www.eysglobal.com

MÓDULO 1

TEMA 9: PRESERVACIÒN DE EVIDENCIAS PARTE 2

PRESERVACIÒN DE EVIDENCIAS : RECOLECCIÓN Y EXAMINACIÓN DE INFORMACIÓN

Una vez se han identificado las posibles fuentes de información, se debe proceder a realizar la recolección y examinación de los datos disponibles.

La secuencia para llevar a cabo la recolección y examinación de medios/información es la siguiente:

- **CREACIÓN DEL ARCHIVO / BITÁCORA DE HALLAZGOS (CADENA DE CUSTODIA),** hablemos un poco sobre este item

PRESERVACIÒN DE EVIDENCIAS

IMAGEN DE DATOS

Consiste en la generación de las imágenes de datos que conciernen al caso en investigación. Se recomienda utilizar herramientas de extracción de imágenes como Linux dd o Encase Forensic Software.

VERIFICACIÓN DE INTEGRIDAD DE LA IMAGEN

Para cada imagen suministrada se debe calcular su compendio criptográfico (SHA1/MD5), comparándolo luego con el de la fuente original. Si la comparación arroja un resultado negativo se debe rechazar la imagen proveída en el primer paso.

PRESERVACIÒN DE EVIDENCIAS

CREACIÓN DE UNA COPIA DE LA IMAGEN SUMINISTRADA

En un análisis de datos nunca se debe trabajar sobre la imagen original suministrada. Debe realizarse una copia master y a partir de esta, se reproducen las imágenes que se requieran.

ASEGURAMIENTO DE LA IMAGEN ORIGINAL SUMINISTRADA

Se debe garantizar que la imagen suministrada no sufra ningún tipo de alteración, con el fin de conservación de la cadena de custodia y del mantenimiento de la validez jurídica de la evidencia.

PRESERVACIÒN DE EVIDENCIAS

REVISIÓN ANTIVIRUS Y VERIFICACIÓN DE LA INTEGRIDAD DE LA COPIA DE LA IMAGEN

Una vez se ha obtenido la copia de la imagen, es necesario asegurar que no tenga ningún tipo de virus conocido.

Luego se debe verificar la integridad de la copia, de la misma forma como se hizo con la original (paso **9.3**). De hecho, esta actividad es de tipo transversal en la metodología, es decir, debe realizarse periódicamente durante el proceso de análisis de datos, de modo tal que se garantice la integridad de los datos desde el comienzo, hasta el fin de la investigación.

EVIDENCIA DIGITAL

Usualmente se asociaba la evidencia digital con delitos electrónicos como falsificación de documentos electrónicos, cajeros automáticos y tarjetas de crédito, robo de identidad, fraudes electrónicos y pornografía infantil. Sin embargo, en la actualidad se utiliza para procesar todo tipo de delitos, pudiendo señalar como los más destacados:

MANEJO DE EVIDENCIAS

El cuidado de la evidencia digital es uno de los pasos más importantes para la obtención del resultado sin alteraciones. Para la correcta manipulación de la misma, es necesario tener en cuenta cinco aspectos:

- Unicidad de formato: hace referencia a aquellos documentos electrónicos que solo pueden preservarse en su estado digital, estos son archivos multimedia, base de datos relacionales, documentos simples con metadatos, entre otros que no pueden plasmarse en papel u otro formato diferente al original.

MANEJO DE EVIDENCIAS

•Alterabilidad: son todos aquellos archivos digitales que poseen metadatos asociados, por lo tanto no pueden manipularse por ser susceptible de tener información relevante como puede ser: la fecha de creación, modificación, acceso u otros datos que exceden al contenido del fichero mismo.

•Interpretación: es la forma de entender los datos que me brindan programas específicos que pueden tener configuraciones complejas, llaves de seguridad o tratamientos en materias concretas. Estamos hablando de casos en los que necesiten de asistencia calificada como por ejemplo: en el caso de peritar software contable, donde el perito requerirá que sea asistido por un contador o experto en el tema, entre otros casos.

MANEJO DE EVIDENCIAS

•Medio activo: el programa que usemos para recolectar la evidencia pueda alterarla, por lo tanto nunca hay que realizar la copia con herramientas del mismo sistema operativo. Esto es debido a que pueden llegar a modificar los metadatos y así alteran la integridad de documentos, siendo recomendado el empleo de software específico para hacer una copia fiel.

•Medio de destino: es el hardware donde se almacenara la información a peritar, aquí hay que considerar varios elementos como pueden ser: la universalidad, es decir la disponibilidad del medio de prueba en el momento de la pericia; la obsolescencia, es la accesibilidad al medio empleado y; la confiabilidad, que esta asociado a lo seguridad del medio para preservar la prueba.

PERITO INFORMATICO

CLASIFICACIONES DE EVIDENCIA DIGITAL

Para hacer un buen planeo de los puntos de pericia es importante tener en claro que queremos probar, donde esta la evidencia y si se puede hacer con los medios disponibles. Es por este motivo que es indispensable planificar antes de actuar, realizar una recolección efectiva sin contaminación, no manipular la evidencia y contar con asesoramiento previo para lograr un mejor escenario. Por este motivo debemos clasificar la evidencia en estática o dinámica.

