

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 licenciadador (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

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	24
Capítulo 5 – Las buenas prácticas en el análisis.	28
Capítulo 6 – El informe pericial	34
Capítulo 7 – Prueba anticipada en un proceso civil	40
Capítulo 8 – Un juicio civil	43
Capítulo 9 – Claves de un forense en juicio	47

Prólogo

A diario los medios de comunicación nos informan de noticias relacionadas con filtraciones, abusos o ataques relacionados con la tecnología y la informática. Esta realidad es cada vez más evidente y no es más que la punta del iceberg. Junto a estos casos juzgados socialmente, se dan otros miles de ellos que se dirimen en una sala y son conocidos sólo por unos pocos, los afectados. Pero sin embargo, para esta gran mayoría de ciudadanos tienen una transcendencia mucho mayor que aquellos casos con un gran impacto social y mediático.

El esclarecimiento de estas situaciones, que pueden acarrear consecuencias mayores, incluida la privación de libertad para los afectados, son tareas de muy pocos y realmente críticas. Evidentemente no se trata de cuestiones que puedan tomarse a la ligera y deben ir acompañadas de investigaciones rigurosas y de los procedimientos adecuados.

Cualquier investigación forense se encuentra rodeada de un cierto “misticismo”. También es así en esta ocasión, cuando la información manejada es fundamentalmente tecnológica. Sin embargo, no debemos olvidar que aunque la carga técnica es importante, existen también en este tipo de escenarios muchos detalles que se encuentran alejados de una visión puramente informática de la situación que se está analizando. Todo ello resulta aún más acusado cuando el caso forense tiene posibilidades de derivar finalmente en un proceso judicial.

Ante estas circunstancias es frecuente que el parapeto tecnológico detrás del cual se protegen muchos consultores desaparezca, dejando paso a situaciones donde los profesionales de la informática no se encuentran cómodos. En un proceso judicial, el técnico ya no se encuentra en su elemento, no es el “juez” ni quién tiene el control de la situación. Es simplemente una parte más dentro del proceso e incluso, aunque no sea la persona enjuiciada, puede llegar a sentirse juzgado en su labor profesional.

Situaciones que técnicamente se dan como definitivas en un entorno profesional informático pueden ser cuestionadas en una vista judicial. 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 tan preparado profesionalmente. El éxito depende de muchos factores de los que a menudo el perito es un mero espectador.

A lo largo de esta publicación, Juan Luis García Rambla Director Técnico del Área de Seguridad de Sidertia Solutions S. L., realizará el análisis de un proceso forense digital completo. Incorporando en él, desde los apartados más técnicos, que incluyen herramientas y procedimientos, hasta aspectos legales que podrían llegar a ser determinantes en un juicio en el que un profesional de la informática interviene en calidad de perito.

En este documento técnico Juan Luis aporta no sólo su conocimiento en la materia sino fundamentalmente su experiencia, procedente de la directa intervención en casos forenses bien como perito informático bien como coordinador de equipos de analistas forenses. Nos aporta su visión particular de la cuestión, pero sin lugar a dudas la información suministrada permitirá al perito llegar al proceso judicial con un mayor porcentaje de posibilidades de éxito.

La publicación será de especial utilidad para aquellos que inician sus pasos en el delicado mundo del análisis forense, pero también ofrece una visión interesante para aquellos analistas experimentados que nunca han participado en un proceso judicial.

Juan Antonio Calles García

Capítulo 1 – El análisis forense

Como especialidad dentro del ámbito de la seguridad informática el análisis forense digital puede aportar al profesional resultados plenamente gratificantes, pero también situaciones realmente desagradables. Escenarios de actuación en principio sencillos, pueden complicarse hasta límites insospechados. A todo esto se suma una circunstancia difícil de digerir, especialmente para un informático, la subjetividad. Por muy técnicos que sean los resultados obtenidos, por metódicos que lleguen a ser los procedimientos y claras las conclusiones técnicas, todo el proceso no deja de estar cargado de cierta subjetividad. Es más, en un determinado momento la decisión final será adoptada por alguien que presenta lógicas limitaciones técnicas para apreciar lo dispuesto en un informe pericial informático.

Desde su inicio un análisis forense digital debe responder a la pregunta ¿es posible que las conclusiones lleguen a un proceso judicial? Inicialmente, esta cuestión puede parecer poco relevante para un análisis técnico. Sin embargo, esta impresión cambia radicalmente al entrar en calidad de perito en la sala donde se desarrolla el proceso.

Probablemente, en el desarrollo del mismo, el tipo de preguntas a las que se enfrente el informático no serán tan claras y directas como las que en sus labores técnicas contesta habitualmente. Y por qué no decirlo, en muchas ocasiones éstas serán directamente malintencionadas e incluso retorcidas. Una mala respuesta puede llegar a desbaratar judicialmente una buena labor de análisis digital.

En estos momentos es cuando se aprecia lo determinante que es haber realizado correctamente el análisis desde sus inicios. De este modo la duda, la inseguridad y falta de claridad en la respuesta serán infrecuentes. La frustración de que estaba “casi” todo bien y de que por lo menos “lo intentamos” será inusual si la labor técnica de análisis ha sido la adecuada.

Enfrentarse a un caso forense implica tener que anticipar inicialmente la posibilidad de llegar a juicio. A menudo, y en función del escenario, es posible que ese hecho no se observe en un principio, pero tal y como se desencadenen los acontecimientos pueda llegar a darse.

Expongamos a continuación un hipotético caso y que sin embargo recoge situaciones que no son inusuales en la realidad y que ilustran la posibilidad de que un análisis técnico

desemboque en un proceso judicial. El equipo de trabajo de un directivo comienza a hacer “cosas raras”. En consecuencia se decide realizar un análisis del mismo y averiguar que está ocurriendo. Se detecta la presencia de un malware. En ese momento son múltiples las cuestiones a abordar: ¿por qué el antivirus no lo ha detectado?, ¿pueden otros ordenadores estar afectados?, ¿cómo eliminarlo? Sin embargo, en el transcurso del análisis digital no sólo se detecta al elemento malicioso, sino que está provocando una fuga de información. Se localiza quién ha sido el actor (denominación judicial, para ir entrando en materia) culpable de la acción maliciosa y a qué tipo de información ha tenido acceso. Se trata de otro empleado de la compañía que ha sustraído información crítica respecto de la política corporativa de recursos humanos. La empresa afectada ¿no querría llevarle a juicio o despedirlo de forma procedente? Probablemente sí.

Frecuentemente en los casos forenses se sabe cuáles son los inicios de la investigación digital, pero no cuál puede ser su final. Por ello es interesante conocer si el promotor de la investigación tiene de partida la intención de llevar el caso a los juzgados. En múltiples ocasiones los interesados desestimarán esta posibilidad. Sin embargo, es posible que no sean conscientes de las circunstancias reales y al disponer progresivamente de mayor información sus intenciones iniciales se pueden modificar.

Es recomendable por lo tanto desde un primer momento indicar que ante la posibilidad ineludible de que el análisis pueda finalizar en una fase judicial, la recogida de evidencias debe realizarse teniendo esta circunstancia en consecuencia o al menos en caso de no hacerlo comunicárselo a los interesados.

En todo momento se debe hablar de posibilidades. El desarrollo de una investigación digital correcta en sus procedimientos y conclusiones, no asegura el éxito de la misma. En un juicio la decisión final se dirime en un momento y localización puntual. En ocasiones sólo la habilidad y experiencia de unos y otros hacen que la balanza se incline hacia uno u otro lado.

No hay que olvidar que el desarrollo de la recogida de evidencias y de todo el análisis atendiendo de forma rigurosa a los procedimientos adecuados demanda una mayor dedicación y en el mundo profesional el tiempo es dinero. En cada escenario es necesario valorar si la inversión económica, el porcentaje de posibilidades de éxito y el propio desgaste del proceso hacen recomendable el inicio del mismo. En ocasiones lo idóneo será desestimar la realización del peritaje. Tras valorar los anteriores factores no es inusual en casos laborales que una organización puede llegar a la conclusión de que le es más conveniente afrontar un despido improcedente que iniciar una investigación.

Es necesario tener presente aquellos análisis que pueden derivar en un juicio, deben ser atendidos con mayor pulcritud y rigor procedimental para que las conclusiones obtenidas a

partir de las evidencias, sean válidas, creíbles y lo más importante “rotundas” e irrefutables sea cuáles fueren los argumentos utilizados. Aquellas actuaciones cuyo objetivo no es atender a un proceso judicial, sino obtener una determinada información, permiten una mayor flexibilidad, reduciendo con ello los tiempos dedicados a la recogida y tratamiento de evidencias.

La tendencia habitual es hacer uso de procedimientos, que siendo más o menos reglados pueden resultar algo imprecisos o inapropiados para tener valor judicial. Póngase un ejemplo. Para tareas de adquisición de evidencias un especialista puede operar haciendo uso de las normas marcadas en la RFC 3227 “*Guía para la recogida y almacenamiento de evidencias*”. Pero actualmente en España, aplicar esta norma de forma escrupulosa puede ser una temeridad, fundamentalmente porque rompe el principio de que “*antes de tocar cualquier evidencia, prevalece la rigurosa recogida de la misma*”. El escenario nunca debe alterarse. Esta circunstancia puede llegar incluso a eliminar la validez de la evidencia.

En otros países, más avanzados judicialmente en materia de procedimientos forenses informáticos y que incluso disponen de leyes y regulaciones para ello, esta RFC pueda tener su validez. Sin embargo, en otros muchos, como es el caso de España, es mucho más importante poder acreditar la no alteración de evidencias que cualquier otra cuestión. Dicho de forma más coloquial, para el perito es crítico poder afirmar en cualquier caso “*cuando yo llegué, esto ya estaba así*”. En caso contrario, las pruebas pueden ser recusadas por posible alteración de las mismas en el análisis. Aunque la imparcialidad del perito es obligatoria por ley, finalmente sus servicios son contratados habitualmente por una de las partes y se diluye por lo tanto esa esencia de independencia asociada a su labor.

Si es claro que independientemente de cómo se desarrolle el caso, éste no acabará en un juicio, el nivel de exigencias y pulcritud se relaja dejando paso a la efectividad en el análisis

Todas estas claves se irán valorando a lo largo de esta publicación. Ser consciente en todo momento de la importancia del proceso que se tiene entre manos, anticiparse a las cuestiones a abordar antes de hacerlo y conocer las herramientas necesarias para ello. Pero especialmente, cómo abordar la “dichosa experiencia” que un juicio supone para cualquiera, pero especialmente para un informático, que además tiene una labor crítica en las actuaciones judiciales.

Capítulo 2 – La importancia de las evidencias

Uno de los aspectos fundamentales a la hora de afrontar un análisis forense digital, constituye la necesidad de contar con evidencias válidas. A priori, todas aquellas correctamente recogidas potencialmente lo son, pero una mala práctica puede llegar a invalidarlas. Hay que tener presente a lo largo de todo el proceso que el perito debe poder defender y contar con el principio de independencia.

Sin lugar a dudas la información proporcionada por el afectado es vital. Sin embargo, su visión de los acontecimientos puede condicionar en exceso al perito, provocando incluso que su impulso e interés por llegar a la realidad de los hechos le haga actuar a éste sobre el equipo e infraestructuras afectadas sin respetar el procedimiento adecuado para ello. Es un riesgo fundamental en el inicio de un análisis digital luchar contra ese impulso.

Cuando se sospecha que sobre un determinado equipo se ha realizado una acción perniciosa y que por lo tanto debe ser objeto de análisis, la prudencia es fundamental. Inicialmente debe asumirse que es posible que contenga evidencias interesantes y que por ello es necesario tratarlo como un sistema con información importante y sensible para el caso. No hacerlo así y “caer en la tentación” de actuar sobre él precipitadamente, permite en caso de juicio poder alegar que las evidencias pueden haber sido manipuladas con el objetivo de favorecer o incriminar a alguien. Este es también habitualmente un argumento frecuentemente utilizado en análisis contra periciales.

Y si no debe tocarse el equipo ¿qué ha de hacerse? A día de hoy no hay nada reglado en este sentido, pero existen una serie de buenas prácticas y normas no escritas cuya aplicación es recomendable. Si el equipo está encendido es una buena opción obtener una fotografía de la pantalla y apagarlo. Puesto que pudiera haber información importante relativa a ficheros temporales o incluso en sistemas Windows, el propio fichero de paginación de memoria, podría optarse por apagar el equipo por la vía rápida, cortando el suministro de energía. En este procedimiento, 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 para adoptar la decisión adecuada. 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, sólo a extraerlos. No obstante, siempre habrá que tener prevista una respuesta en la vista judicial para una defensa de las acciones realizadas.

La presencia de testigos es una cuestión a considerar en procesos comprometidos. Formulados a través de reglamentaciones de uso de medios corporativos o protocolos de seguridad internos, muchas organizaciones cuentan entre sus procedimientos con mecanismos que hacen uso de testigos para la intervención de equipos, en muchas ocasiones herederos de acciones tales como el registro de una taquilla. Para estos casos, suele requerirse que todo el proceso de recogida de las evidencias sea llevado a cabo con la presencia de una persona del comité sindical y el propio afectado, o en su defecto dos personas de la organización, totalmente independientes a las circunstancias del caso. Estos procedimientos ofrecen la seguridad, sobre todo de cara a procesos judiciales, de que, habiéndose realizado una serie de acciones específicas, testigos concretos pueden refrendar los hechos. Estas acciones se tratan de forma muy análoga 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 en este apartado por el criterio empresarial, a pesar de que la sentencia en cuestión da la razón al trabajador, pero sólo por el hecho de que no se justificó el registro tal y como obliga el artículo 18 del Estatuto de los Trabajadores. La resolución afirma implícitamente, que el mencionado artículo 18 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 es siempre tarea del juez atendiendo para ello a su criterio, interpretando las leyes y aplicándolas 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.

Pero finalmente teniendo en consideración lo expuesto hasta el momento, llegará la hora de adquirir las evidencias como fase crítica del proceso. En este momento vuelve a aparecer la cuestión fundamental, ¿cuál es el procedimiento adecuado? De nuevo la respuesta es compleja, no existe un procedimiento único, así como tampoco existen unas herramientas

“validadas” y que sirvan específicamente a efectos judiciales. Como ya se ha indicado, en muchos países de la Unión Europea, entre ellos España, no existe una legislación para el análisis forense digital. Por ello no puede expresarse de forma taxativa qué proceso es el adecuado ni cuáles son las herramientas necesarias y cómo deben utilizarse.

Básicamente hay que dar respuestas a una serie de preguntas fundamentales:

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

Sin lugar a dudas, una operación crítica para el analista forense es la copia. Normalmente los escenarios a los que se enfrentará demandarán procesos complejos y voluminosos de copiado de información, haciendo incluso uso para ello de distintos medios. La propia configuración del equipo analizado, desconocer la ubicación específica de los ficheros o su ubicación en múltiples medios de almacenamiento, son algunas de las circunstancias posibles que pueden complicar la realización de la copia. Muy probablemente el tiempo invertido será alto y el coste en recursos también.

El proceso de copiado de un disco o de determinados ficheros debe de garantizar las siguientes condiciones:

- Las copias realizadas deben ser idénticas al origen y por lo tanto entre ellas también.
- Bajo ningún concepto el origen de datos debe ser alterado. Tampoco el destino. En este caso la copia queda inutilizada para el proceso de análisis y deberá repetirse. Si no se hiciese así todo el proceso de análisis podría quedar invalidado.
- El copiado debe ser completo, incluyendo el supuesto espacio libre. Muchas veces es posible que aparezca allí información interesante, especialmente si se ha hecho uso de herramientas antiforenses.
- Debe aplicarse una función hash sobre la información adquirida con objeto de obtener su huella digital.

Este último aspecto es fundamental. A través de él se garantiza que las conclusiones a las que se llega tras el análisis de las copias realizadas de las evidencias, parten de un disco o ficheros idénticos al original y por lo tanto no ha habido una manipulación de los mismos tras las copias binarias realizadas.

Inicialmente es necesario determinar cuántas copias deben realizarse. Es recomendable un mínimo de dos adicionales al original. Una de ellas destinada al analista forense, la otra a la empresa implicada o al afectado por el caso, para dar continuidad al trabajo, y finalmente el original que deberá salvaguardarse como elemento crítico. Para esto último son varias las posibilidades. En caso de denuncia se podrá presentar junto a ésta, quedar depositada en un notario o bien almacenada por la organización o persona afectada con las garantías de seguridad debidas. Es fundamental tener en cuenta su importancia de cara al posterior juicio.

El hash garantizará que el disco no ha sido manipulado y este aspecto es fundamental. Permite reproducir las pruebas originales ante la posible realización de análisis contrapericiales. Para la obtención del hash 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. Esta se realiza bien por la clonación del disco físico o las unidades lógicas, o bien generando un único fichero de imagen que pueda ser tratado directamente por las herramientas forenses.

Para ello existen 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 a 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 para un proceso de copia, al no disponer de los accesorios adecuados para recuperar un modelo de disco específico. No obstante existen conversores que facilitan la labor, pero que no garantizan que la compatibilidad pueda mantenerse a lo largo del tiempo.

A modo de ejemplo se presentan 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

Ya se ha tratado en el capítulo anterior la importancia de llevar a efecto un procedimiento adecuado para la adquisición de evidencias. Se citaba el equipamiento hardware como la opción más profesional e idónea para realizar los procesos de copiado necesarios. Sin embargo, existen como alternativa, soluciones basadas en software que pueden encargarse de esta fase fundamental en todo análisis forense. La mayor parte de ellas hacen uso de la función *dd*, existente en entornos Unix y Linux, para la copia de un número determinado de bytes o de bloques. En esta publicación se citan y muestran las opciones proporcionadas por las suites forenses *Helix* y *Caine*.

La suite *Helix de e-fense* (<http://www.e-fense.com/>), ha evolucionado en el tiempo, nació con una inspiración diferente, sobre todo en lo que se refiere 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.

Para los no iniciados en el análisis forense, se realiza a continuación una breve descripción de las tipologías mencionadas en el párrafo anterior. El análisis Live Forensics presenta como premisa la obtención de evidencias y análisis de un equipo mientras el sistema operativo se encuentra iniciado. Resulta especialmente interesante en escenarios como los de identificación de aplicaciones con código malicioso o de ataques que se producen en red. Hay que tener especial cuidado con este tipo de análisis, puesto que existe una alta posibilidad de alterar las evidencias. Por lo tanto, será especialmente crítico el haber realizado una copia binaria adecuada antes de iniciar el peritaje.

Por otra parte el análisis Post Mortem se realiza sin arrancar el sistema operativo del equipo a analizar. Es la tipología más frecuentemente utilizada puesto que el riesgo de modificación de evidencias es muy bajo. Es especialmente útil en búsqueda de datos, análisis de registros o reconstrucción de ficheros eliminados por citar algunos ejemplos significativos. Múltiples herramientas forenses basan su funcionalidad en este tipo de investigación.

A día de hoy las distribuciones de este producto presentan un coste, sin embargo todavía es posible localizar en Internet versiones de la suite que como la 1.9 o la 2008 R1 pueden ser

utilizadas para la adquisición de evidencias. Basadas en la distribución de Linux *Knoppix*, pueden utilizar su funcionalidad de Live-CD para la adquisición de discos.

Las distintas versiones presentan diferencias, no sólo en su presentación sino también en las aplicaciones proporcionadas para la ejecución de procedimientos forenses. La versión 1.9 a diferencia de la posterior 2008 R1, aportaba una funcionalidad adicional a través de la aplicación *Air*.

A continuación se muestran dos imágenes con el la interfaz de cada una de las versiones.

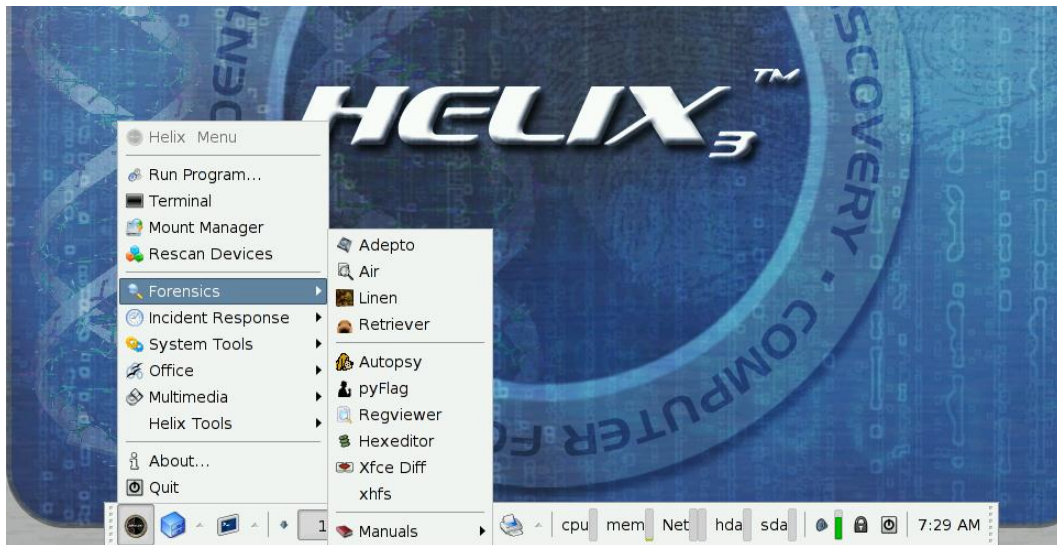


Imagen. 1.- Helix versión 1.9.

Como es posible apreciar las diferencias aparecen tanto en el aspecto visual, como en las herramientas aportadas por cada una de las versiones.



Imagen. 2.- Helix versión 2008 R1.

Ambas versiones incluyen una las aplicaciones más utilizadas para la realización de operaciones de copia, *Adepto*. Esta aplicación permite dos modos diferentes de emplear la funcionalidad *dd* para la adquisición de evidencias:

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

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

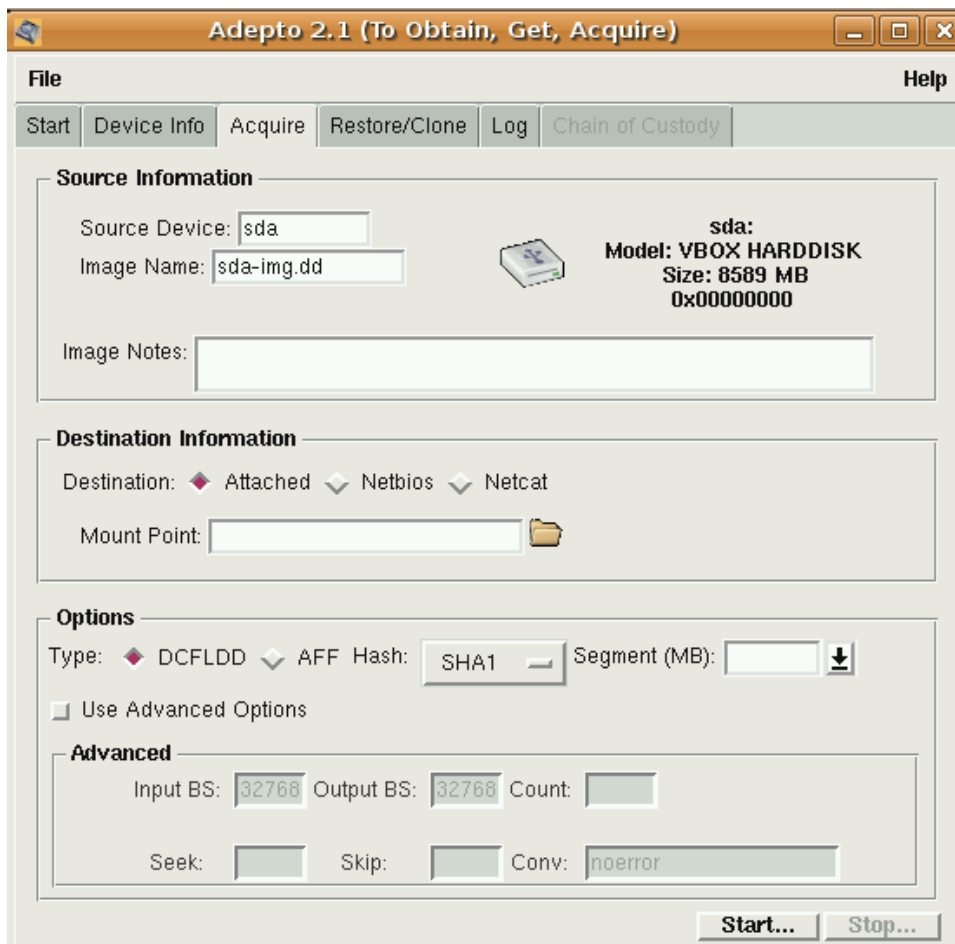


Imagen. 3.- Adquisición de disco.

Como se ha comentado en capítulos anteriores, es un elemento fundamental en el proceso la opción de poder obtener el hash de las evidencias originales. Esta funcionalidad permitirá verificar, en cualquier momento tras la realización de copias, que origen y destino son

idénticos, dando así plena validez a la prueba y a los procesos de análisis que hagan uso de ella, así como a las conclusiones a las que pueda llegarse.

Es recomendable modificar el algoritmo predeterminado de cálculo del hash, MD5. La utilización en su lugar de al menos SHA1 mejora sensiblemente el nivel de seguridad de la operación. Algunas de las motivaciones de esta modificación se recogen en el siguiente artículo del blog “*Legalidad Informática*”:

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

Queda por lo tanto de este modo garantizado que el analista forense no ha realizado manipulación alguna de las pruebas desde el momento en que se realiza la adquisición de las mismas. Claro está que éste no puede extender esta garantía de no alteración con anterioridad a su intervención. No es inusual que los afectados o bien personal informático en su representación, sí que hayan modificado las evidencias originales, de forma más o menos malintencionada dependiendo del caso. Sólo el posterior análisis dará respuesta a esta incertidumbre propia de toda investigación.

Partiendo de la ya mencionada aplicación *dd*, otras metodologías de posible uso como *DCFLDD* y *AFF* presentan características avanzadas en las prácticas de adquisición de evidencias forenses. El primero de estos métodos fue desarrollado por el departamento de los EEUU, *Defense Computer Forensics Lab*. El segundo denominado *Advanced Forensics Format*, fue diseñado como un mecanismo más avanzado que el formato *dd* estándar, siendo más flexible y permitiendo el almacenamiento extensivo de metadatos, además de requerir menor espacio de disco que otros formatos propietarios existentes en el mercado, como el propio de *EnCase*. Teniendo en consideración el tipo de implementación, es recomendable decantarse por la metodología *DCFLDD*.

El segundo de los métodos de adquisición es el proporcionado por *Adepto*, una de las herramientas fundamentales de la suite *Helix*, y basado en la posibilidad de clonación completa de un disco, manteniendo tanto la información como su estructura física, de tal forma que la copia será un calco del disco origen. En esta circunstancia también se realizará una función hash del mismo, que será mostrada a través del sistema Log que proporciona la propia herramienta.

Como es posible observar en la siguiente imagen, también a través del menú de *Restauración/Clonado* de *Adepto*, se ofrece la alternativa de restaurar un fichero tipo *dd* bien sobre un disco o bien sobre otro fichero imagen. De tal forma que se verifique nuevamente la idoneidad del procedimiento mediante función hash del origen y del destino.

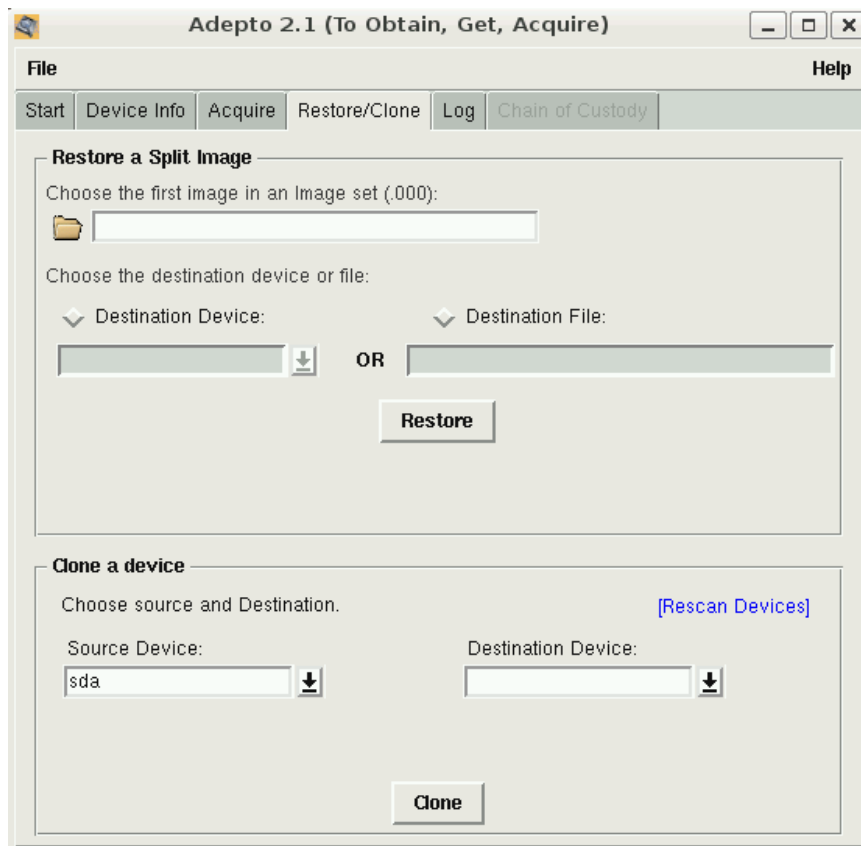


Imagen. 4.- Clonación de un disco

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

- El tamaño de disco es relativamente importante. Los discos origen y destino no deben presentar las mismas características, ni ser idénticos en tamaño, pero al menos el disco destino deberá ser superior en tamaño al de origen.
- Los discos implicados en el proceso de copia no deben ser idénticos en formato. Un disco tipo IDE puede volcarse sobre otro SATA o éste último sobre un disco USB. Para ello es posible utilizar 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 bastante más económico, permitiendo además tratar todos los discos como externos y controlar de este modo la identificación de unidades.
- Puede parecer obvio y realmente lo es, pero la experiencia indica que es útil recordar que en todo proceso de clonación es imprescindible identificar con claridad disco origen y destino. No sería la primera ocasión en que tras la realización de la copia el analista comprueba que origen y destino presentan exclusivamente los ceros que existirían en la supuesta unidad que iba a ser utilizada originalmente como destino.

- Es indispensable que el disco destino no disponga de ningún dato previo. Con ello se evitaría que en el espacio no copiado se encontraran por ejemplo datos de otros casos, con el consiguiente problema de mezcla de evidencias. Sería peculiar ver como el analista intenta desentramar relaciones existentes entre diferentes casos motivado todo ello por el cruce de las evidencias, además de que éstas pueden quedar comprometidas como pruebas del caso. Se tratará posteriormente qué metodología es posible aplicar para que un disco quede limpio de trazas previas.

La utilización de un método u otro de copiado, dependerá fundamentalmente del tipo de escenario al que se enfrente el analista, el tipo de pruebas que sea necesario efectuar y las herramientas con las que se cuente para el análisis. 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 múltiples factores: el espacio a copiar o clonar, la velocidad de los discos, el soporte, el tipo de hash a realizar o si se va a incorporar una verificación de copias son, junto a otros factores, elementos que influyen directamente sobre el tiempo de copiado. Para el que nunca haya realizado una adquisición de este tipo es necesario tener en consideración que se trata de un proceso bastante lento. Como mínimo, para un disco duro convencional y sin que se produzcan errores, estaremos hablando de unas cuantas horas.

Una aportación importante proporcionada por la herramienta *Adepto* es que finalizado el proceso, ésta nos suministrará un fichero de suma importancia en el procedimiento forense, el fichero de cadena de custodia. Este será objeto de tratamiento posterior, pero resulta fundamental como parte de la información que deberá acompañar a cualquier evidencia digital que sea presentada en un proceso judicial.

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 la distribución *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.

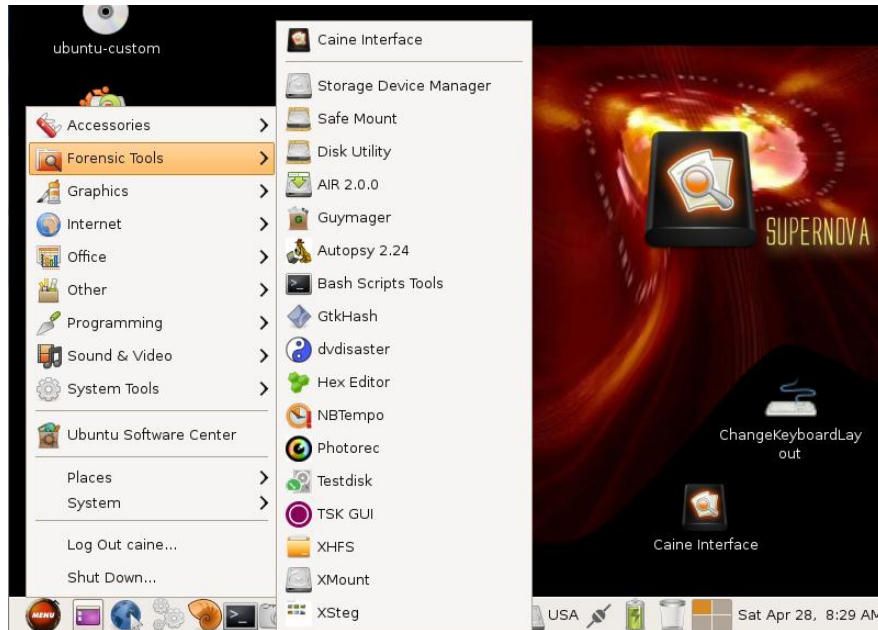


Imagen 5. Utilidades forenses de CAINE V 2.5.1

Para la adquisición de evidencias, la aplicación más destacada con la que cuenta la suite *CAINE* es *AIR* (*Automated Imaged and Restore*). Con ella es posible adquirir discos y realizar algunas operaciones interesantes y habituales en los procedimientos forenses, como es la limpieza de los discos sobre los que realizar el volcado de información.

Tal y como muestra la Imagen 6, a pesar de las diferencias de interfaz y las particularidades de cada herramienta, en esencia *AIR* aporta funcionalidades muy similares a las suministradas por la aplicación *Adepto*, comentada previamente.

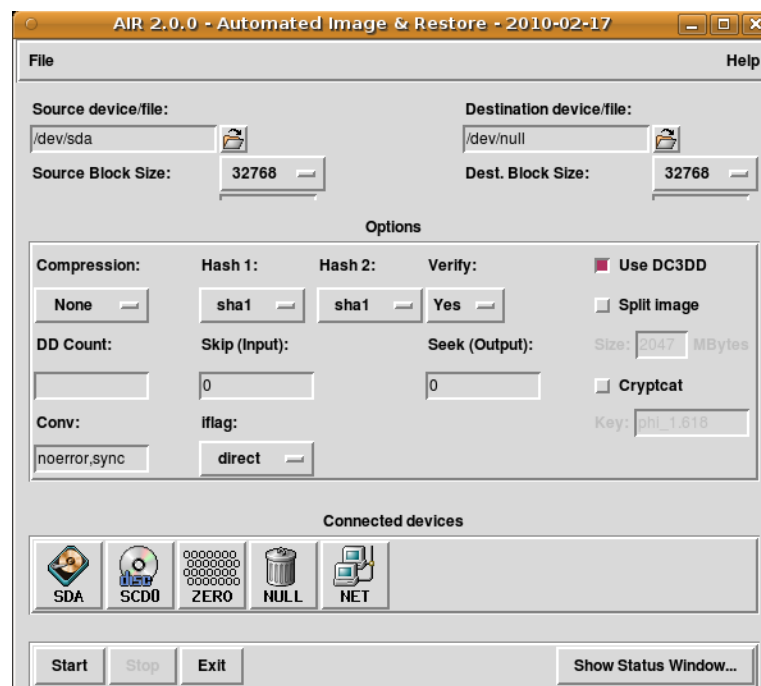


Imagen 6.- Aplicación AIR.

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

Al contrario que en el caso de *Adepto*, la aplicación *AIR* no genera el fichero de cadena de custodia y por lo tanto esta operación deberá efectuarse manualmente, tal y como se mostrará en el siguiente capítulo de esta publicación.

AIR dispone de una interesante función para asegurar la limpieza de discos, *Disk Wiping*. A través de este proceso se vuelcan sobre un disco seleccionado como destino, datos de tipo 0 que serán identificados como origen de los datos, eliminando de este modo cualquier información anterior.

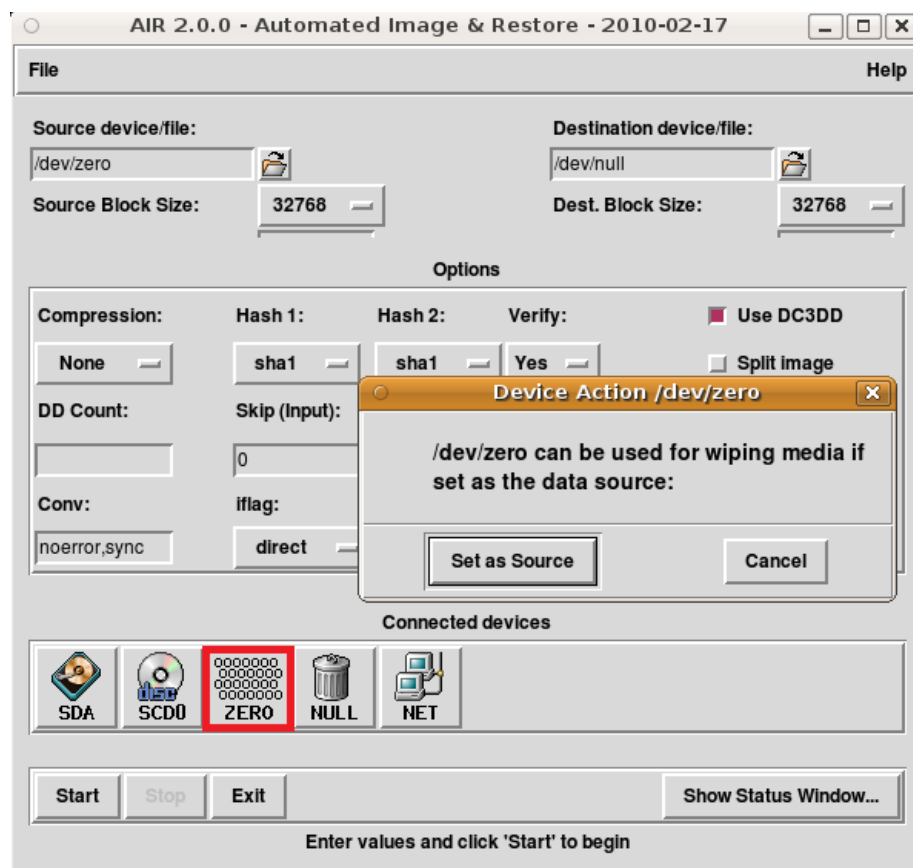


Imagen 7.- Funcionalidad para realizar Disk Wiping.

Tal y como se comentó en páginas previas, esta operación de limpieza constituye un procedimiento indispensable para garantizar la higiene en el tratamiento y posterior análisis de las evidencias de cada caso. De esta forma, existe la certeza de que un disco contendrá información exclusiva de un caso, no quedando rastro de información alojada anteriormente

en el dispositivo. Como hemos visto, esta circunstancia es especialmente importante ante la existencia en un disco de espacio supuestamente no utilizado.

No es inusual que muchos analistas se planteen exclusivamente el análisis del espacio particionado. Sin embargo el no particionado puede contener información perfectamente válida. No debe olvidarse que la eliminación de las particiones de un disco a través de los procedimientos utilizados habitualmente, no elimina la información que pueda residir en el espacio no particionado. Cuando un disco es clonado físicamente, se duplica también el espacio no particionado. De este modo, ante la necesidad de recuperación de ficheros eliminados, que puede darse en determinados procesos forenses, ésta puede efectuarse tanto en el espacio particionado como en aquel que no lo está. Es importante que el disco sobre el que se va a volcar información tenga condiciones lógicas similares al de origen. De este modo, aunque no es obligatorio, sí muy recomendable que si la tecnología del dispositivo origen es USB, IDE o cualquier otra, ésta se corresponda con la del disco destino. Este aspecto resulta crítico en análisis tipo Live Forensics, para evitar la aparición de problemas a la hora de arrancar el sistema operativo y reconocer y trabajar con el disco.

Como es posible apreciar en la Imagen 8, se ha seleccionado como origen el conjunto de bits ZERO y como destino la unidad SDA. Tras aceptar el mensaje de advertencia que aparecerá en pantalla, se iniciará la operación.

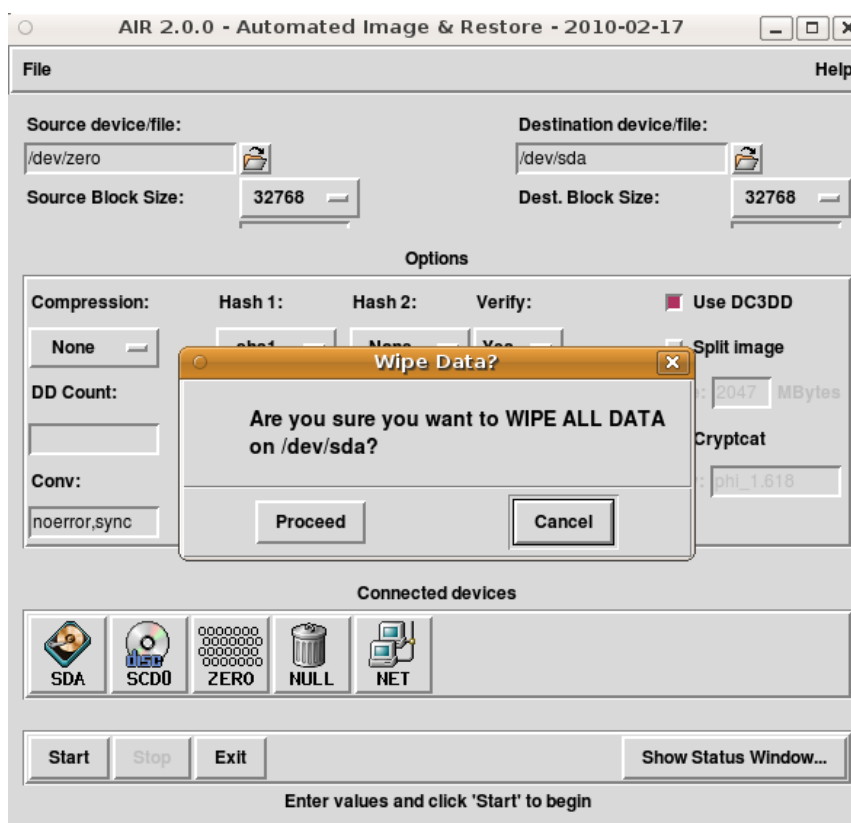


Imagen. 8.- Inicio del proceso de eliminación de datos

La revisión de éste proceso podrá realizarse aprovechando el módulo de estado que proporciona la herramienta *AIR*. En la siguiente imagen, éste muestra información sobre el volcado de bits 0 sobre el disco SDA. Como ya se indicaba para la adquisición de evidencias, estos procesos de copiado son lentos y requieren de un tiempo considerable para ser completados. Esta circunstancia debe tenerse en consideración en la asignación de tiempos que el analista realice para este tipo de operaciones. No olvidemos que en la mayoría de las ocasiones éstas se desarrollan en las instalaciones de los clientes o afectados. En estos escenarios es recomendable contar de partida con discos “limpios”. Los procesos de copiado resultarán por si mismos tediosos, requiriéndose en muchas ocasiones por procedimiento la presencia de varias personas, con lo que es más que aconsejable evitar demoras adicionales provocadas por la necesidad de realizar la limpieza de discos “in situ” con antelación a la adquisición de evidencias propiamente dicha.

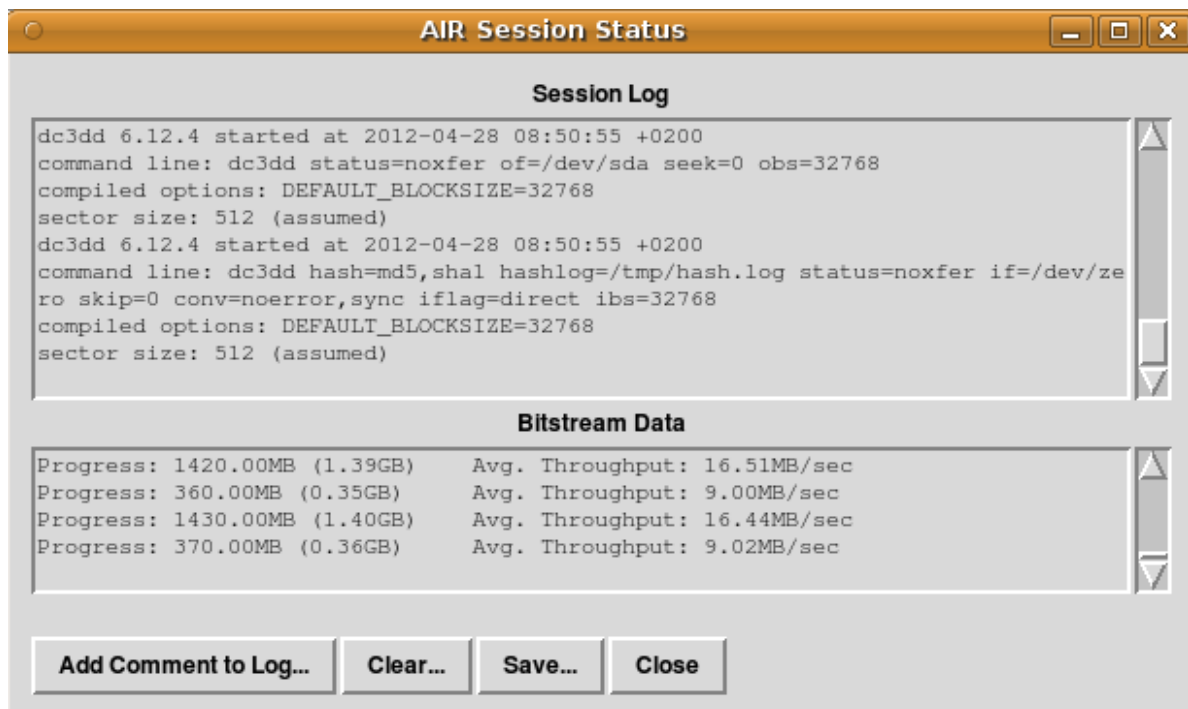


Imagen. 9.- Estado del proceso

El proceso mostrado de *Disk Wiping*, no debe confundirse con el de eliminación segura de información, del que se habla en otras ocasiones. Este último trata de garantizar la no recuperación de la información que hubiese estado alojada en un disco. Para ello se requiere de la realización de varias pasadas de bits de 1 y 0, asegurando de este modo que una información no será recuperable bajo ninguna circunstancia, ni siquiera haciendo uso de elementos hardware altamente especializados. En el caso del proceso de *Disk Wiping*, éste es más ligero, siendo sólo necesario realizar una pasada de bits 1.

Aunque el proceso de eliminación segura de información puede realizarse con *AIR*, resulta más aconsejable hacer uso de soluciones que han sido específicamente diseñadas con este propósito. Sirva de ejemplo el conjunto de aplicaciones *DBAN* (<http://www.dban.org/>), cuyo uso se encuentra ampliamente extendido a nivel mundial en diversidad de grandes empresas y organizaciones para la realización de este tipo de acciones de borrado seguro de información.

Una aplicación para el tratamiento de discos aparentemente más simple, al menos es lo que a su aspecto se refiere, es *Guymager*. Esta forma parte de la suite *CAINE*, mencionada ya en repetidas ocasiones en esta publicación, y aporta también la funcionalidad de adquirir y clonar discos mediante una interface realmente sencilla de manejar.

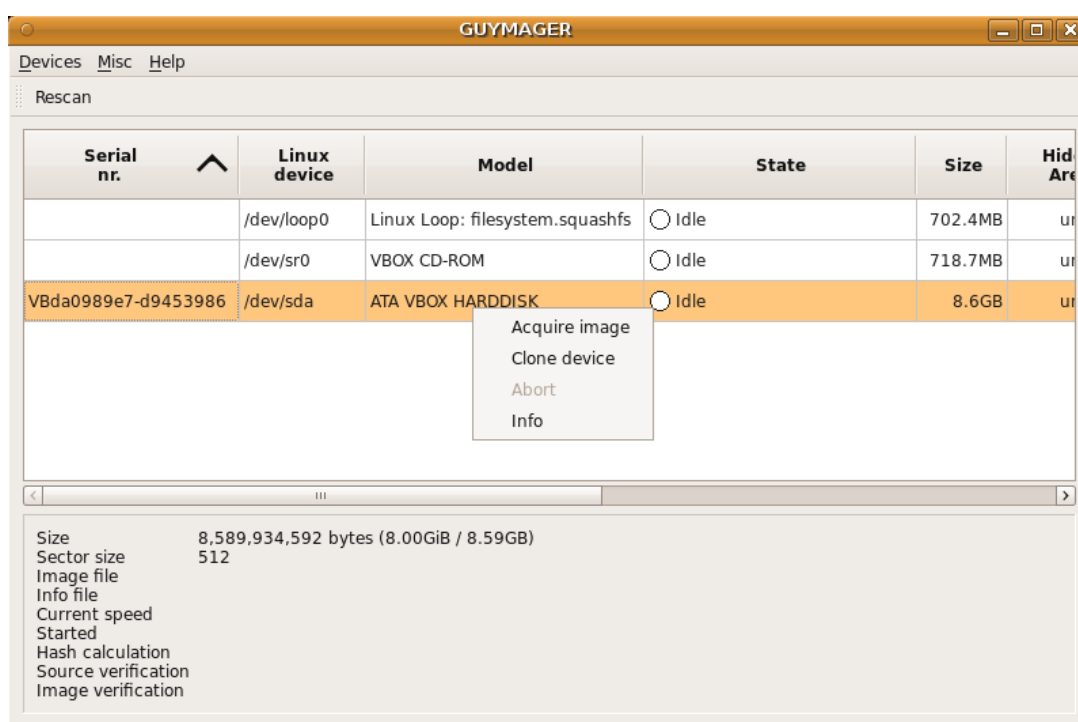


Imagen. 10.- Guymager

Sin embargo la aparente sencillez no debe asociarse necesariamente a la falta de potencia o efectividad. Al seleccionar la opción “Adquirir imagen o clonar dispositivo” será posible introducir un gran número de parámetros y seleccionar diversidad de opciones para la realización del proceso en unas determinadas condiciones. Esto amplía considerablemente las capacidades de la aplicación, haciéndola mucho más versátil que las anteriormente citadas.

La siguiente figura muestra las opciones que la herramienta *Guymager* aporta para la adquisición del fichero imagen. Son varias las posibilidades. No sólo mediante la función *dd*, tal y como se ha mostrado hasta ahora, sino también generando un fichero de formato

nativo utilizado por software de análisis forense, *Encase*. De igual modo, será posible suministrar a la evidencia información relevante para su identificación, incluyendo datos asociados al caso objeto de investigación o al analista responsable de la operación.

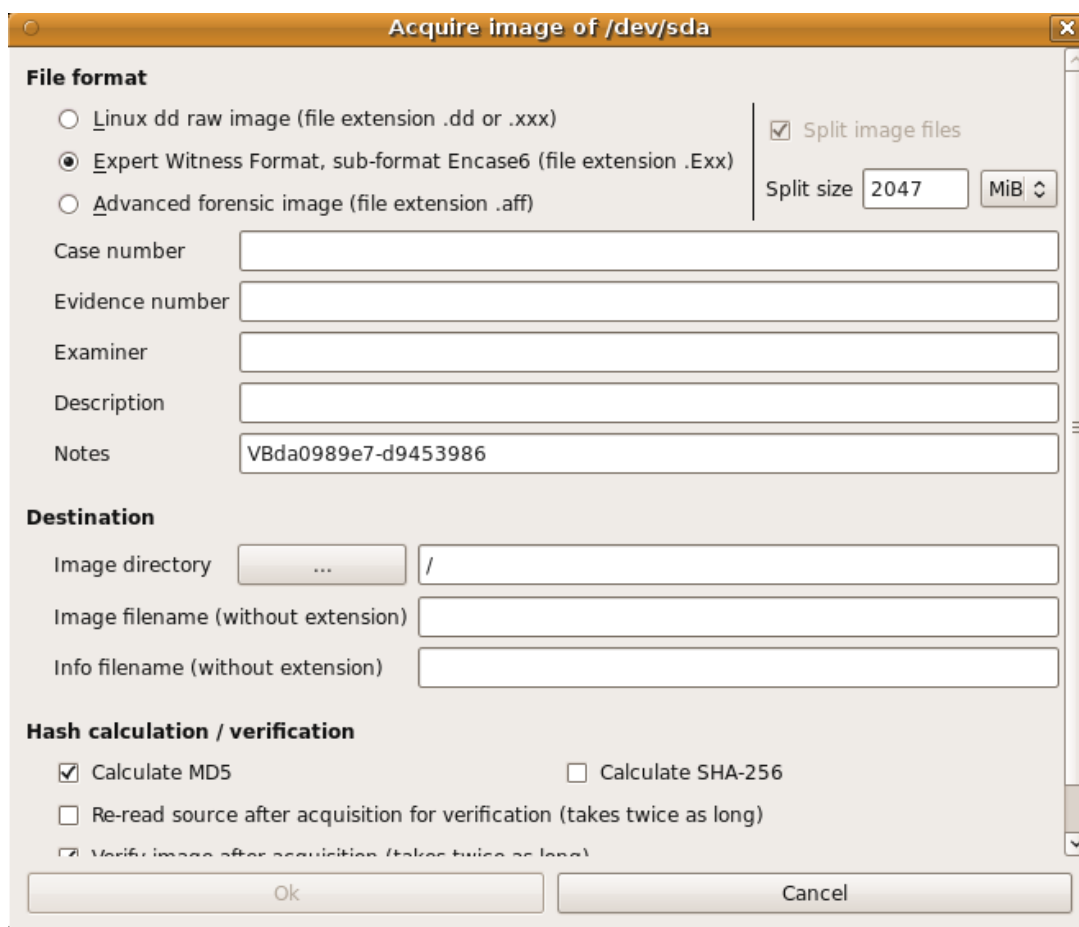


Imagen. 11.- Adquisición de discos

Se ha mostrado en este capítulo la importancia de una correcta adquisición de evidencias, así como algunas de las metodologías para llevarla a efecto. Evidentemente, son múltiples las posibilidades válidas. Sin embargo es crítico para el buen desarrollo de la investigación que en todos los casos la “higiene de las pruebas” sea la máxima observada por el procedimiento utilizado.

Es necesario dar al proceso de copiado de evidencias el tempo adecuado. A pesar de la presión externa y circunstancial de la investigación, que los afectados pueden incluso incrementar, el analista debe ser coherente con su labor profesional, valorando cada aspecto con rigor y siendo consecuente con la responsabilidad que adquiere. En las operaciones de copiado es la persona clave que dispone del conocimiento, especialización y capacitación necesaria. Debe por lo tanto, abstraerse de cualquier presión externa, que con objeto de acelerar los procesos, pueda influir negativamente en el rigor de la operación.

Capítulo 4 – La cadena de custodia

Ha quedado claro en los capítulos anteriores que el fundamento para llegar a un proceso judicial en una buena posición como perito, es garantizar la consistencia de las evidencias digitales adquiridas. Desde un punto de vista formal esto se consigue mediante la utilización de un procedimiento válido que garantice la no alteración de las pruebas. En esta misma línea, la posterior custodia rigurosa y documentada de las evidencias será otro aspecto que afianzará la garantía de no alteración, crítica para el proceso. En este cuarto capítulo se aportará información relacionada con este aspecto.

No existe en España una regulación específica para proceder y garantizar la custodia de pruebas, aunque sí en otros países del ámbito europeo. Sin embargo, se prevé de forma inminente la aparición de la norma que regulará y garantizará la custodia de las pruebas policiales. El encargado de su elaboración ha sido el Instituto Universitario de Investigación en Ciencias Policiales. Actualmente existen protocolos internos pero no unificados. Esta norma deberá tenerse en consideración para las diferentes unidades de cuerpos de seguridad del estado. Sin embargo aunque puede ser tomada como referencia, no afectará a aquellos análisis y peritajes que sean realizados en el ámbito privado.

Sin embargo, aunque no exista 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 asegura en cualquier investigación, sea o no informática, que las pruebas aportadas y las conclusiones a las que se llega partiendo de las evidencias, son consistentes y válidas, no habiendo sido alteradas para ningún fin con posterioridad al momento de su adquisición.

A lo largo de la investigación es necesaria la cesión tanto de las evidencias como de las copias garantizadas de las mismas, fundamentalmente entre distintos peritos, pero también entre personas u organizaciones involucradas en el proceso. Sobre ellos recaerá en cada momento el compromiso de mantenimiento de las pruebas. Es por ello que la cadena de custodia debe recoger en todo momento: ¿quién es el depositario?, ¿durante qué espacio temporal lo es? y ¿cuál es la razón por la que la evidencia queda bajo su custodia?

La cadena de custodia permite identificar con claridad quién ha estado en posesión de las evidencias antes de que éstas sean utilizadas en instancias judiciales, permitiendo que cualquier depositario de las mismas pueda ser citado judicialmente si las evidencias

quedaran en entredicho durante el proceso. Este hecho atiende habitualmente a posibles errores respecto de los procedimientos utilizados durante el peritaje.

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 un procedimiento fundamental que permite 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.

Teniendo en consideración lo anterior, es necesario incorporar un fichero de cadena de custodia para cada evidencia existente. En el caso de los procedimientos que se llevan a cabo en Sidertia Solutions, compañía en la que desarrollo mi labor profesional, también las copias adquiridas se acompañan de su correspondiente fichero para dar mayor consistencia a la investigación.

De este modo, cuando un analista recibe un disco previamente copiado del original, para a su vez realizar otra copia que le permita efectuar acciones de análisis de datos deberá proceder también a formalizar el fichero de cadena de custodia correspondiente. Gracias a ello, será posible también tener identificada y controlada la copia de trabajo generada, que contiene la misma información que será tratada como evidencia en el juicio.

No es posible mencionar la existencia de un único modelo de fichero de cadena de custodia homologado y de uso generalizado. Es posible localizar en la red diversidad de formularios que pueden ser válidos. En otras ocasiones son las propias herramientas de adquisición de evidencias las que proporcionan sus propios modelos. Pero incluso es factible la generación del fichero de forma manual si este recoge la información necesaria. Haciendo uso de

cualquiera de las posibilidades mencionadas, lo importante es contar con algún archivo de cadena de custodia asociado a la evidencia y que contenga la información de identificación imprescindible.

A continuación se muestra el formulario generado por la herramienta *Adepto*, que ha sido objeto de análisis en capítulos anteriores de este documento.

The screenshot displays the 'Adepto 2.0 (To Obtain, Get, Acquire)' application window. The 'Chain of Custody' menu item is selected, opening a form titled 'EVIDENCE CHAIN OF CUSTODY FORM - FOR FORENSIC IMAGES'. The form is divided into several sections:

- Case Information:** 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: dcfldd	Image: hda-img.dd
Storage Drive:	Hash:	Segments: 1	


At the bottom right of the form area is a 'Create PDF...' button. Below the form is a 'Progress' bar and a 'Quit' button. A status bar at the very bottom reads: 'These items will be printed on the Custody Form'.

Imagen. 12.- Funcionalidad de cadena de custodia

Haciendo uso de la funcionalidad que aporta el módulo de cadena de custodia en *Adepto*, es posible generar un fichero PDF conteniendo la información correspondiente al procedimiento realizado y que permitirá acompañar a la prueba desde su adquisición.

La siguiente imagen permite apreciar el archivo generado por *Adepto* tras la operación de adquisición del disco. En él se incorporan los datos que dan validez al procedimiento y que

han sido proporcionados al iniciar la herramienta. De igual modo, se adjunta de forma automática información 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:	HASH:			

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 de Adepto.

Una vez generado el fichero de cadena de custodia, éste debe acompañar siempre a la propia evidencia. La transferencia de la misma de un perito a otro, conlleva el cambio de la custodia y por lo tanto también la actualización y traspaso del fichero. Para su formalización deben suministrarse los datos requeridos, incluyendo el motivo por el que se realiza la transferencia de la evidencia. No es inusual que un profesional sea el encargado de realizar la adquisición, mientras que el proceso de análisis de las pruebas es realizado por un segundo analista.

El fichero de cadena de custodia no implica en esencia más que un formalismo, pero como tal es parte esencial del proceso. Es posible que nunca sea requerido en el proceso judicial, pero en algún caso puede ser crítico para afrontar las dudas y desconfianzas sobre las pruebas que alguna de las partes puede intentar fomentar en su beneficio.

Capítulo 5 – Las buenas prácticas en el análisis.

Llegados a este punto, el analista cuenta con las evidencias del caso, que además han debido ser recogidas a través de los procedimientos y buenas prácticas comentadas en capítulos anteriores. Ha llegado pues el momento de iniciar el análisis propiamente dicho. No es objetivo de este manual realizar un exhaustivo estudio de cómo analizar evidencias digitales. Este aspecto daría lugar a un estudio de mayor calado técnico y cuyo contenido sería indudablemente más extenso. Sí se pretende sin embargo ofrecer toda una serie de buenas prácticas y consideraciones generales, que permitan, teniéndolas en consideración, la obtención de unos correctos resultados en el proceso de análisis.

Evidentemente será necesario valorar que cada escenario presenta sus peculiaridades y no todos pueden analizarse de la misma forma. Las diferencias son significativas de unas situaciones a otras. Poco tiene que ver un caso donde es necesario localizar en un equipo una conversación mantenida a través de Messenger, con otros donde existen indicios de accesos ilícitos a cuentas de correo electrónico corporativo o donde se intenta detectar la posible acción de aplicaciones maliciosas en un caso de espionaje industrial. Los posibles ejemplos objeto de análisis pericial y sus diferencias podrían completar un listado interminable.

¿Porqué no decirlo? El término “forense” conlleva un cierto aire de misterio que puede resultar atractivo. Se asocia a la idea de investigación y descubrimiento y esto también ocurre en el ámbito de la informática. Sin embargo, en la mayoría de las ocasiones, las tareas de análisis no resultan nada edificantes, sino más bien todo lo contrario. Pueden incluso llegar a ser tediosas y requieren de un gran esfuerzo personal para no caer en la desidia. Muchos de los casos forenses que finalizan en un proceso judicial, demandan como tareas fundamentales el análisis de interminables log (registros de actividad) o la búsqueda de cadenas de caracteres entre el gran volumen de ficheros que pueden estar alojados en un determinado servidor o equipo de trabajo. Labores habitualmente poco gratificantes.

Es cierto que hay otros muchos tipos de actividades forenses más atractivas que las citadas anteriormente, sin embargo es inusual que las investigaciones basadas exclusivamente en estas técnicas deriven en un juicio. Los casos relacionados con aplicaciones maliciosas, los análisis de memoria, el descubrimiento de técnicas antiforenses o de ocultación (esteganografía) son algunos ejemplos de los muchos posibles. No debe obviarse que la

información y conclusiones a las que el perito debe llegar tienen que ser rotundas y difícilmente refutables y éstas interesantes técnicas no suelen aportar el nivel de certeza requerido.

Frente a lo anterior, lo habitual es que sean aquellas investigaciones donde sea necesario analizar correos, ficheros de registros o ficheros de datos los que terminen en un proceso judicial. En definitiva hay que hablar de interpretaciones, ante lo cual serán los datos más simples y asequibles, alejados de complejos planteamientos técnicos los más útiles para la labor tanto de peritos como abogados.

Frente a lo anterior, lo habitual es que sean los procedimientos de análisis de correos, logs o ficheros los que aporten datos de valor para una investigación que tenga un fin judicial. En definitiva estamos hablando de interpretaciones, ante lo cual serán los datos más simples y asequibles, alejados de complejos planteamientos técnicos los más útiles para la labor tanto de peritos como abogados.

Planteemos un ejemplo ilustrativo de lo anterior, la necesidad de 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. Además dicha manipulación se produjo por la instalación de una aplicación que aunque en el registro del sistema aparezca realizada por el usuario demandante, se estima que en realidad fue llevada a efecto por el demandado, mediante una intrusión en el sistema a través de una vulnerabilidad en la máquina virtual de Java del equipo del demandante. Como es fácil deducir la posibilidad de transmitir esta información a un juez es una labor casi imposible.

Regularmente, y más en la coyuntura económica actual, son muchos los casos relacionados con despidos que buscan una causa justificada que los convierta en procedentes. De igual modo la gran competitividad hace que sean numerosas las investigaciones por espionaje industrial o robo de propiedad intelectual. Pues bien, este tipo de casos se resuelven habitualmente escarbando entre los registros de los sistemas o en ficheros de datos.

En la actualidad, los casos de investigación forense suelen presentar desde sus inicios objetivos concretos. No suelen ser habituales los análisis realizados en función de la posibilidad de estar afectado por una aplicación maliciosa o sospechas similares poco definidas. Cuando se adopta la decisión de iniciar un proceso, que además puede desembocar en un juicio, es porque existe una clara sospecha o al menos indicios razonables como punto de partida de la investigación. Los análisis realizados con ausencia de objetivos concretos, además de ser más complejos y costosos en el tiempo, suelen dar resultados poco tangibles y en muchas ocasiones incluso denotan falta de coherencia en la sospecha.

Adicionalmente estos resultados finales no suelen satisfacer al cliente, que ha visto “fantasmas donde no los hay”, y que no es inusual que ante ello presente dificultades para abonar los servicios prestados.

En el momento de afrontar el análisis de evidencias, deberán tenerse en consideración una serie de criterios y obtener del cliente unos datos fundamentales para la investigación:

- Definición de la línea temporal. Es crítico en cualquier análisis definir tiempos, tanto para acotar temporalmente la investigación como para definir las conclusiones siguiendo para ello patrones claramente definidos. Muchas de las conclusiones a las que se puede llegar se apoyarán en información de fechas y horas.
- Búsqueda de elementos o palabras clave. En ocasiones los indicios no estarán definidos con claridad, pero resulta totalmente indispensable tener una orientación respecto de qué buscar. Un nombre, una web o una dirección de correo suelen ser datos que el cliente puede llegar a facilitar y que suponen un buen punto de origen para desarrollar el análisis. Sin estos datos es realmente complicado realizar una investigación rápida y fructífera.
- ¿Quién es quién? Es vital conocer los máximos datos posibles de las personas involucradas. Usuarios afectados, direcciones, teléfonos, etc., son elementos que en determinados escenarios son determinantes. A veces en la búsqueda de conversaciones almacenadas en un equipo no aparecen nombres directamente pero sí “alias” de las personas involucradas. Definir un cuadro relacional puede resultar esclarecedor en este tipo de circunstancias. No sería el primer caso en el que tras una investigación pueden salir a la luz relaciones personales, incluso sentimentales, desconocidas hasta el momento por la persona u organización que había solicitado la investigación.

El analista en su labor de investigación debe tener en todo momento amplitud de miras y evitar la posible pérdida de evidencias por haber circunscrito la investigación al marco operativo e indicios originales exclusivamente. Nunca debería descartarse la posibilidad de incorporar nuevas evidencias a un escenario. Cuando la existencia de un caso pasa a ser pública de forma inevitable ante acciones que no pueden efectuarse con discreción, como son la retirada de un ordenador o la comunicación a los investigados, es habitual la eliminación de evidencias por parte de los afectados. En este sentido y en la medida de lo posible, es importante haber sido previsor, planteando al cliente una estrategia de adquisición de evidencias de mayor alcance del que podría considerarse inicialmente. Es por ello que ante la existencia de algún tipo de sospecha, aunque no totalmente fundada sobre una persona, debería procederse a clonar el disco de su equipo desde el momento inicial. De

este modo si en el desarrollo la investigación fuese necesario, sería posible realizar un análisis posterior del disco recogido.

No debe olvidarse que este aspecto puede resultar especialmente conflictivo. Poner en guardia o crear supuestos sospechosos de personas que a larga pudieran no estar involucrados en el caso, genera una desestabilidad palpable en el ambiente laboral. Situación nada deseable en ninguna organización. Por ello, es importante desde un primer momento valorar con el cliente las prioridades, definiendo hasta que punto la correcta adquisición y preservación de las evidencias prevalece sobre el resto de circunstancias.

A la hora de analizar un disco, las búsquedas realizadas sobre el mismo deben ser exhaustivas, incluyendo la localización de información que inicialmente podría parecer inexistente. Mas allá de los escenarios donde se han implementado técnicas antiforenses, muchos casos requieren de la recuperación de ficheros eliminados. No es inusual que el “sospechoso” haya podido tener la precaución de eliminar ficheros o datos que puedan ser contraproducentes para él. Incluso, si dispone de las capacidades para ello, puede que la eliminación de información haya sido irreversible.

La recuperación de ficheros eliminados es una tarea que implica mucho tiempo y a veces los resultados no son positivos o difíciles de gestionar para fines judiciales. A pesar de ello, su recuperación puede aportar al menos indicios importantes para la línea de investigación. Medio fichero es mejor que nada. Herramientas forenses tales como *EnCase* o *FTK (Forensic ToolKit)*, cuentan con módulos para realizar búsquedas de ficheros eliminados y sobre ellos poder localizar palabras o frases clave. La dificultad aquí estriba en hacer creíble la prueba de cara al juicio.

Otro aspecto fundamental en la fase de análisis de muchos casos forenses, es la detección de patrones de conducta más o menos definidos. 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, representan ejemplos de patrones que pueden ser fáciles de rastrear. En un caso abordado recientemente, una cuenta 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 válidos, aunque totalmente diferentes (dominio\usuario y usuario@dominio).

Analizar patrones, a priori puede resultar algo complejo, sin embargo haciendo uso de tablas de relación adecuadas esta labor puede ser un potente instrumento. A nadie se le exige tener la mente analítica, relacional y obsesiva del matemático y economista John Forbes Nash que inspiró la novela y posteriormente la película “Una mente maravillosa”. Sin

embargo, sí es interesante para un forense disponer de ciertas capacidades de razonamiento analítico. Son muchos los casos en los que gracias a ellas, salen a la luz determinados patrones que dan pie en la elaboración de conclusiones bien fundamentadas. Por otra parte, la experiencia muestra que convenientemente introducidas en el juicio, los patrones de comportamiento constituyen un elemento esencial para poder conducir de forma efectiva las alegaciones y conclusiones que se presentan ante el Juez.

Es interesante contrastar los patrones obtenidos con el cliente. En ocasiones se llegará a apreciaciones realmente valiosas para la investigación. Pongamos un sencillo ejemplo de esta afirmación. En un determinado escenario laboral, todos los días se producen determinadas conexiones a recursos corporativos desde un mismo equipo. Sin embargo en determinadas fechas de la línea temporal de investigación puede observarse que esto no sucede así, lo cuál hace sospechar que en esos días la persona que opera desde el equipo en cuestión no desarrolló su labor habitual. Tras contrastar con la organización la inexistencia en esos días de alguna cuestión que justifique estas excepciones, es evidente que en las fechas señaladas sucedió algo “distinto a lo habitual” y que puede ser sintomático de los comportamientos anómalos que la investigación intenta localizar. Estos datos podrán ser introducidos en el informe como parte esencial de las conclusiones derivadas. No obstante hay que matizar que un informe pericial nunca puede encontrarse condicionado por el cliente y mucho menos, parcial o totalmente, elaborado por él. Será tarea del analista solicitar determinada información y por lo tanto atendiendo a su criterio como perito introducirla en el informe en un término u otro.

Este contraste de información con el cliente puede aportar valor a la investigación en algún otro sentido además del ya indicado. Retomemos el escenario anterior para ilustrar esta afirmación y pongámonos en la situación de que a diferencia de lo expuesto, el cambio en el patrón de comportamiento del profesional investigado en determinadas fechas sí responde a causas justificadas, como pueden ser visitas médicas. El analista dispone de esta información tras su comunicación con la organización cliente. Estos resultados por lo tanto afianzan la veracidad de las evidencias utilizadas, puesto que los resultados obtenidos por el investigador no eran conocidos por él de antemano y sin embargo se ha detectado claramente un cambio en el patrón de comportamiento habitual, a pesar de estar en este caso totalmente justificado.

Aprovéchese este breve ejemplo para recalcar que en cualquier caso el analista tendrá que ser muy cuidadoso con el tratamiento de aquellos datos que puedan resultar invasivos de la intimidad de las personas afectadas, pudiendo tener con ello consecuencias nada deseables

ante una posible violación de la intimidad o de los datos personales de las personas objeto de investigación.

Evidentemente es crítico ser extremadamente escrupuloso en la realización del análisis e inevitablemente esto implica ser organizado. Hay que tener claro desde el principio cuales son los objetivos sin desdeñar por ello alternativas. Si eres caótico saltarás desde una pista a otra sin una clara visión y esto se reflejará indefectiblemente sobre el informe resultante de la labor de peritaje. Es importante anotar cualquier apreciación relativa a información obtenida directamente o a partir del cruce de resultados. No hay que confiar nunca en las capacidades de memoria personales, puesto que ante la avalancha de información es posible la pérdida de detalles relevantes. Es una buena práctica llevar un cuaderno de bitácora donde anotar cualquier apreciación, evidencia, horas, fechas, nombres o cualquier dato o impresión que pueda considerarse de interés.

Las herramientas son elementos fundamentales para el desarrollo de tareas de 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 no utilizadas de forma adecuada serán de escasa o nula utilidad. La experiencia ha mostrado lo potentes que pueden llegar a ser aplicaciones sencillas utilizadas por manos expertas. No existen varitas ni teclas mágicas para afrontar en un caso la fase de análisis. Cada uno de ellas presenta sus peculiaridades y es muy importante desprenderse desde un principio de prejuicios y conclusiones preconcebidas. El asesino no siempre es el mayordomo. No debe olvidarse tampoco, que en ocasiones la visión profesional de un tercero puede dar aire fresco a la investigación en momentos de bloqueo de ésta.

Capítulo 6 – El informe pericial

El informe pericial constituye, sino el más importante, uno de los elementos esenciales en un caso forense. En definitiva es el único lugar donde se recoge el resultado y la información de todo el proceso. 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 un proyecto de auditoría, el valor del trabajo reside en el documento y será éste el elemento de juicio fundamental respecto de la labor del analista forense.

Un informe de estas características presenta sus peculiaridades y hay que tener presente que aunque la carga técnica resulta importante, su objetivo final es transmitir información a personas que en muchas ocasiones no tienen una relación directa con la informática. Son meros usuarios tecnológicos. Por lo tanto, sin desdeñar los datos técnicos fundamento de la investigación, el profesional que lo realiza debe tener en consideración en todo momento a quién va dirigido, siendo para él un reto hacerlo inteligible a estas personas, sin que ello implique una pérdida de rigor en la información presentada. Obviamente, será necesario evitar la tentación de que el informe sea una muestra de las amplias capacidades informáticas del perito. Evidentemente no es éste su objetivo.

Un informe pericial ininteligible pierde todo su valor de cara al juicio. Es más, el propio abogado tendrá complicada su intervención en el proceso judicial si no es capaz de conocer y comprender la información esencial contenida en él. Para un neófito en informática, comprender aspectos tan básicos como el concepto de dirección IP, puede suponer un problema. En la elaboración del informe pericial, el analista deberá aplicar en ocasiones una cierta dosis de pedagogía para facilitar su comprensión.

Es necesario tener presente en la elaboración de este documento final del peritaje la condición de independencia del perito. Aunque existirá una tendencia inevitable a reflejar cierta parcialidad en las conclusiones, ésta no debe condicionar la elaboración del informe, que en ningún caso debe recoger otra información que no sea la realidad de los resultados obtenidos en la investigación.

Un informe debe presentar una línea maestra bien definida. No pueden plantearse unos objetivos de inicio y que sin embargo en el desarrollo del informe pericial la información recogida se dirija a otras cuestiones no asociables a su resolución. Es necesario ser

consecuente y evitar en todo término que el informe presente hilos sueltos o cuestiones no resueltas adecuadamente. Este hecho podría arrojar dudas sobre la validez de la totalidad del documento.

El informe forense debe atender a un tempo en su desarrollo, que se vea articulado a través de una estructura de documento claramente definida. En este sentido, pueden ser varias los modelos y apartados incorporados en el informe. Una posible estructura válida puede ser la que se presenta a continuación:

- Antecedentes.
- Evidencias.
- Análisis y tratamiento.
- Resultados.
- Conclusiones y recomendaciones.

Los antecedentes suponen la mejor forma para iniciar el informe. Estos deben recoger tanto los objetivos del caso forense, como las reuniones e informaciones iniciales suministradas al analista. 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 resuelto, en un sentido o en otro. Es importante también exponer a través de los antecedentes las líneas temporales que el análisis debe observar y en que medida se relacionan con el caso.

Como ya se indicó en repetidas ocasiones en capítulos anteriores, el segundo de los apartados es realmente crítico. Se trata de la presentación de las evidencias digitales asociadas al caso. Hay que recordar que son el elemento fundamental del trabajo de investigación y por lo tanto de la posterior elaboración del informe. Su identificación, recogida y almacenamiento son determinantes para esta tarea documental. Los procedimientos empleados deben reflejarse con claridad, garantizando siempre que se han llevado a efecto las buenas prácticas necesarias, evitando cualquier manipulación o alteración de las evidencias

Es muy recomendable que las evidencias aparezcan enumeradas en el informe, facilitando además sobre ellas toda la información posible: cuál es su origen y cuál la motivación de su obtención, cómo han sido tratadas, qué cantidad de copias se han realizado de las mismas, quién las ha recogido, almacenado y analizado y cualquier otra información disponible que el analista considere oportuno incorporar en el informe. Sería importante definir también en el

informe, cuando sea factible, los fundamentos existentes que demuestren la no manipulación de las pruebas. Por ejemplo a través de la firma tomada de las mismas.

Ante la existencia en un determinado caso de evidencias delicadas en lo concerniente a su modo de adquisición, es recomendable motivar en el informe el porqué de la metodología empleada, ahondando en las precauciones que se han tomado y su importancia con respecto al caso. Si determinadas evidencias han sido adquiridas una vez iniciada la investigación, deberá también indicarse esta circunstancia, así como el motivo que la provoca. Un escenario ilustrativo de esto sería aquel en que tras unas pruebas iniciales se detectan indicios de una conversación mantenida desde un determinado equipo. En consecuencia, se procede a realizar un análisis del mismo adquiriendo para ello su disco duro.

Los resultados y conclusiones deberán derivarse en todo momento de las evidencias presentadas. Aquellas afirmaciones que figuren en el informe sin un sustento en las evidencias, serán tomadas como una 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 se afianza siempre esta posición.

El tratamiento de las evidencias digitales adquiridas es el siguiente punto que el informe pericial debe recoger. El análisis de las mismas proporcionará datos a partir de los cuales se puedan establecer relaciones que a su vez deriven en conclusiones. El factor fundamental para la exposición de éstas debe ser el de causa-efecto. Es interesante atender en este sentido al "principio de intercambios" formulado por Locard, que aunque aplicable fundamentalmente a indicios y evidencias físicas, puede ser tenido en consideración también para las de tipo digital. Este principio afirma que "siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto".

En el caso de que el analista detecte la existencia de patrones de comportamiento, éstos 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 reflejará en gran medida en el informe, produciendo unos resultados muy difíciles de consolidar e hilvanar.

El informe pericial en su apartado de análisis debe ir proporcionando paulatinamente los resultados, dosificándolos en su justa medida y preparando con ello los elementos finales del documento. Por otra parte, será este apartado el que habitualmente se encuentre más cargado de tecnicismos. En muchas ocasiones, esta circunstancia es interesante contrarrestarla con la generación de un anexo, en forma de glosario de términos, que facilite

la comprensión del informe, haciéndolo más asequible a posibles lectores que no dispongan de una base de conocimientos informáticos suficiente.

También deben ser presentados como anexos aquellos resultados del análisis que siendo importantes puedan ser repetitivos en exceso, provocando con ello una pérdida de efectividad en la presentación del informe pericial. Un ejemplo de ello pueden ser los resultados obtenidos del análisis de múltiples logs y que es recomendable que se condensen en una serie de tablas descriptivas en este apartado del informe. Adicionalmente, toda la información tratada puede recogerse en un anexo que sea referenciado en el documento. No debe olvidarse que en ocasiones el exceso de información puede desembocar en desinformación o falta de claridad.

Siempre que sea necesaria, podrá establecerse la correlación existente entre los distintos análisis. Sin embargo no es recomendable anticiparse con ello a las conclusiones. En caso de considerarse importante adelantar en este apartado alguna información o relación concluyente, ésta deberá volverse a exponer en las conclusiones, aunque pueda parecer reiterativo. Es factible que determinadas personas, especialmente aquellas con un perfil menos técnico, sólo revisen los resultados y conclusiones del documento.

La información de análisis recogida en el informe debe reflejar la pericia del investigador como factor determinante. También la eficacia de los métodos y aplicaciones empleadas, pero siempre dando paso a la labor pericial como elemento fundamental. Esto en España es aún más acusado dado que no existen herramientas homologadas, ni claro está aquellas cuyo empleo garantice un éxito de cara al juicio.

La exposición de resultados es una continuación de la fase documental de análisis. Aquí se define y presenta toda la información obtenida y que puede ser relevante para el caso. Aunque la correlación de datos es una más propia de las conclusiones, en este apartado del informe inevitablemente se irá adelantando información en este sentido.

Sin embargo, 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. El perito debe tener en consideración todos ellos, sean o no favorables, obligando fundamentalmente por su condición profesional de imparcialidad, pero también valorando la posible ejecución de una investigación contrapericial.

En la medida de lo posible, la presentación de resultados debe ser acorde a la línea temporal definida en los antecedentes y que junto con otros elementos muestra 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.

Las conclusiones son uno de los apartados finales del informe, sin embargo muy probablemente será el punto que se lea en primera instancia. Incluso puede darse el caso de que en aquellos documentos especialmente voluminosos se presenten como uno de los apartados iniciales, a modo de informe ejecutivo.

La labor del analista, fundamental en la elaboración de cualquier elemento del informe, es especialmente determinante a la hora de elaborar las conclusiones. Es en este punto donde, independientemente de las metodologías o herramientas utilizadas, será la experiencia, el buen hacer o la capacidad de análisis y síntesis del analista los factores críticos en el establecimiento de las conclusiones del proceso de investigación.

La importancia del apartado de conclusiones respecto de la toma de decisiones en cada caso es absoluta. Es a partir de este punto principalmente desde el que se adoptará la decisión final de considerar a los implicados como inocentes o por el contrario pasar a iniciar una acción judicial. Es el momento de reflejar relaciones, de presentar las pruebas en toda su crudeza, de defender los patrones detectados que indican conductas maliciosas reiteradas, condicionando con ello la gravedad final de las acciones. No debe olvidarse que para las empresas y organizaciones no será lo mismo la detección de un hecho aislado que una conducta maliciosa reiterativa. Por todo lo anterior, es recomendable que el analista se abstraiga de las circunstancias externas del caso, olvidándose de las consecuencias posteriores que las conclusiones de su labor pueden acarrear.

En definitiva, las conclusiones son la síntesis y el desenlace del caso. Un mayor número de ellas no implica necesariamente un mejor trabajo. En ocasiones la exposición de datos inconexos y faltos de sentido puede distraer al lector del informe de las conclusiones principales, resultando con ello negativo de cara al juicio y facilitando, por su falta de concreción, la posibilidad de desmontar la labor pericial realizada. Pocos argumentos y bien planteados serán mejores que un mayor número de ellos pero desdibujados.

Adicionalmente a los anexos que cada informe forense demande en función de las líneas de investigación desarrolladas, es muy recomendable que en el documento figure un anexo específico que recoja la pericia, experiencia y capacitación del perito. Con ello se reforzará la veracidad, profesionalidad y valor de la información recogida en el informe. Hay que tener presente que quién suscriba el documento pericial se encuentra obligado, si fuese necesario, a prestar declaración en el juicio en calidad de testigo pericial.

Un informe pericial forense podría recoger en su contenido la necesidad de disponer de información que no era inicialmente demandada y cuya obtención posterior podría ser positiva para el esclarecimiento del caso. Debe existir para ello, una causa que lo justifique y que haya podido surgir en el propio desarrollo de la investigación. Un ejemplo clarificador de

esta circunstancia puede ser la aparición de IP públicas, cuya identificación sólo se encuentra en posesión de los proveedores de Internet. No es objetivo del analista elucubrar sobre las posibilidades que pueden aportar estos datos, sino simplemente reflejar que gracias a ellos podría ser posible corroborar o ampliar de una u otra forma las conclusiones.

Para todos aquellos que tengan interés en disponer de un ejemplo de informe pericial de carácter “oficial”, en el siguiente enlace es posible acceder al elaborado por la Interpol sobre los ordenadores y equipos informáticos de las FARC decomisados en 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 irrelevantes dado que la información necesaria se encuentra en manos de un tercero, fuera del alcance del investigador. Un escenario ilustrativo de esto podría ser el mencionado en el capítulo anterior, relacionado con la aparición de direcciones IP públicas en los registros de actividad de un servidor investigado. En esta situación sólo el proveedor de servicios de Internet conoce a quién han podido ser adjudicadas estas direcciones en una fecha y hora concretas. En ocasiones la ausencia de esta información ha provocado que se desestimen evidencias ante la creencia de que no es posible su obtención.

La obtención de estos datos puede resultar totalmente determinante, permitiendo motivar un hecho o incriminar a una persona concreta en el proceso de investigación. Puesto que bajo ninguna circunstancia el analista tiene acceso a la información y elucubrar sobre posibilidades, aunque factible, no tiene validez en el juicio, será por lo tanto necesario solicitar la información.

En este sentido es importante tener en consideración la volatilidad de estos datos. El proveedor de Internet desechará los registros relativos a las conexiones de sus abonados con el paso del tiempo. Por ésta y otras razones, es una buena práctica agilizar todo lo posible su solicitud.

Este procedimiento se denomina solicitud de prueba anticipada. Su base se encuentra en la protección del derecho fundamental a la prueba. Dado que existe el riesgo de que una prueba pudiera no practicarse porque para ello es necesario esperar a que llegue la fase de procedimientos del juicio, es posible requerir el adelantamiento de la prueba. De este modo, 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 motivado y solicitado al tribunal que está llevando el caso siempre con anterioridad al inicio del juicio.

El escrito de solicitud es remitido por el abogado que llevará el caso ante el juzgado correspondiente, mediante una súplica de oficio. Es recomendable que el escrito sea revisado por el analista forense. Aunque está claro que el lenguaje judicial se encuentra

fuera del alcance del investigador, se hace necesario asesorar al abogado y evitar con ello incurrir en errores técnicos que hagan imposible atender a la súplica.

Adicionalmente a otras peticiones que puedan ser cursadas mediante este procedimiento, las de ámbito informático más habituales son las relacionadas con solicitud de datos de actividad a los proveedores de Internet y telefonía. Necesidades de información asociada a direcciones IP públicas o envíos de SMS, uso de dispositivos Smartphone o identificación de correos electrónicos, son algunas de las múltiples circunstancias que hacen necesaria la solicitud de información a un tercero.

El procedimiento de solicitud de prueba anticipada se ve favorecido si se acompaña del máximo de información posible, facilitando con ello su ejecución. Si por ejemplo, se solicita información de direcciones IP es recomendable que en la petición figure el proveedor o proveedores asociados a las mismas, además de la línea temporal de conexión claramente indicada. De esta forma la solicitud al juzgado puede ser encaminada de la forma correcta, facilitando además la labor de éste. En este sentido, es útil recordar las posibles discrepancias que pueden tener los ficheros de log, con las horas locales reales donde opera el proveedor correspondiente.

Un analista en el desarrollo de su labor de investigación debe huir en todo momento de ideas preconcebidas. Estas incluso pueden venir fomentadas ante la repetición habitual de un determinado patrón de comportamiento en el desarrollo del análisis. Sin embargo, cuando el patrón excepcionalmente deja de cumplirse, la duda sobre la validez de la evidencia puede surgir en el analista pudiendo llegar por ello incluso a desestimar la prueba.

Ilustremos este planteamiento con un posible caso. El analista identifica que el autor de los hechos se conecta a una misma hora y desde su casa regularmente. Por el contrario y de forma puntual en determinadas fechas, las conexiones realizadas en una misma franja horaria proceden de direcciones IP pertenecientes a distintos proveedores. Esta excepcionalidad respecto del patrón de comportamiento habitual, genera ciertas dudas en el analista sobre la validez de las evidencias. Esto evidentemente es un error de apreciación, producido fundamentalmente por presuponer que el investigado realiza siempre las conexiones desde su casa. Sin embargo se dan muchas circunstancias para que este hecho sea factible:

- Diferentes actores implicados.
- Un único actor operando desde distintas ubicaciones, por ejemplo desde su casa y la de un familiar o amigo.

- Un único actor utilizando diferentes tecnologías. Por ejemplo, uso de ADSL y smartphone por el que se conecta a través de su equipo, implicando con ello a diferentes proveedores.

Escenarios como los que se acaban de describir de forma somera en los puntos anteriores pueden aportar información de valor para la investigación. De todos modos, tal y como se ha indicado en párrafos anteriores, para llegar a conclusiones definitivas debe esperarse a la resolución de la prueba anticipada.

Este tipo de pruebas suelen ser determinantes en el desenlace de un juicio y por lo tanto hay que hacer todo lo factible para su obtención. 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 del caso, 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 lleguen a tiempo a la vista. El resultado obtenido de la solicitud de prueba anticipada puede llegar a condicionar totalmente la estrategia en el juicio

Capítulo 8 – Un juicio civil

Tras la labor realizada, llega el punto final y definitivo del proceso. Es necesario tener en consideración que aun habiéndose realizado una labor profesional de valor, cualquier investigación forense digital que desemboque en un juicio se dirimirá en éste de forma definitiva. Anteriormente, la empresa, organización o persona afectada habrá utilizado el informe pericial fruto de la investigación como elemento fundamental a la hora de adoptar decisiones, pero el resultado definitivo del peritaje se obtendrá al finalizar el proceso judicial.

Como paso previo a la vista, es necesario preparar junto a los abogados la estrategia que se va a adoptar para la misma. El perito aportará su perspectiva e importantes apreciaciones técnicas que pueden ser hilo conductor de las preguntas que el abogado le formulará en la vista. La preparación de ésta será también de utilidad para intentar anticiparse a las cuestiones que puedan plantearse por parte del abogado de la otra parte. Finalmente, su labor de asesoramiento técnico será también considerada para preparar la testificación de la parte contraria. Sin una preparación adecuada, incluso habiendo realizado una buena labor pericial, el juicio se puede convertir en una auténtica lotería. Una testificación ambigua, poco veraz, no sólo no aportará al desarrollo favorable del proceso judicial, sino que puede llegar a ser abiertamente contraproducente.

En un juicio civil, el abogado preparará una nota judicial que presentará en la vista y donde la información pericial tiene una importancia significativa. A modo de informe ejecutivo, en ella 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 deberá colaborar técnicamente en su elaboración.

El día de la vista el perito deberá asistir a la misma con la correspondiente documentación identificativa, DNI preferiblemente. Este quedará fuera, a la espera de ser llamado en calidad de testigo pericial. De esta forma y como cualquier otro testigo, se logra que se mantenga ajeno lo que está sucediendo en la vista, siendo por lo tanto y llegado el caso, su intervención mucho más objetiva. En un proceso convencional cada parte presentará sus testigos, participando en primer lugar los que presenta el demandado y en segundo los de la parte demandante.

Habitualmente y por cuestiones de estrategia de la parte que presenta el peritaje, el perito suele ser el último de los testigos en declarar, para centrar sobre su testimonio y labor de análisis las correspondientes conclusiones. Sin embargo, en ningún momento debe olvidarse su carácter totalmente imparcial y su deber de independencia.

Tras entrar en la sala, habiendo entregado previamente su documento identificativo, el juez se dirige al él, para identificarlo y comunicarle su deber de prestar la verdad y no dar falso testimonio. Hay que tener en consideración, que en caso de faltar a la verdad, el perito podría ser sancionado con pena de multa o incluso privación de libertad.

En la vista, se le hará entrega del informe pericial presentado como prueba, que deberá reconocer como suyo. Lo tendrá a su disposición para las aclaraciones o referencias a él que puedan ser necesarias, ante cualquier planteamiento que pudiera darse en las preguntas que se le formulen. En primer lugar será interrogado por el abogado de la parte por la que se presenta y en segunda instancia intervendrá la parte contraria. La intervención de ésta es fundamental puesto que habitualmente su estrategia será mermar la credibilidad del perito, su testimonio o el informe pericial presentado. Finalmente es el juez el que le planteará aquellas cuestiones que considere oportunas. La intervención del perito, debido a la relevancia de la información que aporta, se presenta siempre como una de los momentos críticos de la vista judicial y suele ser tenida en gran consideración por parte del juez.

Como ya se indicaba en el capítulo inicial de esta publicación, el informático que desarrolla labores de peritaje se encuentra en una vista judicial fuera de su espacio natural. Por regla general, ningún perito en sus primeras comparecencias suele estar preparado para la situación que debe afrontar. Mantenerse sereno, en la medida de lo posible, es la clave fundamental. Los nervios no permiten visualizar con claridad la situación, exponer las conclusiones de forma veraz, pudiendo incluso errar en las apreciaciones como consecuencia de la tensión del momento.

Los abogados sin embargo, se enfrentan a esta situación con la mayor de las normalidades posibles, están en su espacio profesional y lo controlan, por lo tanto debería dejárseles a ellos el manejar las situaciones.

Considerando lo anterior, es útil tener en consideración una serie de cuestiones relacionadas con la intervención del perito informático en la vista judicial:

- Del perito se espera que disponga de la capacidad para analizar los hechos y aportar su experiencia profesional. Esto difiere del resto de los testigos, dado que éstos sólo declaran en función de los hechos que conocen.

- Hay que estar preparado para las preguntas que pueda plantear la otra parte. No entrar bajo ninguna circunstancia en enfrentamientos, puesto que harían dudar del buen hacer y la imparcialidad pericial. Responder simplemente de forma profesional, sencilla y veraz. Por ello es importante valorar antes del inicio del juicio aquellas preguntas que pudiera formular la otra parte, anticipando así las respuestas y evitando con ello cometer errores o aparecer en la vista de forma dubitativa.
- Aunque un perito es requerido por su capacitación técnica, habitualmente el público al que se dirige no tiene este perfil y por lo tanto deberá ser comedido en la carga técnica de sus respuestas. Cuanto más sencilla y comprensible sea su exposición, mayor claridad aportará al juez para su toma de decisiones.
- A pesar de que muchas preguntas presentarán como objetivo respuestas simples de afirmación o negación, en todo momento podrán hacerse tantas consideraciones como se considere oportuno. En múltiples ocasiones, estas aclaraciones evitarán caer en aquellas “trampas” que pudiesen conllevar respuestas tajantes de sí o no.
- Ante una pregunta dudosa, es recomendable solicitar que se replantee de nuevo si no ha sido comprendida. Esto es siempre preferible a dar una respuesta rápida e inadecuada al no haber entendido correctamente la pregunta.
- Hay que tener presente que es posible suministrar como respuestas un “no recuerdo” o “no lo sé”. Como perito, no es exigible disponer de conocimientos sobre absolutamente todo, sino simplemente no faltar a la verdad.
- Hay que esperar preguntas o incluso afirmaciones que cuestionen el proceso de análisis pericial o las conclusiones emitidas en el informe. Ante todo profesionalidad, suministrando las aclaraciones necesarias para evitar la sensación de duda, pero nunca entrando en conflicto.
- Un aspecto clave suele ser el de las preguntas orientadas a poner en entredicho el tratamiento de las evidencias digitales. Si no existe otra posible defensa, la otra parte podría intentar en su estrategia desmontar la pericia, esgrimiendo para ello manipulación de las pruebas. Si los procedimientos han sido bien llevados, será solo un trámite que incluso podrá reafirmar el valor y la veracidad de la labor forense.
- Ante preguntas realizadas sobre el informe pericial, especialmente si hace tiempo que se realizó, es preferible acudir al mismo y volver a leerlo que dar una respuesta precipitada y contraria al propio documento.

Finalizado su testimonio, el perito podrá presenciar el resto del juicio, debiendo mantener en todo momento la compostura. En la exposición final de conclusiones, los abogados pueden proporcionar información contraria al informe pericial o intentar desvirtuar la actuación del perito en la práctica de las pruebas. A pesar de ello, debe mantenerse la calma en todo momento. Hay que tener en consideración la profesionalidad de los jueces, habituados a las estrategias de los abogados. Los juicios se graban, se dispone del informe pericial así como de toda la información aportada en el juicio como pueden ser las pruebas anticipadas. Todo ello ayudará al juez a emitir su sentencia. Finalizado el juicio y quedando visto para dictamen, todos los testigos, incluidos lógicamente los peritos, procederán a la firma correspondiente que ratifica sus testimonios.

Ahora no queda más que esperar un tiempo a que el juez emita su sentencia. No cabe duda que un juicio constituye una experiencia enriquecedora para cualquier analista forense digital. Ayuda de forma muy especial a comprender la importancia de los procedimientos. Mejora la forma y capacitación para entender y elaborar informes. Cuestiones que inicialmente se consideran muy importantes en los informes, pierden relevancia en el juicio y sin embargo, ocurre lo contrario con otros aspectos a los que originalmente no se les había dado mucha importancia.

Cada juicio es diferente y la intervención de cada profesional, juez, abogado o el propio perito hacen impredecible su resultado final. En ocasiones se pasará por la frustración de una sentencia contraria cuando todo estaba a favor. Pero es parte de un proceso donde en la mejor de las situaciones habrá un 99% de posibilidades de éxito, nunca la absoluta certeza de ello.

Capítulo 9 – Claves de un forense en juicio

Tal y como se ha mostrado en los capítulos anteriores, un analista forense debe seguir en su labor de investigación unos procesos muy concretos y en ocasiones complejos, siendo necesario en todo momento un alto nivel de rigor profesional en su desarrollo. Como ya se ha recogido en esta publicación, en España no existen fundamentos regulatorios para la realización de los procedimientos en unos términos concretos, sin embargo debe atenderse en su ejecución a una serie de buenas prácticas que garanticen, cuando se llega al proceso judicial, la confianza en unos hechos veraces, probables y reproducibles, basados en evidencias que en ningún momento han sido manipuladas.

Este último capítulo, se dedicará a repasar todo el procedimiento que permite defender con garantías un informe pericial en un juicio, así como otros aspectos importantes a tener en consideración dentro del ámbito legal. En definitiva se trata de recoger aquellos elementos fundamentales que se ha abordado en mayor detalle en capítulos anteriores:

- Paso I. Obtener información previa sobre el caso. Antes incluso de iniciar la recogida de evidencias, el analista debe ser conocedor de las circunstancias del escenario en el que se han desarrollado los hechos, así como disponer de la máxima información posible sobre ellos. Para esto es necesario acudir a todos aquellos que pudieran proporcionarla. La complejidad del escenario determinará también la cantidad de evidencias a recuperar y tratar. Cuanto mayor sea el volumen de información inicial obtenida, menor será el número de problemas posteriores derivados de la falta de datos o de la inconexión de los mismos.
- Paso II. Obtención de evidencias. Es determinante la recuperación rigurosa y la firma de las evidencias asociadas a cada caso, generando además los ficheros de cadena de custodia correspondientes. De forma especial en nuestro país, la no alteración bajo ningún concepto de las pruebas y la garantía por lo tanto de su valor pericial son la máxima fundamental a observar en los procesos de recuperación de evidencias. Este mismo concepto deberá regir el almacenamiento seguro de las pruebas recogidas que pudieran posteriormente ser utilizadas en un juicio.
- Paso III. Identificar datos relevantes y la línea temporal de la investigación. Es estratégico identificar los datos importantes en función de las circunstancias de cada caso: nombres, direcciones, correos, números de teléfono, ficheros, etc. Con ello se

facilitará la posibilidad de realizar búsquedas eficaces. De igual modo, debe definirse la línea temporal que se tendrá en consideración para el desarrollo de la investigación pericial. Esto permitirá articular una investigación basada en un proceso secuencial, manejable y que facilite la elaboración de un informe eficaz.

- Paso IV. Ordenar y relacionar los datos obtenidos a partir de las evidencias del caso. Teniendo siempre en consideración la garantía de independencia del perito y la incapacidad para ocultar cualquier dato aunque sea negativo para la parte por la que ha sido contratado. Las conclusiones deben exponerse sin ningún tipo de injerencias si el pericial quiere tener el valor que le corresponde en el juicio. No se debe despreciar tampoco la posibilidad de que pueda realizarse un contrapericial que destape datos que hayan podido ocultarse, con el consiguiente efecto negativo, tanto para la parte como para el propio perito.
- Paso V. Generación del informe pericial. El objetivo es 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. Como ya se ha expuesto en el capítulo correspondiente, un elemento muy importante del informe consiste en reflejar las garantías observadas en el proceso y que permiten dar absoluta veracidad a las evidencias.
- Paso VI. Práctica de prueba anticipada. Toda vez que el informe esté concluido y se tenga en consideración la posibilidad de llegar a juicio, se deberá aconsejar al abogado, la práctica de la prueba anticipada cuando las circunstancias así lo requieran.
- Paso VII. Asesoramiento técnico. Es necesario apoyar al abogado técnicamente en la estrategia a llevar en el juicio para la defensa de la labor e informe pericial, así como en la preparación de la nota que deberá presentarse para la vista. De igual modo, deberán definirse con antelación aquellas preguntas claves que permitan presentar las conclusiones del informe más importantes.
- Paso VIII. Intervención en la vista judicial. En el juicio, el perito desempeña un papel clave. La otra parte en todo momento intentará desmontar los argumentos técnicos que presente, pero también buscará desacreditar su figura, poniendo en duda su imparcialidad. Sabe que cualquier atisbo de duda en este sentido, provocará que pruebas e informes técnicos tengan menor relevancia sobre el veredicto final. La compostura será un punto esencial, no debiendo entrar en confrontación con la otra parte, aunque a veces conseguirlo resulte complicado. Y finalmente, si bien en el

informe pericial se presenta la necesidad de incorporar una argumentación técnica sólida, en la vista judicial es necesario simplificar al máximo la exposición, de la forma más clara y concisa posible para su entendimiento, sin dejar por ello de respetar la realidad en todo momento.

Otro aspecto clave a tener en consideración es la legitimidad de determinadas prácticas de acceso a la información de los investigados en un caso forense. Es frecuente la duda respecto de la realización de determinadas prácticas de investigación, como puede ser el acceso a las cuentas de correo que proporciona la organización a un usuario y donde residen las evidencias necesarias para el esclarecimiento de un caso. En este tipo de escenarios, la línea que delimita la protección de los datos personales no se encuentra claramente definida. 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.

La existencia en las compañías de un buen documento de uso de medios tecnológicos y del que los trabajadores se encuentran adecuadamente informados, facilita considerablemente la situación. Sin embargo la ausencia de éste, deja la interpretación totalmente abierta a la decisión judicial. En este sentido existen sentencias en una y otra dirección. Hay que recordar que la justicia en España se basa en la interpretación de la ley y esta puede orientarse en distintos sentidos.

En una regulación de uso de medios sólida, el documento correspondiente establecerá con claridad que la compañía podrá ejercer el control del uso de los mecanismos que a efectos profesionales se faciliten al trabajador, tal y como recoge el Estatuto de los Trabajadores. Con ello se legitima la posibilidad de controlar el uso de Internet, el mantenimiento de estadísticas o el acceso a las cuenta de correo electrónico, junto a otros aspectos relacionados con la actividad ejercida con medios corporativos por parte de los profesionales. Sin este documento, como se ha indicado, la situación es mucho más compleja y deberá hilarse muy fino, puesto que la experiencia demuestra que circunstancias similares pueden finalizar en dos sentencias totalmente antagónicas. Sirva de ejemplo las que se recogen a continuación.

En el primero de ellos 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 la investigación 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-.”

En contraposición al anterior, 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 por parte de un trabajador del correo electrónico para fines personales, que había desembocado finalmente 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”

Sin embargo, 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 ha sido posible apreciar a lo largo de esta publicación, las situaciones y escenarios propios de una investigación forense son muchos y diversos, con el agravante de poder llegar a complicarse en ocasiones hasta límites insospechados. Recientemente en conversación con un abogado especializado en este tipo de casos, éste me transmitía sus impresiones que me parecen un adecuado final para esta publicación: “Cuanto más experiencia adquiero, mayor es mi incertidumbre por la cantidad de situaciones que he llegado a ver y que me generan la sensación de no saber nunca con certeza como va a finalizar un caso”.

Un forense llevado a juicio



Juan Luis García Rambla

Juan Luis García Rambla, es en la actualidad el Director del Departamento de Seguridad TIC de Sidertia, donde se encuadra el área de análisis forense digital de la compañía. Profesional de contrastada experiencia y reconocimiento en el sector de la seguridad informática, ha desarrollado su actividad a lo largo de más de 18 años en el ámbito tanto civil como militar.

Su participación directa y la coordinación de gran número de casos forenses, así como sus intervenciones como perito informático en juicios de índole civil, le aportan un conocimiento práctico inestimable para la investigación forense. Complementa su sólido perfil técnico con un componente de conocimiento legal de alto valor. Dispone de su propio Blog: “Legalidad Informática”.

Galardonado como Microsoft MVP durante siete años consecutivos en diferentes categorías vinculadas a la seguridad, publica regularmente artículos en revistas y medios especializados. Es autor de tres libros, a los que ahora suma esta nueva publicación, cuya lectura sin lugar a dudas, aportará información de valor tanto a los profesionales de la tecnología como a aquellos vinculados al mundo legal y de la investigación.

“Un forense llevado a Juicio” es una herramienta de inestimable utilidad a la hora de abordar un análisis forense digital que finalice en un proceso judicial. En este tipo de escenarios se mezclan dos áreas profesionales tan dispares como la tecnología informática y el mundo legal, donde el seguimiento de normativas y procedimientos estrictos es determinante. Una buena labor técnica puede desaprovecharse en un juicio al no haber atendido a buenas prácticas no escritas pero que se consideran virtualmente regladas.

Este breve manual aporta la experiencia y el conocimiento de su autor en aspectos fundamentales a la hora de enfocar y desarrollar labores periciales informáticas. La adecuada recogida de las evidencias digitales, la correcta elaboración de un convincente informe para su presentación a juicio son algunos de estos aspectos. Junto a ellos, la publicación muestra los errores más comunes que deben ser evitados o por el contrario las buenas prácticas que permiten llegar a la vista judicial con las garantías de haber realizado una buena labor profesional.