ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

INFORME DE MATERIA DE GRADUACIÓN

"ANÁLISIS FORENSE DE FRAUDE FINANCIERO KERICU INC."

Previa a la obtención del Título de:

LICENCIADO EN REDES Y SISTEMAS OPERATIVOS

Presentado por:

SOLANGE ISABEL RODRIGUEZ TIGRERO

CARLOS MIGUEL GARZÓN CHACÓN

Guayaquil – Ecuador

2013

AGRADECIMIENTO

Primero y siempre a Dios, quien ha sido guía

y nos ha dado vida para seguir cumpliendo

cada meta, cada sueño y nos permite

compartirlo con nuestros seres queridos.

DEDICATORIA

A nuestros padres, porque gracias a su esfuerzo y dedicación en nuestra vida estudiantil estamos a punto de superar una meta más en nuestra vida.

TRIBUNAL DE SUSTENTACIÓN

_____

Ing. Karina Astudillo

PROFESOR DEL SEMINARIO DE GRADUACION

_____

Ing. Albert Espinal

PROFESOR DELEGADO POR LA UNIDAD ACADEMICA

DECLARACIÓN EXPRESA

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

SOLANGE RODRIGUEZ

CARLOS GARZON CHACÓN

RESUMEN

Fuimos participantes del seminario “Computación Forense” y recibimos el caso de Kericu Inc., empresa que sospecha de un posible fraude financiero ejecutado por uno de sus ejecutivos. Con el uso de las diferentes herramientas de libre distribución y diferentes conocimientos aprendidos durante el seminario pudimos determinar el método y hallar la información original del estado financiero de la empresa.

En el primer capítulo, realizamos una recapitulación de lo aprendido durante el seminario, exponemos conceptos teóricos de la computación forense así como su importancia y también desventajas. Además resaltamos las principales características que deben tener un análisis y el analista forense.

También consideramos los procesos que se llevan a cabo durante dicho análisis.

En el segundo capítulo, hacemos un recuento de las herramientas utilizadas durante nuestro proyecto para su desarrollo, considerando que todas son de libre distribución, y detallamos en qué parte del proyecto están siendo utilizadas cada una de ellas.

Así mismo damos a conocer la fuente del caso así como la evidencia proporcionada por el cliente para su análisis.

En el tercer capítulo, contemplamos ya el proceso que empleamos para realizar la obtención de la evidencia, el proceso para extraer la información presente y “ausente”. También exponemos la creación de líneas de tiempo para los dispositivos recibidos por el cliente, así como el análisis de los encabezados de correos. Además gracias a las herramientas usadas establecimos un detalle cronológico de las actividades realizadas en ambas unidades

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

INTRODUCCION

En el mes de Enero, iniciamos el seminario “Computación Forense”, impartido por la Ing. Karina Astudillo, donde revisamos temas relacionados con los diferentes tipos de ataques a diversos dispositivos de comunicación, como computadoras, redes, routers, y cuentas personales de correo, redes sociales y demás.

También, consideramos los temas relacionados con las leyes estadounidenses y nacionales que toman decisiones sobre este tipo de acciones, y en qué momento debemos recurrir a estas.

Como proyecto de Seminario se nos asignó a cada grupo un caso de estudio para realizar el debido análisis mediante el uso de las diferentes herramientas introducidas durante el seminario.

Es así como se nos designó el caso Kericu Inc., empresa desarrolladora de hardware de telecomunicaciones, en la cual sus ejecutivos tienen sospechas de que Rodger Lewis, CEO de Kericu Inc., está alterando sus informes de estados financieros usando sus habilidades por las cuales es conocido y ya acusado por el departamento de justicia.

Para hacer el debido análisis recibimos la respectiva evidencia, disco duro e información de un dispositivo USB del sospechoso, pero como era de esperarse toda la posible información útil ha sido borrada “por completo”.

Es entonces donde empieza nuestro trabajo de Analistas Forenses.

OBJETIVO GENERAL

Investigar electrónicamente dos equipos informáticos de la compañía Kericu, mediante el uso de herramientas de libre distribución, que han sido manipulados por un usuario durante un determinado periodo de tiempo con la finalidad de detectar alguna anomalía en el manejo de los documentos financieros de la empresa.

OBJETIVOS ESPECÍFICOS

- Analizar los archivos contenidos en los dos equipos informáticos, Disco duro de una laptop y un dispositivo USB entregados en evidencia, mediante el uso de un sistema operativo Linux.

- Recuperar los archivos borrados durante el periodo definido y analizar la información financiera.

- Investigar los encabezados de los correos enviados con la finalidad de conocer el autor del fraude financiero.

- Comparación en la información restaurada entre los documentos originales y los modificados con el objeto de confirmar las sospechas de manipulación fraudulenta en los archivos contables.

- Elaborar una línea de tiempo secuencial de la manipulación de los archivos en los dos dispositivos electrónicos.

CAPITULO 1

MARCO TEÓRICO

1.1Computación Forense

El tema de computación forense aún no lo consideramos una ciencia ya que muchos de los temas son tomados desde diferentes ámbitos, no existe un concepto o un régimen a seguir del mismo, puesto que hay mucho conocimiento empírico.

Serie de técnicas metódicas y procedimientos para reunir

Evidencias desde equipos de computación y dispositivos de

Almacenamiento o medios digitales, que puede ser presentado

en una corte de ley en formato coherente y entendible.

Dr. H.B Wolfe

1.2 ¿Por qué es importante la Computación Forense?

A pesar de ser tan importante en la actualidad, carece de uniformidad o estandarización ya que maneja diversas teorías y métodos para llevarla a cabo.

Existen gran variedad de herramientas disponibles en Internet, pagadas y de libre distribución, lo que dificulta la estandarización de la Computación Forense como tal.

Consideramos tan importante el análisis forense a nivel informático, debido al uso masivo de las computadoras para manejar y/o manipular información de nivel crítico para una empresa o institución, ya sea en servidores o dispositivos de almacenamiento extraíble como discos externos, dispositivos USB, entre otros; y como se ve comprometida dicha información en el medio.

A pesar de todos los beneficios que implica revisar y analizar estos temas, la Computación Forense tiene muchas desventajas.

1.3 Desventajas de la Computación Forense

Desafortunadamente, hay muchas desventajas aún en la Computación Forense, como:

- Es un tema que está todavía en etapa de desarrollo.

- El análisis de las evidencias difiere en todos los casos.

- Hay un conocimiento teórico pobre, basado en hipótesis dependiendo de quién analice la evidencia.

- Las conclusiones y recomendaciones no están definidas de manera formal y no siguen un esquema definido, debido a esto no se maneja herramientas estandarizadas, y el trabajo final dependerá enteramente de lo que considere utilizar el analista para trabajar sobre el caso asignado.

1.4 Ataques Informáticos

Llamado también Cyber-Crimen, es el acto ilegal que involucra una computadora, sus sistemas o aplicaciones, como descargar pornografía.

Debemos tomar en cuenta que para considerarse un crimen, este debe ser **Intencional y No Accidental**.

El *crimen* está dividido en ***3T***s:

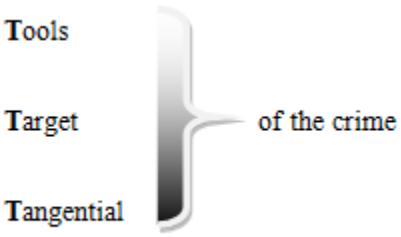


Figura 1: 3T's of the Crime

Las herramientas (Tools) con las que efectuará la vulneración del sistema o robo de la información. El objetivo (Target) que se piensa alterar o hurtar. Y cómo se relaciona con lo que buscamos lograr (Tangential).

1.4 Características de los Cyber-Crímenes

Entre los Cyber-crímenes consideramos los siguientes:

Interno: se realiza desde el interior de una red o de un equipo propio o red.

Externo: cuando se realiza desde otro punto externo al dispositivo afectado.

1.5 Razones del Cyber-Crimen

¿Pero qué los lleva a cometer dichas intrusiones? Entre las motivaciones de estos “Cyber-atacantes” están las siguientes:

- Problemas psicológicos.

- Experimentar el deseo de ser “script kiddies” para aprender.

- Obtención de dinero fácil.

- Espionaje ya sea corporativo o gubernamental.

1.6 Ejemplos de Cyber-Crímenes

Entre los casos que se pueden llevar a cabo como crímenes cibernéticos están:

Robo de propiedad intelectual que hace referencia a cualquier acceso no permitido sobre patentes, secretos, datos y cualquier información que se considere confidencial.

Daño a las redes dentro de una compañía ya sea por envenenamiento de Troyanos, lo que provoca una denegación de servicio, o montaje de una “puerta trasera” para obtener acceso a redes o sistemas.

Fraude Financiero hace referencia a todo lo que comprometa la veracidad de la información financiera de una empresa.

Penetración de un sistema que ocurre mediante el uso de sniffers y herramientas para tomar ventaja de las vulnerabilidades del sistema.

