



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Advanced Incident Response, Threat Hunting, and Digital Forensics (Forensics
at <http://www.giac.org/registration/gcfa>

Table of Contents 1
Oscar_Ruiz_GCFA.doc 2

© SANS Institute 2005, Author retains full rights.

Analista Forense
Certificado

GCFA

Asignación Práctica

1.5

Version en Español

Oscar Ruiz
SANS Great Lakes 2004
/ Chicago IL
Enero 12 de 2004

© SANS Institute 2005, Author retains full rights.

Tabla de Contenido

<u>Resumen</u>	1
<u>Parte 1 – Análisis de una imagen desconocida</u>	2
<u>Detalles de la examinación</u>	2
<u>Detalles de la imagen</u>	24
<u>Detalles forenses</u>	29
<u>Identificación del programa</u>	30
<u>Implicaciones legales</u>	30
<u>Información adicional</u>	31
<u>Parte 2 - Opción 1: Análisis forense de un sistema</u>	32
<u>Sinopsis de los hechos del caso</u>	32
<u>Descripción del sistema</u>	32
<u>Hardware</u>	32
<u>Imagen del medio</u>	33
<u>Análisis de los medios del sistema</u>	45
<u>Análisis cronológico</u>	57
<u>Recuperación de archivos eliminados</u>	57
<u>Búsqueda de secuencias</u>	60
<u>Conclusiones</u>	60
<u>Referencias</u>	61

© SANS Institute 2005, Author retains full rights.

Resumen

El documento presentado a continuación consta de dos partes, la primera es el informe que refleja el análisis forense realizado en el marco de la asignación práctica 1.5 del proceso de certificación como Analista Forense (GCFA) de la Certificación Global del Aseguramiento de la Información (GIAC <http://www.giac.org/>) del Instituto de Administradores de Sistemas, Auditoría, Redes y Seguridad (SANS Institute <http://www.sans.org/>), en la primera parte de esta asignación se encuentra un reto que está relacionado con un posible caso de fuga de información, se parte de la descripción de unos hechos y la imagen del disco flexible (medio sospechoso), el objetivo del informe es dar un concepto técnico que ayude al administrador del sistema a determinar si en realidad se trató de un caso de fuga de información, la forma como se consumó, la información que se comprometió y finalmente las implicaciones legales en el marco de la legislación Colombiana.

La segunda parte corresponde a un informe que refleja el análisis de un sistema de computo confiscado por un ente de control en Colombia, se parte de la metodología usada para la confiscación de la evidencia física, así mismo se describe la metodología usada en la adquisición y análisis de imagen del medio confiscado; el objetivo del informe es dar un concepto técnico que pueda ser presentado como evidencia digital y/o indicio en un eventual proceso penal en el marco de la legislación Colombiana, que aplica desde el pasado enero 1 de 2005 el sistema acusatorio u oral y el cual requiere que los funcionarios de Policía Judicial de Colombia tengan la capacidad de tomar, presentar y sustentar evidencia digital.

Parte 1 – Análisis de una imagen desconocida

Análisis de una imagen de un disco flexible proveída en la parte 1 de la asignación práctica 1.5 del proceso de certificación como Analista Forense (GCFA) de la Certificación Global del Aseguramiento de la Información (GIAC <http://www.giac.org/>) del Instituto de Administradores de Sistemas, Auditoría, Redes y Seguridad (SANS Institute <http://www.sans.org/>) dentro de un caso de fuga de información.

Detalles de la examinación

Se descarga la imagen a analizar (http://www.giac.org/gcfa/v1_5.gz), de la cual se provee la siguiente información sobre la cadena de custodia:

Tag# fl-260404-RJL1
3.5 inch TDK floppy disk
MD5: d7641eb4da871d980adbe4d371eda2ad fl-260404-RJL1.img
fl-260404-RJL1.img.gz

Una vez descargado el archivo se procede a validar el resultado de la función de hash MD5 efectuada sobre la imagen descargada y la información provista por la cadena de custodia.

Se utilizaron los siguientes recursos para el análisis: Portátil HP – Compaq nc6000 Pentium M 1.6Mhz / 512 Mb RAM / Disco Duro de 40 Gb. / Windows XP Profesional SP2 y el programa EnCase Versión 4.20.

Creación de caso en EnCase: Se crea un directorio llamado “Caso SANS” en la raíz del disco duro de la estación forense usada, adicionalmente se crean tres subdirectorios llamados: “Temporal”, “Evidencia” y “Exportados” con el fin de almacenar en cada uno de ellos los archivos referentes al caso, posteriormente se procede a crear un caso llamado Caso SANS, el investigador asignado es Oscar Ruiz y se direccionan los directorios de trabajo del caso a los creados anteriormente.

Se copia el archivo descargado (v1_5.gz) al subdirectorio Evidencia, se procede a montar el disco duro de la estación forense y se obtiene la siguiente información: Valor del hash el cual es igual al proporcionado por la cadena de custodia e información sobre el tipo de archivo proveído en el web site.

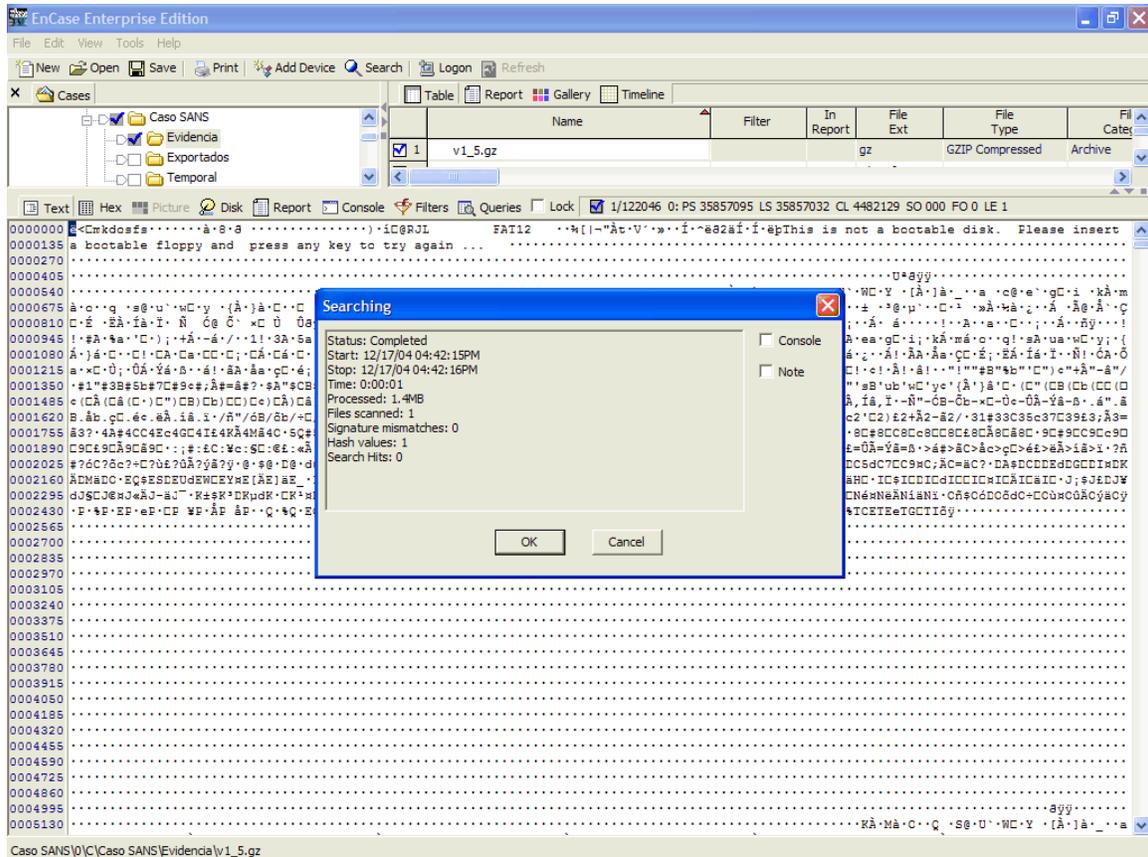


Imagen No. 1 Detalle del proceso de verificación de la imagen descargada e información del archivo descargado.

Por la visualización del contenido del archivo v1_5.gz (ver Imagen No. 1) se determina que NO es un archivo comprimido, se utiliza la funcionalidad de EnCase de visualización de archivos o volúmenes comprimidos el cual arroja como resultado que no es un tipo de archivo comprimido y en el campo de firma reporta mala firma (bad signature) debido a que por el tipo de extensión se catalogaría como un archivo GZIP pero al realizar la comparación con la firma del encabezado de este tipo de archivos, esta no concuerda. Al parecer el archivo entregado es la imagen que ha sido renombrada y se le ha colocado una extensión de archivo comprimido.

Visualizando el contenido del archivo imagen se puede determinar que se trata de una imagen de un disco flexible en un formato plano o tipo "raw" como el que hace la utilidad de linux "dd", es importante anotar que esta utilidad se encuentra también portada para windows y otros sistemas operativos.

Se puede visualizar en el sector de arranque la leyenda: "mkdosfs", "FAT12" y "This is not a bootable disk. Please insert a bootable floppy and press any key to try again" lo cual corrobora que se trata del archivo imagen de la unidad de disco flexible confiscada por el personal de seguridad al Sr. Robert Leszczynski

y entregada por el Sr. David Keen (administrador de seguridad) para este análisis.

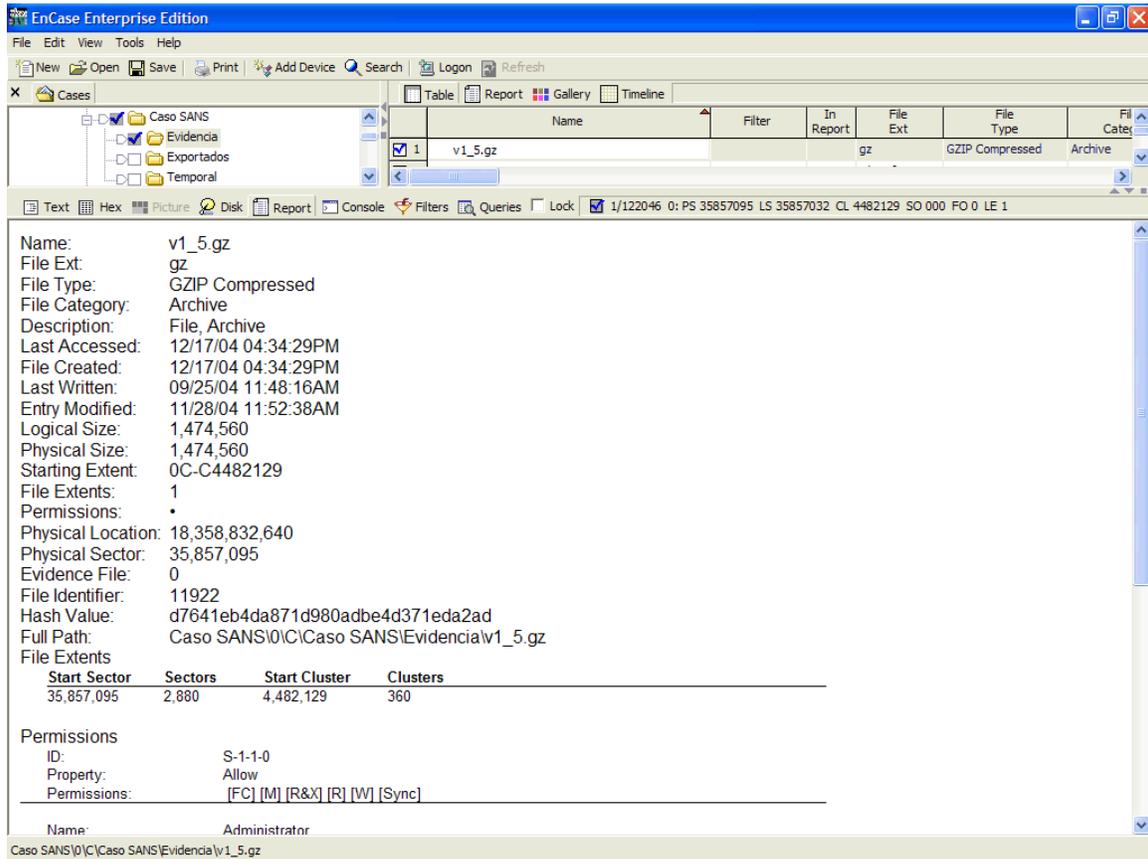


Imagen No. 2 Detalle del resultado del hash de la imagen descargada.

Se valida el resultado obtenido con el programa EnCase:

d7641eb4da871d980adbe4d371eda2ad es igual al MD5:

d7641eb4da871d980adbe4d371eda2ad fl-260404-RJL1.img de la cadena de custodia.

Lo anterior evidencia la integridad del archivo descargado lo cual permite continuar con el proceso de adquisición de evidencia de EnCase y el posterior análisis.

El resultado del proceso de adquisición de evidencia de EnCase es satisfactorio y genera el siguiente valor de hash D7641EB4DA871D980ADBE4D371EDA2AD (ver Imagen No. 3). La imagen obtenida por EnCase se le ha dado el nombre que aparece en la cadena de custodia "fl-260404-RJL1" y la extensión que utiliza EnCase es "e01" y gracias a este formato que cada 64 sectores (32Kb) coloca un CRC (Chequeo de Redundancia Cíclica) y al final el valor del resultado del hash MD5 lo cual permite verificar la integridad (gradualmente) de esta en cualquier momento, adicionalmente y gracias a la característica de compresión las imágenes ocupan mucho menos, por ejemplo el tamaño del

archivo “evidencia” de Encase: “fl-260404-RJL1.e01” es de 524,771 bytes

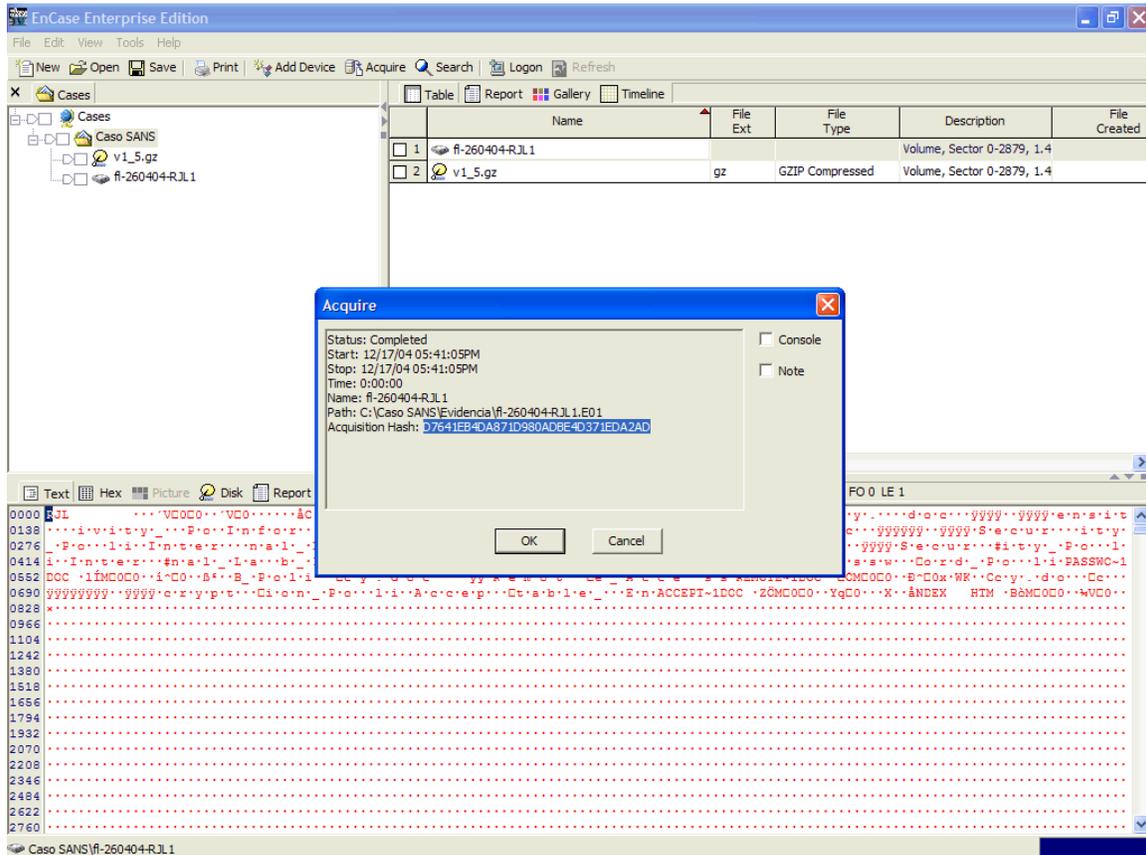


Imagen 3. Detalle del proceso de adquisición de evidencia de EnCase

Utilizando la imagen adquirida por EnCase se procede a analizar el contenido del disco flexible, lo cual evidencia seis (6) Archivos de Word (extensión .doc), un (1) archivo de hipertexto (extensión .htm) y un (1) archivo de librería (extensión .dll), estos dos últimos se encuentran borrados y el archivo correspondiente a la librería se encuentra parcialmente sobre escrito, sin embargo se procede a exportar los seis (6) archivos de documentos y los dos (2) archivos eliminados al subdirectorio de Exportados.

Utilizando la búsqueda por palabras clave de EnCase donde de forma predeterminada se encuentran las de búsqueda para direcciones web y correo se ejecutan sobre la totalidad de la evidencia y arrojan como resultado estos tres web sites:

- <http://download.macromedia.com/> (sector 33)
- <http://www.macromedia.com/> (sector 34)
- <http://www.camouflage.freeseerve.co.uk> (sector 90)

Este último es el primer hallazgo importante ya que el sector en que se halló

pertenece al área de la librería borrada y parcialmente sobre escrita. Una vez encontrada esta pista se procede a buscar en Internet (se utiliza el motor de búsqueda de Google) la relación entre los nombres de la librería y el web site encontrado, lo cual arroja como resultado que la librería es parte del programa “Camouflage”, se intenta ingresar al web site <http://www.camouflage.freemove.co.uk>, pero no se encuentra disponible, sin embargo los resultados de las búsquedas entregan el nombre del binario “instalador” del programa “Camou121.exe” y se logra descargarlo de otro sitio. Se toman las medidas de precaución de descarga de sitios no oficiales tal como verificación por programas antivirus y antiespía (spyware).

Posteriormente se procede a realizar la instalación del programa camouflage y nuevamente se practican las pruebas de antivirus y antiespía, fácilmente se puede entender el modo de uso ya que al estar sobre un archivo y haciendo clic con el botón derecho del ratón salen dos ítems adicionales en el menú, son las opciones “Camouflage” y “Uncamouflage”, después de hacer un par de pruebas sobre archivos planos de texto, imágenes y documentos de Word y Excel se puede entender su funcionamiento, el programa Camouflage se utiliza para esconder un archivo en otro, utilizando una técnica de cifrado y añadiendo esta información final del archivo origen, sin alterar el contenido original de este, pero incrementa el tamaño original, este programa tiene la opción de asignar una clave para la recuperación del o los documentos escondidos.

Se realiza a través de una metodología ensayo / error pruebas sobre los documentos extraídos de la imagen dando como resultado que en uno de los archivos no tiene clave asignada, el nombre del archivo es “Internal_Lab_Security_Policy.doc” y se pueden recuperar el documento original y el un archivo de texto plano llamado “Opportunity.txt” (ver secuencia en las imágenes No. 3, 4, 5, y 6), los archivos son extraídos en el directorio “Camouflage” del subdirectorío de “Exportados” (ver Imagen No. 7), el contenido del archivo “Opportunity.txt” (ver Imagen No. 8) es el segundo hallazgo más importante encontrado en este reto, ya que evidencia las intención del Sr. Robert Leszczynski de entregar información por una alta cifra de dinero, evidencia el envío de una base de datos de ejemplo y diseños, adicionalmente instruye en la forma de “encontrar” la documentación en referencia, escribiendo “Primer Nombre”.

Nuevamente a través de una metodología ensayo / error se realizaron pruebas en los dos archivos identificados como sospechosos, a través de EnCase, se visualizo su contenido y se evidencio un tipo de cifrado al final del archivo, además el solo tamaño de los archivos generaban sospecha por tratarse de documentos de texto. Se probó diferentes claves como el “Primer Nombre” de Mr. Leszczynski (Robert, robert), también con el “primer” apellido (Leszczynski, leszczynski) y así sucesivamente con los nombres del administrado del sistema, los nombres de la compañías involucradas, etc, sin éxito alguno. De

repente una idea sobre la relación con el nombre del archivo fue el “eureka” de este reto, la clave asignada era el “Primer Nombre” (con Mayúsculas y minúsculas) del archivo a descifrar.

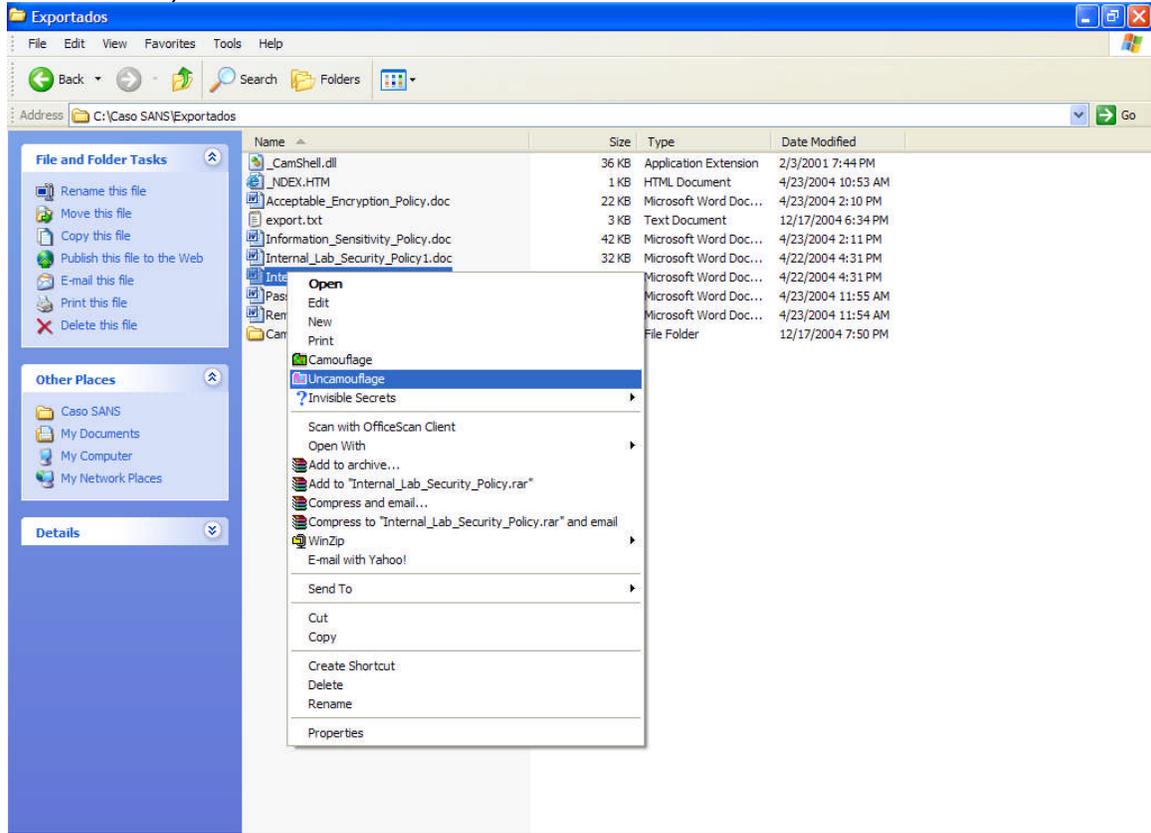


Imagen No. 3 Detalles del uso del programa camouflaje en archivo Internal_Lab_Security_Policy.doc

