Recuperación de Archivos en Linux Como Apoyo a la Informática Forense

Diego Andrés Guerrero Aguirre - Víctor Andrés Mejía Silva
Directora: Ingeniera Claudia Patricia Santiago Cely

Abstract:
One part of the forensic Computer Science is the files recovery when an informatics crime has been occurred.

Because of the lack of tools to recover files in the Linux Operating System, this project has the intention to build one completely free, or to analyze an existing one if there's one already constructed, in any of those cases the "Manuales y procedimientos de buenas prácticas en informática forénse para la ECI" (Manuals and procedures of forensic good practices to the ECI) project will be followed and analyzed.

Palabras claves: Recuperación de archivos, Linux, sistema de archivos, VFS (Sistema virtual de archivos), informática forense.

I. INTRODUCCIÓN

Observando el creciente uso de plataformas Linux a nivel mundial, la importancia que la información tiene hoy en día, a nivel personal y más aún a nivel empresarial, el objetivo criminal en el que la información se a convertido y teniendo en cuenta que no hay una seguridad inquebrantable, surge la necesidad de implementar métodos que permitan, no solo reestablecer el estado normal de un sistema después de haber sido víctima de un atentado, si no que también den la posibilidad de saber las causas para ejecutar acciones correctivas y si es posible conocer los responsables de este hecho; es en este punto donde la Informática Forense juega un papel fundamental, así como también lo juegan las herramientas que la apoyan.

Tomando como referencia el documento Manual y Procedimientos de Buenas Prácticas en Informática Forense para la ECI, el cual deja ver una escasez de herramientas recuperadoras de archivos que sean libres bajo la plataforma Linux, y siendo este tipo de aplicaciones fundamental en el proceso de recolección de pruebas y reestablecimiento de sistemas en la Informática Forense, se hace necesario; contar con una herramienta con estas características y además, que sea funcional en cualquier distribución Linux o cuando menos en las mas importantes.

II. ANTECEDENTES

Este proyecto de grado nació después de la construcción del Manual y Procedimientos de Buenas Prácticas en Informática Forense para la ECI, que es el producto final de un proyecto de grado desarrollado por estudiantes ya egresados de la Escuela de Ingeniería, bajo la dirección de la ingeniera Claudia P. Santiago en el transcurso de año 2005, el

cual muestra entre otras cosas, el resultado de una búsqueda de herramientas para la recuperación de archivos en los sistemas operativos Windows y Linux; tal resultado indica una aparente escasez de este tipo de herramientas para Linux que sean de licencia GNU GPL. Por lo cual no se logró saber a ciencia cierta que tan factible es hacer la recuperación de archivos en este sistema operativo.

Con este artículo se pretende dar a conocer el proceso de evolución del proyecto de grado *Herramientas para la recuperación de archivos en Linux;* para esto se hará una descripción y explicación general de los puntos más relevantes y significativos del proyecto (objetivos, desarrollo del proyecto, producto), y de esta forma mostrar las razones por las cuales se toman las diferentes decisiones a lo largo del mismo.

III. OBJETIVO

Obtener una aplicación que permita realizar recuperaciones de archivos sobre el sistema operativo Linux enfocado al apoyo de la consecución de pruebas de un delito de informática y validar los procedimientos previamente definidos por el proyecto de grado mencionado anteriormente, en este tipo de ambientes.

Como objetivos específicos se tienen:

- Definir los requerimientos de la herramienta basados en un proyecto de grado anterior y aplicaciones similares en ambientes Windows.
- Obtener una aplicación para la recuperación de archivos sobre el sistema operativo Linux, ya sea encontrándola o bien desarrollándola, que tenga un especial enfoque hacia la informática forense siguiendo con los estándares que para este tipo de aplicaciones se encuentran vigentes.
- Validar los procedimientos definidos en el proyecto de grado "Manuales y Procedimientos de Buenas Prácticas en Informática Forense para la ECI".

IV. DESARROLLO DEL PROYECTO

Se buscó en primera instancia recopilar información, por medio de una investigación exhaustiva, la cual resultó ser mas larga de lo planeado en un principio; sin embargo, esta extensión de tiempo fue necesaria, ya que a medida que se iba avanzando en la investigación surgían nuevas variables que tenían que ser tomadas en cuenta para los fines del proyecto. Por ejemplo, en un principio se pensó que un posible problema que podía surgir en la obtención de la herramienta era que fuera funcional sobre cualquier distribución Linux, pero en el proceso nos dimos cuenta que este no era el problema en realidad, ya que las diferentes distribuciones usan el mismo Kernel y por lo tanto una estructura de archivos común, el verdadero problema era que la herramienta funcionara sobre los distintos sistemas de archivos soportados por los sistemas Linux.

