RESUMEN TÉCNICO

La tecnología ha avanzado de tal manera que ya hace mucho tiempo a quedado atrás la época en que toda la información se almacenaba en grandes cantidades de papel, ahora la información se almacena en medios digitales o magnéticos, tales como discos duros, memorias, Cd, Dvd, etc.

Sin duda que esto representa una gran ventaja en varios aspectos pero también surgen nuevos actos delictivos que involucran estos medios informáticos.

Al igual que un crimen en la dimensión física deja evidencias, un crimen informático también deja evidencias, pero dichas evidencias quedan almacenadas de forma digital, en la mayoría de los casos dicha información no se puede leer o recolectar por medios comunes o mecanismos tradicionales. Es aquí donde nace el estudio de la informática forense, que provee el conocimiento y los instrumentos para recolectar evidencia y solucionar este nuevo tipo de delitos.

Objetivos de la informática forense

La informática forense en estos tiempos digitales es muy importante, pero la importancia real proviene de sus objetivos, que son la recolección, comparación, análisis y evaluación de datos procedentes de cualquier medio informático, de tal forma que sea como prueba dentro de un tribunal de justicia.

Proceso

En el objetivo se menciono que lo importante es que la evidencia recolectada se puede usar dentro de un proceso penal, para que esto suceda es necesario que la evidencia se haya extraído con ciertos estándares, que varían dependiendo del país en el que se lleve a cabo la investigación.

Entre las guías de mejores prácticas en computación forense se puede mencionar:

- **RFC3227**, Guía para recolectar y almacenar evidencia, escrita en febrero de 2002, es una guía de alto nivel para recolectar y archivar datos relacionados con intrusiones, también explica algunos conceptos relacionados con la parte legal.
- **Guía del IOCE**, La Organización Internacional de Prueba Informática nos presenta "Guía para las mejores prácticas en el examen forense de tecnología digital", que es un documento que provee una serie de estándares, principios de calidad y aproximaciones para la detección y prevención, recuperación, examinación y uso de la evidencia digital para fines forenses. Cubre los sistemas, procedimientos, personal, equipo y requerimientos de comodidad que se necesitan para todo el proceso forense de evidencia digital, desde examinar la escena del crimen hasta la presentación en la corte de justicia.
- **Investigación en la escena del crimen**, El departamento de justicia de los Estados Unidos pública (Electronic Crime Scene Investigation: A Guide for First Responders), la cual se enfoca más que todo en identificación y recolección de evidencia.
- **Examen forense de evidencia digital**, esta es otra guía del Departamento de Justicia de los Estados Unidos, es "Examen Forense de Evidencia Digital" (Forensic Examination of Digital Evidence: A Guide for Law Enforcement), esta guía motiva el desarrollo de políticas y procedimientos con el fin de darle un buen trato a la evidencia.
- **Mejores prácticas (guía Hong Kong)**, la Sociedad de Seguridad Informática y Forense creada en Hong Kong, publicó "Computer Forensics – Part 2: Best Practices". Esta guía cubre los procedimientos y otros requerimientos necesarios involucrados en el proceso forense de evidencia digital, desde el examen de la

escena del crimen hasta la presentación de los reportes en la corte de justicia.

- **Guía de buenas prácticas para evidencia basada en computadores reino unido**, La ACPO, Association of Chief Police Officers (Asociación de Jefes de Policía), del Reino Unido, mediante su departamento de crimen por computador, publicó "Guía de Buenas Prácticas para Evidencia basada en Computadores" (Good Practice Guide For Computer Based Evidence). La policía creó este documento con el fin de ser usado por sus miembros como una guía de buenas prácticas para ocuparse de computadores y de otros dispositivos electrónicos que puedan ser evidencia.
- **Guía para el manejo de evidencia en IT Australia**, Estándares de Australia (Standards Australia) publico en agosto de 2003 "*Guía Para El Manejo De Evidencia En IT*" (HB171:2003 *Handbook Guidelines for the management of IT evidence*). Es una guía creada con el fin de asistir a las organizaciones para combatir el crimen electrónico.

Delitos informáticos

Casi de forma paralela al avance de la tecnología también han surgido una serie de ilícitos denominados delitos informáticos.

