# 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

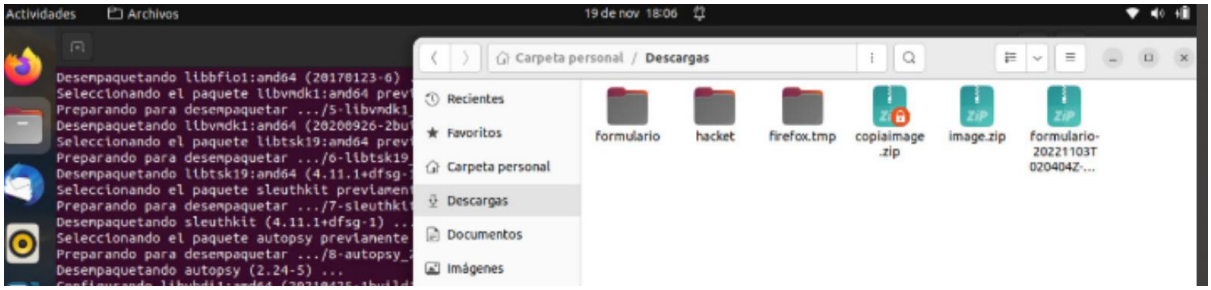
2022

## TABLA DE CONTENIDO

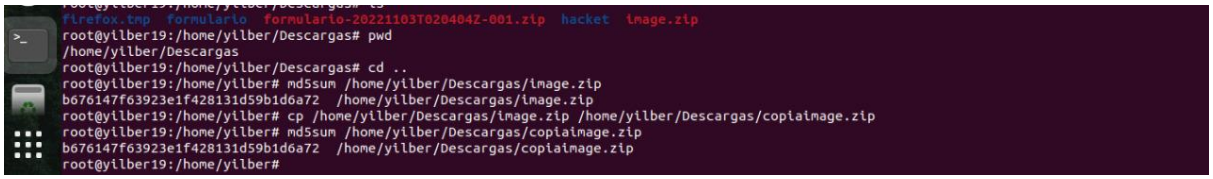
# DESARROLLO ANALISIS FORENCE

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

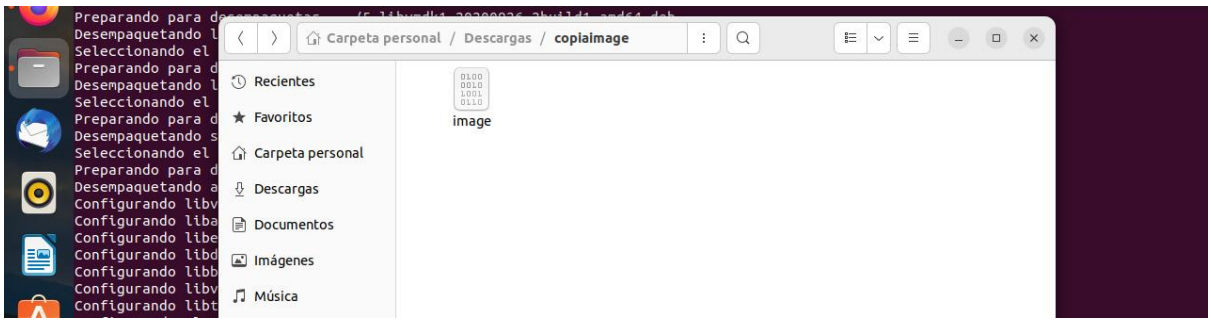
**Paso 1:** Instalación de Autopsy, y se descargó la imagen.



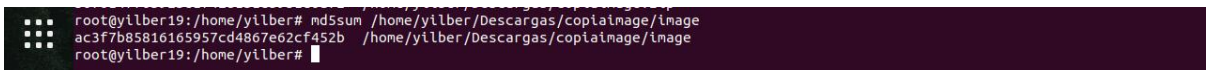

**Paso 2:** Se calcula el hash md5 de la imagen, se hace una copia de la imagen y también se calcula el has md5 para verificar que estamos trabajando con una copia exacta.



