Análisis Forense de Fraude Financiero Kericu Inc.

Carlos Garzón Chacón[(1)], Solange Rodríguez Tigrero[(2)]
Facultad de Ingeniería en Electricidad y Computación
Escuela Superior Politécnica del Litoral (ESPOL)
Campus Gustavo Galindo, Km 30.5 vía Perimetral
Apartado 09-01-5863. Guayaquil-Ecuador
cmgarzon90@gmail.com[(1)], sirt90@gmail.com[(2)]
Febrero 2012 – Febrero 2013
Guayaquil-Ecuador

Director de Tesis MBA. Karina Astudillo, mail karina.astudillo@elixircorp.biz

Resumen

La presente tesis consiste en el Análisis Forense de un posible fraude financiero para la empresa Kericu Inc., con la finalidad de ratificar las sospechas de posibles cambios en los documentos financieros de la empresa por el señor Rodger Lewis.
Contemplamos Aspectos Teóricos y Legales importantes antes de realizar el debido análisis, además de las características del analista así como el espacio en el cual debe desarrollar su análisis. También conoceremos un poco sobre las herramientas utilizadas para el análisis, entre las cuales consideramos Caine Linux, Autopsy Forensic Browser y VMWare Workstation, herramientas que fueron de gran ayuda en el desarrollo de nuestra investigación sobre la evidencia recibida. Contemplamos, con la ayuda de las herramientas el proceso a seguir y la aplicación de comandos para llegar a nuestro objetivo, además de considerar muchos detalles para recordar al momento de asegurar la información de empresas de la manipulación y extracción ilícita de las mismas.

Palabras Claves: *Análisis Forense, Caine Linux, Autopsy Forensic Browser, VMWare Workstation, Kericu Inc.*

Abstract

This research is about the Forensic Analysis of an alleged financial fraud for Kericu Inc. in order to confirm the suspicions of possible changes on the company's financial documents by Mr. Rodger Lewis.
We cover important theoretical and legal aspects before making the analysis, in addition to the characteristics of the analyst and the workspace in which to develop their analysis. Also we learn about some tools used during the analysis, including Caine Linux, Autopsy Forensic Browser and VMWare Workstation, that were helpful in the development of our research on the evidence we received. We see, with the help of the tools, the process to follow and the application of commands to reach our objective, besides considering many details to remember when we try to protect company information from being manipulated or illegally extracted.

Keywords*: Forensics, Caine Linux, Autopsy Forensic Browser, VMWare Workstation, Kericu Inc.*

1. Introducción

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.

2. Aspectos Teóricos

2.1 Computación 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.

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.

2.2 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 3Ts: 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).

2.3 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.

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.

2.4 Procedimiento

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

Identificar el crimen.- Saber qué es lo que está ocurriendo, cuál fue el daño, qué es lo que se quiso afectar.
Reunir la evidencia.- Solicitar y buscar toda la información posible que 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 clara posible para que el juez o jurado tomen la debida decisión en el caso.

3. Herramientas

3.1 CAINE 2.0

Es una distribución de Linux basada en Ubuntu, 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.

3.2AUTOPSY FORENSIC BROWSER

Es una herramienta que viene incluida en el sistema operativo Caine Linux, y sirve como interfaz gráfica para las herramientas de análisis digital de investigación de The Sleuth Kit. Juntos, pueden analizar discos de Windows y UNIX y sistemas de archivos (NTFS, FAT,UFS1/2,Ext2/3).

The Sleuth Kit y Autopsy son de código abierto y funcionan con plataformas UNIX/LINUX. Debido a que la herramienta Autopsy está basada en HTML, es posible conectarse al servidor de Autopsy desde cualquier plataforma usando un navegador HTML.

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

3.3VMWARE WORKSTATION

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.

4. Desarrollo

4.1 Obtención de la evidencia

4.1.1 LEWIS-LAPTOP.DD

Md5: 021c551ea7e36f9806ca4be04c87b6b3
Sha1: 94f678994709b94eb446c356fafeea4e99b6d9e8

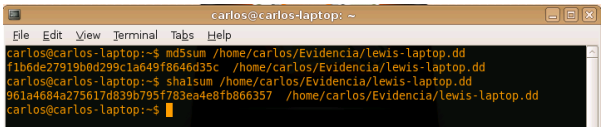

Figura 2: Evidencia Lewis Laptop

4.1.2 LEWIS-USB.DD

Md5:f1b6de27919b0d299c1a649f8646d35c
Sha1: 961a4684a275617d839b795f783ea4e8fb866357

