

# Practica Definitiva

## Informe de Práctica 2: Análisis de Evidencias en Disco

### ÍNDICE

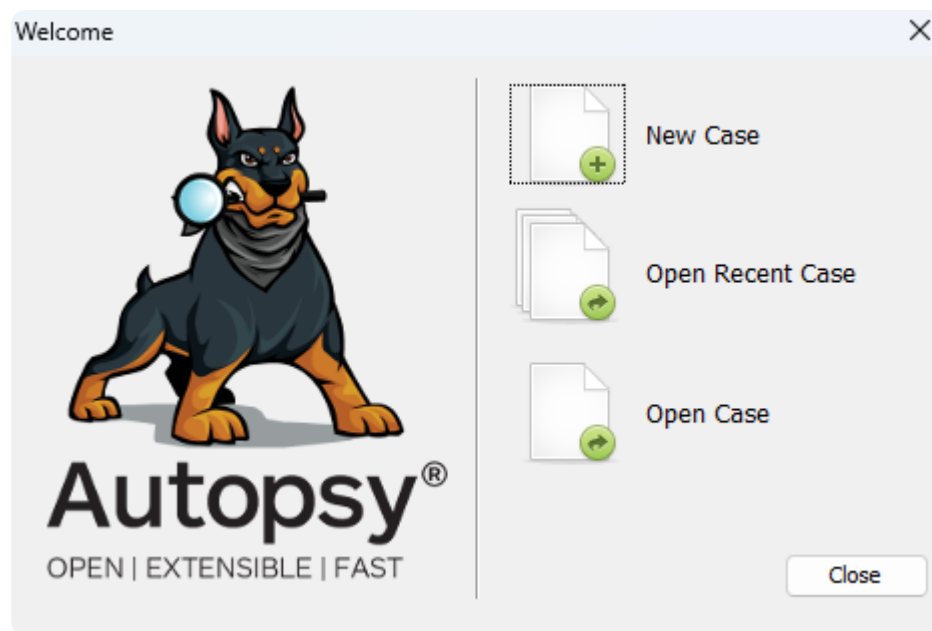
1. Ejercicio 1: Creación de Caso y Recuperación de Partición
  - 1.1 Creación de un nuevo caso en Autopsy
  - 1.2 Adición de la fuente de datos
  - 1.3 Módulos (Ingest Modules)
  - 1.4 Recuperación de archivos y partición eliminados
2. Ejercicio 2: Integridad y Análisis de Archivos Comprimidos
  - 2.1 Verificación de integridad de la evidencia
  - 2.2 Localización de archivos comprimidos
  - 2.3 Acceso y descriptado de ficheros protegidos
3. Ejercicio 3: Análisis de SO, Usuarios y Artefactos Clave
  - 3.1 Sistema operativo instalado
  - 3.2 Identificación de usuarios
  - 3.3 Último inicio de sesión del usuario "jcloudy"
  - 3.4 Información sobre pendrives insertados
  - 3.5 Búsqueda de información sobre armas de fuego
  - 3.6 Archivo "Planning.docx"
  - 3.7 Identificación de la tarjeta gráfica
  - 3.8 Acceso a cuentas en la nube de jcloudy



## 1. Ejercicio 1

### 1.1 Creación de un nuevo caso en Autopsy

- **Descripción del procedimiento:**
  - Selección de opción New Case

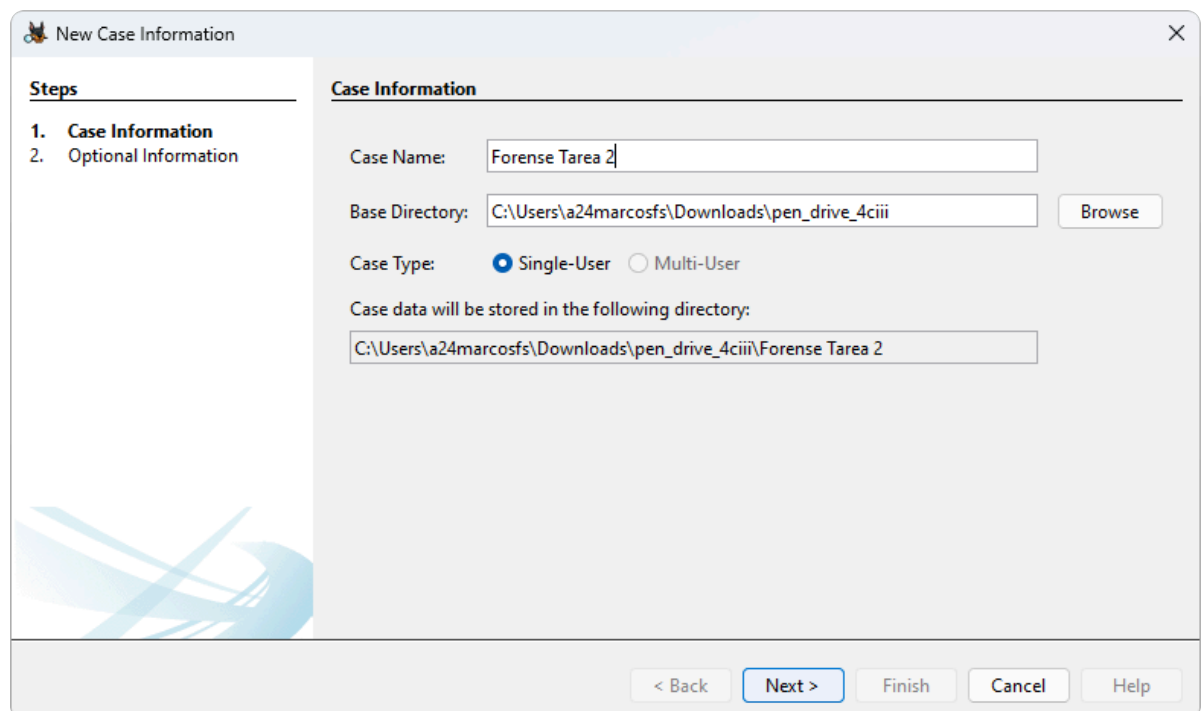


## 1.2 Adición de la fuente de datos

- **Pasos detallados:**

- 1- Creación del proyecto

- 



- 2- Procedimiento para agregar la imagen y definir hora.

**Add Data Source**

**Steps**

1. Select Host
2. Select Data Source Type
3. **Select Data Source**
4. Configure Ingest
5. 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.

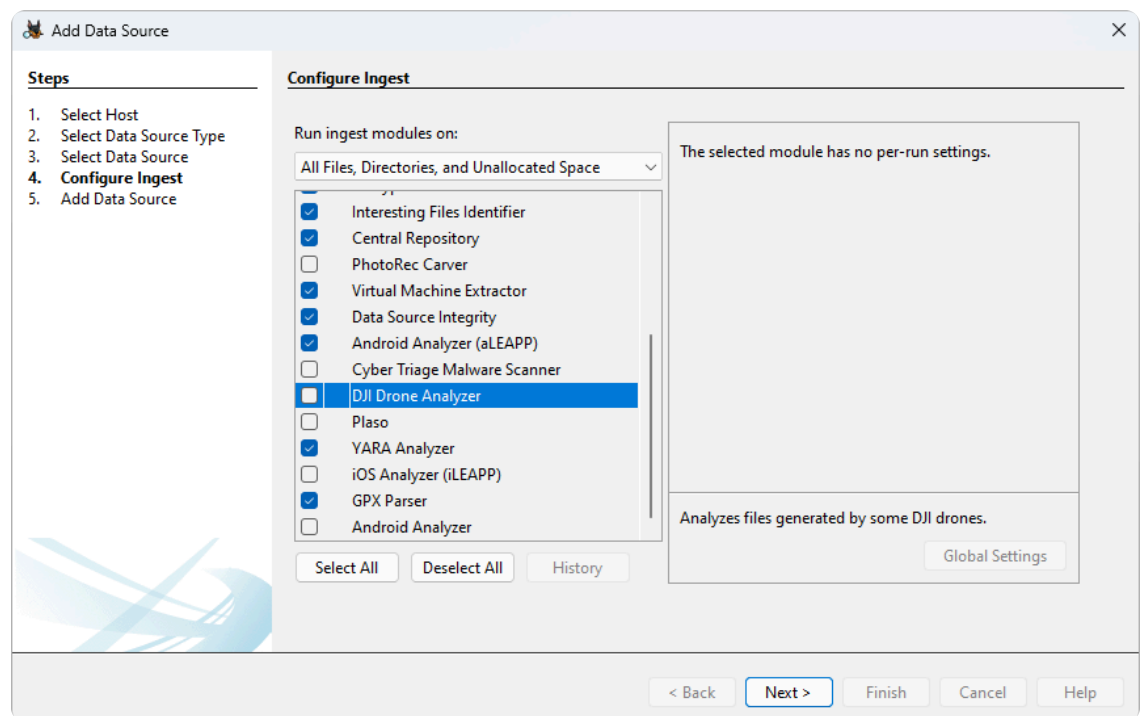
< Back   Next >   Finish   Cancel   Help

