# CÓDIGO DE PRÁCTICAS PARA DIGITAL FORENSICS
# CODE OF PRACTICES FO R DIGITAL FORENSICS
# CP4DF



# AVANCE DE LA METODOLOGÍA

| COMENTARIOS | |
|---|---|
| David González<br>dgonz AT sourceforge.net<br>Versión: 1.3 - Fecha: 07.Noviembre.2003 | Versión 1.3 del documento creado. |
| rcarhuatocto AT sourceforge.net | Revisión 1.2 del documento |
| | |
| | |
| | |
| | |

INDICE

## INTRODUCCION

En la medida que crece y se diversifica el uso de Infraestructuras Tecnológicas, se incrementan también los riesgos http://www.csi.map.es/csi/pg5m20.htm (Guía Magerit) de que los equipos de cómputo, dispositivos electrónicos y sistemas informáticos, conectados o no a Internet, sean vulnerables a ataques o incidentes que ponen en peligro la integridad, disponibilidad y autenticidad de los datos que en ellos se procesa, almacena o transfiere. Y más allá de los datos, el daño a dichas infraestructuras es latente.

Con el incremento del número de incidentes de seguridad, es cada vez más frecuente el tener que analizar las acciones realizadas por los atacantes en los equipos; por un lado para conocer y aprender del *modus operando,* averiguar el alcance del mismo y, llegado el momento, poder tomar las medidas oportunas para denunciar el ataque a las autoridades competentes. Pero por otro lado, para llevar a cabo la actualización o recuperación parcial o completa del equipo atacado, ya que conociendo lo dañado es posible intentar recuperarlo, ello con el fin de asegurar la continuidad del negocio.. Cada vez es más costoso el parar un servicio para efectuar la reinstalación de los sistemas informáticos y aplicaciones; además es conveniente evaluar en profundidad las implicaciones que ha tenido el problema de seguridad mediante las herramientas de análisis forense.

En este trabajo se plantean las bases de una metodología de análisis forense en las Infraestructuras Tecnológicas que cubra los pasos necesarios desde el aseguramiento de la escena del delito hasta la presentación de evidencias ante un Tribunal de Justicia, si fuese el caso, o simplemente aprender del incidente.

Esta metodología pretende ser la base para el desarrollo del Código de Prácticas para Digital Forensics – CP4DF, se crea con la idea de que sea lo más abierta posible, como lo define CP4DF en sus objetivos [http://cp4df.sourceforge.net]. Esto es evidentemente necesario puesto que el mundo de la tecnología informática avanza rápidamente, existen nuevas herramientas y técnicas para la investigación de incidentes de seguridad y cada vez es más urgente constituir grupos de profesionales en el tema que deberán enfrentarse a escenarios nuevos y nuevos desafíos que hacen que se realicen tareas de investigación cada vez más complejas y sin un marco coherente de trabajo la labor se ve duplicada y a veces cuestionada. Por otro lado, el código de prácticas para digital forensics servirá no sólo como guía de trabajo, sino como lista de tareas que hay que hacer en un proceso de investigación, esto sirve mucho a profesionales que se inician en esta nueva labor.

Toda evidencia digital es y debe ser convincente ante un Tribunal de Justicia o en donde haya alguna disputa. Para asegurarla, es importante la homogenización del protocolo de admisibilidad de la prueba, además de un continua aproximación de lo que podría tratarse de una prueba. Esta labor se hace muy difícil en circunstancia en donde no exista una metodología, menos aún, cuando no exista un marco de trabajo.

El proceso tradicional de investigación cuando el delito o evento se haya consumado, consta [según los diversos expertos en la materia (como Dan Farmer, Wietse Venema, Brian Carrier), empresas (como Guidance Software, LC Technology International, NTI New Technologies) e instituciones (como Scientific Working Group

on Digital Evidence (SWGDE), International Organization on Digital Evidence (IOCE))] de las siguientes etapas:

a) Identificación de la evidencia digital.
b) Preservación de la evidencia digital.
c) Análisis de la evidencia digital.
d) Presentación de la evidencia digital.

[Qué pasa cuando el delito se está produciendo?, existen las mismas etapas o fases?, explicar]

Basándonos en estas etapas básicas, planteamos la inclusión de una etapa previa, también importante en el proceso de investigación, creemos más importante para quienes se encuentran en el lado policial ya que dentro de su labor, al margen de ser investigadores, está el asegurar la potencial evidencia. Finalmente las fases o etapas serían:

FASE 1: Asegurar la escena del delito.
FASE 2: Identificación de las evidencias.
FASE 3: Preservación de las evidencias.
FASE 4: Análisis de las evidencias.
FASE 5: Presentación y reporte.

Paralelamente a estas fases se debe realizar en todas y cada una de ellas una documentación profunda y mantenimiento de la cadena de custodia de la evidencia.

Las tres primeras fases normalmente se deberían hacer en la escena del crimen sobre todo por obtener toda evidencia *"in-situ"* que pueda ayudar al caso, pues una vez levantada la escena del crimen no será posible obtenerlas.