Varios son las definiciones de delitos informáticos pero según mi opinión la que más se acerca es la que detalle el mexicano Téllez Valdez, "un delito informático implica cualquier actividad ilegal que encuadra en figuras tradicionales ya conocidas como robo, hurto, estafa, fraude, falsificación, sabotaje, pero siempre que involucre la informática como medio para realizar la ilegalidad".

Tipificación de los delitos informáticos

Para conceptualizar los delitos informáticos se toma en cuenta el reconocimiento que hacen al respecto Las Naciones Unidas.

Fraudes:

Manipulación de los datos de entrada, es el tipo de fraude informático conocido como sustracción de datos, es fácil de cometer y difícil de descubrir.

Manipulación de programas, consiste en modificar los programas existentes en los sistemas de las computadoras, un método muy conocido es el famoso Caballo de Troya.

Manipulación de los datos de salida, se efectúa fijando un objetivo al funcionamiento del sistema informático, un ejemplo común es la clonación de tarjetas de crédito.

Fraude efectuado por manipulación informática, aprovecha las repeticiones automáticas de los procesos de cómputo, es una técnica en la que apenas partes perceptibles de transacciones financieras se van sacando repetidamente de una cuenta y se transfieren a otra.

Falsificaciones:

Como objeto, cuando se alteran datos de documentos almacenados.

Como instrumentos, las computadoras pueden utilizarse para efectuar falsificaciones de documentos.

Daños o modificaciones:

Sabotaje informático, es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema.

Virus, es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos.

Gusanos, es igual que un virus pero este no puede reproducirse.

Bomba lógica o cronológica, poseen un alto potencial de daño y no se pueden descubrir hasta que se detonan.

Al final son pocos los países que disponen de una legislación adecuada que permita enfrentarse a los delitos mencionados, entre estos están Alemania, Austria, Francia y Estados Unidos.

EVIDENCIA DIGITAL

Importancia

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

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

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

Clasificación

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

- **Contenido:** Un e-mail, por ejemplo, puede ser clasificado por su contenido como SPAM, y puede ser individualizado a partir del contenido de sus encabezados, información que por lo general no es visible para el usuario. Por ejemplo, por su dirección de origen.
- **Función:** El investigador puede examinar cómo funciona un programa para clasificarlo y algunas veces individualizarlo. Por ejemplo, un programa que inesperadamente transfiere información valiosa desde un computador confiable a una locación remota podría ser clasificado como un caballo de Troya y puede ser individualizado por la localización remota a la que transfiere la información.
- **Características:** los nombres de archivo, extensiones e inclusive los encabezados internos que identifican los diferentes formatos de archivo que existen pueden ser de utilidad en la clasificación de la evidencia digital.

La idea fundamental es que si se hace una clasificación adecuada basándose en la experiencia y en las técnicas adecuadas se podrá hacer hablar a las "evidencias". Se debe recordar la frase del doctor Edmond Locard[1] (1910) y sentir la profundidad científica de su mensaje: "*Las evidencias son testigos mudos que no mienten*".

Procedimiento de recolección

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

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

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

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

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

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

Orden para obtener la Evidencia Digital.

Cuando la evidencia se compone de listados de cientos de conexiones, decenas de procesos corriendo, y una imagen bit-a-bit[2] de un disco duro con muchos gigabytes, es necesario establecer un plan para la forma de abordar el análisis. Es decir, decidir de antemano qué es importante, qué no lo es, y en qué orden hacer las cosas.

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

[2]Una imagen bit a bit es una réplica exacta de una partición o de un disco duro.

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

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

Durante el proceso de recolección y de análisis de la evidencia digital, es deber del investigador utilizar algún método para mantener y verificar su integridad, ya que un punto clave en la preservación de evidencia digital, es que se recolecte sin alterarla y evitar su manipulación futura, ya que de otra forma no podrán ser usada dentro de una investigación, ni tampoco será creíble.

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

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

Buenas prácticas de preservación evidencia digital.

Criterios de admisibilidad

La admisibilidad está ligada con el aspecto legal, y precisamente basándose en legislaciones modernas, existen cuatro criterios que se

deben tener en cuenta para analizar, al momento de decidir sobre la admisibilidad de la evidencia:

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

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

Tipos de evidencia

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

- **Best evidence,** evidencia primaria u original, no es copia. Es la forma más convincente de evidencia, también la más difícil de cuestionar, sin embargo, hay que ser cuidadoso en lo que se considera evidencia primaria.
- **Secondary,** evidencia secundaria, no es tan sólida como la evidencia primaria. Frecuentemente son copias de la evidencia primaria, y las copias pueden ser alteradas, lo que disminuye la fuerza como evidencia probatoria.
- **Direct evidence,** evidencia directa, prueba o invalida un hecho sin la necesidad de utilizar presunciones o inferencias.
- **Conclusive evidence,** evidencia concluyente, es una evidencia muy poderosa. Por sí misma establece una condición o un hecho.