### • 3- Ingest modules

#### • Justificación de los "ingest modules" seleccionados.

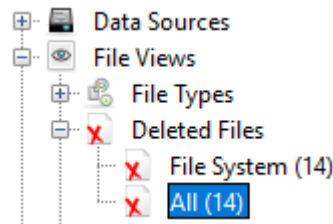
- **Recent Activity:** Permite identificar actividades recientes del sistema, como archivos accedidos y programas ejecutados. Es esencial para rastrear las acciones del usuario.
- **Hash Lookup:** Calcula y verifica los hashes de los archivos para garantizar su integridad y detectar archivos potencialmente sospechosos.
- **File Type Identification:** Identifica los archivos según su tipo real, facilitando la localización de información relevante independientemente de la extensión.
- **Extension Mismatch Detector:** Detecta archivos cuya extensión no coincide con su contenido real, ayudando a identificar archivos ocultos o manipulados.
- **Embedded File Extractor:** Extrae archivos embebidos dentro de otros, como documentos o imágenes, para descubrir contenido oculto.
- **Keyword Search:** Permite buscar palabras clave en archivos y sistemas, facilitando la localización de evidencias textuales relacionadas con el caso.
- **Encryption Detection:** Detecta archivos cifrados o protegidos con contraseñas, señalando potenciales evidencias que requieran un análisis adicional.
- **Interesting Files Identifier:** Filtra automáticamente archivos de interés según criterios predefinidos, optimizando el tiempo de análisis.
- **Picture Analyzer:** Analiza imágenes recuperadas y permite extraer información visual o metadatos de archivos gráficos.
- **Central Repository:** Consolida y organiza la información obtenida, permitiendo correlacionar datos entre archivos y eventos.
- **Virtual Machine Extractor:** Extrae datos de máquinas virtuales presentes en la imagen forense, útiles si se encuentran entornos virtualizados.

- **YARA Analyzer:** Detecta archivos maliciosos o patrones específicos mediante reglas YARA, aportando una capa adicional de análisis forense.
- **Data Source Integrity:** Verifica la integridad de la fuente de datos analizada, asegurando que no ha sido alterada.
- **Justificación de los "ingest modules" no seleccionados.**
  - **Android Analyzer (aLEAPP / Android Analyzer):** Estos módulos están diseñados para analizar dispositivos Android, los cuales no son relevantes en esta práctica enfocada en imágenes de disco Windows.
  - **iOS Analyzer (iLEAPP):** Similar al anterior, analiza dispositivos Apple, que no son objeto del análisis actual.
  - **DJI Drone Analyzer:** Se centra en datos provenientes de drones DJI, los cuales no están presentes en la evidencia proporcionada.
  - **PhotoRec Carver:** Aunque útil para recuperar archivos eliminados, consume demasiados recursos y tiempo, por lo que se evitó su uso en favor de otros módulos más eficientes.
  - **Cyber Triage Malware Scanner:** Orientado a la detección avanzada de malware. No es un requisito prioritario en esta práctica y ralentizaría el análisis.
  - **Plaso:** Genera líneas de tiempo avanzadas, pero su uso no es necesario en esta práctica y afecta al rendimiento general de Autopsy.



## 1.3 Recuperación de archivos y partición eliminados

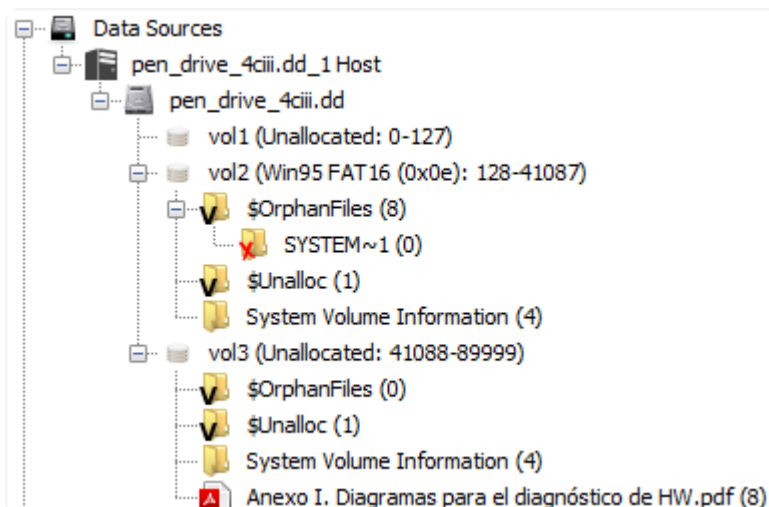
- **Resultados obtenidos:**
  - ¿Se recuperaron los archivos eliminados?
    - Si entramos en Tipo de archivos Deleted Files



- Vemos que hay todos estos archivos eliminados no recuperados

Listing							
All							
Table Thumbnail Summary							
Page: 1 of 1 Pages: < > Go to Page:							
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
✖ Nuevo Documento de texto.txt				2022-11-06 19:34:12 UTC	0000-00-00 00:00:00	2022-11-06 00:00:00 UTC	2022-11-06 19:34:10 UTC
✖ Nombre.txt				2022-11-06 19:34:28 UTC	0000-00-00 00:00:00	2022-11-07 00:00:00 UTC	2022-11-06 19:34:10 UTC
✖ Nuevo Documento de texto.txt				2022-11-06 19:37:02 UTC	0000-00-00 00:00:00	2022-11-06 00:00:00 UTC	2022-11-06 19:37:01 UTC
✖ SYSTEM~1				2022-10-24 18:28:14 UTC	0000-00-00 00:00:00	2022-10-24 00:00:00 UTC	2022-10-24 18:28:13 UTC
✖ _DROPB~1.WRI				2022-11-06 11:31:10 UTC	0000-00-00 00:00:00	2022-11-06 00:00:00 UTC	2022-11-06 11:31:08 UTC
✖ _EXT0.TXT				2022-11-06 11:54:58 UTC	0000-00-00 00:00:00	2022-11-06 00:00:00 UTC	2022-11-06 11:54:57 UTC
✖ TEXTO.TXT				2022-11-06 11:54:58 UTC	0000-00-00 00:00:00	2022-11-06 00:00:00 UTC	2022-11-06 11:54:57 UTC
✖ f1.jpg				2022-11-06 11:55:54 UTC	0000-00-00 00:00:00	2022-11-06 00:00:00 UTC	2022-11-06 11:55:51 UTC
✖ _DROPB~1.WRI				2022-11-06 13:29:10 UTC	0000-00-00 00:00:00	2022-11-06 00:00:00 UTC	2022-11-06 13:29:09 UTC
✖ WPSETT~1.DAT				2022-10-24 18:28:14 UTC	0000-00-00 00:00:00	2022-11-06 00:00:00 UTC	2022-10-24 18:28:13 UTC
✖ INDEXE~1				2022-10-24 18:28:14 UTC	0000-00-00 00:00:00	2022-11-06 00:00:00 UTC	2022-10-24 18:28:13 UTC
✖ Nuevo Documento de texto.txt				2022-11-06 19:35:10 UTC	0000-00-00 00:00:00	2022-11-06 00:00:00 UTC	2022-11-06 19:35:09 UTC
✖ Nombre2.txt				2022-11-06 19:35:28 UTC	0000-00-00 00:00:00	2022-11-07 00:00:00 UTC	2022-11-06 19:35:09 UTC
✖ Nuevo Documento de texto.txt				2022-11-06 19:36:46 UTC	0000-00-00 00:00:00	2022-11-06 00:00:00 UTC	2022-11-06 19:36:44 UTC

- ¿Se recuperó la partición eliminada?
  - La partición eliminada no ha sido completamente reconstruida, pero se han identificado datos y archivos huérfanos en los volúmenes **vol1** y **vol3** (Unallocated).
  - Esto indica que Autopsy pudo recuperar parte de la información.



- Partición eliminada identificada:
  - Los espacios **vol1** (0-127) y **vol3** (41088-89999) son las particiones eliminadas.

vol1 (Unallocated: 0-127)

## 2. Ejercicio 2

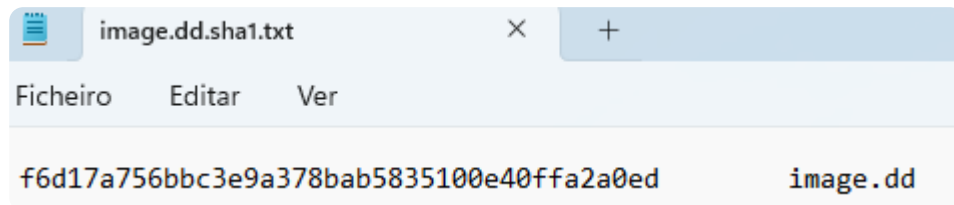
### 2.1 Verificación de integridad de la evidencia

- **Imagen utilizada:** `image.dd.zip`
  - Esta imagen contiene la evidencia forense que vamos a analizar.
- **Procedimiento:**
  1. **Cálculo del hash:**
    - **Comando:** `Get-FileHash -Path "C:\Users\A24marcosfs\Downloads\image.dd\image.dd" -Algorithm SHA1`
    - **Resultado:** `F6D17A756BBC3E9A378BAB5835100E40FFA2A0ED`
    - **Captura de pantalla:**

```
PS L:\> Get-FileHash -Path "C:\Users\A24marcosfs\Downloads\image.dd\image.dd" -Algorithm SHA1
```

Algorithm	Hash	Path
SHA1	<u>F6D17A756BBC3E9A378BAB5835100E40FFA2A0ED</u>	C:\Users\A24marcosfs\Download...

