# Peritaje Informático en Redes Sociales

Tatiana Ruth Arancibia Quiroga
*Postgrado en Informática*
*Universidad Mayor de San Andrés*
La Paz - Bolivia
taruth7@gmail.com

***Resumen*—La presente investigación tiene por objetivo dar un primer enfoque sobre los peligros de las redes sociales que llevan un constante crecimiento de usuarios y la información que circula a través de las mismas; además de mostrar el papel que juega un perito informático como experto en la materia y como un individuo puede recurrir cuando tiene la sospecha de que su información se encuentra disponible en su contra en Internet por medio de una red social o foro.**

***Palabras clave—redes sociales, informática forense, peritaje informático***

## I. Introducción

El análisis Forense Digital consiste en el hallazgo de evidencia digital para ser procesada que permita confirmar una actividad realizada o bien desestimarla sobre algún caso de delito informático. Es importante que en estas situaciones se tomen los recaudos para garantizar el resguardo correcto de la prueba y la continuidad del mismo durante todo el proceso de adquisición, conservación, documentación, análisis y presentación de evidencias, de esta forma se asegura a las partes la inalterabilidad del objeto y la garantía de un proceso pericial sobre el objeto en el estado exacto en que se recolectó.

El análisis forense en redes sociales se ha vuelto más significativo, ya que existe la posibilidad de que la información personal de un individuo sea comprometida y su uso está altamente difundido, principalmente en jóvenes y adolescentes por la flexibilidad de servicios que ofrecen Facebook, WhatsApp, Twitter y LinkedIn, entre algunos de los más populares, se ha extendido de manera tal que es muy común encontrar que los usuarios utilizan estos servicios desde sus equipos móviles inteligentes (smartphones, tablets).

## II. Métodos

### *A. La Investigación Forense y Las Redes Sociales*

Primero un investigador forense o perito informático debe tener claro las características principales de las redes sociales, ya que podría confundirse la perspectiva entre medio social y redes sociales, a esto también se debe tener en consideración sus conceptos. Las tendencias que constituyen las redes sociales y las características por los cuales se logran identificar se pueden mencionar los siguientes aspectos:

1. Son públicas
2. Son compartidas
3. Son de colaboración
4. Son seudónimas
5. Son interactivas
6. Son difíciles de regular y controlar
7. Son ubicuas
8. Son accesibles vía Web o TCP/IP
9. Son personales
10. Son bidireccionales
11. Son informales
12. Son permanentes
13. Son medios independientes

Las redes sociales han revolucionado a un punto que la inmensidad de datos sobre ella hace posible que en la actualidad las empresas pueden utilizar las redes sociales para monitorear las actividades de su personal, los padres de familia para monitorear a sus hijos adolescentes, colegios o instituciones monitorear a sus estudiantes y sus miembros respectivamente o como los gobiernos pueden monitorear a sus ciudadanos.

El investigador forense debe ser lo suficientemente hábil para hallar información de todo el "medio", por ejemplo, una simple fotografía posee metadatos (herramientas para recabar la data EXIF nos proporciona hora, fechas, posición geográfica y otros detalles que son parte de la metadata).

A la hora de abordar un caso es un desafío para el investigador el buscar formas de encontrar la información original o recuperarla si esta fue destruida. Otra consideración que se debe tener en cuenta al momento de la investigación es la localización de la evidencia, en este tipo de investigación la evidencia digital se encuentra en dispositivos como laptops, tablets, smartphones, sistemas de juego, móviles, entre otros.

El segundo desafío al momento de la búsqueda de la evidencia depende de los procesos legales (esto es de acuerdo con la jurisdicción), como ser:

1. El consentimiento del titular de la cuenta
2. Políticas de intercepción de datos
3. Consentimiento de otros para poder acceder a la información de la cuenta del titular
4. El consentimiento de otras personas para el acceso a dispositivos
5. Procesos obligatorios
6. Citación administrativa



**Para referenciar este artículo (IEEE):**
[N] T. Arancibia, «Peritaje Informático en Redes Sociales» *Revista PGI. Investigación, Ciencia y Tecnología en Informática*, nº 7, pp. 100-103, 2020.

7. Citación judicial
8. Citación contenciosa

El investigador forense debe de tomar en consideración los aspectos de "La Doctrina de Terceros" y los "Términos de Servicio", por ejemplo:

¿Cómo el investigador forense puede acceder a los datos de una compañía que brinda el servicio de redes sociales? – con una orden judicial, una citación.

¿Cuál sería el mejor medio para una mejor trazabilidad en una investigación, instalar un equipo GPS al automóvil sin el consentimiento de un individuo o poder llegar a esa misma información con las trazas que me brinda el GPS de un dispositivo móvil proporcionadas por la compañía de telecomunicación?

Los términos de servicio son el espacio que un investigador forense debe de hacer uso en su investigación ya que las redes sociales permiten información al público como: nombre de usuario, ID de usuario, red, fotografías de portada, fotografías de perfil, redes y amistades, etc.

