Evidencia Digital
Procedimientos Técnicos

Rama Judicial
Consejo Superior de la Judicatura
República de Colombia

Escuela Judicial
"Rodrigo Lara Bonilla"

EVIDENCIA DIGITAL
Guía de Aprendizaje Autodirigido en Evidencia Digital y Prueba Electrónica en Colombia
Procedimientos Técnicos

RAMA JUDICIAL DEL PODER PÚBLICO
CONSEJO SUPERIOR DE LA JUDICATURA

Presidenta
DIANA ALEXANDRA REMOLINA BOTÍA

Vicepresidenta
GLORIA STELLA LÓPEZ JARAMILLO

Magistradas y Magistrados
MAX ALEJANDRO FLÓREZ RODRÍGUEZ
MARTHA LUCÍA OLANO DE NOGUERA
AURELIO ENRIQUE RODRÍGUEZ GUZMÁN
JORGE LUIS TRUJILLO ALFARO

Directora Escuela Judicial
"Rodrigo Lara Bonilla"
MARY LUCERO NOVOA MORENO

Revisor - Metodólogo Escuela Judicial
"Rodrigo Lara Bonilla"
ALEXANDER RESTREPO RAMÍREZ

Autores Cartillas Evidencia Digital
y Prueba Electrónica
FREDY BAUTISTA GARCÍA
ÁLVARO JOSÉ MOSQUERA SUÁREZ
ANDRÉS MENESES OBANDO
DANIEL RÍOS SARMIENTO

Diseño e Ilustración de portada
CÉSAR MONROY

Diseño y diagramación
CAROLINA FRANCO

ISBN: En trámite

Podcast Evidencia Digital:
https://anchor.fm/evidenciadigital

Contenido

Pág.

Índice de ilustraciones

Pág.

Índice de tablas

Pág.

1. CONVENCIONES, ABREVIATURAS, SIGLAS Y GLOSARIO

1.1. TABLA DE CONVENCIONES

Tabla 1. Convenciones

O	Objetivo general de la Guía
Og	Objetivo general
Oe	Objetivo específico
Co	Contenidos
Ap	Actividades pedagógicas
Ae	Autoevaluación
J	Jurisprudencia
B	Bibliografía

1.2. LISTA DE ABREVIATURAS

Tabla 2. Abreviaturas

Art.	Artículo
Cap.	Capítulo
CP	Constitución Política
EJRLB	Escuela Judicial Rodrigo Lara Bonilla
MP	Magistrado o Magistrada Ponente
Núm.	Numeral
Tit.	Título
Trad.	Traducción
CSJ	Consejo Superior de la Judicatura
SIGCMA	Sistema Integrado de Gestión de la Calidad y el Medio Ambiente

EDiPE	Evidencia Digital y Prueba Electrónica
TIC	Tecnologías de la Información y de las Telecomunicaciones
IOCE	International Organization On Computer Evidence (Organización Internacional de Evidencia Digital)

1.3. LISTA DE SIGLAS

Tabla 3. Siglas

APB	Aprendizaje Basado en Problemas
CSJ	Consejo Superior de la Judicatura
ICONTEC	Instituto Colombiano de Normas Técnicas y Certificación
MEN	Ministerio de Educación Nacional
GAA	Guía de Aprendizaje Autodirigido
RIAEJ	Red Iberoamericana de Escuelas Judiciales
SEA	Sistema de Evaluación del Aprendizaje
SIGCMA	Sistema Integrado de Gestión de la Calidad y el Medio

1.4. GLOSARIO

1.4.1. Mensaje de Datos MD

La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax (Artículo 2 Ley 527 de 1999 Ley de Comercio Electrónico, Colombia)

1.4.2. Intercambio Electrónico de Datos (EDI)

La transmisión electrónica de datos de una computadora a otra, que está estructurada bajo normas técnicas convenidas al efecto (Artículo 2 Ley 527 de 1999 Ley de Comercio Electrónico, Colombia)

1.4.3. Evidencia Digital

Mensajes de datos que tiene vocación a reconocerse como plena prueba de un hecho, acto o contrato que haya sido suscrito en entornos digitales y que, por ende, es susceptible de ser creada, transmitida o almacenada.

A diferencia de la evidencia física que está compuesta de átomos, la evidencia digital está compuesta de un lenguaje lógico binario que representa un dato.

1.4.4. Logs de conexiones

Un log ("registro", en español) es un archivo de texto en el que constan cronológicamente los acontecimientos que han ido afectando a un sistema informático (programa, aplicación, servidor, etc.), así como el conjunto de cambios que estos han generado.

1.4.5. Prueba Electrónica

Término implementado por el área de derecho administrativo para referenciar la Evidencia Digital, acorde a lo establecido en: Art 216 de Código Administrativo, dispone que: "Será admisible la utilización de los medios electrónicos para efectos probatorios de conformidad con lo dispuesto en las normas que regulan la materia y en concordancia con las disposiciones de este código y las del código de procedimiento civil"[3]

1.4.6. Dispositivo Sanitizados

Hace referencia a un hardware que ha sido sometido a un proceso de borrado previo automatizado (generalmente por software especializado; dicho borrado se realiza con el objetivo de ofrecer un espacio seguro no contaminado de almacenamiento para recolectar y soportar lógicamente los contenidos binarios del mensaje de datos que se propone hacer valer como medio de prueba dentro de un proceso.

1.4.7. Conexiones tipo USB 3.0, ATA, SATA, IDE, SCSI, ZIP

Tipos de conectores que utilizan dispositivos electrónicos con el fin de transmitir datos o corriente a través de otros; la referencia a ellos se hace necesaria tenerlas en cuenta debido al uso comercial y masificación global promovida por las grandes compañías de tecnología.

1.4.8. RANSOMWARE

"Un ransomware (del inglés ransom, «rescate», y ware, acortamiento de software) o "secuestro de datos" en español, es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema operativo infectado, y pide un rescate a cambio de quitar esta restricción.1 Algunos tipos de ransomware cifran los archivos del sistema operativo inutilizando el dispositivo y coaccionando al usuario a pagar el rescate. Se han propuesto algunas alternativas en español al término en inglés, como programa de secuestro, secuestrador, programa de chantaje o chantajista.

Aunque los ataques se han hecho populares desde mediados de la década del 2010, el primer ataque conocido fue realizado a finales de los 80 por el Dr. Joseph Popp.3 Su uso creció internacionalmente en junio del 2013. La empresa McAfee señaló en 2013 que solamente en el primer trimestre había detectado más de 250 000 tipos de ransomware únicos." [1]

1.4.9. USB Bus Universal en Serie

USB El Bus Universal en Serie, más conocido por la sigla USB, es un bus de comunicaciones que sigue un estándar que define los cables, conectores y protocolos usados en un bus para conectar, comunicar y proveer de alimentación eléctrica entre computadoras, periféricos y dispositivos electrónicos.

1 (1) Rae.es. (2019). Real Academia Española. [online] Available at: https://www.rae.es/ransomware [Accessed 22 Dec. 2019].

2. PRESENTACIÓN

En el año 2019, la Escuela Judicial Rodrigo Lara Bonilla (EJRLB) cumplió su vigésimo primer aniversario *"como parte de la Sala Administrativa del Consejo Superior de la Judicatura (CSJ), tiempo en el cual ha venido consolidando su Misión de liderar la formación judicial con los más altos estándares de calidad, objetivo que no sido pensado únicamente en cumplimiento de procesos técnicos, sino de una formación integral que incluye el desarrollo humano, las competencias, el respeto y garantía del multiculturalismo como expresión de la democracia colombiana, y la ética como pilar de toda expectativa social e institucional de justicia y transparencia."* [2]

En el marco del cumplimiento de estos fines institucionales, se presenta, a continuación, la Guía de Aprendizaje Autodirigido en Evidencia Digital y Prueba Electrónica en Colombia, Aspectos Generales conforme con los lineamientos de la NTC 1486, la NTC 1487, y la ISO 9001-2015.

3. SINOPSIS PROFESIONAL Y LABORAL DE AUTORES

3.1 FREDY BAUTISTA GARCÍA

Fundador y primer director del Centro Cibernético de la Policía Nacional de Colombia.

Experto en Ciberseguridad, Investigador de Cibercrimen y Perito en Informática Forense Digital, participó en la redacción de la Ley de Delito Informáticos en Colombia y fue gestor de la Política de Ciberseguridad y Ciberdefensa, actualmente participa en materia de Política de Seguridad Digital en Colombia.

Fue presidente en dos oportunidades del Grupo de Trabajo Jefes de Unidades de Cibercrimen de INTERPOL para las Américas desde donde lideró importantes investigaciones contra el Crimen Transnacional.

Es actualmente docente universitario en los programas de Maestría y Especialización en Derecho Informático y Nuevas Tecnologías de la Universidad Externado de Colombia y participa como docente invitado en el programa de Maestría de Seguridad Informática en la Universidad de los Andes.

Ha sido formador en el Centro de Capacitación Judicial para Centro América y el

2 RAMÍREZ, ALEXANDER RESTREPO. 2019. MANUAL DE AUTORES PARA EL DISEÑO Y REDACCIÓN DE MÓDULOS DE APRENDIZAJE AUTODIRIGIDO. Bogotá D.C.: CONSEJO SUPERIOR DE LA JUDICATURA, 2019. (3 pág. 5)

Caribe en el Taller sobre la Obtención de Evidencia Digital para National Center for State Courts e instructor en el programa de Formación Especializada en Informática Forense para la Oficina Regional para Centro América y el Caribe de la Naciones Unidas en ROPAN.

Es Criminalista y cuenta con posgrados en Derecho Procesal Penal, Auditoria Forense, Administración de Laboratorios de Informática Forense, Crimen Organizado, Corrupción y Terrorismo. Actualmente es consultor de la OEA, FELABAN (Federación Latinoamericana de Bancos) y UNODC para Colombia.

3.2 ÁLVARO JOSÉ MOSQUERA SUÁREZ

Ha sido director del VII Curso de Formación Judicial para Jueces y Magistrados de la República de le Escuela Judicial "Rodrigo Lara Bonilla", Gerente del Programa ReintegraTIC de la Agencia para la Reincorporación y normalización de la Presidencia de la República, Asesor Regional de Teletrabajo, Coordinador de Formación de la Subdirección de Comercio Electrónico del Ministerio TIC, Asesor Nacional de Pedagogía del Programa Computadores para Educar.

Es Magister en Comunicación, Educación y Cultura de la Universidad Autónoma de Barcelona, Especialista en Marketing Digital y Licenciado en Educación Básica con énfasis en Tecnología e Informática.

3.3. ANDRÉS MENESES OBANDO

Magíster en Derecho Informático y de las Nuevas Tecnologías, Universidad Externado de Colombia, especialista en Redes y Servicios Telemáticos, especialista en Gerencia Informática, profesional en Ingeniería de Sistemas.

Se ha desempeñado como docente de Informática jurídica, TIC asociadas al derecho, derecho informático, ingeniería de software II y III y Fundamentos de Derecho, desde la educación básica hasta la educación superior.

Durante su vida profesional ha desempeñado cargos en el Ministerio TIC, con los programas de Computadores para Educar, Revolución y En TIC Confío.

Actualmente se desempeña como perito informático, prestando sus servicios a personas naturales y jurídicas.
Ha realizado estudios de investigación en desarrollo de aplicaciones móviles, pedagogía y evidencia digital.

3.4. DANIEL RÍOS SARMIENTO

Abogado de la Universidad del Rosario y candidato a Magister de Derecho Informático y de las nuevas Tecnologías de la Universidad Externado de Colombia.

Miembro Investigador de postgrado del Centro de Investigación de Derecho Informático CIDI de la Universidad Externado de Colombia. Investigador de la Democracia

Colombiana en la sociedad del conocimiento #CyberDemocraciaCo

Programador y desarrollador certificado en el programa Full Stack y Tecnologías Hibridas por Fedesoft, MinTIC y Colciencias en el 2018. Finalista en Premios Ingenio Categoría educación FEDESOFT 2017.

Programador de Internet de las Cosas IoT, certificado por Cisco Networking Academy 2019 y certificado en Fundamentos de programación y frontend por Bogotá Institute of Tecnology Bictia.com.co 2019

Experto en Derecho de Autor, Propiedad intelectual, marcas, delitos informáticos y programas de informática forense digital trabaja actualmente como abogado externo en las firmas Ríos Sarmiento Abogados, AbogadoTIC y @CyberAbogado y profesor investigador de la Escuela Mayor de Derecho de la Universidad Sergio Arboleda.

4. JUSTIFICACIÓN

La siguiente guía de aprendizaje autodirigido trata los procedimientos técnicos de la Evidencia Digital y Prueba Electrónica (EDiPE) y se propone como una herramienta de capacitación en la normatividad relacionada en la apropiación de las Tecnologías de la Información y de las Telecomunicaciones (TIC).

El propósito de esta guía de aprendizaje es fomentar las competencias de los operadores judiciales, en fundamentos dogmáticos, técnicos y jurídicos necesarios para actualizarse en cuanto a tecnologías aplicadas a la administración de la justicia en Colombia.

Así mismo, fomenta integralmente la apropiación social del conocimiento relacionado con la evidencia digital y prueba electrónica (EDiPE) como posibles herramientas tecnológicas capaces de mejorar el desempeño en el cotidiano oficio del tratamiento de grandes volúmenes de mensajes de datos en la administración de la justicia.

Por otro lado, aclara las directrices de buenas prácticas jurídicas locales y estándares internacionales que procuren evitar cometer errores respecto a la valoración de la evidencia digital y la prueba electrónica (EDiPE), repasando la evolución normativa y las disposiciones que al respecto el Consejo Superior de la Judicatura ha emitido.

5. RESUMEN DE LA GUÍA

La presente obra expone una guía de derecho informático que profundiza integralmente el concepto de procedimientos técnicos de la EDiPE en Colombia, abordando: i) los aspectos generales de los procedimientos técnicos, ii) los procedimientos de preservación y análisis, iii) el marco normativo aplicable y iv) consideraciones para tener en cuenta en dicha materia.

6. RECOMENDACIÓN DE IMPLEMENTACIÓN

Para que tenga en cuenta él/la discente de la Guía Didáctica de aprendizaje autodirigida: esta tiene como finalidad una capacitación práctica sobre los principales procedimientos técnicos de la EDiPE.

Para cumplir dicha finalidad, se recomienda que tenga en cuenta previamente:

6.1. ¿QUÉ ES GUÍA DIDÁCTICA DE APRENDIZAJE AUTODIRIGIDO?

Constituye para la EJRLB y el Plan de Formación de la Rama Judicial, unas:

> *"herramientas con especificaciones para realizar acciones puntuales de estudio autónomo de acuerdo con los objetivos de aprendizaje, recursos y material disponible en una Unidad, Curso/MAA o Diplomado. La GDAA presenta un plan para el desarrollo del curso/módulo; un calendario que organiza sesiones de trabajo virtual (foros), presencial (talleres, conversatorios, mesas de trabajo grupal), y da pautas sobre la consulta de material primario (necesario) o secundario (complementario), es decir, representa una operacionalización del plan de formación."* [3]

En el caso concreto de la Guía Didáctica de Aprendizaje Autodirigido de Evidencia Digital y Prueba Electrónica en Colombia N° 2. Procedimientos técnicos se compone de la siguiente manera:

3 Ibidem (3 pág. 47)

Tabla 4. Modelo guía aprendizaje

<table>
<tr><th>ÍTEM</th><th colspan="3">DESCRIPCIÓN</th></tr>
<tr><td>Procedimientos Técnicos</td><td colspan="3">Guía Didáctica de Aprendizaje Autodirigido de Evidencia Digital y Prueba Electrónica N° 2. Procedimientos técnicos.</td></tr>
<tr><td rowspan="2">Objetivos: ¿para qué?</td><td rowspan="2">Nivel de Formación</td><td rowspan="2">SABER SER</td><td>Apropiar
Fundamentos legales y axiológicos de la Evidencia Digital y Prueba Electrónica en el ámbito judicial.</td></tr>
<tr><td>Apropiar
Instrumentos técnicos y jurídicos que permiten dar certeza al Juez respecto a la integridad de la evidencia digital tales como imagen forense, certificados digitales, estampas cronológicas, firmas digitales, algoritmos.</td></tr>
<tr><td>Requisitos previos:</td><td colspan="3">Lectura de unidad 9 de la Guía Didáctica de Aprendizaje Autodirigido de Evidencia Digital y Prueba Electrónica en Colombia N° 2. Procedimientos técnicos.</td></tr>
<tr><td>Contenidos:</td><td colspan="3">Subtema 2.1: Preservación de la Evidencia Digital y la Prueba Electrónica
Subtema 2.2: Importancia de realizar una imagen forense digital
Subtema 2.3: Conceptos erróneamente utilizados para referirse a las imágenes forense digital
Subtema 2.4: Precedente mala práctica de recolección de mensajes de datos
Subtema 2.5: Cadena de custodia de la Evidencia Digital y Prueba Electrónica
Subtema 2.6: Métodos de Autenticación del Mensaje de Datos
Subtema 2.7: Los Metadatos
Subtema 2.8: Obtención de la línea de tiempo de la Evidencia Digital y Prueba Electrónica
Subtema 2.9: Escenarios de obtención de Mensajes de datos
Subtema 2.10: Informática forense aplicada a la Evidencia Digital y Prueba Electrónica
Subtema 2.11: Método jurisprudencial para determinar fuerza probatoria de mensajes de datos en un proceso judicial
Subtema 2.12: Técnicas antiforenses</td></tr>
<tr><td>Estrategias metodológicas: ¿Cómo?</td><td colspan="3">• Análisis y estudio de casos</td></tr>
</table>

ÍTEM	DESCRIPCIÓN
Actividades: ¿Qué hacer?	**Análisis de casos por Grupos** Acorde a número de participantes, se divide en grupos de cincuenta por ciento (50%) cada uno, para analizar los casos Lectura de la Guía Didáctica de Aprendizaje Autodirigido de Evidencia Digital y Prueba Electrónica en Colombia N° 2. Procedimientos Técnicos. Cada grupo debe resolver el caso defendiendo una postura contraria, basados en la lectura de Unidad 9. de la Guía Didáctica de Aprendizaje Autodirigido de Evidencia Digital y Prueba Electrónica en Colombia N° 2. Procedimientos Técnicos. Se espera que la división por grupos permita ampliar el conocimiento sobre la ruta hermenéutica utilizada para resolver el caso, incluso, no se descarta que haya de manera motivada una desviación de la ruta jurisprudencial propuesta.
Recursos: ¿Qué usar?	Esta información debe ser proporcionada por los facilitadores conforme con la disponibilidad y la logística de cada Plan de Formación.
Temporalización: ¿Cuándo?	**Curso de formación inicial (Curso Concurso de Méritos):** una (1) sesión de ocho (8) horas (Reunión Inicial y Conversatorio local).
Evaluación: ¿qué, cuándo, cómo, con quién y para qué?	Valoración cuantitativa y cualitativa de lo aprendido, destrezas implementadas, habilidades adquiridas, actitudes demostradas, en la resolución de los casos: Lectura Unidad 9 de la Guía Didáctica de Aprendizaje Autodirigido de Evidencia Digital y Prueba Electrónica en Colombia N° 2. Procedimientos Técnicos Para que aplique integralmente los procedimientos técnicos de la Evidencia Digital y Prueba Electrónica en Colombia.

