Caso de Piratería[1]

AUDITORES: GERARDO SANTISTEBAN TRIANA – HENRY MANUEL GONZALEZ CAÑON

Resumen – Este caso de piratería se basó en una computadora portátil Dell que se encontró abandonado junto con una tarjeta PCMCIA inalámbrica y una antena 802.11b externa de fabricación propia. Se sospecha que esta computadora se utiliza con fines de piratería. Aunque no se puede asociar con presuntos piratas informáticos, Greg Scharter también tiene el apodo de "Sr." Evil; de acuerdo al escenario de descripción de este caso, que fue recibido para ser investigado, indica que algunos de sus colegas dijeron que el Sr. Evil estacionaría el vehículo dentro del alcance de los puntos de acceso inalámbricos (como Starbucks y otros puntos de acceso de T-Mobile), y luego interceptaría el tráfico de Internet allí en un intento de obtener números de tarjetas de crédito, nombres de usuario y contraseñas. [1]

Índice de Términos **- Hackeo, robos por internet, inseguridad, piratería, ataques cibernéticos**

I. INTRODUCCIÓN

La presente investigación fue adquirida durante la clase de informática forense, objetivo principal de este curso que conlleva a adquirir el conocimiento de cómo analizar situaciones de la vida real, para este análisis, se estudia un caso de posible piratería a redes locales, en la que un supuesto personaje realizaba a través de programas de software, rastreo y captura de información.

La característica principal de este estudio es el uso apropiado de las herramientas forenses para análisis de información en equipos informáticos, como lo son *FTK Imager y Autopsy;* estos softwares nos permiten encontrar información detallada que se encuentre alojada dentro de un sistema operativo o diferentes tipos de pen drive, así la información sea visible, este oculta o incluso eliminada.

II. HERRAMIENTAS UTILIZADAS PARA EL ANÁLISIS

Para el desarrollo de las investigaciones en casos forenses informáticos, se requiere el uso de software especializados que facilitan la investigación en las evidencias entregadas a los auditores; en este caso de investigación (caso de piratería) se decidió usar dos herramientas FTK Imager y Autopsy:

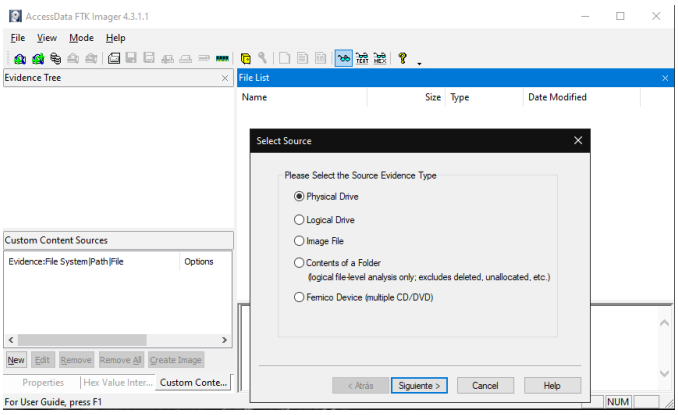


Fig. 1. Autoría propia, captura sacada directamente del programa FTK Imager de AccessData

FTK Imager de AccessData es una herramienta que permite hacer copias exactas para evidencias electrónicas que garantizan poder ser analizadas con herramientas forenses como autopsy, cuenta con un bloqueador de escritura para cualquier tipo de disco, asegurando que cuando se analice no se hagan cambios en la evidencia original.

Para prevenir la manipulación a futuro, de la evidencia original, FTK Imager realizará una imagen duplicada bit a bit, garantizando que la imagen forense sea idéntica a la original.

[1] Este Artículo forense se hizo para optar el título de ingeniero de sistemas; el director de este trabajo es el docente Edicson Pineda Cadena.

