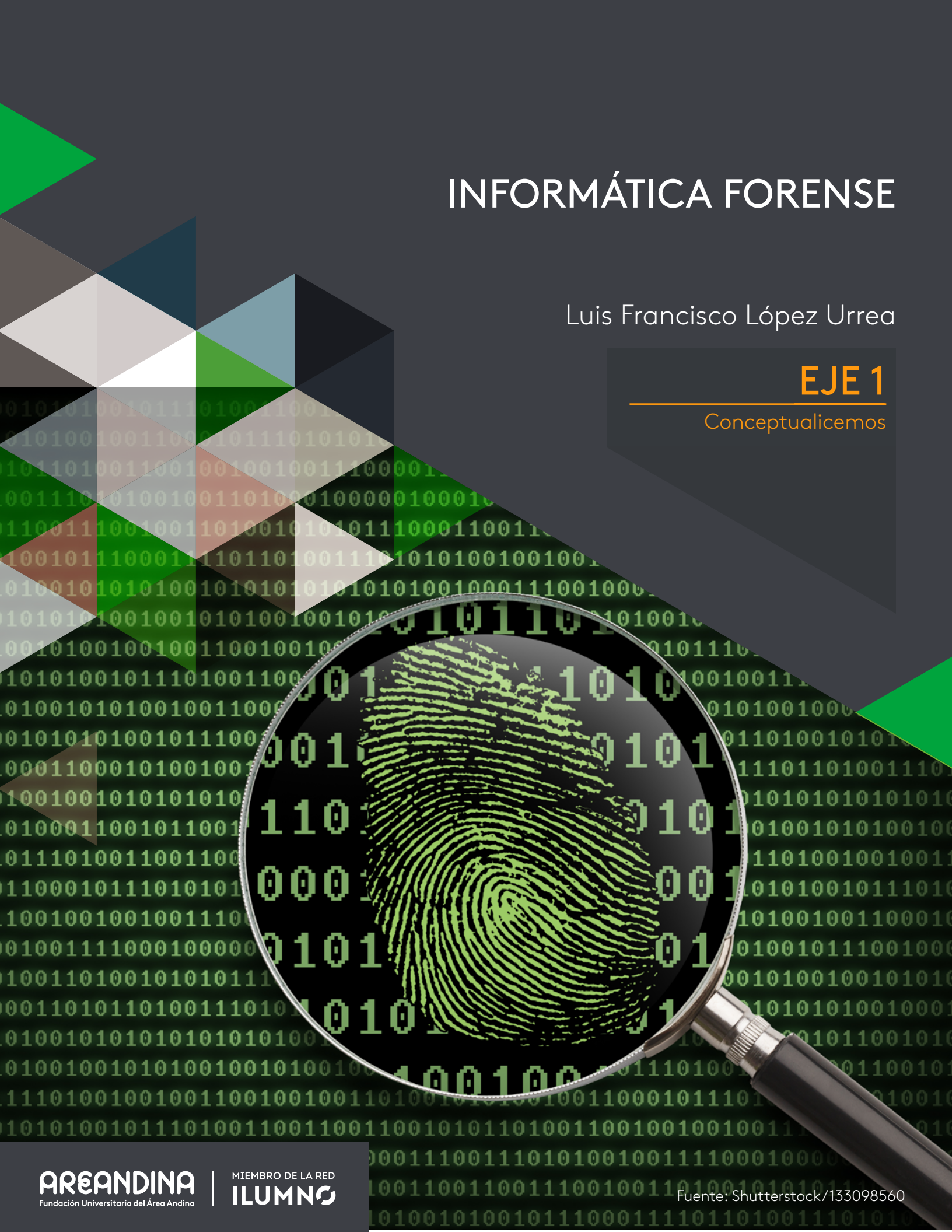
INFORMÁTICA FORENSE

Luis Francisco López Urrea

EJE 1

Conceptualicemos



Fuente: Shutterstock/133098560

AREANDINA
Fundación Universitaria del Área Andina
MIEMBRO DE LA RED
ILUMNO

ÍNDICE

INTRODUCCIÓN

Las condiciones del desarrollo y la evolución de la especie humana no han estado, ni están exentas de situaciones propias de la naturaleza misma de los individuos, así pues, sentimientos como la envidia, la ambición, el odio, el amor o el desamor, entre muchos otros, pueden convertirse en detonantes de situaciones inesperadas, muchas de las cuales pueden cerrar por ejemplo un triángulo amoroso con la muerte de alguno de sus protagonistas.

Así, a lo largo de la historia el ser humano ha sido protagonista de muchas películas en su vida real, que, aunque parezcan extraídas de un guion de Hollywood, lo único que hacen es confirmar aquella frase de algún productor de cine: "la realidad supera la ficción".

Acompáñenme entonces a descubrir el cómo, cuándo, por qué, bajo qué circunstancias, a través de qué medios de muchas de las historias que abordamos como parte del contenido del presente curso, en el que acompañados de mucha **intuición**, variadas herramientas y una computadora intentaremos encontrar las **evidencias** de algunos **delitos** que se cometen tomando como blanco los sistemas informáticos o recurriendo a algún dispositivo tecnológico para obtener información que pueda ayudar en el objetivo de infringir las leyes. Este, apreciado estudiante, es el apasionante mundo de la **informática forense**.

Intuición

Se define como una habilidad que puede ser innata que permite conocer, entender o percibir un suceso o una situación de forma clara y rápida sin que intervenga la razón.

Evidencia

Término con raíz en el latín evidentía, señala una certeza absoluta respecto de algo, frente a la cual no existe la posibilidad de hacer su negación. En el ámbito filosófico se define como un conocimiento que se logra a través de la intuición y permite inferir su validez como verdadera.

Delito

Se puede calificar bajo este término cualquier acción que realizada de forma intencional o por omisión o negligencia da lugar a una situación que produzca un resultado que lesione la vida, bienes o integridad de una persona natural o jurídica y que se encuentra tipificada en las normas o leyes, un delito da lugar a un castigo que se encuentra definido en las normas propias de cada nación.

Informática forense

Según el FBI, la informática (o computación) forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional.

INTRODUCCIÓN

Durante el recorrido por el curso, encontramos historias reales que sustentan la aplicación de las **ciencias digitales forenses** como **disciplina** para ayudar en la obtención de evidencias relacionadas con la investigación de algún delito, además en algunos de los recursos para el aprendizaje, va a encontrar información relevante y pertinente que contribuye a ampliar sus conocimientos sobre el tema. Los términos desconocidos y palabras clave se encuentran resaltados como comentarios para facilitar su búsqueda.

Le recomiendo acceder y analizar en detalle cada uno de los recursos vinculados como parte de la lectura porque a través de ellos y del desarrollo de las actividades y evaluaciones propuestas usted podrá convertirse en un nuevo investigador digital **forense.**

En algunos apartes de esta lectura va a encontrar señaladas reflexiones que le recomiendo desarrollar para socializarlas en los encuentros con el tutor.

Ciencias digitales forenses

El uso de métodos científicamente derivados y probados para la preservación, recolección, validación,

Identificación, análisis, interpretación, documentación y preservación de la evidencia digital derivada de la

Fuentes de información con el fin de facilitar o promover la reconstrucción de hechos considerados criminales o para anticipar las acciones no autorizadas demostrado ser perjudicial para las operaciones planificadas. " DFRWS, 2001

Disciplina

Hace alusión a una asignatura, ciencia o área que se imparte como parte de un plan de estudios.

Evolución de la informática forense

Las ciencias forenses nacen como auxiliares de la investigación criminal desde el siglo VIII después de cristo, se tiene información relacionada con técnicas de investigación condensadas en un manual, en el cual se efectúa el análisis de ciertas evidencias, que pueden ayudar a determinar las causas de la muerte de una persona por ejemplo. Con el paso del tiempo y gracias al avance de las ciencias y las técnicas, el campo de acción de las ciencias forenses se ha hecho más amplio. A partir de la aparición de los dispositivos de procesamiento automático de información y de la revolución de las computadoras, nace un nuevo ámbito de acción, la informática. Por supuesto no podemos restringir la tarea al simple uso de herramientas informáticas para hacer investigaciones de tipo forense, en la actualidad y gracias a la ubicuidad de las tecnologías de la información y las comunicaciones, las computadoras cumplen una doble función; de una parte pueden ser víctimas de ataques externos con el fin de causar daño, robar o extraer datos, cometer fraudes financieros entre muchas otras actividades ilegales, de otra parte para cometer estos delitos también se utilizan computadoras y a su vez para desarrollar el proceso de investigación se emplean herramientas forenses instaladas en los sistemas de computación.

Como pueden ver, las computadoras y los sistemas informáticos se encuentran en el centro de la investigación como víctima, victimario e investigador.

Ciencia
Formulación de forma sistemática de conocimientos, basados en la aplicación del método científico. Se define como el conjunto de conocimientos que se pueden conseguir a partir de la observación, análisis y razonamiento organizados de forma sistemática que pueden originar principios o leyes.

Criminal
Se refiere a las conductas desarrolladas por un individuo con el fin de causar daño en la integridad o bienes de otra persona u organización.

Ubicuidad
Condición inherente a un objeto o elemento que hace posible su presencia en diferentes lugares de forma simultánea.

Ataques
Intento de acceso a un dispositivo electrónico, ya sea exitoso o no, puede tener como fin causar daño, o ingresar a él para obtener información.

Herramientas
Conjunto de elementos, objetos, o en el caso de la informática programas que se emplean para ayudar a desarrollar una tarea o actividad.

