Recuperación de datos con software libre

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

13 de Julio de 2006

Recuperación de datos con software libre

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Introducción

Hardware

Adquisición de datos

Análisis de discos y particiones

Anális del sistema de ficheros

Bibliografía

Enlaces de interés

Recuperación de datos con software libre

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

¿Qué es el análisis digital forense?

El anális digital forense es una disciplina que investiga, en analogía a los estudios médicos forenses, delitos y *fenómenos atípicos* en los sistemas informáticos: intrusiones, pérdida de datos, etc.

La variedad de hardware y software, y la cantidad de escenarios posibles, hacen dificil poder dar soluciones específicas para todos los casos, pero sí líneas generales de proceder en la adquisición y análisis de la información en peligro.

Recuperación de datos con software libre

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

¿Qué es el análisis digital forense?

El anális digital forense es una disciplina que investiga, en analogía a los estudios médicos forenses, delitos y *fenómenos atípicos* en los sistemas informáticos: intrusiones, pérdida de datos, etc.
La variedad de hardware y software, y la cantidad de escenarios posibles, hacen dificil poder dar soluciones específicas para todos los casos, pero sí líneas generales de proceder en la adquisición y análisis de la información en peligro.

Recuperación de datos con software libre

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Software libre e investigación forense

El software libre que permite este procedimiento tiene las ventajas sobre el privativo de ser extensible para según que casos, y más fácilmente auditable, con las consecuencias legales que eso tiene.

Como parte de la investigación forense, la recuperación de información en los sistemas investigados es esencial.

Esta charla se centrará en arquitecturas i386, trabajaremos sobre GNU/Linux con ideas relativas a recuperación en dispositivos de almacenamiento no volátil (discos duros, llaveros USB...).

Recuperación de datos con software libre

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Software libre e investigación forense

El software libre que permite este procedimiento tiene las ventajas sobre el privativo de ser extensible para según que casos, y más fácilmente auditable, con las consecuencias legales que eso tiene.
Como parte de la investigación forense, la recuperación de información en los sistemas investigados es esencial.
Esta charla se centrará en arquitecturas i386, trabajaremos sobre GNU/Linux con ideas relativas a recuperación en dispositivos de almacenamiento no volátil (discos duros, llaveros USB...).

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Software libre e investigación forense

El software libre que permite este procedimiento tiene las ventajas sobre el privativo de ser extensible para según que casos, y más fácilmente auditable, con las consecuencias legales que eso tiene.
Como parte de la investigación forense, la recuperación de información en los sistemas investigados es esencial.
Esta charla se centrará en arquitecturas i386, trabajaremos sobre GNU/Linux con ideas relativas a recuperación en dispositivos de almacenamiento no volátil (discos duros, llaveros USB...).

Recuperación de datos con software libre

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Unas notas sobre hardware (I)

- Identificar claramente la marca, modelo y características del dispositivo a investigar:
  - posibilidad de incompatibilidades con el hardware de laboratorio (limitaciones de BIOS, diferentes modelos de SCSI...)
  - posibilidad de defectos de serie
- Si es preciso, test de hardware: **smartmontools**,**badblocks** (¡solo lectura!).

Recuperación de datos con software libre

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Unas notas sobre hardware (I)

- Identificar claramente la marca, modelo y características del dispositivo a investigar:
  - posibilidad de incompatibilidades con el hardware de laboratorio (limitaciones de BIOS, diferentes modelos de SCSI...)
  - posibilidad de defectos de serie
- Si es preciso, test de hardware: **smartmontools**,**badblocks** (¡solo lectura!).

Recuperación de datos con software libre

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Unas notas sobre hardware (I)

- Identificar claramente la marca, modelo y características del dispositivo a investigar:
  - posibilidad de incompatibilidades con el hardware de laboratorio (limitaciones de BIOS, diferentes modelos de SCSI...)
  - posibilidad de defectos de serie
- Si es preciso, test de hardware: **smartmontools**,**badblocks** (¡solo lectura!).

Recuperación de datos con software libre

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Unas notas sobre hardware (I)

- Identificar claramente la marca, modelo y características del dispositivo a investigar:
  - posibilidad de incompatibilidades con el hardware de laboratorio (limitaciones de BIOS, diferentes modelos de SCSI...)
  - posibilidad de defectos de serie
- Si es preciso, test de hardware: **smartmontools**,**badblocks** (¡solo lectura!).

