ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN

INFORME DE MATERIA DE GRADUACIÓN

"AUDITORIA FORENSE DEL CASO KERICU"

Previa a la obtención del Título de:

LICENCIADO EN REDES Y SISTEMAS OPERATIVOS

Presentado por:

DIANA CAROLINA ANDRADE ROJAS

FREDDY ALBERTO GONZALES APUNTE

Guayaquil – Ecuador

2012

AGRADECIMIENTO

A Dios por ayudarnos a terminar la Universidad, gracias por darnos la fuerza y coraje para hacer nuestro sueño realidad, por estar con nosotros en cada etapa de nuestra vida.

A la Escuela Superior Politécnica del Litoral por darnos la oportunidad de alcanzar esta meta, gracias a los profesores e investigadores quienes durante estos años se esmeraron por dar lo mejor para nuestra formación profesional, por los conocimientos teóricos y las experiencias vividas.

A nuestros padres por sus apoyos incondicionales y sus presiones para lograr nuestras metas.

DEDICATORIA

A Dios, por estar siempre conmigo dándome las fuerzas necesarias para salir adelante todos los días.

A mis padres por todo lo que me han dado en la vida, por su gran apoyo, por su confianza y por ser los pilares fundamentales en mi vida personal y profesional.

A mis profesores por transmitirme sus conocimientos y ayudarme en lo largo de la carrera.

Diana Andrade R.

DEDICATORIA

A Dios por permitirme realizar todos mis estudios y poder terminar con éxito.

A mi familia por estar siempre apoyándome en los momentos difíciles durante mis estudios Universitarios, y por los buenos principios que me enseñaron.

A los profesores que tuve, muchas gracias por haberme brindado sus experiencias y conocimientos, ya que estos me ayudaran en la vida profesional.

Freddy Gonzales A.

D E C L A R A C I Ó N E X P R E S A

“La responsabilidad del contenido de este Informe de Grado, nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral”.

(Reglamento de Graduación de la ESPOL)

_____

Diana Carolina Andrade Rojas

_____

Freddy Alberto Gonzales Apunte

T R I B U N A L D E S U S T E N T A C I O N

_____

Ing. Karina Astudillo

PROFESORA DE LA MATERIA DE GRADUACIÓN

_____

Ing. Miguel Molina

PROFESOR DELEGADO POR EL DECANO DE LA FACULTAD

RESUMEN

El proyecto de graduación consiste en realizar una auditoría de computación forense sobre una alteración de documentos financieros de la compañía Kericu, Inc., para la recuperación de información se utilizó la herramienta Autopsy, la cual nos permitió restablecer documentos e información borrada.

Tenemos el análisis de 2 unidades, un disco duro y un dispositivo usb.

En los correos electrónicos se recuperó un archivo de Excel llamado:

- ✓ “earnings.xls”

En el dispositivo usb se encontraron 2 archivos detallados a continuación:

- ✓ “earnings2.xls”
- ✓ “earnings-original.xls”

El sistema operativo que se utilizó para realizar el análisis y recuperación de los respectivos archivos es CAINE 2.0, en el cual nos proporciona herramientas forenses.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En este proyecto se tendrá como objetivo la investigación del caso asignado en la materia de graduación “CASO KERICU”, el cual tenemos que investigar y analizar archivos financieros que fueron alterados. Para esto no vamos a utilizar herramientas comunes sino que vamos a aplicar informática forense ya que hoy en día la misma está adquiriendo una gran importancia debido al aumento de equipos de cómputo y su manipulación, ya sea para bien o para mal.

Hasta cuando se realiza un crimen, la informática forense influye mucho esto, ya que muchas veces la información necesaria queda almacenada en forma digital en cualquier dispositivo informático. Sin embargo, existe un gran problema, ya dicha la información puede ser borrada de los dispositivos por cualquier usuario y esto no nos permitirá recolectar las evidencias con medios comunes, en este caso es donde la informática forense nos ayuda a recuperar todo los datos que necesitemos, siempre y cuando estos sean digitales.

Tenemos el sistema operativo caine el cual posee herramientas forenses que nos permitirán desde crear una copia de la evidencia sin alterarla hasta recuperar archivos eliminados por el usuario.

CAPITULO 1

ANTECEDENTES Y JUSTIFICACIÓN

1.1 Antecedentes

En 1984, el laboratorio del FBI empezó a desarrollar un programa para examinar evidencias computacionales, en la actualidad se lo conoce como CART (Análisis de Informática y equipo de repuesta).

El primer incidente informático fue el 22 de noviembre de 1988, un simple programa se convirtió en un virus gusano y mediante Internet afectó a muchos ordenadores conectados a la red, esto hizo que los mismos estuvieran inhabilitados durante varios días, quedando empresas sin poder laborar y personas particulares no podían realizar sus tareas comunes.

Pocas personas tomaban en cuenta la importancia que tiene la seguridad informática.

En la actualidad el administrador de sistemas informáticos tiene una gran responsabilidad ya que uno de los factores más importante es la seguridad en los sistemas operativos y las redes, desde la perspectiva del profesional responsable de esto, debe pensar como los atacantes y jamás subestimar su mentalidad, las diferentes etapas que conforman un ataque informático ayudan a obtener ventajas.

Debido a las nuevas tecnologías de la información, la computación forense hizo su aparición ya que la informática nos permite almacenar y alterar grandes cantidades de información, por otro lado el Internet nos permite comunicarnos con personas situadas en otros lugares.

La informática forense nos permite realizar una búsqueda de evidencias digitales y a su vez la reconstrucción de la misma, además de recuperar datos tenemos que considerar todo su entorno. En el ámbito de la Informática Forense se consideran varias ciencias tal como ingeniería del software, redes, electrónica, infraestructura, entre otras.

1.2 Justificación

Desde el punto de vista de persecución de delitos, la informática forense no solo se aplica en nuestro país, también a nivel interno en las empresas, principalmente con el objetivo de detectar si alguien de la misma organización realiza o ha realizado transferencias de información a terceros.

También nos permite validar la seguridad de los ordenadores que realizan las transferencias electrónicas bancarias, idéntica como se ha realizado un ataque a los servidores internos.

Al realizar un análisis forense uno de los aspectos fundamentales a considerar es la confiabilidad de la información ya que cualquier sector de un sistema podría ser modificado y tener datos falsos.

Las empresas que tienen la necesidad de llevar a cabo una investigación en el área de la seguridad informática, la solución ideal es el análisis forense, ya que permite obtener medidas adecuadas para que no vuelva a ocurrir el mismo incidente.

Para obtener la evidencia es necesario hacer uso de la computación forense ya que los fraudes ejecutados por medios tecnológicos merecen atención especial por el alto costo que estos representan para las empresas. La

mayoría de los fraudes son ejecutados por medio de una computadora y es en esta en donde queda almacenada la evidencia, por esto es importante que se cuente con personal especializado en computación forense.

1.3 Descripción del proyecto

Como un examinador forense para un laboratorio forense de delito informático de una entidad de aplicación de la ley, verá un montón de casos que van y vienen. Te has pasado el tiempo reportando violaciones, donde los ejecutivos de alto nivel alteran documentos financieros para que su empresa parezca mejor a los ojos de sus accionistas.

Kericu, Inc., es una compañía desarrolladora de hardware de telecomunicaciones, donde se vieron afectados los estados financieros de la misma. Rodger Lewis, CEO de Kericu, es conocido por sus habilidades informáticas, y ha puesto esas habilidades a mal uso. El Departamento de justicia acusó recientemente a Lewis por alterar los Estados trimestrales para aumentar las ganancias de su empresa. Lewis es conocido por tener "sk1llz" a nivel computacional ("skillz" por la comunidad informática clandestina), con esto se espera que haya limpiado sus huellas. Muy pocas pruebas de equipo pueden estar disponibles. En su experiencia, la mayoría de los medios y avanzados usuarios están conscientes de la evidencia de los software de eliminación, lo que dificulta su trabajo.

Afortunadamente, el Vicepresidente Ejecutivo de Finanzas, Aiden Paluchi, negoció un acuerdo con el Departamento de justicia. Si Paluchi testifica contra el CEO, recibirá inmunidad de cualquier cargo adicional relacionada con este caso. Paluchi suministra el Departamento de justicia un documento que dice Lewis alterado. Paluchi también dice que este documento fue enviado al personal ejecutivo todo a través de correo electrónico. Él suministra con una copia de ese correo electrónico listado aquí:

Para: executives@kericu.com

De: aiden.paluchi@kericu.com

Fecha: Jueves 03 de Julio, 2003 15:33:02 (EDT)

Asunto: Hoja de cálculo Ganancias Q2

Adjuntos: earnings.xls

Señores,

Este documento está listo para su aprobación. Por favor, enviar de vuelta e-mail con cualquier cambio que pude haber perdido. Esperemos que el próximo trimestre sea mejor que éste.

Atentamente,

Aiden Paluchi

Vicepresidente Ejecutivo de Finanzas

Kericu, Inc.

Usted viaja a la sede de la Kericu y comienza su análisis. Empezar por adquirir una duplicación forense de disco duro de ordenador portátil de Lewis utilizando DD. Revisar rápidamente la imagen para un " smoking gun". Como era de esperar, no ha visto earnings.xls en cualquier lugar en el disco duro de Lewis. Su trabajo sólo se hizo mucho más difícil de lo pensado porque tienes que hacer un análisis más profundo. Justo en ese momento, y el agente se encuentra con su oficina y golpea abajo de un dispositivo de memoria USB que se encontró en casa de Lewis. Esperemos que, después de adquirir una duplicación forense del dispositivo, puede encontrar evidencia adicional del crimen de Lewis.

1.3.1 Objetivo general

Realizar una Auditoria Forense del Caso KERICU. Nuestro objetivo abarca el análisis profundo de las copias de las evidencia del disco duro y del dispositivo usb, esto nos permitirá llegar a una conclusión con el responsable de todo.

1.3.2 Objetivos específicos

- ✓ Adquirir una duplicación forense de disco duro del ordenador portátil de Lewis y su USB utilizando DD.

- ✓ Mantener la integridad de los datos sin ninguna alteración. Para esto debemos trabajar con copias bit a bit, si pasa algún error tenemos los originales para continuar con el análisis
- ✓ Realizar un adecuado análisis de Informática forense usando la metodología adecuada.
- ✓ Recuperar datos eliminados de la evidencia proporcionada.
- ✓ Utilizar diferentes herramientas forenses, esto nos permitirá realizar una búsqueda detallada de los archivos y/o datos necesarios.
- ✓ Analizar los historiales del explorador, ya que nos proporcionará las actividades realiza por el usuario.
- ✓ Analizar el correo electrónico para recuperar los archivos, imágenes y/o medios.

CAPITULO 2

MARCO TEÓRICO

2.1 Informática forense

La informática forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional, nos ayuda a detectar pistas sobre ataques informáticos, robo de información, conversaciones o pistas de emails, chats, etc.

La importancia de éstos y el poder mantener su integridad se basa en que la evidencia digital o electrónica es sumamente frágil. El simple hecho de darle doble clic a un archivo modificaría la última fecha de acceso del mismo.

2.2 Importancia de la informática forense

Una de las cosas más importantes en la informática forense es comprender las debilidades comunes las cuales pueden ser aprovechadas y a su vez los riesgos que nos permitirá conocer las diferentes maneras de atacar un sistema informático. Es por eso que con el pasar del tiempo los crimines informáticos cada vez se vuelven más importantes.

2.3 Objetivos de la informática forense

La informática forense tiene 3 objetivos importantes los cuales se detallan a continuación:

- Reconstrucción de los daños causados por los criminales o intrusos.
- Seguimiento y procesamiento judicial de los criminales.
- Creación y aplicación de medidas para prevenir casos similares.

2.4 Uso de la informática forense

Con el uso de la informática forense podemos lograr varios objetivos, como por ejemplo:

- Recuperar archivos y correos borrados, ocultos o dañados.
- Revelado de contraseñas.
- Acceso a información cifrada y/o protegida.

- Recuperar cache e historiales del explorador utilizado.
- Explorar dispositivos para obtener evidencias.

2.5 Metodología de la informática forense

Para poder realizar cualquier trabajo de informática forense, el auditor encargado del caso debe determinar los hallazgos, fraude y corrupción en las empresas, para esto debe de establecer una metodología que esté acorde con las irregularidades encontradas.

En el análisis forense nos vamos a encontrar con 3 fases bien diferenciadas a pesar de que, dependiendo del enfoque y del tipo que sea, dicho análisis se podrá dividir en más fases.

La metodología a utilizarse en nuestro caso es la 3 A's.

2.2.1 Etapas de la metodología de la auditoria forense

El siguiente esquema es el más adecuado para un desarrollo eficiente sobre el tema a tratar.

Figura 1 - Metodología de la Informática Forense

2.2.1.1 Adquirir datos

La adquisición de datos es una de las actividades más críticas en el análisis forense ya que si se realizase mal, todo el análisis e investigación posterior no sería válido debido a que la información saldría alterada.

Adquirimos la evidencia sin alterar ni dañar el original. En este caso vamos a copiar los archivos de imágenes proporcionados en el seminario para ser analizados.

2.2.1.2 Autenticar la evidencia

Tenemos que autenticar las evidencias recogidas que van a ser la base de la investigación, estas deben ser idénticas a las abandonadas por el intruso en la escena del crimen. Para esto debemos utilizar técnicas y herramientas las cuales nos provean el control de hash y así poder verificar la integridad de evidencias.

2.2.1.3 Analizar la evidencia según el problema

Una vez obtenidas las evidencias se procede a realizar el análisis de las mismas, el cual es un proceso que requiere de

gran conocimiento de los sistemas y/o herramientas a utilizar. Las fuentes de recogida de información en esta fase son varias:

- ✓ Registros de los sistemas analizados,
- ✓ Registro de los cortafuegos,
- ✓ Registro de los detectores de intrusión,
- ✓ Ficheros del sistema analizado.

2.6 Definiciones utilizadas

Conceptos más utilizados en el proceso de la informática forense.

- ✓ **Forensia digital (digital forensics):** Nos permite realizar la examinación de evidencias digitales, puede estar en cualquier formato de un medio de almacenamiento como pen drive, cd, dvd, etc.

- ✓ **Cadena de Custodia:** Consiste en garantizar la evidencia. Toda evidencia original no debe ser alterada, siempre se hacen réplicas de estas y es responsabilidad de la persona que maneja la evidencia asegurar que la misma sea registrada durante el tiempo en el cual están en su poder, llevando un registro de los nombres de las personas que manejaron la evidencia con el lapso de tiempo y fechas de entrega y recepción.

- ✓ **Imagen Forense:** Llamada también "Espejo", es una copia bit a bit de un medio electrónico de almacenamiento. En la imagen quedan grabados los espacios que ocupan los archivos incluyendo las áreas borradas y las particiones escondidas.

- ✓ **Análisis de Archivo:** Examina cada archivo digital descubierto y crea una base de datos de la información relacionada al archivo analizado, nos muestra detalles los sectores encontrados como la firma del archivo o hash, autor, tamaño, nombre y ruta, así como su creación, último acceso y fecha de modificación.

- ✓ **Integridad de datos:** Nos garantiza la calidad de los datos de la base de datos ya que estos no pueden ser alterados.

- ✓ **Evidencia Digital:** Es una denominación usada para describir cualquier registro generado o almacenado en un sistema informático que puede ser utilizado como prueba en un proceso legal.

CAPITULO 3

HERRAMIENTAS

3.1 Caine

Figura 2 - Entorno Caine

CAINE (Computer Aided INvestigative Environment) es una distribución Linux basado en el entorno de Ubuntu cuyo objetivo es realizar análisis forense

informático a través de sus herramientas más destacadas del mundo OpenSource.

Este entorno puede ser ejecutado completamente desde un CD o ser instalado en cualquier ordenador, dependiendo de los requerimientos de utilización, con todas sus herramientas incluidas. De esta manera es factible la utilización de CAINE para obtener réplicas de imágenes de los medios físicas en nuestra estación forense.

3.1.1 Objetivos

Los objetivos principales de Caine son los siguientes:

- Entorno interoperable que ayuda al investigador durante la investigación forense.
- Interfaz gráfica amigable.
- Compilación semi-automática de reportes y/o informe final.

3.1.2 Herramientas

A continuación describimos las herramientas de caine más destacadas:

Figura 3 - Herramientas de Caine

3.1.2.1 Air

Automated Image and Restore - Restauración de Imagen Automática, es una herramienta diseñada para crear fácilmente imágenes forenses de disco y/o particiones de bit a bit.

3.1.2.2 Autopsy

Es una herramienta libre, incluye una interfaz gráfica que sirve para el análisis de evidencia digital. Permite realizar un análisis de diversos tipos de evidencia mediante una captura de una

imagen de disco, sistemas de archivos y volúmenes de un equipo.

3.1.2.3 Dvdisaster

Es un programa que nos ayuda a mejorar la información de los discos ópticos por medio de la detección y solución de errores en los datos, finalmente genera una imagen .iso con los datos corregidos y recuperación de la información parcial o total.

3.1.2.4 Gtkhash

Es una herramienta que sirve para generar hash a partir de un archivo. Su uso es muy fácil, ya que solo es cargar el archivo y generar dicho hash.

3.1.2.5 Photorec

Es una herramienta que nos ayuda en la recuperación de archivos perdidos, de discos duros y CD, incluyendo documentos, videos, fotos de memorias de cámaras digitales. La ventaja de esta herramienta es que ignora el sistema de archivos y va directo a los datos subyacentes, esto para archivos borrados o dañados.

3.1.2.6 Testdisk

Es una herramienta la cual realiza la recuperación de datos, está diseñado para recuperar particiones pérdidas o hacer discos no booteables a booteables. Además nos permite recuperar la tabla de particiones.

3.2 Comandos linux

3.2.1 cp

Se utiliza para copiar archivos, su sintaxis es la siguiente:

Sintaxis comando cp			
cp	opciones	archivo-origen	camino-destino
cp	opciones	archivos-origen	directorio-destino

Tabla 1 - Sintaxis del comando cp

Entre las opciones más relevantes, se tiene:

- **-f** Borrar los archivos de destino ya existentes.
- **-p** Proteger los permisos, el usuario y el grupo del archivo a copiar.
- **-R** Copia directorios recursivamente.
- **-v** Presenta los archivos que se van copiando.

3.2.2 cd

Este comando nos sirve para cambiarnos de un directorio a otro. Generalmente cuando cualquier usuario inicia sesión, comienza en su directorio personal. Con este comando podemos cambiarnos desde cualquier directorio hacia otro.

Sintaxis	
cd	Nombre del directorio

Tabla 2 - Sintaxis del comando cd

3.2.3 cat

Nos permite visualizar el contenido de un archivo. También nos ayuda con la creación del mismo y a su vez modificarlo.

Sintaxis	
cat	Nombre del directorio

Tabla 3 - Sintaxis del comando cat

- Cat >nombre-del-archivo: Crear archivo y tipiarlo.

3.2.4 gzip

Es un compresor de archivos muy utilizado en Linux y en muchas aplicaciones para comprimir y descomprimir pero sólo comprime 1 archivo a la vez. No comprime directorios.

Sintaxis	
Comprimir	gzip archivo
Descomprimir	gzip –d archivo.gz

Tabla 4 - Sintaxis del comando gzip

- -d indica descompresión

3.2.5 md5sum

Es una herramienta de seguridad, nos permite verificar la integridad de los datos, realiza un hash MD5 de un archivo. Esta función de hash nos devuelve un valor único para cada archivo.

3.2.6 ls

Ls muestra un listado de directorios y archivos de un determinado directorio. Estos resultados serán visibles alfabéticamente.

Sintaxis		
ls	opciones	archivo

Tabla 5 - Sintaxis del comando ls

Entre las opciones más relevantes, se tiene:

- -a Lista todos los archivos y subdirectorios ocultos incluidos los que empiezan con .(punto), que no se muestran con ls.

- -d Lista los directorios.
- -l Lista los archivos, especificando sus permisos, el nombre del propietario, el grupo al que pertenece, la fecha de la última modificación y el tamaño en bytes.
- -A Lista todos los archivos, menos los ocultos.
- -R Lista el contenido de todos los directorios de forma recursiva.

3.2.7 strings –a

Nos permite visualizar caracteres extrayendo todo el texto ASCII.

