



# Cybersecurity Bootcamp

---

U2M2 - Análisis Forense y Respuesta ante Incidentes (DFIR)

Análisis

## Índice

<b>Análisis</b>	<b>3</b>
<i>3.1. Extrae las firmas hash de los siguientes ficheros</i>	<i>3</i>
<i>3.2. Realiza una imagen forense de un dispositivo externo y extrae ficheros de dicha imagen.</i>	<i>6</i>
<i>3.3. Monta la imagen forense indicada y extrae ficheros de dicha imagen.</i>	<i>17</i>
<i>3.4. Identifica empleando fuentes públicas y las muestras de archivos proporcionadas, qué tipo de familia de ransomware ha cifrado los siguientes archivos.</i>	<i>21</i>
<i>3.5. Trata de identificar en los siguientes logs de eventos de Windows actividad maliciosa o ilegítima.</i>	<i>22</i>
<i>3.6. Realiza un análisis con Loki identificando indicadores de compromiso en los archivos del siguiente fichero.</i>	<i>25</i>

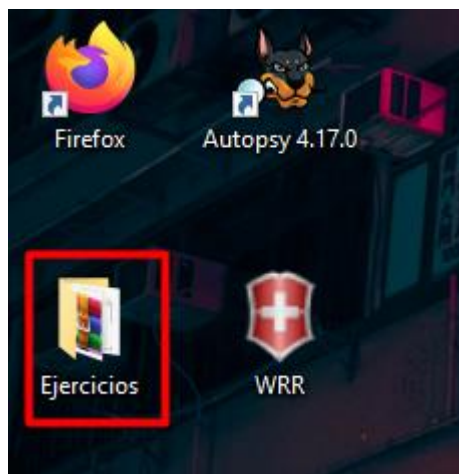
# Análisis

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.

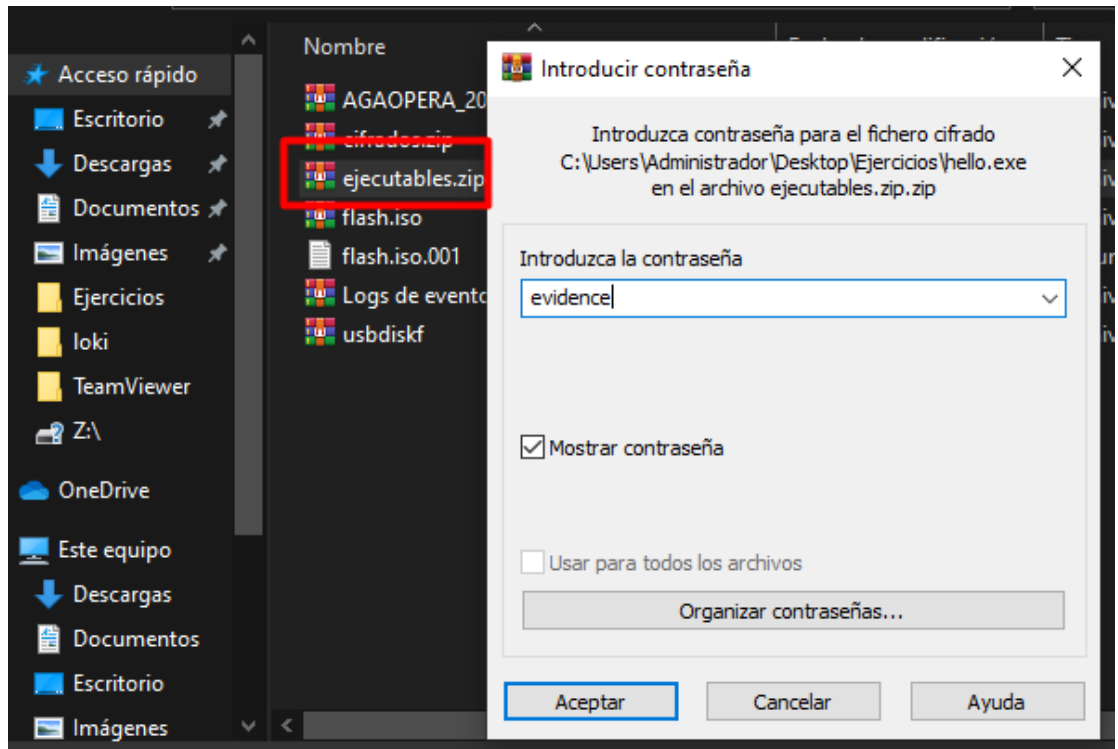
Recuerda que puedes adaptar el tamaño de recursos de la memoria RAM del host que quieres asignarle a la máquina (6GB por defecto).

## 3.1. Extrae las firmas hash de los siguientes ficheros

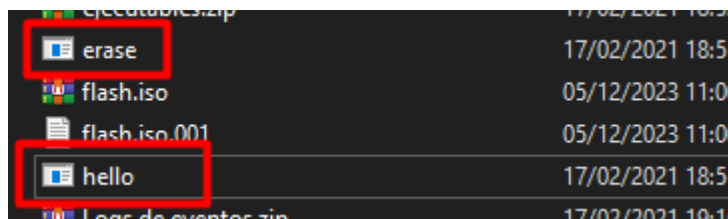
- Ficheros necesarios para el ejercicio: ejecutables.zip (contraseña para descomprimir: *evidence*, dentro se encuentran los archivos hello.exe y erase.exe)  
Abrimos la carpeta de ejercicios



Descomprimos la carpeta

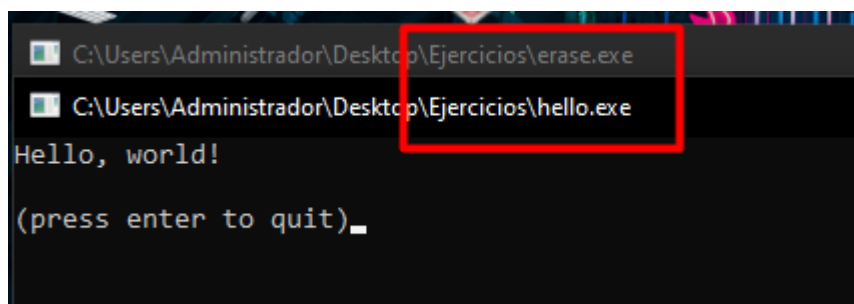


Como resultado tenemos esto



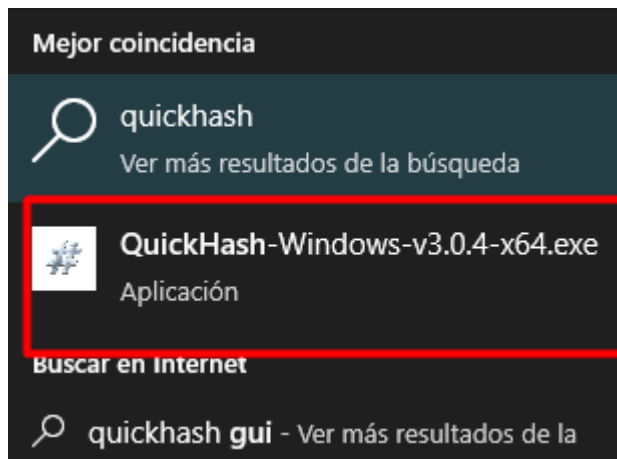
- Primero, ejecuta ambos ficheros (no hay riesgo de compromiso de ningún tipo, y no son necesarios privilegios de administración para su ejecución).

Ejecutamos los dos ficheros

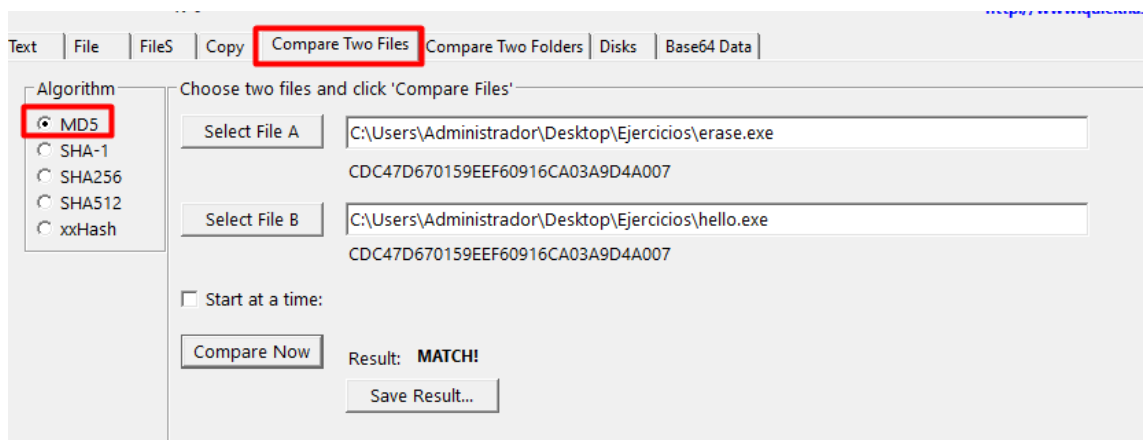


- ¿Son ambos archivos el mismo fichero?
- No
- Calcula las firmas hash MD5 y SHA1 para ambos ficheros.

