Computación forense: Una revisión general de sus fundamentos y aproximaciones

Miguel P. Torrealba S.*
Nandy Devenish G.**

Sumario

Introducción

Desde el punto de vista práctico de un técnico en computación, la computación forense es definida como una serie de procedimientos que permiten, en lo posible, recopilar y analizar datos de un modo tal que los mismos estén libres de distorsión o de cualquier contaminación, para así poder reconstruir otros datos o para determinar lo que sucedió anteriormente en un sistema de

* **Universidad Simón Bolívar**, Profesor Asociado del Departamento de Computación y Tecnología de la información. Consultor de Seguridad de Computadoras y Redes. Miembro de la Red Temática Iberoamericana «Criptored». mtorrealba@usb.ve.

** **Universidad Central de Venezuela**, Abogada. Cursando una Especialización en Ciencias Penales y Criminológicas. **Ministerio Público**, Abogado Adjunto III de la Unidad Criminalística contra la Vulneración de Derechos Fundamentales del Área Metropolitana de Caracas. nandyanubis@gmail.com.

computación[1]. Por otra parte, desde el punto de vista criminológico la computación forense es un macro procedimiento que permite identificar, preservar, analizar y presentar evidencias digitales de forma que puedan aceptarse legalmente[2]. Y es que para el mundo académico la computación forense es una rama de la ciencia forense digital[3], cuya razón de ser es fundamentar adecuadamente los correctos y estrictos procesos que conducen a satisfacer los requerimientos legales en el ámbito digital de los sistemas judiciales. Esta necesidad se debe a la creciente tendencia en el mundo de castigar los crímenes que se realizan con apoyo de computadores o de dispositivos digitales. Esto, a su vez, es una consecuencia de la ubicuidad de computadores y del incremento de acceso a la Internet. De modo que, desde mediados de los años 80, algunas cortes judiciales en diversos países del mundo se han visto en la necesidad de incorporar a peritos en electrónica o computación como parte de los expertos que testifican o avalan la actividad que ocurrió en computadores y redes electrónicas.

Huebner *et alter* señalan que el primer registro de un juicio vinculado con un crimen de computadores se refiere a 1966 en Texas[4] y comentan que las primeras herramientas eran tan simples como un editor hexadecimal. El incidente tuvo una repercusión local y no es muy conocido. En la actualidad, el Instituto Nacional de Justicia de los EE UU (NIJ) participa en el programa de Pruebas de Herramientas de Computación Forense (CFTT) y publica en Internet los resultados de cada evaluación de los instrumentos forenses más reconocidos,

---

1 Farmer, Dan: *Computer Forensic Analysis Class. Introduction*. Láminas de apoyo de una clase libre. 1999, http://www.porcupine.org/forensics/intro.ps.

2 McKemmish, Rodney: «*What is forensic computing*?». En: *Trends and issues in Crime and Criminal Justice*. Nº 118. 1999, http://www.aic.gov.au/media_library/publications/tandi_pdf/tandi118.pdf.

3 Leigland, Ryan. y Krings, Axel: «*A formalization of digital forensics*». En: *International Journal of Digital Evidence.* Vol. 3, Nº 2. 2004, http://www.utica.edu/academic/institutes/ecii/publications/articles/A0B8472C-D1D2-8F98-8F7597844CF74DF8.pdf.

4 Huebner, Ewa; Bem, Derek y Bem, Oscar: *Computer Forensics. Past, Present and Future*. 2007, https://cld.pt/dl/download/a87a98a2-4b85-46b7-8df6-6ac213bbc201/English/Security%20%26%20Hacking/Computer%20Forensics%20-%20Past%20Present%20Future.pdf.

en un modo público[5]. A pesar de ese avance, aún no se dispone de un estándar reconocido en el área.

De manera que, aunque en la práctica esta actividad se ha venido realizando, aún adolece de cierta madurez teórica, por lo que debemos empezar definiendo esta misma actividad. En este trabajo, la computación forense es considerada como una disciplina que combina conocimientos teóricos y prácticos, métodos –algunos formales y otros heurísticos–, procedimientos reconocidos, herramientas computacionales, al igual que la experiencia humana en investigaciones con orientaciones legales, para presentar evidencias digitales o electrónicas que puedan sustentar posturas específicas ante un tribunal.

1. La informática forense en el proceso penal venezolano

Entendiendo el término «forense» como lo concerniente al foro –en la antigua Roma–, es decir, a los tribunales y sus audiencias, se puede colegir *latu sensu* a la actividad forense como aquella que aplica diferentes ramas y áreas del conocimiento para coadyuvar con la resolución de controversias en el ámbito jurídico.

En Venezuela, desde la perspectiva procesal penal y por mandato constitucional, nos regimos por un sistema acusatorio en el cual la titularidad de la acción penal recae sobre el Ministerio Público, quien, respetando las diferentes fases del proceso, iniciará y realizará la investigación pertinente. Esta tiene como alguna de sus principales características los principios de licitud y libertad probatoria, contemplados en los artículos 181 y 182 del Código Orgánico Procesal Penal de 2012 vigente, respectivamente, a saber:

> Artículo 181.- Los elementos de convicción solo tendrán valor si han sido obtenidos por un medio lícito e incorporados al proceso conforme a las disposiciones de este Código.

[5] *Vid*. http://www.nij.gov/publications/pages/publication-list.aspx?tags=Electronic%20Crime%20-%20Cybercrime.

> No podrá utilizarse información obtenida mediante tortura, maltrato, coacción, amenaza, engaño, indebida intromisión en la intimidad del domicilio, en la correspondencia, las comunicaciones, los papeles y los archivos privados, ni la obtenida por otro medio que menoscabe la voluntad o viole los derechos fundamentales de las personas. Asimismo, tampoco podrá apreciarse la información que provenga directa o indirectamente de un medio o procedimiento ilícitos.
>
> Artículo 182.- Salvo previsión expresa en contrario de la ley, se podrán probar todos los hechos y circunstancias de interés para la correcta solución del caso y por cualquier medio de prueba, incorporado conforme a las disposiciones de este Código y que no esté expresamente prohibido por la ley.
>
> Regirán, en especial, las limitaciones de la ley relativas al estado civil de las personas.
>
> Un medio de prueba, para ser admitido, debe referirse, directa o indirectamente, al objeto de la investigación y ser útil para el descubrimiento de la verdad. Los tribunales podrán limitar los medios de prueba ofrecidos para demostrar un hecho o una circunstancia, cuando haya quedado suficientemente comprobado con las pruebas ya practicadas.
>
> El tribunal puede prescindir de la prueba cuando ésta sea ofrecida para acreditar un hecho notorio.

Lo precedentemente citado, hace referencia a que se podrán probar todos los hechos y circunstancias de interés para la correcta solución del caso y por cualquier medio de prueba, incorporado conforme a las disposiciones de ese Código y que no esté expresamente prohibido por la ley, entendiéndose esa incorporación, en el sentido que los elementos de convicción deben cumplir con dos características concurrentes: haber sido obtenidos por un medio lícito e incorporados al proceso conforme a las disposiciones legales.

En resumen, el proceso penal no establece un mecanismo único en su régimen probatorio, lo cual abre la posibilidad de probar «todo con todo» siempre y cuando se respete el debido proceso y las garantías constitucionales que caracterizan a este sistema acusatorio[6].

Este afán del sistema acusatorio por respetar esos derechos y garantías constitucionales en aras de alcanzar la finalidad del proceso penal, la cual es establecer la verdad de los hechos por las vías jurídicas, y la justicia en la aplicación del Derecho, se desprende del contenido del artículo 13 del Código Orgánico Procesal Penal. Es por ello que se entiende que con la sola actuación del profesional de derecho se limitaría ampliamente alcanzar este fin. De modo tal, que se recurre a especialistas de otras áreas, quienes aplicarán sus conocimientos en este sentido regulados por las leyes establecidas para este propósito. Esta figura es denominada por el Código Orgánico Procesal Penal como «peritos», y se describe de la siguiente manera:

> Artículo 224.- Los o las peritos deberán poseer título en la materia relativa al asunto sobre el cual dictaminarán, siempre que la ciencia, el arte u oficio estén reglamentados. En caso contrario, deberán designarse a personas de reconocida experiencia en la materia.
>
> Los o las peritos serán designados o designadas y juramentados o juramentadas por el juez o jueza, previa petición del Ministerio Público, salvo que se trate de funcionarios adscritos o funcionarias adscritas al órgano de investigación penal, caso en el cual, para el cumplimiento de sus funciones bastará la designación que al efecto le realice su superior inmediato.
>
> Serán causales de excusa y recusación para los o las peritos las establecidas en este Código. El o la perito deberá guardar reserva de cuanto conozca con motivo de su actuación.

