INFORMATICA FORENSE

ING. ESP. HAROLD EMILIO CABRERA MEZA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
PASTO – COLOMBIA
2013

TABLA DE CONTENIDO

UNIDAD 1. FUNDAMENTOS DE LA INFORMÁTICA FORENSE 3
CAPITULO 1. INTRODUCCIÓN A LA INFORMÁTICA FORENSE 4
Lección 1. Qué es la Informática forense 4
Lección 2. Definiciones generales 5
Lección 3. Qué es el delito informático 5
Lección 4. Tipos de delito informático 7
Lección 5. Ley 1273 de 2009 Protección de la Información y de los Datos en Colombia. 9
CAPITULO 2. FASES DE LA INFORMÁTICA FORENSE. 13
Lección 6. Descripción de las fases de la Informática Forense. 13
Lección 7. Fase de Identificación 15
Lección 8. Fase de Validación y preservación. 19
Lección 9. Fase de Análisis 21
Lección 10. Fase de Documentación y Presentación de las pruebas 29
CAPITULO 3. ACCIONES EN LA ESCENA DEL FRAUDE INFORMATICO 32
Lección 11. Identificando las vulnerabilidades informáticas. 32
Lección 12. Preservar la escena del Fraude. 33
Lección 13. Claridad de la evidencia. 37
Lección 14. Formato de la evidencia en la escena. 39
Lección 15. Cuidados de la evidencia en la escena. 40
UNIDAD 2. ANÁLISIS DE LAS EVIDENCIAS Y HERRAMIENTAS COMPUTACIONALES PARA INFORMÁTICA FORENSE. 44
CAPITULO 4. RECOLECCION DE EVIDENCIA DIGITAL. 45
Lección 16. Estrategias para la recolección de pruebas electrónicas 45
Lección 17. Orientaciones para Recolección de Evidencias. 47
Lección 18. Volatilidad de la evidencia. 48
Lección 19. Recomendaciones Generales 50
Lección 20. Análisis de la Evidencia Recolectada 51
CAPITULO 5. HERRAMIENTAS DE SOFTWARE UTILIZADAS EN LA INFORMÁTICA FORENSE. 56
Lección 21. Aplicaciones para Investigación Forense 56
Lección 22. Clasificación de herramientas para informática forense 59
Lección 23. Construcción de un kit de herramientas de informática forense 60
Lección 24. Utilizando rastreadores de paquetes para reunir pruebas. 62
Lección 25. Recomendaciones Sobre el uso de software 63
CAPITULO 6. DESARROLLO DE UN CASO DE INFORMÁTICA FORENSE 64
Lección 26. Reconocimiento de los sistemas operativos. 64
Lección 27. Imágenes de Discos Duros. 65
Lección 28. Iniciar un caso de informática forense. 69
Lección 29. Donde buscar evidencia. 69
Lección 30. Analizando información 71

UNIDAD 1. FUNDAMENTOS DE LA INFORMÁTICA FORENSE

CAPITULO 1. INTRODUCCIÓN A LA INFORMÁTICA FORENSE

Lección 1. Qué es la Informática forense

La Informática forense es una nueva disciplina dedicada a la recolección de pruebas digitales desde una maquina computacional para fines judiciales mediante la aplicación de técnicas de análisis y de investigación. La aparición de la informática forense como una disciplina se remonta a 1989 con la creación de la primera "ciencia de la computación forense" en la Ley Federal de los EE.UU.

El tipo de pruebas digitales obtenidas a partir de un examen forense que se realizar a una máquina computacional puede ser útil en una amplia gama de investigaciones judiciales como por ejemplo:

- Litigios civiles en los casos de divorcio y el acoso.
- Evidencia de malversación de fondos, fraude o robo sobre propiedad intelectual.
- Pruebas en la discriminación por edad, sexo, raza o por despido injustificado
- Investigaciones de compañías de seguros cuando se exijan pruebas relativas al seguro
- Fraude, homicidio culposo
- Casos relacionados con seguros y reclamaciones
- se utiliza en la recuperación de información que haya sido borrada, cifrada o dañado.

La evidencia digital como vemos puede ser aplicada en una amplia gama de delitos y la informática forense utiliza una variedad de métodos para descubrir los datos que residen en un computador o sistema informático.

Lección 2. Definiciones generales

El E-discovery o descubrimiento electrónico es la parte del proceso de descubrimiento que se centra en la búsqueda de pruebas en formato electrónico por lo general de un computador.

De acuerdo con el Guidelines for the Management of IT Evidence, la evidencia digital es: "cualquier información, que sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático". En este sentido, la evidencia digital, es un término utilizado de manera amplia para describir "cualquier registro generado por o almacenado en un sistema computacional que puede ser utilizado como evidencia en un proceso legal".

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.

La informática forense hace entonces su aparición como una disciplina auxiliar de la justicia moderna, para enfrentar los desafíos y técnicas de los intrusos informáticos, así como garante de la verdad alrededor de la evidencia digital que se pudiese aportar en un proceso. [Acis06].

Lección 3. Qué es el delito informático

Para comprender porque la informática forense ha adquirido importancia en la actualidad debemos comprender donde se origina el delito.

Definición de Delito Informático

“Delincuencia informática es todo Acto o conducta ilícita e ilegal que pueda ser considerada como Criminal, dirigida a alterar, socavar, destruir, o manipular,

cualquier sistema informático o alguna de sus partes componentes, que tenga Como finalidad causar una lesión o poner en peligro un bien jurídico Cualquiera"[1]

Los delitos informáticos son "toda conducta que revista características delictivas, es decir, sea típica, antijurídica y culpable, y atente contra el soporte lógico de un sistema de procesamiento de información, sea sobre programas o datos relevantes, a través del empleo de las tecnologías de la información, y el cual se distingue de los delitos computacionales o tradicionales informatizados".

Clasificaciones del delito informático

Los delitos informáticos se pueden clasificar en los siguientes grupos de delitos

Fraudes cometidos mediante manipulación de computadores: Entre estos se encuentran la manipulación de datos de entrada y salida y la manipulación de programas. En cada caso, lo que se trata es de colocar datos falsos en un sistema u obtener los datos del sistema en forma ilegal.[2]

Falsificaciones Informáticas: En este punto se trata de usar los computadores como elemento para falsificar entradas, dinero, tickets o cuentas bancarias.

Daños a Datos Computarizados: Aquí se ubican los virus, las bombas lógicas, los gusanos, accesos no autorizados, etc. Se trata, en general, de programas o acciones que de una u otra forma dañan la información de un sistema determinado.

---

[1] CASABONA Romeo, Carlos María, Poder informático y Seguridad jurídica, Editorial Fundesco 1987

[2] BELTRAMONE G, HERRERA R, ZABALE E, Nociones básicas sobre los Delitos Informáticos

Lección 4. Tipos de delito informático

Desde los albores de la humanidad, el hombre ha ido creando una larga serie de normas tendientes a regular la convivencia en sociedad para defenderse de quienes intentan burlar la ley, el derecho, a través de sus operadores en los diferentes campos, fue delineando diferentes soluciones y así surgieron, entre otras, la figura de las presunciones, aquellas que no admiten prueba en contrario, etc.

Tales soluciones han producido excelentes resultados en áreas como las del Derecho Civil, Comercial o Laboral; pero son de imposible aplicación en el Derecho Penal dado que, según lo establecen los modernos ordenamientos jurídicos, lo que no está prohibido está permitido impidiendo a la misma ley, de este modo, recurrir a la analogía, a la presunción de derecho o al fraude a la ley.[3]

Tradicionalmente se ha caracterizado al delito informático como aquél que está íntimamente ligado no sólo a la informática sino también a los bienes jurídicos relacionados con las tecnologías de la información: datos, programas, documentos electrónicos, dinero electrónico, información.
A continuación se presentan las más modernas conductas delictivas que son entendidas como delitos informáticos.[2]

Hacking

Se denomina “hacking” en la jerga informática a la conducta de entrar a un sistema de información sin autorización, es decir violando las barreras de protección establecidas a tal fin. El sujeto que realiza esta actividad es llamado hackers, muy rara vez se conoce su nombre verdadero y en mucho casos actúa y firma en grupo. La actividad de hackear un sistema puede tener diferentes

[3] BELTRAMONE Guillermo, Nociones básicas sobre los Delitos Informáticos

finalidades y alcances. Así, en la mayoría de los casos el romper el sistema o eliminar los pasos de seguridad de un sistema tiene por objeto ver, fisgonear el contenido y la información protegida o extraer copias de la información o destruirla.

Cracking

Cambiar los contenidos de la información que tienen por objeto destruir el sistema, a esto se llama cracking y a los sujetos que lo realizan se los identifica como crackers. Esta es una expresión idiomática que se puede traducir como quebrar, es decir vencer las barreras de seguridad y romper lo que hay detrás de ellas.

En cualquiera de ambos casos, lo que caracteriza las andanzas de los sujetos es su entrada ilegal al sistema, entendiendo el concepto de entrada ilegal como la entrada de toda aquella persona que no tiene los password o no los ha conseguido por los caminos normales.

Phreaking

La actividad de phreaking es, sin duda, la más común de todas las llamadas actividades ilícitas informáticas, es la actividad de obtener ventajas de las líneas telefónicas a los efectos de no pagar los costos de comunicación. Es decir que básicamente se trata de encontrar el medio para evitar pagar por el uso de la red telefónica ya sea ésta pública o privada, digital o inalámbrica.

Carding

Se llama carding a la actividad de cometer un fraude o una estafa con un número de tarjeta de crédito, tarjetas telefónicas caseras que tienen la capacidad de recargarse, puede verse www.islatortuga.com

Este concepto que parece simple tiene sus dificultades. Primero no todo fraude con tarjeta de crédito se transforma en carding, así si se roba o se encuentra una tarjeta y es utilizada por otra persona que no es su titular, ello no es carding es solo un fraude. El carding consiste entonces en usar un número de tarjeta de crédito ya sea real o creado de la nada mediante procedimientos digitales para realizar compras a distancia por Internet y efectuar pagos.

Lección 5. Ley 1273 de 2009 Protección de la Información y de los Datos en Colombia.

En Colombia existe la ley 1273 con la cual se modifico el código penal y se incluyo en lo relacionado al delito informático, para tener un mejor conocimiento de la ley esta se muestra exacta tal y como se rige:

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.

EL CONGRESO DE COLOMBIA

DECRETA:

Artículo 1o. Adiciónase el Código Penal con un Título VII BIS denominado “De la Protección de la información y de los datos”, del siguiente tenor:

CAPÍTULO I

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos

dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 269H: Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

- Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
- Por servidor público en ejercicio de sus funciones.
- Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
- Revelando o dando a conocer el contenido de la información en perjuicio de otro.
- Obteniendo provecho para sí o para un tercero.
- Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
- Utilizando como instrumento a un tercero de buena fe.

Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

CAPÍTULO II

De los atentados informáticos y otras infracciones

Artículo 269I: Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Artículo 269J: Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en

pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

CAPITULO 2. FASES DE LA INFORMÁTICA FORENSE.

Lección 6. Descripción de las fases de la Informática Forense.

Considerando la fragilidad del insumo con el cual trabajan los especialistas en informática forense, es preciso extremar las medidas de seguridad y control que éstos deben tener a la hora de adelantar sus labores, pues cualquier imprecisión en las mismas puede llevar a comprometer el proceso bien sea legal u organizacional [wilson 2003, taylor, r., caeti, t., kall loper, d., fritsch, e y liederbach, j. 2006]. En este sentido, se detalla de manera básica algunos elementos que deben ser considerados para mantener la idoneidad del procedimiento forense adelantado:[4]

Los procedimientos llevados a cabo se dividen en las siguientes etapas:

Identificación

Estando en el lugar de la escena donde se realizó el ataque informático se debe rotular con sus respectivas características físicas el elemento que va ser objeto del análisis forense, para preservar el elemento que puede ser desde un disquette o

[4] CANO JEIMY J . Phd. CFE Introducción a la informática forense

un disco rígido de un computador hasta un conjunto de discos de un servidor, un juego de cintas, o varias computadoras de una organización.

Validación y preservación de los datos adquiridos

Con el elemento identificado se procede a realizar una imagen exacta del contenido de la evidencia asignando un código único correspondiente a una combinación única de bytes que constituye la totalidad del medio en observación. Este código de validación ha de ser lo suficientemente complejo como para evitar vulneraciones en la información rescatada e impedir que cualquier auditor pueda por su cuenta verificar la autenticidad de la imagen tomada, es decir, crear un código que solamente personal calificado y legalmente autorizado pueda manipular para proteger el elemento a ser analizado; esto con el fin de establecer una cadena de custodia consistente. Desde este momento ya se pueden efectuar copias exactamente iguales de la imagen a los efectos de que diferentes actores puedan conservar una copia de seguridad.

Análisis y descubrimiento de evidencia

Se procede a realizar una colección de pruebas en el laboratorio sobre la copia validada. Es posible analizar y buscar información a muchos niveles.

El punto de partida del análisis comienza al detectar una tipo de ataque informático o la sospecha de manipulación no autorizada de información. Una actividad ilícita reportada puede ser el borrado la información que puede comprometer a una persona o información que pudo haber sido ocultada o almacenada en medios no convencionales como disquetes, cd rom, dvd rom, flash drive. El análisis forense está orientado por un caso en particular y aquí es necesaria la información que provee quien solicita la investigación forense.

