UNIVERSIDAD RAFAEL LANDÍVAR
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
LICENCIATURA EN INVESTIGACIÓN CRIMINAL Y FORENSE

"HERRAMIENTAS FORENSES DE ANÁLISIS DIGITAL PARA LA OBTENCIÓN DE INFORMACIÓN APLICADO A ORDENADORES Y DISPOSITIVOS MÓVILES"

TESIS DE GRADO

CARLOS ALEJANDRO MALDONADO ESCOBAR
CARNET 15793-15

QUETZALTENANGO, NOVIEMBRE DE 2020
CAMPUS DE QUETZALTENANGO

UNIVERSIDAD RAFAEL LANDÍVAR

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

LICENCIATURA EN INVESTIGACIÓN CRIMINAL Y FORENSE

"HERRAMIENTAS FORENSES DE ANÁLISIS DIGITAL PARA LA OBTENCIÓN DE INFORMACIÓN APLICADO A ORDENADORES Y DISPOSITIVOS MÓVILES"

TESIS DE GRADO

TRABAJO PRESENTADO AL CONSEJO DE LA FACULTAD DE

CIENCIAS JURÍDICAS Y SOCIALES

POR

CARLOS ALEJANDRO MALDONADO ESCOBAR

PREVIO A CONFERÍRSELE

EL TÍTULO Y GRADO ACADÉMICO DE LICENCIADO EN INVESTIGACIÓN CRIMINAL Y FORENSE

QUETZALTENANGO, NOVIEMBRE DE 2020

CAMPUS DE QUETZALTENANGO

AUTORIDADES DE LA UNIVERSIDAD RAFAEL LANDÍVAR

RECTOR:	P. MARCO TULIO MARTÍNEZ SALAZAR, S. J.
VICERRECTORA ACADÉMICA:	MGTR. LESBIA CAROLINA ROCA RUANO
VICERRECTOR DE INVESTIGACIÓN Y PROYECCIÓN:	LIC. JOSÉ ALEJANDRO ARÉVALO ALBUREZ
VICERRECTOR DE INTEGRACIÓN UNIVERSITARIA:	P. LUIS CARLOS TORO HILTON, S. J.
VICERRECTOR ADMINISTRATIVO:	MGTR. JOSÉ FEDERICO LINARES MARTÍNEZ
SECRETARIO GENERAL:	DR. LARRY AMILCAR ANDRADE - ABULARACH

AUTORIDADES DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

DECANO:	DR. HUGO ROLANDO ESCOBAR MENALDO
VICEDECANA:	MGTR. HELENA CAROLINA MACHADO CARBALLO
SECRETARIO:	LIC. CHRISTIAN ROBERTO VILLATORO MARTÍNEZ

NOMBRE DEL ASESOR DE TRABAJO DE GRADUACIÓN

LIC. LUIS EDUARDO ESCOBAR DE LEÓN

TERNA QUE PRACTICÓ LA EVALUACIÓN

LIC. MOISÉS FRANCISCO LÓPEZ GARCÍA

AUTORIDADES DEL CAMPUS DE QUETZALTENANGO

DIRECTOR DE CAMPUS:	P. MYNOR RODOLFO PINTO SOLIS, S.J.
SUBDIRECTORA ACADÉMICA:	MGTR. NIVIA DEL ROSARIO CALDERÓN
SUBDIRECTORA DE INTEGRACIÓN UNIVERSITARIA:	MGTR. MAGALY MARIA SAENZ GUTIERREZ
SUBDIRECTOR ADMINISTRATIVO:	MGTR. ALBERTO AXT RODRÍGUEZ
SUBDIRECTOR DE GESTIÓN GENERAL:	MGTR. CÉSAR RICARDO BARRERA LÓPEZ

Quetzaltenango, 27 de may. de 2020

Magister
Nelly de León Reyes
Coordinadora Académica
Facultad de Ciencias Jurídicas y Sociales

Respetable Magister Nelly:

Por este medio le saludo cordialmente, a la vez que me permito dirigirme a usted con el objeto de rendir Dictamen sobre la asesoría proporcionada al estudiante CARLOS ALEJANDRO MALDONADO ESCOBAR, quien se identifica con el Carné No. 1579315, en la elaboración de su trabajo de tesis "HERRAMIENTAS FORENSES DE ANÁLISIS DIGITAL PARA LA OBTENCIÓN DE INFORMACIÓN APLICADO A ORDENADORES Y DISPOSITIVOS MÓVILES", el cual se realizó de acuerdo a las técnicas para este tipo de investigación, para la carrera de Licenciatura en Investigación Criminal y Forense.

El tema abordado reviste de suma importancia en la actualidad, a las herramientas forenses de análisis digital que son de utilidad para recabar información en la investigación digital de casos.

Por lo anteriormente expuesto doy mi aprobación y rindo DICTAMEN FAVORABLE al trabajo de tesis elaborado, en virtud de llenar los requisitos del instructivo de tesis respectivo.

Sin más que agregar a la presente, me suscribo de usted con mis altas muestras de consideración y estima.

Atentamente,

Luis Eduardo Escobar de León
Lic. en Investigación Criminal y Forense

Luis Eduardo Escobar de León
Asesor

Universidad Rafael Landívar
Tradición Jesuita en Guatemala

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
No. 072574-2020

Orden de Impresión

De acuerdo a la aprobación de la Evaluación del Trabajo de Graduación en la variante Tesis de Grado del estudiante CARLOS ALEJANDRO MALDONADO ESCOBAR, Carnet 15793-15 en la carrera LICENCIATURA EN INVESTIGACIÓN CRIMINAL Y FORENSE, del Campus de Quetzaltenango, que consta en el Acta No. 07477-2020 de fecha 20 de noviembre de 2020, se autoriza la impresión digital del trabajo titulado:

"HERRAMIENTAS FORENSES DE ANÁLISIS DIGITAL PARA LA OBTENCIÓN DE INFORMACIÓN APLICADO A ORDENADORES Y DISPOSITIVOS MÓVILES"

Previo a conferírsele el título y grado académico de LICENCIADO EN INVESTIGACIÓN CRIMINAL Y FORENSE.

Dado en la ciudad de Guatemala de la Asunción, a los 25 días del mes de noviembre del año 2020.

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
SECRETARIO DE FACULTAD
U.R.L.

LIC. CHRISTIAN ROBERTO VILLATORO MARTÍNEZ, SECRETARIO
CIENCIAS JURÍDICAS Y SOCIALES
Universidad Rafael Landívar

Índice Pág.

LISTADO DE ABREVIATURAS

MP	Ministerio Publico.
PNC	Policía Nacional Civil.
INACIF	Instituto Nacional de Ciencias Forenses.
RAM	random access Memory.
OS	Operative System.
USB	Universal Serial Bus.
DNS	Domain Name System.
SPF	Sender Policy Framework.
MX	Mail Exchanger Record.
CNAME	Canonical Name.
ICANN	Internet Corporation for Assigned Names and Numbers.
NIC	Network Information Center.
LACNIC	Registro de Direcciones de Internet para América Latina y el Caribe.
IP	Internet Protocol.
MB	Megabyte.
GB	Gygabyte.
TB	Terabyte.
VPN	Virtual Private Network.
RFC	Request for Comments.
GPS	Global Positioning System.
CD	Compact Disc.

RESUMEN

En la actualidad, la información juega un papel importante sobre todo en negocios u organizaciones que cuenten con un sistema informático, ya que este puede ser el escenario para cometer distintos delitos, influyendo enormemente en el desarrollo de los mismos.

La presente investigación fue elaborada con el objetivo de reunir una serie de herramientas forenses utilizadas en el mundo digital que son de utilidad para recabar información que pueda ser utilizada en la investigación aportando claridad para la resolución del caso judicial. Así mismo, establecer los procedimientos para la debida recolección, identificación, manejo y resguardo de la evidencia digital en cualquier estado en que pueda ser hallada en una escena. Igualmente, como proceder a elaborar imágenes forenses respaldando todos los archivos existentes en el medio de almacenamiento y que puedan ser parte de la realización del delito, aun cuando estos hayan sido eliminados fuese o no de forma intencional; esto de la forma que se garantice que sea una copia fiel y exacta a la original con la cual, se realizaran los análisis para posteriormente presentarlos ante tribunal competente.

INTRODUCCIÓN

Nunca antes los seres humanos habían dejado rastro de toda la actividad que llevan a cabo. Los millones de personas que, mediante la tecnología, dejan rastro de todos los lugares en los que han estado y comunicaciones que han tenido. Sin embargo, por ser aun un tema relativamente “nuevo”, en las ciencias jurídico-sociales, esta abundante información no ha tenido el impacto que podría llegar a alcanzar, tanto por la ignorancia de operadores jurídicos y a la dificultad de lidiar técnicamente con esta información.

Actualmente en la república de Guatemala, no existe una norma nacional que tenga como objetivo regular cualquier hecho ilícito en donde se encuentre implicado un ordenador. Lo más cercano a ello, es el capítulo VII denominado: De los delitos contra el derecho de autor, la propiedad industrial y delitos informáticos, del Código penal; donde hace referencia a unas cuantas normas pero que, en la actualidad, han quedado obsoletas debido al gran paso con el que evoluciona el mundo digital.

El ámbito del análisis digital forense, es un campo dinámico, que tiene cada vez más un poderoso impacto en una variedad de situaciones, incluyendo ambientes laborales, casos civiles, investigaciones criminales, investigaciones de inteligencia y de asuntos de seguridad nacional. Por lo que la presente investigación tiene como objeto establecer cuáles son las herramientas forenses de análisis digital para la obtención de información aplicada a ordenadores y dispositivos móviles, desarrollándolo a lo largo de cuatro capítulos.

Estos cuatro capítulos tocan temas como los antecedentes que dieron origen a lo que hoy en día se conoce como informática forense, así como su debida definición; se aclarara terminología propia de la informática para poder comprender e interpretar la información extraída de ordenadores y dispositivos móviles; se profundiza en el estudio de mecanismos y técnicas empleadas con distintas herramientas forenses existentes, para la extracción de información que podría ser relevante en la toma de

decisión en un caso jurídico; Así mismo, las medidas que dictan las distintas normativas internacionales relacionadas a la informática.

Delimitando al estudio de las distintas herramientas forenses de análisis digital para la obtención de información aplicado a ordenadores y dispositivos móviles, abarcando el estudio de normas o estándares internacionales publicadas por La Organización Internacional de Normalización y el Instituto Nacional de Estándares y Tecnología, dedicas al desarrollo, estudio y publicación de estándares, incluyendo el desarrollo de temas forenses.

De igual forma, cuenta con el procedimiento que se debe llevar acabo para poder levantar una máquina virtual para que, de esta forma se pueda generar un entorno controlado que sea utilizado como un laboratorio informático forense. De esta forma, aporta datos de los distintos softwares que se utilizan para la extracción de información que guie a los operadores de justicia en su correcto manejo y comprensión, para que la evidencia mantenga los principios de autenticidad, confiablidad, integridad y que, a la vez, cumpla de conformidad a las leyes y reglas para su aceptación como material probatorio en un proceso legal. Así mismo, servirá como precedente para investigaciones posteriores, y como material que oriente a quienes busquen profundizar en el estudio de esta materia.

CAPÍTULO I
INFORMÁTICA FORENSE

1.1 Antecedentes

El campo de la informática tuvo su inicio en la década de 1980, poco tiempo después de que el acceso a la tecnología informática fuera posible gracias a la comercialización de los ordenadores hacia el público consumidor. Esto facilitó el ritmo de vida de las personas, pero a su vez, abrió un nuevo campo para la comisión de delitos, Debido a esto, el gobierno notó que los criminales empezaron a usar la tecnología.

1. *"Magnetic Media Program 1984 - 1991*
   Informática forense - El FBI forma el Magnetic Media Program, que más tarde, en 1991, será el Computer Analysis and Response Team (CART).
2. *AccessData 1987*
   Informática forense - Nace la compañía AccessData, desarrolla productos orientados a la recuperación de contraseñas y el análisis forense.
3. *High Tech Crime Investigation Association 1987*
   Informática forense - Se crea la High Tech Crime Investigation Association (HTCIA), que agrupa a profesionales tanto de agencias gubernamentales como de compañías privadas para centralizar conocimiento e impartir cursos."[1]

En el año 1984, el FBI creo un programa llamado Magnetic Media Program, en español: Programa de Medios Magnéticos, que más tarde pasaría a denominarse CART (equipo de análisis y respuesta informática, por sus siglas en ingles). Que es un centro de respuesta a incidentes de seguridad en tecnologías de la información.

4. *"International Association of Computer Investigative Specialists 1990.*
   Informática forense - Se crea la International Association of Computer Investigative Specialists (IACIS), la cual certifica a profesionales de agencias gubernamentales en el Certified Forensic Computer Examiner (CFCE).
5. *International Organization on Computer Evidence 1995"*

[1] Preceden, Historia de la Ciencia Forense e Informática Forense, 2019. Disponible en: https://www.preceden.com/timelines/300848-historia-de-la-ciencia-forense-e-inform-tica-forense consultado: febrero de 2019

Informática forense - Se funda el International Organization on Computer Evidence (IOCE), con el objetivo de ser punto de encuentro entre especialistas en la evidencia electrónica y el intercambio de información."[2]

Durante la década de 1990, incremento la aparición de empresas dedicadas a la creación tanto de software como de hardware de prevención. Las empresas dedicadas a elaboración de antivirus, empezaron a aportar al campo mediante la detección de intrusos, canales seguros de comunicación, encriptación, firewalls, entre otros. Estas no solo comercializaban sus productos, sino que a la vez ofrecieron consultorías en temas de seguridad, riesgos, repuestas frente a incidentes, recuperación de desastres y otros servicios más.

6. *International Forensic Science Symposium 1996 - 2017*

   Informática forense - La Interpol organiza los International Forensic Science Symposium, un foro para debatir los avances forenses.

7. *Digital Forensic Research Workshop 2001*

   Informática forense - Nace la Digital Forensic Research Workshop (DFRWS), un grupo de debate y discusión internacional para compartir información."[3]

Frente a la década del 2000, incrementó considerablemente el número de delitos informáticos. La cual motivo la aparición de expertos, empresas dedicadas al desarrollo de herramientas forenses, así como la creación de normas o estándares. Se puede nombrar a la ISO (International Organization for Standardization) y a NIST (National Institute of Standards and Technology), entidades de categoría mundial que se dedican al desarrollo, estudio y publicación de estándares, incluyen en su desarrollo estos temas forenses.

Actualmente las compañías de software producen herramientas más robustas y los agentes de la ley y militares entrenan a más personal para responder a los crímenes que involucren tecnología.

En la actualidad, la nueva era de la tecnología y la información, juega un papel muy importante, sobre todo en negocios u organizaciones que cuenten con un sistema informático, ya que este puede ser el escenario para cometer distintos delitos,

[2] *Loc. cit.*
[3] *Loc. cit.*

influyendo enormemente en el desarrollo de los mismos, usurpando archivos confidenciales o dañando el sistema a nivel de software o hardware, causando grandes estragos como una perdida monetaria o el daño, modificación o eliminación de información de importancia contenida en ellos y que puede ser una clave importante para crear riqueza a partir de ella.

Esto se puede llevar a cabo, ya sea por una persona ajena a la organización como de un mismo trabajador de la compañía. Por lo que es de importancia establecer un conjunto de herramientas y acciones a llevar a cabo para revelar en los medios informáticos, la evidencia que haya sido dejada por el autor del hecho, para su correcta interpretación y que pueda ser de ayuda en la resolución de un hecho delictivo. Aquí parte la importancia de la informática forense.

1.2 Definición.

Según el criminólogo José Manuel Ferro Veiga, la informática forense se define como: "*proceso metodológico para la recogida y análisis de los datos digitales de un sistema de dispositivos de forma que pueda ser presentado y admitido ante los tribunales".*[4]

Es una disciplina técnico-legal que auxilia al sector judicial para afrontar los delitos informáticos, mediante metodologías pretende identificar, preservar, analizar y presentar los medios de prueba digital ante un proceso civil o penal.

La informática forense se encargará de la investigación en torno a sistemas informáticos, el esclarecimiento de los hechos, así como detectar al posible autor o autores, a través de la identificación y análisis de la evidencia digital.

Helena Rifa Pous menciona en el libro Análisis forense de sistemas informáticos que "*En el análisis forense se realiza un análisis posterior de los incidentes de seguridad, mediante el cual se trata de reconstruir como se ha penetrado o vulnerado en el sistema. Se intenta responder a las siguientes preguntas: ¿Quién ha realizado el ataque?, ¿Cómo se realizó?,¿Qué hizo el intruso una vez que accedió al sistema?, etc*." [5] El ámbito de actuación de la informática forense se necesita cuando surgen

[4] Ferro Veiga, José Manuel. *La ciencia forense al servicio de la Administración de Justicia y la Autoridad Policial*, España, Createspace Independent Pub, 2014, Pág. 112.

[5] Rifa Pous, Helena y otros. *Análisis forense de sistemas informáticos*, España, Eureca Media, 2009, Pág. 5.

preguntas del tipo: ¿Qué le ha pasado al ordenador?. Ya sea que esto suceda en campo empresarial o en el caso de un particular, para buscar una solución a lo que realmente ha pasado. ha sido mediante un virus o fue que un empleado/conocido entro al ordenador y se ha robado los datos del mismo. Siempre ir enfocado a que se puede llegar a tener un juicio, de ahí la parte forense, porque muchos casos, las actuaciones que ha llevado a cabo el perito se puede llegar a presentar frente a un juez verificando como se tomaron las pruebas, como se extrajo los datos y la evidencia.

1.3 Objetivos de la informática forense

"*Para conseguir sus objetivos, la Informática Forense desarrolla técnicas idóneas para ubicar, reproducir y analizar evidencias digitales con fines legales*." [6] Estas deben ser legalmente aceptables. Cuando un perito se dedica a su labor, debe basarse en una metodología de trabajo que viene marcada por la ley y por la jurisprudencia tanto laboral como penal.

Antonio Sanz redactor web del Instituto Nacional de Ciberseguridad España menciona que "*El objetivo de la informática forense es identificar, adquirir, conservar y recuperar evidencias digitales y presentar hechos objetivos a partir de su análisis. Esto obliga a una serie de metodologías que es necesario conocer y seguir de forma estricta si no queremos que todo el trabajo realizado carezca de valor*." [7]

1. Identificar: "*en esta fase se realiza un estudio inicial mediante entrevistas y documentación entregada por el cliente con el objetivo de tener una idea inicial del problema que nos vamos a encontrar*"[8] Lo importante es entender el entorno, la causa y cuál es el dispositivo que se va a peritar, si es un ordenador, una notebook, un servidor, entre otros. Hay que tomar en cuenta que es lo que será de interés de ese dispositivo. Hay unas buenas prácticas como lo es desconectar un ordenador desde el cable de tensión, de esa manera se evita manipular la información, pero puede ser que el dato de interés se encontraba

[6] Instituto criminalístico forense, informática forense y dispositivos móviles, España, s/a, Disponible en: https://www.icfmurcia.es/seguridad-informatica/ consultado: abril de 2019

[7] Instituto nacional de ciberseguridad, Sanz Antonio, Quieres trabajar en informática forense. España, 2013, Disponible en: https://www.incibe-cert.es/blog/dominios-de-conocimiento-informatica-forense consultado: abril de 2019.

[8] Rifa Pous, Helena y otros. *óp. cit*., Pág. 6.

en la memoria RAM, si se desconectaba esta información se pierde, por eso es importante identificar el entorno.

2. Preservar: "*se realiza una obtención de los datos e información de los datos esenciales para la investigación. Se duplican o clonan los dispositivos implicados para un posterior análisis. En esta fase habrá que tener mucho cuidado en la adquisición de los datos puesto que cabe la posibilidad de incumplir los derechos fundamentales del atacante*",[9] es esencial mantener la integridad de los dispositivos, todo lo que se llega a adquirir, se debe de verificar que es lo mismo que se va a presentar ante una corte y que no sea contaminado de ningún aspecto porque puede llegar a ser tomado como inadmisible en un caso judicial.
3. Analizar: "Se realiza un estudio con los datos adquiridos. En esta fase también habrá que tener mucho cuidado puesto que cabe la posibilidad de incumplir los derechos fundamentales del atacante",[10] a partir de la evidencia adquirida se analizará los datos informáticos para que una vez realizado, se pueda llegar a una conclusión que sirva en la resolución de un caso judicial o al directivo de una empresa que haya llegado a requerir los servicios de un perito informático.
4. Presentar: *"En esta fase se elabora el informe que será remitido a la dirección de la organización o empresa. Posteriormente, se podrá usar para acompañar la denuncia que realicemos a la autoridad competente*."[11] Debe llegar a tener un vocabulario claro, que sea comprensible para las personas a las que sean de interés. Si fuese tratado por un abogado, se debe hablar con su léxico y si se utilizan palabras técnicas se deberá dar una definición, ya que ellos no suelen manejar este tipo de conceptos.

[9] *Loc. Cit.*
[10] *Loc. Cit.*
[11] *Loc. Cit.*

1.4 Importancia de la informática forense

En la actualidad mucha información es manejada mediante la tecnología, simplificando la vida de los usuarios, pero a la vez haciéndolos más vulnerables en cuanto a la manipulación, robo o falsificación de los datos personales.

Los Abogados Portaley, especializados en Nuevas Tecnologías e Internet, mencionan que *"En un proceso judicial relacionado con sistemas de información y software es muy posible necesitar un perito informático que realice una prueba pericial sobre las evidencias del caso."*[12] En un escenario jurídico, un perito en informática forense podrá ser citado de dos formas: judicial o de parte. En el judicial, el perito será brindado por el juez, en su defecto, de INACIF, y en los de parte, el perito irá nombrado por una de los dos partes litigantes.

"En el caso de análisis forense de dispositivos electrónicos (ordenadores personales, servidores, teléfonos móviles, etc.) se persigue la identificación de rastros digitales que evidencien que cierto suceso ha ocurrido en el dispositivo para ser utilizadas en un juicio."[13] En el caso de una investigación que se realice en un ordenador perteneciente a una estructura criminal, se puede llegar a determinar quién estaba a cargo del equipo de cómputo, cual es el historial del manejo de este, cuáles son las vías de comunicación que utilizan para contactar a demás miembros de la estructura, información financiera, proyectos, planes a futuro, modus operandi, entre otros.

Elaine miembro de OnRetrieval: especialistas en Recuperación de Datos, Informática Forense y Ciberseguridad, menciona que *"En caso de que la seguridad de una empresa haya sufrido una brecha, un informático forense tiene otra misión, la de recopilar toda la información y evidencias necesarias para poder averiguar cuál es el origen del ataque o qué ha podido pasar para que se haya producido este suceso."*[14] En una investigación privada, de fuga de información de una empresa, la informática busca detectar y lograr reconstruir el ataque que haya sido realizado con el fin de

[12] Portaley, Portaley, Análisis forense informático: Pruebas Periciales, España, 2013, Disponible en: http://portaley.com/2013/10/analisis-forense-informatico-pruebas-periciales/ Consultado: febrero de 2019

[13] *Loc. cit.*

[14] OnRetrieval, Elaine, Objetivos de la informática forense, España, 2018. Disponible en: https://onretrieval.com/objetivos-de-la-informatica-forense/ consultado: febrero de 2019

obtener datos que pudieran ser manipulados durante el mismo, y lograr identificar de donde fue producido dicho ataque.

1.5 Análisis forense digital

La licenciada Rifa Pous, explica que el análisis forense digital "*permite reconstruir lo que ha sucedido en un sistema tras un incidente de seguridad. Este análisis puede determinar quién, desde dónde, cómo, cuándo y qué acciones ha llevado a cabo un intruso en los sistemas afectados por un incidente de seguridad*."[15] Este se inicia cada vez que un cliente requiera del servicio de un perito informático, brindará datos y dará información. dentro del mundo del análisis forense digital, hay grandes mentiras, como grandes verdades. El propósito de los peritos informáticos forenses será aplicar la experiencia, conocimiento, así como la imaginación al momento de desentrañar lo que será la resolución del caso.

El Ingeniero en Sistemas de Información Matías Porolli menciona que el análisis forense digital *"Corresponde con un conjunto de técnicas destinadas a extraer información valiosa de discos, sin alterar el estado de los mismos. Esto permite buscar datos que son conocidos previamente, tratando de encontrar un patrón o comportamiento determinado, o descubrir información que se encontraba oculta."*[16]

Este será de utilidad para la reconstrucción del hecho delictivo informático que se haya realizado en un sistema tras un incidente de seguridad. En caso de contra peritajes, al perito informático le tocara ver tal peritaje para que se ha realizado de mal en el mismo. Las conclusiones pueden ser diferentes pero los resultados no lo pueden ser. Estos siempre deben de poder volver a reconstruirse desde la copia forense integra.

1.5.1 Tipos de Análisis Forense

Para el éxito en el peritaje informático, una etapa importante es la obtención de la información de medios electrónicos así establecer los hechos y formular hipótesis relacionadas al caso. Dependiendo del punto a analizar, nos encontramos los

[15]Rifa Pous, Helena y otros. *óp.cit*., Pág. 5.

[16]We live security, Porolli Matías, En qué consiste el análisis forense de la información, Eslovaquia, 2013. Disponible en: https://www.welivesecurity.com/la-es/2013/08/12/en-que-consiste-analisis-forense-de-informacion/ consultado: abril de 2019

siguientes tipos *"1. Sistemas de computación abiertos, 2. Sistemas de comunicación, 3. Sistemas convergentes de computación."*[17]

1) Sistemas de computación abiertos: esta clasificación está compuesta por computadores personales con los distintos sistemas operativos, así como sus varias distribuciones: Mac OS, Microsoft Windows, Unix, y sistemas GNU/Linux.

2) Sistema de comunicación: en este se encuentran las de redes de telecomunicaciones, comunicación inalámbrica y el internet. Podemos mencionar las cableadas, Wireless, bluetooth, entre otros.

3) Sistemas de convergentes de computación: engloba los teléfonos celulares inteligentes, mayormente conocidos como los Smartphone y cualquier otro aparato electrónico que posea tecnología digital y de los cuales sea posible la extracción de evidencia digital.

1.6 La evidencia digital

En la informática forense se trabajará con evidencia digital. Eoghan Casey lo define como *"un tipo de evidencia física que está construida de campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales."*[18] Al llamarlo digital, se refiere a la virtualidad del mismo, es decir no es palpable, aunque estos siempre estarán almacenados en un soporte físico, como lo es un ordenador o un dispositivo móvil, por lo que esta evidencia puede considerarse igualmente física. Una particularidad de la misma es que es frágil, esta se puede crear, alterar, copiar y borrar de formas muy simples.

Unicolombia define La evidencia digital como *"cualquier valor probatorio de la información almacenada o transmitida en formato digital de tal manera que una parte o toda puede ser utilizada en el juicio. Antes de aceptar la evidencia digital un tribunal*

[17] Organización de los Estados Americanos, Manual de Manejo de Evidencias Digitales y Entornos Informáticos, 2011.

[18] Casey, Eoghan, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, Estados Unidos, Academic Press, 2000, Pág. 7.

determinará si la prueba es pertinente, auténtica, si es un rumor y si es aceptable una copia o el original es requerido."[19]

Dentro de un caso judicial serán las pruebas que se presentan, ya sea que una parte procesal presenta un email, un correo electrónico, la cual deberá ser constatada por un perito informático para verificar que sea legitima para que pueda ser aceptada como evidencia o si al contrario esta fue adulterada.

"La evidencia digital es la materia prima para los investigadores 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 comunicaciones, es preciso detallar las características propias de dicha evidencia en este entorno. La evidencia digital posee, entre otros, los siguientes elementos que la hacen un constante desafío para aquellos que la identifican y analizan en la búsqueda de la verdad:

- *Es volátil*
- *Es anónima*
- *Es duplicable*
- *Es alterable y modificable*
- *Es eliminable"*[20]

Al tener presentes estas características, se contempla la complicada labor que llevan a cabo los peritos en informática forense, tanto en procedimientos como el uso de las herramientas forenses para tratar la evidencia presente en la escena de un delito informático. Por lo que es de suma importancia tener el conocimiento detallado de las normas y regulaciones asociadas al manejo y recolección de la evidencia digital, para mantener la confiablidad y así analizar de forma correcta y detallada los datos recabados.

