

Análisis con Autopsy



José Enrique Gallego León

Contenido

Introducción	3
1. Iniciación con Autopsy	3
2. Búsqueda de datos e información comprometida.....	6
Schedule visits.xls	8
Cover page.jpgc.....	11
Pasos finales	14
3. Respuestas a las preguntas propuestas	16
Posibles fallos.....	17

José Enrique Gallego León

Introducción

En este documento veremos como resolver un caso de Análisis Forense de manera práctica, el escenario es ficticio y cuenta el caso de Joe Jacobs, un traficante de drogas que se mueve por varias escuelas de secundaria vendiendo a los diferentes escolares.

Herramientas que vamos a utilizar en esta práctica guiada:

- [*Documento explicativo y contexto del caso de Joe Jacobs*](#)
- [*Disquette de Joe Jacobs*](#)
- [*Autopsy v4.21.0*](#)
- [*HxD - Freeware Hex Editor and Disk Editor*](#)

Con toda esta información y las herramientas ya descargadas e instaladas vamos a comenzar.

1. Iniciación con Autopsy

¿Qué es *Autopsy*?

Autopsy es un software de análisis forense digital de código abierto para investigar dispositivos electrónicos y recuperar datos.

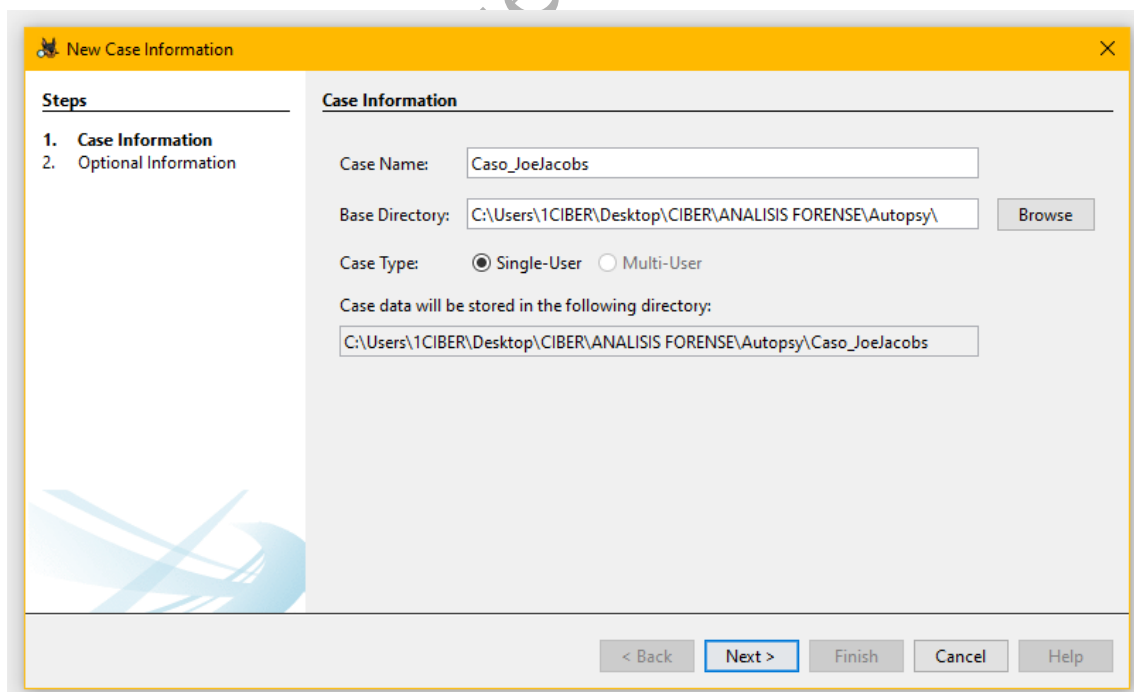
Su función principal es analizar discos duros, sistemas de archivos y dispositivos extraíbles en busca de evidencias, recuperar archivos eliminados, correos electrónicos, registros de actividad y metadatos. Tiene herramientas para análisis de imágenes, búsqueda de palabras clave, detección de actividad en Internet y recuperación de particiones dañadas.

Autopsy se utiliza comúnmente para investigaciones criminales, auditorías de seguridad y análisis post-incidentes.

Al abrir *Autopsy* por primera vez nos aparecerá la siguiente pantalla



Le daremos a nuevo caso



Introducimos el nombre del caso y pulsamos en siguiente

New Case Information

Steps

- Case Information
- Optional Information**

Optional Information

Case

Number: 1

Examiner

Name: José Enrique Gallego León

Phone: 123456789

Email: email@email.es

Notes: Notas sobre el caso

Organization

Organization analysis is being done for: Not Specified Manage Organizations

< Back Next > **Finish** Cancel Help

En la siguiente pantalla rellenamos la información necesaria, para este caso podemos rellenar solo el numero de caso y el nombre el resto de los campos son opcionales, pero es recomendable rellenarlos.

El programa creará los archivos y cargará las herramientas que necesite para realizar el trabajo y nos pedirá que indiquemos datos como el host, con que vamos a trabajar (imagen, disco local, archivos...), que indiquemos la ruta del archivo con el que vamos a trabajar y configurar los plugins con los que se van a trabajar.

Add Data Source

Steps

- Select Host
- Select Data Source Type
- Select Data Source
- Configure Report
- Add Data Source

Select Host

Hosts are used to organize data sources and other data.

