Reporte de inventario de eviencias

Natalia Galeano Valerio

Octubre 2019

1 La evidencia digital

La documentación de la evidencia en la escena es vital en el proceso investigativo. Se debe llevar un registro minucioso de todas las piezas de evidencia. Por ejemplo, documentos, dispositivos, programas, archivos digitales, o cualquier pieza relacionada con el caso. Esta evidencia debe ser procesada usando el protocolo de cadena de custodia donde se registrará los movimientos y características de la misma.

2 La cadena de custodia y la evidencia digital

El objetivo de la cadena de custodia es evitar la sustitución, manipulación, alteración, destrucción, contaminación y falsificación de la evidencia.Por eso la importancia de crear un cuestionario antes de evaluar la evidencia que incluya:

1. Qué tipo de evidencia digital ha sido colectada: Describir tipo de archivo, extensión, nombre, tamaño, lugar de adquisición y proceso de adquisición.
2. Identificar a las personas relacionadas con el uso de esa evidencia: Permitirá dar el seguimiento detallado de las personas que estuvieron involucradas en el manejo de la evidencia con nombres, agencia, horas y lugares.
3. Identificar los métodos usados en la adquisición de la evidencia digital: el software que se usó, características, preparación académica o técnica del investigador que manipuló el software, hardware donde estuvo instalado el software forense, método de adquisición, almacenamiento, transmisión y encriptación.
4. Determinar si a esa evidencia se accesó después: mediante la verificación del proceso de seguridad y autenticación de la evidencia usando la normativa SHA1-512 o MD5, para garantizar la fidelidad de la prueba.
5. Determinar cuándo fue colectada la evidencia y en dónde: Verificación decoordenadas satelitales de la ubicación de la evidencia en el proceso de manipulación y descripción de la zona horaria tanto del dispositivo como de la forma para garantizar su fidelidad.

El cuestionario anterior sirve para garantizar la calidad, autenticidad y seguridad de la evidencia. Además, las reglas en la adquisición de evidencia digital se fundamentará en dos puntos importantes:

1. Admisible: Un término usado para describir la evidencia que pueda ser considerada por un jurado o un juez en los casos civiles y penales.

2. Auténtica: Para confirmar la identidad de una entidad cuando se presenta esa identidad, para verificar la identidad de un usuario, dispositivo de usuario, u otra entidad.

Basandose en esas reglas, se deben cpnsiderar los siguientes puntos de seguridad:

1. Minimizar el uso desmedido de la evidencia para prevenir daños en la misma.

2. Uso de "Logs" en todo el proceso de la investigación.

3. Prepararse correctamente para el proceso de testimonio en la corte.

4. No apagar el sistema antes de colectar la evidencia.

5. No correr ningún programa adicional que afecte el sistema.

3 Cadena de custodia y la protección de la evidencia

Para la proteccion de la evidencia en la cadena de custodia se recomienda seguir los siguientes pasos:

1. 1. Identificación del origen

2. Identificación del destino

3. Seguridad y Proceso de transmisión

    - Método
    - Materiales

4. Consideraciones pre-salida de evidencia

    - Autorización para personal custodio
    - Carta de autorización que incluya: Nombre completo, grado, nombre agencia o laboratorio.
    - Tipo de identificación disponible: Incluya fotografía, y niveles de seguridad estandarizados y comprobados.

5. Descripción de la evidencia que se enviará

6. Punto de salida, ruta y punto de llegada
    - Nombre y título del agente o responsable que firma la carta
    - Inventario y descripción de la evidencia
7. Consideraciones con la envoltura o empaquetamiento
    - Verificar antes de enviar
    - Minimizar el riesgo de daño
    - Usar doble envoltura, y material antiestático, resistente al agua, humedad y otros factores ambientales
    - Marcar todo el paquete como evidencia
    - Agregar recibo con: Nombre Examinador, numero de ID, dirección y contenido recibido.
8. Consideración a la seguridad de envio
    - Información de Hardware o Software o Hash de los archivos, o imágenes
    - Incluya las claves en un sobre separado y sellado
    - No dejar la Evidencia en lugares no autorizados
    - Reportar cualquier incidente sospechoso y no abrir los materiales en ruta.
9. Consideraciones en el arribo de la evidencia:
    - Recibo de entrega, si se moviliza a otro lugar firma de reenvio.

