SSA SERVIDET SOLUCIONES AVANZADAS

Asociación sosdesaparecidos
Asociación de ayuda y difusión de casos de personas desaparecidas.

INFORMÁTICA FORENSE

Guía de actuación con evidencias tecnólogicas EN DESAPARECIDOS

Presentamos esta “Guía de actuación con evidencias tecnológicas en Desaparecidos” elaborada por la firma Servidet Soluciones Avanzadas que colabora habitualmente con nuestra Asociación Sosdesaparecidos y a la vez también con el despacho de criminología DACRIM.

Sabemos que en la actualidad es sumamente importante la INFORMATICA FORENSE en el espacio de los Desaparecidos y la investigación correspondiente.

Esta guía es una ayuda más de información para las familias de desaparecidos que se suma a las dos anteriores, la *Guía Odiseo para las familias frente a los medios de comunicación* y la *Guía para familiares de personas desaparecidas.*

Todas estas guías pueden descargarse en nuestra página web http://sosdesaparecidos.es/

ÍNDICE

INFORMÁTICA FORENSE

La informática forense es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

Dichas técnicas incluyen reconstruir el bien informático, examinar datos residuales, autenticar datos y explicar las características técnicas del uso aplicado a los datos y bienes informáticos.

Como la definición anterior lo indica, esta disciplina hace uso no solo de tecnologías de punta para poder mantener la integridad de los datos y del procesamiento de los mismos; sino que también requiere de una especialización y conocimientos avanzados en materia de informática y sistemas para poder detectar dentro de cualquier dispositivo electrónico lo que ha sucedido.

El conocimiento del informático forense abarca el conocimiento no solamente del software si no también de hardware, redes, seguridad, hacking, cracking, recuperación de información.

La informática forense ayuda a detectar pistas sobre ataques informáticos, robo de información, conversaciones o pistas de emails, chats.

La importancia de éstos y el poder mantener su integridad se basa en que la evidencia digital o electrónica es sumamente frágil. El simple hecho de darle doble clic a un archivo modificaría la última fecha de acceso del mismo.

Adicionalmente, un examinador forense digital, dentro del proceso de informática forense puede llegar a recuperar información que haya sido borrada desde el sistema operativo.

La infraestructura informática a analizar puede ser toda aquella que tenga una Memoria (informática), por lo que se incluyen los siguientes dispositivos:

- Disco duro de un o Servidor
- Documentación referida del caso.
- Tipo de Sistema de Telecomunicaciones
- Información Electrónica MAC address
- Logs de seguridad.
- Información de Firewalls
- IP, redes Proxy. lmhost, host, Crossover, pasarelas
- Software de monitoreo y seguridad
- Credenciales de autentificación
- Trazo de paquetes de red.
- Teléfono Móvil o Tablets
- Agendas Electrónicas (PDA)
- Dispositivos de GPS.
- Impresora
- Memoria USB
- Bios

FASE DE IDENTIFICACIÓN

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:

1. ¿Qué información se necesita?
2. ¿Cómo aprovechar la información presentada?
3. ¿En qué orden ubico la información?
4. ¿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
- Información General
- Información Sobre El Equipo Afectado

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

Etapa 3: 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
- Modo de almacenamiento

FASE DE VALIDACIÓN Y PRESERVACIÓN

En esta fase, es imprescindible definir los métodos adecuados para el almacenamiento y etiquetado de las evidencias. Una vez que se cuenta con todas las evidencias del incidente es necesario conservarlas intactas ya que son las "huellas del crimen", se deben asegurar estas evidencias a toda costa. Para ello se sigue el siguiente proceso:

Etapa 1: Copias de la evidencia.

Como primer paso se debe realizar dos copias de las evidencias obtenidas, generar también una suma de comprobación de la integridad de cada copia mediante el empleo de funciones hash tales como MD5 o SHA1. Incluir estas firmas en la etiqueta de cada copia de la evidencia sobre el propio medio de almacenamiento como CD o DVD etiquetando la fecha y hora de creación de la copia, nombre cada copia, por ejemplo "Copia A", "Copia B" para distinguirlas claramente del original.

Etapa 2: Cadena de custodia

Otro aspecto muy importante es la cadena de custodia, donde se establecen las responsabilidades y controles de cada una de las personas que manipulen la evidencia. Se debe preparar un documento en el que se registren los datos personales de todos los implicados en el proceso de manipulación de las copias, desde que se tomaron hasta su almacenamiento.

FASE DE ANÁLISIS

El Análisis Forense cuyo objetivo es reconstruir con todos los datos disponibles la línea temporal del ataque, determinando la cadena de acontecimientos que tuvieron lugar desde el inicio del ataque, hasta el momento de su descubrimiento.

