

**SPRING 21**

**UNIDAD 2**

**EJERCICIO\_1**

**ANALISIS FORENSE**

**RECUPERACION DE IMAGENES**

**FTK\_IMAGER**

**-- EJERCICIO\_1.-** Para esta actividad lo que debes realizar es la ***recuperación de cinco imágenes*** que se encuentran dentro de la copia de disco. Para ello, se ha hecho uso de las siguientes herramientas:

**-- FTK\_IMAGER.-** herramienta forense digital gratuita que permite crear imágenes exactas de discos duros, unidades USB y otros medios de almacenamiento, realizando copias completas y exactas (bit a bit) del dispositivo, útiles para investigaciones sin alterar los datos originales, permitiendo visualizar y analizar archivos eliminados y datos sin procesar en el dispositivo.

**-- FASE DE ANALISIS:**

1. Se ha precedido a la **verificación** de la evidencia digital, siendo **hasheada** mediante algoritmos de encriptación **MD5 y SHA1** Hash, permitiendo crear una relación biunívoca entre el hash y la evidencia, consiguiendo mantener la **integridad de los datos** y conservar la **cadena de custodia** de la imagen evidencial en **toda la fase de investigación.**

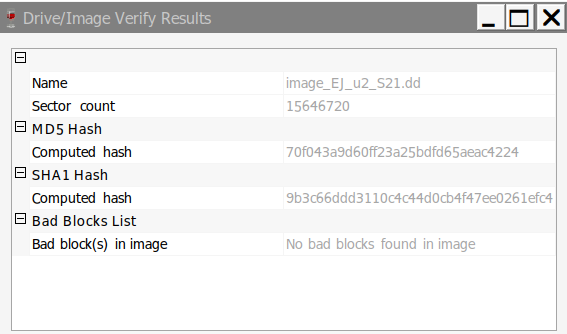


Imagen 1.- resultado del proceso de verificación hecho por el programa

1. La estructura en árbol del disco analizado, muestra una partición con 7639 MB, con varias carpetas, teniendo algunas de ellas archivos en su interior, existiendo una carpeta llamada **501** que se encuentra en la **papelera de reciclaje:**

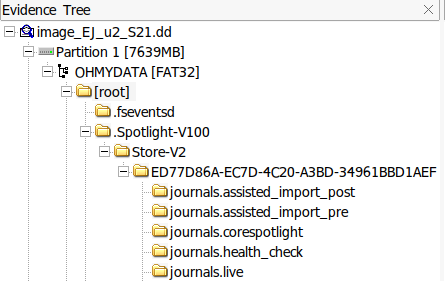
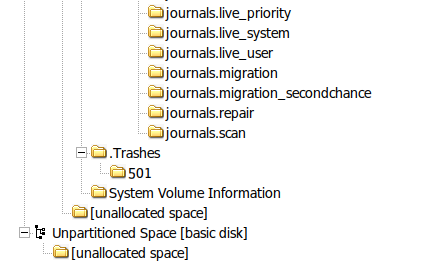
 

Imagen 2.- Árbol de evidencias del disco analizado al completo

1. En la zona inicial del árbol de la evidencia, encontramos la carpeta “root”, la cual contiene muchas de las carpetas del disco, pero centrando el análisis en el objetivo de este ejercicio, observamos:

- 10 archivos de imagen en formato .jpg y .jpeg[[1]](#footnote-0), de las cuales, 8 se encuentran eliminadas del disco

- 2 archivos de música en formato .mp3[[2]](#footnote-1)

- 2 archivos de vídeo en formato .mp4[[3]](#footnote-2)

