Caso de piratería informática

Jhohan Fabian Mendez Olivar & Rafael José Duque Cardozo

Articulo para optar por el título de ingeniero de sistemas de la Universidad Piloto de Colombia.
Director del trabajo:
Edicson Pineda Cadena, Ingeniero de sistemas.

Resumen –

En el presente documento se expone toda la información necesaria para conocer cómo se realizó el desarrollo de un caso de piratería informática, para la recolección de pruebas que pudiesen ser presentadas ante un ente de legislación legal si se verifica que efectivamente se hizo dicho delito. Todo el proceso se realizó aplicando las bases fundamentales de conocimiento para el desarrollo de delitos informáticos más conocido como informática forense. Se utilizaron herramientas que pudiesen ser aceptadas en los penales colombianos, para el análisis de este tipo de caso. El caso se centra en el hallazgo de tres dispositivos que se sospecha eran utilizados para el robo de datos personales (usuarios, contraseñas) y seriales de tarjetas de crédito para su posterior desfalco.

Palabras Claves – Informática forense, delito informático, hacker, evidencia digital, perito informático.

Abstract –

This document presents all the information necessary to know how the development of a case of computer piracy was carried out, for the collection of evidence that could be presented to a legal entity. The entire process was carried out applying the fundamental bases of knowledge for the development of computer crimes, better known as computer forensics. Tools that could be accepted in Colombian prisons were used for the analysis of this type of case. The case focuses on the discovery of three devices that are suspected of being used to steal personal data (users, passwords) and credit card serials for later embezzlement.

Keywords – Computer forensics, computer crime, hacker, digital evidence, computer expert.

I. INTRODUCCIÓN

La informática forense se puede describir como una ciencia enfocada en la adquisición, preservación y presentación de la información y pruebas recolectadas electrónica y sistemáticamente, para que después estas puedan ser guardadas como un soporte informático. Esta temática se ha vuelto día a día más practicada gracias a él gran apogeo que ha conseguido la tecnología en la sociedad actual permitiendo la resolución de delitos informáticos.

Por ende, los entes gubernamentales como lo son sectores enfocados a la investigación y la resolución de delitos así también los peritos informáticos hacen uso de aplicativos – herramientas y siguen una serie de procedimientos específicos para la recolección de información y pruebas en cualquier aparato tecnológico (como lo es computadoras, Tablet, celulares, servidores, etc.)

La informática forense no está enfocada únicamente a la resolución de delitos informáticos. También puede ser aplicada en diferentes casos de otros ámbitos, ya que muchas de las actividades que se desarrollan actualmente se realizan con la ayuda de dispositivos electrónicos o a través de ellos. (Esto siempre genera datos de uso, ya sea en operaciones manuales o automáticas) dejando un registro de las acciones que se realizaron con dichos dispositivos. También, brinda la posibilidad de combinar esta evidencia digital con el resto de la evidencia física que se recolecta en el desarrollo de un caso. Entre la información que se puede analizar se encuentran los correos electrónicos, chats, historiales, ubicaciones, direcciones Ip, etc. En realidad, existe mucho de donde indagar como también son muchos los tipos de delitos informáticos que existen tales como robo de información personal, espionaje, hackeo de cuentas, violación de privacidad, etc. También existen muchos factores que pueden llegar a influir dentro del desarrollo de un caso al momento del levantamiento de información, como lo son el tiempo que se tiene disponible para el análisis de la información, el tipo de delito que se investiga, el tiempo que se tiene para recolectar dicha información, por lo tanto es fundamental el seleccionar debidamente cuales son los

Documento recibido el 27 de mayo de 2021.

dispositivos que pueden soltar pruebas de valor, aunque muchas veces al momento de realizar el análisis irán apareciendo muchos datos que darán la opción de analizar nuevos dispositivos.

En el caso objetivo del desarrollo de este ejercicio nos encontramos con un caso de piratería, y robo de información confidencial de personas comunes. En donde se le busca el desarrollo por medio de la informática forense ya que el caso directamente está relacionado con un personaje que se hace pasar por el alias de "Mr. Evil", que hace uso de dispositivos electrónicos (Una computadora portátil, una tarjeta de red inalámbrica y una antena casera externa) con lo que se sospecha se utilizaba con fines maliciosos. El cual se corroboro que el personaje se dirigía directamente en su vehículo a puntos estratégicos en los que se encontraran redes de conexión a internet abiertas al público (como lo son los terminales, hospitales, Starbucks, etc.) donde aprovecharía para analizar el tráfico de las redes y así robar números de tarjetas de crédito, nombres de usuario y contraseñas.

