ANÁLISIS FORENSE

Unidad 1. Actividad 1

09 DE ABRIL DE 2023

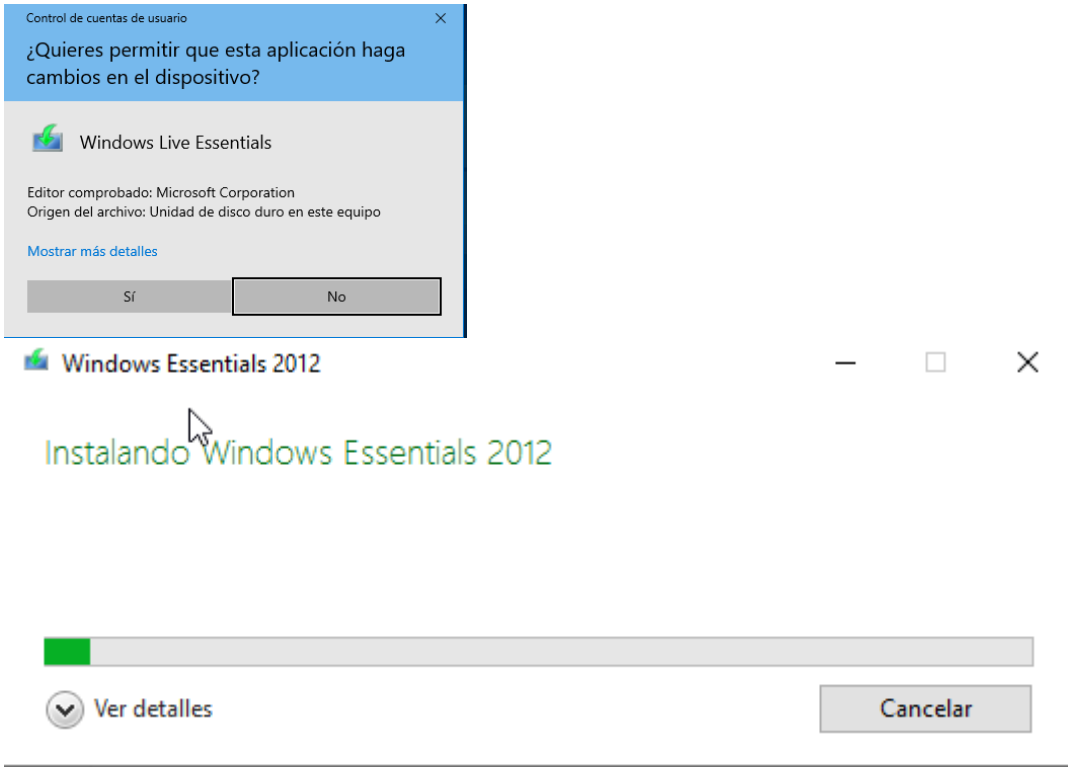
CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

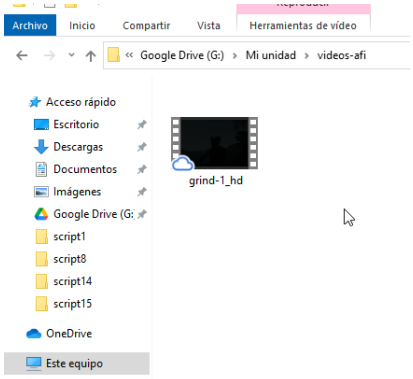
RELACION DE EJERCICIOS T04-R01-Ejercicio 1

Ejercicio 1 (2 puntos) Análisis de Google Drive

Primero nos vamos a descargar Windows essentials en Windows 10(el profesor ha permitido que en vez de hacerlo en Windows server hacerlo en Windows 10).

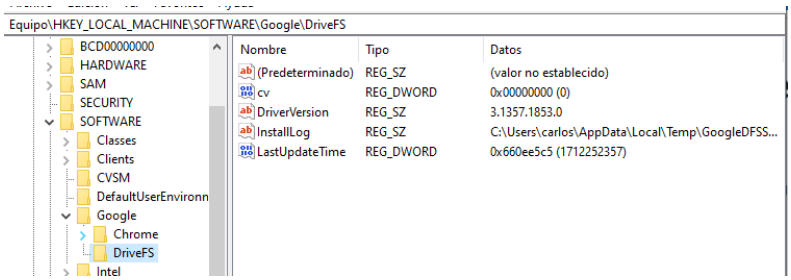


Ahora metemos el archivo grind-1_hd.mp4 en nuestro drive de clase:



a) Haz una captura de pantalla del contenido de cada una las claves del registro de Windows, donde se vea claramente donde está instalado el cliente Google Drive.