La fase de análisis se debería realizar en el laboratorio forense, donde tendremos las condiciones y el equipo idóneo para dicho proceso.

La presentación y reporte se hará en un tribunal de justicia o delante de un cliente.

El personal que responda al incidente debería llevar consigo todo lo necesario para asegurar la escena del delito y aplicar el procedimiento de gestión de incidencias. Las herramientas básicas podrían ser los siguientes:

- Destornilladores.
- Alicates.
- Cinta aislante y cinta de embalaje.
- Cortador de cables.
- Etiquetas.
- Folios o PDA para realizar la documentación de evidencias y documentación de la cadena de custodia.
- Rotuladores de colores.
- Cámara digital de fotografías.
- Cámara digital de vídeo.
- Sistemas de creación de imágenes de dispositivos de almacenamiento. (Ordenadores portátiles con grabadores CD o DVS, sistemas de copia rápida RAID, etc).
- Disquetes y CDs con sistemas operativos autoarrancables.

- Bolsas antiestáticas.
- Plásticos con sistema de “burbujas de aire”.
- Caja de cartón.
- Copias backup de los sistemas que se requieran reconstituir siempre cuando se trate de un equipo crítico.

Toda posible prueba debe ser adecuadamente etiquetada y documentada, además cada paso realizado debe ser registrado y documentado en detalle. A ello le llamamos la Bitácora del Investigador.

Como veremos en la fase de presentación y reporte, el proceso de documentación es fundamental. Cada paso que se hace hay que asegurarse que es reproducible y de proporcionar siempre los mismos resultados.

Se debe tener en cuenta la cadena de custodia desde el momento que se llega a la escena del crimen o lugar de los hechos, se fijan fotográficamente o se graban en vídeo evidencias, se levantan y embalan los indicios o evidencias identificadas obrando registro de día, hora, condiciones especiales (estos datos estarán recogidos del proceso de documentación), pero sobre todo, de las personas que participan y tienen cualquier tipo de contacto o control de la evidencia hasta que se muestran en proceso judicial.

El documento de la cadena de custodia debe estar disponible en cualquier momento y su objetivo es determinar quien accedió a una evidencia, cuando y para qué. Este documento debe ser válido desde el momento de incautación de una evidencia digital hasta su presentación en un proceso judicial.

Estas cinco fases serán secuenciales, aunque dependiendo del tipo de evidencias que tengamos en escena (volátiles o no volátiles) habrá un tratamiento distinto (esencialmente en cuestión de rapidez de la recolección de las evidencias digitales) en las dos primeras fases.

A continuación se describe en profundidad cada una de las fases, en cada una de los cuales se intentará ser lo más genérico posible para poder abarcar el mayor número de tipos de evidencias posibles (debido a que existen sistemas, software y hardware muy heterogéneos).

El receptor de esta metodología sabrá que, dependiendo del tipo de delito informático, de los sistemas, de los componentes hardware y software involucrados en el mismo, podrá aplicar o no las distintas directrices que compongan cada módulo.

Para terminar esta introducción a la metodología comentar que siempre que sea posible los pasos deben ser dados con testigos o notarios que puedan corroborar lo realizado por el experto forense (como mínimo habría que intentarlo en las fases de asegurar la escena del delito, identificación y preservación de las evidencias).

## FASE 1: ASEGURAMIENTO DE LA ESCENA

El primer paso en un proceso de investigación informática forense, al igual que en cualquier otro proceso criminal, es asegurar (restringir el acceso a la zona del delito para no modificar evidencias) la escena del delito informático.

Este primer módulo, idealmente, debería ser realizado por un cuerpo de seguridad del Estado: Guardia Civil, Policía Nacional, etc. junto a un experto en Informática Forense. Como esta situación es bastante ideal y el proceso de aseguramiento se debe hacer lo más rápido posible, aunque la exactitud debe primar sobre la rapidez en todas las fases, este módulo debe ser realizado por una persona "competente" de la organización implicada que pueda explicar los pasos que ha realizado y la implicación de sus acciones.

Normalmente los administradores de los sistemas informáticos serán los primeros en tener contacto con la escena del delito y junto a equipo de respuesta de incidentes realizarán los primeros pasos para "congelar" la escena del delito.

El rol fundamental de las primeras personas en responder al delito es no hacer nada que pueda producir daño. A menos que se esté específicamente entrenado en respuesta a incidentes, la persona que primero llegue a la escena no debería realizar nada de lo que no esté seguro de sus consecuencias. Es muy fácil que un astuto criminal informático inserte un troyano o código hostil que destruya evidencias automáticamente al apagar el ordenador, resetearlo, etc.

Es muy importante que una persona sea asignada con autoridad suficiente para tomar decisiones finales que aseguren la escena del delito, conducir las búsquedas de evidencias y preservar las mismas. Este rol normalmente debe ser asumido por el jefe del equipo forense.