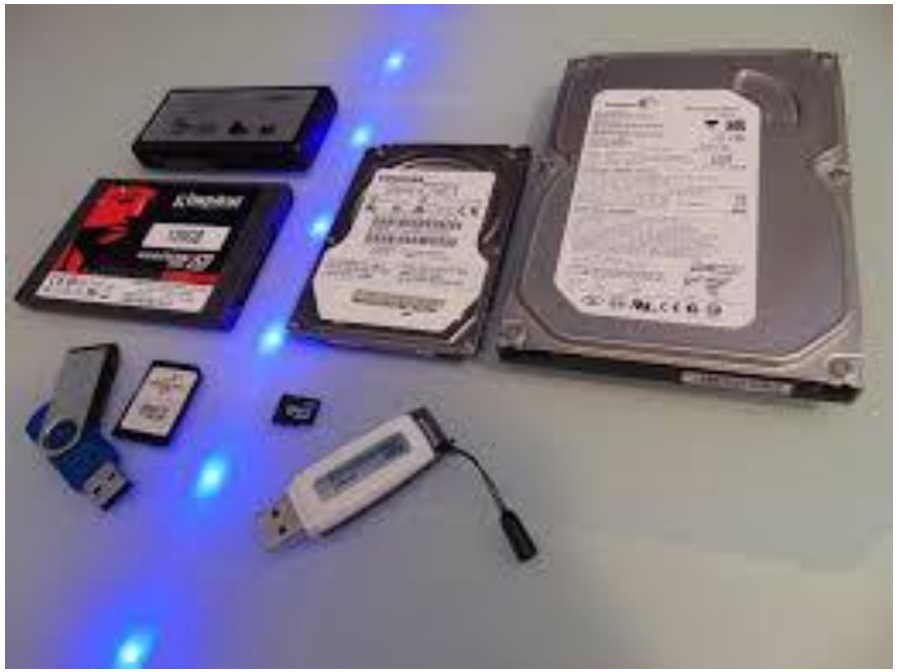
ELEMENTOS DEL PROCEDIMIENTO FRENTE A UN SISTEMA

El primer contacto con el sistema debe ser analizado y siguiendo los pasos necesarios para evitar la perdida de posibles pruebas. Al acceder al recinto donde se encuentran los equipos se debe principalmente asegurar el lugar, pudiendo acceder sin intervención de terceros o personas ajenas al peritaje que con su accionar tengan la posibilidad de alterar la escena. Para intervenir correctamente, se deberá hacer con los guantes adecuados para preservar las huellas, dado que las que estén en la superficie del hardware de los sistemas investigados permutaran saber quienes fueron usuarios de aquel.

CRITERIOS DE PRIORIZACIÒN DE EQUIPOS

Frente a los grandes volúmenes de información y el poco tiempo para determinar o buscar contenido relevante en un equipo aparece el "triage". Este término es utilizado en la medicina para priorizar la atención de pacientes en función de su estado de gravedad. Llevado al ámbito de la informática forense, dicha técnica se aplica para la selección de aquella evidencia digital que debe ser priorizada para llevar a cabo un posterior análisis forense exhaustivo, en función de diversos indicadores o características que pueden ser determinadas de forma inmediata.

OBSERVACIONES EN MEMORIAS DE ALMACENAMIENTO



Al actuar sobre la información el especialista no realiza un backup de los datos, dado que debe trascender más allá de las herramientas que le presenta el sistema operativo. Es así que, ejecuta una "copia forense", la cual emplea una técnica de copiado bit a bit permitiendo la recuperación de archivos borrados por la plataforma operativa del dispositivo. Esto se debe a que, en realidad, solo fueron desindexados los datos, pero pueden encontrarse ocultos en el dispositivo.

ANALISIS DEL TRÁFICO DE DATOS EN REDES

El análisis forense de redes se basa en la certeza de que no existe el anonimato ni en la navegación ni en el uso de Internet. Aunque se utilicen programas que ofrecen navegación anónima como TOR, Proxy y otros; estos servicios también pueden resultar comprometidos o pueden contener fallas.

Los peritos especializados se basan en utilizar los conocimientos acerca del funcionamiento del protocolo TCP/IP y de los instrumentos que emplean los crackers para atacar un sistema informático. Esta especialidad se vale de técnicas y programas que buscan los logs y los archivos de actividad de los distintos protocolos de red.

INVESTIGACIÓN DEL CORREO ELECTRÓNICO

El análisis forense de correos electrónicos es aquel que requiere actividad sobre el equipo y en la red, dado que podemos encontrar datos distribuidos que nos sirvan para darle consistencia a los mails encontrados, permitiendo que sean evidencia valida. Para poder emplearlos como prueba es necesario analizar el completamente un correo, viendo que consta de dos partes la investigación:

REDES SOCIALES

La creación de perfiles falsos es normal, encontrado fácilmente en los residuos de navegación de los dispositivos