

TALLER AUTOPSY

Cristhian Camilo Mosquera Caicedo

Carlos Daniel Mosquera Caicedo

Ficha: 51112

Gerencia en proyectos de Ingeniería

Corporación Unificada Nacional de Educación Superior

Bogotá, Colombia

2022

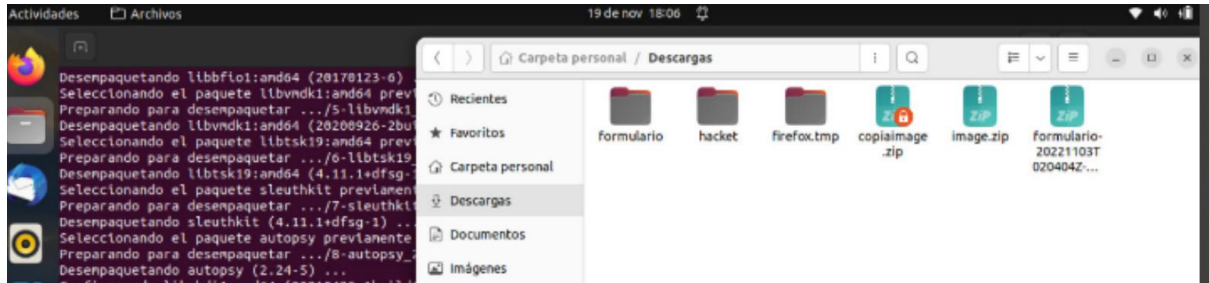
TABLA DE CONTENIDO

DESARROLLO ANALISIS FORENCE	2
PREGUNTAS DEL CASO.....	15

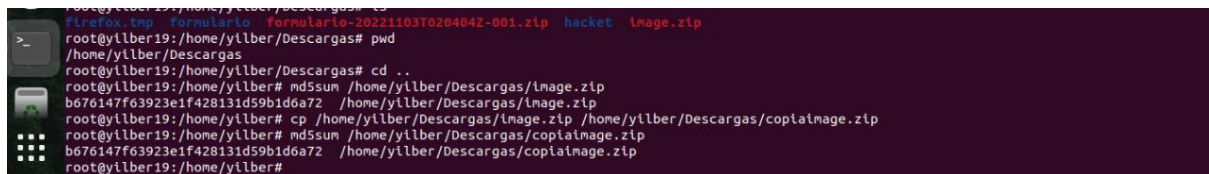
DESARROLLO ANALISIS FORENCE

El taller fue desarrollado en el sistema operativo Linux (Ubuntu).

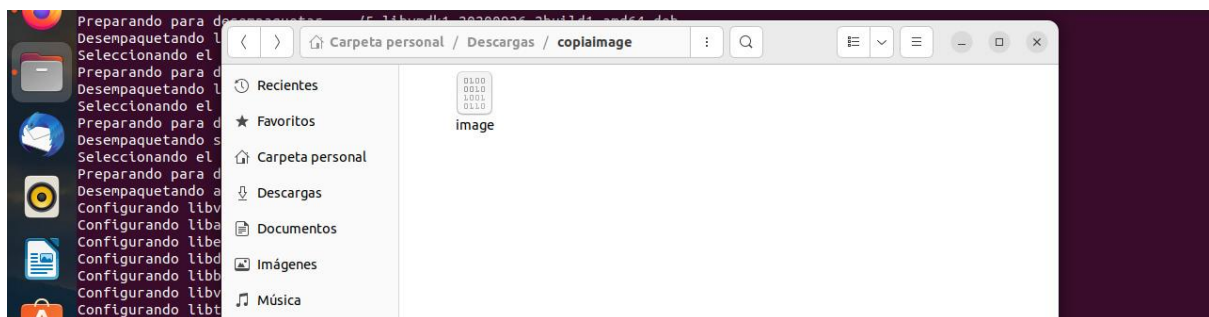
Paso 1: Instalación de Autopsy, y se descargó la imagen.



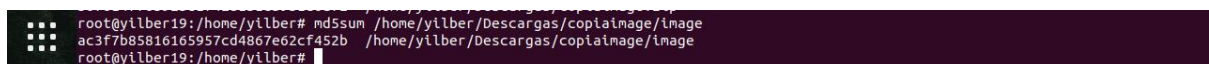
Paso 2: Se calcula el hash md5 de la imagen, se hace una copia de la imagen y también se calcula el has md5 para verificar que estamos trabajando con una copia exacta.



Paso 3: Extraemos el .ZIP y obtenemos la imagen (disk).



Paso 5: Calculamos el hash md5 de la imagen y ejecutamos Autopsy para comenzar con el proceso.



```
ac3f7b85816165957cd4867e62cf452b /home/yilber/Descargas/copiaimage/image
root@yilber19:/home/yilber# autopsy

=====
Autopsy Forensic Browser
http://www.sleuthkit.org/autopsy/
ver 2.24
=====
Evidence Locker: /var/lib/autopsy
Start Time: Sat Nov 19 18:12:05 2022
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:

http://localhost:9999/autopsy

Keep this process running and use <ctrl-c> to exit
```

Paso 6: Abrimos Autopsy.



Paso 7: Creamos el caso.

