

Asignatura	Datos del alumno	Fecha
Análisis Forense	Apellidos: Paz López	11/06/2022
	Nombre: Angel Ramón	

Actividades

Actividad: Dispositivos de almacenamiento y archivos eliminados

Objetivos

El objetivo principal de esta actividad es comprender cómo se estructura un dispositivo de almacenamiento (Esquema de particionado, Particiones, Volúmenes, etc.) y practicar la recuperación de archivos eliminados bajo distintas circunstancias.

Además, esta actividad también ayudará al alumno a asentar los conocimientos adquiridos sobre los metadatos que pueden contener los archivos.

Descripción y pautas de la actividad

Para realizar la actividad, el alumno deberá analizar la imagen forense (archivo evidence.E01) facilitada a través de la plataforma de UNIR. Esta imagen forense se corresponde con un dispositivo de almacenamiento cuyo hash MD5 es: bb898ff8859fec8eb3c24bb368905311.

Para realizar la práctica debe responder a las preguntas planteadas en la plantilla. La contestación a la presente actividad no ocupa más de una hoja. Simplemente debe contestar a lo que se le pregunta.

Si no fuera posible responder a alguna de las preguntas planteadas, tan solo indique dónde podría encontrarse la información necesaria y el motivo por el cual no es posible responder a la pregunta.

¿Cuál es el hash SHA1 del dispositivo que has adquirido?
4fe7bd2f428a6c8603e25d528526915d7f7e3f8b

¿Qué esquema de particionado tiene el dispositivo?
Partition 1 – 10 MB – FAT12 Partition 3 – 67 MB - NTFS

Asignatura	Datos del alumno	Fecha
Análisis Forense	Apellidos: Paz López	11/06/2022
	Nombre: Angel Ramón	

¿Cuántas particiones tiene el dispositivo?

2

De cada partición (puede haber una o varias), indica lo siguiente:

- N° de partición: 1
- Nombre del volumen: VOL01[Fat12]
- Sistema de ficheros: [root], [unallocated space], FAT1, FAT2, reserved vector, VBR
- Tamaño en Bytes: 10 MB = 1e+7 Bytes
- N° de partición: 2
- Nombre del volumen: VOL02[NTFS]
- Sistema de ficheros: [orphan], [root], [unallocated space], backup boot sector, file system slack
- Tamaño en Bytes: 67 MB = 6.7e+7 Bytes

En una de las particiones hay un archivo eliminado. Recupera dicho archivo y analiza sus metadatos.

En base a tu análisis ¿Cuál es el nombre del artista que realizó la fotografía?

Eliot Alderson

Además del archivo recuperado en el punto anterior, en el dispositivo hay otro archivo eliminado. Realiza una recuperación en bruto de los archivos del dispositivo para recuperarlo y analiza sus metadatos.

En base a tu análisis ¿Cuál es el nombre de la ciudad donde se tomó la fotografía? Si detectas alguna incoherencia durante el análisis, indícala.

Chicago Illinois. Inconveniente se hizo un análisis con exi.exe y arroja el resultado City: New York con Coordenadas 41°51'4.37" N, 87°38'3.92" W pero al colocarlas en Google Map pertenece a la ciudad de Chicago Illinois.

Rúbrica

Dispositivos de almacenamiento y archivos eliminados	Descripción	Puntuación máxima (puntos)	Peso %
Criterio 1	Adquisición del dispositivo de almacenamiento	3	30%
Criterio 2	Contestación correcta a las preguntas sobre el esquema de particionado y particiones	2,5	25%
Criterio 3	Recuperación de los archivos eliminados	2,5	25%

