CAPÍTULO II

"Es una equivocación garrafal el sentar teorías antes de disponer de todos los elementos de juicio"
Sir Conan Doyle en Sherlock Holmes

EVIDENCIA DIGITAL

2.1. Importancia de la evidencia digital.

2.2. Clasificación de la evidencia digital.

2.3. Procedimiento de recolección de evidencia digital.

2.4. Criterios de admisibilidad y valor probatorio.

2.5. Tipos de evidencia digital.

2.1. IMPORTANCIA DE LA EVIDENCIA DIGITAL

En el 2005, las pruebas digitales encontradas en un disco duro ayudaron a los investigadores a encarcelar al asesino en serie BTK[1], un criminal que había eludido a la policía desde 1974 y al cual se le atribuyen al menos 10 víctimas.

Pruebas digitales encontradas en un celular llevó a la policía internacional a dar con el paradero de los terroristas responsables de los atentados de Madrid, que resultó con la muerte de al menos 190 personas en el 2004.

Pruebas digitales recogidas de las redes informáticas en las universidades y las instalaciones militares en la década de 1980 condujeron al descubrimiento del espionaje internacional, con el apoyo de un gobierno extranjero hostil a los Estados Unidos.

En el mundo de hoy los agentes de la ley tratan de extraer pruebas digitales de un mayor número de dispositivos, con mayor capacidad de almacenamiento, los dispositivos que se pueden investigar en relación a un delito incluyen computadoras, laptops, memorias flash, dispositivos de almacenamiento externo, cámaras digitales, las consolas de videojuegos y los teléfonos celulares. Indudablemente muchos más dispositivos de los que se tenía tan solo hace un par de años.

Los datos contenidos en estos dispositivos digitales pueden ayudar a hacer cumplir la ley en una investigación criminal o enjuiciamiento de delitos en una variedad de maneras. Por ejemplo, los agentes del orden pueden investigar una denuncia de abuso sexual infantil analizando la computadora de un sospechoso, donde se podría encontrar varias imágenes, en donde el sospechoso abusaba sexualmente de menores.

[1]Dennis Lynn Rader es un asesino en serie estadounidense, su alias era Asesino BTK, letras correspondientes a Bind, Torture and Kill ('Atar, torturar y matar' en español).

En otro ejemplo, una pequeña tarjeta de memoria flash de una cámara digital que se encuentra en posesión de un sospechoso de robar automóviles, puede contener imágenes de los autos robados.

Le evidencia es el aspecto más importante en cualquier disputa legal o extrajudicial y dentro de un delito donde esté involucrado directa o indirectamente un equipo informático.

Evidencia digital son los datos generados por un equipo informático, todo lo que se realice en equipos informáticos como un computador, celular o una palm, etc., queda registrado incluso luego de que el disco duro ha sido formateado, pudiendo ser recuperado y procesado de forma correcta para que sea presentado como evidencia dentro de un proceso legal.

Se puede decir que el término “Evidencia Digital” abarca cualquier información en formato digital que pueda establecer una relación entre un delito y su autor. Desde el punto de vista del derecho probatorio[2], puede ser comparable con “un documento” como prueba legal. Con el fin de garantizar su validez probatoria, los documentos deben cumplir con algunos requerimientos, estos son:

- **Autenticidad:** satisfacer a una corte en que los contenidos de la evidencia no han sido modificados; la información proviene de la fuente identificada; la información externa es precisa.
- **Precisión:** debe ser posible relacionarla positivamente con el incidente. No debe haber ninguna duda sobre los procedimientos seguidos y las herramientas utilizadas para su recolección, manejo, análisis y posterior presentación en una corte. Adicionalmente, los procedimientos deben ser seguidos por alguien que pueda explicar,

[2]El derecho probatorio es aquella rama del Derecho que se ocupa de la fijación, evaluación, práctica y examen de las pruebas en un Proceso para crear en el Juez una convicción de certeza respecto de la causa a juzgar.

en términos "*entendibles*", cómo fueron realizados y con qué tipo de herramientas se llevaron a cabo.

