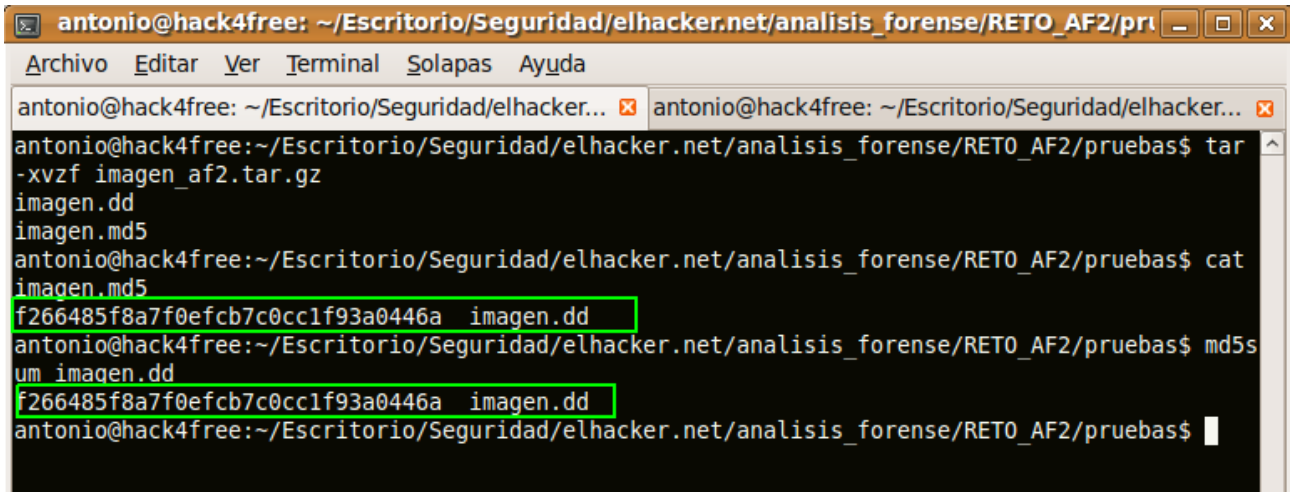
Mini-Guía
Solución 2º reto Análisis Forense

elhacker.net

Kamsky
adonis28850@elhacker.net

Vamos a analizar sin entrar en demasiado detalle, cuales eran las tretas y métodos usados para ocultar la información que se pedía.

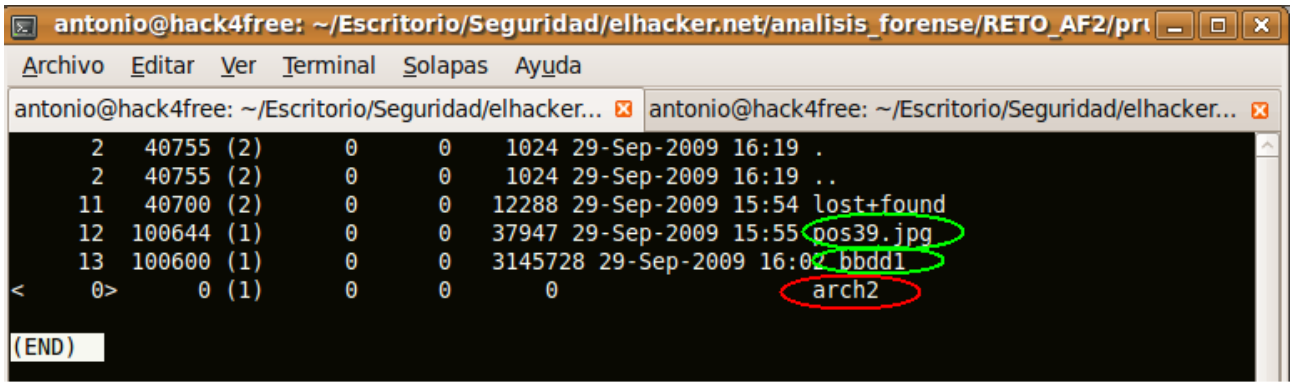
Lo primero que hacemos es descomprimir el zip y comparar que coinciden los checksum:



A continuación procederemos a ver que hay dentro de este sistema de ficheros, no hace falta montarlo, por ejemplo con *debugfs* podemos averiguarlo fácilmente con el siguiente comando:

 # debugfs -w imagen.dd

Y una vez dentro, haciendo un simple *ls -ld*:

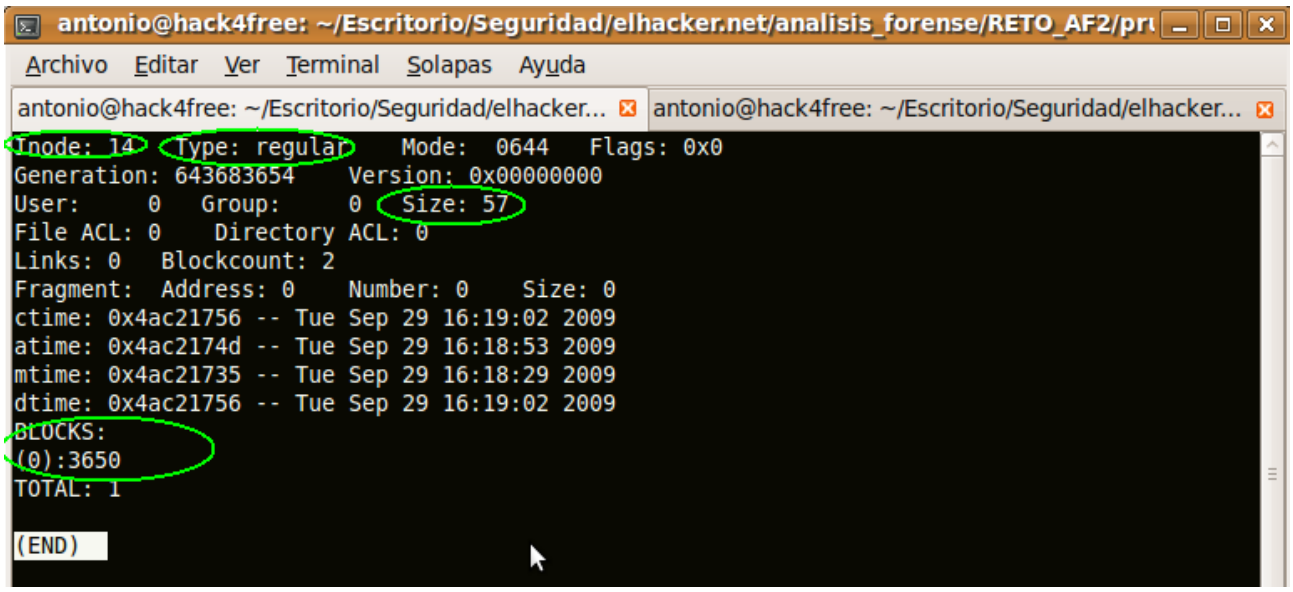


Observamos varias cosas:

- Hay un archivo que en primera instancia parece una imagen jpg
- Un archivo que por el nombre parece una base de datos
- Un fichero que ha sido borrado y que procederemos a rescatar

Si nos fijamos, el número de i-nodos va en orden: 11, 12, 13,...

Seguramente el archivo borrado estuviese linkado con el i-nodo 14, así que probemos a listar la información de este i-nodo, de nuevo con ayuda de debugfs:



Se ve que estábamos en lo cierto, el i-nodo nos indica que este archivo, si no ha sido sobreescrito, se encuentra en el bloque 3650.

Con toda esta información que hemos recopilado, y con ayuda del mismo *debugfs* podemos recuperar los archivos, inclusive el borrado, os dejo de vuestra mano que investiguéis como se lleva esto a cabo.

Una vez que tenemos los 3 archivos en nuestra carpeta de trabajo, echémosle un vistazo por orden.

