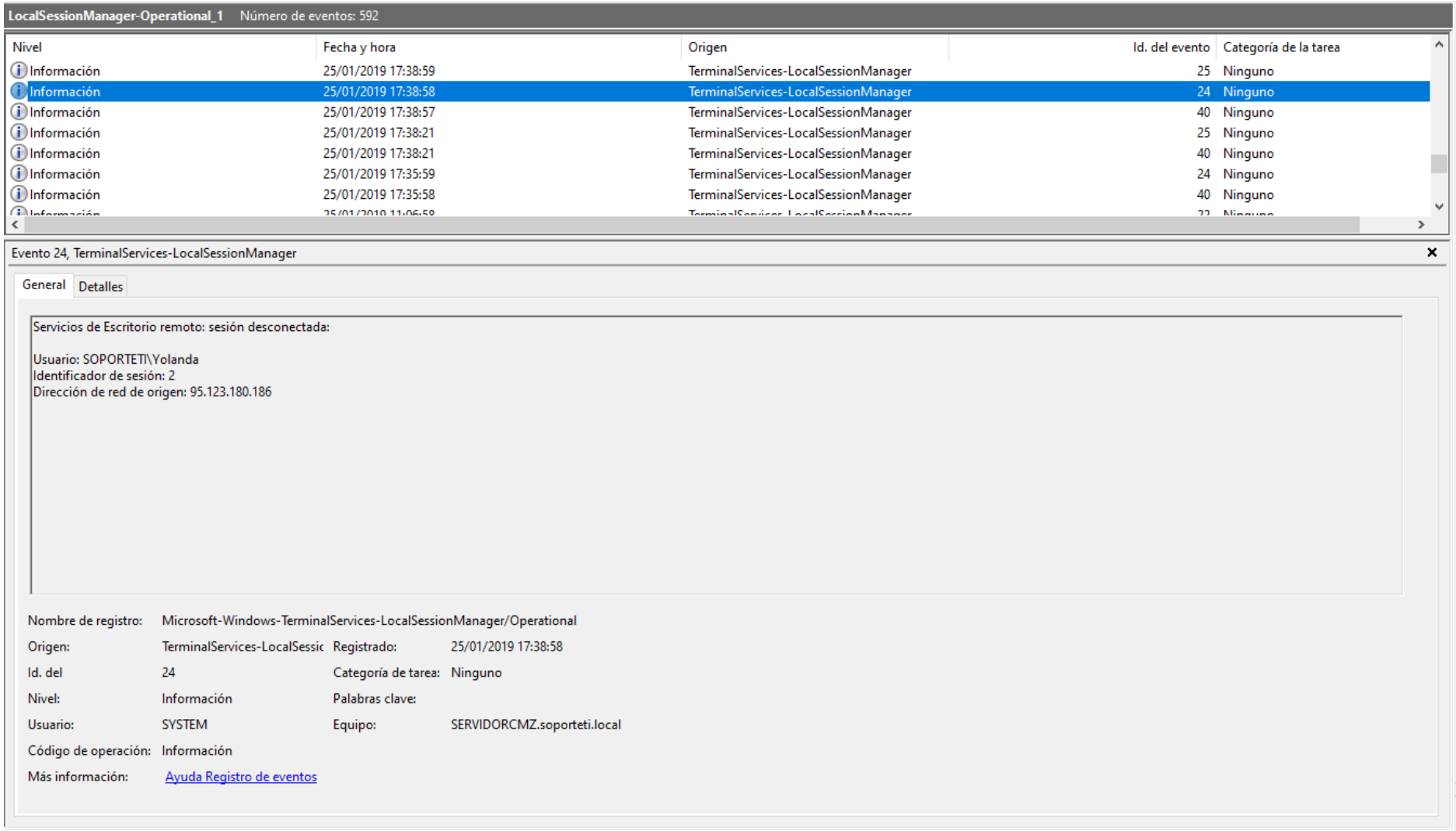


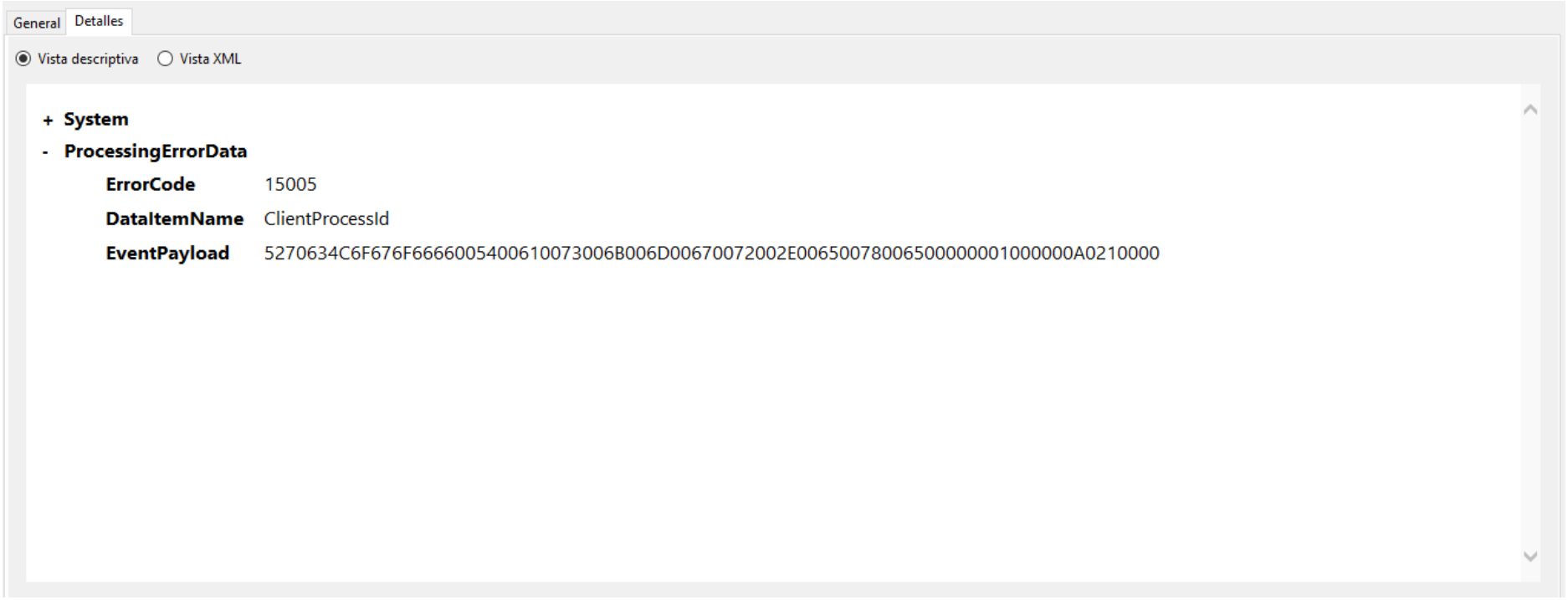

LocalSessionManager-Operational_1 Número de eventos: 592
Nivel Fecha y hora Origen Id. del evento Categoría de la tarea
Información 21/01/2019 18:48:56 TerminalServices-LocalSessionManager 40 Ninguno
Información 21/01/2019 18:48:56 TerminalServices-LocalSessionManager 41 Ninguno
Información 21/01/2019 13:47:39 TerminalServices-LocalSessionManager 24 Ninguno
Información 21/01/2019 13:47:39 TerminalServices-LocalSessionManager 40 Ninguno
Información 21/01/2019 10:56:17 TerminalServices-LocalSessionManager 22 Ninguno
Información 21/01/2019 10:56:17 TerminalServices-LocalSessionManager 21 Ninguno
Información 21/01/2019 10:56:16 TerminalServices-LocalSessionManager 42 Ninguno
Evento 22, TerminalServices-LocalSessionManager
General Detalles
Servicios de Escritorio remoto: notificación de inicio de shell recibida:
Usuario: SOPORTETI\Yolanda
Identificador de sesión: 2
Dirección de red de origen: 83.58.250.22
Nombre de registro: Microsoft-Windows-TerminalServices-LocalSessionManager/Operational
Origen: TerminalServices-LocalSessic Registrado: 21/01/2019 10:56:17
Id. del 22 Categoría de tarea: Ninguno
Nivel: Información Palabras clave:
Usuario: SYSTEM Equipo: SERVIDORCMZ.soporteti.local
Código de operación: Información
Más información: Ayuda Registro de eventos