Pasos a realizar:

1. Identificar la escena del delito. Para ello se debe establecer un perímetro. Esto puede incluir una única sala, incluir varias salas e incluso varios edificios en los cuales el sospechoso hubiese estado trabajando con una compleja red de ordenadores.
2. Realizar una lista con los sistemas involucrados en el delito.
3. Restringir el acceso a la escena del delito, acceso tanto de personas como acceso de otros equipos informáticos.
4. Preservar toda huella digital, uso de guantes de latex.
5. Fotografiar, grabar y esquematizar la escena del delito. Si la información de una fotografía o grabación no es identificable, copiar manualmente la información observable.
6. Mantener el estado de los dispositivos.
   6.1 Comprobar si el dispositivo esta apagado, por ejemplo mirando los *leds* del dispositivo. Muchas veces el aparato puede estar en modo *sleep*, con protector de pantalla, etc.
   6.2 Si el dispositivo está apagado y es un ordenador portátil, quitar la batería.

6.3 Si el dispositivo está encendido
6.3.1 Si el dispositivo tiene pantalla, fotografiar y grabar la misma.
6.3.2 Identificar las evidencias volátiles (Ver fase IDENTIFICAR).

7. Desconectar las conexiones de red.
8. Comprobar y desconectar si existieran las conexiones inalámbricas que puedan permitir la activación de conexiones remotas.
9. Si hay impresoras imprimiendo, dejar que terminen de imprimir.
10. Anotar hora y fecha del sistema antes de apagarlo, documentándolo con fotografías o grabándolo en vídeo si es posible.
11. Los dispositivos encendidos apagarlos quitando la alimentación de la parte posterior del mismo, no del enchufe. Esto evita que se escriban datos en el disco duro del aparato o en el sistema de almacenamiento del dispositivo, si éste tiene alguna protección frente a interrupciones de alimentación.
NOTA: Apagando de esta forma se pierden algunas evidencias, pero se asegura la integridad de las evidencias no pérdidas.
12. Etiquetar cables y componentes
13. Fotografiar y grabar de nuevo los dispositivos con las etiquetas colocadas en los mismos.

## FASE 2: IDENTIFICACION DELAS EVIDENCIAS DIGITALES

Es el proceso de conocer los datos, dónde están localizados y cómo están almacenados.

Al ser un universo tan heterogéneo el de los sistemas de información donde se pueden encontrar evidencias digitales, se hace necesaria una clasificación para poder organizar las mismas.

Debemos realizar una primera distinción entre evidencias volátiles (evidencias que desaparecen pronto debido a falta de alimentación eléctrica, corte de conexiones telemáticas, etc.) y no volátiles (evidencias que perduran aun a falta de alimentación eléctrica, etc.).

El obtener las evidencias volátiles lo más rápidamente posible es fundamental.

La obtención de evidencias volátiles se puede dar en los siguientes lugares:

1. Registros y cache del procesador
2. Tablas de rutas
3. Cache ARP
4. Tabla de procesos
5. Estadísticas del kernel y módulos
6. Memoria RAM
7. Ficheros temporales del sistema
8. Estado de la red
9. Ficheros abiertos
10. Tiempos de los ficheros (tiempos MAC: modificación, acceso y creación)

Hasta aquí habríamos obtenido evidencias que se podrían perder, incluso sin reiniciar el equipo.

Otras evidencias volátiles que seguro se pierden al reiniciar el funcionamiento del equipo y que se deben guardar son:

11. Sistemas de ficheros montados
12. Sistemas de ficheros virtuales (/proc)

Toda evidencia volátil conseguida debe ser grabada como fichero a un dispositivo de almacenamiento y fuera del dispositivo donde están las evidencias, preservando su integridad de la fuente. A partir de este momento, las evidencias volátiles tendrán el mismo tratamiento que las evidencias no volátiles, por lo cual seguirá las mismas fases de la metodología que éstas últimas. Si por cualquier circunstancia no se pueden grabar a fichero las evidencias volátiles, habrá que ver la factibilidad de realizar un estudio on-line de las mismas, con la perdida de evidencias o perdida de integridad de las mismas que ello puede suponer. También debemos clasificar las evidencias en función del tipo de sistema o dispositivo donde se encuentren las mismas:

a) Sistemas de ordenadores (Sistemas Unix / Linux / Windows / Mac / Solaris / SPARC / MVS, etc) y ordenadores portátiles

Donde obtener evidencias:

1. Monitor, teclado y ratón (solo necesario en ciertos casos).
2. Dongles (Mochilas) (dispositivos que se conectan en el puerto paralelo del ordenador y verifican que el programa es original y no es copia).
3. Cámaras de fotos digitales y cámaras de vídeo digitales.
4. Cartuchos Jaz/Zip
5. Cintas de backups
6. Tarjetas PCMCIA
7. Discos duros, disquetes, CDs, DVDs. Normalmente en estos dispositivos es donde más información encontraremos. La evidencia digital estará contenida en los sistemas de ficheros de cada uno de estos dispositivos.
8. Impresoras
9. Escáneres

