



CIBERCRIMEN Y EVIDENCIA DIGITAL

TEMA
INFORMACIÓN Y
EVIDENCIA EN ENTORNOS
DIGITALES

MÓDULO 6

TABLA DE CONTENIDOS

MÓDULO 6	3
INFORMACIÓN Y EVIDENCIA EN ENTORNOS DIGITALES	3
1. OBJETIVO DEL MÓDULO.....	3
2. SISTEMA DE ARCHIVO EN DISCOS DUROS	3
Creación de una copia.....	3
Tipos de copia	4
3. BITS Y VALORES A CONSIDERAR EN ANÁLISIS DE ARCHIVOS	5
Planificando la búsqueda	5
Realizando búsqueda de palabras clave	6
Manejo de resultados de búsqueda	7
Análisis de la evidencia	7
4. MANEJO DE ARCHIVOS ELIMINADOS EN DISCOS DUROS.....	8
5. METADATA EN ARCHIVOS	9
6. REGISTRO DEL SISTEMA	11
Organización del disco duro	11
Registro de Windows	12
7. MÉTODOS DE REPORTAR LOS HALLAZGOS	12
8. ESTRUCTURA Y ELEMENTOS A CONSIDERAR EN LOS REPORTES	13
9. BIBLIOGRAFÍA	15

MÓDULO 6

INFORMACIÓN Y EVIDENCIA EN ENTORNOS DIGITALES

A continuación, se verá el proceso de examinación y análisis de la evidencia. Para esto se hará un enfoque en un caso en particular. Se hará una revisión del proceso de obtención de la copia digital, la búsqueda de data y el análisis que determine elementos de valor, logrando así obtener la información a reportar al público interesado.

1. OBJETIVO DEL MÓDULO

Reconocer el proceso de examinación y análisis en un disco duro con la estructura de archivos del fabricante Windows.

2. SISTEMA DE ARCHIVO EN DISCOS DUROS

Siguiendo lo visto en el módulo anterior, los elementos considerados como evidencia de la escena del crimen han sido transportados finalmente al laboratorio forense para ser examinados. Es importante determinar que los equipos no han sido alterados (la cadena de custodia ayuda en este caso), por lo que la primera tarea del examinador del caso es asegurar la integridad de la información dentro del equipo.

Dado que existen gran cantidad de equipos que pueden haber sido confiscados y que cada uno puede representar un método distinto de análisis, se verá el caso particular del disco duro de una PC o laptop. Los discos duros son unidades de almacenamiento que guardan información sin que esta se pierda en caso el equipo deje de estar energizado. Sin embargo, el simple acceso a la información dentro de la unidad puede suponer la escritura en registro del equipo conectado y las acciones parte de ese acceso.

Creación de una copia

A fin de poder crear la imagen digital de la unidad de almacenamiento requerimos dos elementos (Lallie, 2017):

- **Estación de análisis (Forensic Workstation):** PC o laptop del examinador con las herramientas de software necesarias para la investigación.
- **Protección contra escritura:** Algunos discos duros poseen la opción en ellos de evitar la escritura en los mismos, caso contrario se necesitará un “Write Blocker”. Este último forma un puente entre la estación de análisis y la unidad de almacenamiento, bloqueando toda acción o comando de escritura sobre el equipo. Hay dos técnicas para el bloqueo de escritura:

- Negación de todos los comandos de escritura hacia el disco y reporta a la estación de análisis de que el comando se ejecutó satisfactoriamente.
- Usando memoria cache dentro del dispositivo (cache based) para guardar los comandos de escritura durante la duración de la sesión. Esto hace creer al sistema operativo de que el disco permite la escritura, mientras este usa la memoria interna para que el sistema operativo vea en ella los cambios a los sectores de disco que intenta sobrescribir.

Es importante que como parte de las acciones en la estación de análisis se realice un escaneo de antivirus y que esto sea registrado en la documentación. Del mismo modo, la estación de análisis debe estar aislada, lo cual significa que toda conexión de red debe estar deshabilitada en la misma. Hecho esto y conectando de forma segura el disco duro la estación de análisis (evitando la escritura sobre el disco duro), el siguiente paso es realizar la imagen o copia del disco.



