1. Lee atentamente uno de los libros disponibles en las URLs que se muestran más abajo y realiza un resumen de los aspectos relacionados con el tema 1 que encuentres en el mismo y te resulten significativos.

Capítulo 1:

Un informático está acostumbrado a la rotundidad en su trabajo y a la objetividad de este, no hay matices en la informática.

Sin embargo, en un juicio, un informático pasa a ser un perito, y su trabajo a ser inspeccionado con lupa, a ser interrogado con preguntas ambiguas y malintencionadas, en las cuáles si el peritaje no ha sido realizado de forma correcta, puede hacer que el perito dé una mala respuesta o una que no sea lo suficientemente concisa.

Es por ello, que debemos tener en cuenta que al entrar en la sala de un juicio, nuestro trabajo ha de ser impecable, siguiendo las directrices establecidas por el código judicial, sin que este deje lugar a dudas o ambigüedades.

Capítulo 2:

Para llevar a cabo una recogida adecuada de evidencias que sean válidas en un juicio, es fundamental responder a las siguientes preguntas clave:

1. ¿Cuál es el escenario al que se enfrenta el análisis?
2. ¿Qué se pretende analizar: un archivo, un directorio, un disco completo o todo un sistema?
3. ¿Cuánto tiempo se tiene disponible para adquirir las evidencias?
4. ¿Dónde se almacenarán las evidencias obtenidas?
5. ¿Cuántas copias de las evidencias se deben realizar?

Es crucial, durante la extracción de la información, asegurar que tanto la copia como el original sean completamente idénticos. Además, el proceso debe garantizar que el original no sea alterado y que la copia sea exhaustiva. Para ello, es indispensable utilizar una función hash.

El uso del hash es especialmente importante, ya que permite verificar que las evidencias no han sido modificadas y que el original permanece intacto. Asimismo, debe considerarse cuántas copias de las evidencias es necesario generar para garantizar su seguridad y disponibilidad.

Capítulo 3:

A la hora de hacer un copiado de disco, es importante conocer las herramientas y metodologías que se necesitan.
En el caso del perito forense de este relato, nos encontramos con la suite Helix de e-fense para las dos metodologías de obtención de evidencias.

- Post Mortem: Se realiza sin arrancar el sistema operativo del equipo a analizar.
- Live Forensics: Se realiza mientras el sistema operativo se encuentra iniciado.

Además, de mostrarse diferentes herramientas y metodologías forenses, tales como, distribuciones forenses (Helix y CAINE), la herramienta Adepto, métodos avanzados de adquisición (DCFLDD y AFF), consideraciones técnicas, limpieza de discos (Disk Wiping), y Guymager.

Capítulo 4:

Actualmente en España no existe una regulación específica para procedimentar y garantizar la custodia de pruebas. Sin embargo, aunque no exista oficialización del procedimiento, está ampliamente aceptada la figura de la cadena de custodia como norma de facto para dar garantías al proceso de mantenimiento de las evidencias. La cuál asegura que las pruebas y conclusiones obtenidas a partir de las evidencias aportadas, sean consistentes y válidas, no habiendo sido alteradas para ningún fin con posterioridad al momento de su adquisición.

Dado que a lo largo de la investigación, es necesaria la cesión de tanto las evidencias como de las copias de estas. La cadena de custodia ha de responder a las preguntas: ¿quién es el depositario?, ¿durante qué espacio temporal lo es? y ¿cuál es la razón por la que la evidencia queda bajo su custodia?. Para de esa forma poder identificar quién ha estado en posesión de estas, y así citar a la persona correspondiente si las evidencias quedaran en entredicho.

Cabe destacar que en la Ley 1/2000 de Enjuiciamiento Civil queda recogido el objeto y finalidad del dictamen de peritos a través de su artículo 335.

Y por último, se nos muestra un ejemplo de cómo se trabaja en la empresa del perito de este relato, y cómo cada evidencia y copia realizada de esta, es acompañada de su fichero de cadena de custodia correspondiente. Para así tener identificadas y controladas todas las copias de trabajo generadas durante el proceso.