En cuanto a la metodología que se utilizó en el desarrollo de este caso se puede hablar las segmentación de trabajo en faces, iniciando desde la identificación del caso, asegurando la información para que en ningún momento pueda ser modificada, luego se hizo énfasis en profundizar e identificar el incidente para poder centrar la búsqueda de la información que sirva como prueba, se realizaron las pertinentes copias de la evidencia, siempre respetando la cadena de custodia, se prepararon las herramientas y técnicas necesarias para el análisis, que posteriormente se realiza sobre la información recogida. Se idéntico el autor del delito y se documentó los pasos realizados y los hallazgos encontrados. Posteriormente se recolecto toda la información y se realizaron los documentos necesarios para su presentación.

Para finalizar, en el desarrollo de este caso se buscó aplicar todos los conocimientos adquiridos en el curso de informática forense, con el fin de poder dar solución a este delito, fundamentando las pruebas de tal manera que si se quisiera llevar a un tribunal estas puedan ser presentadas. Ya que los procedimientos aplicados para la recolección, análisis, desarrollo y posterior informe del caso son los aceptados por dichos entes legales.

II. HERRAMIENTAS UTILIZADAS

A. Autopsy

La interfaz gráfica conocida como Autopsy es un conjunto de herramientas open source para el análisis de imágenes de discos duros, actualmente funciona en la plataforma de Windows como también en OS x.

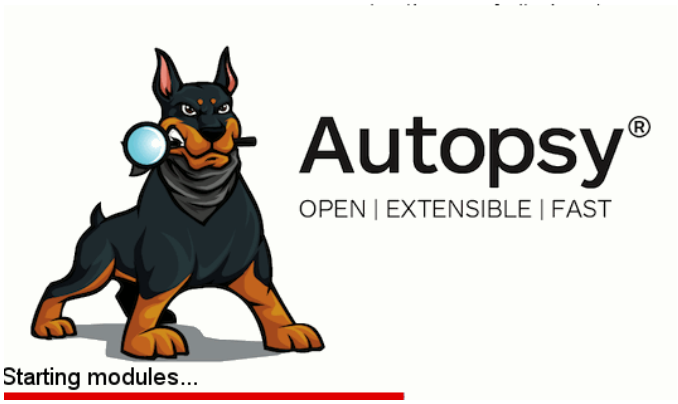

Ilustración 1. Programa autopsy para analizar imágenes de discos. Fuente: autoría propia

La primera impresión al abrir el programa nos regala dos opciones relevantes ya sea, el poder crear un nuevo caso de estudio o abrir uno que ya se haya trabajado en el dispositivo con anterioridad. En donde el caso es una unidad lógica la cual contiene toda la información relacionada con una investigación en desarrollo. Es necesario al crear un nuevo caso ingresar información personal como el nombre, número y persona que estará examinando los datos. Una vez echo eso se procede a ingresa la imagen que se haya creado del disco a analizar, estas imágenes pueden ser creadas con otras herramientas enfocadas en la creación de copias bit a bit.

Luego de ingresa la copia se debe configurar los módulos que se van a utilizar para el análisis los cuales la herramienta ya trae por defecto y brinda opciones de búsqueda que pueden llegar a ser relevantes al momento de analizar una imagen. Estos módulos son:

- **Recent Activity:** Muestra toda la actividad que se realiza recientemente en el dispositivo analizado, entre la información que se selecciona se encuentran los últimos documentos abiertos, los dispositivos externos que fueron conectados, el historial de búsqueda web, las cookies, el historial de descargas, etc.

- **Hash Lookup:** Esta opción permite el añadir las bases de datos locales con sus respectivos valores hash para archivos conocidos. Como lo es la información referente al sistema operativo de la computadora, o las aplicaciones que se encuentran instaladas.

- **Archive Extractor:** Con este módulo se puede conocer los archivos que fueron eliminados del disco, con una función basada en el agrupamiento de metadatos residuales de un disco.

- **Keyword Search:** Se puede agregar una lista de

palabras claves o funciones de expresiones regulares para que se busquen en todo el disco, la herramienta como tal ya trae algunas palabras indexadas básicas para la búsqueda de información relevante como lo es los correos electrónicos, números de cuentas, direcciones ip, etc.