NOTA: De estos dos últimos dispositivos periféricos es difícil encontrar evidencias una vez apagados, pero pueden ser necesarios para analizar otro tipo de evidencias, como huellas digitales.

b) Redes

Donde obtener evidencias:

1. Tarjetas de red de ordenadores.
2. Routers.
3. Hubs.
4. Switch.
5. Modems.

c) Redes inalámbricas

Donde obtener evidencias:

1. Tarjetas inalámbricas.
2. Puntos de accesos.

d) Dispositivos móviles:

Donde obtener evidencias:

1. Teléfonos móviles
2. Organizadores de mano (PDA, PocketPC, etc).

d) Sistemas embebidos

Donde obtener evidencias:

1. Memory Stick

2. Memory Cards (Smart Cards y Compact Flash)

e) Otros dispositivos

Donde obtener evidencias:

1. Buscapersonas.
2. Contestadores
3. Fax
4. Fotocopiadoras
5. Sistemas de cómputo de coches (por ejemplo sistemas de navegación por satélite).
6. Lectoras de tarjetas.

Otros lugares donde puede haber evidencias que sirvan de apoyo para encontrar evidencias digitales son:

1. Manuales hardware y software
2. Cualquier elemento que pueda contener una password (folios, notas,...)
3. Llaves
4. Salidas de impresión.
5. Papel de impresora.

En función de las prioridades del cliente (recuperación de cierta información, saber como ocurrió el delito, obtener la pruebas para llevar a juicio al delincuente, etc.) el experto debe buscar unas evidencias u otras. Dicho experto no debe gastar horas innecesarias recogiendo información que no sea relevante para su caso.

Casi siempre las evidencias estarán localizadas en el sistema de fichero del dispositivo o equipo comprometido, por lo cual el experto forense debe realizar una copia a nivel de bits de dicho sistema de ficheros.

Un último punto de esta fase sería recordar que la forma de localizar las evidencias no vaya en contra de ninguna ley del país. Hay que conocer la normativa legal sobre la interceptación de datos de terceros en medios digitales.

## FASE 3: PRESERVACION DE LAS EVIDENCIAS DIGITALES

Esta es la fase más importante y crítica de la metodología, puesto que una vez que se halla comprobado el delito informático la empresa o institución dañada normalmente deseará llevar a un proceso judicial al atacante. Para ello es necesario poseer evidencias digitales preservadas de tal forma que no haya duda alguna de su verosimilitud y siempre de acuerdo a las leyes vigentes. Este proceso de preservación se debe realizar tan pronto como sea posible.

Siempre que sea posible hay que evitar los cambios en las evidencias y si no se logra, registrarlo, documentarlo y justificarlo, siempre que sea posible con testigos que puedan corroborar las acciones.

Recordemos que las primeras evidencias que hay que obtener son las volátiles, que al guardarlas en ficheros se convertirán en evidencias no volátiles.

Pasos para preservar las evidencias digitales:

1. Si el dispositivo del cual tenemos que hacer copia de su sistema de almacenamiento está encendido, extraerlo siempre que sea posible y ponerlo en una estación de trabajo para la adquisición de datos. Si por cualquier circunstancia no es posible, arrancar el sistema donde está dicho dispositivo con un sistema operativo autoarrancable, desde disquete o CD, sin instalar nada en el sistema.
2. Toda evidencia digital guardada en dispositivos de almacenamiento, y por tanto almacenado en un sistema de ficheros, debe ser copiado mediante procedimientos software que no alteren la evidencia y que sean admisibles en un tribunal de justicia. Para ello realizar una imagen a nivel de bit del sistema de almacenamiento del dispositivo. Una imagen a nivel de bits es una copia que registra cada bit que fue grabado en el dispositivo de almacenamiento original, incluyendo ficheros ocultos, ficheros temporales, ficheros corruptos, ficheros fragmentados y ficheros borrados que todavía no han sido sobrescritos. Estas imágenes usan un método CRC para validar que la copia es la misma que el original.
3. Formas para crear duplicados a nivel de bit de los discos de almacenamiento de información.
   - Extraer el dispositivo origen a copiar.
   - Usar un dispositivo destino para el almacenamiento de la información; se recomienda algún RAID ya que aseguran redundancia y disponibilidad de los datos.
   - Usar una conexión de red, conexión Ethernet, cable cruzado, USB, etc., para transferir el contenido del disco al otro dispositivo de almacenamiento.

   Qué método usar dependen del equipamiento que se tenga a mano. Lo mejor, aunque también lo más caro, es una estación de trabajo portátil o un dispositivo de creación de imágenes. Teniendo sistemas de almacenamiento de capacidad menor a 700 Mb se puede usar un CD que no sea regrabable para realizar la imagen. Si esta capacidad es menor a 17 Gb se podría usar un DVD no regrabable. Usando CDs o DVDs se asegura la integridad de los datos, puesto que en estos dispositivos no puede ser modificados.