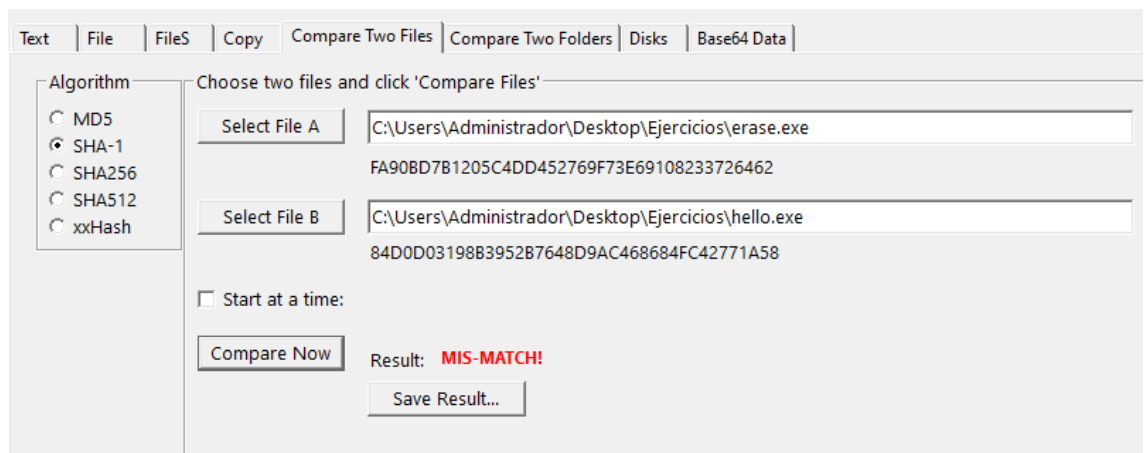
Para esto, utilizamos la siguiente herramienta



Primero vamos con el algoritmo MD5

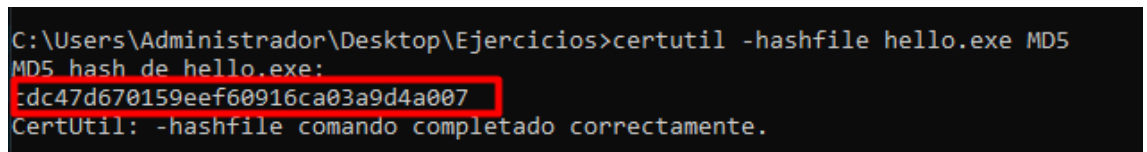


Después cambiamos el algoritmo



Desde el CMD también se puede obtener de la siguiente manera

MD5:



```
C:\Users\Administrador\Desktop\Ejercicios>certutil -hashfile erase.exe MD5
MD5 hash de erase.exe:
cdc47d670159eef60916ca03a9d4a007
CertUtil: -hashfile comando completado correctamente.
```

SHA-1

```
C:\Users\Administrador\Desktop\Ejercicios>certutil -hashfile hello.exe SHA1
SHA1 hash de hello.exe:
84d0d03198b3952b7648d9ac468684fc42771a58
CertUtil: -hashfile comando completado correctamente.

C:\Users\Administrador\Desktop\Ejercicios>certutil -hashfile erase.exe SHA1
SHA1 hash de erase.exe:
fa90bd7b1205c4dd452769f73e69108233726462
CertUtil: -hashfile comando completado correctamente.
```

- ¿Qué conclusiones puedes extraer?

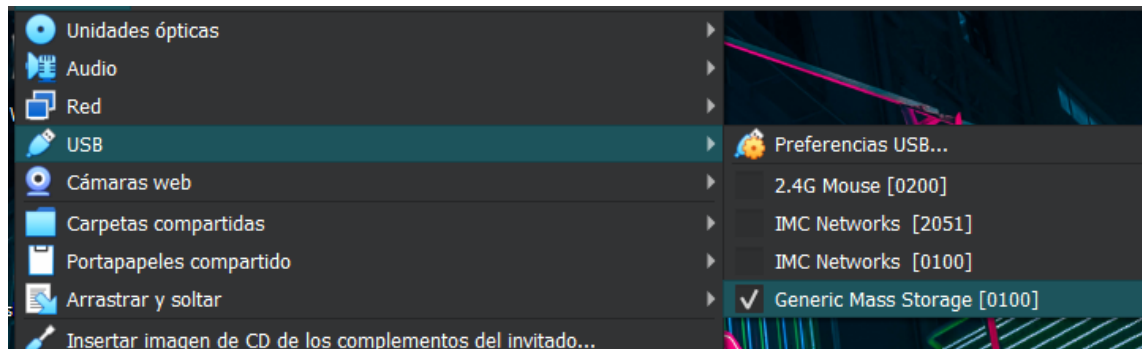
En resumen, al comparar dos archivos utilizando la firma hash MD5, se determinó que son idénticos. Sin embargo, al aplicar el algoritmo SHA-1 a ambos archivos, se observa una variación en el hash resultante, lo que indica que no son considerados como los mismos archivos bajo este algoritmo de hash específico.

Fichero	MD5	SHA1
hello.exe	cdc47d670159eef60916ca03a9d4a007	84d0d03198b3952b7648d9ac468684fc42771a58
erase.exe	cdc47d670159eef60916ca03a9d4a007	fa90bd7b1205c4dd452769f73e69108233726462

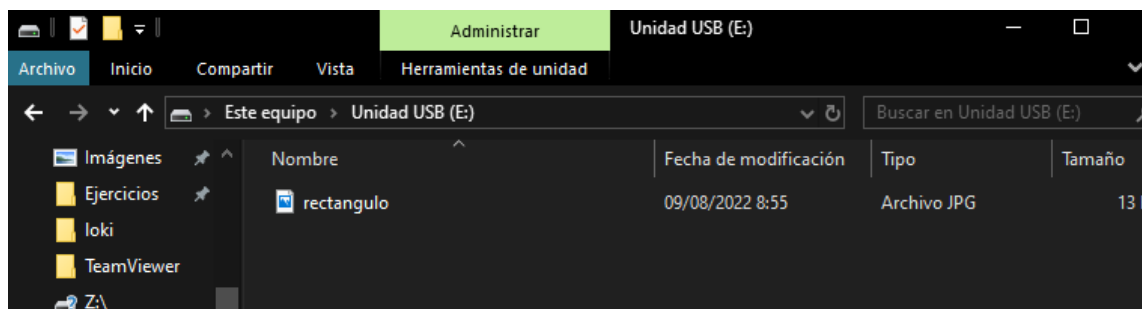
### 3.2. Realiza una imagen forense de un dispositivo externo y extrae ficheros de dicha imagen.

- Guía necesaria para el ejercicio:
- [http://www.reydes.com/d/?q=Crear\\_la\\_Imagen\\_Forense\\_desde\\_una\\_Unidad\\_utilizando\\_FTK\\_Imager](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).

Seleccionamos nuestra unidad USB en la máquina

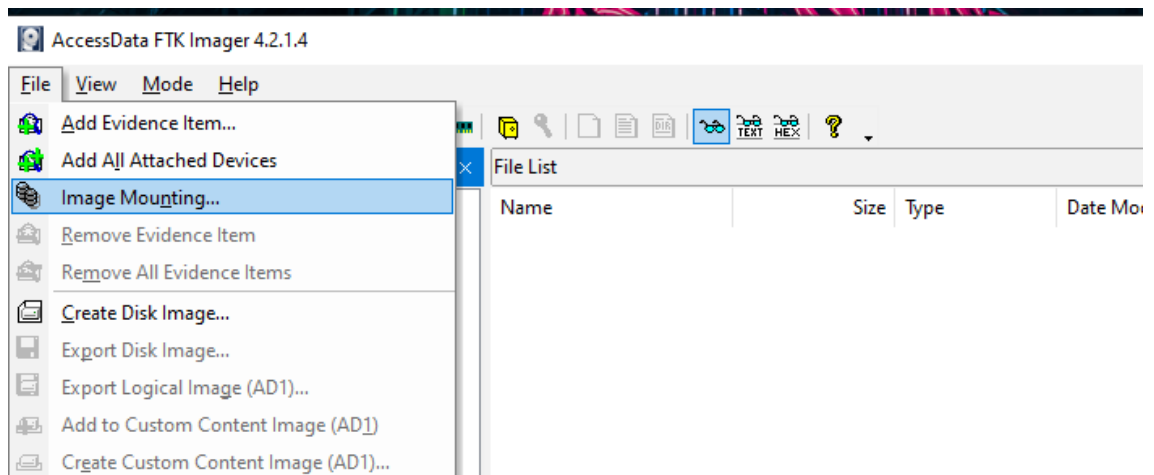


En la memoria dejamos un archivo para que pueda ser más visual el ejercicio que vamos a realizar

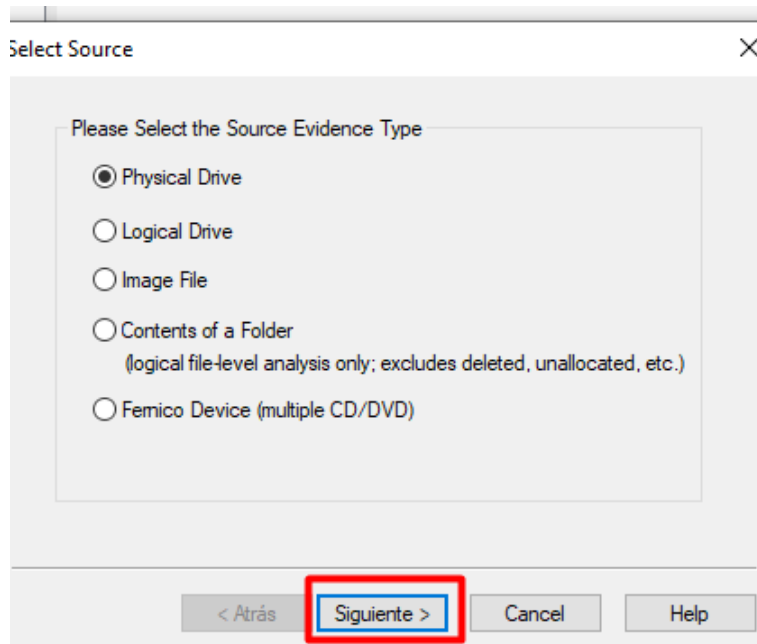


- Realiza una imagen forense completa de la unidad USB con la herramienta FTK Imager siguiendo las instrucciones que encontrarás en el manual.