© SANS Institute

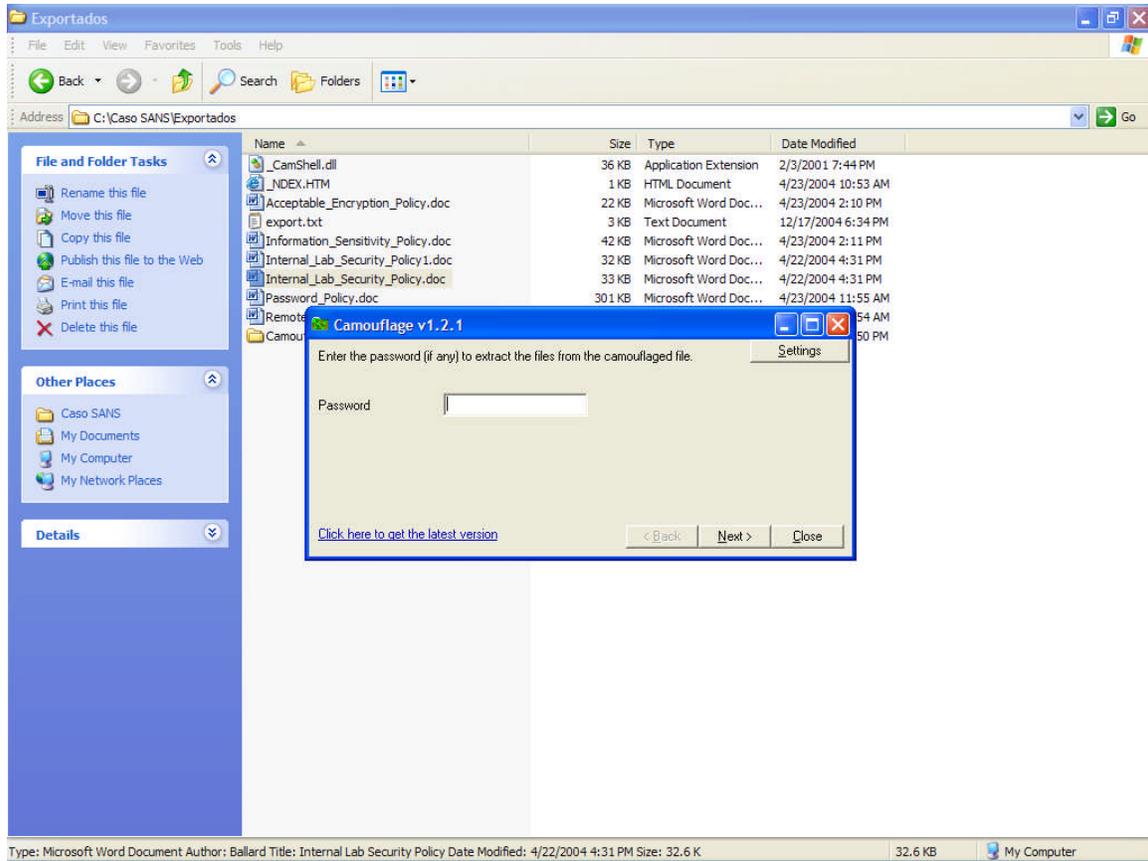


Imagen No. 4 Detalles del uso del programa camouflaje en archivo Internal_Lab_Security_Policy.doc

© SANS Institute 2005

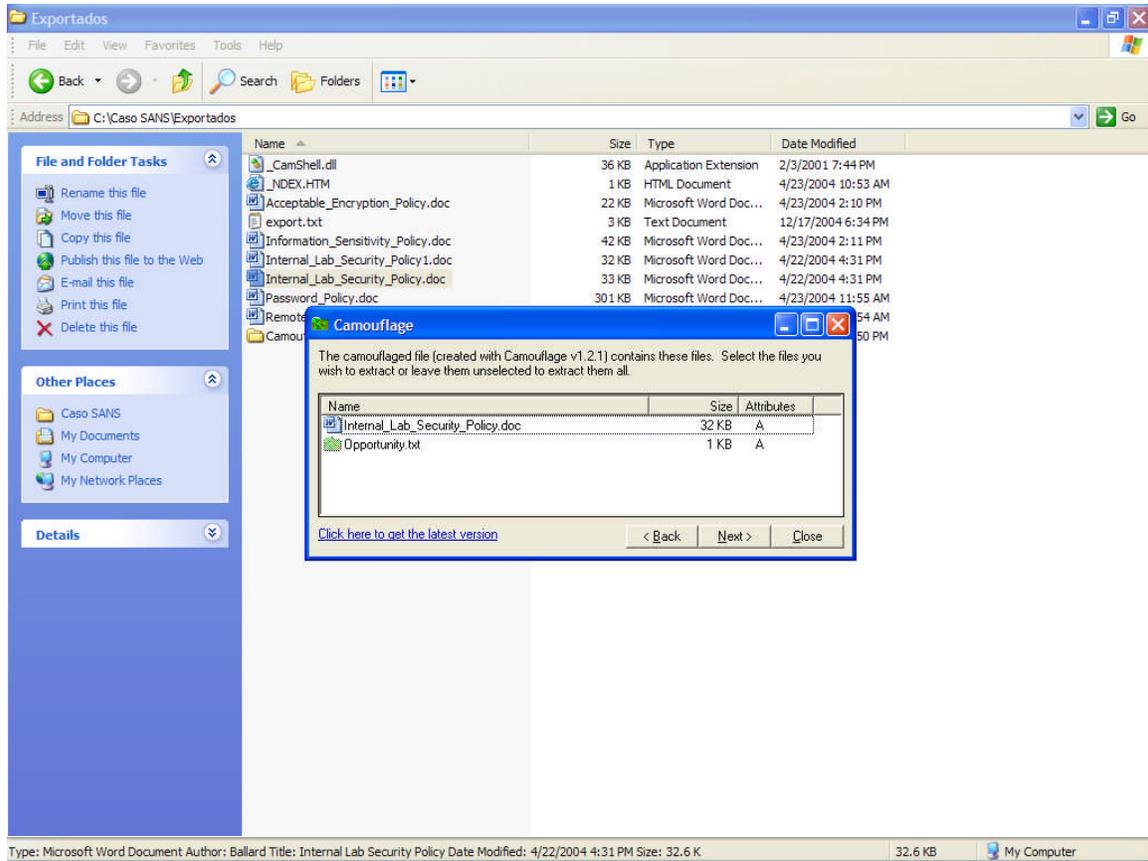


Imagen No. 5 Detalles del uso del programa camouflaje en archivo Internal_Lab_Security_Policy.doc

© SANS Institute 2005

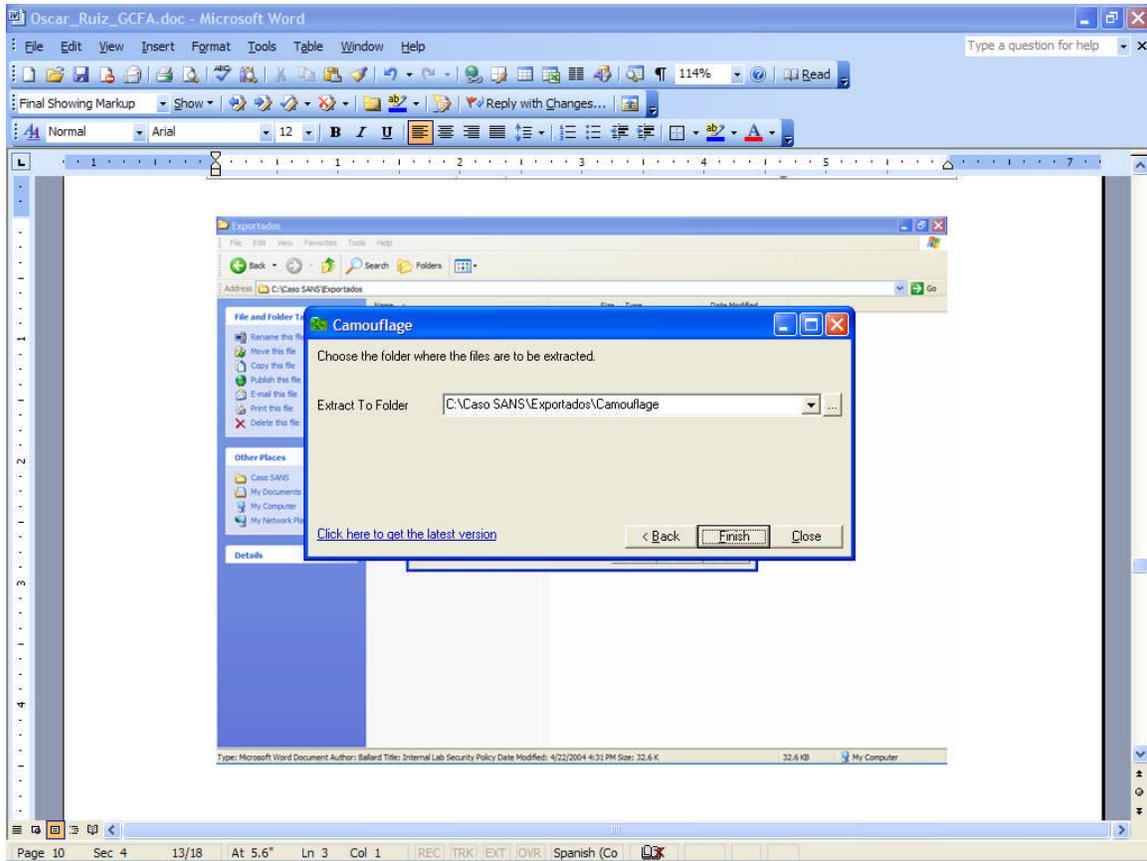


Imagen No. 6 Detalles del uso del programa camouflaje en archivo Internal_Lab_Security_Policy.doc

© SANS Institute 2005

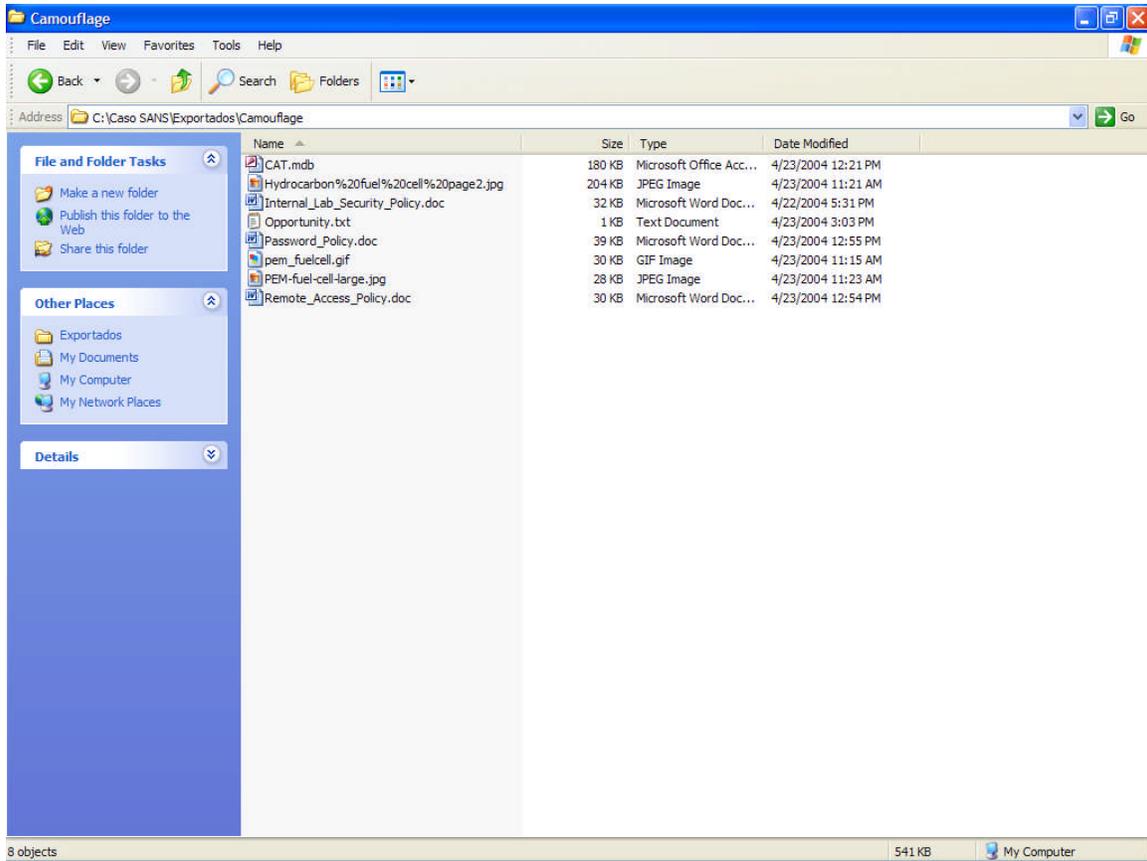


Imagen No. 7 Detalle de los archivos exportados y usados con el programa camuflaje

© SANS Institute 2005

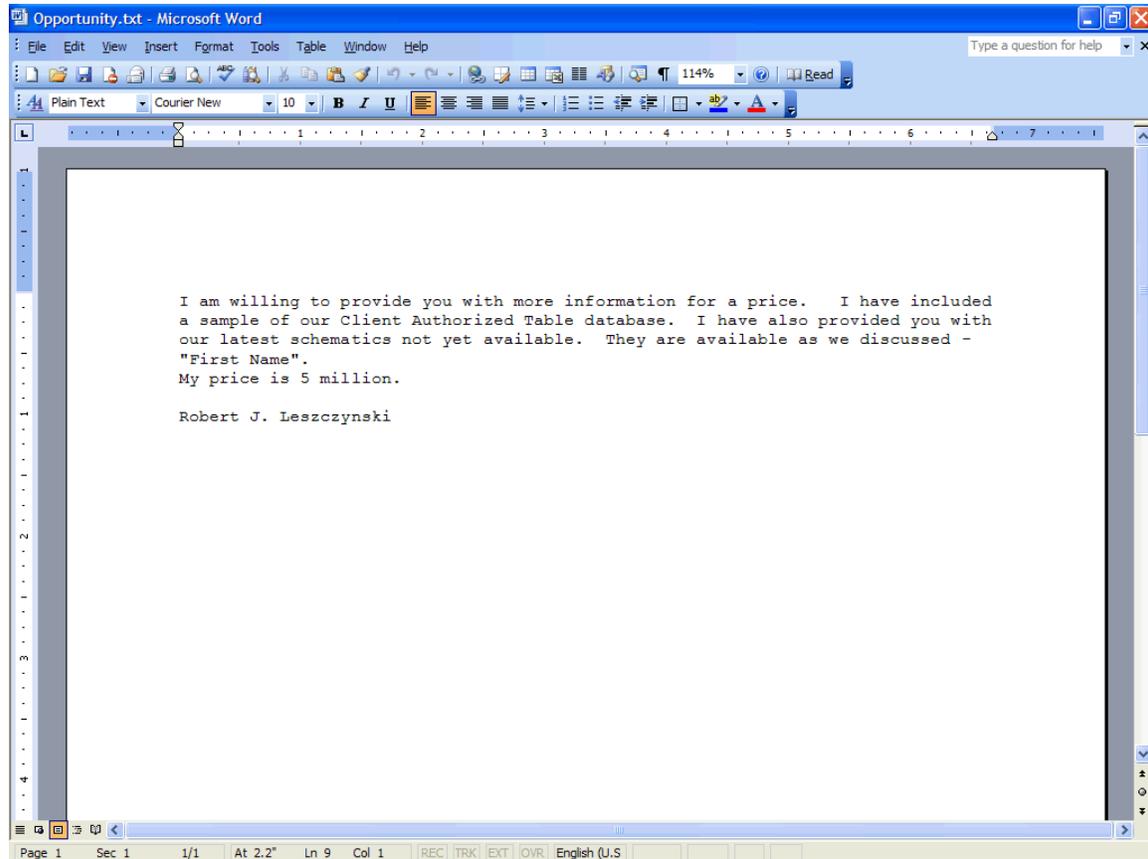


Imagen No. 8 Detalle del archivo Opportunity.txt

Es así como se logró recuperar el contenido de los siguientes archivos:

Password_Policy.doc la clave es: Password (ver Imágenes No. 9, 10 y 11)

El cual contiene los archivos: Password_Policy.doc (texto original de la política de claves)

pem_fuelcell.gif Imagen de un Diseño (ver Imagen No. 12)

PEM-fuel-cell-large.jpg Imagen de un Diseño (ver Imagen No. 13)

Hydrocarbon fuel cell page2.jpg Imagen y Detalles de un Diseño (ver Imagen No. 14)

Remote_Access_Policy.doc la claves: Remote (ver Imágenes No. 15, 16 y 17)

El cual contiene los archivos: Remote_Access_Policy.doc (texto original de la política de acceso remoto)

CAT.mdb Ejemplo de Base de Datos de Clientes (ver Imagen No. 18)

Finalmente se realizaron los cálculos del valor de hash MD5 para esos archivos y se determinó que el valor de hash MD5 del archivo

"Internal_Lab_Security_Policy.doc" extraído del archivo del mismo nombre

hallado en la imagen es igual al archivo *"Internal_Lab_Security_Policy1.doc"*

hallado también en la imagen, lo cual evidencia el uso de la herramienta por el

Sr. Robert Leszczynski (ver Imagenes No. 19 y 20)

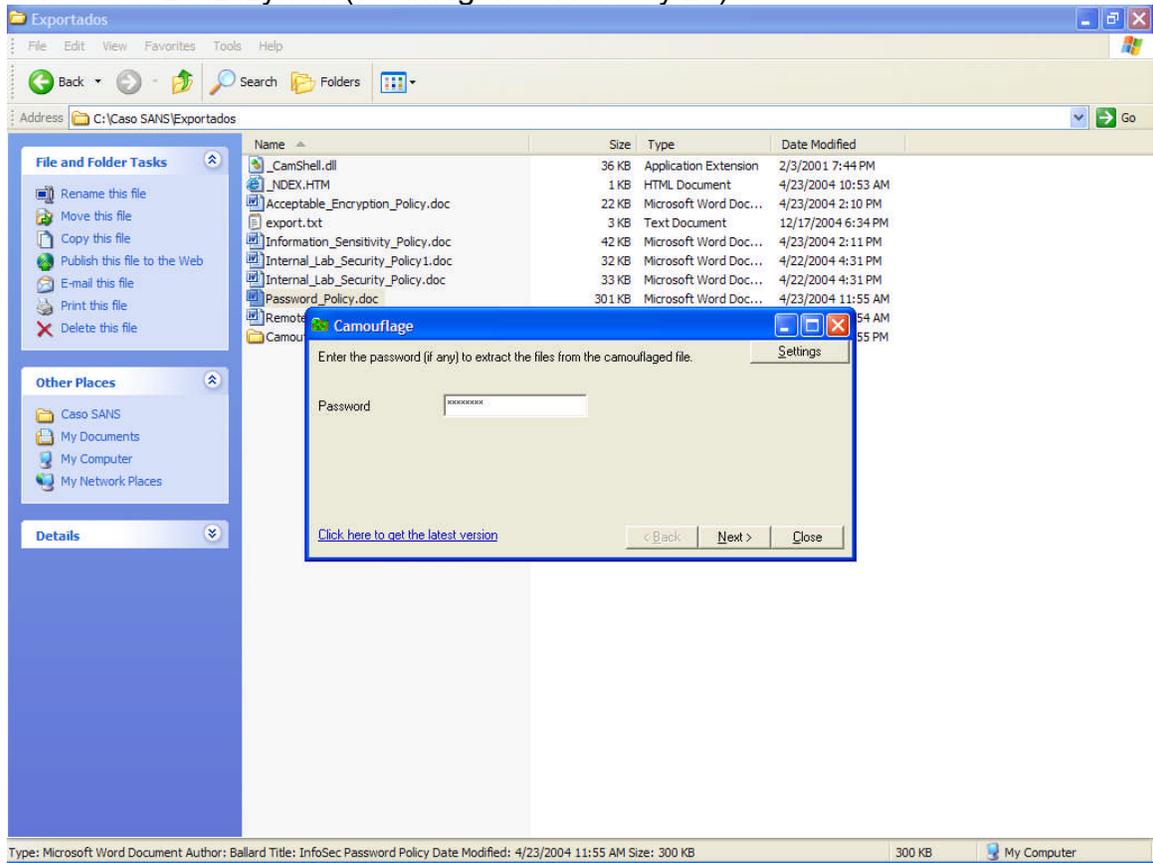


Imagen No. 9 Detalles del uso del programa camouflaje en archivo Password_Policy.doc

© SANS Institute 2005

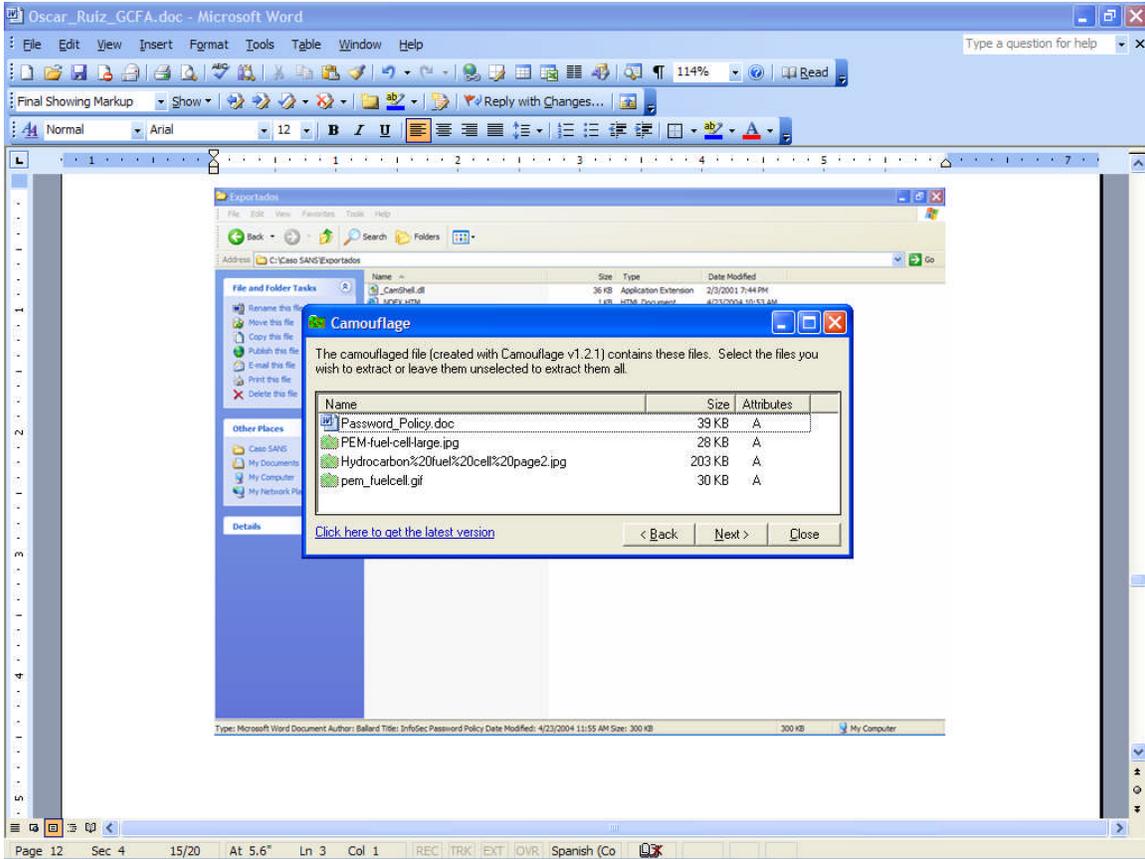


Imagen No. 10 Detalles del uso del programa camouflaje en archivo Password_Policy.doc

