Informática Forense y Auditoría

Grado en Ingeniería Informática del Software

Escuela de Ingeniería Informática de Oviedo

Práctica 3: Ejercicios de Práctica Forense II

Objetivos

En los siguientes ejercicios, pretendemos alcanzar, entre otros, los siguientes objetivos:

- Identificar ficheros utilizando técnicas de carving.
- Recuperación de ficheros borrados a partir de los metadatos remanentes en el sistema de ficheros una vez que aquellos han sido borrados.
- Análisis de ficheros sospechosos con herramientas antimalware.
- Extracción de metadatos EXIF.

Instrucciones comunes a todos los ejercicios

Deberá justificar la realización de los siguientes ejercicios con capturas de pantalla donde quede patente que el ejercicio se realiza con la cuenta del alumno creada en la primera práctica, así como los comandos empleados en la resolución de los mismos y las explicaciones que considere oportunas.

Identificación de archivos utilizando técnicas de carving

El carving es la técnica forense que permite la identificación y extracción de archivos basada en contenido en lugar de la información almacenada en estructuras del sistema de ficheros donde residen (ej.: inodos en Linux). La extracción de ficheros a partir de bloques no asignados por el sistema de ficheros se realiza identificando conjuntos de bytes únicos (**file signatures**) que aparecen al principio y/o al final del archivo y que están asociados con un tipo de fichero específico. Esta técnica también permite detectar lo que se conoce con el nombre de **file mismatch**, que ocurre cuando se intenta modificar la extensión de un archivo para evitar su detección.

Instrucciones comunes a los ejercicios de carving

Para realizar los ejercicios de carving (a excepción del ejercicio 1) descomprima el fichero correspondiente al ejercicio. Para descomprimir el fichero utilice **7-zip**. Una vez descomprimido, tendrá un fichero denominado **nombre_fichero.dd**. Abra la aplicación **Autopsy** instalada en su equipo anfitrión. Cree un nuevo caso desde el interfaz de

Autopsy. Llame al nuevo caso de la siguiente manera: **EjercicioXX_Carving_TipoFicheros_LX**, donde XX es el número del ejercicio que está realizando en este momento, TipoFicheros es el tipo de ficheros sobre los que se intenta realizar el carving (Graphic, Documents, Audio, Video, etc) el cual viene indicado en el fichero comprimido. En el número de caso ponga DDMMAAAA-XX donde DD es el día en el que realiza el ejercicio, MM es el número del mes actual y AAAA es el año actual, siendo XX el número del ejercicio que está realizando. Ponga su nombre y sus datos en la información del examinador (**ponga en el correo su dirección de email de uniovi**). Añada al caso la evidencia correspondiente al ejercicio que está realizando como **Fichero de Imagen de Espacio no Asignado**. Conteste a las preguntas que se le formulan en cada ejercicio o rellene las tablas correspondientes, justificando todo con capturas de pantalla.