☒ Enter a new host name (based on data source name)

☐ Specify new host name

☐ Use existing host

Select Data Source

Path:

☐ Ignore orphan files in FAT file systems

Time zone: (GMT-1000) Europe/Madrid

Sector size: (Auto Detect)

Host Values (optional)

MD5:

SHA-1:

SHA-256:

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

< Back Next > Cancel Help

Add Data Source

Steps

- Select Host
- Select Data Source Type
- Select Data Source
- Configure Report
- Add Data Source

Select Data Source Type

☒ Disk Image or VM File

☐ Local Disk

☐ Logical File

☐ Unallocated Space Image File

☐ Autopsy Logical Image Results

☐ VDI Text Export

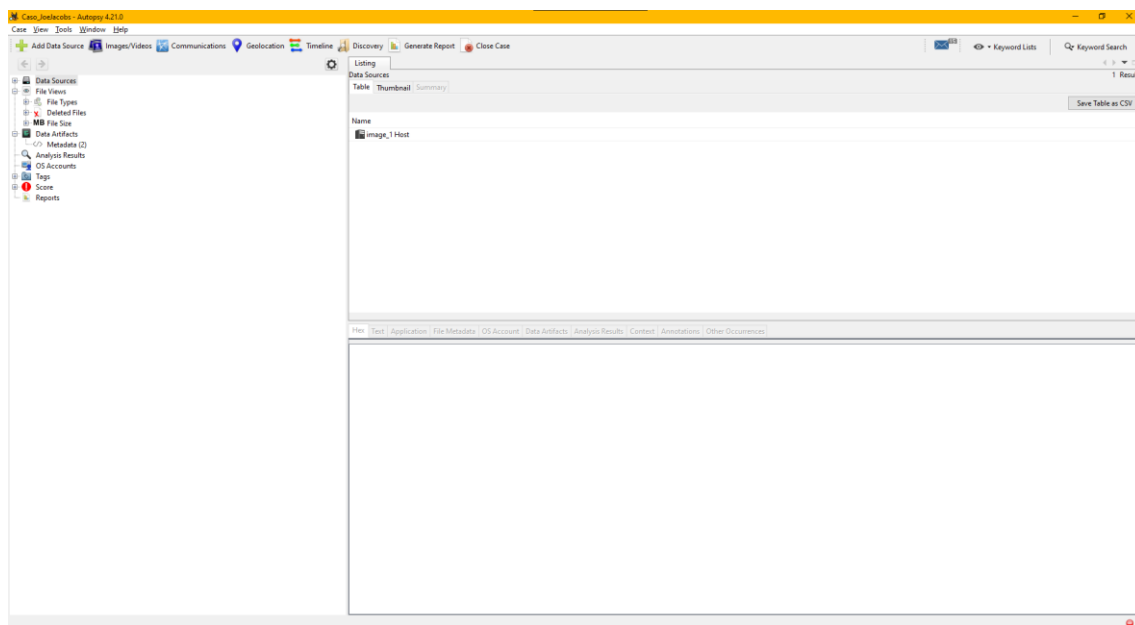
Configure Report

Plugins to be used:

- ☒ File System
- ☒ File System (NTFS)
- ☒ File System (FAT)
- ☒ File System (HFS)
- ☒ File System (Ext2/3)
- ☒ File System (XFS)
- ☒ File System (BFS)
- ☒ File System (JFS)
- ☒ File System (UFS)
- ☒ File System (ZFS)
- ☒ File System (VFS)
- ☒ File System (MFS)
- ☒ File System (CFS)
- ☒ File System (SFS)
- ☒ File System (IFS)
- ☒ File System (CIFS)
- ☒ File System (NFS)
- ☒ File System (SMB)
- ☒ File System (AFP)
- ☒ File System (FUSE)
- ☒ File System (VFS)
- ☒ File System (MFS)
- ☒ File System (CFS)
- ☒ File System (SFS)
- ☒ File System (IFS)
- ☒ File System (CIFS)
- ☒ File System (NFS)
- ☒ File System (SMB)
- ☒ File System (AFP)
- ☒ File System (FUSE)

< Back Next > Cancel Help

Para esta práctica podéis dejar los ajustes mencionados como aparecen en estas imágenes.



Una vez termine de configurar todos los archivos necesarios aparecerá esta pantalla, ya podríamos empezar a investigar.

Autopsy nos clasificará automáticamente todos los archivos e información por tipos, que aparecerán en la parte izquierda de la pantalla lo que facilita mucho el análisis y la búsqueda.

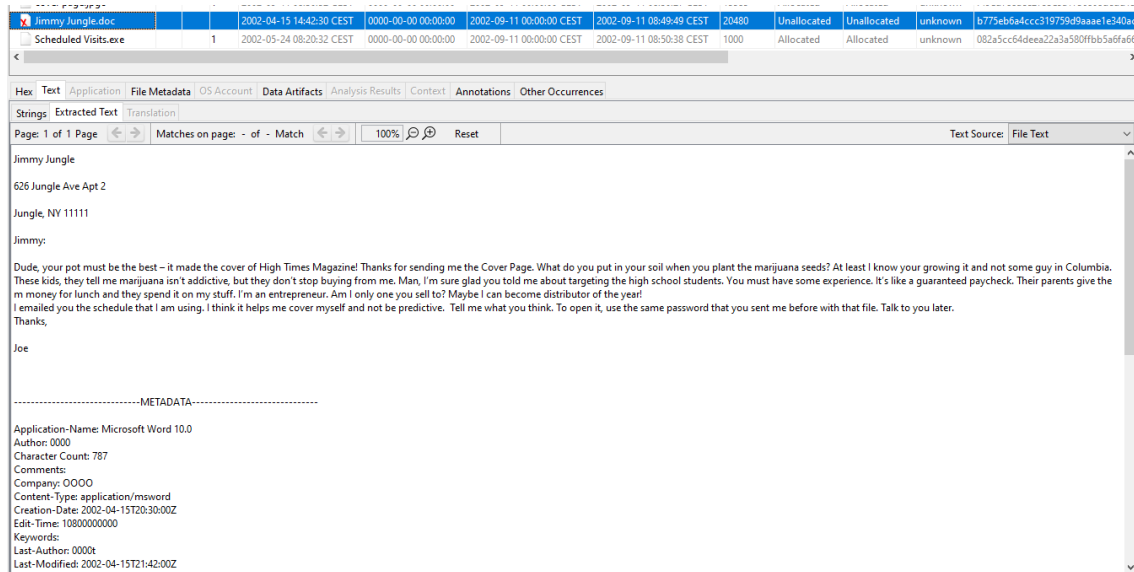
2. Búsqueda de datos e información comprometida

Comencemos por ver todos los archivos que tiene la imagen, ya que es una imagen pequeña encontraremos todos los archivos del sistema rápidamente si entramos a *image_1 Host > image*.