© SANS Institute 2005

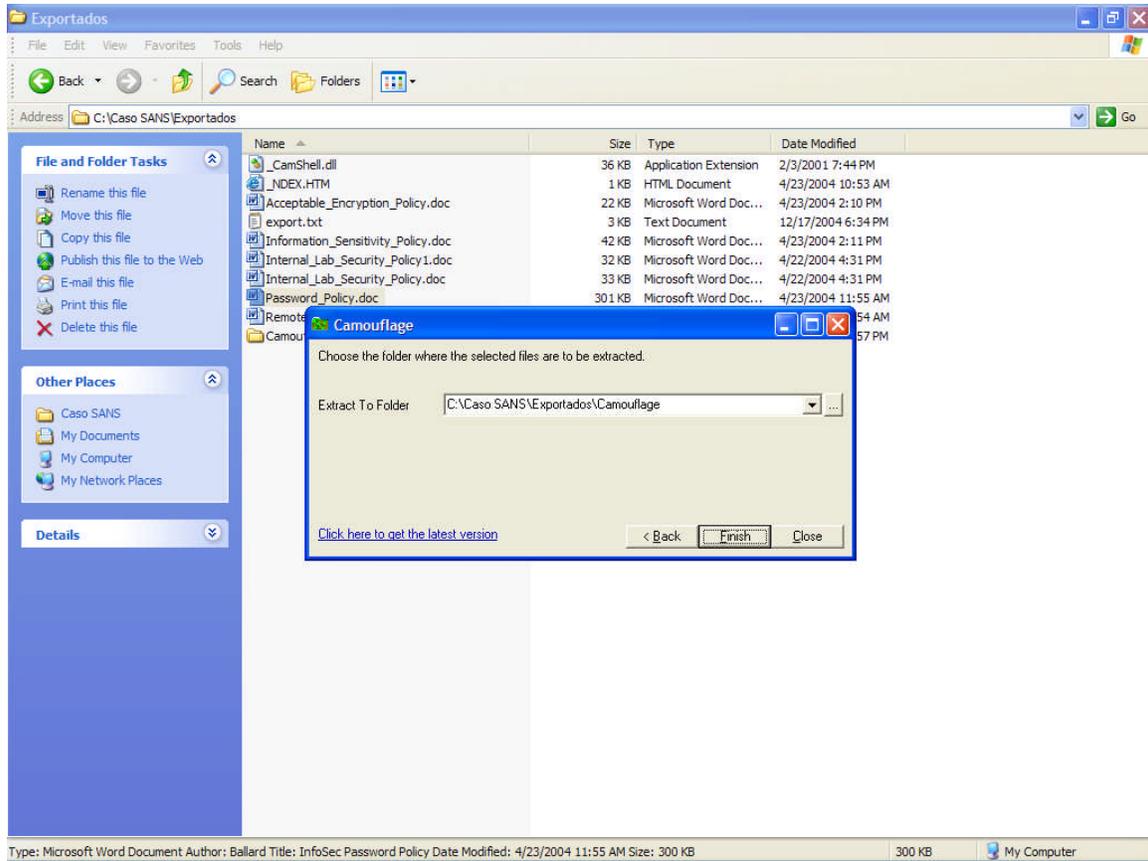


Imagen No. 11 Detalles del uso del programa camouflaje en archivo Password_Policy.doc

© SANS Institute 2005

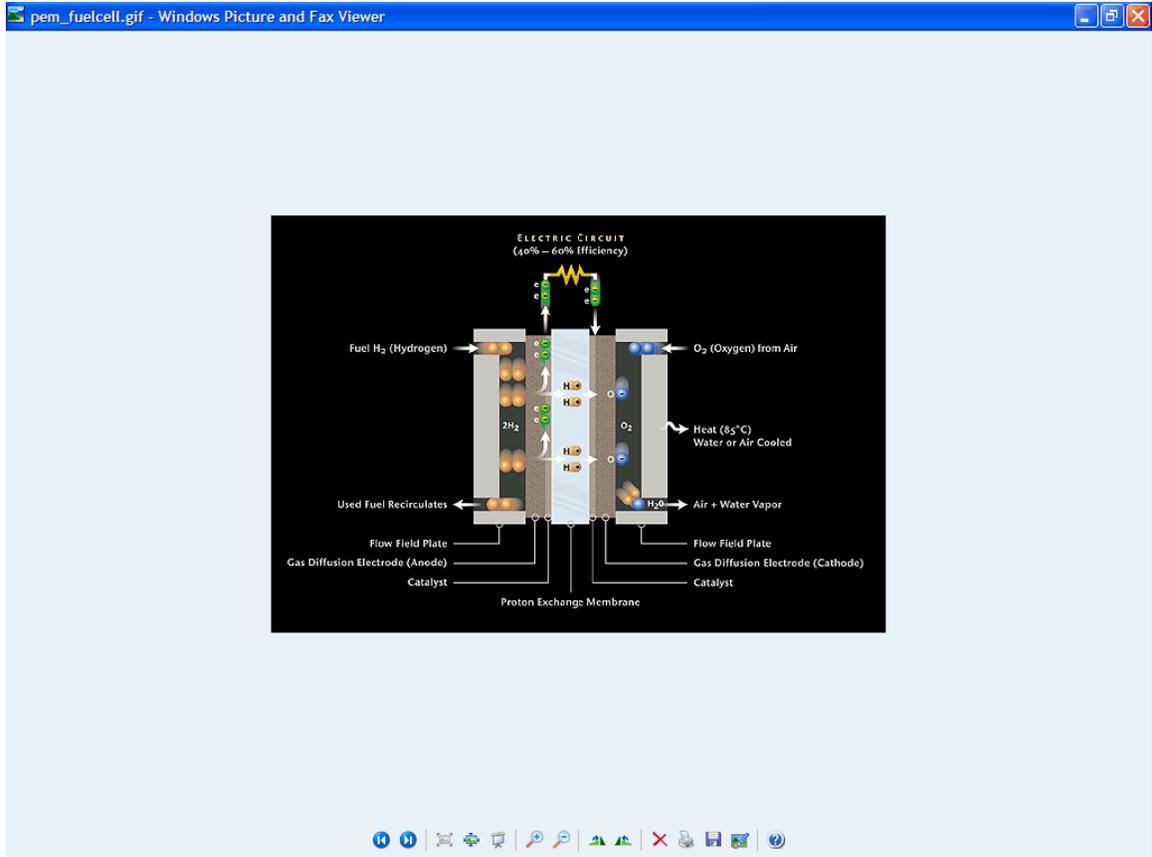


Imagen No. 12 Detalle archivo pem_fuelcell.gif

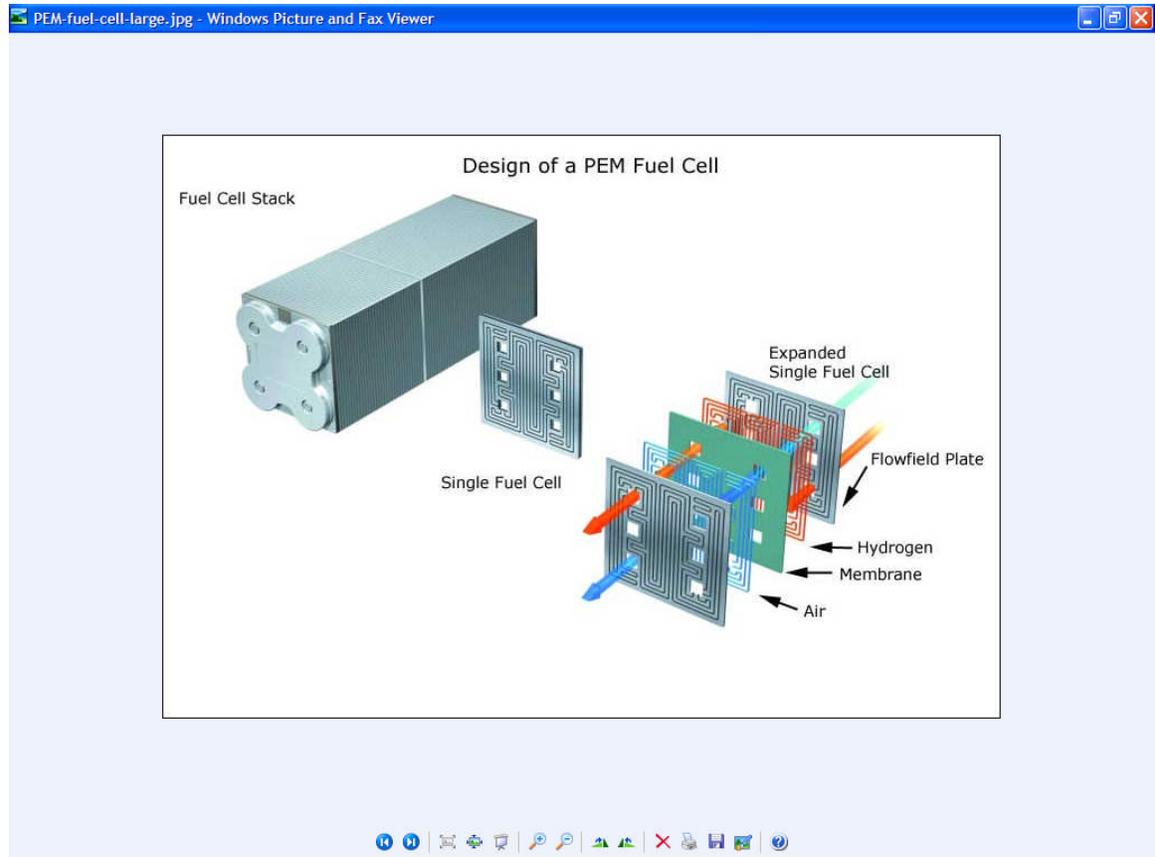


Imagen No. 13 Detalle archivo PEM-fuel-cell-large.jpg

© SANS Institute 2005

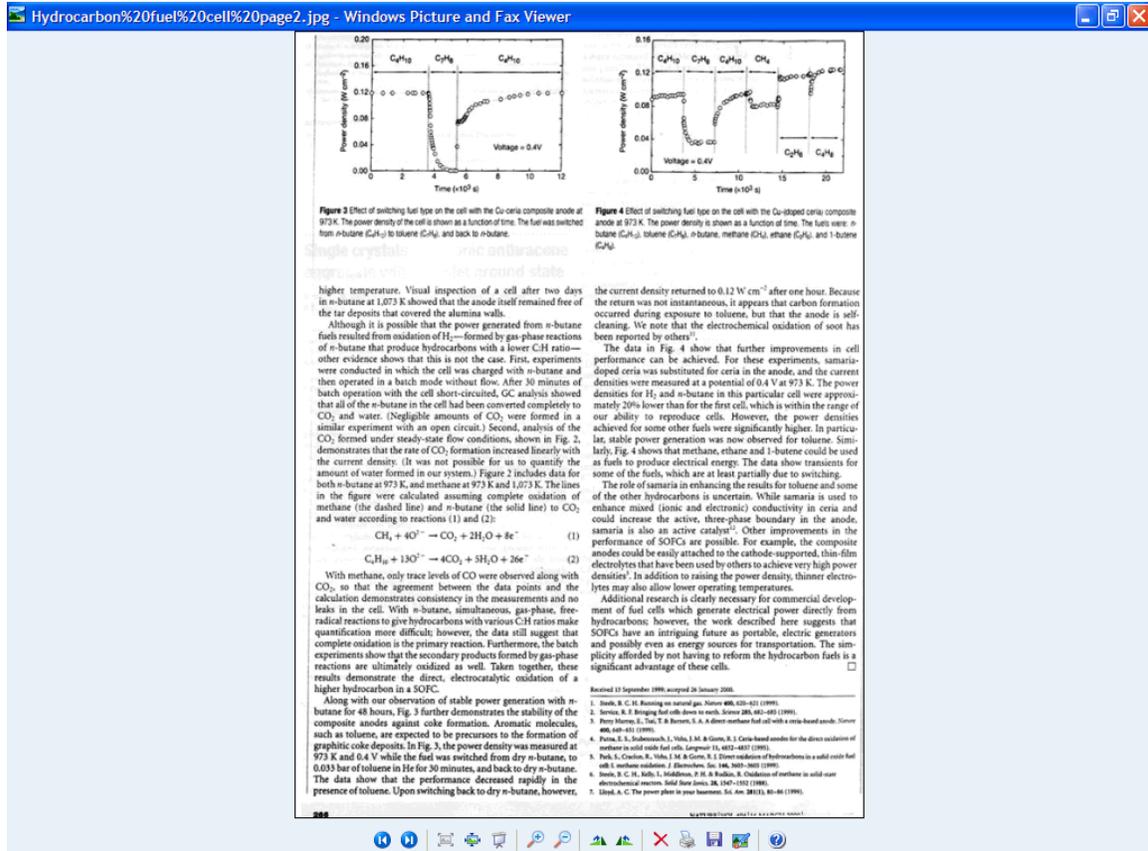


Imagen No. 14 Detalle archivo Hydrocarbon fuel cell page2.jpg

© SANS Institute 2005

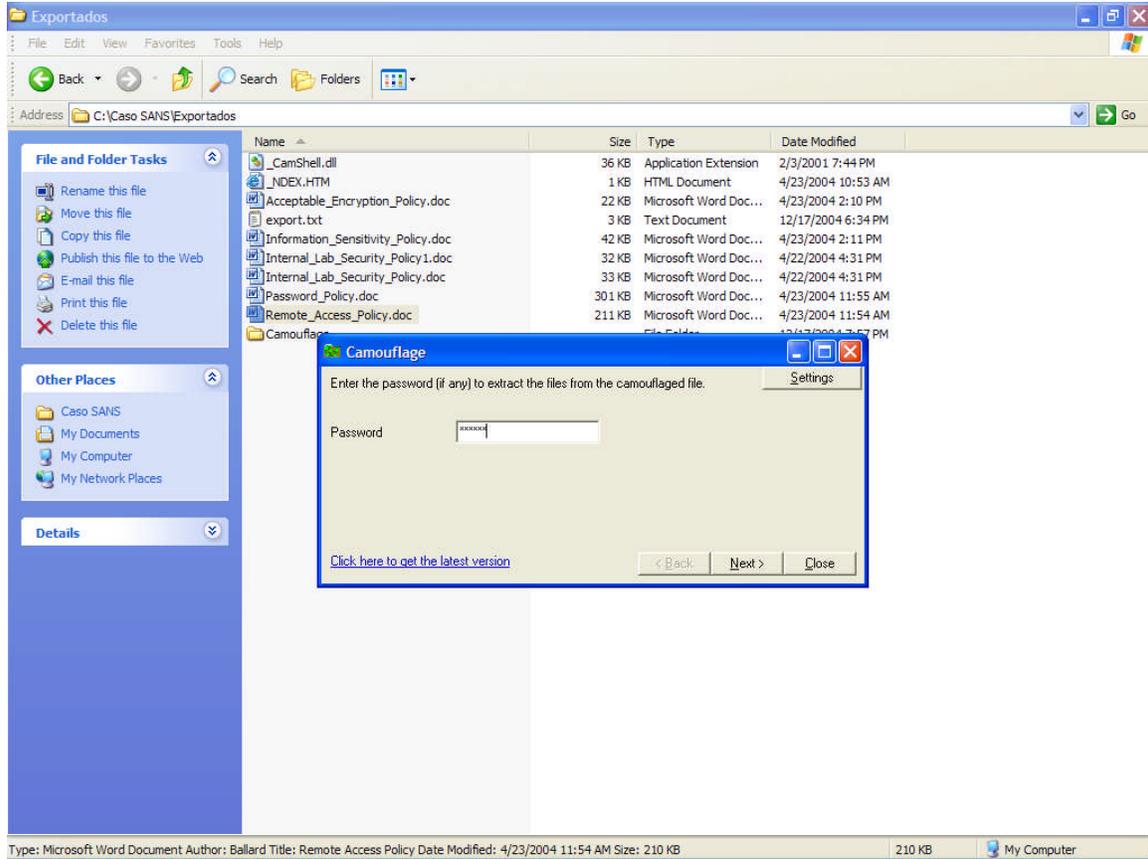


Imagen No. 15 Detalles del uso del programa camouflaje en archivo Remote_Access_Policy.doc

© SANS Institute 2005

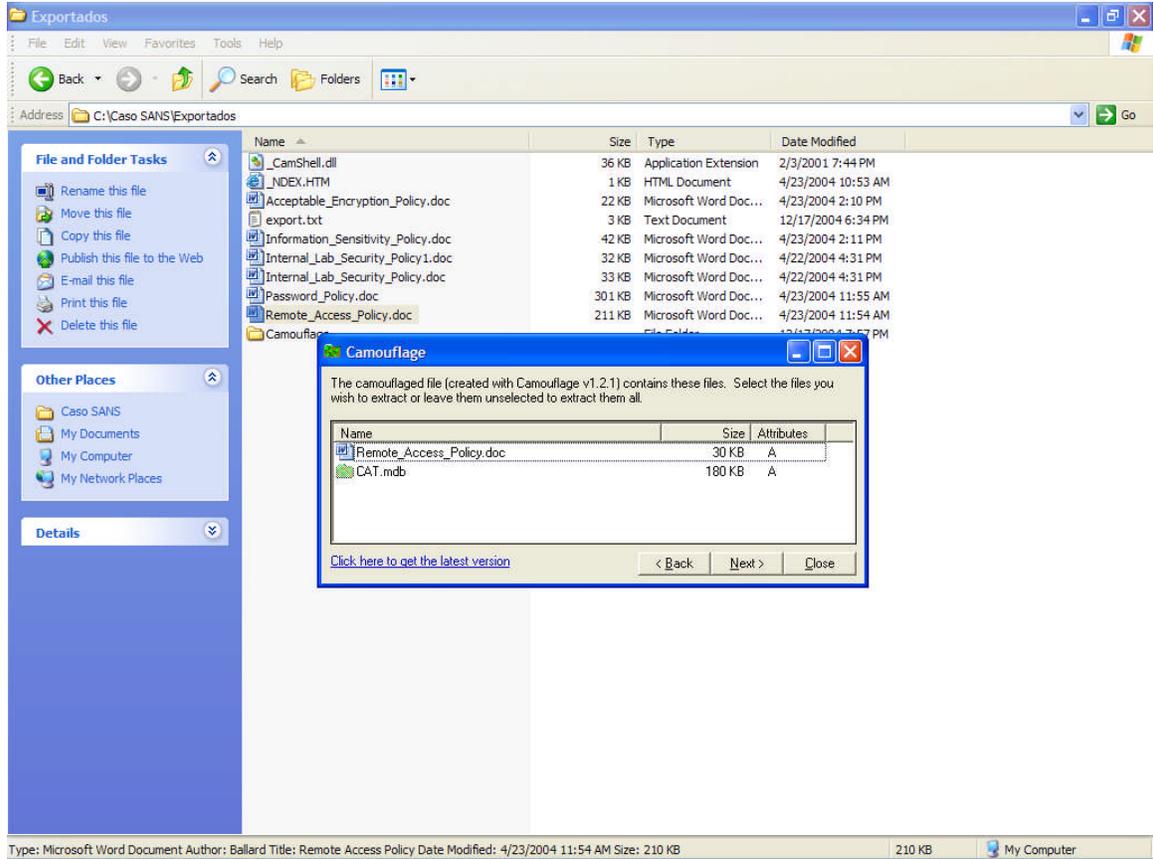


Imagen No. 16 Detalles del uso del programa camouflaje en archivo Remote_Access_Policy.doc

© SANS Institute 2005

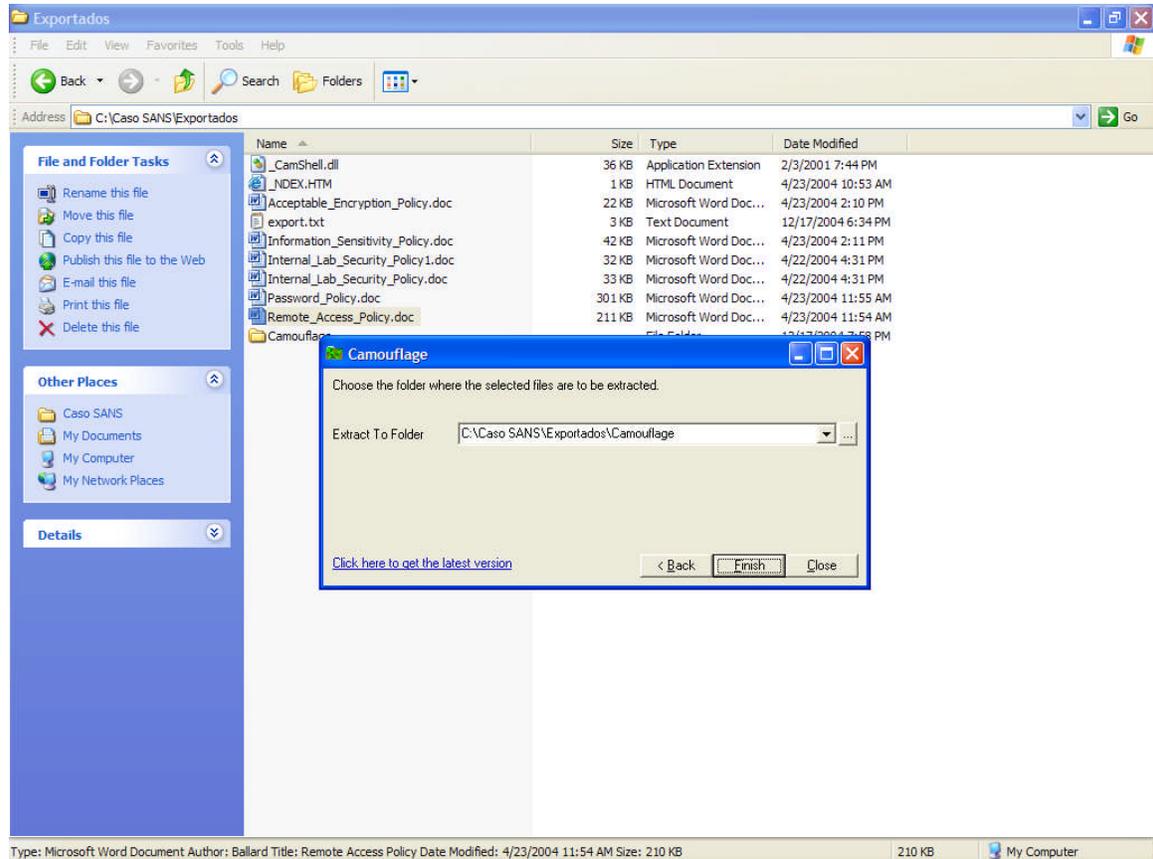


Imagen No. 17 Detalles del uso del programa camouflaje en archivo Remote_Access_Policy.doc