4. Retención de tiempos y fechas.
   El tiempo y fecha de creación o modificación de un fichero puede ser un importante asunto en un delito. Si el usuario puede tener el sistema sin configurar apropiadamente el tiempo o deliberadamente cambiar las propiedades de fecha y hora, los ficheros puede que no sean correspondientes con la fecha real. Esto puede ser un problema si, por ejemplo, el sistema de registro muestra que un fichero fue creado en una fecha concreta y el sospechoso es capaz de probar que esa fecha no usó el ordenador. Por ello se debe anotar hora y fecha del sistema antes de apagarlo, documentando el hecho. Además puede ser prudente fotografiar la pantalla mostrando el acceso a ficheros o tiempos de modificación antes de abrir dichos ficheros. También tener en cuenta el desfase horario que pueda haber entre el dispositivo que contiene la evidencia y el horario real, documentado este desfase. Siempre que sea posible trabajar con zonas de tiempo GMT. El delito puede involucrar varias zonas de tiempo y usando GMT puede ser un punto de referencia que haga el análisis de las evidencias más sencillo.
5. Preservar datos de dispositivos de mano como PDAs, PocketPCs, etc.
   Existen programas que duplican los datos que se están ejecutando sobre el sistema operativo de los dispositivos de mano. Estos programas crean una imagen completa de la memoria del dispositivo, incluidas las aplicaciones, datos de usuario y datos marcados para borrar (estos elementos no se borran hasta la siguiente sesión de sincronización). También se ofrece información sobre la versión del sistema operativo, información sobre el procesador, RAM, ROM, etc. Si no se posee una herramienta otra forma de preservar la información es copiar los ficheros relevantes a una tarjeta de memoria, por ejemplo, memory card.
6. Generar los procesos de checksum criptográfico de la copia y del original.
   Mediante el método de checksum criptográfico, proceso de generación de la integridad de un fichero, conjunto de ficheros o de toda la información contenida en un dispositivo de almacenamiento, se garantiza que la evidencia no será alterada en ni un solo bit. El proceso es sencillo; generar el checksum significa generar un hash, valor único para un determinado conjunto de bytes, de la evidencia. Esto es posible dado que los algoritmos criptográficos de hash son cuidadosamente seleccionados para ser funciones de un solo sentido: dado un determinado checksum criptográfico para un mensaje, es virtualmente imposible adivinar qué mensaje produjo ese checksum. Dicho de otra manera, no es posible hallar mediante cómputos dos mensajes que generen el mismo checksum criptográfico. Gracias a determinado software especializado y algoritmos de verificación de checksum (como MD5 y SHA-1) se comprueba que si la evidencia no se ha alterado produce un hash idéntico al original.
   También podemos usar firma digital para realizar el proceso de autenticación de la copia y del original, puesto que debido a sus características (única, no falsificable, fácil de autenticar, barata y fácil de generar) es ideal para este proceso.
7. Documentar quien preservó la evidencia, donde la preservo, como lo hizo, cuando y porque.

EMBALAJE

8. Empaquetar los dispositivos que contiene las evidencias.
   Los detalles mínimos que deben ser registrados y directa e inequívocamente atribuidos a cada paquete son:
   - Identificador único
   - Nombre de la persona y organización (fuerza de la policía, departamento técnico, etc) responsable de la recolección y empaquetado del material.
   - Breve descripción del material
   - Localización desde donde y a quien fue incautado.
   - Día y hora de la incautación.
9. Los dispositivos magneticos u ópticos (cintas, CDs, discos duros, disquetes, discos Zip / Jaz) u otros dispositivos que expongan placas, deben ser primeramente introducidos en bolsas antiestáticas y después ponerla en una caja cuyo interior podamos rellenar con “plásticos con burbujas” u otro material protector.
10. Documentación en papel (como manuales y libros) en bolsas de plásticos para protegerlos de daños.
11. Toda persona involucrada en un examen forense debería tomar las precauciones necesarias para preservar las evidencias de factores externos tal como electricidad estática, excesivo calor, excesiva humedad, documentado el hecho.

TRANSPORTE

12. Transportar los dispositivos que contiene las evidencias.
    Toda evidencia debe ser transportada a un lugar seguro y cerrado. La cadena de custodia se debe mantener meticulosamente durante el transporte.
13. Si el paquete debe ser enviado mediante correo postal, hay que asegurarse de usar un método que permita el seguimiento del mismo.

En este punto la evidencia digital está preservada.

## FASE 4: ANALISIS DE LAS EVIDENCIAS DIGITALES

El concepto de evidencia digital se forma (normalmente) por el contenido de los ficheros (datos) y la información sobre los ficheros (metadatos). Basándose en estas evidencias el investigador debe intentar contestar a las siguientes preguntas en la fase de análisis:

1. ¿Quién?
Reunir la información sobre el/los individuo/s involucrados en el compromiso.

2. ¿Qué?
Determinar la naturaleza exacta de los eventos ocurridos.

3. ¿Cuándo?
Reconstruir la secuencia temporal de los hechos.

4 ¿Cómo?
Descubrir que herramientas o exploits se han usado para cometer el delito.