Distribución y ejecución de virus y gusanos, estos se encuentran entre los más comunes métodos para cometer Cyber-crimen.

1.7 Análisis Forense

En el análisis forense contemplamos la acción en la que se toma una evidencia y se realiza mediante el uso de diferentes herramientas el análisis de lo que posiblemente sucedió con la misma.

1.8 Características del Análisis Forense

Para hacer un buen trabajo de análisis es necesario que se consideren ciertos detalles:

- **Reducir la necesidad de analizar la evidencia**, para que el riesgo de que la misma sea alterada sea menor.

- **Obedecer las reglas de evidencia** para garantizar la integridad de la misma.

- **Jamás exceder la base de conocimiento**, no sacar conclusiones precipitadas de temas de los que tal vez no estamos seguros, esto podría alterar los resultados o decisiones tomadas sobre el caso.

- **Documentar cada cambio en la evidencia.-** Realizar algún cambio, significativo o no, puede cambiar los datos en la evidencia, como información en los datos del archivo, fecha de accesos a algún documento, entre otros.

Así como el análisis, la persona que lo realiza debe estar apta y contar con varias virtudes para desempeñar este tipo de tareas.

1.8.1 Características del Analista Forense

Para realizar un análisis correcto, el investigador forense debe gozar de un comportamiento correcto que incluye:

- Conducta profesional, lo que haga durante su carrera será lo que identifique y genere un criterio profesional sobre el analista forense.

- Alto nivel ético e integridad moral, que hará del analista una persona confiable.

- Confidencialidad, es una característica representativa ya que nadie querrá que el caso de su empresa sea divulgado.

Luego de considerar éstas sugerencias antes de realizar el análisis, podemos considerar el procedimiento.

A pesar de los inconvenientes que conlleva hacer un análisis de manera esquemática y la no estandarización de herramientas, el analista forense sigue un patrón para realizar el debido análisis.

1.9 Procedimiento

Para llevar a cabo dicho análisis, el procedimiento empírico es el siguiente:

- **Identificar el crimen.-** Saber qué es lo que está ocurriendo, cual fue el daño, qué es lo que se quiso afectar.

- **Reunir la evidencia.-** Solicitar y buscar toda la información posible que me permita aclarar qué sucedió o quién lo hizo, como archivos borrados, encabezados de e-mails, carpetas, entre otros.

- **Construir una cadena de custodia.-** Formato que identifica todo lo que sucede con la evidencia desde que es adquirida hasta que se da los resultados del análisis. Esto garantiza la integridad de la evidencia.

- **Analizar la evidencia.-** Realizar el debido análisis sobre los posibles cambios, sacar las conclusiones y recomendaciones certeras sobre lo visto en el caso. Es importante resaltar que no se debe hacer acusaciones sin tener bases fundamentadas sobre lo que se expresa.

- **Presentar la evidencia.-** Ya sea delante de un juez o de las autoridades de la empresa, se debe presentar un informe sobre lo que encontramos en la evidencia. Debido a lo delicado de la información, previo al análisis se firma un acuerdo de confidencialidad para mantener la información protegida.

- **Testificar.-** Cuando se lleva el caso a un juzgado, se llama a la persona que realizó el análisis, a testificar sobre lo que encontró; éste es denominado **Testigo Experto** el cual debe contestar las preguntas

que el juez realice de la manera más entendible posible para que el juez o jurado tomen la debida decisión en el caso.

1.10 Metodología de Investigación

1.10.1 Reunirse con el cliente

Conversar con la persona afectada ya sea por pérdida de información o intromisión en su sistema nos ayudará a obtener datos que nos servirán luego como pistas claves y tener una idea más clara de lo que ocurrió.

Al momento de adquirir los primeros datos sobre nuestro tema es importante realizar todas las preguntas posibles sobre lo relacionado. Consultar sobre el comportamiento del sospechoso o considerar detalles incluso en su personalidad puede ser de gran importancia pues muchas personas basan sus claves, códigos en sus comportamientos o situaciones vividas incluso que realizan diariamente.

Luego de realizar todas las preguntas posibles, podemos considerar una idea sobre qué es lo que se va a analizar y hacia dónde tenemos que orientar nuestra investigación, lo que nos da ventaja al momento de armar un diseño previo sobre el cual podemos trabajar al obtener la evidencia

1.10.2 Preparar un diseño detallado

Basado en la serie de preguntas hechas y respuestas obtenidas podemos empezar y direccionar nuestro trabajo, y es aquí cuando ponemos en práctica esta guía; pues solicitamos al cliente nos provea el acceso a la evidencia original, ya sea de un disco o una unidad extraíble, sobre la cual obtendremos una copia o imagen forense para trabajar lo solicitado.

Es importante considerar la importancia y volatilidad de la información que se está manejando ya que si llegáramos a alterar un mínimo de la evidencia

estaremos limitando las posibilidades de encontrar solución al caso, por lo que se recomienda:

- No trabajar directamente sobre la copia forense obtenida, ya que si por error, alteramos los tiempos de acceso o borráramos algún documento, la evidencia no sería totalmente pura y podríamos haber perdido la orientación del caso y la efectividad y confianza en nuestro trabajo.

- Generar al menos dos copias sobre las cuales podamos trabajar para garantizar que la copia original entregada por el cliente permanece sin algún acceso que cambie su estado original.

- Si se diera la necesidad de hacer algún cambio para poder proceder con el análisis, los contratantes deben ser informados sobre dicho

cambio y éste a la vez debe ser registrado en la cadena de custodia para futuras consultas.

1.10.3 Determinar los recursos adquiridos

Debemos considerar las herramientas que debemos y podemos utilizar. Esto depende en gran porcentaje del tipo de sistema operativo sobre el cual trabajaremos ya que no todas las herramientas trabajan con la misma efectividad sobre cada sistema operativo.

Debemos tomar en cuenta, además, que no todas las herramientas que podemos utilizar o en su defecto que son necesarias, están a nuestra libre disposición, ya que muchas de éstas por ser de libre distribución muestran varias limitantes en su desempeño y esto en muchas ocasiones nos obliga a adquirir versiones más completas pero que ameritan un valor monetario.

Si se da el caso de solicitar una herramienta pagada, esto debe ser informado a nuestros clientes para que ellos consideren si es posible adquirir la herramienta o limitar nuestro trabajo a herramientas de distribución libre pero que no nos permiten ahondar en el análisis por sus capacidades cortas de desarrollo.

1.10.4 Identificar los riesgos (“¿qué pasaría si…?”)

Cuando trabajamos con un material del cual no tenemos más que el conocimiento que suponen nuestros clientes o de lo que nos pueda comentar la persona que maneja el equipo a analizar, nos exponemos a que nuestro trabajo no se pueda lleva a cabo de manera exitosa.

Consideramos este punto ya que el cliente como tal, no siempre tiene conocimiento completo de todo lo que se pudo realizar en la unidad analizada o de lo que podamos encontrar. Generalmente crean dudas sobre

esto cuando ocurre un acontecimiento no común en el equipo ya sea una inestabilidad en el sistema o la extraña propagación de información importante que se manejaba solo en dicho dispositivo.

Así mismo, si las preguntas sobre la evidencia se realizan a la persona directamente encargada del equipo, si ésta está consciente de que ha hecho algún daño al equipo, lo más probable es que no nos dé la información necesaria y limite nuestra investigación al punto de no poder encontrar la solución.

Si este es el caso, debemos considerar el hecho de que nuestra investigación no sea exitosa y exponerlo a nuestros contratantes, ya que al obviar este punto nuestros clientes pueden dudar de la efectividad de nuestro trabajo por la falta de información que pudimos adquirir. Es decir, si llegáramos a tener poca información para el caso y en este no se pudiera definir con exactitud qué sucedió, al no explicar este punto al cliente y solo le decimos que no pudimos detectar qué fue lo que sucedió, éste dudara de nuestro trabajo y quitará méritos a nuestro análisis.

Además del ámbito ético, es necesario tomar precauciones en todo lo relacionado con la evidencia, como el espacio del disco a analizar ya que no podemos generar copias del mismo sobre discos de menor capacidad. Se deben prever estas posibilidades que podrían retrasar nuestro análisis.

Asimismo, considerar herramientas compatibles con los sistemas operativos sobre los que trabajamos ya que no podemos garantizar un buen resultado si no estamos seguros de que contamos con las herramientas adecuadas para el debido análisis.

1.10.5 Investigar los datos recuperados

Al realizar el análisis de los datos debemos considerar que muy pocas personas tienen conocimiento de que al borrar la información de alguna carpeta de la papelera de reciclaje y de los dispositivos de almacenamiento extraíble, el archivo no se borra totalmente.

Muchas personas piensan que, con el hecho de borrar visualmente un documento éste ya no existe en el sistema, sin embargo es fundamental tener el concepto de archivos borrados claro y la recuperación de los mismos ya que en muchos casos éstos archivos contienen información importante sobre el análisis del caso.