1. Realice este ejercicio en la máquina virtual donde ha instalado CAINE (**IFA-AU-XX**). En este caso vamos a realizar una práctica de carving de forma artesanal. Descarga del campus virtual (**Recursos Prácticas-Práctica 3**), el fichero **L0_Graphic.dd.bz2** y descomprímelo (**bunzip2 –f L0_Graphic.dd.bz2**). Una vez descomprimido, tendrá un fichero denominado **nombre_fichero.dd**. Vamos a utilizar el comando dd como unas "tijeras" para perfilar una imagen JPG contenida en el fichero anterior. Para usar el comando dd deberemos saber dónde comienza la imagen y donde debemos parar de "cortar". Lo primero que debemos hacer es buscar el comienzo de la imagen. Una forma de buscar el inicio de la imagen dentro del fichero es buscar el patrón **ffd8**. En la misma línea que aparezca ese patrón debe aparecer la cadena "JFIF". Si no fuese así, siga buscando la siguiente ocurrencia del patrón. Apunte el offset mostrado al principio de la línea por **xxd** ya que en esa línea se encuentra el inicio del fichero JPG. Pase dicho offset a decimal. Ese será el comienzo real de la imagen en el conjunto de bytes anterior. Una vez tenemos localizado el comienzo de la imagen buscaremos a partir de ese punto el final de la misma; el patrón en este caso que debemos buscar es **ffd9**. Anotaremos el offset del comienzo de la línea donde aparece dicho patrón. Convertiremos dicho offset a decimal. Debemos de tener en cuenta que el offset es el del comienzo de la línea donde aparece el patrón y por tanto deberemos añadir tantos bytes a dicho offset como **2xnumero_grupos_hexadecimales** anteriores al patrón **ffd9**. Calcularemos la diferencia entre el offset final e inicial y tendremos el tamaño del fichero de imagen que queremos extraer. Ya solo nos resta extraer la imagen utilizando el comando dd con las opciones **skip** (para posicionarnos en el offset de inicio del fichero dentro de la imagen), **bs=1** (tamaño de bloque igual a 1 byte) y **count** (número de bloques de tamaño bs a cortar).

2. Descarga del campus virtual (**Recursos Prácticas-Práctica 3**), el fichero **L0_Graphic.dd.bz2**. Almacénelo en una carpeta de Evidencias. Cree un caso siguiendo las instrucciones comunes a todos los ejercicios. Investigue qué posibilidades ofrecen los módulos de ingestión de Autopsy siguientes: **File Type**

Identification, Exif Parser y PhotorecCarver y añádalos como módulos de ingestión de evidencia asociados al proyecto. Realice el proceso de ingestión y una vez haya finalizado, compruebe los resultados obtenidos para rellenar la siguiente tabla.

Indique, por cada imagen encontrada, los siguientes datos:

Nombre del fichero en Autopsy	Tamaño del fichero (en Bytes)	Imagen visible

3. Descarga del campus virtual (**Recursos Prácticas- Práctica 3**), el fichero **L1_Graphic.dd.bz2**. Almacénelo en una carpeta de Evidencias. Cree un caso siguiendo las instrucciones comunes a todos los ejercicios. Incluya los módulos de ingestión de Autopsy siguientes: **File Type Identification, Exif Parser y PhotorecCarver.** Realice el proceso de ingestión y una vez haya finalizado, compruebe los resultados obtenidos para rellenar la siguiente tabla.

Indique, por cada imagen encontrada, los siguientes datos:

Nombre del fichero en Autopsy	Tamaño del fichero (en Bytes)	Imagen visible

4. Descarga del campus virtual (**Recursos Prácticas- Práctica 3**), el fichero **L0_Documents.dd.bz2**. Almacénelo en una carpeta de Evidencias. Cree un caso siguiendo las instrucciones comunes a todos los ejercicios. Incluya los módulos de ingestión de Autopsy siguientes: **File Type Identification, Exif Parser y PhotorecCarver**. Realice el proceso de ingestión y una vez haya finalizado, compruebe los resultados obtenidos para rellenar la siguiente tabla.

Indique, por cada documento encontrado, los siguientes datos:

Nombre del fichero en Autopsy	Tamaño del fichero (en Bytes)	Tipo MIME	Fecha Creación del documento

5. Descarga del campus virtual (**Recursos Prácticas- Práctica 3**), el fichero **L1_Documents.dd.bz2**. Almacénelo en una carpeta de Evidencias. Cree un caso siguiendo las instrucciones comunes a todos los ejercicios. Incluya los módulos de ingestión de Autopsy siguientes: **File Type Identification, Exif Parser y PhotorecCarver**. Realice el proceso de ingestión y una vez haya finalizado, compruebe los resultados obtenidos para rellenar la siguiente tabla.