© SANS Institute 2005

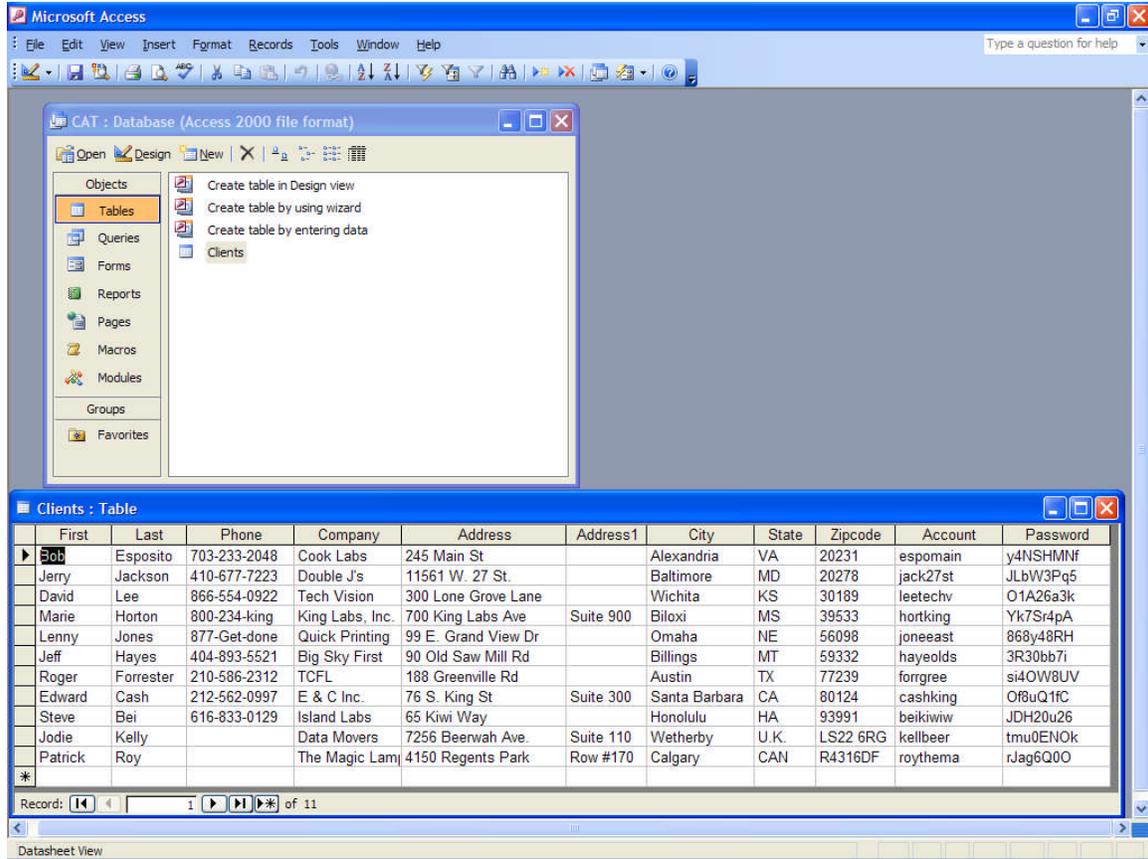


Imagen No. 18 Detalles del archivo CAT.mdb

© SANS Institute 2005

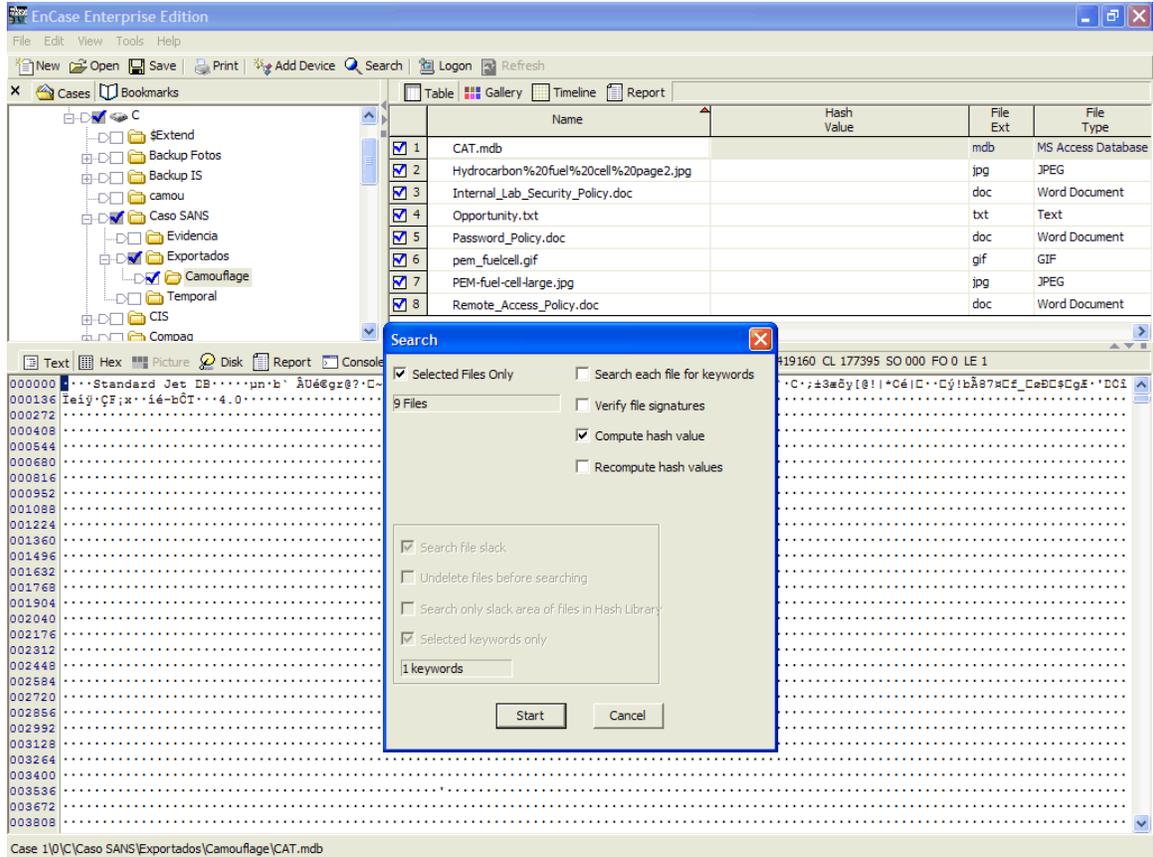


Imagen No. 19 Detalles del valor de Hash MD5 de los archivos usados y escondidos con el programa “Camouflage”

© SANS Institute 2005

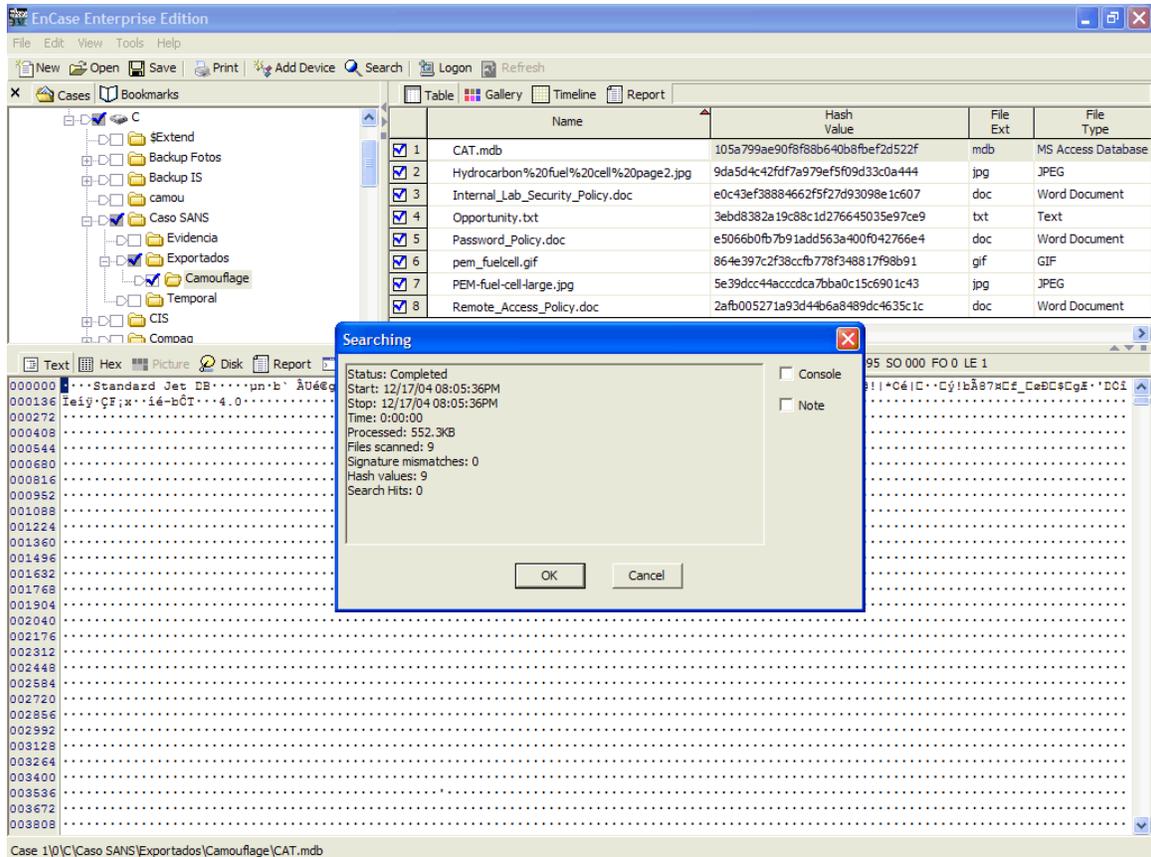


Imagen No. 20 Detalles del valor de Hash MD5 de los archivos usados y escondidos con el programa "Camouflage"

Detalles de la imagen

Listado de todos los archivos en la imagen:

Nombre de archivos en la imagen y (nombre corto):

_NDEX.HTM (INDEX.HTM)
 Acceptable_Encryption_Policy.doc (ACEPT~1.DOC)
 CamShell.dll (CAMSHELL.DLL)
 Information_Sensitivity_Policy.doc (INFORM~1.DOC)
 Internal_Lab_Security_Policy.doc (INTERN~2.DOC)
 Internal_Lab_Security_Policy1.doc (INTERN~1.DOC)
 Password_Policy.doc (PASSWO~1.DOC)
 Remote_Access_Policy.doc (REMOTE~1.DOC)

Nombre verdadero del programa / archivo usado por el Sr. Leszczynski:

Programa utilizado: Camouflage Versión 1.2.1

Nombre de archivos camuflados en archivos de la imagen y (nombre corto):

Internal_Lab_Security_Policy.doc contiene:
 Internal_Lab_Security_Policy.doc (INTERN~1.DOC)
 Opportunity.txt (OPPORT~1.TXT)

Password_Policy.doc contiene:
 Password_Policy.doc (PASSWO~1.DOC)
 pem_fuelcell.gif (PEM_FU~1.GIF)
 PEM-fuel-cell-large.jpg (PEM-FU~1.JPG)
 Hydrocarbon fuel cell page2.jpg (HYDROC~1.JPG)

Remote_Access_Policy.doc contiene:
 Remote_Access_Policy.doc (REMOTE~1.DOC)
 CAT.mdb (CAT.MDB)

Información del Archivo / Tiempo MAC (última modificación, último acceso y último cambio de tiempo)

Nombres y detalles de los archivos en la imagen:

Nombre	Ultimo Acceso	Fecha de Creación	Ultima Escritura
_NDEX.HTM	04/26/04	04/26/04 09:47:36A M	04/23/04 10:53:56A M
Acceptable_Encryption_Policy.doc	04/26/04	04/26/04 09:46:44A M	04/23/04 02:10:50P M
CamShell.dll	04/26/04	04/26/04 09:46:18A M	02/03/01 07:44:16P M
Information_Sensitivity_Policy.doc	04/26/04	04/26/04 09:46:20A M	04/23/04 02:11:10P M
Internal_Lab_Security_Policy.doc	04/26/04	04/26/04 09:46:24A M	04/22/04 04:31:06P M
Internal_Lab_Security_Policy1.doc	04/26/04	04/26/04 09:46:22A M	04/22/04 04:31:06P M
Password_Policy.doc	04/26/04	04/26/04 09:46:26A M	04/23/04 11:55:26A M

Remote_Access_Policy.doc	04/26/04	04/26/04 09:46:36A M	04/23/04 11:54:32A M
--------------------------	----------	----------------------------	----------------------------

Nombres y detalles de los archivos camuflados:

Internal_Lab_Security_Policy.doc contiene:

Nombre	Ultimo Acceso	Fecha de Creación	Ultima Escritura
Internal_Lab_Security_Policy.doc	04/23/04 03:58:29P M	04/22/04 05:30:44P M	04/22/04 05:31:04P M
Opportunity.txt	04/23/04 03:59:09P M	04/23/04 12:19:23P M	04/23/04 03:03:53P M

Password_Policy.doc contiene:

Nombre	Ultimo Acceso	Fecha de Creación	Ultima Escritura
Password_Policy.doc	04/23/04 03:58:21PM	04/23/04 10:22:40AM	04/23/04 12:55:25PM
pem_fuelcell.gif	04/23/04 03:59:36PM	04/23/04 11:19:47AM	4/23/04 11:15:16AM
PEM-fuel-cell-large.jpg	04/23/04 03:59:36PM	04/23/04 11:23:32AM	04/23/04 11:23:23AM
Hydrocarbon fuel cell page2.jpg	04/23/04 03:59:36PM	04/23/04 11:21:26AM	04/23/04 11:21:02AM

Remote_Access_Policy.doc contiene:

Nombre	Ultimo Acceso	Fecha de Creación	Ultima Escritura
Remote_Access_Policy.doc	04/23/04 04:00:23P M	04/23/04 10:22:44A M	04/23/04 12:54:31P M
CAT.mdb	04/23/04 04:00:14P M	04/22/04 04:57:35P M	04/23/04 12:21:06P M

Propietario(s) del archivo. (usuario y/o grupo):

El sistema es FAT12 el cual NO tiene la seguridad de acceso a nivel de usuario y/o grupo

Nombres y tamaño de los archivos en la imagen:

Nombre del Archivo	Tamaño del Archivo en bytes
--------------------	-----------------------------

_NDEX.HTM	727
Acceptable_Encryption_Policy.doc	22,528
CamShell.dll	36,864
Information_Sensitivity_Policy.doc	42,496
Internal_Lab_Security_Policy.doc	33,423
Internal_Lab_Security_Policy1.doc	32,256
Password_Policy.doc	307,935
Remote_Access_Policy.doc	215,895

Nombres y tamaño de los archivos camuflados:

Internal_Lab_Security_Policy.doc contiene:

Nombre del Archivo	Tamaño del Archivo en bytes
Internal_Lab_Security_Policy.doc	32,256
Opportunity.txt	312

Password_Policy.doc contiene:

Nombre del Archivo	Tamaño del Archivo en bytes
Password_Policy.doc	39,936
pem_fuelcell.gif	30,264
PEM-fuel-cell-large.jpg	28,167
Hydrocarbon fuel cell page2.jpg	208,127

Remote_Access_Policy.doc contiene:

Nombre del Archivo	Tamaño del Archivo en bytes
Remote_Access_Policy.doc	30,720
CAT.mdb	184,320

Nombre y Valor del hash MD5 de los archivos de la imagen:

Nombre del Archivo	Valor de Hash
_NDEX.HTM	17282ea308940c530a86d07215473c79
Acceptable_Encryption_Policy.doc	f785ba1d99888e68f45dabeddb0b4541
CamShell.dll	6462fb3acca0301e52fc4ffa4ea5eff8
Information_Sensitivity_Policy.doc	99c5dec518b142bd945e8d7d2fad2004
Internal_Lab_Security_Policy.doc	b9387272b11aea86b60a487fbd1b336
Internal_Lab_Security_Policy1.doc	e0c43ef38884662f5f27d93098e1c607
Password_Policy.doc	ac34c6177ebdc4f4adc41f0e181be1bc
Remote_Access_Policy.doc	5b38d1ac1f94285db2d2246d28fd07e8

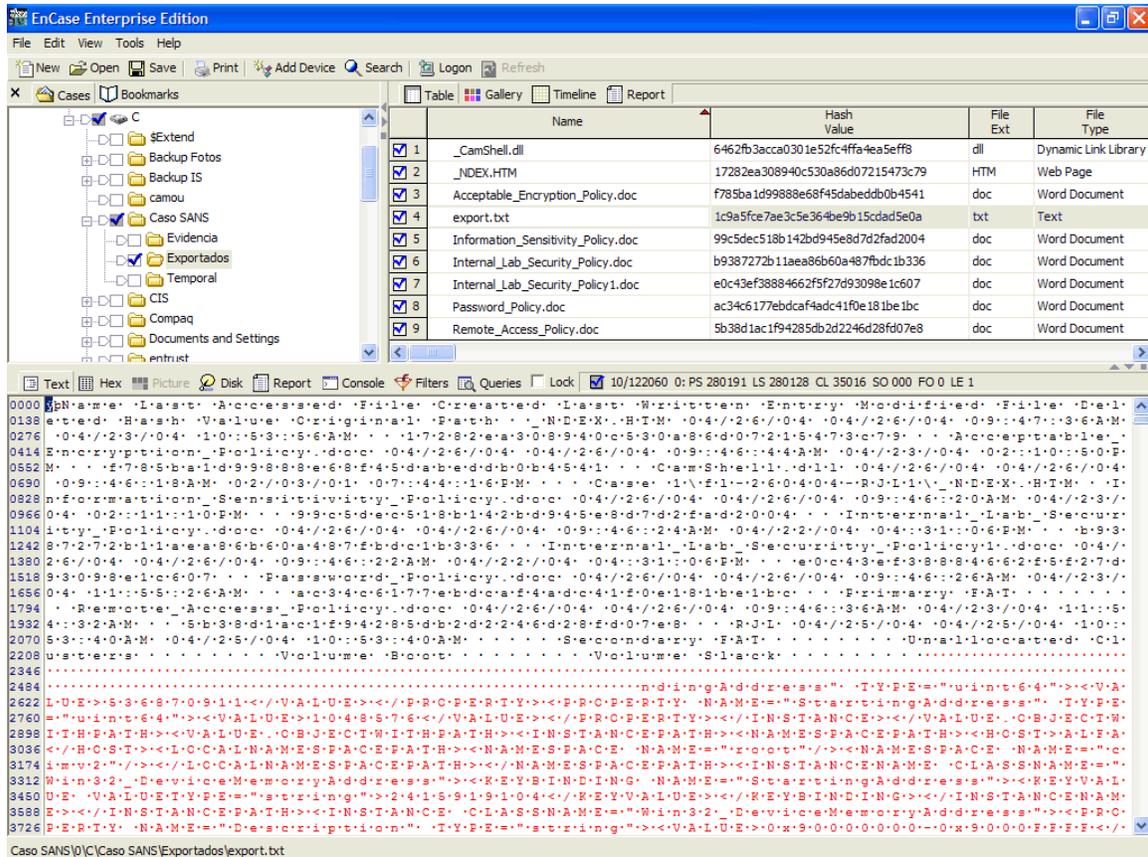


Imagen No. 21 Detalle de los valores de Hash MDS de los archivos de la imagen

Nombre y Valor del hash MD5 de los archivos camuflados:

Internal Lab Security Policy.doc contiene:

Nombre del Archivo	Valor de Hash
Internal_Lab_Security_Policy.doc	e0c43ef38884662f5f27d93098e1c607
Opportunity.txt	3ebd8382a19c88c1d276645035e97ce9

Password Policy.doc contiene:

Nombre del Archivo	Valor de Hash
Password_Policy.doc	e5066b0fb7b91add563a400f042766e4
pem_fuelcell.gif	864e397c2f38ccfb778f348817f98b91
PEM-fuel-cell-large.jpg	5e39dcc44accdcda7bba0c15c6901c43
Hydrocarbon fuel cell page2.jpg	9da5d4c42fdf7a979ef5f09d33c0a444

Remote Access Policy.doc contiene:

Nombre del Archivo	Valor de Hash
Remote_Access_Policy.doc	2afb005271a93d44b6a8489dc4635c1c
CAT.mdb	c3a869ff6b71c7be3eb06b6635c864b1

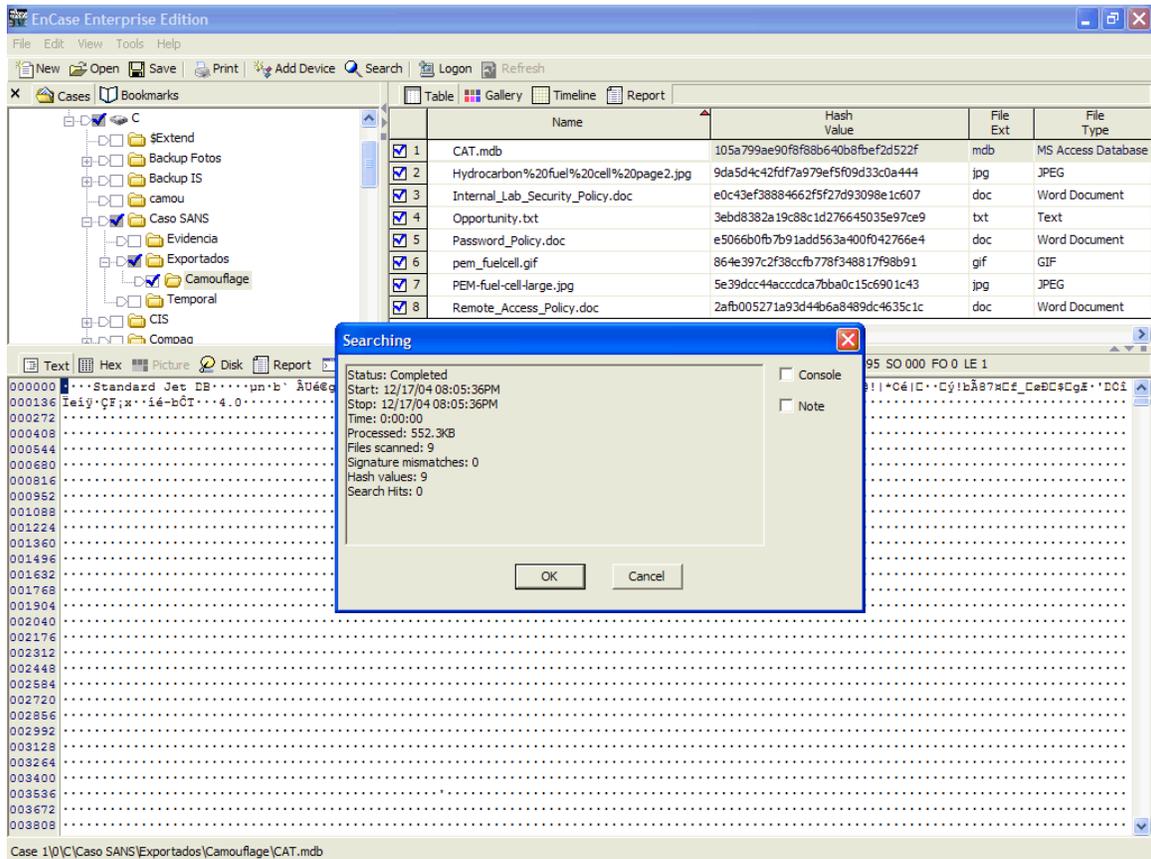


Imagen No. 22 Detalle de los valores de Hash MD5 de los archivos escondidos

Palabras claves encontradas que se asocian al programa / archivo.

El cifrado que utiliza el programa camouflage no permite tener una palabra clave que asocie el uso del producto dentro un archivo sospechoso, sin embargo se puede buscar en diferentes medios por las siguientes palabras para determinar si el sistema contiene una librería, ejecutable ó rastros de su uso:

<http://www.camouflage.freemove.co.uk>

Camouflage

Camou121.exe

Camouflage.exe

CamShell.dll

Detalles forenses

¿Cuál es el nombre del programa usado por Sr. Leszczynski?

Camouflage Versión 1.2.1

<http://www.camouflage.freemove.co.uk>

¿Qué tipo de programa es él?

Es un programa para ocultar un archivo o archivos en otro.

¿Para qué se utiliza?

Ocultar un archivo en otro, apoyado en una técnica de cifrado y añadiéndose al final de un archivo común, esto permite la fuga de información.

¿Cuándo era la vez última que fue utilizado?

Se uso para ocultar archivos en tres archivos de la imagen, el último uso fue en el archivo `Information_Sensitivity_Policy.doc` tiene como última escritura el 04/23/04 02:11:10PM.

Los detalles de la forma de uso del programa y análisis paso a paso se encuentran descritos en los detalles de la examinación.

Identificación del programa

La búsqueda el programa, su instalación y uso están descritos en los detalles de la examinación, se realizaron los cálculos del valor de hash MD5 para los archivos extraídos de los archivos encontrados en la imagen (almacenados en el directorio `camouflage`) y se determinó que el valor de hash MD5 del archivo `"Internal_Lab_Security_Policy.doc"` extraído del archivo del mismo nombre hallado en la imagen es igual al archivo `"Internal_Lab_Security_Policy1.doc"` hallado también en la imagen, lo cual evidencia el uso de la herramienta por el Sr. Robert Leszczynski (ver Imágenes No. 19 y 20)

Implicaciones legales

Administrativamente el Sr. Robert Leszczynski viola la cláusula de confidencialidad, ética y la política aceptable de uso, comunes en todas las empresas hoy en día, dando potestad a Ballard Industries de despedirlo con justa causa y sin perjuicio de indemnización, además debe responder civil y penalmente por los delitos en que incurrió: Al Sr. Robert Leszczynski se le puede juzgar por los delitos que atentan contra el patrimonio y propiedad intelectual en Colombia, la compañía Ballard Industries puede iniciar un proceso ejecutivo y con base en la evidencia encontrada se le puede comprobar la fuga de información hacia la compañía Rift Inc.

Respecto a la compañía Rift Inc., debe responder civil y penalmente por los delitos que incurrió al aceptar y usar la información enviada por el Sr. Robert Leszczynski, se puede iniciar un proceso ejecutivo por competencia desleal y buscar una indemnización por daños y perjuicios ocasionados por la pérdida de órdenes de sus clientes actuales y potenciales, por el uso de los diseños que son propiedad intelectual de Ballard Industries.

A continuación las leyes que rigen en Colombia y que se relacionan con el anterior análisis

Constitución Política de Colombia:

ART. 61.- El Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley.

Contenidos del Código Penal Colombiano:

Artículo 306: El que utilice fraudulentamente nombre comercial, enseña, marca, patente de invención, modelo de utilidad o diseño industrial protegido legalmente o similarmente confundible con uno protegido legalmente, incurrirá en prisión de dos (2) a cuatro (4) años y multa de veinte (20) a dos mil (2000) salarios mínimos legales mensuales vigentes.