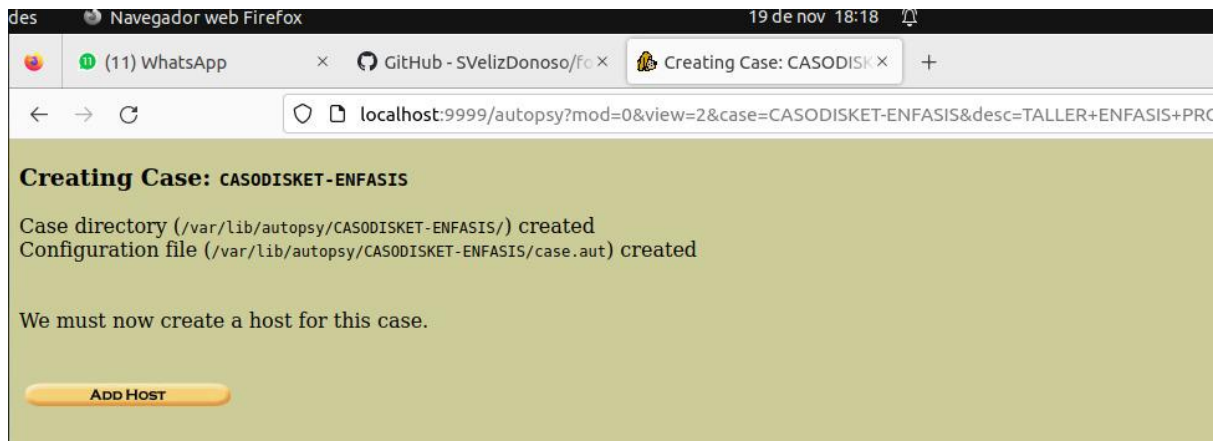
CREATE A NEW CASE

1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

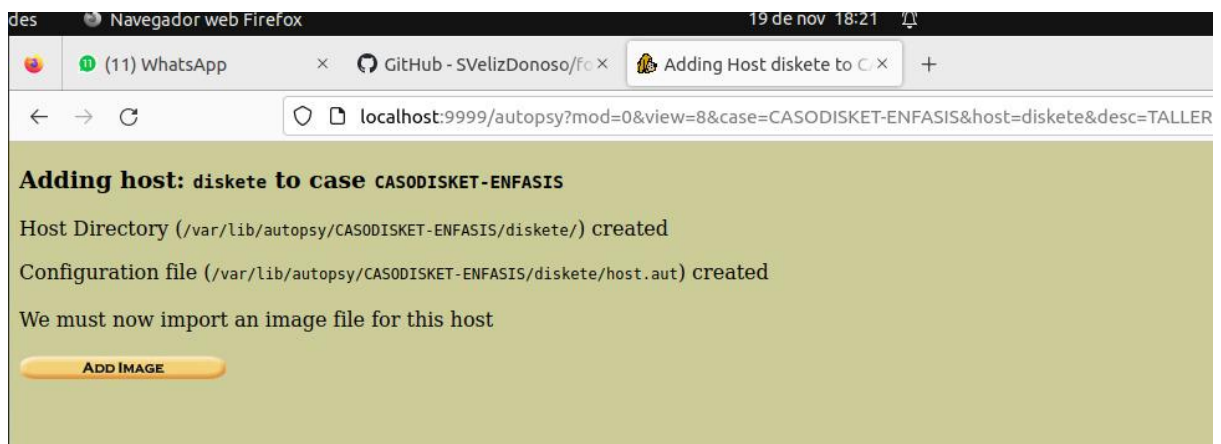
2. **Description:** An optional, one line description of this case.

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

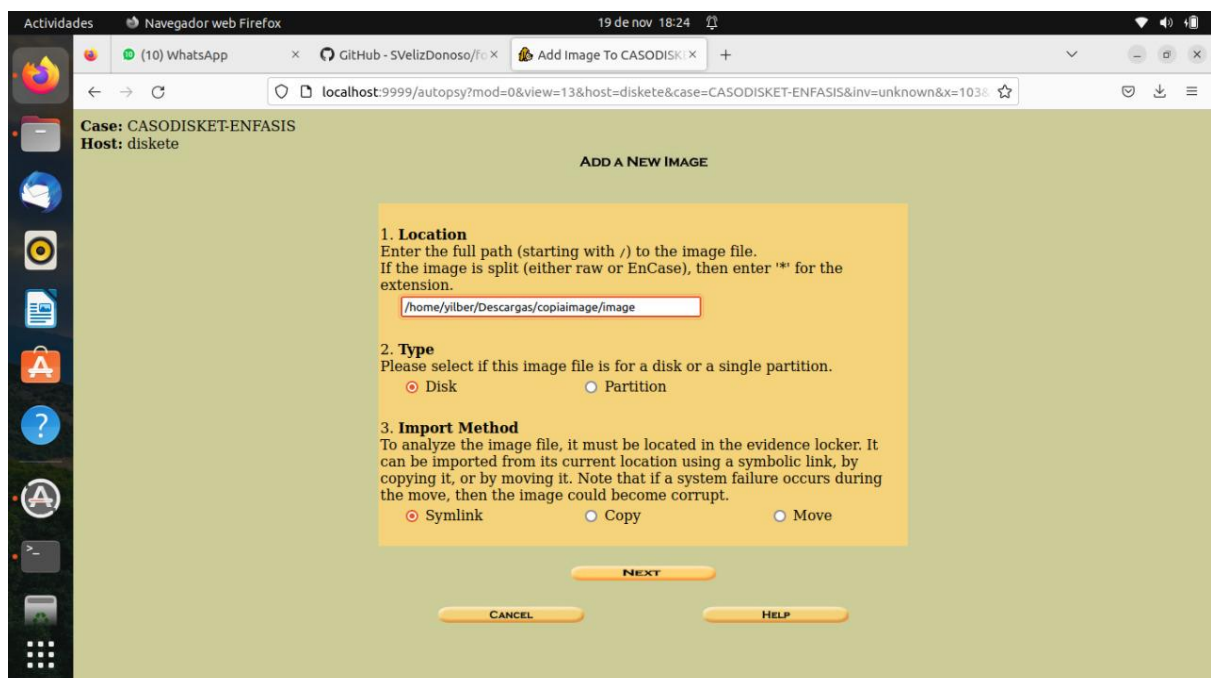
a. <input type="text" value="AN CAMILO MOSQUERA CAICEDO"/>	b. <input type="text" value="OS DANIEL MOSQUERA CAICEDO"/>
c. <input type="text"/>	d. <input type="text"/>
e. <input type="text"/>	f. <input type="text"/>
g. <input type="text"/>	h. <input type="text"/>
i. <input type="text"/>	j. <input type="text"/>

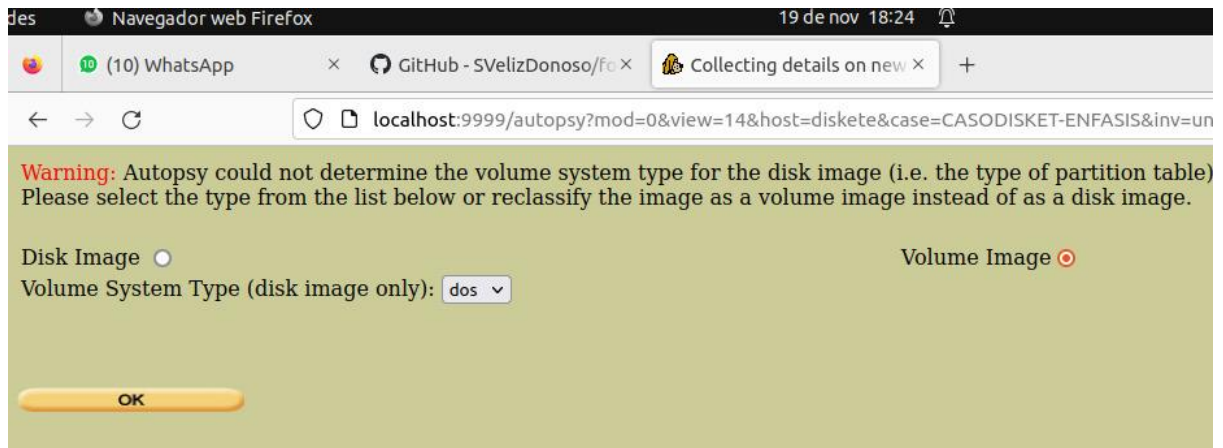


Paso 8: Creamos el host y confirmamos.