1.10.6 Reporte

Luego del análisis de los archivos existentes y de los recuperados, realizamos un informe con las novedades encontradas en el análisis, considerando siempre que no debemos ser sugestivos ni dar nuestras opiniones fuera del campo profesional.

Realizar una acusación en un informe no es ético/profesional y da mal aspecto al trabajo realizado y puede además causarnos inconvenientes a futuro si se demuestra que nuestras acusaciones no son verídicas sino solo conclusiones erradas.

1.10.7 Dar testimonio

Si el caso es legal, debemos presentar en un juzgado las conclusiones y pruebas encontradas para guiar al juez a su veredicto. Si el caso es civil, dirigir nuestro informe y reporte oral a quienes nos contrataron para el análisis, para que puedan tomar su decisión sobre el o los empleados involucrados si fuere el caso.

Considerar al igual que en el reporte, no se debe decir más de lo que esté comprobado, ya que hacerlo podría diferir de los resultados originales del caso y desviar el veredicto tomado ya sea por un juez o clientes.

1.11 Introducción al Caso de Estudio

Al ser contratados por la empresa Kericu, recibimos la siguiente información:

Como un examinador forense para el crimen de una entidad policial de informática forense, se ve una gran cantidad de casos que van y vienen. Usted ha pasado el tiempo reportando violaciones de información confidencial, donde ejecutivos de alto nivel alteran documentos financieros para hacer que su empresa se vea mejor en los ojos de sus accionistas. Una de estas empresas, Kericu, Inc., es un desarrollador de hardware de telecomunicaciones. Sus ejecutivos parecen haber capturado un "error de alteración". El CEO de Kericu, Rodger Lewis, es bien conocido por sus habilidades informáticas, y él pudo haber puesto esas habilidades a mal uso. El Departamento de Justicia recientemente acusó a Lewis de alterar estados de cuenta trimestrales para aumentarlas ganancias de su empresa. Debido a que Lewis es conocido por tener"sk1llz" ("habilidades" como es conocido por la comunidad informática clandestina), se espera que haya limpiado sus huellas. Muy poca evidencia puede estar disponible visualmente en el equipo. Según su experiencia, la mayoría de los usuarios avanzados elimina la información de las máquinas, lo que hace que su trabajo sea difícil.

Afortunadamente, el vicepresidente ejecutivo de finanzas, Aiden Paluchi, negoció un acuerdo con el Departamento de Justicia. Si Paluchi testifica en contra del director general, recibirá la inmunidad de cualquier cargo adicional relacionado con este caso. Paluchi entrega al Departamento de Justicia el documento, que Lewis alteró. Paluchi también dice que este documento fue enviado a la totalidad del personal ejecutivo a través de e-mail. Se le proporcionará una copia de este e-mail, listado aquí:

"To: executives@kericu.com

From: aiden.paluchi@kericu.com

Date: Thursday July 3, 2003 15:33:02 (EDT)

Subject: Q2 Earnings Spreadsheet

Attachments: earnings.xls

Gentlemen,

This document is ready for your approval. Please e-mail back any changes that I may have missed. Hopefully next quarter will be better than this one.

Sincerely,

Aiden Paluchi

Executive VP of Finance

Kericu, Inc.”

Usted viaja a la sede Kericu y comienza su análisis. Se empieza por la adquisición de una duplicación forense de la computadora portátil del disco duro de Lewis en formato .dd. Rápidamente se revisa la imagen. Como era de esperarse, no existe earnings.xls en ningún lugar en el disco duro de Lewis. Su trabajo acaba de tornarse mucho más difícil de lo que pensaba, ya que tendrá que hacer un análisis más profundo. Justo en ese momento, un agente se encuentra con usted en su oficina y le presenta un dispositivo USB que se encontró en casa de Lewis. Esperemos que, después de adquirir una duplicación forense del dispositivo, sea posible encontrar evidencia adicional de la supuesta alteración realizada por Lewis.

CAPITULO 2

HERRAMIENTAS

2.1 CAINE 2.0

Es una distribución de Linux basada en Ubuntu 10.04 para **ANALISTAS FORENSES** y administradores responsables de seguridad.

Caine cuenta con una gran selección de software, una interfaz gráfica amigable y un soporte receptivo.

Se desarrolló en modo LiveCD por ***Giancarlo Giustini***, como un proyecto de Informática Forense para el Centro de Investigación de Seguridad en Italia. Se basó en la distribución ***Ubuntu 10.04*** con el Kernel 2.6.32-24 de Linux.

2.1.1 ¿Por qué lo usamos?

En nuestro caso lo usamos por los siguientes motivos:

- No monta las unidades de Disco automáticamente, hay que hacerlo manual.

- Ambiente grafico amigable y fácil de usar.

- Confiabilidad en el manejo de información.

- Incluye la herramienta AUTOPSY.

Figura 2: Interfaz Caine

2.2 AUTOPSY FORENSIC BROWSER

Es una interfaz gráfica que viene incluida en el sistema operativo CaineLinux para la línea de comando, herramientas de análisis digital de investigación de The Sleyth Kit. Juntos, pueden analizar discos de Windows y UNIX y sistemas de archivos (NTFS, FAT,UFS1/2,Ext2/3).

The Sleyth Kit y Autopsy son de código abierto y funcionan con plataformas UNIX.

Debido a que la herramienta Autopsy está basada en HTML, es posible conectarse al servidor de Autopsy de cualquier plataforma usando un navegador de HTML.

Autopsy provee un Administrador de Archivos y muestra detalles acerca de los datos eliminados y estructuras de sistemas de archivos.

2.2.1 ¿Por qué lo usamos?

- Interfaz gráfica amigable.

- Recuperación de archivos borrados.

- Visualización de clústeres no asignados.

- Exportación y visualización de archivos.

- Creación de la línea de Tiempo.

- Análisis de encabezados de e-mails

Figura 3: Interfaz Autopsy Forensic Browser

2.3 VMWARE WORKSTATION 8.0

VMware es un sistema de virtualización por software. Un sistema virtual por software es un programa que simula un sistema físico (un computador, un hardware) con unas características de hardware determinadas. Cuando se ejecuta el programa (**simulador**), proporciona un *ambiente de ejecución* similar a todos los efectos a un computador físico (excepto en el *puro acceso físico* al hardware simulado), con CPU (puede ser más de una), BIOS, tarjeta

gráfica, memoria RAM, tarjeta de red, sistema de sonido, conexión USB, disco duro (pueden ser más de uno), etc.

2.3.1 ¿Por qué lo usamos?

- Virtualización de S.O.

- Soporta imágenes de Discos duros con extensión .dd

Figura 4: Interfaz VmWare WorkStation

CAPITULO 3

PROCEDIMIENTO

3.1 OBTENCIÓN DE LA EVIDENCIA

Se recibió la evidencia en un DVD el cual contenía dos archivos.

3.1.1 LEWIS-USB.DD

Md5: 021c551ea7e36f9806ca4be04c87b6b3

Sha1: 94f678994709b94eb446c356fafeea4e99b6d9e8

3.1.2 LEWIS-LAPTOP.DD

Md5:f1b6de27919b0d299c1a649f8646d35c

Sha1: 961a4684a275617d839b795f783ea4e8fb866357

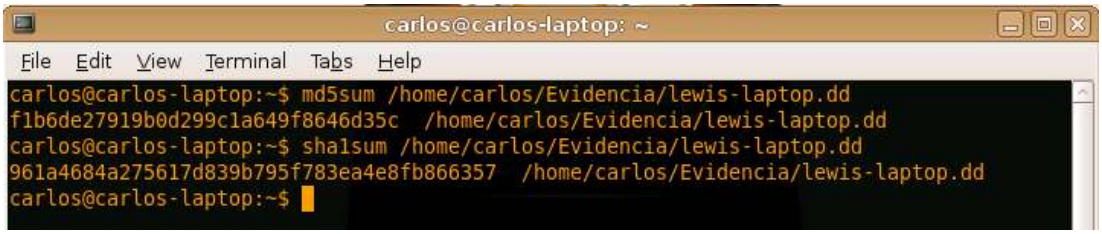


Figura 5: Evidencia Lewis Laptop

Además se recibe un documento que describe el caso el cual incluye información de un correo enviado por Aiden Paluchi, vicepresidente de la compañía, además de un adjunto.

Se escogió trabajar el análisis de los archivos recibidos sobre Caine, Distribución de Linux, la cual está orientada al análisis de imágenes forenses.