   Indique, por cada documento encontrado, los siguientes datos:

Nombre del fichero en Autopsy	Tamaño del fichero (en Bytes)	Tipo MIME	Fecha Creación del documento

6. Descarga del campus virtual (**Recursos Prácticas- Práctica 3**), el fichero **L2_Documents.dd.bz2**. Almacénelo en una carpeta de Evidencias. Cree un caso siguiendo las instrucciones comunes a todos los ejercicios. Incluya los módulos de ingestión de Autopsy siguientes: **File Type Identification, Exif Parser y PhotorecCarver**. En este caso el conjunto de ficheros borrados en el espacio no asignado es el mismo que en los dos ejemplos anteriores, pero los ficheros están fragmentados no secuencialmente. Responda a las siguientes cuestiones:
   a) ¿Cuántos falsos positivos (ficheros borrados) identifica la herramienta?
   b) ¿De qué tipo MIME (incorrecto) son los ficheros carveados?

7. En este ejercicio aplicaremos técnicas de carving sobre ficheros comprimidos (7z, zip, etc.). Descarga del campus virtual (**Recursos Prácticas- Práctica 3**), el fichero **L0_Archive.dd.bz2**. Almacénelo en una carpeta de Evidencias. Cree un caso siguiendo las instrucciones comunes a todos los ejercicios. Investigue las posibilidades que le ofrece el módulo de ingestión **Embedded File Extractor**. Añada además al caso los módulos de ingestión que ha utilizado en los ejercicios anteriores. Realice el proceso de ingestión y una vez haya finalizado, compruebe los resultados obtenidos para rellenar la siguiente tabla.

   Indique por cada fichero comprimido carveado la siguiente información:

Nombre del fichero en Autopsy	Tamaño del fichero (en Bytes)	Tipo MIME

Del contenido extraído de los ficheros comprimidos, obtenga para cada fichero jpg presente en ellos los siguientes datos en caso de que estén disponibles. Utilice para ello la herramienta de línea de comando exiftool que viene incorporada con CAINE.

Nombre del fichero en Autopsy	Fecha y hora de la imagen	Dispositivo con el que se tomó la imagen	Descripción de la imagen

8. En este ejercicio aplicaremos técnicas de carving sobre ficheros comprimidos (7z, zip, etc.). Descarga del campus virtual (**Recursos Prácticas- Práctica 3**), el fichero **L2_Archive.dd.bz2**. Almacénelo en una carpeta de Evidencias. Cree un caso siguiendo las instrucciones comunes a todos los ejercicios. Añada además al caso los módulos de ingestión que ha utilizado en los ejercicios anteriores. Realice el proceso de ingestión y una vez haya finalizado, compruebe los resultados obtenidos para rellenar la siguiente tabla.

Nombre del fichero en Autopsy	Tamaño del fichero (en Bytes)	Tipo MIME

Instale los paquetes **clamav** y **clamtk**. Una vez hecho esto, desde el listado, extraiga el/los archivo/s en cuestión a la carpeta Export del caso. Abra la carpeta y analice el/los archivo con el antivirus anteriormente instalado y capture los resultados.

a) ¿Hay algún fichero que presente alguna particularidad?
b) ¿De qué tipo?

9. En este ejercicio aplicaremos técnicas de carving sobre ficheros de formatos de audio (MP3, WAV, etc.). Descarga del campus virtual (**Recursos Prácticas- Práctica 3**), el fichero **L0_Audio.dd.bz2**. Almacénelo en una carpeta de Evidencias. Cree un caso siguiendo las instrucciones comunes a todos los ejercicios. Añada además al caso los módulos de ingestión que ha utilizado en los ejercicios anteriores (en este caso ya no es necesario el módulo Embedded File Extractor). Realice el proceso de ingestión y una vez haya finalizado, compruebe los resultados obtenidos para rellenar la siguiente tabla.

