Forense en red social Facebook

Gerson Alexander Andrade Mora, Luis Guillermo Castillo Farfán.
Universidad Piloto de Colombia
Bogotá, Colombia.
gerson.andrade543@gmail.com
lgcfarfan@gmail.com

Resumen — Facebook es una de las redes sociales que más ha crecido a nivel mundial, y es también uno de los medios más utilizados para la realización de actividades al margen de la ley. Es por ello que el propósito de este artículo es descubrir las evidencias guardadas en la memoria RAM y en el software navegador de internet. El proceso de análisis inicia con herramientas de adquisición de información física y lógica del equipo, para luego ser examinadas rigurosamente y hallar posteriormente la evidencia. A lo largo de esta investigación, se encuentran hallazgos significativos, objetos muy específicos de Facebook podrían ser ubicadas en diferentes unidades de la memoria RAM incluyendo caché del navegador, archivos de paginación y en los clústeres no asignados.

Abstract — Facebook is a social network that has grown worldwide, and is also one of the most used means for conducting activities outside the law. That is why the purpose of this article is to discover the evidence stored in RAM and Internet browser software. The analysis process begins with acquisition tools physical and logical computer information, and then be examined carefully and then find the evidence. Throughout this research, significant findings are very specific objects of Facebook could be located in different units of RAM including browser cache, paging files and unallocated clusters.

Índice de Términos — Facebook, forense, memoria caché, memoria RAM, navegadores.

I. INTRODUCCIÓN

Facebook es un sitio web de redes sociales creado por Mark Zuckerberg y fundado junto a Eduardo Saverin, Chris Hughes y Dustin Moskovitz. Originalmente era un sitio para estudiantes de la Universidad de Harvard, pero se abrió a cualquier persona con una cuenta de correo electrónico. Lanzado en febrero de 2004. La misión de Facebook es dar a la gente el poder de compartir y hacer el mundo más abierto y conectado [1]. Los usuarios de Facebook pueden crear un perfil personal, agregar otros usuarios como amigos, e intercambiar mensajes, incluyendo notificaciones al actualizar su información de perfil. Además, los usuarios pueden compartir su estado, noticias, notas, fotos, videos, y permiten que sus amigos (o amigos de amigos) puedan comentar sobre ellos. De igual manera los usuarios pueden unirse a grupos con intereses comunes, organizar eventos y crear páginas para un lugar de trabajo o negocio, una escuela o universidad, o incluso la marca de algún producto.

Con todas estas posibilidades y funcionalidades, esta red social es una fuente de gran cantidad de información que constituye una de las mejores posibilidades para que los delincuentes lleven a cabo actividades ilegales tales como estafas, sobornos, ciberbullying, venta de drogas alucinógenas y el comercio del sexo. Facebook tiene más de 1,150 millones de usuarios activos [2]. Sin embargo, se estima que mas del 20% de estos usuarios son niños menores de 17 años con cuentas activas [3]. No es difícil imaginar que los delincuentes podrían usar estas cuentas para ocultar su verdadera identidad.

Debido a la popularidad de Facebook y su potencial para ser mal utilizado, el principal objetivo de este estudio es descubrir la evidencia de las actividades realizadas por el usuario en dicha red social. Esto se logra mediante un análisis minucioso a los registros de memoria e historiales de internet.

II. DESARROLLO

Del funcionamiento de las redes sociales sabemos que el material almacenado se encuentra en los servidores y su recolección se compone de mucha documentación legal internacionalmente, ya que los servidores se encuentran fuera de nuestro país, no obstante resulta posible encontrar evidencia en las computadoras y dispositivos móviles que se utilizaron para subir material, descargar o bien realizar otras actividades como búsquedas o comunicaciones por mensajería instantánea .

En este sentido se destaca que estas evidencias quedan almacenadas en el caché del navegador utilizado para acceder a la red social. Esto nos permitirá analizar artefactos de las redes sociales que pudieran haber sido eliminados como parte del proceso de depuración del

navegador utilizado, facilitando el acceso a datos con mayor antigüedad.

Esta investigación se contempla en las siguientes partes, análisis de la memoria RAM, historial de navegación y análisis, registro de eventos, registro de mensajes o chats, links, imágenes o fotos. En cada una de ellas se analizan las evidencias encontradas, ¿Cómo se encuentran?, ¿Dónde se encuentran, ¿Qué significan? y cómo podemos utilizarlas en la vida diaria o en una investigación muy importante.

A. Memoria RAM

Un aspecto que puede asistir a la investigación es la obtención de imágenes forenses de la memoria RAM de los dispositivos involucrados. Estas imágenes pueden contener evidencia en tanto y cuanto se haya accedido a las redes sociales desde el momento en que el dispositivo fue encendido hasta su recolección con herramientas específicas.

Cuando tenemos acceso a una imagen forense previamente extraída de un equipo sospecho o en investigación, podemos realizar un volcado de memoria para conocer lo que se almacena en la memoria RAM, a través del uso de la herramienta forense Forensic Toolkit (FTK) [4], se extrae una imagen y continuamente es analizada.