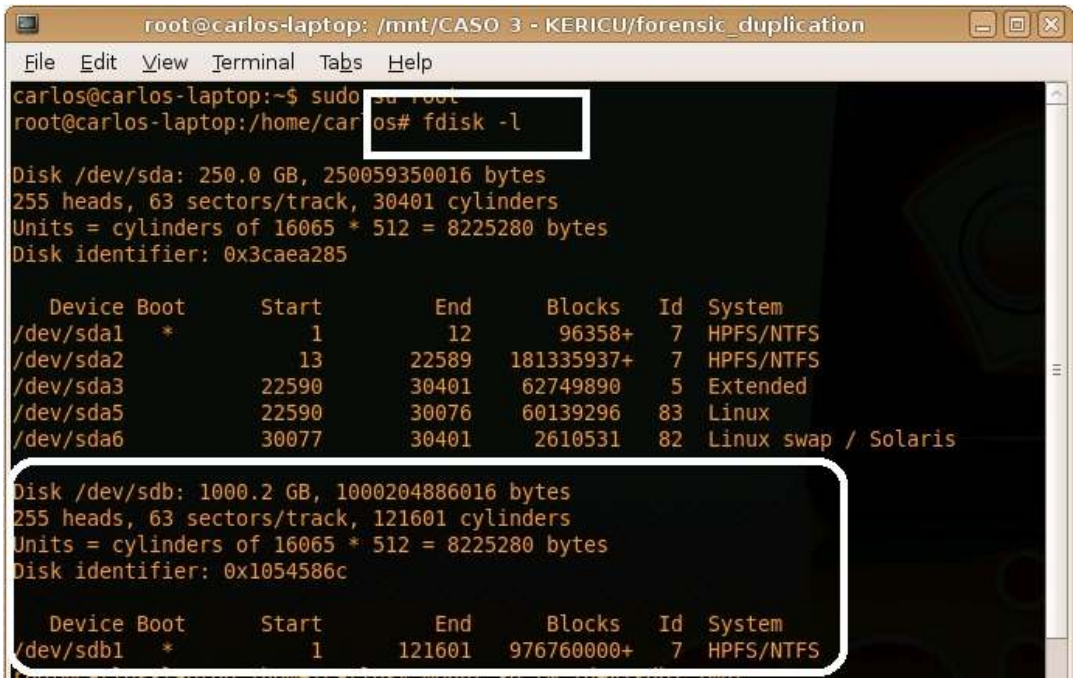


Figura 6: Análisis de Unidades en Disco

Primero, para garantizar la integridad de los datos, se realiza una copia sobre la cual se trabajo dentro ya del ambiente Caine.

Con el comando *fdisk –l* se muestra la ubicación actual de la unidad que se va a analizar, así como todo sus detalles. Con esto se puede pasar a montar la unidad para su debido análisis.

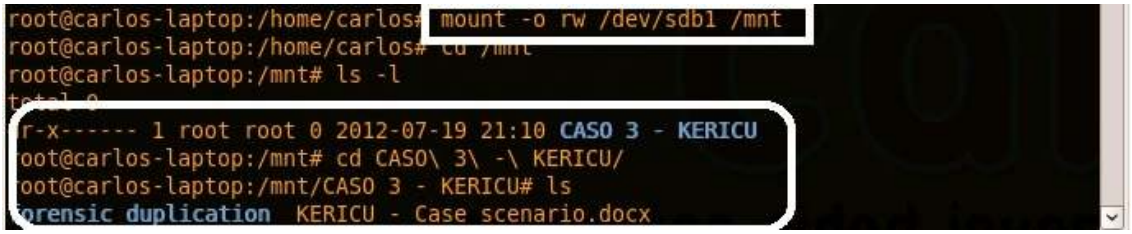


Figura 7: **Montaje de la unidad**

Al montar la unidad se nota el caso presentado y en éste, las copias forenses y la explicación en un documento de Word.

Se descomprime el archivo .gz para realizar el análisis. Para poder descomprimir se tiene que dar permisos lectura y escritura al archivo.

```
root@carlos-laptop:/home/carlos/Evidencia# sudo chmod ugo+rwx lewis-laptop.dd.gz
root@carlos-laptop:/home/carlos/Evidencia# ls -l
total 715624
-rwxrwxrwx 1 root   root   730541531 2012-07-19 21:39 lewis-laptop.dd.gz
```

```
root@carlos-laptop:/home/carlos/Evidencia# gunzip -f lewis-laptop.dd.gz
root@carlos-laptop:/home/carlos/Evidencia# ls -l
total 4200572
-rwxrwxrwx 1 root   root   4294967296 2012-07-19 21:39 lewis-laptop.dd
```

Figura 8: **Descompresión de Disco Lewis Laptop**

Ya se tiene las imágenes listas para que sean analizadas. Para esto se hizo uso de la herramienta **Autopsy**.

Figura 9: **Interfaz Autopsy**

Con la herramienta Autopsy se abrió un nuevo caso para documentar el caso Kericu_Inc, incluimos un detalle del caso además de los nombres de los investigadores.

Figura 10: Creación Nuevo Caso

A continuación, nos pide llenar los formularios con información del caso, como nombre de la máquina que estamos revisando, descripciones de área o rutas de bases de datos. Dichos datos no son obligatorios.

Figura 11 Autopsy: Creación Nuevo Caso

Se agrega la ruta donde se aloja la imagen, el tipo de imagen y la forma en que se mostrará la información que se encuentra en él.

Figura 12 Autopsy: Creación Nuevo Caso

Para garantizar y verificar que no se ha alterado la imagen original, se procede a calcular el valor del hash. Así verificamos que nadie ha cambiado nada en la unidad analizada. Esto debe realizarse cada vez que alguien vaya a trabajar sobre la evidencia, asimismo debe ser registrado en la Cadena de Custodia para control de acceso a la imagen.

Figura 13 Autopsy: Calculo de MD5

El proceso puede demorar varios minutos dependiendo de lo complejo de la imagen.

Figura 14 Autopsy: Calculo de MD5

Ya calculados los hashes nos mostrará la ventana de los casos creados y con esto se puede pasar a buscar los archivos clave según lo expuesto por el cliente.

Figura 15 Autopsy: Resumen de Imágenes

3.2 Análisis de las Unidades

3.2.1 Lewis-Laptop.dd

Al revisar la información del sistema de archivo se encuentra que el Disco Duro de Lewis se manejaba en Windows XP con sistemas de archivos NTFS

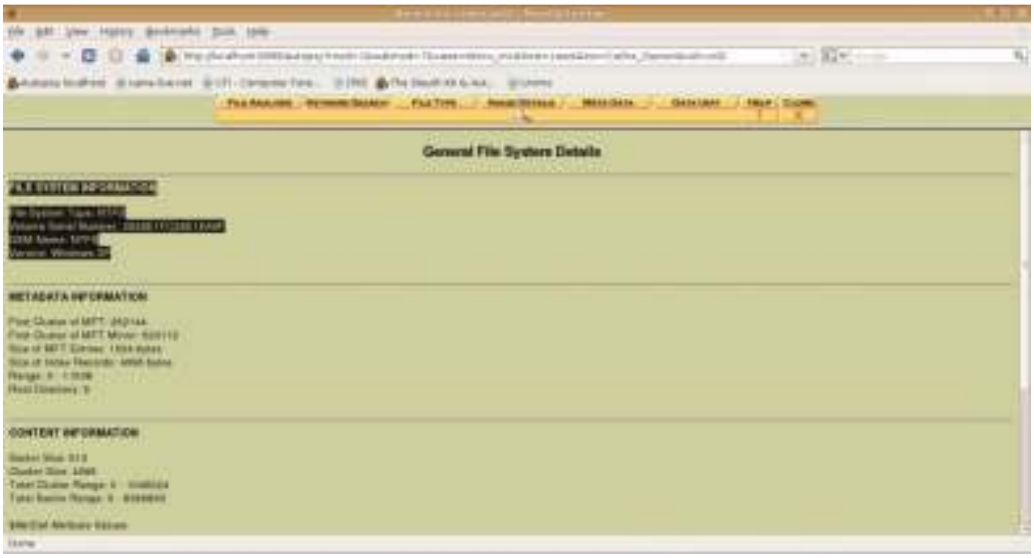


Figura 16 Autopsy: Información Sistema de Archivos

Al dar clic en FILE ANALYSIS se muestra el detalle de todas las carpetas y archivos que se encuentran en el sistema de archivos.