Fuente: Elaboración propia con base en el MANUAL DE AUTORES PARA EL DISEÑO Y REDACCIÓN DE MÓDULOS DE APRENDIZAJE AUTODIRIGIDO DE LA ESCUELA JUDICIAL RODRIGO LARA BONILLA 2019.

7. MISIÓN Y OBJETIVOS DE LA GUÍA

7.1. MISIÓN

Capacitar a él/la discente en la aplicación de los Procedimientos Técnicos de Evidencia Digital y Prueba Electrónica en Colombia: incluyendo una Unidad sobre principios relacionados con el uso Ético Judicial de la EDiPE.

7.2. OBJETIVO GENERAL DE LA GUÍA

Proporcionar a él/la Discente, herramientas de aprendizaje orientadas a potenciar los conocimientos, habilidades y destrezas para desempeñar de forma eficiente y eficaz sus funciones, mediante la realización de procesos de formación y capacitación, promoviendo su desarrollo integral para el mejoramiento de la Administración de Justicia.

7.3. OBJETIVOS ESPECÍFICOS DE LA GUÍA DIDÁCTICA DE APRENDIZAJE AUTODIRIGIDO

7.3.1. Apropiar

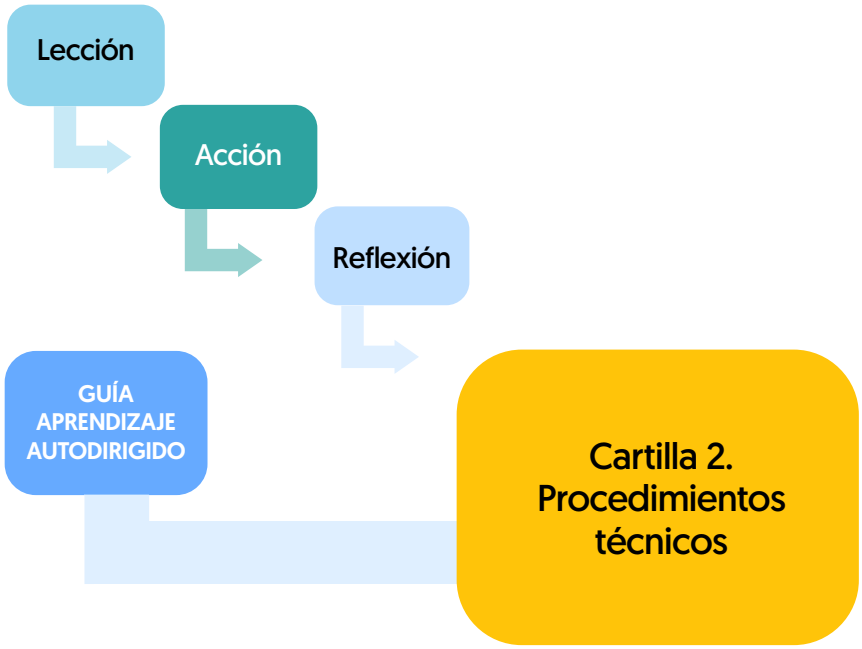
Fundamentos legales y axiológicos de la EDiPE en el ámbito judicial.

7.3.2. Apropiar

Instrumentos técnicos y jurídicos que permiten dar certeza al Juez respecto a la integridad de la evidencia digital tales como imagen forense, certificados digitales, estampas cronológicas, firmas digitales, algoritmos.

8. MAPA CONCEPTUAL DE LA GUÍA

Ilustración 1. Mapa conceptual Guía de Aspectos Generales de la EDiPE



Fuente: Elaboración propia.

9. PROCEDIMIENTOS TÉCNICOS DE LA EVIDENCIA DIGITAL Y PRUEBA ELECTRÓNICA

A continuación, encontrará los principales aspectos técnicos y jurídicos para tener en cuenta para preservar la evidencia digital, a saber:

9.1. PRESERVACIÓN

9.1.1. Imagen Forense

La adquisición de una imagen forense se conoce como "imaging" (obtención de imágenes forenses de datos) y se refiere al proceso mediante el cual se realiza una copia exacta del dispositivo de almacenamiento donde reposa la información electrónicamente almacenada que llegará a tener vocación probatoria en el desenlace del proceso.

Este mismo procedimiento se debe realizar respecto a repositorio de tipo lógico como carpetas que contienen archivos o mensajes de datos.

Ilustración 2. Realización de imagen forense

Fuente: Edición propia

El procedimiento de obtención de imágenes forenses en el contexto de la informática forense es muy diferente del que utiliza normalmente cualquier usuario informático para realizar copias electrónicas de un archivo.

En primer lugar, hay una diferencia metodológica. Para la obtención de imágenes forenses de datos es necesario un programa forense específico y que éste sea utilizado por personas con conocimientos de informática forense.

En el modelo relacional propuesto se incorporan 5 elementos necesarios para la realización de una imagen forense:

9.1.2. Equipo de origen o "Sospechoso"

Se refiere al dispositivo (disco duro) donde se encuentra la información electrónicamente almacenada, que al ser recolectada a través del proceso de imagen refleja una copia idéntica o exacta bit a bit de la información allí contenida.

9.1.3. Bloqueador de lecto/escritura

Se refiere a los dispositivos de hardware empleados para que el experto que accede a la información no contamine la información y evita que se generen cambios como modificaciones en las fechas de último acceso a la evidencia. Ver detalle (Kit de bloqueador para disco duro).

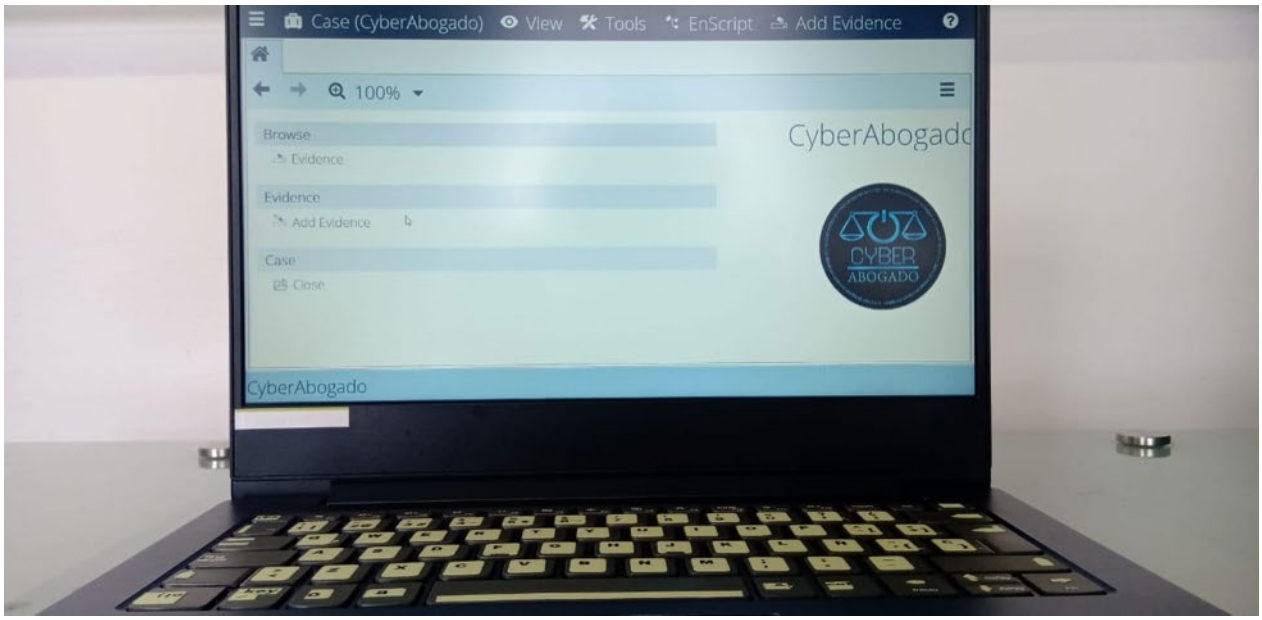
Ilustración 3. Bloqueador de Lecto escritura

Fuente: Edición propia

9.1.4. Equipo Experto

Todo especialista forense debe disponer de un equipo con una configuración robusta que le permita instalar los programas que digitalizarán la imagen forense y gestionen el proceso de volcado de datos o generación de la imagen. Ver detalle Equipo Portátil Utilizado por Especialista Forense.[4]

Ilustración 4. Equipo experto @CyberAbogado



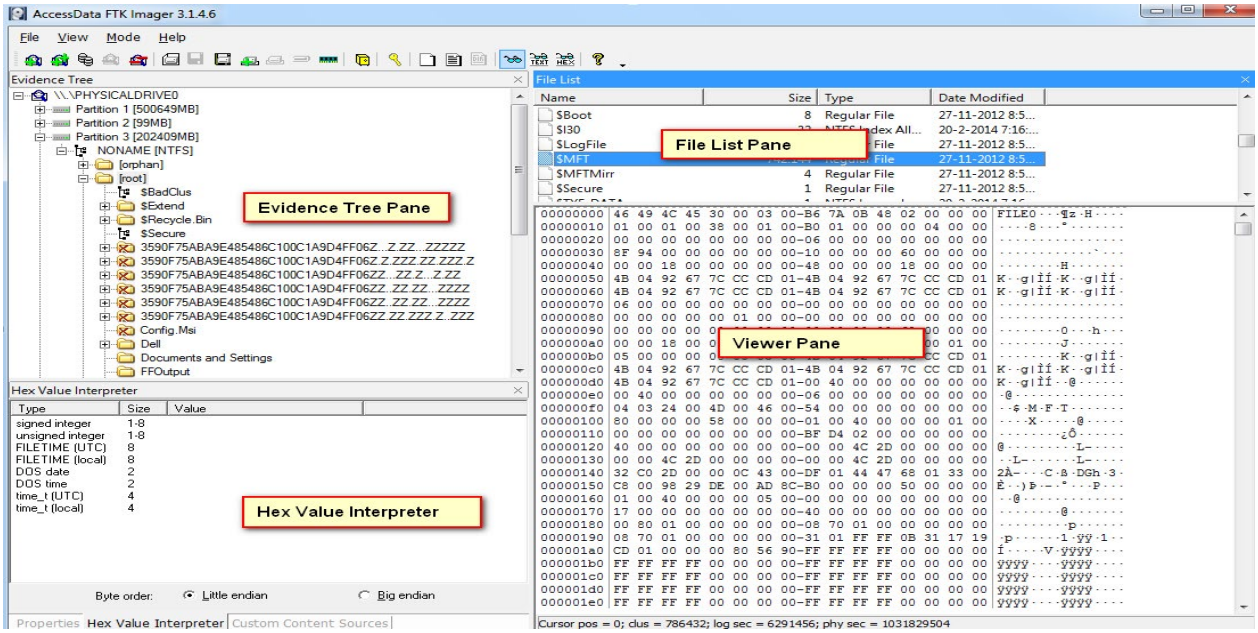
Fuente: Elaboración propia.

4 [3] Inc, Digital Intelligence. YouTube. YouTube. [En línea] Digital Intelligence Inc, 8 de febrero de 2018. [Citado el: 22 de enero de 2020.] https://www.youtube.com/watch?v=FJF0WezsS2k&feature=youtu.be.

9.1.5. Software de digitalización de Imagen Forense Digital

Los programas más utilizados por la comunidad científica internacional son FTK Forensic ToolKit de la casa fabricante Access Data y Encase ®, generalmente los gabinetes privados de informática forense y los laboratorios nacionales de las entidades públicas los utilizan en sus actuaciones. Estos programas permiten realizar el copiado de la información y generar la imagen. A continuación, se muestra una interfaz gráfica del programa forense FTK IMAGER

Ilustración 5. Pantallazo Front Software FTK IMAGER



Fuente: FTK IMAGER SOFTWARE [5]

9.1.6. Disco de Destino o Dispositivo de Almacenamiento

Aquellos componentes lógicos de software y hardware capaz de almacenar la imagen forense, la cual debe estar debidamente sanitizados, o sometidos a borrado seguro, y que está dispuesto a que en él se almacene la imagen forense: Estos dispositivos digitales deben ser iguales o de mayor tamaño que el disco de origen.

Ahora bien, en segundo lugar, la naturaleza de la copia es diferente. Con el proceso de "imaging" se obtiene una copia exacta del disco duro: una copia imagen forense es una copia exacta y a tamaño natural de todos los contenidos y de la estructura de un soporte o un dispositivo de almacenamiento, como un disco duro, una llave USB, un CD o un DVD.

Normalmente se genera un archivo con la copia imagen que está basada en los sectores del soporte (copia de la secuencia de bits), sin tener en cuenta su sistema de archivos. Como tal, la copia imagen contiene toda la información necesaria para reproducir exactamente la totalidad de la estructura y todos los contenidos de un dispositivo de almacenamiento.

5 (4) (Accessdata, 2019)

Como lo describimos en el modelo relacional para la obtención de imágenes forenses de datos es necesario tomar unas precauciones específicas, para lo que se utilizan bloqueadores de escritura o write blockers, con objeto de garantizar que durante ese proceso no se produzca ninguna modificación en la prueba instrumental original.

Ilustración 6. Bloqueador conectado Disco Origen

Fuente: Elaboración propia.

Ilustración 7. Adaptadores para bloqueadores

Fuente: Elaboración propia.

Uno de los principales errores que se cometen por parte de quienes realizan el proceso de recolección de la evidencia digital es el de acceder a el dispositivo origen/sospechoso sin la protección de los bloqueadores de escritura, de tal manera que se consideran como una mala práctica el conectar directamente, por ejemplo un dispositivo USB o similar, al dispositivo origen/sospechoso con la finalidad de copiar los archivos de interés o los mensajes de datos que finalmente se aportarán, sin hacer uso de los dispositivos bloqueadores.

Dada la multiplicidad de dispositivos y los diferentes conectores USB 3.0, ATA, SATA, IDE, SCSI, ZIP, entre otros, los especialistas disponen de variados adaptadores como los observados en la ilustración 7.

La tercera diferencia respecto al copiado normal de información es que la obtención de imágenes forenses lleva asociado un proceso de validación para determinar si la imagen es o no completamente idéntica a la original. Para ello se comparan los valores de hash.

Un valor de hash es una secuencia de números y caracteres generada al utilizar un algoritmo concreto. El valor se genera en función de los datos que figuran en el computador y es absolutamente único para cada dispositivo de almacenamiento.

Al comparar los valores hash generados desde el original con los generados desde la copia, los analistas forenses pueden determinar si la copia está bien hecha.

Si ambos valores coinciden, la copia se ha realizado correctamente; si no coinciden, es necesario repetir todo el proceso.