Este análisis se dará por concluido cuando se descubra cómo se produjo el ataque, quién o quienes lo llevaron a cabo, bajo qué circunstancias se produjo, cuál era el objetivo del ataque, qué daños causaron.

En el proceso de análisis se emplean las herramientas propias del sistema operativo (anfitrión) y las que se prepararon en la fase de extracción y preparación.

FASE DE DOCUMENTACIÓN Y PRESENTACIÓN DE LAS PRUEBAS

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.

Etapa 1: Utilización de formularios de registro del incidente

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.

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, entre tres y cinco, y será de especial interés para exponer lo sucedido al personal no especializado en sistemas tecnológicos.

DISPOSITIVOS INFORMÁTICOS

Para realizar un análisis informático forense es imprescindible contar con el equipamiento necesario, no solo para investigar sino también para proteger la integridad de los dispositivos a analizar, de forma que sigan siendo válidos como prueba judicial.

El uso que se da diariamente a los equipos informáticos pueden arrojarnos mucha información en casos de desapariciones sobre todo en búsquedas en internet, correos electrónicos, mensajería instantánea o movimientos.

La información que se puede recuperar del disco duro que contiene el equipo informático, dependerá del uso que tenga debido a la sobre-escritura que se produce en el mismo.

Se puede recuperar información en algunos casos hasta desde el 1º que se inicio el equipo informático o los siguientes ejemplos :

- Archivos borrados
- Dispositivos USB insertados
- Paginas visitadas
- Descargas
- Correos electrónicos
- Cookies instaladas
- Imágenes descargadas, visualizadas y borradas
- Documentos creados, editados y visualizados
- Línea de tiempo con información de uso por horas

DISPOSITIVOS MÓVILES

Como bien todos sabemos porque esto es totalmente notable los Smartphone se han vuelto una herramienta más que indispensable de comunicación para los seres humanos, tanto que al día de hoy estos dispositivos móviles son usados no solo para realizar llamadas sino además para tener acceso a internet, enviar mensajes, recibir y enviar cualquier tipo de archivos.

En este proceso de adquisición de datos podemos analizar cualquier dispositivos móvil independientemente que sea Android, IOS, Windows Phone o cualquier otro sistema operativo del smartphone.

Se puede recuperar información como detallamos en el siguiente ejemplo :

- Registros de llamadas, incluso historiales borrados
- Contactos
- Datos del teléfono (IMEI/ESN, nº de teléfono)
- ICCID e IMSI
- Fotografías y videos
- Wathsapp o conversaciones en otras app (Line, Viber, Facebook, etc…)
- Archivos de sonido
- Información de localización de la SIM: TMSI, MCC, MNC.

BUENAS PRÁCTICAS PARA CASOS DE DESAPARECIDOS

Ante todo debemos de mantener la calma y utilizar el sentido común para dejarnos guiar por los profesionales de los cuerpos y fuerzas de seguridad del estado, atendiendo en todo momento a sus indicaciones.

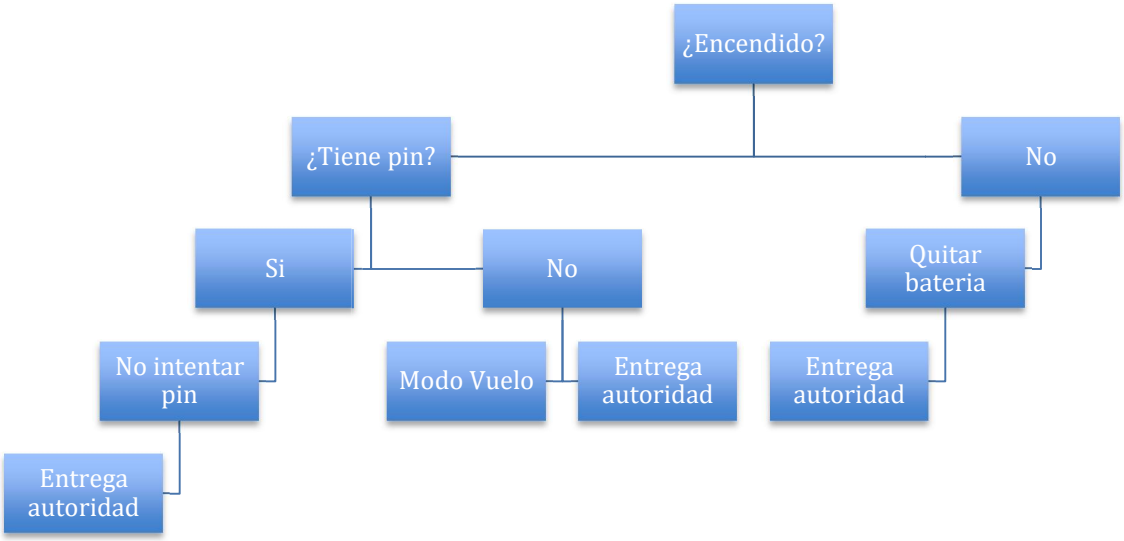
Estas son algunas de las recomendaciones más importantes que los familiares de desaparecidos deben seguir**:**