Los distintos dispositivos que se pueden llegar a ser analizados son variados y cada procedimiento a seguir debe ser capaz de adecuarse según las necesidades de cada caso. Entre ellos se encuentran:

[19] Informática forense Colombia, Unicolombia, La Evidencia Digital, Colombia, 2017. Disponible en: https://www.informaticaforense.com.co/la-evidencia-digital/ consultado: abril de 2019

[20] Loc. Cit.

1) Discos duros.
2) Teléfonos celulares.
3) Memorias USB.
4) Reproductores de audio.

Y cualquier otro dispositivo que tenga la capacidad de almacenar datos, es un candidato a ser analizado a nivel forense.

1.7 Peritos informáticos

Un perito se puede definir como *"persona que, poseyendo determinados conocimientos científicos, artísticos, técnicos o prácticos, informa, bajo juramento, al juzgador sobre puntos litigiosos en cuanto se relacionan con su especial saber o experiencia."*[21] El tema de un perito es ser un auxiliar en justicia, existiendo peritos en varias áreas como dactiloscopia, grafoscopía, en el caso de un homicidio se presentaría un perito en medicina forense, en un accidente vehicular, se necesitaría un perito en hechos de tránsito terrestre. En el caso de incluir un equipo informático, se necesitaría de un perito informático, ayudando a resolver un caso que involucre ordenadores, equipos móviles, servidores, entre otros.

Además de llegar a recolectar la evidencia digital, el perito deberá de observar la escena del crimen en su totalidad, en la búsqueda de hojas que cuentan con usuarios o contraseñas, anotaciones que hayan sido escritas, manuales de herramientas, siempre documentándolas siguiendo las directrices de la evidencia digital.

Los peritos forenses deberán conocer de los campos de sistemas, de programación, ciberseguridad, hacking ético, así como toda la parte legal, para poder condensar este conocimiento como informática forense. Tomando en cuenta que continuamente deberá actualizar sus conocimientos, ya que el campo de la tecnología avanza en grandes pasos, así como es la integración de nuevas ramas como lo son los nuevos móviles y tablets. Por lo que hay que conocer los distintos sistemas operativos, así

[21]Jurisplace, El Perito Judicial y su papel profesional, España, 2013. Disponible en: https://jurisplace.com/articulos/ver_contenido/que_es_perito/32/El%20Perito%20Judicial%20y%20su%20papel%20profesional consultado: abril de 2019

como conocer los métodos para vulnerarlos, como asegurarlos, para que con toda esta información sea posible hacer un análisis forense.

Entre los inconvenientes que se presentan en el tema, es que los planes de formación apenas están empezando en Latinoamérica, en lo que es informática forense. Por lo que a veces hay que investigar en temas que ni se encuentran regulados por la ley. Como lo es el caso del ciberbullying. José Antonio Luengo Latorre en el libro Ciberbullying: prevenir y actuar, define el ciberbullying como "*Una agresión psicológica, sostenida y repetida en el tiempo, perpetrada por uno o varios individuos contra otros, utilizando para ello las nuevas tecnologías."*[22] En casos relacionados en otros países, al tratar esos temas que llegan a juicio, por no estar regulado, no se puede hacer mayor acción en cuanto a procedimientos penales se refiere.

El argentino Héctor Jara menciona en su libro Ethical hacking 2.0 que *"La velocidad con la que avanza el mundo no da tregua para atrasarse, por lo cual resulta indispensable disponer de los medios para estar actualizados y con fuentes de información de confianza."*[23] Un perito informático deberá mantenerse en constante actualización, debido a que la informática en la actualidad, avanza a paso rápido. Aplicaciones o sitios web que cambian su estructura radicalmente en cuestión de meses.

1.7.1 El rol del perito informático forense en el proceso judicial

El perito en un proceso judicial, se encarga tanto de recibir el material informático como el de realizar una labor de investigación de ellas, considerando las distintas medidas de seguridad y control de dichas pruebas para garantizar que estas no fueron alteradas en ningún momento.

El Ingeniero en Informática y Máster en Peritaje Informático e Informática Forense José Delgado García menciona que *"el Juez acordará el Informe Pericial cuando, para conocer o apreciar algún hecho o circunstancia importante en el sumario, fueran*

[22] Luengo Latorre, José Antonio, *Ciberbullying: prevenir y actuar*, España, Colegio oficial de psicólogos de Madrid, 2009, Pág. 105.

[23] Jara, Héctor y Federico Pacheco. *Ethical hacking 2.0*, Argentina, manuales Users, 2009, primera edición, Pág. 25.

necesarios o convenientes conocimientos científicos o artísticos" [24] básicamente lo que el perito pretende es brindar una opinión técnica sobre las pruebas informáticas, que a lo mejor las demás partes procesales les es de interés, pero no son entendidos en la materia. El perito deberá actuar de forma objetiva, es decir de forma neutral, sin apoyar a ninguna de las partes judiciales.

Vanesa Quezada redactora de la página web Xataka, menciona que *"plasmar dichas conclusiones en informes que es capaz de defender ante los Tribunales, con un lenguaje sencillo y llano, ajeno a tecnicismos que desorienten al juez"* [25] siendo esta la parte más importante del labor de un perito informático, saber transmitir lo que se ha llegado a analizar, ya que no es de ir a recibir reconocimiento por el amplio conocimiento o que tan erudito se es en la materia, sino es saber transmitir lo que se conoce y se ha analizado del caso, y que las partes judiciales comprendan perfectamente, ya que, en torno al peritaje emitido, se decidirá la resolución del juicio. Es importante remarcar que un perito informático no puede emitir un juicio de valor de quien es culpable y quien es inocente, ya que este es trabajo exclusivo del juez, el perito solamente actuará como auxiliar de justicia. Se limitará a la explicación de los actos que se llevaron a cabo en el equipo informático, para que el juez llegue a la conclusión lógica.

1.8 Herramientas comerciales y código libre

En el mundo de la computación, existe una enorme cantidad de software para realizar cualquier tipo de actividad, ya sea desde un programa de ofimática para realizar una hoja de cálculo, hasta un simple juego para entretenerse. Estos están regidos por una serie de términos y cláusulas que la persona que los utilice deberá cumplir para poder hacer uso del mismo. Se podría decir que básicamente es un tipo de contrato entre el autor del programa y el usuario.

[24] Peritajes informáticos, Delgado García José, Que es el informe pericial, España, 2018, Disponible en: https://jdgperitajesinformaticos.es/que-es-el-informe-pericial/ consultado: abril de 2019

[25] Xataka, Vanesa Quezada, Cómo se llega a ser el perito informático que analiza los discos duros de Bárcenas, España, 2016, Disponible en: https://www.xataka.com/ordenadores/como-se-llega-a-ser-el-perito-informatico-que-analiza-los-discos-duros-de-barcenas consultado: abril de 2019

Estos se separan en dos grupos, según el objetivo de desarrollo que le haya dejado la empresa que los haya elaborado: software comercial y software libre.

Marker explica que *"El Software comercial es el software desarrollado por una empresa con el objetivo de lucrar con su utilización."*[26] Este tipo de software es el que el fabricante pone a los usuarios un costo determinado, para poder hacer uso del programa que ha comprado. Aunque esto no quiere decir que sea dueño del mismo, ni que pueda modificarlo a su antojo. Sino debe abstenerse a los parámetros ya establecidos por el fabricante.

Franco Rivero en su libro de Windows a Linux, define al software libre como *"la facultad de usar el software para cualquier propósito, tanto si se trata de un sistema operativo como si es un paquete de oficina. Trata sobre la autonomía para estudiar cómo funciona y trabaja el programa, y nos brinda la posibilidad de modificarlo."*[27] Este brinda una gran libertad al usuario, ya que puede usarlo, modificarlo y distribuirlo sin problema alguno. Entre los softwares libres más conocidos están Moxilla, Linux, debian, VLC player. Desde programas hasta sistemas operativos completos.

Esto es de relevancia en el ámbito forense, ya que, al momento de presentar una evidencia analizada y extraída mediante software. Entre los primeros ataques que se puede recibir del lado contrario, es si se cuenta con la licencia del software requerido. Si en tal caso no se tuviera, la evidencia presentada pasaría a ser ilegal, ya que no se cuenta con la facultad de poder utilizar legalmente el software. Debido a la gran cantidad de trabajo que conlleva el desarrollar este software forense, su precio también es considerablemente alto, por lo que son pocas las oficinas privadas dedicadas a la informática forense que cuenten con licencias. Aquí es donde entra el software libre. Debido a que este mismo es gratis, cualquier análisis y resultado que nos brinden los mismos, pueden ser presentados ante un juicio con toda la legalidad posible, ya que se cuenta con la autorización para que cualquiera pueda usarlo.

[26] Tecnología & informática, Graciela Marker, Tipos de licencias de software, España, 2016, Disponible en: https://tecnologia-informatica.com/tipos-licencias-software-libre-comercial/ consultado: abril de 2019

[27] Rivero, Franco. *De Windows a Linux*, Argentina, manuales Users, 2009, primera edición, Pág. 5.

1.9 Aplicabilidad de la informática forense

La informática forense es aplicable para poner al descubierto actividades tales como el crimen electrónico también conocido como cibercrimen, que agobia con operaciones ilícitas principalmente en entornos empresariales en donde llega a existir el robo de información de carácter privado o con derecho de autor.

También es aplicable a actividades ilícitas que se llevan a cabo mediante internet tales como dañar, destruir o intervenir medios informáticos, por ejemplo, Hackear un equipo de cómputo, una página web, cualquier dispositivo que este o no conexión a internet, el simple hecho de intervenirlo constituye un delito y está contemplado como destrucción de registros informáticos en el artículo 274 A del Código Penal. Por mencionar algunas actividades: suplantación de identidad, denegación de servicios, ataques a redes informáticas, SQL inyection.

Esta ciencia, también ayuda a detectar casos de pornografía infantil, delitos contra la privacidad, violaciones de derecho de autor. En casos empresariales podría existir la sustracción de secretos comerciales que estuviesen localizados en algún soporte informático, o hasta en la sustracción, alteración o falsificación de información tributaria para simular la situación real del contribuyente, la aplicabilidad aumenta en actualidad que todo soporte ha sido absorbido por la tecnología.

1.9.1 Falsificación de correos electrónicos

El correo electrónico, también conocido como E-mail es definido por Pupo Martínez como: "*servicio de Red que permite a los usuarios enviar y recibir mensajes y archivos rápidamente mediante sistemas de comunicación electrónicos."* [28] Este es un servicio que se presenta en internet, con el fin de permitir a los usuarios el intercambio de mensajes a través de sistemas de comunicación electrónicos. Entre estos sistemas los más conocidos están: Gmail, Yahoo!, Outlook, que antiguamente fue conocido como Hotmail, entre otros. Estos permiten, no solo él envió de texto, sino, él envió de cualquier tipo de documento digital. Como imágenes, audios, videos, documentos como Word, PowerPoint, Excel, por mencionar algunos.

[28] EcuRed, Pupo Martínez Pavel David, Correo electrónico, Ecuador, 2010, Disponible en: https://www.ecured.cu/Correo_electr%C3%B3nico consultado: abril de 2019

La forma en que trabajan los correos electrónicos es similar al correo postal. Ambos permiten el enviar y recibir mensajes que llegan a su destino con la ayuda de una dirección.

Un correo electrónico, como una carta, se compone de varias partes. Estas son:

1. Destinatario: en este apartado, va colocado lo que será las direcciones de correo electrónico a las cuales se le será enviado el e-mail. Así como también presenta la opción de ocultar a los demás destinatarios, a quienes les fue enviado el correo electrónico.
2. Asunto: como el nombre lo indica, aquí se coloca de forma breve y concisa, el tema que trata el correo electrónico.
3. Mensaje: en este apartado, es donde se redactará el mensaje que se desea transmitir. Presenta distintas herramientas que facilitaran la escritura mediante la selección de tipo de letra, color, hipervínculos, entre otros.
4. Archivos anexos: entre las ventajas que presentan los correos electrónicos, es la de poder adjuntar distintos tipos de archivos, ya sean textos, hojas de cálculo, bases de datos, fotografías, audios, por mencionar algunos.

El o los destinatarios que reciban el correo electrónico, contaran con la posibilidad de poder responder al emisor, como poder archivarlo, guardar una copia local en el ordenador, así como poder borrarlo de forma permanente.

Pero así, como presenta ventajas, cuenta con desventajas como lo es la fácil falsificación de los propios correos electrónicos. Por lo cual los ciberdelincuentes, ven esto como una oportunidad. Aquí nace el también conocido phishing. Héctor Jara en el libro Ethical hacking 2.0 define el *término phishing, "en informática, denota un uso de la ingeniería social para intentar adquirir información confidencial, por ejemplo, contraseñas, cuentas bancarias, datos de tarjetas, etcétera, de manera fraudulenta."* [29] los ciberdelincuentes mediante la utilización de bancos de información, extraen grandes cantidades de direcciones de correo electrónicos, con el fin de enviarles un correo donde, mediante la utilización de la ingeniería social, como lo es el hacerse pasar por un familiar, una empresa, un empresario, llegan a solicitar información de relevancia como el número de una cuenta de banco, una contraseña o cualquier

[29] Jara, Héctor y Federico Pacheco*. tóp.cit*, Pág. 300.

información personal. Engañando al destinatario, para que este brinde su información y posteriormente los delincuentes puedan usarla para su propio beneficio.

El origen del término phishing que significa pesca en español, hace referencia al intento de hacer que los usuarios muerdan el anzuelo para que brinden la información personal.

Al enviar estos correos electrónicos, también se estarían enviando detalles del destinatario como del remitente. De estos datos, es de donde el perito informático podrá verificar si el correo a analizar es verídico o si, por el contrario, es falsificado.

Para conocer el modo de reconocer el origen de un correo electrónico, se debe conocer lo que son los DNS (Domain Name System), en español sistema de nombres de dominio. Dentro de los DNS que, en sí, "*guían la información de manera que indican hacia qué servidor se debe encaminar la consulta para poder mostrar la información que se ha pedido, o marcan la ruta de un correo electrónico hacia su destino."* [30]. Los dominios que normalmente conocemos como por ejemplo "miejemplo@hotmail.com", en la red se maneja con una serie de números separados por puntos, conocidos como IP (Internet Protocol) identificando a un servidor en la red. los DNS son los encargados de traducir los nombres de los dominios en las direcciones IP. "*El lugar donde se configuran las entradas DNS para cada dominio son los servidores de nombres. Los diferentes tipos de entradas de registro son registro A, registro CNAME, registro TXT, registro MX."* [31]

1. Registro A: este será el encargado de responder los dominios con las direcciones IP.
2. Registro CNAME: "*Un CNAME o registro de Canonical Name es un tipo de registro que puede encontrarse en un DNS y que permite al usuario especificar el alias de un nombre de dominio.*" [32] este tendrá a cargo los subdominios o también conocidos como alias, esto es importante en el campo del Hacking, para determinar que servidor atacar.

[30] Hostinet, ¿Qué son los DNS y que registros existen?, España, 2017, Disponible en: https://www.hostinet.com/formacion/general/que-son-dns-tipos-registros/ consultado: julio de 2019
[31] *Loc. Cit.*
[32] InternetLab, Filippi Simone, ¿Qué es CNAME y para qué sirve?, España, 2010, Disponible en: https://www.internetlab.es/post/972/que-es-cname-y-para-que-sirve/ consultado: agosto de 2019

3. Registro MX: "*El Registro MX (Mail Exchanger Record) es el registro que permite la recepción de correo. Especifica los servidores de correo que tiene el dominio."* [33] Este identifica el servidor del correo entrante, quiere decir que si una persona indica cuál es su registro MX, significa que ese será el servidor al cual entraran los correos electrónicos, sin embargo, no significa que ese servidor enviara correos en nombre de la persona. Que es un error bastante común, ya que se llega a asumir erróneamente que el servidor que recibe puede enviar.
4. Registro TXT: "*SPF es el acrónimo de Sender Policy Framework, una protección contra la falsificación de direcciones en el envío de correo electrónico. Identifica a los servidores de correo SMTP autorizados para el transporte de los mensajes a través de los registros de nombres de dominio (DNS)."* [34] también conocido como registro SPF, que indica cual es el servidor que se ha llegado a autorizar para enviar correos.

Esto es importante, ya que para verificar correos electrónicos y determinar si un correo es falso o es verdadero, se debe basa en los DNS y conocer los distintos registros. *"Con la información del encabezado técnico podemos verificar el origen del mensaje enviado, buscando con el número IP registrado el dominio de donde se originó el mensaje. Para eso se utiliza una interfaz, ¿"WHOIS?" que significa "¿Quién es?", para determinar el servicio utilizado, ubicar la dirección geográfica de los servidores y los puntos de contacto, y localizar (a veces) la instalación donde se encuentra un computador."* [35]

El análisis formal de un correo electrónico se hace de la siguiente forma:

1. Se debe conocer las cabeceras del correo electrónico, sin importar que sea Hotmail, Yahoo!, Gmail, entre otros, todos permitirán la revisión de estas.

[33] CDmon, como configurar el registro de correo o registro MX, España, 2018, Disponible en: https://ticket.cdmon.com/es/support/solutions/articles/7000006119-c%C3%B3mo-configurar-el-registro-de-correo-o-registro-mx consultado: agosto de 2019

[34] CDmon, Cómo configurar el registro SPF para el correo en el DNS estático, España, 2017, Disponible en: https://ticket.cdmon.com/es/support/solutions/articles/7000006117-cómo-configurar-el-registro-spf-para-el-correo-en-el-dns-estático consultado: julio de 2019

[35] Organización de los estados americanos, Manual de Manejo de Evidencias Digitales y Entornos Informáticos, 2011.

Outlook, Yahoo!, Gmail, en la parte derecha del correo entrante, existe la opción de “Mas”, una vez seleccionada, aparecerá la opción de “ver original” o “ver origen del mensaje”.

El cliente de correos Gmail, llega a interpretar todo lo expuesto en la cabecera, siendo el único que lo realiza. Llegando a mostrar directamente los registros SPF, MX y TXT. Mostrando que servidor fue el que lo envió. De lo contrario se deberá buscar detenidamente dentro de listado, la información referente con SPF, como se muestra a continuación:

“Authentication-Results: spf=pass (sender IP is 205.218.20.104)”

2. Cuando veamos un comando parecido al escrito anteriormente, aparece cual es el servidor que lo envió, señalando concretamente la IP de ese servidor, el cual es: 205.218.20.104. hasta aquí se lleva el cincuenta por ciento del trabajo hecho, el otro cincuenta por ciento, consta de revisar públicamente que indica esta IP.
3. El siguiente paso será dirigirse a una página que permita ver la información del SPF, esto se hará para poder ver que IP pueden enviar a nombre del correo electrónico de interés. Son varias páginas que serán de ayuda para esto, como lo son MXToolBox (https://mxtoolbox.com/) o Kitterman (www.kitterman.com/), por mencionar algunos. Para ejemplificar utilizaremos MXToolBox.

   Dentro de la página se seleccionará “SPF Record Lookup”. Dentro de la casilla se colocará la dirección del correo que se desea conocer el IP correspondiente. Seguidamente, se desplegará una lista con información correspondiente, donde mostrará una casilla con la denominación de SPF:

   “v=spf1 ip4: 205.218.20.104/25”.

Este IP debe concordar con el IP que se consiguió al inicio desde la cabecera del correo electrónico. Si llegan a ser la misma dirección, se estaría verificando que el correo que fue enviado, es completamente real y autentico.

Si en determinado caso, no llegase a desplegar el registro SPF, significaría que cualquier persona podría falsificar el correo electrónico. Esto en caso de llegar a juicio, puede complicar la situación, debido a que no se puede verificar la autenticidad del correo, existiendo la duda razonable dentro del caso.

Por eso, se debe prevenir a los clientes y poder asesorarlos en ese sentido. El no tener registrado el SPF, complica la tarea del perito informático. ya que, en el juicio, a la contraparte le beneficia ese desconocimiento.

Pueden existir varios registros SPF autorizados para enviar correos electrónicos a nombre de un dominio. De aquí, se desglosa lo que se denomina como Regla dura. Si al final de los registros SPF, aparece un "-all" significa que solo estarán autorizados las IP que aparecen anteriormente. Si llegase a recibir un correo electrónico que no es proveniente de ninguno de los IP mencionados, estos serán directamente eliminados por parte del cliente de correos.

"Si en caso, al final de los registros SPF, aparece "~all" o el signo "?", se le denomina como regla suave. Esto significa que, si se llegase a recibir un correo electrónico que no es de ninguno de los dos, es posible que sea autentico, pero aplicando las políticas anti-spam por parte del cliente del correo electrónico."[36]

Un punto muy importante a considerar en torno a los correos electrónicos, es que, para presentarlos en un juicio, se debe hacer mediante orden judicial; para presentarlo de forma directa, se debe ofertar el ordenador como evidencia, y ya con esto, el perito informático designado frente a juez, se encargará de peritar el correo electrónico. Ya que, de otra forma, se puede incurrir en delito al violentar la privacidad del dueño del correo.

1.9.2 Suplantación de identidad

Acá es de gran ayuda el servicio: Who Is? La cual su dirección es la siguiente: www.whois.domaintools.com. Esta ayudara en conocer quien registro un dominio, es decir una página web. en los casos que sería de ayuda este servicio, sería que, en el sector privado, un cliente llegue con el caso que tiene una empresa registrada como "Panadería El Éxito" pero existe una página web denominada como "PanaderiaElExito.com.gt" que se hace pasar por la empresa del cliente. Tiene una cuenta bancaria distinta a la del dueño de la empresa, y esta está recibiendo pagos en su nombre. Pero el cliente no tiene relación alguna con la página. Por lo que están

[36] Symantec, Implementar registros SPF en Email Security.cloud, España, 2017, Disponible en: https://support.symantec.com/es/es/article.tech226211.html consultado: julio de 2019

suplantando su identidad. Nos interesa saber quién es la persona que está detrás de esta página web.

Pablo García menciona que *"En primer lugar hay que indicar que ICANN es una organización sin ánimo de lucro y por lo tanto está regulada por la legislación de este tipo de organizaciones. Es la encargada de coordinar el sistema de nombres de dominio (DNS), aunque debido a las altas dimensiones de la tarea se delega en otras organizaciones."* [37] Hay que tener claro que, a nivel internacional existen dos entidades que pueden registrar dominios.

- ICANN: esta es una entidad que opera a nivel internacional. El significado de las siglas es "Internet Corporation for Assigned Names and Numbers", su traducción en español es Corporación de internet para la asignación de nombres y números. Esta se encarga de la venta de los dominios. "*Estos dominios se venden a través de un gran número de "registradores", que pueden estipular libremente el precio de sus servicios, aunque en cada caso pagan una cuota fija por dominio al registro concreto bajo cuyo nombre está registrado el dominio*." [38] Por lo que esta sería la única entidad internacional que puede registrar dominios: .com, .net, .info, entre otros.
- NIC: Network Information Center, registro de nombres de dominio en español. Esta es la "*única entidad encargada de mantener el registro de nombres de dominio de Internet con el código de país asignado*" [39] existe un NIC en cada país, ya sea NIC México, NIC Argentina, NIC Guatemala. Por lo que estaría la encargada de brindar los dominios con terminación ".gt". en el caso de Guatemala. La ICANN fue la responsable de crear al NIC de cada país. Buscando que estuviese bajo el control de una universidad, con el objetivo de que fuese una entidad neutral, en caso de que al gobierno no le gustase un dominio, no pudieran censurarlo. En el caso de NIC Guatemala, se encuentra bajo control de la universidad Del Valle.

[37] Nerion García, Pablo, ¿Qué es y cómo funciona ICANN?, España, 2017, Disponible en: https://www.nerion.es/blog/que-es-y-como-funciona-icann/ consultado: julio de 2019

[38] Sitio de la ICANN y su comunidad regional, sobre ICANN, Estados Unidos, 2018, Disponible en: http://icannlac.org/sobre-ICANN consultado: agosto de 2019

[39] Registro de dominios GT, Universidad del Valle, sobre nosotros, Guatemala, 2018, Disponible en: https://www.gt/sitio/us.php consultado: agosto de 2019

Si en caso, esta suplantación de identidad se llevara a juicio, se debe ir directamente hacia la entidad ICANN para requerirle la información de quien es la persona que está detrás del dominio que sea de interés. Esta requerirá que se le comprueba la veracidad del juicio. Por lo que puede llegar a solicitar que se le envié escaneada la demanda o que se envié de forma física el expediente del caso. La forma de participación es muy colaborativa. Aunque siempre existe la opción que mediante orden de juez puede brindar la información.

Cuando alguien adquiere un dominio, tiene la opción de que por un aporte económico extra puede llegar a ocultar los datos personales de la persona y que aparezcan a nombre de la empresa que registro el domino. Esto es conocido como Who Is privado. Si este fuese el caso, la ICANN tiene las facultades de exigirle a la empresa que haya registrado el dominio, de requerirle la información del dueño legitimo del dominio. Si en algún caso la empresa se llegara a rehusar, ICANN puede quitarle la facultad de registro de dominios a la empresa. Situación que no le conviene a la empresa. Por lo cual la empresa brindara los datos como el nombre del dueño, así como país donde reside, tarjeta de crédito que haya utilizado y toda información relacionada.

1.9.3 Geolocalización de dirección IP

En el caso que se quiera determinar la geolocalización de la dirección IP, se debe acudir al sitio de LACNIC este es "*el Registro de Direcciones de Internet para América Latina y el Caribe, es una organización no gubernamental internacional establecida en Uruguay en el año 2002. Es responsable de la asignación y administración de los recursos de numeración de internet (IPv4, IPv6)"*[40] a este, se procederá a solicitar el proveedor de direcciones IP, así como domicilio de la cuenta a la cual fue asignada. Debido a que las direcciones IP trabajan de forma dinámica, es decir, no siempre tendrá asignada la misma dirección al conectarse a la red, por lo que, el informático forense deberá anotar la fecha, hora y zona horaria, para poder determinar el domicilio que tenía asignada la IP en ese momento.

[40] Lacnic, Société Générale de Surveillance, Acerca de Lacnic, Caribe, 2017. Disponible en: https://www.lacnic.net/966/1/lacnic/acerca-de-lacnic consultado: agosto de 2019

Seguidamente ya se podrá constatar que efectivamente existe el domicilio, ya sea realizada por miembros del ministerio Publico o mediante la utilización de sistema informático de Google Street View.

Posteriormente se podrá solicitar a juez competente una autorización para la realización de allanamiento en el domicilio, con el objetivo de obtener todos los dispositivos electrónicos que podrían ser de ayuda para aclarar el hecho realizado.

1.9.4 Zona H

"Zone-h es un repositorio que contiene más de dos millones de copias de web defacements de todo el mundo. Así se llama a la acción de entrar ilegalmente en un sitio y cambiar su portada, poniendo textos reivindicativos o, simplemente, una pintada." [41] Esta es una página web que funciona como el salón de la fama de los Hackers, ya que cuando un atacante consigue el control de una página de internet, se dirige al sitio web Zona H y reporta el hackeo que acaba de realizar. Esto muchas veces son ataques al azar, al ser páginas web con un diseño simple que puede ser bastante vulnerable.

Depende del objetivo del hacker puede que solo afecte la estructura de la página web, buscando humillar, pero un buen hacker lo que busca es pasar desapercibido porque no busca que se le cierre el acceso, pudiendo estar todo el tiempo en el sistema para poder sustraer información sensible de la empresa.

Esto es de ayuda en el entorno forense ya que, al momento de llegar un cliente con un caso donde su página web fue hackeada, se puede proceder a ver en Zona H, si esa página web ya fue reportada como hackeada, ya se conocerá quien fue el hacker que realizo el ataque, siendo el mismo que realizo el reporte. Si no fuese ese el caso, podría tratarse de un hackeo enfocado.

[41] El País, Hackeada Zone-h, la principal base de datos de páginas 'hackeadas', España, 2017. Disponible en: https://elpais.com/diario/2007/01/18/ciberpais/1169091332_850215.html consultado: agosto de 2019

1.10 Criptografía

Graciela Marker redactora de Tecnología & Informática describe la Criptografía como *"la ciencia y arte de escribir mensajes en forma cifrada o en código. Es parte de un campo de estudios que trata las comunicaciones secretas. Los métodos de criptografía actuales son seguros y eficientes y basan su uso en una o más llaves."*[42]

Para la informática forense es de vital importancia este apartado, ya que dé el, podremos rectificar que la evidencia no ha sido manipulada desde el momento de su recolección hasta la presentación ante una corte judicial, gracias a los algoritmos Hash.