Capítulo 5:

Lo primero, destacar que cada escenario presenta sus particularidades, y que no hay una forma perfecta para todos los casos a la hora de realizar un análisis forense.

Lo segundo, es el hecho de que la mayoría de las veces, las tareas de un forense no son las más divertidas. Siendo la mayor parte de las tareas análisis de log o búsquedas de cadenas de caracteres en un gran volumen de ficheros. Además de no olvidarse que las evidencias han de ser rotundas y difícilmente refutables.

Y por último, también se ha de tener en cuenta, que muchas veces los resultados finales no suelen satisfacer al cliente, que ha visto “fantasmas donde no los hay”.

Aún así, un perito deberá de afrontar el análisis de evidencias teniendo en consideración los siguientes criterios:

- Definición de la línea temporal.

- Búsqueda de elementos o palabras clave.
- ¿Quién es quién?

Por supuesto, hay más materias a tener en cuenta, tales como:

- Las prioridades del cliente. Definiendo hasta qué punto la correcta adquisición y preservación de las evidencias prevalece sobre el resto de circunstancias.
- A la hora de analizar un disco, las búsquedas realizadas sobre el mismo deben ser exhaustivas.
- Medio fichero es mejor que nada.
- Detección de patrones de conducta más o menos definidos.
- Analizar patrones.
- Contrastar los patrones obtenidos con el cliente.
- Ser muy cuidadoso con el tratamiento de aquellos datos que puedan resultar invasivos de la intimidad de las personas afectadas.
- Ser extremadamente escrupuloso en la realización del análisis e inevitablemente esto implica ser organizado.
- Las herramientas son elementos fundamentales para el desarrollo de tareas de análisis, pero ni mucho menos lo más esencial.
- La experiencia, eficacia y buen hacer del especialista, son la clave para obtener resultados válidos y fiables.
- Desprenderse desde un principio de prejuicios y conclusiones preconcebidas.
- La visión profesional de un tercero puede dar aire fresco a la investigación en momentos de bloqueo de ésta.

<u>Capítulo 6:</u>

Es importante tener en cuenta que por muy buenos que hayan sido los procedimientos llevados a cabo, las técnicas empleadas y los resultados obtenidos, si no se reflejan correctamente en un documento, no tendrán valor alguno. Ya que al final, el valor del trabajo reside en el documento y será éste el elemento de juicio fundamental respecto de la labor del analista forense.

Un informe de estas características tiene como objetivo final transmitir información a personas que en muchas ocasiones no tienen una relación directa con la informática. Siendo esto especialmente importante, pues el propio abogado tendrá complicada su intervención en el proceso judicial si no es capaz de conocer y comprender la información esencial contenida en él.

También se ha de tener en cuenta la imparcialidad del perito, que en el informe solo deberá mostrar los resultados obtenidos en la investigación. Presentando este una línea maestra bien definida. Siendo necesario que el perito sea consecuente y evite que el informe presente hilos sueltos.

Un ejemplo de estructura válida para un informe sería:

- Antecedentes.
- Evidencias.
- Análisis y tratamiento.
- Resultados.
- Conclusiones y recomendaciones.

Por último, destacar que el análisis debe seguir una línea clara y estructurada para evitar confusión, y que las conclusiones deben estar basadas únicamente en las evidencias presentadas. Además debe incluir anexos y términos técnicos cuando sea necesario, para facilitar la comprensión

Capítulo 7:

En algunas ocasiones, el perito puede no tener acceso a la información, provocando que se desestimen evidencias ante la creencia de que no es posible su obtención, pudiendo estas resultar determinantes. Es por ello que será necesario solicitar esa información. Siendo importante tener en consideración la volatilidad de estos datos.

Es aquí donde surge la solicitud de prueba anticipada. Dado que existe el riesgo de que una prueba pudiera no practicarse porque para ello es necesario esperar a que llegue la fase de procedimientos del juicio, es posible requerir el adelantamiento de la prueba. Dicho proceso puede ser invocado por cualquiera de las partes, debiendo ser motivado y solicitado al tribunal que está llevando el caso siempre con anterioridad al inicio del juicio.

