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.**

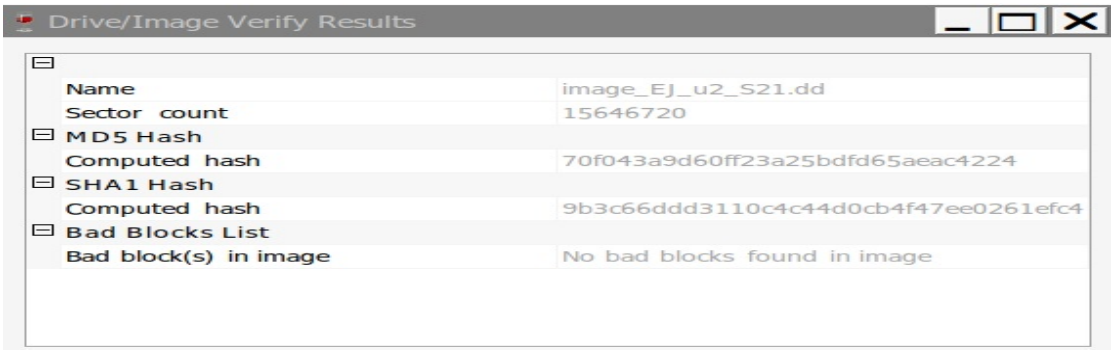


Imagen 1.- resultado del proceso de verificación hecho por el programa

2. 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:**

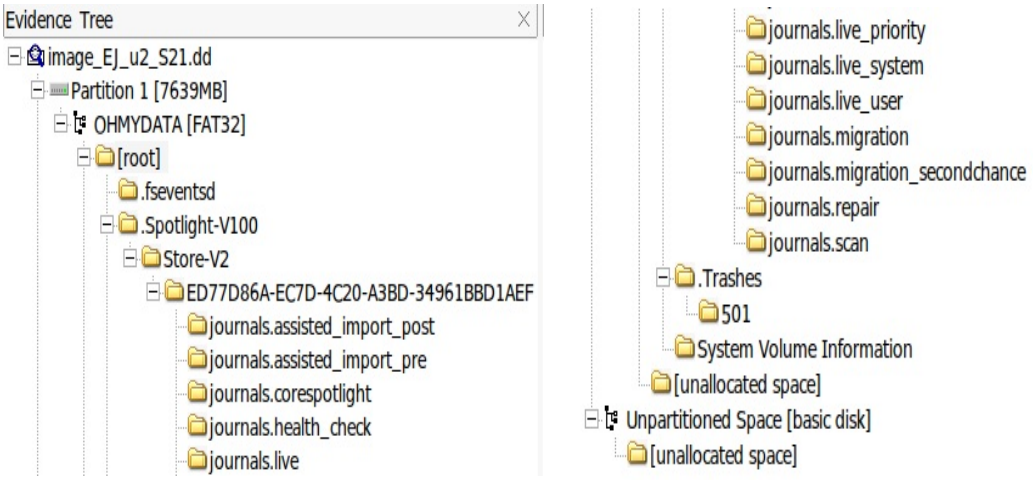
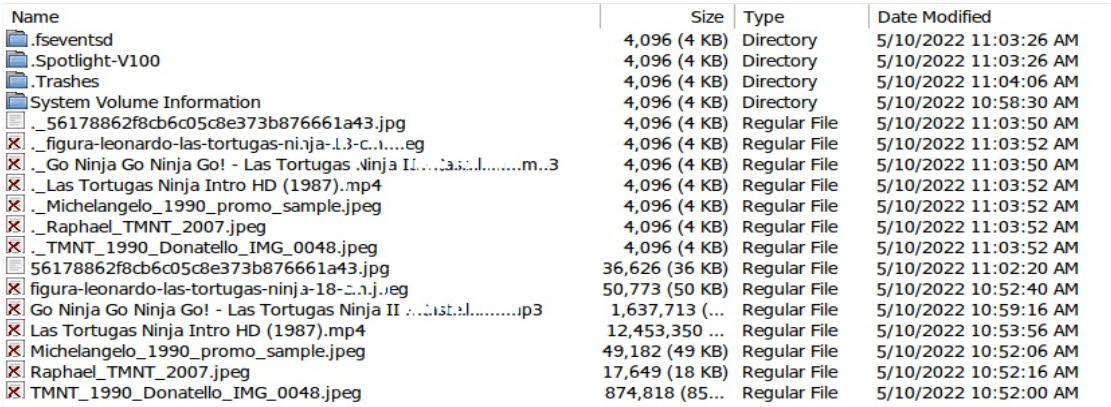