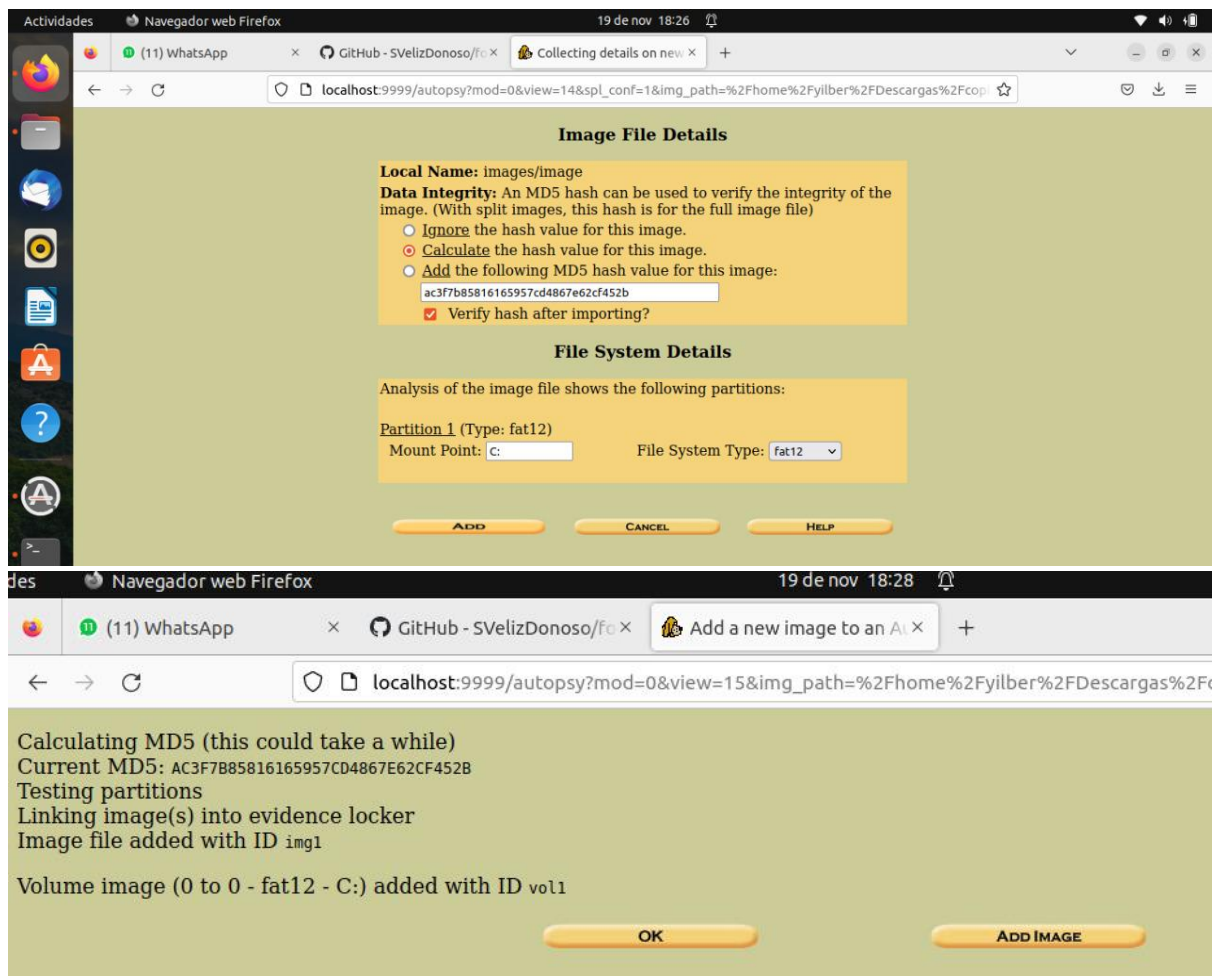


Paso 9: Agregamos la evidencia a revisar y configuramos los volúmenes.

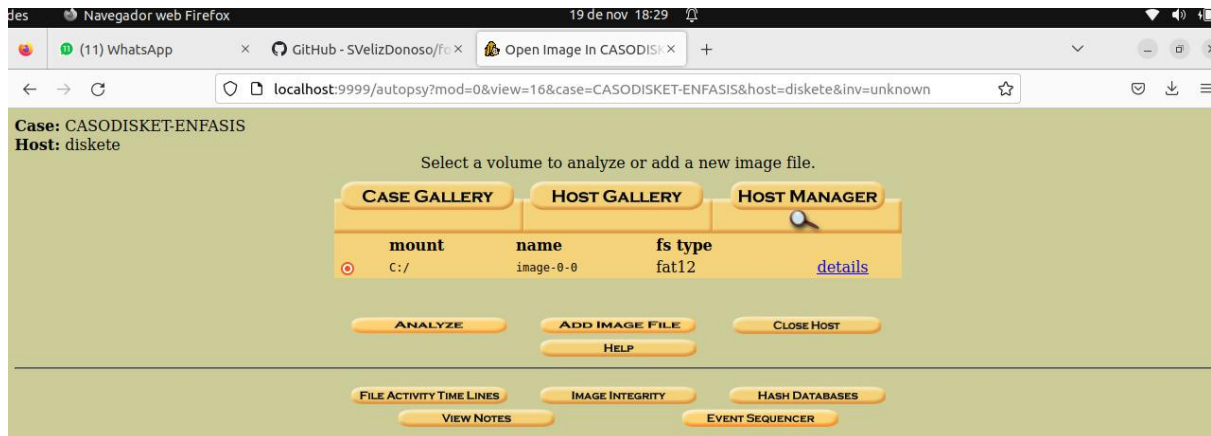




Paso 10: Configuramos el detalle de la imagen e ingresamos el hash md5 de la imagen obtenido anteriormente.

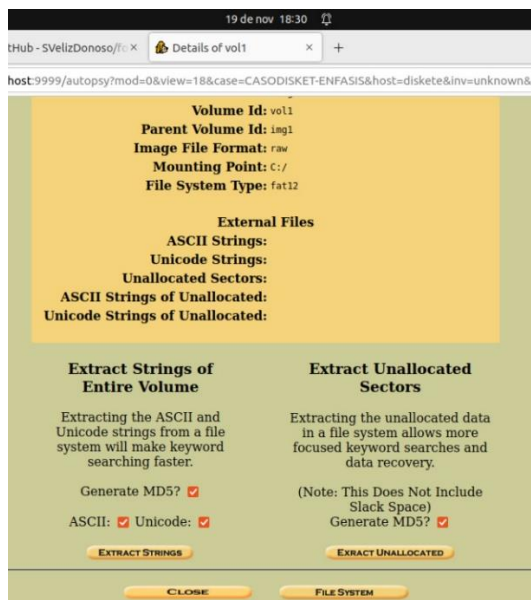


Paso 11: Comenzamos el análisis.

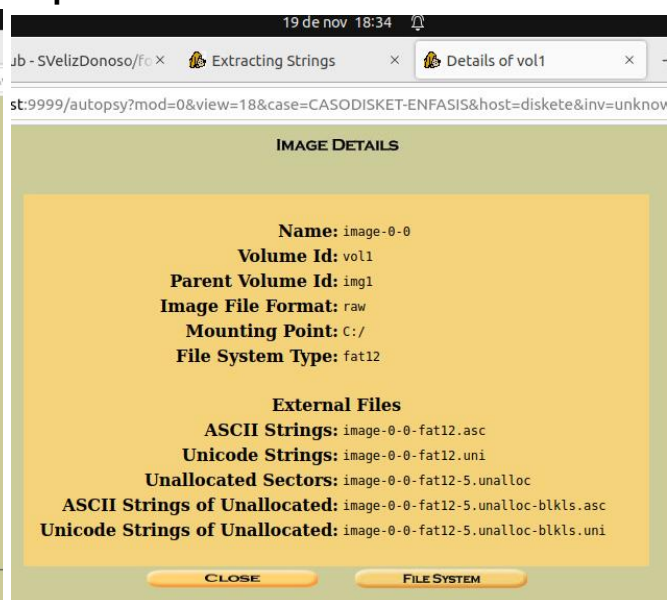


Paso 12: Creamos los índices de búsqueda en el disco.