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Unas notas sobre hardware (y II)

- En discos duros, la muerte de la controladora y demás, se puede solventar:
  - Reemplazándola si es posible, reconectando/resoldando el cableado
  - Reemplazando toda la carcasa: muy peligroso (pero barato)
  - Enviándolo a empresas especializadas. Actualmente hay dos o tres en toda España con cámaras especiales para desmontarlos.
- En dispositivos USB si hay un problema de hardware... a rezar

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Unas notas sobre hardware (y II)

- En discos duros, la muerte de la controladora y demás, se puede solventar:
  - Reemplazándola si es posible, reconectando/resoldando el cableado
  - Reemplazando toda la carcasa: muy peligroso (pero barato)
  - Enviándolo a empresas especializadas. Actualmente hay dos o tres en toda España con cámaras especiales para desmontarlos.
- En dispositivos USB si hay un problema de hardware... a rezar

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Unas notas sobre hardware (y II)

- En discos duros, la muerte de la controladora y demás, se puede solventar:
  - Reemplazándola si es posible, reconectando/resoldando el cableado
  - Reemplazando toda la carcasa: muy peligroso (pero barato)
  - Enviándolo a empresas especializadas. Actualmente hay dos o tres en toda España con cámaras especiales para desmontarlos.
- En dispositivos USB si hay un problema de hardware... a rezar

Recuperación de datos con software libre

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Unas notas sobre hardware (y II)

- En discos duros, la muerte de la controladora y demás, se puede solventar:
  - Reemplazándola si es posible, reconectando/resoldando el cableado
  - Reemplazando toda la carcasa: muy peligroso (pero barato)
  - Enviándolo a empresas especializadas. Actualmente hay dos o tres en toda España con cámaras especiales para desmontarlos.
- En dispositivos USB si hay un problema de hardware... a rezar

Recuperación de datos con software libre

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Decisiones

- Acceso através de BIOS (limitaciones INT13h) o directo al disco (Linux)
- Análisis en vivo (riesgo de pérdida/sobreescritura de más información) o en muerto (pérdida de la información de la memoria principal)
- Volcado de la información a disco(hay que delimitar el fin de la imagen) o a fichero (mucho más cómodo y habitual)
- Formato de la imagen embebido (algunas herramientas privativas) o *raw* (crudo) (dd, dcfldd,...)
- Imagen comprimida o no
- *to hash or no to hash*

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Decisiones

- Acceso através de BIOS (limitaciones INT13h) o directo al disco (Linux)
- Análisis en vivo (riesgo de pérdida/sobreescritura de más información) o en muerto (pérdida de la información de la memoria principal)
- Volcado de la información a disco(hay que delimitar el fin de la imagen) o a fichero (mucho más cómodo y habitual)
- Formato de la imagen embebido (algunas herramientas privativas) o *raw* (crudo) (dd, dcfldd,...)
- Imagen comprimida o no
- *to hash or no to hash*

Recuperación de datos con software libre

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Decisiones

- Acceso através de BIOS (limitaciones INT13h) o directo al disco (Linux)
- Análisis en vivo (riesgo de pérdida/sobreescritura de más información) o en muerto (pérdida de la información de la memoria principal)
- Volcado de la información a disco(hay que delimitar el fin de la imagen) o a fichero (mucho más cómodo y habitual)
- Formato de la imagen embebido (algunas herramientas privativas) o *raw* (crudo) (dd, dcfldd,...)
- Imagen comprimida o no
- *to hash or no to hash*

Recuperación de datos con software libre

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Decisiones

- Acceso através de BIOS (limitaciones INT13h) o directo al disco (Linux)
- Análisis en vivo (riesgo de pérdida/sobreescritura de más información) o en muerto (pérdida de la información de la memoria principal)
- Volcado de la información a disco(hay que delimitar el fin de la imagen) o a fichero (mucho más cómodo y habitual)
- Formato de la imagen embebido (algunas herramientas privativas) o *raw* (crudo) (dd, dcfldd,...)
- Imagen comprimida o no
- *to hash or no to hash*

Recuperación de datos con software libre

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Decisiones

- Acceso através de BIOS (limitaciones INT13h) o directo al disco (Linux)
- Análisis en vivo (riesgo de pérdida/sobreescritura de más información) o en muerto (pérdida de la información de la memoria principal)
- Volcado de la información a disco(hay que delimitar el fin de la imagen) o a fichero (mucho más cómodo y habitual)
- Formato de la imagen embebido (algunas herramientas privativas) o *raw* (crudo) (dd, dcfldd,...)
- Imagen comprimida o no
- *to hash or no to hash*

