



ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

“ANÁLISIS FORENSE EN SITIOS WEB”

INFORME DE MATERIA DE GRADUACIÓN

Previa a la obtención del Título de:
**LICENCIATURA EN REDES Y SISTEMAS
OPERATIVOS**

Presentada por:
**SHIRLEY VANESSA SORIA PANCHANA
JOSÉ SANTIAGO PARRALES TENELEMA**

GUAYAQUIL – ECUADOR

AÑO

2013

AGRADECIMIENTO

A Dios, por llenar nuestras vidas de bendiciones

A la Escuela Superior Politécnica del Litoral que nos brinda sus instalaciones como centro de educación.

A la Ingeniera Karina Astudillo por su colaboración para la realización de este proyecto.

A los profesores en general, ya que son los encargados de transmitir sus conocimientos.

A nuestros padres por el esfuerzo diario, que realizan para que logremos todas nuestras metas.

DEDICATORIA

A mi familia que me ha apoyado en todo momento y por ser la razón de mi esfuerzo diario.

A las personas que desean aprender un poco más sobre análisis y herramientas forenses, ya que poco a poco va tomando mayor fuerza e importancia en nuestro medio de la informática.

Shirley Soria Panchana.

En primera instancia a mi padre que a pesar de su ausencia siempre sentí su apoyo en transcurso de la carrera, a mi madre que se esforzó día a día para que no me faltara nada, convirtiéndose en madre y padre a la vez. A mis hermanos que en convivencia me impulsaban a seguir mejorando día a día en mis estudios. A todos mis demás familiares, en especial a mi prima Marjorie, que supo darle apoyo y armonía a mi familia.

José Parrales Tenelema.

TRIBUNAL DE SUSTENTACIÓN

Ing. Karina Astudillo

PROFESOR DE MATERIA DE GRADUACIÓN

Ing. Albert Espinal

PROFESOR DELEGADO POR EL DECANO DE LA FACULTAD

DECLARACIÓN EXPRESA

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

JOSÉ PARRALES TENELEMA

SHIRLEY SORIA PANCHANA

RESUMEN

La computación forense, se la utiliza hoy en día para resolver casos públicos y corporativos, debido a que la mayoría de documentos digitales e información confidencial, son almacenados en discos duros, en medios magnéticos u ópticos, en servidores o en centros de datos, que es de donde se obtiene la mayor parte de la información a ser analizada, como recuperación de contraseñas, archivos que aparentemente que han sido eliminados, entre otros.

Existe una gama de herramientas comerciales y gratuitas, para realizar el análisis de computación forense, pero en caso de una investigación, debemos tener cuidado de que las herramientas que se vayan a utilizar sean aceptadas ante una corte o tribunal de justicia.

Este mecanismo es utilizado para causas o casos comunes como: espionaje corporativo, casos de imitación, filtración de información, cybercrimen, entre otras.

En esta tesis se realiza el análisis de sitios web, donde se han obtenido una gran cantidad de descargas de archivos ilícitos, y visita de sitios web sospechosos.

ÍNDICE GENERAL

AGRADECIMIENTO	ii
DEDICATORIA	iii
TRIBUNAL DE SUSTENTACIÓN	iv
DECLARACIÓN EXPRESA	v
RESUMEN	vi
ÍNDICE GENERAL	vii
ÍNDICE DE FIGURAS	ix
CAPÍTULO 1	14
1.1 ANTECEDENTES.....	14
1.2 JUSTIFICACIÓN	15
1.3 DESCRIPCIÓN DEL PROYECTO	16
1.3.1 OBJETIVO GENERAL.....	17
1.3.2 OBJETIVOS ESPECÍFICOS	17
1.4 METODOLOGÍA.....	18
CAPÍTULO 2	20
2.1 INTRODUCCION	20
2.2 COMPUTACIÓN FORENSE	21
2.3 METODOLOGÍA GENERAL DEL PROCESO DE INVESTIGACIÓN.....	25

2.4	COMPUTACIÓN FORENSE EN NAVEGADORES WEB.....	26
2.5	CÓDIGO PENAL DE DELITOS INFORMÁTICOS EN EL ECUADOR.....	28
2.5.1	LEGISLACIÓN VIGENTE Y CONVENIOS INTERNACIONALES.....	29
2.5.2	NUEVO CÓDIGO ORGÁNICO INTEGRAL PENAL.....	31
CAPÍTULO 3	33
3.1	INTRODUCCION.....	33
3.2	BINARYVIEWER.....	35
3.3	INDEX.DAT ANALYZER.....	36
3.4	WEB HISTORY.....	38
3.5	PASCO.....	39
CAPÍTULO 4	40
4.1	INTRODUCCION AL CASO FIRMA DE ABOGADOS.....	40
4.2	OBJETIVOS DE LA AUDITORÍA.....	41
4.3	ADQUISICIÓN DE LA EVIDENCIA.....	41
4.4	ANÁLISIS DE LA EVIDENCIA.....	49
CONCLUSIONES Y RECOMENDACIONES	81
IMPLEMENTACIÓN DE POLITICAS DE SEGURIDAD	85
BIBLIOGRAFÍA	88

ÍNDICE DE FIGURAS

Figura 1 Proceso de Investigación.....	25
Figura 2: Herramienta Binary Viewer	36
Figura 3: Herramienta Index.dat Analyzer	37
Figura 4: Herramienta Web Historian.....	38
Figura 5: Herramienta PASCO	39
Figura 6: Evidencia recibida.....	42
Figura 7: Herramienta Binary Viewer	43
Figura 8: Versión archivo index.dat	44
Figura 9: Hash index.dat.....	45
Figura 10: URLs index.dat	46
Figura 11: Herramienta index.dat analyzer	48
Figura 12: Muestra el usuario que accedió al navegador web.....	49
Figura 13: Contenido del archivo index.dat.....	50
Figura 14: Ventana de la terminal de Caine Linux	59
Figura 15: Directorio de la herramienta PASCO	59
Figura 16: Instalación de la herramienta PASCO en línea de comandos.	60
Figura 17: Exportar información a un archivo de fácil lectura .csv	60
Figura 18: Resultado de la exportación del archivo index.dat.....	61
Figura 19: Búsqueda en google “cracking docustodian licensing”	62
Figura 20: Búsqueda en google con la palabra “cracking licensing software”	63

Figura 21: Acceso al sitio web http://slashdot.org	64
Figura 22: Búsquedas en google de hoteles en Sao Paulo Brasil	65
Figura 23: Sitio web del hotel Gran Hyatt Sao Paulo.....	66
Figura 24: Cotización de vuelos a Sao Paulo	67
Figura 25: Visita a la página web barnesandnoble en busca de códigos de hacking	69
Figura 26: Búsqueda con palabra clave software cracking.....	70
Figura 27: Accediendo al sitio web http://www.freeseicals.com/	71
Figura 28: Búsquedas de licencias de Docustodian	72
Figura 29: Ingresando a la página http://www.findcracks.com	73
Figura 30: Búsqueda de licencias docustodian.....	74
Figura 31: Ventana principal del correo joeschmo1980.....	75
Figura 32: Composición de un correo	76
Figura 33: Ventana post-envío del mail	77
Figura 34: Bandeja de entrada de la cuenta de correo.....	78
Figura 35: Buzón de entrada vacío.....	79
Figura 36: Imágenes encontradas en el index.dat	80

ÍNDICE DE TABLAS

Tabla 1: Tabla Comparativa de diferentes Herramientas Forenses.....	34
---	----

INTRODUCCIÓN

La computación forense, cada vez toma mayor fuerza y adquiere considerable importancia, debido al aumento de información almacenada de forma digital, al incremento del uso de computadores dentro de las compañías, y otros medios como el Internet. Cuando se comete algún delito informático, queda registrada información en estos medios de almacenamiento.

Gracias a las leyes de la física, la electricidad y el magnetismo, que permiten que la información se pueda analizar, leer e incluso recuperar archivos que fueron aparentemente eliminados.

La computación forense está siendo utilizada con el fin de identificar los hechos de un delito informático ejecutado, ya sea por fallas humanas o por el procesamiento sobre la infraestructura.

Es preciso establecer un conjunto de herramientas, estrategias y acciones para descubrir en los medios informáticos, la evidencia digital que sustente y verifique las afirmaciones realizadas sobre los hechos delictivos que se han materializado en el caso bajo estudio.

Se ha realizado esta investigación para una firma de abogados, que presentó un problema en su servidor principal, debido que se almacenaba una gran cantidad de información innecesaria descargada desde el Internet a su servidor, impidiendo su correcto funcionamiento.

Utilizaremos los principios de la computación forense con sus herramientas, para identificar quién o quiénes han incumplido con las políticas establecidas por la empresa, identificar el tiempo exacto en el que sucedieron los eventos; determinar si la acción fue realizada por usuarios internos o externos; establecer cuál fue el propósito del ataque, y a la vez mejorar la seguridad de la información de la empresa, por medio del establecimiento de política

CAPÍTULO 1

ANTECEDENTES Y JUSTIFICACION

1.1 ANTECEDENTES

Con el pasar del tiempo, los ataques informáticos se han ido incrementando, ya que, buscamos la forma de tener en nuestros sistemas informáticos toda la información necesaria por la facilidad de acceso que esta tiene, creando así un alto interés en las personas (hackers, crackers) en acceder a nuestra información, ya sea esta confidencial o privada; ahora no sólo debemos preocuparnos de ataques realizados por virus, sino también de grietas que tenemos en los sistemas, puertas abiertas a información confidencial. Cada día se encuentran más métodos para vulnerar y buscar debilidades en nuestra red y servidores, aun sin que estas personas gocen de un alto conocimiento informático debido a que en Internet se encuentran infinidad de herramientas, con las que se realizan fraudes informáticos, espionajes corporativos, casos de imitación y clonación.

Se ha considerado la existencia de dos tipos de ataques, estos son: los internos que en su mayoría son logrados de manera exitosa, y los

externos, que en algunos de los casos tienen algún contacto interno quien con engaños o con conocimiento de lo que se va a realizar proporciona la información que el atacante desea obtener.

Se debe tener en consideración que nunca debemos exceder la base de conocimientos, es decir que debemos basarnos siempre en la evidencia, y no realizar hipótesis o asumir situaciones en algún informe.

1.2 JUSTIFICACIÓN

Hoy en día el tener toda la información en servidores locales, discos duros, en Internet, y manejar la mayoría de documentos de manera digital, hace que tengamos mucho interés en la seguridad que se le pueda brindar a dicha información, ya que existen en la actualidad diversas maneras con las que se pueda llevar a cabo el espionaje corporativo o filtro de información.

Cuando realizamos una investigación o una auditoría, debemos tener claro el objetivo de nuestra investigación, lograr la recopilación de la mayor cantidad de evidencia posible, hacer uso de la cadena de custodia, tener un registro exacto de todas las personas que han

manipulado la evidencia, tener cuidado de no adulterar la evidencia original. Para ello se realizan copias necesarias las cuales debemos garantizar que sean idénticas a la original, se efectúan las pruebas sobre las copias manteniendo la integridad en el momento de ser analizadas, de modo que si el caso es llevado a la corte se pueda testificar con la evidencia.

De tener algún cambio en la evidencia se debe documentar todo lo realizado. Es importante realizar auditorías cada vez que la empresa considere necesario, debido a que ayudan a verificar cualquier anomalía, y evitar vulnerabilidades en nuestros sistemas.

1.3 DESCRIPCIÓN DEL PROYECTO

Nuestro proyecto busca lograr: Análisis de sitios en Internet, encontrar las páginas accedidas desde la máquina involucrada, ver los tiempos de acceso, verificar quien ha incumplido con las políticas internas de la empresa, saber la coordinación de administración de red de la empresa, conocer cuáles son las vulnerabilidades que dieron paso a las faltas cometidas. El escenario de análisis del presente proyecto se muestra en la primera sección del cuarto capítulo.

1.3.1 OBJETIVO GENERAL

Con la evidencia proporcionada para este caso, nuestro objetivo es analizar, descubrir e interpretar la información mediante herramientas informáticas, para establecer los hechos nos permitirán formar la hipótesis y la estructura del caso, ayudándonos de herramientas y técnicas de las que disponemos, para llegar al resultado real de la investigación, teniendo en consideración que no podemos asumir ni dar por entendido nada, apegados a lo que establecen las leyes sobre delitos informáticos

1.3.2 OBJETIVOS ESPECÍFICOS

- Determinar la autenticidad e integridad de las visitas de páginas web sospechosas, para realizar cierto tipo de ataques sobre el protocolo HTTP y que afectan a la disponibilidad de los servicios y recursos
- Establecer si la utilización de correos electrónicos se puede relacionar con elementos de contenido tales como el remitente, dirección destinataria, el computador que se utilizó, la persona destinataria, y cuál sería la relación entre estos elementos.

1.4 METODOLOGÍA

Para lograr nuestros objetivos propuestos debemos aplicar procedimientos con herramientas rigurosas que nos ayuden a resolver los diferentes tipos de delitos informáticos, apoyándonos en teorías científicas; aplicando métodos para la recolección de la información, análisis, y verificación de las pruebas digitales; establecer los mecanismos idóneos que nos permitan la adquisición, preservación, y la presentación de datos que han sido procesados electrónicamente y guardados en un equipo de computación.

Cabe recalcar que la computación forense no se encarga de prevenir delitos, de esto se encarga la seguridad informática; pero es importante tener claro el marco de actuación entre la informática forense, la seguridad informática y la auditoría informática.

La metodología forense consta de la adquisición segura de datos de diferentes medios y evidencias digitales, sin alterar de ninguna manera los datos de origen.

A cada fuente de información se le realiza una copia exacta y se la cataloga para prepararla para su posterior análisis, se debe documentar cada prueba aportada, tener fotos de lo que se encontró en primera instancia, y de haber sido manipulada por alguien, documentar en qué estado se recibió la evidencia. Las evidencias

digitales recabadas permiten determinar un dictamen claro, conciso, fundamentado y con justificación de las hipótesis en base de las cuales se han realizado las investigaciones a partir de las pruebas recogidas.

En todo procedimiento que vayamos a realizar debemos tener presente las leyes que la rigen. Y sus requerimientos, para no faltar en ningún momento a los derechos de terceros; y así de ser necesario, toda la evidencia sea aceptada sin problemas por los tribunales y poder construir una prueba bien fundamentada para alcanzar resultados favorables.

Dependiendo de la evidencia que tengamos también va a variar el tipo de metodología y los principios científicos que debemos considerar tales como:

- Recuperar documentos de un dispositivo dañado.
- Hacer una copia exacta de una evidencia digital.
- Generar una firma digital con un algoritmo hash MD5 o HA1 de un texto para asegurar que este no se ha modificado.
- Firmar digitalmente un documento para poder afirmar que es auténtico y preservar la cadena de evidencias.

CAPÍTULO 2

AUDITORÍA FORENSE

2.1 INTRODUCCION

El avance tecnológico se encuentra en constante crecimiento, así como el uso de Internet, de los equipos móviles, los centros de datos, y de las TIC'S; en general la gran cantidad de información de las empresas y usuarios se encuentran en estos medios, por lo cual también se desarrollan constantemente métodos para vulnerar la seguridad y tener acceso a dicha información. Cuando se presentan casos de estas vulnerabilidades da lugar la necesidad de realizar investigaciones más exhaustivas, basado en mecanismos y herramientas informáticas más eficientes y no visibles para un usuario común.

En cuanto al marco legal actual, en nuestro país se están realizando estudios para hacer mejoras en las leyes ya establecidas y así poder penalizar los delitos informáticos.

2.2 COMPUTACIÓN FORENSE

En general, computación forense se refiere a la investigación de datos, que pueden ser obtenidos de medios de almacenamiento estático y/o volátil con la finalidad de obtener la mayor cantidad de información posible. Es importante entender los dos tipos de datos con los que nos podemos encontrar, la parte visible y la no visible:

Visible:

- Documentos, Hojas de Cálculo, archivos de imágenes, correos electrónicos.
- Archivos y carpetas
- Programas y aplicaciones
- Accesos directos y enlaces
- Archivos de Logs

No Visible

- Documentos borrados, hojas de cálculo, correos electrónicos
- Archivos y carpetas borrados o en modo oculto
- Historiales de Internet
- Trabajos de Impresión
- Memoria de Acceso Aleatorio (RAM)

- Protección de claves ingresadas vía Web

Esta información localizada se la puede obtener a través de una imagen, de la data original utilizando herramientas para hacer copias exactas que no la afecten o alteren. Es importante que nos aseguremos con las herramientas idóneas que la copia sea idéntica a la prueba original (bit a bit), ya que vamos a realizar nuestro proceso de investigación sobre las copias, no se puede trabajar sobre la evidencia original, porque se debe tener la evidencia original sin alteraciones en lo posible, en el caso que sea necesario llevar la investigación y dar declaraciones ante una corte.

Una vez obtenida la información podremos comenzar a determinar el tipo de ataque es al que se estuvo expuesto, y la serie de eventos que dieron lugar al crimen a investigar.

Dentro de la investigación se deben analizar archivos de Logs, para verificar quienes han tenido acceso al computador, que URLs han visitado y si se ha borrado algún tipo de registro o información.

Es de suma relevancia garantizar la pureza de la evidencia, por lo cual se utiliza el método “Cadena de Custodia”, diseñado para controlar la confiabilidad de la prueba, desde el momento en que ocurrió el

incidente, hasta la finalización de la investigación. Puede ser utilizada como prueba legal y ayudar a la autoridad a tomar la decisión más precisa y justa posible.

El proceso de investigación debe estar basado en los siguientes puntos:

- 1.- **Identificación:** Determinar y edificar la evidencia del proceso o caso a evaluar.
- 2.- **Preservación:** Guardar y documentar todo lo que estuvo presente en el crimen.
- 3.- **Recolección:** Recopilación y documentación de información para demostrar que no se ha alterado ni fabricado evidencia.
- 4.- **Indagación:** Realizar extracciones y poner todos los archivos sólo en modo lectura para así no alterar la evidencia.
- 5.- **Análisis:** Basándose en realizar la reconstrucción de los hechos.
- 6.- **Presentación:** Es el reporte final donde se da a conocer la conclusión del caso, basado en todos los sucesos presentados, a través de un resumen ejecutivo. De ser un caso público, se debe presentar ante un juzgado.