#### 2. Comparación del hash:



- Este paso confirma que la imagen no ha sido alterada.



### 2.2 Localización de los archivos comprimidos

- **Objetivo:** Encontrar ficheros de tipo `.zip` que puedan contener información relevante.
- **Procedimiento:**
  1. Abrí la imagen en **Autopsy** e inicié el análisis general.
  2. Filtré los resultados por **extensión** `.zip` para identificar los archivos comprimidos.
  3. Revisé cada archivo `.zip` en búsqueda de contenido potencialmente importante.
- **Resultados:**
  - Se identificaron dos archivos comprimidos principales:

1. Your new password is.rar

2. TrueCrypt Setup 7.1a(1).rar

- Capturas de pantalla:

Name	S	C	O	Modified Time
Zr5FTg3.jpg				2013-08-11 21:52:49 UTC
private				2014-01-05 06:12:18 UTC
[current folder]				2014-01-05 06:12:18 UTC
[parent folder]				2014-01-05 06:12:18 UTC
Cxm5Xlgh.jpg				2013-06-22 01:40:11 UTC
Cxm5Xlgh.jpg:Zone.Identifier				2013-06-22 01:40:11 UTC
Your new password is.rar	!			2014-01-05 08:52:43 UTC

TrueCrypt Setup 7.1a(1).rar				2013-06-22 01:49:07 UTC
-----------------------------	--	--	--	-------------------------



## 2.3 Acceso al contenido de los ficheros comprimidos

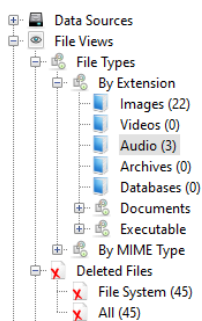
En este punto, la dificultad es que algunos archivos `.zip` se encuentran protegidos con contraseña. Esto nos obliga a identificar, en la misma imagen forense, posibles pistas que permitan obtener esa contraseña.

- Herramientas utilizadas:

- **7-Zip:** Para extraer y manipular los archivos comprimidos.

### 1. Indicaciones en un audio

- Se descubrió un **archivo de audio** dentro de la evidencia; al reproducirlo, menciona que la contraseña del `.zip` es **un número de teléfono**.
- Captura en Autopsy:

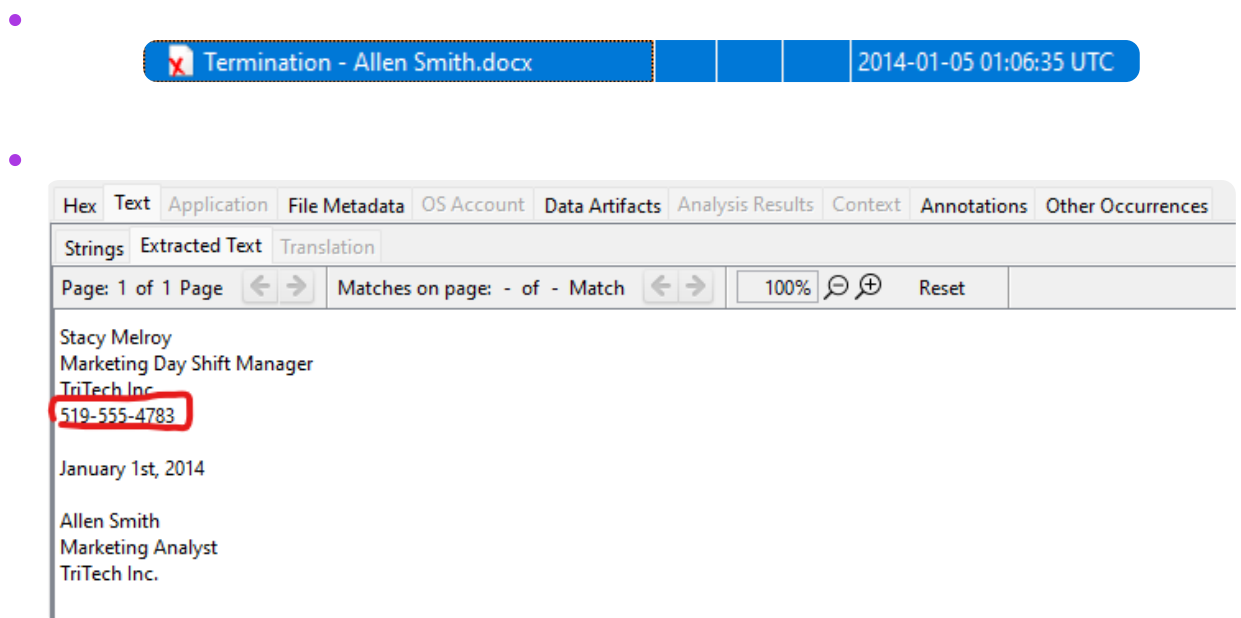


Name	S	C	O	Modified Time
Voicemail 1.wav				0000-00-00 00:00:00
Voicemail 1.wav:Zone.Identifier				2013-06-22 02:28:35 UTC
Voicemail 1.wav				2013-06-22 02:28:35 UTC

### 2. Localización de la contraseña

- Investigando los archivos de texto y registros, encontramos **un número telefónico** anotado en la carpeta de documentos del usuario.

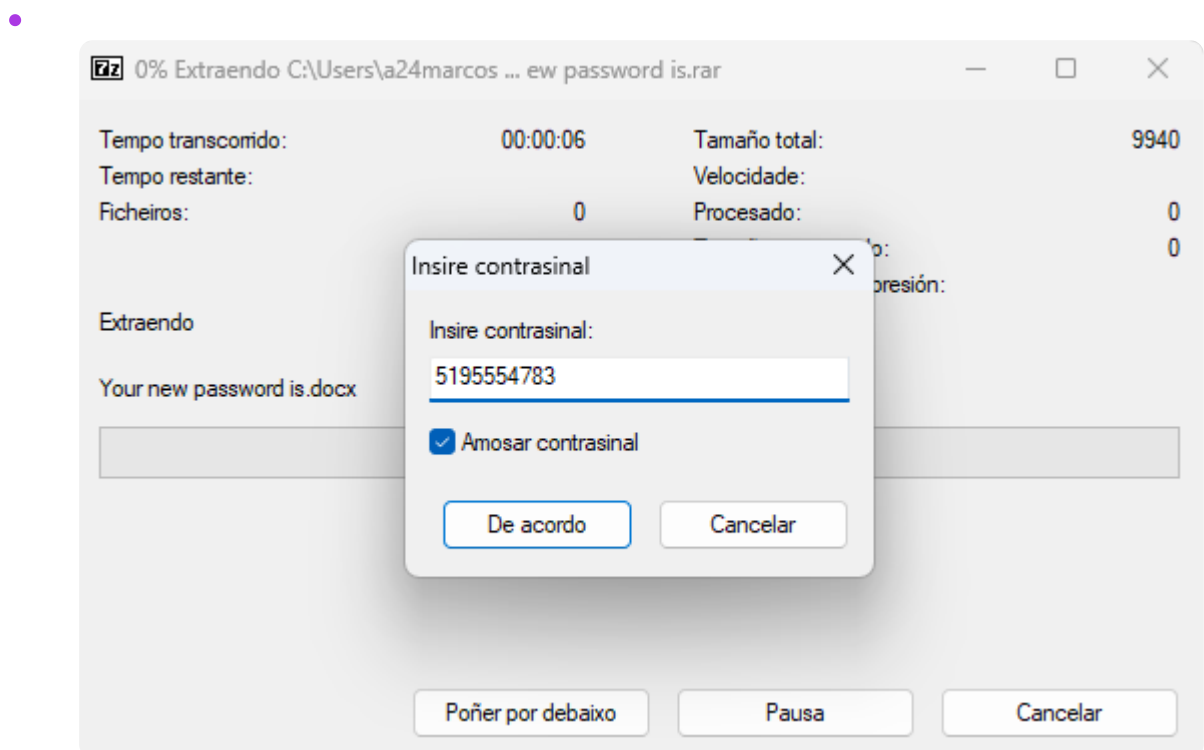
- Capturas que muestran este número:



- Por la relación con el audio, este número se convirtió en nuestro principal candidato para **descomprimir** los archivos **.zip**.