La herramienta autopsy permite la exploración completa del disco, tiene muchas opciones de visualización del contenido, y permite el ingreso de expresiones regulares para la búsqueda detallada de palabras claves al momento de realizar en enfoque de una investigación. Para finalizar el análisis se menciona que las pruebas, resultados pueden ser exportados directamente desde la herramienta, ya que lo permite por medio de un documento en formato HTML, para su correspondiente presentación. Esto apoyando a que los resultados puedan ser visualizados desde cualquier dispositivo sin necesidad de que se tenga instalada la aplicación de autopsy.

B. Ftk imager

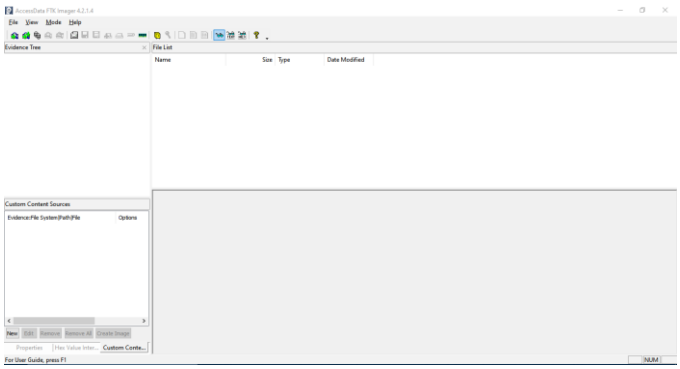

Ilustración 2 programa ftk imager para crear imágenes y copias de discos. Fuente: autoría propia

Forensic Toolkit (FTK) es una plataforma completa para investigaciones digitales, desarrollada para ayudar al trabajo de los profesionales que trabajan en los sectores de seguridad de la información, tecnología y aplicación de la ley.

A través de tecnologías innovadoras utilizadas en filtros y el motor de indexación, se puede acceder rápidamente a la evidencia relevante de los casos de investigación, lo que reduce drásticamente el tiempo para realizar el análisis.

Las herramientas informáticas forenses deben mantenerse actualizadas para abordar problemas como el aumento del tamaño de los discos duros y el uso de cifrado para reducir el tiempo necesario para realizar la adquisición y el análisis de datos.

AccessData tiene dos versiones de la plataforma:

FTK forensics: esta versión de FTK, que se utilizó en esta investigación, tiene la capacidad de realizar la adquisición y análisis de los dispositivos digitales como discos duros de computadoras, unidades USB, dispositivos de memoria flash, teléfonos inteligentes, tabletas y otros medios digitales. Su enfoque está relacionado con un proceso llamado análisis forense informático post-mortem, que ocurre cuando la computadora se apaga.

AD Enterprise: en general, AD Enterprise tiene las mismas características que la versión forense de FTK, además de la capacidad de analizar varias computadoras en su empresa simultáneamente. Otra característica importante de esta versión es la capacidad de adquirir y analizar datos volátiles, como RAM. El proceso de investigación es totalmente confidencial y el usuario investigado no tendrá conocimiento del análisis, incluso si se realiza a través de la red y con el equipo objetivo en uso.

Este aplicativo sirve para realizar copias y deja visualizar previamente datos de un disco, dichas copias llegar a ser idénticamente perfectas ya que se realiza un copiado bit a bit, esto permite trabajar con una copia que es prácticamente la original. Se recomienda el uso de un bloqueador al momento de trabajar con la aplicación y al instante de realizar una copia, para que no se pueda llegar a alterar la información.

Las copias bit a bit previenen la manipulación de las pruebas originales, como también se evita que se pueda llegar a cambiar algo intencional o accidentalmente en la información original, esta copia forense es tan idéntica que incluye el espacio en blanco que contenga el disco original, permitiendo que con el uso de otras herramientas se pueda llegar a recuperar información eliminada, o particiones ocultas.

III. ETAPAS

El análisis forense digital es un grupo de procedimientos para la recolección y análisis exhaustivo de datos. Por el cual se cuida con tal delicadeza la información para no llegar a realizar ningún tipo de cambio en esta cuando se está realizando su análisis. Para que después pueda ser presentada como prueba por algún incidente o delito en un marco legal. El delito o incidente es un evento en el cual se vulnera la seguridad de un sistema, por ende, se busca entender que fue lo que realmente paso en dicho delito.