Indique por cada fichero de audio carveado la siguiente información:

Nombre del fichero en Autopsy	Tamaño del fichero (en Bytes)	Tipo MIME	Autor	Género	Duración	Tasa Muestreo

10. En este ejercicio aplicaremos técnicas de carving sobre ficheros de formatos de audio (MP3, WAV, etc.). Descarga del campus virtual (**Recursos Prácticas- Práctica 3**), el fichero **L2_Audio.dd.bz2**. Almacénelo en una carpeta de Evidencias. Cree un caso siguiendo las instrucciones comunes a todos los ejercicios. Añada además al caso los módulos de ingestión que ha utilizado en el ejercicio anterior. Realice el proceso de ingestión y una vez haya finalizado, compruebe los resultados obtenidos para rellenar la siguiente tabla.

    Indique por cada fichero de audio carveado la siguiente información:

Nombre del fichero en Autopsy	Tamaño del fichero (en Bytes)	Tipo MIME	Autor	Género	Duración	Tasa Muestreo

11. En este ejercicio aplicaremos técnicas de carving sobre ficheros de formatos de vídeo (MP3, WAV, etc.). Descarga del campus virtual (**Recursos Prácticas- Práctica 3**), el fichero **L0_Video.dd.bz2**. Almacénelo en una carpeta de Evidencias. Cree un caso siguiendo las instrucciones comunes a todos los ejercicios. Añada además al caso los módulos de ingestión que ha utilizado en el ejercicio anterior. Realice el proceso de ingestión y una vez haya finalizado, compruebe los resultados obtenidos para rellenar la siguiente tabla.

    Indique por cada fichero de video carveado la siguiente información:

Nombre del fichero en Autopsy	Tamaño del fichero (en Bytes)	Tipo MIME	FPS	Resolución	Tasa Muestreo	Duración	Fecha

Recuperación de ficheros borrados a partir de sus metadatos

En el siguiente conjunto de ejercicios veremos la eficiencia de Autopsy en la recuperación de ficheros borrados a partir de los metadatos (inodos, dentries, etc.) remanentes en el sistema de ficheros una vez que aquellos han sido borrados. Los metadatos son usados una vez que el fichero ha sido borrado para intentar reconstruir el fichero original.

La mayoría de las imágenes con las que trabajaremos contienen unos pocos ficheros, algunos de los cuales han sido borrados. Las imágenes de los discos pueden contener una o más particiones y estar formateadas con diversos sistemas de ficheros: FAT12, FAT16, FAT32, NTFS, extX u otros que el alumno tendrá que averiguar a través de la información proporcionada por Autopsy.

Instrucciones comunes a los ejercicios de recuperación de ficheros borrados

Abra una terminal en la máquina en la que ha instalado CAINE (IFA-AU-XX) y descomprima el fichero correspondiente al ejercicio en la carpeta en la que lo ha almacenado. Para descomprimir el fichero utilice el comando **bunzip2 –f nombre_fichero.bz2** Una vez descomprimido tendrá un fichero denominado nombre_fichero.dd. Abra la utilidad Autopsy desde **Menú->Forensic Tools->Autopsy**. Cree un nuevo caso desde el interfaz de Autopsy. Llame al nuevo caso de la siguiente manera: EjercicioXX_BorradoFicheros, donde XX es el número del ejercicio que está realizando en este momento. En el número de caso ponga DDMMAAAA-XX donde DD es el día en el que realiza el ejercicio, MM es el número del mes actual y AAAA es el año actual, siendo XX el número del ejercicio que está realizando. Ponga su nombre y sus datos en la información del examinador (**ponga en el correo su dirección de email de uniovi**). Añada al caso la evidencia correspondiente al ejercicio que está realizando como **Imagen de disco o fichero VM**. Conteste a las preguntas que se le formulan en cada ejercicio justificándolas con capturas de pantalla. Se recomienda también consultar las siguientes referencias webográficas para intentar interpretar los resultados obtenidos:

https://en.wikipedia.org/wiki/Comparison_of_file_systems

https://forensicswiki.xyz/wiki/index.php?title=MAC_times

12. Descarga del campus virtual (**Recursos Prácticas- Práctica 3**), el **dfr-01-gbu.dd.bz2**. Almacénelo en una carpeta de Evidencias. Cree un caso siguiendo las instrucciones comunes a todos los ejercicios. Añada como módulos de ingestión de evidencia asociados al proyecto los módulos siguientes: **File Type Identification, PhotorecCarver**.