Las más habituales suelen ser las relacionadas con solicitud de datos de actividad a los proveedores de Internet y telefonía.

Se ha de tener en cuenta que a mayor información, mejor podrá el juzgado encaminar la solicitud, facilitando además su labor. También, es importante destacar las posibles discrepancias que pueden tener los ficheros de log, con las horas locales reales donde opera el proveedor correspondiente.

Este tipo de pruebas suelen ser determinantes en el desenlace de un juicio y por lo tanto hay que hacer todo lo factible para su obtención. Ya que al ser una información que solo puede aportar un tercero ajeno al caso, cobra una gran importancia. Por lo tanto la súplica deberá realizarse con la debida anticipación para que las pruebas lleguen a tiempo a la vista. Pues el resultado obtenido de la solicitud de prueba anticipada puede llegar a condicionar totalmente la estrategia en el juicio.

Capítulo 8:

Como paso previo, es necesario preparar una estrategia junto a los abogados. Ya que las perspectiva y apreciaciones del perito pueden servir como hilo conductor de las preguntas del abogado, además de servir para intentar anticiparse a las cuestiones del abogado contrario. Pues sin preparación previa, todo el trabajo de peritaje puede quedarse en nada o ser contraproducente para el cliente.

Durante el juicio el abogado presentará una nota judicial en la vista, donde la información pericial tiene gran importancia. El perito deberá colaborar técnicamente en su elaboración.

El día de la vista el perito deberá acudir con el DNI, a la espera de ser llamado como testigo pericial. Soliendo ser llamado en última instancia.

Al entrar, el juez identifica al perito y le recuerda su deber de decir la verdad, advirtiéndole sobre las sanciones por falso testimonio. Durante la vista, el perito debe reconocer el informe pericial que presenta como prueba y estará sujeto a preguntas del abogado de la parte que lo presenta, así como de la parte contraria, que intentará cuestionar su credibilidad y el informe.

También se ha de tener en cuenta que no todo el mundo está dentro del mundo de la informática, y por ello deberá intentar simplificar su lenguaje técnico. Así como mantener la calma ante preguntas relacionadas con su trabajo.

Al final del juicio, deberá firmar un documento que ratifica su testimonio y esperará la sentencia del juez, reconociendo que cada juicio es único y los resultados son impredecibles, con una posibilidad de éxito que nunca es absoluta.

Capítulo 9:

Tras lo visto en los capítulos anteriores, se vuelven a repasar los pasos claves:

- Obtener información previa: Antes de recoger evidencias, el analista debe conocer el contexto del caso y recopilar toda la información posible.
- Obtención de evidencias: La recuperación y firma rigurosa de evidencias son esenciales, asegurando su integridad y cadena de custodia.
- Identificar datos relevantes: Se deben identificar los datos importantes y establecer una línea temporal para facilitar la investigación.
- Ordenar y relacionar los datos: Es fundamental mantener la independencia del perito y asegurar que las conclusiones sean objetivas.
- Generación del informe pericial: El informe debe ser técnico y legible, reflejando garantías que aseguren la veracidad de las evidencias.
- Práctica de prueba anticipada: Si es posible, se debe asesorar al abogado sobre la práctica de pruebas anticipadas antes del juicio.

- Asesoramiento técnico: Se debe apoyar al abogado en la estrategia del juicio y en la formulación de preguntas clave.
- Intervención en la vista judicial: El perito juega un papel crucial, debiendo simplificar la exposición de su informe mientras se mantiene la compostura ante posibles ataques a su imparcialidad.

Por último, se aborda la legitimidad de prácticas de acceso a información en el ámbito laboral, destacando la importancia de contar con regulaciones claras para evitar violaciones de derechos. Presentándose sentencias que demuestran las complejidades legales en el acceso a correos electrónicos y otras pruebas en investigaciones forenses.