HERRAMIENTAS DE INVESTIGACIÓN FORENSE

Herramientas de informática forense

En los últimos años se ha disparado el número de herramientas para computación forense, es posible encontrar desde las más sencillas y económicas, como programas de prestaciones muy limitadas y con costos de menos deUS$300, hasta herramientas muy sofisticadas que incluyen tanto software como hardware. Con esa amplia cantidad de alternativas, es necesario tener claro el objetivo que se persigue, ya que existen varios tipos básicos de herramientas, no todos los productos sirven para todo, algunos están diseñados para tareas muy específicas y más aún, diseñados para trabajar sobre ambientes muy específicos, como determinado sistema operativo.

Herramientas para la recolección de evidencia digital

Las herramientas para la recolección de evidencia representan el tipo de herramienta más importante en la informática forense, porque su centro de acción se enfoca en el que para muchos es el punto central. Su uso es necesario por varias razones:

- Gran volumen de datos que almacenan los computadores actuales.
- Variedad de formatos de archivos, los cuales pueden variar enormemente, aún dentro del contexto de un mismo sistema operativo.
- Necesidad de recopilar la información de una manera exacta, que permita verificar que la copia es idéntica al original y además mantener inalterada la escena del delito.
- Limitaciones de tiempo para analizar toda la información.
- Volatilidad de la información almacenada en los computadores, alta vulnerabilidad al borrado, con una sola instrucción se pueden eliminar hasta varios gigabytes.
- Empleo de mecanismos de encripción, o de contraseñas.
- Diferentes medios de almacenamiento, discos duros, CDs y cintas.

Algunas herramientas de este tipo son EnCase, The Coroner's Toolkit (TCT), ByteBack - TechAssist, Inc, The Access Data Forensic Toolkit (FTK), Recovery Kit – LCTechonogy, COFEE, Safe Back - New Technologies Inc, The Forensic Tool Kit, The Sleuth Kit and Autopsy, Helix CD, F.I.R.E (Forensics and Incident Response Bootable CD).

Herramientas para el monitoreo y/o control de computadores

Si lo que se requiere es conocer el uso de los computadores, es necesario contar con herramientas que los monitoreen para recolectar información. Existen herramientas que permiten recolectar desde las pulsaciones de teclado hasta imágenes de las pantallas que son visualizadas por los usuarios, y otras donde las máquinas son controladas remotamente.

Herramientas de marcado de documentos

Básicamente el objetivo de este tipo de herramientas es el de insertar una marca a la información sensible para poder detectar el robo o tráfico con la misma, si bien no equivale al sistema LoJack de rastreo y localización de vehículos hurtados, si podría compararse con las marcas que se hace a los vehículos. A través de estas herramientas es posible marcar no solo documentos, sino también software.

Herramientas de Hardware

El proceso de recolección de evidencia debe ser lo menos invasivo posible con el objeto de no modificar la información. Esto ha dado origen al desarrollo de herramientas que incluyen dispositivos como conectores, unidades de grabación, etc. Es el caso de herramientas como DIBS "Portable Evidence Recovery Unit" y una serie de herramientas de Intelligent Computer Solutions; Link MASSter Forensic Soft Case, Link MASSter Forensic Hard Case, Image MASSter Solo 2 Forensic Kit With Hard Case.

Td1 - Duplicador Forense

INFORMÁTICA FORENSE, INSERCIÓN JURÍDICA

Informática forense y su realidad procesal en el Ecuador

El delito informático se puso de moda en Ecuador desde que en 1999 se puso en el tapete la discusión del proyecto de Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas.

Según esta ley y su correspondiente código penal se puede concluir que el dueño de la acción penal y de la investigación tanto procesal como preprocesal es el Fiscal, quien contará con la ayuda de la Policía Judicial para que se haga la investigación de los delitos.