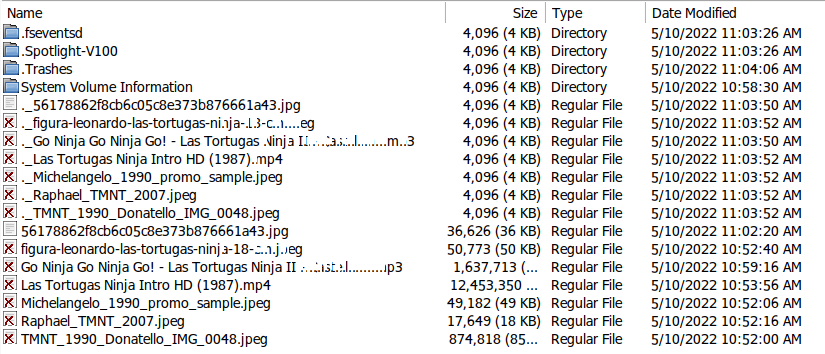


Imagen 3.- Archivos existentes en la raíz del directorio “root”

1. El resto de carpetas contiene archivos de otros tipos, no requeridos en este ejercicio, excepto en una carpeta que se encuentra en la papelera de reciclaje con el nombre **“501”** la cual contiene archivos con los ***mismos nombres, pesos y horas de modificación*** que los encontrados eliminados en la carpeta **“root”:**

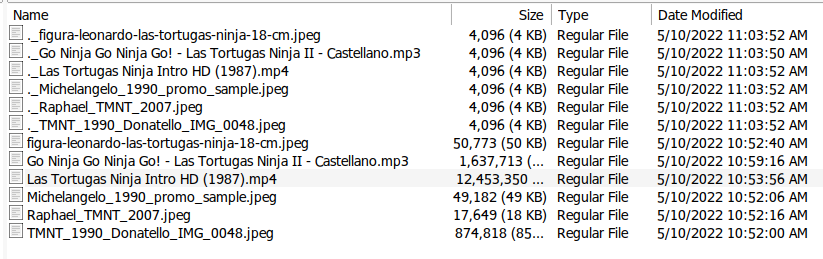


Imagen 4.- Contenido de la carpeta 501 hallada en la papelera de reciclaje

1. Se procede a la extracción de todos los archivos para su estudio, llegando a las siguientes consideraciones:

**- DIRECTORIO ROOT:**

* De las 14 imágenes extraídas del disco evidencial, unicamente se ha podido recuperar 7, pudiendo verse solo ***56178862f8cb6c05c8e373b876661a43.jpg***, la cual al darle click encima de la imagen apertura un script llamado ***“image magic”*** con funciones de apertura de imágenes y modificaciones, siendo probado con algunas de las imágenes del la carpeta root, siendo infructuoso, saliendo un mensaje de error:

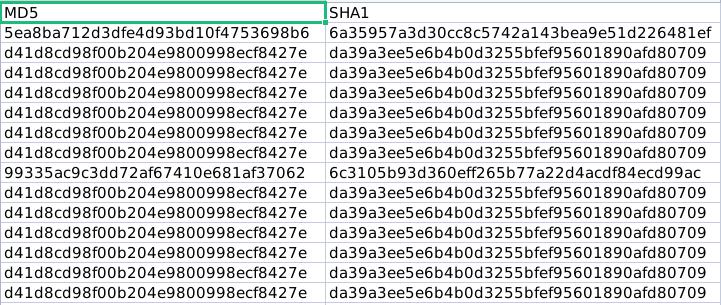
Imagen 5.- Hashes de los 14 archivos extraídos del directorio “root”



Imagen 6.- rutas de origen de cada uno de los archivos del directorio root



Imagen 7.- Los 7 archivos extraídos realmente a la Kali y el script del maestro astilla



Imagen 8.- Respuesta del script del maestro astilla al intentar aperturar una imagen de la carpeta root.

**-- DIRECTORIO “501”:**

* De las 12 archivos extraída del disco evidencial, unicamente se han podido recuperar **4 archivos de imagen**, siendo todas de la saga de las ***“Tortugas Ninjas”***, concretamente Leonardo, Raphael, Michelangelo y Donatello.

