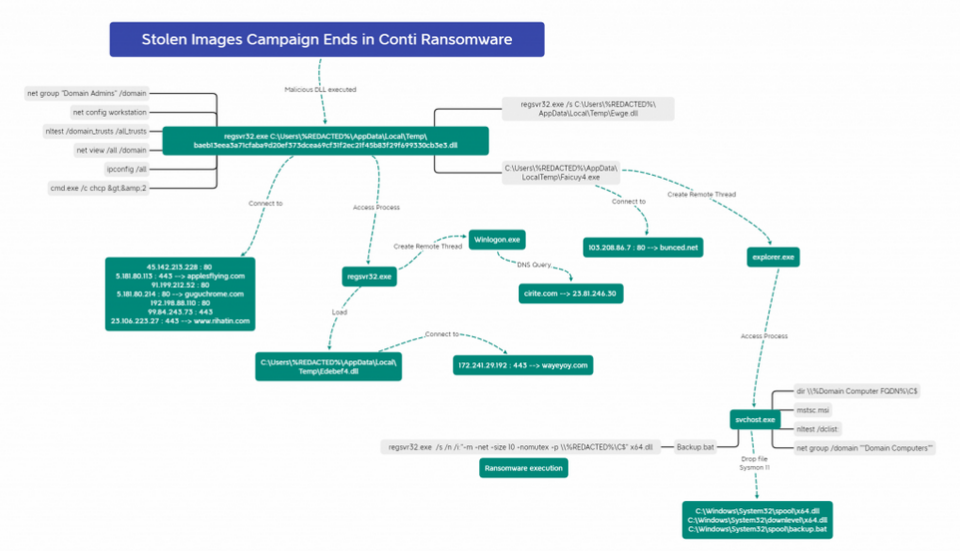
1.- Documentación y elaboración de informes de análisis forenses.

Caso práctico



The DFIR Report (Captura de pantalla.)

María después de duras semanas de trabajo, tiene que plasmar todo el trabajo realizado. Desde el análisis y procesado de todas las evidencias hasta la extracción de las debidas conclusiones.

Son muchas evidencias, informes, documentos y datos que necesita reflejar en el informe de forma clara y precisa.

Para ello, y aunque no existe un modelo oficial de informe, se basará en el formato y esquema que se considera dentro de las buenas prácticas del sector.

Sabe que todo su trabajo valdrá de poco si no es capaz de trasladarlo de una manera objetiva tanto a nivel ejecutivo como técnico en el informe.

El informe forense es clave para poner en valor el trabajo realizado.

Deberemos de ser capaces de realizar de forma correcta y reproducible la parte más importante de un análisis forense: Explicar que ha sucedido.

Para realizar este punto necesitaremos responder a las preguntas iniciales (5Q) planteadas. Si hay alguna de ellas que no se puede responer porque no se dispone de evidencias o algún otro factor externo se indicará en el informe.

1.1.- Objetivo y Alcance.

Pixabay (Dominio público)

El objetivo que tenemos llegados a este punto es claro, producir un informe que refleje todo nuestro trabajo, desde un punto de vista ejecutivo y técnico. ¿Qué características tiene que tener nuestro informe?:

- **Reproducible**: Lo primero de todo es que nuestro informe tiene que ser reproducible. Es decir, todas las acciones y conclusiones estarán basadas en hechos de tal manera que otro analista forense partiendo de las mismas evidencias, puede realizar llegaría al mismo resultado.

- **Verdadero**: Todas las afirmaciones que se indican en el informe deberán de ser objetivas y son ciertas, y cuando no haya un grado de certeza alto se hablará de hipótesis y estarán debidamente justificadas.

- **Correcto**: Las afirmaciones y conclusiones del informe deben de responder las preguntas planteadas.