- **No debemos** de encender dispositivos para ver información. (Solo con arrancar un dispositivo podemos perder información muy valiosa ña cual posteriormente nos será imposible recuperar en su totalidad)

- **Prestar especial atención** a todo el entorno donde se encuentran los dispositivos telemáticos (Notas con claves, CD's, pendrive, etc…) es de vital importancia entregar todo a los investigadores.

- **No debemos** introducir patrones o contraseñas de bloqueo podríamos perder la información del dispositivo de forma definitiva.

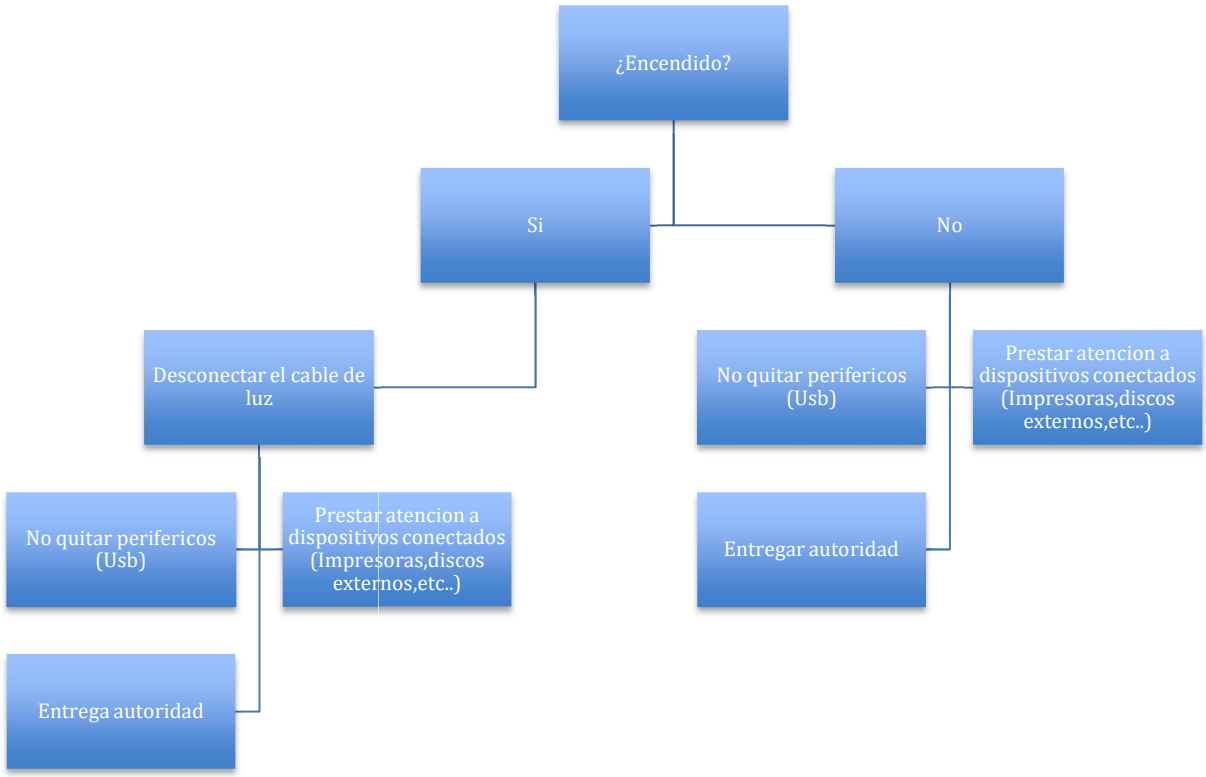
ESQUEMA EN DISPOSITIVOS MÓVILES



IMPORTANTE

- Mantener los complementos que el dispositivo pueda tener, como tarjeta SIM o tarjeta SD.
- Nunca intentar introducir el código PIN, la tarjeta SIM o patrones de desbloqueo en los dispositivos
- No intentar acceder al dispositivo o recuperar información. Esto puede ser muy negativo al causar sobre-escritura de archivos y resultar totalmente imposible una recuperación de datos posterior.

ESQUEMA EN DISPOSITIVOS INFORMÁTICOS



IMPORTANTE

- Nunca intentar acceder o arrancar el dispositivo informático
- Bajo ningún concepto intentar instalar y recuperar datos con un software específico para ello. Esto podría sobre-escribir datos irrecuperables.