GUIA DE BUENAS PRÁCTICAS PARA EL PERITAJE INFORMATICO EN RECUPERACION DE IMAGENES Y DOCUMENTOS

Madrid, 20 Octubre 2003

Agradecimientos: A Javier Pagès López, Francisco García Lombardía y los Ingenieros en Informática que construyen Infoperitos, por sus aportaciones y comentarios.

Ignacio Boixo

Es Informático del Banco de España, en coordinación de Asuntos Europeos. Ingeniero en Informática. Perito Judicial. Responsable del Peritaje Informático en la Brigada de Investigación del Banco de España. Ha colaborado como consultor en el Banco Central Europeo y en la Supervisión Bancaria de Bosnia-Herzegovina., y como revisor de proyectos en la Comisión Europea. Preside la Asociación de Ingenieros en Informática de Madrid y coordina su Gabinete Técnico y Facultativo *Infoperitos*. Colegiado en el Colegio Profesional de Ingenieros en Informática de Castilla y León. Socio de ISSA y de ATI.

Índice

INTRODUCCIÓN

Esta guía de buenas prácticas tiene como objeto el difundir un protocolo común, y homogeneizar la realización de peritajes informáticos, especialmente los orientados a recuperar documentos e imágenes.

Estas buenas prácticas son el resultado de variadas experiencias en la realización de pericias informáticas, así como de la consulta de documentación referente al tema. Son una plasmación de los códigos de práctica y conducta del Gabinete Técnico Facultativo de Peritos Informáticos -Infoperitos- de la Asociación de Ingenieros en Informática -AI2-. Las referencias y bibliografía se pueden encontrar básicamente a través de www.infoperitos.com.

El ámbito del peritaje informático en recuperación de imágenes y documentos está orientado a extraer de equipos informáticos intervenidos aquellos ficheros que puedan ser relevantes, muchas veces en un contexto de ámbito penal, aunque también puede seguirse, exactamente el mismo procedimiento, para el ámbito civil u otros.

La lógica del peritaje de este tipo está basada en presentar el contenido de ficheros que puedan tener relevancia jurídica, informando de su significado y características. Esos ficheros deben haberse mantenido en una "cadena de custodia", por lo que se detallarán los pasos desde que se intervienen o reciben los equipos informáticos, hasta que se presentan los ficheros relevantes. El peritaje ha de poder ser repetido, por lo que no se pueden alterar los elementos informáticos originales, trabajándose siempre sobre copias clónicas.

La mayoría de estos peritajes están referidos a ordenadores de usuario con sistema operativo Windows. Para efectuar peritajes en equipos servidores y/o en otros sistemas operativos, se seguirán los mismos pasos con las correspondientes adaptaciones al entorno.

Los pasos a realizar en este tipo de peritajes informáticos son básicamente cuatro:

1. Intervención. Se aprehenden los elementos informáticos.
2. Revisión preliminar. Se descartan los elementos informáticos irrelevantes y se preparan los demás.
3. Exploración de ficheros. Se localizan, imprimen y describen los ficheros informáticos relevantes.
4. Informe pericial. Se confecciona el informe, y se cierra el peritaje.

Siguiendo estas precauciones, el peritaje se explicará por sí mismo, y el perito simplemente se remitirá a lo ya expuesto en su peritaje. Cuanto más claro e irrefutable el peritaje, menos presencia posterior del perito.

1.- INTERVENCION

En la entrada a los locales donde estén los equipos informáticos, se deberá acudir provisto de máquina fotográfica o vídeo, rotulador para CD y destornilladores.

La máquina fotográfica será utilizada para obtener imágenes de las pantallas de los ordenadores, en el caso de que estuvieran en funcionamiento. También se fotografiarán los equipos.

No se deberá permitir que nadie toque los ordenadores encendidos bajo ningún concepto.