Esta clase de procedimientos tomaron fuerza en la última década, gracias al masivo uso de tecnologías y dispositivos de información digital en la sociedad, actualmente se aplica en muchos casos de estudio en donde suceden delitos financieros, acoso, pedofilia, robo de información personal, suplantación de identidad en la web, ciberterrorismo, etc.

El análisis forense se compone de cinco fases o etapas las cuales son necesarias cumplir con dicho orden ya que permiten mantener el estudio de un caso estructuradamente, con el fin de dar veracidad y rigor a las pruebas. A continuación, se profundizará las etapas del análisis forense:

1. ADQUISICIÓN

En esta etapa es donde se debe realizar las debidas copias de seguridad de toda información que se sospecha puede estar vinculada a un caso en investigación. Estando seguro de no llegar a modificar dicha información es recomendable casi obligatorio el crear copias de bit a bit con herramientas y dispositivos adecuados. Destacando que estas copias son necesarias ya que abren la posibilidad de recuperar archivos borrados, como también particiones del disco ocultas, que como resultado deja una imagen del mismo tamaño que tiene el disco que se está estudiando.

En cuanto a las pruebas físicas como los son los dispositivos de hardware (discos duros) se deben marcar con fecha y hora de revisión, para posteriormente aislarlos y para que no se lleguen a dañar.

La volatilidad de las muestras del tipo de información que se maneja produce que se tenga que seguir una regla fundamental que es, por ejemplo: Primero recolectar la información de las áreas más volátiles como lo son la cache y por último la información que se encuentra en el soporte de almacenamiento como lo son los documentos y archivos.

2. PRESERVACIÓN

En esta etapa se garantiza que la información recolectada no se toque, ya que podría producir cambios en esta o daños. Por lo tanto, nunca se debe realizar el análisis sobre la muestra de información incautada. Para eso se realizan las copias bit a bit, entonces, sobre estas copias es que se debe realizar el debido proceso.

3. ANÁLISIS

La etapa más importante, ya que una vez se consigue y se preserva la información se llega a la etapa técnica que es el análisis de dicha información, donde se deben utilizar herramientas específicas para el análisis forense tanto software como hardware. El resultado tiende a variar dependiendo de las herramientas con las que se analice la información, como también las habilidades y experiencia que tenga el sujeto que realiza dicho análisis.

4. DOCUMENTACIÓN

Se recomienda en esta etapa el ir anotando cada uno de los pasos, y acciones que se realizaron en su debido momento de ocurrencia, esto permitirá el poder enfocarnos en apartados que al momento de análisis llamaron bastante la atención. Se debe citar y adjuntar la información obtenida relacionándola directamente con las pruebas y las tareas que se realizaron para obtener dichas pruebas.

5. PRESENTACIÓN

Existen muchas formas de poder llegar a presentar dichas evidencias obtenidas, Principalmente se tiene que hacer entrega de un informe ejecutivo en donde se muestre las pruebas más importantes de forma resumida y ponderada por su criterio en la etapa de investigación, sin muchos tecnicismos. También se debe entregar un informe técnico en el cual se tiene que detallar con mayor precisión todo el análisis realizado.

IV. DESARROLLO DEL CASO

La evidencia digital es una muestra que los investigadores procesan. Una cosa para considerar es que la información digital obtenida no debe cambiarse a los datos originales del disco, de lo contrario la prueba no será válida. Por lo tanto, cada investigador debe verificar o estudiar estas copias más repetidamente para hacerlas iguales a las copias en disco. En el caso de los CD delictivos o maliciosos, se procesarán varias tecnologías a lo largo del proceso y sus hashes MD5 se compararán constantemente para verificar la integridad de la evidencia subyacente. A continuación, se mostrará la evidencia digital actual, que forma parte del marco legal que se tratará en este caso. Es por ello por lo que, para obtener los resultados del caso, se utilizó una imagen DD (en siete partes: 1, 2, 3, 4, 5, 6, 7, 8 y notas) y una imagen EnCase (segunda parte) de la computadora abandonada; Estas imágenes se estudiaron mediante el programa que se menciona en la sección de Herramientas Utilizadas (Autopsy y Forensic Toolkit (FTK)).