7.- Decisión: Reporte donde se da la conclusión y las posibles decisiones que se tomarán para la solución del problema.

Para la fase de investigación se debe contar con una estación de trabajo para realizar análisis forenses, se debe tener dos computadoras o laptops como mínimo, sin conexión a Internet, y adicional una con conexión a red para la respectiva búsqueda. Así mismo contar con redundancia en el cableado eléctrico y energía regulada, por medio del uso de UPS (Uninterruptible power supply).

La ubicación de la estación de trabajo debe ser un lugar donde no afecten en lo posible los desastres naturales, preferible que no se posea ventanas que den a los exteriores, recomendable el uso de cámaras, alarmas, bitácoras de visita donde conste fecha, hora y motivo de visita, protección contra incendios y armarios metálicos empotrados en la pared y con su respectiva seguridad, difícil de violar, ya que aquí se deberá guardar la evidencia.

2.3 METODOLOGÍA GENERAL DEL PROCESO DE INVESTIGACIÓN

- ✓ **Adquirir:** Adquisición de la evidencia sin modificarla o corromperla.
- ✓ **Autenticación:** Garantizar que la copia que se ha obtenido es idéntica a la original y tener una firma de verificación.
- ✓ **Analizar:** El trabajo de análisis de la evidencia en busca de información se lo debe realizar evitando alteraciones. Ej.: tiempo de acceso.

Guía de proceso de investigación. Fuente Metodología de la Inspección Ocular en Informática Forense.

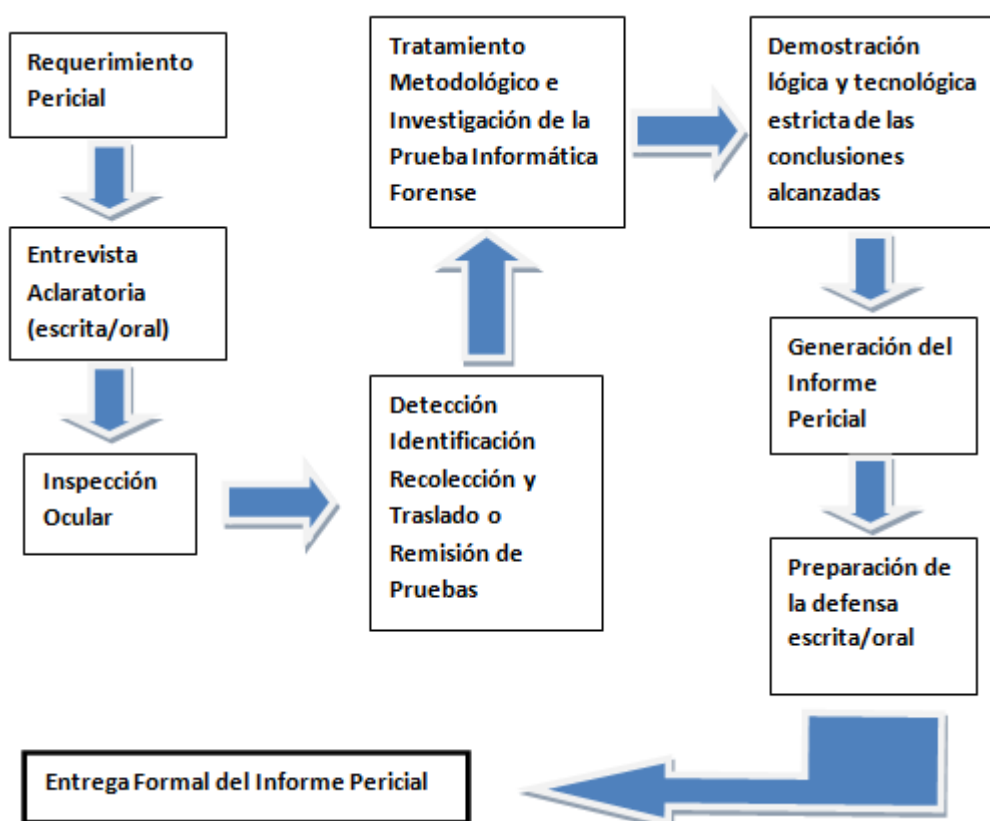


Figura 1 Proceso de Investigación.

2.4 COMPUTACIÓN FORENSE EN NAVEGADORES WEB.

En la actualidad, mucha información se ha digitalizado y compartido en red; el Internet ayuda a acceder a la misma, como: noticias, artículos, monografías, enciclopedias, revistas, etc., que nos mantienen al tanto de lo que pasa en el mundo. Lamentablemente en el Internet también tienen acceso personas malintencionadas que solo buscan cometer actos delictivos como fraude, terrorismo, estafas, extorsión, pornografía infantil, etc.

Para llevar a cabo este tipo de actos sean delictivos o de investigación, las personas, para poder acceder a la red necesitan de un Navegador (Internet Explorer, Google Chrome, Firefox, Opera, Safari, etc.). La elección del mismo, depende del usuario, al cual se adapte mejor según sus necesidades, o facilidades de uso.

Para el presente trabajo hablaremos del navegador Internet Explorer que forma parte del tema de investigación.

Internet Explorer.- Es un navegador web desarrollado por Microsoft que está integrado en el sistema operativo Windows y a esto se debe su popularidad a nivel mundial.

Durante sus inicios mantuvo su fortaleza ante los competidores, pero al pasar de los años fue muy criticado por no implementar medidas de seguridad y privacidad, pese a que fue lanzando nuevas versiones.

Otra razón de crítica fue su falta de soporte. A partir del 2006 los creadores se preocuparon más en estos aspectos, sin dejar a un lado su estética y funcionamiento.

Parte importante del navegador web para un investigador forense es la caché. Al acceder a la red con el navegador Internet Explorer toda esta actividad genera archivos temporales que son almacenados dentro de la caché para su carga rápida de la página en posteriores accesos, reduciendo el uso del ancho de banda. El contenido de la caché se encuentra en una base de datos indexado llamado index.dat, entre la información existente hay contenidos como imágenes, páginas web visitadas, cookies, historial, formularios, claves, etc.

En las primeras versiones del Internet Explorer no se podía borrar la información de la caché, siendo un problema para la privacidad del usuario. Hoy en día si permite borrar todos estos archivos, ya sea de forma manual o automática.

Existen usuarios familiarizados con el Internet Explorer y saben que pueden borrar el contenido de su movimiento en la Internet, accediendo a "Opciones de Internet"; pero lo que la mayoría no sabe es que a pesar de borrar este contenido desde el navegador la base de datos index.dat se mantiene intacta, y es ahí donde el investigador forense puede realizar la búsqueda de actos sospechosos o delictivos,

o simplemente actividades que van en contra de las políticas de una empresa u organización.

2.5 CÓDIGO PENAL DE DELITOS INFORMÁTICOS EN EL ECUADOR

En los últimos años el Ecuador ha estado sometido a varios robos de cuentas bancarias, suplantación de páginas web a nivel gubernamental, entre los más sonados. Con respecto al año 2011, hasta el mes de noviembre, ocurrieron débitos bancarios de forma ilegal a un gran número de cuenta ahorristas.

Con el fin de lograr una pronta solución a este creciente problema, los bancos se comprometieron a mejorar la seguridad en los cajeros y sistemas informáticos, así como el acceso a la cuentas de los usuarios en línea, y de esa manera brindarle tranquilidad a los millones de usuarios del sistema bancario nacional; adicionalmente se iniciaron campañas de concientización a los usuarios para que tomen las medidas correctas en el momento de ingresar a sus cuentas, como por ejemplo el verificar la correcta dirección url del banco, que esté la página certificada por alguna entidad emisora de certificados, no divulgar por ningún medio las claves personales, tener cuidado al

momento de recibir correos electrónicos de los bancos, verificando que la información recibida sea del emisor correspondiente antes de abrir algún enlace, y verificar que el protocolo a utilizar sea seguro como (https).

Por estas razones de ámbito informático, se ha enviado a la asamblea, propuestas para las reformas del Código Penal. El texto referente a los delitos informáticos sería: “toda acción consciente y voluntaria que provoca perjuicio a persona natural o jurídica, en el que se emplean sistemas informáticos o telemáticos”. Y siendo las sanciones de estas leyes, de uno a siete años.

2.5.1 LEGISLACIÓN VIGENTE Y CONVENIOS INTERNACIONALES ¹

Mientras se reforma el Código Penal, en Ecuador se trabaja actualmente con leyes supletorias, tales como:

- Código Penal, en especial el Art. 202
- Ley de Comercio electrónico , firmas electrónicas y bases de datos
- Resolución 55/63 aprobada por la Asamblea de la ONU de la Lucha contra la utilización de la tecnología de la información con fines delictivos.

¹ Legislación vigente y convenios internacionales: tomado de www.interfutura.com.ec

- Convenio de Cibercriminalidad de Budapest, del cual podremos ser signatarios una vez que contemos con una normativa legal específica para estos delitos, y;
- Reglamento 124/7 de la Interpol para el tratamiento de datos. Gracias al convenio realizado con este organismo y a través de éste, en los casos de los delitos que se cometan a través de redes sociales, el Agente Fiscal, de considerar necesario, puede solicitar la información pertinente a empresas como Facebook y Google.

2.5.2 NUEVO CÓDIGO ORGÁNICO INTEGRAL PENAL ²

La nueva ley, en proceso de creación, traerá cambios significativos para el tratamiento del delito informático. El capítulo que tendría dentro de este Código sería el de “Protección de datos e información” y lo más destacado de este nuevo cuerpo legal es la incorporación de los siguientes tipos penales:

- Apropiación fraudulenta
- Estafa informática
- Base ilegal de datos
- Falsificación electrónica
- Falsedad informática
- Intromisión indebida a los sistemas informáticos de información telemática
- Filtración a base de datos

Así mismo, se incorporaría al Código de Procedimiento Penal, en el capítulo pertinente a las pruebas, la evidencia digital como otro elemento de convicción y posterior prueba en la etapa de juicio, para su respectivo cómputo forense.

² Nuevo código orgánico integral penal: tomado de www.justiciapenalecuador.com.ec

³Para delitos relacionados en el robo de bases de datos, como obtener, copiar, archivar, transferir, comercializar o procesar datos personales sin autorización judicial o de su titular, tienen establecida la pena, que es la privación de la libertad de uno a tres años.

El daño informático, como el de impedir el funcionamiento normal de programas, recibirá una sanción de tres a cinco años de prisión y una multa que irá de las 10 a las 20 remuneraciones básicas unificadas.

Quien modifique, desarrolle, trafique, comercialice, ejecute, programe o imite una página web, enlaces o ventanas emergentes, es decir, genere falsedad informática, pagará una pena de prisión de siete a nueve años

³ Obtenidos de www.hoy.com.ec

CAPÍTULO 3

HERRAMIENTAS

3.1 INTRODUCCION

Existen diversas herramientas para realizar auditorías forenses a continuación se muestra una tabla referencial con las herramientas más usadas.

Tabla Comparativa Herramientas para Computación Forense

HERRAMIENTA	COSTO	PLATAFORMA	EVALUACION
The Coroners toolkit	Gratis	Linux	Media
		SUN Solaris	
		RedHat Linux	
The Sleuth Kit y Autopsy	Gratis	Unix/Linux	Alto
		Windows	
Foundstone Forensic Toolkit	Comercial	Windows	Alto
BackTrack	Gratis	GNU/Linux	Alto
Encase	Comercial	Windows	Medio
Pasco	Gratis	Linux	Medio
		Windows	
Web History	Gratis	Windows	Medio
Index.dat Analyzer	Gratis	Windows	Alto
Binary Viewer	Gratis	Windows	Medio

Tabla 1: Tabla Comparativa de diferentes Herramientas Forenses

Para el desarrollo del caso del presente proyecto, se nos ha proporcionado entre los archivos que vamos a analizar un "Index.dat" y tres carpetas que contienen indicios de actividad en línea, sitios que se han visitado, lista de URLs, archivos y documentos a los que se han accedido. Toda esta información se encuentra codificada en binario, por lo cual utilizamos la herramienta BinaryViewer, y para una

visualización más detallada y organizada de las actividades nos ayudamos con la herramienta Index.dat Analyzer.

3.2 BINARYVIEWER

Características técnicas mínimas recomendadas para operar BinaryViewer:

Requisitos: Microsoft.Net Framework 3.5 Service Pack 1

Plataforma: Windows 2K/ XP/ Vista x86/ Vista 64/ 7 x86/ 7 64

Características de funcionamiento nos permite abrir y ver su contenido en formato decimal, octal, hexadecimal, y texto (ASCII), de archivos codificados en formato binario, soporta archivos de hasta 4 GB, permite la búsqueda de datos dentro del contenido, copiado y pegado en un portapapeles.

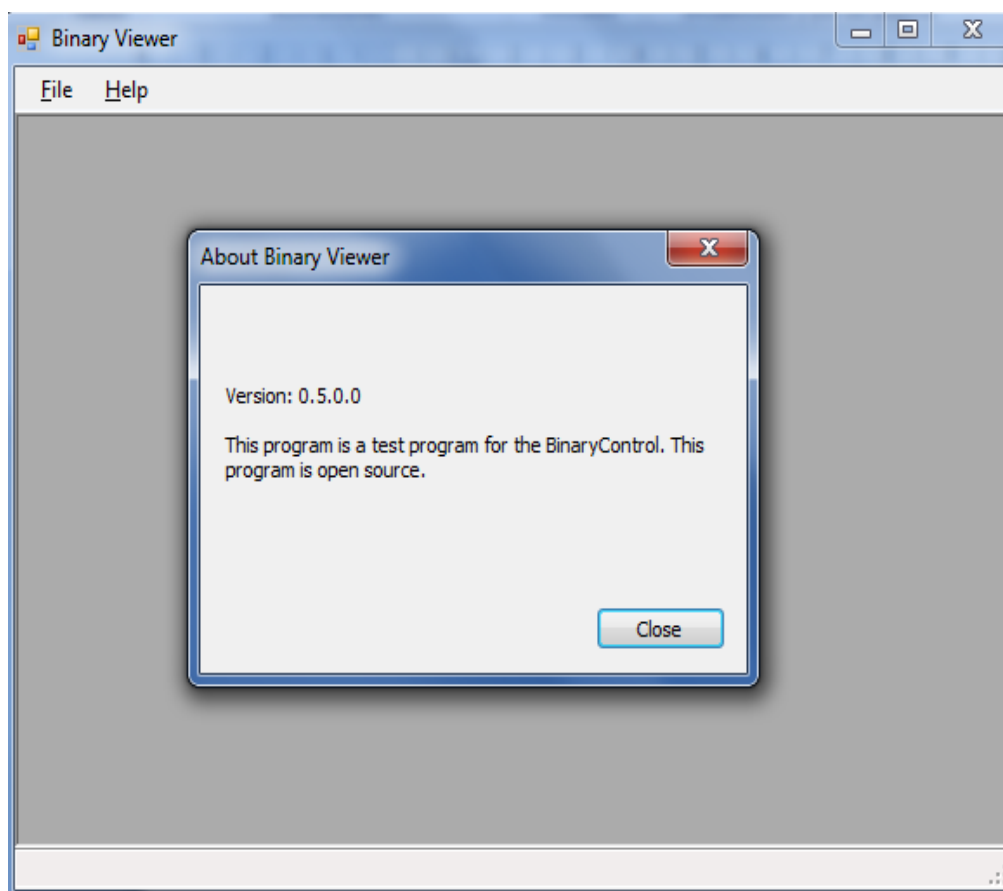


Figura 2: Herramienta Binary Viewer

3.3 INDEX.DAT ANALYZER

Esta herramienta permite ver y borrar el contenido del archivo index.dat que es donde se almacenan las páginas que un usuario ha visitado, encontrando referencias de cookies, historial de navegación y páginas de caché.

El análisis de esta información permite determinar la actividad que realiza el usuario en Internet, como: descargas, documentos, fecha y hora de acceso, fecha de creación de la página web.

Para un mejor manejo de la información la herramienta permite extraer el contenido en un archivo .exe (EXCEL) y así tener una búsqueda más óptima.

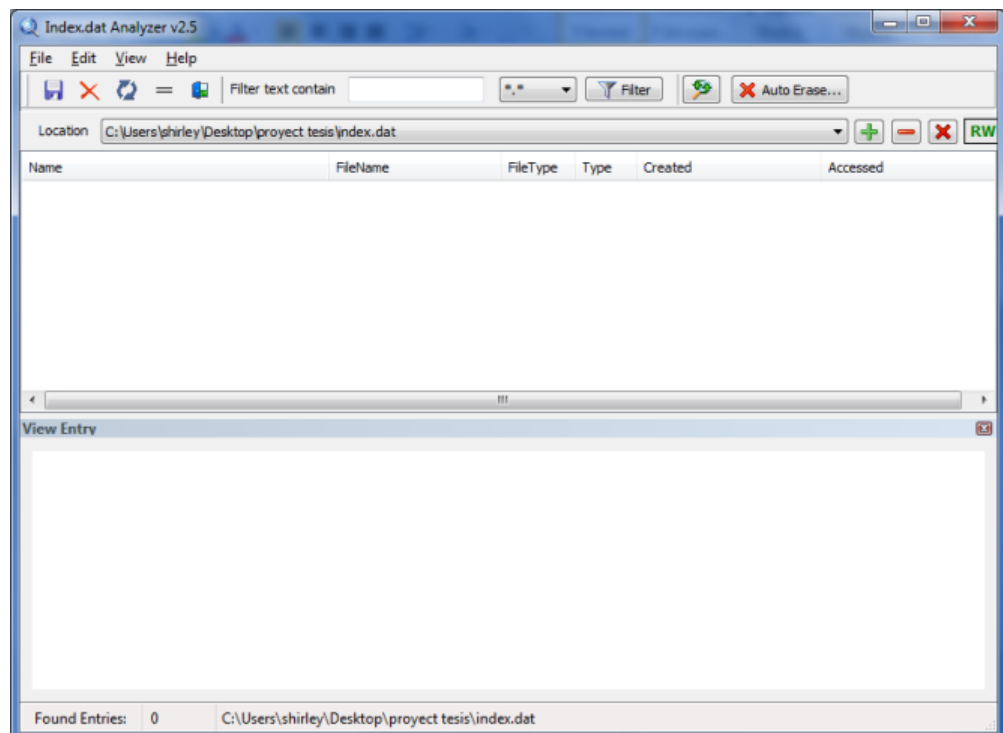


Figura 3: Herramienta Index.dat Analyzer

3.4 WEB HISTORY

Es un software libre de la Corporación Mandiant Historiador de la web, analiza los archivos del historial de Internet Explorer, Firefox, Google Chrome y Safari.