3.3 Web historian

Es un programa que ayuda al investigador encargado del caso a reunir, analizar y mostrar datos ocultos o borrados de la navegación que se ha realizado en el equipo. Esta herramienta nos ofrece una interfaz gráfica pero de una manera muy simple de ver y navegar con grandes volúmenes de datos.

La característica más potente de esta herramienta es la capacidad de relacionar los datos, incluyendo gráficos y línea de tiempo. Todo esto lo hace a través del analizador y la herramienta web de perfiles, a su vez ayuda al investigar para llegar a las conclusiones acertadas.

3.4 Pasco

Es una herramienta utilizada con frecuencia en el análisis de la actividad de Internet, fue desarrollada por Keith J. Jones, Consultora Informática Forense Principal en Foundstone, Inc. Este software funciona en sistemas operativos Unix o Windows como una herramienta de línea de comandos.

Permite escanear los discos duros para encontrar los archivos indexados al navegador Web, luego de este proceso reconstruye los datos en un archivo de texto. Este archivo se puede exportar a una hoja de cálculo de Excel, nos facilita el proceso el análisis de los datos. Pasco ayuda a obtener la siguiente información:

- ✓ Los registros de usuario, si este accede a una URL directamente, o utiliza un proxy.
- ✓ La URL que visitó el usuario.
- ✓ Fecha que tuvo acceso a la dirección.

3.5 Galleta

Galleta es una herramienta forense para el análisis de los cookies de Internet Explorer que también fue desarrollado por Keith J. Jones, Consultora Informática Forense Principal en Foundstone, Inc. Muchas investigaciones

de delitos informáticos requieren la reconstrucción de los archivos de cookies de Internet Explorer y ya que esta técnica de análisis se ejecuta regularmente, galleta analiza la estructura de los datos encontrados en los archivos de cookies.

Galleta está basada en analizar la información en un archivo de cookies y mostrar los resultados de una manera delimitada, que también se puede abrir en una hoja de cálculo de Excel. Galleta está diseñada para funcionar en múltiples plataformas y se ejecutará en Windows, Mac OS X, Linux.

3.6 Eindeutig

Es una utilidad que permite reconocer formatos de archivos de correos, extrae su contenido y lo exporta a una hoja de calculo. Tambien nos muestra los archivos adjuntos si estos existieran.

3.7 Munpack

Munpack es una utilidad que nos permite recuperar los archivos adjuntos de un correo electrónico.

CAPITULO 4

DESARROLLO DEL PROYECTO

4.1 Imágenes lewis-laptop.gz y lewis-usb.dd

4.1.1 Respaldar imágenes

Según la metodología utilizada en este caso vamos a adquirir la evidencia copiando los archivos de imágenes de lewis-laptop.gz y lewis-usb.dd las cuales fueron proporcionadas durante el seminario para su respectivo análisis, en un directorio ubicado en el escritorio de nuestra maquina local. Para esto utilizamos el comando `cp origen del archivo destino del archivo.`

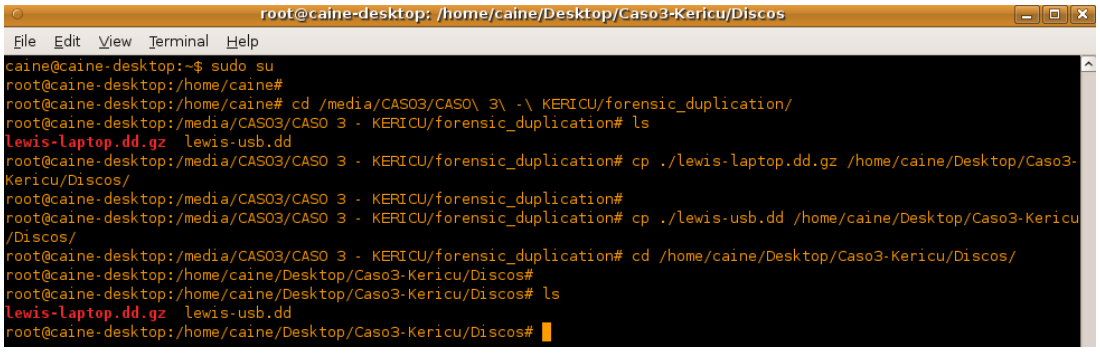


Figura 4 - Copiando la evidencia

Antes de copiar los archivos, utilizamos el comando cd para ubicarnos en el directorio del cdrom y con ls podemos visualizar los archivos ubicados en el directorio respectivo para proceder a copiarlos.

4.1.2 Descomprimir imágenes

Luego de respaldar las evidencias, con el comando ls -l vamos a visualizar el contenido de cada directorio con muchos más detalles.

Nos ubicamos en el directorio respectivo en este caso "Discos", utilizamos el comando cd el cual nos sirve para cambiarnos de un directorio a otro.

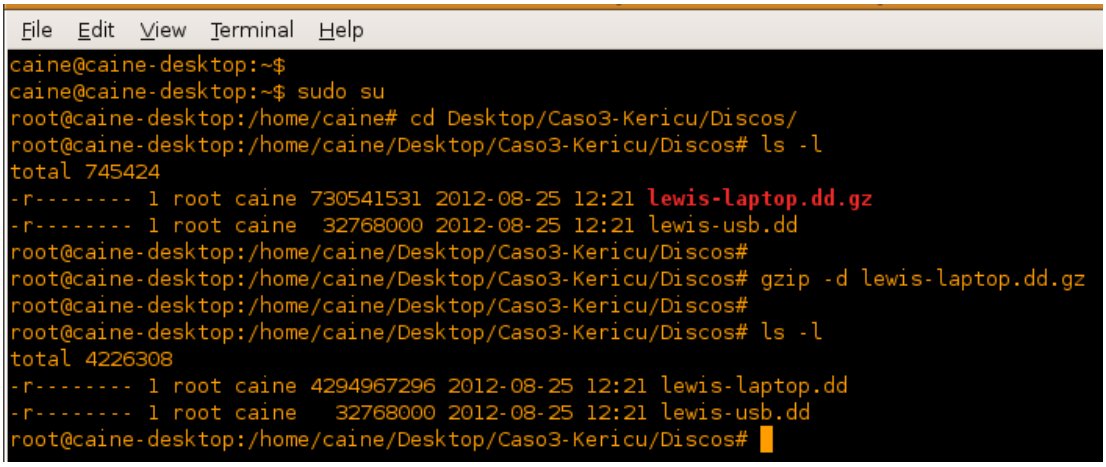


Figura 5 - Descomprimir imagen .gz

El archivo “lewis-laptop” está en formato .gz y para esto se descomprimió utilizando el comando gzip quedando de la siguiente manera:

#gzip -d lewis-laptop.dd.gz

Quedando así ambas imágenes con la extensión de archivo .dd, "lewis-laptop.dd" y "lewis-usb.dd".

4.1.3 Hash de archivos de imágenes

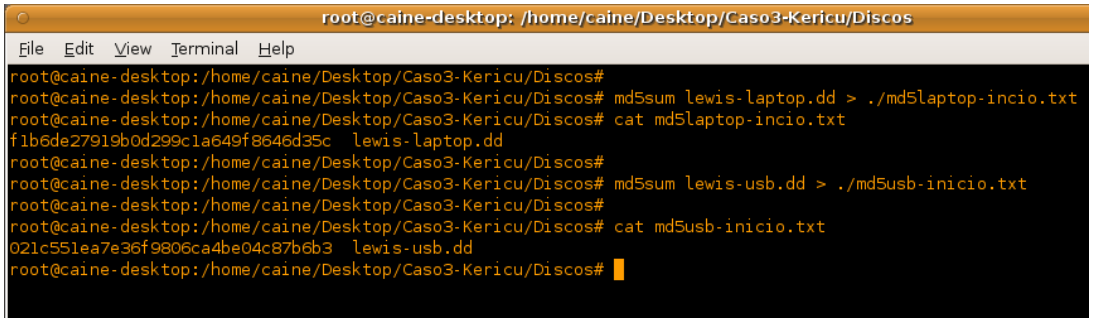


Figura 6 - Autenticar evidencia

Antes de realizar cualquier tipo de análisis adquirimos los hash de cada una de las imágenes, tanto de Lewis-laptop como de Lewis-usb para analizar la integridad de los datos, que no se ha alterado dicha evidencia.

Utilizamos los comandos:

```
md5sum archivo > ./archivo.inicio.txt
```

```
cat archivo.inicio.txt
```

4.1.4 Montaje y análisis del archivo lewis-laptop en autopsy

Una vez descomprimida la imagen procedemos a montarla y para esto vamos a utilizar Autopsy el cual trabaja dividiendo cada investigación en casos. Cada caso puede contener uno o más hosts, y cada uno de ellos puede a su vez contener una o varias imágenes de su sistema de ficheros. Por otra parte cada caso puede tener asignados uno o más investigadores.

Figura 7 - Iniciando caso en Autopsy

Empezaremos a crear el caso correspondiente a nuestra investigación pulsando sobre “New Case”.

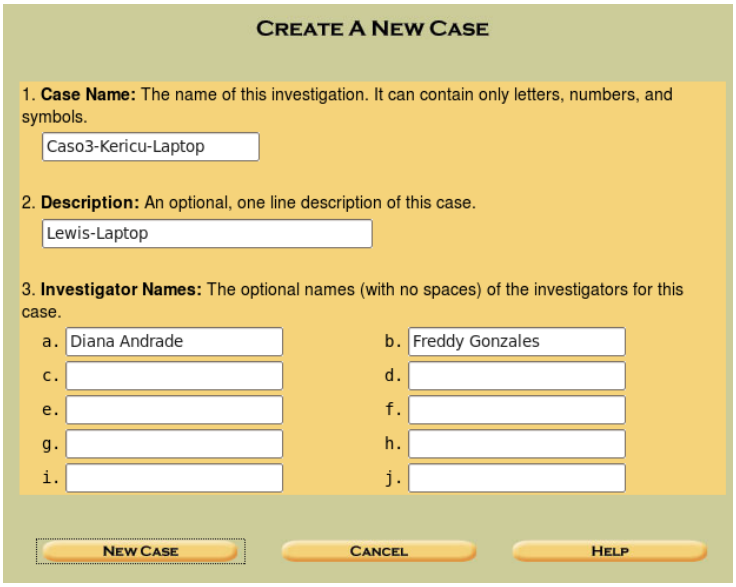


Figura 8 - Creación de caso

Aparecerá una nueva pantalla donde introduciremos la siguiente información:

- Nombre del caso a crear
- Descripción
- Nombres de los investigadores

Nuestro caso se va a llamar Caso3-Kericu-Laptop, en descripción pondremos Lewis-Laptop y por último los nombres de los investigadores.

Una vez completada la información pulsaremos sobre “New Case”.

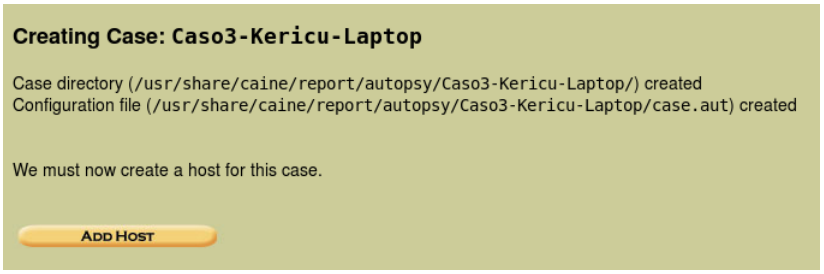


Figura 9 - Caso3-Kericu-Laptop creado

Como resultado se creará un directorio con el nombre Caso3-Kericu-Laptop en el cual se nos almacenará todo el proceso de la investigación. Ahora deberemos agregar el host al caso. Para ello vamos a dar click en “Add Host”.

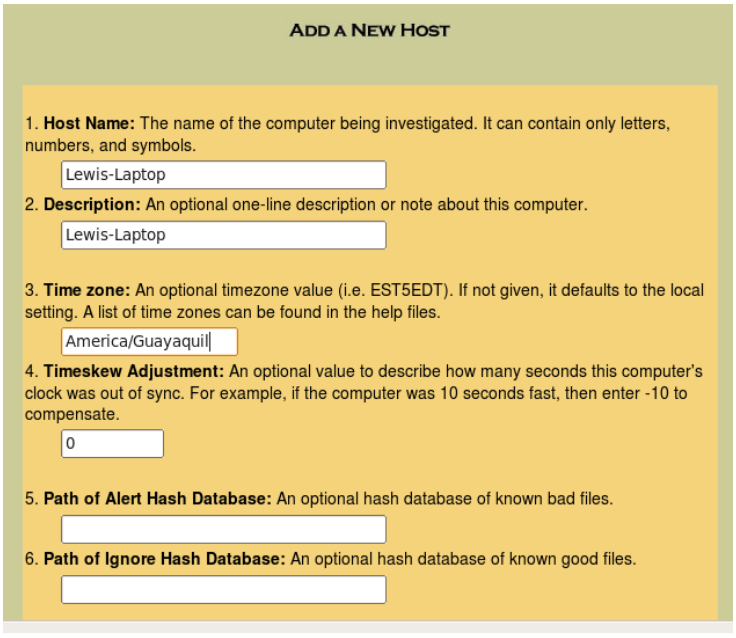


Figura 10 - Agregar Nuevo Host

Agregamos el nuevo host, como nombre ponemos Lewis-Laptop y en descripción lo mismo para poder identificarlo, en huso horario América/Guayaquil, por último en el campo tiempo de ajuste le pondremos 0 (cero) ya que no tenemos diferencia de tiempo.

Nuevamente damos click sobre “Add Host”, con esto hemos agregado una entrada para la máquina en el Caso3-Kericu-Laptop.

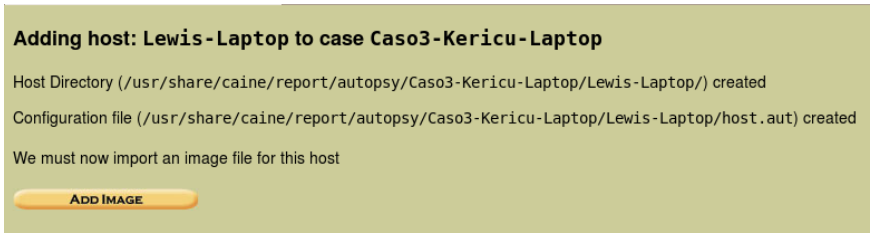


Figura 11 - Host Lewis-Laptop creado

Ahora vamos a vincular las imágenes respectivas a investigar en dicho caso. Para ello pulsaremos sobre “Add Image”.

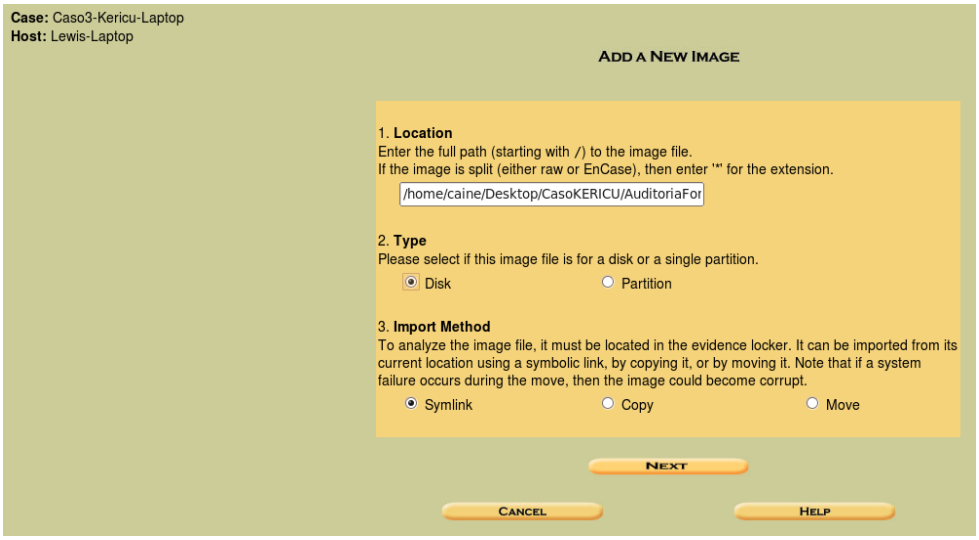


Figura 12 - Agregar Imagen de Sistema de ficheros

En la figura 12 nos muestra la información que necesitamos para agregar la nueva imagen.

En la opción de ubicación pondremos la ruta absoluta de la ubicación del fichero de imagen.

La siguiente opción nos permite especificar si la imagen es un disco completo o solo una partición.

La tercera opción especifica el tipo de fichero de imagen.

- Con symlink se crea un enlace simbólico en el directorio del caso respectivo y este apuntará a la ubicación original de la imagen.
- Las otras dos opciones permiten mover o copiar el fichero.

Ahora pulsamos “Next” y obtendremos una nueva pantalla donde debemos indicar algunos valores adicionales.

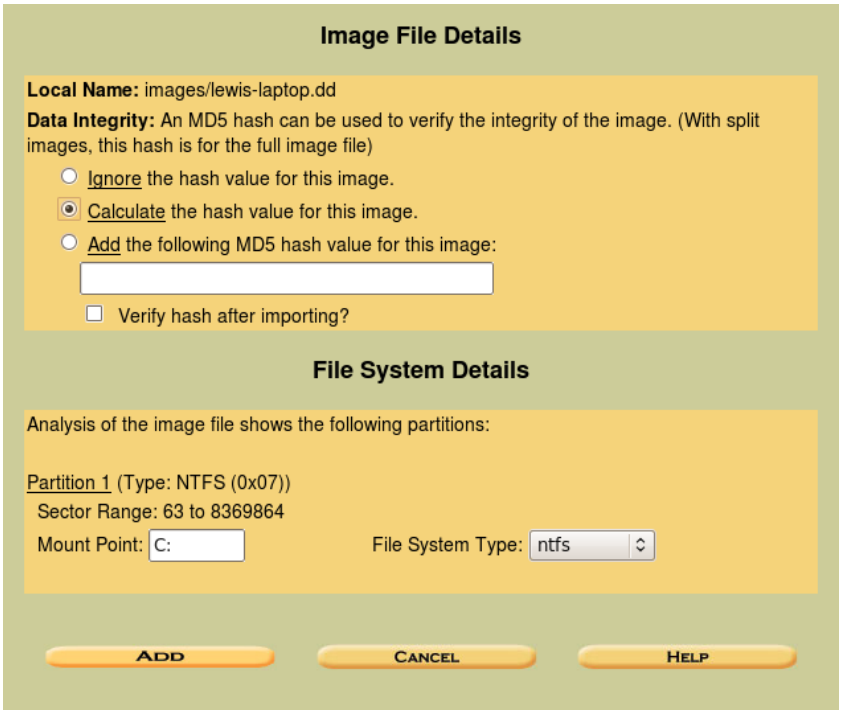


Figura 13 - Detalles de la imagen agregada

Calculamos el hash de la imagen y a seleccionar el tipo de archivo. Una vez completados los datos damos click en “Add”.

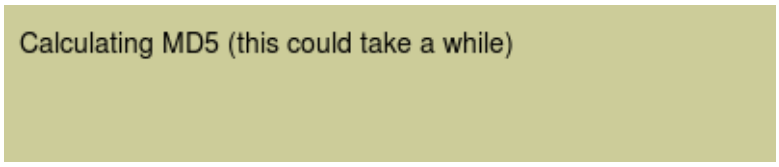


Figura 14 - Calculando MD5

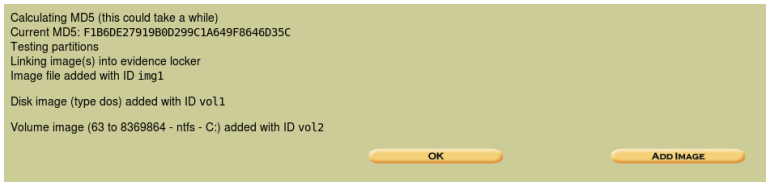


Figura 15 - Resultados del cálculo MD5

Una vez calculado el proceso de MD5 aparecerá un resumen indicando el resultado como se refleja en la figura 15 la cual nos muestra un resumen de la operación. Damos click en “OK” en el caso de haber terminado y sobre “Add Image” para añadir otra imagen.