El uso del término ciencias forenses se remonta a la Edad Media, aunque con un nombre diferente y solo apegado a la investigación criminal; así para presentar ante los estrados judiciales (el foro) un **caso** objeto de investigación por algún crimen se requería exponer ante los presentes las circunstancias, probables causas, tipo de armas y un sinnúmero de informes que ayudarán a los administradores de justicia a establecer el nivel de responsabilidad de los involucrados en los hechos. Así, las ciencias forenses usan un conjunto de técnicas y métodos de investigación, con el fin de encontrar, explicar y de ser posible probar a través de evidencias, la existencia de un delito, o de una infracción. A partir de allí y a través del análisis busca dar con los responsables, identificar a las **víctimas** y determinar el tipo de ataque cometido y sus consecuencias.

Caso
en términos forenses hacer referencia a toda la información reunida con el fin de exponer ante un tribunal las situaciones relacionadas con la presencia de un delito y sus presuntos responsables.

Victimas
Personas u organizaciones o elementos que pueden haber sufrido un daño producto de un delito.

Uno de los principios de más amplia difusión y aplicación en el contexto de la investigación forense se desarrolló en el año 1910, por el investigador francés Edmond Locard, y se conoce con el nombre de "principio de intercambio" de Locard, el cual establece: "siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto". Así, en el campo de la investigación forense se hace énfasis en la "escena del crimen" como el escenario en el que se puede obtener la mayor cantidad de información posible para tratar de responder las preguntas que planteamos en el párrafo introductorio; pues según el principio si una persona estuvo en la escena de un crimen allí debió quedar un cabello, una huella, una marca de zapato, una muestra de ADN, algo que dé cuenta de la presencia del individuo en la escena. Además, en su ropa en su piel o en sus efectos personales puede llevar algo de la escena del crimen como una fibra de una alfombra, una marca de pintura, una marca de madera o algún elemento que permita validar su presencia.

Principiio de intercambio

Se refiere al planteamiento del Investigador francés Edmond Locard, según el cual cuando en una escena de un crimen siempre habrá algún rastro de la persona que estuvo allí, a su vez siempre que una persona está en un lugar lleva consigo algo de ese lugar; por ejemplo, una fibra de alfombra, un rastro de pintura entre otros.

Escena del crimen

Lugar en que se ha producido que puede constituir un delito que requiere una investigación adecuada en la que se apliquen todos los principios de la investigación criminal.

PRINCIPIO DE TRANSFERENCIA DE LOCARD ENTORNO DIGITAL

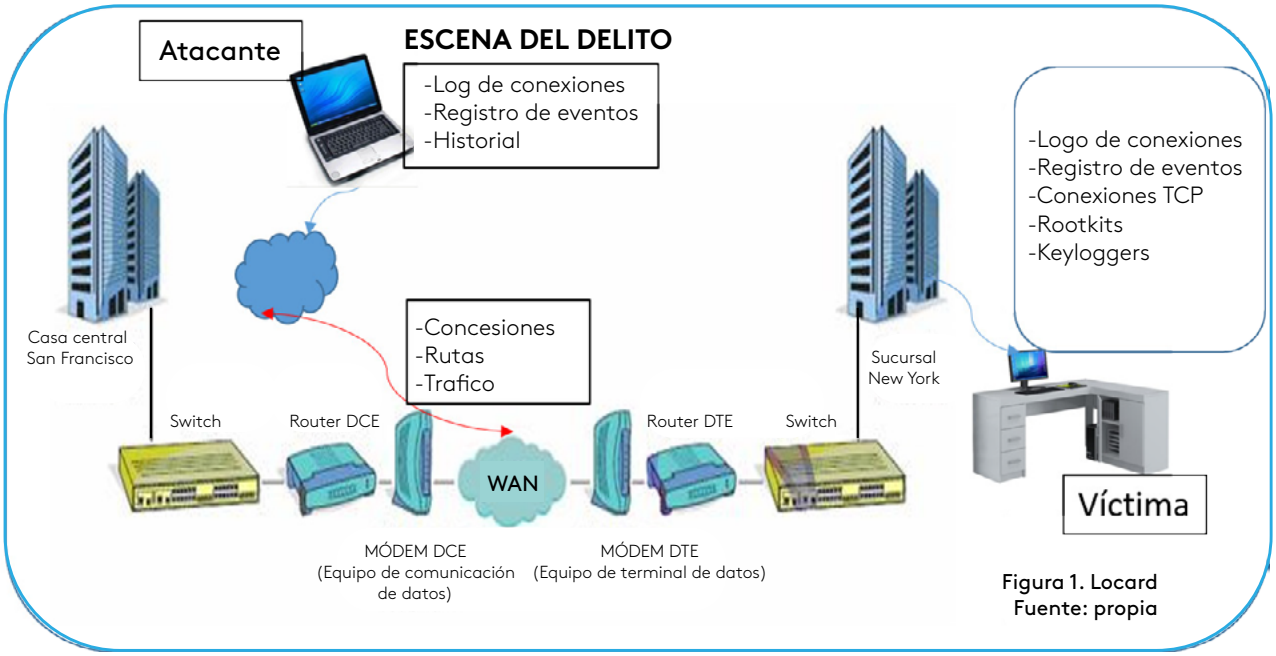


Figura 1. Locard
Fuente: propia

Así, el uso del método científico debía primar en el desarrollo de la investigación, de ahí que usemos el término ciencias y, obvio, muchas de ellas como la medicina, la antropología, la odontología, la patología, la toxicología, la ingeniería y en la actualidad la informática son empleadas para desarrollar el proceso de investigación con el fin de exponer ante estrados judiciales las evidencias obtenidas, su análisis, los resultados y las conclusiones obtenidas como fruto de la investigación.

Delito informático

El concepto de delito informático varía un tanto según la legislación de cada país en el que se realice, sin embargo existe un amplio consenso en definirlo como una actividad que puede ser calificada como ilícita con carácter delictivo, que se desarrolla usando tecnologías de la información y contraviene la legislación o código penal de un Estado (Téllez, 2009).

El delito informático debe ser tipificado en alguna norma o decreto, para el caso particular de Colombia en el año 2009 se expide la Ley 1273 "Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado –denominado 'de la protección de la información y de los datos'- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

De acuerdo con la legislación vigente en cada país y según la tipificación del delito quien participe de un delito informático en calidad de autor, encubridor o cómplice puede afrontar desde multas económicas hasta penas privativas de la libertad.

Delito informático
Actividad ilícita de carácter delictivo que se desarrolla tomando como blanco un sistema informático o usando para su desarrollo herramientas informáticas como ordenadores, pda, smartphones entre otras.

Consenso
Situación en la que múltiples personas o fuentes de información encuentra un punto en común.

Contraviene
Se encuentra en contraposición o viola una norma o ley.

Código penal
Norma o conjunto de normas que define y establece las categorías de los delitos que se pueden cometer y establece las penas de acuerdo al tipo de falta y las condiciones bajo las cuales se desarrolla.

Bien jurídico
Se refiere a cualquier tipo de bien material o inmaterial que es objeto de protección legal y a través del derecho.

Tipificación del delito
Descripción detallada de las acciones a las que se asigna la categoría de delito según el código penal y que son objeto de una sanción o pena.

Autor
Persona o personas que acomete de forma intencional o pasiva la comisión de un delito.

Encubridor
Persona o personas que conocen de un hecho delictivo y a través de sus acciones contribuyen para que el autor consume el delito sin ser descubierto o alertar a las autoridades.

Cómplice
Persona que participa junto al autor en la comisión de un delito.

