

Juan Luis García Rambla

Un forense llevado a juicio



FLU - PROJECT

_sidertia



"Hay ciertas pistas en la escena de un crimen que por su naturaleza nadie puede recoger o examinar ¿cómo se recoge el Amor, la Ira, el Odio, el Miedo...? son cosas que hay que saber buscar"

Dr. James T Reese.





Reconocimiento-NoComercial 2.5 España

Usted es libre de:

-  copiar, distribuir y comunicar públicamente la obra.
-  hacer obras derivadas.

Bajo las condiciones siguientes:

-  **Reconocimiento.** Debe reconocer los créditos de la obra de la manera especificada por el autor o el licenciador (pero no de una manera que sugiera que tiene su apoyo o apoyan el uso que hace de su obra).
 -  **No comercial.** No puede utilizar esta obra para fines comerciales.
- Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra.
 - alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor.
 - Nada en esta licencia menoscaba o restringe los derechos morales del autor.

Los derechos derivados de usos legítimos u otras limitaciones reconocidas por ley no se ven afectados por lo anterior.

Esto es un resumen legible por humanos del texto legal (la licencia completa) disponible en la siguiente dirección:

<http://creativecommons.org/licenses/by-nc/2.5/es/legalcode.es>



Indice

Prólogo.....	3
Capítulo 1 – El análisis forense	5
Capítulo 2 – La importancia de las evidencias	8
Capítulo 3 – El procedimiento de copiado de discos.....	12
Capítulo 4 – La cadena de custodia	25
Capítulo 5 – Las buenas prácticas en el análisis.....	29
Capítulo 6 – El informe pericial	34
Capítulo 7 – Prueba anticipada en un proceso Civil	39
Capítulo 8 – Un Juicio Civil	42
Capítulo 9 – Claves de un forense en Juicio	46



Prólogo

Muchas de las noticias que salpican a diario las noticias tienen que ver con filtraciones, abusos o ataques relacionados con la tecnología. Sin embargo por encima de aquellos que destacan, hay muchísimos miles de casos que no se juzgan socialmente, sino que se dirimen en una sala y son conocidos por unos pocos. Sin embargo cada uno de ellos puede resultar mucho más importante para cada persona implicada y otras de las que ni siquiera son conscientes, que aquellos de gran impacto social.

En la labor de muy pocos está el llegar a esclarecer situaciones que en ocasiones son muy críticas y que pueden tener como consecuencia la cárcel para algún afectado. Evidentemente esto no es algo que puede tomarse a la ligera y cualquier investigación requiere de su debida importancia y el llevar unos procedimientos adecuados.

La investigación forense se rodea muy a menudo de un misticismo entre todos aquellos que trabajan con tecnología. Sin embargo hay que tener presente que aunque la carga técnica es importante existen muchos detalles que se encuentran muy alejados de la visión general que se tiene. Esto resulta mucho más acusado cuando un caso forense deriva en la posibilidad de llegar a juicio.

Ante esta circunstancia todo el componente técnico del que se visten muchos consultores debe dejar paso a procesos en los que no se encuentran tan cómodos. En un juicio el técnico ya no se encuentra en su elemento, aquí el ya no es el “Juez”, sino que incluso en ocasiones se siente juzgado.

Situaciones que técnicamente se dan por sentado en el entorno profesional informático pueden ser cuestionadas en una vista. El especialista forense digital debe por lo tanto conjugar su pericia técnica con la capacidad para enfrentarse a temas para los que no se encuentra a menudo preparado. El éxito depende de muchos factores y en los que a menudo el propio perito es un mero espectador.

A lo largo del manual, Juan Luis García Rambla, Director Técnico de seguridad de Sidertia Solutions dará un repaso a todo un proceso forense. Desde los apartados más técnicos, tratando herramientas y procedimientos a seguir, hasta los aspectos legales

que podrían llegar a ser el determinante en un juicio en el que un técnico formase parte como perito.

Toda la información que proporciona la ha obtenido de su propia experiencia en la participación de casos forenses, bien sea como perito o coordinando equipos de analistas forenses. Aporta a través de este manual una visión muy particular pero que sin duda permite llegar a un juicio con unas garantías de éxito significativas.

Resulta muy útil especialmente para aquellos que inician sus pasos en el delicado mundo del análisis forense, pero también ofrece una visión particular muy interesante para todos aquellos que aunque ya experimentados nunca han asistido a un juicio.

Juan Antonio Calles García



Capítulo 1 – El análisis forense

Un análisis forense compete una de las actividades que dentro de la seguridad informática puede ser de las más gratificantes o de las más desagradables. Tiene la perspectiva de poder complicarse a límites insospechados algo que a priori presentaba visos de ser muy sencillo. A todo ello se une un componente difícil de digerir que consiste en que por muy técnicos que pueden ser los resultados, por muy metódicos que lleguen a ser los procedimientos y por muy claro que puedan ser las conclusiones, no deja de estar cargado todo el proceso de cierta subjetividad. Es más en un determinado momento la decisión será tomada por alguien que tendrá limitaciones técnicas para apreciar lo dispuesto en el informe.

La realización de un análisis forense plantea de inicio un dilema esencial para que este pueda llegar a buen puerto, ¿las conclusiones tendrán cómo resultado que se llegue o no a un juicio? Esta cuestión para todos los que son técnicos, no parece tener mucha importancia... hasta el momento en el que se entra en la sala donde se celebra el juicio y que desarrollará sus labores como perito. Allí puede enfrentarse a las preguntas más retorcidas y para las que seguramente no se encuentre totalmente preparado. Es en ese momento cuando uno se da cuenta de la importancia de haber hecho bien las cosas y de qué con solo una sola pregunta malintencionada y una mala respuesta (por muy bienintencionada que sea) puede llegar a desbaratarse el mejor de los periciales que haya llegado a realizarse. Es ahí cuando se aprende, a que si no las cosas no se han hecho bien desde principio, lo que se opinaba que acabaría en una sonora ovación, acabará en la frustración de que estaba “casi” todo bien y un por lo menos “lo intentamos”.

Enfrentarse a un caso forense es tener que anticipar de primeras la posibilidad de llegar a juicio. A menudo, y en función del escenario, es posible que ese hecho no se plantee inicialmente, pero tal y como se desencadenen los acontecimientos podría llegar a acabar de una forma diferente a como originalmente se esperaba. Supóngase un caso de malware en una empresa donde el equipo de un directivo estuviera haciendo “cosas raras”. El objetivo inicial que plantearía la empresa pasaría

seguramente por conocer qué está pasando, por qué su antivirus no lo habría detectado y qué podrían hacer para saber si está en otros ordenadores. Sin embargo, en el transcurso del forense no solo se detecta al elemento malicioso, sino la actividad malsana que está realizando. Esto podría derivar en llegar a detectar a quién lo ha colocado allí y en conocer la información que se obtiene del directivo. Suponiendo que el actor (denominación judicial, para ir entrando en materia) fuera de la empresa y su objetivo un tanto “torticero”, la empresa ¿no querría llevarlo a juicio?

Muchas veces en casos forenses se sabe cómo comienza, pero en ninguna circunstancia como puede llegar a acabar. Con lo cual a riesgo de ser pesado, es mejor asegurarse por parte del interesado si su objetivo es llevar o no el caso a los juzgados. En muchas ocasiones los interesados, dirán que no, que ese no es el objetivo. Sin embargo, no son conscientes de la circunstancia y de cómo puede acabar el caso (recuérdese la casuística anterior). Es mejor de antemano platearles la situación real e indicar que existe el riesgo de que determinados procedimientos pueden conllevar que la recogida o análisis de una forma pudieran ser válidos y en otras no tanto. Siempre se habla de posibilidades puesto que en un juicio la decisión final se dirime en una habitación y en ocasiones solo la habilidad y/o experiencia de unos y otros hacen que la balanza se incline hacia uno u otro lado.

Y es que desgraciadamente determinados procedimientos, para que estén bien hechos requieren de un tiempo. Y en eso no hay que engañarse, en muchas ocasiones todo es cuestión de dinero, puesto que el tiempo se traduce en eso. En ocasiones una organización evaluará si le sale más rentable realizar el pericial u olvidarse del tema, no sea que les salga más caro todo el proceso que lo que podría suponer tener que pagar un despido improcedente, aunque estén valorando un despido procedente incierto, donde la labor pericial sea crítica.

Hay que tener presente que los procesos que pueden derivar en un juicio deben ser realizados más pulcramente para que las conclusiones, partiendo de las evidencias, sean válidas, creíbles y quizás lo más importante “rotundas”. Aquellas actuaciones que no requieren llegar a juicio, pueden ser más flexibles, evidentemente con un acorte en tiempo importante para la recogida y tratamiento de las evidencias.

En muchas ocasiones se tiende a seguir procedimientos, que siendo más o menos reglados pueden resultar algo imprecisos. Por ejemplo en tareas de adquisición de evidencias un especialista podría llegar a operar haciendo uso de las normas marcadas en la RFC 3227 “guía para la recogida y almacenamiento de evidencias”. Sin embargo a día de hoy en España, en aquellos procesos que pueden desembocar en un juicio,

aplicarla escrupulosamente puede ser una verdadera temeridad. ¿Por qué? Fundamentalmente porque rompe el principio de “antes de tocar, prevalece el recoger”. Nunca debería alterarse el escenario, sino se quiere que aparezca manchado o lo que puede ser peor, con los dedos en él.

La RFC 3227 establece entre otras cosas que la recogida de información se establecerá en función de su volatilidad. Indica como recoger la información de la memoria, de las tablas de enrutamiento, de la cache, etc. Esto está muy bien, ¿pero cómo adquirir esa información, sin alterar el escenario?

En determinados países donde quizás estén más avanzados judicialmente en procedimientos forenses informáticos, puesto que tienen hasta leyes y regulaciones para ello, esta RFC pueda tener su validez. Sin embargo, en muchos países como en el caso de España, es muchísimo más importante el tener claro que “cuando yo llegué, esto ya estaba así”. No sea que la cuestión acabe en una recusación por haber querido malversar las pruebas para incriminar a alguien. Y es que aunque a los peritos se les estime la virtud de la independencia, cuando hay dinero por medio quizás se diluye esa esencia.

Claro está que si después de asegurarse bien, independientemente de cómo se desarrolle el caso, que este no acabará en un juicio, los procedimientos, herramientas y resultados no tendrán ni la exigencia ni la pulcritud que demandaría de la otra forma.

A lo largo de este libro se irán revelando esas claves. La importancia de anticipar las cosas, de saber lo que se trae uno entre manos, de conocer las herramientas y sobre todo de la dichosa experiencia.



Capítulo 2 – La importancia de las evidencias

Uno de los aspectos fundamentales a la hora de afrontar un forense, constituye la necesidad de contar con unas evidencias válidas. Todas las evidencias son inicialmente válidas pero una mala práctica puede llegar a invalidarlas. Hay que tener presente en todo el procedimiento que el perito debe gozar y contar con el principio de independencia.

Aunque la información que proporciona el afectado es vital, hay que tener en cuenta que a veces condiciona a ver las cosas de una manera y puede perderse esa visión esencial para hacer bien las cosas. Como técnicos el primer impulso ante un comentario suele ser querer ver lo que pasa, pero eso implica tocar el equipo sin haber llevado a cabo las acciones oportunas.

Supóngase un equipo del cual se sospecha que se haya realizado una acción perniciosa, este se encuentra encendido y con evidencias interesantes que pudiera tener almacenadas. Desconocemos si las tiene o no, y quizás el primer impulso es verificarlo, pero esto constituiría el primer error. La opción más lógica es asumir que las evidencias están ahí (aunque pudiera ser posible que no) y tratarlo como un sistema con información importante y sensible para el caso. Tocar de antemano puede implicar que en caso de juicio alguien podría alegar que pudiéramos haber manipulado las evidencias (no hay que perder de vista que este argumento lo podemos usar también en un *contrapericial*) para favorecer o incriminar a alguien.

Y si no puede tocarse el equipo ¿qué ha de hacerse? A día de hoy no hay nada reglado en este sentido, pero existen una serie de normas no escritas que son las aplicadas habitualmente. Si el equipo está encendido es buena opción sacar una fotografía de la pantalla y apagarlo. Puesto que pudiera haber información importante relativa a ficheros temporales o en el caso de sistemas Windows fichero de paginación, podría optarse por apagar el equipo por vía la rápida: cortando el suministro de energía. La pérdida más importante la constituye la información de conectividad de red y la memoria RAM, pero hay que tener presente las circunstancias del caso y el tipo de escenario al que hay que enfrentarse. Si esa información resulta vital, sería

imprescindible contar con testigos que pudieran refrendar las acciones realizadas y que pudieran atestiguar que no se ha realizado ninguna acción enfocada a manipular datos, solo a extraerlos (no obstante siempre habrá que tener prevista una respuesta en el juicio para una defensa de las acciones realizadas).

El tema de los testigos es algo que no solo en caso de llegar a tocar el equipo se debe realizar sino en todo un proceso que pueda ser comprometido. Muchas organizaciones cuentan entre sus procedimientos (formulados a través del uso de medios o bien de los protocolos de seguridad internos), que mecanismos hay que emplear en determinadas circunstancias, en muchas ocasiones herederos de acciones tales como el registro de una taquilla. Para estos casos suele requerirse que todo el proceso sea llevado a cabo con la presencia de una persona del comité y el afectado, o con dos personas de la organización totalmente independientes a las circunstancias del caso. Estos procedimientos ofrecen la seguridad (sobre todo de cara al juicio) de que habiéndose realizado una serie de acciones, unos testigos podrán refrendar los hechos. Estas acciones se tratan de forma muy análoga estos procesos al hecho de la apertura de una taquilla y que en cierta medida quedan regulados por el Estatuto de los Trabajadores.

