Manual de Manejo de Evidencias Digitales y Entornos Informáticos. Versión 2.0

Dr. Santiago Acurio Del Pino
Director Nacional de Tecnología de la Información

1.- Importancia

Increíblemente los delincuentes hoy están utilizando la tecnología para facilitar el cometimiento de infracciones y eludir a las autoridades. Este hecho ha creado la necesidad de que tanto la Policía Judicial, la Fiscalía General del Estado y la Función Judicial deba especializarse y capacitarse en estas nuevas áreas en donde las TICs[1] se convierten en herramientas necesarias en auxilio de la Justicia y la persecución de delito y el delincuente.

La obtención de Información (elementos de convicción) se constituye en una de las facetas útiles dentro del éxito de en una investigación criminal, aspecto que demanda de los investigadores encargados de la recolección preservación, análisis y presentación de las evidencias digitales una eficaz labor que garantice la autenticidad e integridad de dichas evidencias, a fin de ser utilizadas posteriormente ante el Tribunal Penal.

2.- Objetivo del Manual

La prueba dentro del proceso penal es de especial importancia, ya que desde ella se confirma o desvirtúa una hipótesis o afirmación precedente, se llega a la posesión de la verdad material.

[1] Tecnologías de la Información y la Comunicación

De esta manera se confirmará la existencia de la infracción y la responsabilidad de quienes aparecen en un inicio como presuntos responsables, todo esto servirá para que el Tribunal de Justicia alcance el conocimiento necesario y resuelva el asunto sometido a su conocimiento.

El objetivo de la Informática forense es el de recobrar los registros y mensajes de datos existentes dentro de un equipo informático, de tal manera que toda esa información digital, pueda ser usada como prueba ante un tribunal.

El presente Manual pretende ser una guía de actuación para miembros de la Policía Judicial a si como de los Funcionarios de la Fiscalía, cuando en una escena del delito se encuentren dispositivos Informáticos o electrónicos que estén relacionados con el cometimiento de una infracción de acción pública.

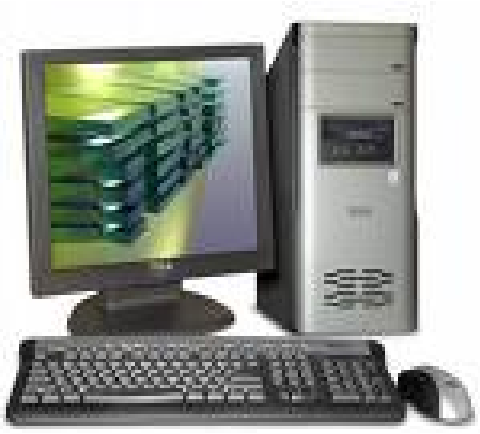
3.- Principios Básicos

1. El funcionario de la Fiscalía o de la Policía Judicial nunca debe acudir solo al lugar de los hechos, este tipo de actividad debe ser realizada como mínimo por dos funcionarios. Un segundo funcionario, por un lado, aporta seguridad personal y, por otro, ayuda a captar más detalles del lugar de los hechos. Los funcionarios deberían planear y coordinar sus acciones. Si surgen problemas inesperados, es más fácil resolverlos porque “dos cabezas piensan más que una.
2. Ninguna acción debe tomarse por parte de la Policía Judicial, la Fiscalía o por sus agentes y funcionarios que cambie o altere la información almacenada dentro de un sistema informático o medios magnéticos, a fin de que esta sea presentada fehacientemente ante un tribunal.
3. En circunstancias excepcionales una persona competente puede tener acceso a la información original almacenada en el sistema informático objeto de la investigación, siempre que después se explique detalladamente y de manera razonada cual fue la forma en la que se produjo dicho acceso, su justificación y las implicaciones de dichos actos.
4. Se debe llevar una bitácora de todos los procesos adelantados en relación a la evidencia digital. Cuando se hace una revisión de un caso por parte de una tercera parte ajena al mismo, todos los archivos y registros de dicho caso y el proceso aplicado a la evidencia que fue recolectada y preservada, deben permitir a esa parte recrear el resultado obtenido en el primer análisis.
5. El Fiscal del Caso y/o el oficial a cargo de la investigación son responsables de garantizar el cumplimiento de la ley y del apego a estos principios, los cuales se aplican a la posesión y el acceso a la información almacenada en el sistema informático. De igual forma debe asegurar que cualquier persona que acceda a o copie dicha información cumpla con la ley y estos principios.

4.- Principios del Peritaje

1. **OBJETIVIDAD:** El perito debe ser objetivo, debe observar los códigos de ética profesional.
2. **AUTENTICIDAD Y CONSERVACIÓN**: Durante la investigación, se debe conservar la autenticidad e integridad de los medios probatorios
3. **LEGALIDAD:** El perito debe ser preciso en sus observaciones, opiniones y resultados, conocer la legislación respecto de sus actividad pericial y cumplir con los requisitos establecidos por ella
4. **IDONEIDAD:** Los medios probatorios deben ser auténticos, ser relevantes y suficientes para el caso.
5. **INALTERABILIDAD:** En todos los casos, existirá una cadena de custodia debidamente asegurada que demuestre que los medios no han sido modificados durante la pericia.
6. **DOCUMENTACIÓN:** Deberá establecerse por escrito los pasos dados en el procedimiento pericial

Estos principios deben cumplirse en todas las pericias y por todos los peritos involucrados



5.- Reconocimiento de la Evidencia Digital

Es importante clarificar los conceptos y describir la terminología adecuada que nos señale el rol que tiene un sistema informático dentro del *iter criminis* o camino del delito. Esto a fin de encaminar correctamente el tipo de investigación, la obtención de indicios y posteriormente los elementos probatorios necesarios para sostener nuestro caso. Es así que por ejemplo, el procedimiento de una investigación por homicidio que tenga relación con evidencia digital será totalmente distinto al que, se utilice en un fraude informático, por tanto el rol que cumpla el sistema informático determinara DONDE DEBE SER UBICADA Y COMO DEBE SER USADA LA EVIDENCIA.