Listing						
/img_image						
Table	Thumbnail	Summary				
Name	S	C	O	Modified Time	Change Time	Access Time
📁 \$OrphanFiles				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
📄 \$FAT1			2	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
📄 \$FAT2			2	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
📄 \$MBR			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
📁 \$CarvedFiles				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
📁 \$Unalloc				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
📄 cover page.jpgc			1	2002-09-11 08:30:52 CEST	0000-00-00 00:00:00	2002-09-11 00:00:00 CEST
📄 Jimmy Jungle.doc				2002-04-15 14:42:30 CEST	0000-00-00 00:00:00	2002-09-11 00:00:00 CEST
📄 Scheduled Visits.exe			1	2002-05-24 08:20:32 CEST	0000-00-00 00:00:00	2002-09-11 00:00:00 CEST

Con un simple vistazo ya observamos que uno de los archivos (Jimmy Jungle.doc) estaba borrado y *Autopsy* lo ha recuperado.

Analicemos ese archivo recuperado, pulsamos sobre el y nos mostrará la información del documento:



Es un documento Word, que contenía un mensaje para *Jimmy Jungle* que vive en 626 Jungle Ave Apt 2 / Jungle, NY 11111

El mensaje dice:

“Jimmy:

Amigo, tu hierba debe ser la mejor; ¡salió en la portada de la revista High Times! Gracias por enviarme la portada. ¿Qué le pones a la tierra cuando plantas las semillas de marihuana? Al menos sé que la estás cultivando tú y no algún tipo en Colombia. Estos chicos me dicen que la marihuana no es adictiva, pero no paran de comprarme. Hombre, estoy muy agradecido de que me dijeras lo de enfocarme en los estudiantes de secundaria. Debes tener experiencia en esto. Es como un sueldo garantizado. Sus padres les dan dinero para el almuerzo y lo gastan en mi producto. Soy un emprendedor. ¿Soy el único al que le vendes? ¡Tal vez pueda convertirme en el distribuidor del año!

Te envié por correo el horario que estoy usando. Creo que me ayuda a cubrirme y a no ser predecible. Dime qué opinas. Para abrirlo, usa la misma contraseña que me enviaste antes con ese archivo. Hablamos luego.

*Gracias,
Joe”*

Por lo que vemos el mensaje lo envía Joe Jacobs a Jimmy Jungle diciéndole que su marihuana es la mejor y la está vendiendo muy bien, por lo tanto, ya podríamos sacar la información de la primera pregunta que tenemos que responder:

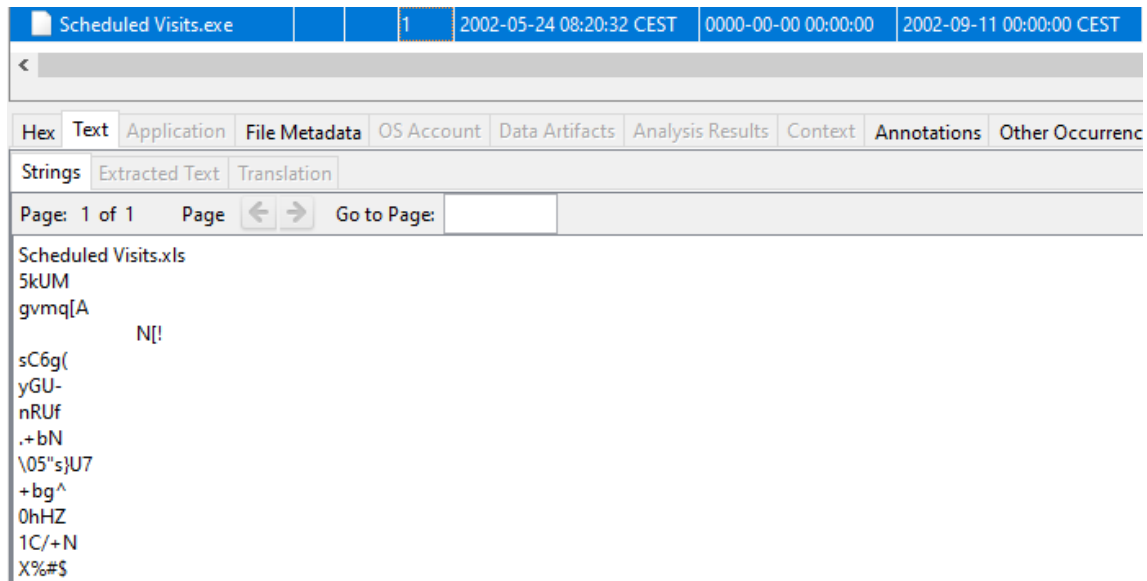
¿Quién es el proveedor de marihuana de Joe Jacobs y cuál es su dirección?