Imagen 2.- Árbol de evidencias del disco analizado al completo

3. 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:

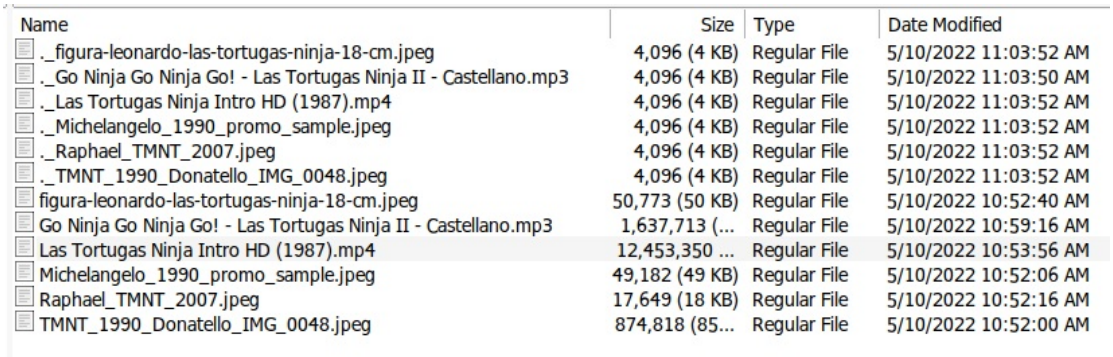
   - 10 archivos de imagen en formato .jpg y .jpeg[1], de las cuales, 8 se encuentran eliminadas del disco
   - 2 archivos de música en formato .mp3[2]
   - 2 archivos de vídeo en formato .mp4[3]



Name	Size	Type	Date Modified
.fseventsd	4,096 (4 KB)	Directory	5/10/2022 11:03:26 AM
.Spotlight-V100	4,096 (4 KB)	Directory	5/10/2022 11:03:26 AM
.Trashes	4,096 (4 KB)	Directory	5/10/2022 11:04:06 AM
System Volume Information	4,096 (4 KB)	Directory	5/10/2022 10:58:30 AM
._56178862f8cb6c05c8e373b876661a43.jpg	4,096 (4 KB)	Regular File	5/10/2022 11:03:50 AM
._figura-leonardo-las-tortugas-ni.ja-1.3-c..1....eg	4,096 (4 KB)	Regular File	5/10/2022 11:03:52 AM
._Go Ninja Go Ninja Go! - Las Tortugas .Ninja I.....a.....m..3	4,096 (4 KB)	Regular File	5/10/2022 11:03:50 AM
._Las Tortugas Ninja Intro HD (1987).mp4	4,096 (4 KB)	Regular File	5/10/2022 11:03:52 AM
._Michelangelo_1990_promo_sample.jpeg	4,096 (4 KB)	Regular File	5/10/2022 11:03:52 AM
._Raphael_TMNT_2007.jpeg	4,096 (4 KB)	Regular File	5/10/2022 11:03:52 AM
._TMNT_1990_Donatello_IMG_0048.jpeg	4,096 (4 KB)	Regular File	5/10/2022 11:03:52 AM
56178862f8cb6c05c8e373b876661a43.jpg	36,626 (36 KB)	Regular File	5/10/2022 11:02:20 AM
figura-leonardo-las-tortugas-ninja-18-..n.j..eg	50,773 (50 KB)	Regular File	5/10/2022 10:52:40 AM
Go Ninja Go Ninja Go! - Las Tortugas Ninja II ..a.....p3	1,637,713 (...	Regular File	5/10/2022 10:59:16 AM
Las Tortugas Ninja Intro HD (1987).mp4	12,453,350 ...	Regular File	5/10/2022 10:53:56 AM
Michelangelo_1990_promo_sample.jpeg	49,182 (49 KB)	Regular File	5/10/2022 10:52:06 AM
Raphael_TMNT_2007.jpeg	17,649 (18 KB)	Regular File	5/10/2022 10:52:16 AM
TMNT_1990_Donatello_IMG_0048.jpeg	874,818 (85...	Regular File	5/10/2022 10:52:00 AM