- **Suficiencia (completa):** debe por sí misma y en sus propios términos mostrar el escenario completo, y no una perspectiva de un conjunto particular de circunstancias o eventos.

Así como se han establecido diferentes definiciones para los delitos informáticos, también se han establecido diferentes y especiales consideraciones para su principal insumo que es la evidencia digital.

De acuerdo a la conceptualización de Eoghan Casey en su libro Digital Evidence and Computer Crime, "*la evidencia digital es un tipo de evidencia física. Está construida de campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales*".

Miguel López Delgado[14] en su publicación Análisis Forense Digital, define la evidencia digital como: "*el conjunto de datos en formato binario, esto es, comprende los ficheros, su contenido o referencia a estos (metadatos) que se encuentran en los soportes físicos o lógicos del sistema vulnerado o atacado*".

Según Jeimy J. Cano M[3]. "*La evidencia digital es la materia prima para los investigadores, donde la tecnología informática es parte fundamental del proceso*". La evidencia digital posee, entre otros, los siguientes elementos que la hacen un constante desafío para aquellos que la identifican y analizan en la búsqueda de la verdad: Es volátil, es anónima, es duplicable, es alterable y modificable, es eliminable. Estas características advierten sobre la exigente labor que se requiere por parte de los especialistas en temas de informática forense, tanto en procedimientos, como en técnicas y herramientas tecnológicas para

[3]Ingeniero y Magíster en Ingeniería de Sistemas y Computación de la Universidad de los Andes, COLOMBIA. Certificado en Computer Forensic Analysis (CFA).

obtener, custodiar, revisar, analizar y presentar la evidencia presente en una escena del delito. Además, revela con respecto al tratamiento de la evidencia digital, que se debe guardar especial cuidado a: su debido registro, admisibilidad, valor probatorio, preservación transformación y recuperación.

Con estos argumentos, la evidencia digital, es un insumo de especial cuidado, para el proceso de investigación de delitos informáticos, que debe ser tratada por parte de los especialistas, de tal forma que se conserven todas las medidas de precaución necesarias para no contaminarla, ya que cualquier indicio de modificación sería objeto de desaprobación ante un proceso litigioso[4].

2.2. CLASIFICACIÓN DE LA EVIDENCIA DIGITAL

Harley Kozushko (2003), menciona que la evidencia digital se puede clasificar, comparar, e individualizar, es decir es el proceso por el cual se buscan características generales de archivos y datos, características que diferencian evidencia similar y que deben ser utilizadas a criterio del investigador, por ejemplo:

- **Contenido:** Un e-mail, por ejemplo, puede ser clasificado por su contenido como SPAM, y puede ser individualizado a partir del contenido de sus encabezados, información que por lo general no es visible para el usuario. Por ejemplo, por su dirección de origen.
- **Función:** El investigador puede examinar cómo funciona un programa para clasificarlo y algunas veces individualizarlo. Por ejemplo, un programa que inesperadamente transfiere información valiosa desde un computador confiable a una locación remota podría ser clasificado como un caballo de Troya y puede ser

[4]El litigio es un conflicto de intereses, donde existe la pretensión por una parte y la resistencia por otra.

individualizado por la localización remota a la que transfiere la información.

- **Características:** los nombres de archivo, extensiones e inclusive los encabezados internos que identifican los diferentes formatos de archivo que existen pueden ser de utilidad en la clasificación de la evidencia digital.

