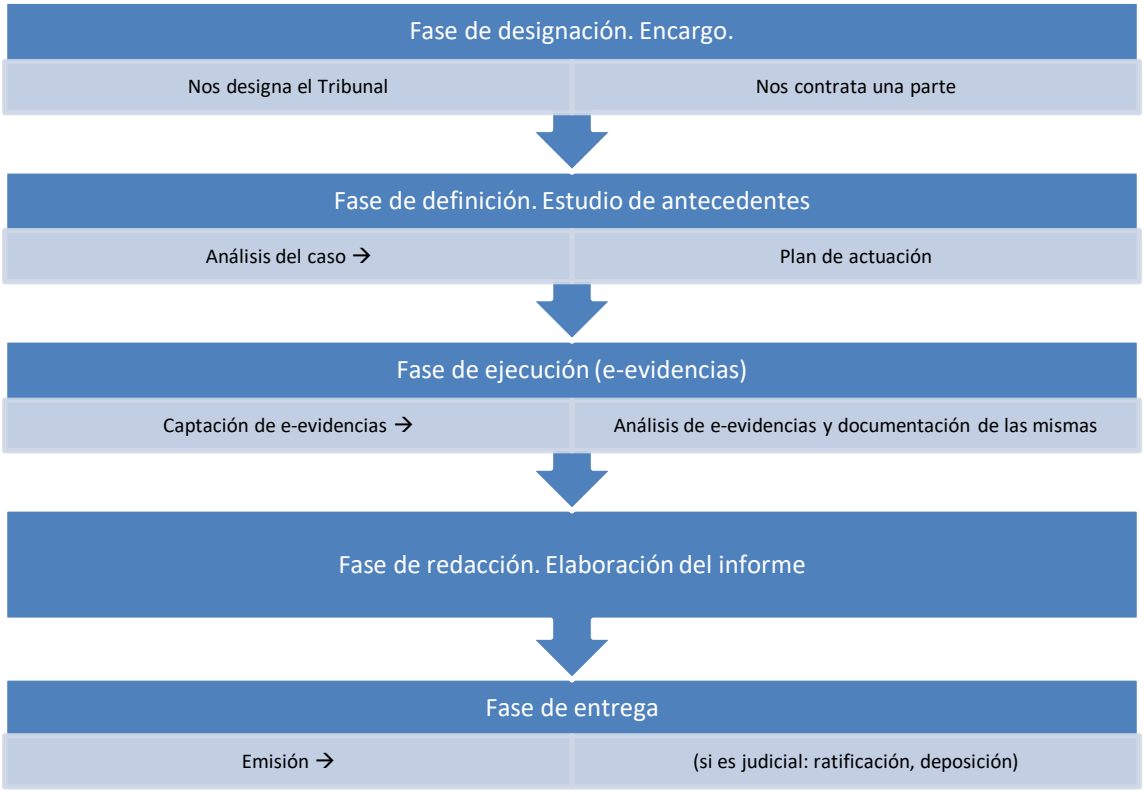
Trabajo de campo y cumplimiento

Si analizamos las fases de trabajo en la imagen siguiente:



Podemos ver que la fase central, la de ejecución, es el corazón de todo nuestro trabajo. Puede enturbiarse si no tenemos bien planteado el asunto (fases previas) o si nuestro informe termina siendo una birria (últimas fases), pero donde de verdad descansa todo es en cómo hemos captado las e-evidencias y… que hemos hecho con ellas. A esto de manera informal lo llamamos trabajo de campo.

Es crucial, porque no solo identificamos las evidencias con las posibles pruebas que se usarán, sino que de lo que hagamos con ellas (y cómo lo hagamos) dependerá la validez de la prueba. Esto es: no debemos contaminarlas, echarlas a perder… junto con las malas praxis en el mantenimiento de la cadena de custodia es lo que determina los fracasos en las actuaciones periciales.

Vamos en estas páginas a analizar todo este entorno.

e-evidencias

Sería esa información (ojo, información en el sentido de que será lo que se digiera en un tribunal, no implica que solo consideremos datos de los dispositivos, y no los dispositivos en sí mismo, las redes, las personas…) o indicios digitalizados que potencialmente pueden ser empleadas como medio de prueba.

¿Dónde están? ¡En muchos sitios y con distintos formas! Lo habitual es que la encontremos en un dispositivo, pero podemos hablar de infinidad de cosas: paquetes en la red, trazas de actividades…

Debemos, pues, distinguir entre fondo y forma: entre la información relevante para el estudio y su formato, el cómo está codificada y donde está alojada: el medio (dispositivo físico o virtual) que la contiene.