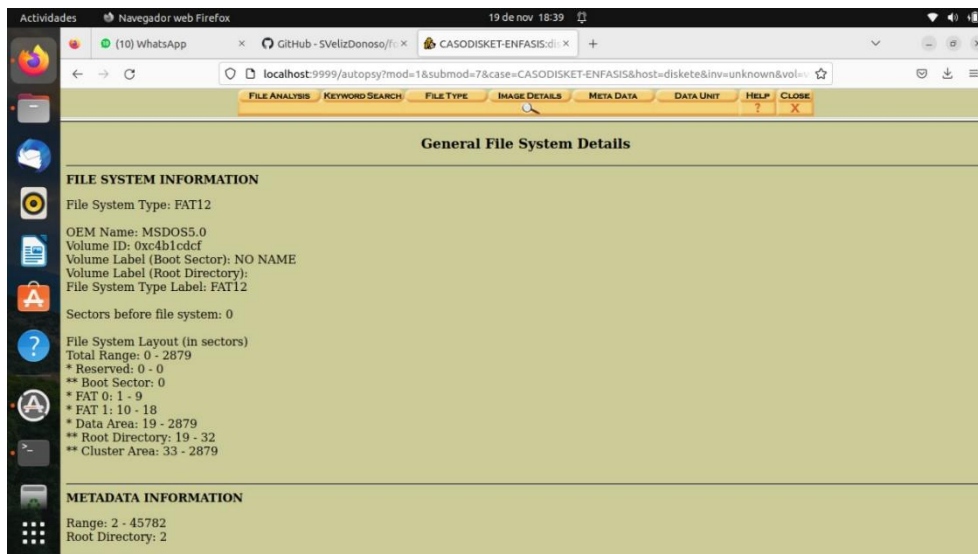
Antes:



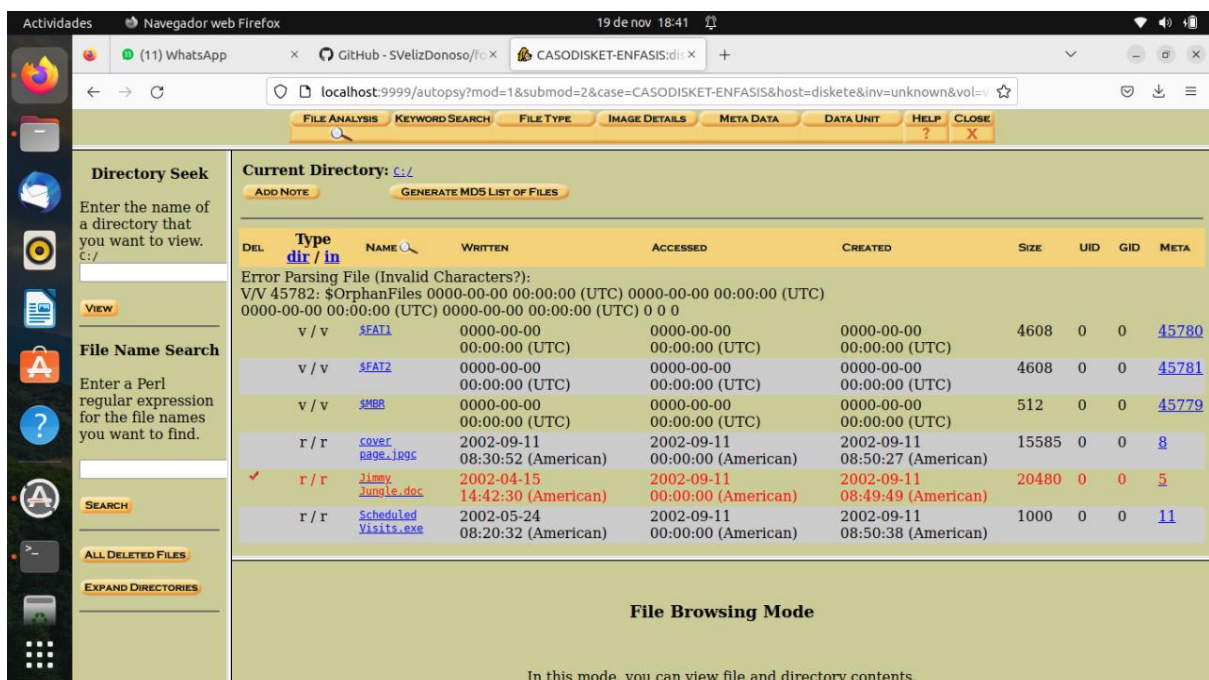
Despues:



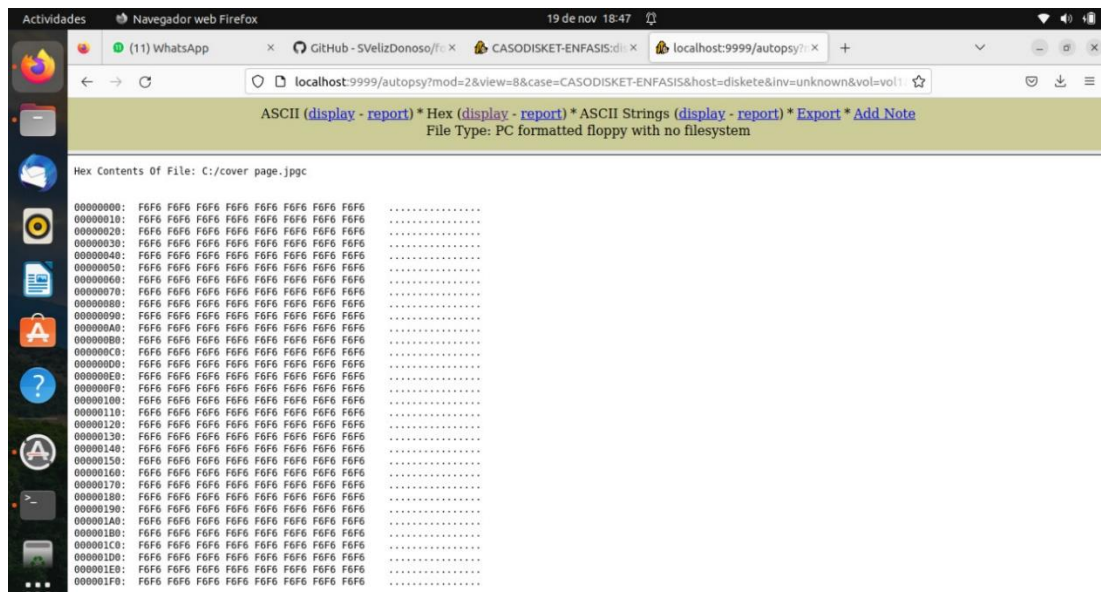
Paso 13: Analizamos la imagen y vemos el detalle.



Paso 14: Después de mirar el tamaño del clúster, memoria y metadatos pasamos a analizar cada uno de los archivos.