Ahora bien para este propósito se han creado categorías a fin de hacer una necesaria distinción entre el elemento material de un sistema informático o hardware (*evidencia electrónica*) y la información contenida en este (*evidencia digital*). Esta distinción es útil al momento de diseñar los procedimientos adecuados para tratar cada tipo de evidencia y crear un paralelo entre una escena física del crimen y una digital. En este contexto el hardware se refiere a todos los componentes físicos de un sistema informático, mientras que la información, se refiere a todos los datos, programas almacenados y mensajes de datos trasmitidos usando el sistema informático.

5.1.- Hardware o Elementos Físicos

SISTEMA INFORMÁTICO	
HARDWARE (Elementos Físicos)	**Evidencia Electrónica**
• El hardware es mercancía ilegal o fruto del delito.	• El hardware es una mercancía ilegal cuando su posesión no está autorizada por la ley. Ejemplo: en el caso de los decodificadores de la señal de televisión por cable, su posesión es una violación a los derechos de propiedad intelectual y también un delito. • El hardware es fruto del delito cuando este es obtenido mediante robo, hurto, fraude u otra clase de infracción.
• El hardware es un instrumento	• Es un instrumento cuando el hardware cumple un papel importante en el cometimiento del delito, podemos decir que es usada como un arma o herramienta, tal como una pistola o un cuchillo. Un ejemplo serían los snifers y otros aparatos especialmente diseñados para capturar el tráfico en la red o interceptar comunicaciones.
• El hardware es evidencia	• En este caso el hardware no debe ni ser una mercancía ilegal, fruto del delito o un instrumento. Es un elemento físico que se constituye como prueba de la comisión de un delito. Por ejemplo el scanner que se uso para digitalizar una imagen de pornografía infantil, cuyas características únicas son usadas como elementos de convicción

5.2.- Información

SISTEMA INFORMÁTICO	
INFORMACIÓN	**Evidencia Digital**
• La información es mercancía ilegal o el fruto del delito.	La información es considerada como mercancía ilegal cuando su posesión no está permitida por la ley, por ejemplo en el caso de la pornografía infantil. De otro lado será fruto del delito cuando sea el resultado de la comisión de una infracción, como por ejemplo las copias pirateadas de programas de ordenador, secretos industriales robados.

SISTEMA INFORMÁTICO	
INFORMACIÓN	**Evidencia Digital**
• La información es un instrumento	La información es un instrumento o herramienta cuando es usada como medio para cometer una infracción penal. Son por ejemplo los programas de ordenador que se utilizan para romper las seguridades de un sistema informático, sirven para romper contraseñas o para brindar acceso no autorizado. En definitiva juegan un importante papel en el cometimiento del delito.
• La información es evidencia	Esta es la categoría más grande y nutrida de las anteriores, muchas de nuestras acciones diarias dejan un rastro digital. Uno puede conseguir mucha información como evidencia, por ejemplo la información de los ISP's, de los bancos, y de las proveedoras de servicios las cuales pueden revelar actividades particulares de los sospechosos

5.3.- Clases de Equipos Informáticos y Electrónicos

Algunas personas tienden a confundir los términos evidencia digital y evidencia electrónica, dichos términos pueden ser usados indistintamente como sinónimos, sin embargo es necesario distinguir entre aparatos electrónicos como los celulares y PDAs y la información digital que estos contengan. Esto es indispensable ya que el foco de nuestra investigación siempre será la evidencia digital aunque en algunos casos también serán los aparatos electrónicos.

A fin de que los investigadores forenses tengan una idea de dónde buscar evidencia digital, éstos deben identificar las fuentes más comunes de evidencia. Situación que brindará al investigador el método más adecuando para su posterior recolección y preservación.

Las fuentes de evidencia digital pueden ser clasificadas en tres grande grupos:

1. **SISTEMAS DE COMPUTACIÓN ABIERTOS**, son aquellos que están compuestos de las llamadas computadores personales y todos sus periféricos como teclados, ratones y monitores, las computadoras portátiles, y los servidores. Actualmente estos computadores tiene la capacidad de guardar gran cantidad de información dentro de sus discos duros, lo que los convierte en una gran fuente de evidencia digital.
2. **SISTEMAS DE COMUNICACIÓN,** estos están compuestos por las redes de telecomunicaciones, la comunicación inalámbrica y el Internet. Son también una gran fuente de información y de evidencia digital.
3. **SISTEMAS CONVERGENTES DE COMPUTACIÓN,** son los que

están formados por los teléfonos celulares llamados inteligentes o SMARTPHONES, los asistentes personales digitales PDAs, las tarjetas inteligentes y cualquier otro aparato electrónico que posea convergencia digital y que puede contener evidencia digital.

Dada la ubicuidad de la evidencia digital es raro el delito que no esté asociado a un mensaje de datos guardado y trasmitido por medios informáticos. Un investigador entrenado puede usar el contenido de ese mensaje de datos para descubrir la conducta de un infractor, puede también hacer un perfil de su actuación, de sus actividades individuales y relacionarlas con sus víctimas.