La forma de apagar los ordenadores es directamente quitándoles la energía eléctrica. Esto se debe a que, en un apagado ordenado, parte de los ficheros temporales, que pudieran ser significativos, serían automáticamente borrados. Tampoco se tiene la garantía de que, en el proceso de apagado, no se

borren o introduzcan intencionadamente ficheros, lo que podría invalidar el peritaje. De esta manera, apagando los equipos sin ninguna manipulación, no ha lugar a ningún tipo de conjetura sobre la cadena de custodia. Un perito profesional informático podría, antes de apagar, extraer una imagen pericial del estado de los procesos en ejecución mediante herramientas periciales del tipo de Forensic and Incident Response Environment. Si se quitase algún cable antes de apagar, quizá se disparase un autoapagado, lo que se debe evitar.

Los elementos a peritar en una intervención son fundamentalmente los soportes de datos.

Los siguientes elementos informáticos no son relevantes a efectos de pericias informáticas:

- Pantallas de ordenador
- Teclados y ratones
- Impresoras
- Equipos de telecomunicaciones
- Cables
- CD o DVD grabado en fábrica
- Aquellos equipos que no almacenen datos

De todos estos elementos lo único que se debe hacer es inventariarlos, y fotografiarlos, para poder señalar en su momento que fueron encontrados en el lugar de la intervención. Físicamente, su peritación no aportaría ninguna luz. En el caso de las impresoras, no hay un método eficiente para individualizar una en concreto a través de su "huella" en el papel, por lo que no son relevantes en peritajes informáticos.

Se deberán intervenir los siguientes elementos informáticos:

- Ordenadores (sobremesa, portátiles y agendas PDA)
- Discos ópticos -CD y DVD- (excepto los grabados en fábrica)
- Discos flexibles -disquetes-
- Discos duros de ordenador
- Unidades de almacenamiento externas (PenDrive, Reproductores MP3, Discos, Memorias, dispositivos USB…)
- Teléfonos móviles (almacenan agendas e información)
- Todo tipo de soporte de almacenamiento permanente de datos en general.

Los lectores grabadores de tarjetas magnéticas (si existiesen) se intervendrán, por ser equipos que habitualmente carecen de uso fuera de la manipulación de tarjetas.

Todos los soportes de datos deberán ser inventariados.

Los discos duros tienen número de serie. Los discos ópticos suelen tener un número de serie en la parte transparente del orificio central. Los discos flexibles tienen números de serie frecuentemente repetidos, y eso cuando los tienen. Una alternativa es firmar con un rotulador de CD todos los discos ópticos y discos flexibles intervenidos.

Los ordenadores portátiles deben ser intervenidos, por la dificultad que entraña extraer sus sistemas de almacenamiento en el mismo lugar de la intervención.

En los ordenadores de sobremesa se recomienda extraer e intervenir sus sistemas de almacenamiento. La carcasa, CPU, placas, memoria RAM y otros componentes del ordenador no tienen interés a efectos de pericias informáticas. Sólo los sistemas de almacenamiento permanente de datos son relevantes.

Para extraer los sistemas de almacenamiento de datos de un ordenador de sobremesa, normalmente solo se necesita un destornillador de estrella y seguir las siguientes instrucciones:

1. Apagar el ordenador
2. Quitar la carcasa

3. Desconectar el cable de datos (normalmente IDE) y de alimentación del disco duro
4. Quitar los tornillos al disco duro
5. Extraer el disco duro SIN TOCAR LOS CIRCUITOS (peligro de daños)
6. Firmar el disco duro
7. Guardar el disco duro en un sobre antiestático[1] o de papel
8. Una vez extraído el o los discos duros, se volverá a conectar el ordenador, para abrir el lector de CD y extraer algún CD, DVD o disquete que hubiera dentro
9. Inventariar los números de serie del ordenador y de los elementos extraídos y fotografiarlos

En muchas ocasiones, el perito no estará presente en la intervención. En lo posible, el perito deberá informar a quien haga la intervención del contenido de este capítulo. Para ellos se recomienda distribuir el siguiente decálogo:

1. Inventariar y fotografiar los equipos informáticos
2. Intervenir todos los discos: flexibles (disquetes), compactos (CD), y video (DVD).
3. Intervenir los ordenadores portátiles, agendas (PDA) y teléfonos móviles con sus cargadores.
4. Intervenir los ordenadores de sobremesa, o mejor extraer el disco duro (sin tocar su circuito, y guardarlo en un sobre antiestático o de papel), DVD, CD y disquetes.
5. Intervenir dispositivos y tarjetas de memoria, así como cualquier medio de almacenamiento
6. Intervenir lectores y grabadores de tarjetas magnéticas
7. No intervenir equipos que no almacenen datos, como pantallas, teclados, ratones, impresoras, cables,…
8. Nadie toque un ordenador encendido: fotografiar la pantalla y quitar la energía eléctrica.
9. Firmar todos los equipos informáticos intervenidos.
10. En caso de duda, consultar en www.infoperitos.com

2.- REVISION PRELIMINAR

Discos flexibles y ópticos

Los discos flexibles y ópticos pueden leerse en cualquier ordenador personal. Se tomará la precaución de mover la pestaña en los discos flexibles para que queden en posición de “solo lectura”. Tomadas estas precauciones, los discos ópticos y flexibles pueden explorarse en cualquier ordenador personal, abriendo los ficheros sin miedo a alterar el soporte original.

En caso de que un disco de errores de lectura, o esté deteriorado, se le hará una copia clónica, intentando recuperar los sectores defectuosos, y solo se utilizará la copia clonada.

Para hacer una copia clónica de un disco flexible, es suficiente la utilidad de copia de discos del explorador de Windows.

Para hacer una copia de un disco óptico, cualquier clonador de CDs es válido. Si los sectores defectuosos lo son por sistemas antipiratería, es irrelevante como queden. Si los sectores defectuosos lo son por daños en el medio físico, da igual que la copia clónica tenga ese sector dañado de la misma manera o de cualquier otra. Lo importante es que la copia clónica del disco óptico sea completa.

[1] Sobres antiestáticos se encuentran en Caycon S.L.

Discos Duros

La precaución es evitar cualquier modificación del disco duro. Al abrir un fichero, muchos programas crean un fichero temporal en la misma carpeta. Esto altera el disco duro original, y no es una buena práctica. Arrancar un ordenador hace que se modifiquen y escriban múltiples ficheros, por lo que se ha de evitar siempre.

Se recomienda clonar el disco duro intervenido y explorar la copia clonada. Con esto se evita modificar en lo más mínimo el disco duro intervenido, lo que podría invalidarle como prueba pericial.

Para hacer una copia clónica de un disco duro, se necesita un disco duro virgen, un ordenador de sobremesa, y cualquier programa de copia de discos autoarrancable desde disquete -que no intervenga para nada el sistema operativo del disco duro-, como puede ser Drive Image o Knoppix STD. El disco duro copia ha de estar limpio de cualquier tipo de dato previo. Se recomienda un disco duro de fábrica a estrenar. Si se quiere reutilizar algún disco duro, previamente habrá que hacerle un formateo completo a bajo nivel, rellenándolo de ceros binarios. El objetivo es evitar que sectores existentes en el disco duro que va a recibir la copia, puedan aparecer como pertenecientes al disco duro intervenido. La copia ha de ser clónica, incluyendo todos los sectores, para evitar que ficheros en borrado lógico queden sin copiar. La partición del disco duro intervenido y la de la copia han de tener, por tanto, el mismo tamaño. Es admisible que la partición en la copia no sea primaria, sino secundaria o extendida, para poder poner varios discos duros intervenidos dentro de un solo disco duro de copia físico. El disco duro copia se etiquetará con las indicaciones de los discos duros originales intervenidos. Los discos originales intervenidos no se tocarán más.