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

4. 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”:**



Name	Size	Type	Date Modified
._figura-leonardo-las-tortugas-ninja-18-cm.jpeg	4,096 (4 KB)	Regular File	5/10/2022 11:03:52 AM
._Go Ninja Go Ninja Go! - Las Tortugas Ninja II - Castellano.mp3	4,096 (4 KB)	Regular File	5/10/2022 11:03:50 AM
._Las Tortugas Ninja Intro HD (1987).mp4	4,096 (4 KB)	Regular File	5/10/2022 11:03:52 AM
._Michelangelo_1990_promo_sample.jpeg	4,096 (4 KB)	Regular File	5/10/2022 11:03:52 AM
._Raphael_TMNT_2007.jpeg	4,096 (4 KB)	Regular File	5/10/2022 11:03:52 AM
._TMNT_1990_Donatello_IMG_0048.jpeg	4,096 (4 KB)	Regular File	5/10/2022 11:03:52 AM
figura-leonardo-las-tortugas-ninja-18-cm.jpeg	50,773 (50 KB)	Regular File	5/10/2022 10:52:40 AM
Go Ninja Go Ninja Go! - Las Tortugas Ninja II - Castellano.mp3	1,637,713 (...	Regular File	5/10/2022 10:59:16 AM
Las Tortugas Ninja Intro HD (1987).mp4	12,453,350 ...	Regular File	5/10/2022 10:53:56 AM
Michelangelo_1990_promo_sample.jpeg	49,182 (49 KB)	Regular File	5/10/2022 10:52:06 AM
Raphael_TMNT_2007.jpeg	17,649 (18 KB)	Regular File	5/10/2022 10:52:16 AM
TMNT_1990_Donatello_IMG_0048.jpeg	874,818 (85...	Regular File	5/10/2022 10:52:00 AM

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

---

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

2 formato de archivo de audio comprimido que utiliza compresión con pérdida para reducir el tamaño del archivo, manteniendo una calidad de sonido aceptabl.

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.

5. 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:

MD5	SHA1
5ea8ba712d3dfe4d93bd10f4753698b6	6a35957a3d30cc8c5742a143bea9e51d226481ef
d41d8cd98f00b204e9800998ecf8427e	da39a3ee5e6b4b0d3255bfef95601890afd80709
d41d8cd98f00b204e9800998ecf8427e	da39a3ee5e6b4b0d3255bfef95601890afd80709
d41d8cd98f00b204e9800998ecf8427e	da39a3ee5e6b4b0d3255bfef95601890afd80709
d41d8cd98f00b204e9800998ecf8427e	da39a3ee5e6b4b0d3255bfef95601890afd80709
d41d8cd98f00b204e9800998ecf8427e	da39a3ee5e6b4b0d3255bfef95601890afd80709
d41d8cd98f00b204e9800998ecf8427e	da39a3ee5e6b4b0d3255bfef95601890afd80709
99335ac9c3dd72af67410e681af37062	6c3105b93d360eff265b77a22d4acdf84ecd99ac
d41d8cd98f00b204e9800998ecf8427e	da39a3ee5e6b4b0d3255bfef95601890afd80709
d41d8cd98f00b204e9800998ecf8427e	da39a3ee5e6b4b0d3255bfef95601890afd80709
d41d8cd98f00b204e9800998ecf8427e	da39a3ee5e6b4b0d3255bfef95601890afd80709
d41d8cd98f00b204e9800998ecf8427e	da39a3ee5e6b4b0d3255bfef95601890afd80709
d41d8cd98f00b204e9800998ecf8427e	da39a3ee5e6b4b0d3255bfef95601890afd80709
d41d8cd98f00b204e9800998ecf8427e	da39a3ee5e6b4b0d3255bfef95601890afd80709