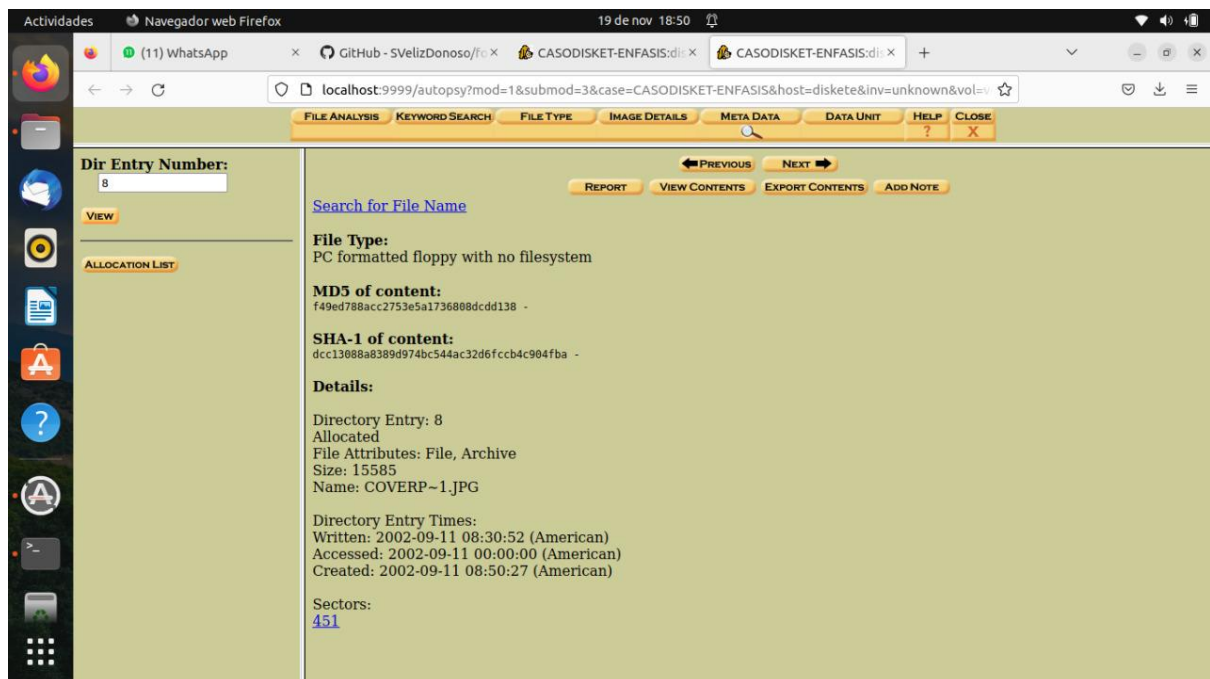


Paso 15: Analizamos el primer archivo (cover page.jpgc).



Evidenciamos que el archivo no es reconocido con extensión (.jpeg).

Visualizamos metadatos.



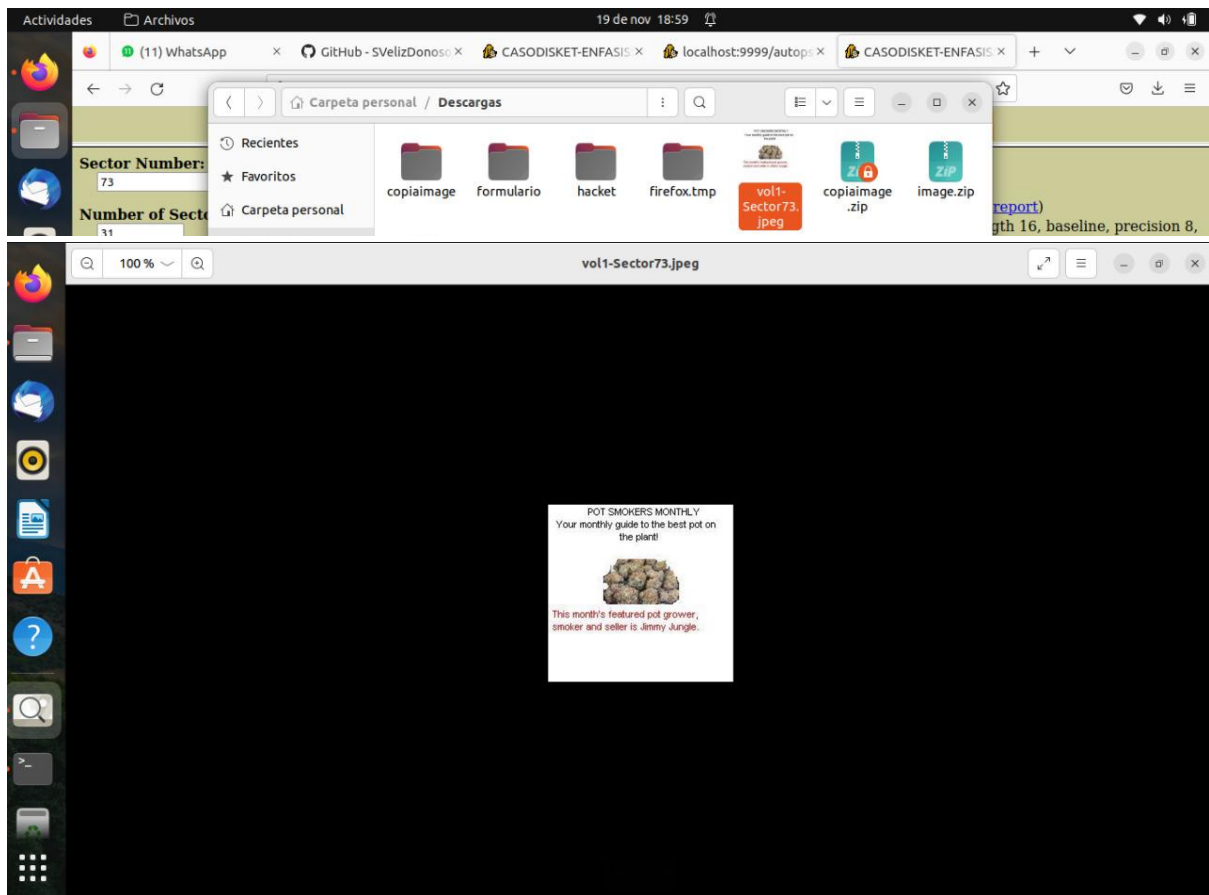
Procedemos al cálculo del archivo, obtenemos los sectores necesarios para reconstruir la imagen.

The screenshot shows the CASODISKET-ENFASIS application interface. On the left sidebar, the 'Sector Number' is set to 74, 'Number of Sectors' is 1, 'Sector Size' is 512, 'Address Type' is 'Regular (dd)', and 'Lazarus Addr.' is unchecked. The main panel displays 'Sector: 74', 'Status: Allocated', and 'File Type: data'. Below this, the 'Hex Contents of Sector 74 in image-0-0' are shown in a hex dump format, with columns for offset, hex data, and ASCII representation.