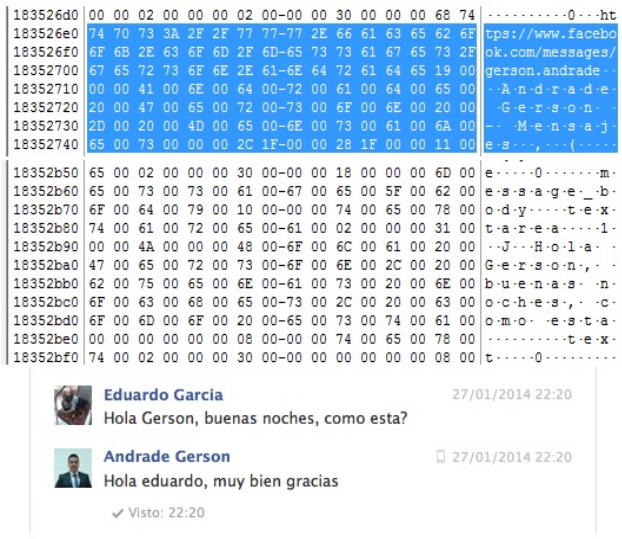

Fig. 1 Segmento de memoria RAM.

En la figura 1 se observa una conversación chat a través de la red Social Facebook entre 2 usuarios. Tomando la información de la memoria RAM del equipo de cómputo de uno de los usuarios del chat, vemos que la información todavía se encuentra almacenada en la memoria y se enseña la ubicación en el disco.

Esto posible gracias que el equipo aun se encontraba encendido a la hora de la recolección. Debemos notar que aunque la conversación se pueda borrar directamente en el chat de conversación, la misma aún se encuentra localizada en la memoria RAM, ya que en esta se almacenan todos los eventos realizados hasta que no se apague el equipo de forma convencional.

B. Historial de navegación y análisis.

El historial de navegación es el registro donde se guarda toda la información de los últimos lugares o paginas web consultadas en la maquina. Estos registros contienen las ultimas paginas web consultadas, auto llenado de formularios o acceso, últimos archivos abiertos, últimos comandos escritos.

En la figura 2 podemos visualizar el historial de navegación en la estación de trabajo con los distintos navegadores que pueda tener instalados. Esta información es posible obtenerla haciendo uso de la herramienta Internet Examiner 3.9.0 [5] y en este caso encontramos que los navegadores más utilizados son “Internet explorer” y “google chrome”, navegadores sobre los cuales debemos centrar aún mas nuestra atención en la búsqueda de información importante.

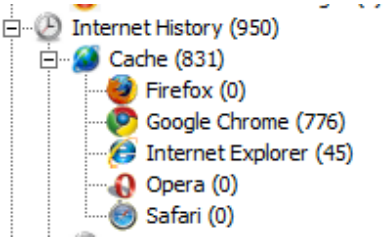

Fig. 2 Historial de internet.

Una vez identificado el navegador de mayor utilización, se procede a analizar su historial o cache y es así como en la figura 3 podemos ver que hay mucha actividad hacia la página de la red social Facebook.

Fig. 3 Historial navegación google chrome.

En este punto podemos establecer que el usuario de este equipo de cómputo, utiliza el navegador Google Chrome para hacer uso masivo de la red social Facebook. Esta estación de trabajo ahora constituye una fuente de información considerable y como veremos más adelante, podrá brindarnos información definitiva que permita establecer la actividad realizada por este usuario en la red social, como son los mensajes de chats, eventos, amigos e imágenes compartidas del usuario.

C. Registro de eventos.

Los eventos son actividades de interés que pueden ser publicadas en un área especial, por ejemplo una reunión de amigos, un concierto, una fiesta en algún lugar seleccionado, la presentación de algún articulo, etc.

Continuando con el proceso de investigación, encontramos los eventos que ha realizado o se ha unido el usuario, también como información muy importante.

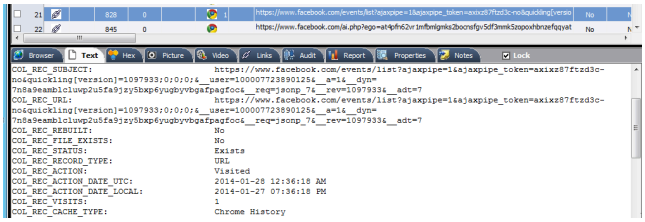

Fig. 4 Captura de evento en Facebook.

En la figura 4, vemos como a través de la aplicación Internet Examiner 3.9.0, podemos visualizar gran cantidad de información a partir de una de las páginas visitadas por el usuario. Vemos por ejemplo información acerca de la fecha y la hora en la cual fue accedido el sitio, se evidencia información del ID del usuario y/o número de identificación del usuario en Facebook.

Recordemos que estos eventos pueden ser muy importantes a la hora de analizar evidencia que comprometan al usuario en la divulgación de actos vandálicos, bien sea para encuentros en las calles para maltrato físico o para realizar matoneo a una determinada persona o en algunos casos animales.

