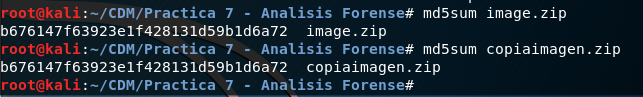
CDM – Practica 7 Analisis Forense

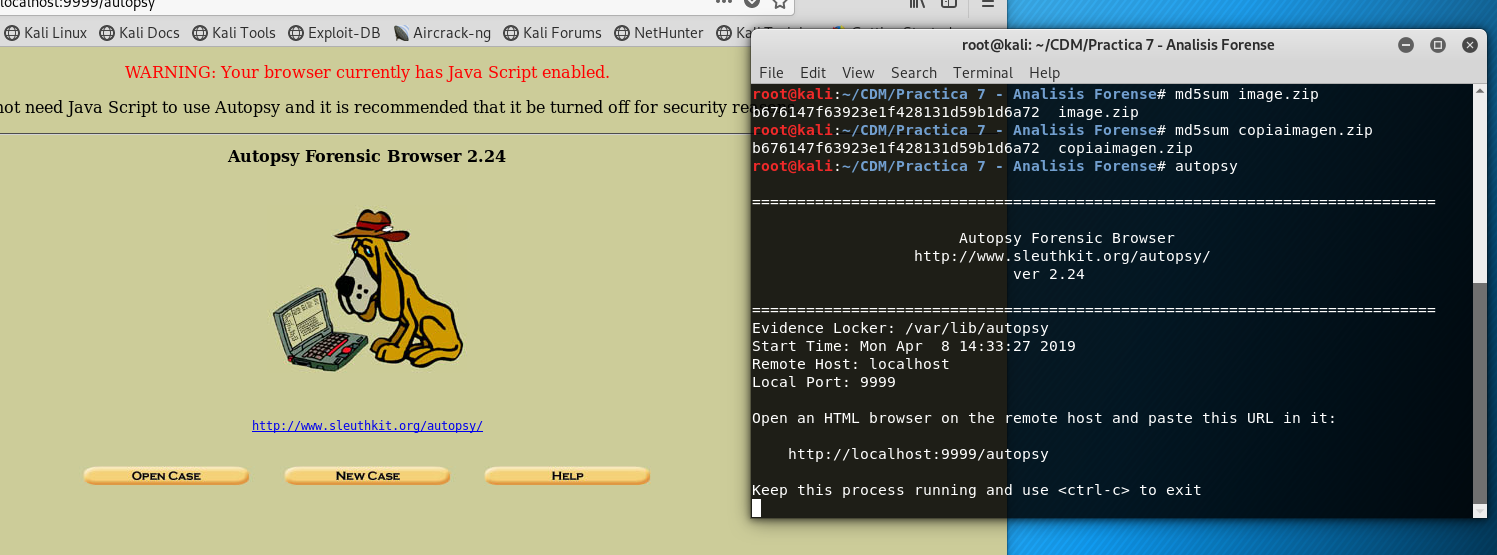
Nombre : Adrian Tendero Lara

La pracnica nos pide que estudiemos un caso policial donde tenemos que analizar una imagen de un dispositivo, lo primero que tenemos que hacer es el md5 de la imagen obtenida y de la copia realizada para probar que son idénticos.



Ahora podemos garantizar que empezamos con una copia idéntica de la original pudiendo repetir los pasos realizados y obtener los mismos resultados.

Para realizar el análisis vamos ha utilizar autopsy con la imagen que contiene el archivo zip anterior (siempre trabajando sobre la copia para preservar el original intacto)



Abrimos el caso en autopsy y rellenamos toda la información pertinente.