“Write blocker” usado para evitar la escritura en unidades de disco duro (Wikimedia Commons, 2011)

Tipos de copia

Anteriormente se presentaron algunas herramientas (programas) usados para la clonación de un disco duro (por ejemplo: FTK Imager y EnCase Forensic Image). Estos programas tienen como objetivo realizar la copia bit por bit de la unidad de almacenamiento, incluyendo todos los

sectores del disco duro. El resultado de la copia es un archivo igual de extenso que el disco duro, por lo que realizar el proceso de copia demora varias horas según la capacidad del disco. Hay tres tipos de copia posible (Lallie, 2017):

- **Imagen:** Copia bit por bit de todas las porciones del disco original.
- **Copia espejo:** Copia de todos los elementos “visibles” del disco original.
- **Copia a bit:** Copia de sector por sector a tal punto que el investigador puede cargar la copia y arrancar su estación de análisis desde el sistema almacenado en la copia, como si fuera el disco duro original.

Al finalizar la copia, el siguiente paso es realizar un cálculo hash tanto de la copia original como de la copia. En algunos casos, el valor hash es calculado por el software encargado de hacer la copia digital.

Finalmente, en nuestro escenario se usará una imagen. Para creación de imágenes se puede usar FTK.

3. BITS Y VALORES A CONSIDERAR EN ANÁLISIS DE ARCHIVOS

La copia digital por sí sola no es suficiente para poder realizar la etapa de Examinación. Se requiere de una herramienta que permita analizar la amplia data que guarda la copia. La cantidad de archivos que puede guardar una unidad de disco es tanta que se requieren de palabras claves, indicios y extensiones en particulares que puedan guardar la información que buscamos.

Una de las herramientas de análisis de software es **Autopsy**, un software libre (no requiere de licencia) que sirve de punto de inicio a aquellos que desean aprender a realizar investigaciones. Tras cargar una copia, esta herramienta permite la búsqueda rápida de toda la información presente en la imagen (archivos en memoria, eliminados, recuperados, etc).

La herramienta Autopsy es de código abierto, lo que permite a personas experimentadas ver el código fuente y cambiar el funcionamiento de este. Módulos y algoritmos pueden ser mejorados por el usuario haciendo así la investigación más eficiente. Sin embargo, esta herramienta es únicamente para entrenamiento y aprendizaje, ya que la capacidad de manipulación que se tiene sobre el mismo puede ser cuestionado en corte. Para investigaciones penales se tienen otras opciones licenciadas (ejemplo: EnCase).

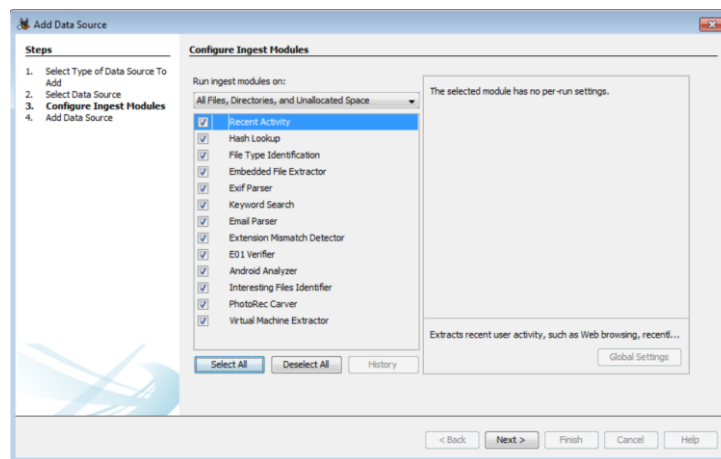
Planificando la búsqueda

Cuando un objeto se pierde, podemos buscar en todos los lugares posibles examinándolos detenidamente. Si bien esto ayudaría a encontrar el objeto con certeza, el tiempo que nos

tomaría lo haría una tarea imposible. Es distinto tratar de buscar unas llaves en un cuarto que en un edificio de 25 pisos. De forma similar sucede al buscar un elemento de evidencia en el mar de bytes del disco duro.

Como punto de partida, el examinador tiene presente el Case statement. En él se describe el objetivo, los elementos a investigar y los tiempos que se tienen para la búsqueda. Esto permite establecer palabras claves de búsqueda y priorización de tiempos.