- El archivo borrado, contiene la siguiente frase:

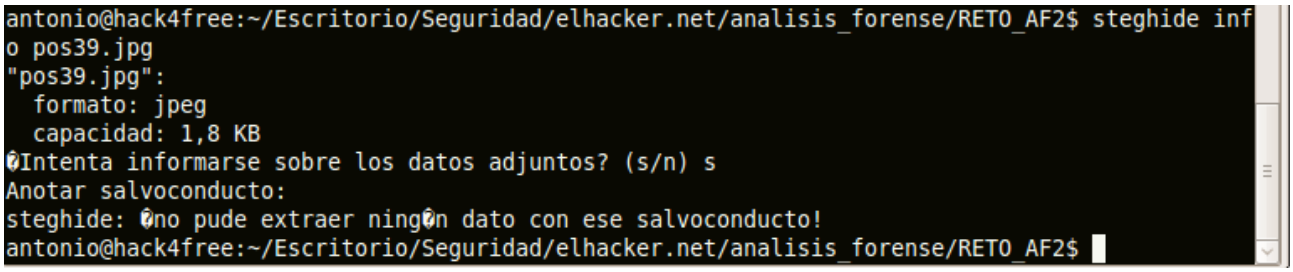
  "Hay que ser precavido y Encriptar las cosas de Verdad..."

  Como bien indicaron en el foro, si pensamos un poco y le buscamos las vueltas, esto probablemente indique que en algún momento dado, se ha utilizado TrueCrypt, así que nos lo apuntamos por si más adelante nos pudiera ser de utilidad.

- El siguiente archivo es una imagen, más en concreto un problema de ajedrez.

  Lo más probable es que esta esconda algo, mediante técnicas de Steganografía.

  Vamos a intentar ver que pasa si usamos uno de los programas más conocidos bajo linux para estos menesteres.



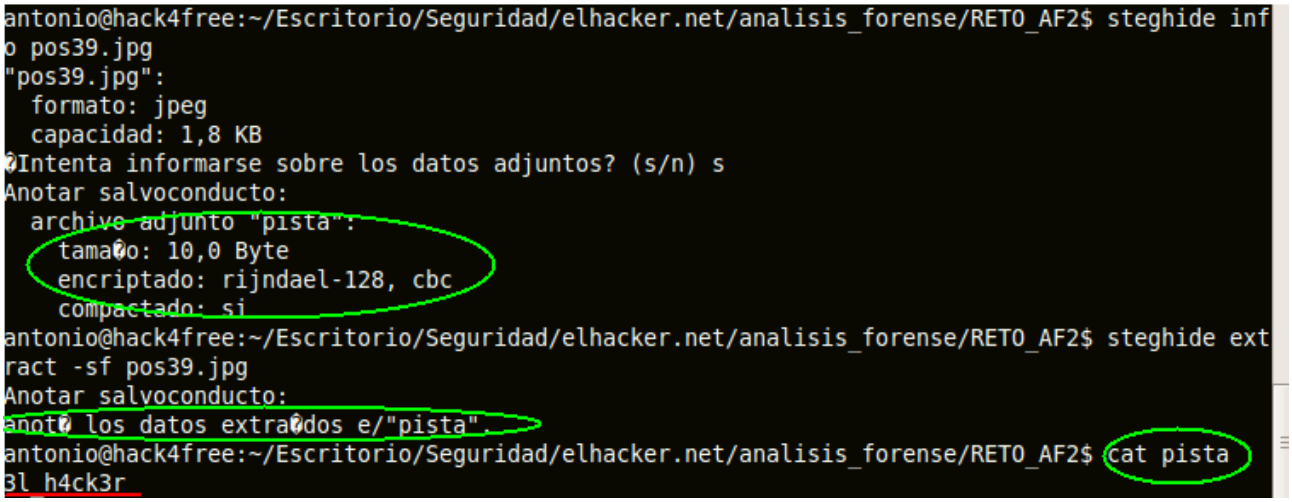
Vemos que nos pide un salvoconducto, introducimos uno cualquiera y nos dice que naranjas de la china...