Características del programa:

Nombre del programa: Mandiant Web Historian

Editores: Mandiant

Distribuidor sitio: <http://www.mandiant.com/>

Sistema operativo: Windows 2003, XP, 2000, 98, Me, NT

Requisitos: No hay requisitos

Tamaño: 19.53MB

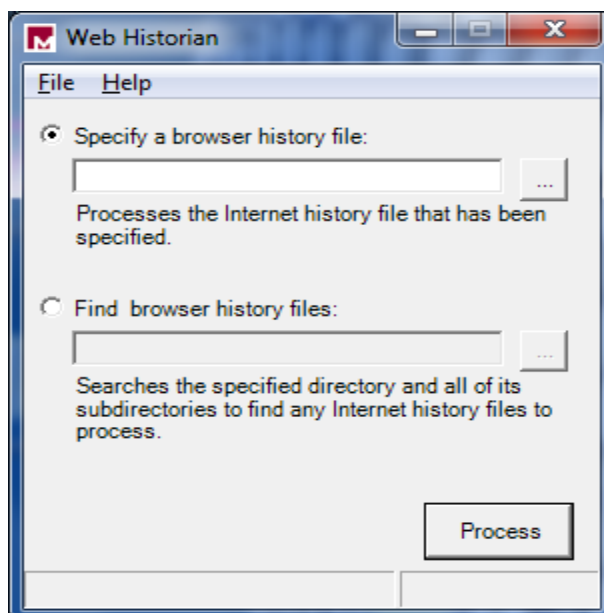


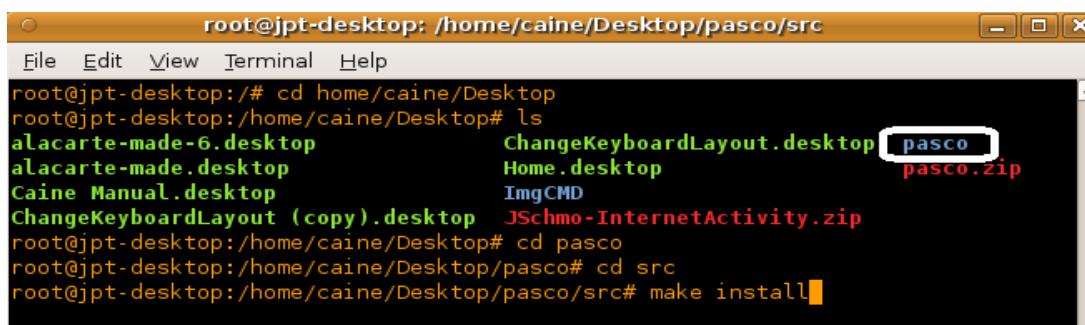
Figura 4: Herramienta Web Historian

3.5 PASCO

Es una herramienta Forense que analiza la actividad del Internet Explorer, desarrollado por Keith J. Jones.

Nos permite generar un archivo legible y entendible con un margen de error mínimo, y así tener una correcta documentación en el transcurso de la investigación.

Muchas investigaciones de delitos informáticos requieren la reconstrucción de la actividad en Internet de un sujeto. Pasco, que en latín significa buscar, fue desarrollada para examinar el contenido de los archivos de caché de Internet Explorer. El fundamento principal de Pasco se basa en analizar información de un archivo index.dat y mostrar los resultados de una manera que podamos mejorar su visibilidad por medio de una hoja de cálculo



```
root@jpt-desktop: /home/caine/Desktop/pasco/src
File Edit View Terminal Help
root@jpt-desktop:/# cd home/caine/Desktop
root@jpt-desktop:/home/caine/Desktop# ls
alacarte-made-6.desktop      ChangeKeyboardLayout.desktop pasco
alacarte-made.desktop       Home.desktop                 pasco.zip
Caine Manual.desktop        ImgCMD
ChangeKeyboardLayout (copy).desktop JSchmo-InternetActivity.zip
root@jpt-desktop:/home/caine/Desktop# cd pasco
root@jpt-desktop:/home/caine/Desktop/pasco# cd src
root@jpt-desktop:/home/caine/Desktop/pasco/src# make install
```

Figura 5: Herramienta PASCO

CAPÍTULO 4

Desarrollo del Proyecto

4.1 INTRODUCCION AL CASO FIRMA DE ABOGADOS

El 18 de marzo del 2005 a las 20:25, un asociado de un prestigioso bufete de abogados acababa de terminar el borrador de un contrato de venta de una propiedad para su cliente, pero no se pudo guardar el documento en el servidor central de almacenamiento alojado en Docustodian, INC. En sus intentos de cargar el documento se mostró el siguiente error: “Se ha llegado al límite de almacenamiento por favor, comuníquese con su administrador de sistema”.

El Asociado Sénior llamó a Joe Schmo, quien es el administrador de IT de la firma de abogados. Pero, su llamada se desvió al correo de voz de Joe indicando que estaba de vacaciones desde el 7 de marzo al 21 del mismo mes, 2005.

Esto no fue un hecho aislado. Un estudio interno reveló que más de 500 GB de archivos MP3, software pirata, y películas se almacenan en el sistema, bajo el perfil de Joe Schmo. Después de encontrar una posible instrucción de lo que había ocurrido, la firma de abogados rápidamente llegó a la conclusión que era necesario realizar una investigación de violación potencial a las políticas internas, o a la

realización de actividades fuera de lo normal, que debe desarrollar como administrador de IT, de esta forma la firma de abogados contrató una empresa de seguridad profesional para dirigir la investigación.

4.2 OBJETIVOS DE LA AUDITORÍA

- El principal objetivo de la investigación es probar o refutar si el administrador de TI fue quien realizó la serie de actividades ilícitas.
- Determinar quién es el responsable de que se haya permitido la descarga de archivos ilegales, análisis minucioso de la evidencia, extracción de la información contenida en el archivo index.dat.

4.3 ADQUISICIÓN DE LA EVIDENCIA

Para el análisis del caso no se tuvo un acceso físico a los equipos ni mayor información con respecto a las personas que tienen acceso a los mismos, posesión de claves, horarios laborales, ni si el señor Jhon Schmo tuvo algún remplazo, durante sus vacaciones.

Previamente se nos ha entregado un CD con los siguientes archivos y carpetas:

 8R9KCL4N	Fecha de modificación: 21/03/2005 16:36
 B3B0BSCG	Fecha de modificación: 21/03/2005 16:36
 ICJNEDI2	Fecha de modificación: 21/03/2005 16:34
 KYRPJUXG	Fecha de modificación: 21/03/2005 16:37
 index.dat Tipo: Archivo DAT	Fecha de modificación: 12/03/2005 12:38 Tamaño: 288 KB

Figura 6: Evidencia recibida

De acuerdo a la gráfica mostrada tenemos 4 carpetas y un archivo Index.dat, en el cual tenemos información relevante para este caso ya que contiene indicios de todas las actividades realizadas en Internet. Debido a que el contenido del archivo se encuentra en formato binario, utilizamos como primera herramienta BinaryViewer versión 0.5.0.0 (programa de prueba del BinaryControl, Open Source)

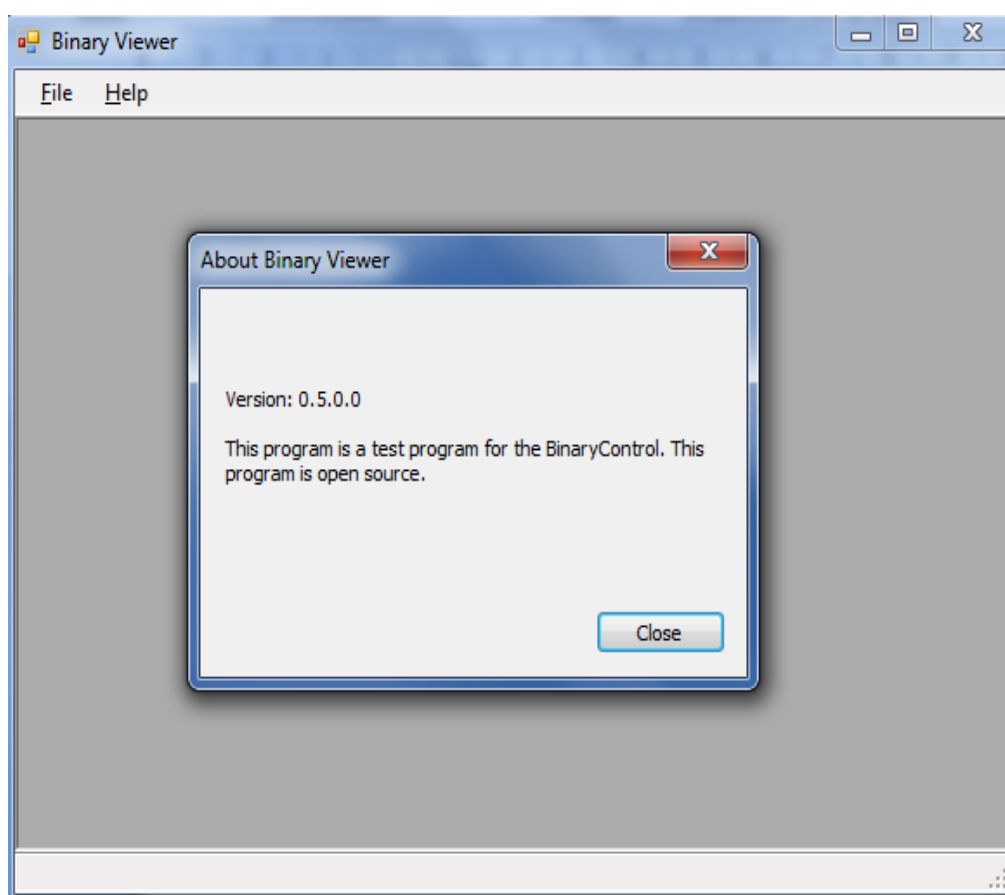


Figura 7: Herramienta Binary Viewer

Como procedimiento inicial al abrir el archivo index.dat se mostró su contenido en formato hexadecimal y ASCII (texto) de lo cual se pudo sacar la siguiente información:

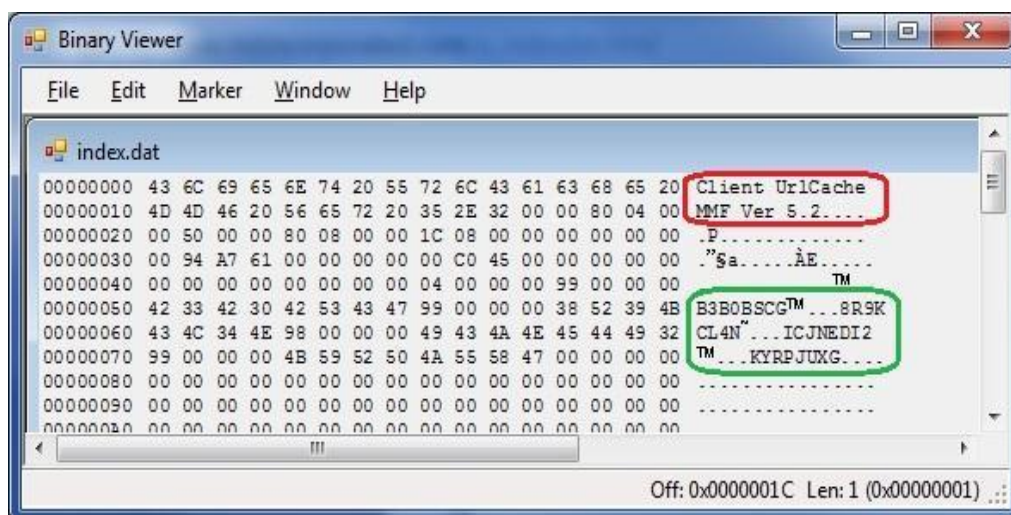


Figura 8: Versión archivo index.dat

ClientUrlCaché MMF Ver 5.2; es la versión del archivo index.dat que está relacionada con la versión del Internet Explorer siendo esta IE 5.2
 Los siguientes 4 nombres (Verde) son las 4 subcarpetas en donde se encuentran almacenados todos los archivos de la caché de Internet:
B3B0BSCG, 8R9KCL4N, ICJNEDI2, HYRPJUXG.

```

Binary Viewer
File Edit Marker Window Help
index.dat
00005000 48 41 53 48 20 00 00 00 00 70 01 00 00 00 00 00 HASH .....p.....
00005010 00 C4 74 C3 00 75 00 00 00 AB CB 2D 80 02 01 00 .ÄtÄ.u...«E-...
00005020 80 32 DB 11 00 60 02 00 80 1A A6 BB 00 F4 02 00 2Ü.....|».ö..
00005030 C0 39 9C 7E 80 19 03 00 00 B6 A3 14 80 45 03 00 Å9ø.....t.E...
00005040 C0 28 53 B6 00 74 03 00 80 5F 47 39 00 A0 00 00 Å(SF.t...G9...
00005050 00 96 83 B1 80 77 02 00 C0 01 4A 5D 00 88 02 00 .-f#w...Ä.J]...
00005060 00 57 C5 15 80 AA 02 00 00 DB 12 1C 80 B9 02 00 .WÄ..*...Ü..¹..
00005070 C0 7C 86 4F 80 E2 02 00 00 04 07 78 80 09 04 00 Ä|†Oä.....x...
00005080 00 5D 81 7B 00 E6 00 00 C0 2A DC 7F 00 F4 00 00 .}|(.æ...Ä+Ü.ö..
00005090 40 37 F4 EE 00 FF 00 00 00 EC 10 65 00 2D 01 00 @7öi.y...i.e...
000050A0 40 4B 52 BD 80 DD 01 00 40 BA CF CB 80 E8 01 00 @KRMý...@°iÈè..
000050B0 00 9C 26 59 80 0D 02 00 00 2F 75 3B 00 63 00 00 .osY..../u;c...
000050C0 40 8D 46 84 00 BF 00 00 C0 E2 1F 90 80 81 01 00 @F...;...ÄÄ...
000050D0 00 50 AA 46 80 92 02 00 C0 24 C2 28 80 B3 02 00 .p*f'...ÄsÄ(*...
000050E0 80 98 EB BD 00 C3 02 00 C0 0F 2A B8 00 3E 03 00 "e*.Ä..Ä..*.,>..
000050F0 80 53 D0 74 80 84 01 00 00 DA 24 FF 00 3D 02 00 Söc....Ûsý=...
00005100 80 F0 94 EB 00 5D 02 00 C0 CA 1C AD 80 F2 02 00 s"e.]...ÄÄ.ö...
00005110 80 F6 50 BF 80 79 03 00 00 F1 24 66 80 AA 03 00 öP;ÿ...Äsf*...
00005120 80 4E 50 A5 80 D9 03 00 80 9C 8F 1E 00 C1 00 00 NP#Ü...æ..Ä...
00005130 80 56 B9 81 00 F8 01 00 00 1B 07 BC 80 F9 01 00 V¹.æ....kù...
00005140 00 64 1B F5 80 43 02 00 00 BE C4 8C 00 57 02 00 .d.öC...*ÄCE.W..
00005150 40 3D 37 36 80 83 02 00 80 21 9E B2 80 F5 02 00 @=76f...!ö...
00005160 00 99 D4 F0 80 E4 00 00 00 A8 16 FA 80 ED 00 00 .TMösa...".úí...
00005170 40 A5 FB 6C 80 5B 02 00 00 A9 7D D7 00 67 02 00 @w1l[...@}*g...
00005180 80 15 07 22 80 86 02 00 00 4F 6A BA 80 39 03 00 ..."†...Oj*9...
00005190 80 21 24 A7 80 76 03 00 40 16 87 48 00 95 00 00 !sÿv...@.iH...
000051A0 40 AF 66 98 80 67 01 00 80 78 4D 27 00 F2 01 00 @-f"q...xM'.ö...
000051B0 40 BA 4B F3 80 58 02 00 00 4A C4 C5 00 27 03 00 @°KóX...JÄÄ.'...
000051C0 C0 43 9C EE 80 72 03 00 00 EF 3A 22 00 9D 03 00 ÅCöär...i:....
000051D0 40 CE BA DB 00 4B 01 00 C0 4C 77 36 00 E7 01 00 @i°Ü.K..ÄLw6.ç...
000051E0 C0 9E FA 15 00 EF 01 00 00 1D 24 14 80 5E 02 00 Äú...i....s.^...
000051F0 03 00 00 00 03 00 00 00 03 00 00 00 03 00 00 00
  
```

Figura 9: Hash index.dat

Hash, son los índices hashes del contenido del archivo index.dat y no presenta información privada.