- **Completo**: El informe debe contener todas las evidencias analizadas y las conclusiones para dar respuesta a las preguntas planteadas, en caso de que no se haya podido procesar una evidencia o haya alguna pregunta que no se pueda responder se

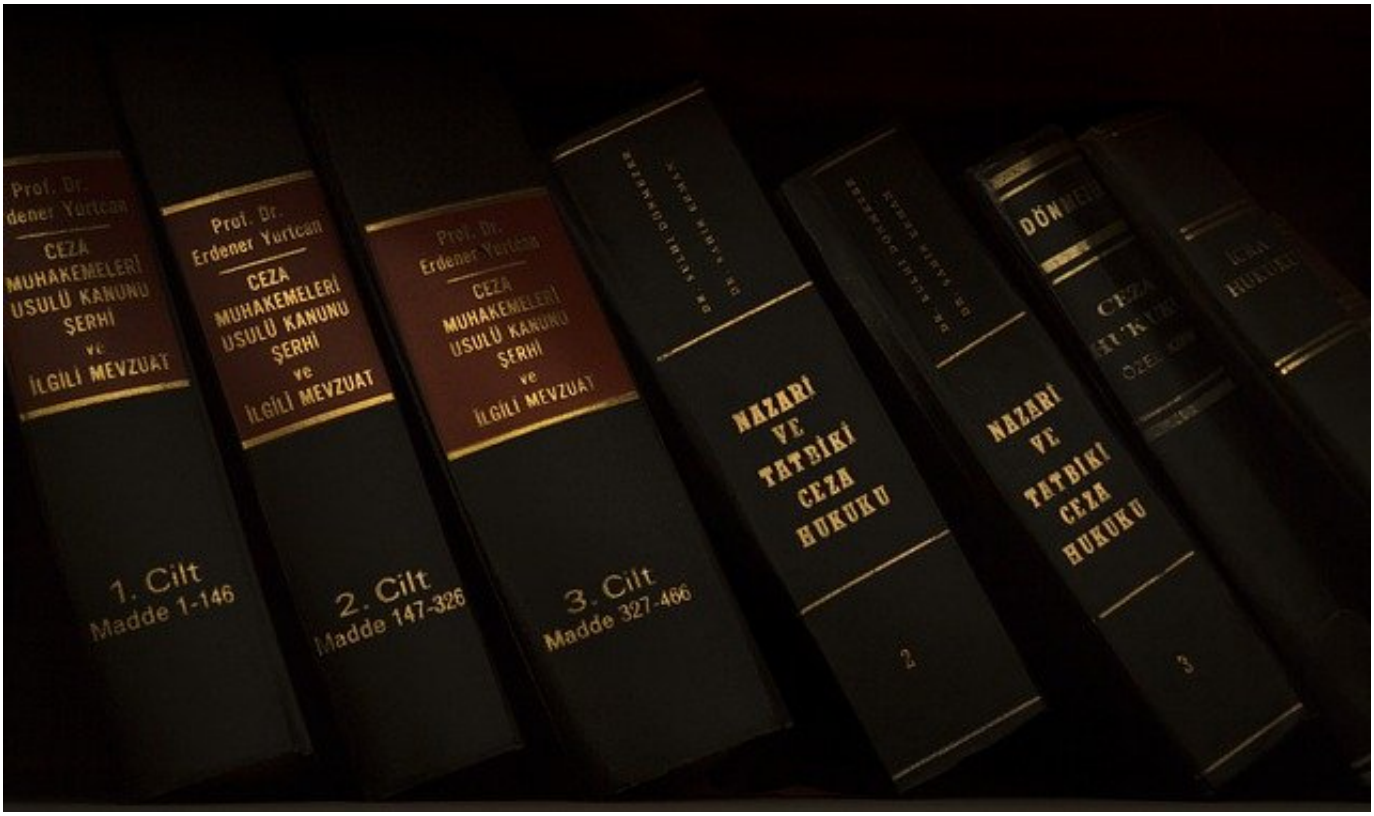
indicarán los motivos que así lo obligan.

- **Comprensible**: El informe tiene que tener dos vertientes una ejecutiva a través del resumen ejecutivo donde se plasmen las principales conclusiones a alto nivel y por otro lado en el análisis debe estar redactado de forma que sea comprensible para una persona técnica claramente de forma general.