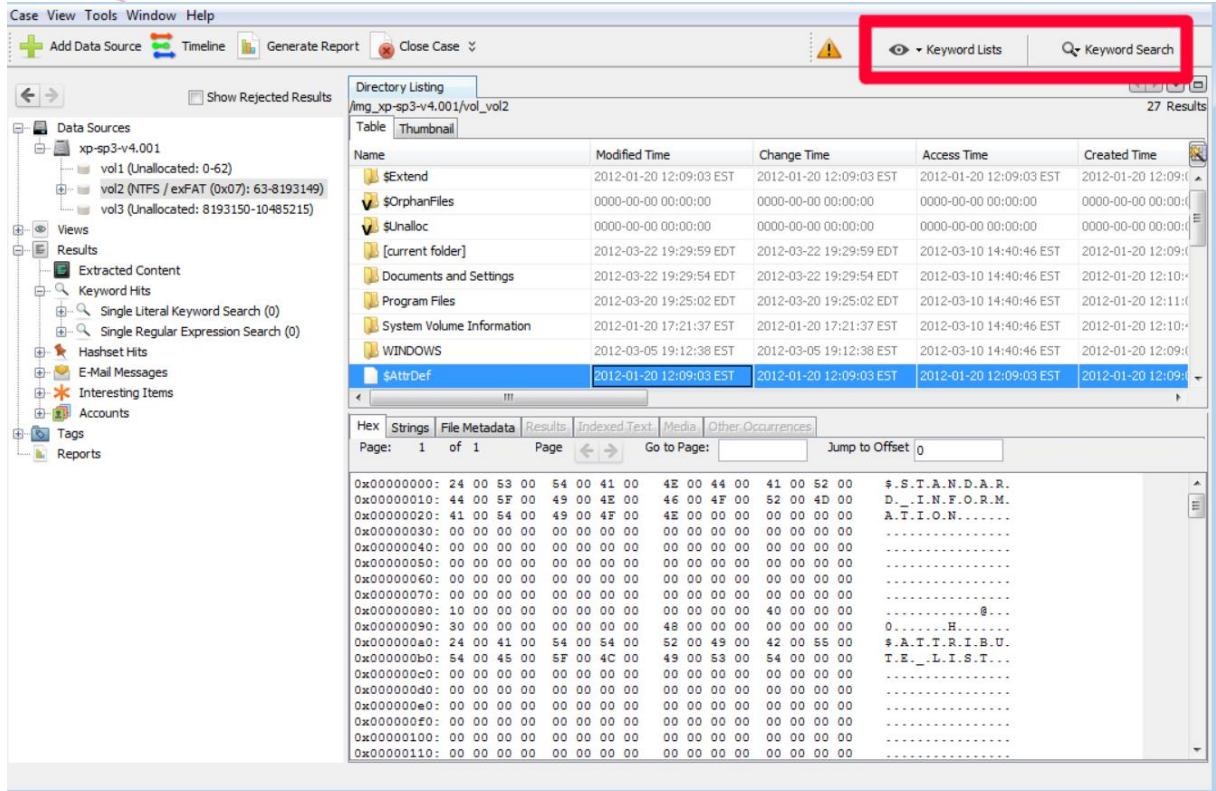
Por otro lado, varias herramientas incluyendo Autopsy durante la ingesta del archivo tienen módulos de pre-búsqueda que permiten buscar ciertos tipos de archivo según lo indique el examinador. Esto facilita la búsqueda de información y sirve como punto de partida.



Ventana de elección de módulos de ingestión de datos en Autopsy (Basis Technology, 2020)

Realizando búsqueda de palabras clave

Las palabras claves no deben ser muy cortas o pueden generar muchos resultados. Por lo general las búsquedas pueden llegar incluso a durar toda la noche. Estas búsquedas pueden ser guardadas para futura referencia en caso se desee buscar diversas palabras asociadas (por ejemplo: una búsqueda con palabras claves relacionadas a drogas como cocaína o marihuana, y otra búsqueda con palabras claves relacionadas a homicidio como asesinato o sicario).



The screenshot shows the Autopsy software interface. At the top, there is a menu bar (Case, View, Tools, Window, Help) and a toolbar with buttons for 'Add Data Source', 'Timeline', 'Generate Report', and 'Close Case'. A red box highlights the 'Keyword Lists' and 'Keyword Search' buttons. The main window displays a 'Directory Listing' for the path '/img_xp-sp3-v4.001/vol_vol2'. It shows a table of files with columns: Name, Modified Time, Change Time, Access Time, and Created Time. The files listed include \$Extend, \$OrphanFiles, \$Unalloc, [current folder], Documents and Settings, Program Files, System Volume Information, WINDOWS, and \$AtrDef. Below the directory listing, there is a 'Hex' view showing the raw data of the selected file, with columns for Hex, Strings, File Metadata, Results, Indexed Text, Media, and Other Occurrences. The 'Results' column shows the search results for the keyword 'S.T.A.N.D.A.R.D.'.