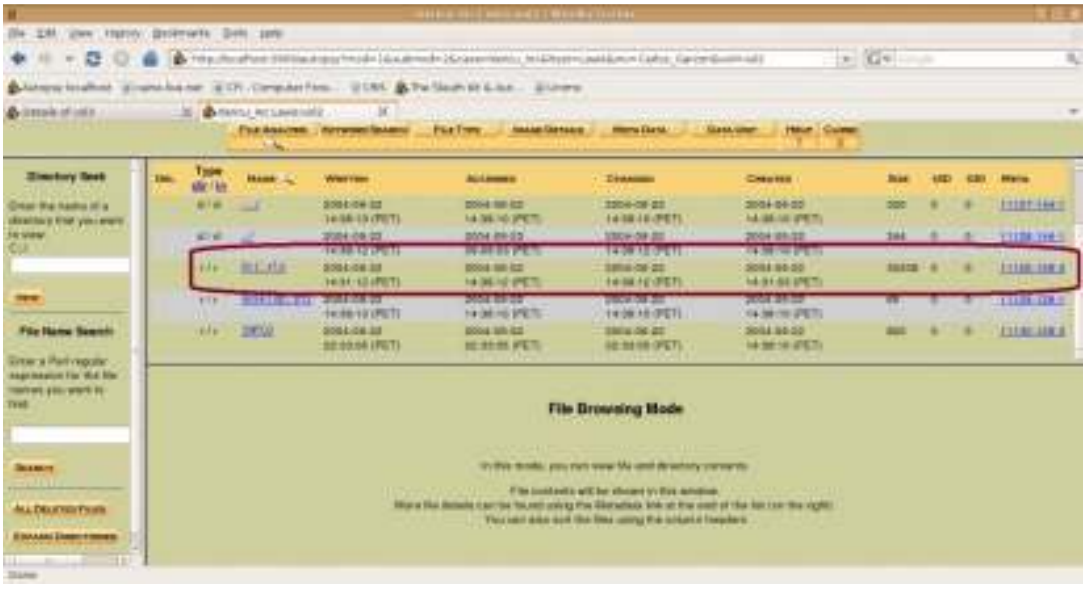


Figura 17 Autopsy: Análisis archivos Lewis-Laptop

Basándose en las palabras clave se encontró un archivo en la papelera de reciclaje un archivo borrado llamado earnings.xls y se procedió a recuperar para su análisis.

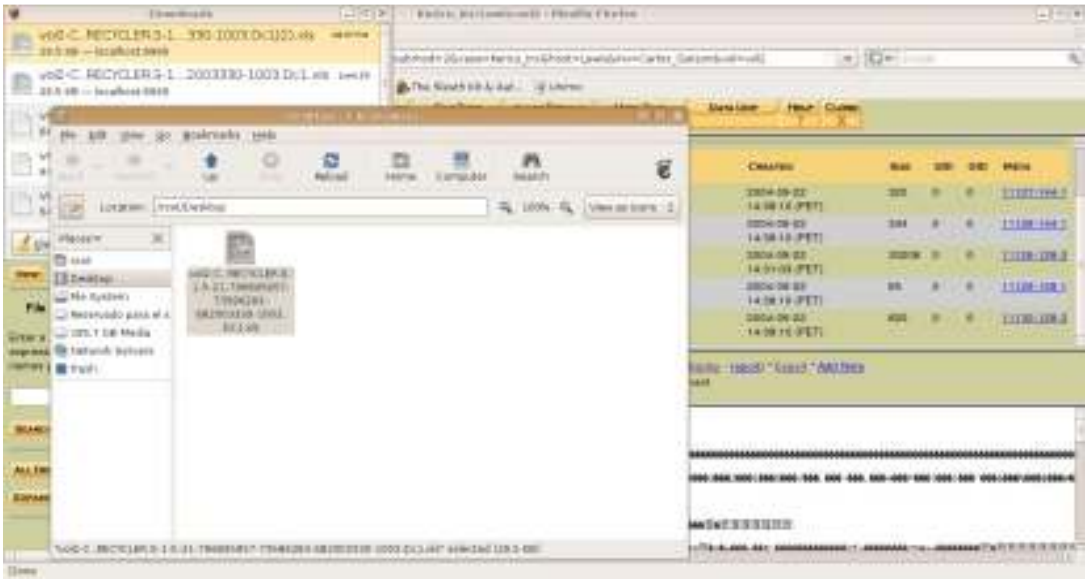


Figura 18 Recuperación de Archivo Borrado Lewis-Laptop

El archivo que encontramos nos mostró la siguiente información:

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		$311.033,92
Total	**$5.200.497,23**	**$5.620.373,78**	**$4.956.327,47**	**$15.777.198,48**

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	$4.732.686,97	$10.758.019,57

Figura 19 **Archivo Recuperado Lewis-Laptop**

3.2.2 Lewis-USB.dd

De la misma forma analizamos la unidad USB y se encontró dos archivos similares: earning-original.xls y el archivo earnings2.xls los cuales no se encontraban guardados, es decir estaban borrados, se procedió a recuperarlos para su respectivo análisis.

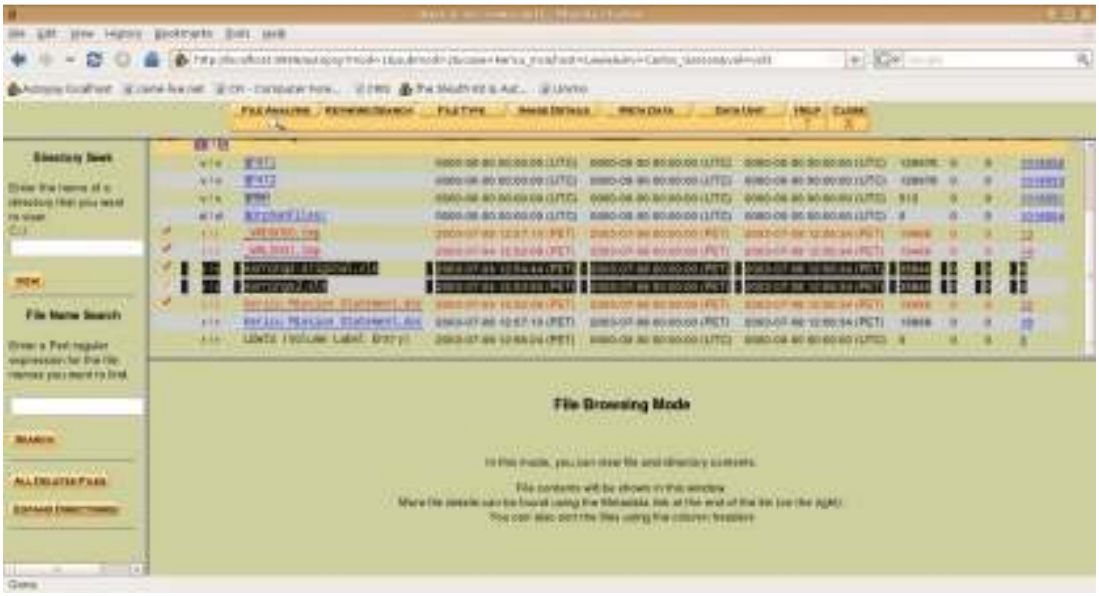
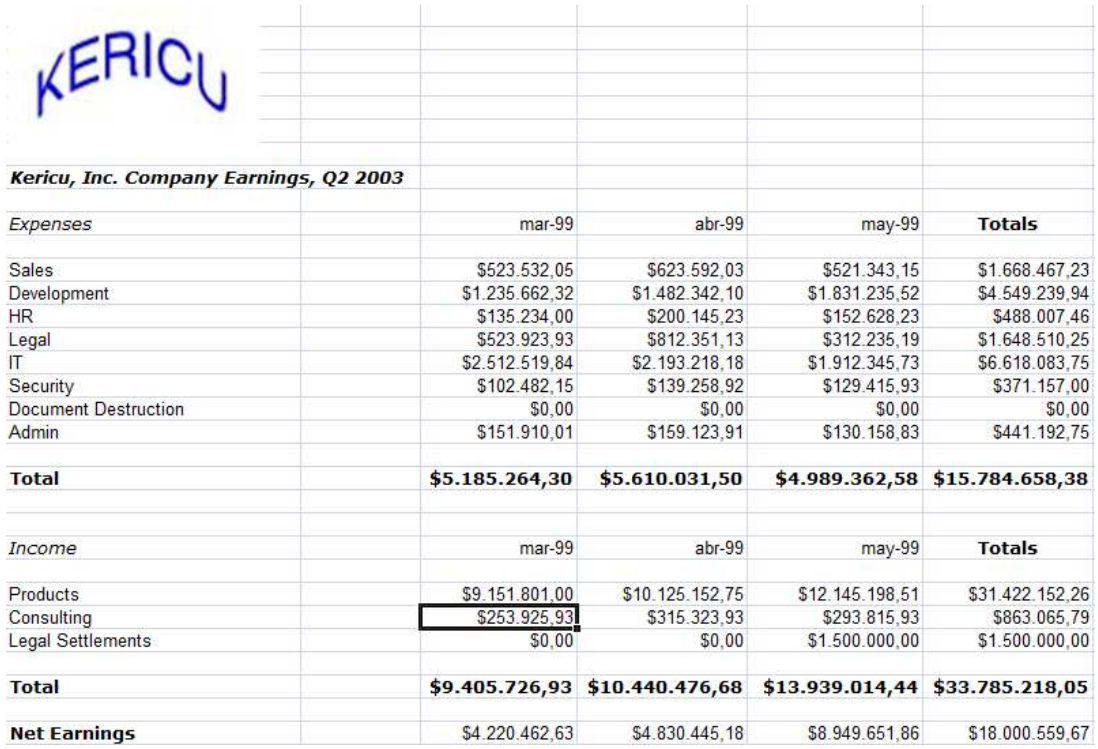


Figura 20 Análisis Archivos Lewis-USB

EARNINGS-ORIGINAL.XLS

El archivo earnings-original.xls contiene la siguiente información:



KERICU

Kericu, Inc. Company Earnings, Q2 2003				
Expenses	mar-99	abr-99	may-99	**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	$0,00	$0,00	$0,00	$0,00
Admin	$151.910,01	$159.123,91	$130.158,83	$441.192,75
Total	**$5.185.264,30**	**$5.610.031,50**	**$4.989.362,58**	**$15.784.658,38**
Income	mar-99	abr-99	may-99	**Totals**
Products	$9.151.801,00	$10.125.152,75	$12.145.198,51	$31.422.152,26
Consulting	$253.925,93	$315.323,93	$293.815,93	$863.065,79
Legal Settlements	$0,00	$0,00	$1.500.000,00	$1.500.000,00
Total	**$9.405.726,93**	**$10.440.476,68**	**$13.939.014,44**	**$33.785.218,05**
Net Earnings	$4.220.462,63	$4.830.445,18	$8.949.651,86	$18.000.559,67

Figura 21 **Archivo Recuperado USB**

También se realiza el respectivo reporte con Autopsy para validar la integridad del archivo.