Aunque con una orientación diferente sirva como ejemplo una sentencia de noviembre del 2000 de la Sala de lo Social en Málaga del Tribunal Superior de Justicia de Andalucía, en la que se juzgaba la denuncia efectuada por un trabajador contra el empresario que le intervino y copió todos sus correos y ficheros personales, aún en presencia del comité de empresa. La sentencia se inclina por el criterio empresarial, (a pesar de que la sentencia en cuestión da la razón al trabajador, pero solo por el hecho de que no se justificó el registro como obliga el artículo 18). La resolución afirma, aún implícitamente, que el artículo 18 del Estatuto de los Trabajadores autoriza el registro en la terminal de ordenador que utiliza el trabajador. A todos los efectos un equipo se asimila a la taquilla, basándose en que el ordenador es un instrumento de trabajo propiedad de la empresa. Por lo tanto no deberá ser utilizado con otros fines diferentes que la realización de la propia actividad laboral.

Sin embargo nunca deberá obviarse el hecho de que en un juicio la palabra y la interpretación última de todas las circunstancias la tiene siempre el juez y ahí la cosa no siempre está tan clara. El Juez interpreta las leyes y las aplica según su entender. Por lo tanto cualquiera de los procesos efectuados y las acciones llevadas a cabo son validadas y refrendadas exclusivamente por su señoría.

Teniendo esto presente en todo análisis llegará la hora de adquirir las evidencias. En este sentido se plantea siempre la misma incógnita: ¿cuál es el procedimiento adecuado? La respuesta resulta compleja, y es que realmente no existe un único procedimiento, así como tampoco existen unas herramientas “validadas” y que sirvan específicamente a efectos judiciales. Nuevamente hay que tener presente que en España (así como en muchos países de la Unión Europea) no hay una legislación para el análisis forense. Por lo tanto no puede expresarse que tal proceso es el bueno y cuales de las herramientas con correctas en su empleo y cuáles no. Básicamente hay que plantearse los siguientes elementos

- ¿Cuál es el escenario ante el que hay que enfrentarse?
- ¿Qué quiere analizarse: un fichero, un directorio, un disco o todo un sistema?
¿De cuánto tiempo se dispone para hacer la adquisición de las evidencias?
- ¿Dónde se almacenarán las evidencias?
- ¿Cuántas copias deben realizarse?

Normalmente los escenarios a los que se enfrentará el analista forense, requieren posiblemente de la copia de varios medios (bien por la configuración del equipo o por saber de la existencia de ficheros pero no conocer dónde se ubican y encontrarse en el escenario múltiple medio). Con lo cual, habitualmente debe tener presente esa circunstancia. Este hecho no puede tomarse a la ligera (copiar todo lo existente) puesto que el tiempo invertido será alto y el coste en recursos también. Este proceso de copiado de un disco (o bien de determinados ficheros) no puede hacerse de cualquier manera, sino que por el contrario hay que garantizar:

- Que las copias a realizar deben ser idénticas y sin ninguna alteración del origen ni del destino.
- Que se copie también el supuesto espacio libre. Muchas veces puede aparecer allí información interesante, sobre todo en circunstancia de uso de herramientas de tipo antiforense.
- Que se aplique una función hash sobre la información copiada.

Esto último es vital porque garantiza que las conclusiones a las que se lleguen de las evidencias adquiridas, parten de un disco o ficheros idéntico al original y por lo tanto no ha habido una manipulación del mismo tras la copia binaria. Con respecto a esto, el planteamiento inicial siempre debe consistir en determinar cuántas copias deberían realizarse. Es recomendable que se realicen un mínimo de dos, además de mantener el

original. Una de las copias estará destinada al analista forense, la otra copia debería ser para la empresa o el afectado y el original que deberá salvaguardarse. Para esta última existen varias posibilidades. Podrá presentarse junto a la denuncia, quedar en manos de un notario que de fe del hecho o bien almacenado por la organización con las garantías de seguridad debidas teniendo en cuenta su importancia de cara al posterior juicio.

El hash garantizará que el disco no ha sido manipulado y por lo tanto las pruebas reproducibles si llegara el caso la realización de un contrapericial. Aunque existen multitud de algoritmos, se recomienda el uso de al menos SHA-1 (Secure Hash Algorithm) para ello.

Las herramientas enfocadas al procedimiento de copiado utilizan habitualmente la función *dd* para el copiado. Esto se realiza bien por la clonación del disco físico o las unidades lógica o bien generando un único fichero de imagen que pueda ser tratado directamente por las herramientas forenses.

Existe para ello elementos hardware que permiten realizar estos procesos de forma cómoda, precisa y con altas garantías. Aunque no es la solución más económica si es la que ofrece mayor profesionalidad y seguridad para un analista forense. No obstante hay que tener en cuenta la diversidad de tipos de discos existentes en el mercado. Su evolución llega a suponer que un determinado hardware adquirido podría no ser válido en un proceso de copia al no disponer de los accesorios adecuado para recuperar un tipo de disco específico. Existen conversores no obstante que facilitarán la labor pero no garantías de que la compatibilidad pueda mantenerse a lo largo del tiempo.

A modo de ejemplo se ponen a continuación algunos enlaces orientativos sobre dispositivos existentes en el mercado que permiten las operaciones de adquisición de evidencias.

- Logicube (<http://www.logicube.com/>)
- ICS (<http://www.ics-iq.com/Computer-Forensic-Hand-Held-Units-s/33.htm>)
- Data Device International (<http://www.datadev.com/hard-drive-forensics-dod-approved-data-security-erase.html>)



Capítulo 3 – El procedimiento de copiado de discos

En el anterior capítulo se hablaba de la importancia de establecer un buen procedimiento para la adquisición de evidencias. Aunque lo idóneo sería contar con un equipamiento hardware, existe la posibilidad de utilizar soluciones tipo software para la realización del mismo. Prácticamente la mayor parte de ellas, se basan en el empleo de la función `dd` existente en entornos Unix y Linux, para la copia de un número especificado de bytes o de bloques. Se citan y muestran en este libro las que proporcionan las suites forenses Helix y Caine.

La suite Helix de e-fense (<http://www.e-fense.com/>) nació con una inspiración diferente a la que puede encontrarse a día hoy, sobre todo en lo que se refiere fundamentalmente al aspecto económico. Era una solución de libre distribución y ofrecía funcionalidades para realizar análisis Live Forensics sobre sistemas Microsoft y Post Mortem a través de un arranque sobre distribución Linux. Totalmente gratuito tanto en el análisis Live Forensics como Post Mortem proporcionaba mecanismos para la realización de copias de evidencias digitales que podrían ser utilizadas en los casos forenses.

Aunque a día de hoy las distribuciones de este producto presentan un coste, todavía puede encontrarse en Internet versiones de la misma que como la 1.9 o la 2008 R1 pueden ser utilizadas para la adquisición de evidencias. Basada en Knoppix, puede utilizarse su funcionalidad de Live-CD para la adquisición de discos con múltiples funcionalidades.

Existen algunas diferencias entre las diferentes versiones del producto, tanto en su aspecto físico como en las aplicaciones que facilitaban para los procedimientos forenses. La versión 1.9 frente a la versión posterior 2008 R1, aportaba una funcionalidad adicional en la adquisición de evidencias, a través de la aplicación Air.

A continuación se muestran dos imágenes con el aspecto visual de cada una de las versiones.



Img. 1.- Helix versión 1.9

Puede verse las diferencias existentes tanto a nivel visual como las herramientas que aportan cada una de ellas.



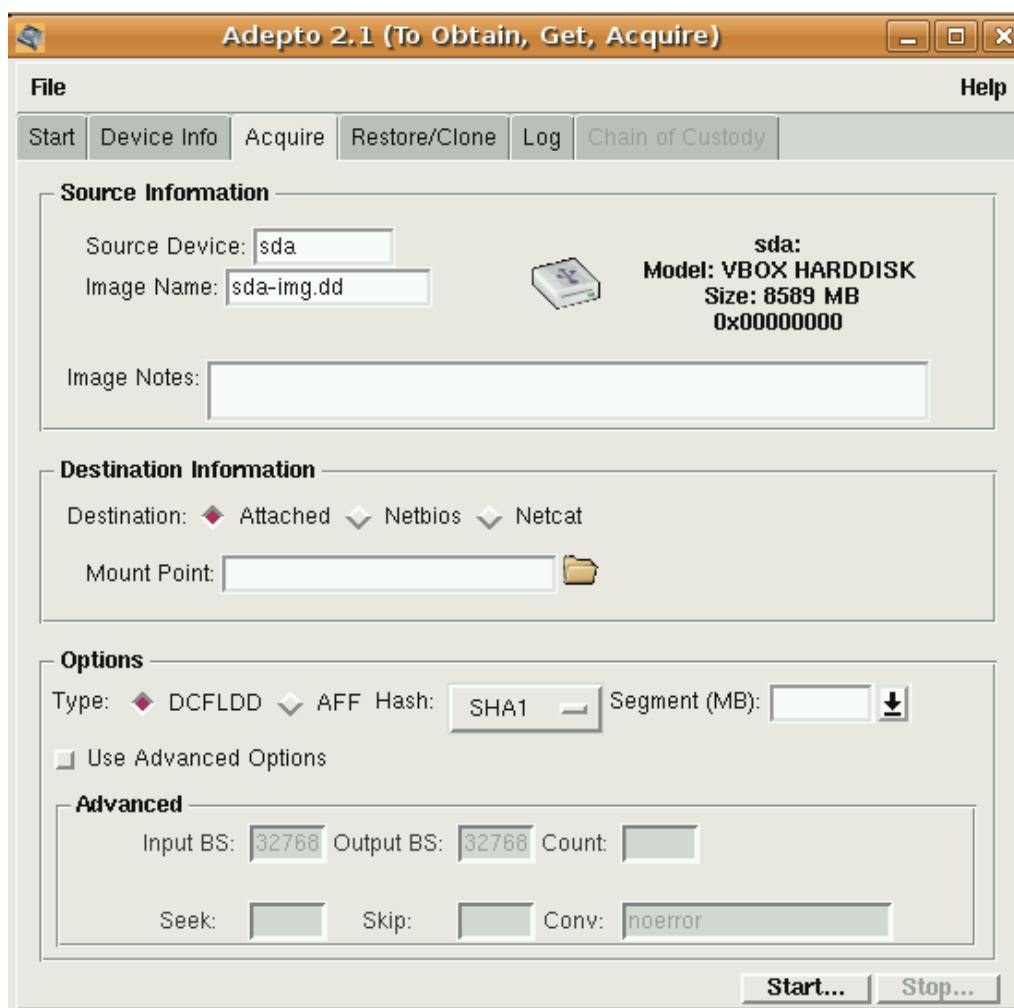
Img. 2.- Helix versión 2008 R1

Aunque también hay que contar con que ambas versiones traigan una de las aplicaciones más utilizadas para la realización de las actividades de copia: Adepto.

Esta aplicación permite dos formas diferentes de emplear la funcionalidad *dd* para la adquisición de evidencias:

- Adquisición en un único fichero *dd* volcando todo el contenido del disco seleccionado.
- Realizando una clonación del disco, generando una copia idéntica del disco seleccionado.

La siguiente imagen muestra la operación de la adquisición de disco con la aplicación Adepto. Dentro de las opciones significativas que puede observarse, se encuentra la ruta de destino donde volcar la información. Para ello podrá hacerse uso de una ruta local, una conexión de red tipo Netbios o bien realizando uso de la salida de datos a través de Netcat sobre la dirección IP y puerto especificado.



Img. 3.- Adquisición de disco.