Soportes de datos de Lectura/Escritura

En cualquier soporte de datos que admita escritura, se utilizará la misma estrategia que en los discos duros, esto es, se clonarán a un soporte de datos virgen del mismo tipo.

Ordenador portátil

Para obtener una copia de los datos de un portátil existen varias soluciones.

Si el portátil dispone de grabador de CDs, se arrancará el portátil con un programa con sistema operativo integrado (no arrancar desde el disco duro) y se obtendrá una imagen del disco duro en un disco óptico. El disco óptico se volcará a su vez, a través de un ordenador de sobremesa a un disco duro virgen.

Otra opción es extraer el disco duro del portátil, y con un adaptador conectarlo a un ordenador personal, para entonces copiarlo a un disco duro virgen.

En todo caso, nunca se debe arrancar el ordenador portátil desde su disco duro, pues lo alteraría.

Ficheros borrados

Una vez realizada una exploración de los ficheros existentes, se deberá utilizar un programa de recuperación de ficheros borrados (como el programa Revive) para localizar potenciales ficheros relevantes que hubiesen sido borrados. El los discos ópticos, se puede grabar a continuación de lo ya grabado, haciendo inaccesible lo anterior: también se deberán revisar estas grabaciones previas, si existiesen.

En caso de incluir un fichero borrado y recuperado en el informe pericial, deberá explicarse prolijamente el método por el que se ha obtenido.

3.- EXPLORACION DE FICHEROS

Imágenes

Las imágenes, sobre todo las referentes a falsificaciones, tienen una característica fundamental: para tener cierta calidad han de tener bastante tamaño.

El procedimiento más sencillo para localizar las imágenes de un medio es el programa estándar de exploración de Windows. Se utilizará la búsqueda, seleccionando opciones de búsqueda para que el tamaño mínimo del fichero a buscar sea superior a un tamaño determinado, por ejemplo 100 KB.

Teniendo en cuenta que la gran mayoría de los ficheros en un ordenador son de pequeño tamaño, seleccionar todos los ficheros superiores a un límite determinado reduce enormemente el número de ficheros. Una vez seleccionados los ficheros superiores a un tamaño, se procede a revisar los resultados, clasificándolos por fecha, o por carpeta o por tipo.

Normalmente la experiencia indica que los ficheros relevantes se suelen encontrar en los directorios normales de usuario, por ejemplo en “Mis documentos”.

Las técnicas de esteganografía, basadas en ocultar una imagen relevante dentro de otra imagen de apariencia anodina, no suelen estar al alcance de personas sin sólidos conocimientos informáticos, por lo que, salvo en casos muy concretos, no se realizarán análisis esteganográficos.

Un caso particular es la localización de imágenes en Internet. Normalmente, los ficheros de un ordenador, a efectos periciales, se pueden dividir en aquellos referidos a Internet y aquellos no referidos a Internet.

Una buena práctica, si se dispone de tiempo y recursos, especialmente en aquellos discos duros que contienen un gran número de imágenes, es copiar la información de Internet a una partición y el resto a otra partición, explorando entonces cada partición por separado. Una forma de realizar esta copia es clonar el disco duro y luego, desde el explorador de Windows cortar y pegar el directorio de Internet (dentro de las carpetas del sistema operativo Windows) a otra participación en el disco copia.

Hay que tener en cuenta que los ficheros de Internet, especialmente los gráficos, tienen tamaños menores que los ficheros distribuidos en soporte físico. En temas de fotografías de menores, es en los ficheros del directorio de Internet el sitio más probable donde encontrar ficheros relevantes. También en el directorio de Internet es más probable localizar ficheros de imágenes relevantes que identifiquen actividades a las que el usuario del ordenador se ha dedicado. Por ejemplo gestiones bancarias o de otro tipo donde va a figurar el nombre y la identificación del usuario. Esto es muy interesante a la hora de poder justificar que ese disco duro ha sido utilizado por un usuario determinado.