Esa información relevante, además, no siempre es una foto fija. A nuestros efectos, establecemos tres categorías de la misma:

- Estática: está almacenada, podemos consultarla, borrarla, modificarla… y hay peligro de que sea alterada por el uso normal de la misma.
- Dinámica: su alojamiento es temporal, está siendo procesada o en espera de ello, un simple apagón puede hacer que desaparezca o, por sus características, desaparecer al cabo de un tiempo breve.
- Encaminada: en movimiento por la red como paquete de información que puede ser capturado o almacenado.

Vemos que el peligro de perderla si no actuamos rápidamente se acelera conforme pasamos por las categorías. Efectivamente, cada una de esas categorías lleva implícitas técnicas y herramientas diferentes entre sí que permiten al perito capturarlas, conservarlas y garantizar la cadena de custodia. No vamos (no es nuestro propósito) a ahondar en estas técnicas, pero si es preciso de cara a nuestro punto de vista dejar claros unos puntos:

1. Siempre que sea posible hay que clonar la información sin afectar ni contaminar a la información original ni contaminarla.
2. Esta información clonada debe guardarse siempre con, al menos una copia, preservada de posibles escrituras (modo solo lectura). Este paso es fundamental para iniciar con éxito una cadena de custodia[1].
3. Cuando nos encontremos con informaciones no estáticas debemos almacenarlas en dispositivos seguros que eviten la volatilidad de las mismas y permitan preservar a las e-evidencias.
4. Todo análisis forense que se realice debe hacerse sobre las copias, nunca sobre los originales. Tengamos en cuenta que es posible que la mera observación puede cambiar el elemento estudiado.

Cadena de custodia

Volvemos a ella. Ya nos hemos acercado desde distintos prismas, pero ahora vamos a hacerlo pensando en ese trabajo de campo que nos ocupa. A estos efectos, conviene dejar una vez más claro de qué estamos hablando: sería un proceso de control sobre las e-evidencias

[1] Esto nos debe llevar a dejar claro, desde este momento, si disponemos de las herramientas necesarias para la extracción de las e-evidencias, su almacenamiento, su traslado, cómo vamos a organizarla y clasificarla y, por último pero no menos importante ¿de qué volumen de información hablamos?

durante todo el ciclo de vida de las mismas, desde su identificación inicial hasta su valoración por los Tribunales, manteniendo las premisas de no alteración y no contaminación que imposibilite de forma intencional o accidental cualquier tipo de alteración, sustitución, degradación o destrucción.

Como ya sabemos, hay distintas categorías de e-evidencias, lo que a su vez nos provocará distintas características y condicionantes al preparar la cadena de custodia de las mismas, pero con el marco común de un registro riguroso, claro y sin ambigüedad alguna que incluya a todo elemento susceptible de contener e-evidencias, bien haya sido incautado en una actuación, bien haya sido estudiado en el transcurso del proceso, que incluya quien ha tenido acceso en cada momento y quien ha hecho que sobre cada uno de ellos. No se escapará al lector la ventaja que tenemos frente a médicos o químicos, sin ir más lejos: dado que trabajamos con copias clónicas, podemos hacerles todas las perrerías que consideremos oportunas, siempre podemos volver al estado de partida.

Vamos a hablar con un poco de detalle de la cadena de custodia en los pasos más delicados.

Identificación

En este primer momento es cuando identificamos (localizamos o consideramos) algo como una e-evidencia. Es el momento de empezar a registrar identificando, de acuerdo a las características comentadas, esos elementos indicando la relación con nuestro caso y, sobre todo, quien es el responsable desde ese momento de su integridad.

Debemos añadir por cada elemento toda información Identificativa, descriptiva y significativa oportuna, si es preciso con fotos, esquemas, etc. Ese registro debe ser entregado en copia al fedatario público (p.e. el secretario del Tribunal) para que lo registre.

Incautación

Aquí debemos bifurcar los caminos. No será lo mismo lo que hagamos si estamos actuando por designación de un juez o por un encargo privado. Si actuamos a través de una orden judicial y precisamos llevarnos unos equipos, nos acompañará un Secretario Judicial con una orden para la ejecución de la actuación. Si es una de las partes la que nos hace un encargo privado, ellos nos facilitarán dispositivos e información sobre la que actuar. En este caso además del encargo (contrato) quien dará fe si es preciso será un notario.

Una vez tenemos claro que disponemos de esa orden judicial o ese encargo, estaremos autorizados. Es el momento de fijar, con esa orden o encargo, su alcance, al que nos debemos ceñir y, si tenemos dudas del mismo, consultarlas y si es menester solicitar autorización antes de actuar.