La evidencia almacenada debe ser analizada para extraer la información relevante y recrear la cadena de eventos sucedidos. El análisis requiere un conocimiento profundo de lo que se está buscando y como obtenerlo. Hay que asegurarse que la persona que analiza la evidencia está totalmente cualificada para ello.

Cualquier elemento enviado para su análisis forense debería ser en primer lugar revisado para comprobar la integridad del paquete antes de empezar dicho análisis. Cualquier deficiencia en el paquete se debe documentar.

Es importante que el cliente especifique que información es prioritaria de modo que si no se puede lograr una recuperación completa (en caso que el cliente desee dicha recuperación), la recuperación se concentre sobre lo más importante.

Analizar las evidencias digitales va a depender del tipo de datos a analizar, del tipo de sistema en el cual se clasifique el dispositivo comprometido (ordenadores, dispositivos móviles, etc.). Además en función del tipo de delito (fraude, pornografía infantil, drogas, etc.) se deberán analizar unos tipos de evidencias y en un determinado orden (el orden permitirá al investigador forense llegar lo antes posibles y de la forma más precisa a las evidencias digitales para llegar a resolver el delito informático). En el peor de los casos el investigador forense deberá analizar todas las evidencias digitales que posea para resolver el delito.

Existen cuatros categorías de datos:

1. Datos lógicamente accesibles.
   Son los datos más comunes. Las dificultades que podemos encontrar en estos datos son:

- Que haya una gran cantidad de información a analizar (los actuales dispositivos de almacenamiento pueden contener una cantidad ingente de ficheros).
- Que estén cifrados. Si están cifrados con programas como por ejemplo Office es fácil romper la clave; en otros casos (como puede ser al usar PGP) es virtualmente imposible romperlo.
- Que estén corruptos o que tengan trampa (por ejemplo código hostil que al producirse cierta situación puede hacer que se formatee el disco duro, etc.). Se debe usar buscadores de virus para encontrar una clave maliciosa metida en archivos de evidencias, antes de que puedan crear estragos. Aunque la mayoría de los virus residen en programas ejecutables que raramente serán ejecutados en el transcurso de una investigación forense, los nuevos virus (específicamente macrovirus como Melissa o virus de Visual Basic como LoveLetter) aprovechan las vulnerabilidades de algunos S.O y aplicaciones y pueden ser accionados simplemente al ver los documentos en los cuales residen.

  Para saber si un fichero es un troyano podemos realizar a dicho fichero un checksum criptográfico y compararlo con el del fichero original que sabemos que está limpio de código hostil (este checksum criptográfico podría estar en una base de datos).

2. Datos que han sido eliminados (si no han sido sobreescritos se pueden volver a recuperar).
3. Datos en "ambient data" (espacio no asignado, ficheros de swap/page file, espacio entre sectores, espacio entre particiones, datastreams alternativos, etc). Este tipo de datos necesita software especial para poder ser recuperados.
4. Datos en estenografía (proceso por el cual se puede ocultar datos dentro ficheros). Los forenses informáticos pueden usar técnicas esteganográficas para buscar información oculta en los sistemas. Otras veces simplemente buscará la presencia de herramientas comunes de estenografía. Existen varios programas "antiestenografía" que permiten detectar la presencia de datos que están ocultos dentro de ficheros usando técnicas de estenografía. Detectar la presencia de estenografía es más fácil que la extracción de los datos ocultos en si mismo.

A continuación se verá una clasificación de delitos informáticos, propuesta por Naciones Unidas http://www.un.org :

a) Fraudes cometidos mediante manipulación de ordenadores.
b) Manipulación de programas.
c) Manipulación de datos de salida.
d) Fraude efectuado por manipulación informática o por medio de dispositivos informáticos.
e) Falsificaciones informáticas.
f) Sabotaje informático.
g) Virus, gusanos y bombas lógicas.
h) Acceso no autorizado a Sistemas o Servicios de Información.
i) Reproducción no autorizada de programas informáticos de protección legal.
j) Producción / Distribución de pornografía infantil usando medios telemáticos.
k) Amenazas mediante correo electrónico.
l) Juego fraudulento on-line.

Elementos a analizar en función del tipo de sistema:

a) Sistemas informáticos

a.1 Sistemas Windows

- Registro del sistema
- Contenido de Sistema de Fichero Cifrados (EFS)
- FAT o MTF (Tablas de Metadatos de sistemas de ficheros Windows)
- Fichero BITMAP (Fichero creado durante el formateo de volúmenes NTFS para Windows NT y superiores)
- Papelera de reciclaje
- Ficheros de acceso directo
- Active Directory (Windows 2000 y superiores)
- Log de visor de eventos

a.2 Sistemas Unix/Linux

- Listado descriptores de ficheros
- Ficheros SUID/SGID
- Trabajos planificados (schedule jobs)
- Ficheros del historial de la shell

Localización común de evidencias en los sistemas mencionados anteriormente y otros como pueden ser Solaris, SPARC, MVS, etc.:

- Evidencias volátiles.
- Mensajes de correo electrónico.
- Ficheros de trabajo de impresión.
- Archivos temporales de los browsers.
- Cache de los browsers.
- Historiales de los browsers.
- Favoritos de los browsers.
- Ficheros de cookies de los browsers.
- Logs del sistema operativo.
- Logs de aplicaciones.
- Logs de clientes de chat.
- Documentos de texto (cuyas extensiones pueden ser doc, wpd, wps, rtf, txt, etc.).
- Hojas de cálculo (cuyas extensiones pueden ser xls, wgl, wkl, etc.).
- Ficheros gráficos (cuyas extensiones pueden jpg, gif, tif, bmp, etc.).