4.1.4.1 Detalles del primer volumen

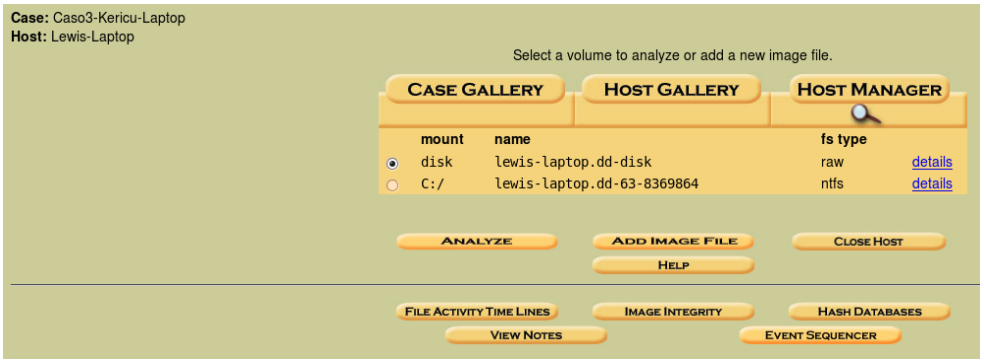


Figura 16 - Volúmenes encontrados

Una vez concluido el proceso de agregar imágenes, se obtienen los volúmenes que fueron encontrados en la imagen, para su respectiva exploración.

Damos click en details de lewis-laptop.dd-disk y se nos desplazan algunas opciones en este caso vamos a dar click en EXTRACT STRINGS el cual nos permite extraer los strings.

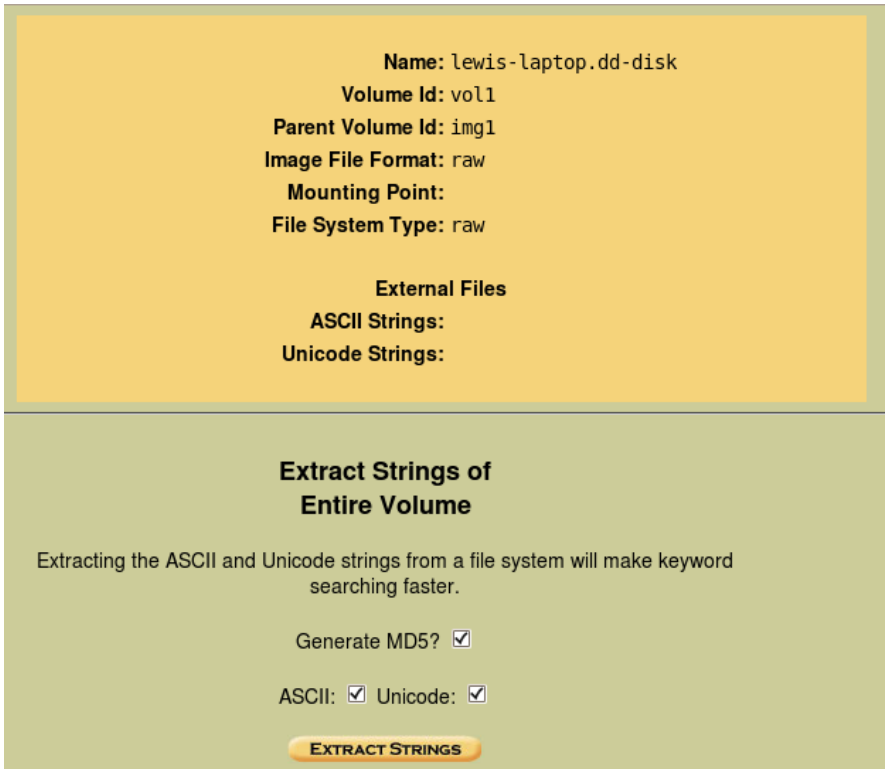


Figura 17 - Detalles de lewis-laptop.dd-disk vol1

Extraer strings se significa que podemos visualizar archivos binarios encontrados en la imagen analizada.

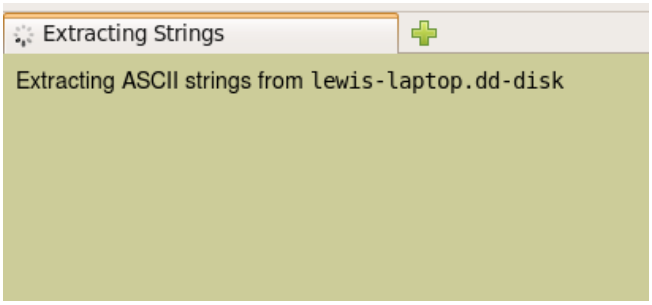


Figura 18 - Extrayendo strings

Una vez extraídos los strings de la imagen como lo podemos observar en la figura 18 y 19 procedemos hacer los mismos pasos con el volumen ntfs que se nos generó.

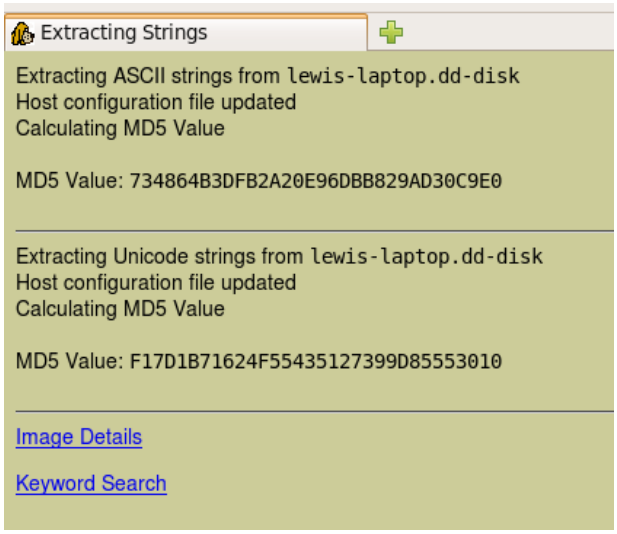


Figura 19 – Strings extraídos

También podemos visualizar detalles de imagen la cual hemos extraido los strings.

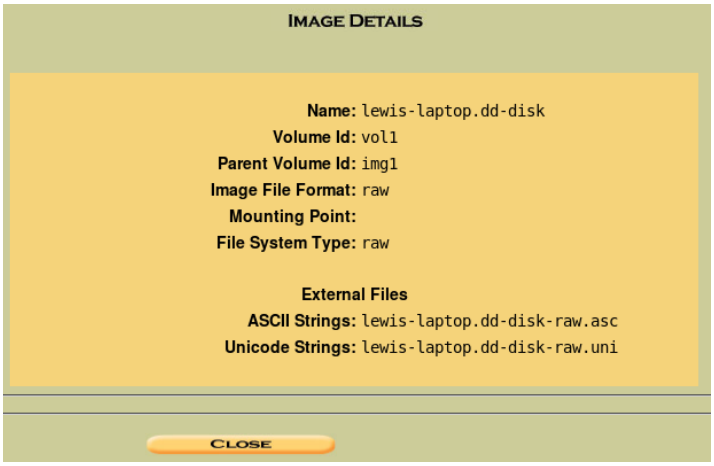


Figura 20 - Detalles de la imagen

4.1.4.2 Detalles del segundo volumen

Figura 21 - Análisis del 2do volumen

Una vez culminado el analisis del 1er volumen continuamos con el siguiente, primeramente los seleccionamos y damos clic en details (detalles) dando como resultado la siguiente figura.

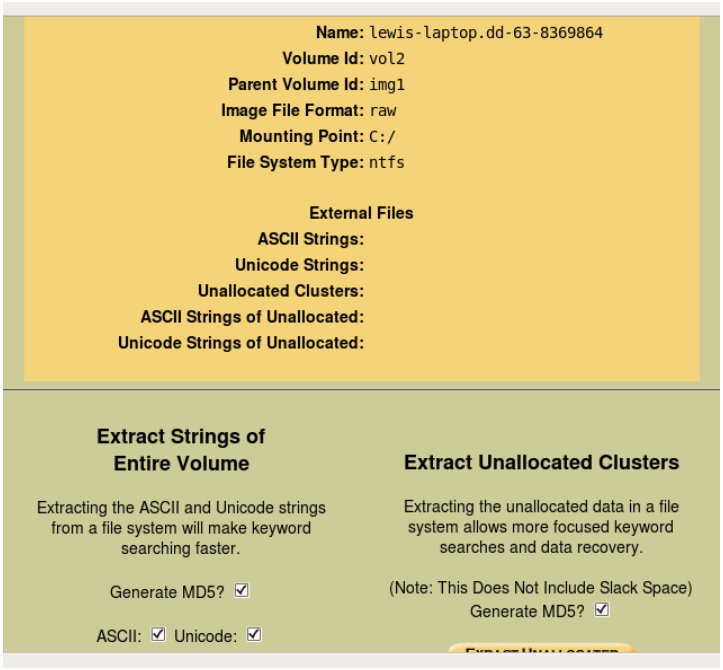


Figura 22 - Detalles de lewis-laptop.dd-disk vol2

Como nos podemos dar cuenta este volumen está en formato ntfs. Tenemos que extraer los strings del volumen, los espacios no asignados y los strings de los espacios no asignados.

Damos clic en Extraer Strings y se nos va a desplaegar la siguiente pantalla, tenemos que esperar que culmine el proceso.

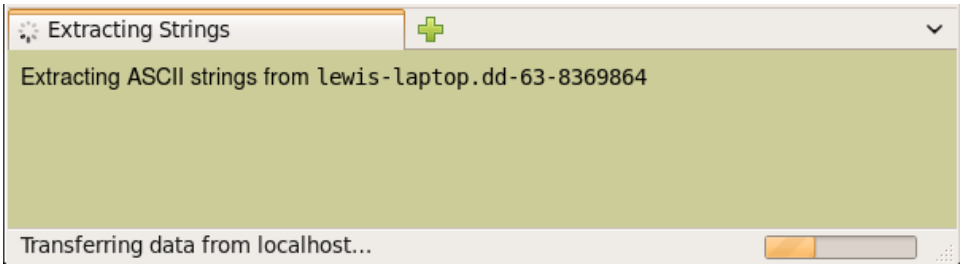


Figura 23 - Extrayendo strings de lewis-laptop.dd vol2

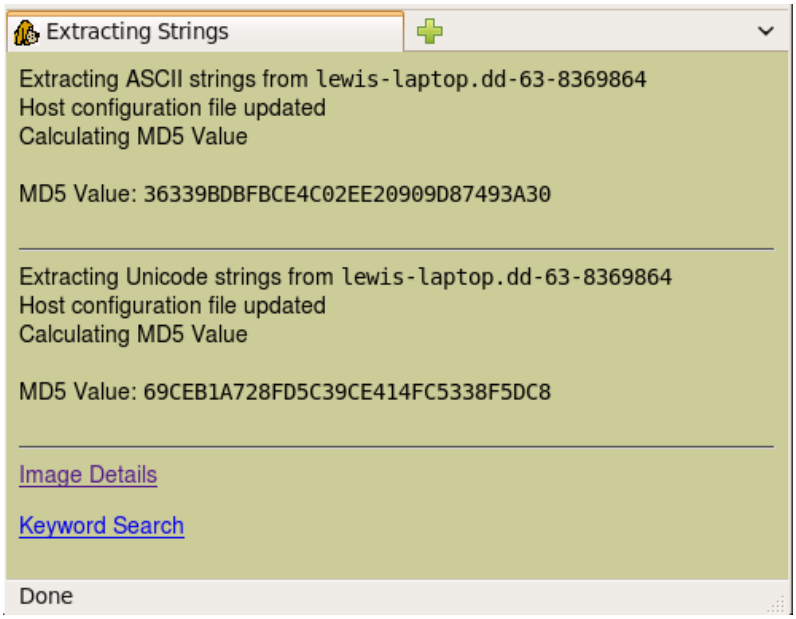


Figura 24 - Strings extraídos de lewis-laptop.dd vol2

Una vez extraidos los strings del segundo volumen de la imagen lewis-laptop.dd nos genera los detalles (ver figura 24).

Damos clic en Image Details (detalles de imagen) y se nos muestra con mas detalles las acciones tomadas.

Figura 25 - Detalles de la imagen vol2

Procedemos a extraer los espacios no asignados.

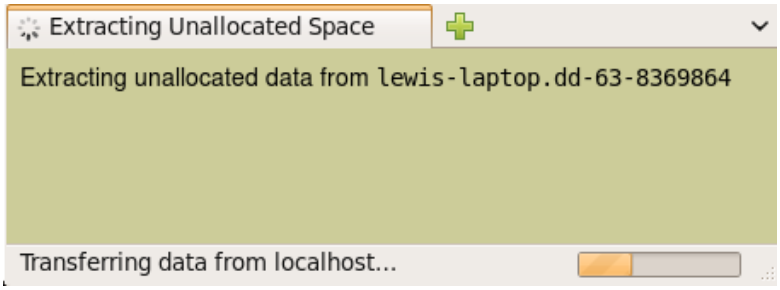


Figura 26 - Extrayendo los espacios no asignados

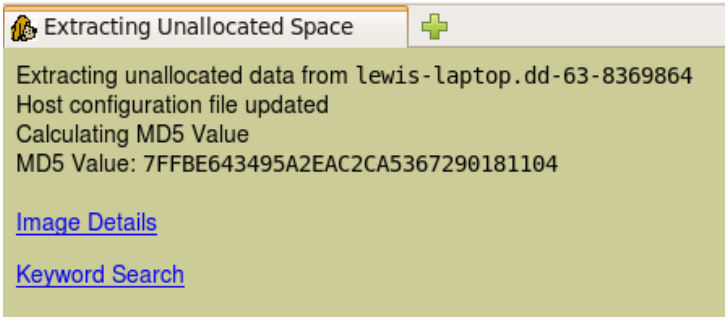


Figura 27 - Espacios no asignados extraídos

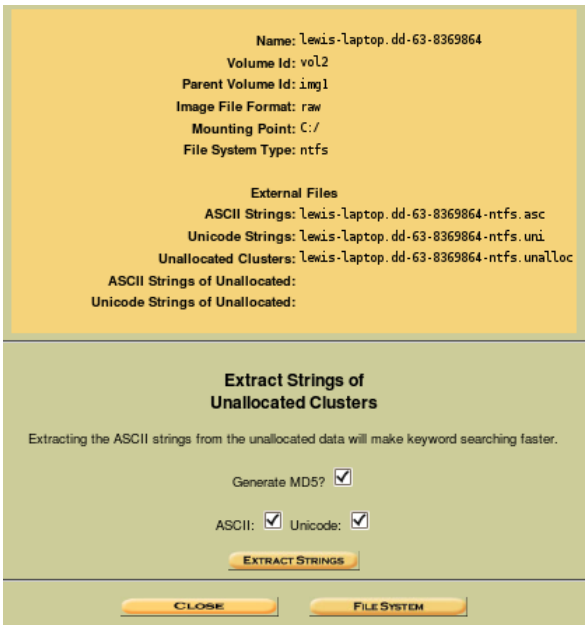


Figura 28 - Detalles de acciones tomadas

Concluido el proceso de extraer strings, extraer los espacios no asignados, continuamos a extraer los strings de los espacios no asignados.

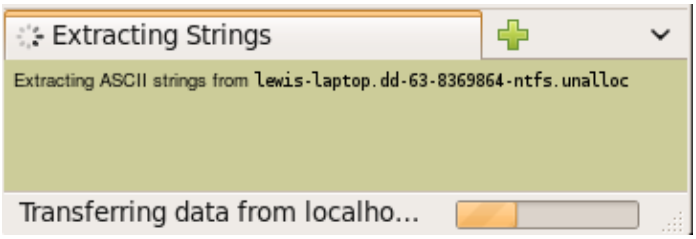


Figura 29 - Extrayendo strings de los espacios no asignados

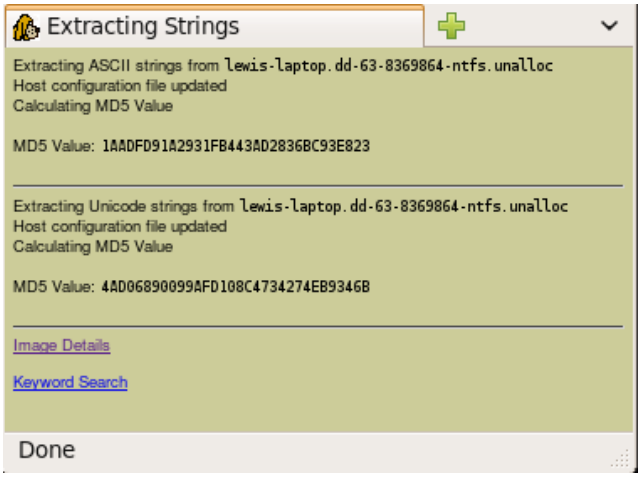


Figura 30 - Strings extraídos de los espacios no asignados

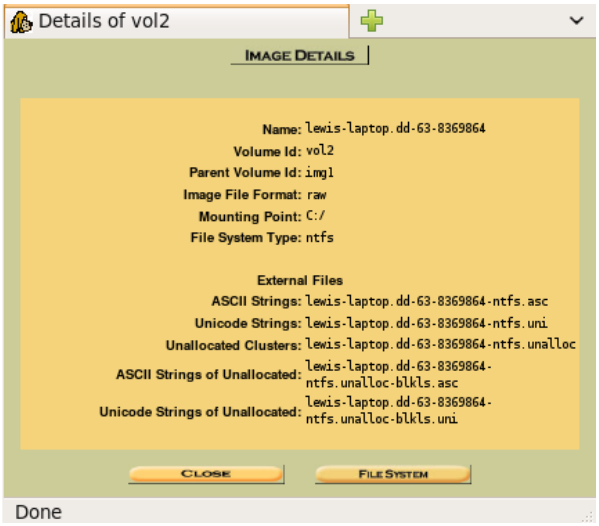
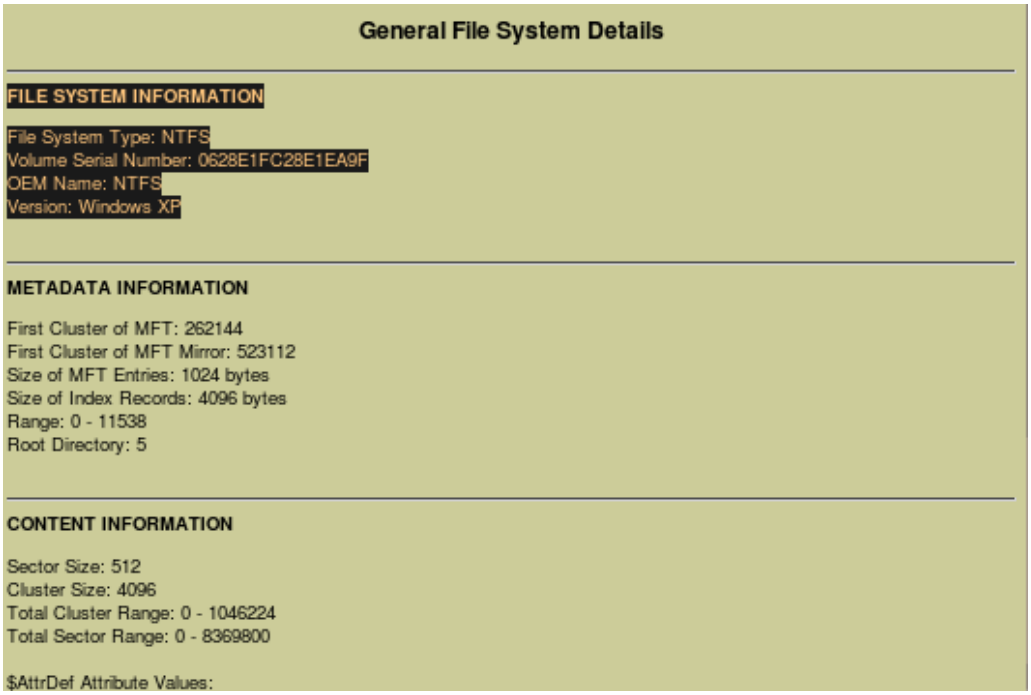


Figura 31 - Detalles de imagen lewis-laptop.dd vol2



General File System Details

FILE SYSTEM INFORMATION

File System Type: NTFS
Volume Serial Number: 0628E1FC28E1EA9F
OEM Name: NTFS
Version: Windows XP

METADATA INFORMATION

First Cluster of MFT: 262144
First Cluster of MFT Mirror: 523112
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 11538
Root Directory: 5

CONTENT INFORMATION

Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 0 - 1046224
Total Sector Range: 0 - 8369800

$AttrDef Attribute Values:

Figura 32 - Detalles Generales de lewis-laptop.dd vol2

En esta imagen podemos visualizar los detalles generales del sistema de archivos de la imagen lewis-laptop. Tenemos que el sistema operativo de la laptop es Windows XP con sistema de archivo NTFS.