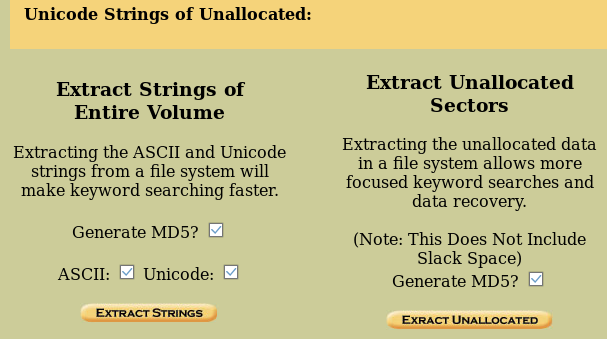


Como se puede ver tras la importación la imagen con la que trabaja autopsy es la misma que la original.

(\*Me salto todo el proceso ya que no hay ninguna dificultad y es seguir los pasos indicados\*)

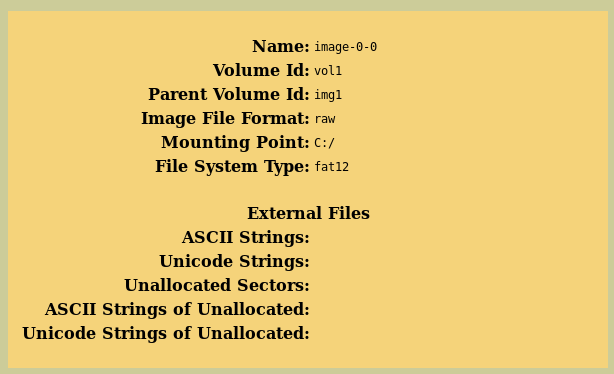
Una vez abierto el caso ya podemos empezar ha analizar las evidencias.

Ahora vamos ha crear los índices de la búsqueda y para eso tenemos que ir ha los detalles de la imagen importada y extraemos los String y los Unallocated con estos 2 botones

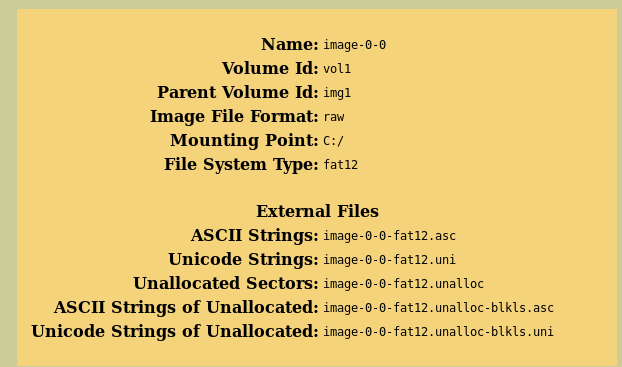


Esto nos permitirá pasar de no tener ningún dato para buscar a tener ya todos los datos extraídos para poder realizar las busquedas.

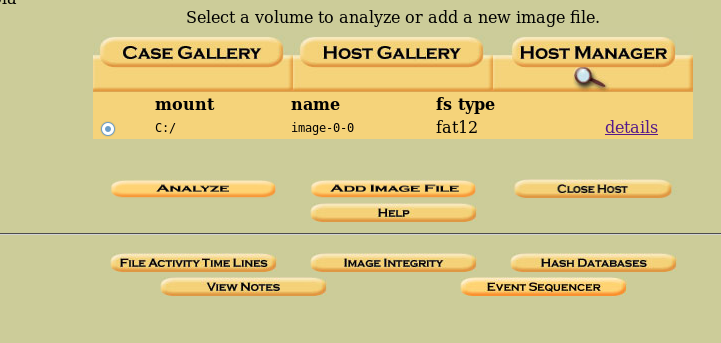
Estado de la imagen ANTES:



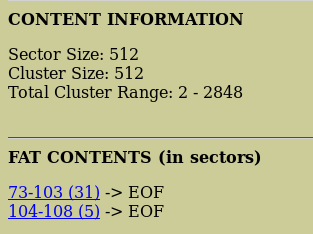
DESPUES:



Ahora vamos a analizar, para eso apretamos el botón de analizar



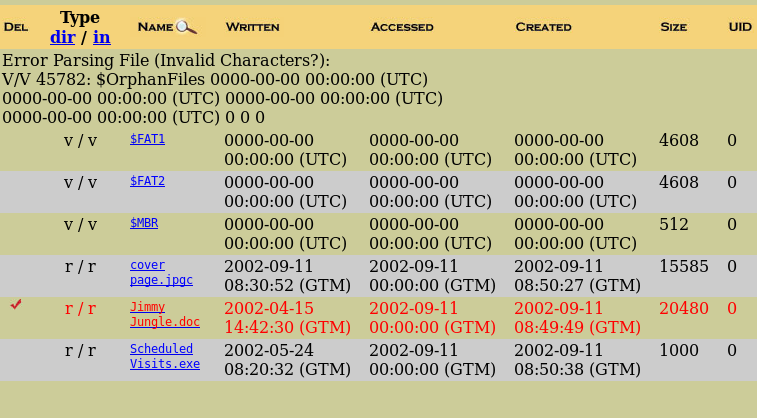
Primero vamos ha analizar por si hay imágenes en la unidad del disco, para eso nos vamos ha image Detalls y obtenemos la siguiente información.



Esto nos indica donde están localizado (en sectores), para poder extraerlo y observarlo utilizando la información anterior procederemos a analizar los sectores con el file Analysis.



Lo que nos muestra varios archivos.



De los cuales solo hay un jpg (imagen) que nos centraremos ahora en visualizarla.

Para ello primero visualizaremos los metadatos de la imagen



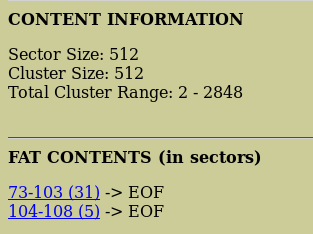
Esto nos señala una inconsistencia ya que el tamaño de la imagen es superior al de los sectores asignados, por tanto vamos ha analizar la discrepancia.

El tamaño fat 12 es de 512 bits por sector y la imagen ocupa 15585 bits por tanto con un simple calculo podemos saber cuantos sectores ocupa la imagen realmente.

(15585 + 511)/512 = 31

Con esta informacion podemos hacer 2 cosas:

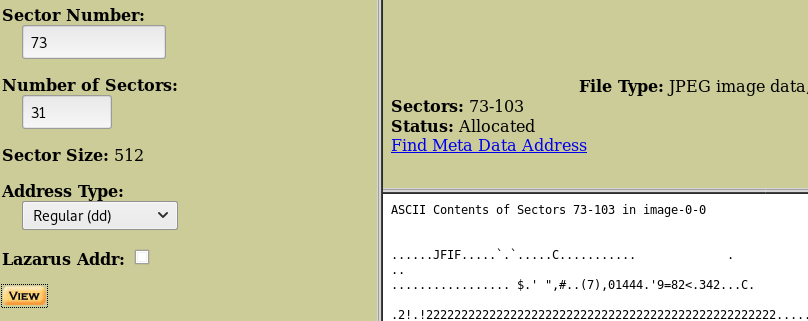
La primera es ir recorriendo los sectores 1 a 1 desde el 451 en sentido descendente o pararnos y revisar las notas que ya hemos obtenido, con lo cual vemos lo siguiente.



Con esto podemos apreciar que al analizar los detalles de las imágenes encontramos una imagen que ocupa los sectores del 73-103 es decir 31 sectores.

Para comprobar si realmente contiene el inicio del la imagen analizaremos su código hexagesimal. Para ello nos iremos ha analizar los Data Unit del sector 73 al 103.

Esto nos muestra el siguiente resultado



Como se puede apreciar el sistema reconoce los ficheros como una imagen jpeg y también lo podemos comprobar por que al inicio del fichero esta la cabecera de un fichero JPEG “JFIF”, ahora procedemos ha descargarlo, aplicar la extensión correcta (raw 🡪jpg) y la visualizamos.

