



La informática forense y el cuestionamiento de las evidencias digitales

Hay que regresar a la antigua Roma para entender lo que se ha dado en llamar "Informática Forense". La palabra "forense" viene del adjetivo latino "forensis", que significa "perteciente o relativo al foro", y se refiere al hecho de que, en la Roma clásica, una acusación criminal suponía presentar el caso delante de un grupo de autoridades públicas en el foro romano. Tanto el acusado como el acusador pronunciaban discursos, y el que mejor argumentaba su postura, terminaba ganando el caso. Esta es la fuente de los dos significados modernos que tiene la palabra "forense", como "evidencia legal" y como categoría en la oratoria pública.

La **ciencia forense** es lo que resulta de aplicar un amplio espectro de técnicas y ciencias distintas para intentar responder cuestiones que son de interés para el sistema de Justicia, tanto en un delito penal, como en una acción civil. Sin embargo, la actividad forense va más allá y se ocupa de las normas y metodologías científicas válidas, bajo la luz de las cuales, los hechos de un acontecimiento, un artefacto o cualquier otro objeto físico pueden ser "autenticados" dentro de un proceso judicial. La **autenticación**¹, en este contexto legal, es el hecho de establecer o confirmar que algo o alguien es

Con el establecimiento de la sociedad digital han aparecido variantes digitales de algunas actividades clásicas, y eso es lo que le ha pasado a la ciencia forense. Se habla de la Informática forense y ya lleva unos años en marcha, por lo que es tiempo de ver qué es lo que ha conseguido. Siguiendo el principio de reacción, son muchas las medidas que dificultan la investigación forense en medios digitales, por lo que no está claro que se pueda obtener realmente evidencias legales de un ordenador. Éste y otros aspectos quizás más sutiles, son el objeto de este escrito.

auténtico; es decir, que esa naturaleza o esa identidad son ciertas. La **Informática forense** entiende de los estándares que marcan qué



digitales son muchos y graves, y van de la mano de los virus informáticos, del deterioro electromagnético o mecánico del soporte, e incluso con la presencia

cadena de custodia; 4) documentar todo lo que se ha hecho y 5) en el razonamiento desarrollado no ir nunca más allá de lo que uno realmente sabe.

La televisión ya se ha encargado de familiarizarnos con la fase inicial de la investigación en la que el equipo forense toma fotos del área y busca medios digitales de almacenamiento que sean removibles (CDs, DVDs, memorias USB, MP3s,

Hay que establecer la relación entre lo que hay en un ordenador y su dueño, ya que en los escenarios habituales es prácticamente imposible probar que uno realmente controla y es responsable de todo lo que hay en su equipo, o de lo que pasa a través de él.

evidencias y qué modos de obtenerlas son admisibles ante un tribunal de justicia.

Las evidencias electrónicas pueden recogerse en diferentes sitios y de diferentes fuentes, y podrán encontrarse en cualquier elemento o sistema que se esté utilizando para transmitir o almacenar los datos. Así pues, habrá evidencias en la estación de trabajo utilizada por el sospechoso, en el servidor al que ha accedido y en la red que conecta a ambos. En una investigación forense digital se presta una especial atención al cuidado en la manipulación de los ficheros sospechosos. Los peligros para las evidencias

de trampas dejadas por el atacante a modo de minas anti-persona.

Las reglas básicas que ayudan a asegurar que la evidencia no se destruye o queda comprometida (contaminada) durante la investigación son: 1) utilizar solo herramientas y métodos que hayan sido **probados y evaluados previamente**² para determinar su precisión y sensibilidad reales; 2) **manipular lo menos posible** la evidencia original para evitar cambiar los datos; 3) establecer y **mantener una**

MP4s, tokens de seguridad, etc.), y anotaciones, tanto ocultas como a la vista, que pueden contener contraseñas o instrucciones secretas de acceso. Si la máquina analizada está todavía encendida, además se pueden obtener otras informaciones útiles de saber qué aplicaciones están abiertas en ese momento. No toda la información útil está siempre almacenada en los discos duros sino que también está en la memoria volátil del equipo cuyo contenido, en principio, no se

¹ Del griego *αυθεντικός*, real o genuino, y de *authentes*, autor.

² En aras a verificar que una herramienta es utilizable en investigaciones forenses, ésta debe ser probada específicamente para verificar las capacidades reales de la herramienta. En muchos países hay agencias gubernamentales que se dedican a atender y satisfacer esas peticiones de evaluación.

puede recuperar después de haber apagado el sistema. Esto lleva a que, cuando sea posible, se recopilen los datos volátiles del ordenador desde el primer momento.

Herramientas

En cuanto a la instrumentación necesaria para realizar este tipo de investigaciones, hay que decir que son bastantes las herramientas de código abierto que permiten realizar un análisis de puertos abiertos, ver qué discos están montados, incluso si lo están a través de una conexión VPN, determinar qué contenedores cifrados están abiertos y montados en el sistema, etc. Utilizando esas herramientas y otras comerciales, es posible obtener una imagen muy detallada de toda la información contenida en la memoria conjunta del sistema.