"*tendremos un mensaje en texto plano, que es la información que queremos almacenar o bien transmitir; la clave, que dependiendo del tipo de algoritmo pueden ser dos, una para cifrar y otra para descifrar; el algoritmo de cifrado, encargado de llevar adelante los procesos de cifrado y descifrado; y finalmente, un mensaje cifrado, que es la información en texto plano luego de haber pasado por el proceso de cifrado. En el caso de una transmisión entre dos puntos, una vez que el receptor recibió el mensaje, se produce el proceso inverso y se obtiene, finalmente, el mensaje en texto plano*."[43]

Es un campo muy amplio, que durante el proceso forense se encontrara bastantes cuestiones criptográficas. Un ejemplo de esto es cuando tenemos un texto plano, al agregarle un algoritmo o una clave, esta pasara a estar a ser un texto cifrado. Este texto solamente podrá ser leído por los que tengan la clave, que abrirá el algoritmo para volver a obtener el texto plano.

1.10.1 Firma Hash

El director del departamento de seguridad TI en Sidertia Solutions, Juan Luis García Rambla explica que *"Esta funcionalidad permitirá verificar que origen y destino son idénticos, dando así validez a la prueba. Se garantiza que las copias son idénticas y válidas. Así en la presentación de conclusiones partiendo de las evidencias adquiridas,*

[42] Tecnología & Informática, Graciela Marker, ¿Qué es la Criptografía?, España, 2016, Disponible en: https://tecnologia-informatica.com/que-es-la-criptografia/ consultado: abril de 2019
[43] Rivero, Franco. *óp. cit*, Pág. 253.

podrán reproducirse si se dieran las circunstancias." [44] Estos a diferencia de los otros algoritmos criptográficos, donde se pueden cifrar o descifrar, el algoritmo Hash es conocido como de una sola vía, esto significa que, a partir del hash, nunca se podrá llegar al archivo original. Donde al archivo de entrada se le aplica una función de hash y se obtiene un valor o un Hash. Este valor será hexadecimal y finito. Si al archivo de entrada se le agrega o modifica un dato, por más mínimo que sea y aplicando la misma función hash, dará un valor hash completamente distinto al anterior.

La importancia del algoritmo hash dentro de las practicas forenses, es que con esta función se puede asegurar la integridad de la evidencia. De esta manera el perito puede llevar los dispositivos desde el momento en que se realizó la adquisición hasta el momento de la entrega del informe pericial, asegurando que es la misma evidencia presentada de la adquirida a la presentada.

"Una propiedad fundamental del hashing es la que dicta que, si dos resultados de una misma función son diferentes, entonces las dos entradas que generaron dichos resultados también lo son "[45] Esto lo podremos ver como un sello, siendo visible que, si es cambiado un solo byte de información del volumen original de la copia forense, el Hash cambiara completamente. Por este medio se puede demostrar técnicamente que no ha sido modificada. Por lo tanto, se garantiza que este es totalmente igual a la evidencia que se llegó a encontrar en la escena del crimen.

Xiaoyun Wang en el artículo de como romper un MD5 y otras funciones Hash, menciona que los algoritmos conocidos como el MD5 y SHA1, se consideran como rotos, ya que ya existen métodos para poder falsificar el valor hash de estos dos algoritmos. Varias universidades han elaborado artículos científicos donde se comprueba que dos imágenes completamente distintas pueden tener la misma firma digital.[46] Los recomendados a utilizar son SHA256 y SHA512, puesto que llevan más caracteres dentro de la firma y por ende, es más complicado llegar a romperlo.

Actualmente los Hash utilizados en el medio judicial guatemalteco, son MD5 y SHA1. Estos no ofrecen tal integridad como deberían. Esto es de relevancia, ya que da

[44] García Rambla, Juan Luis. *Un forense llevado a juicio*, España, Creative Commons, 2014, Pág. 15.
[45] Rifa Pous, Helena y otros*. óp.cit., Pág* 26.

[46] Wang, Xiaoyun. "How to Break MD5 and Other Hash Functions", China, 2004, Shandong University.

abertura a la duda razonable de que si el Ministerio Publico obtuvo una copia forense con la firma digital MD5, la contraparte puede alegar que sea rechazado el medio de prueba ya que la firma es obsoleta, donde universidades han explicado claramente que dos archivos completamente distintos pueden tener la misma firma digital, esto significa que en algún momento de obtener la evidencia, pudo haber sido sembrado elementos incriminatorios en la copia forense sin que se llegase a alterar la firma digital, con el fin de acusar injustamente al sindicado. Por lo cual el caso judicial podría darse de baja.

Montoya Rojas menciona que *"Adicional a los algoritmos de hash hay otra clase de algoritmos que también pueden ser utilizados para el análisis de datos, pero que quizás su forma de uso es más compleja y trae el mismo resultado, son igualmente confiables, es por esto que los algoritmos de HASH son la herramienta más usada en seguridad informática a lo largo del mundo"* [47]

MD5 son 32 caracteres hexadecimales, SHA1 son 40 caracteres, SHA2 son 64 caracteres, esto quiere decir que, aunque el disco duro sea de 1 Terabyte, de 1Megabyte, la firma digital siempre contara la misma cantidad de caracteres, según sea el caso.

[47] Montoya Rojas, Alejandra. "La informática forense como herramienta para la aplicación de la prueba electrónica", *Revista CES*, vol.1, núm. 1, Colombia, 2010, pág. 11.

CAPÍTULO II:
EVIDENCIA DIGITAL Y SU PROCESAMIENTO

2.1 Recolección Evidencia Digital

Lucas Paus redacta en la web We live security lo siguiente*: "nos ayudan a mantener un estudio estructurado, facilitando la verificabilidad, la reproducibilidad del análisis."* [48] Estas serán todos los pasos que los peritos informáticos deberán tomar en cuenta para mantener la idoneidad del procedimiento forense. La informática forense consta de fases, las cuales deben seguirse de manera cronológica.

Entre el método de recolección, se encuentran señalados en el Manual de Manejo de Evidencias Digitales y Entornos Informáticos; Pautas para la identificación, recolección, adquisición y preservación de evidencia digital y Pautas para la recopilación de evidencia y archivos. entre algunos de los puntos en común que recalcan estos 3 manuales son los siguientes:

1) Colocarse guantes.
2) Fotografiar la escena, así como filmar todos componente que se encuentre dentro del área de inspección.
3) Fotografiar los dispositivos, desde vista frontal, lateral y posterior. Números de serie, periféricos y etiquetas que posean.
4) Elaborar un listado que lleve el control del hardware recolectado y detallando: tipo, marca, serie y estado en el que se encuentra.
5) Elaborar el croquis de la escena, colocando la ubicación donde se hallaron los dispositivos para que, si fuese necesario, posteriormente se pueda recrear el escenario mediante infografía forense.

Entre los materiales que se deben tener previamente preparados, se mencionan algunos:

1) Cinta de embalaje.
2) Cajas de cartón de distintos tamaños.
3) Discos duros vacíos.
4) Disco duro con las herramientas forenses.

[48]We live security, Paus Lucas, 5 fases fundamentales del análisis forense digital, España, 2015, Disponible en: https://www.welivesecurity.com/la-es/2015/04/15/5-fases-analisis-forense-digital/ consultado: abril de 2019

5) Cámara fotográfica.
6) Etiquetas.
7) Bolsas Faraday.
8) bolsas antiestáticas.

2.1.1 Identificación y registro

"*En esta fase se obtienen copias de la información que se sospecha que puede estar vinculada con algún incidente. De este modo, hay que evitar modificar cualquier tipo de dato utilizando siempre copias bite a bite con las herramientas y dispositivos adecuados. Cabe aclarar este tipo de copia es imprescindible, debido a que nos dejara recuperar archivos borrados o particiones ocultas, arrojando como resultado una imagen de igual tamaño al disco estudiado."*[49] Como en toda escena del crimen, se debe realizar la adecuada identificación, anotando las características físicas, y el número de serial, en el caso que este fuese visible, el sistema operativo o sistema de archivos, ya sea un ordenador o un disco duro, según sea el caso. Posteriormente se realizará una copia bit a bit al dispositivo y seguidamente se calculará el valor hash del mismo. Para garantizar que la copia es idéntica a la evidencia recabada. Para así poder trabajar sobre esta y evitar alterar la evidencia original. Así mismo, poder recolectar entrevistas con los administradores de los sistemas y personal si fuese realizado en una empresa.

Tomar en cuenta la toma de datos volátiles, la obtención de hora y fecha del sistema, ficheros que sean relevantes, si existiesen, la obtención de copias de seguridad del sistema, así como todos los registros de los routers, servidores, VPN.

También se debe tomar en cuenta que tipo de delito se va a actuar, ya que no es lo mismo analizar un caso investigado por homicidio que uno de fraude. En determinado caso fuese el delito de fraude, se deberá dar mayor énfasis documentos de ofimática, impresoras, scanner; en casos de pornografía infantil, se le podría dar mayor importancia a objetos como las cámaras digitales.

[49] *Loc. Cit.*

"Establecer qué es relevante. En caso de duda es mejor recopilar mucha información que poca." [50] Otro punto a considerar, será la recolección exclusivamente de información que será de ayuda en la resolución judicial, para que, en lugar de copiar la totalidad de los datos, sea solo una porción de esta, ahorrando tiempo y gastos económicos que puede generar esto.

2.1.2 Protección del dispositivo

"*En esta etapa se debe garantizar la información recopilada con el fin de que no se destruya o sea transformada. Es decir que nunca debe realizarse un análisis sobre la muestra incautada, sino que deberá ser copiada y sobre la copia se deberá realizar la pericia."* [51] Esta será una fase muy importante, ya que, si no se llegase a preservar de manera correcta la evidencia, se puede caer la investigación o que estas no sean admitidas en un tribunal. Hay que llevar el control de la cadena de custodia anotando el lugar, fecha y técnicos que estuvo a cargo de la misma, para garantizar la seguridad, preservación, autenticidad e integridad de los elementos materiales recolectados. Existe la norma de carácter internacional RFC 3227. Di Lorio explica que "*este documento, uno de los primeros en ser adoptados por la comunidad de informática forense, es una guía general para recolectar y almacenar información relacionada con incidentes. Propone una serie de buenas prácticas para determinar la volatilidad de los datos, decidir qué recolectar, como efectuar la recolección y determinar de qué manera almacenar y documentar los datos, considerando muy pocos aspectos legales, que naturalmente, son particulares del ordenamiento legal de cada país"* [52] señala las directrices a seguir para la recopilación de evidencias y su almacenamiento. El cual se analiza a lo largo de este capítulo.

Es recomendable la toma de fotografías de todo el sistema, así como en lugar donde se encuentran. Seguidamente podrá darse inicio a la realización de la copia bit a bit de los dispositivos de almacenamiento. Al tener la copia forense, se procederá a

[50] The Internet Society, RFC 3227, Pautas para la recopilación de evidencia y archivos, 2002.
[51] *Loc. Cit*.
[52] Di Lorio, Ana Haydee. *óp.cit*, Pág. 276.

realizar la verificación del número Hash con la evidencia original sean idénticos, comprobando la integridad de los datos.

2.1.3. Recopilación para el acceso a los dispositivos de almacenamiento volátil

La volatilidad es sobre la relación a la cantidad de tiempo en la que se encuentre disponible cierta información, por lo que, cuando se denomine volátil a los datos, es porque el tiempo de disponibilidad será corto. En el manual de Pautas para la recopilación de evidencia y archivos producido por Internet Society, menciona que *"Al recopilar pruebas, debe pasar de lo volátil a lo menos volátil. Aquí hay un ejemplo de orden de volatilidad para un típico sistema.*

1. *registros, caché.*
2. *sistemas de archivos temporales.*
3. *logs del sistema.*
4. *configuración física.*
5. *Documentos."*[53]

Este es seria un orden recomendado para la recopilación de los datos que contenga un ordenador. Por lo cual se le debe dar prioridad a la memoria RAM, que es la que contendrá toda la información volátil como los registros, cache, los archivos temporales, por lo que lo que, el primer paso a realizar, si se encontrase el ordenador encendido seria realizar un volcado de memoria RAM.

En el caso de la memoria RAM hace mención en las pautas para la recopilación de evidencia y archivos lo siguiente*: "No cierre hasta que haya completado la recopilación de pruebas. Se puede perder mucha evidencia y el atacante puede haber alterado el Inicio / apagados, scripts / servicios para destruir la evidencia."*[54]

Si el dueño del ordenador fuera "paranoico" y utiliza el programa CCleaner. Lo que hace este software es poder, mediante la modificación de los parámetros, realizar borrados a bajo nivel, cuando se apague el equipo de cómputo. Si el investigador recurre al apagado normal del computador, podría estar corriendo una de las tantas

[53] The Internet Society, RFC 3227, Pautas para la recopilación de evidencia y archivos, 2002.
[54] loc.cit.

herramientas que pueden alterar por completo la información. Siendo ese el motivo de que nunca se debe apagar el equipo de cómputo de forma completa.

Ejecutar un intérprete de comandos confiables. Estos deben ser portables, para que, a la hora de utilizarlos, no contaminen la evidencia. Arrellana recalca los siguientes puntos:

1. *"Registrar la fecha, hora del sistema, zona horaria.*
2. *Determinar quién o quiénes se encuentran con una sesión abierta, ya sea usuarios locales o remotos.*
3. *Registrar los tiempos de creación, modificación y acceso de todos los archivos.*
4. *Verificar y registrar todos los puertos de comunicación abiertos.*
5. *Registrar las aplicaciones relacionadas con los puertos abiertos.*
6. *Registrar todos los procesos activos.*
7. *Obtener y examinar la información contenida en la memoria RAM del sistema."*[55]

Un dato importante en el caso de encontrarse con un computador con sistema operativo Linux con la actualización del kernel 2.4, aunque se consiga permisos de superadministrador o sea el usuario root, el sistema bloquea a nivel kernel, acceso al archivo "/MEM", por lo que la explicación técnica es que no se puede realizar un volcado de memoria en Linux con esas actualizaciones y posteriores.

"No confíes en los programas del sistema. Ejecute su evidencia Recopilación de programas de medios adecuadamente protegidos."[56] nunca habrá que utilizar ningún programa del ordenador, aunque nos fuese de ayuda. Lo recomendable es portar siempre un disco duro con todas las herramientas forenses en calidad de portable, por dos motivos: que seamos lo menos intrusivos en el sistema, para que no se llegue a alterar la evidencia y que puede existir el caso que el usuario del ordenador haya modificado previamente los softwares en el mismo. Esto nos puede arrojar resultados completamente distintos a los reales.

1) Programas para listar y examinar procesos.

---

[55] Arellano, Luis Enrique. *"*La cadena de custodia informático-forense*"*, *Revista Activa, S*/V, núm. 3, Colombia, Tecnológico de Antioquia, Pág. 70.

[56] The Internet Society, RFC 3227, Pautas para la recopilación de evidencia y archivos, 2002.

2) Programas para examinar el estado del sistema.
3) Programas para realizar copias bit a bit. [57]

2.1.4. Posibles estados que se puede encontrar el ordenador

En la escena donde se llevaron a cabo los delitos, puede encontrarse el equipo de cómputo de dos formas, cada una de estas tendrá su forma de proceder para mantener la integridad de la evidencia que posteriormente se presentará ante juez judicial. Estos estados son:

2.1.4.1 Encendido

Entre uno de los dilemas que se llegan a encontrar en la escena será la de apagar o no el equipo informático. Esto puede acarrear distintas consecuencias, ya sea perdida de información en la memoria RAM, los usuarios conectados, procesos que se estén llevando a cabo, entre otros. La forma valida de apagar el equipo de cómputo es desconectando todos los cables.

Se tiene la creencia que al desconectar la corriente eléctrica del computador, esto puede ser perjudicial para el mismo, pues no es así. los discos duros están hechos para soportar variaciones de voltaje. Por lo que esta es la mejor forma de mantener a salvo los datos.

Si el computador tuviese un sistema de cifrado como lo son BitLocker, truecrypt, veracrypt, por mencionar algunos. Todos realizan lo siguiente: un disco duro cuando es cifrado, físicamente este encriptado. Cuando es iniciado el sistema operativo, este pide contraseña para poder descifrarlo. Cuando se procede a ingresar la contraseña, el computador procede a crear un disco duro virtual descifrado, pero físicamente el disco duro sigue estando cifrado. Esto es así para evitar tener que cifrar y descifrar el disco una y otra vez, acción que, dependiendo el tamaño del disco duro, podría tardar horas o incluso días.

Si el computador de interés está encendido, naturalmente el disco duro virtual estará descifrado, por lo cual es el momento indiciado para proceder a realizar una copia forense al disco duro.

---

[57] *Loc. Cit*.

2.1.4.2 Apagado

Si en la escena, el computador se encuentra apagado, al realizar la recolección de evidencia se deberá trabajar con dispositivos de arranque con el modo de "Solo lectura" para que no sobrescriba datos sobre la evidencia.

Al momento de tener que desconectar el equipo, si el caso fuese de una laptop, notebook o un teléfono celular, habrá que desmontar la batería del mismo, con el objetivo que este no se encienda de forma accidental.

2.2 Copia forense

En los delitos informáticos nunca se trabaja sobre el medio físico, ya que se debe de salvaguardar la integridad de este, por lo cual se le debe realizar una copia desde el primer hasta el último sector de un dispositivo, lo cual realizará un espejo de un disco duro, de una USB, de un teléfono celular, a modo que lo mismo que se encuentra en el dispositivo, se tenga acceso desde un archivo, este archivo es lo que denominará copia bit a bit, copia forense o imagen forense.

La Asesora jurídica en Corporación Tecnnova, Alejandra Montoya Rojas menciona que *"La copia bit a bit es una herramienta que originalmente no fue creada para ser utilizada por la informática forense, sino para la administración de sistemas y para hacer respaldo de datos, pero dados los resultados se comenzó a utilizar, específicamente el programa "dd" que permite hacer el proceso de copia de la información contenido en el medio de almacenamiento desde cualquier computador y tiene un porcentaje de efectividad del 100%."*[58]

Lo que consisten en sí, las copias forenses, es en realizar un respaldo de todos los archivos existentes en el medio de almacenamiento, tanto archivos como imágenes, videos, documentos, así como los archivos de programas y el sistema operativo en caso fuese copia de un ordenador. Existe la posibilidad de poder recuperar los datos que fueron borrados anteriormente, ya sea por accidente o intencionalmente. Este se realizará sobre otro medio de almacenamiento distinto, normalmente un disco duro,

[58] Montoya Rojas, Alejandra *óp. Cit.*, pág. 10.

por la capacidad de guardado que tienen. Así mismo, se certifica su contenido con una firma hash, para garantizar que es una copia y fiel y exacta del original.

García Rambla menciona que *"Existe para ello elementos hardware que permiten realizar estos procesos de forma cómoda, precisa y con altas garantías. Aunque no es la solución más económica si es la que ofrece mayor profesionalidad y seguridad para un analista forense."* [59] Hay que tomar en cuenta que no solamente se necesita del equipo forense en sí, también es de uso discos duros de gran capacidad para el almacenamiento de los datos, bloqueadores de escritura para que no se llegue a alterar la evidencia, cables y adaptadores, tomando en cuenta que en el mundo de los dispositivos de terminales móviles, no existe una estandarización como en los ordenadores de los conectores adecuados, estos pueden variar por marca y modelo. Entre los modelos hardware de creación de imágenes forenses encontramos LogiCube, Hard Copy 2, ImageMaster 3.

Arellano menciona que *"Es necesario tener en cuenta que un bit no es similar, sino idéntico a otro bit. De ahí que una copia bit a bit de un archivo digital es indiferenciable de su original, esto significa que no puede establecerse cuál es el original y cuál su copia, salvo que hayamos presenciado el proceso de copiado y tengamos conocimiento sobre cuál era el contenedor del original y cuál el de la copia".* [60] Esto presenta una ventaja ya que es posible mantener por completo la integridad del dispositivo original, así mismo se podría presentar cualquier copia ante el juzgado siempre que se verifique que la firma hash es la misma a la presentada inicialmente como evidencia. Con esto, a lo contrario a como se trabajaría con una pericial caligráfica en un documento, donde el perito solamente puede realizar su informe basado en originales. En las evidencias digitales, se puede realizar la pericial sin ningún inconveniente.

Los pasos a seguir para realizar una imagen forense al disco duro de un ordenador, será el siguiente:

1) Se desconectará la fuente de poder del equipo de cómputo.

[59] García Rambla, Juan Luis. óp. Cit., Pág. 11.
[60] Arellano, Luis Enrique. *óp. Cit.,* Pág. 70.

2) se retirarán del computador cualquier disco, USB o medio de almacenamiento externo que se encuentre conectado.
3) Descargar la propia electricidad estática, tocando alguna parte metálica y abrir el gabinete.
4) Desconectar la conexión con la que cuenta el disco duro, puede ser IDE o SCSI.
5) Desconectar la alimentación eléctrica del disco duro.
6) Conectar el dispositivo que se utilice como destino para hacer la duplicación del disco rígido este debe ser de tamaño superior al disco original.
7) Duplicar el dispositivo de los datos con la herramienta hardware o software seleccionada.
8) Realizar el algoritmo hash para verificar que la copia se ha realizado de forma correcta.
9) Un paso que recalca Luis enrique Orellano es el de realizar dos copias o más si fuese necesario, una se deja en el lugar del hecho, para permitir la continuidad de las actividades, otra copia se utiliza para el análisis en el laboratorio de informática forense y el original se deja en depósito judicial o si la pericia ha sido solicitada por un particular, registrarlo ante abogado y guardarlo, según lo indicado por el solicitante de la pericia y el abogado.[61]

Hay que tomar en cuenta que este es el paso más importante de la investigación electrónica, ya que, si se llegase a realizar mal esta, podría llegar a convertirse en inadmisible en el caso judicial.

Otro dato a tomar en cuenta, es que, en sitio, no se puede ir al ordenador y bajar las herramientas forenses, ya que se altera la evidencia de forma inaceptable. Por lo cual, lo que se debe hacer es llevar un disco duro en XFAT, ya que este es compatible con sistemas Mac, Windows y Linux. Esta es el mejor sistema de archivos. ¿Por qué no se puede llevar en Fat32? Esto porque el tamaño para copiar archivos esta limita a 4Gigabytes, y si el volcado de la maquina es de mayor a 4Gygabytes, no se puede llevar la copia en ese disco duro.

[61] Arellano, Luis Enrique. *óp. cit*, Pág. 75.

2.3 Embalaje y traslado

Martínez Retenaga explica en su libro Guía de toma de evidencias en entorno Windows que *"Se debe almacenar la información en dispositivos cuya seguridad haya sido demostrada y que permitan detectar intentos de acceso no autorizados."* [62] *"recomendamos ir documentando todas las acciones, en lo posible, a medida que vayan ocurriendo. Aquí ya debemos tener claro por nuestro análisis qué fue lo sucedido, e intentar poner énfasis en cuestiones críticas y relevantes a la causa. Debemos citar y adjuntar toda la información obtenida, estableciendo una relación lógica entre las pruebas obtenidas y las tareas realizadas, asegurando la repetibilidad de la investigación."*[63] Esta documentación, será la que nos respaldará frente a un juzgado, en todas las acciones y metodologías que llevamos a cabo para el análisis digital, sin llegar en algún momento a alterar la evidencia.

Para proteger el equipo se deberá colocar en bolsas antiestáticas, dejando registradas en ellas toda información del equipo. el nombre y apellido del perito informático forense, así como su firma. En el caso de dispositivos celulares, estos deberán llevarse en bolsas Faraday. Estas bolsas Faraday están "*Pensadas para agencias de gobierno, militares e investigadores, estas bolsas de Faraday están especialmente diseñadas para la recolección, preservación, transporte y análisis de dispositivos móviles e inalámbricos. El material de estas bolsas forma un blindaje alrededor de teléfonos celulares, GPS, netbooks, dispositivos bluetooth, laptops, etc., bloqueando toda señal celular, WIFI o de radio."*[64] Evitar utilizar bolsas plásticas, ya que estas pueden generar estática que puede llegar a alterar o destruir los datos contenidos en los dispositivos.

Estos deberán colocarse en cajas rígidas, de preferencia que sean ligeramente más grandes que los equipos para evitar las áreas de espacio vacío. Seguidamente, estas cajas se deben colocar una caja que tenga la capacidad de contenerlas, esto, con el objetivo de mantener los elementos juntos, evitando confusión, separación o perdida.

---

[62] Martínez Retenaga, Asier. *Guía de toma de evidencias en entorno Windows*, España, Creative Commons, 2014, Pág. 18.
[63] *Loc. Cit*.
[64] División Forense, Bolsa de Faraday para dispositivos móviles, Argentina, 2015, Disponible en: https://www.division-forense.com/bolsa-faraday.html consultado: septiembre de 2019

Luego, se deberá rellenar el espacio restante con material que amortigüe. Se asegurará y se sellará la caja con cinta de embalaje.

El destino del traslado, del equipo será hacia la bodega del Ministerio público, posteriormente, se deberá hacer la solicitud hacia el Instituto Nacional de Ciencias Forenses para que realice el peritaje correspondiente.

2.3.1 Aislamiento del dispositivo de la red cableada e inalámbrica

Con respecto a la conectividad. Existe el concepto de que, si el equipo de cómputo está conectado a la red, un atacante externo se puede conectar y llegar a alterar toda la información. Esto es cierto, pero, existen herramientas hackers como Meterpreter o Armitage, con el que pueden tomar control de un computador, mediante archivos malintencionados, que pueden detectar cuando el computador esta Offline, si fuese así, se autodestruye, ya que ha sido programado para ello, debido a que puede ser investigado. Por lo que, en un escenario real, si el ordenador está conectado vía Ethernet o vía Wifi, de esa manera se debe dejar, procediendo seguidamente a buscar el Router, y a este se le debe desconectar de Internet ya que este es el encargado de asignarle la dirección IP al ordenador, y al ser desconectado de la red, no llega a modificar las IPs, por lo que el archivo malintencionado se sigue ejecutando esperando salida a Internet. En cambio, si se le desconecta la conectividad directa al ordenador, el archivo malintencionado puede detectarlo y autodestruirse.

En el caso de que lo que se necesite aislar de la red fuese un teléfono celular, se deberá almacenar en lo que se conoce como bolsa Faraday, para prevenir la interferencia de señales inalámbricas, para evitar el caso de que los propietarios de los mismos, no puedan realizar un borrado remoto de la información contenida en ellos.

2.4 Manejo evidencia digital en la cadena de custodia

Torales define la cadena de custodia como 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*" [65]

Es algo esencial dentro de la practica forense, ya que es la manera de asegurar que no se han llegado a alterar los dispositivos recolectados desde el momento de su adquisición hasta que son presentados ante un juez. Esta va a estar relacionada con los algoritmos Hash dentro de la cadena de custodia. se colocarán todos los valores hash de todos los dispositivos que se recolectaron para que, a la hora de estar frente al juez se pueda verificar que llegaron de forma íntegra.

Con la cadena de custodia se asegurará que pertenecen al caso investigado, sin que haya que sufrir alteraciones, modificaciones o sustracciones desde su inicio hasta la culminación del proceso. sí en determinado caso, se llega a especular que dicha cadena de custodia no se llevó a cabo siguiendo las debidas directrices, la contraparte o el mismo juez podría fácilmente descalificarla.

Debe estar identificado en todo momento quien lo ha tenido, para que lo ha tenido, cuanto tiempo ha dispuesto de la evidencia, así como el propósito de ello. Este será básicamente un documento donde se guarda un historial de la evidencia indicando en manos de quien ha pasado.