Ilustración 8. Valores Hash de una imagen forense

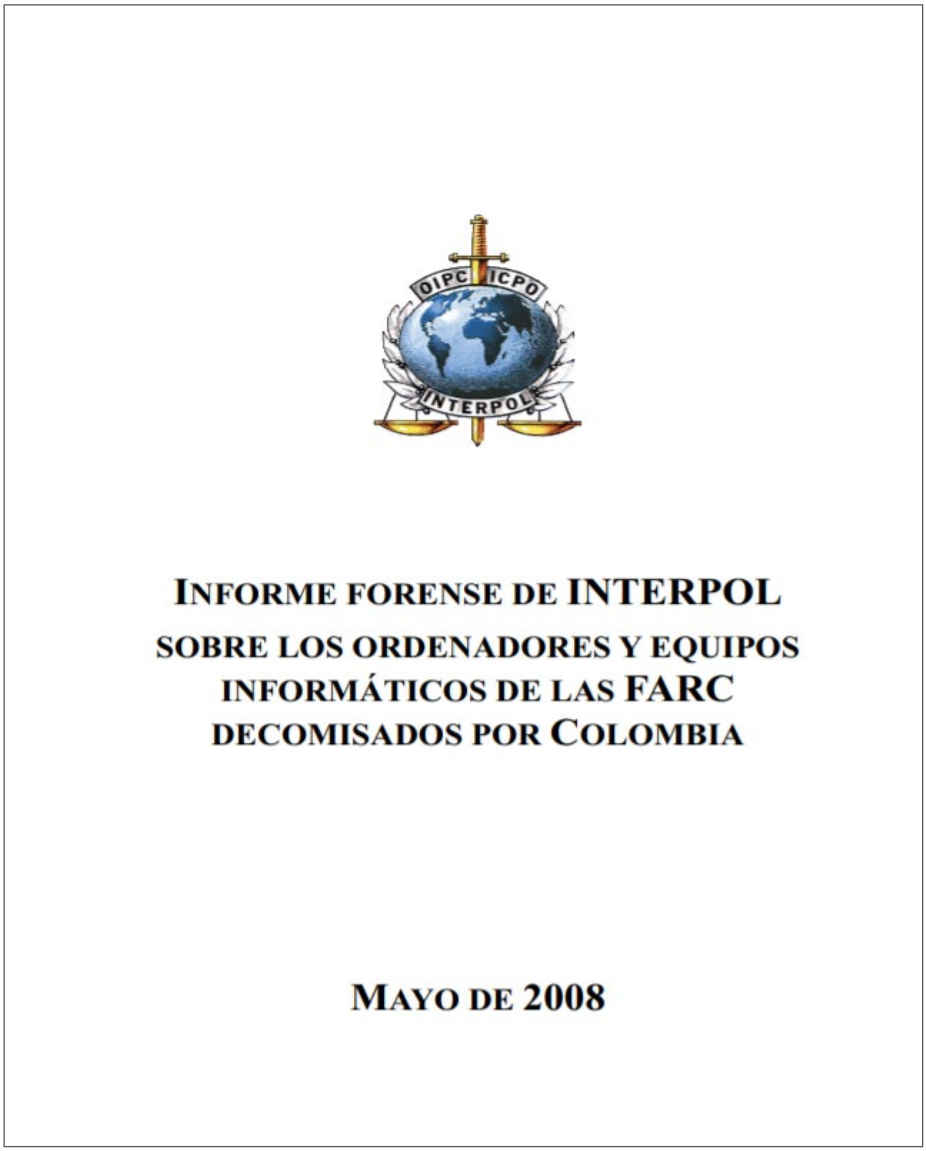
```
[Computed Hashes]
 MD5 checksum:    61b0c589c1477f57dfd7d4d94ef05458
 SHA1 checksum:   d2fcf477e2ff90faedc81c4a5769ad647ff1ac65

Image Information:
 Acquisition started:   Tue Dec 10 06:46:35 2019
 Acquisition finished:  Tue Dec 10 06:51:18 2019
 Segment list:
  C:\Users\Cr. Fredy Bautista\Desktop\imagen forense usb verbatim\imagen forense caso3.E01

Image Verification Results:
 Verification started:  Tue Dec 10 06:51:18 2019
 Verification finished: Tue Dec 10 06:51:38 2019
 MD5 checksum:    61b0c589c1477f57dfd7d4d94ef05458 : verified
 SHA1 checksum:   d2fcf477e2ff90faedc81c4a5769ad647ff1ac65 : verified
```

Fuente: Elaboración propia.

Más adelante se profundizará acerca del valor hash y su importancia en el contexto probatorio.

9.2. IMPORTANCIA DE REALIZAR UNA IMAGEN FORENSE DIGITAL

Ilustración 9. Portada Informe Forense INTERPOL 2008



Fuente: Informe INTERPOL 2008 LINK: http://static.eluniversal.com/2008/05/15/infointerpol.pdf

Como lo describimos en el modelo relacional para la obtención de imágenes forenses de datos es necesario tomar unas precauciones específicas, para lo que se utilizan bloqueadores de escritura o write blockers, con objeto de garantizar que durante ese proceso no se produzca ninguna modificación en la prueba instrumental original.

> *"Estas diligencias tuvieron por génesis el hecho que el 1 de marzo de 2008, la Fuerza Pública realizó un operativo contra la guerrilla de las "FARC", donde murió el guerrillero LUIS ÉDGAR DEVIA SILVA (a. RAÚL REYES) y entre sus enseres fueron encontrados computadores, discos duros y USB"* [6]

Luego de la solicitud de asistencia y cooperación internacional policial, solicitada por el Estado colombiano a través de la cancillería a la Secretaria General de INTERPOL, con el fin de acreditar el trabajo realizado por las autoridades policiales en el caso precitado, este organismo internacional asistió con la entrega del denominado Informe Forense de Interpol en el que se relacionan los hallazgos más importante desde el punto de vista técnico mencionados por los expertos en las conclusiones del informe.

Para efectos de esta guía se citará la conclusión No 2b que señala lo siguiente:

> *"Entre el 1 de marzo de 2008, fecha en que las autoridades colombianas incautaron a las FARC las ocho pruebas instrumentales de carácter informático, y el 3 de marzo de 2008 a las 11.45 horas, momento en que dichas pruebas fueron entregadas al Grupo Investigativo de Delitos Informáticos de la Dirección de Investigación Criminal (DIJIN) de Colombia, el acceso a los datos contenidos en las citadas pruebas no se ajustó a los principios reconocidos internacionalmente para el tratamiento de pruebas electrónicas por parte de los organismos encargados de la aplicación de la ley."* [7]

Y la conclusión No. 3 que indica:

> *"Asimismo, el análisis informático forense de INTERPOL confirmó que, según habían reconocido las fuerzas del orden colombianas, el acceso a los datos contenidos en las citadas ocho pruebas instrumentales realizado entre el 1 de marzo de 2008, fecha en que fueron decomisadas por las autoridades colombianas, y el 3 de marzo de 2008 a las 11.45 horas, momento en que fueron entregadas al Grupo Investigativo de Delitos Informáticos de la policía judicial colombiana, no se realizó conforme a los principios reconocidos internacionalmente aplicables al manejo ordinario de pruebas electrónicas por parte de los organismos encargados de la aplicación de la ley. Esto es, en lugar de tomar el tiempo necesario para hacer copias protegidas contra la escritura de cada una de las ocho pruebas instrumentales decomisadas antes de acceder a ellas, este acceso se hizo directamente."* [8]

6 INTERPOL. eluniversal.com. [En línea] 2008. http://static.eluniversal.com/2008/05/15/infointerpol.pdf. [5 pág. 8]
7 Ibidem [5 pág. 8]
8 Ibidem [5 pág. 9]

9.3. CONCEPTOS ERRÓNEAMENTE UTILIZADOS PARA REFERIRSE A LAS IMÁGENES FORENSE DIGITAL

Tabla 5. Términos erróneos respecto de la Imagen Forense Digital

Término	Descripción	Usos
Back Up o respaldo de información	En informática (ver definición aquí: https://concepto.de/informatica/), se entiende por un *backup (del inglés: back up, "respaldo", "refuerzo")*, respaldo, copia de seguridad o copia de reserva a una copia de los datos originales de un sistema de información o de un conjunto de software (ver definición aquí: https://concepto.de/software/) (archivos, documentos, etc.) que se almacena en un lugar seguro o una región segura de la memoria del sistema.	Al no realizarse con fines forenses, un Back Up se utiliza con el fin de poder volver a disponer de la información en caso de alguna eventualidad, accidente o desastre ocurra y ocasione su pérdida del sistema (ver definición aquí: https://concepto.de/sistema-de-informacion/.) Es decir, ayuda a recuperarse por ejemplo de un evento de Ransomware.
Clonación de disco o copia espejo	La clonación de discos es el proceso de copiar los contenidos de un disco duro (ver definición aquí: https://es.wikipedia.org/wiki/Unidad_de_disco_duro) de una computadora (ver definición aquí: (https://es.wikipedia.org/wiki/Computadora) a otro disco o a un archivo (ver definición aquí: https://es.wikipedia.org/wiki/Archivo_(informática)) imagen (ver definición aquí: https://es.wikipedia.org/wiki/Imagen_ISO.) El procedimiento es útil para cambiar a un disco diferente o para restaurar el disco a un estado previo.	**Reinicio y restauración –.** Se usa en ciertos cibercafés e institutos educativos y de entrenamiento y sirve para asegurarse ante: i) la posible desconfiguración del equipo ii) los efectos ocasionados por bajar programas iii) contenidos inapropiados iv) infecte a la computadora con un virus, v) esta será restaurada a un estado limpio y de trabajo pleno. **Equipamiento de nuevas computadoras** **Actualización del disco duro –** Un usuario individual puede utilizar la copia del disco (clonación) para pasar a un nuevo disco duro, a veces incluso de mayor capacidad. **Copia de seguridad de todo el sistema –** Un usuario puede crear una copia de seguridad (ver definición aquí: https://es.wikipedia.org/wiki/Copia_de_seguridad) completa de su sistema operativo y de los programas instalados. Recuperación del sistema Transferencia a otro usuario.

Término	Descripción	Usos
Copiado de Seguridad o copia de información	También conocidas como copia de respaldo, se refieren a los BackUp.	Usos del referido BackUp

Fuente: Elaboración propia.

9.4 PRECEDENTE MALA PRÁCTICA DE RECOLECCIÓN DE MENSAJES DE DATOS

El caso refiere a la aplicación del documento RFC 3227[9] que establece lineamientos técnicos que enseñan que NO se debe iniciar (encender) el computador o sistema que contiene la información almacenada toda vez que independientemente del sistema operativo que se utilice, al encender el ordenador se producen modificaciones de ciertos datos del disco duro que afectan el principio de integridad de la prueba.

Aunque puedan ser invisibles e irrelevantes para el usuario, estas operaciones del sistema son importantes para los expertos forenses, porque ellos no sólo analizan los archivos de usuario, tales como los documentos de texto y los archivos de imagen y sonido, sino también los datos ocultos y la información contenida en los archivos de sistema, por ejemplo, la información que el ordenador genera "automáticamente" cuando trata la información.

Esta situación igualmente fue referida en el Informe de INTERPOL del mediático caso "Los Computadores de Raúl Reyes", la mención a esta mala práctica quedó consignada en la Conclusión no 3 del informe que expone lo siguiente:

> *"INTERPOL no ha encontrado indicios de que, tras la incautación a las FARC de las ocho pruebas instrumentales de carácter informático, efectuada el 1 de marzo de 2008 por las autoridades colombianas, se hayan creado, modificado o suprimido archivos de usuario en ninguna de dichas pruebas. El acceso directo entre el 1 y el 3 de marzo de 2008 a las ocho pruebas instrumentales de carácter informático decomisadas a las FARC dejó rastros en los archivos de sistema, como ya se ha explicado.*[10]

Aquellos rastros que indica el informe son huellas de alteraciones lógicas al archivo original, lo cual de cierta manera se puede interpretar como modificación de la composición del Mensaje de Datos MD, dicha huella no debió producirse, existen herramientas metodológicas para ello, se trata del bloqueo y realizar una copia imagen forense del equipo incautado.

9 (Véase Documento RFC 3227 en el siguiente enlace: https://tools.ietf.org/html/rfc3227)
10 Ibidem (5 pág. 35)

No obstante, los especialistas de INTERPOL no encontraron en ninguna de las ocho pruebas archivo de usuario alguno que hubiera sido creado, modificado o suprimido con posterioridad al decomiso, practicado el 1 de marzo de 2008. Utilizando sus herramientas forenses, los especialistas hallaron un total de 48.055 archivos cuyas marcas de tiempo indicaba que habían sido creados, abiertos, modificados o suprimidos como consecuencia del acceso directo a las ocho pruebas instrumentales por parte de las autoridades colombianas entre el momento del decomiso de éstas, el 1 de marzo de 2008, y el 3 de marzo de 2008 a las 11.45 horas." [11]

En términos generales la imagen forense es el procedimiento técnico mediante el cual se garantiza la condición de integridad de la evidencia digital, entendiendo entonces que no realizarla puede generar cambios a la información allí almacenada, dichas alteraciones deben ser reflejadas mediante informe de un especialista forense que identifica accesos a los archivos y las consecuentes modificaciones.

Las imágenes forenses pueden realizarse a carpetas y archivos cuando se requiere presentar e incorporar a la actuación judicial uno o varios archivos contenidos en estas ubicaciones de tipo lógico.

9.5. CADENA DE CUSTODIA DE LA EVIDENCIA DIGITAL Y PRUEBA ELECTRÓNICA

La Cadena de Custodia se ha definido en Colombia, como el conjunto de procedimientos encaminados a asegurar y demostrar la autenticidad de los elementos materiales probatorios y evidencia física.

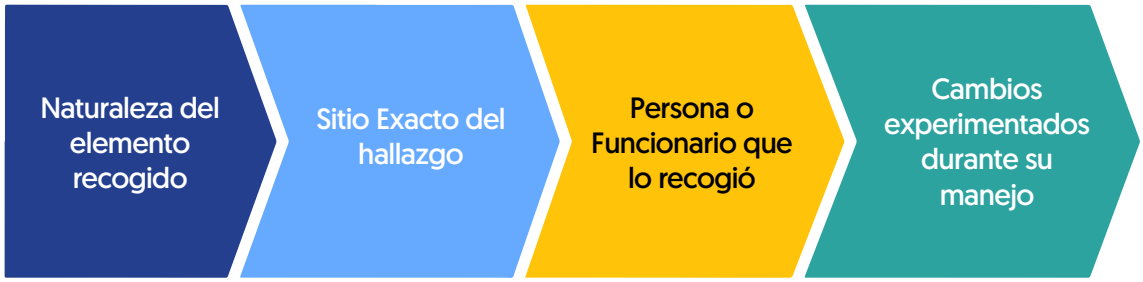
Este conjunto de procedimientos es realizado por él/la Discente y personas cuya responsabilidad, en un proceso judicial, es aportar elementos de convicción que respalden la validez integral de la prueba y certifique que se cumplió con los estándares técnicos y jurídicos en la totalidad de las etapas del proceso.

Este procedimiento inicia con la actuación de un funcionario que representa a la autoridad encargada de recolectar los mensajes de datos que se pretendan hacer valer como medios de prueba, desde el momento en que un juez competente ordena la recolección y finaliza con el fallo de sentencia expedido por el juez que ordenó la recolección del material, con el fin de determinar si es válida o no, en otras palabras, si ese material recopilado demuestra la existencia de un hecho, acto o contrato.

La siguiente gráfica representa los pasos que debe tener en cuenta él/la discente que colecta el material y que sin los cuales, la recolección sería en vano debido a que sería rechazada por no cumplir con el debido proceso de cadena de custodia.

11 Ibidem (5 pág. 33)

Ilustración 10. Proceso de Cadena de custodia



Fuente: Elaboración propia

No se requiere de mayores esfuerzos intelectivos para comprender que el proceso de embalaje y rotulación del elemento y, en general, el protocolo de cadena de custodia es mucho más relevante cuando se trata de material confundible o alterable, que frente a aquel que es identificable a simple vista por sus características externas, o las que son susceptibles de ser marcadas y han sido sometidas a este procedimiento como forma de identificación.

En evidencia digital la cadena de custodia ha sido uno de los mayores desafíos de orden legal y técnico, pues la escasa preparación de algunos intervinientes en la interacción con las fuentes de evidencia ha ocasionado que, en la mayoría de los casos, no se registren debidamente los datos que permiten construir la continuidad de la custodia, o tratamiento de la material o mensaje de datos.

Algunos de los errores que la experiencia permite identificar como recurrentes son los siguientes:

9.5.1. Error por no uso de White blokers o bloqueadores de escritura

Acceder a la evidencia sin el debido cuidado de elementos de bloqueo de escritura, lo anterior ocasiona cambios a las fechas de acceso, modificación y lectura de los archivos o mensajes de datos.

Esta mala práctica genera dudas en el operador judicial al momento de establecer la integridad de la evidencia a valorar.

9.5.2. Error por desincronización de la estampa cronológica

Los relojes de los equipos anfitriones que generan la evidencia o mensaje de datos no tienen sincronizada la hora estándar para Colombia y los registros de copiado forense o de imagen explicados en la cartilla dos (2) sobre procedimientos contendrán fechas erróneas o que no corresponden a la temporalidad de la actuación.

Este error da al traste con la condición de trazabilidad, tratada en la cartilla 1 de aspectos generales, debido a que no se consignan los datos de horas y fechas o no se dejan el debido registro en el informe técnico.