Ejemplos de aparatos electrónicos e informáticos

- Computador de escritorio
- Computador Portátil
- Estación de Trabajo
- Hardware de Red
- Servidor – *aparato que almacena o transfiere datos electrónico por el Internet*
- Teléfono celular
- Teléfono inalámbrico
- Aparato para identificar llamadas
- Localizador - *beeper*
- "GPS" – *aparato que utiliza tecnología satélite capaz de ubicar geográficamente al persona o vehículo que lo opera*
- Cámaras, videos
- Sistemas de seguridad
- Memoria "flash" – *Pequeño dispositivo que puede conservar hasta 4 gigabytes de datos o 4,000,000,000 bytes de información*
- "Palm" – *asistente personal electrónico que almacena datos y posiblemente tiene conectividad inalámbrica con el Internet*
- Juegos electrónicos – *en su unidad de datos se puede guardar, incluso, una memoria de otro aparato*
- Sistemas en vehículos – *computadoras obvias y computadoras del sistema operativo del vehículo que registra cambios en el ambiente y el mismo vehículo*
- Impresora
- Copiadora
- Grabadora
- Videograbadora, DVD
- Duplicadora de discos
- Discos, disquetes, cintas magnéticas
- Aparatos ilícitos – *tales como los aparatos que capturan el número celular de teléfonos cercanos para después copiarlo en otros teléfonos, o los llamados sniffers, decodificadores, etc.*

5.4.- Incautación de Equipos Informáticos o Electrónicos

Si el investigador presume que existe algún tipo evidencia digital en algún aparato electrónico o en algún otro soporte material relacionado con el cometimiento de una infracción. Este debe

pedir la correspondiente autorización judicial para incautar dichos elementos, de igual forma debe tener la autorización judicial para acceder al contenido guardado, almacenado y generado por dichos aparatos.

Antes de realizar un allanamiento e incautación de Equipos Informáticos o Electrónicos se debe tomar en cuenta lo siguiente:

1. ¿A qué horas debe realizarse?
   - Para minimizar destrucción de equipos, datos
   - El sospechoso tal vez estará en línea
   - Seguridad de investigadores
2. Entrar sin previo aviso
   - Utilizar seguridad
   - Evitar destrucción y alteración de los equipos, o la evidencia contenida en esta.
3. Materiales previamente preparados (Cadena de custodia)
   - Embalajes de papel
   - Etiquetas
   - Discos y disquetes vacíos
   - Herramienta
   - Cámara fotográfica
4. Realizar simultáneamente los allanamientos e incautación en diferentes sitios
   - Datos pueden estar en más de un lugar, sistemas de red, conexiones remotas.
5. Examen de equipos
6. Aparatos no especificados en la orden de allanamiento
7. Creación de Respaldos en el lugar, creación de imágenes de datos.
   - Autorización para duplicar, reproducir datos encontrados (por ejemplo, un aparato contestador)
8. Fijar/grabar la escena
   - Cámaras, videos, etiquetas
9. Códigos/claves de acceso/contraseñas
10. Buscar documentos que contienen información de acceso, conexiones en redes, etc.
11. Cualquier otro tipo de consideración especial (consideraciones de la persona involucrada: médicos, abogados, información privilegiada, etc.)

La falta de una orden de allanamiento e incautación que ampare las actuaciones (*sobre los equipos y sobre la información*) de la Policía Judicial y la Fiscalía puede terminar con la exclusión de los elementos probatorios por violación de las Garantías Constitucionales. Art. 66 de la Constitución

6.- En la Escena del Delito

Los Investigadores que llegan primero a una escena del crimen tienen ciertas responsabilidades, las cuales resumimos en el siguiente cuadro:

- **OBSERVE Y ESTABLEZCA LOS PARÁMETROS DE LA ESCENA DEL DELITO**: El primero en llegar a la escena, debe establecer si el delito está todavía en progreso, luego tiene que tomar nota de las características físicas del área circundante. Para los

investigadores forenses esta etapa debe ser extendida a todo sistema de información y de red que se encuentre dentro de la escena. En estos casos dicho sistema o red pueden ser blancos de un inminente o actual ataque como por ejemplo uno de denegación de servicio (DoS).

- **INICIE LAS MEDIDAS DE SEGURIDAD**: El objetivo principal en toda investigación es la seguridad de los investigadores y de la escena. Si uno observa y establece en una condición insegura dentro de una escena del delito, debe tomar las medidas necesarias para mitigar dicha situación. Se deben tomar las acciones necesarias a fin de evitar riesgos eléctricos, químicos o biológicos, de igual forma cualquier actividad criminal. Esto es importante ya que en una ocasión en una investigación de pornografía infantil en Estados Unidos un investigador fue muerto y otro herido durante la revisión de una escena del crimen.
- **FACILITE LOS PRIMEROS AUXILIOS**: Siempre se deben tomar las medidas adecuadas para precautelar la vida de las posibles víctimas del delito, el objetivo es brindar el cuidado médico adecuado por el personal de emergencias y el preservar las evidencias.
- **ASEGURE FÍSICAMENTE LA ESCENA**: Esta etapa es crucial durante una investigación, se debe retirar de la escena del delito a todas las personas extrañas a la misma, el objetivo principal es el prevenir el acceso no autorizado de personal a la escena, evitando así la contaminación de la evidencia o su posible alteración.
- **ASEGURE FÍSICAMENTE LAS EVIDENCIAS**: Este paso es muy importante a fin de mantener la cadena de custodia[2] de las evidencias, se debe guardar y etiquetar cada una de ellas. En este caso se aplican los principios y la metodología correspondiente a la recolección de evidencias de una forma práctica. Esta recolección debe ser realizada por personal entrenado en manejar, guardar y etiquetar evidencias.
- **ENTREGAR LA ESCENA DEL DELITO**: Después de que se han cumplido todas las etapas anteriores, la escena puede ser entregada a las autoridades que se harán cargo de la misma. Esta situación será diferente en cada caso, ya que por ejemplo en un caso penal será a la Policía Judicial o al Ministerio Público; en un caso corporativo a los Administradores del Sistema. Lo esencial de esta etapa es verificar que todas las evidencias del caso se hayan recogido y almacenado de forma correcta, y que los sistemas y redes comprometidos pueden volver a su normal operación.
- **ELABORAR LA DOCUMENTACIÓN DE LA EXPLOTACIÓN DE LA ESCENA**: Es Indispensable para los investigadores documentar cada una de las etapas de este proceso, a fin de tener una completa bitácora de los hechos sucedidos durante la explotación de la escena del delito, las evidencias encontradas y su posible relación