Autopsy Dir Entry Report

GENERAL INFORMATION

Dir Entry: 8

Pointed to by file(s):

C:/earnings-original.xls (deleted)

MD5 of istat output: 701a5b6d90eb3cb7b0cbcb2de6513ce9 -

SHA-1 of istat output: 37a5bdffac4d7b02694c961fa0d2b569ffea4872 -

Image: '/usr/share/caine/report/autopsy/Kericu_Inc/Lewis/images/lewis-usb.dd'

Offset: Full image

File System Type: fat16

Date Generated: Sun Aug 19 17:37:48 2012

Investigator: Carlos_Garzon

META DATA INFORMATION

Directory Entry: 8

Not Allocated

File Attributes: File, Archive

Size: 35840

Name: _ARNIN~2.XLS

Directory Entry Times:

Written: Fri Jul 4 12:54:44 2003

Accessed: Tue Jul 8 00:00:00 2003

Created: Tue Jul 8 12:56:34 2003

Sectors:

599

Recovery:

599 600 601 602 603 604 605 606

607 608 609 610 611 612 613 614

615 616 617 618 619 620 621 622

623 624 625 626 627 628 629 630

631 632 633 634 635 636 637 638

639 640 641 642 643 644 645 646

647 648 649 650 651 652 653 654

655 656 657 658 659 660 661 662

663 664 665 666 667 668

File Type: Microsoft Office Document

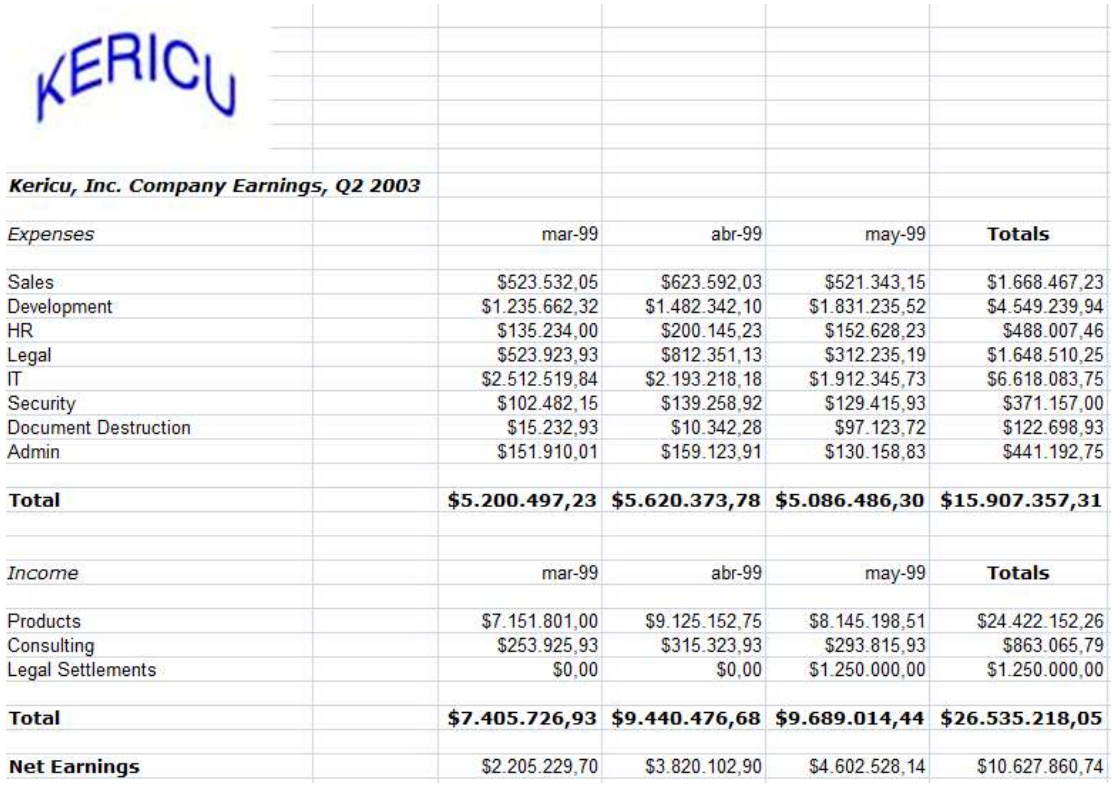
VERSION INFORMATION

Autopsy Version: 2.20

The Sleuth Kit Version: 3.0.0

EARNINGS2.XLS

El archivo earnings2.xls contiene la siguiente información:



Kericu, Inc. Company Earnings, Q2 2003				
Expenses	mar-99	abr-99	may-99	**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	mar-99	abr-99	may-99	**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 22 Archivo Recuperado USB

También se realiza el respectivo reporte con Autopsy para validar la integración del archivo:

Autopsy Dir Entry Report

GENERAL INFORMATION

Dir Entry: 5

Pointed to by file(s): C:/earnings2.xls (deleted)

MD5 of istat output: 4f096102b1003b6ffa419959545d648a -

SHA-1 of istat output: bfa7dda2bf55790b1332810b194d4a053cda06a3 -

Image: '/usr/share/caine/report/autopsy/Kericu_Inc/Lewis/images/lewis-usb.dd'

Offset: Full image

File System Type: fat16

Date Generated: Sun Aug 19 17:40:02 2012

Investigator: Carlos_Garzon

META DATA INFORMATION

Directory Entry: 5

Not Allocated

File Attributes: File, Archive

Size: 35840

Name: _ARNIN~1.XLS

Directory Entry Times:

Written: Fri Jul 4 12:53:50 2003

Accessed: Tue Jul 8 00:00:00 2003

Created: Tue Jul 8 12:56:34 2003

Sectors:

529

Recovery:

529 530 531 532 533 534 535 536

537 538 539 540 541 542 543 544

545 546 547 548 549 550 551 552

553 554 555 556 557 558 559 560

561 562 563 564 565 566 567 568

569 570 571 572 573 574 575 576

577 578 579 580 581 582 583 584

585 586 587 588 589 590 591 592

593 594 595 596 597 598

File Type: Microsoft Office Document

VERSION INFORMATION

Autopsy Version: 2.20

The Sleuth Kit Version: 3.0.0

3.3 Línea de Tiempo

Con la ayuda de Autopsy se crea la línea de tiempo para las unidades revisadas.

Escogemos la opción de crear línea de datos para empezar a definir nuestra línea de tiempo.

Figura 23 Autopsy: Creación Línea de Tiempo

Luego nos mostrará varios formularios donde debemos escoger la unidad sobre la cual se creará la línea de tiempo, los archivos recopilados y el nombre del archivo generado.

Figura 24 Autopsy: Creación Línea de Tiempo

Luego se ejecutará un comando para crear la línea de tiempo, este es invisible para el usuario. Agrega la entrada, valida el MD5 y crea la línea de tiempo.

Figura 25 Autopsy: Validación MD5

Para mostrar la línea de tiempo nos pedirá escribir los parámetros en los cuales se basará la misma.

