Universidad de Buenos Aires

Facultades de Ciencias Económicas,

Ciencias Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final de Especialización

Tema

Informática Forense

Título

- Normalización de la Práctica Forense -

Subtítulo

- Una mirada hacia un Sistema de Gestión de Evidencia Digital -

Autor: Lic Antonio Javier Maza

Tutor: Ing Hugo Pagola.

Agosto 2019

Cohorte: 2017

[Página dejada en blanco intencionalmente]

LICENCIA

Bajo los siguientes términos

Atribución: en cualquier explotación de la obra autorizada por la licencia será necesario reconocer la autoría (obligatoria en todos los casos).

No Comercial: la explotación de la obra queda limitada a usos no comerciales.

Sin obras derivadas: la autorización para explotar la obra no incluye la posibilidad de crear una obra derivada.

DECLARACION JURADA

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

Lic. Antonio Javier Maza

DNI 27.810.784

0.1 Resumen ejecutivo

El presente Trabajo Final de Especialización tiene como finalidad exponer los principios de la informática forense y actividades vinculadas con la obtención de evidencia digital, basados en reglas de buena práctica, instructivos, procedimientos operativos, manuales, guías, normas y estándares existentes en la materia.

En tal sentido, el objetivo principal es brindar un marco de referencia integral, mediante la yuxtaposición de documentos técnicos inherentes al cómputo forense y evidencia digital, permitiendo una interpretación práctica e implementación en una organización de cualquier índole, con independencia de su actividad o envergadura, como así también su ejecución por parte de profesionales con incumbencia en ese ámbito, garantizando en todo momento el cumplimiento de principios fundacionales aceptados por la comunidad científica, lo que permitirá:

- Obtener una visión integral respecto de las reglas de buena práctica en torno del análisis forense e investigación digital.
- Realizar una autoevaluación que posibilite identificar de forma ágil el estado de madurez de una organización y adoptar una conducta proactiva.
- Incrementar la eficacia y eficiencia de las metodologías aplicadas en los laboratorios forenses digitales.
- Evaluar la posibilidad de establecer un Sistema de Gestión de Evidencia Digital en pos de la mejora continua.

Del mismo modo, cabe destacar la importancia que la informática forense ha tomado en torno a la seguridad de la información, ya que se encuentra estrechamente vinculada con la gestión de riesgos de una empresa, brindando un conjunto de herramientas y el conocimiento necesario para identificar las causas basales que dieron lugar a un incidente disruptivo, así como su impacto y alcances dentro de la infraestructura tecnológica de una organización.

Palabras Clave

Reglas de buena práctica, Instructivos, Procedimientos Operativos, Manuales, Guías, Normas, Estándares, Informática Forense, Cadena de Custodia, Identificación, Preservación, Análisis, Presentación, Dispositivo Informático, Evidencia Digital, Recolección, Adquisición, Imagen Forense, Valor Hash, Incidente, Amenazas, Internet, Ciberespacio, Cibercrimen.

0.2 Índice de contenidos

1 Introducción 11
1.1 Planteamiento del problema 13
1.2 Objetivo General 14
1.3 Objetivos Específicos 14
1.4 Alcance y limitaciones 14
1.5 Criterio de selección de normas y estándares 15
1.6 Orígenes 16

2 Materiales y métodos 17
2.1 Marco teórico conceptual 17
2.1.1 Conceptos fundamentales básicos 17
2.1.2 El Crimen Organizado 2.0 24
2.1.3 Principales amenazas en materia de cibercrimen 27
2.1.4 Aspectos legales en nuestro país 31
2.1.5 El convenio de Budapest 34
2.2 Marco Teórico Referencial 36
2.2.1 La Evidencia Digital 37
2.2.2 La Informática Forense [14] 40
2.2.3 Normas y estándares vinculados a la Informática Forense 42

3 Resultados 51
3.1 Confronte de normas y estándares forenses 52
3.1.1 Etapa preparativa 53
3.1.2 Etapa de identificación 54
3.1.3 Etapa de preservación 55
3.1.4 Etapa de análisis 56
3.1.5 Etapa de presentación 57
3.1.6 Etapa de evaluación 58
3.2 Identificación de roles y competencias requeridas 59
3.2.1 El investigador 60
3.2.2 El primer interviniente en manejo de evidencia digital 61
3.2.3 El especialista en análisis de evidencia digital 62
3.3 Metodología general para el análisis forense 63
3.4 Ciclo de vida y categorización de la evidencia digital 63

4 Conclusiones 65

5 Bibliografía específica 67

6 Anexos 73
6.1 Equipamiento básico para el primer interviniente 73
6.1.1 Elementos para resguardo 73

6.1.2 Equipamiento específico 74
6.2 Adquisición de imágenes Forenses 75
6.2.1 Consideraciones generales 75
6.2.2 Bloqueadores de escritura 76
6.2.3 Adquisición bajo entornos Windows y Linux 79
6.2.4 Adquisición de dispositivos móviles 93
6.3 Cadena de custodia 97
6.3.1 Anverso 97
6.3.2 Reverso 98
6.4 Herramientas Forenses 99
6.4.1 Autopsy 99
6.4.2 Digital Forensics Framework (DFF) 101
6.4.3 Bulk Extractor 103
6.4.4 DEFT 104
6.4.5 CAINE 105
6.4.6 FTK Imager 107
6.4.7 EnCase 108
6.4.8 Magnet AXIOM 109
6.4.9 UFED 4 PC 110
6.4.10 Oxygen Forensic 111
6.5 Firmas de archivo 115

0.3 Índice de ilustraciones

Ilustración 1: Distintos alcances del análisis forense digital. 19
Ilustración 2: Principales amenazas en materia de cibercrimen. 31
Ilustración 3: Orden de volatilidad de la Evidencia Digital. 39
Ilustración 4: Fases del análisis forense digital. 40
Ilustración 5: Roles y responsabilidades. 59
Ilustración 6: Metodología general para el análisis forense. 63
Ilustración 7: Categorización de la evidencia digital. 64
Ilustración 8: Bloqueador de escritura Tableau T35u (SATA/IDE) 77
Ilustración 9: Bloqueador de escritura Phrozen Safe USB v1.0. 78
Ilustración 10: FTK Imager - Creación de imagen de disco 80
Ilustración 11: FTK Imager - Selección de tipo de origen. 81
Ilustración 12: FTK Imager - Selección de disco de origen. 81
Ilustración 13: FTK Imager - Selección de formato de imagen. 82
Ilustración 14: FTK Imager - Información de la evidencia. 82
Ilustración 15: FTK Imager - Selección de ruta de destino. 83
Ilustración 16: FTK Imager - Chequeo de parámetros y 83
Ilustración 17: FTK Imager – Obtención de la imagen 84
Ilustración 18: FTK Imager – Verificación de la imagen. 84
Ilustración 19: FTK Imager – Finalización del proceso. 85
Ilustración 20: FTK Imager – Reporte correspondiente. 85
Ilustración 21: Guymager - Ventana de inicio. 86
Ilustración 22: Guymager - Configuración de la Imagen. 87
Ilustración 23: Guymager - Inicio de la adquisición. 87
Ilustración 24: Guymager - Finalización de la adquisición. 88
Ilustración 25: Guymager - Reporte de la imagen forense. 88
Ilustración 26: Comando DD - Identificación del medio de origen. 90
Ilustración 27: Comando DD - Hash SHA1 del medio de origen 91
Ilustración 28: Comando DD - Obtención de la imagen forense y resumen. 91
Ilustración 29: Comando DD – Hash de la imagen forense. 92
Ilustración 30: Comando DD – Comprobación de la imagen forense. 92
Ilustración 31: Herramienta forense Autopsy. 101
Ilustración 32: Herramienta forense Digital Forensics Framework. 102
Ilustración 33: Herramienta forense Bulk Extractor. 104
Ilustración 34: Herramienta forense DEFT. 105
Ilustración 35: Herramienta forense CAINE. 106
Ilustración 36: Herramienta forense FTK Imager. 107
Ilustración 37: Herramienta forense EnCase. 109
Ilustración 38: Herramienta forense Magnet AXIOM. 110
Ilustración 39: Herramienta forense UFED 4 PC. 111
Ilustración 40: Herramienta forense Oxygen Forensic. 113

0.4 Índice de Tablas

Tabla 1: Etapa preparativa..... 53
Tabla 2: Etapa de identificación. 54
Tabla 3: Etapa de Preservación. 55
Tabla 4: Etapa de Análisis. 56
Tabla 5: Etapa de Presentación. 57
Tabla 6: Etapa de Evaluación. 58
Tabla 7: El investigador; actividades y competencias requeridas. 60
Tabla 8: El primer interviniente; actividades y competencias requeridas. 61
Tabla 9: El especialista en análisis; actividades y competencias requeridas. 62
Tabla 10: Ventajas y desventajas de los bloqueadores de escritura por hardware. 78
Tabla 11: Ventajas y desventajas de los bloqueadores de escritura por software..... 79
Tabla 12: Listado con firmas de archivos. 113

[Página dejada en blanco intencionalmente]

1

Introducción

El constante avance de la tecnología de la información trae aparejado fenómenos sociales, políticos y económicos, entre otros, al igual que resulta un escenario propicio para la proliferación de diferentes modalidades delictivas.

Sin duda, el cibercrimen se ha convertido en una de las actividades criminales más rentables de los últimos tiempos, cuyos ingresos anuales durante el último periodo ascienden aproximadamente al billón y medio de dólares americanos.

Si hiciéremos un paralelismo con el PIB de los países más ricos del mundo, el cibercrimen ocuparía la onceava posición inmediatamente después de Canadá y antes que Corea del Sur, con un ingreso que promedia los mil quinientos millones de dólares americanos.

Resulta quizás uno de los fenómenos de mayor crecimiento a escala global, fomentado por el anonimato, la interconectividad y transnacionalidad, permitiendo que delincuente cibernético pueda encontrarse en Singapur, el sistema afectado en Nueva York y la víctima en Argentina.

Por tal motivo, la complejidad de este panorama requiere del trabajo mancomunado de las múltiples partes interesadas, fomentando el networking y la colaboración internacional, tanto desde el punto de vista de agentes encargados de hacer cumplir la ley, operadores judiciales, demás organismos del Estado, entidades del sector privado y ciudadanos.

Aun así, Internet ha impulsado grandes cambios en la sociedad en la que vivimos, modificando la forma en que nos relacionamos e impactando directamente en el mundo que nos rodea.

Ya en el año 2011 la Asamblea General de las Naciones Unidas declaró que el acceso a Internet es un derecho humano, por tratarse de una herramienta que colabora activamente en el crecimiento y progreso de la sociedad.

Sin lugar a dudas Internet se ha convertido en un instrumento imprescindible que promueve la libertad de expresión, por cuanto más que un canal de comunicación, ésta se ha convertido en una necesidad por el grado de interconectividad existente a nivel global.

La era digital e Internet se han incrustado en el ADN del ser humano, llevándonos a trascender tiempo y espacio, seguramente en el futuro, nuestra generación sea recordada por haber colonizado el ciberespacio, aprendimos a convivir en línea, sin embargo la fragilidad de este ecosistema digital nos hace permeables a todo tipo de amenaza cibernética.

Internet es la tecnología que nos catapultó desde la era industrial a la era de la información y posteriormente del conocimiento. Esta red interconectada que opera inclusive sin necesidad de medios físicos, nos permite interactuar en todo momento y lugar, de diferentes maneras y libre de cualquier límite espacial.

Si bien Internet no es algo nuevo, Arpanet[1] (su primer antepasado) se desarrolló en el año 1969, pero no estuvo disponible para los usuarios particulares sino hasta la década de 1990, propagándose por el mundo a una velocidad extraordinaria.

Hoy podemos decir sin temor a equivocarnos que casi la totalidad de la población mundial se encuentra conectada, a pesar de la brecha digital en algunas regiones, contabilizándose un total de 7.000 millones de dispositivos inalámbricos diseminados en todo el planeta tierra, cuya población asciende a 7.700 millones de habitantes.

Internet es el centro de las comunicaciones, alimentándose diariamente de millones de datos que crecen exponencialmente, al punto que en algún momento toda la información del mundo podría encontrarse digitalizada y disponible on-line.

[1] Acrónimo de *Advanced Research Projects Agency Network*, red creada por encargo del Departamento de Defensa de los Estados Unidos.

Vivimos al ritmo vertiginoso de la información, la comunicación transforma nuestro entorno y se manifiesta en diferentes aspectos, sin embargo a pesar de los múltiples intentos para regular las actividades desarrolladas en el ciberespacio no se vislumbra posibilidad fáctica de establecer una soberanía en ese ámbito [1].

1.1 Planteamiento del problema

La computación forense es una disciplina que desde sus orígenes se ha materializado como un desafío para los profesionales de ciencias de la computación y tecnología de la información, como así también para los criminalistas tradicionales.

En la actualidad, resulta indudable la necesidad de contar con profesionales en la materia, dotados de un amplio grado de experticia, que actúen en aquellos casos donde la informática y la tecnología se encuentren presentes, en consonancia con procedimientos básicos de la criminalística y reglas de buena práctica forense, de amplia aceptación por la comunidad científica y que permita garantizar el valor probatorio de la información digital en el marco de una investigación judicial.

El constante avance de la tecnología, al igual que su profunda inserción en la vida de las personas e implementación en las organizaciones y nuevas arquitecturas de negocios, conforman un ecosistema de múltiples partes interesadas, que evoluciona a un ritmo vertiginoso y cada vez con mayor tendencia al entorno digital.

En ese mismo orden de ideas, desde una perspectiva criminalística, a las evidencias tradicionales relevadas en el lugar del hecho, tales como armas de fuego, huellas digitales, fluidos corporales, etc, se incorporan los rastros digitales contenidos diferentes soportes de almacenamiento como por ejemplo discos rígidos, discos de estado sólido, discos ópticos, dispositivos USB, dispositivos de conexión y equipos de telefonía celular, entre otros elementos.

Por tal motivo, en virtud del incremento de ataques informáticos y auge del cibercrimen en la región, resulta imprescindible que las organizaciones empoderen a la informática forense como parte integral de las políticas, normas y procedimientos organizacionales, alineada con los intereses y continuidad del negocio, logrando de esta manera mayor transparencia en la gestión de incidentes, aportando valor

agregado y una considerable reducción de costos vinculados a incidentes de seguridad, sobre la base de una mejora continua de calidad y excelencia.

1.2 Objetivo General

- Brindar un marco de referencia integrador mediante la investigación sobre documentación técnica relacionada al cómputo forense y evidencia digital, a fin de facilitar su interpretación por parte de aquellos profesionales que deban implementar este tipo de normativa en el ámbito de la Seguridad de la Información.

1.3 Objetivos Específicos

- Adquirir un amplio conocimiento sobre documentación técnica relacionada a la informática forense y relevamiento de evidencia digital.
- Proporcionar conciencia sobre la importancia de la informática forense y su estrecha relación con la gestión de incidentes.
- Facilitar la identificación del estado de madurez de una organización mediante su autoevaluación.
- Sentar el andamiaje sobre el que reposará el trabajo de Tesis de Maestría, sirviendo como guía para un abordaje de mayor profundidad y elaboración de un Sistema de Gestión de Evidencia Digital.

1.4 Alcance y limitaciones

En razón de la complejidad del objeto de estudio, el ecosistema digital y ciclo de vida de la evidencia digital, por lo que se definen como bases del mismo:

- Se realizará un análisis crítico sobre documentación técnica existente y vinculada con los pilares de la informática forense, con origen en el ámbito nacional e internacional.

- El análisis de la documentación se efectuará independientemente de los tipos de dispositivos o sistemas operativos existentes en el mercado, circunscribiéndose al plano teórico.
- En virtud del tipo de estudio practicado, no se realizaran simulaciones con dispositivos físicos, limitándose únicamente a efectuar recomendaciones sobre determinadas técnicas y/o herramientas forenses.
- Se delineará un marco de trabajo que permitirá un abordaje de mayor profundidad sobre la disciplina planteada mediante la Tesis de Maestría.
- Se dejará abierta la posibilidad de realizar una revisión sobre legislación y antecedentes jurídicos en la materia, a fin de evaluar su posible vinculación e impacto sobre los procedimientos técnicos.

1.5 Criterio de selección de normas y estándares

Durante la etapa de relevamiento de reglas de buena práctica, instructivos, procedimientos operativos, manuales, guías, normas y estándares existentes en materia de informática forense y evidencia digital, se realizó una minuciosa y exhaustiva investigación sobre toda aquella documentación que potencialmente podría ser incorporada.

Cabe destacar el esfuerzo que implicó llevar adelante tal actividad, en virtud de la cantidad de documentación existente y variedad de autores, tanto de organismos oficiales como entidades del sector privado a nivel nacional e internacional, a pesar de la existencia de ciertos referentes y documentos con mayor reconocimiento en la comunidad científica internacional.

Por tal motivo, se determinó la necesidad de contar con un criterio que permita seleccionar aquellos documentos que serían añadidos al presente trabajo, el que consistió en incorporar normas cuyo contenido se encuentre estrechamente vinculado con el análisis forense digital y etapas del mismo desde una perspectiva amplia, excluyendo todo aquel documento con predominancia de cuestiones técnicas, herramientas y/o acotadas únicamente a la fase de investigación digital.

1.6 Orígenes

Durante el presente trabajo, se pretende clasificar y correlacionar reglas de buena práctica, instructivos, procedimientos operativos, manuales, guías, normas y estándares existentes en materia de informática forense y evidencia digital, con el objetivo de someter a un mismo plano de comparación dicha documentación. Entre los documentos incorporados, se encuentran:

- Guía Para Recolectar y Archivar Evidencia (RFC 3227/2002) [2].
- Directrices para la Gestión Evidencia de Tecnología Informática (SAI HB 171/2003) [3].
- Guía para integrar técnicas forenses en respuesta a incidentes (NIST 800-86-2006) [4].
- Investigación en la Escena del Crimen Electrónico: una guía para primeros intervinientes (US DoJ NCJ 219941/2008) [5].
- Computación Forense - Parte 2: mejores prácticas (ISFS/2009) [6].
- Guía de Buenas Prácticas para evidencia basada en computadoras (ACPO/2012) [7].
- Evidencia Electrónica - Una guía básica para primeros intervinientes (ENISA/2014) [8].
- Principios para identificación, recolección, adquisición y preservación de pruebas digitales (ISO/IEC 27037/2016) [9].
- Guía de obtención, preservación y tratamiento de evidencia digital (PGN 756/2016) [10].
- Protocolo General de Actuación para las Fuerzas Policiales y de Seguridad en la investigación y proceso de recolección de pruebas en Ciberdelitos (MINSEG RES 234/2016) [11].

2
Materiales y métodos

En este capítulo se plasmarán una serie de conceptos que se consideran necesarios para la correcta comprensión del presente trabajo.

2.1 Marco teórico conceptual

En este apartado se aportarán conceptos del área de conocimiento general mediante conceptos y/o teorías de importancia.

2.1.1 Conceptos fundamentales básicos

A continuación, se brindan una serie de definiciones básicas relacionadas con la informática forense:

2.1.1.1 Informática

Ciencia de la información automatizada. Tiene relación con el procesamiento de datos y, para ello, utiliza las computadoras y/o los equipos de procesos automáticos de información [12].

2.1.1.2 Forense

Conjunto de disciplinas científicas que ayudan a la policía y a la justicia a determinar las circunstancias exactas de la comisión de una infracción y a identificar a sus autores [13].

2.1.1.3 Análisis forense digital

Disciplina de las ciencias forenses que se encarga de identificar, preservar, analizar y presentar datos que han sido procesados electrónicamente, y almacenados en un medio digital [14].

2.1.1.4 Computación forense

Rama del análisis forense digital cuyo objetivo es el estudio de sistemas informáticos, medios de almacenamiento o documentos electrónicos [15].

2.1.1.5 Análisis forense de dispositivos móviles

Subdivisión del análisis forense digital relacionado con la recuperación de evidencia digital de dispositivos móviles [15].

2.1.1.6 Análisis forense de redes

Variante del análisis forense digital que se ocupa de la supervisión y el estudio del tráfico de la red informática en sus diferentes formatos, a fin de recolectar evidencia digital o detectar intrusos [15].

2.1.1.7 Análisis forense de datos

Rama del análisis forense digital que tiene como finalidad examinar datos estructurados con el objetivo de descubrir y determinar patrones de actividades fraudulentas [15].

2.1.1.8 Análisis forense de base de datos

Subdivisión del análisis forense digital relacionada con el estudio de bases de datos y sus metadatos [15].

Ilustración 1: Distintos alcances del análisis forense digital.

2.1.1.9 Archivos de evidencias lógicas

Es probable que las copias de respaldo de evidencias lógicas de datos a partir de dispositivos de origen "activos" sean una fuente primaria de datos relevantes. Estos incluirían redes de datos, servidores de archivos, servidores de correo electrónico, computadoras de escritorio, computadoras portátiles, máquinas virtuales e incluso teléfonos inteligentes.

Es probable que al momento de la realización del análisis forense estos sistemas estén en uso o se hayan retirado recientemente y probablemente contengan datos que puedan conservarse o recopilarse durante operaciones regulares.

Ejemplos de datos que podrían ser obtenidos mediante copias de seguridad de evidencias lógicas incluyen documentos de texto, hojas de cálculo, imágenes, código fuente o correos electrónicos almacenados en un servidor con años de antigüedad.

Los registros electrónicos no deben ser pasados por alto como fuentes de datos relevantes, archivar es el proceso de mover datos de sistemas, como el correo electrónico, a otro sistema, como a un servidor de archivos, paquetes de datos, tablas de conexión, etc.

Del mismo modo, las copias de seguridad de sistemas y datos generadas como parte de las operaciones regulares de una empresa u organización, son una fuente de datos para preservación y recolección por parte de los investigadores forenses. Es probable, además, que existan procesos escritos, registros técnicos asociados y que se realicen de manera periódica.

Por otro lado, la mayoría de las empresas u organizaciones rotan sus medios de respaldo a través de un cronograma de almacenamiento, ya sea dentro o fuera de sus instalaciones. Dependiendo del período de tiempo en el que se requieran los datos, será necesario que el investigador forense tenga que recuperar copias de seguridad externas.

2.1.1.10 Imágenes forenses

A continuación, se brindan una serie de definiciones básicas relacionadas con la adquisición de imágenes forenses:

- Copia bit a bit: réplica exacta de los bits de un volumen lógico o de una unidad física. Cuando la copia se realiza en otro disco, se la denomina duplicado forense. Cuando la copia se realiza en uno o varios archivos, se la denomina imagen forense.
- Duplicado forense: conjunto de archivos que se obtiene creando una copia exacta de un dispositivo de almacenamiento. Dicha copia replica la estructura y contenidos en un nuevo dispositivo.
- Imagen forense: archivo o conjunto de archivos que se obtiene al crear una copia completa de un dispositivo de almacenamiento, replicar su estructura y contenidos e incluir el espacio libre y el espacio no asignado.

- Imagen forense sin formato (RAW): imagen sin formato que no contiene metadatos y no está comprimida. Puede adjuntarse por separado un archivo que contiene metadatos sobre la imagen, como fecha en que fue adquirida, nombre de la herramienta utilizada y hash criptográfico.
- Imagen forense embebida: imagen de disco que contiene incrustados metadatos sobre la imagen, tales como nombre de la herramienta utilizada, fecha de adquisición, datos relacionados al caso, investigador, evidencia relevada y hash criptográfico correspondiente.

2.1.1.11 Estándares de imágenes forenses

Las imágenes forenses generalmente se almacenan en formatos especializados y propietarios, que en ocasiones incluyen metadatos sobre la evidencia recolectada, entre los que se encuentran:

- *Advanced Forensic Format* (AFF): es de formato abierto y posee tres variantes: AFF, AFD y AFM. AFF almacena todos los datos y metadatos en un solo archivo, AFD almacena los datos y metadatos en múltiples archivos pequeños, y por último, AFM almacena los datos en un formato sin procesar y los metadatos se almacenan en un archivo separado.
- *Expert Witness* (EWF): formato abierto desarrollado por ASR Data. Las imágenes de disco como EWF incluyen metadatos integrados, como la fecha de creación, datos proporcionados por el usuario y otros elementos necesarios para una correcta cadena de custodia y auditoría.
- EnCase[2] (EF): formato propietario definido por Guidance Software para su uso por intermedio de la herramienta forense EnCase. Su formato predecesor es el formato Expert Witness, al que agregó nuevos metadatos. Podría decirse que es el estándar de facto para el análisis forense por parte de fuerzas de

[2] EnCase es una plataforma de informática forense desarrollada por la firma "GUIDANCE SOFTWARE", que posee un conjunto de funcionalidades específicas destinadas a la identificación, análisis, preservación y presentación de evidencia digital.

seguridad y agentes de la ley.

- *Generic Forensic Zip* (Gfzip): formato abierto que si bien utiliza estructuras similares a AFF, los metadatos y el enfoque de almacenamiento son diferentes. Un archivo gfzip puede ser compatible en bruto para que los metadatos se almacenen después de los datos de evidencia y también ofrece un modo empaquetado donde los bloques de datos redundantes no se almacenan.
- iXImager: utilizado por la herramienta iLook, desarrollada por el Servicio de Rentas Internas (IRS) del gobierno de Estados Unidos. Dicho formato está restringido a la aplicación de la ley y uso exclusivo del gobierno.
- ProDiscover: formato abierto definido por Technology Pathways para su empleo en la familia de herramientas de seguridad ProDiscover. Incluye metadatos integrados relacionados a la imagen forense, como la fecha de obtención, datos del caso proporcionados por el usuario, etc.
- RAW (DD, RAW, IMG): formato sin procesar compuesto simplemente por un archivo que contiene los datos exactos que se deben almacenar. El archivo podría contener cualquier tipo de datos, incluidos sectores de disco duro, archivos y paquetes de red. Los archivos brutos pueden ser fácilmente creados y leídos por cualquier herramienta, pero no almacenan ningún metadato y no se comprimen.

Sin perjuicio de lo expresado, resulta importante señalar que en la actualidad los dos formatos que se utilizan con mayor frecuencia son el formato de archivo de evidencia EnCase y los formatos de archivo de imagen en bruto.

2.1.1.12 Concepto de Hash

Se define al HASH[3] como el proceso de tomar una cantidad de datos determinada (como un archivo o el flujo de bits de un disco duro) y aplicar un

3 El algoritmo HASH es una función algebraica unidireccional que permite representar datos de longitud variable como un dato de longitud fija, tiene como objetivo garantizar la integridad de los registros informáticos.

algoritmo matemático complejo para generar un identificador numérico relativamente compacto (el valor hash) exclusivo de esos datos [16].

Como ejemplo, un valor hash generado respecto de un documento será único; si se modificara, alterara o destruyere parcialmente dicho documento, el valor hash resultante será diferente.

Existen varios puntos relevantes sobre los algoritmos hash.

- Son irreversibles. Los algoritmos (funciones hash iterativas y unidireccionales) que se utilizan para generar el valor de hash no se pueden revertir para reconstruir los datos originales de entrada [17].
- Baja probabilidad de colisiones. Las probabilidades de que dos datos no idénticos generen el mismo algoritmo es ínfima y se encuentra limitada por formato del algoritmo empleado. A modo de ejemplo se pueden citar el formato MD5[4] el cuál se trata de un algoritmo de reducción criptográfico de 128 bits cuya longitud es de 32 caracteres o el formato SHA1[5] , el cuál se trata de un algoritmo de reducción criptográfico de 160 bits cuya longitud es de 40 caracteres.

2.1.1.13 Firmas de archivo

En computación forense, la firma de un archivo o “número mágico” es aquella información utilizada para identificar o verificar el contenido de un archivo. En particular, se refiere a aquellos bytes ubicados al principio de un archivo que son utilizados para identificar el formato del archivo, si bien no existe una longitud determinada, en general se encuentran representados por una secuencia corta de bytes.

4 Acrónimo de "Message-Digest Algorithm 5", el cuál se trata de un algoritmo de reducción criptográfico de 128 bits cuya longitud es de 32 caracteres.
5 Acrónimo de "Secure Hash Algorithm 1", el cuál se trata de un algoritmo de reducción criptográfico de 160 bits cuya longitud es de 40 caracteres.

2.1.1.14 Artefacto forense

Este término hace referencia a cualquier registro informático correspondiente a una aplicación o programa de software, que desempeña alguna función específica.

2.1.1.15 Cadena de custodia

Es el registro cronológico y minucioso de la manipulación adecuada de los elementos, rastros e indicios hallados en el lugar del hecho, durante todo el proceso judicial [18].

2.1.2 El Crimen Organizado 2.0

Desde sus inicios, este tipo de organizaciones han tenido como único objetivo adquirir un mayor rédito económico, adoptando diferentes técnicas y/o maniobras criminales.

Estas estructuras criminales han mutado a lo largo del tiempo, en busca de nuevos horizontes que permitan desarrollar sus actividades, donde Internet se ha convertido en el principal facilitador.

En tal sentido, los crímenes convencionales han migrado al ciberespacio, fruto de una sociedad cada vez mas informatizada y sustentados por los avances de la tecnología, generando nuevas amenazas.

Como conjugación de los factores señalados, podría decirse que un nuevo paradigma delincuencial se encuentra pleno desarrollo y evolución, marcado por grupos cuyos integrantes poseen alto grado de profesionalidad, que no necesariamente se encuentran en el mismo espacio o lugar físico, lo que les permite operar en diferentes jurisdicciones.

Hoy el cibercrimen se ha posicionado como un tema de actualidad, despertando el interés de diferentes sectores y al mismo tiempo una gran señal de alerta.

