ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

CENTRO DE INVESTIGACIÓN CIENTÍFICA Y TECNOLÓGICA

AUDITORÍA FORENSE DEL CASO KERICU

Diana Andrade Rojas [(1)]; Freddy Gonzales Apunte [(2)]
Facultad de Ingeniería en Electricidad y Computación
Escuela Superior Politécnica del Litoral
Campus Gustavo Galindo Velasco, Km. 30.5 vía Perimetral
Apartado 09-01-5863. Guayaquil - Ecuador
dincar89@hotmail.com [(1)]; fgonzal87@hotmail.com [(2)]
Febrero del 2012 – Febrero del 2013
Guayaquil – Ecuador

Directora de Tesis Ing. Karina Astudillo, mail karina.astudillo@elixircorp.biz

Resumen

La presente tesis consiste en realizar una Auditoría Forense del Caso Kericu, la cual 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 habilidades a nivel computacional en forma clandestina. Se adquiere una copia del disco duro de la portátil de Lewis y del dispositivo usb encontrado en la casa de él. Se realiza un análisis rápido de las evidencias y como era de esperar todo ha sido borrado ya que no se encuentra el archivo "earnings.xls". Con esto se pone complicado el caso ya que se tiene que realizar un análisis profundo de la evidencia.

Palabras claves: *Estados financieros, CEO, USB, Disco Duro, Earnings.*

Abstract

This work consists in the execution of a Forensic Audit for the company Kericu, which is a developer of telecommunications hardware that saw affected its financial statements. Rodger Lewis, CEO of Kericu, is known for his computer skills and he has previously put those skills to misuse. The Justice Department recently accused Lewis of altering the company's quarterly profits statements. Lewis is known in the underground his computational skills. A hard copy of Lewis' laptop hardrive and from usb device found in his house was acquired. During a quick analysis of the evidence it is evident that everything has been deleted, because the file "earnings.xls" is missing. With this in mind the case becomes complex because we will have to make a thorough analysis of the evidence.

Keywords: *Financial Statements, CEO, USB, HDD, Earnings.*

1. Introducción

En este proyecto se tendrá como objetivo la investigación del caso asignado en la materia de graduación, "CASO KERICU", en el cual tendremos 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.

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

Para el análisis usaremos el sistema operativo Caine Linux, el cual posee herramientas forenses que nos permitirán desde crear una copia de la evidencia sin alterarla, hasta recuperar archivos eliminados por el usuario.

2. Metodología

Para poder realizar cualquier trabajo de informática forense, el auditor encargado del caso debe determinar los hallazgos, y emitir conclusiones en base a las evidencias, 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 de 3 A's. El siguiente esquema es el más adecuado para un desarrollo eficiente sobre el tema a tratar.

Figura 1 - Metodología de la Informática Forense

2.1 Adquirir 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 serían válidos debido a que la información saldría alterada.

2.2 Autenticar 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 permitan verificar la integridad de evidencias.

2.3 Análisis e investigación

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.

3. Desarrollo del Proyecto

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 máquina local.

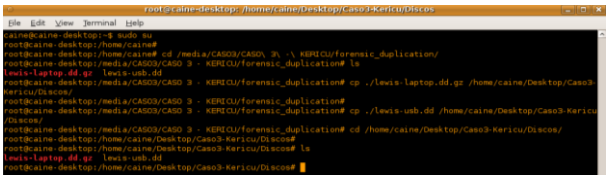
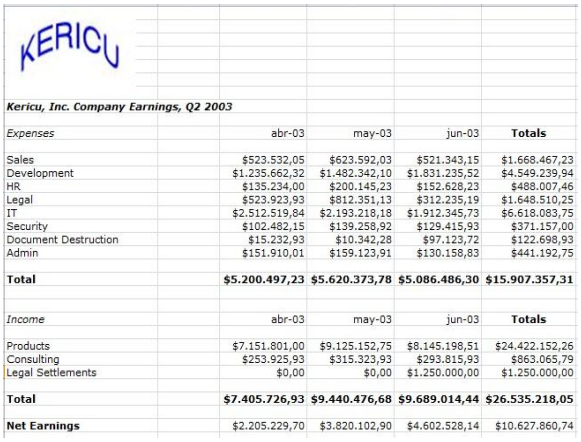