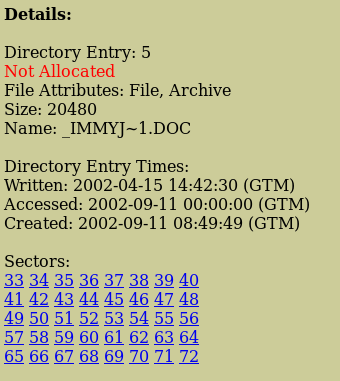


Esta imagen nos proporciona la evidencia de quien es el vendedor, que es **Jimmy Jungle**

Tras esto ahora continuaremos con otros archivos, en concreto el archivo Jimmy jungle.doc que esta eliminado.



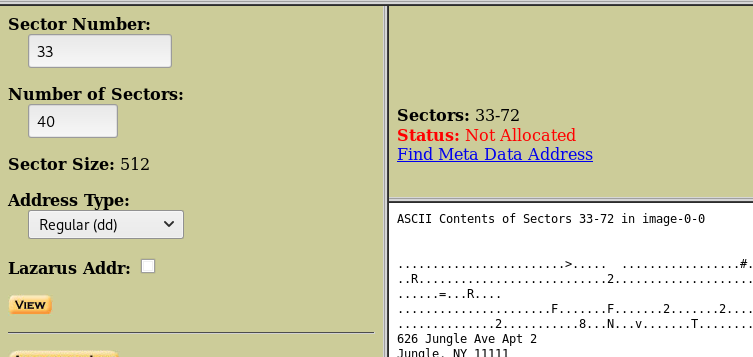
Para ello miraremos primero que nada sus metadatos en busca de información útil



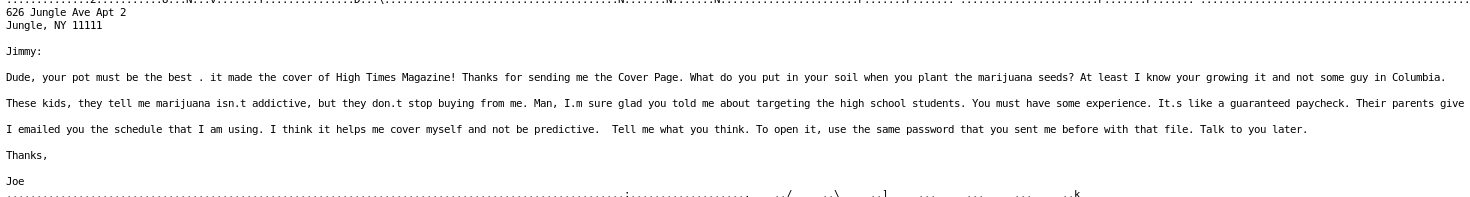
En este caso si que nos muestra los sectores que ocupa el archvio 33 – 72 -> 40 Sectores

Ahora vamos ha proceder ha reconstruir el fichero analizando los datos de esos 40 sectores.

Esto nos muestra el siguiente resultado



El sistema lo reconoce como un documento de texto y muestra parte de dicho texto donde los permite conocer y confirmar quien es el vendedor de maría y cual es su dirección… respondiendo a las preguntas 1 y 2 de las practicas.



