LA INFORMÁTICA FORENSE: EL RASTRO DIGITAL DEL CRIMEN

Francisca Rodríguez Más (*)

Alfredo Doménech Rosado (**)

El cadáver se halla a un lado de la cama. Un armario, una mesa y una silla completan el mobiliario de tan adusta dependencia. Mientras los investigadores indagan sobre la tormentosa vida conyugal de la víctima, los especialistas de policía científica continúan con su labor, examinando la escena, tomando fotografías y realizando un reportaje videográfico. Un arma de fuego corta asoma tras el cuerpo de la víctima, y al otro lado de la habitación, sobre una puerta, se adivina la oquedad dejada por un proyectil, el cual, no ha sido encontrado... todavía. ¿Suicidio? ¿Asesinato? Encima de la mesa hay un ordenador portátil y un teléfono móvil. Todas las evidencias lofoscópicas, biológicas y balísticas se recogen aplicando las técnicas adecuadas, pero... ¿qué hacer con el ordenador?... ¿Qué hacer con el teléfono móvil?...

Oculto tras el anonimato, en su oscuro despacho, solamente iluminado por la tenue luz del atardecer, consulta sus mensajes electrónicos privados

(*) Licenciada en Criminología | francisca.rodriguez.mas@gmail.com

(**) CNP | Especialista en informática forense | alfre.domenech@gmail.com

y profesionales, y... ¿por qué no?... los de algunos de sus compañeros de trabajo también. ¿Qué clientes tienen? ¿Alguna relación amorosa inconfesable? ¿Algún problema económico? ¿Algún escándalo político? En fin, algún dato que pueda ser tenido en cuenta... profesionalmente o como chismorreo. Sobresaltado por la aparición en la puerta del director y una comitiva, trata de cerrar las ventanas que estaba consultando... demasiado tarde... le han pillado. Pero... ¿qué hacer con el ordenador?... ¿cuáles son los pasos a seguir?...

En la calle no hay ni un alma. Hace demasiado calor. Es el momento ideal. Tres individuos suben una fotocopiadora... pero los agentes, vigilantes y sigilosos, aprovechan el momento para subir tras ellos e iniciar un registro en el local. En ese momento no hay discos compactos grabados, no hay papel, sólo un ordenador y algunos periféricos, máquinas cortadoras, impresoras, cámaras fotográficas, impresoras de tarjetas, tarjetas blancas con banda magnética, y otro tipo de material. Parece ser que no hay pruebas claras de la comisión de un ilícito penal. Pero... ¿qué hacer con el ordenador? ¿La impresora? ¿La cámara?...

Estas situaciones reales, que suceden a nuestro alrededor –con más o menos frecuencia– ponen de manifiesto que, si bien es cierto que las técnicas forense tradicionales no pueden ser en absoluto descartadas, no es menos cierto que es necesario la aplicación de nuevas disciplinas que apoyen las hipótesis formuladas para el esclarecimiento de ciertos hechos.

Las huellas digitales, con valor identificativo, no fueron usadas hasta finales del siglo XIX. Las pruebas genéticas fueron utilizadas por primera vez en un tribunal a finales del siglo XX, en el año 1996.

A lo largo de todos estos años, la ciencia forense, sin perder su espíritu, ha ido evolucionando hacia un campo muy bien documentado y disciplinado, con gran variedad de niveles de calidad, los cuales son cada vez más exigentes, ya que ha medida que el conocimiento técnico y científico se expande, así también lo hace la ciencia forense. Aún así, ésta siempre irá por detrás de los avances de la ciencia en algún aspecto; sirva como ejemplo que en los años 80 la prueba genética ya fue utilizada en Nueva Zelanda, pero no aparece como prueba válida hasta años después, en los tribunales de los Estados Unidos de América.

Considerando pues los aspectos de que la ciencia forense como disciplina se está desarrollando desde hace más de 800 años, y que lleva menos de un siglo presentándose normalmente ante los tribunales, el campo de la informática forense está en su más tierna infancia.

Breve historia de la informática forense

Muchas son las definiciones que de informática forense podemos encontrar en gran número de publicaciones, pero todas ellas –de una manera u otra– hacen hincapié en unos puntos esenciales; así, de una forma simple, podríamos definir la informática forense como *un proceso metodológico para la recogida y análisis de los datos digitales de un sistema de dispositivos de forma que pueda ser presentado y admitido ante los tribunales*.