Recuperación de datos con software libre

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Decisiones

- Acceso através de BIOS (limitaciones INT13h) o directo al disco (Linux)
- Análisis en vivo (riesgo de pérdida/sobreescritura de más información) o en muerto (pérdida de la información de la memoria principal)
- Volcado de la información a disco(hay que delimitar el fin de la imagen) o a fichero (mucho más cómodo y habitual)
- Formato de la imagen embebido (algunas herramientas privativas) o *raw* (crudo) (dd, dcfldd,...)
- Imagen comprimida o no
- *to hash or no to hash*

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Herramientas (I)

- dd: un clásico
  http://www.gnu.org/software/coreutils/
- ddrescue: versión de dd para recuperación de datos
  http://www.gnu.org/software/ddrescue/ddrescue.html
- dd_rescue: tamaño de bloque dinámico y marcha atrás
  http://www.garloff.de/kurt/linux/ddrescue/

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Herramientas (I)

- dd: un clásico
  http://www.gnu.org/software/coreutils/
- ddrescue: versión de dd para recuperación de datos
  http://www.gnu.org/software/ddrescue/ddrescue.html
- dd_rescue: tamaño de bloque dinámico y marcha atrás
  http://www.garloff.de/kurt/linux/ddrescue/

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Herramientas (I)

- dd: un clásico
  http://www.gnu.org/software/coreutils/
- ddrescue: versión de dd para recuperación de datos
  http://www.gnu.org/software/ddrescue/ddrescue.html
- dd_rescue: tamaño de bloque dinámico y marcha atrás
  http://www.garloff.de/kurt/linux/ddrescue/

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Herramientas (y II)

- dcfldd: suma md5 *on the fly*, posibilidad de troceado de imágenes
  http://dcfldd.sourceforge.net/
- sdd: reescritura de dd, más rápido, tamaño de bloque de entrada diferente al de salida
  http://directory.fsf.org/sysadmin/Backup/sdd.html
- Automated Image and Restore (AIR): front-end para dd y dcfldd

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Herramientas (y II)

- dcfldd: suma md5 *on the fly*, posibilidad de troceado de imágenes
  http://dcfldd.sourceforge.net/
- sdd: reescritura de dd, más rápido, tamaño de bloque de entrada diferente al de salida
  http://directory.fsf.org/sysadmin/Backup/sdd.html
- Automated Image and Restore (AIR): front-end para dd y dcfldd

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail:
tsao@enelparaiso.org

Herramientas (y II)

- dcfldd: suma md5 *on the fly*, posibilidad de troceado de imágenes
  http://dcfldd.sourceforge.net/
- sdd: reescritura de dd, más rápido, tamaño de bloque de entrada diferente al de salida
  http://directory.fsf.org/sysadmin/Backup/sdd.html
- Automated Image and Restore (AIR): front-end para dd y dcfldd

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail:
tsao@enelparaiso.org

Parámetros más relevantes de dd

```
dd if=a of=b bs=n skip=m count=l
conv=parametro1, parámetro 2...
```

- a=fichero/dispositivo de entrada
- b=fichero/dispositivo de salida
- n=tamaño de bloque (de 2 a 8 K, por defecto 512 bytes (tamaño de bloque))
- m=número de bloques que evita antes de empezar a leer
- l=numero de bloques que lee
- parámetros:
  - noerror: no se detiene cuando hay error de lectura
  - sync:mantiene la numeración original

Recuperación de datos con software libre

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Parámetros más relevantes de dd

```
dd if=a of=b bs=n skip=m count=l
conv=parametro1, parámetro 2...
```

- a=fichero/dispositivo de entrada
- b=fichero/dispositivo de salida
- n=tamaño de bloque (de 2 a 8 K, por defecto 512 bytes (tamaño de bloque))
- m=número de bloques que evita antes de empezar a leer
- l=numero de bloques que lee
- parámetros:
  - noerror: no se detiene cuando hay error de lectura
  - sync:mantiene la numeración original

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Parámetros más relevantes de dd

```
dd if=a of=b bs=n skip=m count=l
conv=parametro1, parámetro 2...
```