LocalSessionManager-Operational_1 Número de eventos: 592
Nivel Fecha y hora Origen Id. del evento Categoría de la tarea
Información 21/01/2019 18:48:56 TerminalServices-LocalSessionManager 40 Ninguno
Información 21/01/2019 18:48:56 TerminalServices-LocalSessionManager 41 Ninguno
Información 21/01/2019 13:47:39 TerminalServices-LocalSessionManager 24 Ninguno
Información 21/01/2019 13:47:39 TerminalServices-LocalSessionManager 40 Ninguno
Información 21/01/2019 10:56:17 TerminalServices-LocalSessionManager 22 Ninguno
Información 21/01/2019 10:56:17 TerminalServices-LocalSessionManager 21 Ninguno
Información 21/01/2019 10:56:16 TerminalServices-LocalSessionManager 42 Ninguno
Evento 40, TerminalServices-LocalSessionManager
General Detalles
La sesión 2 se ha desconectado. Código de motivo: 0
Nombre de registro: Microsoft-Windows-TerminalServices-LocalSessionManager/Operational
Origen: TerminalServices-LocalSessic Registrado: 21/01/2019 13:47:39
Id. del 40 Categoría de tarea: Ninguno
Nivel: Información Palabras clave:
Usuario: SYSTEM Equipo: SERVIDORCMZ.soporteti.local
Código de operación: Información
Más información: Ayuda Registro de eventos


LocalSessionManager-Operational_1 Número de eventos: 592
Nivel
Fecha y hora
Origen
Id. del evento
Categoría de la tarea
Información 25/01/2019 17:38:59 TerminalServices-LocalSessionManager 25 Ninguno
Información 25/01/2019 17:38:58 TerminalServices-LocalSessionManager 24 Ninguno
Información 25/01/2019 17:38:57 TerminalServices-LocalSessionManager 40 Ninguno
Información 25/01/2019 17:38:21 TerminalServices-LocalSessionManager 25 Ninguno
Información 25/01/2019 17:38:21 TerminalServices-LocalSessionManager 40 Ninguno
Información 25/01/2019 17:35:59 TerminalServices-LocalSessionManager 24 Ninguno
Información 25/01/2019 17:35:58 TerminalServices-LocalSessionManager 40 Ninguno
Evento 25, TerminalServices-LocalSessionManager
General
Detalles
Servicios de Escritorio remoto: reconexión de sesión correcta:
Usuario: SOPORTETI\Yolanda
Identificador de sesión: 2
Dirección de red de origen: 95.123.180.186
Nombre de registro: Microsoft-Windows-TerminalServices-LocalSessionManager/Operational
Origen: TerminalServices-LocalSessic
Registrado: 25/01/2019 17:38:21
Id. del 25
Categoría de tarea: Ninguno
Nivel: Información
Palabras clave:
Usuario: SYSTEM
Equipo: SERVIDORCMZ.soporteti.local
Código de operación: Información
Más información: Ayuda Registro de eventos


LocalSessionManager-Operational_1 Número de eventos: 592
Nivel Fecha y hora Origen Id. del evento Categoría de la tarea
Información 25/01/2019 17:38:59 TerminalServices-LocalSessionManager 25 Ninguno
Información 25/01/2019 17:38:58 TerminalServices-LocalSessionManager 24 Ninguno
Información 25/01/2019 17:38:57 TerminalServices-LocalSessionManager 40 Ninguno
Información 25/01/2019 17:38:21 TerminalServices-LocalSessionManager 25 Ninguno
Información 25/01/2019 17:38:21 TerminalServices-LocalSessionManager 40 Ninguno
Información 25/01/2019 17:35:59 TerminalServices-LocalSessionManager 24 Ninguno
Información 25/01/2019 17:35:58 TerminalServices-LocalSessionManager 40 Ninguno
Evento 40, TerminalServices-LocalSessionManager
General Detalles
La sesión 2 se ha desconectado. Código de motivo: 0
Nombre de registro: Microsoft-Windows-TerminalServices-LocalSessionManager/Operational
Origen: TerminalServices-LocalSessic Registrado: 25/01/2019 17:38:57
Id. del 40 Categoría de tarea: Ninguno
Nivel: Información Palabras clave:
Usuario: SYSTEM Equipo: SERVIDORCMZ.soporteti.local
Código de operación: Información
Más información: Ayuda Registro de eventos