Continuando con el análisis vamos verificar los archivos borrados, historiales del navegador utilizado, cabeceras de correos electrónicos, etc.

Figura 33 - Análisis de lewis-laptop.dd - ntfs

Damos clic en analyze (analisis) y se nos genera lo siguiente:

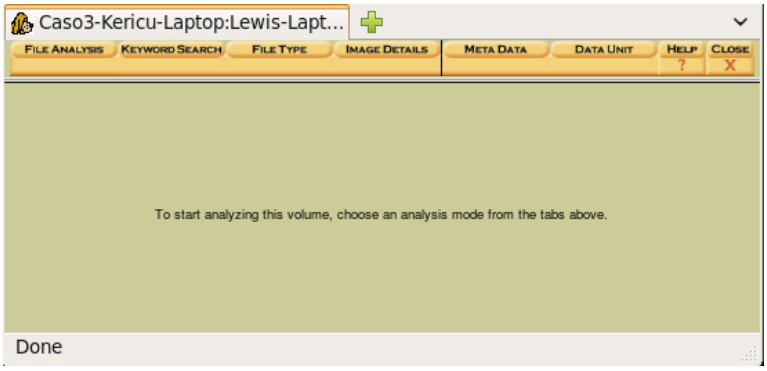
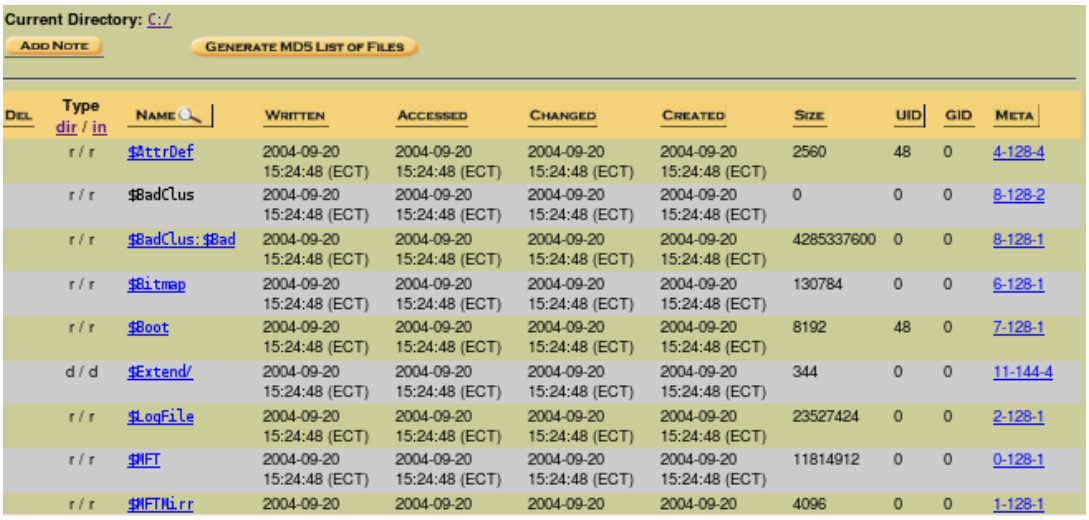


Figura 34 - Proceso de análisis de lewis-laptop.dd - ntfs

Ingresamos a File Analysis (Analisis de archivo), nos permite visualizar todos los archivos y directorios de la imagen del equipo.



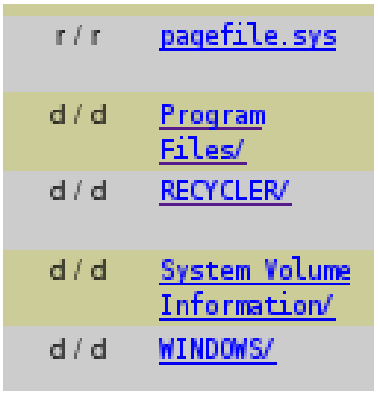
Current Directory: C:/

ADD NOTE | GENERATE MD5 LIST OF FILES

DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CHANGED	CREATED	SIZE	UID	GID	META
	r / r	$AttrDef	2004-09-20 15:24:48 (ECT)	2004-09-20 15:24:48 (ECT)	2004-09-20 15:24:48 (ECT)	2004-09-20 15:24:48 (ECT)	2560	48	0	4-128-4
	r / r	$BadClus	2004-09-20 15:24:48 (ECT)	2004-09-20 15:24:48 (ECT)	2004-09-20 15:24:48 (ECT)	2004-09-20 15:24:48 (ECT)	0	0	0	8-128-2
	r / r	$BadClus:$Bad	2004-09-20 15:24:48 (ECT)	2004-09-20 15:24:48 (ECT)	2004-09-20 15:24:48 (ECT)	2004-09-20 15:24:48 (ECT)	4285337600	0	0	8-128-1
	r / r	$Bitmap	2004-09-20 15:24:48 (ECT)	2004-09-20 15:24:48 (ECT)	2004-09-20 15:24:48 (ECT)	2004-09-20 15:24:48 (ECT)	130784	0	0	6-128-1
	r / r	$Boot	2004-09-20 15:24:48 (ECT)	2004-09-20 15:24:48 (ECT)	2004-09-20 15:24:48 (ECT)	2004-09-20 15:24:48 (ECT)	8192	48	0	7-128-1
	d / d	$Extend/	2004-09-20 15:24:48 (ECT)	2004-09-20 15:24:48 (ECT)	2004-09-20 15:24:48 (ECT)	2004-09-20 15:24:48 (ECT)	344	0	0	11-144-4
	r / r	$LogFile	2004-09-20 15:24:48 (ECT)	2004-09-20 15:24:48 (ECT)	2004-09-20 15:24:48 (ECT)	2004-09-20 15:24:48 (ECT)	23527424	0	0	2-128-1
	r / r	$MFT	2004-09-20 15:24:48 (ECT)	2004-09-20 15:24:48 (ECT)	2004-09-20 15:24:48 (ECT)	2004-09-20 15:24:48 (ECT)	11814912	0	0	0-128-1
	r / r	$MFTMirr	2004-09-20	2004-09-20	2004-09-20	2004-09-20	4096	0	0	1-128-1

Figura 35 - Archivos analizados en lewis-laptop.dd

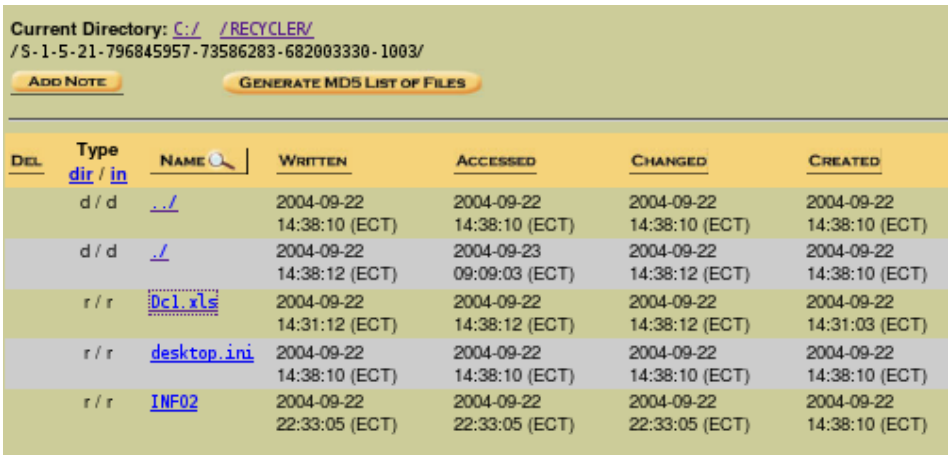
Los archivos encontrados se ordenan de forma alfabetica por defecto, pero nosotros tambien podemos elegir a nuestra preferencia. Pulsamos sobre el directorio RECYCLER/ para poder revisar todos los archivos contenidos en el mismo, los cuales han sido borrados.



r / r	pagefile.sys
d / d	Program Files/
d / d	RECYCLER/
d / d	System Volume Information/
d / d	WINDOWS/

Figura 36 - Directorio Recycler

Exportamos los archivos encontrados para su respectivo analisis y conclusion.



Current Directory: C:/ /RECYCLER/
/S-1-5-21-796845957-73586283-682003330-1003/

ADD NOTE | GENERATE MD5 LIST OF FILES

DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CHANGED	CREATED
	d / d	../	2004-09-22 14:38:10 (ECT)	2004-09-22 14:38:10 (ECT)	2004-09-22 14:38:10 (ECT)	2004-09-22 14:38:10 (ECT)
	d / d	./	2004-09-22 14:38:12 (ECT)	2004-09-23 09:09:03 (ECT)	2004-09-22 14:38:12 (ECT)	2004-09-22 14:38:10 (ECT)
	r / r	Dc1.xls	2004-09-22 14:31:12 (ECT)	2004-09-22 14:38:12 (ECT)	2004-09-22 14:38:12 (ECT)	2004-09-22 14:31:03 (ECT)
	r / r	desktop.ini	2004-09-22 14:38:10 (ECT)	2004-09-22 14:38:10 (ECT)	2004-09-22 14:38:10 (ECT)	2004-09-22 14:38:10 (ECT)
	r / r	INFO2	2004-09-22 22:33:05 (ECT)	2004-09-22 22:33:05 (ECT)	2004-09-22 22:33:05 (ECT)	2004-09-22 14:38:10 (ECT)

Figura 37 - Contenido del directorio Recycler

Tenemos el archivo Dc1.xls en cual se nos visualiza en una hoja de calculo como un estado financiero acerca de las ganacias de la empresa. Tambien podemos obtener la informacion del o de los usurios que tuvieron acceso a ese archivo y lo manipularon, todo esto a traves de la informacion general del mismo.

Pointed to by file:
C:/RECYCLER/S-1-5-21-796845957-73586283-682003330-1003/Dc1.xls

File Type:
CDF V2 Document, Little Endian, Os: MacOS, Version 10.3, Code page: 10000, Author: Rodger Lewis, Last Saved By: Keith Jones, Name of Creating Application: Microsoft Excel, Create Time/Date: Fri Aug 22 15:45:21 2003, Security: 0

MD5 of content:
cba952fb0c109cf5b72905c871de3dfa -

SHA-1 of content:
e4b3917ec20b259fe7c16f7cf7694a0de220b6ef -

Details:

MFT Entry Header Values:
Entry: 11126 Sequence: 1
$LogFile Sequence Number: 30054408
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0
Security ID: 387 ()
Created: Wed Sep 22 14:31:02 2004

Figura 39 - Informacion general del archivo Dc1.xls

KERICU

Kericu, Inc. Company Earnings, Q2 2003

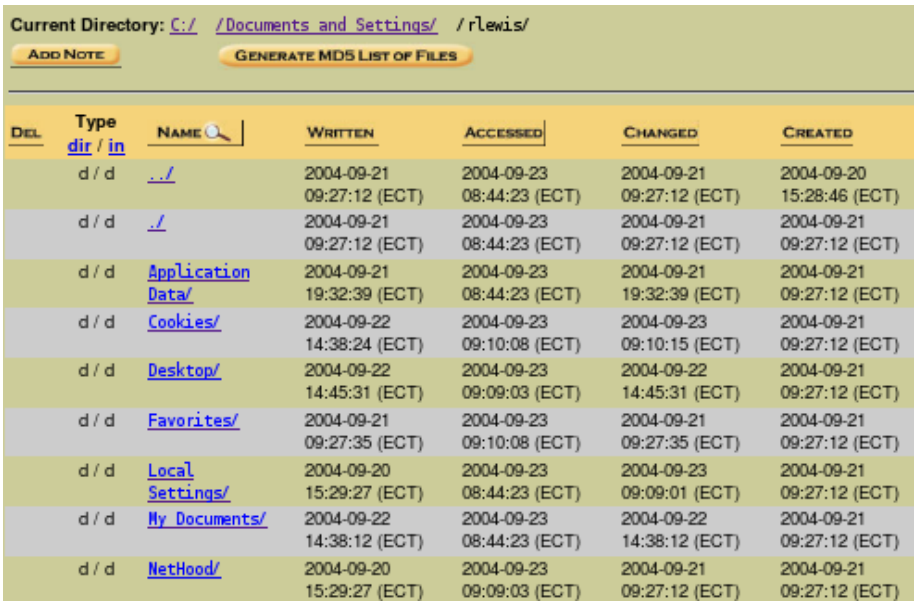
Expenses	abr-03	may-03	jun-03	**Totals**
Sales	$523.532,05	$623.592,03	$521.343,15	$1.668.467,23
Development	$1.235.662,32	$1.482.342,10	$1.831.235,52	$4.549.239,94
HR	$135.234,00	$200.145,23	$152.628,23	$488.007,46
Legal	$523.923,93	$812.351,13	$312.235,19	$1.648.510,25
IT	$2.512.519,84	$2.193.218,18	$1.912.345,73	$6.618.083,75
Security	$102.482,15	$139.258,92	$129.415,93	$371.157,00
Document Destruction	$15.232,93	$10.342,28	$97.123,72	$122.698,93
Admin	$151.910,01	$159.123,91	$130.158,83	$441.192,75
Total	**$5.200.497,23**	**$5.620.373,78**	**$5.086.486,30**	**$15.907.357,31**

Income	abr-03	may-03	jun-03	**Totals**
Products	$7.151.801,00	$9.125.152,75	$8.145.198,51	$24.422.152,26
Consulting	$253.925,93	$315.323,93	$293.815,93	$863.065,79
Legal Settlements	$0,00	$0,00	$1.250.000,00	$1.250.000,00
Total	**$7.405.726,93**	**$9.440.476,68**	**$9.689.014,44**	**$26.535.218,05**
Net Earnings	$2.205.229,70	$3.820.102,90	$4.602.528,14	$10.627.860,74

Figura 38 - Documento Dc1.xls encontrado en Recycler

4.1.4.3 Actividad navegadores web

Continuamos con el analisis de las actividades de los navegadores utilizados en el equipo y para esto nos ubicamos en el directorio del usuario respectivo, en nuestro caso es rlewis.



Current Directory: C:/ /Documents and Settings/ /rlewis/

ADD NOTE | GENERATE MD5 LIST OF FILES

DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CHANGED	CREATED
	d / d	../	2004-09-21 09:27:12 (ECT)	2004-09-23 08:44:23 (ECT)	2004-09-21 09:27:12 (ECT)	2004-09-20 15:28:46 (ECT)
	d / d	./	2004-09-21 09:27:12 (ECT)	2004-09-23 08:44:23 (ECT)	2004-09-21 09:27:12 (ECT)	2004-09-21 09:27:12 (ECT)
	d / d	Application Data/	2004-09-21 19:32:39 (ECT)	2004-09-23 08:44:23 (ECT)	2004-09-21 19:32:39 (ECT)	2004-09-21 09:27:12 (ECT)
	d / d	Cookies/	2004-09-22 14:38:24 (ECT)	2004-09-23 09:10:08 (ECT)	2004-09-23 09:10:15 (ECT)	2004-09-21 09:27:12 (ECT)
	d / d	Desktop/	2004-09-22 14:45:31 (ECT)	2004-09-23 09:09:03 (ECT)	2004-09-22 14:45:31 (ECT)	2004-09-21 09:27:12 (ECT)
	d / d	Favorites/	2004-09-21 09:27:35 (ECT)	2004-09-23 09:10:08 (ECT)	2004-09-21 09:27:35 (ECT)	2004-09-21 09:27:12 (ECT)
	d / d	Local Settings/	2004-09-20 15:29:27 (ECT)	2004-09-23 08:44:23 (ECT)	2004-09-23 09:09:01 (ECT)	2004-09-21 09:27:12 (ECT)
	d / d	My Documents/	2004-09-22 14:38:12 (ECT)	2004-09-23 08:44:23 (ECT)	2004-09-22 14:38:12 (ECT)	2004-09-21 09:27:12 (ECT)
	d / d	NetHood/	2004-09-20 15:29:27 (ECT)	2004-09-23 09:09:03 (ECT)	2004-09-21 09:27:12 (ECT)	2004-09-21 09:27:12 (ECT)

Figura 40 - Directorios de actividades de navegación

IE utiliza tres ubicaciones en las que podemos encontrar evidencia:

- ✓ Historial web de navegación.
- ✓ Cookies.
- ✓ Archivos temporales de Internet (Caché).

El historial de navegacion de Internet contiene las direcciones URL’s de los sitios web que visitó el sospechoso. El directorio contiene las cookies. Las cookies que el usuario acepta mientras navega en la Web. El directorio más importante, el directorio Archivos temporales de Internet, no solo contiene el historial de navegación web, sino también una copia de los archivos que se utilizaron para descargar copias de las páginas web de modo que la próxima vez que un usuario vaya a un sitio web, IE solo descargará las secciones del sitio web que han cambiando.

Cada una de las ubicaciones de IE mencionados anteriormente contiene un archivo importante de la informacion guardada, el nombre del archivo es index.dat.

El archivo index.dat contiene informacion de los enlaces guardados en el disco duro del usuario con la informacion adquirida de internet.

Directorio	Propósito
C:\Documents and Settings\ <<profilename>>\Cookies\	Este directorio contiene un archivo index.dat y todos los archivos cookies para el usuario llamado <<profilename>>
C:\Documents and Settings\ <<profilename>>\Local Settings\History\History.IE5\	Este directorio contiene un archivo index.dat para todo el historial que el usuario <<profilename>> a visitado.
Subdirectorios en C:\Documents and Settings\<<profilename>>\Local Settings\History\History.IE5\	Este directorio contiene un archivo index.dat para cada uno de los dias que el usuario <<profilename>> a navegado
C:\Documents and Settings\ <<profilename>>\Temporary Internet Files\Content.IE5\	Este directorio contiene un archivo index.dat para todo el contenido cache que el usuario <<profilename>> a visitado en la web. El archivo index.dat apunta a subdirectorios que contienen el contenido web en caché.
Subdirectorios en C:\Documents and	Estos directorios contienen todos los archivos almacenados en caché para

Settings\<<profilename>>\Temporary Internet Files\	el usuario llamado <<profilename>> que IE almaceno al ver los sitios web.

Tabla 6 - Directorios correspondientes a los archivos de IE

Tres herramientas principales opensource nos permiten reconstruir la actividad web de Lewis:

- ✓ Web Historian (Red Cliff Consulting)
- ✓ Galleta
- ✓ Pasco

Estas herramientas son independientes de la plataforma, lo que significa que se puede ejecutar en Linux, Windows, Mac OS X. Pasco fue desarrollado debido a la falta de codigo abierto, herramientas multiplataforma capaces para el analisis forense.