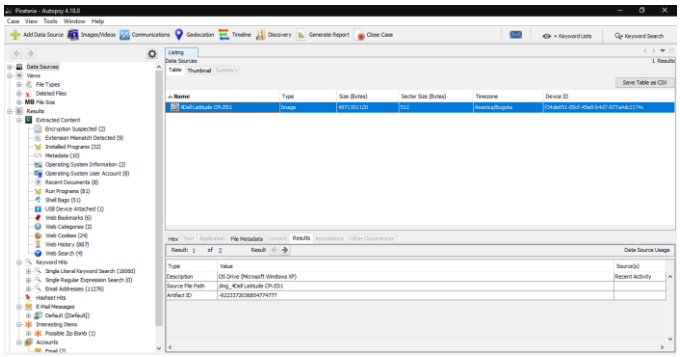


Fig. 2. Autoría propia, captura sacada directamente del programa Autopsy

El software Autopsy permite realizar consultas sencillas en la que se pueden buscar por palabras especificas o cadena de caracteres, como también se pueden hacer consultas con expresiones regulares utilizando patrones que permiten buscar coincidencias con combinaciones de caracteres dentro de cadenas de texto, y de esta manera lograr encontrar información en los resultados, ver a detalle las acciones que realizó el usuario durante su actividad; los resultados del análisis se centran en archivos que guardan la información de las acciones realizadas por el usuario. Se puede analizar gran variedad de sistemas como son Windows y UNIX, así como discos de archivos (NTFS, FAT, UFS1 / 2, Ext2 / 3).

III. ETAPAS

El análisis forense está definido como el proceso de técnicas que se efectúan para la búsqueda exhaustiva de datos, esta técnica está dividida en cinco fases que nos ayudan a mantener un estudio estructurado, facilitando la integridad, y los procesos del análisis.

- **Adquisición**
  En esta fase se recogen las copias de la información que se consideran sospechosas y que tienen alguna conexión con el caso a investigar. Para esta fase hay que tener en cuenta que para cuando se reciben las evidencias, es necesario hacer copias bit a bit con los softwares adecuados.

- **Preservación**
  En esta etapa se garantiza la integridad de la información, con la intención de que no sea manipulada o destruida, por esta razón no se deben realizar análisis sobres las muestras originales, es acá donde se define el concepto de cadena de custodia que corresponde a un acta donde se registra hora fecha y lugar de la copia realizada.

- **Análisis**
  Cuando ya se ha obtenido la información y ha sido preservada, se procede a realizar la fase más complicada donde se utilizan software especialmente diseñados para el análisis forense, es necesario tener muy en claro que es lo que se está buscando para así ser más preciso en las búsquedas.

- **Documentación**
  En esta etapa es donde todo los registros y búsquedas se guardan para realizar el informe final, por esta razón es necesario ir documentando a medida que se vaya encontrando evidencia, para este punto de acuerdo al análisis que realizamos ya debemos tener un posible de que fue lo sucedido con la información encontrada.

- **Presentación**
  Para este caso se entrega un informe técnico que contiene el detallado de toda la investigación en general, con acceso a los archivos o evidencias encontradas, y un informe ejecutivo que corresponde a este mismo documento, en el que se muestran las evidencias más importantes de forma resumida sin entrar en detalles técnicos.

IV. DESARROLLO DEL CASO

Para el desarrollo de este caso se realiza una línea de tiempo en la que se describe como fue el proceso para la investigación del caso de piratería, cabe recordar que esta investigación está basada en un supuesto caso de hackeo a través de redes wifi en que el victimario lograba substraer datos como números de tarjetas de crédito, usuarios y contraseñas de sus víctimas y así poder realizar sus robos

Fig. 3. Autoría propia, línea de tiempo de todas las etapas del desarrollo.

A continuación, se describe el paso a paso de la línea de tiempo:

Fig. 4. Autoría propia, captura sacada de la línea de tiempo de las etapas de desarrollo - parte recibe información.

Se recibe la información:
En este punto se reciben las imágenes o dispositivos a ser investigados, así como toda la información concerniente al caso, se estudia a detalle los datos, informes y las personas implicadas.