También resulta sumamente importante la decisión de uso del Hash. Esta funcionalidad permitirá verificar que origen y destino son idénticos, dando así validez a la prueba. Se garantiza que las copias son idénticas y válidas. Así en la presentación de conclusiones partiendo de las evidencias adquiridas, podrán reproducirse si se dieran las circunstancias. Se recomienda modificar el tipo predeterminado de MD5 al menos a SHA1, por lógicas razones de seguridad. Algunas de las motivaciones para ello pueden verse el siguiente enlace del blog “Legalidad Informática”:

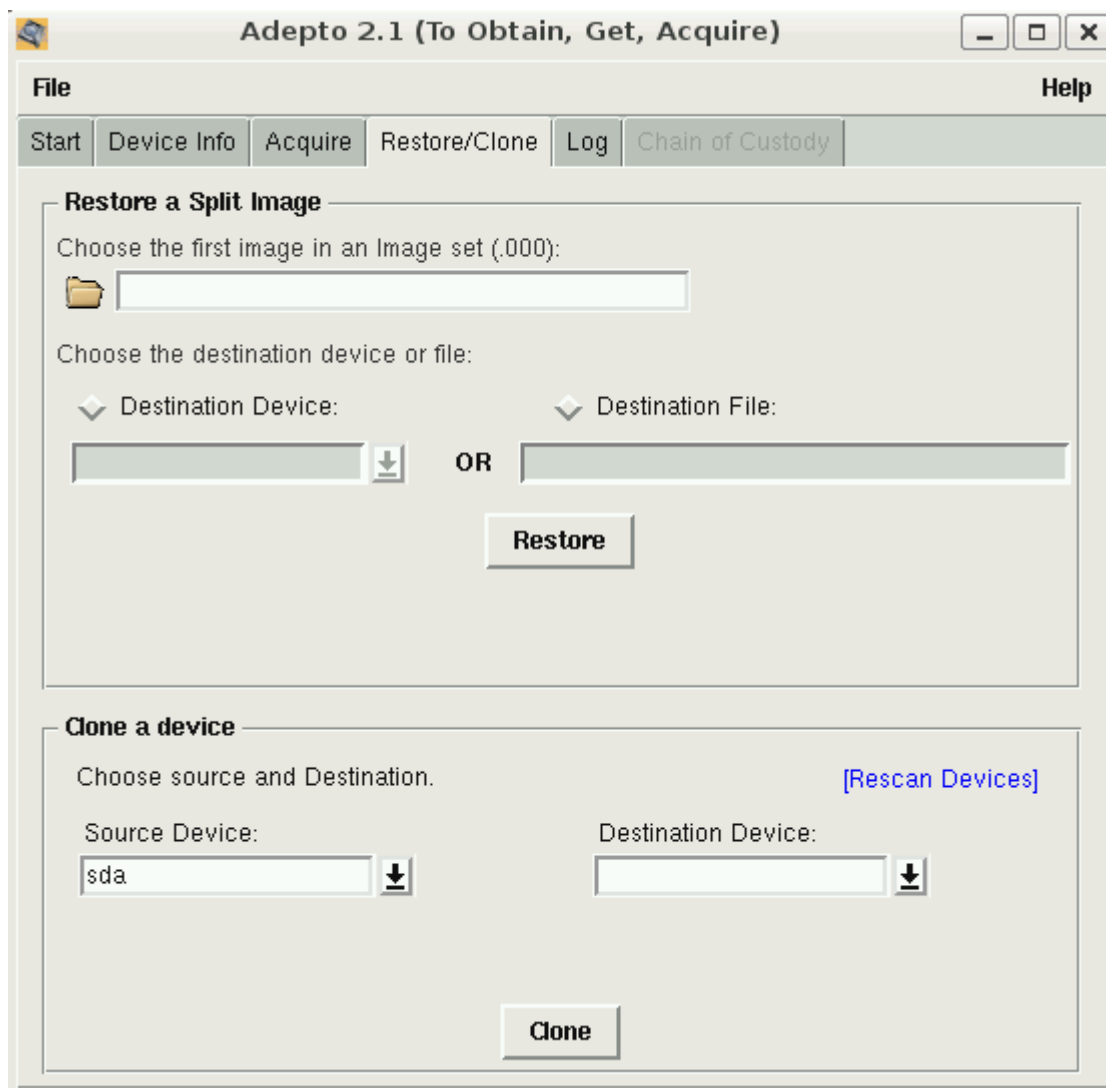
<http://legalidadinformatica.blogspot.com.es/2012/04/md5-prohibido-su-uso-en-la.html>

De esta forma se garantizará que el analista forense no ha hecho manipulación de las pruebas desde el momento en que se realiza la adquisición de las mismas. Claro está el analista forense bajo ninguna circunstancia podrá apelar bajo esta condición que previa a su intervención no ha habido manipulación de las evidencias por parte de los afectados. Solo el análisis podrá dar respuesta a esta incertidumbre propia de toda investigación.

Los tipos de metodologías que pueden utilizarse *DCFLDD* y *AFF* representan características avanzadas para el uso de la aplicación *dd* en las prácticas de adquisición de evidencias forenses. El primero de ellos fue desarrollado por el departamento de los EEUU, *Defense Computer Forensics Lab*. El segundo de los formatos: *Advance Forensics Format*, fue diseñado como un mecanismo más avanzado que el formato *dd* estándar siendo más flexible y permitiendo el almacenamiento de extensivo de metadatos requiriendo menos espacio de disco que otros formatos propietarios existentes en el mercado (como el de *EnCase*). Por el tipo de implementación es favorable decantarse por el primero de ellos.

El segundo de los métodos de adquisición que proporciona *Adepto* se basa en la posibilidad de clonar un disco completamente, manteniendo tanto la información como la estructura física, de tal forma que será un espejo del disco origen. En esta circunstancia también se realizará una función hash del mismo, mostrado a través del sistema Log que proporciona la herramienta.

También a través de este menú de restauración/clonado, se ofrece la alternativa de restaurar un fichero tipo *dd* sobre un disco o sobre otro fichero imagen. De tal forma que se verifique nuevamente la idoneidad del procedimiento mediante función hash del origen y del destino.



Img. 4.- Clonación de un disco

En ambas circunstancias es importante tener en cuenta una serie de detalles:

- El tamaño de disco es relativamente importante. Los discos origen y destino no deben ser ni de las mismas características, ni tener idénticos en tamaño, pero sí el segundo en espacio ser superior al primero.
- Tampoco deben ser idénticos en formato. Un disco tipo IDE puede volcarse sobre un SATA o este sobre un USB. Venden para ello unos componentes hardware que permiten la conversión y conexión de diferentes tipos de unidades de disco a USB. Aunque es un método bastante más lento e inseguro que el uso de una clonadora convencional, resulta un proceso bastante más económico. Permitiendo tratar todos los discos como de tipo externos y controlar así la identificación de unidades.

- Sobre todo en el proceso de clonación es absolutamente imprescindible cerciorarse de cuál es el disco origen y cual el destino. No sea que al final se produzca una confusión y sobre el disco de las evidencias se acaben volcando exclusivamente los ceros que existirían en la supuesta unidad que iba a ser utilizada como destino.
- También es indispensable que el disco destino no tenga ningún dato previo. Esto evitaría que en el espacio no copiado se encontraran por ejemplo datos de otros casos, con el consiguiente problema de mezclar evidencias. Sería peculiar ver como el analista intenta desentramar relaciones existentes entre diferentes casos motivados por el cruce de las evidencias. Se tratará a posteriori que proceso puede ser llevado a cabo para que un disco quede limpio de trazas previas.

Utilizar un método u otro, dependerá fundamentalmente del tipo de escenario al que se enfrente el analista, el tipo de pruebas a efectuar y las herramientas con las que se cuente. Por ejemplo en un análisis de malware donde hay un componente muy importante de análisis activo sería necesario realizar un clonado de disco. Sin embargo si se va a realizar un rastreo en busca de una determinada cadena de caracteres o un documento concreto el método adecuado podría ser la generación de un fichero único de imagen.

El tiempo de adquisición de una evidencia dependerá de varios factores: espacio a copiar o clonar, velocidad de los discos, soporte, tipo de hash a realizar, si se va a realizar una verificación de copias, etc. Para el que nunca haya realizado una adquisición de este tipo deberá tener en cuenta que este proceso es bastante lento. Puede llegar a tardar unas cuantas horas en concluirse completamente todo el proceso sobre un disco duro convencional, si no hay errores.

Un detalle importante que proporciona la herramienta Adepto es que finalizado el proceso, aportará un fichero de suma importancia en el procedimiento forense: el fichero de cadena de custodia. Este será objeto de tratamiento posterior pero resulta vital como parte de la información que deberá acompañar cualquier evidencia digital que sea presentado en cualquier caso que se encuentre judicializado.

Otra suite interesante para la adquisición de evidencias y análisis forenses es CAINE (<http://www.caine-live.net/>). Computer Aided INvestigative Environment es un conjunto de herramientas de libre distribución, agrupadas en una suite GNU/Linux Live basada en UBUNTU. Es de origen italiano y se encuentra dirigida como Product Manager por Nanni Bassetti.

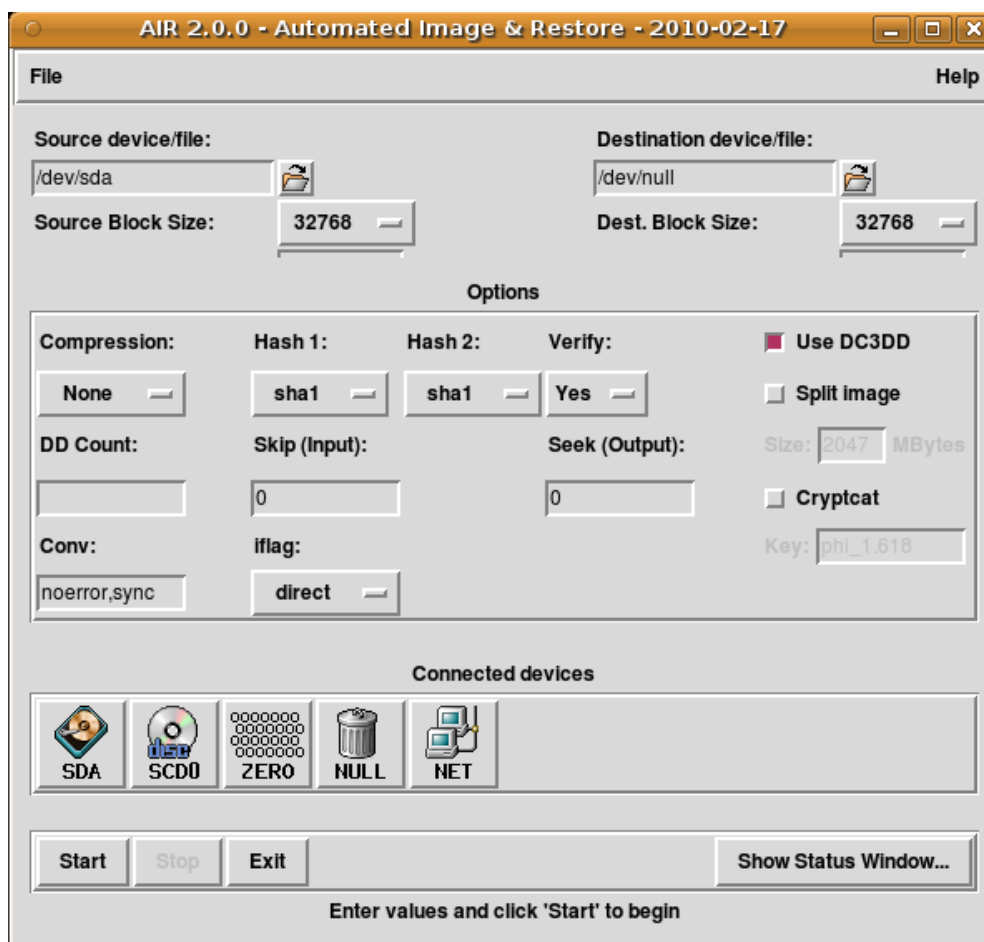
CAINE ofrece un conjunto de herramientas que al igual que en el caso de HELIX opera en modalidad tipo Live-CD. Aporta algunas aplicaciones para interactuar con discos y poder realizar también la adquisición de los mismos.



Img. 5.- Utilidades forense de CAINE V 2.5.1

Para la adquisición de evidencias la aplicación más destacada con la que cuenta es AIR (Automated Imaged and Restore). Con ella se puede adquirir discos y realizar algunas operaciones interesantes que deben ser llevados a cabo en los procedimientos forenses, como es la limpieza de los discos sobre los que realizar el volcado de información.

En esencia aporta funcionalidades muy similares a la aplicación Adepto que ya fue comentada previamente tal y como se puede apreciar en la imagen siguiente, aunque presente para ello utiliza una interface diferente y también sus particularidades.

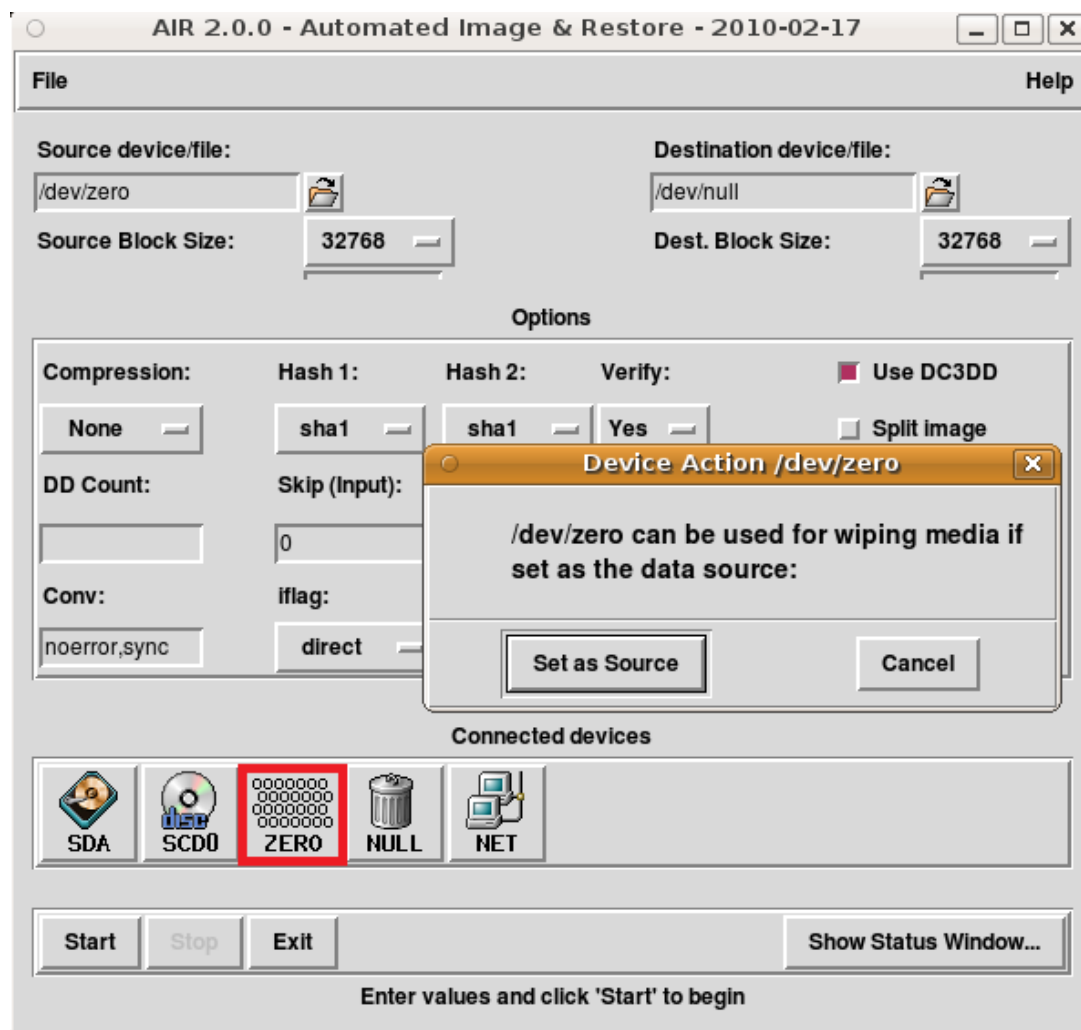


Img. 6.- Aplicación AIR.