De acuerdo con el HB: 171-2003 Guidelines for the Management of ITEvidence[5], la evidencia digital que contiene texto se clasifica en 3 categorías:

- **Registros generados por computador:** Estos registros son aquellos, que como dice su nombre, son generados como efecto de la programación de un computador. Los registros generados por computador son inalterables por una persona. Estos registros son llamados registros de eventos de seguridad (logs) y sirven como prueba tras demostrar el correcto y adecuado funcionamiento del sistema o computador que generó el registro.
- **Registros no generados sino simplemente almacenados por o en computadores:** Estos registros son aquellos generados por una persona, y que son almacenados en el computador, por ejemplo, un documento realizado con un procesador de palabras. En estos registros es importante lograr demostrar la identidad del generador, y probar hechos o afirmaciones contenidas en la evidencia misma. Para lo anterior se debe demostrar sucesos que muestren que las afirmaciones humanas contenidas en la evidencia son reales.
- **Registros híbridos que incluyen tanto registros generados por computador como almacenados en los mismos:** Los registros híbridos son aquellos que combinan afirmaciones humanas y logs.

[5]Directrices para la gestión de TI evidencia, manual publicado en agosto de 2003. Proporciona orientación sobre la gestión de registros electrónicos que pueden utilizarse como evidencia en procedimientos judiciales o administrativos, ya sea como demandante, demandado, o testigo.

Para que estos registros sirvan como prueba deben cumplir los dos requisitos anteriores.

La idea fundamental es que si se hace una clasificación adecuada basándose en la experiencia y en las técnicas adecuadas se podrá hacer hablar a las "evidencias". Se debe recordar la frase del doctor Edmond Locard[6] (1910) y sentir la profundidad científica de su mensaje: "*Las evidencias son testigos mudos que no mienten*".

2.3. PROCEDIMIENTO DE RECOLECCIÓN DE EVIDENCIA DIGITAL

La única forma de recolectar evidencia digital es seguir las buenas prácticas para este proceso, ya que como se ha mencionado antes, de esto depende que tan exitosa sea la investigación.

La adquisición de la evidencia electrónica se debe hacer siempre de forma que el sistema examinado se vea impactado o modificado en su estado lo mínimo posible.

En un entorno como el informático, en el que el estado contenido de registros, memoria, estado del procesador, etc., de los sistemas cambia continuamente, esto es difícil, si no imposible, de cumplir en la práctica. Siempre que existe una interacción por leve y cuidadosa que sea, del investigador o sus herramientas con el sistema examinado, se produce una alteración de este último.

En la práctica forense moderna, se considera que ciertos tipos de evidencia son más útiles o importantes que otros, y se acepta la

[6]Edmon Locard (1877-1966) fue un criminalista francés, ciencia en la que se le considera uno de los principales pioneros. Es famoso por enunciar el conocido como "Principio de intercambio de Locard".

modificación del estado de la evidencia siempre que esta alteración sea conocida y predecible.

2.3.1. Herramientas para Informática Forense

Para ello es importante conocer las herramientas a utilizar. No sólo hay que conocer el tipo de información que extrae o qué informes genera, sino saber, con detalle, cual es la interacción de la herramienta con el sistema sobre el que corre: cómo afecta a la memoria, qué archivos modifica, a qué recursos del sistema accede, etc.

Dentro de las herramientas frecuentemente utilizadas en procedimientos forenses en informática se detalla algunas, al menos brevemente, por el momento, ya que luego serán estudiadas con más detalle:

	LICENCIA	IMAGEN	CONTROL DE INTEGRIDAD	ANÁLISIS
ENCASE	SI	SI	SI	SI
FORENSIC TOOLKIT	SI	SI	SI	SI
WINHEX (Forensic edition)	SI	SI	SI	SI

Tabla. 2.1. Algunas herramientas para Informática Forense

Como ya se mencionó las anteriores son solo algunas de las herramientas disponibles, aunque existen muchas más de código abierto y que no necesitan licencia, como es el caso de Coroner's Toolkit.

Las características técnicas mínimas que deben cumplir las herramientas forenses para que la evidencia recolectada y/o analizada por ellas sea confiable son las siguientes:

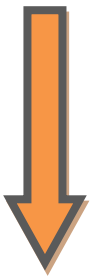
- ***Manejar diferentes niveles de abstracción:*** dado que el formato de la información en su nivel más bajo es difícil de leer,

la herramienta debe interpretar la información y ofrecer acceso en diferentes niveles.