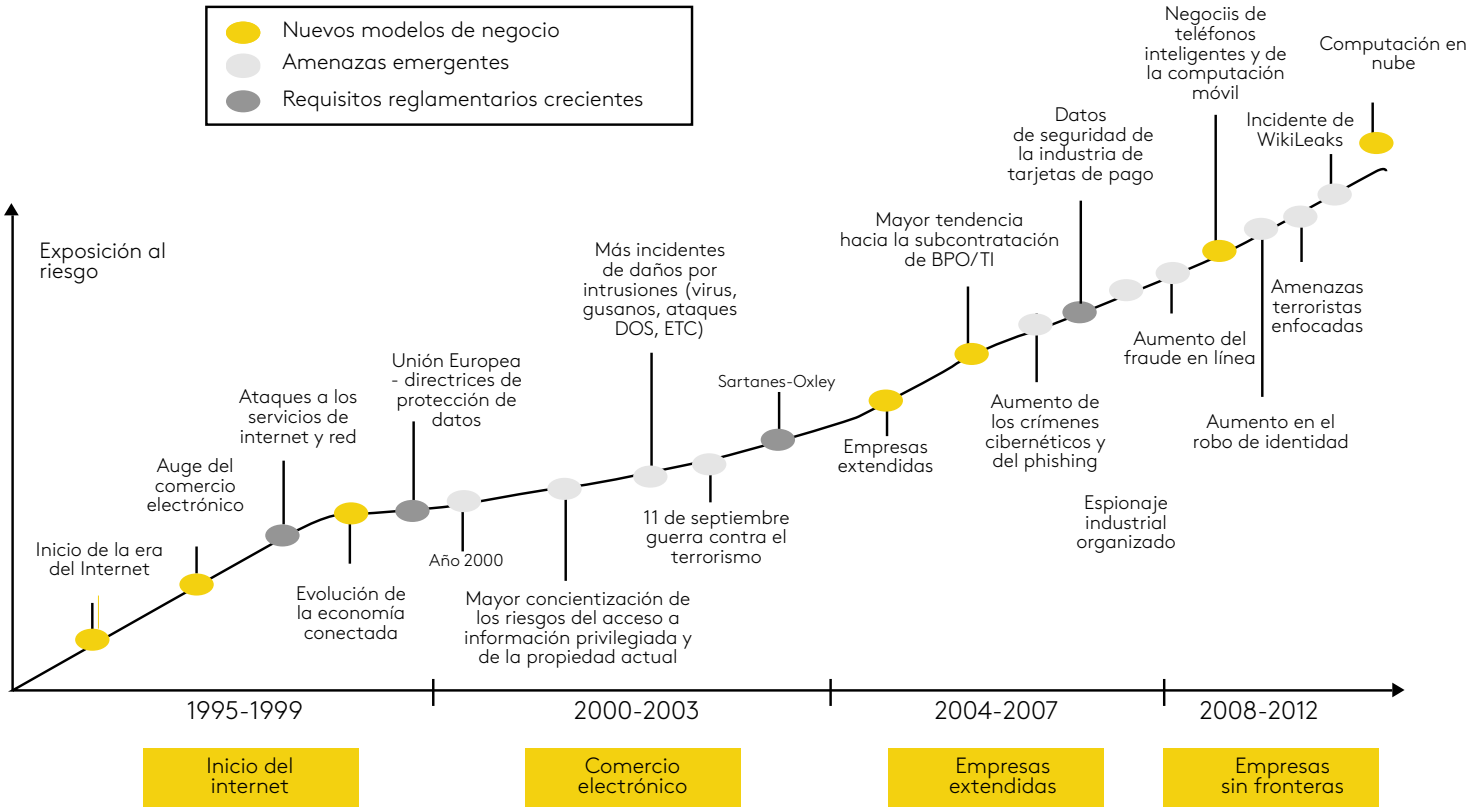


Figura 2. Evolución de los riesgos informáticos
Fuente: https://goo.gl/QDfrzr

No obstante, la anterior definición, existen situaciones en las que el individuo que está pensando cometer un delito consulta en la red Internet información relacionada con el ilícito, así, un individuo que desea envenenar a su pareja, busca en el navegador información relacionada con venenos y su efecto. Posterior a la muerte de la mujer, en la vivienda de la víctima, los investigadores deben identificar todos los elementos que puedan suministrar información respecto a los hechos, allí de encontrar una computadora, es su deber asegurarla, ponerla en cadena de custodia y en el laboratorio forense examinar el contenido, en especial el historial de navegación; es posible que se lleven más de una sorpresa.

Cadena de custodia

Término relacionado con la investigación criminal, que hace referencia al manejo de las evidencias desde el momento de la intervención inicial de los investigadores observando normas estrictas respecto a su recolección, adquisición, conservación, análisis y presentación como prueba.

Laboratorio forense

Lugar destinado al desarrollo de investigaciones de carácter forense, que cuenta con las herramientas, condiciones físicas, logísticas y de seguridad acordes con el tipo de material a depositar y analizar.

Historial de navegación

Registro que construyen los programas que se emplean para acceder a la información de la red INTERNET en las que se incorporan entradas de los sitos visitados por los usuarios que acceden al dispositivo.

El análisis forense

Es necesario recordar que los resultados de un análisis forense serán usados como prueba ante un tribunal en el desarrollo de un proceso judicial, o a solicitud de una organización para establecer posibles infracciones a la seguridad de sus sistemas de información; en todo caso e independiente del objetivo de la información, usted como investigador digital forense debe responder civil y, depende del caso, penalmente por las fallas, omisiones, alteraciones o pérdida de las evidencias que se ponen bajo su custodia para que efectúe el análisis. Así, nunca está de más tomar todas las precauciones debidas, las que detallamos más adelante en este documento y en todos los manuales de análisis forense respecto a la forma de tratar las evidencias.

Alteración
Situaciones relacionadas con la modificación bien sea intencional o no, de las evidencias obtenidas como parte de una investigación.

Custodia
Situación en la que un objeto, o elemento, o bien se deposita en manos de una persona para que la conserve. En investigación criminal, hace referencia a la conservación y preservación de la evidencia bajo unas condiciones estrictas.

El análisis forense a un sistema de información, se desarrolla por lo general luego de que este ha sido víctima de un ataque o un intento de ataque o vulneración; así lo que buscamos es encontrar las respuestas a algunas preguntas clave como las siguientes:

- ¿Quién o quiénes pudieron realizar el ataque?
- ¿Desde qué lugar se realizó el ataque?
- ¿Cómo se realizó el ataque?
- ¿Cuándo se desarrolló?
- ¿Cuál era el propósito del ataque?
- ¿Qué consecuencias trajo para el sistema?

Análisis forense
Actividad en la cual el investigador aplica las herramientas, métodos, técnicas y conocimientos para identificar las circunstancias bajo las cuales una o varias evidencias obtenidas pueden justificar la existencia de un delito y determinar el grado de responsabilidad de uno o varios individuos.

Infracción
Situación en la que, a causa de un incumplimiento a las normas o reglas, se pone en riesgo la integridad de una persona, organización o sistema de información.

Investigador digital forense
Persona con altos conocimientos y calificación en las tecnologías de la información que cuenta con los conocimientos y el nivel de experiencia necesario para acometer una investigación con evidencias digitales de acuerdo a los protocolos de investigación criminal para ser usada como evidencia en un proceso judicial.

Civil
En términos del derecho hace relación a los contratos o acuerdos que rigen las relaciones entre dos o más individuos y sus posibles responsabilidades, en el ámbito patrimonial y/o moral.

Penalmente
Hace referencia a condiciones bajo las cuales se aplica el código penal, es decir normas expedidas por el estado que califican los delitos y establecen las penas respectivas.

Omisión
Situación en la que una persona se abstiene de adelantar una actuación o conducta que implica una obligación legal, de acuerdo a las circunstancias puede ser considerada un delito o falta.

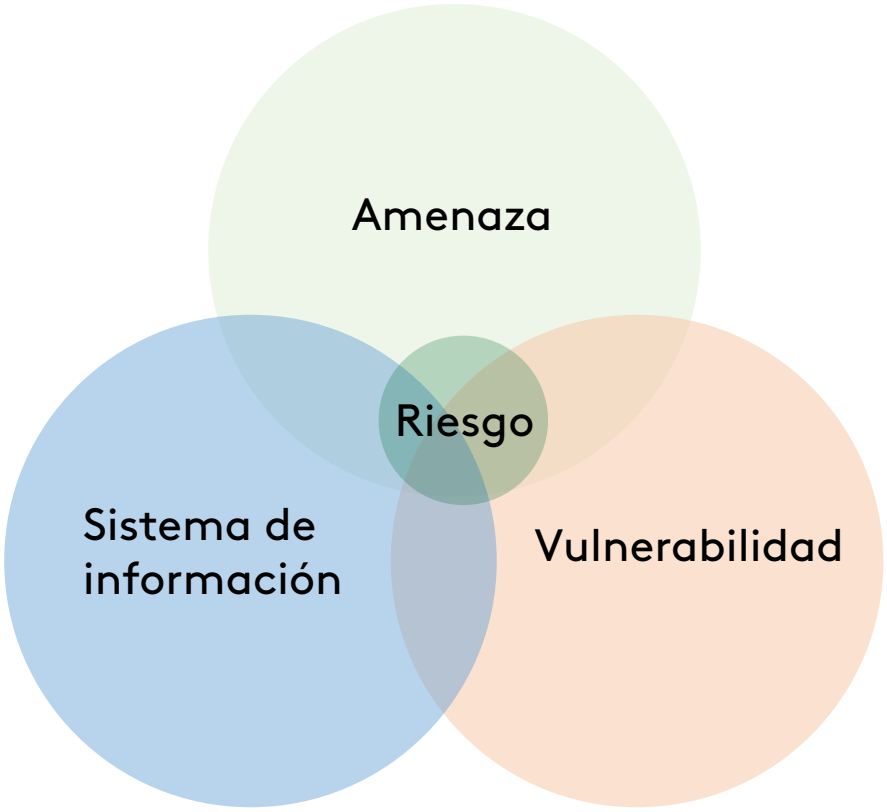


Figura 3. Riesgo
Fuente: propia

Video

Este escenario implica llevar a cabo un análisis forense, los distintos análisis de tipo forense que se pueden adelantar a un sistema informático se describen a continuación. Pero antes revise la vídeocápsula Trabajo del perito informático forense en la página principal del eje.
https://www.youtube.com/watch?v=HHM66N2P0j4&t=37s

Tipos de análisis forense

Existen diferentes categorías para su agrupación, así cuando se hace bajo la perspectiva de sobre qué elemento o elementos se desarrollarán, podemos definir los siguientes tipos.

- Análisis forense de sistemas: se enfoca en analizar sistemas de cómputo (estaciones o servidores) que hayan sido víctimas de un ataque exitoso o no, o de una vulneración a su integridad. Es necesario destacar que se habla de cualquier estación de trabajo, o computador no conectado a ninguna red o servidor que funcionen bajo cualquier sistema operativo e independiente de su arquitectura.

- Análisis forense de redes: este tipo de análisis, se puede hacer sobre cualquier topología física o lógica de red e independiente del medio de transmisión de los datos (lan, wlan, bluetooth, fibra óptica) incluye los dispositivos intermediarios, switch, firewall físico, router.

- Análisis forense de sistemas embebidos: analiza los incidentes de seguridad relacionados con dispositivos móviles, asistentes personales digitales entre otros, su análisis es semejante al que se realiza a las estaciones de trabajo.

Modos de análisis forense

El análisis forense que se realiza sobre cualquiera de los elementos descritos en los numerales anteriores puede realizarse bajo dos circunstancias particulares; en todo caso, es necesario tener en cuenta que la respuesta inicial que se dé cuando un sistema es víctima de una vulneración o ataque es de suma importancia para la investigación.

Así por ejemplo cuando un sistema es víctima de un ataque, una de las primeras opciones por las que se inclina el administrador del sistema es desconectar y apagar los equipos que están siendo afectados; apagar el sistema que se analizará puede afectar evidencia crítica, únicamente los sistemas basados en UNIX pueden recuperar la información que se encontraba en el archivo de intercambio SWAP. En sistemas tipo Windows o Linux esta función no está disponible; además, los atacantes pueden correr algún tipo de malware que solo se ejecuta en memoria RAM, después de apagar el sistema se borrará la evidencia, así señor investigador una de sus decisiones críticas consiste en decidir qué pasos seguir cuando es víctima de un ataque.