El proveedor es Jimmy Jungle y vive en 626 Jungle Ave Apt 2 / Jungle, NY 11111

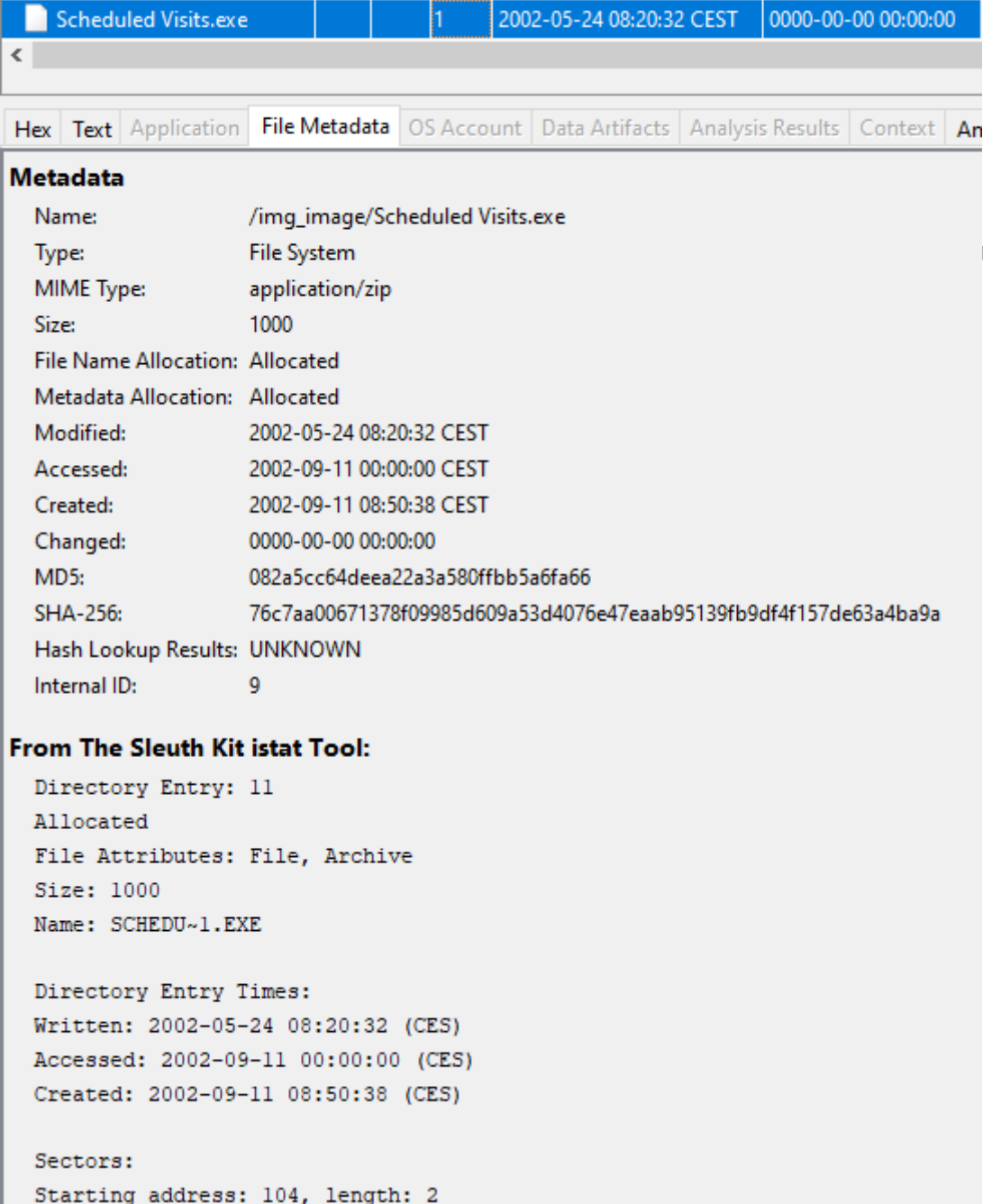
Schedule visits.xls

En el mensaje que envía Joe se comenta que ha enviado el horario en el que vende, y que la contraseña para abrirlo es la misma que el Jimmy le envió anteriormente, busquemos ese archivo.

Si vemos, en los archivos que hemos encontrado hay uno que se llama Schedule Visits.exe (Programa/Horario de visitas.exe), por lo tanto ese podría ser el archivo que nos de la información que buscamos.



Dentro del archivo, vemos que hay un Schedule visits.xls, formato Excel, y cuando hemos pulsado sobre el se indica que el archivo es .exe. Sospechoso, veamos los metadatos del archivo para buscar mas datos sobre este archivo:

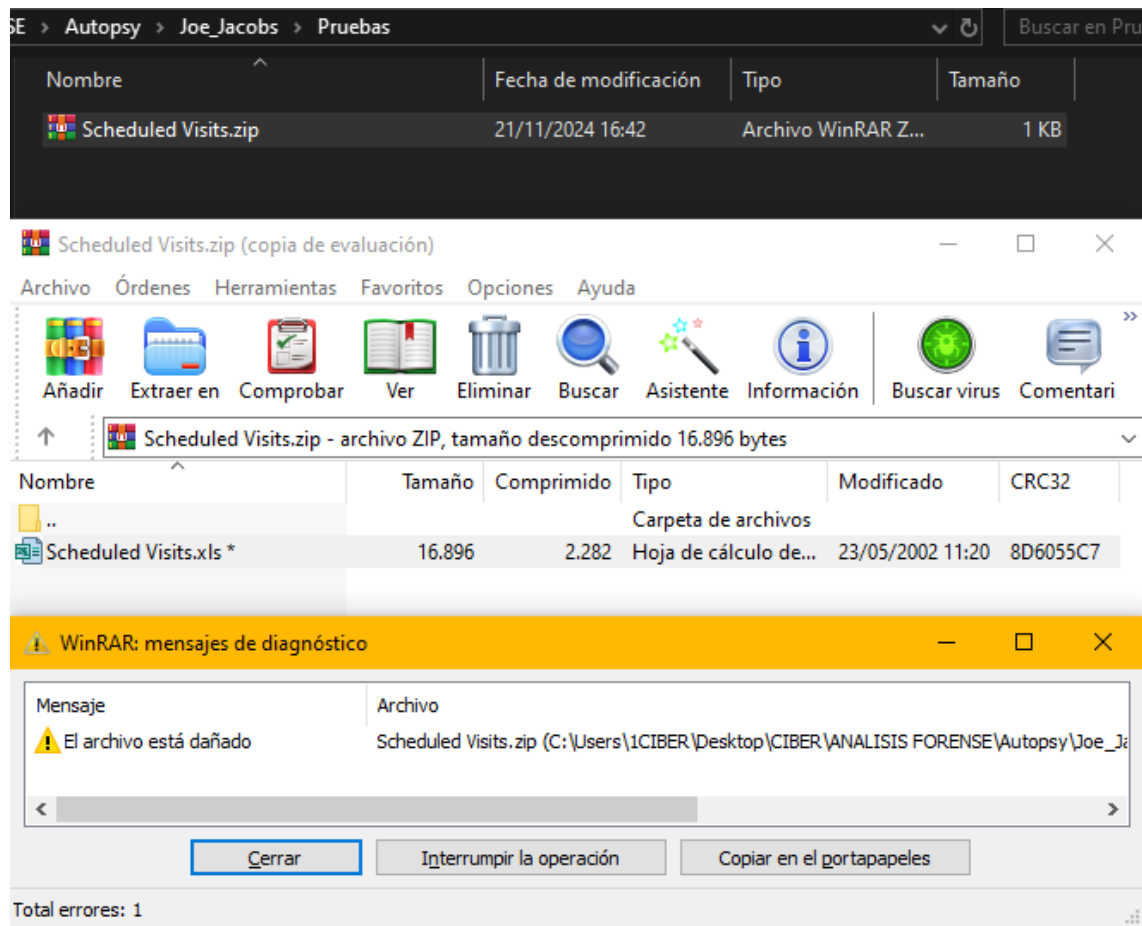


The screenshot shows the Autopsy interface with the 'File Metadata' tab selected. The file 'Scheduled Visits.exe' is highlighted in the top bar. The metadata table lists various file properties, including name, type, MIME type, size, and timestamps. Below the table, the 'From The Sleuth Kit istat Tool:' section provides additional file statistics and directory entry information.

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	An
Metadata								
Name:	/img_image/Scheduled Visits.exe							
Type:	File System							
MIME Type:	application/zip							
Size:	1000							
File Name Allocation:	Allocated							
Metadata Allocation:	Allocated							
Modified:	2002-05-24 08:20:32 CEST							
Accessed:	2002-09-11 00:00:00 CEST							
Created:	2002-09-11 08:50:38 CEST							
Changed:	0000-00-00 00:00:00							
MD5:	082a5cc64deea22a3a580ffb5a6fa66							
SHA-256:	76c7aa00671378f09985d609a53d4076e47eaab95139fb9df4f157de63a4ba9a							
Hash Lookup Results:	UNKNOWN							
Internal ID:	9							
From The Sleuth Kit istat Tool:								
Directory Entry: 11								
Allocated								
File Attributes: File, Archive								
Size: 1000								
Name: SCHEDU~1.EXE								
Directory Entry Times:								
Written: 2002-05-24 08:20:32 (CES)								
Accessed: 2002-09-11 00:00:00 (CES)								
Created: 2002-09-11 08:50:38 (CES)								
Sectors:								
Starting address: 104, length: 2								

Los metadatos indican que es un archivo .zip, por lo tanto realmente el archivo es un .zip que contiene un archivo .xls donde probablemente se encuentre el horario en el que Joe Jacobs vende los estupefacientes, saquemos el archivo a nuestro equipo y veamos el .xls.

Esto lo haremos dando click derecho sobre el archivo y seleccionando “*Extract file(s)*”.

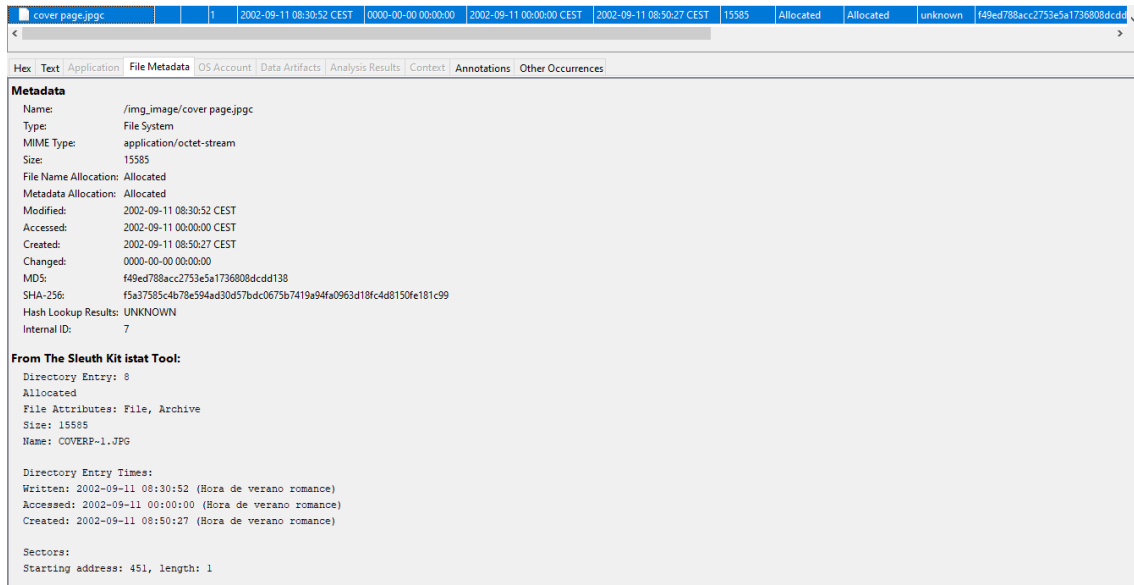


Ya que sabemos que es un archivo .zip podemos cambiarle la extensión para extraerlo, pero al intentarlo salta un error ya que el archivo está corrupto.