[2] La cadena de custodia es un sistema de aseguramiento que, basado en el principio de la "mismidad", tiene como fin garantizar la autenticidad de la evidencia que se utilizará como "prueba" dentro del proceso. La información mínima que se maneja en la cadena de custodia, para un caso específico, es la siguiente: a) Una hoja de ruta, en donde se anotan los datos principales sobre descripción de la evidencia, fechas, horas, custodios, identificaciones, cargos y firmas de quien recibe y quien entrega; b) Recibos personales que guarda cada custodio y donde están datos similares a los de la hoja de ruta; c) Rótulos que van pegados a los envases de las evidencias, por ejemplo a las bolsas plásticas, sobres de papel, sobres de Manila, frascos, cajas de cartón, etc.; d) Etiquetas que tienen la misma información que los rótulos, pero van atadas con una cuerdita a bolsas de papel kraft, o a frascos o a cajas de cartón o a sacos de fibra; e) Libros de registro de entradas y salidas, o cualquier otro sistema informático que se deben llevar en los laboratorios de análisis y en los despachos de los fiscales e investigadores.

con los sospechosos. Un investigador puede encontrar buenas referencias sobre los hechos ocurridos en las notas recopiladas en la explotación de la escena del Delito.

6.1.- Reconstrucción de la Escena del Delito

La reconstrucción del delito permite al investigador forense comprender todos los hechos relacionados con el cometimiento de una infracción, usando para ello las evidencias disponibles. Los indicios que son utilizados en la reproducción del Delito permiten al investigador realizar tres formas de reconstrucción a saber:

- *Reconstrucción Relacional*, se hace en base a indicios que muestran la correspondencia que tiene un objeto en la escena del delito y su relación con los otros objetos presentes. Se busca su interacción en conjunto o entre cada uno de ellos;
- *Reconstrucción Funcional*, se hace señalando la función de cada objeto dentro de la escena y la forma en que estos trabajan y como son usados;
- *Reconstrucción Temporal*, se hace con indicios que nos ubican en la línea temporal del cometimiento de la infracción y en relación con las evidencias encontradas.

6.2.- Qué hacer al encontrar un dispositivo informático o electrónico

- No tome los objetos sin guantes de hule, podría alterar, encubrir o hacer desaparecer las huellas dactilares o adeníticas existentes en el equipo o en el área donde se encuentra residiendo el sistema informático.
- Asegure el lugar.
- Asegure los equipos. De cualquier tipo de intervención física o electrónica hecha por extraños.
- Si no está encendido, no lo encienda *(para evitar el inicio de cualquier tipo de programa de autoprotección*
- Verifique si es posible el Sistema Operativo a fin de iniciar la secuencia de apagado a fin de evitar pérdida de información.
- Si usted cree razonablemente que el equipo informático o electrónico está destruyendo la evidencia, debe desconectarlo inmediatamente.
- Si está encendido, no lo apague inmediatamente *(para evitar la pérdida de información "volátil")*
- \- SI ES POSIBLE, LLAME UN TÉCNICO.

Cuando no hay técnico:

- No use el equipo informático que está siendo investigado, ni intente buscar evidencias sin el entrenamiento adecuado.
- Si está encendido, no lo apague inmediatamente.
- Si tiene un "Mouse", muévalo cada minuto para no permitir que la pantalla se cierre o se bloqueé.
- Si una Computadora Portátil (Laptop) no se apaga cuando es removido el cable de alimentación, localice y remueva la batería, esta generalmente se encuentra debajo del equipo, y tiene un botón para liberar la batería

del equipo. Una vez que está es removida debe guardarse en un lugar seguro y no dentro de la misma máquina, a fin de prevenir un encendido accidental.