### *B. El perito informático como asesor tecnológico independiente*

Una de las principales funciones del perito informático como profesional libre, es la de ejercer una labor de asesoramiento tecnológico como profesional independiente y experto

Contar con el asesoramiento de un perito informático a la hora de contratar la realización de un proyecto informático, es vital si se desea que el desarrollo del proyecto o del producto contratado se ejecute de forma satisfactoria, con el objetivo focalizado, exclusivamente, en el beneficio para el cliente.

### *C. El perito informático en la suplantación de identidad en internet*

Un perito informático es requerido para la realización de un informe pericial en el que se deje constancia de que la identidad de una persona ha sido suplantada. En algunas ocasiones, también, el perito informático es requerido para demostrar justamente lo contrario, es decir, que una persona acusada de suplantación de identidad no tiene por qué ser culpable de la comisión del delito.

La labor del perito informático, en ambos casos, es ceñirse a las evidencias aportadas por el cliente, analizando la cadena de eventos de principio a fin y obteniendo conclusiones a partir de la misma.

La identidad de una persona se puede suplantar en Internet de varias formas, por ejemplo: abriendo páginas en redes sociales a nombre de esa persona sin su autorización, publicando anuncios en páginas de contactos con datos personales y teléfono reales de un tercero, creando una cuenta de correo electrónico con su nombre y apellidos exactos y enviando información maliciosa a otras personas, etc.

Es muy importante acudir rápidamente a un perito informático, ya que la información en Internet es volátil, es decir, puede perderse de forma irremediable, por lo que sería imposible efectuar la denuncia.

## III. RESULTADOS

### *A. Caso analizado "Trata y tráfico de personas"*

- Escenarios
  - Creación de perfil falso
  - Captación de menores de edad de sexo femenino
  - Explotación sexual
- La Ley
  - Ley 263-Ley integral contra la trata y tráfico de personas
- El culpable
  - Samuel Montaño Galarza alias "Renzo Schultz"
- El motivo
  - Económico
- Modus operandi
  - El modus operandi de este sujeto era captar jóvenes incautas en redes Sociales para luego explotarlas sexualmente.

### *B. Análisis del caso - Estado del caso*

Según el informe se presume que existen 1200 implicadas de los cuales un caso fue resuelto y solo se llegó a un individuo, no se tiene más culpables y menores de edad implicados.

- Estado–la investigación continúa.
- Se desconoce la operación realizada por la FELCC.
- No se tiene detalles de cómo fue encontrada la menor que permitió descubrir al responsable.
- Se desconoce el uso de métodos y herramientas usadas en el caso,
- Se desconoce avances posteriores realizados a la captura del implicado.

## IV. ANÁLISIS DEL CASO CON EL USO DE UNA METODOLOGÍA

Identificar, las cuentas de Facebook que pueden tener evidencia, preservar, la evidencia contra daños, para ello se puede tomar como apoyo la herramienta EnCase Forensic v.6.4, pero antes es recomendable obtener una copia de las conversaciones de la cuenta de Facebook, esto se encuentra en el directorio de:

> Configuraciones.

- Crear una imagen forense de la evidencia
- Comprobar identidad criptográfica
- Análisis de datos sospechosos
- Buscar evidencias y generar documentos, analizar la imagen obtenida.
- Presentar resultados del caso analizado al juez. Tomar en cuenta: Aspectos legales básicos de acuerdo con las normas del país.

La Ingeniería Social también se extiende a las búsquedas de empresas y de amigos en las redes sociales LinkedIn y Facebook

respectivamente, donde los criminales utilizan para generar confianza y obtener datos. Con bastante frecuencia, el resultado final es la extorsión o el robo. Sin embargo, en el lado de la investigación con fines de averiguar qué pudo pasar, se puede utilizar la misma herramienta para obtener lo credenciales de una persona que tiene malas intenciones con su cuenta de Facebook, o correo electrónico.

## V. SET (SOCIAL-ENGINEERING TOOLKIT)

SET es una herramienta completa dedicada a la ingeniería social, que nos permite automatizar tareas que van desde el de envío de SMS (mensajes de texto) falsos, con los que podemos suplantar el número telefónico que envía el mensaje, a clonar cualquier página web y poner en marcha un servidor.

Se inicia la herramienta en Kali Linux.

Se visualiza la variedad de herramienta para utilizar, se selecciona un ataque de ingeniería social.


Fig. 1. Inicializar herramienta settoolkit

La siguiente opción crear un vector de ataque, seleccionamos 2.

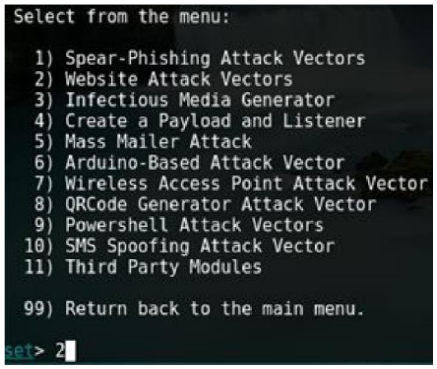


Fig. 2. Selección de opción 2

Se quiere clonar una página, que será el anzuelo.