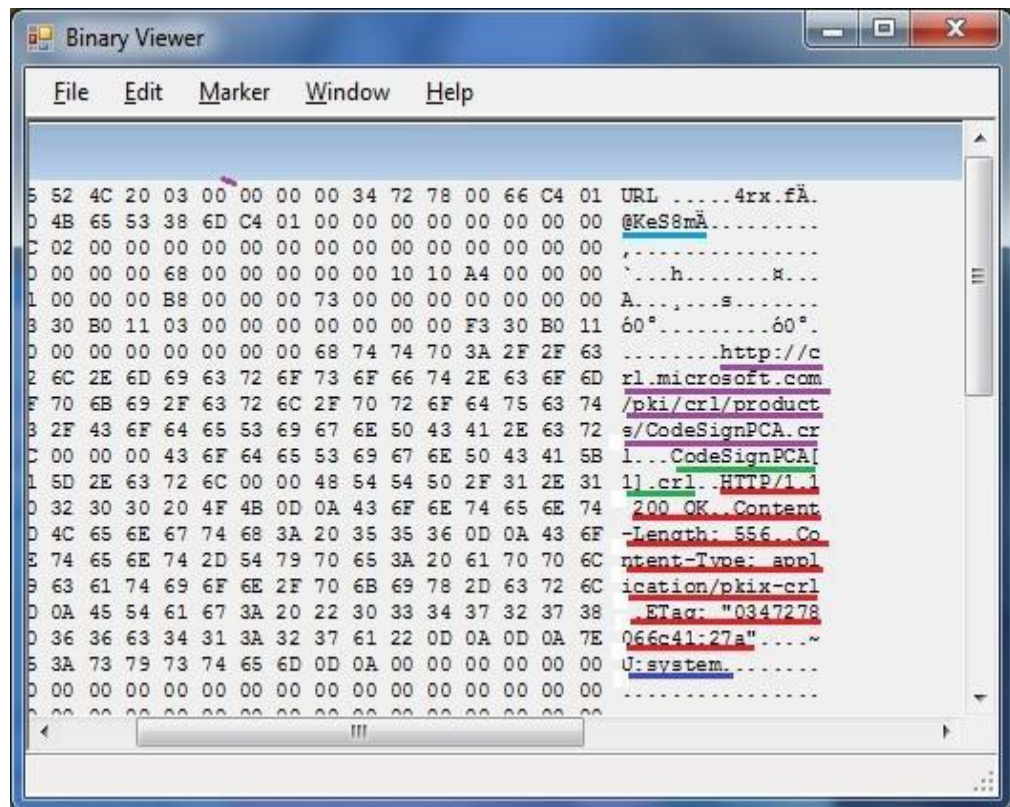


Figura 10: URLs index.dat

Archivos URL, como primer parámetro (azul turquesa) tenemos la fecha y hora pero están codificados no presentan una fácil interpretación. Como siguiente (morado) es la dirección URL completa del archivo cargado. A continuación (verde) el nombre del archivo con su respectiva extensión: CodeSignPCA [1].crl. Lo siguiente (rojo) es la cabecera completa del HTTP que recibió como respuesta del servidor web:

HTTP/1.1 200 OK Versión del protocolo HTTP (1.1) y que la solicitud fue recibida correctamente (200 OK)

Content-Length: 556 (Longitud del cuerpo de la respuesta)

Content-Type: application/pkix-crl (Tipo del contenido del cuerpo de la respuesta)

ETag: "0347278066c41:27a"

Y por último es el nombre de la cuenta de usuario (azul):

U: system

La segunda herramienta usada **Index.dat Analyzer** nos brinda un historial completo en un formato fácilmente legible para nosotros.

Entre la información que nos proporciona tenemos:

Nombre del archivo, tipo de archivo, fecha de creación y fecha de acceso.

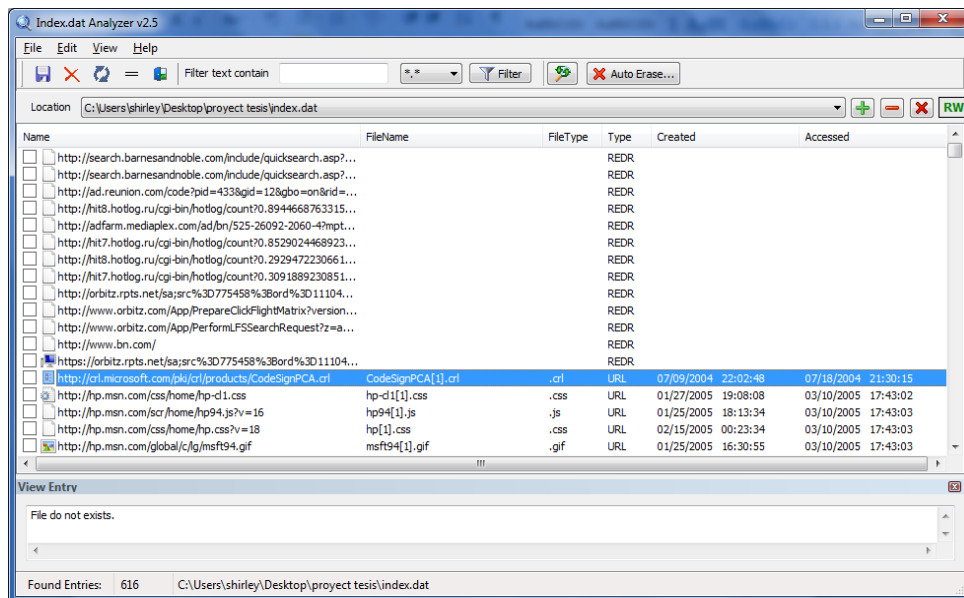


Figura 11: Herramienta index.dat analyzer

4.4 ANÁLISIS DE LA EVIDENCIA.

Ya con las herramientas necesarias procedemos al análisis de la evidencia, de primera mano con la Binary Viewer podemos fijarnos que todas las navegaciones se lo hicieron con el Usuario jschmo el cual es un indicio de que se utilizó la cuenta del administrador Joe Schmo para realizar estas actividades. Pero para ello tendríamos que corroborar que al usuario Joe Schmo le corresponde el alias jschmo.

```

Binary Viewer - [index.dat]
File Edit Marker Window Help
00006DE0 00 00 00 00 00 00 00 68 74 74 70 3A 2F 2F 68 .....http://h
00006DF0 70 2E 6D 73 6E 2E 63 6F 6D 2F 31 56 2F 57 48 45 p.msn.com/1V/WHE
00006E00 33 21 46 4E 52 38 5F 31 5A 56 58 33 53 53 50 51 3!FNRS_12VX3SSPQ
00006E10 5B 41 43 2E 6A 70 67 00 57 48 45 33 21 46 4E 52 [AC.jpg.WHE3!FNR
00006E20 38 5F 31 5A 56 58 33 53 53 50 51 5B 41 43 5B 31 8_12VX3SSPQ[AC[1
00006E30 5D 2E 6A 70 67 00 00 48 54 54 50 2F 31 2E 31 l.jpg...HTTP/1.1
00006E40 20 32 30 30 20 4F 4B 0D 0A 43 6F 6E 74 65 6E 74 200 OK..Content
00006E50 2D 4C 65 6E 67 74 68 3A 20 32 30 31 34 0D 0A 43 -Length: 2014..C
00006E60 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 69 6D 61 content-Type: ima
00006E70 67 65 2F 6A 70 65 67 0D 0A 45 54 61 67 3A 20 22 ge/jpeg..ETag: "
00006E80 38 31 61 65 34 64 64 35 31 39 32 35 63 35 31 3A 81ae4dd51925c51:
00006E90 38 62 32 22 0D 0A 50 33 50 3A 20 43 50 3D 22 42 8b2"...P3P: CP="B
00006EA0 55 53 20 43 55 52 20 43 4F 4E 6F 20 46 49 4E 20 US CUR CONo FIN
00006EB0 49 56 44 6F 20 4F 4E 4C 20 4F 55 52 20 50 48 59 IVDo ONL OUR PHY
00006EC0 20 53 41 4D 6F 20 54 45 4C 6F 22 0D 0A 0D 0A 7E SM TELo".....U
00006ED0 55 3A 6A 73 63 68 6D 6F 0D 0A 00 00 00 00 00 U: jschmo
00006EE0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00006EF0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00006F00 55 52 4C 20 03 00 00 00 00 7D AA 5F 05 25 C5 01 URL .....}*_%A.
00006F10 20 BE A1 85 C2 25 C5 01 B8 38 F0 BC 00 00 00 00 00 %;A%A.88%....
00006F20 F1 09 00 00 00 00 00 00 00 00 00 00 00 00 00 A.....
00006F30 60 00 00 00 68 00 00 00 01 00 10 10 98 00 00 00 .....h.....
00006F40 41 00 00 00 B8 00 00 00 A2 00 00 00 00 00 00 00 A.....e.....
00006F50 6A 32 63 B5 01 00 00 00 00 00 00 00 6A 32 63 B5 j2cp.....j2cp
00006F60 00 00 00 00 00 00 00 68 74 74 70 3A 2F 2F 68 .....http://h
00006F70 70 2E 6D 73 6E 2E 63 6F 6D 2F 34 38 2F 21 5A 57 p.msn.com/48!/ZW
00006F80 7E 38 37 4F 4B 37 47 33 31 2C 4D 5B 54 41 43 33 ~87OK7G31,M[TAC3
00006F90 4E 37 41 2E 6A 70 67 00 21 5A 57 7E 38 37 4F 4B N7A.jpg.!ZW~87OK
00006FA0 37 47 33 31 2C 4D 5B 54 41 43 33 4E 37 41 5B 31 7G31,M[TAC3N7A[1
00006FB0 5D 2E 6A 70 67 00 00 48 54 54 50 2F 31 2E 31 l.jpg...HTTP/1.1
00006FC0 20 32 30 30 20 4F 4B 0D 0A 43 6F 6E 74 65 6E 74 200 OK..Content
00006FD0 2D 4C 65 6E 67 74 68 3A 20 32 35 34 35 0D 0A 43 -Length: 2545..C
00006FE0 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 69 6D 61 content-Type: ima
00006FF0 67 65 2F 6A 70 65 67 0D 0A 45 54 61 67 3A 20 22 ge/jpeg..ETag: "
00007000 66 37 31 32 64 34 35 66 35 32 35 63 35 31 3A 38 f712d45f525c51:8
00007010 62 32 22 0D 0A 50 33 50 3A 20 43 50 3D 22 42 55 b2"...P3P: CP="BU
00007020 53 20 43 55 52 20 43 4F 4E 6F 20 46 49 4E 20 49 S CUR CONo FIN I
00007030 56 44 6F 20 4F 4E 4C 20 4F 55 52 20 50 48 59 20 VDo ONL OUR PHY
00007040 53 41 4D 6F 20 54 45 4C 6F 22 0D 0A 0D 0A 7E 55 SM TELo".....U
00007050 3A 6A 73 63 68 6D 6F 0D 0A 00 00 00 00 00 00 U: jschmo
00007060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00007070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
Off: 0x00000000

```

Figura 12: Muestra el usuario que accedió al navegador web

Haciendo uso de la siguiente herramienta Index.dat Analyzer que como lo habíamos indicado anteriormente nos provee información más completa y entendible, pudimos extraer las páginas que se había visitado, como: www.hotmail.com, www.google.com, www.saopaulo.grand.hyatt.com, www.barnesandnoble.com, www.findcracks.com, www.freeseentials.com, www.orbitz.com, www.slashdot.org.

Si filtramos la búsqueda a archivos .htm y lo ordenamos por tiempo de acceso obtenemos el siguiente resultado:

The screenshot shows the Index.dat Analyzer v2.5 interface. The main window displays a list of files extracted from the index.dat file, filtered to show only .htm files. The files are sorted by access time. Below the list, there is a search bar with the text 'cracking docustodian licensing' and a search button. The search results show that no documents were found for this query.

Name	FileName	FileType	Type	Created	Accessed
http://www.google.com/search?hl=en&q=cracking+docustodian+licensing+&btnG=Google+Search	search[1].htm	.htm	URL	01-01-1601 00:00:00	03-10-2005 17:44:10
http://www.google.com/search?hl=en&q=cracking+licensing+software	search[1].htm	.htm	URL	01-01-1601 00:00:00	03-10-2005 17:44:21
http://pagead2.googlesyndication.com/pagead/ads?client=ca-pub-6162369826930049&dt=1110494684187&mt=1110494684187&format=120x600_as...	CANVG106.htm	.htm	URL	01-01-1601 00:00:00	03-10-2005 17:44:46
http://news.google.com/	news.google[1].htm	.htm	URL	01-01-1601 00:00:00	03-10-2005 17:45:14
http://ad.doubleclick.net/ad/N2537.ecommercetimes.com/B1527521.5;sz=728x90;ord=11104947277466?	B1527521[1].htm	.htm	URL	01-01-1601 00:00:00	03-10-2005 17:45:35
http://ad.doubleclick.net/ad/N2537.ecommercetimes.com/B1563006.4;sz=336x280;ord=11104947271785?	B1563006[1].htm	.htm	URL	01-01-1601 00:00:00	03-10-2005 17:45:35
http://ad.doubleclick.net/ad/N815.ecommercetimes.com/B1555812.4;sz=728x90;ord=11104947275778?	B1555812[1].htm	.htm	URL	01-01-1601 00:00:00	03-10-2005 17:45:35
http://ad.doubleclick.net/ad/N815.ecommercetimes.com/B1555812.3;sz=120x600;ord=11104947275322?	B1555812[1].htm	.htm	URL	01-01-1601 00:00:00	03-10-2005 17:45:38
http://slashdot.org/	slashdot[1].htm	.htm	URL	01-01-1601 00:00:00	03-10-2005 17:46:02
http://ads.osdn.com/?ad_id=6420&alloc_id=13925&site_id=18&request_id=8246091	ads.osdn[1].htm	.htm	URL	01-01-1601 00:00:00	03-10-2005 17:46:11
http://www.google.com/	google[1].htm	.htm	URL	01-01-1601 00:00:00	03-10-2005 17:47:17
http://www.google.com/search?hl=en&q=sao+paulo+hotels	search[2].htm	.htm	URL	01-01-1601 00:00:00	03-10-2005 17:47:33
http://saopaulo.grand.hyatt.com/	saopaulo.grand.hyatt[1]...	.htm	URL	01-01-1601 00:00:00	03-10-2005 17:47:41
http://www.orbitz.com/	orbitz[1].htm	.htm	URL	01-01-1601 00:00:00	03-10-2005 17:47:50
http://www.orbitz.com/html.ng/domain=orbitz&channel=home§ion=main&adsize=342x188&OrbitzCookieName=OSC&orbitzID=CwOIEaWQlel-1...	domain=orbitz&channel...	.htm	URL	01-01-1601 00:00:00	03-10-2005 17:47:51
http://www.orbitz.com/html.ng/domain=orbitz&channel=home§ion=main&adsize=homeText180&OrbitzCookieName=OSC&orbitzID=CwOIEaWQlel-1...	domain=orbitz&channel...	.htm	URL	01-01-1601 00:00:00	03-10-2005 17:47:52
http://www.orbitz.com/html.ng/domain=orbitz&channel=home§ion=main&adsize=homeText180&OrbitzCookieName=OSC&orbitzID=CwOIEaWQlel-1...	domain=orbitz&channel...	.htm	URL	01-01-1601 00:00:00	03-10-2005 17:47:52
http://www.orbitz.com/html.ng/domain=orbitz&channel=home§ion=main&adsize=homeText380&OrbitzCookieName=OSC&orbitzID=CwOIEaWQlel-1...	domain=orbitz&channel...	.htm	URL	01-01-1601 00:00:00	03-10-2005 17:47:52
http://www.orbitz.com/html.ng/domain=orbitz&channel=home§ion=main&adsize=1x180&OrbitzCookieName=OSC&orbitzID=CwOIEaWQlel-15742...	domain=orbitz&channel...	.htm	URL	01-01-1601 00:00:00	03-10-2005 17:47:52

View Entry

Go to Google Home Web Images Groups News Froogle Local **Local** more »

cracking docustodian licensing Search Advanced Search Preferences

Web

Tip: Try [Google Answers](#) for help from expert researchers

Your search - **crackina docustodian licensina** - did not match any documents.

Found Entries: 616 C:\Users\Holger\Desktop\New folder\index.dat

Figura 13: Contenido del archivo index.dat

Información extraída de la herramienta index.dat Analyzer

Name:

<http://www.google.com/search?hl=en&q=cracking+docustodian+licensing+&btnG=Google+Search>

FileName: search[1].htm

File Type: .htm

Type: URL

Date Created: 01/01/1601 00:00:00

Date Accessed: 03/10/2005 17:44:10

Name:

<http://www.google.com/search?hl=en&lr=&q=cracking++licensing+software>

FileName: search[1].htm

File Type: .htm

Type: URL

Date Created: 01/01/1601 00:00:00

Date Accessed: 03/10/2005 17:44:21

Name: <http://slashdot.org/>

FileName: slashdot[1].htm

File Type: .htm

Type: URL

Date Created: 01/01/1601 00:00:00

Date Accessed: 03/10/2005 17:46:02

Name: <http://www.google.com/search?hl=en&q=sao+paulo+hotels>

FileName: search[2].htm

File Type: .htm

Type: URL

Date Created: 01/01/1601 00:00:00

Date Accessed: 03/10/2005 17:47:33

Name: <http://saopaulo.grand.hyatt.com/>

FileName: saopaulo.grand.hyatt[1].htm

File Type: .htm

Type: URL

Date Created: 01/01/1601 00:00:00

Date Accessed: 03/10/2005 17:47:41

Name: <http://www.orbitz.com/>

FileName: orbitz[1].htm

File Type: .htm

Type: URL

Date Created: 01/01/1601 00:00:00

Date Accessed: 03/10/2005 17:47:50

Name:

<http://www.orbitz.com/App/ViewFlightSearchResults?z=apz1&r=12>

FileName: ViewFlightSearchResults[1].htm

File Type: .htm

Type: URL

Date Created: 01/01/1601 00:00:00

Date Accessed: 03/10/2005 17:48:32

Name: <http://www.barnesandnoble.com/>

FileName: barnesandnoble[1].htm

File Type: .htm

Type: URL

Date Created: 01/01/1601 00:00:00

Date Accessed: 03/10/2005 17:48:34

Name:

<http://search.barnesandnoble.com/booksearch/results.asp?WRD=code%20hacking&userid=pv4dUK5Bu2&cds2Pid=946>

FileName: results[1].htm

File Type: .htm

Type: URL

Date Created: 01/01/1601 00:00:00

Date Accessed: 03/10/2005 17:48:44

Name:

<http://www.orbitz.com/App/ViewFlightSearchResults?z=bcb0&r=as>

FileName: ViewFlightSearchResults[2].htm

File Type: .htm

Type: URL

Date Created: 01/01/1601 00:00:00

Date Accessed: 03/10/2005 17:49:01

Name:

<https://www.orbitz.com/Secure/SubmitFlightSelection?version=1&selectIndex=0&action=purchase&carrier=AV&z=bcec&r=cq>

FileName: SubmitFlightSelection[1].htm

File Type: .htm

Type: URL

Date Created: 01/01/1601 00:00:00

Date Accessed: 03/10/2005 17:49:05

Name: <http://www.freeseicals.com/>

FileName: freeseicals[1].htm

File Type: .htm

Type: URL

Date Created: 01/01/1601 00:00:00

Date Accessed: 03/10/2005 17:49:43

Name:

<http://search.barnesandnoble.com/booksearch/results.asp?WRD=software%20cracking&userid=pv4dUK5Bu2>

FileName: results[2].htm

File Type: .htm

Type: URL

Date Created: 01/01/1601 00:00:00

Date Accessed: 03/10/2005 17:50:30

Name: <http://www.findcracks.com/>

FileName: findcracks[1].htm

File Type: .htm

Type: URL

Date Created: 01/01/1601 00:00:00

Date Accessed: 03/10/2005 17:50:44

Name:

[http://www.freeserials.com/serials/search.php?q=docustodian&query=](http://www.freeserials.com/serials/search.php?q=docustodian&query=Search+%21)

[Search+%21](http://www.freeserials.com/serials/search.php?q=docustodian&query=Search+%21)

FileName: search[3].htm

File Type: .htm

Type: URL

Date Created: 01/01/1601 00:00:00

Date Accessed: 03/10/2005 17:50:58

Name: <http://www.findcracks.com/?q=docustodian+licensing>

FileName: findcracks[1].htm

File Type: .htm

Type: URL

Date Created: 01/01/1601 00:00:00

Date Accessed: 03/10/2005 17:52:52

Name: <http://login.passport.net/ui/login.srf?id=2af815441>

FileName: uilogin[1].htm

File Type: .htm

Type: URL

Date Created: 01/01/1601 00:00:00

Date Accessed: 03/10/2005 17:53:12

Name: http://by23fd.bay23.hotmail.msn.com/cgi-bin/hmhome?fti=yes&curmbox=F000000001&a=1028e6c155aa3ce4f917f32f82d3f2f2&_lang=EN&country=US

FileName: hmhome[1].htm

File Type: .htm

Type: URL

Date Created: 01/01/1601 00:00:00

Date Accessed: 03/10/2005 17:53:35

Name: <http://by23fd.bay23.hotmail.msn.com/cgi-bin/compose?&curmbox=F000000001&a=1028e6c155aa3ce4f917f32f82d3f2f2>

FileName: compose[1].htm

File Type: .htm

Type: URL

Date Created: 01/01/1601 00:00:00

Date Accessed: 03/10/2005 17:53:57

Name: <http://by23fd.bay23.hotmail.msn.com/cgi-bin/premail/5238>

FileName: 5238[1].htm

File Type: .htm

Type: URL

Date Created: 01/01/1601 00:00:00

Date Accessed: 03/10/2005 18:08:41

Name: [http://by23fd.bay23.hotmail.msn.com/cgi-](http://by23fd.bay23.hotmail.msn.com/cgi-bin/HoTMaiL?curmbox)

[bin/HoTMaiL?curmbox](http://by23fd.bay23.hotmail.msn.com/cgi-bin/HoTMaiL?curmbox)

[=F000000001&a=cec03517f01c559b0265ea3012e5ed60](http://by23fd.bay23.hotmail.msn.com/cgi-bin/HoTMaiL?curmbox)

FileName: HoTMaiL[1].htm

File Type: .htm

Type: URL

Date Created: 01/01/1601 00:00:00

Date Accessed: 03/10/2005 18:08:51

Name: <http://by23fd.bay23.hotmail.msn.com/cgi-bin/HoTMaiL>

FileName: HoTMaiL[1].htm

File Type: .htm

Type: URL

Date Created: 01/01/1601 00:00:00

Date Accessed: 03/10/2005 18:09:02

Se utilizó la herramienta Pasco para un análisis exhaustivo del archivo index.dat en un ambiente Linux bajo el Sistema Operativo Caine que es una distribución de Ubuntu.

Se ingresa al lugar donde tenemos el instalador de pasco

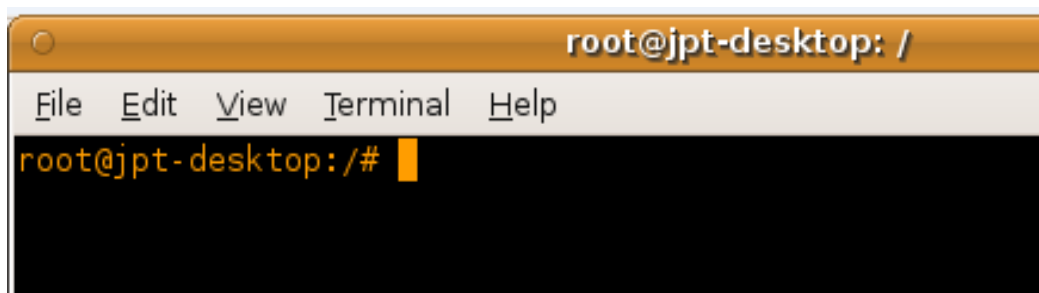


Figura 14: Ventana de la terminal de Caine Linux

Accedemos a la carpeta y con la ayuda del comando ls hacemos una vista del contenido

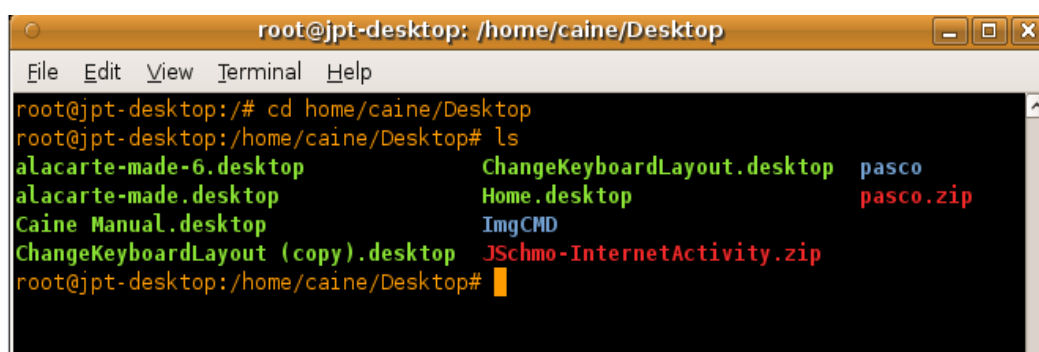
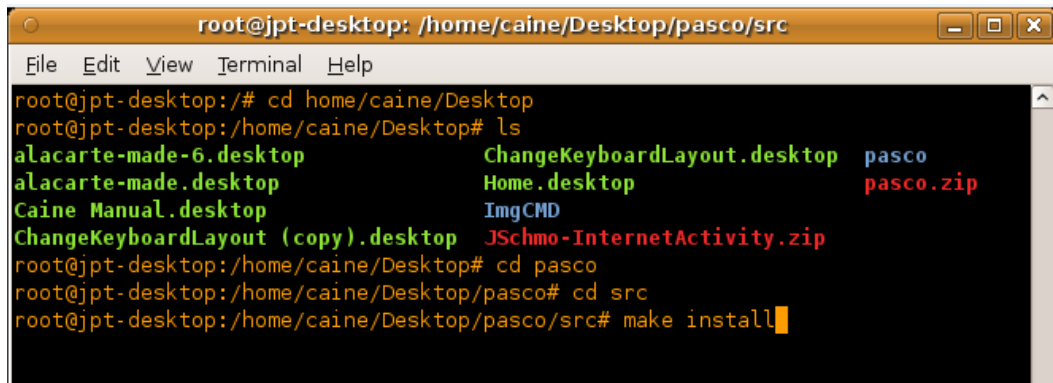


Figura 15: Directorio de la herramienta PASCO

Procedemos a realizar la instalación de Pasco con el comando “make install”.



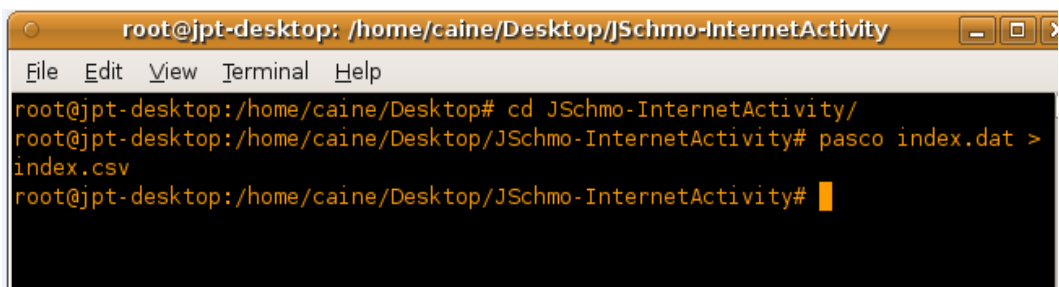
```

root@jpt-desktop: /home/caine/Desktop/pasco/src
File Edit View Terminal Help
root@jpt-desktop:/# cd home/caine/Desktop
root@jpt-desktop:/home/caine/Desktop# ls
alacarte-made-6.desktop      ChangeKeyboardLayout.desktop  pasco
alacarte-made.desktop       Home.desktop                  pasco.zip
Caine Manual.desktop        ImgCMD
ChangeKeyboardLayout (copy).desktop JSchmo-InternetActivity.zip
root@jpt-desktop:/home/caine/Desktop# cd pasco
root@jpt-desktop:/home/caine/Desktop/pasco# cd src
root@jpt-desktop:/home/caine/Desktop/pasco/src# make install

```

Figura 16: Instalación de la herramienta PASCO en línea de comandos.

Para tener una facilidad en la lectura del archivo lo cambiamos a un formato .csv que nos permite visualizar el resultado de la búsqueda en una hoja de cálculo.



```

root@jpt-desktop: /home/caine/Desktop/JSchmo-InternetActivity
File Edit View Terminal Help
root@jpt-desktop:/home/caine/Desktop# cd JSchmo-InternetActivity/
root@jpt-desktop:/home/caine/Desktop/JSchmo-InternetActivity# pasco index.dat >
index.csv
root@jpt-desktop:/home/caine/Desktop/JSchmo-InternetActivity#

```

Figura 17: Exportar información a un archivo de fácil lectura .csv

El resultado del uso de la herramienta nos permite visualizar el historial del navegador con su respectivo url, fecha de creación de página, la cabecera, y el usuario desde donde se realizaron las visitas.

History File: index.dat Version: 5.2	
TYPE	URL
MODIFIED TIME	ACCESS TIME
FILE NAME	DIRECTORY
HTTP HEADERS	
URL	http://hp.msn.com/55/LN!H2WS26G5_YXFO_2F2P.gif03/10/2005 08:01:3903/10/2005 17:43:04LN!H2WS26G5_YXFO_2F2P[1].gifCJNEDI2HTTP/1.1 200 OK Content-Length: 1894 Co
URL	http://ad.doubleclick.net/adi/N2537.ecommercetimes.com/B1563006.4
URL	http://www.orbitz.com/Marketing/Images/hotwire-125x175-message2.gif07/11/2004 01:02:1403/10/2005 17:49:01hotwire-125x175-message2[1].gifCJNEDI2HTTP/1.1 200 OK ETag
URL	https://www.orbitz.com/img/security/verisign_footer.gif12/20/2004 05:40:1503/10/2005 17:49:07verisign_footer[2].gif8R9KCL4NHTTP/1.1 200 OK ETag: "6483b6-d8e-41c6ac0f" Co
URL	http://a1055.g.akamai.net/f/1055/1401/5h/images.barnesandnoble.com/gresources/navbar/tab4_textbooks_cold.gif01/13/2005 22:24:3503/10/2005 17:50:30tab4_textbooks_colc
URL	http://a1055.g.akamai.net/f/1055/1401/5h/images.barnesandnoble.com/pimages/gresources/linePagination.gif08/10/2004 08:56:2503/10/2005 17:50:30linePagination[1].gifCJN
URL	http://a1055.g.akamai.net/f/1055/1401/5h/images.barnesandnoble.com/images/2650000/2657694.gif08/29/2000 19:51:3103/10/2005 17:50:312657694[1].gifKYRPUXGHTTP/1.0 200
URL	http://macslash.org/images/sr.gif07/04/2002 18:16:3103/10/2005 17:44:42sr[1].gifKYRPUXGHTTP/1.1 200 OK X-Powered-By: Slash 2.002006 X-Fry: If this is some kind of scam, I dor
URL	http://a1055.g.akamai.net/f/1055/979/5h/images.barnesandnoble.com/gresources/navbar/vcart4_topbot_rule.gif01/12/2005 11:43:2303/10/2005 17:48:36vcart4_topbot_rule[1].g
URL	http://a1055.g.akamai.net/f/1055/979/5h/images.barnesandnoble.com/gresources/navbar/tab4_usedoop_cold.gif01/13/2005 05:04:2703/10/2005 17:48:37tab4_usedoop_cold[1].
URL	http://a1055.g.akamai.net/f/1055/979/5h/images.barnesandnoble.com/images/8180000/8188722.gif08/26/2004 13:58:2903/10/2005 17:48:388188722[1].gifCJNEDI2HTTP/1.0 200 C
URL	http://www.orbitz.com/App/ViewFlightSearchResults?z=bc0&r=as03/10/2005 17:49:01ViewFlightSearchResults[2].htmlCJNEDI2HTTP/1.1 200 OK Content-Length: 55374 Content
URL	https://www.orbitz.com/img/global/nav/bg_right_bigtabs.gif12/20/2004 05:40:0603/10/2005 17:49:05bg_right_bigtabs[1].gif8R9KCL4NHTTP/1.1 200 OK ETag: "810214-a9-41c6ac06"

Figura 18: Resultado de la exportación del archivo index.dat

Se obtiene una vista de las páginas visitadas, organizadas por fecha, donde la primera visita fue a google en donde hizo las siguientes búsquedas:

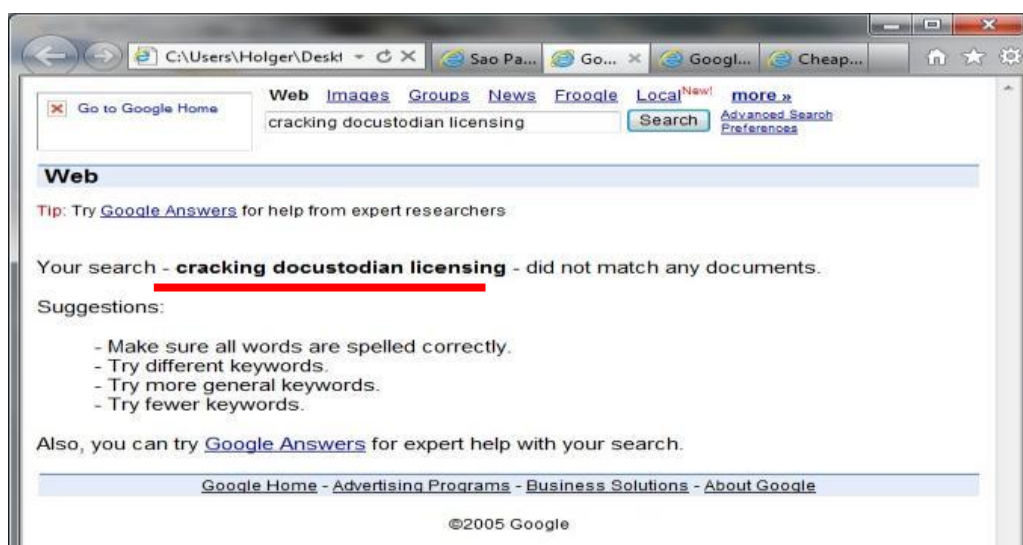


Figura 19: Búsqueda en google “cracking docustodian licensing”

Una búsqueda inusual en donde trata de tener información sobre como vulnerar licencias docustodian que es la empresa encargada de los servidores de la compañía, desde ya podemos sospechar que trata o tratará de realizar un acto ilícito.

Tiempo de acceso: 10/03/2005 17:44:10

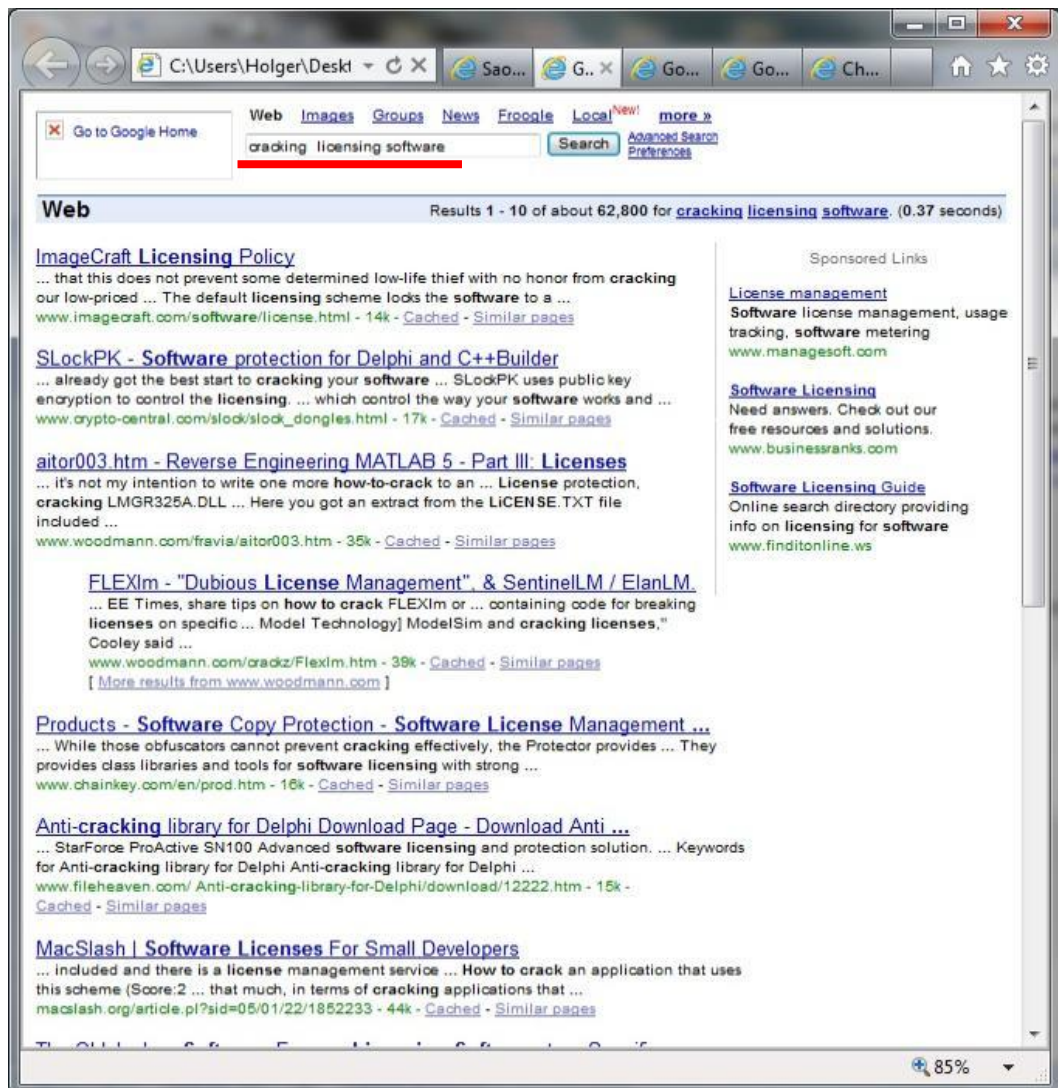


Figura 20: Búsqueda en google con la palabra "cracking licensing software"

En vista que no consiguió información concreta de licencias docustodian, esta vez realizó una búsqueda general de cómo craquear licencias de software.