SWAP
Del inglés intercambiar, es un archivo de paginación o espacio del disco para guardar este archivo, en él se puede guardar copia de los procesos que se están ejecutando en la memoria física.

Análisis post-mortem: hace referencia a los análisis que se realizan a equipos que se encuentran apagados, bien sea a causa de un posible ataque o porque fruto del ataque o vulneración se toma la decisión de apagarlos. El análisis post-mortem se debe realizar con un equipo que se usa exclusivamente para el análisis forense de sistemas informáticos, en él se puede analizar discos duros, datos, o cualquier elemento obtenido de un sistema que ha sufrido un incidente, es necesario aquí destacar que para que la evidencia obtenida sea considerada válida se debe aplicar los principios de "cadena de custodia" que se detallarán más adelante. No olvide que apagar un sistema puede afectar el funcionamiento de la red y por ende de los servicios que ofrece la compañía, la promesa de valor de muchas empresas en línea es que el sitio siempre estará activo. ¿usted como investigador forense está dispuesto a asumir las pérdidas que por apagar los servidores pueda tener la empresa? Para efectuar un análisis post mortem se recomienda:

Capturar todos los datos del disco duro del equipo afectado o usado como evidencia, el dispositivo puede haber sido apagado o reiniciado más de una vez.

a. La copia del disco duro debe realizarse bajo herramientas válidas en el sector de la investigación criminal para este fin, además debe hacerse bit a bit, se recomienda usar la utilidad DD (Linux) o la herramienta encase (de pago).

b. Aplicar cálculo de integridad de información con HASH y los algoritmos que se recomienden en la investigación, en algunos escenarios ya no se aceptan MD5 y SHA. Este proceso se debe hacer tanto en los discos duros como en los archivos que puedan parecer sospechosos o contengan información relevante del sistema.

MD5
Algoritmo para la creación de HASH, es el acrónimo de algoritmo de resumen de mensaje 5, aplica una criptografía de 128 bits para reducir el mensaje.

SHA
Algoritmo para resumen de mensajes; es el acrónimo de Secure Hash Algoritm, fue diseñado por el departamento de defensa de los Estados Unidos, a la versión más actual se conoce como SHA-3, posee encriptación de 128 o 256 bits, puede ser útil no solo para comprobar integridad, además permite crear firmas y huellas digitales.

c. Se debe extraer la evidencia y trabajar en el disco duro copia, no en el original. nunca trabaje sobre la evidencia original, siempre debe trabajar sobre las réplicas.

d. Se recomienda tomar fotografías o videos de la escena y del proceso.

e. Siempre recuerde usar guantes adecuados para extraer y manipular las evidencias.

Análisis en vivo: se conoce también como "en caliente" se hace sobre un sistema del que se presume ha sufrido o está sufriendo un ataque o incidente de seguridad. Para hacer este análisis se recomienda el uso de herramientas o medios que no afecten la integridad del sistema, en el caso de sistemas Windows que no incorporen cambios o se inscriban en el registro, así siempre será aconsejable usar herramientas que se ejecutan en modo autoejecutable y

DD
Comando nativo de los sistemas operativos tipo Linux que permite crear una réplica exacta de un disco duro en otro, permite también copiar desde discos duros deteriorados. La copia es idéntica al original.

Encase
Utilidad en línea que le acompaña durante todo el proceso del desarrollo de un análisis forense, cuida elementos clave como la cadena de custodia, línea de tiempo, rotulación entre muchos otros y dispone de herramientas para el clonado de discos, volcado de memorias, comparación de ficheros. Para más información visite el sitio:

https://www.guidancesoftware.com/encase-forensic

Integración de información
Hace referencia al posible cambio de que puede ser objeto la información que se recolecta como evidencia durante todo el proceso de adquisición y análisis, así siempre es necesario aplicar un procedimiento que permita verificar que la información obtenida en la fecha y hora de recolección coincide de forma idéntica con la expuesta en el momento de usar la prueba ante una corte.

HASH
Se conocen como funciones de resumen, se basan en un algoritmo que crea con base en una entrada (un archivo, un mensaje, un texto) un valor alfanumérico con longitud fija en el que se crea un resumen de todos los datos que recibió. Con los datos de entrada elabora una cadena que solo se puede generar de nuevo con los mismos datos. Así, el hash de cada archivo es único y aunque hubiese dos hash idénticos cada uno contiene el resumen de un archivo diferente.

desde unidades extraíbles, así se recomienda usar distribuciones como Kali Linux de las que hablaremos en los contenidos del eje praxiológico.

Usted como investigador forense debe recordar que siempre que trabaje en un sistema vivo debe desconfiar de todo lo que está visualizando, el sistema puede estar comprometido debido al ataque. Cuando se hace el análisis de un sistema vivo se recomienda obtener un log de los eventos, hacer una Figura de la memoria física, esta figura se debe computar con hash SHA-3, SHA-256 para asegurar su confiabilidad.

Ejemplo

Usted como investigador digital forense acompaña al equipo de la Policía Nacional en la atención de un incidente en el que se reporta el virus WANNACRY en algunos computadores de una red corporativa que ofrece servicios en la nube. Desarrolle las cuestiones planteadas en relación con su intervención.

A partir del contexto enunciado responda los interrogantes planteados. Argumente las respuestas.

1. ¿Qué tipo de análisis forense desarrollaría en los equipos afectados?, ¿por qué?

2. ¿Independiente de la respuesta planteada en el numeral anterior, sería conveniente apagar el servidor de la red?, ¿por qué?

3. ¿Qué situación puede pesar más para la integridad de la información y la seguridad de la compañía? ¿Apagar todos los equipos o permitir que sigan trabajando con los riesgos que el ataque puede implicar? ¿Cuál de los dos escenarios recomendaría usted?, ¿por qué?

4. Explique los elementos básicos que debe obtener del sistema cuando decide hacer un análisis en vivo.

5. Desarrolle y exponga los argumentos relacionados con la siguiente reflexión: usted como investigador forense puede asumir la responsabilidad de afectar así sea por cinco minutos el funcionamiento de un sitio en línea con miles de usuarios conectados alrededor del mundo, ¿qué riesgos podría tener apagar el sistema?

Otros tipos de datos que se recomienda obtener en un sistema en vivo son:

-Hora y fecha del sistema.

-Procesos que se están ejecutando en el momento del ataque.

-Conexiones de red.

-Puertos abiertos y aplicaciones asociadas.

-Usuarios que se encuentran trabajando en el sistema.

-Contenido de la memoria y archivos de intercambio SWAP o pagefile.

Fases de un análisis forense

Es fundamental que usted como investigador informático forense tenga en cuenta el concepto de cadena de custodia; en ciencias forenses y en cualquier tipo de investigación se hace necesario asegurar las evidencias obtenidas a través de un proceso estricto que busca:

- Registrar cómo se adquiere la evidencia.
- Registrar cómo se custodia la evidencia.
- Detallar cómo se controla la evidencia.
- Registrar cómo se transfiere la evidencia
- Detallar el procedimiento que realiza para analizar la evidencia.
- Registrar cualquier incidente o intervención que pueda alterar en su integridad o en parte la evidencia.

La siguiente figura detalla los procedimientos para aplicar la cadena de custodia a evidencias relacionadas con sistemas informáticos.

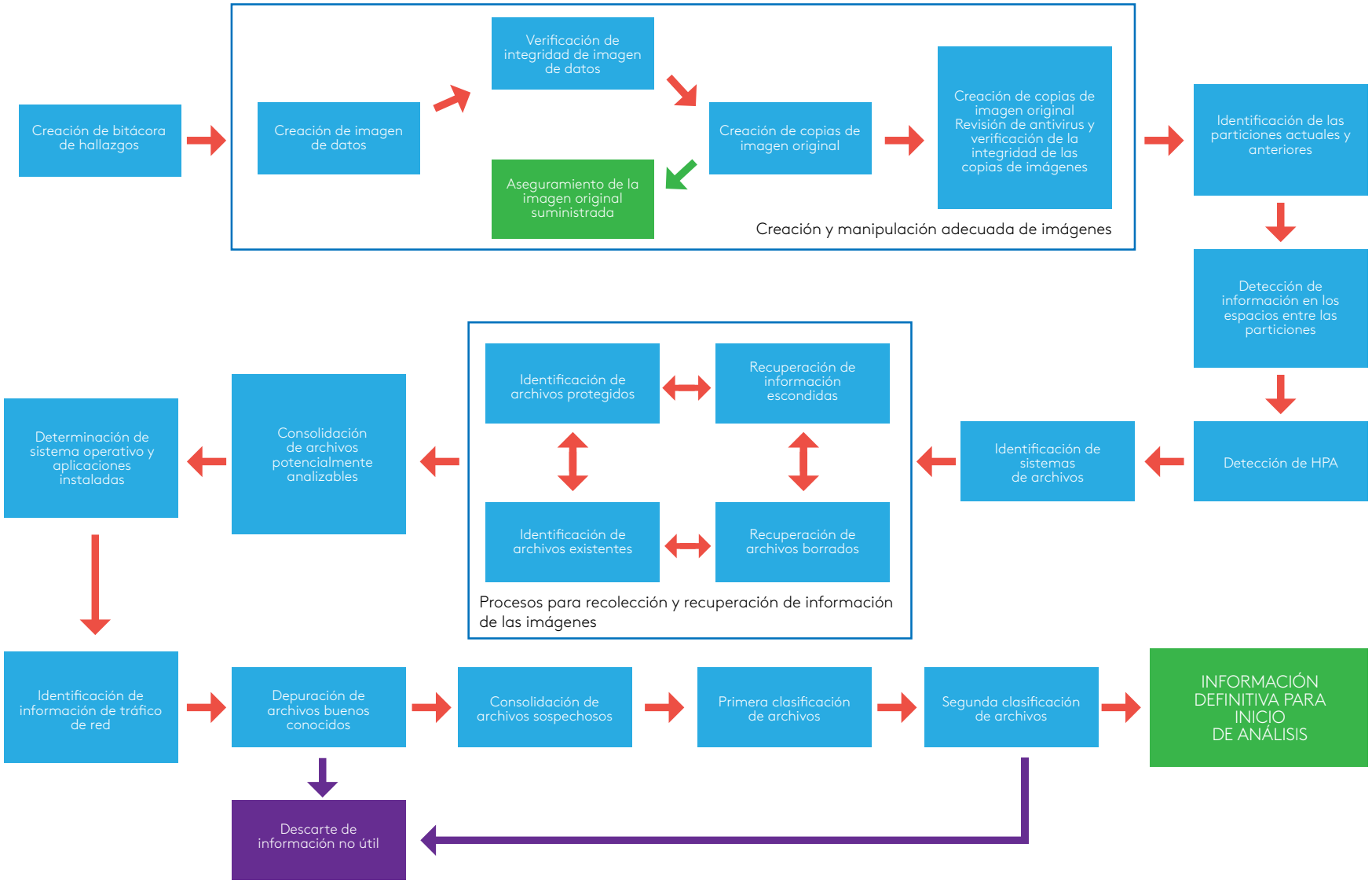


Figura 4. Recolección de información
Fuente: Mintic (2016).