4 Fuentes de evidencia

Algunos de los componentes de ciberneticos considerados fuentes de evidencia son los siguientes:

- Dispositivos de almacenamiento: Discos duros, flash drive, tarjetas móviles de almacenamiento o cualquier otro dispositivo que guarde información.
- Dispositivos electrónicos de procesamiento de información: Juegos electrónicos, tabletas, cámaras digitales, teléfonos celulares, GPS y demás dispositivos que procesen información.
- Comunicación de datos: Dispositivos de redes, servidores, base de datos, correo electrónico local, nubes con (sistemas de almacenamiento, sistemas virtualizados, servicios web y más) y demás servicios de transferencia y almacenamiento de información.
- Internet: Páginas web, redes sociales, y demás sitios privados o públicos que presenten información vinculada en una investigación.

5 Validación de evidencia digital

5.1 Evaluación de dispositivos y servicios

Si el dispositivo está apagado:

1. Documente y fotografíe dispositivos y cables conectados al equipo.
2. Etiquete todos los cables y dispositivos que almacenan evidencia digital
3. Verifique si existe unidades de almacenamiento dentro de los dispositivos como CD, DVD, USB y más, los cuales deben ser sellados con TAPE de evidencia.
4. Grabar modelo, marca, número de serie, y marcas distintivas del equipo.
5. Sella con tape los puertos USB y conector de Energía.
6. Empaquetar los dispositivos de acuerdo a los protocolos de fabricantes de hardware para la prevención de daños en la transportación.

Cuando el dispositivo esté prendido:

1. Identificar la información que muestre la pantalla.
2. Requerir asistencia a personal con experiencia en captura y preservación de información volátil.
3. Verificar si existe indicios que muestren alguna actividad sospechosa del sistema estableciéndose que el equipo fue borrado o formateado.
4. Verificar si existe indicios que muestren alguna actividad sospechosa del sistema estableciéndose que el equipo fue borrado o formateado.
5. Desconectar el equipo si el mismo está borrándose o formateando el sistema de almacenamiento.

5.2 Empaquetamiento del dispositivo electrónico y/o la evidencia digital

1. Toda evidencia digital debe empaquetarse en fundas y recipientes antiestáticos.
2. No se debe usar fundas plásticas ya que producen estática, permite humedad y condensación.
3. Los empaques de evidencia digital deben prevenir: rayones, golpes, movimientos bruscos.
4. Los dispositivos electrónicos móviles deben mantenerse como se encontraron, apagados o prendidos.

5.3 Traslado del dispositivo electrónico y/o evidencia digital

1. Mantener la evidencia digital lejos de campos magnéticos, como los producidos por emisoras de radio, los imanes de los altavoces y magnéticos de luces de emergencia.
2. No mantener la evidencia en el vehículo por prolongados transcursos de tiempo.
3. Prevenir la caída y vibración de los equipos especialmente dispositivos de almacenamiento externos o internos.
4. Usar la técnica de validación y seguridad de evidencia digital.

5.4 Almacenamiento de dispositivo electrónico y/o evidencia digital

1. Estar seguro de que la evidencia digital fue inventariada correctamente.
2. Asegurarse de que la evidencia digital es guardada en un lugar seguro, que incluya un sistema de climatización, ya que la evidencia digital no está sujeta a extremas temperaturas y humedad.
3. Establecer el principio de validación y seguridad de evidencia digital.

6 Inventario de envidencias

En términos de lo que contiene una cadena de custodia adecuada, hay varias secciones cada una con sus propios detalles que deben proporcionarse.

6.1 Detalles del dispositivo electrónico

1. Numero de item: Se debe incluir un número de item único en el formulario.
2. Descripción: Esta debe ser una descripción general del artículo. Esta puede ser una declaración simple, como un disco duro SATA de 500 GB.
3. Fabricante: Este detalle ayuda en el caso de múltiples pruebas con fabricantes potencialmente diferentes.
4. Modelo: Esto detalla más la evidencia específica para la separación posterior si es necesario.
5. Numero de serie: Esta es una pieza crítica en el caso de que un incidente involucre una cantidad de sistemas con exactamente la misma configuración.

6.2 Cadena de custodia

1. Numero de rastreo: Este número indica el paso en el ciclo de vida que tomó la evidencia.

2. Fecha y Hora: Esta es una información crítica en cualquier cadena de custodia y se aplica por igual a cada paso que tomaron las pruebas. Esto permite que cualquiera que vea la cadena de custodia pueda reconstruir hasta cada minuto cada paso en el ciclo de vida de la cadena de custodia.

3. De y Para: Estos campos pueden ser una persona o un lugar de almacenamiento.

4. Motivo: Mover una pieza de evidencia nunca debe hacerse sin una razón. En esta parte de la cadena de custodia, se completa el motivo.