Respecto al alcance, debemos de incluir

- Todas las evidencias identificadas.
- Todas las evidencias procesadas.
- Principales conclusiones.
- Línea temporal que abarque todos los sucesos relacionados y las evidencias que lo sustenten.

1.2.- Formato y esquema del informe.



Pixabay (Dominio público)

Aunque no existe un modelo unificado y dentro del ámbito forense podremos encontrar desde informes periciales a informes de respuesta ante incidentes. Debemos de hacer constar quien es el autor o autores del informe y qué capacitación tenemos en la materia para ello incluiremos los siguientes punto

Resumen ejecutivo

- Principales conclusiones a alto nivel.

Presentación

- Nombre completo de los autores.
- Número de colegiado o tarjeta profesional de la organización profesional en la que están colegiados los autores.
- Titulación académica.
- Resumen de nuestra capacitación en el área.
- Parte que nos requiere (un juzgado, un cliente, etc)

Alcance

- Ámbito de nuestra investigación
- Motivo o situación de nuestra contratación

- Preguntas específicas que debamos dar respuesta.

Antecedentes

- Plantilla de toma de datos inicial.
- Autorización de acceso.
- Contexto o situación particular de la investigación.

Investigación

- Fuentes de información y datos de partida.
- Estandartes, normas, reglamentos y leyes aplicables citados en los distintos apartados.
- Terminología y abreviatura.
- Herramientas utilizadas.
- Limitaciones.
- Garantía de custodia y salvaguarda de evidencias.
- Extracción de evidencias declaradas en el acta notarial.
- Geolocalización.
- Línea de tiempo.
- Investigación realizada.
- Proceso de análisis.

Conclusiones

- Dictamen final.
- Conclusiones finales.
- Hechos que soportan las conclusiones.

Anexos

- Contienen toda la información en bruto necesaria para que el análisis pueda ser reproducible por una tercera parte.
  - Documentos de análisis detallados.
  - Documentos regulatorios o específicos.
  - Documento de garantías de evidencias.

Autoevaluación

Identifica si las siguientes frases son verdaderas o falsas

El resumen ejecutivo expresa las conclusiones y debería ir por tanto con las conclusiones al final del documento.

○ Verdadero ○ Falso

Falso

El resumen ejecutivo debe de ir al principio del documento (despues de la portada, introducción de los autores, etc) y reflejar las principales conclusiones, de una manera resumida y directa sin entrar en tecnicismos.

Se considera buena práctica introducir a los autores y sus capacitaciones para con la materia.

○ Verdadero ○ Falso

Verdadero

Es una de las prácticas estándar.

Si las conclusiones son muy extensas se pueden poner como anexo al informe.

○ Verdadero ○ Falso

Falso

Las conclusiones deben de ir dentro del informe, son uno de los principales items del informe.

Debe de dotarse de contexto la investigación durante la fase de antecendentes.

○ Verdadero ○ Falso

Verdadero

El lector debe de entender los condicionantes o situaciones particulares del análisis forense.

1.3.- Normas y Recomendaciones.

BOE - Ley Enjuiciamiento Civil (Captura de Pantalla)

A nivel de recomendaciones generales del informe deberemos de:

- **Ser objetivos**, evitar opiniones o comentarios no basados en hechos
- Ceñirnos a las evidencias, evitando comentar aspectos no relacionados con las mismas.
- Expresar el **resumen ejecutivo con lenguaje formal y directo**
- Utilizar un lenguaje técnico en el proceso de análisis.
- **Explicar como llegamos de forma reproducible** a las conclusiones.
- El informe deberá de ser **legible** y por tanto deberemos de trabajar la **economía del lenguaje** (es decir expresar la información con el mínimo de la palabras necesarias pero que sea claro y conciso).
- No mencionar o hacer referencias a aspectos fuera del alcance definido, es decir, **ceñirnos al alcance.**
- **El informe ejecutivo se hace al final,** partiendo de las conclusiones finales, siendo directos y con un lenguaje ejecutivo.