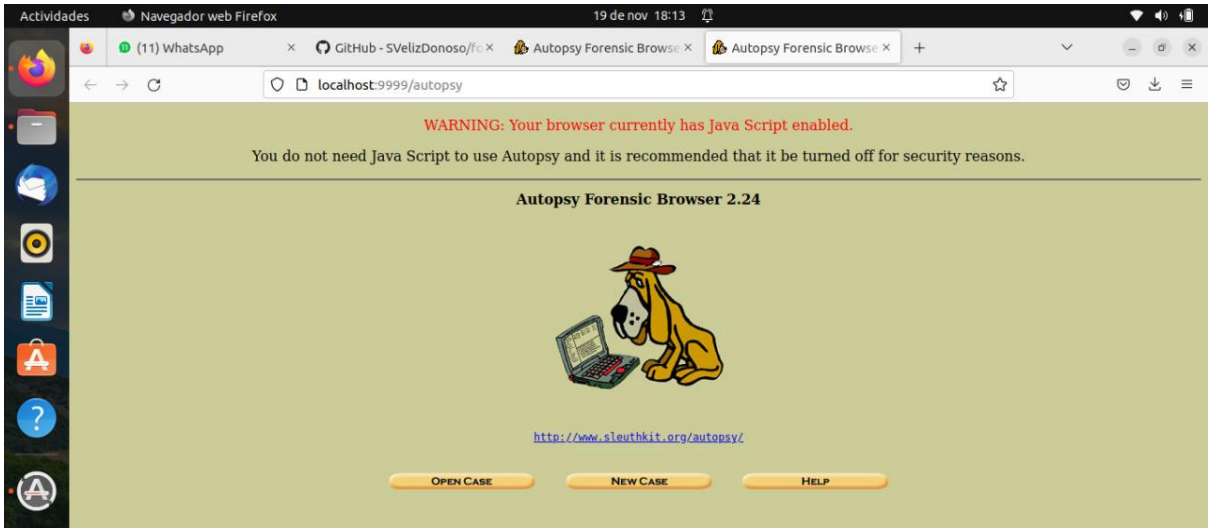

**Paso 3:** Extraemos el .ZIP y obtenemos la imagen (disk).



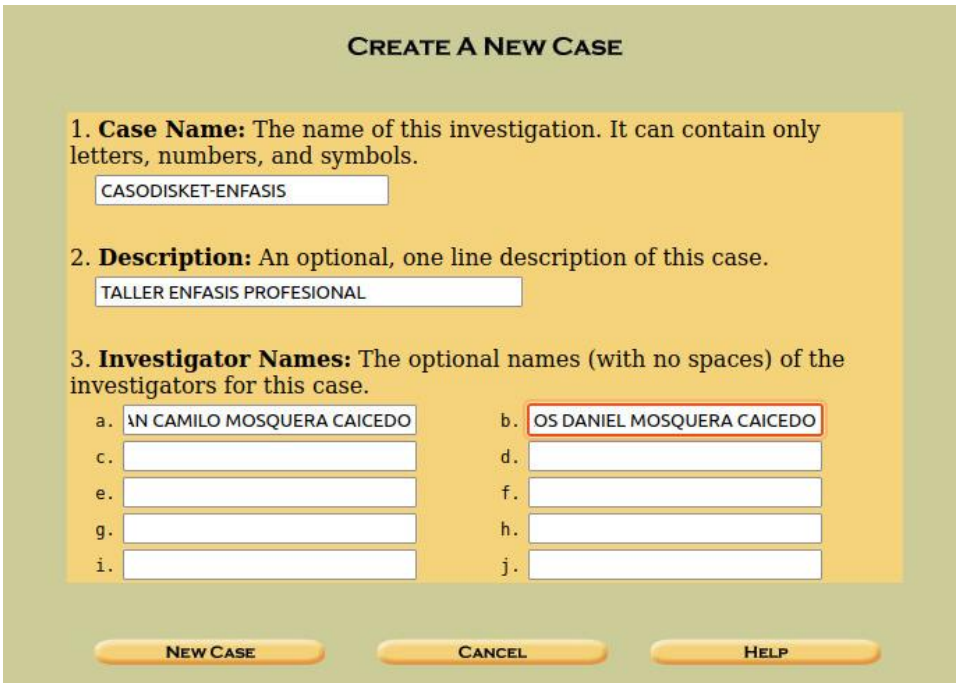

**Paso 5:** Calculamos el hash md5 de la imagen y ejecutamos Autopsy para comenzar con el proceso.

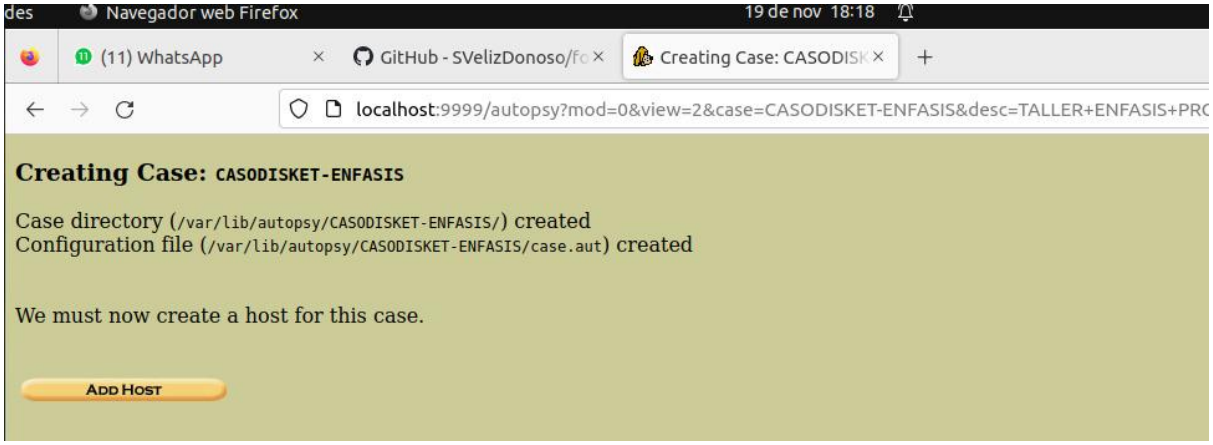



**Paso 6:** Abrimos Autopsy.



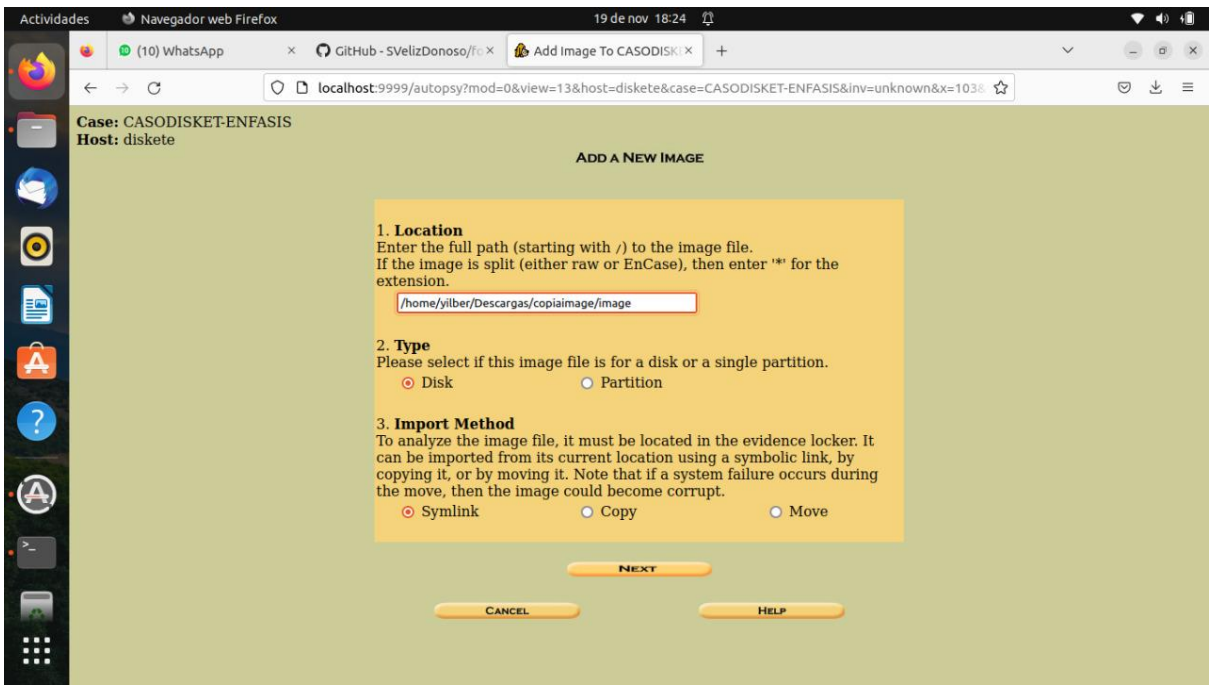

**Paso 7:** Creamos el caso.

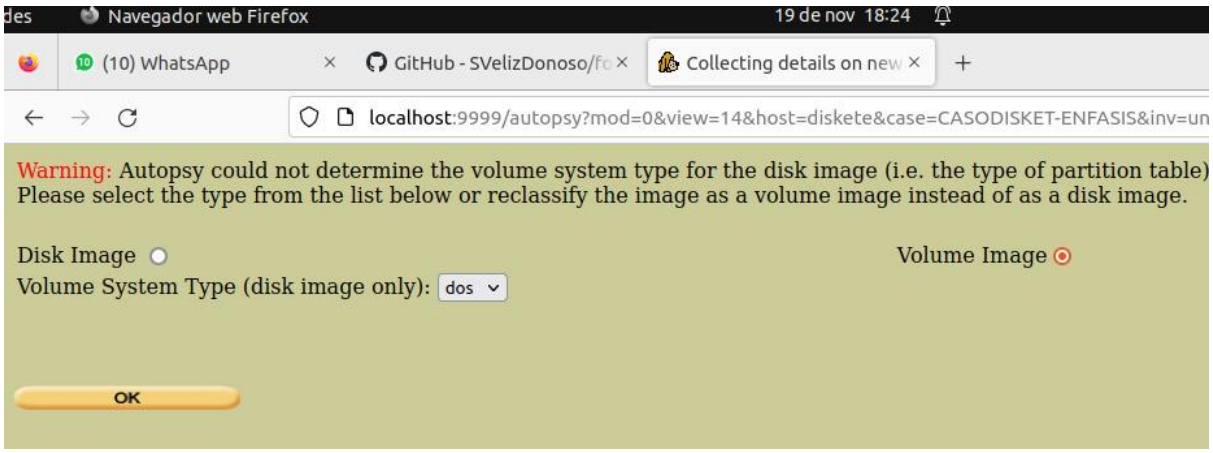




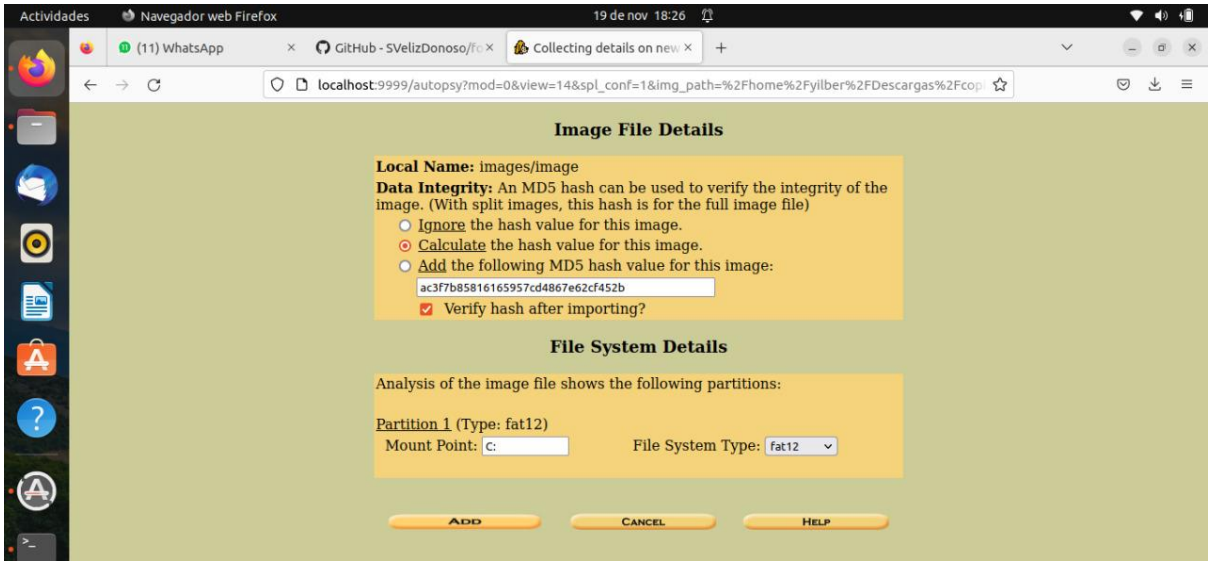