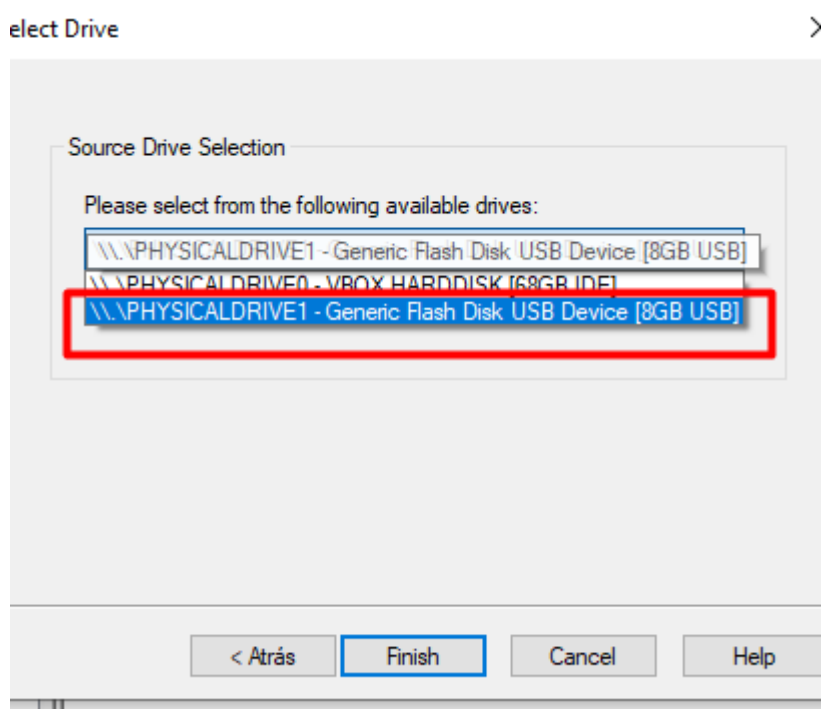
Para esto abrimos la herramienta y seguimos los siguientes pasos



Después de clicar *create disk image* continuamos con la selección predeterminada

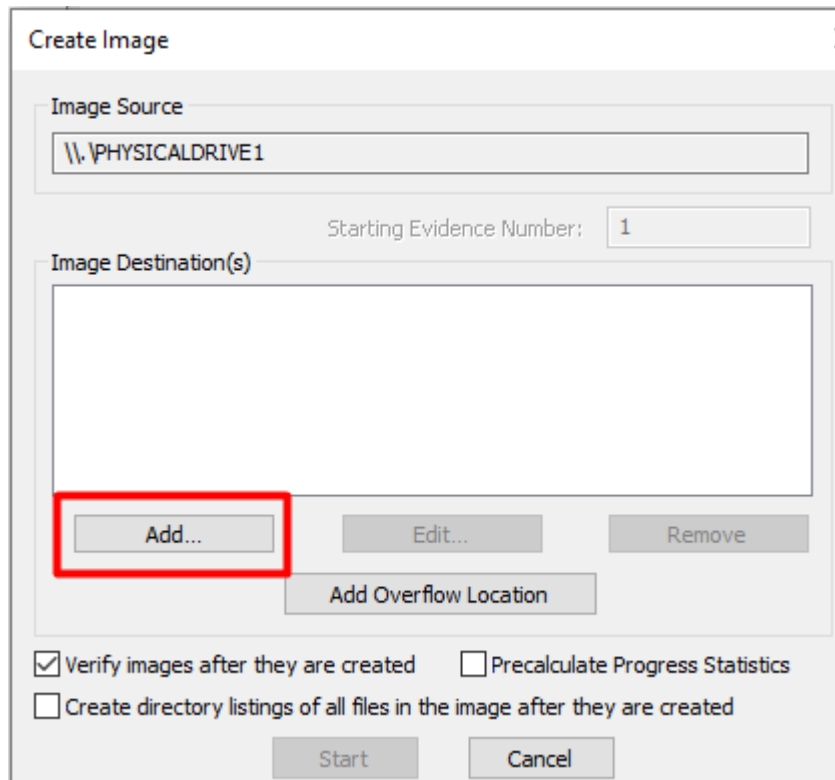


Seleccionamos la memoria



Y tras finalizar añadimos el tipo de imagen





Create Image

Image Source  
\\.\PHYSICALDRIVE1

Starting Evidence Number: 1

Image Destination(s)

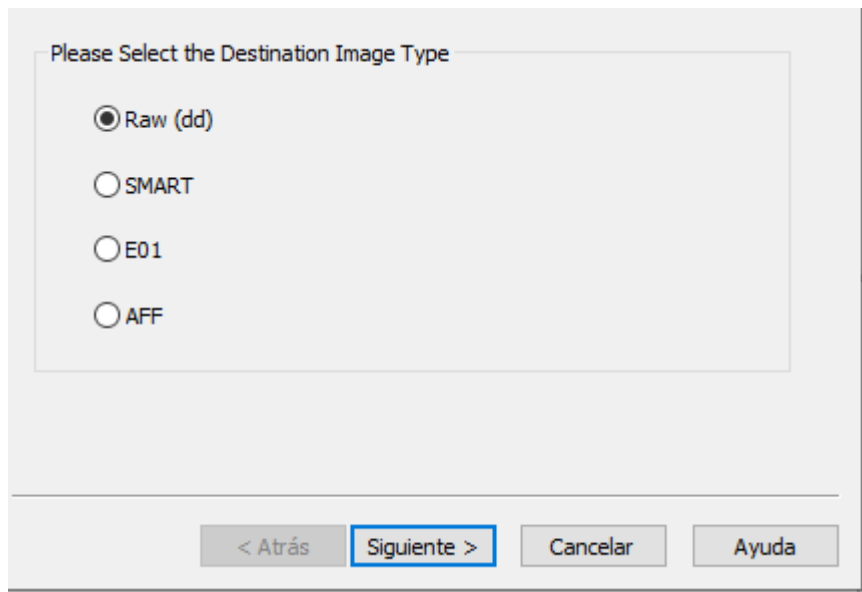
Add... Edit... Remove

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

Hecho esto dejamos la selección predeterminada



Please Select the Destination Image Type

☒ Raw (dd)  
☐ SMART  
☐ E01  
☐ AFF

< Atrás Siguiete > Cancelar Ayuda

Continuamos con la información complementaria

Evidence Item Information

Case Number: 0101

Evidence Number: 0101

Unique Description: -

Examiner: Ginner Baron

Notes:

< Atrás **Siguiente >** Cancel Help

Seleccionamos el destino y ponemos la fragmentación a 0 para que no la haga

Select Image Destination

Image Destination Folder  
C:\Users\Administrador\Desktop Browse

Image Filename (Excluding Extension)  
UnidadUSB

Image Fragment Size (MB) 0

For Raw, E01, and AFF formats: 0 = do not fragment

Compression (0=None, 1=Fastest, ..., 9=Smallest) 0

Use AD Encryption ☐

< Atrás **Finish** Cancel Help

Este es el resumen de nuestro procedimiento

Create Image

Image Source  
\\.\PHYSICALDRIVE1

Starting Evidence Number: 1

Image Destination(s)  
C:\Users\Administrador\Desktop\UnidadUSB [raw/dd]

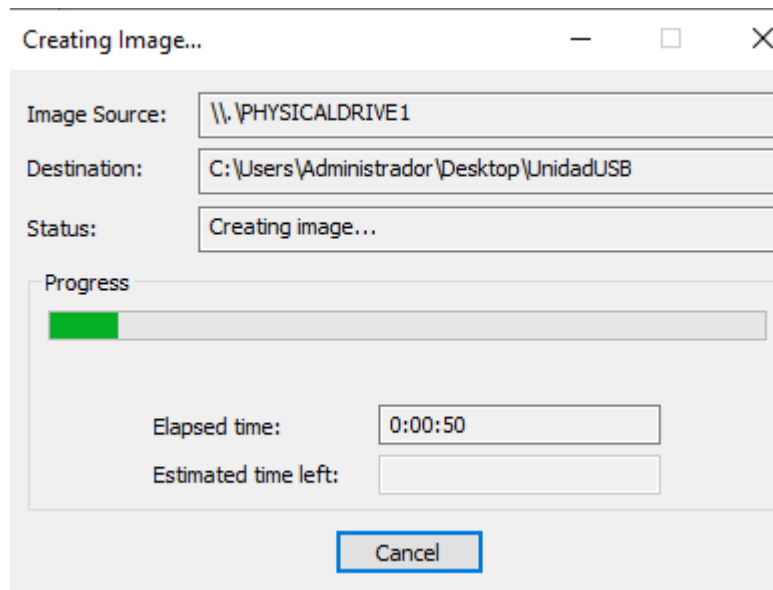
Add... Edit... Remove

Add Overflow Location

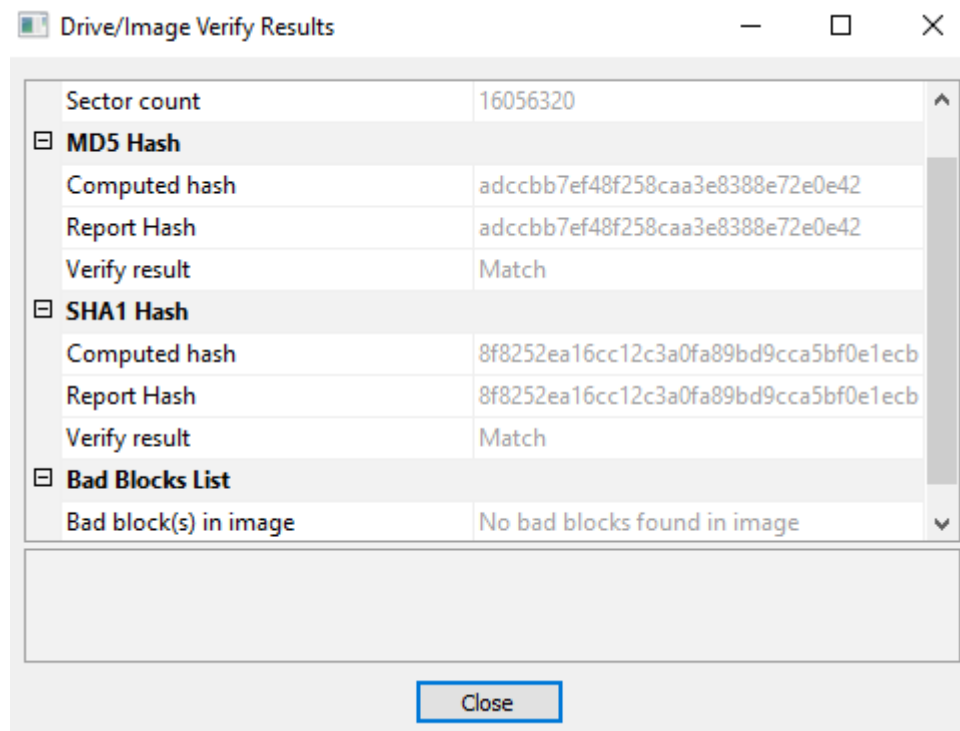
☒ Verify images after they are created ☐ Precalculate Progress Statistics

