Profesor

Constantino Malagón

Seguridad Informática

Forensics Carving

Universidad Francisco de Vitoria UFV Madrid

Grado en Ingeniería Informática
Escuela Politécnica Superior

Forensics carving

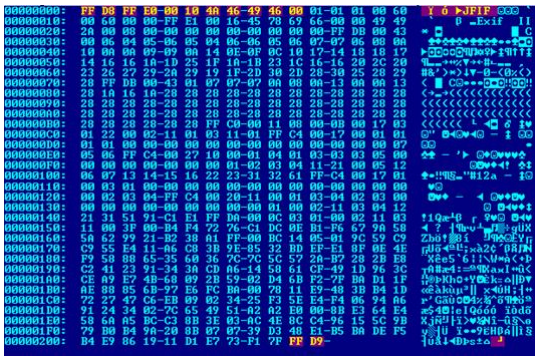
Universidad Francisco de Vitoria UFV Madrid

- Llamamos Forensics carving al proceso de recuperación de ficheros a partir de sus metadatos
- Para ello se analiza el contenido del archivo en bruto (raw) y a partir de aquí intentar identificar si es una imagen, texto, mp3, etc…
- Esto se hace a partir de los llamados “magical numbers” o firma del fichero que identifican el principio y el final de un fichero

Forensics carving

Universidad Francisco de Vitoria UFV Madrid

- Por ejemplo, atendiendo a su estructura, todos los ficheros JPG/JFIF empiezan por FF D8 FF E0 y terminan por FF D9



Forensics carving

Universidad Francisco de Vitoria UFV Madrid

- Esta técnica es realmente útil en multitud de casos, como por ejemplo aquellos en los que los dispositivos de almacenamiento se hayan corrompido o dañado, o en casos en los que se realice una investigación en la que se utilice un análisis forense
- Más información: https://resources.infosecinstitute.com/file-carving/

Universidad Francisco de Vitoria UFV Madrid

Recuperación de archivos

Forensics carving

Universidad Francisco de Vitoria UFV Madrid

- Vamos a intentar recuperar archivos en diferentes escenarios:
  - Archivos que han sido borrados
  - Archivos que se han corrompido y no puedo abrirlos
  - Recuperar todas las imágenes de un disco duro (pederastia)
- También podemos utilizarlo si hemos borrado nosotros accidentalmente un fichero, aunque esto no es específicamente *file carving*

Herramientas de recuperación de archivos

Universidad Francisco de Vitoria UFV Madrid

- Es necesario conocer varias herramientas y usarlas, para tener una mejor recuperación
- No nos deberíamos quedar con una sola
- Vamos a ver cuatro herramientas:
  - 1) Foremost
  - 2) Scalpel
  - 3) Recoverjpeg
  - 4) Photorec

Foremost

Universidad Francisco de Vitoria UFV Madrid

- Arrancamos Foremost (en Aplicaciones/forensics)
- Herramienta para recuperar archivos
  - man foremost
  - Conecto un disco externo USB
  - Pongo fdisk –l y veo cómo se llama
- Uso: foremost –h (help)

Foremost

Universidad Francisco de Vitoria UFV Madrid

- Imaginemos que queremos recuperar todas las fotos que tiene guardadas un pederasta en un disco duro externo
- foremost –i /dev/sdb (también puedo dar como argumento una imagen de disco iso o dd) –o /tmp/images1 –t png,jpg –T
- Voy a /tmp/images y ahí tengo todas las fotos
- Lo hemos hecho fácilmente y en muy poco tiempo

Foremost

Universidad Francisco de Vitoria UFV Madrid

- Otro ejemplo: https://digitalcorpora.org/corpora/disk-images
- nps-2009-canon2 — *A set of images taken on with a Canon digital camera that can be used to test basic file recovery, fragmented file recovery, and file carving.*
- Realizar el proceso anterior con esta imagen

Scalpel

- Recuperar archivos borrados con Scalpel
- Está en Aplicaciones/Forensics/Forensic Carving Tools
- Vemos la ayuda: man scalpel
- Abrimos su fichero de configuración: /etc/scalpel/scalpel.conf
- Tenemos que descomentar las líneas de los tipos de ficheros que queremos recuperar
- Por ejemplo, la línea de PNG, JPEG, etc…

Scalpel

- Ejecutamos lo siguiente desde un terminal:
  - scalpel /dev/sdb -o /tmp/ (si quiero guardar los archivos recuperados en /tmp)
- Lo probaremos con nuestra imagen que nos hemos bajado antes
- nps-2009-canon2 — *A set of images taken on with a Canon digital camera that can be used to test basic file recovery, fragmented file recovery, and file carving.*

Recoverjpeg

Universidad Francisco de Vitoria UFV Madrid

- También podemos usar la herramienta Recoverjpeg
- Vemos la ayuda: man recoverjpeg
- Está como siempre en Forensics/Forensic Carving Tools
  - recoverjpg /dev/sdb -o /tmp/ (si quiero guardar los archivos recuperados en /tmp)
- Lo probaremos con nuestra imagen que nos hemos bajado antes
- nps-2009-canon2 — *A set of images taken on with a Canon digital camera that can be used to test basic file recovery, fragmented file recovery, and file carving.*

Photorec

Universidad Francisco de Vitoria UFV Madrid

- PhotoRec – data recovery tool
- Recupera archivos de un disco duro (incluidos borrados y corruptos)
- https://www.cgsecurity.org/wiki/PhotoRec
- PhotoRec *is file data recovery software designed to recover lost files including video, documents and archives from hard disks, CD-ROMs, and lost pictures (thus the Photo Recovery name) from digital camera memory. PhotoRec ignores the file system and goes after the underlying data, so it will still work even if your media's file system has been severely damaged or reformatted.*

Forensics carving

- *For more safety, PhotoRec uses read-only access to handle the drive or memory card you are about to recover lost data from.*
- *Important: As soon as a picture or file is accidentally deleted, or you discover any missing, do NOT save any more pictures or files to that memory device or hard disk drive; otherwise you may overwrite your lost data.*

Forensics carving

- Instalamos primero dependencias: sudo apt install testdisk
- Arrancamos photorec: sudo photorec
- Va a identificar todos los discos que están montados (internos y externos)
- Luego elijo el disco y dónde quiero guardar los ficheros recuperados

Forensics carving

Universidad Francisco de Vitoria UFV Madrid

- Probarlo con un pendrive conectado a nuestro equipo, para ver qué recupera o con nuestra imagen bajada de Internet.

Análisis de archivos

Universidad Francisco de Vitoria UFV Madrid

- Ahora vamos a analizar una imagen obtenida mediante dc3dd o FTK Imager
- Herramienta: Bulk extractor
  - man bulk_extractor
- Escanea una imagen de disco para buscar en él expresiones (direcciones de mail, direcciones de una calle, etc…) ya predefinidas
- Lo arranco en el menu forensics

Análisis de archivos

Universidad Francisco de Vitoria UFV Madrid

- Me bajo la imagen de digitalcorpora (nps-2009-canon2)
- Me bajo el primer fichero (E01)
- Uso: bulk_extractor –o /tmp nombre_fichero.E01
- Salida: varios ficheros con la búsqueda predefinida
  - ccn.txt – credit card number
  - telephone.txt