ANEXO C

ANEXO C

Presentación de la evidencia digital

El último paso que debemos realizar del proceso de investigación es la presentación de la información recopilada como evidencia, esta consiste en la elaboración del informe con los resultados obtenidos en cada una de las etapas de la investigación. El informe que presentemos debe ser totalmente imparcial sin mostrar una sentencia de conducta del acusado, esto puede llevar a que su trabajo sea descalificado.

El investigador es el responsable de todo lo señalado y expuesto en el informe de resultados del análisis de la exanimación de la evidencia digital.

La eficacia para probar la investigación realizada se basa fundamentalmente en el aseguramiento de la prueba desde el momento de su secuestro en este caso desde el día que ponemos las manos sobre la máquina a investigar, de aquí en mas todas las manipulaciones que se den a esta máquina serán en copias autentificadas para así no correr riesgos de alteración de la información.

Expuesta esta situación debemos tener muy en cuenta cómo debemos presentar un informe sobre la investigación de tal manera que sea, objetiva, precisa y que contenga suficientes argumentos que determinen la fiabilidad de la investigación. A continuación exponemos algunas consideraciones esenciales para la presentación del informe:

1. Debe ser Admisible, es decir debe tener 3 aspectos importantes que son:

    - Autenticidad: Evidencia relacionada con el caso y no alterada
    - Confiabilidad: Forma de registro comprobable

- Eficacia: Correlación de eventos

2. Criterio de razonabilidad

El poder dar un criterio de la investigación tan razonable como entendible.

3. Cuál es el fin de la investigación El fin de la investigación es brindar al afectado las pruebas suficientes para que pueda decidir con certeza sobre el asunto del proceso.

Al igual que un documento normal, la presentación de la evidencia digital debe cumplir las siguientes condiciones:

- Debe estar compuesto por un texto.

Con un contenido relevante al ámbito jurídico.

- Un autor:

Este debe estar claramente identificado

- Debe ser comprensible: El texto debe contener un lenguaje apropiado y comprensible.
- Detalles de resultados: Esta sección debe describir en mayor detalle los resultados de las exanimaciones y puede incluir:
  - Archivos específicos relacionados con la petición.
  - Otros archivos, incluyendo los archivos suprimidos, que utilizan los resultados.
  - Búsquedas de cadena, búsquedas de palabra clave, y búsquedas de cadena de texto.
  - Evidencia relacionada con internet, tal como análisis de tráfico del Web site, archivos de la memoria inmediata, E-mail, y actividad del grupo de las noticias.
  - Análisis de imágenes, gráficos.
  - Materiales que utilizan: Enumere los materiales y procesos que utilizó, que se incluyen con el informe, de las copias digitales de la evidencia, y del encadenamiento de la documentación de la custodia.

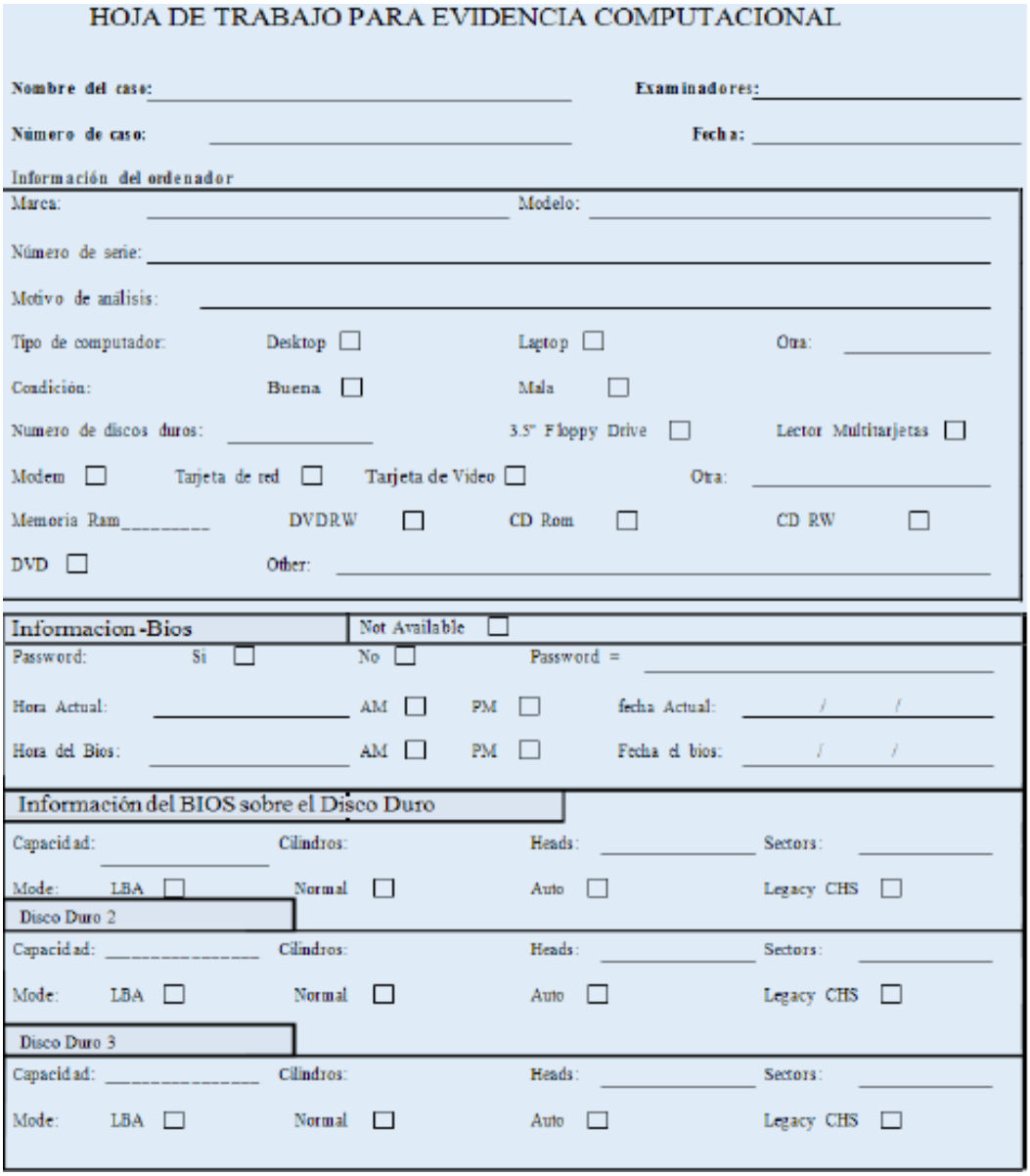
- Glosario: Se puede incluir un glosario para asistir al programa de lectura en entender cualquier término tecnológico usado. Utilice una fuente generalmente aceptada para la definición de los términos e incluya las referencias apropiadas.