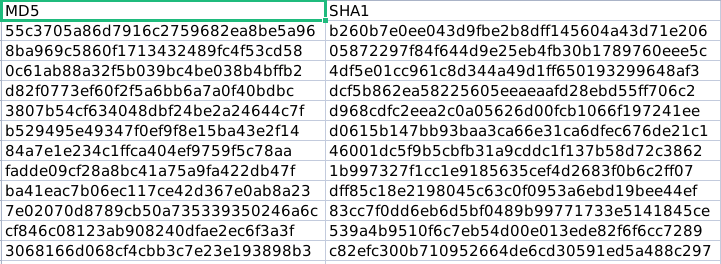
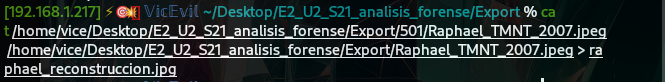
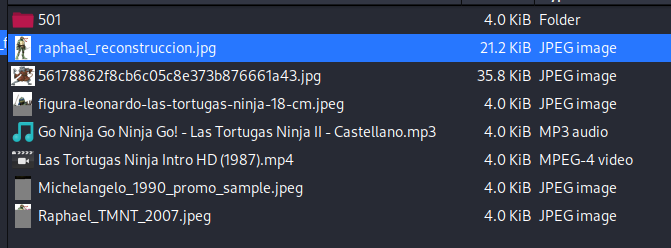


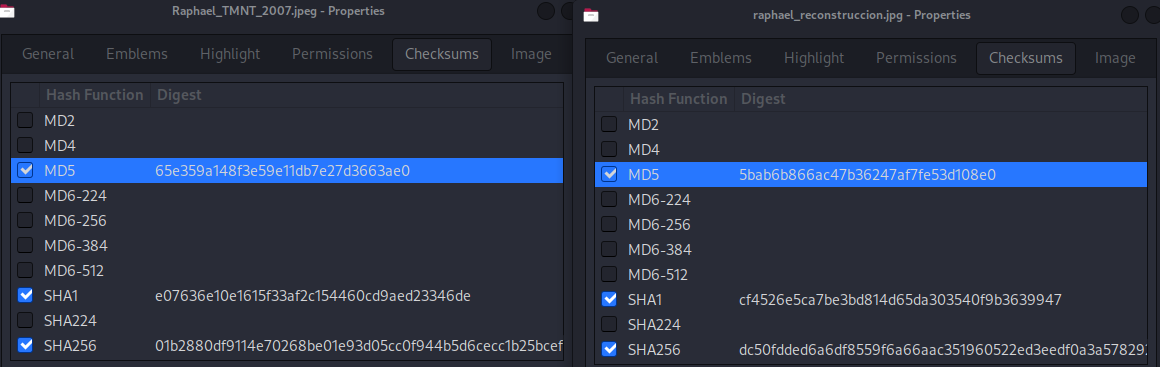
Imagen 9.- Hashes de los 12 archivos extraídos del directorio “501”



Imagen 10.- rutas de origen de cada uno de los archivos del directorio “501”

* Usando la función de concatenación de archivos del comando cat, ya que tenemos fragmentos de la misma fotografía, se procede a concatenar dos trozos de la misma fotografío resultando las reconstrucciones de:
* Con el archivo de imagen “Raphael\_TMNT\_2007.jpeg” del directorio root, existiendo datos válidos unicamente la parte superior, mas el archivo de la carpeta “501”, que si aparece completa con el mismo nombre, ***reconstruimos una nueva fotografía*** con la imagen completa de “Raphael”:

Imagen 11.- Comando “cat” concatenando 2 fotografías para su reconstrucción

Imagen 12.- Comparación de hashes entre la original de Raphael y la reconstrucción -> imágenes diferentes