En la actualidad en Ecuador no existe una Unidad Especializada, como existe en otros países, tal es el caso de Estados Unidos donde el FBI cuenta con el COMPUTER CRIME UNIT, o en España la Guardia Civil cuenta con un departamento especializado en esta clase de delitos, eso solo por mencionar algunos.

En el caso de Ecuador en un inicio se creó la una unidad de Delitos Informáticos del Ministerio Público, esta se denominó UDIMP y estaba estructurada de la siguiente forma:

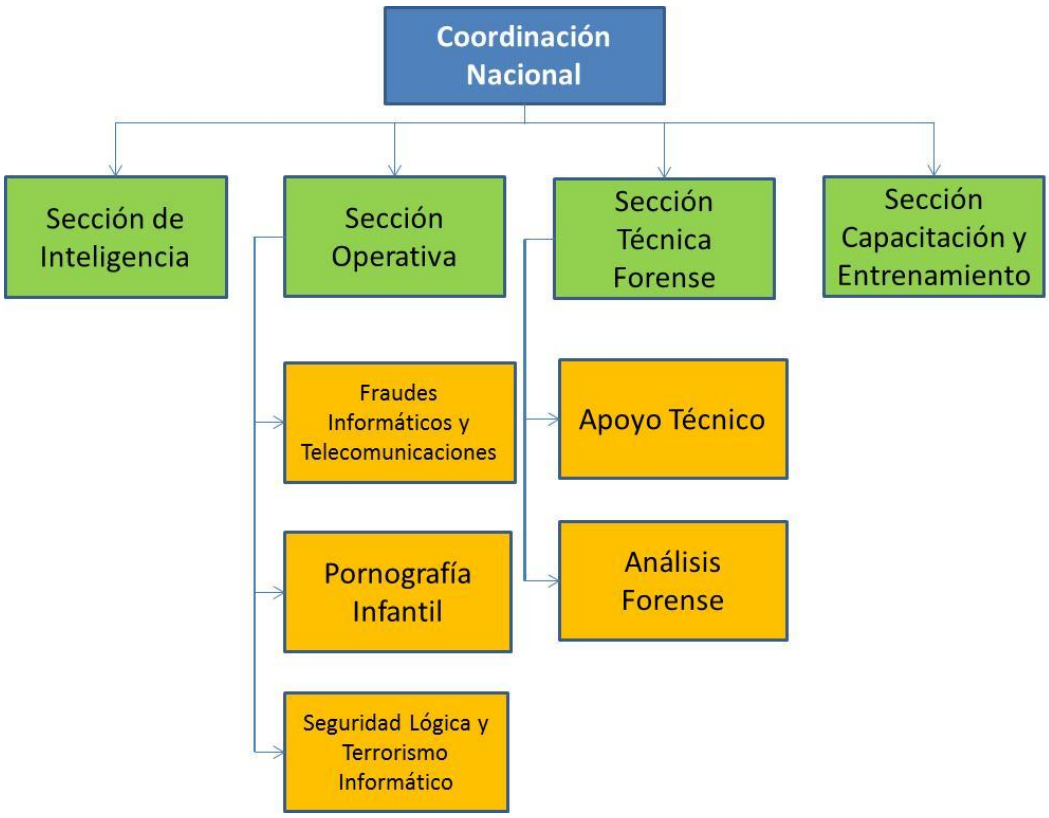
Coordinación Nacional**,** es la encargada de dar las políticas y directrices generales de la investigación de los Delitos Informáticos a nivel nacional.

Sección de Inteligencia, es la encargada de recoger la información, datos y otros indicios que tengan relación con el cometimiento de uno o más delitos informáticos.

Sección Operativa, encargada de realizar las investigaciones de todo lo relacionado con la llamada criminalidad informática.

Sección Técnica y Forense, encargada de brindar el apoyo técnico y realizar el análisis forense de las evidencias encontradas en la escena del delito.

Sección de Capacitación y Entrenamiento, se encarga de la formación continua del personal de la unidad mediante talleres de capacitación, seminarios, charlas y prácticas.



Estructura de la Unidad Delitos Informáticos Ministerio Público.

Fuente: Plan operativo de creación de la Unidad de Delitos Informáticos del Ministerio Público – Dr. Santiago Acurio del Pino

En la actualidad la UDIMP ahora es, el Departamento de Investigación y Análisis Forense de la Fiscalía General Del Estado

Informática forense, leyes internacionales

Entre los países que más se destacan actualmente tanto por sus leyes como su infraestructura para tratar este tipo de delitos están España, Estados Unidos, Bolivia, Argentina, Chile, Brasil, Colombia, Francia, Holanda, Gran Bretaña, Venezuela.