D. Registro de mensajes o chats.

El chat en Facebook es un servicio de mensajería instantánea que es ofrecido para la comunicación con mas usuarios de esta red social, se pueden comunicar bien sea entre la lista de amigos o conocidos, hasta cualquier persona que tenga habilitada la opción de chat, así este no se encuentre en su lista de amigos.

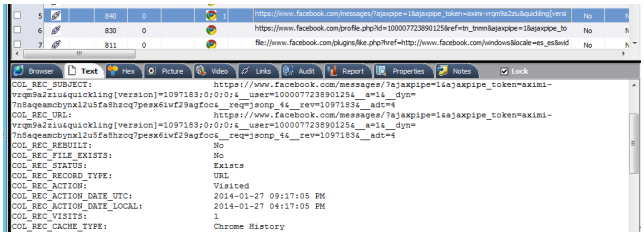

Fig. 5 Captura mensaje en Facebook

En este caso se halla un mensaje escrito donde se evidencian la fecha y hora del mismo, entendiendo que realmente se ha realizado un mensaje de chat con un usuario especifico, bien sea un amigo, conocido o cualquier otra persona de esta red social.

Asimismo como podemos ver la fecha y hora del mensaje, también podemos observar el user ID, este es del usuario de quien creó o redacto el mensaje enviado, en la siguiente etapa veremos como se relaciona este user ID.

E. Links, Imágenes o fotos.

Además de crear un perfil con información personal, crear eventos, enviar y recibir mensajes instantáneos, también se pueden cargar y/o compartir imágenes o fotos personales.

Al cargar una imagen o foto, se almacenan en un álbum, este a su vez contiene mas imágenes que se han cargado con anterioridad. Facebook proporciona un nombre muy particular tanto al álbum como a las fotos cargadas, se imprime un numero muy especifico que contiene una información muy importante como la veremos a continuación:

Link:

"https://www.facebook.com/photo.php?fbid=10150328800777409&set=a.443960772408.221899.703732408&type=1&theater"

Detallando la URL anteriormente referenciada, encontramos varios datos que son de mucho interés, tales como:

10150328800777409 es la identificación de la foto o "photo ID", única para esta foto.

443960772408 es la identificación del álbum o "álbum ID", donde se encuentran todas las fotos cargadas a este álbum.

703732408 es la identificación del usuario o "user ID", indica la identificación del usuario ante Facebook.

Con esta información obtenida después de un riguroso análisis, vemos como a raíz de una imagen forense se obtienen muchos datos que apuntan a un usuario especifico, y como queda registrada toda su actividad en esta y muchas paginas web, además de la actividad en el equipo empleado.

III. CONCLUSIONES

Estudiando las diferentes características y pensando en una protección para cada usuario de esta Red, vimos la necesidad de implementar una técnica de análisis forense para detectar las diferentes vulnerabilidades ejecutando un proceso que nos ayuda a minimizar las posibilidades de un fraude o una clonación de los diferentes perfiles del Facebook.

Para recolectar evidencia que reside en los servidores de las redes sociales será necesario solicitarla por vía judicial, ya que como es usual estos servidores se encuentran fuera de la jurisdicción de nuestro país. En este caso será necesario conocer cuales son las políticas unilaterales establecidas por los administradores de cada red social respecto de cual es el contenido que ellos almacenan y durante cuanto tiempo se encuentra disponible. Además de un sin número de documentación que resulta ser en la mayoría de los casos difícil de recolectar, por términos legales.

Como alternativa, resulta posible recolectar evidencia de los equipos comprometidos con algún acto que involucre la actividad en las redes sociales o en cualquier ámbito.

Todas los registros que se realicen en un dispositivo o equipo, son almacenadas en su memoria RAM y en su unidad de Disco Duro, gracias a ellos podemos realizar un estudio detallado para encontrar estos registros y poner en evidencia real y legal, que se han realizado en tiempos y horas concretas, no obstante debemos recordar que antes de hacer estos estudios se debe tener documentación legitima donde nos autoricen el procedimiento de análisis forense a dichos dispositivos.

REFERENCIAS

[1] Facebook - Info, Facebook Inc., Consultado el 25 de enero de 2014, disponible en http://www.facebook.com/facebook?sk=info

[2] El universal. (2013) Facebook llega a 1,150 millones de usuarios al mes. [Online]. Available: http://www.eluniversal.com.mx/computacion-tecno/2013/facebook-millones-usuarios-79305.html

[3] Wikimedia, wikimedia commons. [Online]. Available: https://commons.wikimedia.org/wiki/File:Facebook_users_by_age.PNG

[4] Forensic Toolkit (www.accessdata.com) – Forensic Toolkit (FTK) is a leading computer forensics and image acquisition software solution, because it is designed with an enterprise-class architecture that is database driven.

[5] Internet Examiner - V3, Internet forensics recovery, analysis and reporting tool available to governments, law enforcement and corporate security professionals. Available: http://www.siquest.com/productdetailPage.php?pID=4&mid=253af8zzy