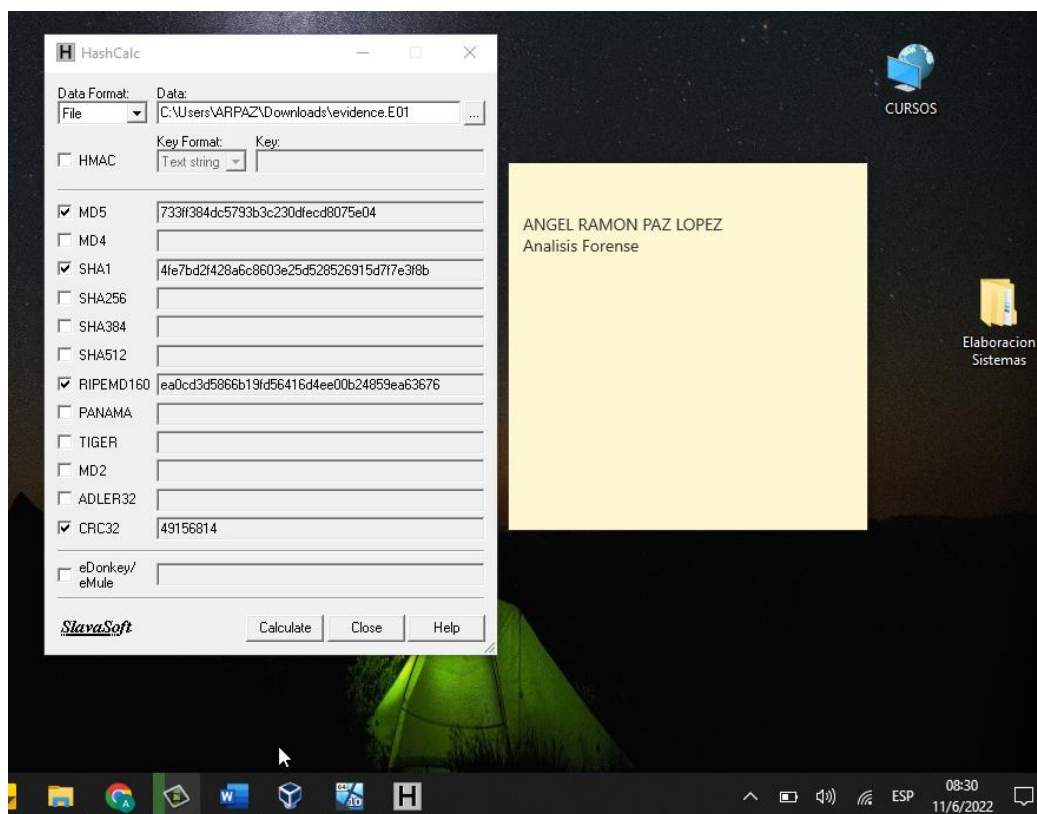
Asignatura	Datos del alumno	Fecha
Análisis Forense	Apellidos: Paz López	11/06/2022
	Nombre: Angel Ramón	

Criterio 4	Análisis correcto de los metadatos de los archivos recuperados	2	20%
		10	100 %

Extensión máxima: La actividad debe responderse completando la plantilla adjunta sin superar las dos páginas de extensión, letra Georgia 11, interlineado 1,5, margen superior e inferior 2,5 cm y margen izquierdo y derecho 3,25 cm.