Figura 26 Autopsy Creación de Línea de Tiempo

Luego nos mostrará los cambios en el sistema de archivos así como la fecha en la que se realizaron. A continuación, las líneas de tiempo del disco de la laptop así como de la unidad USB:

3.3.1 Lewis Laptop

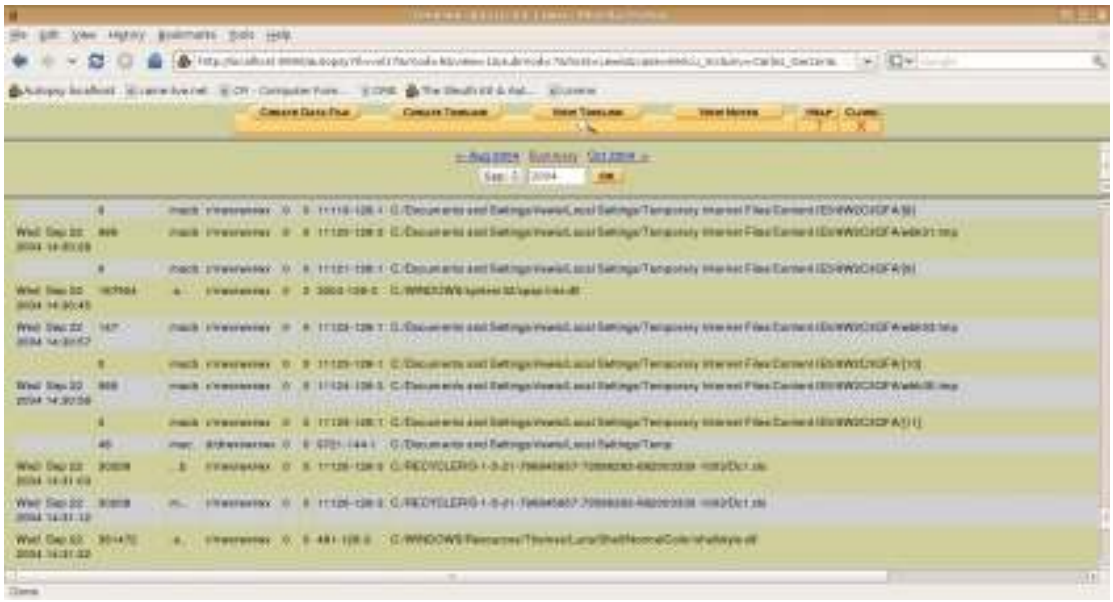


Figura 27 Autopsy Línea de Tiempo Lewis Laptop

Aquí podemos ver cuando el archivo Dc1.xls pasa a ser borrado y almacenarse en la papelera. Este archivo contiene información financiera.

3.3.1 Lewis-USB

Figura 28 Autopsy: Línea de Tiempo Lewis-USB

Aquí podemos observar los accesos a los archivos.

3.4 Virtualización de Disco Lewis-Laptop.dd

Accediendo mediante ambiente gráfico con la herramienta VMware Workstation podemos verificar una vez más que se trata de un ambiente de Windows XP PROFESSIONAL.

El usuario es *rlewis* y la contraseña de acceso es *sk1llz* deducible por las características mencionadas en la información proporcionada para la investigación. .

Figura 29 VMWare: Lewis-Laptop

También se da a notar que en la papelera de reciclaje se encuentra un archivo borrado llamado earnings.

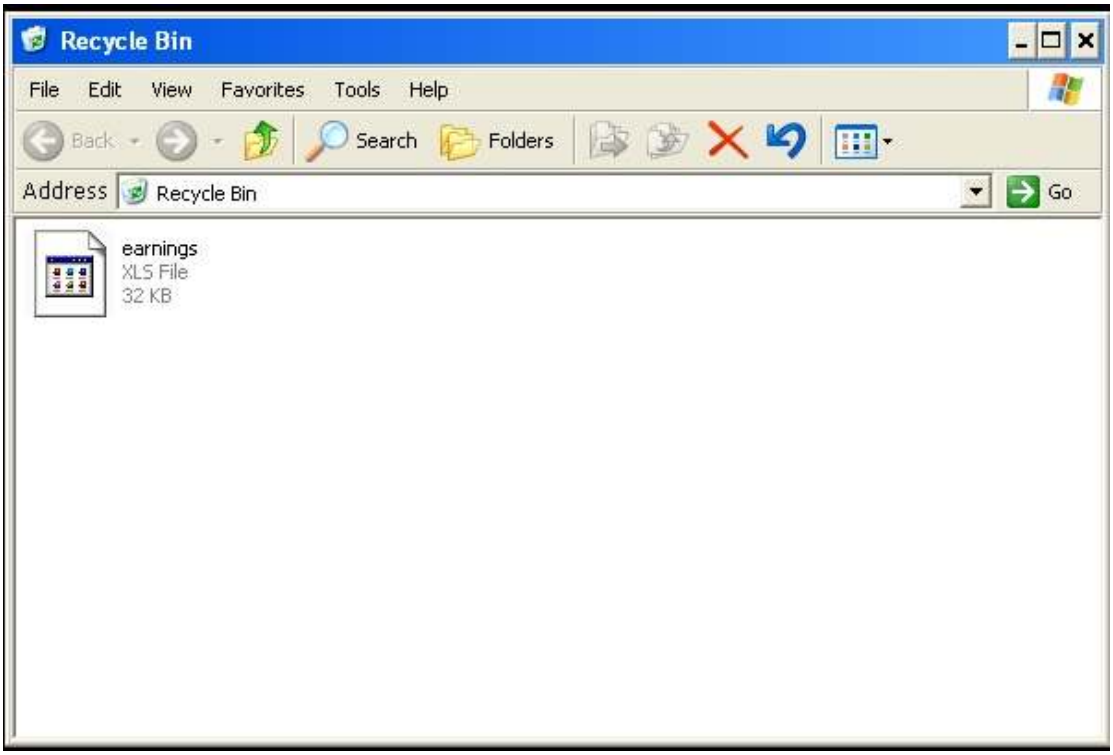


Figura 30 VMWare: Papelera de Reciclaje Lewis Laptop

Podríamos recuperar dicho archivo pero al hacerlo alteraríamos la evidencia. Solo ingresamos para confirmar que dicho archivo ha sido borrado.

3.5 Análisis de los encabezados de los correos de rlewis@kericu.com alojados en la laptop.

Joe Harvey envía un correo Rodger Lewis con Asunto: All Company Meeting el 22 de Septiembre del 2004 a las 3:18:00

From: "Joe Harvey" <jharvey@kericu.com>

To: <rlewis@kericu.com>

Sent: Wednesday, September 22, 2004 3:18 PM

Subject: All Company Meeting

Rodger Lewis responde correo a Joe Harvey el 22 de Septiembre del 2004 a las 15:20:26, se muestra encabezado:

"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 Harvey responde al Correo de Rodger Lewis con un archivo Adjunto nombrado: earnings.xls el 22 de Septiembre a las 15:20:00

--Apple-Mail-4--537455129

Content-Transfer-Encoding: base64

Content-Type: application/octet-stream;

x-unix-mode=0755;

name="earnings.xls"

Content-Disposition: attachment;

filename=earnings.xls

To: "Rodger Lewis" <rlewis@kericu.com>

X-Mailer: Apple Mail (2.619)

X-Spam-Checker-Version: SpamAssassin 2.63 (2004-01-11) on www.aidenjones.com

X-Spam-Status: No, hits=1.1 required=5.0 tests=NO_DNS_FOR_FROM autolearn=no

version=2.63

X-Spam-Level: *

--Apple-Mail-4--537455129

Content-Transfer-Encoding: 7bit

Content-Type: text/plain;

charset=US-ASCII;

format=flowed

3.6 CRONOLOGÍA

3 Julio del 2003 15:33:02: Aiden Paluchi envía correo a los ejecutivos adjuntando archivo earnings.xls y con asunto Q2 Earnings Spreadsheet.

4 de Julio del 2003 12:53:50: Escritura en archivo earnings2.xls en dispositivo USB.

4 de Julio del 2003 12:54:44: Escritura en archivo earnings-original.xls en dispositivo USB.

8 de Julio del 2003 00:00:00: Acceso al archivo earnings2.xls en dispositivo USB.

8 de Julio del 2003 00:00:00: Acceso al archivo earnings-original.xls en dispositivo USB.

8 de Julio del 2003 12:56:34: Se elimina el archivo earnings2.xls en dispositivo USB.

8 de Julio del 2003 12:56:34: Se elimina el archivo earnings-original.xls en dispositivo USB.

22 de Septiembre del 2004 15:18:00: Joe Harvey Envía correo a Rodger Lewis Con Asunto: All Company Meting.

22 de Septiembre del 2004 15:20:00: Rodger Lewis envía un correo con Asunto RE: All Company Meeting

22 de Septiembre del 2004 15:29:00: Joe Harvey Envía correo a Rodger Lewis Con Asunto: RE: All Company Meting con archivo adjunto earnings.xls

CONCLUSIONES

1. En la imagen lewis-laptop.dd se verifica que es una partición con Sistema de Archivo NTFS y de Sistema Operativo WINDOWS XP PROFESSIONAL SP2.

Al momento de inicio de sesión nos muestra predeterminadamente el usuario rlewis listo para introducir la contraseña, la cual basándonos en las pistas recolectadas en la información personal de Rodger Lewis probamos con la contraseña **sk1llz** lo cual fue exitoso.

Una vez adentro se verifica que en la papelera de reciclaje se encuentra un archivo llamadoearnings.xls.