**Paso 8:** Creamos el host y confirmamos.


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

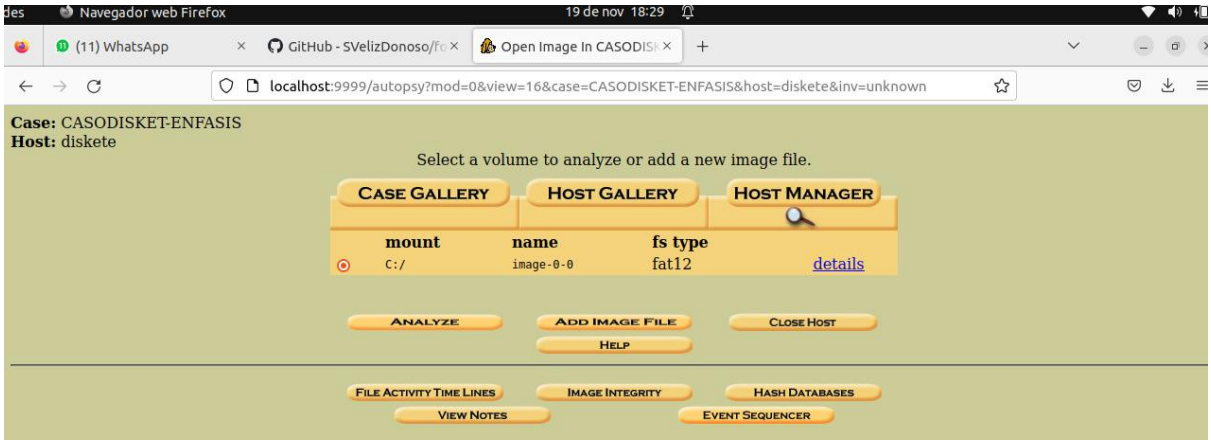





**Paso 10:** Configuramos el detalle de la imagen e ingresamos el hash md5 de la imagen obtenido anteriormente.

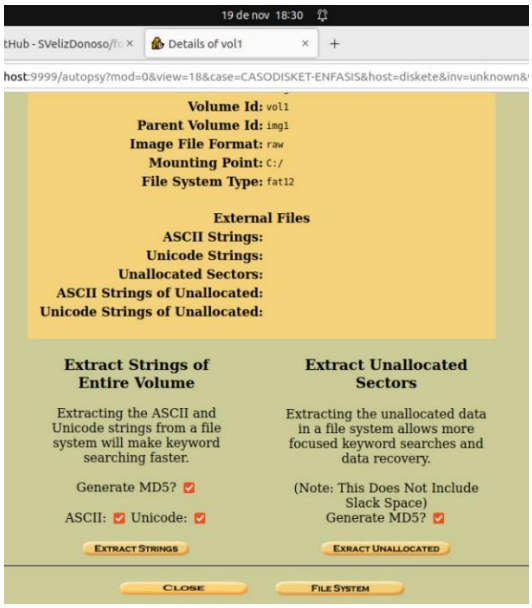



**Paso 11:** Comenzamos el análisis.

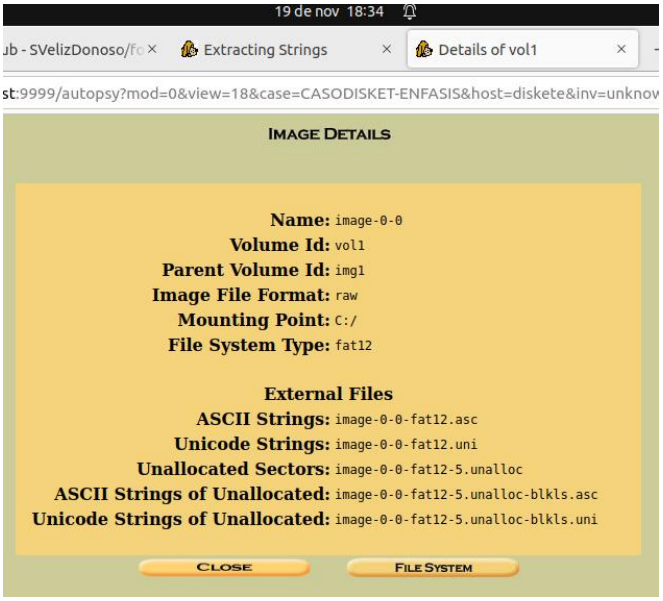



**Paso 12:** Creamos los índices de búsqueda en el disco.

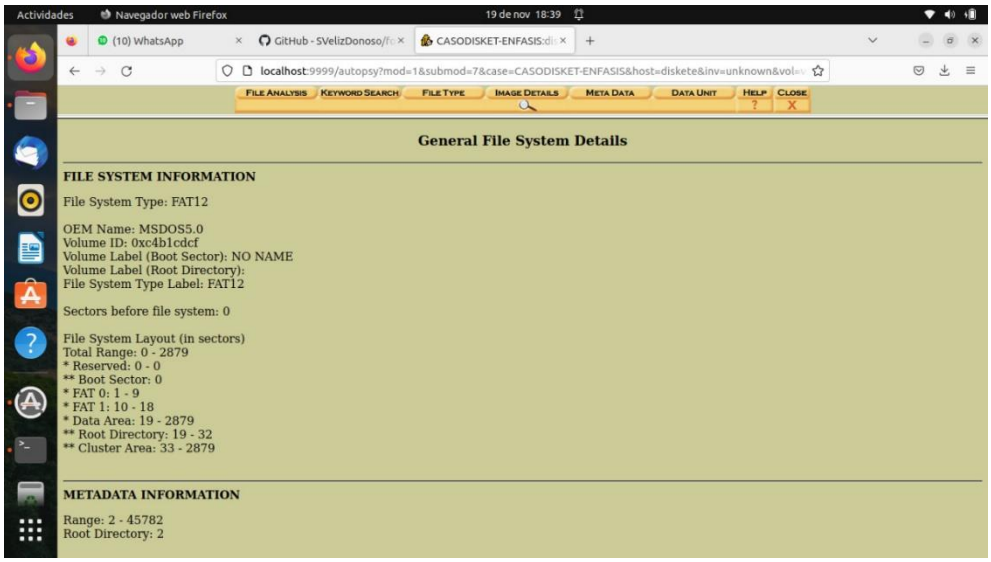
**Antes:**

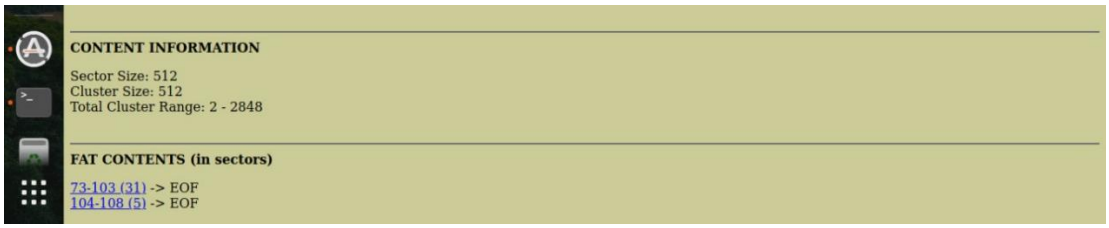



