CIBERCRIMEN Y EVIDENCIA DIGITAL

TEMA
DESCUBRIMIENTO Y ANÁLISIS DE EVIDENCIA

MÓDULO 5

TABLA DE CONTENIDOS

MÓDULO 5

DESCUBRIMIENTO Y ANÁLISIS DE EVIDENCIA

En el presente módulo se profundizará en el proceso de investigación, siguiendo paso a paso el proceso de un investigador forense y los diversos actores que forman parte de la investigación.

1. OBJETIVO DEL MÓDULO

Reconocer el procedimiento a seguir durante una investigación de elementos digitales, siguiendo lineamientos fundamentales a fin de mantener la validez de la evidencia a encontrar.

2. PLANIFICACIÓN DE LA BÚSQUEDA

Previo a la investigación

Citando nuevamente a Sammons (2012), la investigación requiere tener distintos elementos listos para cuando la necesidad de investigar sea requerida. El lugar donde la investigación se llevará a cabo puede ser:

- **Laboratorio forense**: Lugar físico creado específicamente para llevar a cabo investigaciones de este tipo. Compuesto de varios equipos y personal entrenado en el área. Requiere de una gran inversión y personas dedicadas, pero ofrece también la opción de brindar entrenamiento y brindar estándares de seguridad y protección de la información trabajada. Opción usada por policías y fuerzas del orden.
- **Laboratorio virtual:** El centro con la evidencia y los investigadores se encuentran en lugares geográficamente distintos. Los investigadores pueden también trabajar remotamente y aprovechar de recursos ubicados en la nube. Debe considerarse tener una seguridad robusta para no generar dudas en la corte, buena conectividad de los miembros al entorno virtual y la inversión necesaria debido a los grandes recursos computacionales que conlleva.

En ambos escenarios, el acceso a la evidencia es el punto principal que considerar. Se debe tener un lugar con acceso restringido a únicamente las personas necesarias. La evidencia debe ser protegida de peligros físicos (fuego, agua, polvo, etc.) así como otras personas que puedan robarlo o manipularlo.

RETO: Buscar información sobre dos laboratorios forenses, comparándolos y determinando qué características guardan en común para poder decir que son laboratorios forenses. PISTA: Pueden que salgan más resultados si se buscan como “digital forensics laboratory”.

Case statement

Al inicio de toda nueva investigación, hay ciertas preguntas que nos ayudan a confirmar los elementos en la escena del crimen que pueden constituir evidencia (Lallie, 2017):

- **Delimitar el alcance:** Establecer los tiempos para buscar y analizar evidencia, así como el tiempo para reportar los hallazgos. En casos judiciales, la fiscalía tiene un tiempo por ley para investigar casos y en algunas situaciones como abuso infantil, la presión de determinar pruebas de posible abuso acorta el tiempo que se tiene para brindar pruebas iniciales (a fin de solicitar prisión preventiva, por ejemplo). Finalmente, se debe determinar claramente lo que se busca reportar: evidencia relacionada a algún crimen, información confidencial puesta a venta por un empleado, etc.
- **Establecer el contexto:** Las investigaciones surgen a raíz de un indicio o hecho que puede suponer indicios de un crimen o un acto que amerita investigación. El contexto ayuda a establecer posibles lugares iniciales donde buscar evidencia.
- **Determinar elementos a investigar:** Según el contexto y los tiempos, la investigación puede apuntar a priorizar ciertos elementos. Por ejemplo, si se sospecha que un empleado dirigió correos a una empresa rival, se examinaría su laptop y teléfono; o si existe indicios de haber grabaciones de cámaras de seguridad de un posible crimen, se analiza el sistema de almacenamiento de video. Este análisis también permite distinguir la especialización requerida del investigador forense (un investigador suele especializarse en un equipo o área en particular):
  - **Hardware:** Teléfono, computadoras, equipos en tiempo real, servidores de almacenamiento.
  - **Software:** Sistema operativo, software de un fabricante en particular
- **Tipo de investigación:** Criminal, civil, corporativa. Cada una tiene un distinto comportamiento.

Todo el alcance mencionado en los puntos anteriores queda registrado en un documento (case statement) que es usado al inicio de las investigaciones.

Plan de trabajo y documentación

Todo laboratorio cumple con procedimientos para el manejo de evidencia debidamente documentados. Para cada investigación se establecen los pasos y las personas necesarias dentro del mismo. Esto para asegurar “un análisis de resultados acertados y confiables” (Sammons, 2012, p. 32). Además de las acreditaciones, hardware y software necesarios para lograr este objetivo, se debe establecer un plan de trabajo adecuado y la documentación a entregar producto de la investigación.

El plan de trabajo, indiferente de la metodología a usarse, refleja los tiempos indicados en el Case Statement y las tareas con sus respectivos intervalos de tiempo para lograr el objetivo de la investigación. Las tareas confirman la evidencia a buscar, la cantidad de información que el tiempo permite analizar y las personas responsables de cada una de las tareas.

Finalmente, la documentación que arroja la investigación puede considerar lo siguiente (Lallie, 2017) (Sammons, 2012):

- **Formularios:**
  - Usados como guía durante la ejecución de las tareas que guardan la información relevante.
  - Ejemplos: Descripción de evidencias, cadena de custodia, etc.
- **Registros:** Notas del examinador donde detalla fechas y tiempos, hallazgos, y acciones realizadas durante la investigación.
- **Reportes:**
  - Generados al final de una tarea (por el investigador, oficiales de la ley, etc), así como al final de la investigación.
  - El reporte final del examinador es el documento a entregar al fiscal o cliente que detalla la evidencia analizada, **el resumen de las acciones** que formaron parte de la investigación (registro), **los resultados y las conclusiones**, entre otros.

En el reporte final se debe establecer claramente las acciones y los resultados de la investigación a fin de que puedan ser entendidos por la audiencia a la que va dirigido el documento.

3. CADENA DE CUSTODIA

Registros en la cadena de custodia

La cadena de custodia es un documento que funciona como registro de la forma en que la evidencia ha sido manejada. Indica las personas sobre las cuales la evidencia se encontraba bajo su cuidado y responsabilidad:

- Donde la evidencia fue encontrada (incluir aparte fotografías y etiquetas identificando las circunstancias del hallazgo).
- La persona que lo recuperó de la escena del crimen, incluyendo fecha y hora.
- La persona que recibió la evidencia, incluyendo fecha y hora.
- Las distintas personas que tuvieron acceso a la evidencia, incluyendo fecha y hora.

Todo movimiento de la evidencia debe ser documentado al detalle, tratando siempre de minimizar el tiempo en que cualquier persona necesaria tenga acceso a los equipos. De no cumplir con este procedimiento, la evidencia podría considerarse comprometida y finalmente no ser aceptada por el fiscal o el cliente como fuente confiable de información. Esto podría terminar desbaratando la hipótesis, aun cuando la evidencia argumente sin cuestión a duda la validez de la tesis fiscal.

Del mismo modo, la evidencia debe ser plenamente identificada a lo largo de la cadena de custodia para evitar cualquier supuesto de suplantación de esta. Para ello se pueden usar etiquetas o marcadores permanentes con algún código que los una a la cadena de custodia, e incluso la persona que recolectó la evidencia puede ser llamada a testificar y confirmar que la evidencia es la misma que encontró en la escena del crimen y que las marcas que lo identifican son las que la persona escribió

(Sammons, 2012, p. 52). Ambos deben ir a la par, uno siendo la fuente de información y el otro el registro de lo sucedido con la fuente.

Aseguramiento de la evidencia

Sammons (2012) también indica el tratamiento de evidencia de dimensiones pequeñas. Mediante el uso de bolsas selladas, las cuales pueden ser de papel, plástico o material antiestático para evitar daños por electricidad estática, se coloca sobre el sello la fecha a fin de detectar cualquier alteración sobre el sello que pueda confirmar la manipulación de la evidencia.

A continuación, se muestra un documento que lleva el registro de evidencias para casos de incendio. Si bien no es directamente aplicado para casos de evidencia digital, sólo ayuda a entender que la importancia de la cadena de custodia aplica a todo tipo de investigaciones.

ITU Academy
empowering minds

ATS

APPLIED TECHNICAL SERVICES, INCORPORATED

1190 Atlanta Industrial Drive Marietta, GA 30066 (770) 423-1400 Fax (770) 424-6415 e-mail fire@atslab.com

EVIDENCE TRANSMITTAL

Date:_____ Verbal Report To: _____

Phone #: _____

Submitted By:_____ Written Report To:_____

_____ _____

_____ _____

_____ _____

File #:_____ Invoice To:_____

Insured:_____ _____

Claim Number:_____ _____

Date of Loss:_____ _____

ATS Reference #_____ _____

Description of Evidence: Container, Size Type of Material, Condition of Material (burned or unburned)	Location Collected
1._____	_____
2._____	_____
3._____	_____
4._____	_____
5._____	_____
6._____	_____

Special Instructions:_____

Chain of Evidence
(Signature Required)

From:_____ To:_____ Date:_____ Time:_____

From:_____ To:_____ Date:_____ Time:_____

From:_____ To:_____ Date:_____ Time:_____

From:_____ To:_____ Date:_____ Time:_____

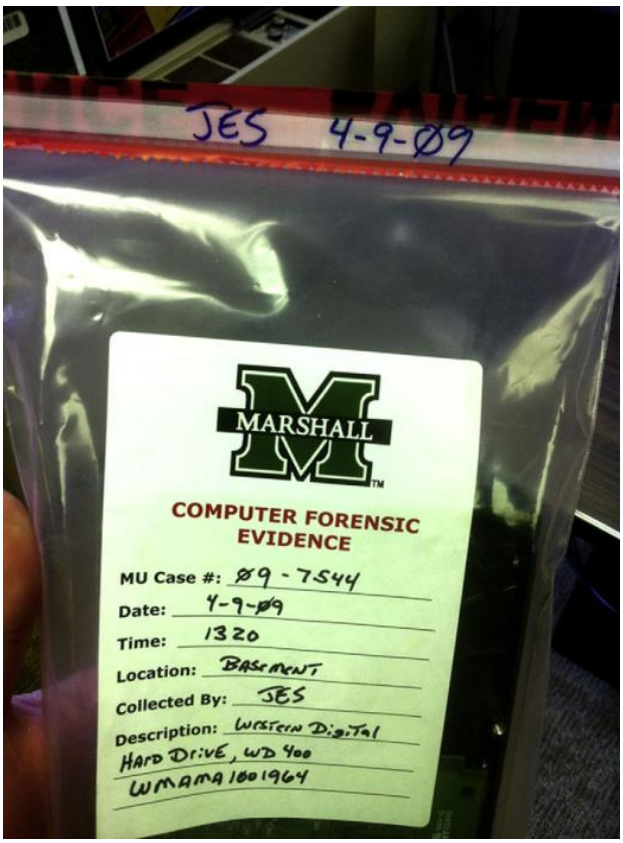
ATS 800 (10/99)

Professional Engineers
Design • Consulting • Testing and Inspection
Members in AAFS, ACS, ASM, ASME, ASNT, ASQC, ASTM, AWS, FSCT, IAAI, NACE, NCSL, NFPA, SAFS
GEORGIA SOCIETY OF PROFESSIONAL ENGINEERS, NATIONAL SOCIETY OF PROFESSIONAL ENGINEERS

Ejemplo de documento indicando la cadena de custodia de evidencia (Lentini, 2013)

RETO: Encontrar un ejemplo de un documento que presente la cadena de custodia para investigación forense de equipos digitales y compararlos con la imagen previa

Finalmente, un último ejemplo del etiquetado de evidencia, esta vez mediante el uso de bolsas para elementos pequeños.



Evidencia sellada en una bolsa de plástico (Sammons, 2012, p. 53)

4. MANEJO DE ESCENA DEL CRIMEN

El investigador de la escena del crimen tiene una tarea muy importante a la hora de requisar la evidencia ya que cualquier acción a realizar puede dañar e invalidar la evidencia. La persona encargada debe estar bien entrenada para reaccionar ante una escena del crimen (sea un caso penal o civil). Son dos tareas principales las que un investigador tiene a cargo:

- Capturar información que pueda perderse más adelante (live data). Un ejemplo es la memoria RAM de un equipo y documentando lo que se encontraba ejecutándose en el equipo.
- Requisar evidencia a ser usada más adelante.

Dada la interconectividad que Internet y redes empresariales proveen a los equipos, en algunos casos, la escena del crimen puede encontrarse en lugares físicamente separados o fuera de nuestra jurisdicción.

En general, las acciones para la requisitoria de elementos considerados como evidencia son los siguientes (Lallie, 2017):

1. **Cuarentena de la escena:** Evitar que otras personas, principalmente el sospecho, se acerquen a los equipos y zona de interés. La cuarentena requiere determinar un perímetro donde solo personal calificado puede pasar. Dentro del perímetro se identifican las fuentes de energía y switch principal para evitar cualquier corte o manipulación de estos que puedan afectar a los equipos digitales. Por último, se requiere identificar a las personas que tienen acceso a los equipos dentro de la zona de cuarentena ya que pueden existir limitantes en la investigación como contraseñas.

2. **Cortar toda comunicación y energía hacia los equipos de interés:** Esto debe ser realizado una vez toda información en vivo ha sido capturada. La conexión de energía a retirar debe hacerse desde el extremo más cercano al equipo (por ejemplo, en una laptop sería el extremo de cable de energía conectado al equipo, y la batería). Esto se debe a que equipos que brindan energía de respaldo (ejemplo: UPS) pueden brindar energía una vez la conexión a pared se corta. Hay que mencionar que en este caso se está cortando de energía al equipo, no apagando. Se debe confirmar que el equipo está totalmente desconectado de energía y no simplemente en hibernación. Dado que desconectar la información de esta forma puede hacer perder información, se requiere tener el conocimiento para evitar la pérdida de evidencia y decidir si se requiere o no capturar la data que pueda perderse.

3. **Inspección visual, documentación y fotografías de la escena**: La inspección visual consta de la revisión de los equipos para detectar cualquier problema en ellos o cualquier distintivo que los identifique. Se debe realizar un mapa del perímetro y la ubicación de los distintos elementos dentro de ella. Notas sobre los tiempos, las personas en la escena, descripciones de la evidencia y como fue obtenida, sistemas operativos y procesos de red corriendo, todo debe ser recogido ya que constituye parte del proceso de investigación y puede ser utilizado más adelante para llegar a las mismas conclusiones si un tercero llegara a hacer la investigación. La documentación para el paso 3 se realiza tanto al momento de llegar a la escena del crimen describiendo lo encontrado, como al momento de confiscar los equipos a investigar.

4. **Requisitoria de los elementos de interés y transporte:** Visto en el apartado 6.

El paso 1 (cuarentena) también aplica a escenarios corporativos, donde se cuenta con el apoyo de personal de Tecnologías de Información y personal de infraestructura para entender mejor la interconexión de las fuentes de energía, si existen fuentes de backup, y si algunos equipos no pueden ser apagados (por ejemplo, servidores en producción).

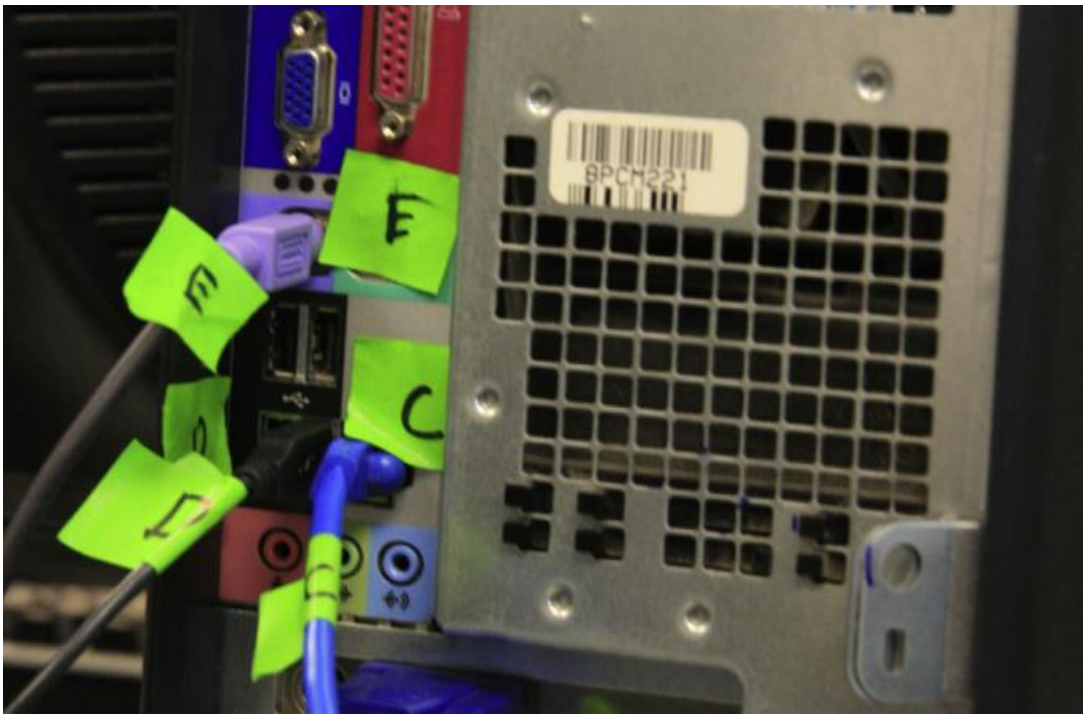
Un dato importante que considerar cuando se registra visualmente equipos como PCs o laptops es no tomar capturas de pantalla. Una captura de pantalla sobrescribe bloques de memoria en la RAM y la

inserción de equipos externos como USBs para almacenar la captura modifican el registro del sistema. En el caso que una cámara no esté disponible, recurrir al dibujo a mano alzada.

Documentación producida

La documentación por producir al llegar a la escena del crimen es:

- Descripción de la escena.
- Tipos de media encontrados.
- Detalles de las personas que ocupan regularmente el espacio donde los equipos fueron encontrados.
- Comentarios y notas de los usuarios de los equipos requisados (contraseñas, datos importantes sobre su uso, etc).
- Acciones realizadas, incluyendo horas, en la escena del crimen.
- Acciones realizadas sobre la evidencia.
- Detalles sobre cualquier otra evidencia no digital dentro de la escena del crimen (ejemplos: post-it con contraseñas, cuaderno de notas, etc).
- Formatos de Cadena de Custodia para cada elemento a requisar.



Fotografía del etiquetado de los cables y los puertos a los que los mismos estaban conectados
(Sammons, 2012)

Finalmente, dentro del paso 2, debemos considerar también la comunicación de red (cables de red o WiFi) cuando se decide confiscar los equipos. Esto se verá con mayor detalle en el siguiente apartado.

5. RED DE COMUNICACIÓN Y OTROS ELEMENTOS A CONSIDERAR EN ESCENARIOS DIGITALES

Los equipos digitales hacen que aún un equipo en reposo se encuentre transmitiendo y recibiendo información, afectando los datos presentes en la tarjeta de memoria, memoria RAM e incluso disco duro.

RETO: Investigar un ejemplo de Memory Capture Tool (usado para capturar lo que se encuentra en la memoria RAM) y cómo es usado sin modificar el equipo.

Las conexiones de red pueden considerarse también como "Live Collection" o recolección en tiempo real. Según Sammons (2012), tomar la decisión de capturar data en tiempo real implica un trabajo ininterrumpido hasta terminar el proceso donde es necesario tener todos los elementos a la mano (pausas implican añadir posibles errores dentro de la captura). Además, recordar que toda interacción en la computadora (y la respuesta de ella) debe ser anotado como parte de la documentación.

Desconectar un cable de red puede terminar deteniendo un proceso que puede formar parte de la evidencia a analizar (descarga de un archivo, conexión hacia un equipo remoto, etc). Más interrogantes se pueden presentar como la posibilidad de que un agente externo pueda conectarse de forma remota al equipo, o que un ataque digital se encuentre en proceso.

Debemos reconocer los elementos de red que indican actividad de red del equipo:

- **Tarjeta de red del equipo:** En equipos informáticos conectados a un cable de red, es posible ver actividad de red al observar el puerto de red. Las tarjetas de red suelen tener leds que parpadean si tráfico pasa a través de ellas. En el caso de conexiones inalámbricas, la información es transmitida por el aire por lo que existen equipos que pueden monitorear la actividad radioeléctrica y capturar paquetes de red transmitidos de equipos cercanos.
- **Switches:** En caso de red cableada, el cable de red llega desde el computador hasta el switch o conmutador. El switch posee también puertos con leds que indican si tráfico corre a través del cable.
- **Firewall:** El firewall o cortafuegos suele ser la puerta de salida de equipos hacia redes inseguras como Internet. En caso el equipo se esté comunicando con el exterior, el firewall debería ser capaz de reconocer las conexiones asociadas al equipo.

Registros (logs)

Sammons (2012) nos recuerda que muchos equipos informáticos cuentan con "logs", registros digitales de diversas actividades dentro de un equipo o una red de computadoras. Ejemplos de logs son:

- **Firewall logs:** Registro de conexiones filtradas por el equipo cortafuegos, el encargado de proteger la red de computadoras y establecer zonas de seguridad.
- **Logs de aplicación:** Registros de actividad de aplicaciones dentro de un equipo informático, incluyendo acciones que involucran recursos dentro o fuera del equipo informático.
- **Logs del sistema operativo:** Acciones hechas a nivel de sistema como encendido, apagado, reinicio, etc.

Todos estos registros llevan fechas, horas y descripción de la acción realizada, entre otra información dependiendo del sistema operativo y/o el fabricante del equipo. Esta es una fuente de información inicial que está guardada en la computadora y se actualiza conforme nuevas acciones suceden.

Tráfico de red

Otro punto en la investigación es el registro del tráfico en tiempo real del equipo. Los logs permiten saber las acciones realizadas, pero no se sabe la información que es transmitida de un punto a otro. En un escenario de red, es posible capturar la información sin afectar al equipo interviniendo la red por la que se transmite la información. Dependiendo del escenario, es posible capturar la información entrante y saliente del equipo sin interrumpir las conexiones.

RETO: Determinar si es posible analizar conexiones bluetooth y cómo.

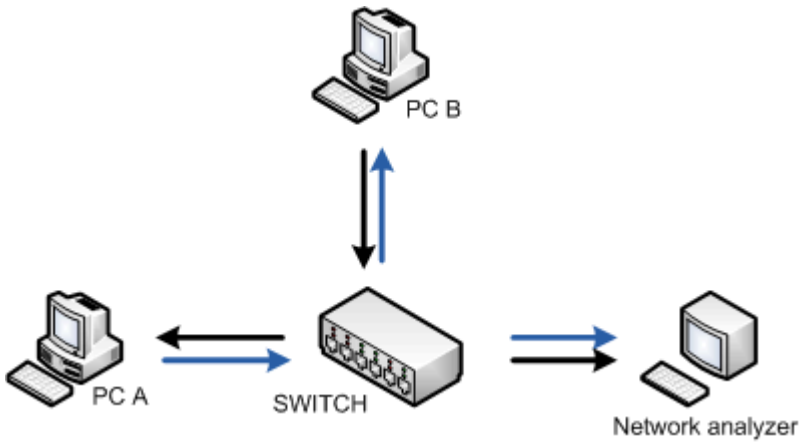


Imagen de la comunicación entre PC A y PC B, siendo enviada por un equipo intermedio (SWITCH) a un tercero (Semperboni, 2020)

No solo las computadoras y laptops son las que se comunican a través de la red. Otros equipos como impresoras y teléfonos también pueden hacer uso de recursos de red por lo que, de hacer una investigación forense de estos equipos, si la investigación lo requiere, se deberá considerar las conexiones que puedan estar cursando por los mismos.

Limitantes a este último método de investigación son la posibilidad de comunicaciones encriptadas donde no es posible observar la información transmitida de un extremo a otro. Sin embargo, en el entorno corporativo, es posible que las comunicaciones de los equipos estén siendo monitoreadas como parte de las políticas de seguridad, por lo que las comunicaciones encriptadas son transparentes para el administrador de red y, con su ayuda, para el investigador.

6. LINEAMIENTOS PARA LA ADQUISICIÓN DE EVIDENCIA

Se han visto todos los elementos que pueden terminar siendo parte de la investigación. Desde computadoras hasta consolas de videojuegos e impresoras pueden terminar siendo parte de la investigación. Hasta este punto se ha logrado investigar a fondo todos los elementos que forman parte de la escena del crimen y sólo queda transportarlos de forma segura a un lugar donde puedan ser almacenados y cuidados de forma segura. Como parte de la documentación producida, todos los elementos han sido etiquetados y descripciones de las evidencias (junto con la cadena de custodia) se encuentran listos para su transporte.

A fin de poder realizar su transporte, se recomienda dejar enfriar a los equipos (en caso estuvieran encendidos) para proceder con su transporte. Todos los elementos en este punto se colocarán en empaques (sea cartón, plástico, etc) debidamente sellados e identificados.

Como se discutió antes, la propiedad juega un papel importante. En casos donde las fuerzas del orden son las llamadas a confiscar los elementos, se deberá contar con la orden del juez que indique los alcances de los elementos que pueden ser obtenidos producto del allanamiento. Sammons (2012) menciona que dependiendo de las leyes del país y de lo indicado en la orden del juez, sólo equipos que puedan suponer estén relacionados con la materia de investigación pueden ser requisados. Sin embargo, en entornos privados suele ser la empresa la dueña de los equipos por lo que la requisición no requiere del visto bueno del usuario.

Los elementos requisados son en primer lugar enviados al lugar donde se hará la investigación. Es aquí donde se hará la copia digital de la memoria en los equipos, lo cual puede tomar varias horas. Es por ello que esta actividad se hace fuera de la escena del crimen, a diferencia de la captura de data en vivo. Una vez hecha la imagen digital de los elementos, estos serán enviados a un lugar de almacenamiento donde permanecerán nuevamente sellados y fuera del contacto de personas ajenas al responsable de su cuidado (indicado en la cadena de custodia).

7. BIBLIOGRAFÍA

Lallie, H., 2017. *Course: Digital Forensics.* Coventry: s.n.

Lentini, J., 2013. Evidence Collection at Fire Scenes. En: *Encyclopedia of Forensic Sciences.* s.l.:Elsevier, pp. 387-391.

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

Semperboni, F., 2020. *How to analyze traffic with SPAN feature.* [En línea]
Available at: https://www.ciscozine.com/how-to-analyze-traffic-with-span-feature/
[Último acceso: 26 Setiembre 2020].