Es necesario estudiar a detalle todo lo que tiene que ver con la investigación para comprender qué tipo de información nos sirve como evidencia, según el informe recibido, este caso corresponde a un presunto sospechoso de piratería que pretendía robar datos personales de personas, el implicado rastrea las redes de internet a través de puntos wifi para robar números de tarjetas de crédito, nombres de usuario y contraseñas, según el informe este sospechoso trabajaba bajo el nombre de “Greg Schardt”.

Fig. 5. Autoría propia, captura sacada de la línea de tiempo de las etapas de desarrollo – programas usados – dispositivos.

Programas o software a ser usado:
Como se había indicado anteriormente en el punto II, FTK Imager de AccessData nos permite hacer la copia bit a bit del disco y el software que se usó para analizar la información es Autopsy, a través de este programa se logra analizar a detalle toda la información y descubrir que medios fueron utilizados o qué tipo de periféricos hacían parte del presunto sospechoso.

En al análisis de lo que nos fue entregado, se reporta lo siguiente:

- una computadora portátil Dell CPi
- una tarjeta PCMCIA inalámbrica
- una antena 802.11b casera externa

estos elementos periféricos son de gran ayuda para la investigación, debido a que con las características de las tarjetas y demás, se puede buscar que tipo de acciones realizó en el portátil.

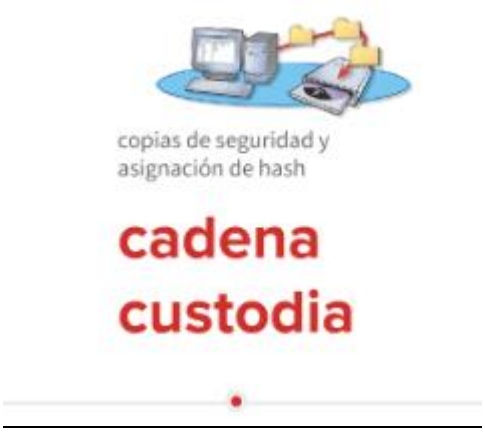


Fig. 6. Autoría propia, captura sacada de la línea de tiempo de las etapas de desarrollo – cadena de custodia.

Cadena de custodia:
En este paso se recibe el disco para ser analizado, se preserva la evidencia lo más seguro posible, se hace copia de seguridad por protocolo y cuestiones de seguridad de la integridad de la información, se realizan copia bit a bit utilizando el software FTK Imager de AccessData, se genera hash único y se procede hacer la investigación en la copia generada, con el objetivo de poder analizar y tener acceso a cada acción o registro hecho en el disco, culminado el análisis se genera el reporte técnico y se realiza el informe ejecutivo, se procede hacer la entrega de toda la evidencia encontrada.

El resultado de la copia arroja como resultado un hash único para ser identificado en caso de que sea manipulada la información, el Hash correspondiente a esta unidad es **AEE4FCD9301C03B3B054623CA261959A,**

Image Type:	E01
Size:	4,87 GB (4871301120 bytes)
Unallocated Space:	3,19 GB (3189226610 bytes)
Sector Size:	512 bytes
MD5:	aee4fcd9301c03b3b054623ca261959a
SHA1:	
SHA256:	

Fig. 7. Autoría propia, captura sacada del software Autopsy – caso de piratería – hash – encontrado en propiedades del disco.

Hash: "es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija".

Fig. 8. Autoría propia, captura sacada de la línea de tiempo de las etapas de desarrollo – análisis.

Habiendo llegado a esta etapa, que en las investigaciones forenses son las más cruciales e importantes, debido a que es en este punto donde se analiza a detenimiento todas y cada una de las partes de donde se encuentra evidencia para el informe correspondiente, se da inicio con los conceptos básicos.

