# INVESTIGACION FORENSE EN REDES SOCIALES

**Gustavo Daniel Presman** [*]
**ARGENTINA**

## INTRODUCCION

El análisis Forense tradicional consiste en la obtención de imágenes forenses de las computadoras y demás objetos que almacenan evidencia digital, para luego ser procesada en búsqueda de artefactos forenses que permitan confirmar una actividad realizada o bien desestimarla . Es fundamental en estos casos tomar los recaudos para garantizar el resguardo correcto de la prueba y la continuidad del mismo durante todo el proceso , de esta forma se asegura a las partes la inalterabilidad del objeto y por ende la garantía de un proceso pericial sobre el objeto en el estado exacto en que se recolectó.

Las redes sociales han irrumpido fuertemente en la sociedad y su uso está altamente difundido, especialmente en la franja eraria de jóvenes y adolescentes al punto tal que el uso de las mismas está desplazando otras vías de comunicación como la telefonía e incluso los tradicionales servicios de mensajería instantánea come el MSN Windows Live Messenger . La portabilidad extrema a la que se han llevado servicios como Facebook , Twitter y Linkedin , entre otros se ha extendido de manera tal que es muy común encontrar que los usuarios utilizan estos servicios desde sus teléfonos móviles inteligentes (smartphones) como Iphone , blackberry y otros con plataforma Android . Rápidamente se están comenzando a adoptar las tabletas con acceso a Internet a través de WiFi o la red celular , augurándonos un futuro explosivo en el uso de las redes sociales desde dispositivos móviles.

Por que resulta tan atractiva la utilización de estas aplicaciones ? Una respuesta posible es que los usuarios pueden mantener en un único centro de control y diversión todas sus actividades cotidianas dentro de su grupo de pertenencia. Las aplicaciones para este entorno crecen día a día y la convergencia de las plataformas de estas redes sociales atrae y mantiene al usuario dentro de la misma incorporando día a día nuevas funciones para las que hoy necesita aplicaciones diferentes.

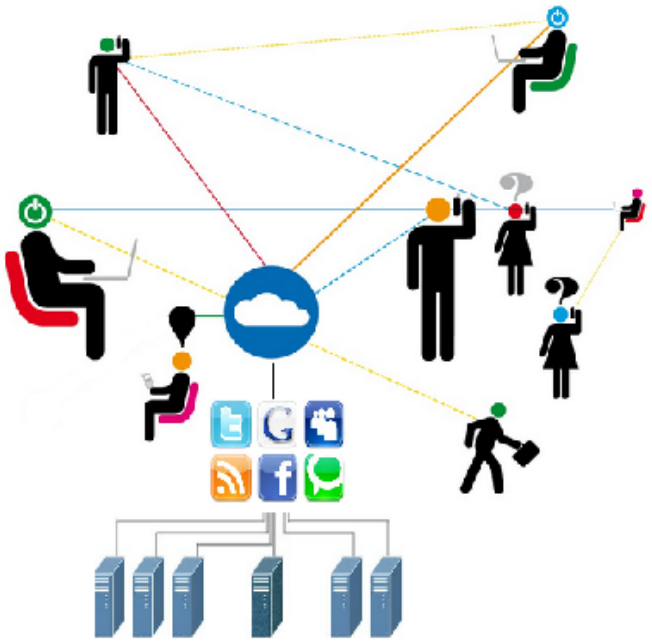
Frente a este escenario es importante conocer como y donde reside la información que se almacena y circula por las redes sociales para poder acceder a la misma en caso de ser necesario resguardarla con fines probatorios.

En este punto es importante comprender que el usuario que utiliza estos servicios interactúa con servidores de aplicaciones y con otros usuarios, siendo su principal

---

[*] Ingeniero Electrónico egresado en 1987 de la Facultad de Ingeniería UBA . Master Executive en TICs del Programa Gadex , España. Posee las certificaciones Internacionales CCE ( Certified Computer Examiner) , EnCE (Encase Certified Examiner) , FCA (Forensic Computer Advisor) y NPFA (Network Packet Forensic Analyst). Profesor de la Maestría en Seguridad Informática de la UBA y de los posgrados en seguridad de la Información de la USAL y Derecho Informático de la UNSL. Consultor en Investigación corporativa y entrenador de Fuerzas Armadas, Poderes judiciales provinciales y Policías de la Argentina y de varios países latinoamericanos en Investigación Forense Informática. Miembro de las principales asociaciones internacionales de Investigadores y peritos Informático Forenses como HTCC y HTCIA.

interlocutor el servidor de almacenamiento de la red social, es decir que la información viaja de la computadora del usuario hacia los servidores de aplicación que se encuentran en algún lugar del Internet.
Este esquema, brindado por todas las redes sociales es conocido como computación o servicios en la nube. De esta forma entendemos que el contenido de las redes sociales puede encontrarse o bien en las computadoras o dispositivos móviles de los usuarios participantes como material generado o descargado de estos nodos o mayoritariamente almacenado en los servidores de aplicación de la red social , en algún lugar de la nube...
En el siguiente gráfico se observa como los integrantes de una red social intercambian información , pudiendo estar en línea o desconectados , utilizando diferentes dispositivos de conexión como computadoras , celulares , encontrándose en el centro de todas esas comunicaciones los servidores de las redes sociales.
En el siguiente gráfico se observa como los integrantes de una red social intercambian información



**RECOLECCION DE EVIDENCIA EN LAS REDES SOCIALES**
Para describir la metodología de obtención de evidencia de las redes sociales debemos separar la obtención de evidencia en los extremos y en los servidores.
***Evidencia de Servidores de Redes Sociales:*** 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. Hésete ultimo punto es fundamental a la hora de establecer si la recolección será efectiva o puede tornarse

ilusoria para el caso en que el trámite judicial demore más tiempo que el de retención establecido por la red social.
En todos los casos será necesario consultar las guías para fuerzas de la ley que cada red social posee y sortear otros aspectos judiciales como la existencia de un domicilio de notificación en el país o la constatación del tipo de pieza procesal requerida para la solicitud.
Usualmente para la obtención de datos de tráfico , es decir para conocer logs de conexión u otros que contengan la dirección IP que permita llegar a un domicilio desde donde se efectuó alguna comunicación desde o hacia la red social , es suficiente con un oficio del juez interviniente. Si se trata de obtener contenido de las comunicaciones o contenido almacenado en los servidores de la red social, el mismo solo se encuentra disponible para jueces de la jurisdicción donde se encuentra la administración de la red social (Estados Unidos mayormente) por lo que un juez local deberá realizar un exhorto internacional por la vía diplomática, proceso que puede demorar un lapso incompatible con la política de retención de la red social.

***Evidencia en los extremos:*** Del funcionamiento de las redes sociales sabemos que el material almacenado se encuentra en los servidores y su recolección ya fue explicada en el parágrafo anterior, 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 .
Para el resguardo de la evidencia que permita el análisis posterior se requiere la realización de imágenes forenses del contenido de computadoras, smartphones y tabletas involucradas en el uso de las redes sociales.
Un punto a considerar es si las imágenes forenses deben ser de la totalidad del contenido de los elementos digitales involucrados, es decir imágenes forenses físicas o por el contrario solo sería suficiente con una imagen lógica de aquellas áreas que puedan contener evidencia de utilización de la red social. En es sentido se destaca que la evidencia de redes sociales queda almacenada en el caché de Internet del navegador utilizado para acceder a la red social o del aplicativo específico, el cual usualmente trabaja interrelacionado con el navegador.
La recolección de imágenes forenses de la totalidad de las unidades físicas permitirá que el investigador pueda 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. Por el contrario la imagen forense lógica que solo contenga el caché reciente se realizará en un tiempo sustancialmente menor pero sin chance de obtener objetos eliminados. Naturalmente esta será una decisión del investigador o perito forense, teniendo en cuenta las características puntuales de la investigación que esté realizando.
La obtención de imágenes forenses del contenido de dispositivos móviles como teléfonos celulares o tabletas, requerirá de equipamiento específico para el bloqueo de señales del sistema de telefonía celular, así como también para la extracción de datos por tipo de dispositivo, teniendo en cuenta la gran variedad de arquitecturas propietarias de hardware así como también la diversidad de sistemas operativos.

Un punto importante a considerar es la gran cantidad de imágenes que circulan en las redes sociales, situación que puede incrementar la recolección de evidencia digital, incluyendo cámaras fotográficas y tarjetas de almacenamiento donde pueden residir imágenes, activas o borradas por el usuario, cuyos metadatos pueden asistir a la investigación en curso.

El proceso investigativo que lleva a la recolección de evidencia en los servidores y en los extremos muchas veces se origina con la obtención de información de logs de conexiones de los servidores que permite llegar a los domicilios donde se encuentran las computadoras , dispositivos móviles y cámaras fotográficas a las que hice referencia en este apartado.

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. Naturalmente este tipo de recolección de evidencia solo es viable si el dispositivo se encuentra encendido al momento de la captura de los datos. En esta línea de trabajo suele ser de utilidad el de análisis forense de archivos de paginación o particiones de intercambio (swap) tanto de computadoras como de teléfonos inteligentes y tabletas.

Una alternativa final en la recolección de evidencia es la captura de tráfico en la línea de conexión a Internet de un usuario final. Este procedimiento consiste en capturar y almacenar el tráfico en un medio de almacenamiento intermedio, el que posteriormente se autenticará como una evidencia lógica y podrá ser procesado mediante una herramienta que permita la reconstrucción de paquetes de datos.

Esta técnica permite la presentación más completa y amigable pero solo puede ser empleada para el análisis de la actividad en redes sociales “a futuro”, es decir a partir de un determinado momento y nunca puede obtenerse evidencia de actividades pasadas.

Los métodos de recolección descriptos pueden aplicarse de manera complementaria, según los objetivos de la investigación forense y el mejor criterio del perito informático interviniente.

**ANALISIS DE EVIDENCIA EBN REDES SOCIALES**

El análisis de la evidencia es la etapa donde se buscará a través de los artefactos de cada tipo de red social información de interés para los hechos investigados.

Este trabajo es introductorio y no pretende ser exhaustivo describiendo cada una de las redes sociales, siendo el objetivo sentar las bases para el entendimiento de los tópicos relacionados, por lo que describiré los artefactos y protocolos que son comunes a prácticamente todas y cada una de las redes sociales actuales.

Entre los artefactos comunes a las redes sociales podemos destacar:

- ✓ **Comentarios (posts)**: subidos por miembros de la red social que pertenecen a los contactos del usuario comentado. Estos pueden contener archivos adjuntados con carácter multimedial (archivos de video, audio e imágenes) con metadatos propios.
- ✓ **Mensajería instantánea (chat)** : Comunicaciones con la lista de contactos

- ✓ **Búsqueda de contactos** : Actividad de búsqueda de nuevos contactos para invitarlos y agregarlos a su lista actual
- ✓ **Publicación de eventos** : Actividades de interés que pueden publicarse en un área especial
- ✓ Envío de notificaciones al correo electrónico: Son enviadas a los miembros cada vez que son mencionados en la red social.

Con relación a los protocolos empleados nos referimos al lenguaje con que se intercambian los mensajes entre los servidores de las redes sociales y los extremos. Estos pueden variar según el tipo de red social y el dispositivo de conexión empleado para conectarse a la misma , no obstante en todos los casos se utilizan variables del HTML.

Particularmente suele utilizarse el formato JSON (Java Script Oriented Notation) por ser liviano y no requerir XML (eXtensible Markup Language) para el intercambio de datos .

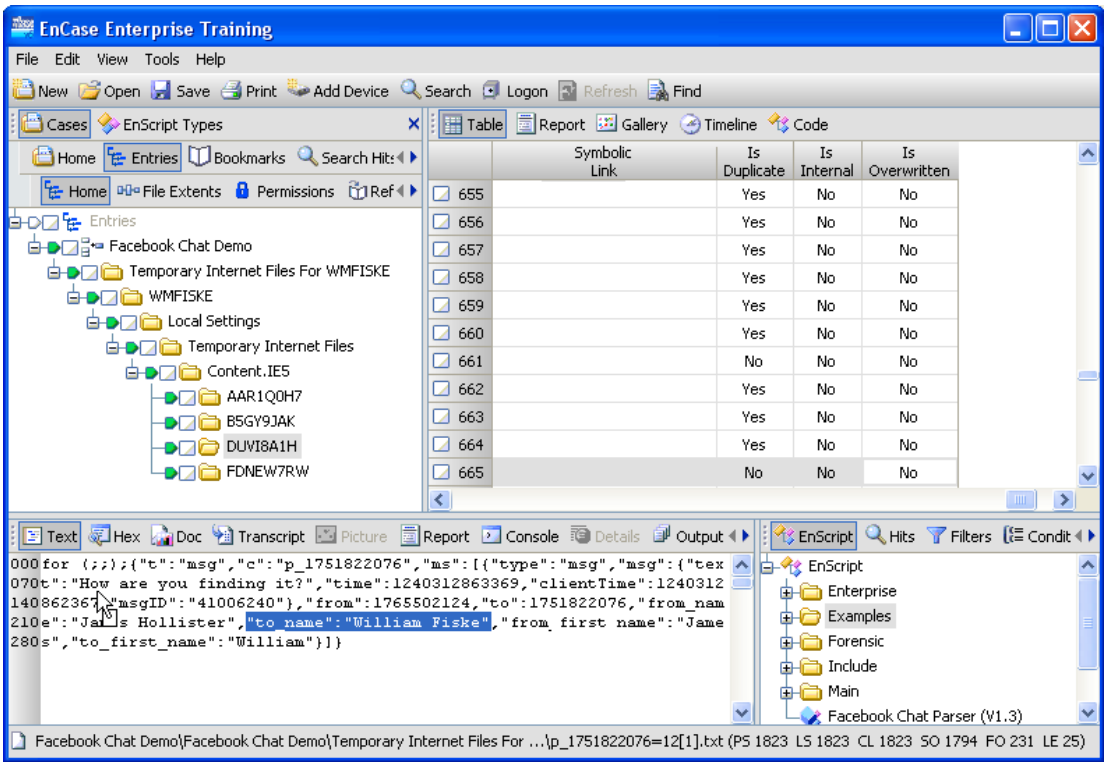
Las redes sociales suelen almacenar , en los extremos participantes , es decir en los equipos utilizados para conectarse a ellas , fragmentos de los intercambios correspondientes en formato JSON dentro de archivos de texto plano TXT .

El análisis forense requiere la identificación de estos archivos y luego el análisis (parsing) de su estructura, teniendo en cuenta los estándares definidos por la organización que sustenta JSON y que se encuentran publicados en www.json.org así como las implementaciones de cada red social considerada.

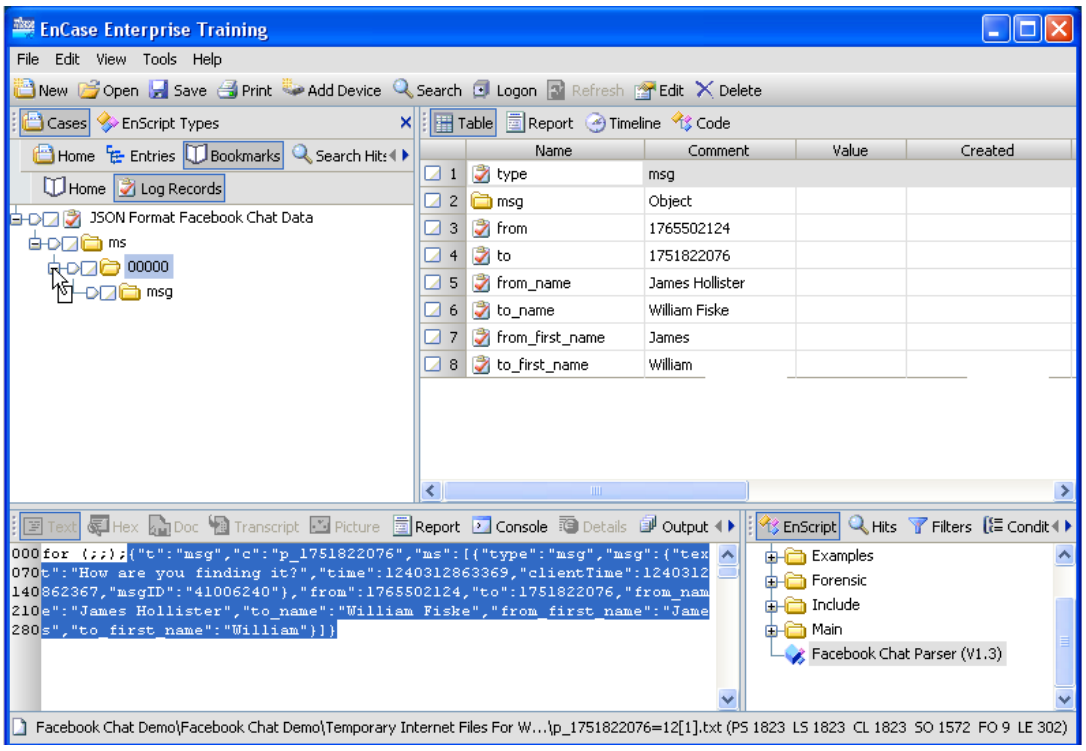
## EJEMPLO DE ANALISIS DE EVIDENCIA

Para concluir este trabajo mostraré como se identifica un fragmento de una conversación de chat de FACEBOOK , para lo cual se requiere de una herramienta forense capaz de identificar y decodificar los archivos TXT en protocolo JSON . En este caso se utilizó EnCase Forensic versión 6.19.

En la siguiente imagen se observa un archivo TXT conteniendo un fragmento de una conversación por mensajería instantánea de facebook :

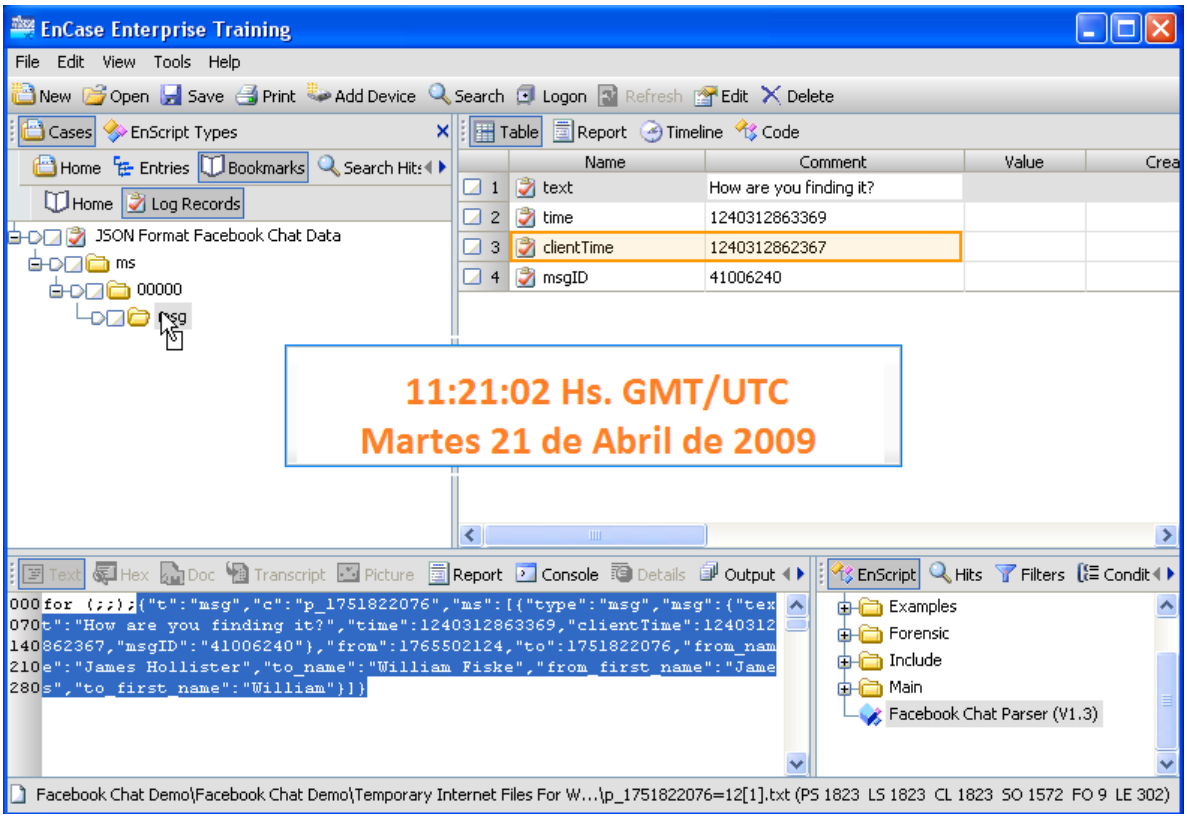



En la misma se identifican los participantes, el texto intercambiado y otros datos adicionales como el horario de envío y recepción del mensaje según se aprecia en la siguiente imagen:




Para las variables que indican la fecha y la hora de envío del mensaje TIME y CLIENT TIME , las mismas están expresadas en Tiempo Unix o Tiempo POSIX el cual se

define como la cantidad de segundos transcurridos desde las cero horas del 1 de enero de 1970 , de modo que para conocer el tiempo expresado de manera usual es necesario efectuar la conversión.
En la imagen siguiente se observa  el horario en que fue enviado ese fragmento de conversación, en Tiempo Unix y se muestra en el recuadro la conversión indicando  la fecha y hora real:




## CONCLUSIONES

- El análisis forense en los servidores de las redes sociales requiere información almacenada en el titular de la red social. Su obtención puede ser tediosa y hasta ilusoria, teniendo en cuenta los tiempos procesales.
- A pesar de lo anterior , resulta posible recolectar evidencia de redes sociales en las computadoras , celulares, y otros dispositivos digitales que el participante haya utilizado
- También resulta posible recolectar evidencia a futuro , capturando el tráfico de Internet de un participante determinado