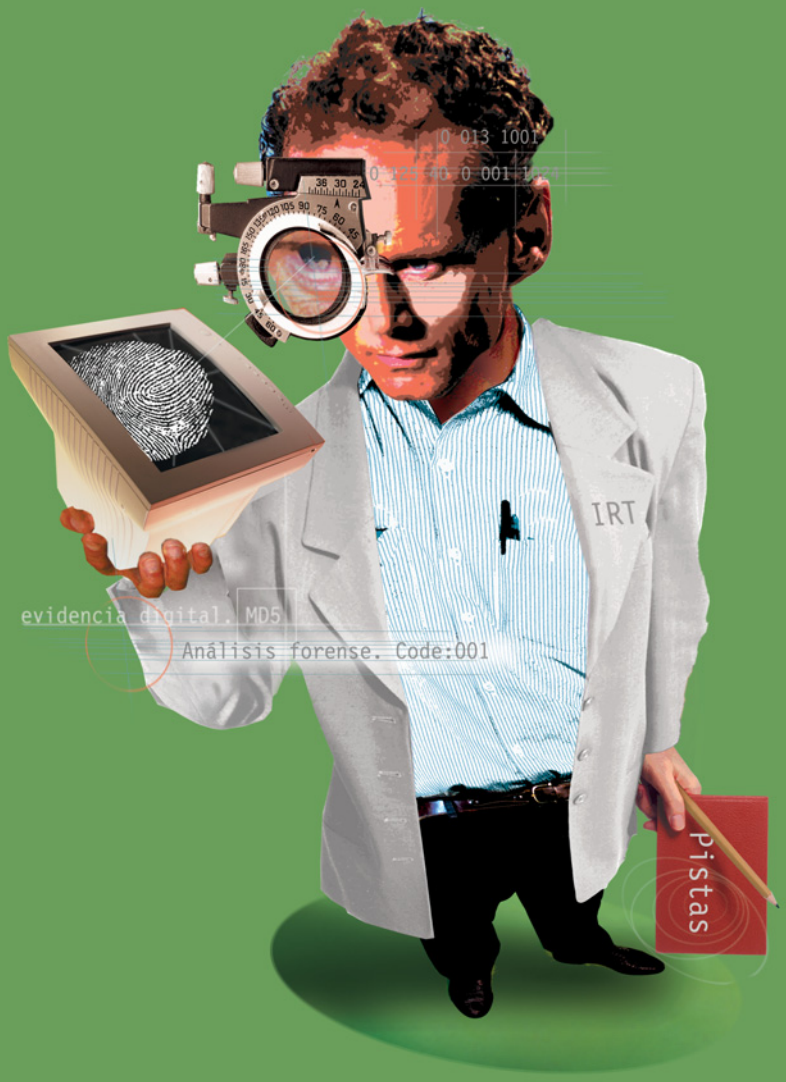
La formación de un Equipo de Respuesta a Incidentes Forense

En este artículo se tratan los aspectos principales del análisis forense de sistemas, revelando los puntos más importantes para abordar la creación de un equipo de respuesta a incidentes (IRT) cualificado, los perfiles típicos de los cibercriminales, la formación de cada investigador o miembro del equipo, la definición de procedimientos y guías de buenas prácticas, imprescindibles en cualquier ciencia forense, el material necesario para llevar a cabo la recopilación de evidencias y análisis de los datos de forma correcta y eficiente, siempre prestando especial atención en no alterar las evidencias, siguiendo una metodología rigurosa y científica, fijando como objetivo principal aumentar al máximo las posibilidades de éxito en la Corte, por si fuera necesario acudir a un proceso judicial, algo que *a priori* es posible que no se tenga en cuenta, hasta que no se determine la gravedad del incidente.



Antonio Javier García Martínez

Tanto el contexto internacional actual, en el que La Red deja de ser una mera aliada, pasando de aportar sólo ventajas a ser el medio canalizador y quizás también catalizador de muchos males (terrorismo, *spam*, abusos, fraudes, virus, etc.), como el aún más cercano contexto nacional, con la introducción de nuevas leyes como la LSSI o la LOPD, que fuerzan a las empresas a tomar medidas de seguridad acordes con la compleja tecnología actual, configuran un entorno hostil en el que no basta sólo con ser capaz de recuperarse ante un incidente, sino que además es necesario demostrar que se estaban cumpliendo los requisitos mínimos exigidos por la ley para evitar el castigo económico y/o la pérdida de imagen; más aún, se exige disponer de la capacidad de determinar el motivo del mismo, es decir, el qué, el cómo y el cuándo, y en muchas ocasiones, el autor.

Por otra parte, aunque algunas veces puede no ser muy complicado llegar a responder estas preguntas, siempre se debe tener especial cuidado en respetar todos los procedimientos y aspectos legales, de forma que, si fuera necesario acudir a la justicia, se haga con todas las garantías necesarias para convencer a un

tribunal de la validez y autenticidad de las evidencias, demostrando que, a pesar de la volatilidad y facilidad de manipulación de las evidencias, sobre todo las digitales, se dispone de un método, un procedimiento científico, estricto y reconocido por la empresa, cuya finalidad no es sino el recopilado y manipulación adecuada de las evidencias, respetando ante todo la preservación de las mismas.

A pesar de las defensas y medidas que se tomen, la seguridad total no existe; la probabilidad de sufrir un incidente de seguridad podrá ser minimizada y controlada por los planes de gestión de riesgo y las medidas tomadas conforme a los mismos; sin embargo, tarde o temprano ocurrirá un incidente de mayor o menor gravedad y con toda seguridad alguien querrá saber exactamente qué ocurrió: aquí es dónde el equipo de respuesta ante incidentes con una alta formación en análisis forense deberá entrar en acción. Este artículo guía al lector acerca de cómo formar un IRT forense y todo el equipo y procedimientos que necesitará para realizar su trabajo.