Web Historian analiza los datos desde cualquier navegador web y se presenta en una aplicación nativa de Windows.
Analizamos en archivo index.dat de la ruta:

C:\Documents and Settings\rlewis\Local Settings\History\History.IE5\

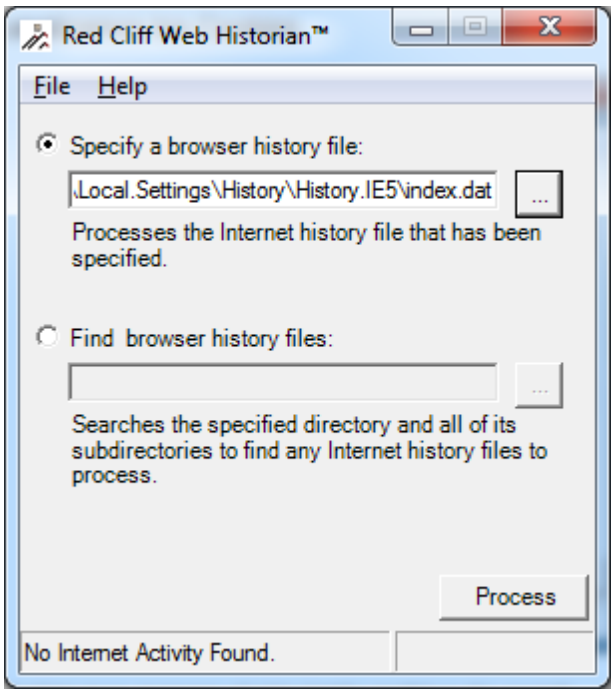
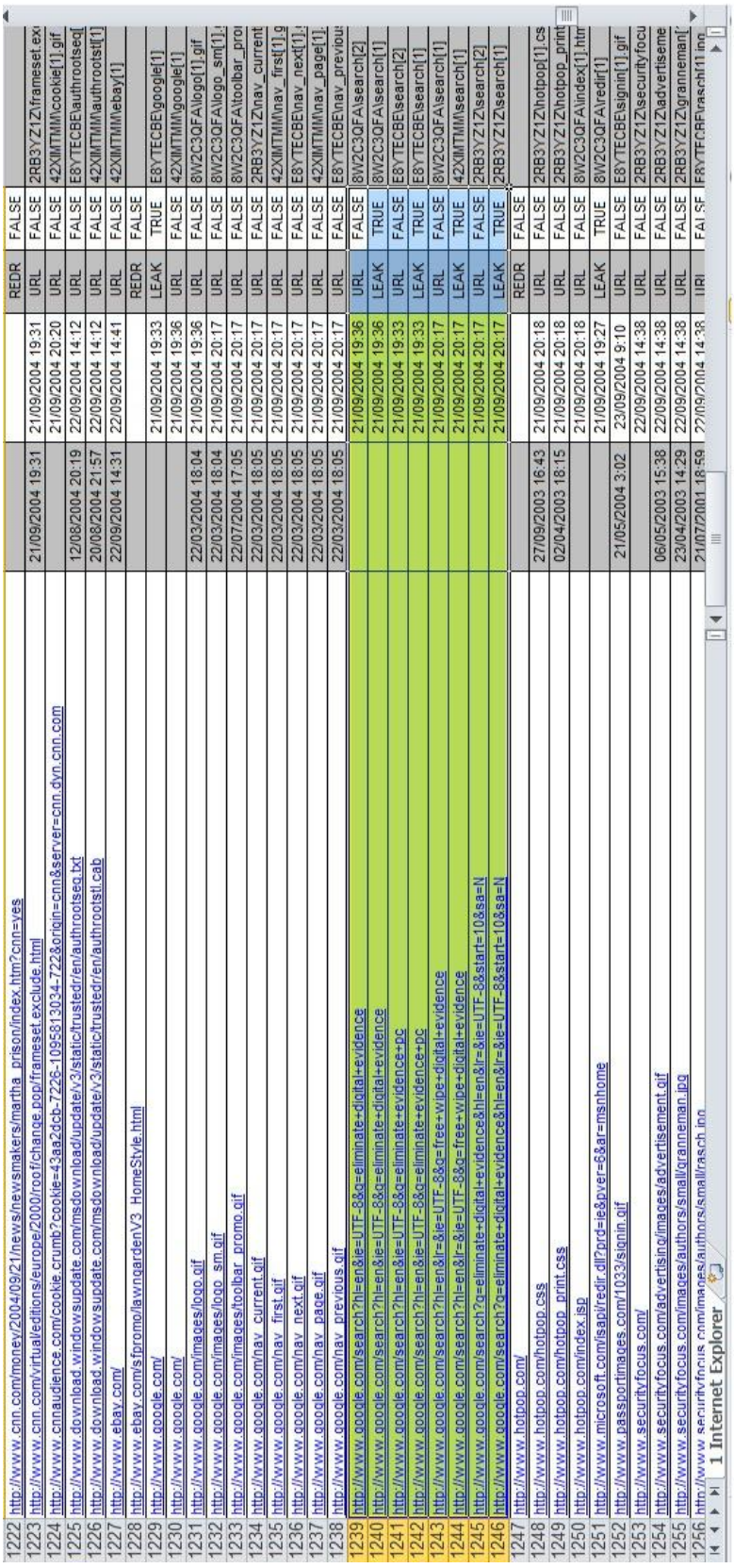


Figura 41 - Web historian

Damos clic en procesar y automáticamente se nos va a generar una hoja de cálculo indicando las actividades realizadas con el respectivo usuario quien ha manipulado dicha información.

2	URL Address	Modified Time	Accessed Time	Type	Deleted
3	Visited: rlewis@http://www.google.com/search?hl=en&ie=UTF-8&q=eliminate+evidence+pc	21/09/2004 19:33	21/09/2004 19:33	URL	FALSE
4	Visited: rlewis@http://www.sysinternals.com/ntw2k/utilities.shtml	22/09/2004 14:01	22/09/2004 14:01	URL	FALSE
5	Visited: rlewis@http://us.rd.yahoo.com/reg/login/new_ym/us/*http://billing.mail.yahoo.com/bm/MailReg?signup=Sign+Up+Now	21/09/2004 19:28	21/09/2004 19:28	URL	FALSE
6	Visited: rlewis@http://us.f613.mail.yahoo.com/ym/ShowLetter?Idx=0&Search=&YY=15002&order=down&sort=date&pos=0	21/09/2004 19:31	21/09/2004 19:31	URL	FALSE
7	Visited: rlewis@http://us.f613.mail.yahoo.com/ym/ShowLetter?Msgld=7007_3633_284_974_447_0_5_-	22/09/2004 7:59	22/09/2004 7:59	URL	FALSE
8	Visited: rlewis@http://edit.yahoo.com/config/last_subscribe	21/09/2004 19:30	21/09/2004 19:30	URL	FALSE
9	Visited: rlewis@http://us.f613.mail.yahoo.com/ym/login	22/09/2004 20:11	22/09/2004 20:11	URL	FALSE
10	Visited: rlewis@http://www.evidence-eliminator.com/product.d2w	21/09/2004 19:33	21/09/2004 19:33	URL	FALSE
11	Visited: rlewis@http://billing.mail.yahoo.com/bm/MailReg?signup=Sign+Up+Now	21/09/2004 19:28	21/09/2004 19:28	URL	FALSE
12	Visited: rlewis@http://cgi.ebay.com/ws/eBayISAPI.dll?ViewItem&category=29520&item=4325403610&rd=1	22/09/2004 14:41	22/09/2004 14:41	URL	FALSE
13	Visited: rlewis@http://www.cnn.com/2004/US/09/21/lottery.winner.burglar.ap/index.html	21/09/2004 19:31	21/09/2004 19:31	URL	FALSE
14	Visited: rlewis@http://www.google.com/search?q=eliminate+digital+evidence&hl=en&lr=&ie=UTF-8&start=10&sa=N	21/09/2004 20:17	21/09/2004 20:17	URL	FALSE
15	Visited:	21/09/2004 20:18	21/09/2004 20:18	URL	FALSE
16	Visited: rlewis@http://www.sysinternals.com/ntw2k/source/sdelete.shtml	22/09/2004 14:45	22/09/2004 14:45	URL	FALSE
17	Visited: rlewis@http://us.f613.mail.yahoo.com/ym/Compose?YY=7811&inc=25&order=down&sort=date&pos=0&view=a&head=b&box=Inbox	21/09/2004 20:12	21/09/2004 20:12	URL	FALSE
18	Visited: rlewis@http://www.securityfocus.com	22/09/2004 14:38	22/09/2004 14:38	URL	FALSE
19	Visited: rlewis@http://us.f613.mail.yahoo.com/ym/ShowLetter?Msgld=3198_1616_22_523_447_0_3_-	21/09/2004 19:34	21/09/2004 19:34	URL	FALSE
20	Visited:	21/09/2004 20:34	21/09/2004 20:34	URL	FALSE
21	Visited: rlewis@http://www.msn.com	22/09/2004 14:38	22/09/2004 14:38	URL	FALSE
22	Visited: rlewis@http://www.ebay.com	22/09/2004 14:41	22/09/2004 14:41	URL	FALSE
23	Visited:	21/09/2004 19:44	21/09/2004 19:44	URL	FALSE
24	Visited: rlewis@http://cgi.ebay.com/ws/eBayISAPI.dll?ViewItem&category=79670&item=4325234088&rd=1	22/09/2004 14:41	22/09/2004 14:41	URL	FALSE
25	Visited: rlewis@http://us.f613.mail.yahoo.com/ym/ShowLetter?Msgld=5868_6552_902_1007_894_0_9_-	22/09/2004 22:32	22/09/2004 22:32	URL	FALSE
26	Visited: rlewis@http://view.atdmt.com/FKQ/iview/brstmdrc00100061fkq/direct/035555?click=http://www.burstnet.com/ads/ad10937a-	21/09/2004 20:34	21/09/2004 20:34	URL	FALSE
27	Visited: rlewis@http://us.f613.mail.yahoo.com/ym/ShowLetter?Msgld=3003_1110_22_449_55_0_1_-	21/09/2004 19:31	21/09/2004 19:31	URL	FALSE
28	Visited: rlewis@http://misc.weather.com/common/outlets/vi.html?lswe=20006	21/09/2004 19:32	21/09/2004 19:32	URL	FALSE
29	Visited:	21/09/2004 19:33	21/09/2004 19:33	URL	FALSE
30	Visited: rlewis@http://mail.yahoo.com	21/09/2004 19:28	21/09/2004 19:28	URL	FALSE
31	Visited: rlewis@http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome	22/09/2004 14:38	22/09/2004 14:38	URL	FALSE
32	Visited: rlewis@http://us.f613.mail.yahoo.com/ym/Compose?YY=13492	21/09/2004 20:12	21/09/2004 20:12	URL	FALSE
33	Visited:	21/09/2004 20:13	21/09/2004 20:13	URL	FALSE
34	Visited: rlewis@http://edit.yahoo.com/config/eval_register?.v=&.intl=&new=1&.done=&.src=ym&.partner=&.p=&promo=&.last=	21/09/2004 19:28	21/09/2004 19:28	URL	FALSE
35	Visited: rlewis@about:blank	21/09/2004 19:32	21/09/2004 19:32	URL	FALSE
36	Visited: rlewis@http://www.amazon.com/exec/obidos/search-handle-url/index=dvd&field-actor=Edward%20Norton/102-6876763-3564954	21/09/2004 20:18	21/09/2004 20:18	URL	FALSE

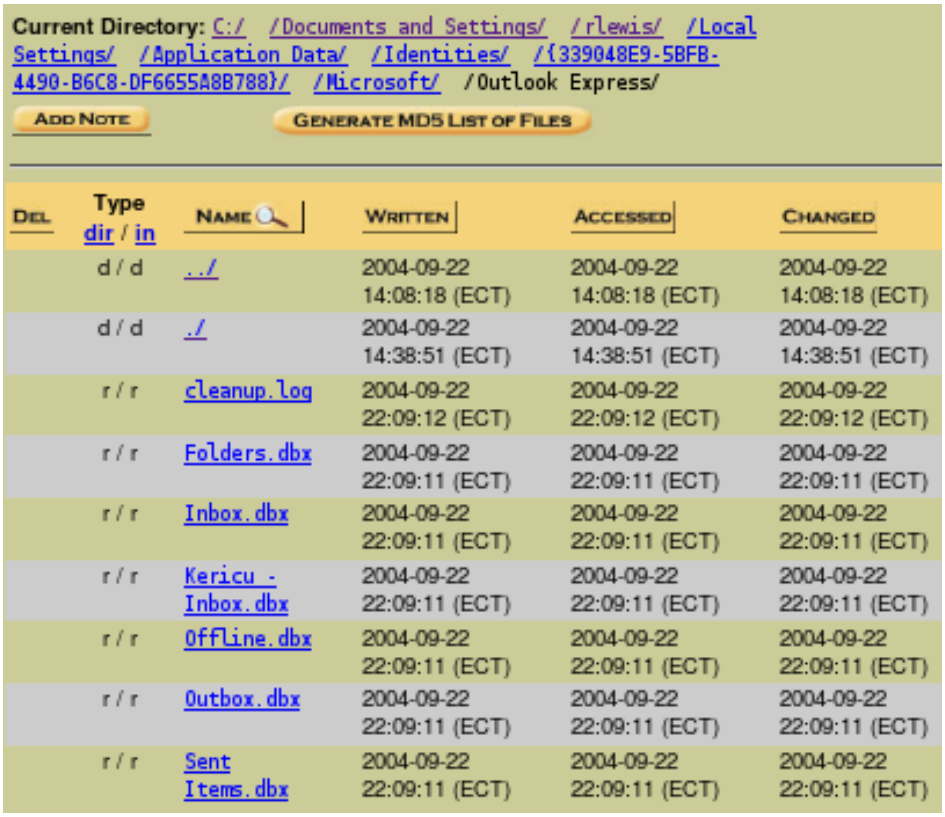
Figura 42 - Resultados de la búsqueda con web historian



1222	http://www.cnn.com/money/2004/09/21/news/newsmakers/martha_prison/index.htm?cnn=yes				REDR	FALSE		
1223	http://www.cnn.com/virtualeditions/europe/2000/roof/change.pop/frameset.exclude.html	21/09/2004 19:31	21/09/2004 19:31		URL	FALSE	2RB3YZ1Z\frameset.ex	
1224	http://www.cnnaudience.com/cookie.crumb?cookie=43aa2dcb-7226-1095813034-722&origin=cnn&server=cnn.dyn.cnn.com		21/09/2004 20:20		URL	FALSE	42XMTMM\cookie[1].gif	
1225	http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootseq.txt	12/08/2004 20:19	22/09/2004 14:12		URL	FALSE	E8YTECBE\authrootseq[	
1226	http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab	20/08/2004 21:57	22/09/2004 14:12		URL	FALSE	42XMTMM\authrootstl[1]	
1227	http://www.ebay.com/	22/09/2004 14:31	22/09/2004 14:41		URL	FALSE	42XMTMM\ebay[1]	
1228	http://www.ebay.com/s/promo/lawngardenV3_HomeStyle.html				REDR	FALSE		
1229	http://www.google.com/		21/09/2004 19:33		LEAK	TRUE	E8YTECBE\google[1]	
1230	http://www.google.com/		21/09/2004 19:36		URL	FALSE	42XMTMM\google[1]	
1231	http://www.google.com/images/logo.gif	22/03/2004 18:04	21/09/2004 19:36		URL	FALSE	8W2C3QFA\logo[1].gif	
1232	http://www.google.com/images/logo_sm.gif	22/03/2004 18:04	21/09/2004 20:17		URL	FALSE	8W2C3QFA\logo_sm[1].g	
1233	http://www.google.com/images/toolbar_promo.gif	22/07/2004 17:05	21/09/2004 20:17		URL	FALSE	8W2C3QFA\toolbar_pro	
1234	http://www.google.com/nav_current.gif	22/03/2004 18:05	21/09/2004 20:17		URL	FALSE	2RB3YZ1Z\nav_current	
1235	http://www.google.com/nav_first.gif	22/03/2004 18:05	21/09/2004 20:17		URL	FALSE	42XMTMM\nav_first[1].g	
1236	http://www.google.com/nav_next.gif	22/03/2004 18:05	21/09/2004 20:17		URL	FALSE	E8YTECBE\nav_next[1].g	
1237	http://www.google.com/nav_page.gif	22/03/2004 18:05	21/09/2004 20:17		URL	FALSE	42XMTMM\nav_page[1].g	
1238	http://www.google.com/nav_previous.gif	22/03/2004 18:05	21/09/2004 20:17		URL	FALSE	E8YTECBE\nav_previou	
1239	http://www.google.com/search?hl=en&ie=UTF-8&q=eliminate+digital+evidence		21/09/2004 19:36		URL	FALSE	8W2C3QFA\search[2]	
1240	http://www.google.com/search?hl=en&ie=UTF-8&q=eliminate+digital+evidence		21/09/2004 19:36		LEAK	TRUE	8W2C3QFA\search[1]	
1241	http://www.google.com/search?hl=en&ie=UTF-8&q=eliminate+evidence+pc		21/09/2004 19:33		URL	FALSE	E8YTECBE\search[2]	
1242	http://www.google.com/search?hl=en&ie=UTF-8&q=eliminate+evidence+pc		21/09/2004 19:33		LEAK	TRUE	E8YTECBE\search[1]	
1243	http://www.google.com/search?hl=en&lr=&ie=UTF-8&q=free+wipe+digital+evidence		21/09/2004 20:17		URL	FALSE	8W2C3QFA\search[1]	
1244	http://www.google.com/search?hl=en&lr=&ie=UTF-8&q=free+wipe+digital+evidence		21/09/2004 20:17		LEAK	TRUE	42XMTMM\search[1]	
1245	http://www.google.com/search?q=eliminate+digital+evidence&hl=en&lr=&ie=UTF-8&start=10&sa=N		21/09/2004 20:17		URL	FALSE	2RB3YZ1Z\search[2]	
1246	http://www.google.com/search?q=eliminate+digital+evidence&hl=en&lr=&ie=UTF-8&start=10&sa=N		21/09/2004 20:17		LEAK	TRUE	2RB3YZ1Z\search[1]	
1247	http://www.hotpop.com/				REDR	FALSE		
1248	http://www.hotpop.com/hotpop.css	27/09/2003 16:43	21/09/2004 20:18		URL	FALSE	2RB3YZ1Z\hotpop[1].cs	
1249	http://www.hotpop.com/hotpop_print.css	02/04/2003 18:15	21/09/2004 20:18		URL	FALSE	2RB3YZ1Z\hotpop_print	
1250	http://www.hotpop.com/index.jsp		21/09/2004 20:18		URL	FALSE	8W2C3QFA\index[1].htm	
1251	http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome		21/09/2004 19:27		LEAK	TRUE	8W2C3QFA\redir[1]	
1252	http://www.passportimages.com/1033/signin.gif	21/05/2004 3:02	23/09/2004 9:10		URL	FALSE	E8YTECBE\signin[1].gif	
1253	http://www.securityfocus.com/		22/09/2004 14:38		URL	FALSE	2RB3YZ1Z\securityfocu	
1254	http://www.securityfocus.com/advertising/images/advertisement.gif	06/05/2003 15:38	22/09/2004 14:38		URL	FALSE	2RB3YZ1Z\advertiseme	
1255	http://www.securityfocus.com/images/authors/small/oranneman.jpg	23/04/2003 14:29	22/09/2004 14:38		URL	FALSE	2RB3YZ1Z\oranneman[	
1256	http://www.securityfocus.com/images/authors/small/trasch.jpg	21/07/2001 18:59	22/09/2004 14:38		URL	FALSE	E8YTECBE\trasch[1].jpg	

Figura 43 - Resultados de la búsqueda de historiales

4.1.4.4 Análisis de correos electrónicos



Current Directory: C:/ /Documents and Settings/ /rlewis/ /Local Settings/ /Application Data/ /Identities/ /{339048E9-5BFB-4490-B6C8-DF6655A8B788}/ /Microsoft/ /Outlook Express/

ADD NOTE | GENERATE MD5 LIST OF FILES

DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CHANGED
	d / d	../	2004-09-22 14:08:18 (ECT)	2004-09-22 14:08:18 (ECT)	2004-09-22 14:08:18 (ECT)
	d / d	./	2004-09-22 14:38:51 (ECT)	2004-09-22 14:38:51 (ECT)	2004-09-22 14:38:51 (ECT)
	r / r	cleanup.log	2004-09-22 22:09:12 (ECT)	2004-09-22 22:09:12 (ECT)	2004-09-22 22:09:12 (ECT)
	r / r	Folders.dbx	2004-09-22 22:09:11 (ECT)	2004-09-22 22:09:11 (ECT)	2004-09-22 22:09:11 (ECT)
	r / r	Inbox.dbx	2004-09-22 22:09:11 (ECT)	2004-09-22 22:09:11 (ECT)	2004-09-22 22:09:11 (ECT)
	r / r	Kericu - Inbox.dbx	2004-09-22 22:09:11 (ECT)	2004-09-22 22:09:11 (ECT)	2004-09-22 22:09:11 (ECT)
	r / r	Offline.dbx	2004-09-22 22:09:11 (ECT)	2004-09-22 22:09:11 (ECT)	2004-09-22 22:09:11 (ECT)
	r / r	Outbox.dbx	2004-09-22 22:09:11 (ECT)	2004-09-22 22:09:11 (ECT)	2004-09-22 22:09:11 (ECT)
	r / r	Sent Items.dbx	2004-09-22 22:09:11 (ECT)	2004-09-22 22:09:11 (ECT)	2004-09-22 22:09:11 (ECT)

Figura 44 - Análisis de correos electrónicos

En nuestro proyecto a analizar tenemos como correo electronico el outlook express en cual se compone de una serie de ficheros con extensión DBX.