Al momento de iniciar el análisis se prepararon las herramientas y técnicas que conforman el entorno de trabajo propuesto, estas herramientas fueron fundamentales para esta investigación, ya que Forensic Toolkit o FTK, permitió crear una copia BIT a BIT a la computadora del sospechoso (Mr. Evil); Hay que tener en cuenta que para estos casos lo esencial y primordial que se realiza es duplicar la evidencia principal para poder trabajar con dicha copia. La siguiente herramienta que se utilizó (Autopsy), permitió la verificación, escaneo y consulta de todas la

información, movimientos y rastros que el sospechoso (Mr. Evil) fue dejando en los registros del sistema; Gracias a estas herramientas se permite confirmar y verificar dichas sospechas en contra de Mr. Evil, dando certeza y culpabilidad al sospechoso mencionado.

Program Name	Install Date/Time	Source File	Tags
123 Write All Stored Passwords	2004-08-20 15:13:08 COT	/img_SCHARDT/vol_vol2/WINDOWS/system32/config/software	
AddressBook	2004-08-19 22:31:51 COT	/img_SCHARDT/vol_vol2/WINDOWS/system32/config/software	
Anonymizer Bar 2.0 (remove only)	2004-08-20 15:05:09 COT	/img_SCHARDT/vol_vol2/WINDOWS/system32/config/software	
Branding	2004-08-19 22:37:31 COT	/img_SCHARDT/vol_vol2/WINDOWS/system32/config/software	
Cain & Abel v2.5 beta45	2004-08-20 15:05:58 COT	/img_SCHARDT/vol_vol2/WINDOWS/system32/config/software	Bookmark
Connection Manager	2004-08-19 22:21:41 COT	/img_SCHARDT/vol_vol2/WINDOWS/system32/config/software	
CuteFTP	2004-08-20 15:09:02 COT	/img_SCHARDT/vol_vol2/WINDOWS/system32/config/software	
CuteHTML	2004-08-20 15:09:03 COT	/img_SCHARDT/vol_vol2/WINDOWS/system32/config/software	
DirectAnimation	2004-08-19 22:31:52 COT	/img_SCHARDT/vol_vol2/WINDOWS/system32/config/software	
DirectDrawEx	2004-08-19 22:31:32 COT	/img_SCHARDT/vol_vol2/WINDOWS/system32/config/software	
Ethereal 0.10.6 v.0.10.6	2004-08-27 15:29:19 COT	/img_SCHARDT/vol_vol2/WINDOWS/system32/config/software	
Faber Toys v.2.4 Build 216	2004-08-20 15:07:25 COT	/img_SCHARDT/vol_vol2/WINDOWS/system32/config/software	
Fontcore	2004-08-19 22:31:32 COT	/img_SCHARDT/vol_vol2/WINDOWS/system32/config/software	
Forté Agent	2004-08-20 15:08:19 COT	/img_SCHARDT/vol_vol2/WINDOWS/system32/config/software	
ICW	2004-08-19 22:31:51 COT	/img_SCHARDT/vol_vol2/WINDOWS/system32/config/software	
IE40	2004-08-19 22:31:32 COT	/img_SCHARDT/vol_vol2/WINDOWS/system32/config/software	
IE4Data	2004-08-19 22:31:32 COT	/img_SCHARDT/vol_vol2/WINDOWS/system32/config/software	
IE5BAKEX	2004-08-19 22:31:32 COT	/img_SCHARDT/vol_vol2/WINDOWS/system32/config/software	
IEData	2004-08-19 22:31:32 COT	/img_SCHARDT/vol_vol2/WINDOWS/system32/config/software	
Look@LAN 2.50 Build 29	2004-08-25 15:56:11 COT	/img_SCHARDT/vol_vol2/WINDOWS/system32/config/software	
MPlayer2	2004-08-19 23:04:36 COT	/img_SCHARDT/vol_vol2/WINDOWS/system32/config/software	
Microsoft NetShow Player 2.0	2004-08-19 23:04:36 COT	/img_SCHARDT/vol_vol2/WINDOWS/system32/config/software	
MobileOptionPack	2004-08-19 22:31:32 COT	/img_SCHARDT/vol_vol2/WINDOWS/system32/config/software	
NetMeeting	2004-08-19 22:31:52 COT	/img_SCHARDT/vol_vol2/WINDOWS/system32/config/software	
Network Stumbler 0.4.0 (remove only)	2004-08-27 15:12:15 COT	/img_SCHARDT/vol_vol2/WINDOWS/system32/config/software	
OutlookExpress	2004-08-19 22:31:51 COT	/img_SCHARDT/vol_vol2/WINDOWS/system32/config/software	
PCHealth	2004-08-19 22:32:06 COT	/img_SCHARDT/vol_vol2/WINDOWS/system32/config/software	
Powertoys For Windows XP v.1.00.0000	2004-08-20 15:12:43 COT	/img_SCHARDT/vol_vol2/WINDOWS/system32/config/software	
SchedulingAgent	2004-08-19 22:31:32 COT	/img_SCHARDT/vol_vol2/WINDOWS/system32/config/software	
WebFldrs XP v.9.50.5318	2004-08-19 23:04:50 COT	/img_SCHARDT/vol_vol2/WINDOWS/system32/config/software	
WinPcap 3.01 alpha	2004-08-27 15:15:19 COT	/img_SCHARDT/vol_vol2/WINDOWS/system32/config/software	
mIRC	2004-08-20 15:10:04 COT	/img_SCHARDT/vol_vol2/WINDOWS/system32/config/software	