Algunas herramientas forenses de código abierto para PCs son **Knoppix**³ y **Helix**⁴, y las herramientas comerciales más populares de duplicado son el **Forensic Toolkit 2.0**⁵ y la aplicación **EnCase**⁶. Todas estas herramientas pueden escanear la memoria volátil y no volátil del sistema, y registrar la información histórica que hay en los ordenadores (sitios web, web-mails, identidades utilizadas, MS Outlook, etc.). El proceso de crear un duplicado exacto de las evi-

dencias originales a menudo se denomina *"imaging"*. Utilizando un duplicador independiente de discos duros o herramientas software tales como **DCFLdd**⁷ o **IXimager**⁸, se puede copiar el disco duro completo. Una vez copiado, el disco original se pone a buen recaudo para prevenir que pueda ser alterado. La corrección del proceso y el mantenimiento de la integridad de las pruebas se verifica, de vez en cuando, utilizando la función *hash* SHA-1 o MD5



El poder de las investigaciones forenses es enorme si se aplican en escenarios en los que sólo hay usuarios comunes e inocentes; pero conviene apuntar que empiezan a aparecer medidas "anti-análisis forense" (anti-forensics). Bajo este nombre se engloban los métodos para prevenir que las investigaciones forenses consigan su meta: la detección, la obtención y el análisis de evidencias.

como detectores de diferencias.

Cuando hay un sistema de almacenamiento como el **EFS**⁹, las claves de cifrado necesarias para acceder a esos datos se pueden obtener si la recolección de datos se hace en caliente, pero en frío, con el ordenador apagado, las cosas pueden ser (mucho) más difíciles. Con el lanzamiento del Microsoft Vista y su uso del **BitLocker**¹⁰ y del **Trusted Platform Module**¹¹ (TPM), en general, la obtención de información

son impracticables durante un análisis de campo.

"Trabas cibernéticas" y doble uso

El poder de las investigaciones forenses es enorme si se aplican en escenarios en los que sólo hay usuarios comunes e inocentes; pero conviene apuntar que empiezan a aparecer medidas "anti-análisis forense" (*anti-forensics*). Bajo este nombre podemos englobar aquellos métodos para prevenir que las investigaciones forenses consigan su meta: la detección, la obtención y el análisis de evidencias. Estas medidas no son nuevas y ya se han visto en casos de fraude corporativo, donde las mismas organizaciones necesitaban generar y diseminar evidencias fraudu-

lentas que les sirvieran de escusa o tapadera. Lo que es más novedoso es que estas *"trabas cibernéticas"* se hayan hecho muy frecuentes en incidentes relacionados con el espionaje industrial.

Una contramedida es el **cifrado de los datos** utilizando tanto algoritmos privados como **algoritmos comunes con una clave almacenada en un puesto remoto**. Un ejemplo de ello lo tenemos en el empaquetamiento de código malicioso que se realiza antes de depositarlo y almacenarlo en

el servidor comprometido. Otra medida es el recurso a la **esteganografía**¹², vetusta técnica que consiste en ocultar los datos para que sean mucho más difíciles de identificar. Las contramedidas también pueden ser instaladas en el sistema operativo; de hecho, se pueden utilizar algunos *rootkits*, disponibles en la red, para evitar que se hagan ciertos cambios en el equipo (apuntes de *log*), o hacer que otros cambios (actualización de los tiempos de modificación en ficheros alterados) no sean visibles ni para usuarios ni para investigadores.

Hay disponibles un amplio surtido de herramientas *anti-análisis forense*. Algunos *wipers* (escobillas) muy comunes son *srn*, *wipe*, *fwipe* y *grind*. El *Defiler's Toolkit*, comenta-

³ Ver <http://www.knoppix-es.org/>

⁴ Ver <http://www.e-fense.com/helix/>

⁵ Ver <http://www.accessdata.com/Products/ftk2test.aspx>

⁶ Ver http://www.guidancesoftware.com/products/ef_index.asp

⁷ Ver <http://dcfldd.sourceforge.net/>

⁸ Ver <http://www.ojp.usdoj.gov/nij/pubs-sum/217678.htm>

⁹ EFS = **Encrypting File System**, de Microsoft. Ver http://en.wikipedia.org/wiki/Encrypting_File_System

¹⁰ Ver <http://en.wikipedia.org/wiki/BitLocker>

¹¹ Ver http://en.wikipedia.org/wiki/Trusted_Platform_Module

¹² Ver <http://en.wikipedia.org/wiki/Steganography>

do en **Phrack**¹³ nº 59 de 2002, es una colección de programas para dificultar el análisis forense en los sistemas de ficheros ext2fs. *Necrofile*¹⁴, uno de sus componentes, permite identificar los i-nodos que tengan cierta fecha y hora de borrado, permitiendo así su eliminación. Esto asegura que no solo los datos son borrados, sino que también desaparecen los metadatos que darían indicios sobre la existencia previa. *Klismafile*, elimina rastros y permite la sobrescritura de las entradas de un directorio. *RuneFS* utiliza el i-nodo de *bad block*, para ocultar bloques de datos del atacante y esto engaña a herramientas forenses comunes como son **TCT**¹⁵ y **TASK**¹⁶. Más recientemente, en 2005, se inició el proyecto *Metasploit*¹⁷ que se centra en el desarrollo de medidas contra la indagación forense. Dentro del **Metasploit Anti-Forensic Investigation Arsenal (MAFIA)**, hay disponibles varias herramientas muy potentes y eficaces en su tarea de borrar pistas e indicios.