Cada carpeta de mensajes en Outlook Express tiene la extensión dbx, las mismas que contienen los mensajes de

entrada, salida, borrador e información adicional para acceder a estos.

Por ejemplo, la carpeta Inbox.dbx o bandeja de Entrada.dbx corresponde a los correos entrantes.
Adcional tenemos otras carpetas dbx predeterminadas en el directorio de Outlook Express:

- **Folders.dbx**

  Almacena la estructura de las carpetas en forma jerarquica.

- **Offline.dbx**

  Contiene todos los datos de acceso interactivo de cuentas Hotmail si estuviera disponible.

Según el analisis realizado en caine, logramos copiar el archivo de correos electronicos. Una de las herramientas más completa capaz de reconocer los formatos que se utilizan en clientes y servidores de correo electrónico es FTK pero esta herramienta es comercial. En nuestro analsis vamos a utilizar eindeutig ya que es una herramienta Open Source.

Los archivios de la carpeta DBX podemos encontrarlos en la siguiente ruta: C:\Documents.and.Settings\rlewis\Local.Settings\Application.Data\Identities\{339048E9-5BFB-4490-B6C8-DF6655A8B788}\Microsoft\Outlook.Express\

La utilidad eindeutig recupera los correos electrónicos aunque el usuario los haya eliminado pero siempre que exista el fichero DBX.

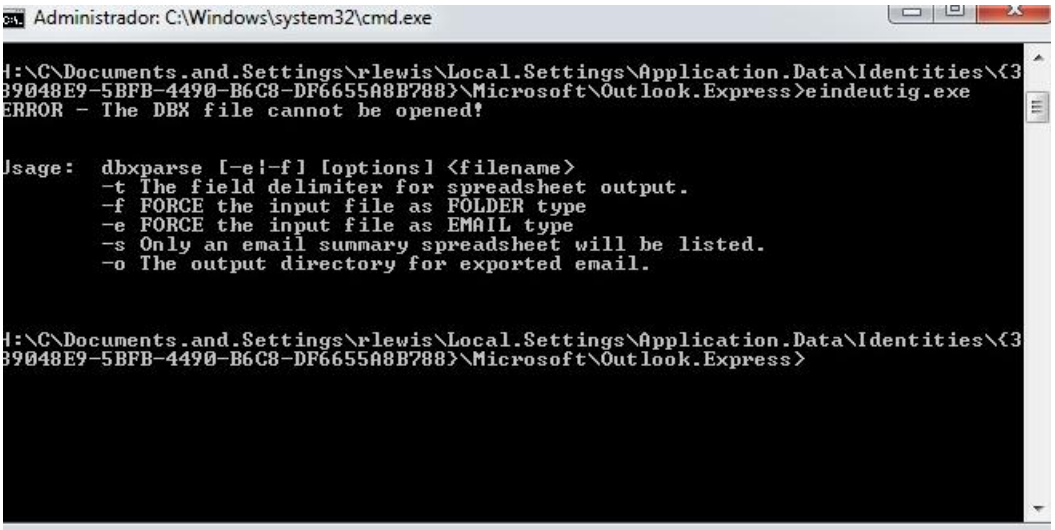


Figura 45 - Utilidad Eindeutig

Vamos a ejecutar la utilidad eindeutig dentro de la ruta antes mencionada, lo cual nos proporcionarà un error porque debemos seleccionar el archivo DBX que vamos a visualizar.

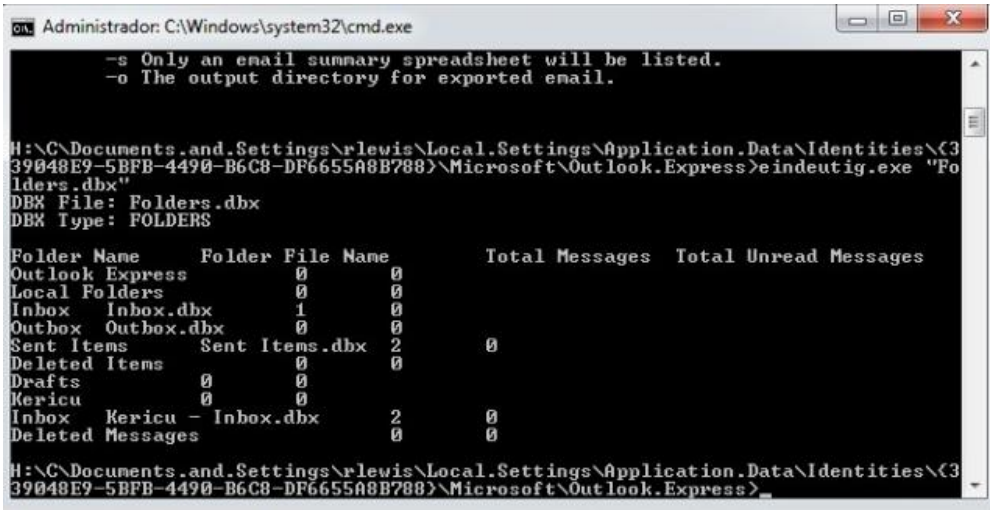


Figura 47 - Reconstruyendo el archivo Folders.dbx con eindeutig

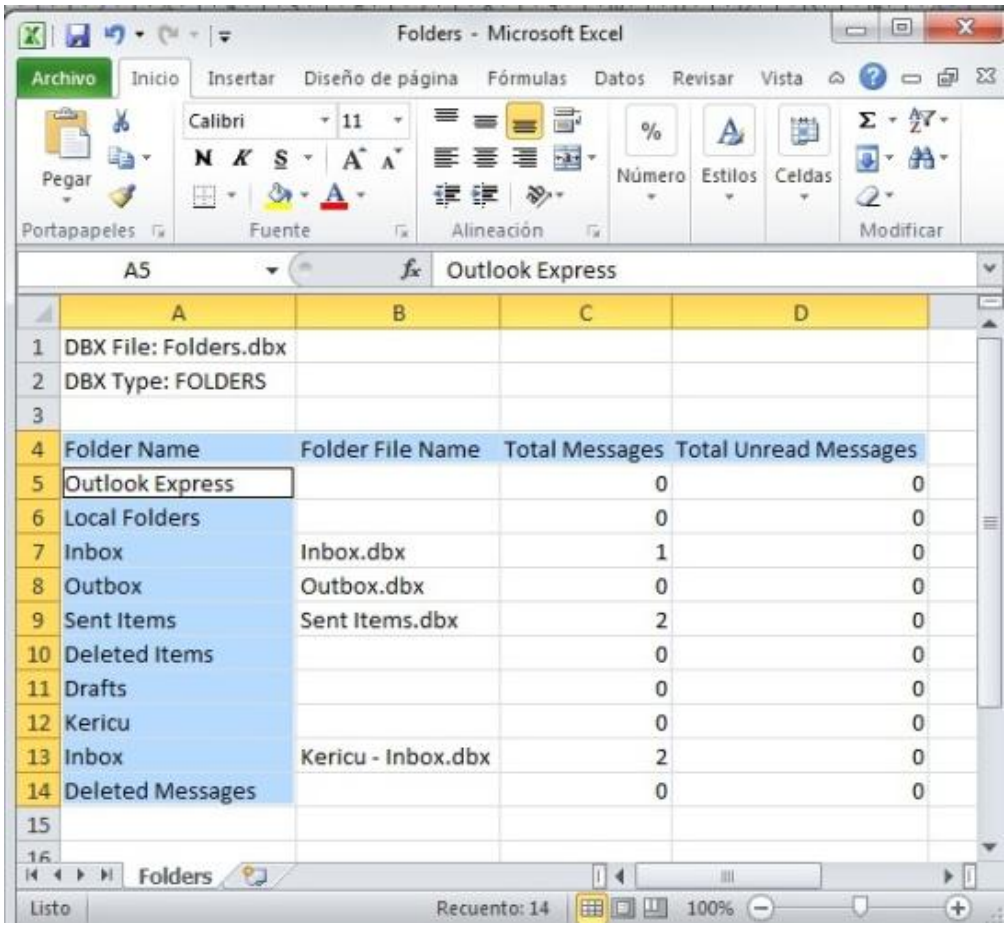


Figura 46 - Archivo Folders.dbx en xls

Ahora vamos a ejecutar eindeutig en el archivo Folders.dbx de lewis y nos mostrará la cantidad de correos que tenemos en cada carpeta creada del respectivo correo.Tambien podemos importar todos estos datos en una hoja de calculo para tener constancia de un reporte como una evidencia.

Podemos visualizar que tenemos 5 mensajes en el repositorio del correo de Outlook Express de Lewis. Nos especifica cuantos mensajes tenemos en cada archivo DBX. Como siguiente paso vamos a reconstruir a los mensajes que tienen una mayor importancia en nuestra investigación.

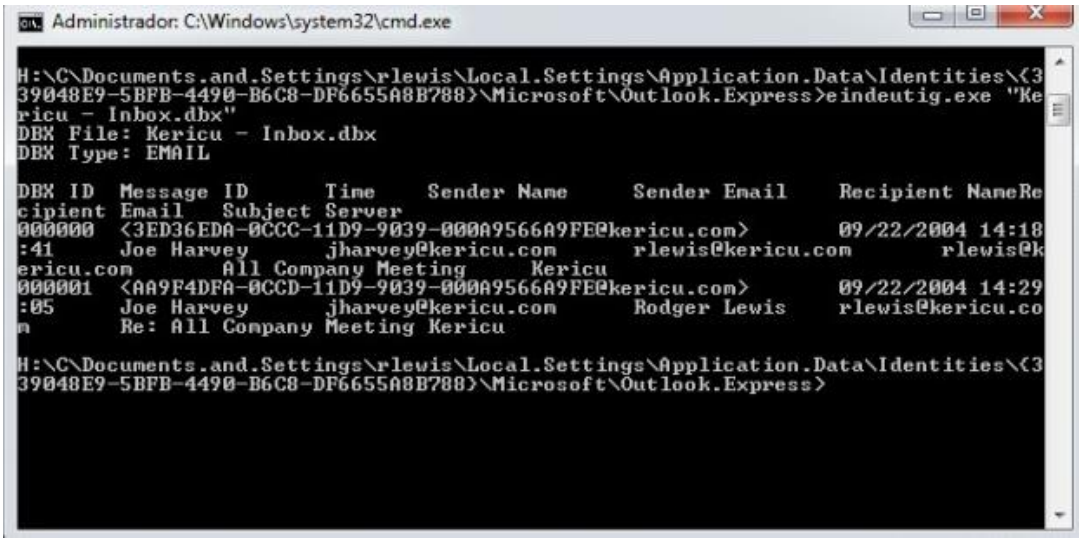


Figura 48 - Procesando eindeutig en el archivo Kericu Inbox.dbx

Examinamos el repositorio del archivo Kericu – Inbox.dbx como lo hicimos en el 1er ejemplo. Podemos notar que nos aparecen 2 archivos y estos también se nos han creado en nuestro directorio donde nos encontramos direccionados.

Como podemos darnos cuenta, tenemos un campo llamado DBX ID el cual es usado unicamente para identificar el correo en una estación forense. En la figura anterior podemos observar que se han creado 2 archivos: 000000.txt y 00001.txt. Cada uno de estos correos corresponden al DBX ID.

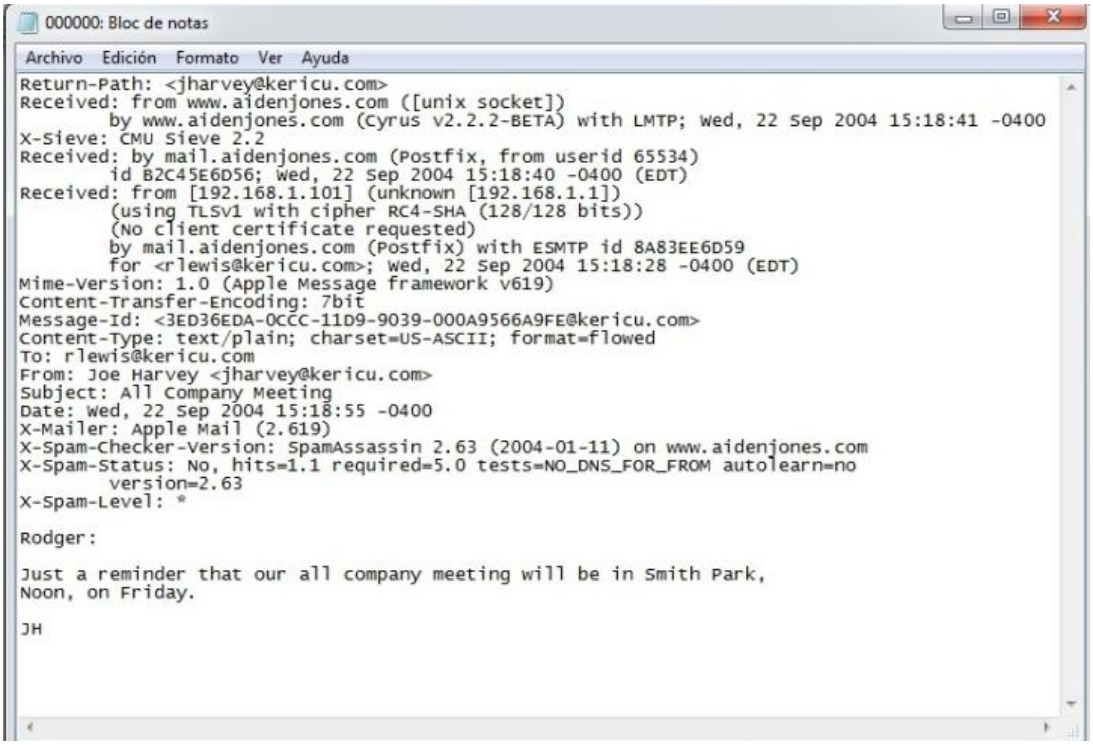


Figura 49 - Contenido del archivo 000000.txt

También podemos revisar cada uno de estos mail con el formato estándar de txt.

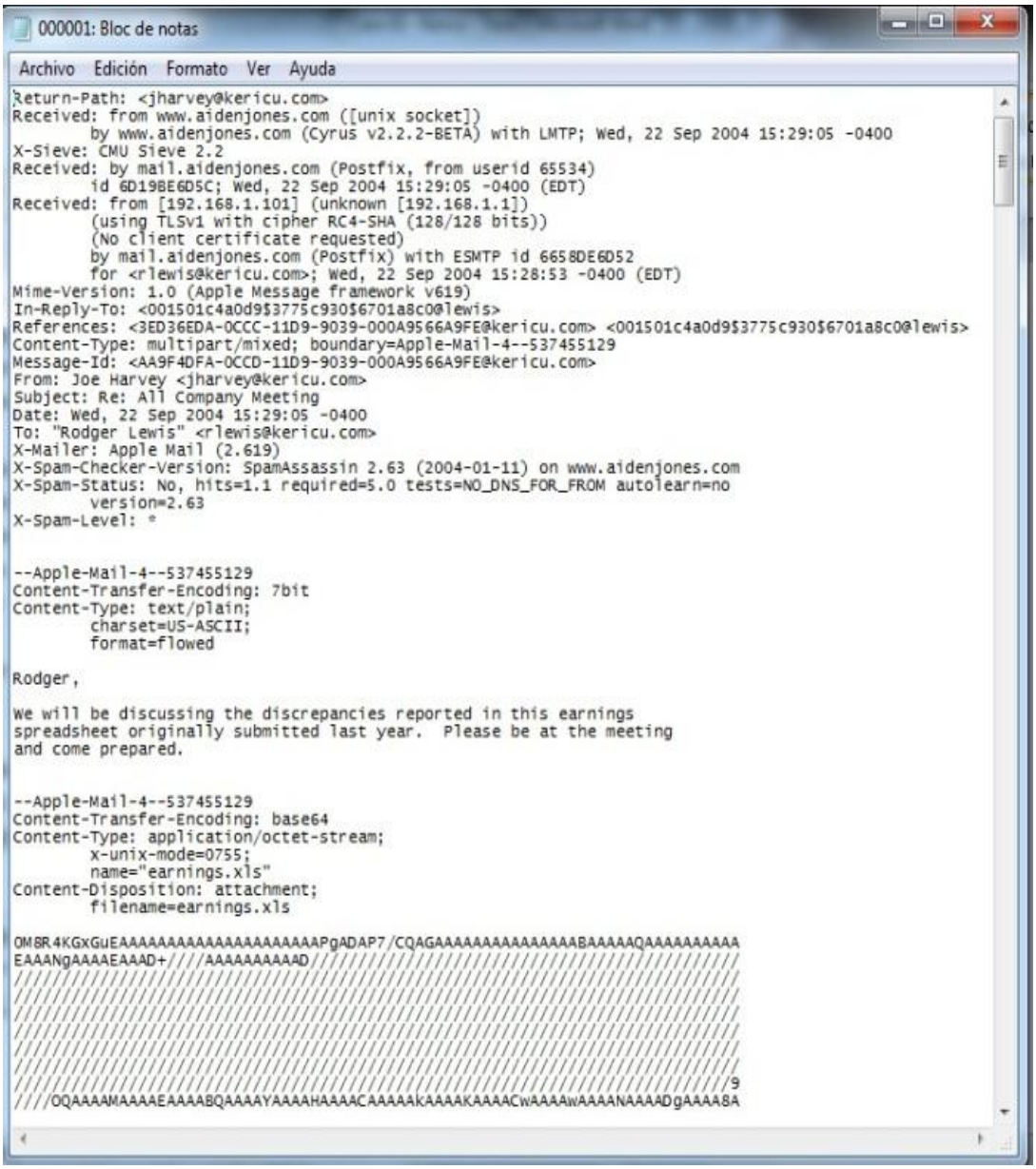


Figura 50 - Contenido del archivo 000001.txt

Podemos notar que tenemos adjunto un archivo en el e-mail.

Nuestra tarea va hacer reconstruir el archivo adjunto utilizando la herramienta munpack.

