www.eysglobal.com

MÓDULO 1

TEMA 9: PRESERVACIÒN DE EVIDENCIAS PARTE 1

PRESERVACIÒN DE EVIDENCIAS

PRESERVACIÒN DE EVIDENCIAS

- Por **evidencia** entendemos cualquier dato o información que pueda ser utilizado para determinar o demostrar la veracidad, que prueba un hecho una vez realizado o bien que no ha sido realizado.
- Por **evidencia digital y electrónica** entendemos cualquier evidencia soportada en formato que se ha sido generada, transmitida, recibida por un dispositivo electrónico o informático que permiten archivar y reproducir la palabra, el sonido, la imagen y datos de cualquier otra clase.
- En definitiva son **campos magnéticos y pulsos electrónicos** que pueden ser recogidos y analizados usando técnicas y herramientas especiales

PRESERVACIÒN DE EVIDENCIAS

- En un mundo donde el uso de la redes de comunicaciones es cada vez es más intensivo (celulares, Internet, redes sociales y entornos 2.0 por poner algunos ejemplos) y, por lo tanto, donde las relaciones interpersonales se canalizan a través de medios electrónicos y telemáticos, es lógico que empiece a surgir la necesidad de probar o acreditar las actuaciones legítimas transferencias bancarias, declaraciones de impuestos….) o las conductas ilícitas de las que somos víctimas (fraudes informáticos como el PHISING, acosos a través de redes sociales, amenazas mediante SMS) en el formato en que se producen: el digital.

EVIDENCIA DIGITAL

Ahora se recibe un mensaje en el chat o un SMS en donde el componente digital o electrónico generan varios problemas:

1.- la manipulación (¿puede un juez estar completamente seguro de que el mensaje de datos que se le muestra no ha sido manipulado por el receptor?),

2.- **la volatilidad** (se puede borrar, perder, alterar) y cómo llevar ese mensaje de datos a un proceso con garantías de que no ha sido manipulado ante un Tribunal de Justicia

NECESIDAD DE LA PRUEBA

- La prueba dentro del proceso judicial es de especial importancia, ya que desde ella se confirma o desvirtúa una hipótesis o afirmación precedente, el objetivo del proceso conduce hacia la averiguación de la verdad formal.

METODOLOGÍA GENERAL DEL PROCEDIMIENTO DE EVIDENCIA DIGITAL

La metodología general del procedimiento de evidencia digital, se centra en 4 pasos principales ilustrados a continuación:

1. AISLAMIENTO DE LA ESCENA
Restringir el acceso a la zona del incidente, para evitar algún tipo de alteración en la posible evidencia a recolectar

2. IDENTIFICACIÓN DE FUENTES DE INFORMACIÓN
Los datos relacionados con un evento específico son identificados y evaluados a su vez que el incidente se controla, para posteriormente proceder con la fase de recolección y examinación

METODOLOGÍA GENERAL DEL PROCEDIMIENTO DE EVIDENCIA DIGITAL

3. EXAMINACIÓN Y RECOLECCIÓN DE INFORMACIÓN

Técnicas y herramientas forenses son aplicadas a los datos recolectados para extraer la información relevante, sin alterar la integridad de los datos

4. ANÁLISIS DE DATOS

Realiza el análisis de la información prioritaria o relevante obtenida en la fase de examinación y se centra en encontrar las respuestas para el caso, realizando la correlación de los eventos, archivos y diferentes datos

5. REPORTE

Reporte de los resultados del análisis que puede incluir los procedimientos que se llevaron a cabo, si quedaron verificaciones pendientes, mejoras,

VERIFICACIÓN Y CONFIRMACIÓN DEL INCIDENTE

Previo a la iniciación del procedimiento de evidencia digital, es necesario verificar que el evento que está siendo reportado, es realidad un incidente que atenta contra la confidencialidad, integridad o disponibilidad de la información. Esta labor es realizada en el proceso de evaluación y decisión de incidentes. Una vez se confirma la autenticidad, es necesario también determinar si dicho incidente requiere o no de un análisis forense (procedimiento de evidencia digital). Una vez se definen estas condiciones, se debe proceder con la primera fase.

FASE I. AISLAMIENTO DE LA ESCENA

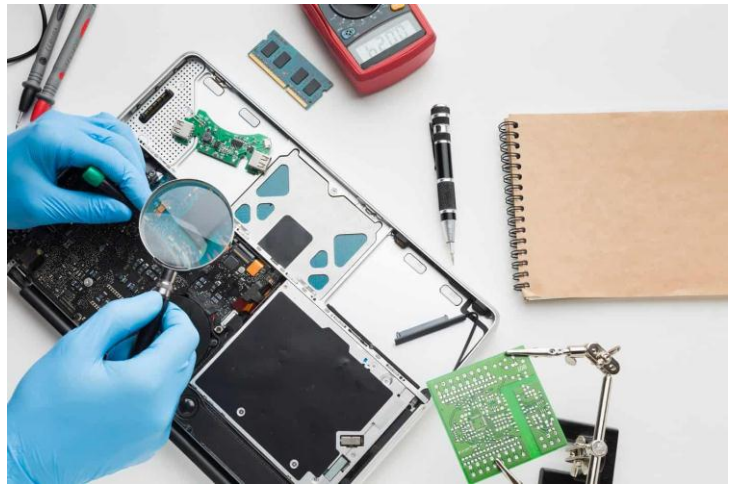
Una vez el evento reportado se cataloga como un incidente de seguridad de la información, es necesario restringir el acceso a la zona donde se produjo el incidente para evitar cualquier tipo de alteración o contaminación a la evidencia que pueda recolectarse para la posterior investigación.

CADENA DE CUSTODIA

vamos a volver a nombrar este tema y que hace parte fundamental del proceso de la preservación de evidencias como lo habíamos dicho en el tema 5, La cadena de custodia es un procedimiento que debe tenerse en cuenta desde el mismo instante que se decida realizar el proceso de evidencia forense, ya que este procedimiento, basado en el principio de la “mismidad”, tiene como fin garantizar la autenticidad e integridad de las evidencias encontradas en alguna situación determinada, es decir, que lo mismo que se encontró en la escena, es lo mismo que se está presentando al tribunal penal o comité disciplinario según sea el caso.

FUENTES DE INFORMACIÓN, PASOS INICIALES DE ADQUISICIÓN DE INFORMACIÓN

El primer paso a realizar para ejecutar la recolección de datos, es identificar fuentes potenciales de información de donde se puedan extraer datos para soportar el proceso de evidencia digital



ADQUISICIÓN DE DATOS

La adquisición de los datos debe realizarse teniendo en cuenta 3 pasos principales:

- **Planificación de la adquisición de datos:** Se debe planificar bien a que fuentes de información se les extraerá la información y el orden en el que se debe hacer teniendo en cuenta aspectos como, volatilidad de la información, complejidad para obtener los datos o por experiencia propia del analista.

ADQUISICIÓN DE DATOS

- **Adquisición de los datos :** El proceso general de recolección generalmente requiere del uso de herramientas forenses para copiar los datos volátiles y poderlos almacenar, así como también para adquirir la información de fuentes no volátiles. El proceso de recolección puede variar si es posible acceder localmente al sistema o si se puede hacer a través de la red.
- **Verificación de la integridad de los datos recolectados:** Una vez se recolectan los datos, se debe asegurar que la información mantiene su integridad y no ha sido modifica. Esto se puede realizar empleando herramientas de cálculo de resumen de mensajes que generan un valor determinado. Dicho valor debe ser igual tanto en la fuente original como en la copia. Esta verificación de integridad se utiliza principalmente para efectos legales, para que la información se certifique como auténtica