Opción de búsqueda de palabras claves y listas de palabras en Autopsy (Basis Technology, 2020)

Finalmente, Autopsy posee información detallada de su uso en el siguiente enlace:

<http://sleuthkit.org/autopsy/docs/user-docs/4.17.0//>

Manejo de resultados de búsqueda

Antes de poder empezar con el análisis, se requiere revisar los resultados de la búsqueda de una forma no tan detallada. Esto porque los resultados pueden seguir siendo muchos y no todos merecen la atención del examinador. Durante esa búsqueda rápida manual, cualquier elemento que el examinador considere importante puede ser marcado para futuro análisis. De ese modo el examinador escoge lo que considera merece su atención y pasará a la fase de análisis. A este proceso se le conoce también como Bookmarking (Lallie, 2017). Hay que considerar que es posible marcar incluso archivos eliminados listados por la herramienta.

No existe una guía para el bookmarking, depende enteramente del conocimiento y experiencia del examinador los elementos que considera valen la pena analizar. De ver necesario, se pueden realizar más búsquedas y marcar elementos para futuro análisis. Estando satisfecho el examinador, el siguiente paso es el Análisis de los elementos identificados como relevantes.

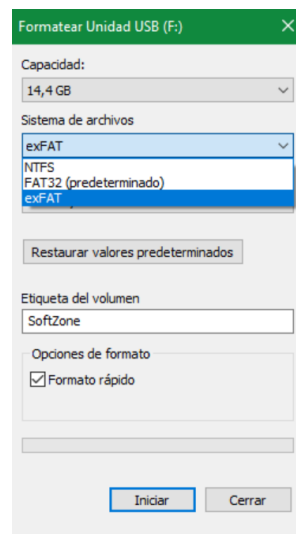
Análisis de la evidencia

4. MANEJO DE ARCHIVOS ELIMINADOS EN DISCOS DUROS

Sammons (2012) apunta a entender cómo funciona la eliminación de un archivo. Un usuario tiende a borrar archivos en Windows al enviarlos a la Bandeja de Reciclaje. La eliminación final de un archivo de cara al usuario puede ser el vaciado de la Bandeja de Reciclaje. Si bien a nivel de usuario el archivo puede no encontrarse dentro de su alcance, de cara al sistema, el archivo aún sigue presente.

La forma en que la computadora entiende la eliminación de un archivo es que el espacio de memoria que ocupa el archivo está disponible para ser sobrescrito y usado. Esto significa que hasta que el sistema no haga uso de ese espacio de memoria, el archivo puede recuperarse. Es más, aún si parte del espacio de memoria es usado por el sistema, parte del archivo aún puede ser recuperable.

Otro ejemplo de archivos eliminados recuperables es el Formato Rápido. Cuando tenemos una memoria USB, tenemos la opción de escoger si usar esta opción o no.



Ejemplo de opciones de formato de un USB (Velasco, 2019)

Escoger formato rápido es similar a marcar el espacio de memoria en cuestión como disponible. Algunos usuarios con conocimiento de este detalle pueden usar software para sobrescribir espacios libres de memoria y así ocultar la información borrada.

5. METADATA EN ARCHIVOS

Los archivos poseen información que no se aprecia directamente cuando abrimos y editamos el mismo. Datos como fechas, autores, entre otros se encuentran dentro del archivo, pero a la vez no es apreciable a simple vista. Lo mismo sucede con las imágenes. Para entender más este concepto, analizaremos una imagen para entender mejor lo que sucede.

El concepto detrás de esta información aparentemente inexistente pero presente es **metadata**. Metadata puede entenderse como “información sobre información”. Es parte del archivo que sirve para entender la información que guarda, así como características de ella.

RETO: Descargar la siguiente imagen: https://exiv2.org/include/img_1771.jpg. Buscar un visualizador de data EXIF (EXIF viewer) y subir la imagen. Reportar que información sobre la imagen brinda el visualizador.

Viendo el reto anterior, podemos apreciar que una imagen puede guardar gran cantidad de información no visible en la imagen misma. ¿Cómo logra el visualizador EXIF descifrar la imagen? Eso es porque el visualizador analiza el contenido del archivo a nivel de bits y según los valores determina lo que la imagen guarda internamente.