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

FileNames
image_EJ_u2_S21.dd\Partition 1 [7639MB]\OHMYDATA [FAT32]\[root]\._56178862f8cb6c05c8e373b876661a43.jpg
image_EJ_u2_S21.dd\Partition 1 [7639MB]\OHMYDATA [FAT32]\[root]\._figura-leonardo-las-tortugas-ninja-18-cm.jpeg
image_EJ_u2_S21.dd\Partition 1 [7639MB]\OHMYDATA [FAT32]\[root]\._Go Ninja Go Ninja Go! - Las Tortugas Ninja II - Castellano.mp3
image_EJ_u2_S21.dd\Partition 1 [7639MB]\OHMYDATA [FAT32]\[root]\._Las Tortugas Ninja Intro HD (1987).mp4
image_EJ_u2_S21.dd\Partition 1 [7639MB]\OHMYDATA [FAT32]\[root]\._Michelangelo_1990_promo_sample.jpeg
image_EJ_u2_S21.dd\Partition 1 [7639MB]\OHMYDATA [FAT32]\[root]\._Raphael_TMNT_2007.jpeg
image_EJ_u2_S21.dd\Partition 1 [7639MB]\OHMYDATA [FAT32]\[root]\._TMNT_1990_Donatello_IMG_0048.jpeg
image_EJ_u2_S21.dd\Partition 1 [7639MB]\OHMYDATA [FAT32]\[root]\56178862f8cb6c05c8e373b876661a43.jpg
image_EJ_u2_S21.dd\Partition 1 [7639MB]\OHMYDATA [FAT32]\[root]\figura-leonardo-las-tortugas-ninja-18-cm.jpeg
image_EJ_u2_S21.dd\Partition 1 [7639MB]\OHMYDATA [FAT32]\[root]\Go Ninja Go Ninja Go! - Las Tortugas Ninja II - Castellano.mp3
image_EJ_u2_S21.dd\Partition 1 [7639MB]\OHMYDATA [FAT32]\[root]\Las Tortugas Ninja Intro HD (1987).mp4
image_EJ_u2_S21.dd\Partition 1 [7639MB]\OHMYDATA [FAT32]\[root]\Michelangelo_1990_promo_sample.jpeg
image_EJ_u2_S21.dd\Partition 1 [7639MB]\OHMYDATA [FAT32]\[root]\Raphael_TMNT_2007.jpeg
image_EJ_u2_S21.dd\Partition 1 [7639MB]\OHMYDATA [FAT32]\[root]\TMNT_1990_Donatello_IMG_0048.jpeg

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

otros
501
root_hash.csv
Leonardo_reconstruccion
raphael_reconstruccion.jpg
56178862f8cb6c05c8e373b876661a43.jpg
figura-leonardo-las-tortugas-ninja-18-cm.jpeg
Go Ninja Go Ninja Go! - Las Tortugas Ninja II - Castellano.mp3
Las Tortugas Ninja Intro HD (1987).mp4
Michelangelo_1990_promo_sample.jpeg
Raphael_TMNT_2007.jpeg
TMNT_1990_Donatello_IMG_0048.jpeg

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

```
insufficient image data in file `/home/vice/Desktop/E2_U2_S21_analisis_forense/FTK_IMAGER/._figura-leonardo-las-tortugas-ninja-18-cm.jpeg' @ error/jpeg.c/ReadJPEGImage_/1184:
```

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.

MD5	SHA1
55c3705a86d7916c2759682ea8be5a96	b260b7e0ee043d9fbe2b8dff145604a43d71e206
8ba969c5860f1713432489fc4f53cd58	05872297f84f644d9e25eb4fb30b1789760eee5c
0c61ab88a32f5b039bc4be038b4bffb2	4df5e01cc961c8d344a49d1ff650193299648af3
d82f0773ef60f2f5a6bb6a7a0f40bdbc	dcf5b862ea58225605eeaeaafd28ebd55ff706c2
3807b54cf634048dbf24be2a24644c7f	d968cdfc2eea2c0a05626d00fcb1066f197241ee
b529495e49347f0ef9f8e15ba43e2f14	d0615b147bb93baa3ca66e31ca6dfec676de21c1
84a7e1e234c1ffca404ef9759f5c78aa	46001dc5f9b5cbfb31a9cddc1f137b58d72c3862
fadde09cf28a8bc41a75a9fa422db47f	1b997327f1cc1e9185635cef4d2683f0b6c2ff07
ba41eac7b06ec117ce42d367e0ab8a23	dff85c18e2198045c63c0f0953a6ebd19bee44ef
7e02070d8789cb50a735339350246a6c	83cc7f0dd6eb6d5bf0489b99771733e51418 45ce
cf846c08123ab908240dfae2ec6f3a3f	539a4b9510f6c7eb54d00e013ede82f6f6cc7289
3068166d068cf4cbb3c7e23e193898b3	c82efc300b710952664de6cd30591ed5a488c297