**Despues:**

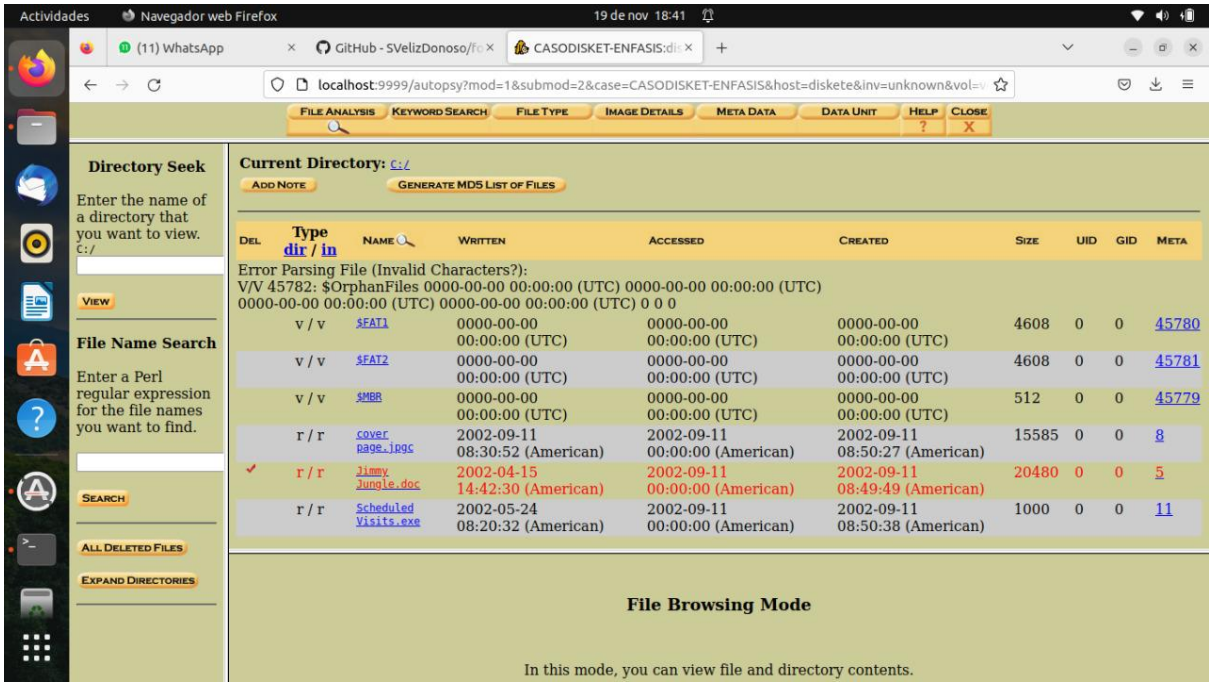


**Paso 13:** Analizamos la imagen y vemos el detalle.

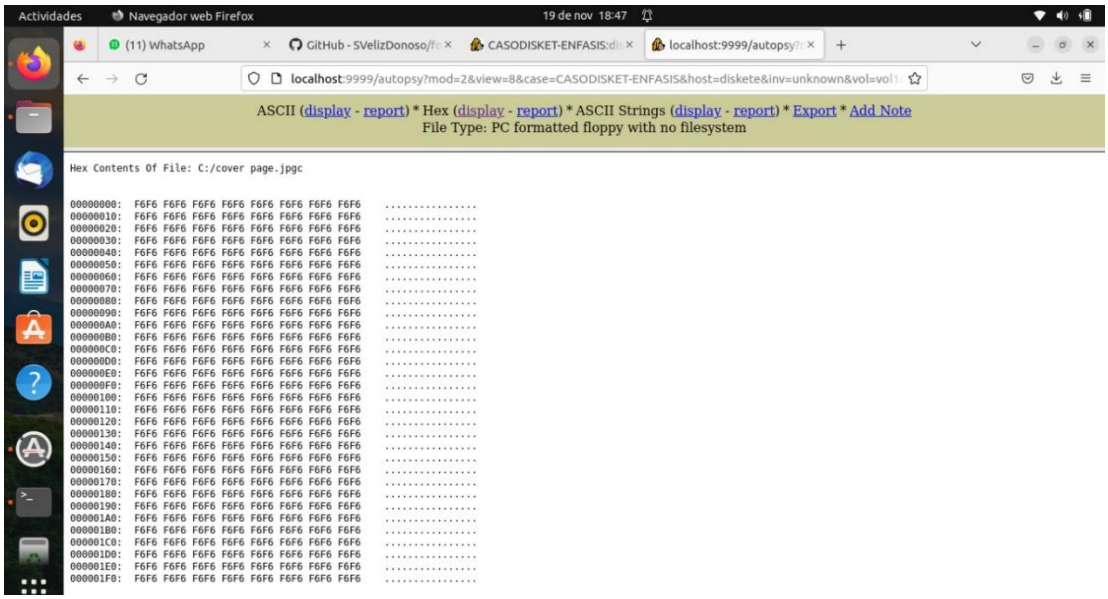



**Paso 14:** Después de mirar el tamaño del clúster, memoria y metadatos pasamos a analizar cada uno de los archivos.

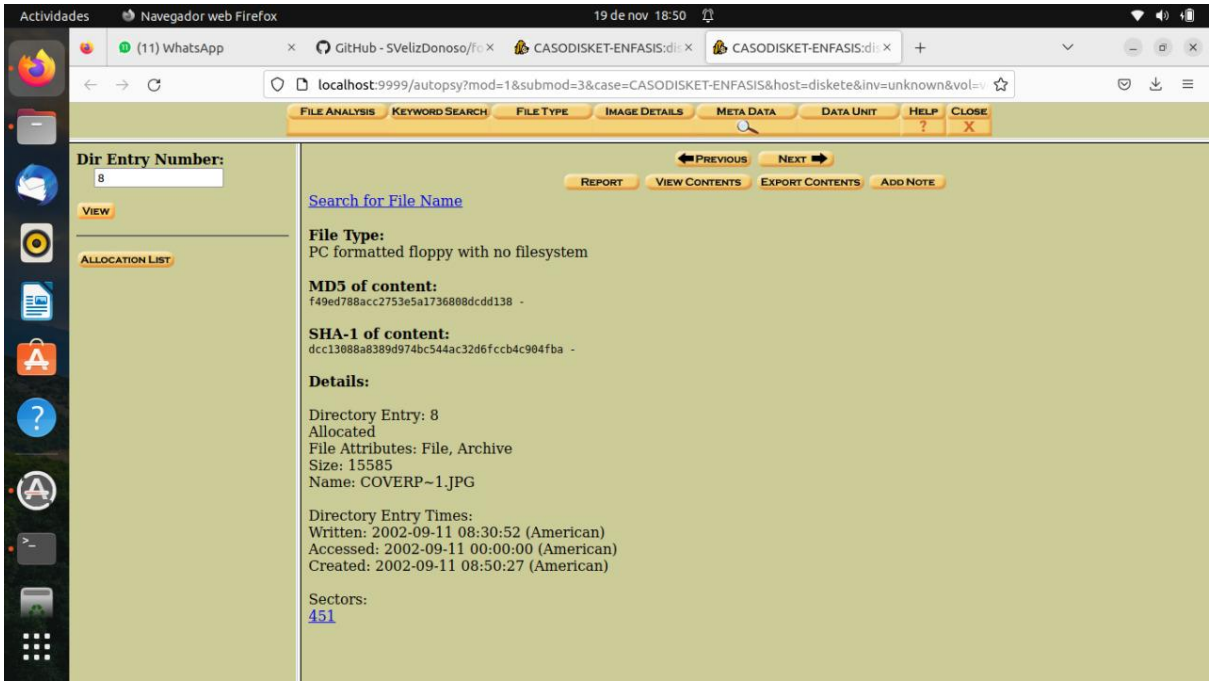


**Paso 15:** Analizamos el primer archivo (cover page.jpgc).

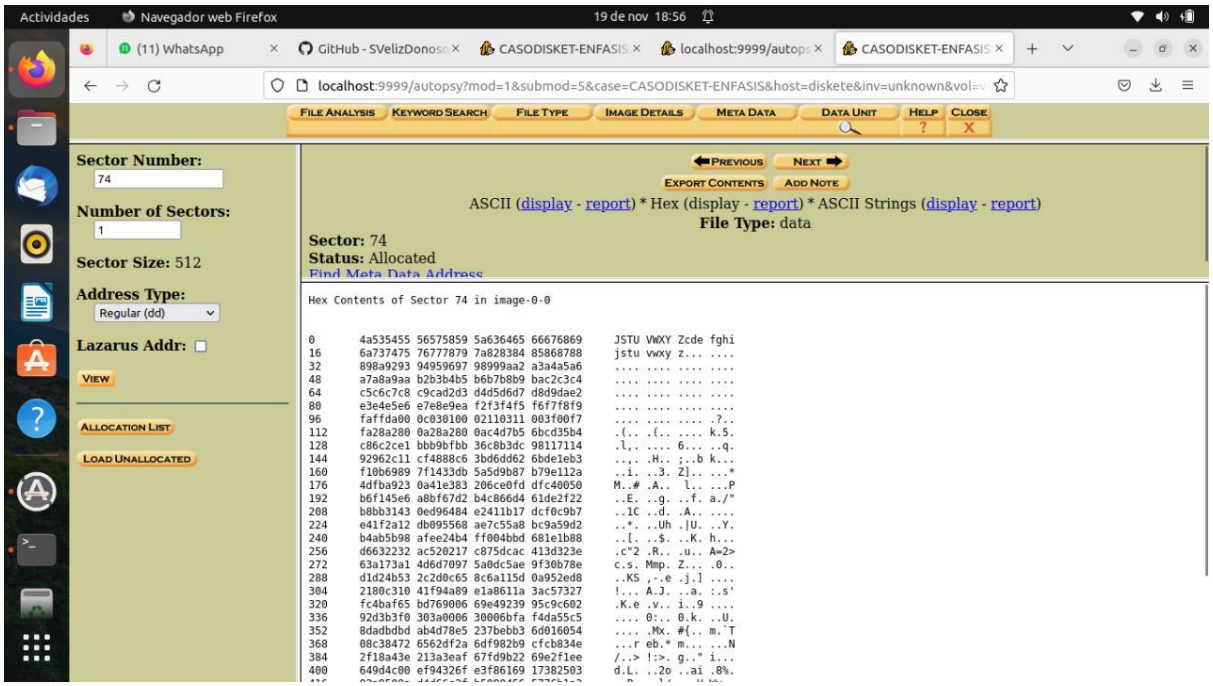



Evidenciamos que el archivo no es reconocido con extensión (.jpeg).

