¿Qué son las pruebas digitales? La evidencia digital es cualquier información de valor probatorio que se almacena o transmite en forma digital (datos en binario a bajo nivel). Los dispositivos digitales registran evidencias de todo lo que haces. Los dispositivos digitales incluyen: portátiles, ordenadores de escritorio, teléfonos inteligentes, consolas, televisores inteligentes, cajeros automáticos, etc. Muchas veces, el análisis forense digital se confunde con la recuperación de datos, pero debemos distinguir ambos términos. Informática forense se centra en recuperar evidencias que el usuario ha ocultado, eliminado o simplemente dejado atrás mientras realizaba sus actividades.

Las pruebas pueden ser inculpatorias o exculpatorias.

Por el contrario, la recuperación de datos está enfocada en recuperar información que se liberó

Por error o se perdió durante la sobrecarga de energía. Por lo general, sabes lo que estás buscando porque, de lo contrario, este proceso puede ser realmente costoso tanto en tiempo como en recursos y podría llevar a un callejón sin salida. Ahora dos definiciones principales. Forense se refiere a la aplicación de la ciencia para resolver un problema legal. Y forense digital corresponde a "la aplicación de la informática y los procedimientos de investigación para un propósito legal que implica el análisis de las evidencias digitales, la cadena de custodia, la validación con matemáticas, el uso de herramientas validadas, la repetitividad y la presentación de informes y la posible presentación por parte de los expertos", tal como definió Zatyko en 2007. En cuanto a su aplicabilidad. La informática forense se puede aplicar en investigaciones penales. Por ejemplo: pornografía infantil, robo de identidad y homicidios. Pero también se puede aplicar en litigios

civiles, e inteligencia. Un principio importante es el Principio de intercambio de Locard: Dice que cuando las personas entran o salen de la escena del crimen dejarán o se llevarán algo, por ejemplo, ADN, huellas dactilares, cabello o fibras. Esto también es cierto para las evidencias digitales, como pueden ser archivos de registro y artefactos del sistema. Se deben considerar algunos consejos finales. La ciencia forense es nueva y algunos procedimientos aún están en desarrollo, por lo que el analista forense necesita estar actualizado. Como analista forense necesitamos ser objetivos, neutrales y seguir las evidencias donde sea que conduzcan. Como experto, debemos estar cualificados para emitir una opinión y debemos ser un comunicador efectivo.

Principales conceptos de ciencia forense: Bits y bytes son conceptos esenciales a considerar. En el nivel más bajo del ordenador, la información se almacena en bits y bytes. Un bit almacena un valor de 0 o 1. 1 byte es un grupo de 8 bits. Los conceptos de encabezado y pie de fichero también son notables en este contexto. El encabezado y pie de página del fichero describen el tipo de fichero. A menudo se denominan firma del archivo. Estos corresponden a los primeros y últimos bytes del fichero respectivamente, los primeros bytes se refieren al encabezado y los últimos al pie del fichero. Ahora hablemos sobre la recuperación de los datos. La recuperación de datos es el proceso de extraer una colección de datos de un conjunto de datos más grande. Las técnicas de recuperación de datos se utilizan con frecuencia durante una investigación digital cuando se analiza el espacio del sistema de archivos no asignado para extraer ficheros. Garfinkel y Metz propusieron una taxonomía para la recuperación de ficheros. En primer lugar explicaremos las técnicas principales. Encabezado y pie de fichero: es un método para buscar

fichero a partir de datos y procesar utilizando encabezados y un pie de fichero de distintos tipos de fichero. Encabezado y tamaño máximo del archivo: es un método para buscar ficheros a partir de datos sin procesar utilizando distintos encabezados y tamaño máximo del tipo de archivo. Encabezado y tamaño embebido del fichero:

Es un método para buscar ficheros a partir de datos sin procesar utilizando encabezados distintos y la longitud del fichero que está incrustada en el propio fichero. Otros métodos utilizados son los siguientes: propiedades estadísticas de la entrada (por ejemplo, entropía, que es la aleatoriedad de la entrada); semántica de los datos, que se basa en el análisis lingüístico del contenido del archivo (por ejemplo, si algunas frases en español se identifican en un documento HTML escrito en inglés, el buscador semántico podría concluir que las frase en español son parte de un fichero asignado previamente); otro método es la información de la estructura del sistema de ficheros (su uso requiere conocimientos de Sistemas Operativos a bajo nivel). Existen más métodos, aunque hemos mencionado los más relevantes. Un punto interesante es identificar si las técnicas de recuperación de datos son igualmente efectivas en un disco magnético, llamado HDD, que en un disco de estado sólido, llamado SSD. La efectividad se basa el funcionamiento de los discos HDD y SSD. En el caso de usar SSD, las posiciones en la memoria no se pueden sobrescribir si no se han eliminado previamente. Primero se borran los datos que fueron marcados para su liberación y posteriormente se escriben las zonas de memoria que hayan sido previamente borradas. Para el borrado de los datos se utiliza el comando TRIM. Por el contrario, HDD aplica una técnica muy diferente para escribir o acceder a los datos. Cuando se accede a los datos hay que volver las partes mecánicas del disco, lo que consume

tiempo. Con respecto a la eliminación de los archivos, cuando se elimina algo, en lugar de borrarlo de forma permanente, los datos únicamente son desvinculados. El concepto de TRIM es esencial para la recuperación de datos porque cuando se aplica, los datos ya no se pueden recuperar. Esto sólo aplica a los discos SSD.

Un informe técnico forense se compone de las siguientes 7, secciones: resumen ejecutivo, antecedentes y objetivos, evidencias analizadas, hallazgos relevantes y detalles del proceso, pistas abiertas, conclusiones y anexos. El resumen ejecutivo consiste en uno o dos párrafos que resumen su informe. Debe contener una breve descripción del caso, información de los antecedentes y los principales hallazgos y conclusiones. En cuanto a los antecedentes y objetivos, esta sección contiene toda la información relevante respecto al contexto, incluyendo una descripción de por qué un examen forense de este ordenador, dispositivo o datos era necesario y qué hipótesis inicial (si alguna) se consideró. También incluye un resumen de todas las tareas realizadas en la investigación. La sección de evidencias analizadas presenta todas las evidencias recopiladas y analizadas durante su investigación. El uso de una tabla suele ser apropiado. Los hallazgos relevantes y los detalles del proceso presentan los principales hallazgos de la investigación. Cada hallazgo relevante debe venir acompañado con un análisis en profundidad. La sección de pistas abiertas se corresponde a tareas incompletas. Incluye evidencias que no pudieron ser analizadas, por ejemplo, no conoce la contraseña de un archivo importante, y no se puede analizar su contenido. En la última sección, conclusiones, se resume los principales hallazgos técnicos de la investigación. También se puede expresar su opinión como experto forense. Finalmente, un

consejo: ¡no olvide que todas las afirmaciones deben estar respaldadas por las evidencias!