Vendedor : **Jimmy Jungle** (confirmando la evidencia anterior)

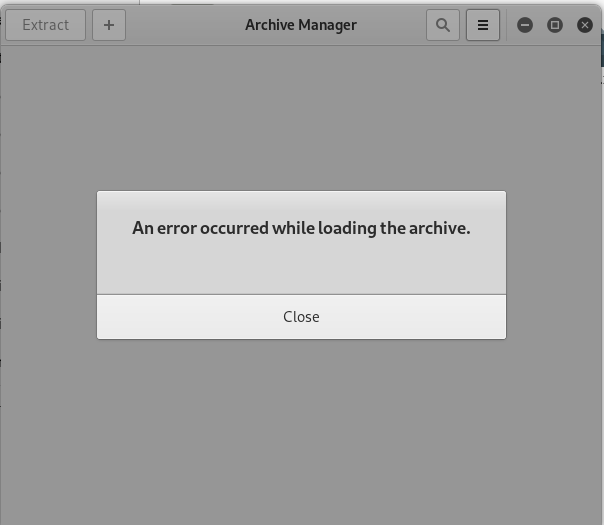
Direccion: **626 Jungle Ave Apt 2**

Ahora procederemos ha analizar el Scheduled Visits.exe, para ello miramos sus metadatos como antes



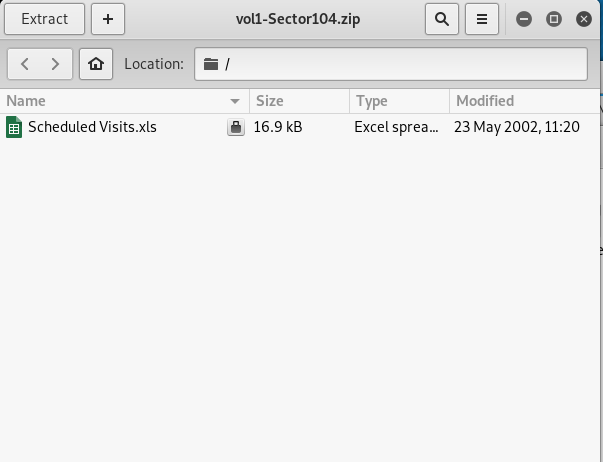
Con esto nos indica que ocupa 100 bits y los sectores 104 y 105, parece que no hay discrepancias, asique repetimos el proceso y buscamos los datos en dichos sectores y lo descargamos.

Para nuestra sorpresa el archivo esta corrupto



Lo que puede indicar que el tamaño de dicho archivo sea mas grande que el indicado en los metadatos por lo que iremos probando añadiendo 1 sector cada vez hasta que se abra o nos cansemos.

En nuestro caso probando nos ha salido que el fichero Ocupaba realmente 6 sectores pero al fin lo hemos podido abrir.



Vemos que contiene un fichero xls, pero el zip esta comprimido con contraseña por tanto nos es imposible acceder al fichero.

Para intentar abrir el fichero vamos ha revisrar los datos que ya tenemos en busca de pistas sobre la contraseña.

Leyendo los contenidos del documento encontramos una buena pista sobre donde encontrar la contraseña, en nuestro caso nos indica esto.



Asique volvemos ha analizar la imagen que es el otro archivo disponible al que hace referencia el mensaje

Pero no podemos encontrar nada ninguna pista en la imagen salvo 1 detalle que es interesante, al final del fichero de imagen encontramos unos extraños símbolos sin sentido ﻿

“(…” que podría indicar que alguien ha aumentado el tamaño de la imagen intencionadamente por lo que añadimos un sector extra a la imagen y procedemos ha analizar el final del fichero por si hay información.

Esto nos muestra una frase bastante interesante



Pw podría indicar password (contraseña) para el zip pero el archivo podría contener mas información asique seguimos examinando el fichero y encontramos otra evidencia interesante



Una clara referencia al fichero que intentamos abrir por tanto podemos tener cierta certeza que la frase anterior pw=goodtimes puede ser la contraseña que andamos buscando.

Probamos la contraseña y funciona por tanto podemos ver los contenidos del fichero.



Esto parece ser un intinerario de algún tipo que indica que el sospechoso podría estar frequentaqndo los siguientes institutos:

A -Smith Hill High School

B- Key High School

C- Leet High School

D – Birard High School

E- Richer Hight School

F – Hull High Scholl

Con toda esta informacion concluye el informe y las preguntas de la practica