9.5.3. Error por Corrupción

Otros eventos se encuentran vinculados a actos de corrupción de los funcionarios encargados de la custodia del material recopilado, existen antecedentes que desafortunadamente dan cuenta de

irregularidades que afectan directamente la integridad de la prueba y por ende causan la pérdida total de validez en un proceso judicial.

Las irregularidades causan pérdidas, cambios parciales de los contenedores de hardware (Computadores, Discos Duros, SSD, USB) y/o destrucción total.

Ejemplo de las irregularidades las podemos identificar en el caso mediático documentado en Prensa de la siguiente manera: (EL PAÍS CALI. (2014). Dos detenidos por robo en almacén de evidencias de la Fiscalía de Cali. 19/12/2019, de DIARIO EL PAÍS CALI Sitio web: https://www.elpais.com.co/judicial/dos-detenidos-por-robo-en-almacen-de-evidencias-de-la-fiscalia-de-cali.html)

9.6. MÉTODOS DE AUTENTICACIÓN DEL MENSAJE DE DATOS

Una de las causas más comunes por las cuales se rechazan los materiales recopilados o se cuestiona severamente su admisibilidad por irregularidades en poder demostrar su autenticidad, es porque se omite utilizar las técnicas para tal fin.

La comunidad científica internacional reconoce como válidos los siguientes procedimientos

Ilustración 11. Método de autenticación de mensaje de datos

Fuente: Elaboración propia.

9.6.1. Certificados Digitales

La definición técnica de:

"Los certificados digitales permiten la identificación exclusiva de una entidad; en esencia, son tarjetas de identificación electrónica emitidas por compañías de confianza. Los certificados digitales permiten a un usuario verificar a quién se ha emitido un certificado, así como el emisor del certificado. Los certificados digitales son el vehículo que SSL utiliza para la criptografía de clave pública. La criptografía de clave pública utiliza dos claves criptográficas diferentes: una clave privada y una clave pública. La criptografía de clave pública también se conoce como criptografía asimétrica, porque puede cifrar la información con una clave y descifrarla con la clave complementaria desde un par de claves pública-privada determinado."[12]

9.6.2. Valor HASH

Las funciones criptográficas hash se utilizan para asegurar la integridad de los mensajes, en pocas palabras, para estar seguros de que algunas comunicaciones o archivos no fueron alterados de alguna forma, se pueden examinar los valores hash creados antes y después de la transmisión de los datos.

12 (IBM, 2019) (IBM. (2019). CERFIFICADOS DIGITALES. 18/12/2019, de IBM Sitio web: https://publib.boulder.ibm.com/tividd/td/TRM/SC23-4822-00/es_ES/HTML/user276.htm) (6 pág. Parrafo 1)

Si los dos valores hash son idénticos, significa que no ha habido ninguna alteración y las funciones criptográficas hash se utilizan también para asegurar la integridad de los mensajes de datos que se proponen como material probatorio de un hecho, acto o contrato jurídicamente relevante.

9.6.2.1. SHA 1

Es uno de los estándares de valor hash más usados en el mundo y referente de valor probatorio, significa Algoritmo de hash seguro en inglés y fue publicado por el Instituto Nacional de Normas y Tecnología, INNT (NIST en idioma inglés) de EE. UU. en 1995.

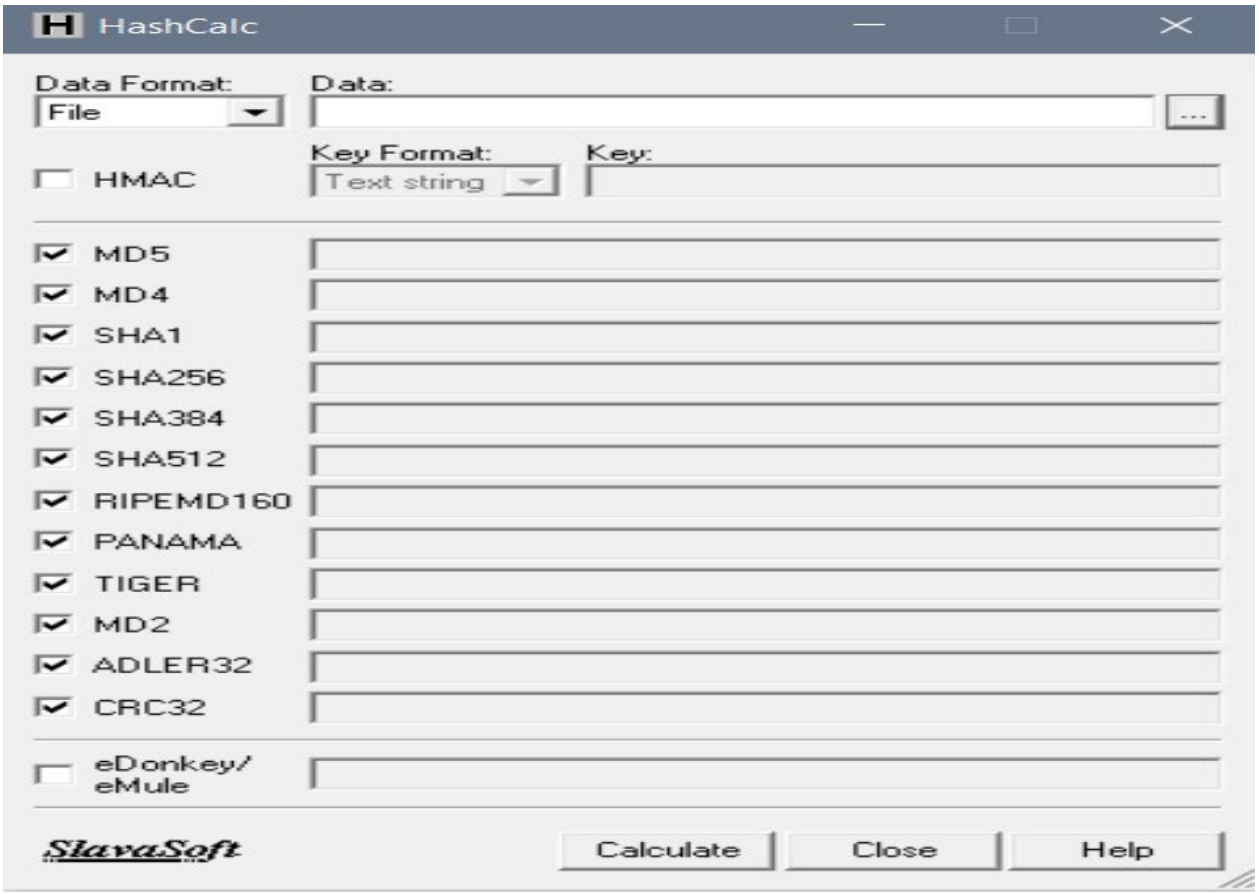
9.6.2.2.MD5

Es uno de los estándares de valor hash más usados en el mundo y referente de valor probatorio, significa Algoritmo de Resumen de Mensajes por sus siglas en inglés, y es un algoritmo de reducción criptográfico de 128 bits.

9.6.2.3.Algoritmos complementarios

Así mismo, existen otros protocolos que también se pueden tener en cuenta al momento de aplicar un valor hash, el programa software especializado HASHCALC, los retrata de la siguiente manera en su interfaz gráfica:

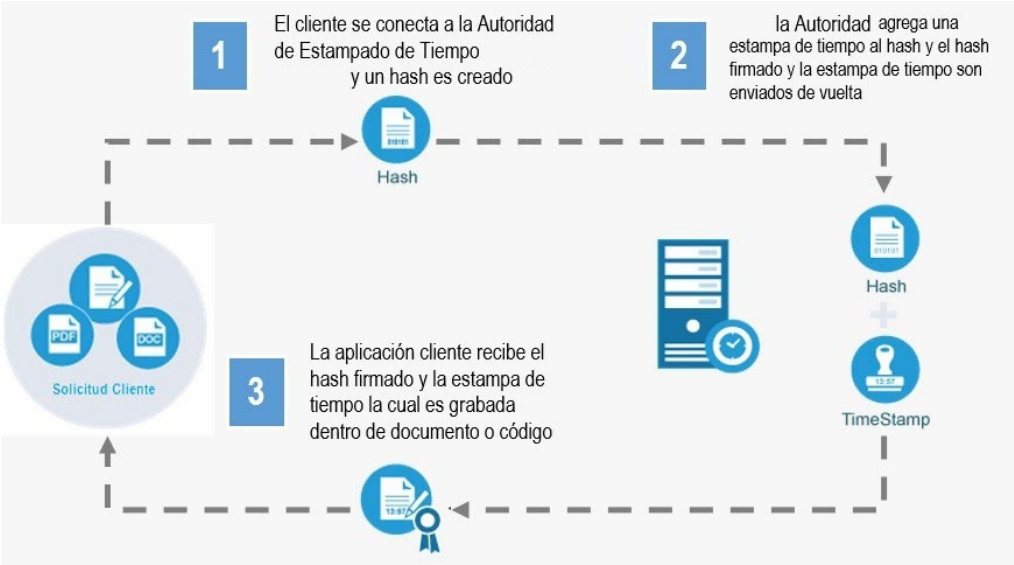
Ilustración 12. Algoritmos complementarios de Valor Hash de Software HASHCALC



FUENTE: (SlavaSoft Inc.. (2019). SlavaSoft Inc.. 19/12/2019, de SlavaSoft Inc. Sitio web: http://www.slavasoft.com/?source=HashCalc.exe)

9.6.3 Estampado cronológico

Ilustración 13. Proceso de estampado cronológico



Fuente: Página IETF.org

No existe consenso frente a la obligación o necesidad de introducir un estampado cronológico, sin embargo, hacerlo puede considerarse una buena práctica, y puede tener entre otros los siguientes usos:

(i) Un usuario quiere obtener un sello de tiempo para un documento electrónico que él posee;

(ii) Un resumen digital (técnicamente un hash) se genera para el documento en el computador del usuario;

(iii) Este resumen forma la solicitud que se envía a la entidad de certificación que presta el servicio de estampado cronológico;

(iv) La entidad de certificación que presta el servicio de estampado cronológico genera un sello de tiempo (o estampa cronológica) con esta huella, la fecha y hora obtenida de una fuente fiable y la firma digital. De esta manera, al estampar cronológicamente esta representación resumida del documento, lo que realmente se está haciendo es sellar el documento original;

(v) El sello de tiempo se envía de vuelta al usuario; y **(vi)** La entidad de certificación que presta los servicios de estampado cronológico mantiene un registro de los sellos emitidos para su futura verificación.

Ilustración 14. Estampado digital

Tipo de estandar	Enlace de instrumento
RFC 3628	http://www.rfcarchive.org/getrfc.php?rfc=3628
Protocolo TSP (Time-Stamp Protocol)	http://www.rfcarchive.org/getrfc.php?rfc=3161
RFC 4810. Cómo preservar la información a largo plazo	https://www.rfc-editor.org/rfc/rfc4810.html

"El estampado cronológico es un servicio mediante el cual se puede garantizar la existencia de un documento (o mensaje de datos en general) en un determinado tiempo. Mediante la emisión de una estampa de tiempo es posible garantizar el instante de creación, modificación, recepción, etc., de un determinado mensaje de datos impidiendo su posterior alteración.

Las Estampas Cronológicas Certificadas emitidas por Certicámara cumplen con el estándar TSA (Time Stamp Authority) descrito en los documentos RFC 3628 y 3161. Igualmente, cumple con los estándares establecidos por la Ley 527 de 1999.

La información contenida en la estampa cronológica certificada proporciona 3 datos:
Tiempo del día: expresado en hora, minuto y segundo (hh : mm : ss) de acuerdo con el Sistema Internacional de Medidas

Fecha: expresada en día, mes y año (dd : mm : aaaa)
Firma de los datos realizada con el certificado de Certicámara.

En Colombia las empresas certificadoras pueden a través de a proporciona los valores asignados al tiempo del día y la fecha con base en la hora legal de la República de Colombia tomada directamente de los patrones de referencia del Laboratorio de Tiempo y Frecuencia de la Superintendencia de Industria y Comercio.

Los valores asignados al tiempo del día y la fecha de una estampa cronológica certificada no tienen en cuenta ni aplican en ningún caso los valores que el sistema informático del solicitante señale y ningún tercero puede cambiar o solicitar la aplicación de valores distintos de tiempo del día y fecha." [13]

13 BOGOTÁ, CAMARA DE COMERCIO DE. Camara Comercio Bogotá 19/12/2019, . Firma digital y estampado cronológico. [En línea] 2019. https://www.ccb.org.co/Inscripciones-y-renovaciones/Registro-Unico-de-Proponentes/Tramites-virtuales-del-Registro-Unico-de-Proponente. [7 pág. 2]

9.6.4. Certificados digitales

Las Entidades de Certificación Digital son TERCEROS DE CONFIANZA que se dedican a la prestación de servicios de certificación digital, a través de un Sistema de Certificación Digital.

De acuerdo con la ley .527 de 1999, art. 30, las entidades de Certificación autorizadas para operar en Colombia prestan, entre otros, los servicios de estampado cronológico o sello de tiempo. El aumento de uso de documentos electrónicos y la necesidad de establecer relaciones entre un documento y su tiempo de generación, modificación, firma, transmisión y recepción trae como consecuencia la necesidad de crear evidencias de la posesión de esos datos en un momento determinado.

La solución consiste en introducir, señales de tiempo relacionadas con el momento de creación, modificación, firma, transmisión y recepción mediante el uso del servicio de estampado cronológico, cuya única finalidad es probar que un determinado instante de tiempo, todos los agentes involucrados declararon disponer o disponían de un documento.

El servicio de estampado cronológico time stamping, sello de tiempo o fechado digital como se le conoce en otros países, parte de una premisa fundamental, y es que el tiempo ha sido, es y seguirá siendo una de las variables más importantes en el desarrollo de cualquier actividad humana y, por tanto, referencia básica de la mayor parte de los procedimientos y trámites que tienen lugar entre el sector público y el sector privado.

Tradicionalmente la constancia expresa de la fecha y hora de la realización de un acto ha sido realizada sobre soporte papel, circunstancia que inevitablemente se ve modificada con la utilización generalizada de las nuevas tecnologías de la información.

9.7. LOS METADATOS

Se conocen como los datos detrás de los datos y están inyectados de manera oculta en cualquier archivo que se genere en un equipo informático bajo cualquier software que edite o modifique ese archivo.

Los metadatos más comunes los podemos encontrar en todos los tipos de archivos, ejemplos: Power Point, Word, Excel, PDF, imágenes, etc. Aunque su principal uso es para ayudar en tareas de indexación de archivos, para fines de autenticación, e integridad pueden resultar otro elemento a considerar.

Un archivo de Word puede contener información adicional en forma de metadatos que no se ve, como, por ejemplo:

Tabla 6. Tipos de archivo susceptibles de estampa cronológica

Tipo de Archivo	Metadatos posibles de extracción
Archivo Ofimática	Autor, usuario, título de documento Fecha de creación, acceso, modificación Estado de copyright Aviso de copyright Impresión Sistema Operativo, Versión, Última Edición
Correo electrónico	**Las cabeceras MIME del correo electrónico** Remitente y receptor Hora de la comunicación **Metadatos de los archivos adjuntos** Fecha y hora de creación.
Fotografía	**Datos EXIF:** Modelo, marca y número de serie de una cámara, versión del sistema operativo. Latitud, longitud, altura. Fecha y hora en la que fue tomada la fotografía.

Fuente: Edición propia.

9.8. OBTENCIÓN DE LA LÍNEA DE TIEMPO DE LA EVIDENCIA DIGITAL Y PRUEBA ELECTRÓNICA

Se refiere a la realización de la reconstrucción de los hechos a partir de los atributos de tiempo de los archivos, lo que permite correlacionarlos enriqueciendo la evidencia.

Se debe tener en cuenta que muchos los sistemas pueden manejan varias estampas de tiempo para sus archivos. Las estampas de tiempo más comunes son:

9.8.1. Fecha de modificación

Indica la última vez que el archivo fue modificado de cualquier manera, así sea a través de otro programa.

9.8.2. Fecha de acceso

Es la última vez que el archivo fue accedido (abierto, impreso o visto).

9.8.3. Fecha de creación

Es la fecha en la que el archivo fue creado por primera vez en un sistema, sin embargo, cuando un archivo es copiado hacia otro sistema, la fecha de creación se renovará para dicho sistema, sin embargo, la fecha de modificación si permanecerá intacta.

Estas estampas de tiempo pueden llegar a ser fundamentales para el proceso de análisis del incidente de seguridad de la información que

se encuentra activo o recientemente contenido, por ello, se recalca de la importancia de la sincronización de todos los sistemas de información (incluyendo PC, Laptops) a través de NTP.

En algunas ocasiones, y dependiendo del sistema de archivos del volumen analizado, puede ser imposible realizar un análisis temporal, situación que, como todos los hallazgos, debe ser consignada en el informe final.