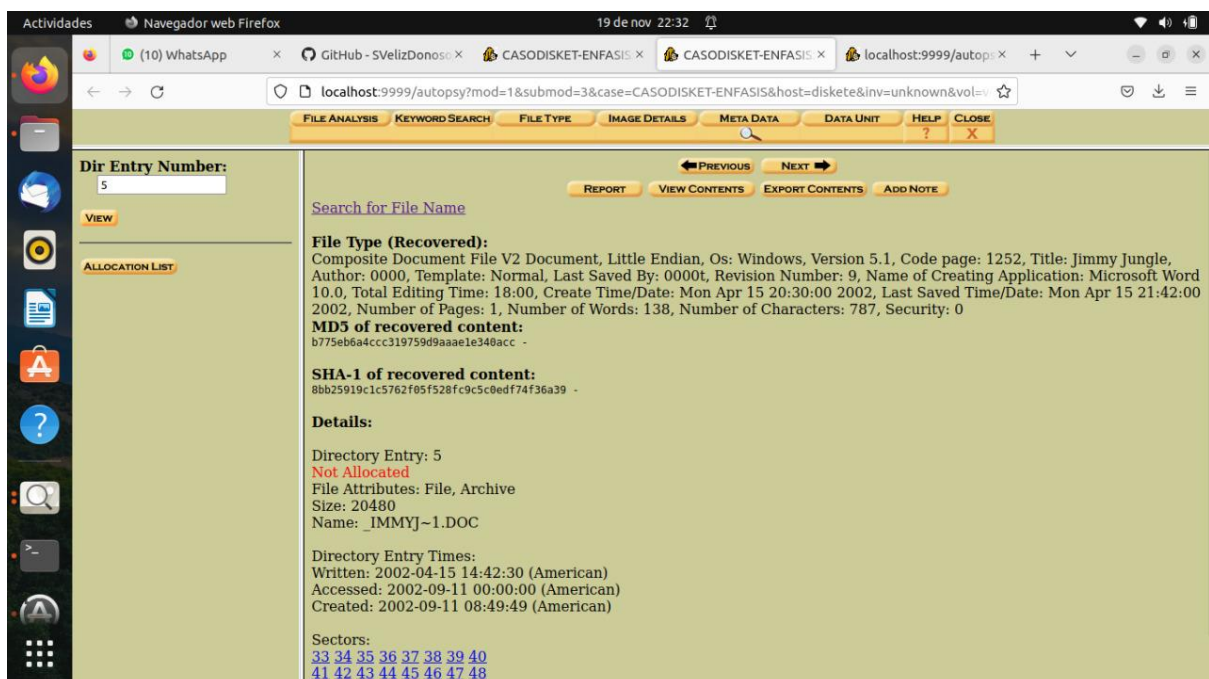
Como se encontraron 31 sectores, significa que debemos empezar desde el sector 73, sectores a seleccionar $73 + 31 = (73 - 103)$.

The screenshot shows the CASODISKET-ENFASIS application interface with 'Sector Number' set to 73 and 'Number of Sectors' set to 31. The main panel displays 'Sectors: 73-103', 'Status: Allocated', and 'File Type: JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 208x199, components 3'. Below this, the 'Hex Contents of Sectors 73-103 in image-0-0' are shown in a hex dump format, with columns for offset, hex data, and ASCII representation.

Procedemos a descargar la imagen y a cambiar su formato.



Paso 16: Analizamos el segundo archivo (Jimmy Jungle.doc). Verificamos sus metadatos.



Cálculo del archivo: número de sectores 72 – 32 = 40

The screenshot shows the Autopsy web interface in a Firefox browser. The left sidebar contains input fields for 'Sector Number' (33), 'Number of Sectors' (40), 'Sector Size' (512), 'Address Type' (Regular (dd)), and 'Lazarus Addr'. The main area displays the results for sectors 33-72, including a hex dump of the contents. The file type is identified as 'Composite Document File V2 Document, Can't read SAT'.

Sector Number: 33
Number of Sectors: 40
Sector Size: 512
Address Type: Regular (dd)
Lazarus Addr: ☐
VIEW
ALLOCATION LIST
LOAD UNALLOCATED

PREVIOUS NEXT
EXPORT CONTENTS ADD NOTE
ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report)
File Type: Composite Document File V2 Document, Can't read SAT
Sectors: 33-72
Status: Not Allocated
Hex Contents of Sectors 33-72 in image-0-0

Offset	Hex	ASCII
0	d0cfile0 albl1ael 00000000 00000000
16	00000000 00000000 3e000300 feff0900>.....
32	00000000 00000000 00000000 01000000
48	23000000 00000000 00100000 25000000	#.....
64	01000000 feffffff 00000000 22000000
80	ffffff...
96	ffffff...
112	ffffff...
128	ffffff...
144	ffffff...
160	ffffff...
176	ffffff...
192	ffffff...
208	ffffff...
224	ffffff...
240	ffffff...
256	ffffff...
272	ffffff...
288	ffffff...

Procedemos a descargar el archivo.

The screenshot shows the file download process. A file manager window displays the 'Descargas' folder with files including 'vol1-Sector33.doc'. Below, the LibreOffice Writer application opens the document 'vol1-Sector33.doc', displaying a letter from Jimmy Jungle to Joe.

Archivos
19 de nov 22:35
localhost:9999/autopsy/...
Carpeta personal / Descargas
Recientes
Favoritos
Carpeta personal
Descargas
copiainmage
formulario
hacket
firefox.tmp
vol1-Sector33.doc
vol1-Sector73.jpeg
copiainmage.zip

LibreOffice Writer
vol1-Sector33.doc - LibreOffice Writer
Archivo Editar Ver Insertar Formato Estilos Tabla Formulario Herramientas Ventana Ayuda
Estilo de párrafo pred Times New Roman 12 pt
¡Ayúdenos a mejorar aún más LibreOffice!
Sus donaciones apoyan nuestra comunidad internacional.
Participar
Donar

Jimmy Jungle
626 Jungle Ave Apt 2
Jungle, NY 11111
Jimmy:
Dude, your pot must be the best – it made the cover of High Times Magazine! Thanks for sending me the Cover Page. What do you put in your soil when you plant the marijuana seeds? At least I know your growing it and not some guy in Columbia.
These kids, they tell me marijuana isn't addictive, but they don't stop buying from me. Man, I'm sure glad you told me about targeting the high school students. You must have some experience. It's like a guaranteed paycheck. Their parents give them money for lunch and they spend it on my stuff. I'm an entrepreneur. Am I only one you sell to? Maybe I can become distributor of the year!
I emailed you the schedule that I am using. I think it helps me cover myself and not be predictive. Tell me what you think. To open it, use the same password that you sent me before with that file. Talk to you later.
Thanks,
Joe

Página 1 de 1 175 palabras, 910 caracteres Estilo de página predeterminado Inglés (EE. UU.) 90 %

Paso 17: Análisis el tercer archivo (Scheduld Visits.exe).

Verificamos los datos hexadecimales entregados en la aplicación.

The screenshot shows the CASODISKET-ENFASIS application interface. The 'FILE ANALYSIS' tab is active, displaying a table of file analysis results. The table includes columns for file name, size, and various timestamps. The file 'Scheduled Visits.exe' is highlighted in blue. Below the table, there is a section for 'Hex Contents Of File: C:\Scheduled Visits.exe' showing the hex dump of the file.

File Name	Size	Timestamps
V/V 45782: \$OrphanFiles	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)
v / v \$EAT1	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)
v / v \$EAT2	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)
v / v \$MBR	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)
r / r cover page.jpg	15585	2002-09-11 08:30:52 (American)
r / r 21mmv Jungle.doc	20480	2002-04-15 14:42:30 (American)
r / r Scheduled Visits.exe	1000	2002-05-24 08:20:32 (American)

Hex Contents Of File: C:\Scheduled Visits.exe

```
00000000: 504B 0304 1400 0100 0800 985A B72C C755 PK.....Z...U
00000010: 608D EA08 0000 0042 0000 1400 0000 5363 ..B.....Sc
00000020: 6865 6475 6C65 6420 5669 7369 7473 2E78 deduled Visits.x
00000030: 6C73 94C8 312A E349 0B0B AB10 C270 90FC ls..I.....P.
00000040: 1003 31A2 8C48 E83C 4B81 75C9 8B86 51AF ..1.H.k.u...0
00000050: DF2A 36C3 240B 1A7E 7546 98EE 4E56 4F85 .*6$.-uF..NV0.
00000060: BA8D C460 3654 0E11 AB2E 23A5 E816 0252 ...6T...#....R
00000070: E21F EF90 A3F5 232D 3410 0248 54C1 62CB .....#-4..HT.b.
00000080: SEF1 3F91 5272 E3DC 668A 4A20 D3E2 02CF ..7.Rr...f.J....
00000090: 789A 3568 554D B798 FB88 615F 8399 0553 x.5kUW....a...S
000000A0: 4123 C03B 9A51 68EB A98F BCEC 108A FB87 A#.;.0k.....
000000B0: 40FA 1187 C63B 8537 0356 53AD 118A 117A T...9 UC...+
```

Verificamos sus metadatos.