* Con el archivo de imagen ***“figura leonardo las tortugas ninja 18cm”*** del directorio *root*, existiendo datos válidos unicamente la parte superior de la imagen, mas el archivo de la carpeta *“501”*, que si aparece completo con el mismo nombre, ***reconstruimos una nueva fotografía*** con la imagen completa de ***“Leonardo”***:

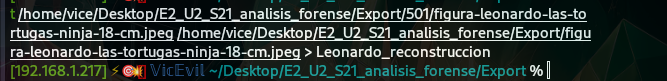


Imagen 13.- Comando “cat” concatenando 2 fotografías para su reconstrucción

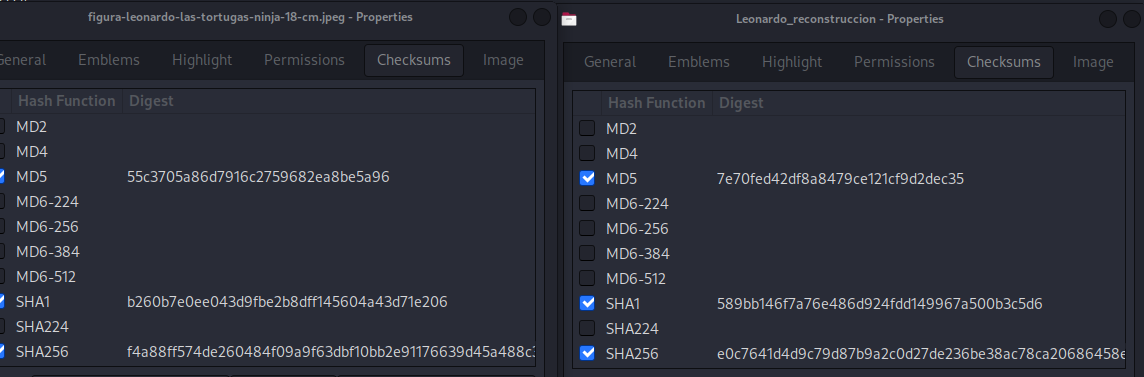
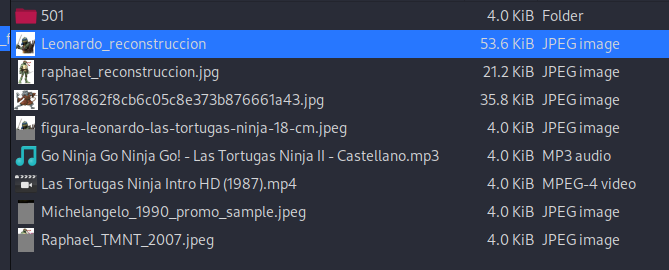


Imagen 14.- Comparación de hashes entre la original de Leonardo y la reconstrucción -> imágenes diferentes

**-- CONCLUSIONES:**

- Se ha extraído un total de **4 archivos de imagen** integras y totalmente validas de la carpeta “501” correspondiendo a las imágenes de Leonardo, Raphael, Michelangelo y Donatello.

- Posteriormente mediante la técnica de la concatenación de archivos de la misma fotografía se han realizado una reconstrucción de **2 archivos de imagen**: Leonardo y Raphael, que aunque a nivel visual sean la misma fotografía, se ha demostrado que tienen hashes diferentes, por lo que son diferentes fotografías.

1. Extensiones de archivo para el mismo formato de imagen: JPEG (***Joint Photographic Experts Group***), siendo usados, indistintamente, para imágenes comprimidas con pérdida de calidad para reducir el tamaño del archivo, haciéndolos ideales para fotografías y uso en la web [↑](#footnote-ref-0)
2. formato de archivo de audio comprimido que utiliza compresión con pérdida para reducir el tamaño del archivo, manteniendo una calidad de sonido aceptabl. [↑](#footnote-ref-1)
3. Es popular por su alta calidad y compresión eficiente, lo que lo hace ideal para transmisión en línea y almacenamiento en dispositivos con espacio limitado. [↑](#footnote-ref-2)