Legislación de Países Latinoamericanos	Ley de Propiedad Intelectual	Ley de Habeas Data	Ley de comercio Electrónico, Mensajes de Datos	Ley de Delitos Informáticos	Ley de Transparencia y Acceso a la Informática	Ley de Pornografía Infantil	Ley de Uso de correo Electrónico
Argentina	●	●	●	●			
Bolivia					Proyecto		
Brasil		●	●				
Chile	●		●	●		●	
Colombia		●	●	●	●		
Costa Rica				●			
Ecuador	●	●	●		●		
Guatemala			●				
México				Proy.	●		
Panamá			●				
Paraguay					●		
Perú			●	●	●		●
República Dominicana			●				
Uruguay							Proy.
Venezuela			●	●			

Leyes en países Latinoamericanos.

Fuente: Estadísticas de la Organización de Estados Americanos (OEA)

Leyes ecuatorianas e internacionales

Si bien es cierto, la ley Ecuatoriana de Comercio Electrónico se realizó basada en leyes ya existentes en otros países, ésta se acopló a la realidad de nuestro país por lo tanto es una ley netamente territorial.

En este sentido el código penal Ecuatoriano sostiene que la ley penal es aplicable cuando la infracción ha sido cometida dentro del territorio, en este momento esto debe cambiar, teniendo en cuenta el nuevo escenario en donde se presentan este tipo de delitos que son de carácter transnacional, es decir delitos que se cometen en el Ciberespacio, un lugar donde no existen fronteras.

Pero en el caso de los delitos informáticos como se mencionó se debe aplicar el principio de universalidad y justicia mundial, este principio básicamente lo que dice es que la ley aplicable es la ley del país que primero capture al delincuente.

Otras consideraciones

Ecuador ha dado los primeros pasos en el desarrollo de iniciativas que permiten la investigación y sanción de los delitos informáticos, sin embargo, es preciso desarrollar, mejorar e implementar mecanismos que permitan que dichas investigaciones se desarrollen dentro de marcos regulados, controlados y mediante el uso de tecnología apropiada por parte de los entes y profesionales dedicados a su investigación.

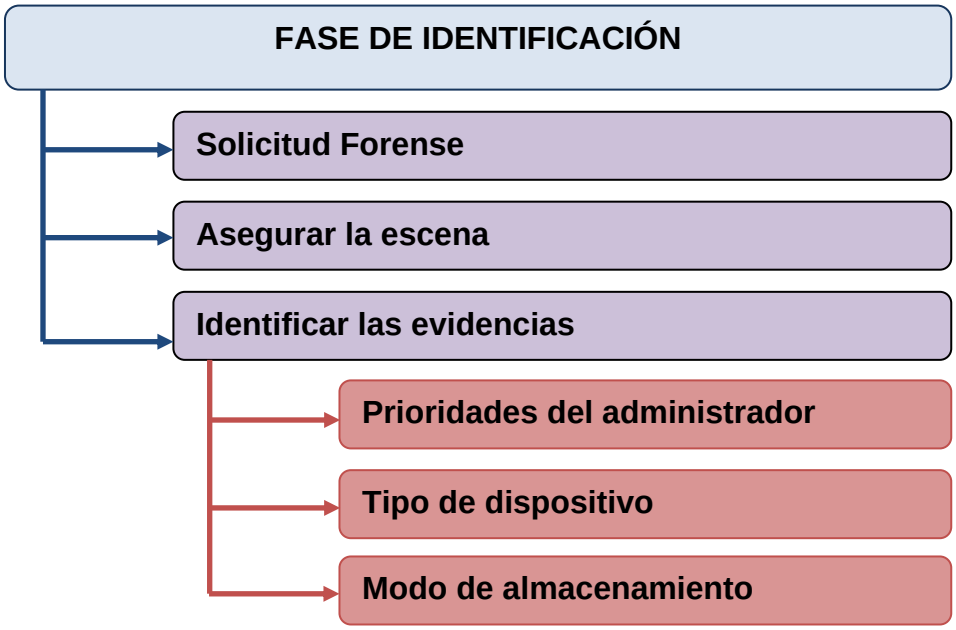
Es indudable el avance tecnológico y la necesidad de establecer mecanismos que permitan la persecución de actos ilícitos cometidos utilizando medios tecnológicos.