Otras localizaciones “no tan visibles” (conocido como “ambient data”) que necesitan software especializado para poder ser obtenida la evidencia digital:

- FileSlack (Espacio entre el final de un fichero y el final del cluster en el que se encuentra).
- Ficheros de intercambio (Swap File y Page File).
- Espacio no asignado (Unallocate space).
- Espacio entre sectores.
- Espacio entre particiones.

Otras evidencias (como por ejemplo imágenes que usen estenografía para ocultar otros datos) pueden encontrase en los sistemas de ficheros de otros dispositivos distintos a los anteriormente mencionados (como CDs, DVDs, etc.) o memorias o buffers propios de otros dispositivos (escáneres, impresoras, cámaras de fotos digitales, cámaras de vídeo digitales, etc.).

b) Redes

- Información proporcionada por la tarjeta de red (dirección MAC, dirección IP,...).
- Tabla de direcciones IP asignadas por el servidor DHCP (Protocolo de Configuración de Host Dinámico).
- Cache de ARP (Protocolo de Resolución de Direcciones).
- Logs del IDS (Sistema de detección de intrusos).
- Memoria del IDS.
- Logs del firewall.
- Memoria del firewall.
- Logs de servidores (Web, FTP, de correo electrónico).
- Mensajes de correo electrónico almacenados en el servidor.
- Logs de modems.
- Información de routers:
  RAM con información de configuración.
  Cache ARP.
  Logs del router.
- Datagramas almacenados cuando el tráfico es alto.
- Información de servidores DIAL-UP (Servidores ISP).
- Logs del servidor DIAL-UP.
- Memoria del servidor DIAL-UP.
- Logs del servidor de autentificación.
- Memoria del servidor de autentificación.
- Logs del servidor VPN
- Memoria del servidor VPN

c) Redes inalámbricas

Dentro de las redes inalámbricas debemos diferenciar 2 tipos:

c.1 Redes LAN Inalámbricas (Wireless LAN):

- Información proporcionada por las tarjetas inalámbricas de red (direcciones MAC, direcciones IP, etc.).
- Puntos de acceso.
- Logs de modems wireless.

c.2 Redes inalámbricas basadas en conmutación de circuitos (por ejemplo de telefonía móvil):

- Registros de facturación CDR (Charging Detail Records). Registros que contienen información para cada llamada realizada, como número que se llamó, el día de la llamada, duración, entre otros, organizados por clientes para efectos de facturación. Estos registros son archivados y están

disponibles en un periodo aproximado de varios años, dependiendo de las políticas de la operadora.

- HLR (Home Location Register).Contiene información del subscriptor, referente a sus capacidades móviles contratadas (clase de servicio), la identificación de la unidad móvil, la ubicación actual de la misma ya sea en el área de cubrimiento de la red proveedora o de otras redes celulares (roaming), la información de autenticación, el nombre de la cuenta y la dirección de facturación.
- VLR (Visitor Location Register). Almacena información física, electrónica y de radio, acerca de todos los usuarios que están actualmente autenticados dentro de una red particular del MSC (Mobile Switching Center o centro de conmutación móvil). Dicha información incluye la localización actual del dispositivo móvil y el estado del mismo (activo, en espera, etc.).
- OMC (Operation and Maintenance Center o Centro de operación y administración). Realiza tareas administrativas como obtener datos de la MSC para propósitos de facturación y administra los datos de la HLR. Además, proporciona una visión del estatus de operación de la red, la actividad de red y las alarmas. A través de éste, es posible examinar una o rastrear una llamada móvil particular en progreso (*móbile trace*).

d) Dispositivos móviles:

d.1 Teléfonos móviles

- Ficheros con distinta información almacenada en la tarjeta del movil (SIM: Subscriber Identity Module, código PIN, código PUK). Esta tarjeta es una Smart Card (ver sección Memoria Cards)
- Chips de memoria Flash (Estas memorias contienen información sobre el teléfono así como software interno del mismo).
- Numero IMEI (International Mobile Equipment Identity)
- Números de teléfonos almacenados
- Mensajes de texto
- Configuraciones (lenguaje, día/hora, tono/volumen, etc).
- Grabaciones de audio almacenadas.
- Programas ejecutables almacenados
- Configuraciones de Internet, GPRS, WAP
- Log de llamadas (llamadas realizadas, recibidas, perdidas).
- Datos (logs de sesiones, números marcados, etc) contenidos en dispositivos a los que se haya conectado el teléfono móvil (computadoras de sobremesa, ordenadores portátiles,...).

d.2 Organizadores de mano (PDAs, Pockets PC, etc.)