### 3. Desencriptado del .zip

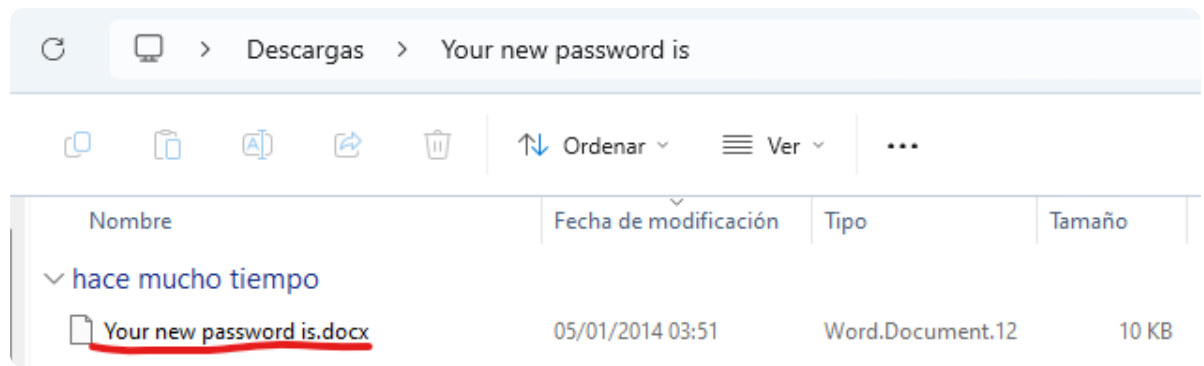
- Utilicé **7-Zip** con la contraseña obtenida y logré extraer el contenido de **evidence1.zip** sin problemas.
- **Captura del proceso:**



### 4. Archivos recuperados tras desencriptar



- Al desencriptar correctamente, apareció un nuevo fichero de extensión **.docx** (o **.pdf**, según el caso).
- Captura que muestra el archivo dentro de la carpeta extraída:



### 5. Acceso al contenido final

- Al abrir dicho archivo, se pudo comprobar que contenía información sensible o relevante para el caso:

Your new password is 'qPYgbs0w5&?i{8a'.

## 3. Ejercicio 3

### 3.1 Sistema operativo instalado

Este ejercicio se centra en descubrir y confirmar el **sistema operativo** que estaba instalado en la imagen de disco que se está analizando.

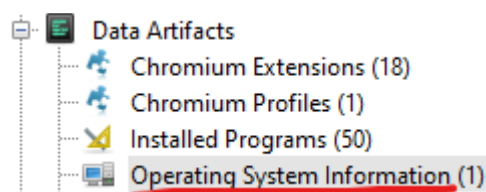
#### • Procedimiento en Autopsy:

##### 1. Revisión de artefactos relacionados con la configuración del SO:

- Dentro de **Autopsy**, me dirigí a la sección de "*Data Artifacts*" (Artefactos de datos) y busqué en las categorías relacionadas con la configuración de Windows.
- Identifiqué varias rutas de interés, entre ellas el contenido del **Registro (Registry)**, en particular la sección **SYSTEM**, que suele mostrar la versión exacta del sistema operativo.



##### 2. Capturas de pantalla:

- A continuación se muestran algunas capturas que ejemplifican la navegación en Autopsy:



(Aquí se ve la sección donde se listan los datos de artefactos, incluyendo información del sistema operativo).

- Al adentrarnos en la clave **SYSTEM**, observamos:


Listing							
Operating System Information							
Table Thumbnail Summary							
Source Name	S	C	O	Name	Domain	Version	Processor Architecture
 <b>SYSTEM</b>				DESKTOP-PM6C56D		Windows_NT	AMD64
 <b>SOFTWARE</b>							

- (Visualización de la estructura interna del registro del sistema).
- Se identifica la **versión de Windows** como Windows NT:

Hex	Text	Application	Source File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Result: 11 of 39 Result < >									
Operating System Information									
Type	Value								Source(s)
Name	DESKTOP-PM6C56D								Recent Activit
Domain									Recent Activit
Version	Windows_NT								Recent Activit
Processor Arc	AMD64								Recent Activit
Temporary Fil	%SystemRoot%\TEMP								Recent Activit
Source File Pa	/img_LoneWolf.E01/vol_vol7/Windows/System32/config/SYSTEM								
Artifact ID	-9223372036854775622								

- **Confirmación con Windows Registry Recovery:**

- Para **validar** lo visto en Autopsy, usé la herramienta **Windows Registry Recovery** (u otra similar).
- **Captura del análisis:**



Type: Windows NT Registry  
Last modified: 15/01/2025 19:56:10  
Hive name: SYSTEM  
Checksum: 8F1B7EEB  
Number of keys: 33123  
Number of HBINs: 2704  
Loading time: 0,78 s

CRC32: 486EC467  
CRC64: B83EA4A9BFDDED2E1  
MD5: 2F6CFBCC55D5C8137FEB4F3BA2D30C74  
SHA1: FBBDDBD0EB39A87BB9C10F50BB28000DE71F8641  
SHA256: 9154E260ABDC4AC206EF9D872DD4E1ADD0150B869BDA5B112944AF2FF5EC39B4

- Allí se confirma la versión, la edición y posibles valores adicionales que ayudan a corroborar que se trata de **Windows NT**.

## Conclusión:

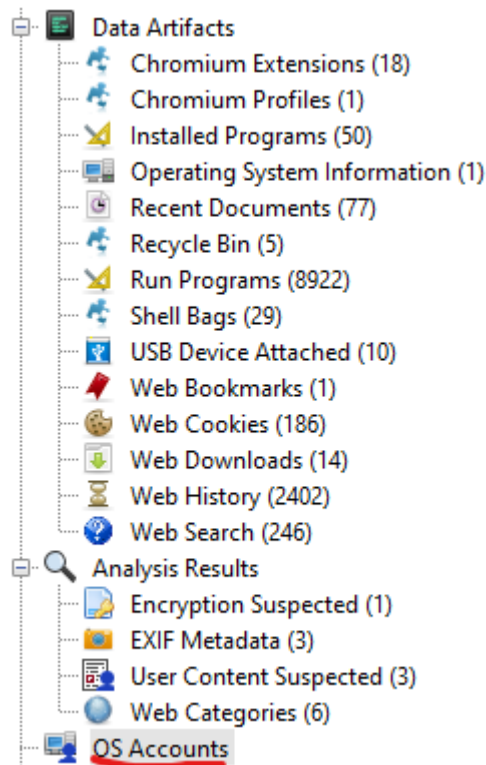
La evidencia indica que el sistema operativo es **Windows NT**. Con la confirmación cruzada de Autopsy y Windows Registry Recovery, nos aseguramos de que la información es confiable.

## 3.2 Identificación de usuarios

En este apartado, la meta es **encontrar a los usuarios** registrados en el sistema y recopilar información básica de sus cuentas (nombres, SID, tipos de cuenta, etc.).

- **Procedimiento:**

1. Dentro de **Autopsy**, en la sección **OS Accounts**, se listan las cuentas de usuario que el sistema ha identificado.



2. Revisión de la lista para buscar el usuario de interés, en este caso **"jcloudy"**.

Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time
S-1-5-18				SYSTEM	LoneWolf.E01_1 Host	Local	NT AUTHORITY	
S-1-5-80-956008885-3418522649-1831038044-18532			0		LoneWolf.E01_1 Host	Local	NT SERVICE	
S-1-5-21-2734969515-1644526556-1039763013-1001			0	jcloudy	LoneWolf.E01_1 Host	Domain		2018-03-27 09:18:58 UTC
S-1-5-80-3028837079-3186095147-955107200-37019			0		LoneWolf.E01_1 Host	Local	NT SERVICE	
S-1-5-20				NETWORK SERVICE	LoneWolf.E01_1 Host	Local	NT AUTHORITY	
S-1-5-19				LOCAL SERVICE	LoneWolf.E01_1 Host	Local	NT AUTHORITY	
S-1-5-21-397955417-626881126-188441444-4882392			0		LoneWolf.E01_1 Host	Domain		
S-1-5-21-2734969515-1644526556-1039763013-503			0	DefaultAccount	LoneWolf.E01_1 Host	Domain		2018-03-27 12:13:26 UTC
S-1-5-21-2734969515-1644526556-1039763013-500			0	Administrator	LoneWolf.E01_1 Host	Domain		2018-03-27 12:13:26 UTC
S-1-5-21-2734969515-1644526556-1039763013-501			0	Guest	LoneWolf.E01_1 Host	Domain		2018-03-27 12:13:26 UTC
S-1-5-21-2734969515-1644526556-1039763013-504			0	WDAGUtilityAccount	LoneWolf.E01_1 Host	Domain		2018-03-27 12:13:26 UTC

3. Comprobación de atributos de la cuenta, como el nombre completo o las propiedades del SID, para confirmar que se trata efectivamente de la cuenta **Jcloudy**.

#### Basic Properties

Login: jcloudy  
Full Name:  
Address: S-1-5-21-2734969515-1644526556-1039763013-1001  
Type:  
Creation Date: 2018-03-27 09:18:58 UTC  
Object ID: 785

### Conclusión:

Se encontraron exitosamente las cuentas y datos relacionales.



## 3.3 Último inicio de sesión del usuario "jcloudy"

El objetivo aquí es establecer la **fecha y hora** del último inicio de sesión de **jcloudy**, un dato muy relevante en la investigación forense, pues permite entender cuándo se usó la cuenta por última vez.

### Procedimiento:

#### 1. Extracción del registro y análisis:

- Se accedió a la información de la cuenta "**jcloudy**" en la base de datos del **Registro** (o en los artefactos que Autopsy interpreta), buscando la sección que registra el **Last Login**.

S-1-5-21-2734969515-1644526556-1039763013-1001	0	jcloudy	LoneWolf.E01_1 Host	Domain	2018-03-27 09:18:58 UTC
--	---	---------	---------------------	--------	-------------------------

- Aquí se observa la fecha y hora del último inicio de sesión.