Documentación

Dentro del proceso de análisis debemos utilizar un sin número de documentos que nos respaldaran al momento de presentar los resultados de la investigación.

A continuación presentamos algunos que deberemos realizar durante el proceso de un análisis forense.

Empezamos con una hoja de trabajo que debemos llenar al iniciar la investigación:



HOJA DE TRABAJO PARA EVIDENCIA COMPUTACIONAL

Nombre del caso: _____ **Examinadores:** _____

Número de caso: _____ **Fecha:** _____

Información del ordenador

Marca: _____ Modelo: _____

Número de serie: _____

Motivo de análisis: _____

Tipo de computador: Desktop ☐ Laptop ☐ Otra: _____

Condición: Buena ☐ Mala ☐

Numero de discos duros: _____ 3.5" Floppy Drive ☐ Lector Multitarjetas ☐

Modem ☐ Tarjeta de red ☐ Tarjeta de Video ☐ Otra: _____

Memoria Ram_____ DVDRW ☐ CD Rom ☐ CD RW ☐

DVD ☐ Other: _____

Informacion -Bios — Not Available ☐

Password: Si ☐ No ☐ Password = _____

Hora Actual: _____ AM ☐ PM ☐ fecha Actual: / /

Hora del Bios: _____ AM ☐ PM ☐ Fecha d bios: / /

Información del BIOS sobre el Disco Duro

Capacidad: _____ Cilindros: Heads: _____ Sectors: _____

Mode: LBA ☐ Normal ☐ Auto ☐ Legacy CHS ☐

Disco Duro 2

Capacidad: _____ Cilindros: Heads: _____ Sectors: _____

Mode: LBA ☐ Normal ☐ Auto ☐ Legacy CHS ☐

Disco Duro 3

Capacidad: _____ Cilindros: Heads: _____ Sectors: _____

Mode: LBA ☐ Normal ☐ Auto ☐ Legacy CHS ☐

Firmas de constancia:

_____ _____

Atte. Atte.

Otro documento que debemos llevar es el que detalla objetos expuestos junto al computador. Este lo realizamos al momento del secuestro del equipo.

Serie /Modelo	Tipo	Donde fue encontrado

Al momento de tener los datos anteriores que son previos al análisis, entramos a ver la documentación que utilizaremos durante la investigación.

El siguiente formulario contiene detalles del análisis sobre un disco duro en el que hemos trabajado.

Hoja Trabajo de Evidencia del Disco Duro

Nombre de caso: _____ Examinadores: _____

Número de caso: _____ Fecha: _____

Disco Duro 1☐ - 2☐ - 3☐. Etiqueta de Información. (No Disponibles☐)

Manufacturado: _____
Modelo: _____
Número serial: _____
Capacidad: _____ Cilindros: _____
Heads: _____ Sectores: _____
Control Rev: _____

IDE: ☐ ____Pin SCSI☐ SATA : ☐ Otro: _____

Jumper: Master ☐ Slave ☐ Clave Select ☐ No determinado ☐

Parámetros de Información del Disco

Software utilizado:

Capacidad: _____ Cilindros: _____ Heads: _____ Sectores: _____

LBA : _____ Capacidad de Disco formateado: _____

Nombre de Volumen: _____

Particiones:

Nombre	Booteable	Inicio	Finalización	Tipo
	☐			
	☐			
	☐			
	☐			

Información de la imagen de disco

Software Utilizado:_____

Método utilizado: Raw ☐ SMART ☐ E01 ☐ Otro:_____

Información de la Plataforma de Análisis

Sistema Operativo usado: _____ Versión:_____

Software de análisis Utilizado: _____ Versión: _____

Después del trabajo se Mantuvo la integridad de la imagen Si ☐ No ☐

Lista de software Utilizado

Software / comandos	Versión	Trabajo realizado

Responsables:

_____ _____

Atte. Atte.

Como se estudio en uno de los capítulos la cadena de custodia es sumamente importante debiendo detallar paso a paso lo desarrollado en el análisis. Aquí un formulario que nos puede ser útil para este trabajo.

Hoja Trabajo para cadena de Custodio

Nombre de caso: _____ Examinadores: _____

Número de caso: _____ Fecha: _____

Tipo de dispositivo: _____ Número de Serie: _____

Modelo: _____ Marca: _____

Fecha	Hora	Software Utilizado	Datos encontrados	Observaciones