Corporación Unificada Nacional de Educación Superior

INFORMATICA FORENSE

Fases de aplicación.

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].

Fase de Identificación1

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

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

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. Está fase está 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.

Preservar la escena del Fraude2.
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 omento 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
o El texto es sobre un fondo sólido (generalmente negro).
o El mensaje contiene una letra de unidad y utiliza las barras contrarias.
o El indicador por lo general termina con un signo mayor que (>).
- Procedimientos de cierre
o Fotografiar la pantalla y anotar los programas en ejecución.
o Retire el cable de alimentación de la pared.

Sistema Operativo Windows 3.X
- Características
o Barra de títulos de colores
o Menú estándar de opciones
Procedimientos de cierre
o Fotografiar la pantalla y anotar los programas en ejecución.
o Retire el cable de alimentación de la pared.

Sistema Operativo Windows NT 3.51
- Características
o Barra de título de colores
o Menú estándar de opciones
o Los iconos representan equipos de red y personas
.

- Procedimientos de cierre
o Fotografiar la pantalla y anotar los programas en ejecución.
o Retire cable de alimentación de la pared

Sistema Operativo Windows 95/98/NT 4.0/2000
- Características
o El botón de inicio tiene un símbolo de Windows.- Procedimientos de cierre
o Fotografiar la pantalla y anotar los programas en ejecución.
o Retire cable de alimentación de la pared

Sistema Operativo Unix / Linux
- Características
o El botón de inicio tiene un símbolo de la versión Unix / Linux - Procedimientos de cierre
o Fotografiar la pantalla y anotar los programas en ejecución.
o Haga clic derecho en el menú.
o Desde el menú, haga clic en Consola.
o 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.
o 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
o Posee un símbolo de Apple en la esquina superior izquierda.
o Pequeñas líneas horizontales en las barras de menú de las ventanas
o Un solo botón sencillo en cada esquina de la ventana
o Icono de Papelera
- Procedimientos de cierre
o Fotografiar la pantalla y anotar los programas en ejecución.
o Registre el tiempo desde la barra de menú
o Haga clic en Especial.
o Haga clic en Cerrar.
o En la ventana dice que es seguro apagar el equipo.
o Retire el cable de alimentación de la pared.

Fase de Documentación y Presentación de las pruebas4

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.

E tapa 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, 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:
1. Introducción: Descripción del objetivo del análisis del sistema previamente atacado y comprometido, también se incluye la información de la evidencia proporcionada.
2. Análisis: Descripción del entorno de trabajo y de las herramientas de análisis forense seleccionadas así como la cantidad de tiempo empleado en el mismo.
3. Sumario del incidente: Resumen del incidente tras el análisis de la evidencia aportada.
4. Principales Conclusiones del análisis: Detalle de las conclusiones ha las que se llegó una vez terminado el proceso de análisis.
5. Solución al incidente: Descripción de la solución para recuperación del incidente.
6. Recomendaciones finales: pasos que se deben realizar para garantizar la seguridad de los equipos y que el incidente no vuelva a suceder.

DOCUMENTOS DE REFERENCIA

1 PINZON OLMEDO Fredy Bolivar, La Informática Forense, Universidad católica de Loja
Documentos 1 corte, (2014), Informática Forense Ing FERNANDO JIMENEZ:

.