El Ingeniero en computación Jocsan Laguna Romero, menciona que en casos laborares, se puede contar también con un Abogado, para que, mediante actas, se deje constado, las acciones que se realizaron en el dispositivo informático para realizar la clonación del equipo, buscando garantizar la inviolabilidad de la toma de datos. *"Si esa información resulta vital, sería imprescindible contar con testigos que pudieran refrendar las acciones realizadas y que pudieran atestiguar que no se ha realizado ninguna acción enfocada a manipular datos, solo a extraerlos".* [66] En caso no se contará con el tiempo para contactar un notario, se podrían utilizar testigos, si fuese posible miembros de la empresa. Preparando un acta con el nombre y los cargos en

[65] Torales, Eloy E., *Manual de procedimiento para la preservación del lugar del hecho y la escena del crimen,* Argentina, Ministerio de Justicia y Derechos Humanos de la Nación, 2014, primera edición, Pág. 47.

[66] García Rambla, Juan Luis. *óp. Cit.*, Pág. 9.

la empresa de las personas que han estado presentes durante la labor del perito informático. Tomando en cuenta que siempre habrá que tener prevista una respuesta si en el juicio, fuesen cuestionadas las acciones realizadas.

Entre los puntos que habrá de dejar muy claro en la cadena de custodia, son los siguientes:

1) *"¿Dónde?, ¿cuándo? y ¿quién? descubrió y recolectó la evidencia.*
2) *¿Dónde?, ¿cuándo? y ¿quién? manejó la evidencia.*
3) *¿Quién ha custodiado la evidencia?, ¿cuánto tiempo? y ¿cómo la ha almacenado?*
4) *En el caso de que la evidencia cambie de custodia indicar cuándo y cómo se realizó el intercambio, incluyendo número de albarán, etc."*[67]

Ruth sala Ordoñez, una abogada penalista española especialista en Delincuencia informática menciona en conferencias, que cuando un abogado señala la cadena de custodia, en el aspecto de que no se ha tenido en cuanta algún detalle o parámetro, es porque en realidad, la parte atacante tiene bastante complicado el poder señalar la información, es que ya tiene pocas posibilidades de poder contrarrestar el peritaje por lo cual podríamos señalar que no tiene más cartas con las cuales jugar.

2.5 Análisis de la evidencia

En el manual Pautas para la recopilación de evidencia y archivos explica que el análisis de evidencia *"es la fase más técnica, donde se utilizan tanto hardware como software específicamente diseñados para el análisis forense. Si bien existen métricas y metodologías que ayudan a estructurar el trabajo de campo, se podrán obtener grandes diferencias dependiendo de las herramientas que se utilicen, las capacidades y experiencia del analista."*[68] Dentro de esta fase se incluye lo que es la recuperación de información, cuando está ha sido borrada o ha sido dañada, existen varios métodos con los cuales se puede llegar a recuperar información que ha sido eliminada de algún dispositivo ya sea intencional o accidentalmente. Ya recuperada la mayor cantidad de

[67] The Internet Society, RFC 3227, Pautas para la recopilación de evidencia y archivos, 2002.
[68] *Loc. Cit*.

información posible, se procederá a realizar el respectivo análisis, que es la parte más compleja, con la finalidad de encontrar evidencias tales como:

1. Archivos modificados.
2. Archivos con extensiones cambiadas.
3. Conversaciones de WhatsApp.
4. Fotografías eliminadas.
5. Documentos.
6. Videos.
7. Audios.
8. Otros.

En esta fase, el perito informático tendrá que utilizar sus conocimientos, experiencias e imaginación para poder recrear el incidente. Hay que tomar en cuenta que tipo de incidente es, para saber por dónde iniciar la investigación y nunca descartar una hipótesis por más obvia que sea. La metodología a utilizar dependerá de factores como: sensibilidad de la información, estado de los sistemas afectados, la habilidad del atacante, entre otros.

2.6 Presentación de la evidencia

una vez analizada la información que se ha obtenido siguiendo el orden de las distintas fases de la informática forense, deberá elaborarse un reporte donde quedará plasmado todos los hallazgos encontrados. *"Normalmente se suelen usar varios modelos para la presentación de esta documentación. Por un lado, se entrega un informe ejecutivo mostrando los rasgos más importantes de forma resumida y ponderando por criticidad en la investigación sin entrar en detalles técnicos."* [69] Este informe conocido como ejecutivo deberá presentarse con un lenguaje claro y entendible que es el que se le será entregado al cliente que haya requerido de los servicios forenses, para que, aun sin conocer la terminología informática, logre entender lo que ha sucedido.

"Un segundo informe llamado "Informe Técnico" es una exposición que detalla en mayor grado y precisión todo el análisis realizado, resaltando técnicas y resultados

[69] *Loc. Cit*.

encontrados, poniendo énfasis en modo de observación y dejando de lado las opiniones personales."[70] En este informe ya se procederá a describir el hecho de forma más técnica y precisa, explicando que metodología fue la que se empleó, los datos encontrados, forma en que se procedió a analizar los datos y software empleado a lo largo del análisis forense, se habla también de las firmas hash que aseguran la integridad de los archivos, con el objetivo que todo el proceso sea reproducible cuantas veces sea necesarias.

"Es necesario estar preparado para testificar, incluso es posible que el juicio o audiencia se lleva a cabo años después, describiendo todos acciones que tomaste y a qué horas. Las notas detalladas serán de vital importancia."[71] Tomando en cuenta que el tiempo que se alargue un proceso judicial, o puede que se decida proceder legalmente tiempo considerable después del incidente informático, hay que contar con bitácoras que anoten cada detalle y procedimiento que se haya realizado o recabado de la evidencia, por si en el debate, la contraparte quiera atacar alguna parte del procedimiento informático forense.

2.6.1 Consideraciones Legales

Como lo dicta los artículos 181 y 183 del Código Procesal penal, decreto 51-92 del Congreso de la Republica, las pruebas deben tener las siguientes características:

1. Legal: la prueba deber conseguirse por medio de procesos permitidos, de conforme a la ley, sin llegar a quebrantar ningún derecho que asegure la Constitución Política.
2. Útil: la prueba deberá ser de aporte para la averiguación de la verdad, brindando conocimientos referentes a lo que se pretenda probar.
3. No abundante: si se diera el caso que ya se propusieron varios medios de prueba que llegan a probar el mismo hecho, se le denomina prueba abundante, por lo que no es necesario proponer todos los medios, sino, solo los más relevantes.

[70] *Loc. Cit*.
[71] *Loc. Cit*.

4. Pertinente: esto hace relación a que los medios de prueba guarden relación entorno al caso que se esté llevando a cabo en un tribunal.
5. Objetiva: la prueba deberá ser imparcial y desinteresada. Siendo neutral y buscando lo justo.

A parte de estos requisitos, un tribunal pedirá que el inicio de la cadena de custodia se desde la creación de la imagen forense, que esta haya sido llevada a cabo sin contaminación alguna de la evidencia y así mismo, que cada evidencia extraída cuenta con su respectiva firma Hash. No existe un fundamento legal como tal en Guatemala, que regule como se llevara a cabo los procedimientos informáticos forenses, solamente se debe cuidar que como mínimo, se garantice que los hechos serán probables y reproducibles.

2.6.2 Imagen forense

En cuanto a imágenes forenses, se debe realizar varias copias, debido a que debe quedar almacenada una copia en la bodega del ministerio público para su resguardo para su posterior presentación si fuese necesario ante tribunal; la copia que se utilizara para el respectivo análisis forense llevado a cabo por el perito informático; una copia extra, para el perito, por si se llegase a presentar algún tipo de inconveniente con la copia anterior. Esta copia deberá quedar guardada en un dispositivo de almacenamiento de gran capacidad, como lo es un disco duro. Este debe ser descontaminado anterior a la creación de la imagen forense. Para, de esta forma, evitar que haya quedado restos de casos anteriores que se hayan presentado en el mismo.

2.6.3 Bloqueadores de escritura

Javier Alamillo explica que *“Una bloqueadora de escritura es una herramienta fundamental para el perito informático, ya que permite analizar un disco duro en modo de bloqueo de escritura, es decir, sin tener que preocuparse de que algún sector del disco pueda ser escrito accidentalmente, por lo que se mantiene la cadena de custodia*

durante el análisis forense del disco duro."[72] Un bloqueador de escritura cumple la función de impedir que se escriba datos nuevos sobre un dispositivo de almacenamiento, por lo que, aun después de haberlo analizado, debería mantener su integridad y por consecuente, su firma hash intacta.

2.6.3.1 Hardware

"Tras la conexión del disco duro a la bloqueadora de escritura y la posterior activación de ésta, es necesario seleccionar, bien el modo de lectura y escritura, bien el modo de sólo lectura, poniendo sumo cuidado en seleccionar este último para no escribir accidentalmente en el disco duro." [73] Usualmente, las conexiones que se utiliza es según la entrada del disco duro SATA, IDE y SCSI, esta es conectada hacia el bloqueador de escritura y está a la vez, mediante conexión USB, es conectada al ordenador en el cual se realizara el respecto análisis informático forense. Puede que el modo de solo lectura, sea mediante un puerto, a través de un botón dedicado o por medio de la selección en menú, si es que cuenta con una pantalla ya sea táctil o mediante cursores de desplazamiento. Por mencionar algunos hardware:

- FireFly Digital intelligence
- UltraBlock
- WiebeTech ComboDock V5
- Tableau Forensic Duplicator

2.6.3.2 Software

Existe las alternativas por medio de software igualmente confiable para uso, en cuanto a bloqueo de escritura se refiere. Estos bloquean la modalidad de escritura de los puertos USB del equipo de cómputo que se esté utilizando del laboratorio forense. Por lo que, al acceder a la evidencia, se estaría realizando en el modo "Solo lectura",

[72] Javier Rubillo Alamillo Perito informático, Análisis forense mediante bloqueo de escritura de un disco duro, 2016. Disponible en: https://peritoinformaticocolegiado.es/blog/caso-practico-de-peritaje-informatico-analisis-forense-mediante-bloqueo-de-escritura-de-un-disco-duro/ consultado: septiembre de 2019

[73] *Loc. Cit*.

evitando contaminar por error la misma. Esta opción viene incluida en las suites forenses que se trataran en el siguiente capítulo.

CAPÍTULO III:
HERRAMIENTAS FORENSES DE ANÁLISIS DIGITAL PARA LA OBTENCIÓN DE INFORMACIÓN.

3.1 Microsoft Windows

entre las herramientas que se podrá encontrar en el entorno del sistema operativo Windows, encontramos las siguientes herramientas, que son utilizadas por distintas empresas privadas de seguridad para resolver casos tanto a nivel judicial como empresarial.

3.1.1 Máquina Virtual

"Una máquina virtual es un equipo con software que, al igual que un equipo físico, ejecuta un sistema operativo y aplicaciones. La máquina virtual está compuesta por un conjunto de archivos de configuración y especificaciones, Además, cuenta con el respaldo de los recursos físicos de un host. Todas las máquinas virtuales tienen dispositivos virtuales que ofrecen la misma funcionalidad que un hardware físico, son más portátiles, más seguras y más fáciles de administrar". [74] La virtualización de una máquina es de gran aporte en materia forense, ya que la copia forense ya se podrá manipular montándola como una máquina virtual, teniendo así un entorno controlado. Cuando se virtualiza la copia forense, se cuenta con ventajas como el aislamiento completo para evitar que sea intervenido desde el mundo exterior, utilizar herramientas de extracción de información sin llegar a perjudicar el entorno real, buscar información de una forma más rápida y fácil como si se tratase de forma nativa, entre otros.

Para poder llevar acabo el montaje de una máquina virtual, se podrá recurrir a distintos softwares, en este caso, se empleará VMware Workstation para ejemplificar, los pasos a seguir, son los siguientes:

1. Hacer clic sobre la ventana "File" localizada en la parte superior izquierda, se desplegará una lista. Cliquear la pestaña "New Virtual Machine…".
2. Se utilizará la configuración "Typical (recommended)".

[74] VMware, VShere. *Administrar máquinas virtuales de vSphere*, España, VMware, Inc., 2009, Pág. 11.

3. En esta ventana, se podrá seleccionar levantar una máquina virtual desde un DVD o desde un archivo con extensión .iso, como lo es el caso de una imagen forense.
4. Seguidamente, se seleccionará el tipo de sistema operativo con el que cuenta la copia forense, ya sea Microsoft Windows, Linux, Solaris, entre otros, así como la versión del mismo.
5. Se ingresa el nombre con el que se guardará la máquina virtual, así como la ubicación donde este será alojado.
6. En la siguiente ventana, se designará la capacidad del disco para la máquina virtual, aquí no será necesario designarle una cantidad mayor a la de la copia forense, ya que el objetivo es realizar un análisis, por lo cual no será necesario espacio de almacenamiento para instalar un programa, por ejemplo; Pero tampoco una mínima cantidad, ya que en el proceso podría recuperarse archivos de interés y estos serían alojados en el disco virtual.
7. Se desplegará un listado con la información de la configuración con la cual se va a crear, así como la posibilidad de configurar el hardware de la máquina virtual, cantidad de RAM, procesadores, adaptador de red, por mencionar algunos.
8. Cliquear en “Finish”.

Un punto a tomar en cuenta, al momento de realizar una copia forense, es que, si la copia se llegó a realizar por fragmentos, esta imagen forense no podrá ser levantada en una máquina virtual ya que se encuentra fragmentada. También se podrá levantar una máquina con los sistemas operativos de Tequila, Caine o que fueron creados con enfoque forense para realizar desde ahí el análisis.

3.1.2 Tequila SO

“Está basado en GNU/Linux y se creó pensando en dar una herramienta especializada para la informática forense como no existía: Con manuales y soportes oficiales en español. Tequila v0.1 está basado en Kali, Deft y Caine, sistemas que cumplen

similarmente con la función." [75] Tequila SO es el primer sistema operativo dedicado a la informática forense desarrollado por el ingeniero mexicano en computación Jocsan Laguna Romero, por lo cual cuenta con manuales en idioma español, simplificando a los informáticos forenses latinoamericanos su uso.

Como el mismo sistema operativo está basado en Linux, este es libre y gratuito, y fue desarrollado en la Universidad Nacional Autónoma de México, por lo que su uso es aceptado en tribunales. Su descarga es posible desde la siguiente dirección web: https://tequila-so.org/descargar/. Esta podrá ser usada tanto como un sistema operativo cargado en el ordenador, acceder desde Live CD o levantarla desde una máquina virtual.

Como el sistema operativo ya trae un usuario precargado, se deberá acceder a él para poder entrar al sistema. Por lo cual su usuario y contraseña son los siguientes:

- User: root
- Pass: unam

Ya en este sistema operativo, se encuentran distintas herramientas forenses para poder llevar a cabo análisis de datos, por mencionar algunas de estas: Exiftool que será de utilidad en el análisis de datos provenientes de archivos Jpeg, Png, Gif, entre otros; Volatility será de ayuda al momento de analizar un volcado de memoria RAM, John The Ripper que aplicará ataques de fuerza bruta para descifrar contraseñas, entre muchas otras.

3.1.3 FTK Imager

"FTK Imager, es un software que se utiliza para crear archivos de imagen de disco o montar imágenes de disco o dispositivos de almacenamientos y luego podemos realizar análisis de la estructura del disco, recuperar datos, etc. Este software permite localizar archivos perdidos o buscar datos escaneando la imagen de disco mediante palabras claves." [76] Esta es una herramienta muy recurrente en el ámbito forense,

[75] Tequila SO, Laguna Romero Jocsan, acerca de, 2016. Disponible en: https://tequila-so.org/acerca-de/ consultado: octubre de 2019

[76] Solvetic, Solvetic Seguridad, Analizar imagen de disco con FTK Imager, 2016. Disponible en: https://www.solvetic.com/tutoriales/article/2567-analizar-imagen-de-disco-con-ftk-imager/ consultado: octubre de 2019

debido a que simplicidad en cuanto a su uso y a sus grandes capacidades tanto como generar volcados de memoria, imágenes forenses, recuperar archivos, así como realizar búsquedas a nivel hexadecimal, así como identificar el tipo de archivo por medio de los “Magic Numbers”.

Para realizar el volcado de memoria, se deberá proceder de la siguiente manera:

1) Se abrirá la pestaña “File”, seguidamente en la opción “Memory Capture”.
2) Se procederá a seleccionar el destino donde se ubicará el volcado, así mismo solicitará que se le designe un nombre, por defecto se denominara: memdump.mem.
3) Cliquear en “Capture Memory”.

El archivo que se creara tendrá el tamaño de la memoria RAM que tenga el equipo.

En el caso que ya se haya realizado el volcado de memoria y se tuviera conocimiento de, por ejemplo, un delincuente en ese computador haya realizado las reuniones por medio de la red social Facebook. Este volcado de memoria RAM, se llevará al laboratorio para seguidamente ser analizado. Este procedimiento solamente se debe realizar en la zona de trabajo, no en el ordenador analizado ya que se puede llegar a alterar la evidencia. Siendo de conocimiento que el delincuente estaba en uso de la red social, es de interés conocer su usuario y contraseña.

Al realizar la investigación manual del volcado de memoria, nos interesará saber la contraseña de la red social, contraseña será igual a “pass” este elemento será importante para realizar la investigación manual. Si se realizado de esta manera, la ventaja es que se ahorra dinero, la desventaja es que es llevara bastante tiempo.

Los pasos a seguir son los siguientes:

1. Se abrirá la pestaña “File”, seguidamente en la opción “Add evidence ítem…”.
2. Como la evidencia que se analizara será el volcado de memoria RAM, por el tipo de archivo, se seleccionara “Image File” y luego en siguiente.
3. se proseguirá a localizar el archivo y a seleccionarlo, cliquear en “Finish”.
4. Se desplegará una lista de caracteres alfanuméricos que de manera codificada identifican un archivo, que, en sí, será toda la estructura del volcado de memoria RAM.

5. Se dará clic derecho a la lista de caracteres alfanuméricos, seguidamente se seleccionará la opción “Find”.
6. En la casilla “Find What” se escribirá lo que se necesita buscar, en este caso será la palabra “find”. En la lista de “Type” se debe seleccionar “Text”, seguidamente se cliqueará en “Find”.
7. El sistema seleccionara en la lista de caracteres alfanumérica, los campos que contengan la palabra “Pass”. Habrá que analizar el contexto, como en el caso se busca la contraseña de Facebook, habrá que buscar el sector que contenga las palabras Facebook y Pass. Así a lo largo de toda la lista alfanumérica.

Otra de las funcionalidades de la herramienta forenses, es la creación de imágenes forenses. Para realizar esto, se procederá de la siguiente manera:

1. Se abrirá la pestaña “File”, seguidamente se cliqueará la opción “Create Disk Image”.
2. Se seleccionará el tipo de fuente de la evidencia
    A. Physical Drive: este se seleccionará en caso, la imagen forense se desea que se realiza a partir de un dispositivo de almacenamiento físico.
    B. Logical Drive: este será de utilidad cuando se necesite crear la imagen forense a partir de una partición de un disco duro.
    C. Image File: este se seleccionará si la fuente de la evidencia es una imagen forense.
    D. Contents of a Folder: este se utiliza para realizar una imagen forense a partir de carpetas. Este no es recomendable ya que no realizara la copia de los archivos que fueron eliminados anteriormente, de los sectores no asignados ni lo metadatos.
    E. Femico Device: este se utilizará en caso, se necesitará realizar una copia forense a partir de un disco óptico como por ejemplo CDs o DVDs.

En el caso de necesitar información de los usuarios de un equipo de cómputo existe el archivo SAM. Las contraseñas de Windows, luego de haber sido logueado en el computador, esta se cifra y se convierte en un grupo de caracteres que se vuelve irreconocible. Este grupo de caracteres se guarda en el archivo denominado SAM.

Este archivo SAM se encuentra ubicado en “C:\Windows\System32\config\SAM”. En este, se encuentra información sobre quien el ultimo usuario en iniciar sesión, cuando fue la última vez que se cambió la contraseña del usuario, entre otros.

Para poder extraer este archivo, se procederá a acceder a la herramienta de FTK Imager, para posteriormente cargar la evidencia de donde se pretende extraer el archivo SAM. En el árbol de evidencias, se localizará la ubicación mencionada antes. Normalmente se encontrará dentro de la partición más grande, dentro de la carpeta Root.

Una vez ubicado, se dará sobre el archivo clic derecho y se seleccionará la opción “Export File”, luego se elegirá la locación para exportarlo.

Posteriormente se accederá a otra herramienta denominada Registry Viewer, parte de la misma empresa creadora de FTK Imager: AcessData. está permite *“visualizar el contenido de los registros de sistemas Windows. A diferencia del editor de registro de Windows, el cual muestra solo el registro del sistema actual, Registry Viewer permite visualizar los archivos de registro de cualquier sistema. Registry Viewer también permite acceder al almacenamiento protegido del registro, el cual contiene contraseñas, nombres de usuario, y otra información no factible de acceder con el editor de registro de Windows.”*[77] Como se menciona, este software podrá acceder a los registros en uso del sistema operativo Windows, entre estos de importancia el archivo SAM.

Al cargar en la herramienta el respectivo archivo SAM, se desplegará un árbol de evidencias. Se tendrá que desglosar las siguientes carpetas:

- Sam
    - Domains
        - Account
            - Users.

Dentro de la carpeta “Users” se encontrarán distintas carpetas, que, dentro del nombre, contendrán la numeración dentro del rango 500, ya sea 501, 502, por defecto

[77] Reydes, Caballero Quezada Alonso Eduardo, Extraer Información del Registro de Windows con Registry Viewer, 2014. Disponible en: http://www.reydes.com/d/?q=Extraer_Informacion_del_Registro_de_Windows_con_Registry_Viewer consultado: octubre de 2019

son creados por el sistema; A partir del rango 1000, 1001, 1002 estos son los usuarios que ha creado la persona que ha tenido contacto con el ordenador. Estos son relevantes, ya que se visualiza cuantas veces ha iniciado sesión, cuando fue la última vez que inicio sesión, cuantas veces se ha ingresado mal la contraseña, cuando fue la última vez que se cambió la contraseña.

3.1.4 Maltego

"Maltego, servicio que tiene el potencial de encontrar información sobre personas y empresas en Internet, permitiendo cruzar datos para obtener perfiles en redes sociales, servidores de correo, etc." [78] Esta es una herramienta de gathering information, por lo cual, al tener el número de teléfono, el correo electrónico, el nickname de un usuario o con tan solo el nombre de un individuo o una empresa, se podrá ingresar para que el software lo busque alrededor de toda la red, ya sean redes sociales o foros. por lo que nos retornara información de en qué páginas web y servicios se encuentra relacionado, por lo cual se empieza a depurar y seleccionar la información que nos sea de relevancia.

Para utilizar el software, además de instalar el software en el ordenador, se necesitará registrarse en la página "www.paterva.com" para poder utilizar el programa con los servidores gratuitos. Una vez realizada la instalación del software, se deberá proceder a darse de alta en la página, para posteriormente iniciar sesión.

Para iniciar a recabar información, se debe crear una hoja de búsqueda nueva y seleccionar el tipo de búsqueda que se necesita llevar acabo:

1. Correo electrónico.
2. Alias.
3. Nombre de Usuario.
4. Documentos.
5. Imágenes.
6. El nombre de una persona.

[78] We live security, Pérez Ignacio, Maltego la herramienta que te muestra que tan expuesto estas en internet, 2014. Disponible en: https://www.welivesecurity.com/la-es/2014/02/19/maltego-herramienta-muestra-tan-expuesto-estas-internet/ consultado: junio de 2019

7. Números de teléfono.
8. Una frase o cualquier texto.
9. Dominios.
10. Servidores DNS.

Una vez conociendo el objeto de búsqueda a realizar, se le dará doble clic sobre el icono que se necesite para acceder a los parámetros del mismo, optando por la información puntual a buscar, ya sea direcciones ip o de un sitio web, entre otros. Seguidamente se ingresará el nombre a buscar para que sea recabada toda la información que se encuentre contenida en la red donde aparezca el nombre ingresado. Al terminar, el software presentará un esquema donde se desplieguen todos los sitios donde se hace mención relacionada. Tanta es la potencia de la herramienta que, si se encontrase relacionada al perfil de una red social, nos podrá desglosar las amistades con las que este perfil cuenta.

"Maltego tiene un modelo de licencia que limita los registros procesados / visualizados para las versiones de la comunidad, lo que requiere que compre una versión comercial para grandes conjuntos de datos." [79] Un dato a tener en cuenta del software, es que es de paga, pero cuenta de una versión gratis, la cual brindará una cantidad de resultados limitados, pero considerables a la hora de analizar un caso cibernético.

3.1.5 Passware Kit Forensic

"informa todos los elementos protegidos por contraseña en una computadora y los descifra. El software reconoce más de 280 tipos de archivos y funciona en modo por lotes recuperando sus contraseñas." [80] Este software ayuda a recuperar contraseñas de todo tipo de archivos, ya sea documentos de ofimática como Word, Excel, documentos PDF, archivos comprimidos como lo son realizados con WinRAR y WinZip, cuentas de correo registradas en el ordenador con Outlook, contraseñas

[79] (ISC) ² Comunidad, Análisis forense: ¡Autopsy 4.7 agrega visualización de enlaces, ZIP cifrado, base de datos y soporte de volatilidad!, 2018. Disponible en: https://community.isc2.org/t5/Industry-News/Forensics-Autopsy-4-7-adds-link-visualization-encrypted-ZIP/td-p/10442 consultado: octubre de 2019

[80]Passware, Passware kit forensic, Estados Unidos, 2014, Disponible en: https://www.passware.com/kit-forensic/ consultado: abril de 2019

guardadas en navegadores web, entre muchas otros. Así mismo, puede localizar a través de todo el disco duro, archivos que se encuentren encriptados.

La metodología a seguir cuando se necesite descifrar un archivo encriptado. Se puede utilizar un ataque con valores predefinidos, pero para esto, se debió realizar un ataque anteriormente. Existen varias opciones para descifrar:

1. Run Wizard: esta opción “llevara de la mano” al usuario, guiando paso a paso en el hacer el análisis, pudiendo modificar aspectos básicos del mismo.
    A. One dictionary Word: palabras simples como avión, Piedra, barco. Una sola palabra.
    B. More tan one dictionary Word: palabras compuestas como árbol verde, manzana roja.
    C. One or more dictionary words: en esta ya se realizan varias combinaciones de caracteres ya sea utilizando números o símbolos como manzana123!.
    D. I know nothing about the password: esta opción se utilizará si no se tuviera algún indicio referente a la contraseña.

    La selección de estos parámetros, acortara el tiempo de análisis de la contraseña, esto se realizará según sea el perfil del delincuente, ya sea en el caso que sea una persona paranoica, podría ser una contraseña con combinaciones, letras y caracteres especiales.

    Seguidamente el software solicitara el lenguaje del diccionario de contraseñas con el que hará el análisis, ya sea español, inglés, ruso, alemán, entre otros. Así como se podrá colocar en parámetros con cuantos caracteres puede hacer el análisis ya sea desde 5 caracteres hasta 128. Aunque hay que tomar en cuenta que entre más caracteres tenga la contraseña, más tiempo le llevara al software poder encontrarla.
2. Advanced: customize settings: por defecto trae todos los tipos de análisis activados como dictionary, xieve, brute-force, known password/part y previous passwords.

A. Dictionary: este ataque verifica miles de palabras como posibles contraseñas. Con cada palabra se prueban con variaciones según se haya configurado los parámetros del ataque.
B. Xieve: utiliza palabras que suenan similares, pero se escriben diferente en el idioma inglés. Este en el caso del español, no es de ayuda
C. Brute-force: produce el ataque realizando todas las combinaciones de existentes, utilizando mayúsculas, minúsculas, números, símbolos.
D. Known password/part: este en caso que se conozco parcialmente la contraseña, se realizará un ataque de diccionario
E. Previous passwords:

En un escenario real, se puede analizar el perfil de la persona, para saber que parámetros colocar, también existe la posibilidad descargar diccionarios de contraseñas desde la red. Para que pruebe las combinaciones más comunes a nivel mundial como posibles contraseñas.

Un inconveniente de este software es que es de licencia comercial, por lo cual hay que pagar la licencia para poder desbloquear la totalidad de las funciones. Al utilizarlo solamente en modo de prueba, al lograr obtener la contraseña, solo dejara a la vista 3 caracteres del mismo. Aunque al conocer estos 3 caracteres, ya nos facilita el poder realizar la búsqueda de una contraseña mediante el análisis manual del volcado de memoria.