#### LoneWolf.E01\_1 Host Details

Last Login: 2018-04-06 14:26:27 CEST

#### 2. Confirmación con Windows Registry Recovery:

- Realicé una segunda revisión de la misma clave usando Windows Registry Recovery o una herramienta similar, para confirmar la precisión.
- Se observó una **discrepancia horaria** (posiblemente por la **zona horaria** o DST), aunque los **minutos y segundos** coinciden.

SAM	
NAVIGATOR	General Groups and Users
File Information	Users
Security Records	Administrator
SAM	Guest
Windows Installation	DefaultAccount
	WDAGUtilityAccount
	jcloudy
	Property Value
	SID S-1-5-21-2734969515-1644526556-1039763013-1001
	Last login 06/04/2018 12:26:27
	Last password set 27/03/2018 09:18:58
	Account expiration 30/12/1899 02:48:05
	Last incorrect password 06/04/2018 03:30:52

- Se determinó que la causa del desfase podría ser la configuración horaria del sistema al momento de la toma de la imagen.

### Conclusión:

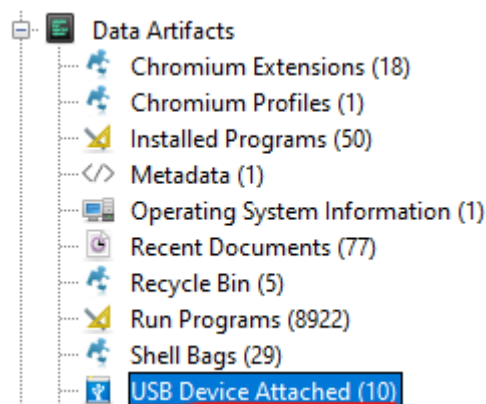
El último inicio de sesión de **jcloudy** ocurrió en la hora encontrada en Autopsy (2018-04-06 14:26:27 CEST), con una pequeña variación de 2 horas atribuible a la configuración horaria del equipo.



## 3.4 Información sobre pendrives insertados

Aquí se busca rastrear los **dispositivos USB** (memorias, discos externos, etc.) que se han conectado a la máquina y cuándo.

- **Marca y modelo:**
  - Para identificar estos datos, se emplea Autopsy y las secciones de **artefactos USB** (o "USB Device").
- **Procedimiento:**
  1. Dentro de **Autopsy**, navegué a "Data Artifacts" > "USB Device":





2. Aparecen varios registros que muestran el **VID** (Vendor ID), **PID** (Product ID), fechas de primera y última inserción, y a veces el nombre comercial del dispositivo.

Listing								
USB Device Attached								
Table Thumbnail Summary								
Source Name	S	C	O	Date/Time	Device Make	Device Model	Device ID	Data Source
SYSTEM			1	2018-03-27 21:45:42 UTC		ROOT_HUB20	48x1671a218&0	LoneWolf.E01
SYSTEM			1	2018-03-27 21:45:42 UTC		ROOT_HUB20	48xb21407d8&0	LoneWolf.E01
SYSTEM			1	2018-03-27 21:45:43 UTC		ROOT_HUB30	48x2d689036&0&0	LoneWolf.E01
SYSTEM			1	2018-03-27 12:13:16 UTC	SanDisk Corp.	SDCZ80 Flash Drive	AA010215170355310594	LoneWolf.E01
SYSTEM			1	2018-03-27 21:45:44 UTC	SanDisk Corp.	SDCZ80 Flash Drive	AA010603160707470215	LoneWolf.E01
SYSTEM			1	2018-03-27 21:45:44 UTC	Microdia	Dell Integrated HD Webcam	68xc0f0d73&0&5	LoneWolf.E01
SYSTEM			1	2018-03-27 21:45:44 UTC	Microdia	Dell Integrated HD Webcam	78x2bca401f&0&0000	LoneWolf.E01
SYSTEM			1	2018-03-27 21:45:44 UTC	Dell Computer Corp.	BCM20702A0 Bluetooth Module	28E347017777	LoneWolf.E01
SYSTEM			1	2018-03-27 21:45:43 UTC	Intel Corp.	Integrated Rate Matching Hub	58x182c2717&0&1	LoneWolf.E01
SYSTEM			1	2018-03-27 21:45:44 UTC	Intel Corp.	Integrated Rate Matching Hub	58x2cd6d949&0&1	LoneWolf.E01

3. Revisando la información concreta de cada uno, se obtienen detalles como:

- **Marca** (por ejemplo, Kingston, SanDisk, etc.).
- **Modelo** (identificación genérica u oficial, según qué tan completa sea la información guardada en Windows).

#### 4. Capturas con ejemplos de la información que se puede ver:

Hex	Text	Application	Source File Metadata	OS Account	Data Artifacts	Analysis Results	Context
Result: 1 of 38      Result  							
Type	Value						
Date/Time	2018-03-27 21:45:42 UTC						
Device Make							
Device Model	ROOT_HUB20						
Device ID	4&1671a21&0						
Source File Path	/img_LoneWolf.E01/vol_vol7/Windows/System32/config/SYSTEM						
Artifact ID	-9223372036854775632						

Hex	Text	Application	Source File Metadata	OS Account	Data Artifacts	Analysis Results	Context
Result: 2 of 38      Result    ⏪    ⏩							
Type		Value					
Date/Time		2018-03-27 21:45:42 UTC					
Device Make							
Device Model		ROOT_HUB20					
Device ID		48&b21407d&0					
Source File Path		/img_LoneWolf.E01/vol_vol7/Windows/System32/config/SYSTEM					
Artifact ID		-9223372036854775631					

Hex	Text	Application	Source File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Result: 3 of 38      Result    ⏪    ⏩									
Type		Value							
Date/Time		2018-03-27 21:45:43 UTC							
Device Make									
Device Model		ROOT_HUB30							
Device ID		48x2d6890368x08x0							
Source File Path		/img_LoneWolf.E01/vol_vol7/Windows/System32/config/SYSTEM							
Artifact ID		-9223372036854775630							



- 

Result: 8 of 38 Result < >	
Type	Value
Date/Time	2018-03-27 21:45:44 UTC
Device Make	Dell Computer Corp.
Device Model	BCM20702A0 Bluetooth Module
Device ID	28E347017777
Source File Path	/img_LoneWolf.E01/vol_vol7/Windows/System32/config/SYSTEM
Artifact ID	-9223372036854775625

- 

Result: 9 of 38 Result < >	
Type	Value
Date/Time	2018-03-27 21:45:43 UTC
Device Make	Intel Corp.
Device Model	Integrated Rate Matching Hub
Device ID	5&182c2717&0&1
Source File Path	/img_LoneWolf.E01/vol_vol7/Windows/System32/config/SYSTEM
Artifact ID	-9223372036854775624

- 

Result: 10 of 38 Result < >	
Type	Value
Date/Time	2018-03-27 21:45:44 UTC
Device Make	Intel Corp.
Device Model	Integrated Rate Matching Hub
Device ID	5&2cd6d949&0&1
Source File Path	/img_LoneWolf.E01/vol_vol7/Windows/System32/config/SYSTEM
Artifact ID	-9223372036854775623

### Conclusión:

Identificamos varios dispositivos USB, con información de **fechas de conexión** y posibles detalles de su **fabricante** o **modelo**, lo que podría ser crucial para entender qué datos se transfirieron y cuándo.



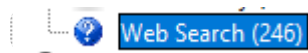
## 3.5 Búsqueda de información sobre armas de fuego

En este paso, se investigó si el usuario realizó **búsquedas o visitas web** sobre temas de armas de fuego.