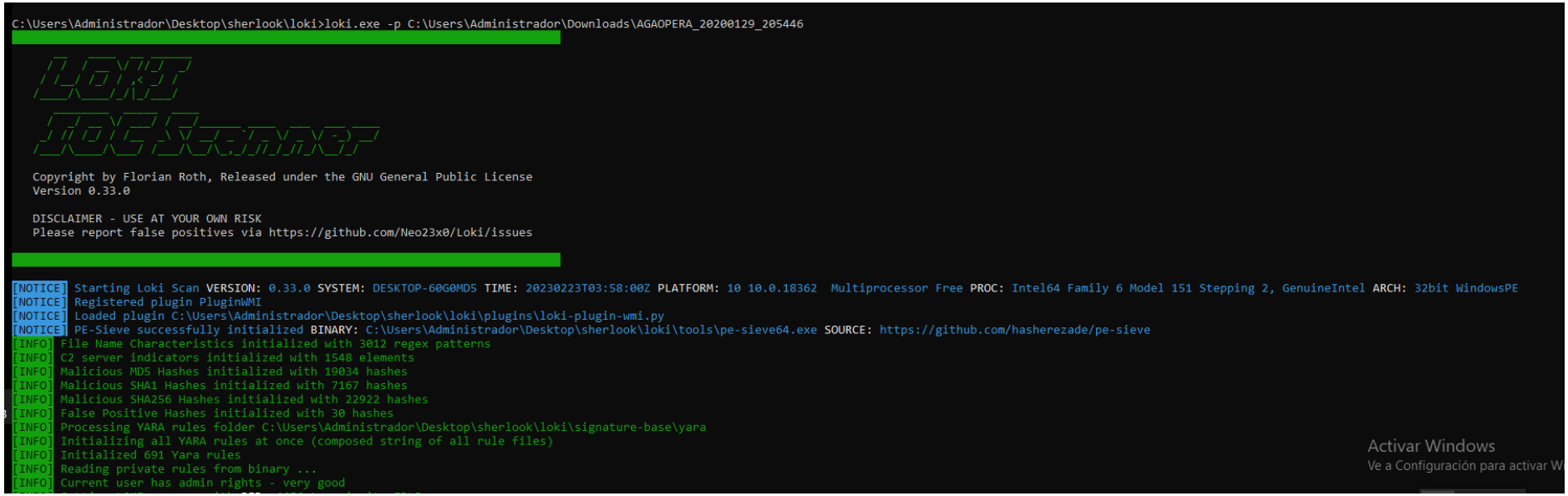

LocalSessionManager-Operational_1 Número de eventos: 592
Nivel Fecha y hora Origen Id. del evento Categoría de la tarea
Información 25/01/2019 17:38:59 TerminalServices-LocalSessionManager 25 Ninguno
Información 25/01/2019 17:38:58 TerminalServices-LocalSessionManager 24 Ninguno
Información 25/01/2019 17:38:57 TerminalServices-LocalSessionManager 40 Ninguno
Información 25/01/2019 17:38:21 TerminalServices-LocalSessionManager 25 Ninguno
Información 25/01/2019 17:38:21 TerminalServices-LocalSessionManager 40 Ninguno
Información 25/01/2019 17:35:59 TerminalServices-LocalSessionManager 24 Ninguno
Información 25/01/2019 17:35:58 TerminalServices-LocalSessionManager 40 Ninguno
Evento 24, TerminalServices-LocalSessionManager
General Detalles
Servicios de Escritorio remoto: sesión desconectada:
Usuario: SOPORTETI\Yolanda
Identificador de sesión: 2
Dirección de red de origen: 95.123.180.186
Nombre de registro: Microsoft-Windows-TerminalServices-LocalSessionManager/Operational
Origen: TerminalServices-LocalSessic Registrado: 25/01/2019 17:38:58
Id. del 24 Categoría de tarea: Ninguno
Nivel: Información Palabras clave:
Usuario: SYSTEM Equipo: SERVIDORCMZ.soporteti.local
Código de operación: Información
Más información: Ayuda Registro de eventos