En el análisis forense se pueden buscar: archivos borrados, archivos creados, accedidos o modificados dentro de determinado rango de fechas, tipos de archivos con un formato particular que hayan sido alterados, por ejemplo archivos de un sistema de contabilidad renombrados como archivos de un procesador de texto, imágenes, mensajes de correo electrónico, actividad desarrollada en internet, a diferentes niveles palabras claves tales como un número telefónico, el nombre de una ciudad o una empresa, etc.

En base a este análisis se determina un patrón de comportamiento del usuario en cuanto a la creación, modificación y borrado de mensajes, actividad de correo electrónico, etc.

Informe

Se presenta un informe escrito en un lenguaje a la vez técnico y claro y un Cd donde se hace accesible al usuario no especializado de una forma ordenada la evidencia recuperada y su interpretación.

Aunque a menudo se subestima la importancia de los pasos 1 y 2 y se considera el paso 3 el específico de la informática forense, hay que tener en cuenta que la evidencia informática es por definición frágil y puede ser alterada haciendo que la misma pierda su validez frente a un tribunal.

Lección 7. Fase de Identificación[5]

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:

[5] PINZON OLMEDO Fredy Bolivar, La Informática Forense, Universidad católica de Loja

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

La identificación debe prever los desafíos que se pasaran durante los procesos de las fases de preservación y extracción. Esta fase culmina con un Plan a seguir.

Etapa 1: Levantamiento de información inicial para el Análisis Forense

La solicitud forense es un documento donde el administrador del equipo afectado notifica de la ejecución de un incidente y para ello solicita al equipo de seguridad la revisión del mismo, donde incluye toda la información necesaria para dar inicio al proceso de análisis. La información incluida en el documento debe ser la siguiente:

Descripción Del Delito Informático

- Fecha del incidente
- Duración del incidente
- Detalles del incidente

Información General

- Área
- Nombre de la dependencia
- Responsable del sistema afectado
- Nombres y Apellidos
- Cargo
- E-mail

- Teléfono
- Extensión
- Celular
- Fax

Información Sobre El Equipo Afectado

- Dirección IP
- Nombre del equipo
- Marca y modelo
- Capacidad de la RAM
- Capacidad del disco duro
- Modelo del procesador
- Sistema operativo (nombre y versión)
- Función del equipo
- Tipo de información procesada por el equipo
- Toda la información del incidente, la evidencia digital, copias o imágenes de la escena del crimen.

Reconocer un incidente mediante indicadores y determinar su tipo. Esto no esta incluido dentro del análisis forense, pero es significativo en los siguientes pasos. Esta fase esta dividida en dos procesos iníciales que son:

Etapa 2: Asegurar la escena

Para asegurar que tanto los procesos como las herramientas a utilizar sean las más idóneas se debe contar con un personal idóneo a quien se le pueda asignar la conducción del proceso forense, para ello el equipo de seguridad debe estar capacitado y entender a fondo la metodología.

Identificar las evidencias

El siguiente paso y muy importante es la identificación de la evidencia presentada en nuestra escena del "crimen", la misma que estará sujeta a todos los procesos necesarios para la presentación de resultados finales, la evidencia se clasificara según:

- Tipo de dispositivo

A las evidencias también se las puede clasificar según el tipo de dispositivo donde se encuentran:

- Sistemas informáticos
- Redes
- Redes Inalámbricas
- Dispositivos móviles
- Sistemas embebidos
- Otros dispositivos

- Modo de almacenamiento

A las evidencias también se las clasifica según el medio de almacenamiento. Como pueden ser:

- Volátiles: Aquellas que se perderán al apagar el equipo como la hora del sistema y desfase de horario, contenido de la memoria, procesos en ejecución, programas en ejecución, usuarios conectados, configuración de red, conexiones activas, puertos abiertos, etc.
- No volátiles: medios físicos de almacenamiento como memorias flash, CD, discos duros.

El primer proceso del análisis forense comprende la identificación, búsqueda y recopilación de evidencias, se debe identificar qué cosas pueden ser evidencias, dónde y cómo están almacenadas, qué sistema operativo se está utilizando. A partir de estos pasos, el equipo forense puede identificar los procesos para la recuperación de evidencias adecuadas, así como las herramientas a utilizar.

Lección 8. Fase de Validación y preservación. [6]

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:

Etapa 1: Copias de la evidencia.

Como primer paso se debe realizar dos copias de las evidencias obtenidas, generar también una suma de comprobación de la integridad de cada copia mediante el empleo de funciones hash tales como MD5 o SHA1. Incluir estas firmas en la etiqueta de cada copia de la evidencia sobre el propio medio de almacenamiento como CD o DVD etiquetando la fecha y hora de creación de la copia, nombre cada copia, por ejemplo “Copia A”, “Copia B” para distinguirlas claramente del original.

[6] PINZON OLMEDO Fredy Bolivar, La Informática Forense, Universidad católica de Loja

Si además se extrae los discos duros del sistema para utilizarlos como evidencia, se debe seguir el mismo procedimiento, colocando sobre ellos la etiqueta "Evidencia Original", incluir además las correspondientes sumas hash, fecha y hora de la extracción del equipo, datos de la persona que realizó la operación, fecha, hora y lugar donde se almacenó por ejemplo en una caja fuerte.

Tener en cuenta que existen factores externos como cambios bruscos de temperatura o campos electromagnéticos que pueden alterar la evidencia. Toda precaución es poca, incluso si decide enviar esos discos a que sean analizados por empresas especializadas.

Etapa 2: Cadena de custodia

Otro aspecto muy importante es la cadena de custodia, donde se establecen las responsabilidades y controles de cada una de las personas que manipulen la evidencia. Se debe preparar un documento en el que se registren los datos personales de todos los implicados en el proceso de manipulación de las copias, desde que se tomaron hasta su almacenamiento. El documento debe contener la siguiente información:

- Dónde, cuándo y quién examinó la evidencia, incluyendo su nombre, su cargo, un número de identificación, fechas y horas, etc.
- Quién estuvo custodiando la evidencia, durante cuanto tiempo y dónde se almacenó.
- Cuando se cambie la custodia de la evidencia también se deberá documentar cuándo y como se produjo la transferencia y quién la transportó.

Todas estas medidas harán que el acceso a la evidencia sea muy restrictivo quedando claramente documentado, posibilitando detectar y pedir responsabilidades ante manipulaciones incorrectas, intentos de acceso no

autorizados o que algún otro dispositivo electromagnético se use dentro de un determinado radio.

Lección 9. Fase de Análisis[7]

Antes de iniciar esta fase se deben preparar 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, iniciamos 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. 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.

Etapa 1: Preparación para el análisis

Antes de comenzar el análisis de las evidencias se deberá:

- Acondicionar un entorno de trabajo adecuado al estudio que se desea realizar.

[7] PINZON OLMEDO Fredy Bolivar, La Informática Forense, Universidad católica de Loja

- Trabajar con las imágenes que se recopiló como evidencias, o mejor aún con una copia de éstas, tener en cuenta que es necesario montar las imágenes tal cual estaban en el sistema comprometido.
- Si dispone de recursos suficientes preparar dos estaciones de trabajo, una de ellas contendrá al menos dos discos duros.
- Instalar un sistema operativo que actuará de anfitrión y que servirá para realizar el estudio de las evidencias. En este mismo computador y sobre un segundo disco duro, instalar las imágenes manteniendo la estructura de particiones y del sistema de archivos tal y como estaban en el equipo atacado.
- En otro equipo instalar un sistema operativo configurado exactamente igual que el equipo atacado, además mantener nuevamente la misma estructura de particiones y ficheros en sus discos duros. La idea es utilizar este segundo ordenador como "conejillo de Indias" y realizar sobre él pruebas y verificaciones conforme se vayan surgiendo hipótesis sobre el ataque.

Si no se dispone de estos recursos, se puede utilizar software como VMware[8], que permitirá crear una plataforma de trabajo con varias máquinas virtuales. También se puede utilizar una versión LIVE de sistemas operativos como Caine[9], que permitirá interactuar con las imágenes montadas pero sin modificarlas. Si se está muy seguro de las posibilidades y de lo que va a hacer, se puede conectar los discos duros originales del sistema atacado a una estación de trabajo independiente para intentar hacer un análisis en caliente del sistema, se deberá tomar la precaución de montar los dispositivos en modo sólo lectura, esto se puede hacer con sistemas anfitriones UNIX/Linux, pero no con entornos Windows.

[8] VMware es un programa propietario que permite montar maquinas virtuales que recrean el sistema operativo donde estaba instalado el disco duro atacado.
[9] Caine es un software libre montado en Ubuntu que permite realizar una análisis forense por la gran cantidad de herramientas que posee

Etapa 2: Reconstrucción del ataque

Si ya se tienen montadas las imágenes del sistema atacado en una estación de trabajo independiente y con un sistema operativo anfitrión de confianza, se procede con la ejecución de los siguientes pasos:

- Crear una línea temporal o timeline de sucesos, para ello se debe recopilar la siguiente información sobre los ficheros:

- Marcas de tiempo MACD (fecha y hora de modificación, acceso, creación y borrado).
- Ruta completa.
- Tamaño en bytes y tipo de fichero.
- Usuarios y grupos a quien pertenece.
- Permisos de acceso.
- Si fue borrado o no.

Sin duda esta será la información que más tiempo llevará recopilar, pero será el punto de partida para el análisis, podría plantearse aquí el dedicar un poco de tiempo a preparar un script que automatizase el proceso de creación del timeline, empleando los comandos que proporciona el sistema operativo y las herramientas utilizadas.

- Ordenar los archivos por sus fechas MAC, esta primera comprobación, aunque simple, es muy interesante pues la mayoría de los archivos tendrán la fecha de instalación del sistema operativo, por lo que un sistema que se instaló hace meses y que fue comprometido recientemente presentará en los ficheros nuevos, fechas MAC muy distintas a las de los ficheros más antiguos.

La idea es buscar ficheros y directorios que han sido creados, modificados o borrados recientemente o instalaciones de programas posteriores a la del sistema operativo y que además se encuentren en rutas poco comunes. Pensar que la mayoría de los atacantes y sus herramientas crearán directorios y descargarán sus "aplicaciones" en lugares donde no se suele mirar, como por ejemplo en los directorios temporales.

A modo de guía centrarse en la siguiente búsqueda:

- los archivos de sistema modificados tras la instalación del sistema operativo.
- averiguar la ubicación de los archivos ocultos, de qué tipo son
- identificar también los archivos borrados o fragmentos de éstos, pues pueden ser restos de logs y registros borrados por los atacantes, destacar la importancia de realizar imágenes de los discos pues se puede acceder al espacio residual que hay detrás de cada archivo, (recordar que los ficheros suelen almacenarse por bloques cuyo tamaño de clúster depende del tipo de sistema de archivos que se emplee), y leer en zonas que el sistema operativo no ve.
- Pensar que está buscando "una aguja en un pajar", por lo que se deberá ser metódico, ir de lo general a lo particular, por ejemplo partir de los archivos borrados, intentar recuperar su contenido, anotar su fecha de borrado y compararla con la actividad del resto de los archivos, puede que en esos momentos se estuviesen dando los primeros pasos del ataque.
- Comenzar a examinar con más detalle los ficheros logs y registros que se examinaron durante la búsqueda de indicios del ataque, intentar buscar una correlación temporal entre eventos. Pensar que los archivos log y de registro son generados de forma automática por el propio sistema operativo o por aplicaciones específicas, conteniendo datos sobre accesos al equipo, errores de inicialización, creación o modificación de usuarios, estado del sistema, etc. Por lo que tendrá que buscar entradas extrañas y compararlas

con la actividad de los ficheros. Editar también el archivo de contraseñas y buscar la creación de usuarios y cuentas extrañas sobre la hora que considere se inició el ataque del sistema.

Etapa 3: Determinación del ataque

Una vez obtenida la cadena de acontecimientos que se han producido, se deberá determinar cuál fue la vía de entrada al sistema, averiguando qué vulnerabilidad o fallo de administración causó el agujero de seguridad y que herramientas utilizó el atacante para aprovecharse de tal brecha.