Como ya hemos planteado, el avenimiento de la era digital ha propiciado que la tecnología de la información penetre en la sociedad, donde Internet ha jugado un papel preponderante, convirtiéndose en canal de comunicación que promueve la interconexión entre los seres humanos y organizaciones de todo tipo, facilitando la generación y diseminación de conocimiento.

Sin embargo, el uso intensivo de esta tecnología en pos del desarrollo de las actividades económico-sociales, en un mundo donde cada día estamos mas interconectados, ha permitido el surgimiento de conductas delictivas que con el pasar del tiempo han mutado hasta alcanzar un alto grado de sofisticación, convirtiéndose en verdaderas amenazas para esta comunidad digital en la que hoy nos encontramos inmersos.

2.1.2.1 Sentido formal

Según este punto de vista podríamos decir que el cibercrimen versa sobre aquellas actividades delictivas contempladas dentro del marco legal vigente.

- Contenido de material relacionado con abuso de menores (Ley 26388, 2008) [19].
- Accesos no autorizados (Ley 26388, 2008) [19].
- Interceptación de comunicaciones (Ley 26388, 2008) [19].
- Violación de secretos (Ley 26388, 2008) [19].
- Fraude electrónico (Ley 26388, 2008) [19].
- Daños informáticos (Ley 26388, 2008).
- Denegación de servicio (Ley 26388, 2008) [19].
- Ciberacoso (Ley 26904, 2013) [20].
- Infracciones a la propiedad intelectual (Ley 11723, 1933) [21].
- Infracciones marcarias (Ley 22362, 1980) [22].

2.1.2.2 Sentido amplio

En este aspecto, la conducta delictiva guarda relación con todas aquellas actividades donde las tecnologías de la información se encuentran presentes ya sea como fin, medio o mero símbolo, como por ejemplo:

- *Phishing*.
- *Sextorsion*.
- Suplantación de identidad digital.
- Compromiso de e-mail corporativo.

2.1.2.3 Cuantificación de la actividad cibercriminal

Debido a la confluencia de diferentes factores, resulta muy difícil cuantificar los motivos y alcance de los incidentes de seguridad que atentan contra la seguridad de la información, ya sea personal u organizacional.

- Las organizaciones son reticentes a informar incidentes de seguridad, por temar a sufrir pérdida de reputación y clientes.
- Los usuarios no reportan incidentes de seguridad debido a las dificultades que afrontan para dar a entender lo sucedido.
- La inexistencia de estadísticas oficiales o bien datos inconsistentes reportados por diferentes organismos.
- La complejidad que conlleva determinar el impacto real de un incidente de seguridad en materia de cibercrimen.
- La dificultad para recolectar datos que permitan para auditar las actividades involucradas en un incidente.
- La falta de una estandarización que permita cuantificar incidentes de forma homogénea.

2.1.2.4 Características de los grupos criminales

Si bien debido a la complejidad de las organizaciones criminales no resulta factible definir este fenómeno, si resulta posible señalar algunas características que las identifican.

- Poseen una estructura jerárquica claramente establecida, con alto grado de adaptabilidad, lo que les permite mantenerse en el tiempo.
- Restringen la selección de sus miembros, quienes deben posees capacidad con alta exigencia profesional.
- Se destacan por el grado de profesionalismo con el que realizan sus actividades, llegando al grado de captar especialistas para determinadas tareas.
- Sus actividades criminales revisten un grado de complejidad elevado y son desarrolladas a nivel internacional.

2.1.2.5 Cibercrimen como servicio

En la actualidad, debido a la rentabilidad del modelo de negocio de servicios en Internet los cibercriminales proporcionan soporte para quienes deseen contratarlos, ya sea para introducirse en este mundo y obtener un rédito económico o bien solamente para adquirir algún tipo de producto, como por ejemplo malware diseñado a medida.

Este tipo de actividades se desarrollada por sujetos con un alto grado de experiencia y conocimiento técnico, quienes tienen inclusive cierta reputación que los avala.

2.1.3 Principales amenazas en materia de cibercrimen

El cibercrimen se ha instaurado como una amenaza latente en la vida que nos rodea y el entorno digital donde desarrollamos nuestras actividades, ya sea como individuos o sociedad, al mismo tiempo que las estadísticas indican que las víctimas se incrementan de forma exponencial.

Durante los últimos periodos se ha visto que la tendencia de actividades cibercriminales ha evolucionado notablemente, expandiéndose hacia diferentes sectores como la salud y el sector financiero.

La sustentabilidad y crecimiento de este tipo de actividades genera un movimiento continuo de las propias organizaciones criminales, las cuales se ven obligadas a expandirse sin restricciones geográficas.

A este fenómeno se suma en contrapartida la alta demanda de profesionales en materia de seguridad de la información, a fin de afrontar este flagelo que muy lejos está de ser contenido y mucho menos mitigado, mutando constantemente en diferentes tipos de actividades cibercriminales y marcando tendencias [23].

2.1.3.1 Ransomware

A pesar de las múltiples campañas de concienciación llevadas a cabo a nivel global, este tipo de actividades aún se perfila como líder en cuanto a infecciones se refiere.

Estas aplicaciones maliciosas tienen como finalidad infectar dispositivos informáticos, cifrando los archivos del usuario y exigiendo el pago de un rescate, que por lo general se cotiza en criptoactivos como Bitcoin y Monero.

Si bien en sus orígenes este tipo de malware afectaba a usuarios comunes, hoy sus objetivos principales son grandes organizaciones o entidades como pueden ser los hospitales u organismos estatales.

2.1.3.2 Crímenes relacionados con abuso sexual infantil

Hoy el anonimato e interconectividad que brinda Internet ha sido aprovechado por delincuentes sexuales, quienes transmiten y comparten material vinculado a abuso sexual infantil.

Dichas actividades suelten utilizar como medios de comunicación servicios de correo electrónico, redes sociales o aplicaciones móviles.

2.1.3.3 Botnets

Existen grandes redes conformadas por equipos informáticos infectados, situación por lo general desconocida por su propietario.

Dichas infraestructuras, obedecen a un centro de comando y control, que ante una orden determinada podría ser capaz de realizar una denegación de servicio a un servidor Web, interrumpiendo su operatividad.

Por lo general, este tipo de servicios puede ser rentado por una cantidad de tiempo o volumen de datos determinados.

2.1.3.4 Fraudes con medios de pago

Aun cuando las medidas de seguridad en torno a los medios de pago se han robustecido durante los últimos años, continúan los ataques contra las tarjetas de crédito y débito.

Un claro ejemplo es la técnica denominada como *skimming*, que logra hacerse de la información almacenada en la banda magnética de las tarjetas, permitiendo su posterior clonación.

Por otro lado, técnicas mas avanzadas como el *jackpotting* han logrado vulnerar los sistemas instalados en los cajeros automáticos mediante técnicas de malware que se aprovechan de diferentes vulnerabilidades, ya sea de hardware como de software.

2.1.3.5 Criptoactivos

La mayoría de actividades cibercriminales perciben sus ingresos en criptoactivos o las también mal denominadas monedas digitales.

Su principal ventaja consiste en el anonimato, dado que si bien las transacciones son públicas y auditables, estas no se encuentran vinculadas a una persona física.

2.1.3.6 Ingeniería Social

Consiste en manipular a una persona o grupo de personas para obtener un resultado determinado.

Esta técnica es empleada habitualmente para efectuar fraudes como por ejemplo *phishing* o comprometer un e-mail corporativo, a fin de impersonar a sus legítimos usuarios y autorizar o solicitar operatorias bancarias fraudulentas.

2.1.3.7 Cryptojacking

Debido al incremento de costo computacional requerido para la minería de criptoactivos, los ciberdelincuentes han optado por esta novedosa técnica, mediante la que se busca tomar control todo tipo de dispositivos, desde computadoras de escritorio y equipos portátiles hasta teléfonos inteligentes e incluso servidores web, a fin de utilizar dicho poder de procesamiento.

Esta amenaza emergente, tiene como capacidad permanecer oculto de forma casi imperceptible, salvo por aquellos casos donde el equipo comprometido ve disminuido significativamente su rendimiento.

2.1.3.8 Mayor cantidad de usuarios en la *Darknet*

Dado que la complejidad para acceder a esta porción de Internet ha disminuido, la cantidad de personas que visitan la *Darknet* se ha visto incrementada.

Si bien muchos de sus usuarios se conectan por curiosidad, otro tanto lo hacen para enmascarar actividades ilegales.

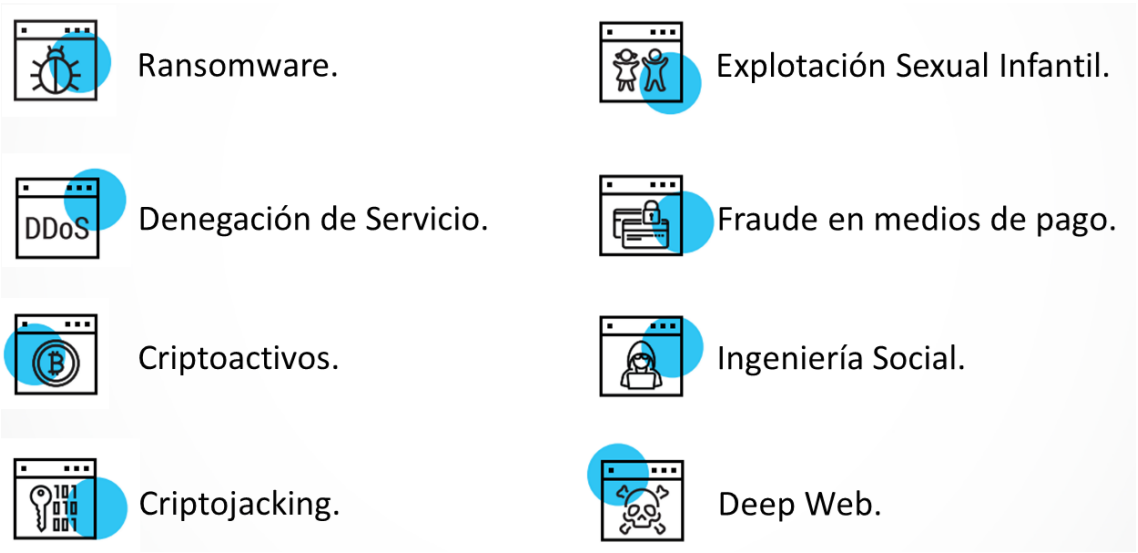

Ilustración 2: Principales amenazas en materia de cibercrimen.

2.1.4 Aspectos legales en nuestro país

A fin de brindar un panorama sobre el marco legal vigente en nuestro país al momento de haberse realizado el presente trabajo, se describirán sucintamente aquellas normas consideradas de interés y que guardan relación con la temática propuesta.

2.1.4.1 Contexto general

En un principio, dentro de la normativa penal de nuestro país no se encontraban contemplados aquellos delitos relacionados con el uso de las nuevas tecnologías de la comunicación e información.

Sin embargo, a fin de suplir este vacío legal, surgieron ciertas figuras penales que relacionaban esta temática con ciertas leyes especiales.

- Ley 11723 de Propiedad Intelectual, contempla aquellos delitos relacionados con los derechos de autor [21].
- Ley 22362 de Registros Marcarios, ampara los delitos que atentan contra las designaciones marcarias [22].

- Ley 25326 de Protección de Datos Personales, cuyo bien jurídico tutelado es la intimidad y privacidad de información sensible [24].
- Ley 24766 de Confidencialidad, que ampara la sustracción de secretos comerciales contenidos en medios informáticos [25].
- Ley Penal Tributaria 24769, que contempla la alteración dolosa de registros [26].
- Ley Antidiscriminatoria 23592, norma los delitos relacionados con conductas xenofóbicas [27].

2.1.4.2 Ley 26388 [19]

A fin de distinguir aquellas actividades criminales relacionadas con el uso de la tecnología de la información y propósito de lo anterior, en el año 2008 fue sancionada la ley 26388, conocida localmente como la ley de delitos informáticos, la cual tipifica e incorpora al Código Penal diferentes conductas delictivas vinculadas a esta temática.

- Daños informáticos.
- Fraudes informáticos.
- Alteración de pruebas.
- Pornografía infantil.
- Delitos contra la privacidad.
- Delitos contra la seguridad pública e interrupción de las comunicaciones
- Falsificación de documentos electrónicos.

2.1.4.3 Ley 26904 [20]

A fin de incorporar el acoso por medios electrónicos al Código Penal, en el año 2013 fue sancionada la ley 26904, conocida localmente como la ley de ciberacoso, la cual tipifica e incorpora conductas delictivas contra la integridad sexual de los menores por medio de:

- Comunicaciones electrónicas.
- Telecomunicaciones.
- Cualquier otra tecnología de transmisión de datos.

2.1.4.4 Normativa complementaria

- Resolución Nro 580/2011 de La Jefatura de Gabinete de Ministros, crea el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad en el ámbito de la Oficina Nacional de Tecnologías de Información (ONTI) [28].
- Disposición Nro 3/2011 de La Oficina Nacional de Tecnologías De Información (ONTI), establece el "Formulario de adhesión al Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad" [29].
- Disposición Nro 2/2013 de la Oficina Nacional de Tecnologías de Información (ONTI), crea el grupo de trabajo "ICIC – CERT" (Computer Emergency Response Team) en el marco del "Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad" [30].
- Decreto Nro 1067/2015, establece que en el Organigrama de la Administración Pública Nacional se instituye a la Subsecretaría de Protección de Infraestructuras Críticas de Información y Cibserseguridad en el ámbito de la Secretaría de Gabinete de la Jefatura de Gabinete de Ministros [31].
- Disposición Nro 5/2015 de la Jefatura de Gabinete, crea en la Subsecretaría de Protección de Infraestructuras Críticas de Información y Ciberseguridad el "Registro de Equipos de Respuesta ante Incidentes de Seguridad Informática" [32].
- Resolución Nro 1046/2015 de la Jefatura de Gabinete de Ministros, establece la estructura organizativa de la Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad [33].

- Resolución Nro 1252/2015 de la Jefatura de Gabinete de Ministros, conforma el Comité de Seguridad de la Información de la Jefatura de Gabinete de Ministros y deroga la Resolución 970/2014 de la JGM [34].
- Resolución PGN Nro 2035/14 de la Procuración General de la Nación, designa al "punto focal" de la Procuración General de la Nación en materia de ciberdelincuencia [35].
- Resolución PGN Nro 3743/15 de la Procuración General de la Nación, crea la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) [36].
- Ley Nro 27.126, establece dentro de las funciones de la Agencia Federal de Inteligencia (AFI) la producción de inteligencia criminal referida a los delitos federales complejos relativos a ciberdelitos [37].
- Resolución PGN Nro 756/16 de la Procuración General de la Nación, brinda una serie de recomendaciones para analizar y preservar evidencia digital [10].
- Resolución Nro 234/16 del Ministerio de Seguridad de la Nación, establece un Protocolo General de Actuación para las Fuerzas Policiales y de Seguridad en la investigación y proceso de recolección de pruebas en Ciberdelitos [11].
- Decisión Administrativa Nro 564/2018 de la Jefatura de Gabinete de Ministros, establece la Dirección de Investigaciones del Ciberdelito en el ámbito de la Dirección Nacional de Investigaciones [38].

2.1.5 El convenio de Budapest

El 22 de noviembre de 2017 nuestro poder legislativo aprobó la Ley 27411 sobre la adhesión de Argentina al Convenio de Budapest [39], un convenio internacional sobre ciberdelito.

El Convenio de Budapest tiene como principal objetivo estandarizar aquellas definiciones relacionadas con los delitos informáticos y fundar bases sólidas que permitan fomentar la cooperación internacional en cuestiones de ciberseguridad.

Por intermedio de esta adhesión, la Justicia argentina cuenta con nuevas herramientas para investigar este tipo de problemática, como pueden ser las estafas electrónicas, la pornografía infantil y otras temáticas vinculadas a la propiedad intelectual.

El Convenio de Budapest o de Cibercriminalidad, data de noviembre del año 2001 y fue concebido en la ciudad que le otorga su nombre en el seno del Consejo de Europa.

Si bien este tratado fue creado en el ámbito de una institución europea, permite la adhesión de otros estados, como lo es el caso de los 56 países que lo consignaron. Por el lado de Latinoamérica, además de Argentina ya son parte Chile, Costa Rica, República Dominicana y Panamá.

El convenio entró en vigencia oficialmente en el año 2004, constituyendo en la actualidad el único documento de carácter internacional que trata específicamente el tema del cibercrimen, mediante sus 48 artículos divididos en 4 capítulos.

2.1.5.1 Primer capítulo:

Se refiere a terminología mediante diferentes definiciones.

- Sistemas informáticos, comprende todo tipo de dispositivos, ya sean de forma individual o interconectados, que procesan datos automáticamente mediante la ejecución de un programa informático.
- Datos informáticos, toda representación vinculada al procesamiento informático, inclusive aquellos programas que permiten la ejecución de los sistemas.
- Proveedor de servicio, toda aquella entidad, ya sea pública o privada, que comunica a los usuarios mediante un sistema informático. También incluye otras entidades que procesan o almacenan datos informáticos vinculados a los usuarios y/o servicios de comunicación.

- Datos de tráfico, son aquellos relacionados a la comunicación por intermedio de sistemas informáticos y producidos por estos, que indican el origen, destino, hora y fecha u otra información existente.

2.1.5.2 Segundo capítulo

Establece aquellas medidas que los estados parte deben adoptar en relación a los Ciberdelitos, teniendo como precepto la necesidad de criminalizar determinadas conductas establece las figuras de acceso ilícito a sistemas informáticos, fraude informático, abuso de dispositivos, interceptación ilícita de datos, pornografía infantil y propiedad intelectual.

Del mismo modo, señala medidas relacionadas con el procedimiento de investigación, como por ejemplo conservación de datos, identificación y secuestro de dispositivos, obtención de datos de tráfico e incluso interceptación de contenido.

2.1.5.3 Tercer capítulo

Se encuentra labrado en el marco de la cooperación internacional, tiene en cuenta aspectos fundamentales, tales como la asistencia mutua, conservación de medios de prueba, obtención de datos de tráfico e interceptación de contenido.

2.1.5.4 Cuarto capítulo

Menciona cuestiones administrativas, como por ejemplo fecha de entrada en vigencia, forma en que otros estados pueden adherirse y reservas permitidas.

2.2 Marco Teórico Referencial

En esta sección se brindarán los conceptos que se consideran primordiales para la comprensión del desarrollo del presente trabajo.

2.2.1 La Evidencia Digital

Resulta difícil enunciar una definición universal, sin embargo se puede señalar que la evidencia digital es un tipo de evidencia física construida de campos magnéticos y pulsos electrónicos, que por sus características deben ser recolectados y analizados con herramientas y técnicas especiales [40].

Cabe destacar que el término evidencia digital es una denominación empleada de manera extensa, describiendo de esta manera cualquier registro generado o almacenado en un sistema computacional o dispositivo informático, cuya clasificación puede realizarse según sus características, naturaleza, orden de volatilidad y admisibilidad:

2.2.1.1 Características

La evidencia digital es la materia prima para los investigadores forenses donde la tecnología informática es parte fundamental del proceso. Sin embargo y considerando el ambiente tan cambiante y dinámico de las infraestructuras de computación y telecomunicaciones, es preciso detallar las características propias de dicha evidencia en este entorno [41].

Acorde a lo expuesto precedentemente, podría decirse que la evidencia digital es un constante desafío para los investigadores forenses, destacándose por su:

- Volatilidad: periodo de disponibilidad que posee en función del tiempo.
- Anonimato: capacidad de ocultar la identidad de quién generó el registro.
- Capacidad de duplicación: posibilidad de realizar copias idénticas.
- Posibilidad de alteración y modificación: capacidad de ser manipulada.
- Alta probabilidad de eliminación: fácil acceso y carencia de permisos.

2.2.1.2 Según su naturaleza

Conforme lo define el Manual de Estándares de Australia[6] HB: 171/2003 "Directrices para la Gestión Evidencia de Tecnología Informática" [3], la evidencia digital puede subdividirse en tres categorías:

- Registros almacenados en el equipo de tecnología informática (por ejemplo, correos electrónicos, archivos de aplicaciones de ofimática, imágenes, etc.).
- Registros generados por los equipos de tecnología informática (registros de auditoría, registros de transacciones, registros de eventos, etc.).
- Registros que parcialmente han sido generados y almacenados en los equipos de tecnología informática (hojas de cálculo, consultas en bases de datos, vistas parciales de datos, etc.).

Nótese que la presente clasificación engloba a la evidencia digital en su totalidad, debiendo prestar especial atención en el factor humano, dado que resulta determinante identificar si fue una persona o un dispositivo informático quien creó el contenido del registro o archivo.

2.2.1.3 Conforme el orden de volatilidad

La RFC 3227/2002 "Guía Para Recolectar y Archivar Evidencia" [2] de *Internet Society*[7], establece el siguiente orden de volatilidad y por tanto de recopilación de evidencias:

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

[6] Documento elaborado por la Organización de estándares de Australia, creada con el fin de asistir a las organizaciones para combatir el crimen electrónico.
[7] Sociedad de Internet, organización no gubernamental y sin fines de lucro, con dedicación exclusiva sobre el desarrollo mundial de Internet.

- Contenido de otros dispositivos de almacenamiento.

En tal sentido, resulta pertinente hacer notar que primeros cuatro apéndices representan datos de carácter volátil, es decir que se perderán o modificarán si apaga o reinicia el sistema, resultando es por tanto muy fácil eliminar evidencias de forma inadvertida.

Por el contrario los dos últimos apéndices, hacen referencia a medios de almacenamiento (discos rígidos, discos de estado sólido, soportes ópticos, etc), cuya información perdura en el tiempo bajo condiciones normales de uso y una adecuada cadena de custodia.

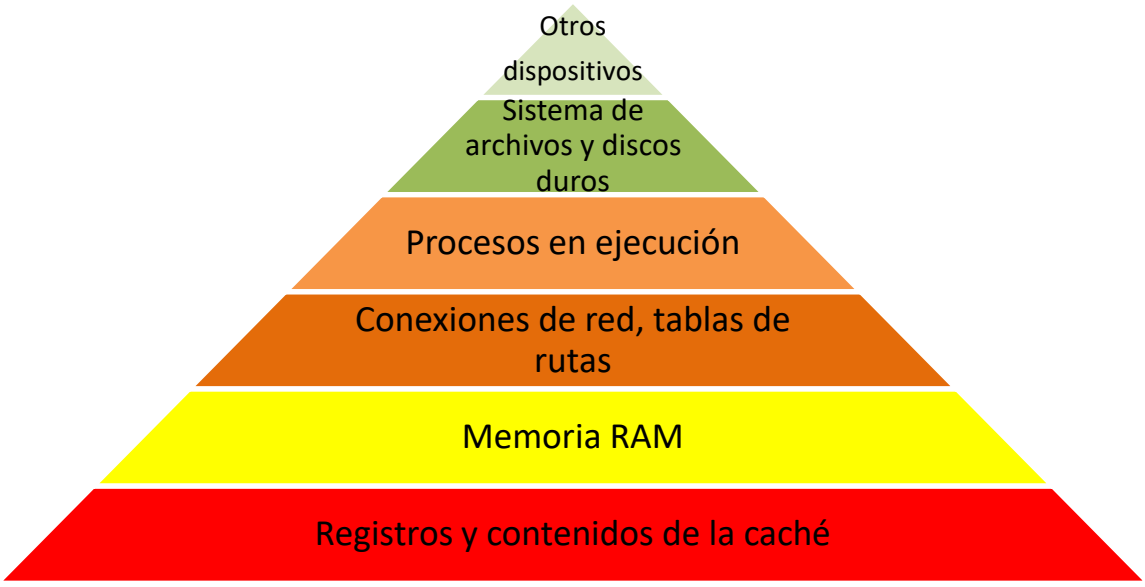

Ilustración 3: Orden de volatilidad de la Evidencia Digital.

2.2.1.4 Criterios de admisibilidad

En legislaciones modernas, existen ciertos criterios que se deben tener en cuenta [41]. Los mismos son:

- Admisibilidad: debe tener valor legal.
- Autenticidad: debe ser verídica y no haber sufrido manipulación alguna. A tal fin, se calculan firmas digitales que garantizan su integridad.

- Completitud: la prueba debe ser presentada desde un punto de vista objetivo y técnico, sin valoraciones personales o prejuicios.
- Credibilidad: debe ser creíble y de fácil comprensión.
- Confiabilidad: las técnicas utilizadas para su obtención no deben generar duda sobre su veracidad y autenticidad.

2.2.2 La Informática Forense [14]

Según el Departamento Federal de Investigaciones de los Estados Unidos, la Informática Forense es considerada una rama de las ciencias forenses, que tiene como finalidad identificar, preservar, analizar y presentar datos que han sido procesados electrónicamente, y almacenados en un medio digital.

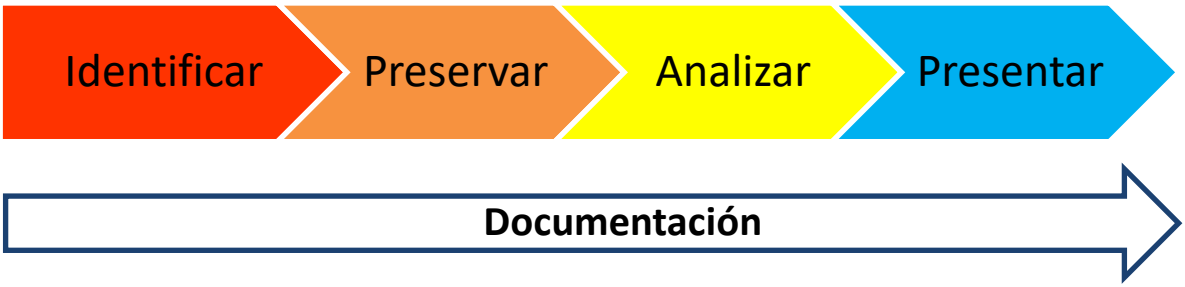

Ilustración 4: Fases del análisis forense digital.

Conforme la definición planteada, se pueden observar cuatro etapas discriminadas taxativamente como:

2.2.2.1 Identificación

Constituye el primer acercamiento a los medios de prueba digitales, implica procesos tendientes a su individualización unívoca (marca, modelo, tipo de dispositivo, etc), a fin de dilucidar posteriormente interrogantes como por ejemplo qué cosas pueden ser evidencias y cuáles no, dónde y cómo están almacenados los registros, etc.

Brinda un punto de partida que permite al investigador establecer las metodologías de adquisición y recuperación de evidencias adecuadas, así como las herramientas forenses a utilizar en los pasos subsiguientes, tanto de hardware como de software.

2.2.2.2 Preservación

Tiene como finalidad salvaguardar la integridad y autenticidad de las evidencias digitales relevadas, garantizando la seguridad de la cadena de custodia. Cualquier cambio en la evidencia deberá ser documentado.

En tal sentido, se aplican DOS (2) Algoritmos HASH distintos: MD5 y SHA1. El cálculo de los mismos garantiza, en todo momento, la integridad y autenticidad de las evidencias digitales recolectadas. Es dable de mencionar, que se calculan DOS (2) algoritmos de manera simultánea, ya que de esa manera se garantiza que los mismos, de manera conjunta, resultan ser otra forma de identificar *UNÍVOCAMENTE* a tales registros.

Sin perjuicio de lo expresado, si bien los algoritmos de seguridad MD5 y SHA1 son empleados con mayor frecuencia, no solo por los investigadores forenses de todo el mundo sino también provistos por defecto mediante distintas herramientas, resulta oportuno destacar que los mismos pueden presentar colisiones[8], por cuanto existen otros formatos de mayor complejidad como por ejemplo SHA2, algoritmo de reducción criptográfico de 256 bits cuya longitud es de 64 caracteres.

2.2.2.3 Análisis

Consiste en el conjunto de técnicas y procedimientos empleados a fin de inspeccionar y examinar los datos contenidos en los medios de prueba remitidos para estudio, conforme la requisitoria pericial planteada.

Debe contener un detalle de las herramientas informáticas empleadas, así como las operaciones realizadas y resultados obtenidos. La identificación de hallazgos

8 Situación que se produce cuando se aplica una misma función hash sobre dos entradas diferentes y se produce el mismo resultado.

o recopilación de evidencia notable puede resultar complicada, puesto que no se debe dañar ninguna de sus características; teniendo en cuenta que es susceptible a variaciones y tendencia a perderse si no se trata adecuadamente.

2.2.2.4 Presentación

Consiste en el proceso de elaborar un reporte a fin de presentar la evidencia relevada en un formato legalmente aceptable y comprensible, incluso por quien no posea experiencia computacional, caso contrario el esfuerzo impreso en el trabajo no tendrá sentido.

Al mismo tiempo, se adjuntan las evidencias recolectadas mediante dispositivos de almacenamiento, permitiendo disponer en todo momento de un respaldo de los archivos que resultan de interés para la investigación.

2.2.3 Normas y estándares vinculados a la Informática Forense

En primer lugar, es importante destacar que no existe un procedimiento estándar empleado para el análisis forense digital. Sin embargo, un gran número de instituciones y organismos han creado diferentes directrices consideradas guías o reglas de buena práctica que abordan la temática desde diferentes enfoques, con el objetivo gestionar e identificar la evidencia digital para ser empleada dentro de una investigación.

Estas reglas se basan en el método científico para concluir o deducir algo acerca de la información, presentando una serie de etapas para recolectar la mayor cantidad de evidencia digital y permitir incluso la posterior reconstrucción de determinados eventos o incidentes informáticos.