    a) Responda a las siguientes cuestiones:

Número de Partición	Sector de Comienzo	Sector de Finalización	Tipo Sistema de Ficheros

b) ¿Cuantos ficheros de texto (borrados o no) se encuentran en las particiones detectadas en la imagen?
c) Por cada fichero borrado indique la siguiente información:

				MAC times por cada fichero antes del borrado (GMT)		
Nombre	Tamaño	Sector relativo	Partición	Acceso	Modificación	Creación

d) Muestre la línea temporal de cada uno de los ficheros borrados localizados por la herramienta.

13. Descarga del campus virtual (**Recursos Prácticas- Práctica 3**), el **dfr-02-fyu.dd.bz2**. Almacénelo en una carpeta de Evidencias. Cree un caso siguiendo las instrucciones comunes a todos los ejercicios. Añada como módulos de ingestión de evidencia asociados al proyecto los módulos siguientes: **File Type Identification, PhotorecCarver**. Realice el proceso de ingestión y una vez haya finalizado, compruebe los resultados obtenidos para rellenar la siguiente tabla.

a) Rellene la información correspondiente a cada partición identificada:

Número de Partición	Sector de Comienzo	Sector de Finalización	Tipo Sistema de Ficheros

b) ¿Cuantos ficheros de texto plano (borrados o no) se encuentran en las particiones detectadas en la imagen?
c) Por cada fichero borrado indique la siguiente información:

			MAC times por cada fichero antes del borrado (GMT)		
Nombre	Tamaño	Partición	Acceso	Modificación	Cambio

d) Muestre la línea temporal de cada uno de los ficheros borrados localizados por la herramienta.

14. Descarga del campus virtual (**Recursos Prácticas- Práctica 3**), el fichero **dfr-03-mugt.dd.bz2**. Almacénelo en una carpeta de Evidencias. Cree un caso siguiendo las instrucciones comunes a todos los ejercicios. Añada como módulos de ingestión de evidencia asociados al proyecto los módulos siguientes: **File Type Identification, PhotorecCarver.**

Responda a las siguientes cuestiones:

Número de Partición	Sector de Comienzo	Sector de Finalización	Tipo Sistema de Ficheros

a) ¿Cuantos ficheros de tipo mime text/plain borrados se encuentran en las particiones detectadas en la imagen?
b) Por cada fichero anterior indique la siguiente información:

			MAC times por cada fichero antes del borrado (GMT)			
Nombre	Tamaño	Partición	Acceso	Modificación	Cambio	Creación

c) Por cada fichero de texto plano borrado muestre su línea temporal.

Extracción de metadatos EXIF

EXIF es una especificación diseñada originalmente por los fabricantes de cámaras digitales japoneses para los ficheros de imagen. Esta especificación añade etiquetas (tags) con metadatos a los formatos de archivo (JPEG, TIFF, RIFF, PNG, WAV etc.) que pueden generar las cámaras digitales. Dichos metadatos contienen información variada, como por ejemplo:

- Información de fecha y hora.
- Configuración de la cámara:
    - Modelo de cámara y fabricante.
    - Apertura: Se mide en f/valor. A un mayor valor menor apertura y viceversa. Con grandes aperturas (valor menor que 4) se consigue menor profundidad de campo y nitidez ayudando al enfoque selectivo. Con pequeñas aperturas (valores mayores que 4) se consigue gran profundidad de campo y nitidez.
    - Velocidad del obturador o de disparo: Hace referencia al tiempo que está abierto el diafragma. Tiempos cortos (<1/60 segundo) congelan el movimiento mientras que tiempos largos (>=1/60 segundo) se consiguen mayores sensaciones de desplazamiento.
    - Distancia focal.
    - Medidor de exposición que da las medidas equivalentes de apertura de diafragma y velocidad de obturación.
    - Velocidad de la película: Esto ha sido adaptado a las cámaras digitales. Un número de la escala alto indica que el valor de la sensibilidad de la película es grande, por lo que se requerirá menor iluminación que si se tuviera un valor de escala bajo.
- Información sobre localización: Siempre que la cámara o el Smartphone desde que se tome la imagen dispongan de uno y tenga activo incorporar la ubicación donde fueron tomadas las imágenes.
- Descripción e información sobre el copyright.
- …