De la definición vemos que se trata de un proceso, técnico y científico, que debe estar sujeto a una metodología, tendente primero a la recogida y después al análisis de los datos digitales que se pueden extraer de un sistema o conjunto de dispositivos informáticos o electrónicos, y todo ello con el propósito de ser presentados ante un tribunal. El fin último y principal objetivo que se deduce de la palabra *forense*, es su uso en un procedimiento judicial.

A comienzo de los años 90, el FBI (*Federal Bureau of Investigation*) observó que las pruebas o evidencias digitales tenían el potencial de convertirse en un elemento de prueba tan poderoso para la lucha contra la delincuencia, como lo era el de la identificación por ADN. Para ello, mantuvo reuniones en su ámbito, y a finales de los años 90 se creó la IOCE (*International Organization of Computer Evidence*) con la intención de compartir información sobre las prácticas de informática forense en todo el mundo.

En marzo del año 1998, el G8 –a través del subgrupo de trabajo denominado *The High Tech Crime*, conocido como el Grupo de Lyón– encargó a la IOCE el desarrollo de una serie de principios aplicables a los procedimientos para actuaciones sobre pruebas digitales, así como la armonización de métodos y procedimientos entre las naciones que garantizasen la fiabilidad en el uso de las pruebas digitales recogidas por un estado para ser utilizadas en tribunales de justicia de otro estado. La IOCE, trabajó en el desarrollo de estos principios a lo largo de dos años.

La *Scientific Working Group on Digital Evidence* (SWGDE*)*, principal portavoz de la IOCE en Estados Unidos, y la *Association of Chief Police Officers* (ACPO) del Reino Unido, propusieron una serie de puntos que luego englobaron los principios generales que se presentaron en el año

2000 al Grupo de Lyón.

Principios básicos

Una vez estudiado el informe, el G8 aprobó un conjunto de principios básicos para luego dictar una serie de recomendaciones aplicables a las evidencias digitales:

- Todos los principios generales de procedimientos y técnicas forenses deben ser aplicados cuando se manipulen pruebas digitales. Cualquier institución con atribuciones en la búsqueda, recolección, y análisis de pruebas debe tener una metodología o unos principios generales definidos con el objetivo de proteger los intereses de todas las partes. Dichos principios han de tener en cuenta las peculiaridades de cada ordenamiento jurídico.
- En la manipulación de pruebas digitales, las acciones que se lleven a cabo no deben alterar dicha prueba. Siempre que sea posible, no se realizará ninguna acción, durante la búsqueda, recolección, o manipulación de las pruebas digitales, que conlleve una alteración de la misma. En caso de que se tenga que actuar de tal forma que se altere la prueba, las acciones deberán ser completamente documentadas.
- Cuando sea necesario que una persona tenga acceso a una prueba digital original, dicha persona debe estar formada para ese propósito. Aunque es ampliamente aceptado que la mejor práctica es realizar una imagen digital de la prueba a analizar, y actuar sobre la copia, puede haber ocasiones, en el curso de una actuación, en que se tenga que acceder a la prueba digital original. Dicha acción, además de seguir el principio anterior, debe realizarse por una persona que esté formada en dicho aspecto.
- Toda actividad relativa a la recogida, acceso, almacenamiento, o transferencia de pruebas digitales debe ser completamente documentada, conservada y disponible para su estudio. Todas las manipulaciones que se lleven a cabo deben ser documentadas de forma total y comprensible, de manera que las acciones que se están registrando puedan ser reproducidas si fuera necesario. Es vital mantener la cadena de custodia.
- Cada persona es responsable de todas las acciones tomadas con respecto a la prueba digital mientras dicha prueba esté a su cargo. Dicha responsabilidad es personal y no corporativa.

- Cualquier institución o grupo, que sea responsable de la recogida, acceso, almacenamiento, o transferencia de una prueba digital, es responsable de cumplir y hacer cumplir estos principios. Las instituciones con atribuciones en la recogida y manipulación de pruebas digitales, velarán para que estos principios se lleven a cabo, siendo un marco de referencia y trasladándose éstos a los procedimientos de actuación que se desarrollen en dichas instituciones.

Todas las técnicas utilizadas para la recogida y análisis de evidencias digitales, deben estar respaldadas por una buena metodología científica y documentadas en un protocolo de actuación, que recoja tanto los aspectos técnicos de la informática como los aspectos legales que se derivan de su peculiaridad forense.

Para asegurar que las pruebas digitales son recogidas, preservadas, examinadas o transferidas de manera que se salvaguarde su integridad, fiabilidad, y precisión, todas las instituciones forenses, cuya función esté relacionada con *dichas pruebas* digitales, deberán establecer y mantener un sistema de calidad efectivo, sin olvidar tampoco la formación del personal.

Metodología

Diversas metodologías han surgido publicadas por diversas instituciones y organizaciones, así como por expertos en la materia, encajando algunos modelos mejor que otros, según el tipo de investigación que se esté llevando a cabo. Podríamos hablar pues de dos metodologías principales atendiendo al hecho, su repercusión, y la actuación de unos especialistas u otros.

Desde el punto de vista de la comisión de un hecho delictivo, y de la actuación de los Cuerpos y Fuerzas de Seguridad, se puede establecer una metodología aplicable a la informática forense que, en términos generales, debe seguir estos puntos:

- Identificación: Consiste en el conocimiento y la comprobación del hecho delictivo. Por regla general la actuación será iniciada a requerimiento de un grupo investigador o bien a requerimiento de la autoridad judicial.
- Preparación: La preparación y planificación de las herramientas, las técnicas a utilizar y la obtención de los permisos necesarios para efectuar las acciones pertinentes. Los equipos de laboratorio deben estar revisados, actualizados, en buen estado, y no contaminados. Los manuales de operación y los manuales de instrucción deben estar

preparados, y las aplicaciones de creación de copias y de análisis han de estar comprobados y validados. La formación de los especialistas debe ser la adecuada y debe ser continua.

- Planificación estratégica: Desarrollar una estrategia tendente a maximizar la recolección de pruebas y minimizar el impacto sobre la víctima. Cuando un registro vaya a ser llevado a cabo, en donde estén o no envueltos equipos o dispositivos electrónicos, una preparación preliminar es conveniente.

  En lo que se refiere a pruebas digitales, es necesario obtener la máxima información posible sobre el tipo, lugar, y conexiones de cualquier sistema de ordenadores. Si se sospecha la existencia de redes de ordenadores medias o grandes, se debería contar con el asesoramiento de especialistas, mientras que si, como en la mayoría de los casos, se trata de ordenadores personales, cualquier persona, con una formación básica, es suficiente para llevar a cabo la tarea. Hay que recordar, que no sólo en los ordenadores se puede encontrar información que puede resultar imprescindible para el esclarecimiento de un hecho.

  De cualquier forma no siempre es posible una información tan detallada, por lo que queda a decisión del investigador la mejor opción a la hora de recoger las pruebas, teniendo en cuenta el motivo por el que se realiza el registro. No se debe perder de vista el riesgo que conlleva una mala actuación sobre una prueba digital.

- Aseguramiento de la escena, tanto física como digital: En todo escenario de un hecho delictivo, y al igual que se toman las debidas medidas y precauciones para no contaminar la escena de aquellos vestigios que sean susceptibles de ser enviados a los laboratorios para su examen (huellas digitales, ADN, elementos balísticos, etc.), así se deben tomar las debidas precauciones para no contaminar la escena digital, ya sea por medios físicos o electrónicos.

  La contaminación física puede alterar una evidencia digital: una manipulación incorrecta puede conllevar una modificación e incluso una pérdida total de la evidencia. Sirva como ejemplo que la electricidad estática que podemos portar, al tocar un circuito, puede inutilizar éste completamente; un imán cerca de un dispositivo altera los datos almacenados en el mismo; los golpes no se llevan bien con las partes mecánicas de un disco duro; etcétera.

  La contaminación electrónica proviene de un mal aislamiento del dispositivo frente a su entorno, sobre todo en su embalaje. Dispositivos que acepten datos de forma inalámbrica (*routers*, teléfonos móviles, agendas electrónicas, *tablets*, etc.) deben ser

aislados adecuadamente para que la congelación de la escena sea efectiva, especialmente aquellos que no deben ser apagados.

- Recogida de pruebas: Registrar la escena del delito, recoger y empaquetar adecuadamente las evidencias digitales, garantizando su integridad, y prestando atención a la cadena de custodia son, posiblemente, las acciones en que más cuidado hay que tener debido a la gran cantidad de situaciones y evidencias que se pueden hallar.

  Como en todo registro, la búsqueda y recogida de dispositivos ha de hacerse siguiendo los procedimientos generales en casos de una entrada y registro y los específicos sobre los dispositivos digitales. Allí donde sea posible, los elementos deben ser examinados en un laboratorio en vez de ser examinados in situ. En caso de que no sea posible de este modo, éstos han de ser examinados de forma que no sean alterados o bien lo sean en la menor medida posible, registrando todos y cada uno de los pasos que se están tomando. Es importante realizar la copia o el clonado de la evidencia digital y realizar su firma digital.

  Mención especial deben tener los dispositivos de telefonía móvil, ya que su correcta manipulación puede evitar desagradables sorpresas en fases posteriores.

- Examen: Tanto esta fase como la siguiente, requieren una mayor especialización técnica. No se ha de olvidar el cumplimiento exacto de la cadena de custodia, y se debe estar en posesión de la autorización necesaria para proceder al examen y análisis de las evidencias. Se realiza un estudio preliminar de los dispositivos recogidos en cuanto a características físicas y técnicas, estructura, formato, etc.

- Análisis e interpretación: Analizar metódicamente las pruebas. Interpretar los datos que se obtengan e interrelacionarlos adecuadamente para tratar de explicar los hechos y su distribución temporal. Es la fase más larga de todo el proceso, y está íntimamente relacionada con el hecho que se está investigando.

- Documentación: El objetivo final de un análisis forense, es plasmar por escrito de una forma exacta, comprensible, clara, y completa, los pasos realizados en el análisis, los hallazgos, su interpretación y la conclusión que de ellos se derivan. No hay que perder de vista el carácter forense que tiene el análisis, por lo que, a lo largo de la redacción del informe, hay que tener presente a quien va dirigido y en muchos casos el destinatario final no tiene los conocimientos técnicos suficientes sobre la materia, por lo que la terminología usada y la manifestación de los hechos debe adecuarse a esta

situación.

El sentido común, la aplicación de una buena metodología, el desarrollo de Procedimientos Básicos de Actuación, y la formación general y especializada, primordialmente, son, entre otras, características esenciales y requisitos imprescindibles para garantizar el buen hacer ante cualquier reto de análisis y su puesta a disposición de la autoridad judicial.

Todas las disciplinas forenses evolucionan a medida que aparecen nuevos hallazgos, mejoran las técnicas y se desarrollan nuevas metodologías científicas, por lo que no es de extrañar que surjan más técnicas que favorezcan el trabajo de investigación y análisis que los especialistas forenses realizan día a día, y tampoco es descabellado pensar que aparecerán más disciplinas que puedan ser aplicadas tanto para la resolución de hechos, cómo para el apoyo a la autoridad judicial.

Lo que sí es seguro es que en el ámbito de la informática forense los especialistas no pueden bajar la guardia, ya que la evolución en este campo no puede medirse ni en años ni en meses, sino en días.

Bibliografía

- Guidelines for Evidence Collection and Archiving; *RFC 3227*; http://www.faqs.org/rfcs/rfc3227.html
- G8 Proposed Principles For The Procedures Relating To Digital Evidence; *International Organization on Computer Evidence (IOCE)*;http://www.ioce.org
- Good Practice Guide For Computer-Based Electronic Evidence; *Association of Chief Police Officers (ACPO)*;http://www.acpo.police.uk
- Forensic Examination of Digital Evidence: A Guide for Law Enforcement; *National Institute of Justice*; 2004;http://www.nij.gov
- First Responders Guide to Computer Forensics; *Richard Nolan, Colin O'Sullivan, Jake Branson, Cal Waits*; Carnegie Mellon University; 2005
- The Evolution of Computer Forensic Best Practices: An Update on Programs and Publications; *Alan E. Brill, Mark Pollit, Carrie Morgan Whitcomb*; Journal of Digital Forensic Practice; 2006.
- Best Practices for Computer Forensics; *Scientific Working Group on Digital Evidence (SWGDE)*; 2006
- Special Considerations When Dealing With Cellular Phones;

Scientific Working Group on Digital Evidence (SWGDE); 2007

- Modelos y Principios en la Informática Forense; *A. Doménech, A. Cebrián, E. Peiro*; 2007
- Model Standard Operating Procedures Manual for Computer Forensics; SWGDE; 2011
- Electronic Crime Scene Investigation: A Guide for First Responders; *National Institute of Justice*; 2008;http://www.nij.gov