Figura 2 - Copiando la evidencia

3.1 Análisis de la imagen Lewis-laptop

Mediante el sistema operativo Caine montamos la imagen lewis-laptop para luego analizarla con la herramienta Autopsy. Ingresamos al directorio RECYCLER/ (papelera de reciclaje), en el cual encontramos el archivo Dc1.xls. Este archivo se nos visualiza en una hoja de cálculo como un estado financiero mostrándonos las ganancias de la empresa.

Adicionalmente podemos obtener la información del o de los usuarios que tuvieron acceso a ese archivo y lo manipularon, todo esto a través de la información general del mismo.



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 2 – Archivo Dc1.xls encontrado en Recycler

Continuamos con el análisis 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 C:/Documents and Settings/rlewis.

Con la herramienta Web Historian analizamos los datos desde cualquier navegador web y se nos presenta en una hoja de cálculo como nos muestra la siguiente figura.

URL Address
Visited: rlewis@http://www.google.com/search?hl=en&ie=UTF-8&q=eliminate+evidence+pc
Visited: rlewis@http://www.sysinternals.com/ntw2k/utilities.shtml
Visited: rlewis@http://us.rd.yahoo.com/reg/login/new_ym/us/*http://billing.mail.yahoo.com/bm/MailReg?signup=Sign+Up+Now
Visited: rlewis@http://us.f613.mail.yahoo.com/ym/ShowLetter?Idx=0&Search=&YY=15002&order=down&sort=date&pos=0
Visited: rlewis@http://us.f613.mail.yahoo.com/ym/ShowLetter?Msgid=7007_3633_284_974_447_0_5_-
Visited: rlewis@http://edit.yahoo.com/config/last_subscribe
Visited: rlewis@http://us.f613.mail.yahoo.com/ym/login
Visited: rlewis@http://www.evidence-eliminator.com/product.d2w
Visited: rlewis@http://billing.mail.yahoo.com/bm/MailReg?signup=Sign+Up+Now
Visited: rlewis@http://cgi.ebay.com/ws/eBayISAPI.dll?ViewItem&category=29520&item=4325403610&rd=1
Visited: rlewis@http://www.cnn.com/2004/US/09/21/lottery.winner.burglar.ap/index.html
Visited: rlewis@http://www.google.com/search?q=eliminate+digital+evidence&hl=en&lr=&ie=UTF-8&start=10&sa=N
Visited:
Visited: rlewis@http://www.sysinternals.com/ntw2k/source/sdelete.shtml
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
Visited: rlewis@http://www.securityfocus.com
Visited: rlewis@http://us.f613.mail.yahoo.com/ym/ShowLetter?Msgid=3198_1616_22_523_447_0_3_-
Visited:
Visited: rlewis@http://www.msn.com
Visited: rlewis@http://www.ebay.com
Visited:
Visited: rlewis@http://cgi.ebay.com/ws/eBayISAPI.dll?ViewItem&category=79670&item=4325234088&rd=1
Visited: rlewis@http://us.f613.mail.yahoo.com/ym/ShowLetter?Msgid=6868_6552_902_1007_894_0_9_-
Visited: rlewis@http://view.atdmt.com/FKQ/iview/brstmdrc00100061fkq/direct/0355557click=http://www.burstnet.com/ads/ad10937a-
Visited: rlewis@http://us.f613.mail.yahoo.com/ym/ShowLetter?Msgid=3003_1110_22_449_55_0_1_-
Visited: rlewis@http://misc.weather.com/common/outlets/vi.html?lswe=20006
Visited:
Visited: rlewis@http://mail.yahoo.com
Visited: rlewis@http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome
Visited: rlewis@http://us.f613.mail.yahoo.com/ym/Compose?YY=13492
Visited:
Visited: rlewis@http://edit.yahoo.com/config/eval_register?.v=&.intl=&new=1&.done=&.src=ym&.partner=&.p=&promo=&.last=
Visited: rlewis@about:blank
Visited: rlewis@http://www.amazon.com/exec/obidos/search-handle-url/index=dvd&field-actor=Edward%20Norton/102-6878763-3564954

Figura 3 - Resultados de la búsqueda con Web Historian

La utilidad Eindeutig nos va ayudar en el análisis de los correos electrónicos ya que nos permite recuperarlos aunque el usuario los haya eliminado. Con esta herramienta vamos a visualizar todas las carpetas creadas en el correo respectivo.