Estos datos, al igual que en el caso anterior, se deberán obtener de forma metódica, empleando una combinación de consultas a archivos de logs, registros, claves, cuentas de usuarios. El siguiente proceso permitirá conocer que acciones realizo el atacante:

- Revisar los servicios y procesos abiertos que se recopilaron como evidencia volátil, así como los puertos TCP/UDP y conexiones que estaban abiertas cuando el sistema estaba aún funcionando. Examinar con más detalle aquellas circunstancias que resultan sospechosas cuando se buscó indicios sobre el ataque, y realizar una búsqueda de vulnerabilidades a través de Internet, emplear Google o utilizar páginas específicas donde se encuentran perfectamente documentadas ciertas vulnerabilidades.
- Si ya se tiene claro cuál fue la vulnerabilidad que dejó el sistema desprotegido, es necesario ir un paso más allá y buscar en Internet algún exploits[10] anterior a la fecha del incidente, que utilice esa vulnerabilidad. Generalmente se encontrará en forma de rootkit[11] y un buen lugar donde

[10] Exploit (del inglés *to exploit*, explotar, aprovechar) es el nombre con el que se identifica un programa informático malicioso, o parte del programa, que trata de forzar alguna deficiencia o vulnerabilidad de otro programa.
[11] Rootkit es un conjunto de herramientas usadas frecuentemente por los intrusos informáticos o crackers que consiguen acceder ilícitamente a un sistema informático.

comenzar la búsqueda es, nuevamente, Google aunque también será de utilidad utilizar la información presentado en la corrección de vulnerabilidades sobre reporte de vulnerabilidades así como la siguiente dirección: http://www.packetstormsecurity.org

- Reforzar cada una de las hipótesis empleando una formulación causa - efecto, también es el momento de arrancar y comenzar a utilizar la máquina preparada como "conejillo de Indias". Probar sobre la máquina los exploits[9] que se encontró, recordar que en el análisis forense un antecedente es que los hechos han de ser reproducibles y sus resultados verificables, por lo tanto comprobar si la ejecución de este exploit[9] sobre una máquina igual que la afectada, genere los mismos eventos que ha encontrado entre sus evidencias.

Etapa 4: Identificación del atacante.

Si ya se logro averiguar cómo entraron en el sistema, es hora de saber quién o quiénes lo hicieron. Para este propósito será de utilidad consultar nuevamente algunas evidencias volátiles que se recopiló en las primeras fases, revisar las conexiones que estaban abiertas, en qué puertos y qué direcciones IP las solicitaron, además buscar entre las entradas a los logs de conexiones. También se puede indagar entre los archivos borrados que se recuperó por si el atacante eliminó alguna huella que quedaba en ellos.

Si se tiene pensado llevar a cabo acciones legales o investigaciones internas, debe realizar este proceso caso contrario se debe saltar y empezar con la recuperación completa del sistema atacado y mejorar su seguridad. Pero si se decide perseguir a los atacantes, se deberá:

- Realizar algunas investigaciones como parte del proceso de identificación. Primero intentar averiguar la dirección IP del atacante, para ello revisar con detenimiento los registros de conexiones de red y los procesos y servicios

que se encontraban a la escucha. También se podría encontrar esta información en fragmentos de las evidencias volátiles, la memoria virtual o archivos temporales y borrados, como restos de email, conexiones fallidas entre otros.

- Al tener una IP sospechosa, comprobarla en el registro Ripe Ncc (www.ripe.net)[12] o la Icann[13] a quién pertenece. Pero, no sacar conclusiones prematuras, muchos atacantes falsifican la dirección IP con técnicas de spoofing[14]. Otra técnica de ataque habitual consiste en utilizar "ordenadores zombis", éstos son comprometidos en primera instancia por el atacante y posteriormente son utilizados para realizar el ataque final sin que sus propietarios sepan que están siendo cómplices de tal hecho. Por ello, para identificar al atacante se tendrá que verificar y validar la dirección IP obtenida.
- Utilizar técnicas hacker pero solo de forma ética, para identificar al atacante, por si el atacante dejó en el equipo afectado una puerta trasera o un troyano, está claro que en el equipo del atacante deberán estar a la escucha esos programas y en los puertos correspondientes, bien esperando noticias o buscando nuevas víctimas.

Si se procede de esta forma, se puede usar una de las herramientas como nmap[15], para determinar qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones) ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando y así muchas mas características que poseen los equipos.

[12] El Centro de Coordinación de redes IP europeas (Réseaux IP Européens Network Coordination Centre (RIPE NCC)) es el Registro Regional de Internet (RIR) para Europa, Oriente Medio y partes de Asia Central.
[13] ICANN se fundó en 1998 como asociación sin ánimo de lucro y en ella se reúnen personas de todo el mundo cuyo objetivo es asegurar que Internet sea segura, estable e interoperativa. Esta asociación promueve la competencia y desarrolla políticas de identificadores únicos de Internet
[14] spoofing se conoce a la creación de tramas TCP/IP utilizando una dirección IP falsa
[15] Nmap es un programa de código abierto que sirve para efectuar rastreo de puertos

Etapa 5: Perfil del atacante

Otro aspecto muy importante es el perfil de los atacantes y sin entrar en muchos detalles se podrá encontrar los siguientes tipos:

Hackers: Son los más populares y se trata de personas con conocimientos en técnicas de programación, redes, Internet y sistemas operativos. Sus ataques suelen tener motivaciones de tipo ideológico (pacifistas, cologistas, anti globalización, anti Microsoft entre otros.) o simplemente lo consideran como un desafío intelectual.

SciptKiddies: Son una nueva especie de delincuentes informáticos. Se trata de jóvenes que con unos conocimientos aceptables en Internet y programación emplean herramientas ya fabricadas por otros para realizar ataques y ver que pasa. Su nombre viene de su corta edad y del uso de los scripts, guías de ataques que encuentran por Internet.

Profesionales: Son personas con muchísimos conocimientos en lenguajes de programación, en redes y su equipamiento (routers, firewall, etc.), Internet y sistemas operativos tipo UNIX. Suelen realizar los ataques bajo encargo, por lo que su forma de trabajar implica una exhaustiva preparación del mismo, realizando un estudio meticuloso de todo el proceso que llevará a cabo, recopilando toda la información posible sobre sus objetivos, se posicionará estratégicamente cerca de ellos, realizará un tanteo con ataques en los que no modificará nada ni dejará huellas cuando lo tenga todo bien atado entonces atacará, este tipo de atacantes se encuentra muy poco y además se dedica a dar grandes golpes.

Etapa 6: Evaluación del impacto causado al sistema

Para poder evaluar el impacto causado al sistema, el análisis forense ofrece la posibilidad de investigar qué es lo que han hecho los atacantes una vez que accedieron al sistema. Esto permitirá evaluar el compromiso de los equipos y realizar una estimación del impacto causado. Generalmente se pueden dar dos tipos de ataques:

Ataques pasivos: En los que no se altera la información ni la operación normal de los sistemas, limitándose el atacante a fisgonear por ellos.

Ataques activos: En los que se altera y en ocasiones seriamente tanto la información como la capacidad de operación del sistema.

Se deberá tener en cuanta, además otros aspectos del ataque como los efectos negativos de tipo técnico que ha causado el incidente, tanto inmediatos como potenciales además de lo crítico que eran los sistemas atacados, por ejemplo ataques al cortafuegos, el router de conexión a Internet o Intranet, el servidor Web, los servidores de bases de datos, tendrán diferente repercusión según el tipo de servicio que presta la Universidad y las relaciones de dependencia entre los usuarios.

Lección 10. Fase de Documentación y Presentación de las pruebas[16]

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.

[16] PINZON OLMEDO Fredy Bolivar, La Informática Forense, Universidad católica de Loja

Etapa 1: Utilización de formularios de registro del incidente

Es importante que durante el proceso de análisis se mantenga informados a los administradores de los equipos y que tras la resolución del incidente se presenten los informes Técnico y Ejecutivo. El empleo de formularios puede ayudarle bastante en este propósito, estos deberán ser rellenados por los departamentos afectados o por el administrador de los equipos. Alguno de los formularios que debería preparar serán:

- Documento de custodia de la evidencia
- Formulario de identificación de equipos y componentes
- Formulario de incidencias tipificadas
- Formulario de publicación del incidente
- Formulario de recogida de evidencias
- Formulario de discos duros.

Etapa 2: Informe Técnico

Este informe consiste en una exposición detallada del análisis efectuado. Deberá describir en profundidad la metodología, técnicas y hallazgos del equipo forense. A modo de orientación, deberá contener, al menos, los siguientes puntos:

- Introducción
- Antecedentes del incidente
- Recolección de los datos
- Descripción de la evidencia
- Entorno del análisis
- Descripción de las herramientas
- Análisis de la evidencia
- Información del sistema analizado
- Características del SO
- Aplicaciones

- Servicios
- Vulnerabilidades
- Metodología
- Descripción de los hallazgos
- Huellas de la intrusión
- Herramientas usadas por el atacante
- Alcance de la intrusión
- El origen del ataque
- Cronología de la intrusión
- Conclusiones
- Recomendaciones específicas
- Referencias
- Anexos

Etapa 3: Informe Ejecutivo

Este informe consiste en un resumen del análisis efectuado pero empleando una explicación no técnica, con lenguaje común, en el que se expondrá los hechos más destacables de lo ocurrido en el sistema analizado. Constará de pocas páginas, entre tres y cinco, y será de especial interés para exponer lo sucedido al personal no especializado en sistemas informáticos, como pueda ser el departamento de Recursos Humanos, Administración e incluso algunos directivos. En este informe constara lo siguiente:

- Introducción: Descripción del objetivo del análisis del sistema previamente atacado y comprometido, también se incluye la información de la evidencia proporcionada.
- Análisis: Descripción del entorno de trabajo y de las herramientas de análisis forense seleccionadas así como la cantidad de tiempo empleado en el mismo.

- Sumario del incidente: Resumen del incidente tras el análisis de la evidencia aportada.
- Principales Conclusiones del análisis: Detalle de las conclusiones a las que se llego una vez terminado el proceso de análisis.
- Solución al incidente: Descripción de la solución para recuperación del incidente.
- Recomendaciones finales: pasos que se deben realizar para garantizar la seguridad de los equipos y que el incidente no vuelva a suceder.

CAPITULO 3. ACCIONES EN LA ESCENA DEL FRAUDE INFORMATICO[17]

Lección 11. Identificando las vulnerabilidades informáticas.

En el consenso general entre los expertos en seguridad informática la gran mayoría de los delitos informáticos no están detectados o reportados, esto se debe a que muchos delitos informáticos no son fácilmente detectados, ya que si un individuo roba información de un computador , el intruso hará una copia de la información y los datos originales permanecen sin alteraciones en el computador y siguen siendo accesibles para el propietario, por ello es importante identificar ciertas vulnerabilidades informáticas como:

- Los empleados hacen mal uso de los sistemas por ejemplo, violaciones de las políticas de uso de Internet
- Código malicioso por ejemplo, virus, los gusanos o troyanos.
- Las intrusiones o piratería: Monitoreo electrónico no autorizado (sniffers, eyloggers,)
- Web site falsas o vandalismo

[17] Incident Response, Computer Forensics Toolkit, Douglas Schweitzer

- El acceso no autorizado a información confidencial
- Las herramientas automatizadas de escaneo
- Sabotaje ejecutivo a través de espionaje o empleados descontentos.

Lección 12. Preservar la escena del Fraude.

Identificado la posible causa del fraude informático se considera necesario cuidar los dispositivos que contienen la evidencia del ataque por lo cual se hace necesario preservar los elementos en el momento de hacer el análisis forense en la o las máquinas atacadas, cuidando los procedimientos a realizar con los equipos para evitar alteraciones de la siguiente manera:

Aislamiento del sistema informático.

Para que las evidencias no se pierdan es de suma importancia aislar la maquina afectada junto con todos los medios de almacenamiento encontrados, además, de las notas escritas a mano y los documentos que se encuentran en las proximidades del equipo en cuestión, estos elementos pueden ser de valiosa información para el curso de la investigación forense, los elementos que se debe proteger son los cd - dv - roms, medios de almacenamiento en cinta, discos duros adicionales, disquetes y flash drive que se encuentren en el área del computador, los cuales también deben estar aislados y protegidos. A continuación se sugieren las siguientes acciones:

- El acceso a estos elementos debe ser completamente restringido, incluyendo especialmente a la persona sospechosa de cometer la violación siempre debe estar alejada del equipo
- No se debe permitir el contacto con los medios de almacenamiento o el computador implicado en el incidente de seguridad ya que individuos con extensa experiencia pueden destruir todos los datos magnéticos en un disco duro.

Procedimiento de apagado para preservar la evidencia.

Tener en cuenta el apagado del sistema informático de manera que no dañe la integridad de los archivos existentes, es un procedimiento de seguridad informática complicado, ya que al apagar el sistema puede omitir archivos que estén en los dispositivos volátiles, en este caso se debe documentar el estado inicial de la máquina reportada y proceder a apagar la máquina sin modificar ningún archivo o ejecutar programa alguno.

La simple visualización de un archivo o la manipulación equivocada de un medio de comunicación del equipo atacado darían lugar a una alteración de la información y en estos casos en un litigio legal ya no sería evidencia original y puede ser inadmisible en cualquier actuación jurídica o administrativa.

Cuando se abre un archivo se altera la fecha y hora del último acceso, esto puede no parecer una cuestión importante, sin embargo, más tarde podría llegar a ser muy importante en la determinación de quién cometió la violación y cuando ocurrió.

El aislamiento del sistema informático es lo ideal, pero si esto no puede llevarse a cabo debido a los requisitos de funcionamiento, no se debe intentar recuperar o ver los archivos.