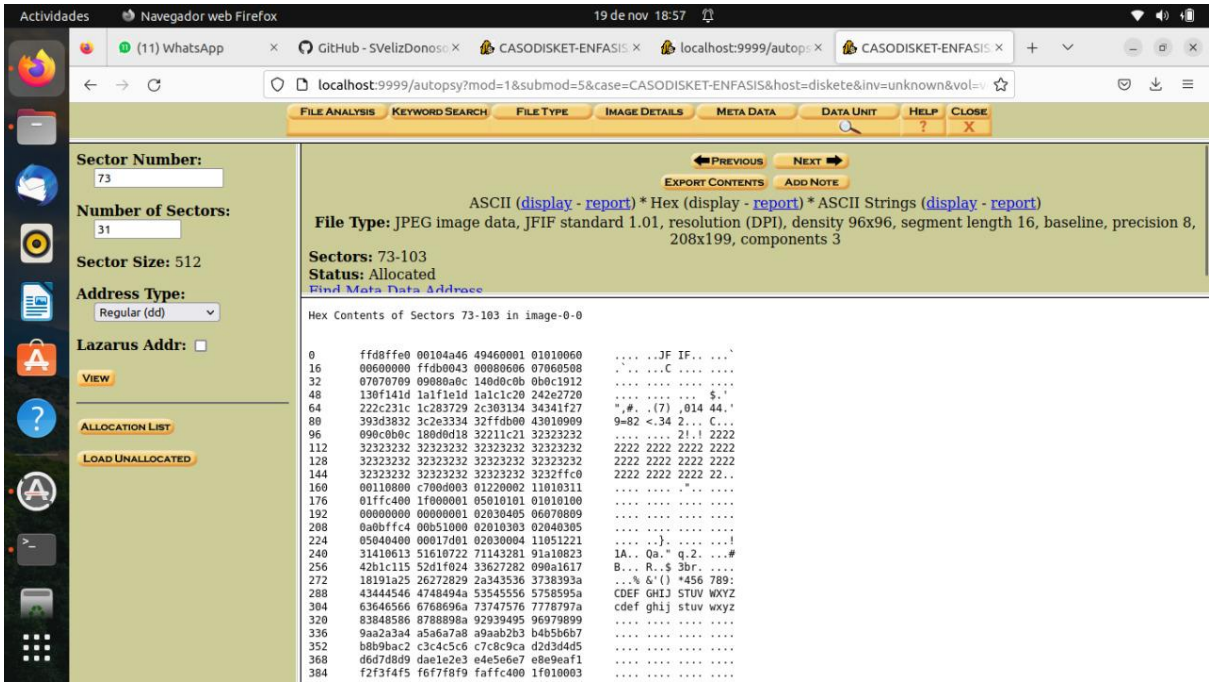
Visualizamos metadatos.



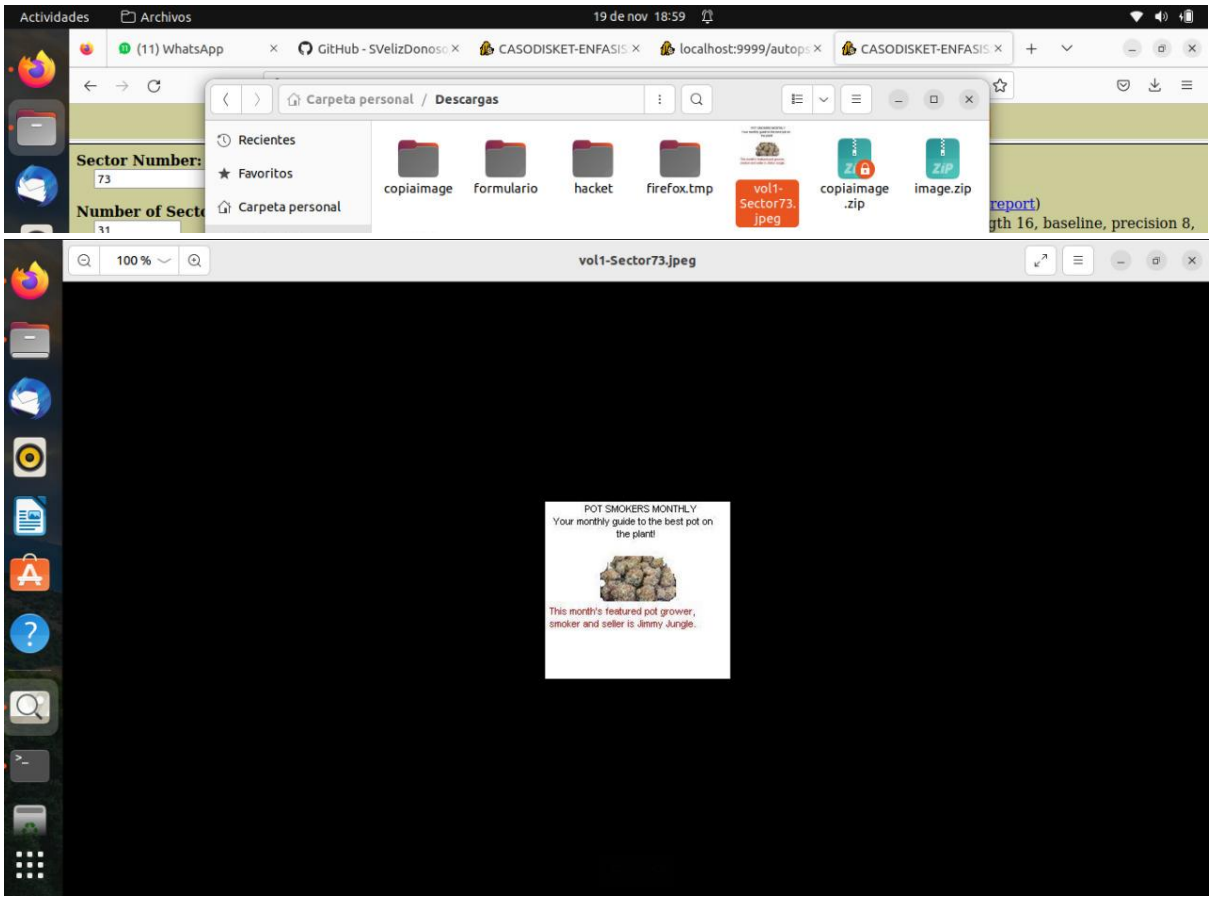
Procedemos al cálculo del archivo, obtenemos lo sectores necesarios para reconstruir la imagen.



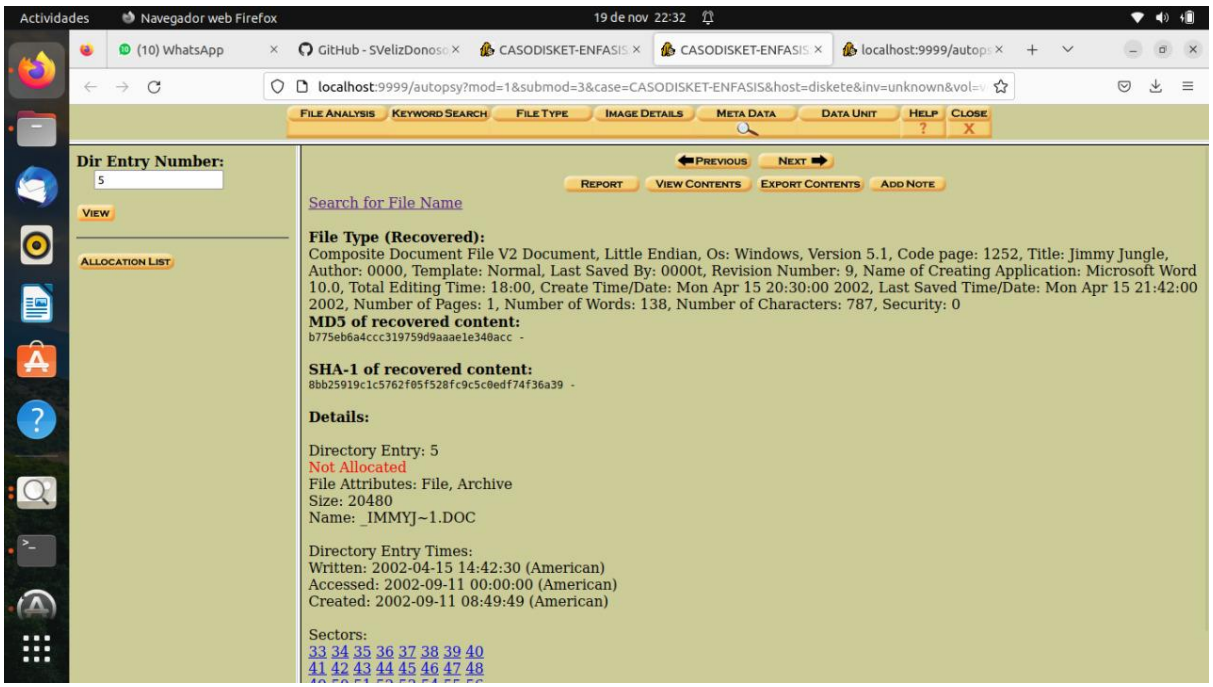

Como se encontraron 31 sectores, significa que debemos empezar desde el sector 73, sectores a seleccionar 73 + 31 = (73 - 103).



