



Tras extraer, catalogar y correlar, sin duda no nos queda otra que haber custodiado las pruebas con las que pretendemos denunciar las actividades sospechosas detectadas. En realidad la custodia de las pruebas comienza en el mismo momento en el que pretendemos analizar el entorno del ataque, ya que deberemos salvaguardar una copia íntegra sin manipular para poder presentar ante las autoridades. La CdC - Cadena de Custodia es un procedimiento riguroso de actuación con el que pretendemos salvaguardar las pruebas para determinar ante las autoridades y tribunales cómo, cuándo, quién, dónde y porqué.

Este procedimiento de control debe ser absolutamente riguroso, tanto con la prueba, como los hechos que la afectan, así como con el personal que tiene acceso a la misma, de tal forma que cuando ésta - o cualquier informe que se genere sobre ella -, llegue a manos del juez, no pueda dudarse ni por un instante de su validez, tanto de la prueba, como del informe, en su defecto, o como acompañamiento de la misma.

En muchos textos se define la cadena de custodia como *“el procedimiento de control que se aplica al indicio material relacionado con el delito, desde su localización, hasta que es valorado por los órganos de la administración de Justicia.”* Esta primera parte de la definición es válida como concepto genérico pero, en informática, hay que precisar que un conjunto de datos obtenidos en el primer análisis - el de campo, en el lugar de los hechos -, se destruye necesariamente al apagar los equipos. Nos referimos a las memorias volátiles o memoria RAM.

La cadena de custodia no se aplica sólo *“al indicio material relacionado con el delito”*, sino que, habría que ampliar esta definición, de tal forma que cubriese y amparase igualmente aquellos datos obtenidos de dispositivos con información volátil que hayan sido obtenidos sobre el terreno. Una muestra fotográfica del proceso de captación de datos y de las diferentes pantallas del router, así como de los datos característicos como número de serie, modelo, forma física del mismo servirán para relacionar el continente con el contenido.

Hay que ser conscientes de que en otros campos de actuación de la cadena de custodia, el principio de preservación de la prueba es sumamente importante, pero habría que establecer una serie de matices en la prueba digital. En el caso de la informática forense, hay una parte de la prueba que - si bien ha de ser custodiada en todo momento-, puede ser duplicada tantas veces como sea preciso (es el caso del contenido de un disco duro, o un lápiz usb, o tarjeta de memoria, etc.), pero para que este duplicado tenga validez jurídica ha de aplicarse esta cadena de custodia al elemento resultante, como si del original se

tratase. Sin embargo existe otra parte de la prueba que desaparecerá una vez desconectado el dispositivo, por lo que el documento generado tras el trabajo realizado “in situ”, antes de la desconexión, será la única prueba fehaciente de los datos que existían previamente. Es por esto que el documento resultante tendrá que ser sometido a cadena de custodia, para garantizar así que los datos obtenidos en ese instante no han tenido una posterior adulteración.

Por tanto podríamos definir que la cadena de custodia es “el procedimiento de actuación relativo a la seguridad y manipulación que ha de seguirse durante el período de vida de una prueba, desde que ésta se consigue o genera, hasta que se destruye o deja de ser necesaria”.