Por tal motivo y a fin de realizar el presente trabajo, conforme los criterios de selección señalados con antelación, se procederá a listar aquella documentación incorporada, en tenor de su alcance y estrecha vinculación con el análisis forense digital, brindándose además una somera descripción de su contenido, que luego será

ponderado en función de una serie de parámetros delimitados cualitativamente al momento de realizar la comparación respectiva.

2.2.3.1 Guía Para Recolectar y Archivar Evidencia (RFC 3227/2002)

Esta guía fue elaborada en el año 2002 por *Internet Society*, la cual provee reglas de buena práctica para determinar la volatilidad de la evidencia digital, decidir qué y cómo recolectarla, y determinar su almacenamiento y documentación. Dentro de estructura se aprecian:

- Introducción.
- Principios de recolección de evidencia digital.
- El proceso de recolección.
- El proceso de archivo.
- Herramientas necesarias.

2.2.3.2 Directrices para la Gestión Evidencia de Tecnología Informática (SAI HB 171/2003) [3]

El documento fue confeccionado por *Standards Australia International*[9], con el fin de asistir a las organizaciones para combatir el crimen electrónico, estableciendo puntos de referencia para la preservación y la recolección de la evidencia digital. Detalla el ciclo de administración de evidencia de la siguiente forma:

- Diseño de la evidencia.
- Producción de la evidencia.
- Recolección de la evidencia.
- Análisis de la evidencia.

[9] Estándares Internacionales de Australia, es un organismo que tiene como finalidad el desarrollo y aplicación de estándares técnicos y productos y servicios relacionados.

- Reporte y presentación.
- Determinación de la relevancia de la evidencia.

2.2.3.3 Guía para integrar técnicas forenses en respuesta a incidentes (NIST 800-86-2006) [4]

Esta guía pertenece al *National Institute of Standards and Technology*[10], la misma establece normas y directrices, incluyendo requisitos mínimos para proporcionar una adecuada seguridad de la información en las operaciones y activos de una organización. Posee la siguiente disposición:

- Introducción.
- Establecer y organizar las capacidades forenses.
- Realizar el proceso forense.
- Recolectar datos de archivos de datos.
- Usar datos de sistemas operativos.
- Recabar datos del tráfico de red.
- Emplear datos de aplicaciones.
- Utilizar datos de múltiples fuentes.
- Anexos (recomendaciones, escenarios, glosario, acrónimos, recursos de impresión, herramientas y recursos en línea).

[10] Instituto Nacional de Estándares y Tecnología, agencia de la Administración de Tecnología del Departamento de Comercio de Estados Unidos que promueve la innovación y competitividad industrial mediante el avance de la ciencia, los estándares y la tecnología.

2.2.3.4 Investigación en la Escena del Crimen Electrónico: una guía para primeros intervinientes (US DoJ NCJ 219941 /2008) [5]

Esta guía fue concebida en el seno del *United States Department of Justice*[11], centra su enfoque en la identificación y recolección de evidencia. Contempla los siguientes aspectos:

- Tipos de dispositivos electrónicos.
- Herramientas y equipamiento forense.
- Reglas de preservación y evaluación de la escena del hecho.
- Pasos para documentación de la escena.
- Procedimientos para recolección de evidencia.
- Elementos para preservación de la evidencia.
- El análisis forense y clasificación de delitos.
- Anexos (glosario, recursos legales, técnicos y de capacitación).

2.2.3.5 Computación Forense - Parte 2: mejores prácticas (ISFS/2009) [6]

Esta guía de buenas prácticas fue redactada por *Information Security and Forensic Society*[12], contemplando procedimientos y requerimientos involucrados en el análisis forense de la evidencia digital, desde el examen de la escena del delito hasta la presentación de los correspondientes reportes. Su estructura se encuentra conformada por:

- Introducción a la computación forense.
- Calidad en la computación forense.

[11] Departamento de Justicia de los Estados Unidos, Ministerio del gobierno de Estados Unidos, encargado de la administración de la justicia.

[12] Sociedad de Seguridad de la Información y Computación Forense, organismo de Hong Kong cuya misión es abogar y hacer cumplir el profesionalismo, integridad e innovación en tal materia.

- Evidencia digital.
- Recolección de evidencia.
- Consideraciones legales.
- Anexos.

2.2.3.6 Guía de Buenas Prácticas para evidencia basada en computadoras (ACPO/2012) [7]

Este documento fue elaborado por *Asociation of Chief Police Officers*[13], tiene por finalidad ser empleado como guía de buenas prácticas para casos con equipos de computación y diferentes dispositivos electrónicos que puedan ser considerados como evidencia. Enumera los siguientes aspectos:

- Principios de la evidencia digital.
- Agentes de la ley en la escena del delito.
- Agentes de la ley investigadores.
- Expertos en recuperación de la evidencia digital.
- Testigos.
- Anexos (casos de estudio, recursos técnicos y de capacitación).

2.2.3.7 Evidencia Electrónica - Una guía básica para primeros intervinientes (ENISA/2014) [8]

La guía se redactó por European Network and Information Security Agency[14], la misma provee principios de calidad para la detección, la prevención, la recuperación

[13] Asociación de Jefes de Policía de Inglaterra, Gales e Irlanda del Norte, es una sociedad limitada sin fines de lucro que lidera el desarrollo de prácticas policiales en diferentes temáticas.

[14] Agencia Europea de Seguridad de las Redes y de la Información, agencia de la Unión Europea que tiene como finalidad contribuir al desarrollo de una cultura de red y seguridad de la información para el beneficio de los ciudadanos, consumidores, empresas y organizaciones de la región.

y el análisis de la evidencia digital. Contempla los sistemas, los procedimientos, el personal, el equipo y los requerimientos necesarios desde la escena del delito hasta su presentación. Su esquema abarca:

- Objetivos.
- Alcance.
- Fondo.
- Introducción.
- Reunión de evidencia electrónica.
- Principios de recopilación de evidencia electrónica.
- Antes de llegar a la escena del crimen.
- Juego de herramientas para los primeros intervinientes.
- Computadora portátil forense del primer interviniente.
- Herramientas y comandos del primer interviniente.
- Al llegar a la escena.
- Implementación.
- Memoria forense.
- Examen de pruebas.
- Extracción.
- Análisis.
- Evaluación y presentación de la evidencia.
- Observaciones finales.
- Anexos.

2.2.3.8 Principios para identificación, recolección, adquisición y preservación de pruebas digitales (ISO/IEC 27037/2016) [9]

Esta guía fue elaborada por el *International Standarization Organization*[15] e *International Electronic Comission*[16], proporcionando pautas para actividades específicas en el manejo de evidencia digital potencial. Estos procesos son: identificación, recopilación, adquisición y preservación de la evidencia digital. Contempla los siguientes apartados:

- Introducción.
- Alcance.
- Referencia normativa.
- Términos y definiciones.
- Términos abreviados.
- Visión de conjunto.
- Componentes clave de identificación, recopilación, adquisición y preservación de evidencia digital.
- Instancias de identificación, colección, adquisición y preservación.
- Anexos (descripción de competencias básicas del primer interviniente y requisitos mínimos de documentación).

[15] Organización Internacional de Normalización, organización con sede en Suiza que tiene como finalidad crear y promover estándares propietarios, industriales y comerciales a nivel mundial.

[16] Comisión Electrotécnica Internacional, organización de normalización en los campos eléctrico, electrónico y tecnologías relacionadas en Estados Unidos.

2.2.3.9 Guía de obtención, preservación y tratamiento de evidencia digital (PGN 756/2016) [10]

En virtud de las actividades desarrolladas por la Unidad Fiscal Especializada en Ciberdelincuencia[17], se elaboró un documento señalando una serie de herramientas de investigación como forma de reforzar las actividades del Ministerio Público Fiscal en aquellos casos donde se deba tratar con evidencia digital. El mismo tiene como finalidad establecer aquellos principios que permitirán llevar a cabo investigaciones y recolección de pruebas electrónicas en materia de ciberdelitos, contemplando diferentes aspectos.

- Introducción.
- La evidencia digital.
- Principios de tratamiento de la evidencia digital
- Recolección y preservación de evidencia digital.
- Presupuestos Generales.
- Principios especiales.
- Embalaje, traslado y resguardo de la evidencia digital.
- Manipulación idónea del hardware.
- Imagen o copia forense y uso de hash.
- Aspectos a tener en cuenta al momento de analizar la evidencia digital recolectada en función de los delitos a investigar en los que el medio digital puede ser relevante.

[17] Fiscalía especializada en materia de ciberdelincuencia, que tiene como finalidad la lucha contra el cibercrimen de manera articulada con otras áreas de la Procuración General de la Nación que se dedican a la investigación del crimen organizado.

2.2.3.10 Protocolo General de Actuación para las Fuerzas Policiales y de Seguridad en la investigación y proceso de recolección de pruebas en Ciberdelitos (MINSEG RES 234/2016) [11].

Debido a que las cifras de los ciberdelitos se incrementan exponencialmente con el correr de los años, el estado nacional ha propiciado la creación de Unidades Especiales de Investigación en aquellas Fuerzas de la ley dependientes del Ministerio de Seguridad, cuya actuación se encuentra normada mediante la Resolución 234/2016 "Protocolo General de Actuación para las Fuerzas Policiales y de Seguridad en la Investigación y Proceso de Recolección de Pruebas en Ciberdelitos".

Dicho protocolo de actuaciones tiene como finalidad establecer los principios para llevar a cabo investigaciones y recolección de pruebas electrónicas en materia de ciberdelitos, contemplando diferentes aspectos.

- Reglas generales, definiciones y principios.
- Principios generales de intervención.
- Principios específicos de intervención.
- Pautas específicas de actuación.
- Capacitaciones.

3
Resultados

Resulta menester destacar que a la hora de iniciar el análisis forense digital, el perito informático se encontrará con diferentes tecnologías, diversos sistemas operativos, métodos de almacenamiento o sistemas de archivo, tecnologías o procesos intrínsecos que naturalmente eliminan evidencias, mecanismos propietarios de protección de la información, carencia de herramientas específicas o que bien que cubren de forma parcial las necesidades operativas, diferentes sistemas de criptografía o enmascaramiento de la información.

Dados los pormenores de la complejidad del escenario planteado y los múltiples obstáculos que se deben sortear durante el desarrollo del análisis forense, se desprende la imperiosa necesidad de contar con profesionales altamente calificados desde lo técnico, en consonancia con sólidos lineamientos como las reglas de buena práctica forense, garantizando en todo momento un proceso reproducible de identificación, preservación, análisis y presentación de la evidencia digital, para afianzar su valor probatorio.

Por tal motivo, en el presente capítulo se expondrán los resultados obtenidos a partir del análisis practicado sobre la documentación seleccionada, en función de las fases que componen el análisis forense digital y otros aspectos de relevancia, para luego determinar si resulta factible la implementación de un Sistema de Gestión de Evidencia Digital.

A tal efecto, se realizará un abordaje que permitirá discernir una metodología de trabajo con una visión estratégica e integral, tomando como principios fundacionales aspectos relevantes identificados durante el análisis de la documentación seleccionada.

3.1 Confronte de normas y estándares forenses

Por medio del análisis de reglas de buena práctica, instructivos, procedimientos operativos, manuales, guías, normas y estándares existentes en materia de informática forense y evidencia digital, se procedió a someter la documentación seleccionada bajo un mismo plano de comparación respecto de las fases que conforman el análisis forense digital, definidas previamente como identificación, preservación, análisis y presentación de las evidencias recolectadas.

Sin perjuicio de lo expresado, en función del estudio practicado, resultó factible identificar diferentes etapas complementarias, una al inicio que denominaremos de preparación, donde se enuncian actividades preliminares para responder ante el incidente o requerimiento planteado, y otra al finalizar que a fines del presente trabajo será denominada evaluación de hallazgos.

Del mismo modo, a medida que los procedimientos ejecutados avanzan entre una fase y otra del análisis forense digital, el riesgo decrece, dado que se reduce la posibilidad de alteración, modificación, daño o pérdida de evidencia digital, todo ello en virtud de las múltiples medidas preventivas que deben ser adoptadas para su correcta preservación y resguardo, garantizando además la integridad de tales elementos de prueba en todo momento.

Por tal motivo y conforme lo expresado hasta el momento, a los efectos de una mejor interpretación, se procede a graficar los resultados obtenidos mediante diferentes tablas comparativas en función de actividades específicas.

3.1.1 Etapa preparativa

Es aquella etapa complementaria donde se enuncian actividades preliminares para responder ante el incidente o requerimiento planteado, que tiene como finalidad planificar y organizar el proceso de investigación digital.

	ETAPA PREPARATIVA				
	Recepción del requerimiento	Revisión de capacidades	Definición del alcance	Equipamiento básico[18]	Planificación y diseño
RFC 3227/2002			●		●
SAI HB 171/2003		●	●		●
NIST 800-86-2006		●	●	●	●
US DoJ NCJ 219941/2008			●	●	●
ISFS/2009		●	●	●	●
ACPO/2012			●		●
ENISA/2014			●	●	
ISO/IEC 27037/2016	●	●	●		●
PGN 756/2016			●	●	●
MINSEG RES 234/2016			●		●

Tabla 1: Etapa preparativa.

[18] El listado de equipamiento básico se encuentra detallado en el Anexo "Equipamiento básico" del presente Trabajo Final de Especialización.

3.1.2 Etapa de identificación

Es el primer acercamiento a los medios de prueba digitales, permitiendo al investigador su individualización unívoca y prever metodologías adecuadas para su adquisición, recuperación y preservación.

	ETAPA DE IDENTIFICACIÓN				
	Tipos de infraestructura	Tipos de dispositivos	Categorización de posibles evidencias	Otras evidencias físicas	Requisitos previos a la adquisición
RFC 3227/2002		●	●		
SAI HB 171/2003	●	●			
NIST 800-86-2006	●	●	●		●
US DoJ NCJ 219941/2008	●	●	●		●
ISFS/2009	●	●	●	●	●
ACPO/2012	●	●			●
ENISA/2014	●	●	●		
ISO/IEC 27037/2016	●	●	●	●	●
PGN 756/2016		●	●		●
MINSEG RES 234/2016		●		●	●

Tabla 2: Etapa de identificación.

3.1.3 Etapa de preservación

Tiene como finalidad salvaguardar la integridad y autenticidad de las evidencias digitales identificadas, mediante la cadena de custodia correspondiente.

	ETAPA DE PRESERVACIÓN[19]				
	Orden de volatilidad	Tipos Evidencia (Física/Lógica)	Algoritmos de seguridad	Consideraciones legales	Cadena de custodia[20]
RFC 3227/2002	●	●		●	●
SAI HB 171/2003	●	●			●
NIST 800-86-2006	●	●	●	●	●
US DoJ NCJ 219941/2008				●	●
ISFS/2009	●	●	●	●	●
ACPO/2012	●	●		●	
ENISA/2014	●		●	●	●
ISO/IEC 27037/2016	●	●	●	●	●
PGN 756/2016	●	●	●	●	●
MINSEG RES 234/2016			●	●	●

Tabla 3: Etapa de Preservación.

[19] Las consideraciones relacionadas con la obtención de imágenes forenses se plasman en el Anexo "Adquisición de imágenes Forenses" del presente Trabajo Final de Especialización.

[20] Los requisitos mínimos para garantizar la cadena de custodia y trazabilidad de las evidencias recolectadas se plasman en el Anexo "Cadena de custodia" del presente Trabajo Final de Especialización.

3.1.4 Etapa de análisis

Tiene como finalidad establecer la existencia de evidencia notable y documentar dichos hallazgos, conforme la requisitoria pericial planteada.

	ETAPA DE ANÁLISIS[21]				
	Lista de artefactos forenses	Línea de tiempo	Firmas de archivo[22]	Palabras clave	Técnicas y herramientas para procesamiento
RFC 3227/2002					
SAI HB 171/2003					
NIST 800-86-2006	●	●	●	●	●
US DoJ NCJ 219941/2008	●		●		
ISFS/2009	●	●			
ACPO/2012	●			●	
ENISA/2014	●	●	●	●	
ISO/IEC 27037/2016					
PGN 756/2016					●
MINSEG RES 234/2016	●			●	

Tabla 4: Etapa de Análisis.

[21] Una reseña sobre las herramientas forenses de amplio reconocimiento por los investigadores digitales se enumeran en el Anexo “Herramientas Forenses” del presente Trabajo Final de Especialización.

[22] El listado conteniendo aquellas firmas de archivo consideradas como convencionales se enumeran en el Anexo “Firmas de Archivo” del presente Trabajo Final de Especialización.

3.1.5 Etapa de presentación

Involucra aquellas actividades que permiten elaborar un reporte a fin de presentar y remitir los hallazgos relevados.

	ETAPA DE PRESENTACIÓN				
	Reporte de resultados	Remisión de hallazgos	Mecanismos para su preservación	Modelos de trabajo	Recomendaciones
RFC 3227/2002					
SAI HB 171/2003					
NIST 800-86-2006	●				●
US DoJ NCJ 219941/2008					
ISFS/2009	●				●
ACPO/2012	●				●
ENISA/2014	●				●
ISO/IEC 27037/2016					
PGN 756/2016					
MINSEG RES 234/2016					

Tabla 5: Etapa de Presentación.

3.1.6 Etapa de evaluación

Es aquella etapa complementaria que permite evaluar los resultados obtenidos a fin de ponderar la utilidad de los mismos, aportando información que permita la toma de decisiones.

	ETAPA DE EVALUACIÓN				
	Análisis de los resultados obtenidos	Ponderación de los resultados obtenidos	Revisión de metodologías aplicadas	Identificación de interrogantes adicionales	Reformulación del alcance
RFC 3227/2002					
SAI HB 171/2003					
NIST 800-86-2006	●	●			
US DoJ NCJ 219941/2008					
ISFS/2009					
ACPO/2012					
ENISA/2014					
ISO/IEC 27037/2016					
PGN 756/2016					
MINSEG RES 234/2016					

Tabla 6: Etapa de Evaluación.

3.2 Identificación de roles y competencias requeridas

Cabe destacar que a cada etapa del análisis forense le corresponden determinadas tareas y/o actividades específicas, las que deben ser ejecutadas por especialistas, cuyos roles requieren una formación particular y diferentes grados de especificidad.

Valga la redundancia, resulta oportuno enfatizar que tales roles y grado de capacidad técnica hacen al perfil profesional del especialista en informática forense, cualidades que se encuentran relacionadas de forma directamente proporcional con aquellas diligencias que deben materializarse.

Por tal motivo, se identificaron los roles correspondientes al investigador, primer interviniente en manejo de evidencia digital[23] y especialista en análisis de evidencia digital[24], como piezas claves que de forma conjunta interactúan en torno al análisis forense digital, cuya descripción, actividades y competencias requeridas serán desglosadas posteriormente.

Ilustración 5: Roles y responsabilidades.

23 Término que en adelante adoptará el acrónimo "PIED" en el presente Trabajo Final de Especialización.
24 Término que en adelante adoptará el acrónimo "EAED" en el presente Trabajo Final de Especialización.

3.2.1 El investigador

DESCRIPCIÓN
Es aquella persona encargada de planificar y organizar todo el proceso de investigación digital, coordinando diferentes actividades a desarrollarse. Por lo general, este rol puede ser desempeñado por un individuo designado por la organización involucrada o autoridad judicial competente, a fin de velar por el cumplimiento de aquellos objetivos planteados para el desarrollo de la investigación.

ACTIVIDADES
• Solicitar el inicio de la investigación. • Señalar el escenario del incidente. • Aportar detalles sobre los eventos investigados. • Establecer el alcance de la investigación. • Estudiar las conclusiones aportadas. • Ponderar los hallazgos identificados. • Realizar nuevos requerimientos.

COMPETENCIAS REQUERIDAS	EXPERIENCIA	• Usuario general de tecnología de la información. • Conceptos fundamentales básicos de análisis forense. • Alcance y limitaciones de herramientas forenses.
	CONOCIMIENTO	• Trabajo en equipo. • Comunicación. • Resolución de problemas.
	HABILIDAD	• Marco legal y normativo. • Procedimientos de investigación. • Análisis de información.

Tabla 7: El investigador; actividades y competencias requeridas.

3.2.2 El primer interviniente en manejo de evidencia digital

DESCRIPCIÓN
Es aquella persona involucrada en la identificación, recolección y preservación de la evidencia digital en la escena del incidente. Este rol lo desempeñan profesionales que poseen amplia experiencia, habilidad y conocimientos en el manejo de evidencia digital, lo que será crucial para su preservación en virtud de la fragilidad que presenta.

ACTIVIDADES
• Evaluar el escenario del incidente. • Planificar, diseñar y ejecutar sus actividades de forma eficiente. • Identificar aquellos dispositivos y registros digitales de interés para la investigación. • Preservar evidencias digitales según diferentes grados de volatilidad. • Establecer requisitos para recolectar evidencia digital de forma lógica y/o física. • Seleccionar herramientas forenses adecuadas para obtener evidencias digitales. • Evaluar riesgos que pudieran modificar, alterar o eliminar tales indicios. • Documentar los procedimientos implementados. • Velar por la cadena de custodia de los elementos recolectados y remitirlos al laboratorio de análisis forense.

COMPETENCIAS REQUERIDAS	EXPERIENCIA	• Administración de tecnología de la información. • Cadena de custodia. • Marco legal y normativo.
	CONOCIMIENTO	• Identificación de dispositivos y equipos informáticos. • Procedimientos investigativos en la escena del hecho. • Planificación y ejecución de actividades operativas.
	HABILIDAD	• Utilización de herramientas forenses para adquisición. • Optimización de procesos para recolección de evidencia digital. • Preservación de evidencias digitales.

Tabla 8: El primer interviniente; actividades y competencias requeridas.

3.2.3 El especialista en análisis de evidencia digital

DESCRIPCIÓN
Es aquella persona que lleva adelante el análisis y procesamiento de las evidencias digitales recolectadas, para luego elaborar el informe pericial correspondiente. Este rol corresponde a profesionales que poseen experiencia, conocimientos y habilidades con alto grado de especificidad en el análisis de evidencia digital, además pueden ejecutar aquellas actividades correspondientes a los primeros intervinientes.

ACTIVIDADES
• Verificar la integridad de la evidencia digital remitida para análisis. • Realizar copias de respaldo de aquellas evidencias remitidas para análisis y verificar su integridad. • Seleccionar herramientas forenses adecuadas de análisis. • Realizar análisis integral de las evidencias digitales y artefactos forenses. • Clasificar los hallazgos identificados en función de los requerimientos planteados. • Exportar hallazgos identificados, garantizando su disponibilidad e integridad. • Correlacionar hallazgos identificados mediante una línea de tiempo. • Documentar los procedimientos realizados mediante la confección del informe correspondiente. • Velar por la cadena de custodia de los elementos recolectados originalmente, las copias de respaldo obtenidas y hallazgos identificados.

COMPETENCIAS REQUERIDAS	EXPERIENCIA	• Administración avanzada de tecnología de la información. • Confección de reportes de forma clara y concisa. • Aseguramiento de la cadena de custodia.
	CONOCIMIENTO	• Artefactos forenses. • Técnicas antiforenses. • Metodologías de trabajo y reglas de buena práctica.
	HABILIDAD	• Utilización de herramientas forenses para análisis. • Correlación de eventos. • Presentación de reportes.

Tabla 9: El especialista en análisis; actividades y competencias requeridas.

3.3 Metodología general para el análisis forense

Acorde a los resultados obtenidos, resulta factible enunciar la posibilidad de adoptar una metodología general para el análisis forense, independientemente de la magnitud y madurez de la organización donde deba implementarse.

Este procedimiento se encuentra compuesto por atapas consecutivas, cuya ejecución se realiza de forma lineal, teniéndose presente además una posible retroalimentación a raíz de los resultados remitidos mediante informes correspondientes, generando nuevos interrogantes periciales a la luz de aquellos hallazgos identificados.

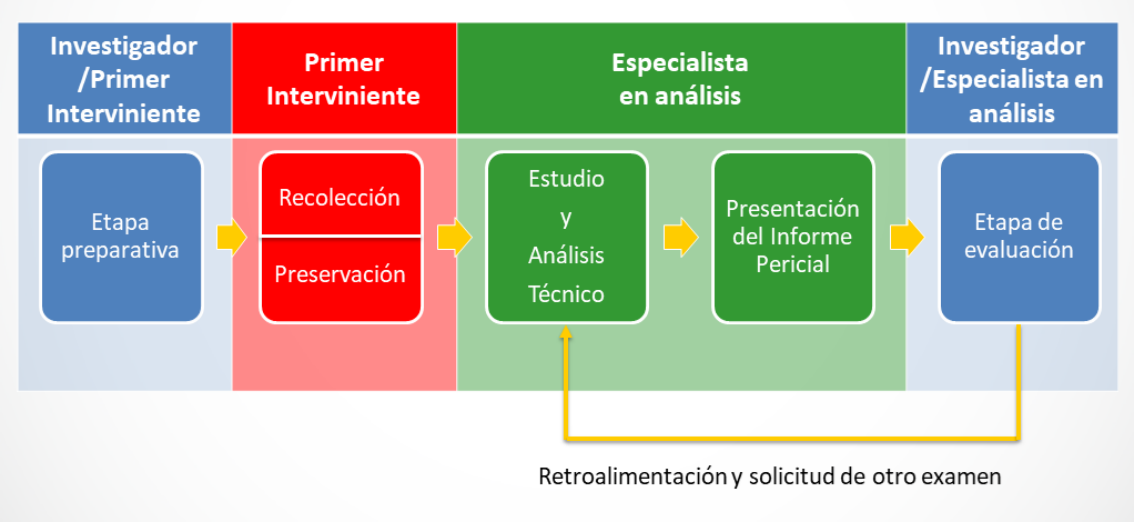

Ilustración 6: Metodología general para el análisis forense.

3.4 Ciclo de vida y categorización de la evidencia digital

Por otro lado, en cuanto al ciclo de vida y categorización de las evidencias digitales, se debe tener presente el tratamiento de este tipo de elementos desde su identificación y preservación en el lugar del hecho hasta su remisión al laboratorio de análisis forense.

En tal sentido, será el primer interviniente quién deberá establecer un procedimiento que le permita recolectar las evidencias digitales en función de los requerimientos planteados, para su posterior análisis por parte del especialista en análisis.

Por tal motivo, la experiencia profesional del primer interviniente resulta crucial a la hora de tomar este tipo de decisiones, dado que en muchos casos aquellas evidencias que no son colectadas en el lugar del hecho muy difícilmente puedan ser adquiridas con posterioridad.

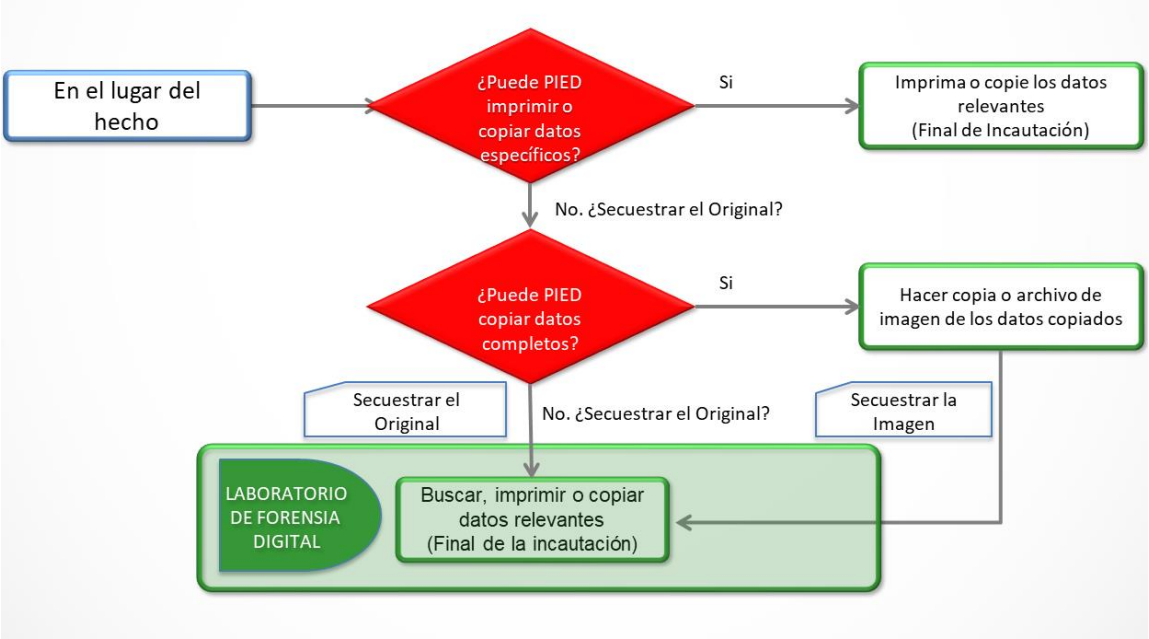

Ilustración 7: Categorización de la evidencia digital.

4

Conclusiones

Acorde a las actividades realizadas durante el desarrollo del presente Trabajo Final de Especialización, basado en la investigación exploratoria y documental sobre reglas de buena práctica, instructivos, procedimientos operativos, manuales, guías, normas y estándares existentes en materia de informática forense y evidencia digital, tanto nacionales y como del extranjero, resultó factible establecer múltiples aristas en común respecto de la temática en cuestión.

