CIBERCRIMEN Y EVIDENCIA DIGITAL

TEMA
EVIDENCIA DIGITAL

MÓDULO 4

TABLA DE CONTENIDOS

MÓDULO 4

EVIDENCIA DIGITAL

En el presente módulo se explica con mayor detalle el concepto de evidencia. Se muestran las diferentes formulaciones y principios detrás de la obtención de la misma, a fin de mantener su admisibilidad ante un tribunal.

1. OBJETIVO DEL MÓDULO

Entender el concepto y características de la evidencia, y los principios a seguir para la obtención de evidencia en medios digitales.

2. DEFINICIÓN DE EVIDENCIA EN MEDIOS DIGITALES

Diversas interacciones con equipos informáticos pueden generar datos: correr una aplicación, insertar un dispositivo USB en una computadora, poner al equipo en hibernación, descargar un archivo, el archivo en sí dentro del disco duro, entre otros. Tras establecer los lineamientos de una investigación, es posible determinar cuáles de los datos pueden considerarse evidencia o no. **La evidencia solo puede ser considerada como tal si es que permite probar una hipótesis**. Por ejemplo, en un caso de espionaje corporativo, un correo de un empleado hacia un gerente de la empresa rival podría ser considerado evidencia y por lo tanto debe ser analizado.

La otra duda por resolver es dónde podemos hallar esta evidencia. Se mencionó que descargar un archivo es un dato que podría ser considerado más adelante como evidencia. El investigador debe tener el conocimiento para poder determinar en qué parte del sistema buscar la información de archivos descargados. Aún más, acciones como prender y apagar el equipo, conexión de dispositivos periféricos (teclado, mouse, etc.) al equipo, son también posibles fuentes de evidencia. Generalmente, todas estas acciones pueden definirse como **transacciones digitales**, donde producto de una acción un archivo del sistema ha sufrido un cambio en su estado. El investigador debe buscar en las transacciones a fin de encontrar la evidencia.

Principios para la recuperación de evidencia

Existen 4 principios respecto a la recuperación e investigación de evidencia basada en computadoras (Williams, 2012, p. 6). El objetivo de establecer estos principios es garantizar la integridad de la evidencia y permitir replicar los resultados con precisión. Esto remueve dudas sobre lo hallado, así como la oportunidad que pueda ser criticado en la corte.

Los principios a continuación fueron escritos por la Asociación de Jefes de Policía del Reino Unido (ACPO por sus siglas en inglés), la cual fue disuelta en el 2016 y ahora se ha convertido en el Consejo Nacional de Jefes de Policía (NPCC por sus siglas en inglés) (National Police Chiefs' Council, 2020):

- **Principio 1:** Ninguna acción de las fuerzas del orden, personas empleadas por estas agencias, o sus agentes deben cambiar los datos que puedan ser llevados a corte
- **Principio 2:** En circunstancias donde una persona encuentre necesario acceder a la data original, esa persona debe ser lo suficientemente competente para hacerlo y luego ser capaz de dar evidencia explicando la relevancia e implicaciones de sus acciones.
- **Principio 3:** Un registro de auditoría u otro registro de todos los procesos aplicados a la evidencia digital debe ser creado y preservado. Un tercero independiente debe ser capaz de examinar esos procesos y obtener el mismo resultado.
- **Principio 4:** La persona a cargo de la investigación tiene toda la responsabilidad de asegurar que esta se adhiera a la ley y a estos principios.

Los principios mencionados tienen un fin importante: asegurar que la corte reciba la misma evidencia que fue recabada inicialmente. En medios digitales, distintos programas pueden alterar el contenido de las unidades de almacenamiento, incluso sin conocimiento del usuario. Por ejemplo: cuando el usuario trabaja con un documento de texto, y tras sufrir una pérdida de energía en el equipo es posible encontrar una versión recuperada del trabajo realizado aun cuando no se había guardado la información antes del incidente.

Si bien estos principios son aplicables a investigaciones criminales, explican las necesidades que deben tomarse en cuenta al trabajar con evidencia digital. La evidencia digital debe, en lo posible, manejarse a través de una imagen de esta, a fin de preservar la evidencia original y permitir a terceros reexaminar la evidencia y llegar al mismo resultado (Williams, 2012, p. 7). Esta imagen puede ser física o lógica, total o parcial.

Problemas en la obtención de evidencia digital

Los principios mencionan la necesidad de elaborar imágenes de la evidencia, siempre cuando esto sea posible. La razón de esta explicación se debe al principio de Locard: Todo contacto deja una huella (The Forensics Library, 2020). Hay situaciones que generan problemas para la recolección de información, haciendo difícil no alterar la evidencia.

Algunos ejemplos donde es difícil mantener la evidencia sin alteraciones:

- **Conexiones de red:** El principio de Locard puede no aplicarse en este escenario. Algunas interacciones pueden no dejar huellas en los equipos informáticos, o para poder hacer simulaciones sobre la imagen puede requerirse de la conexión hacia un servidor externo. Hasta este punto se ha asumido que es posible incautar e investigar el equipo fuera de línea.

- **Servicios en la nube:** No todos los datos trabajados en dispositivos son almacenados localmente. Actualmente se tiene la posibilidad del trabajo remoto o el almacenamiento de archivos en sistema de almacenamientos manejados por externos, a los que es posible acceder mediante una conexión a Internet. A estos sistemas accesibles en línea se presentan nuevos retos: evidencia fuera del control del investigador, la evidencia puede contener datos de otras organizaciones fuera de la investigación, etc. (Lallie & Pimlott, 2012).

3. PRINCIPIOS A SEGUIR SOBRE EL MANEJO DE EVIDENCIA

Integridad de la evidencia

La evidencia puede ser declarada inadmisible cuando hay suficiente base para cuestionar la continuidad de la integridad, visto en el caso Bando vs Gates (THE GATES RUBBER COMPANY, a Colorado corporation, Plaintiff, vs. BANDO CHEMICAL INDUSTRIES, LIMITED, a Japanese company, 1996). Este caso es importante al ilustrar lo que implica el manejo de evidencias digitales.

Investigador sin las credenciales o experiencia necesaria: El caso hace mención de la importancia de contar con investigadores con conocimientos y experiencia en el campo de la investigación digital forense a fin de dar peso al testimonio y hallazgos que se puedan dar. Cuando cada parte en el caso presentó a su experto, el juez le dio más relevancia a lo dicho por el que mostraba tener mejores credenciales.

Uso de copias digitales vs Recuperación de archivos: Dentro de los cuestionamientos, se menciona la necesidad de crear copias digitales en vez de la instalación de software para recuperación de información o la copia de archivo por archivo. Si bien se puede instalar un software en un equipo para obtener la evidencia, la instalación misma podría reescribir espacio en el disco con información relevante (evidencia). Cualquier alteración del espacio en memoria podría arruinar la evidencia. Por otro lado, la copia de archivo por archivo no permite obtener archivos borrados.

Sobre el último punto en mención, a fin de confirmar la integridad de la evidencia y evitar dudas sobre la alteración de la misma, una técnica muy común usada es el hashing. Hashing es un proceso criptográfico que recibe un número largo de valores y mediante un proceso lo transforma en un valor de tamaño dijo, de tal modo que este valor sea único para el número de valores inicial. En resumen:

- Misma entrada → Misma salida
- Diferente entrada → Diferente salida

De este modo, el valor hash de la copia digital (imagen) y el valor hash de la evidencia digital deben ser el mismo. Así se corrobora que, en la hora del juicio, la investigación hecha sobre la copia digital guarda concordancia con la evidencia incautada y por lo tanto es integra.

RETO: Explicar mediante un diagrama el proceso de elaboración de un hash.

Integridad del proceso

En el caso de Bando vs Gates, el cuestionamiento fue dirigido hacia la integridad de la evidencia. Otro punto a tomar en cuenta es el procedimiento. El valor probatorio que pueda tener la evidencia puede ser cuestionado debido al proceso usado para su obtención, para esto véase el caso del Sargento Virdi vs MPS (Turner, 2017).

Simulaciones e investigación directamente sobre el medio a investigar: En medios informáticos, es posible hacer uso de diversas técnicas como revisión del registro de eventos ocurridos en el sistema (logs) o simulaciones sobre el mismo equipo a investigar para analizar los resultados. La palabra "log" es usada para describir a un registro que indica un evento ocurrido en el sistema. Su estructura más básica indica una fecha, hora y descripción del evento. Cada acción realizada en el sistema genera un log. Es por ello que el principio de Locard se aplica en este caso, haciendo que cada simulación genere más logs y esto conlleva a que la evidencia se dañe con nueva información ingresada.

Uso de técnicas no formuladas/aptas para la investigación forense: Dentro de otros campos pueden existir el uso de diversas técnicas para el análisis de equipos físicos, software o registros. Uno de los principios mencionados es que dentro del marco de la investigación debe ser posible que una tercera persona pueda realizar los mismos procedimientos. El problema de no estandarizar los métodos de investigación es que si la tercera persona realizar la investigación con una técnica que no considera confiable, los resultados tampoco serán validados por este tercero.

Finalmente, otros puntos a tomar en cuenta son:

- **Cadena de custodia:** A fin de evitar dañar la evidencia, la memoria digital donde reside debe ser manipulada el tiempo mínimo suficiente para generar la imagen digital de la misma y luego poner en resguardo el original. El original quedará en manos de una o más personas quienes asumirán la responsabilidad de resguardar la memoria a fin de que no sufra alteración alguna hasta la fecha del juicio. En ese punto, se comparará el valor hash de ambas.

- **Alcance de la investigación:** Se debe determinar la extensión a investigar: el total o parte de un sistema de almacenamiento, de un equipo o varios.

4. PROPIEDAD Y EMBARGO DE MEDIOS INFORMÁTICOS A INVESTIGAR

Embargo de evidencia

El primer principio a tener en cuenta es el de la propiedad. Para que un investigador pueda tener acceso a la evidencia, se requiere de la autoridad para incautar, manejar y procesar evidencia. La autoridad no es del investigador, sino que es adquirida a través de un juez o el propietario de la evidencia.

En el ámbito judicial, el juez es quien da la orden de incautación para obtener evidencia del caso. Una orden de un juez está sustentada en que existen las pruebas suficientes para permitir tal acción. Por lo general, en estas órdenes se especifica el lugar, los objetos y las personas que están sujetas a la búsqueda. Es importante considerar ciertos aspectos a la hora de requisar un equipo (Williams, 2012, pp. 8-9):

- Hay posibilidades de que el equipo pueda contener evidencia.
- Se debe llevar un registro de los detalles en que el equipo fue encontrado.
- Considerar las fechas que forman parte del tiempo a investigar. Ejemplos: recuperar una grabación de un asalto dado en un día y hora específico; una laptop nueva que fue adquirida después de un ataque informático perpetrado por el investigado.
- Diferenciar la propiedad de los distintos equipos que puedan encontrarse en la búsqueda
- Verificar si el equipo guarda evidencia en la nube. Puede suceder que el equipo tenga permisos suficientes para acceder a la información guardada online.

RETO: De los siguientes elementos de evidencia online, determinar cuáles son del ámbito privado (requieren de autorización para poder ser investigados) y cuales no:

- **Post de una cuenta de Facebook**
- **Información en un blog del investigado**
- **Datos personales en una cuenta de Google**
- **Conversaciones de WhatsApp**

En el escenario corporativo, en los contratos de trabajo se suele estipular los lineamientos del uso de equipos electrónicos provistos por la empresa, o el uso de equipos personales para realizar labores dentro de la empresa. Esto último es conocido como Trae Tu Propio Dispositivo (BYOD por sus siglas en inglés). El primer caso suele establecer a la empresa como dueña de los equipos provistos al empleado, por lo que los equipos están sujetos a su requisición o monitoreo a criterio de la empresa, así como a las reglas de uso.

Clonación

Sammons define la clonación como “una copia exacta, bit por bit, de un disco duro (también conocido como ‘bit stream image’)” (Sammons, 2012, p. 52). Esto significa que toda la información contenida en una copia refleja fielmente lo contenido en la evidencia. Esto no significa copiar y pegar la información ya que esto solo copia la data accesible para el usuario (Sammons, 2012). Debemos considerar también otros elementos en memoria que no podemos ver a nivel de usuario: archivos eliminados, registros del sistema, archivos ocultos.

Realizar una copia toma bastante tiempo en realizarse (varias horas) por lo que suele hacerse en un lugar seguro distinto a la escena del crimen. Mientras la evidencia es guardada y forma parte de una cadena de custodia, la copia digital es guardada en una unidad de almacenamiento debe poseer mayor capacidad de almacenamiento que la memoria de origen. La unidad de almacenamiento destino para la copia es limpiada de cualquier otro dato que pueda tener y el resultado de la clonación es una imagen que puede ser visto también como un archivo (Sammons, 2012, p. 55).

Tabla con algunas herramientas para la creación de imágenes (Vandeven, 2014)

Herramienta	Plataformas			Evidencia a clonar				Codificación		Formato de salida			
	Windows	Linux	iOS	Disco físico	Volumen lógico	Archivos	Folders	Compresión	Encriptación	Raw	E01	Ex01	Split
FTK Imager 3.2	☑			☑	☑		☑	☑	☑	☑	☑		☑
FTK Imager CLI 3.1.1	☑	☑	☑	☑	☑		☑	☑	☑	☑	☑		☑
EnCase Forensic Imager 7.0	☑			☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Para poder validar que la evidencia no ha sido alterada y que la copia digital le pertenece a la evidencia en custodia, durante la clonación se realiza un cálculo matemático que genera un valor conocido como Hash. Este valor se asemeja a una serie de números y caracteres que son producto de un cálculo matemático que incluyen a todos los bits dentro del elemento marcado como evidencia. Al realizar este cálculo sobre el medio digital y la copia, ambos deberán arrojar el mismo valor hash. Basta que un bit dentro de la evidencia sea distinto para que el valor hash cambie.

Finalmente, hay otros elementos de memoria que pueden estar guardando información. Por ejemplo, cuando una computadora está encendida, la memoria RAM está guardando información como las aplicaciones corriendo. Si bien en este curso no se cubre este escenario a fondo, es parte de la investigación (de ser el caso) capturar la información guardada en la memoria RAM u otros elementos de memoria que, una vez cortada la energía, perderán la información.

5. TIPOS DE EVIDENCIA

La labor del investigador es imparcial, solo se remite a las pruebas y hallazgos en su investigación, sin tomar partido o inclinación hacia algún lado. A la hora de definir la evidencia encontrada, esta puede caer en las siguientes categorías

- **Inculpatoria:** Apoya la teoría inicial, la hipótesis con la que inició la investigación.
- **Exculpatoria:** Contradice la teoría inicial o genera duda razonable en torno a ella. Apelando al principio de imparcialidad, el investigador está en la obligación de presentar la evidencia.

Ya sea uno u otro tipo de evidencia, estas pueden ser del siguiente tipo:

- **Directa:** Apoya la veracidad de un argumento sin necesidad de inferencias u otros elementos que den significado a la misma.
- **Circunstancial:** Evidencia que, mediante la lógica, otros elementos y/o circunstancias dadas permiten llegar a una conclusión o hecho en apoyo a la veracidad de un argumento.

RETO: Plantear posibles ejemplos de evidencia(s) circunstancial(es) en medios digitales.

Yendo más a detalle sobre los distintos medios digitales que podríamos encontrar, a continuación, se muestra un detalle de algunos elementos digitales que podríamos encontrar según Sammons (2012):

Medios extraíbles

Hace referencia a todo elemento de almacenamiento que podamos encontrar en la escena. Desde dispositivos USB, discos duros externos, tarjetas de memoria (SD), DVDs, entre otros. Aún si algunos de los elementos mencionados pueden caber incluso en una billetera, actualmente estos elementos tienen la capacidad de transportar grandes cantidades de información.

En algunos casos, estos elementos usualmente no se encuentran conectados a un equipo, por lo que no suelen existir factores externos que puedan poner en peligro la integridad de la información contenida. Caso contrario, el equipo al que se encuentra conectado puede modificar la información contenida (incluso “desconectando de forma segura” una memoria). Por ejemplo, de estar una memoria USB conectada a una PC, el desconectarlo directamente del equipo podría dañar la

información contenida dentro de él. Otra posibilidad es que el investigado se encuentre haciendo modificaciones a un archivo guardado en esta memoria, por lo que desconectarla podría generar pérdida de información.

Recordemos también que estos elementos no necesariamente están a simple vista. En programas policiales solemos ver cámaras de vigilancia que monitorean y graban actividad alrededor de una zona de interés. Estas cámaras transmiten la información y suelen grabar lo captado en un sistema de almacenamiento. Casos similares podemos encontrar en distintos elementos en casa y trabajo. Por ejemplo: ciertas impresoras de oficina tienen la capacidad de guardar los documentos escaneados en memoria, por lo que algunas políticas prohíben el uso de estas impresoras para documentos considerados confidenciales dentro de la empresa.

Finalmente, se debe considerar los casos en que la memoria se encuentre encriptada de modo que no se puede realizar investigación alguna sobre ella. Actualmente existen varias opciones para encriptar toda la data dentro de un disco duro o memoria extraíble, donde para poder acceder a la información se suele recurrir a una contraseña. Desencriptar esta información suele ser difícil, por lo que se recomienda ver la forma de evitar llegar a ese punto (averiguando la contraseña a través de otra pista en la escena, por ejemplo).

RETO: Determinar y argumentar si los siguientes equipos poseen memoria que pueda contener evidencia:

- **Google Chromecast**
- **Smartwatch (escoger un fabricante y modelo en particular)**
- **Amazon Echo**

NOTA: Obviar el hecho de que transmitan información a Internet.

Teléfonos móviles

Los teléfonos móviles guardan otro tipo de información: lista de llamadas, mensajería instantánea, correos, redes sociales, entre otros. Con estos equipos se mantiene el principio de no alterar la evidencia, pero esto suele ser muy difícil por las siguientes razones:

- Conexión a Internet: Aun estando en posesión de la policía, el equipo sigue recibiendo y enviando información (notificaciones, correos, información de localización, etc)
- Energía: Estos equipos poseen una batería para su operación, la cual con el tiempo termina descargándose. Al requisar un teléfono, debe requisarse también el cargador.
- Borrado remoto: Fabricantes y ciertos programas antivirus tienen la capacidad de borrar el contenido del celular de manera remota en casos de robo. Mediante un mensaje SMS o una orden desde internet, toda la información en el equipo puede desaparecer.

A fin de preservar la integridad de la información dentro del equipo, se puede apagar el mismo o colocar en un medio aislante (bolsa Faraday o un recipiente cerrado de metal).

Bolsa Faraday (Sammons, 2012, p. 48)

Algunos puntos adicionales como volatibilidad (tiempo de vida de la información en un elemento electrónico) y buenas prácticas para la recolección de información son mencionadas por Paul Henry dentro de las referencias de este documento (Henry, 2009) (Sammons, 2012, p. 49).

6. BIBLIOGRAFÍA

Henry, P., 2009. *Best Practices in Digital Evidence Collection.* [En línea]
Available at: https://www.sans.org/blog/best-practices-in-digital-evidence-collection/
[Último acceso: 26 Setiembre 2020].

Lallie, H. S. & Pimlott, L., 2012. Challenges in applying the ACPO principles in cloud forensic investigations. *Journal of Digital Forensics Security and Law,,* 7(1).

National Police Chiefs' Council, 2020. *Frequently Asked Questions.* [En línea]
Available at: https://www.npcc.police.uk/About/QuestionsandAnswers.aspx
[Último acceso: 8 Marzo 2020].

Sammons, J., 2012. *The basics of digital forensics: The primer for getting started in digital forensics.* s.l.:Syngress.

The Forensics Library, 2020. *Edmond Locard - The Forensics Library.* [En línea]
Available at: http://aboutforensics.co.uk/edmond-locard/
[Último acceso: 8 Marzo 2020].

THE GATES RUBBER COMPANY, a Colorado corporation, Plaintiff, vs. BANDO CHEMICAL INDUSTRIES, LIMITED, a Japanese company (1996) Schlatter, O. Edward.

Turner, M., 2017. *Computer Evidence - Case of Sergeant Gurpal Virdi.* [En línea]
Available at: http://www.computerevidence.co.uk/Cases/Virdi/Articles/Virdi.htm
[Último acceso: 8 Marzo 2020].

Vandeven, S., 2014. *Forensic Images: For Your Viewing Pleasure.* s.l.:SANS Institute.

Williams, J., 2012. *ACPO Good Practice Guide for Digital Evidence,* s.l.: Metropolitan Police Service.


ITU