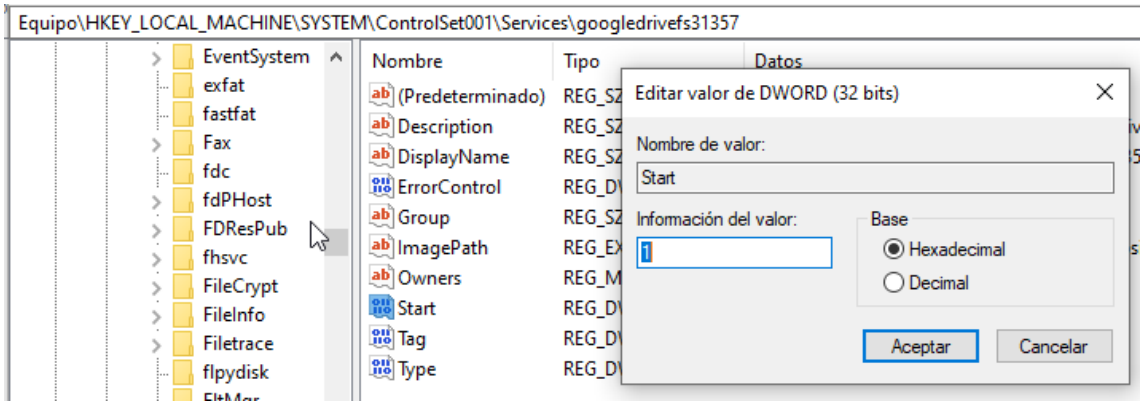
Las claves de registro:



-Haz una captura de pantalla donde aparezca la configuración para el servicio de drive que tiene este usuario.

-Busca la clave donde aparece el estado del servicio de drive e indica que clave hay que hacer para desactivarlo.

Aquí es donde tenemos el servicio activado:



Con el valor 1 significa que al arrancar el Windows funciona el programa, con el valor 0 se desactiva.

b) Busca en las bases de datos del cliente de Google Drive información sobre el archivo de video que has subido, la carpeta que has creado y donde lo has movido.

Para hacer esto tenemos que descargarnos db browse sql e ir al directorio:

DB Browser for SQLite - C:\Users\carlos\AppData\Local\Google\DriveFS\100463083543912996952\mirror_metadata_sqlite.db

Y ahora nos vamos a item_properties y vemos como tenemos nuestri archivo(en mi caso hay dos pq lo he metido dos veces por que no estoy seguro si lo quiere en esa carpeta o en la de informaticaforense):

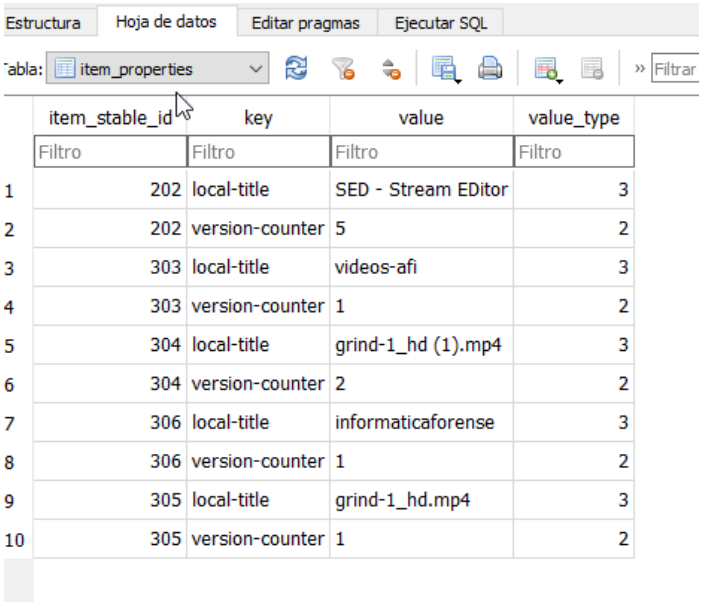

Estructura | Hoja de datos | Editar pragmas | Ejecutar SQL

Tabla: item_properties

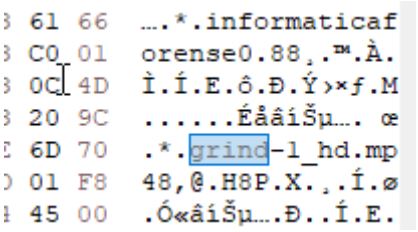
	item_stable_id	key	value	value_type
	Filtro	Filtro	Filtro	Filtro
1	202	local-title	SED - Stream EDitor	3
2	202	version-counter	5	2
3	303	local-title	videos-afi	3
4	303	version-counter	1	2
5	304	local-title	grind-1_hd (1).mp4	3
6	304	version-counter	2	2
7	306	local-title	informaticaforense	3
8	306	version-counter	1	2
9	305	local-title	grind-1_hd.mp4	3
10	305	version-counter	1	2

c) Busca en los logs de Google Drive los datos de acceso del usuario al drive y el archivo que has subido.