☐ Create directory listings of all files in the image after they are created

Start Cancel

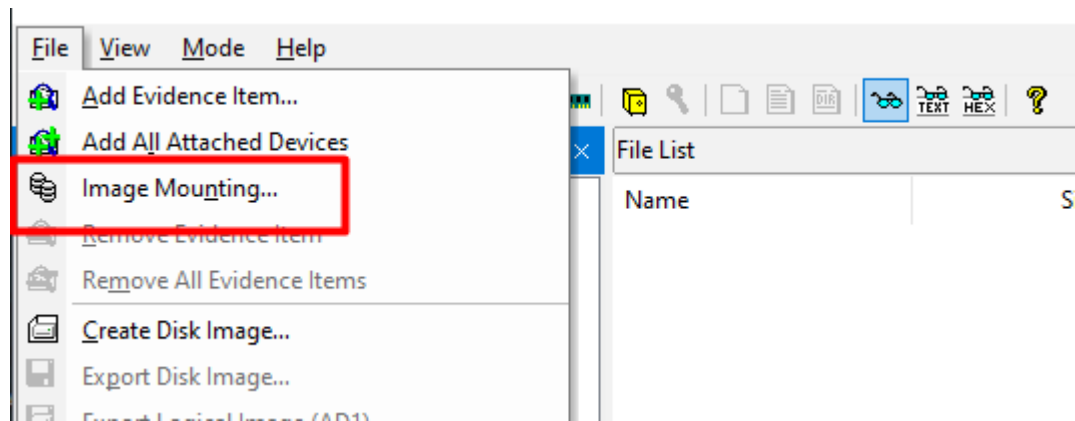


Como resultado tenemos lo siguiente

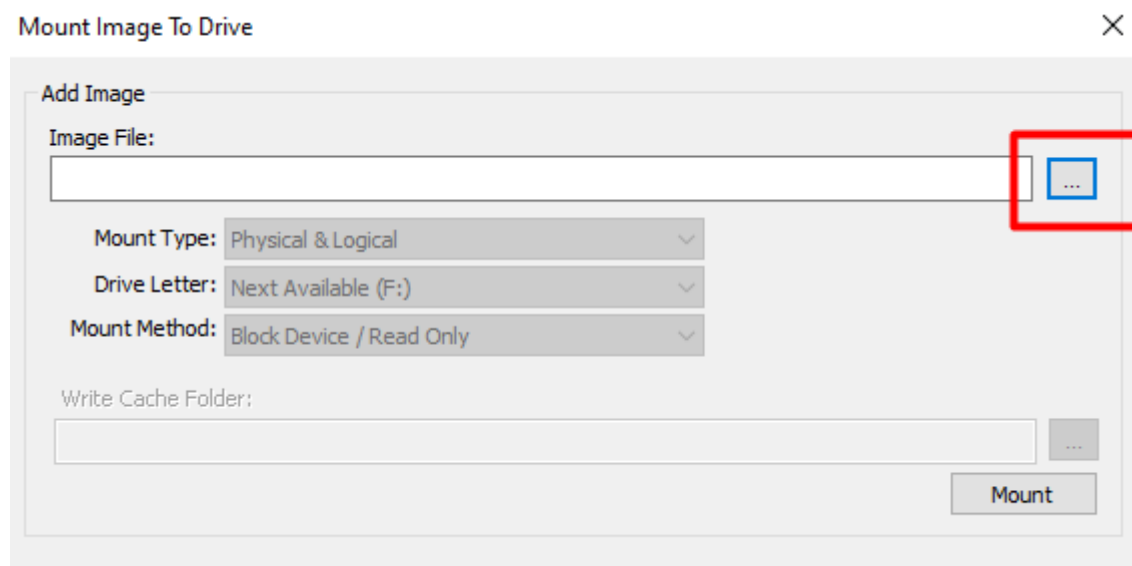


- Una vez generada la imagen, móntala con la herramienta FTK Imager y navega por el árbol de directorios del dispositivo.

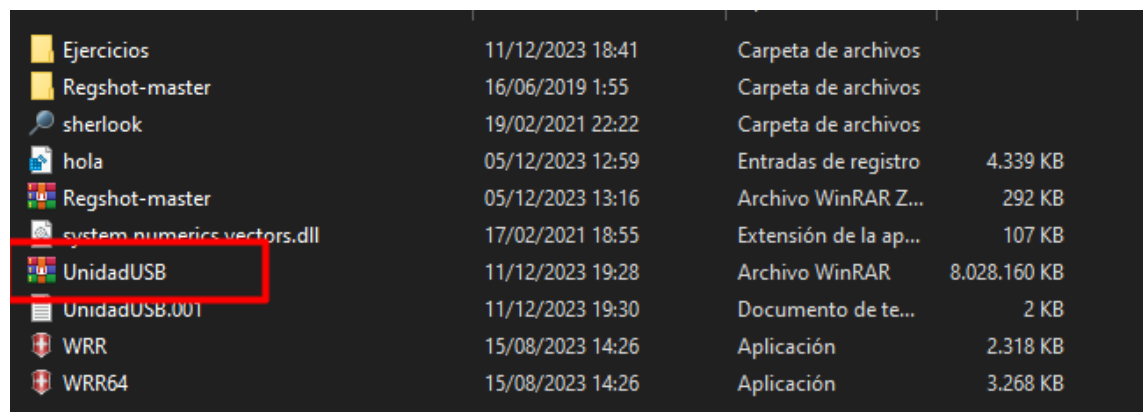
Para esto vamos a la pestaña file



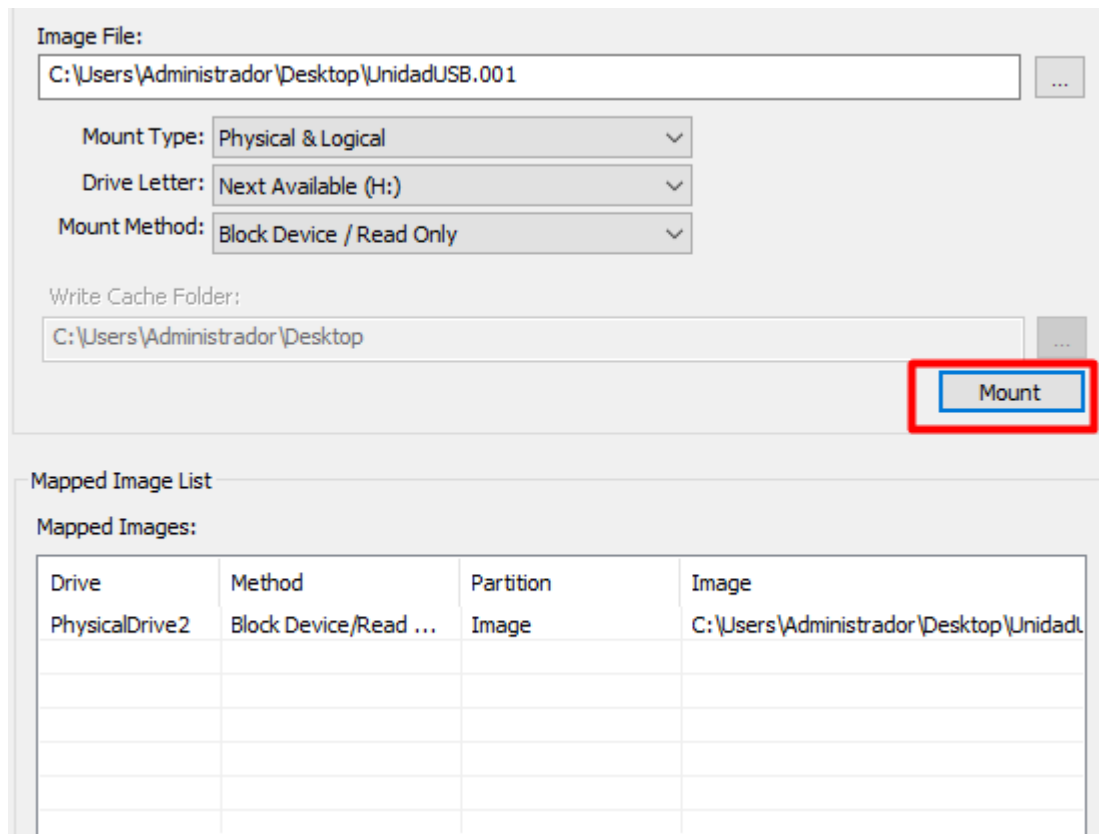
Seleccionamos los tres puntos



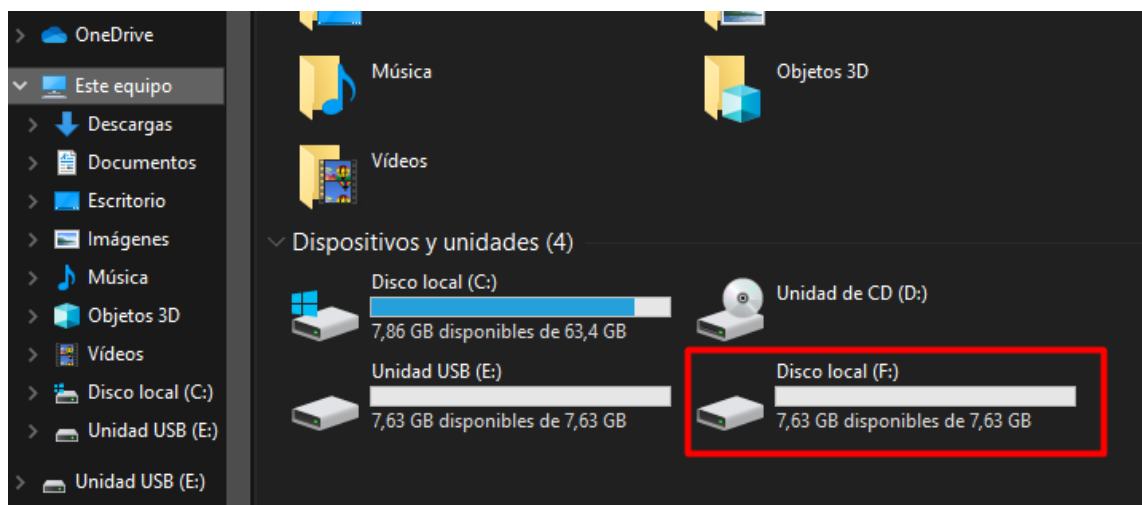
Seleccionamos nuestro archivo creado



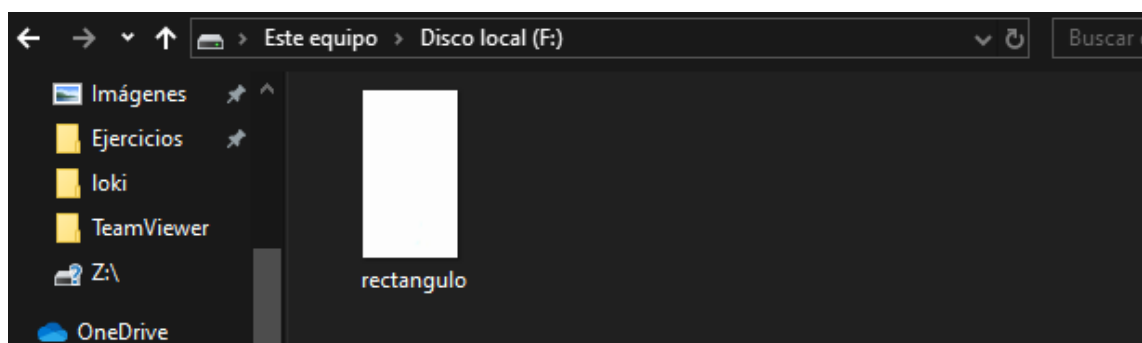
La montamos



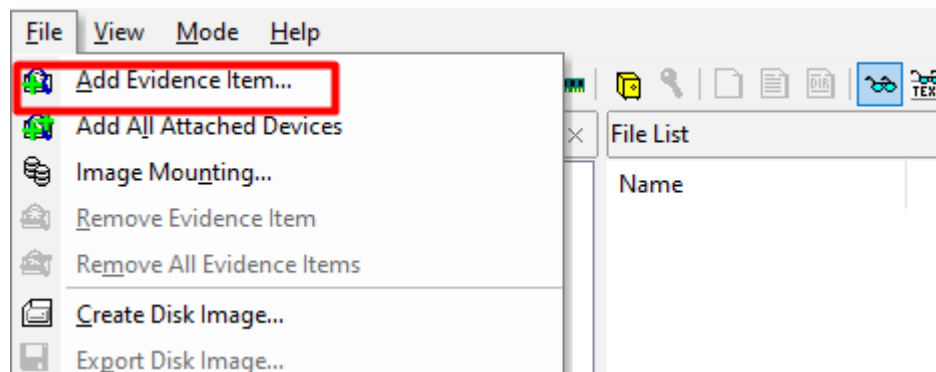
Como resultado tendríamos un nuevo disco



