Sampaoli, Javier A.

Peritaje informático: marco teórico-practico

Tesis de Licenciatura en Sistemas y Computación
Facultad de Química e Ingeniería "Fray Rogelio Bacon"

Facultad de Química e Ingeniería del Rosario

Universidad Católica Argentina

Peritaje - Marco Técnico Práctico

"Presentado en cumplimiento parcial de los requisitos para la obtención del título de LICENCIADO EN SISTEMAS Y COMPUTACIÓN"

Alumno: Javier A. Sampaoli

Profesor/Tutor: Cristina Bender

Fecha de Presentación: 6 de Diciembre de 2018

AGRADECIMIENTOS

Agradecer es mirar atrás, volver a andar el camino recorrido, observar desde la distancia y sentir que todas y cada una de las personas aquí nombradas debieron participar para que este trabajo llegue a concretarse. Agradecer es una necesidad del alma, porque sabemos que juntos, se puede llegar mejor, se puede llegar más lejos, se aprende de la visión del otro, y, además, se disfruta del camino. Es por esto que quiero agradecer:

A mis padres Marta y Juan Carlos, que hicieron un gran esfuerzo y me inculcaron principios, honestidad, perseverancia y a mis hermanos que estuvieron a mi lado siempre.

A profesionales y colegas como: Dra. Ma. Jimena Bertolotti, Juan Casales, José Marusich, quienes me apoyaron técnicamente y moralmente para que esto sucediera.

A la Facultad de Química e Ingeniería, mi facultad, en la cual conviví tantos años y agradezco esos momentos tan lindos que pase, junto a mis compañeros de curso, al personal docente y no docente.

Al Sr. Carlos Contrino, por estar siempre, en todos estos años de estudio y de compartir tan gratos momentos.

A la Profesora y tutora Cristina Bender, a Eduardo Rodriguez y al Decano Dr. Francisco Casiello por darme la posibilidad de responder a este último trabajo y compromiso con la Facultad.

Y Por último un especial agradecimiento a mi señora y a mis hijos que son mi sostén y que día a día me ayudan a seguir adelante y a tomar responsabilidades como esta.

A todos muchas gracias…..

RESUMEN

El aumento progresivo de la tecnología, en lo referente a equipos informáticos y de telecomunicaciones con acceso a internet, ha traído como consecuencia que se incremente de manera significativa los incidentes de seguridad informática.

Aquí es donde entra a jugar un papel importante la informática forense a través del peritaje, la cual se enfoca en la búsqueda de posibles autores de delitos informáticos.

La informática forense aplica una serie de técnicas y métodos de investigación que permiten reconstruir, lo más fielmente posible, la secuencia de eventos que tuvieron lugar en uno o en varios equipos informáticos, o en toda una plataforma tecnológica, para la ejecución exitosa de un incidente de seguridad informático.

La finalidad de este trabajo es ofrecer un documento de referencia actualizado, de carácter general y práctico, con los aspectos técnico-legales que el futuro perito informático forense debe conocer y brindar una mirada introductoria a la informática forense mediante un caso práctico completo, donde la evidencia digital es la protagonista del proceso que finaliza con el dictamen del informe pericial. Uno de los objetivos es enfocar esta ciencia desde el prisma del derecho informático, la deontología, la ética y el profesionalismo del perito informático. La gran demanda de expertos en peritaje y análisis forense digital abre las puertas al mercado laboral a estudiantes y profesionales informáticos. En este contexto, el presente trabajo sirve para consolidar conceptos de buenas prácticas y encauzar al lector en esta novedosa ciencia: **Informática Forense.**

Palabras Clave: Perito, Informática, Forense, Incidente, Análisis, Digital, Delito.

INDICE

INTRODUCCION

Es imposible dejar de reconocer la importancia que en la actualidad poseen los sistemas informáticos como motor fundamental en la gestión y procesamiento de la información sostenida en una organización, para el cumplimiento a cabalidad de su lógica de negocio. Y en forma concomitante ha crecido en importancia todo lo relacionado con la seguridad informática para las organizaciones.

Hoy es prácticamente imposible para una organización no estar sistematizada y por ende dejar de preocuparse por la seguridad de sus activos de información, los cuales se ven enfrentados a unas amenazas latentes generadas principalmente por la interconexión de su red interna con redes externas gracias al enlace proporcionado por el proveedor que le da salida a internet. Aunque existen otras amenazas importantes no derivadas por esta condición, como la ingeniería social, de la cual también hablaremos en este trabajo.

Es muy importante tener en cuenta que dependiendo la magnitud de la organización y su importancia en el mercado, así deberá manejar su proceso de gestión de la seguridad tanto de su plataforma tecnológica como de sus activos de información. Esto se explica en el sentido de que una organización con un reconocimiento ínfimo en el mercado no tendrá el mismo interés de ser atacado en su plataforma tecnológica, que aquella organización con una imagen sólida.

Lastimosamente ningún sistema informático puede ofrecer una seguridad absoluta, siempre existen vulnerabilidades que no se pueden anular y en este caso las organizaciones deben tratar de mitigarlas al máximo. Esto se consigue mediante la implementación de un Sistema de Gestión de Seguridad de la Información.

En atención a lo anterior, los incidentes de seguridad informática en las organizaciones serán noticia permanente, ya que no existe forma de impedir que se den ataques que traten de aprovecharse de las vulnerabilidades que se pueden dar en un sistema informático en busca de un objetivo específico, como puede ser robo de información misional, robo de datos financieros (cuentas bancarias, tarjetas débito / crédito), denegación de servicio, web defacement, satisfacción personal, etc.

Aquí es donde cobra un papel primordial un área de la seguridad informática denominada análisis informático forense, como conjunto de técnicas aplicadas a la resolución de un incidente de seguridad informática.

El análisis informático forense permite, aplicando unas metodologías y unas técnicas en conjunto con una serie de herramientas tanto de hardware como de software, intentar

descubrir inquietudes sobre el incidente tales como: **¿desde dónde?**, **¿qué se atacó?**, **¿de qué forma?**, **¿quién(es) atacó(aron)?** y **¿en qué periodo de tiempo?** se dieron los hechos.

MOTIVACION Y ENFOQUE

El análisis informático forense es un área de la seguridad informática que evoluciona en forma constante con los avances tecnológicos y en paralelo con el perfeccionamiento de los ataques informáticos. Es un área que se apoya sustancialmente en el software para el cumplimiento de sus objetivos, para lo cual existe una amplia gama de aplicativos que permiten investigar un incidente desde muchas perspectivas. Estos aplicativos, al igual que la rama de la informática que soportan, siguen evolucionando al paso de la tecnología para lograr los mejores resultados.

Una de las circunstancias que hace al análisis forense informático tan atractivo, es porque le permite al investigador encontrar siempre las herramientas de software idóneas frente a lo que esté investigando. Claro que esto se debe combinar con aspectos importantes como los son la experiencia y la proactividad del investigador.

A través del presente trabajo se tratará de presentar de la forma más objetiva, clara, detallada y profesional, la efectividad y aplicabilidad de algunas de las herramientas de software más representativas del mercado encaminadas a la investigación informática forense y proponer un marco de trabajo (Frameworks), de buenas prácticas para asegurar un buen desempeño en la labor de Perito Informático.

PROPOSITO

El propósito de este trabajo es servir como marco de referencia para estudiantes, docentes e investigadores de la informática forense en sus procesos de peritaje y enseñanza, demostrando mediante pruebas de hardware y software simuladas y el acompañamiento de imágenes y gráficos detallados, la efectividad y aplicabilidad de herramientas de software según la función que desarrolla cada una de ellas.

ALCANCE

El alcance de este trabajo a nivel académico es muy amplio, ya que abarca a estudiantes, docentes e investigadores, esparcidos en todo el planeta a donde ha llegado la tecnología y las telecomunicaciones, lógicamente Internet, y por ende la amenaza real de ataques informáticos.

ESTRUCTURA DEL TRABAJO

Este trabajo se estructura de la siguiente manera:

En el capítulo 1 se presenta el Estado del Arte en lo que corresponde al tema escogido. En este capítulo se hace referencia a definiciones, conceptos y literatura base existente para el entendimiento de los temas posteriores.

En el capítulo 2 se presenta al Hardware Forense, los distintos equipos informáticos realizados físicamente para la extracción de datos, como la copia bit a bit (clonado) y con conexiones externas de hardware con información, como discos rígidos, celulares, etc., para realizar la labor el perito en los distintos dispositivos que se presentan en un incidente en caliente.

En el Capítulo 3 se presenta el Software Forense, en forma clara y detallada las distintas herramientas de aplicación orientados a extraer datos de los dispositivos informáticos y resguardar la integridad de los mismos como el uso de la técnica del Hashing.

En el capítulo 4 se presenta el Aseguramiento "físico" de las pruebas, lo que debe tener en cuenta un perito informático para cuidar que la cadena de custodia se cumpla, rotulando y etiquetando todo dispositivo informático y la evidencia digital, asegurando la validez de la prueba en un proceso penal.

En el Capítulo 5 se presenta la Evidencia Digital y la descripción de los componentes a peritar para obtener dicha Evidencia, los principios y consideraciones para realizar la extracción.

En el Capítulo 6 se presenta Actas, las formalidades de un acta en un peritaje, el contenido, el formato y el ingreso de los datos según los las Reglamentaciones vigentes, normalmente utilizadas en un allanamiento.

En el Capítulo 7 se presentan las Buenas Prácticas, las metodologías y el marco de trabajo(frameworks), propuesto como objetivo, de acuerdo a las distintas normas internacionales y de casos de éxito respecto a la labor del perito en un análisis informático forense, que permitan alcanzar el objetivo principal frente a un incidente: descubrir la verdad de lo sucedido, con las conclusiones finales de la temática elegida acompañada de las biografías, referencias y cibergrafía consultada para tal fin.

1. ESTADO DEL ARTE

1.1. Conceptualización.

1.1.1 Informática.

El diccionario de la Real Academia de la Lengua Española (2001), presenta la siguiente definición: “Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores”. [1]

La palabra Informática tiene su origen en Francia, procede de la palabra francesa informatique, formada por la conjunción de las palabras "information" y "automatique". La historia nos dice que esta palabra fue utilizada por primera vez por el ingeniero Philippe Dreyfus en el año 1962.

Una definición más acorde con lo que esta palabra representa en la actualidad sería decir que la informática es la ciencia que estudia el tratamiento automático y racional de la información en equipos de cómputo, equipos electrónicos y sistemas de información, la cual se basa en múltiples ciencias como la física, la matemática, la electrónica, entre otras.

- Historia y Evolución: La informática nació para facilitar tareas al hombre, ya que gracias a ella podemos realizar procedimientos complejos con gran exactitud, minimizando la probabilidad del error y con una rapidez imposible de alcanzar de forma manual o mecánica. Desde sus inicios ha ido evolucionando en forma progresiva y sin latencia. Podemos señalar como un momento fundamental en el desarrollo de la informática:
    - el momento en que IBM mostró en sociedad el primer computador personal, con un procesador Intel 8088 y software desarrollado por Bill Gates y Paul Allen, específicamente sistema operativo D.O.S y lenguaje de desarrollo BASIC.
    - ARPANET, la cual derivó en Internet y en 1990 aparecería la World Wide Web. En 1996 nace la segunda versión de Internet, más rápida, con más capacidad de carga y transporte de archivos, luego llegaría la conexión por modem, por microondas y actualmente por fibra óptica y vía satélite.

  Actualmente la informática está involucrada en casi todos los procesos humanos de la vida cotidiana, llámese familiar,

social, laboral, intelectual, etc., a tal punto que no se concibe la creación de un negocio o microempresa sin el acompañamiento de una plataforma informática. En lo que tiene que ver con la vida académica podemos decir que la informática es prácticamente un aspecto inalienable a ella, desde la educación básica hasta la doctoral, donde el computador y el internet se han convertido en algo imprescindible para cualquier estudiante.

1.2.1 Perito

Del latín perītus, un perito es una persona experimentada, hábil o entendida en una ciencia o arte. El perito es el experto en una determinada materia que, gracias a sus conocimientos, actúa como fuente de consulta para la resolución de conflictos.

1.2.2. Perito Informático

El perito informático es una persona especializada en la informática y en las nuevas tecnologías.

En la gran mayoría de países modernos la limitación de jueces y tribunales sobre cuestiones como la especialización del perito informático hace necesaria la presencia de estos profesionales. Que sirven para ofrecer sus conocimientos y resolver casos relacionados con la tecnología de la forma más adecuada posible.

Cuando en un procedimiento judicial se ven implicados hechos o pruebas relacionadas con el medio informático, es necesario que un perito informático se encargue de estudiar y valorar de manera objetiva. Este es un profesional cualificado y de confianza. Una vez realizado esto, asesora al juez o tribunal encargado del caso para que estos puedan realizar de forma completa la labor.

En resumen, un perito informático es una figura definida por la Ley como un profesional experto en los conocimientos sobre aquellos temas relacionados con la informática y las nuevas tecnologías. Es encargado del asesoramiento directo en procedimientos judiciales. Así el juez o tribunal tendrán la información necesaria que solo se puede obtener de un profesional que tenga conocimientos especializados.

1.2.3. Tipos de Peritos en la Justicia Argentina

- **Perito de Oficio**: son aquellos elegidos por el Juez dentro de los funcionarios público y en su defecto del listado de las Cámaras. Si uno desea actuar como perito en informática deberá inscribirse en tribunales de Córdoba. Son llamados a actuar mediante oficio o por sorteo. Al hacerse cargo de la pericia deben aceptar el cargo y prestar juramento. No cobran sueldo, sino que se le regulan honorarios a sentencia.

Art. 183. - La prueba pericial, cuando procediere, se llevará a cabo por UN (1) solo perito designado de oficio. No se admitirá la intervención de consultores técnicos. [2]

Art. 327 - El diligenciamiento se hará en la forma establecida para cada clase de prueba, salvo en el caso de la pericia, que estará a cargo de un perito único, nombrado de oficio. [2]

- **Perito de Oficial (Instituciones Oficiales)**: son aquellos que integran los gabinetes especializados de instituciones como PFA, GNA, PNA, PDI, Aduana, etc. Actúan exclusivamente para el fuero penal. También se incluyen los que forman parte de los cuerpos técnicos del poder Judicial y los profesionales de las universidades nacionales y los técnicos de organismos públicos específicos como INTI, ONTI, DNDA, etc. Cobran sueldo del estado en función de la jerarquía que desempeñen en las instituciones. Son nombrados por las Autoridades Judiciales en la Justicia Nacional por la Corte Suprema de Justicia. Juran por única vez cuando son designados. Cobran sueldo del estado.
- **Perito de Parte**: son los propuestos por una de las partes. Actúan en cualquier fuero. En algunos ámbitos dictaminan conjuntamente con los peritos oficiales. Deben acreditar su idoneidad profesional con título habilitante y prestar juramento al aceptar el cargo. Pueden firmar el dictamen conjuntamente con el Perito Oficial, si están de acuerdo con el mismo o emitir su propio dictamen en disidencia si no lo están, pero siempre tratando que dicha pericial forme un solo legajo. Cobran honorarios de la parte que lo propuso y / o a sentencia.
- **Consultor Técnico**: cada parte tiene la facultad de designar un consultor técnico. En los peritajes del Civil Comercial y laboral, etc. dentro de la competencia de la Justicia Nacional y Federal, sólo se admite un perito único de oficio y las partes pueden nombrar Consultores Técnicos. Éstos son asesores de parte y suponen parcialidad. No son auxiliares del órgano judicial, como lo es el perito. No aceptan el cargo. Pueden o no presentar dictamen. Pueden formular observaciones fundadas o acordar con el contenido del dictamen del perito de oficio u oficial. Los honorarios los pueden cobrar a

la parte que los designó o bien regulados a sentencia. En la audiencia que se fije para que los peritos den explicaciones, los consultores técnicos podrán observar lo que fuera pertinente. Pueden presenciar las operaciones técnicas que realicen los peritos y formular las observaciones que consideren pertinentes.

1.2.4. Principios del Peritaje

1. **OBJETIVIDAD**: El perito debe ser objetivo, debe observar los códigos de ética profesional.

2. **AUTENTICIDAD Y CONSERVACIÓN**: Durante la investigación, se debe conservar la autenticidad e integridad de los medios probatorios.

3. **LEGALIDAD**: El perito debe ser preciso en sus observaciones, opiniones y resultados, conocer la legislación respecto de su actividad pericial y cumplir con los requisitos establecidos por ella.

4. **IDONEIDAD**: Los medios probatorios deben ser auténticos, ser relevantes y suficientes para el caso.

5. **INALTERABILIDAD:** En todos los casos, existirá una cadena de custodia debidamente asegurada que demuestre que los medios no han sido modificados durante la pericia.

6. **DOCUMENTACIÓN**: Deberá establecerse por escrito los pasos dados en el procedimiento pericial.

Estos principios deben cumplirse en todas las pericias y por todos los peritos Involucrados. [4]

1.3.1. Delito.

Un delito es un comportamiento que, ya sea por propia voluntad o por imprudencia, resulta contrario a lo establecido por la ley. El delito, por lo tanto, implica una violación de las normas vigentes, lo que hace que merezca un castigo o pena. [5]

> También lo podemos definir como el acto u hecho, ya sea voluntario o involuntario, que viola una norma o ley. Si bien la definición de Delito no está

especificado en el Código Penal de la Nación Argentina, está comprendido en la Ley 11179 art. 79 a 305 Libro 2 "de Los Delitos".

- Historia y Evolución: El delito desde sus inicios se concibe como aquel acto indebido que es realizado por una o varias personas en perjuicio de alguien, ya sea persona natural o jurídica y que está en contra de lo permitido por la ética y la moral. Antes de la llegada de los computadores a la industria y al hogar los delincuentes debían estar cerca a la víctima para cometer el acto ilegal. Hoy en día el delito va más allá, hasta el punto de involucrar actores en puntos equidistantes al momento de cometer el delito, los cuales pueden gracias a la tecnología, actuar en conjunto para lograr el cometido.

1.3.2. Delito Informático.

Diversos autores y organismos han propuesto definiciones de los delitos informáticos, aportando distintas perspectivas y matices al concepto. Algunos consideran que es innecesario diferenciar los delitos informáticos de los tradicionales, ya que, según éstos se trata de los mismos delitos, cometidos a través de otros medios (como el tecnológico).

Tomando como referencia el "Convenio de Ciberdelincuencia del Consejo de Europa", podemos definir los delitos informáticos como: "los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos". [6]

También lo podemos definir como el acto u hecho, ya sea voluntario o involuntario, que viola una norma o ley y utiliza medios tecnológicos para su consecución y que están encaminados a atacar la integridad, confidencialidad y disponibilidad de los activos de información en un sistema informático.

- Historia y Evolución: Podemos decir que el primer tipo de delito informático que se dio fue el de robo de información en un computador, por rompimiento de contraseña. Hoy en día los delitos han evolucionado hasta tal punto que actualmente existe toda una ramificación de tipos y subtipos. Entre algunos delitos informáticos encontramos:

- **Fraude informático**: es inducir a otro a hacer o a restringirse en hacer alguna cosa de lo cual el criminal obtendrá un beneficio, casi siempre económico, utilizando medios informáticos.
- **Contenido obsceno u ofensivo**: Cuando se envían mensajes a través de internet con contenido que atenta contra la integridad de una o más personas u organizaciones (por medio de redes sociales, emails, etc.).
- **Hostigamiento / acoso**: Delito que se concreta cuando se contacta a una persona para que realice o entregue algo bajo una situación de amenaza.
- **Terrorismo Virtual**: Se da cuando se ataca una organización o estado para hacer daño a su sistema de información (ataques 0-days, denegación de servicio, acceso no autorizado, etc.).
- **Pornografía Infantil**: Delito que se comete cuando se envían archivos de imágenes o video por la web con contenido sexual explicito con menores de edad.
- **Propiedad Intelectual**: Delito que se comete en el momento que se accede a información privada o confidencial sin la autorización expresa de su autor, ya sea para su difusión gratuita o comercialización.

1.4.1. Vulnerabilidad.

Vulnerabilidad es el riesgo que una persona, sistema u objeto, (sea o no tecnológico), puede sufrir frente a los peligros, sean ellos desastres naturales, desigualdades económicas, políticas, sociales o culturales.

La palabra vulnerabilidad deriva del latín vulnerabilis. Está compuesto por vulnus, que significa 'herida', y el sufijo -abilis, que indica posibilidad; por lo tanto, etimológicamente, vulnerabilidad indica una mayor probabilidad de ser herido. Las vulnerabilidades adoptan diferentes formas, dependiendo de la naturaleza del objeto de estudio, sus causas y consecuencias. Frente a un desastre natural como un huracán, por ejemplo, la pobreza es un factor de vulnerabilidad que deja a las víctimas inmovilizadas sin capacidad de responder adecuadamente. Algunos sinónimos para la palabra vulnerabilidad son debilidad, flaqueza, susceptibilidad, riesgo y amenaza.

1.4.2. Vulnerabilidad Informática.

Una vulnerabilidad es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software. [6]

Pero una cosa sí que es cierta, que exista una vulnerabilidad no significa que se produzca un daño en el equipo de forma automática. Es decir, la computadora tiene un punto flaco, pero no por eso va a fallar, lo único que ocurre es que es posible que alguien ataque el equipo aprovechando ese punto débil.

Características: Es común descubrir vulnerabilidades constantemente en variados programas del computador y su rápida propagación por internet, inclusive mucho antes de que se descubra la solución o se publique la misma.

Podemos mencionar como vulnerabilidades comunes:

- **Buffer overflow o desbordamiento de pila**: Es un fallo de software debido a una mala programación que se ve reflejado durante la ejecución de un programa, el cual no logra controlar de forma adecuada la cantidad de datos que se deben copiar en el área de memoria reservada para el buffer, permitiendo que este espacio se supere, sobrescribiendo espacios de memorias continuas a éste incluyendo el contenido de la misma.
- **Inyección SQL**: Es un método que se aprovecha de un fallo de programación, específicamente en la validación de entrada de datos en una consulta SQL. Este método se aprovecha de una vulnerabilidad en la validación de entrada durante la construcción de una Sentencia SQL que se va a ejecutar frente una Base de Datos, permitiendo alterar la consulta de tal forma que el atacante puede obtener datos valiosos de los registros almacenados en las diferentes tablas existentes en la base de datos atacada, como de su estructura e inclusive de los usuarios administradores de la misma, permitiéndole escalar privilegios en el sistema.
- **Secuestro de sesiones**: Primero definamos cookie, el cual es un archivo generado al iniciar sesión en un sitio web y que identifica de forma unívoca a la dualidad que se da entre la cuenta de usuario y el servicio web enlazado. Entonces un

secuestro de sesión es un método de ataque informático en el cual se captura la cookie activa de un usuario en la red, lo cual permitirá al atacante acceder al servicio web enlazado a esa cookie sin pasar por las medidas de autenticación requeridas. De esta manera el atacante puede actuar de la misma forma que el usuario titular frente al servicio web enlazado con la cookie secuestrada.

- **Ejecución de código remoto**: Método que consiste en aprovechar una vulnerabilidad que permite tomar privilegios sobre una máquina remota y ejecutar código en ella, lo cual le daría la potestad al atacante de alterar, borrar o consultar información no autorizada e inclusive escalar privilegios en la maquina atacada.
  - XSS (Cross-Site Scripting): En español, Secuencias de Comandos en Sitios Cruzados. Vulnerabilidad común en las aplicaciones Web, que le brinda la oportunidad a un atacante inyectar en una página web código escrito en lenguajes tipo script como JavaScript o VBScript, lo cual le permitiría esquivar los controles establecidos dentro de las políticas de seguridad del sistema de información atacado.

Norma ISO 27001: es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

El estándar ISO 27001:2013 para los Sistemas Gestión de la Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

La aplicación de ISO-27001 significa una diferenciación respecto al resto, que mejora la competitividad y la imagen de una organización.

La Gestión de la Seguridad de la Información se complementa con las buenas prácticas o controles establecidos en la norma ISO 27002.

1.5.1. Amenaza

Una amenaza es un fenómeno o proceso natural o causado por el ser humano que puede poner en peligro a un grupo de personas, sus cosas y su ambiente, cuando no son precavidos. Existen diferentes tipos de amenazas. Algunas son naturales, otras son provocadas por el ser humano, como las llamadas industriales o tecnológicas (explosiones, incendios y derrames de sustancias tóxicas). Las guerras y el terrorismo también son amenazas creadas por el ser humano. [6]

1.5.2. Amenaza Informática.

Una amenaza informática es la probabilidad de ocurrencia de cualquier tipo de evento o acción que tenga la capacidad de ocasionar daño a los elementos de un sistema informático, tanto a nivel de software como de hardware.

1.6.1. Ataque o Incidente de Seguridad Informática.

Se puede definir como el intento de violación o la violación efectiva (penetración) a la seguridad de un sistema informático con fines delictivos. Las fases de un Ataque o Incidente de Seguridad Informática son:

- **Descubrimiento o Identificación**: Esta fase trae consigo la adquisición de datos relacionados con una posible víctima, la cual puede ser una persona o una entidad. Esta fase se puede comparar con los conocidos test de penetración realizados por hackers éticos. También se le conoce en el idioma inglés como “Information Gathering”.

  En esta fase se utilizan herramientas que analizan el tráfico de la red de datos, conocidas como sniffers (término en idioma inglés), además se complementa con técnicas de ingeniería social y con la ayuda de buscadores como shodan, google y bing. Además los buscadores google y bing ofrecen una metodología de búsqueda y filtrado en la web por medio de comandos conocidos como “DORKS”, muy efectivos a la hora de encontrar información oculta en la web. De esta forma se estarían garantizando resultados valiosos y positivos para el ataque. En síntesis, el delincuente en esta fase se dedica investigar en profundidad sobre la plataforma tecnológica que va a atacar, utilizando para ello técnicas

pasivas de levantamiento de información, tratando de encontrar la mayor cantidad de información pública sobre la misma. Entre la información a encontrar podemos mencionar:

- Dirección física de la entidad.
- Direcciones IP y Rangos.
- Direcciones IP de servicios contratados.
- Correos electrónicos.
- Nombres de empleados.
- Números telefónicos.
- Detección de redes WiFi.
- Análisis de vulnerabilidades al portal WEB.

- **Exploración**: En esta fase y con base en la información obtenida en la fase anterior, se busca profundizar en el sistema a violentar, obteniendo información como dirección o direcciones de red, rango y subrangos de red, nombres de equipos, datos de autenticación, sistemas operativos implementados, servidores web utilizados, etc. En esta fase se suelen utilizar herramientas informáticas tales como escáner de vulnerabilidades, escáner de red, escáner de puertos, mapeadores de red y de puertos, analizadores de protocolos, detección remota de servicios, detección remota de equipos activos y sistemas operativos, identificación de software y versiones, análisis de banners y búsqueda de aplicaciones web. Además de análisis de la configuración en las redes WiFi.

  En otras palabras se usan técnicas no intrusivas que permiten descubrir todas las vulnerabilidades potenciales a explotar durante el ataque.
- **Evaluación**: Luego de encontrar las vulnerabilidades que nos permitirán violar el sistema, estas comienzan a explotarse mediante las técnicas directamente relacionadas con ellas, tales como ataques de denegación de servicios, ataques de desbordamiento de buffers, filtrado de contraseñas, etc. En esta fase se dan las siguientes tareas:
  - Escaneo Automatizado de Vulnerabilidades. Mediante herramientas sistematizadas que permiten:

- Detectar vulnerabilidades en los Sistemas Operativos y en los demás servicios que se estén ejecutando. Generar reportes con información técnica relevante de seguridad.
- Permitir, si es posible, explotar toda vulnerabilidad detectada.

  - Escaneo Manual de Vulnerabilidades. Este se realiza a través de sitios web con información sobre vulnerabilidades reportadas. Para ello se verifica la existencia de vulnerabilidades que afecten a las versiones del software instalado. Algunos de estos sitios web poseen bases de datos con exploits públicos, los cuales pueden ser de utilidad para el ataque.

- **Intrusión**: Esta fase, considerada como la más compleja en un ataque informático, se caracteriza por darle utilidad a todo lo detectado y recabado en etapas previas, tratando de encontrar las herramientas adecuadas que permitan realizar la intrusión y obtener el control del sistema mediante el escalamiento de privilegios (proceso por el cual se obtienen niveles de acceso superior en una plataforma especifica). Casi siempre este proceso no se realiza en forma inmediata y a menudo requiere la explotación en conjunto de dos o más vulnerabilidades para hacerse efectivo. En esta fase el atacante se asegura de implantar en el sistema atacado herramientas que permanezcan lo más indetectable posible y que le permitan volver a penetrar el sistema en un futuro desde cualquier lugar donde exista conexión a internet. Estas herramientas (o mejor, Malware) suelen ser del tipo:
  - Troyanos: Es un malware que se muestra como un software autentico y luego de alojado en un equipo permite al atacante tomar el control del mismo.
  - Rootkits: Malware que se compone de varios elementos que otorgan a un atacante el acceso al sistema de la víctima.
  - Backdoors: Líneas de código dentro de un programa de forma intencional, el cual está destinado para controlar remotamente el equipo víctima.

Uno de los pasos finales de todo atacante informático es el de eliminar cualquier evidencia o rastro que lo pueda incriminar con el

delito informático cometido y más aún que le permita al responsable de la seguridad informática y/o de la información de la empresa detectar su presencia en tiempo real. Para lo cual se vale de herramientas que borran esas evidencias, como pueden ser herramientas para borrado de logs y de alarmas generadas por los IDS instalados.

1.7.1. Evidencia Digital.

"Información de valor probatorio almacenada o transmitida en forma digital" (Cano, 2005)[7]. En otras palabras la podemos definir como las pruebas digitales encontradas en una escena de un delito que pueden servir en un proceso judicial como evidencia probatoria. La evidencia digital se puede dividir en tres categorías:

- Registros almacenados en un equipo informático: Correos electrónicos, imágenes, documentos ofimáticos, etc.
- Registros generados por un equipo informático: Logs de Eventos, logs de errores, logs de transacciones, etc.
- Registros parcialmente generados y almacenados en un equipo informático: por ejemplo aquellos archivos generados temporalmente por el navegador de internet mientras consultamos el ciberespacio o aquellos archivos generados cuando se ejecuta un procedimiento por lotes o un procedimiento almacenado en una base de datos.

Se tiene que anotar que una evidencia digital es anónima, duplicable, alterable y eliminable.

1.8.1. Auditoria.

Alice, Naranjo (2009) afirma: “La palabra auditoría viene del latín auditorius y de ésta proviene la palabra auditor, que en español significa aquel que tiene la virtud de oír y revisar cuentas. La auditoría debe estar encaminada a un objetivo específico que es el de evaluar la eficiencia y eficacia con que se está operando el área analizada, para que por medio del señalamiento de cursos alternativos de acción, se tomen decisiones que permitan corregir los errores, en caso de que existan, o bien, mejorar la forma de actuación.” [8]

También se puede definir al término auditoria como la evaluación desarrollada por un grupo de profesionales a una entidad, del orden público o privado, con el fin de detectar fallas y hacer las respectivas sugerencias para subsanarlas.

- **Historia**: La auditoría es tan antigua como lo es la aparición del hombre sobre la tierra. En sus inicios ésta se desarrollaba de manera empírica. En la época de la conquista estaban los "oidores" de la corona, que en el fondo eran auditores, ya que vigilaban el pago de tributos a la corona española.

  En la era moderna la auditoria se implementa en cualquier empresa o entidad para encontrar falencias misionales y posteriormente proseguir con implementar el correctivo necesario.
- **Aplicabilidad**: La aplicabilidad de un proceso de Auditoria abarca un rango amplio de entidades, de procesos, de procedimientos y de ejecuciones. Se aplica a cualquier entidad o empresa que desee detectar falencias en su lógica de negocio para su posterior corrección o como mínimo alcanzar su mayor mitigación.

1.8.2. Auditoria Informática.

Gonzalo Alonso Rivas (1989) la define así: "…es un examen metódico del servicio informático, o de un sistema informático en particular, realizado de una forma puntual y de modo discontinuo, a instancias de la Dirección, con la intención de ayudar a mejorar conceptos como la seguridad, la eficacia, y la rentabilidad del servicio, o del sistema, que serán auditados." [9]

1.9.1. Seguridad.

En la enciclopedia en línea Wikipedia se encuentra la siguiente definición: El término seguridad proviene del latín "securitas". Cotidianamente se puede referir a la seguridad como la ausencia de riesgo o también a la confianza en algo o alguien. [10]

1.9.2. Seguridad de la Información.

Se puede decir que al hablar de seguridad de la información nos referimos a todas las metodologías implementadas como medidas de seguridad en un sistema informático, que permitan contrarrestar las amenazas a las que están expuestos sus activos de información o a mitigar el impacto de las mismas. Según Álvarez Marañón, Gonzalo (2004), "La seguridad de la información es una disciplina que se ocupa de gestionar el riesgo dentro de los sistemas informáticos" [11]

1.9.3. Seguridad Informática

La seguridad informática es un conjunto de herramientas, procedimientos y estrategias que tienen como objetivo garantizar la integridad, disponibilidad y confidencialidad de la información de una entidad en un sistema.

La seguridad informática se caracteriza por la protección de datos y de comunicaciones en una red asegurando, en la medida de lo posible, los tres principios básicos:

La integridad de los datos: la modificación de cualquier tipo de información debe ser conocido y autorizado por el autor o entidad.

La disponibilidad del sistema: la operación continua para mantener la productividad y la credibilidad de la empresa.

La confidencialidad: la divulgación de datos debe ser autorizada y los datos protegidos contra ataques que violen este principio.

La seguridad informática es una disciplina o rama de la Tecnología de la Información, que estudia e implementa las amenazas y vulnerabilidades de los sistemas informáticos especialmente en la red como, por ejemplo, virus, gusanos, caballos de troya, ciber-ataques, ataques de invasión, robo de identidad, robo de datos, adivinación de contraseñas, intercepción de comunicaciones electrónicas, entre otros.

1.10.1. Análisis Forense

El análisis forense en un sistema informático es una ciencia moderna que permite reconstruir lo que ha sucedido en un sistema tras un incidente de seguridad. Este análisis

puede determinar quién, desde dónde, cómo, cuándo y qué acciones ha llevado a cabo un intruso en los sistemas afectados por un incidente de seguridad. [12]

1.10.2. Informática Forense

Definición: "Es el proceso de identificar, preservar, analizar y presentar evidencia digital, de manera que esta sea legalmente aceptable" [13]

Historia: La historia nos dice que la informática forense tiene su origen en los Estados Unidos en los años 90, en atención de las necesidades por parte del FBI de peritos en delitos informáticos. Esta necesidad se generaba de las actuaciones procesales en actividades probatorias donde estaban involucradas evidencias tecnológicas o en la recolección de estas evidencias en una escena del crimen, en donde las pruebas o evidencias digitales en un proceso legal tenían el potencial de convertirse en un elemento probatorio tan poderoso para la lucha contra la delincuencia, como lo era el de la identificación por ADN.

A finales de los años 90 se creó la IOCE (International Organization of Computer Evidence) cuya finalidad principal es compartir información sobre las prácticas de informática forense alrededor del mundo.

A raíz de esto nace como tal la labor del perito informático o informático forense, cuyo objetivo principal es encontrar pruebas en un delito informático que le permita identificar de forma tácita y real el origen y la forma como se llegó a la consecución del mismo.

- **Objetivos:** La informática forense persigue tres objetivos puntuales, basados en la recolección de evidencias:
  - Búsqueda y llevada a juicio de los ciberdelincuentes.
  - El resarcimiento de todos los delitos cometidos.
  - Identificación de la vulnerabilidad y establecimiento de los controles pertinentes para su mitigación.
- **Importancia:** La Informática Forense es una disciplina criminalística que se enfoca en investigar hechos delictivos en los que están involucrados sistemas informáticos y con base en esa investigación hallar pruebas o evidencias que tengan la suficiencia jurídica necesaria para poder ser presentada como prueba válida ante un ente judicial.

Para esto la Informática Forense desarrolla y perfecciona técnicas que permiten encontrar, analizar, salvaguardar y documentar hallazgos o evidencias tecnológicas frente a instancias legales.

- **Aplicabilidad**: La Informática Forense es una disciplina criminalística que se puede aplicar en las siguientes áreas:
    - Investigación Científica: En la actualidad entidades de educación superior se valen de la informática forense para el estudio y análisis de amenazas y vulnerabilidades informáticas y su posible solución o mitigación al máximo grado posible.
    - Investigación Criminal: La informática forense es aplicada como ayuda para solucionar delitos con variadas tipificaciones: Financieros, Narcotráfico, Pornografía Infantil, Trata de Blancas, Grupos Extremistas, Homicidios, etc.
    - Proceso Judicial: La informática forense es aplicada como ayuda para solucionar procesos judiciales relacionados con Estafas, Fraudes, Acosos, Espionaje, Robo de Información, etc.
    - Hogar: Existen múltiples aplicativos con tecnología forense que un usuario normal puede utilizar con finalidad particular, como recuperar archivos borrados accidentalmente, entre otros.

1.10.3. Tipos de Análisis Informático Forense.

- **Análisis Forense de Redes:** Mediante el cual se analiza en investiga un delito informático en el cual se ve involucrada una red de computadores.
- **Análisis Forense en Sistemas Embebidos:** Es el Proceso mediante el cual se analizan dispositivos electrónicos como tablets, smartphones, etc., que estén involucrados en un delito informático.
- **Análisis Forense de Sistemas:** Mediante el cual se analizan computadores tipo servidores o de escritorio, los cuales hayan sido protagonistas para un delito informático, ya sea como medio para lograrlo o como objetivo final del mismo.

1.10.4. Principios de la Informática Forense.

De acuerdo a la entrevista con integrantes de la Policía Judicial de Córdoba debemos tener en cuenta que cualquier institución con atribuciones en la búsqueda, recolección, y análisis de pruebas debe tener una metodología o unos principios generales definidos con el objetivo de proteger los intereses de todas las partes. Dichos principios han de tener en cuenta las siguientes peculiaridades de cada ordenamiento jurídico:

- **Organización y documentación detallada**: El investigador forense debe ser una persona plenamente organizada en su trabajo investigativo, debe dejar trazabilidad de cada uno de los pasos que desarrolló durante el mismo, de las herramientas informáticas que utilizó durante la investigación. Además debe brindar un reporte del análisis de las evidencias encontradas bien detallado y soportado con toda la documentación pertinente para la misma, para que al momento de ser consultado por cualquier persona, ésta entienda y valide lo que está leyendo sin problema alguno. Esto permite al investigador tener tranquilidad sobre la veracidad e integridad de su trabajo, y en el eventual caso de que se realicé por otras personas una investigación adicional sobre la misma evidencia, que los resultados sean iguales y se pueda salir avante frente a una comparación de los mismos.
- **Integridad de la evidencia**: El investigador forense debe garantizar que las evidencias digitales obtenidas y las copias de éstas no se puedan alterar o modificar en ninguno de las fases de la investigación forense hasta su entrega a la instancia judicial competente y la emisión de los informes respectivos. Para lo cual se debe implementar la cadena de custodia tal cual como lo dictan las normas estandarizadas y las buenas prácticas reconocidas para este proceso.
- **Validar el proceso de custodia**. Todo proceso de custodia debe cumplir con ciertos lineamientos preestablecidos en lo concerniente al diligenciamiento de información mediante el cual se le da soporte y trazabilidad a todos los procesos que se dieron durante ese proceso de custodia. Esto con todo el rigor y la importancia que el tema merece. [14]

1.10.5. Herramientas Informáticas como medio delictivo.

El avance desenfrenado de los equipos informáticos y las telecomunicaciones ha traído como consecuencia el aumento exponencial de la delincuencia informática, esto por ende se ha visto reflejado en el desarrollo de nuevas herramientas tanto a nivel de software como de hardware para la protección de los activos de información de una organización. Me centraré en este trabajo en lo concerniente a herramientas de software como apoyo en el proceso de análisis forense informático.

1.10.6. Pruebas básicas a identificar según el tipo de delito informático.

Los riesgos que existen en Internet se encuentran a la orden del día. Millones de usuarios quedan expuestos constantemente a ataques y fraudes perpetrados por malintencionados que buscan hacerse de una gran cantidad de datos personales, cuentas, claves bancarias y tarjetas de crédito con el objeto de usarlos con fines delictivos.

A partir de la utilización de sofisticada tecnología buscan hacerse de esta información para luego venderla o manipularla como medio para la extorsión.

Sin embargo, es importante saber que no todos los fraudes pueden catalogarse como ciberdelitos.

Entonces, no siempre se encuentra el amparo legal que permita sentenciar este tipo de prácticas que tanto dolor de cabeza pueden generar en los usuarios de Internet.

En las entrevistas realizadas a Peritos Informáticos Forenses [15], los cuales realizan peritajes judiciales podemos enumerar una serie de pruebas basadas en buenas prácticas, en lo que corresponde al análisis informático forense, dependiendo del tipo de delito informático investigado.

- **Investigaciones de Fraude Financiero**: En este tipo de procesos se deben analizar las evidencias para encontrar aspectos relacionados con las cuentas utilizadas en portales dedicados a subastas online, software contable u hojas de cálculo con información contable, agenda con direcciones, conversaciones virtuales (correos, chats, foros, etc.), información de tarjetas bancarias (débito o crédito), información financiera de bienes, datos de clientes y software de edición de imágenes.

- **Investigaciones relacionadas con la pedofilia, pornografía y abuso Infantil:** En este tipo de procesos se deben analizar las evidencias para encontrar aspectos relacionados con: agenda con direcciones, conversaciones virtuales (correos, chats, foros, etc.), software de edición de imágenes, software de conectividad con cámaras digitales, imágenes, videos, software de juegos, historial de navegación en browsers y metadatos de directorios e imágenes.
- **Investigaciones relacionadas con la penetración ilegal a una red de cómputo y fraudes en telecomunicaciones:** En este tipo de procesos se deben analizar las evidencias para encontrar aspectos relacionados con la agenda con direcciones y nombres de usuarios, conversaciones virtuales (correos, chats, foros, etc.), software de edición de imágenes, software de conectividad con cámaras digitales, imágenes, videos, software de juegos, historial de navegación en browsers y metadatos de directorios e imágenes.
- **Investigación de Homicidios:** En este tipo de procesos se deben analizar las evidencias para encontrar aspectos relacionados con las cuentas utilizadas en portales dedicados a subastas online, software contable u hojas de cálculo con información contable, agenda con direcciones, conversaciones virtuales (correos, chats, foros, etc.), información de tarjetas bancarias (débito o crédito), información financiera de bienes, documentos legales de propiedad de bienes (escrituras, testamentos, etc.),datos de clientes y software de edición de imágenes, historia médica, imágenes y violencia intrafamiliar.
- **Investigaciones relacionadas con el narcotráfico:** En este tipo de procesos se deben analizar las evidencias para encontrar aspectos relacionados con la agenda con direcciones, conversaciones virtuales (correos, chats, foros, etc.), software de edición de imágenes, software de conectividad con cámaras digitales, imágenes, videos, software de juegos, historial de navegación en browsers y metadatos de directorios e imágenes.
- **Investigaciones relacionadas con los derechos de autor:** En este tipo de procesos se deben analizar las evidencias para encontrar aspectos relacionados con la agenda con direcciones y nombres de

usuarios, conversaciones virtuales (correos, chats, foros, etc.), software de edición de imágenes, software de conectividad con cámaras digitales, imágenes, videos, software de juegos, historial de navegación en browsers y metadatos de directorios e imágenes.

2. HARDWARE

2.1. Opciones de Hardware / Equipamiento Físico para Análisis Forense Digital.

Casi todo o gran parte de lo que se puede clasificar como equipamiento o hardware especializado para la práctica de peritaje o análisis forense digital es en realidad una solución conjunta de software y hardware.

Aun en los casos en que se trate de simples interfaces, deberán recurrir o contar con un controlador o driver (salvo en los casos obvio en que las interfaces se constituyan de cables y conectores USB).

Avanzando sobre la investigación de la oferta disponible en el mercado, cuando más completa sea la solución, mayor será la participación del componente software en la solución.

Una de las premisas en el análisis forense es mantener las pruebas inalterables, asegurar la manipulación de los objetos sujetos a análisis en dicha condición, de inalterables.

Entonces, además de buenas prácticas que debe emplear el perito forense (o analista forense) para asegurar la cadena de custodia en cada una de las fases de un análisis forense, para respaldar esto, debe contar o recurrir al empleo de herramientas adecuadas para tal fin.

Es por ello que, en la búsqueda del equipamiento necesario para la tarea, pueden encontrarse múltiples ofertas que van desde un sencillo cable de conexión USB o USB Type-C, a una compleja y completa solución basada en un conjunto de dispositivos físicos (hardware) que se complementan necesariamente con un componente software para su funcionamiento.

En ese camino entre uno y otro extremo, es decir, desde el más simple y elemental al más completo equipamiento, existe una amplia gama de opciones, entre las que pueden

encontrarse: dispositivos para la replicación de discos y/o unidades de memoria (para efectuar copias forenses, bit a bit), dispositivos para adquisición de datos de teléfonos inteligentes (smartphones) y otros móviles (GPSs por ejemplo), placas o interfaces para evitar escrituras en las unidades de almacenamiento a analizar (bloqueadores de escritura), dispositivos de almacenamiento de copias forenses, y un sinnúmero de cables, adaptadores y mucho más.

Otra clasificación que se puede realizar sobre el equipamiento para la tarea de pericia informática es el destinado a trabajo de campo, el cual se caracteriza por ser de tamaño adecuado para transportarlo hasta donde debe efectuarse la práctica; y el destinado a equipar un laboratorio informático.

2.1.1. Equipamiento para Trabajos de Campo.

Para los equipos destinados para trabajo de campo no sólo es requisito que sea transportable, sino que a la vez tiene que ser robusto y resistente y de igual manera tiene que ofrecer las mayores posibilidades de acceso o conexión a distintos medios o unidades de almacenamiento, dispositivos móviles tal como smartphones, GPSs, tabletas digitales, etc. Quizá no cuente con las mayores capacidades de cómputo que sean necesarias para procesar, analizar, buscar, filtrar grandes volúmenes de datos, pero justamente estos equipos o "kits de herramientas" están orientados para ser empleados en tareas prontas y/o urgentes o que requieran de una intervención inmediata por parte del analista, ya sea, por ejemplo, para la adquisición de datos.

Los "kits de herramientas" para trabajo de campo bien puede estar constituidos por una laptop o notebook más un completo conjunto de cables, conectores y adaptadores para acceder a la mayor variedad de marcas y modelos de teléfonos móviles, como también una o varias interfaces (placas electrónicas con sus conectores varios y contenidas por un gabinete adecuado) para acceder o conectar unidades de almacenamiento (HDD, SSD, memorias SD, MMC, etc.), duplicadoras de disco, bloqueadoras de escritura, etc.

Cada analista deberá equiparse de los dispositivos que le serán de utilidad para el área de interés sobre la materia de análisis forense digital a la que se vincule, para reunir o hacerse de la "suite" más completa.

Existen en el mercado varias opciones o alternativas, unas más completas y onerosas que otras, que le ahorraran tiempo valioso al analista hasta conformar un "kit"

adecuado, ya que suponen gran inversión en investigación y desarrollo que garantizan la preservación de las pruebas.

Unas propuestas pueden centrarse en un gabinete específico, con componentes de hardware "portátiles poderosos" (motherboards con varios conectores, procesador más potente posible, mayor cantidad de memoria RAM disponible, unidades de HD/SDD, bahías para montar interfaces de adquisición de datos, bloqueos de escritura, etc.), pudiendo en algunos casos contar con su propia pantalla y dispositivo de entrada (teclado, apuntador o mouse), o en otros, recurrir a fuente externa para visualizar salida gráfica.

Otras opciones que se encuentran en el mercado, directamente toman algún modelo de laptop o notebook del tipo profesional y en ella instalan herramientas, utilidades y/o suites de software para análisis forense y componen un kit completándolas con un conjunto de cables, conectores y adaptadores, más el adicionado de una o varias unidades externas para adquisición de datos / "evidencias", replicación o duplicación de unidades de disco, etc.

También, pueden encontrarse propuestas más simples que recurren o se basan en una tablet más un conjunto de conectores, cables y adaptadores e interfaces externas.

Sobre estos equipos puede mencionarse que la oferta es bien variada, con simples o mayores prestaciones, capacidades, resistencias a ambientes agresivos, interferencias electromagnéticas, etc.

Mayores detalles se brindarán en páginas posteriores en las que se mencionan y detallan algunas propuestas comerciales, disponibles en nuestro mercado nacional, a las que puede accederse por medio de representantes y/o distribuidores locales o regionales, o bien, contactando a distribuidores internacionales (Gran Bretaña, EE.UU., Alemania, Taiwán, etc.), o también, en algunos casos, directamente con sus fabricantes.

2.1.2. Equipamiento para Laboratorios Forenses.

El equipamiento con el que debe estar dotado un laboratorio forense no sólo se circunscribe a una PC o estación de trabajo potente, sino que también debe contar con los mencionados cables, conectores y adaptadores para trabajo de campo o equipos

móviles, como de igual manera, interfaces para conectar o acceder a los equipos que deberán analizarse.

Estas interfaces bien pueden ser externas, es decir plaquetas electrónicas contenidas por su propio gabinete, con múltiples o diversos conectores, o bien, placas internas que se conectan a puertos PCI/PCI-E de servidores, PCs o estaciones de trabajo.

Otros dispositivos indispensables que deben equipar un laboratorio son duplicadoras o replicadoras "forenses" de discos, bloqueadores de escritura, dispositivos de adquisición de información de teléfonos móviles, etc.

En cuanto a cómo debe estar dotado en lo referido al ítem computadoras o PCs, dependerá, como es obvio de la envergadura del laboratorio y de los casos a los que oriente su investigación.

Pero, siempre es recomendable adquirir o ensamblar un equipo lo más potente posible, de acuerdo a lo que permita el presupuesto destinado para tal fin.

Es que, cada vez son necesarios mayores recursos en cuanto a componentes de hardware, ya sea de microprocesadores (cuantos más núcleos, mayor capacidad de multitareas simultáneas, más memoria caché, mucho mejor), memoria RAM (ídem que para procesadores, cuanto mayor y más rápidas, mucho mejor), una placa base o motherborad con un factor de forma acorde (ATX por ejemplo) para que permita montar distintas placas PCI/PCI-E y otras interfaces que se montan en bahías 5 1/4 de los gabinetes para Servers/Workstations, unidades de almacenamiento con gran capacidad, la mayor cantidad posible, del mayor tamaño posible, y un gabinete que pueda contener de forma adecuada los componentes antes mencionados, garantizando funcionamiento a mayor requerimiento a temperaturas de trabajo recomendadas.

Existen propuestas estándares y que se ofrecen bajo catálogo, que emplean gabinetes profesionales, bien pudiendo ser del tipo industrial, para montar allí los componentes de hardware (motherboard o placa base, microprocesador o microprocesadores, unidades de memoria RAM, unidades de almacenamiento (HD/SSD/etc.), placas PCI/PCI-E de interface, NICs, placas de video, interfaces con guías o para montaje en bahías de 5 ¼" estándares, etc.

En algunos casos ofrecen equipamiento similar "a la carta", pudiendo personalizar algunas opciones como procesador, memoria RAM, almacenamiento, etc.

Se recomienda disponer de más de un servidor, estación de trabajo, para ejecutar tareas específicas en cada uno de ellos, como también ejecutar tareas en simultáneo, por ejemplo, en una máquina (estación de trabajo) se efectúa copia o copias de unidades de almacenamiento sujetas a análisis, mientras en otra (servidor) se ejecutan procesos de computo intensivo para verificación o análisis de la información para la búsqueda de un patrón o dato específico.

2.1.3. "OTRO" Equipamiento Físico Necesario.

Más allá de lo mencionado en las secciones referidas a equipamientos requeridos para trabajos de campo o de laboratorio, el analista forense deberá contar con otro equipamiento y material físico al que deberá recurrir en cualquier momento y deberá tener a disposición inmediata, a saber: dispositivos de almacenamiento limpios (unidades HD, SSD, unidades cintas magnéticas para copias de seguridad, unidades ópticas CDR/DVDR); pendrives; unidades de disco USB; bolsas Faraday (bloqueo de interferencias o campos electromagnéticos); gabinetes Faraday; gabinetes plásticos herméticos; bolsas antiestáticas (para guardado de pruebas, dispositivos a analizar); sobres de papel; cintas de seguridad (para asegurar pruebas o dispositivos a analizar); etiquetas de seguridad; etiquetas para identificación; marcadores permanentes; notas, actas y formularios de actuaciones e informes; etc.

2.2. Una mirada sobre lo que existe en el mercado, Basada en Casos de Éxito Renombrados y/o Recomendaciones de Analistas o Laboratorios de Referencia del Sector.

Uno de los productos o "conjunto de productos" que se destacan, porque son los referentes del sector, son los propuestos por "Cellebrite (https://www.cellebrite.com)", y particularmente con su producto estrella UFED. En realidad Cellebrite ofrece un amplio y completo abanico de soluciones, conjunto de productos de software y hardware.

Así se constituyeron ya que alguna solución de esta empresa fue empleada para la resolución de ciertos casos renombrados y con trascendencia en diversos medios informativos, por lo cual lograron trascendencia mediática.

Otra propuesta que puede considerase similar es la que ofrece la compañía Micro Systemation AB (MSAB), que al igual que lo ofrecido por Cellebrite, plantea diversas soluciones para cada caso o utilidad.

Y, también, tal como Cellebrite, Micro Systemation AB no ofrece un único producto, sino un conjunto de ellos, y así mismo, se conforma por componentes de hardware con la complementación de componentes de software.

Estas soluciones mencionan y trabajan en conjunto con laboratorios forenses de organizaciones gubernamentales, ya sean de las fuerzas de seguridad, del servicio seguridad interna, de cancillería, etc.

¿Qué significa esto último? Que emplean y se ajustan a altos estándares por lo cual, luego, lo que ponen a consideración en su portafolio pueden garantizar al analista forense una tarea profesional y eficiente, con el consiguiente beneficio de garantizar la preservación de la cadena de custodia (esto si el profesional se apega a lo que se conoce como "buenas prácticas", o bien, en el caso que corresponda, se apegue a un protocolo establecido).

Más alternativas se encuentran en otros fabricantes:

TABLEAU HARDWARE (GUINDANCE SOFTWARE / OPENTEXT): cuenta con un catálogo amplio de dispositivos tales como duplicadores forenses, bloqueadores de escritura, recuperadores de contraseñas, adaptadores y conectores (para unidades HD IDE, SATA, SSD, M.2, para puertos FireWire, etc.)

OXYGEN FORENSICS: Basa su propuesta en soluciones de software, de manera opcional ofrece un kit de cables.

MEDIACLONE INC: ofrece equipamiento variado, clasificado en tres grandes grupos: unidades para "trabajo de campo" con opciones de arranque dual (Linux & Windows); plataformas y kits forenses (también con opción de arranque dual); unidades para laboratorios forenses (dual boot con Linux y Windows).

ACE (ADVANCED COMPUTER ENGINEERS) / ACE LABORATORY: son especialistas en desarrollo de interfaces (hardware y software) para la extracción y recuperación de datos de unidades de almacenamiento. Cuentan con múltiples opciones de dispositivos (placas internas para montar en puertos PCI/PCI-E de placas base, o unidades externas)

para extraer y/o recuperar información/archivos de unidades de disco duro SATA y PATA, unidades USB HDD, SSHD, etc.

2.3. Valores de Marcado y Aplicabilidad en Argentina.

El Hardware fabricado a nivel mundial es muy interesante y amplio desde el punto de del peritaje informático, existen desde pequeños dispositivos unipersonales y para trabajos de los que denominamos “de campo” (es aquel trabajo que realizan los peritos de oficio y oficiales en el domicilio que en donde se debe hacer la pericia y se necesita el transporte de los dispositivos), hasta grandes equipos para laboratorios forenses y de instituciones públicas como GNA(Gendarmería Nacional Argentina), PNA(Prefectura Naval Argentina, PFA,(Policía Federal Argentina), PSA (Policía de Seguridad Aeroportuaria).

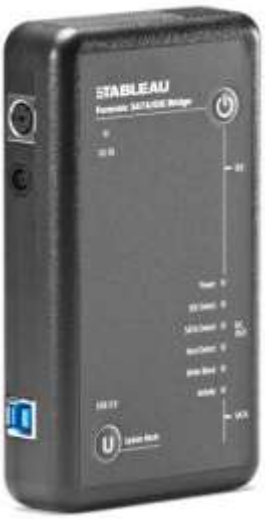
A continuación en los siguientes ejemplos de Hardware (equipos para peritaje forense), se ofrecen aquellos equipos de posible uso en Argentina, cotizados en la web:

DISPOSITIVOS PARA TRABAJO EN CAMPO

(URL: https://www.tableau.com/es-es/products)

Tableau Forensic T35u IDE/SATA Kit U$S 359.00*

Tableau T35u USB 3.0 Forensic SATA/IDE Bridge Kit



TDA Multipack U$S 185.00* (URL: https://www.tableau.com/es-es/products)

Kit Adaptador de Discos.

Incluye:

- TC6-2 - 2" IDE 80-conductor Cinta.
- TDA3-1 - 3.5" SATA - microSATA adaptador de disco rígido.
- TDA3-2 - SATA - Blade-Type estado sólido Drive (SSD) Adaptador.
- TDA3-LIF con 2 LIF cables.
- TDA5-18 -1.8" IDE Adaptador.
- TDA5-25 - 2.5" IDE Adaptador.
- TDA5-ZIF con TC20-BNDL cables
- Negra TB4 cartera/maletín.

Tableau TP5 Power Supply U$S 79.99* (URL: https://www.tableau.com/es-es/products)

Tableau TP5 Fuente de Alimentación Universal esta Diseñado para alimentar todo el Tableau forense Puentes y duplicadores.

Ultimate Forensic Write Protection Build-A-Kit U$S 360.00* (URL: https://www.tableau.com/es-es/products)

Construye tu propio kit de protección contra escritura forense. Seleccione hasta cinco puentes. Se incluirán los cables necesarios para cada puente.

The base kit price includes:

- Maleta de transporte con inserto de espuma.
- DosTP2 Fuentes de Alimentación
- Lector de Tarjetas Read/Write.
- Tableau Kit Adaptador (TKA5-AD).

Ultimate Forensic Write Protection Kit II (Mobile Ver.) U$S 1,799.00* (URL: https://www.tableau.com/es-es/products)

Forensic Write Protection Kit

- **Forensic Bridges**
  - Una Tableau T35u USB 3 para puente SATA/IDE de solamente lectura.
  - Una Tableau T35u USB 3 para puente SATA/IDE de lectura/escritura
  - Un Puente Tableau T8u Forensic para USB 3
  - Un puente Tableau T6u de USB 3 a SAS
- **Cables**
  - Dos USB 3.0 Cables
  - Cable Unificado para Señal SAS y Alimentación
  - Dos Cables 8 Pulg. SATA
  - Dos Cables 8 Pulg. IDE
  - Un Cable 2 Pulg. IDE Cable
  - Dos Cables 3M para Alimentación

- Dos Cables 3M a Hembra 4-pin Molex de Alimentación

- **Ensamblado de Alimentación**
  - Dos Fuentes de Alimentación Tableau TP2.
  - Dos Cordones de Alimentación
- **Media Reader**
  - Lector de Tarjetas (Lectura Solamente)
- **Estuche de Transporte**
  - Estuche rígido moldeado por inyección.

Tableau TD2u Forensic Duplicator U$S 1,479.00* (URL: https://www.tableau.com/es-es/products)

TD2u: Extremadamente Rápida. Real. Rápida para usar.

Construido para sobresalir tanto en el campo como en el laboratorio, el Duplicador Forense TD2u de Tableau es la combinación perfecta de fácil operación, confiabilidad y rendimiento de imágenes forenses ultra-rápido. Las imágenes duplicadoras de cuarta generación de Tableau a velocidades excepcionales de más de 15 GB / min mientras que al mismo tiempo calculan hashes MD5 y SHA-1. La velocidad de imágenes forenses un rasgo de Tableau en un punto a tener en cuenta respecto al precio. Construido con la tecnología más avanzada, eso ofrece TD2u.

Mobile Acquisition Bundle U$S 1,899.00* (URL: https://www.tableau.com/es-es/products)

El paquete de adquisición móvil Forensic Computers toma el puente forense T356789iu de Tableau y lo encierra en un gabinete personalizado diseñado y fabricado para Computadoras Forenses.

La MoAB podrá adquirir de Unidades IDE/SATA/SAS/Firewire/USB3.0/PCIe. El gabinete cuenta con ventiladores duales en la parte superior de la unidad que permitirán la colocación de un disco duro. El disco duro se mantiene a temperaturas óptimas, incluso durante las acciones de lectura intensivas.

Tableau TX1 Forensic Imager U$S 2,999.99*

(URL: https://www.tableau.com/es-es/products)

Tableau TX1 Forensic Imager es lo último y mejor de Tableau y es una alternativa portátil para llevar una estación de trabajo forense al campo.

Es un generador de imágenes totalmente forense habilitado para redes que ofrece un rendimiento de imagen local y de red superior sin compromisos. El Tableau TX1 establece el estándar para imágenes forenses.

Tableau Forensic TD2u Ultimate Kit Be the first to review this product $3,199.00*

(URL: https://www.tableau.com/es-es/products)

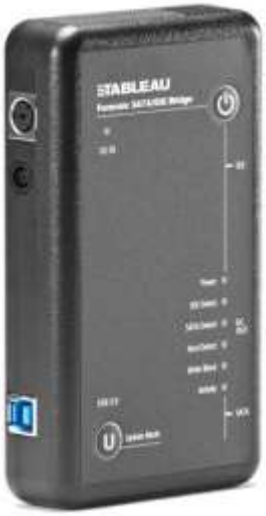
El Kit TD2u Ultimo es una combinación de la Tableau TD2u y el Kit Ultimo de Protección de Escritura Forense. Esto ofrece flexibilidad tanto para la adquisición de un disco duro como para la adquisición directa en la computadora de investigación.

DISPOSITIVOS PARA TRABAJO EN LABORATORIO

Tableau Forensic T35u IDE/SATA Kit U$S 359.00

(URL: https://www.tableau.com/es-es/products)

Tableau T35u USB 3.0 Forensic SATA/IDE Bridge Kit



TDA Multipack U$S 185.00

(URL: https://www.tableau.com/es-es/products)

Drive Adapter Kit.

Tableau TP5 Power Supply U$S 79.99

(URL: https://www.tableau.com/es-es/products)

La fuente de alimentación universal de Tableau TP5 está diseñado para alimentar todo el Tableau forense

Puentes y duplicadores.

M.2/MSATA SATA Adapter U$S 28.99*

(URL: https://www.tableau.com/es-es/products)

Úselo para conectar fácilmente cualquiera de los 6 tamaños diferentes M.2 o mSATA

SSDs a cualquier puerto SATA.

Tableau T3iu Forensic SATA Imaging Bay U$S319.00

La Bahía de Imágenes SATA Forense de Tableau T3iu está diseñada para adquisiciones extremadamente rápidas y bloqueadas por escritura de discos duros SATA de 3.5 "y 2.5". T3iu fue diseñado para una fácil integración en estaciones de trabajo nuevas o existentes usando una única conexión de host USB 3.0 de alta velocidad.

El ancho de banda de transferencia de datos ofrecido por USB 3.0 brinda a los integradores de sistemas la oportunidad de escalar la capacidad de generación de imágenes SATA de las estaciones de trabajo al agregar varias unidades T3iu. Ya sea que se use solo o en combinación con el Puente Combinado Forense T35689iu de Tableau, el T3iu es una forma rentable de eliminar su acumulación de imágenes SATA.

Tableau Forensic T356789iu IDE/SATA/SAS/FW/USB3.0/PCIe U$S 1,079.00*

(URL: https://www.tableau.com/es-es/products)

Tableau Forensic T356789iu es el último puente forense OEM integrado de Tableau. El T356789iu ha sido completamente rediseñado. Las ganancias de rendimiento del T356789iu en comparación con la generación anterior del T35689iu puede ser mucha.

OPCIONALES

Tableau TD2u Forensic Duplicator U$S 1,479.00*

(URL: https://www.tableau.com/es-es/products)

TD2u: Extremadamente Rápida. Real. Rápida para usar.

Construido para sobresalir tanto en el campo como en el laboratorio, el Duplicador Forense TD2u de Tableau es la combinación perfecta de fácil operación, confiabilidad y rendimiento de imágenes forenses ultra-rápido. Las imágenes duplicadoras de cuarta generación de Tableau a velocidades excepcionales de más de 15 GB / min mientras que al mismo tiempo calculan hashes MD5 y SHA-1. La velocidad de imágenes forenses un rasgo de Tableau en un punto a tener en cuenta respecto al precio. Construido con la tecnología más avanzada, Eso ofrece TD2u.

Tableau TX1 Forensic Imager U$S 2,999.99*

(URL: https://www.tableau.com/es-es/products)

Tableau TX1 Forensic Imager es lo último y mejor de Tableau y es una alternativa portátil para llevar una estación de trabajo forense al campo.

Es un generador de imágenes totalmente forense habilitado para redes que ofrece un rendimiento de imagen local y de red superior sin compromisos. El Tableau TX1 establece el estándar para imágenes forenses.

PC / WORKSTATION U$S 4,990

(http:www.air-computers.com.ar)

Descripción: PC “POTENTE” Para equipamiento de LABORATORIO:

-Marca de las más Conocidas del Mercado como HPE

-PROCESADOR CORE I7 7MA/8VA/Xeon GENERACION

-MOTHERBOARD FACTOR ATX C/SOPORTE 64/128 GB MEMORIA, PUERTOS FIREWIRE, USB 3.0, E-SATA, SOPORTE PCI/PCI-E, ETC

-MEMORIA RAM DDR4 3200/3600 MHZ 64 GB

-PLACA DE VIDEO PCI-E QUADRO O SIMILAR

-UNIDAD DISCO SSD 250/500 GB

-UNIDAD DISCO HDD 4 TB WD CAVIAR BLACK/SEAGATE / WD VELOCIRAPTOR X 3

-UNIDAD OPTICA DVD-RW 24X SATA LG/SAMSUNG

-GABINETE TOWER C 5 BAHIAS 5 ¼" / 5 BAHIAS 3 1/2"

-FUENTE ALIMENTACION CERTIFICADA 96% 1200 VA C/6/8 CONECTORES ALIMENTACION UNIDADES

-MONITOR DE 22" HDMI

-**UPS** 2 X 1200 VA

INSUMOS BASICOS / ELEMENTALES (PARA TRABAJO DE CAMPO Y LABORATORIO)

UNIDAD DISCO EXTERNO 4 TB USB 3.0 X 2 UNIDADES

UNIDAD DISCO HDD 4/6/8 TB WD CAVIAR BLACK/SEAGATE …. X 4 UNIDADES

PENDRIVE 8 / 16 / 64 GB X 6/8 UNIDADES

DISCOS DVD-R - VARIOS

CALBES Y CONECTORES VARIOS

UNIDAD EXTERNA LECTORA DE TARJETAS DE MEMORIAS

UNIDAD INTERNA LECTORA DE TARJETAS DE MEMORIAS

CUNA/DOCKING USB 3.0 LECTORA DE DISCOS HDD IDE/SATA CON BLOQUEO DE ESCRITURA Y CABLES INTERFASE

CUNA/DOCKING USB 3.0 LECTORA DE DISCOS HDD IDE/SATA CON CABLES INTERFASE

CASE/COFRE/CARRY PARA DISCOS HDD IDE/SATA 2,5" / 3,5"

PARA TRABAJO DE CAMPO PARA OPERAR CON TELÉFONOS MÓVILES

- **UFED Touch "2" Ultimate: U$S 10,499.00* (MSRP)**

url: CELLEBRITE UFED Touch2 (https://digitalshield.net/products/cellebrite-ufed)

Esta plataforma de ciencia forense digital portátil de última generación brinda capacidades integrales de extracción en el sitio en donde se necesite ya sea en el laboratorio, en una ubicación remota o en el campo. Avance más rápido, reduzca los pendientes, libere hardware valioso y produzca evidencia defendible con Touch2.

Poderosa y compacta, Touch2 está disponible con UFED Ultimate y se ofrece con un conjunto de accesorios forenses. Extraiga datos de manera rápida y segura en un entorno cerrado, separado de otras aplicaciones y elimine cualquier riesgo de realizar contaminación cruzada de la evidencia digital. Visualice registros de llamada, imágenes, videos y otros datos lógicos clave directamente desde Touch2 en el punto de extracción para un acceso rápido a evidencia clave. Con la versatilidad del cómputo rápido y una mayor vida útil de la batería, Touch2 es una experiencia de extracción con solidez forense y prácticamente sin mantenimiento.

Funciones:

- 1024 alta resolución, pantalla multitáctil
- Lector SIM múltiple incorporado

- DDR3L 8GB RAM
- USB fase 3.1, 1 axilar (hasta 5Mbps)
- Wi-Fi bgnac (hasta 350 Mbps)
- Disco duro grande y rápido (SSD 128GB)
- Windows 10 personalizado

Conjunto de ciencia forense digital de Cellebrite:

- Conjunto de punta y cable
- Organizador de punta y cable
- Lector de tarjeta de memoria UFED
- Adaptador de SIM múltiple
- Tarjetas SIM de clonado de ID UFED
- Microtarjetas SIM de clonado de ID
- Nanotarjetas SIM de clonado de ID
- Cable de alimentación de teléfono
- Cepillo de limpieza para conectores de teléfono
- Correa con velcro para punta
- Cartucho de puntas de repuesto

Unidad flash USB

Cable de alimentación de extensión de USB Cámara UFED opcional

(*) Los Precios son indicativos en el país de origen y en valor Dólar Estadounidenses, no incluye impuestos a la importación (35%-45%), porcentaje de IVA y otros costos como los de logística/transporte.

2.4. Conclusiones

En distintos países existen instituciones privadas que dedican su trabajo a peritajes informáticos, para realizar la adquisición y el análisis de la evidencia digital. En nuestro país es casi imposible realizar la adquisición de estos “equipos”, pues debido a que sería imposible amortizar su “costo”, la fabricación de estos sofisticados equipos respecto a lo que realizan y la durabilidad de los mismos son realizados en empresas extranjeras y cotizan en Dólares Estadounidenses (U$S) o Euros y la conversión de los mismos a nuestra moneda pesos ($) Argentinos hace que directamente sea algo inalcanzable.

Estos equipos varían su costo teniendo en cuenta cuestiones técnicas como su "velocidad de procesamiento", cantidad de información a analizar, si son como explicábamos anteriormente equipos de campo portátiles o equipos para laboratorios de análisis forense.

La empresa EIF (estudio de Informática Forense), de Argentina [EIF], nos hizo llegar cotizaciones de equipos comercializados en nuestro país y sus recomendaciones.
La persona de contacto fue el Ing. Gustavo Daniel Presman [GDP] (contestación correo electrónico recibido 11-10-2018), quien nos sugirió para trabajo de campo lo siguiente:

Recomiendo normalmente para iniciarse (básico):
La adquisición de un Kit Bloqueador de escritura IDE/SATA (para no modificar la Evidencia), que servirá para los discos más utilizados. Este Kit incluye el bloqueador, fuente de alimentación, cables IDE/SATA, Cable de datos USB 3.0 y bolso de transporte. (Esta es una herramienta muy básica para levantar la imagen forense, falta todo lo referente a el análisis de la evidencia digital y montar nuestro laboratorio forense).
Costo en Pesos Argentinos $ 29800 + IVA (10,5%), Total > $ 32929.-

Con esto se demuestra que para que un perito informático cuente con el Hardware necesario para realizar un peritaje informático libre de errores, rápido y que el dictamen realmente sirva como medio de prueba para la justicia, necesita hacer grandes inversiones que hoy en día nunca podrá amortizar, de todos modos está capacitado para hacerlo por los conocimientos técnicos adquiridos.

3. SOFTWARE.

3.1. Tipos de Herramientas de Software Aplicadas en el Análisis Informático Forense.

Existen múltiples herramientas de software que tienen como marco de acción el análisis forense informático, las cuales permiten encontrar pistas, descubrir detalles, que sirven como medio de prueba para el descubrimiento de los objetivos a cubrir por un análisis informático forense, en la siguiente explicación de cada tipo de herramientas no solo vamos a explicar su técnica y sino que también vamos a hacer practica de los mismas en funcionamiento, en cuyas figuras (captura de imágenes del programas en ejecución), obtendremos el sitio web (url) de donde se obtuvieron los software. Los programas se clasifican por tipo de herramientas:

- **Herramientas de red:** Existen múltiples variedades de herramientas de red, entre los más comunes tenemos a los capturadores de tráfico, que permiten la captura de los paquetes de datos que se transmiten y reciben por equipos informáticos en una red local; están los sistemas de detección de intrusos (o IDS abreviatura de sus definición en inglés Intrusion Detection System) que son aplicativos que permiten detectar cualquier acceso no autorizado a un solo computador o a una red de computadores. Se conocen dos tipos de Sistemas de Detección de Intrusos:
    - **HIDS (HostIDS)**: Un IDS para Hosts. Este permite detectar en el equipo donde se encuentra instalado rastros de las actividades de los intrusos.
    - **NIDS (NetworkIDS)**: un IDS basado en red. Este permite detectar en todo el segmento de la red donde se encuentre instalado, el rastro dejado por los intrusos, para lo cual la interfaz debe funcionar en modo promiscuo, lo cual le permitirá capturar la totalidad del tráfico de la red.

      Este tipo de software está basado en un análisis exhaustivo de la información que circula en la red donde se encuentran instalados.

      Información que es confrontada frente a firmas de ataques reconocidos almacenados en una base de datos propia del IDS.
- **Herramientas de encriptación:** Mediante este tipo de software se cifran archivos o documentos utilizando un algoritmo específico. Este tipo de software se usa para proporcionar un nivel de seguridad fuerte en lo concerniente a la accesibilidad de archivos privados o confidenciales.
- **Editores Hexadecimales:** Un editor hexadecimal, también llamado editor de archivos binarios, es un tipo de software que permite leer y modificar el contenido de archivos binarios. También se les conoce como “editores de sectores” porque pueden leer datos almacenados en sectores específicos en una unidad de almacenamiento magnético y modificarlos de igual forma que si estuvieran modificando un archivo binario.

  Por medio de este tipo de software se puede editar el contenido de cualquier archivo binario, lo cual permite entre otras cosas analizar si existe algún tipo de malware embebido en un archivo binario o alguna función maliciosa.

- **Herramientas de virtualización:** Son programas que permiten transportar una infraestructura física de un equipo informático (incluyendo su software) a una plataforma de software que simula la totalidad de los componentes de su arquitectura.

  Mediante este tipo de software se puede instalar en un sistema real, un sistema virtualizado que simula el funcionamiento de un equipo informático sin afectar la configuración de su huésped pero si aprovechando sus recursos físicos (disco duro, memoria RAM, etc.), permitiendo en este sistema virtualizado instalar y verificar cualquier software sin comprometer nuestro sistema real.
- **Emuladores:** Tipo de software que permite ejecutar software (programas o videojuegos) en una plataforma diferente para el que fue desarrollado, tanto a nivel de hardware como de sistema operativo.

  Mediante un emulador se imita de la forma más fiel posible un dispositivo y su plataforma de tal manera que funcione como si se tratara del dispositivo original.
- **Herramientas de borrado de archivos:** Son programas que permiten borrar archivos en un dispositivo de almacenamiento de manera segura, de tal forma que no se pueda recuperar el archivo borrado mediante un programa especializado en recuperación de archivos. Para ello utiliza una serie de algoritmos de borrado que permiten que el archivo sobre el que se aplique su funcionalidad quede irrecuperable.

  Este tipo de software se suele utilizar en la medida que necesitamos eliminar documentación confidencial de un dispositivo de almacenamiento, al cual puede tener acceso personal sin la autorización pertinente para su lectura.
- **Herramientas de recuperación de Contraseñas:** Herramientas que permiten recuperar contraseñas usadas en el sistema operativo investigado.
- **Herramientas de recuperación de datos o archivos**: Son programas que permiten recuperar archivos borrados previamente. Utilizan varios formas de recuperación como recuperación en bruto (cuando ha sido formateado el dispositivo de almacenamiento), recuperación rápida (cuando ha sido borrado el archivo recientemente), entre otros.

Este tipo de software se suele utilizar en la medida que necesitamos recuperar documentación borrada de un dispositivo de almacenamiento, ya sea de forma intencional o no.

- **Herramientas de investigación y análisis**: Son aplicativos orientados a la investigación y análisis forense. Entre otras funcionalidades ofrecen recolección de evidencia digital, realización de análisis de la evidencia digital recolectada e informe detallado del mismo.

  Son aplicativos que tienen una gran importancia en la investigación informática forense, por la cantidad de funcionalidades que ofrece en la consecución y análisis de evidencias digitales.
- **Herramientas de análisis de discos (Montaje y Recuperación)**: Software que permite montar imágenes de discos, producto de copias a la evidencia original, para su análisis especializado y determinar si la imagen está afectada en su integridad.
- **Clonación:** Software especializado en copiar bit a bit la información contenida en una unidad de almacenamiento lógico (disco duro, pendrive, etc.) y volcar esta información en otro dispositivo de igual o mayor capacidad; también permite volcar esta información en un archivo digital que se puede tratar mediante software especializado como si fuese la unidad de almacenamiento lógica original. Este tipo de software es de gran importancia al momento de tratar una o más unidades de almacenamiento lógicas como evidencia en un delito informático, ya que permite clonarlos para realizar los análisis sobre las copias y de esta forma preservar la evidencia original.
- **Herramientas de adquisición y análisis de memoria:** Herramientas de software que permite tener acceso a la memoria RAM de un equipo, adquirirla y exportarla a un archivo para su análisis posterior.
- **Distribución LiveCD de Linux:** Es un tipo de distribución Linux que no requiere instalarse en el computador, ya que se puede ejecutar directamente desde un pendrive o un dvd.

3.1.2. Herramientas de Informática Forense.

Herramientas de red:

- **TCPDump**: Es un software analizador de trafico de paquetes de red, funciona a nivel de línea de comandos. Esta herramienta permite analizar el funcionamiento de aplicaciones, detectar problemas en la red o capturar datos que se transmiten por la red y se encuentre sin encriptación alguna (Figura 1). Hay una versión similar para entorno Windows llamada Windump (Figura 2).

*Figura 1

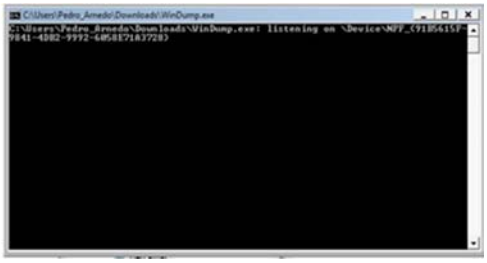


*Figura 2

- **NetworkMiner:** Herramienta que permite capturar información de red. Permite analizarla aplicando filtros de búsqueda de datos.

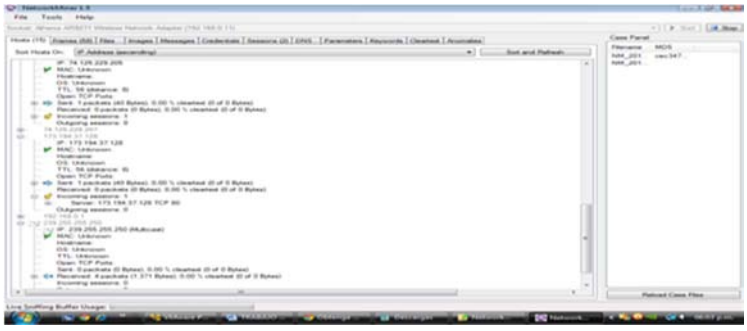


*Figura 3

- **Network Appliance Forensic Toolkit**: Paquete de herramientas forenses desarrolladas en lenguaje Python, que se especializan en la captura de tráfico en la red y análisis del mismo.
- **WireShark**: Es un software que permite capturar tramas y paquetes que circulan a través de una interfaz de red. Este aplicativo posee todas las características mínimas requeridas por un analizador de protocolos.

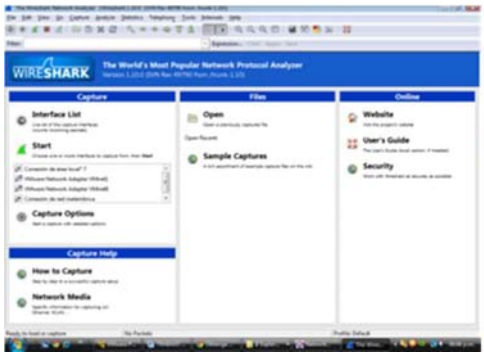


*Figura 4

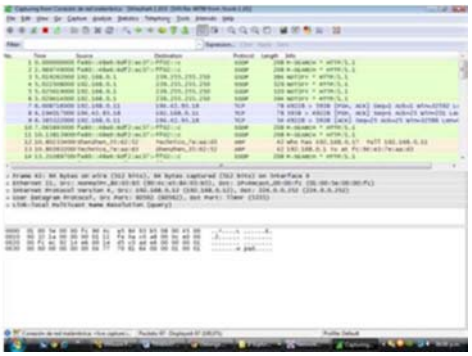


*Figura 5

- **Xplico**: Software que permite capturar el tráfico de la red, con la particularidad que permite extraer los datos transmitidos mediante el protocolo HTTP y los mensajes de correos electrónicos que tienen implementado los protocolos POP y SMTP.

*Figura 6

o **Splunk:** Software que funciona en los sistemas operacionales más importantes del mercado, permite monitorear y analizar el tráfico de la red, detectando entre otros aspectos transacciones, registros de llamadas y lugares de navegación de los usuarios. Cuenta con un módulo de firmado de datos, que permite generar una prueba de autenticidad en cualquier proceso de análisis forense o auditor.

*Figura 7

- **Snort.**: Es un software libre y de código abierto que funciona como un sistema de prevención de intrusiones de red (NIPS) y sistema de detección de intrusiones de red (NIDS). Este software tiene la capacidad de realizar un análisis de tráfico en tiempo real y registro de paquetes generados por el protocolo IP, lo cual deja plasmado en una bitácora o archivo tipo log, para su análisis posterior.

  Snort puede ser configurado en tres modos principales:

  - Rastreador: se comporta como un registrador de paquetes y de detección de intrusiones en la red;
  - Sniffer, en este modo el software lee los paquetes de red, los muestra en la consola y los registra en el disco.
  - Detección de intrusos: en este modo el software rastrea el tráfico de red y lo analiza frente a un conjunto de reglas definidas por el usuario, de acuerdo a lo obtenido de este análisis ejecutará la acción adecuada para su mitigación o corrección.

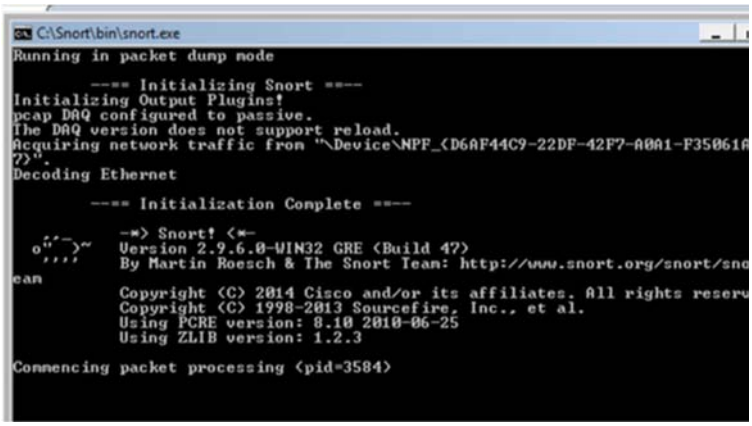


*Figura 8

Las Herramientas de red en su mayoría reflejan cualquier aspiración de un analista de paquetes de red y obtener los datos necesarios para el análisis forense de aplicaciones de internet, a partir de todo lo relacionado con el tráfico de red, en busca de patrones anómalos, malware, conexiones sospechosas, identificación de ataques, fallos en las políticas de seguridad y hasta envió de correos electrónicos (protocolos POP y SMTP). En las Direcciones y links encontrados en las referencias de las figuras de cada software

se pueden bajar y comprar las versiones de los programas con licencia propietaria, y hasta bajar versiones de prueba.

Respecto a los costos existen herramientas gratis bajo entornos de DOS, también versiones como triales o free con limitantes de tráfico diario (ej. 500 mb, o 1 GB. Diarios, o más), cantidad de usuarios (uno, cinco, veinte o más) y tipo de servicios tales como monitoreo y así van elevando el costo de cada versión. Estas van desde u$s 75 en versiones Lights, hasta de u$s 150 la versión Enterprise por mes, con facturación anual y siempre con los limitantes mencionados anteriormente.

LINUX es la mejor plataforma para el despliegue de herramientas de análisis forense**.** Hay disponibles más herramientas forenses para LINUX que para ningún otro sistema operativo, siendo la mayoría de estas herramientas no sólo gratuitas sino de código abierto (*Open Source*) lo que permite al perito adaptar y configurar las mismas a la medida de sus preferencias y de las necesidades de cada caso en concreto.

Herramientas de Cifrado:

- **PGP:** Aplicativo desarrollado por Phil Zimmermann, el cual tiene como funcionalidad principal la de proteger archivos de datos mediante el uso de criptografía de clave pública y además ofrece la facilidad de autenticación de documentos a través de firmas digitales.

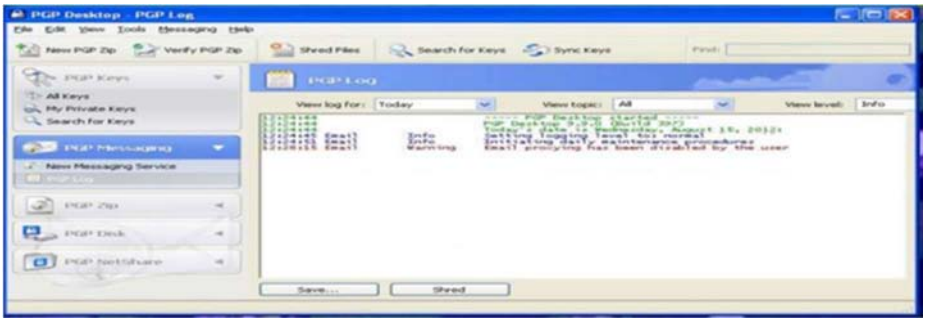


*Figura 9

- **GpG4Win:** Aplicativo que sirve para encriptar datos mediante un sistema de clave pública bajo Windows.

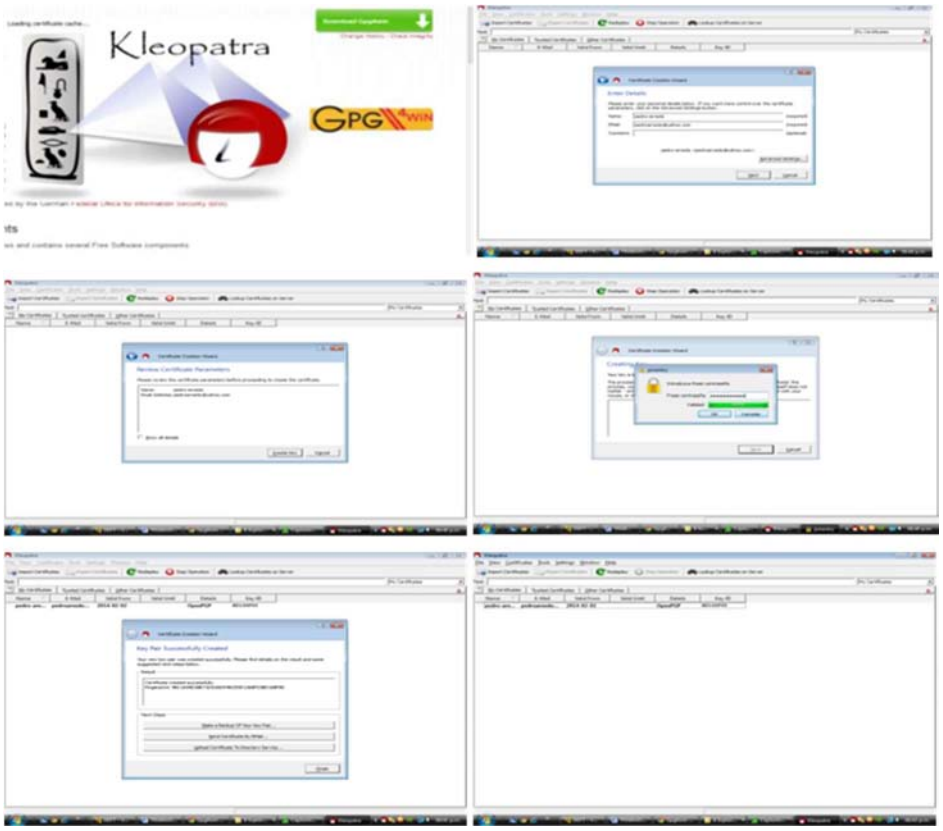


*Figura 10

Editores.

- **WinHEX:** Es un editor hexadecimal que permite editar todos los tipos de archivos, dispositivos de almacenamiento y memorias RAM. Además permite recuperar archivos borrados en dispositivos de almacenamiento con sistemas de archivos corruptos.

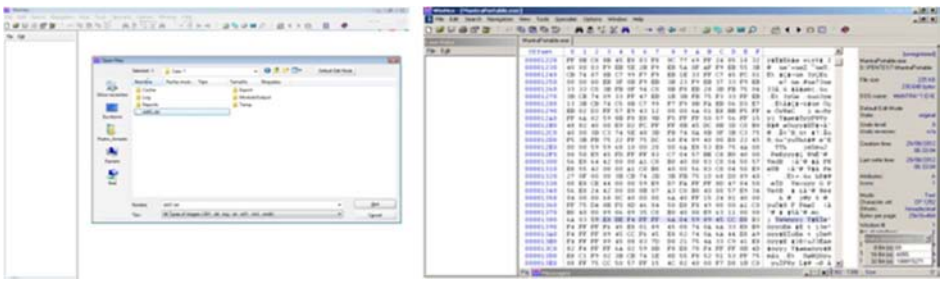


*Figura 11

- **GHEX**. Es un editor hexadecimal que permite editar todos los tipos de archivos, dispositivos de almacenamiento y memorias RAM. Software para ambiente Linux.

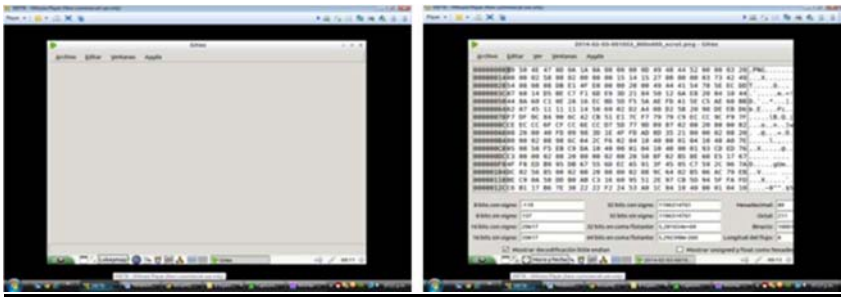


*Figura 12

Herramientas de Virtualización.

- **VMWare:** Software de virtualización para arquitecturas x86 y x86-64. Mediante este software se pueden crear virtualmente múltiples computadoras x86 y x86-64 en un sistema operativo huésped, cada una con su propio sistema operativo (Unix, Linux, Windows, etc.).

*Figura 13

- **VirtualBox:** Software de virtualización para arquitecturas x86/amd64. Mediante este software se pueden crear virtualmente múltiples computadoras, cada una con su propio sistema operativo (Unix, Linux, Windows, etc.)

*Figura 14

- **XEN:** La enciclopedia online Wikipedia define esta herramienta como: "Es un monitor de máquina virtual de código abierto desarrollado por la Universidad de Cambridge. La meta del diseño es poder ejecutar instancias de sistemas operativos con todas sus características, de forma completamente funcional en un equipo sencillo. Xen proporciona aislamiento seguro, control de recursos, garantías de calidad de servicio y migración de máquinas virtuales en caliente".

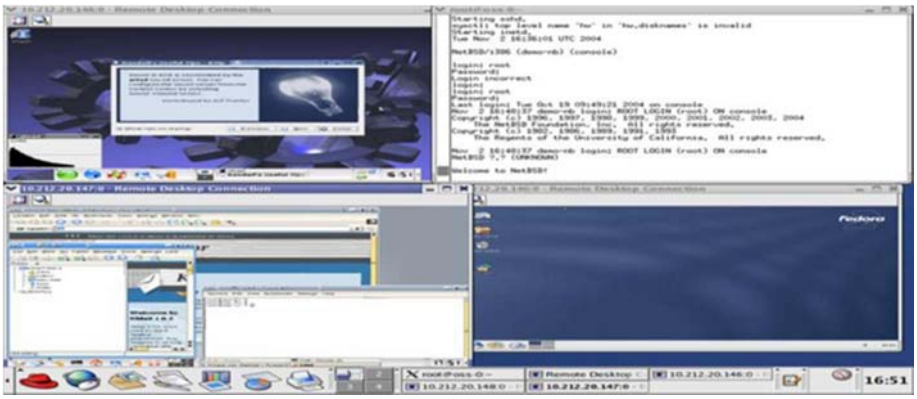


*Figura 15

Emuladores

- **Wine:** Es una re implementación de la interfaz de programación de aplicaciones de Win16 y Win32 para sistemas operativos basados en Unix. Permite la ejecución de programas diseñados para MS-DOS, y las versiones de Microsoft Windows.
- **Cygwin:** Software que permite tener un entorno de Linux dentro de un sistema Windows. Recuperación de archivos. En esta parte es importante definir un proceso conocido como "Carving", que en si es el proceso de extracción de un conjunto de datos utilizando una técnica de análisis de información que no se basa en la estructura del sistema de archivos. También se podría definir como la extracción de un conjunto de datos que se encuentran inmersos en otro conjunto de datos.

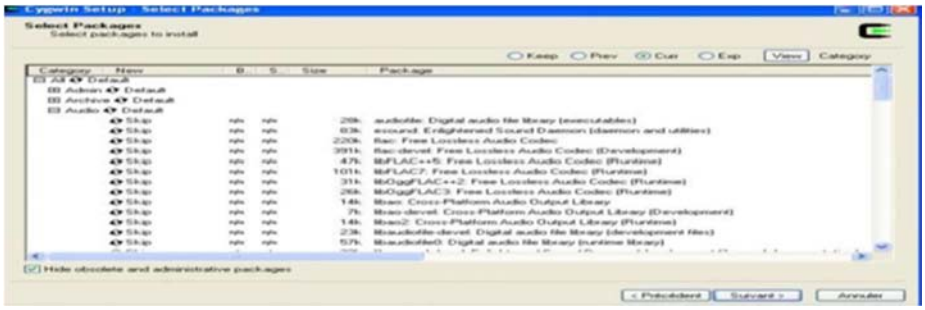


*Figura 16

- **Raid Reconstructor:** Herramienta que permite recuperar datos de un sistema RAID 0 o RAID 5 dañado.

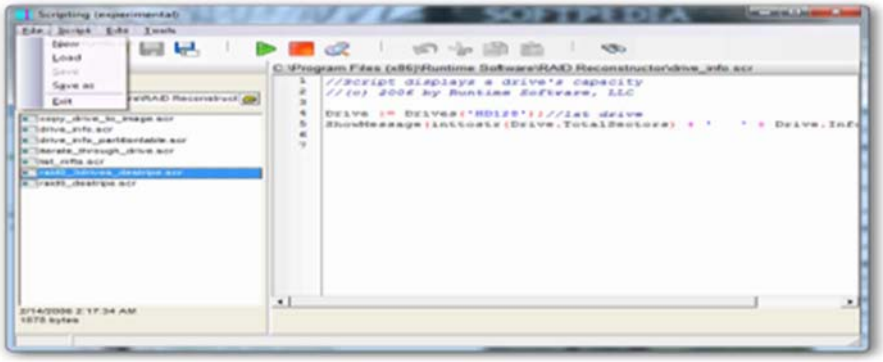


*Figura 17

- **Raid Recovery:** Herramienta que permite recuperar datos de un sistema RAID 0 o RAID 5 dañado. Desarrollado por la reconocida empresa DiskInternals.
- **NTFS Recovery:** Software que permite la recuperación de archivos eliminados en sistemas NTFS. Desarrollado por DiskInternals.

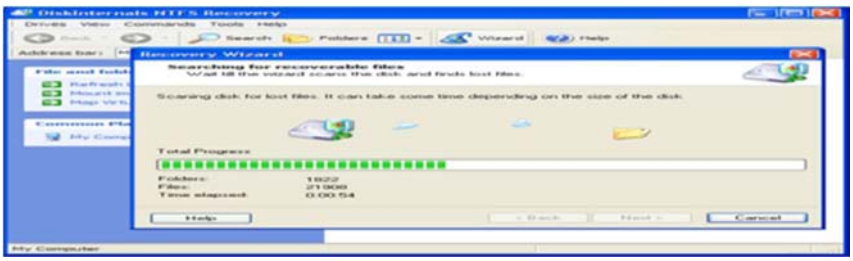


*Figura 18

- **Fat Recovery:** Software que permite la recuperación de archivos eliminados en sistemas FAT. Desarrollado por Diskinternals.

- **Linux Recovery:** Software que permite la recuperación de archivos eliminados en sistemas Ext2/Ext3 desde Windows. Desarrollado por Diskinternals.
- **Recuva:** Software especializado en la recuperación de archivos eliminados.

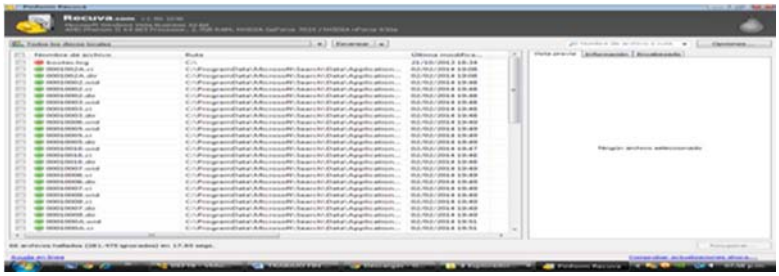


*Figura 19

- **CNW Recovery:** Herramienta que permite recuperar sectores dañados.

  Permite extraer datos de mediante Carving.

*Figura 20

- **Rstudio**: Software que permite recuperar archivos de múltiples sistemas de archivos, entre otros: NTFS, NTFS5, ReFS, FAT12/16/32, exFAT, FS/HFS, UFS1/UFS2 y particiones Ext2/Ext3/Ext4.

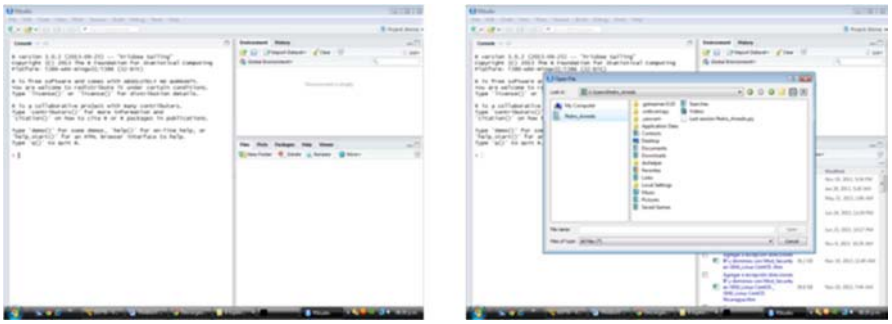


*Figura 21

- **FreeRecover:** Herramienta que permite recuperar archivos borrados en discos duros o unidades de almacenamiento con partición NTFS.

- **IEF (Internet Evidence Finder):** Software que permite buscar evidencias en las imágenes de discos (o en discos directamente) extrayendo mediante el proceso de Carving, datos sobre archivos abiertos desde portales que ofrecen almacenamiento en la nube, tales como dropbox, google drive, skydrive, entre otros. Entre los datos que trata de encontrar están :tamaño y nombres de archivos, fechas y horas de acceso, nombres de usuario y tamaño de los archivos.

*Figura 22

- **Bulk_extractor**: Software que permite extraer datos desde un archivo o imagen e inclusive desde carpetas.

*Figura 23

Borrado de archivos

- **Wipe**: Software que tiene como finalidad borrar archivos de cualquier medio de almacenamiento de forma segura y recuperar el espacio libre existente en el mismo. Además permite eliminar cualquier registro relacionado con la actividad personal en el equipo informático.

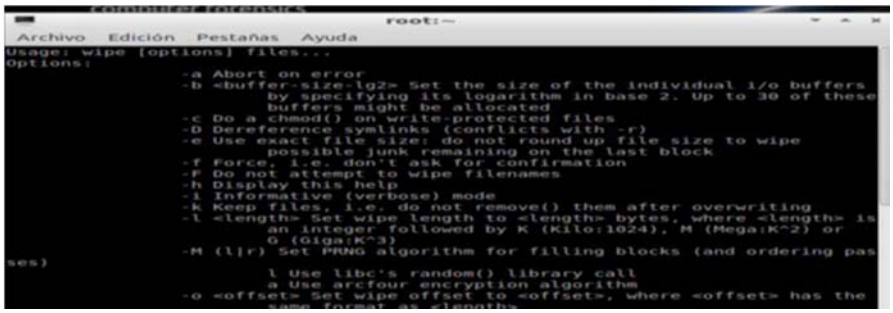


*Figura 24

- **HardWipe**: Software que tiene como finalidad borrar archivos de cualquier medio de almacenamiento de forma segura y recuperar el espacio libre existente en el mismo. Cuenta con varios algoritmos de borrado seguro como GOST R, DOD 5220, Schneier y Gutmann.

Recuperación de Contraseñas:

- **Ntpwedit :** Software que permite cambiar o eliminar contraseñas en sistemas Windows versiones 2000, XP, Vista, 7, 8 y 10, pero no aplica para sistemas Windows que implementen Active Directory (Windows Server).

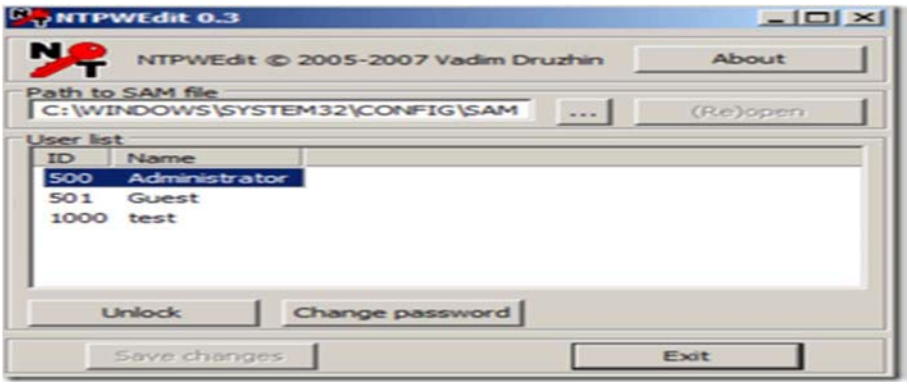


*Figura 25

- **John The Ripper:** Programa que permite descubrir contraseñas a base de fuerza bruta. La interfaz gráfica se denomina Johnny.

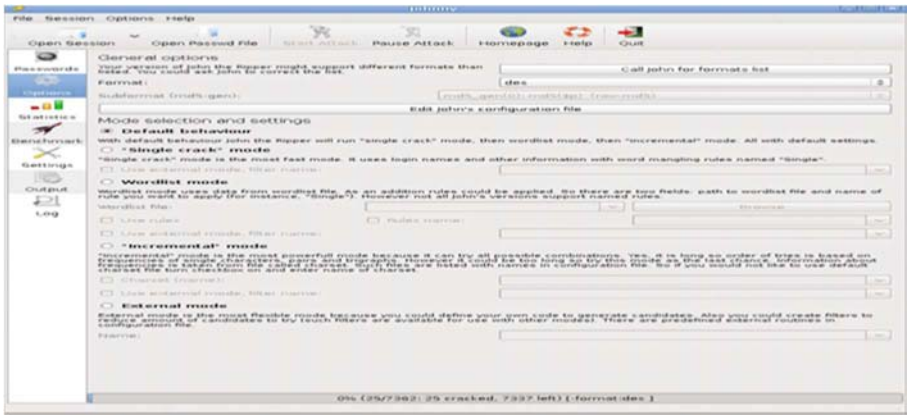


*Figura 26

- **Ntpasswd**: Software parecido a Ntpwedit, con la particularidad que permite arrancar el sistema desde un CDLive y ejecutarse desde allí para su proceso de recuperación.
- **Cain & Abel:** Aplicativo para analizar tráfico y permite también recuperar contraseñas bajo entorno Windows.

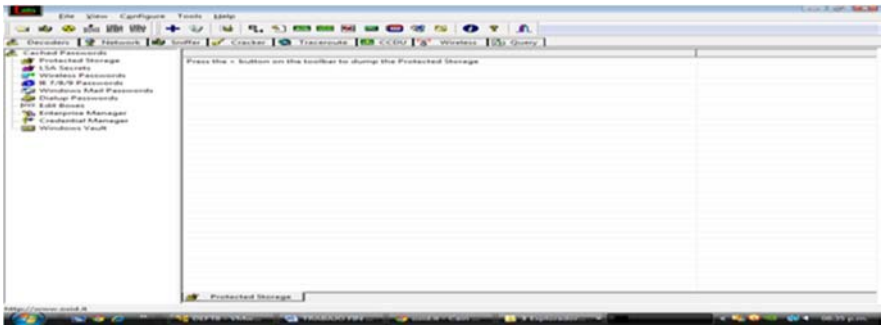


*Figura 27

Frameworks (Suite de herramientas estandarizadas para el análisis forense):

- **Sleuth Kit y Autopsy**: Sleuth Kit es una colección de herramientas robustas para el análisis forense de volumen de sistema y archivos.

  Autopsy es la interfaz gráfica que permite utilizar de una forma más fácil y amigable todo el potencial de este aplicativo.

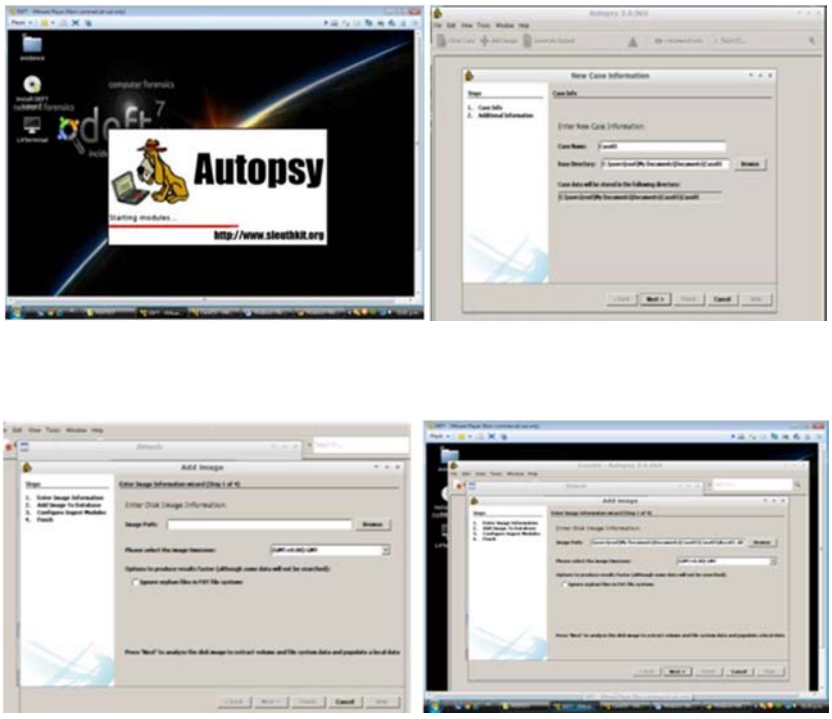


*Figura 28

- **Encase Forensic:** Software líder mundial para el análisis forense informático, desarrollada por la empresa Guidance Software Inc., mediante la cual se recolectan datos digitales, se realizan análisis y se realizan informes sobre descubrimientos en la escena del crimen. Entre muchas características relevantes de ENCASE que la convierte en un marco referencia en el mundo del software informático forense se puede destacar:
  - Copiado de Discos Fuente en formato Comprimido. Encase permite crear copias comprimidas sin perdidas de datos durante el proceso de compresión. Además las copias comprimidas se pueden tratar en todo el proceso de análisis forense de igual forma que se manejaría el dispositivo original. Esto genera ventajas como el ahorro de espacio en el disco del equipo donde se hace el trabajo forense.
  - Encase permite al equipo investigador hacer comparativos en paralelo con otras copias sin complicaciones. La evidencia puede ser analizada en forma local o en red por el investigador y Encase permite además que pueda ser colocada en dispositivos de diferentes características como puede ser de tecnología IDE, SCSI, ZIP, etc.

- Encase permite analizar las cabeceras de los archivos en un dispositivo o copia digital permitiendo descubrir tipos de archivos ocultos o modificados intencionalmente para su no detección.

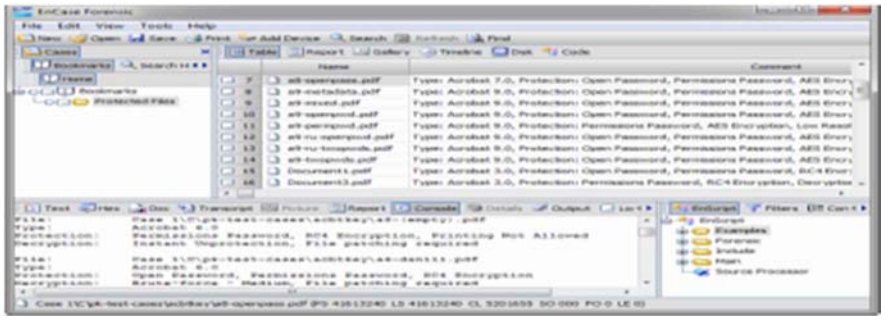


*Figura 29

- **OSForensics**: Conjunto de herramientas forenses, que permiten entre muchas opciones realizar análisis sobre copias de discos montados en el sistema, búsqueda de archivos y generación de Hash.

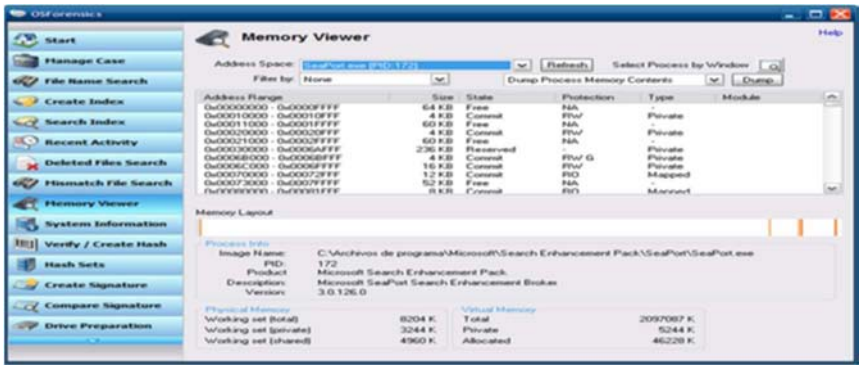


*Figura 30

- **Forensic Toolkit**: Desarrollado por AccessData, es un aplicativo forense muy completo. Entre sus características más sobresalientes se pueden destacar:
  - Permite analizar cientos de ficheros en búsqueda de características predefinidas, lo cual favorece al investigador forense a descubrir evidencias más rápidamente.
  - Maneja 270 tipos de formato de ficheros diferentes.
  - Permite recuperar particiones borradas.
  - Permite recuperar correos electrónicos borrados parcial o totalmente.
  - Ubica archivos por tipo analizando la cabecera de los mismos, detectando extensiones y archivos modificados intencionalmente.

- Permite extraer datos de ficheros comprimidos con los algoritmos comunes de compresión (Zip, Rar, Gzip, Tar. Permite generar informes detallados.

*Figura 31

- **Digital Forensic Framework (DFF)**: Framework para análisis forense, con licenciamiento libre y código abierto. Cuenta con su propio entorno gráfico lo que permite ser usado más fácilmente por personal no experto. Entre las funcionalidades que ofrece están:
  - Preservación de la evidencia digital (cadena de custodia). Ofrece funcionalidad en cuanto a bloqueo de escritura de software y cálculo de hash criptográfica.
  - Acceso a dispositivos locales y remotos. Unidades de disco, dispositivos extraíbles, sistemas de archivos remotos.
  - Lee formatos de archivos forenses digitales. Ewf, AFF 3, formatos de archivo RAW.
  - Reconstrucción de disco de máquina virtual. Reconstruye discos virtuales corruptos compatibles con VMware.
  - Análisis de archivos en Windows y Linux. Registro, buzones, NTFS, los sistemas de archivos FAT 16/12/32.
  - Búsqueda de (meta) datos. Las expresiones regulares, diccionarios, búsqueda de contenidos, etiquetas, etc.
  - Recupera objetos ocultos y eliminados.
  - Análisis de la memoria RAM. Procesos, archivos locales, extracción binaria, conexiones de red.

Análisis de discos (Montaje, Virtualización y /o Recuperación).

- **Smart**: Desarrollado por ASR Data, software cuya finalidad es el apoyo al análisis forense. Este permite detectar todos los dispositivos de almacenamiento conectados a un computador, su estructura lógica (particionamiento) y demás características, entre las que se destacan marca, modelo, capacidad y serial.
- **ILook:** Software muy completo para el análisis forense informático, entre sus principales características podemos detallar que permite extraer y analizar imágenes digitales de medios de almacenamiento, analizar cabeceras de archivos para validación real de tipo de archivos, editor hexadecimal integrado, entre otras.
- **ImDisk:** Software que permite crear virtualmente unidades de discos y de CD/DVD usando imágenes de discos o la memoria del sistema.

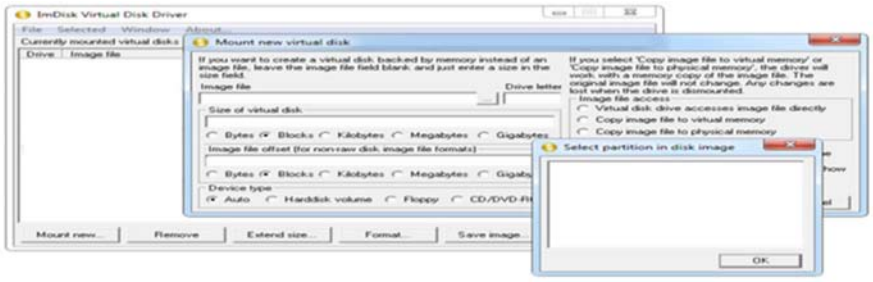


*Figura 31

- **Daemon Tools**: Software que permite montar imágenes de disco. Es comercial pero presenta una versión lite con mucha funcionalidad.

*Figura 32

- **PassMark OSFMount**: Software que permite montar imágenes de discos en unidades virtuales.

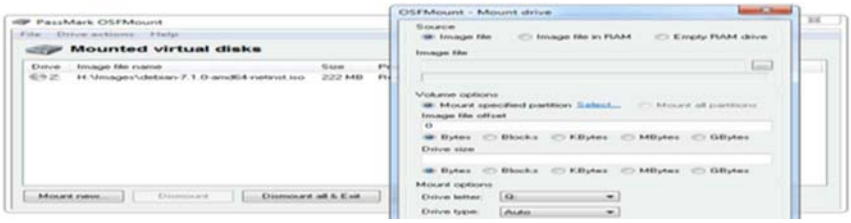


*Figura 33

- **LiveView:** Herramienta que toma una imagen de disco y genera con ésta una máquina virtual que se puede utilizar con la herramienta VMware.
- **MountImagePro**: Software que permite montar imágenes de discos en unidades virtuales.
- **PhotoRec:** Herramienta que tiene entre muchas otras funcionalidades la del tratamiento de imágenes de discos.

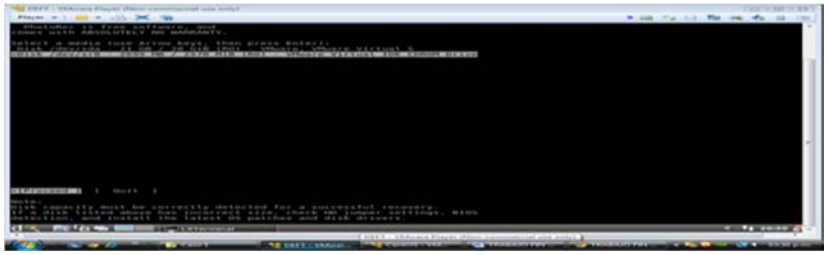


*Figura 34

Clonación:

- **Ghosts:** Software que permite clonar o crear imágenes de un medio de almacenamiento permitiendo copiar el contenido completo o una partición específica. Este clonado se puede realizar a otro disco de igual o superior tamaño o como un archivo que se puede restaurar posteriormente.

*Figura 35

- **Acronis**: Este software de clonado permite crear una imagen exacta del disco o de los discos de un servidor Windows o Linux, incluyendo el sistema operativo, las bases de datos y las aplicaciones instaladas en el mismo. Esta clonación posteriormente se puede migrar a servidores virtuales o físicos.

*Figura 36

- **Dc3dd:** Software que permite crear imágenes o copias de unidades de almacenamiento.

*Figura 37

Adquisición y Análisis de Memoria.

- **RedLine:** Software, con interfaz gráfica, que permite adquirir la memoria RAM y analizarla.
- **FTK Imager**: Software que se especializa principalmente en la adquisición de memoria RAM.

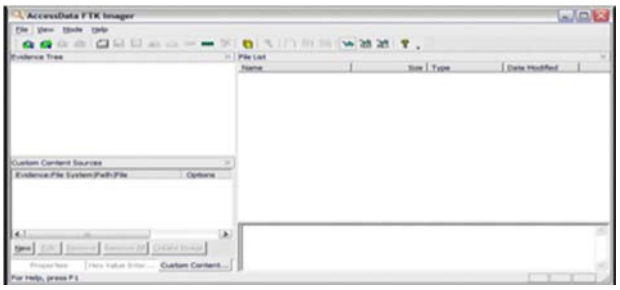


*Figura 38

- **Proccess Dumper (PD)**: Herramienta que permite exportar un proceso de la memoria RAM a un archivo.

- **DumpIt**: Aplicativo que permite realizar volcados de la memoria RAM a un archivo.

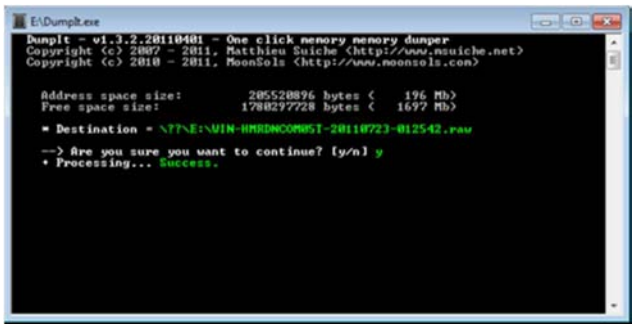


*Figura 39

- **Volatility**: Herramienta que permite analizar los procesos que se están ejecutando en la memoria RAM y extrae de ellos información relevante.

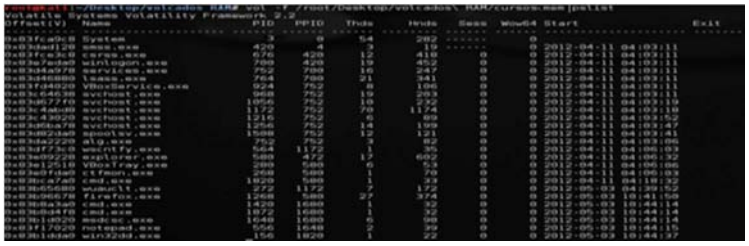


*Figura 40

Sistema de Archivos: Tipo de software para el tratamiento de archivos.

En este ítem es pertinente conocer la definición de "Tabla Maestra de Archivos" (MFT: Master File Table), la cual podemos enunciar como una base de datos que contiene entradas que relacionan en su totalidad los archivos de sistema, archivos del usuario y directorios que componen un volumen de disco.

También es importante conocer la definición de "Directorio Prefetch", el cual es un directorio presente en el sistema de archivos de Windows que almacena información en una serie de archivos pequeños correspondiente a los programas que se abren regularmente en un equipo, para que al momento de iniciar un computador el reconozca estas preferencias y permita ejecutar estos programas más rápidamente. Si el directorio prefech se vacía, los programas comunes tardaran más en ejecutarse la próxima vez después del vaciado.

Las siguientes herramientas permiten el tratamiento directo sobre la Tabla Maestra de Archivos:

- AnalyzeMFT, MFT Extractor, MFT Tools, MFT_Parser.

  Las siguientes herramientas permiten el tratamiento directo sobre el directorio prefetch:

- Prefetch Parser, Winprefectchview

Análisis Registro de Windows.

En este ítem es importante anotar el concepto de shellbags, que se refiere a los espacios donde el sistema operativo Windows guarda la información correspondiente a las preferencias de los usuarios en lo concerniente a las propiedades de visualización de sus interfaces gráficas. Entre otras propiedades podemos mencionar: posición de las ventanas en la pantalla, tamaño de las ventanas, etc.

- **RegRipper:** Es una aplicación para la extracción, la correlación, y mostrar la información del registro.
- **WRR:** Software que permite obtener de forma gráfica importantes datos del sistema, usuarios y aplicaciones, tomando como base para extraer esta información el registro de windows.
- **Shellbag Forensics**: Software que permite analizar los shellbags de Windows.

Linux Distribución LiveCD

- **Backtrack:** Distribución de Linux especializada Seguridad Informática. Basada en Ubuntu, viene como LIVECD pero permite instalar la distribución en nuestro computador.

*Figura 41

- **KALI:** Distribución de Linux especializada Seguridad Informática. Basada en Debian, viene como LIVECD pero permite instalar la distribución en nuestro computador. Distribución dirigida a realizar auditorías de seguridad orientadas al sector profesional.

*Figura 42

- **CAINE**: Distribución de Linux de origen italiano, especializada en el análisis forense. Basada en Ubuntu, viene como LIVECD pero permite instalar la distribución en nuestro computador.

*Figura 43

- **DEFT:** Distribución de Linux especializada en el análisis forense, no solo de discos duros, también se pueden realizar análisis forenses de redes y de dispositivos móviles. Basada en Ubuntu, viene como LIVECD pero permite instalar la distribución en nuestro computador.

*Figura 44

- **MATRIUX.** Distribución de Linux dedicada a la seguridad con buenas herramientas de Informática Forense.

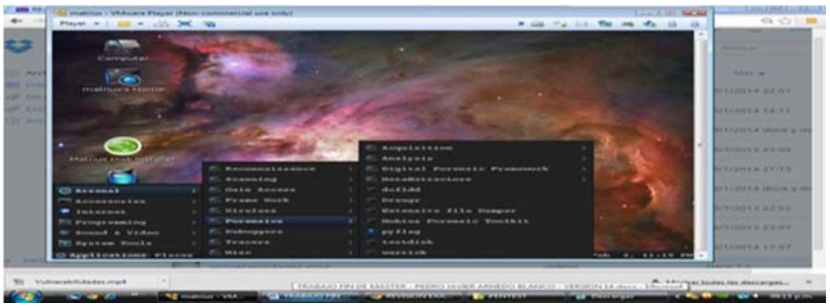


*Figura 45

- **BUGTRAQ:** Distribución de Linux que ofrece una gran cantidad de aplicativos para realizar pruebas de penetración y análisis forense. Esta distribución permite instalarse en un computador o utilizarse como un LiveCD desde un DVD o USB.

*Figura 46

3.2. Conclusiones

El perito puede utilizar LINUX para extraer y analizar las evidencias objeto de la pericia procedentes de otros sistemas operativos. Es decir, el uso de LINUX no impide analizar sistemas que ejecuten otros sistemas operativos. Por ejemplo, podemos usar LINUX para analizar una imagen de un disco duro procedente de un sistema WINDOWS.

VENTAJAS DE LINUX COMO HERRAMIENTA FORENSE

- Es gratuito. Además del ahorro que esto supone, su sistema de licencias permite al perito disponer de varios sistemas especializados en diferentes problemáticas.
- Existen muchas herramientas gratuitas (y de pago) desarrolladas para este sistema operativo.

- Existen multitud de distribuciones que proporcionan conjuntos de herramientas forenses listas para usar.
- Es fácil tener un sistema autónomo (LIVE CD) que permite acceder a los sistemas a analizar sin modificar el contenido del mismo.

DESVENTAJAS DE LINUX COMO HERRAMIENTA FORENSE

- Es más difícil de utilizar y configurar que un sistema comercial.
- Es menos conocido fuera del ámbito técnico por lo que su utilización puede generar inseguridad entre abogados y jueces.
- Las herramientas utilizadas no suelen tener licencias comerciales, ni empresas de software que garanticen el soporte de las mismas.
- La configuración de algunas herramientas y su adaptación a cada caso puede ser compleja y requerir conocimientos de programación.

Los sistemas bajo el entorno de LINUX son los más Utilizados por técnicos, profesionales y peritos, por la **relación costo-Beneficio**.

4. ASEGURAMIENTO FÍSICO

4.1. Aseguramiento Físico, Seguridad Perimetral y Central Informática Pericial

4.1.1. Consideraciones

Tener en cuenta en el momento de un aseguramiento de pruebas:

– Cuando se van a realizar grabaciones se deben utilizar dispositivos nuevos (embalaje original cerrado). CDs, DVDs, pendrives, rígidos, etc.

– Se deben separar las personas que trabajen sobre los equipos informáticos lo antes posible y no permitirles volver a utilizarlos. Desconectar equipos de la red.

– Fotografiar la pantalla / equipo / ubicación. Fotografiar una toma completa del lugar donde se encuentren los equipos informáticos.

– Hacer una imagen de los discos del equipo para preservar la integridad de los originales y comprobar la integridad de la imagen para asegurarse de que la misma sea exacta.

–Tomar las medidas necesarias para resguardar la información volátil (la contenida en almacenamientos temporales, tales como memoria RAM, memoria caché, etc.).

–Una vez que el equipo o dispositivo se apaga la información contenida en este tipo de almacenamiento se destruye.

–Precintar cada equipo informático en todas sus entradas eléctricas y todas las partes que puedan ser abiertas o removidas.

–Identificar correctamente toda la evidencia. Rotular el hardware con los siguientes datos:

- Para computadoras, notebooks, palms, celulares, etc.: N° del Expediente Judicial, Fecha y Hora, Número de Serie, Fabricante, Modelo.
- Para DVDs, CDs, Diskettes, discos Zip, etc: almacenarlos en conjunto en un sobre antiestático, indicando N° del Expediente Judicial, Tipo (DVDs, CDs, Diskettes, discos Zip, etc.) y Cantidad, marca y nro de serie.

4.2. Objetivo

Mantener la Cadena de Custodia de los elementos probatorios, desde su secuestro hasta la finalización del proceso judicial, a fin de garantizar la autenticidad e integridad de la evidencia.

4.3. Marco Legal

Código Procesal Penal

Art. 208 CPP: "... Los efectos secuestrados serán inventariados y puestos bajo segura custodia, a disposición del tribunal. En caso necesario podrá disponerse el depósito de los mismos." "...Si fuere necesario remover los sellos, se verificará previamente su identidad e integridad. Concluido el acto, aquellos serán repuestos y de todo se dejará constancia. "

Art. 237 CPP: “Tanto el Juez como los peritos procurarán que las cosas a examinar sean en lo posible conservadas, de modo que la pericia pueda repetirse.” [11]

Es imposible atribuir responsabilidades por el faltante de elementos si no se identifica y asegura el material que se envía a peritaje "desde el momento del allanamiento". Estas etiquetas de seguridad evitan fallas en el procedimiento de secuestro/transporte de los elementos probatorios.

4.4. Distribución

Las etiquetas se distribuyen a los Juzgados de Instrucción.

Este material puede ser requerido a la División Suministros como cualquier insumo, con la salvedad de que deberá mantenerse un estricto control en la entrega de las etiquetas por cuestiones de costos y demora en el reaprovisionamiento.

El personal de la División Suministros de la Administración General registrará los números de serie entregados a cada dependencia judicial. Por costos y dificultades en el reaprovisionamiento, las etiquetas de seguridad deberán estar bajo custodia de un funcionario judicial.

4.5. Utilización

Las etiquetas de seguridad deberán ser entregadas al Fiscal o al Oficial actuario de la Policía al momento de expedir una orden de allanamiento (en una cantidad razonable a la magnitud del procedimiento). Se adjuntará al acta de allanamiento una copia de la "Guía operativa para el secuestro de tecnología informática".

Durante el procedimiento judicial, las etiquetas serán colocadas por el Personal Policial en todos aquellos lugares que permitan la apertura de un equipo informático, bloqueando cualquier conector de energía eléctrica o que permita el acceso al dispositivo. El personal policial registrará en el Acta de Allanamiento todos los números de serie de las etiquetas de seguridad utilizadas.

Al finalizar el procedimiento, deberán reintegrarse al Juzgado de Instrucción las etiquetas de seguridad que no hayan sido utilizadas, las que serán resguardadas por el Secretario para usos posteriores.

Una vez que los objetos secuestrados ingresen al Laboratorio Pericial Informático, se realizará una inspección general, dejando constancia de cualquier alteración o ausencia de etiquetas de seguridad.

Finalizado el peritaje, se colocarán nuevas etiquetas de seguridad, detallando los números de serie en el Dictamen y se remitirán los secuestros a la dependencia de origen.

Detalle para el llenado de la Etiqueta de Seguridad

Referencias:

A: Número de Serie: un identificador único e irrepetible que debe registrarse al colocar la etiqueta de seguridad en un dispositivo informático (Acta de Allanamiento, acta elaborada por un Funcionario Judicial del Juzgado o dictamen del Perito).

B: Número de Expediente-Datos del Juzgado o Fiscalía-Carátula.

Opcional: Lugar donde se encuentra el objeto.

C: Código para uso interno del Laboratorio Pericial (NO COMPLETAR).

D: Nombre y Apellido del responsable que colocó la etiqueta de seguridad.

E: Momento en que se realizó el procedimiento judicial. Formato: dd/mm/aaaa

F: Firma del responsable que colocó la etiqueta de seguridad.

g1 y g2: Espacios opcionales para la firma de Testigos.

5.1. EVIDENCIA DIGITAL

5.1.1. Definición

La evidencia digital es todo registro informático almacenado en un dispositivo informático o que se transmite a través de una red informática y que pudiera tener valor probatorio para una investigación. [1]

Se considera evidencia digital a cualquier información que, sujeta a una intervención humana, electrónica, y/o informática, ha sido extraída de cualquier clase de medio tecnológico informático –computadoras, etc.

Técnicamente, es un tipo de evidencia física que está constituida por campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas técnicas especiales. [2]

La importancia de la evidencia digital reside en la necesidad de demostrarle al juez la prueba fehaciente que convierte en responsable al sospechoso. Por eso, es fundamental la correcta selección de la prueba relevante por parte del experto para no ser sobre abundante o superflua. El correcto tratamiento de la evidencia digital es fundamental para que sea admisible: haber sido obtenida respetando las garantías y procedimientos legales, basada en una previa autorización judicial o del director de investigación, justificando su tratamiento en los procedimientos de obtención, preservación, análisis y presentación ante el tribunal, respetando la cadena de custodia, cuyos pasos deberá desprenderse de un manual de buenas prácticas.

Asimismo, deben poder justificarse todos los métodos y acciones realizadas en el tratamiento de la evidencia digital, a través de la demostración de la validación de los métodos utilizados y de los procesos realizados.

También se deberá documentar las acciones realizadas y justificar todas las decisiones en las etapas del proceso, y se deben obtener los mismos resultados en caso de aplicar el mismo procedimiento, pero con herramientas diferentes, en cualquier momento.

La evidencia digital es una denominación usada de manera amplia para describir cualquier registro generado o almacenado en un sistema computacional que puede ser utilizado como prueba en un proceso legal. De acuerdo con el HB: 171 2003 Guidelines for the Managment of IT Evidence, la evidencia digital es cualquier información que, sujeta a una intervención humana u otra semejante, ha sido extraída de un medio

informático. El documento mencionado establece también que la evidencia digital puede dividirse en tres categorías:

- Registros almacenados en el equipo de tecnología informática (por ejemplo, correos electrónicos, archivos de aplicaciones de ofimática, imágenes, etc.).
- Registros generados por los equipos de tecnología informática (registros de auditoría, registros de transacciones, registros de eventos, etc.).
- Registros que parcialmente han sido generados y almacenados en los equipos de tecnología informática. (hojas de cálculo financieras, consultas especializadas en bases de datos vistas parciales de datos, etc.).La evidencia digital es única, cuando se la compara con otras formas de evidencia. A diferencia dela evidencia física, la evidencia digital es frágil y una copia de un documento almacenado en un archivo es idéntica al original. Otro aspecto único es su potencial de realizar copias no autorizadas de archivos, sin dejar rastro alguno. La evidencia digital posee, entre otras, las siguientes características:

    1. **Es volátil**: Si no es preservada adecuadamente puede cambiar o variar con facilidad de forma poco previsible.
    2. **Es duplicable:** Puede ser duplicada de manera exacta y copiada tal como si fuese el original.
    3. **Es alterable y modificable**: Con las herramientas adecuadas es relativamente fácil alterar destruir, alterar o modificar
    4. **Es eliminable:** Con las herramientas adecuadas puede ser eliminada por completo.

  Tales características sugieren la exigente labor requerida por los especialistas cuando tenga que llevarse adelante investigaciones sobre la delincuencia informática, en procedimientos, técnicas y herramientas tecnológicas para obtener, custodiar, revisar, analizar y presentar la evidencia encontrada en la escena del crimen.

5.1.2. Importancia

Increíblemente los delincuentes hoy están utilizando la tecnología para facilitar el cometimiento de infracciones y eludir a las autoridades. Este hecho ha creado la necesidad de que tanto la Policía Judicial, la Fiscalía General del Estado y la Función Judicial deba especializarse y capacitarse en estas nuevas áreas en donde las

TICs[1] se convierten en herramientas necesarias en auxilio de la Justicia y la persecución de delito y el delincuente.

La obtención de Información (elementos de convicción) se constituye en una de las facetas útiles dentro del éxito de en una investigación criminal, aspecto que demanda de los investigadores encargados de la recolección preservación, análisis y presentación de las evidencias digitales una eficaz labor que garantice la autenticidad e integridad de dichas evidencias, a fin de ser utilizadas posteriormente ante el Tribunal Penal.

5.1.3. Objetivo

La prueba dentro del proceso penal es de especial importancia, ya que desde ella se confirma o desvirtúa una hipótesis o afirmación precedente, se llega a la posesión de la verdad material.

De esta manera se confirmará la existencia de la infracción y la responsabilidad de quienes aparecen en un inicio como presuntos responsables, todo esto servirá para que el Tribunal de Justicia alcance el conocimiento necesario y resuelva el asunto sometido a su conocimiento.

El objetivo de la Informática forense es el de recobrar los registros y mensajes de datos existentes dentro de un equipo informático, de tal manera que toda esa información digital, pueda ser usada como prueba ante un tribunal.

5.1.4. Principios Básicos

1. El funcionario de la Fiscalía o de la Policía Judicial nunca debe acudir solo al lugar de los hechos, este tipo de actividad debe ser realizada como mínimo por dos funcionarios. Un segundo funcionario, por un lado, aporta seguridad personal y, por otro, ayuda a captar más detalles del lugar de los hechos. Los funcionarios deberían planear y coordinar sus acciones. Si surgen problemas inesperados, es más fácil resolverlos porque “dos cabezas piensan más que una”.

2. Ninguna acción debe tomarse por parte de la Policía Judicial, la Fiscalía o por sus agentes y funcionarios que cambie o altere la información almacenada dentro de

un sistema informático o medios magnéticos, a fin de que esta sea presentada fehacientemente ante un tribunal.

3. En circunstancias excepcionales una persona competente puede tener acceso a la información original almacenada en el sistema informático objeto de la investigación, siempre que después se explique detalladamente y de manera razonada cual fue la forma en la que se produjo dicho acceso, su justificación y las implicaciones de dichos actos.

4. Se debe llevar una bitácora de todos los procesos adelantados en relación a la evidencia digital. Cuando se hace una revisión de un caso por parte de una tercera parte ajena al mismo, todos los archivos y registros de dicho caso y el proceso aplicado a la evidencia que fue recolectada y preservada, deben permitir a esa parte recrear el resultado obtenido en el primer análisis.

5. El Fiscal del Caso y/o el oficial a cargo de la investigación son responsables de garantizar el cumplimiento de la ley y del apego a estos principios, los cuales se aplican a la posesión y el acceso a la información almacenada en el sistema informático. De igual forma debe asegurar que cualquier persona que acceda a o copie dicha información cumpla con la ley y estos principios.

5.1.5. Reconocimiento de la Evidencia Digital

Es importante clarificar los conceptos y describir la terminología adecuada que nos señale el rol que tiene un sistema informático dentro del "iter criminis" o camino del delito. Esto a fin de encaminar correctamente el tipo de investigación, la obtención de indicios y posteriormente los elementos probatorios necesarios para sostener nuestro caso. Es así que por ejemplo, el procedimiento de una investigación por homicidio que tenga relación con evidencia digital será totalmente distinto al que, se utilice en un fraude informático, por tanto el rol que cumpla el sistema informático determinara DONDE DEBE SER UBICADA Y COMO DEBE SER USADA LA EVIDENCIA.

Ahora bien para este propósito se han creado categorías a fin de hacer una necesaria distinción entre el elemento material de un sistema informático o hardware (evidencia

electrónica) y la información contenida en este (evidencia digital). Esta distinción es útil al momento de diseñar los procedimientos adecuados para tratar cada tipo de evidencia y crear un paralelo entre una escena física del crimen y una digital. En este contexto el hardware se refiere a todos los componentes físicos de un sistema informático, mientras que la información, se refiere a todos los datos, programas almacenados y mensajes de datos trasmitidos usando el sistema informático.

5.2. Descripción de un Sistema Informático.

Un sistema informático es un conjunto de elementos que hace posible el tratamiento automático de la información. En los siguientes cuadros explicamos la Evidencia Digital en relación con un sistema informático.

SISTEMA INFORMÁTICO	
HARDWARE (Elementos Físicos)	**Evidencia Electrónica**
El hardware es mercancía ilegal o fruto del delito.	El hardware es una mercancía ilegal cuando su posesión no está autorizada por la ley. Ejemplo: en el caso de los decodificadores de la señal de televisión por cable, su posesión es una violación a los derechos de propiedad intelectual y también un delito. El hardware es fruto del delito cuando este es obtenido mediante robo, hurto, fraude u otra clase de infracción.
El hardware es un instrumento	Es un instrumento cuando el hardware cumple un papel importante en el cometimiento del delito, podemos decir que es usada como un arma o herramienta, tal como una pistola o un cuchillo. Un ejemplo serían los snifers y otros aparatos especialmente diseñados para capturar el tráfico en la red o interceptar comunicaciones.
El hardware es evidencia	En este caso el hardware no debe ni ser una mercancía ilegal, fruto del delito o un instrumento. Es un elemento físico que se constituye como prueba de la comisión de un delito. Por ejemplo el scanner que se uso para digitalizar una imagen de pornografía infantil, cuyas características únicas son usadas como elementos de convicción

Cuadro 1: El Hardware contiene **evidencia electrónica**.

SISTEMA INFORMÁTICO	
INFORMACIÓN	**Evidencia Digital**
La información es mercancía ilegal o el fruto del delito.	La información es considerada como mercancía ilegal cuando su posesión no está permitida por la ley, por ejemplo en el caso de la pornografía infantil. De otro lado será fruto del delito cuando sea el resultado de la comisión de una infracción, como por ejemplo las copias pirateadas de programas de ordenador, secretos industriales robados.

Cuadro 2: La información es **Evidencia Digital**.

SISTEMA INFORMÁTICO	
INFORMACIÓN	**Evidencia Digital**
La información es un instrumento	La información es un instrumento o herramienta cuando es usada como medio para cometer una infracción penal. Son por ejemplo los programas de ordenador que se utilizan para romper las seguridades de un sistema informático, sirven para romper contraseñas o para brindar acceso no autorizado. En definitiva juegan un importante papel en el cometimiento del delito.
La información es evidencia	Esta es la categoría más grande y nutrida de las anteriores, muchas de nuestras acciones diarias dejan un rastro digital. Uno puede conseguir mucha información como evidencia, por ejemplo la información de los ISP's, de los bancos, y de las proveedoras de servicios las cuales pueden revelar actividades particulares de los sospechosos

Cuadro 3: La información es **Evidencia Digital**

5.2.1. Clases de Equipos Informáticos y Electrónicos

Algunas personas tienden a confundir los términos evidencia digital y evidencia electrónica, dichos términos pueden ser usados indistintamente como sinónimos, sin embargo es necesario distinguir entre aparatos electrónicos como los celulares y PDAs y la información digital que estos contengan. Esto es indispensable ya que el foco de nuestra investigación siempre será la evidencia digital aunque en algunos casos también serán los aparatos electrónicos.

A fin de que los investigadores forenses tengan una idea de dónde buscar evidencia digital, éstos deben identificar las fuentes más comunes de evidencia. Situación que brindará al investigador el método más adecuando para su posterior recolección y preservación.

Las fuentes de evidencia digital pueden ser clasificadas en tres grande grupos:

1. **SISTEMAS DE COMPUTACIÓN ABIERTOS**, son aquellos que están compuestos de las llamadas computadores personales y todos sus periféricos como teclados, ratones y monitores, las computadoras portátiles, y los servidores. Actualmente estos computadores tiene la capacidad de guardar gran cantidad de información dentro de sus discos duros, lo que los convierte en una gran fuente de evidencia digital.

2. **SISTEMAS DE COMUNICACIÓN**, estos están compuestos por las redes de telecomunicaciones, la comunicación inalámbrica y el Internet. Son también una gran fuente de información y de evidencia digital.

3. **SISTEMAS CONVERGENTES DE COMPUTACIÓN**, son los que están formados por los teléfonos celulares llamados inteligentes o SMARTPHONES, los asistentes personales digitales PDAs, las tarjetas inteligentes y cualquier otro aparato electrónico que posea convergencia digital y que puede contener evidencia digital.

Dada la ubicuidad de la evidencia digital es raro el delito que no esté asociado a un mensaje de datos guardado y trasmitido por medios informáticos. Un investigador entrenado puede usar el contenido de ese mensaje de datos para descubrir la conducta de un infractor, puede también hacer un perfil

de su actuación, de sus actividades individuales y relacionarlas con sus víctimas.

5.3. Descripción de Componentes a Peritar.

Detallamos a continuación los distintos tipos de Hardware a tener en cuenta al momento de realizar el peritaje informático.

Identificación de Partes:

- *Computador de escritorio*
- *Computador Portátil*
- *Estación de Trabajo*
- *Hardware de Red*
- *Servidor – aparato que almacena o transfiere datos electrónicos por el Internet*
- *Teléfono celular*
- *Teléfono inalámbrico*
- *Aparato para identificar llamadas*
- *Localizador - beeper*
- *"GPS" – aparato que utiliza tecnología satélite capaz de ubicar geográficamente a la persona o vehículo que lo opera*
- *Cámaras, videos*
- *Sistemas de seguridad*
- *Memoria "flash" – Pequeño dispositivo que puede conservar hasta 4 gigabytes de datos o 4,000,000,000 bytes de información*
- *"Palm" – asistente personal electrónico que almacena datos y posiblemente tiene Conectividad inalámbrica con el Internet*
- *Juegos electrónicos – en su unidad de datos se puede guardar, incluso, una memoria*

De otro aparato

- *Sistemas en vehículos – computadoras obvias y computadoras del sistema operativo*

Del vehículo que registra cambios en el ambiente y el mismo vehículo

- *Impresora*
- *Copiadora*
- *Grabadora*
- *Videograbadora, DVD*
- *Duplicadora de discos*
- *Discos, disquetes, cintas magnéticas*
- *Aparatos ilícitos – tales como los aparatos que capturan el número celular de teléfonos cercanos para después copiarlo en otros teléfonos, o los llamados sniffers, decodificadores, etc.*

5.4. Tratamiento de la Evidencia Digital.

5.4.1. Incautación de Equipos Informáticos o Electrónicos

Si el investigador presume que existe algún tipo evidencia digital en algún aparato electrónico o en algún otro soporte material relacionado con el cometimiento de una infracción. Este debe pedir la correspondiente autorización judicial para incautar dichos elementos, de igual forma debe tener la autorización judicial para acceder al contenido guardado, almacenado y generado por dichos aparatos.

Antes de realizar un allanamiento e incautación de Equipos Informáticos o electrónicos se debe tomar en cuenta lo siguiente:

1. ¿A qué hora debe realizarse?
   - Para minimizar destrucción de equipos, datos
   - El sospechoso tal vez estará en línea
   - Seguridad de investigadores
2. Entrar sin previo aviso
   - Utilizar seguridad
   - Evitar destrucción y alteración de los equipos, o la evidencia contenida en esta.

3. Materiales previamente preparados (Cadena de custodia)

   - Embalajes de papel
   - Etiquetas
   - Discos y disquetes vacíos
   - Herramienta
   - Cámara fotográfica

4. Realizar simultáneamente los allanamientos e incautación en diferentes sitios

   - Datos pueden estar en más de un lugar, sistemas de red, conexiones remotas.

5. Examen de equipos

6. Aparatos no especificados en la orden de allanamiento

7. Creación de Respaldos en el lugar, creación de imágenes de datos

   - Autorización para duplicar, reproducir datos encontrados (por ejemplo, un aparato contestador)

8. Fijar/grabar la escena

   - Cámaras, videos, etiquetas

9. Códigos/claves de acceso/contraseñas

10. Buscar documentos que contienen información de acceso, conexiones en redes, etc.

11. Cualquier otro tipo de consideración especial (consideraciones de la persona involucrada: médicos, abogados, información privilegiada, etc.)

La falta de una orden de allanamiento e incautación que ampare las actuaciones (sobre los equipos y sobre la información) de la Policía Judicial y la Fiscalía puede terminar con la exclusión de los elementos probatorios por violación de las Garantías Constitucionales. Art. 42 de la Constitución.

5.4.2. En la Escena del Delito.

Los Investigadores que llegan primero a una escena del crimen tienen ciertas responsabilidades, las cuales se resumen en los siguientes puntos:

- **OBSERVE Y ESTABLEZCA LOS PARÁMETROS DE LA ESCENA DEL DELITO**: El primero en llegar a la escena, debe establecer si el delito está todavía en progreso, luego tiene que tomar nota de las características físicas del área circundante. Para los investigadores forenses esta etapa debe ser extendida a todo sistema de información y de red que se encuentre dentro de la escena. En estos casos dicho sistema o red pueden ser blancos de un inminente o actual ataque como por ejemplo uno de denegación de servicio (DoS).
- **INICIE LAS MEDIDAS DE SEGURIDAD:** El objetivo principal en toda investigación es la seguridad de los investigadores y de la escena. Si uno observa y establece en una condición insegura dentro de una escena del delito, debe tomar las medidas necesarias para mitigar dicha situación. Se deben tomar las acciones necesarias a fin de evitar riesgos eléctricos, químicos o biológicos, de igual forma cualquier actividad criminal.

  Esto es importante ya que en una ocasión en una investigación de pornografía infantil en Estados Unidos un investigador fue muerto y otro herido durante la revisión de una escena del crimen.

  Siempre se deben tomar las medidas adecuadas para precautelar la vida de las posibles víctimas del delito, el objetivo es brindar el cuidado médico adecuado por el personal de emergencias y el preservar las evidencias.

- **ASEGURE FÍSICAMENTE LA ESCENA:** Esta etapa es crucial durante una investigación, se debe retirar de la escena del delito a todas las personas extrañas a la misma, el objetivo principal es el prevenir el acceso no autorizado de personal a la escena, evitando así la contaminación de la evidencia o su posible alteración.
- **ASEGURE FÍSICAMENTE LAS EVIDENCIAS**: Este paso es muy importante a fin de mantener la cadena de custodia[3] de las evidencias, se debe guardar y etiquetar cada una de ellas. En este caso se aplican los principios y la metodología correspondiente a la recolección de evidencias de una forma práctica. Esta recolección debe ser realizada por personal entrenado en manejar, guardar y etiquetar evidencias.
- **ENTREGAR LA ESCENA DEL DELITO:** Después de que se han cumplido todas las etapas anteriores, la escena puede ser entregada a las autoridades que se harán cargo de la misma. Esta situación será diferente en cada caso, ya que por ejemplo en un caso penal será a la Policía Judicial o al Ministerio Público; en un caso corporativo a los Administradores del Sistema. Lo esencial de esta etapa es verificar que todas

las evidencias del caso se hayan recogido y almacenado de forma correcta, y que los sistemas y redes comprometidos pueden volver a su normal operación.

- **ELABORAR LA DOCUMENTACION DE LA EXPLOTACIÓN DE LA ESCENA:** Es Indispensable para los investigadores documentar cada una de las etapas de este proceso, a fin de tener una completa bitácora de los hechos sucedidos durante la explotación de la escena del delito, las evidencias encontradas y su posible relación con los sospechosos. Un investigador puede encontrar buenas referencias sobre los hechos ocurridos en las notas recopiladas en la explotación de la escena del Delito.

5.4.3. Reconstrucción de la Escena del Delito.

La reconstrucción del delito permite al investigador forense comprender todos los hechos relacionados con el cometimiento de una infracción, usando para ello las evidencias disponibles. Los indicios que son utilizados en la reproducción del Delito permiten al investigador realizar tres formas de reconstrucción a saber:

- **Reconstrucción Relacional**, se hace en base a indicios que muestran la correspondencia que tiene un objeto en la escena del delito y su relación con los otros objetos presentes. Se busca su interacción en conjunto o entre cada uno de ellos.
- **Reconstrucción Funcional**, se hace señalando la función de cada objeto dentro de la escena y la forma en que estos trabajan y como son usados.
- **Reconstrucción Temporal**, se hace con indicios que nos ubican en la línea temporal del cometimiento de la infracción y en relación con las evidencias encontradas.

5.4.4. Qué hacer al encontrar un dispositivo informático o electrónico

1. No tome los objetos sin guantes de hule, podría alterar, encubrir o hacer desaparecer las huellas dactilares existentes en el equipo o en el área donde se encuentra residiendo el sistema informático.
2. Asegure el lugar.
3. Asegure los equipos. De cualquier tipo de intervención física o electrónica hecha por extraños.

4. Si no está encendido, no lo encienda (para evitar el inicio de cualquier tipo de programa de autoprotección.
5. Verifique si es posible el Sistema Operativo a fin de iniciar la secuencia de apagado a fin de evitar pérdida de información.
6. Si usted cree razonablemente que el equipo informático o electrónico está destruyendo la evidencia, debe desconectarlo inmediatamente.
7. Si está encendido, no lo apague inmediatamente (para evitar la pérdida de información "volátil") .
8. SI ES POSIBLE, LLAME UN TÉCNICO.

Cuando no hay técnico:

1. No use el equipo informático que está siendo investigado, ni intente buscar evidencias sin el entrenamiento adecuado.
2. Si está encendido, no lo apague inmediatamente.
3. Si tiene un "Mouse", muévalo cada minuto para no permitir que la pantalla se cierre o se bloqueé.
4. Si una Computadora Portátil (Laptop, notebook) no se apaga cuando es removido el cable de alimentación, localice y remueva la batería, esta generalmente se encuentra debajo del equipo, y tiene un botón para liberar la batería del equipo. Una vez que está es removida debe guardarse en un lugar seguro y no dentro de la misma máquina, a fin de prevenir un encendido accidental.
5. Si el aparato está conectado a una red, anote los números de conexión, (números IP).
6. Fotografíe la pantalla, las conexiones y cables.
7. Usar bolsas especiales antiestática para almacenar diskettes, discos rígidos, y otros dispositivos de almacenamiento informáticos que sean electromagnéticos (si no se cuenta, pueden utilizarse bolsas de papel madera). Evitar el uso de bolsas plásticas, ya que pueden causar una descarga de electricidad estática que puede destruir los datos.
8. Coloque etiquetas en los cables para facilitar la reconexión posteriormente.
9. Anote la información de los menús y los archivos activos (sin utilizar el teclado)

Cualquier movimiento del teclado puede borrar información importante.

10. Si hay un disco, un disquete, una cinta, un CD u otro medio de grabación en alguna unidad de disco o grabación, retírelo, protéjalo y guárdelo en un contenedor de papel.
11. Bloqueé toda unidad de grabación con una cinta, un disco o un disquete vacío aportado por el investigador (NO DEL LUGAR DE LOS HECHOS). Al utilizar algún elemento del lugar del allanamiento o de los hechos, se contamina un elemento materia de prueba con otro.
12. Selle cada entrada o puerto de información con cinta de evidencia.
13. De igual manera selle los tornillos del sistema a fin de que no se puedan remover o reemplazar las piezas internas del mismo.
14. Desconecte la fuente de poder.
15. Quite las baterías y almacénela de forma separada el equipo(si funciona a base de baterías o es una computadora portátil).
16. Mantenga el sistema y medios de grabación separados de cualquier tipo de imán, o campo magnético.
17. Al llevar aparatos, anote todo número de identificación, mantenga siempre la CADENA DE CUSTODIA.
18. Lleve todo cable, accesorio, conexión.
19. Lleve, si es posible, manuales, documentación, anotaciones.
20. Tenga en cuenta que es posible que existen otros datos importantes en sistemas periféricos, si el aparato fue conectado a una red, por tanto desconecte el cable de poder de todo hardware de Red (Router, modem, Swich, Hub).

Si el equipo es una estación de trabajo o un Servidor (conectado en red) o está en un negocio, el desconectarla puede acarrear (SIEMPRE CONSULTE A UN TÉCNICO EXPERTO EN REDES):

- Daño permanente al equipo.
- Responsabilidad Civil para la Policía Judicial y la Fiscalía General del Estado.
- Interrupción ilegal del giro del negocio.

5.5. Otros Dispositivos Electrónicos.

5.5.1. Teléfonos Inalámbricos, Celulares, Smartfones, Cámaras Digitales

Se puede encontrar evidencia potencial contenida en los teléfonos inalámbricos tal como:

- Números llamados.
- Números guardados en la memoria y en el marcado rápido.
- Identificador de llamadas, llamadas entrantes.
- Otra información guardada en la memoria del teléfono.
- Números marcados.
- Nombres y direcciones.
- Números personales de Identificación (PIN).
- Número de acceso al correo de voz.
- Contraseña del correo de voz.
- Números de tarjetas de crédito.
- Números de llamadas hechas con tarjeta.
- Información de acceso al Internet y al correo electrónico.
- Se puede encontrar valiosa información en la pantalla del aparato.
- Imágenes. Fotos, grabaciones de voz.
- Información guardada en las tarjetas de expansión de memoria.

REGLA DEL ENCENDIDO “ON” Y APAGADO “OFF”

1. Si el aparato está encendido "ON", no lo apague "OFF".
    - Si lo apaga "OFF" puede iniciarse el bloqueo del aparato.
    - Transcriba toda la información de la pantalla del aparato y de ser posible tómele una fotografía.
    - Vigile la batería del aparato, el transporte del mismo puede hacer que se descargue. Tenga a mano un cargador.
    - Selle todas las entradas y salidas.
    - Selle todos los puntos de conexión o de admisión de tarjetas o dispositivos de memoria.
    - Selle los tornillos para evitar que se puedan retirar o reemplazar piezas internas.
    - Buscar y asegurar el conector eléctrico.

- Colocar en una bolsa de FARADAY, (especial para aislar de emisiones electromagnéticas), si no hubiere disponible, en un recipiente vacío de pintura con su respectiva tapa.
- Revise los dispositivos de almacenamiento removibles. (Algunos aparatos contienen en su interior dispositivos de almacenamiento removibles tales como tarjetas SD, Compact flash, Tarjetas XD, Memory Stick, etc.)

2. Si el aparato está apagado "OFF", déjelo apagado "OFF".

- Prenderlo puede alterar evidencia al igual que en las computadoras.
- Antes del análisis del aparato consiga un técnico capacitado en el mismo.
- Si no existe un técnico use otro teléfono.
- Es necesario que el investigador busque el manual del usuario relacionado con el aparato encontrado.

5.5.2. Aparatos de mensajería instantánea, beepers

Se puede encontrar evidencia potencial contenida en los teléfonos inalámbricos tal como:

1. Beepers Numéricos (reciben solo números y sirven para transmitir números y códigos)

2. Beepers Alfanuméricos (reciben números y letras, pueden cargar mensajes completos en texto)

3. Beepers de Voz (pueden transmitir la voz y también caracteres alfanuméricos)

4. Beepers de dos vías (contienen mensajes de entrada y salida)

5. Buenas Prácticas

- Una vez que el beeper está alejado del sospechoso, este debe ser apagado. Si se mantiene encendido los mensajes recibidos, sin tener una

orden judicial para ello puede implicar una interceptación no autorizada de comunicaciones.

6. Cuando se debe buscar en el contenido del aparato.

   - Cuando es la causa de la aprehensión del sospechoso.
   - Cuando haya presunción del cometimiento de un delito Flagrante.
   - Con el consentimiento del dueño o receptor de los mensajes.

5.5.3. Máquinas de Fax

1. En las máquinas de fax podemos encontrar:

- Listas de marcado rápido.
- Fax guardados (transmitidos o recibidos)
- Bitácoras de transmisión del Fax (transmitidos o recibidos)
- Línea del Encabezado
- Fijación de la Hora y Fecha de la transmisión del Fax

2. Buenas Prácticas

- Si la máquina de fax es encontrada prendida "ON", el apagarla causaría la perdida de la memoria de último número marcados así como de los facsímiles guardados.

3. Otras consideraciones

- Busque la concordancia entre el número de teléfono asignado a la máquina de fax y la línea de teléfono a la que está conectada.
- De igual forma busque que el encabezado del mensaje y el número impreso coincidan con el del usuario y la línea telefónica.
- Es necesario que el investigador busque el manual del usuario relacionado con el aparato encontrado.

5.5.4. Dispositivos de Almacenamientos.

Los dispositivos de almacenamiento son usados para guardar mensajes de datos e información de los aparatos electrónicos. Existen dispositivos de almacenamiento de tres clases, a saber: dispositivo magnético (como discos duros o los disquetes), dispositivos de estado sólido o memoria solida (como las memorias flash y dispositivos USB) y los dispositivos ópticos (como los discos compactos y DVD).

Existen gran cantidad de Memorias USB en el mercado y otros dispositivos de almacenamiento como tarjetas SD, Compact flash, Tarjetas XD, Memory Stick, etc.

BUENAS PRÁCTICAS

- Recolecte las instrucciones de uso, los manuales y las notas de cada uno de los dispositivos encontrados.
- Documente todos los pasos al revisar y recolectar los dispositivos de almacenamiento.
- Aleje a los dispositivos de almacenamiento de cualquier magneto, radio trasmisores y otros dispositivos potencialmente dañinos.

6. ACTAS

6.1. Conceptualización

Para definir lo que es un acta pericial debemos explicar algunos conceptos básicos contenidos en dicha definición. [1]

6.1.1. Prueba

La prueba es aquella que tiene como medio demostrar la existencia o no de un hecho **delictivo**.

6.1.2. Objeto

Es aquello susceptible de ser probado, aquello sobre lo que debe o puede recaer la prueba.

6.1.3. Medios de Prueba

Es el procedimiento a través del cual, se ingresa un **elemento de prueba** en el proceso, establecido por la ley.

Medios de Prueba

6.1.4. Elemento de Prueba

Es el **dato objetivo** que se incorpora legalmente al proceso, capaz de producir un conocimiento cierto o probable a cerca de los extremos de la imputación delictiva (objetivo, legal, pertinente y relevante).

6.1.5. Órgano o Sujeto de la Prueba

Sujeto que aporta un **elemento** de prueba y lo transmite al proceso (accidental o encargo judicial). Ej.: Testigo, perito.

6.1.6. Objeto de la Prueba

Aquello susceptible de ser probado, sobre lo que recae la prueba. Lo que se puede o debe probar (No los notorios ni evidentes). Ej.: Lo que se quiere probar.

6.1.7. Valoración de la Prueba

La sana crítica es el método de apreciación de la prueba, donde **el juez** la valorará de acuerdo a la lógica, las máximas de la experiencia y los conocimientos científicamente afianzados.

6.2. Acta

6.2.1. Definición [2]

- Es uno de los medio de prueba más eficiente, a través de cual se ingresa elementos probatorios en determinado tiempo, lugar y modo.
- Relación escrita que hace el funcionario público, encargado de documentar los actos, que se cumplen en su presencia. Son instrumentos públicos.

6.2.2. Marco Legal

Código Procesal Penal de la Nación:

Capitulo IV: Actas

Art. 138.- Cuando el funcionario público que intervenga en el proceso deba dar fe de los actos realizados por él o cumplidos en su presencia, labrará un acta en la forma prescrita por las disposiciones de este Capítulo. A tal efecto, el juez y el fiscal serán asistidos por un secretario, y los funcionarios de policía o fuerzas de seguridad por dos testigos, que en ningún caso podrán pertenecer a la repartición cuando se trate de las actas que acrediten los actos irreproducibles y definitivos, tales como el secuestro, inspecciones oculares, requisa personal.

Art. 139.- Las actas deberán contener La fecha- el nombre y apellido de las personas que intervengan; el motivo que haya impedido, en su caso, la intervención de las personas obligadas a asistir; la indicación de las diligencias realizadas y de su resultado; las declaraciones recibidas; si éstas fueron hechas espontáneamente o a requerimiento; si las dictaron los declarantes.

Concluida o suspendida la diligencia, el acta será firmada, previa lectura, por todos los intervinientes que deban hacerlo. Cuando alguno no pudiere o no quisiere firmar, se hará mención de ello.

Si tuviere que firmar un ciego o un analfabeto, se le informará que el acta puede ser leída y, en su caso, suscrita por una persona de su confianza, lo que se hará constar.

6.2.3. Acta de Procedimiento

Es el instrumento público que da fe de lo sucedido y el relato valedero del que se nutren los distintos tribunales que intervienen en la causa para tener por acreditados los hechos que en ella se describen.[3]

6.2.4. Contenido de un Acta

Un Acta debe Tener: [2]

- **Claridad**: Entendible.
- **Precisión**: Sin divagaciones, determinando las partes principales del suceso.
- **Circunstanciado**: De tiempo, modo, lugar y personas.
- **Especificidad**: En caso de pluralidad de hechos, relato de cada uno por separado.

Sobre la base de:

- **Tiempo**: Día y hora y lo más ajustado posible en fechas tope; precisar cada uno de los momentos que sean mencionados en el relato.
- **Lugar**: Espacio físico, de cada uno de los mencionados.
- **Modo**: Mecánica o desarrollo del hecho y elementos intervinientes, con aquellas particularidades que puedan agrandar o atenuar un delito.
- **Personas**: Aquellas que produjeron el hecho delictivo y las que concomitantemente o posteriormente tuvieron relación con el hecho o rol dentro del acto.

6.2.5. Formato de un Acta [2]

En la .....de ....., a los .....días del mes de ..... del año dos mil....., siendo las ..... horas aproximadamente, el ...., en presencia del testigo hábil del acto Señor/a ..... D.N.I N° ..... con domicilio en calle ..... de la ....., en el marco de la causa identificada como ...., con conocimiento e intervención de .....; a los fines legales que corresponda SE HACE CONSTAR: Que en fecha y hora señalada, ...

6.2.6. Cierre de un Acta

Que es todo cuanto hay que hacer constar, con lo que se da por finalizado el acto, previa lectura y ratificación de todo su contenido, firmando los mencionados.-

7. BUENAS PRÁCTICAS.ESTANDARES INTERNACIONALES.

7.1. Marco de Trabajo (Frameworks)-Propuesta

Respecto al Marco de Trabajo que podemos utilizar en el peritaje informático forense, se entiende a aquellos métodos a aplicar o normas a seguir ya fueran éstas del tipo reglamentadas (por Instituciones u Organizaciones conformadas o constituidas con el objetivo de elaborar y dictar las mismas), establezcan estándares, o constituyan “manuales” o “guías” de buenas prácticas, para llevar adelante los pasos o cubrir las etapas para el análisis forense y llegar al dictamen o informe libre de errores. Todo ello contribuirá a consolidar a lo que se considera “un buen profesional”.

A continuación, se enuncian los métodos de investigación utilizados durante la propuesta.

Existen varias metodologías para el análisis forense propuesto por algunos autores como:

- **Modelo según la Norma UNE 71506:2013, de AENOR.**[1]
- Modelo según Francisco Lázaro Domínguez en su libro introducción a la Informática Forense.[2]
- **Modelo según el NIST, en su "Special Publication 800-86".**[3]
- Modelo según DFRWS (2001), en su informe técnico que lleva por título "A Road Map for Digital Forensic Research".[4]
- Modelo según IDIP (2003), propuesto por Carrier y Spafford.[5]
- **Conjunto de Normas ISO/IEC basadas o con "pivot" sobre la Nº 27037 (27035, 27037, 27041, 27042, 27043, 27050).**[6]
- **RFC 3227,** Directrices para la identificación, recolección, adquisición y preservación de evidencia digital.[7]

Todas estas metodologías tienen sus fases bien diferenciadas reflejando en cada una de ellas los mismos principios básicos. Por ello cualquiera de estas metodologías es aplicable a un análisis forense, sin embargo, se podría escoger entre una de ellas dependiendo de las necesidades que se requiera, ya que algunas tienden a ser muy generales y otras más específicas.

Referencias:

AENOR: Asociación Española de Normalización y Certificación

NIST: Instituto Nacional de Normas y Tecnología

DFRWS: Taller Digital de Investigación Forense

IDIP: Proceso de Investigación Digital Integrado.

ISO/IEC: International Organization for Standardization / International Electrotechnical Commission.

RFC/IETF: Request for Comments/Internet Engineering Task Force.

Para el desarrollo del presente marco de trabajo, se decidió implementar la siguiente metodología, respecto a manejo de evidencias digitales, no obstante, será complementado con la normativa vigente para garantizar la admisibilidad en los tribunales y no ser vulnerable a una objeción de descalificación; La Fig. 1 ilustra la metodología propuesta en este trabajo.

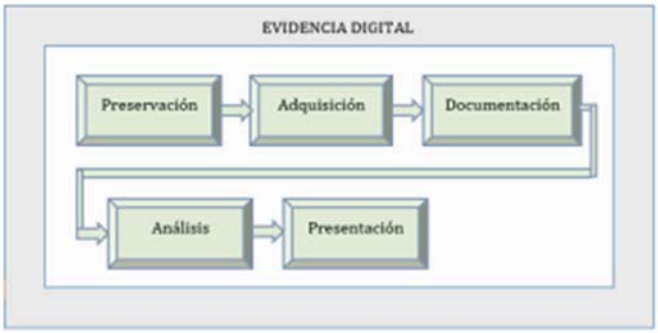


Fig. 1. Metodología propuesta

A continuación, se detallan las distintas fases.

1. FASE DE PRESERVACIÓN

En esta fase la prioridad es asegurar la integridad de la evidencia original en la escena del delito, es decir, no se debe realizar modificaciones, alteraciones o destrucción sobre dicha evidencia.

Para lo cual se elaboraron sub-fases enmarcadas en la escena del delito como se ilustra en la Fig. 2.

Fig. 2. Sub-fases de la Fase de Preservación.

a. Sub-fase de reconocimiento

Los Peritos Informáticos realizarán las respectivas diligencias de reconocimiento del lugar de los hechos en territorio digital, servicios digitales, medios o equipos tecnológicos, preservando en todo momento la escena del delito para evitar que se realicen modificaciones o destrucciones de la evidencia digital existente.

b. Sub-fase de autorización

Antes de iniciar su experticia y encontrar información relacionada con el caso, los Peritos Informáticos deberán obtener una autorización por escrito por parte de la autoridad competente o las partes procesales, ya que en ciertos casos se debe romper claves de seguridad o investigar sobre archivos personales.

Sin esta autorización, el análisis no tendría una validez legal y de hecho, se estaría cometiendo un delito sobre la violación a la intimidad, además que la alteración o destrucción de vestigios de evidencias materiales u otros elementos de prueba, serán sancionadas según los códigos procesales ya estudiados.

c. Sub-fase de identificación

Los Peritos Informáticos efectuarán la identificación sobre 2 tipos de evidencia digital:

• **Evidencia electrónica.** - Comúnmente será todo elemento material de un sistema informático o hardware, este último refiriéndose a todos los componentes físicos que lo integra.

• **Evidencia digital.** - Es toda la información obtenida en un sistema informático como puede ser datos, programas almacenados y mensajes transmitidos para su posterior análisis y puedan ser presentadas como evidencias.

Es crucial efectuar este análisis, ya que de esto dependerá que los procedimientos se realicen de manera adecuada para cada tipo de evidencia, a fin de encaminar correctamente el análisis forense.

Es importante mencionar además que el marco de trabajo propuesto se enmarca en la evidencia digital proporcionando al Perito Informático los métodos más adecuados para su posterior recolección y almacenamiento.

En esta sub-fase de identificación es necesario mencionar algunas consideraciones o reglas para que la evidencia sea admisible.

1) Llevar indumentaria adecuada para evitar descargas electrostáticas.

2) Evitar contaminarla con software que no garantice un proceso limpio.

3) Alejar a todas las personas no autorizadas de la escena.

4) Mantener el estado de los dispositivos si están encendidos, no apagarlo y viceversa.

5) Identificar los equipos afectados, que pueden ser equipos informáticos o a su vez dispositivos de almacenamiento.

6) Realizar una evaluación de las herramientas de software, hardware y procedimientos que se van a utilizar sobre el equipo afectado a analizar.

7) Asegurar que todo el proceso que se realice en esta sub-fase debe ser claramente documentado.

Como recomendación final se debe tomar todas las precauciones necesarias para minimizar la posibilidad de contaminar de la evidencia accidentalmente.

2. FASE DE ADQUISICIÓN

Según la metodología propuesta se debe realizar en esta fase de adquisición un clonado a bajo nivel de los datos originales del soporte de almacenamiento de datos, para lo cual se tomará de guía el **RFC 3227** (Directrices para la recopilación de evidencias y su almacenamiento), son directrices que contienen las mejores prácticas relacionado durante la recolección de evidencia y su almacenamiento.

Por lo mencionado anteriormente se elaboraron sub-fases enmarcadas en la evidencia original como se ilustra en la Fig. 3.

Fig.3 Sub Fase de la Fase de Adquisición

a. Sub-fase de recopilación

El primer paso es verificar el estado del equipo, si este se encuentra encendido o apagado, debido a que los procedimientos de recopilación serán diferentes para mantener la integridad de la evidencia original.

Es importante determinar el escenario del equipo:

• Equipo apagado

No encender el equipo, siempre debe estar apagado, ya que, si se enciende, se puede alterar la evidencia.

Por norma, no se debe trabajar con la evidencia original del soporte de almacenamiento de datos sino con una copia a bajo nivel del mismo comúnmente llamado imagen forense; para realizar la copia se debe utilizar medios forenses estériles, empleando para ello herramientas de software especial que asegure que la evidencia no sea contaminada.

Cuando se realiza una imagen completa del soporte de almacenamiento de datos, ésta incluye todas las particiones, los espacios de disco duro sin utilizar entre las mismas, el sector de arranque e incluso zonas reservadas como HPA y la DCO, toda esta información será útil para analizar el contenido de los mismos y otras tareas de investigación, detallando lo mencionado en la Fase de análisis.

Existen procedimientos tanto de software como de hardware que permiten la adquisición de una imagen forense.

• *Procedimiento por Software*: las herramientas que se muestran en la **Tabla I** se han convertido principalmente en un estándar de referencia en el campo de la Informática Forense.

TABLA I

HERRAMIENTAS DE SOFTWARE PARA ADQUISICIÓN DE LA IMAGEN FORENSE

	Herramienta	Distribución	Independientemente del Software
	EnCASE	Propietario	
	F-RESPONSE	Propietario	que se utilice es recomendable
Herramientas para soporte de Almacenamiento de Datos	FORENSETOOLKIT(FTK)	Propietario	
	HELIX	Libre	utilizar el Bloqueador de escritura
	DEFF(DIGITAL FORENSIC FRAMEWORK)	Libre	como por ejemplo TABLEAU ULTRABLOCK
	DEFT(DIGITAL EVIDENCE & FORENSIC TOOLKIT)	Libre	FIREWIRE KIT, forzando a que el soporte
	DCDD3	Libre	
	GUYMAGER	Libre	de almacenamiento de datos funcione solo
	LINRES	Libre	
	(AIR) AUTOMATED IMAGE AND RESTORE	Libre	en modo de lectura y no de escritura

HPA: Área protegida del anfitrión.

DCO: Superposición de la configuración de datos.

• *Procedimiento por Hardware*: existen dispositivos dedicados a la copia completa del soporte de almacenamiento de datos, como los que se muestran en la **Tabla II**.

TABLA II

HERRAMIENTAS DE SOFTWARE PARA ADQUISICIÓN DE LA IMAGEN FORENSE		
	Herramienta	Descripción
Herramientas de HARDWARE	TABLEAU T8u USB 3.0	Ideal para Prevenir escritura sobre aquellos dispositivos de almacenamiento
	FORENSE BRIDGE KIT	
	FORENSE ULTRADOCK V5	
	WIEBETECH MEDIA	
	WRITEBLOKER	
	WIEBETECH FORENSIC	
	ULTRADOCK	
	WIEBETECH DITTO	
	FORENSIC FIELDSTATION	
	PARABEN MOBILE FIELD	

Una vez obtenida la imagen forense se debe proceder a calcular el Hash de la información extraída. El Hash son algoritmos de cifrado que realiza una operación matemática sobre el conjunto de datos de cualquier longitud y su salida es un número hexadecimal de 32 dígitos, básicamente la salida es una huella digital única para cada conjunto de datos cifrado.

NIST publicó la versión final del algoritmo de Hash SHA-3 siendo una herramienta de última generación para asegurar la integridad de la información.

El procedimiento habitual consiste en hacer en primer lugar un Hash del soporte de almacenamiento de datos original donde se encuentra la evidencia original. Acto seguido se obtiene otro Hash de la imagen forense extraída. Es importante mencionar que los dos Hashes deben ser iguales.

Es importante que acompañe al Perito en este proceso de recopilación otra persona, que actúe como testigo de las acciones realizadas, de preferencia una autoridad competente.

Una regla importante es documentar toda la información sobre el soporte de almacenamiento de datos o si este se encuentra alojado en un equipo, números de serie, hora de inicio y de fin de cada uno de los procedimientos que se realicen, etc., de preferencia siempre es recomendable tomar una fotografía de lo mencionado anteriormente.

Si se realizaron los procedimientos mencionados anteriormente de manera adecuada se garantizará la integridad de la evidencia y no podrá ser objetada o descartada como medio probatorio.

• Equipo encendido

Es importante que la recopilación de la evidencia se realice siguiendo el orden de mayor a menor volatilidad de la información.

El orden de volatilidad se enmarca al período de tiempo donde cierta información es accesible, es por eso que se debe hacer la recopilación de la información que va a estar durante un tiempo menor, es decir cuya volatilidad sea mayor.

Se establecerá el siguiente orden de volatilidad según lo establecido en el **RFC 3227** al momento de realizar la recolección de evidencias;

- Registros y contenidos de la caché.
- Contenidos de la memoria.
- Estado de las conexiones de red, tablas de rutas.
- Estado de los procesos en ejecución.
- Contenido del sistema de archivos y de los discos duros.
- Contenido de otros dispositivos de almacenamiento.

Se tomará como prioridad los 4 primeros puntos, ya que si por algún error involuntario se reinicia o se apaga el equipo podría modificarse o perder toda la información.

De igual manera es de vital importancia recuperar información del sistema en tiempo real como:

- Fecha y hora.
- Procesos activos.
- Conexiones de red.
- Puertos TCP/UDP abiertos.
- Usuarios conectados remota y localmente.

Por lo mencionado anteriormente se listan algunas recomendaciones que se podrían tomar en cuenta si el equipo se encuentra encendido:

- Si lo apaga, se puede bloquear el equipo por alguna contraseña.
- Sellar todas las entradas y salidas del equipo.
- Sellar todos los puntos de conexión o de admisión de tarjetas o dispositivos de memoria.
- Sellar todos los tornillos del equipo para evitar que se puedan reemplazar o retirar piezas internas.
- Revisar los dispositivos de almacenamiento removibles. (Algunos equipos contienen en su interior dispositivos de almacenamiento removibles tales como tarjetasSD, Compactflash, TarjetasXD, MemoryStick, etc.).

Es importante mencionar que no se debe apagar el equipo, ya que se puede perder conectados remota y localmente, procesos que se estén ejecutando, sistema de archivo, etc., siendo muy difícil de volver a reunir toda esta información, si se decide apagar el equipo.

El atacante puede dejar instalando herramientas o scripts que podrían modificar, sustituir y eliminar archivos; sin embargo, en el peor de los casos puede ser que el atacante siga on-line y detecte nuestra presencia y actué con una acción evasiva o, peor aún, destructiva eliminando todo tipo de información.

Si la información es gravemente comprometida por la severidad del ataque, el equipo debe ser apagado sin dudarlo. Se puede perder información volátil de la memoria RAM, micro, etc., pero se conservará la mayor cantidad posible de información y que podrá ser de utilidad para posterior análisis sobe el ataque.

En este punto es donde se debe proceder a recopilar toda la información volátil del sistema para lo cual se podría emplear un script en Perl para sistemas UNIX/Linux o un archivo de proceso por lotes para sistemas Windows para que realice el proceso de copiado de forma automatizada.

Otra opción es emplear herramientas de trasmisión de datos por la red tipo “netcat” o “dc3dd”, “dcfldd” o “FTK Imager”, enviando la información a una portátil conectada en la misma red o a su vez directamente a la portátil conectada directamente con el equipo afectado.

Una vez obtenida la imagen forense se debe proceder a calcular el Hash de la información extraída.

Si estamos manipulando dispositivos móviles debemos tener precaución de que no entren en contacto con redes inalámbricas, evitando manipular los datos contenidos dentro de ellos. Por consiguiente, se debe poner el dispositivo en “modo avión”, de esta forma se evita que se pueda conectar a las redes celulares e inalámbricas.

La imagen forense del dispositivo móvil puede obtenerse por medio de una herramienta de software con “dd” y “netcat” o a su vez se puede utilizar kits forenses como el Cellebrite UFED, un excelente kit especializado en el análisis de dispositivos móviles.

Si se realizó los procedimientos mencionados anteriormente de forma adecuada se garantizará que la recolección de la evidencia se efectuó de manera transparente e integra.

b. Sub-fase de almacenamiento

Una vez obtenida la imagen forense, es fundamental definir métodos adecuados para el almacenamiento y etiquetado de las evidencias. Este proceso es comúnmente llamado “CADENA DE CUSTODIA”.

Para la elaboración de estos métodos se tomará de guía estándares para el manejo y almacenamiento de la evidencia digital como son: el **RFC 3227, ISO 27370**, Modelo Extendido de Séamus Ó Ciardhuain.

El Perito Informático deberá aplicar la respectiva cadena de custodia a elementos físicos o contenido digital materia de prueba, garantizando la autenticidad, acreditando su identidad y estado original.

Sin embargo, hay que tener claro que la cadena de custodia inicia en el lugar donde se obtiene o encuentra el elemento de prueba.

Para poder iniciar con el proceso de cadena de custodia se debe contar con la presencia de la autoridad competente.

La cadena de custodia debe realizarse de la siguiente manera:

1) Manejo del lugar de los hechos

El área debe ser aislada y acordonada, toda actividad debe ser claramente documentada.

Se debe realizar una eficaz investigación en la búsqueda de elementos materia de prueba o evidencias físicas.

2) Fijación del lugar de los hechos

Se debe realizar actividades que permitan la descripción detallada del lugar de los hechos y la localización de los elementos materia de prueba o evidencias utilizando técnicas establecidas que pueden ser fotografías, videos, imágenes, embalaje y rotulado entre otros.

3) Recolección de la evidencia

Este punto es crucial ya que se debe analizar el estado del equipo, aplicando las herramientas tanto de software como hardware se obtendrá la imagen forense según el orden de volatilidad.

4) Embalaje y rotulado de las evidencias

Registrar fotográficamente los equipos y sus conexiones antes de su embalaje, durante el embalaje y al finalizar el embalaje y rotulado. Para el sellado de los equipos se debe realizar con la cinta adecuada que brinden seguridad y preservación del mismo, para soportes de almacenamiento de datos se deben introducir en bolsas antiestáticas y posterior a ello ponerla en una caja de cartón o sobre “manila” cuyo interior se pueda rellenar con plásticos con films o bolsas de polietileno con burbujas de aire u otro material protector, siempre en lo posible, del

tipo antiestático. Previamente se debe confeccionar e imprimir un documento que contenga mínimamente datos representativos del dispositivo contenido, ID/Número, marca, modelo, número de serie y demás datos representativos y/o identificatorios, como también cualquier marca u rasgo característico que sea distintivo o particular. Luego, éste documento sebe ser completado con las firmas correspondientes y colocado sobre el contenedor en la parte de su cierre y sobre esta adhiera cinta de sello/cinta de seguridad, cintas o etiquetas o "fajas de seguridad" del tipo "void". Dependiendo del contenedor y el objeto, puede ser conveniente y recomendable guardar copia en interior de caja, sobre u otro contenedor. Rotular de manera consecutiva cada uno de los elementos a ser incautados relacionados con la evidencia.

5) Transporte de la evidencia

Toda evidencia, así como los elementos incautados, debe ser transportada al laboratorio forense respectivo. La cadena de custodia se debe mantener meticulosamente durante el transporte.

6) Abrir el embalaje de la evidencia

El embalaje sólo podrá ser abierto por el Perito Informático para su estudio o análisis.

Si se realizaron y se documentaron correctamente los procedimientos mencionados anteriormente se garantiza la integridad, conservación e inalterabilidad de la evidencia.

3. FASE DE DOCUMENTACIÓN

En esta Fase el Perito Informático debe tener todas las consideraciones mínimas para redactar el informe pericial, de tal manera que todas las actividades realizadas desde la Fase de Preservación hasta la Fase de Análisis queden plasmadas en el documento.

El Informe Pericial obligatoriamente debe ser presentado y subido al Sistema Informático Pericial, en archivo tipo PDF; el mismo que pueda ser descargado, conocido, estudiado por las y los interesados. Sus explicaciones o aclaraciones, se presentarán de forma verbal y/o escrita, de conformidad con la normativa procesal correspondiente.

El Informe Pericial traslada el conocimiento experto al proceso judicial, estableciendo para ello requisitos mínimos que no solo estandaricen la presentación, sino que exista un formato general, siendo claro y entendible para las autoridades competentes.

Los requisitos obligatorios de todo informe pericial son los siguientes:

1) Datos generales del juicio, o proceso de indagación previa.

El Informe Pericial deberá contener los datos del juicio y la identificación del perito como requisito que tiene por objeto la determinación de la responsabilidad en caso de incumplimiento de obligaciones.

2) Parte de antecedentes.

En este punto se debe delimitar claramente el encargo realizado, esto significa, se tiene que especificar el tema sobre el que informará en base a lo ordenado por la autoridad competente y/o lo solicitado por las partes procesales. Cabe recalcar que es la guía que limita la intervención pericial, con la prohibición de efectuar juicios de valor.

3) Parte de consideraciones técnicas o metodología a aplicarse.

Este punto es de suma relevancia ya que el Perito debe explicar claramente, cómo aplico sus conocimientos especializados de su profesión al caso. Deberá relacionar los contenidos de sus conocimientos y experticia con el objeto de la pericia encargada.

4) Parte de conclusiones.

Es el fruto del conocimiento del Perito, es lo que idealmente servirá de fundamento para la decisión judicial. Después de las consideraciones técnicas las conclusiones que se redactarán en el informe serán claras, directas y solamente se referirán a los temas materia de la pericia debidamente delimitados y explicados en los antecedentes. Debe ser lo suficientemente clara y concisa para que pueda ser entendido por toda persona no especialista en el área del perito, pero concreta y correcta para que no pueda ser observada ni objetada por parte alguna.

5) Documentos de respaldo, anexos, o explicación de criterio técnico.

El Perito deberá sustentar sus conclusiones ya sea con documentos y objetos de respaldo (fotos, láminas demostrativas, copias certificadas de documentos, grabaciones de audio y video, etc.).
El Perito claramente debe exponer y justificar desde todo punto de vista las razones especializadas para llegar a la conclusión correspondiente incluidas en el informe.

6) Otros requisitos.

El Perito podrá incluir requisitos adicionales a los establecidos por el reglamento siempre y cuando la ley procesal correspondiente determine la inclusión de estos.

7) Información adicional.

A más de las obligaciones mínimas mencionadas anteriormente el Perito podrá incluir también en el informe cualquier otro tipo de información adicional siempre y cuando se encuentren dentro de los límites del objeto de la pericia, y que sirvan de soporte y fundamento de la práctica pericial y sus conclusiones.

8) Declaración juramentada.

El Perito deberá declarar bajo juramento que toda la información que ha proporcionado es auténtica, al igual que el informe es independiente y corresponde a su real convicción profesional.

9) Firma y rúbrica

Al finalizar el Informe Pericial deberá constar con la siguiente información: la firma y rúbrica del Perito, el número de cédula de ciudadanía, y el número de su calificación y acreditación pericial.

4. FASE DE ANÁLISIS

Una vez que la imagen forense fue recopilada, almacenada y documentando correctamente todo el proceso. Comienza la fase de Análisis, en donde el Perito Informático mediante un examen detallado pondrá todos sus conocimientos en la búsqueda de vestigios de lo que se quiere encontrar.

El objetivo del análisis se enfoca principalmente en:

- **Realizar la reconstrucción de la línea de tiempo**, es decir, determinar la evolución de los hechos desde el instante anterior al inicio del ataque, hasta el momento de su descubrimiento.
- **Llevar a cabo un examen detallado** de los sistemas de archivos, detectar archivos sospechosos, realizar operaciones de búsqueda de caracteres, búsqueda de archivos específicos, recuperación de información y ejecutar otras tareas de investigación.

Esta fase es de vital importancia y laboriosa, ya que por medio de la evidencia digital y del análisis que se realice aplicando procedimientos, herramientas y técnicas, se llegará a responder las interrogantes de quién, cómo, cuándo, y donde sucedieron los hechos.

Por lo mencionado anteriormente se elaboraron sub-fases. Teniendo en cuenta que el análisis únicamente lo debe realizar en el Laboratorio Forense como se ilustra en la **Fig. 4**.

Fig. 4 Sub-Fases de la Fase de Análisis

a. Análisis de una imagen forense

Antes de realizar un análisis se debe seguir una metodología basada en niveles de funcionamiento, muy similar al modelo de capas OSI de redes de informática.

Permitiendo recolectar información en cada nivel como se ilustra en la **Fig. 5**.

Este es un enfoque propuesto por Brian Carrier en su publicación "Investigación Forense de Sistemas de Archivos", puede ser aplicado para cualquier sistema de archivos y tecnología de soporte de datos.

Para el análisis es importante la reconstrucción de la línea de tiempo y esto se logra recopilando información a través de la extracción lógica.

Este tipo de información es la que llevará más tiempo recopilar, pero actualmente existen muchas herramientas como por ejemplo The Sleuth Kit de distribución Libre, permitiendo que el análisis sea mucho más detallado y fácil de interpretar.

La idea es encontrar información eliminada en rutas poco comunes y que es desapercibida por una persona común.

Fig.5.Niveles de Análisis de una imagen forense.

1) Recuperación de archivos eliminados

La recuperación de archivos se puede realizar con una técnica denominada redireccionamiento, la cual permite introducir la salida de un comando como entrada de otro. Esta técnica está disponible en todos los Sistemas Operativos basados en línea de comando, como, por ejemplo, Unix/Linux, MS-Windows y Mac OSX. Con lo cual garantizamos que el archivo generado contiene los mismos datos que el original.

2) Firmas características

¿Es posible saber de qué tipo es un archivo recuperado?

Sí, basta con examinar la firma característica del archivo mediante un editor hexadecimal, por ejemplo, HxD, con lo cual se determinará el tipo de archivo y si en este no se utilizaron técnicas de ocultación.

3) Documentos.

Los documentos de texto encontrados en el transcurso de una investigación pueden ser:
Open Office (OOXML), Open Document, Documentos RTF, Archivos Microsoft Office.
Estos documentos tienen mucha importancia e interés no solo por su contenido sino porque alojan otro tipo de información en su interior. Toda esta información es llamada metadatos.

4) Archivos gráficos

Las imágenes encontradas en el transcurso de una investigación pueden ser: GIF, PNG, TIFF, Archivos JPEG, contienen metadatos que pueden ser útiles al momento de recopilar información como: fecha y hora de cuando se tomó, modelo de la cámara y coordenadas geográficas (este último en dispositivos móviles equipados con cámara y GPS)

5) Multimedia

Los archivos multimedia encontrados en el transcurso de una investigación pueden ser:
MPEG-1, WMV, MPEG-3 (MP3), ACC/M4A, contienen metadatos como: dimensiones de la imagen, caudal de datos en video y audio, etc.

6) Archivos ejecutables

Este tipo de archivos constituyen un caso especial, ya que al momento de analizar los metadatos se debe evitar que se ejecuten intencionalmente dañando con esto el sistema, para lo cual es recomendable trabajar en un entorno seguro que puede ser un sandbox, una máquina virtual o una plataforma aislada de hardware.

7) Data carving

Data carving es el proceso de volver a ensamblar o "rearmar" archivos de computadora a partir de fragmentos en ausencia de metadatos del sistema de archivos.

La mayor parte de archivos antiguos se habrán perdido, debido a que el soporte de almacenamiento de datos se ha formateado o se sobrescribieron con nuevos archivos, pero gracias al data carving se puede recuperar estos archivos antiguos.

b. Análisis de sistema operativo Microsoft Windows

Cuando el equipo a investigar contenga un Sistema Operativo Microsoft Windows es imprescindible recopilar toda la información posible en tiempo real (cuando el equipo este encendido).

1) Fecha y hora del sistema

Es importante obtener la fecha y hora del sistema para poder comenzar a elaborar una buena línea de tiempo.

En una consola de comandos (cmd) de Windows se procede a teclear el siguiente comando:

- time
- date

2) Conexiones de red abiertas

En ocasiones suele suceder que los atacantes aún están conectados al equipo a investigar por medio de equipos remotos, esto se puede comprobar de la siguiente manera.

El siguiente comando:

- netstat –n

Obteniendo información relacionada a conexiones que el sistema mantiene abiertas, indicando direcciones IP tanto locales como remotas, con lo cual se sabrá si alguien está accediendo al sistema desde una IP sospechosa.

3) Puertos TCP o UDP abiertos

El siguiente comando:

- netstat –n

Obtiene información de todos los puertos abiertos y si estos están en estado LISTENING (esperando por una conexión), ESTABLISH (conexión establecida) y CLOSE_WAIT / TIME WAIT (Cerrada).

4) Usuarios conectados al sistema

Se puede obtener información de si existen usuarios conectados al sistema, si están accediendo a recursos compartidos o realizando tareas de otro tipo.
Para ello se debe utilizar PSLoggedOn, perteneciente a la suite de herramientas PsTools.

5) Tabla de enrutamiento interna
El siguiente comando:
• netstat –rn
Obteniendo información de ruta sobre redes remotas y conectadas directamente, con se podría conocer si el atacante está desviando el tráfico de red para evadir cortafuegos o IDS.

6) Procesos en ejecución
Si además de los procesos normales del sistema y aplicaciones del usuario, existe algún otro proceso dejado por el atacante que pudiera ser sospechoso se debe utilizar Pslist, perteneciente a la suite de herramientas PsTools.
PsList muestra un listado de procesos junto con sus números PID incluso a detectar procesos que han sido creados con el mismo nombre de procesos legítimos del sistema.
7) Archivos abiertos
PsFile perteneciente a la suite de herramientas PsTools, muestra una lista de todos los archivos del sistema que han sido abiertos de forma remota.

8) Papelera de reciclaje
Cuando alguien borra un archivo ya sea de forma accidental o intencionada estos se envían a la papelera de reciclaje y se genera un archivo llamado INFO2, el cual es invisible y no se muestra en un listado de directorio normal. Este archivo registra las rutas completas de los archivos que han sido eliminados.
El siguiente comando:
• dir/a
Permite analizar directamente el contenido de este archivo.
Existen herramientas que permiten la visualización con una interfaz gráfica para el análisis y la interpretación, por ejemplo: Mount Image Pro, Flu y Rifiuti.

9) Historial de Internet
En la actualidad los ordenadores ya no se utilizan solo para tareas estáticas como: redactar informes, llevar contabilidad o solo como entornos de programación. Ahora con las telecomunicaciones, la Web, el acceso universal a Internet y conexiones de banda ancha, los

usuarios emplean sus ordenadores para navegar por varias páginas en Internet y realizar diferentes tipos de actividad.

Los navegadores Web, como por ejemplo Internet Explorer, Firefox, Chrome, Opera o Safari conservan por defecto las páginas web que se visitan. Por consiguiente, el lugar más aconsejable para iniciar una investigación es en el historial del navegador.

• Microsoft Internet Explorer: el archivo a analizar es index.dat, que contiene el historial de navegación con las páginas visitadas y otros elementos de interés. El archivo index.dat es de tipo binario pero su contenido puede ser examinado con la herramienta Pasco.

• Mozilla/Firefox: Es importante mencionar que este navegador guarda toda su información en bases de datos SQLite. El archivo a analizar se llama profiles.ini el cual contiene archivos como: formhistory.sqlite, downloads.sqlite, cookies.sqlite y place.sqlite con toda la información sobre los historiales de navegación.

• Chrome: Al igual que Firefox, este navegador utiliza base de datos SQLite para poder organizar los datos que se generan por la actividad del usuario, siendo el archivo a analizar place.sqlite.

10) Correo electrónico

Otro de los objetivos del análisis forense es investigar el correo electrónico almacenado localmente en el equipo a través de un cliente de correo electrónico ya sea Outlook, Eudora, Opera Mail, Mozilla Thunderbird o cualquier otro tipo mediante protocolos POP3 o IMAP.

Los elementos de Outlook ya sean mensajes de correo electrónico, el calendario y demás elementos se conservan en un archivo de tipo .pst y .ost. Herramientas como PST- Viewer permiten analizar estos archivos.

Sin embargo, si es un cliente de correo basado en código libre el archivo a analizar es: .mbx o .mbox que fácilmente pueden ser interpretados por un editor de texto.

11) Búsqueda de caracteres

El objetivo consiste en localizar texto revelador de las actividades delictivas llevadas a cabo por un sospechoso. Actualmente existen herramientas que emplean funciones para rastrear los sectores de un disco a bajo nivel en busca de cadena de caracteres. WinHex permite realizar búsqueda por cadenas tanto de texto como de código hexadecimal.

12) Metadatos

Los metadatos de modo simplificado son datos que hacen referencia a otros datos constituyendo otra fuente de información de gran valor para el investigador forense.

Cuando el usuario crea o edita documentos de cualquier tipo, como: MS-Office, imágenes, Audio, etc., automáticamente está produciendo información sobre su actividad en el sistema. FOCA es una herramienta útil ya que permite localizar metadatos en documentos de diversos formatos.

13) Registro de Windows

El análisis al Registro de Windows constituye un amplio campo para la investigación forense no solo por la gran cantidad de información almacenada, sino también por el tipo de información que se puede obtener analizando este Registro como: conocer si el sospechoso conecto un dispositivo USB, si se instaló algún tipo de aplicación, los últimos archivos abiertos, si el sistema está contaminado por algún tipo de malware; constituyendo así esta información en elementos de evidencia el cual puede lograrse con el comando:

• regedit.exe

Sin embargo, si el ordenador está apagado también puede obtener esta información con la herramienta Windows Registry Recovery de la empresa Mitec.

c. Análisis de sistema operativo Unix/Linux

En la actualidad un conocimiento sobre los sistemas Unix /Linux le va a permitir al investigador forense:

• Montar su estación de trabajo sin las cuantiosas inversiones que requiere un software comercial.

• Lograr Beneficios a nivel operativo que puede ser: realización de imágenes in situ, técnicas de recuperación de archivos eliminados mediante técnicas de data carving (proceso de volver a ensamblar archivos de computadora a partir de fragmentos en ausencia de metadatos del sistema de archivos), etc.

• Ofrecer nuevas oportunidades para el aprendizaje de la profesión por medio de: tecnología, herramientas, recursos y abundante documentación.

• Por lo mencionado anteriormente el conocimiento de Linux resulta imprescindible para moverse en números ámbitos de la investigación forense actual.

1) Montaje automático de particiones

Para comenzar el análisis forense, existen una amplia gama de distribuciones en la página web www.distrowatch.com y se puede elegir la más apropiada.

Es importante mencionar sobre el journaling (registro de transacciones diarias, registro de actividades por día, registro de "auditoría"), y lo que repercutiría en la integridad de la evidencia y la conservación de la cadena de custodia sino se toma las debidas precauciones al respecto.

Un sistema de journaling ("auditoría de transacciones u operaciones") funciona a base de archivos auxiliares que registra de manera provisional el estado de una transacción ejecutada por el sistema de archivos (abrir, copiar, modificar o borrar un archivo). En otras palabras, el montaje automático de una partición con journaling modifica datos, con lo cual el hash de un soporte de almacenamiento de datos montado con posterioridad a su adquisición forense no volverá a coincidir con el de la imagen realizada originalmente.

Para evitar este inconveniente del montaje automático de particiones con journaling, (NTFS, ext3, ReiserFS)

• Al realizar una copia a bajo nivel deben realizarse a través de bloqueadores de escritura.

• Desactivar udev, HAL, d-messagesbus en los scripts del arranque o inicio de Linux.

2) Marca de tiempo

Por medio de una marca de tiempo se puede determinar de qué manera un archivo ha sido manipulado en un ordenador a ser investigado.

La información que se puede obtener es: archivos escritos por última vez, si el archivo fue leído o ejecutado y si el archivo sufrió cambio en los metadatos de su "inode", esto en Linux. Para el estudio de las marcas de tiempo debe hacerse desde una perspectiva crítica que no afecte a la integridad de la evidencia.

3) Información volátil

Para proceder con el análisis de un equipo en funcionamiento con sistema Linux se debe tener en cuenta:

• Fecha y hora del sistema

Esta información puede marcar un preciso límite para diferenciar entre manipulaciones realizadas por el sospechoso y de las que posteriormente se deriven en el análisis.

• Puertos y conexiones abiertas

Existe la posibilidad de que el sistema esté infectado por un rootkit (software -o conjunto de- que permite un acceso de privilegio/"con derechos", a un equipo o dispositivo informático) cuando el sospechoso accedió al equipo de forma remota.

Posterior a ello se puede emplear una serie de comandos como se ilustra en la **Tabla III** para examinar las conexiones abiertas verificando si existe alguna dirección IP sospechosa. Para los

cual se recomienda utilizar programas compilados estáticamente desde un CD en lugar de herramientas locales del sistema.

TABLA III

HERRAMIENTAS DE SOFTWARE PARA ADQUISICIÓN DE LA IMAGEN FORENSE	
Comando	**Descripción**
ipconfig -a	Conecciones de red activas
netstat –anp	tabla de enrutamiento del Kernel
netstat -m	
lsof	archivos abiertos por procesos en ejecución

• Procesos en ejecución

Al momento de obtener la lista de procesos es importante tener mucho cuidado con los procesos parásitos ya que tienen la mala costumbre de camuflarse bajo los nombres de otros legítimos para confundir al investigador.

4) Adquisición forense

Una vez que ya se adquirió la información volátil, se procede a apagar el equipo, pero no ejecutando el comando “shutdown” (“apagar equipo”) sino por el método tradicional en las investigaciones forenses cortando directamente el suministro de corriente del equipo.

Posterior a ello se puede emplear herramientas para realizar la adquisición de la imagen forense.

5) Línea de tiempo

TSK (The Sleuth Kit) está compuesto por un conjunto de herramientas que funcionan en línea de comando, en la actualidad TSK se encuentra incluido en todas las distribuciones Linux especializadas en seguridad informática, por ejemplo, el comando “fls” permite la elaboración de una línea de tiempo a partir de la imagen forense mostrando un listado de archivos con sus marcas de tiempo.

6) Recuperación de archivos eliminados

Para obtener una lista de archivos eliminados en un directorio se puede recurrir a "fls" de TSK, posteriormente a ello se utiliza el comando "icat" para recuperar el archivo eliminado con el mismo grado de funcionalidad y las mismas características.
Con el comando file identifica el tipo de archivo y para examinar el contenido el comando "strings".

7) Otras herramientas
Chrootkit y Rkhunter son scripts que utilizan comandos como "strings" o "grep" para localizar cadenas de texto sospechosas.

d. Análisis de dispositivos móviles

Es importante como en la actualidad y con el pasar de los años los dispositivos móviles se han convertido en el diario vivir de las personas.
El mercado de dispositivos parece estar en una etapa estandarizada de marcas reducidas como: Apple iOS, Android, Windows Mobile y BlackBerry. Todo apunta a un crecimiento exponencial con el pasar de los años ofreciendo ventajas significativas, así como también muchos retos para la informática forense.
El análisis forense en dispositivos móviles no solo implica un examen detallado de la información que sea relevante y que pueda estar almacena, escondida y cifrada, sino también implica el uso de técnicas y procedimientos para la adquisición y análisis de la información; con una base amplia de conocimientos sobre las plataformas y herramientas.

1) Información obtenible
El investigador forense sin problemas puede rescatar información de la SIM, una lista de contactos, registro de llamadas, algunos SMS y un poco más en un teléfono móvil antiguo. Con el pasar del tiempo el teléfono móvil amplió sus capacidades y una infinidad de posibilidades toda esta evolución de mejoras le facilitaron llegar a lo que es en la actualidad un smartphone.
Un smartphone almacena gran cantidad de información, por ejemplo: información referente a aplicaciones, historial de navegación web, Logs y archivos de registro.
Esta información es el resultado de una exploración lógica por medio de un backup convencional del smartphone por medio del software de sincronización. Pero el investigador puede ir un poco más profundo en la exploración de información menos accesible con técnicas especiales.

2) Análisis de dispositivos Apple iOS

Para mantener la integridad de la evidencia el análisis del dispositivo se realizará por medio de niveles algo similar al estudio de las redes informáticas.

• Primer nivel: la extracción manual o visualización directa de los datos, para lo cual se debe tomar fotografías de toda la pantalla y de todas las operaciones realizadas.

• Segundo nivel: Se realizará lo siguiente poner el dispositivo en modo avión para evitar que se conecte a redes celulares e inalámbricas, luego proteger el dispositivo en una jaula de Faraday que no permita un borrado remoto, finalmente se procede a la adquisición lógica con el software de sincronización o aplicaciones de transferencia de archivos desarrolladas por terceros.

Para la adquisición lógica este proceso suele ser automático, pero se debe tener ciertas consideraciones para evitar la destrucción accidental de la evidencia si no se tiene en cuenta: el estado de las aplicaciones, mensajes de advertencia, descargar nuevas versiones del iTunes, sincronización de aplicaciones y otros parámetros de ajuste, caso contrario iTunes dejará intacto las copias de respaldo que hay en el dispositivo para realizar un nuevo backup.

La adquisición física para un dispositivo iPhone u otras versiones del software iOS se utilizará herramientas de terceros que son: Oxygen Forensics, XRY, Lantern, Paraben

Device Seizure o EnCase Neutrino.

Existe la posibilidad de utilizar dispositivos hardware como Cellebrite UFED (Universal Forensics Extraction Device).

• Tercer nivel: En este nivel de extracción física es mucho más exigente y sofisticado

ya que consiste en la realización de una imagen forense del dispositivo. El procedimiento desarrollado por Jonathan Zdziarski, antiguo investigador de McAfee, requiere herramientas que deben ser descargadas de la página web de Zdziarski permitiendo transferir al iPhone un agente de software capaz de crear y transferir la imagen forense al ordenador del investigador.

• Niveles superiores: Son niveles con procedimientos muy costosos en recursos económicos y tiempo en donde se deben aplicar técnicas que únicamente están al alcance de técnicos especializados, por ejemplo en microelectrónica.

3) Dispositivos Android

El investigador forense primeramente deberá realizar una imagen forense a aquellos dispositivos móviles que disponen de un slot para tarjetas microSD o SD.

La extracción se lo realiza en base a procedimientos y herramientas mencionados anteriormente.

De igual manera se procede a la adquisición lógica con el ordenador del investigador, un cable y el software de sincronización que en este caso es Samsung Kies Pc, un software gratuito y descargable del Internet, dando comienzo con el proceso de adquisición de la información.

En la adquisición física para un dispositivo Android se debe tener en cuenta que el dispositivo móvil este en depuración USB para que funcione como un soporte de almacenamiento de datos. El "rooting" en dispositivos móviles Android consiste en proporcionar privilegios al directorio raíz (/) de un dispositivo móvil.

Hay que tener en cuenta que el momento de lograr hacer "rooting" al dispositivo no implicará una sobreescritura de la partición del sistema y que variará del modelo y versión del sistema operativo del dispositivo móvil. Una vez conseguido lo anterior se podrá realizar una imagen forense.

Posterior a ello se deben tener algunas consideraciones:

a) Realizar la imagen forense a cada uno de estos archivos mtd3 (archivos del sistema operativo) y mtd5 (datos del usuario).

b) Disponer en el slot del dispositivo una tarjeta completamente vacía y con espacio suficiente para realizar la extracción de la imagen forense.

Finalmente, para el análisis de la tarjeta microSD o SD se puede utilizar las utilidades que proporciona la herramienta de TSK.

4) Otros dispositivos

En el caso de que algún dispositivo móvil antiguo llegue a las manos del investigador es posible aplicar un método general de trabajo con buenas prácticas, guías de procedimiento y normas internacionales orientadas a la identificación, recolección, adquisición y preservación de evidencia digital con particulares referencias a dispositivos móviles NIST 800-101.

"Cualquier cambio debería ser analizado en profundidad para determinar si se trata de archivos del sistema operativo o bien son archivos de usuario con el objeto de intentar determinar la razón de dichos cambios".

De la misma manera el Perito Informático debe aplicar los conocimientos especializados y tener presente los aportes de otras guías de mejores prácticas y de procedimiento a nivel internacional, (ACPO & 7SAFE), (SWGDE -1).

5) Privacidad

Los castigos pueden ser severos cuando no se realiza una adecuada investigación forense en dispositivos móviles. Ya que en el momento de la audiencia se pueden oír argumentos de este tipo: ¿y quién le dio permiso para poder espiar la información personal de mi cliente? con el propósito de anular los informes periciales de que se inicie nuevamente el proceso de indagación e incluso con privación de libertad, sobre la violación a la intimidad.

5. FASE DE PRESENTACIÓN

Con esta fase culmina el marco de trabajo propuesto, cuyo resultado es la obtención del informe final pericial resultante de todo el procedimiento llevado en cada una de las fases anteriores.

Se podría decir que es el desenlace de la investigación realizada remitiendo el informe al solicitante de la pericia.

El informe final pericial debe ser redactado con un lenguaje compresible para un público no técnico explicando las razones por las cuales se ha llegado a tal o cual conclusión.

El Perito Informático no pondrá juicios de valor en el informe.

El Perito deberá sustentar oralmente los resultados del peritaje como una de sus obligaciones tanto en procesos Penales y Civiles, respondiendo al interrogatorio y al contrainterrogatorio de los sujetos procesales.

La defensa oral tiene por objeto la ratificación, aclaración o ampliación de la pericia ya que sin ella las conclusiones del examen pericial, carecerán de valor y no hará parte de la prueba que deba ser valorada por el juez.

La inasistencia injustificada del Perito a defender su informe, será considerada como falta gravísima perdiendo su acreditación e incluso pudiendo ser llevado a la audiencia mediante el uso de la fuerza pública.

El Perito tendrá la capacidad técnica y profesional de manejar y defender su informe presentado, sin desviarse de su especialidad y del objeto mismo de la pericia, para así no caer en contradicciones, falsedades o juicios de valor, explicando, detallando y defendiendo su experticia.

Existen algunas habilidades y destrezas que todo Perito debe exponer en audiencias que son:

• Forma de vestir adecuada al contexto lo cual denotara respeto a los sujetos procesales y la profesión de quien expone.

• Revisar otras experticias en el caso de haberlas.

• Mantener una actitud respetuosa y cordial al otro profesional que discrepa con nuestro criterio es señal de madurez psicológica y solvencia profesional.

• Utilizar un lenguaje claro y comprensible en la defensa de la audiencia.

• Responder las preguntas con calma y tranquilidad, siempre teniendo coherencia por lo escrito en el informe y lo expuesto oralmente.

• Recordar que cuando escuche la palabra “Objeción” por parte de uno de los abogados, deberá esperar a que únicamente el juez le indique si debe responder o no.

• El interrogatorio directo es el que realiza la parte que introdujo al perito al proceso.

Para lo cual el Perito deberá acreditar su experiencia y exponer los fundamentos de los resultados de su pericia.

• Se pueden realizar preguntas y presentar pruebas no anunciadas oportunamente orientadas a determinar su parcialidad y no idoneidad, a desvirtuar el rigor técnico o científico de sus conclusiones, así como impugnar su credibilidad.

• No caer en la trampa con las estrategias de desacreditación de la contraparte en el contrainterrogatorio al Perito.

• Los Peritos podrán responder las preguntas del interrogatorio de las partes por cualquier medio y acompañar sus informes mediante ilustraciones gráficas.

• Si hay informes periciales divergentes, el juez dispondrá un debate entre los peritos concluido este se abrirá un interrogatorio y contrainterrogatorio de las partes hacia el Perito para aclarar los puntos en controversia.

De la misma manera en esta fase serán devueltos todos los elementos que fueron incautados como parte de la investigación, dando por finalizado así el caso asignado al Perito Informático.

CONCLUSIONES

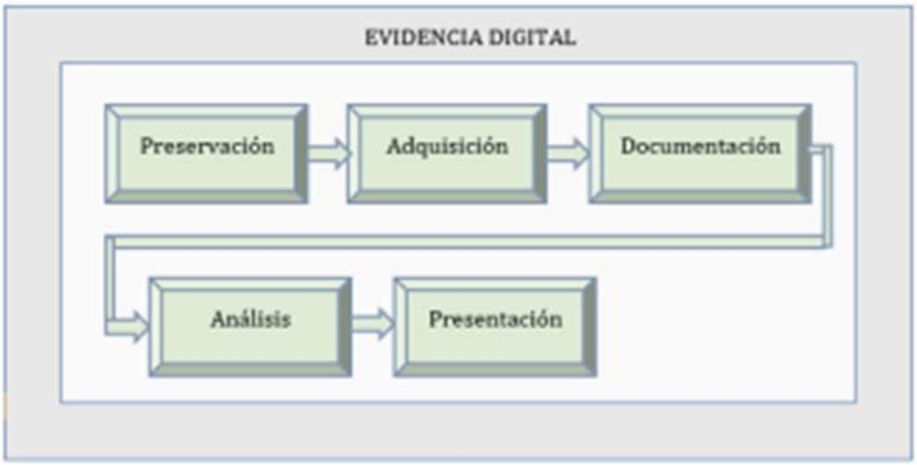
Se ha elaborado o propuesto un marco de trabajo estandarizado para el análisis forense de la evidencia digital en equipos informáticos y dispositivos móviles tomando como puntos importantes las acciones más relevantes de las buenas prácticas, normas y estándares internacionales para que los “Peritos Informáticos” acreditados tomen en cuenta al momento de realizar una investigación forense.

El contar con un marco de trabajo estandarizado garantizará la admisibilidad de la evidencia de manera contundente en un procedimiento Penal o Civil.

Los delitos informáticos que se cometen o cometan con el uso de tecnología para violentar la integridad, confidencialidad y disponibilidad de los datos personales tienen o tendrán la oportunidad de ser sancionados, pero, para ello, y a modo de soporte o apoyo en la toma de decisiones (dictámenes judiciales y aplicación de sanciones) a las organizaciones y personas responsables de la administración y aplicación de la justicia (jueces, fiscales, investigadores oficiales, fuerzas policiales, etc.), es preciso desarrollar y establecer mecanismos para el análisis forense, permitiendo que estas se desarrollen dentro de marcos regulados y controlados.

La metodología propuesta por las Normas UNE 71505/71506:2013, considero, conforman un marco confiable y una alternativa a tener en cuenta para realizar un Análisis Forense (“Pericia”) como “Perito de Parte” / “perito de Control”, pues son normas bastante completas para el manejo o gestión (en cada una de sus etapas) de evidencias digitales.

No obstante, y dependiendo del caso que eventualmente le sea propuesto al perito, será de gran importancia también tener en cuenta otras normas arriba mencionadas como por ejemplo las ISO y la RFC 3227, como así también, tantas otras las cuales apoyadas con la normativa vigente sirven para garantizar la admisibilidad en los tribunales y no ser vulnerable a una objeción de descalificación.



Norma Propuesta en este Trabajo de Buenas Prácticas para la Informática Forense

Bibliografía/Referencias/Cibergrafía:

Capítulo 1:

[1]Real Academia Española. (2001). Informática. En Diccionario de la lengua española (22.a ed.). Recuperado de http://lema.rae.es/drae/?val=inform%C3%A1tica

[2] [3] Art. 183 -Art.327. Código Procesal Civil y Comercial de la Nación http://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/16547/texact.htm#5

[4] INTRODUCCIÓN A LA INFORMÁTICA FORENSE. Dr. Santiago Acurio Del Pino, Director Nacional de Tecnologías de la Información de la Fiscalía General del Estado. 2009

[5] definiciones.de/delito: Significado

[6] delitosinformaticos.info. Definición. Características.

[6] https://www.codejobs.com/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo

[7] Cano José, Jeimy. (2005). Evidencia Digital: Conceptos y Retos. Bogotá: Legis.

[8] Alice, Naranjo. (2009). Conceptos de la auditoria de sistemas. Argentina: El Cid Editor.

[9] Rivas, Gonzalo Alonso. (1988). Auditoría Informática. España: Ediciones Díaz de Santos S.A

[10] https://es.wikipedia.org/wiki/Seguridad

[11] Álvarez Marañón, Gonzalo & Pérez García, Pedro Pablo. (2004). Seguridad informática para empresas y particulares. España: Editorial McGraw-Hill.

[12]http://jlrivas.webs.uvigo.es/downloads/publicaciones/Analisis%20forense%20de%20sistemas%20informaticos.pdf

[13] https://es.wikipedia.org/wiki/C%C3%B3mputo_forense

http://www.neuquen.gov.ar/seguridadinformatica/pdf/Informatica%20Forense%20-%20Hernan%20Herrera.pdf – Hernán Herrera – Sebastián Gómez

Bendinelli, Maximiliano. MP 1883 - MN 5608 (2012). Evidencia digital: la informática forense crece como aliada de los procesos judiciales.

[14] Sergio Martínez-Perito Informático Oficial-Poder Judicial de Córdoba- División Criminalística – Villa María – Córdoba-Entrevista 5-10-2018 Tribunales Villa María

Arnedo Blanco Pedro (2014) - Herramientas de Análisis Forense y su Aplicabilidad en la investigación de Delitos Informáticos

https://www.iprofesional.com/notas/139289-Evidencia-digital-la-informatica-forense-crece-%20como-aliada-de-los-procesos-judiciales

http://www.egov.ufsc.br/portal/conteudo/publica%C3%A7%C3%A3o-inform%C3%A1tica-jur%C3%ADdica-e-direito-eletr%C3%B4nico

[15] Pablo Rodríguez Romeo Ingeniero. MP 49452. MN 5117. Perito informático forense

Alberto Uez. Profesional Informático matricula Nº 442 otorgada por el Consejo Profesional de Ciencias Informática de la Provincia de Córdoba. Perito Oficial de los Juzgados Federales de Córdoba.

Capítulo 2:

Cellebrite – Sitio Web Oficial

https://www.cellebrite.com

https://www.cellebrite.com/es/plataformas-es/

https://www.cellebrite.com/es/laboratorio/

MSAB - Micro Systemation AB – Sitio Web Oficial

https://www.msab.com

https://www.msab.com/es/productos/

https://www.msab.com/es/productos/msab-platforms/

Decision Group Inc. – Sitio Web Oficial

http://www.edecision4u.com

http://www.edecision4u.com/PRODUCTS.html

Tableau Hardware (Guidance Software / OpenText) – Sitio Oficial

https://www.guidancesoftware.com/tableau

https://www.guidancesoftware.com/

ACE (Advanced Computer Engineers) / ACE Laboratory – Sitio Oficial

https://www.acelaboratory.com/d

https://www.acelaboratory.com/catalog/

MediaClone Inc. – Sitio Oficial

http://www.media-clone.net

https://www.media-clone.net/Digital-Forensics-Imaging-Investigation-Platform-s/1477.htm

Sumuri – Sitio Web Oficial

https://sumuri.com/

https://sumuri.com/product-category/hardware/

Forensic Store

https://forensicstore.com/

https://forensicstore.com/all-products/

Avatu

https://www.avatu.co.uk/

https://www.avatu.co.uk/security-and-digital-Forensics-technologies/digital-forensics

ACME Portable Machines - Digital Forensics

http://acmeportable.com.tw

http://acmeportable.com.tw/digital-forensics

RF Electronics - Sitio Web Oficial

https://rfelectronics.net/

https://rfelectronics.net/1-rf-shield-box

Passware - Sitio Web Oficial

https://www.passware.com

https://www.passware.com/kit-forensic/

Digital Intelligence - Sitio Web Oficial

https://digitalintelligence.com/

https://digitalintelligence.com/products/

Oxygen Forensic - Sitio Web Oficial

https://www.oxygen-forensic.com/en/

IEEE *Xplore* Digital Library

Improving Performance in Digital Forensics: A Case Using Pattern Matching Board

https://ieeexplore.ieee.org/document/5066601

High speed search for large-scale digital forensic investigation

https://www.semanticscholar.org/paper/High-speed-search-for-large-scale-digital-forensic-Jee-Lee/e2c4f984286eb20b2031db6bd2d0bda32990128a?tab=citations

Improving Performance in Digital Forensics: A Case Using Pattern Matching Board

https://www.semanticscholar.org/paper/Improving-Performance-in-Digital-Forensics%3A-A-Case-Lee-Un/5b827a90106edfb8a0bad1065089da49b22bd586

Computer Forensic Laboratory: Aims, Functionalities, Hardware and Software

https://www.researchgate.net/publication/268458795_Computer_Forensic_Laboratory_Aims_Functionalities_Hardware_and_Software

Performance Comparison of AccessData's®

Forensic Toolkit®

and Guidance Software's EnCase®

Forensic software.

https://es.scribd.com/doc/205720878/ftkversusencase

Hardware Para Forense Digital

Alonso Eduardo Caballero Quezada

http://www.reydes.com/d/?q=Hardware_para_Forense_Digital

Metodología de Análisis Forense Informático

ADACSI_Ardita_Analisis_Forense_Informaticov2.pdf

Herramienta de Apoyo para el Análisis Forense de Computadoras

Proyecto Fin de Carrera

José Arquillo Cruz

Guía actualizada para futuros peritos informáticos. Últimas herramientas de análisis forense digital. Caso práctico

Jorge Navarro Clérigues

Trabajo Fin de Grado

http://www.pensamientopenal.com.ar/system/files/2016/05/doctrina43429.pdf

[EIF] Estudio de Informática Forense - Sitio Web Oficial - http://www.presman.com.ar/

Proveedor en Argentina de Marcas como:

Guidance Software – Magnet Forensics – Decisión Compiters Group Inc. – Paraben Forensics – Media Clone.

[GDP] Ing. Gustavo Daniel Presman MCP – EnCE – CCE – EnCI - ACE

Especialista certificado internacionalmente en técnicas de Informática Forense, incluyendo exploración de discos, recuperación de datos y búsqueda de archivos ocultos y eliminados. Comunicaciones y Teleinformática.

Veinte años de actividad profesional privada en las áreas de Informática y redes de computadoras. Docente de materias afines. Perito Judicial de parte y consultor técnico en la especialidad.

Instructor de Fuerzas Armadas y miembros del Poder Judicial en procedimientos de Informática Forense.

Miembro del Consejo Profesional de Ingeniería Electrónica, Telecomunicaciones y Computación de jurisdicción Nacional y del Colegio de Ingenieros de la Provincia de Buenos Aires. Miembro de sociedades Internacionales de Informática Forense.

Curriculum Vitae: http://www.presman.com.ar/#cuv

Capítulo 3:

Estos programas fueron descargados en versión Freeware o Trial y ejecutados personalmente para revisar y estudiar su funcionamiento, las marcas son derecho de propiedad intelectual de cada una de las empresas aquí nombradas.

*Figura 1: **Sitio Oficial Web** (http://www.tcpdump.org/)

*Figura 2: https://www.winpcap.org/windump/install/default.htm

*Figura 3: https://www.netresec.com/?page=Networkminer

*Figura 4: **Sitio Oficial Web** (https://www.wireshark.org/#download)

*Figura 5: **Sitio Oficial Web** (https://www.wireshark.org/#download)

*Figura 6: **Sitio Oficial Web** (https://www.xplico.org/)

*Figura 7: **Sitio Oficial Web** (https://www.splunk.com/es_es)

*Figura 8: **Sitio Web Oficial** (https://www.snort.org/downloads)

*Figura 9: **Sitio Web Oficial** (https://www.openpgp.org/)

*Figura 10: **Sitio Web Oficial** (https://www.gpg4win.org/)

*Figura 11: **Sitio Web Oficial** (http://www.winhex.com/winhex/hex-editor.html)

*Figura 12: https://github.com/GNOME/ghex

*Figura 13: **Sitio Web Oficial** (https://www.vmware.com/) (https://my.vmware.com/web/vmware/downloads)

*Figura 14: **Sitio Web Oficial** (https://www.virtualbox.org/)

*Figura 15: Sitio Web oficial (https://xenserver.org/blog/entry/xenserver-7-6-now-available-for-download.html) (https://www.xenproject.org/downloads.html)

*Figura 16: **Sitio Web oficial (**https://www.cygwin.com/)

*Figura 17: **Sitio Web Oficial** (https://www.runtime.org/raid.htm)

*Figura 18: **Sitio Web Oficial** (https://www.diskinternals.com/ntfs-recovery/)

*Figura 19: https://descargarrecuva.com/

*Figura 20: **Sitio Web Oficial** (https://www.cnwrecovery.com/)

*Figura 21: **Sitio Web Oficial** (https://www.r-studio.com/)

*Figura 22: **Sitio Web Oficial** (https://www.magnetforensics.com/computer-forensics/internet-evidence-finder-triage-edition/)

*Figura 23: **Sitio Web Oficial** (http://downloads.digitalcorpora.org/)

*Figura 24: **Sitio Web Oficial** (http://www.diskwipe.org/)

*Figura 25: http://cdslow.org.ru/en/ntpwedit/

*Figura 26: https://www.openwall.com/john/

*Figura 27: http://www.oxid.it/cain.html**;** (http://www.oxid.it/ca_um/);

*Figura 28: **Sitio Web Oficial** (https://www.autopsy.com/);

https://www.autopsy.com/download/

*Figura 29: **Sitio Web Oficial** (https://www.guidancesoftware.com/encase-forensic-imager)

*Figura 30: **Sitio Web Oficial** (https://www.osforensics.com) ;

https://www.osforensics.com/download.html

*Figura 31: **Sitio Web Oficial** (https://accessdata.com/products-services/forensic-toolkit-ftk)

*Figura 32: **Sitio Web Oficial** (http://www.ltr-data.se/opencode.html/#ImDisk)

*Figura 33: **Sitio Web Oficial** (https://www.osforensics.com/tools/mount-disk-images.html)

*Figura 34: **Sitio Web Oficial** (https://www.cgsecurity.org/wiki/PhotoRec_ES)

*Figura 35: **Sitio Web Oficial** (http://www.symantec-norton.com/Norton_Ghost_15.0_p115.aspx?lang=es-AR&par=goo_arbmm_norton_ghost&gclid=CjwKCAiAiarfBRASEiwAw1tYv1nwn-Hvz8T8ir2IIpKvt8V5s-mEz9MiLS5xlij1HXSmty78FkJuyxoCAt4QAvD_BwE): Licencia Propietaria

*Figura 36: **Sitio Web Oficial** (https://www.acronis.com/es-mx/personal/true-image-features/?gclid=CjwKCAiAiarfBRASEiwAw1tYvwzxEbIHuYRI399f83AMMEhos_64_ymgwKI7OAEYJMaj58lXGTxQTBoCvkkQAvD_BwE)

*Figura 37: **Sitio Web Oficial** (https://sourceforge.net/projects/dc3dd/)

*Figura 38: **Sitio Web Oficial** (https://accessdata.com/product-download/ftk-imager-version-3.4.3)

*Figura 39: (https://www.aldeid.com/wiki/Dumpit)

*Figura 40: **Sitio Web Oficial** (https://www.volatilityfoundation.org/26)

*Figura 41: **Sitio Web Oficial** (https://www.backtrack-linux.org/)

*Figura 42: **Sitio Web Oficial** (https://www.kali.org/downloads/)

*Figura 43: **Sitio Web Oficial** (https://www.caine-live.net/)

*Figura 44: **Sitio Web Oficial** (http://www.deftlinux.net/)

*Figura 45: **Sitio Web Oficial** (http://www.matriux.com) http://www.matriux.com/index.php?page=download

*Figura 46: **Sitio Web Oficial** (http://bugtraq-team.com/); http://bugtraq-team.com/downloads.html

Capítulo 4:

Poder Judicial de la Provincia de Neuquén – Protocolo de Actuación de Pericias Informáticas

http://200.70.33.130/images2/Biblioteca/ProtocoloActuacionPericiasInformaticas.pdf

Registro y el allanamiento en el proceso penal – Maximiliano Hairabedián

Manual de instrucción de sumarios – Ministerio Público Fiscal – Policía Judicial de Córdoba (Laura Cantore y E. Tomas Casas)

Capacitación destinada a los sumariantes de las Unidades Judiciales de Córdoba – María Dolores Morales de Cáceres y otros. (Colección INV- Tomo 7)

Capítulo 5:

[1] PRESMAN-SALLIS, Procedimiento para el manejo, tratamiento y recolección de la evidencia digital.

[2] Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense. Info-Lab. Guia Integral de Empleo de la Informática Forense en el Procedimiento Penal. Segunda Edición. Abril 2016

[3] Cadena de Custodia: La cadena de custodia es un sistema de aseguramiento que, basado en el principio de la "mismidad", tiene como fin garantizar la autenticidad de la evidencia que se utilizará como "prueba" dentro del proceso.

Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática – GECTI Facultad de Derecho Universidad de los Andes
2006 - All rights reserved. *Jeimy J. Cano, Ph.D, CFE* - Documento GECTI 7

INTERNATIONAL ORGANIZATION OF COMPUTER EVIDENCE –IOCE. (2002)Guidelines for the best practices in the forensic examination of digital technology.http://www.ioce.org/2002/ioce_bp_exam_digit_tech.html.consultado :1-10-2018

BREZINSKI, D. y KILLALEA, T. (2002) RFC 3227: Guidelines for Evidence Collectionand Archiving. Network Working Group. February. https://tools.ietf.org/html/rfc3227 consultado: 1-10-2018

Dr. Santiago Acurio Del Pino - Director Nacional de Tecnología de la Información

CANO, J. (2003) Admisibilidad de la evidencia digital: Algunos elementos de revisión y análisis. Revista Electrónica de Derecho Informático. No. 61. http://www.alfa-redi.org/rdi-articulo.shtml?x=1304.

ASOCIATION OF CHIEF POLICE OFFICERS (1999) Good practice guide for computer based evidence. https://www.digital-detective.net/acpo-good-practice-guide-for-digital-evidence/ Revised Good Practice Guide for Digital Evidence_Vers 5_Oct 2011.pdf .Consultado: 06-10-2018

DEPARTMENT OF JUSTICE. (2004) Forensic examination of digital evidence. A guide for law enforcement. Special Report. https://www.ncjrs.gov/pdffiles1/nij/199408.pdf consultado: 01-10-2018

STANDARDS AUSTRALIA INTERNATIONAL. (2003) HB171:2003 Handbook Guidelines for the management of IT evidence.
https://www.saiglobal.com/PDFTemp/Previews/OSH/as/misc/handbook/HB171.PDF.
Consultado 09-10-2018

INFORMATION SECURITY AND FORENSICS. (2004) Computer forensics. Part2.Best practices. http://www.isfs.org.hk/manual.html.Consultado: 11-10-2018

Capítulo 6:

[1] Manual de instrucción de sumarios – Ministerio Público Fiscal – Policía Judicial de Córdoba (Laura Cantore y E. Tomas Casas)

Capacitación destinada a los sumariantes de las Unidades Judiciales de Córdoba – María Dolores Morales de Cáceres y otros. (Colección INV- Tomo 7)

[2] Registro y el allanamiento en el proceso penal – Maximiliano Hairabedián

[3] Boletin Oficial. Ministerio de Seguridad. Resolución 535-E/2017

Capitulo 7:

Búsquedas y resultados variados en la web.
Posterior recopilación y lectura de publicaciones/artículos diversos.

KASPERSKY LAB – SECURELIST
"Desarrollo de las amenazas informáticas en el tercer trimestre de 2016".
https://securelist.lat/it-threat-evolution-q3-2016/84162/
"Desarrollo de las amenazas informáticas en el tercer trimestre de 2017".
https://securelist.lat/it-threat-evolution-q3-2017/85686/

[1] ***AENOR:***

Sitio Web OFICIAL
https://www.aenor.com/normas-y-libros/normas

Aenor norma UNE 71506:2013
https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma/?c=N0051414

AENOR "La Asociación Española de Normalización y Certificación", 2016,
http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0051414#.WKHjgDvhAdV

[2] "INTRODUCCION A LA INFORMÁTICA FORENSE", RA-MA, ISBN: 9788499642093, 2015.
Francisco Lázaro Domínguez

Karen Kent, "Guide to Integrating Forensic Techniques into Incident Response", 2006,
http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=50875

[4] Collective work of all DFRWS attendees, "A Road Map for Digital Forensic Research", 2001,
http://dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf

[5] "INVESTIGATION PROCESS", 2003
Carrier y Spafford
https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2003-29.pdf

"File System Forensic Analysys", Adisson Wesley Professional, ISBN: 0-32-126817-2,
Brian Carrier
http://www.campus64.com/digital_learning/data/cyber_forensics_essentials/info_file_system_forensic_analysis.pdf

"ZDZIARSKI'S BLOG OF THINGS", 2017
Jonathan Zdziarski
https://www.zdziarski.com/blog/?cat=11

"Guidelines on Mobile Device Forensics",2014
Rick Ayers
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf

"Good Practice Guide for Computer-Based Electronic Evidence",1996
Dan Haagman
https://www.cps.gov.uk/legal/assets/uploads/files/ACPO_guidelines_computer_evidence[1].pdf

SWGDE Best Practices for Mobile Phone Forensics, "cientific Working Group on Digital Evidence", version 2.0, 2013
https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Mobile%20Phone%20Forensics

"Metodologìa para el desarrollo de procedimientos periciales en el ambito de la informatica forense",
Juan Miguel Tocados, Trabajo de Fin de Grado, 2015
https://ruidera.uclm.es/xmlui/bitstream/handle/10578/6667/TFG_Juan_Miguel_Tocados.pdf?sequence=1&isAllowed=y

"Desarrollo de una Guía de Asistencia para el Análisis Forense Informático en un Ambiente Piloto",
Pereyra, Damián; Eterovic, Jorge
http://sedici.unlp.edu.ar/bitstream/handle/10915/43214/Documento_completo.pdf?sequence=1

"Análisis forense de dispositivos de telefonía celular mediante procedimientos operativos estandarizados",2015,
Leopoldo Sebastián Gómez
http://sedici.unlp.edu.ar/bitstream/handle/10915/55345/Documento_completo.pdf-PDFA.pdf?sequence=1

Guide to Integrating Forensic Techniques into Incident Response
Timothy Grance, Suzanne Chevalier, Karen Kent Scarfone, Hung Dang
NIST Special Publication 800-86
https://www.nist.gov/publications/guide-integrating-forensic-techniques-incident-response

A Framework for Harmonizing Forensic Science Practices and Digital/Multimedia Evidence
Mark Pollitt, Eoghan Casey, David-Olivier Jaquet-Chiffelle, Pavel Gladyshev, OSAC Task Group on Digital/Multimedia Science
OSAC Technical Series 0002
https://www.nist.gov/sites/default/files/documents/2018/01/10/osac_ts_0002.pdf

Guidance for Evaluating Contactless Fingerprint Acquisition Devices
John M. Libert, John D. Grantham, Bruce Bandini, Stephen S. Wood, Michael D. Garris, Kenneth Ko, Frederick R. Byers, Craig I. Watson
NIST Special Publication 500-305
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-305.pdf

Securing Electronic Health Records on Mobile Devices
Gavin W. O'Brien, Nate V. Lesser, Brett Pleasant, Sue Wang, Kangmin Zheng, Colin Bowers, Kyle Kamke
NIST Special Publication 1800-1
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-1.pdf

Protocolo unificado de los ministerios públicos de la República Argentina Guía para el levantamiento y conservación de la evidencia
Ministerio de Justicia y Derechos Humanos de la Nación - República Argentina

http://www.jus.gob.ar/media/3262247/Protocolo%20unificado.pdf

Lineamientos para la creación de laboratorios informáticos forenses
Gastón Semprini - Jefe del área de informática forense del Poder Judicial de Río Negro
http://sedici.unlp.edu.ar/bitstream/handle/10915/58306/Documento_completo.pdf-PDFA.pdf?sequence=1

Aspectos Estratégicos, Organizacionales y de Infraestructura en el Diseño de Laboratorios Judiciales de Informática Forense
Di Iorio, Constanzo, Vega, Lamperti, Giaccaglia, Cistoldi, Nuñez*
Univerisdad FASTA
http://info-lab.org.ar/images/pdf/laboratorios_ciiddi.pdf

The Governance of Corporate Forensics using COBIT, NIST and Increased Automated Forensic Approaches
Henry Nnoli, Dale Lindskog, Pavol Zavarsky, Shaun Aghili, Ron Ruhl - ATB Financial, Canada
Information Systems Security Management, Concordia University College of Alberta, Canada
https://ieeexplore.ieee.org/document/6406300

Reflexiones sobre la norma ISO/IEC 27037:2012 para la identificación, recolección y preservación de evidencia digital
Ana Horvat, 2013
http://www.informaticalegal.com.ar/2013/09/15/reflexiones-sobre-la-norma-isoiec-270372012-directrices-para-la-identificacion-recoleccion-adquisicion-y-preservacion-de-la-evidencia-digital/

Test Results for Mobile Device Acquisition Tool: Zdziarski's Method
https://www.nij.gov/publications/pages/publication-detail.aspx?ncjnumber=232383

Guidelines for the Management of IT Evidence
APEC Telecommunications and Information Working Group
http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN016411.pdf

14a Conferencia Europea sobre Guerra Cibernética y Seguridad, Hatfield, Reino Unido, 2015
https://www.researchgate.net/publication/283226153_Standard_ISO_270372012_and_Collection_of_Digital_Evidence_Experience_in_the_Czech_Republic

Norma UNE 197010:2015 para la elaboración de Informes Periciales TIC
Rafael López Rivera, 2016
https://peritoit.com/2016/10/17/norma-une-1970102015-para-la-elaboracion-de-informes-periciales-tic/

Estándares nacionales e internacionales que puede seguir un perito informático para realizar el análisis forense de una evidencia y para la elaboración de un peritaje informático
Javier Rubio Alamillo, 2016
https://peritoinformaticocolegiado.es/blog/estandares-nacionales-e-internacionales-que-puede-seguir-un-perito-informatico-para-realizar-el-analisis-forense-de-una-evidencia-y-para-la-elaboracion-de-un-peritaje-informatico/

Análisis Forense v1
Reinaldo Mayol
http://www.eslared.org.ve/walc2012/material/track4/An%E1lisis%20Forense%20v1.pdf

Análisis Forense Digital
Miguel López Delgado
https://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

El tratamiento de la evidencia digital y las normas ISO/IEC 27037:2012
Roatta, Casco, Fogliato
http://sedici.unlp.edu.ar/bitstream/handle/10915/50586/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y

Informe sobre el Peritaje Informático
José Luis García Gómez, Trabajo Final de Máster
http://www.institutopascualmadoz.es/wp-content/uploads/2016/06/TFM-Jos%C3%A9-Luis-Garc%C3%ADa-G%C3%B3mez.pdf

Modelo para el análisis forense y la legalización de evidencia digital atípica en procesos judiciales en Ecuador
Juan Sebastián Grijalva Lima, Byron Loarte Cajamarca
https://dialnet.unirioja.es/servlet/articulo?codigo=6163708

Cadena de Custodia Digital de las Evidencias para la realización de un Peritaje
Carlos Romeo García Dahinten, Trabajo de Graduación, 2014
Universidad de San Carlos de Guatemala, Facultad de Ingeniería
http://biblioteca.usac.edu.gt/tesis/08/08_0755_CS.pdf

Metodología para un Análisis Forense
Carles Gervilla Rivas, Trabajo de Final de Máster
http://openaccess.uoc.edu/webapps/o2/bitstream/10609/39681/6/cgervillarTFM1214memoria.pdf

Guía actualizada para futuros peritos informáticos. Últimas herramientas de análisis forense digital. Caso práctico.
Jorge Navarro Clérigues - Trabajo Fin de Curso - 2015/2016
Universitat Politècnica de València
http://www.pensamientopenal.com.ar/system/files/2016/05/doctrina43429.pdf

Protocolos, Normas, Estándares

[3] **NIST:**
NIST - CYBERSECURITY FRAMEWORK
This voluntary Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk.
The Cybersecurity Framework's prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security.

Framework for Improving Critical Infrastructure Cybersecurity
https://www.nist.gov/cyberframework
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Framework Resources
https://www.nist.gov/cyberframework/framework-resources-0

Recover
Guide for Cybersecurity Event Recovery
NIST Special Publication 800-184
https://www.nist.gov/cyberframework/recover

Identify
https://www.nist.gov/cyberframework/identify
Information Security Handbook: A Guide for Managers
NIST Special Publication 800-100

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf
Guide to Information Technology Security Services
NIST Special Publication 800-35
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-35.pdf
Managing Information Security Risk
NIST Special Publication 800-39
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

Protect
https://www.nist.gov/cyberframework/protect
Security Considerations in the System Development Life Cycle
NIST Special Publication 800-64 Revision 2
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-64r2.pdf
Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
NIST Special Publication 800-160
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf

Detect
https://www.nist.gov/cyberframework/detect
Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
NIST Special Publication 800-137
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf
SITUATIONAL AWARENESS For Electric Utilities
NIST Special Publication 1800-7
https://www.nccoe.nist.gov/sites/default/files/library/sp1800/es-sa-nist-sp1800-7-draft.pdf

Respond
https://www.nist.gov/cyberframework/respond
Contingency Planning Guide for Federal Information Systems
NIST Special Publication 800-34 Rev. 1
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

[6] ISO/IEC:

ISO/IEC 27035:
IS Incident Management
Publicada el 17 de Agosto de 2011. Proporciona una guía sobre la gestión de incidentes de seguridad en la información. Consta de 3 partes: 27035-1, Principios en la gestión de incidentes (Publicada en Noviembre de 2016); 27035-2, guías para la elaboración de un plan de respuesta a incidentes (Publicada en Noviembre de 2016); 27035-3, guía de operaciones en la respuesta a incidentes (que el momento está parado su desarrollo).

ISO/IEC 27036:
Information security for supplier relationships
Guía en cuatro partes de seguridad en las relaciones con proveedores: 27036-1, visión general y conceptos (Publicada el 24 de Marzo de 2014); 27036-2, requisitos comunes (Publicada el 27 de Febrero de 2014); 27036-3, seguridad en la cadena de suministro TIC (Publicada el 08 de Noviembre de 2013); 27036-4, guía de seguridad para entornos de servicios Cloud (Publicada en Octubre de 2016).

ISO/IEC 27037
Evidence Acquisition
Guidelines for identification, collection, acquisition and preservation of digital evidence
https://www.iso.org/obp/ui/#iso:std:iso-iec:27037:ed-1:v1:en

Publicada el 15 de Octubre de 2012. 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 y para que puedan ser utilizadas con valor probatorio y en el intercambio entre las diferentes jurisdicciones.

ISO/IEC 27038
Specification for digital redaction
Publicada el 13 de Marzo de 2014. Es una guía de especificación para seguridad en la redacción digital.

ISO/IEC 27039
Selection, deployment and operations of intrusion detection and prevention systems (IDPS)
Publicada el 11 de Febrero de 2015. Es una guía para la selección, despliegue y operativa de sistemas de detección y prevención de intrusión (IDS/IPS). Existe una (corrección al contenido inicial de 28 de Abril de 2016).

ISO/IEC 27040:
Storage security
Publicada el 05 de Enero de 2015. Es una guía para la seguridad en medios de almacenamiento.

ISO/IEC 27041
Guidance on Assuming Suitability and Adequacy of Investigation Methods
Publicada el 19 de Junio de 2015. Es una guía para la garantizar la idoneidad y adecuación de los métodos de investigación.

ISO/IEC 27042
Analysis & Interpretation
Publicada el 19 de Junio de 2015. Es una guía con directrices para el análisis e interpretación de las evidencias digitales.

ISO/IEC 27043
Investigative Principles & Process
Publicada el 04 de Marzo de 2015. Desarrolla principios y procesos de investigación para la recopilación de evidencias digitales.

ISO/IEC 27050
Electronic discovery of Electronically Stored Information
Norma desarrollada en tres partes sobre la información almacenada en dispositivos electrónicos en relación a su identificación, preservación, recolección, procesamiento, revisión, análisis y producción: 27050-1, conceptos generales (Publicada en Noviembre de 2016); 27050-2, Guía para el gobierno y gestión (En desarrollo); 27050-3, código de buenas prácticas (En desarrollo).

[7] RFC - Request For Comments

RFC Base
www.rfc-base.org

Internet Engineering Task Force
www.ietf.org

ITEF Tools
tools.ietf.org

RFCs:

RFC 3227
Guidelines for Evidence Collection and Archiving

https://tools.ietf.org/html/rfc3227
https://tools.ietf.org/rfc/rfc3227.txt
https://tools.ietf.org/pdf/rfc3227.pdf

RFC 7970
Incident Object Description Exchange Format
https://tools.ietf.org/pdf/rfc7970.pdf

Digital Forensics Extension for IODEF (RFC 5070/7970)
https://tools.ietf.org/pdf/draft-inacio-mile-forensics-00.pdf

RFC 4810
Extensible Markup Language Evidence Record Syntax (XMLERS)
https://tools.ietf.org/html/rfc6283

RFC 4998
Evidence Record Syntax (ERS)
https://tools.ietf.org/html/rfc4998

RFC 6283
Long-Term Archive Service Requirements
https://tools.ietf.org/html/rfc4810

**** MUY ESPECIAL ATENCION A LOS DOCUMENTOS PUBLICADOS Y SITIOS WEBS REFERNCIADOS ****
Framework
Risk Management Resources
https://www.nist.gov/cyberframework/general-resources

City of Houston's
Cybersecurity Control Implementation Interface (CCII) *****
http://www.dot.state.fl.us/ois/RFQ/ISRA/B-FCSRiskAssessmentToolV1.0.xlsx

Florida Agency for State Technology's *****
FCS Risk Assessment Tool *****
http://www.dot.state.fl.us/ois/RFQ/ISRA/B-FCSRiskAssessmentToolV1.0.xlsx

Referencia Internacional a:
Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento
AGESIC - URUGUAY
Marco de ciberseguridad v4.0 *****
https://www.agesic.gub.uy/innovaportal/v/5823/1/agesic/marco-de-ciberseguridad.html
https://www.agesic.gub.uy/innovaportal/file/5823/1/marco-de-ciberseguridad-4.0-completo.pdf

Herramientas, Software, Tools, Etc.

Belkasoft (free & de pago)
Belkasoft Evidence Center
https://belkasoft.com/get

The Sleuth Kit
https://www.sleuthkit.org/

Autopsy

https://www.sleuthkit.org/autopsy/

Golden Image by Mathias Vetsch and Luca Taennler
https://github.com/colapse/Autopsy-GoldenImage

NetArchae by Emily Wicki
https://github.com/thePidge/netArchae

Parse SQLite Del Rec by Mark McKinnon
https://github.com/markmckinnon/Autopsy-Plugins

P2P Forensic by Carlos Cilleruelo Rodríguez
https://github.com/CarlosLannister/P2PForensic

HashDump by John Lukach
https://github.com/jblukach/AutopsyMultiUserModules

USN Parser by Mark McKinnon
https://github.com/markmckinnon/Autopsy-Plugins

Mount Image Pro
http://www.mountimage.com/download-computer-forensics-software.php

PsTools
https://docs.microsoft.com/en-us/sysinternals/downloads/pstools

VMMap
https://docs.microsoft.com/en-us/sysinternals/downloads/vmmap

Forensic Toolkit (FTK)
Registry Viewer
FTK Imager
MPE+ / MPE+ INVESTIGATOR / MPE+ nFIELD
https://accessdata.com/product-download

ODESSA
The Open Digital Evidence Search and Seizure Architecture is a cross-platform framework for performing Computer Forensics and Incident Response.
https://sourceforge.net/projects/odessa/

Flu Project
Herramientas Varias
https://github.com/fluproject

Androl4b
A Virtual Machine For Assessing Android applications, Reverse Engineering and Malware Analysis
https://github.com/sh4hin/Androl4b

INFOLAB
http://info-lab.org.ar
Aplicaciones Forenses
http://info-lab.org.ar/index.php/proyectos/aplicaciones-forenses
- CIRA: Framework de File Carving.
- BIP-M: Framework de análisis forense de memoria volátil para Win 7.
- FOMO: Forensia en Móviles (Análisis y Visualización de Información extraída).
- FOMO - Android: Analizador para Android.
- FOMO - Windows Phone: Analizador para WP (+UNNOBA).

- SAVE: Herramientas de análisis inteligente de extracciones forenses (+UNNOBA +CIJ MPF CABA).
- SHERLOQ Media: Análisis Digital de Imagen y Vídeo. Alumno de Proyecto Final de Graduación de Ingeniería Informática UFASTA.

Herramientas LINUX para análisis forense
Javier Tobal
http://www.javiertobal.com/herramientas-linux-para-analisis-forense-detalle/

Forensics PowerTools
Muy completa recopilación (listado) de herramientas para análisis forense, incluyendo una breve descripción y enlace (link) a cada una de ellas.
(Incluye tanto del tipo libres, free, gratis como también comerciales, de pago -aunque puede mencionar algunas comerciales, pero free también-).
Pedro Sánchez Cordero
http://conexioninversa.blogspot.com/2013/09/forensics-powertools-listado-de.html