Los procesos que se llevan a cabo como en todas las herramientas de este tipo, son similares debiendo establecerse los orígenes y destinos, bien sean de ficheros o de dispositivos completos. Se procederá como en las circunstancias anteriores a la adquisición de un fichero tipo dd o bien a la realización de un clonado del disco. En la realización de estos procesos debe tenerse también en cuenta la comprobación del hash.

Al contrario que en el caso de Adepto la aplicación AIR no genera el fichero de cadena de custodia y por lo tanto este deberá generarse de forma manual tal y como se mostrará en el siguiente capítulo.

Esta herramienta cuenta con una función muy interesante para realizar una limpieza del disco: Disk Wiping. A través de este proceso se vuelcan sobre un disco que será seleccionado como destino, datos de tipo 0 que serán identificados como origen de los datos.



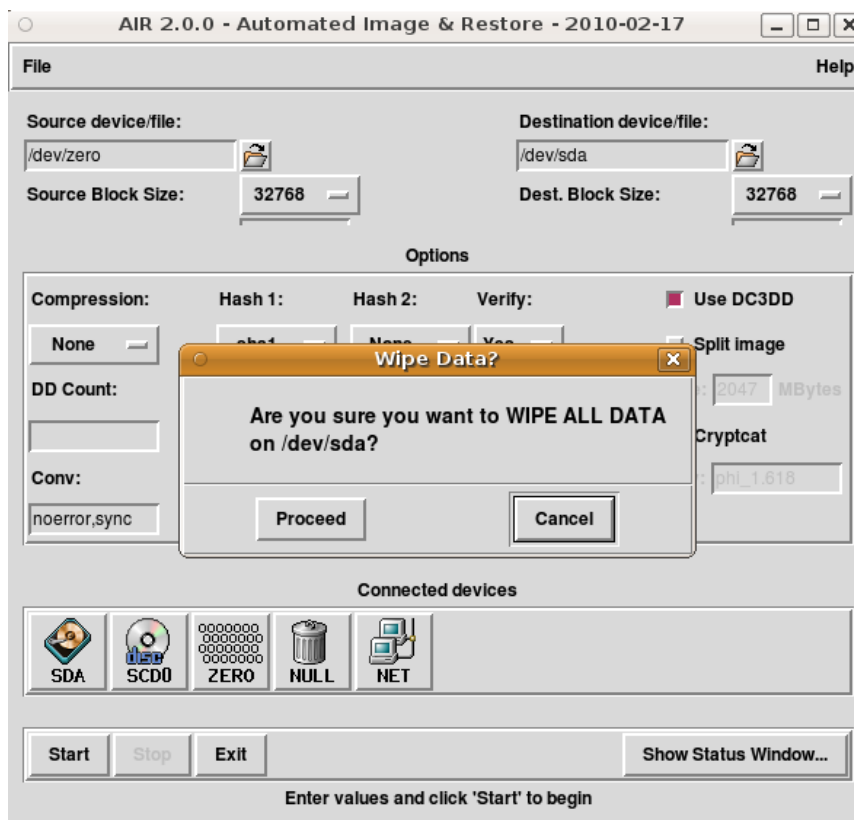
Img. 7.- Funcionalidad para realizar Disk Wiping.

Tal y como se comentó en páginas previas, esto constituye un procedimiento indispensable para garantizar una higiene en el tratamiento y posterior análisis del caso. De esta forma existe la certeza de que un disco contendrá información exclusiva de un caso. Este hecho es importante sobre todo por el detalle del supuesto espacio de disco no utilizado.

En ocasiones muchos analistas tienden a plantearse el análisis exclusivo del análisis particionado. Así cuando se elimina de forma informal una partición del disco se “elimina” solo ese espacio, sin embargo la parte no particionado puede contener perfectamente información válida. Al clonar un disco a nivel físico, se clona también el espacio no particionado. El proceso de recuperación de ficheros eliminados que se realiza en determinadas circunstancias del proceso forense puede recuperar datos de la parte no particionada y por lo tanto recuperar ficheros tanto del propio caso que se estuviera investigando como el de otros casos. Es importante que siempre el disco

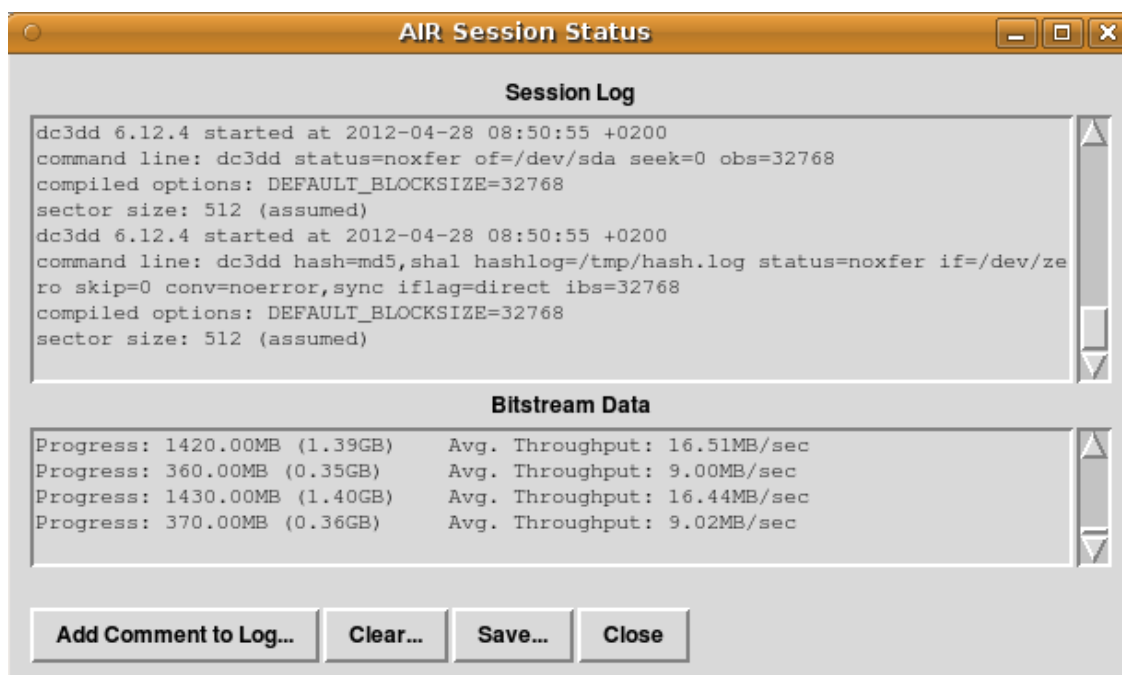
sobre el que se va a volcar información tenga condiciones lógicas similares a las de fábrica.

Como se aprecia en la siguiente imagen se ha seleccionado como origen el conjunto de bits ZERO y como destino la unidad SDA. El proceso será iniciado tras aceptar el mensaje de advertencia que saldrá por pantalla.



Img. 8.- Inicio del proceso de eliminación de datos

Todo el proceso puede ser revisado a través del módulo de estado que proporciona AIR. La siguiente imagen muestra el estado del proceso de volcado de bits 0 sobre el disco SDA. Al igual que en la adquisición de evidencias, estos procesos son lentos y requieren de un tiempo para que sean completados. Por lo tanto debería tenerse en cuenta este hecho antes de visitar al cliente para un proceso de copia. Es preferible llevar los deberes hecho y contar para ello con discos limpios antes de iniciar el proceso, que resultará ya de por sí tedioso y para el cual se requerirá de la presencia de varias personas.

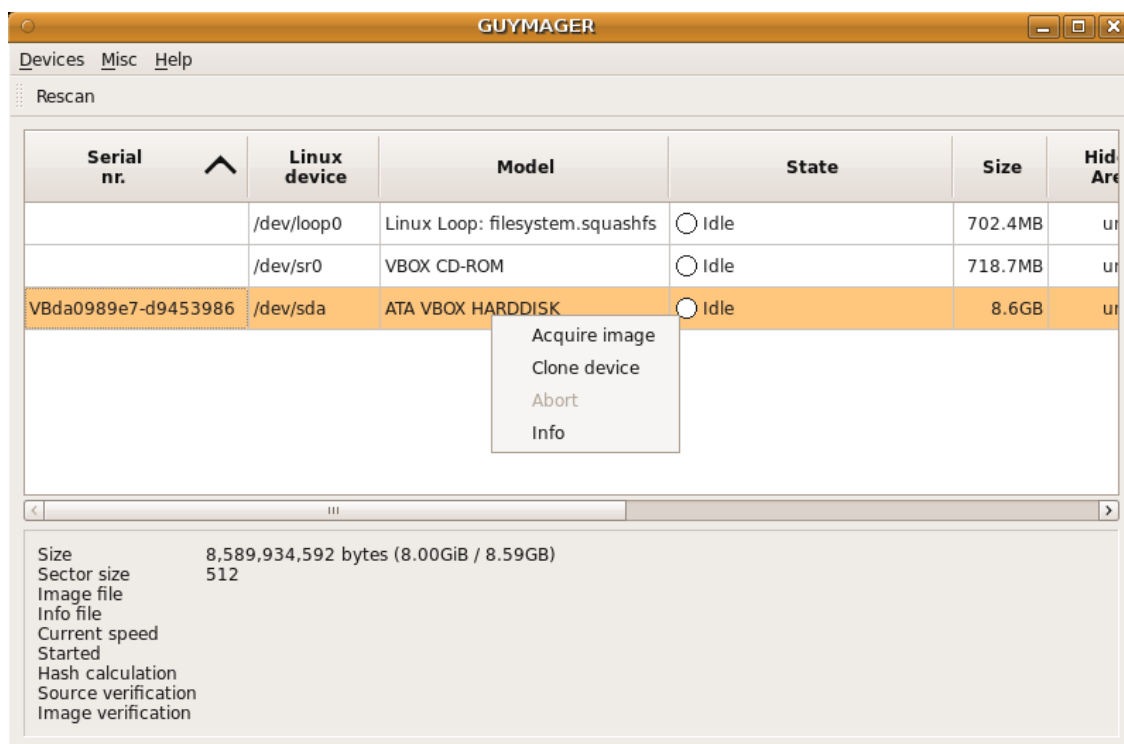


Img. 9.- Estado del proceso

El proceso de Disk Wiping mostrado, no debe confundirse con el de eliminación segura del que se habla en otras ocasiones. Este último trata de garantizar la no recuperación de la información que existiera en un disco. Para ello se requiere de la realización de varias pasadas de bits de 1 y 0 con objeto de garantizar que una información no es recuperable ni haciendo uso de elementos hardware altamente especializados. En el caso del proceso de Disk Wiping solo es necesario realizar un pasada de unos.

Aunque el proceso de eliminación segura puede realizarse con Air, resulta más aconsejable hacer uso de software que ha sido específicamente diseñado con ese propósito. Sirva de ejemplo el conjunto de aplicaciones DBAN (<http://www.dban.org/>) utilizado en muchos procedimientos de agencias a nivel mundial.

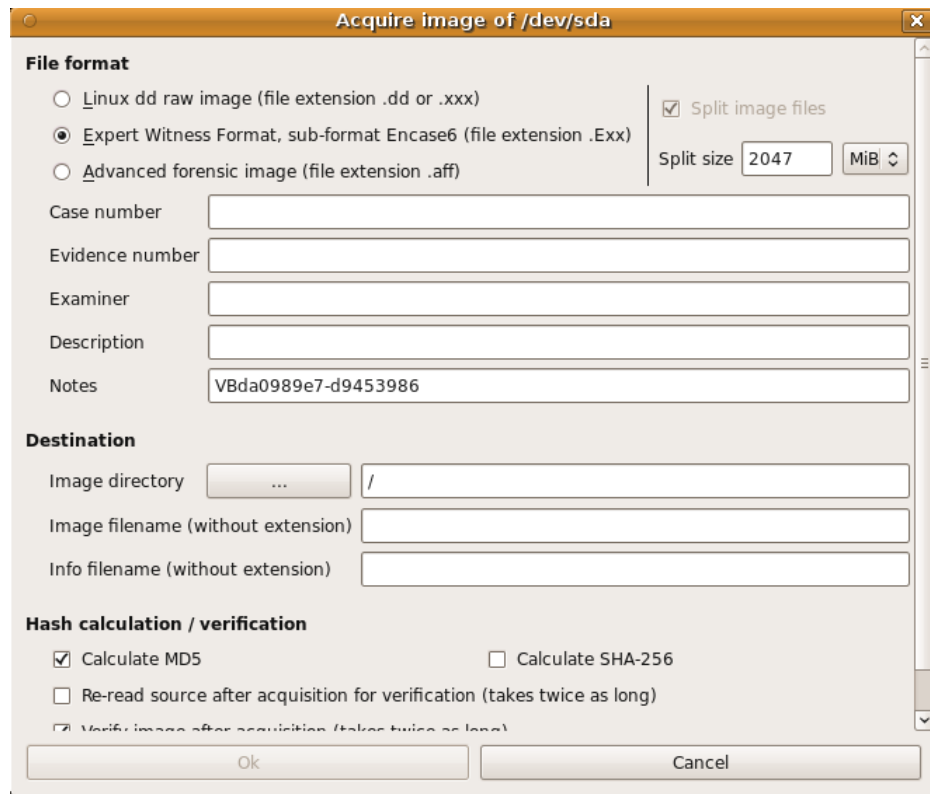
Una aplicación más simple, en lo que corresponde inicialmente a su aspecto, que proporciona CAINE para el tratamiento de disco es Guymager. Esta herramienta permite también la funcionalidad de adquirir y clonar discos mediante una interface bastante sencilla de manejar.