- **Metodología:**



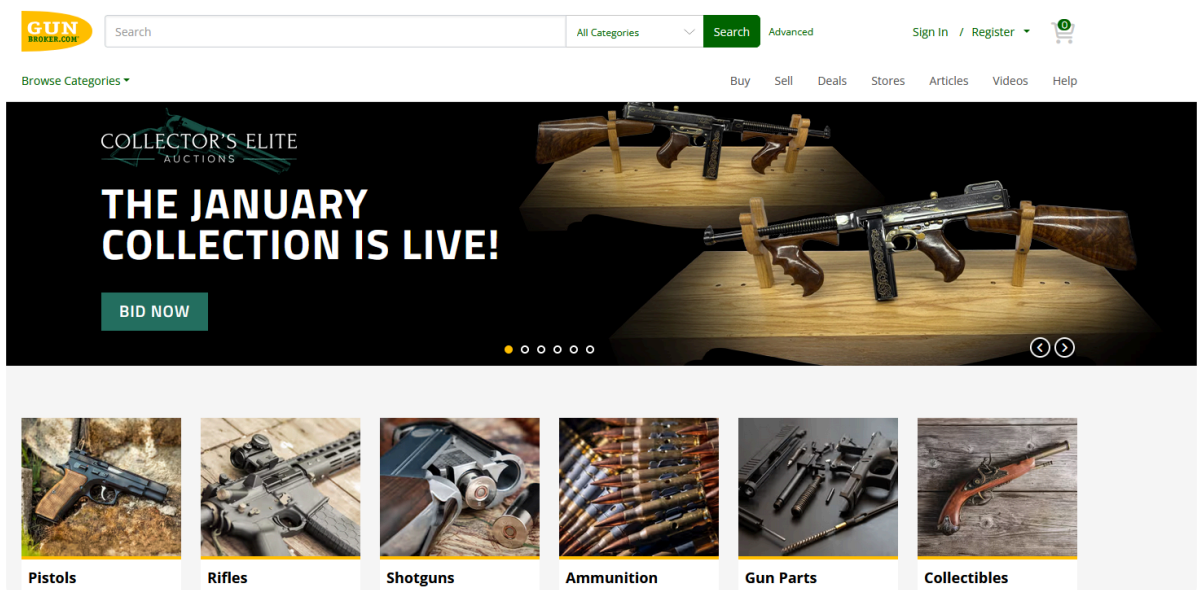
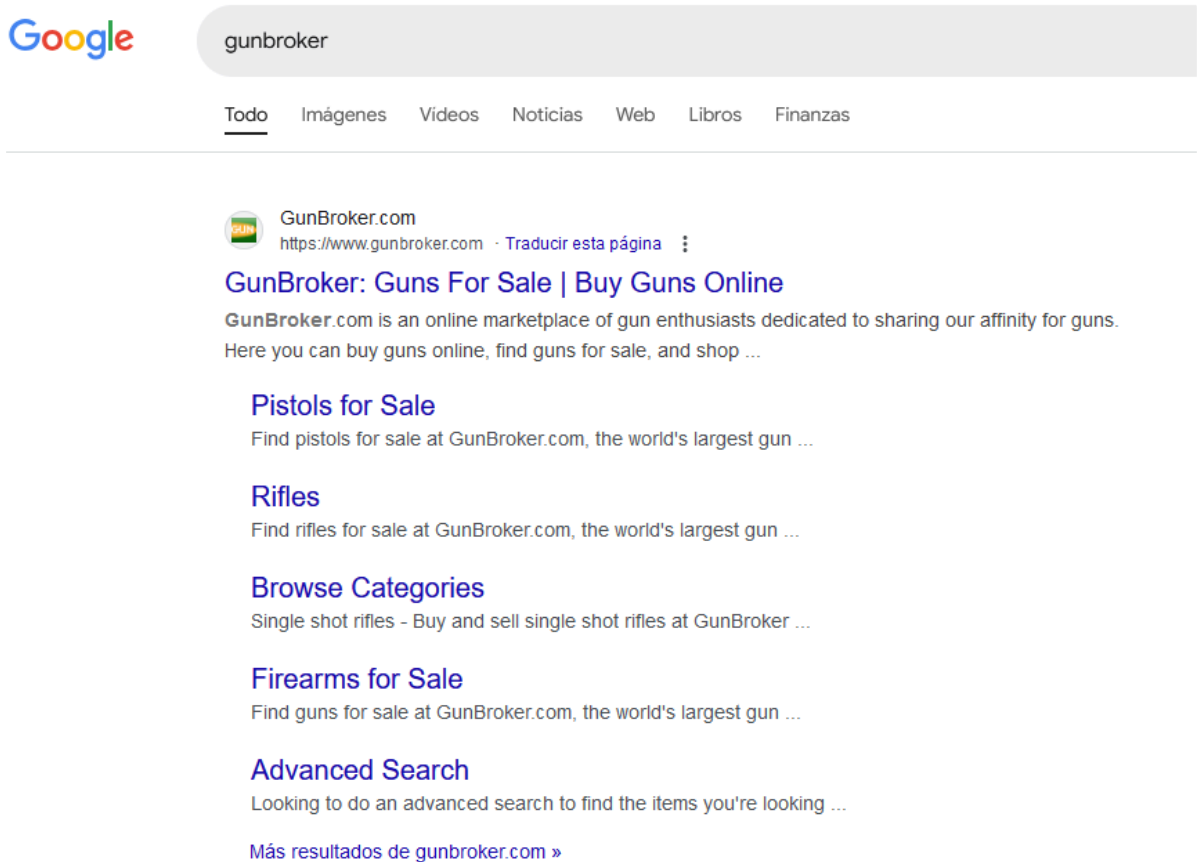
1. Revisión de la sección "Web Search" en Autopsy:



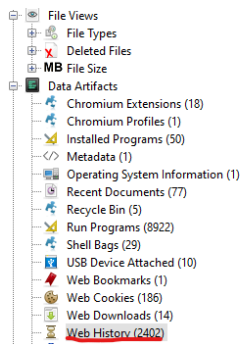
2. Identificación de **Gunbroker** en el historial de búsquedas y/o de navegación:



3. Correlación con búsquedas en Google o enlaces directos que apunten a la **tienda de armas**



#### 4. Confirmación final en la sección de "History":



History	Count	URL	Time
History	1	https://www.google.com/search?q=shooting+range+...	2018-03-28 01:09:33 UTC
History	0	https://www.gunbroker.com/FN-P90/Browse.aspx?Ke...	2018-03-28 01:10:15 UTC
History	0	https://www.gunbroker.com/#home-footer	2018-03-28 01:10:21 UTC
History	0	https://www.gunbroker.com/All/search	2018-03-28 01:10:27 UTC
History	0	https://www.gunbroker.com/All/search?Keywords=fn...	2018-03-28 01:10:28 UTC
History	0	https://www.gunbroker.com/All/search?Keywords=fn...	2018-03-28 01:10:28 UTC
History	0	https://www.gunbroker.com/All/search?Keywords=fn...	2018-03-28 01:11:02 UTC
History	0	https://www.gunbroker.com/All/search?Keywords=fn...	2018-03-28 01:11:01 UTC
History	0	https://www.gunbroker.com/All/search?Keywords=fn...	2018-03-28 01:11:00 UTC
History	0	https://www.gunbroker.com/All/search?Keywords=fn...	2018-03-28 01:11:01 UTC
History	0	https://www.gunbroker.com/All/search?Keywords=fn...	2018-03-28 01:11:00 UTC
History	0	https://www.gunbroker.com/All/search?Keywords=fn...	2018-03-28 01:11:00 UTC
History	0	https://www.gunbroker.com/All/search?Keywords=fn...	2018-03-28 01:11:02 UTC
History	0	https://www.gunbroker.com/All/search?PageSize=24...	2018-03-31 04:34:15 UTC
History	0	https://www.gunbroker.com/All/search?Keywords=fn...	2018-03-28 01:11:09 UTC
History	0	https://www.gunbroker.com/All/search?Keywords=fn...	2018-03-28 01:11:10 UTC

#### Conclusión:

Los registros de navegación evidencian que el usuario realizó consultas sobre **armas de fuego** en sitios web especializados (como Gunbroker). Esta información podría ser relevante para la hipótesis investigativa (por ejemplo, intenciones de compra, investigación, etc.).

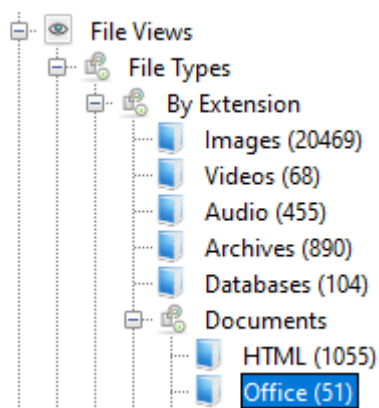


### 3.6 Archivo "Planning.docx"

El archivo "Planning.docx" parece ser un documento clave que aparece en distintos lugares del disco.

#### • Ocurrencias encontradas:

1. Dentro de **File Views > File Types > By Extension > Documents > Office**, se listan múltiples instancias de **Planning.docx**.



Planning.docx			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
~\$anning.docx			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
~\$RPORT INFORMATION.docx			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
AIRPORT INFORMATION.docx:com.dropbox.attrs			2018-04-05 02:13:38 UTC	2018-04-06 12:35:28 UTC	2018-04-06 12:35:28 UTC	2018-04-06 12:35:25 UTC
Planning.docx:com.dropbox.attrs			2018-04-05 02:14:03 UTC	2018-04-06 12:35:28 UTC	2018-04-06 12:35:28 UTC	2018-04-06 12:35:25 UTC
Operation 2nd Hand Smoke.pptx			2018-04-04 05:11:27 UTC	2018-04-05 02:11:18 UTC	2018-04-05 02:11:16 UTC	2018-04-04 05:32:03 UTC
Operation 2nd Hand Smoke.pptx			2018-04-04 05:11:27 UTC	2018-04-04 05:11:53 UTC	2018-04-04 05:11:27 UTC	2018-04-04 04:56:19 UTC
Operation 2nd Hand Smoke.pptx			2018-04-04 05:11:27 UTC	2018-04-06 12:35:19 UTC	2018-04-04 05:32:30 UTC	2018-04-04 05:32:30 UTC
Operation 2nd Hand Smoke.pptx			2018-04-04 05:11:27 UTC	2018-04-04 05:32:04 UTC	2018-04-04 05:31:54 UTC	2018-04-04 05:31:54 UTC
Operation 2nd Hand Smoke.pptx			2018-04-04 05:11:27 UTC	2018-04-04 05:11:53 UTC	2018-04-04 05:32:34 UTC	2018-04-04 05:32:34 UTC
TM02835233[[fn=Text Sidebar (Annual Report Red z			2018-03-30 02:16:24 UTC	2018-03-30 02:16:24 UTC	2018-03-30 02:16:24 UTC	2018-03-30 02:16:24 UTC
AIRPORT INFORMATION.docx			2018-04-04 04:59:32 UTC	2018-04-05 02:21:10 UTC	2018-04-05 02:21:10 UTC	2018-04-04 04:59:32 UTC
Planning.docx			2018-04-04 05:30:41 UTC	2018-04-05 02:21:04 UTC	2018-04-05 02:21:04 UTC	2018-04-04 05:30:41 UTC