Tiempo de acceso: 10/03/2005 17:44:21

Entre los resultados de google apareció esta página <http://slashdot.org/> donde encuentra muchos foros informáticos. Que sin realizar ninguna búsqueda o interés específico en la página. Sólo la abrió y cerró.

Tiempo de acceso: 10/03/2005 17:46:02

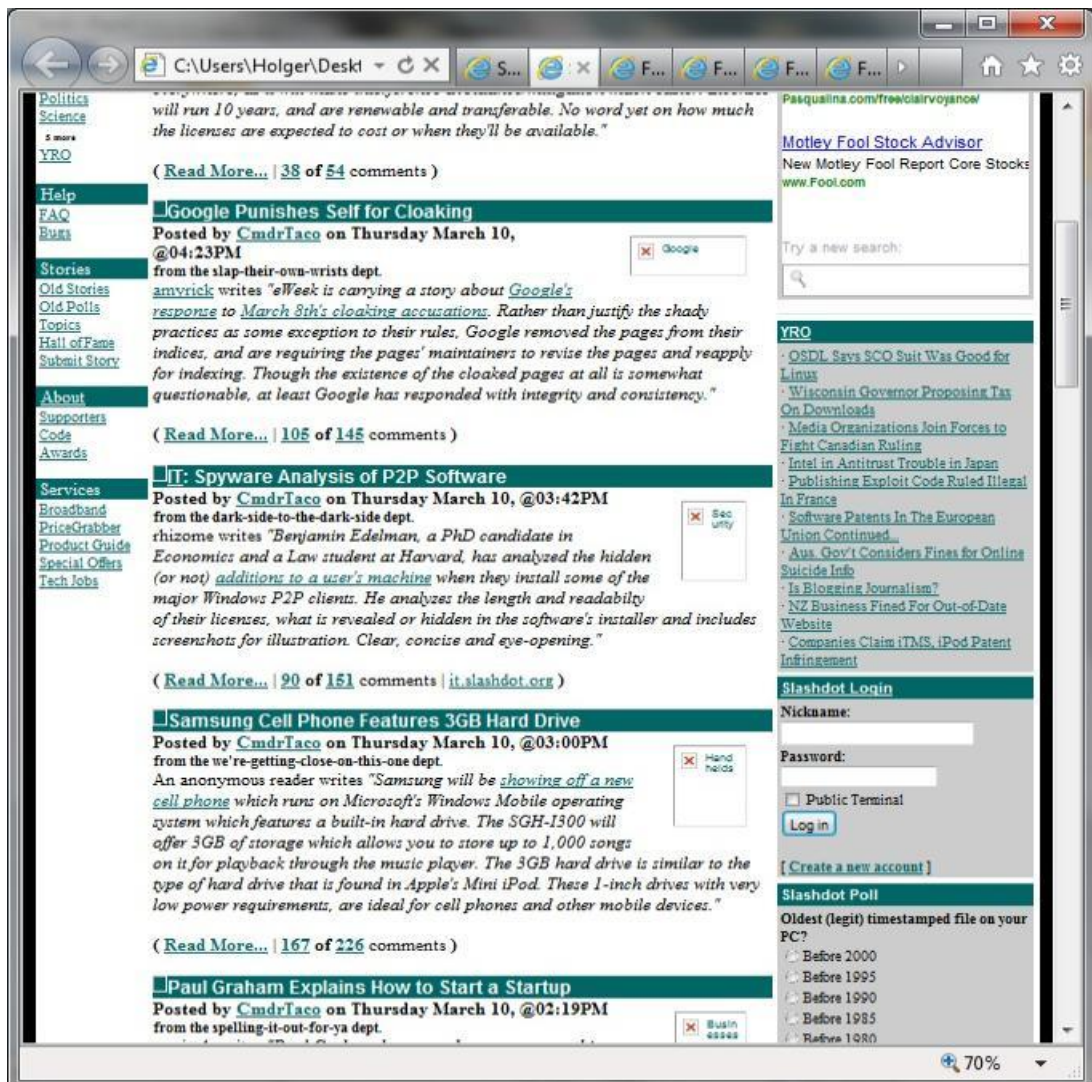


Figura 21: Acceso al sitio web <http://slashdot.org>

Por alguna otra razón “desconocida” hizo búsqueda de hoteles en Sao Paulo – Brasil.

Tiempo de acceso: 10/03/2005 17:47:33

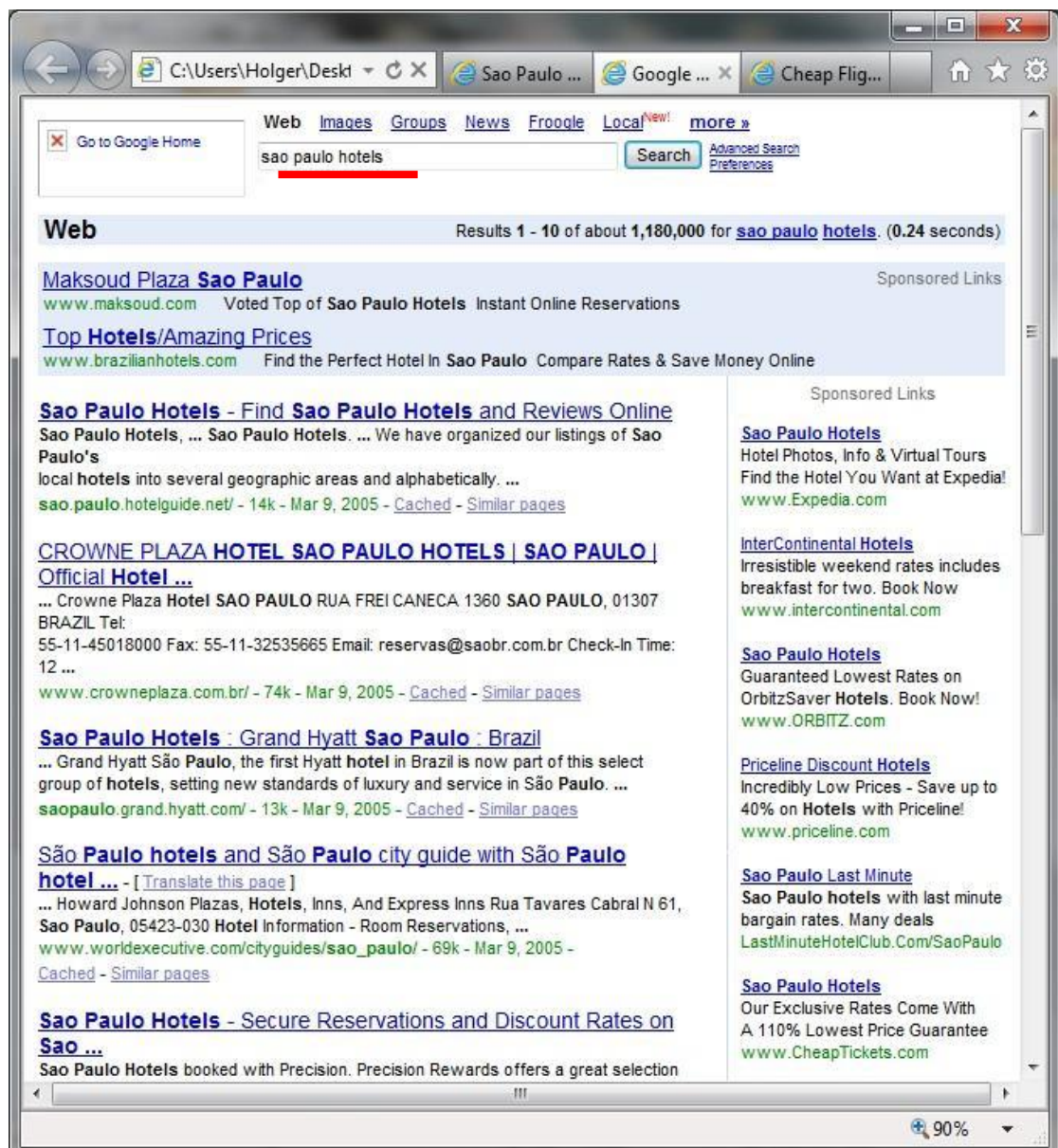


Figura 22: Búsquedas en google de hoteles en Sao Paulo Brasil

El hotel de interés fue Grand Hyatt Sao Paulo.

Tiempo de acceso: 10/03/2005 17:47:41

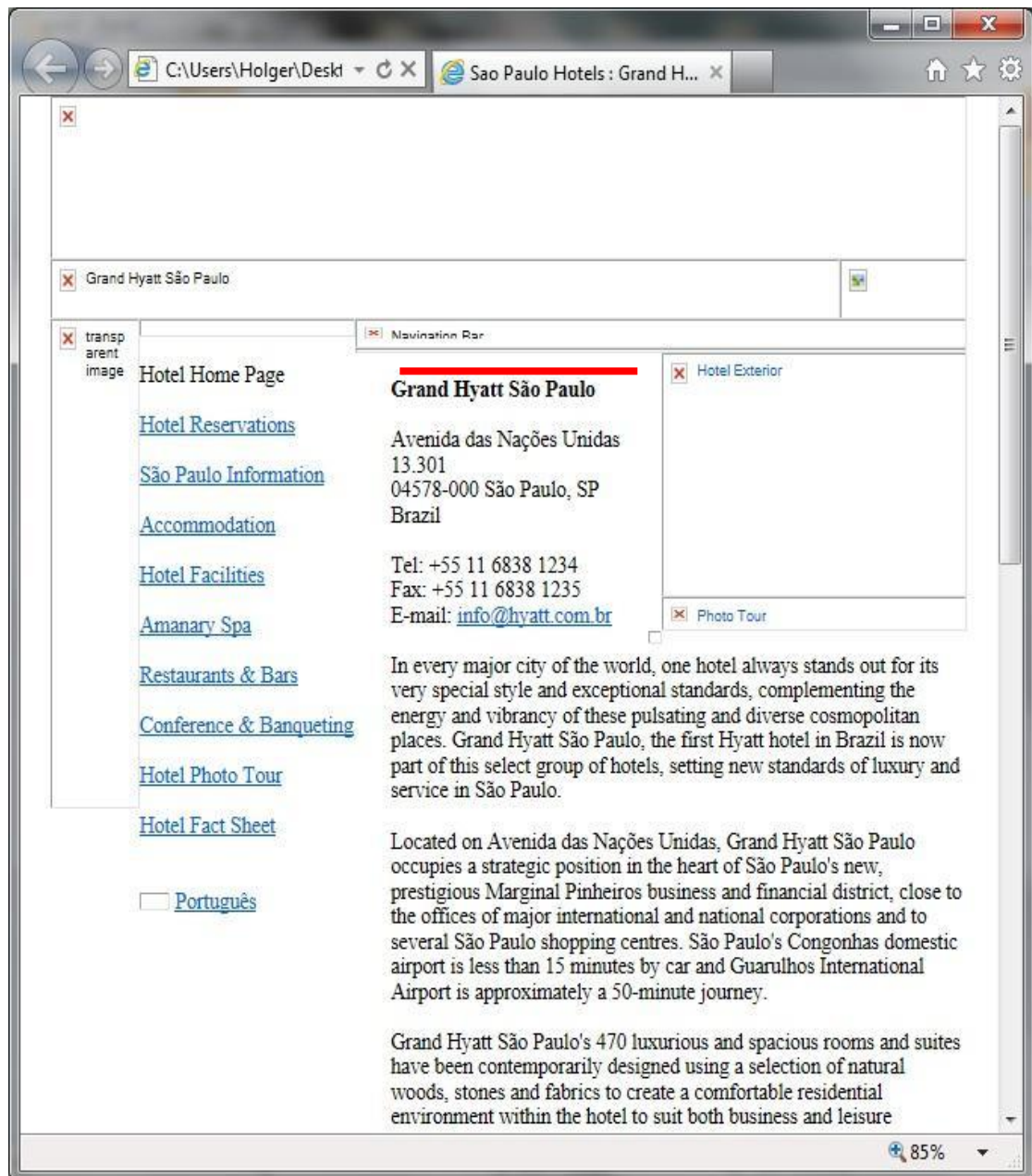


Figura 23: Sitio web del hotel Gran Hyatt Sao Paulo

Posteriormente hizo uso de una página de búsqueda de aerolíneas y vuelos www.orbitz.com, en donde cotizó vuelos desde New York a Sao Paulo – Brasil, fecha de salida el 31 de Marzo del 2005 y retorno el 11 de Abril del mismo año para un solo pasajero.

Fecha de acceso: 10/03/2005 17:48:32



Figura 24: Cotización de vuelos a Sao Paulo

Retomó su búsqueda de software y hardware de hacking, aquí visitó la página de la empresa Barnes and Noble. www.barnesandnoble.com. Dedicada a la venta de libros. En donde indagó sobre códigos de hacking.

Fecha de acceso: 10/03/2005 17:48:44

The screenshot shows the Barnes & Noble website interface. At the top, there's a navigation bar with the B&N logo, a 'FAST & FREE DELIVERY' banner, and links for 'CART' (0 items) and 'CHECK OUT'. Below this is a secondary navigation bar with categories like 'HOME', 'BOOKS', 'USED & OUT OF PRINT', etc. A search bar is present with the text 'Keyword' and a 'SEARCH' button. A promotional banner reads 'Save 40% -- Better Homes & Gardens.' The main content area is titled 'SEARCH RESULTS' and displays 'We found 39 titles with the keywords "code hacking."'. The results are sorted by 'Top Matches'. Three results are visible:

- Code Book: How to Make It, Break It, Hack It, or Crack It** by Simon Singh. Format: Hardcover. Pub. Date: March 2002. B&N Price: \$13.56 (Save 20%).
- iPod & iTunes Hacks: Tips & Tools for Ripping, Mixing, and Burning (Hacks Series)** by Hadley Stern. Format: Paperback. Pub. Date: October 2004. B&N Price: \$19.96 (Save 20%).
- Hardware Hacking: Have Fun while Voiding Your Warranty** by Joe Grand, Ryan Russell, Kevin D. Mitnick (Editor), Kevin Mitnick (Editor). Format: Paperback. Pub. Date: February 2004. B&N Price: \$39.95.

Each result includes a 'Book Cover' placeholder, a 'NEW FROM B&N' badge, and shipping information. The website footer shows a zoom level of 80%.

Figura 25: Visita a la página web barnesandnoble en busca de códigos de hacking

Extendió su búsqueda a Craqueo de Software en donde lucieron los siguientes resultados.

Fecha de acceso: 10/03/2005 17:50:30

The screenshot shows a web browser window displaying search results for the keyword "software cracking". The browser's address bar shows the path "C:\Users\Holger\Desk". The search results are displayed in a list format with the following items:

Rank	Title	Author(s)	Format	Pub. Date	Price	Shipping
1.	Access 2003 VBA: Programmer's Reference	Patricia Cardoza, Graham Seach, Armen Stein, Teresa Hennig	Paperback	April 2004	List Price: \$39.99 B&N Price: \$31.99 (Save 20%) Member Price: \$30.39	Usually ships within 24 hours - Same Day delivery in Manhattan
2.	Programming for Embedded Systems: Cracking the Code	Dreamtech Software Team	Paperback BK&CD-ROM	June 2002	B&N Price: \$49.99 Member Price: \$47.49	Usually ships within 24 hours - Same Day delivery in Manhattan
3.	Cracking the Boards: USMLE Step 2	John Mariani, John J. Mariani	Paperback 2ND	December 2000	B&N Price: \$29.95 Member Price: \$28.45	Usually ships within 24 hours
4.	Multi-Platform Wireless Web Applications: Cracking the Code	Manufactured by Hungry Minds, Dreamtech Software Team	Paperback BK&CD-ROM	November 2001	List Price: \$49.99 B&N Price: \$19.99 (Save 60%) Member Price: \$18.99	Usually ships within 24 hours - Same Day delivery in Manhattan

Figura 26: Búsqueda con palabra clave software cracking

Otra página de su interés fue <http://www.freeseentials.com/>; aquí se encuentra un sinnúmero de seriales de diversos tipos de software.