La ventaja de ver un archivo en hexadecimal y no a través de visualizadores es que los valores en bits no mienten. Un usuario puede cambiar la extensión del archivo, pero esto no convertirá al archivo de imagen en un documento de texto. Por ejemplo, podría cambiar la extensión JPG a DOCX. El sistema intentará abrir el documento con Microsoft Word y asumirá que el archivo está dañado. Para otro usuario, el archivo no es más que un archivo dañado y seguramente lo eliminará evitando identificar los artefactos o evidencia oculto en él. Sin embargo, cambiar la extensión no significa cambiar la estructura de la metadata.

00000	FF	D8	FF	E0	00	10	4A	46-49	46	00	01	01	01	00	F0	y0yà--JFIF....8
00010	00	F0	00	00	FF	FE	00	83-46	69	6C	65	20	73	6F	75	..8..ÿp..File sou
00020	72	63	65	3A	20	68	74	74-70	3A	2F	2F	63	6F	6D	6D	rce: http://comm
00030	6F	6E	73	2E	77	69	6B	69-6D	65	64	69	61	2E	6F	72	ons.wikimedia.or
00040	67	2F	77	69	6B	69	2F	46-69	6C	65	3A	4C	75	6E	61	g/wiki/File:Luna
00050	72	5F	52	65	67	6F	6C	69-74	68	5F	37	30	30	35	30	r_Regolith_70050
00060	5F	66	72	6F	6D	5F	41	70-6F	6C	6C	6F	5F	31	37	5F	_from Apollo 17
00070	69	6E	5F	4E	61	74	69	6F-6E	61	6C	5F	4D	75	73	65	in_National_Muse
00080	7F	6D	5F	6F	6C	6F	4E	61	61	6C	5F	4D	75	73	65	um_of_Natural_Hi

Primeros bytes en hexadecimal de una imagen visto desde Autopsy (Fuente propia)

Por ejemplo, imágenes con el formato JPEG pueden ser identificados con el valor FF D8 al inicio del archivo (Start of Image) (Harran, et al., 2017). Después de ello, los dos siguientes bytes indican en el siguiente marcador. En el caso de la imagen, los valores FF E0 indican que el siguiente encabezado es JFIF. Sin ir en mayor detalle, podemos buscar más información sobre el encabezado JFIF y así determinar que significan los siguientes elementos en hexadecimal.

Image 16.jpg	5,159	Regular File	9/11/2017 ...
Image 17.JPG	2,133	Regular File	9/11/2017 ...
Image 18.jpg	5,694	Regular File	9/11/2017 ...
Image 19.jpg	5,007	Regular File	9/11/2017 ...

000000	FF	D8	FF	E1	88	7E	45	78-69	66	00	00	49	49	2A	00	ÿÿá~Exif..II*.
000010	08	00	00	00	0B	00	0E	01-02	00	0B	00	00	00	92	00
000020	00	00	0F	01	02	00	06	00-00	00	B2	00	00	00	10	01
000030	02	00	0B	00	00	00	CA	00-00	00	12	01	03	00	01	00
000040	00	00	01	00	00	00	1A	01-05	00	01	00	00	00	D8	00
000050	00	00	1B	01	05	00	01	00-00	00	E0	00	00	00	28	01
000060	03	00	01	00	00	00	02	00-00	00	31	01	02	00	0F	00
000070	00	00	E8	00	00	00	32	01-02	00	14	00	00	00	08	01
000080	00	00	13	02	03	00	01	00-00	00	02	00	00	00	69	87
000090	04	00	01	00	00	00	1C	01-00	00	C0	03	00	00	20	20
0000a0	20	20	20	20	20	20	20	20-00	00	00	00	00	00	00	00

Ejemplo de una imagen con encabezado EXIF (Fuente propia)

Por ejemplo, en la imagen anterior, tenemos nuevamente los valores FF D8 que indican el inicio de la imagen. A diferencia de la imagen anterior, los siguientes dos bytes muestran el valor FF E1. Este valor indica que el encabezado siguiente es EXIF.

RETO: Ir al siguiente enlace: <https://www.media.mit.edu/pia/Research/deepview/exif.html>. Leyendo a partir del apartado Exif data structure, tratar de descifrar el significado de los valores resaltados. Usar otras fuentes de información para descifrar estos valores a discreción.