- Si el aparato está conectado a una red, anote los números de conexión, (números IP).
- Fotografíe la pantalla, las conexiones y cables
- Usar bolsas especiales antiestática para almacenar diskettes, discos rígidos, y otros dispositivos de almacenamiento informáticos que sean electromagnéticos (si no se cuenta, pueden utilizarse bolsas de papel madera). Evitar el uso de bolsas plásticas, ya que pueden causar una descarga de electricidad estática que puede destruir los datos
- Coloque etiquetas en los cables para facilitar reconexión posteriormente
- Anote la información de los menús y los archivos activos (sin utilizar el teclado) *Cualquier movimiento del teclado puede borrar información importante.*
- Si hay un disco, una disquete, una cinta, un CD u otro medio de grabación en alguna unidad de disco o grabación, retírelo, protéjalo y guárdelo en un contenedor de papel
- Bloqueé toda unidad de grabación con una cinta, un disco o un disquete vacío aportado por el investigador (NO DEL LUGAR DE LOS HECHOS). *Al utilizar algún elemento del lugar del allanamiento o de los hechos, se contamina un elemento materia de prueba con otro.*
- Selle cada entrada o puerto de información con cinta de evidencia
- De igual manera deben selle los tornillos del sistema a fin de que no se puedan remover o reemplazar las piezas internas del mismo.
- Desconecte la fuente de poder
- Quite las baterías y almacénela de forma separada el equipo (si funciona a base de baterías o es una computadora portátil)
- Mantenga el sistema y medios de grabación separados de cualquier tipo de imán, o campo magnético
- Al llevar aparatos, anote todo número de identificación, mantenga siempre la CADENA DE CUSTODIA
- Lleve todo cable, accesorio, conexión
- Lleve, si es posible, manuales, documentación, anotaciones
- Tenga en cuenta que es posible que existen otros datos importantes en sistemas periféricos, si el aparato fue conectado a una red, por tanto desconecte el cable de poder de todo hardware de Red (Router, modem, Swich, Hub).

Si el equipo es una estación de trabajo o un Servidor (conectado en red) o está en un negocio, el desconectarla puede acarrear (SIEMPRE CONSULTE A UN TÉCNICO EXPERTO EN REDES):

- Daño permanente al equipo
- Responsabilidad Civil para la Policía Judicial y la Fiscalía General del Estado
- Interrupción ilegal del giro del negocio.

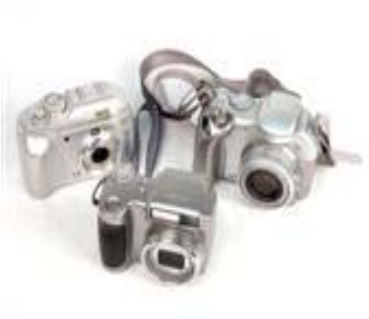
7.- Otros aparatos electrónicos

7.1.- Teléfonos Inalámbricos, Celulares, Smartfones, Cámaras Digitales

Se puede encontrar evidencia potencial contenida en los teléfonos inalámbricos tal como:

- Números llamados
- Números guardados en la memoria y en el marcado rápido
- Identificador de llamadas, llamadas entrantes
- Otra información guardada en la memoria del teléfono
- Números marcados
- Nombres y direcciones
- Números personales de Identificación (PIN)
- Número de acceso al correo de voz
- Contraseña del correo de voz
- Números de tarjetas de crédito
- Números de llamadas hechas con tarjeta
- Información de acceso al Internet y al correo electrónico
- Se puede encontrar valiosa información en la pantalla del aparato
- Imágenes. Fotos, grabaciones de voz
- Información guardada en las tarjetas de expansión de memoria

REGLA DEL ENCENDIDO "ON" Y APAGADO "OFF"



1. Si el aparato está encendido "ON", no lo apague "OFF".
    - Si lo apaga "OFF" puede iniciarse el bloqueo del aparato.
    - Transcriba toda la información de la pantalla del aparato y de ser posible tómele una fotografía.
    - Vigile la batería del aparato, el transporte del mismo puede hacer que se descargue. Tenga a mano un cargador
    - Selle todas las entradas y salidas.
    - Selle todos los puntos de conexión o de admisión de tarjetas o dispositivos de memoria
    - Selle los tornillos para evitar que se puedan retirar o reemplazar piezas internas.
    - Buscar y asegurar el conector eléctrico.
    - Colocar en una bolsa de FARADAY, (especial para aislar de emisiones electromagnéticas), si no hubiere disponible, en un recipiente vacío de pintura con su respectiva tapa.
    - Revise los dispositivos de almacenamiento removibles. (Algunos aparatos contienen en su interior dispositivos de almacenamiento removibles tales como tarjetas SD, Compact flash, Tarjetas XD, Memory Stick, etc.)

2. Si el aparato está apagado "OFF", déjelo apagado "OFF".
    - Prenderlo puede alterar evidencia al igual que en las computadoras.
    - Antes del análisis del aparato consiga un técnico capacitado en el mismo.
    - Si no existe un técnico use otro teléfono.
    - Es necesario que el investigador busque el manual del usuario relacionado con el aparato encontrado.

7.2.- Aparatos de mensajería instantánea, beepers.

1. Beepers Numéricos (reciben solo números y sirven para transmitir números y códigos)
2. Beepers Alfanuméricos (reciben números y letras, pueden cargar mensajes completos en texto)
3. Beepers de Voz (pueden transmitir la voz y también caracteres alfanuméricos)
4. Beepers de dos vías (contienen mensajes de entrada y salida)
5. Buenas Prácticas
   - Una vez que el beeper está alejado del sospechoso, este debe ser apagado. Si se mantiene encendido los mensajes recibidos, sin tener una orden judicial para ello puede implicar una interceptación no autorizada de comunicaciones.
6. Cuando se debe buscar en el contenido del aparato.
   - Cuando es la causa de la aprehensión del sospechoso
   - Cuando haya presunción del cometimiento de un delito Flagrante
   - Con el consentimiento del dueño o receptor de los mensajes

7.3.- Máquinas de Fax

1. En las máquinas de fax podemos encontrar:
   - Listas de marcado rápido
   - Fax guardados (transmitidos o recibidos)
   - Bitácoras de transmisión del Fax (transmitidos o recibidos)
   - Línea del Encabezado
   - Fijación de la Hora y Fecha de la transmisión del Fax
2. Buenas Prácticas
   - Si la máquina de fax es encontrada prendida "ON", el apagarla causaría la perdida de la memoria de último número marcados así como de los facsímiles guardados.
3. Otras consideraciones
   - Busque la concordancia entre el número de teléfono asignado a la máquina de fax y la línea de teléfono a la que está conectada.
   - De igual forma busque que el encabezado del mensaje y el número impreso coincidan con el del usuario y la línea telefónica.
   - Es necesario que el investigador busque el manual del usuario relacionado con el aparato encontrado.