9.9. ESCENARIOS DE OBTENCIÓN DE MENSAJES DE DATOS

A continuación, se presentarán los principales dispositivos que representan el lugar físico y lógico de obtención de la evidencia digital, de tal manera que se consideren como escenario principal de la obtención de material o mensaje de datos que tengan vocación a ser prueba, a saber:

9.9.1. Teléfonos celulares

Teniendo en cuenta que estos dispositivos son los más usados actualmente en el mundo para la información y comunicación en el entorno digital, este puede llegar a ser el escenario más común de acontecimiento digitales que ameriten una revisión forense, para este propósito se deben seguir los siguientes pasos:

9.9.1.1. Superación de limitaciones de seguridad

Poder introducir un número ilimitado de contraseñas para desbloquear el smartphone. Actualmente es necesario un código que puede ser versión código, reconocimiento de huella o facial o un patrón previamente programado para acceder a los datos, pero si se introduce un código equivocado una serie de veces, el sistema borra todos los datos o no dejará acceder a ellos.

9.9.1.2. Bloquear y duplicar imagen forense

Poder conectar el lugar de la evidencia (celular) con una computadora o equipo forense, con el fin de introducir automáticamente elevadas cantidades de códigos diferentes combinaciones de códigos en un tiempo muy corto, se han dado casos en los cuales, por la complejidad de la contraseña, este proceso ha tomado más de cinco años.

9.9.1.3. Apoyo tecnológico de prestadores de servicio

Poder Controlar el proceso una vez se accede al dispositivo, un ejemplo de ello lo vemos en el caso Apple que involucra al FBI en una supuesta estrategia conjunta para permitir a Apple manipular el dispositivo de Farook en sus propios laboratorios, evitando así que el software para acceder a este iPhone saliera de la compañía.

9.9.2. Wearables

Hace referencia a dispositivos electrónicos que tienen vocación a ser incorporados o ajustados con relación a un cuerpo humano y son capaces de monitorear o verificar el

cumplimiento de una funcionalidad específica.

Este tipo de dispositivos son incorporados con un carácter continuo y tiene la vocación a integrarse con dispositivos externos con el fin de envío y procesamiento de datos recopilados.
De la recopilación y el procesamiento de datos surge una fuente muy detallada de material o mensajes de datos que pueden ser jurídico relevantes en materia probatoria.

Por ejemplo, datos de geolocalización son almacenados en aplicaciones sincronizadas a relojes pulseras tipo deportivo, que además recolectan datos sobre la salud de quien lo porta, por ejemplo, pulsaciones, tensión arterial, curvas de actividad e inactividad física, que pueden llegar a ser considerados como sensibles.

9.9.3. Drones

"Comúnmente conocidos como: "RPAS (del inglés Remotely Piloted Aircraft System), comúnmente conocido como dron, hace referencia a una aeronave que vuela sin tripulación, la cual ejerce su función remotamente.

Un VANT es un vehículo sin tripulación, reutilizable, capaz de mantener de manera autónoma un nivel de vuelo controlado y sostenido, y propulsado por un motor de explosión, eléctrico o de reacción.

El diseño de los VANT tiene una amplia variedad de formas, tamaños, configuraciones y características. Históricamente surgen como aviones pilotados remotamente o drones, aumentando a diario el empleo del control autónomo de los VANT. Existen dos variantes: los controlados desde una ubicación remota, y aquellos de vuelo autónomo a partir de planes de vuelo preprogramados a través de automatización dinámica." [14]

Este tipo de dispositivos es capaz de documentar los siguientes tipos de mensajes de datos:

- "Identificadores: Modelo del dispositivo y números de serie, números de serie de las baterías conectadas

- Medios: Imágenes, videos, metadatos de ubicaciones, marcas de tiempo e identificadores de cámara

- Telemetría: Ubicaciones, puntos de la ruta, rutas, ubicaciones de inicio, altura y velocidad" [15]

Esta es una clasificación del tipo de actividades que se pueden hacer con Drones y cada una de ellas involucra un diferente nivel de tensión respecto a los derechos fundamentales que se ven involucrados y posiblemente vulnerados por la actividad de recolección, a saber:

14 [Wikipedia, 2019] (Wikipedia. [2019]. Dron. 19/12/2019, de Wikipedia Sitio web: https://es.wikipedia.org/wiki/Veh%C3%ADculo_a%C3%A9reo_no_tripulado) [8 pág. 1]
15 Aepd. Aepd. Aepd. [En línea] 2019. https://www.aepd.es/sites/default/files/2019-09/guia-drones.pdf. [9 pág. 1]

Tabla 7. Drones VS Derechos Fundamentales

Actividad	Derecho Fundamental Vulnerado	Recomendación
Operaciones cotidianas	Privacidad e intimidad	Vuelos recreativos realizados por aficionado, usualmente debe hacerse con drones de gama media y baja y su finalidad debe ser solo documentar datos cotidianos.
Operaciones con riesgo de forma colateral o inadvertida	Datos personales	Solo aplica a actividades que desarrollan eventos públicos comerciales los cuales requieren minimizar la presencia de personas y objetos que permitan su identificación (bañistas, matrículas de vehículos, transeúntes, etc.) en el lugar de la operación. Se recomienda realizar los vuelos en horarios en los que no exista gran afluencia de público.
Operaciones que tienen por finalidad un tratamiento de datos personales	Debido proceso	Se relaciona con aquellas actividades que están asociadas vigilancia y seguridad, generalmente realizadas por autoridades, se recomienda tener previo orden judicial. En este caso en concreto tiene la obligación de notificar a los posibles afectados de la actividad que se va a desarrollar so pena de incurrir en la posible conducta contraria al régimen de protección de datos personales.

Fuente: Elaboración propia.

En Colombia, únicamente se ha expedido regulación de drones por parte de la Aeronáutica civil a través de la Resolución No. 04201 del 27 de Diciembre de 2018, la cual tiene como propósito ampliar la información e impartir instrucciones de cumplimiento en referencia a los requisitos de Aeronavegabilidad y Operaciones necesarios para inscripción de explotadores, operadores y equipos, y para solicitar permiso para realizar vuelos de UAS, de acuerdo a lo establecido en el apéndice 13 de los Reglamentos Aeronáuticos de Colombia (RAC 91), en lo relacionado con la realización de operaciones de Sistemas de Aeronaves Pilotadas a Distancia - RPAS en Colombia.

9.9.4. IoT (Internet de las cosas)

Otro tipo de dispositivo capaz de almacenar o recopilar datos que pueden tener vocación a ser material probatorio son los relacionados con el Internet de las cosas, a saber:

"el Internet of Things es un concepto que se basa en la interconexión de cualquier producto con cualquier otro de su alrededor. Desde un libro hasta el frigorífico de tu propia casa. El objetivo es hacer que todos estos dispositivos se comuniquen entre sí y, por consiguiente, sean más inteligentes e independientes. Para ello, es necesario el empleo del protocolo IPv6 y el desarrollo de numerosas tecnologías que actualmente están siendo diseñadas por las principales compañías del sector." [16]

Ejemplo de la capacidad de los dispositivos IOT para recopilar datos, está en el famoso asistente de voz llamado ALEXA, creado por la compañía Amazon, el cual, en principio, recopila todo lo que sucede alrededor en tiempo real y de manera masiva.

El BIG DATA generado por estos aparatos es almacenado y tratado por la empresa de tecnología precitada, y está disponible para ser consultada en caso de algún requerimiento especial.

Un posible requerimiento especial es el expedido por un Juez de la República que ordena la a empresa que entregue datos específicos con el fin de esclarecer un hecho, acto o contrato jurídicamente relevante, y en principio esta empresa no busca obstruir ninguna investigación legal y tiende a colaborar.

El problema a estos requerimientos se haya cuando lo solicitado está compuesto de datos personales o sensibles, en este caso la empresa se encuentra en el dilema de si proteger los derechos de privacidad de sus clientes o acatar la orden impartida por un juez.

9.9.5. Aplicaciones de mensajería instantánea

Del mismo modo que Twitter y Facebook, las aplicaciones de mensajería instantánea han ido introduciéndose en los Tribunales en todo tipo de procesos y, con ello, los avances tecnológicos se han adelantado en una doble vía en este asunto y han permitido demostrar que a través de un virus controlado de manera remota o de modo manual es posible alterar todo o parte del contenido de los mensajes almacenados.

No solo se está haciendo referencia a que es posible la modificación de mensajes de datos conectando el dispositivo móvil a un computador y valiéndose de algunos comandos que brinden control sobre el teléfono y las conversaciones guardadas en este, sino que recientes estudios han recopilado algunas de las aplicaciones con las que se pueden llevar a cabo acciones más sofisticadas: WhatsApp Toolbox, Fake SMS Sender, SQLite Editor, entre otras.

Se ha demostrado técnicamente que los mensajes de WhatsApp se pueden manipular sin dejar rastro alguno, razón por la cual es absolutamente imposible certificar su autenticidad, por lo que el perito informático se debe remitir únicamente a poder asegurar que no existen indicios de manipulación en los mismos.

16 Rivera, Nicolas. Hipertextual. hipertextual.com. [En línea] 20 de junio de 2015. [Citado el: 22 de enero de 2020.] https://hipertextual.com/2015/06/internet-of-things. [10 pág. 1]

Es necesario para lo anterior realizar un análisis forense del dispositivo, bien sea teléfono o tableta, en el cual se encuentran almacenados dichos mensajes, que pueden haber sido enviados desde este dispositivo y/o recibidos en el mismo.

Este análisis se realiza con algún dispositivo forense especializado en este caso se utiliza la estación forense Cellebrite UFED Touch, ya que es con la que cuentan los expertos peritos que poseen en su laboratorio de informática forense.

Esta herramienta es la más potente del mercado para realizar este tipo de análisis y es utilizada por todas las Fuerzas y Cuerpos de Seguridad del mundo.

Una vez se ha analizado el dispositivo y se ha certificado que no existen indicios de manipulación en los mensajes de WhatsApp, se debe realizar un informe pericial informático firmado por el perito informático donde se evidencien los pasos realizados y las pruebas obtenidas.

Posteriormente, dicho informe pericial podrá ser aportado en un estrado judicial en la que se desee demostrar que no se han encontrado indicios de manipulación en las conversaciones de WhatsApp analizadas.

Al coleccionar los mensajes e información adicional del Smartphone es posible cumplir con los criterios que la Ley señala y su poder probatorio será mayor.

Para ello es importante que se apliquen procedimientos óptimos donde se pueda demostrar que se realizó una correcta cadena de custodia, es decir que se ejecutó un procedimiento de recolección de evidencias y estas no han sido víctimas de alteración o suplantación así mismo que sea confiable la colección forense de las evidencias para que sean válidas en un proceso jurídico.

La recomendación en este aspecto es evitar el documentar datos personales como rostros de personas o actividades que tengan un carácter de seguridad pública.

9.9.6. Evidencia digital en la Nube

Los datos en la nube refieren a una infraestructura ubicada en un domicilio especifico que ofrece servicios de almacenamiento, acceso y administración remota de datos a personas, naturales o jurídicas, que están ocasionando que en el mundo se exponga una migración permanente y masiva de datos, lo que significa que diferentes partes del mundo puede ubicarse tus datos al mismo tiempo.

Esto puede crear dificultades para saber adónde se deben enviar las solicitudes de prueba electrónica que requiere inspeccionar el servidor que aloja los mensajes de datos.

Aunque un prestador de servicios (SP) extranjero puede ofrecer un servicio en un Estado, esto no significa necesariamente que la legislación nacional pueda exigir que el SP (ubicado en otro Estado) divulgue la prueba electrónica.

La legislación nacional a menudo se refiere al concepto tradicional de territorio de un Estado y no a la extraterritorialidad, lo cual no ayudará a las investigaciones en la obtención de datos de la nube o bajo la custodia y el control de un SP en otro Estado. Varios Estados han comenzado a explorar las condiciones en las cuales las autoridades pueden solicitar el acceso a los datos, utilizando sus propias herramientas nacionales. (Tema a tratar en guía tercera de ámbito internacional de la EDiPE)

La decisión de Yahoo en Bélgica es un ejemplo de un caso judicial reciente que se centra en la legitimidad del uso de órdenes de producción nacionales para empresas cuyo asiento principal se encuentra fuera del Estado requirente, pero proporcionan un servicio en el territorio de ese Estado.

La fragmentación resultante puede generar incertidumbre legal, retrasos, así como inquietudes sobre la protección de los derechos fundamentales y garantías procesales para las personas relacionadas con dichas solicitudes.

La Comisión Europea está proponiendo nuevas reglas para facilitar y hacer que sea más rápido que las autoridades judiciales y policiales obtengan pruebas electrónicas de la nube a través de lo siguiente:

- Orden de conservación europea: esto le permite a una autoridad judicial de un Estado miembro obligar a un SP que ofrece servicios en la Unión Europea y que esté establecido o representado en otro Estado miembro a conservar datos específicos parque la autoridad pueda solicitar esta información más tarde a través de MLA, una orden de investigación europea o una orden de producción europea.
- Orden de producción europea: permite a una autoridad judicial de un Estado miembro solicitar pruebas electrónicas directamente a un proveedor de servicio SP que ofrezca servicios en la Unión Europea y que esté establecido o representado en otro Estado miembro, independientemente de la ubicación de los datos, que será obligado a responder dentro de 10 días, y dentro de 6 horas en caso de emergencia.

El 23 de marzo de 2018, se emitió la ley conocida como "CLOUD Act" (Ley de Aclaración del Uso Legítimo de Datos en el Extranjero) en Estados Unidos para abordar algunos de los desafíos actuales que enfrentan las agencias del orden público con respecto a la prueba electrónica.

Esta ley restaura el statu quo que siguieron los SP de Estados Unidos durante años y aclaró que las garantías de Estados Unidos requieren que los SP produzcan datos en su poder, custodia o control, independientemente de si eligen almacenar los datos dentro o fuera de Estados Unidos.

El alcance de la autoridad de garantías en la CLOUD Act es, por un lado, consistente con los principios internacionales, incluido el Convenio de Budapest sobre la ciberdelincuencia, y por otro, una autoridad que muchos otros Estados también reconocen.

Esa ley también autoriza al gobierno a celebrar acuerdos ejecutivos en virtud de los cuales Estados Unidos y sus Estados socios pueden comprometerse a eliminar los impedimentos legales para el cumplimiento transfronterizo mediante órdenes legales en casos que involucran delitos graves, incluido el terrorismo.

Solo los Estados con leyes sólidas que protegen la privacidad y las libertades civiles son elegibles para tales acuerdos. El marco es un suplemento y no un reemplazo para la cooperación disponible a través de las MLA.

9.10. FORMÁTICA FORENSE APLICADA A LA EVIDENCIA DIGITAL Y PRUEBA ELECTRÓNICA

El contar con un marco estandarizado en materia de informática forense, garantizará la admisibilidad de la evidencia digital, para atender un procedimiento penal o civil.

Por otra parte, en Colombia, los delitos informáticos son sancionados siguiendo los lineamientos establecidos en la Ley 1273 del año 2009, por lo que se hace indispensable desarrollar y establecer mecanismos para el análisis forense, permitiendo que se desarrollen dentro de los marcos controlados y regulados.

Los avances tecnológicos, las tendencias en las herramientas de informática forense, los litigios de tipo penal y civil conllevan a la reorganización de la realidad de personas, estados, entidades y empresas.

La administración pública, no es ajena a los cambios, en cambio que la realidad que va a ser objeto de protección y tutela jurídica tiene cada vez más, su origen en relaciones y hechos de naturaleza electrónica, soportando la informática forense, como eje principal de una prueba.

9.10.1. Estándar ISO/IEC 27037:2012

Bajo el estándar ISO/IEC 27037:2012 existen tres principios internacionales que permiten establecer un análisis respecto a la relevancia, confiabilidad y suficiencia de la Evidencia digital.

Tabla 8. Estándar ISO / IEC 27037:2012

PRINCIPIO	CONTEXTO	FINALIDAD	UTILIDAD
RELEVANCIA	Condición jurídica que contempla elementos analizados bajo la pertinencia de los mismos respecto del caso.	Probar o no la hipótesis planteada a partir de la exclusión del material que resulte irrelevante.	Si se encuentran elementos que no cumplan esta condición deben ser excluidos.

PRINCIPIO	CONTEXTO	FINALIDAD	UTILIDAD
CONFIABILIDAD	Permite desde la parte técnica facilitar la contradicción.	Validar la repetibilidad y auditabilidad del proceso aplicado para la obtención de evidencia	Si un tercero (Contraparte) sigue el mismo proceso debe obtener los mismos resultados.
SUFICIENCIA	Permite entender la experiencia y formalidad del perito.	Validar si las evidencias recolectadas y analizadas tienen elementos suficientes para sustentar los hallazgos.	Analiza la completitud de las pruebas.

Fuente: Edición propia.

Adaptando la propuesta del Experto doctrinante, PhD Jeimy Cano, se proponen las siguientes preguntas útiles para el entendimiento y validación de estos principios.

Relevancia: ¿La evidencia que se aporta vincula al sujeto con la escena del crimen y la víctima?

Ilustración 15. Relevancia

Fuente: Edición propia.

Se debe analizar detalladamente si existen por ejemplo logs de conexiones, que de estar disponibles pueden aportar información valiosa para establecer si hubo interacción entre el autor de la conducta o emisor de mensaje dado el caso, con el sistema afectado o con el sistema del receptor del mensaje. Este tipo de bitácoras dan información muy detallada.