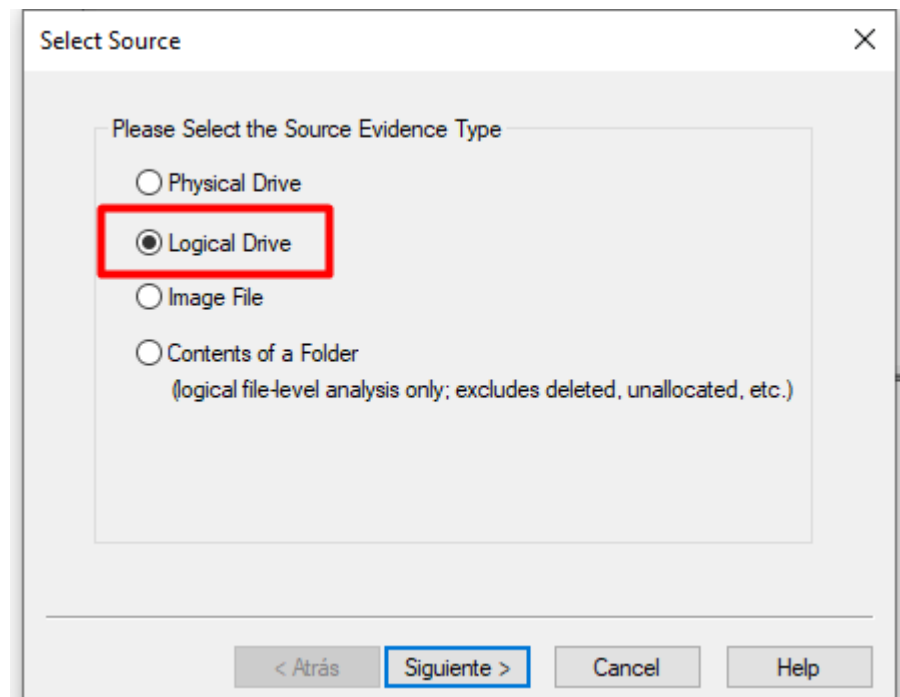
Y el contenido sería el siguiente



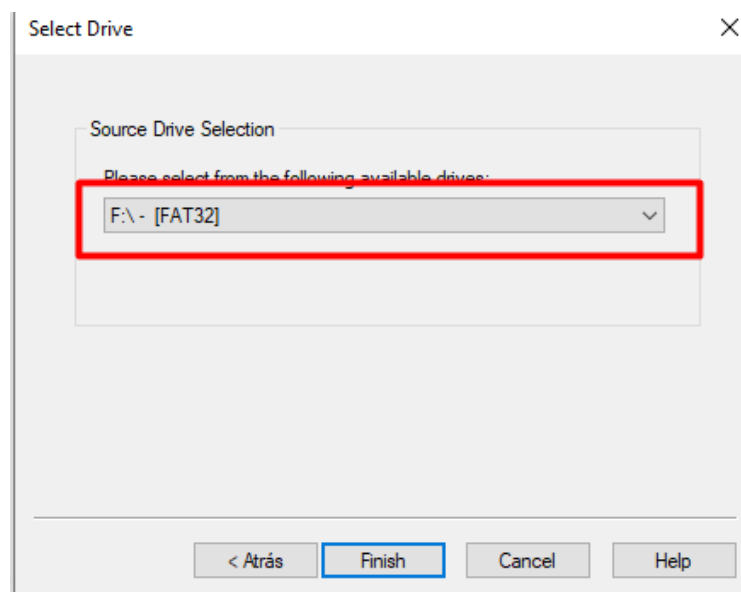
Para poder visualizarlo en la herramienta nos dirigimos a la siguiente pestaña