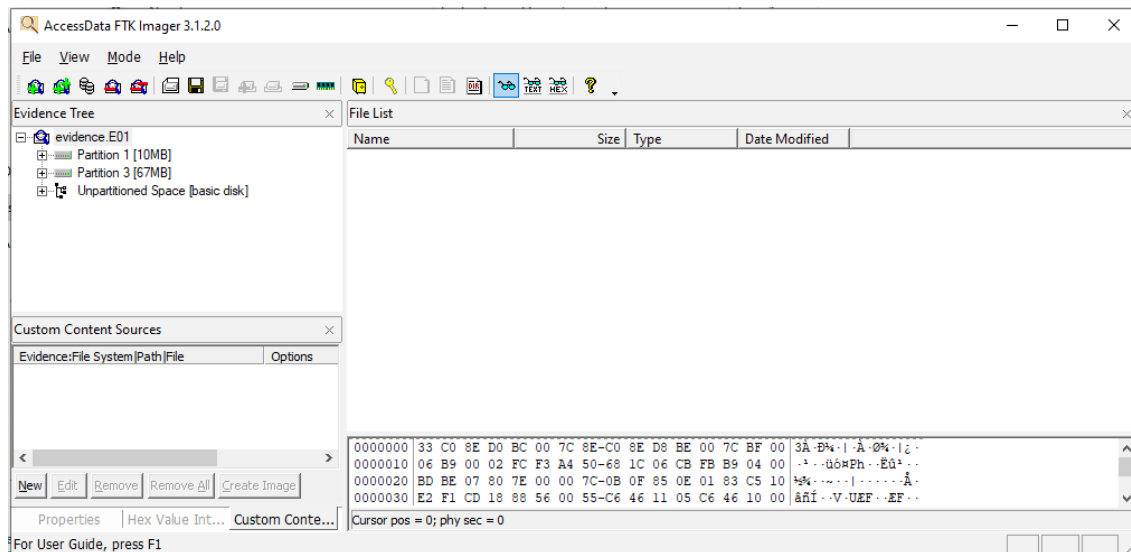
PROCEDIMIENTO

Para encontrar el hash SHA1 del dispositivo usamos la herramienta HashCalc



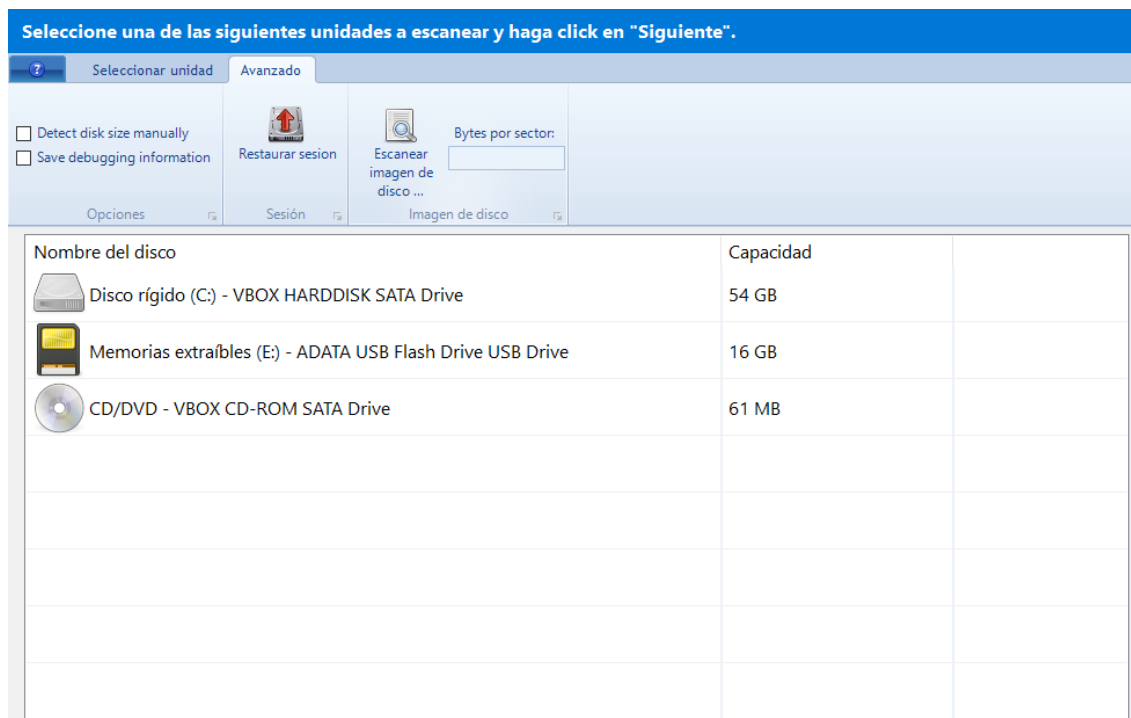
Para ver la información de la evidencia usamos la herramienta FTK Imager en el cual agregar la evidencia a analizar como Logical Drive y tendremos cierta información

Asignatura	Datos del alumno	Fecha
Análisis Forense	Apellidos: Paz López	11/06/2022
	Nombre: Angel Ramón	