¿La evidencia prueba algunas hipótesis concretas que se tienen del caso en estudio?

Después de analizadas las condiciones de licitud de la evidencia y demás aspectos propios de autenticidad y confiabilidad es muy importante revisar si las hipótesis pudieran soportarse en las evidencias aportadas: Un acceso abusivo desde una IP externa sobre la cual se ha podido establecer es la que habitualmente utiliza la persona implicada. La misma IP corresponde al plan de datos cuya suscripción ante el proveedor de servicios de internet se ha podido establecer.

¿La evidencia recolectada valida un indicio clave que permita esclarecer los hechos objeto de estudio?

Por ejemplo, un ex empleado de una empresa afectada por una violación de datos personales de clientes o la revelación de secretos profesionales, ha sido objeto de una inspección en su computador personal. El hallazgo permite identificar que una USB ha sido utilizada en ese equipo portátil y que el número serial de la memoria USB, se coincide con la huella digital de la USB utilizada para copiar la información desde el repositorio original de la empresa afectada.

Confiabilidad

¿Los procedimientos efectuados sobre los dispositivos tecnológicos han sido previamente probados?

Existen diferentes guías y documentos de buenas prácticas que describen los procedimientos que se deben seguir por parte de los expertos en el tratamiento de la evidencia digital, estos estándares deberán ser tenidos en cuenta para el adecuado tratamiento de la evidencia digital.

¿Se conoce la tasa de error de las herramientas forenses informáticas utilizadas?

Al respecto se ha documentado muy poco en la comunidad científico, sin embargo, existen White Papers o documentos blancos que son liberados con frecuencia y que sirven de consulta para los peritos. Igualmente es recomendable utilizar dos herramientas forenses para efectos de convalidar o contrastar los resultados obtenidos por la herramienta 1 versus la herramienta 2

¿Se han efectuado auditorías sobre la eficacia y/o eficiencia de los procedimientos herramientas utilizados para adelantar el análisis forense informático?

En el proceso de certificación de un laboratorio de informática se deben realizar auditorías que permitan identificar y cuantificar los resultados obtenidos en términos de eficacia y eficiencia de las herramientas y procedimientos utilizados.

Suficiencia

¿Se ha priorizado toda la evidencia recolectada en el desarrollo del caso, basada

en su apoyo a las situaciones que se deben probar?

La priorización de la evidencia digital señala, el orden de análisis y como se da importante énfasis en aquella que contribuye a fortalecer las hipótesis planteadas en el caso. Establecer el origen de un mensaje de datos, identificando al iniciador, los mecanismos de autenticidad utilizados podría ser un orden para priorizar.

¿Se han analizado todos los elementos informáticos identificados en la escena del crimen?

Se trata de una condición que obliga a analizar todos los elementos y no dejar de considerar alguno de los elementos que han sido recopilados.

¿Se tiene certeza de que no ha se eliminado o sobre escrito evidencia digital en los medios analizados?

Para ello se deben analizar los metadatos que permiten establecer fechas de creación, modificación, acceso a un determinado mensaje de datos.

9.11. MÉTODO JURISPRUDENCIAL PARA DETERMINAR FUERZA PROBATORIA DE MENSAJES DE DATOS EN UN PROCESO JUDICIAL

En una sentencia hito de la EDiPE, la Corte Suprema de Justicia extrajo los mejores estándares técnicos y legales, tanto nacionales como extranjeros, para darle al ordenamiento Jurídico aplicable una directriz precisa de como valorar y validar una EDiPE en el marco de un proceso judicial.

Tabla 9. Método de valoración y validez de MD a EDiPE jurisprudencial

MÉTODO JURISPRUDENCIAL PARA DETERMINAR LA FUERZA PROBATORIA DEL MENSAJE DE DATOS EN UN PROCESO JURÍDICAMENTE RELEVANTE			
TIPO VERIFICACIÓN	VERIFICACIÓN DE:	DEFINICIÓN	EJEMPLO
CONFIABILIDAD	**1.** INTEGRALIDAD	El texto del documento transmitido por vía electrónica sea recibido en su integridad por el destinatario.	TRAZABILIDAD DE PRESTADOR DE SERVICIO DE EMAIL
	2. INALTERABILIDAD	El documento generado por primera vez en su forma definitiva no sea modificado.	AUTENTICACIÓN NOTARIAL

TIPO VERIFICACIÓN	VERIFICACIÓN DE:	DEFINICIÓN	EJEMPLO
	3. RASTREABILIDAD	Posibilidad de acudir a la fuente original de creación o almacenamiento de este con miras a verificar su originalidad y su autenticidad.	ACCESO AL EMAIL PARTE DEL MENSAJE DE DATOS
	4. RECUPERABILIDAD	Condición física por cuya virtud debe permanecer accesible para ulteriores consultas.	ACCESO A SERVIDOR DONDE ESTA UBICADO EL MENSAJE DE DATOS
	5. CONSERVACIÓN	Prevenir su pérdida, ya sea por el deterioro de los soportes informáticos en que fue almacenado, o por la destrucción ocasionada por "virus informáticos" o cualquier otro dispositivo o programa ideado para destruir los bancos de datos informáticos.	CREACIÓN DE IMAGEN FORENSE DIGITAL
AUTENTICIDAD	**6.** Mecanismos tecnológicos que permiten identificar el autor de este y asociarlo con su contenido		FIRMA ELECTRÓNICA (FIRMA ESCANEADA, MÉTODO BIOMÉTRICO, Y FIRMA DIGITAL)

Fuente: Diseño propio, contenido Corte Suprema de Justicia (Sala de Casación Civil) RAD. 11001 3110 005 2004 01074 01. del 16 de diciembre de 2010)

9.12. TÉCNICAS ANTI-FORENSES

Como definimos anteriormente, el análisis forense digital se ocupa del estudio de la adquisición, preservación y presentación de mensajes de datos electrónicos para ser procesados y conservados de tal forma que puedan utilizarse como prueba legal.

El uso ético del análisis digital trata de entender y contestar preguntas referidas a cómo, cuándo y desde dónde se produjo el incidente, así como cuál fue su impacto y a que afectó.

Ahora, imaginando la otra cara de la moneda, entendida como un uso no ético de la metodología forense, podría inferirse que la técnica antiforense es el estudio de la adquisición, preservación y presentación de mensajes de datos para ser procesados y conservados de tal forma que puedan utilizarse como herramienta para la comisión de un delito.

Existen algunos objetivos que persiguen las estrategias antiforense, entre otros, limitar la

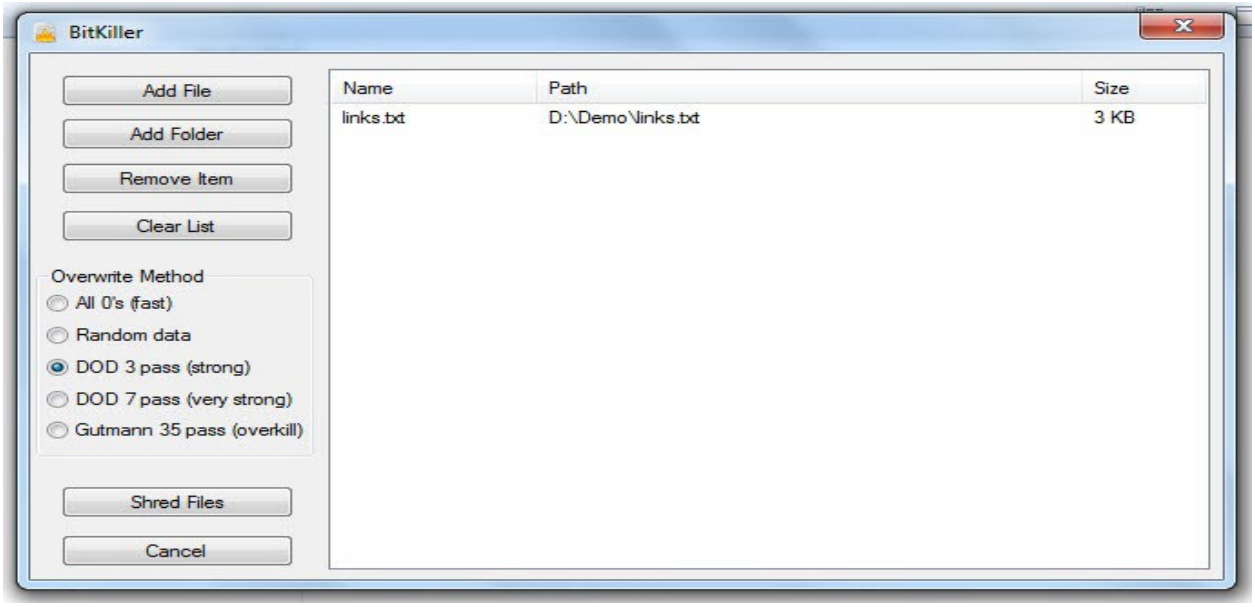
detección, distorsionar la información que se encuentre residente en él tratar de limitar el uso de las herramientas utilizadas, incluso realizar una actividad dolosa de ataque sistémico.

9.12.1. Técnica de borrado o destrucción de los MD

Retomando el error que ocasionó la pérdida del material recopilado en el caso de Raúl Reyes, previsto en el taller, esta primera técnica refiere a cometer dolosamente el apagado del equipo con miras a modificar, alterar y/o destruir el material e impedir que se pueda recuperar.

Existe herramientas lógicas que permiten desplegar la actividad señalada, a propósito de las cuales están capacitadas para acceder a dispositivos, rastrear archivos y borrar o alterar de tal manera que permita extraer todo rastro posible de datos de interés. Una de ellas está plenamente expuesta en una guía de referencia técnica de la compañía ESET[17] sobre prácticas antiforense digital.

Ilustración 16. Software de borrado de mensaje de datos Bitkiller



Fuente: (https://www.welivesecurity.com/la-es/2015/07/02/tecnicas-anti-forenses/)[18]

17 Véase publicación ESE ubicada en el siguiente enlace: https://www.welivesecurity.com/la-es/2015/07/02/tecnicas-anti-forenses/
18 ESET. Técnicas antiforenses. welivesecurity.com. [En línea] 2 de julio de 2015. [Citado el: 22 de enero de 2020.] https://www.welivesecurity.com/la-es/2015/07/02/tecnicas-anti-forenses. (11 pág. 1)

Respecto del acceso a dispositivo para realizar este tipo de prácticas téngase en cuenta que uno de los métodos más usados es el envío de ransomware entendido como paquetes de virus que alteran y modifican el correcto funcionamiento del dispositivo y permite un control remoto preprogramado.

En la práctica relacionada con la actividad estatal, es muy común observar que en entidades sujetas a cambios temporales de administraciones sean susceptibles de ser víctima de estos virus informáticos ransomware debido al fácil acceso a los dispositivos para instalar dichos sistemas y bajo nivel de seguridad de firewall.

9.12.2. Ocultación

Al igual que las técnicas de borrado, la intención de la ocultación es evitar que el interesado pueda acceder a la información que le es de su interés, al respecto se diferencia del borrado, en que el sujeto que realiza la dolosa actuación no destruye el archivo o mensaje de datos, sino que se propone ubicarlo en un repositorio lógico o físico de difícil acceso.

Este es el caso de estrategia que se utiliza a menudo como herramienta de comunicación e información entre personas que desean ocultar el contenido de sus manifestaciones a través de programas de ocultación.

> *"Esta técnica, llamada esteganografía, puede llegar a ser muy eficiente de ser bien ejecutada, pero conlleva muchos riesgos para el atacante o intruso. Al no modificar la evidencia, de ser encontrada puede ser válida en una investigación formal y por lo tanto servir para la incriminación e identificación del autor de dicho ataque."* [19]

9.12.3. Sobreescritura de metadatos

Este método tiene como fin hacerle llegar al interesado una información alterada en su componente lógico o físico de originalidad de tal manera que conduzca a un error en el hecho, acto o contrato que se pretenda probar con dicha información.

Un uso práctico de este método es usual en escenarios judiciales debido a que el alterar un mensaje de datos significa y representa la pérdida de veracidad del material de tal suerte que se rechaza su contenido y con ello la posibilidad de un debido proceso justo para las partes en conflicto.

> *"Existen varias herramientas comúnmente utilizadas con este fin, como ExifTool o Metasploit que en conjunto con Meterpeter permiten borrar o cambiar estos parámetros."* [20]

19 Ibidem [11 pág. 1]
20 Ibidem [11 pág. 1]

Ilustración 17. Sobreescritura de datos en mensaje de datos

```
meterpreter > timestomp lineadetiempo.txt -f c:\\autoexec.bat
[*] Setting MACE attributes on lineadetiempo.txt from c:\autoexec.bat
meterpreter > timestomp lineadetiempo.txt -v
Modified      : 2009-06-10 17:42:20 -0400
Accessed      : 2009-07-13 22:04:04 -0400
Created       : 2009-07-13 22:04:04 -0400
Entry Modified: 2011-10-05 10:41:42 -0400
```

Fuente: Edición propia.

9.12.4. Cifrado de información

Teniendo en cuenta la necesidad de transmisión como factor determinante en el valor de un dato, la posibilidad de que en el transcurso en que viaja el mensaje se vulnere su seguridad, es por esto por lo que existe el método de cifrado del mensaje de datos, de tal manera que:

i) Permita la transmisión y posible rastreo por parte de terceros y

ii) Aunque haya sido rastreada, no evidencie el mensaje de datos sino a través de un ciframiento de seguridad.

El Método de ciframiento se vale de unas operaciones matemáticas llamadas a alterar el mensaje de datos de tal manera que, solo aplicando una llave o código de descifrado, se logre el acceso a al contenido original.

Sin el ánimo de entrar a detalles técnicos, la analogía básica se puede identificar respecto de la famosa “regla de tres” la cual consiste en un juego de coordenadas que compone una ecuación, de la siguiente manera:

Tabla 10. Regla de tres numérica para hallar el valor de una incógnita, ejemplo de ciframiento.

x	**100**
y	**?**

Fuente: Elaboración propia.

Descriptivamente sería: ¿Si X vale 100, a cuanto equivale Y?

En el mismo ejemplo, Y sería el mensaje cifrado, dado que es una incógnita, nadie sabe a qué equivale Y. En ese orden de ideas la única manera de descifrar la incógnita, ósea que es igual a Y, entonces debemos acceder a una llave que descifre el enigma.

En el supuesto en que nosotros seamos los titulares de la llave que desencripta Y queramos transmitir dicha información a otra persona, a través de un medio público, previamente tuve que ponerme de acuerdo con el receptor de la información con miras a que él también tuviera la llave de descifrado.

Lo anterior garantiza que solo emisor y receptor puedan acceder a la información, los demás verán solo la incógnita.

Si la llave que descifra el anterior ejemplo fuera (X + Y = 122) ¿A qué equivale Y?

9.13. ANÁLISIS JURISPRUDENCIAL

A continuación, se presenta el fallo de la CORTE SUPREMA DE JUSTICIA SALA DE CASACIÓN CIVIL, Magistrado Ponente Pedro Octavio Munar Cadena Bogotá, D.C., del dieciséis (16) de diciembre de dos mil diez (2010). Ref.: Expediente No.11001 3110 005 2004 01074 01, en virtud del cual se enmarca el modelo de procedimiento a seguir en caso de valoración de mensajes de datos dentro de un proceso en el que se quiere hacer valer como material probatorio de un hecho, acto o contrato jurídicamente relevante.