Planning.docx			2018-04-04 05:30:41 UTC	2018-04-05 02:21:04 UTC	2018-04-05 02:21:04 UTC	2018-04-04 05:30:41 UTC
The Cloudy Manifesto.docx			2018-04-02 01:35:27 UTC	2018-04-05 02:11:16 UTC	2018-04-05 02:11:15 UTC	2018-04-02 01:36:38 UTC
AIRPORT INFORMATION.docx			2018-04-04 04:59:32 UTC	2018-04-04 04:59:40 UTC	2018-04-04 04:59:32 UTC	2018-03-30 02:29:57 UTC
Cloudy thoughts (4apr).docx			2018-04-05 02:39:30 UTC	2018-04-05 02:39:41 UTC	2018-04-05 02:39:30 UTC	2018-04-05 02:39:29 UTC
Planning.docx			2018-04-04 05:30:41 UTC	2018-04-04 05:30:49 UTC	2018-04-04 05:30:41 UTC	2018-03-30 02:16:48 UTC
The Cloudy Manifesto.docx			2018-04-02 01:35:27 UTC	2018-04-02 01:35:39 UTC	2018-04-02 01:35:27 UTC	2018-04-02 01:35:27 UTC
AIRPORT INFORMATION.docx			2018-04-05 02:13:38 UTC	2018-04-06 12:35:28 UTC	2018-04-06 12:35:28 UTC	2018-04-06 12:35:25 UTC
Planning.docx			2018-04-05 02:14:03 UTC	2018-04-06 12:35:28 UTC	2018-04-06 12:35:28 UTC	2018-04-06 12:35:25 UTC
The Cloudy Manifesto.docx			2018-04-02 01:35:27 UTC	2018-04-02 01:43:42 UTC	2018-04-02 01:36:45 UTC	2018-04-02 01:36:45 UTC
The Cloudy Manifesto.docx			2018-04-02 01:35:27 UTC	2018-04-02 01:36:35 UTC	2018-04-02 01:36:28 UTC	2018-04-02 01:36:28 UTC
AIRPORT INFORMATION.docx			2018-04-04 04:59:32 UTC	2018-04-05 02:21:38 UTC	2018-04-05 02:21:38 UTC	2018-04-05 02:21:37 UTC
Planning.docx			2018-04-04 05:30:41 UTC	2018-04-05 02:21:37 UTC	2018-04-05 02:21:37 UTC	2018-04-05 02:21:37 UTC
The Cloudy Manifesto.docx			2018-04-02 01:35:27 UTC	2018-04-02 01:35:39 UTC	2018-04-02 01:36:52 UTC	2018-04-02 01:36:52 UTC
AIRPORT INFORMATION.docx:com.dropbox.attri			2018-04-05 02:13:38 UTC	2018-04-06 12:35:28 UTC	2018-04-06 12:35:28 UTC	2018-04-06 12:35:25 UTC
Operation 2nd Hand Smoke.pptx:com.dropbox.attr			2018-04-04 05:11:27 UTC	2018-04-06 12:35:19 UTC	2018-04-04 05:32:30 UTC	2018-04-04 05:32:30 UTC
Planning.docx:com.dropbox.attributes			2018-04-05 02:14:03 UTC	2018-04-06 12:35:28 UTC	2018-04-06 12:35:28 UTC	2018-04-06 12:35:25 UTC
The Cloudy Manifesto.docx:com.dropbox.attribute			2018-04-02 01:35:27 UTC	2018-04-02 01:43:42 UTC	2018-04-02 01:36:45 UTC	2018-04-02 01:36:45 UTC

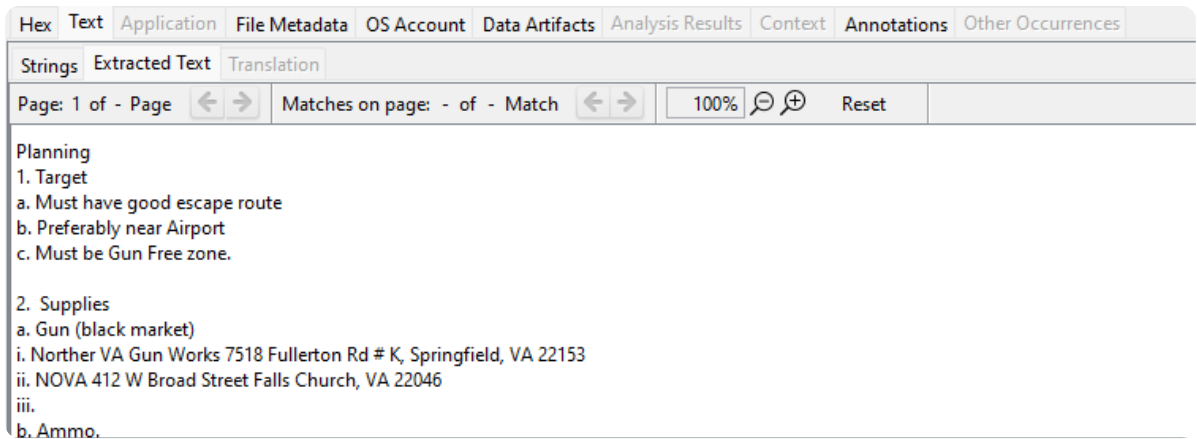
2. Algunas copias podrían ser recuperadas de la papelera o de archivos temporales, lo que explica la **multiplicidad** de ocurrencias.

### • Primera aparición:

- De acuerdo con las **marcas de tiempo** en la metadata del archivo, la primera creación (fecha más antigua) data de **2018-03-30**.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
Operation 2nd Hand Smoke.pptx				2018-04-04 05:11:27 UTC	2018-04-06 12:35:19 UTC	2018-04-04 05:32:30 UTC	2018-04-04 05:32:30 UTC
Operation 2nd Hand Smoke.pptx				2018-04-04 05:11:27 UTC	2018-04-04 05:32:04 UTC	2018-04-04 05:31:54 UTC	2018-04-04 05:31:54 UTC
Operation 2nd Hand Smoke.pptx				2018-04-04 05:11:27 UTC	2018-04-04 05:11:53 UTC	2018-04-04 05:32:34 UTC	2018-04-04 05:32:34 UTC
TM02835233[[fn=Text Sidebar (Annual Report Red z				2018-03-30 02:16:24 UTC	2018-03-30 02:16:24 UTC	2018-03-30 02:16:24 UTC	2018-03-30 02:16:24 UTC
AIRPORT INFORMATION.docx				2018-04-04 04:59:32 UTC	2018-04-05 02:21:10 UTC	2018-04-05 02:21:10 UTC	2018-04-04 04:59:32 UTC
Planning.docx				2018-04-04 05:30:41 UTC	2018-04-05 02:21:04 UTC	2018-04-05 02:21:04 UTC	2018-04-04 05:30:41 UTC
The Cloudy Manifesto.docx				2018-04-02 01:35:27 UTC	2018-04-05 02:11:16 UTC	2018-04-05 02:11:15 UTC	2018-04-02 01:36:38 UTC
AIRPORT INFORMATION.docx				2018-04-04 04:59:32 UTC	2018-04-04 04:59:40 UTC	2018-04-04 04:59:32 UTC	2018-03-30 02:29:57 UTC
Cloudy thoughts (4apr).docx				2018-04-05 02:39:30 UTC	2018-04-05 02:39:41 UTC	2018-04-05 02:39:30 UTC	2018-04-05 02:39:29 UTC
Planning.docx				2018-04-04 05:30:41 UTC	2018-04-04 05:30:49 UTC	2018-04-04 05:30:41 UTC	2018-03-30 02:16:48 UTC

- Al abrir el contenido, se observan referencias que indican **planes, cronogramas** o información sensible:



- **Motivo por el cual hay varias apariciones**

- Porque es un recurso al que se accede mucho debe ser algo de trabajo o un planing que hay que consultar a menudo y cambiar cosas

**Conclusión:**

“Planning.docx” tiene una importancia significativa en el caso, por la temática de su contenido (posiblemente planes u organización del usuario), y la fecha más antigua nos da una pista de cuándo comenzó a elaborarse la información.

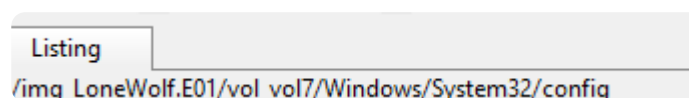


## 3.7 Identificación de la tarjeta gráfica






















Por último, se explora el **hardware** presente en el sistema, concretamente la **tarjeta gráfica**.