No hace falta ahondar mucho en la oferta de contramedidas para percibir que éstas son diseñadas a la imagen y semejanza de las herramientas usadas en la investigación forense, y en los mecanismos que utilizan los ordenadores para hacer sus funciones. Pudiendo definir lo que son pruebas con valor legal, también estamos definiendo un objetivo nítido para las contramedidas utilizadas

por los atacantes. Teniendo que utilizar una serie de aplicaciones software para la investigación forense también abrimos la posibilidad de utilizar los errores, *bugs* y limitaciones de éstas para que las huellas del atacante pasen inadvertidas; pero no definir públicamente esas herramientas, le quitaría el valor de evidencia digital a sus resultados.

Muchas de las contramedidas anti-forenses mencionadas pueden evitarse utilizando mejores sistemas de monitorización y registro (*logs*), y eliminando las limitaciones y *bugs* que hay en la actual genera-



La investigación forense como evaluación de la seguridad de los sistemas debe avanzar, pero su uso en la investigación legal debe tomarse con mucho más cuidado y basarse en otras pruebas no digitales para condenar a alguien; no vaya a ser que se repita el caso de dos inocentes, Sacco y Vanzetti.

ción de herramientas para la informática forense. Los *wipers* dejarían de tener sentido colocando los datos que sean críticos para la seguridad del sistema **en sitios donde el atacante no pueda sobrescribirlos**; por ejemplo, mandando los ficheros a un **servidor de logs** o a un **medio WORM remoto**.

Aunque parece ser anecdótico el uso del cifrado como contramedida para dificultar el análisis forense, no sería raro que su utilización proliferase en los próximos años. También es

cierto que hay noticias que indican que **los cuerpos policiales recuperan claves criptográficas utilizando spyware, keyboard loggers y otras tácticas más propias de sus enemigos que de los defensores de la ley y el orden**. El atacante prudente está más seguro si procede a la "limpieza de pruebas" en vez de utilizar la criptografía, ya que el borrado destruye la información y la criptografía solo la hace no disponible. Lo que sí está claro es que, manteniéndose otros factores iguales, los atacantes que utilicen tecnología anti-investigación forense serán más difíciles de detener y condenar, que

hablando de evidencias digitales que pueden arruinar, meter en la cárcel y, en algunos países, costarle la vida al acusado, por lo que **hay que exigir una madurez que está por llegar**, tanto a las herramientas como a los equipos humanos que se dedican a la Informática Forense. Además de esto, **hay que establecer la relación entre lo que hay en un ordenador y su dueño, ya que en los escenarios habituales es prácticamente imposible probar que uno realmente controla y es responsable de todo lo que hay en su ordenador, o de lo que pasa a través de él.**

aquellos que no la utilicen, lo cual apunta a una exitosa proliferación de este tipo de tecnologías.

Dado que el objetivo de las medidas contra el análisis forense es confundir a los investigadores, es posible que su uso e incluso su misma posesión terminen siendo prohibidas y criminalizadas dentro de algunas organizaciones y países. Sin embargo, esas mismas tecnologías anti-forenses serán necesarias dentro de los sistemas operativos de todos los ciudadanos si se quiere realmente proteger sus datos personales, y quizás sea este bien mayor el que impida su mera prohibición.

Sea como sea, hemos de recordar que estamos

La investigación forense como evaluación de la seguridad de los sistemas debe avanzar, pero su uso en la investigación legal debe tomarse con mucho más cuidado y basarse en otras pruebas no digitales para condenar a alguien; no vaya a ser que se repita el caso de dos inocentes, **Sacco y Vanzetti**¹⁸, que fueron electrocutados en agosto de 1927 por la xenofobia del juez Webster Thayer y gracias a una evidencia balística amañada por él. ■

JORGE DÁVILA MURO
Consultor independiente
Director
Laboratorio de Criptografía
**LSIIS – Facultad
de Informática – UPM**
jdavila@fi.upm.es

¹³ Ver <http://www.phrack.org/issues.html?issue=59>

¹⁴ Ver <http://necrofile.archivospc.com/>

¹⁵ Ver <http://www.porcupine.org/forensics/tct.html>

¹⁶ Carrier, Brian et al: Sleuth Kit (antes TASK) Forensic Software Suite; <http://www.sleuthkit.org>

¹⁷ Ver <http://www.metasploit.net/home/>

¹⁸ Ver http://en.wikipedia.org/wiki/Sacco_and_Vanzetti