Img. 10.- Guymager

No hay que obviar sin embargo que la sencillez no está reñida con potencia, puesto que cuando se selecciona la opción requerida (adquirir o clonar), permite introducir un gran número de parámetros y seleccionar opciones para realizar el proceso. Esto amplía las capacidades de la aplicación y la hacen mucho más versátil que las anteriormente citadas.

La imagen siguiente muestra las opciones para la adquisición del fichero, donde se permite por ejemplo realizar una adquisición en un único fichero, no solo mediante la función *dd* tal y como se ha mostrado hasta ahora. También permite generar un fichero en el formato propio que utiliza el software de análisis forense EnCase. Tal y como se puede apreciar en la siguiente imagen, se podrá proporcionar toda la información importante que debe acompañar a una evidencia permitiendo así identificar entre otros los datos del caso y del analista encargado de realizar la operación.



Img. 11.- Adquisición de discos.

Se ha mostrado en este capítulo la importancia de adquirir correctamente evidencias y algunas de las metodologías para llevarlo a efecto. Evidentemente hay multitud de formas de realizarlo y cada cual puede ser buena a su forma, pero es importante seguir siempre un buen procedimiento, no perdiendo nunca la perspectiva de garantizar la higiene de las pruebas.

A menudo en este proceso las prisas no son buenas aliadas puesto que provocan fallos que a posteriori pueden costar caro. A pesar de la presión del momento, de la circunstancias y de las propias personas que pueden estar involucradas en el hecho, el analista debe pensar varias veces las cosas y ser consecuente con la responsabilidad que se espera de él. En este momento es la persona clave puesto que tiene toda la capacidad y conocimiento para hacer las cosas como deben hacerse. Si ve abrumado por las circunstancias o por las consideraciones de personas que son espectadores del proceso y que en muchas ocasiones le piden premura, a buen seguro no estará operando como se espera de un buen analista.



Capítulo 4 – La cadena de custodia

Tal y como se ha comentado en los anteriores capítulos, uno de los fundamentos principales para llegar en una buena posición a un proceso judicial, consiste en garantizar la consistencia de las evidencias. Desde un punto de vista puramente formal esto se consigue mediante un procedimiento válido y la garantía de la no alteración de las pruebas.

Oficialmente en España no se encuentra estipulado el procedimiento para garantizar la custodia de las pruebas, aunque sí en otros países de ámbito europeo. Se estima que a efectos reales España contará a finales de 2012 o principios del 2013 con una norma que regulará y garantizará la custodia de las pruebas policiales. La elaboración de dicha normativa se ha encargado al Instituto Universitario de Investigación en Ciencias Policiales. Actualmente existen protocolos internos pero no unificados. Este hecho no obstante debe tenerse en consideración para las diferentes unidades de cuerpos de seguridad del esto. Sin embargo aunque puede ser tomado como referencia la normativa no afectará a análisis y peritajes ajenos a las mismas.

Aunque no exista la oficialización del procedimiento, está ampliamente aceptada la figura de la cadena de custodia como norma de facto para dar garantías al proceso de mantenimiento de las evidencias. La cadena de custodia ofrece en cualquier proceso, sea o no informático, que las pruebas que se aportan y las conclusiones a las que se ha llegado partiendo de las evidencias son consistentes y válidas, no habiendo sido alteradas con ningún fin desde el momento de su adquisición.

De una u otra forma la transmisión de las evidencias se da entre cada perito o persona desde el momento en que se recogen. Sobre estas personas recae el compromiso de mantenimiento de las pruebas. Por lo tanto la cadena de custodia recoge precisamente los siguientes elementos:

- ¿Quién?
- ¿Cuándo?
- ¿Por qué?

A través de este hecho podrá identificarse quién ha estado en posesión de las evidencias. Para ello hay que tener presente que cualquiera que apareciera en una cadena de custodia podría llegar a ser testigos en el juicio si quedaran en entredicho las evidencias, motivadas fundamentalmente por defectos que arrojaran duda sobre los procedimientos efectuados. Queda recogido en la Ley 1/2000 de Enjuiciamiento Civil el objeto y finalidad del dictamen de peritos a través de su artículo 335:

“Objeto y finalidad del dictamen de peritos. Juramento o promesa de actuar con objetividad.

- 1. Cuando sean necesarios conocimientos científicos artísticos, técnicos o prácticos para valorar hechos o circunstancias relevantes en el asunto o adquirir certeza sobre ellos, las partes podrán aportar al proceso el dictamen de peritos que posean los conocimientos correspondientes o solicitar, en los casos previstos en esta Ley, que se emita dictamen por perito designado en el Tribunal.*
- 2. Al emitir el dictamen todo perito deberá manifestar, bajo juramento o promesa de decir la verdad, que ha actuado y, en su caso, actuará con la mayor objetividad posible, tomando en consideración tanto lo que pueda favorecer como lo que sea susceptible de causar perjuicio a cualquiera de las partes, y que conoce las sanciones penales en las que podrá incurrir si incumpliere su deber como perito.”*

La custodia de las pruebas, se convierte por lo tanto en una máxima permitiendo al perito garantizar la independencia y objetividad en la elaboración de sus conclusiones, sin haber realizado manipulación de las evidencias para favorecer a alguna de las partes. Desde un punto de vista formal sería necesario incorporar un fichero de cadena de custodia por cada evidencia existente. En el caso de los procedimientos que se llevan a cabo en Sidertia Solutions se hacen tanto para cada elemento adquirido, como de las posibles copias derivadas de los mismos.

Así si un analista recibe un disco adquirido y procede a realizar otra copia para realizar una serie de test sobre los datos y no alterar el origen, debe proceder a formalizar la realización del fichero de cadena de custodia. De esta forma podrá seguirse la pista también a esta copia, puesto que nunca hay que obviar el hecho de que contiene la misma información que será tratada como evidencia en el juicio.

Estrictamente no existe un fichero formal que recoja la información necesaria. Pueden encontrarse en Internet diferentes formularios que podrían ser válidos. En ocasiones

puede ser que la propia herramienta para la adquisición de evidencias utilizada proporcione uno, pero si no bien puede generarse uno de forma manual. Lo importante es contar con alguno e incorporarlo como parte del proceso.


A continuación se muestra el que genera la herramienta Adepto que fue objeto de análisis en capítulos anteriores.

The screenshot displays the 'Adepto 2.0 (To Obtain, Get, Acquire)' application window. The 'Chain of Custody' tab is active, showing an 'EVIDENCE CHAIN OF CUSTODY FORM - FOR FORENSIC IMAGES'. The form includes fields for 'Case Number' (SDT00001), 'Page' (of:), 'HARD DRIVE/COMPUTER DETAILS' (Item#, Description, Manufacturer, Model: Virtual HD, Serial), 'IMAGE DETAILS' (Date/Time: 05/05/12, Created By: Juan Luis Rambla, Method: dcfidd, Image: hda-img.dd, Storage Drive, Hash, Segments: 1), and a 'Create PDF...' button. A 'Progress' bar and a 'Quit' button are at the bottom. A status bar at the very bottom states 'These items will be printed on the Custody Form'.

Img. 12.- Funcionalidad de cadena de custodia

Haciendo uso de la funcionalidad que aporta el módulo de cadena de custodia en Adepto, se puede generar un fichero PDF que contendrá la información correspondiente al procedimiento realizado y permitirá acompañar a la prueba desde el inicio.

Tal y como se ve en la siguiente imagen, tras la realización de una adquisición de disco, se inicia la custodia con la generación del fichero correspondiente donde se incorporan los datos que dan validez al procedimiento y que han sido proporcionados al iniciar la herramienta. También se adjunta de forma automática datos como la identificación del disco y las opciones empleadas para la adquisición.



ADEPTO DIGITAL EVIDENCE CHAIN OF CUSTODY FORM

Case No: SDT00001 **Page:** of:

ELECTRONIC MEDIA/COMPUTER DETAILS

Item No:	Description:		
Manufacturer:	Model No:	Serial No:	
	Virtual HD		

IMAGE DETAILS

Date/Time:	Created By:	Method Used:	Image Name:	Segments:
05/05/12 16:41:33	Juan Luis Rambla	dcfldd	hda-img.dd	1
Storage Drive:	H.A.S.H:			

CHAIN OF CUSTODY

Tracking No:	Date/Time:	FROM:	TO:	Reason:
NA	Date:	Name/Org:	Name/Org:	Initiate Custody
	05/05/12	dcfldd	Juan Luis Rambla	
	Time:	Signature:	Signature:	
	16:41:33	See Hash		
	Date:	Name/Org:	Name/Org:	

Img. 13.- Fichero de cadena de custodia

Una vez generado el fichero de cadena de custodia este siempre debe acompañar a la propia evidencia. El paso de la misma de un perito a otro, conlleva el cambio de la custodia y por lo tanto también del traspaso del fichero. Esto se realiza formalmente anotando en el mismo los datos requeridos, incluyéndose en ello el motivo por el que se realiza el traspaso. Por ejemplo una persona es la encargada de realizar la adquisición, mientras que se pasa a una segunda, encargada del análisis de las evidencias recogidas.

El fichero de cadena de custodia no implica en esencia más que un formalismo, pero como tal es parte esencial del proceso. Podría ser que no nunca sea requerido en un juicio, pero nunca se sabe las argucias que puede intentar esgrimir el abogado de la otra parte en un juicio.



Capítulo 5 – Las buenas prácticas en el análisis.

Una vez que se cuenta con las evidencias y teniendo claro que el procedimiento seguido ha sido el correcto, es momento de ponerse manos a la obra. No es objeto de este manual enseñar como analizar evidencias, pero sí de ofrecer consejos para obtener buenos resultados a la hora de realizar el análisis. Es importante tener en cuenta que cada escenario presenta sus peculiaridades y evidentemente no pueden analizarse de la misma forma un caso donde hay que buscar en un equipo una conversación mantenida de Messenger, donde existan indicios de accesos ilícitos a cuentas de correo electrónico o bien tener que detectar la posible acción de aplicaciones maliciosas en un caso de espionaje industrial.

A pesar que la ciencia forense se encuentra rodeado por un halo de mística sensación, en la mayoría de las ocasiones, las tareas de análisis no resultan para nada edificantes. En muchos casos las tareas resultan tediosas y requieren de un gran esfuerzo personal para no caer en la desidia. Mucho de los casos forenses que acaban en juicio tienen una alta dosis de análisis de logs o búsqueda de cadenas de caracteres entre el sinfín de ficheros que puede contener un puesto de trabajo o un servidor.

Si bien es cierto que los casos de aplicaciones maliciosas, análisis de memoria, antiforense o esteganografía por poner algunos ejemplos resultan los más interesantes, son menos las circunstancias que conlleven el poder ir a juicio con ellos. Es más, la investigación en estos casos puede tener tantos derroteros que ir con una confianza plena en la aportación de las conclusiones al juicio se antoja mucho más difícil. Es mucho más fácil desde un punto de vista formal y procedimental analizar correos, logs o ficheros y por lo tanto que resulte la forma más habitual que un caso tenga un fin judicial. Al final todo se basa en interpretación y cuando los datos son más simples y planos, sin connotaciones que requieran planteamientos complejos la labor de un abogado y del perito resultará más fácil. Si no plantéese el tener que explicar a un juez que a través de la identificación de una dirección de memoria se tiene constancia de la manipulación de un proceso del sistema que interfiere en las pulsaciones del teclado. Y que dicha manipulación se produjo por la implantación de

una aplicación que aunque en el registro del sistema aparezca realizada por el usuario demandante, se estima que en realidad fue realizada por el demandado mediante una intrusión en el sistema a través de una vulnerabilidad en la máquina virtual de Java del equipo del demandante.

Es más, la coyuntura económica actual incide en la proliferación de casos relacionados con despidos que buscan una causa justificada para hacer procedente el mismo (en muchas ocasiones razonada, aunque en otras no tanto). También la competitividad hace que el espionaje industrial o el robo de propiedad intelectual sean otro de los orígenes de casos que se dan muy a menudo a día de hoy. Estos tipos de casos se resuelven habitualmente escarbando entre los registros de los sistemas o en ficheros de datos.

Hay que tener en cuenta que nadie que contrate un caso, por lo menos a día de hoy, aunque esto podría no ser así hace algunos años, lo haga sin tener un objetivo concreto. Analizar “por si tengo una aplicación maliciosa” no suele ser lo más habitual. Si tiene decidido el ir a juicio será porque existe una clara sospecha o tiene indicios razonables. Esto tiene que ser el punto inicial de partida de la investigación. Analizar porque sí, suele ser lo más complejo y muchas veces detrás hay más fantasmas que algo tangible y concreto. Si el resultado no satisface al cliente, fundamentalmente por ver cosas donde no las hay, cobrarlo será más complejo si cabe que realizar la propia investigación.

Al afrontar el análisis deberán tenerse en cuenta una serie de criterios y obtener del cliente unos datos interesantes para la investigación:

- Definición de la línea temporal. Es crítico en casi cualquier análisis definir tiempos, tanto para acotar la investigación como para definir las conclusiones siguiendo patrones claramente definidos. Muchas conclusiones deberán apoyarse en esta circunstancia y las vaguedades aquí suelen dar resultados poco satisfactorios.
- Búsqueda de elementos o palabras clave. En ocasiones los indicios no estarán definidos pero resulta totalmente indispensable tener consciencia de qué buscar. Un nombre, una web o una dirección de correo suelen ser datos que el cliente puede llegar a facilitar y suponen un buen punto de origen para analizar con consecuencia. Sin estos datos claros hay que despedirse de un análisis rápido y fructífero.
- ¿Quién es quién? Es vital conocer lo máximo posible de las personas involucradas. Usuarios afectados, direcciones, teléfonos, etc., son elementos

que en determinados escenarios son vitales. A veces en la búsqueda de conversaciones almacenadas en un equipo no aparecen nombres directamente pero sí por ejemplo motes. Establecer un cuadro relacional puede resultar esclarecedor en determinadas circunstancias. No sería el primer caso en el que tras una investigación se tuviera la convicción de la existencia de relaciones sentimentales desconocidas para la propia organización (también para sus propias parejas).

Mirar más allá de lo que se tiene resulta vital para el caso y sobre todo el no perder evidencias por no tomar la debida precaución. Nunca debería descartarse la posibilidad de incorporar nuevas evidencias a un escenario. Cuando se destapa el inicio del caso, por retirada de un ordenador o comunicación a los investigados, pudiera resultar que la información sensible estuviera en otro equipo y así dar margen a que estas evidencias pudieran ser eliminadas. Es importante hacer notar esta posibilidad al cliente para que puedan tomarse medidas oportunas o plantear una estrategia de adquisición de evidencias con mayor alcance del previsto inicialmente. Por ejemplo si hay sospechas, aunque no totalmente fundadas sobre una persona, debería procederse a clonar el disco de su equipo desde el inicio por si la investigación base y conductora del caso derive también en la necesidad de tener que analizarlo a posteriori.

Este punto resulta especialmente conflictivo puesto que poner en guardia o crear supuestos sospechosos de personas que pudieran ser inocentes generan una desestabilidad palpable en el trabajo. Pero hay que valorar siempre con el cliente, si el caso está por encima de todo, a excepción de la ley. Es decir recuperar el disco sin un procedimiento válido desde el punto de vista judicial, o el procedimental de la empresa recogido en el uso de medios, puede dar con un caso invalidado por muy claras que muestren ser las conclusiones. Siempre hay que tener en mente la adquisición y preservación de las evidencias sobre el resto de circunstancias.

A la hora de analizar un disco resulta casi imprescindible buscar en todos los lugares, incluidos en los potencialmente inexistentes. Más allá de los escenarios antiforense, muchos casos requieren de la recuperación de ficheros eliminados. Un “sospechoso” obsesivo puede tener el cuidado necesario para eliminar ficheros o datos que puedan ser contraproducentes para él. Pero también hay que ser conscientes de que lo mismo, éste posee los conocimientos necesarios para hacer que la eliminación de los datos sea irreversible.

Recuperar ficheros eliminados es una tarea que lleva mucho tiempo y a veces sin resultado nada positivos y difíciles de gestionar en un juicio, pero al menos puede dar indicios importantes. Medio fichero es mejor que nada. Las herramientas forense tales como EnCase o FTK cuentan con módulos para hacer búsqueda de ficheros eliminados y sobre ellos poder hacer también uso de búsqueda de palabras o frases clave. La dificultad aquí estriba en hacer creíble la prueba de cara al juicio.

Es también vital en muchos casos forenses, el buscar patrones más o menos definidos de conducta. Usuarios que se conectan a unas horas concretas, correos que se envían desde unas IP específicas que aunque dinámicas pertenecen a un mismo rango, frases o palabras muy especiales, representa ejemplos de patrones que pueden ser fáciles de rastrear. En un caso reciente una misma cuenta de usuario que accedía a datos de otros usuarios de forma ilegítima, era utilizada por dos personas diferentes. Se llegó a esta conclusión, además de por otros indicios, porque en el método de validación empleado se usaban dos patrones de autenticación totalmente diferentes aunque válidos (dominio\usuario y usuario@dominio).

Analizar patrones, a priori puede resultar algo complejo, sin embargo con una buena tabla y dosis de relación puede ser un potente instrumento. A nadie se le exige tener la mente analítica, relacional y obsesiva de John Forbes Nash, pero sí es una capacidad interesante para un forense contar con capacidades de razonamiento. En muchos de los casos en los que se ha participado acaban destacando determinados patrones que dan pie en la elaboración de las conclusiones. También se ha podido observar que convenientemente introducidas en el juicio, citar los patrones constituye un puntal esencial para poder conducir las alegaciones y/o conclusiones que se presentan ante el Juez.

Los patrones deberían ser cotejados con el cliente, puesto que a veces se pueden observar apreciaciones muy interesantes. Por ejemplo todos los días se producen conexiones desde una misma máquina pero un día determinado no se produjeron. Cotejándolo con información mantenida por la organización, puede resultar que ese día la persona sospechosa no acudió a trabajar puesto que fue al médico. Cuidado también en este sentido con el tratamiento de datos que puedan resultar invasivos en la intimidad de las personas afectadas, no sea que el juicio acabe derivando en otro por violación de la intimidad.

Estos datos podrán ser introducidos en el informe como parte esencial de las conclusiones derivadas, no obstante hay que matizar las condiciones del mismo. Un informe pericial nunca puede encontrarse condicionado por el cliente y mucho menos

en parte o su totalidad elaborado por él. Será tarea del analista solicitar determinada información y por lo tanto a su criterio como perito introducirla en el informe como una conclusión más.

Es muy importante ser escrupuloso con los análisis. Ser un buen analista forense, implica ser organizado. Hay que tener claro desde el principio cuales son los objetivos pero sin desdeñar alternativas. Si eres caótico saltarás desde una pista a otra sin una clara visión y esto se refleja indefectiblemente sobre el informe, y como no en un mal trabajo. Hay que anotar cualquier apreciación relativa a información obtenida o bien que se obtenga por el cruce de resultados. No hay que confiar nunca en la buena cabeza puesto que ante la avalancha de información que se obtendrá, se acabarán perdiendo muchos detalles importantes. Es una buena práctica llevar un cuaderno de bitácora donde anotar cualquier apreciación, evidencia, horas, fechas, nombres, etc.

Las herramientas son una parte importante de los análisis, pero ni mucho menos lo más esencial. La experiencia, eficacia y buen hacer del especialista, son la clave para obtener resultados válidos y fiables. Las herramientas sin unas manos que las dirijan no servirán de nada. La experiencia ha mostrado lo potente que pueden ser aplicaciones “de andar por casa” en manos expertas. No existen varitas ni teclas mágicas para afrontar un caso. Cada uno de ellos es un mundo y es muy importante sobre todo perder prejuicios y conclusiones preconcebidas. El asesino no siempre es el mayordomo. Y a veces también una visión lejana de un tercero en momentos de bloqueo puede dar aire fresco.



Capítulo 6 – El informe pericial

El informe constituye, sino el más importante, uno de los elementos esenciales en un caso forense. Hay que tener presente que por muy buenos que hayan sido los procedimientos llevados a cabo, las técnicas empleadas y los resultados obtenidos, si no se reflejan correctamente en un documento, no tendrán valor alguno. Al final, al igual que en una auditoría, el valor del trabajo reside en el documento y por ello el analista será valorado.

Un informe de este tipo, presenta sus características y hay que tener presente que aunque la carga técnica resulta importante el objetivo final es transmitir también una parte de él a personas que en muchas ocasiones no tienen una relación directa con la informática. Son meros usuarios tecnológicos. Por lo tanto conjugar el arte de hacer lo técnico, no hay que obviar que no deja de ser un pericial, entendible es quizás el mayor reto de todos. Al enfrentarse al papel en blanco hay que evitar el primer hecho de intentar parecer el más de los gurús técnicos.

Algo no entendible pierde todo su valor de cara al juicio. Es más el propio abogado tendrá complicado la defensa si no es capaz de conocer la información esencial. Algo como una dirección IP para un neófito en tecnología puede suponer un problema a la hora de entender el informe.

Hay que tener presente siempre en su elaboración la independencia de la que parte el perito, reflejando la realidad de los resultados. Aunque existirá una tendencia a reflejar cierta parcialidad en las conclusiones, esto no debe condicionar su elaboración.

Un informe debe tener una línea maestra definida. No pueden plantearse unos objetivos de inicio y acabar hablando de lo divino y lo humano. Debe ser consecuente y por lo tanto no dejar hilos sueltos sin haberlos atado, puesto que podría arrojar dudas sobre la validez del documento.

El informe tiene un tempo en su desarrollo, dimensionado a través de las diferentes fases:

- Antecedentes.

- Evidencias.
- Análisis y tratamiento.
- Resultados.
- Conclusiones y/o recomendaciones.

Los antecedentes suponen la mejor forma para iniciar el informe. Debe reflejar tanto los objetivos, como las reuniones iniciales. Es importante definir los motivos por los que se ponen en contacto con nosotros para iniciar el proceso definiendo así el alcance del mismo. Estos objetivos constituyen la línea maestra de la investigación y las conclusiones deben ser fiel reflejo de haberlos culminado (en un sentido o en otro). Es importante también exponer a través de los antecedentes las líneas temporales que habrán formado parte de los análisis y en qué medida se relacionan con el caso.

El segundo punto es de los críticos: la presentación de las evidencias. Hay que recordar que estas son la piedra de toque del informe. Tal y como se ha reflejado en los anteriores puntos su identificación, recogida y almacenamiento es clave para la elaboración del informe. Los procedimientos empleados deben reflejarse en el informe, para garantizar siempre que se han llevado a efecto las buenas prácticas en su mantenimiento, evitando cualquier manipulación de las mismas que pudiera implicar un perjuicio a cualquiera de las partes.

Hay que enumerarlas y facilitar toda la información que se pueda de ellas. De dónde han salido, cuál es la motivación para su obtención, los fundamentos de su adquisición, cómo se han tratado, copias existentes de las mismas, quién las ha recogido, almacenado y analizado, son algunas de las cuestiones que debe reflejar el informe con respecto a las mismas. Sería importante definir también en el informe, cuando sea factible, los fundamentos existentes que muestren la no manipulación de las pruebas. Por ejemplo a través de la firma tomada de las mismas.

Si hubiera alguna evidencia delicada en lo concerniente a su modo de adquisición, podría motivarse el porqué de la metodología empleada, ahondando en las precauciones que se han tomado, y la importancia de su relación con respecto al caso. Si determinadas evidencias han sido adquiridas una vez que la línea de investigación ha sido iniciada, deberá también indicarse, así como el motivo para ello. Por ejemplo en las pruebas iniciales se detecta parte de una conversación mantenida desde un equipo X. Se procede por ello a realizar un análisis del mismo adquiriendo su disco duro.

Los resultados y conclusiones deberán derivarse de las evidencias presentadas. Si hay conclusiones que se proporciona sin un sustento en las evidencias, serán tomadas como elucubración y por lo tanto su valor puede ser puesto en entredicho. La valoración del perito es válida mientras demuestre su imparcialidad, pero con las evidencias bien definidas afianza siempre esta postura.

El tratamiento de las evidencias adquiridas es el siguiente punto del informe. El análisis de las mismas proporcionará unos datos de los cuales se espera una relación. El factor fundamental para la exposición, debe ser el de causa-efecto. Es interesante en este sentido atender al principio de intercambios de indicios o de Locard, que aunque aplicados fundamentalmente a los indicios o evidencias físicas, pueden ser tenidos en consideración también en las de tipo digital.

En el caso de que el analista detecte la existencia de patrones, deberán citarse como un aspecto importante a la hora de elaborar las conclusiones. El análisis debe ser escrupuloso, metódico y cuidadoso en su ejecución. La falta de método se refleja en gran medida en el informe, produciendo unos resultados muy difíciles de consolidar e hilvanar.

La fase de análisis debe ir proporcionando paulatinamente los resultados, dosificándolos en su justa medida y preparando las últimas fases del informe. Esta fase estará cargada de tecnicismos lo que deberá ser contrarrestado con un anexo en forma de glosario que permita de una forma clara y comprensible explicar los mismos. También serán presentados como anexos aquellos resultados que puedan ser repetitivos y que aunque de importancia, desvistan al informe de su peso específico. Por ejemplo si se ha realizado un análisis de múltiples ficheros de logs, estos deberían condensarse en una serie de tablas descriptivas en el informe y presentarse como anexos toda la información tratada, referenciándose para ello en el documento.

Los diferentes análisis deben establecer siempre que fuera necesaria la correlación existente entre ellos, pero no deben anticiparse las conclusiones, fundamentalmente para no obviar los hechos en el punto final. Si se considera importante anticipar a través de los análisis una determinada información o relación, deberá volverse a exponer en las conclusiones, aunque pueda parecer reiterativo. Es factible que determinadas personas solo revisen resultados y conclusiones.

Los análisis deben reflejar la pericia del investigador. Aunque también muestran las eficacias de los métodos y aplicaciones empleadas, deben dejar siempre paso a la labor pericial (por lo menos en España donde no existen las herramientas validadas, ni aquellas que su empleo garanticen un éxito de cara al juicio).

La exposición de resultado es una continuación de la fase de análisis. Aquí se definen toda la información obtenida y que puede ser relevante para el caso. Aunque en mente se encuentre ya la correlación de los datos, es una tarea que debe ser más propia de las conclusiones, aunque puede irse ya atisbando las peculiaridades. Los datos deben ser fríos y mostrar el fiel reflejo del análisis. Deben prestarse al hilo conductor de la investigación, reflejando y realizando los más significativos frente a los menos importantes. Deberán tenerse en cuenta todos, sean o no favorables, puesto que siempre hay que pensar en un posible contrapericial y en la imparcialidad con la que cuenta el perito.

En la medida de lo posible la presentación de resultado debe ser acorde a la línea temporal definida a través de los antecedentes y que junto con otros elementos muestran el hilo conductor del caso. Información sensible, particularidades, referencias y un largo etcétera de elementos deberán ser parte también de la presentación de los hechos.

El punto final, pero será indudablemente lo primero que se lea del informe, lo constituyen las conclusiones. En algunos informes, especialmente en aquellos de una voluminosidad considerable, se presentan casi al principio, a modo de informe ejecutivo. Si en los puntos anteriores el investigador era parte importante, aquí lo es todo. No existe ni método, ni herramienta, ni nada, salvo experiencia, buen hacer o capacidad de análisis y síntesis en lo que apoyarse. Aquí realmente es donde se juega todo y donde existe la diferencia en el que alguien pueda llegar a ser considerado inocente o bien la empresa piense en iniciar una acción judicial. Es el momento de reflejar relaciones, de presentar las pruebas en toda su crudeza, en defender los patrones detectados que indican conductas reiteradas y que puede marcar el gradiente final de una sanción. Las empresas tienen en cuenta que no es lo mismo un hecho aislado a algo que se realiza con asiduidad. Es importante abstraerse de las circunstancias, al igual que si el analista fuera jurado, obviando el hecho de que lo que se escribe podría conllevar la cárcel para alguien.

Las conclusiones son la síntesis y el desenlace del caso. Un mayor número de conclusiones no tiene por qué reflejar siempre un mejor trabajo. A veces se exponen datos inconexos y sin sentidos que distraen de la acción principal y que resultan perniciosos para un juicio, puesto que la otra parte los identificará claramente y los utilizará para desmontar el pericial realizado. Poco y bien planteado es mejor que mucho y desdibujado.

Un informe además de los anexos que correspondieran, puede acompañarse por la solvencia del analista forense. Refleja su pericia y no da pie a que se pueda dudar de su validez. Hay que tener presente que quien suscriba el informe se encuentra ligado a la necesidad de prestar declaración en el juicio, en calidad de testigo pericial.

Un informe podría presentar flecos o la necesidad de obtener información que ha sido imposible conocer de antemano siempre y cuando exista una causa justificada, por ejemplo la aparición de una información como direcciones IP públicas que solo se encuentra en posesión de los proveedores de Internet. No es objetivo del analista elucubrar con las posibilidades que pueden arrojar esos datos, sino simplemente razonar circunstancias y esperar a que los datos corroboren de una u otra forma sus conclusiones.

Para todos aquellos que tengan interés como es un informe pericial de carácter “oficial”, en el siguiente enlace puede verse un informe forense de Interpol sobre los ordenadores y equipos informáticos de las FARC decomisados por Colombia.

- <http://static.eluniversal.com/2008/05/15/infointerpol.pdf>



Capítulo 7 – Prueba anticipada en un proceso Civil

En determinadas circunstancias un análisis forense puede llegar a un punto muerto o bien a unas conclusiones “inconcluyentes” porque la información necesaria se encuentra fuera del alcance del investigador. En manos de un tercero. Por ejemplo en un análisis de una intrusión, en los registros de un servidor podrían haberse quedado reflejadas unas direcciones IP públicas de las que solo el proveedor conoce a quién ha podido ser adjudicada en una fecha y hora concretas. En ocasiones se ha visto como se iban a desechar esas pruebas ante la creencia de que no podría obtenerse la información correlacionada del ISP.

Obtener esos datos resulta totalmente vital pues es la información precisa que permitirá en condiciones adecuadas motivar un hecho o en otras incriminar a una determinada persona. Puesto que bajo ninguna circunstancia el analista tendrá acceso a la información y elucubrar sobre la posibilidad, aunque factible, no tiene validez en el juicio al no poder probar nada, será necesario solicitar la información.

Es importante en este sentido tener en cuenta la volatilidad de estos datos y pensar en solicitarlas ante la posibilidad de que puedan ser destruidas. Por ejemplo que el proveedor de Internet deseche los registros relativos a las conexiones de sus abonados.

Este procedimiento se denomina solicitud de prueba anticipada. Su base se encuentra en la protección del derecho fundamental a la prueba. Puesto que existe el riesgo de que una prueba pudiera no practicarse porque hay que esperar a que llegue el tiempo necesario a la fase de procedimientos para su práctica, se requiere el adelantamiento de la prueba. Aunque el proceso judicial no haya sido iniciado podrá solicitarse que se practique el proceso de solicitud anticipada.

La Ley 1/2000 de Enjuiciamiento Civil a través de su sección IV que comprende los artículos del 293 al 298 recoge precisamente el ordenamiento de la prueba anticipada. Dicho proceso puede ser invocado por cualquiera de las partes, debiendo ser motivada y solicitada al tribunal que está llevando el caso siempre con anterioridad al inicio del juicio.

El escrito es remitido por el abogado que llevará el caso ante el juzgado que correspondiera, a través de una súplica de oficio. En este sentido es recomendable que el escrito sea revisado por el analista forense. Aunque está claro que el lenguaje judicial se encuentre fuera del alcance del investigador sería recomendable aconsejar técnicamente puesto que pueda ser factible que se pueda cometer un error a nivel técnico que haga imposible atender la súplica.

Adicionalmente a otras peticiones que puedan ser cursadas mediante este procedimiento, las más relacionadas con las pruebas informáticas, suelen ser aquellas que poseen los proveedores de Internet. El ejemplo anterior de direcciones IP públicas, datos de envío de SMS, uso de Smartphone o identificación de correos electrónicos son algunas de las circunstancias que haría necesario la acción de un tercero.

Toda la información que pueda ser aportada en este sentido resulta sumamente crítica, debiendo afinar lo máximo posible para hacer factible la petición. Por ejemplo si se conoce la o las direcciones IP (habitual en el uso dinámico de las mismas), sería conveniente determinar cuál es el proveedor asociado a la misma. De esta forma la petición al juzgado puede ser encaminada de la forma correcta.

Existe la tendencia a dudar de pruebas donde puedan existir conexiones con un patrón similar, pero que procedan desde direcciones IP de diferentes proveedores. La primera impresión que se tiene, es que el análisis ha sido llevado de forma incorrecta. Se duda a la hora de realizar la solicitud por miedo el fracaso o un resultado no esperado. Sin embargo se dan muchas circunstancias para que este hecho sea factible:

- Que existan actores diferentes implicados en el hecho.
- Que haya un único actor pero que ha operado por ejemplo desde su casa y la de un familiar o algún amigo.
- Que sea un único actor pero haga uso de diferentes tecnologías. Por ejemplo uso de ADSL y Smartphone que impliquen a diferentes proveedores.

La petición debe ir acompañada de toda la referencia máxima que pueda ser aportada. Por ejemplo en el caso de las direcciones IP, deben aportarse los datos del proveedor y fecha y hora de la conexión. Hay que tener en cuenta en esta circunstancia las posibles discrepancias que pueden tener los ficheros de Logs con las horas locales reales donde opere el proveedor.

Estas pruebas suelen ser determinantes para un juicio y por lo tanto hay que hacer todo lo factible para obtenerlas. Es indudable que ante una información que solo puede aportar un tercero, como que en una fecha concreta una IP está asociada

directamente a uno de los actores, ésta cobra importancia extrema en el juicio. La imparcialidad total del tercero, al no conocer ni estar involucrado en la causa, hace que la prueba tome mucha fuerza si el abogado la utiliza apropiadamente. Por lo tanto la súplica deberá realizarse con la debida anticipación para que las pruebas puedan llegar a tiempo a la vista.

Tras la obtención de los resultados resulta evidente que la estrategia de cara al juicio puede influir decisivamente el resultado obtenido de la solicitud de prueba anticipada.



Capítulo 8 – Un Juicio Civil

Tras las labores realizadas y todo el esfuerzo empleado, llega la hora final. Hay que tener presente que cualquier forense o pericial que se precie por muy bueno que pueda llegar a ser, se dirime finalmente en el juicio. De forma previa habrá servido para que la empresa de un paso hacia delante a la hora de tomar decisiones, pero donde se la juega finalmente y también el perito, es en el juicio.

El paso previo a la vista, debería consistir en mantener una reunión con el abogado. Aquí debería en la medida de lo posible establecerse la estrategia que deberá seguirse. También es importante aprovechar el momento para que el perito pueda aportar apreciaciones interesantes o su perspectiva en cuanto a las cuestiones importantes que podrían ser el hilo conductor de las preguntas. También planteará sus apreciaciones sobre las cuestiones que de índole técnico podrían utilizarse contra la testificación de la otra parte. Sin esta preparación, el juicio puede ser una verdadera lotería. O el perito es muy hábil y tiene experiencia sobrada, o sin saber por donde irán las preguntas pudiera realizar una testificación ambigua, poco veraz o en ocasiones hasta contraproducente.

El abogado en un juicio de tipo civil preparará una nota que será acompañada el día de la vista y donde la información pericial tiene una importancia significativa. A modo de informe ejecutivo se describen los conceptos y conclusiones más importantes que acompañados de los fundamentos legales, permitirán llegar al objetivo perseguido: atender o desestimar una demanda. El perito debería ayudar técnicamente en su elaboración.

El día de la vista el perito deberá asistir junto con un documento, DNI preferiblemente, que permita identificarlo. Este deberá quedar fuera a la espera de ser llamado. De esta forma se logra que los testigos desconozcan lo que se está fraguando dentro y pueda ser lo más objetivo posible en su intervención. En el proceso convencional cada parte presentará sus testigos, entrando en primer lugar los que presenta el demandado y en segundo los del demandante.

Por estrategia, el perito suele ser el último en declarar de la parte implicada, para centrar sobre él las conclusiones. Hay que tener en cuenta siempre su carácter totalmente imparcial con las partes y su deber de independencia. Tras entrar en la sala, habiendo entregado su documento identificativo se le dirige el Juez para identificarlo y comunicarle su deber de prestar la verdad y no dar falso testimonio. Hay que tener en cuenta que en caso de faltar a la verdad podría ser castigado con pena de prisión y multa.

Se le hará entrega del informe pericial, que deberá reconocer como suyo. Lo tendrá a su disposición para las aclaraciones o poder referirse a él ante cualquier planteamiento que pudiera darse a las preguntas que se le hagan. En primer lugar le realizará preguntas el abogado de la parte por la que se presenta, en segunda instancia la otra parte. Este punto es fundamental puesto que normalmente se pueden presentar como objetivo atacar la credibilidad del perito o bien la credibilidad del testimonio. Para finalizar, si el juez tiene alguna pregunta que realizar también se la transmitirá al perito.

Debido a la relevancia de la información que aporta, esta parte del juicio se presenta siempre como una de las críticas y suele ser tenida en gran consideración por parte del Juez. No obstante no hay que olvidar nunca, para no desacreditar su criterio, la garantía de independencia que se espera del mismo.

Por regla general ningún perito en su primer juicio suele estar preparado para la situación que se le presenta. Los nervios no permiten visualizar con claridad la situación y puede errar en sus apreciaciones, por lo tanto hay que ir lo más sereno posible. Los abogados se enfrentan a esta situación con la mayor de las normalidades posibles, están en su mundo y lo controlan, por lo tanto debería dejárseles a ellos el manejar las situaciones. Sin embargo es muy importante tener en cuenta las siguientes consideraciones:

- Del perito se espera que tenga capacidad de analizar los hechos y aportar su experiencia. Esto difiere de los testigos puesto que estos solo declaran por los hechos que conocen.
- Hay que estar preparado para las preguntas que pueda hacer la otra parte. No entrar bajo ninguna circunstancia en enfrentamientos, puesto que harían dudar del buen hacer de la pericial. Sería importante pensar antes del inicio del juicio en aquellas preguntas que pudiera hacer la otra parte para anticipar las respuestas y no dudar ni herrar en la vista.

- Aunque un perito es considerado como técnico, habitualmente el público ante el que habla no lo es y por lo tanto deberá ser comedido en la forma que expone sus respuestas. Cuanto más sencillo y comprensible, más claro lo podrá tener el juez.
- Aunque muchas preguntas tienen como objetivo respuestas simples de sí o no, podrán hacerse tantas consideraciones como sean oportunas para aclarar sobre todo situaciones que puedan ser trampas.
- Ante una pregunta dudosa se puede solicitar que se replantee de nuevo si no ha sido comprensible. Es preferible que se pregunte de nuevo a que se de una respuesta rápida e inadecuada por no haber entendido la pregunta.
- También hay que tener presente que pueden darse como respuestas un “no recuerdo” o “no lo sé”. No se exige que haya que saberlo absolutamente todo, pero siempre sin faltar a la verdad.
- Hay que esperar preguntas o afirmaciones que cuestionen del proceder en el pericial o las conclusiones emitidas en el informe. Ante todo profesionalidad y aclarar para que no quede duda, pero nunca entrar en conflicto.
- Un momento clave suele ser el de las preguntas orientadas a poner en entredicho las evidencias. Si no existe otra posible defensa, la otra parte podría intentar en su estrategia desmontar la pericia esgrimiendo manipulación de las pruebas. Si los procedimientos han sido bien llevados, será solo un trámite que incluso podrá reafirmar el valor del forense.
- Ante preguntas del informe pericial, sobre todo si hace tiempo que se realizó, es preferible darse un tiempo a leérselo antes de dar una respuesta precipitada y contraria al propio documento.

Finalizadas las preguntas el perito podrá presenciar el resto del juicio. Conviene en este sentido mantener en todo momento la compostura. En la puesta final de las conclusiones los abogados pueden proporcionar información contraria al informe o intentar desvirtuar las palabras dichas por el perito en la práctica de las pruebas, debe mantenerse la calma. Hay que tener en cuenta que los jueces son profesionales y cuentan con esas artimañas de los abogados. De hecho los juicios se graban y los jueces tendrán el pericial y toda la información aportada en el juicio tales como las pruebas anticipadas, que le ayudarán a emitir la sentencia.

Finalizado el juicio y quedando visto para dictamen firmarán todos incluidos los peritos en calidad de testigos. Ahora deberá esperarse un tiempo a que el Juez emita su

sentencia. No cabe duda que un juicio constituye una experiencia enriquecedora para cualquier analista forense. Ayuda sobre todo a comprender la importancia de los procedimientos. Mejora sobre todo la forma de entender y elaborar los informes. Cuestiones que inicialmente se consideran muy importantes en los informes la pierden a veces en los juicios, sin embargo las ganan otras que se creían mucho menos importantes.

Cada juicio es diferente en sí y la personalidad de cada uno Juez, abogado o el propio perito hacen impredecible su resultado. En ocasiones se pasará por la frustración de una sentencia contraria cuando todo estaba a favor. Pero es parte de un juego donde en la mejor de las situaciones habrá un 99% de posibilidades de ganar.



Capítulo 9 – Claves de un forense en Juicio

Tal y como se ha mostrado a lo largo de los diferentes capítulos, un forense sigue unos procesos muy concretos y a veces complejos, siendo necesario ser muy cuidadoso en los mismos. Formalmente no existen fundamentos regulatorios en España para la realización de los procedimientos, sin embargo deben seguirse unas buenas prácticas que como mínimo garanticen llegar al juicio con la confianza de unos hechos probables y reproducibles. Este último capítulo se dedicará a repasar el procedimiento que permita defender con garantías un informe pericial en un juicio y a otros aspectos importantes a tener en cuenta dentro del ámbito legal:

- Paso I. Obtener información previa sobre el caso. Antes de comenzar siquiera la recogida de evidencias, el analista deberá estar seguros de las circunstancias. Es preciso obtener la máxima información del caso, de aquellos que pudieran proporcionarla. El escenario puede ser complejo o simple y ello determinará también la cantidad de evidencias a recuperar y tratar. Cuanta más información se obtenga de forma inicial, menor será el número de problemas posteriores derivados por falta de datos o que los mismos sean inconexos.
- Paso II. Obtención de evidencias. Recuperar y firmar las evidencias, generando los ficheros de cadenas de custodias correspondientes. Frente a circunstancias que puedan producirse en otros países, en España este proceso pasa por no alterar las pruebas y garantizar la validez de la prueba pericial. Deberá aconsejarse de los procedimientos para almacenar de forma segura cualquier evidencia que pueda ser aportada al juicio.
- Paso III. Obtener cualquier dato importante que pueda facilitar la parte, de acuerdo a las circunstancias del caso: nombres, direcciones, correos, números, ficheros, etc. Estos datos serán utilizados para realizar búsquedas de manera eficaz. Debe establecerse también una línea temporal que sirva como base para la realización del pericial y articular así un proceso secuencial, manejable y que permita hacer un informe eficaz.

- Paso IV. Ordenar y relacionar los datos obtenidos de las evidencias, nunca deberá ocultarse aunque pudiera ser negativo a la parte contratante. No hay que olvidar que en un perito debe primar la garantía de independencia. El exponer las conclusiones sin injerencia por las partes es una máxima si el pericial quiere tener el valor que le corresponde en el juicio. Tampoco hay que despreciar la posibilidad de que pueda realizarse un contrapericial que destape las cuestiones ocultas y los resultados por lo tanto ser muy contraproducentes, tanto para la parte como para el propio perito.
- Paso V. Construir un informe escrupuloso, técnico pero legible y con unas conclusiones sólidas que permitan arrojar luz sobre el caso. Deberán evitarse las verdades a medias y cualquier apreciación dudosa emitida a través de prejuicios obtenidos en los pasos previos. Un elemento muy importante del informe consiste en definir las garantías que permiten dar veracidad a las evidencias.
- Paso VI. Toda vez que el informe esté concluido y se estime llegar a juicio, se deberá aconsejar al abogado correspondiente, la práctica de la prueba anticipada cuando la circunstancia lo requiera.
- Paso VII. Se debe apoyar al abogado técnicamente en la estrategia a llevar en el juicio para la defensa del pericial y en la preparación de la nota que deberá llevar a la vista. Deberán definirse aquellas preguntas claves para presentar las conclusiones más importantes del informe.
- Paso VIII. En el juicio, el perito juega un papel clave y por lo tanto la otra parte intentará desmontar su figura así como los argumentos más importantes que presente. Debe tenerse siempre en cuenta el carácter imparcial y objetivo del que goza. Si este se pierde, resultarán mucho menos eficaces tanto las pruebas como el informe. La compostura será un punto esencial, no debiendo entrar en confrontación con la otra parte, aunque a veces resulta complicado. Si en el informe se establecía la necesidad de realizar la argumentación técnica necesaria, en el juicio deberemos desprendernos de esa faceta intentando transmitir la información de la forma más clara y concisa para su entendimiento.

Existen muchos aspectos que no han sido tratados evidentemente a lo largo del manual, fundamentalmente por la gran cantidad de circunstancias que pueden darse. Sin embargo hay una serie de consideraciones esenciales para no pasar determinadas fronteras. En ocasiones, y fundamentalmente las empresas, se sobrepasan ciertos

límites que más allá de lo decoroso o no que puedan ser, suponen acciones ilegítimas y que atentan contra determinados principios.

A veces se duda de la realización de determinadas prácticas como el acceso a las cuentas de correo que proporciona la organización a un usuario, cuando las evidencias se encuentren ahí. Existen lagunas interpretativas entre la protección en el ámbito estrictamente personal y la que goza la propia empresa para hacer un uso razonable de los medios que proporciona. Sin un buen documento de uso de medios tecnológicos las organizaciones se enfrentan a la decisión judicial. En este sentido existen sentencias en uno y otro sentido y es que hay que recordar que la justicia en España se basa en la interpretación de la ley y esta puede tener varias caras.

Ante una circunstancia así lo primero a considerar es si la empresa tiene un documento sólido de uso de medios donde se establezca que la misma podrá ejercer el control del uso de los mecanismos que a efectos profesionales se faciliten y que viene reflejado en el estatuto de los trabajadores. Se podría por ejemplo controlar accesos a internet, llevar estadísticas o incluso acceder a las cuentas de correo. Sin este documento deberá hilarse muy fino puesto que las circunstancias podrían desencadenar en dos sentencias totalmente antagónicas. Sirva de ejemplo las siguientes.

En la primera de ellas se estima una demanda por despido improcedente al considerar violación de la intimidad el acceso al correo electrónico de un trabajador en el transcurso de un pericial (<http://www.bufetalmeida.com/64/violacion-de-correo-electronico-de-trabajadores-despido-improcedente.html>). Se proporciona a continuación un extracto de la sentencia que recoge este proceder.

“Del anterior relato de los hechos se dimana que, en el marco del conflicto laboral al que tantas veces se ha hecho alusión y, además, en paralelo a la interposición por la actora de la papeleta de conciliación para la extinción contractual, el empresario encargó a una empresa especializada un análisis (monitorización) de los contenidos del ordenador de la actora, con especial referencia a sus archivos personales (es este último un extremo que queda diáfano al acto del juicio, ante la clara respuesta dada por el perito compareciente a instancias de la empresa a pregunta de este magistrado). A estos efectos, dicha persona -por órdenes de la empresa- entró en archivos de correo electrónico de la demandante, sacó copia y se aportaron como prueba documental. Hay que decir que algunos de dichos correos son de carácter íntimo y personal (especialmente los que figuran numerados como 129 y 136 del ramo de prueba de la demandada).

Dichas consideraciones han de comportar la valoración de si estas pruebas son contrarias a derechos constitucionales y, más en concreto, a lo establecido en el art. 18.3 de nuestra "norma normarum". En el caso de que se diera una respuesta positiva a esta cuestión, las pruebas practicadas resultarían inhábiles, en aplicación de lo contemplado en el art. 11.1 LOPJ.

Séptimo.- Como se puede desprender del anterior relato fáctico -en el que no se ha nombrado en este extremo- este juzgador ha llegado a la conclusión de que dicha prueba es contraria al derecho fundamental al secreto de las comunicaciones - consagrado en el art. 18.3 CE, ya citado-."

Por el contrario puede citarse también el famoso caso de Deutsche Bank donde se recurrió una sentencia en suplicación ante el Tribunal Superior de Justicia de Cataluña por un uso abusivo del correo electrónico para fines personales por parte de un trabajador que había desembocado en despido. Se citan a continuación algunos párrafos significativos de la sentencia.

"doctrina jurisprudencial ha venido señalando (en aplicación al art. 54.2d ET) como esta causa de despido comprende, dentro de la rúbrica general de transgresión de la buena fe contractual, todas las violaciones de los deberes de conducta y cumplimiento de la buena fe que el contrato de trabajo impone al trabajador (STS 27 octubre 1982), lo que abarca todo el sistema de derechos y obligaciones que disciplina la conducta del hombre en sus relaciones jurídicas con los demás y supone, en definitiva, obrar de acuerdo con las reglas naturales y de rectitud conforme a los criterios morales y sociales imperantes en cada momento histórico (STS 8 mayo 1984); debiendo estarse para la valoración de la conducta que la empresa considera contraria a este deber, a la entidad del cargo de la persona que cometió la falta y sus circunstancias personales (STS 20 octubre 1983); pero sin que se requiera para justificar el despido que el trabajador haya conseguido un lucro personal, ni sea exigible que tenga una determinada entidad el perjuicio sufrido por el empleador, pues simplemente basta que el operario, con intención dolosa o culpable y plena consciencia, quebrante de forma grave y relevante los deberes de fidelidad implícitos en toda prestación de servicios, que deben observar con celo y probidad para no defraudar los intereses de la empresa y la confianza en él depositada (STS 16 mayo 1985)."

"En el presente supuesto, la naturaleza y características del ilícito proceder descrito suponen una clara infracción del deber de lealtad laboral que justifica la decisión empresarial de extinguir el contrato de trabajo con base en el citado arts. 54.2.d), al

haber utilizado el trabajador los medios informáticos con que cuenta la empresa, en gran número de ocasiones, para fines ajenos a los laborales (contraviniendo, así –con independencia de su concreto coste económico-temporal- un deber básico que, además de inherente `a las reglas de buena fe y diligencia que han de presidir las relaciones de trabajo –ex art. 5ª ET-, parece explicitado en el hecho 11) y comprometiendo la actividad laboral de otros productores”

A pesar del fallo favorable a la empresa, posteriormente se realizó por parte de la persona despedida una demanda contra cuatro directivos por el delito de descubrimiento y revelación de secretos

Como puede verse, las situaciones pueden llegar a enturbiarse hasta límites insospechados. Como comentaba recientemente con un abogado especialista en casos de este tipo, “yo cuanto más experiencia tengo, más nervioso voy por todo lo que he visto y porque no se por dónde puede salir la cosa”.

Un forense llevado a juicio



Juan Luis García Rambla

Es en la actualidad el Director del departamento de seguridad TI en Sidertia Solutions, en el que se encuadra el área de forense digital. Lleva más de 18 años trabajando con tecnología y relacionado con el mundo de la seguridad informática, tanto a nivel militar como civil. Ha participado y coordinado una gran cantidad de casos forense, habiendo tenido que intervenir como perito en juicios de índole civil.

Galardonado por Microsoft con el premio MVP durante siete años consecutivos en diferentes categorías vinculadas a la seguridad, une su experiencia técnica a un conocimiento de aspectos legales que le hacen tener una visión muy interesante a la hora de enfrentarse a los diferentes casos forense en los que se acaba involucrando

Un forense llevado a Juicio, contiene referencias de las peculiaridades de como debe realizarse un análisis forense de un caso que se enfrenta al reto de ser llevado a Juicio. A menudo las características y peculiaridades de los técnicos informáticos resultan incompatibles con la visión de los especialistas en la interpretación de las leyes. Buenos trabajos a nivel técnico fracasan en un Juicio al no haber seguido unas normas y procedimientos que aunque no escritos se consideran virtualmente reglados.

Este manual aporta la experiencia de los procesos judiciales, pero también la visión de cómo llevar a cabo la investigación y realizar un correcto informe para su presentación en un Juicio. Muestra los errores comunes, cómo deben evitarse y trata de las buenas prácticas para llegar al Juicio con las garantías de haber realizado el trabajo profesional que se espera de cualquier perito forense.