Intentemos sacar más información y volveremos a este problema más tarde.

Cover page.jpggc

Si retrocedemos hasta todos los archivos que tiene la imagen aún nos quedan archivos que analizar, y una de las preguntas que nos proponen, se encuentra relacionada con el archivo *cover page.jpggc* veámoslo.



The screenshot shows the 'File Metadata' tab for the file 'cover page.jpggc'. The metadata includes:

- Name: /img_image/cover page.jpggc
- Type: File System
- MIME Type: application/octet-stream
- Size: 15585
- File Name Allocation: Allocated
- Metadata Allocation: Allocated
- Modified: 2002-09-11 08:30:52 CEST
- Accessed: 2002-09-11 00:00:00 CEST
- Created: 2002-09-11 08:50:27 CEST
- Changed: 0000-00-00 00:00:00
- MD5: f49ed788acc2753e5a1736808dcd138
- SHA-256: f5a37585c4b78e594ad30d57bdc0675b7419a94fa0963d18fc4d8150fe181c99
- Hash Lookup Results: UNKNOWN
- Internal ID: 7

From The Sleuth Kit istat Tool:

- Directory Entry: 8
- Allocated
- File Attributes: File, Archive
- Size: 15585
- Name: COVERP-1.JPG

Directory Entry Times:

- Written: 2002-09-11 08:30:52 (Hora de verano romance)
- Accessed: 2002-09-11 00:00:00 (Hora de verano romance)
- Created: 2002-09-11 08:50:27 (Hora de verano romance)

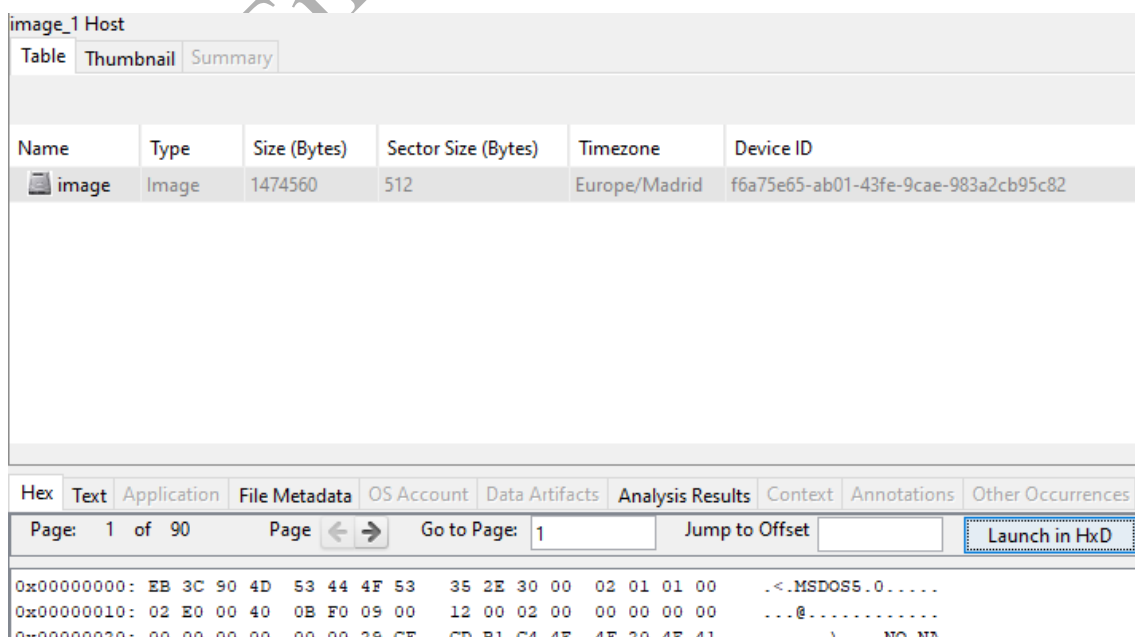
Sectors:

- Starting address: 451, length: 1

Al analizar los metadatos vemos que es un archivo extraño, ya que su extensión indica que es una foto, pero en los metadatos nos da la información que es un octet stream.

Algo más que no cuadra es el tamaño del archivo, ya que es demasiado grande y nos informa de que empieza en el sector 451 y solo ocupa 1 sector. Vayamos a ese sector en el disco y analicemos el código.