Inspeccionar el sistema operativo

De acuerdo al tipo de sistema operativo que una empresa utiliza se dictan las normas de apagado de las máquinas computaciones y también la forma en como se conectan los computadores a la fuente de energía, sea por circuitos eléctricos compartidos, fuentes de poder reguladas o sistemas eléctricos protegidos. Con algunos sistemas operativos, se hace necesario extremar el suministro continuo de energía para evitar caídas del sistema operativo. En la escena del fraude

informático se debe verificar este tipo de conexiones observando como los cables de conexión suministran la corriente al equipo afectado ya que usualmente los delincuentes informáticos desconectan abruptamente la fuente de energía pretendiendo con esta acción que el sistema operativo pierda su secuencia de arranque y se destruyan los archivos de registro de inicio de sesión y de programas que se estén ejecutando en el instante del delito y en raras ocasiones querer un daño en el disco duro.

A continuación se mencionan algunas características de los sistemas operativos más comunes, se menciona el procedimiento para su cierre:

Sistema Operativo Ms – Dos

- Características
    - El texto es sobre un fondo sólido (generalmente negro).
    - El mensaje contiene una letra de unidad y utiliza las barras contrarias.
    - El indicador por lo general termina con un signo mayor que (>).
- Procedimientos de cierre
    - Fotografiar la pantalla y anotar los programas en ejecución.
    - Retire el cable de alimentación de la pared.

Sistema Operativo Windows 3.X

- Características
    - Barra de titulos de colores
    - Menú estándar de opciones
- Procedimientos de cierre
    - Fotografiar la pantalla y anotar los programas en ejecución.
    - Retire el cable de alimentación de la pared.

Sistema Operativo Windows NT 3.51

- Características
  - Barra de titulo de colores
  - Menú estándar de opciones
  - Los iconos representan equipos de red y personas
- Procedimientos de cierre
  - Fotografiar la pantalla y anotar los programas en ejecución.
  - Retire cable de alimentación de la pared

Sistema Operativo Windows 95/98/NT 4.0/2000

- Características
  - El botón de inicio tiene un símbolo de Windows.
- Procedimientos de cierre
  - Fotografiar la pantalla y anotar los programas en ejecución.
  - Retire cable de alimentación de la pared

Sistema Operativo Unix / Linux

- Características
  - El botón de inicio tiene un símbolo de la versión Unix / Linux
- Procedimientos de cierre
  - Fotografiar la pantalla y anotar los programas en ejecución.
  - Haga clic derecho en el menú.
  - Desde el menú, haga clic en Consola.
  - Verificar el indicador de usuario root #. Si no está presente, cambie al usuario root (teclee su -). En ese momento se le pedirá la contraseña de root. Si la contraseña está disponible, entrar en él. En el signo #, teclear sync; sync; halt y el sistema se apagará. Si no tienen la contraseña de root, tire del cable de alimentación de la pared.
  - Si el signo # se muestra en la consola, escriba el tipo de identificación pulse Intro. Si usted ve que su ID de usuario es root,

teclear sync; sync; halt y pulse Enter. Esto apagará el sistema. Si el ID de usuario no es root, tire del cable de alimentación de la pared.

Sistema Operativo Mac OS

- Características
  - Posee un símbolo de Apple en la esquina superior izquierda.
  - Pequeñas líneas horizontales en las barras de menú de las ventanas
  - Un solo botón sencillo en cada esquina de la ventana
  - Icono de Papelera
- Procedimientos de cierre
  - Fotografiar la pantalla y anotar los programas en ejecución.
  - Registre el tiempo desde la barra de menú
  - Haga clic en Especial.
  - Haga clic en Cerrar.
  - En la ventana dice que es seguro apagar el equipo.
  - Retire el cable de alimentación de la pared.

Lección 13. Claridad de la evidencia.

La evidencia digital es información de valor probatorio constituida por campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales. Abarca cualquier información en formato digital que pueda establecer una relación entre un delito y su autor.

Para ser valorada como tal, el proceso de recolección de la misma debe ser avalado por las leyes propias del lugar y debe ser reconocida como evidencia por una entidad oficial. La evidencia digital hace parte de la evidencia física, pero tiene como características propias que puede ser duplicada y copiada sin alteraciones respecto a la original. Desde el punto de vista del derecho probatorio, puede ser

comparable con "un documento" como prueba legal. Con el fin de garantizar su validez probatoria, debe reunir las siguientes características:[18]

Autenticidad

Garantizar que sus contenidos no han sido modificados; que la información proviene de la fuente identificada y que la información externa a ella es precisa.

Precisión

Debe ser posible relacionarla positivamente con el incidente. Los procedimientos seguidos y las herramientas utilizadas para su recolección, manejo, análisis y posterior presentación en una corte deben ser confiables. Adicionalmente, debe haber alguien que pueda explicar cómo fueron realizados los procedimientos y con qué tipo de herramientas se llevaron a cabo.

Suficiencia

Debe, por sí misma y en sus propios términos, mostrar el escenario completo, y no una perspectiva de un conjunto particular de circunstancias o eventos.

Con el fin de garantizar la validez de la evidencia digital manejada en una investigación judicial, La organización Internacional de Evidencia Computacional IOCE[19], por sus siglas en inglés, definió cinco principios para la recuperación, preservación y posterior análisis de la misma, mostradas a continuación:

- En la incautación de la evidencia digital, las acciones tomadas no deben cambiar la evidencia.

[18] Tomado de http://bdigital.eafit.edu.co/PROYECTO/P005.42CDB562/marcoTeorico.pdf
[19] International Organizatiion on Computer Evidence

- Cuando es necesario para una persona acceder a la evidencia digital original, esa persona debe ser competente en ciencias forenses.
- Toda actividad relacionada con la incautación, acceso, almacenamiento o transferencia de evidencia digital tiene que estar completamente documentada, preservada y disponible para revisión.
- Todo individuo es responsable de todas las acciones tomadas con respecto a la evidencia digital mientras ésta esté en su posesión.
- Cualquier organización que es responsable de incautar, acceder, almacenar o transferir evidencia digital es responsable de actuar conforme a estos principios.

Además, la IOCE definió que los principios de la evidencia digital debían estar regidos por los siguientes atributos:

- Consistencia con todos los sistemas legales.
- Permitir el uso de un lenguaje común.
- Durabilidad.
- Habilidad para cruzar límites internacionales.
- Habilidad para infundir confianza en la integridad de la evidencia.
- Aplicabilidad a toda la evidencia forense.
- Aplicabilidad en todos los niveles, incluido el individuo, la organización y el país.

Los principios fueron presentados y aprobados en la Conferencia Forense Internacional de crimen de alta tecnología, en octubre de 1999.

Lección 14. Formato de la evidencia en la escena.

Un formato de archivo es una forma específica de codificar datos digitales que van de acuerdo al programa donde fue diseñado (hoja de calculo, procesadores de texto, base de datos o diseñadores gráficos entre otros) El formato de un archivo

es necesarios para ser identificado dentro de un máquina computacional, ya que de acuerdo a su formato se podrá almacenar, manipular y borrar.

El tipo de archivo más común es el de texto. De éste, el más simple y útil es el texto plano, que consiste únicamente en los códigos binarios de los caracteres legibles (como las letras de un alfabeto, los números y los signos de puntuación) y los de un grupo de caracteres de control. Una de las ventajas más grandes del formato de archivo de texto plano es que es fácilmente legible, rápido de examinar y hacer búsqueda en sus contenidos, aún si no se cuenta con software especializado, y además, es fácil hacer conversiones desde otros formatos de archivo.

La identificación de los formatos de archivo varía de acuerdo al sistema operativo. Por ejemplo, en los sistemas operativos Windows, el formato del archivo se determina con base en la extensión, mientras que en Linux y otros sistemas operativos basados en Unix, el formato se identifica con el número de identificación, el cual es un número incrustado al inicio o cerca del inicio del archivo.

Lección 15. Cuidados de la evidencia en la escena.

Realizadas las diferentes inspecciones iniciales se hace necesario tener especial cuidado sobre los equipos atacados, para ello se hace necesario tener en cuenta las siguientes observaciones:[20]

Esterilidad de los medios informáticos de trabajo

Los medios informáticos utilizados por los profesionales en esta área, deben estar certificados de tal manera, que éstos no hayan sido expuestos a variaciones

[20] CANO, Jeimy J. Ph.D, CFE, Introducción a la informática forense

magnéticas, ópticas (láser) o similares, so pena de que las copias de la evidencia que se ubiquen en ellos puedan estar contaminadas. La esterilidad de los medios es una condición fundamental para el inicio de cualquier procedimiento forense en informática, pues al igual que en la medicina forense, un instrumental contaminado puede ser causa de una interpretación o análisis erróneo de las causas de la muerte del paciente.

Verificación de las copias en medios informáticos

Las copias efectuadas en los medios previamente esterilizados, deben ser idénticas al original del cual fueron tomadas. La verificación de éstas debe estar asistida por métodos y procedimientos matemáticos que establezcan la completitud de la información traspasada a la copia. Para esto, se sugiere utilizar algoritmos y técnicas de control basadas en firma digitales que puedan comprobar que la información inicialmente tomada corresponde a la que se ubica en el medio de copia. Adicionalmente, es preciso que el software u aplicación soporte de esta operación haya sido previamente probado y analizado por la comunidad científica, para que conociendo su tasa de efectividad, sea validado en un procedimiento ante una diligencia legal.

Documentación de los procedimientos, herramientas y resultados sobre los medios informáticos analizados

El investigador debe ser el custodio de su propio proceso, por tanto cada uno de los pasos realizados, las herramientas utilizadas (sus versiones, licencias y limitaciones), los resultados obtenidos del análisis de los datos, deben estar claramente documentados, de tal manera, que cualquier persona externa pueda validar y revisar los mismos. Ante una confrontación sobre la idoneidad del proceso, el tener documentado y validado cada uno de sus procesos ofrece una importante tranquilidad al investigador, pues siendo rigurosos en la aplicación del

método científico es posible que un tercero reproduzca sus resultados utilizando la misma evidencia.

Mantenimiento de la cadena de custodia de las evidencias digitales

Este punto es complemento del anterior. La custodia de todos los elementos del sistema allegados al caso y en poder del investigador, debe responder a una diligencia y formalidad especiales para documentar cada uno de los eventos que se han realizado con la evidencia en su poder. Quién la entregó, cuándo, en qué estado, cómo se ha transportado, quién ha tenido acceso a ella, cómo se ha efectuado su custodia, entre otras, son las preguntas que deben estar claramente resueltas para poder dar cuenta de la adecuada administración de las pruebas a su cargo.

Informe y presentación de resultados de los análisis de los medios informáticos

Este elemento es tan importante como los anteriores, pues una inadecuada presentación de los resultados puede llevar a falsas expectativas o interpretación de los hechos que ponga en entredicho la idoneidad del investigador. Por tanto, la claridad, el uso de un lenguaje amable y sin tecnicismos, una redacción impecable sin juicios de valor y una ilustración pedagógica de los hechos y los resultados, son elementos críticos a la hora de defender un informe de las investigaciones. Generalmente existen dos tipos de informes, los técnicos con los detalles de la inspección realizada y el ejecutivo para la gerencia y sus dependencias.

Administración del caso realizado

Los investigadores forenses en informática deben prepararse para declarar ante un jurado o juicio, por tanto, es probable que en el curso de la investigación o del caso, lo puedan llamar a declarar en ese instante o mucho tiempo después. Por

tanto, el mantener un sistema automatizado de documentación de expedientes de los casos, con una adecuada cuota de seguridad y control, es labor necesaria y suficiente para salvaguardar los resultados de las investigaciones y el debido cuidado, diligencia y previsibilidad del profesional que ha participado en el caso.

Auditoría de los procedimientos realizados en la investigación

Finalmente y no menos importante, es recomendable que el profesional investigador mantenga un ejercicio de autoevaluación de sus procedimientos, para contar con la evidencia de una buena práctica de investigaciones forenses, de tal manera que el ciclo de calidad: PHVA - Planear, Hacer, Verificar y Actuar, sea una constante que permita incrementar la actual confiabilidad de sus procedimientos y cuestionar sus prácticas y técnicas actuales para el mejoramiento de su ejercicio profesional y la práctica de la disciplina.

UNIDAD 2. ANÁLISIS DE LAS EVIDENCIAS Y HERRAMIENTAS COMPUTACIONALES PARA INFORMÁTICA FORENSE.

CAPITULO 4. RECOLECCION DE EVIDENCIA DIGITAL.

Lección 16. Estrategias para la recolección de pruebas electrónicas

Llevar un orden de recopilación de información

Si la recolección de datos se realiza correctamente y de una manera ordenada, es mucho más útil en la detención del atacante y, como tal, tiene una posibilidad mucho mayor de ser admisible en un proceso judicial. El orden de recopilación debe llevarse a cabo siguiendo los siguientes pasos básicos[21]:

Buscar la evidencia.

Determinar dónde puede estar la evidencia que se esta buscando y si esta se encuentra almacena en el sistema atacado, para ello se hace necesario hacer una listado de verificación que puede ayudar en el proceso de recolección, comprobando que todo lo que se está buscando este en el sistema.

Determinar la relevancia de los datos.

Al descubrir la evidencia, se debe decidir qué partes de ella son relevantes para el caso, para estar seguro, se debe recopilar toda la información necesaria y no excluir ninguna prueba que tenga afinidad con el caso reportado, es necesario trabajar rápido y no perder tiempo recogiendo información que no será de utilidad para el caso.