Para ver los logs lo podemos ver en :

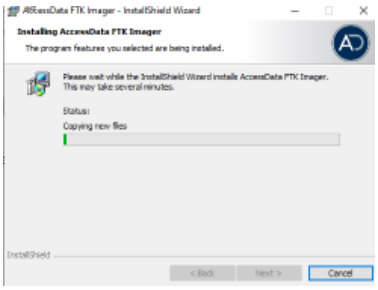
· [C:\Users\carlos\AppData\Local\Google\DriveFS\Logs\structured_log_100463083543912996952]

Y aquí tenemos todos los logs, simplemente vamos a buscar por las palabras claves(he usado un programa llamado hxd):

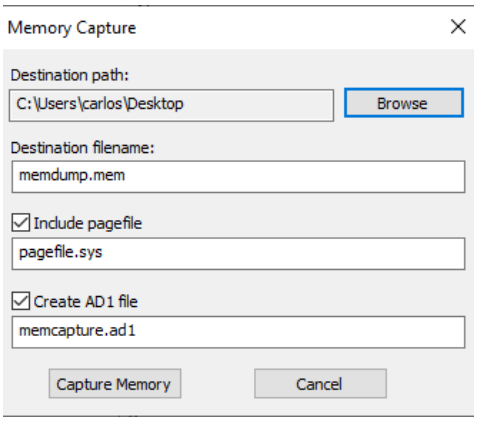


d) Accede a Google Drive con el navegador web, haz un volcado de memoria RAM con FTK Imager y busca las credenciales de acceso al Drive. Inserta una captura de pantalla donde se vea la identificación y otra donde se vea la contraseña.

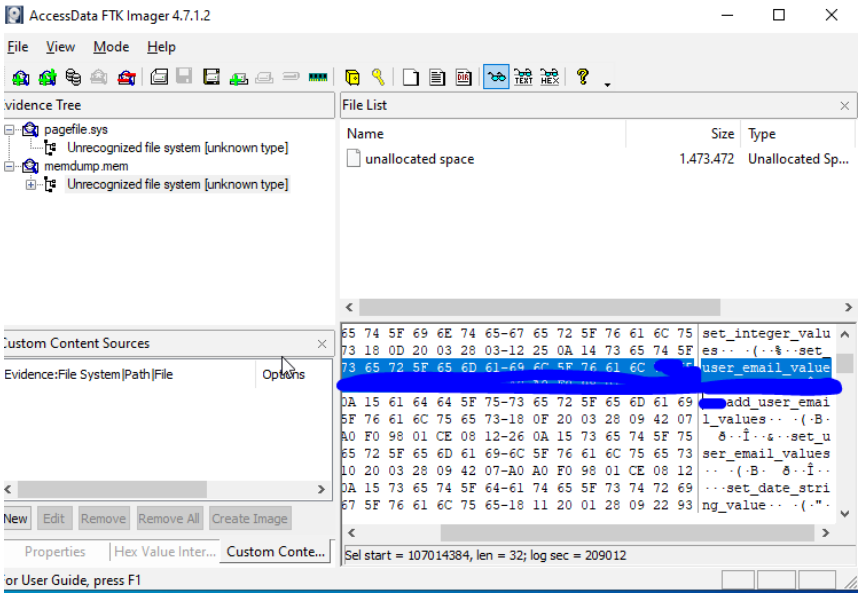
Primero nos descargamos FTK imager:



Ahora hacemos la captura:

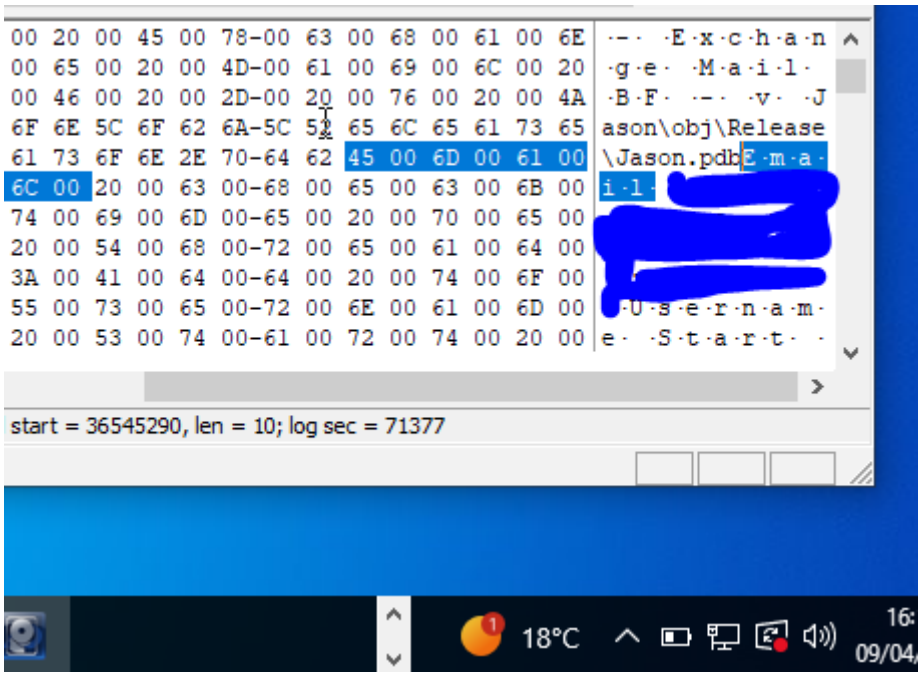


Ahora al abrir el memdumo.mem podemos encontrar cosas como nuestro identificador de email:



Y pagefile.sys podemos encontrar nuestro email de inicio y nuestra contraseña:

Email:



Contraseña: