NORMALIZACION DIGITAL FORENSE - ¿Qué es y cómo se gestiona la evidencia digital?

Palabras claves: análisis, digital, forense, pericias, informática, normalización, electrónica, evidencia, smartphones, móviles, proceso, justicia, investigación, dispositivos, computadoras, ISO, IEC, NIST,

A fines del siglo pasado, evidencia digital se definía como aquella información de valor probatorio que se almacenaba o transmitía en forma binaria. Posteriormente, el adjetivo binario cambia por digital. De acuerdo con esta definición, la evidencia no solo se circunscribe a aquella que se encuentra dentro de computadoras, sino que el concepto se extiende para incluir la información presente en todo tipo de dispositivos electrónicos digitales, como sistemas de telecomunicaciones, multimedia, smartphones, sistemas electrónicos hogareños, industriales, etc. No se limita a los delitos informáticos tradicionales, como la piratería e intrusión, sino que engloba todas las categorías de delitos.

Actualmente se considera que la evidencia digital es la información o los datos almacenados o transmitidos en formato binario que se ha determinado como relevantes para una investigación a través del proceso de análisis.

Si se ha procesado correctamente puede aprovecharse al máximo en distintos escenarios y, en cada uno de ellos, existe una orientación diferente respecto de lo que se pretende obtener:

- calidad probatoria,
- precisión en el análisis,
- restauración del servicio, o
- el costo de la recolección de la evidencia.

La evidencia digital debe ser **relevante**, un concepto jurídico que indica que debe estar relacionada con los hechos investigados. También debe ser **confiable**, esto es repetible y auditable por un tercero que usando el mismo principio de operación llegue a idénticos resultados. Finalmente, la evidencia recolectada debe ser **suficiente** para sustentar los hallazgos obtenidos.

La evidencia digital presente en la memoria principal de una computadora o servidor es **evidencia volátil**, que se pierde cuando se apaga la computadora o el servidor donde reside. Esta es una característica intrínseca de las memorias RAM que mantienen sus datos solo mientras la alimentación está conectada (mientras permanece encendido el dispositivo). Por el contrario, las memorias FLASH, los discos de estado sólido y magnéticos en todas sus variantes contienen **evidencia no volátil**, que permanece aún con el sistema sin energía eléctrica.

A lo largo del mundo se han abordado diferentes aproximaciones, modelos teóricos y procedimientos prácticos para la obtención, manipulación y gestión de la evidencia digital. En la República Argentina no existe un modelo integral o protocolo común, solo iniciativas aisladas de algunas universidades y dependencias del poder judicial de diversa calidad académica.

Para proporcionar **credibilidad** a la investigación se necesita aplicar una adecuada metodología y contar con individuos calificados para desarrollar las tareas especificadas en la metodología. En **Cyber Analytics S.A** cubrimos ambos requisitos. El procedimiento para el manejo de la evidencia digital que utilizamos sistematiza la identificación, recolección, adquisición, análisis y preservación de la misma. Estos procesos están diseñados para mantener la integridad de la evidencia con una metodología aceptable para contribuir a su admisibilidad en procesos legales y en sintonía con las normas ISO 27037:2012 y desde julio del corriente año, también con su contraparte argentina IRAM ISO 27037:2022. La evidencia digital se manipula en nuestro laboratorio dentro de una jaula de Faraday que produce un perfecto blindaje electromagnético y, nuestros profesionales son todos ingenieros con estudios de posgrado, profesores universitarios y con experiencia de muchos años en análisis digital forense aplicados tanto a instituciones estatales como privadas/corporativas.

Es muy importante destacar que la evidencia digital es por naturaleza frágil y puede alterarse o destruirse con una gestión inadecuada. Por ejemplo, al abrir un archivo de texto simplemente para visualizar su contenido se modifica la última fecha de acceso al mismo. La admisibilidad de la evidencia en un tribunal de justicia es consecuencia del correcto tratamiento de la misma, respetando protocolos de actuación estándar. Los organismos de referencia en la normalización de estos protocolos son el Instituto Nacional de Estándares y Tecnologías (NIST, del inglés National Institute of Standars and Technologies) y la Organización Internacional de Normalización. (ISO, del inglés International Organization for Standardization). El NIST es una agencia encargada de la definición y el mantenimiento de estándares y recomendaciones que promueven la innovación y la competencia industrial dentro de los Estados Unidos. ISO es una organización independiente y no gubernamental que genera y promueve el uso de estándares a nivel mundial. El Comité Conjunto Técnico ISO/IEC se encarga desde 1987 de desarrollar, mantener, promover y facilitar estándares relacionados con la Tecnología de la Información. No es suficiente con seguir procedimientos estándar, se necesita además que los individuos que intervienen sean competentes para identificar los riesgos y las consecuencias de posibles cursos de acción. La norma ISO/IEC 27037:2012 es un estándar global para identificar, recolectar, adquirir y preservar evidencia digital. Esta norma define dos roles de especialistas en la gestión de la evidencia digital potencial: el DEFR (Digital Evidence First Responder) y el DES (Digital Evidence Specialist).

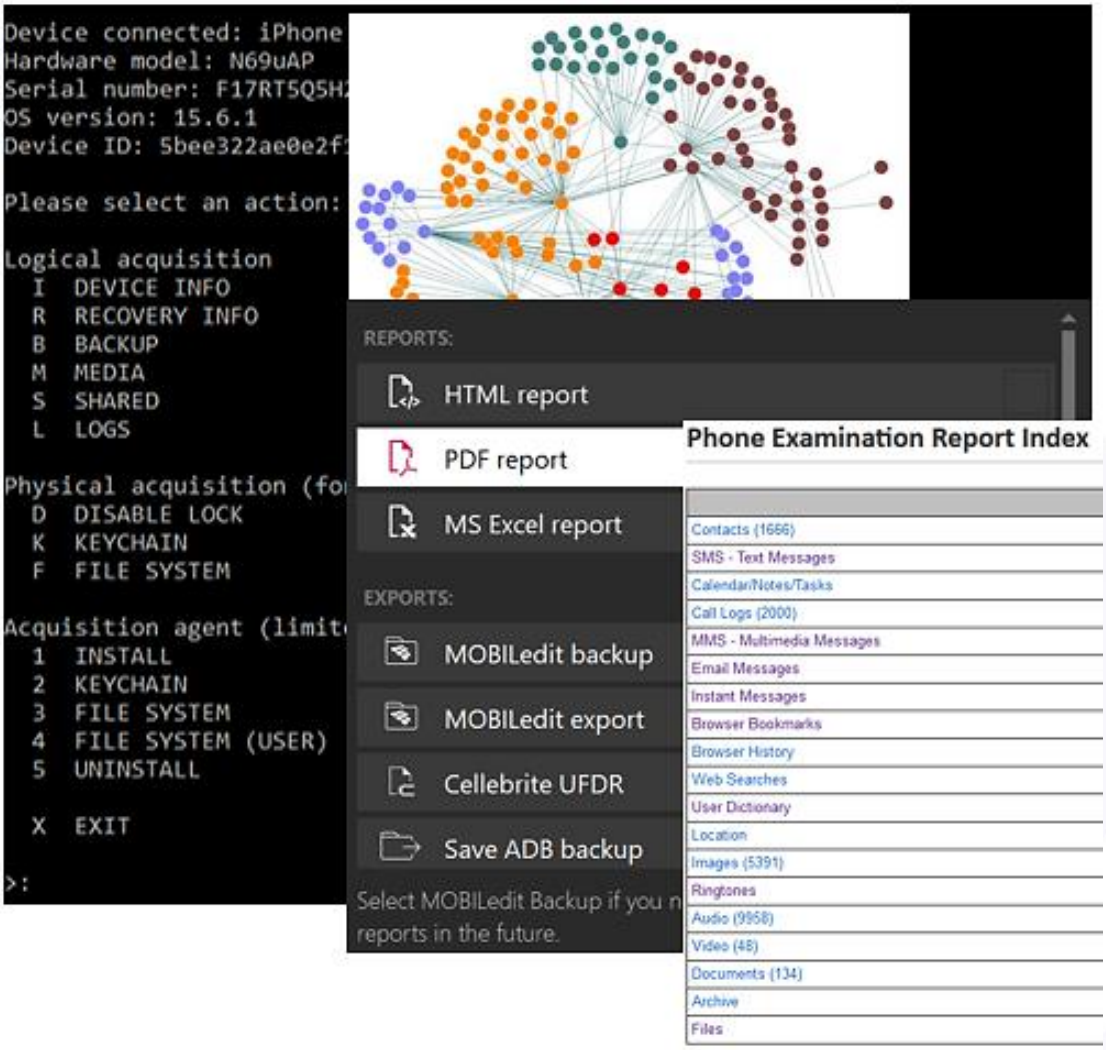
El DEFR es aquella persona que está autorizada, formada y habilitada para realizar el trabajo de campo en la escena de un incidente, recolectando las evidencias digitales con las debidas garantías.

El rol del **DEFR** es llevado a cabo, en nuestro país, por personal policial debidamente capacitado. Para garantizar la autenticidad y confiabilidad de la evidencia, el DEFR minimiza la manipulación de los datos y los dispositivos digitales; documentando todas las acciones y cambios que se hagan a la evidencia de forma tal que un tercero pueda validar y emitir opinión respecto de la confiabilidad de la evidencia recolectada. Debe además proceder conforme el marco legal y no actuar más allá de su área de competencia.

El **DES** es aquella persona que comúnmente llamamos perito y por supuesto, su incumbencia incluye a la del DEFR. El DES debe tener competencias específicas y formación profesional para aplicar de manera correcta protocolos y herramientas forenses, así como la experiencia necesaria para desarrollar la tarea encargada. Su función es llevar a cabo todo el proceso de análisis digital forense a partir de los oficios y solicitudes que encarguen los órganos judiciales o las partes para concluir con un informe pericial describiendo los procedimientos empleados y el razonamiento lógico aplicado.

Pero, ¿Qué es el análisis digital forense? En el artículo El tratamiento de la evidencia digital y las normas ISO/IEC 27037:2012, S. Roatta, M. E. Casco, M. Fogliato presentado en el XXI Congreso Argentino de Ciencias de la Computación en Junín, 2015; acuñamos por primera vez la expresión **análisis digital forense** como la aplicación de **técnicas científicas y analíticas especializadas que permiten identificar, recolectar, adquirir, preservar, analizar y presentar datos que sean válidos en un proceso legal**.

Imágenes de diversas herramientas forenses:



Es una disciplina que comienza con los orígenes mismos de la electrónica digital pero se ha desarrollado de manera diferente. Mientras el hardware digital y la informática han tenido un desarrollo y difusión tan extendido que son un acabado ejemplo de la llamada globalización; la informática forense tiene un modelo de actuación propio según las leyes de cada país. El principio de intercambio de Locard, base de la ciencia forense, afirma que *"siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto"*. Esto se cumple también cuando se manipulan evidencias digitales, por lo que es importante ser muy cuidadoso en todo el proceso de análisis para que las evidencias no se alteren o contaminen. Buenas prácticas con metodologías probadas evitan cometer errores graves de los cuales no hay retorno.

El análisis digital forense tiene un desarrollo bastante reciente en Argentina, en donde los peritos particulares o de oficio se matriculan en colegios profesionales que regulan su actividad profesional y se inscriben en listas del poder judicial donde las pericias se asignan mediante sorteos.

El artículo 183 del Código Procesal Penal de la Provincia de Santa Fe define quienes pueden ser peritos: *"Los peritos deberán tener título de tales en la materia sobre la que han de expedirse, siempre que la profesión, arte o técnica, estuvieran reglamentados. De existir peritos oficiales, la designación recaerá en los que correspondan; en caso contrario, entre los funcionarios públicos, que en razón de su título profesional o de su competencia se encuentren habilitados para emitir dictamen acerca del hecho o circunstancia que se quiera establecer. En su defecto, si no los hubiera, y no mediando acuerdo de partes, deberá designarse a persona de idoneidad manifiesta".*

Las actividades de los peritos pueden comprometer el interés público y sus profesiones están incluidas en la nómina del artículo 43 de la Ley N° 24.521. La resolución 1254/2018 del Ministerio de Educación define las actividades profesionales reservadas de aquellas profesiones que están reguladas por el estado en virtud de que su ejercicio puede comprometer el interés público.

Un exhaustivo análisis de esta resolución circunscribe los peritos a las siguientes profesiones: Ingeniería Electrónica, Licenciatura en Ciencias de la Computación, Licenciatura en Sistemas, Licenciatura en Sistemas de Información, Licenciatura en Informática, Ingeniería en Computación, Ingeniería en Sistemas de Información e Ingeniería en Informática. En el fuero penal los fiscales eligen el laboratorio del gobierno que consideren adecuado para realizar una pericia: la Policía Federal Argentina, las policías provinciales, la Policía de Seguridad Aeroportuaria, Gendarmería Nacional, Prefectura Naval Argentina, la Agencia Federal de Investigaciones y algunas procuradurías y ministerios públicos de la acusación de diversas jurisdicciones. No es habitual que sus peritos posean alguna de las profesiones enumeradas en el párrafo anterior, lo que constituye una gran debilidad a solucionar. Es por esto que, en casos complejos, los jueces recurren a universidades públicas o a profesionales particulares de trayectoria reconocida.

En algunos casos nuestro trabajo finaliza con la interpretación de la evidencia digital, esto es la evaluación y el análisis dentro del contexto de lo solicitado, produciendo una explicación de los hechos encontrados durante el análisis. Si los hechos se prestan a más de una interpretación razonable el resultado del análisis debe mostrar todas las alternativas indicando si es posible sus respectivas probabilidades.

Autor del artículo: **Santiago Enrique Roatta**. Ingeniero Electrónico. Jefe del Laboratorio de electrónica forense de Cyber Analytics S.A. Docente en Ingeniería Electrónica de la Universidad Nacional de Rosario. Docente de Sistemas de Hardware y Seguridad Informática de Ingeniería en Sistemas Informáticos de la Universidad Abierta Interamericana. Perito en el laboratorio forense de la Escuela de Electrónica de la Universidad Nacional de Rosario desarrollando tareas para cumplir el convenio de la Corte Suprema de Justicia con la UNR.

30 de Septiembre de 2022