- RAM.
- ROM. Memoria en la que se encuentra el sistema operativo y las aplicaciones base.
- FLASH-ROM. Memoria en la que podemos guardar aplicaciones y datos que no queremos perder por un reseteo del dispositivo o porque no tenga batería.
- Datos (de sincronización, contactos, tareas, etc.) contenidos en dispositivos a los que se en dispositivos a los que se haya conectado el teléfono móvil ( ordenadores de sobremesa, ordenadores portátiles, teléfonos móviles, ...).

e) Sistemas embebidos

e.1 Memory sticks y memory cards (Smarts Card y Compact Flash)

Básicamente su recolección de datos es igual que la de un disco duro puesto que se basan en sistemas de ficheros tipo FAT (normalmente).

Las estructuras de datos en las que se pueden analizar evidencias son:

- CIS (Card Information System) Area oculta que contiene información del fabricante.
- MBR (Master Boot Record) En las tarjetas este sector esta presente por razones de compatibilidad y raramente se usará como arranque de un disco duro (aunque los delincuentes, podría ocultar aquí información).
- Sector de arranque. Se usa junto al MBR para establecer la geometría del dispositivo.
- FAT. Contiene la lista que describe los cluster ocupados por los ficheros.
- El área de datos que contiene los datos de los ficheros actuales.

f) Otros dispositivos

Normalmente la mayoría de estos dispositivos serán sistemas embebidos. Debido a la exclusividad de cada uno de ellos, habrá que conseguir la documentación propia del dispositivo (a través del fabricante, Internet, etc.) para saber donde puede almacenar evidencias.
Podemos hacer la siguiente clasificación:

f.1 Sistemas de oficina

- Teléfonos fijos.
- Fax.
- Fotocopiadoras.

f.2 Sistemas de comunicación

- Enlaces de radio y TV.
- Enlaces de satélite.
- Sistemas de llamadas.

f.3 Sistemas de transporte

- GPS (Global Positioning System).
- Sistemas embebidos en coches, trenes, etc., como pueden ser airbag, sistemas de navegación, cierres electrónicos, etc.
- Sistemas de monitorización.
- Sistemas de control de tráfico.
- Sistemas de control de tráfico aéreo.
- Sistemas de radar.

f.4 Equipamientos domésticos

- Alarmas contra robos.

f.5 Sistemas de mantenimiento de edificios

- Sistemas de emergencia (UPS, etc.).
- Sistemas de control de acceso.
- Sistemas de registros.
- Cámaras de circuito cerrado.

f.6 Sistemas de producción

- Sistemas CAM.
- Sistemas CAD.
- Sistemas de control de energía (electricidad, agua, gas, etc.).
- Sistemas de producción de energía (electricidad, agua, gas, etc.).
- Sistemas de registro de tiempo.
- Sistemas de simulación.
- Robots.

f.7 Bancos

- Cajeros automáticos
- Sistemas de tarjeta de crédito

f.8 Sistemas médicos

- Equipo para imagen y procesamiento (radiografías, resonancias magnéticas, etc.).
- Equipo cardiaco.
- Equipo de ventilación.
- Equipo de respiración asistida.
- Equipo de anestesia.
- Equipo de esterilización.
- Equipo de desinfectación.

## FASE 5: PRESENTACION Y REPORTES

Basándose en las fases anteriores, en toda la documentación disponible del caso y basándose también en la cadena de custodia, la presentación y/o sustentación del informe pericial es la fase de comunicar el significado de la evidencia digital, los hechos, sus conclusiones y justificar el procedimiento empleado.

El propósito de la presentación de los informes es proporcionar al lector toda la información relevante de las evidencias de forma clara, concisa, estructurada y sin ambigüedad para hacer la tarea de asimilación de la información tan fácil como sea posible.

La forma de presentación es muy importante y debe ser entendible por personas no conocedoras del tema en discusión.

Es decisivo que el investigador presente las evidencias en un formato sencillo de entender, acompañado de explicaciones que eviten la jerga y la terminología técnica.

Durante un juicio la investigación debe presentar evidencias informáticas de una manera lógica, precisa y persuasiva de forma que el jurado entenderá y que el abogado de la parte opuesta no podrá contradecir. Esto requiere que las acciones del experto forense puedan ser reconstruidas paso a paso con fechas, horas, cuadros y gráficos (el uso de programas como Excel, Word, PowerPoint, etc. puede ser de gran ayuda en este punto).

Si el abogado del sospechoso es capaz de levantar dudas sobre la integridad de la prueba o si es capaz de demostrar que el investigador realizó algún procedimiento no sustentable, todo el informe puede ser rechazado. Es importante, más allá de lo que esté escrito en el informe pericial, que el investigador sepa sustentar correctamente ante jurado cada tarea realizada en sus investigación.