www.eysglobal.com

ESTUDIO DEL CASO
PARTE 1

PLANTEAMIENTO DEL PROBLEMA

La empresa de salud VIDA SANA tiene dentro de sus funciones entregar el medicamento a los usuarios, en la auditoría realizada se encontraron anomalías en la droguería de la empresa en cuanto a la compra de medicamentos y despacho de las mismas a los usuarios.

ESTUDIO DEL CASO

Se encontró que uno de los empleados junto con algunos directivos de la empresa de salud está alterando el precio de compra de los medicamentos que dan los proveedores por otros más altos y así hacerse a la diferencia. Otro aspecto que se ha detectado es que a los pacientes se les agrega más medicamentos de los formulados para con esto justificar las compras extras y hacer compras ficticias para hacerse a esos dineros.

El fraude esta detectado pero no se tienen las pruebas para comprobar todo este delito, se dio a los funcionarios involucrados algunos días de receso mientras se esclarecen los hechos, se tiene a disposición las oficinas de los sospechosos con todos los elementos computaciones y físicos sin alterar.

ESTUDIO DEL CASO

Pero antes de continuar refresquemos un poco la memoria

El fraude cibernético e informático se refiere al fraude realizado a través del uso de una computadora o del Internet. La piratería informática (hacking) es una forma común de fraude: el delincuente usa herramientas tecnológicas sofisticadas para acceder a distancia a una computadora con información confidencial. Otra forma de fraude involucra la intercepción de una transmisión electrónica. Esto puede ocasionar el robo de la contraseña, el número de cuenta de una tarjeta de crédito u otra información confidencial sobre la identidad de una persona.

ESTUDIO DEL CASO

RESULTADOS

ANÁLISIS DE LA SITUACIÓN

Antes de iniciar con el análisis del ejercicio propuesto se debe partir de las siguientes preguntas:

1. ¿El personal que realiza la auditoria es interno o externo de la empresa VIDA SANA ?
2. ¿Con que periodicidad se realizan la auditoria?
3. ¿Se hace un arqueo del inventario o existencia a corte de mes?
4. ¿Qué lleva a pensar que un empleado y algunos directivos están alterando la información?
5. ¿Las personas que aprueban las compras son las mismas que pagan?
6. ¿Quiénes son las directivas de VIDA SANA y por qué solicitan una investigación del posible hecho punible?

ESTUDIO DEL CASO

CASO GENERAL

1. IDENTIFICAR EL SISTEMA OPERATIVO Y LAS ACCIONES REALIZADAS PARA PRESERVAR LA INFORMACIÓN

Se debe realizar una verificación física en cada uno de los equipos implicados en el problema de fraude, ya que al conocerlo se puede determinar cuál de éstos equipos presenta vulnerabilidad en la seguridad y que acciones se realizaron en el tiempo transcurrido durante el robo de la información, se conocen seis (6) clases de sistemas operativos que son: Unix, Windows, PC_DOS, Linux, MacOS de Macintosh, Solaris, siendo los más populares Los tres primeros mencionados anteriormente.

ESTUDIO DEL CASO

Una vez identificado el S.O. de cada equipo, se procede a la verificación de acciones realizadas y una copia de seguridad de la información que posea cada disco duro de los equipos informáticos realizando o teniendo en cuenta los cinco principios básicos que son:

•Conocer el Inventario de la Información Archivos y Computadoras que se tienen.

•Reducir los archivos, manteniendo únicamente la información que se requiere o se necesita.

•Proteger la Información que se mantiene

•Eliminar la información que sea innecesaria.

•Elaborar un plan de las violaciones de seguridad más frecuentes que se presentan a nivel general.

ESTUDIO DEL CASO

De acuerdo con el S.O. y con las circunstancias que rodean el hecho se debe analizar si es conveniente o no apagar el equipo con los protocolo correspondientes para preservar la información como evidencia, en caso de determinar el apagado del equipo en Windows se procede de la siguiente manera:

Fotografiar la pantalla y anotar los programas en ejecución.
Retire cable de alimentación de la pared
Ahora bien, para realizar el procedimiento en los tres principales sistemas
operativos se procede como sigue:

En Linux:
Bajo la línea de comandos ejecutar el comando lsb_release a, este nos mostrará información acerca de la distribución, versión entre otros detalles.

ESTUDIO DEL CASO

Mac

Ir al menú Apple que se encuentra en la barra de menú, (lado superior izquierdo) dar clic y seleccionar la opción “Acerca de este Mac”, en ventana emergen – te va aparecer la identificación correspondiente al sistema instalado en el equipo.

Windows

Hacer clic en el botón Inicio, ir la opción Equipo y dar clic en esta, por ultimo hacer clic en Propiedades y listo, se puede ver la información detallado del SO.

ESTUDIO DEL CASO

Acciones para preservar la información

Para preservar la evidencia, se hace necesario que luego de haber obtenido la aprobación de la solicitud inicial de investigación del caso, se despeje y se asegure la escena del fraude o delito informático, velando porque no haya actores o factores externos que contaminen las pruebas a secuestrar para su posterior análisis forense. Se realice luego un registro detallado de la evidencia encontrada en el lugar, esto es; realizar una inspección visual por parte del perito informático forense quien tendrá la experiencia y experticia suficiente para determinar cuáles son los elementos que serán objeto de secuestro, cuáles serán los más importantes y cuales se considera pueden ayudar a esclarecer de manera contundente los hechos acaecidos en el suceso.

ESTUDIO DEL CASO

2. EL PROCEDIMIENTO Y ACCIONES REALIZADAS PARA CREAR LAS IMÁGENES DE DISCO DURO Y DISPOSITIVOS DE ALMACENAMIENTO ENCONTRADOS EN LA ESCENA.

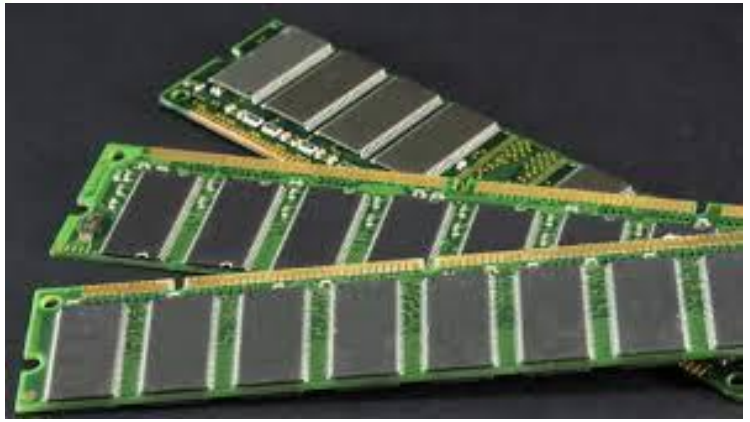
Para el caso de los discos duros: Es necesario el realizar una copia bit a bit de los dispositivos identificados en la fase anterior de identificación, esto con el fin de asegurar que los dispositivos originales no sean usados en el análisis forense y por ende mantener su pureza probatoria es decir que estos no sean contaminados durante la investigación.

ESTUDIO DEL CASO

Dichas copias se realizaran en dispositivos de almacenamiento externo CD, DVD, Discos Rígidos y de los cuales a estos últimos se les hará un formateo a bajo nivel. Estos serán comprobados en su integridad mediante el uso de funciones hash (MD5, SHA1) las cuales permitirán tener una copia fidedigna del original, se hace necesario tomar una copia el cual será el segundo original y el cual se conservara en un lugar altamente seguro atendiendo todos protocolos existentes para su salvaguarda y custodia. Luego de esta segunda copia original se generaran las dos copias necesarias para el análisis forense las cuales se nombraran como:

Copia A: Usada como SO principal y sobre el cual se realizaran pruebas de análisis forense con las herramientas dispuestas para tal fin.
Copia B: Usada como SO secundario y sobre el cual se analizaran los posibles ataques realizados desde la instalación inicial del SO pudiendo ver las posibles modificaciones y demás eventos hasta el día del ataque o suceso del incidente.

ESTUDIO DEL CASO



Para el caso de las memorias RAM:

Aunque la información de este dispositivo volátil es accesible y posible de recuperar, la información contenida en este, se recomienda no ser accedida mediante herramientas de acceso a la información del equipo en caliente. Pues, este factor haría que la simple visualización de un archivo o manipulación equivocada de un medio de comunicación del equipo en etapa de investigación forense, 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.

ESTUDIO DEL CASO

Para el caso de las memorias USB: Se puede aplicar al igual que el procedimiento de creación de imágenes para los discos duros y con la ayuda de herramientas de software forenses, la copia bit a bit de estos.

Adicional a los medios de almacenamiento encontrados en la escena del fraude, se hace necesario el acudir a otras fuentes de información complementarias en la investigación para dar más veracidad a los hallazgos y demás sucesos en el incidente reportado, entre estos está el tomar información de sistemas vivos como:

ESTUDIO DEL CASO

- Tomar y asegurar información de la cache del sistema.
- Tomar y asegurar registro de archivos temporales.
- Tomar y asegurar un registro de los sucesos del sistema.
- Tomar y asegurar un registro de eventos internos y externos de dispositivos de red tales como firewalls, servidores proxys, routers, modems entre otros.
- Tomar y asegurar un registro de Logs del sistema y aplicaciones del mismo.
- Tomar y asegurar las tablas de enrutamiento (ARP, Cache NetBios, Memoria, Kernel entre otros.
- Tomar y asegurar registros remotos de conexión y monitoreo.

ESTUDIO DEL CASO

3. CUALES ACCIONES SE APLICARÒN PARA DAR INICIO AL CASO DE INFORMÁTICA FORENSE.

Requisición o solicitud pericial: Este aspecto es el punto inicial de toda una investigación forense y es quizás la razón porque existen profesionales en las ramas de informática forense y seguridad informática en el mundo. Esta requisición o solicitud pericial hace referencia al planteamiento de una necesidad por parte de un afectado que ha sufrido un incidente informático, donde se han visto comprometidos sus intereses, datos y demás bienes valuados de una organización. Es el inicio de un proceso investigativo minucioso y riguroso que busca esclarecer las causas, consecuencias, móviles y demás actores involucrados en un hecho delictivo que ha puesto en riesgo la integridad de la información administrada por esta.

ESTUDIO DEL CASO

Entrevista con el cliente: Luego de haber obtenido la autorización por parte de quienes han solicitado y autorizado la apertura de investigación a un caso informático, es hora de realizar una entrevista con el interesado. La finalidad de esta, es recolectar toda la información posible sobre el caso a tratar y sobre los aspectos más relevantes que el investigador desee obtener.

ESTUDIO DEL CASO

Inspección ocular: Luego de haber realizado la entrevista inicial con el solicitante y previa autorización acordada para desplazarse, el investigador forense se traslada al sitio donde ocurrieron los hechos con el fin de realizar una inspección ocular justificada, documentando mediante procedimientos y herramientas, todo lo que considera es importante para su análisis e investigación.

La experiencia y experticia del investigador son cualidades que le han de permitir encontrar y validar la información obtenida tras el proceso evaluativo, estos factores serán decisivos a la hora de dar solución a un sin número de casos particulares, cuyos aspectos de fondo varían de uno a otro y cuyas similitudes distan de ser iguales entre sí.

ESTUDIO DEL CASO

Recolección de evidencias: El proceso de recolección de las evidencias es uno de los puntos más sensibles e importantes en el proceso de apertura y posterior análisis forense en un caso informático determinado. Este ayuda notablemente en la construcción de los hechos acaecidos y que circunscriben por qué ocurrió el incidente reportado, para este proceso es necesario acudir al uso de procedimientos, herramientas y demás actividades concernientes a la salvaguarda de los elementos probatorios del caso a investigar.

ESTUDIO DEL CASO

Acta de secuestro con soportes: En situaciones legales esta herramienta probatoria, permitirá demostrar ante la justicia y la ley, que los elementos secuestrados son vitales para el desarrollo del pro – ceso investigativo, por esto que; se hace necesario que se plasme en un documento firmado por quienes en el proceso de levantamiento de información intervinieron, las firmas, nombres, registros documentales, digitales, fílmicos y/o auditivos que hacen parte del acervo probatorio en la investigación forense informática.

ESTUDIO DEL CASO

Croquis ilustrativo: Como última acción para dar inicio al caso de análisis e investigación forense, se hace necesario realizar un dibujo adecuado, croquis, esquicio, esquicio panorámico, croquis con abatimiento, croquis en cruz, gráfico, esquema entre otros que el investigador forense desee aportar a la actividad de indagación, para plantear una hipótesis de sobre cuál fue el hecho ocurrido y de qué forma pudo haberse producido.

ESTUDIO DEL CASO

Este, es recomendable brinde algunos aspectos básicos que permitan su inclusión el proceso investigativo como lo son:

a. La fidelidad de este frente a la realidad observada.

b. La claridad de lo representado, pues; este debe representar de forma univoca los hechos posiblemente ocurridos para quienes no entienden o no estuvieron en el lugar.

c. La legibilidad que permite entender de manera acertada mediante dibujos y textos la finalidad de este croquis, y por último.

d. La nitidez que permite tener una visibilidad amena con la representación gráfica expuesta.