Para lo que se debe preparar a una nueva generación de profesionales que den respuesta a la creciente necesidad de la sociedad de contar con asesores entendidos, y capaces de brindar sustento y respaldo legal a cada una de las actividades que se desarrollan con soporte de las tecnologías de la información.

METODOLOGÍA DE TRABAJO PARA INVESTIGACIÓN

En la actualidad existen muchas metodologías para llevar a cabo un análisis informático forense, pero una metodología se debe distinguir por su practicidad y la eficiencia que ofrezca.

Fase de Identificación



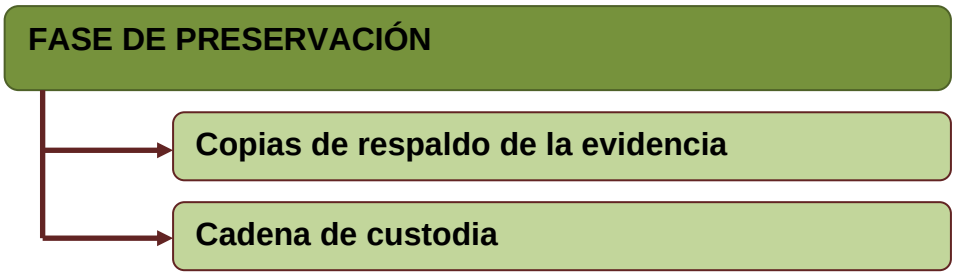
Componentes Fase de Identificación

La fase de identificación se refiere a la recopilación de información necesaria para trabajar sobre la fuente de datos presentada por el administrador de los servidores (solicitud forense). Aquí se pregunta:

- ¿Qué información se necesita?
- ¿Cómo aprovechar la información presentada?
- ¿En qué orden ubico la información?
- ¿Acciones necesarias a seguir para el análisis forense?

El producto final de esta fase, debe entregar un documento detallado con la información que permita definir un punto de inicio para la adquisición de datos y para la elaboración del documento final.

Fase de Preservación

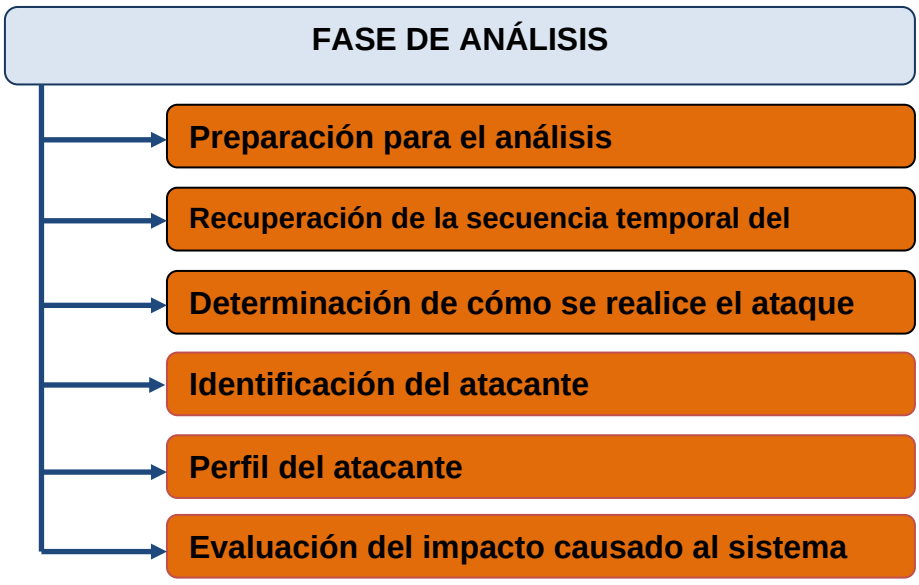


Componentes Fase de Preservación

Aunque el primer motivo de la recopilación de evidencias sea la resolución del incidente, puede ser que posteriormente se necesite iniciar un proceso legal contra los atacantes y en tal caso se deberá documentar de forma clara cómo ha sido preservada la evidencia tras la recopilación.

En esta fase, es imprescindible definir los métodos adecuados para el almacenamiento y etiquetado de las evidencias. Una vez que se cuenta con todas las evidencias del incidente es necesario conservarlas intactas ya que son las “huellas del crimen”, se deben asegurar estas evidencias a toda costa. Para ello se sigue el siguiente proceso.

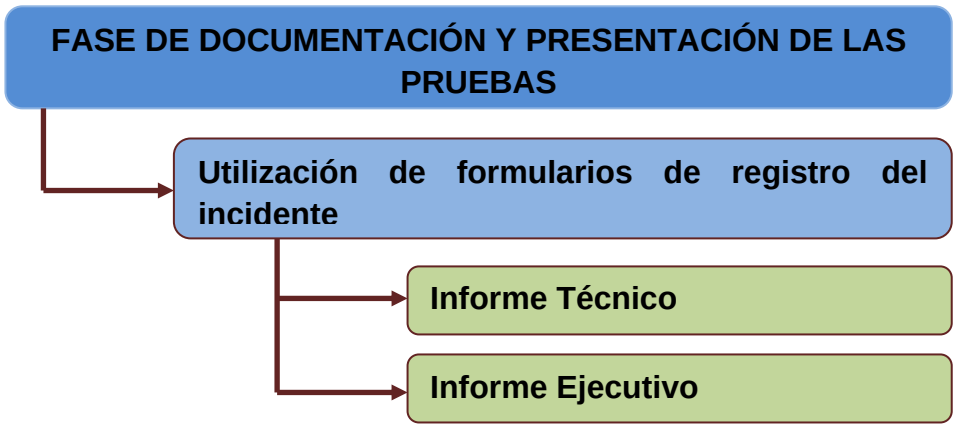
Fase de Análisis



Antes de iniciar esta fase se deben prepararlas herramientas, técnicas, autorizaciones de monitoreo y soporte administrativo para iniciar el análisis forense sobre las evidencias obtenidas o presentadas por el administrador de los servidores. Una vez que se dispone de las evidencias digitales recopiladas y almacenadas de forma adecuada, se inicia la fase más laboriosa, el Análisis Forense propiamente dicho, cuyo objetivo es reconstruir con todos los datos disponibles la línea temporal del ataque, determinando la cadena de acontecimientos que tuvieron lugar desde el inicio del ataque, hasta el momento de su descubrimiento.

Este análisis se dará por concluido cuando se descubra cómo se produjo el ataque, quién o quienes lo llevaron a cabo, bajo qué circunstancias se produjo, cuál era el objetivo del ataque, qué daños causaron, etc. En el proceso de análisis se emplean las herramientas propias del sistema operativo (anfitrión) y las que se prepararon en la fase de extracción y preparación.

Fase de documentación y presentación de las pruebas



Es muy importante comenzar a tomar notas sobre todas las actividades que se lleven a cabo. Cada paso dado debe ser documentado y fechado desde que se descubre el incidente hasta que finaliza el proceso de análisis forense, esto permitirá ser más eficiente y efectivo al tiempo que se reducirá las posibilidades de error a la hora de gestionar el incidente.

CONCLUSIONES

La Informática Forense en la actualidad ha tomado gran importancia porque permite encontrar las evidencias necesarias y suficientes de un siniestro, evidencia que pueden ser de gran valor en el momento de resolver un caso, en muchos de estos casos puede ser la única evidencia disponible

Este trabajo de alguna forma pretende dar a conocer la importancia de la Informática Forense. Debido a que esta ciencia integra otros conceptos como: auditoría, ingeniería inversa, esteganografía, así como aspectos legales que se enmarcan en el perfil profesional integral.

Al final de la investigación se pudo determinar que la metodología no solo se puede aplicar a sistemas operativos Windows y Linux como se lo planteaba el trabajo sino que se puede aplicar a cualquier otro sistema operativo.

RECOMENDACIONES

La mejor forma de evitar situaciones o actos delictivos informáticos es estableciendo controles, pero la mejor forma de defenderse es promover una cultura de seguridad en los hogares y organizaciones.

Incluir en la oferta académica de las universidades del país por lo menos una materia que esté relacionada con este tema de la Informática Forense, así como impartir seminarios y ofertar retos forenses que incentiven aun más a los estudiantes y futuros profesionales.

Los cambios tecnológicos y procesos globalizados demandan mayor rapidez, eficacia, efectividad y un mayor control, por lo cual los profesores y estudiantes vinculados a la investigación, así como los directivos de las instituciones educativas deben profundizar en estos temas de actualidad.