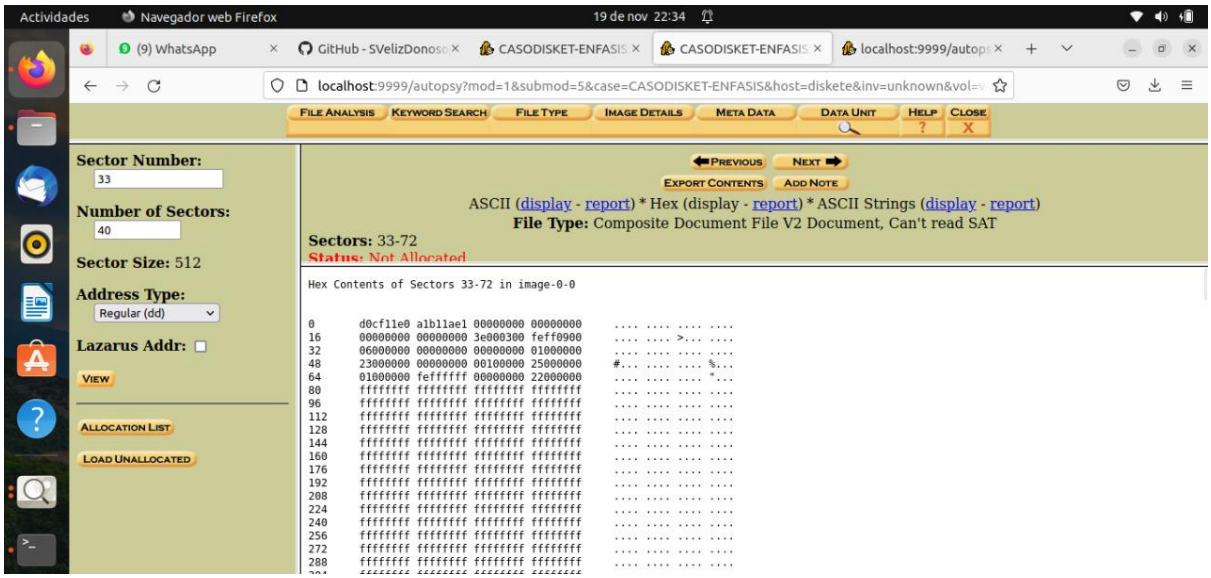
Procedemos a descargar la imagen y a cambiar su formato.



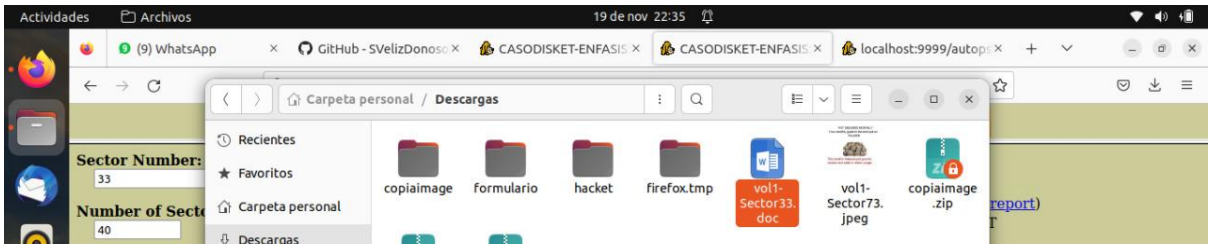

**Paso 16:** Analizamos el segundo archivo (Jimmy Jungle.doc). Verificamos sus metadatos.

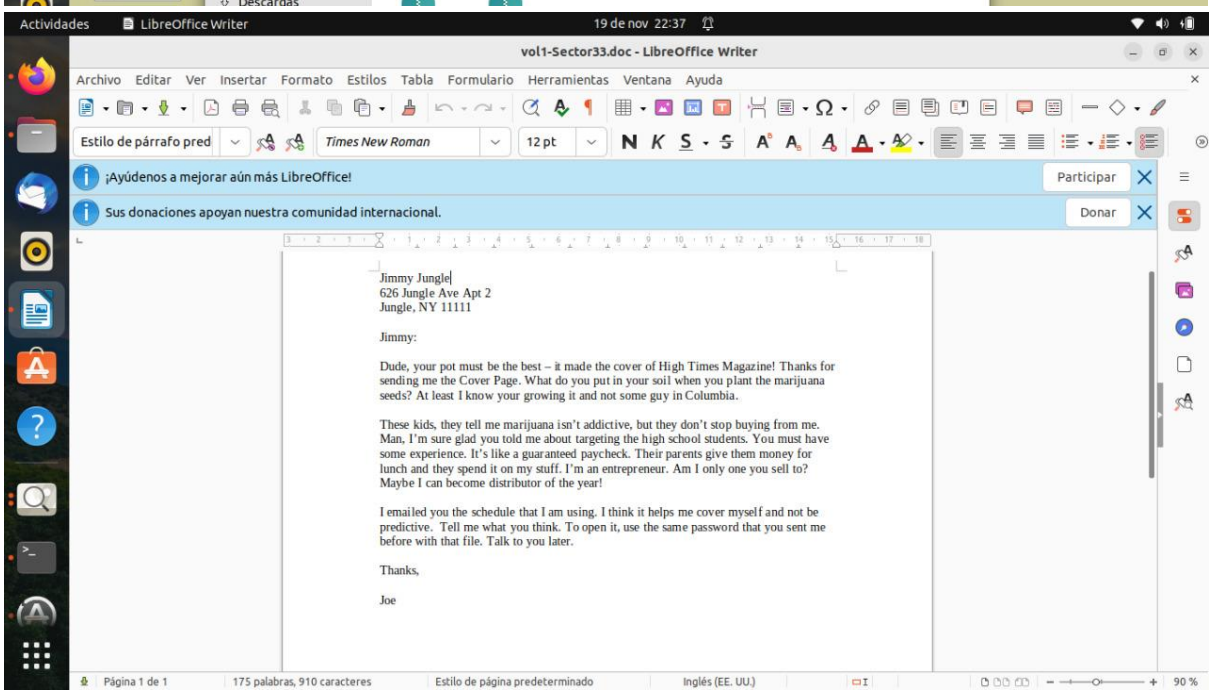


**Cálculo del archivo:** número de sectores 72 – 32 = 40



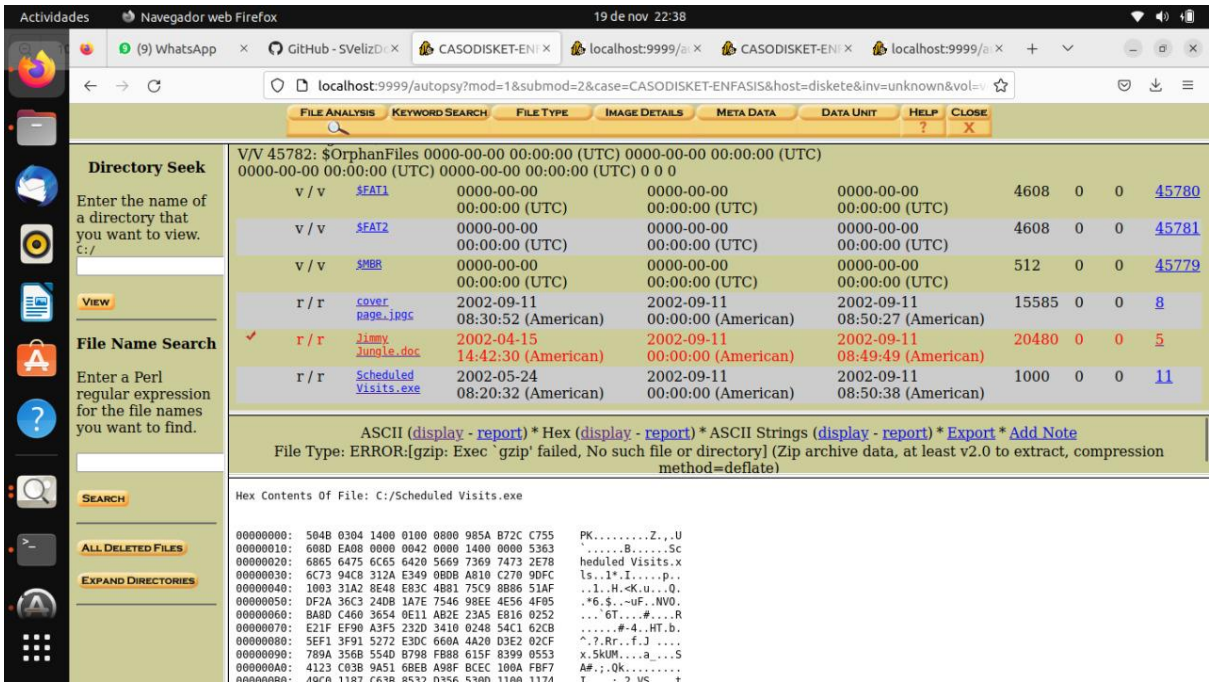

Procedemos a descargar el archivo.