Pero claro, no iba a ser tan fácil, no?. Si pensamos un poco, la imagen es un problema de ajedrez, si hacemos una búsqueda del nombre del archivo tal cual, podemos llegar fácilmente a la

página de donde ha sido sacado, y en la que si buscamos un poco, encontraremos la solución al problema de ajedrez (Dxc4, muy bonita por cierto), en caso de que no lo encontrásemos tenemos 2 opciones:

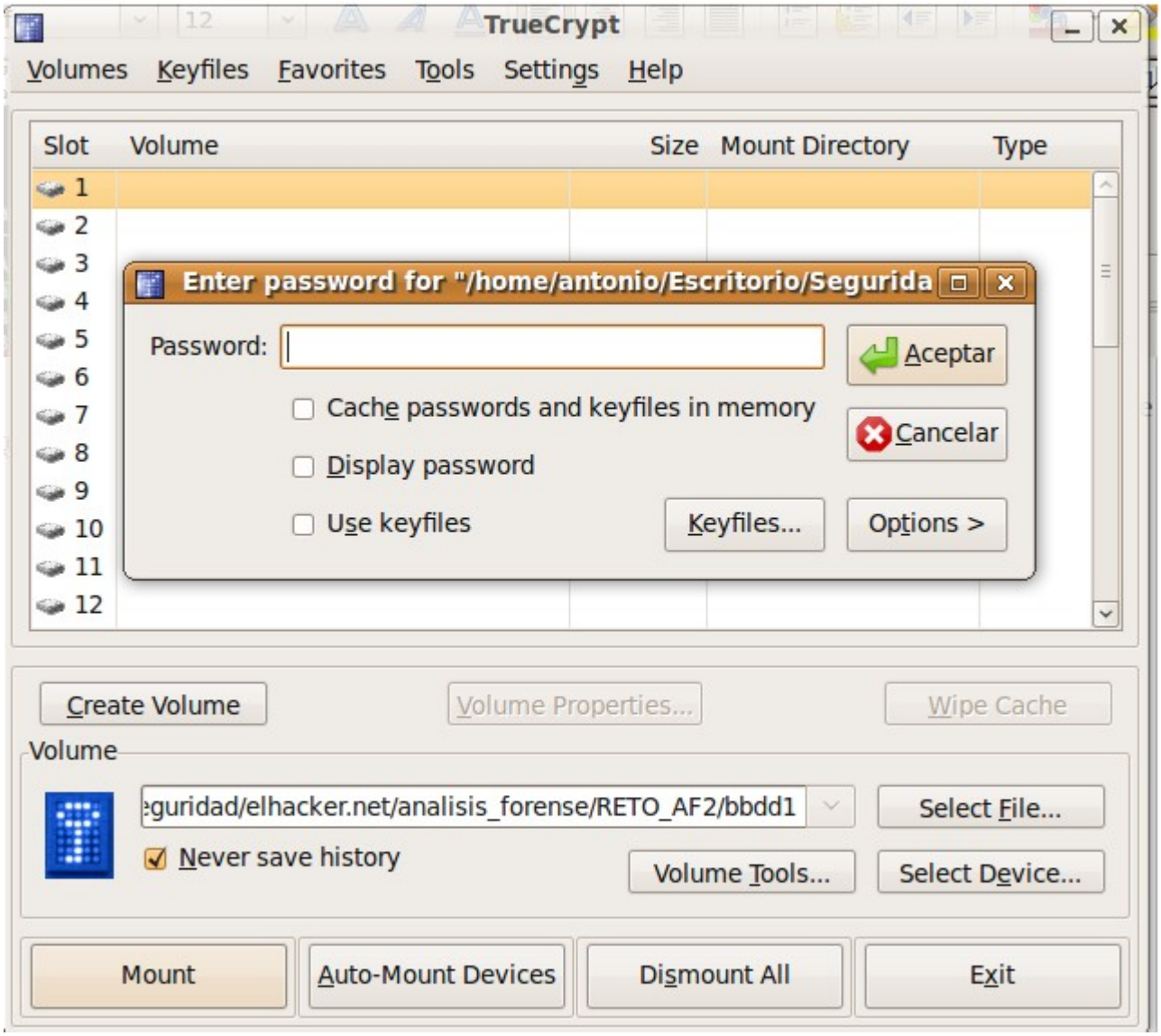
- Resolverlo nosotros mismos
- Usar un motor de ajedrez, que en un periquete nos dirá la jugada