- ***Deben tener la capacidad de extraer una imagen bit a bit de la información.*** Todo byte debe ser copiado de la fuente, desde el inicio hasta el final sin importar si hay fragmentos en blanco.
- ***Deben tener un manejo robusto de errores de lectura.*** Si el proceso de copia falla al leer un sector del medio, se debe marcar en el medio destino un sector del mismo tamaño y en la misma ubicación que identifique el sector que no pudo leerse, adicionalmente estas fallas deben ser documentadas.
- ***La aplicación debe tener la habilidad de realizar pruebas y análisis de una manera científica.*** Estos resultados deben poder ser reproducibles y verificables por una tercera persona.

2.3.2. Cómo obtener la Evidencia Digital?.

Como regla general se debe obtener la evidencia de la forma menos destructiva posible, y siempre en orden de más volátil a menos volátil, específicamente en el orden que se muestra a continuación.



Contenido de la memoria
Conexiones de red establecidas
Procesos corriendo en el sistema
Puertos abiertos
Usuarios conectados al sistema
Contenidos de archivos de paginación y swap
Contenidos de sistemas de archivos
Configuración de hardware y periféricos

Tabla. 2.2. Orden para obtener la Evidencia Digital.

A continuación se presenta otra clasificación según el orden de volatilidad.

Tipo de Almacenamiento	Importancia Forense
CPU (Registros, Cache), Memoria de video	Por lo general la información en estos dispositivos es de mínima utilidad, pero debe ser capturada como parte de la imagen de la memoria del sistema.

Tabla. 2.3. Evidencia altamente volátil

Tipo de Almacenamiento	Importancia Forense
RAM	Incluye información sobre los procesos en ejecución. El hecho de capturarla hace que cambie, requiere de conocimiento especializado para poder reconstruirla, pero no se requiere de mucho conocimiento para buscar palabras clave.
Tablas del Kernel (Estado de la red y procesos en ejecución)	Permite analizar la actividad de red y los procesos que pueden ser evidencia de actividades no autorizadas.

Tabla. 2.4. Evidencia medianamente volátil

Tipo de Almacenamiento	Importancia Forense
Medios fijos (discos duros)	Incluye área de swap[7], colas, directorios temporales, directorios de registro, logs y otros directorios. La información recolectada en el área de swap y en las colas permite analizar los procesos y la información de los mismos, en un tiempo en particular. Los directorios permiten recuperar eventos.
Medio removible (cintas y CR-Rom)	Usualmente son dispositivos para almacenamiento de contenidos históricos del sistema. Si existen previamente a un incidente pueden ser usados para acotar e periodo de tiempo en el cual sucedió.
Medio Impreso (papel)	Difíciles de analizar cuando hay muchos, ya que no se pueden realizar búsquedas automáticas sobre ellos.

Tabla. 2.5. Evidencia poco volátil

Cuando la evidencia se compone de listados de cientos de conexiones, decenas de procesos corriendo, y una imagen bit-a-bit[8] de un disco duro con muchos gigabytes, es necesario establecer un plan para la forma de abordar el análisis. Es decir, decidir de antemano qué es importante, qué no lo es, y en qué orden hacer las cosas.

[7]Swap, es el espacio de intercambio es una zona del disco que se usa para guardar las imágenes de los procesos que no han de mantenerse en memoria física, su homólogo en Windows es el llamado archivo de paginación (pagefile.sys).
[8]Una imagen bit a bit es una réplica exacta de una partición o de un disco duro.

Esto también depende mucho del caso al que el investigador se está enfrentando, la mayoría de los casos son conocidos, entre ellos se puede mencionar:

- Hacker accede a un sistema explotando una vulnerabilidad de un servicio. A continuación, si es necesario, eleva sus privilegios hasta nivel de super-usuario, e instala un kit de herramientas que le permita volver a acceder al sistema cuando desee, aunque la vulnerabilidad original se haya solucionado.
- Usuario legítimo del sistema provoca una infección del computador en el que trabaja, este instala un troyano que convierte al sistema en un "zombie"[9] parte de una "botnet"[10].
- Empleado inconforme sabotea los sistemas de su propia empresa.
- Se sospecha de la posesión por parte del usuario de material no autorizado o ilegal (software pirata, propiedad intelectual, pornografía infantil)
- Empleado roba documentación e información confidencial, o la envía a la competencia.
- Otro tipo de casos de carácter policial (tráfico de drogas, terrorismo, etc.)

Ninguna investigación forense se inicia sin tener al menos una sospecha de la conducta o incidente a investigar, y esto permite adaptar la metodología al caso en particular.

2.3.3. ¿Apagar o no apagar?

Un elemento de la metodología que es importante tener claro es la decisión de apagar o no apagar la máquina, y si la decisión es no apagar, si mantenerla conectada a la red o no.

[9]Los sistemas zombies son aquellos, que sin conocimiento de su legítimo propietario, son usados por terceros para usos ilegales.
[10]Hace referencia a un conjunto de robots informáticos o bots, que se ejecutan de manera autónoma y automática.

Toda decisión que se toma desde el momento que se inicia la investigación debe estar meditada, calculada, y evaluada en relación a sus posibles beneficios y posibles perjuicios del caso particular.

En los casos donde la actividad maliciosa está clara, y en los que cada segundo que pasa se hace más daño a la organización, debería ser una buena práctica apagar el equipo con solo tirar del cable de alimentación, esto es mejor que apagar usando la función de apagado normal o shutdown del sistema, porque tiende a alterar más el estado de la evidencia. Claro que en este caso se tuvo que haber decidido que el contenido de la memoria no es importante, o haber obtenido previamente una imagen de memoria o información útil sobre los procesos activos.

Existen casos en los que apagar o desconectar de la red un sistema, particularmente servidores de aplicaciones críticas de línea de negocio, no es una opción. Ya sea por el impacto que puede tener en el negocio, o por motivos regulatorios o de procesos estrictos de gestión del cambio, una caída no planificada de un sistema crítico puede ser peor que el delito que se está investigando, un caso claro de lo que se menciona son las instituciones bancarias.

En cualquier caso, si se apaga o no, mientras la metodología esté documentada y justificada, queda a la elección del investigador el método exacto a seguir, y de ahí la importancia de la experiencia del investigador.

2.3.4. Preservación de la Evidencia

La preservación de la evidencia lo que busca es de alguna manera reforzar aún más la fuerza probatoria de la información digital, ya que la forma como se haya conservado la integridad de la misma, genera confiabilidad.

Durante el proceso de recolección y de análisis de la evidencia digital, es deber del investigador utilizar algún método para mantener y verificar su integridad, ya que un punto clave en la preservación de evidencia digital, es que se recolecte sin alterarla y evitar su manipulación futura, ya

que de otra forma no podrán ser usada dentro de una investigación, ni tampoco será creíble.

Las buenas prácticas para la preservación de la evidencia digital son:

Inventariar los dispositivos de almacenamiento de evidencia digital removibles (DVDs, CDs, pendrives, memorias flash, discos rígidos, cintas)
Utilizar bolsas antiestáticas para proteger dispositivos magnéticos.
Registrar detalladamente los elementos a secuestrar en el acta de allanamiento (ejemplo: fabricante, modelo y número de serie), su ubicación y el posible propietario o usuario.

Tabla. 2.6. Buenas prácticas de preservación evidencia digital.

Pero estas buenas prácticas también están relacionadas con el método que se haya utilizado, para la obtención de la evidencia digital, los cuales brindan ciertas ventajas y desventajas, el siguiente cuadro esquematiza de mejor manera este tema:

Método	Ventajas	Desventajas
Secuestrar hardware	▪ Requiere poca experticia técnica. ▪ Simple, sin críticas. ▪ El hardware puede ser examinado en un entorno controlado. ▪ El hardware está disponible para varios peritajes o aplicación de distintas técnicas forenses.	▪ Riesgo de dañar el equipamiento en el traslado. ▪ Riesgo ante evidencia encriptada. ▪ Riesgo de pérdida de evidencia digital (ej. RAM). ▪ Genera cuestionamientos por interrumpir la normal operatoria de un negocio. ▪ Riesgo de no ser capaces de poder encender el equipo (ej. password a nivel de BIOS).
Adquirir toda la evidencia digital on-site	▪ La evidencia digital puede ser examinada a posteriori. ▪ El trabajo con una imagen forense evita daños sobre la evidencia original. ▪ Minimiza el impacto en la operatoria del negocio y evita daños al hardware.	▪ Requiere entrenamiento y recursos tecnológicos forenses. ▪ Riesgo de imposibilidad de acceso a la evidencia encriptada. ▪ Riesgo de pérdida de evidencia digital (ej. RAM). ▪ Requiere tiempo (a veces es prohibitivo). ▪ Los métodos pueden ser cuestionados mucho más que al secuestrar el hardware, y pueden surgir impedimentos técnicos.

Adquirir selectivamente la evidencia digital on-site	▪ Se puede aprovechar alguna asistencia local (ej. administrador de sistemas, si no está sospechado). ▪ Rápida y sin consumir demasiados recursos tecnológicos.	▪ Requiere experticia, entrenamiento y recursos tecnológicos forenses. ▪ Riesgo de perder o destruir evidencia (ejem. rootkit[11]). ▪ Los métodos pueden ser cuestionados mucho más que al secuestrar hardware y pueden surgir impedimentos técnicos.

Tabla. 2.7. Ventajas y desventajas de los métodos de obtención de Evidencia Digital.

2.4. CRITERIOS DE ADMISIBILIDAD Y VALOR PROBATORIO

La admisibilidad está ligada con el aspecto legal, y precisamente basándose en legislaciones modernas, existen cuatro criterios que se deben tener en cuenta para analizar, al momento de decidir sobre la admisibilidad de la evidencia:

- Autenticidad.
- Confiabilidad.
- Completitud o suficiencia.
- Apego y respeto por las leyes y reglas del poder judicial.

2.4.1. Autenticidad

La evidencia digital será autentica siempre y cuando se cumplan dos elementos:

[11]rootkit es una herramienta, que tiene como finalidad esconderse a sí misma y esconder otros programas, procesos, etc., que permiten al intruso mantener el acceso a un sistema para remotamente comandar acciones o extraer información sensible.

- El primero, demostrar que dicha evidencia ha sido generada y registrada en el lugar de los hechos.
- El segundo, la evidencia digital debe mostrar que los medios originales no han sido modificados, es decir, que los registros corresponden efectivamente a la realidad y que son un fiel reflejo de la misma.

A diferencia de la evidencia física o evidencia en medios no digitales, en los digitales se presenta gran volatilidad y alta capacidad de manipulación. Por esta razón es importante aclarar que es indispensable verificar la autenticidad de las pruebas presentadas en medios digitales contrarios a los no digitales, en las que aplica que la autenticidad de las pruebas aportadas no será refutada.

Para asegurar el cumplimiento de la autenticidad se requiere que una arquitectura exhiba mecanismos que certifiquen la integridad de los archivos y el control de cambios de los mismos.

Al contar con mecanismos y procedimientos de control de integridad se disminuye la incertidumbre sobre la manipulación no autorizada de la evidencia aportada, y el proceso se concentra en los hechos y no en errores técnicos de control de la evidencia digital bajo análisis.

2.4.2. Confiabilidad

Jeimy Cano dice que "*los registros de eventos de seguridad son confiables si provienen de fuentes que son creíbles y verificables*". Para probar esto, se debe contar con una arquitectura de computación en correcto funcionamiento, la cual demuestre que los logs que genera tiene una forma confiable de ser identificados, recolectados, almacenados y verificados.

El mismo autor menciona que una prueba digital es confiable si el "*sistema que lo produjo no ha sido violado y estaba en correcto funcionamiento al momento de recibir, almacenar o generar la prueba*". La arquitectura de computación del sistema logrará tener un funcionamiento correcto siempre que tenga algún mecanismo de sincronización del

registro de las acciones de los usuarios del sistema y que posea un registro centralizado e íntegro de los mismos registros.

2.4.3. Suficiencia o completitud de las pruebas

Esta es una característica que igual a las anteriores es crítica en el éxito de las investigaciones, frecuentemente la falta de pruebas o la falta de elementos probatorios ocasionan la terminación de un proceso que pudo haberse resuelto.

Para que una prueba esté considerada dentro del criterio de la suficiencia debe estar completa. Para asegurar esto es necesario contar con mecanismos que proporcionen integridad, sincronización y centralización, para lograr tener una vista completa de la situación. Para lograr lo que se menciona es necesario hacer una verdadera correlación de eventos[12], la cual puede ser manual o sistematizada.

En este sentido, actualmente uno de los pilares en los que se basa la gestión de riesgos de seguridad de la información es, sin duda, el análisis y la gestión de logs[13] y la correlación de eventos, lo que se entiende por SIEM (Security Information and Event Management).

Si se analiza esta posibilidad, es posible obtener relaciones entre los datos y eventos presentados, canalizando las inquietudes y afirmaciones de las partes sobre comportamientos y acciones de los involucrados, sustentando esas relaciones con hechos y con registros que previamente han sido asegurados y sincronizados.

2.4.4. Conformidad con las leyes y las regulaciones de la administración de justicia

Esta característica se refiere a que la evidencia digital debe cumplir con los códigos de procedimientos y disposiciones legales del

[12]Proceso de analizar los datos de eventos para identificar patrones, causas comunes y causas iníciales. La correlación de eventos analiza los eventos entrantes para estados predefinidos mediante reglas predefinidas y para relaciones predefinidas.
[13]Archivos de texto que registran toda la actividad de un equipo, aplicación o software. El mismo es presentado cronológicamente con datos adicionales muy detallados que se utilizan generalmente para llevar estadísticas de uso de un determinado sitio, aplicación o software.

ordenamiento del país. Es decir, debe respetar y cumplir las normas legales vigentes en el sistema jurídico.

Así como también a los procedimientos internacionalmente aceptados para la recolección, aseguramiento, análisis y reporte de la evidencia digital, en este sentido como se había mencionado en un capitulo anterior existen iniciativas internacionales como las del IOCE (International Organization of Computer Evidence), la Convención de Cibercrimen presentado por la comunidad Europea, el Digital Forensic Research Workshop, entre otros, donde lo que hacen es establecer lineamientos de acción y parámetros que incluyen el tratamiento de la evidencia en medios electrónicos, los cuales a manera de recomendación deberían ser analizados y revisados por las leyes Ecuatorianas para su posible incorporación y aplicación.

2.5. TIPOS DE EVIDENCIA DIGITAL

Con el incremento del número de delitos informáticos presentados en todo el mundo, gran cantidad de países se han visto obligados a tener en cuenta este concepto en sus Legislaciones y a reglamentar la admisión de la evidencia digital en una corte.

La evidencia digital debe ser cuidadosamente recopilada y manejada, para posteriormente cumplir con los requisitos de admisibilidad en una corte. Independiente de una legislación particular, es esencial garantizar la confiabilidad e integridad de la evidencia.

Una vez que se obtiene la evidencia digital, esta se puede clasificar en los siguientes tipos:

- **Best evidence**

  Evidencia primaria u original, no es copia. Es la forma más convincente de evidencia, también la más difícil de cuestionar, sin embargo, hay que ser cuidadoso en lo que se considera evidencia primaria. Lo que puede lucir primario en la superficie puede no serlo. Es importante validar, no solo la fuente si hay preguntas

sobre su autenticidad, sino la autenticidad misma, pues con no escasa frecuencia, los investigadores pueden haber trabajado y certificado o basado sus opiniones sobre evidencia falsa o falseada.