Haciendo un resumen de lo arrojado por la investigación se tiene lo siguiente: Los sistemas Linux están en capacidad de usar una gran cantidad de sistemas de archivos (ej. Ext2, Ext3, ReiserFS, NTFS, etc.),

gracias a que el kernel provee un módulo llamado sistema virtual de archivos (Virtual File System o VFS); esta capa de software, provee una serie de interfaces que permiten a las aplicaciones de usuario interactuar con cualquier sistema de archivos que se adapte a las interfaces que el VFS provee para los sistemas de archivos concretos (*ver figura 1*). Además de esto el VFS implementa una serie de estructuras u objetos, en las cuales se implementan las funciones básicas que cualquier sistema de archivos debería tener; sin embargo esta funcionalidad general abarcada por el VFS no incluye lo necesario para realizar la recuperación de archivos de la forma tradicional, que es usar la información de gestión de espacio libre del dispositivo.

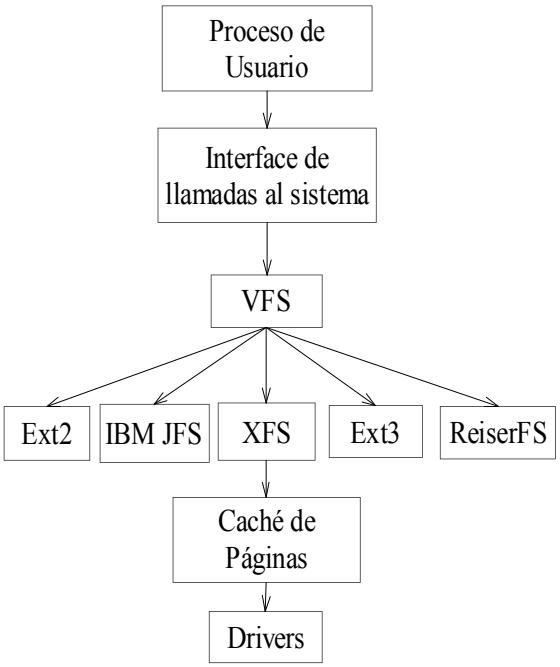

Figura 1. Entorno del VFS:

Pero sin duda alguna, lo más destacado de lo obtenido de la investigación realizada, es que se encontró que existen dos métodos de hacer la recuperación de archivos los cuales se explican de forma resumida a continuación:

- **Basados en la estructura del sistema de archivos:** Este es el más usado y conocido. Como su nombre lo indica, en ésta forma de recuperar los archivos se usan las estructuras del sistema de archivos, más específicamente el *Gestor de Espacio Libre* del sistema de archivos, para obtener información de los archivos que han sido borrados y usa dicha información para ubicar la información perdida.

  Aunque las herramientas que usan este método son relativamente rápidas, estas tienen varias desventajas, una de ellas es que son dependientes de algún sistema de archivos específico; esto quiere decir que si recupera en el sistema de archivos Ext2, no es capaz de recuperar en JSF por ejemplo, a no ser que la herramienta cuente con la una implementación diferente para hacer la recuperación sobre cada sistema de archivo. Esto se debe a que cada sistema de archivos, aunque tienen características comunes, gestiona de manera particular los archivos sobre el dispositivo de almacenamiento; otra desventaja importante es que no son capaces de recuperar los archivos después que se ha hecho formateo lógico del dispositivo. En la *figura 2* se muestran algunas de las herramientas de recuperación de archivos basadas en las estructuras del sistema de archivos.

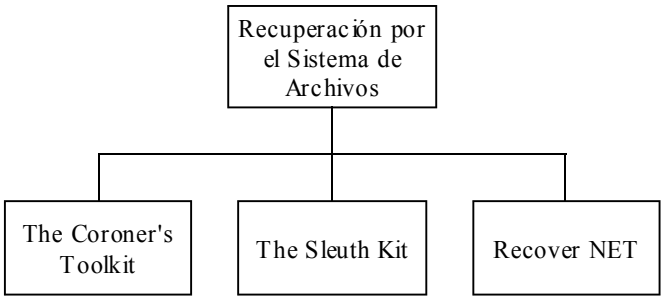

Figura 2. Herramientas de recuperación de archivos basadas en la estructura del sistema de archivos.

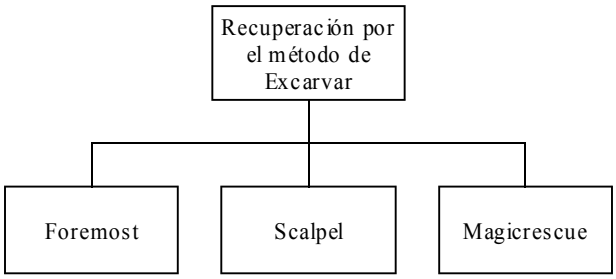

Figura 3. Herramientas de recuperación de archivos basadas en el método de excavar.