Abriremos la imagen y nos posicionaremos en el apartado del código Hexadecimal y lo abriremos con HxD:



The screenshot shows the 'image_1 Host' window with the 'Table' tab selected. It displays a table of files:

Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID
image	Image	1474560	512	Europe/Madrid	f6a75e65-ab01-43fe-9cae-983a2cb95c82

Below the table, the 'Hex' tab is selected, showing the hexadecimal data of the file. The first few lines of the hex view are:

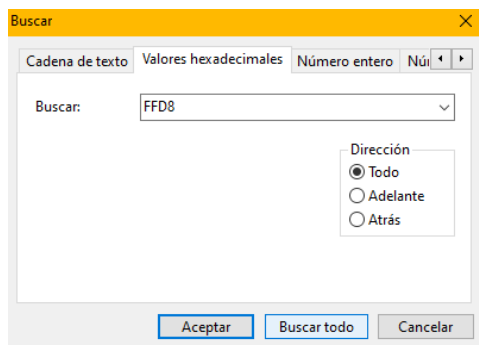
```
0x00000000: EB 3C 90 4D 53 44 4F 53 35 2E 30 00 02 01 01 00 .<.MSDOS5.0....
0x00000010: 02 E0 00 40 0B F0 09 00 12 00 02 00 00 00 00 00 ...@.....
0x00000020: 00 00 00 00 00 00 28 0F 0B B1 04 4F 4F 30 4F 41 \  N N
```

Vamos al sector 451:

```
00000440 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000450 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000460 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

Y como vemos no hay nada en ese sector, es raro. Vamos a utilizar los números mágicos, esto se refiere al conjunto de bytes que identifican sin equivocación el tipo de archivo que se está analizando.

El numero mágico de las fotos jpg es: FFD8, vamos a buscar en el disco.



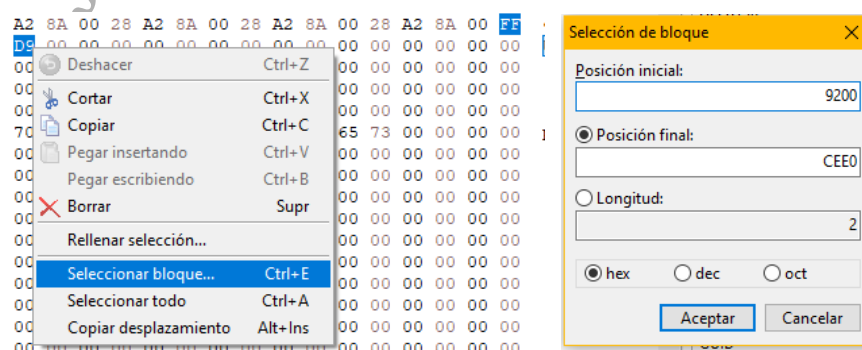
```
000091F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00009200 FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 60 JFIF.....
00009210 00 60 00 00 FF DB 00 43 00 08 06 06 07 06 05 08 ...ÿÛ.C.....
```

En el sector 9200 se encuentra el inicio del archivo, busquemos la cola del archivo (FFD9):

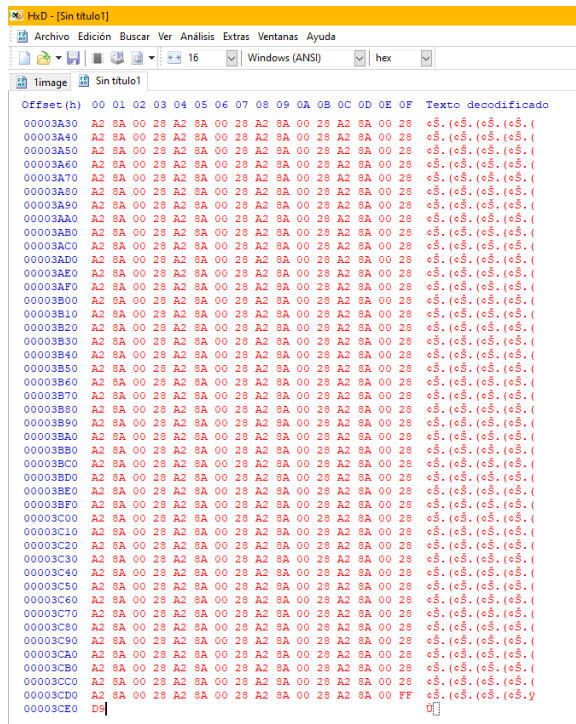
```
0000CED0 A2 8A 00 28 A2 8A 00 28 A2 8A 00 28 A2 8A 00 FF cŠ. (cŠ. (cŠ. (cŠ.
0000CEE0 D9 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0000CF00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0000CF10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0000CF20 70 77 3D 67 6F 6F 64 74 69 6D 65 73 00 00 00 pw=goodtimes....
```

En el sector CED0 / CEE0 se encuentra la cola del archivo y justo unos sectores más abajo nos encontramos el texto *pw=goodtimes* esta podría ser la contraseña del archivo que ya localizamos, por lo tanto la apuntamos.

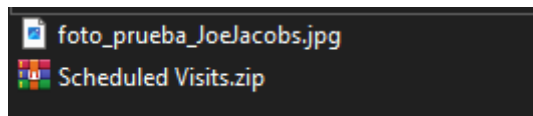
Ahora vamos a unir el inicio y la cola del archivo para poder sacarlo:



Lo copiamos y abrimos un nuevo archivo arriba a la izquierda, y lo copiamos:



Y lo guardamos como .jpg:



Perfecto, hemos conseguido una gran prueba y respondido a una de las preguntas que se plantean:

¿Qué dato clave está disponible dentro del archivo coverpage.jpg?

Dentro de los códigos de la imagen hemos encontrado la contraseña del Excel con los horarios.

Lo que acabamos de realizar es File Carving: es un proceso de reensamblaje o reconstrucción de archivos a partir de los metadatos. Se suele utilizar para el análisis forense o para recuperar archivos dañados o borrados.

Pasos finales

Hagamos el mismo proceso con el archivo dañado .zip

Número mágico .zip: 50 4B 03 04

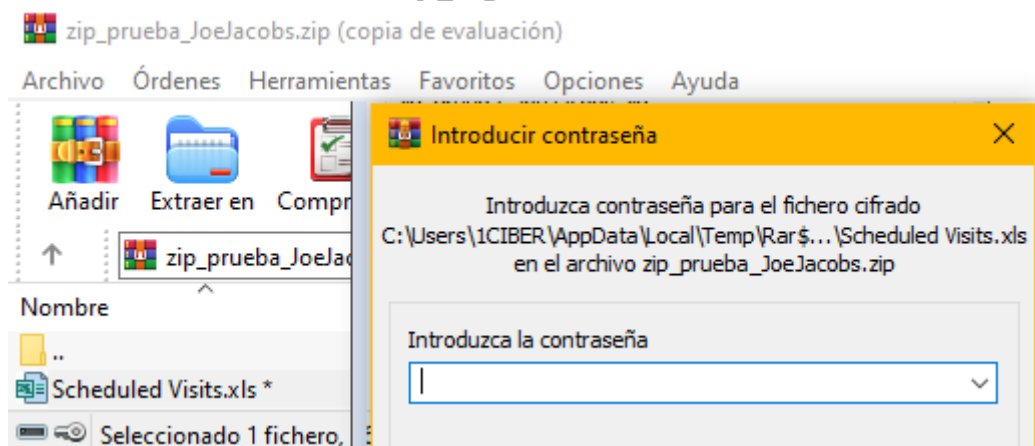
```
0000CFF0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0000D000 50 4B 03 04 14 00 01 00 08 00 98 5A B7 2C C7 55 PK.....~Z.,ÇU
0000D010 60 8D EA 08 00 00 00 42 00 00 14 00 00 00 53 63 `..è....B.....Sc
```

Cola del archivo .zip: 50 4B 05 06