Podemos acceder a los metadatos de un fichero desde el propio Sistema Operativo, simplemente seleccionando el fichero en cuestión y desde su menú contextual seleccionamos la opción Propiedades y desde ella la pestaña Detalles.
Existen herramientas específicas que permiten la extracción de metadatos (no solamente los Exif) tanto en ficheros de imagen como ficheros de otros formatos. Entre estas herramientas se encuentra **Exiftool** que es una herramienta que permite el análisis, la eliminación, la modificación y la edición de metadatos. Se puede utilizar tanto en línea de comandos como en interfaz gráfica y está disponible para Sistemas Operativos Windows, Mac y Linux.

15. Descarga e instala desde el siguiente enlace (https://exiftool.org/) la versión de línea de comandos de Exiftool para windows. Descomprime el fichero y renombra el ejecutable para que pueda utilizarse desde la línea de comandos. Para no tener que escribir la ruta absoluta al ejecutable cada vez que quieras utilizarlo, puedes incluir dicha ruta en la variable de entorno PATH del usuario. Instala a continuación el entorno gráfico de Exiftool, el cual está disponible desde el siguiente enlace (https://exiftool.org/gui/). Lee atentamente el apartado **Requirements and preparation** antes de realizar la instalación (especialmente los puntos 1 y 2).

16. Descarga del campus virtual (Recursos Prácticas- Práctica 3), el fichero **imagenesEXIF.zip**. Almacénelo en una carpeta de Evidencias. Descomprime dicho archivo y, ayudado por las herramientas instaladas en los dos ejercicios anteriores, obtén para cada archivo la siguiente información a partir de sus etiquetas:

    - Fecha en la que fue tomada la imagen
    - Marca de la cámara.
    - Modelo de la cámara.
    - Características de la imagen:
        - Ancho y alto de la imagen en pixels.
        - Resolución en el eje X (ppp o dpi).
        - Resolución en el eje Y (ppp o dpi).
        - Bits de color por pixel.
    - Tamaño del archivo.
    - Ubicación GPS (si disponible)
    - Lugar correspondiente a la ubicación. A partir de coordenadas de posicionamiento GPS utilizando Google Maps.

Fichero	imagen1	imagen2	imagen3	imagen4	imagen5
Fecha captura de la imagen (AAAA-MM-DD hh:mm:ss)					
Marca cámara					
Modelo cámara/dispositivo					
AnchoxAlto					
Resolución horizontal (ppp)					
Resolución vertical (ppp)					
Bits de color por pixel					

Tamaño archivo (KB)					
Ubicación GPS (Latitud y Longitud)					
Lugar correspondiente a la ubicación					
Fichero	imagen6	imagen7	imagen8	imagen9	imagen10
Fecha captura de la imagen (AAAA-MM-DD hh:mm:ss)					
Marca cámara					
Modelo cámara/dispositivo					
AnchoxAlto					
Resolución horizontal (ppp)					
Resolución vertical (ppp)					
Bits de color por pixel					
Tamaño archivo (KB)					
Ubicación GPS (Latitud y Longitud)					
Lugar correspondiente a la ubicación					

a) Suponiendo que las fotos fueron adquiridas de un mismo dispositivo, ¿qué sitios visitó su propietario en orden cronológico?

Firmado por GARCIA TAMARGO, MARCO ANTONIO (FIRMA) el día 25/09/2024 con un certificado emitido por AC DNIE 006