Comenzaremos por la definición de cibercrimen, o crimen de ordenador, que entenderemos como un acto criminal en el que un ordenador es esencial para perpetrar el crimen, o si no fuera esencial para la realización del mismo, sí que actuaría como almacenaje de información concerniente a dicho crimen.

Cibercriminal sería pues, aquel que comete un cibercrimen.

Todo el argumento gira en torno a la evidencia digital con el propósito de demostrar cómo puede ser usada para identificar al sospechoso, castigar al culpable, defender al inocente y comprender el comportamiento y motivaciones del cibercriminal. Para alcanzar este fin, es necesario conocer en mayor o menor medida los siguientes campos:

– Ciencia informática: que proporcionará el conocimiento técnico para comprender los aspectos específicos de las evidencias digitales.

– Ciencia forense: proporciona una aproximación general al análisis de cualquier evidencia digital.

– Modelos de comportamiento: un nuevo campo que proporciona la posibilidad de conocer y comprender mejor las motivaciones y comportamiento del cibercriminal.

Nos centraremos sobre todo en el campo de la ciencia forense, aunque puede ser imprescindible un conocimiento suficiente de muchos apartados de la informática como la criptografía, los sistemas operativos, las redes, etc. El análisis y determinación del perfil del cibercriminal puede permitir adelantarnos a sus actos.

Para entender perfectamente el resto del artículo se precisa de la definición de dos términos importantes:

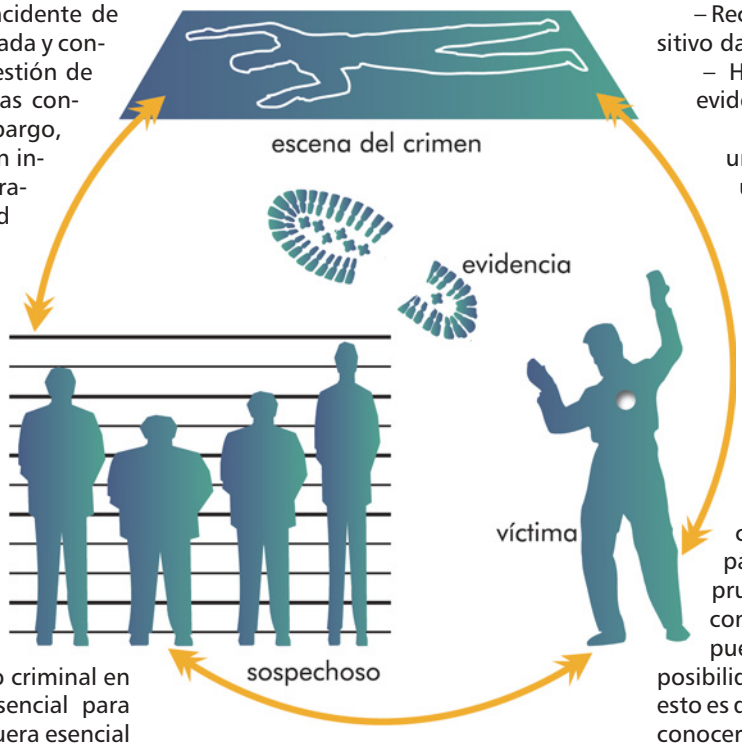


Figura 1: Principio de transferencia de Locard.

Incidente de seguridad, como cualquier evento no programado (anomalía) que pudiera afectar a la seguridad de la información, entendiendo "afectar a la seguridad" como una pérdida de disponibilidad, integridad o confidencialidad.

Un IRT, o *equipo de respuesta a incidentes* , que no es más que una organización o grupo responsable de recibir, revisar y responder frente a notificaciones o descubrimientos de incidentes de seguridad. Un IRT puede ser tanto un equipo formalmente constituido, donde sus miembros responden a incidentes como su principal función de trabajo o un equipo *ad-hoc* que, en cambio, se reúne para tratar incidentes de seguridad en curso o inminentes. En adelante se hablará indistintamente de IRT o equipo forense siendo, a efectos prácticos, la misma cosa.

CIENCIA FORENSE

La ciencia forense proporciona los principios y técnicas que facilitan la investigación del delito criminal, en otras palabras: cualquier principio o técnica que puede ser aplicada para identificar, recuperar, reconstruir o analizar la evidencia durante una investigación criminal forma parte de la ciencia forense.

Los principios científicos que hay detrás del procesamiento de una evidencia son reconocidos y usados en procedimientos como:

– Recoger y examinar huellas dactilares y ADN.

– Recuperar documentos de un dispositivo dañado.

– Hacer una copia exacta de una evidencia digital.

– Generar una huella digital con un algoritmo *hash* MD5 o SHA1 de un texto para asegurar que éste no se ha modificado.

– Firmar digitalmente un documento para poder afirmar que es auténtico y preservar la cadena de evidencias.

Un forense aporta su entrenamiento para ayudar a los investigadores a reconstruir el crimen y encontrar pistas. Aplicando un método científico, analiza las evidencias disponibles, crea hipótesis sobre lo ocurrido para crear la evidencia y realiza pruebas, controles para confirmar o contradecir esas hipótesis..., lo que puede llevar a una gran cantidad de posibilidades sobre lo que pudo ocurrir; esto es debido a que un forense no puede conocer el pasado, no puede saber qué ocurrió ya que sólo dispone de una información limitada. Por tanto, sólo puede presentar posibilidades basadas en la información limitada que posee.