Durante la investigación se analiza que el presunto sospechoso operaba bajo un sistema operativo Windows XP, como este sistema operativo ya no recibe actualizaciones, pues es más propenso a realizar vulneraciones

Type	Value
Program Name	Microsoft Windows XP
Date/Time	2004-08-19 22:48:27
Path	C:\WINDOWS
Product ID	55274-640-0147306-23684
Owner	Greg Schardt
Organization	N/A
Source File Path	/img_4Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32/config/software
Artifact ID	-9223372036854774815

Fig. 9. Autoría propia, captura sacada del software Autopsy – OS

También se observa que efectivamente el usuario indicado corresponde al registrado en el equipo, pero esto genera una sospecha debido a que en las cuentas de usuario que se hallaron en el equipo, nos reporta un usuario diferente

User ID	Username	Date Created	Count	Account Type
S-1-5-21-2000478354-688789844-1708537768-500	Administrator	2004-08-19 11:59:24 COT	0	Default Admin User
S-1-5-21-2000478354-688789844-1708537768-1003	Mr. Evil	2004-08-19 18:03:54 COT	15	Default Admin User
S-1-5-21-2000478354-688789844-1708537768-1002	SUPPORT_388945a0	2004-08-19 17:35:19 COT	0	Custom Limited Acct
S-1-5-21-2000478354-688789844-1708537768-501	Guest	2004-08-19 11:59:24 COT	0	Default Guest Acct
S-1-5-21-2000478354-688789844-1708537768-1000	HelpAssistant	2004-08-19 17:28:24 COT	0	Custom Limited Acct

Fig. 10. Autoría propia, captura sacada del software Autopsy – nombre usuario

Ante esto se puede sacar dos hipótesis, el sospechoso hackeo las credenciales de la cuenta administrador o el sospechoso y

el usuario Mr Evil son el mismo. A parte de la cuenta principal, se hallaron 4 cuentas adicionales las cuales no presentan uso, solo la cuenta principal con más uso.

	Username	Date Created	Count
-1708537768-500	Administrator	2004-08-19 11:59:24 COT	0
-1708537768-1003	Mr. Evil	2004-08-19 18:03:54 COT	15
-1708537768-1002	SUPPORT_388945a0	2004-08-19 17:35:19 COT	0
-1708537768-501	Guest	2004-08-19 11:59:24 COT	0
-1708537768-1000	HelpAssistant	2004-08-19 17:28:24 COT	0

Fig. 11. Autoría propia, captura sacada del software Autopsy – cuentas de usuario.

Program Name	Domain	Username
Internet Explorer		Mr. Evil
Internet Explorer	microsoft.com	Mr. Evil
Internet Explorer	cnn.com	Mr. Evil
Internet Explorer	wardriving.com	Mr. Evil
Internet Explorer	ethereal.com	Mr. Evil
Internet Explorer	yahoo.com	Mr. Evil
Internet Explorer	mosnews.com	Mr. Evil
Internet Explorer	maktoob.com	Mr. Evil
Internet Explorer	t50.com	Mr. Evil
Internet Explorer	msn.com	Mr. Evil
Internet Explorer	mondadori.com	Mr. Evil
Internet Explorer		Mr. Evil
Internet Explorer	ethereal.com	Mr. Evil

Fig. 12. Autoría propia, captura sacada del software Autopsy – usuario frecuente.

Habiéndonos inmerso más a fondo en el análisis del caso, se confirma que el sospechoso es el mismo usuario Mr Evil debido a una búsqueda que se hizo con el nombre Greg Schardt y todo porque el usuario instaló en el computador un programa llamado Look@LAN, este software permite al usuario analizar y rastrear el tráfico de una red, esta información se halló en un archivo llamado *"irunin.ini"* todo el registro de la instalación se almacenó en este archivo indicando el propietario, cuenta y tipo de instalación.