3.1.6 Alternate Stream View

"*es una característica del sistema de ficheros NTFS que consiste en incluir metainformación en un fichero. Podríamos decir que son ficheros secundarios "ocultos*" *guardados dentro de otros ficheros. El objetivo inicial es almacenar información extra acerca del fichero principal, pero esta técnica también fue muy usada para propagar virus de forma transparente para el usuario."* [81] Existe la

[81] Security Artwork, Olmedo Yolanda, Alternate Data Stream: ADS – Flujo de datos alternativos en NTFS, 2015. Disponible en: https://www.securityartwork.es/2015/02/23/alternate-data-stream-ads-flujo-de-datos-alternativos-en-ntfs/ consultado: junio de 2019

posibilidad de que un delincuente, haya ocultado información o hasta un programa dentro de un simple bloc de notas.

- Con esta herramienta solamente bastará con seleccionar en el navegador o Browse, la ubicación en donde se necesita que se lleve a cabo la búsqueda de Flujo alterno de datos y seguidamente se dará clic en escanear o Scan. Si se requiere, se puede analizar por completo el disco duro.

Seguidamente, Alternate Stream View desplegara un listado con todos los archivos del sistema que tengan Flujo alterno de datos. Como muchos de estos son de utilidad al sistema para su funcionamiento. Los que son de interés para los peritos informáticos forenses serán los que terminen con extensión ".TXT". a excepción de los archivos denominados: "Zone.Identifier:$DATA". estos no tienen por qué tener más propiedades. Por lo cual estos serán de interés forense. Al detectar estos archivos .TXT, el programa nos indica su ubicación, para posteriormente, realizar el análisis forense mediante consola de comandos.

3.1.7 ChromePass

"ChromePass es una sencilla aplicación para Windows desarrollada por Nirsoft que nos va a permitir ver los nombres de usuario y las contraseñas que hemos guardado a lo largo de los años en nuestro navegador Google Chrome. Esta herramienta analiza la base de datos que genera el navegador" [82] Como su nombre lo indica, este logra extraer la información de contraseñas utilizadas en el navegador Google Chrome. Un dato importante de esta herramienta, es que extrae el archivo que almacena las evidencias, lo traslada a la memoria RAM, y desde acá, las interpreta. Motivo por el cual, no llega a alterar la evidencia.

Basta con ejecutar la herramienta. Esta desplegara un listado, indicando la dirección web donde se utiliza, el nombre de usuario y la respectiva contraseña.

Si en dado caso, desplegara un mensaje de algún antivirus, es normal. Ya que la herramienta lo toma como un programa malicioso, debido a que, si un programa

[82]Redes Zone, Velasco Rubén, ChromePass, una aplicación para ver las contraseñas de Google Chrome, 2016. Disponible en: https://www.redeszone.net/2016/09/06/chromepass-una-aplicacion-para-ver-las-contrasenas-de-google-chrome/ consultado: octubre de 2019

intenta extraer las contraseñas del navegador, el antivirus que tenga el ordenador, bloqueara esta acción. Esto puede suceder al extraer en sitio, aunque si no fuese posible, se puede proceder a extraer las contraseñas en el laboratorio.
Aunque esta no es la única desarrollada por Nirsoft, pues cuenta con su versión para cada navegador, así como lo es IE History View o Mozilla History View.

3.1.8 My Last Search

"*Mylastsearch es una pequeña utilidad gratuita que permite conocer las últimas búsquedas realizadas mediante nuestro navegador (Firefox, IE) en los buscadores Google, Yahoo y MSN"* [83] Con esta herramienta forense, podremos extraer las búsquedas que se han hecho a través de los navegadores. Este nos desplegara un listado con el texto buscado, el motor de búsqueda que se utilizó, la fecha y hora en la cual se realizó la búsqueda, el navegador que se utilizó y la dirección web de la búsqueda. No basta más que ejecutar la herramienta, para que despliegue toda la información que sea de interés forense.

3.1.9 CurrPorts

"El programa nos va a permitir monitorizar nuestra conexión de red y poder saber en tiempo real las aplicaciones que están haciendo uso de puertos TCP y UDP. Además, el programa dará información completa y detallada al usuario sobre la aplicación que está haciendo uso de dicho puerto (nombre, versión, path completo, propietario, fecha de instalación). También indicará el tiempo transcurrido desde que se comenzó a usar dicho puerto y el estado en el que se encuentra la conexión establecida."[84]
Este software indica los puertos del ordenador que se encuentran abiertos. Si alguno de estos, llega a llamar la atención al informático forense, indicara la dirección IP (Remote Address), así como al puerto al que se encuentra conectado (Local Port), y la aplicación si fuese el caso (Process Name), que este haciendo uso de esta

[83]Soft Zone, Gómez Hugo, MyLastSearch 1.35, 2009. Disponible en: https://www.softzone.es/2009/02/04/mylastsearch-135-conoce-las-ultimas-busquedas-realizadas-en-tu-navegador-con-mylastsearch/ consultado: octubre de 2019
[84]Redes Zone, Crespo Adrián, CurrPorts: averigua que programas acceden a internet en tu PC, 2013. Disponible en: https://www.redeszone.net/2013/02/21/currports-averigua-que-programas-acceden-a-internet-en-tu-pc/ consultado: octubre de 2019

conexión. Aunque siempre existe la ocasión donde el puerto se encuentra abierto, y la IP es de Windows, seguramente, será porque se está llevando a cabo una actualización del sistema.

3.1.10 Recuva

Una de las herramientas más conocidas, para la recuperación de datos informáticos. Para hacer uso de la herramienta, se debe hacer lo siguiente:

1. Al ejecutar la herramienta, desplegará una pequeña bienvenida al mismo, indicando que será de ayuda para recuperar los datos borrados. Se procederá a cliquear en “Next”.
2. Estará una lista donde pregunta qué tipo de archivos es de nuestro interés, como
    A. fotos (pictures).
    B. música (music).
    C. documentos (documents).
    D. videos (video).
    E. archivos comprimidos (compressed).
    F. correos electrónicos (emails).

    Por defecto tendrá seleccionado todos los archivos. Naturalmente entre menos tipos de archivos se elija, menos tiempo llevará el análisis de la herramienta, por lo cual se podrá recuperar la información en menor tiempo. Se cliquea en “Next”.
3. La herramienta pedirá la ubicación donde se requiere que se lleva a cabo el análisis:
    A. No estoy seguro (Im not sure): en esta opción buscara todos los sectores del ordenador.
    B. En tarjetas extraíbles o Ipod (on my media card or IPod): en esta opción, buscara en tarjetas extraíbles que se encuentren conectadas al computador, a excepción de CD.
    C. En mis documentos (in my documents): en esta opción, buscara en todas las carpetas de documentos del ordenador.

D. En papelera de reciclaje (in te recycle bin): buscara los archivos borrados dentro de la papelera de reciclaje.
E. ubicación especifica (In a specific location): en esta opción, permite que, mediante el buscador, se seleccione la ubicación exacta donde se requiere que se lleve a cabo el análisis.
F. En un CD/DVD (on a CD/DVD): permitirá seleccionar el CD que se encuentre dentro del ordenador.
G. Existirá la opción de activar una búsqueda profunda por parte del buscador, si fuese necesario hacerlo, se debe cliquear en la casilla con la leyenda “Enable Deep scan” y seguidamente cliquear en iniciar (start).
H.

3.1.11 TestDisk

“TestDisk es un poderoso software gratuito de recuperación de datos. Fue principalmente diseñado para ayudar a recuperar particiones perdidas y/o volver discos no booteables a booteables nuevamente cuando estos síntomas son causados por software con fallas, ciertos tipos de virus o error humano.[85] Esta herramienta será de ayuda cuando un disco duro haya perdido su sistema de archivos ya sea NTFS, FAT, EXT2, hasta arreglos RAID. Cuando tenga algún problema de arranque, se haya eliminado las particiones, entre otros. La herramienta es de uso gratuito, por lo cual no habrá ningún inconveniente al haberla utilizado en el ámbito forense.

Los pasos a seguir son:

1. Al ejecutar el programa, nos abrirá una venta similar a una consola de comandos. Se seleccionará la opción “Create” y luego pulsar Enter.
2. Seleccionar el disco duro que sea de interés, en esta parte los individualiza por su marca, modelo y capacidad. Luego se seleccionará “Proceed” y se presionará Enter.
3. Se deberá seleccionar según sea el tipo de partición, sea de Apple “APFS”, partición de Xbox, GPT, o el caso que fue un disco duro de ordenador, se seleccionara Intel (PC partition). Se presionará Enter.

[85] Cgsecurity, TestDisk, 2019. Disponible en: https://www.cgsecurity.org/wiki/TestDisk_ES consultado: junio de 2019

4. Se seleccionará “Analyse” y luego se presiona Enter. En esta ventana, también existirán las opciones avanzadas, donde se podrá modificar el sistema de archivos del disco, cambiar la geometría del disco, sobrescribir código sobre el mismo, este seria de interés en caso se quiere eliminar de forma permanente algún dato, y borrar toda información que se encuentre en la partición.
5. Se seleccionará la opción “Quick Search”.
6. Seguidamente, la herramienta desplegara una lista con las particiones existentes en el disco duro. Se deberá seleccionar la partición que se desea recuperar y luego presionar Enter.
7. Posteriormente se seleccionará la opción “Write” y luego se presionará Enter.
8. La herramienta pedirá que se confirme la acción, por lo cual se procederá a presionar la tecla “Y”.
9. Al finalizar, se presionará la tecla Enter y se deberá reiniciar el ordenador para que se apliquen los cambios realizados y poder visualizar la partición recuperada.

Como trabajan estas herramientas de recuperación, es que, mediante los magic numbers, que son los datos hexadecimales de cada archivo, por lo que cuando la herramienta indica que solo es recuperable un 85%, lo que hace para poder recuperar por ejemplo una imagen, rellena la información hexadecimal que hace falta, según el tipo de archivo. Esto es lo que marca la diferencia entre las distintas herramientas, ya que algunas cuentan con ciertos algoritmos para la rellenar la información restante en fotografías, otros serán mejores para la recuperación de audios.

3.1.12 Foca Pro

“es una herramienta para encontrar Metadatos e información oculta en documentos de Microsoft Office, Open Office y documentos PDF/PS/EPS, extraer todos los datos de ellos exprimiendo los ficheros al máximo y una vez extraídos cruzar toda esta información para obtener datos relevantes de una empresa.”[86] Con esta herramienta

[86] DragonJar, Restrepo Gómez Jaime Andrés, FOCA – Herramienta para análisis de Meta Datos, 2010. Disponible en: https://www.dragonjar.org/foca-herramienta-para-analisis-meta-datos.xhtml consultado: junio de 2019

se extraen todos los metadatos así como descarga todos los archivos ofimáticos que contenga un dominio y brindara los nombres de los usuarios que han llegado a trabajar con esos documentos.

Este también puede analizar archivos de forma local para extraer los nombres de usuarios que han trabajado con un archivo, este es el punto de interés forense.

Los pasos a seguir son los siguientes:

1. En la pestaña Proyect, se seleccionará “new Proyect”.
2. Al generar el proyecto habrá que llenar unos datos como lo es nombre del proyecto y dominio. En este campo no es necesario que exista el sitio web, pero si debe tener la estructura de .com, .net o similares. Seguidamente se cliqueará Crear.
3. Se abrirá una ventana donde se seleccionará una ubicación para guardar el caso.
4. Luego en la ventana del lado derecho, se dará clic derecho y se seleccionará “add file”, aquí se agregará el archivo de interés.
5. Se dará clic derecho sobre el archivo y se seleccionará “Extract all Metadata”
6. Aquí se abrirá una estructura que los ordene por documentos, Word, Excel, PowerPoint, entre otros. En seleccionar el archivo en esta estructura, desplegara un listado con los usuarios que han trabajado con el archivo, la fecha de creación, veces que ha sido impreso, así como nombre y modelo de la impresora usada, revisiones realizadas, el sistema operativo y la versión de ofimática con el que se creó y trabajo.

Un inconveniente que presenta la herramienta en relación a los metadatos referente a imágenes, es que solamente indicara que un archivo cuenta con metadatos, pero no desplegara información como GPS, por ejemplo.

Un dato importante es que, en casos de fuga de información, no solamente se da mediante dispositivos de almacenamiento, sino también se puede hacer de forma física, que un empleado haya impreso un archivo Word con datos importantes de la empresa. Este puede ser otro tipo de escenario para fuga de información.

Colocando un caso hipotético de un secuestro y el secuestrador enviase por correo electrónico la fotografía de alguien raptado. Envió un archivo de Word con la imagen

contenida en el mismo, puede que esta imagen haya sido capturada mediante la cámara de un celular. Esta fotografía podría contener datos GPS.

Para extraer esta imagen sin llegar a perder los metadatos, que son vitales para la investigación entorno a fotografías, imágenes, se debe acceder al software WinRAR que es un software *"compresor y descompresor de datos multifunción desarrollado por RarLab. Sirve para comprimir todo tipo de documentos o programas de forma que ocupen menos espacio en disco y se puedan almacenar o trasmitir por internet más rápidamente."*[87] Y realizar un desempaquetado del archivo donde se encuentre la fotografía.

La metodología seria la siguiente:

1. Dirigirme directamente a WinRAR, y desde aquí, localizar la ubicación del archivo.
2. Seleccionar el archivo, y en las pestañas superiores, seleccionar "extraer en".
3. Desplegara una ventana donde solicitara la ubicación donde se sea extraer el archivo, por defecto traerá la ubicación donde se encuentra el archivo.

Seguidamente WinRAR creara una carpeta con el mismo nombre del archivo. Esta carpeta contendrá la estructura de todo el archivo.

3.1.13 WinAudit

"Es una aplicación que me permite realizar una auditoria muy completa de toda la información del sistema, los programas instalados, las configuraciones, el hardware del equipo, los parches instalados, etc., el informe que arroja la herramienta es bastante detallado y bien organizado en formato html lo que facilita la búsqueda de la información."[88] Esta herramienta esta lista para ser utilizada, por lo cual, no llegara a instalar archivos ni a modificar el registro del sistema, por lo cual es apta para uso forense. no se necesitará modificar parámetros. Para darle uso a la herramienta. Se debe realizar lo siguiente:

[87] WinRAR, que es WinRAR, 2013. Disponible en: https://www.winrar.es/soporte/articulo/30 consultado: septiembre de 2019

[88] DragonJar, Restrepo Gómez Jaime Andrés, Automatizando la extracción de evidencia forense en Windows, 2014. Disponible en: https://www.dragonjar.org/automatizando-la-extraccion-de-evidencia-forense-en-windows.xhtml consultado: junio de 2019

1. Ir a la pestaña “Archivo” localizada en la parte superior izquierda, cliquear.
2. En las ventanas desplegadas, se deberá dar clic en “Recolectar Información”.
3. Esperar a que la herramienta realiza un inventario de la información del equipo

El programa genera el inventario que se podrá desplegar desde la parte izquierda del software, catalogadas en:

4. vista general: mostrara información general del equipo como nombre del computador, nombre del dominio, fabricante, sistema operativo, procesadores, número de serie, versión de la BIOS, cuentas, hora local y última actualización del equipo.
5. Software Instalado: aquí se mostrará el software para el correcto funcionamiento del computador, así como la versión de software con la que cuenta.
    A. Programas instalados: aquí colocara los distintos programas que se encuentran instalados en el ordenador, brindando información del nombre del fabricante, versión del programa, ubicación de instalación, compañía registrada, número de registro, ID del software, entre otros.
    B. Periféricos: se adjuntará información de los dispositivos conectados como teclado, mouse, monitor, fax, impresora.
6. Seguridad: en este apartado, se localizará información de los puertos abiertos así como el nombre del proceso; los permisos con los que cuentan los equipos de impresión, información del cortafuegos, así como restauraciones que haya tenido el equipo.
7. Grupos y Usuarios: desplegara información de los grupos locales, grupos globales y cuentas de usuarios, así como los miembros, políticas de uso.
8. Tareas Programadas: se crearán apartados de las aplicaciones que se encuentras programas en el uso del ordenador, así como estado actual, nombre de la tarea, comando utilizado, última fecha en que se realizó y la próxima en realizarse.
9. Error Logs: este apartado desplegara los distintos sucesos que ha sufrido el ordenador tanto si fueran de aplicativos como a nivel de hardware, colocando el nombre del error así como la descripción del mismo.

10. Red TCP/IP: el apartado desplegara información de la tarjeta de red así como la banda inalámbrica que utiliza, la dirección MAC, IP, DNS, entre otros.
11. Dispositivos: clasificara la información dentro de componentes de software, bluetooth, adaptadores de red, cámaras, entradas y salidas de audio, entre otros.
12. Discos Físicos: colocara la capacidad, tipo, modelo y fabricante del disco duro que este montado en el ordenador, así como sus sectores y número de serie.
13. Discos Lógicos: los dividirá por las particiones que cuente el disco duro, así como el porcentaje, espacio usado o libre y el sistema de archivos que utiliza.
14. Programas de Arranque: desplegara el nombre, ubicación y comando que utilizan las aplicaciones que se ejecutan desde el momento en que es iniciado el ordenador.
15. Programas en ejecución: colocara todos los procesos que se están llevando a cabo en el momento que es realizado el inventario en el computador.

La herramienta también cuenta con las opciones de guardar el informe, imprimirlo o enviarlo a través de correo electrónico, colocando la fecha y hora en que se realizó el mismo.

3.1.14 USBDeview

"USBDeview nos listará todos los dispositivos USB que hayan pasado por nuestra máquina. Para cada uno de ellos, muestra su nombre, descripción, tipo de dispositivo, número de serie, fecha en que se añadió, ... Con esta lista podremos desinstalar los que queramos, por ejemplo, si no vamos a usarlos más o desconectar los que estén conectados en ese momento." [89] Con esta herramienta se podrá tener acceso a la información de todos los dispositivos que han sido conectados al ordenador, tal como el nombre del dispositivo, descripción, número de serie, última vez que se realizó la conexión, entre otros.

[89] Genbeta, Fuentes Sacha, USBDeview, todos los dispositivos USB del sistema, 2009. Disponible en: https://www.genbeta.com/herramientas/usbdeview-todos-los-dispositivos-usb-del-sistema consultado: octubre de 2019

Así mismo, cuenta la posibilidad de generar un reporte de los dispositivos en su totalidad o los que sea de interés. Generando un documento con alguno de los siguientes formatos: html, xml, txt o csv. A elección del perito forense. Otra capacidad de la herramienta será la de realizar un borrado de toda la información recabada de los dispositivos que en algún momento fueron conectados al ordenador.

3.1.15 Whatinstartup

"muestra la lista completa de aplicaciones que son cargadas automáticamente cada vez que iniciamos el sistema Windows. Para cada aplicación se muestran varias columnas informativas: Startup Type (según sea desde el Registro de Windows o la carpeta de Inicio del sistema), Command-Line String (los parámetros de ejecución que recibe la aplicación, junto a la ruta completa), si está o no desactivada, el nombre del producto, la versión del fichero, la compañía desarrolladora de la aplicación, su localización en el Registro de Windows o en el sistema de ficheros, etcétera."[90] Esta herramienta será de ayuda al momento de querer conocer si hay algún archivo .exe, de dudosa procedencia se ejecuta al momento de arrancar el computador. Brindando información de si fue la misma máquina o el usuario que ordeno su ejecución, la línea de comando utilizada, nombre del software, versión, descripción, compañía, locación, entre otros atributos del mismo.

Para el uso de la herramienta, bastará con únicamente iniciarla, puesto que automáticamente brindará la información de interés, sin realizar mayor esfuerzo.

3.2 Suites Forenses

El perito informático Pedro de la Torre define las suites forenses como *"Se trata de packs de herramientas forenses de tipo software de muy distinto uso y alcance. Las hay tanto de pago como gratuitas y se usan tanto para el estudio de ficheros*

[90] Hipertextual, Sepharad, WhatInStartup controla qué se carga al iniciar Windows, 2009. Disponible en: https://hipertextual.com/archivo/2009/11/whatinstartup-controla-que-se-carga-al-iniciar-windows/ consultado: octubre de 2019

electrónicos como logs de navegadores, dispositivos móviles, memoria RAM y un largo etcétera."[91]

Las suites forenses son herramientas más complejas que compila todas las funciones que son utilizadas para poder extraer información de los ordenadores, así como de dispositivos móviles. Entre las suites forenses más destacadas, se encuentran:

3.2.1 Autopsy

"Es una interfaz gráfica para el análisis forense informático, mediante herramientas de líneas de comandos. El cual permite a los investigadores lanzar auditorías forenses no intrusivas en los sistemas a investigar. Estos análisis se centran en análisis genérico de sistemas de archivos y líneas temporales de ficheros."[92] Esta es una suite forense, esta herramienta ya permite realizar un análisis profundo, incluyendo el recuperar las páginas que se visitaron en modo incognito o todos los datos que fueron eliminados. Los pasos a seguir para poder abrir una nueva investigación, es la siguiente:

1. Al ejecutar la herramienta en modo administrador, se proceder a abrir un nuevo caso. Clic en "New case".
2. En este apartado, se ingresará información relevante como el nombre y número de caso, el nombre y datos de contacto del perito informático forense que llevará a cabo el análisis. un punto importante es que, en el apartado de base del directorio, se recomienda es que sea seleccionado un disco duro independiente. Esto debido a que la herramienta creara la estructura, desempaquetara y guardara los datos temporalmente para analizarlos. No se recomienda que se seleccione el disco local C como base de directorio, ya que se genera lo que se conoce "cuello de botella" "*Simplificando al máximo el concepto, el cuello de botella se produce cuando la falta de potencia de uno de los componentes lastra el rendimiento de otro, impidiendo que éste desarrolle*

[91] Indalics, De La Torre Rodríguez Pedro, Herramientas de informática forense, S/A. Disponible en: https://indalics.com/peritaje-informatico/herramientas-de-informatica forense#Suites_de_herramientas_forenses consultado: octubre 2019

[92] Ecured, Autopsy, 2011. Disponible en: https://www.ecured.cu/Autopsy consultado: octubre de 2019

todo su potencial." [93.] Esto sucede ya que el ordenador, está corriendo el sistema operativo, está corriendo la herramienta autopsy y al mismo tiempo, debe estar escribiendo la base del directorio, ejecutándolos desde el mismo disco duro, por lo que se sobrecarga de trabajo, provocando que el análisis lleve mucho más tiempo de lo que llevaría si se seleccionara la base de directorio un disco duro independiente.

El apartado de multiusuario se seleccionará en el caso que se realice una conexión entre varios ordenadores, para que simultáneamente, todos trabajen el caso. Disminuyendo el tiempo de análisis, aunque lleva conexiones de hardware, implicando una inversión económica considerable, para que esta opción sea rentable.

3. La siguiente ventana se agregará el tipo de evidencia que se va a analizar:
    A. Disk Image or VM file: este se seleccionará si la evidencia a analizar es una imagen forense o un archivo de VMware, en caso ya estuviera montado en una máquina virtual.
    B. Local Disk: se seleccionará cuando se analice como evidencia un disco local o un medio de almacenamiento externo.
    C. Logical Files: se seleccionará en el caso que, lo que se desea analizar, este contenido dentro de carpetas.
    D. Unallocated Space Image File: se seleccionará cuando la evidencia a analizar sea un medio extraíble con espacio no asignado.

    Una vez seleccionado el tipo de evidencia a trabajar, se cliqueará en Next.
4. En la siguiente ventana se seleccionará la ubicación de la evidencia a analizar.
5. La herramienta tendrá los distintos módulos a investigar:
    A. Recent Activity: esta opción brindara toda la información de actividad de los usuarios, incluyendo lo que ya ha sido eliminado, como la navegación en modo incognito, uso de CCleaner.

[93] Computerhoy, Rubén Andrés, Qué es cuello de botella en el PC y cómo evitarlo, 2018. Disponible en: https://computerhoy.com/noticias/hardware/que-es-cuello-botella-pc-como-evitarlo-79447 consultado: octubre de 2019

B. Hash Lookup: entrara a la carpeta de Windows System32, generando firmas hash de todos los archivos, con el objetivo de comparar estas firmas digitales con una instalación limpia del sistema operativo. Para que, para saber si el sistema no ha sido modificado por medio de un ataque.
C. File Type Identification: si se habilita esta opción, verificara a nivel hexadecimal, que cada archivo sea realmente lo que su extensión dicte. Incluye los archivos que han sido eliminados.
D. Embedded File Extractor: se encargará de que se descompriman los archivos que se encuentran empaquetados, para que estos sean analizados a nivel hexadecimal. Un dato importante es que esta opción no tiene la capacidad de romper contraseñas de archivos cifrados.
E. Exif Parser: todos los archivos de imagen les extrae los metadatos. Esto puede ser de ayuda en caso donde las imágenes sean relevantes como en casos de pornografía infantil.
F. Keyword Search: consulta todas las cadenas de texto que se encuentren en la copia forense y aplicara algoritmos, para detectar direcciones IP, números de teléfono, números de tarjetas bancarias, entre otros.
G. Email Parser: lo que realiza es que desempaqueta los archivos con extensión .ost y .pst. estos son los formatos que utilizan los aplicativos de correo electrónico como Outlook, que, en sí, es un archivo compreso con todos los correos electrónicos de la cuenta enlazada.
H. Extension Mismatch Detector: busca extensiones extrañas. Si en dado caso un usuario cambia la extensión de un archivo a uno no existente, y tampoco llega a detectar su extensión a nivel hexadecimal, la herramienta colocara todos esos archivos en una carpeta adicional.
I. E01 Verifier: este verificara que la copia se mantenga intacta por medio de la firma electrónica E01.
J. Interesting Files Identifier: lo que realiza la herramienta, será colocar filtros como nombre, extensión, peso, entre otros. Mientras realiza el procesamiento, si llegase a encontrar un archivo que coincida con los

parámetros que se establecieron anteriormente, la herramienta lo pondrá a la vista.

K. PhotoRec Carver: lo que realiza la herramienta es analizar todo el disco duro, así como el espacio vacío y ubica los archivos que fueron eliminados.
L. Correlation Engine: este será ayuda al analizar equipos de cómputo relacionados. Este solo será de ayuda en ciertos casos. ¿Por qué? En casos de ser computadoras de una misma empresa, al analizarlos, la herramienta detecta que los dos ordenadores tienen archivos en común o compartiendo ciertas similitudes. Ya a nivel forense puede ser de interés el por qué ambos están trabajando con los mismos archivos, que estaban realizando, acaso el empleado tenía autorización para trabajar con cierto documento. No tendría caso que se emplee esta opción en casos que los ordenadores fueran de casos separados.
M. Encryption Detection: esta opción detectara los archivos cifrados. Un dato a tomar en cuenta es que no se encargara de descifrar ni de realizar ataques de fuerza bruta, solamente se encargara de ubicar los archivos.
N. Virtual Machine Extractor: si la copia forense contara con máquinas virtuales, la herramienta las va a extraer y las va a analizar con las características heredadas.
O. Android Analyzer: si en dado caso se encontrara el backup de un teléfono celular Android, con la extensión. Adb, lo analizara con los parámetros heredados. Aunque no es muy común encontrar backup, ya que es un proceso algo tedioso y no existe herramienta oficial de Google que brinde este soporte.

Conforme va analizando, en el panel izquierdo se irá extendiendo el mismo conforme los resultados que va encontrando. Mientras que, del panel derecho, se podrá ver a detalle cada dato que haya recabado. La herramienta es muy potente, pero se debe de elegir con responsabilidad que es lo que se necesita. ¿Por qué? Por el tiempo que implicaría.

Un añadido de autopsy es que, posterior al análisis que se lleva acabo, puede realizar una línea de tiempo de la evidencia extraída, facilitando al perito informático forense poder correlacionar eventos de la realización del delito cometido y así el análisis puede llegar a ser más concluyente.

Para todos los archivos que haya extraído del análisis, brinda los metadatos, con información como fecha de creación, última vez que se accedió, fecha de última modificación, entre otros. Al haber terminado el análisis, la herramienta brinda la opción de poder producir un reporte que puede generarse en formato XLSX, HTML, TXT, entre otros, según le sea más cómodo el uso al perito.

Un dato importante a tener en cuenta, es que el antivirus puede llegar a saltar en alguna ocasión, debido a que se está accediendo a información del sistema, lo recomendado es que en el mismo, se dé la opción de excluir la carpeta donde se designó la base de datos del directorio, porque mientras lo está procesando, es de interés que autopsy vea toda la información, ya que puede que de la copia forense provenga un archivo infectado, el antivirus puede eliminarlo, por lo que la herramienta forense puede que no llegue a analizarlo.

La herramienta ya que es de uso gratuito, se puede descargar desde el sitio web oficial: http://www.sleuthkit.org/sleuthkit/download.php

3.2.2 OSForensic

"OSForensics es una aplicación que te permite conducir un escaneo a fondo del ordenador en busca de cualquier pieza de evidencia que pueda ofrecerte una pista, verificando todo, desde los archivos de email, archivos borrados, incluso el historial del navegador. Además, te permite organizar la evidencia creando casos separados, lo que te permitirá mantener todos los datos separados."[94] es una suite completa para análisis forense, aunque a diferencia de las demás herramientas que se han mencionado anteriormente, esta es de venta comercial, por lo cual se necesita la licencia de uso para utilizar dicho software en un caso judicial, aunque esta misma cuenta con una versión demostración.

[94] Proyecto TIC, OSForensics, realiza un análisis forense a tu ordenador, 2009. Disponible en: https://www.proyecto-tic.es/osforensics/ consultado: octubre de 2019

1. Manage Case: esta opción cumple como gestionador de casos, es un módulo que se utiliza para los resultados agregados de las funcionalidades con las que cuenta la herramienta.
2. Create Index: permite buscar textos dentro del disco duro para posteriormente generar un listado con los procesos completos y que archivos generaron error.
3. Search Index: al haber realizado el índice con create index, en este apartado se podrá realizar a cabo la búsqueda puntual entre el índice generado y así como filtrar los resultados por tipos de archivos.
4. File Name Search: esta opción realiza la búsqueda entre todos los archivos que contengan las letras o palabras que se ingresen, así como filtros de tipo de archivos que necesita buscar ya sean archivos comprimidos, videos, documentos, entre otros.
5. Recent Activity: generara un reporte de toda la actividad que tiene el equipo de cómputo, a diferencia de las demás herramientas, este análisis también incluirá las Wlan, las redes inalámbricas a las que se ha conectado el ordenador, las cookies de las páginas de internet que se han visitado, instaladores utilizados, búsqueda realizadas con el asistente, entre mucha más información de las últimas actividades que se llevaron a cabo en el ordenador.
6. Passwords: con esta opción, la herramienta extraerá todas las contraseñas que hayan quedado guardadas en el computador, así mismo, los seriales con los que se han registrado las aplicaciones.
7. Deleted Files Search: permite recuperar archivos que fueron eliminados en determinado momento, ya sea intencional o accidentalmente.
8. Mismatch File Search: permite encontrar archivos que cuenten con extensiones distintas a su origen, como si un archivo de imagen de extensión. Jpeg se haya cambiado a .TXT.
9. Memory Viewer: como su nombre lo indica es un visor de memoria. Permite al perito informático forense recolectar y analizar la evidencia contenida en una memoria volátil, como lo es una memoria RAM, visualizando los

procedimientos que la misma está llevando a cabo, así como realizar un volcado de memoria.

10. Prefetch Viewer: esta funcionalidad muestra la información almacenada del sistema operativo como cuando y con qué frecuencia se ejecuta una aplicación, la última vez que se llegó a iniciar, así como todos los archivos que llego a utilizar y a acceder la aplicación seleccionada.
11. Raw Disk Viewer: esta funcionalidad permite analizar a nivel hexadecimal unidades de volúmenes como discos duros completos, así como hacer búsquedas concretas o colocar un punto de lectura ya sea por bytes o por sectores.
12. Registy Viewer: es un explorador de archivos del sistema que genera un listado con la configuración y registros de archivos de seguridad, software, sistema, así como del archivo SAM que contiene la contraseña de los usuarios del ordenador, entre otros.
13. Web Browser: es un navegador web que incluye la herramienta. Que cuenta con la característica de exportar las páginas web como imágenes de extensión .png.
14. Drive Preparation: esta característica permite eliminar datos que contenga un disco duro con propósito forense de forma segura y verificando que no contenga errores, esto, con el objetivo de eliminar rastros de imágenes forenses pasadas y evitar que algún momento se lleguen a mezclar datos de dos o más casos.
15. Forensic Imaging: esta opción permite la creación de imágenes forenses, así como simultáneamente generarle su firma digital o seleccionar el formato de la imagen.
16. Mount Drive Image: Una de los puntos a tener en cuenta al momento de usarla es que la herramienta no trabaja con archivos con extensión .iso, que es el formato que utilizan las imágenes forenses, solamente trabaja con unidades de disco duro. Para lo cual se encuentra esta opción, la cual consiste en montar la imagen forense como un disco duro virtual, para que, de esta forma, la herramienta ya pueda analizar la evidencia. Tomar en

cuenta que, al terminar de utilizarla herramienta, se desmonte la unidad virtual, de lo contrario, el ordenador montara la unidad virtual todas las veces que se arranque el equipo.

17. System Information: genera un listado con información detallada del ordenador como nombre del equipo, sistema operativo, puertos, memoria RAM, tarjeta gráfica, impresoras, ente otros. Ya sea del ordenador que se está corriendo o de una imagen forense.
18. Verify/Create Hash: esta opción, permitirá calcular la firma hash de archivos individuales, textos, hasta discos duros completos. Calculando funciones Sha-1, MD5 y Sha-256, así como la posibilidad de realizar dos cálculos a la vez. Cuenta también con la funcionalidad de comparar con otra firma Hash.

La herramienta es un muy potente, pero cuenta con la desventaja que esta no es portable, por lo cual no se puede llevar en el disco duro que se utiliza para la extracción de información en la escena del crimen. La forma de poder utilizarlo de forma provechosa, es que, en el laboratorio forense, con la imagen forense se levante una máquina virtual, ya dentro de esa máquina virtual, utilizar esta herramienta para que realice el análisis. Es de importancia que se utilice una de las copias extras, para que, si en algún momento se llegase a modificar información relevante, esto no llegue a perjudicar la investigación y se pueda proseguir con una de las otras copias de la imagen forense.

Uno de los mayores inconvenientes de las suites forenses, es que no son prácticas en sitio, ya que se demoran mucho tiempo. Una suite como autopsy, analizando un disco duro de una capacidad de 1TB, con un equipo de cómputo con un procesador Intel I7 y con una capacidad de 16GB en la memoria RAM puede llegar a tardar de 5 a 7 días aproximadamente. Por lo que, en escena, se utilizaran las herramientas libres para analizar rápidamente y de forma no intrusiva, los datos que sean de relevancia. Para que, posteriormente en el laboratorio, se pueda agregar la copia forense y se pueda extraer esta información.

3.3 Sistemas operativos basados en Unix

Los sistemas operativos basados en Unix como lo es Linux, no se tomarán en cuenta en el capítulo III, debido a que para extraer la información de este tipo de sistema, se realiza mediante comandos en consola, por lo tanto no se estaría haciendo uso de herramientas forenses. Solamente se desarrollan los temas de cómo llevar a cabo una imagen forense del disco duro y el proceso a seguir para acceder a la información de los usuarios que existen dentro del equipo de cómputo.

Un dato a considerar es que se tendrán que conocer comandos básicos utilizados en consola, como los son los comandos: Ls, cd, mkdir, cat, entre otros, para poder navegar dentro del sistema operativo.

3.3.1 Información de usuarios

Los tipos de usuarios que se pueden crear en Linux son: usuario superadministrador, usuario del sistema.

Al iniciar una ventana de comandos en Linux, en la línea de comandos desplegara información muy importante, por ejemplo: “Jose@Tequila” el primer nombre detrás de la arroba, es el nombre del usuario del cual la sesión se encuentra en uso y el nombre después de la arroba, es el nombre que recibe el equipo de cómputo. Luego en la misma línea, puede llegar a aparecer un símbolo de dólar “$”, este signo lo que indica es que se estará en la carpeta Home del usuario que se encuentra en uso.

En la ubicación “/Home” en el sistema Linux, es el directorio raíz. Equivalente a disco local C en el sistema operativo Windows. Por lo que en esta ubicación, estarán las carpetas de todos los usuarios existentes en el equipo de cómputo. Con el Comando “Cat”, el sistema desplegara la información de un archivo en la terminal. Por lo que aquí se podrán visualizar archivos importantes que se encuentran dentro de la carpeta “/ etc”, se encontrarán los siguientes archivos:

- /passwd: en este archivo, se registran los usuarios del sistema.
- /Shadow: En este, se almacena las contraseñas cifradas.
- /group: este fichero, contiene la información de los grupos utilizados en el ordenador.

Para poder ingresar a esta información, se utilizará el siguiente comando en la terminal: “cat /etc/shadow”. Un dato a tener en cuenta es que para acceder a información del sistema, Linux restringe el accedo a esta, hasta que no se invoque al Superadministrador. Para hacer esto, anterior del comando se deberá colocar “Sudo” antes del comando. Por lo cual, el comando debería quedar así:

“sudo cat /etc/shadow”.

El sistema requerirá la contraseña del usuario superadministrador.

“<nombre><password cifrado><1><2><3><4><5><6>

<nombre> Nombre del usuario.

<password cifrado> Pues eso…

1- *Días transcurridos desde 1-1-1970 donde el password fue cambiado por última vez.*

2- *El mínimo número de días entre cambios de contraseña.*

3- *Días máximos de validez de la cuenta.*

4- *Días que avisa antes de caducar la contraseña.*

5- *Días después de que un password caduque para deshabilitar la cuenta*

6- *Fecha de caducidad. días desde 1-1-1970, donde la cuenta es deshabilitada y el usuario no podrá iniciar sesión.”*[95]

Desplegara la información de los usuarios que existen dentro del equipo de cómputo. A la par del nombre del usuario, luego de los dos puntos, se encontrará la contraseña del usuario cifrada. Si no apareciera, es porque la cuenta no cuenta con contraseña. Así mismo será el equivalente al archivo SAM en el sistema operativo Windows, desplegando información de veces de cambio de contraseña, validez de dicha contraseña, entre otros.

[95] Nexolinux, Ficheros de usuarios /etc/passwd y /etc/shadow, 2013. Disponible en: http://www.nexolinux.com/ficheros-de-usuarios-etcpasswd-y-etcshadow/ consultado: noviembre de 2019

Para entrar al fichero con las contraseñas, se utilizará el siguiente comando dentro de la terminal: “cat /etc/passwd”. Aquí desplegara dos puntos importantes. El usuario, así como la ubicación de la carpeta “/Home”.

Para mandar toda esta información en un archivo, se podrá usar el comando “>” seguido de la ubicación a crear un archivo de texto, por lo que como ejemplo podría quedar de la siguiente manera: “cat /etc/passwd > /home”

Para poder realizar una firma digital del archivo que se creó de una forma muy sencilla, mediante el comando “sha512sum” seguido del nombre del archivo para verificar la integridad. siendo esto interesante de parte del sistema operativo Linux, que no es necesaria una herramienta, para poder extraer la firma digital de un archivo.

3.3.2 Imagen Forense en Linux

Para realizar una copia forense a través de la línea de comandos de Linux, se debe seguir el siguiente protocolo, el comando es bastante sencillo.

dd: con este comando, el ordenador interpreta que se llevara a cabo la copia del disco.

if=: se indica cual es el archivo o medio de almacenamiento del que se va a realizar la copia forense. La carpeta donde se encuentra ubicada los medios de almacenamiento es: “/dev/”. Ya según se encuentre designado cada punto de montaje, se encontrarán como “sda”, “sdb”, “sdc”, etc. No se puede escribir algo dentro de, por ejemplo: “/dev/sda”. puesto que esto es únicamente para identificarlo física y lógicamente, por lo que incluiría exclusivamente las particiones existentes dentro del disco duro.

OF=: esta será la salida de la imagen, donde se ubicará la imagen forense al terminar de copiarse. “Un dato a tomar en cuenta a la hora de colocar la dirección de salida es no equivocarse al indicar las unidades de origen y salida puesto que, podría provocar la pérdida de la evidencia”. [96] Al final de la

[96] ByteMind, ByteMind, Backup de seguridad en Linux con el comando dd, 2019. Disponible en: https://byte-mind.net/backup-de-seguridad-en-linux-con-el-comando-dd/ consultado: noviembre de 2019

dirección, se colocará el nombre con el que se designara la imagen forense seguido de la extensión “.dd”.

Quedando de la siguiente manera:

“dd if=Dev/sda of=/root/media/usb/imagenforense.dd”

De esta forma, la imagen forense estaría completa, pero hay que considerar que tiene limitantes. sí en el medio de almacenamiento se encontrará un sector dañado no se podría llevar a cabo la copia. Para resolver este tipo de casos, se deberá colocar seguido al comando: “conv=noerror,sync” el cual será interpretado por el ordenador de manera que, los sectores dañados serán colocados con digito 0 a nivel hexadecimal, logrando que continúe la copia de los demás sectores.

El comando final quedaría de la siguiente manera:

“dd if=Dev/sda of=/root/media/usb/imagenforense.dd conv=noerror,sync”

Al finalizar el procedimiento, la consola desplegara información como numero de bytes copiados, duración del proceso y la velocidad estimada de copiado.

3.4 Dispositivos Móviles

Tomar en cuenta que para que la extracción de información del móvil se lleve a cabo con éxito, hay que considerar los siguientes puntos:

1. Hacer lo posible por conseguir el dispositivo desbloqueado.
2. Colocar el dispositivo Android en modo depuración, para que pueda ejecutar ordenes enviadas desde el ordenador.
3. Mantener la pantalla activa en todo momento.
4. Mantener cargado el dispositivo móvil para evitar que se llegue a apagar en el momento del análisis.

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

a. *Números llamados*
b. *Números guardados en la memoria y en el marcado rápido*
c. *Identificador de llamadas, llamadas entrantes*
d. *Números marcados*
e. *Nombres y direcciones*

f. *Números de tarjetas de crédito*
g. *Números de llamadas hechas con tarjeta*
h. *Información de acceso al Internet y al correo electrónico*
i. *Se puede encontrar valiosa información en la pantalla del aparato*
j. *Imágenes. Fotos, grabaciones de voz*
k. *Información guardada en las tarjetas de expansión de memoria"*[97]

A la hora de llevar a cabo la extracción de información del dispositivo móvil, se puede realizar de dos maneras: extracción física o extracción lógica.

1. Extracción física: esta es la recomendable, ya que se podrá realizar una copia bit a bit del dispositivo, incluyendo los datos del usuario como del propio sistema, facilitando en casos que sea necesario recuperar datos que hayan sido eliminados. aunque cuenta con desventajas, se necesitara que el teléfono se encuentre con permisos cedidos anteriormente de superadministrador también conocido como "Root". No aconsejable realizarlo ya que de esta manera se estaría alterando los datos incluidos dentro del dispositivo, provocando que el mismo no sea admitido como evidencia. A partir de aquí, de acuerdo a la marca y modelo del dispositivo móvil se realizará la copia mediante el software propietario de cada marca.
2. Extracción lógica: esta extracción se basará en tener acceso a los datos del usuario, ya sean imágenes, videos, notas de voz, mensajes y contactos de la agenda. Esto se puede llevar a cabo mediante la herramienta AFLogical, localizada en el sistema operativo Santoku que trabaja de forma automática para extraer y realizar una copia de los archivos.

3.4.1 Wacrypt

"Wacrypt un software en terminales Android para el tratamiento de las evidencias recogidas en WhatsApp que, nos guste más o menos, es la aplicación de mensajería instantánea más usada en todo el mundo con un cálculo aproximado de más de 60.000 millones de mensajes enviados a diario. Casi nada. Esto da una idea de la

[97] Organización de los estados americanos, Manual de Manejo de Evidencias Digitales y Entornos Informáticos, 2011.

importancia que puede tener en ciertas circunstancias buscar de manera sencilla los mensajes, desencriptar las conversaciones y guardarlas en un dispositivo para revisarlas o analizarlas." [98] Esta herramienta tiene un punto muy fuerte, que es la automatización, por lo que un usuario sin mayores conocimientos técnicos podrá utilizar dicha herramienta para poder extraer la información de interés. Otro punto a favor es que el dispositivo móvil del que se desea extraer la conversación no será necesario que se encuentre rooteado en caso contase con sistema operativo Android, lo cual es de ayuda ya que no se estaría alterando la evidencia.

Al ejecutar la herramienta, se encontrará con una interfaz muy sencilla. Cuenta con dos modalidades de trabajo, los cuales son:

1. Local: se puede utilizar la herramienta para poder interpretar los mensajes que se encuentren alojados en el backup de un dispositivo móvil siendo ficheros con la extensión .db y .crypt; un dato a tomar en cuenta, es que para poder descifrar, se necesita del archivo Key, que se recupera en el momento de la extracción. Esta es única para cada usuario de WhatsApp, por lo cual no se puede acceder con ninguna otra.
2. Extracción: en este modo será donde, mediante conexión USB, se extraerán las conversaciones del terminal Android.

Un dato importante es que previamente a realizar la extracción, se deberá activar el modo depuración USB dentro de las configuraciones de dispositivo móvil. Esto para que el ordenador y el terminal se conecten directamente y puedan pasarse información.

Otra gestión que debe realizar el perito informático forense será confirmar la solicitud de backup en el dispositivo Android, para que la herramienta pueda realizar la extracción.

La herramienta se encargará de organizar la información extraída ya sea en formato PDF o HTML, incluyendo las conversaciones que fueron eliminadas, la recuperación de thumbnails de imágenes que fueron transferidas, los thumbnails son las imágenes

[98] Yolanda Corral, Yolanda Corral, Wacrypt, software para la extracción de conversaciones de WhatsApp, realiza un análisis forense a tu ordenador, 2019. Disponible en: https://www.yolandacorral.com/wacrypt-software-analisis-whatsapp/ consultado: octubre de 2019

a baja resolución pero visible perfectamente el contenido de la misma, brindando la ventaja que, independientemente la imagen haya sido o no descargada en el dispositivo móvil, el thumbnail existe en la conversación; Así como las conversaciones grupales, desplegando información de mensajes multimedia enviados, número de participantes, cantidad de audios enviados, así como cuenta con la posibilidad de calcular la firma hash, aunque se recomienda generar la firma digital por aparte, ya que esta herramienta la trabaja con MD5 y como se mencionó anteriormente, está ya puede llegar a ser falseada.

La herramienta cuenta con la característica de ser portable, por lo cual se podrá portar en el disco duro con las herramientas forenses sin la necesidad que se encuentre instalada en el ordenador.

La herramienta se puede solicitar en el siguiente contacto: info@thesecuritysentinel.es, perteneciente a Matías Moreno, consultor de Seguridad TI y hacking ético y desarrollador del software de Wacrypt. Hay que tomar en cuenta que dicha herramienta no es de código libre, pero tener al creador de la misma, siempre es un tanto a favor.

Un dato a tomar en cuenta, todas las imágenes que han sido enviadas por medios como lo son Facebook, Twitter o WhatsApp, por seguridad las empresas llegan a eliminar los metadatos de las imágenes con objetivos de privacidad. Aunque no ocurre lo mismo con todas las redes sociales, como lo es el caso de Google+, Flickr o Tumblr o los servicios de nube como Dropbox o Google Drive, ya que, en estas los archivos no son modificados.

3.4.2 Santoku Linux

"Es una distribución basada en Linux especialmente desarrollada para auditar dispositivos móviles en busca de vulnerabilidades, fallos o simplemente cualquier aspecto que pueda comprometer nuestra privacidad al utilizar cualquiera de estos dispositivos móviles."[99] Este es un sistema operativo forense con enfoque en los

[99] Redes Zone, Velazco Rubén, Santoku Linux, un sistema operativo para auditar dispositivos móviles, 2015. Disponible en: https://www.redeszone.net/2015/03/14/santoku-linux-un-sistema-operativo-para-auditar-dispositivos-moviles/ consultado: noviembre de 2019

dispositivos móviles, donde se puede realizar ingeniería inversa en las aplicaciones, detectar vulnerabilidades en software del dispositivo, hasta realizar una imagen forense del mismo.

Este último es el de interés para los peritos informáticos forenses. Para llevar a cabo la imagen forense, se utilizará la herramienta incluida en el sistema operativo: AFlogical, con esta herramienta se puede extraer y realizar una copia de los archivos como imágenes, videos, notas de voz, contactos, mensajes de texto y registro de llamadas. Así mismo realizar un reporte de los archivos encontrados de la misma manera que la información de marca, modelo, IMEI, toda información que individualice al dispositivo móvil.

Antes de llegar a utilizar la herramienta, hay que hacer unos pequeños pasos en el dispositivo móvil para que la realización de la imagen forense se lleve a cabo con éxito:

1. Colocar el dispositivo móvil en modo depuración: esta opción se encuentra dentro de “opciones de desarrollador”, modo que de fábrica viene oculto. Para desbloquearlo, se deberá acceder en la sección “acerca del teléfono” luego, en el apartado de “numero de compilación” tocar 7 veces para que las opciones de desarrollador aparezcan en el listado de ajustes del teléfono.
2. Permitir instalación de orígenes desconocidos: para llevar esto a cabo, dirigirse a “ajustes del teléfono”, acceder al apartado de “seguridad” y luego activar “fuentes desconocidas”

Ya iniciada la máquina virtual con el sistema operativo Santoku se procederá a seguir los siguientes pasos:

1. En la parte inferior izquierda cliquear la ventana en forma cuchillo. Esta es equivalente a la ventana “inicio” del sistema operativo Microsoft Windows.
2. Al ser está desplegada, se localizará el puntero en el apartado denominado “Santoku” seguidamente. En la nueva ventana desplegada, se colocará el puntero en el apartado “Device Forensics”.
3. Abrir la herramienta AF Logical OSE.
4. En la terminal se coloca el comando siguiente: “aflogical-ose”. Pedirá contraseña la cual se dejará en blanco. Se presionará “Enter”. Esto instalara la herramienta en el dispositivo móvil.

5. En el dispositivo móvil se desplegará una ventana con los apartados que se desean extraer. En este se seleccionarán los que sean de interés.
    a. Calling Calls: en este se extraerán los datos de las llamadas recientes realizadas en el dispositivo móvil.
    b. Contacts Phones: se realizará respaldo de los numero de teléfono que se encontraban almacenados en contactos.
    c. MMS: extraerá los mensajes multimedia que haya recibido el dispositivo móvil por medio de la red móvil.
    d. SMS: en este se extraerá los mensajes de texto que haya recibido el dispositivo móvil por medio de la red móvil.
6. seleccionar la opción de “Capture” en la herramienta de AFLogical en el dispositivo móvil
7. presionar la tecla “Enter” en la máquina virtual.

En el administrador de carpetas de Santoku, en la carpeta “aflogical”, se creará la carpeta nombrada con la fecha en la que se realiza la extracción. Dentro de ella, se localizarán los documentos generados que contienen información en relación al registro de llamadas, a los números telefónicos, mensajes de texto, así como la información del dispositivo móvil del cual se ha realizado la extracción.

Tomar en cuenta que los procedimientos descritos anteriormente deben ser muy bien documentados y justificados en la cadena de custodia, existiendo la posibilidad que la contraparte, pueda alegar en juicio que se estuvo manipulando la evidencia. Pero se debe aclarar al juez que es la única forma humanamente posible de poder tener acceso a la información almacenada dentro del dispositivo móvil.

Un punto negativo de esta herramienta es que no puede recuperar los datos que fueron borrados del dispositivo, cuando se trata de mensajes, contactos o llamadas realizadas.

Hay que tomar en cuenta que no existe una herramienta forense que cuente con soporte para obtener información de todos los dispositivos existentes, por lo que debe haber software especializado para cada modelo. Acto que, para los laboratorios informáticos forenses, sería un gasto considerable comprar la licencia de cada uno, debido al alto costo que esto significa.

También existe hardware forense especializado en la extracción de información de dispositivos móviles, tales como MSAB Office o el famoso equipo UFED que automatizan gran parte del análisis de dispositivos móviles, llegando a ahorrar horas de trabajo, que a la vez significa menor gasto económico.

3.4.3 MSAB Office

Desarrollado por la empresa MSAB, quien desarrolla soluciones forenses aplicados a dispositivos móviles. *"MSAB Office es el sistema forense multiusos de MSAB que ofrece las soluciones de productos XRY en un paquete. MSAB Office permite a los investigadores acceder a todos los métodos posibles para recuperar datos de un dispositivo móvil. XRY es una solución específica basada en software, completa con todo el hardware necesario para recuperar datos de dispositivos móviles de una manera forense segura. Con MSAB Office puede lograr más y profundizar en un dispositivo móvil para recuperar datos vitales."* [100] Este kit se conecta junto a un ordenador para poder producir un informe forense junto a la información que fue extraída del equipo móvil utilizando archivos de extensión HTML, DOCX O GPX, entre otros. Esta herramienta funciona bajo el sistema operativo de Windows, por lo que no podría ser utilizado en el sistema operativo basado en Unix.

La herramienta incluye todos los tipos de adoptadores de conexión con los puertos de los dispositivos móviles, desde versiones anteriores de celulares como Nokia, motorola Sony Ericsson así como puertos de tipo micro USB y tipo C que son las conexiones actualmente por la mayoría de fabricantes de dispositivos móviles. También cuenta con un asistente que cuenta con la capacidad de examinar 3 dispositivos móviles diferentes al mismo tiempo. También cuenta con un archivo que es de ayuda al proporcionar información de cada dispositivo soportado, de qué tipo de archivos es posible o no recuperar de cada uno.

Hay que tomar en cuenta que esta herramienta trabaja con tecnología forense de bastante potencia, por lo que la empresa MSAB presta servicio a unidades militares,

[100] MSAB, MSAB Office, 2018. Disponible en: https://www.msab.com/es/productos/msab-platforms/#office consultado: noviembre de 2019

organizaciones gubernamentales o empresas privadas de seguridad o investigación. No prestan servicio a particulares.

3.4.4 UFED

"El equipo UFED extrae datos vitales, como agenda de contactos, fotografías de la cámara, vídeos, audio, mensajes de texto, registros de llamadas, ESN/IMEI, ICCID e información de IMSI en más de 1,600 modelos de teléfono móvil, incluidos dispositivos Symbian, Windows Mobile, BlackBerry y Palm OS." [101] Esta herramienta es la más utilizada a nivel mundial. Esta herramienta es capaz de acceder a los datos almacenados en los dispositivos móviles, aun cuando este cuente con bloqueo sea patrón, PIN, incluso huella digital. Su uso es bastante simple, basta con seleccionar que modelo de dispositivo se va a analizar, así como tipo de información que se desea extraer. Seguidamente se selecciona el almacenamiento externo en el cual quedara guardada la información. Luego, desplegara una lista con pasos concretos a seguir según sea el modelo del dispositivo para llevar a cabo el análisis.

El proceso a seguir para la extracción de información utilizando el equipo elaborado por CelleBrite UFED, es el siguiente:

1. Identificar el tipo de dispositivo móvil.
2. Conectar mediante el puerto del dispositivo con el cable que proporciona el equipo
3. Conectar a un ordenador o un medio de almacenamiento.
4. Iniciar el proceso en el equipo.

El proceso demorara según la cantidad de información que contenga el dispositivo móvil. Al finalizar, desplegara el informe detallado del análisis el cual contara con la opción de imprimir o ser enviado mediante correo electrónico.

Al tener esta herramienta conexión con el CPU y la memoria interna, podrá extraer información como:

1. Registro de llamadas, incluidas las borradas de la tarjeta SIM.
2. Contactos.

[101] OnData International, Análisis de microteléfonos móviles, España, 2015. Disponible en: https://www.ondata.es/recuperar/ufed.htm/ consultado: noviembre de 2019

3. Imágenes.
4. Videos.
5. Archivos de audio.
6. Geo-etiquetas generadas por la aplicación de Google maps.

Siendo una herramienta poderosa de gran ayuda para los peritos informáticos forenses al contar con soporte para la mayoría de equipos en el mercado, y automatizar la mayor parte del análisis, y sumando la capacidad de ser portátil, podría ser utilizado en escena para realizar ahí mismo la extracción de datos de forma rápida y sencilla.

3.5 Sistema operativo MacOS

Referente a los sistemas operativos elaborados por parte de Apple, MacOS y IOS, al ser apagadas, se reinician y son cifradas con contraseñas con demasiados dígitos, provocando que el descifrar sea una acción que lleve demasiado tiempo y por consecuencia bastante costosa.