Un principio fundamental en la ciencia forense, que usaremos continuamente para relacionar un criminal con el crimen que ha cometido, es el Principio de Intercambio o transferencia de Locard, (**Edmond Locard**, francés fundador del instituto de criminalística de la universidad de Lion). Se puede ver el esquema en la **figura 1**.

Este principio fundamental viene a decir que cualquiera o cualquier objeto que entra en la escena del crimen deja un rastro en la escena o en la víctima y viceversa (se lleva consigo); en otras palabras: "cada contacto deja un rastro". En el mundo real significa que si piso la escena del crimen con toda seguridad dejaré algo mío ahí: pelo, sudor, huellas, etc. Pero también me llevaré algo conmigo cuando abandone la escena del crimen, ya sea barro, olor, una fibra, etc. Con algunas de estas evidencias, los forenses podrán demostrar que hay una posibili-

dad muy alta de que el criminal estuviera en la escena del crimen.

En este ejemplo hemos hablado de evidencias físicas; en la ciencia forense tradicional hay varios tipos de evidencias físicas:

– **Evidencia transitoria**: como su nombre indica es temporal por naturaleza, por ejemplo un olor, la temperatura, o unas letras sobre la arena o nieve (un objeto blando o cambiante).

– **Evidencia curso o patrón**: producidas por contacto, por ejemplo la trayectoria de una bala, un patrón de rotura de un cristal, patrones de posicionamiento de muebles, etc.

– **Evidencia condicional**: causadas por una acción o un evento en la escena del crimen, por ejemplo la localización de una evidencia en relación con el cuerpo, una ventana abierta o cerrada, una radio encendida o apagada, dirección del humo, etc.

– **Evidencia transferida**: generalmente producidas por contacto entre personas, entre objetos o entre personas y objetos. Aquí descubrimos el **concepto de relación**.

En la práctica, las evidencias transferidas se dividen en dos, conocidas como:

– Transferencia por **rastro**: aquí entra la sangre, semen, pelo, etc.

–Transferencia por **huella**: huellas de zapato, dactilares, etc.

Aunque en la realidad, estas últimas suelen mezclarse, por ejemplo una huella de zapato sobre un charco de sangre.

Repasemos lo aprendido; el principio de intercambio de Locard se puede resumir así:

1. El sospechoso se llevará lejos algún rastro de la escena y de la víctima.
2. La víctima retendrá restos del sospechoso y puede dejar rastros de si mismo en el sospechoso.
3. El sospechoso dejará algún rastro en la escena.

El objetivo es establecer una relación entre los diferentes componentes:

– la escena del crimen
– la víctima
– la evidencia física
– el sospechoso

Para la correcta resolución del caso, todos estos componentes deben estar relacionados. Esto se conoce como el **concepto de relación**, que es lo que nos faltaba para completar el principio de intercambio de Locard.

Las evidencias pueden, a su vez, ser transferidas de dos formas distintas:

1. Transferencia directa: cuando es transferida desde su origen a otra persona u objeto de forma directa.

2. Transferencia indirecta: cuando es transferida directamente a una localización y, de nuevo, es transferida a otro lugar.

Resulta importante resaltar que cualquier cosa y todo puede ser una evidencia.

La ciencia forense facilita las herramientas, técnicas y métodos sistemáticos (científicos) que pueden ser usados para analizar una evidencia digital y usar dicha evidencia para reconstruir qué ocurrió durante la realización del crimen con el último propósito de relacionar al autor, a la víctima y la escena del crimen.

EVIDENCIA DIGITAL

La evidencia digital, aunque la hemos nombrado a menudo, aún no ha sido explicada ni incluida en la categorización realizada anteriormente de tipos de evidencias físicas, pero sí, una evidencia digital es un tipo de evidencia física, aunque es menos tangible que otros tipos de evidencias físicas (como la sangre, o un componente de un ordenador); las evidencias digitales son campos magnéticos y pulsos electrónicos que pueden ser recogidos y analizados usando técnicas y herramientas especiales. Además, los tribunales sostienen que a pesar de su propiedad de intangibles, pueden ser admitidas como evidencia.

Las evidencias digitales son campos magnéticos y pulsos electrónicos que pueden ser recogidos y analizados usando técnicas y herramientas especiales. Además, los tribunales sostienen que a pesar de su propiedad de intangibles, pueden admitirse como evidencia.

Ventajas de las evidencias digitales sobre otros conjuntos de evidencias físicas son:

– Pueden ser duplicadas de forma exacta y la copia puede examinarse como si fuera el original.

– Con las herramientas adecuadas es muy fácil determinar si la evidencia ha sido modificada o falsificada comparándola con la original.

– Es relativamente difícil de destruir, incluso borrándola, la evidencia digital puede ser recuperada de un disco.

– Si alguien intenta destruir las evidencias, podemos tener copias igual de válidas lejos del alcance del criminal.

Un ejemplo de evidencia digital y del principio de Locard es el intercambio de claves públicas que se realiza al conectarse a un servidor vía un cliente de ssh. Si tuviéramos acceso vía orden judicial al ordenador del criminal, encontraríamos la llave pública del servidor, esto sería el "rastro" que la escena del crimen deja en el sospechoso y es una prueba inequívoca de que el sospechoso estuvo allí.

Otro ejemplo similar sería recibir un correo amenazante; si analizamos las cabeceras del correo podríamos encontrar por ejemplo el cliente de correo que se utilizó, (imaginemos que a través de las etiquetas de la cabecera el X-mailer es mutt), si tras una orden judicial en el equipo del sospechoso encontráramos el mismo cliente mutt, y es más, con un poco de suerte puede haber olvidado borrar el correo que mandó de su carpeta de enviados, con lo que tendríamos una tendríamos una evidencia de mucho peso, al ser obtenida en el equipo del sospechoso.

El ejemplo típico es golpear un cristal con un puño: en la escena del crimen quedarán cristales y sangre y restos del agresor, pero a la vez éste se llevará consigo, junto a arañazos y heridas, restos microscópicos de ese mismo cristal que ha roto.

ANÁLISIS FORENSE

Definimos análisis forense como una recopilación de evidencias de cara a un proceso judicial. Hablamos de evidencias, porque estas no serán pruebas hasta que el juez las admita.

Un análisis forense tiene cuatro fases principales: Identificación, Preservación de la evidencia, Análisis e Informe.

Un examen forense es aquel análisis forense que se realiza bajo tales condiciones que está completamente documentado, es reproducible y sus resultados son verificables. Un examen forense no borra ni altera ningún dato en la evidencia original, preservando los mismos de forma precintada, e independientemente de quién lleve a cabo el examen, con qué herramientas y metodologías, debe siempre llevar a los mismos resultados.

Las evidencias digitales suelen pasarse por alto, o recolectarse incorrectamente o analizarse ineficientemente debido a mala formación técnica y desconocimiento de la normativa legal; sin embargo es muy importante tener el conocimiento y la pericia necesaria para usar con efectivi-

dad la evidencia digital en cualquier tipo de investigación.

¿QUIÉN PUEDE IDENTIFICAR Y RECOLECTAR EVIDENCIAS DIGITALES?

La primera pregunta que deberíamos hacernos durante una investigación es "¿quién está autorizado para recolectar y analizar las evidencias digitales relevantes?".

Con las evidencias físicas, sólo expertos autorizados y especialmente entrenados pueden hacer este trabajo; no sucede así con las evidencias digitales. Mientras que los análisis realizados sobre evidencias físicas son en su mayor parte realizados por expertos especialmente entrenados en sus propios laboratorios, con los forenses informáticos el estudio se realiza en muchas ocasiones sobre equipos y entornos que no les son familiares y en muchos casos les resultan hostiles, (centro de datos con bajas temperaturas, con mucho ruido de fondo, con movimiento de gente continuamente, etc.) y en muchas ocasiones no disponen del entrenamiento adecuado, (simples detectives u oficiales de policía con escasos conocimientos de ciencia forense o quizás incluso de informática).

A menudo, suele ocurrir que los propios empleados o expertos de sistemas colaboran con las fuerzas de la ley, probablemente porque ellos conocen el sistema al ser empleados o expertos, y las fuerzas del orden agradecen la ayuda.

En España, recomendamos avisar siempre a las fuerzas del orden, aunque haciendo una correcta y demostrable recolección y análisis de las evidencias de la escena del crimen ya depende del juez que las acepte o no; se trata pues de convencer al juez de que hemos actuado de forma profesional, científica, eficiente y explicárselo de forma que lo pueda entender pues es muy probable que el juez no posea conocimientos avanzados de estas materias. Tanto mejor si hay testigos para todo y si las evidencias, (incluso las digitales) están impresas en papel, firmado por los testigos y con etiquetados con fecha y hora, huella *hash* y comentarios sobre la evidencia recogida según un formato prestablecido en los procedimiento, ya que a veces, de cara al juez, parece tener más peso y menos volatilidad y facilidad de manipulación algo físico como es un documento impreso y firmado por testigos, que el mismo documento en formato electrónico.

Sin embargo, las evidencias que el sospechoso se ha llevado consigo, sólo deben ser obtenidas por las fuerzas de la ley y previa orden judicial para poder ser presentadas en los tribunales, ya que el equipo forense no puede ejercer la función de investigador, aunque sí de perito en el juicio.

Un ejemplo muy ilustrativo de identificación de evidencia es un cadáver en lo alto de una cumbre nevada con arena alrededor. En este caso la arena es una evidencia, la nieve es ruido. Es pues imprescindible saber reconocer y aislar las evidencias del ruido de la escena del crimen.

PROCEDIMIENTO PARA RECOLECCIÓN DE EVIDENCIAS

Aislar la escena del crimen

Ante todo se necesita aislar (en argot técnico se suele denominar congelar) y acotar con un perímetro la escena del crimen, para evitar la corrupción de la misma y de las evidencias que en ella puedan hallarse. Se pretende evitar que nadie pueda manipular las evidencias y éstas o todo el caso sea desestimado por una mala gestión de evidencias. Sin embargo, debemos tener en cuenta que en la mayoría de los casos encontraremos contaminada la escena del crimen, (de nuevo el principio de Locard), pues es muy difícil que el IRT sea el que descubra el incidente; normalmente será un administrador que inmediatamente tratará de minimizar daños, cambiará la contraseña de *root* para tratar de impedir (inútilmente en la mayoría de los casos) la entrada del intruso, con la consecuente alteración de evidencias.

Nótese que todo el mundo, incluso los empleados, son sospechosos, cualquiera puede ser el autor del crimen; es más, en la mayoría de los casos la persona que avisa a la policía tiene algún tipo de relación con lo ocurrido en la escena del crimen.

Cadena de custodia

Es necesario definir la función y responsabilidad de cada miembro del equipo forense para cada uno de los distintos tipos de evidencias que podamos esperar hallar. Algunas funciones serán comunes, pero otras dependerán del grado de especialización de cada componente del equipo.

Con el objetivo de llevar a juicio las evidencias recopiladas se debe establecer lo que se denomina la cadena de custodia de las evidencias; todo debe quedar debidamente documentado y precintado, con un riguroso control de acceso a las mismas y a sus contenedores; por ejemplo, los ordenadores del equipo forense en los que se estudiarán las evidencias deberían disponer de una red propia aislada del resto de la red corporativa. Recordemos que todo el mundo es sospechoso.

Es necesario definir el conjunto de materiales y herramientas válidas a emplear por el equipo forense, y entrenar al mismo para un correcto uso, (puede ser interesante por ejemplo contratar a una empresa experta para que comprometa un sistema y realizar un entrenamiento tratando de hacer un análisis forense). Otra opción válida es colocar un *honeypot* (tarro de miel) para aprendizaje y entrenamiento real del equipo forense. Este tipo de prácticas es muy importante pues la primera fase de todo análisis forense es la identificación del evidencias, tarea nada sencilla, sobre todo si no se tiene el entrenamiento adecuado.

Es importantísimo definir un método de almacenamiento y etiquetado de evidencias, de manera que estas se guarden por la persona designada y acompañadas de su firma temporal (*timestamp*) y su firma digital (MD5 o SHA1) para garantizar la fiabilidad de las evidencias; es muy útil incluir comentarios descriptivos, como podría ser el nombre y ruta del fichero, lo que nos permitirá, si hay una correcta elección de nomenclatura, realizar búsquedas de determinados tipos de ficheros sin necesitar acceder al contenido del mismo.

Lo ideal sería hacer dos copias de cada evidencia, teniendo en cuenta la facilidad de duplicación de las mismas de forma exacta. Esto es así para poder constatar evidencias que han viajado por un canal inseguro o deben permanecer en la escena del crimen o que podrían estropearse durante el transporte. Teniendo en cuenta que cualquiera puede ser sospechoso, si recogemos una evidencia y nos la enviamos por *e-mail* desde la misma escena del crimen, si el administrador de correo estuviera implicado podría llegar a interceptar la evidencia (por ejemplo evitando que abandone el servidor de correo hasta que logre falsificarla). Recordemos la necesidad de definir responsables de custodia de las evidencias en los recipientes adecuados.

Ejemplo de manipulación incorrecta de evidencias es el sacar un disco duro de un CPD que dispone de una temperatura controlada a 11º C a temperatura ambiente, que en algunos sitios podría ser perfectamente hasta 45º C (pensemos en Sevilla en pleno agosto). Es probable que someter a un dispositivo delicado como un disco a un cambio de temperatura tan brusco provoque un mal funcionamiento del mismo y, por consiguiente, una pérdi-

da de datos.

Otro ejemplo típico lo constituyen los electroimanes que se colocan en las entradas de los centros de datos, de forma que si alguien trata de sacar un disco o una máquina, la información que contiene queda inutilizada.

Una vez clasificada y etiquetada la evidencia debe ser fotografiada, precintada y entregada a un custodio, que tendrá la responsabilidad de la custodia y la manipulación correcta de las mismas para evitar este tipo de problemas. Para ello, repetimos, necesita el material y entrenamiento adecuado. Todo esto en presencia de testigos.

Equipo necesario

En mi trabajo diario he abordado diversos proyectos desde finales del 2002 y los primeros nueve meses del 2003 para la adquisición de las herramientas software y hardware así como los procedimientos necesarios para realizar la fase de identificación y recogida de evidencias con éxito.

Herramientas

Uno de estos proyectos era el de adquisición de hardware y software, denominado "Kit portable de análisis forense", con el objetivo de disponer de todo el material necesario para, en caso de detección de intrusión o compromiso de redes o sistemas, disponer de un equipo físico de respuesta rápida ante incidentes (IRT) con la movilidad suficiente como para desplazarse con todo el equipo necesario para la recogida y análisis forense de los equipos comprometidos.

Tras un análisis preliminar de las opciones de mercado nos decantamos por un equipo portable, por la características propias de la empresa, con una gran dispersión geográfica de centrales y edificios.

El componente principal del *kit* portable se denomina "F.R.E.D.D.I.E", (Forensic Recovery of Evidence Device Diminutive Interrogation Equipment); consiste en un ordenador portable, más que portátil, especialmente diseñado para la recuperación de datos de todo tipo de dispositivos, con posibilidades de bloqueo de discos para evitar modificaciones accidentales del material estudiado y otras características que lo convirtieron en el equipo ideal. (Más información sobre este dispositivo en <http://www.digitalintel.com/freddie.htm>)

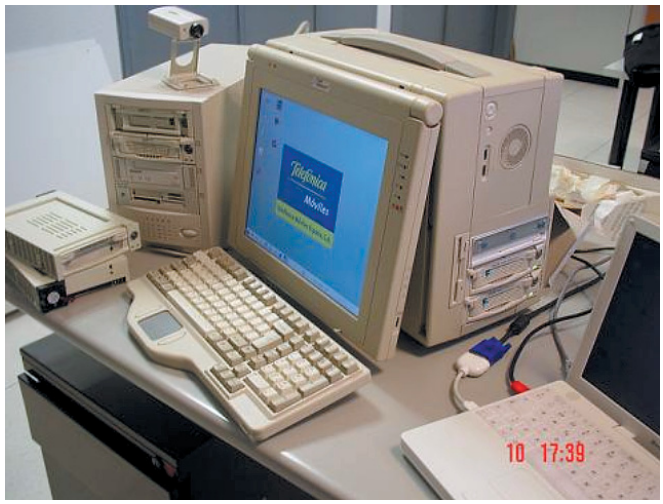


Figura 2: F.R.E.D.D.I.E. con *sidecar*.

Los requisitos mínimos del *kit* forense fueron:

1. Cuaderno: para todo experto forense es imprescindible un lápiz y cuaderno para tomar notas debido a la importancia de obtener una línea temporal de eventos, tanto de los actos realizados por el equipo forense como por el autor del crimen. Sin embargo decidimos que el cuaderno debía ser electrónico por asegurar la cadena de custodia aún más, ya que muchas notas podrían ser contraseñas o datos delicados o reservados que, en caso de pérdida del cuaderno, cualquiera podría obtener. Con un cifrado de los datos estos permanecen aislados de terceros.

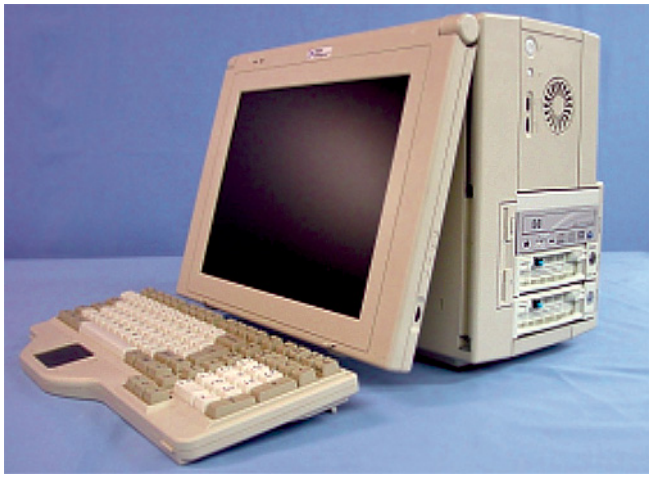


Figura 3: Vista lateral de F.R.E.D.D.I.E. con teclado y pantalla desplegados, (sin *sidecar*).

2. Material de registro y precinto: necesarios para una vez congelada la escena del crimen marcar cada una de las pruebas con etiquetas descriptivas que diferencien de forma única cada evidencia. Se adquirió una grabadora de voz, una cámara fotográfica digital (importante que permita sobreponer a la imagen una fecha, ver **figura 2**) y una etiquetadora. La cámara es muy útil para por ejemplo guardar números de serie de dispositivos comprometidos sin posibilidad de error humano al copiar grandes ristras de números, o para guardar una imagen exacta del contenido de una pantalla de un ordenador comprometido, o de la misma escena del crimen.

3. Equipo portable de análisis forense: el FREDDIE antes comentado. El requisito principal era que fuera un ordenador portable diseñado para duplicar y manejar grandes cantidades de información en múltiples dispositivos, con conectores externos y bahías extraíbles que permitan realizar copias de forma fácil y cómoda, sin necesidad de abrir la carcasa. Importante que disponga de software especializado para adquisición y análisis de datos y características especiales para garantizar la integridad de los datos estudiados, (como por ejemplo el bloqueo hardware de los discos para evitar escrituras accidentales).

4. Conjunto portable de duplicación de discos: elemento sencillo destinado para duplicar discos IDE-IDE e IDE-SCSI, con presentación automática de un informe impreso con datos del disco (número de serie, cilindros, capacidad, fecha y hora de la copia, etc.). Este equipo era interesante porque, aunque ya disponíamos de esta capacidad en FREEDIE, podíamos usarlo para hacer duplicados masivos de servidores clónicos de forma sencilla, o para la simple realización de *backups* de seguridad.

5. Impresora portable, inalámbrica: se adquirió por la importancia del papel y la burocracia en todo proceso judicial, de forma que al disponer de cuadernos electrónicos podríamos llevar ahí los formularios adecuados para cada caso e imprimirlos en la impresora portable (ligera y con batería) vía infrarrojos o *bluetooth* y conseguir así sobre el terreno datos tan importantes como la firma de testigos o rellenar formularios de adquisi-

ción de datos o incidencias por parte de los responsables de los equipos comprometidos.

6. Soporte inalámbrico para todos los dispositivos del kit: era un requisito importante, para ello se estudió minuciosamente cada componente para comprobar que disponía de soporte inalámbrico, (*bluetooth*, infrarrojos o WiFi).

7. Software dedicado para análisis forense: se adquieron herramientas y software útil para el cometido del *kit*, por ejemplo ficheros de firmas digitales de binarios de diferentes sistemas operativos, SMART (software forense comercial para plataformas linux), Autopsy de @Stake, etc.

8. VMWARE: para poder ejecutar sobre entornos controlados y virtuales posibles troyanos o copias de sistemas capturadas durante una investigación.

9. Dispositivos varios: llaveros de almacenamiento masivo por USB, disco USB 2.0 de alta capacidad (80 GB), etc.

Procedimientos

Otro proyecto llevado a cabo durante 2003 fue la realización de la estructura documental de un manual de gestión de incidentes de seguridad.

Este manual es imprescindible para el equipo forense, pues una condición *sine qua non* de la ciencia forense es justamente la existencia de procedimientos y metodologías científicas y sistemáticas para evitar dejar todo a la improvisación en el momento del incidente y minimizar al máximo los posibles errores, producto de la improvisación y trabajo bajo presión en un momento delicado, como podría ocurrir en el caso de sufrir un incidente de seguridad.

Se pretenden definir los procedimientos y políticas a seguir tanto por el IRT cómo por otros departamentos que pudieran verse implicados, antes, durante y después de cualquier posible incidente de seguridad.

El manual es por tanto un compendio de procedimientos para la gestión de incidentes de seguridad por un equipo de respuesta ante incidentes (las siglas en inglés son IRT o CSIRT, acrónimo de *Computer Security Incident Response Team*) con capacidad para respuesta y coordinación en caso de incidentes de seguridad.

La composición básica de este manual está dividido en dos grandes partes, una de procedimientos exclusivamente para el IRT y otra para el resto de departamentos. Se muestra a continuación un resumen:

* Procedimientos para **externos** al IRT:
– Cómo contactar con el IRT.
– Procedimientos de actuación para los centros de relación con el cliente.
– Procedimientos de actuación para asesoría jurídica.
– Procedimiento de actuación para usuario corporativo que encuentra un problema de seguridad.
– Procedimiento de actuación para administradores de sistemas que encuentra un problema de seguridad.

* Procedimientos **propios** del IRT:
– Procedimiento de actuación en caso de compromiso de sistema.
– Procedimiento de recuperación.
– *Scripts* de recogida de información.
– Tabla/árbol de contacto para escalado de incidentes.
– Manual de procedimiento de análisis forense.

Los 'hackers' suelen ser por norma general muy olvidadizos, o quizás confiados; en muchas ocasiones no borran pistas, o al menos no todas. Por ejemplo, es típico encontrar lo que han editado en el ".viminfo", ya que guarda las últimas modificaciones y ficheros accedidos.

A todos estos procedimientos se les añaden formularios de diversos tipos, que deberán ser rellenados por los departamentos afectados por el incidente de seguridad y entregados al IRT. Algunos de estos formularios son de uso tanto para el IRT como para el departamento implicado. La lista de formularios actualmente desarrollados es:

1. Documento de custodia de la evidencia (receptor de la evidencia, testigo, responsable, cadena de custodia, disposición final, etc.).

2. Formulario de identificación de máquina (responsable, ubicación, números de serie, S.O., etc.).

3. Formulario de incidencia (denuncia de un departamento al IRT).

4. Formulario de publicación de incidente (del IRT al resto).

5. Formulario de recogida de datos: atención al cliente. (Por ejemplo si un cliente denuncia un incidente o un *hacker* se pone en contacto, tomar los datos necesarios).

6. Formulario adquisición de datos CISCO (específico para recogida de información útil/volátil de un sistema CISCO).

7. Formulario de discos duros (nº particiones, cilindros, etc.).

8. Formulario de acciones realizadas (bitácora, tanto para el IRT como para el departamento afectado; así conoceremos qué han tocado antes de que el IRT congelara la escena del crimen).

9. Formularios de incidentes tipificados: especiales, dedicados para incidentes tipo SPAM, DoS/DdoS, ataques ingeniería social, contacto con intruso, etc. Hay uno por cada ataque que se pueda encasillar fácilmente.

Recuperación y análisis

Una vez las evidencias digitales han sido recogidas de forma adecuada, precintadas, con un método de localización y recuperación de las mismas (por ejemplo estaría bien tenerlas localizadas en bases de datos), comienza la fase más laboriosa y, probablemente, larga. Un análisis forense de un caso complejo puede durar meses, incluso años.

Debemos procurar trabajar sobre imágenes de discos, esto es así para no trabajar a nivel de sistema de ficheros, pues podemos perder información valiosa, como son los datos que hay en la zona no ocupada del disco o en el espacio residual que hay detrás de cada fichero (recordemos que los ficheros suelen almacenarse por bloques, un fichero de un octeto ocupará un clúster de disco, que en un disquete serán dos sectores de 512 octetos, es decir 1024 octetos, de los cuales sólo se usa 1 octeto, el resto del espacio podría ser usado por un intruso para almacenar información no accesible para las herramientas disponibles con el sistema operativo, pero sí para las herramientas forenses. Por esto es necesario trabajar sobre imágenes, además deben montarse en modo sólo lectura, (Linux permite esto), sistemas como Windows no lo permiten pero podrían usarse dispositivos como el que hemos mencionado (FREDDIE), que permite hacer un bloqueo hardware del disco analizado. La mejor herramienta para realizar los volcados bit a bit es "dd". No hay que olvidar la revisión de todas las partes del disco, incluido swap (o fichero de intercambio).

Las herramientas forenses permitirán recuperar ficheros borrados, por ejemplo se ha recuperado el *exploit* usado durante el reciente compromiso que han sufrido diversas organizaciones como Debian o la FSF. Concretamente la vulnerabilidad afectaba a los núcleos Linux iguales o inferiores a la versión 2.4.22 y se debe a un problema en la comprobación de los límites de la función do_brk(); dicha vulnerabilidad permitía el escalado de privilegios a administrador del sistema. Sin embargo el *exploit* estaba cifrado con un motor

criptográfico (TESO-Engine) y fue necesario la acción de un experto en criptografía para descubrir qué hacía.

En ocasiones nos encontraremos con discos de criminales de los que no podremos obtener mucha información, pues los ficheros más interesantes estarán cifrados con software criptográfico como PGP, un software de cifrado basado en clave pública y privada creado por Philip Zimmerman, que ni siquiera agencias como el FBI o la CIA tienen capacidad para atacar en un plazo de tiempo razonable.

Este es uno de los problemas que encontrará el analista forense; las técnicas anti-forense son cada vez más avanzadas, pudiendo eliminar un fichero con herramientas tipo "wipe", que sobrescribe múltiples veces un fichero con contenidos aleatorios, cambia el nombre del mismo varias veces y posteriormente lo elimina del disco. Con este tipo de herramientas no podríamos recuperar ficheros borrados, salvo que tengamos acceso a un carísimo microscopio de efecto túnel o de barrido, capaz de buscar patrones magnéticos que quedan de forma persistente, aunque sólo son efectivos para recuperar ficheros sobrescritos unas 8 ó 10 veces.

Existen muchas más técnicas de ocultación de información, una de las más interesantes es la ocultación en imágenes mediante técnicas conocidas como esteganográficas.

Nuestro objetivo es crear la línea temporal de eventos de lo ocurrido durante el compromiso. Para ello debemos tomar nota de la hora del sistema, por si no estuviera bien sincronizado (de hecho un buen *hacker* lo primero que haría sería tratar de modificar la hora para que no cuadren los *logs* o ficheros de auditoría del sistema). Existen técnicas para cambiar la fecha de un fichero (véase orden touch). Para crear la línea de eventos temporales, las herramientas forenses como Autopsy utilizan las conocidas como MAC times, propiedades de los ficheros que indican cuándo se ha modificado, accedido o cambiado (por ejemplo el propietario), muy importantes para la resolución del caso.

Debemos utilizar binarios estáticos, sobre todo durante la recogida de datos volátiles del sistema comprometido, pues un sistema comprometido no es confiable. Existen *rootkits* y módulos de *kernel* que falsifican la salida ocultando al administrador los procesos intrusos en el sistema, últimamente muy avanzados y difíciles de detectar.

Es importante comparar las huellas digitales (MD5 o SHA1) de los binarios del sistema comprometido con las huellas de un sistema similar sano; existen bases de datos de firmas de ficheros buenos conocidos (una web interesante en este sentido es: <http://www.knowngoods.org/>), también existen firmas de ficheros malos conocidos, de forma que podemos buscar ficheros delictivos (por ejemplo una foto típica de pornografía infantil) de forma muy rápida en un disco duro.

Es muy interesante poder ordenar los ficheros de diversas formas, por ejemplo por tipo de fichero (según extensión, según salida de la orden "file", etc.), por i-nodos (un sistema instalado hace meses y comprometido recientemente, presentará i-nodos muy distintos en los nuevos ficheros que aparezcan en directorios tipo /bin, etc.

No se debe acusar al propietario de una IP hasta tener evidencias firmes de su implicación; con esto quiero resaltar que hay que tener mucho cuidado con los falsificadores de *logs*, pues a veces hace más daño modificar un *logs* que borrarlo.

Los ordenadores del equipo forense en los que se estudiarán las evidencias deberían disponer de una red propia aislada del resto de la red corporativa.

De todas formas los *hackers* suelen ser por norma general muy olvidadizos, o quizás confiados; en muchas ocasiones no borran pistas, o al menos no todas. Por ejemplo, es típico encontrar lo que han editado en el ".viminfo", ya que guarda las últimas modificaciones y ficheros accedidos.

No olvidemos que todas las hipótesis que planteemos deberán ser probadas. La mejor forma de convencer al juez y anular a la defensa es aportar toda la información rigurosa posible.

PERFILES

Últimamente se le da mucha importancia a los modelos de comportamiento;, lo cierto es que si se conoce cómo trabaja un *hacker* es probable conseguir un ahorro de trabajo, pues todos somos humanos y tendemos a tener costumbres. Sin embargo el analista forense debe huir de las costumbres y no dar nada por supuesto.

En de resaltar la moda que hay últimamente y que consiste en *hackers* que quizás no se conocen de nada pero que en La Red quedan e intercambian información, por ejemplo un *hacker* español pide a uno rumano que realice una exploración de su máquina víctima y le facilite los resultados, de esta forma el *hacker* español evita comprometerse, y el *hacker* rumano no tiene problemas, pues en su país no hay legislación para este tipo de delitos.

Los perfiles que podemos encontrar abarcan desde el *hacker* experto, hasta el *script* kiddie, que ejecuta las herramientas automáticas que han programado los expertos. A los investigadores suele serles muy útil conocer las motivaciones y patrones típicos de comportamiento para localizar a un criminal.

CONCLUSIONES

La falta de diversidad en los distintos entornos operativos provoca un efecto dominó, en el que las amenazas contra las vulnerabilidades una vez hechas públicas se extienden en pocos minutos por medio mundo, haciendo muy difícil conocer el origen del problema, aunque esta falta de diversidad, a su vez, facilita el estudio forense de los sistemas, ya que la existencia de una plataforma mayoritaria hace más fácil procedimentar el análisis de entornos homogéneos. Esta falta de diversidad nos hace débiles y vulnerables, provocando que muchas empresas estén comprometidas desde meses sin ser conscientes de ello.

No hay que presuponer que nunca va a pasar nada, pues no basta con poner medidas de seguridad y confiar en que nadie "pasará"; se debe suponer que algún día tendremos un problema y debemos estar preparados para afrontarlo.

Cualquier empresa que disponga de un IRT bien formado y equipado para realizar análisis forense tendrá más posibilidades de éxito en incidentes de seguridad. Es imprescindible en empresas que están en la cresta de la ola y necesitan estar atentas a cualquier intento de espionaje o sabotaje industrial, tráfico de información, etc.

Para montar un IRT se necesita un equipo de expertos, facilitarles el entrenamiento y material que necesiten para su trabajo, definir unos procedimientos sistemáticos y científicos de gestión de incidentes de seguridad y darlos a conocer a toda la organización. ■

Antonio Javier García Martínez
Experto en seguridad de redes y servicios
Gerencia de Seguridad de Redes y Servicios
TELEFÓNICA MÓVILES ESPAÑA
garcia_aj2@tsm.es