COMPENDIO DEL AUTOR

COMPUTACIÓN FORENSE

UNIDAD 1

Introducción al Dominio de la Computación Forense

Autor: Luis Javier Castillo Heredia

FR0018/ v3.01

UNEMI
UNIVERSIDAD ESTATAL DE MILAGRO

ÍNDICE

1. Unidad 1: Introducción al Dominio de la Computación Forense

Tema 1: Fundamentos de Computación Forense

Objetivo

Adquirir conocimientos sobre la computación forense.

Introducción

Bienvenidos al emocionante mundo de la computación forense en este apartado vamos aprender todo lo concerniente a los fundamentos básicos de la computación forense; empezaremos hablando una introducción a la computación forense, para después abordar el concepto de un perito informático forense.

Hablaremos también de los diferentes archivos de interés que contienen los diferentes sistemas operativos como, por ejemplo: Windows, Linux y Mac OS, para que finalmente veamos cómo aplicar la computación Forense en el sistema operativo Windows.

2. Información de los Subtemas

2.1 Subtema 1: Introducción a Computación Forense

Introducción

Hoy en día las TICs o también llamado las Tecnologías de la Información, se han convertido en un pilar fundamental para el correcto desempeño de una empresa u organismo, la automatización de varios procesos y el avance tecnológico en las distintas áreas de nuestro diario vivir, sumado el avance de la conectividad de internet, ha ayudado a simplificar los procesos y protocolos de cada empresa, ahorrando de esa manera tiempo y dinero.

Pero por otra parte también ha dado lugar a que las redes o sistemas sean víctimas de delitos informáticos o también conocidos como ciber-delitos, acciones ilícitas realizado por medio de la tecnología o apoyado en ella. Con esta premisa es que se ha creado la computación forense, una ciencia donde se aplican técnicas y buenas prácticas para analizar los dispositivos electrónicos, extraer información y determinar los posibles delitos ocasionados.

También podemos decir de la informática forense que es una disciplina que se basa en la adquisición de información, el análisis del mismo y finalmente plasmamos los resultados del mismo.

Para describir a la computación forense desde otros diferentes puntos de vista vamos a citar a Miguel Torrealbas (2017):

“Por otra parte, desde el punto de vista criminológico la computación forense es un macro procedimiento que permite identificar, preservar, analizar y presentar evidencias digitales de forma que puedan aceptarse legalmente. Y es que para el mundo académico la computación forense es una rama de la ciencia forense digital, cuya razón de ser es fundamentar adecuadamente los correctos y estrictos procesos que conducen a satisfacer los requerimientos legales en el ámbito digital de los sistemas judiciales. Esta

necesidad se debe a la creciente tendencia en el mundo de castigar los crímenes que se realizan con apoyo de computadores o de dispositivos digitales. Esto, a su vez, es una consecuencia de la ubicuidad de computadores y del incremento de acceso a la Internet. De modo que, desde mediados de los años 80, algunas cortes judiciales en diversos países del mundo se han visto en la necesidad de incorporar a peritos en electrónica o computación como parte de los expertos que testifican o avalan la actividad que ocurrió en computadores y redes electrónicas." (Pág. 2).

Objetivos de la computación forense

En la actualidad los delitos informáticos son más recurrentes, los delitos pueden ser desde ir desde robos de información personal a personas cotidianas, como también delitos a gran escala, es decir a empresas o entidades donde la información que manejan puede incurrir en grandes pérdidas como por ejemplo: la información de las credenciales de acceso de sus clientes, las fórmulas de producción de una empresa, información sensible en entidades gubernamentales, información personal de los empleados de una empresa, etc.

Para esto la computación forense o también llamado informática forense analiza los diferentes métodos y técnicas, que se utiliza para detectar los diferentes delitos antes descritos. Para profundizar el tema podemos citar a Rimero Martha (2020):

"El objetivo principal de la informática forense es generar evidencias legales para procedimientos judiciales, las evidencias desde el punto de vista que ocupa, son el conjunto de recursos y datos a los que ha tenido acceso un perito para extraerlos, analizarlos, verificar su autenticidad y poder así responder a las cuestiones técnicas planteadas por la parte que le contrate o por un tribunal. Según Estrada (2010) la informática forense permite dar solución a problemas relacionados con la seguridad de la información, con el objetivo de salvaguardar la información digital, en el caso de haber ocurrido un delito, utilizando como medio a el computador o algún equipo digital." (Pag.15).

Además de profundizar en los métodos y técnicas también se aborda los protocolos que se debe tener para realizar la extracción o adquisición de información que luego lo

llamaremos evidencia digital, para con esto entrar en la cadena de custodia, en apartados posteriores de esta misma materia abordaremos más a profundidad los conceptos básicos y avanzados de evidencia digital, cadena de custodia y análisis de dichas evidencias.

Figura 1: Fragmento base de código

Fuente: https://www.atlas.com.co/informatica-forense-para-descubrir-el-mal-uso-de-los-datos-y-fraude/

Desde otro punto de vista como el empresarial podemos decir que la informática forense puede dar soluciones a los inconvenientes tecnológicos que tengan que ver con la seguridad informática o ciberseguridad, como también con la protección del activo más valioso de una empresa que es la información o los datos. Con el beneficio de la informática forense se puede dar solución a los problemas de fraude informático, pérdida de información o robo del mismo, atentado con la confidencialidad de la información de los sistemas de la empresa, atentado con la privacidad de la información del mismo, espionaje informático ya sea de las empresas de la competencia o de personas que quieran vender a la competencia información sensible, a esto lo denominamos competencia desleal.

Para concluir podemos decir que los objetivos de la informática forense son los siguientes según el Grupo Ático (2020):

- "Ayuda a recuperar, analizar y preservar el ordenador y los materiales relacionados de tal manera que ayuda a la agencia de investigación a presentarlos como evidencia en un tribunal de justicia.
- Ayuda a postular el motivo detrás del crimen y la identidad del principal culpable.
- Diseñar procedimientos en una presunta escena del crimen que ayudan a garantizar que la evidencia digital obtenida no esté corrupta.
- Adquisición y duplicación de datos: recuperación de archivos eliminados y particiones eliminadas de medios digitales para extraer la evidencia y validarlos.
- Ayuda a identificar la evidencia rápidamente y también permite estimar el impacto potencial de la actividad maliciosa en la víctima
- Producir un informe forense informático que ofrece un informe completo sobre el proceso de investigación.
- Preservar la evidencia siguiendo la cadena de custodia." (s/p).

Tipos de informática forense

En el campo de la computación forense se pueden clasificar diferentes tipos según el área informática en la cual se va aplicar la extracción y el análisis de la información, dentro de los cuales tenemos los siguientes:

- **Informática forense de sistemas operativos**

Se utiliza cuando se necesita analizar información de un Sistema Operativo que puede ser de un móvil o también un ordenador. El propósito de este tipo de computación forense es extraer evidencias digitales del sistema operativo contra el infractor.

Lo interesante de este tipo de investigación es dominar los archivos de interés que tiene el sistema operativo junto con el análisis del sistema de ficheros, con los cuales es más fácil seguir las rutas de árboles que tiene el disco duro y poder examinar todo lo que contiene el disco duro y el sistema operativo.

- **Informática forense de redes**

Este tipo de computación forense se basa en la adquisición, control y análisis de los eventos de la red para revelar los posibles ataques que haya tenido la red, el tipo de virus, forma de alteración o instrucción a la red. Según el grupo Atico34 (2020) dice:

"el análisis forense de la red se considera junto con el análisis forense móvil o el análisis forense de imágenes digitales, como parte del análisis forense digital. Por lo general, se usa cuando se trata de ataques a la red. En muchos casos, se usa para monitorizar una red para identificar proactivamente el tráfico sospechoso o un ataque inminente. Por otro lado, se utiliza para recopilar pruebas mediante el análisis de datos de tráfico de red para identificar la fuente de un ataque" (s/p)

- **Informática forense en dispositivos móviles**

Este tipo de informática forense se encarga de obtener información se los dispositivos móviles y realizar el respectivo análisis del mismo, para que la información obtenida sea una evidencia digital confiable se tiene que seguir ciertos protocolos, para que la información no sea alterada y sea válida para su análisis y posteriores conclusiones o resultados que se obtengan.

- **Informática forense en la nube o cloud**

Este tipo de análisis se lo realiza gracias al avance de la tecnología y la necesidad de las empresas y personas particulares de guardar su información en la nube, para profundizar a detalle el concepto del mismo citaremos lo descrito por el grupo Atico34 (2020):

"El análisis forense de la nube combina la computación en la nube y el análisis forense digital, que se centra principalmente en la recopilación de información forense digital de una infraestructura de la nube. Esto significa trabajar con una colección de recursos informáticos, como activos de red, servidores (tanto físicos como virtuales), almacenes, aplicaciones y cualquier servicio que se brinde. Para la mayoría de las situaciones, este entorno permanecerá (al menos parcialmente) en vivo, y puede reconfigurarse rápidamente con un mínimo esfuerzo. Al final, cualquier tipo de evidencia recopilada debe ser adecuada para su presentación en un tribunal de justicia." (s/p).

2.2 Subtema 2: El Perito Informático Forense

Introducción

Como ya hemos abordado el concepto claro de la computación forense, sus implicaciones, objetivos e importancia del caso ahora vamos hablar de la persona que aplica estas técnicas, procedimientos y protocolos y las ejecuta de manera oportuna.

Para que todas estas técnicas sean aplicadas se necesita de una persona que tenga el conocimiento requerido del tema para que pueda ejecutar las valorizaciones y emitir unos resultados objetivos, sabiendo que los resultados no fueron alterados y confiando que el análisis fue el oportuno.

El perito informático es aquella persona que brinda de manera oportuna sus servicios en un juicio, puede ser al juez, la parte demandada, la parte que realiza la demanda o la fiscalía. La figura del perito informático consta como válida en el "Código de Procedimiento Penal" Art. 95.

Para tener un panorama más amplio de los detalles de un perito informático nos vamos a basar en Santiago Acurio (2019):

> "La pericia es un medio de prueba específicamente mencionado por la Ley procesal, con el cual se intenta obtener para el proceso, un dictamen fundado en especiales conocimientos científicos, técnicos o artísticos, útil para el descubrimiento o valoración de un elemento de prueba. Un informe pericial, sus conclusiones u observaciones no son definitivos ni concluyentes, la valoración jurídica del informe pericial queda a criterio del Fiscal, Juez penal o Tribunal penal, quienes pueden aceptarlo o no con el debido sustento o motivación. Se fundamenta en la necesidad de suplir la falta de conocimiento del Juez o del Fiscal, porque una persona no puede saber lo todo, sobre todo en un mundo tan globalizado, donde las ciencias se han multiplicado y diversificado, así como los actos delictivos. El Perito Informático requiere la formación de un perito informático integral que siendo especialista en temas de Tecnologías de información, también debe ser formado en las disciplinas jurídicas, criminalísticas y forenses. En este sentido, el perfil que debe mostrar

el perito informático es el de un profesional híbrido que no le es indiferente su área de formación profesional y las ciencias jurídicas.” (Pag.15).

Ahora que ya conocemos los detalles a profundidad de un perito informático vamos a revisar cuales son los requisitos que debe tener un perito informático para ejercer su profesión, los cuales son los siguientes:

- Ser especializado en el área de conocimiento con experiencia y conocimiento comprobada por el Consejo de la Judicatura.
- Ser mayor de edad, es decir tener la edad de 18 años en adelante.
- Conocimientos claros y específicos de lo que vaya analizar.

Roles en la investigación forense

Una vez que ya conocemos quien es un perito informático, sus funciones y los requisitos para ejercer esta profesión, ahora vamos a conocer cuáles son los roles que tiene la persona o las personas en la escena de un delito, por lo cual lo vamos a dividir en las siguientes fases:

1) **Especialista en escena el delito informático**

   Son las primeras personas en asistir a la escena del delito, es la persona responsable de delimitar o acotar la escena del crimen y extraer las evidencias físicas y digitales, para esta fase se necesita un conocimiento básico del tema, es decir reconocer cuales son las evidencias necesarias del caso que se encuentren en la escena y tener el cuidado del caso para no alterar la evidencia.

2) **Examinador de la evidencia digital**

   Es la persona encargada de procesar o examinar la evidencia informática que recolecto el especialista antes mencionado, cabe recalcar que en ocasiones pueden ser diferentes personas el que recolecta las evidencias y el que los analiza, pero en otras oportunidades puede ser la misma persona que realiza ambas actividades.

Para realizar esta fase el perito tiene que tener un conocimiento avanzado, ya que tiene que conocer e identificar las técnicas pertinentes para examinar la información, así también necesita saber que herramientas adecuadas emplear.

3) Investigador de delito informático

Es la persona que tiene un conocimiento general y la capacidad de reconstruir la escena del delito para que se pueda emitir un informe y conclusiones finales del análisis realizado.

2.3 Subtema 3: Archivos de Interés en Windows, Linux y Mac OS

Introducción

En este apartado vamos a identificar cuáles son los archivos de interés en los diferentes sistemas operativos (Windows, Linux, Mac OS) donde podemos buscar información que puedan ser potenciales evidencias digitales, por lo cual vamos a identificar dichos archivos o sistemas de ficheros donde podemos revisar clasificados por cada sistema operativo.

Archivos de interés en Windows

En el sistema operativo Windows lo vamos a dividir en 3 archivos o ficheros de interés los que nos van a servir para recolectar información valiosa al momento de buscar evidencias digitales, las cuales son las siguientes:

1. El registro de Windows
2. Los archivos de eventos
3. Los archivos de paginación e hibernación

1) Registro de Windows

El registro de Windows es una base de datos donde se encuentra toda la información importante que concierne al sistema operativo, como también todos los softwares que se encuentra instalado en el sistema operativo. De este podemos encontrar información como:

- El hardware que está instalado y configurado en el ordenador.
- El historial de los dispositivos externos conectados al equipo.
- El software que se encuentra instalado en el sistema operativo.
- Las credenciales de acceso de los usuarios
- Las redes inalámbricas que los equipos a estado conectado

El registro de Windows está compuesto por varios archivos, los cuales, en Windows 7 y 8 son: «SAM», «SECURITY», «SOFTWARE» y «SYSTEM», ubicados en la ruta «[WINDOWS INSTALL DIR]\System32\config\». Además del archivo «NTUSER.DAT» ubicado en la carpeta personal de cada usuario. Estos archivos pueden ser analizados fácilmente con la herramienta *Windows Registry Recóvery* de MiTeC.

2) Archivos de eventos

Son ficheros donde se encuentran almacenados todos los eventos que han sucedido en el Sistema Operativo, entre los eventos que podemos encontrar están los siguientes: el registro de la creación de los usuarios en el sistema operativo, las conexiones de la red del equipo que pertenecía, el acceso de los usuarios registrados en el sistema operativo, etc.

Los archivos de eventos de Windows 7 y 8 se encuentran en la ruta «[WINDOWS INSTALL DIR]\System32\winevt\» y tienen extensión *.EVTX (en versiones anteriores de Windows la extensión es *.EVT). Estos archivos pueden ser analizados desde el propio sistema operativo o con la herramienta *Event Log Explorer* de *FSPro Labs*.

3) Archivos de paginación e hibernación de Windows

Estos ficheros guardan la información que se encontró en la memoria RAM, sin embargo, esa información que ya no se encuentra en ese momento en la memoria RAM, debido a dos situaciones: por archivos de paginación, es decir por qué el espacio de la memoria RAM se ha llenado y se ha eliminado, la otra situación es los archivos de hibernación, es decir porque el equipo ha entrado en estado de suspensión.

Estos archivos suelen estar ubicados en la **raíz del dispositivo** y en Windows 7 (y en prácticamente todas las versiones de Windows) son los archivos «pagefile.sys» e «hiberfile.sys», aunque no tienen por qué encontrarse en el dispositivo.

Archivos de interés de Linux

En los ficheros del sistema operativo Linux también tenemos archivos de interés donde podemos encontrar información valiosa que nos pueden servir como evidencia digital para lo cual vamos a basarnos en lo siguiente según Unir (2020):

> **"La partición de intercambio «swap»,** o archivos de intercambio añadidos al sistema (archivos con extensión «. swap»). Similar al archivo de paginación en sistemas Windows. **El archivo «/etc/sudoers»,** indica qué usuarios pueden ejecutar comandos como administrador (mediante los comandos «su» o «sudo»). **El archivo «/etc/ passwd»,** contiene el listado de usuarios del sistema, el grupo a que dichos usuarios pertenecen y su contraseña cifrada. **El archivo «.bash_history»**, el cual se encuentra en la carpeta del usuario y almacena el historial de comandos ejecutados en la consola del equipo. **La carpeta «/var/log/»**, contiene toda la lista de archivos logs del sistema operativo. Podemos ver que se escribe en cada uno de estos archivos leyendo el fichero de configuración «/etc/rsyslog.conf». **La carpeta «/var/spool/cron/crontabs»** en la cual se almacenan las tareas programadas de cada uno de los usuarios del sistema." (s/p).

Archivos de interés en Mac OS

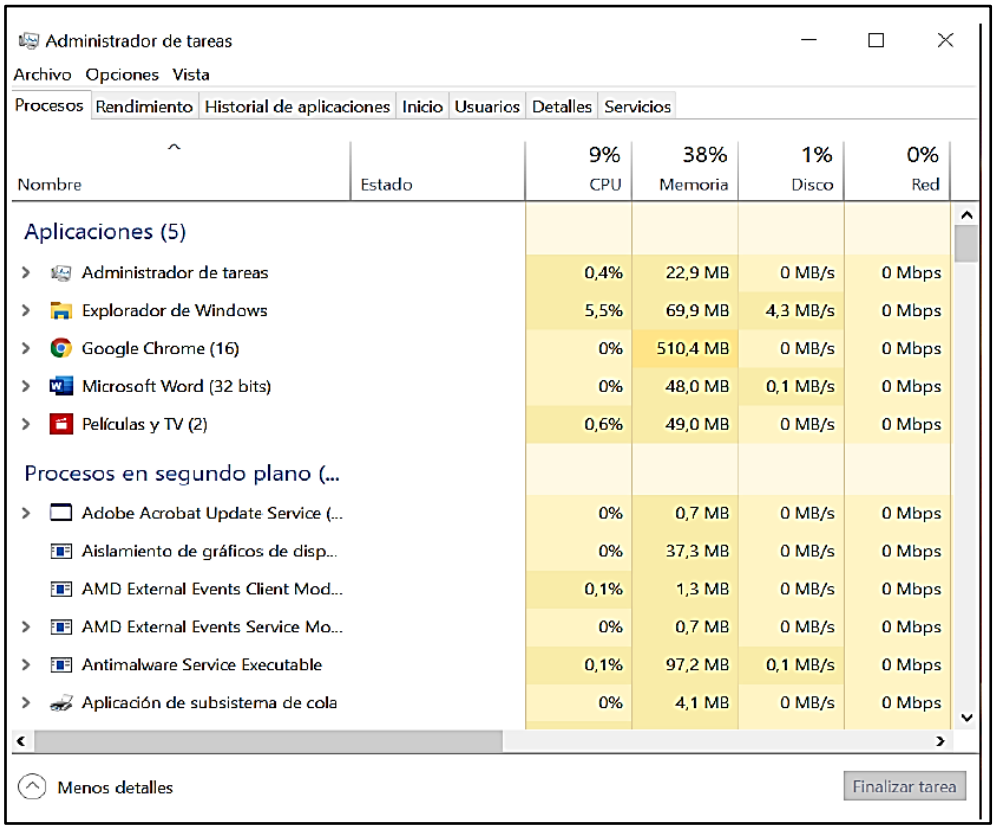
Cuando estemos tratando un equipo con sistema operativo Mac Os, cabe recalcar que se refiere al sistema operativo de ordenadores de mesa o de computadoras portátiles, pero no de dispositivos móviles; en esta categoría descrita se encuentran los siguientes archivos:

- Carpeta «/private/var/vm». Contiene los archivos «sleepimage» y «swapfile», similares a los archivos de paginación e hibernación en sistemas Windows.
- Carpeta «/private/var/log». Contiene los logs del sistema operativo. También es posible encontrar ficheros de log (archivos con extensión *.log) en otras rutas, como la carpeta «/Users/[username]/Library/Logs» que contiene los *logs* correspondientes al usuario.
- Carpetas «/Library/», «/Users/[username]/Library/» y «/System/Library/».
- Archivos con extension «*.plist». Son archivos en formato XML que almacenan información similar a la contenida en el registro de un sistema Windows.
- Carpetas «/private/var/db/shadow», «/Library/Keychains/» y «/Network/Library/Keychains/». Contiene las contraseñas de acceso al equipo y las guardadas por el usuario (redes *Wifi*, exploradores, etc.).

2.4 Subtema 4: Computación Forense en Windows

En este corto apartado se tiene como objetivo dar una breve explicación de los ficheros más importantes del sistema operativo Windows, se ha dado prioridad a este sistema operativo debido a que es el más utilizado a nivel mundial desde hace varios años, por lo cual empezamos la clasificación y descripción de los archivos más importantes.

Figura 2: Administrador de tareas de Microsoft Windows.



Fuente: https://www.atlas.com.co/informatica-forense-para-descubrir-el-mal-uso-de-los-datos-y-fraude/

Para familiarizarnos con algunos ficheros descritos lo tenemos en la Figura 2 donde podemos apreciar el administrador de tareas en un sistema operativo Windows versión 10.

Archivos claves del sistema

Los archivos que se describen a continuación vienen a ser los de interés o de alto impacto al momento de recolectar evidencias digitales, según Unir (2020):

- ntdetect.com, es un programa de Windows NT, que se ejecuta durante el proceso de arranque del sistema para identificar el hardware disponible en la computadora.
- ntbootdd.sys, es el controlador de dispositivos SCSI para comunicar con dispositivos de almacenamiento.
- hal.dll, es controlador que ejerce como capa de abstracción del hardware del equipo, respecto al sistema, se ejecuta en el kernel del sistema por lo que su integridad es crítica.
- winlogon.exe, es el programa encargado de identificar a los usuarios del sistema y cargar sus perfiles.
- explorer.exe, el proceso que administra la interfaz de usuario el escritorio, las ventanas, la barra de inicio, etc.” (s/p).

3. Preguntas de Comprensión de la Unidad 1

1. Pregunta de comprensión Nro. 1

¿Cómo también es llamado la computación forense?

A. Informática forense.
B. Tecnologías de la información.
C. Converge Tecnologías.
D. Nueva información.

Respuesta: La informática forense es también conocida como informática o análisis forenses.

2. Pregunta de comprensión Nro. 2

¿Cuál es un tipo de computación forense?

A. Informática forense de redes.
B. Informática forense de datos.
C. Informática forense de errores.
D. Informática forense.

Respuesta: La respuesta correcta es informática forense de redes ya que extrae información del tráfico de la red en la que se encuentra conectado el ordenador a analizar.

3. Pregunta de comprensión Nro. 3

¿Cuál es un rol del investigador forense?

A. Informativo del caso.
B. Especialista en escena el delito informático.
C. Entrega resultados.
D. Asiste al juicio.

Respuesta: La respuesta correcta es especialista de escena del delito informático y es el que extrae las evidencias físicas y digitales.

4. Pregunta de comprensión Nro. 4

¿Cuál no es un registro de interés de Windows?

A. Registro de Windows.
B. Archivos de eventos.
C. Archivos de paginación e hibernación.
D. Archivos del disco principal.

Respuesta: La respuesta correcta es archivos del disco principal, ya que no forma parte de los archivos de interés del sistema operativo Windows.

5. Pregunta de comprensión Nro. 5

¿Cuál es el sistema operativo donde se especializan más los análisis por ser el más utilizado?

A. Linux.
B. Mac OS.
C. Huawei.
D. Windows.

Respuesta: La respuesta correcta es Windows, ya que es el sistema operativo más utilizado a nivel mundial, por lo cual nos encontramos con más frecuencia con este caso.

4. Material Complementario

Los siguientes recursos complementarios son sugerencias para que se pueda ampliar la información sobre el tema trabajado, como parte de su proceso de aprendizaje autónomo:

Videos de apoyo:

- https://www.youtube.com/watch?v=SEZKuTWMZ_o
- https://www.youtube.com/watch?v=sALmfGj9wfA
- https://www.youtube.com/watch?v=RYdkVAy2cgA

Links de apoyo:

- https://www.ra-ma.es/libro/introduccion-a-la-informatica-forense_49027/
- https://wikis.fdi.ucm.es/ELP/Informatica_Forense
- https://www.atlas.com.co/informatica-forense-para-descubrir-el-mal-uso-de-los-datos-y-fraude/
- https://protecciondatos-lopd.com/empresas/informatica-forense/

5. Bibliografía

- Romero Castro, M., & Choez Chele, M. (2020). La informática forense desde un enfoque práctico. Ciencias Editorial.
- Arellano, L., & Castañeda, C. (2012). La Cadena de Custodia informático - forense. Ediciones Activa.
- Carrier, B.. (2015). *File Systems Forensics Analysis*. Michigan: Addison Wesley Professional.
- Vandeven, S. (2014). *Forensic Images: For Your Viewing Pleasure*. Bethesda: SANS Institute Reading Room.
- Peelman, N. (S. f.). *Basic Mac Forensics*. Indiana: Purdue University.
- Altheide, C. y Carvey, H. (2011). *Computer forensics with Open Source tools*. Syngress.
- Dominguez F. (2018). Introducción a la Informática Forense.
- Brown, C. L. T. (2010). *Computer evidence. Collection and preservation*. Boston: Course Technology PTR.
- EC-Council. (2016). Computer Forensics: Investigation Procedures and Response. Massachusetts: Cengage Learning.
- Hassan, N. A. (2019). Digital Forensics Basics: A Practical Guide Using Windows OS. Nueva York: Apress.
- NIST. (2006). Performing the Forensic Process. En Guide to integrating forensic techniques into incident response.