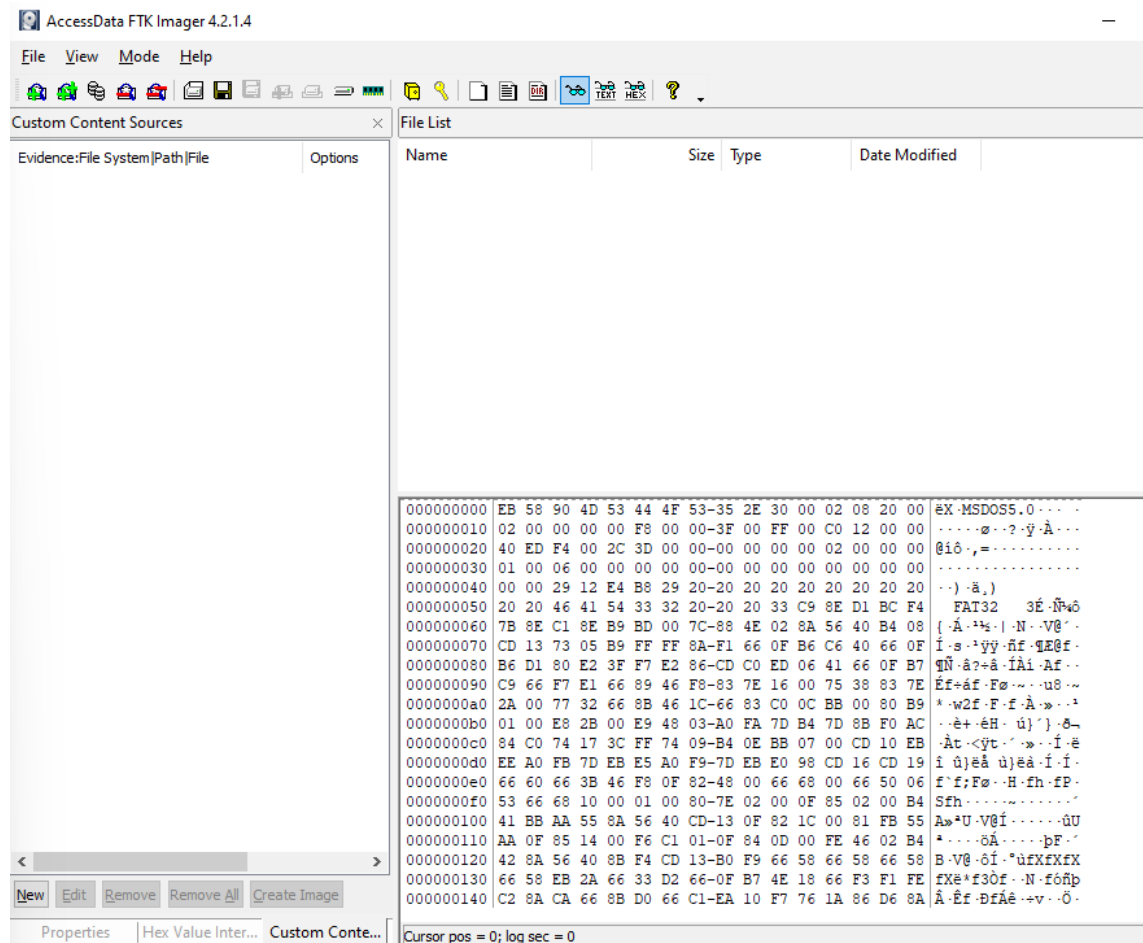
Cambiamos de tipo



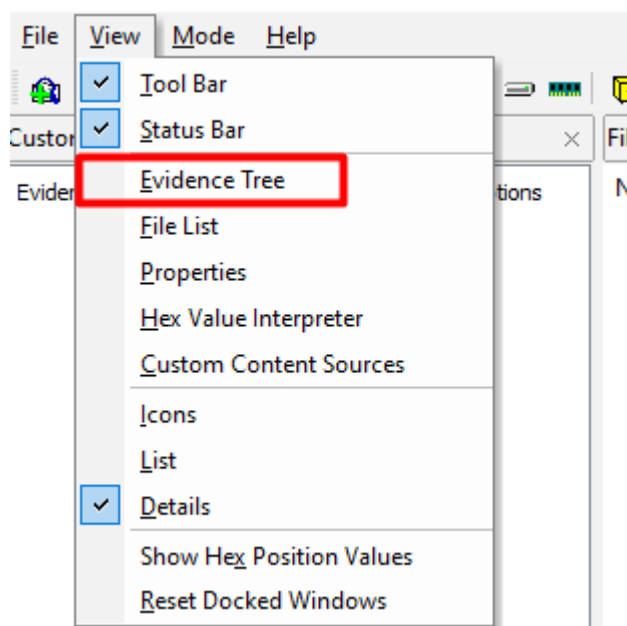
Cambiamos nuestro disco al F



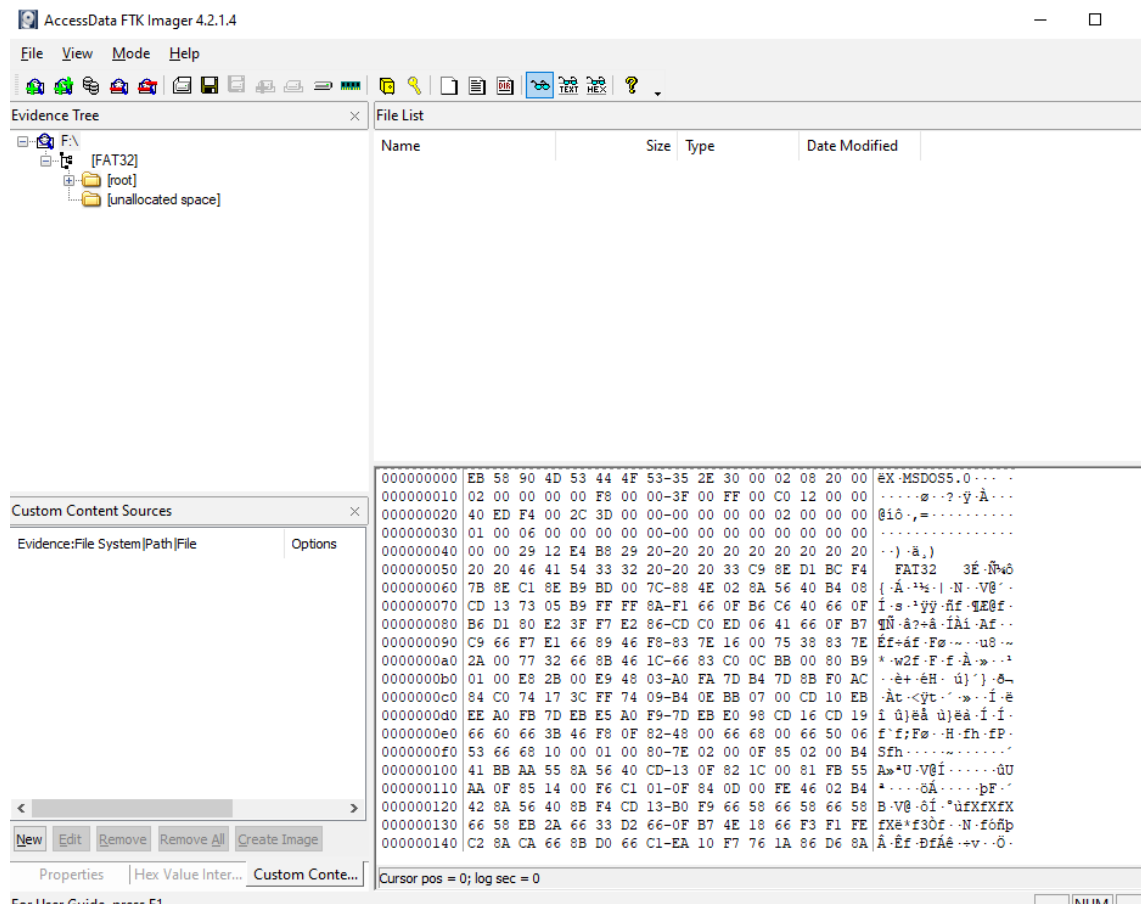
Y ya la tendríamos en nuestra herramienta



Para poder navegar abrimos la siguiente pestaña

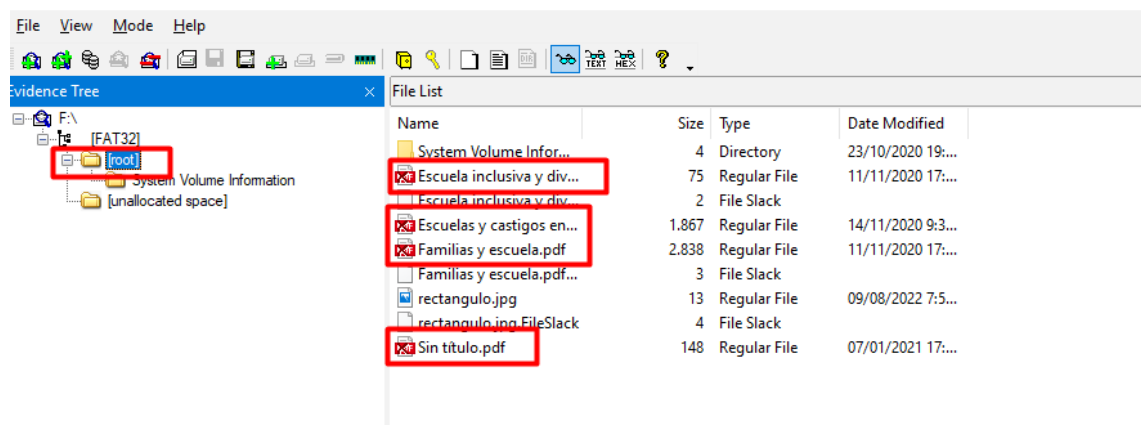


Y tendríamos la información estructurada de esta forma



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

Si nos dirigimos a la carpeta root obtenemos los siguientes archivos que estan marcados con una X lo que significa que son archivos eliminados





### 3.3. Monta la imagen forense indicada 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 ex empleado 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?  
FlashDisk
  - ¿En qué momento se modificó el contenido del USB por última vez?  
El día 10-03-2020
  - ¿Observas indicios de que se haya podido producir un potencial incidente de seguridad?  
Sí, existen datos médicos en el Excel de COVID
  - En caso afirmativo, ¿podrías indicar si resulta necesario notificar el incidente y ante qué organismos?  
Debes informar a la Agencia Española de Protección de Datos (AEPD) dentro de las 72 horas posteriores a la toma de conocimiento, utilizando el enlace provisto en su Sede electrónica
  - ¿Puedes identificar alguna información adicional del presunto dueño del USB (nombre, aficiones, etc.)?  
El CV incluye datos relevantes como contacto, formación, experiencia laboral y habilidades.

Realizamos lo siguiente para poder obtener toda la información

**Steps**

1. Case Information
2. Optional Information

**Case Information**

Case Name:

Base Directory:

Case Type: ☒ Single-user ☐ Multi-user

Case data will be stored in the following directory:

< Back **Next >** Finish Cancel Help

Tras esto continuamos con los pasos

**Steps**

1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source

**Select Data Source**

Path:

☐ Ignore orphan files in FAT file systems

Time zone:

Sector size:

Hash Values (optional):

MD5:

SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

< Back **Next >** Finish Cancel Help

Una vez acabado, obtendríamos esta pantalla

Data Sources

Views

- File Types
  - Deleted Files
  - File System (3)
  - All (6)
- MB File Size
- Results
- Tags
- Reports

6 Ret


Table Thumbnail Summary

Save Table as CS

Name	S	C	O	Modified Time	Change Time	Access Time
rolloutfile.tv13			0	2020-03-06 09:33:22 CET	2020-03-06 09:33:22 CET	2020-03-10 18:14:25 CET
CV.pdf			1	2020-03-05 16:30:33 CET	2020-03-05 17:55:39 CET	2020-03-10 18:03:19 CET
CV.pdf:Zone.Identifier			0	2020-03-05 16:30:33 CET	2020-03-05 17:55:39 CET	2020-03-10 18:03:19 CET
f0000000.mp3			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0014104.mp3			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0023296.pdf			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00

Hex Text Application File Metadata Context Results Annotations Other Occurrences

1 of 1 100% 1:1



**Manolo Ruiz Ortega**

Product Owner

manolo.ruiz1981@gmail.com

+34 675 436 156

Madrid - España

manolo.ruiz1981.skype

**EXPERIENCIA PROFESIONAL**

De 10/09/2005  
3/06/2010  
(Madrid-España)

**SER Madrid,**  
Asistent

Tareas realizadas:  
Desarrollo de una aplicación web para avisar automáticamente de los estacionamientos que superan el límite o el tiempo de aparcamiento establecido.

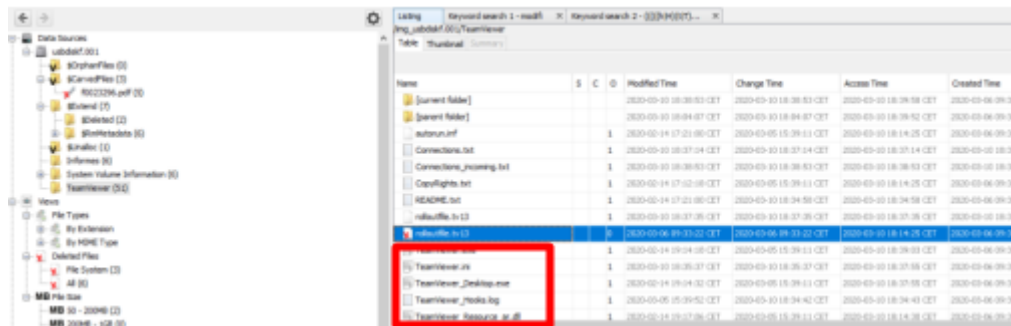
Si vamos a la timeline obtenemos los siguientes archivos

Timeline				
Display Times In: <input checked="" type="radio"/> Local Time Zone <input type="radio"/> GMT / UTC		View Mode: <input checked="" type="radio"/> Counts <input checked="" type="radio"/> Details <input type="radio"/> List		
<input checked="" type="button"/> History <input type="button"/> Back <input type="button"/> Forward		<input checked="" type="button"/> Add Event <input type="button"/> Snapshot Report		
Filters <input checked="" type="button"/> Apply <input type="button"/> Reset <input type="checkbox"/> Must include text: enter filter string <input type="checkbox"/> Must be tagged <input type="checkbox"/> Must have hash hit <input type="checkbox"/> Limit data sources to <input type="checkbox"/> Limit file types to <input checked="" type="checkbox"/> Limit event types to		270 events		
Date/Time	Event Type	Description	Tagged	Hash Hit
2018-09-28 08:07:30	Document L...	Document Last Saved : :		
2020-02-14 17:12:18	M_...	/TeamViewer/CopyRights.txt		
2020-02-14 17:21:00	M_...	/TeamViewer/README.txt		
2020-02-14 17:21:00	M_...	/TeamViewer/autorun.inf		
2020-02-14 17:44:52	M_...	/TeamViewer/tv_w32.dll		
2020-02-14 17:44:58	M_...	/TeamViewer/tv_w32.exe		
2020-02-14 17:45:04	M_...	/TeamViewer/tv_x64.dll		
2020-02-14 17:45:10	M_...	/TeamViewer/tv_x64.exe		
2020-02-14 19:14:18	M_...	/TeamViewer/TeamViewer.exe		
2020-02-14 19:14:32	M_...	/TeamViewer/Team ... wer_Desktop.exe		
2020-02-14 19:14:38	M_...	/TeamViewer/TeamViewer_StaticRes.dll		
2020-02-14 19:15:32	M_...	/TeamViewer/Team ... _Resource_de.dll		
2020-02-14 19:15:40	M_...	/TeamViewer/Team ... _Resource_en.dll		
2020-02-14 19:15:48	M_...	/TeamViewer/TeamV ... _Resource_fr.dll		
2020-02-14 19:15:56	M_...	/TeamViewer/TeamV ... _Resource_it.dll		
2020-02-14 19:16:04	M_...	/TeamViewer/Team ... _Resource_da.dll		
2020-02-14 19:16:10	M_...	/TeamViewer/Team ... _Resource_nl.dll		
2020-02-14 19:16:18	M_...	/TeamViewer/Team ... _Resource_es.dll		
2020-02-14 19:16:26	M_...	/TeamViewer/Team ... _Resource_pt.dll		
2020-02-14 19:16:34	M_...	/TeamViewer/Team ... _Resource_ko.dll		
2020-02-14 19:16:42	M_...	/TeamViewer/Team ... _Resource_ru.dll		
2020-02-14 19:16:50	M_...	/TeamViewer/Team ... _Resource_ja.dll		
2020-02-14 19:16:58	M_...	/TeamViewer/Team ... _Resource_cs.dll		