4.2 Análisis de las Unidades

4.2.1 Lewis-Laptop.dd

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

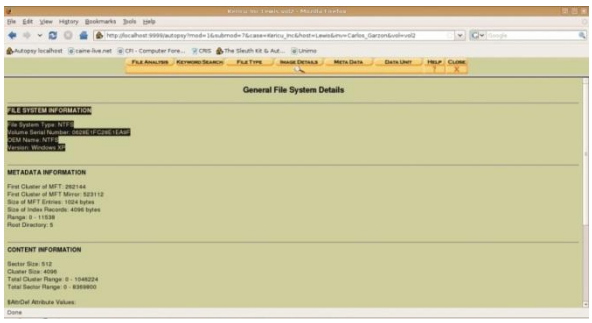

Figura 3: Autopsy: Información Sistema de Archivos

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

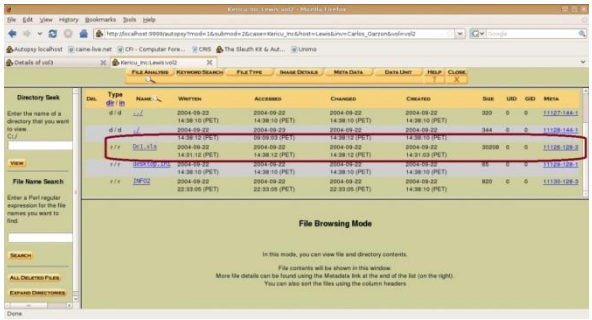

Figura 4: Autopsy: Análisis archivos Lewis-Laptop

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.

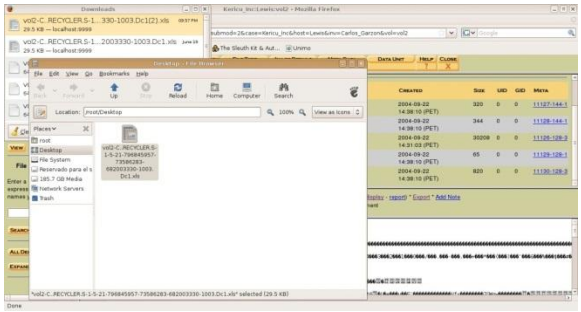

Figura 5: Recuperación de Archivo Borrado Lewis-Laptop

El archivo que encontramos nos mostró la siguiente información:

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		$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 6: Archivo Recuperado Lewis-Laptop

4.2.2Lewis-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.

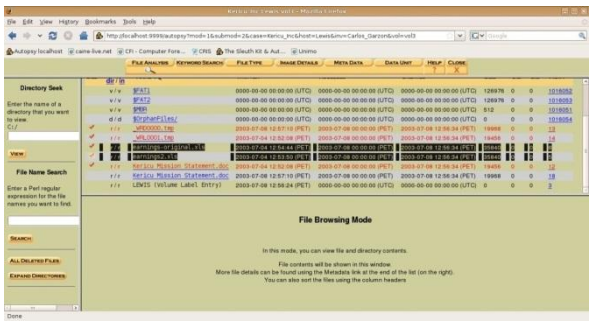

Figura 7: Análisis Archivos Lewis-USB

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 8: Archivo Recuperado USB

EARNINGS2.XLS

El archivo earnings2.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	$136.234,00	$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	$4.602.628,14	$10.627.860,74

Figura 9: Archivo Recuperado USB

4.3Línea de tiempo

4.3.1 Lewis Laptop

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

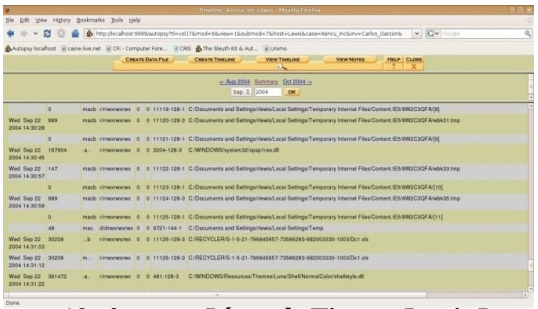

Figura 10: Autopsy Línea de Tiempo Lewis Laptop

4.3.2 Lewis-USB

Aquí podemos observar los accesos a los archivos.

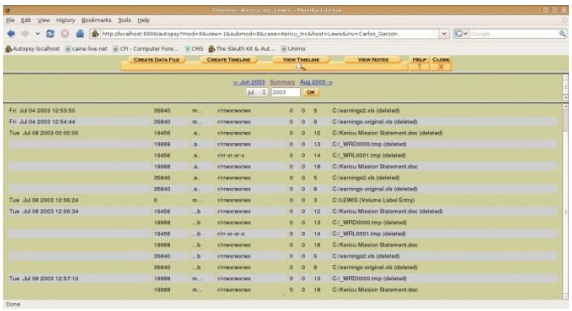

Figura 11: Autopsy: Línea de Tiempo Lewis-USB

4.4 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

5. Conclusiones

5.1 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 llamado earnings.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

5.2 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.

5.**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.

6. Recomendaciones

6.1 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).

6.2 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.

6.3 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.

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.

7. Referencias

[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/