- a=fichero/dispositivo de entrada
- b=fichero/dispositivo de salida
- n=tamaño de bloque (de 2 a 8 K, por defecto 512 bytes (tamaño de bloque))
- m=número de bloques que evita antes de empezar a leer
- l=numero de bloques que lee
- parámetros:
  - noerror: no se detiene cuando hay error de lectura
  - sync:mantiene la numeración original

Recuperación de datos con software libre

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Parámetros más relevantes de dd

```
dd if=a of=b bs=n skip=m count=l
conv=parametro1, parámetro 2...
```

- a=fichero/dispositivo de entrada
- b=fichero/dispositivo de salida
- n=tamaño de bloque (de 2 a 8 K, por defecto 512 bytes (tamaño de bloque))
- m=número de bloques que evita antes de empezar a leer
- l=numero de bloques que lee
- parámetros:
  - noerror: no se detiene cuando hay error de lectura
  - sync:mantiene la numeración original

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Parámetros más relevantes de dd

```
dd if=a of=b bs=n skip=m count=l
conv=parametro1, parámetro 2...
```

- a=fichero/dispositivo de entrada
- b=fichero/dispositivo de salida
- n=tamaño de bloque (de 2 a 8 K, por defecto 512 bytes (tamaño de bloque))
- m=número de bloques que evita antes de empezar a leer
- l=numero de bloques que lee
- parámetros:
  - noerror: no se detiene cuando hay error de lectura
  - sync:mantiene la numeración original

Recuperación de datos con software libre

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Parámetros más relevantes de dd

```
dd if=a of=b bs=n skip=m count=l
conv=parametro1, parámetro 2...
```

- a=fichero/dispositivo de entrada
- b=fichero/dispositivo de salida
- n=tamaño de bloque (de 2 a 8 K, por defecto 512 bytes (tamaño de bloque))
- m=número de bloques que evita antes de empezar a leer
- l=numero de bloques que lee
- parámetros:
  - noerror: no se detiene cuando hay error de lectura
  - sync:mantiene la numeración original

Recuperación de datos con software libre

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Parámetros más relevantes de dd

```
dd if=a of=b bs=n skip=m count=l
conv=parametro1, parámetro 2...
```

- a=fichero/dispositivo de entrada
- b=fichero/dispositivo de salida
- n=tamaño de bloque (de 2 a 8 K, por defecto 512 bytes (tamaño de bloque))
- m=número de bloques que evita antes de empezar a leer
- l=numero de bloques que lee
- parámetros:
  - noerror: no se detiene cuando hay error de lectura
  - sync:mantiene la numeración original

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Chequeo y recuperación de particiones(I)

Además del análisis físico de los dispositivos, puede resultar recomendable/necesario una revisión del estado lógico de la información:

- Estabilidad de particiones (espacios sin asignación, solapamientos...):
  `TSK: mmls -t tipo -r unidad`
  - tipo:dos, bsd,...
  - unidad: volumen/partición/imagen de volumen

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Chequeo y recuperación de particiones(y II)

- Pérdida de la tabla de particiones:
  `gpart -v unidad`
  Hace un scan sobre toda la unidad intentando reconstruir la estructura
  `gpart -W unidad2 unidad1`
  Escribe la (presunta) tabla de particiones de la unidad 1 en la unidad2 (que puede ser la misma: *"This of course may be extremely dangerous to your health and social security, so beware."*)

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Categorías de datos

Brian Carrier define cinco categorías de datos para organizar la investigación:

- Categoría del **sistema de ficheros**: distribución de la información. Vg., en ext3: superbloque, descriptor de grupo
- Categoría de **contenido**: información contenida en los ficheros: el contenido y el estado de los bloques
- Categoría de **metadatos**: descripción de los ficheros: accessos y localización
- Categoría de **nombres**: entradas en directorios, enlaces, puntos de montaje...
- Categoría de **aplicación**: información adicional a la gestión de ficheros: journal

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Categorías de datos

Brian Carrier define cinco categorías de datos para organizar la investigación:

- Categoría del **sistema de ficheros**: distribución de la información. Vg., en ext3: superbloque, descriptor de grupo
- Categoría de **contenido**: información contenida en los ficheros: el contenido y el estado de los bloques
- Categoría de **metadatos**: descripción de los ficheros: accessos y localización
- Categoría de **nombres**: entradas en directorios, enlaces, puntos de montaje...
- Categoría de **aplicación**: información adicional a la gestión de ficheros: journal

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Categorías de datos

Brian Carrier define cinco categorías de datos para organizar la investigación:

- Categoría del **sistema de ficheros**: distribución de la información. Vg., en ext3: superbloque, descriptor de grupo
- Categoría de **contenido**: información contenida en los ficheros: el contenido y el estado de los bloques
- Categoría de **metadatos**: descripción de los ficheros: accessos y localización
- Categoría de **nombres**: entradas en directorios, enlaces, puntos de montaje...
- Categoría de **aplicación**: información adicional a la gestión de ficheros: journal

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Categorías de datos

Brian Carrier define cinco categorías de datos para organizar la investigación:

- Categoría del **sistema de ficheros**: distribución de la información. Vg., en ext3: superbloque, descriptor de grupo
- Categoría de **contenido**: información contenida en los ficheros: el contenido y el estado de los bloques
- Categoría de **metadatos**: descripción de los ficheros: accessos y localización
- Categoría de **nombres**: entradas en directorios, enlaces, puntos de montaje...
- Categoría de **aplicación**: información adicional a la gestión de ficheros: journal

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Categorías de datos

Brian Carrier define cinco categorías de datos para organizar la investigación:

- Categoría del **sistema de ficheros**: distribución de la información. Vg., en ext3: superbloque, descriptor de grupo
- Categoría de **contenido**: información contenida en los ficheros: el contenido y el estado de los bloques
- Categoría de **metadatos**: descripción de los ficheros: accessos y localización
- Categoría de **nombres**: entradas en directorios, enlaces, puntos de montaje...
- Categoría de **aplicación**: información adicional a la gestión de ficheros: journal

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Técnicas principales de recuperación de archivos

- basadas en metadatos: búsqueda de la situación de los bloques de información
- basadas en aplicación: búsqueda por tipos de ficheros, *data carving*, por journal

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Técnicas principales de recuperación de archivos

- basadas en metadatos: búsqueda de la situación de los bloques de información
- basadas en aplicación: búsqueda por tipos de ficheros, *data carving*, por journal

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Herramientas (I)

- generales:
  - The Coroner's Toolkit (TCT)
  - The Sleuth Kit + Autopsy

Herramientas (y II)

- *data carving*
  - foremost:United States Air Force Office of Special Investigations and The Center for Information Systems Security Studies and Research, http://foremost.sourceforge.net/ `foremost -o directoriovacio -c ficherodeconfiguracion unidad`
  - lazarus: TCT

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Libros

- Carrier, B., *"File System Forensics Analysis"*, Addison Wesley, 2005
- Farmer, D., W. Venema, *"Forensic Discovery"*, Addison Wesley, 2004

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Artículos

- Card, R., Ts'o, T., Tweedie, S. *"Design and Implementation of the Second Extended Filesystem"*, http://web.mit.edu/tytso/www/linux/ext2intro.html
- Carrier, B., *"Why Recovering a Deleted Ext3 File is Difficult..."*, Linuxworld Magazine, 12 de agosto de 2005 (http://linux.sys-con.com/read/117909.htm)
- Tweedie,S. *"EXT3, Journaling Filesystem"*, transcripción de la ponencia 20 de julio de 2000, http://olstrans.sourceforge.net/release/OLS2000-ext3/OLS2000-ext3.html

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail: tsao@enelparaiso.org

Enlaces de interés (I)

- The Sleuth Kit:
  http://www.sleuthkit.org/
- The Coroner's Toolkit:
  http://www.porcupine.org/forensics/tct.html
- Open Source Digital Forensics
  http://www.opensourceforensics.org/
- Penguin Sleuth:
  http://www.linux-forensics.com/
- Proyecto Necromantux:
  http://necromantux.gpul.org

Recuperación de datos con software libre

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail:
tsao@enelparaiso.org

Enlaces de interés (y II)

- Página personal de Brian Carrier:
  http://www.digital-evidence.org
- Página personal de Wietse Zweitze Venema:
  http://www.porcupine.org
- Página personal de Dan Farmer:
  http://www.fish2.com/
- The Sleuth Kit Informer:
  http://www.sleuthkit.org/informer/index.php
- Electronic Evidence Information Center:
  http://www.e-evidence.info/
- Forensics.nl:
  http://forensics.nl
- SecurityFocus (listas de correo de análisis forense):

Recuperación de datos con software libre

Francisco Javier Tsao Santín
Grupo de Programadores y Usuarios de Linux-Coruña
Linux Users Group (GPUL-CLUG)
e-mail:
tsao@enelparaiso.org