- **Método de análisis:**

1. Ubicación de claves de registro que enumeran hardware, incluido el adaptador de video:
  - En la ruta /img\_LoneWolf.E01/vol\_vol7/Windows/System32/config



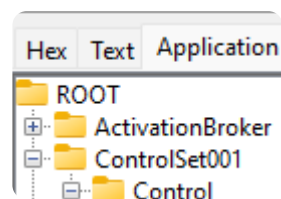
- Encontramos el archivo SYSTEM

Listing	
/img_LoneWolf.E01/vol_vol7/Windows/System32/config	
Table	Thumbnail Summary
Name	
	ELAM{426bc134-a4f2-11e7-aa16-e41d2d129fe0}.TM
	ELAM{426bc134-a4f2-11e7-aa16-e41d2d129fe0}.TM
	SAM
	SAM.LOG1
	SAM.LOG2
	SAM{47a6a13d-a514-11e7-a94e-ec0d9a05c860}.TM
	SAM{47a6a13d-a514-11e7-a94e-ec0d9a05c860}.TM
	SAM{47a6a13d-a514-11e7-a94e-ec0d9a05c860}.TM
	SECURITY
	SECURITY.LOG1
	SECURITY.LOG2
	SECURITY{47a6a12e-a514-11e7-a94e-ec0d9a05c860
	SECURITY{47a6a12e-a514-11e7-a94e-ec0d9a05c860
	SECURITY{47a6a12e-a514-11e7-a94e-ec0d9a05c860
	SOFTWARE
	SOFTWARE.LOG1
	SOFTWARE.LOG2
	SOFTWARE{47a6a11d-a514-11e7-a94e-ec0d9a05c860
	SOFTWARE{47a6a11d-a514-11e7-a94e-ec0d9a05c860
	SOFTWARE{47a6a11d-a514-11e7-a94e-ec0d9a05c860
	SYSTEM

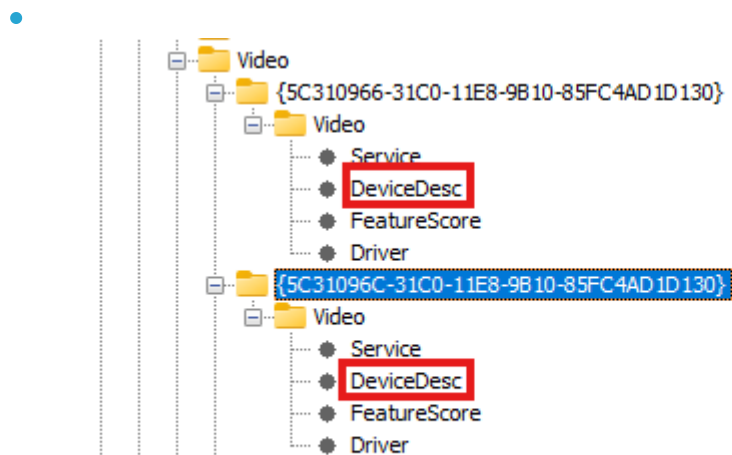
2. En una subcarpeta de **Control** o similar, encontramos la mención explícita a **Intel(R) HD Graphics 4000 Y A Nvidia NVS 5200M:**

- En la ruta ROOT/ControlSet001/Control

•



- Accedemos a



- Y encontramos en esos dos archivos 2 tarjetas graficas
  - La grafica integrada HD Graphics 4000

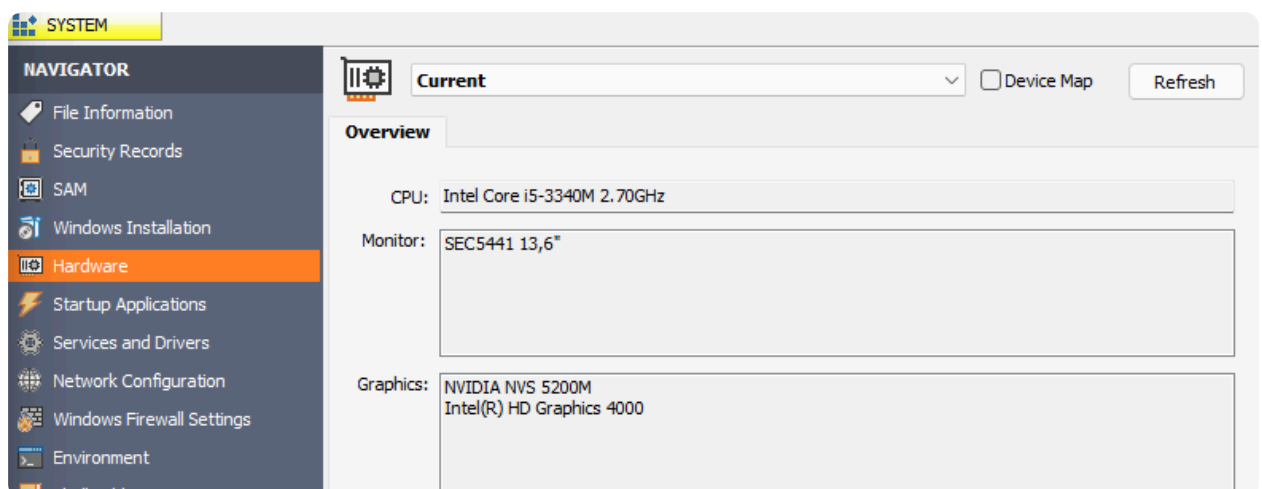
Metadata
Name: <b>DeviceDesc</b>
Type: REG_SZ
Value
@oem9.inf,%iivbgm0%;Intel(R) HD Graphics 4000

- Y la grafica externa de NVIDIA NVS 5200M

Metadata
Name: <b>DeviceDesc</b>
Type: REG_SZ
Value
@oem4.inf,%nvidia_dev.0dfc.1534.1028%;NVIDIA NVS 5200M

3. Confirmación en Autopsy o Windows Registry Recovery de que la tarjeta es **Intel(R) HD Graphics 4000**.

4.



• **Resultados:**

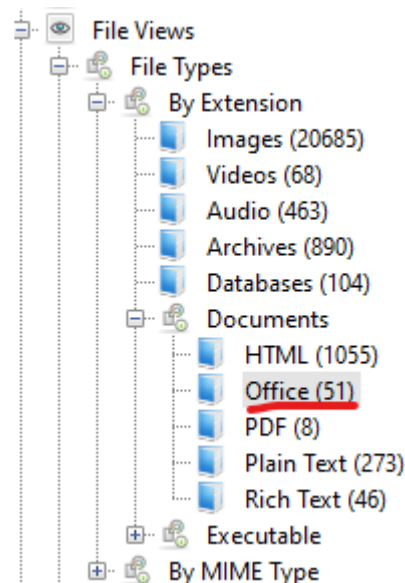
- **Marcas:** Intel , Nvidia
- **Modelo:** HD Graphics 4000 , NVS 5200M

### Conclusión:

Se determinó con precisión qué gráfica estaba instalada, lo cual puede ser útil si, por ejemplo, se investiga si la máquina cumplía ciertos requisitos para instalar software específico o para manipular archivos de video/imágenes de alta resolución.

## 3.8 Acceso a cuentas en la nube de jcloudy

- **Identificación de la otra persona:**
  - En tipos de archivo por extension de "office"



- Se encuentra le archivo Cloudy thoughts.docx

Listing

Office

Table











Thumbnail

Summary

Page: 1 of 1

Pages: < >

Go to Page:

Name	S	C	O	Modified Time
 Operation 2nd Hand Smoke.pptx			1	2018-04-04 05:11:27 UTC
 Operation 2nd Hand Smoke.pptx			1	2018-04-04 05:11:27 UTC
 Operation 2nd Hand Smoke.pptx			1	2018-04-04 05:11:27 UTC
 TM02835233[[fn= Text Sidebar (Annual Report Red a			0	2018-03-30 02:16:24 UTC
 AIRPORT INFORMATION.docx			1	2018-04-04 04:59:32 UTC
 Planning.docx			1	2018-04-04 05:30:41 UTC
 The Cloudy Manifesto.docx			1	2018-04-02 01:35:27 UTC
 AIRPORT INFORMATION.docx			1	2018-04-04 04:59:32 UTC
 Cloudy thoughts (4apr).docx			0	2018-04-05 02:39:30 UTC
 Planning.docx			1	2018-04-04 05:30:41 UTC

- Que contiene la información de que el Nombre es Paul

Page: 1 of 1 Page   Matches on page: - of - Match   100%   Reset   Text Source: File Text

I don't know if this plan will work. Plans never survive first contact. I don't expect to fail, but there are so many possibilities. But now the weather. Its going to snow, and the winds will be strong. No problem for the attack, but if my flight is delayed or cancelled, that might prove to be a problem.

I'm stressed and writing used to help me calm down. It seems to be working. Im leaving a lot behind, and the weight of this responsibility is almost too much to handle. I wont stop now, though. Even if I'm killed at the site, I know that what im doing is just and right. Freedom requires sacrifice. If I must be that lamb, then I walk to my slaughter freely of my own accord.

I am saving everything to the cloud on several accounts. I don't want my words mixed up, and I don't want my thoughts deleted. I want my family to understand why I did this. I think they will keep my secret if I am successful and leave the country without problems. The only record will remain in the cloud and Paul will have the only other keys.

My fate will be in God's hands. I pray I have the strength and the luck necessary to persevere. Please let the weather clear!

Paul will have the only other keys.

## Conclusión:

**La existencia del archivo *Cloudy thoughts.docx* demuestra que el usuario jcloudy comparte o almacena parte de su información en la nube, y que colabora con una persona identificada como Paul\*\*.** Esto sugiere la posibilidad de comunicación o intercambios de ficheros con terceros, información que podría resultar clave para la investigación forense si se precisan vínculos o redes de contactos del usuario.