Ilustración 3 Aplicaciones instaladas en la computadora. Fuente: autoría propia
Herramienta Utilizada: Autopsy

Se inicia la investigación buscando en los programas instalados de la computadora como se muestra en la *Ilustración 3*, se encontraron varias aplicaciones en el sistema operativo que hacen énfasis a la piratería, tales como: Caín y Abel, Ethereal, 123 Write All Stored Password, Anonymizer, CuteFTP, Look&LAN y NetStumbler. ya que la mayoría de estas tienen como función analizar el tráfico de las redes, burlando su seguridad.

```
[Perfil]
Compilación = "32.560"
FullName = "Mr Evil"
EMailAddress = "whoknowsme@sbcglobal.net"
EMailAddressFormat = 0
ReplyTo = ""
Organización = "N / A"
DoAuthorization = 1
SavePassword = 1
Nombre de usuario = "whoknowsme@sbcglobal.net"
Contraseña = "84106D94696F"
SMTPLoginProtocol = 2
SMTPUsePOPLogin = 0
SMTPUserName = "whoknowsme@sbcglobal.net"
SMTPSavePassword = 1
SMTPPassword = "84106D94696F"
Está registrado = 0
IsRegistered19 = 0
IsLicensed = 3
Clave = ""
EnableSupportMenu = 0
```

Ilustración 4 Correo electrónico SMTP del sujeto. Fuente: autoría propia
Herramienta Utilizada: Autopsy

En la *Ilustración 4* se evidencia la dirección del servidor de correo electrónico SMTP, (Protocolo para transferencia simple de correo), siendo que el hacker de sombrero negro Mr. Evil, (responsable sobre el robo de información personal de terceros), fue el que utilizo dicho correo electrónico para él envió de la información robada.

```
[Servidores]
NewsServer = "news.dallas.sbcglobal.net"
MailServer = "smtp.sbcglobal.net"
POPServer = ""
NNTPPort = 119
SMTPPort = 25
POPPort = 110
SMTPServerPort = 25
```

Ilustración 5 Configuraciones del servidor de noticias en el que publicaba el sujeto en cuestión. Fuente: autoría propia
Herramienta Utilizada: Autopsy

De acuerdo con la *Ilustración 5* expuesta, se puede identificar las configuraciones NNTP, (Protocolo de transporte de noticias en red) que utilizaba Mr. Evil en servidor "news.dallas.sbcglobal.net" para leer y publicar artículos de noticias sobre métodos y formas de hackeo de las redes de internet en zonas públicas.

«alt«.2600.cardz.dbx
«alt«.2600.cardz.dbx-slack
«alt«.2600.codez.dbx
«alt«.2600.codez.dbx-slack
«alt«.2600.crackz.dbx
«alt«.2600.crackz.dbx-slack
«alt«.2600.dbx
«alt«.2600.dbx-slack
«alt«.2600.hackerz.dbx
«alt«.2600.hackerz.dbx-slack
«alt«.2600.moderated.dbx
«alt«.2600.moderated.dbx-slack
«alt«.2600.phreakz.dbx
«alt«.2600.phreakz.dbx-slack
«alt«.2600.programz.dbx
«alt«.2600.programz.dbx-slack

Ilustración 6 grupos de noticias en los que el sujeto estaba registrado. Fuente: autoría propia
Herramienta Utilizada: Autopsy