7.4.- Dispositivos de Almacenamiento

Los dispositivos de almacenamiento son usados para guardar mensajes de datos e información de los aparatos electrónicos. Existen dispositivos de almacenamiento de tres clases, a saber: dispositivo magnético (como discos duros o los disquetes), dispositivos de estado sólido[3] o

[3] Más conocidos como SSD (Solid-State Drive) son dispositivos de almacenamientos de datos que usan una memoria solida para almacenar la información de forma constante de forma similar que un disco duro usando lo que se conoce como SRAM (Memoria de Acceso Randómico Estático) o DRAM

memoria solida (como las memorias flash y dispositivos USB) y los dispositivos ópticos (como los discos compactos y DVD).

Existen gran cantidad de Memorias USB en el mercado y otros dispositivos de almacenamiento como tarjetas SD, Compact flash, Tarjetas XD, Memory Stick, etc.

1. **BUENAS PRÁCTICAS**

- Recolecte las instrucciones de uso, los manuales y las notas de cada uno de los dispositivos encontrados.
- Documente todos los pasos al revisar y recolectar los dispositivos de almacenamiento
- Aleje a los dispositivos de almacenamiento de cualquier magneto, radio trasmisores y otros dispositivos potencialmente dañinos.

8.- Rastreo del Correo Electrónico

El Correo Electrónico nos permite enviar cartas escritas con el computador a otras personas que tengan acceso a la Red. El correo electrónico es casi instantáneo, a diferencia del correo normal. Podemos enviar correo a cualquier persona en el Mundo que disponga de conexión a Internet y tenga una cuenta de Correo Electrónico.

Al enviar un correo electrónico, la computadora se identifica con una serie de números al sistema del proveedor de servicios de Internet (*ISP*). Enseguida se le asigna una dirección IP y es dividido en paquetes pequeños de información a través del protocolo *TCP/IP*. Los paquetes pasan por una computadora especial llamada servidor *(server*) que los fija con una identificación única (*Message-ID*) posteriormente los sellan con la fecha y hora de recepción (*Sello de tiempo*). Más tarde al momento del envió se examina su dirección de correo para ver si corresponde la dirección IP de alguna de las computadoras conectadas en una red local (*dominio*). Si no corresponde, envía los paquetes a otros servidores, hasta que encuentra al que reconoce la dirección como una computadora dentro de su dominio, y los dirigen a ella, es aquí donde los paquetes su unen otra vez en su forma original a través del protocolo *TCP/IP*. (Protocolo de Control de Transferencia y Protocolo de Internet). Siendo visible su contenido a través de la interface gráfica del programa de correo electrónico instalado en la máquina destinataria.

Hay que tomar en cuenta que los correos electrónicos se mantienen sobre un servidor de correo, y no en la computadora del emisor o del destinatario, a menos que el operador los guarde allí. Al redactarlos se transmiten al servidor de correo para ser enviados. Al recibirlas, nuestra computadora hace una petición al Servidor de correo, para los mensajes sean transmitidos luego a la computadora del destinatario, donde el operador la puede guardar o leer y cerrar. Al cerrar sin guardar, la copia de la carta visualizada en la pantalla del destinatario desaparece, pero se mantiene en el servidor, hasta que el operador solicita que sea borrada.

En algunas ocasiones es necesario seguir el rastro de los Correos Electrónicos enviados por el Internet. Los rastros se graban en el encabezamiento del e-mail recibido. Normalmente, el

(Memoria de Acceso Randómico Dinámico). Estas memorias simulan la interfaz de un disco magnético convirtiéndose en dispositivos de almacenamiento masivo.

encabezamiento que aparece es breve. La apariencia del encabezamiento está determinada por el proveedor de servicios de Internet utilizado por nuestra computadora, o la de quien recibe el correo electrónico. Para encontrar los rastros, se requiere un encabezamiento completo o avanzado, posibilidad que existe como una opción en nuestro proveedor de servicios de Internet.

Para poder elegir la opción de un encabezamiento técnico, seleccione "encabezamiento completo o avanzado" por medio de **opciones** o **preferencias** en la barra de herramientas de la página Web de su proveedor de Correo Electrónico (YAHOO, GMAIL, HOTMAIL, etc.) El encabezamiento completo contiene información fácil y difícil de interpretar, por ejemplo: "TO", "FROM" "CC", datos fáciles de entender (el destinatario, el emisor, una copia enviada a, y el título del mensaje). Otros datos son más difíciles de entender, como los números IP: *148.235.52.34* O *Message-id: NIBBLHGCOLIEFEEJKGEBCCAAA.* abelardolopez98@prodigy.net.mx>. Esta información requiere interpretación.

8.1.- Encabezado General

Español	Ingles	Contenido
DE:	FROM:	Abelardo López <abelardolopez98@prodigy.net.mx>
ENVIADO :	SENT:	Miércoles, 11 de febrero, 2004 7:16 PM
PARA :	TO:	< kylegrimes@msn.com>
COPIA:	CC:	Gabriel Grimes <grimesgk@hotmail.com>
TITULO:	SUBJECT:	Hace mucho tiempo

El encabezamiento breve se lee desde arriba hacia abajo.