En la misma pena incurrirá quien financie, suministre, distribuya, ponga en venta, comercialice, transporte o adquiera con fines comerciales o de intermediación, bienes producidos o distribuidos en las circunstancias previstas en el inciso anterior.

Código de Comercio Colombiano:

ARTÍCULO 76. El perjudicado por actos de competencia desleal tendrá acción para que se le indemnicen los perjuicios causados y se condene en la sentencia al infractor, bajo multas sucesivas hasta de cincuenta mil pesos, convertibles en arresto, a fin de que se abstenga de repetir los actos de competencia desleal.

El juez, antes del traslado de la demanda, decretará de plano las medidas cautelares que estime necesarias, siempre que a la demanda se acompañe prueba plena, aunque sumaria, de la infracción y preste la caución que se le señale para garantizar los perjuicios que con esas medidas pueda causar al demandado o a terceros durante el proceso.

Código Civil Colombiano:

ART 671.- Las producciones del talento o del ingenio son una propiedad de sus autores. Esta especie de propiedad se registrará por leyes especiales

Información adicional

<http://www.fiscalia.gov.co/pag/divulga/Decla02/intelec.htm>

Acciones de la Fiscalía para proteger la propiedad industrial y posibles reformas al Código Penal para mejorar esta protección.

http://www.secretariassenado.gov.co/leyes/C_COMERC.HTM

Código de Comercio Colombiano.

http://www.secretariassenado.gov.co/leyes/L0256_96.HTM#33

LEY 256 DE 1996 (Enero 15) Diario Oficial No. 42.692, de 18 de enero de 1996.

Por la cual se dictan normas sobre competencia desleal

© SANS Institute 2005, Author retains full rights.

Parte 2 - Opción 1: Análisis forense de un sistema

Análisis de un disco duro de un portátil confiscado por un entidad de control en Colombia dentro de un proceso de investigación por narcotráfico y lavado de activos para ser usado como evidencia en el sistema acusatorio Colombiano.

Los hechos, nombres y registros del siguiente análisis han sido modificados por motivos de seguridad y reserva del sumario, sin embargo estos están basados en un caso de la vida real.

Sinopsis de los hechos del caso

En el marco de la operación ACME II se detuvo al presunto jefe del cartel ACME dentro de la diligencia se encontró un portátil que al parecer pertenece al sujeto detenido, el reto es identificar si este es el computador personal del sujeto investigado e identificar el uso que de este hacia (correo electrónico, documentos, programas contables, etc). El objetivo principal es usar el portátil como evidencia dentro del eventual proceso judicial en el nuevo sistema acusatorio Colombiano.

Descripción del sistema

Detalles del computador portátil:

Marca: ACME

Modelo: 1111-a00

Procesador: Pentium 1.5 Ghz

Memoria RAM: 256 Mb.

Disco Duro: 40Gb.

Sistema Operativo: Windows 98b

El computador se encuentra cerrado y aparentemente apagado o en estado de hibernación, no tiene cable de red y en la ubicación donde se realiza el allanamiento no se encuentran equipos activos de red, únicamente se encuentra los conectores de datos de un equipo móvil de comunicación celular.

Hardware

Evidencia # ACME II - 00012

Descripción: Equipo de cómputo portable

Marca: ACME

Modelo: 111-a00

S/N: ABC1234XYZ

Otros: El portátil contiene: 1 Disco Duro Interno (Marca: Sayonara, Modelo: ABC123456D1EF00, S/N: 11A22B3333C4D5EFG67H89J, Capacidad: 40Gb)
1 Unidad interna de DVD-Rom CDWR, 1 Tarjeta de interna de sonido y video, 4 puertos USB, 1 puerto serial, 1 puerto paralelo, 1 salida s-video, 1 salida audio, 1 salida video, 1 tarjeta de red interna, 2 entradas PCMCIA.

Etiqueta # ACME II - 00013

Descripción: Equipo Celular

Marca: Sayonara

Modelo: X123

S/N: 01234567890

ESN: 571333777777

Etiqueta # ACME II - 00014

Descripción: Cable de Datos para Celular

Imagen del medio

El operativo se hace en horas de la madrugada tomando por sorpresa al sujeto que se encontraba dormido, el portátil a analizar se encuentra cerrado (aparentemente apagado), tiene conectada la fuente de poder y reposa sobre una mesa, adicionalmente se encuentra un teléfono celular con los conectores de datos (al parecer el sistema de comunicación personal y del portátil).

Después de labor de fijación de la escena y del equipo de dactiloscopia sobre el portátil, se procede a tomar la imagen maestra del disco duro, para esto se utiliza un equipo de cómputo forense de campo el cual está compuesto por un computador portátil con la versión de EnCase FIM (modelo de inteligencia en campo – de uso exclusivo del gobierno) y un dispositivo de hardware de protección de escritura (FastBloc FE). Se retira el disco duro del portátil y se procede a la adquisición de la imagen maestra, una vez adquirida se toman dos imágenes para uso de la investigación (una imagen será puesta a disposición del investigador y la otra será un respaldo en caso de pérdida o daño). La evidencia real y la digital (imágenes) se les asignan una forma (cadena de custodia) para su manejo (ver secuencia en Imágenes No. 23, 24, 25 y 26)

El resultado de este proceso es la obtención de una copia bit a bit de la evidencia original en un archivo de formato de Imagen de EnCase, paralelamente a la labor de adquisición se realiza el cómputo de los valores de hash MD5 para el sistema de archivos con el de la imagen en su totalidad y la verificación de las firmas de los archivos.

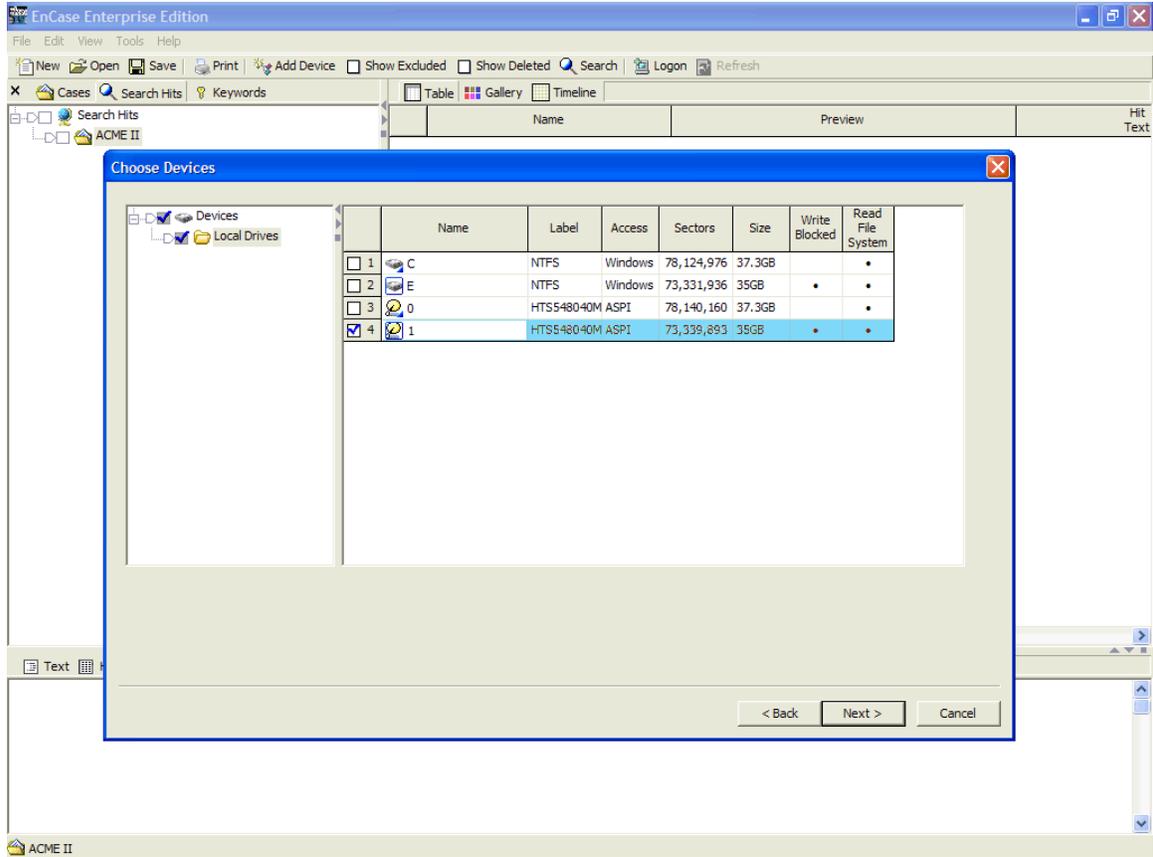
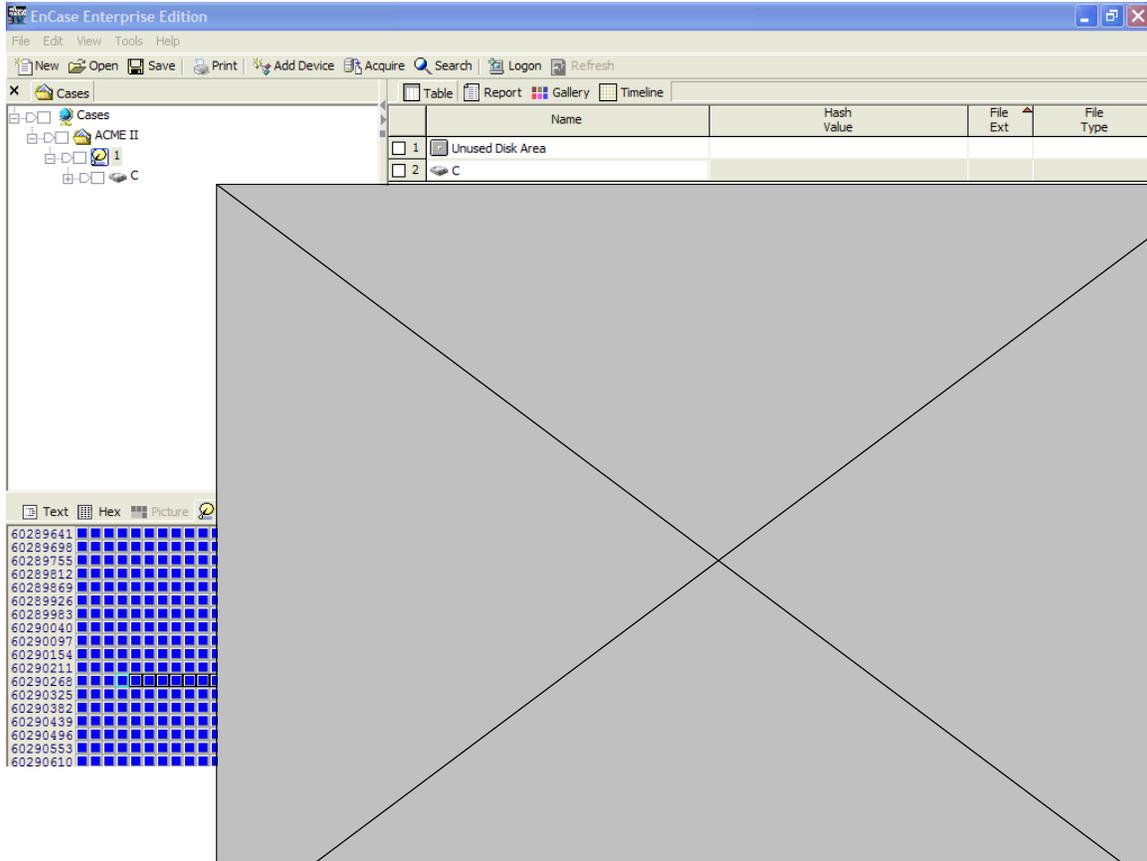


Imagen No. 23 Detalle del procedimiento de adquisición de evidencia.

En el área resaltada se puede visualizar el disco duro interno del portátil es reconocido por la estación forense y se encuentra protegido contra escritura por el dispositivo de hardware FastBloc FE.

© SANS Institute



© SANS Institute 2005,

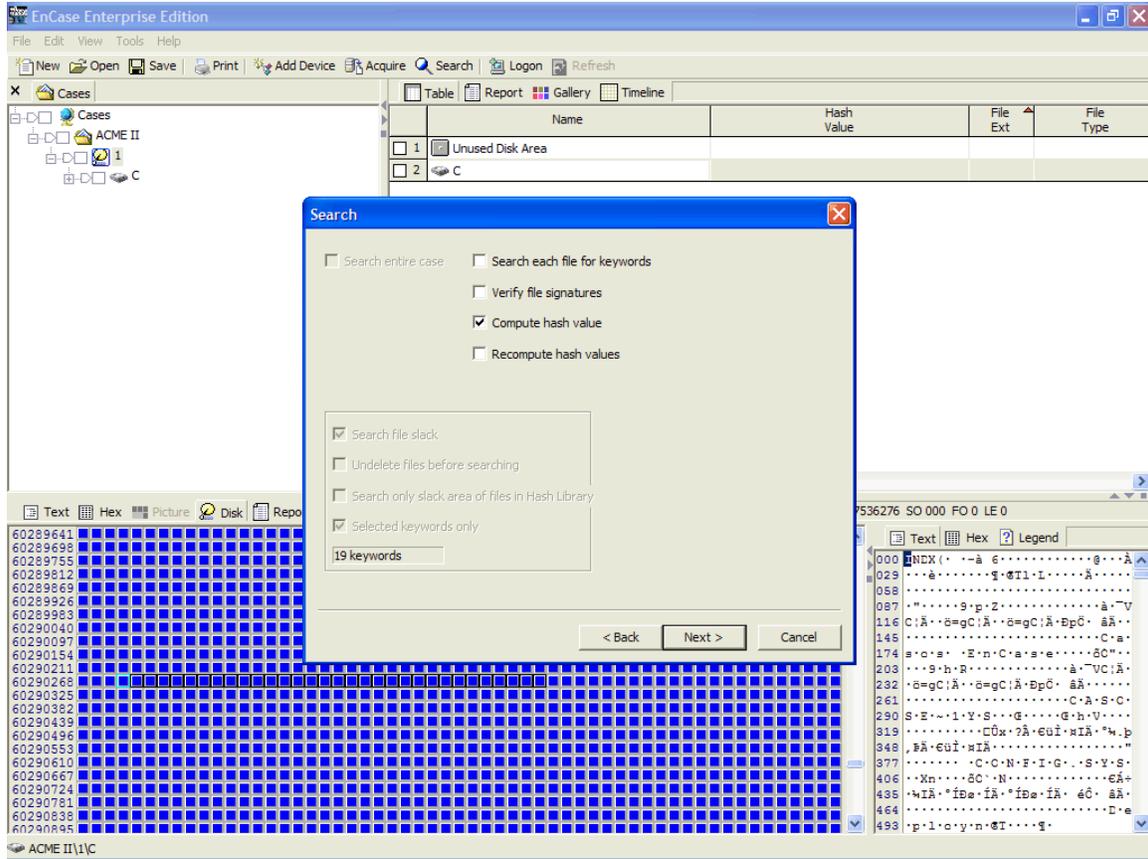


Imagen No. 25 Detalle del procedimiento de adquisición de evidencia.

Menú de opciones de búsqueda, en el mismo proceso de adquisición se aprovecha para realizar la búsqueda por palabras clave (previamente ingresadas), verificación de firmas de los archivos y el cómputo ó recómputo de los valores de hash

© SANS Institute

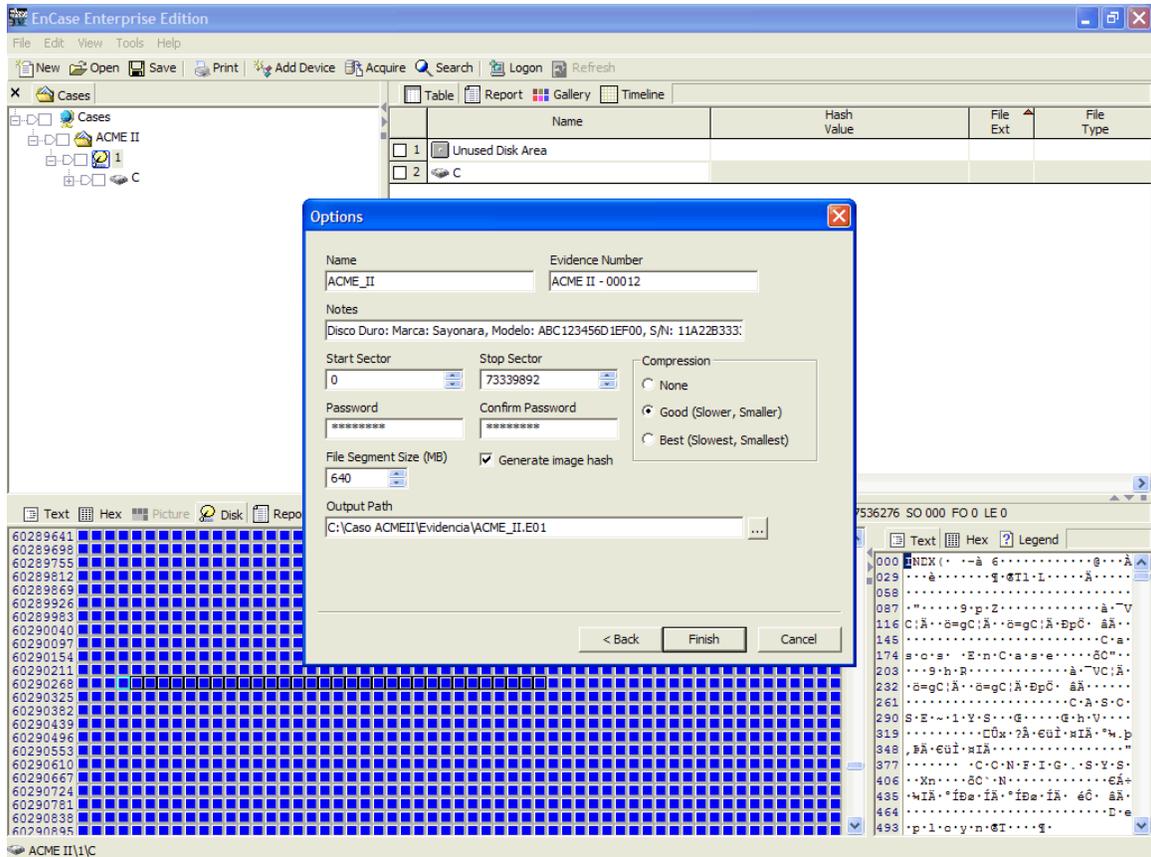


Imagen No. 26 Detalle del procedimiento de adquisición de evidencia.

Finalmente las opciones de nombre, número de evidencia, notas adicionales, asignación de clave para el uso de la imagen, el tipo de compresión, la segmentación de archivos de la evidencia (lo cual permite almacenar la imagen en cd-rom) y la ruta donde se almacenará la imagen.

A continuación se describe la metodología utilizada en la adquisición, análisis y presentación de la evidencia digital, esta metodología es el resultado de un documento liderado por Edwin Lugo del Servicio Secreto de Estados Unidos y que gracias al aporte y comentarios de profesionales de la seguridad de la información de habla hispana, entre los que me encuentro, ha servido como guía en los diferentes entes de control de los países de habla hispana.

Puntos Básicos:

1. Proteger la prueba original
2. En ocasiones, existen circunstancias especiales en las cuales es necesario acceder a la información directamente en el medio o evidencia original. En esos casos, es importante verificar si la persona que accede a la información está debidamente capacitada para hacerlo y si cuenta con la autorización del coordinador de la posible acción judicial. En el momento en que se accede a la prueba original, es importante contar

con la presencia de un testigo, de preferencia alguien que no sea parte de la investigación.

- Ejemplo I: Un sitio Web que contiene información médica de vital importancia y cuyo acceso inmediato es indispensable ha sido objeto de piratería. Es necesario decidir si conviene apagar y desconectar temporalmente el servidor principal, con el objeto de recuperar la información, lo cual exige autorización por parte de una autoridad judicial.
 - Ejemplo II: Una bomba está programada para estallar y la información para desactivarla se encuentra en un computador específico. Si bien es un tema difícil de entender y dadas las circunstancias especiales, es más importante en ese momento salvar vidas que el posterior resultado de la investigación. Con este ejemplo pretendemos demostrar un caso en que “las circunstancias exigen” una respuesta. Es muy sencillo: “si espera, habrá muertos” y, por lo tanto, es indispensable acceder al computador de inmediato.
3. Conserve la cadena de custodia de la prueba y simultáneamente documente quién tuvo acceso al medio / prueba original.
 4. Es importante mantener la continuidad del oficial a cargo de la investigación, al igual que la de los peritos responsables del análisis. Nota: En lo posible, trate de evitar que el investigador principal sea el mismo técnico analista. Independientemente de lo eficiente que parezca, pueden presentarse conflictos de interés, como en el caso del investigador que, debido a la presión por resolver el caso, se concentra demasiado en un solo aspecto del análisis y pasa por alto una evidencia clave.
 5. Confirme lo que encuentre. Cuando se utiliza un software diseñado específicamente para el análisis de evidencia, es importante establecer como norma la utilización rutinaria de un software diferente, con el fin de confirmar si se obtienen los mismos resultados / pruebas.
 6. Por naturaleza, la evidencia electrónica es frágil. Protéjala y confirme si el proceso utilizado por usted ha sido empleado en ocasiones anteriores con buenos resultados. A veces es bueno practicar con una copia del dispositivo cuestionado.

Preparación previa:

Verifique la estabilidad del lugar de los hechos. Usted no debe ser el primero en entrar. La unidad de allanamiento debe entrar primero, acordonar el lugar y llevar a los indiciados a otro lugar, lejos de los equipos (inclusive de los celulares, agendas electrónicas, beepers y computadores)

Es importante asignar a la persona indicada para cada tarea. Asegúrese de que los investigadores se encuentren en el lugar que les corresponde. En primer lugar, averigüe cuál de los miembros del grupo es el mejor en los siguientes campos:

- Recaudo de evidencia
- Guantes (protección personal)
- Documentación / Cadena de custodia
- Rotulado / numeración de evidencia
- Croquis / dibujos de los sistemas y su ubicación
- Fotografía (incluir fotos de la entrada y la salida del grupo)
- Entrevista (recuperación de claves de acceso)
- Experiencia con sistemas operativos específicos
- Calibración y cuidado del equipo
- Embalaje de evidencia (la energía estática puede destruir la investigación)
- Organización de todo lo anterior (por lo general, se presentan deficiencias en este aspecto, lo cual obstaculiza la investigación desde el comienzo)

Practique lo que hace y la forma de hacerlo. Asegúrese de conocer muy bien el equipo que va a emplear, tanto en el laboratorio, como en el lugar de los hechos. También es esencial conocer a los miembros de la unidad que van con usted. Aunque estoy plenamente consciente de que rara vez contamos con varios investigadores para la investigación de delitos electrónicos, es importante practicar con ellos tanto como sea posible. Con anterioridad al allanamiento, reúna la mayor cantidad de información de inteligencia posible sobre el delito, los indiciados y el sitio en cuestión.

Llegada al lugar de los hechos:

- Asuma formalmente la responsabilidad del lugar de los hechos. Si usted es parte del grupo investigativo original, excluya a todas las personas que no van a participar en la investigación electrónica.
- Es importante documentar, entrevistar y dar cuenta de todos los indiciados y testigos (no olvide los dispositivos electrónicos que se encuentren en su poder).
- Cuando sea posible entrevistar al (los) indiciado(s), deje que el miembro más calificado del grupo lleve a cabo la entrevista en un sitio alejado del lugar de los hechos (interróguelo acerca de las claves de acceso y los códigos).
- Es importante dejar encendidos los computadores que estén encendidos y apagados los que estén apagados; verifique si, de hecho, los equipos están apagados y si se encuentran en el modo de protector de pantalla o “dormidos”.
- Tenga en cuenta que muchos dispositivos se activan solamente con abrir la tapa.
- Fotografías del lugar de los hechos, de la entrada, de la ubicación del equipo, de las pantallas de computador y de los puntos de acceso del equipo (líneas telefónicas, líneas de transmisión de datos).
- Dibuje un croquis del lugar de los hechos. A veces no es claro si el equipo está conectado o desconectado.