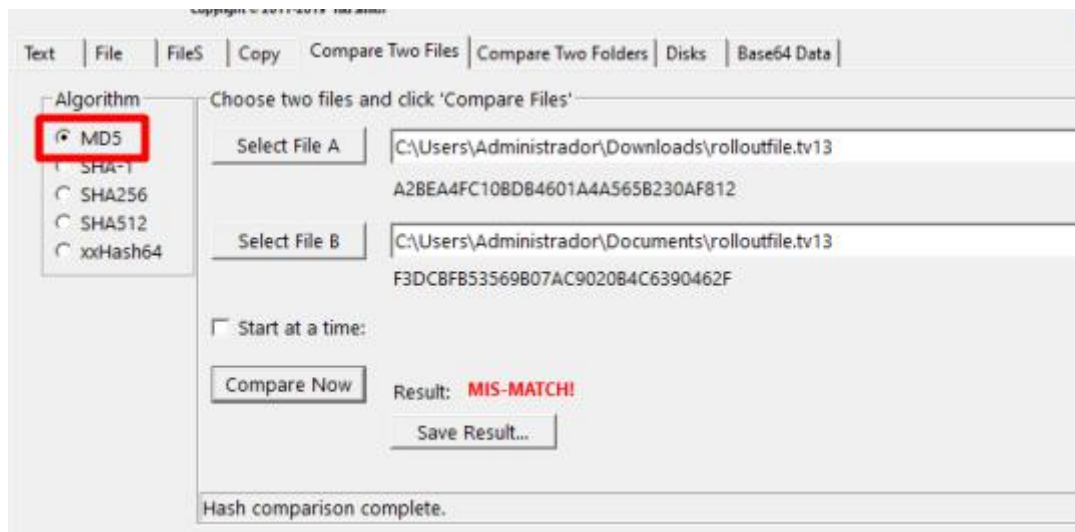
Observamos la última modificación del archivo el día 10 de marzo de 2020

2020-03-10 18:37:35	MABC	/TeamViewer/rolloutfile.tv13		
2020-03-10 18:37:55	_A_	/TeamViewer/TeamV ... _Resource_fr.dll		
2020-03-10 18:37:55	_A_	/TeamViewer/TeamViewer_StaticRes.dll		
2020-03-10 18:37:55	_A_	/TeamViewer/Team ... _Resource_de.dll		
2020-03-10 18:37:55	_A_	/TeamViewer/Team ... _Resource_en.dll		
2020-03-10 18:37:55	_A_	/TeamViewer/TeamViewer.ini		
2020-03-10 18:37:55	_A_	/TeamViewer/Team ... wer_Desktop.exe		
2020-03-10 18:37:55	_A_	/TeamViewer/Team ... _Resource_es.dll		
2020-03-10 18:38:06	_A_	/TeamViewer/tv_w32.dll		
2020-03-10 18:38:53	M_C	/TeamViewer		
2020-03-10 18:38:53	_A_	/TeamViewer/tv_x64.dll		
2020-03-10 18:38:53	MABC	/TeamViewer/Conn ... ons_incoming.txt		
2020-03-10 18:39:03	_A_	/TeamViewer/TeamViewer.exe		
2020-03-10 18:39:04	MA_C	/\$Extend/\$RmMet ... 0000000000000001		
2020-03-10 18:39:04	MA_C	/\$Extend/\$RmMeta ... fLog/\$TxfLog.blf		
2020-03-10 18:39:24	_A_	/System Volume Information		
2020-03-10 18:39:24	_A_	/System Volume In ... n/WPSettings.dat		
2020-03-10 18:39:28	_A_	/System Volume I ... dexerVolumeGuid		
2020-03-10 18:39:52	_A_	/		
2020-03-10 18:39:58	_A_	/TeamViewer		
2020-03-10 18:39:58	_A_	/TeamViewer/tv_w32.exe		
2020-03-10 18:39:58	_A_	/TeamViewer/tv_x64.exe		

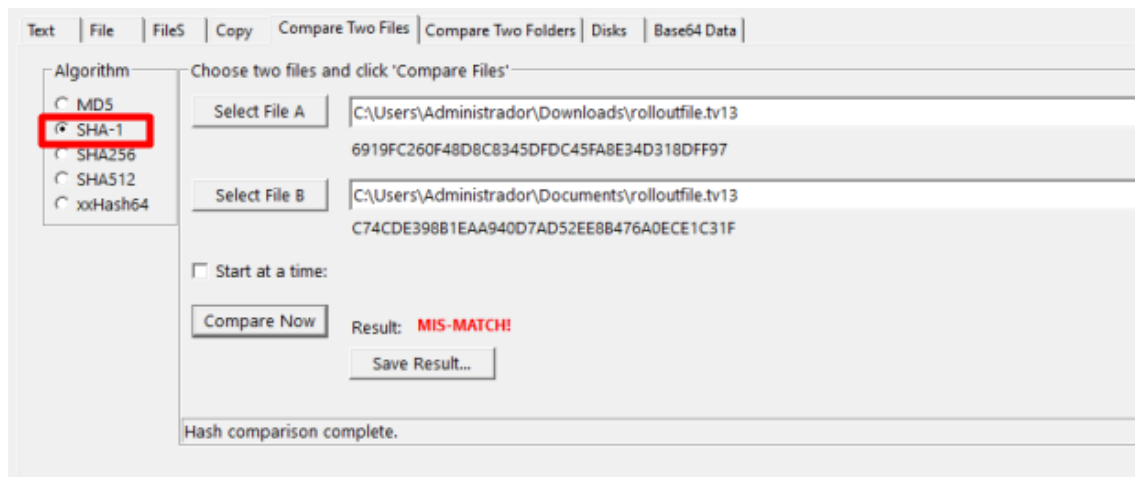
La principal brecha de seguridad la encontramos en la herramienta TeamViewer



Así que una vez hemos realizado esto adquirimos los hashes y los comparamos con FTK, el resultado Mis-match quiere decir que son diferentes hashes



En este caso ocurre lo mismo



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

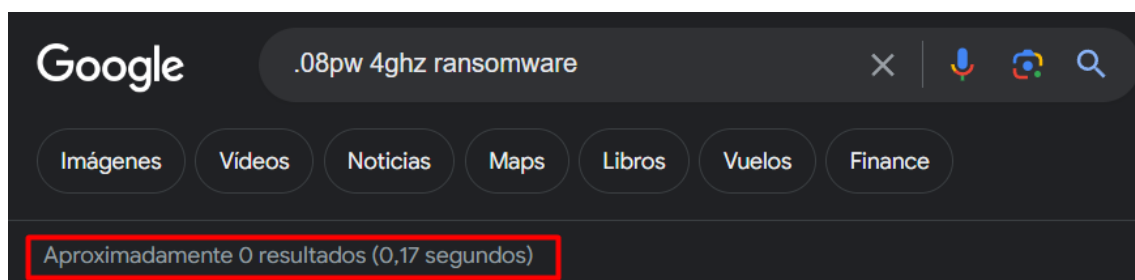
- Ficheros necesarios para el ejercicio: cifrados.zip
- ¿Qué indicadores se emplean para identificar la familia de *ransomware*?

Muestra	Familia	Extensión	¿Es descifrable?
banner_image.png.zeoticus	Zeoticus 2.0	.2020FIN	Sí
CV Teresa Martinez.PDF.08pw4ghz	N/A	N/A	Sí
Garden.jpg.WNCRY	WCRY	WCRY	Sí
Objeto social.pdf.id.Devos	Phobos	.Devos	Sí

**Muestra**      **descifrable**      →      **Objeto**      social.pdf.id[125DFD2B-2686].[CYBERTRUCK2048@protonmail.com].Devos

**Es descifrable?** → En esta página viene información reseñable para poder conseguirlo, los pasos son largos y tediosos. <https://malwaretips.com/blogs/remove-devos-virus/#remove-the-devos-ransomware-and-recover-the-files>

**Es descifrable?** → Al buscar información del archivo .08pw4ghz no se obtuvo información reseñable



**Es descifrable?** → al buscar información de jpg.WNCRY encuentro un análisis en el siguiente enlace.

<https://www.joesecurity.org/reports/report-db349b97c37d22f5ea1d1841e3c89eb4.html>

## 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<sup>2</sup>, inicios exitosos, modificaciones de permisos de usuarios, creación de nuevos usuarios, etc.

<sup>2</sup> 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?

Código de inicio de sesión correcto 4624

The screenshot shows the Windows Event Viewer interface. On the left, the 'Tunneling' log is selected under 'Registros guardados'. The main pane displays a list of 18 events. The event with ID 4624 at 13/02/2019 16:15:04 is highlighted. Below the list, a detailed view of event 4624 is shown, indicating a successful logon.

Nivel	Fecha y hora	Origen	Id. del evento	Categoría d...
Información	13/02/2019 16:31:31	Microsoft ...	4624	Logon
Información	13/02/2019 16:31:19	Microsoft ...	4624	Logon
Información	13/02/2019 16:29:40	Microsoft ...	4624	Logon
Información	13/02/2019 16:26:53	Microsoft ...	4624	Logon
Información	13/02/2019 16:19:51	Microsoft ...	4624	Logon
Información	13/02/2019 16:17:38	Microsoft ...	4624	Logon
Información	13/02/2019 16:17:38	Microsoft ...	4624	Logon
Información	13/02/2019 16:15:36	Microsoft ...	4624	Logon
Información	13/02/2019 16:15:08	Microsoft ...	4624	Logon
Información	13/02/2019 16:15:08	Microsoft ...	4624	Logon
Información	13/02/2019 16:15:07	Microsoft ...	4624	Logon
Información	13/02/2019 16:15:05	Microsoft ...	4624	Logon
Información	13/02/2019 16:15:05	Microsoft ...	4624	Logon
Información	13/02/2019 16:15:05	Microsoft ...	4624	Logon
Información	13/02/2019 16:15:05	Microsoft ...	4624	Logon
Información	13/02/2019 16:15:04	Microsoft ...	4624	Logon
Información	13/02/2019 16:15:04	Microsoft ...	4624	Logon
Información	13/02/2019 16:14:52	Microsoft ...	4624	Logon

Evento 4624, Microsoft Windows security auditing.