Un programa muy útil para la localización de imágenes es el que busca y muestra todas las imágenes de una carpeta o de un soporte determinado, selecciona aquellas que contienen imágenes, y las presenta como miniaturas en pantalla. El programa ACDsee es paradigmático en este aspecto. Con un programa de este tipo se pueden recuperar, por ejemplo, todas las imágenes contenidas en el directorio de Internet y presentarlas en pantalla como miniaturas, inclusive clasificadas por tamaño. De esta manera se puede revisar rápidamente miles de imágenes.

Por cada imagen relevante seleccionada se procederá de la siguiente manera:

1. Se obtendrá una "foto" del directorio donde estaba el fichero. Esto se puede hacer mediante el explorador de Windows hasta localizar el fichero. Luego se "fotografía" la pantalla pulsando simultáneamente las teclas “alt” y “impr pant” y, en un documento de Word, pulsar el botón derecho del ratón y seleccionar “pegar”. La "foto" quedará pegada en el documento Word.

2. Se copiará la imagen a un directorio de trabajo, que podemos denominar “imágenes relevantes”.
3. Se imprimirá cada imagen con un pie que consista en la ruta completa del fichero. Para ello se utilizará un buen programa de tratamiento de imágenes, como Photoshop o PhotoPaint. Estas hojas con las imágenes impresas formarán el "Anexo II: ficheros relevantes" del informe pericial.

En el caso de falsificación de billetes o documentos con números de serie, se hará una ampliación digital de los números de serie. El objetivo es revisar si los números de serie, especialmente los últimos dígitos han sido manipulados. Es habitual encontrar una misma imagen que da lugar a distintas falsificaciones por el procedimiento de alterar el número de serie. También revisar formularios sellados en blanco, por si hubiesen sido manipulados para borrar lo escrito y dejar los campos en blanco.

Documentos

La exploración de documentos no tiene relación con la exploración de imágenes. Los ficheros de documentos son de tamaños muy variados, y también pueden estar en cualquier sitio.

La buena práctica indica que los ficheros con documentos suelen estar en las carpetas de usuario, y además con las extensiones habituales (.doc .xls .txt . pdf .rtf .htm y similares). Por tanto es muy útil el explorador de Windows, buscando en el disco duro completo por tipo de fichero.

Es importante localizar ficheros relevantes que identifiquen al usuario del ordenador, especialmente los ficheros donde figuren el nombre y los datos del usuario. Esto es muy interesante a la hora de poder justificar que ese disco duro ha sido utilizado por un usuario determinado.

Hay gran cantidad de ficheros de distribución que pueden dificultar la búsqueda de ficheros relevantes. Habitualmente, con una simple clasificación por fecha, se detecta rápidamente cuales son los ficheros de distribución de un producto determinado, ya que suelen tener todos la misma fecha.

Para ver el contenido de un fichero que no tiene una extensión reconocida, y no es de un gran tamaño, una opción muy rápida es abrirlo con el programa de utilidad “bloc de notas”.

Programas

Desde el punto de vista pericial, es también importante determinar qué programas se han utilizado en un ordenador. No es lo mismo que el ordenador disponga exclusivamente de los programas de tratamiento de imágenes que vienen ya instalados con el sistema operativo, a que se encuentre toda una panoplia de software de exploración, de tratamiento y de impresión de imágenes, sobre todo si también se encuentran imágenes relevantes.

Aunque cada uno de estos programas no tiene relevancia independiente, el conjunto de un elenco de programas de tratamiento de imágenes con ficheros con imágenes de falsificaciones si que puede tener relevancia. Los efectos de la relevancia no han de ser determinados por el Perito, que deberá ceñirse a indicar si los medios técnicos, programas y ficheros forman un conjunto apto para el tratamiento de imágenes.