Del mismo modo, por medio del presente estudio, se diseñó y elaboró una metodología general de trabajo, sobre la base de cada una de las etapas del análisis forense digital, identificándose tareas y/o actividades propias de cada una de ellas, lo que permite:

- Brindar un marco de referencia integral y estratégico, facilitando su interpretación práctica e implementación en diferentes organizaciones, independientemente de su actividad, envergadura o grado de madurez, garantizando en todo momento el cumplimiento de aquellos principios fundacionales aceptados por la comunidad científica.
- Incrementar la eficacia y eficiencia de los procesos llevados a cabo en los laboratorios forenses digitales, garantizando la calidad de los servicios prestados, en pos de una mejora continua.
- Identificar roles y competencias requeridas, enfatizando la imperiosa necesidad de contar con especialistas en informática forense cuyo perfil profesional posea un alto grado de capacitación y habilidades técnicas específicas, que le permitirán desarrollar de forma acabada sus actividades.

Los resultados del presente trabajo, sientan las bases para tomar como posible línea de investigación, desarrollo e innovación, el diseño y elaboración de un Sistema de Gestión de Evidencia Digital, haciendo foco en procesos operativos como por ejemplo la recolección, adquisición, preservación, análisis, recuperación de información y servicio de asesoría en materia de análisis forense digital.

Asimismo, permitirá prever una serie de recomendaciones vinculadas a infraestructura y requerimientos mínimos que deberán poseer laboratorios forenses de diferentes magnitudes, acorde a factores tales como cantidad de puestos de trabajo, presupuesto, espacio disponible y alcance, entre otros.

5
Bibliografía específica

[1] J. P. BARLOW, *Declaración de Independencia de Internet,* Suiza, 1996.

[2] N. W. Group, «www.ietf.org,» Febrero 2002. [En línea]. Available: https://www.ietf.org/rfc/rfc3227.txt. [Último acceso: 01 Abril 2019].

[3] S. Australia, «https://www.saiglobal.com,» Marzo 2003. [En línea]. Available: https://www.saiglobal.com/PDFTemp/Previews/OSH/as/misc/handbook/HB171.PDF. [Último acceso: 01 Abril 2019].

[4] N. I. o. S. a. Technology, «https://nvlpubs.nist.gov,» Agosto 2006. [En línea]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf. [Último acceso: 01 Abril 2019].

[5] U. D. o. Justice, «https://www.ncjrs.gov,» Abril 2008. [En línea]. Available: https://www.ncjrs.gov/pdffiles1/nij/219941.pdf. [Último acceso: 01 Abril 2019].

[6] I. S. a. F. Society, «http://www.isfs.org.hk,» Agosto 2009. [En línea]. Available: http://www.isfs.org.hk/publications/ISFS_ComputerForensics_part2_20090806.pdf. [Último acceso: 01 Abril 2019].

[7] A. o. C. P. Officers, «http://www.digital-detective.net,» Marzo 2012. [En línea]. Available: http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf. [Último acceso: 01 Abril 2019].

[8] E. U. A. f. N. a. I. S. (ENISA), «https://www.enisa.europa.eu,» 2014. [En línea]. Available: https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders/at_download/fullReport. [Último acceso: 01 Abril 2019].

[9] I. S. Organization, *ISO/IEC 27037/2016 "Guidelines for identification, collection,*

acquisition, and preservation of digital evidence", USA, 2016.

[10] P. G. d. l. Nación, «https://www.fiscales.gob.ar,» Marzo 2016. [En línea]. Available: https://www.fiscales.gob.ar/wp-content/uploads/2016/04/PGN-0756-2016-001.pdf. [Último acceso: 01 Abril 2019].

[11] M. d. S. d. l. Nación, «http://servicios.infoleg.gob.ar,» 07 Junio 2016. [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/260000-264999/262787/norma.htm. [Último acceso: 01 Abril 2019].

[12] C. Gispert, Enciclopedia Autodidactica Interactiva, México: Océano, 2002.

[13] C. N. d. I. C. y. Técnicas, «https://www.conicet.gov.ar,» Abril 2016. [En línea]. Available: https://www.conicet.gov.ar/programas/ciencia-y-justicia/ciencia-forense/. [Último acceso: 01 Abril 2019].

[14] M. G. Noblett, «https://archives.fbi.gov,» Octubre 2000. [En línea]. Available: https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/oct2000/computer.htm. [Último acceso: 01 Abril 2019].

[15] R. C. &. Associates, «https://www.tech4law.co.za/,» 02 Marzo 2015. [En línea]. Available: https://www.tech4law.co.za/tech-advisor/107-digital-forensics/1528-what-is-digital-forensics/. [Último acceso: 01 Abril 2019].

[16] R. Salgado, «https://federalevidence.com,» 02 Febrero 2013. [En línea]. Available: https://federalevidence.com/pdf/2013/02Feb/EE-4thAmSearch-Power%20of%20Hash.pdf. [Último acceso: 01 Abril 2019].

[17] N. I. o. S. a. Technology, «https://csrc.nist.gov,» 01 Agosto 2002. [En línea]. Available: https://csrc.nist.gov/csrc/media/publications/fips/180/2/archive/2002-08-01/documents/fips180-2.pdf. [Último acceso: 01 Abril 2019].

[18] E. E. Torales, Manual de procedimiento para la preservación del lugar del hecho y la escena del crimen, Buenos Aires: Ediciones Infojus, 2014.

[19] S. y. C. d. D. d. l. N. Argentina, «http://servicios.infoleg.gob.ar,» 04 Junio 2008. [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm. [Último acceso: 01 Abril 2019].

[20] S. y. C. d. D. d. l. N. Argentina, «http://servicios.infoleg.gob.ar,» 13 Noviembre 2013. [En línea]. Available:

http://servicios.infoleg.gob.ar/infolegInternet/anexos/220000-224999/223586/norma.htm. [Último acceso: 01 Abril 2019].

[21] S. y. C. d. D. d. l. N. Argentina, «http://servicios.infoleg.gob.ar,» 26 Septiembre 1933. [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/42755/norma.htm. [Último acceso: 01 Abril 2019].

[22] S. y. C. d. D. d. l. N. Argentina, «http://servicios.infoleg.gob.ar,» 26 Diciembre 1980. [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/18803/texact.htm. [Último acceso: 01 Abril 2019].

[23] I. O. C. T. Assessment, «Internet Organised Crime Threat Assessment (IOCTA) 2018,» European Union Agency for Law Enforcement Cooperation 2018, La Haya, 2018.

[24] S. y. C. d. D. d. l. N. Argentina, «http://servicios.infoleg.gob.ar,» 04 Octubre 20. [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm. [Último acceso: 01 Abril 2019].

[25] S. y. C. d. D. d. l. N. Argentina, «http://servicios.infoleg.gob.ar,» 18 Diciembre 1996. [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/41094/norma.htm. [Último acceso: 01 Abril 2019].

[26] S. y. C. d. D. d. l. N. Argentina, «http://servicios.infoleg.gob.ar,» 19 Diciembre 1996. [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/41379/norma.htm. [Último acceso: 01 Abril 2019].

[27] S. y. C. d. D. d. l. N. Argentina, «http://servicios.infoleg.gob.ar,» 03 Agosto 1988. [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/20000-24999/20465/texact.htm. [Último acceso: 01 Abril 2019].

[28] J. D. G. D. MINISTROS, «http://servicios.infoleg.gob.ar,» 28 Julio 2011. [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/185000-189999/185055/norma.htm. [Último acceso: 01 Abril 2019].

[29] J. D. G. D. MINISTROS, «http://servicios.infoleg.gob.ar,» 16 Septiembre 2011. [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/185000-189999/187698/norma.htm. [Último acceso: 01 Abril 2019].

[30] J. D. G. D. MINISTROS, «http://servicios.infoleg.gob.ar,» 08 Agosto 2013. [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/215000-219999/219212/norma.htm. [Último acceso: 01 Abril 2019].

[31] A. P. NACIONAL, «http://servicios.infoleg.gob.ar,» 10 Junio 2015. [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/245000-249999/247971/norma.htm. [Último acceso: 01 Abril 2019].

[32] J. D. G. D. MINISTROS, «http://servicios.infoleg.gob.ar,» 10 Noviembre 2015. [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/255000-259999/255201/norma.htm. [Último acceso: 01 Abril 2019].

[33] J. D. G. D. MINISTROS, «http://servicios.infoleg.gob.ar,» 20 Agosto 2015. [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/250000-254999/251022/norma.htm. [Último acceso: 01 Abril 2019].

[34] J. D. G. D. MINISTROS, «http://servicios.infoleg.gob.ar,» 29 Septiembre 2015. [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/250000-254999/252983/norma.htm. [Último acceso: 01 Abril 2019].

[35] P. G. d. l. Nación, «http://www.mpf.gov.ar,» 09 Septiembre 2014. [En línea]. Available: http://www.mpf.gov.ar/resoluciones/mp/2014/MP-2364-2014-001.pdf. [Último acceso: 01 Abril 2019].

[36] P. G. d. l. Nación, «http://www.mpf.gov.ar,» 18 Noviembre 2015. [En línea]. Available: http://www.mpf.gov.ar/resoluciones/pgn/2015/PGN-3743-2015-001.pdf. [Último acceso: 01 Abril 2019].

[37] S. y. C. d. D. d. l. N. Argentina, «http://servicios.infoleg.gob.ar,» 25 Febrero 2015. [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/240000-244999/243821/norma.htm. [Último acceso: 01 Abril 2019].

[38] J. D. G. D. MINISTROS, «http://servicios.infoleg.gob.ar/,» 17 Abril 2018. [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do;jsessionid=23CCB3ABC553E34C90CE231F2AC0A15A?id=308989. [Último acceso: 01 Abril 2019].

[39] S. y. C. d. D. d. l. N. Argentina, «http://servicios.infoleg.gob.ar,» 15 Diciembre 2017. [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/300000-304999/304798/norma.htm. [Último acceso: 01 Abril 2019].

[40] E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3ra ed., San Diego (CA): Academic Press, 2011.

[41] J. J. C. Martínez, «Admisibilidad de la Evidencia Digital: Algunos Elementos de Revisión y Análisis,» *Revista Electrónica de Derecho Informático,* nº 61, 2003.

[42] N. I. o. S. a. Technology, «https://www.nist.gov,» 09 05 2017. [En línea]. Available: https://www.nist.gov/sites/default/files/documents/2017/05/09/wb-spec-jan-07-1.pdf. [Último acceso: 01 04 2019].

[43] «File Signatures,» [En línea]. Available: https://www.filesignatures.net/. [Último acceso: 01 Abril 2019].

[Página dejada en blanco intencionalmente]

6
Anexos

6.1 Equipamiento básico para el primer interviniente

6.1.1 Elementos para resguardo

El primer interviniente en el manejo de evidencia digital debe contar con un conjunto de herramientas que les permita arribar a la escena y recopilar la mayor cantidad de evidencia disponible, asegurando su integridad para una investigación posterior. Dicho equipamiento básico de herramientas debe incluir, entre otros, los siguientes elementos:

- Cámaras de fotografía y video: para capturar imágenes de la escena y registrar el estado de los elementos electrónicos.
- Un reloj digital: para utilizar como referencia, de modo que las marcas de tiempo sean visibles también como imagen y no solo como metadatos.
- Cajas de cartón o bolsas seguras de evidencia: aptas para recolectar, preservar la evidencia y su posterior transporte al laboratorio.
- Registros de inventario de evidencia, cinta de evidencia, bolsas, rótulos o etiquetas: crucial para garantizar la integridad y continuidad de la evidencia encontrada en la escena.
- Guantes: para protegerse contra los contaminantes presentes en la escena.
- Bolsas y equipos antiestáticos y kit de herramientas no magnéticas: para permitir la recolección segura de evidencia, protegiendo su integridad.

6.1.2 Equipamiento específico

Del mismo modo, en aquellos casos donde la adquisición de evidencias (físicas/lógicas) sea en la escena o exista una alta probabilidad de ello, es necesario que algunos equipos adicionales formen parte del equipamiento básico de herramientas, a saber:

- Computadora portátil con herramientas forenses que permita la adquisición en escena.
- Herramientas para obtener un volcado de memoria.
- Dispositivo de protección contra escritura forense para proteger evidencias digitales.
- Dispositivos para interceptar el tráfico de red puede ser necesario (hub/ switch).
- Cables de conexión necesarios.
- Medios desinfectados para almacenar imágenes de cualquier evidencia digital.

Como regla general, el equipamiento básico de herramientas de los primeros intervinientes en el manejo de evidencia digital, debe permitir recopilar evidencia digital de dispositivos estándar de PC / laptop, teléfonos móviles, tabletas, televisores inteligentes, consolas de juegos y todos los demás dispositivos modernos que contengan medios de almacenamiento digital. Cuando se trata de teléfonos móviles, se debe considerar usar bolsas de Faraday[25] para aislarlos y garantizar su preservación.

Cabe destacar que todo el equipo utilizado durante el trabajo forense debe ser apropiado para tal propósito y mantenido periódica y adecuadamente por consideraciones operativas, donde solo las herramientas, técnicas y procedimientos evaluados adecuadamente deben utilizarse para un examen forense, además que todos los medios utilizados para hacer copias forenses deben ser estériles.

[25] Elementos de resguardo especialmente diseñados para la recolección, preservación, transporte y análisis de dispositivos móviles e inalámbricos, para aislarlos de la red de comunicaciones y protegerlos contra descargas electrostáticas.

6.2 Adquisición de imágenes Forenses

6.2.1 Consideraciones generales

A continuación, se presenta la metodología general, independiente del sistema operativo empleado, con la finalidad de obtener este tipo de evidencias lógicas. Se recomienda preservar en todo momento la integridad y la autenticidad de información recolectada.

- Uso de herramientas forenses: los kits de herramientas forenses son herramientas especializadas, diseñadas para cumplir con los criterios de las investigaciones forenses. Permiten acceder y adquirir datos de manera que los cambios en los medios de origen son mínimos. Entre las diferentes opciones se encuentran desde aplicaciones de distribución libre y sistemas operativos de arranque de LiveCD en medios extraíbles, hasta aplicaciones comerciales de nivel empresarial.
- No realizar modificaciones: durante el proceso de preservación y recolección de evidencias lógicas, en la medida de lo posible, no se debe modificar, eliminar ni agregar datos en los medios de origen. Como ya se hubiera indicado, el empleo de herramientas forenses reducirá el impacto de esta actividad, dado que están diseñadas para acceder a los medios en un estado de solo lectura y no crearán ni modificarán archivos en los sistemas de origen, a menos que sea absolutamente necesario. Estas herramientas suelen publicar una lista que contiene los archivos que se modifican en caso de ser empleadas en un sistema "en vivo".
- Realizar el hash criptográfico: el uso de hash garantizará la autenticidad e integridad de las evidencias lógicas recolectadas a lo largo de la investigación forense. Todas estas deben ser hasheadas al momento de su recolección, transferencia y montaje para análisis. Los valores de hash deben registrarse en múltiples ubicaciones, como el registro del investigador forense y formularios de cadena de custodia.

- Documentar lo actuado: los investigadores forenses deben mantener registros detallados de las acciones que realizan durante el proceso de adquisición y recopilación. Si bien los registros se pueden crear y mantener, ya sea en papel o en formato electrónico según la preferencia del investigador forense, cada opción tendrá un impacto en el proceso. Los registros de papel son menos susceptibles de ser manipulados o alterados, aun cuando es menos probable que contengan información técnica detallada, ya que debería ingresarse a mano. Los registros electrónicos pueden contener información técnica detallada, pero son menos tangibles, susceptibles de ser alterados, por lo cual resultan menos fiables. Sin embargo, la integridad de los registros electrónicos debe garantizarse mediante el cálculo hash correspondiente.

- Registrar y preservar la cadena de custodia: la cadena de custodia, en combinación con hash, resulta esencial para garantizar la autenticidad e integridad de la evidencia lógica recolectada. La cadena de custodia debe comenzar con la recolección de datos y mantenerse hasta su aceptación como evidencia.

- Realizar copias: una vez que la evidencia lógica es recolectada, la misma debe duplicarse y almacenarse en medios limpios, preferiblemente inalterables, como soportes ópticos en formato CD-R o DVD-R. A tal efecto, cada archivo de evidencia lógica debe ser hasheado de forma individual, para garantizar que dichas copias sean idénticas al original y se reflejen en la cadena de custodia. Se debe contar con al menos dos copias de la evidencia lógica recolectada, una para resguardo y otra para el análisis.

6.2.2 Bloqueadores de escritura

Existen una serie de requisitos generales que deben cumplir estos dispositivos, por ejemplo, la herramienta no debe permitir cambios en la unidad protegida, tampoco impedirá obtener información de o sobre cualquier unidad, ni ejecutar operaciones en las unidades que no estén protegidas [41].

6.2.2.1 Bloqueadores por hardware

Se tratan de dispositivos que permiten conectar una unidad de disco a un sistema informático mediante diferentes puertos (USB/E-SATA/FIREWARE), para obtener imágenes forenses del disco y garantizar que todas las operaciones de escritura en el disco se encuentren bloqueadas.

Ilustración 8: Bloqueador de escritura Tableau T35u (SATA/IDE)[26].

6.2.2.2 Bloqueadores por software

Básicamente, los bloqueadores por software permiten conectar una unidad de disco a un sistema informático mediante un puerto USB configurado en modo "solo lectura", para obtener de esta manera imágenes forenses del disco y garantizar que las operaciones de escritura en el disco se encuentren bloqueadas.

Si bien los puertos USB pueden configurarse de forma manual, por ejemplo mediante la herramienta Regedit[27], existen diferentes soluciones que realizan esta maniobra de forma automática.

[26] Bloqueador de escritura por hardware desarrollado por la firma Guidance Software.
[27] Regedit es el nombre de la herramienta que permite editar el registro del sistema operativo Windows. Este registro es la base de datos donde se guardan las preferencias del usuario en materia de configuraciones.

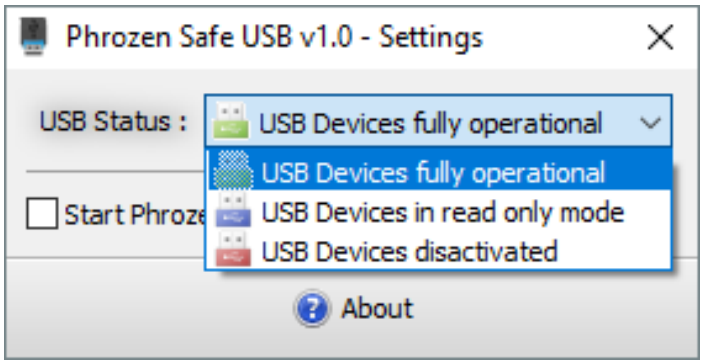

Ilustración 9: Bloqueador de escritura Phrozen Safe USB v1.0[28].

Cabe destacar que los bloqueadores de escritura de software y hardware realizan el mismo trabajo. Evitan escrituras en dispositivos de almacenamiento. La principal diferencia entre ambos es que los bloqueadores de escritura de software se instalan en una estación de trabajo informática forense, mientras que los bloqueadores de escritura de hardware tienen un software de bloqueo de escritura instalado en un chip controlador dentro de un dispositivo físico portátil. A continuación, se detallan ventajas y desventajas de las dos variantes planteadas.

BLOQUEADORES DE ESCRITURA POR HARDWARE	VENTAJAS	• No depende del sistema operativo subyacente. • Resulta más fácil de explicar a personas que no son técnicas. • Posee indicaciones visuales de la función a través de luces e interruptores físicos. • Por lo general proporciona interfaces para diferentes dispositivos de almacenamiento (IDE, SATA, etc.). • Parece ser más aceptado en la comunidad forense general.
	DESVENTAJAS	• Constituye un dispositivo adicional para transportar. • Requiere cierto mantenimiento. • Se encuentra limitado a las interfaces integradas en el dispositivo.

Tabla 10: Ventajas y desventajas de los bloqueadores de escritura por hardware.

[28] Bloqueador de escritura por software freeare desarrollado por la firma Phrozen.

BLOQUEADORES DE ESCRITURA POR SOFTWARE	VENTAJAS	• Se instala directamente en su estación de trabajo del investigador. • Utiliza las interfaces disponibles en la estación de trabajo del investigador, lo que evita gastos adicionales.
	DESVENTAJAS	• Podría necesitar adaptadores externos para interfaces nuevas. • Puede ser más difícil de explicar a personas no técnicas. • Siempre se debe comprobar su funcionalidad antes de conectar un dispositivo para análisis.

Tabla 11: Ventajas y desventajas de los bloqueadores de escritura por software.

6.2.3 Adquisición bajo entornos Windows y Linux

Como ya se hubiera indicado, la plataforma de trabajo se encontrará ligada a cada escenario posible, al igual que la experiencia del investigador forense, quien al final de cuentas definirá el entorno de trabajo de acuerdo a las necesidades imperantes, familiaridad con la herramienta forense empleada e incluso factores tales como la optimización de tiempo de trabajo.

6.2.3.1 Entorno Windows y uso de FTK Imager[29]

Posee una interfaz gráfica amigable. Se pueden obtener imágenes forenses en formato (DD, SMART, E01 y AFF).

Para realizar una imagen forense a partir de FTK Imager se deben seguir los siguientes pasos:

- Iniciar la aplicación, seleccionar la opción Archivo y luego, Crear Imagen de Disco.
- Seleccionar la unidad de origen (Disco físico/Disco lógico/Archivo de imagen/Contenido de una carpeta/Unidades ópticas tipo CD/DVD).
- Escoger el formato de la imagen forense (DD/SMART/E01/AFF).

[29] FTK Imager es una herramienta forense desarrollada por AccessData empleada, entre otras actividades, para la adquisición imágenes forenses.

- Completar datos relacionados al caso, evidencia e investigador.
- Acto seguido, se debe escoger la ruta de destino de la imagen forense, nombre de la misma, si se obtendrá un archivo único o la misma será spliteada en segmentos de determinado tamaño.
- A continuación, se debe chequear el origen y destino de la imagen forense, como así también seleccionar la verificación de la misma, para luego iniciar su obtención.
- Finalizado el proceso de obtención y comprobación, se aprecia un reporte con los algoritmos de seguridad hash (MD5/SHA1).
- Como resultado, en la ruta de destino se aprecian los archivos correspondientes a la imagen forense obtenida y su respectivo reporte.

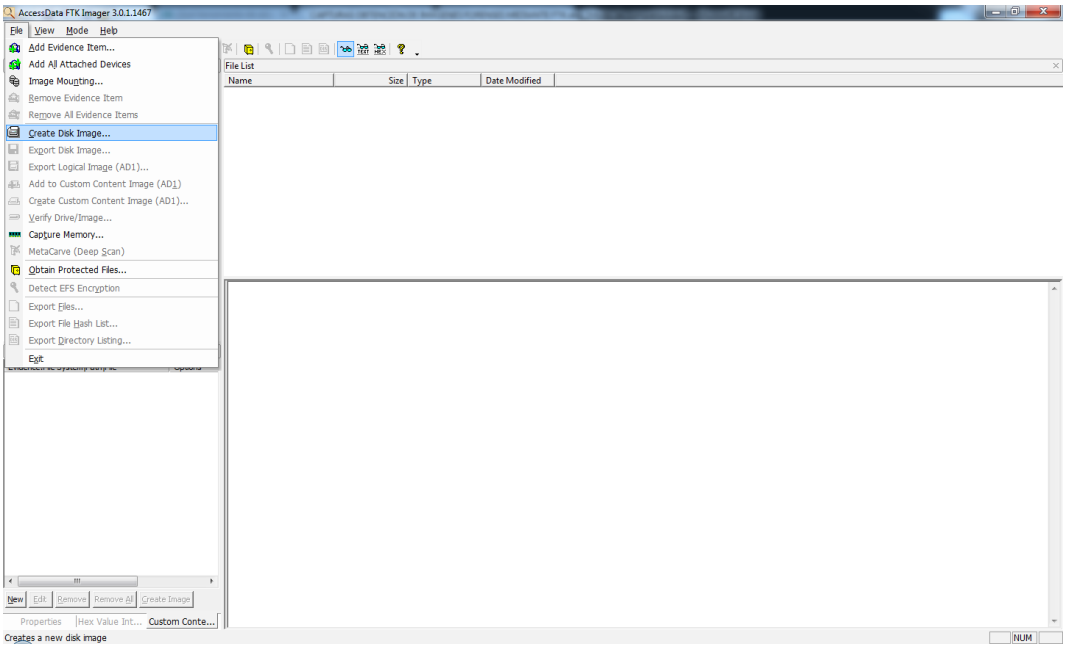

Ilustración 10: FTK Imager - Creación de imagen de disco.

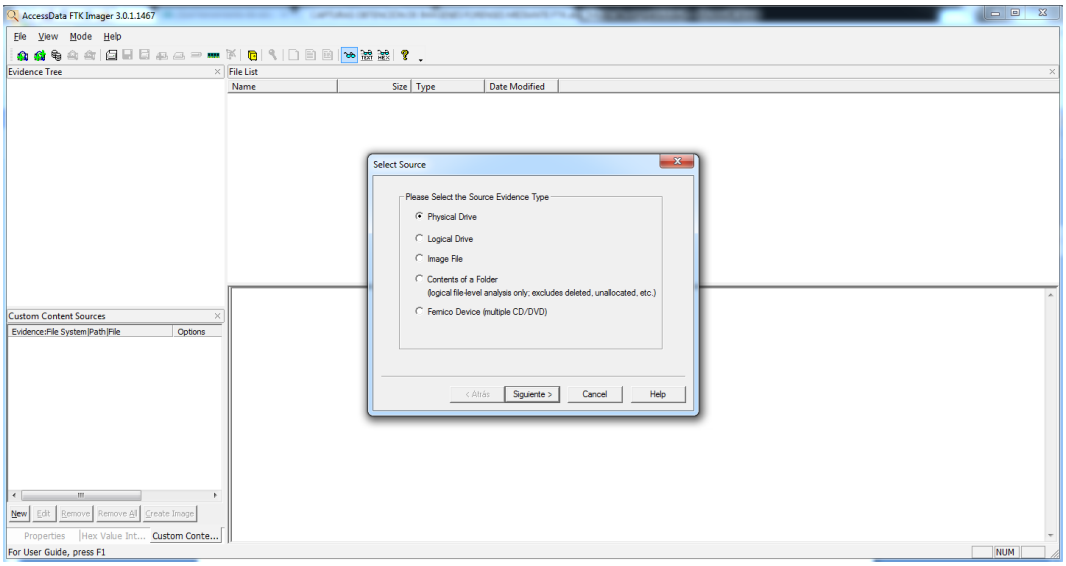

Ilustración 11: FTK Imager - Selección de tipo de origen.

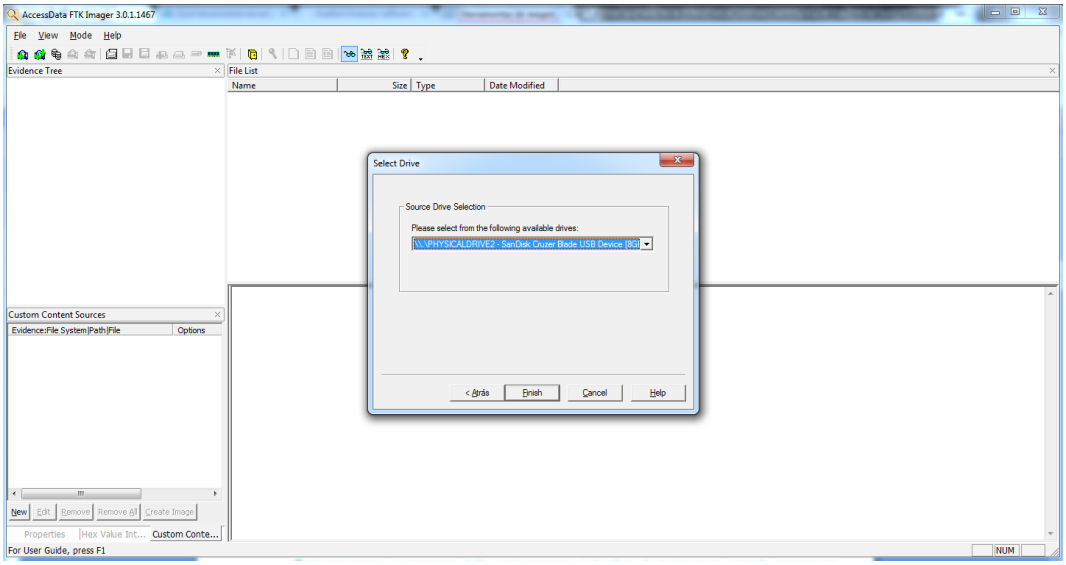

Ilustración 12: FTK Imager - Selección de disco de origen.

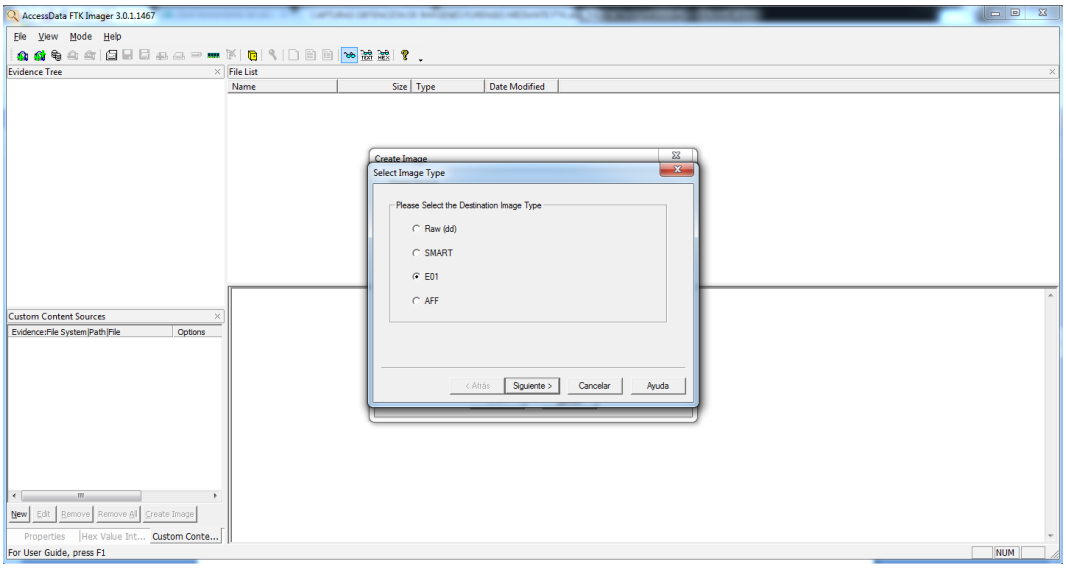

Ilustración 13: FTK Imager - Selección de formato de imagen.