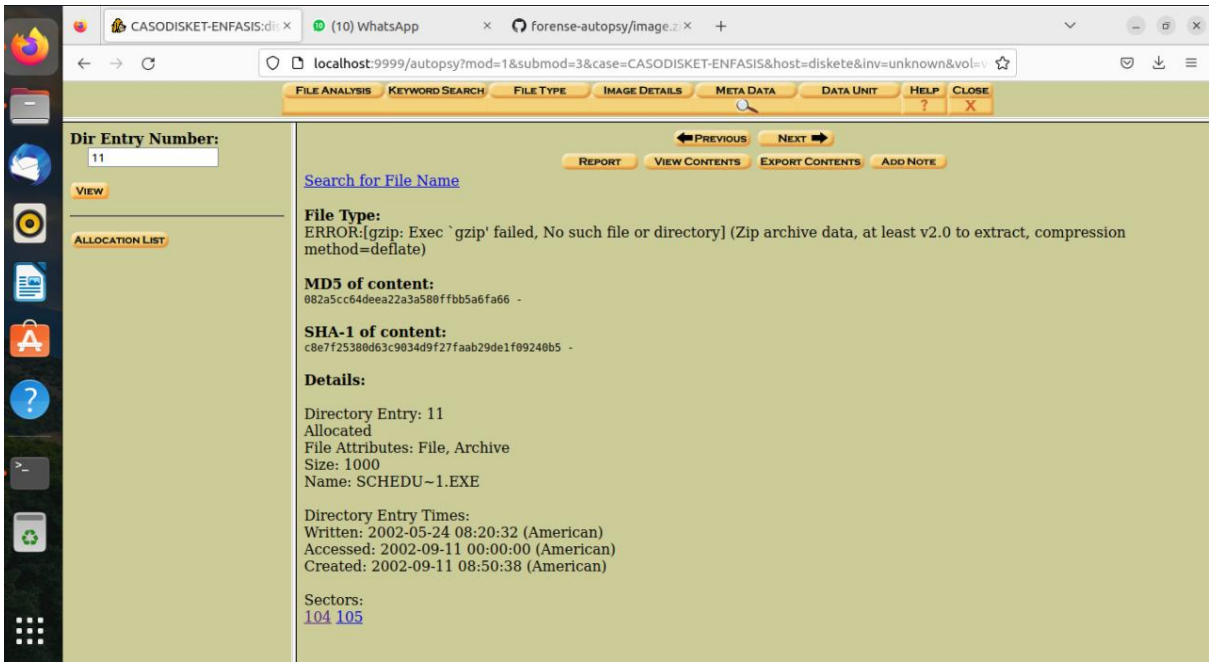



**Paso 17:** Análisis el tercer archivo (Schedueld Visits.exe).

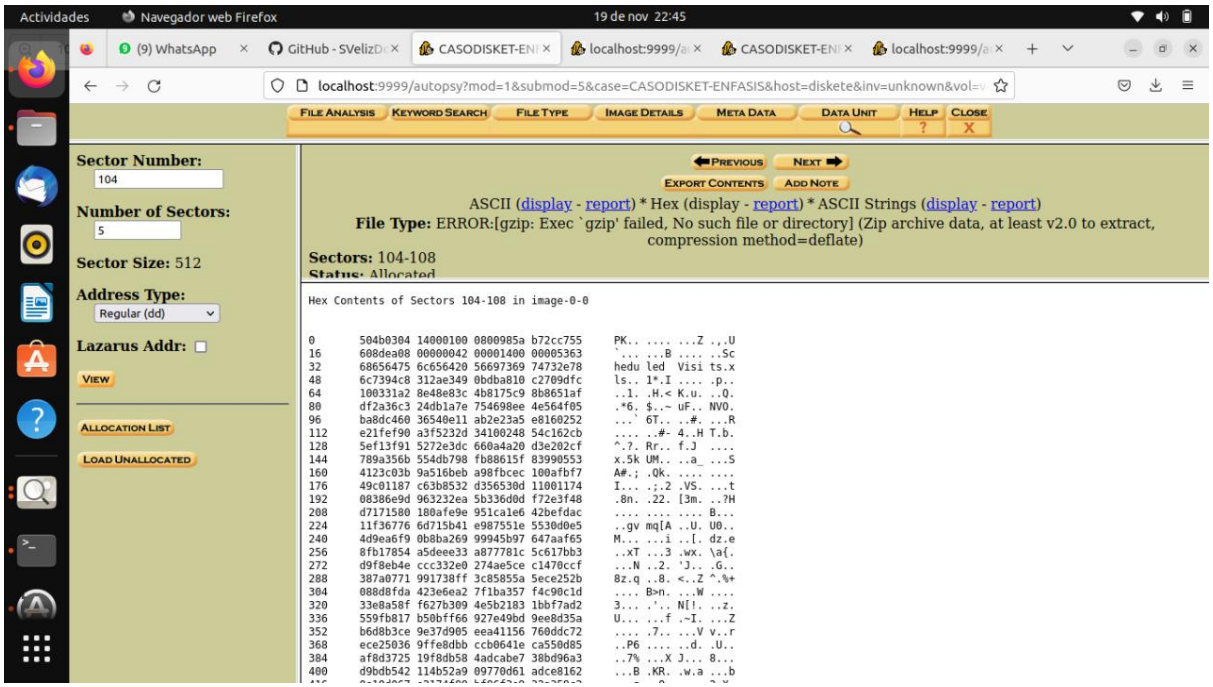
Verificamos los datos hexadecimales entregados en la aplicación.



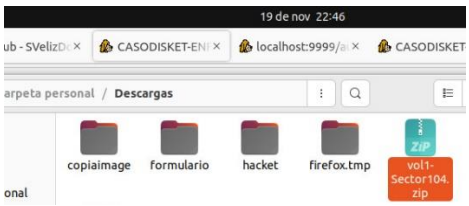

Verificamos sus metadatos.



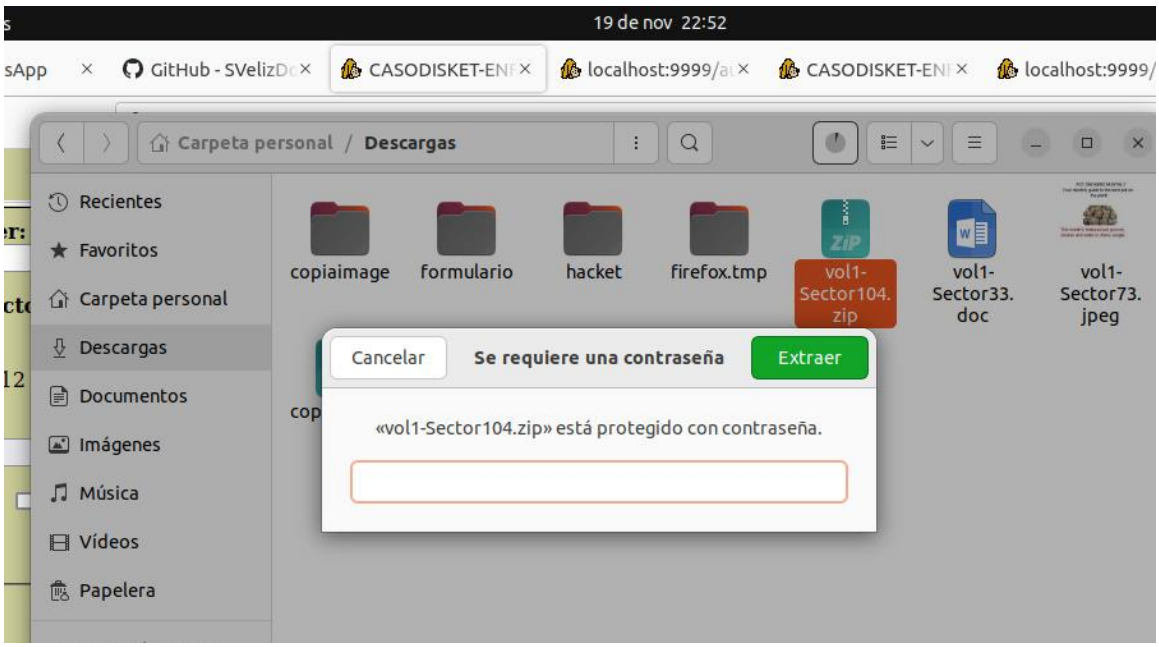
Calculamos los sectores necesarios para construir el archivo, bloque 104 a 108.