Análisis jurisprudencial Ref.: Expediente No.11001 3110 005 2004 01074 01 CSJ		**PÁGINA**
ENLACE DE ACCESO A SENTENCIA COMPLETA https://arkhaios.com/wp-content/uploads/2011/07/DOCUMENTO-ELECTRNICO-autenticidad-y-veracidad.pdf		
ANTECEDENTES	La actora pidió que se declarara que entre ella y el demandado existió una unión marital de hecho, desde antes de diciembre de 2000 o, en su defecto, en la fecha que resulte probada, hasta el día en que éste abandonó el hogar; y que, en consecuencia, surgió entre ellos una sociedad patrimonial, cuya liquidación debe ordenarse.	1
	La admisión del escrito introductor del litigio fue notificada personalmente al señor Pulido Casas, por conducto de su apoderado judicial, quien presentó la respectiva réplica, en la que se opuso a la prosperidad de las súplicas y formuló las excepciones que denominó “causa ilícita para pretender la declaración de existencia de la unión marital”, “falta de los requisitos legales necesarios para la conformación de la sociedad patrimonial entre compañeros permanentes” e “ilegitimidad e ilicitud de las pruebas aportadas”.	3

	Sustentó la no comparecencia en este caso de "singularidad" que requiere la unión marital debido a que, este recibió un mensaje de datos, enviado desde la dirección electrónica josealejandro7880@latinmail.com al correo gpulido@escuelaing.edu.co , siendo remitente el señor José Fernando Cerón Quintero, "primer esposo" en el cual supuestamente indica que la señora le era infiel con el ex esposo y que lo utilizaba solo por dinero.	
	El Juez 5º de Familia de Bogotá, tras imprimirle al asunto el trámite pertinente, dictó sentencia el 31 de marzo de 2008, mediante la cual declaró la existencia de la unión marital y la consecuente sociedad patrimonial, fijando su marco temporal entre el 14 de febrero de 2001 y el 27 de octubre de 2003. Las demás pretensiones las negó. Téngase en cuenta que no le dio validez probatoria al email enviado desde la dirección electrónica josealejandro7880@latinmail.com al correo gpulido@escuelaing.edu.co.	4
	Esa decisión fue confirmada por el tribunal al desatar la alzada interpuesta por las partes, salvo la fecha de iniciación de la relación marital, pues resolvió que había surgido el 2 de febrero de 2001.	4
	El demandado recurrió en casación dicha providencia, impugnación que ahora es objeto de decisión, aduciendo violados los preceptos de la Ley 527 de 1999 y Sentencia C 662 de 2000, dado que el considera que " adosó a la mentada réplica la reproducción impresa del contenido del mensaje de datos y entregó éste en un "CD", bien "podría confirmarse la integridad del mismo" y, por lo tanto, debió dársele el valor probatorio que el referido ordenamiento concede a ese tipo de documentos. Alude el recurrente a la "necesidad de aplicar las facultades oficiosas para llegar a la certeza sobre la integridad del medio probatorio", expuso que el accionado hizo lo que estaba a su alcance, aportó la prueba magnética en forma correcta y garantizó con su entrega no sólo la contradicción de la misma, sino, también, la posibilidad, ante cualquier duda, de que el juez a través de expertos, y acudiendo a la facultad de decretar	11

	pruebas de oficio en la búsqueda de la verdad material, ahondara en la integridad del mensaje de datos, para conferirle el mérito probatorio reconocido por la Ley 527 de 1999, el cual desconoció el sentenciador. Insiste, entonces, en que el juzgador, en ejercicio de las facultades oficiosas conferidas por el ordenamiento procesal (artículos 37 num.4º, 179 y 180 del C. de P. Civil), debió adoptar las medidas conducentes para identificar plenamente al autor del correo en cuestión, dar certeza de la participación exclusiva de esa persona en el acto mismo de la emisión y asociarla con el contenido del documento.	
PROBLEMA JURÍDICO	¿El fallo del Tribunal violó o no, la ley a causa de haber incurrido en error de derecho por no hacer uso de las facultades oficiosas con miras a establecer la autenticidad del mensaje de datos enviado al opositor, cuyo texto fue aportado con la contestación de la demanda?	10
TESIS	En mérito de lo expuesto, la Corte Suprema de Justicia, Sala de Casación Civil, administrando justicia en nombre de la República de Colombia y por autoridad de la ley, NO CASA la sentencia proferida el 3 de julio de 2009, por la Sala de Familia del Tribunal Superior del Distrito Judicial de Bogotá, dentro del proceso ordinario promovido por MARTHA HELENA PILONIETA frente a GABRIEL HUMBERTO PULIDO CASAS.	25
TIPO DE PROBLEMA JURÍDICO	De Derecho - Conflicto de método de interpretación	
FUENTES JURÍDICAS	Artículo 42 de la Constitución Política;	
	Artículos 2º, 3º, 5º al 12º de la Ley 527 de 1999	
	Sentencia C 662 de 2000	
	Artículos 1º y 2º de la Ley 54 de 1990	
	Artículos 37 núm.4º, 179 y 180 del estatuto procesal civil (NORMA DEROGADA)	

EXTRACTOS RELEVANTES	Por supuesto que la autenticidad y la veracidad son atributos distintos de la prueba documental, pues hacen referencia a aspectos disímiles. La primera concierne con la certeza que debe tener el juzgador respecto de la persona a quien se le atribuye la autoría del documento, certidumbre que alcanzará en la medida que se encuentre en alguna de las hipótesis específicamente previstas por el ordenamiento (artículos 252 y 276 del Código de Procedimiento Civil, entre otros). Establecida la autenticidad del documento, podrá el juzgador avanzar en su estimación con miras a establecer su vigor probatorio, particularmente su credibilidad, empeño que deberá abordar de la mano de las reglas de la sana crítica.	13
	A raíz de los avances tecnológicos en el campo de los computadores, las telecomunicaciones y la informática surgió el "documento electrónico", concebido por la doctrina jurídica como "cualquier representación en forma electrónica de hechos jurídicamente relevantes, susceptibles de ser asimilados en forma humanamente comprensible", y reconocido por la legislación patria, concretamente, por la Ley 527 de 1999, declarada exequible mediante las sentencias C-662 de 8 de junio de 2000 y C-831 de 8 de agosto de 2001, estatuto inspirado en la Ley Modelo sobre Comercio Electrónico elaborada por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI), uno de cuyos principios vertebrales es el de "la equivalencia funcional" de los documentos de esa especie y que se funda en un análisis de los objetivos y funciones que cumple el documento sobre papel con miras a determinar la manera de satisfacerlos en el contexto tecnológico.	16
	Para determinar la fuerza probatoria del mensaje de datos, el artículo 11 de la Ley 527, señala, como ya se pusiera de presente, que deben atenderse las reglas de la sana crítica, así como la confiabilidad que ofrezca la forma como se haya generado, archivado o comunicado el mensaje, la confiabilidad de la forma en que se hubiere conservado la integridad de la información, la forma como se identifique a su iniciador, y cualquier otro factor relevante.	19

Fuente: Elaboración propia.

10. AUTOEVALUACIÓN

Ahora que ha terminado de estudiar esta temática, conviene reforzar una serie de conceptos generales que debieron ser aprendidos en esta sección. Lea con atención las siguientes preguntas y formule la respuesta que consideraría que mejor se ajusta a lo estudiado en la sección. Una vez considere que su respuesta es la ideal, revise la respuesta propuesta por los autores y contraste las dos respuestas, reflexionando sobre las similitudes y diferencias obtenidas.

¿Qué es Imagen forense?

La adquisición de una imagen forense se conoce como "imaging" (obtención de imágenes forenses de datos) y se refiere al proceso mediante el cual se realiza una copia exacta del dispositivo de almacenamiento donde reposa la información electrónicamente almacenada que llegará a tener vocación probatoria en el desenlace del proceso.

Este mismo procedimiento se debe realizar respecto a repositorio de tipo lógico como carpetas que contienen archivos o mensajes de datos.

¿Cómo valorar y validar una EDiPE en un proceso judicial?

Si el Mensaje de datos cumple con los siguientes requisitos esenciales:

Tabla 11. Método de valoración y validez de MD a EDiPE jurisprudencial

MÉTODO JURISPRUDENCIAL PARA DETERMINAR LA FUERZA PROBATORIA DEL MENSAJE DE DATOS EN UN PROCESO JURÍDICAMENTE RELEVANTE			
TIPO VERIFICACIÓN	**VERIFICACIÓN DE:**	**DEFINICIÓN**	**EJEMPLO**
CONFIABILIDAD	**1.** INTEGRALIDAD	El texto del documento transmitido por vía electrónica sea recibido en su integridad por el destinatario.	TRAZABILIDAD DE PRESTADOR DE SERVICIO DE EMAIL
	2. INALTERABILIDAD	El documento generado por primera vez en su forma definitiva no sea modificado.	AUTENTICACIÓN NOTARIAL

TIPO VERIFICACIÓN	VERIFICACIÓN DE:	DEFINICIÓN	EJEMPLO
	3. RASTREABILIDAD	Posibilidad de acudir a la fuente original de creación o almacenamiento de este con miras a verificar su originalidad y su autenticidad.	ACCESO AL EMAIL PARTE DEL MENSAJE DE DATOS
	4. RECUPERABILIDAD	Condición física por cuya virtud debe permanecer accesible para ulteriores consultas.	ACCESO A SERVIDOR DONDE ESTA UBICADO EL MENSAJE DE DATOS
	5. CONSERVACIÓN	Prevenir su pérdida, ya sea por el deterioro de los soportes informáticos en que fue almacenado, o por la destrucción ocasionada por "virus informáticos" o cualquier otro dispositivo o programa ideado para destruir los bancos de datos informáticos.	CREACIÓN DE IMAGEN FORENSE DIGITAL
AUTENTICIDAD	**6.** Mecanismos tecnológicos que permiten identificar el autor de este y asociarlo con su contenido		FIRMA ELECTRÓNICA (FIRMA ESCANEADA, MÉTODO BIOMÉTRICO, Y FIRMA DIGITAL)

Fuente: Diseño propio, contenido Corte Suprema de Justicia (Sala de Casación Civil) RAD. 11001 3110 005 2004 01074 01. del 16 de diciembre de 2010)

11. ACTIVIDADES PEDAGÓGICAS: TALLER DE ESTUDIO DE ANÁLISIS DE CASOS

11.1. INSTRUCCIONES DE IMPLEMENTACIÓN

Lea con atención cada ficha técnica del caso que se le presenta, identifique cual es el problema jurídico central y con base a lo repasado en la guía de ámbitos internacionales de la EDiPE, responda la pregunta de cada caso particular.

11.2. LECTURA PREVIA

En la parte inferior del título de cada caso encontrará unos antecedentes que debe leer como contexto de cada caso particular. Debe ser abordada esta lectura antes de responder lo requerido.

11.3. ESTRATEGIA DE EVALUACIÓN

11.3.1. CASO "CAMBIAZO ADMINISTRATIVO"

NOTA: Caso de la vida real, se cambiaron los nombres y situaciones reales con fines académicos.

ANTECEDENTES	El día 2 de septiembre de 2014 en una diligencia de allanamiento y registro, avalada plenamente por una orden judicial, en virtud de una investigación por el presunto delito de fraude electoral, miembros de la policía judicial incautaron cinco computadores portátiles y siete teléfonos celulares, todos ellos de gama alta.
	El día 3 de septiembre de 2014, los miembros de la policía judicial presentan, en audiencia preliminar ante un juez de control de Garantías, los elementos incautados junto con las imágenes forenses digitales de los dispositivos para que se les imparta control constitucional de legalidad, lo cual concluye con un fallo del Juez, reconociendo la totalidad de dispositivos incautados y la imagen forense digital de los mismos como prueba anticipada.
	El día 4 de septiembre de 2014 según se dispuso por la autoridad competente, se ordenó remitir los elementos informáticos, con cadena de custodia, al almacén de evidencias dispuesto para informática forense, con fines de almacenamiento. En el mismo sentido fueron remitidas las imágenes forenses de esos elementos al laboratorio dispuesto para informática forense, mediante orden de trabajo con fines de análisis y obtención de posible evidencia digital.
	El día 17 de enero de 2015 se hace entrega de los informes de laboratorio y resultados obtenidos por la imagen forense al Juzgado de conocimiento, y el Juez, muy prudentemente, decide solicitar una inspección judicial para garantizar que los datos reseñados en el informe que refieren a los contenidos en la imagen forense eran los mismos que se hallaban almacenados en los dispositivos incautados.

	El día 8 de mayo de 2015, los elementos incautados fueron remitidos mediante formato de cadena de custodia, al despacho judicial que los requirió para diligencia judicial ordenada.
	En la diligencia de inspección judicial comparecen las partes y se le solicita al experto forense digital realizar el cotejo. Cuando el experto forense digital procedió a destapar el paquete de sellamiento que contenía los dispositivos electrónicos incautados, se dio cuenta que estos habían sido cambiados y desvalijados. Los computadores eran solo carcasa, faltaban sus componentes internos, incluyendo disco duro y los celulares habían sido remplazados por versiones de plástico simulado.
	Ante la gravedad de los hechos, la defensa del acusado solicita se desestime en el proceso las dos pruebas presentadas por el experto forense digital que ejerce funciones de policía judicial, dada la destrucción de los dispositivos electrónicos que imposibilita demostrar relación con los datos presentados en informe forense digital.
	La Fiscalía, por su parte, solicita sean tenidas en cuenta la imagen forense digital como suficiente para justificar que los datos contenidos sean tenidos en cuenta como material de valoración y validez probatoria en el proceso.
PROPÓSITO DEL ESTUDIO DE CASO	Identificar las fuentes de derecho que regulan aspectos tratados en el caso en concreto.
	Analizar las características técnicas relacionadas con los mensajes de datos objeto de debate en el caso en concreto.
	Aplicar los conocimientos prácticos obtenidos en la Guía de Evidencia Digital y Prueba electrónica para dirimir el caso en concreto.
PREGUNTA DE REFLEXIÓN	¿Cuál de las dos posturas, defensa o fiscalía, es admisible a la luz del ordenamiento jurídico colombiano? justifique su respuesta.
UNIDAD DE ANÁLISIS	Guía de aprendizaje autodirigido de Evidencia Digital y Prueba Electrónica: Aspectos generales.
MÉTODO E INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN	Uso de método cualitativo con énfasis en comprender las perspectivas de las personas involucradas en el caso en concreto.

	Uso de instrumento de entrevista semiestructurada dirigido a funcionario judicial participante en el caso que expone hechos de la vida real.
MÉTODO DE ANÁLISIS DE LA INFORMACIÓN	La información recolectada se analizó acorde a las preguntas del caso en concreto.

11.3.2. CASO "Raúl Reyes"

NOTA: Caso de la vida real, se cambiaron los nombres y situaciones reales con fines académicos.

ENLACE INFORME INTERPOL: http://static.eluniversal.com/2008/05/15/infointerpol.pdf
SENTENCIA CORTE SUPREMA DE JUSTICIA SALA DE CASACIÓN PENAL acta No. 269. ENLACE:
https://www.ambitojuridico.com/BancoMedios/Documentos%20PDF/auto%2029877%20(01-08-2011)%20reposici%C3%B3n%20wilson%20borja.pdf

ANTECEDENTES	*"1. Durante los días 26 y 27 de febrero de 2008, en la Sede de la Dirección de Inteligencia de la Policía Nacional de Colombia, en la ciudad de Bogotá D.C., personal de la Policía Nacional con la participación de integrantes del EJÉRCITO NACIONAL y FUERZA AÉREA COLOMBIANA, iniciaron reuniones para la planeación de la operación "FENIX" dirigida a localizar un campamento del frente 48 de las FARC, en el cual se encontraría el terrorista alias "RAÚL REYES"* [21]
	"2. El 280208 se inició el desplazamiento del personal militar y policial a la base militar ubicada en Larandia, Caquetá para constatar y verificar la información recolectada, según la cual, en las coordenadas N 00 23 10 W 076 20 59 funcionaba un área campamentaria del grupo terrorista FARC, específicamente del frente 48" [22]
	3. Agotado el procedimiento de tratamiento, evaluación y análisis de la información, se decidió realizar la operación a partir de las 00:15 horas del día 010308
	4. Dos horas antes de lanzar la operación, se conoció una nueva coordenada de la ubicación del campamento N 00–21–45 W 76–20–20." [23]
	"5. El 010308 a las 0015 horas el personal asignado, partió desde la base ya en tres helicópteros Blakc Hawk y un "arpía" con cuarenta y ocho (48)

21 Colombia, Corte Suprema de Justicia. ambitojuridico.com. ambitojuridico.com. [En línea] 18 de mayo de 2011. [Citado el: 22 de enero de 2020.] https://www.ambitojuridico.com/BancoMedios/Documentos%20PDF/auto%2029877%20(01-08-2011)%20reposici%C3%B3n%20wilson%20borja.pdf. (12 pág. 2)
22 Ibidem (13 pág. 2)
23 Ibidem (13 pág. 2)

unidades del EJÉRCITO NACIONAL, POLICÍA NACIONAL (COPES) y ARMADA NACIONAL, llegando al punto de desembarco a las 00:35 horas, aproximadamente, el cual queda a un kilómetro del campamento". [24]

"6. Se inició el desplazamiento a pie hacia el campamento, llegando aproximadamente a las 03:00 horas, siendo recibidos con disparos de arma de fuego de largo alcance, entrando en combate, el cual duró, aproximadamente, una hora, al cabo de la cual se tomó el control del campamento". [25]

"7. Posteriormente se tomó seguridad perimetral con el fin de realizar el registro del campamento tomando fotografías y filmaciones de este".[26]

"8. El registro se realizó, tomando como punto de partida lo que al parecer era el cambuche del cabecilla, su oficina y áreas privadas; a tres metros de estos lugares se encontró el cuerpo sin vida de quien por sus características físicas se dedujo que se trataba del terrorista de las FARC alias "RAÚL REYES". Junto a este cuerpo se encontró el cadáver de una mujer al parecer alias "GLORIA". [27]

"9. En el lugar se encontraron dos cajas que contenían tres computadores portátiles y los demás elementos que se relacionan (...). "Así mismo se encontraron, aproximadamente, diez (10) cuerpos sin vida ubicados en diversas partes del campamento. "Se encontraron dos mujeres lesionadas, a las cuales se les prestaron los primeros auxilios médicos". [28]

"10. Mientras se realizaba la recolección de los elementos materiales de prueba y la filmación del lugar de los hechos, terroristas del frente 48 de las FARC continuaban disparando armas de fuego y explosivos en contra del personal militar y policial, lo cual dificultó la labor de fijación de las evidencias y la evacuación de las lesionadas". [29]

El funcionario de Policía judicial encuentra en el lugar ocho (08) elementos informáticos a saber 3 portátiles 3 discos duros y 2 memorias USB.

Respecto de los tres portátiles, les metió una USB propia para extraer archivos.