Así como se pudo observar en el caso San Bernandino que fue un tiroteo que acabo con la vida de 14 personas, en la ciudad de California, Estados Unidos. En el cual un dispositivo móvil IPhone fue obtenido por el FBI. *"El FBI tuvo un conflicto de alto perfil para obligar a Apple Inc. a desbloquear el iPhone, incluso acudió a los tribunales en un caso que enfrentaba a la seguridad nacional con la privacidad digital."* [102] Este análisis solo pueden llevarse a cabo mediante hardware bastante potente y por ende, costoso. Como son los equipos desarrollados por UFED y MSAB, los cuales serán temas tratados a nivel general, ya que las empresas prestan servicios únicamente a entidades de seguridad o empresas privadas con enfoque forense, no contando con mayor información del equipo en los sitios web oficiales, más que datos de soporte técnico para los que cuenten con permiso de licencia de uso.

Si en caso se encontrara una maquina sin algún parámetro de bloqueo, la imagen forense con un sistema operativo MacOS montado, podrá ser analizado mediante las

[102] Los Ángeles Times, Tanfani Joseph, La carrera para desbloquear el iPhone del terrorista de San Bernardino, se retrasó debido a la pobre comunicación del FBI, según un informe, 2018. Disponible en: https://www.latimes.com/espanol/eeuu/la-es-la-carrera-para-desbloquear-el-iphone-del-terrorista-de-san-bernardino-se-retraso-debido-a-la-pobre-20180327-story.html consultado: octubre de 2019

herramientas de FTK Imager, Autopsy o OSForensic, herramientas cuya metodología ya fue detallada anteriormente.

3.6 Funcionamiento de un ordenador

Los ordenadores son de las herramientas que la sociedad utilizada día a día, ya sea en cuestiones laborales, estudiantiles o meramente de óseo, puesto que el ordenador "*es una máquina capaz de realizar multitud de acciones con una gran precisión y rapidez. Para realizar esta estas tareas deben recibir unos datos de entrada llevar a cabo el tratamiento de esos datos (procesarlos) y brindar una salida o resultado. La entrada de datos es facilitada por los periféricos de entrada (teclado, ratón, escáner, etc.). La salida es gestionada por los dispositivos de salida (monitor, impresora, plóter, etc.).*"[103] por lo que los ordenadores son perfectos para poder almacenar información así como contenido multimedia, lo cual lo hace perfecto para poder realizar investigaciones o conocer más a fondo a los usuarios del mismo.

"*En este momento, es bueno recordar que un sistema informático está constituido en forma tripartita por los recursos de hardware, los recursos de software y los usuarios, siendo cada una de sus partes tan importante como las otras dos*".[104] Como se menciona, los recursos hardware *"es el conjunto de componentes físicos de los que está hecho el equipo"*[105] serán todas aquellas partes palpables de un ordenador, como lo es la tarjeta madre, la memoria RAM, el disco duro, etc.; *"El Software son los programas de aplicación y los sistemas operativos que permiten que la computadora pueda desempeñar tareas inteligentes, dirigiendo a los componentes físicos o hardware."*[106] Este será el encargado de brindar los datos e instrucciones al hardware

[103] Información Jurídica Inteligente, Duarte Abraham, El ordenador personal y sus componentes físicos, 2016. Disponible en: https://libros-revistas-derecho.vlex.es/vid/ordenador-personal-componentes-445312734 consultado: octubre de 2019

[104] Fox, Andina. *Linux desde cero: guía práctica de instalación, configuración y administración*, Argentina, Gradi S.A., 2011, Pág.19.

[105] GCFGlobal, Informática Básica - ¿Qué es hardware y software?, S/A. Disponible en: https://edu.gcfglobal.org/es/informatica-basica/que-es-hardware-y-software/1/ consultado: noviembre de 2019

[106] Milenium, software, México, 2017. Disponible en: https://www.informaticamilenium.com.mx/es/temas/que-es-software.html consultado: noviembre de 2019

para desempeñarse; el usuario será la persona que utilice el ordenador y lleve a cabo distintas acciones en el mismo.

"Hablando de aplicaciones, debemos dejar de lado el concepto de aplicaciones para Windows. Es un error muy común pensar que podremos utilizar programas desarrollados para el sistema operativo de Microsoft en Linux. En líneas generales, las aplicaciones son compatibles con el sistema operativo para el que han sido creadas. Por ejemplo, los programas para Mac OSX sólo funcionan en él, y esto se repite para todos los sistemas operativos" [107] actualmente se ha podido solucionar esto, mediante software como VMware Workstation. capaz de montar una máquina virtual con un sistema operativo distinto al que se tiene instalado en el ordenador. Siendo de gran utilidad en el mundo forense, al poder montar en una máquina virtual la imagen forense de un equipo bajo investigación y poder trabajar con él, como si de la computadora original se tratara.

3.6.1 Hardware de interés forense en los ordenadores

el hardware serán las partes que entraran en contacto con el perito forense, por lo que el perito deberá conocer las de importancia forense, siendo estas las mencionadas a continuación:

3.6.1.1 Disco duro

"El disco duro es un dispositivo de almacenamiento permanente (su contenido no se borra al apagar el ordenador). Está colocado dentro de la Unidad Central. No es visible desde el exterior a menos que se desmonte la tapa." [108] En este, se almacenara el sistema operativo, información utilizada por el software instalado en el ordenador, así como archivos ya sean de video, audio, imágenes, documentos, etc. Un dato interesante es que un mismo ordenador puede estar formado por más de un disco

---

[107] Fox, Andina. *Linux desde cero: guía práctica de instalación, configuración y administración*, Argentina, Gradi S.A., 2011, Pág.19.

[108] Vishub, El ordenador: hardware y software, España, S/A. Disponible en: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&cad=rja&uact=8&ved=2ahUKEwjx1-v1pYfoAhWsVt8KHWT9BToQFjAFegQIBhAB&url=https%3A%2F%2Fvishub.org%2Fdocuments%2F5875%2Fdownload&usg=AOvVaw3kdqyuY-5Rbh28KHiPkQD5 consultado: noviembre de 2019

interno. El disco interno es el que se encuentro dentro de la carcasa del ordenador, de la misma forma, se le pueden colocar discos externos a través de puertos USB o SATA.

Debido a que el perito informático forense manipulara en la mayoría de casos este dispositivo, debe tomar en cuenta que este *"Tiene dos cables, uno de suministro eléctrico para sus motores y circuitos, y otro de datos por el que 'viaja' la información desde el disco a la placa base y por ella a la CPU, la memoria y otras partes del ordenador."*[109]

3.6.1.1.1 Borrado Seguro

Muchas veces los usuarios piensan que con borrar la información y vaciar la carpeta de reciclaje, eliminaran de forma permanente los datos, o ya se mediante el formateo de una USB o un disco duro, esto es completamente falso. Aun cuando realicen este procedimiento. Mediante un file carving es posible recuperar información.

"*se requiere de la realización de varias pasadas de bits de 1 a 0 con objeto de garantizar que una información no es recuperable ni haciendo uso de elementos hardware altamente especializados."* [110] El tema de un borrado seguro, para garantizar que la información ha sido eliminada por completo, quedara determinado según las "pasadas" que se realizan sobre la misma información. Las pasadas hacen referencia a las veces que sobrescriba información nueva sobre la información vieja que se quiere eliminar.

"Cuando borras un archivo de un disco duro, generalmente no lo estás borrando realmente. Estás eliminando la referencia a ese archivo. Es como si hicieras desaparecer la ficha de un libro en una biblioteca, no tienes referencia al libro en ningún sitio, pero sigue estando ahí, en las estanterías, en alguna parte, y si buscas con paciencia lo puedes encontrar."[111] Los discos duros están formados por pequeños sectores a los cuales se les denomina Clousters. Entonces, al realizar un borrado,

---

[109] *Loc. cit.*

[110] García Rambla, Juan Luis. óp. Cit., Pág.22.

[111] La libertad digital, Rodríguez Herrera Daniel, Método Guttman: ¿por qué el PP borró el disco duro de Bárcenas 35 veces, y no 34 o 36?, España, 2016. Disponible en: https://www.libertaddigital.com/ciencia-tecnologia/tecnologia/2016-02-15/metodo-guttman-por-que-el-disco-duro-de-barcenas-se-borro-35-veces-y-no-34-o-36-1276567859/ consultado: agosto de 2019

solamente se eliminará la dirección de la ubicación de los sectores por lo cual, se puede acceder a estos mediante software especializado para recuperar la información. Ahora mismo existen herramientas desarrolladas por militares, que, para salvaguardar información, ya a niveles muy alto de seguridad e investigación, con dar 20 pasadas sobre la información, aun siendo estos datos aleatorios, puede llegar a borrar de forma definitiva la información de relevancia.

"*Sirvan como ejemplo aparatos como el Garner PD-5 Hard Drive SSD Flash Data Destroyer, una imponente máquina que consigue que cualquier dato, por sensible que sea, desaparezca del todo."*[112] Siempre existen las alternativas de software para estos casos, como lo podemos ver con Darik's Boot and Nuke o por sus siglas DBAN siendo este gratuito (www.dban.org). O por medio de herramientas incluidas en suites forenses como en el caso de Caine (www.caine-live.net)

Este tema es de ayuda al perito informático forense ya que antes de almacenar una copia forense dentro de un medio de almacenamiento, previamente deberá realizar una sanitización del mismo, mediante un borrado seguro para que no intervengan datos de imágenes forenses que hayan sido almacenadas anteriormente en el mismo disco duro.

3.6.1.2 Memoria RAM

"memoria de acceso aleatorio. es la memoria principal del ordenador. Es una memoria volátil, su contenido se borra al apagar el ordenador. En ella se carga el sistema operativo, el programa o programas que estemos usando y los archivos de trabajo: textos, fotos, sonido, etc. También se almacenan en ella otros programas como el antivirus que están gestionados directamente por el sistema operativo."[113] Esta es donde el ordenador guarda la información que está utilizando en el momento, la

[112] La Vanguardia, Otto Carlos, No hacía falta formatear 35 veces el ordenador de Bárcenas: así puedes borrar todo en sólo dos pasos, España, 2016. Disponible en: https://www.lavanguardia.com/tecnologia/20160806/403712293181/metodo-gutmann-barcenas-disco-duro-pp-formatear-dos-pasadas.html consultado: agosto de 2019

[113] Vishub, El ordenador: hardware y software, España, S/A. Disponible en: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&cad=rja&uact=8&ved=2ahUKEwjx1-v1pYfoAhWsVt8KHWT9BToQFjAFegQIBhAB&url=https%3A%2F%2Fvishub.org%2Fdocuments%2F5875%2Fdownload&usg=AOvVaw3kdqyuY-5Rbh28KHiPkQD5 consultado: noviembre de 2019

principal diferencia de la RAM es que trabaja de una forma más rápida pero al momento de que el ordenador sea apagado, todos los datos que contiene, serán eliminados.

3.6.2 Sistemas Operativos en ordenadores

Dentro del software, lo más importante para el perito informático forense es conocer y poder manejar los distintos sistemas operativos existentes, para que a la hora que, en una escena del crimen se encuentre un ordenador con un sistema operativo fuera de lo cotidiano, pueda desempeñar su labor de la forma más efectiva posible. Los sistemas operativos según el Ingeniero en Telemática Santiago Felici, "se tratan de *"un software que proporciona un acceso sencillo y seguro al soporte físico del ordenador (hardware), ocultando al usuario detalles de la implementación particular."* [114] más comunes entre computadores son:

3.6.2.1 Microsoft Windows

"Windows es un sistema operativo creado por Microsoft. Consiste en un conjunto de programas que permiten la ejecución de los recursos que tiene un ordenador. El significado del término (Windows, ventanas) hace alusión a su interfaz gráfica, que presenta un modelo basado en tareas y compartimentos independientes, con sus propios menús y controles." [115] El sistema más común alrededor del mundo, a diferencia de GNU/Linux, cuenta con una interfaz gráfica amigable para que sea utilizado por los usuarios de forma intuitiva. Debido a esto, este el sistema operativo que cuenta con más herramientas desarrolladas para poder recabar todo tipo información de índole forense para poder llegar a la verdad de los hechos de un delito donde se encuentre implicado un equipo informático.

Un inconveniente que presenta este sistema operativo para montar un laboratorio informático forenses es que, debido a que la interfaz gráfica y otros factores, necesita de potencia para poder correrlo, se requiere que cuente con un ordenador con

[114] Universitat de Valencia, Felici Santiago, Sistemas operativos, España, S/A. Disponible en: https://informatica.uv.es/it3guia/FT/cap5-ssoo-ft.pdf consultado: noviembre de 2019

[115] SoftwareLab, ¿Qué es Windows? Definición e historia, España, 2017. Disponible en: https://softwarelab.org/es/windows-historia/ consultado: noviembre de 2019

hardware potente, para llevar a cabo investigaciones y que todo corra de forma fluida.

3.6.2.2 MacOS

"Mac OS, Sistema Operativo de Macintosh es el nombre del sistema operativo creado por Apple en 1984, para su línea de computadoras Macintosh (Mac). Es conocido por haber sido el primer sistema dirigido al público en contar con una GUI (Interfaz Gráfica de Usuario), compuesta por la interacción del mouse con ventanas, Icono y menús." [116] Sistema operativo caracterizado por su seguridad, y su pequeño porcentaje de virus. Mismo aspecto que no permite mayor configuración o personalización por parte del usuario.

Entre los inconvenientes de este sistema operativo es que en cuestiones forenses, si se desea utilizar como laboratorio forense, no pocas las herramientas que podrán ser utilizadas desde ella. Lo aconsejable es montar una máquina virtual con el sistema operativo Windows, Santoku, Kali Linux, entre otros. para poder realizar análisis forenses de una forma más completa.

3.6.2.3 GNU/Linux

Linux *"es un sistema operativo que, al igual que cualquier otro (como puede ser Windows o Solaris), nos brinda operatividad sobre una computadora."* [117] Entre las diferencias que encontramos de este sistema operativo es que su software es 100%libre, lo que significa que existen distintas versiones o distribuciones desarrolladas y adoptadas para distintas necesidades. Así mismo se podrá recurrir a soporte oficial, alguna empresa o recurrir a la comunidad Linux en busca de soporte.

Entre las desventajas que presenta este sistema operativo es que, en caso se necesite instalar una herramienta, cada distribución tendrá una manera distinta para instalar estas mismas.

---

[116] Revistas Publicando, Loarte Cajamarca Byron Gustavo, Desarrollo de una Guía Metodológica para el Análisis Forense en Equipos de Cómputo con Sistema Operativo Mac OS X, Ecuador, 2018. Disponible en: https://revistapublicando.org/revista/index.php/crv/article/view/1093 consultado: noviembre de 2019

[117] Rivero, Franco, *tóp.cit*, Pág. 19.

Un problema considerable con el que se puede topar un perito informático forense en escena, si el equipo sospechoso, contara con una de las distribuciones del sistema operativo GNU/Linux, el volcado de memoria RAM no sería posible que se llevase a cabo, debido a que el kernel de Linux, bloquea el exceso a esta, por lo cual el volcado no es posible. Salvo en una circunstancia muy particular, con fines científicos, instalando herramientas que deben ser compiladas específicamente para la maquina a analizar, llegando a dar permisos de superadministrador para que este pueda tener acceso a nivel Kernel y se pueda realizar el volcado, pero ya en escenario esto no es práctico, y hay que tomar en cuenta que al dar permiso de Superadministrador, se estaría modificando el equipo de cómputo.

3.7 Funcionamiento Dispositivos Móviles

“Hoy en el mundo de la tecnología tenemos diferentes artefactos alrededor del mundo que forman parte de nuestro día a día, estos son llamados "Dispositivos móviles". Un dispositivo móvil, lo podemos definir, como un aparato de pequeño tamaño, el cual posee un sin fin de funciones, entre las cuales podemos mencionar, el procesamiento e intercambio de información, la conexión a alguna red, todo esto a través de una memoria interna e ilimitada.” Dentro de estos aparatos de un tamaño reducido con la capacidad de ser portátiles se encuentran: teléfonos inteligentes, tablets, cámaras digitales, entre otros. Estos cuentan con sistemas operativo como los ordenadores para poder llevar a cabo las ordenes que les ordene el usuario, así como poder entrelazar y comunicarse entre sí.

3.7.1. Hardware de interés forense en los dispositivos móviles

3.7.1.1 Tarjeta SIM

el Subscriber Identity Module, también conocido como tarjeta SIM. “*es una pequeña tarjeta de plástico que tiene un chip pegado a ella, y que tienes que insertar en tu teléfono móvil o smartphone. En este chip, almacena de manera segura tu número de teléfono, así como las claves de acceso de un usuario concreto en una operadora de*

telefonía." [118] Esta es una tarjeta inteligente desmontables con el objetivo de almacenar datos así como identificarse dentro de una red. El interés forense en ella, es debido a que almacena nombres y números de teléfono, así como mensajes de texto e información de configuración de la red.

3.7.1.2 Memoria del Dispositivo

Los dispositivos móviles actuales cuentan con una memoria de almacenamiento interna que puede ser de 16GB hasta 1TB. A la misma vez pueden ser ampliados mediante Tarjetas SD. Estas son "*provee a un teléfono celular o a un teléfono inteligente con memoria expandida, lo que te permite agregar más contenido, como videos, fotos y música."* [119] De esta es posible fotos, videos, notas de voz, todo tipo de archivos multimedia almacenados dentro del dispositivo móvil, siendo posible recuperar datos que hayan sido eliminados.

3.7.2 Sistemas Operativos en los dispositivos móviles

Los sistemas operativos que han pasado por Android, han sido varios, pero muchos de estos les han dejado de dar soporte como en el caso de Windows Phone y BlackBerry OS, por lo que ya no se encuentran en el mercado. Por lo que actualmente suelen encontrarse en este tipo de dispositivos los 2 siguientes:

3.7.2.1 Android

"Android es un sistema operativo inicialmente pensado para teléfonos móviles, al igual que iOS, Symbian y BlackBerry OS. Lo que lo hace diferente es que está basado en Linux, un núcleo de sistema operativo libre, gratuito y multiplataforma." [120] El más común de los sistemas operativos puesto que lo portan distintas marcas fabricantes de dispositivos como lo son Samsung, LG, Huawei, HTC, entre otros. así mismo, este

[118] Xataka, Yubal FM, Tarjeta SIM: cómo funciona y cómo saber de qué tipo es la tuya, España, 2019. Disponible en: https://www.xataka.com/basics/tarjeta-sim-como-funciona-como-saber-que-tipo-tuya consultado: noviembre de 2019

[119] Techlandia, Lou Martin, ¿Qué hace una Micro SD por tu teléfono celular?, España, 2019. Disponible en: https://techlandia.com/micro-telefono-celular-info_146799/ consultado: noviembre de 2019

[120] Xataka Android, Nieto González Alejandro, ¿Qué es Root? ¿Qué es Android?, España, 2019. Disponible en: https://www.xatakandroid.com/sistema-operativo/que-es-android consultado: noviembre de 2019

sistema operativo cuenta con la posibilidad de poder modificar hasta ciertos parámetros del mismo.

A partir de estos parámetros, en el mundo Android existe lo que se le conoce como "rootear". *"La palabra root proviene del inglés y su traducción al castellano es "raíz". Ser usuario root en un sistema Unix (como Android, Linux) significa tener acceso al directorio raíz, ese donde tenemos instalado todo el sistema operativo."* [121] Cediendo permisos de superadministrador al usuario para poder realizar cualquier modificación o tener acceso completo a información contenida en el dispositivo móvil.

Esto es de ayuda al perito informático forense ya que si en dado caso encontrase el dispositivo Android rooteado participe de un delito informático, podría realizar una copia bit a bit del dispositivo, que incluya datos tanto del usuario como del propio sistema, facilitando en casos que sea necesario recuperar datos que hayan sido eliminados.

A pesar de ser de ayuda para el desempeño del perito informático forense, cuenta con la desventaja que no se debe realizar a un dispositivo móvil que sirva de evidencia, ya que al rootear el dispositivo, se estaría alterando el mismo y por ende, será rechazado en tribunales.

3.7.2.2 IOS

"iPhone OS como antes era denominado, es un sistema operativo desarrollado por Apple, inicialmente solo para el teléfono inteligente de la compañía (el iPhone), luego fue extendido a otros dispositivos como el iPod Touch y el iPad." [122] Este sistema operativo solamente se encontrará en dispositivos desarrollados por la empresa Apple.

Realizar cambios en los parámetros del dispositivo es bastante limitado. Al igual que en Android existe el procedimiento "jailbreak". *"El jailbreak es el término genérico que se le ha puesto a los métodos que hay para saltarse las medidas de seguridad impuestas por Apple en su sistema iOS y poder instalar, modificar y cambiar cualquier*

[121] Androidpit, Calvo Daniel, ¿Qué es Root? Ventajas e inconvenientes de rootear tu Android, España, 2019. Disponible en: https://www.androidpit.es/root-que-es consultado: noviembre de 2019

[122] GCFGlobal, Sistema operativo móvil IOS, S/A. Disponible en: https://edu.gcfglobal.org/es/ipad/sistema-operativo-movil-ios/1/ consultado: noviembre de 2019

cosa del sistema."[123] Para ceder al directorio raíz del sistema operativo y tener acceso a toda la información contenida en el mismo.

En el caso de los dispositivos móviles, es un poco más complicado que un ordenador, donde se tiene el disco duro, se puede sacar de la carcasa y leer mediante software forense, pero al momento de hablar de un celular o una tableta, se puede realizar una copia forense al móvil, pero en alguna situación, se llegara a que se necesitar extraer información que solo es posible obtenerla mediante la elevación de privilegios. Pero esto ya cuenta como una modificación al equipo, y se toma como que se ha violentado la integridad de la evidencia.

Existe hardware y software automatizado que es aceptado en los juicios directamente, que logra realizar la extracción de la información de relevancia que no está al alcance a la metodología manual sin llegar a alterar en algún punto la evidencia.

[123] Cinco días El País, Bolaños David, Qué es el jailbreak y por qué, y cómo, debería hacérselo (o no) al iPhone 6, 2014. Disponible en: https://cincodias.elpais.com/cincodias/2014/10/23/lifestyle/1414081833_201902.html consultado: noviembre de 2019

CAPITULO VI
PRESENTACIÓN DE RESULTADOS

4.1 Presentación, análisis y discusión de resultados

A lo largo de la presente investigación, se realizó la depuración y selección de herramientas informáticas, las cuales fueron empleadas para la extracción de información, mediante criterio de validez y confiabilidad de los datos proporcionados por dichos softwares. Estos Softwares también son utilizados en el día a día de la empresa mexicana destinada la de ciberseguridad y computo forense: Duriva. La cual se encuentra avalada por la American Council For Security. Las herramientas comerciales mencionadas anteriormente, se solicitaron los demos de las herramientas, las cuales son efectivas alrededor de 25 días.

De esta forma, El objetivo referente a establecer las herramientas forenses de análisis digital para la obtención de información aplicado a ordenadores y dispositivos móviles, se ha conseguido, brindando elementos con los cuales poder combatir los delitos informáticos que se realizan en Guatemala, esclareciendo de marera clara y concisa la forma en que se llevó a cabo el delito y de la misma manera, la o las personas que participaron.

El software forense recomendable bajo criterio propio y, tomando en cuenta que las suites forenses son más las completas, dado que cuentan con el compendio de herramientas necesarias para poder extraer un buen porcentaje de información necesaria para poder esclarecer el modus operandi del hecho informático. Esta herramienta es Tequila.

Lo que destaca a este software de las demás herramientas libres es que se encuentra Herramienta desarrollada en la universidad Nacional Autónoma de México. validada a la vez por el Consejo Nacional de Ciencia y Tecnología, la secretaria de la Defensa Nacional de México, así como distintas policías cibernéticas. Este software es capaz

de investigar cualquier delito informático, ya haya sido realizado en un ordenador o un dispositivo móvil.

Debido a que esta herramienta es completamente gratuita, lo cual no presentaría problema alguno si se necesitase presentar evidencia extraído con este mismo software frente a un tribunal competente. Así mismo, de este software se desprende lo que se conoce como Agave, que es una herramienta que se puede portar ya sea mediante USB o CD para ser utilizada en primera respuesta a un incidente que incluya equipo informático. puede extraer información crucial en la misma escena con el beneficio que no modificara los parámetros del ordenador, lo que no alteraría el indicio y por ende, pueda ser presentado de forma exitosa en un juicio.

Esta además es la herramienta más completa de todas, puesto que con ella se puede realizar desde copias forenses, poder interpretar información de los usuarios de una imagen forense, capaz de romper contraseñas ya sea de archivos o cuentas, verificar la autenticidad de un correo electrónico, entre otros. Contando con varias alternativas dentro de la misma para poder extraer un mismo tipo de información, por cual se podrá elegir con el cual el perito informático forense se sienta más cómodo.

La interface que utiliza es amigable, por lo que cual puede ser utilizada por principiantes, aunque hay que tener en cuenta es que, si se desea poder utilizar el potencial de Tequila al cien por ciento, se necesita contar con conocimientos en el manejo de GNU/Linux, ya que es mediante comandos en consola que se le da las ordenes exactas al software para que esta extraiga la información de interés.

Un aspecto a tomar en cuenta, es que los peritos informáticos forenses deberán mantener en constante actualización de conocimientos en el empleo de estas herramientas o las cuales se vayan desarrollando con el paso del tiempo en el campo de la informática. Puesto que esto les permitirá llevar a cabo el análisis forense con técnicas a la vanguardia, resolviendo casos de la manera más efectiva y brindando datos fieles al sucedido.

Esto con el fin de atenuar el inconveniente que existe en Guatemala. Debido a la falta de una ley penal enfocada a regular los delitos informáticos provoca que muchas veces, las partes judiciales no tengan claro cómo proceder ante estos casos, causando que acciones del hecho, queden ser esclarecidas o que estas mismas conductas malintencionadas queden impunes. Así mismo, la falta de capacitación del personal de respuesta ante hecho ilícito informático, obstaculiza la persecución penal llegando al punto de invalidar los indicios que puedan ser.

Estos pueden ser invalidados por dos puntos importantes: romper la cadena de custodia y la contaminación la evidencia digital, lo cual disminuye la confiabilidad de la misma, provocando que la parte contraparte puede cuestionar y finalmente generar dudas en la validez de la evidencia por parte del juez.

CUADRO DE COTEJO

Unidades de Análisis

INDICADOR	OSForensic	Autopsy	Tequila
Casa productora	La casa productora de esta suite forense es la empresa: PassMark Software Pty Ltd. Grupo especializado en desarrollar servicios de Tecnologías de la Información (TI). Así mismo, presta resultados de referencia de pruebas comparativas y de rendimiento.	La casa productora de la suite forense es: The Sleuth Kit (TSK). Biblioteca y colección de comandos basados en Unix y Windows enfocado al análisis forense de equipos informáticos.	Elaborado en la facultad de Ingeniería de la Universidad Nacional Autonomía de México (UNAM).
Plataforma (Sistema operativo)	• Microsoft Windows: Windows 7 x32 x64, Windows 10, Windows 8, Windows Vista. Windows Server 2000, 2003, 2008, 2012, 2016, 2019.	• Microsoft Windows: Windows 7, Windows 10, Windows 8, Windows Vista. En las variantes de x32 y 64x. • Linux: mediante líneas de comando.	No es posible instalarla dentro de un sistema operativo Windows Linux o Mac, puesto que es casi como un sistema operativo en sí, el cual se encuentra basado en GNU/Linux.

		• Mac: OS X.	
Requisitos de Hardware	• excluir del antivirus del ordenador, la carpeta donde se designó la base de datos del directorio, para evitar que este interfiera con los resultados. • Tomar en cuenta que si el ordenador que se utilizara como laboratorio, es un equipo de alto rendimiento, menor será el tiempo de espera para poder extraer la información.	• Si el equipo utilizado de laboratorio cuenta con antivirus, este deberá se desactivado por el tiempo en que se lleve a cabo el análisis forense. Ya que puede borrar o bloquear resultados que produzca la suite forense. • Tomar en cuenta que si el ordenador que se utilizara como laboratorio, es un equipo de alto rendimiento, menor será el tiempo de espera para poder extraer la información.	• El ordenador deberá contar con una partición disponible para instalar en ella el software forense. • Tomar en cuenta que si el ordenador que se utilizara como laboratorio, es un equipo de alto rendimiento, menor será el tiempo de espera para poder extraer la información.

Tamaño de Archivo	133 megabytes aproximadamente.	824 megabytes Aproximadamente.	2.0 Gigabytes aproximadamente.
Tipo de código	Basado en GNU/Linux	Basado en GNU/Linux	Basado en GNU/Linux
Ventajas	• Es una herramienta forense automatizada, por lo cual el poder extraer información de una imagen forense será simple. • Realiza una línea de tiempo de la evidencia extraída, facilitando al perito forense el correlacionar eventos digitales del delito. • A diferencia con las demás suites, cuenta con la posibilidad de poder realizar un cotejo del sistema operativo comparándolo con los archivos de una instalación limpia con	• Herramienta forense automatiza, por lo cual extraer información de un equipo de cómputo será simple. • Podrá trabajar directamente con un archivo de VMware, una máquina virtual. • Esta suite forense es de código libre, por lo cual no es necesario comprar la licencia para poder utilizarla y presentar evidencias extraídas con ella en un proceso judicial.	• Al ser un sistema operativo, esta cuenta con una gran cantidad de herramientas para poder llevar acabo análisis forenses, aun mas que las demás suites mencionadas. • La suite forense es de código libre por lo cual es libre y gratuito. • Cuenta con comunidad de apoyo donde todos los

	el objetivo de localizar si algún archivo ha sido modificado. • Cuenta con el apartado Android Analyzer el cual será capaz de analizar el backup de un dispositivo móvil Android. • Posibilidad de ir validando en el proceso de análisis si la imagen forense permanece integra. • En la página web oficial de PassMark, ofrece cursos de capacitación en línea dirigido a investigadores forenses digitales con el objetivo de ampliar sus habilidades en el empleo de OSForensic en casos judiciales, preparando a los aspirantes un certificado al completar el examen "OSForensic Certified	• La empresa Basis Technology especializada en técnicas de inteligencia artificial es la fuente autorizara para impartir cursos en el adiestramiento del programa. Mediante video conferencias y laboratorios prácticos. http://www.cybertriage.com/	interesados pueden contribuir para enriquecer el sistema, consultarse y ayudarse los unos a los otros. • La empresa Duriva, liderada por uno de los desarrolladores de tequila: Jocsan Laguna, imparte cursos y certificaciones a través de Latinoamérica en peritaje informático abarcando la misma suite: https://duriva.com/cursos/

	Examiner”. https://www.osforensics.com/		
Desventajas	• La herramienta cuenta con un periodo de prueba de 30 días, posteriormente si desea utilizarse, deberá de ser comprada la licencia.	• No existe una versión portable de la misma, por lo cual no se podrá llevar en el disco duro que se utiliza para la extracción de información en escena. • No cuenta con una oficina física, número de teléfono o correo electrónico al cual contactarse para soporte. • a pesar de ser gratis, los cursos impartidos para utilizar de la forma más eficiente la suite,	• Se maneja mediante comandos de Linux, por lo cual previamente se deberá de tener conocimientos en estos para poder aprovechar al cien por ciento el potencial de las herramientas. • Para poder utilizar esta suite forense será necesario instalarla en alguna partición del equipo de cómputo o bien,

		son más caros que los demás vistos.	levantar una máquina virtual.
Soporte/Contacto	• PassMark Software Inc. 370 Convention Way, Nivel 2 Redwood City, California 94063 Estados Unidos • info@passmark.com • +1 650 216 2306 +1 650 251 4144	Soporte brindado únicamente a través de la página web oficial: https://www.autopsy.com/support/ Este soporte es pagado; puede publicar preguntas en el foro público: https://sleuthkit.discourse.group/	• Ciudad Universitaria – UNAM Edificio Q "Luis G. Valdés Vallejo", 2do piso PROTECO Anexo de Ingeniería, Ciudad Universitaria, Ciudad de México.
Descarga	https://www.osforensics.com/download.html	https://www.autopsy.com/download/	https://tequila-so.org/descargar/
Función Hash	SHA-1: DE256751CE1543858 - 71954F669D562C7B02906E2	SHA-1: 70B94ACAB1DDC9B3 - EE438A972EF29F7D97137984	SHA-1: 683CEED434C294CCC - A991BAF35BF96DC23CFF43B

CONCLUSIONES

1. Con el avance tecnológico a grandes pasos, se ha logrado que se creen nuevas formas de poder contrarrestar los delitos informáticos mediante las herramientas que utilizan cada vez requisitos menos exigentes, así mismo han sido automatizadas permitiendo a los peritos informáticos forenses realizar análisis profundos obteniendo información una forma más simple y rápida.

2. A pesar de los avances a nivel global de la informática forense, en la mayor parte de Latinoamérica aún tienen mucho camino por recorrer referente a la elaboración de leyes que regulen los delitos informáticos, sobre todo si se compara con países como Estados Unidos o España, donde existen infinidad de planes de formación a la vanguardia para la profesionalización en Informática forense.

3. La Informática varía mucho a las demás ciencias forenses, puesto que el desarrollo tecnológico avanza a una velocidad increíble, llegando a evolucionar de forma constante el hardware y el software que componen a los dispositivos electrónicos. Provocando que los delincuentes obtén por utilizar nuevas formas de vulnerar estos equipos. Motivo por el cual es imprescindible mantenerse a la vanguardia para estar preparado ante las distintas situaciones que se puedan llegar a presentar.

4. Uno de los hechos que ayudan de forma positiva a los peritos informáticos forenses son las rutinas que los usuarios llevan a cabo en los ordenadores o dispositivos móviles, ya que, a la hora de analizar los datos extraídos de estos, es posible detectar los eventos que se salen de las actividades diarias, permitiendo localizar por donde darle seguimiento a esta irregularidad y contribuir a la reconstrucción los hechos.

5. La informática podrá ser aplicada en la resolución de casos incluso donde un ordenador no se relacione de forma directa con el hecho delictivo, puesto que puede extraer o recuperar información eliminada intencionalmente que oculte información de: números de teléfono en caso fuera un delito de extorsión; los números de

cuentas bancarias si se hablase de algún tipo de fraude; números de tarjetas de crédito si se tratase de un caso de carding. Esto de manera certera, reuniendo la evidencia suficiente para esclarecer algún hecho delictivo.

RECOMENDACIONES

1. Cada una de los softwares forenses que se estudiaron a lo largo de esta investigación, presentan características diferentes, por lo que es se recomienda hacer usa de ellas en conjunto ya que complementándose se logra obtener mayor información y por ende, una visión más completa y aproximada de los hechos sucedidos en el delito.

2. Se recomienda brindar capacitaciones constantes en el tema a personal designado a respuestas ante un hecho delictivo, puesto que puede existir la posibilidad de encontrar equipo informático en la escena y por falta de conocimiento en cuanto al manejo, puede provocar que estos sean invalidados en el proceso judicial.

3. Si no se contase con bolsas Faraday, existe la alternativa más económica y casera de poder elaborar una caja que cumpla con esta función. Se necesita una caja ya sea de zapatos por ejemplo, y esta cubrirla de forma superpuesta con papel aluminio, con el objetivo de crear una estructura uniforme de aluminio. Buscando que esta sea lo más herméticamente posible para evitar que puedan ingresar o egresar señales que puedan alterar al dispositivo almacenado dentro.

REFERENCIAS

Bibliográfica

1. Di Lorio, Ana Haydee y otros. *El rastro digital del delito: aspectos técnicos, legales y estratégicos de la informática forense*, España, Universidad FASTA ediciones, 2017.
2. Ferro vega, José Manuel. *La ciencia forense al servicio de la Administración de Justicia y la Autoridad Policial*, España, Createspace Independent Pub, 2014.
3. García Chávez, Manuel. *Análisis forense con distribuciones GNU/Linux*, México, Universitat Oberta de Catalunya, 2016.
4. Keisler, Peter D. y otros. *Investigative Uses of Technology: Devices, Tools, and Techniques*, Estados Unidos, s/e, 2007.
5. Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense InFo-Lab, *Guía integral de empleo de la informática forense en el proceso penal*, Argentina, Universidad FASTA, 2016, segunda edición revisada.
6. Rifa Pous, Helena y otros. *Análisis forense de sistemas informáticos*, España, Eureca Media, 2009.
7. Casey, Eoghan, *Digital Evidence and Computer Crime*: Forensic Science, Computers, and the Internet, Estados Unidos, Academic Press, 2000.
8. Luengo Latorre, José Antonio, *Ciberbullying: prevenir y actuar*, España, Colegio oficial de psicólogos de Madrid, 2009.
9. Jara, Héctor y Federico Pacheco. *Ethical hacking 2.0*, Argentina, manuales Users, 2009, primera edición.
10. Rivero, Franco. *De Windows a Linux*, Argentina, manuales Users, 2009, primera edición.
11. García Rambla, Juan Luis. *Un forense llevado a juicio*, España, Creative Commons, 2014.
12. Wang, Xiaoyun. *How to Break MD5 and Other Hash Functions*, China, 2004, Shandong University.
13. Martínez Retenaga, Asier. *Guía de toma de evidencias en entorno Windows*, España, Creative Commons, 2014.

14. Torales, Eloy E., **Manual de procedimiento para la preservación del lugar del hecho y la escena del crimen**, Argentina, Ministerio de Justicia y Derechos Humanos de la Nación, 2014, primera edición.
15. VMware, VShere. *Administrar máquinas virtuales de vSphere*, España, VMware, Inc., 2009.
16. Fox, Andina. *Linux desde cero: guía práctica de instalación*, configuración y administración, Argentina, Gradi S.A., 2011.

Normativa

17. Organización Internacional de Normalización, ISO/IEC 27001:2013 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información – Requisito, 2013.
18. Organización Internacional de Normalización, ISO/IEC 27037:2012 Pautas para la identificación, recolección, adquisición y preservación de evidencia digital, 2012.
19. The Internet Society, RFC 3227, Pautas para la recopilación de evidencia y archivos, 2002.
20. Estados del Consejo de Europa, Convención sobre el Ciberdelito, convenio No.185, 2001.
21. Organización de los estados americanos, Manual de Manejo de Evidencias Digitales y Entornos Informáticos, 2011.

Electrónicas

22. Detectives Madrid: Agencia de Detectives Privados en Madrid, Historia de la informática forense y su actual aplicación, España, 2018. Disponible en: https://www.detectives-madrid.es/informatica-forense/historia-informatica-forense-aplicacion/
23. Disk Drill, Lista de las mejores herramientas de informática forense, Recuperación forense de datos, Análisis forense digital, Estados Unidos, 2018. Disponible en: https://www.cleverfiles.com/howto/es/computer-forensic.html
24. ElHacker, Introducción a la informática forense en entornos Windows 1ª parte, 2016. Disponible en: https://www.elhacker.net/InfoForenseWindows.html

25. Erick Programador, diferencia entre software libre y software comercial, 2015. Disponible en: https://programadorerick.wordpress.com/2015/10/02/diferencia-entre-software-libre-y-software-comercial/
26. HighSec, Análisis forense – parte 1 – como montar un laboratorio forense y clonar con DD, España, 2013. Disponible en: http://highsec.es/2013/09/analisis-forense-parte-i-como-montar-un-laboratorio-forense-y-clonar-con-dd/
27. Introducción a la informática forense Jeimy J. Cano, España, s/a. Disponible en http://52.0.140.184/typo43/fileadmin/Revista_96/dos.pdf
28. Okhosting, Software Comercial, 2014. Disponible en: https://okhosting.com/blog/software-comercial/
29. OnRetrieval, Elaine, Objetivos de la informática forense, España, 2018. Disponible en: https://onretrieval.com/objetivos-de-la-informatica-forense/
30. Preceden, Historia de la Ciencia Forense e Informática Forense, 2019. Disponible en: https://www.preceden.com/timelines/300848-historia-de-la-ciencia-forense-e-inform-tica-forense
31. Portaley, Análisis forense informático: Pruebas Periciales, España, 2013, Disponible en: http://portaley.com/2013/10/analisis-forense-informatico-pruebas-periciales/
32. Recovery Labs: Departamento de Peritaje Informático, Evidencia electrónica, España, 2018 Disponible en: http://delitosinformaticos.info/peritaje_informatico/evidencia_electronica.html
33. We live security. 3 distribuciones gratuitas recomendadas para el análisis forense, Argentina, 2016. Disponible en: https://www.welivesecurity.com/la-es/2016/02/23/distribuciones-gratuitas-analisis-forense/
34. We live security, Herramientas de informática forense: cómo encontrar la indicada para cada incidente, 2018. Disponible en: https://www.welivesecurity.com/la-es/2018/08/29/herramientas-informatica-forense-para-cada-incidente/
35. Instituto criminalístico forense, informática forense y dispositivos móviles, España, s/a, Disponible en: https://www.icfmurcia.es/seguridad-informatica/

36. Instituto nacional de ciberseguridad, Sanz Antonio, Quieres trabajar en informática forense. España, 2013, Disponible en: https://www.incibe-cert.es/blog/dominios-de-conocimiento-informatica-forense
37. Informática forense Colombia, Unicolombia, La Evidencia Digital, Colombia, 2017. Disponible en: https://www.informaticaforense.com.co/la-evidencia-digital/
38. Jurisplace, El Perito Judicial y su papel profesional, España, 2013. Disponible en: https://jurisplace.com/articulos/ver_contenido/que_es_perito/32/El%20Perito%20Judicial%20y%20su%20papel%20profesional
39. Peritajes informáticos, Delgado García José, Que es el informe pericial, España, 2018, Disponible en: https://jdgperitajesinformaticos.es/que-es-el-informe-pericial/
40. Xataka, Vanesa Quezada, Cómo se llega a ser el perito informático que analiza los discos duros de Bárcenas, España, 2016, Disponible en: https://www.xataka.com/ordenadores/como-se-llega-a-ser-el-perito-informatico-que-analiza-los-discos-duros-de-barcenas
41. Tecnología & informática , Graciela Marker, Tipos de licencias de software, España, 2016, Disponible en: https://tecnologia-informatica.com/tipos-licencias-software-libre-comercial/
42. EcuRed, Pupo Martínez Pavel David, Correo electrónico, Ecuador, 2010, Disponible en: https://www.ecured.cu/Correo_electr%C3%B3nico
43. Hostinet, ¿Qué son los DNS y que registros existen?, España, 2017, Disponible en: https://www.hostinet.com/formacion/general/que-son-dns-tipos-registros/
44. InternetLab, Filippi Simone, ¿Qué es CNAME y para qué sirve?, España, 2010, Disponible en: https://www.internetlab.es/post/972/que-es-cname-y-para-que-sirve/
45. CDmon, como configurar el registro de correo o registro MX, España, 2018, Disponible en: https://ticket.cdmon.com/es/support/solutions/articles/7000006119-c%C3%B3mo-configurar-el-registro-de-correo-o-registro-mx

46. CDmon, Cómo configurar el registro SPF para el correo en el DNS estático, España, 2017, Disponible en: https://ticket.cdmon.com/es/support/solutions/articles/7000006117-cómo-configurar-el-registro-spf-para-el-correo-en-el-dns-estático
47. Symantec, Implementar registros SPF en Email Security.cloud, España, 2017, Disponible en: https://support.symantec.com/es/es/article.tech226211.html
48. Nerion, García Pablo, ¿Qué es y cómo funciona ICANN?, España, 2017, Disponible en: https://www.nerion.es/blog/que-es-y-como-funciona-icann/
49. Sitio de la ICANN y su comunidad regional, sobre ICANN, Estados Unidos, 2018, Disponible en: http://icannlac.org/sobre-ICANN
50. Registro de dominios GT, Universidad del Valle, sobre nosotros, Guatemala, 2018, Disponible en: https://www.gt/sitio/us.php
51. Lacnic, Société Générale de Surveillance, Acerca de Lacnic, Caribe, 2017. Disponible en: https://www.lacnic.net/966/1/lacnic/acerca-de-lacnic
52. El País, Hackeada Zone-h, la principal base de datos de páginas 'hackeadas', España, 2017. Disponible en: https://elpais.com/diario/2007/01/18/ciberpais/1169091332_850215.htmll
53. Tecnología & Informática, Graciela Marker, ¿Qué es la Criptografía?, España, 2016, Disponible en: https://tecnologia-informatica.com/que-es-la-criptografia/
54. We live security, Paus Lucas, 5 fases fundamentales del análisis forense digital, España, 2015, Disponible en: https://www.welivesecurity.com/la-es/2015/04/15/5-fases-analisis-forense-digital/
55. División Forense, Bolsa de Faraday para dispositivos móviles, Argentina, 2015, Disponible en: https://www.division-forense.com/bolsa-faraday.html
56. Javier Rubillo Alamillo Perito informático, Análisis forense mediante bloqueo de escritura de un disco duro, 2016. Disponible en: https://peritoinformaticocolegiado.es/blog/caso-practico-de-peritaje-informatico-analisis-forense-mediante-bloqueo-de-escritura-de-un-disco-duro/
57. Tequila SO, Laguna Romero Jocsan, acerca de, 2016. Disponible en: https://tequila-so.org/acerca-de/

58. Solvetic, Solvetic Seguridad, Analizar imagen de disco con FTK Imager, 2016. Disponible en: https://www.solvetic.com/tutoriales/article/2567-analizar-imagen-de-disco-con-ftk-imager/
59. Reydes, Caballero Quezada Alonso Eduardo, Extraer Información del Registro de Windows con Registry Viewer, 2014. Disponible en: http://www.reydes.com/d/?q=Extraer_Informacion_del_Registro_de_Windows_con_Registry_Viewer
60. We live security, Pérez Ignacio, Maltego la herramienta que te muestra que tan expuesto estas en internet, 2014. Disponible en: https://www.welivesecurity.com/la-es/2014/02/19/maltego-herramienta-muestra-tan-expuesto-estas-internet/
61. (ISC) ² Comunidad, Análisis forense: ¡Autopsy 4.7 agrega visualización de enlaces, ZIP cifrado, base de datos y soporte de volatilidad!, 2018. Disponible en: https://community.isc2.org/t5/Industry-News/Forensics-Autopsy-4-7-adds-link-visualization-encrypted-ZIP/td-p/10442
62. Passware, Passware kit forensic, Estados Unidos, 2014, Disponible en: https://www.passware.com/kit-forensic/
63. Security Artwork, Olmedo Yolanda, Alternate Data Stream: ADS – Flujo de datos alternativos en NTFS, 2015. Disponible en: https://www.securityartwork.es/2015/02/23/alternate-data-stream-ads-flujo-de-datos-alternativos-en-ntfs/
64. Redes Zone, Velasco Rubén, ChromePass, una aplicación para ver las contraseñas de Google Chrome, 2016. Disponible en: https://www.redeszone.net/2016/09/06/chromepass-una-aplicacion-para-ver-las-contrasenas-de-google-chrome/
65. Soft Zone, Gómez Hugo, MyLastSearch 1.35, 2009. Disponible en: https://www.softzone.es/2009/02/04/mylastsearch-135-conoce-las-ultimas-busquedas-realizadas-en-tu-navegador-con-mylastsearch/
66. Redes Zone, Crespo Adrián, CurrPorts: averigua que programas acceden a internet en tu PC, 2013. Disponible en:

https://www.redeszone.net/2013/02/21/currports-averigua-que-programas-acceden-a-internet-en-tu-pc/

67. Cgsecurity, TestDisk, 2019. Disponible en: https://www.cgsecurity.org/wiki/TestDisk_ES
68. DragonJar, Restrepo Gómez Jaime Andrés, FOCA – Herramienta para análisis de Meta Datos, 2010. Disponible en: https://www.dragonjar.org/foca-herramienta-para-analisis-meta-datos.xhtml
69. WinRAR, que es WinRAR, 2013. Disponible en: https://www.winrar.es/soporte/articulo/30
70. DragonJar, Restrepo Gómez Jaime Andrés, Automatizando la extracción de evidencia forense en Windows, 2014. Disponible en: https://www.dragonjar.org/automatizando-la-extraccion-de-evidencia-forense-en-windows.xhtml
71. Genbeta, Fuentes Sacha, USBDeview, todos los dispositivos USB del sistema, 2009. Disponible en: https://www.genbeta.com/herramientas/usbdeview-todos-los-dispositivos-usb-del-sistema
72. Hipertextual, Sepharad, WhatInStartup controla qué se carga al iniciar Windows, 2009. Disponible en: https://hipertextual.com/archivo/2009/11/whatinstartup-controla-que-se-carga-al-iniciar-windows/
73. Indalics, De La Torre Rodríguez Pedro, Herramientas de informática forense, S/A. Disponible en: https://indalics.com/peritaje-informatico/herramientas-de-informatica forense#Suites_de_herramientas_forenses
74. Ecured, Autopsy, 2011. Disponible en: https://www.ecured.cu/Autopsy
75. Computerhoy, Rubén Andrés, Qué es cuello de botella en el PC y cómo evitarlo, 2018. Disponible en: https://computerhoy.com/noticias/hardware/que-es-cuello-botella-pc-como-evitarlo-79447
76. Proyecto TIC, OSForensics, realiza un análisis forense a tu ordenador, 2009. Disponible en: https://www.proyecto-tic.es/osforensics/
77. Nexolinux, Ficheros de usuarios /etc/passwd y /etc/shadow, 2013. Disponible en: http://www.nexolinux.com/ficheros-de-usuarios-etcpasswd-y-etcshadow/

78. ByteMind, ByteMind, Backup de seguridad en Linux con el comando dd, 2019. Disponible en: https://byte-mind.net/backup-de-seguridad-en-linux-con-el-comando-dd/
79. Yolanda Corral, Yolanda Corral, Wacrypt, software para la extracción de conversaciones de WhatsApp, realiza un análisis forense a tu ordenador, 2019. Disponible en: https://www.yolandacorral.com/wacrypt-software-analisis-whatsapp/
80. Redes Zone, Velazco Rubén, Santoku Linux, un sistema operativo para auditar dispositivos móviles, 2015. Disponible en: https://www.redeszone.net/2015/03/14/santoku-linux-un-sistema-operativo-para-auditar-dispositivos-moviles/
81. MSAB, MSAB Office, 2018. Disponible en: https://www.msab.com/es/productos/msab-platforms/#office
82. OnData International, Análisis de microteléfonos móviles, España, 2015. Disponible en: https://www.ondata.es/recuperar/ufed.htm/
83. Los Ángeles Times, Tanfani Joseph, La carrera para desbloquear el iPhone del terrorista de San Bernardino, se retrasó debido a la pobre comunicación del FBI, según un informe, 2018. Disponible en: https://www.latimes.com/espanol/eeuu/la-es-la-carrera-para-desbloquear-el-iphone-del-terrorista-de-san-bernardino-se-retraso-debido-a-la-pobre-20180327-story.html
84. Información Jurídica Inteligente, Duarte Abraham, El ordenador personal y sus componentes físicos, 2016. Disponible en: https://libros-revistas-derecho.vlex.es/vid/ordenador-personal-componentes-445312734
85. GCFGlobal, Informática Básica - ¿Qué es hardware y software?, S/A. Disponible en: https://edu.gcfglobal.org/es/informatica-basica/que-es-hardware-y-software/1/
86. Milenium, software, México, 2017. Disponible en: https://www.informaticamilenium.com.mx/es/temas/que-es-software.html
87. Vishub, El ordenador: hardware y software, España, S/A. Disponible en: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&cad=rja&uact=8&ved=2ahUKEwjx1-

v1pYfoAhWsVt8KHWT9BToQFjAFegQIBhAB&url=https%3A%2F%2Fvishub.org%2Fdocuments%2F5875%2Fdownload&usg=AOvVaw3kdqyuY-5Rbh28KHiPkQD5

88. La libertad digital, Rodríguez Herrera Daniel, Método Guttman: ¿por qué el PP borró el disco duro de Bárcenas 35 veces, y no 34 o 36?, España, 2016. Disponible en: https://www.libertaddigital.com/ciencia-tecnologia/tecnologia/2016-02-15/metodo-guttman-por-que-el-disco-duro-de-barcenas-se-borro-35-veces-y-no-34-o-36-1276567859/
89. La Vanguardia, Otto Carlos, No hacía falta formatear 35 veces el ordenador de Bárcenas: así puedes borrar todo en sólo dos pasos, España, 2016. Disponible en: https://www.lavanguardia.com/tecnologia/20160806/403712293181/metodo-gutmann-barcenas-disco-duro-pp-formatear-dos-pasadas.html
90. Vishub, El ordenador: hardware y software, España, S/A. Disponible en: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&cad=rja&uact=8&ved=2ahUKEwjx1-v1pYfoAhWsVt8KHWT9BToQFjAFegQIBhAB&url=https%3A%2F%2Fvishub.org%2Fdocuments%2F5875%2Fdownload&usg=AOvVaw3kdqyuY-5Rbh28KHiPkQD5
91. SoftwareLab, ¿Qué es Windows? Definición e historia, España, 2017. Disponible en: https://softwarelab.org/es/windows-historia/
92. Universitat de Valencia, Felici Santiago, Sistemas operativos, España, S/A. Disponible en: https://informatica.uv.es/it3guia/FT/cap5-ssoo-ft.pdf
93. Revistas Publicando, Loarte Cajamarca Byron Gustavo, Desarrollo de una Guía Metodológica para el Análisis Forense en Equipos de Cómputo con Sistema Operativo Mac OS X, Ecuador, 2018. Disponible en: https://revistapublicando.org/revista/index.php/crv/article/view/1093
94. Dialnet, Ponce Vázquez Diego, Observaciones acerca de los dispositivos móviles, Ecuador, 2017. Disponible en: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwjB14CuiJHoAhVKiOAKHd52A3cQFjABegQIBBAB&url=https%3A%2

F%2Fdialnet.unirioja.es%2Fdescarga%2Farticulo%2F6155633.pdf&usg=AOvVaw0qPVba9BAGGYVFpMmbqLEe

95. Xataka Android, Nieto González Alejandro, ¿Qué es Root? ¿Qué es Android?, España, 2019. Disponible en: https://www.xatakandroid.com/sistema-operativo/que-es-android
96. Androidpit, Calvo Daniel, ¿Qué es Root? Ventajas e inconvenientes de rootear tu Android, España, 2019. Disponible en: https://www.androidpit.es/root-que-es
97. GCFGlobal, Sistema operativo móvil IOS, S/A. Disponible en: https://edu.gcfglobal.org/es/ipad/sistema-operativo-movil-ios/1/
98. Cinco días El País, Bolaños David, Qué es el jailbreak y por qué, y cómo, debería hacérselo (o no) al iPhone 6, 2014. Disponible en: https://cincodias.elpais.com/cincodias/2014/10/23/lifestyle/1414081833_201902.html

Otras

99. Agregalo de la Torre, Jo Se Manuel. Informática forense: auditoria de seguridad, España, 2014, Tesis de ingeniero de telecomunicaciones, Universidad Autónoma de Madrid.
100. Arnedo Blanco, Pedro Javier. Herramientas de análisis forense y su aplicabilidad en la investigación de delitos informático, España, 2014, trabajo fin de master en seguridad informática, Universidad Internacional de la Rioja.
101. Francisco Mora, Marlene del Carmen. Evolución y desarrollo de la informática forense, México, enero 2011, tesis de Licenciada en informática, Universidad de Sotavento A.C.
102. Hamud Fuentes, Alejandro. El funcionamiento de los discos duros, memorias usb y como trabajan las herramientas de informática forense en la recuperación de datos en estos dispositivos, México, 2010, tesis de licenciado en informática, Universidad Nacional Autónoma de México.
103. Iglesias Leonardo Rafael. Herramientas open source para informática forense, Argentina, 2015, Tesis licenciado en Seguridad Informática, Universidad de Buenos Aires.

104. Rodríguez, Francisca. “La informática forense: El rastro digital del crimen”, Derecho y Cambio Social, revista no.25, Perú, 2016.

105. Rosales García, Marcos Arturo. Informática forense como método de investigación en los delitos informáticos, México, julio 2005, tesis de ingeniero en computación, Universidad nacional autónoma de México.

Anexos
Cuadro de cotejo

	Unidades de Análisis		
INDICADOR	**OSForensic**	**Autopsy**	**Tequila**
Casa productora			
Plataforma (Sistema operativo)			
Requisitos de Hardware			
Tamaño de Archivo			
Tipo de código			
Ventajas			
Desventajas			
Soporte/Contacto			
Descarga			

Función Hash			