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

```
FileNames
image_EJ_u2_S21.dd\Partition 1 [7639MB]\OHMYDATA [FAT32]\[root]\.Trashes\501\figura-leonardo-las-tortugas-ninja-18-cm.jpeg
image_EJ_u2_S21.dd\Partition 1 [7639MB]\OHMYDATA [FAT32]\[root]\.Trashes\501\._figura-leonardo-las-tortugas-ninja-18-cm.jpeg
image_EJ_u2_S21.dd\Partition 1 [7639MB]\OHMYDATA [FAT32]\[root]\.Trashes\501\Go Ninja Go Ninja Go! - Las Tortugas Ninja II - Castellano.mp3
image_EJ_u2_S21.dd\Partition 1 [7639MB]\OHMYDATA [FAT32]\[root]\.Trashes\501\._Go Ninja Go Ninja Go! - Las Tortugas Ninja II - Castellano.mp3
image_EJ_u2_S21.dd\Partition 1 [7639MB]\OHMYDATA [FAT32]\[root]\.Trashes\501\Las Tortugas Ninja Intro HD (1987).mp4
image_EJ_u2_S21.dd\Partition 1 [7639MB]\OHMYDATA [FAT32]\[root]\.Trashes\501\._Las Tortugas Ninja Intro HD (1987).mp4
image_EJ_u2_S21.dd\Partition 1 [7639MB]\OHMYDATA [FAT32]\[root]\.Trashes\501\Michelangelo_1990_promo_sample.jpeg
image_EJ_u2_S21.dd\Partition 1 [7639MB]\OHMYDATA [FAT32]\[root]\.Trashes\501\._Michelangelo_1990_promo_sample.jpeg
image_EJ_u2_S21.dd\Partition 1 [7639MB]\OHMYDATA [FAT32]\[root]\.Trashes\501\Raphael_TMNT_2007.jpeg
image_EJ_u2_S21.dd\Partition 1 [7639MB]\OHMYDATA [FAT32]\[root]\.Trashes\501\._Raphael_TMNT_2007.jpeg
image_EJ_u2_S21.dd\Partition 1 [7639MB]\OHMYDATA [FAT32]\[root]\.Trashes\501\TMNT_1990_Donatello_IMG_0048.jpeg
image_EJ_u2_S21.dd\Partition 1 [7639MB]\OHMYDATA [FAT32]\[root]\.Trashes\501\._TMNT_1990_Donatello_IMG_0048.jpeg
```

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”:

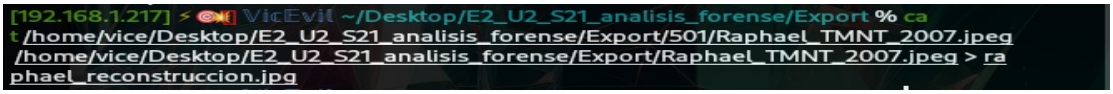


Imagen 11.- Comando “cat” concatenando 2 fotografías para su reconstrucción

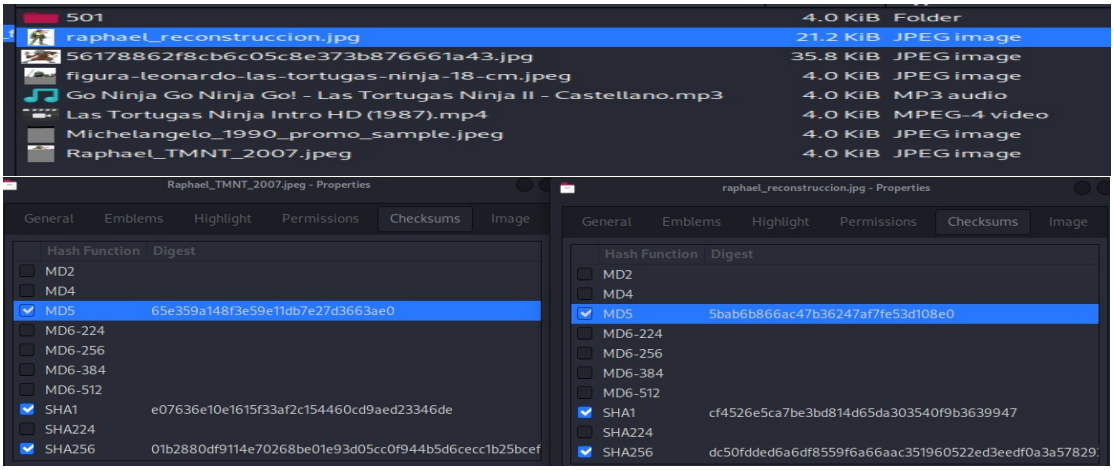


Imagen 12.- Comparación de hashes entre la original de Raphael y la reconstrucción -> imágenes diferentes

- Con el archivo deimagen ***“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”***:

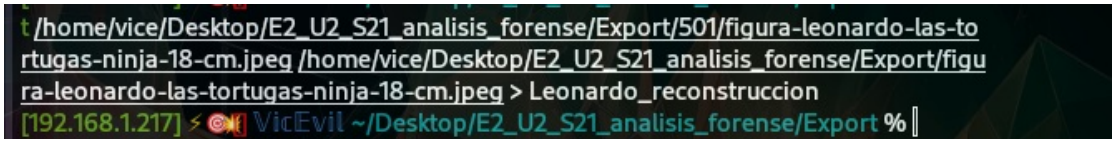


Imagen 13.- Comando “cat” concatenando 2 fotografías para su reconstrucción

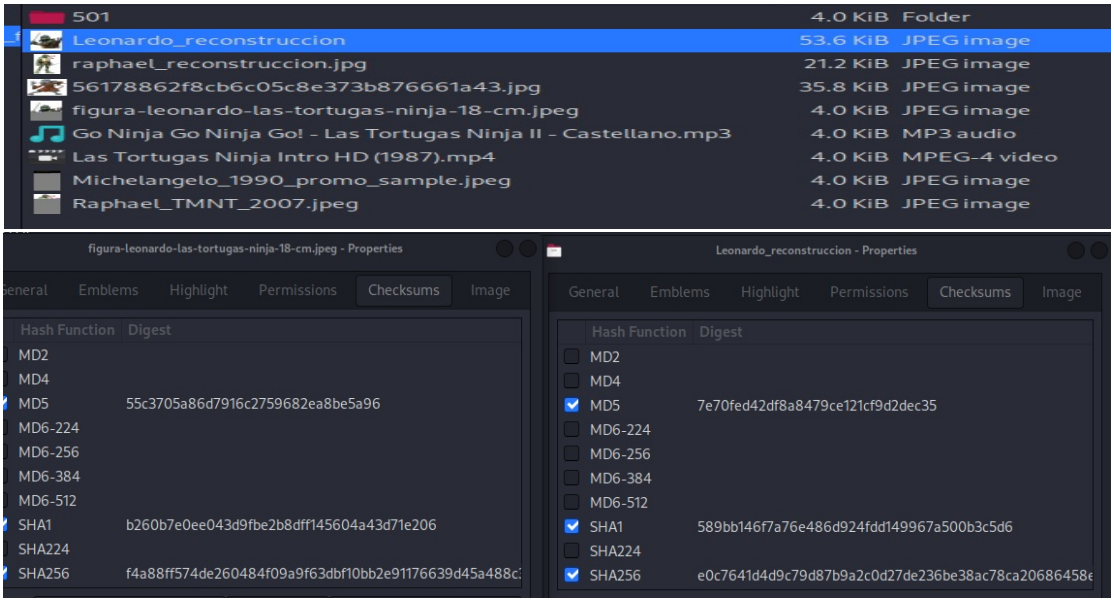


Imagen 14.- Comparación de hashes entre la original de Leonardo y la reconstrucción -> imágenes diferentes

-- 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.