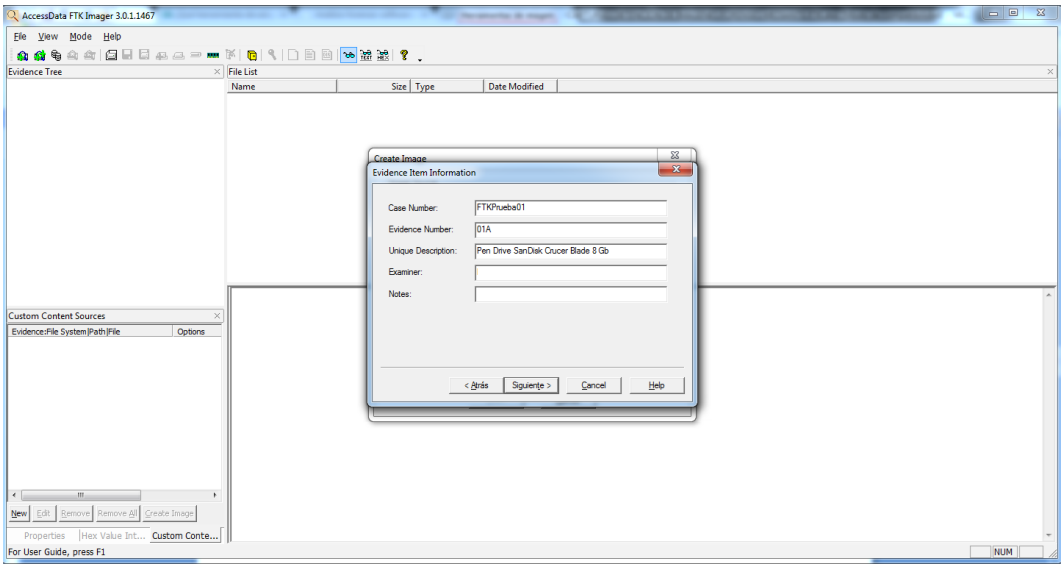

Ilustración 14: FTK Imager - Información de la evidencia.

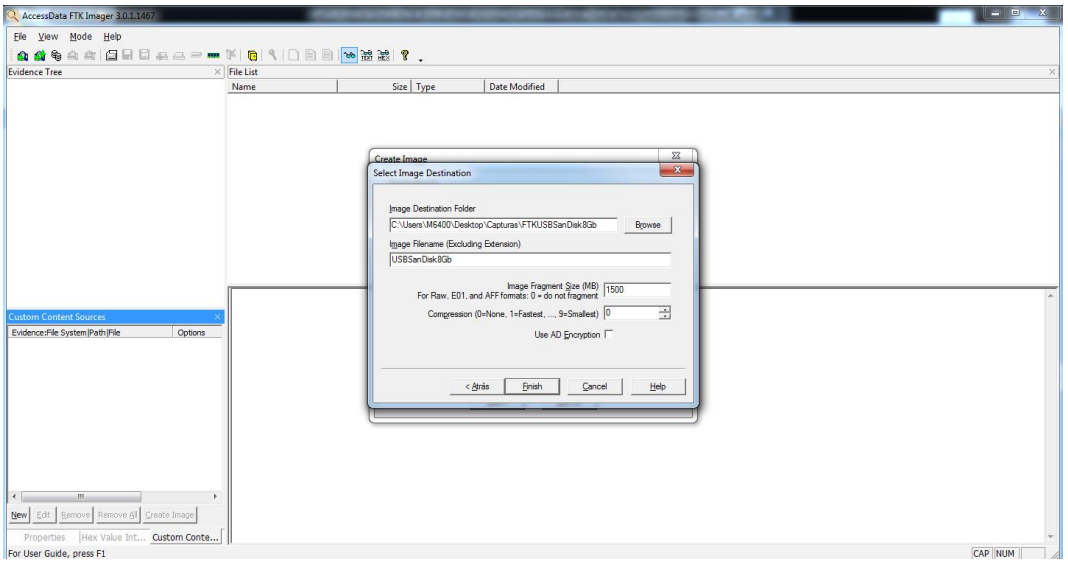

Ilustración 15: FTK Imager - Selección de ruta de destino.

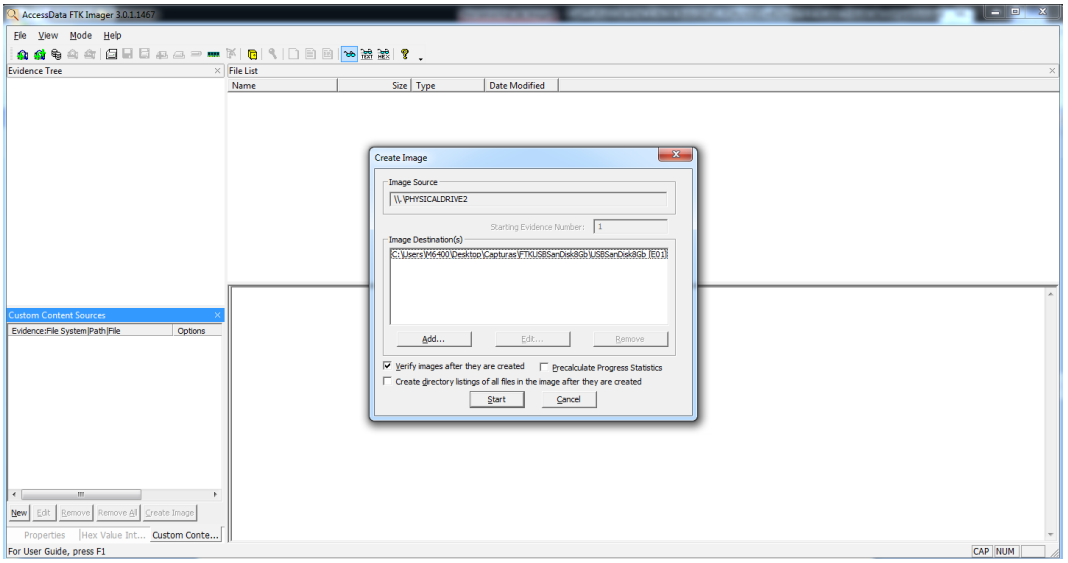

Ilustración 16: FTK Imager - Chequeo de parámetros y selección de verificación de la imagen.

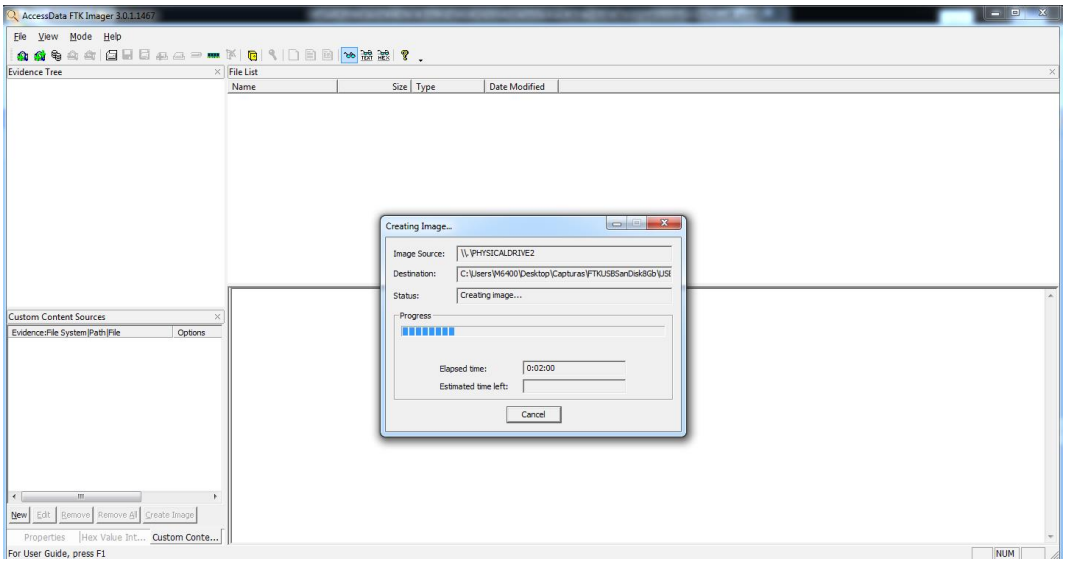

Ilustración 17: FTK Imager – Obtención de la imagen.

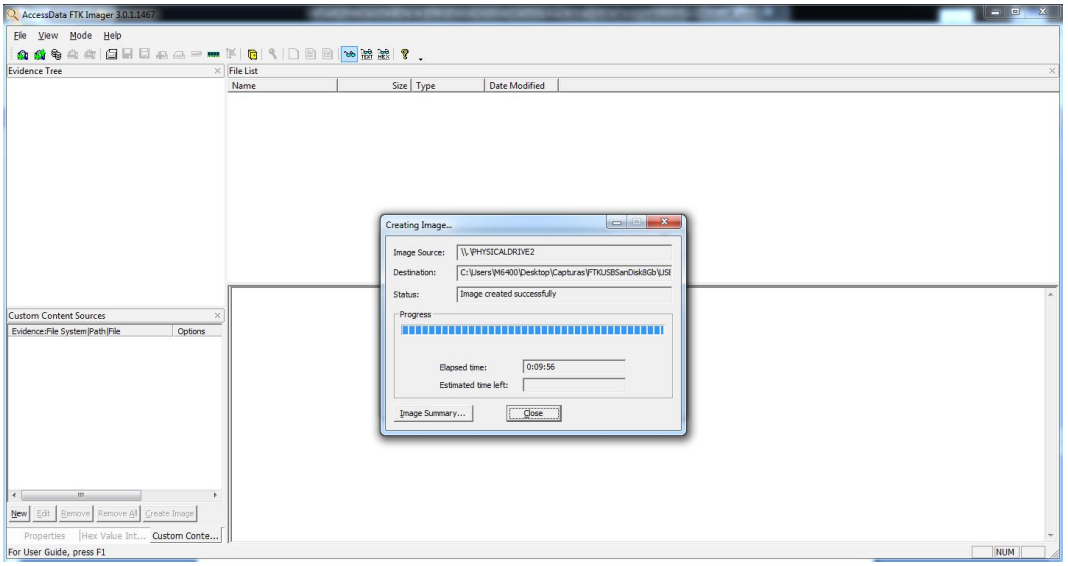

Ilustración 18: FTK Imager – Verificación de la imagen.

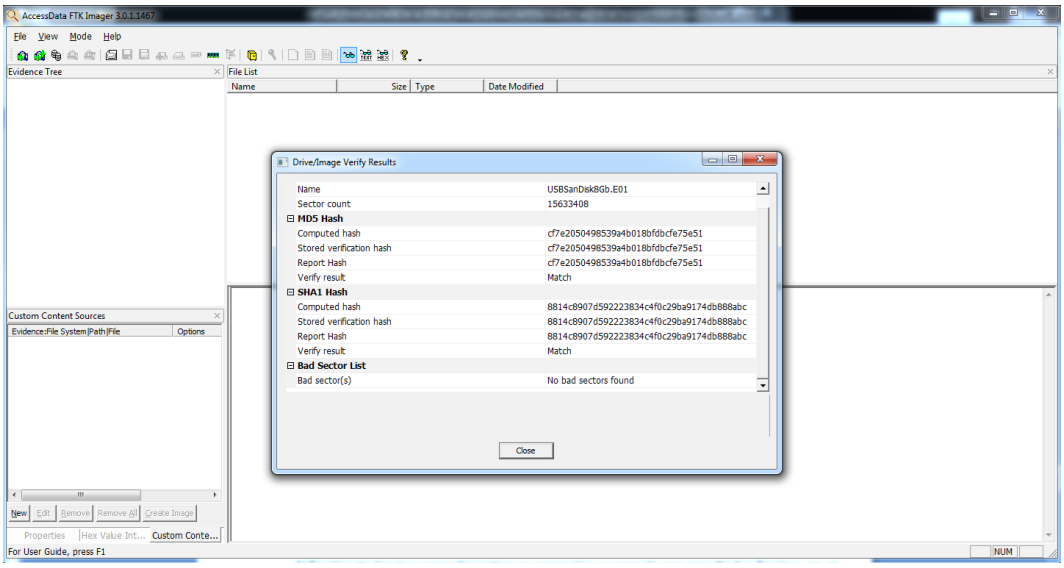

Ilustración 19: FTK Imager – Finalización del proceso.

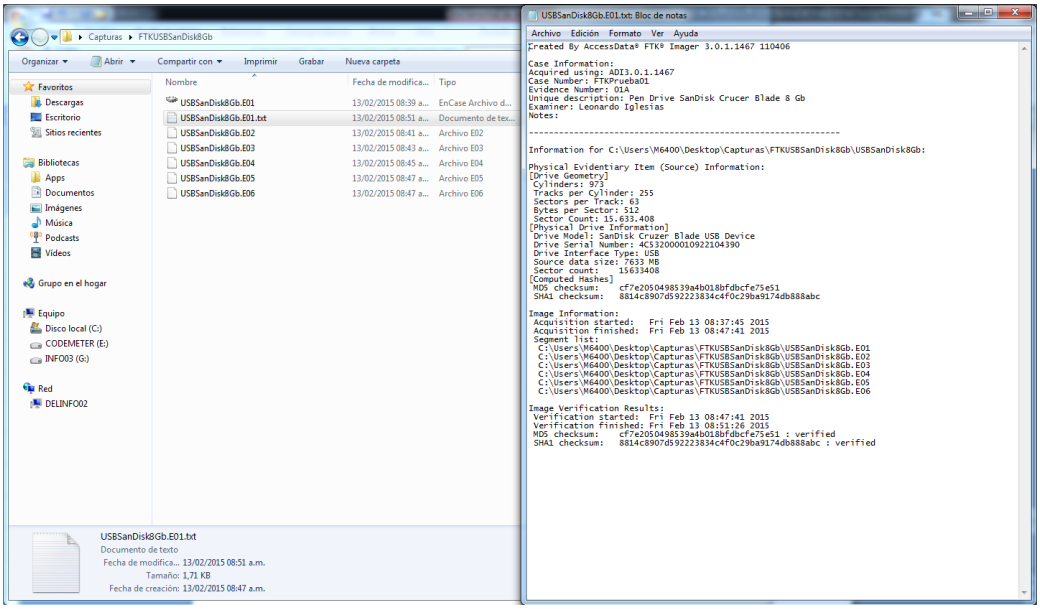

Ilustración 20: FTK Imager – Reporte correspondiente.

6.2.3.2 Entorno Linux - Uso de Guymager[30]

Posee una intuitiva interfaz gráfica y gran velocidad de copiado, debido a su diseño y eficaz uso de tecnología multiprocesador. Se pueden obtener imágenes

[30] Guymager es una herramienta forense de fuente abierta para adquisición de imágenes forenses.

forenses en formato DD y EWF (E01), además cuenta con la opción de duplicar discos. Para realizar una imagen forense a partir de Guymager se deben realizar los siguientes pasos:

- Iniciar la aplicación, seleccionar la unidad de origen y a partir del menú desplegable indicar la opción deseada (adquirir imagen o duplicar disco).
- Definir parámetros tales como formato de la imagen (DD/EWF), datos relacionados a la evidencia y caso de análisis, ruta de destino de la imagen forense, nombre de la misma, si se obtendrá un archivo único o la misma será spliteada [31] en segmentos de determinado tamaño. Asimismo, se puede seleccionar la habilitación para comprobación y cálculo de algoritmos de seguridad hash (MD5/SHA1/SHA256).
- Realizada esta configuración previa, se inicia el proceso de obtención de la imagen y se muestra en pantalla que se encuentra en ejecución.
- Finalizado el proceso, dicha actividad se visualiza en pantalla y como resultado, en la ruta de destino se aprecian los archivos correspondientes a la imagen forense obtenida y su respectivo reporte.

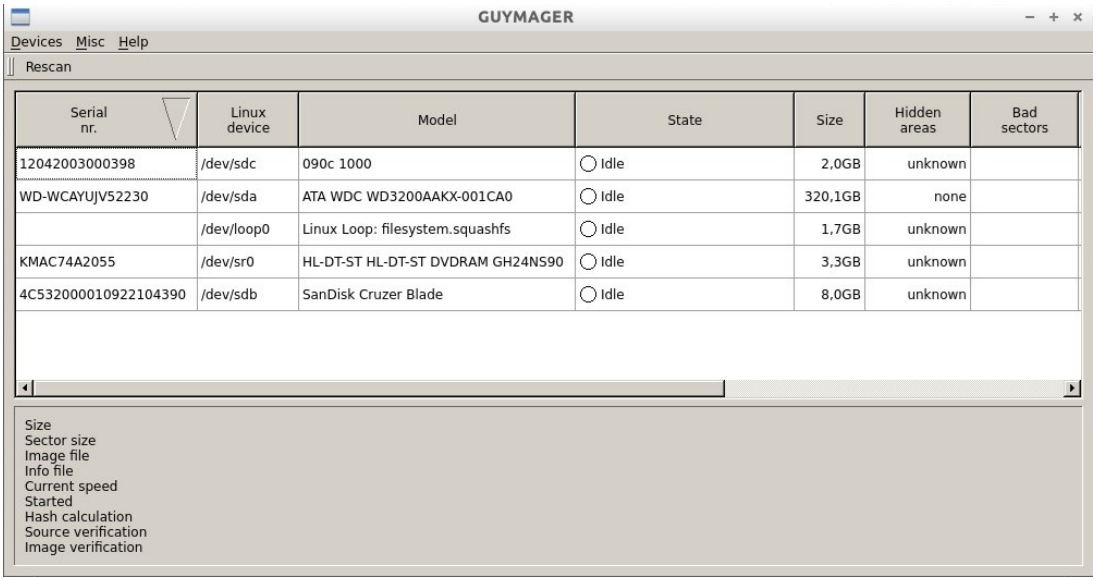

Ilustración 21: Guymager - Ventana de inicio.

[31] Divisiones según capacidades preconfigurables por el usuario y generadas de forma automática por la herramienta forense.

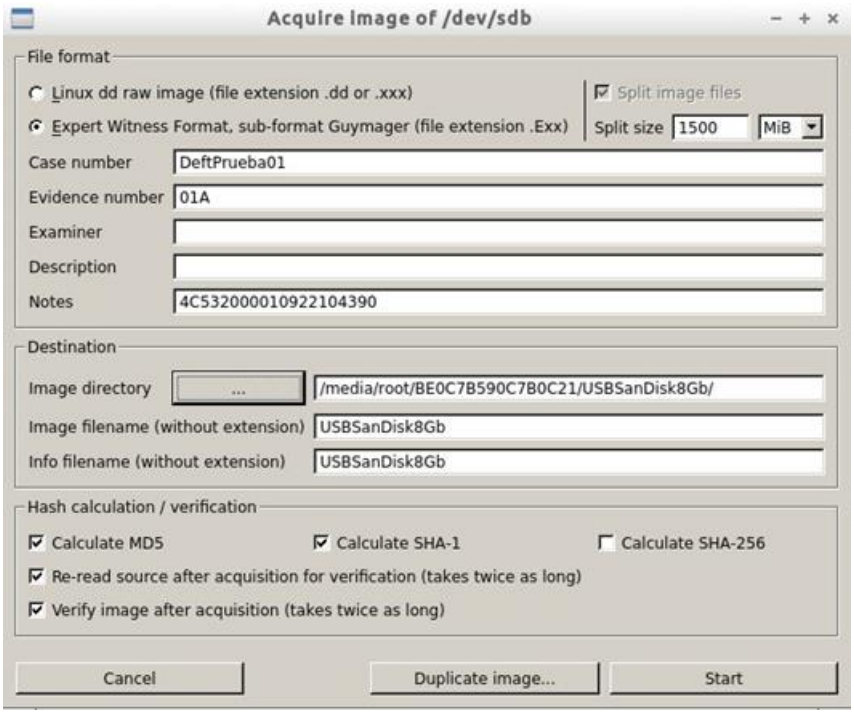

Ilustración 22: Guymager - Configuración de la Imagen.

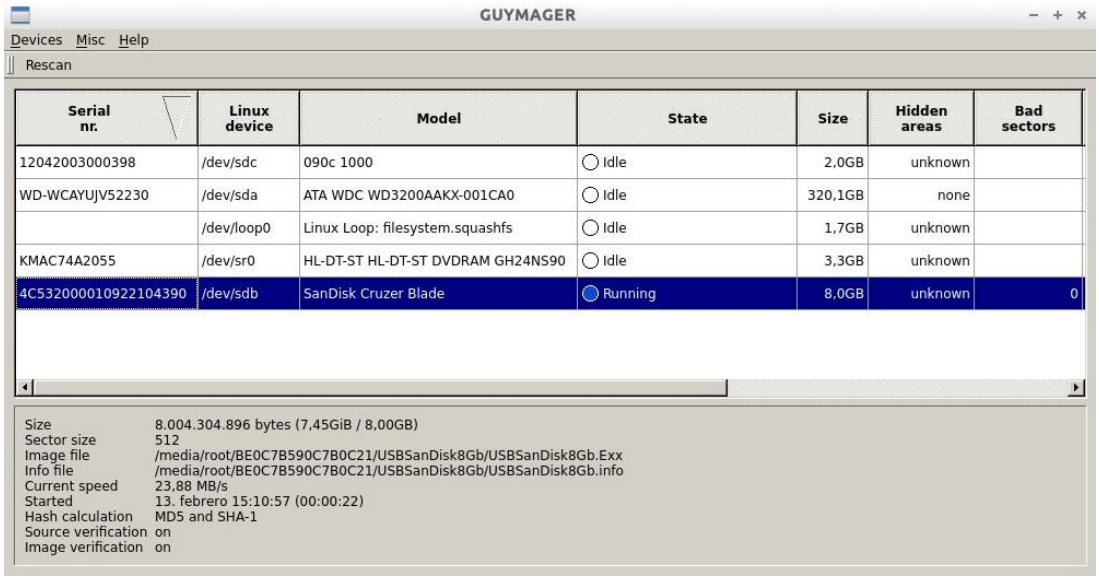

Ilustración 23: Guymager - Inicio de la adquisición.

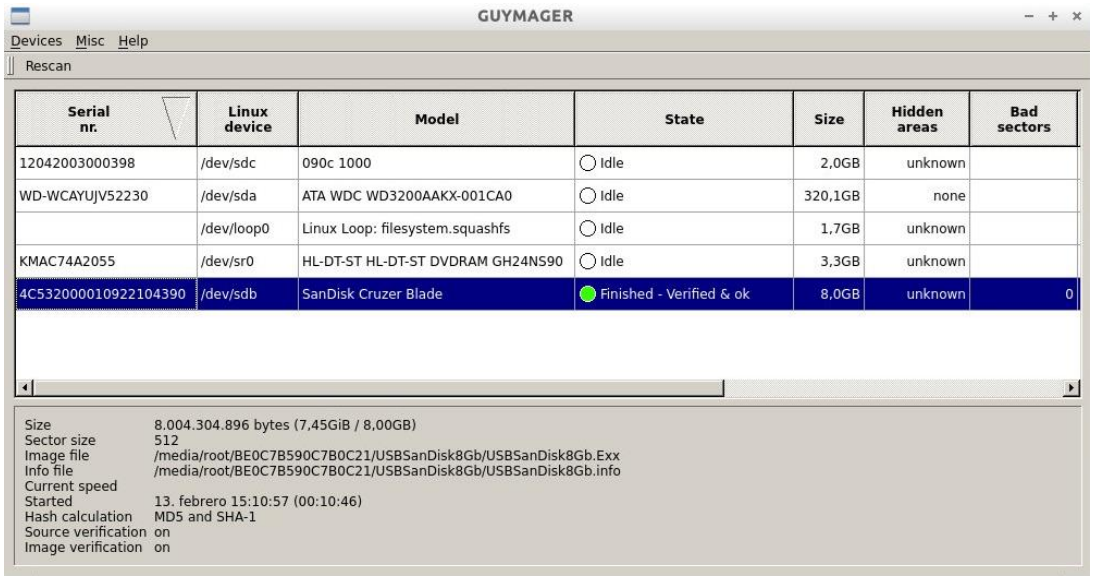

Ilustración 24: Guymager - Finalización de la adquisición.

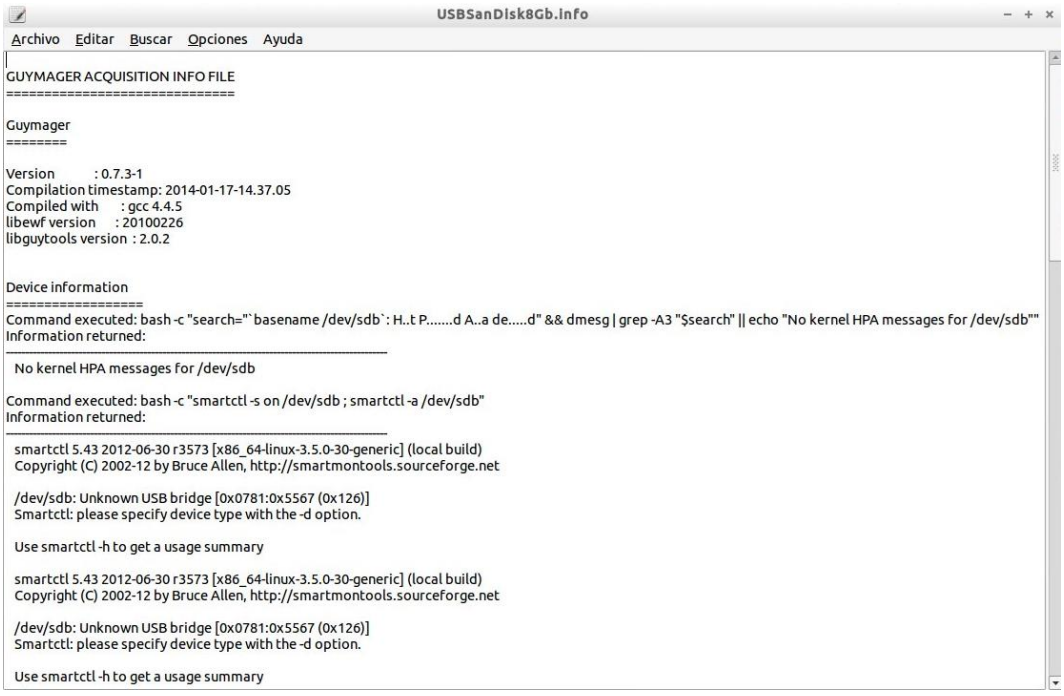

Ilustración 25: Guymager - Reporte de la imagen forense.

6.2.3.3 Entorno Linux - Comando DD[32]

Para ello, se ingresa código mediante consola. Se pueden obtener imágenes forenses en formato ISO, RAW (DD), la realización de imágenes forenses a partir del comando DD consta de los siguientes pasos:

- Abrir una consola de comando.
- Identificar el dispositivo de origen y sus respectivas tablas de partición mediante el comando “fdisk-l”.
- Calcular el algoritmo de seguridad hash del medio de origen (sdX) mediante el comando “sudo sha1sum /dev/sdc > /tmp/hash_sdc.sha1” y chequearlo mediante el comando “cat /hash_sdc.sha1”.
- Abrir una nueva consola y obtener la imagen del medio de origen mediante la herramienta “dd”, utilizar el comando “sudo dd if=/dev/sdX of=/tmp/sdZ.dd conv=noerror,sync”. Donde “if” indica la unidad de origen (sdX) y “of” la de destino (sdZ). Asimismo, el parámetro “conv” convierte el archivo de acuerdo a la lista de símbolos delimitados por comas, el parámetro “noerror” garantiza la continuidad de la operación aun cuando existan errores de lectura y por último “sync” se emplea para rellenar bloques con ceros en caso de error.
- Finalizado el proceso se aprecia un resumen con información de la actividad, como por ejemplo registros de ingreso y salida, bytes copiados, tiempo transcurrido para la obtención y promedio de la velocidad de copiado.
- A fin de realizar la comprobación de la imagen forense obtenida, se procede a calcular su algoritmo de seguridad hash mediante el comando “sha1sum /dev/sdZ.dd”.

[32] El comando DD, acrónimo de (Dataset Definition) es una herramienta provista por distribuciones Linux que, entre otras actividades, puede ser empleada para la adquisición imágenes forenses.

```
sansforensics@siftworkstation: ~
/dev/sda2      1044385790  1048573951     2094081    5  Extended
/dev/sda5      1044385792  1048573951     2094080   82  Linux swap / Solaris

Disk /dev/sdb: 536.9 GB, 536870912000 bytes
214 heads, 31 sectors/track, 158060 cylinders, total 1048576000 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0xdeb1c7df

   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1            2048  1048575999   524286976   83  Linux

Disk /dev/sdc: 15.6 GB, 15610576896 bytes
255 heads, 63 sectors/track, 1897 cylinders, total 30489408 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x20ddee48

   Device Boot      Start         End      Blocks   Id  System
/dev/sdc1            2048    30488575    15243264    b  W95 FAT32
sansforensics@siftworkstation:~$
```

Ilustración 26: Comando DD - Identificación del medio de origen.