[21] Incident Response, Computer Forensics Toolkit, Douglas Schweitzer

Determinar la volatilidad de la información.

Una vez que se haya determinado en qué lugares se va ha buscar la información, también se debe decidir en qué orden se van ha recolectar, es necesario establecer que dispositivos son volátiles y pueden contener información (un dispositivo volátil es el que funciona en un instante determinado), por lo cual se debe actuar de manera ágil mientras el dispositivo este funcionando, por lo cual se recomienda hacer una lista de elementos con prioridad de apagado para conservarlos activos mientras dure la indagación.

Eliminar la interferencia exterior.

Es muy importante no alterar los datos originales, ya que la información alterada no es fuente confiable de evidencia por lo cual es necesario impedir cualquier contaminación, en algunos casos los atacantes pueden instalar un interruptor que puede borrar evidencia una vez el equipo se desconecta de la red o de Internet.

Recoger la evidencia.

Para iniciar el proceso de recolección puede utilizar todas las herramientas de software disponibles para esta tarea, recuerde que existen programas libres y propietarios que ayudan a esta tarea. Examine los elementos que ya ha recogido anteriormente y revise que elementos en su listado pueden faltar para que inspeccione nuevamente la escena.

Documentar todas las acciones realizadas.

En los litigios legales cualquier método de recolección de evidencia que se presenta podrá ser puesto en duda, por lo cual es indispensable mantener un registro de todo lo que se hace en el proceso de recolección. Las marcas de tiempo, las firmas digitales, y las declaraciones firmadas sirven para validar el

proceso de recolección de evidencia, incluir toda la justificación que comente los procesos de recolección.

Lección 17. Orientaciones para Recolección de Evidencias.[22]

El procedimiento para la recolección de evidencia varía de país a país, sin embargo, existen unas guías básicas que pueden ayudar a cualquier investigador forense.

El aspecto más importante a la hora de recolectar evidencia, es la preservación de la integridad de ésta; en el caso particular de la información almacenada en medios magnéticos, la naturaleza volátil de ésta hace que dicha labor sea particularmente difícil.

Cantidad de Información recolectada.

La primera gran decisión que se debe tomar a la hora de recolectar evidencias, es la cantidad. Un investigador podría estar tentado a llevarse todo el equipo computacional que encuentre en la escena, con el fin de no arriesgarse a dejar piezas de información potencialmente importantes. Sin embargo, esta alternativa tiene sus inconvenientes, ya que el investigador podría terminar siendo demandado por dañar o alterar el sistema informático, desde este punto de vista, quizás lo indicado sería incautar sólo lo mínimo necesario para efectuar una investigación. Aunque en último, es la severidad y la categoría del crimen las que determinan cuánta evidencia digital se debe recolectar.

[22] Incident Response, Computer Forensics Toolkit, Douglas Schweitzer

Cuidados al Hardware.

El hardware es uno de los elementos que se debe tener en cuenta a la hora de la recolección de evidencia, debido a que puede ser usado como instrumento, como objetivo del crimen, o como producto del crimen. Generalmente, es necesario recolectar elementos de almacenamiento cd, dvd, cintas magnéticas, diskettes, memorias flash que puedan contener evidencia. En este punto se debe tomar otra decisión crítica: ¿los equipos involucrados en una investigación deben ser apagados o deben permanecer prendidos?, muchas agencias de investigación recomiendan apagar los equipos en todas las situaciones y algunos expertos insisten en que es la mejor alternativa debido a la posibilidad de que la evidencia sea destruida mientras el computador permanece encendido. Aún así, hay casos en que apagar un equipo puede causar más daños que beneficios, por ejemplo, si se trata de un servidor que presta servicios a muchas personas que no necesariamente están involucradas en una investigación, como siempre, la mejor opción para el investigador es utilizar su buen juicio y sentido común para determinar las acciones a seguir.

Lección 18. Volatilidad de la evidencia.[23]

Con el fin de resolver un delito informático o violación a los sistemas con eficacia, es necesario examinar el sistema más como un detective que como un usuario de computador, en este sentido se debe examinar cada elemento con cuidado ya que pueden presentar información que nunca se pueda recuperar si se ha hecho alguna manipulación sobre los elementos, por lo cual se debe tener en consideración las siguientes apreciaciones:

- La evidencia desaparece con el tiempo, ya sea como resultado de la actividad normal del sistema o como resultado de los actos de los usuarios.

[23] Incident Response, Computer Forensics Toolkit, Douglas Schweitzer

- Cada paso podrá destruir la información, por lo que todas las medidas que tome deben ser bien aplicadas la primera vez o se puede perder mucha información valiosa.
- Es importante que no se busque información en áreas que normalmente no tienen razón alguna para ser accedida (como archivos personales) a menos que se haya notificado al usuario (por ejemplo, a través de un banner de inicio de sesión) que toda la información almacenada en el equipo es objeto de embargo o si se tiene razones suficientes para creer que un incidente de seguridad está ocurriendo o ha ocurrido.

En general, la evidencia informática debe ser

- Admisible: Las pruebas deben cumplir con ciertas normas legales antes de que puedan presentarse un tribunal. Esto se explica más adelante en este capítulo.
- Auténtica: Debe ser posible vincular positivamente el material probatorio a los hechos, demostrando que la evidencia se relaciona con el incidente de una manera relevante.
- Completa: Se debe contar toda la historia y no sólo una perspectiva particular. No sólo debe reunir pruebas que puedan demostrar las acciones del atacante, pero también evidencia de que podría ser su inocencia.
- Confiable: No debe haber nada acerca de cómo la evidencia fue recogida y, posteriormente, manejado que arroja dudas sobre su autenticidad y veracidad.
- Creíble y comprensible: La evidencia debe ser fácilmente creíble y capaz de entender por un tribunal de justicia. No tiene sentido en la presentación de la salida de un volcado de memoria si un jurado no tiene idea de lo que significa.

La evidencia volátil es evidencia la que rápidamente puede desaparecer o es sólo de carácter temporal, este tipo de pruebas tiene que ser recogida antes de que la

máquina sea desconectada de la red y sea apagada. La recopilación de pruebas se debe hacer de la más volátil a la menos volátil. A continuación se presenta un ejemplo de elementos volátiles

- Memoria física y virtual
- Los procesos en ejecución
- Red conexiones y todo lo que se ejecuta en modo promiscuo.
- Sistemas de almacenamiento permanente: Discos duros, disquetes, cintas, y DVD – CD - RWs/ ROMs).

Es muy fácil destruir involuntariamente las pruebas en un dispositivo volátil cuando se está en el proceso de recolección de pruebas, recuerde tomar las siguientes precauciones:

- No apague el sistema hasta que haya completado todos los procedimientos de recolección de pruebas para pruebas volátiles. Muchas pruebas se pueden perder cuando un sistema está apagado y el atacante puede haber alterado la puesta en marcha, apagado y servicios para destruir la evidencia.
- No confiar en los programas activos en el sistema.
- Ejecutar los programas de obtención de pruebas (software forense) en los medios de comunicación debidamente protegidos.
- No ejecute programas que modifican el tiempo de acceso de todos los archivos en el sistema (por ejemplo tar o xcopy).

Lección 19. Recomendaciones Generales

El proceso de recolección de evidencia electrónica puede ser costoso en términos de horas - hombre y del tiempo de inactividad del sistema, ya que los procesos de recolección pueden consumir mucho tiempo y los sistemas afectados pueden no

estar disponibles para un uso normal durante un tiempo prolongado mientras se llevan a cabo la recopilación y análisis de los datos.

Cuando llegue el momento de comenzar la recolección de pruebas la primera regla que se debe seguirse es la de no apresurarse. Es común que la victima desee saber rápidamente que información fue vulnerada y ejerce mucha ansiedad sobre el investigador, sin embargo, si el investigador se apresura en los procedimientos de recolección de datos, la evidencia puede ser pasada por alto, recuerde que un error en la recolección y preservación de la evidencia a menudo es irreversible.

Lección 20. Análisis de la Evidencia Recolectada

Recolección

La recolección de evidencia informática es un aspecto frágil del la informática forense porque requiere de prácticas y cuidados adicionales que no se tienen en la recolección de evidencia convencional. Es por esto que:

- Se debe proteger los equipos del daño.
- Se debe proteger la información contenida dentro de los sistemas de almacenamiento de información (muchas veces, estos pueden ser alterados fácilmente por causas ambientales, o por un simple campo magnético).
- Algunas veces, será imposible reconstruir la evidencia (o el equipo que la contiene), si no se tiene cuidado de recolectar todas las piezas que se necesiten.

Análisis

Antes de iniciar esta fase se deben preparar las herramientas técnicas, autorizaciones de monitoreo y soporte administrativo, para iniciar 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 y qué daños causaron. 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.

- **Preparación para el análisis**

Antes de comenzar el análisis de las evidencias se deberá:

1) Acondicionar un entorno de trabajo adecuado al estudio que se desea realizar.
2) Trabajar con las imágenes que se recopiló como evidencias o mejor aún con una copia de éstas, tener en cuenta que es necesario montar las imágenes tal cual estaban en el sistema comprometido.
3) Si dispone de recursos suficientes preparar dos estaciones de trabajo, una de ellas contendrá al menos dos discos duros.
4) Instar un sistema operativo que actuará de anfitrión y que servirá para realizar el estudio de las evidencias. En este mismo ordenador y sobre un segundo disco duro, instalar las imágenes manteniendo la estructura de particiones y del sistema de archivos tal y como estaban en el equipo atacado.

5) En otro equipo instar un sistema operativo configurado exactamente igual que el equipo atacado, además mantener nuevamente la misma estructura de particiones y ficheros en sus discos duros., la idea es utilizar este segundo ordenador como "conejillo de Indias" y realizar sobre él pruebas y verificaciones conforme se vayan surgiendo hipótesis sobre el ataque.

Si no se dispone de estos recursos, se puede utilizar software como VMware[24], que permitirá crear una plataforma de trabajo con varias máquinas virtuales. También se puede utilizar una versión LIVE de sistemas operativos como Linux en versiones Ubuntu - Caine[25], que permitirá interactuar con las imágenes montadas pero sin modificarlas.

Si se está muy seguro de las posibilidades y de lo que va a hacer, se puede conectar los discos duros originales del sistema atacado a una estación de trabajo independiente para intentar hacer un análisis en caliente del sistema, se deberá tomar la precaución de montar los dispositivos en modo sólo lectura, esto se puede hacer con sistemas anfitriones UNIX/Linux, pero no con entornos Windows.

Reconstrucción de la secuencia temporal del ataque

Si ya se tienen montadas las imágenes del sistema atacado en una estación de trabajo independiente y con un sistema operativo anfitrión de confianza, se procede con la ejecución de los siguientes pasos:

1. Crear una línea temporal o timeline de sucesos, para ello se debe recopilar la siguiente información sobre los ficheros:

    - Marcas de tiempo (fecha y hora de modificación, acceso, creación y borrado).

[24] Software para informática forense http://www.forensicfocus.com/vmware-forensic-tool
[25] Caine proyecto Digital Forensics disponible en http://www.caine-live.net/

- Ruta completa.
- Tamaño en bytes y tipo de archivo.
- Usuarios y grupos a quien pertenece.
- Permisos de acceso.
- Si fue borrado o no.

Esta será la información que más tiempo llevará recopilar y será el punto de partida para el análisis, podría plantearse aquí el dedicar un poco de tiempo a preparar un script que automatizase el proceso de creación del timeline, empleando los comandos que proporciona el sistema operativo y las herramientas utilizadas.

2. Ordenar los archivos por sus fechas MAC[26], esta primera comprobación, aunque simple, es muy interesante pues la mayoría de los archivos tendrán la fecha de instalación del sistema operativo, por lo que un sistema que se instaló hace meses y que fue comprometido recientemente presentará en los ficheros nuevos, fechas MAC muy distintas a las de los ficheros más antiguos.

La idea es buscar archivos y directorios que han sido creados, modificados o borrados recientemente o instalaciones de programas posteriores a la del sistema operativo y que además se encuentren en rutas poco comunes. Pensar que la mayoría de los atacantes y sus herramientas crearán directorios y descargarán sus “aplicaciones” en lugares donde no se suele mirar, como por ejemplo en los directorios temporales.

A modo de guía centrarse primero en buscar los archivos de sistema modificados tras la instalación del sistema operativo, averiguar después la ubicación de los archivos ocultos, de qué tipo son, identificar también los archivos borrados o

[26] MAC times, abreviación de tiempos de "Modificación, Acceso, y Cambio"; (*"Modification, Access, and Change" times*) en un archivo residente en un computador.

fragmentos de éstos, pues pueden ser restos de logs[27] y registros borrados por los atacantes. Aquí cabe destacar la importancia de realizar imágenes de los discos pues se puede acceder al espacio residual que hay detrás de cada archivo, (recordar que los ficheros suelen almacenarse por bloques cuyo tamaño de clúster depende del tipo de sistema de archivos que se emplee), y leer en zonas que el sistema operativo no ve. Pensar que está buscando "una aguja en un pajar", por lo que se deberá ser metódico, ir de lo general a lo particular, por ejemplo partir de los archivos borrados, intentar recuperar su contenido, anotar su fecha de borrado y compararla con la actividad del resto de los archivos, puede que en esos momentos se estuviesen dando los primeros pasos del ataque.