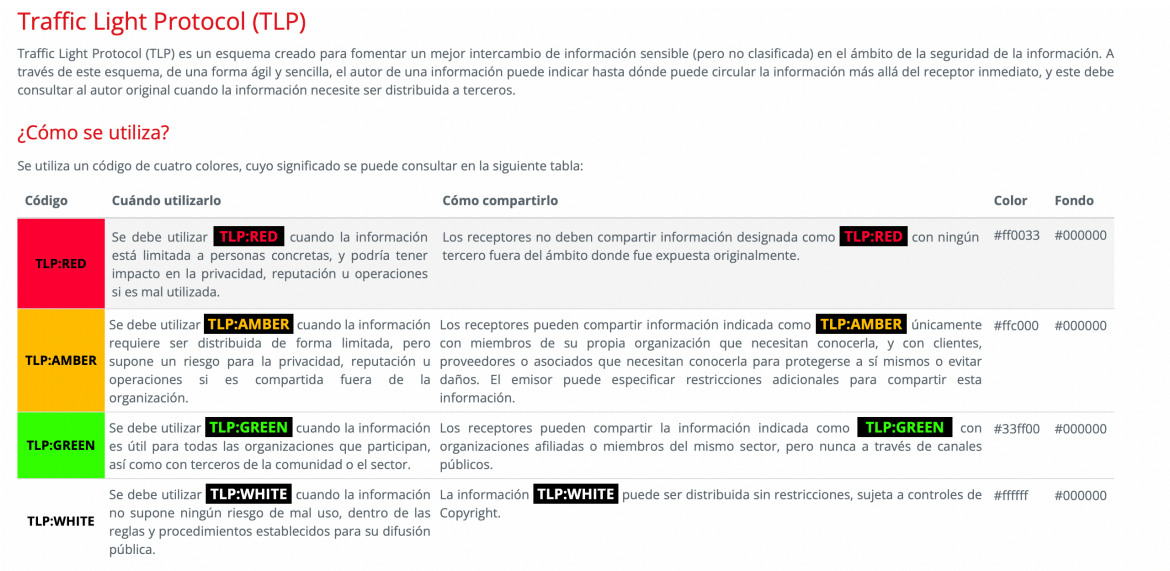
A nivel de legislación deberemos de recordar que el peritaje informático se rige por la Ley de Enjuiciamiento Civil recogida aquí.

Este punto también hace que sea recomendable estar al día de cambios legales o de legislación que pudiera afectarnos.

Debes conocer

Uno de los puntos más importantes es conocer el tipo de información que estamos escribiendo, ya que la mayoría de las veces contiene información sensible. Durante los últimos años se ha trabajo en hacer una clasificación o sellado de la información sensible pero no clasificada en el ámbito de la Seguridad de la Información mediante el protocolo TLP.

Tiene una excelente guía en la web oficial de INCIBE aquí.



Traffic Light Protocol (TLP)

Traffic Light Protocol (TLP) es un esquema creado para fomentar un mejor intercambio de información sensible (pero no clasificada) en el ámbito de la seguridad de la información. A través de este esquema, de una forma ágil y sencilla, el autor de una información puede indicar hasta dónde puede circular la información más allá del receptor inmediato, y este debe consultar al autor original cuando la información necesite ser distribuida a terceros.

¿Cómo se utiliza?