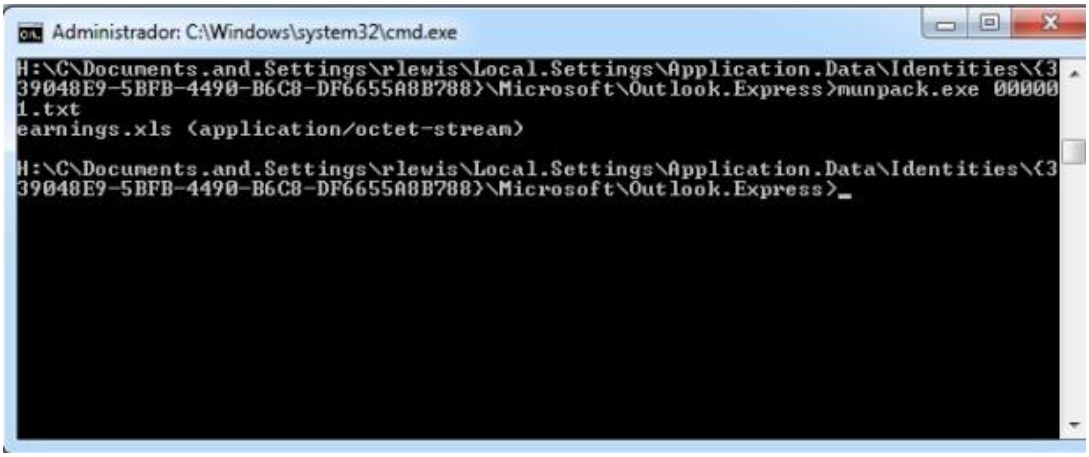
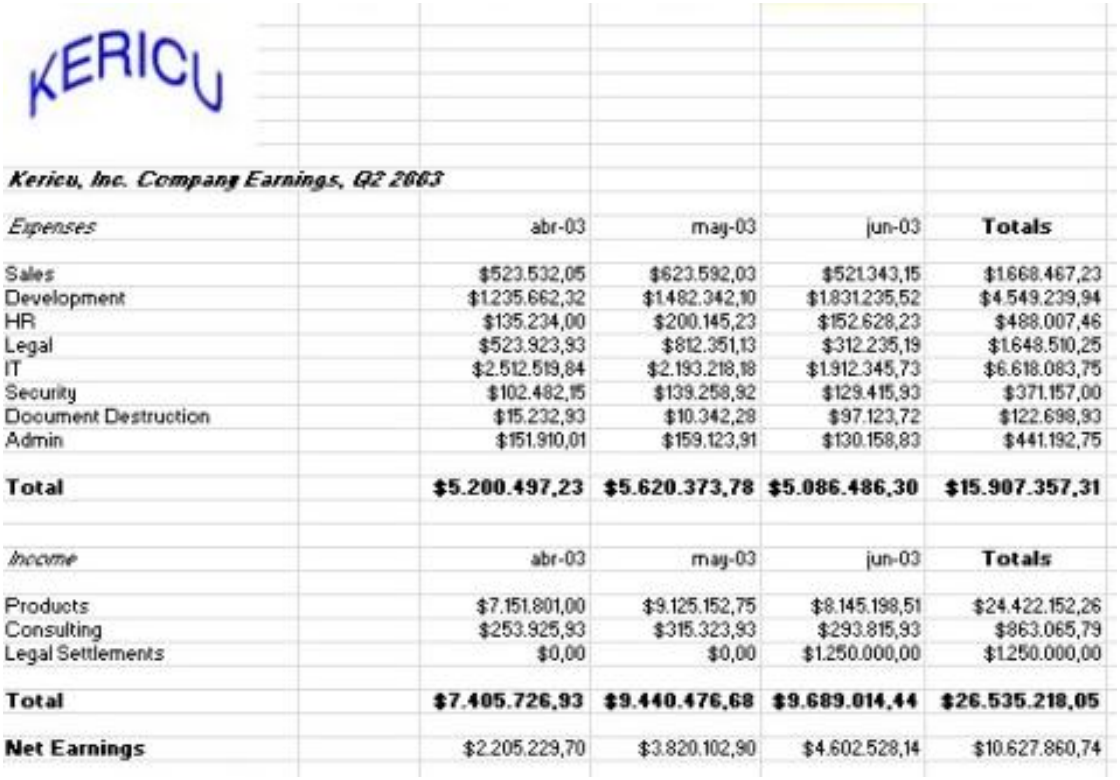


Figura 51 - Reconstruir archivo adjunto con munpack

Ejecutamos munpack en el archivo “000001.txt” , esta utilidad nos reconstruye el archivo que fue adjuntado, “earnings.xls” se nos crea en el directorio donde estamos ubicados.



KERICU

Kericu, Inc. Company Earnings, Q2 2003

Expenses	abr-03	may-03	jun-03	**Totals**
Sales	$523.532,05	$623.592,03	$521.343,15	$1.668.467,23
Development	$1.235.662,32	$1.482.342,10	$1.831.235,52	$4.549.239,94
HR	$135.234,00	$200.145,23	$152.628,23	$488.007,46
Legal	$523.923,93	$812.351,13	$312.235,19	$1.648.510,25
IT	$2.512.519,84	$2.193.218,18	$1.912.345,73	$6.618.083,75
Security	$102.482,15	$139.258,92	$129.415,93	$371.157,00
Document Destruction	$15.232,93	$10.342,28	$97.123,72	$122.698,93
Admin	$151.910,01	$159.123,91	$130.158,83	$441.192,75
Total	**$5.200.497,23**	**$5.620.373,78**	**$5.086.486,30**	**$15.907.357,31**

Income	abr-03	may-03	jun-03	**Totals**
Products	$7.151.801,00	$9.125.152,75	$8.145.198,51	$24.422.152,26
Consulting	$253.925,93	$315.323,93	$293.815,93	$863.065,79
Legal Settlements	$0,00	$0,00	$1.250.000,00	$1.250.000,00
Total	**$7.405.726,93**	**$9.440.476,68**	**$9.689.014,44**	**$26.535.218,05**
Net Earnings	$2.205.229,70	$3.820.102,90	$4.602.528,14	$10.627.860,74

Figura 52 - Archivo adjunto recuperado “earnings.xls”

El archivo earnings.xls es exactamente igual al archivo encontrado anteriormente en la papelera de reciclaje, Dc1.xls el cual fue borrado por el usuario.

Una vez recuperado el archivo adjunto, tambien revisamos los correos enviados por Lewis, estos se encuentran en “Sent Items.dbx”, realizando el mismo procedimiento anterior con la herramienta eindeutig obtenemos el siguiente correo.

```
D:\C\Documents.and.Settings\rlewis\Local.Settings\Application.Data\Identities\{3
39048E9-5BFB-4490-B6C8-DF6655A8B788}\Microsoft\Outlook.Express>eindeutig.exe "Se
nt Items.dbx"
DBX File: Sent Items.dbx
DBX Type: EMAIL

DBX ID  Message ID      Time    Sender Name     Sender Email    Recipient NameRe
cipient Email   Subject Server
000000          09/22/2004 14:12:34     Rodger Lewis    rlewis@kericu.comrlewis@
kericu.com      <rlewis@kericu.com>     Test email      Kericu
```

Figura 54 - Procesando eindeutig en el archivo Sent Items.dbx

000001.txt: Bloc de notas

Archivo Edición Formato Ver Ayuda

```
From: "Rodger Lewis" <rlewis@kericu.com>
To: "Joe Harvey" <jharvey@kericu.com>
References: <3ED36EDA-0CCC-11D9-9039-000A9566A9FE@kericu.com>
Subject: Re: All Company Meeting
Date: Wed, 22 Sep 2004 15:20:26 -0400
MIME-Version: 1.0
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: 7bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2800.1106
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1106

Joe,

I will be unable to make the meeting due to a family event.

Please send along any notes you may have from the meeting.


----- Original Message -----
From: "Joe Harvey" <jharvey@kericu.com>
To: <rlewis@kericu.com>
Sent: Wednesday, September 22, 2004 3:18 PM
Subject: All Company Meeting


> Rodger:
>
> Just a reminder that our all company meeting will be in Smith Park,
> Noon, on Friday.
>
> JH
>
>
>
>
```

Figura 53 – Contenido del archivo 000001.txt en Sent Items

4.1.5 Análisis del archivo de imagen lewis-usb

Adquirimos la imagen del dispositivo usb en formato dd, podemos montarla como un dispositivo loopback ya que existe una diferencia entre un dispositivo usb y un disco duro normal lo cual es la tabla de particiones. En un disco duro podemos crear múltiples particiones pero en un dispositivo usb únicamente tenemos una partición FAT.

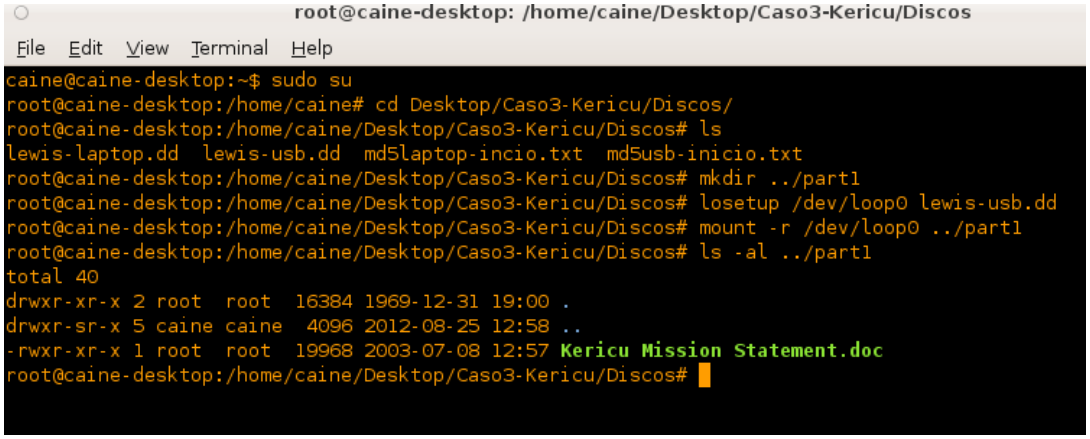


Figura 55 - Montar imagen del dispositivo usb

Creamos el directorio part1 para montar el dispositivo loopback el cual va hacer la imagen del dispositivo USB y accerde a sus respectivos archivos en el mismo.

Luego de verificar los archivos logicos del sitema, podemos ver unicamente un archivo de la evidencia. Si procedemos a

visualizar el archivo con el comando strings para extraer todos el texto ASCII, podemos ver que esto es algo irrelevante para nuestra investigacion.

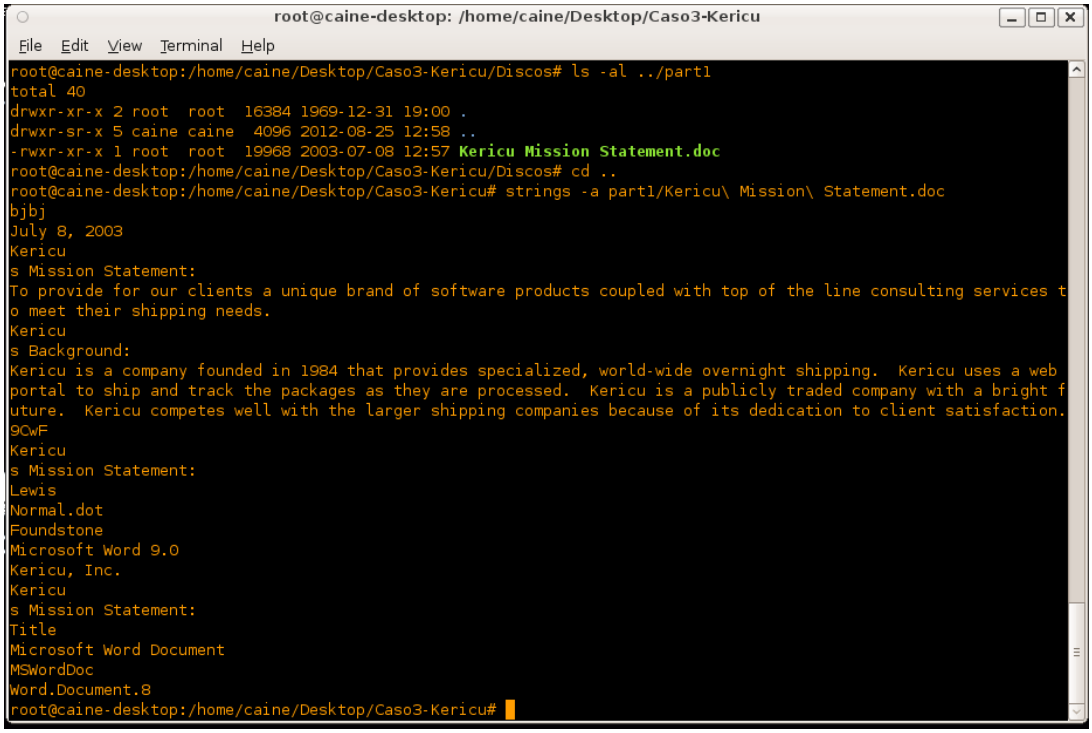


Figura 56 - Archivo encontrado en usb

Hasta el momento no hemos encontrado nada importante para nuestro proyecto. Tenemos que buscar si hay archivos borrados u ocultos y esto lo vamos hacer utilizando el comando fls en la evidencia.

En la siguiente figura podemos observar los archivos borrados encontrados en el dispositivo usb. Los archivos que estan

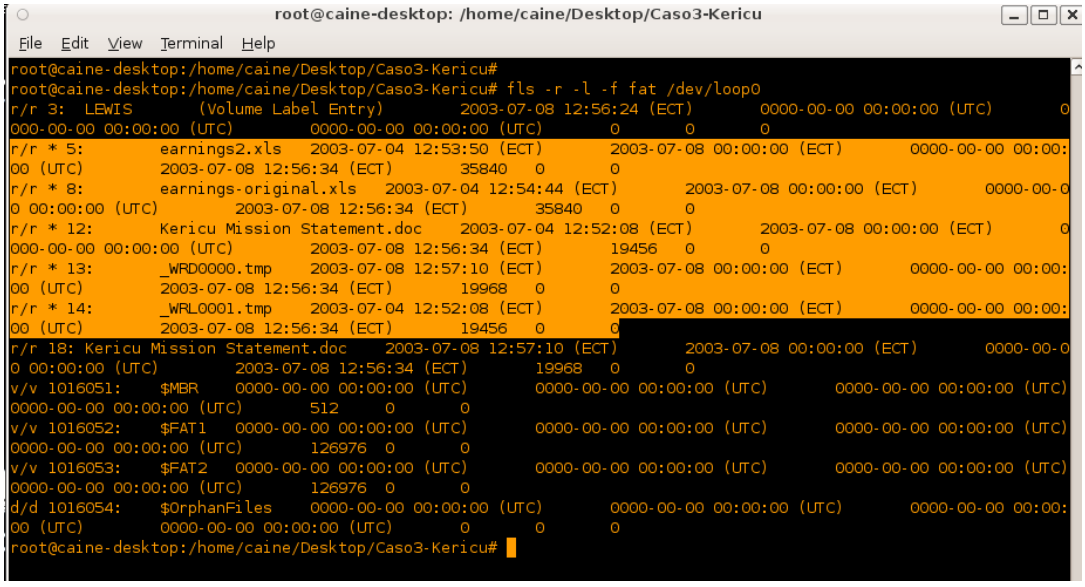


Figura 57 - Archivos borrados encontrados en usb

representados por un asterisco son los que han sido borrados por el usuario, en la figura hemos sombreado los archivos para una mejor ilustracion.

Los archivos estan en formato .xls de Microsoft excel y tienen un tamaño aproximado de 35Kb. El archivo de Microsoft word tiene un tamaño de 20Kb aproximadamente y los demas

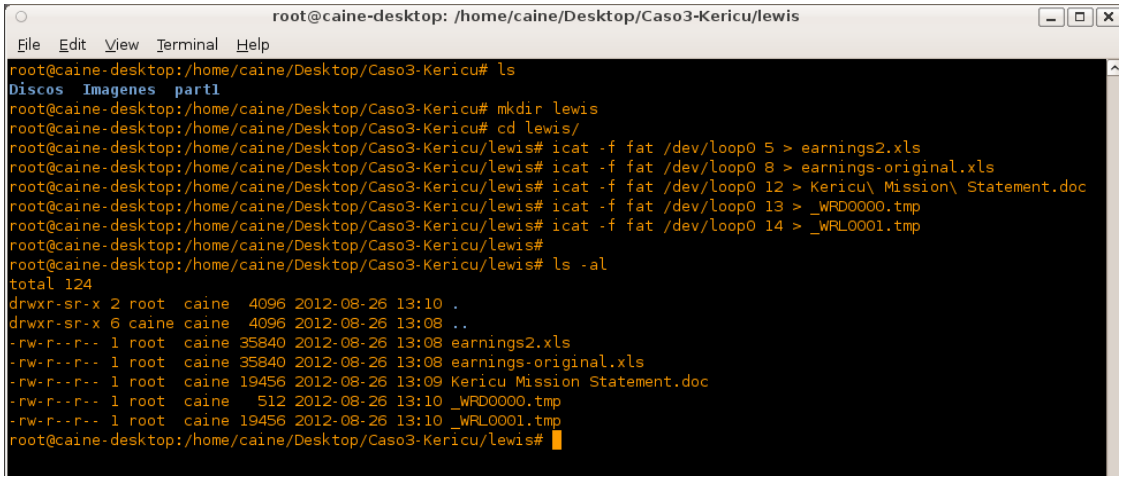


Figura 58 - Duplicación de archivos borrados

archivos son temporales.

Para los archivos forenses vamos a utilizar el comado icat, realizamos una duplicacion de los mismos en el directorio llamado lewis, luego vemos los archivos recuperados en dicho directorio con el comando ls –al. Archivo encontrados en el dispositivo USB:

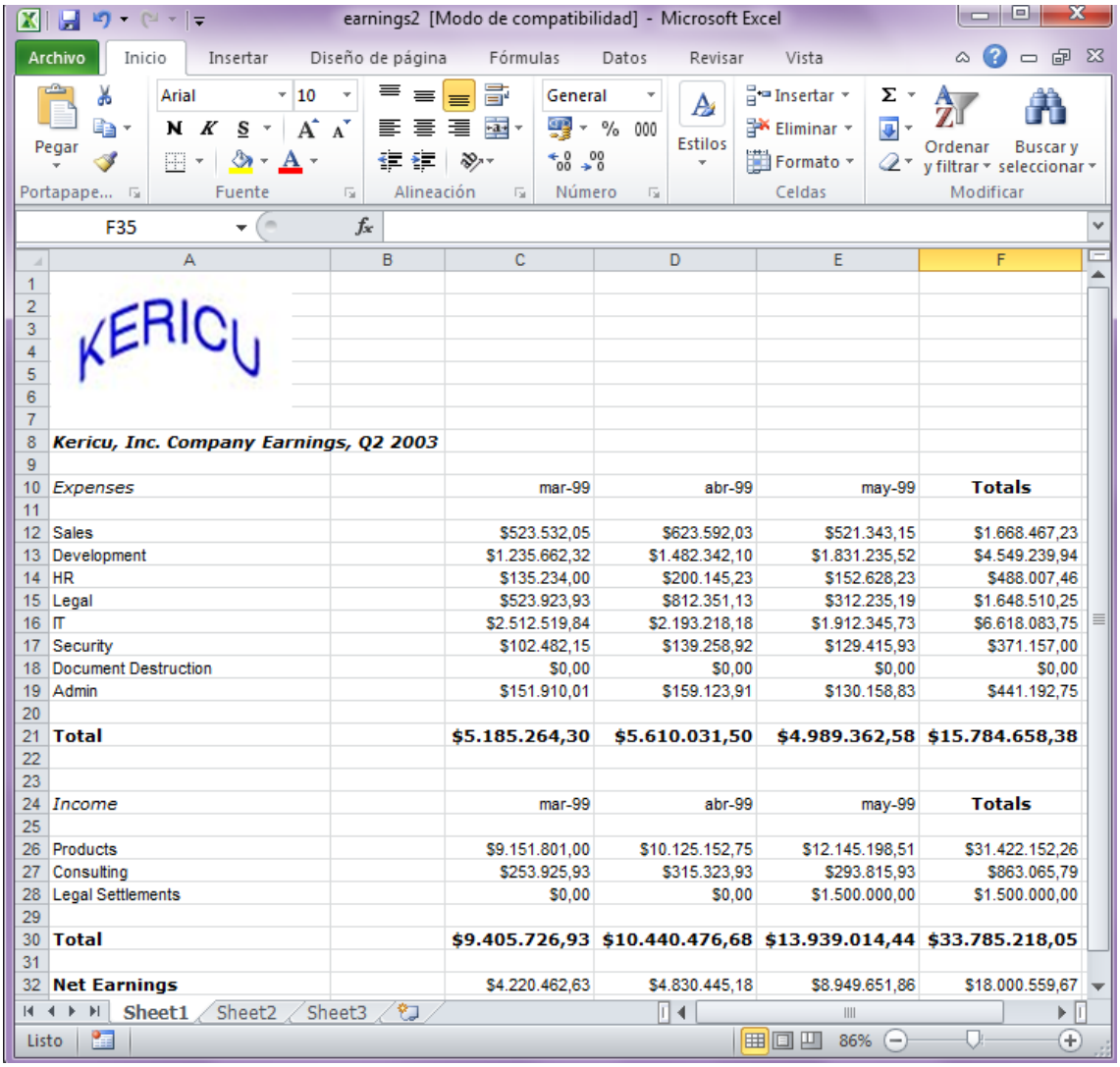
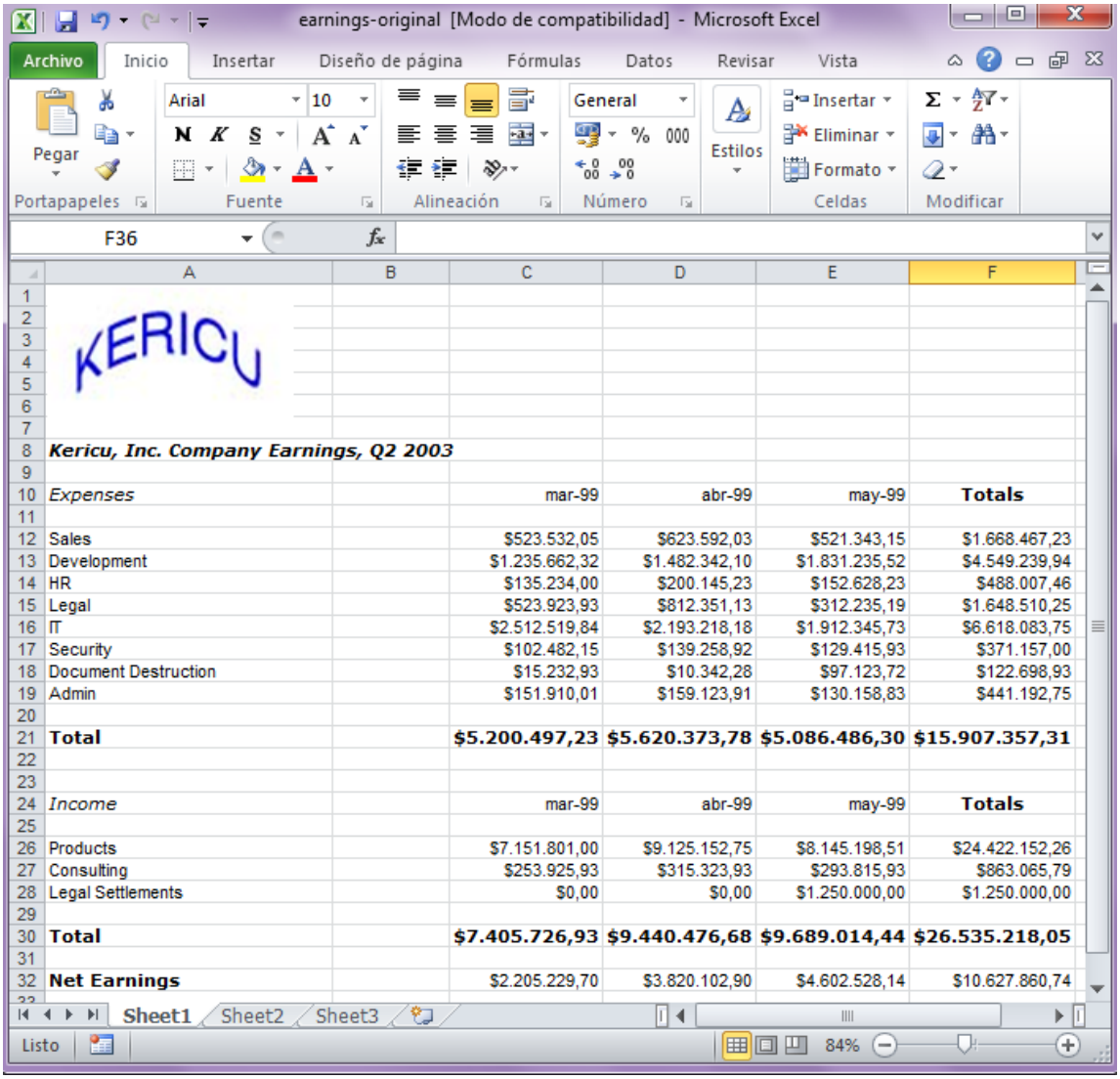