3. Comenzar a examinar con más detalle los ficheros logs y registros que se examinaron durante la búsqueda de indicios del ataque, intentar buscar una correlación temporal entre eventos. Pensar que los archivos log y de registro son generados de forma automática por el propio sistema operativo o por aplicaciones específicas, conteniendo datos sobre accesos al equipo, errores de inicialización, creación o modificación de usuarios, estado del sistema. Tendrá que buscar entradas extrañas y compararlas con la actividad de los ficheros. Editar también el archivo de contraseñas y buscar la creación de usuarios y cuentas extrañas sobre la hora que considere se inició el ataque del sistema.

4. Examinar los fragmentos del archivo donde se detectan y registran los accesos FTP, estos nos permitirá descubrir si sobre esa fecha y hora se crearon varios archivos bajo el directorio de la máquina comprometida, además, se debe tener presente que este directorio puede ser borrado por el atacante y deberá ser recuperado.

[27] Un log es un registro oficial de eventos durante un rango de tiempo en particular. Para los profesionales en seguridad informática es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre para un dispositivo o aplicación.

CAPITULO 5. HERRAMIENTAS DE SOFTWARE UTILIZADAS EN LA INFORMÁTICA FORENSE.

Lección 21. Aplicaciones para Investigación Forense

En la actualidad existen cientos de herramientas, el uso de herramientas sofisticadas se hace necesario debido a:

- La gran cantidad de datos que pueden estar almacenados en un computador.
- La variedad de formatos de archivos, los cuales pueden variar enormemente, aún dentro del contexto de un mismo sistema operativo.
- La necesidad de recopilar la información de una manera exacta, y que permita verificar que la copia es exacta.
- Limitaciones de tiempo para analizar toda la información.
- Facilidad para borrar archivos de computadores.
- Mecanismos de encriptación, o de contraseñas.

Son herramientas que realizan una exploración completa del computador afectado en un solo paquete informático, se instala en el computador y se realiza la exploración del sistema de archivos y de usuarios. Entre los más populares se encuentran:

EnCase

EnCase es un ejemplo de herramientas de este tipo. Desarrollada por Guidance Software Inc. (http://www.guidancesoftware.com), permite asistir al especialista forense durante el análisis de un crimen digital. Algunas de las características más importantes de EnCase se relacionan a continuación:

- Copiado Comprimido de Discos Fuente

- Búsqueda y Análisis de Múltiples partes de archivos adquiridos
- Diferente capacidad de Almacenamiento
- Varios Campos de Ordenamiento, Incluyendo Estampillas de tiempo.
- Análisis Compuesto del Documento.
- Búsqueda Automática y Análisis de archivos de tipo Zip y Attachments de E-Mail.
- Firmas de archivos, Identificación y Análisis
- Análisis Electrónico Del Rastro De Intervención.
- Soporte de Múltiples Sistemas de Archivo.
- Vista de archivos y otros datos en el espacio Unallocated.
- Genera el reporte del proceso de la investigación forense como un estimado.
- Visualizador Integrado de imágenes con Galería.

Osforensics

OSForensics es un conjunto de utilidades para informática forense para comprobar qué se ha hecho con un computador. OSForensics se puede instalar en memorias USB y cuenta con un gestor de casos. Sus características principales son:

- buscar textos e imágenes
- recopilar rastros de actividad
- buscar archivos borrados y disfrazados
- visualizar el contenido de la memoria RAM
- crear un informe del sistema.
- Numerosas herramientas de investigación
- Instalador para unidades USB
- Base de datos de firmas (hash sets)
- Gestor de casos y generador de informes

Access Data Forensic Tool Kit (Ftk)

Forensic Toolkit de AccessData® (FTK™) ofrece a los profesionales encargados de controlar el cumplimiento de la ley y a los profesionales de seguridad la capacidad de realizar exámenes forenses informatizados completos y exhaustivos. FTK posee funciones eficaces de filtro y búsqueda de archivos. Los filtros personalizables de FTK permiten buscar en miles de archivos para encontrar rápidamente la prueba que necesita. FTK ha sido reconocida como la mejor herramienta forense para realizar análisis de correo electrónico. Sus principales funciones son:

- Fácil de usar
- Opciones de búsqueda avanzadas
- Registry viewer
- Análisis de correo electrónico y de archivos zip
- Diseño de capa de base de datos
- Montaje seguro de dispositivos remotos

Forense Toolkit (TCT)

TCT incluye una variedad de utilidades para el estudio y la recopilación de datos las partes principales de la caja de herramientas son ladrón de tumbas (un programa de recolección de datos), Lazaruns (un programa de reconstrucción de datos), y mactime (un sistema de archivos de sello de tiempo representanteórter).

Caine

CAINE (Medio ambiente de investigación asistido por computador) es una versión italiana de GNU / Linux, fue creado como un proyecto forense digital CAINE ofrece un completo entorno forense que está organizado para integrar herramientas de

software existentes como módulos de software y proporcionar una interfaz gráfica amigable.[28]

Los objetivos de diseño principales de CAINE son los siguientes:

- un entorno interoperable que admite el investigador digital durante las fases de la investigación digital
- Una interfaz gráfica de usuario amigable
- una recopilación semiautomática del informe final

Lección 22. Clasificación de herramientas para informática forense.

Herramientas para el Monitoreo y/o Control de Computadores

Algunas veces se necesita información sobre el uso de los computadores, por lo tanto existen herramientas que monitorean el uso de los computadores para poder recolectar información. Existen algunos programas simples como key loggers o recolectores de pulsaciones del teclado, que guardan información sobre las teclas que son presionadas, hasta otros que guardan imágenes de la pantalla que ve el usuario del computador, o hasta casos donde la máquina es controlada remotamente “KeyLogger” es un ejemplo de herramientas que caen en esta categoría. Es una herramienta que puede ser útil cuando se quiere comprobar actividad sospechosa; guarda los eventos generados por el teclado, por ejemplo, cuando el usuario teclea la tecla de 'retroceder', esto es guardado en un archivo o enviado por e-mail. Los datos generados son complementados con información relacionada con el programa que tiene el foco de atención, con anotaciones sobre las horas, y con los mensajes que generan algunas aplicaciones.

[28] http://www.caine-live.net/

Herramientas de Marcado de documentos

Un aspecto interesante es el de marcado de documentos; en los casos de robo de información, es posible, mediante el uso de herramientas, marcar software para poder detectarlo fácilmente.

El foco de la seguridad está centrado en la prevención de ataques. Algunos sitios que manejan información confidencial o sensitiva, tienen mecanismos para validar el ingreso, pero, debido a que no existe nada como un sitio 100% seguro, se debe estar preparado para incidentes.

Herramientas de Hardware

Debido a que el proceso de recolección de evidencia debe ser preciso y no debe modificar la información se han diseñado varias herramientas como el DIBS "Portable Evidence Recovery Unit".

Lección 23. Construcción de un kit de herramientas de informática forense.

El componente esencial de toda la investigación del delito informático es como se hace la recolección de las evidencias, esto es esencial para la investigación ya que se puede extraer y proporcionar información detallada sobre un equipo o red de trabajo que se haya atacado.

Los Kits de herramientas para informática forense vienen en dos tipos: uno que puede montar directamente el investigador y otro el prefabricada que se puede descargar o comprar, hay que tener en cuenta que en algunos momentos de la investigación forense se necesite controlar el trafico de datos y romper la contraseñas, por ello, el kit forense debe contener los programas necesarios para realizar cada una de estas tareas.

Para crear su kit de herramientas personalizado puede hacerlo a través de una combinación de utilidades freeware y/o shareware. Los siguientes son los tipos de herramientas que deben ser incluidos la hora de realizar un examen de informática forense básica:

- Una herramienta para capturar el tráfico de la red para el análisis (por ejemplo, un rastreador de red)
- Una utilidad para crear imágenes de disco o clones a nivel de bits
- Una herramienta para crackear las contraseñas
- Una herramienta que informa sobre puertos TCP / IP abiertos y detecte las procedencias de esos puertos
- Una herramienta para recuperar borrados (borrado) de datos
- Una utilidad para realizar copias de seguridad y editar el Registro de Windows
- Una utilidad para mostrar toda la actividad del sistema de archivos en tiempo real
- Una herramienta para analizar las propiedades del archivo
- Una herramienta de monitorización que muestra toda la actividad del Registro en tiempo real
- Una utilidad que muestra los recursos compartidos de red tanto local y remota
- Una herramienta de monitorización que muestra los inicios de sesión, los cierres de sesión y el uso de privilegios
- Una herramienta que muestra los archivos abiertos, los procesos de objetos, las claves de registro, archivos DLL y los propietarios de los procesos de objetos

La lista anterior está pensada sólo como un ejemplo y no esta todo incluido, además, al seleccionar las herramientas, hay algunas pautas a seguir:

- Herramientas de línea de comandos son los mas recomendados, evitar las herramientas que utilizan un interfaz (GUI)
- Crear varios disquetes, cd rom, usb que contienen sus herramientas de recolección de datos más importantes.
- Utilice herramientas probadas que sabemos que funcionan

Lección 24. Utilizando rastreadores de paquetes para reunir pruebas.

Las Investigaciones forenses en algunas ocasiones ameritan la captura de datos en tiempo real a medida que viajan a través de la red computacional de una organización. Estos datagramas a medida que atraviesan una red se les conocen como paquetes Sniffing, y los programas diseñados para detectaros son llamados sniffers, analizadores de protocolo o analizadores de red.

Lo que hacen los sniffers es analizar el tráfico en un segmento de red Ethernet escuchando el tráfico de red, al ejecutar un sniffer en una red se pueden recoger pruebas de intrusión en un sistema informático, hay muchos sniffers entre los caules se tiene:

- **Snort:** es un programa de código abierto (freeware) de intrusiones de red del sistema de detección de Unix y Linux, es capaz de realizar análisis en tiempo real del tráfico y paquetes sesión en las redes IP. Mientras que sobresale como un sistema de detección de intrusiones, también puede ser utilizado como un analizador de paquetes. Para más información o para descargar una copia, visite www.snort.org.

- **Ngssniff:** es pequeño y fácil de usar, captura de paquetes de red y el programa de análisis. Se requiere Windows 2000 o XP para operar y permite a los usuarios capturar, guardar, y analizar el tráfico de red. Este paquete sniffer se puede descargar en www.nextgenss.com / products / ngssniff.html.

- **Ethereal:** es un analizador de protocolos de red gratuito con versiones para Unix y sistemas operativos de Windows. Le permite examinar datos de una red activa o de un archivo de captura en disco. Se puede descargar desde www.ethereal.com.

Lección 25. Recomendaciones Sobre el uso de software

El software se clasifica para su uso en los denominados propietarios y los de uso libre, los de tipo propietario requieren la compra de una licencia de funcionamiento con la cual se subscribe un contrato de uso y no de propiedad del software entre los productores de software y los usuarios, al adquirir la licencia de uso no se "compra" los códigos fuentes del programa y la utilización queda restringida a lo que el productor provee. Los programas de uso libre son programas que, para cualquier propósito, se puede usar, copiar, distribuir y modificar libremente, es decir, es software incluye archivos fuentes modificables para conveniencia del usuario que lo utiliza.

Cuando se inicia el peritaje en un caso de informática forense se hace necesario utilizar herramientas software que nos permitan indagar y recopilar evidencia en los medios informáticos que fueron atacados. Por ello el uso de programas es necesario y vital dentro del proceso investigativo, pero se debe tener en cuenta que como investigador forense digital debe contar con herramientas legalmente adquiridas ya que el uso de un programa no licenciado o de distribución libre no legalizado haría que los jueces no avalen el procedimiento de recolección de evidencia.

CAPITULO 6. DESARROLLO DE UN CASO DE INFORMÁTICA FORENSE

Lección 26. Reconocimiento de los sistemas operativos.

Después de la BIOS, el sistema operativo (SO) es el primer programa de software que se encuentra cuando se enciende un computador, el sistema operativo permite que las aplicaciones (programas) se comuniquen con el equipo y entre otros programas a un nivel básico.

Cada computador de propósito general requiere algún tipo de sistema operativo que le indique al computador como operar e informando sobre las aplicaciones a utilizar y sobre el hardware que está instalado en ese equipo.

Hay esencialmente dos tipos de sistemas operativos, los dirigidos hacia el usuario doméstico y los orientados a las empresas o usuarios avanzados. Los sistemas operativos más utilizados se pueden dividir en tres familias: la familia de Microsoft Windows, la familia Unix / Linux y los sistemas operativos de Apple Macintosh. Cada una de estas familias también ofrece versiones de sistemas operativos que están específicamente dirigidos a la administración de redes, por lo que son los más ampliamente utilizados en todo el mundo, de hecho, los sistemas Unix / Linux se consideran los sistemas operativos más seguros, estos están diseñados específicamente para la administración de redes.