Se utiliza un código de cuatro colores, cuyo significado se puede consultar en la siguiente tabla:

Código	Cuándo utilizarlo	Cómo compartirlo	Color	Fondo
TLP:RED	Se debe utilizar TLP:RED cuando la información está limitada a personas concretas, y podría tener impacto en la privacidad, reputación u operaciones si es mal utilizada.	Los receptores no deben compartir información designada como TLP:RED con ningún tercero fuera del ámbito donde fue expuesta originalmente.	#ff0033	#000000
TLP:AMBER	Se debe utilizar TLP:AMBER cuando la información requiere ser distribuida de forma limitada, pero supone un riesgo para la privacidad, reputación u operaciones si es compartida fuera de la organización.	Los receptores pueden compartir información indicada como TLP:AMBER únicamente con miembros de su propia organización que necesitan conocerla, y con clientes, proveedores o asociados que necesitan conocerla para protegerse a sí mismos o evitar daños. El emisor puede especificar restricciones adicionales para compartir esta información.	#ffc000	#000000
TLP:GREEN	Se debe utilizar TLP:GREEN cuando la información es útil para todas las organizaciones que participan, así como con terceros de la comunidad o el sector.	Los receptores pueden compartir la información indicada como TLP:GREEN con organizaciones afiliadas o miembros del mismo sector, pero nunca a través de canales públicos.	#33ff00	#000000
TLP:WHITE	Se debe utilizar TLP:WHITE cuando la información no supone ningún riesgo de mal uso, dentro de las reglas y procedimientos establecidos para su difusión pública.	La información TLP:WHITE puede ser distribuida sin restricciones, sujeta a controles de Copyright.	#ffffff	#000000

INCIBE (Captura de pantalla)

Debes conocer

Uno de los ejemplos de estar al día con los cambios de lesgislación podría ser:

Artículo 299.2 Ley de Enjuiciamiento Civil: Medios de prueba*«También*

se admitirán, conforme a lo dispuesto en esta Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso»

Por tanto, un medio de prueba puede ser una prueba informática que pueda ser estudiada, almacenada y obtener conclusiones reproducibles.

Artículo 340 Ley de Enjuiciamiento Civil El artículo 340.1 de la Ley de Enjuiciamiento Civil (LEC) que determina respecto a las condiciones de los peritos: «*los peritos deberán poseer el título oficial que corresponda a la materia objeto del dictamen y a la naturaleza de este*».

Si se tratara de materias que no estén comprendidas en títulos profesionales oficiales, «habrán de ser nombrados entre personas entendidas en aquellas materias».

Por otra parte, en el artículo 457 de la Ley de Enjuiciamiento Criminal (LECrm) se incluyen otras consideraciones a tener en cuenta sobre como ser perito judicial al determinar que:

- Los peritos pueden ser o no titulares.
- Son peritos titulares los que tienen título oficial de una ciencia o arte cuyo ejercicio esté reglamentando por la Administración.
- Son peritos no titulares los que, careciendo de título oficial, tienen sin embargo, conocimientos o práctica especiales en alguna ciencia o arte”

1.4.- Conclusiones

Pixabay (Dominio público)

Es el punto más importante de todo el informe, las conclusiones.

Aquí trasladamos en valor todo nuestro trabajo realizado y a partir de este punto se construye el resumen ejecutivo.

El punto más importante a remarcar es **separar de una manera clara los hechos probados de las conclusiones**. Los **hechos probados son fehacientes**, de una manera clara y objetiva cualquier otro forense llegaría al mismo hecho que nosotros después de procesar las evidencias. El problema surge porque muchas veces podemos testar muy seguros de una conclusión debido a nuestra creencia basada en nuestra experiencia pero no tener la evidencia o prueba fehaciente que lo soporte, por lo que en vez de clasificarlo como hecho lo calificaríamos como hipótesis.

Algunos consejos prácticos para el analista forense:

- Trata de ser claro y directo en las conclusiones.
- Habla de hechos si tienes todas las garantías y puedes dar fe de ellas, sino es así o todavía faltan evidencias que sustenten el hecho, habla de hipótesis.
- Hablar de hipótesis no es algo malo, a veces no podemos garantizar un hecho, trata de

darles relevancia aportando datos adicionales (casos similares, otros informes periciales, evidencias que sugieren o dan cuerpo a esa hipótesis).

- Construye el resumen ejecutivo basado en las conclusiones. Intenta resumir en el menor número de palabras los hechos mas relevantes siendo claro y coherente.