Un caso especial son los programas utilizados para la falsificación de tarjetas magnéticas. Se suelen reconocer porque están escritos en Visual Basic (extensión .vba). Abierto el fichero con el bloc de notas, se pueden ver los comentarios del programa que indicarán su uso. Por su propia naturaleza, no hay software de difusión masiva para el manejo de lectores grabadores de tarjetas magnéticas, que sea accesible al público en general, por lo que es habitual el desarrollo de programas "ad hoc". Es muy

conveniente relacionar el programa con los lectores de tarjetas magnéticas intervenidos, ya que cada programa suele tener opciones para el manejo de unos determinados modelos de lectores grabadores de tarjetas.

4.- INFORME PERICIAL

Los informes periciales suelen seguir la misma pauta cuando se refieren a similares asuntos. Se adjunta un informe tipo utilizado en informes periciales referentes a falsificación de billetes.

Los apartados más relevantes son los siguientes:

Portada

Deberá orientarse a identificar clara y rápidamente el contenido del informe pericial. Donde se ha hecho el peritaje, la referencia y a quien va destinado (normalmente identificando Juzgado y diligencias). Los datos de la portada se resumirán y repetirán como pie de página a lo largo del peritaje.

Peritos

Identificación del Perito o los Peritos. En los peritajes de índole penal, es muy común omitir el nombre y apellidos del Perito y sustituirlo por un número de identificación, como puede ser un número de colegiado.

Antecedentes

Es un inventario de los equipos intervenidos y de su procedencia.

Prueba pericial

Se describen los pasos dados desde la recepción de los equipos intervenidos hasta la obtención de los ficheros relevantes.

Se debe indicar el código o códigos de conducta o de buenas prácticas que se han seguido. Por ejemplo el código de práctica y conducta de Infoperitos.

Se describe los pasos realizados para la obtención de discos copia.

Se detallan las características técnicas de los elementos informáticos intervenidos.

Se enumeran los ficheros relevantes encontrados, y los equipos informáticos donde fueron hallados.

Ficheros relevantes

Se describe, para cada fichero relevante encontrado, el contenido que le hace relevante. En los casos de falsificación, este apartado suele ser cumplimentado por un experto pericial en falsificaciones.

Conclusiones

Se indica en que componentes informáticos se han encontrado ficheros relevantes, y un resumen del contenido que les hace relevantes, inclusive enlazando con datos de identificación de usuario que se hubieran encontrado. Este apartado es generalmente un resumen del apartado de ficheros relevantes.

Firma

Se inventarían los elementos informáticos relevantes que quedan como resultado de la prueba pericial, y que se remiten con el informe, esto es, todos los soportes de almacenamiento donde se han encontrado ficheros relevantes. Es muy conveniente grabar los ficheros relevantes y el propio informe pericial en un CD, (grabarlo con sesión “cerrada” para que no se pueda manipular), que permitirá acceder con facilidad a los ficheros relevantes.

En otra relación, se devuelven los elementos informáticos que no hayan resultado relevantes.

El Perito no debe quedarse con ningún elemento informático intervenido. Debe devolverlos todos, señalando y distinguiendo aquellos elementos informáticos que contienen elementos relevantes de aquellos donde no se han encontrado elementos relevantes.

Anexos I: equipos peritados

Se incluirán las fotografías de los equipos peritados, así como de las imágenes de las carpetas donde se encontraron los ficheros relevantes.

Anexo II: ficheros relevantes

Se incluirá el contenido de cada fichero relevante con la ruta completa donde fue encontrado.

Conservación de elementos periciales

Una vez realizado el informe pericial se deben conservar los siguientes elementos en poder del Perito:

1. Copia del informe pericial
2. Copia del CD con los ficheros relevantes y el informe pericial
3. Disco duro copia utilizado en la realización del peritaje.

Si por algún motivo el disco duro copia se alteró durante la realización del peritaje, deberá volver a clonarse de nuevo, para su conservación.

5.- ENLACES

Asociación de Ingenieros en Informática www.ai2.as

Asoc. Ing. Informática Madrid www.ai2madrid.org

Infoperitos www.infoperitos.org

Information Systems Security Assc. www.issa.org

Ignacio Boixo ignacio@boixo.com