- ***From o De***, Emisor de la correspondencia, contiene el nombre del autor, **Abelardo López**, su identificación en el Internet, **abelardolopez98**, su nombre de dominio primario es un proveedor de servicios de Internet, **prodigy**, que tiene un dominio de red, .**net**, y un dominio territorial, .**mx**, que pertenece a México.

- ***Sent o Enviado***, es la fecha y hora de su envió, designado por la computadora de origen, **Miércoles, 11 de Febrero, 2004, 7:16 PM.**

- ***To o Para,*** destinatario de la correspondencia, contiene su identificación en el Internet, **kylegrimes**, su nombre de dominio primario es un proveedor de servicios de Internet, **msn** (Microsoft Network), que tiene un dominio de comercio, **com**.

- ***CC,*** copia enviada a, contiene el nombre de otro destinatario secundario, **Gabriel Grimes**, su identificación en el Internet, **grimesgk**, su nombre de dominio primario es un proveedor de servicios de correspondencia electrónica, **hotmail**, que tiene un dominio de comercio, **com**.

- ***Subjec o Título,*** es el tema de la correspondencia escrita por el emisor, **Hace mucho tiempo**.

Los signos de puntuación, como los puntos, < >, y la @ son indicaciones para el protocolo de manejo en el Internet.

8.2.- Encabezado Técnico

MIME-Version: 1.0
Received: from [216.136.226.197] by hotmail.com (3.2) with ESMTP id MHotMailBD737B61008E4D888E2C506160; Thu, 20 Sep 2001 11:07:30-0700
Received: from [12.26.159.122] by web20808.mail.yahoo.com via HTTP; Thu, 20 Sep 2001 11:07:29 PDT
From: Polaris99992001@yahoo.com Thu, 20 Sep 2001 11:07:58 -0700
Message-id: <20010920180729.36281.qmail@web20808.mail.yahoo.com>

El encabezamiento completo se lee desde abajo hacia arriba.

- ***Message-id***, **20010920180729.36281.qmail@web20808.mail.yahoo.com**, indica una identificación asignada al correo electrónico por el servidor que inicialmente procesó la correspondencia original. La identificación es única, y sirve para verificar la originalidad del mensaje.

- ***From,*** el emisor del mensaje y la fecha y hora de su envío (según la computadora que lo envió). Siempre se debe verificar el uso horario a fin de tener la hora correcta.

- ***Received from***, muestra el número IP de la computadora del origen, **12.26.159.122**, que puede ser un compuesto del numero local y la red que procesa el mensaje, *by*, o por, el servidor que inicialmente procesó el mensaje, **web20808.mail.yahoo.com**, *via*, o por cual protocolo, **http** (protocolo de transferencia de hipertexto), fecha y hora del Internet, **Thu, 20 Sep 2001 11:07:29 PDT** (hora normal de la Zona del Pacífico).

- ***Received from***, el número IP mencionado del destinatario, **216.136.226.197**, *by*, o por, el servidor de HOTMAIL, **hotmail.com**, *with ESMTP id,* una nueva identificación del mensaje asignado por el nuevo servidor, **MHotMailBD737B61008E2C506160**, la fecha y hora de su recepción, **Thu, 20 Sep 2001 11:07:30-0700.**

- ***MIME-Version: 1.0***, Es la versión de encabezado

Con la información del encabezado técnico podemos verificar el origen del mensaje enviado, buscando con el número IP registrado el dominio de donde se origino el mensaje. Para eso se utiliza una interfaz, "WHOIS?**"** que significa "¿Quién es?", para determinar el servicio utilizado, ubicar la dirección geográfica de los servidores y los puntos de contacto, y localizar (a veces) la instalación donde se encuentra un computador.

Se puede poner la dirección IP en la página Web: http://samspade.org para averiguar los datos antes señalados, también se puede acudir a la página de INTERNIC.

Podemos usar también meta buscadores como GOOGLE, ALTAVISTA, YAHOO, etc.

9.- Glosario de Términos:

- **BASE DE DATOS:** Conjunto completo de ficheros informáticos que reúnen informaciones generales o temáticas, que generalmente están a disposición de numerosos usuarios.
- **BROWSER (BUSCADOR):** El software para buscar y conseguir información de la red WWW. Los más comúnmente usados son Microsoft Explorer, Firefox y Opera.
- **COOKIE**: Es un archivo o datos dejados en su computadora por un servidor u otro sistema al que se hayan conectado. Se suelen usar para que el servidor registre información sobre aquellas pantallas que usted ha visto y de la información personalizada que usted haya mandado. Muchos usuarios consideran esto como una invasión de privacidad, ya que casi ningún sistema dice lo que está haciendo. Hay una variedad de "anti-cookie" software que automáticamente borra esa información entre visitas a su sitio.
- **DIALUP (MARCAR)**: El método de conectarse con Internet vía la línea de teléfono normal mediante un modem, en vez de mediante una LAN (Red Local) o de una línea de teléfono alquilada permanentemente. Esta es la manera más común de conectarse a Internet desde casa si no ha hecho ningún arreglo con su compagina de teléfono o con un ISP. Para conexiones alternativas consulte con su ISP primero.
- **DIGITAL SIGNATURE (FIRMA DIGITAL)**: El equivalente digital de una firma autentica escrita a mano. Es un dato añadido a un fichero electrónico, diciendo que el dueño de esa firma escribió o autorizo el Archivo.
- **DOCUMENTO ELECTRÓNICO:** Es la representación en forma electrónica de hechos jurídicamente relevantes susceptibles de ser presentados en una forma humanamente comprensible[4].
- **DOMAIN NAME (NOMBRE DE DOMINIO)**: Un nombre de dominio es su propiedad en el mundo cibernético. Esta propiedad, tal y como su homologo tangible, tiene valor dependiendo de su dirección y de su contenido. Usted puede cobrar a sus invitados o darles un tour gratis, o llevar un negocio paralelo como parte de la propiedad. Igual que una dirección de la 5 Avenida que es limitada y también más valorada que la inmensa mayoría de las demás direcciones, el valor de su dominio puede variar de unos cuantos dólares por ejemplo, algunos están en el millón de dólares. No le podemos decir que muebles, obras de arte, o negocio paralelo debe tener en su propiedad en el mundo cibernético, pero su dirección es bien segura que realzara el valor de su contenido, o igual lo eliminara si ese nombre no atrae clientes. Técnicamente, es un concepto creado para identificar y localizar computadoras en Internet. Los nombres de dominio son un sistema de direcciones de Internet fácil de recordar, que pueden ser traducidos por el Sistema de Nombres de Dominio a las