General Detalles

Se inició sesión correctamente en una cuenta.

Nombre de registro: Seguridad

Origen: Microsoft Windows security Registrado: 13/02/2019 16:15:04

Id. del: 4624 Categoría de tarea: Logon

Nivel: Información Palabras clave: Auditoría correcta

Usuario: No disponible Equipo: PC02.example.corp

Código de operación: Información

## Registro: Seguridad

### Ubicación del registro:

%SystemRoot%\System32\Winevt\Logs\Security.evtx

### ID de evento: [4624](#)

**Nombre del proveedor:** Microsoft-Windows-Security-Auditing

**LogonType:** Tipo 3 (Red) cuando [NLA](#) está habilitado (y en ocasiones incluso cuando está no) seguido del Tipo 10 (RemoteInteractive/también conocido como Terminal Services/también conocido como Escritorio remoto) O Escriba 7 desde una IP remota (si se trata de una reconexión desde una IP anterior /sesión RDP existente)

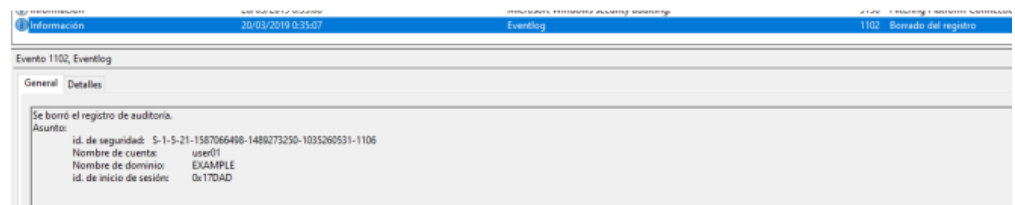
**Descripción:** Se inició sesión correctamente en una cuenta"

¿Qué información de interés recoge este tipo de eventos?

Obtenemos información que puede ser interesante como fechas, qué usuario es y que PC es.

- 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?

Para esto nos dirigimos a seguridad y el id del evento es 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

Filtrar registro actual X

Filtro XML

Registrado: En cualquier momento

Nivel del evento: ☐ Crítico ☐ Advertencia ☐ Detallado  
☐ Error ☐ Información

☒ Por registro Registros de eventos: file:///C:/Users/Administrador/Desktop/Ejercicios/Logs de eventos/Tunneling.evtx

☐ Por origen Orígenes del evento:

Para incluir o excluir los id. de evento, escriba números o intervalos de id. separados por comas. Para excluir criterios, antecédalos con un signo de menos. Ej: 1,3,5-99,-76

4624

Categoría de la tarea:

Palabras clave:

Usuario: < Todos los usuarios >

Equipo(s): < Todos los equipos >

Borrar

Aceptar Cancelar

Obtenemos esto

Filtrados: Registro: file:///C:/Users/Administrador/Desktop/Ejercicios/Logs de eventos/Tunneling.evtx;

Nivel	Fecha y hora	Origen	Id. del evento	Categoría d...
Información	13/02/2019 16:31:31	Microsoft ...	4624	Logon
Información	13/02/2019 16:31:19	Microsoft ...	4624	Logon
Información	13/02/2019 16:29:40	Microsoft ...	4624	Logon
Información	13/02/2019 16:26:53	Microsoft ...	4624	Logon
Información	13/02/2019 16:19:51	Microsoft ...	4624	Logon
Información	13/02/2019 16:17:38	Microsoft ...	4624	Logon
Información	13/02/2019 16:17:38	Microsoft ...	4624	Logon
Información	13/02/2019 16:15:36	Microsoft ...	4624	Logon
Información	13/02/2019 16:15:08	Microsoft ...	4624	Logon
Información	13/02/2019 16:15:08	Microsoft ...	4624	Logon
Información	13/02/2019 16:15:07	Microsoft ...	4624	Logon
Información	13/02/2019 16:15:05	Microsoft ...	4624	Logon
Información	13/02/2019 16:15:05	Microsoft ...	4624	Logon
Información	13/02/2019 16:15:05	Microsoft ...	4624	Logon
Información	13/02/2019 16:15:04	Microsoft ...	4624	Logon
Información	13/02/2019 16:15:04	Microsoft ...	4624	Logon
Información	13/02/2019 16:15:04	Microsoft ...	4624	Logon
Información	13/02/2019 16:14:52	Microsoft ...	4624	Logon



A continuación, guardamos lo obtenido

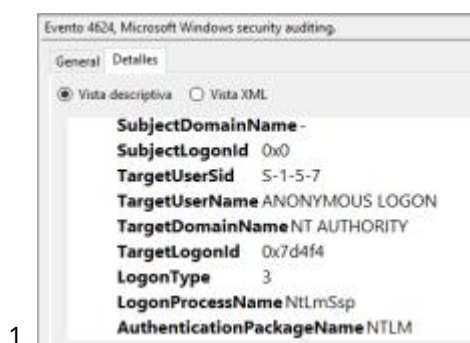


Los logs son los siguientes

Nombre	Fecha de modificación	Tipo	Tamaño
LocalSessionManager-Operational	16/03/2020 4:09	Registro de eventos	1.092 KB
Security	16/03/2020 4:09	Registro de eventos	1.092 KB
Security_Share	16/03/2020 4:09	Registro de eventos	1.092 KB
Tunneling	16/03/2020 4:08	Registro de eventos	68 KB
Tunneling_TerminalServices-RemoteCon...	16/03/2020 4:09	Registro de eventos	1.092 KB

- 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	Event ID	Fecha y Hora	Actividad Maliciosa Destacada
1.Tunneling.evtx	4624	13/02/2019 16:15:36	Elevación de Privilegios
2.Tunneling_Terminal - Services- RemoteControl.evtx	1149	13/02/2019 18:51:19	Conexión Remota
3.Security.evtx	1102	20/02/2019 00:35:07	Borrado del registro
4.Security_Share.evtx	5145	18/03/2019 15:23:26	Descarga de malwr.exe compartición de fichero
5.LocalSessionManager - Operational.evtx	17	18/02/2019 14:01:29	Códigos de errores múltiples en la fecha y hora



Evento 1149, TerminalServices-RemoteConnectionManager

General	Detalles
Usuario: administrator Dominio: example Dirección de red de origen: fe80::80ac:4126:fa58:1b81%10	
Nombre de registro:	Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational
Origen:	TerminalServices-RemoteCo Registrado: 13/02/2019 18:51:19

2.

## + System

## - EventData

**SubjectUserSid** S-1-5-21-1587066498-1489273250-1035260531-500  
**SubjectUserName** Administrator  
**SubjectDomainName** EXAMPLE  
**SubjectLogonId** 0xfc635  
**ObjectType** File  
**IpAddress** 10.0.2.15  
**IpPort** 55632  
**ShareName** \\\*\C\$\br/>
**ShareLocalPath** \??\C:\br/>
**RelativeTargetName** malwr.exe ●  
**AccessMask** 0x120089  
**AccessList** %%1538 %%1541 %%4416 %%4419 %%4423  
**AccessReason** -

4.

## 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_205446_Processing_Details.txt	Detects a set of reconnaissance commands on Windows system
PsLoglist.txt	Detects hack tool used in Operation Wilted Tulip

Abrimos CMD y nos dirigimos a la carpeta Escritorio y ejecutamos el archivo loki.exe

```
C:\Users\Administrador\Desktop\sherlook\loki>loki.exe

LOKI
AGAOPERA

Copyright by Florian Roth, Released under the GNU General Public License
Version 0.33.0

DISCLAIMER - USE AT YOUR OWN RISK
Please report false positives via https://github.com/Neo23x0/Loki/issues
```

Lo dejamos correr y podremos ver el análisis del archivo .zip de manera detallada

```
WARNING:
File: C:\Users\Administrador\Desktop\Ejercicios\AGAOPERA_20200129_205446.zip AGAOPERA_20200129_205446\AGAOPERA_20200129_205446_Processing_Details.txt SCORE: 60 TYPE: UNKNOWN
Size: 30424
FIRST_BYTES: 4f5320547070653a2057096e640f7773200d0a43 / OS Type: Windows C
MD5: 7034a4e4316f2c81252004f1b4b0d08
SHA1: b0cc84562150e501f603013a0e3fffc6ef93e4c
SHA256: d0d97cfc052dcfb308e2228f05d1123a3ac55431c25984d5f55065d0a7e6cf34 CREATED: Tue Dec 5 20:41:14 2023 MODIFIED: Wed Jan 29 21:22:38 2020 ACCESSED: Tue Dec 5 21:00:00 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/MSJCKP
MATCHES: Str1: netstat -an Str2: whoami Str3: systeminfo Str4: arp -a
[REDACTED]
FILE: C:\Users\Administrador\Desktop\Ejercicios\AGAOPERA_20200129_205446.zip\AGAOPERA_20200129_205446\liveResponseData\BasicInfo\PsiLoglist.txt SCORE: 70 TYPE: UNKNOWN SIZE: 3505178
FIRST_BYTES: 53797374656d206c6f67206f6e205c5c4147414f / System log on \AGAD
MD5: 709f184a60ed40fd5dbbe6617993f241
SHA1: 13a5e3beff14555c01046f8240c0009916c92b45
SHA256: 524e583f516fc1564dc049f018935c7780f74e8a9471a26a345f4f4117729 CREATED: Tue Dec 5 20:41:14 2023 MODIFIED: Wed Jan 29 21:22:34 2020 ACCESSED: Tue Dec 5 21:00:00 2023
REASON 1: Yara Rule MATCH: WiltedTulip.WindowsTask SUBSCORE: 70
DESCRIPTION: Detects hack tool used in Operation Wilted Tulip - Windows tasks REF: http://www.clearysec.com/tulip
MATCHES: Str1: -prognosis command -prognosis command -prognosis command -prognosis command -prognosis command -prognosis command -prognosis command -prognosis command -prognosis command -prognosis command
```