No olvide que la manipulación de las evidencias se debe realizar ajustada a los más altos principios éticos y jurídicos que su formación exige, una alteración o pérdida de evidencia puede ser fundamental para el resultado de la investigación.

¡Lectura recomendada!

En el formato de cadena de custodia que encuentra en la página principal del eje como lectura recomendada Protocolos de cadena de custodia dos grandes etapas: preservación y procesamiento se puede verificar todos los detalles que se deben observar para asegurar la evidencia desde el momento en que se inicia la investigación hasta cuando es usada como prueba ante las autoridades o quien contrató la investigación.

¡Lectura recomendada!

Para conocer en mayor detalle lo relacionado con la cadena de custodia de la evidencia en Colombia lo invito a consultar el Manual de procedimientos para cadena de custodia (Fiscalía General de la Nación) en la página principal del eje.

Cuando usted como profesional en ingeniería de sistemas y con un amplio conocimiento de la informática forense, es contactado para realizar una investigación forense, debe cumplir con rigurosidad una serie de etapas que buscan asegurar y dar confiabilidad al informe pericial que entrega al final del proceso, las etapas que debe seguir para cumplir este propósito se detallan en el siguiente tema, por lo que lo invito a revisar en la página principal del eje, la siguiente vídeocápsula:

Video

"Ganador Premios ÍNDIGO 2016 C34 N5 #ViveDigitalTV"
https://www.youtube.com/watch?v=hYJ1n9j8KS4

Metodología para realizar un analisis forense

1. Identificar y/o evaluar la situación: este momento es llamado en el ámbito de la investigación forense, el momento cero (0), es aquí donde se toman decisiones tan importantes como: ¿en qué momento tomó la evidencia?, ¿lo hago a través de un análisis en caliente (en vivo)? Y muchas otras decisiones que pueden afectar el desarrollo y los resultados de la investigación; en esta fase como informático forense:

   - Evalúe los recursos, fije los objetivos y estime el alcance de la investigación.

   - Reúna los permisos y/o autorizaciones necesarias, así como los acuerdos de confidencialidad para desarrollar la investigación.

   - Registre todas las acciones que se presentan previas al evento, las situaciones asociadas a su llamado a investigar, las decisiones que se toman para responder al incidente, esta información orientará el desarrollo de las siguientes fases de la investigación.

   - De ser necesario organizar y delimitar el equipo de investigación, allí asignar responsabilidades y funciones.

   - Documentar el contexto de la situación a investigar, debe ser muy claro y tener en cuenta hasta los más pequeños detalles relacionados con la incidencia, fecha, hora, personas presentes durante el evento, cargo, nivel de responsabilidad, equipos afectados, tipo de daño entre otros, con esta información se podrá definir las posibles líneas de investigación.

   - Evaluar el impacto del incidente sobre las diversas líneas de acción de la empresa o del dueño del sistema, de ser posible tasar en dinero cada una de las situaciones derivadas del incidente, por ejemplo, tiempo de inactividad, costos de la investigación, baja en la productividad, costo de las acciones, por ejemplo.

   - Registrar y señalar los equipos afectados, su ubicación, su función (host servidor, estación de trabajo, switch, router).

   - Reseñar y describir los dispositivos de almacenamiento u otros elementos que forman parte de los sistemas y que pueden estar involucrados o suministrar información relevante para el análisis de la incidencia.

   - Identificar a los funcionarios, trabajadores, colaboradores, visitantes que usan o pudieron accedido a los equipos y tengan alguna relación con la investigación, sus perfiles de usuario, tipo de contraseñas entre otras y reunir toda la información posible que contribuya a conocer en su totalidad el contexto del ataque.

   - Recuperar los registros de eventos de los dispositivos intermediarios y de comunicaciones asociados a la red de datos.

Nota:

Previo a la adquisición de la evidencia es necesario diligenciar en todos sus detalles el formulario de cadena de custodia.

2. Recolectar y adquirir las evidencias: una vez se han cumplido los pasos del numeral anterior y se efectúe el registro detallado de la documentación de la cadena de custodia (primera parte), como informático forense debe proceder a efectuar la adquisición de la evidencia, no olvide que existe una gran diferencia entre recolectar y adquirir; el proceso de recolección es simple e implica identificar cada uno de los elementos que fueron víctimas del ataque o se pudieron usar para cometer el delito y acceder a ellos. La adquisición es un proceso técnico en el cual mediante herramientas válidas para la investigación se obtienen copias idénticas de los elementos u objetos que desea usar como evidencia, así le recomiendo que en primera instancia busque obtener información relacionada con los datos que pueden desaparecer con un apagado o reinicio del sistema (volátil):

   - Memoria caché del sistema.
   - Archivos temporales.
   - Procesos en ejecución.
   - Registro de eventos
   - Dispositivos conectados como enrutadores, cortafuegos, servidores, switchs.
   - Registro del sistema.
   - Toda la información relacionada con las conexiones de red abiertas en el momento del incidente.

Para el caso de un sistema apagado (post-mortem) es necesario que la adquisición de la información se haga en un espacio seguro, exclusivo para este trabajo y su posterior análisis, siempre observando con detalle diligenciar la documentación relacionada con la cadena de custodia. No olvide registrar como mínimo los siguientes datos relacionados con los dispositivos recolectados como evidencia:

- Fabricante y modelo del dispositivo.
- Tamaño, particiones (disco duro).
- Tipo de dispositivo (EIDE, SATA), maestro o esclavo.
- Puerto o puertos a los que está conectado.
- Descripción del equipo al que se encuentra conectado.

No efectúe ninguna prueba de integridad o aplique ninguna herramienta de verificación sobre los discos o unidades de almacenamiento originales, cualquier procedimiento que pueda alterar la integridad de la evidencia solo puede ser realizado sobre la copia adquirida. nunca trabaje sobre el original.

¡Lectura recomendada!

Sobre este tema lo invitamos a realizar la lectura Guía para la recogida de evidencia digital, en la página principal del eje.

3. Asegurar y manejar las evidencias: generar una firma o resumen con los algoritmos de cálculo de integridad o HASH. Este paso busca asegurar que el archivo original que tomó como evidencia conserva su integridad desde el momento de la adquisición y no ha sido objeto de manipulación durante el tiempo transcurrido entre la adquisición de la evidencia y la presentación como prueba, es indispensable observar algunas precauciones básicas para proteger y asegurar las evidencias y las copias:

   - Mantener los discos o unidades de almacenamiento en un lugar adecuado, que no permita su manipulación por terceros.

   - Evitar que equipos como discos duros o medios de almacenamiento puedan encontrase cerca de fuentes de interferencia electromagnética o estática, esto puede alterar su integridad.

   - De ser posible obtenga una nueva copia del original y trabajar sobre la segunda copia, para evitar posibles pérdidas de evidencia.

   - Asegurar por medios físicos y digitales la evidencia, cajas fuertes, claves para acceder al dispositivo.

   - Todos los pasos mencionados documentarlos en detalle en la documentación relacionada con la cadena de custodia (parte 2).

¡Recordemos que!

En el documento de cadena de custodia debe quedar registrada la información de la o las personas que acceden a la evidencia, la hora en la que acceden a ella, la hora en la que se retiran entre otras.

4. Analizar las evidencias: en esta etapa se hace la validación relacionada, con las preguntas clave de la investigación forense: cómo, quién, dónde, cuándo. Aquí se accede a elementos clave para la investigación como los metadatos de los archivos, estos pueden suministrar información valiosa para el investigador no solo para hallar un responsable, también por ejemplo a través de los metadatos de archivos como fotografías podemos ubicar la latitud, longitud y dar con su paradero. También como análisis de evidencia podemos tomar el ejemplo de la copia de la memoria RAM de un servidor objeto de un ataque por una persona con amplios conocimientos en seguridad informática, en un delito relacionado con Sarlaft en el tema de prevención de lavado de activos. El análisis de los datos se divide en tres grandes etapas que se indican a continuación.

Sarlaft
Categoría de delitos que agrupa el lavado de activos y financiación del terrorismo.

- Análisis de los datos de la red: es necesario reconocer cuales son los dispositivos que hacen parte de la red de datos en la cual se encuentra el equipo víctima o atacante, encontrar routers, switch, firewall, proxys, y examinar sus registros de eventos a través de software destinado para tal fin, allí podremos encontrar información vital para la investigación.

- Análisis de los datos del host: este análisis se hace de forma preferente en sistemas vivos, se recomienda obtener datos relevantes del sistema que ayuden a la investigación puesto que el volumen de la información que se obtenga puede entorpecer la labor del investigador, así por ejemplo se recomienda hacer un volcado de memoria física, registro de eventos, registro de puertos y conversaciones (TCP) abiertas entre otros.

- Análisis de medios y dispositivos de almacenamiento: usar de forma preferente la segunda copia, organizar los archivos con una estructura que facilite obtener la información relacionada con el incidente, obtener copia del registro de eventos del sistema operativo, identificar sobre que archivo o archivos ha prosperado el daño o amenaza, examinar el registro del sistema y los logs de booteo, información de active directory, historiales de navegadores entre otros.

- Identificar y analizar los metadatos de archivos que puedan estar involucrados con un delito o incidencia.

5. Diseñar y presentar los informes: algunos autores consideran esta etapa como la más importante del proceso, pues la solidez de los argumentos expuestos y el cumplimiento cabal de cada una de las etapas descritas en los pasos anteriores dará soporte a la información suministrada en el informe.

¡Recordemos que!

Una de las razones más frecuentes por las que no se acepta la evidencia presentada en un proceso legal es la manipulación inadecuada de las pruebas, es decir no se cumplió de forma adecuada con la cadena de custodia. Por ello no hay que olvidar cumplir de forma estricta con diligenciar de forma cuidadosa de todas y cada una de las acciones que se desarrollan a partir del punto uno.

El informe que se presente como resultado de la investigación puede tener dos tipos de destinatarios, así de acuerdo al público destino se puede realizar dos tipos de informe:

- Informe ejecutivo.
- Informe técnico pericial.

La forma y el contenido de cada informe se presentan en el desarrollo del eje 4.

Se recomienda que el investigador, antes de hacer un análisis forense, construya una línea de tiempo relacionada con la investigación; en ella se deben registrar algunos filtros o parámetros relacionados con momentos clave de la investigación, de suma importancia para el ciclo de la investigación y la organización de la información obtenida. Un caso práctico del uso de la línea de tiempo puede identificarse en el análisis de navegadores; por ejemplo, si un delito se presentó en cierta fecha, no tiene sentido que se haga el análisis de información registrada en momentos en que ni siquiera existían vínculos entre víctima y victimario.

Principios que debe observar el peritaje informático

Para asegurar la validez del procedimiento que el investigador forense desarrolla, se deben observar algunos requisitos mínimos que garanticen, ante los destinatarios del informe, que se han cumplido unas normas mínimas en relación con el desarrollo de su labor, así estos principios deben asegurar:

- Objetividad: su trabajo no puede basarse en prejuicios o juicios subjetivos, debe ajustarse a altos principios éticos.

- Autenticidad y conservación: como investigador debe garantizar que los medios usados como prueba no han sido objeto de alteración o manipulación, voluntaria o accidental.

- Idoneidad: los medios que usted emplee como prueba deben ser originales, y tener la importancia y pertinencia necesaria para el caso que investiga.

- Legalidad: en desarrollo del peritaje se deben observar todas las normas contempladas en la legislación vigente, además las apreciaciones y juicios emitidos deben ajustarse a estos parámetros.

- Inalterabilidad: con base en la cadena de custodia, se debe garantizar que los medios que se usan como prueba no han sido objeto de manipulación o modificación.

- Documentación: todos los pasos que se desarrollan durante el proceso deben ser registrados y apoyados con los documentos de cadena de custodia.

Escenarios de uso de la informática forense

Es claro que la ubicuidad de las tecnologías de la información pone en todos los escenarios de nuestra vida diaria dispositivos tecnológicos, así los individuos que ven en los sistemas informáticos una oportunidad para desarrollar actividades ilegales cada día inventan nuevos métodos, en la actualidad podemos definir algunos escenarios como los más comunes para el uso de la informática forense que se presentan a continuación, pero igualmente se recomienda la lectura complementaria, y la videocápsula *Tecnología forense: CTI*, que encuentra en la página principal del eje.

¡Lectura recomendada!

Contexto actual de la formación del perito informático en el escenario internacional y su realidad en Colombia.

Video

"Tecnología Forense: CTI" https://www.youtube.com/watch?v=5CmM9K_FCqc

- Ocurrencia de un delito informático común.

- Sospechas respecto a la pérdida de información al interior de la organización.

- Infecciones provocadas por amenazas como malware.

- Existencia de ataques informáticos convencionales o por técnicas comunes, malware, fuerza bruta, ataque por diccionario, denegación de servicios.

- Robos de información.

- Uso de las tecnologías de la información para adelantar delitos como las amenazas y/o extorsiones.

- Delitos informáticos de alto impacto como el ciber terrorismo, trata de personas y la pedofilia entre otros.

Problemas habituales en el análisis forense

En el desarrollo del presente documento, se ha hecho énfasis en la cadena de custodia y la necesidad de su aplicación y cuidado estricto durante toda la investigación, por supuesto, esta es tan solo una de las situaciones complejas que usted como informático forense deberá afrontar durante el desarrollo de una investigación; a continuación, se detallan algunas situaciones comunes.

- Cuando se clona un disco duro u otro medio de almacenamiento es necesario usar las utilidades reconocidas como válidas y aprobadas por los entes judiciales correspondientes; además, se debe buscar que la copia de discos duros se realice sobre dispositivos nuevos y formateados a bajo nivel previamente. De ser posible se recomienda usar dispositivos diseñados de forma específica para copia de discos y no una computadora común.

- La protección de datos personales es un tema complejo y delicado en cada uno de los países, por esta razón es necesario que cuando se reciba el dispositivo y se registre los documentos de cadena de custodia ser muy específico en qué se va a analizar y con qué fin.

- No olvidar que la inviolabilidad de las comunicaciones personales el derecho a la intimidad entre otros son derechos fundamentales de los ciudadanos en Colombia; así, si al analizar la evidencia usted no cuenta con la autorización requerida para verificar ciertos contenidos del disco, los dispositivos, o el tráfico de red obtenidos absténgase de analizarlos o revisarlos puede estar cometiendo un delito con serias consecuencias penales. Los apartes relacionados con la legislación existente para la protección de datos personales y la investigación de delitos informáticos serán revisados en detalle en el desarrollo del eje articulador sociocrítico.

- Se deben solicitar las autorizaciones necesarias por parte de las autoridades judiciales para examinar muchas de las evidencias que pueda haber obtenido durante la recolección, para esto se recomienda consultar con un abogado.

- Durante el análisis de la evidencia es común que no se pueda determinar la identidad del individuo que pudo haber alterado el sistema, o borrado un archivo, por ejemplo, esta situación implica que tengamos que entrar a demostrar que el "sospechoso" fue quien ingreso al sistema, bien sea de forma directa al equipo o a través de una red.

- Una dificultad básica consiste en establecer la conexión entre el incidente y las consecuencias, así ha de ser muy cuidadoso en la lectura e información relacionada con los sistemas a analizar para identificar conexiones entre uno y otros eventos.

- En las secciones anteriores se recomendó elaborar la línea de tiempo como un elemento básico del ciclo de investigación para establecer el momento exacto en que se presentó el ataque o vulneración, así usted debe tener en cuenta sincronizar los relojes de los dispositivos que use para la investigación a través de herramientas como NTP.

Evidencia digital

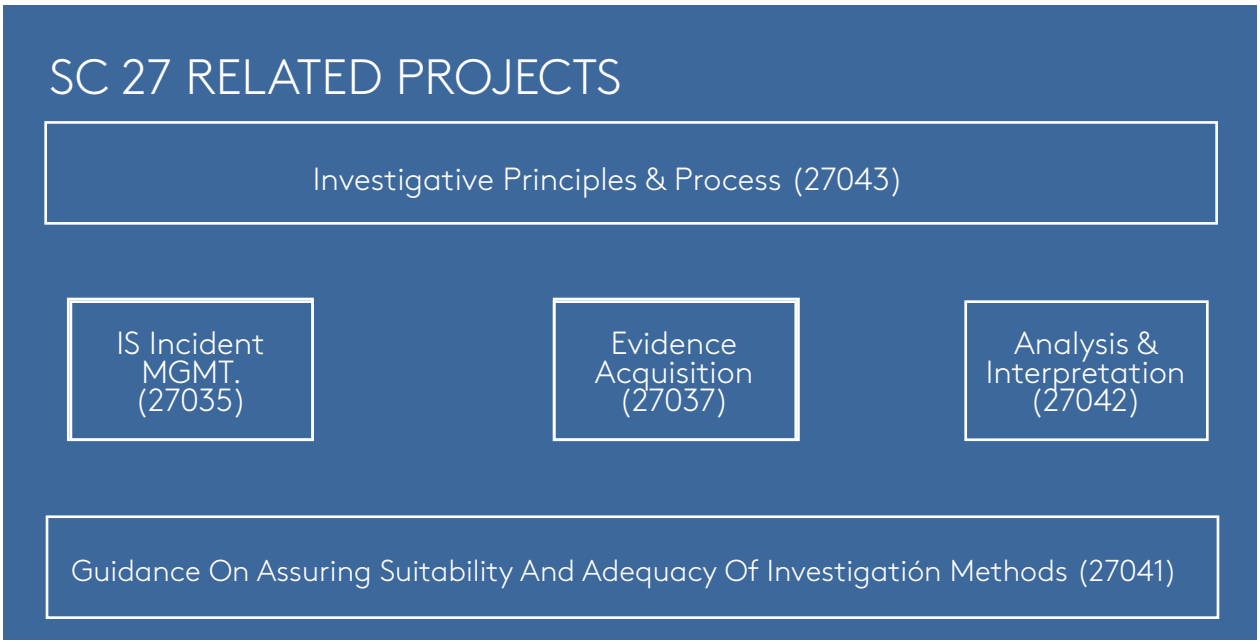


Figura 5. Desarrollo de estándares internacionales
Fuente: Cloud security Alliance; mapping the forensic estándar ISO/IEC 27037 to cloud computing.

Estamos por finalizar nuestro recorrido por toda la información que usted, como investigador informático forense, necesitará para resolver la pregunta que da origen al presente documento, a lo largo de él hemos definido conceptos que enriquezcan su glosario y contribuyan a una mayor comprensión del tema. Sin embargo, es necesario detenernos a analizar un concepto adicional que debemos atender como parte de nuestro trabajo y es la evidencia digital.

Fernández (2004) define la evidencia digital como la información almacenada en dispositivos electrónicos, bien sea medios magnéticos, ópticos, estado sólido, que puede ser usada como prueba en procesos de carácter judicial. Para usarla con este propósito se debe cumplir de forma estricta un conjunto de técnicas y procedimientos para su recolección, adquisición, almacenamiento y análisis.

Casey (2004) establece que cualquier dato que pueda aportar información sobre la comisión de un delito, o proporcione alguna conexidad entre delito y víctima, o delito y autor se considera evidencia digital, además extiende su definición y la considera un tipo de evidencia física construida a partir de campos magnéticos y pulsos electrónicos que se pueden agrupar y analizar usando técnicas y herramientas específicas.

Caldana, Correa y Ponce (2014) la definen como la "información creada, transmitida, procesada, registrada y/o mantenida electrónicamente, que respalda el contenido de un informe de auditoría y que puede tomar diferentes formas, tales como texto, imagen, audio, video, entre otros".

Características de la evidencia digital

La evidencia digital, contrario a la evidencia física, reúne una serie de características que exige que la labor del investigador en su recolección y cumpla con unos parámetros muy exigentes, algunos de ellos se encuentran registrados en la RFC 3227, en esta "request for comments" se definen los lineamientos para la recolección y archivo de evidencia digital.

Algunas de sus características más relevantes son:

- Fragilidad: este tipo de evidencia puede ser alterada, modificada o destruida con un simple descuido del investigador o alguna persona en la escena; por ejemplo, el abrir un archivo del que se sospecha está relacionado con un ataque cambiará su fecha de modificación, lo cual podría hacerlo inservible para la investigación.

- La posibilidad de realizar múltiples copias de la información sin que exista un registro de quien los realizó, puede afectar el secreto o confidencialidad de los datos, sin que el investigador pueda establecer el responsable de un robo de información.

- La posibilidad de duplicación bit a bit de la evidencia digital proporciona al investigador herramientas para hacer un análisis exhaustivo de un conjunto de datos sin alterar la evidencia original.

- Es posible trabajar con una copia idéntica del sistema y simular las condiciones de funcionamiento del momento del ataque o incidente sin alterar la evidencia.

- La trazabilidad de las actividades efectuadas a través de un sistema informático, hace posible que el investigador obtenga información valiosa.

- Eliminar la evidencia digital es un proceso complicado y poco exitoso; gracias a las herramientas de análisis forense existentes en el mercado

es posible recuperar la información contenida en un disco duro o en un medio de almacenamiento extraíble aun después de un formateo lógico o partición física, es decir todo deja huellas.

- El diseño de los sistemas de información y características propias de los sistemas operativos entre otros hacen que de una actividad que desarrolla el individuo en el computador puedan quedar rastros en diferentes archivos y ubicaciones.

Clasificación de la evidencia digital

Existen varias categorías para clasificar la evidencia, una de ellas depende del tipo de sistema sobre el que se efectúa la recolección.

- Evidencia volátil: hace referencia a la evidencia que en procedimientos estándar puede ser obtenida en sistemas en vivo, las evidencias que se pueden obtener fueron descritas en la segunda parte de este documento.

- Evidencia perdurable: se refiere a la evidencia recolectada en sistemas post-mortem, copias adquiridas de discos duros, unidades ópticas, unidades extraíbles entre otras.

Según el medio en que se puede encontrar la evidencia, Stephenson (2014) la clasifica en:

- Evidencia física: cuando la evidencia a recolectar se encuentra en un medio físico como discos duros, unidades extraíbles, teléfonos móviles, memoria RAM entre otros.

- Evidencia de transmisión: es la evidencia digital que se encuentra o ha sido transmitida a través de algún medio de red, por ejemplo, la captura de una trama en medios locales, un paquete de datos en un router.

En el mismo sentido Stephenson (2003), clasifica la evidencia digital según el medio o artefactos en los cuales se pueda encontrar, la clasificación propuesta según el origen es la siguiente, pero antes no está de más recordar algunos conceptos con esta actividad:

- Artefactos del sistema de archivos: hace referencia a las evidencias obtenidas o relacionadas con los sistemas de archivos de un sistema de procesamiento de información, tablas de asignación en sistemas FAT, tabla maestra en sistemas NTFS, súper bloque en sistemas tipo Linux o Unix, o árbol-B+ para sistemas tipo OS.

- Artefactos del sistema operativo: hacen referencia a los archivos volátiles creados por los distintos sistemas operativos, que por lo general se construyen después de su instalación y se modifican de forma permanente durante su ejecución, por

ejemplo, el registro de Windows,/etc. para sistemas Linux, plist para sistemas tipo OS.

- Artefactos de aplicación: se denomina así a los sistemas de archivos y archivos y objetos creados por aplicaciones o programas instalados en el sistema o medio.

- Artefactos de usuario: se refieren a los archivos creados en las cuentas de los usuarios que han iniciado sesión en el equipo, dentro de ellos se incluyen los correos electrónicos, imágenes, documentos, conversaciones de chat y cualquier otro archivo que se genera cuando el usuario inicia sesión en el equipo.

Otros términos relacionados con la evidencia digital son definidos por Stephenson (2003), para referirse al estado (material o no) en que se puede hallar, así según esta clasificación podemos hablar de:

- Evidencia digital lógica: es aquella cuya integridad y disponibilidad se encuentra intacta, y se puede acceder a ellos sin la necesidad de herramientas adicionales, no necesita de reconstrucción, pero el investigador debe observar especial cuidado de abrir o ejecutar algún archivo puesto que estas acciones pueden modificar los metadatos y volver inservible un archivo para la investigación.

- Evidencia digital de seguimiento o traza: se refiere a la información o datos relacionados con la investigación a los cuales no se puede acceder de forma directa a través del sistema y para obtenerlos se emplean utilidades de recuperación de archivos o particiones, por ejemplo, información proveniente de discos duros formateados, memorias borradas, correos electrónicos y conversaciones eliminados, entre otros.

Manejo de la evidencia digital

La rápida incursión de las tecnologías de la información y las comunicaciones en el ámbito de la investigación forense, ha sido objeto de regulación y estudio por parte de múltiples organismos internacionales, así previo a la existencia de una norma de carácter mundial, la investigación informática forense tomó como base los lineamientos expedidos por el FBI y el Instituto Nacional de Estándares y Tecnología.

En el año 2012 la organización internacional para la estandarización, expide la norma ISO/IEC 27037 (2012), a través de la cual se formulan los lineamientos para las actividades específicas relacionadas con la manipulación de evidencia digital como la identificación, recolección, adquisición, y preservación de evidencia digital potencial que puede ser valorada como evidencia en un proceso. La Organización Internacional para la Estandarización (ISO) por sus siglas en Inglés, se encuentra desarrollando un amplio conjunto de normas relacionadas con todo el ciclo de la informática forense, en la actualidad solo se encuentra desarrollada la norma referente al manejo de la evidencia digital, pero a futuro se espera contar con el conjunto de normas técnicas estándar para que la evidencia o

investigación que se inicia en un territorio pueda ser usado en otro sin problemas de carácter legal relacionados con la legislación existente en cada uno, la figura muestra la estructura del marco normativo que propone la organización para el ciclo digital forense:

La Normativa ISO 27037 detalla los siguientes aspectos en relación con la evidencia digital:

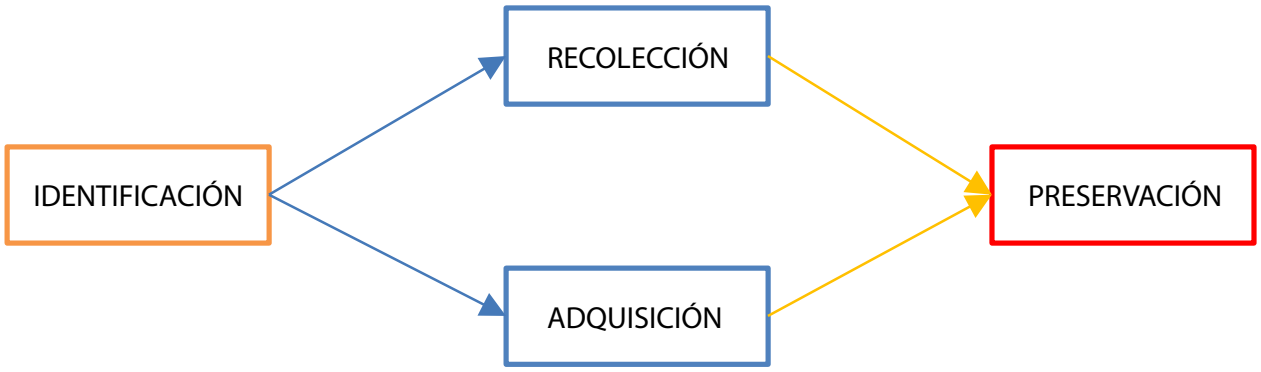


Figura 6. Evidencia digital ISO 270371
Fuente: propia

- Identificación: es el inicio del proceso forense, en él se accede a la escena del delito y/o a los equipos y sistemas que fueron víctimas de un ataque o fueron usados para él, la norma lo define como "el procedimiento de búsqueda, reconocimiento y documentación de evidencia digital potencial" (ISO 27037, 2012).

- Recolección y adquisición: la norma establece diferencias entre los dos términos así:

- La recolección, "es el proceso a través del cual se recopilan elementos que contienen evidencia digital potencial" (ISO 27037, 2012).

- La adquisición, "es el proceso de creación de una copia de datos como parte de un conjunto definido".

- Así, y apelando a las definiciones y recomendaciones contempladas en la norma la recolección se aplica de forma más común en procesos que involucran autoridades judiciales, en las cuales a partir de una orden se pueden incautar los equipos que el investigador considere necesarios para la investigación, trasladarlos a un laboratorio e iniciar el proceso de análisis.

- En tanto la adquisición se emplea más en investigaciones de carácter corporativo, investigaciones internas por ejemplo en las que es fundamental garantizar la continuidad del negocio, por tanto, los equipos no pueden ser apagados o removidos de su sitio y el investigador debe proceder a "adquirir" copias de la información necesaria para la investigación. Es necesario tener en cuenta que independiente

del escenario, usted apreciado investigador debe efectuar las copias de discos, medios, volcados de memoria RAM, a través de herramientas aceptadas en los procesos de investigación, con un proceso bien documentado, defendible en el que se garantice la integridad de la información y que las copias obtenidas no han sido modificadas a partir de su adquisición.

- En todo caso el proceso de recolección, siempre será mucho más sencillo que el de adquisición, sin embargo, le recuerdo que en los detalles sencillos existe el mayor riesgo. No olvide la cadena de custodia.

- Preservación; la norma ISO 27037, la define como el proceso de mantener y salvaguardar la integridad y/o condición original de la evidencia digital potencial.

- Preservar la evidencia potencial digital es un proceso sumamente importante, una adecuada preservación puede contribuir a que la evidencia pase de potencial a usable en un proceso judicial. Es decir, en un proceso legal, solo cuando la evidencia recolectada y adquirida es presentada ante el juez junto a su relevancia en la investigación, cadena de custodia, procedimiento de identificación, adquisición y preservación puede pasar a convertirse en prueba del proceso, si el juez decide aceptarla.

Es necesario aclarar que la preservación de la evidencia digital es tal vez uno de los procesos más críticos dentro de la investigación forense, la evidencia digital potencial, es muy frágil y puede ser destruida o alterada con mucha facilidad.

¡Lectura recomendada!

Esto puede evidenciarlo en la lectura complementaria Preservación digital en la página principal del eje.

El paso del tiempo entre el inicio de la investigación y su presentación ante un juez como prueba puede tardar mucho tiempo, en Colombia por ejemplo es mayor a un año en el mejor de los casos. Así, las recomendaciones de la norma respecto a su preservación destacan las siguientes condiciones:

1. La evidencia debe ser recolectada siguiendo los más altos estándares relacionados con la investigación forense, debe efectuarse por personal experto y autorizado, no debe manipularse directamente (use guantes especiales). Durante la recolección tenga cuidado de etiquetar cada uno de los elementos recolectado, las etiquetas no deben cubrir información de identificación de los elementos y se recomienda que sigan las condiciones previstas por las autoridades y sujeto a la cadena de custodia.

2. Los dispositivos móviles deben ser sellados por el investigador en las partes susceptibles de realizar conexiones, por ejemplo, en un Smartphone se debe sellar su puerto de carga y las ranuras de las tarjetas SIM y de memoria. Los stickers de los sellos deben llevar la firma del investigador.

3. Los dispositivos que contienen información volátil que depende de una batería, deben ser guardados anotando esta observación y se debe verificar con frecuencia el estado de las baterías para evitar que se pierda la información.

4. De requerir transporte de los dispositivos, estos deben ser dispuestos en recipientes para tal fin que los protejan del calor, las vibraciones y las interferencias electro magnéticas y electro estáticas.

5. El investigador debe acompañar la evidencia durante el transporte asegurándose que se cumpla con las normas locales previstas para este fin.

6. El lugar en que se almacene la evidencia digital potencial debe garantizar como mínimo las siguientes condiciones, según las recomendaciones efectuadas por Watson y Jones (2013):

    - Iluminación, ventilación y nivel de humedad adecuados para almacenar este tipo de evidencias.

    - Se debe generar un registro de control de visitantes y personas que pueden acceder a la evidencia para su análisis en el que se identifique la persona, el cargo, las fechas y horas exactas en que accede a la evidencia la razón por la que la solicita y el tipo de trabajo que realiza.

    - El almacén en el que se mantiene la evidencia debe garantizar que el acceso o movimiento de los dispositivos solo se realice para efectos relacionados con esa investigación, por ejemplo se almacenan o apilan tres gabinetes de computador de distintas investigaciones uno tras otro y para acceder al tercero se necesita mover los otros dos que son de investigaciones diferentes, durante este movimiento o por estas condiciones se puede, por ejemplo, causar un pequeño rayón en uno de los gabinetes, marca que no estaba en el proceso de recolección de la evidencia y por un detalle tan pequeño como este, que para nada afectó la integridad de la información, los abogados de la contraparte y el juez pueden invalidar esta evidencia.

Reflexionemos

Si dadas las condiciones anteriores, usted como investigador fuera declarado responsable de negligencia por no cuidar la evidencia de forma rigurosa, ¿qué argumentos usaría en su defensa?

Antes de realizar la evaluación pongámonos a prueba con la actividad de repaso:

Usted como investigador digital forense acompaña al equipo de la Policía Nacional en la atención de un incidente en el que se reporta el virus WANNACRY en algunos computadores de una red corporativa que ofrece servicios en la nube. Desarrolle las cuestiones planteadas en relación con su intervención.

Dentro de los procedimientos más comunes para el aislamiento de la escena, se encuentran los siguientes:

De ser preferible, tomar una fotografía del equipo o sitio del incidente antes de tocarlo.

Establecer un perímetro de seguridad, para que nadie pueda acercarse.

Si el equipo se encuentra encendido, no se debe apagar, deberá procederse a realizar los siguientes procedimientos:

- Sellar los puertos USB, firewire, unidades CD/DVD, etc... para impedir alguna alteración posterior al registro de la escena.

- Tomar fotografías de lo que se puede ver en la pantalla (software corriendo, documentos abiertos, ventanas de notificación, hora y fecha ilustrados)

- Asegurar el equipo (si es portátil, tratar de mantenerlo encendido con el cargador hasta hacer entrega o iniciar el análisis respectivo).

- Si es posible capturar información volátil del equipo antes de que se apague, debe hacerse empleando las herramientas forenses necesarias.

Si el equipo se encuentra apagado, no realizar el encendido, esto puede alterar la escena o borrar información que podría lograr obtenerse posteriormente.

Llevar los elementos necesarios para la recolección de información como estaciones forenses, dispositivos de backups, medios formateados y/o estériles, cámaras digitales, cinta y bolsas para evidencia, papel de burbuja, bolsas antiestáticas, cajas de cartón, rótulos o etiquetas etcétera.

Almacenar la información original en un sitio con acceso restringido, para garantizar la cadena de custodia de la información.

Obtener información de dispositivos que tuvieron contacto o interacción con el equipo en cuestión (switches, firewalls, Access Points, etcétera).

Tomado de *Guía 13 Seguridad y Privacidad de la Información (Mintic, 2016)*.

Con base en las recomendaciones expedidas por el Ministerio de las Tecnologías de la Información y las Comunicaciones para el manejo de la evidencia digital, y de acuerdo con el caso expuesto en la descripción de la guía, elabore un informe en el que explique las acciones que desarrolló para la atención del incidente en el que asistió como investigador.

BIBLIOGRAFÍA

Bbrezinski, D. y Killalea, T. (2002). *RFC 3227: Guidelines for Evidence Collection and Archiving. Network Working Group*. Recuperado de http://www.rfceditor.org/rfc/rfc3227.txt

Cano, D. (2011). *Contra el fraude: prevención e investigación en América Latina*. Buenos Aires, Argentina: Ediciones Granica.

Casey, E. (2004). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Baltimore, EE. UU.: Eoghan Casey.

Cano. J. (2010). *El peritaje informático y la evidencia digital en Colombia: conceptos, retos y propuestas*. Bogotá, Colombia: Universidad de los Andes.

Ormazábal, S. G., Pasamar, A. y Bellido M. (2006). *Empresa y prueba informática*. Barcelona, España: J y B.

Fernández, D. (2004). *Encuentro de hacking ético*. SIMO, Sevilla, España.

Fiscalía General de la Nación (2006). *Manual de procedimientos de cadena de custodia*. Bogotá, Colombia: Fiscalía General de la Nación.

Insa, M. F., y Lázaro, H. C. (2008). *Pruebas electrónicas ante los tribunales en la lucha contra la cibercriminalidad: un proyecto europeo*. Caracas, Venezuela: Red Enlace.

Instituto Nacional de Ciencias Penales. (2012). *Protocolos de cadena de custodia: dos grandes etapas: preservación y procesamiento*. Ciudad de México, México: Instituto Nacional de Ciencias Penales.

Miller, M. (2014). Exercise C - *Locard Exchange Principle,* Crime Scene Investigation Laboratory Manual, 15-20. Doi:10.1016/B978-0-12-405197-3.00003-4

Ministerio de las Tecnologías de la Información y las Comunicaciones. (2014). *Guía 21. Guía para la gestión y clasificación de incidentes de seguridad de la información*. Bogotá, Colombia: Ministerio de las Tecnologías de la Información y las Comunicaciones.

Ministerio de las Tecnologías de la Información y las Comunicaciones. (2016). *Guía 13, Evidencia digital. Serie seguridad y privacidad de la información*. Bogotá, Colombia: Ministerio de las Tecnologías de la Información y las Comunicaciones.

Stephenson, P. (2003). Structured Investigation of Digital Incidents in Complex Computing Environments. *Information Systems Security, 12*(3), 29-38.

BIBLIOGRAFÍA

Téllez, J. (2009). *Derecho informático*. Ciudad de México, México: McGraw-Hill Interamericana.

Watson, D. y Jones, A. (2013). *Digital Forensics Processing and Procedures*. Londres, Reino Unido: Ed. Syngress.

ISO/IEC. (2012). *Information technology - Security techniques - Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence*. Ginebra, Suiza: ISO.