Luego apago los dispositivos.

24 Ibidem (13 pág. 2)
25 Ibidem (13 pág. 2)
26 Ibidem (13 pág. 2)
27 Ibidem (13 pág. 3)
28 Ibidem (13 pág. 3)
29 Ibidem (13 pág. 3)

	Los tres discos duros y 2 memorias USB, el funcionario conecto a su computador personal y copio y pego todos los archivos
PROPÓSITO DEL ESTUDIO DE CASO	Identificar las fuentes de derecho que regulan aspectos tratados en el caso en concreto.
	Analizar las características técnicas relacionadas con los mensajes de datos objeto de debate en el caso en concreto.
	Aplicar los conocimientos prácticos obtenidos en la Guía de Evidencia Digital y Prueba electrónica para dirimir el caso en concreto.
PREGUNTA DE REFLEXIÓN	¿Cuáles son las normas y procedimientos técnicos que se omitieron en este caso? justifique su respuesta.
UNIDAD DE ANÁLISIS	Guía de aprendizaje autodirigido de Evidencia Digital y Prueba Electrónica: Aspectos generales.
MÉTODO E INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN	Uso de método cualitativo con énfasis en comprender las perspectivas de las personas involucradas en el caso en concreto.
	Uso de instrumento de entrevista semiestructurada dirigido a funcionario judicial participante en el caso que expone hechos de la vida real.
MÉTODO DE ANÁLISIS DE LA INFORMACIÓN	La información recolectada se analizó acorde a las preguntas del caso en concreto.

11.3.3. CASO Anti soporte PATIT CORPORATION

NOTA: Caso de la vida real, se cambiaron los nombres y situaciones reales con fines académicos.

ANTECEDENTES	El 20 de diciembre de 2016, Liliana Silva, ciudadana colombiana, de edad de 19 años, quien residía en La Habana Cuba, viajó a Bogotá D.C. para pasar navidad con su familia.
	El 21 de diciembre, Liliana Silva decide realizar una videoconferencia con su novio, de nacionalidad cubana y residente en la Habana.
	La videoconferencia la realizo en su computadora marca PATIT CORPORATION comprado la noche anterior ante un establecimiento comercial distribuidor autorizado de PATIT CORPORATION

El tono de la conversación contenía temas de índole explicito.
Producto de esa conversación quedaron registros en formatos de:
i) Fotografía (archivos que contenían mensajes de datos de extensión png)
ii) Videos (archivos que contenían mensajes de datos de extensión mp4)

El 21 de diciembre, Liliana Silva notó, luego de una videoconferencia con su novio, que el computador presentó fallas. (Se apagó y no volvió a funcionar).

El 22 de diciembre Liliana Silva decidió llevar la computadora, avalada por la vigencia de la garantía, ante el establecimiento comercial distribuidor autorizado de PATIT CORPORATION,

Al llegar al establecimiento, fue atendida a través del canal de PQRS y se remitió a el área de Soporte Técnico donde le solicitaron a Liliana Silva que dejara el equipo esa noche para tener el tiempo suficiente de hacer un diagnóstico de lo que podría tener.

El 26 de diciembre el Área de Soporte Técnico del establecimiento comercial distribuidor autorizado de PATIT CORPORATION cito a Liliana para presentar diagnóstico y solución a su requerimiento. Al acudir al llamado, a Liliana Silva le comunicaron que: las fallas se debieron a unas actualizaciones de software específicas que ya fueron debidamente instaladas y el computador presentaba desempeño normal.

El 27 de diciembre, contactaron a Liliana Silva desde un número internacional, en el cual le escriben desde un chat de la aplicación WhatsApp, una exigencia de envió de fotografías desnudas de ella, extorsionándola con la amenaza que, si no cumplía con el envío, publicaría videos y fotos previas que “según” el extorsionador, tenía en su poder.

Durante los días 28, 29 y 30 se repitieron las comunicaciones vía WhatsApp desde el número internacional y como mecanismo de presión enviaron efectivamente algunos fragmentos de video y fotografías suyas de cuerpo desnudo.

El día 31 de diciembre, Liliana Silva decide ofrecer dinero al presunto delincuente, pero por recomendación de familiares bloquea su WhatsApp y solo utiliza como medio de contacto el correo personal carol@hotmail.com

El novio de Carolina, niega cualquier participación, con la cuartada que se encuentra ahora en viaje de fin de año en EE. UU.

	El presunto delincuente continúa exigiendo dinero y se pacta como medio de transacción 10 Millones en Bitcoin. La transacción se realizó finalmente el 02 de enero de 2017 a la billetera electrónica suministrada por el criminal.
	El 17 de febrero de 2017, después de una denuncia y sospecha de Liliana Silva ante el Centro de cibercrimen de la Policía, y previa orden judicial, se realiza un registro y allanamiento al establecimiento comercial distribuidor autorizado de PATIT CORPORATION Allí encuentran a un empleado que al ver la presencia de las autoridades confiesa tener en su poder abundante material videográfico de la víctima y de otras personas.
	El empleado, rompe en llanto en plena diligencia de allanamiento y confiesa que ha estado practicando el mismo modus operandi con al menos otras 04 personas en situación similar a Liliana Silva. Así mismo dice que está arrepentido y que tiene todo el material en el casillero del establecimiento.
PROPÓSITO DEL ESTUDIO DE CASO	Identificar todas las posibles fuentes de evidencia digital y las oportunidades de análisis de esta.
	Analizar las características técnicas relacionadas con los mensajes de datos objeto de debate en el caso en concreto.
	Aplicar los conocimientos prácticos obtenidos en la Guía de Evidencia Digital y Prueba electrónica para dirimir el caso en concreto.
PREGUNTA DE REFLEXIÓN	¿Cómo proceder, a la luz de las normas y estándares técnicos a la recopilación de material con miras a convertirlo en evidencia digital y respetando los derechos fundamentales de las posibles víctimas? justifique su respuesta.
UNIDAD DE ANÁLISIS	Guía de aprendizaje autodirigido de Evidencia Digital y Prueba Electrónica: Aspectos generales.
MÉTODO E INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN	Uso de método cualitativo con énfasis en comprender las perspectivas de las personas involucradas en el caso en concreto.
	Uso de instrumento de entrevista semiestructurada dirigido a funcionario judicial participante en el caso que expone hechos de la vida real.
MÉTODO DE ANÁLISIS DE LA INFORMACIÓN	La información recolectada se analizó acorde a las preguntas del caso en concreto.

12. JURISPRUDENCIA

A continuación, se presenta a él/la discente, una lista de precedentes jurisprudenciales ordenados cronológicamente para conocer los principales conceptos definidos y relacionados con la Evidencia Digital y Prueba Electrónica en Colombia.

El objetivo de esta lista es proveer a él/la discente de un instrumento de consulta directa y detallada de los conceptos unificados resultantes del ejercicio continuo de fallos jurisprudenciales, que son fuente directa de derecho aplicable a casos concretos.

AÑO	MAGISTRADO PONENTE	FUENTE DE DERECHO	RELEVANCIA	TEMA	CATEGORIA	LINK
2007	M.P. DR. JAIME CÓRDOBA TRIVIÑO	Sentencia 405/2007	Autodeterminación sobre la propia imagen.	Prevalencia del bloque de constitucionalidad.	El derecho a: la imagen, intimidad, honra y al buen nombre del ser humano.	https://www.corteconstitucional.gov.co/relatoria/2007/T-405-07.htm
2012	M.P. D.R. HUMBERTO ANTONIO SIERRA PORTO	Sentencia T-260/ 2012	Principio del interés superior del menor-consagración constitucional e internacional/derechos de los niños, niñas y adolescentes-obligación del estado de brindar una protección especial	Intimidad y habeas data en página web o sitio de internet-	Acceso a redes sociales de niños, niñas y adolescentes-debe darse con acompañamiento de los padres o personas responsables de su cuidado.	https://www.corteconstitucional.gov.co/relatoria/2012/T-260-12.HTM
2013	M. P. DRA. MARÍA VICTORIA CALLE CORREA	Sentencia T-634/2013	Régimen de Protección de Datos Personales	Derecho a la imagen, Autorización para el uso de la propia imagen	Uso de Imagen como Dato Sensible	https://www.corteconstitucional.gov.co/relatoria/2013/t-634-13.htm
2016	M.P. DR. LUIS GUILLERMO GUERRERO PÉREZ	Sentencia T-145/2016	UNIFICACIÓN DE CONCEPTOS JURISPRUDENCIALES EN TORNO A LOS CONFLICTOS OCASIONADOS EN EL	Libertad de expresión stricto sensu y libertad de información	Caso en que a través de la red social Facebook, se publicó foto del rostro de accionante en	https://www.corteconstitucional.gov.co/relatoria/2016/t-145-16.htm

AÑO	MAGISTRADO PONENTE	FUENTE DE DERECHO	RELEVANCIA	TEMA	CATEGORIA	LINK
			ÁMBITO DE LAS REDES SOCIALES [30]		primer plano, acompañada de un comentario injurioso y contrario a su buen nombre	
2016	M.P. DR. GABRIEL EDUARDO MENDOZA MARTELO	Sentencia T-050/2016	ESTADO DE INDEFENSION-Configuración cuando se da la circulación de información u otro tipo de expresiones a través de medios que producen un alto impacto social que trascienden la esfera privada de quienes se ven involucrados.	Libertad de expresión en internet y redes sociales	Estado de Indefensión	https://www.corteconstitucional.gov.co/Relatoria/2016/T-050-16.htm
2017	M.P. DR. CARLOS BERNAL PULIDO	Sentencia T-593/17	Exoneración de carga de la prueba cuando se trata de afirmaciones y negaciones indefinidas	Derechos al buen nombre y honra frente a libertad de expresión y opinión	Mensaje fue difundido mediante la aplicación "WhatsApp y Facebook.	https://www.corteconstitucional.gov.co/relatoria/2017/T-593-17.htm

30 (i) Las redes sociales pueden convertirse en centros de amenaza, en particular para los derechos fundamentales a la intimidad, a la imagen, al honor y a la honra.

(ii) Cuando se presentan amenazas o violaciones a derechos fundamentales en una red social, el problema de índole jurídico debe resolverse a la luz de las disposiciones constitucionales y no a partir de la regulación establecida por la red social específica de que se trate.

(iii) Las tecnologías de la información y las comunicaciones (redes sociales y otras) potencializan el daño causado a las víctimas de acoso y maltrato.

(iv) El derecho a la intimidad se trasgrede cuando se divulgan datos personales de alguien que no corresponden a la realidad.

(v) El derecho a la imagen emana del derecho al libre desarrollo de la personalidad y del derecho al reconocimiento de la personalidad jurídica. Se trasgrede cuándo la imagen personal es usada sin autorización de quien es expuesto o si se altera de manera falsa o injusta la caracterización que aquél ha logrado en la sociedad.

(vi) Los derechos al buen nombre y a la honra se lesionan cuando se utilizan expresiones ofensivas, falsas, erróneas o injuriosas en contra de alguien.

(vio) El derecho a la libertad de expresión, materializado a través de cualquier medio, tiene límites. Así, no ampara la posibilidad de exteriorizar los pensamientos que se tienen sobre alguien de manera ostensiblemente descomedida, irrespetuosa o injusta. (viii) El derecho a la libertad de expresión en principio tiene prevalencia sobre los derechos al buen nombre y a la honra, salvo que se demuestre que en su ejercicio hubo una intención dañina o una negligencia al presentar hechos falsos, parciales, incompletos o inexactos que violan o amenazan los derechos fundamentales de otros, en tanto los derechos de los demás en todo caso constituyen uno de sus límites.

(ix) En el ejercicio de la libertad de opinión no puede denigrarse al semejante ni publicar información falseada de éste, so pena de que quien lo haga esté en el deber de rectificar sus juicios de valor. (x) Ante casos de maltrato en redes sociales el juez constitucional debe propender porque se tomen medidas para que este cese y, además, para que se restauren los derechos de los afectados, siempre que así lo acepten éstos últimos, condición que se exige en aras de evitar una nueva exposición al público de situaciones que hacen parte de su esfera privada.

AÑO	MAGISTRADO PONENTE	FUENTE DE DERECHO	RELEVANCIA	TEMA	CATEGORIA	LINK
2018	M.P. DR. JOSÉ FERNANDO REYES CUARTAS	Sentencia T-454/18	en las redes sociales –Facebook, Twitter, Instagram, etc.- pueden generar un estado de indefensión entre particulares, debido al amplio margen de control que tiene quien la realiza	Derecho a la honra y al buen nombre frente a libertad de expresión e información, Derecho de rectificación de información, Derecho a la imagen Redes sociales	Derecho a la información y a la honra, buen nombre en sociales	https://www.corteconstitucional.gov.co/relatoria/2018/T-454-18.htm
2018	M.P. DR. CRISTINA PARDO SCHLESINGER	Sentencia T-277/18	Caso en que se realizaron publicaciones en Facebook sobre la gestión como alcalde del accionante	Derechos a la intimidad, buen nombre y honra frente a libertad de expresión y opinión-	Derechos Fundamentales	https://www.corteconstitucional.gov.co/relatoria/2018/T-277-18.htm
2018	M.P. DR. CARLOS BERNAL PULIDO	Sentencia T-121/18	Casos en que se solicita rectificación de información difundida y eliminación de video de la plataforma YouTube	Derecho a la honra y al buen nombre en redes sociales-	Derechos Fundamentales	https://www.corteconstitucional.gov.co/relatoria/2018/t-121-18.htm
2018	M.P. DRA. DIANA FAJARDO RIVERA	Sentencia T-243/18	Vulneración en red social por una publicación donde se acusaba de hurto sin haber sentencia judicial que así lo soportara	Derecho a la honra y al buen nombre de empleada doméstica en redes sociales-	Derechos Fundamentales	https://www.corteconstitucional.gov.co/relatoria/2018/T-243-18.htm
2019	M.P. DR. ALEJANDRO LINARES CANTILLO	Sentencia T-179/19	No se reconoce protección constitucional a los derechos fundamentales a la honra, intimidad y buen nombre	Libertad de expresión en redes sociales	Derechos Fundamentales	https://www.corteconstitucional.gov.co/relatoria/2019/T-179-19.htm#_ftn15

13. BIBLIOGRAFÍA

1. Rae.es. (2019). *Real Academia Española. [online] Available at: https://www.rae.es/ransomware [Accessed 22 Dec. 2019].*

2. Restrepo, Alexander. *Manual de Autores para el diseño y redacción de módulos de Aprendizaje Autodirigido.* Bogotá D.C.: Consejo Superior de la Judicatura, 2019.

3. Inc, Digital Intelligence. *YouTube. [En línea] Digital Intelligence Inc, 8 de febrero de 2018. [Citado el: 22 de enero de 2020.] https://www.youtube.com/watch?v=FJF0WezsS2k&feature=youtu.be.*

4. Accessdata. [En línea] 2019. *https://accessdata.com/product-download.*

5. INTERPOL. eluniversal.com. [En línea] 2008. *http://static.eluniversal.com/2008/05/15/infointerpol.pdf.*

6. IBM. *Certificados digitales*. s.l.: IBM, 2019.

7. BOGOTÁ, CAMARA DE COMERCIO DE. Camara Comercio Bogotá 19/12/2019, . *Firma digital y estampado cronológico*. [En línea] 2019. https://www.ccb.org.co/Inscripciones-y-renovaciones/Registro-Unico-de-Proponentes/Tramites-virtuales-del-Registro-Unico-de-Proponente.

8. Wikipedia. Wikipedia. Drones. [En línea] 2019. *https://es.wikipedia.org/wiki/Veh%C3%ADculo_a%C3%A9reo_no_tripulado.*

9. Aepd. [En línea] 2019. https://www.aepd.es/sites/default/files/2019-09/guia-drones.pdf.

10. Rivera, Nicolas. *Hipertextual. hipertextual.com.* [En línea] 20 de junio de 2015. [Citado el: 22 de enero de 2020.] https://hipertextual.com/2015/06/internet-of-things.

11. ESET. Técnicas antiforenses. *welivesecurity.com.* [En línea] 2 de julio de 2015. [Citado el: 22 de enero de 2020.] https://www.welivesecurity.com/la-es/2015/07/02/tecnicas-anti-forenses.

12. PENAL, CORTE SUPREMA DE JUSTICIA SALA DE CASACIÓN. *Sentencia Proceso* No 29.877. Colombia: CJS, 2011.

13. Colombia, Corte Suprema de Justicia. ambitojuridico.com. *ambitojuridico.com.* [En línea] 18 de mayo de 2011. [Citado el: 22 de enero de 2020.] https://www.ambitojuridico.com/BancoMedios/Documentos%20PDF/auto%2029877%20(01-08-2011)%20reposici%C3%B3n%20wilson%20borja.pdf.

Podcast Evidencia Digital:
https://anchor.fm/evidenciadigital

CONSEJO SUPERIOR DE LA JUDICATURA
ESCUELA JUDICIAL "RODRIGO LARA BONILLA"

escuelajudicial.ramajudicial.gov.co
CALLE 11 # 9 A – 24, PISO 4
PBX (+57) 355 06 66
BOGOTÁ D.C., COLOMBIA
2020