Figura 59 - Hoja de cálculo “earnings2” encontrada en dispositivo usb



earnings-original [Modo de compatibilidad] - Microsoft Excel

Archivo | Inicio | Insertar | Diseño de página | Fórmulas | Datos | Revisar | Vista

F36

	A	B	C	D	E	F
8	***Kericu, Inc. Company Earnings, Q2 2003***					
10	*Expenses*		mar-99	abr-99	may-99	**Totals**
12	Sales		$523.532,05	$623.592,03	$521.343,15	$1.668.467,23
13	Development		$1.235.662,32	$1.482.342,10	$1.831.235,52	$4.549.239,94
14	HR		$135.234,00	$200.145,23	$152.628,23	$488.007,46
15	Legal		$523.923,93	$812.351,13	$312.235,19	$1.648.510,25
16	IT		$2.512.519,84	$2.193.218,18	$1.912.345,73	$6.618.083,75
17	Security		$102.482,15	$139.258,92	$129.415,93	$371.157,00
18	Document Destruction		$15.232,93	$10.342,28	$97.123,72	$122.698,93
19	Admin		$151.910,01	$159.123,91	$130.158,83	$441.192,75
21	**Total**		**$5.200.497,23**	**$5.620.373,78**	**$5.086.486,30**	**$15.907.357,31**
24	*Income*		mar-99	abr-99	may-99	**Totals**
26	Products		$7.151.801,00	$9.125.152,75	$8.145.198,51	$24.422.152,26
27	Consulting		$253.925,93	$315.323,93	$293.815,93	$863.065,79
28	Legal Settlements		$0,00	$0,00	$1.250.000,00	$1.250.000,00
30	**Total**		**$7.405.726,93**	**$9.440.476,68**	**$9.689.014,44**	**$26.535.218,05**
32	**Net Earnings**		$2.205.229,70	$3.820.102,90	$4.602.528,14	$10.627.860,74

Sheet1 | Sheet2 | Sheet3

Listo

84%

Figura 60 - Hoja de cálculo "earnings-original" encontrada en dispositivo usb

Observamos que hasta el momento los archivos Dc1.xls, earnings.xls y earnings-original.xls son iguales.

CAPITULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

1.- La presente tesis se enfocó en investigar quien o quienes habían alterado los estados financieros de la empresa a su favor. El objetivo general fue alcanzado ya que se realizó una auditoria forense del caso, analizando las imágenes proporcionadas de los dispositivos que tenía Lewis como su laptop y su usb.

2.- Analizar los historiales del explorador utilizado nos permitió visualizar las páginas de internet accedidas por el usuario rlewis ya que esta información se guarda en archivos temporales con todos los datos respectivos, estos

datos también se van eliminando conforme se van acumulando según las peticiones del usuario para liberar espacio y acelerar el proceso del explorador utilizado. Estos archivos temporales encontrados en la imagen lewis-laptop.dd nos demostró que dicho usuario ha estado buscando información de eliminar evidencia digital en su equipo.

3.- Respecto a Outlook Express luego de recuperar y analizar el archivo .dbx, el cual contiene todas las carpetas del correo electrónico, nos presentó 5 correos (total), nos enfocamos en el repositorio Kericu - Inbox.dbx el cual tenía 2 correos del usuario jharvey y unos de estos correos tenía un archivo adjunto (hoja de cálculo, earnings), este archivo en uno de los estados financieros de la compañía.

4.- La papelera de reciclaje, donde por defecto se guardan los archivos eliminados por el usuario, también se encontró un archivo de Excel y este es exactamente igual al que encontramos anteriormente en el correo electrónico.

5.- Por otra parte en el dispositivo usb de Lewis encontramos 2 archivos de Excel (hoja de cálculo), tienen el nombre de earnings2.xls y earnings-original.xls, los mismos que demuestran la alteración de los estados financieros ya que los archivos earnings-original.xls, Dc1.xls (papelera de

reciclaje) y a earnings.xls (correo electrónico) son exactamente idénticos los cuales son los estados financieros originales y el alterado es earnings2.xls encontrado en el dispositivo usb como lo indicamos anteriormente.

6.- Esto demuestra que los estados financieros fueron alterados por Roger Lewis, por lo cual representa un grave problema ya que una alteración de estados financieros es un delito penal y el responsable de esto puede terminar en prisión en caso que los afectados lo denuncien. En la mayoría de las empresas los fraudes y los delitos informáticos los realizan personal interno de la compañía, generalmente las personas que tienen un cargo importante, es por esto que las compañías deberían realizar auditoria de seguridad cada cierto tiempo.

5.2 Recomendaciones

Es importante realizar diferentes restricciones a los accesos a búsquedas, o el acceso a información delicada de la empresa, datos que no deben ser modificados o alterados por alguna persona de la empresa.

5.2.1 Auditar eventos de seguridad

Crear un plan de auditoría clasificando el tipo de información que deseamos obtener mediante la recopilación de eventos de la organización. Realizar un seguimiento de las actividades de los

usuarios como por ejemplo si los intrusos obtienen derechos y permisos de administrador, o si los administradores abusan de sus derechos y permisos y borran el registro de seguridad, sin dejar rastro de sus acciones, así como los sucesos relacionados con la creación, apertura o eliminación de archivos u otros objetos. Una entrada de auditoría en el registro de seguridad contiene la información siguiente:

- ✓ La acción que se realizó.
- ✓ El usuario que realizó la acción.
- ✓ El éxito o el error del suceso y la hora a la que se produjo el suceso.

5.2.2 Restringir el uso de medios removibles

Restringir el uso de los medios removibles ya que a los usuarios les resulta más difícil hacer copias no autorizadas de los datos de la empresa si en sus equipos no pueden instalar dichos dispositivos. Por ejemplo, si los usuarios no pueden instalar un dispositivo CD-R, no podrán hacer copias de los datos de la empresa en un CD grabable. Esta ventaja no puede impedir el robo de datos, pero crea otra barrera ante su extracción no autorizada. También podemos reducir el riesgo del robo de datos utilizando Group Policy para impedir a los usuarios el acceso de escritura a los dispositivos removibles o que utilizan

medios removibles. Al utilizar Group Policy podemos otorgar acceso por grupo.

5.2.3 Filtrado de datos adjuntos en servidores de correo

Se debe de implementar un sistema de filtrado de archivos adjuntos, ya que pueden contener algún tipo de virus dañino que puede causar un daño significativo a la computadora del usuario o a la organización, como también dañar documentación importante o divulgar información sensible al público, para esto se debe crear una lista de ciertos tipos de archivos que serán bloqueados antes de que ingresen a la organización, se filtra por el tipo del contenido del archivo adjunto o por el nombre del archivo adjunto.

5.2.4 Sistema de administración de documentos

Establecer un sistema de administración de documentos (DMS) con el objetivo de centralizar el almacenamiento compartido de archivos de computadoras y manejar adecuadamente los permisos de acceso a la documentación de acuerdo a los niveles de clasificación establecidos por la organización.

GLOSARIO DE TERMINOS

ASCII: El Código Estándar Americano para Intercambio de Información, es un esquema de codificación de caracteres originalmente basado en el alfabeto Inglés. Códigos ASCII representa texto en computadoras, comunicaciones, equipos y otros dispositivos que utilizan texto. La mayoría de los modernos esquemas de codificación de caracteres están basados en ASCII, a pesar de que soportan muchos más caracteres.

Bash: (Bourne Again Shell), Es un programa informático cuya función consiste en interpretar órdenes, está basado en la shell de Unix, se encuentra en todos los sistemas Linux y en muchos otros UNIX.

Bit: (Binary digit). Un bit es un dígito del sistema de numeración binario. Mientras que en el sistema de numeración decimal se usan diez dígitos, en el binario se usan sólo dos dígitos, el 0 y el 1.

CD: (Compact disk), Disco óptico circular para el almacenamiento de información de forma binaria. La información se almacena de forma digital, o sea, unos y ceros. Almacenan hasta 640 MB, aunque puede extenderse esa capacidad un poco más.

CEO: (Chief Executive Officer), Se dice que el CEO es la persona quien tiene el máximo nivel de decisión en la compañía a la que representa. Por lo general, en empresas de América Latina, este título se conoce como Director General, Gerente General o Jefe ejecutivo.

Cookies: Es un archivo de texto muy pequeño que un servidor de páginas Web coloca en su unidad de disco duro, almacenando información sobre sus preferencias a nivel de la web.

DD: (DiskDoubler), Es una extensión de archivo, la cual nos permite comprimir datos. A diferencia de la mayoría de otros programas que comprimen numerosos archivos en uno solo para la transmisión, DD comprime archivos individuales para ahorrar espacio en el disco.

Delito informático: Son aquellos actos delictivos realizados con el uso de la computadora o medios electrónicos, aquellas operaciones ilícitas realizadas por medio de Internet o que tienen como objetivo destruir y dañar ordenadores.

Duplicación forense de disco: Es una copia idéntica con el contenido completo de un dispositivo o medio de almacenamiento de datos, como un disco duro, un disquete o un disco óptico (CD, DVD). Una duplicación forense

de disco usualmente se produce creando una copia completa, sector por sector, del medio de origen y por lo tanto replicando perfectamente la estructura y contenidos de un dispositivo de almacenamiento.

DVD: (Digital Versatile Disc, disco versátil digital). Es un dispositivo de almacenamiento óptico, no es más que una evolución del CD. Físicamente es muy parecido a los CD-ROM, pero se diferencia de éstos en la forma de almacenar los datos.

Espacio no asignado: Es un espacio lógico en el disco duro en el cual se almacenan los archivos borrados por el usuario ya que cuando los archivos se borran o se eliminan en los sistemas operativos DOS, Windows, Windows 95, Windows 98 y Windows NT, el contenido del archivo en realidad no se borra.

FAT: (File Allocation Table - Tabla de Ubicación de Ficheros). Es un sistema de archivos desarrollado para MS-DOS. FAT es relativamente sencillo. A causa de ello, es un formato popular para disquetes admitido prácticamente por todos los sistemas operativos existentes para computadora personal.

Group Policy: (Directivas de grupo) Es una infraestructura jerárquica que permite a un administrador de red encargado de Active Directory implementar

configuraciones específicas para usuarios y equipos. Las políticas de grupo se definen en dos secciones: la primera que modifica la configuración de clientes o servidores y la segunda que configura el ambiente para los usuarios.

GZ: Extensión de archivos comprimidos mediante el comando gzip en la plataforma Linux.

Hash: Es un valor hexadecimal único que identifica a un archivo o unidad. Es una función para resumir o identificar probabilísticamente un gran conjunto de información.

Hexadecimal: Sistema numérico en base 16, esto significa que contiene 16 símbolos únicos para representar datos: los números del 0 al 9 y las letras de la A a la F (0 1 2 3 4 5 6 7 8 9 A B C D E F).

Host: Termino que se le da a un dispositivo conectado a una red informática. Puede ser un ordenador, un servidor de archivos, un dispositivo de almacenamiento por red, una máquina de fax, impresora, etc.

Hubs: Es un equipo de redes que permite conectar entre sí otros equipos o dispositivos retransmitiendo los paquetes de datos desde cualquiera de ellos hacia todos los demás.

Imagen ISO: Es un archivo que posee una copia idéntica de determinado sistema de archivos. Es decir que podría haber imágenes ISO producidas en base a copias de una partición de un disco duro, de un diskette, de una memoria USB, o de un CD o DVD, aunque este último caso es el más común, dado que suelen distribuirse vía Internet imágenes completas de sistemas operativos u otro tipo de software, generalmente con extensión ".iso".

Integridad de datos: La exigencia de integridad de los datos garantiza la calidad de los datos de la base de datos ya que estos no pueden ser alterados.

Loopback: Es una interfaz de red virtual. La dirección ip 127.0.0.1 se suele utilizar cuando una transmisión de datos tiene como destino el propio host. La dirección de loopback es una dirección especial que los hosts utilizan para dirigir el tráfico hacia ellos mismos.

MD5: (Message Digest Algorithm 5, Algoritmo de Resumen del Mensaje 5) es un algoritmo que se utiliza para verificar la integridad de los datos a través de la creación de un resumen del mensaje de 128 bits de entrada de datos.

Medios booteables: Son medios de almacenamiento donde se guarda la información necesaria para el arranque de algún programa específico o ya sea del propio sistema operativo.

Memorias USB: (Universal Serial Bus - USB), es un dispositivo de almacenamiento que utiliza una memoria flash para guardar información. Se la conoce también con el nombre de unidad flash USB, pen drive, entre otros. Estas memorias son resistentes a los rasguños (externos), al polvo, y algunos hasta al agua, factores que afectaban a las formas previas de almacenamiento portátil, como los disquetes, discos compactos y los DVD.

Open source: (Código abierto), Es el término con el que se conoce al software distribuido y desarrollado libremente. Fue utilizado por primera vez en 1998 por algunos usuarios de la comunidad del software libre, tratando de usarlo como reemplazo al ambiguo nombre original en inglés del software libre (free software).

Proxy: Es un programa o dispositivo que realiza una tarea acceso a Internet en lugar de otro ordenador. Un proxy es un punto intermedio entre un ordenador conectado a Internet y el servidor que está accediendo. Cuando navegamos a través de un proxy, nosotros en realidad no estamos accediendo directamente al servidor, sino que realizamos una solicitud sobre el proxy y es éste quien se conecta con el servidor que queremos acceder y nos devuelve el resultado de la solicitud.

Router: También conocido como enrutador, es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un router (mediante bridges), y que por tanto tienen prefijos de red distintos.

Scripts: Es un archivo de texto que incluye un conjunto de comandos. Son ejecutados desde la primera línea hasta la última (de forma secuencial). Permiten la atomización de tareas creando pequeñas utilidades. Es muy utilizado para la administración de sistemas UNIX.

Smoking gun: Es una pieza de evidencia que demuestra que algo es cierto o que alguien es responsable de un delito.

String: Es una cadena de caracteres incluido el espacio en blanco, una secuencia ordenada de elementos que pertenecen a un cierto lenguaje formal, una frase o a una oración. En general, una cadena de caracteres es una sucesión de caracteres (letras, números u otros signos o símbolos).

Tabla de particiones: Es donde se guarda la información correspondiente a su organización. En esta se almacena toda la información básica sobre las particiones: si es arrancable, si no lo es, el formato, el tamaño y el sector de inicio.

URL: (Uniform Resource Locator - Localizador Uniforme de Recurso) es un medio estándar de identificar direcciones de internet en la Web. Tiene dos partes, separadas por dos puntos:

- ✓ Antes de los dos puntos: especifica el método de acceso (http, ftp, mail, news...)
- ✓ Después de los dos puntos: se interpreta según el método de acceso. Suele contener direcciones y puntos de acceso en una máquina.

BIBLIOGRAFÍA

[1] Zuccardi, G. y Gutiérrez, J. D., Informática Forense, http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf, fecha de consulta 15 de septiembre 2012.

[2] Rifá, H., Serra, J., Rivas, J. L., Análisis Forense de Sistemas Informáticos, Barcelona Eureca Media SL, septiembre 2009.

[3] Caracciolo, C. B., Más allá de nuestros ojos. Análisis Forense. Quito: Root- Secure, 21 diapositivas, http://www.slideshare.net/lucosa/delitos-informaticos-presentation-758235, noviembre 2010.

[4] Ponce Díaz, V., Peñafiel Anchundia, W., Cobeña Pino, C., Implementación de un Web Site de Comercio Electrónico utilizando una infraestructura de red segura: Autoridad de Certificación, usando esquema PKI para generación de firmas digitales y certificados, Tópico de Graduación previo a la obtención del Título de Ingeniero en Computación Especialización Sistemas Tecnológicos, ESPOL, Guayaquil, 2005.

[5] Keith, J., Belani, R., Web Browser Forensics, Part 1, Symantec, http://www.symantec.com/connect/articles/web-browser-forensics-part-1, fecha de consulta octubre 2012.

[6] Keith, J., Belani, R., Web Browser Forensics, Part 2, Symantec, http://www.symantec.com/connect/articles/web-browser-forensics-part-2, fecha de consulta octubre 2012.

[7] IE History, Biblioteca Gratuita a Internet, http://flylib.com/books/en/3.85.1.140/1/, fecha de consulta octubre 2012.

[8] Martínez, G., Documental sobre el algoritmo MD5, Seguridad en redes http://gabriel-sanmart.blogspot.com/2009/10/definicion-y-funcionamiento.html, octubre 2009.

[9] Keith, J., Reconstrucción de actividades de Internet Explorer, http://ufpr.dl.sourceforge.net/project/fast/Whitepapers/Internet%20Explorer%20Documents/IE_Internet_Activity_Reconstruction.pdf, marzo 2003.

[10] Carrier, B., Herramientas Open Source para evidencia digital, http://www2.opensourceforensics.org/tools/windows, 2003.

[11] Padilla, H., Comando ls Linux, opciones del mismo, http://www.slideshare.net/hpadillaharo/comando-ls, diciembre 2011.

[12] Microsoft. (s.f.), MSDN http://www.microsoft.com, fecha de consulta noviembre 2012.