```
0000D940 00 00 20 00 B6 81 00 00 00 00 53 63 68 65 64 75 .. .f.....Schedu
0000D950 6C 65 64 20 56 69 73 69 74 73 2E 78 6C 73 50 4B led Visits.xlsPK
0000D960 05 06 00 00 00 00 01 00 01 00 42 00 00 00 1C 09 ..B.....
```

Y realizamos lo mismo que en el archivo anterior, unimos el archivo lo copiamos, y lo sacamos al ordenador:

foto_prueba_JoeJacobs.jpg	25/11/2024 16:52	Archivo JPG	16 KB
Scheduled Visits.zip	21/11/2024 16:42	Archivo WinRAR Z...	1 KB
zip_prueba_JoeJacobs.zip	25/11/2024 17:10	Archivo WinRAR Z...	3 KB



Nos pide la contraseña del archivo que como hemos descubierto es *goodtimes*

<u>Month</u>	<u>DAY</u>	<u>HIGH SCHOOLS</u>
2002		
April	Monday (1)	Smith Hill High School (A)
	Tuesday (2)	Key High School (B)
	Wednesday (3)	Leetch High School (C)
	Thursday (4)	Birard High School (D)
	Friday (5)	Richter High School (E)
	Monday (1)	Hull High School (F)
	Tuesday (2)	Smith Hill High School (A)
	Wednesday (3)	Key High School (B)
	Thursday (4)	Leetch High School (C)
	Friday (5)	Birard High School (D)
	Monday (1)	Richter High School (E)
	Tuesday (2)	Hull High School (F)
	Wednesday (3)	Smith Hill High School (A)
	Thursday (4)	Key High School (B)
	Friday (5)	Leetch High School (C)
	Monday (1)	Birard High School (D)
	Tuesday (2)	Richter High School (E)
	Wednesday (3)	Hull High School (F)
	Thursday (4)	Smith Hill High School (A)
	Friday (5)	Key High School (B)
	Monday (1)	Leetch High School (C)
	Tuesday (2)	Birard High School (D)
May		
	Wednesday (3)	Richter High School (E)
	Thursday (4)	Hull High School (F)
	Friday (5)	Smith Hill High School (A)
	Monday (1)	Key High School (B)

Lo hemos conseguido, sacamos los horarios de venta de Joe Jacobs.

Además, podemos responder a otra pregunta de las que nos proponen:

¿Qué otras escuelas secundarias (si hay) adicionales a Smith Hill, frecuenta Joe Jacobs?

Key High School, Leetch High School, Birard High School, Richter High School...

3. Respuestas a las preguntas propuestas

¿Quién es el proveedor de marihuana de Joe Jacobs y cuál es su dirección?

El proveedor es Jimmy Jungle y vive en 626 Jungle Ave Apt 2 / Jungle, NY 11111

¿Qué dato clave está disponible dentro del archivo coverpage.jpg?

Dentro de los códigos de la imagen hemos encontrado la contraseña del Excel con los horarios.

¿Qué otras escuelas secundarias (si hay) adicionales a Smith Hill, frecuenta Joe Jacobs?

Key High School, Leetch High School, Birard High School, Richter High School...

Para cada archivo recuperado, ¿qué proceso fue adelantado por el sospechoso para ocultarlo en el disco?

El sospechoso borro el archivo donde redactaba el mensaje a Jimmy Jungle, compresión con contraseña del archivo donde se redactaban los horarios de venta y el cambio a la extensión .exe de ese mismo archivo

¿Qué proceso realizó usted como investigador para examinar con éxito el contenido completo de cada archivo?

Se ha utilizado el método File Carving para reconstruir los archivos y poder verlos y analizarlos

¿Puede decir qué programa fue usado para crear el archivo coverpage.jpg? ¿Cómo lo puede probar?

Podríamos pensar y llegar a la conclusión de que el archivo fue modificado con algún programa de Microsoft que maneje la conversión de formatos gráficos o escaneo de imágenes.

Posibles fallos

Uno de los posibles fallos es a la hora de reconstruir el archivo Schedule Visits.zip es que aún eligiendo los sectores correctos siga indicando que el archivo se encuentra corrupto.

Para esto simplemente deberemos seleccionar todo el sector como se muestra en la imagen, así podremos solucionar el problema y abrir el archivo