- **Secondary**
  Evidencia secundaria, no es tan sólida como la evidencia primaria. Frecuentemente son copias de la evidencia primaria, y las copias pueden ser alteradas, lo que disminuye la fuerza como evidencia probatoria.

- **Direct evidence**
  Evidencia directa, prueba o invalida un hecho sin la necesidad de utilizar presunciones o inferencias. Un ejemplo, es el examen de un testimonio directo de un testigo que ha observado o presenciado el evento.
- **Conclusive evidence**
  Evidencia concluyente, es una evidencia muy poderosa. Por sí misma establece una condición o un hecho. La evidencia concluyente es más fuerte que cualquier otro tipo de evidencia. Solo puede extraerse una conclusión única y razonable de la evidencia concluyente.

2.6. BIBLIOGRAFÍA

[1] Análisis forense. Cómo investigar un incidente de seguridad. Tomado de: http://www.idg.es/pcworldtech/Analisis-forense.-Como-investigar-un-incidente-de-/art194718-Seguridad.htm

[2] Evidencia digital en el contexto colombiano. Tomado de: http://www.acis.org.co/index.php?id=856

[3] Derecho informático. Tomado de: http://www.puce.edu.ec/sitios/documentos_DGA/9_21_2102_2009-01_12539_1713627071_S_1.pdf

[4] Digital Evidence. Tomado de: http://www.justnet.org/TechBeat%20Files/DigitalEvidence.pdf

[5] Digital Evidence: Its True Value. Tomado de: http://www.policeone.com/police-products/crime-scene-investigation/articles/1805790-Digital-evidence-its-true-value/

[6] Forensic Examination of Digital Evidence: A Guide for Law Enforcement. Tomado de: http://www.ncjrs.gov/pdffiles1/nij/199408.pdf

[7] Cano Martínez Jeimy José, Mosquera González José Alejandro, Certain Jaramillo Andrés Felipe. Evidencia Digital: contexto, situación e implicaciones nacionales. Abril de 2005. Tomado de: http://derecho.uniandes.edu.co/derecho1/export/derecho/descargas/texto/NasTecnologias6.pdf

[8] Informática Forense como medio de pruebas. Tomado de: http://www.mundomedellin.com/archive/index.php/t-12007.html

[9] Investigaciones Forenses Informáticas. Tomado de: http://www.scribd.com/doc/5565363/INTERPOL-Juan-Millian

[10] Auditores forenses. Tomado de: http://auditoriaforense.net/index.php?option=com_content&task=view&id=34&Itemid=39

[11] Digital evidence. Tomado de: http://infohost.nmt.edu/~sfs/Students/HarleyKozushko/Presentations/DigitalEvidence.pdf

[12] A Log Correlation Model to Support the Evidence Search Process in a Forensic Investigation, Jorge Herrerias; Roberto Gomez; Systematic Approaches to Digital Forensic Engineering, 2007. SADFE 200, Tomado de: http://homepage.cem.itesm.mx/rogomez/publi.html

Libros y Revistas Formato Digital

[13] Casey, E. (2004). Digital Evidence and Computer Crime (2 Ed.). Academic Press. Tomado de: http://books.google.co.cr/books?hl=es&lr=&id=Xo8GMt_AbQsC&oi=fnd&pg=PR7&dq=Eoghan+Casey+%2B+Digital+Evidence+and+Computer+Crime&ots=-XU7LR72OI&sig=3vdxNpxwzZd6MfGWBz2kVe9jVj8#v=onepage&q&f=false

[14] Miguel López Delgado. (2007). Análisis Forense Digital (2 ed.). Tomado de: http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

[15] ACIS. Edición No. 89 julio – septiembre de 2004. Tomado de: http://www.acis.org.co/index.php?id=855

[16] ALFA – REDI. Revista de Derecho Informático. No. 095 - Junio del 2006. Tomado de: http://www.alfa-redi.org/rdi-articulo.shtml?x=6216