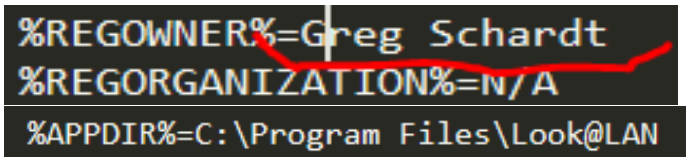


Fig. 13. Autoría propia, captura sacada del archivo irunin.ini del programa Look@LAN - extraído del software Autopsy – registro de instalación

Se encontró que el usuario contaba con tarjetas de red, en este caso se encontraron dos modelos:

- Xircom CardBus Ethernet 100 + Modem 56
- Compaq WL110 Wireless LAN P Card

Fig. 14. Autoría propia, captura sacada del software Autopsy – tarjeta Compaq

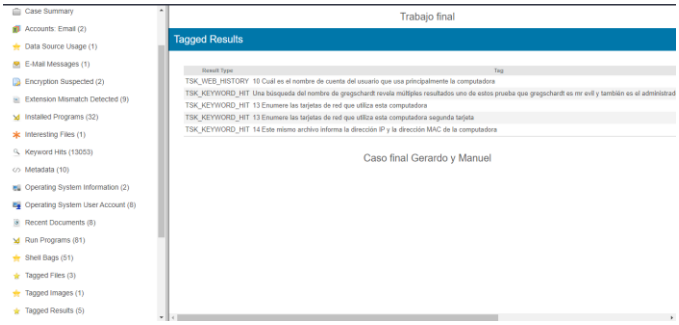
Fig. 15. Autoría propia, captura sacada del software Autopsy – tarjeta Xicom

Este resultado se puede evidenciar más a detalle en el informe técnico que se generó del software Autopsy, a través de estas tarjetas es posible que se realizaran conexiones a internet para hacer los pirateos.

Fig. 16. Autoría propia, captura sacada de la línea de tiempo de las etapas de desarrollo – informe técnico.

Informe Técnico:

Habiendo culminado con el análisis de todo el disco, se procede a exportar el informe técnico que corresponde al que genera el programa autopsy, este informe es complemento del informe ejecutivo.



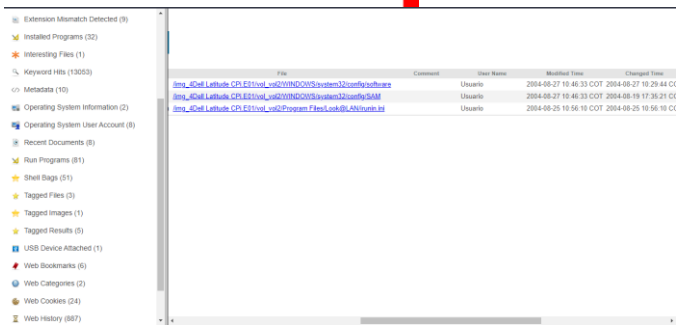


Fig. 17-18. Autoría propia, captura sacada del informe generado por el software Autopsy.

V. CONCLUSIONES

- Las herramientas y técnicas que se implementaron durante esta investigación fueron el resultado de todo el proceso investigativo y preparatorio de la clase de informática forense, dichas técnicas fueron puestas en práctica, de acuerdo a lo aprendido.

- El sospechoso tenía conocimientos profundos en informática, esto se deduce a raíz de las tarjetas y los programas que se encuentran instalados en el equipo que son para tipos de rastreo.

- Se deduce que el usuario Greg Schardt si realizaba tipos de rastreo, por los registros de los periféricos que tenía instalados en su computador, así como los programas de rastreo de red que instaló en su momento a lo que un usuario común no tendría.

VI. REFERENCIAS

[1] @soji256, «soji256,» 12 junio 2019. [En línea]. Available: https://www.cfreds.nist.gov/Hacking_Case.html.

[2] «eset.com,» 15 abril 2015. [En línea]. Available: https://www.welivesecurity.com/la-es/2015/04/15/5-fases-analisis-forense-digital/.

[3] «Autpsy,» [En línea]. Available: http://www.sleuthkit.org/autopsy/.

[4] A. Caballero, «ReYDeS,» 02 mayo 2014. [En línea]. Available: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..

[5] S. M. Gómez-Calcerrada, «adictosaltrabajo.com,» 29 01 2015. [En línea]. Available: https://www.adictosaltrabajo.com/2015/01/29/regexsam/. [Último acceso: 2021].