Para recuperar los archivos adjuntos utilizamos la herramienta Munpack, la cual reconstruirá todos los archivos adjuntos encontrados en los emails que nos interesen. Encontramos un archivo de Excel con el nombre "earnings.xls" el cual nos refleja un estado financiero. 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.

3.2 Análisis de la 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.

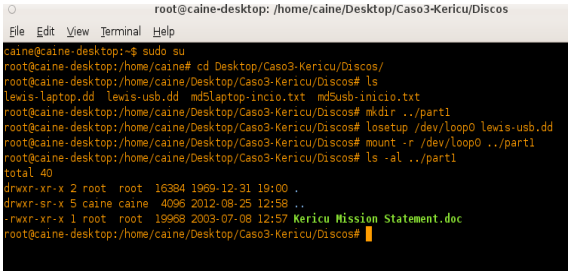
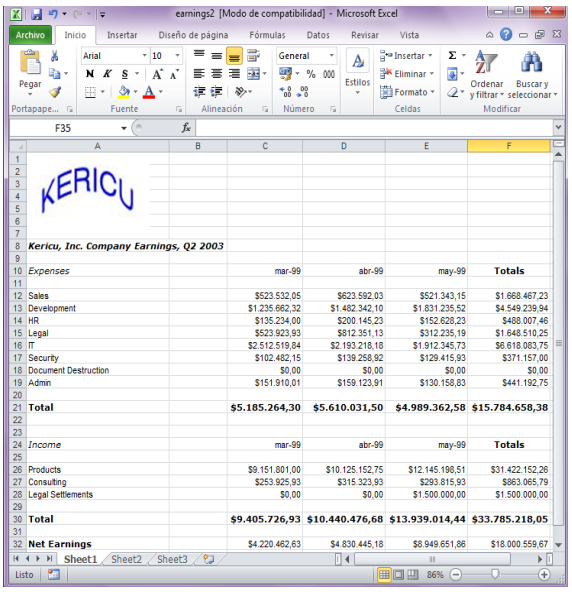


Figura 4 - Montar imagen del dispositivo usb

Creamos el directorio part1 para montar el dispositivo loopback el cual va hacer la imagen del dispositivo USB y acceder a sus respectivos archivos en el mismo. Luego de verificar los archivos lógicos del sistema, podemos ver únicamente un archivo de la evidencia.

Tenemos que buscar si hay archivos borrados u ocultos y esto lo vamos hacer utilizando el comando fls en la evidencia.



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 5 - Hoja de cálculo "earnings2" encontrada

Entre los archivos borrados encontramos "earnings2" y "earnings-original", los cuales son archivos de estados financieros. Los archivos Dc1.xls (papelera de reciclaje), earnings.xls (correo electrónico) y earnings-original.xls (dispositivo usb) son iguales.

4. Conclusiones

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 auditoría forense del caso, analizando las imágenes proporcionadas de los dispositivos que tenía Lewis como su laptop y su usb.

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.

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.

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.

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.

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 realiza personal interno de la compañía, generalmente las personas que tienen un cargo importante, es por esto que las compañías deberían realizar auditorías de seguridad cada cierto tiempo.

5. 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.

1.- Auditar eventos de seguridad creando 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.

2.- Restringir el uso de 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. Esta ventaja no puede impedir el robo de datos, pero crea otra barrera ante su extracción no autorizada.

3.- Filtrar los datos adjuntos en servidores de correo implementando 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.

4.- 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.

6. Referencias

[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.