Fecha de acceso: 10/03/2005 17:49:43

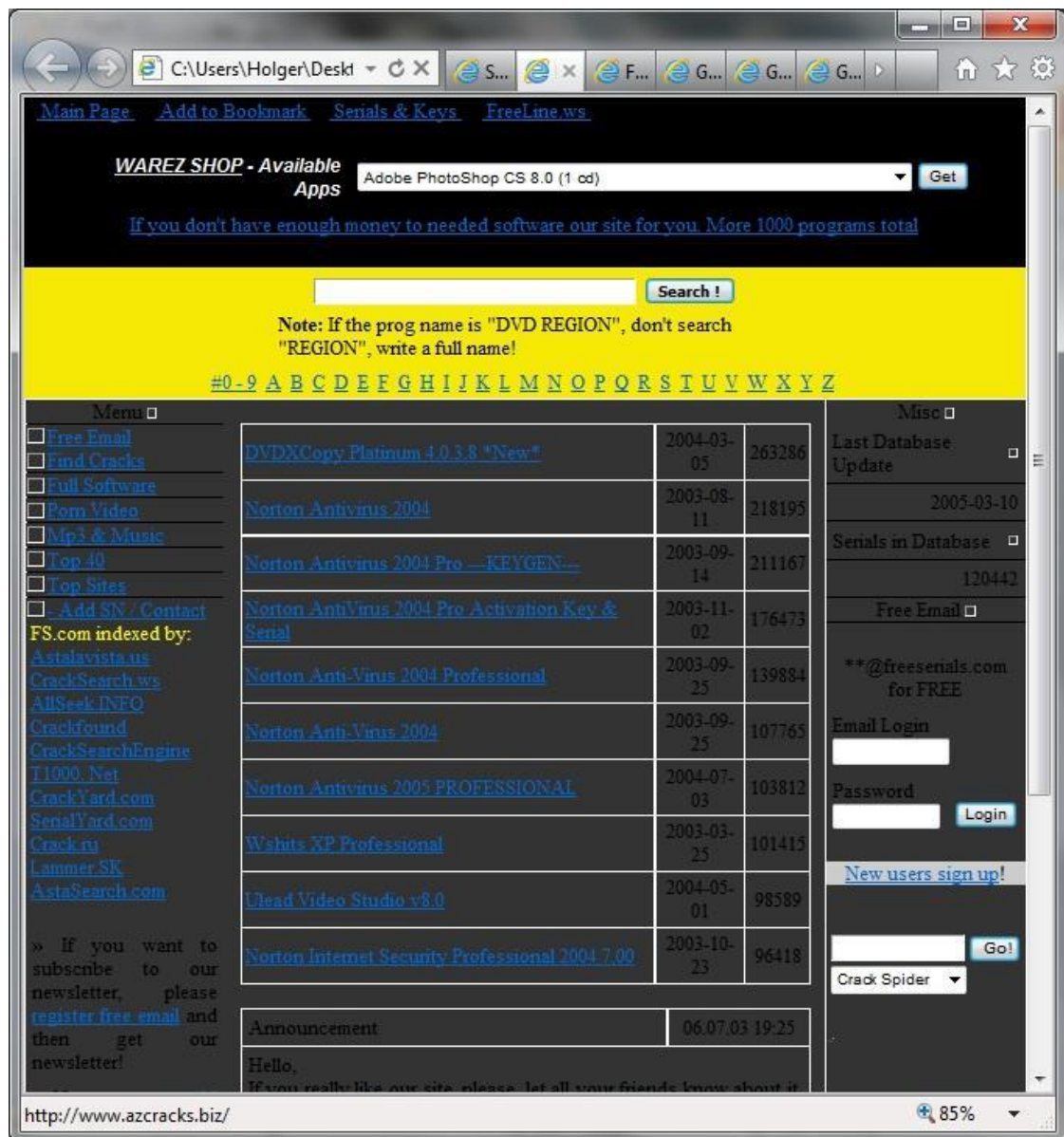


Figura 27: Accediendo al sitio web <http://www.freeseentials.com/>

Como palabra clave de búsqueda utilizó Docustodian, pero no encontró resultados.

Fecha de acceso: 10/03/2005 17:50:58



Figura 28: Búsquedas de licencias de Docustodian

Insistiendo en su exploración ingresó a la página <http://www.findcracks.com/> que acoge aplicaciones para craquear.

Fecha de acceso: 10/03/2005 17:50:44

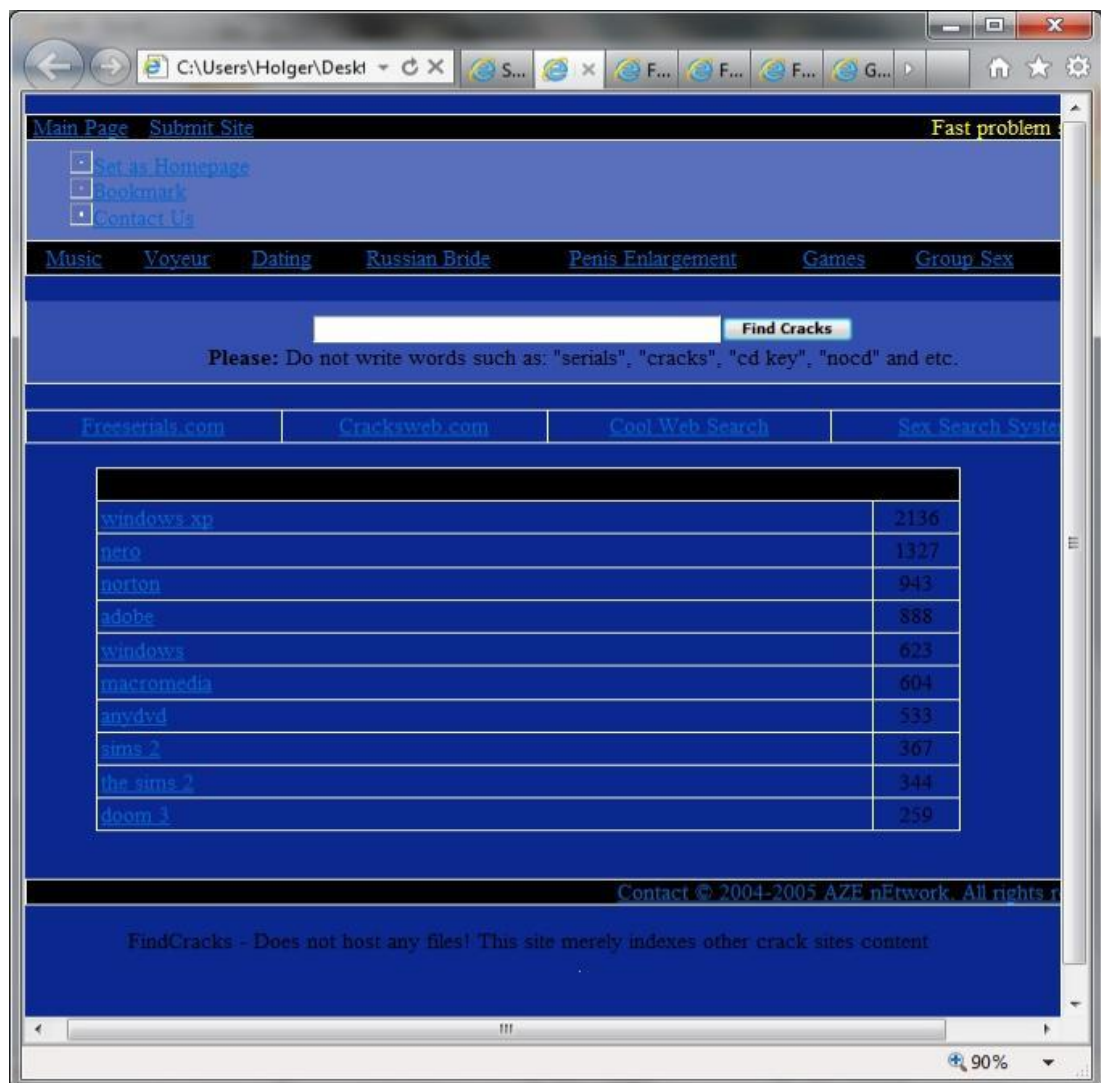


Figura 29: Ingresando a la página <http://www.findcracks.com>

Y al igual que en la anterior página buscó con el nombre de Licencias Docustodian

Fecha de acceso: 10/03/2005 17:52:52

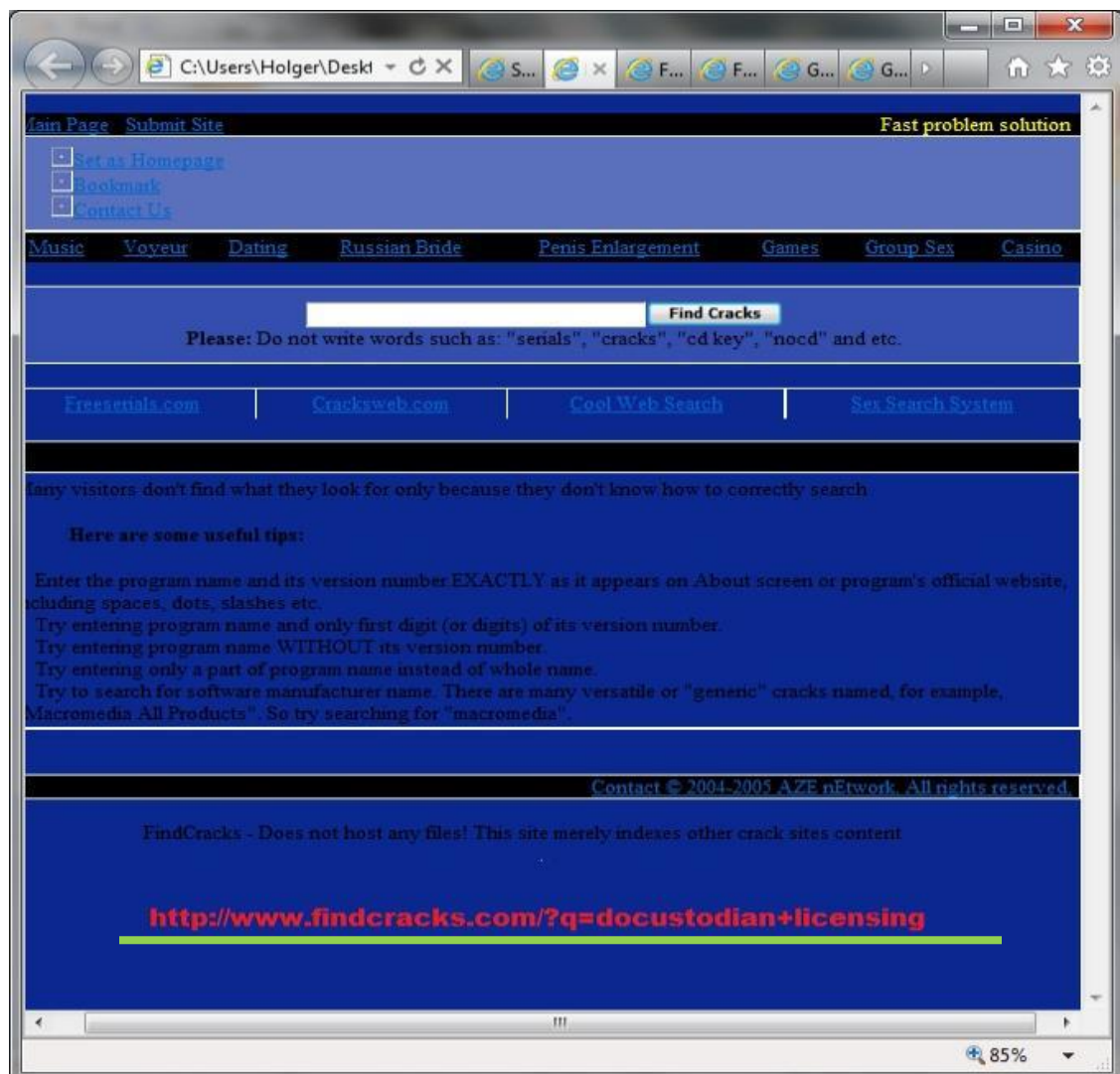


Figura 30: Búsqueda de licencias docustodian

Ya culminada la búsqueda de las herramientas procedió a ingresar a su cuenta de correo electrónico personal cuyo servidor es Hotmail.

La cuenta es: joeschmo1980@hotmail.com, en la imagen podemos observar que tiene un mensaje en su buzón de entrada pero ninguno de entre sus contactos.

Fecha de acceso: 10/03/2005 17:53:35

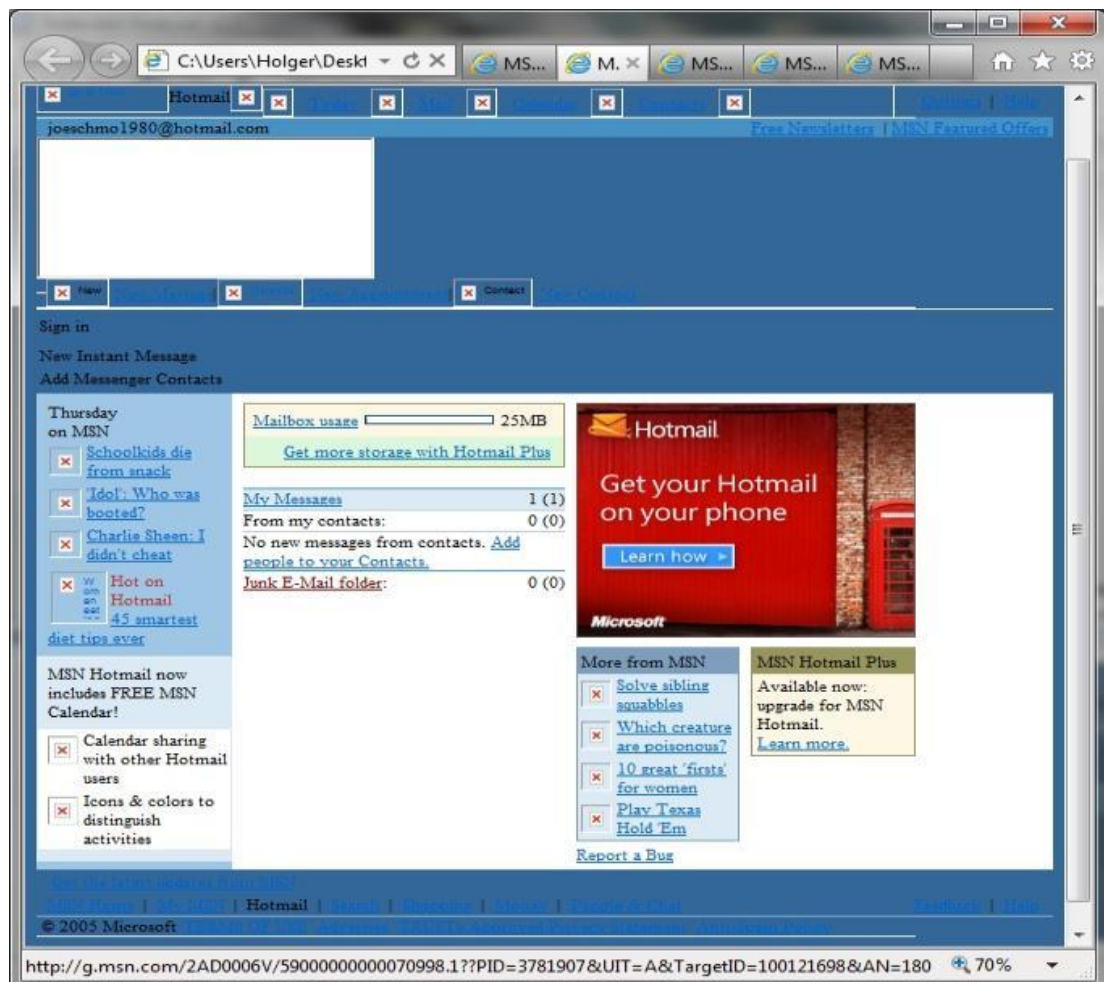


Figura 31: Ventana principal del correo joeschmo1980

Procedió a la composición de un mensaje cuyo contenido es desconocido.

Fecha de acceso: 10/03/2005 17:53:57

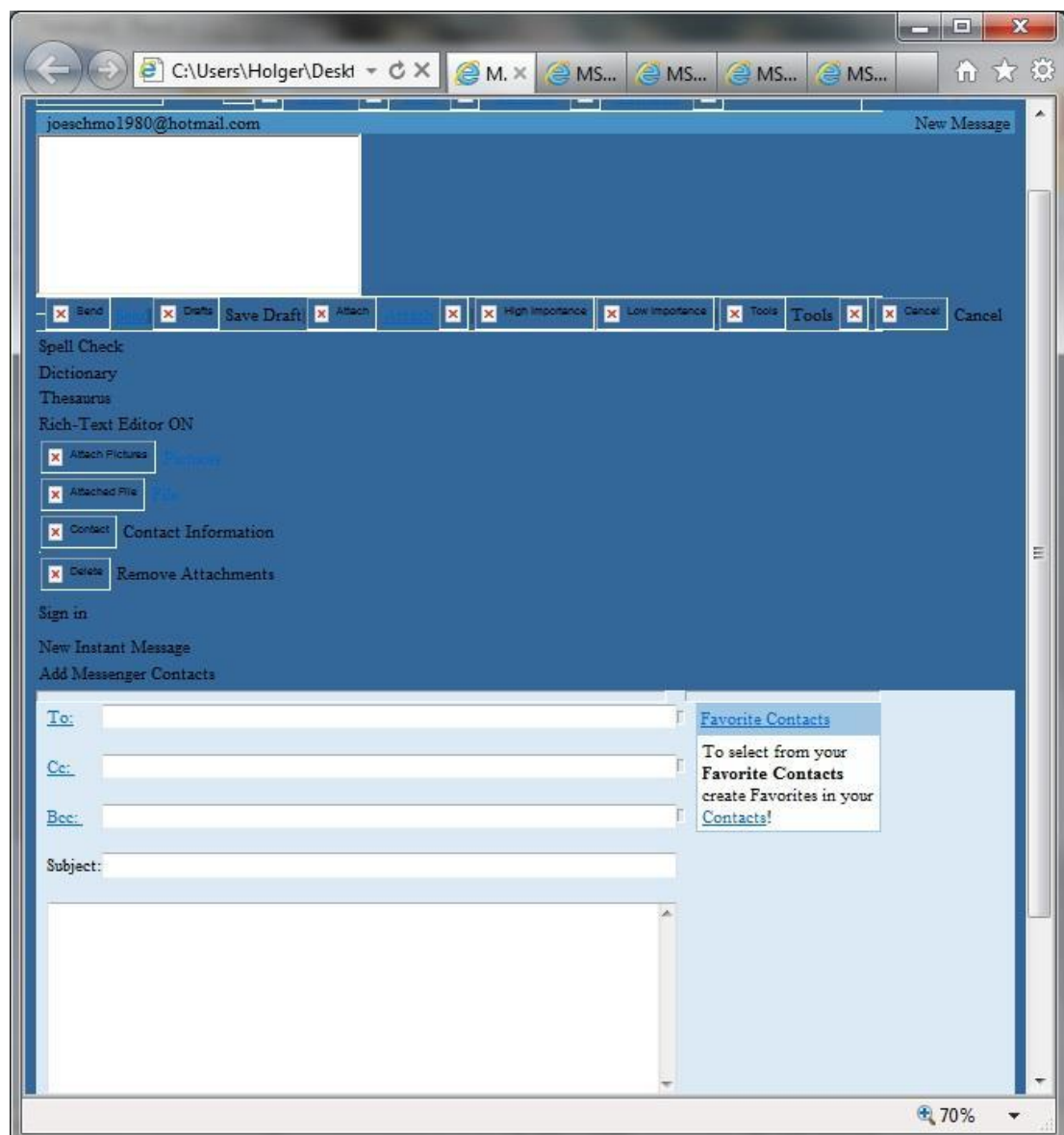


Figura 32: Composición de un correo

Lo que si podemos ver es que el mensaje fue dirigido a tres diferentes cuentas:

yputin1976@gmail...; tomgreen17@rediff...; cgaylej123@gmail...

