Análisis forense con herramientas GPL.

Para la Linuv Party 2005.

Angel Alonso Párrizas
Miguel Colomer Pastor

13 de Marzo de 2005

1. Introducción.

1.1. ¿Qué es el análisis forense?

- Se realiza a *posteriori*.
- Motivos:
  - Análisis de causas.
  - Recolección de pruebas.
- Es necesario el sistema de ficheros a examinar.
- Se debe analizar en un entorno limpio e independiente.
- Resumen de procedimiento.
  - Extraer imagen de los sistemas de ficheros.
  - Asegurar la integridad de la imagen.
  - Llevar el sistema de ficheros al entorno de análisis.
  - Buscar evidencias o causas de fallos.

1.2. ¿Por qué usar herramientas GPL?

- Validez legal.
- Es posible comprobar la integridad de las evidencias.
- Flexibilidad y adaptabilidad.

2. Sleuthkit.

- Sistemas de ficheros soportados:
  - NTFS, FAT.
  - ext2, ext3
  - bsdi, netbsd, openbsd
  - solaris
  - Swap Raw
- Herramientas a nivel de usuario.
- Permite recuperación de ficheros borrados.
- Permite consultar fechas de modificacion, acceso y cambio (mac).
- Permite realizar líneas de tiempo.

- Descripción de comandos básicos:
  - icat: muestra el contenido de un fichero a partir del nodo-i.
  - fls: lista ficheros y directorios de una imagen.
  - istat: muestra los detalles del fichero a partir del nodo-i.
  - mactime: genera una línea de tiempos mac.

3. Autopsy.

- Interfaz web para el análisis forense.
- Utiliza comandos sleuthkit.
- Permite navegar por los sistemas de ficheros.
- Permite mostrar la línea de tiempo.
- Permite descargar ficheros y realizar strings.

4. Referencias.

http://www.sleuthkit.org/
http://www.sleuthkit.org/autopsy/index.php