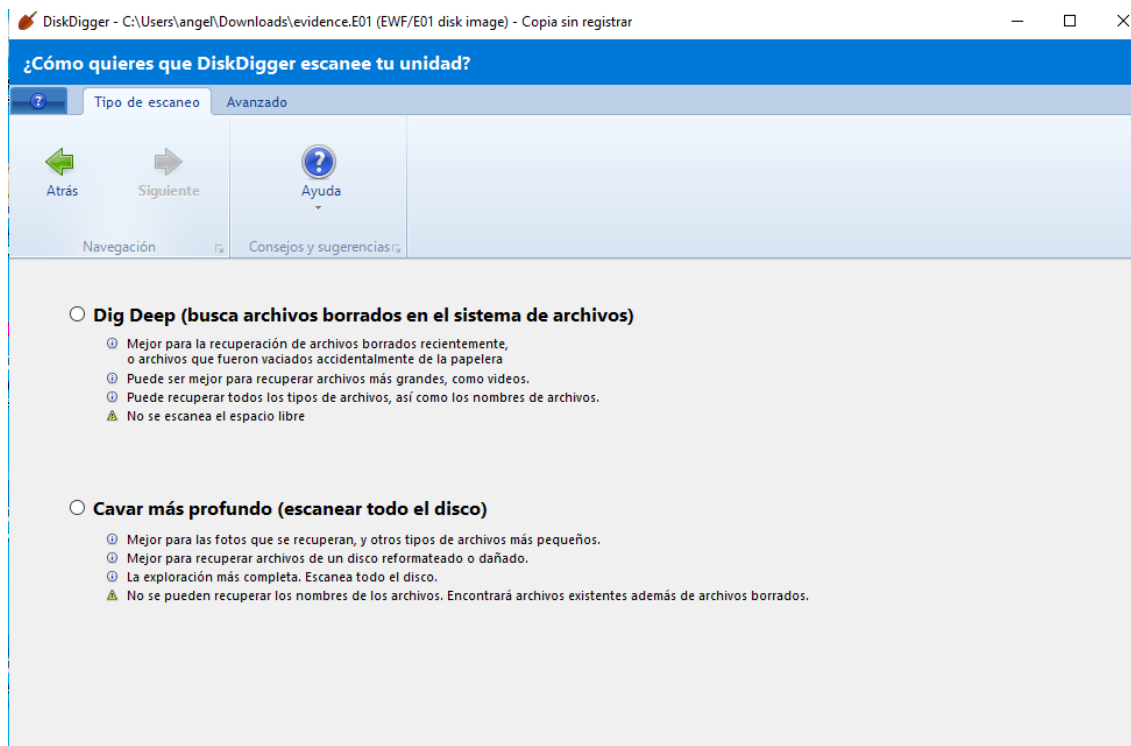
Podemos notar dos particiones con sus respectivos tamaños y directorios

Después usamos la herramienta diskdigger para buscar archivos borrados en las unidades, pero primero tendremos que ir a avanzado y buscar la opción Escanear imagen del disco

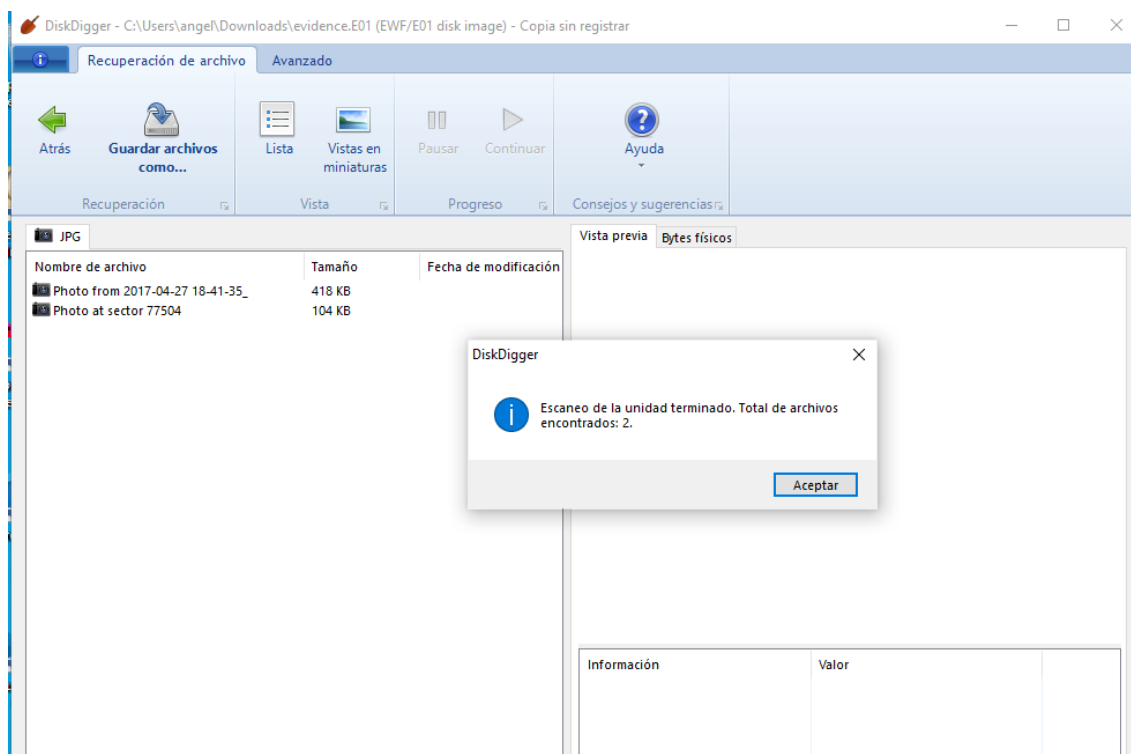


Realizamos un escaneo profundo

Asignatura	Datos del alumno	Fecha
Análisis Forense	Apellidos: Paz López	11/06/2022
	Nombre: Angel Ramón	