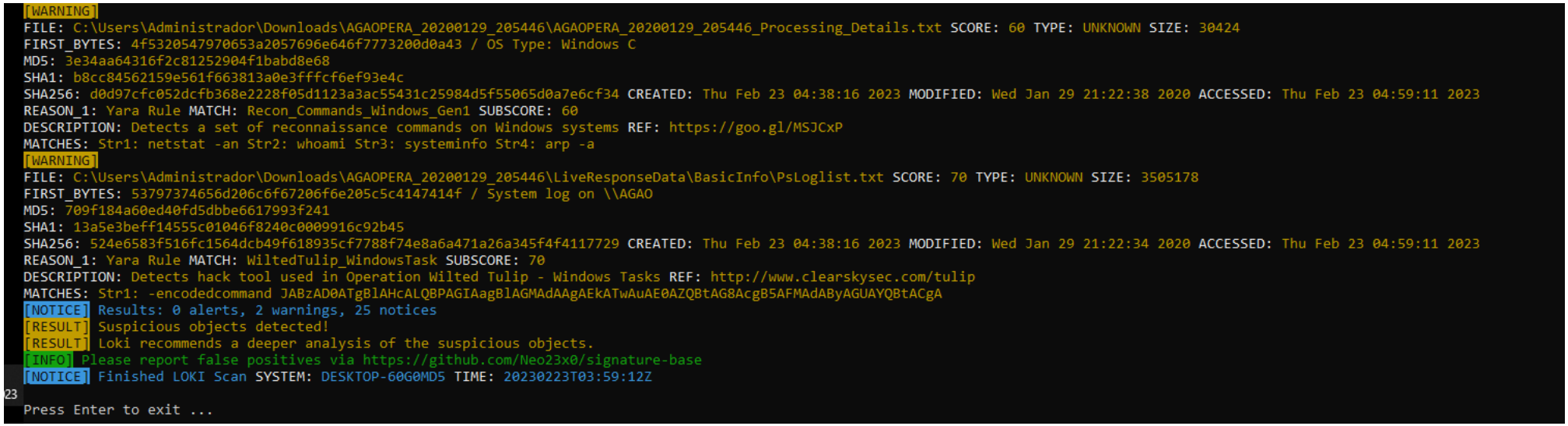

General
Detalles
Vista descriptiva
Vista XML
+ System
- ProcessingErrorData
ErrorCode 15005
DataItemName ClientProcessId
EventPayload 5270634C6F676F6666005400610073006B006D00670072002E0065007800650000000100000A0210000

3.6. Realiza un análisis con Loki identificando indicadores de compromiso en los archivos del siguiente fichero.

- Ficheros necesarios para el ejercicio: AGAOPERA_20200129_205446.zip

Artefacto	Tipo de Compromiso
AGAOPERA_20200129_203446_Processing_Details.txt	detecta un conjunto de comandos de reconocimiento en el sistema de Windows
AGAOPERA_20200129_205446\LiveResponseData\BasicInfo\PsLoglist.txt	Detecta la herramienta de pirateo utilizada en la Operación Tulipán marchito - Tareas de Windows




[WARNING]
FILE: C:\Users\Administrador\Downloads\AGAOPERA_20200129_205446\AGAOPERA_20200129_205446_Processing_Details.txt SCORE: 60 TYPE: UNKNOWN SIZE: 30424
FIRST_BYTES: 4f5320547970653a2057696e646f7773200d0a43 / OS Type: Windows C
MD5: 3e34aa64316f2c81252904f1babd8e68
SHA1: b8cc84562159e561f663813a0e3fffcf6ef93e4c
SHA256: d0d97cfc052dcfb368e2228f05d1123a3ac55431c25984d5f55065d0a7e6cf34 CREATED: Thu Feb 23 04:38:16 2023 MODIFIED: Wed Jan 29 21:22:38 2020 ACCESSED: Thu Feb 23 04:59:11 2023
REASON_1: Yara Rule MATCH: Recon_Commands_Windows_Gen1 SUBSCORE: 60
DESCRIPTION: Detects a set of reconnaissance commands on Windows systems REF: https://goo.gl/MSJCxP
MATCHES: Str1: netstat -an Str2: whoami Str3: systeminfo Str4: arp -a
[WARNING]
FILE: C:\Users\Administrador\Downloads\AGAOPERA_20200129_205446\LiveResponseData\BasicInfo\PsLoglist.txt SCORE: 70 TYPE: UNKNOWN SIZE: 3505178
FIRST_BYTES: 53797374656d206c6f67206f6e205c5c4147414f / System log on \\AGAO
MD5: 709f184a60ed40fd5dbbe6617993f241
SHA1: 13a5e3beff14555c01046f8240c0009916c92b45
SHA256: 524e6583f516fc1564dcb49f618935cf7788f74e8a6a471a26a345f4f4117729 CREATED: Thu Feb 23 04:38:16 2023 MODIFIED: Wed Jan 29 21:22:34 2020 ACCESSED: Thu Feb 23 04:59:11 2023
REASON_1: Yara Rule MATCH: WiltedTulip_WindowsTask SUBSCORE: 70
DESCRIPTION: Detects hack tool used in Operation Wilted Tulip - Windows Tasks REF: http://www.clearskysec.com/tulip
MATCHES: Str1: -encodedcommand JABzAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgA
[NOTICE] Results: 0 alerts, 2 warnings, 25 notices
[RESULT] Suspicious objects detected!
[RESULT] Loki recommends a deeper analysis of the suspicious objects.
[INFO] Please report false positives via https://github.com/Neo23x0/signature-base
[NOTICE] Finished LOKI Scan SYSTEM: DESKTOP-60G0MD5 TIME: 20230223T03:59:12Z
23
Press Enter to exit ...