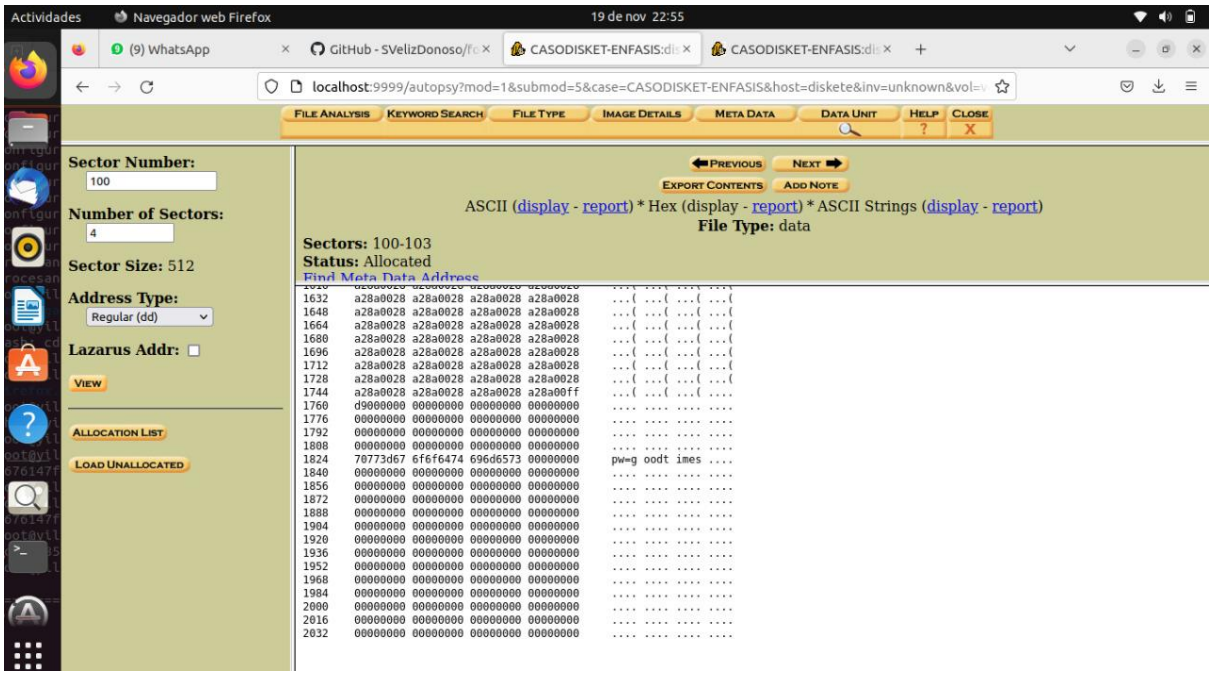

Descargamos el archivo



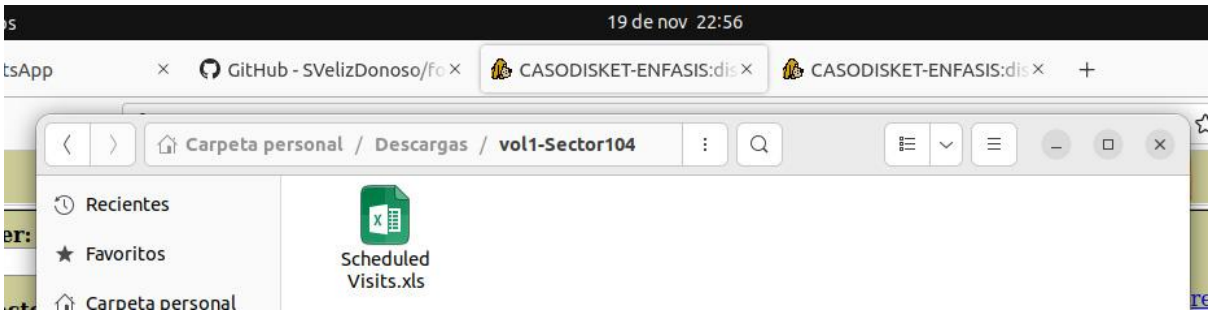

Intentamos descomprimirlo, pero nos damos cuenta que el archivo está protegido.

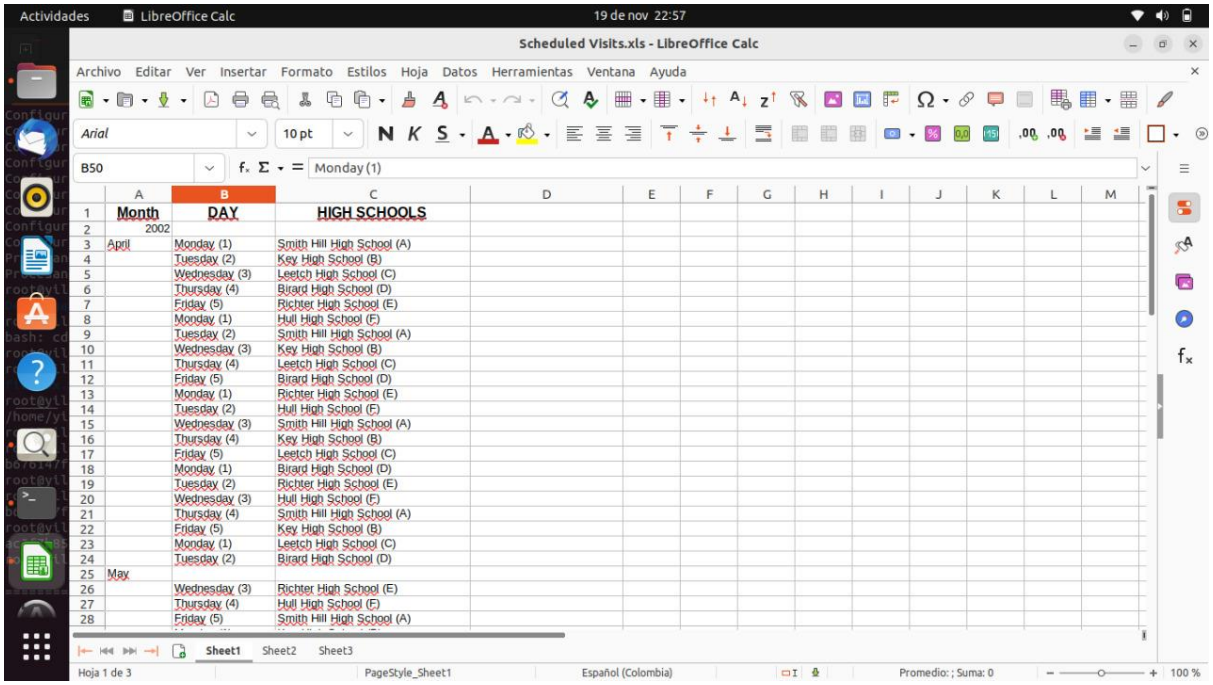


Verificamos las evidencias obtenidas, para ver si pasamos un dato relevante que nos indique la contraseña. En los datos hexadecimales del archivo cover page.jpgc del sector 100 a 103 encontramos  una palabra (pw=goodtimes) que hace referencia a una contraseña.




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






| | A | B | C |
|---|---|---|---|
| 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) |

## PREGUNTAS DEL CASO

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

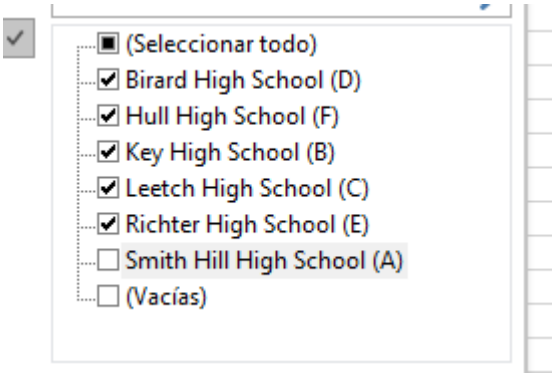
   **Nombre:** Jimmy Jungle
   **Dirección:** 626 Jungle Ave Apt 2, Jungle, NY 11111

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.