Conociendo que el sujeto hacia uso de un servidor de noticias se quiso averiguar a qué grupos estaba inscrito para saber el tipo de información que este buscaba en la red. En la presente *Ilustración 6* se evidencia que Mr. Evil estaba suscrito a grupos de noticias donde exportaba información para exponer sus fechorías.

```
privado = 1,1,1,1
otro = 1,1,1,1,1,1,1
pos = 20,20
[mirc]
usuario = Mini Yo
email=none@of.ya
nick = Sr.
anick = mrevilrulez
host = Undernet: EE. UU., CA, LosAngeles SERVIDOR: losangeles.ca.us.undernet.org: 6660 GRUPO: Undernet
```

Ilustración 7 configuración del sujeto en el programa de chat MIRC. Fuente: autoría propia
Herramienta Utilizada: Autopsy

Esta *Ilustración 7* resume la configuración del usuario Mr. Evil en el distinguido programa de IRC (Internet Relay Chat) llamado MIRC. Que se mostraban cuando dicho sujeto estaba en línea y en un canal de chat comunicándose con personas anónimas en web para planear y compartir información y métodos de hacer delitos informáticos.

```
Session Start: Fri Aug 20 10:54:55 2004
Session Ident: m5tar
[10:54] Session Ident: m5tar (~blo@80.78.130.154)
[10:54] <m5tar>  └3 Looking for └12LOVE └7 FUN └5 SEX └3 .what are you waiting for? it is FREE ..└7 http://fly.to/girls4loving
Session Close: Fri Aug 20 11:00:08 2004
```

Ilustración 8 log del ingreso del usuario a un canal de chat IRC. Fuente: autoría propia
Herramienta Utilizada: Autopsy

De acuerdo con la *Ilustración 8* se puede visualizar y verificar las sesiones registradas por este programa IRC (Internet Relay Chat), el cual mantenía Mr. Evil en la computadora.

«interception«	/img_SCHARDT/vol_vol2/Documents and Settings/Mr. Evil/interception
«interception«	/img_SCHARDT/vol_vol2/Documents and Settings/Mr. Evil/interception
«interception«	/img_SCHARDT/vol_vol2/Documents and Settings/Mr. Evil/interception
«interception«	/img_SCHARDT/vol_vol2/Documents and Settings/Mr. Evil/interception
«interception«-slack	/img_SCHARDT/vol_vol2/Documents and Settings/Mr. Evil/interception-slack
«interception«-slack	/img_SCHARDT/vol_vol2/Documents and Settings/Mr. Evil/interception-slack
«interception«-slack	/img_SCHARDT/vol_vol2/Documents and Settings/Mr. Evil/interception-slack

Ilustración 9 archivo en donde se guardaba el tráfico de las redes atacadas por el sujeto. Fuente: autoría propia
Herramienta Utilizada: Autopsy

Se pudo comprobar que estaba instalado (Ethereal), un popular programa de "rastreo" que se puede utilizar para interceptar paquetes de Internet por cable e inalámbricos. Cuando los paquetes TCP se recopilan y se vuelven a ensamblar, el directorio de almacenamiento predeterminado de los archivos de este programa es el directorio users \ My Documents, donde se encontró un archivo con el nombre inteception como se muestra en la *ilustración 9* que contenía todo el tráfico interceptado de las redes que el sujeto atacaba.

```
Accept: */*
UA-OS: Windows CE (Pocket PC) - Version 4.20
UA-color: color16
UA-pixels: 240x320
UA-CPU: Intel(R) PXA255
UA-Voice: FALSE
Referer: http://mobile.msn.com/hm/folder.aspx?ts=1093601294&fts=1093566459&folder=ACTIVE&msg=0
UA-Language: JavaScript
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)
Host: mobile.msn.com
Connection: Keep-Alive
```

Ilustración 10 características de la computadora de la víctima. Fuente: autoría propia
Herramienta Utilizada: Autopsy

En la *ilustración 10* se puede visualizar un archivo en formato de texto, el cual muestra información de la computadora que estaba usando la víctima de Mr. Evil, (persona a la que se le registró su navegación por Internet).

Ilustración 11 dirección de la página web falsa de MSN (Hotmail) a la que ingresaban las víctimas del sujeto. Fuente: autoría propia
Herramienta Utilizada: Autopsy

En la presente *ilustración 11* se puede observar el sitio web al que accedió la víctima al momento en el que Mr. Evil le robo su información, (MSN Email). Esta plataforma más conocida como Hotmail sirve para chatear entre usuarios, lo que hacía esté sujeto era que creaba una página web con la misma apariencia que la original y redireccionaba a las víctimas a su página copiada, por lo tanto, cuando dichas victimas ingresaban sus fatos de acceso (usuario, contraseña) inmediatamente estos datos se enviaban al correo personal de Mr. Evil.