Método de Excavar: Este método por el contrario del anterior no es muy conocido, sin embargo desde el punto de vista de la informática forense es el mas efectivo, ya que aquí la rapidez con el que se recupere la información no es lo mas relevante, si no que lo que realmente importa es recuperar la mayor cantidad de información borrada, y en esto este tipo de herramientas son muy superiores a las basadas en las estructuras del sistema de archivos, además de esto, con este método no importa el sistema de archivos ya que trabaja a un nivel mas bajo, haciendo búsquedas de bajo nivel "excavaciones" sobre el dispositivo, con el fin de encontrar patrones de bytes que coincidan con el tipo(s) de documento(s) buscado(s), y es por esta razón que son capaces de hacer la recuperación aún después de haber formateado lógicamente el dispositivo de almacenamiento, algo que tampoco es posible con el método antes mencionado. En la *figura 3* se muestran algunas de las herramientas de recuperación de archivos que usan el método de excavar.

Para los dos métodos de recuperación de archivos, se encontraron herramientas, sobre las cuales se hicieron las debidas pruebas y evaluaciones, y cuyos resultados corroboraron lo dicho anteriormente en la descripción de cada uno de ellos.

V. ESTADO ACTUAL DEL PROYECTO

Como se pudo observar, en el desarrollo del proyecto, se logró encontrar una serie de herramientas de recuperación de archivos de licencia GNU GPL para los diferentes métodos de hacer esta tarea, sin embargo, a todas ellas, les hace falta tener un enfoque hacia la informática forense, que hace parte de uno de los objetivos del proyecto. Es por esta razón que en este momento nos encontramos en el terminando el desarrollo de una herramienta llamada *El Recuperador,* la cual pretende cumplir con dicho enfoque y aprovechar las fortalezas o bondades de cada una de las herramientas de recuperación encontradas y todas aquellas que tengan la posibilidad de ser ejecutadas por línea de comandos.

El Recuperador, permite integrar herramientas de recuperación de archivos

ya sean basadas en las estructuras del sistema de archivos o basadas en el método de excavar, dando la facilidad de usar una gran variedad de herramientas y de esta forma tener mejores resultados en el momento de la consecución de evidencia en algún delito informático.

Dado que *El Recuperador* tiene un enfoque a la informática forense, este permite administrar los casos de investigación en donde se ven involucrados dispositivos de almacenamiento cuya información ha sido borrada de forma lógica. A dichos dispositivos se les hará un proceso de recuperación por medio de alguna o varias de las herramientas de recuperación de archivos integradas a el, siendo alguno o varios investigadores forenses los encargados de ejecutar las operaciones sobre dicho dispositivo, con el fin de obtener evidencia, y de esta forma asociarla al caso de investigación correspondiente.

Figura 4. Funcionamiento de *El Recuperador*

VI. REFERENCIAS

- Understanding The Linux Kernel 2nd / Daniel P. Bovet, Marco Cesati. Ed. O'Reilly Diciembre 2002
- Sistemas Operativos Quinta Edición / Willinam Stallings. Ed. Pearson. 2005
- El Linux Virtual File System, Juan Antonio Martínez En:http://es.tldp.org/Articulos-periodisticos/jantonio/ en 25/Agosto/2006

Víctor Andrés Mejía, Estudiante de décimo semestre de Ingeniería de Sistemas de la Escuela Colombiana de Ingeniería, participante a lo largo de la carrera en el desarrollo de diversos proyectos entre los más destacados están: SME "Desarrollo de un Sistema Manejador de Encuestas para Mercadatos" donde se encargó del diseño y construcción de dos casos de uso.
FWJDC "Desarrollo de un Framework de Juegos Discretos con Contrincante", desarrollado en el Segundo semestre del 2005, es otro proyecto que tuvo un gran éxito, en el cual desempeñó el rol de Líder de Desarrollo.
También cuenta con experiencia trabajando con las soluciones JES Directory Server (implementación de LDAP de Sun) y JES Messaging Server.
vamsp7@yahoo.com

Diego Andrés Guerrero Aguirre, Estudiante de décimo semestre de Ingeniería de Sistemas de la Escuela Colombiana de Ingeniería, constante investigador de las diferentes ramas de la computación, y tecnologías, certificado en "Computer Fundamentals (Win XP)" en Marzo de 2003, participante de varios proyectos de software libre desarrollados como estudiante de La Escuela Colombiana de Ingeniería, tales como lo son la construcción de un portal para publicación de proyectos de Software Libre, construido para Noviembre de 2005, desarrollador de SSConstruir, sistema manejador de facturación para una organización no gubernamental llamada Corporación Construir (Enero – Abril 2006), participante en el diseño y desarrollo de SIPLA 2, software para el manejo de lavado de activos, construido por la empresa IBISCOM (Marzo – Abril 2006).
diego.guerrero.a@gmail.com.