Tal y como apuntábamos, debemos ser impolutos en el escenario y evitar contaminarlo, pues podemos llegar a crear indicios falsos. Esa exquisitez en nuestro comportamiento debemos registrarla, si es preciso, con fotos, vídeos y esquemas del escenario, siendo prolijos sobre todo en aquello que parezca no habitual en escenarios similares. Debemos registrar donde está todo, como es, p.e., la topología de la red, que medidas de seguridad tiene la estancia, etc[2]. Al recoger e-evidencias hay que registrarlas, identificándolas quizá hasta con etiquetas numeradas (es más claro). Todo lo que nos vayamos a llevar (dispositivos, documentación impresa, etc.) debe ser "captado (fotos, vídeos…) con todo lujo de detalle: etiquetas identificativas, números de serie, etc. Una vez hecho el registro, se genera un inventario con todo[3].

Pero el registro no solo cubre objetos, también personas: presentes y los que en ese momento no están, con sus roles, niveles de seguridad, etc.

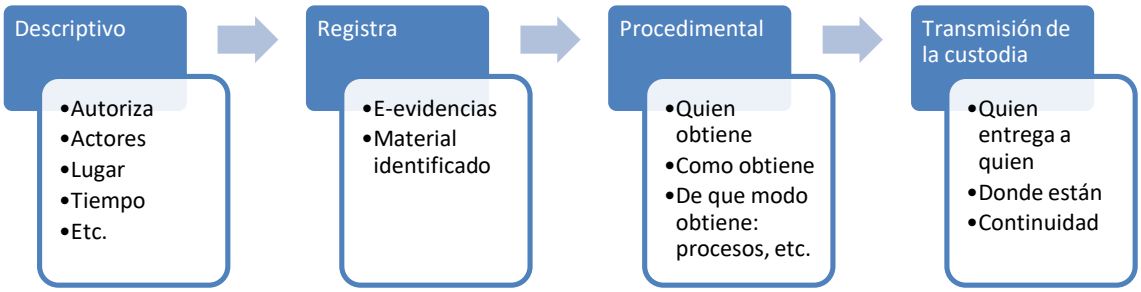
Tengamos en cuenta que si el dispositivo está apagado, no se debe arrancar… y viceversa. Recordemos lo preciso de esa copia clónica que permita certificar (hash) la información. El no apagar un dispositivo obedece a poder salvaguardar los elementos dinámicos (RAM, registro de conexión etc.) Si el dispositivo se encuentra conectado a una red hay que valorar pros y contras: lo que podemos perder versus la posibilidad de acceso por terceros en ese mismo momento. En todo caso, recordemos, toda e-evidencia debe ser identificada y registrada. Una vez tenemos todo lo preciso de esos dispositivos incautados, deben ser precintados, documentados y, con el registro anterior, entregados al notario o secretario judicial, según el caso, para su custodia y traslado. El fedatario le entregará un recibo de entrega en custodia que nos permitirá cubrir esa parte de la cadena de custodia.

Estos notarios y secretarios judiciales, son la piedra angular para la creación y mantenimiento de la cadena de custodia, son fedatarios: dan fe. En este caso dan fe de lo que pasa la actuación y de que lo que se refleja en las documentaciones periciales de identificación y de registro es fidedigno.

En la siguiente imagen podemos ver sus funciones:

[2]Te propongo un ejercicio: realiza un croquis de éste laboratorio, todo lo prolijo que puedas. Supuesto inicial: desde uno de los ordenadores se está suplantando a un profesor para poner notas a un grupo de alumnos.

[3] Para abundar más en esto: consulta la RFC 3227 o la UNE ISO/IEC 27037



En cuanto a lo descriptivo, hablamos del entorno, contexto, ubicación, etc. donde se realiza la actuación pericial y las condiciones del mismo, incluyendo quienes intervienen de forma directa o indirecta. En un segundo momento, todo eso se registra: todo lo que va a ser incautado ha de estar identificado y si es posible precintado. El Fedatario Público da fe del contenido la lista de registro, con sus identificadores, de forma que quede claro que responden a la realidad. El siguiente paso es el procedimental: dependiendo de quién y cómo lo haga podemos contaminar las pruebas e incluso destruirlas. No podemos tampoco dejar de lado aquellos casos donde pueden verse comprometidos derechos de las personas, en particular la privacidad. Buscamos en esta parte dejar claro que las actuaciones no podrán anular las e-evidencias[4]. "Tan solo" queda la transmisión de la custodia: el perito una vez ha recabado una e-evidencia, la entrega para su custodia, análisis y para la continuidad del proceso. El fedatario debe dar fe del proceso de transmisión, lo que implica un cambio de la titularidad de la responsabilidad de custodia.

[4] Aquí el fedatario puede dar fe de cómo se han desembalado pendrives, que herramientas sw se han empleado, etc.