The screenshot shows the CASODISKET-ENFASIS application interface. The 'FILE ANALYSIS' tab is active, displaying the metadata for the file 'Scheduled Visits.exe'. The 'Dir Entry Number' is 11. The 'File Type' is 'ERROR:[gzip: Exec 'gzip' failed, No such file or directory] (Zip archive data, at least v2.0 to extract, compression method=deflate)'. The 'MD5 of content' is '082a5cc64de322a3a580ffbb5a6fa66'. The 'SHA-1 of content' is 'c8e7f25380d63c9034d9f27faab29de1f09240b5'. The 'Details' section shows the directory entry number, allocated status, file attributes, size, and name. The 'Directory Entry Times' section shows the written, accessed, and created times. The 'Sectors' section shows the sectors 104 and 105.

Dir Entry Number: 11

File Type: ERROR:[gzip: Exec 'gzip' failed, No such file or directory] (Zip archive data, at least v2.0 to extract, compression method=deflate)

MD5 of content: 082a5cc64de322a3a580ffbb5a6fa66 -

SHA-1 of content: c8e7f25380d63c9034d9f27faab29de1f09240b5 -

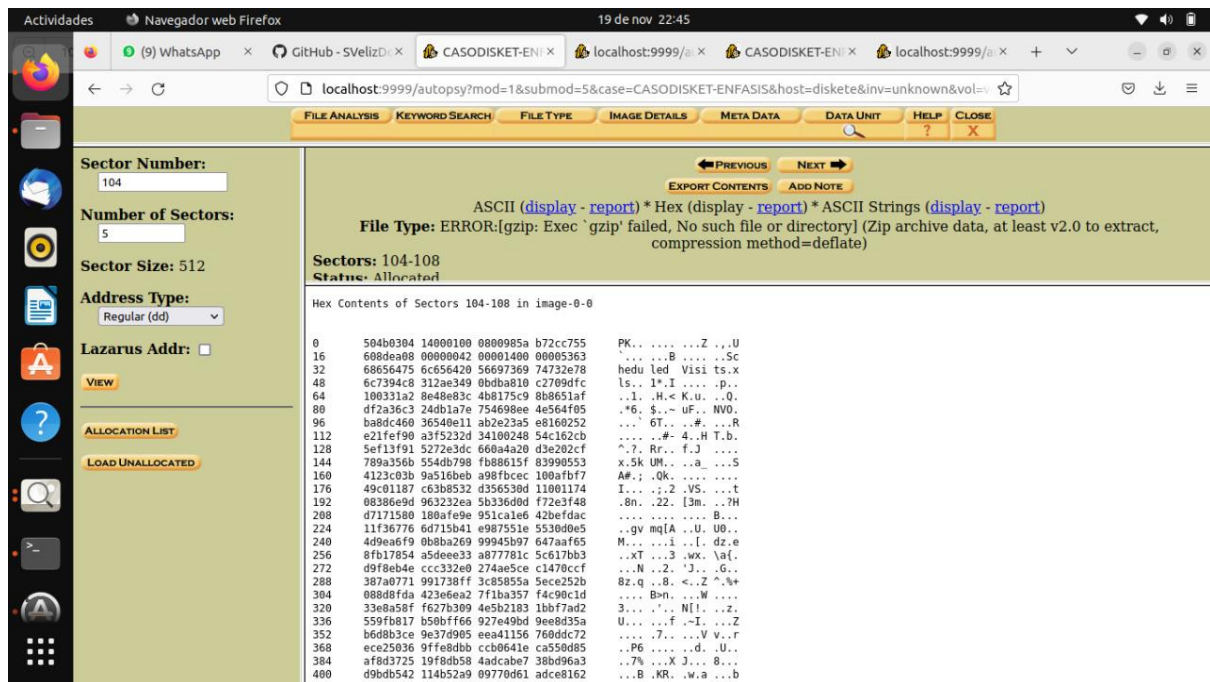
Details:

Directory Entry: 11
Allocated
File Attributes: File, Archive
Size: 1000
Name: SCHEDU~1.EXE

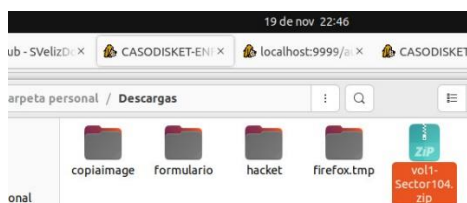
Directory Entry Times:
Written: 2002-05-24 08:20:32 (American)
Accessed: 2002-09-11 00:00:00 (American)
Created: 2002-09-11 08:50:38 (American)

Sectors: 104 105

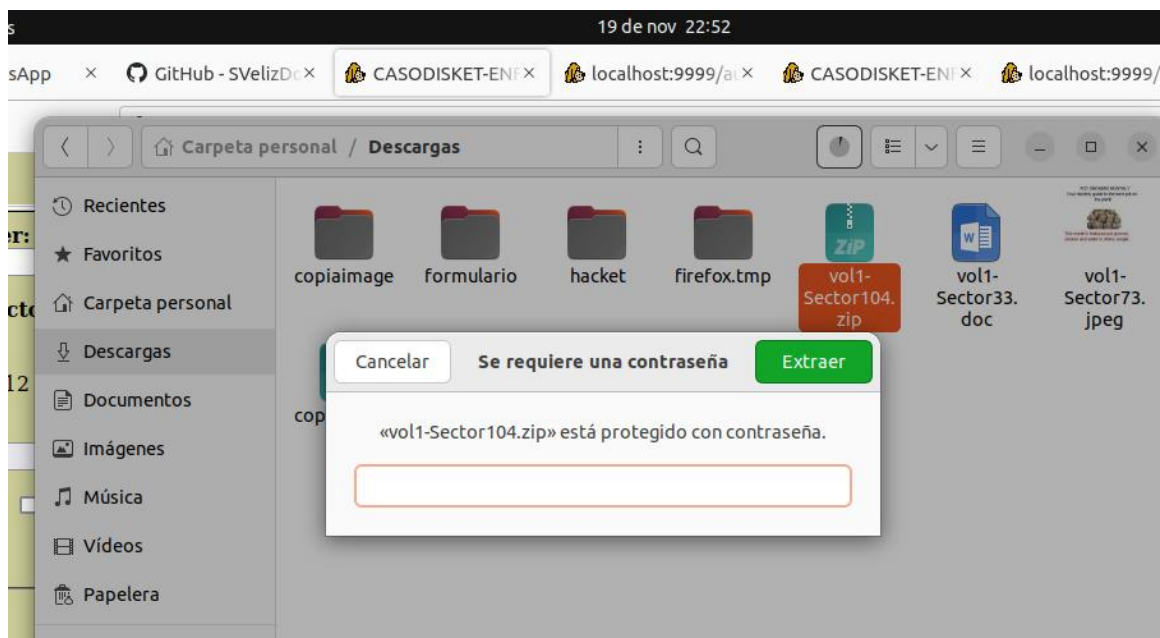
Calculamos los sectores necesarios para construir el archivo, bloque 104 a 108.