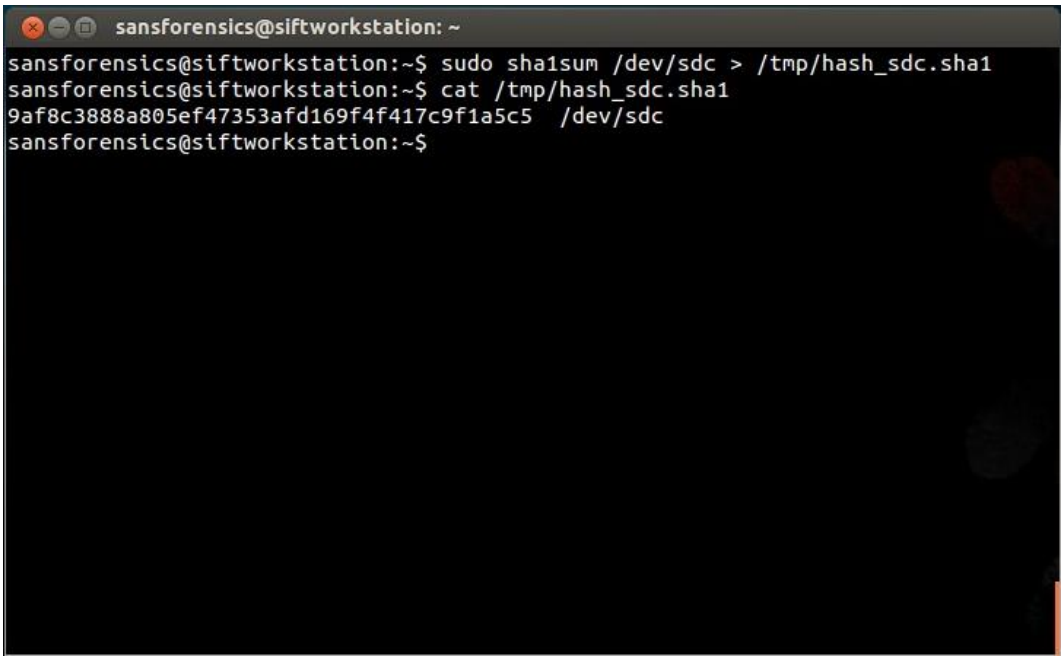

Ilustración 27: Comando DD - Hash SHA1 del medio de origen.

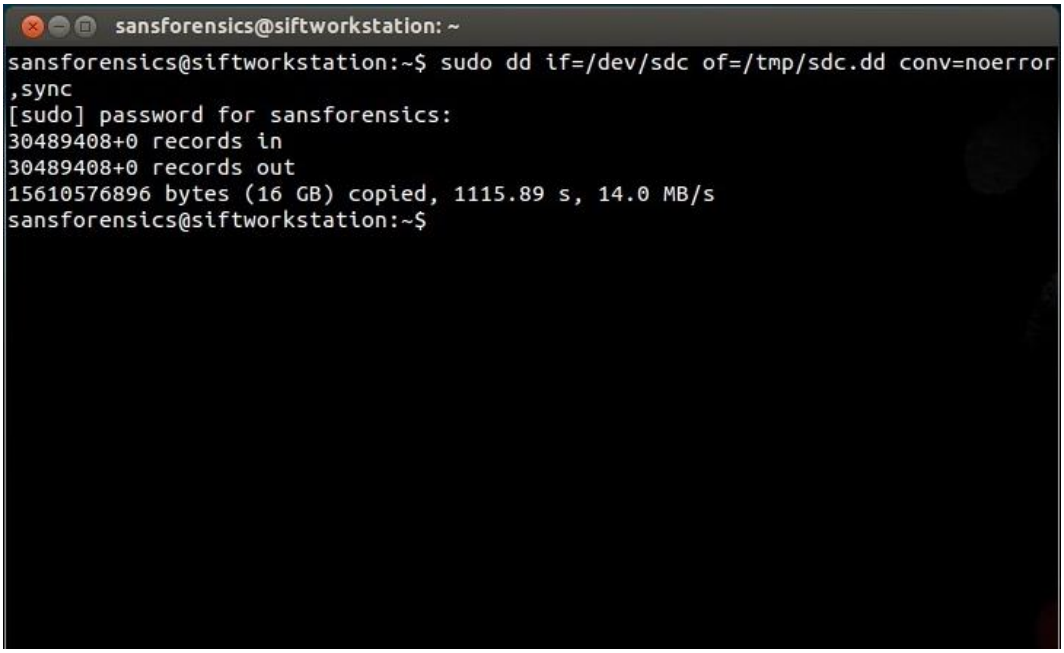

Ilustración 28: Comando DD - Obtención de la imagen forense y resumen.

```
sansforensics@siftworkstation: ~
sansforensics@siftworkstation:~$ sudo dd if=/dev/sdc of=/tmp/sdc.dd conv=noerror
,sync
[sudo] password for sansforensics:
30489408+0 records in
30489408+0 records out
15610576896 bytes (16 GB) copied, 1115.89 s, 14.0 MB/s
sansforensics@siftworkstation:~$ sha1sum /tmp/sdc.dd
9af8c3888a805ef47353afd169f4f417c9f1a5c5  /tmp/sdc.dd
sansforensics@siftworkstation:~$
```

Ilustración 29: Comando DD – Hash de la imagen forense.

```
sansforensics@siftworkstation: ~
sansforensics@siftworkstation:~$ sudo sha1sum /dev/sdc > /tmp/hash_sdc.sha1
sansforensics@siftworkstation:~$ cat /tmp/hash_sdc.sha1
9af8c3888a805ef47353afd169f4f417c9f1a5c5  /dev/sdc
sansforensics@siftworkstation:~$

sansforensics@siftworkstation: ~
sansforensics@siftworkstation:~$ sudo dd if=/dev/sdc of=/tmp/sdc.dd conv=noerror
,sync
[sudo] password for sansforensics:
30489408+0 records in
30489408+0 records out
15610576896 bytes (16 GB) copied, 1115.89 s, 14.0 MB/s
sansforensics@siftworkstation:~$ sha1sum /tmp/sdc.dd
9af8c3888a805ef47353afd169f4f417c9f1a5c5  /tmp/sdc.dd
sansforensics@siftworkstation:~$
```

Ilustración 30: Comando DD – Comprobación de la imagen forense.

6.2.4 Adquisición de dispositivos móviles

El contenido de la memoria de un dispositivo móvil a menudo contiene información, como datos eliminados, cuya accesibilidad dependerá del tipo de adquisición realizada por parte del investigador forense.

Podría decirse que existe un orden jerárquico en función de la complejidad del tipo de técnica empleada para la adquisición de evidencias móviles.

6.2.4.1 Evidencia Lógica en móviles

Dicha técnica copia los objetos almacenados en la memoria del dispositivo móvil, sincronizando la terminal con una estación de trabajo mediante mecanismos dispuestos originalmente por el fabricante.

La conexión puede ser realizada por un medio físico (Cable USB) o inalámbrico (WiFi), solicitando al sistema operativo del dispositivo móvil que envíe la información requerida por el examinador.

Como ventaja podemos indicar la sencillez de dicho proceso, aunque por el otro lado ofrece una cantidad acotada de información.

6.2.4.2 Evidencia Física en móviles

Este método es el todo analista forense prefiere a la hora de iniciar el análisis forense de un dispositivo móvil, dado que permite efectuar una imagen forense idéntica del original, preservando la totalidad evidencias que podrían encontrarse almacenadas en memoria.

Como ventaja podríamos citar que a partir de esta técnica resulta factible recuperar elementos eliminados, pero en contrapartida es un procedimiento complejo en relación con otros métodos, al igual que su procesamiento conlleva una mayor inversión de tiempo.

6.2.4.3 Chip-OFF[33]

Esta extracción requiere remover físicamente la memoria flash, proporcionando a los examinadores forenses la capacidad de crear una imagen binaria del chip removido, que una vez completada puede ser analizada.

Este tipo de adquisición es el que se podría asemejar a los métodos de adquisición directa relacionado con las imágenes físicas de unidades de disco duro como en el análisis forense digital tradicional.

Asimismo, este tipo de técnicas requieren una amplia capacitación para realizar operaciones exitosas, constituyendo un desafío por la amplia variedad de tipos de chips, formatos de datos sin procesar y el riesgo de causar daño físico al chip durante el proceso de extracción.

6.2.4.4 JTAG[34]

Por medio de esta interfaz los examinadores forenses pueden comunicarse con un componente compatible con JTAG utilizando dispositivos programadores independientes diseñados especialmente para testear puntos de prueba definidos.

JTAG ofrece a los especialistas otra vía para obtener la imagen de dispositivos bloqueados, con daños menores o que no pueden interconectarse adecuadamente de otra manera.

El método consiste en conectar una interfaz física o arnés de cableado desde una estación de trabajo a la interfaz JTAG del dispositivo móvil y acceder a la memoria a través de su microprocesador para obtener una imagen forense.

Las extracciones de JTAG son invasivas, dado que para su acceso y conexiones de cableado se requiere desmontar parte de un dispositivo móvil.

Las denominadas Flasher Box son dispositivos diseñados originalmente para actividades de reparación o actualización de dispositivos móviles, las que en la

[33] Los métodos de chip-off se refieren a la adquisición de datos directamente desde la memoria flash de un dispositivo móvil.
[34] La mayoría de los fabricantes admiten el estándar JTAG (Joint Test Action Group), que define una interfaz de prueba común para procesadores, memorias y otros tipos de chips semiconductores.

actualidad son utilizadas para realizar adquisiciones físicas, acompañadas de software para facilitar al acceso de datos. Entre sus limitaciones podemos señalar:

- Se requiere con frecuencia el reinicio del dispositivo móvil para comenzar el proceso de extracción, lo que incrementa las posibilidades de activar mecanismos de autenticación impidiendo un análisis más profundo.
- Muchas Flash Box recuperan datos en formato encriptado, requiriendo que el examinador forense deba utilizar software provisto por el fabricante de la caja para descifrar la información o incluso utilizar técnicas de ingeniería inversa por parte del analista.
- Muchos modelos de teléfonos no proporcionan la adquisición de todo el rango de memoria, encontrándose disponibles solo ciertas porciones lo que implica un volcado parcial de información.
- La falta de documentación sobre el uso de estas herramientas es común, por cuanto los métodos de extracción se comparten de manera informal, por ejemplo mediante foros moderados por usuarios más experimentados.

A pesar de estas limitaciones, el uso de Flash Boxs es una opción viable para muchos casos forenses, donde la capacitación adecuada, experiencia y comprensión de su funcionamiento son claves de éxito.

El uso de esta técnica requiere una amplia gama de experiencia y una capacitación adecuada para extraer y analizar imágenes binarias con estos métodos, que incluyen la ubicación y la conexión a puertos JTAG, la creación de cargadores de arranque personalizados y la recreación de sistemas de archivos.

[Página dejada en blanco intencionalmente]

6.3 Cadena de custodia

6.3.1 Anverso

PLANILLA DE CADENA DE CUSTODIA			
DATOS DEL LUGAR	LUGAR:	FECHA:	HORA:
	UNIDAD INTERVINIENTE:		
	JUZGADO/FISCALÍA:		
	SECRETARIA:		
	CARÁTULA:		
	SUMARIO/CAUSA NRO:		
	OBSERVACIONES:		
ELEMENTOS	**ELEMENTOS SECUESTRADOS**		
	DESCRIPCIÓN:		
	LUGAR DE RECOLECCIÓN:		
	MODO DE CONSERVACIÓN: SOBRE DE PAPEL ☐ CAJA CARTÓN ☐ BOLSA PLÁSTICA ☐ OTROS:		
	MODO DE TRASLADO:		
	DESTINO:		

TESTIGOS	NOMBRES Y APELLIDO	D. N. I.	FIRMA
1			
2			

PRIMER INTERVINIENTE			
COLECTADO POR	NOMBRES Y APELLIDO	HORA Y FECHA	FIRMA
	CARGO:		

6.3.2 Reverso

	NOMBRES Y APELLIDO	GRADO - CE- LP - DNI	FIRMA
ENTREGA			
RECIBE			
MOTIVO DE ENTREGA: CUSTODIA ☐ TRASLADO ☐ PERITAJE ☐ DESTRUCCIÓN ☐			
FECHA / HORA: OBSERVACIONES:			
	NOMBRES Y APELLIDO	GRADO - CE- LP - DNI	FIRMA
ENTREGA			
RECIBE			
MOTIVO DE ENTREGA: CUSTODIA ☐ TRASLADO ☐ PERITAJE ☐ DESTRUCCIÓN ☐			
FECHA / HORA: OBSERVACIONES:			
	NOMBRES Y APELLIDO	GRADO - CE- LP - DNI	FIRMA
ENTREGA			
RECIBE			
MOTIVO DE ENTREGA: CUSTODIA ☐ TRASLADO ☐ PERITAJE ☐ DESTRUCCIÓN ☐			
FECHA / HORA: OBSERVACIONES:			
	NOMBRES Y APELLIDO	GRADO - CE- LP - DNI	FIRMA
ENTREGA			
RECIBE			
MOTIVO DE ENTREGA: CUSTODIA ☐ TRASLADO ☐ PERITAJE ☐ DESTRUCCIÓN ☐			
FECHA / HORA: OBSERVACIONES:			
	NOMBRES Y APELLIDO	GRADO - CE- LP - DNI	FIRMA
ENTREGA			
RECIBE			
MOTIVO DE ENTREGA: CUSTODIA ☐ TRASLADO ☐ PERITAJE ☐ DESTRUCCIÓN ☐			
FECHA / HORA: OBSERVACIONES:			
	NOMBRES Y APELLIDO	GRADO - CE- LP - DNI	FIRMA
ENTREGA			
RECIBE			
MOTIVO DE ENTREGA: CUSTODIA ☐ TRASLADO ☐ PERITAJE ☐ DESTRUCCIÓN ☐			
FECHA / HORA: OBSERVACIONES:			

6.4 Herramientas Forenses

Una vez efectuada la obtención de imágenes forenses, acompañadas de sus respectivos algoritmos de seguridad hash y cadenas de custodia, se da paso al análisis de la información contenida en las evidencias recolectadas.

En tal sentido, el análisis forense digital debe cumplimentar los requisitos periciales objeto de la investigación e identificar aquellos artefactos forenses de interés, para su posterior presentación mediante los informes correspondientes.

Existen diferentes herramientas informáticas de amplio reconocimiento en la comunidad científica, las cuáles desempeñan funciones específicas.

6.4.1 Autopsy

Plataforma forense digital con interfaz gráfica de la firma The Sleuth Kit. Es utilizado por los encargados de hacer cumplir la ley, militares e investigadores forenses corporativos, cuyas principales características se listan a continuación:

- Múltiples sistemas operativos: posee versiones tanto para Windows como para Linux.
- Casos multiusuario: posibilidad de colaborar con otros investigadores forenses en casos con gran volumen de información.
- Análisis de línea de tiempo: muestra los eventos del sistema mediante una interfaz gráfica que facilita la identificación de actividad en disco.
- Búsqueda de palabras clave: permite la búsqueda mediante términos específicos, indexación e incluso patrones de expresiones regulares.
- Artefactos web: recolecta actividad web de los navegadores y permite identificar la actividad de cada usuario.
- Análisis del registro: utiliza RegRipper para identificar los documentos y dispositivos USB a los que se accedió recientemente.

- Análisis de archivos LNK: identifica accesos directos y documentos accedidos recientemente.
- Análisis de correo electrónico: soporta el formato MBOX, como por ejemplo Thunderbird.
- EXIF: permite extraer la ubicación geográfica e información de la cámara mediante archivos JPEG.
- Clasificación de tipo de archivo: permite agrupar los archivos por tipo para separar rápidamente imágenes o documentos.
- Reproducción de medios: videos e imágenes se reproducen en la aplicación sin la necesidad de un visor externo.
- Visor de miniaturas: muestra miniaturas de las imágenes para una visualización rápida.
- Análisis del sistema de archivos robusto: soporte para sistemas de archivo comunes, incluyendo NTFS, FAT12 / FAT16 / FAT32 / ExFAT, HFS +, ISO9660 (CD-ROM), Ext2 / Ext3 / Ext4, yaffs2 y UFS del kit de detective.
- Filtro de conjunto de hash: permite eliminar los archivos buenos conocidos. Utiliza NSRL y marca archivos maliciosos conocidos. Para ello usa hashsets personalizados en los formatos HashKeeper, md5sum y EnCase.
- Etiquetas: facilita el etiquetado de archivos con nombres arbitrarios, como 'favoritos' o 'sospechosos', y agregar comentarios.
- Extracción de cadenas Unicode: permite extraer cadenas de espacios no asignados y tipos de archivos desconocidos en diferentes idiomas (árabe, chino, japonés, etc.).
- Soporta la detección de tipos de archivo mediante firmas digitales y detección de desajuste de extensión.
- Compatibilidad con Android: extrae datos de SMS, registros de llamadas, contactos, diccionario y más.

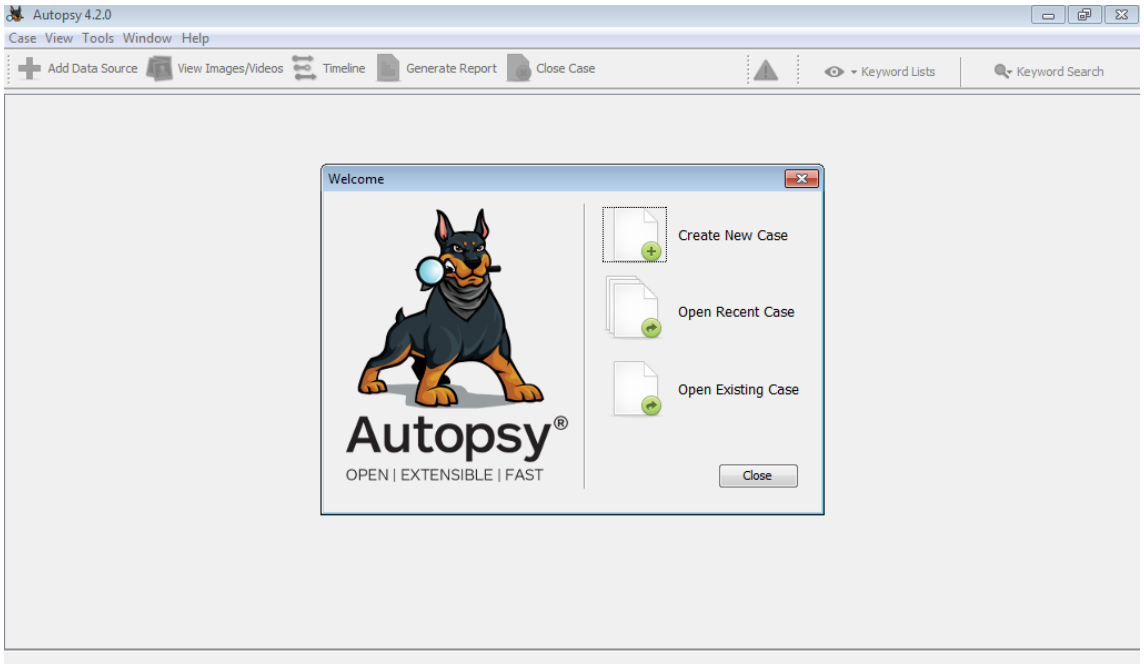

Ilustración 31: Herramienta forense Autopsy.

6.4.2 Digital Forensics Framework (DFF)

Framework forense empleado por investigadores forenses corporativos, examinadores encargados de hacer cumplir la ley, estudiantes forenses digitales y profesionales de la seguridad en todo el mundo. Escrito en Python y C ++. DFF combina una interfaz de usuario intuitiva con un diseño modular y multiplataforma. A continuación se enumeran sus principales características:

- Interfaz de usuario: explorador de archivos, marcadores, ventanas acoplables, entorno de desarrollo integrado e intérprete (Python), línea de comando, multilenguaje, administrador de tareas.
- Visores: imágenes, videos, texto, web, estadísticas de sistemas de archivos.
- Análisis de línea de tiempo: vista gráfica, extracción virtual y reducción, filtros de metadatos.
- Visor hexadecimal: compatibilidad con archivos grandes, navegación de página, navegación y visualización de píxeles, búsqueda, etc.
- Volúmenes: particiones, VMDK (VMware).

- Manipulación de ficheros: corte, fusión, extracción, reducción de repuestos.
- Metadatos: EXIF, día y fecha, estructuras de datos, etc.
- Memoria volátil: Windows XP (Volatility).
- Sistemas de archivos: FAT 12/16/32, NTFS, EXTFS 2/3/4.
- Recuperación de datos: algoritmos de sistemas de archivos, tallado de archivos.
- Registro de Windows: reconstrucción y análisis.
- Otro: dispositivos locales, hash (md5, sha *), zip, unxor.

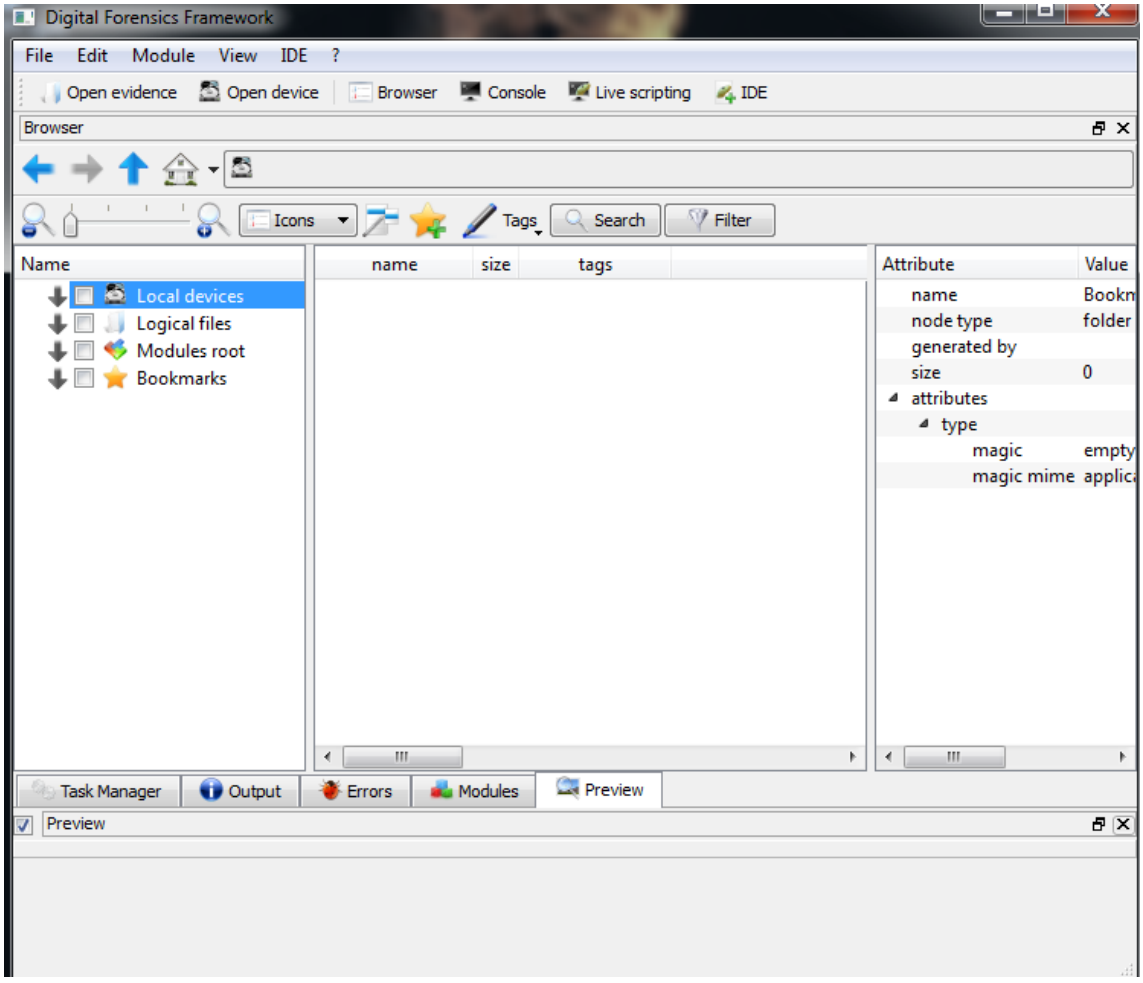

Ilustración 32: Herramienta forense Digital Forensics Framework.

6.4.3 Bulk Extractor

Software forense que extrae funciones tales como direcciones de correo electrónico, números de tarjetas de crédito, URL y otros tipos de información de archivos de pruebas digitales. A continuación, se listan sus principales características:

- Permite el análisis de direcciones de correo electrónico, URL y números de tarjetas de crédito.
- Puede manejar datos comprimidos (como archivos ZIP, PDF y GZIP), así como datos incompletos o parcialmente corruptos, relevar archivos JPEG, documentos de ofimática y otros tipos de archivos a partir de fragmentos de datos comprimidos. Puede detectar y extraer automáticamente archivos RAR encriptados.
- Soporta la creación de listas de palabras basadas en todas las palabras encontradas en los datos, incluso archivos comprimidos que no tienen espacio asignado. Estas listas de palabras se pueden usar para descifrar contraseñas.
- Permite multiproceso para optimizar el tiempo de análisis.
- Después del análisis, crea un histograma con la información relevada.
- Soporta el análisis de imágenes de disco, archivos o directorios de archivos y recolección de información sin analizar el sistema de archivos o la estructura del sistema de archivos.
- Posee un visualizador con funciones de exploración e interfaz gráfica.
- Contiene una suite de programas en Python para análisis adicional.

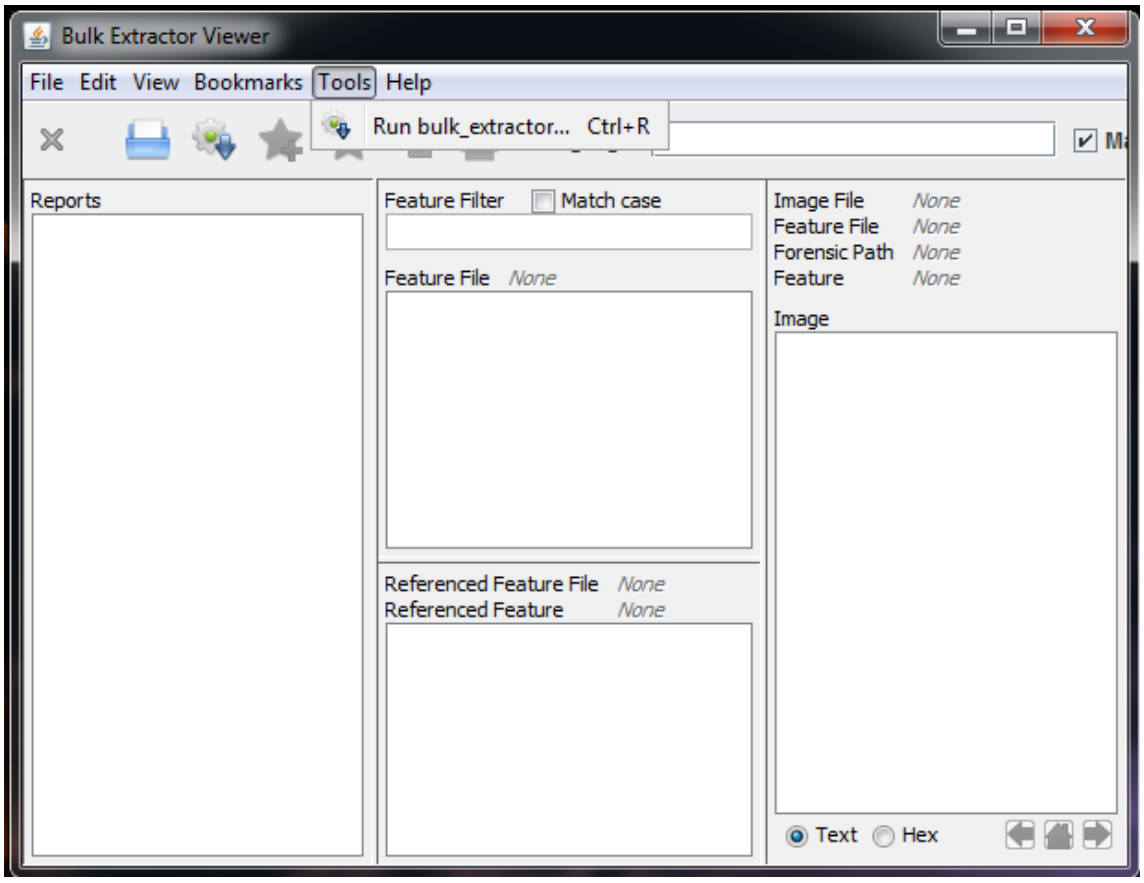

Ilustración 33: Herramienta forense Bulk Extractor.

6.4.4 DEFT

Acrónimo de Digital Evidence and Forensics Toolkit, es una distribución Linux basada en Ubuntu. Desarrollada para el análisis forense digital, con el propósito de analizar sistemas en vivo sin alterar o contaminar los dispositivos de almacenamiento conectados a la PC donde se lleva a cabo el proceso de arranque. Actualmente es utilizado por personal militar, oficiales del gobierno, fuerzas del orden, investigadores forenses corporativos, auditores de TI, universidades, entre otros. Sus principales capacidades se detallan a continuación:

- Multiplataforma: puede ejecutarse en vivo (mediante DVD-R o pendrive USB), instalarse o ejecutarse como un dispositivo virtual en VMware o Virtualbox.
- Soporta herramientas de análisis de ficheros de diferentes tipos.
- Contiene antimalware para búsqueda de rootkits, virus, malware.

- Posee software para la recuperación de ficheros.
- Permite la realización de cálculo de hashes de diferentes formatos: SHA1, SHA256, MD5.
- Contiene aplicaciones para realizar clonados y adquisición de imágenes de discos duros u otros orígenes.
- Permite el análisis forense de dispositivos móviles.

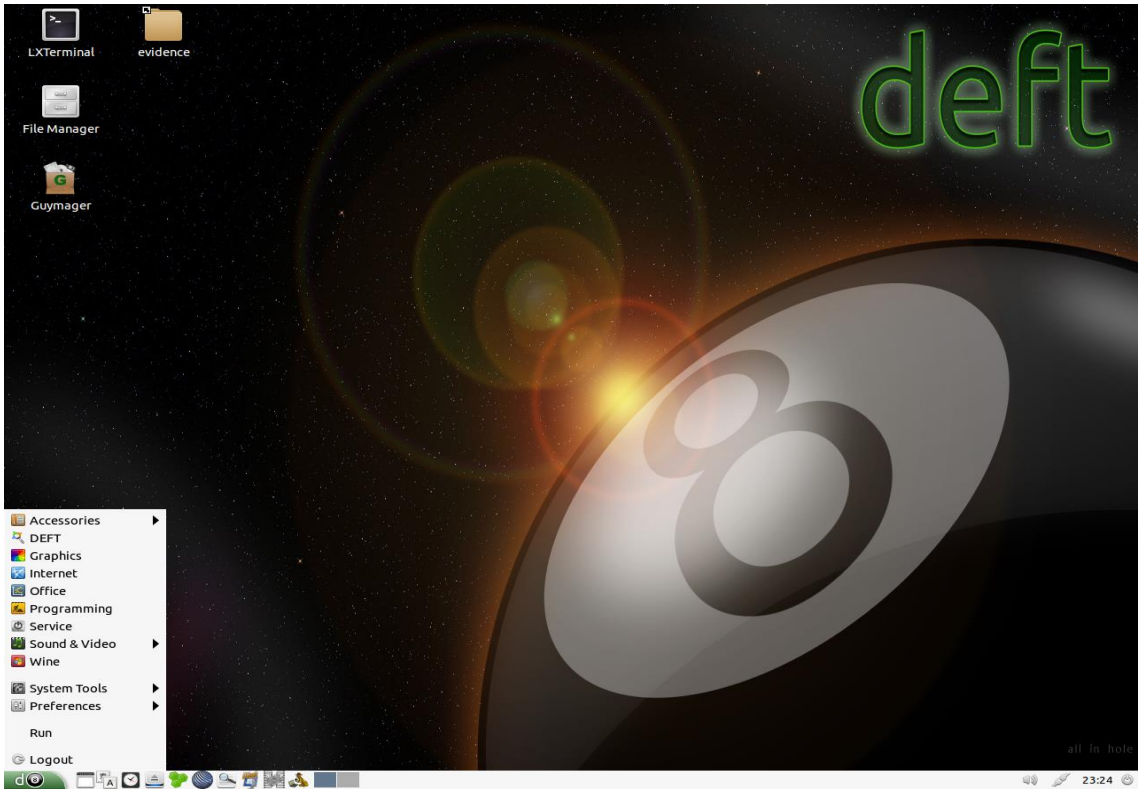

Ilustración 34: Herramienta forense DEFT.

6.4.5 CAINE

Acrónimo de Computer Aided Investigative Environment, es una distribución Linux basada en Ubuntu, desarrollada para el análisis forense digital con el propósito de ofrecer un entorno forense completo y organizado para integrar herramientas y módulos de software. Proporciona una interfaz gráfica amigable. Actualmente es utilizado por personal militar, fuerzas del orden, investigadores forenses corporativos, auditores de TI, entre otros. A continuación se listan sus principales características:

- Multiplataforma: puede ejecutarse en vivo (mediante DVD-R o pendrive USB), instalarse o ejecutarse como un dispositivo virtual en VMware o Virtualbox, tanto en Linux como Windows.
- Permite el apoyo a las investigaciones mediante un entorno que ayuda al investigador en las cuatro fases del cómputo forense.
- Se encuentra provista de una interfaz gráfica amigable.
- Posee un kit de herramientas forenses cuyo empleo no resulta dificultoso.
- Entre tales herramientas se encuentran: Nirsoft suite, WinAudit, MWSnap, Arsenal Image Mounter, FTK Imager, Hex Editor, JpegView, herramientas de red, NTFS Journal viewer, Photorec y TestDisk, QuickHash, NBTempoW, USB Write Protector, VLC, Windows File Analyzer, entre otras.

Ilustración 35: Herramienta forense CAINE.

6.4.6 FTK Imager

Acrónimo de Forensic Toolkit Imager, es un software informático forense desarrollado por AccessData, cuyas principales capacidades se detallan a continuación:

- Multiplataforma: puede ejecutarse en vivo (mediante DVD-R o pendrive USB), instalarse o ejecutarse en el equipo del investigador, tanto en Linux como Windows.
- Permite la adquisición de imágenes forenses de discos físicos, lógicos, archivos de imagen, contenidos de carpetas e incluso unidades ópticas, en diferentes formatos (RAW, SMART, E01, AFF).
- Posee herramientas para volcado de memoria RAM.
- Permite la visualización y navegación por la estructura de directorios.
- Posee herramientas para la visualización en formato hexadecimal, vistas previas de documentos y ANSI latino.
- Permite la búsqueda mediante palabras clave.

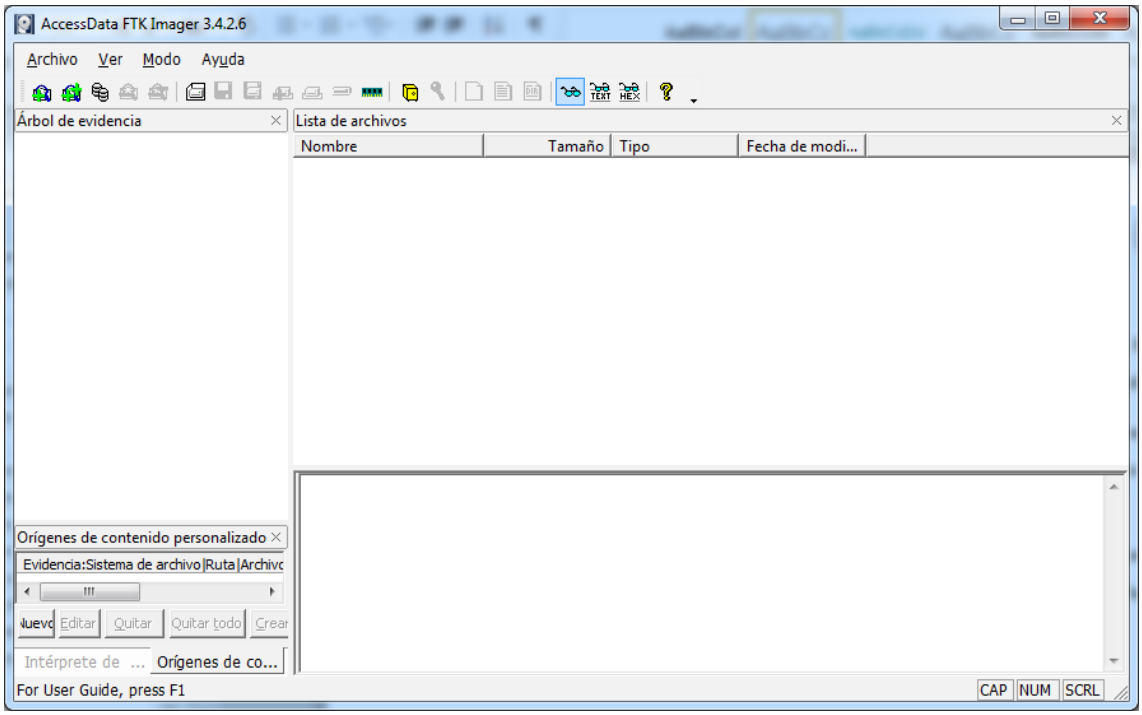

Ilustración 36: Herramienta forense FTK Imager.

6.4.7 EnCase

Respecto de EnCase, resulta oportuno destacar que se trata de uno de los productos líderes en el mercado, en gran parte gracias a las diferentes herramientas que provee y a un poderoso motor de búsqueda, entre sus principales características se encuentran:

- Vista de los datos en línea de tiempo.
- Soporte para múltiples sistemas de archivos para el trabajo con evidencia digital.
- Motor de búsqueda y relacionamiento de datos propio.
- Soporte para múltiples arreglos de discos dinámicos y recuperación de archivos de sistemas de archivos ext 2/3,
- Trabajo sobre teléfonos inteligentes y tabletas de forma integrada, al igual que sobre discos rígidos así como memorias y/o dispositivos extraíbles y portables.
- Generar base de datos de hash y búsqueda por palabras clave.
- Integración con otros softwares de análisis forense.
- Recolección de evidencia de forma remota, permitiendo la conexión a equipos y la extracción de evidencia digital a nivel de unidades de almacenamiento como de memoria.
- Posee dos métodos de búsqueda, indexado y palabras clave.
- Permite recuperar particiones reconstruyendo la estructura de volúmenes.
- Soporta el análisis del historial navegador web, artefactos de internet.
- Es compatible con diferentes formatos de correo electrónico (Pst/Ost de Outlook, Dbx de Outlook Express, Edb de Microsoft Exchange, Lotus Notes Versión 6.0.3, 6.5.4 y 7, Pfc de AOL 6.0, 7.0, 8.0 y 9.0, Yahoo, Hotmail, Netscape mail, archivos Mbox).
- Interpreta y analiza formatos de imágenes de VMware, Microsoft Virtual PC, DD y Safeback Versión 2.

- Permite realizar reportes en Html o texto enriquecido.

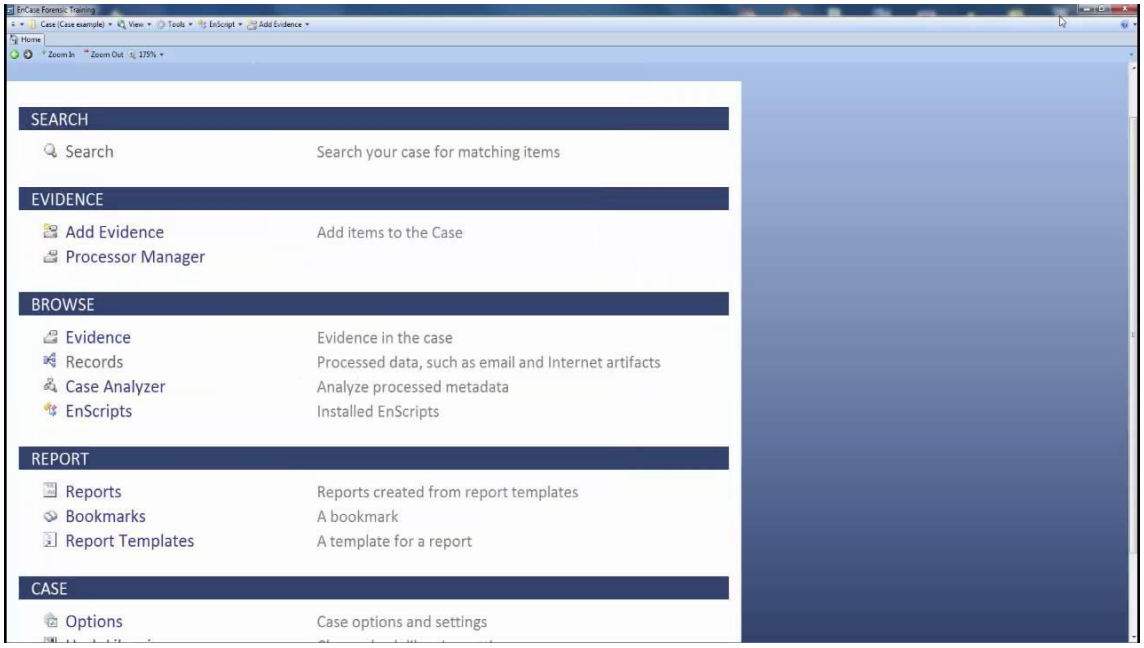

Ilustración 37: Herramienta forense EnCase.

6.4.8 Magnet AXIOM

Magnet AXIOM es considerada como una plataforma de investigación digital bastante completa, permitiendo investigadores forenses adquirir y analizar evidencias forenses de forma transparente, dentro de sus capacidades se pueden señalar:

- Vista de los datos en línea de tiempo.
- Compatible con equipos de computación Windows y Mac, al igual que teléfonos celulares y dispositivos tipo Tablets del mercado.
- Obtención y análisis forense de artefactos de internet, espacio asignado y no asignado, tales como redes sociales y sus aplicaciones, Webmail, aplicaciones de chat, servicios de almacenamiento en la nube y actividad de navegadores de internet.
- Imágenes y videos con metadatos exif.
- Copias de respaldo de dispositivos móviles.

- Búsqueda de palabras clave.
- Aplicar filtros, generar marcadores y crear notas.
- Visualizar línea de tiempo.
- Visualizar ubicaciones en mapa.

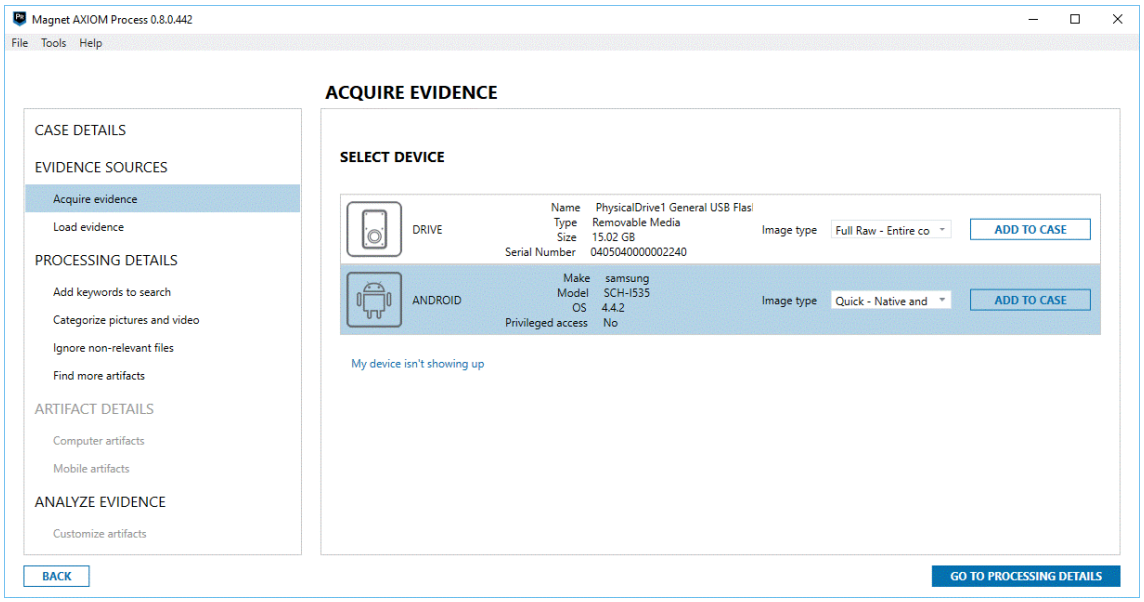

Ilustración 38: Herramienta forense Magnet AXIOM.

6.4.9 UFED 4 PC

Respecto de UFED 4 PC, cabe destacar que es un producto de análisis forense de dispositivos móviles con gran renombre en el mercado, en gran parte gracias a las prestaciones que posee, entre las que se encuentran:

- Compatibilidad con gran cantidad de teléfonos celulares y dispositivos móviles del mercado con sistemas operativos Symbian, Microsoft Mobile, BlackBerry, Palm y Apple iPhone.
- Uso para la extracción en tiempo real de información y datos procesables de teléfonos celulares, teléfonos y dispositivos inteligentes, dispositivos de posicionamiento global (gps).

- Capacidad para recolectar información sobre agenda de contactos, registro de llamadas (marcadas, recibidas y perdidas), imágenes, audios, videos, calendario, correo electrónico, mensajes de texto, aplicaciones de mensajería y chat, archivos multimedia, etiquetas geográficas, información de ubicación (WiFi, celda y aplicaciones de navegación), posiciones GPS, audio.
- Relevar información el dispositivo tal como marca, modelo, IMEI, ESN.
- Colectar sistemas de archivos completos (volcado de memoria).
- Extracción de contraseñas de usuarios y de archivos.
- Exportar la información y presentarla mediante informes claros y concisos.

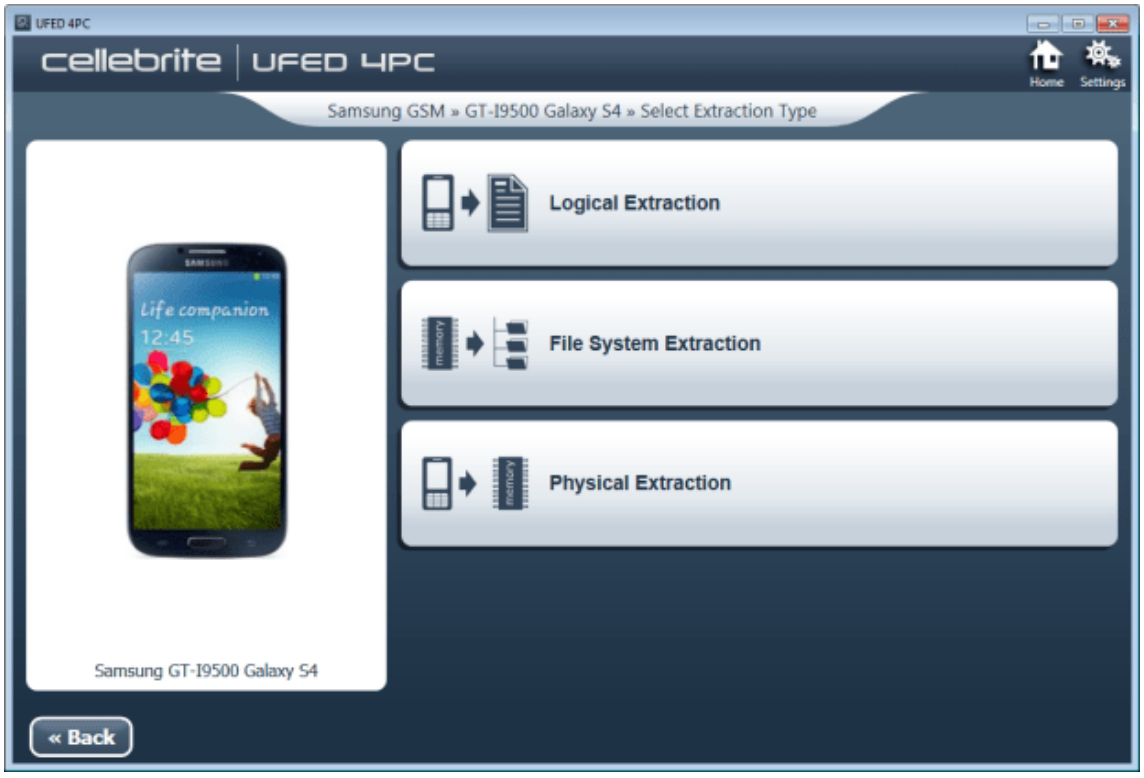

Ilustración 39: Herramienta forense UFED 4 PC.

6.4.10 Oxygen Forensic

Respecto de Oxygen Forensic, esta herramienta se trata de uno de los productos líderes en el mercado respecto de análisis forense para dispositivos móviles,

en gran parte gracias a la cantidad de dispositivos que soporta, incluyendo unidades GPS y Drones, como así también las múltiples herramientas que provee, entre las que podemos destacar:

- Compatibilidad con gran cantidad de teléfonos celulares y dispositivos móviles del mercado con sistemas operativos Symbian, Microsoft Mobile, BlackBerry, Palm y Apple iPhone.
- Uso para la extracción en tiempo real de información y datos procesables de teléfonos celulares, teléfonos y dispositivos inteligentes, dispositivos de posicionamiento global (gps).
- Capacidad para recolectar información sobre agenda de contactos, registro de llamadas (marcadas, recibidas y perdidas), imágenes, audios, videos, calendario, correo electrónico, mensajes de texto, aplicaciones de mensajería y chat, archivos multimedia, etiquetas geográficas, información de ubicación (WiFi, celda y aplicaciones de navegación), posiciones GPS, audio.
- Relevar información el dispositivo tal como marca, modelo, IMEI, ESN.
- Colectar sistemas de archivos completos (volcado de memoria).
- Realizar extracción de información almacenada de diferentes fuentes en la nube.
- Extracción de contraseñas de usuarios y de archivos.
- Posicionamiento geográfico de eventos.
- Línea de tiempo.
- Estadísticas de comunicación.
- Marcar evidencias clave.
- Grafo de análisis de actividades.
- Exportar la información y presentarla mediante informes claros y concisos.

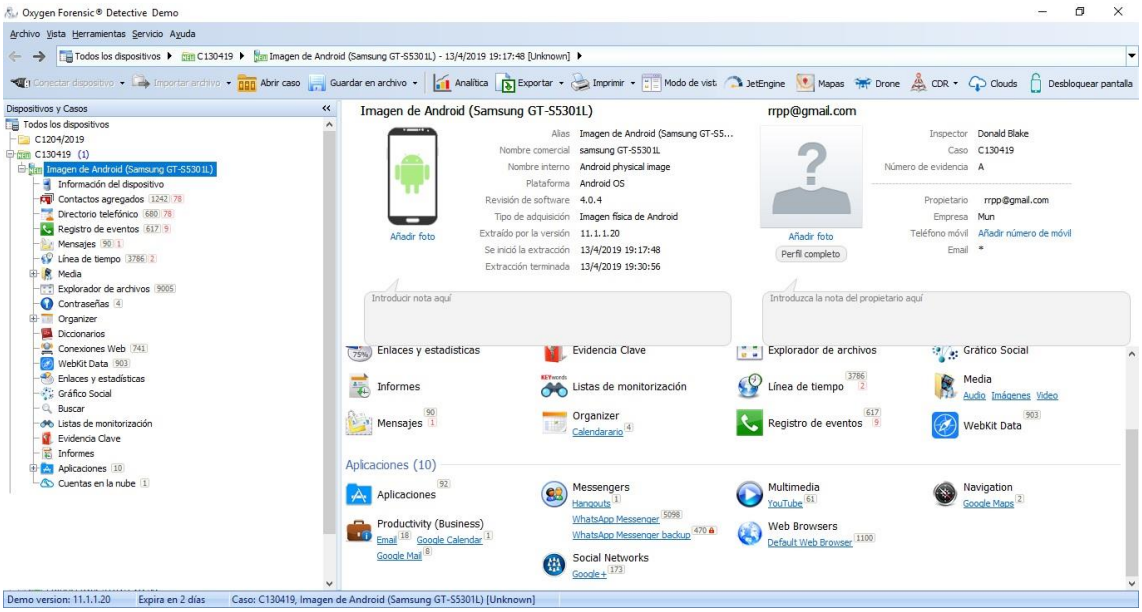

Ilustración 40: Herramienta forense Oxygen Forensic.

[Página dejada en blanco intencionalmente]

6.5 Firmas de archivo

A continuación se listan las firmas de archivo [43] con sus encabezados hexadecimales y descripciones correspondientes.

EXTENSIÓN	FIRMA	DESCRIPCIÓN
*	41 43 53 44	AOL parameter|info files
*	62 70 6C 69 73 74	Binary property list (plist)
*	00 14 00 00 01 02	BIOS details in RAM
*	30 37 30 37 30	cpio archive
*	7F 45 4C 46	ELF executable
*	A1 B2 CD 34	Extended tcpdump (libpcap) capture file
*	04 00 00 00	INFO2 Windows recycle bin_1
*	05 00 00 00	INFO2 Windows recycle bin_2
*	AC ED	Java serialization data
*	4B 57 41 4A 88 F0 27 D1	KWAJ (compressed) file
*	CD 20 AA AA 02 00 00 00	NAV quarantined virus file
*	53 5A 20 88 F0 27 33 D1	QBASIC SZDD file
*	6F 3C	SMS text (SIM)
*	53 5A 44 44 88 F0 27 33	SZDD file format
*	A1 B2 C3 D4	tcpdump (libpcap) capture file
*	34 CD B2 A1	Tcpdump capture file
*	EF BB BF	UTF8 file
*	FE FF	UTF-16|UCS-2 file
*	FF FE 00 00	UTF-32|UCS-4 file
*	62 65 67 69 6E	UUencoded file
*	D4 C3 B2 A1	WinDump (winpcap) capture file

EXTENSIÓN	FIRMA	DESCRIPCIÓN
*	37 E4 53 96 C9 DB D6 07	zisofs compressed file
123	00 00 1A 00 05 10 04	Lotus 1-2-3 (v9)
386	4D 5A	Windows virtual device drivers
3GP	00 00 00 14 66 74 79 70	3GPP multimedia files
3GP	00 00 00 20 66 74 79 70	3GPP2 multimedia files
3GP5	00 00 00 18 66 74 79 70	MPEG-4 video files
4XM	52 49 46 46	4X Movie video
7Z	37 7A BC AF 27 1C	7-Zip compressed file
ABA	00 01 42 41	Palm Address Book Archive
ABD	51 57 20 56 65 72 2E 20	ABD | QSD Quicken data file
ABI	41 4F 4C 49 4E 44 45 58	AOL address book index
ABI	41 4F 4C	AOL config files
ABY	41 4F 4C 44 42	AOL address book
ABY	41 4F 4C	AOL config files
AC	72 69 66 66	Sonic Foundry Acid Music File
ACCDB	00 01 00 00 53 74 61 6E 64 61 72 64 20 41 43 45 20 44 42	Microsoft Access 2007
ACM	4D 5A	MS audio compression manager driver
ACS	C3 AB CD AB	MS Agent Character file
AC_	D0 CF 11 E0 A1 B1 1A E1	CaseWare Working Papers
AD	52 45 56 4E 55 4D 3A 2C	Antenna data file
ADF	44 4F 53	Amiga disk file
ADP	D0 CF 11 E0 A1 B1 1A E1	Access project file
ADX	03 00 00 00 41 50 50 52	Approach index file
ADX	80 00 00 20 03 12 04	Dreamcast audio
AIFF	46 4F 52 4D 00	Audio Interchange File

EXTENSIÓN	FIRMA	DESCRIPCIÓN
AIN	21 12	AIN Compressed Archive
AMR	23 21 41 4D 52	Adaptive Multi-Rate ACELP Codec (GSM)
ANI	52 49 46 46	Windows animated cursor
API	4D 5A 90 00 03 00 00 00	Acrobat plug-in
APR	D0 CF 11 E0 A1 B1 1A E1	Lotus|IBM Approach 97 file
ARC	41 72 43 01	FreeArc compressed file
ARC	1A 02	LH archive (old vers.|type 1)
ARC	1A 03	LH archive (old vers.|type 2)
ARC	1A 04	LH archive (old vers.|type 3)
ARC	1A 08	LH archive (old vers.|type 4)
ARC	1A 09	LH archive (old vers.|type 5)
ARJ	60 EA	ARJ Compressed archive file
ARL	D4 2A	AOL history|typed URL files
ASF	30 26 B2 75 8E 66 CF 11	Windows Media Audio|Video File
AST	53 43 48 6C	Underground Audio
ASX	3C	Advanced Stream Redirector
AU	64 6E 73 2E	Audacity audio file
AU	2E 73 6E 64	NeXT|Sun Microsystems audio file
AUT	D4 2A	AOL history|typed URL files
AVI	52 49 46 46	Resource Interchange File Format
AW	8A 01 09 00 00 00 E1 08	MS Answer Wizard
AX	4D 5A 90 00 03 00 00 00	DirectShow filter
AX	4D 5A	Library cache file
BAG	41 4F 4C 20 46 65 65 64	AOL and AIM buddy list
BAG	41 4F 4C	AOL config files

EXTENSIÓN	FIRMA	DESCRIPCIÓN
BDR	58 54	MS Publisher
BIN	42 4C 49 32 32 33 51	Speedtouch router firmware
BMP	42 4D	Bitmap image
BZ2	42 5A 68	bzip2 compressed archive
CAB	49 53 63 28	Install Shield compressed file
CAB	4D 53 43 46	Microsoft cabinet file
CAL	73 72 63 64 6F 63 69 64	CALS raster bitmap
CAL	53 75 70 65 72 43 61 6C	SuperCalc worksheet
CAL	B5 A2 B0 B3 B3 B0 A5 B5	Windows calendar
CAP	58 43 50 00	Packet sniffer files
CAP	52 54 53 53	WinNT Netmon capture file
CAS	5F 43 41 53 45 5F	EnCase case file
CAT	30	MS security catalog file
CBD	43 42 46 49 4C 45	WordPerfect dictionary
CBK	5F 43 41 53 45 5F	EnCase case file
CDA	52 49 46 46	Resource Interchange File Format
CDR	52 49 46 46	CorelDraw document
CDR	45 4C 49 54 45 20 43 6F	Elite Plus Commander game file
CDR	4D 53 5F 56 4F 49 43 45	Sony Compressed Voice File
CFG	5B 66 6C 74 73 69 6D 2E	Flight Simulator Aircraft Configuration
CHI	49 54 53 46	MS Compiled HTML Help File
CHM	49 54 53 46	MS Compiled HTML Help File
CLASS	CA FE BA BE	Java bytecode
CLB	43 4F 4D 2B	COM+ Catalog
CLB	43 4D 58 31	Corel Binary metafile

EXTENSIÓN	FIRMA	DESCRIPCIÓN
CMX	52 49 46 46	Corel Presentation Exchange metadata
CNV	53 51 4C 4F 43 4F 4E 56	DB2 conversion file
COD	4E 61 6D 65 3A 20	Agent newsreader character map
COM	4D 5A	Windows|DOS executable file
COM	E8	Windows executable file_1
COM	E9	Windows executable file_2
COM	EB	Windows executable file_3
CPE	46 41 58 43 4F 56 45 52	MS Fax Cover Sheet
CPI	53 49 45 54 52 4F 4E 49	Sietronics CPI XRD document
CPI	FF 46 4F 4E 54	Windows international code page
CPL	4D 5A	Control panel application
CPL	DC DC	Corel color palette
CPT	43 50 54 37 46 49 4C 45	Corel Photopaint file_1
CPT	43 50 54 46 49 4C 45	Corel Photopaint file_2
CPX	5B 57 69 6E 64 6F 77 73	Microsoft Code Page Translation file
CRU	43 52 55 53 48 20 76	Crush compressed archive
CRW	49 49 1A 00 00 00 48 45	Canon RAW file
CSH	63 75 73 68 00 00 00 02	Photoshop Custom Shape
CTF	43 61 74 61 6C 6F 67 20	WhereIsIt Catalog
CTL	56 45 52 53 49 4F 4E 20	Visual Basic User-defined Control file
CUIX	50 4B 03 04	Customization files
CUR	00 00 02 00	Windows cursor
DAT	52 49 46 46	Video CD MPEG movie
DAT	A9 0D 00 00 00 00 00 00	Access Data FTK evidence
DAT	73 6C 68 21	Allegro Generic Packfile (compressed)

EXTENSIÓN	FIRMA	DESCRIPCIÓN
DAT	73 6C 68 2E	Allegro Generic Packfile (uncompressed)
DAT	41 56 47 36 5F 49 6E 74	AVG6 Integrity database
DAT	03	MapInfo Native Data Format
DAT	45 52 46 53 53 41 56 45	EasyRecovery Saved State file
DAT	43 6C 69 65 6E 74 20 55	IE History file
DAT	49 6E 6E 6F 20 53 65 74	Inno Setup Uninstall Log
DAT	50 4E 43 49 55 4E 44 4F	Norton Disk Doctor undo file
DAT	50 45 53 54	PestPatrol data|scan strings
DAT	1A 52 54 53 20 43 4F 4D	Runtime Software disk image
DAT	52 41 5A 41 54 44 42 31	Shareaza (P2P) thumbnail
DAT	4E 41 56 54 52 41 46 46	TomTom traffic data
DAT	55 46 4F 4F 72 62 69 74	UFO Capture map file
DAT	57 4D 4D 50	Walkman MP3 file
DAT	43 52 45 47	Win9x registry hive
DAT	72 65 67 66	WinNT registry file
DB	D0 CF 11 E0 A1 B1 1A E1	MSWorks database file
DB	08	dBASE IV or dBFast configuration file
DB	00 06 15 61 00 00 00 02 00 00 04 D2 00 00 10 00	Netscape Navigator (v4) database
DB	44 42 46 48	Palm Zire photo database
DB	53 51 4C 69 74 65 20 66 6F 72 6D 61 74 20 33 00	SQLite database file
DB	FD FF FF FF	Thumbs.db subheader
DB3	03	dBASE III file
DB4	04	dBASE IV file
DBA	00 01 42 44	Palm DateBook Archive
DBB	6C 33 33 6C	Skype user data file

EXTENSIÓN	FIRMA	DESCRIPCIÓN
DBF	4F 50 4C 44 61 74 61 62	Psion Series 3 Database
DBX	CF AD 12 FE	Outlook Express e-mail folder
DCI	3C 21 64 6F 63 74 79 70	AOL HTML mail
DCX	B1 68 DE 3A	PCX bitmap
dex	64 65 78 0A 30 30 39 00	Dalvik (Android) executable file
DIB	42 4D	Bitmap image
DLL	4D 5A	Windows|DOS executable file
DMG	78	MacOS X image file
DMP	4D 44 4D 50 93 A7	Windows dump file
DMP	50 41 47 45 44 55	Windows memory dump
DMS	44 4D 53 21	Amiga DiskMasher compressed archive
DOC	D0 CF 11 E0 A1 B1 1A E1	Microsoft Office document
DOC	0D 44 4F 43	DeskMate Document
DOC	CF 11 E0 A1 B1 1A E1 00	Perfect Office document
DOC	DB A5 2D 00	Word 2.0 file
DOC	EC A5 C1 00	Word document subheader
DOCX	50 4B 03 04	MS Office Open XML Format Document
DOCX	50 4B 03 04 14 00 06 00	MS Office 2007 documents
DOT	D0 CF 11 E0 A1 B1 1A E1	Microsoft Office document
DRV	4D 5A	Windows|DOS executable file
DRW	07	Generic drawing programs
DRW	01 FF 02 04 03 02	Micrografx vector graphic file
DS4	52 49 46 46	Micrografx Designer graphic
DSN	4D 56	CD Stomper Pro label file
DSP	23 20 4D 69 63 72 6F 73	MS Developer Studio project file

EXTENSIÓN	FIRMA	DESCRIPCIÓN
DSS	02 64 73 73	Digital Speech Standard file
DSW	64 73 77 66 69 6C 65	MS Visual Studio workspace file
DTD	07 64 74 32 64 64 74 64	DesignTools 2D Design file
DUN	5B 50 68 6F 6E 65 5D	Dial-up networking file
DVF	4D 53 5F 56 4F 49 43 45	Sony Compressed Voice File
DVR	44 56 44	DVR-Studio stream file
DW4	4F 7B	Visio|DisplayWrite 4 text file
DWG	41 43 31 30	Generic AutoCAD drawing
E01	45 56 46 09 0D 0A FF 00	Expert Witness Compression Format
E01	4C 56 46 09 0D 0A FF 00	Logical File Evidence Format
ECF	5B 47 65 6E 65 72 61 6C	MS Exchange configuration file
EFX	DC FE	eFax file
EML	58 2D	Exchange e-mail
EML	52 65 74 75 72 6E 2D 50	Generic e-mail_1
EML	46 72 6F 6D	Generic e-mail_2
ENL	40 40 40 20 00 00 40 40 40 40	EndNote Library File
EPS	C5 D0 D3 C6	Adobe encapsulated PostScript
EPS	25 21 50 53 2D 41 64 6F	Encapsulated PostScript file
ETH	1A 35 01 00	WinPharoah capture file
EVT	30 00 00 00 4C 66 4C 65	Windows Event Viewer file
EVTX	45 6C 66 46 69 6C 65 00	Windows Vista event log
EXE	4D 5A	Windows|DOS executable file
FDF	25 50 44 46	PDF file
FLAC	66 4C 61 43 00 00 00 22	Free Lossless Audio Codec file
FLI	00 11	FLIC animation

EXTENSIÓN	FIRMA	DESCRIPCIÓN
FLT	4D 5A 90 00 03 00 00 00	Audition graphic filter
FLT	76 32 30 30 33 2E 31 30	Qimage filter
FLV	46 4C 56	Flash video file
FM	3C 4D 61 6B 65 72 46 69	Adobe FrameMaker
FON	4D 5A	Font file
FTR	D2 0A 00 00	WinPharoah filter file
GHO	FE EF	Symantex Ghost image file
GHS	FE EF	Symantex Ghost image file
GID	3F 5F 03 00	Windows Help file_2
GID	4C 4E 02 00	Windows help file_3
GIF	47 49 46 38	GIF file
GPG	99	GPG public keyring
GRP	50 4D 43 43	Windows Program Manager group file
GX2	47 58 32	Show Partner graphics file
GZ	1F 8B 08	GZIP archive file
HAP	91 33 48 46	Hamarsoft compressed archive
HDMP	4D 44 4D 50 93 A7	Windows dump file
HDR	49 53 63 28	Install Shield compressed file
HDR	23 3F 52 41 44 49 41 4E	Radiance High Dynamic Range image file
hip	48 69 50 21	Houdini image file. Three-dimensional modeling and animation
HLP	00 00 FF FF FF FF	Windows Help file_1
HLP	3F 5F 03 00	Windows Help file_2
HLP	4C 4E 02 00	Windows help file_3
HQX	28 54 68 69 73 20 66 69	BinHex 4 Compressed Archive

EXTENSIÓN	FIRMA	DESCRIPCIÓN
ICO	00 00 01 00	Windows icon|printer spool file
IDX	41 4F 4C 44 42	AOL user configuration
IDX	41 4F 4C	AOL config files
IDX	50 00 00 00 20 00 00 00	Quicken QuickFinder Information File
IFO	44 56 44	DVD info file
IMG	50 49 43 54 00 08	ChromaGraph Graphics Card Bitmap
IMG	EB 3C 90 2A	GEM Raster file
IMG	53 43 4D 49	Img Software Bitmap
IND	41 4F 4C 49 44 58	AOL client preferences|settings file
IND	41 4F 4C	AOL config files
INFO	E3 10 00 01 00 00 00 00	Amiga icon
INFO	54 68 69 73 20 69 73 20	GNU Info Reader file
INFO	7A 62 65 78	ZoomBrowser Image Index
ISO	43 44 30 30 31	ISO-9660 CD Disc Image
IVR	2E 52 45 43	RealPlayer video file (V11+)
JAR	50 4B 03 04	Java archive_1
JAR	5F 27 A8 89	Jar archive
JAR	4A 41 52 43 53 00	JARCS compressed archive
JAR	50 4B 03 04 14 00 08 00	Java archive_2
JFIF	FF D8 FF E0	JPEG IMAGE
JFIF	FF D8 FF E0	JFIF IMAGE FILE - jpeg
JG	4A 47 03 0E	AOL ART file_1
JG	4A 47 04 0E	AOL ART file_2
JNT	4E 42 2A 00	MS Windows journal
JP2	00 00 00 0C 6A 50 20 20	JPEG2000 image files

EXTENSIÓN	FIRMA	DESCRIPCIÓN
JPE	FF D8 FF E0	JPEG IMAGE
JPE	FF D8 FF E0	JPE IMAGE FILE - jpeg
JPEG	FF D8 FF E0	JPEG IMAGE
JPEG	FF D8 FF E2	CANNON EOS JPEG FILE
JPEG	FF D8 FF E3	SAMSUNG D500 JPEG FILE
JPG	FF D8 FF E0	JPEG IMAGE
JPG	FF D8 FF E1	Digital camera JPG using Exchangeable Image File Format (EXIF)
JPG	FF D8 FF E8	Still Picture InterchangeFile Format (SPIFF)
JTP	4E 42 2A 00	MS Windows journal
KGB	4B 47 42 5F 61 72 63 68	KGB archive
KOZ	49 44 33 03 00 00 00	Sprint Music Store audio
KWD	50 4B 03 04	KWord document
LBK	C8 00 79 00	Jeppesen FliteLog file
LGC	7B 0D 0A 6F 20	Windows application log
LGD	7B 0D 0A 6F 20	Windows application log
LHA	2D 6C 68	Compressed archive
LIB	21 3C 61 72 63 68 3E 0A	Unix archiver (ar)|MS Program Library Common Object File Format (COFF)
LIT	49 54 4F 4C 49 54 4C 53	MS Reader eBook
LNK	4C 00 00 00 01 14 02 00	Windows shortcut file
LOG	2A 2A 2A 20 20 49 6E 73	Symantec Wise Installer log
LWP	57 6F 72 64 50 72 6F	Lotus WordPro file
LZH	2D 6C 68	Compressed archive
M4A	00 00 00 20 66 74 79 70 4D 34 41	Apple audio and video files
MANIFEST	3C 3F 78 6D 6C 20 76 65 72 73 69 6F 6E 3D	Windows Visual Stylesheet

EXTENSIÓN	FIRMA	DESCRIPCIÓN
MAR	4D 41 72 30 00	MAr compressed archive
MAR	4D 41 52 43	Microsoft|MSN MARC archive
MAR	4D 41 52 31 00	Mozilla archive
MDB	00 01 00 00 53 74 61 6E 64 61 72 64 20 4A 65 74 20 44 42	Microsoft Access
MDF	01 0F 00 00	SQL Data Base
MDI	45 50	MS Document Imaging file
MID	4D 54 68 64	MIDI sound file
MIDI	4D 54 68 64	MIDI sound file
MIF	3C 4D 61 6B 65 72 46 69	Adobe FrameMaker
MIF	56 65 72 73 69 6F 6E 20	MapInfo Interchange Format file
MKV	1A 45 DF A3 93 42 82 88	Matroska stream file
MLS	4D 49 4C 45 53	Milestones project management file
MLS	4D 56 32 31 34	Milestones project management file_1
MLS	4D 56 32 43	Milestones project management file_2
MLS	4D 4C 53 57	Skype localization data file
MMF	4D 4D 4D 44 00 00	Yamaha Synthetic music Mobile Application Format
MNY	00 01 00 00 4D 53 49 53 41 4D 20 44 61 74 61 62 61 73 65	Microsoft Money file
MOF	FF FE 23 00 6C 00 69 00	MSinfo file
MOV	6D 6F 6F 76	QuickTime movie_1
MOV	66 72 65 65	QuickTime movie_2
MOV	6D 64 61 74	QuickTime movie_3
MOV	77 69 64 65	QuickTime movie_4
MOV	70 6E 6F 74	QuickTime movie_5
MOV	73 6B 69 70	QuickTime movie_6

EXTENSIÓN	FIRMA	DESCRIPCIÓN
MP	0C ED	Monochrome Picture TIFF bitmap
MP3	49 44 33	MP3 audio file
MPG	00 00 01 BA	DVD video file
MPG	00 00 01 B3	MPEG video file
MSC	D0 CF 11 E0 A1 B1 1A E1	Microsoft Common Console Document
MSC	3C 3F 78 6D 6C 20 76 65 72 73 69 6F 6E 3D 22 31 2E 30 22 3F 3E 0D 0A 3C 4D 4D 43 5F 43 6F 6E 73 6F 6C 65 46 69 6C 65 20 43 6F 6E 73 6F 6C 65 56 65 72	MMC Snap-in Control file
MSI	D0 CF 11 E0 A1 B1 1A E1	Microsoft Installer package
MSI	23 20	Cerius2 file
MSV	4D 53 5F 56 4F 49 43 45	Sony Compressed Voice File
MTW	D0 CF 11 E0 A1 B1 1A E1	Minitab data file
NRI	0E 4E 65 72 6F 49 53 4F	Nero CD compilation
NSF	1A 00 00 04 00 00	Lotus Notes database
NSF	4E 45 53 4D 1A 01	NES Sound file
NTF	1A 00 00	Lotus Notes database template
NTF	4E 49 54 46 30	National Imagery Transmission Format file
NTF	30 31 4F 52 44 4E 41 4E	National Transfer Format Map
NVRAM	4D 52 56 4E	VMware BIOS state file
OBJ	4C 01	MS COFF relocatable object code
OBJ	80	Relocatable object code
OCX	4D 5A	ActiveX|OLE Custom Control
ODP	50 4B 03 04	OpenDocument template
ODT	50 4B 03 04	OpenDocument template
OGA	4F 67 67 53 00 02 00 00	Ogg Vorbis Codec compressed file
OGG	4F 67 67 53 00 02 00 00	Ogg Vorbis Codec compressed file

EXTENSIÓN	FIRMA	DESCRIPCIÓN
OGV	4F 67 67 53 00 02 00 00	Ogg Vorbis Codec compressed file
OGX	4F 67 67 53 00 02 00 00	Ogg Vorbis Codec compressed file
OLB	4D 5A	OLE object library
ONE	E4 52 5C 7B 8C D8 A7 4D	MS OneNote note
OPT	D0 CF 11 E0 A1 B1 1A E1	Developer Studio File Options file
OPT	FD FF FF FF 20	Developer Studio subheader
ORG	41 4F 4C 56 4D 31 30 30	AOL personal file cabinet
OTT	50 4B 03 04	OpenDocument template
P10	64 00 00 00	Intel PROset|Wireless Profile
PAK	1A 0B	PAK Compressed archive file
PAK	50 41 43 4B	Quake archive file
PAT	47 50 41 54	GIMP pattern file
PAX	50 41 58	PAX password protected bitmap
PCH	56 43 50 43 48 30	Visual C PreCompiled header
PCX	0A 05 01 01	ZSOFT Paintbrush file_3
PCX	0A 03 01 01	ZSOFT Paintbrush file_2
PCX	0A 02 01 01	ZSOFT Paintbrush file_1
PDB	4D 69 63 72 6F 73 6F 66 74 20 43 2F 43 2B 2B 20	MS C++ debugging symbols file
PDB	4D 2D 57 20 50 6F 63 6B	Merriam-Webster Pocket Dictionary
PDB	AC ED 00 05 73 72 00 12	BGBlitz position database file
PDB	73 7A 65 7A	PowerBASIC Debugger Symbols
PDB	73 6D 5F	PalmOS SuperMemo
PDF	25 50 44 46	PDF file
PF	11 00 00 00 53 43 43 41	Windows prefetch file
PFC	41 4F 4C	AOL config files

EXTENSIÓN	FIRMA	DESCRIPCIÓN
PFC	41 4F 4C 56 4D 31 30 30	AOL personal file cabinet
PGD	50 47 50 64 4D 41 49 4E	PGP disk image
PGM	50 35 0A	Portable Graymap Graphic
PIF	4D 5A	Windows|DOS executable file
PKR	99 01	PGP public keyring
PNG	89 50 4E 47 0D 0A 1A 0A	PNG image
PPS	D0 CF 11 E0 A1 B1 1A E1	Microsoft Office document
PPT	FD FF FF FF 43 00 00 00	PowerPoint presentation subheader_6
PPT	FD FF FF FF 1C 00 00 00	PowerPoint presentation subheader_5
PPT	D0 CF 11 E0 A1 B1 1A E1	Microsoft Office document
PPT	FD FF FF FF 0E 00 00 00	PowerPoint presentation subheader_4
PPT	A0 46 1D F0	PowerPoint presentation subheader_3
PPT	0F 00 E8 03	PowerPoint presentation subheader_2
PPT	00 6E 1E F0	PowerPoint presentation subheader_1
PPTX	50 4B 03 04	MS Office Open XML Format Document
PPTX	50 4B 03 04 14 00 06 00	MS Office 2007 documents
PPZ	4D 53 43 46	Powerpoint Packaged Presentation
PRC	74 42 4D 50 4B 6E 57 72	PathWay Map file
PRC	42 4F 4F 4B 4D 4F 42 49	Palmpilot resource file
PSD	38 42 50 53	Photoshop image
PSP	7E 42 4B 00	Corel Paint Shop Pro image
PUB	D0 CF 11 E0 A1 B1 1A E1	MS Publisher file
PWI	7B 5C 70 77 69	MS WinMobile personal note
PWL	E3 82 85 96	Win98 password file

EXTENSIÓN	FIRMA	DESCRIPCIÓN
PWL	B0 4D 46 43	Win95 password file
QBB	45 86 00 00 06 00	QuickBooks backup
QCP	52 49 46 46	Resource Interchange File Format
QDF	AC 9E BD 8F 00 00	QDF Quicken data
QEL	51 45 4C 20	QDL Quicken data
QEMU	51 46 49	Qcow Disk Image
QPH	03 00 00 00	Quicken price history
QSD	51 57 20 56 65 72 2E 20	ABD | QSD Quicken data file
QTS	4D 5A	Windows|DOS executable file
QTX	4D 5A	Windows|DOS executable file
QXD	00 00 4D 4D 58 50 52	Quark Express (Motorola)
QXD	00 00 49 49 58 50 52	Quark Express (Intel)
RA	2E 72 61 FD 00	RealAudio streaming media
RA	2E 52 4D 46 00 00 00 12	RealAudio file
RAM	72 74 73 70 3A 2F 2F	RealMedia metafile
RAR	52 61 72 21 1A 07 00	WinRAR compressed archive
REG	52 45 47 45 44 49 54	WinNT Registry|Registry Undo files
REG	FF FE	Windows Registry file
RGB	01 DA 01 01 00 03	Silicon Graphics RGB Bitmap
RM	2E 52 4D 46	RealMedia streaming media
RMI	52 49 46 46	Resource Interchange File Format
RMVB	2E 52 4D 46	RealMedia streaming media
RPM	ED AB EE DB	RedHat Package Manager
RTD	43 23 2B 44 A4 43 4D A5	RagTime document
RTF	7B 5C 72 74 66 31	RTF file

EXTENSIÓN	FIRMA	DESCRIPCIÓN
RVT	D0 CF 11 E0 A1 B1 1A E1	Revit Project file
SAM	5B 76 65 72 5D	Lotus AMI Pro document_2
SAM	5B 56 45 52 5D	Lotus AMI Pro document_1
SAV	24 46 4C 32 40 28 23 29	SPSS Data file
SCR	4D 5A	Screen saver
SDR	53 4D 41 52 54 44 52 57	SmartDraw Drawing file
SH3	48 48 47 42 31	Harvard Graphics presentation file
SHD	67 49 00 00	Win2000|XP printer spool file
SHD	4B 49 00 00	Win9x printer spool file
SHD	66 49 00 00	WinNT printer spool file
SHD	68 49 00 00	Win Server 2003 printer spool file
SHW	53 48 4F 57	Harvard Graphics presentation
SIT	53 74 75 66 66 49 74 20	StuffIt compressed archive
SIT	53 49 54 21 00	StuffIt archive
SKF	07 53 4B 46	SkinCrafter skin
SKR	95 01	PGP secret keyring_2
SKR	95 00	PGP secret keyring_1
SLE	3A 56 45 52 53 49 4F 4E	Surfplan kite project file
SLE	41 43 76	Steganos virtual secure drive
SLN	4D 69 63 72 6F 73 6F 66 74 20 56 69 73 75 61 6C	Visual Studio .NET file
SNM	00 1E 84 90 00 00 00 00	Netscape Communicator (v4) mail folder
SNP	4D 53 43 46	MS Access Snapshot Viewer file
SOU	D0 CF 11 E0 A1 B1 1A E1	Visual Studio Solution User Options file
SPL	00 00 01 00	Windows icon|printer spool file
SPO	D0 CF 11 E0 A1 B1 1A E1	SPSS output file

EXTENSIÓN	FIRMA	DESCRIPCIÓN
SUD	52 45 47 45 44 49 54	WinNT Registry|Registry Undo files
SUO	FD FF FF FF 04	Visual Studio Solution subheader
SWF	46 57 53	Shockwave Flash player
SWF	43 57 53	Shockwave Flash file
SXC	50 4B 03 04	StarOffice spreadsheet
SXD	50 4B 03 04	OpenOffice documents
SXI	50 4B 03 04	OpenOffice documents
SXW	50 4B 03 04	OpenOffice documents
SYS	FF	Windows executable
SYS	EB	Windows executable file_3
SYS	E9	Windows executable file_2
SYS	E8	Windows executable file_1
SYS	FF 4B 45 59 42 20 20 20	Keyboard driver file
SYS	4D 5A	Windows|DOS executable file
SYS	FF FF FF FF	DOS system driver
SYW	41 4D 59 4F	Harvard Graphics symbol graphic
TAR	75 73 74 61 72	Tape Archive
TAR.BZ2	42 5A 68	bzip2 compressed archive
TAR.Z	1F A0	Compressed tape archive_2
TAR.Z	1F 9D 90	Compressed tape archive_1
TB2	42 5A 68	bzip2 compressed archive
TBZ2	42 5A 68	bzip2 compressed archive
TIB	B4 6E 68 44	Acronis True Image
TIF	4D 4D 00 2A	TIFF file_3
TIF	49 49 2A 00	TIFF file_2

EXTENSIÓN	FIRMA	DESCRIPCIÓN
TIF	49 20 49	TIFF file_1
TIF	4D 4D 00 2B	TIFF file_4
TIFF	49 49 2A 00	TIFF file_2
TIFF	49 20 49	TIFF file_1
TIFF	4D 4D 00 2B	TIFF file_4
TIFF	4D 4D 00 2A	TIFF file_3
TLB	4D 53 46 54 02 00 01 00	OLE|SPSS|Visual C++ library file
TR1	01 10	Novell LANalyzer capture file
UCE	55 43 45 58	Unicode extensions
UFA	55 46 41 C6 D2 C1	UFA compressed archive
VBX	4D 5A	VisualBASIC application
VCD	45 4E 54 52 59 56 43 44	VideoVCD|VCDImager file
VCF	42 45 47 49 4E 3A 56 43	vCard
VCW	5B 4D 53 56 43	Visual C++ Workbench Info File
VHD	63 6F 6E 65 63 74 69 78	Virtual PC HD image
VMDK	4B 44 4D	VMware 4 Virtual Disk
VMDK	23 20 44 69 73 6B 20 44	VMware 4 Virtual Disk description
VMDK	43 4F 57 44	VMware 3 Virtual Disk
VOB	00 00 01 BA	DVD video file
VSD	D0 CF 11 E0 A1 B1 1A E1	Visio file
VXD	4D 5A	Windows virtual device drivers
WAB	81 32 84 C1 85 05 D0 11	Outlook Express address book (Win95)
WAB	9C CB CB 8D 13 75 D2 11	Outlook address file
WAV	52 49 46 46	Resource Interchange File Format
WB2	00 00 02 00	QuattroPro spreadsheet

EXTENSIÓN	FIRMA	DESCRIPCIÓN
WB3	3E 00 03 00 FE FF 09 00 06	Quatro Pro for Windows 7.0
WIZ	D0 CF 11 E0 A1 B1 1A E1	Microsoft Office document
WK1	00 00 02 00 06 04 06 00	Lotus 1-2-3 (v1)
WK3	00 00 1A 00 00 10 04 00	Lotus 1-2-3 (v3)
WK4	00 00 1A 00 02 10 04 00	Lotus 1-2-3 (v4|v5)
WK5	00 00 1A 00 02 10 04 00	Lotus 1-2-3 (v4|v5)
WKS	0E 57 4B 53	DeskMate Worksheet
WKS	FF 00 02 00 04 04 05 54	Works for Windows spreadsheet
WMA	30 26 B2 75 8E 66 CF 11	Windows Media Audio|Video File
WMF	D7 CD C6 9A	Windows graphics metafile
WMV	30 26 B2 75 8E 66 CF 11	Windows Media Audio|Video File
WMZ	50 4B 03 04	Windows Media compressed skin file
WP	FF 57 50 43	WordPerfect text and graphics
WP5	FF 57 50 43	WordPerfect text and graphics
WP6	FF 57 50 43	WordPerfect text and graphics
WPD	FF 57 50 43	WordPerfect text and graphics
WPF	81 CD AB	WordPerfect text
WPG	FF 57 50 43	WordPerfect text and graphics
WPL	4D 69 63 72 6F 73 6F 66 74 20 57 69 6E 64 6F 77 73 20 4D 65 64 69 61 20 50 6C 61 79 65 72 20 2D 2D 20	Windows Media Player playlist
WPP	FF 57 50 43	WordPerfect text and graphics
WPS	D0 CF 11 E0 A1 B1 1A E1	MSWorks text document
WRI	BE 00 00 00 AB	MS Write file_3
WRI	32 BE	MS Write file_2
WRI	31 BE	MS Write file_1

EXTENSIÓN	FIRMA	DESCRIPCIÓN
WS	1D 7D	WordStar Version 5.0|6.0 document
WS2	57 53 32 30 30 30	WordStar for Windows file
XDR	3C	BizTalk XML-Data Reduced Schema
XLA	D0 CF 11 E0 A1 B1 1A E1	Microsoft Office document
XLS	FD FF FF FF 10	Excel spreadsheet subheader_2
XLS	09 08 10 00 00 06 05 00	Excel spreadsheet subheader_1
XLS	FD FF FF FF 29	Excel spreadsheet subheader_7
XLS	FD FF FF FF 28	Excel spreadsheet subheader_6
XLS	FD FF FF FF 23	Excel spreadsheet subheader_5
XLS	D0 CF 11 E0 A1 B1 1A E1	Microsoft Office document
XLS	FD FF FF FF 22	Excel spreadsheet subheader_4
XLS	FD FF FF FF 1F	Excel spreadsheet subheader_3
XLSX	50 4B 03 04	MS Office Open XML Format Document
XLSX	50 4B 03 04 14 00 06 00	MS Office 2007 documents
XML	3C 3F 78 6D 6C 20 76 65 72 73 69 6F 6E 3D 22 31 2E 30 22 3F 3E	User Interface Language
XPI	50 4B 03 04	Mozilla Browser Archive
XPS	50 4B 03 04	XML paper specification file
XPT	50 4B 03 04	eXact Packager Models
XPT	58 50 43 4F 4D 0A 54 79	XPCOM libraries
ZAP	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF	ZoneAlam data file
ZIP	50 4B 03 04 14 00 01 00	ZLock Pro encrypted ZIP
ZIP	50 4B 07 08	PKZIP archive_3
ZIP	50 4B 05 06	PKZIP archive_2
ZIP	50 4B 03 04	PKZIP archive_1
ZIP	50 4B 53 70 58	PKSFX self-extracting archive

EXTENSIÓN	FIRMA	DESCRIPCIÓN
ZIP	50 4B 4C 49 54 45	PKLITE archive
ZIP	57 69 6E 5A 69 70	WinZip compressed archive
ZOO	5A 4F 4F 20	ZOO compressed archive

Tabla 12: Listado con firmas de archivos.