- Verifique el procedimiento a seguir para apagar los equipos que están encendidos. Algunos computadores puede corromper o cambiar los datos si no se apagan correctamente (UNIX, LINUX).
- Una vez determine el equipo que se va a incautar para efectos de análisis, éste debe ser rotulado. Es vital tomar fotografías y adjuntarlas o tenerlas a mano para armar el equipo nuevamente, en caso necesario.
- Tome el software / manuales correspondientes al computador incautado o al delito.
- Documente lo que sucede en el lugar de los hechos, pues este registro va a ser de vital importancia cuando surjan interrogantes sobre las condiciones en las cuales se halló el lugar o el equipo.
- En algunos países, la ley obliga a los investigadores a dejar una lista de los objetos incautados en el lugar de los hechos, con el propietario o con la persona a cargo del lugar. En ese caso, se debe dejar una copia y no el original.

Tenga en cuenta el entorno al cual va a llevar el equipo que se incautó y confirme si va a transportar los computadores incautados en el baúl del vehículo de policía, sin ninguna protección (consideraciones ambientales) (tenga en cuenta que las unidades de radio de la mayoría de los vehículos de policía se encuentran en el baúl y emiten un volumen significativo de señales magnéticas, cuando el radio está en uso) o si es mejor llevarlo en el asiento trasero y asegurarlo con una cinta, con el objeto de protegerlo durante el traslado.

La siguiente es una lista de los elementos que deben ser incautados:

- CPU
- Monitor
- Teclado
- Ratón
- Cables
- Módems
- Puertos paralelos USB
- Unidades adicionales de disco duro
- Cámaras digitales
- Disquetes
- Unidades de almacenamiento "Jazz", "Iomega"
- CD – ROM
- Copias de Seguridad (backup)
- Equipo de redes inalámbricas
- DVD
- Unidad de memoria extraíble (ZIP)
- Tarjetas PCMCIA
- Barras / tarjetas de memoria

Cuando vuelva al laboratorio, tenga en cuenta que el Internet ofrece una variedad enorme de información y muy posiblemente tenga un sitio Web dedicado a una parte específica del equipo o incluso un manual de

instrucciones.

Los siguientes son algunos elementos que se suelen pasar por alto:

- Beepers
- Teléfonos celulares
- Fax
- Contestadores automáticos especiales
- Equipo de conexión a Internet
- Equipo de conexión inalámbrica (busque los elementos que podrían estar conectados al equipo inalámbrico)
- PDA (agendas electrónicas / asistentes personales de datos)
- Tarjetas multi media

Preservación de la cadena de custodia:

El documento de cadena de custodia constituye el eslabón entre el momento en que usted entra al lugar de los hechos y el momento en que se destina la evidencia. Además, es tan importante como el informe final... En otras palabras, el informe final carece de valor si en algún momento se rompe la cadena de custodia. El registro de la custodia refleja las personas que tuvieron acceso a la evidencia, cuándo y por qué, y en qué momento se devolvió. Todos los actos relacionados con la evidencia original “deben estar documentados” o de lo contrario el procedimiento investigativo se pondrá en tela de juicio.

Búsqueda de evidencia:

Después de allanar el lugar de los hechos y de tener en cuenta todo lo anterior, viene la etapa de “Recuperación de Evidencia”. En este momento, vale la pena mencionar la carga que representa para el investigador responsable de la investigación el hecho de que sus superiores estén ansiosos por obtener resultados. No obstante, es importante no dejarse presionar por la premura del tiempo, pues a veces se encuentra información investigativa y otras veces no. Lo peor que puede suceder en esas circunstancias cruciales es hacer conjeturas.

Clonación de la evidencia física:

Es importante contar con la capacidad de “copiar exactamente” la evidencia cuestionada. Una vez clonada, puede estar tranquilo, pues no está manipulando la evidencia original y por consiguiente tendrá mayor flexibilidad que si trabaja con ella.

Determine el método que va a utilizar para recuperar la evidencia:

Hoy en día existen en el mercado una serie de paquetes de software diseñados para revisar evidencia, los cuales incluyen todo lo necesario, menos el “Experto Certificado”. Tenga en cuenta que el software le da al usuario la sensación de que está en capacidad de hacer cosas que solamente debería manejar el “experto”. Es peligroso tratar de revisar la evidencia original con un software que desconoce.

Esfuerzo analítico:

En la mayoría de los casos, una vez protegida (clonada) la evidencia, su trabajo termina, hasta el momento en que el especialista le indique qué tipo de evidencia se busca. Posiblemente le pidan clonar la evidencia y reconstruir el entorno en el cual se encontró la evidencia original. Esto significa que si la evidencia es un disco duro, se debe clonar la unidad original de disco duro y colocarla en un computador independiente, que no esté en red. Posteriormente, se debe poner a funcionar el disco y protegerlo, con el fin de que no se pueda escribir encima. En ese momento, el especialista a cargo del análisis puede hacer su trabajo, es decir, buscar evidencia específica. Trate de no involucrarse en los procedimientos investigativos en curso. Esta puede ser una medida poco inteligente, especialmente si, a pesar del esfuerzo, “no se encuentra evidencia en el equipo incautado”.

Mantenga un proceso consistente de análisis y concéntrese en el cumplimiento de los procedimientos estandarizados. Por ejemplo, en alguna parte de su informe, demuestre que siguió los pasos normales, como confirmar que no se pueda escribir sobre la evidencia o que buscó archivos borrados o programas ocultos o particiones.

Informe final:

La presentación de un informe conciso y específico depende de la información solicitada al investigador de delitos informáticos y de la forma como se admita la información en el proceso judicial.

Elementos básicos:

- Número del caso
- Fecha del análisis
- Persona que solicita el análisis
- Persona que realiza el análisis
- Información de contacto del analista
- Elementos presentados para análisis
- Desglose de los elementos incautados
- Equipo utilizado para el análisis
- Software asociado con el hecho punible
- Procesos y resultados
- Firma interna que autoriza la divulgación de información

Todos los departamentos de policía tienen sus propios requisitos en lo que se refiere a la forma en que se deben presentar los informes dentro del sistema y del proceso judicial. Absténgase de expresar opiniones personales en su informe y concéntrese únicamente en lo que descubrió.

Personas autorizadas para acceder a sus hallazgos: (divulgación de evidencia e informe final)

Este elemento es de vital importancia para la judicialización de la evidencia. Es esencial controlar el acceso a su informe, de acuerdo con los requisitos y reglamentos de su institución. Además, la divulgación debe ser controlada por el representante judicial del tribunal correspondiente.

Conservación de la evidencia:

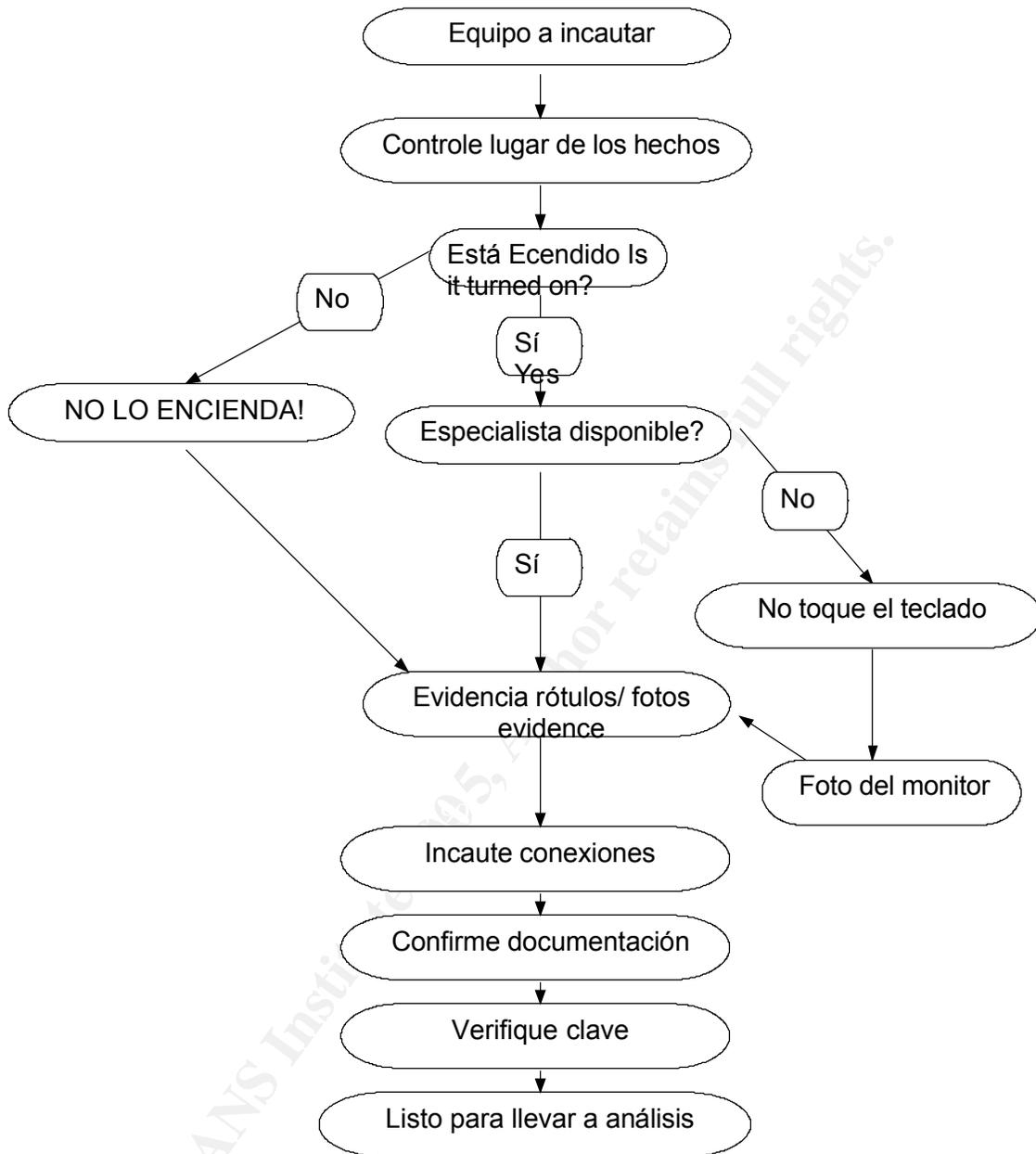
Toda evidencia original se debe guardar en un lugar seguro y protegido del medio ambiente (sin cambios drásticos de temperatura y sin la posibilidad de picos eléctricos). Las instalaciones de almacenamiento, el lugar y el acceso deben formar parte de la información documentada en la cadena de custodia.

Calibración del equipo:

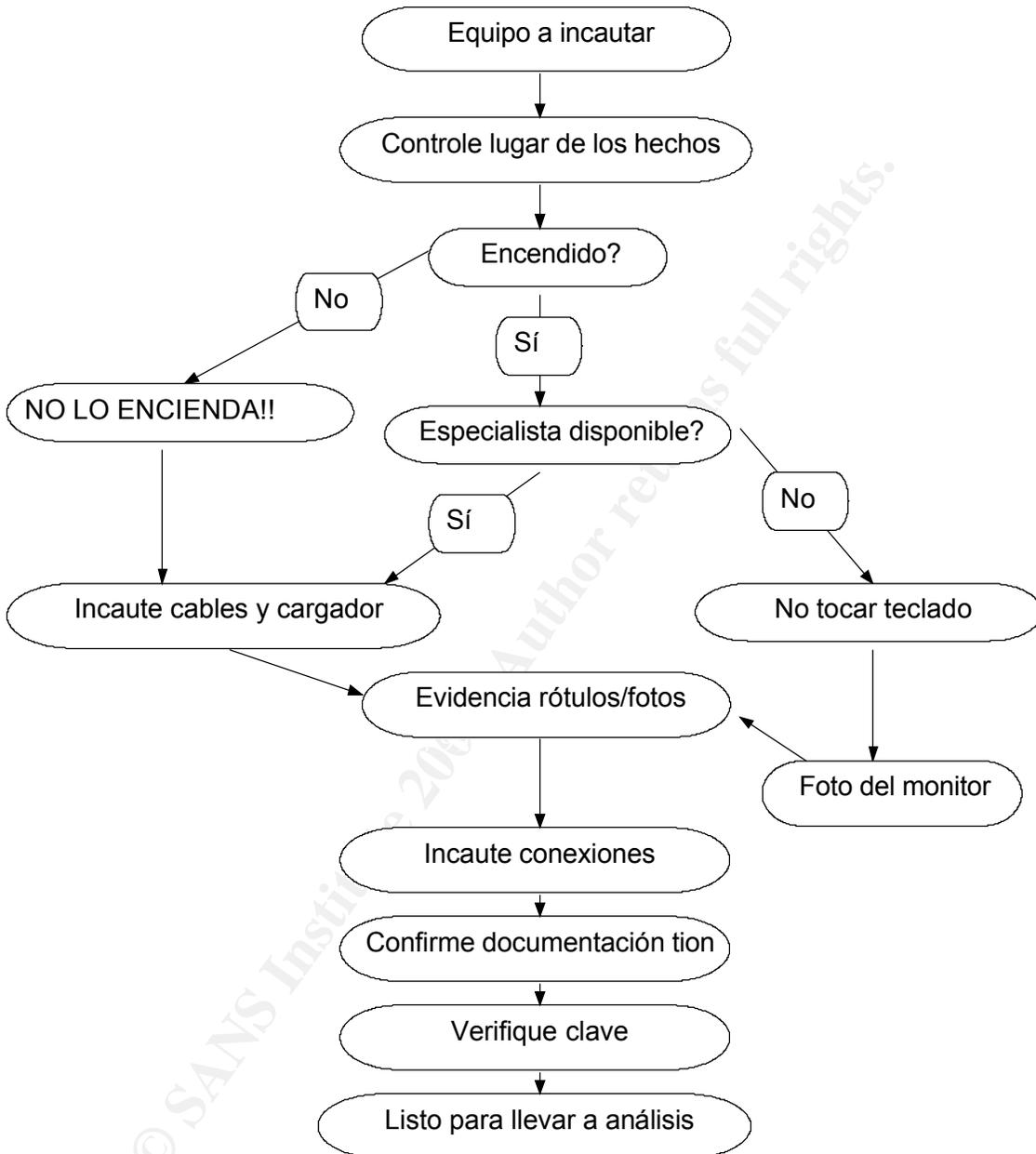
Cuando esté listo para volver a empezar, se debe preparar el equipo para la próxima vez que lo necesite. No tome a la ligera el requisito de “limpiar” el equipo y sus herramientas. Es un grave error suponer que tendrá oportunidad de prepararlo más adelante. La preparación previa y contar con todo lo necesario es señal de profesionalismo.

Diagrama de Flujo para la Incautación de evidencia electrónica

© SANS Institute 2005, Author retains full rights.



© SANS Institute 2005. Author retains full rights.

Diagrama de Flujo para la Incautación de Agendas Electrónicas / Celulares / Beepers***Análisis de los medios del sistema***

Gracias a la funcionalidad de emulación de disco de EnCase y usando el programa VMWare Workstation Versión 4.5.2 se emuló el hardware para poder visualizar el estado real de la máquina (apagada o en hibernación) y contar con

la capacidad de visualizar e interactuar con lo que sería la evidencia real, claro está sin poner en riesgo tanto la evidencia real como las imágenes tomadas.

Se ejecutan los scripts del programa EnCase para agilizar los proceso de búsqueda.

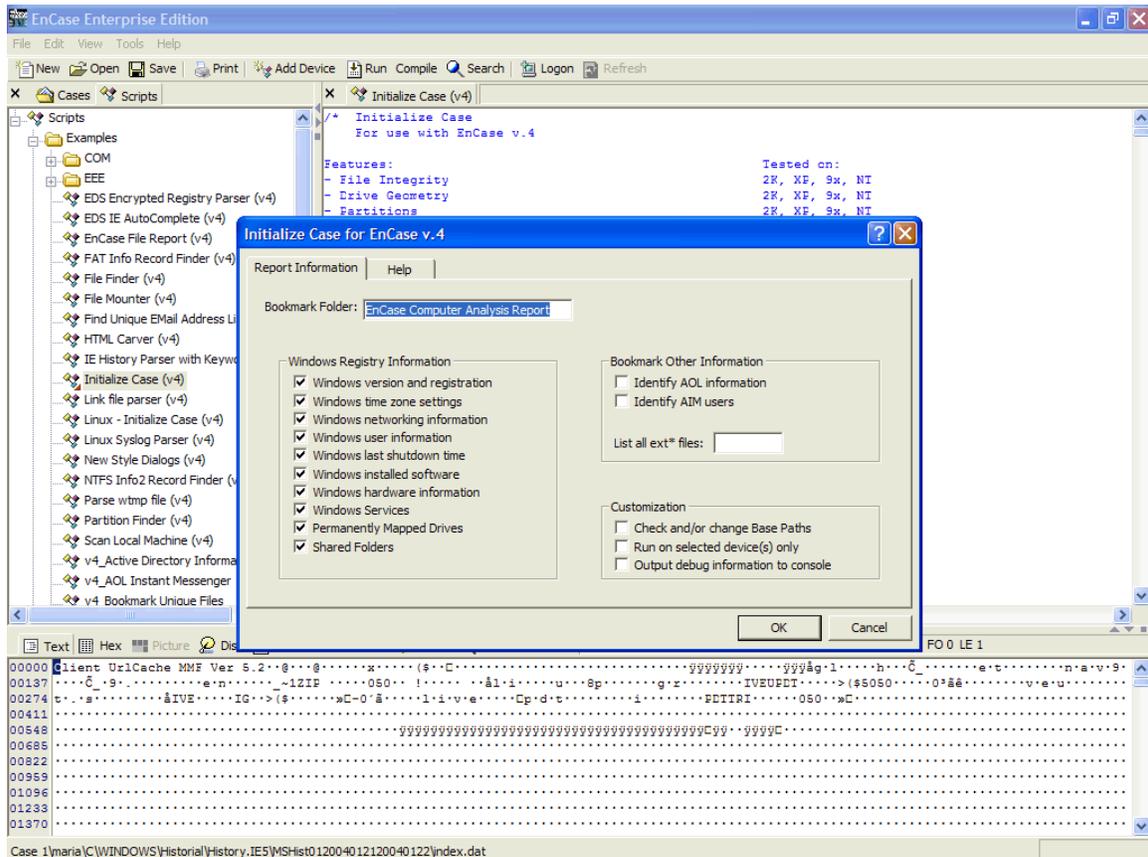


Imagen 27. Ejecución del script de inicialización del caso.

El resultado es un informe donde aparecerá los detalles del sistema operativo, configuración de zona horaria, configuración de red, información de los usuarios del sistema, la fecha y hora del último apagado, información sobre el hardware y software, servicios del sistema operativo, recursos de red y recursos compartidos. Debido a la naturaleza del caso solo se presentaran algunos pantallas de los resultados obtenidos que no comprometen la investigación y que han sido autorizados para su divulgación por el investigador principal.

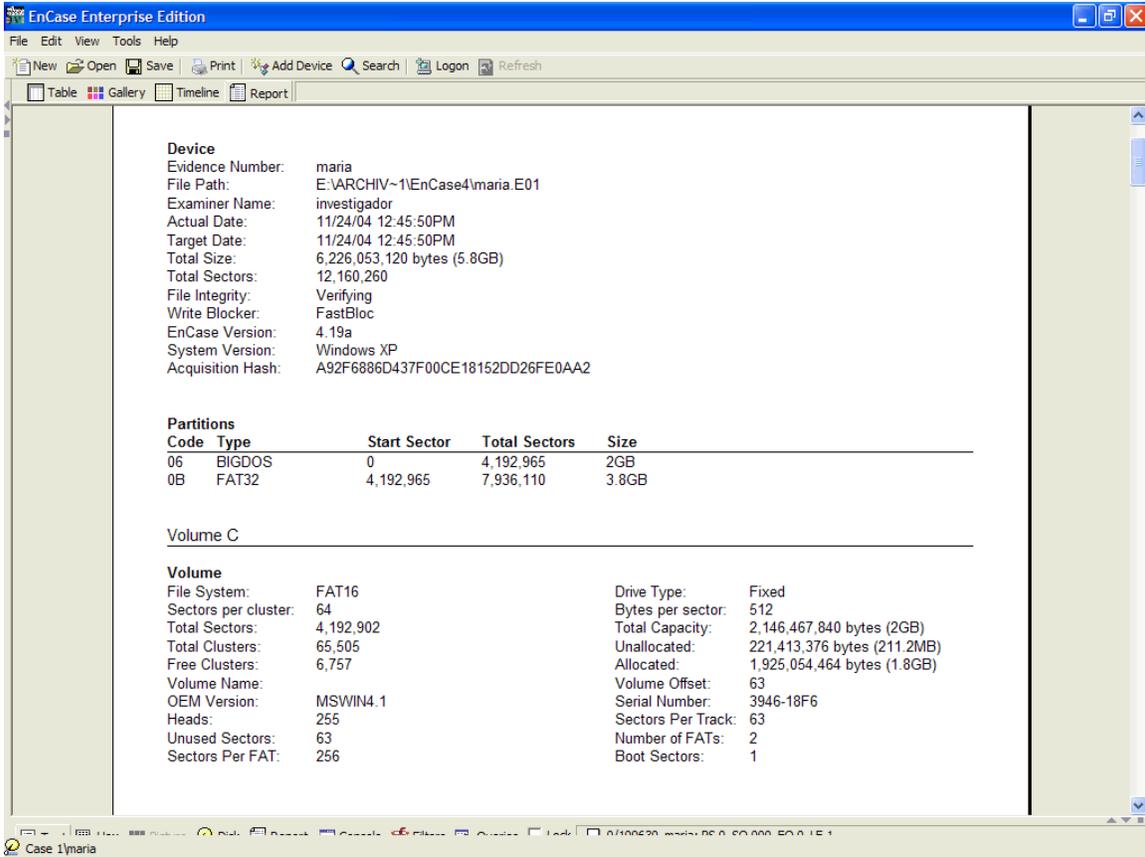


Imagen 28. Resultados del script de inicialización del caso.

Se encuentra en este informe el valor de hash de la adquisición, detalles del programa que tomo la imagen, detalles de la particiones del disco y el detalle del volumen C.

© SANS Institute

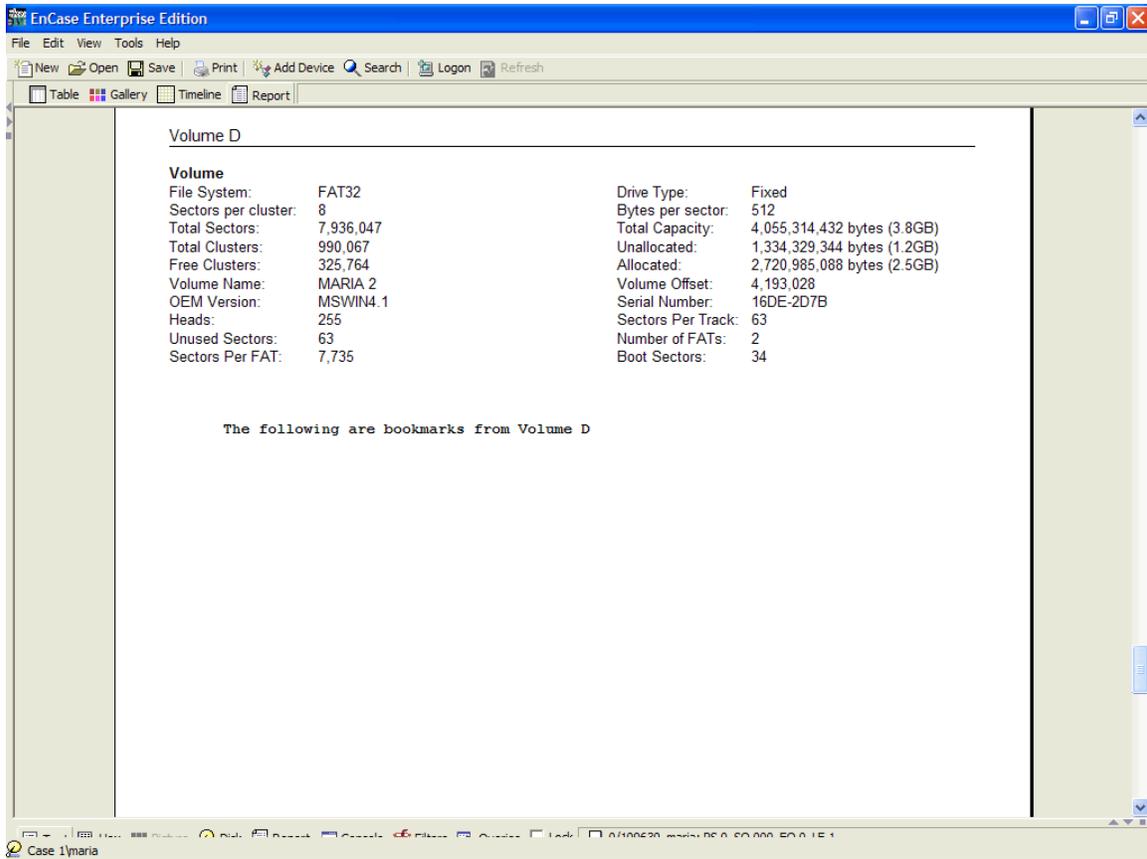


Imagen 29. Resultados del script de inicialización del caso.