El examinador no solo examina a fondo cada pieza de información. A partir del nivel de conocimiento en temas técnicos del sospecho, la búsqueda puede volverse más y más compleja debido a archivos encriptados, estenografía, etc. Si bien el curso no cubre estos elementos, en caso de tener más curiosidad buscar Estenografía.

La metadata no solo abarca imágenes y archivos, esta puede encontrarse asociada como parte de:

- Sistemas operativos
- Aplicaciones

Finalmente, otra razón para saber el nivel de conocimiento técnico del sospechoso es porque la metadata puede ser alterada o removida completamente. En estos casos, el examinador debe apelar a su conocimiento y sentido común para determinar si la información puede ser considerada evidencia (Lallie, 2017).

6. REGISTRO DEL SISTEMA

El disco duro no solo busca guardar la información, también debe organizarla a fin de poder reconocer más adelante donde encontrar en memoria la información guardada previamente. Uno de estos formatos de organización usados en el disco duro es el File Allocation Table (FAT). Esta tabla o base de datos define la estructura del disco. La tabla FAT enlaza los distintos archivos del sistema con posiciones de memoria dentro del disco duro (Lallie, 2017).

Adicionalmente, un disco puede tener particiones lógicas. En ese caso, una de las particiones queda marcada como la partición activa, la que posee el sistema operativo para el arranque del sistema (Lallie, 2017).

Registro de Windows

El registro de Windows contiene información que el sistema operativo usa como referencia constantemente para sus operaciones (Lallie, 2017):

- Perfiles de usuario.
- Aplicaciones instaladas en la computadora.
- Tipos de documentos que las aplicaciones pueden crear.
- Hardware existente en el sistema.
- Puertos usados.

La estructura como tal es muy compleja, pero el examinador especializado en Windows es capaz de viajar dentro del registro del sistema y obtener la metadata dentro del registro. Para el investigador, esta metadata puede resultar de gran utilidad ya que guarda elementos como los comandos más recientes ejecutados por el usuario, lista de archivos más recientes usados por el usuario, programas previamente instalados (que fueron desinstalados más adelante), etc. Si bien, usuarios más especializados podrían borrar sus huellas dentro del registro, el hecho de ser usuarios con el conocimiento comprobado para hacer esto, hace que se desconfíe del hecho de no encontrar evidencias y suponer que es por obra del usuario.

7. MÉTODOS DE REPORTAR LOS HALLAZGOS

El reporte final es la pieza que engloba los resultados toda investigación realizada. El mayor reto para el examinador siempre será presentar sus hallazgos de forma que satisfaga al público objetivo. Un público cuya especialización no es la de la investigación forense, se sentirá apabullado por toda la información técnica relacionada con la búsqueda. Por otro lado, puede darse que el reporte vaya a un grupo de expertos que busquen refutar lo hallado, por lo que demostrar el nivel de conocimientos y detalle técnico es una necesidad.

En cualquiera que sea el caso, el investigador debe evitar las siguientes situaciones (Lallie, 2017):

- **Comunicación no efectiva:** Necesidad de llamar al examinador para explicar el reporte.
- **Cuestionamiento a la capacidad del examinador:** El reporte no tiene el nivel de profesionalismo requerido y se termina dudando de las capacidades técnicas del examinador.
- **Información insuficiente:** Necesidad de llamar a otro experto para que brinde más detalles que ayuden a esclarecer la evidencia.

Algunas herramientas de análisis forense ofrecen opciones de generación de reportes que dan una estructura inicial sobre la cual construir el reporte final, o simplemente ser anexado al reporte final dado que son generalmente muy técnicos y difícilmente una audiencia amplia puede entender.

El reporte final no tiene una estructura definida, sin embargo, debe considerar los siguientes puntos (Sammons, 2012):

- Acciones realizadas.
- Elementos encontrados (evidencia, artefactos, etc.)
- Análisis hecho de los elementos y conclusiones (manteniendo siempre la imparcialidad).

Además, el documento debe registrar tres declaraciones que buscan confirmar fuera de toda duda el trabajo hecho por el examinador (Lallie, 2017):

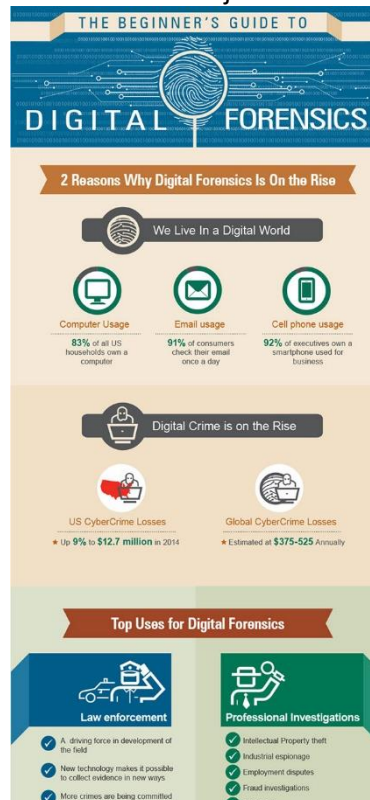
- Declaración de conformidad (Statement of compliance): Declaración del examinador de imparcialidad sobre la materia a investigar, limitándose a brindar solamente su conocimiento y profesionalismo.
- Declaración de veracidad (Declaration of Truth): Declaración de que el reporte en toda su extensión refleja solamente la verdad de lo hallado por el examinador.
- Declaración de conflictos (Statement of conflicts): Declaración de no existir conflicto de intereses por parte del examinador.

En caso el reporte no sea suficiente, otro método de reportar los hallazgos obtenidos será siempre presentarse como testigo experto para explicar con detalles lo indicado en el reporte y despejar las dudas que puedan existir.

8. ESTRUCTURA Y ELEMENTOS A CONSIDERAR EN LOS REPORTES

Se mencionó que el reporte final no tiene una estructura definida. Esto significa que la estructura queda a criterio del examinador y la forma en que vea la información llegue de modo más efectivo. Se puede incluir otros elementos como material suplementario, que puede que sea parte o toda la documentación realizada durante la investigación a fin de probar el cuidado que se tuvo respecto al trabajo realizado.

Opciones gráficas también son opciones para la presentación de la información. Una infografía mostrando el proceso de la investigación, un Flow chart con el paso a paso de las acciones, todo material que pueda ayudar en transmitir el mensaje no debe ser descartado.



Fragmento de infografía explicando la ciencia de la investigación digital forense (Prudential Associates, 2020)

Finalmente, como ayuda, se indican los siguientes lineamientos que puede tener un reporte final (Lallie, 2017) (Sammons, 2012):

- Encabezado de página:
 - Reporte de [nombre del examinador]
 - Campo de especialización
 - A nombre de [defendido/litigante]
- Carátula
 - Número de caso o investigación
 - Reporte final de [nombre de examinador]
 - Área de especialización del examinador
 - Fecha
 - Agencia encargada de la investigación
 - Información de contacto

RETO: Buscar dos reportes digitales forenses y analizar lo siguiente:

- **Similitudes entre ellos.**

Luego, escoger uno y analizar lo siguiente:

- **Público objetivo (determinar si es muy técnico o para todo público)**
- **La relación entre los resultados obtenidos y las conclusiones (analizar el pensamiento crítico del investigador).**

9. BIBLIOGRAFÍA

Basis Technology, 2020. *Autopsy User Documentation - Ad Hoc Keyword Search*. [En línea]

Available at: http://sleuthkit.org/autopsy/docs/user-docs/4.17.0//ad_hoc_keyword_search_page.html

[Último acceso: 26 Setiembre 2020].

Basis Technology, 2020. *Autopsy User Documentation - Ingest Modules*. [En línea]

Available at: http://sleuthkit.org/autopsy/docs/user-docs/4.17.0//ingest_page.html

[Último acceso: 26 Setiembre 2020].

Harran, M., Farrelly, W. & Curran, K., 2017. A method for verifying integrity & authenticating digital media. *Applied Computing and Informatics*.

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

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

Velasco, R., 2019. *Cómo formatear un USB para que funcione en Windows, macOS, Linux, Android y cualquier Smart TV*. [En línea]

Available at: <https://www.softzone.es/manuales-software-2/formatear-usb/>

[Último acceso: 26 Setiembre 2020].

Wikimedia Commons, 2011. *Wikimedia Commons*. [En línea]

Available at: https://commons.wikimedia.org/wiki/File:Portable_forensic_tableau.JPG

[Último acceso: 26 Setiembre 2020].

Prudential Associates, 2020. *A Beginner's Guide to Digital Forensics - Infographic*. [En línea]

Available at: <https://prudentialassociates.com/a-beginners-guide-to-digital-forensics-infographic/>

[Último acceso: 26 Setiembre 2020].