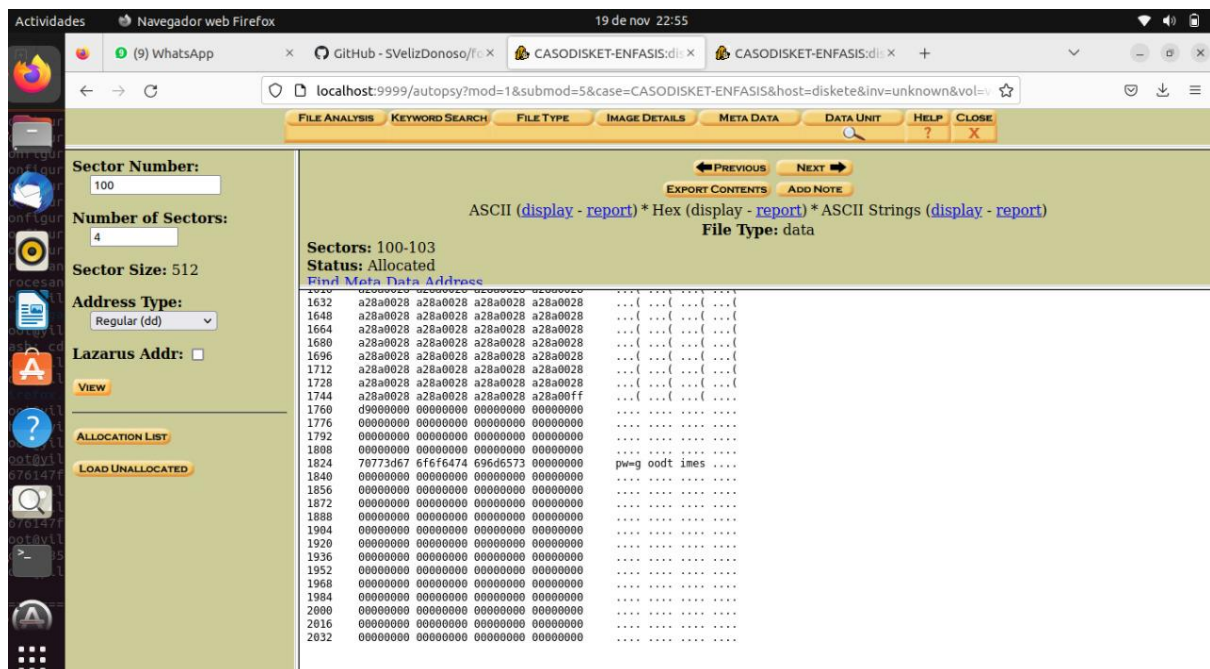
Descargamos el archivo



Intentamos descomprimirlo, pero nos damos cuenta que el archivo está protegido.



Verificamos las evidencias obtenidas, para ver si pasamos un dato relevante que nos indique la contraseña. En los datos hexadecimales del archivo cover page.jpgc del sector 100 a 103 encontramos una palabra (pw=goodtimes) que hace referencia a una contraseña.



Con la información anterior logramos descomprimir el (.zip) encontramos un archivo Excel.



Actividades LibreOffice Calc 19 de nov 22:57

Scheduled Visits.xls - LibreOffice Calc

Archivo Editar Ver Insertar Formato Estilos Hoja Datos Herramientas Ventana Ayuda

Arial 10 pt N K S A

B50 f. Σ = Monday (1)

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Month	DAY	HIGH SCHOOLS										
2	2002												
3	April	Monday (1)	Smith Hill High School (A)										
4		Tuesday (2)	Key High School (B)										
5		Wednesday (3)	Leetch High School (C)										
6		Thursday (4)	Birard High School (D)										
7		Friday (5)	Richter High School (E)										
8		Monday (1)	Hull High School (F)										
9		Tuesday (2)	Smith Hill High School (A)										
10		Wednesday (3)	Key High School (B)										
11		Thursday (4)	Leetch High School (C)										
12		Friday (5)	Birard High School (D)										
13		Monday (1)	Richter High School (E)										
14		Tuesday (2)	Hull High School (F)										
15		Wednesday (3)	Smith Hill High School (A)										
16		Thursday (4)	Key High School (B)										
17		Friday (5)	Leetch High School (C)										
18		Monday (1)	Birard High School (D)										
19		Tuesday (2)	Richter High School (E)										
20		Wednesday (3)	Hull High School (F)										
21		Thursday (4)	Smith Hill High School (A)										
22		Friday (5)	Key High School (B)										
23		Monday (1)	Leetch High School (C)										
24		Tuesday (2)	Birard High School (D)										
25	May												
26		Wednesday (3)	Richter High School (E)										
27		Thursday (4)	Hull High School (F)										
28		Friday (5)	Smith Hill High School (A)										

Sheet1 Sheet2 Sheet3

Hoja 1 de 3 PageStyle_Sheet1 Español (Colombia) Promedio: Suma: 0 100 %

PREGUNTAS DEL CASO

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

Nombre: Jimmy Jungle

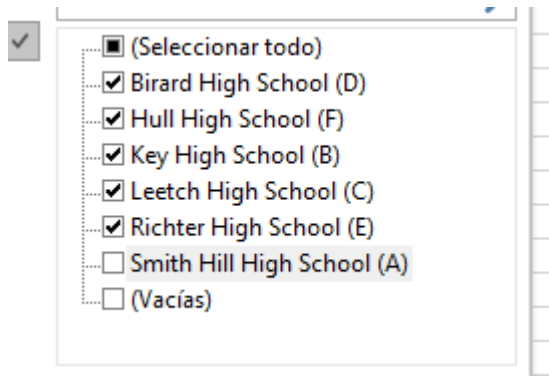
Dirección: 626 Jungle Ave Apt 2, Jungle, NY 11111

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

En el archivo, entre el sector 100 a 103 se encontró el siguiente texto (pw=goodtimes).

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

- Key High School (B)
- Leetch High School (C)
- Birard High School (D)
- Richter High School (E)
- Hull High School (F)



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

Se borro el archivo Jimmy Jungle.doc, se guardo en un archivo (.zip), protegió el archivo con una contraseña e renombro el archivo con extensión (.exe).

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

Visualización con herramienta Autopsy, construcción de imagen "cover page.jpgc" a través de los sectores, construcción de archivo "Jimmy Jungle.doc", recuperación de archivo "Scheduled Visits.exe", transformación y extracción de información con la herramienta Winzip, utilizamos Libre Office para visualizar el archivo Excel.

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

La imagen fue creada en una herramienta de Microsoft, posiblemente en (Word o Power Point) donde pudo ser renderizada y exportada, o simplemente se saco un recorte o screenshop. También cabe mencionar la posibilidad que pudo ser echa en la herramienta Power Point, donde de forma fácil podemos crear imágenes insertando nuevas y añadiéndoles cualquier propiedad, en este caso el texto.