Una vez seleccionado la opción Cavar más profundo obtuvimos como resultado dos imágenes eliminadas de la evidencia por lo cual damos en Guardar archivos como...



Asignatura	Datos del alumno	Fecha
Análisis Forense	Apellidos: Paz López	11/06/2022
	Nombre: Angel Ramón	

Ahora procederemos a analizar la metadata de las imágenes





Vista previa Bytes físicos	
Información	Valor
● JFIF version	1.1
● JFIF horizontal density	72 dpi
● JFIF vertical density	72 dpi
● 8BIM tag	1028
● 8BIM tag	1061
● Image description	MR. ROBOT -- "eps3.1_undo.gz" E...
● Hacer	SONY
● Model	DSC-RX1RM2
● Orientation	1
● X resolution	300
● Y resolution	300
● Resolution unit	2
● Software	Adobe Photoshop CC 2015 (Macin...
● Fecha de creación	2017-10-17T19:18:44-04:00
● Artist	USA Network
● Copyright	2017 USA Network Media, LLC
● Exposure time	0.005
● F-number	2
● Exposure program	1
● ISO speed ratings	6400
● Exif version	"0220" (48 50 50 48)
● DateTime original	2017-04-27 18:41:35

Vista previa Bytes físicos	
Información	Valor
● JFIF version	1.1
● JFIF horizontal density	72 dpi
● JFIF vertical density	72 dpi
● 8BIM tag	1028
● 8BIM tag	1061
● Image description	MR. ROBOT -- "eps3.1_undo.gz" E...
● Hacer	SONY
● Model	DSC-RX1RM2
● Orientation	1
● X resolution	300
● Y resolution	300
● Resolution unit	2
● Software	Adobe Photoshop CC 2015 (Macin...
● Fecha de creación	2017-10-17T19:18:44-04:00
● Artist	USA Network
● Copyright	2017 USA Network Media, LLC
● Exposure time	0.005
● F-number	2
● Exposure program	1
● ISO speed ratings	6400
● Exif version	"0220" (48 50 50 48)
● DateTime original	2017-04-27 18:41:35

Colocamos los datos del GPS en google maps para ver la localizacion.

Asignatura	Datos del alumno	Fecha
Análisis Forense	Apellidos: Paz López	11/06/2022
	Nombre: Angel Ramón	

Vista previa Bytes físicos	
	
Información	Valor
JFIF version	1.1
JFIF horizontal density	72 dpi
JFIF vertical density	72 dpi
8BIM tag	1028
8BIM tag	1061
Image description	MR. ROBOT -- "eps3.1_undo.gz" E...
Hacer	SONY
Model	DSC-RX1RM2
Orientation	1
X resolution	300
Y resolution	300
Resolution unit	2
Software	Adobe Photoshop CC 2015 (Macin...
Fecha de creación	2017-10-17T19:18:44-04:00
Artist	USA Network
Copyright	2017 USA Network Media, LLC
Exposure time	0.005
F-number	2
Exposure program	1
ISO speed ratings	6400
Exif version	"0220" (48 50 50 48)
DateTime original	2017-04-27 18:41:35

Vista previa Bytes físicos	
	
Información	Valor
JFIF version	1.1
JFIF horizontal density	72 dpi
JFIF vertical density	72 dpi
8BIM tag	1028
8BIM tag	1061
Image description	MR. ROBOT -- "eps3.1_undo.gz" E...
Hacer	SONY
Model	DSC-RX1RM2
Orientation	1
X resolution	300
Y resolution	300
Resolution unit	2
Software	Adobe Photoshop CC 2015 (Macin...
Fecha de creación	2017-10-17T19:18:44-04:00
Artist	USA Network
Copyright	2017 USA Network Media, LLC
Exposure time	0.005
F-number	2
Exposure program	1
ISO speed ratings	6400
Exif version	"0220" (48 50 50 48)
DateTime original	2017-04-27 18:41:35