Se encuentra en este informe el detalle del volumen D.

© SANS Institute 2005

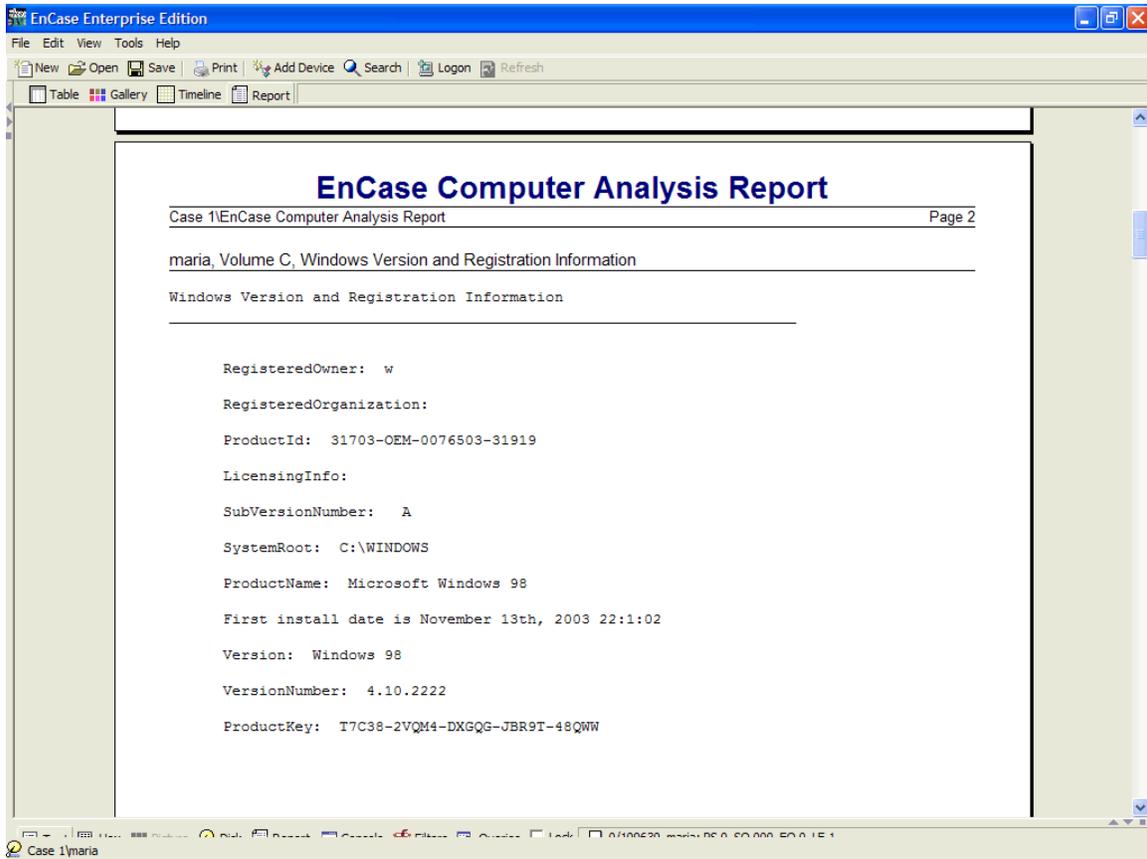


Imagen 30. Resultados del script de inicialización del caso.

Se encuentra en este informe los detalles del sistema operativo y registro.

© SANS Institute 2005

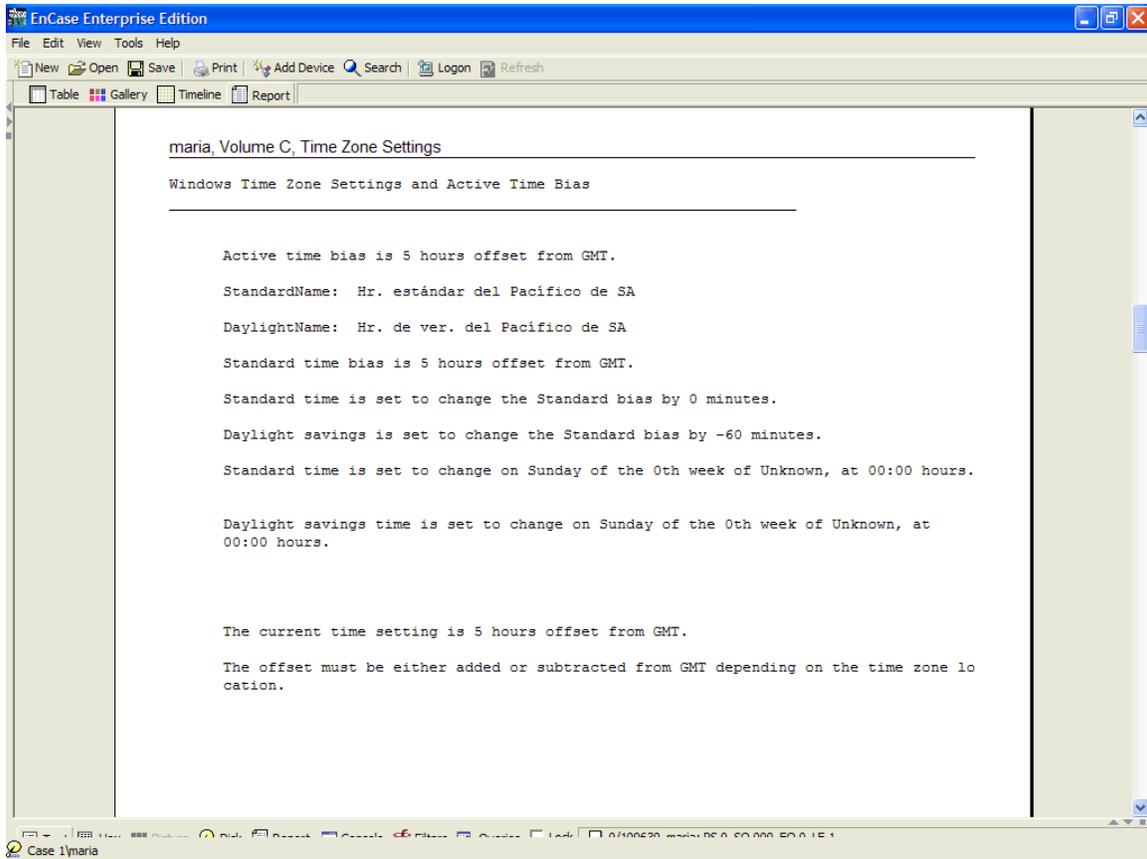


Imagen 31. Resultados del script de inicialización del caso.

Se encuentra en este informe el detalle de la configuración de la zona horaria.

© SANS Institute 2005

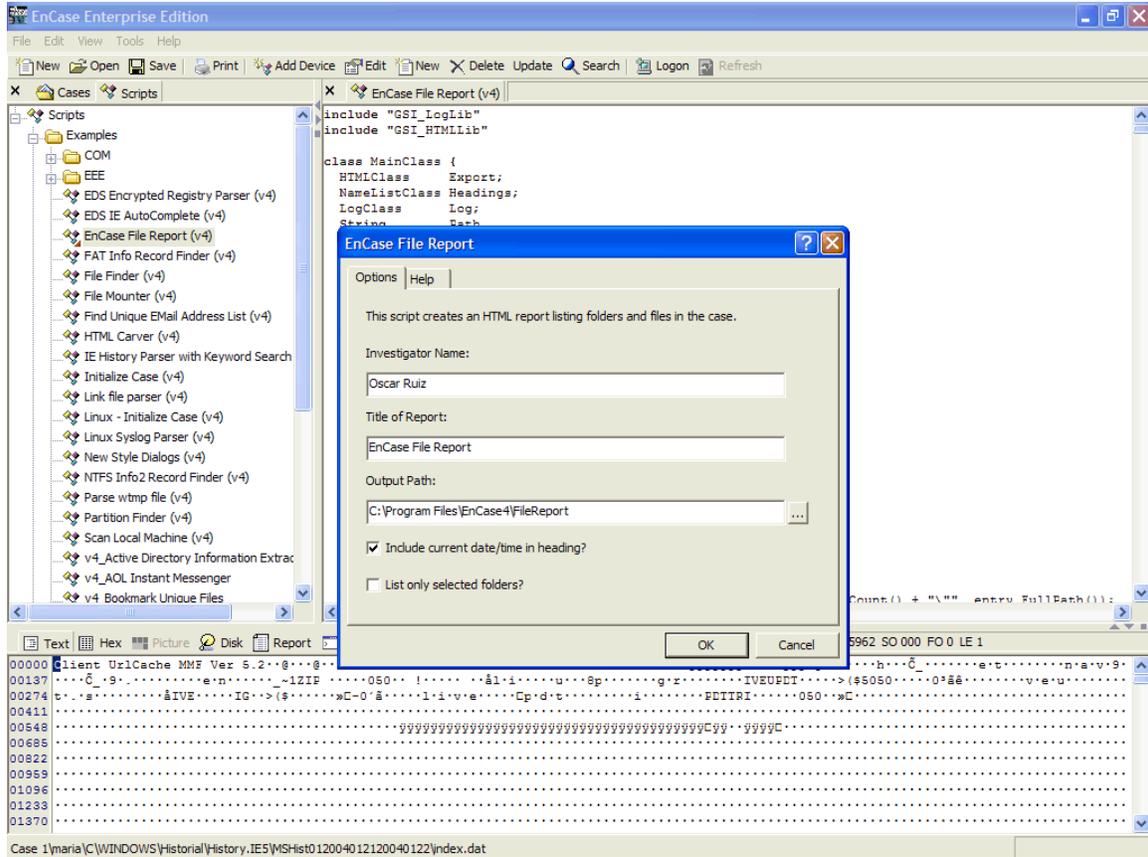


Imagen 28. Ejecución del script que realiza el reporte de los archivos del sistema.

Por consideraciones de seguridad y reserva del sumario, no se presentan los resultados que son el reporte detallado de los archivos del sistema.

© SANS Institute 2005

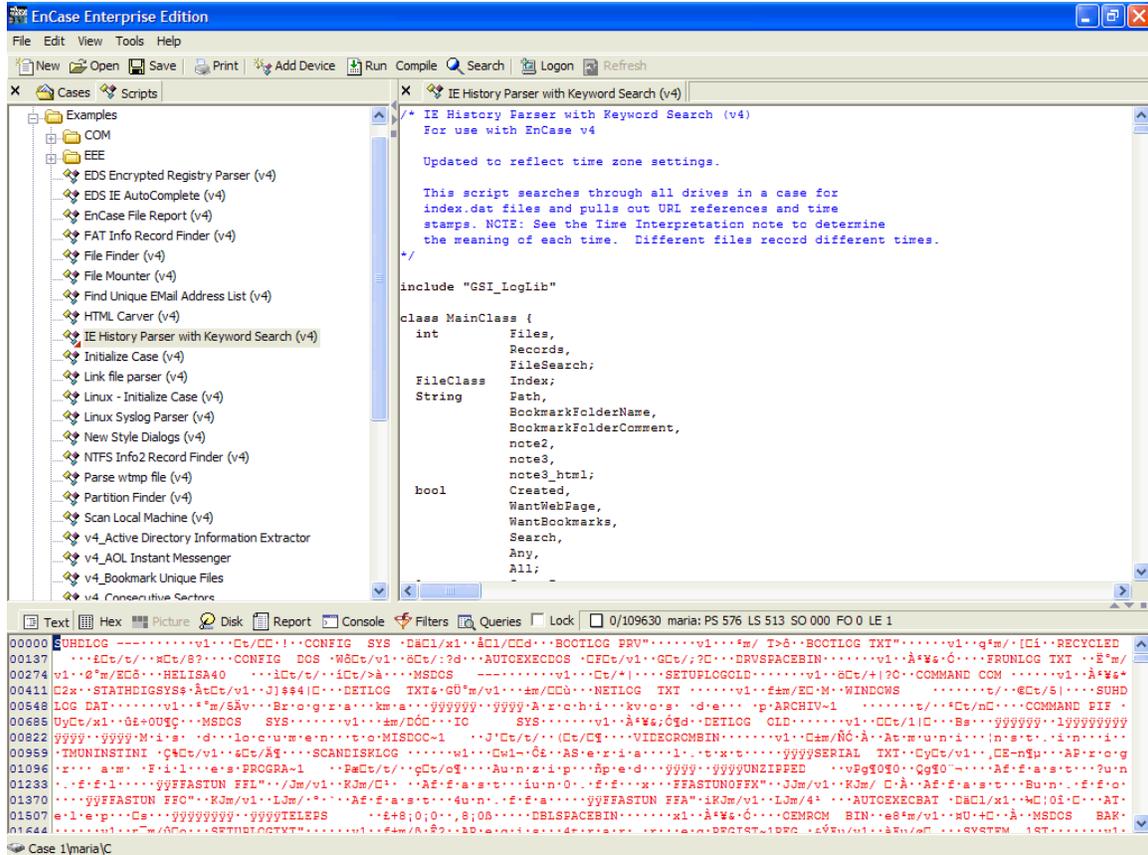


Imagen 29. Ejecución del script que realiza el reporte del historial de uso del Internet Explorer con opción de búsqueda por palabra clave.

Este script permite buscar en los archivos .dat el historial de uso del programa de navegación Internet Explorer, allí quedan registradas las URLs ingresadas (aún cuando hayan borrado el historial y el caché de navegación). Para este caso ayudó a la investigación aportando cronológicamente los hábitos de uso del sujeto investigado, permitiendo encontrar su correo privado de comunicación, páginas a las que visitaba frecuentemente, etc. estos indicios permiten realizar una búsqueda exhaustiva dentro de los archivos temporales de internet (actuales y eliminados) y encontrar la información de los correos intercambiados con diferentes tipos de individuos, se pudo determinar el uso correo tipo web y el uso del programa "Outlook Express", se encontró información de correos recibidos y enviados (aún cuando en el correo web no estaba habilitada la opción de guardar el mensaje)

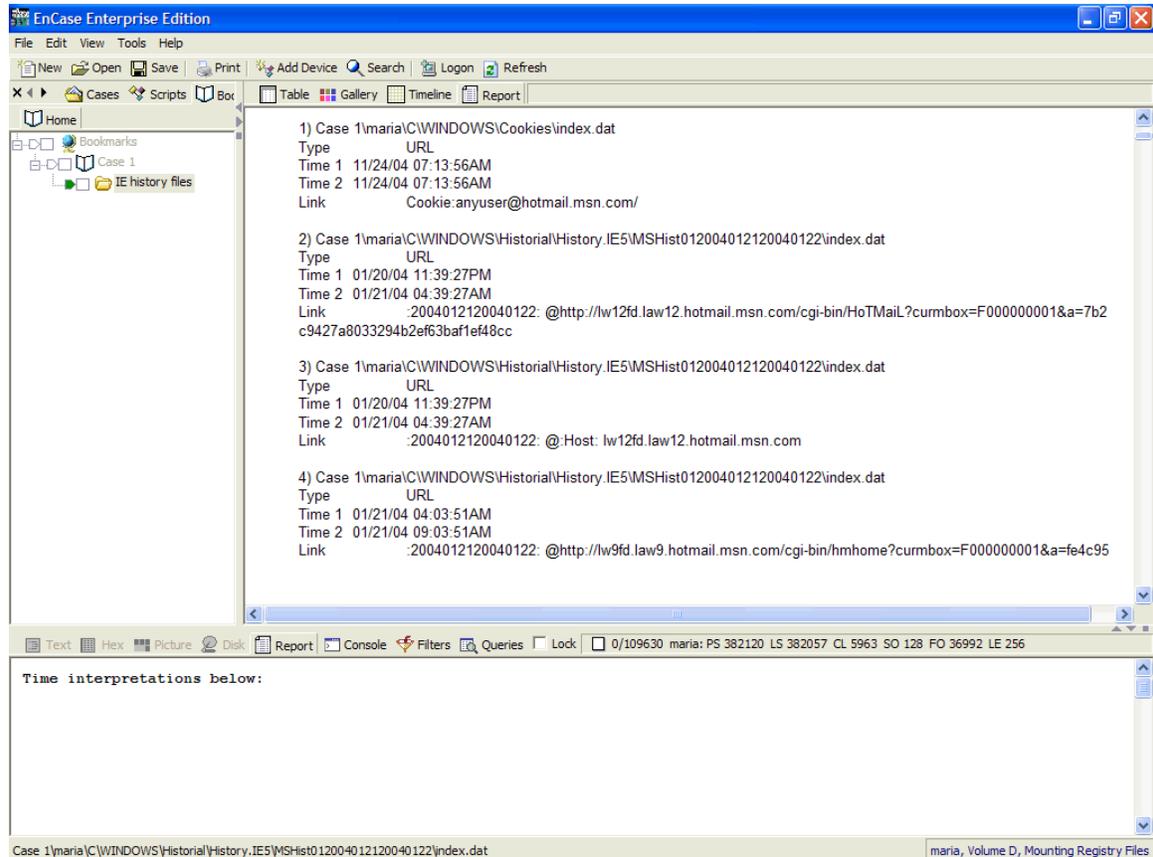


Imagen 30. Resultados del script que realiza el reporte del historial de uso del Internet Explorer con opción de búsqueda por palabra clave.

Por consideraciones de seguridad y reserva del sumario, solo se presentan algunos los resultados que son parte del el reporte detallado del historial de uso del Internet Explorer con la opción de búsqueda con la palabra clave: "Hotmail".

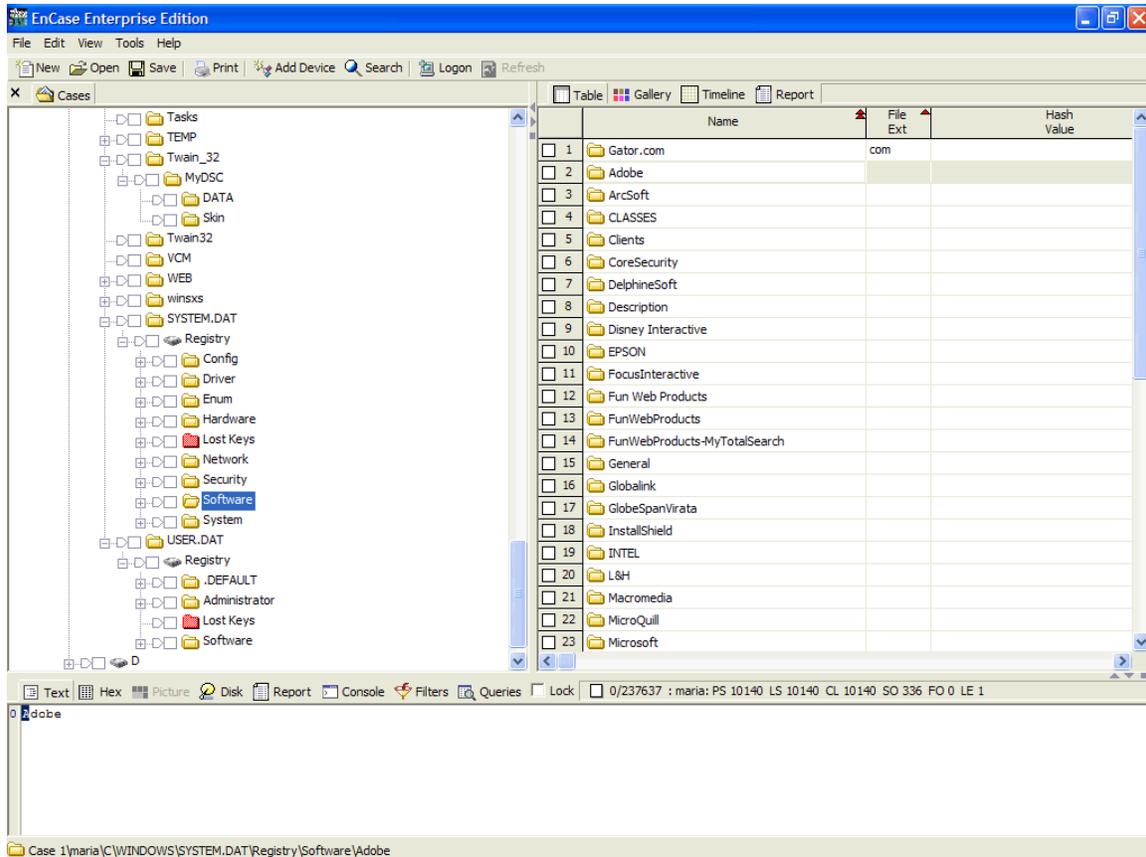


Imagen No. 31 Detalle del registro del sistema y del usuario.

Se utiliza una la funcionalidad de EnCase para montar y visualizar los archivos de registro System.dat y User.dat

Finalmente a continuación se describe la metodología utilizada para la investigación, esta se denomina “Diario de investigación científica”, cuyo concepto es registrar el proceso de investigación o los pasos tomados durante la investigación de la evidencia y el propósito es aplicar este método de investigación como herramienta para resolver el problema, esta metodología es el resultado de un documento liderado por Edwin Lugo del Servicio Secreto de Estados Unidos y que gracias al aporte y comentarios de profesionales de la seguridad de la información de habla hispana, entre los que me encuentro, ha servido como guía en los diferentes entes de control de las países de habla hispana.

- Escribir en el diario o registrar la información.
- Discutir y registrar el problema bajo investigación o preguntar qué se esta investigando.
- Iniciar la discusión con el objeto de que los investigadores planteen sus preguntas sobre el problema. Solicitar a los investigadores que registren sus preguntas.

- Revisar las diferentes fuentes de información a disposición de los investigadores para adelantar la investigación y monitoreo, en desarrollo de una lluvia de ideas y proyectar la evidencia potencial que contribuirá a aclarar las preguntas registradas.
- La tarea del investigador es animarlos a registrar las posibles hipótesis.
- Preparar un área de trabajo, seleccionar el material y adelantar exámenes. Además, recordarles que registren los procedimientos y resultados de su investigación en el cuestionario o en el informe de la investigación.
- Reunirse con los investigadores para analizar la información y las conclusiones y dar retroalimentación e instrucciones, cuando sea necesario. Pedir a los investigadores que registren sus conclusiones en el cuestionario o en el informe de la investigación.
- Retomar el proceso investigativo, estimulando la evaluación del proceso que se siguió para resolver el problema/ buscando otro método.

Formato modelo del proceso de investigación:

Proceso de Investigación	Escriba sus respuestas
Problema Identificar el problema?	
Pregunta Cuál es la Pregunta?	
Investigación Investigar lo suficiente para obtener una buena pregunta	
Hipótesis (Que cree que pasó?)	
Procedimiento Cual será su metodología?	
Materiales Qué necesita?	
Resultados Qué pasó?	
Conclusión Qué indican los datos?	

Reflexión Que hará diferente la próxima vez?	
--	--

© SANS Institute 2005, Author retains full rights.

Análisis cronológico

El sistema operativo fue instalado el 13 de Noviembre de 2003 a las 22:01:02 (ver detalles en Imagen No. 30)

Por consideraciones de seguridad y reserva del sumario, no se presentan los resultados que son el reporte detallado de los archivos del sistema.

Recuperación de archivos eliminados

Utilizando el programa EnCase se procedió a recuperar total o parcialmente los archivos suprimidos del portátil, se identificaron documentos de Word, Excel, pdf, texto plano, entre otros.

Por consideraciones de seguridad y reserva del sumario, solo se presentan algunos de los archivos eliminados.