En la familia de Microsoft se encuentran los sistemas operativos Windows NT 4.0, 2000, Server, que se utilizan mas comúnmente en la administración de las redes de las organizaciones. Debido a que son fáciles de configurar y de usar, también, tienen una gran cantidad de aplicaciones desarrolladas para ellos siendo los sistemas operativos más populares y ampliamente utilizados en todo el mundo.

La familia Apple Macintosh (en la actualidad en la versión OS X) es un sistema de red basado en Unix con funciones de red potente y muchas características de

seguridad. Sin embargo, debido a ciertas diferencias de arquitectura inherentes a los equipos de Apple, Mac OS no han alcanzado la popularidad de los sistemas operativos Windows. (Mac OS es, sin embargo, considerado por muchos como el más adecuado para las organizaciones que utilizan gráficos intensos programas como CAD / CAM).

Si bien todos los sistemas operativos actuales ofrecen alguna medida de seguridad, son los sistemas operativos de red los que poseen las capacidades más grandes de seguridad. Permiten que los administradores de red especifiquen los privilegios de acceso a los archivos individuales, directorios y dispositivos de hardware.

Todos estos sistemas operativos tienen un amplio esquema de auditoría que permite el seguimiento de archivos y de registros, además, los sistemas operativos de red tienen un valor agregado el cual permite capturar y preservar las pruebas en el caso de un potencial análisis forenses.

Lección 27. Imágenes de Discos Duros.

El principio rector de la informática forense es reunir las posibles pruebas que luego serán analizadas y presentadas a un tribunal para demostrar la presencia de una actividad ilegal. Es importante aclarar que la información en un caso de informática forense no haya alteración, daño o alteración de los datos recolectados.

El primer paso para llevar a cabo un análisis forense adecuado es recopilar evidencia informática. Debido a que existe un cierto grado de volatilidad de los datos almacenados en un disco duro, crear una imagen bit a bit es uno de los primeros procedimientos que se deberán llevar a cabo, este procedimiento se hace después de que los contenidos de la memoria del computador han sido copiados y almacenados correctamente.

Crear una imagen del disco indica que se hace una copia espejo o una reproducción de los datos contenidos en el disco duro. La reproducción es una copia perfecta del disco duro sector por sector de la unidad, incluyendo todos los espacios no utilizados y los sobrescritos parcialmente.

El proceso de creación de imágenes del disco duro no es un procedimiento destructivo con los datos y no se requiere que el sistema operativo este activo, esto asegura que el sistema no se alterará de ninguna manera durante el proceso de creación de las imágenes y se conservaran las pruebas.

Cuando se tiene creada la imagen del disco duro el análisis forense se realiza únicamente sobre la imagen creada y por ningún motivo en el disco duro original, es recomendable tener 2 imágenes como respaldo al análisis.

La capacidad de almacenamiento de los discos duros de las computadoras ha crecido exponencialmente en los últimos años. Como resultado, los discos duros son capaces de almacenar enormes cantidades de datos y hace que el procedimiento de toma de imágenes sea más complicado, para ello, se recomienda utilizar una herramienta que cree imágenes de disco ya que estos hacen una copia exacta del disco duro. No se recomendable utilizar software como Partition Magic de PowerQuest para copiar el disco duro original ya que esto puede potencialmente contaminar la evidencia ya que este tipo de programas no capturan todos los datos residuales (por ejemplo, archivos eliminados, espacio de holgura, y intercambio de archivos) necesarios para realizar un análisis forense completo.

Cómo elegir y utilizar la herramienta adecuada es imprescindible en una investigación en informática forense. De acuerdo con las especificaciones de imágenes de disco publicados por el Instituto Nacional de Estándares y Tecnología (NIST), las exigencias de un alto nivel de imágenes de disco herramienta son las siguientes:

- La herramienta hará una duplicación del flujo de bits o una imagen de un disco original
- La herramienta no modificará el disco original.
- La herramienta será capaz de acceder tanto a discos IDE y SCSI.
- La herramienta deberá ser capaz de verificar la integridad de un archivo de imagen de disco.
- La herramienta deberá registrar los errores de entrada / salida (E / S).
- La documentación de la herramienta deberá ser correcta.

Además, el NIST recomienda los siguientes requisitos para todas las herramientas de imágenes en disco:

- La herramienta no deberá alterar el original.
- Si no hay errores de acceso a los medios de origen, la herramienta deberá crear un duplicado del original bit a bit.
- Si hay errores I / O para acceder a los medios de origen, la herramienta deberá crear un duplicado del flujo de datos identificando las áreas no accedidas y documentando en el registro este proceso.
- La herramienta deberá registrar los errores de E / S, incluyendo el tipo de error y la ubicación del error.
- La herramienta deberá ser capaz de acceder a las unidades de disco a través de una o más de los siguientes interfaces: acceso directo a la controladora de disco, interfaz BIOS, interfaz BIOS extendida, interfaz SCSI o interfaz de Linux.

La documentación debe ser correcta en la medida en que la obligatoria y todos los requisitos aplicados opcionales se refiere. Por ejemplo, si un usuario siguiendo procedimientos documentados de la herramienta produce el resultado esperado, entonces la documentación se considera correcta.

- La herramienta deberá copiar una fuente a un destino que es mayor o igual

al tamaño de la fuente, y deberá documentar el contenido de las áreas sobre el destino que no forman parte de la copia.

- La herramienta deberá notificar al usuario si la fuente es mayor que el de destino.

Las siguientes herramientas para crear imágenes de disco se encuentran entre las pocas que en la actualidad cumplen con los requisitos dispuestos por el NIST:

- **Linux dd** es una utilidad gratuita para cualquier sistema Linux que crea la imagen y copia de todos los sectores en todos los discos duros SCSI e IDE. Esta utilidad incluye un mecanismo de MD5, Linux dd se puede encontrar en www.redhat.com.
- **SnapBack DatArrest,** por Columbia Data Producís, Inc. (CDP), es una completa aplicación para crear imágenes de disco se ejecuta desde un solo disquete. Según su fabricante, se puede acceder a datos a una velocidad de hasta 300MB por minuto, así como también crear una copia de seguridad para DOS, Windows, Windows 95, Windows NT, y Unix, los detalles adicionales y los precios pueden ser encontrado en www.snapback.com.

Lección 28. Iniciar un caso de informática forense.

Un caso de ataque informático, se puede presentar de diferentes maneras según la ley 1273 de 2009 en Colombia, de acuerdo al ataque se origina el delito informático, una vez determinado el ataque se hace necesario establecer que tipo de fraude se desea comprobar para esto se hace necesario realizar un análisis a los equipos computacionales afectados para obtener las pruebas suficientes que demuestren el fraude.

De a cuerdo a las lecciones estudiadas en este modulo se indica en este espacio los aspectos más relevantes para iniciar la investigación en su orden:

1. Inspeccionar el sistema operativo instalado para determinar la forma de apagado del sistema
2. Apagar el sistema de acuerdo a las condiciones dadas para cada sistema operativo
3. Aislar los equipos informáticos, medios de almacenamiento y anotaciones
4. Crear las imágenes de los dispositivos encontrados en la escena del incidente
5. Determinar la cantidad de Información a recolectar.
6. Documentar todas las acciones realizadas anteriormente

Lección 29. Donde buscar evidencia.

Evidencia Digital Almacenada en Dispositivos

Cuando se presenta el caso en que la evidencia está en formato digital el objetivo de la investigación debe ser el contenido del computador, no el hardware. Hay dos opciones cuando se recolecta evidencia digital: copiar todo, o sólo copiar la información necesaria. Si se dispone de mucho tiempo y no se sabe a ciencia cierta qué se está buscando, lo ideal es copiar todo el contenido del computador y examinar todo detenidamente. Por otra parte, si lo que se necesita es una pista rápida, como pasa en la mayoría de casos o sólo se necesita una porción de la evidencia digital, es más práctico buscar en el computador y tomar sólo lo que se necesite.

Cuando se recolecta todo el contenido de un computador, en general los pasos a seguir son los mismos:

- Toda la evidencia importante debe ser leída de la memoria RAM.
- El computador debe ser apagado.
- El computador debe ser reiniciado usando otro sistema operativo que desvíe el existente y no cambie el contenido de el (los) disco(s) duro(s).
- Debería sacarse una copia de la evidencia digital encontrada en el (los) disco(s) duro(s).
- Debe tenerse en cuenta que cuando se habla de hacer una "copia" de un disco duro, ésta debería ser una copia bit-a-bit de todo el contenido de éste; muchísima información está "escondida" en sitios no convencionales de un disco duro.

Evidencia Digital en Redes

Otra categoría de evidencia que puede ser recolectada en el caso de los crímenes informáticos es la evidencia presente en las redes. Todo el flujo de información que corre a través de una red, sea interna o externa a una organización o aún en Internet podría contener evidencia potencialmente útil a la hora de investigar un delito informático.

Adicionalmente, hay ciertos tipos de crímenes, como la falsificación de correos electrónicos, intercambio de información ilegal a través de Internet (por ejemplo pornografía infantil) o uso del IRC para concertar crímenes (práctica común entre la comunidad hacker) que no podrían cometerse sin la utilización de redes. En este caso la evidencia digital difiere de aquella que está almacenada en un solo computador porque se encuentra almacenada en computadores remotos o no está almacenada en ninguna parte. Los investigadores deberán hacer esfuerzos

adicionales para poder demostrar que la evidencia en Internet es auténtica y no ha sido modificada mientras estaba siendo transmitida o recolectada.

La evidencia presente en redes debe ser buscada de manera activa y su recolección puede ser bastante dispendiosa puesto que la información podría estar almacenada en muchos sitios diferentes.

Lección 30. Analizando información.

Recolección

Tal y como se a mencionado con anterioridad, en lo referente a la cadena de custodia que se puede aplicar a la evidencia forense, la recolección adecuada de los rastros de evidencia implica establecer un mecanismo el cual asegure a quien debe realizarse la evaluación y el juicio, que los elementos ofrecidos como prueba documental informática, son confiables, esto quiere decir que durante su recolección o manipulación para su análisis, no han sufrido alteración o adulteración alguna. Para la consecución de este objetivo, se considera aplicar como metodología propuesta la aplicación de una cadena de custodia, la cual es considerada como un procedimiento controlado que se aplica a los indicios materiales relacionados con un hecho delictivo o no, y la cual comienza desde su localización hasta su valoración por el personal encargado de dicho proceso y que tiene como fin asegurar la transparencia y efectividad en la aplicación de las técnicas para el manejo de los mismos, evitando incurrir en alteraciones, sustituciones, contaminaciones o destrucciones, hasta su disposición definitiva ya sea dada por orden judicial o el personal responsable.

Para asegurar la efectividad de estas acciones es necesario establecer un riguroso y detallado registro, que identifique tanto la evidencia como la posesión de la misma, determinando el lugar, hora, fecha, nombre y dependencia involucrada.

Este proceso comienza con la detección, identificación, fijación, recolección, protección, resguardo, empaque y traslado de la evidencia en el lugar del hecho ya sea real o virtual, hasta la presentación como elemento probatorio, de igual manera es necesario considerar el significado o el valor que los elementos recolectados van a tener en el proceso de investigación, análisis y argumentación del cual dependen. Lo cual genera la necesidad de evitar la impugnación de los mismos en razón de errores metodológicos, propios de la informática forense, por ejemplo el asegurar la integridad de la prueba secuestrada mediante un algoritmo Hash sobre el archivo.

Es necesario entender que para que la prueba documental informática sea tenida por válida y adquiera fuerza probatoria, es necesario que la misma garantice su confiabilidad, evitando principalmente suplantaciones, modificaciones, alteraciones, adulteraciones o simplemente su destrucción, ya sea mediante borrado o denegación de servicio, como ocurre con la información volátil. Por tal razón para las actividades a realizarse desde su recolección, hasta su disposición final, debe implementarse un procedimiento con soporte teórico científico, metodológico criminalística, estrictamente técnico y procesalmente adecuado.

Es necesario tener en cuenta que para la identificación de estas actividades, se tiene como condición para el manejo adecuado de la información recolectada, el caso en que el Perito Informático Forense efectúe la recolección de la evidencia a partir del equipo apagado, para lo cual deberá previamente asegurarse que el dispositivo de inicio del equipo no se realice a través del disco rígido o algún dispositivo de almacenamiento secundario instalado.

Si el perito desea acceder a la información secuestrada, deberá utilizar dispositivos de arranque en el modo solo lectura, con herramientas informáticas forenses para realizar la detección, recolección y registro de indicios probatorios, es necesario que una vez seleccionado el medio de almacenamiento secuestrado

se le aplique algún método para la protección de la información, por ejemplo la configuración física mediante el uso de jumpers y si no fuera posible la realización de copias de los mismos.

Para la recolección de los datos probatorios se recomienda la realización de las siguientes actividades, utilizando la aplicación CAINE como software de análisis:

1. Apague el equipo desconectando el cable de alimentación eléctrica
2. Retire cualquier otro dispositivo de almacenamiento que pueda se utilizado para el inicio del equipo (CD, PenDirve, Zip, otros).
3. Elimine la posibilidad de dañar los elementos de almacenamiento por descargas de electricidad estática, eliminando la propia, tocando alguna parte metálica o mediante el uso de una manilla antiestática y prosiga a abrir el gabinete
4. Desconecte la interfaz o el bus de datos del disco duro.
5. Desconecte la alimentación eléctrica del disco duro.
6. En este momento es necesario recolectar la información referente al equipo al cual esta conectado el dispositivo que se va a emplear como prueba, para realizar esto haga lo siguiente:
7. Conecte el equipo a la corriente eléctrica, enciéndalo e ingrese a la CMOS o BIOS, para lo cual debe seleccionar el conjunto de teclas que se muestran en la pantalla de inicio, los mas comunes son F2, Sup, F9, entre otros.
8. Verifique la fecha y hora del CMOS, regístrelas en un formulario de recolección de evidencia, el cual deberá permitir documentar todo tipo de dato que el Perito Informático Forense considere relevante de igual manera para comprobar la integridad de la información recolectada, además del proceso de documentación es necesario obtener evidencias graficas de los datos recolectados, tal es el caso de fotografías, videos u otros.
9. Ubicado en la BIOS del equipo, diríjase al apartado de Menú de Inicio y modifique la unidad de arranque del sistema operativo, para este caso y

como se esta empleado la distribución CAINE, se deberá seleccionar la unidad de CD y se procede a grabar los cambios.

10. Coloque la distribución de CAINE en la unidad de arranque y verifique que el equipo inicie con esta unidad.
11. Continúe apagando nuevamente el equipo y reconecte la unidad de disco duro o PenDrive que ha sido secuestrada como evidencia.
12. Ubique y conecte un dispositivo adicional para el almacenamiento forense.
13. Encienda el equipo e inicie con la versión de CAINE seleccionada.
14. Una vez iniciado CAINE proceda con la duplicación y autenticación de la prueba, haciendo uso de las herramientas para la recolección de información (AIR[29], GUYMAGER[30]) que se encuentran en esta distribución.
15. Realice la comprobación de la imagen mediante la verificación del hash MD5[31], haciendo uso del aplicativo GtkHash.
16. Obtenga una copia digital de este valor mediante la captura de pantalla y guarde el resultado en el dispositivo de almacenamiento forense.
17. Proceda a registrar el resultado del hash MD5 en un formulario de recolección de la evidencia.

Se recomienda realizar el proceso de creación de imágenes por lo menos dos veces para poder comprobar de forma futura la integridad de la información recolectada.

Resguardo y traslado de las pruebas

Cuando el proceso de recolección finaliza se debe continuar con el procedimiento para el resguardo de la prueba y preparación para su traslado, para lo cual es necesario, seguir los siguientes pasos:

[29] AIR. Caine proyecto Digital Forensics disponible en http://www.caine-live.net/
[30] GUYMAGER. Caine proyecto Digital Forensics disponible en http://www.caine-live.net/
[31] MD5: En criptografía, MD5 (abreviatura de Message-Digest Algorithm 5, Algoritmo de Resumen del Mensaje 5) es un algoritmo de reducción criptográfico de 128 bits ampliamente usado.

1. Proceda al apagado del equipo, mediante el uso del comando de apagado de la distribución CAINE, en la opción de finalización con expulsión del CD.
2. Desconecte el bus de datos y la alimentación del disco duro o retire el PenDrive u otro dispositivo.
3. Ubíquese en una zona despejada, para realizar el proceso de rotulado y registro.
   - Registre en un formulario de registro de la evidencia cada uno de los elementos secuestrados, conforme a lo expresado en el formulario y agregando cualquier otra información que se considere pertinente
   - Encárguese de proteger los elementos obtenidos empacándolos en empaques como: Bolsas antiestáticas, para los elementos informáticos de almacenamiento secundario, registrando los datos de fecha y hora del secuestro, tipo, Nro de serie del elemento, tamaño de capacidad de almacenamiento, datos generales del perito, Firma del Perito Informático Forense, finalice rotulando la evidencia.
   - Si existe en su inventario, transpórtelos en bolsas manufacturadas con filamentos de cobre y níquel para prevenir la interferencia de señales inalámbricas celulares, gps, entre otros.
4. Proteja con plástico o con bolsas estériles cualquier otro elemento que considere relevante y rotúlelo con los datos pertinentes al elemento y al perito informático forense.
5. Documente el proceso de recolección mediante la elaboración de un acta de secuestro
6. Coloque los elementos una vez identificados y registrados en una caja o recipiente de traslado que asegure la suficiente rigidez, aislamiento térmico, electromagnético y protección para evitar daños accidentales en el traslado de los elementos probatorios.
7. Traslade, si es posible, los elementos secuestrados reunidos en un único recipiente, evitando la confusión, separación o pérdida durante su almacenamiento posterior.

Cuando el resguardo finaliza se procede al traslado de la evidencia de informática forense que tendrá como destino el Laboratorio de Informática Forense seleccionado. De acuerdo a la evolución del proceso judicial en donde se encuentre involucrada la prueba de informática forense, esta podrá ser posteriormente entregada y resguardada en un lugar o destino específico para su resguardo y depósito final o definitivo.

Una vez finalizado el proceso de almacenamiento, y ya en el laboratorio forense, se continua con el análisis de la información, el cual busca básicamente responder los interrogantes que el ente solicitante del proceso ha solicitado, por ejemplo la existencia o no de información sobre el juicio que se esta desarrollando o evidencias del ataque al cual fue expuesto el equipo.

Análisis

Para el análisis de la información existen diferentes técnicas que pueden ser aplicadas, las cuales dependen de la información que se desee recolectar, como se esta haciendo uso de la distribución CAINE, se empleara el software Autopsy para el análisis de las evidencias recolectadas a continuación se presenta en detalle los pasos a seguir para realizar el proceso según sea el tipo de datos que se busca identificar.

1. Inicialmente se hace necesario identificar si se trata de una imagen de disco, una partición u otro tipo de imagen, para este propósito se analizan los primeros bytes de la imagen con un editor hexadecimal, como Hex Editor (Ghex) que se encuentra en la distribución CAINE.
2. Continúe iniciando el software Autopsy[32]
3. Ingrese los datos referentes al caso

[32] Autopsy, es un frontal Web que permite realizar operaciones de análisis forense sirviendo como interfaz gráfico del popular juego de herramientas forenses The Sleuth Kit (TSK). TSK es un referente en el mundo del análisis forense mediante la línea de mandatos, y que permite a los investigadores lanzar auditorías forenses no intrusivas en los sistemas a investigar.

- Nombre del caso
- Descripción
- Datos de los investigadores
- Zona Horaria
- Tiempo de desincronización de ajuste
- Ruta de la imagen opcional si la copia del archivo esta dañado
- Ruta de la imagen opcional si la copia del archivo se encuentra bien

4. Adicione la imagen con la cual se va a realizar el análisis, se recomienda emplear imágenes con extensión img, llene los siguientes datos:
   - Ubicación
   - Tipo de imagen (Disco o partición)
   - Método de importación

5. Calcule el valor hash MD5 de la imagen y compárelo con el valor generado al momento de recolectar la información para determinar la valides de la imagen, llene el formulario de registro de evidencias al igual que obtenga una imagen de la pantalla para el registro de la documentación.
6. En primer lugar, se hace necesario responder a las siguiente interrogantes, con el análisis de la imagen que se tiene por evidencia, ya sea en el lugar del hecho o en el laboratorio, para la realización del estudio se empleara alguna de las herramientas disponibles en el compilado CAINE, sin embargo se aplicara como herramienta principal para la recolección de evidencias Autopsy tal y como se presenta a continuación:

Tabla 1. Evidencias a recolectar durante el análisis y herramientas empleadas

Tipo de información a buscar	Herramientas de Caine	Función
Tipo de Sistema Operativo Fecha, hora y zona horaria del Sistema Operativo Versión del Sistema Operativo	Autopsy: Categoria Fyle System	fstat: Muestra la informacion del sistema de archivos
Número de particiones, Tipo de particiones y Esquema de la tabla de particiones	Autopsy: Categoria Fyle System	fstat: Muestra la informacion del sistema de archivos
	Hex Editor (Ghex)	Editor Hexadecimal que permite verificar los bits de identificacion de una imagen
Listado de todos los nombre de archivos, fecha y hora	Autopsy: Categoria File name	ffind: Busca el nombre de un archivo o directorio a partir de la direccion de la estructura de metadatos
		Fls: Genera un listado de los nombres de archivo asignados o borrados en una imagen de datos
Registro del espacio descuidado o desperdiciado Incluido el MBR Incluida la tabla de particiones Incluida la partición de inicio del sistema y los archivos de comandos	Autopsy: Categoria Fyle System	fstat: Muestra la informacion del sistema de archivos

Registro del espacio no asignado	Autopsy: Categoria Fyle System	fstat: Muestra la informacion del sistema de archivos
Registro del espacio de intercambio	Autopsy: Categoria Fyle System	fstat: Muestra la informacion del sistema de archivos
Recuperación de archivos eliminados	Ddrescue	Herramienta de recuperacion de datos este programa copia los datos de un archive o bloques de datos a otra ubicacion.
	Dvdisaster	Recupera datos en CD/DVD/BD, permite recuperaciones completas ignorando posibles errors de lectura.
Búsqueda de archivos ocultos con las palabras claves en el	Autopsy: Categoria File name	ffind: Busca el nombre de un archivo o directorio a partir de la direccion de la estructura de metadatos
		Fls: Genera un listado de los nombres de archivo asignados o borrados en una imagen de datos
Listado de todas las aplicaciones existentes en el sistema	Autopsy: Categoria Otros	mactime: Muestra los eventos de un sistema ordenados cronologicamente
Búsqueda de programas ejecutables sospechosos	Autopsy: Categoria Otros y File name	mactime: Muestra los eventos de un sistema ordenados cronologicamente
		ffind: Busca el nombre de un archivo o directorio a partir de la

		direccion de la estructura de metadatos
		Fls: Genera un listado de los nombres de archivo asignados o borrados en una imagen de datos
Identificación de extensiones de archivos sospechosas	Autopsy: Categoria File name	ffind: Busca el nombre de un archivo o directorio a partir de la direccion de la estructura de metadatos
		Fls: Genera un listado de los nombres de archivo asignados o borrados en una imagen de datos
Listado del contenido de los archivos de cada usuario en el directorio raíz y si existen, en los subdirectorios	Autopsy: Categoria File name	ffind: Busca el nombre de un archivo o directorio a partir de la direccion de la estructura de metadatos
		Fls: Genera un listado de los nombres de archivo asignados o borrados en una imagen de datos
Verificación del comportamiento del sistema operativo: Integridad de los comandos, Integridad de los módulos Captura de pantallas	Autopsy: Categoria Otros y File name	mactime: Muestra los eventos de un sistema ordenados cronologicamente
		ffind: Busca el nombre de un archivo o directorio a partir de la direccion de la estructura de metadatos

		Fls: Genera un listado de los nombres de archivo asignados o borrados en una imagen de datos
		File y sorter: Permite clasificar los archivos en la imagen de disco por tipo
Elaboracion de reportes	CAINE, Modulo Reportes	Presenta la posibilidad de documentar los resultados obtenidos en el analisis digital, presentando un reporte estructurado de manera sencilla sin la presentacion de detalles tecnicos innecesarios.

7. Una vez identificados los elementos anteriormente seleccionados, volver a generar la autenticación matemática de los datos a través del algoritmo de hash al finalizar la detección, recolección y registro, para validar los resultados obtenidos, de igual manera a medida que se va realizando el proceso de recolección de información debe documentarse todo el proceso en los formularios correspondientes y en el software Autopsy que se emplea como herramienta principal para el análisis de evidencias.
8. Se debe realizar un proceso documentado en el cual se describa la forma en la que se conservan las copias del software utilizado y realizar el proceso de almacenamiento final de las mismas.

REFERENCIA

Handbook Guidelines for the management of IT evidence (2003). Disponible en: http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN016411.pdf

Distribuciones linux específicas para informática forense Sitio web: http://biatchux.dmzs.com

SUNDT, C. (2006) Information security and the law. Information Security Technical. Report. Vol.2 No.9

Cano Martines Jeimy José. Admisibilidad de la Evidencia Digital: Algunos Elementos de Revisión y Análisis. Agosto de 2003. http://www.alfa-redi.org/rdi-articulo.shtml?x=1304

BREZINSKI, D. y KILLALEA, T. (2002) RFC 3227: Guidelines for Evidence Collection and Archiving. Network Working Group. February. Disponible: http://www.rfceditor.org/rfc/rfc3227.txt

IOCE, Guidelines for the best practices in the forensic examination of digital technology, 2002. Disponible:
http://www.ioce.org/2002/ioce_bp_exam_digit_tech.html

CANO MARTINES, Jeimy José. Introducción a la informática forense. Revista ACIS Junio de 2006 Disponible en:
http://www.acis.org.co/fileadmin/Revista_96/dos.pdf
http://www.informaticaforense.com/criminalistica/
http://www.nist.gov/itl/

SIERRA, José María, HERNÁNDEZ, Julio Cesar y RIBAGORDA, Arturo. Retos de la informática forense. Agora Sic. Volumen 33. Agosto 2003.
Herramientas y manuales para Informática Forense. Disponibles en: http://www.jbex.net/seguridad-informatica/manuales