Probemos ahora con este salvoconducto...



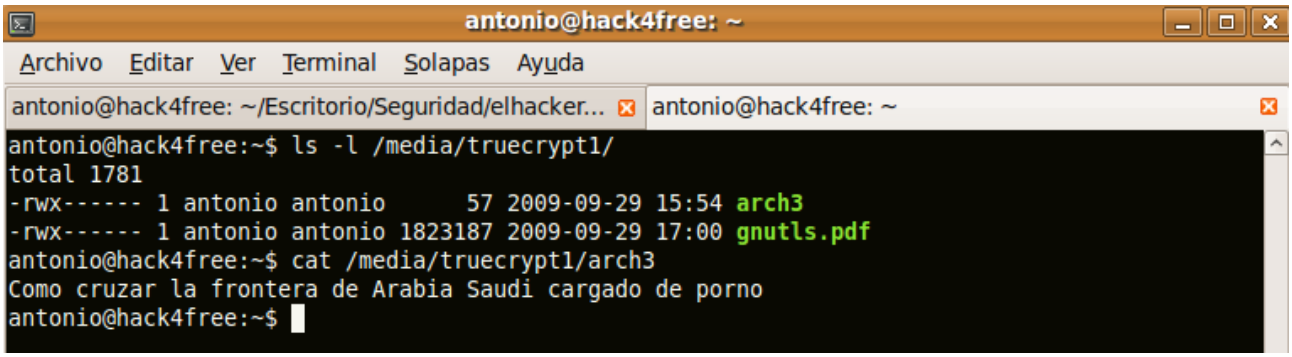
Eureka! Vemos que había escondido un archivo llamado pista, y que contiene una cadena de text: **3l_h4ck3r**

- El tercer archivo, parece un montón de bits sin sentido, si le hacemos un *file*, no nos aporta mucho, así que, si unimos todos los cabos sueltos... seguramente tengamos razón y esto no sea más que un contenedor de un volumen cifrado con TrueCrypt, será la cadena que conseguimos antes la contraseña para abrir este volumen?
  Comprobémoslo:



Si introducimos el archivo con nombre bbdd1, y ponemos la cadena, vemos que así es!

Ahora bien, si vamos al volumen recién montado, nos encontramos con lo siguiente:



- Un PDF con información sobre la librería gnuTLS
- Un archivo de texto con la cadena que se observa en pantalla

La cadena es, cuanto menos, sugerente! Pero en un principio no nos dice nada útil, o sí?
Probemos a introducir esa cadena en google, a ver que se cuenta...

Después de buscar un rato, encontramos el siguiente enlace:

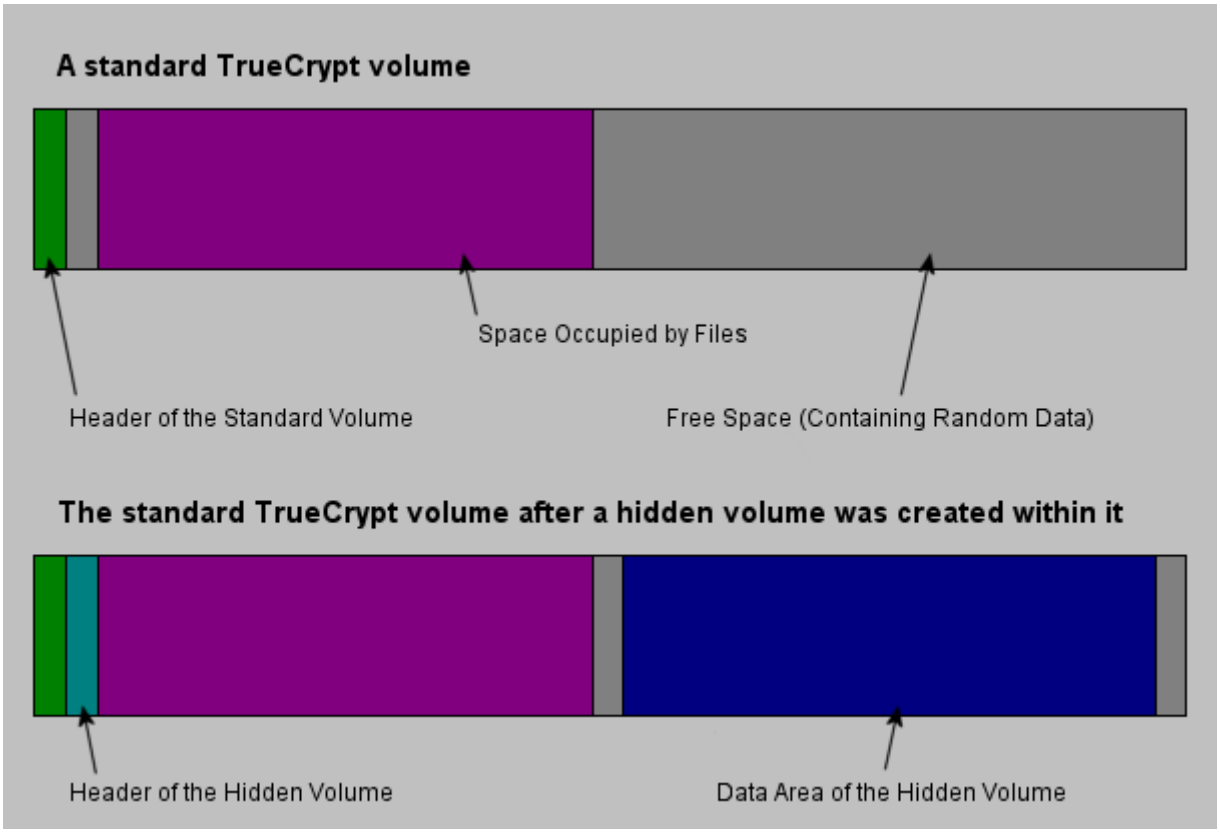
http://www.securitybydefault.com/2008/12/como-cruzar-la-frontera-de-arabia-saudi.html

Donde se nos indica paso por paso como meter porno en un PDF! :P
Bromas aparte, se nos muestra una forma de ocultar información en un PDF, y... casualidades de la vida, el otro archivo que aparece en el volumen recién montado es un PDF, así que si seguimos paso por paso el post, nos encontramos como resultado con un nuevo archivo, que contiene en su interior la siguiente cadena:

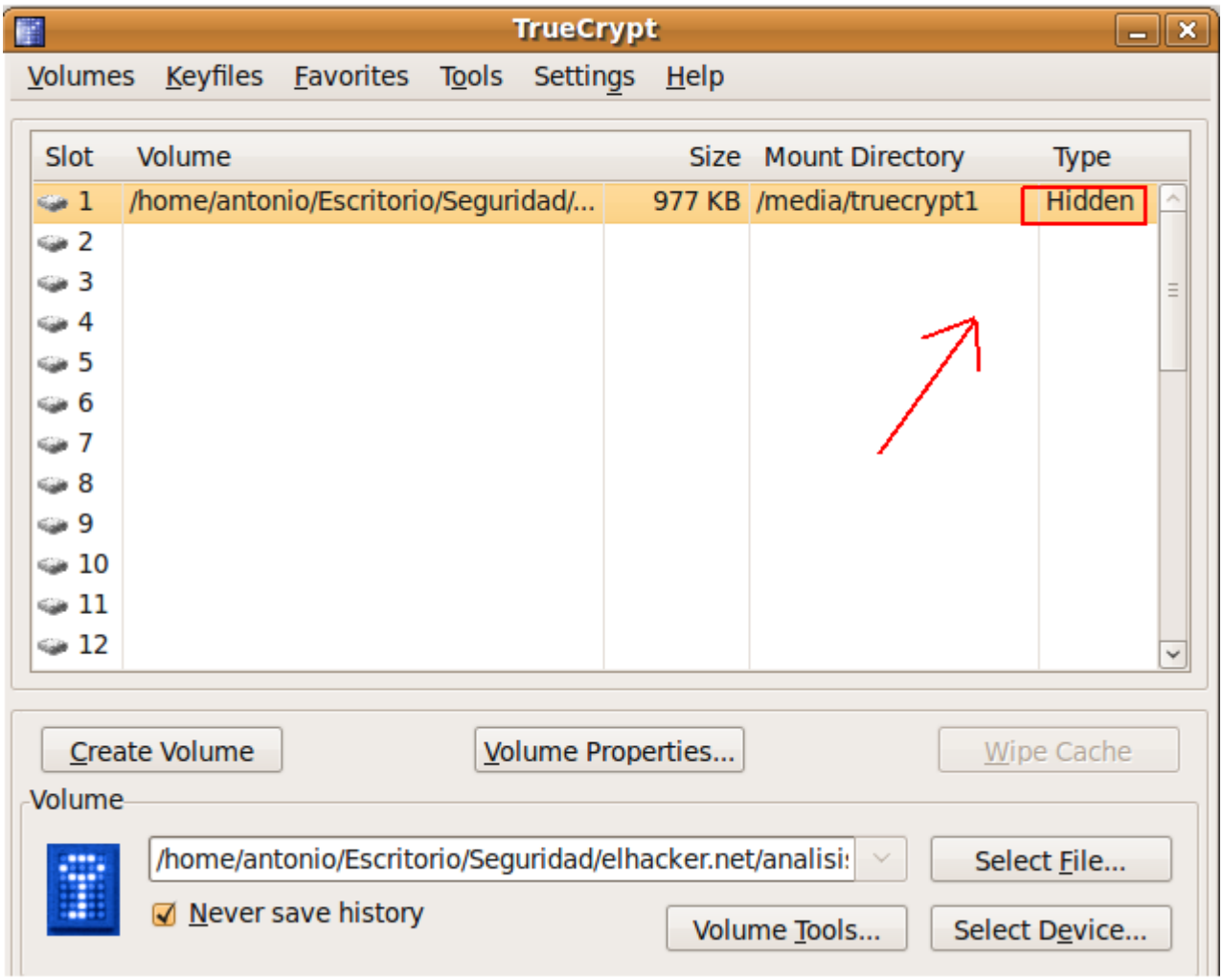
p7890as&yu

Y esto ahora que es lo que es!!?? Si ya no hay más imágenes donde ocultar información, ni archivos borrados (se puede comprobar por ejemplo con debugfs, foremost, etc...), ni contenedores donde guardar volúmenes con TrueCrypt!, o si... ?¿

TrueCrypt nos permite crear un tipo especial de volúmenes, que realmente son iguales que el que hemos visto, pero con una pequeña peculiaridad, está oculto!
De forma que la gente puede pensar que ha conseguido recuperar la información de turno que estuviese encriptada, pero en realidad ha caído en la trampa del atacante y ha encontrado lo que el quisiese que encontrase.
Para ver como funciona someramente, podemos observar la siguiente imagen:



Así que una vez entendido su funcionamiento, probemos a usar de nuevo TrueCrypt con bbdd1, pero esta vez introduzcamos este último string descubierto:



Parece que hubo suerte!

Como se observa en la imagen, este volumen es del tipo hidden, y si lo abrimos nos encontramos finalmente con: