EL PERITO INFORMÁTICO, ESE GRAN DESCONOCIDO

EL PERITO PUEDE SER EN OCASIONES UNA HERRAMIENTA DETERMINANTE PARA UN MAGISTRADO A LA HORA DE ARROJAR LUZ SOBRE LOS HECHOS RELATIVOS A UN DETERMINADO PROCESO JUDICIAL

Juan Martos

DIRECTOR DE INFORMÁTICA FORENSE
RECOVERY LABS

Es muy frecuente que, bien las partes litigantes o bien el propio juez encargado del caso, soliciten la opinión de un experto que les ayude en sus argumentaciones mediante la elaboración de un dictamen pericial. La función del perito informático consiste por tanto en el análisis exhaustivo de los equipos informáticos, y sobre todo de las unidades de almacenamiento de datos en busca de todos aquellos elementos que puedan constituir prueba o indicio en el caso en cuestión.

El perfil de un perito informático debe ser claramente técnico. Es vital que el perito esté familiarizado con las técnicas de recuperación de datos, ya que en ocasiones las pruebas no se encuentran en un estado de uso ideal. Es muy frecuente encontrarse, por ejemplo, con que los datos que pueden ser la clave de la investigación, han sido eliminados por el usuario de la máquina. En estos casos, es necesario llevar a cabo una labor de restauración de los archivos borrados. Como complemento a dicha labor, el perito debe establecer si los datos han sido eliminados por un fallo del sistema, por un virus, o si por el contrario ha sido necesaria la intervención de un usuario. Pero además, el perito debe estar bien asesorado legalmente en todo momento, si no quiere que su informe sea desestimado por algún defecto de forma.

> El perfil de un perito informático debe ser claramente técnico. Es vital que el perito esté familiarizado con las técnicas de recuperación de datos

Existen tres fases bien diferenciadas en la elaboración de un informe pericial: fase de adquisición de las pruebas, fase de investigación y elaboración de la memoria. Cada uno de estos procesos requiere un especial cuidado, ya que el más mínimo defecto de forma puede dar lugar a la desestimación del informe del experto.

La fase de adquisición de las pruebas consiste, tal y como su nombre indica, en la recogida por parte del perito de todos los elementos que van a intervenir en la investigación. Es importante que el proceso de intervención de las máquinas, se lleve a cabo con todas las garantías para las partes. Cuantos más testigos haya presentes durante el acto, mayor fiabilidad le estaremos aportando a la prueba pericial. La documentación del proceso de adquisición es una información que debe formar parte del informe del experto informático.

Durante la fase de investigación, los elementos que deben regir el desarrollo del trabajo del perito son la no alteración de la prueba y el principio de imparcialidad. La mejor manera que tiene un perito para garantizar la no alteración de una prueba es la elaboración de una imagen de todos los dispositivos de almacenamiento. Aquí debo confesar que el perito informático dispone de una ventaja de la que lamentablemente carecen los

expertos del resto de disciplinas: la posibilidad de crear un número ilimitado de clones de la prueba principal, eliminando de este modo las posibilidades de contaminación involuntaria de la evidencia y reduciendo al mínimo las de un posible fallo en la unidad analizada.

Si se cumple con todos estos preceptos, es muy difícil que durante la fase de exposición el testimonio del perito pueda ser puesto en evidencia. De hecho, un buen informe puede llevar a las partes a adoptar algún tipo de acuerdo sin que el juicio llegue a celebrarse. No obstante, lo más frecuente es que el perito tenga que acudir al Tribunal para ratificarse en su informe y responder a las preguntas que, las partes implicadas y el propio juez, le hagan en relación al documento. La fase de declaración es el colofón a todo el trabajo del perito. Si existen dudas, titubeos o contradicciones, el perito pondrá en entredicho su credibilidad y la de su dictamen.

En determinadas ocasiones, el trabajo del perito puede llegar a ser bastante complicado. He aquí un ejemplo: a principios de este año, una empresa requirió de nuestros servicios ante la sospecha de que uno de sus trabajadores estaba utilizando el material informático que la compañía le había proporcionado, con fines extra laborales. Para ser más exactos, pensaban que el trabajador en concreto realizaba conexiones a Internet con el ordenador portátil de la empresa a páginas de descarga ilegal de archivos musicales. Una vez en marcha el proceso de investigación, observé que efectivamente existían archivos musicales en el disco del equipo. Como punto de partida para la averiguación de la procedencia de los archivos, estuve explorando los archivos de registro de una instalación del programa e-mule que estaba presente en la unidad. La exploración sin embargo, no dio resultados positivos. El programa e-mule estaba instalado pero no parecía estar en uso. No había indicios de actividad. Comencé la búsqueda de fuentes alternativas de las posibles descargas ilegales de música. Para ello, decidí investigar los archivos temporales de Internet.

Al proceder a la inspección de los elementos temporales, mi hallazgo fue lamentablemente mucho más desagradable de lo que cabía esperar: había más de 20.000 imágenes de contenido pornográfico. Hasta ahí, 'normal'. Lo peor es que una parte importante de las imágenes de acababa de encontrar, eran de contenido pornográfico infantil. Estuve horas extrayendo y clasificando las imágenes que iba encontrando. La obligación del perito en un caso como el descrito es la de poner todo en conocimiento de las autorida-

des, ya que de otro modo, estaría actuando como encubridor. Es tentadora sin duda la idea de redactar un informe que desprestigie a nivel personal al usuario de la máquina. Pero esto no sería muy profesional. Además, ciñéndonos a los aspectos técnicos nos encontramos con que: por un lado no es posible establecer una correspondencia física entre un ordenador y el usuario de dicho ordenador. Es decir, no hay forma de saber con certeza quién ha llevado a cabo las conexiones a los sitios de contenido ilegal. Por otro lado, nos guste o no, el hecho de que las imágenes estén almacenadas como archivos temporales de Internet, es una consecuencia del comportamiento por defecto del sistema operativo. Es decir, han sido almacenadas sin el conocimiento ni el consentimiento del usuario del equipo. En fin, elementos de peso como para plantearlos en la denuncia y en la redacción del informe.

Sin embargo, no todos los casos son tan desagradables como el que acabo de describir. Algunos tienen un punto mucho más…misterioso. Recientemente, una empresa contactó con nosotros ante la sospecha de que el responsable del departamento de informática estaba sacando de la empresa archivos de contenido confidencial. El reto era sin duda interesante, puesto que me enfrentaba a un usuario altamente experimentado. Pues bien, durante el análisis del equipo pude comprobar que por el mismo habían pasado archivos que en principio no tenían porqué estar ahí: actas del consejo de administración, nóminas de empleados, y un largo etcétera. Caso cerrado…¿o no? La verdad es que no. No podía ser tan fácil.

Cuando me puse en contacto con los responsables de la empresa y les hice partícipes de mis hallazgos, estos respondieron que las fechas y horas de acceso a los documentos confidenciales habían sido llevados a cabo coincidiendo con los periodos en los que el trabajador en cuestión no se encontraba dentro de la empresa. ¿Y ahora qué? ¿cómo era posible tal situación? Los responsables de la empresa aseguraban que como administrador de toda la red, era el jefe de sistemas el único que conocía el password de acceso a su ordenador. Al mismo tiempo, afirmaban que los registros de entrada y salida del despacho de esta persona, demostraban que no había nadie en dicho despacho dentro de la franja horaria en cuestión.

> La función del perito informático consiste en el análisis exhaustivo de los equipos informáticos, y sobre todo de las unidades de almacenamiento

A modo de broma se llegó a pensar que era un claro caso de telequinesia. Y fue al tener ese pensamiento cuando se encendió la bombilla. Solicité que se me permitiese tener acceso al router de la empresa. El router es un aparato cuya misión es gestionar las conexiones a Internet de todos los equipos de una empresa. Lo normal, es que el administrador de los sistemas informáticos cierre toda posibilidad de acceso a los equipos que están bajo su responsabilidad, desde el exterior de la misma. Pude comprobar, que dicha limitación había sido prevista por el protagonista de nuestra investigación. Sin embargo, el informático había establecido una excepción, de forma que se había concedido acceso a los ordenadores de la empresa mediante una conexión remota desde el equipo de su domicilio particular.

Inmediatamente, procedí al análisis de los registros de alertas del sistema. El sistema operativo mantiene un registro de todos los mensajes de alerta que se producen en el equipo con fines de diagnóstico. Así, en el caso de que, por ejemplo, nuestro ordenador portátil se apague y no sepamos la razón, podremos consultar el registro de alertas y comprobar que lo que ha sucedido es que nos hemos quedado sin batería. Podríamos considerar el registro de alertas como una especie de caja negra. Pues bien, la inspección del registro de alertas nos llevó a la conclusión de que el usuario administrador del sistema, había iniciado sesiones remotas desde su domicilio en las horas en las que, obviamente, el responsable de sistemas no se encontraba en la oficina. Dichas conexiones habían sido efectuadas utilizando una IP fija. Al ser fija, este dato nos permitió identificar de manera inequívoca el domicilio desde el que se habían llevado a cabo las conexiones. La casa del responsable de sistemas de la empresa. ¿Caso cerrado? Ahora sí.