---

6 *Vid*. TSJ/SC, sent. Nº 3167, del 09-12-02, http://historico.tsj.gob.ve/decisiones/scon/diciembre/3167-091202-02-2154.HTM.

> En todo lo relativo a los traductores o traductoras e intérpretes regirán las disposiciones contenidas en este artículo.

Se trata, entonces, de profesionales ajenos al área jurídica, quienes mediante una juramentación realizada por el órgano jurisdiccional ingresan al proceso penal, al ser reconocidos empírica y/o académicamente como conocedores de una ciencia u oficio específico y que pueden ayudar a esclarecer asuntos vinculados a la investigación realizada sobre la presunta comisión de un hecho punible.

En ese abanico de posibilidades es donde la informática forense, a través de su método científico y herramientas anteriormente señaladas, atendiendo a un hecho que sea objeto de investigación, prestará sus servicios al «foro». Su participación en el proceso penal se da mediante la realización de experticias definidas por el Código de la forma descrita a continuación:

> Artículo 223.- El Ministerio Público realizará u ordenará la práctica de experticias cuando para el examen de una persona u objeto, o para descubrir o valorar un elemento de convicción, se requieran conocimiento o habilidades especiales en alguna ciencia, arte u oficio.
>
> El o la Fiscal del Ministerio Público, podrá señalarle a los o las peritos asignados, los aspectos más relevantes que deben ser objeto de la peritación, sin que esto sea limitativo, y el plazo dentro del cual presentarán su dictamen.

De allí que el ahora perito, o también conocido como «experto», vaciará el procedimiento, análisis y conclusiones de lo practicado en lo que se denomina un dictamen o informe pericial, con las características requeridas en el artículo 225 *eiusdem*, a saber:

> Artículo 225.- El dictamen pericial deberá contener, de manera clara y precisa, el motivo por el cual se practica, la descripción de la persona o cosa que sea objeto del mismo, en el estado o del modo en que se halle, la relación detallada de los exámenes practicados, los resultados obtenidos y las conclusiones que se formulen respecto del

> peritaje realizado, conforme a los principios o reglas de su ciencia o arte.
>
> El dictamen se presentará por escrito, firmado y sellado, sin perjuicio del informe oral en la audiencia.

Una vez realizado el informe pericial y remitido para su incorporación en el expediente del tribunal, el perito debe cumplir con la última fase de su participación en el proceso, la declaración en el juicio oral y público o privado, según sea el caso, sobre el peritaje realizado, en la forma que refiere el artículo 337 *eiusdem*. Éste señala que en su declaración debe responder directamente a las preguntas que formulen las partes y el tribunal, y cuenta con la posibilidad de consultar notas y dictámenes, sin reemplazar con esa lectura su declaración. Es este el momento para que los expertos aporten los datos de interés que sirvan como elementos de convicción del hecho investigado y que concatenados con los otros elementos expuestos en el juicio oral, serán valorados por el juez de juicio mediante la «sana crítica». El procedimiento se hará tomando en consideración los conocimientos científicos expuestos por el informático forense, en este caso, observando las reglas de la lógica y las máximas de experiencia, tal como lo prescribe el artículo 22 del Código Orgánico Procesal Penal.

Ahora bien, la era moderna se ha caracterizado por el despliegue tecnológico y el uso de equipos móviles inteligentes o *smartphones*, así como cámaras digitales y de seguridad. Su uso masificado brinda una mayor oportunidad de registro de eventuales hechos acaecidos en lugares concurridos, o donde se disponga de estos equipos. Es así como el análisis de los mismos, mediante el uso de la informática forense, se ha proyectado como vanguardia en el despliegue investigativo de delitos que son cometidos en las calles y filmados por algún transeúnte, testigo o cámaras de seguridad.

De igual manera, en algunos de los delitos previstos en la Ley contra el Secuestro y la Extorsión y la Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo, la informática forense ha participado de forma activa mediante la intervención de las comunicaciones, previa orden

judicial, o con el análisis y vaciado de contenido de las evidencias de origen informático que sean colectadas por los órganos de investigación.

Además, en Venezuela se cuenta con la Ley Especial contra Delitos Informáticos[7], la cual tiene como objeto:

> Artículo 1.- La protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías, en los términos previstos en esa ley.

En esta Ley se cuenta con un glosario de términos relacionados al área, así como un catálogo de 20 delitos, desarrollados en los capítulos siguientes: I. De los delitos contra los sistemas que usan tecnologías de información; II. De los delitos contra la propiedad; III. De los delitos contra la privacidad de las personas y las comunicaciones; IV. De los delitos contra niños, niñas o adolescentes, y V. De los delitos contra el orden económico.

En este sentido, se puede clasificar una categoría de delitos especiales, determinados por su medio de comisión y naturaleza, lo que antes podría ocasionar un obstáculo a la investigación penal. Sin embargo, con colaboración de la informática forense y sus expertos, pueden ser desentrañados desde la perspectiva probatoria y, aunque se entiende que no lo es todo, generar un aporte que se adminiculará posteriormente con los otros medios de prueba promovidos para llegar a una conclusión ajustada a Derecho.

Pero ¿cuál es la naturaleza de este aporte? Para responder a ello debe aclararse, en primer lugar, que evidentemente no se trata de un aporte jurídico, sino técnico científico, que puede coadyuvar en la elaboración de la tesis investigativa del medio o móvil de comisión de un hecho punible, creando, fortaleciendo o eliminado el nexo causal entre el presunto sujeto activo del delito y el hecho acaecido. El profesional del Derecho tomará este aporte para verificar si existió por

[7] *Gaceta Oficial de la República Bolivariana de Venezuela* Nº 37313, del 30-10-10.

parte del presunto autor una «conducta», entendiendo a esta como un acto exteriorizado procedente de un ser humano, dado que el pensamiento no puede ser sancionado –*cogitationis poenam nemo patitur*– y que este acto sea conducible por la voluntad[8].

De igual manera, las conclusiones elaboradas por el experto informático forense pueden colaborar con las partes a determinar una vez que se constate que efectivamente hubo una conducta, si sus características se adecúan de manera tal que pueda considerársele como típica, y si puede determinarse la existencia de un error de tipo o de prohibición. Es decir, que puede generar luces que hagan al jurista establecer su dictamen jurídico basado en el análisis de la teoría del delito.

2. Límites de la computación forense

Por la propia naturaleza de los sistemas computacionales modernos y redes de computadoras, la potencial evidencia digital que sobre ellos reside o transita es dinámica[9] y volátil[10]. Mientras que un registro interno de una Unidad Central de Procesamiento (CPU) puede almacenar un dato como es la dirección en Memoria de Acceso Aleatorio (RAM) de la próxima instrucción a ejecutar y nanosegundos más tarde cambiar ese valor, tradicionalmente un Disco de Vídeo Digital (DVD), conocido como «memoria secundaria», es capaz de almacenar el contenido interno de un archivo de datos por décadas. De modo que dependiendo de la naturaleza física, y primordialmente del funcionamiento del elemento constituyente de un equipo electrónico, los *bits*[11] que sobre él se procesen persistirán por tiempo limitado. Adicionalmente, la desaparición de estos tiende a ocurrir cuando otros valores se colocan sobre el espacio que anteriormente se les había otorgado a ellos.

---

8 Modolell, Juan: *Derecho Penal.Teoría del Delito*. UCAB. Caracas, 2015, pp. 27 y ss.

9 Casey, Eoghan: *Handbook of digital forensics and investigation*. Academic Press. Massachusetts, 2009.

10 Farmer, Dan y Venema, Wietse: *Forensic discovery*. Addison-Wesley Professional. New Jersey, 2005.

11 Unidad mínima de información que procesa un dispositivo digital y que solamente acepta dos valores: «uno» o «cero».

Así pues, es común que un investigador de computación forense se enfrente a la complicada situación de que los computadores ejecutan programas constantemente y con ello cambian sus estados, incluso cuando no tienen ningún usuario final interactuando con ellos. Otra situación que también resulta un reto durante un examen forense es cómo establecer la autenticidad de lo que se recopila. En su esencia básica, el mundo digital únicamente procesa *bits*, secuencias de *bits*. Todo se maneja con el sistema de numeración binario y las conversiones permiten trasladar números decimales o caracteres a patrones de *bits* y viceversa. Físicamente, un *bit* es un elemento electrónico o magnético con varias características específicas, por lo cual no se diferencia de otro por su naturaleza en sí, sino por la posición que ocupa dentro de la secuencia. Cuando un *bit* sustituye a otro en la misma posición, lo único que lo diferencia es la línea del tiempo en que ocupó ese espacio. De forma que si un investigador no puede precisar en forma lícita, verificable y confiable esa temporización, no será capaz de recabar evidencia digital.

Todo esto deja planteada una pregunta más en el inicio de cada investigación forense: ¿lo que se va a detectar es lo que sucedió o lo que se desea hacer creer que aconteció? La solución a esta interrogante viene dada por el estricto y temprano cumplimiento de los procedimientos que preservan el estado original del sistema. Una cadena de custodia (artículo 187 del Código Orgánico Procesal Penal) que es parte de esto, resulta vital para aquellos casos en donde las evidencias deben ser traspasadas entre diferentes sujetos.

En lo referente a recuperar información supuestamente eliminada, también existen límites en este campo. Los sistemas digitales de hoy en día permiten borrar información en diferentes formas, siendo algunos mecanismos los que facultan a un usuario final, revertir fácilmente lo hecho, mientras que otros exigen un esfuerzo profundo y muy especializado para obtener algo[12]. Así por ejemplo, se puede optar por alternativas que van desde colocar la información

[12] Gutmann, Peter: *Secure deletion of data from magnetic and solid-state memory*. *Sixth Usenix security symposium proceedings*. 1996, https://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html.

a borrar en una «papelera virtual de reciclaje», hasta incinerar discos o sumergirlos en ácido. Pero si lo que se desea es eliminar información en un disco que seguirá siendo usado, existen variadas opciones. Por ejemplo cifrar la información o usar el comando *shred*[13] de Linux, que sobrescribe varias veces el espacio originalmente ocupado[14] con patrones pseudoaleatorios. Aquí nuevamente resulta crucial comprender que la línea de tiempo es lo que permite identificar un *bit* de su predecesor.

Otro tema que recientemente se discute en el mundo académico es si algunas tendencias modernas de la informática –la nube, el almacenamiento masivo de datos, la proliferación de formatos para registrar los datos y el aumento de *software* maligno que no requiere persistir en la memoria secundaria– van a conducir a una crisis a la computación forense[15]. Es decir, esta área demanda nuevos estándares y nuevas aproximaciones modulares para procesar datos y modelar nuevas investigaciones en este campo.

3. La confianza como elemento central de los descubrimientos forenses

Todo sistema de seguridad tiene una raíz de confianza[16] y para la computación forense esta sentencia también aplica. Comúnmente se establece una relación de confianza hacia las herramientas que usa el técnico durante el proceso, e incluso hacia él mismo. Y aunque ello puede ir precedido de una revisión detallada de las herramientas que se utilizarán, conocida como esterilizar el instrumental, o de la grabación y supervisión de cada parte del proceso

[13] En español, el nombre comando se puede traducir como trizas, tiras o pedazos. La idea es hacer trizas el contenido del archivo que se elimina, a razón de que más tarde este no pueda ser reconstruido.

[14] Dependiendo del tipo de Sistema de Archivos de Linux o de ciertas condiciones, puede ser que el comando *shred* sobrescriba áreas diferentes a las originales. Esto quiere decir que también existen límites para este tipo de herramientas de *software*.

[15] Garfinkel, Simson: «*Digital forensics research: the next 10 years*». En: *Digital Investigation 7*. 2010, http://dfrws.org/2010/proceedings/2010-308.pdf.

[16] Garfinkel, Simson; Spafford Gene y Schwartz, Alan: *Practical Unix & Internet Security*. 3ª, O'Reilly Media. California, 2003.

en sí, en general, si se emplean instrumentos reconocidos –preferiblemente del tipo *software* libre[17] y con algoritmos clásicos– y se cumple con los estándares del área, entonces se otorga confianza en los resultados que se produzcan. Así por ejemplo, si se hace una imagen de un disco empleando el comando dd (*Dataset Definition*) del sistema operativo *GNU Linux*®[18], o si se verifica la integridad de un archivo a través de una herramienta que internamente use el algoritmo md5 (*Message-Digest Algorithm 5*)[19], la mayoría de los tribunales concederá que los resultados que se obtengan con ellos son confiables.

En lo que respecta al propio ejecutor de la investigación, de trasfondo está planteado la confianza inicial en su comportamiento ético e íntegro[20], y ello resulta acorde con el histórico desempeño de otras ramas profesionales autorizados para los trabajos forenses.

4. La combinación de destrezas es requisito de un experto en computación forense

Los técnicos experimentados en el área combinan saberes propios de la computación con el de los detectives, y ello no es la única tarea que impone ese cruce. La identificación de fallas de programación, conocidas comúnmente como *bugs*, también lo hace. Y es que descubrir y reconstruir una serie de acontecimientos demanda observar, suponer hipótesis, buscar, razonar, hilar señales, analizar y comprobar. Pero también exige conocer los sistemas computacionales en detalles y aplicar técnicas sofisticadas. Se mezclan así elementos provenientes de una ciencia determinista con la subjetividad humana[21] y se pro-

---

17 Con el *software* libre se tiene acceso al código fuente del sistema, por lo que se puede examinar la constitución en sí del mismo. Se dispone de una técnica preventiva o para estudiar cada instrucción que se ejecutará o que se procesó.

18 Negus, Chris: *Linux Bible. 2010 Edition*. Wiley Publishing, Inc. Indianapolis, 2010.

19 Rivest, R.: *The MD5 Message-Digest Algorithm*. Request for Comments 1321. 1992, http://www.ietf.org/rfc/rfc1321.txt.

20 Kishore, Neha; Gupta, Chetna y Dawar, Dhvani: «*An Insight view of Digital Forensics*». En: *International Journal on Computational Sciences & Applications (IJCSA)*. Vol. 4, Nº 6. 2014, http://airccse.org/journal/ijcsa/papers/4614ijcsa08.pdf.

21 García, Juan: *Un forense llevado a juicio*. 2012, http://www.fluproject.hol.es/descargasDirectas/pdf/Un%20forense%20llevado%20a%20juicio.pdf.

vee espacio para hacer uso de la imaginación, sin violentar el marco legal que limita los procedimientos a emplear. Pero la subjetividad ha de limitarse para adaptar la investigación y llevarla a una conclusión correcta, pero nunca para identificar o interpretar los resultados.

En la práctica, situaciones extraordinarias pueden suceder, tales como que la investigación esté dirigida por sujetos con poco conocimiento técnico, que deliberadamente o por incapacidad, limiten u orienten el trabajo en un modo que no arroje resultados reales. La conocida diferencia de enfoque sobre cómo hacer el trabajo entre el físico Richard FEYNMAN y el abogado William ROGERS durante la investigación de las causas de la tragedia del transbordador espacial «Challenger», entorpecieron notablemente ese esfuerzo desde los primeros días e hicieron que el físico ganador del Premio Nobel pensara que el resultado sería un fracaso técnico, pero que serviría a las necesidades políticas en Washington[22].

Así que el valor de un investigador en esta área técnica obedece más a la actitud, la conducción profesional, la acumulación de conocimientos específicos y la experiencia real que se tenga que al empleo de herramientas de computación forense. Es decir, poseer un dominio notable de un instrumento como *Encase® Forensic* no basta para transformar a un técnico de computadoras en un experto de la computación forense, al igual que disparar con tino un revólver no transforma al sujeto con esa habilidad en un policía. El entendimiento profundo de la estructura de los múltiples Sistemas de Archivo (*File Systems*), al igual que el funcionamiento de los protocolos de comunicaciones del TCP/IP, son, en nuestros días, frecuentemente necesitados en cualquier investigación. Ello sucede porque la mayoría de los archivos son almacenados en memoria secundaria y es común que las redes de computadoras modernas se comuniquen con la Internet. Así pues, un archivo almacenado en un teléfono inteligente se guarda en un sistema de archivos local, en modo parecido a como un archivo de computadoras se deposita en la nube.

[22] FEYNMAN, Richard: *What do you care what other people think*? 1988, http://202.114.108.237/Download/d84fa222-921a-43de-a8f3-87388597371e.pdf.

Aquí la diferencia principal es que para este último escenario el sistema de archivos está ubicado remotamente. Las diferencias estructurales entre los archivos o de los sistemas de archivos son variaciones que demandan destrezas técnicas peculiares para poder procesar su contenido, pero el fenómeno en sí responde a la misma necesidad. Entonces, los instrumentos sofisticados pueden facilitar el proceso de recopilar, visualizar, buscar y presentar los datos, pero la lógica, el análisis y la interpretación de lo que se obtiene son procesos vinculados al investigador. Incluso hay autores que sostienen que hay destrezas y habilidades que se pueden aprender, mientras que hay talentos con los cuales se nace, por ejemplo, lo que denominan coloquialmente «el olfato del investigador»[23].

Como una investigación puede demandar muchos saberes técnicos, puede resultar necesario coordinar el trabajo en equipo. Existen diversas propuestas y también una ontología para escenarios de misiones complejas[24]. Algunas se enfocan en expertos por áreas, como telefonía celular, tabletas, portátiles, computadores de servicios, dispositivos de interconexión, entre muchas, mientras que otras se inclinan por individuos con capacidad de desarrollar diferentes roles, el del intruso, el administrador y el investigador a medida que avanza el trabajo[25]. Es decir, se debe tener la capacidad para pensar como el que supuestamente habría cometido el delito, también como el que había configurado el sistema que se examina y como el experto que descubre las evidencias. Bajo uno u otro modo, el proceso forense en computación es lo que en sí constituye la razón de ser del trabajo. Y para ello, el análisis táctico combinado con el pensamiento estratégico se convierte en un proceso vital de todo trabajador de la investigación forense digital[26].

---

23 SHINDER, Debra: *Scene of the cybercrime. Computer forensics handbook*. Syngress Publishing, Inc. Ed TITTEL, editor. Massachusetts, 2002.

24 NOGUEIRA, José y VASCONCELOS, Wamberto: «*Ontology for complex mission scenarios in forensic computing*». En: *The International Journal of Forensic Computer Science, IjoFCS*. Vol. 3, Nº 1. 2008, http://www.ijofcs.org/abstract-v03n1-pp04.html.

25 CANO, Jeimy: *Computación forense. Descubriendo los rastros informáticos*. Alfaomega Grupo Editor. México D.F., 2009.

26 GARFINKEL: ob. cit. («*Digital forensics research*…»), *passim*.

5. Principios y estructura del proceso forense

La computación forense existente se sostiene con base en el principio enunciado por Edmond LOCARD: «Siempre que dos objetos entran en contacto, transfieren al otro objeto parte del material que incorporan», o dicho en modo más simple: «Todo intercambio o contacto deja su traza»[27]. De esta forma, se parte de la idea de que toda actividad digital o electrónica registrará señales o signos de qué aconteció y, posiblemente, de cómo y cuándo sucedió. Ello es lo que un investigador busca en distintos lugares, cuidando en extremo no trastocar la potencial evidencia y también evitando destruirla después de que la recolecte. El producto revelado se logra hacer visible y se expone con un significado, para que aporte información en un tribunal. Tradicionalmente, ello acontece ante personal no necesariamente experto en la ejecución tecnológica de los crímenes electrónicos, lo cual significa que incluye un proceso de exposición simplificada, pero sin perder la esencia de lo importante. Adicional a esto, el grupo investigador documenta su proceder, por si él mismo es puesto en tela de juicio[28]. Esta labor demanda un entrenamiento que va más allá de lo meramente técnico, ya que buscar evidencias conforma también una tarea detectivesca. Se deben encontrar, identificar y organizar todas las piezas de un rompecabezas hasta darle sentido sólido a la explicación de una averiguación. Por lo tanto, este tipo de trabajo comúnmente se enmarca dentro de un proceso de investigación mayor. Es así como en su obra *Evidencia digital y crimen en computadoras* los especialistas CASEY, DUNNE y MATTEI discuten su eficacia final:

> La evidencia digital es usualmente circunstancial y hace dificultoso atribuir la actividad en un computador a un individuo. Por lo tanto, la evidencia digital puede ser solamente un componente de una investigación sólida. Si un caso se sostiene sobre una única forma de fuente de

[27] CHISUM, Jerry y TURVEY, Brent: «*Evidence dynamics: Locard's exchange principle & crimen reconstruction*». En: *Journal of Behavioral Profiling*. Vol. 1, Nº 1. 2000.

[28] National Institute of Justice: *Electronic crime scene investigacion. A guide for firts responders*. 2001, https://www.ncjrs.gov/pdffiles1/nij/187736.pdf.

> evidencia digital, tal como la fecha y hora asociada con archivos de computadores, entonces ese caso es inaceptablemente débil[29].

Para poder establecer con rigurosidad lo que aconteció, se requiere disponer con antelación de la capacidad para hacer una traza del pasado. Este procedimiento se acostumbra a designarlo como trazabilidad. Este concepto está muy vinculado al de auditoría de la tecnología de la información, ya que el primero hace factible al segundo. Sea porque el fabricante del sistema colocó anticipadamente mecanismos para registrar ciertas actividades del sistema o porque el examinador logra coleccionar ciertas datos, que puestos coherentemente en una misma línea del tiempo permiten establecer el origen y cómo transcurrieron los hechos, la traza se constituye en el eje central de lo que se señalará finalmente, ya que lo que se indique deberá diferenciarse de eventos fortuitos o meras coincidencias. Para lograr eso es común que el investigador fije su atención en un número limitado de objetos y se enfoque en descubrir cómo se desempeñaron estos en un lapso[30].

De modo que, en su sentido tradicional, computación forense trata de un proceso de investigación que apoya a otro mayor y en el que cada caso debe ser visto como único[31]. A pesar de ello, en modo general, este esfuerzo puede ser descompuesto en cuatro tareas principales:

> i. Obtener una copia fiel del sistema a procesar. Esto va desde recolectar, retener y etiquetar cada elemento involucrado en el caso, hasta obtener imágenes digitales de los discos y cualquier otro tipo de memoria.

---

29 Casey, Eoghan: *Digital evidence and computer crime: Forensic science, computers and the Internet*. 2ª, Academic Press. Boston, 2004.

30 Cano, Jeimy: «Trazabilidad de las operaciones electrónicas. Un reto para la gerencia de tecnologías de la información». En: *ISACA Journal Online*. 2005, http://www.isaca.org/Journal/archives/2005/Volume-6/Documents/jopdf0506-Trazabilidad-de-las.pdf.

31 Casey: ob. cit. (*Digital evidence*…), *passim*.

ii. Recorrer todo su contenido para recabar datos. En algunas ocasiones antes de iniciar esta labor, hay que proceder a eliminar cualquier información que por razones de la política imperante de privacidad de los usuarios, pueda estar en conflicto con el contenido de la imagen fiel[32].

iii. Identificar, analizar, interpretar y comprobar los datos hasta establecer las evidencias o completar la reconstrucción posible de datos. Esta labor es iterativa con la anterior, y se repite mientras el investigador establece que se puede ir más allá.

iv. Presentar o documentar los hallazgos como soporte técnico de un proceso judicial.

Para obtener una copia fiel, los investigadores se enfrentan al primer problema: ¿cómo hacer estático un sistema dinámico por naturaleza? Si el sistema está operando, con cada segundo que sigue activo ciertas operaciones se ejecutan y ello contribuye a cambiar su estado. Por otra parte, si se apaga el sistema algunas potenciales evidencias se perderán. De forma que resulta difícil lograr una solución óptima. En ciertas ocasiones puede intentarse desconectar las conexiones de red y proceder a copiar los discos y examinar la memoria principal, pero ello depende también de si el sistema tolera tales alteraciones. Para aquellos que están en producción y ofrecen servicios en red, es posible que deba procederse mientras este funciona. En caso de que el análisis se fundamente en archivos de bitácoras o datos respaldados, el trabajo dependerá de la política de retención de datos que opere en el lugar de los hechos. En otras situaciones, una política oficial de puesta fuera de servicio y retención del sistema podría facultar a los investigadores para actuar; numerosos cuerpos policiales o de seguridad del Estado hacen uso de esa prerrogativa.

En general, existen dos tipos de análisis forense digital: uno estático y tradicional que se enfoca en la memoria secundaria, y otro más complejo y dinámico

[32] SRINIVASAN, S.: «*Security and privacy* vs. *computer forensics capabilities*». En: *ISACA Journal Online*. 2007, http://www.isaca.org/Journal/archives/2007/Volume-4/Documents/jopdf0704-security-and-privacy.pdf.

que se concentra en la primaria y se llama análisis forense en vivo[33]. Este último puede presentar resultados de difícil credibilidad en un tribunal, ya que estos son difíciles de repetir e incluso podrían variar. Pero para sistemas que se reciben apagados, es más común proceder con el análisis estático y allí lo ideal es copiar las imágenes que se requieren, alterando el arranque normal del sistema. Esto significa que se puede intentar retirar físicamente el disco y colocarlo en un ambiente preparado para replicar, o actuar con una solución más común que es iniciar el sistema con una unidad que se le coloca por algún puerto de *hardware* –comúnmente USB o de red– y que provee facilidades para iniciar y hacer las imágenes. Por citar, *DEFT® Linux*, *CAINE® Linux* o *Wireshark®* son ejemplos del tipo de instrumentos que están disponibles y en modo gratuito en la red de redes.

Es por todo esto que lo ideal es establecer un «plan para obtener los datos»[34] donde se considere el posible valor o importancia de los datos, la volatilidad de estos, el esfuerzo que requerirá obtenerlos, el costo de los mecanismos que deberán emplearse, posibles conflictos con datos que puedan ser considerados privados y el tiempo disponible para ello.

6. Métodos y técnicas comunes en el proceso forense

Toda investigación forense es única, pero existe un conjunto de patrones comunes en el desarrollo de la misma, que constituye en sí un método genérico. Seguidamente, describiremos un caso real paso a paso que ayudará a ilustrar en la práctica cómo se presentan y suceden los hechos. Por razones de ocultar la identidad de la persona jurídica perjudicada, algunos datos serán deliberadamente trastocados, mas no ignorados.

---

[33] Rahman, Shuaibur y Khan. M. N. A: «*Review of live forensic analysis techniques*». En: *International Journal of Hybrid Information Technology.* Vol. 8, Nº 2. 2015, http://www.sersc.org/journals/IJHIT/vol8_no2_2015/35.pdf.

[34] Kent, Karen *et alter*: *Guide to integrating forensic techniques into incident responses*. NIST Special Publication. 2006, http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf.

En general, toda investigación forense cubre los siguientes estados: i. Recepción de la información del caso. ii. Planificación. iii. Obtención del *hardware*, *software* y datos vinculados al caso. iv. Selección de las herramientas y mecanismos a aplicar. v. Búsqueda, recuperación y/o restauración de los datos. vi. Análisis de los datos. vii. Reconstrucción y correlación de los eventos. viii. Revisión y/o ajuste. Si se requiere, hay que repetir, revisar o ampliar la investigación al ir de retorno al punto iii o iv. En caso contrario, se establecen los resultados del trabajo. ix. Elaboración del informe y presentación del caso.

El primer estado se refiere a la recepción de la notificación de que ha sucedido un incidente y que el mismo debe investigarse en su modo forense. Aquí también es importante establecer el objeto de la investigación. Y es que la evidencia que se determine estará dirigida a satisfacer el propósito definido. En nuestro caso de ilustración, una unidad de investigaciones forenses de computación de una institución fue informada de que un consultor jurídico había recibido un mensaje de correo electrónico, con información confidencial aparentemente filtrada y sin poder identificar al remitente. El mensaje anónimo pretendía ser una denuncia de posible corrupción en una negociación. La notificación que recibió el equipo investigador fue emitida por los canales regulares de comunicación empresarial e incluyó la indicación precisa de lo que se esperaba, y ello fue que se identificara al autor del mensaje.

Para el segundo estado, el trabajo se concentra en la planificación de cómo se ejecutará la investigación. Un plan combina datos de entrada, acciones, resultados parciales, instrumentos, verificaciones y elementos a cotejar. Además, decisiones y la presentación de resultados parciales a los superiores inmediatos. Y es que toda planificación es un momento para revisar la información preliminar y formular un plan, que permita dirigir inicialmente la investigación hacia una meta exacta. Hay que determinar los elementos que se requieren encontrar y los ámbitos en donde estos podrían obtenerse. Se debe planear cómo podría completarse el trabajo y cuáles hallazgos serán los que indiquen si se ha alcanzado el objetivo. Los recursos, una estimación del tiempo y los costos deberán ser adicionalmente estimados.

Esta aproximación obliga a buscar la fuente original que identificó el incidente, es decir, entrevistarse directamente con el consultor jurídico y solicitarle además una copia digital del mensaje que recibió. En el inicio de la investigación que se describe, se desconocía por qué se sostenía que el mensaje era anónimo y ello condujo a descubrir la interpretación que los usuarios finales, no los especialistas del área, hacían sobre el fenómeno en sí. ¿Por qué señalaban que el mensaje se consideraba anónimo, si había sido enviado a través de una cuenta de correo electrónico? Para un especialista, la cuenta era una identidad en la red de mensajería por correo digital, pero para el resto era anónimo, ya que no podían señalar directamente a una persona real. Adicionalmente, para ese momento se estableció que era necesario recopilar toda la información asociada que residía en los archivos de bitácora del servidor de correo corporativo, a efectos de cotejar los hechos e ir construyendo una línea de tiempo. Posteriormente, y en función del contenido de esas bitácoras, también se decidió buscar los registros históricos del servidor dinámico de direcciones IP, que se suponía debió haber provisto el rango de direcciones que incluía la del cliente del servidor de correo electrónico, que en el instante de la conexión hecha, fue registrada como la fuente del mensaje electrónico. A partir de ese último registro se esperaba obtener las direcciones de *hardware* de los equipos de computación involucrados en el suceso. Esto era porque, en caso de que se obtuviera esa información, se dispondría de mayor detalle para identificar al equipo que había estado asociado con el empleado corporativo durante el incidente de la filtración. Y si se lograba reconocer con exactitud el computador usado, se podían recopilar las cuentas de acceso de los usuarios que operaron en el mismo, así como también las bitácoras y los registros locales. Se estableció entonces que, a partir de ese momento, sería posible entrevistar a los sujetos vinculados y establecer las primeras responsabilidades. Ejecutar ese plan dependía de la ubicación física de los sistemas y de las personas, al igual que de la cantidad de investigadores y recursos disponibles, pero no fue elaborado ni dirigido con base en una herramienta específica. Podía haber sido instrumentado con distintas herramientas o combinaciones de ellas, y es que una investigación en computación forense no debe estar estrictamente ceñida a lo que provee un instrumento específico. El investigador debe formular su plan sin depender de ninguna herramienta que no sea su mente inquisitiva y experimentada.

Otro aspecto que la planificación debió considerar fue el costo en recursos, tiempo y dinero que impondría ejecutar el trabajo. Este estuvo concebido para tres especialistas, laborando cuatro días consecutivos, por las distancias que deberían recorrer a cada una de las fuentes a recopilar y analizar. Inicialmente se dispuso de una estimación aproximada de seis mil dólares estadounidenses ($ EE UU 6000). Posteriormente, se consideraron las herramientas a usar, dado que los archivos de bitácora a examinar y el mensaje de correo electrónico se proveerían en formato de caracteres *Unicode*® –ver Figura 1–. Por ello se decidió que para iniciar el trabajo técnico era suficiente disponer de las herramientas de comandos como las que provee un *Shell* de Linux.

Figura 1: Muestra de uno de los archivos bitácoras revisados en el caso.

El tercer estado de la investigación es la obtención y recopilación de las primeras informaciones previamente planificadas. La entrevista con el consultor jurídico aclaró que el anonimato no era tal, sino que el mensaje se había emitido en una cuenta de correo electrónica usada por aproximadamente 50

personas. Esto violaba los lineamientos y normas corporativas, pero era producto de la implementación de una mala cultura tecnológica de la institución. Otro aspecto crucial que se descubrió fue que el mensaje original incluía cinco archivos confidenciales, en modo adjunto, que provenían de una carpeta *web* compartida entre los mismos 50 usuarios y uno del cual no parecía existir ninguna copia. La carpeta compartida estaba en un servidor que no registraba los accesos y manipulaciones de esa información. Colateralmente, se recibió copia[35] de las bitácoras del servidor de correo electrónico y se descubrió, además, que existía un servidor de atención y recepción de las conexiones para formular el mensaje a enviar o consultar el buzón electrónico, del tipo *front end*. Ese servidor era un sistema del tipo IMAP/POP3 *Dovecot*® de fuente abierta. Por eso se procedió a solicitar sus bitácoras para la fecha en que se emitió el mensaje de correo electrónico. Esto no había sido inicialmente considerado, pero el mismo curso de la investigación forense condujo a que se realizara. De modo que con dos servidores registrando datos, surgió el potencial problema de la necesidad de sincronizar la hora entre ellos, ya que no se disponía de un servidor de tiempo común para la red. Así que se consultó la fecha y hora de cada uno y se calculó la diferencia en segundos. Ese valor resultaba notable, ya que en un segundo un servidor hace cientos de operaciones.

Con esa nueva información se procedió entonces a aplicar una técnica de reconstruir en reversa la emisión del mensaje de correo electrónico. Es decir, a partir del mensaje recibido en el buzón del consultor jurídico se inició una búsqueda de cuándo el servidor *Sendmail*® lo había procesado. Parámetros tales como serial, tamaño y fecha del elemento buscado debían coincidir para poder precisar cuándo se identificara correctamente en el otro equipo. Luego, se buscó la correspondiente entrada en el servidor IMAP/POP3 que incluiría además una dirección IP. La coherencia entre las entradas se hizo a partir de

[35] Cada elemento recibido implicó previamente emitir documentos formales a los responsables de la administración técnica de cada sistema para su entrega y exigir, además, que se suministraran esos objetos con su producto correspondiente del número de verificación, que era el resultado del uso de una Función *Hash*. Para ello se empleó el comando *md5sum* de Linux. De ese modo, se eliminó dudas respecto al origen de cada información recibida. Se consideró, además, la cadena de custodia.

parámetros del mensaje y la diferencia en segundos de los servidores. Con la dirección de red se fue a buscar la dirección de Control de Acceso al Medio (MAC) que registraba el servidor del Protocolo de Control de Asignación Dinámica de Direcciones a *Host* (DHCP). Como esa dirección no se repetía en toda la corporación e identifica a una tarjeta de red única en un computador, se procedió entonces a buscar los registros y se descubrió el equipo en el cual se había instalado la misma. La información descubierta arrojó también otros elementos claves para cotejar la certeza de lo que se hacía, como, por ejemplo, el tipo y la versión del navegador que el usuario había usado. Toda esta operación se constituyó en sí, como ver una película hacia atrás y con ello se fue construyendo una línea de tiempo, preliminar y en reversa de los hechos.

Otra operación que se hizo en modo paralelo durante este mismo estado de la investigación forense, fue el examen de la «Metadata» de cada uno de los archivos adjuntos a los mensajes de correo electrónico. De los cincos archivos, se identificaron a los autores de cada uno, al igual que sus fechas de creación y modificación. Dicha operación no demandaba el empleo de ninguna herramienta especializada, y pudo ser realizada desde el mismo sistema operativo de la máquina donde se recibió el mensaje de correo electrónico –ver Figura 2–, pero existen herramientas especializadas para procesarla –ver Figura 3–. Luego, se verificó el resultado con la fuente original de la carpeta compartida y se descubrió una diferencia en uno de los archivos añadidos al mensaje de correo electrónico. Ello mostró un primer error del remitente de la filtración de información. Este había modificado muy ligeramente un archivo de texto, sin advertir que la operación de copiar y pegar que había ejecutado entre la carpeta remota y su sistema de archivos local hizo que el sistema de operación registrara la alteración de la Metadata original de los archivos fuente. Es decir, el infractor descargó un archivo y para adjuntarlo decidió ver su contenido completo, de forma que podría cerciorarse de lo que enviaría y al llegar al final agregó una línea vacía de más. Los investigadores dedujeron, entonces, que el empleado infractor no tenía grandes conocimientos en el uso de computadoras, ya que al oprimir la tecla para suministrar la línea final (*Enter*) desde la interfaz computacional de usuario que usó para generar el mensaje de correo electrónico, el procesador de texto invocado por dicha

interfaz automáticamente había guardado la nueva copia en el disco local y para ello debió registrar nueva Metadata de ese archivo temporal. Allí nació una diferencia que había capturado parámetros del computador local, como es la identificación del nombre de la cuenta usada para esa sesión de trabajo. Para realizar esta tarea se usaron comandos clásicos como *cmp*, *diff*, *wdiff* de Linux y un editor hexadecimal de *software* libre llamado *ghex*. Luego, cuando se examinó el contenido de los archivos buscando diferencias y fue cuando se observó que la diferencia era la presencia de una línea vacía al final del archivo. Al establecer la sutil diferencia, se procedió a examinar toda la Metadata y se consiguió el nombre de otra cuenta de usuario, al igual que otra fecha de última actualización de esos datos. Se dispuso así, de una pista que por primera vez señalaba a una persona real y de la hora de la computadora involucrada en la falta.

Figura 2: Examen básico de la Metadata de un archivo en la carpeta RECYCLER.

Figura 3: Herramienta de *software* Libre *Exiftool*® para el examen de la Metadata de cualquier archivo[36].

A este nivel de la investigación fue posible ajustar la planificación inicial para precisar la táctica que permitiera consolidar el objetivo final. Al haber determinado el computador de donde se suponía que se había emitido el mensaje de correo electrónico, se decidió que en él se requería encontrar algún registro de que de allí se había usado la cuenta de correo compartida entre las 50 personas. Además, era necesario encontrar copia del archivo que se había modificado allí. Esos elementos permitirían justificar que se interrogara al usuario responsable del equipo y al de la cuenta de donde se había originado el envío. Si ambos usuarios coincidían, entonces era más fácil suponer el individuo detrás de la filtración.

[36] La imagen está tomada del sitio http://www.hackingDNA.com.

El cuarto estado de la investigación impuso acciones más técnicas y menos deductivas. Con la dirección IP que registraban los servidores como fuente del mensaje filtrado, se buscó la ubicación física del equipo. De forma que los investigadores debieron estudiar el patrón de la dirección IP establecida y deducir la zona del país a la cual este se asociaba. Pero aquí surgió una primera complicación por el manejo inapropiado de los sistemas en red. Por escasez de espacio de almacenamiento, el servidor DHCP de ese estado de la región no registró la información previa mayor a los últimos tres días. Este tipo de situaciones puede ser suficiente para bloquear cualquier investigación forense, pero los profesionales del área saben que hay diversos modos de reconstruir los acontecimientos pasados. De modo que lanzaron la primera conjetura, buscaron la máquina desde donde acostumbraba a conectarse el usuario que aparecía en la Metadata de la alteración aparentemente inadvertida y la incautaron. El computador se encontró en una planta industrial y se decidió que se examinaría detalladamente para tratar de encontrar cualquier elemento que respaldara la creencia de que podía ser la fuente desde donde se realizó la infracción. Si se identificaban datos que coincidieran con los archivos enviados en modo adjunto, se verificaba el uso de la cuenta de correo electrónica involucrada para la fecha y, en caso de que el patrón de la dirección IP tuviera alguna semejanza básica con la que mostraban los servidores de correo, entonces se podría aventurar interrogar a la persona indiciada. Esta conjetura pudo no haber sido necesaria si la administración técnica de la red se hubiese desempeñado tal como indican los estándares internacionales y la teoría del área, pero, lamentablemente, es común que en la práctica las investigaciones forenses deban enfrentar anomalías en las operaciones, pues la complejidad en mantener una red corporativa de datos y comunicaciones tiende a incrementarse y además se elevan sus costes. Las organizaciones descuidan ciertos detalles en los registros de eventos y tienden a enfocarse en mantener los servicios operativos.

En otras ocasiones, pueden surgir intereses internos para tratar de ocultar, bloquear o desestimar la investigación en progreso. De modo que resulta común que los investigadores experimentados continuamente repasen todos los hechos y consideren varias alternativas para recopilar la información buscada. Así, cuando un obstáculo surge pueden disponer de otras formas para no abortar la investigación y progresivamente examinar la coherencia de lo que suponen aconteció.

Un elemento que reforzó la confianza en la conjetura establecida tuvo que ver con el contenido de uno de los archivos enviados en modo adjunto. Su contenido hacía referencia a una adquisición que se había realizado dentro de la planta industrial, un acuerdo que generalmente no era conocido fuera de ese lugar. Por lo tanto, el hecho de que el archivo formara parte de los adjuntos, reforzaba la idea del autor de los mensajes filtrados conocía el funcionamiento de la planta.

Para examinar el equipo que se incautaría, se requirió desarrollar una herramienta que permitiera buscar exhaustivamente los archivos sin posibilidad de error. Por eso se decidió apoyar la comparación en el uso de una función matemática del tipo *hash* y se usó la herramienta *md5sum*. La Figura 4 muestra parte del *guión shell* elaborado para detectar la presencia de los archivos enviados en modo adjunto. Se seleccionó programar en *Bash Shell* dado lo fácil y rápido con que se podía elaborar la herramienta, pero para discos de tamaño considerable y para acelerar la búsqueda, se podría haber usado C o C++.

Figura 4: Código desarrollado para buscar en un computador los archivos haciendo uso del algoritmo MD5.

De modo que empleando el programa desarrollado se entró al nivel 5, búsqueda, restauración y/o recuperación de los datos. Allí se requiere de instrumentos y métodos precisos para ubicar un archivo entre los miles que normalmente almacena un disco duro moderno. Para ello los dispositivos, sistemas, bitácoras y demás elementos que podían servir como fuente para la búsqueda debieron ser solicitados o incautados. Cada entrega se apegó además a los estándares del área, como es, por ejemplo, usar una cadena de custodia de cada potencial objeto que se examinaría.

Pero usar una herramienta demanda cierto dominio sobre su uso, y es que las herramientas a usar deberían, previamente, haber sido probadas sobre sistemas similares a razón de no alterar nada fuera de lo que será planificado. Existen numerosas revisiones, comparaciones y tutorías en la red de redes, sobre las distintas opciones de herramientas que existen y facilitan el dominio de las mismas[37]. De forma que cada imagen a extraer puede ser estimada en su tiempo de elaboración. Cualquier adaptación a los procedimientos a seguir es posible en esta etapa, siempre que mantenga el postulado de que los datos recopilados sean fieles a los que se vieron involucrados en el incidente.

En la Figura 5, se muestra a una técnico elaborando la imagen forense de un disco duro de un equipo. La gráfica muestra un dispositivo de memoria que se puede remover fácilmente, conectado a través de un puerto de *Bus Serial Universal* (USB). Ese dispositivo contiene una instalación de la distribución *Computer Aided Investigative Environment* (CAINE) Linux que puede iniciar desde allí sin tocar el disco duro del computador. De ese modo, el computador está operando pero sin alterar los datos que guarda la memoria secundaria desde la última vez que estuvo encendido. La gráfica también revela que hay un disco externo conectado, en modo temporal, también sobre otro puerto USB del equipo. La copia de la imagen del disco duro que se haga, reposará sobre ese dispositivo y a partir del mismo se podrán hacer otras copias.

---

[37] Jain, Nilakshi y Kalbande, Dhananjay: «*A comparative study based digital forensic tool: Complete automated tool*». En: *The International Journal of Forensic Science, IJoFCS*. Vol. 9, Nº 1. 2014, http://www.ijofcs.org/V09N1-PP03-A-Comparative-Study.pdf.

Figura 5: Técnico procediendo a elaborar una imagen forense de un disco duro.

De modo que el computador involucrado arranca con un sistema de operación diferente al que originalmente posee, para así evitar que se altere el estado del mismo en el disco duro. Ese sistema de operación posee facilidades para poder montar los discos temporales que se conecten al computador, a través de puertos USB, al igual que el disco duro interno del equipo. Es común emplear comandos como *fdisk*, *sfdisk*, *hdparm*, *df* y *mount* para identificar los dispositivos presentes, sus parámetros y montarlos –ver Figura 6–.

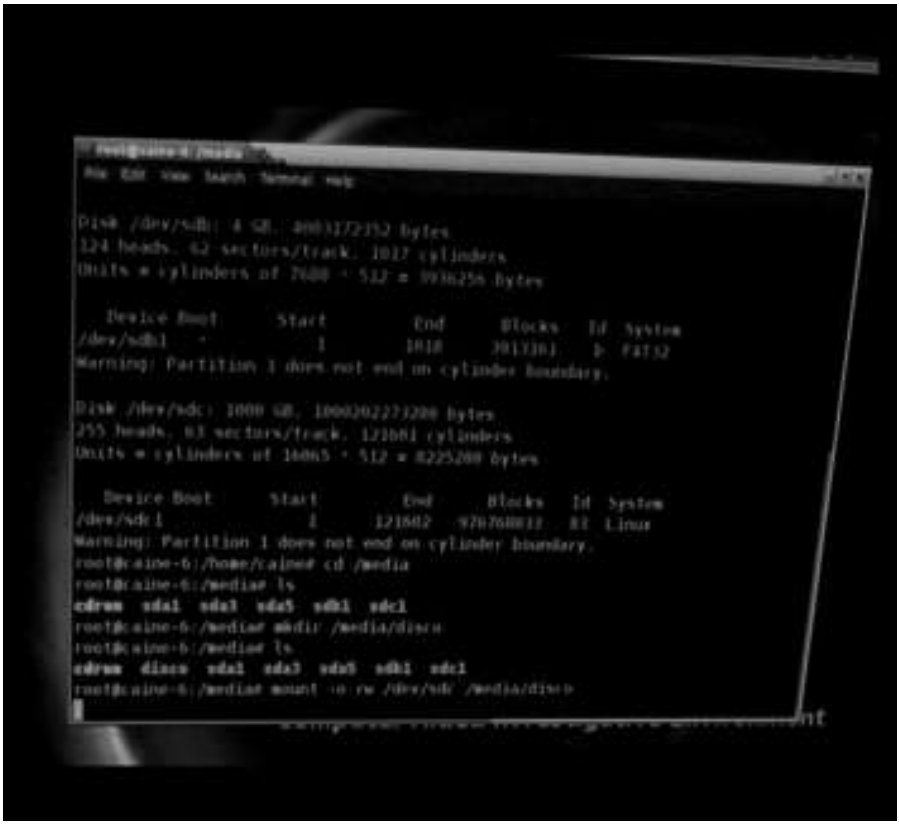

Figura 6: Ejemplo de una sesión de comandos para manejar los volúmenes a montar.

Luego, empleando comandos como *dcfldd*[38], *ddrescue*[39] y *tshark*[40], es posible realizar la captura de todos los datos almacenados en un dispositivo. Adicionalmente, para verificar que el trabajo se haga adecuadamente, suelen emplearse comandos como *dhash*, *shasum*, *sha1sum*, *sha224sum*, *sha512sum* para obtener resultados de funciones del tipo *hash* que se aplican a todo el disco y que sirven para verificar la exactitud de la copia a procesar.

Para el caso que se viene relatando, antes de elaborar la imagen forense del primero de los computadores incautados, los investigadores revisaron si tendrían conflicto con datos privados de los usuarios y encontraron que ello no sucedería, ya que la política de seguridad de la información de la institución involucrada declaraba expresamente que la información a procesar y guardar en los equipos de los computadores que se asignaba a los empleados, debía limitarse al interés de la organización. Vigilar el cumplimiento de esa norma era una obligación de los trabajadores que recibían temporalmente los computadores. Adicionalmente, se expresaba que la institución se reservaba el derecho de examinar todo lo almacenado sin notificación previa. Por lo tanto, se hizo la imagen de los discos enteros.

En el quinto estado se realizó la búsqueda de los archivos con el programa diseñado especialmente, pero, antes de proceder con ello, se decidió que era necesario recuperar los archivos que el usuario eliminó. Esto con el fin de incluir en la búsqueda a aquellos archivos que el usuario hubiese procesado y posteriormente borrarlos, con el fin de eliminar cualquier rastro posible. Esa recuperación pudo llevarse a cabo gracias a herramientas del tipo *software* libre, como

---

38 Esa herramienta es una ampliación del comando *dd*, un clásico para realizar imágenes forenses, realizada en el Laboratorio de Computación Forense del Departamento de Defensa de los EE UU.

39 Este comando incluso permite registrar errores originales en el disco que se clonará. Fratepietro, Stefano; Rossetti, Alessandro y dal Checco, Paolo: *DEFT 7 Manual. Digital evidence & forensic toolkit*. 2012, http://www.deftlinux.net/doc/EN-deft7.pdf.

40 Este instrumento forma parte de la aplicación *Wireshark* y en general, permite desde una consola de comandos procesar eventos de redes almacenados en formato *pcap*. Lamping, Ulf; Sharpe, Richard y Warnicke, Ed: *Wireshark user's guide. For Wireshark 2.1*. 2014, https://www.wireshark.org/download/docs/user-guide-us.pdf.

Foremost® que fue desarrollada en la Oficina de Investigaciones Especiales de la Fuerza Aérea de EE UU *Photorec*® del grupo de desarrollo *cgsecurity*, *The Sleuth kit*® y *Autopsy*® –ver Figura 7– de Brian Carrier y Basis Technology.

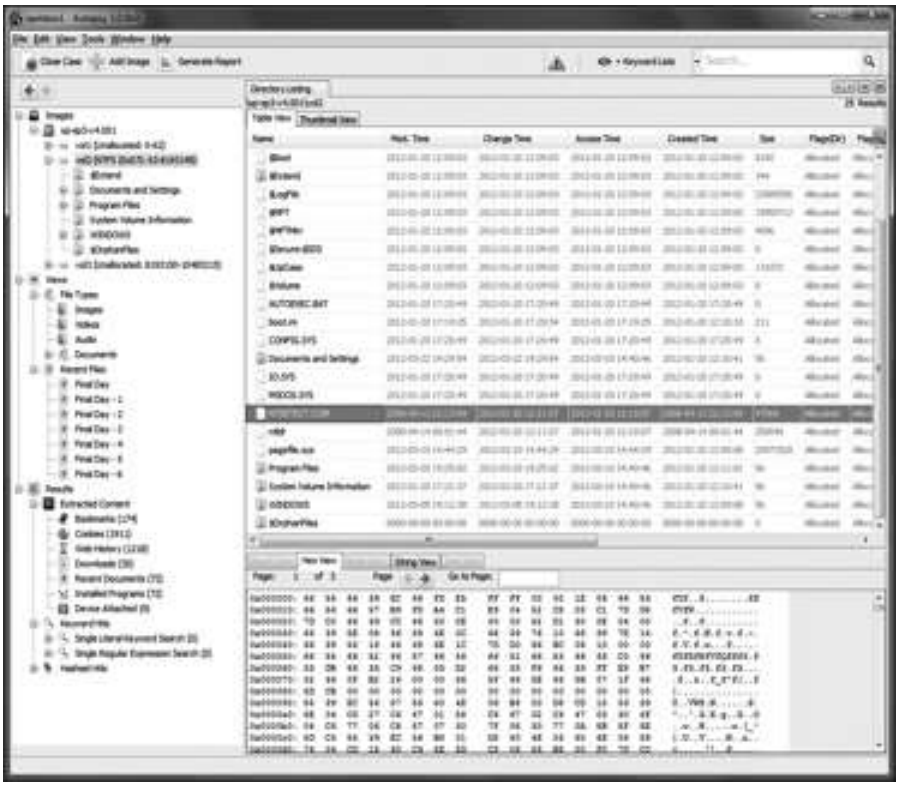

Figura 7: Ejemplo de la pantalla del programa *Autopsy* que es una GUI de *Sleuth Kit*[41].

Una de las tareas inmediatas que tuvieron que ejecutar los investigadores del caso fue construir una línea del tiempo. Este producto facilita reconocer, desde niveles superiores, cómo transcurrieron los eventos y se basa en la determinación de las fechas y horas que registran cada tipo de archivo del sistema.

[41] La imagen está tomada de http://www.sleuthkit.org.

Comúnmente cada archivo contiene la fecha y hora en que se creó, en que se accedió al mismo por última vez y, en ciertas ocasiones, se registra la fecha y hora de su última modificación[42]. Resulta común agrupar estos tiempos de modificación, acceso y creación por sus iniciales, en el término *MACtime*.

El sexto estado de la investigación refiere al análisis de los datos obtenidos. Durante el desarrollo del caso, entre los archivos restaurados los investigadores descubrieron cinco de los seis archivos que habían sido adjuntados en los mensajes de correo electrónico. Verificaron además las bitácoras que mantiene el sistema de operación y encontraron que el sistema a veces había empleado la dirección IP buscada. El examen de las *cookies* con la herramienta *dumpzilla*®, un instrumento desarrollado en el lenguaje *Phyton* que permite extraer información de algunos navegadores comerciales como *Firefox*®, mostró que la cuenta del usuario que usaba el equipo había hecho uso de la cuenta de correo electrónico de uso común. La fecha de creación de la «galleta» estaba en el rango de lo que coincidía con la de los envíos que filtraron la información.

El séptimo estado de la investigación es la reconstrucción y correlación de eventos. Disponiendo de evidencias que fueron recabadas con consultas a personas, exámenes de bitácoras y recopilación de datos clarificadores por herramientas forenses especializadas, así como de una línea de tiempo, fue posible cotejar la hipótesis inicial elaborada contra los hechos ya constatados. Como hubo concordancia no fue necesario volver a atrás y revisar las pistas, pero este acierto no es muy común.

El octavo estado fue la revisión y ello llevó a solicitar el apoyo especializado de una unidad de investigaciones interna a la corporación, que estaba preparada para conducir averiguaciones con el examen de elementos físicos e interrogatorios particulares a personas. Este auxilio fue vital, ya que se buscaba

[42] Carbone, R. y Bean, C.: *Generating computing forensic super-timelines under Linux. A comprehensive guide for Windows-based disk images*. Defense R & D Canada. Valcartier. Technical Memoradum. 2011, https://forensicfocus.files.wordpress.com/2012/08/generating-computer-forensic-supertimelines-under-linux-a-comprehensive-guide-for-windows-based-disk-images1.pdf.

una confirmación aún más sólida de la que otorga el mundo cibernético. Se deseaba afinar el vínculo entre la cuenta de usuario empleada en los mensajes con filtración y un individuo real. Para ello, había que revisar grabaciones de cámaras de vídeo digital, revisar listados de asistencia a ciertas áreas, buscar testigos y entrevistar directamente al presunto implicado. Se requirió observar y estudiar las reacciones del sujeto durante el interrogatorio, así como sus respuestas y aseveraciones. A veces este estado no se aplica en la investigación de computación forense, ya que únicamente se espera que se provea de lo que arroja el análisis de datos de los dispositivos electrónicos, pero, en otras ocasiones, se desea identificar al supuesto autor de la infracción.

Para el caso descrito, predominó la segunda orientación, por lo que la entrevista se realizó con un plan de preguntas previamente elaboradas, que incluía consultas que permitirían verificar si hallazgos claros en los sistemas coincidían con las respuestas que el entrevistado suministraría. De ese modo se hacía un aporte valioso para establecer el nivel de confianza en las respuestas que se obtendrían. Por otra parte, se incorporaron aseveraciones que sirvieron para denotar las emociones y reacciones inmediatas. Además, la sesión se grabó con una cámara de vídeo, para revisar posteriormente lo sucedido en ella, al incorporar a un psicólogo que ayudó a establecer la veracidad de lo emitido por el entrevistado.

El resultado de esta etapa fue favorable a lo propuesto por los investigadores, pues este no era experto en el manejo de computadoras. Por lo tanto, el entrevistado varias veces se sorprendió de que se hubiesen descubierto algunas de sus acciones, que erróneamente había pensado se desconocerían, puesto que las había realizado en la soledad de su oficina. Por ello cooperó y optó por señalar que no había deseado perjudicar a la institución, sino denunciar una anormalidad.

El estado final de la investigación fue la elaboración del informe final, que se apoyó en el informe de la unidad de investigaciones corporativas, que disponía de abogados, exagentes policiales y psicólogos especializados. Se incluyó el acta y la declaración firmada por el sujeto entrevistado y un tomo de anexos

con copias impresas y en disco compacto de cada una de las evidencias y documentos empleados durante la investigación. Para la elaboración de este documento, lo primero que se consideró fue que el objetivo perseguido en la investigación de identificar al autor de la filtración se había logrado y no era necesario describir posibilidades alternas. La evidencia era sólida a razón de proceder a describir cronológicamente los eventos acontecidos durante el incidente. El segundo aspecto tratado fue que el informe estuvo dirigido al departamento de asistencia legal de la empresa, quien decidiría si procedía a acusar al trabajador señalado. El informe se dividió en tres secciones principales: un resumen ejecutivo, una descripción general del proceso realizado y los resultados obtenidos. Una serie de anexos complementaron los detalles de la recolección, los hallazgos relevantes, los hechos identificados, el análisis, una descripción clara del nivel de certeza de los descubrimientos, las entrevistas y la opinión de los expertos[43].

Conclusión

Toda investigación forense requiere una preparación, planificación, destreza, recursos, observación y lógica deductiva. Por lo tanto, es una disciplina que entremezcla una orientación detectivesca con un dominio técnico propio de la tecnología digital. Combinar ambas orientaciones, es un reto para las sociedades modernas. Dado el creciente y extendido uso de la tecnología digital, es posible suponer que en los próximos años aumentará la demanda por la categoría de especialistas de esta área. Bien sea en los cuerpos de seguridad del Estado o en la seguridad interna de las corporaciones modernas, la preparación de estos trabajadores se hará cada vez más notable.

* * *

Resumen: El uso de la tecnología informática se extiende cada vez más en el mundo occidental. Los usuarios se asisten en sus trabajos, haciendo mayor uso de dispositivos digitales,

[43] EC-Council: *Computer forensics. Evidence collection & preservation*. EC-Council Press. New York, 2010.

como, por ejemplo, los teléfonos inteligentes. Los delitos no escapan a esta tendencia y por ello a algunas instituciones del Estado les resulta imprescindible conocer, comprender y aplicar en modo práctico la realidad de la computación forense moderna. Este trabajo describe una revisión general de lo que trata la disciplina de la computación forense. Igualmente, describe un caso real a modo de ilustrar la aplicación organizada de la misma. **Palabras clave**: Computación forense, investigación digital, seguridad de computadoras. Recibido: 24-04-17. Aprobado: 13-07-17.