[4] Definición dada por EDIFORUM.(Foro de Intercambio Electrónico de Datos)

direcciones numéricas usadas en la red. Un nombre de dominio es jerárquico y usualmente acarrea información sobre el tipo de entidad que usa ese nombre de dominio. Un nombre de dominio es simplemente una etiqueta que representa un dominio, que a su vez es un subgrupo del total del espacio de nombres del dominio. Nombres de dominio en el mismo nivel jerárquico tienen que ser únicos: solo puede haber un .com al nivel más alto de la jerarquía, y solo un DomainMart.com en el siguiente nivel.

- **FTP O FILE TRANSFER PROTOCOL (PROTOCOLO DE TRANSFERENCIA DE FICHERO)** Un estándar de Internet para transferir ficheros entre ordenadores. La mayoría de las transferencias FTP requieren que usted se meta en el sistema proveyendo la información mediante un nombre autorizado de uso y una contraseña. Sin embargo, una variación conocida como "FTP anónimo" le permite meterse como anónimo: no necesita contraseña o nombre.
- **HTML (HYPER TEXT MARKUP LANGUAGE)**: El lenguaje de computador usado para crear paginas de red para Internet. Aunque estándares "oficiales" de Internet existen, en la práctica son extensiones del lenguaje que compañías como Netscape o Microsoft usan en sus buscadores (browsers).
- **HTTP (HYPER TEXT TRANSPORT PROTOCOL)**: El conjunto de reglas que se usa en Internet para pedir y ofrecer paginas de la red y demás información. Es lo que pone al comienzo de una dirección, tal como "http:/," para indicarle al buscador que use ese protocolo para buscar información en la pagina.
- **INTERNET PROTOCOL (IP) NUMBERS O IP ADRESSES (PROTOCOLO DE INTERNET, NÚMEROS)**: Un identificador numérico único usado para especificar anfitriones y redes. Los números IP son parte de un plan global y estandarizado para identificar computadores que estén conectados a Internet. Se expresa como cuatro números del 0 al 255, separado por puntos: 188.41.20.11. La asignación de estos números en el Caribe, las Américas, y África la hace la American Registry for Internet Numbers.
- **INTERNET SERVICE PROVIDER (ISP) (PROVEEDOR DE SERVICIO DE INTERNET)** Una persona, organización o compagina que provee acceso a Internet. Además del acceso a Internet, muchos ISP proveen otros servicios tales como anfitrión de Red, servicio de nombre, y otros servicios informáticos.
- **MENSAJE DE DATOS:** Es toda aquella información visualizada, generada enviada, recibida, almacenada o comunicada por medios informáticos, electrónicos, ópticos, digitales o similares.
- **MODEM**: Un aparato que cambia datos del computador a formatos que se puedan transmitir más fácilmente por línea telefónica o por otro tipo de medio.
- **SISTEMA TELEMÁTICO.** Conjunto organizado de redes de telecomunicaciones que sirven para trasmitir, enviar, y recibir información tratada de forma automatizada.

- **SISTEMA DE INFORMACIÓN:** Se entenderá como sistema de información, a todo sistema utilizado para generar, enviar, recibir, procesar o archivar de cualquier forma de mensajes de datos[5].
- **SISTEMA INFORMÁTICO:** Conjunto organizado de programas y bases de datos que se utilizan para, generar, almacenar, tratar de forma automatizada datos o información cualquiera que esta sea.
- **SOPORTE LÓGICO:** Cualquiera de los elementos (tarjetas perforadas, cintas o discos magnéticos, discos ópticos) que pueden ser empleados para registrar información en un sistema informático.
- **SOPORTE MATERIAL:** Es cualquier elemento corporal que se utilice para registrar toda clase de información.
- **TCP/IP: TRANSMISIÓN CONTROL PROTOCOL/INTERNET PROTOCOL:** Conjunto de protocolos que hacen posible la interconexión y tráfico de la Red Internet

10. - Bibliografía

- **THE BEST PRACTICES FOR SEIZING ELECTRONIC EVIDENCE, VERSIÓN 3.0,** US. Department of Home Land Security, *and the United States Secret Service*.
- **INTRODUCCIÓN A LA INFORMÁTICA FORENSE**. *Dr. Santiago Acurio Del Pino, Director Nacional de Tecnologías de la Información de la Fiscalía General del Estado. 2009*
- **MANUAL DE PERITAJE INFORMATICO**. Maricarmen Pascale, Fundación de Cultura Universitaria. Uruguay. 2007

[5] Definición entregada por La Ley Modelo de Comercio Electrónico de la UNCITRAL