El Análisis integral de la evidencia digital

Gastón Semprini, Poder Judicial de Río Negro. Licenciado en Sistemas de Información por la Univ. de Belgrano y Experto en informática forense por la Univ. Tecnológica Nacional.

Jefe del área de informática forense del Poder Judicial de Río Negro.

gsemprini@jusrionegro.gov.ar

Abstract. Los Laboratorios Informáticos Forenses deben estar preparados para poder abordar todas las competencias o ramas que ésta disciplina de la ciencia forense establece, en pos de garantizar una correcta reconstrucción del hecho investigado y cumpliendo con los principios del manejo de la evidencia digital establecidos en las normas ISO 27037, la relevancia, la confiabilidad y la suficiencia.

Keywords: competencias de la informática forense, evidencia digital, ISO 27037, suficiencia, SOPs, análisis de registro.

1 Introducción

En el transcurso de los últimos años el Poder Judicial de Rio Negro, ha venido trabajando en el fortalecimiento de las áreas relacionadas a la rama de las ciencias forenses. [1]

Año a año el laboratorio de Informática Forense del Poder Judicial de Rio Negro, viene trabajando en la creación de nuevos protocolos de actuación, procedimientos, metodologías y aplicación de técnicas forenses para llevar adelante el tratamiento de la evidencia digital almacenada en distintos dispositivos tecnológicos. [2] [3]

El objetivo de este trabajo es mostrar la importancia de contar con todos los dispositivos tecnológicos y así poder analizar la evidencia digital en su totalidad, pudiendo de esta manera cumplir con los tres requisitos de manejo de la evidencia digital establecidos en la norma estándar ISO 27037 [4] que son la relevancia, la confiabilidad y la suficiencia.

El avance y la complejidad de los distintos escenarios hacen necesario que el personal que interviene en los secuestros de dispositivos tecnológicos deba contar con las capacitaciones en incautación para garantizar la suficiencia de la evidencia. Más allá de las habilidades y conocimientos de dicho personal, hoy

es posible que se omita o no sea posible el secuestro de todos los dispositivos en el lugar del hecho. Un aporte que puede realizar el informático forense es la incorporación de una etapa de análisis aplicando métodos, técnicas y herramientas forenses que permitan determinar la existencia de dispositivos tecnológicos faltantes en la investigación.

En este análisis se abordarán técnicas específicas que permitan la obtención de información relacionada a la configuración de dispositivos con sistema operativo Windows, el mismo puede extrapolarse a otros sistemas operativos.

2 La interrelación de las competencias en Informática Forense

Teniendo en cuenta lo establecido por diferentes autores, como ser Jeimy Cano, quien asemeja la informática forense con la "digital forensic" [5], acentuando que todas las definiciones de esta especialidad, abordan aspectos ya sea generales y específicos que en todos los casos convergen hacia la identificación, la preservación, la extracción, el análisis, la interpretación, la documentación y la presentación de la evidencia digital.

Los procedimientos, técnicas y herramientas forenses utilizadas serán acorde a las normas estándares y procedimientos de buenas prácticas desarrollados por entidades de gobierno y autores reconocidos.

Dentro de la "Digital Forensic" se encuentra establecida su incumbencia o competencia dividiéndose en diferentes ramas que la constituye. [6]

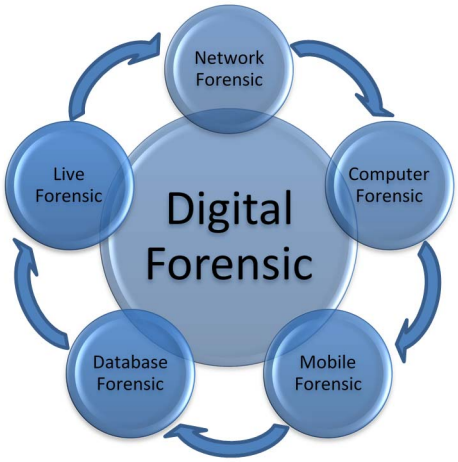

Gráfico 1: Digital Forensic

2.1 **Computer Forensic** es una disciplina de la ciencias forense que, considerando las tareas propias asociadas con la evidencia, procura descubrir e interpretar la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso; o también denominada como la disciplina científica y especializada que, entendiendo o conociendo los elementos propios de las tecnologías de los equipos de computación, ofrece un análisis de la información residente en dichos equipos. [5]

2.2 **Móvil Forensic** la forensia de dispositivos móviles se dedica a la extracción, análisis e interpretación de la información almacenada en los dispositivos móviles tales como Smarphones, Tablet, GPA, PDA, etc. [7]

2.3 **Network Forensic** se encarga de entender las operaciones de las redes computacionales, siguiendo los protocolos y la formación criminalística para establecer los rastros, movimientos y acciones que un intruso ha desarrollado para concluir su acción. Para ello es necesario comprender la manera como los protocolos, las configuraciones y las infraestructuras de comunicaciones se conjugan para dar como resultado un momento especifico en el tiempo y un comportamiento particular. [5]

2.4 **Database Forensic** se encarga del estudio forense de las bases de datos y sus metadatos relacionados. Las bases de datos son inherentemente multidimensionales desde una perspectiva forense, debiendo tener conocimientos específicos que permitan relacionar y determinar acciones sobre los datos almacenados. [7]

2.5 **Live Forensics** se encarga de la recopilación y el análisis de la evidencia, mientras el sistema bajo investigación se encuentra funcionando en tiempo real. La implementación de esta rama se debe a que muchos casos al apagarse el sistema del equipo comprometido se pierde información valiosa que no puede ser recuperada con el análisis tradicional en el laboratorio.

Estas áreas de incumbencia deben trabajar en conjunto y retroalimentándose en el laboratorio, si bien en cada una de ellas se aplican procedimientos, técnicas y herramientas diferentes, es necesario combinarlas para poder analizar la evidencia digital en su totalidad, con el objeto de poder garantizar los tres principios establecidos en la norma ISO 27037, la relevancia, la confiabilidad, y la suficiencia.

3 ISO/IEC 27037: Principio de suficiencia de la evidencia digital.

Con el paso de estos últimos años se ha venido trabajando en la mejora de los procedimientos no solo para secuestro de los distintos dispositivos tecnológicos en el lugar del hecho sino también en métodos y técnicas forenses para el análisis de la evidencia digital.

En una investigación es importante tener claros los conceptos y utilizar los términos más adecuados que determinen el rol que tiene el componente o sistema informático en el procedimiento. Esto nos determinará el tipo de análisis o investigación que llevaremos adelante para la obtención de indicios y más adelante las pruebas necesarias donde se sustente las hipótesis del caso investigado.

Con este propósito se categorizan las pruebas para distinguir entre el elemento hardware y la información contenida en éste, también denominadas evidencia electrónica y digital respectivamente. Esta distinción facilita el diseño de las metodologías y procedimientos adecuados en el manejo y estudio de cada tipo de evidencia consiguiendo un paralelismo entre el escenario físico y el entorno digital. Se debe prestar especial atención a los procedimientos de recopilación y almacenamiento de las evidencias en la escena del delito y asegurar la cadena de custodia de las mismas. Aplicar métodos y pautas para que estas no se alteren a lo largo del proceso y que sean reproducibles por terceras partes en cualquier momento. Permitiendo seguir en todo el proceso las fases de análisis forense digital basadas en un método normalizado. Para lograrlo, los informáticos forenses basan sus investigaciones periciales y análisis forenses digitales en normas y guías de buenas prácticas publicadas al respecto, como RFC (Request for Comments), e ISO (International Organization for Standardization), entre otras. [1]

Las evidencias digitales están adquiriendo formas cada vez más inesperadas en nuevos dispositivos o componentes tecnológicos que desafían los procedimientos y metodologías actuales. En este sentido, los informáticos forenses tratan de entender y asimilar el conocimiento de la tecnología y su forma de operar, para interpretar correctamente la evidencia digital almacenada en ella.[8]

La norma ISO/IEC 27037 “Guía para la identificación, recolección, adquisición y preservación de evidencias digitales”. [4] Es una guía que proporciona directrices para las actividades relacionadas con la identificación, recopilación, consolidación y preservación de evidencias digitales potenciales localizadas en teléfonos móviles, tarjetas de memoria, dispositivos electrónicos personales, sistemas de navegación móvil, cámaras digitales y de video, redes TCP/IP, entre otros dispositivos, para que puedan ser utilizadas con valor probatorio y en el intercambio entre las diferentes jurisdicciones. Esta norma proporciona orientación para los siguientes dispositivos y circunstancias:

1. Medios de almacenamiento digital, como discos duros, discos ópticos, cintas, etc, que se suelen emplear en computadoras y sistemas informáticos.

2. Teléfonos móviles, PDAs, dispositivos personales electrónicos, tarjetas de memoria

3. Sistemas de navegación georreferenciados (GPS)

4. Cámaras digitales y de vídeo

5. Equipos con conexión de red

6. Redes TCP/IP y otros protocolos digitales

7. y todos aquellos dispositivos con funciones similares a los anteriores

La misma hace referencia a tres principios fundamentales de la evidencia digital: la relevancia, la confiabilidad y la suficiencia. Estos tres elementos definen la formalidad de cualquier investigación basada en evidencia digital para garantizar la admisibilidad de la misma.

La relevancia es una condición técnicamente jurídica, que habla sobre aquellos elementos que son pertinentes a la situación que se analiza o investiga, con el fin de probar o no una hipótesis que se ha planteado alrededor de los hechos. Todo aquello que no cumpla con este requisito será irrelevante y excluido del material probatorio recabado para efectos del caso bajo estudio.

La confiabilidad es otra característica fundamental, que busca validar la repetibilidad y auditabilidad de un proceso aplicado para obtener una evidencia digital. Esto es, que la evidencia que se extrae u obtiene es la que deber ser, y que, si un tercero sigue el mismo proceso, deberá obtener resultados similares verificables y comprobables.

Finalmente el tercer principio es la suficiencia, la cual está relacionada con completitud de pruebas informáticas, es decir que, con las evidencias recolectadas y analizadas tenemos elementos suficientes para sustentar las hipótesis del hecho investigado. Este elemento está sujeto a la experiencia y formalidad del informático forense en el desarrollo de sus procedimientos y priorización de esfuerzos.

Esta norma ha determinado que estos tres principios, establecen las condiciones necesarias y suficientes para que los expertos en informática forense recaben, aseguren y preserven elementos materiales probatorios sobre medios digitales, los cuales podrán ser revisados y analizados por terceros interesados.

En toda investigación judicial, pueden encontrarse distintos dispositivos tecnológicos que fueran previamente secuestrados para establecer un hecho determinado. El funcionario, magistrado o los propios informáticos forenses no tienen la certeza si se cuenta con todos los dispositivos tecnológicos que permitan esclarecer dicha investigación.

Ahora bien, para garantizar la **suficiencia** con respecto a los dispositivos involucrados en el lugar del hecho, es necesario incorporar en la etapa de análisis, un procedimiento que permita determinar el faltante de dispositivos tecnológicos que no se hayan tenido en cuenta en la etapa de secuestro y que podrían contener evidencia digital importante para sustentar las hipótesis del hecho investigado.

Para ello es necesario aplicar métodos y técnicas de análisis forenses a los dispositivos tecnológicos secuestrados, que puedan brindar información de otros dispositivos que puedan haber tenido participación en el hecho investigado y que no se encuentren secuestros. Una de las técnicas más frecuentes en este tipo de análisis, es determinar los últimos dispositivos que fueron conectados en forma física o inalámbrica como ser USB, Wifi, bluetooth, etc.

4 Procedimientos para fortalecer el principio de suficiencia

Para poder determinar la interrelación de los dispositivos, es necesario conocer su estructura y la manera en que guardan información de los eventos y acciones llevadas a cabo.

Para los dispositivos con sistema Windows toda esta información se almacena en una gran base de datos denominada Registro de Windows o también Registry [9].

Es importante entender qué es el Registro, por qué existe y los tipos de información que contiene. Prácticamente todo lo hecho en Windows se almacena en el Registro. Con cada acción tomada por el usuario se hace referencia al Registro de una manera u otra.

La estructura del Registro está conformada por claves y valores. Hay 5 claves raíz predefinidas, que son HKEY_CLASSES_ROOT (HKCR), HKEY_CURRENT_USER (HKCU), HKEY_LOCAL_MACHINE (HKLM), HKEY_USERS (HKU), HKEY_CURRENT_CONFIG (HCU).

Para el análisis previo relacionado a la suficiencia, será necesario verificar la información contenida en HKLM, ya que esta almacena configuración especificas del equipo. Esta calve, contiene 4 sub claves SAM, SECURITY, SYSTEM, SOFTWARE, las cuales se cargan en el tiempo de arranque de sus respectivos archivos ubicados en \Windows\System32\config

SAM contiene todas las cuentas integradas (principalmente alias de grupo) y cuentas configuradas (usuarios, grupos y sus alias, incluyendo cuentas invitadas y cuentas de administrador), creadas y configuradas en su respectivo dominio, ya que cada cuenta en ese dominio contiene el nombre de usuario que se puede utilizar para iniciar sesión en ese dominio, el identificador interno y ex-

clusivo del usuario en el dominio, una función hash criptográfica de la contraseña de cada usuario para cada protocolo de autenticación habilitado, la ubicación del almacenamiento de su subárbol de registro de usuario, varios indicadores de estado (por ejemplo si la cuenta se puede enumerar y hacer visible en la ventana emergente de inicio de sesión), y la lista de dominios (incluido el dominio local) en el que se configuró la cuenta.

SECURITY está vinculada a la base de datos de seguridad del dominio en el que ha iniciado sesión el usuario.

SYSTEM Contiene información sobre el programa de instalación del sistema de Windows, la lista de los dispositivos montados, contienen configuraciones alternativas de los servicios y controladores del hardware del sistema, todos los dispositivos Plug-and-Play conocidos y los asocia a los controladores de sistema instalados, todos los programas que funcionan como servicios, controladores de hardware y la configuración del resto del sistema.

SOFTWARE contiene ajustes de software y de Windows (en el perfil predeterminado de hardware). Resulta modificada principalmente por los instaladores del sistema y de las aplicaciones.

4.1 Detección de dispositivos en sistema Windows.

Para la detección de los dispositivos que interactuaron, es necesario realizar un análisis de registro del sistema analizado y obtener al menos la siguiente información:

Dispositivos conectados por USB.

Saber qué dispositivos USB se han conectado a un sistema ayudara al informático forense en detectar posibles pruebas adicionales que pueden ser cruciales para la investigación. Es importante destacar que cada vez que un dispositivo se conecta al bus serie universal (USB), los controladores se consultan y la información del dispositivo como ser el ID del producto, nombre, fecha de conexión se almacena en el registro. Dichos dispositivos USB pueden ser discos externos, una cámara digital, pendrive, dispositivos móviles, gps, memorias sd, etc y última fecha de conexión. Esta información es obtenida de la clave HKLM\SYSTEM\ControlSet00x\Enum\USBSTOR

Dispositivos en red de área local.

Esta información ayudara al informático forense a poder detectar otros dispositivos conectados en una red local. Windows implementa una herramienta de asignación de red denominada *Mi lugar de red*, que permite a los usuarios encontrar fácilmente otros usuarios dentro de una LAN o Red de área local. Un

equipo en una LAN debidamente configurada debe poder mostrar todos los usuarios de esa red a través de Mi lugar de red. Esta lista de usuarios u ordenadores, como muchas otras cosas, se almacena en el Registro. Por lo tanto, incluso después de que el usuario ya no está conectado a la LAN, la lista de dispositivos sigue permaneciendo. La clave de Registro donde se almacena esta información es HKCU\Software\ Microsoft \ Windows \ CurrentVersion \ Explorer \ ComputerDescriptions. La clave ComputerDescriptions es útil para determinar si un usuario estaba conectado a determinados equipos o pertenecía a una LAN específica.

Dispositivos montados

Esta información puede ser útil para el informático forense, ya que muestra los dispositivos de hardware que deben conectarse al sistema. Por lo tanto, si un dispositivo se muestra en la lista de MountedDevices y ese dispositivo no está físicamente en el sistema, puede indicar que el usuario retiró la unidad en el intento de ocultar la evidencia. En este caso, el examinador sabrá que tienen pruebas adicionales que deben ser incautadas. La clave de registro que hace posible ver cada unidad asociada con el sistema es HKLM\SYSTEM\MountedDevices y almacena una base de datos de volúmenes montados que es utilizada por el sistema de archivos NTFS.

Conexiones inalámbricas

Una placa de red inalámbrica obtiene puntos de acceso inalámbricos dentro de su rango, que están identificados por su SSID o identificador de conjunto de servicios. Cuando un usuario se conecta a una red o hotspot, el SSID se registra en el sistema de Windows como una conexión de red preferida. La información se guarda en la clave de registro HKLM\SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces.

Además de registrar el nombre del SSID, Windows también registra la configuración de red de esa conexión en particular, como la dirección IP, el dominio DHCP, la máscara de subred, etc. La clave del registro en la que se puede encontrar es HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces.

4.2 Herramientas para garantizar la suficiencia.

Si bien dentro del laboratorio del Poder Judicial de Rio Negro se utilizan herramientas licenciadas como EnCase, FTK, IEF, es importante destacar que no es indispensable contar con estas herramientas ya que hay disponible software open source como ser RegRipper, Forensic Registry EDitor (FRED) que permiten obtener la información anteriormente detallada. La única diferencia

que podemos observar es la forma de presentación o reporte de los datos recolectados.

Todas estas herramientas tienen en común que la información recolectada se realiza desde las claves anteriormente explicadas.

4.3 Procedimiento Operativo Estandarizado de Registro de Sistema

Tomando el modelo propuesto por el SWGDE (Scientific, Working Group on Digital Evidence), se establece el siguiente procedimiento operativo.

Propósito:

Este procedimiento representa la extracción y análisis de los principales archivos del sistema operativo windows, con el objetivo de visualizar las características del hardware analizado, usuarios que utilizaron el dispositivo, los distintos dispositivos externos que se conectaron, última instalación y ultimo inicio del sistema operativo, configuración de zona horaria, etc.

Alcance:

Este procedimiento se aplica al examen y análisis de imágenes forenses.

Equipamiento:

Hardware:

a. Computadora Forense

Software:

a. Software Forense

Limitaciones:

Los resultados dependerán de las capacidades y limitaciones de las herramientas elegidas, como así también la experiencia del perito.

Procedimiento:

Los pasos del procedimiento deben ser documentados con suficiente detalle, de manera que permita a otro forense, competente en la misma área, ser capaz de identificar que se ha hecho y evaluar los resultados independientemente.

1. Identificación de datos

a. Realizar identificación de los archivos de sistema (SAM, SYSTEM, SECURITY, SOFTWARE) y configuración perteneciente a cada usuario (NTUSER.DAT).

b. Exportar archivos y sus respectivos hash

2. Análisis

2.1 Procesar con software forense el registro de sistema

a. Obtener características del Sistema Operativo (ultimo inicio, ultimo usuario que lo utilizo, apagado y reinstalación del sistema)

b. Obtener las características de los dispositivos USB conectados y compararlos con los demás dispositivos aportados.

c. Obtener todos los usuarios registrados en el sistema operativo y sus respectivos ID.

d. Obtener último acceso a la red. (IP de conexión local y público).

e. Obtener últimos documentos (impresos y consultados)

3. Reporte.

a. Extraer los resultados a un anexo

b. Incluir en el informe pericial listado de dispositivos conectados que no fueron aportados

5 Conclusión: la importancia de la suficiencia

El informático Forense es “la persona que permitirá avanzar en la búsqueda de la verdad, en el análisis de la información residente en los dispositivos tecnológicos y realizar una reconstrucción de los hechos en base a la evidencia digital analizada” [5].

En la práctica la implementación de este SOP nos ha permitido brindar datos específicos para dar con el responsable del hecho investigado. En un allanamiento puede suceder que no se encuentre presente el principal sospechoso, faltando secuestrar los elementos que tenga en su poder. Un caso concreto de distribución de pornografía infantil que hemos tenido en el Departamento de Informática Forense del Poder Judicial de Rio Negro, el principal sospechoso no se encontraba en el domicilio allanado, secuestrándose todos los dispositivos tecnológicos. Con esta técnica de análisis pudimos determinar que faltaban elementos, un dispositivo móvil marca Samsung, modelo SM-J700M/DS y un disco externo de 1TB marca Toshiba. Con un nuevo allanamiento hemos podido dar con más elementos que no solo permitieron relacionar y vincular esos dispositivos físicos con el presunto autor, sino también establecer las distintas maniobras realizadas para el consumo y distribución de pornografía infantil, analizando las distintas actividades en redes sociales, accesos a internet, conversaciones de whatsapp, imágenes, videos distribuidos por distintos medios.

La medida de un nuevo allanamiento estará enmarcada en la ley 5020 en el Capítulo III (Desarrollo de la Investigación) del nuevo Código Procesal Penal de la Provincia de Rio Negro en los artículos 134 (Informe de Experto), 138 (Allanamiento y Registro de Morada), 140 (Autorización), 142 (Entrega de Objetos o Documentos), 143 (Procedimiento para el Secuestro) y 150 (Anticipo Jurisdiccional de Prueba) respectivamente. [11]

Para poder realizar una reconstrucción de los hechos investigados es importante contar con todos los dispositivos tecnológicos involucrados, garantizando el principio de “suficiencia” establecido en la norma ISO 27037. Si bien la norma estándar, no se establece el “como” contemplar dicho principio, se planteó la necesidad de incorporar al análisis este SOP para el descubrimiento de dispositivos que no hayan sido secuestrados. En este trabajo se abordaron técnicas sobre dispositivos con sistemas operativos Windows, que nos llevó a la creación de un “procedimiento operativo estandarizado de Registro de Sistema” que entre otras finalidades, permite la detección de dispositivos faltantes relacionados con los analizados.

Para probar la hipótesis del hecho investigado es importante contar con toda la evidencia digital. La integración y el análisis de la misma en su totalidad, permitirá al informático forense entender la correspondencia que tiene un dispositivo y su relación con los otros dispositivos presentes, logrando así una reconstrucción del hecho investigado.

6 Referencias:

1. Lic. Gaston Semprini “Lineamientos para la creación de un Laboratorio Informático Forense” SID 2016. Anuales 45 JAIIO – Jornadas Argentinas de Informática. Capital Federal
2. Lic. Gerardo Nilles, Lic. Gaston Silva “Pericias informáticas para casos de pornografía infantil” SID 2016. Anuales 45 JAIIO – Jornadas Argentinas de Informática. Capital Federal
3. Lic. Gaston Semprini “Estandarización de procedimientos y protocolos del laboratorio de Informática Forense”. SID 2015. Anuales 44 JAIIO – Jornadas Argentinas de Informática – Rosario
4. International Standard ISO/IEC 27037, adquiridas por el Poder Judicial de Rio Negro.
5. Cano, Jeimy. Computación Forense. Descubriendo los Rastros Informáticos. Alfaomega. Méjico. (2009)
6. https://www.tech4law.co.za/tech-advisor/107-digital-forensics/1528-what-is-digital-forensics
7. Olivier, Martin S. (March 2009). "On metadata context in Database Forensics”
8. Guía actualizada para futuros peritos informáticos. Últimas herramientas de análisis forense digital. Caso práctico. http://www.pensamientopenal.com.ar/system/files/2016/05/doctrina43429.pdf
9. Registro de Windows. https://technet.microsoft.com/en-us/library/cc939931.aspx
10. Análisis de Registro. http://www.forensicfocus.com/a-forensic-analysis-of-the-windows-registry
11. Ley 5020 Código Procesal Penal de La Provincia de Rio Negro http://servicios.jusrionegro.gov.ar/inicio/web/normativa/NCPP.php