	Name	File Ext	File Created	Hash Value	Description	File Type	Last Written
1905	0002819062003.txt	txt	06/24/03 12:22:48PM	89932960e53619cf7d89df5955f27aad	File, Deleted, Archive	Text	06/24/03 12:22:48PM
1906	0002829062001.txt	txt	08/06/01 03:25:08PM	5bced9f67e79d2a3fe0aefef30dddffd7	File, Deleted, Archive	Text	08/06/01 03:25:08PM
1907	0002830052002.txt	txt	06/05/02 10:22:54AM	ff5f584fecc7ee037293c09a347362d4	File, Deleted, Archive	Text	06/05/02 10:22:54AM
1908	0002928062002.txt	txt	07/31/02 10:07:40AM	ab74646559f44f7e891e6dc955ecc139	File, Deleted, Archive	Text	07/31/02 10:07:40AM
1909	0002929062001.txt	txt	08/06/01 03:25:08PM	ef7a1922097ffa6e988c544a47d33629	File, Deleted, Archive	Text	08/06/01 03:25:08PM
1910	0003028062002.txt	txt	07/31/02 10:07:34AM	11a0e33c9afc2b54b3829c5af224db07	File, Deleted, Archive	Text	07/31/02 10:07:34AM
1911	0003029062001.txt	txt	08/06/01 03:25:08PM	da23620139a273a6b04ea7a5c6c69100	File, Deleted, Archive	Text	08/06/01 03:25:08PM
1912	000309032000.txt	txt	09/24/01 09:16:50AM	1ccc1953deb0673db1e6668c3d3af01d	File, Deleted, Archive	Text	09/24/01 09:16:50AM
1913	000310022003.txt	txt	02/17/03 11:15:52AM	94a8e93f8226ac3ac9b915a8e54fde53	File, Deleted, Archive	Text	02/17/03 11:15:52AM
1914	000310041997.txt	txt	09/24/01 08:47:22AM	ecbf9927dd273c33a56d3f9cb38b7583	File, Deleted, Archive	Text	09/24/01 08:47:22AM
1915	0003110072001.txt	txt	08/12/01 08:41:08PM	c152dea622d5e3243f3d6cc469f15	File, Deleted, Archive	Text	08/12/01 08:41:08PM
1916	000311061996.txt	txt	09/24/01 08:34:56AM	61f54f5d324153f976f485a30692fb2b	File, Deleted, Archive	Text	09/24/01 08:34:56AM
1917	0003111072002.txt	txt	07/31/02 10:07:32AM	ea8053aff8d5f12dbe0537365c4f8286	File, Deleted, Archive	Text	07/31/02 10:07:32AM
1918	000313101998.txt	txt	09/24/01 09:06:06AM	57c97642b0e46fda21bbc78f7be98c28	File, Deleted, Archive	Text	09/24/01 09:06:06AM
1919	000316092002.txt	txt	10/05/02 12:16:04PM	c21d6014846c11f5e7c02b53181e132	File, Deleted, Archive	Text	10/05/02 12:16:04PM
1920	0003217072002.txt	txt	07/31/02 10:07:30AM	75faf4842aa911bf86a5d57843e49e36	File, Deleted, Archive	Text	07/31/02 10:07:30AM
1921	0003219072001.txt	txt	08/12/01 08:41:10PM	f071caef9b47cf3370853ec533cd1513	File, Deleted, Archive	Text	08/12/01 08:41:10PM
1922	000324012002.txt	txt	05/04/02 11:58:34AM	eac30c8d0469388ba043b20cc92138f6	File, Deleted, Archive	Text	05/04/02 11:58:34AM
1923	000326012000.txt	txt	01/13/02 05:42:28AM	b6a8048f873e95764fc87d3356535691	File, Deleted, Archive	Text	01/13/02 05:42:28AM
1924	000327022001.txt	txt	09/24/01 09:30:08AM	f5d8c1ed3d8a201c604d80476aa8757e	File, Deleted, Archive	Text	09/24/01 09:30:08AM
1925	0003302082002.txt	txt	08/26/02 03:03:32PM	947fcf9e67369c0213e3a5e37e8b0d1a	File, Deleted, Archive	Text	08/26/02 03:03:32PM
1926	0003319072001.txt	txt	08/12/01 08:41:10PM	948629ef89f4f7e0cc2b39cf21f78c4	File, Deleted, Archive	Text	08/12/01 08:41:10PM
1927	0003403082001.txt	txt	08/12/01 07:01:12PM	844a0b4e19ee24bdedd3d456c4f79435	File, Deleted, Archive	Text	08/12/01 07:01:12PM
1928	0003414082002.txt	txt	08/26/02 03:03:28PM	14419f7ca8026045b454c12eaabd9d8e	File, Deleted, Archive	Text	08/26/02 03:03:28PM
1929	0003503092001.txt	txt	10/05/01 03:25:20PM	5a9aea38dbc36f30d32f3fadd0b543c	File, Deleted, Archive	Text	10/05/01 03:25:20PM
1930	0003516082002.txt	txt	08/26/02 03:03:30PM	6b5ecc25f677172741d6f6c693b6e6fa	File, Deleted, Archive	Text	08/26/02 03:03:30PM
1931	0003605092001.txt	txt	10/05/01 03:25:18PM	96a0e0b679ebf58ee3938a014868a4e3	File, Deleted, Archive	Text	10/05/01 03:25:18PM
1932	0003623082002.txt	txt	08/26/02 03:03:26PM	29c4d78ad8521cda6e8df7a29c55875a	File, Deleted, Archive	Text	08/26/02 03:03:26PM
1933	0003711092001.txt	txt	10/05/01 03:18:24PM	0f81d60581f65a34dd4458f1bce9dda6	File, Deleted, Archive	Text	10/05/01 03:18:24PM

Imagen No. 32 Detalle de archivos de texto eliminados.

	Name	File Ext	File Created	Hash Value	Description	File Type	Last Written
19214	\$_DASI~1.DOC	DOC	11/21/04 09:40:56PM	98d1b77830912f0906f841c1020e1aaf	File, Deleted, Hidden, Archive	Word Document	11/21/04 09:40:58PM
19215	\$_CUME~1.DOC	DOC	07/27/04 08:58:08AM	c6decc21c853aacefb9888cbfa7531b4	File, Deleted, Hidden, Archive	Word Document	07/27/04 08:58:10AM
19216	carta de retro Moldi...	doc	07/24/04 06:28:54PM	6f5755dd4d2faeb4d5f639f108805c2a	File, Deleted, Archive	Word Document	05/25/04 06:06:42PM
19217	ENVIO INFORMES U...	doc	05/21/04 01:00:46PM	daae41617dae6ca553c90d087b1ebde1	File, Deleted, Archive	Word Document	08/02/04 12:50:18PM
19218	2004ConvocatoriaD...	doc	07/27/04 08:41:04PM	bfb8736d347f4571a743812acce01ab6	File, Deleted, Archive	Word Document	07/27/04 09:36:44PM
19219	A Y M 0602.doc	doc	05/21/04 11:06:14AM	edf4b38b94bef4e24874b96090f3e4e4	File, Deleted, Archive	Word Document	06/02/04 06:57:08PM
19220	_ELI34XX.DOC	DOC	11/20/03 12:40:34PM	9fe0e217d540435690df2a060debcade	File, Deleted	Word Document	03/09/00 04:21:20PM
19221	_ELI34XX.DOC	DOC	07/23/04 08:25:24PM	c54a2668fb778fd34742db1968863fb	File, Deleted, Archive	Word Document	03/09/00 04:21:20PM
19222	_ELI34XX.DOC	DOC	08/06/04 12:54:26PM	c54a2668fb778fd34742db1968863fb	File, Deleted, Archive	Word Document	03/09/00 04:21:20PM
19223	\$_CORREO.DOC	DOC	08/28/04 07:40:18PM		File, Deleted, Overwritten, Hid	Word Document	08/28/04 07:40:18PM
19224	Pablo Escobar.doc	doc	07/29/04 09:50:12PM	a9fcc121bb020a2ea3635c5024228b4f	File, Deleted, Archive	Word Document	07/29/04 09:46:10PM
19225	_ELI34XX.DOC	DOC	08/06/04 11:42:28AM	c54a2668fb778fd34742db1968863fb	File, Deleted, Archive	Word Document	03/09/00 04:21:20PM
19226	_ELI33XX.DOC	DOC	11/20/03 12:40:26PM	3009fd7b7d5ea4e85997d90b83011d91	File, Deleted	Word Document	03/09/00 03:03:10PM
19227	_ELI33XX.DOC	DOC	08/06/04 11:42:26AM	3009fd7b7d5ea4e85997d90b83011d91	File, Deleted, Archive	Word Document	03/09/00 03:03:10PM
19228	_INWORD.DOC	DOC		1a5bfb9857b21b989d67c84e94a49f66	File, Deleted, Archive	Word Document	05/05/99 10:22:00PM
19229	EL ENSAYO.doc	doc	05/14/04 06:50:08PM	b1f3543e71242499b85b1281681473fd	File, Deleted, Archive	Word Document	05/18/04 08:28:02PM
19230	SECRETARÍA DE HA...	doc	07/24/04 06:28:54PM	31d901b259dd346da9f80ccfa7b7461d	File, Deleted, Archive	Word Document	03/24/04 08:00:42AM
19231	_INWORD2.DOC	DOC		02c4c0727b30d3011a7b7cbadba4800d	File, Deleted, Archive	Word Document	05/05/99 10:22:00PM
19232	FORMULARIORUT.doc	doc	09/12/04 06:06:06PM	24c70933ac1a9a1d7b585d08416629a4	File, Deleted, Archive	Word Document	09/12/04 06:06:06PM
19233	Formulario de presen...	doc	03/11/04 11:36:22PM	b83df0bbb162c4a7cbf5baccac857d8b	File, Deleted, Archive	Word Document	03/11/04 11:36:22PM
19234	_INWORD8.DOC	DOC	08/01/97 08:37:00AM	e617348b8947f28e2a280dd93c75a6ad	File, Deleted, Archive	Word Document	08/01/97 08:37:00AM
19235	Página principal pers...	doc	12/19/96 12:00:00AM	28b78df42be423c07b3d44f9dcbb3de	File, Deleted, Archive	Word Document	12/19/96 12:00:00AM
19236	_ELI33XX.DOC	DOC	07/23/04 08:25:18PM	3009fd7b7d5ea4e85997d90b83011d91	File, Deleted, Archive	Word Document	03/09/00 03:03:10PM
19237	_ELI33XX.DOC	DOC	08/06/04 12:54:22PM	3009fd7b7d5ea4e85997d90b83011d91	File, Deleted, Archive	Word Document	03/09/00 03:03:10PM
19238	\$_BROS~1.DOC	DOC	11/19/04 06:21:18AM		File, Deleted, Overwritten, Hid	Word Document	11/19/04 06:21:20AM
19239	_ELI32XX.DOC	DOC	11/20/03 12:40:18PM	8ac83db8a52e8f925dd1df193b5676ac	File, Deleted	Word Document	03/21/04 08:56:44PM
19240	_ELI32XX.DOC	DOC	08/06/04 11:42:22AM	8ac83db8a52e8f925dd1df193b5676ac	File, Deleted, Archive	Word Document	03/21/04 08:56:44PM
19241	_ELI32XX.DOC	DOC	08/06/04 12:54:18PM	8ac83db8a52e8f925dd1df193b5676ac	File, Deleted, Archive	Word Document	03/21/04 08:56:44PM
19242	_ELI32XX.DOC	DOC	07/23/04 08:25:14PM	c438bf705d02eebf6df892bdaf5c101e	File, Deleted, Archive	Word Document	11/15/04 12:20:28PM
19243	\$_CUME~1.DOC	DOC	11/21/04 09:55:32PM	98d1b77830912f0906f841c1020e1aaf	File, Deleted, Hidden, Archive	Word Document	11/21/04 09:55:32PM

Imagen No. 33 Detalle de archivos de Word eliminados.

© SANS Institute 2005

Name	File Ext	File Created	Hash Value	Description	File Type	Last Written
100607	ANEXOSCGN9...	xls	05/28/01 04:44:12PM	ee60b1a8db4a7bc44fc4d12aac56aa	File, Deleted, Archive	MS Excel Spreadsheet 05/29/01 08:54:28AM
100608	BALANCE ABR...	xls	05/23/04 10:29:50AM	8d2806b85aa76bc14884c02fc809e314	File, Deleted, Archive	MS Excel Spreadsheet 05/08/04 08:44:34AM
100609	BALANCE ABR...	xls	12/12/03 05:01:58AM	3bce45fc059993137268153abf360ef3	File, Deleted, Archive	MS Excel Spreadsheet 12/12/03 05:34:28AM
100610	BALANCE de Liq...	xls	11/15/04 01:09:20PM	d54c7374b1f85c880b2e84e3bd8e97c9	File, Deleted, Archive	MS Excel Spreadsheet 11/15/04 01:13:16PM
100611	BALANCES CC...	xls	05/19/04 09:44:02AM	cb06e03931fb4911bcedd8ba6ae09b63	File, Deleted, Archive	MS Excel Spreadsheet 04/29/04 08:47:02AM
100612	BALANCES CC...	xls	05/19/04 09:44:02AM		File, Deleted, Overwritten, Ar	MS Excel Spreadsheet 05/19/04 10:43:34AM
100613	BALANCES AN...	xls	05/14/04 12:15:50PM	5f71f16745ba022308e310fb5f972e87	File, Deleted, Archive	MS Excel Spreadsheet 05/14/04 12:38:36PM
100614	BALANCES AN...	xls	05/19/04 08:13:46AM	3b3b10f031cfe67df8f60878dcb8a19	File, Deleted, Archive	MS Excel Spreadsheet 05/19/04 10:43:30AM
100615	BALANCES CA...	xls	09/01/04 04:07:50PM	dd8078997a2d59adb56ca28cab33f855	File, Deleted, Archive	MS Excel Spreadsheet 09/01/04 04:54:40PM
100616	BALANCES CA...	xls	05/18/04 08:16:34AM	5b77773bff69f6a6e0d3636327d5f6e0	File, Deleted, Archive	MS Excel Spreadsheet 05/18/04 09:05:52AM
100617	BALANCES CO...	xls	10/29/04 09:39:12AM	63a0f802ff30d250a8b30a5cf4811b10	File, Deleted, Archive	MS Excel Spreadsheet 01/08/09 10:19:38AM
100618	BALANCES CO...	xls	11/04/04 11:16:42AM	c87c213316ea2d229460cccc78b308be	File, Deleted, Archive	MS Excel Spreadsheet 11/04/04 02:41:06PM
100619	BALANCES EL...	xls	05/19/04 08:14:10AM	075c2f669269bb00cf9940ec971868a3	File, Deleted, Archive	MS Excel Spreadsheet 05/19/04 08:27:06AM
100620	BALANCES FA...	xls	08/05/02 07:55:26AM	bd17a00fb4b0e1ac1f0a9110399bacfc	File, Deleted, Archive	MS Excel Spreadsheet 04/14/04 10:15:42PM
100621	BALANCES FA...	xls	08/04/02 08:10:04PM	0e77978e24a09d5ecb86e9c619cfff81a	File, Deleted, Archive	MS Excel Spreadsheet 02/04/04 04:42:42AM
100622	BALANCES FLI...	xls	04/27/04 08:53:38AM	329b3f8598ba33d7138925e37cce2663	File, Deleted, Archive	MS Excel Spreadsheet 04/28/04 05:25:00PM
100623	BALANCES GU...	xls	06/23/02 06:22:20AM	68366e804064cae39134b41147e40316	File, Deleted, Archive	MS Excel Spreadsheet 03/11/00 01:38:22PM
100624	BALANCES LA...	xls	01/14/04 05:07:22AM	6a079a9ee2e4997f0c60698a991103fb	File, Deleted, Archive	MS Excel Spreadsheet 10/28/04 07:37:34PM
100625	BALANCES LA...	xls	10/28/04 07:48:20PM	7b6426b8a8269cc0f29f34f6cab8741	File, Deleted, Archive	MS Excel Spreadsheet 10/28/04 07:37:52PM
100626	BALANCES LA...	xls	08/05/02 07:55:26AM	67eca71ee497c166e9f059ac35f6205	File, Deleted, Archive	MS Excel Spreadsheet 10/28/04 07:38:10PM
100627	BALANCES LEY...	xls	05/11/04 09:23:30PM	bdc5d53625a7e6542fdda4e5f801efb8	File, Deleted, Archive	MS Excel Spreadsheet 07/22/04 10:40:10AM
100628	BALANCES LEY...	xls	05/24/04 05:32:16PM	b7c50784741d92f59fc9666385f1274e	File, Deleted, Archive	MS Excel Spreadsheet 11/15/03 04:32:58PM
100629	BALANCES LO...	xls	04/22/04 02:05:54PM	803c79578013cdce6aed0b2bcc16ead9	File, Deleted, Archive	MS Excel Spreadsheet 10/21/04 10:07:18AM
100630	BALANCES MA...	xls	06/23/02 06:22:20AM	ce7be980f6fe8009a2136009a1e7d4af	File, Deleted, Archive	MS Excel Spreadsheet 05/06/01 01:07:06PM
100631	BALANCES MA...	xls	04/26/04 11:45:10AM		File, Deleted, Overwritten, Ar	MS Excel Spreadsheet 04/26/04 11:54:34AM
100632	BALANCES MO...	xls	10/31/04 06:16:42PM		File, Deleted, Overwritten, Ar	MS Excel Spreadsheet 11/01/04 06:56:38PM
100633	BALANCES MO...	xls	10/31/04 06:16:44PM	bc0cf19b98998f33991c5e68dc56f3e0	File, Deleted, Archive	MS Excel Spreadsheet 10/29/04 01:20:08PM
100634	BALANCES SE...	xls	05/24/04 05:33:06PM	e4d0ce00eda8495b861302e9584ae362	File, Deleted, Archive	MS Excel Spreadsheet 09/19/04 10:31:12PM
100635	BALANCES ST...	xls	11/26/03 04:03:44AM	2f6c02ceae4eceb6e138dd0421e85db8	File, Deleted, Archive	MS Excel Spreadsheet 11/26/03 04:06:40AM
100636	BALANCES ST...	xls	08/04/03 08:10:19PM	00f4402ca3e30770d4046417e5e136	File, Deleted, Archive	MS Excel Spreadsheet 03/11/00 11:46:47AM

Imagen No. 34 Detalle de archivos de Excel eliminados.

© SANS Institute 2005

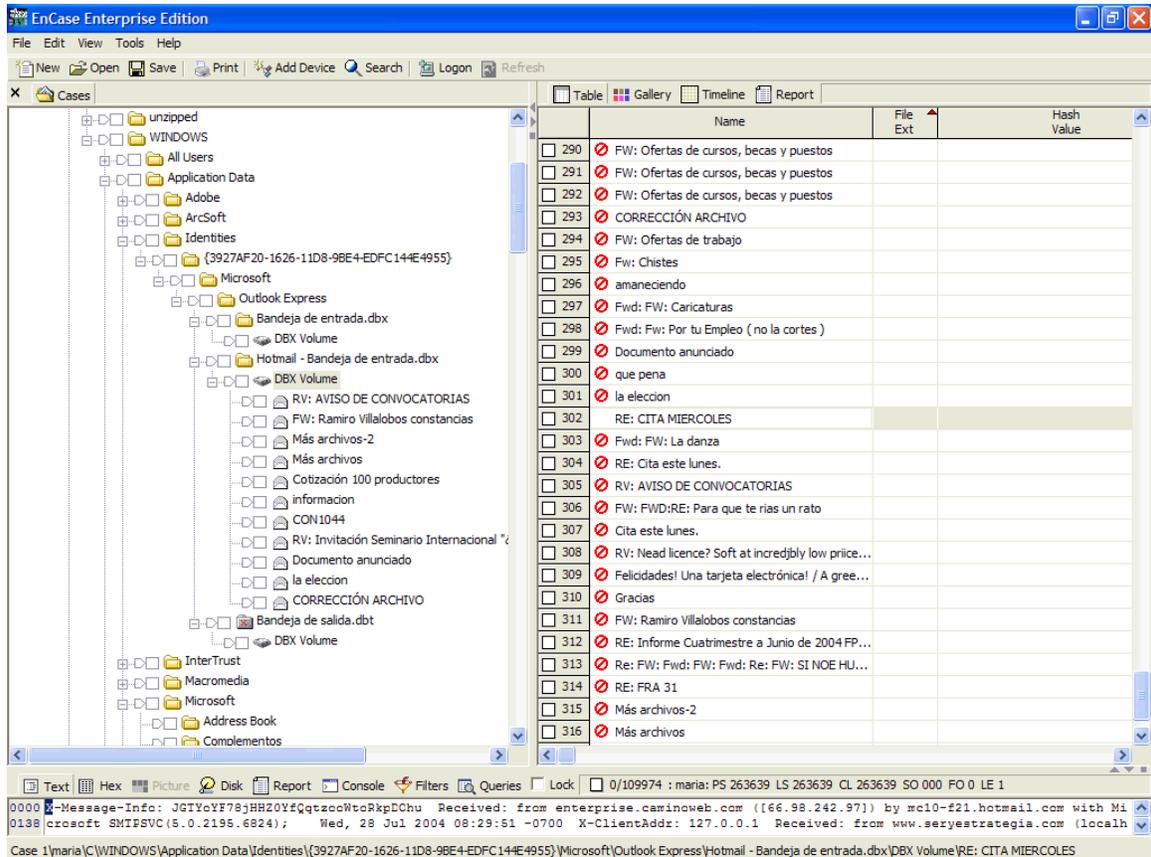


Imagen No. 35 Detalle de correos electrónicos eliminados.

Se utiliza una funcionalidad de EnCase que permite montar y visualizar los archivos de Outlook Express Hotmail – Bandeja de entrada.dbx, también permite el montaje y visualización de archivos de Outlook de extensión *.pst

Búsqueda de secuencias

Como parte de la metodología usada en el análisis forense se tiene la elaboración de una lista de palabras clave, esta lista inicialmente fué suministrada por el investigador principal de la operación y retroalimentada con el grupo interdisciplinario a medida de que se encontraban documentos, correos, etc. Son importantes estas búsquedas ya que vinculan áreas no visibles a través del sistema operativo como “Unallocated Clusters”, archivos de paginación, etc., los resultados ayudan a encontrar vínculos entre diferentes tipos de actividades de un sujeto y la evidencia digital.

Conclusiones

De acuerdo a los hallazgos encontrados, se puede precisar el uso de

programas de ofimática como el procesador de texto Word y la hoja de cálculo Excel para la realización de informes, el uso de programa contables para llevar las cuentas de varias empresas, el uso de programas especializados en el manejo de ganados y caballos para el control de este tipo de negocio, el uso de correo electrónico para el intercambio de información y los hábitos de navegación; el usuario al parecer no posee conocimientos en técnicas de protección como la asignación de claves a documentos ó cifrado, ya que no se encontró indicios de uso de estas, lo que facilitó en gran parte el éxito de la operación ya que quizá más importante aún que el sujeto detenido es la información que este manejaba.

Los hallazgos encontrados son analizados por grupos especializados en contabilidad, inteligencia, financieros, etc. cada uno de estos grupos aporta su conocimiento en el tema y emite un concepto que alimenta la investigación. Hay datos que se ingresan a un sistema especializado de inteligencia para su correlación.

Finalmente es importante resaltar que el análisis forense es una técnica fundamental hoy en día en las investigaciones que de una u otra forma vinculen computadores, agendas electrónicas, etc. y bajo las directrices del investigador principal y con el trabajo con grupos interdisciplinarios se logran buenos resultados.

Referencias

Guidance Software. Información sobre la Solución FIM de EnCase®
www.guidancesoftware.com – www.encase.com – www.missioncapable.com

Guidance Software. EnCase® Internet and E-mail Examinations. Manual de entrenamiento de GSI. 2004.

Guidance Software. EnCase® Field Intelligence Model, Live Forensic Investigations. Manual de entrenamiento de GSI. 2004.

Lugo, Edwin y otros. Manual de Incautación de Evidencia Electrónica. CD-ROM. Servicio Secreto de los Estados Unidos. Documento utilizado en el Programa Internacional de Asistencia en Entrenamiento en Investigación Criminal. (International Criminal Investigative Training Assistance Program, United States Secret Service and all law enforcement sections at the United States Embassy Bogotá, Colombia)

Policía Nacional de Colombia. Diplomado de Policía Judicial. CD-ROM. Material de Entrenamiento de la Escuela Nacional de Policía General Santander - Facultad de Investigación Criminal. 2004

SANS Institute. Track 8 - Firewall System Forensics, Investigation and Response. 2004.

© SANS Institute 2005, Author retains full rights.