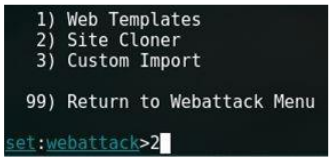


Fig. 3. Captura de herramienta settoolkit

Antes necesitamos la IP donde se alojará las capturas que se realicen.

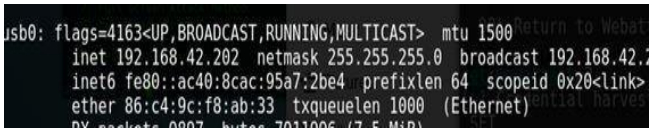


Fig. 4. Captura de herramienta settoolkit

Ahora se debe digitar nuestro IP de captura y la página a clonar.


Fig. 5. Captura de herramienta settoolkit

Finalmente se tiene dentro de nuestra red, un medio de captura de credencial.


Fig. 6. Captura de inicio de Facebook

Finalmente se tiene la captura de usuario y contraseña, para la identificación y nuestros fines de investigación.

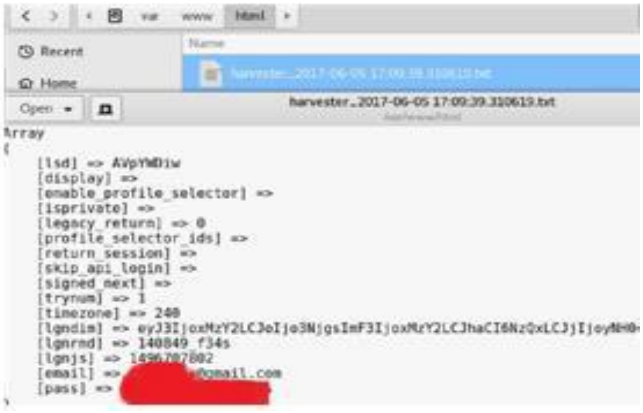


Fig. 7. Claves capturadas

## VI. DISCUSIÓN

Las Redes Sociales, es un ambiente considerado muy complejo, por el alcance que tiene en la Sociedad, siendo en la actualidad una de las plataformas más utilizadas, para interactuar entre personas.

También conlleva un peligro en su uso si no se usa de forma responsable, ya que la delincuencia hace uso de este medio de alcance masivo con fines negativos.

Hacer una investigación sobre temas de trata y tráfico de personas, no es tan sencillo, ya que, al ser redes sociales gratuitas, no es fácil tener acceso inmediato a información

eliminada y no existen herramientas que puedan vulnerar a los gigantes de las redes sociales, ya que se debe tomar en cuenta los términos de servicio y privacidad. Los monstruos de las redes sociales son empresas con mucho poderío en recursos, infraestructura, que hace muy difícil acceder a sus datos, sin embargo, se puede hacer uso de las mismas herramientas que utilizan los criminales, para investigar.

Como en la vida real, las redes sociales pueden ser un buen lugar para encontrarse con los amigos y conocer a otras nuevas amistadas, pero no está libre de peligros. Por esta razón es bueno estar informados de los peligros que lleva consigo estas aplicaciones supuestamente gratuitas donde muchas personas exhiben su diario vivir, fotografías de sus hogares y sus hijos pequeños, exponiendo su seguridad y privacidad a un peligro constante.

## REFERENCIAS


[1] 26 Abril, 2016, Peritaje Informático España http://peritoinformaticocolegiado.es/page/2/ 2016

[2] http://peritoinformaticocolegiado.es/el-peritoinformatico-y-el-rastro-en-internet-y-las-redessociales/

[3] *El Derecho.* (2019). Obtenido de https://cpiicm.es/: http://www.cpiicm.es/wp-content/uploads/sites/3/2017/04/ tecnologia_elderecho_com_tecnologia_internet.pdf

[4] Gómez, J. L. (2015). *"Informe sobre el Peritaje Informático".* Madrid.

[5] ReYDeS. (1 de abril de 2016). *Clonar un Sitio Web para Capturar Credenciales utilizando Social-Engineer Toolkit (SET)*. Obtenido de http://www.reydes.com/d/?q=Clonar_un_Sitio_Web_para_Capturar_Credenciales_utilizando_Social_Engineer_Toolkit_SET


Breve CV de la autora

**Tatiana Ruth Arancibia Quiroga** es Licenciada en Ingeniería de Sistema por la Universidad Autónoma Tomas Frías de Potosí, diplomada en Educación Superior por CIPIES-UMSA. Actualmente realiza la Maestría en Informática Forense, Seguridad de la Información y Auditoría Informática en el Postgrado en Informática UMSA. Es analista de mantenimiento y soporte de sistemas en UNIVida S.A. Fue analista de desarrollo de sistemas en Laboratorios COFAR, Consultora en proyectos de grado y desarrollo de sistemas en la empresa Case, Asistente de mantenimiento en Infraestructuras TI Universidad Privada Franz Tamayo. Su interés investigativo es el desarrollo de software. Email: taruth7@gmail.com.