Se verifica en los programas instalados predeterminadamente como el OUTLOOK EXPRESS 6, en el cual pudimos encontrar varios correos entre Joe Harvey y Rodger Lewis. En el último correo de Joe a Rodger se encuentra un Adjunto llamado earnings.xls.

El adjunto enviado en el correo que nos proporcionaron se encuentra en la papelera de la máquina de Lewis.

El archivo original se creó en la máquina de Rodger Lewis

2. El archivo ernings2.xls y el archivo earning-original.xls son archivos tipo Microsoft EXCEL, es decir, son Hojas de Cálculo que se encontraron en el dispositivo de almacenamiento USB que nos proporcionaron.

Los dos archivos en mención se encontraron en el dispositivo USB que pertenece a Rodger Lewis pero no se encontraban almacenados, es decir se encontraban borrados de la partición y se los recuperó con la herramienta AUTOPSY.

Se hace un informe individual de los dos archivos lo cual muestra que se encuentran eliminados, también muestra las fechas de modificación, MD5 y

SHA-1 de cada archivo que valida el contenido de los mismos y los cambios encontrados.

Dentro de cada Hoja de Cálculo se encuentran cambios en la declaración de gastos de destrucción de documentos y en la declaración de ingresos de productos.

3. Basados en los resultados de los hashes, podemos notar que el archivo earnings que contiene la información financiera de la empresa ha sido modificado y se han generado otras copias de las cuales una ha sido presentada como archivo de origen.

RECOMENDACIONES

Para evitar que ocurran este tipo de incidentes es recomendable considerar:

1.VALIDAR INFORMACION DIGITAL CON INFORMACION FISICA

Para poder mantener la integridad de la información y tener soporte de los mismos en este caso se recomienda un sistema contable con una base de

datos, para que todo movimiento contable sea registrado y tener un soporte con lo físico (Facturas) y lo digital (Base de datos).

También se recomienda que esta información sea validada diariamente e informando vía correo a los ejecutivos.

Además se recomendaría que los ejecutivos tengan acceso a esa información remotamente por medio de una VPN a la red interna y asignarle los permisos dependiendo de la información que debe consultar y así el ejecutivo tendría ya un respaldo digital diario sobre la información.

Se recomienda hacer un respaldo diario sobre la base de datos por parte del personal de sistemas para que no haya pérdida y mala manipulación de los datos

2.SISTEMA DE GESTION DE DOCUMENTOS

Se recomienda implementar un sistema DMS, utilizado para rastrear y almacenar documentos electrónicos e imágenes de documentos en papel. Suele proporcionar el almacenamiento, la seguridad y las capacidades de recuperación e indexación del contenido.

Con este sistema tendrían un repositorio de documentos importantes y valiosos para la empresa con fácil búsqueda

3.PREVENCIÓN DE PERDIDA DE INFORMACIÓN

Se recomienda un sistema DLP que está diseñado para proteger los activos informáticos de la empresa, con la mínima interferencia a los procesos de negocios.

Empresas de servicios financieros típicamente lo usan sobre su red y sistemas de almacenamiento para asegurarse de que ni empleados ni terceros hagan uso inapropiado o compartan los activos informáticos en formas que violen las políticas de la empresa.

DLP les permite asegurarse de que solo el equipo de cómputo contenga la información que necesita dependiendo de su área y no haya manipulación de otra información que no corresponde a su área.

GLOSARIO

Archivo XML: Permite definir la gramática de lenguajes específicos para estructurar documentos grandes en la estructura de página WEB.

Active Directory: Es el término que usa Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores

Ataques de puerta trasera: Explotar la vulnerabilidad en un sistema que fue elaborado por el desarrollador intencional o no intencional.

BIOS: Es un tipo de firmware que localiza y prepara los componentes electrónicos o periféricos de una máquina

Cadena de custodia: Es la aplicación de una serie de normas tendientes a asegurar, embalar y proteger cada elemento material probatorio para evitar su destrucción, suplantación y contaminación lo que podría implicar tropiezos en la investigación.

CEO: Director Ejecutivo.

Clúster: Es un conjunto contiguo de sectores que componen la unidad más pequeña de almacenamiento de un disco.

Cyber-atacantes: Personas que realizan explotan vulnerabilidades en la redes causando daño en las mismas.

Extensión .dd: Es la Compresión de un Disco Duro.

Gusano: Es un programa que tiene la propiedad de duplicarse a sí mismo.

Hash: Se refiere a una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc.

Kernel: Es el principal responsable de facilitar a los distintos programas acceso seguro al hardware de la computadora o en forma básica, es el encargado de gestionar recursos, a través de servicios de llamada al sistema.

Live Cd: Es un sistema operativo almacenado en un medio extraíble, tradicionalmente un CD o un DVD (de ahí sus nombres), que puede ejecutarse desde éste sin necesidad de instalarlo en el disco duro de una computadora, para lo cual usa la memoria RAM como disco duro virtual y el propio medio como sistema de archivos.

Routers: Es un dispositivo que proporciona conectividad a nivel de red.

Script Kiddies: Es un término despectivo utilizado para describir a aquellos que utilizan programas y scripts desarrollados por otros para atacar sistemas de computadoras y redes.

Servidores: Es una computadora que, formando parte de una red, provee servicios a otras computadoras denominadas clientes.

Sniffer: Es un programa informático que registra la información que envían los periféricos, así como la actividad realizada en un determinado ordenador.

Software de código abierto/libre distribución: Es el software que está licenciado de tal manera que los usuarios pueden estudiar, modificar y mejorar su diseño mediante la disponibilidad de su código fuente.

Troyanos: Software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo pero al ejecutarlo ocasiona daños.

Ubuntu: Es un sistema operativo mantenido por Canonical y la comunidad de desarrolladores. Utiliza un núcleo Linux.

Virus: Es un programa que tiene por objeto alterar el normal funcionamiento de la computadora

Volatilidad: Retención de datos informáticos durante algún intervalo de tiempo.

Vulneración: Explotar una debilidad.

BIBLIOGRAFÍA

[1] Kleiman Dave, The Official CHFI Exam 312-49, Syngress, 2007.

[2] Altheide Cory y Carvey Harlan, Digital Forensics with Open Source Tools, Syngress, 2011.

[3] Nanni Bassetti, CAINE (Computer Aided INvestigative Environment), http://www.caine-live.net/.

[4] Carrier Brian, Autopsy Forensic Browser, http://www.todoprogramas.com/macintosh/autopsyforensicbrowser/

[5] Wikipedia, Vmware Player, http://es.wikipedia.org/wiki/VMware#VMware_Player/

ANEXOS

Entorno de trabajo

Para realizar el análisis utilizamos el siguiente entorno de trabajo:

1 Laptop HP Elite Book 8440p

Características:

HDD: 250 GB

MEMORIA RAM: 6 GB

PROCESADOR: I5 2.40 GHZ

Sistemas Operativos:

Windows 7 Home Premium 64 BITS

Caine 2.0

Archivo Recibido para el caso

KERICU'S SEC VIOLATION

As a forensic examiner for a law enforcement entity's computer crime forensic lab, you see a lot of cases come and go. You've spent time reporting violations, where high-level executives alter financial documents to make their company look better in the eyes of their stockholders. One such company, Kericu, Inc., is a well-known telecommunications hardware developer. Its executives seem to have caught the "alteration bug". Kericu's CEO, Rodger Lewis, is well known for his computer skills, and he may have put those skills to evil use. The Department of Justice recently indicted Lewis for altering quarterly statements to boost his company's earnings. Because Lewis is renowned for having computer "sk1llz"

("skills" as known by the computer underground), you expect he has cleaned his tracks. Very little computer evidence may be available. In your experience, most medium to advanced users are aware of evidence elimination software, which makes your job difficult.

Fortunately, the executive vice president of finance, Aiden Paluchi, negotiated a deal with the Department of Justice. If Paluchi testifies against the CEO, he will receive immunity from any additional charges related to this case. Paluchi supplied the DOJ with the document he says Lewis altered. Paluchi also says this document was sent to the whole executive staff through e-mail. He supplies you with a copy of this e-mail, listed here:

To: executives@kericu.com

From: aiden.paluchi@kericu.com

Date: Thursday July 3, 2003 15:33:02 (EDT)

Subject: Q2 Earnings Spreadsheet

Attachments: earnings.xls

Gentlemen,

This document is ready for your approval. Please e-mail back any changes that I may have missed. Hopefully next quarter will be better than this one.

Sincerely,

Aiden Paluchi

Executive VP of Finance

Kericu, Inc.

You travel to Kericu headquarters and begin your analysis. You begin by acquiring a forensic duplication of Lewi's laptop hard drive using dd. You quickly review the image for a "smoking gun". As you expected, you did not see earnings.xls anywhere on Lewis's hard drive. Your job just became much harder than you thought because you will have to do a deeper analysis. Just then, and agent runs into your office and slaps down a USB memory device that was found in Lewis's home. Hopefully, after you acquire a forensic duplication of the device, you may find additional evidence of Lewis's crime.