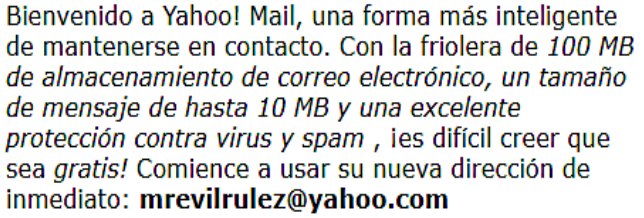

Ilustración 12 dirección del correo electrónico principal del sujeto. Fuente: autoría propia
Herramienta Utilizada: Autopsy

Con la *Ilustración 12* se puede resumir y esclarecer la dirección de correo electrónico basada en la web del principal sospechoso Mr. Evil, un correo creado en la plataforma de Yahoo! por el cual el sujeto se comunicaba con personas anónimas.

Ilustración 13 nombre del archivo que guarda las copias del correo electrónico del sujeto. Fuente: autoría propia
Herramienta Utilizada: Autopsy

Como se muestra en la *ilustración 12* se puede verificar que, en el aplicativo Yahoo! Mail, el cual Mr. Evil utilizo, guarda las copias de seguridad del correo electrónico con el respectivo nombre de archivo Showletter [1].htm.

V. CONCLUSIONES

Cuando se está estudiando un caso existen muchos factores externos que pueden llegar a ser relevantes al momento de poder dar una explicación, por lo tanto, se recomienda conocer muy bien la naturaleza de este, ser muy cuidadoso al instante de trabajar y recolectar la evidencia, seguir detalladamente las fases, a la vez, ir anotando todo lo que se está haciendo en su momento, en cuanto a estas anotaciones ser bastante claro y detallarlas precisamente.

Es primordial el preservar, mantener y resguardada la evidencia original en el mejor estado posible, trabajar con copias bit a bit, utilizar herramientas conocidas y que como resultados den un soporte que pueda llegar a presentarse en una institución que lo requiera.

A través de la informática forense, que se considera una ciencia, se pueden realizar diferentes investigaciones sobre cualquier delito que sea informático, y se pueden obtener pruebas necesarias y efectivas en los tribunales, porque ayudarán a enjuiciar al sospechoso y/o responsable de los delitos. Crimen o participación.

En cuanto al caso analizado por medio de las técnicas de informática forense, se pudo recolectar la evidencia necesaria para llevar a un tribunal y juzgar al personaje Mr. Evil sospechoso de robo de información personal, usuarios y contraseñas. Esclareciendo que efectivamente con los dispositivos allanados (computadora portátil, tarjeta de red y antena externa) el sujeto Mr. Evil realizaba dichos delitos.

REFERENCIAS

López, Ó., Amaya, H., León, R., & Acosta, B. (2001). Informática Forense: Generalidades, aspectos técnicos y herramientas. *Universidad de los Andes. Colombia*.

Dominguez, F. L. (2013). *Introducción a la informática forense*. Grupo Editorial RA-MA.

Saavedra, L. F. C., & Jaime, J. A. B. (2015). Informática Forense en Colombia. *Ciencia, innovación y tecnología*, *2*, 83-94.

Weliverysecurity by eset. (15 de abril de 2015). *5 fases fundamentales del análisis forense digital.* Weliverysecurity. https://www.welivesecurity.com/la-es/2015/04/15/5-fases-analisis-forense-digital/

Weliverysecurity by eset. (23 de septiembre de 2013). *Cómo realizar un análisis forense con Autopsy.* Weliverysecurity. https://www.welivesecurity.com/la-es/2013/09/23/como-realizar-analisis-forense-autopsy/

Caballero, A. E. (2 de mayo de 2014). *Crear la Imagen Forense desde una Unidad utilizando FTK Imager.* ALONSO CABALLERO / REYDES. http://www.reydes.com/d/?q=Crear_la_Imagen_Forense_desde_una_Unidad_utilizando_FTK_Imager#:~:text=FTK%20Imager%20de%20AccessData%20es,forense%20como%20AccessData%20Forensic%20Toolkit.

Carbone, F. (2014). *Informática forense con FTK*. Packt Publishing Ltd.