Fecha de acceso: 10/03/2005 18:08:41

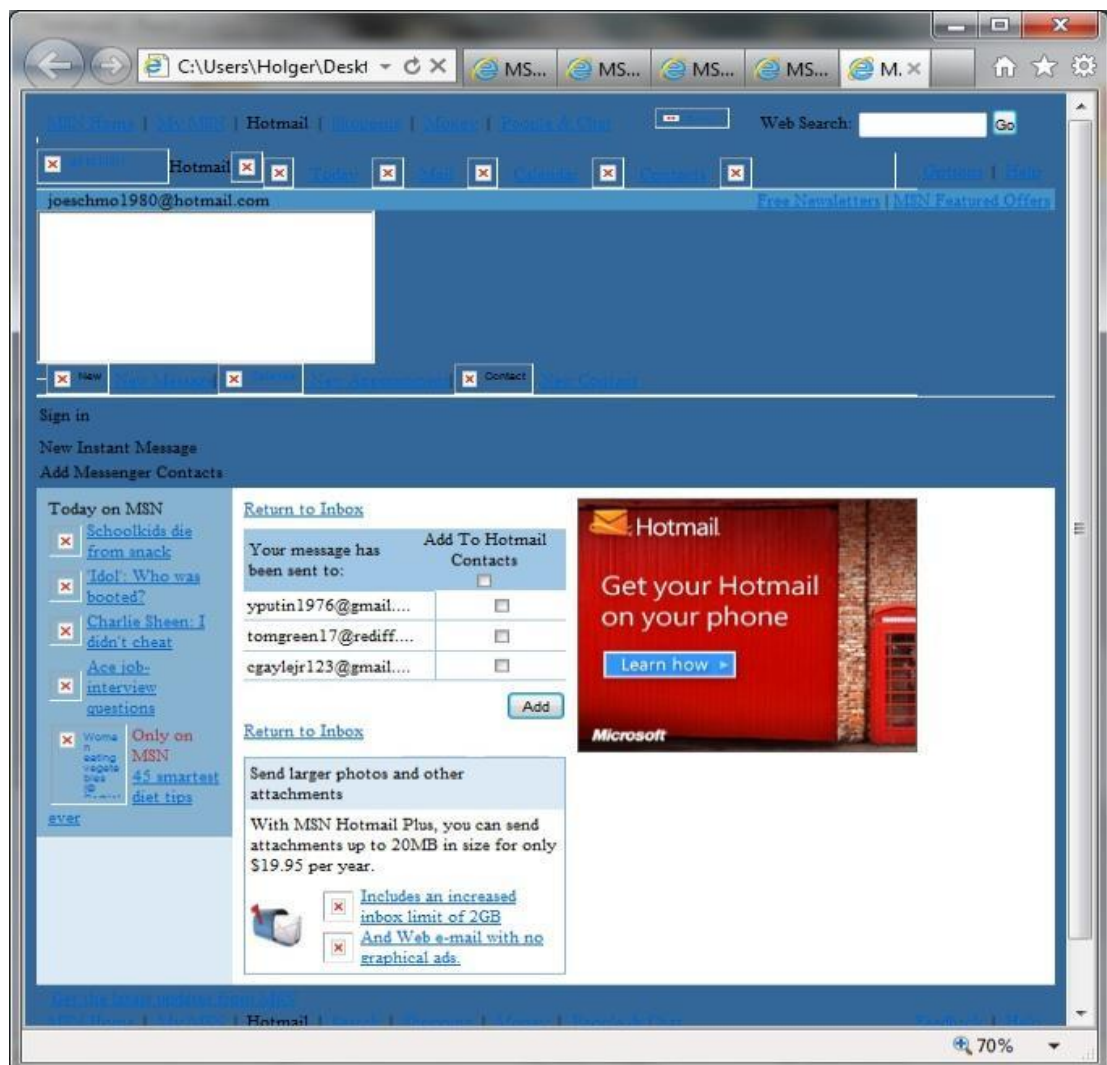


Figura 33: Ventana post-envío del mail

Luego retornó a su buzón de entrada y podemos ver dos mails uno del equipo de Hotmail dándole la bienvenida. Por lo que se puede asegurar que la cuenta fue recién creada el mismo mes de marzo. El otro mensaje es uno de error que llega cuando una cuenta a la que se escribió (entre los tres contactos) no existe.

Fecha de acceso: 10/03/2005 18:08:51

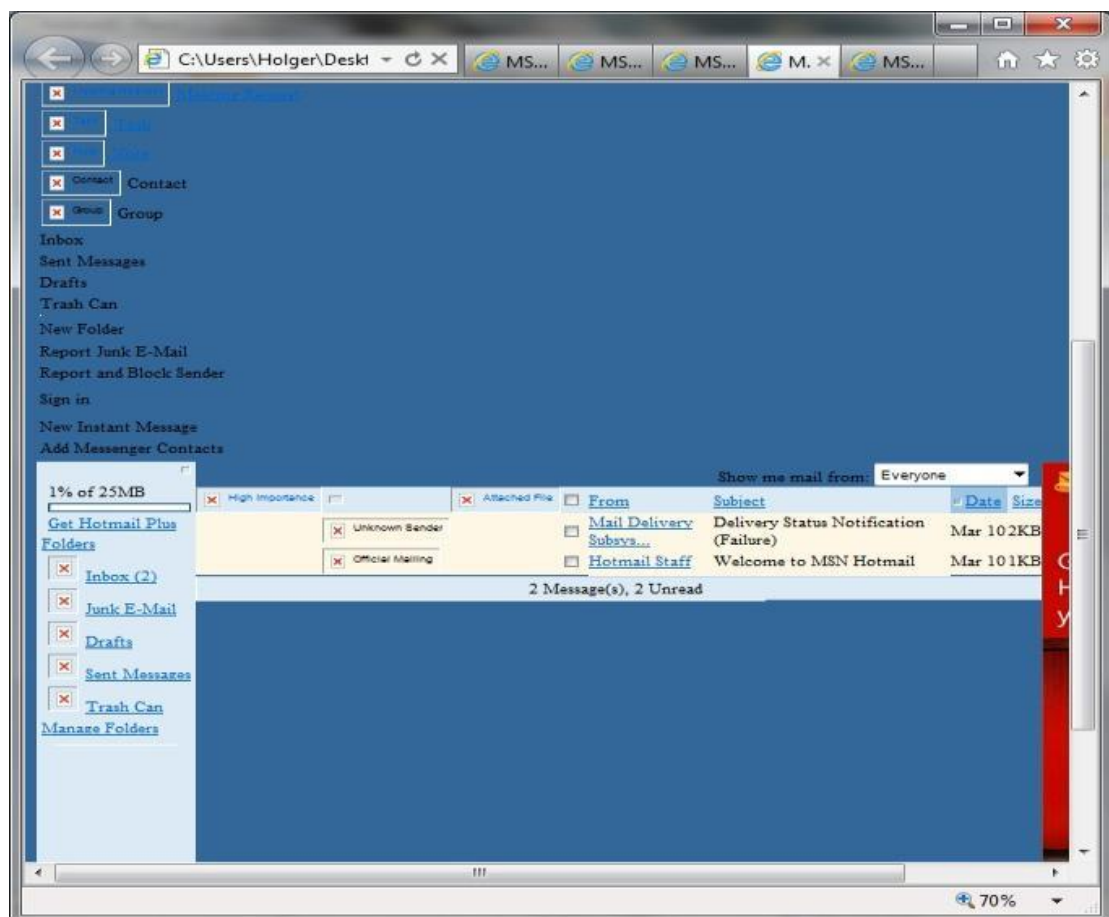


Figura 34: Bandeja de entrada de la cuenta de correo

Por último procedió a borrar sus mails.

Fecha de acceso: 10/03/2005 18:09:02

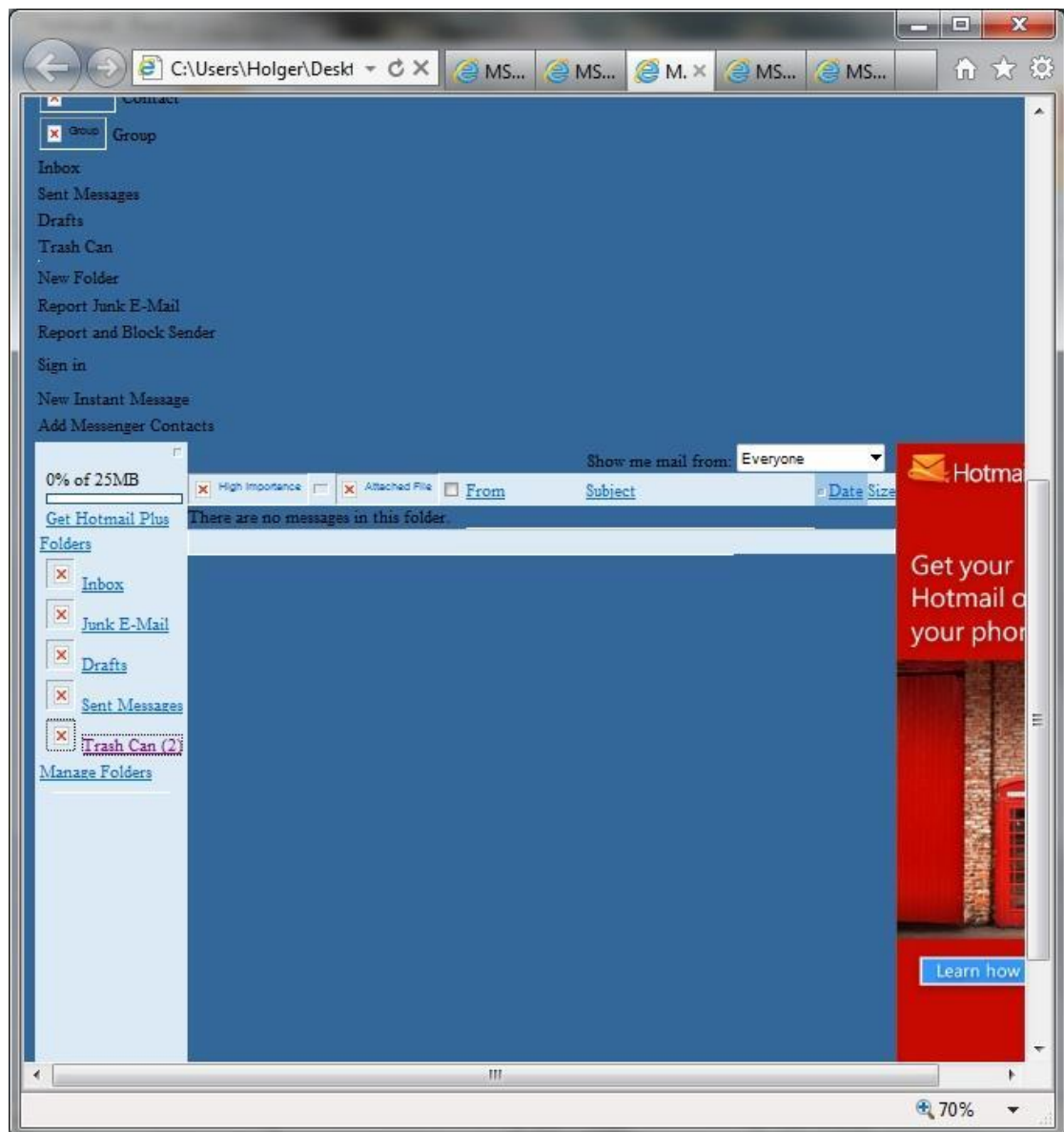


Figura 35: Buzón de entrada vacío.

Esto ha sido lo más relevante encontrado y analizado en el index.dat, entre otros de sus decenas de archivos hay botones e información multimedia propia de las páginas o publicidad inmersa como gif, jpg, png, swf. Información, como la estructura de las diferentes páginas web visitadas (css-hojas de estilo en cascada).



Figura 36: Imágenes encontradas en el index.dat

CONCLUSIONES Y RECOMENDACIONES

De acuerdo al problema escogido para esta investigación, no se cuenta con la suficiente información para inculpar a alguien, tenemos una limitante de información lo que no nos permite ser determinantes, más bien se considera un bajo control en cuanto al sistema de navegación, políticas de conectividad.

Para determinar algo contundente se debería realizar la sustracción de la memoria caché como parte de una investigación con mayor profundidad ya que esta posee información relevante para este caso, como conocer desde qué direcciones ip se realizaron las conexiones y si las imágenes que observamos son correctas a través de la meta data; dependemos de varios factores para poder llegar a la causante del caso: registros de políticas de usuarios, horarios, la zona horaria de la computadora, verificar si la cuenta era la del administrador principal, de no ser así qué tipos de privilegios este posee y realizar la comparación de las cuentas en la base de datos.

Según lo analizado con el index.dat podríamos decir que el señor Joe Schmo no pudo ser el culpable de las descargas ilícitas, debido a que las actividades ilícitas fueron realizadas cuando él se encontraba de vacaciones; más se podría decir que el intruso busca ponerlo como único culpable del posible

fraude, intentando violar toda la seguridad en busca de claves y vulnerabilidades en sitios webs.

Esa sería la única base, la cual no nos resulta sustentable para inculparlo o no.

La empresa debe tener en cuenta las siguientes observaciones:

Con la información asignada para este tipo de investigación, dentro de un proceso de ámbito legal no se puede determinar nada.

En cuanto al ámbito técnico se realiza un planteamiento según lo analizado, por lo que se debe tomar en cuenta las recomendaciones planteadas a continuación.

1. Debemos estar conscientes que el avance tecnológico es diario y como tal debemos tener la responsabilidad de mantenernos actualizados y prevenir cualquier tipo de ataque alineado a la institución, aplicativos y los servicios que desarrollen.
2. Realizar un análisis de vulnerabilidades mensual y un hacking ético anual de la infraestructura de la seguridad informática de la empresa, sobretodo de los servicios que se encuentran publicados en Internet.
3. Avisos de alerta en cuanto a eventos fuera de lo normal.
4. Realizar monitoreo de las actividades de los usuarios.
5. Segmentación física y lógica de la red LAN.

El uso de estas recomendaciones, nos pueden ayudar a tener un mejor control del sistema y de los recursos, y en el caso de tener algún ataque poder determinar con mayor facilidad si es de tipo interno o externo, y a dependiendo de qué vía se está realizando.

IMPLEMENTACIÓN DE POLITICAS DE SEGURIDAD

Debido al incidente ocasionado en la firma de abogados y considerando la falta de información para la investigación, según la infraestructura y labores realizadas dentro de la institución exhortamos elaborar una Política de Seguridad Informática corporativa basada en el estándar ISO 27001, que incluya como mínimo las siguientes recomendaciones con el fin de salvaguardar la información y la seguridad que le ofrecen a sus clientes, las cuales vamos a proceder a detallar:

- 1.** Todo acceso a los servidores o dispositivos de comunicación será con usuario y contraseña de dominio o locales, a fin de realizar procesos de auditoría y acciones ejecutadas sobre los mismos.
- 2.** Las claves de los usuarios de nivel administrador deberán ser actualizadas cada mes y puestas en custodia por el área de seguridad informática.
- 3.** Todo software adquirido por terceros deberá estar certificado bajo la plataforma en la que se desenvuelve la empresa.
- 4.** Toda información confidencial de la empresa deberá ser almacenada de forma cifrada en los servidores.
- 5.** Se deberán realizar auditorías internas cada seis meses para verificar el cumplimiento de las políticas.

6. Se realizarán respaldos de logs de servidores y dispositivos de los dispositivos de comunicación principales.
7. Si alguno de los usuarios se encuentra en periodo vacacional su cuenta debe ser bloqueada.
8. La información debe estar limitada según el tipo de usuario.
9. Todos los ordenadores deberán tener instalado software anti-spyware.
10. Deshabilitar reproductores de CD, ya que a través de estos medios, se puede tomar el control del ordenador de forma sencilla, también sería conveniente tener bajo control las memorias USB. Para evitar problemas con virus o programas para vulnerar el sistema.
11. Todo programa de acceso remoto debe usarse con precaución.
12. Usar un sistema IDS, y así proteger el sistema de amenazas en la conectividad en red.
13. Implementar un control de acceso a red, y así ir corrigiendo los nodos que no cumplan las normativas antes de permitirles el acceso en el sistema de red.
14. Utilización de Herramientas para fortalecer la seguridad como por ejemplo: Sistemas anti-spam, firewall, IDS, antivirus.

15. Utilización de servicios de seguridad como por ejemplo: detectores de intrusos, detectores de vulnerabilidades y consultorías.

BIBLIOGRAFÍA

- (1) Código Integral Penal. Obtenido de <http://www.justiciapenalecuador.com.ec>
- (2) Legislación Vigente y Convenios Internacionales. Obtenido de <http://www.interfutura.ec/blog/delitos-informaticos-en-ecuador-lo-que-vendria-en-la-nueva-legialacion/>
- (3) Nuevo Código Orgánico Integral Penal. Obtenido de <http://www.hoy.com.ec/noticias-ecuador/codigo-penal-incluirea-delitos-informaticos-513190.html>
- (4) Especialistas en Criminología. Obtenido de <http://www.estudiocriminal.com.ar>
- (5) Bryan Carrier, File System Forensic Analysis
- (6) Bakker, Paul. "SearchTools, Indexed Searching in Forensic Images." Sleuth Kit Informer #16