www.eysglobal.com

MÓDULO 1

TEMA 15:

APLICACIÒN DE TÈCNICAS DE ANÀLISIS SOBRE LOS DATOS ADQUIRIDOS

APLICACIÒN DE TÈCNICAS DE ANÀLISIS SOBRE LOS DATOS ADQUIRIDOS

Teniendo en cuenta que la informática forense es una disciplina compleja en su manejo, se deben extremar las medidas de seguridad al personal especializado en el manejo de estas evidencias con el fin de evitar que se cometa cualquier error que implique fallas en un proceso legal. Algunas de Las técnicas, que deben considerarse al momento de adelantar un análisis sobre los datos adquiridos son:

APLICACIÒN DE TÈCNICAS DE ANÀLISIS SOBRE LOS DATOS ADQUIRIDOS

Esterilidad de los medios informáticos de trabajo: Cada elemento utilizado por los investigadores debe estar certificado para garantizar que no se haya vulnerado su integridad, debido que si este elemento fue expuesto a vibraciones magnéticas u otro tipo de exposición, la evidencia recolectada en este medio quedaría contaminada y no sería confiable en ningún procedimiento forense. Este se relaciona con la medicina forense en donde una mala interpretación o análisis de las pruebas recogidas puede determinar una falsa hipótesis sobre la muerte de un paciente.

APLICACIÒN DE TÈCNICAS DE ANÀLISIS SOBRE LOS DATOS ADQUIRIDOS

Verificación de las copias en medios informáticos: Al momento de extraer las copias de información de los medios tecnológicos, estas deben ser exactas a la original y deben estar asistidas por un método y un procedimiento utilizando algoritmos y técnicas basadas en firmas digitales que comprueben su veracidad. De esta misma manera, el software utilizado debe estar probado por la comunidad científica para que la tasa de efectividad de la misma sea validado antes de presentarse ante una instancia legal.

APLICACIÒN DE TÈCNICAS DE ANÀLISIS SOBRE LOS DATOS ADQUIRIDOS

Documentación de los procedimientos, herramientas y resultados de los medios informáticos utilizados:.La custodia de todas las evidencias y los procedimientos ejecutados durante el análisis de las evidencias recolectadas, están a cargo del investigador y deben estar debidamente documentados, con el fin de que una persona externa pueda validar la información obtenida de dicho análisis. De esta manera se puede tener un parte de confianza y tranquilidad al investigador evitando que un tercero utilice la misma evidencia.

APLICACIÒN DE TÈCNICAS DE ANÀLISIS SOBRE LOS DATOS ADQUIRIDOS

Mantenimiento de la cadena de custodia de las evidencias digitales. Este punto es complemento del anterior teniendo en cuenta quien entrego la información, cuando, en qué estado, como, entre otras preguntas para poder rendir cuentas de la correcta administración de las pruebas a cargo del investigador

APLICACIÒN DE TÈCNICAS DE ANÀLISIS SOBRE LOS DATOS ADQUIRIDOS

Informe y presentación de resultados de los análisis de los medios informáticos. Una adecuada presentación de los resultados es fundamental para la interpretación de las pruebas extraídas, si este requisito no se cumple, el investigador puede poner en entredicho su idoneidad y experticia en el manejo de la información. Es por esto que la claridad en la redacción y la ilustración pedagógica de los hechos y los resultados, son elementos críticos a la hora de defender un informe de las investigaciones, entre los cuales encontramos los técnicos con los detalles de la inspección realizada y el ejecutivo para la gerencia y sus dependencias

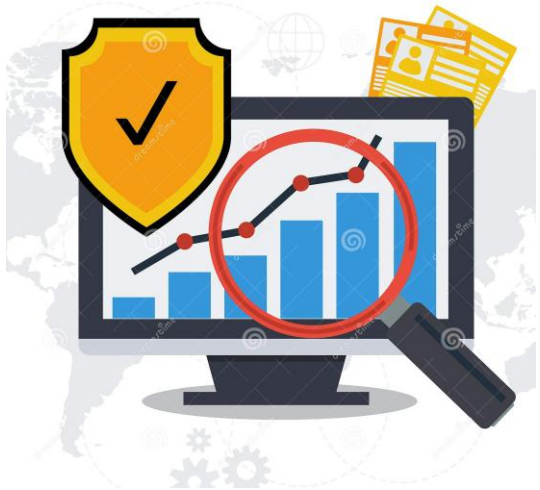
APLICACIÒN DE TÈCNICAS DE ANÀLISIS SOBRE LOS DATOS ADQUIRIDOS

Administración del caso realizado. Una vez sean recopiladas, analizadas y documentadas las pruebas, los investigadores forenses en informática deben prepararse para declarar ante un jurado o juicio, con el fin de servir en los procesos judiciales como declarante en ese mismo momento o en un tiempo determinado. Es por ello la importancia de mantener documentado y bajo extrema seguridad y control todos los expedientes que contienen información puntual sobre el caso en el cual el profesional ha participado

APLICACIÒN DE TÈCNICAS DE ANÀLISIS SOBRE LOS DATOS ADQUIRIDOS

Auditoría de los procedimientos realizados en la investigación. Por último es recomendable que el investigador autoevalúe los procedimientos realizados para contar con la evidencia de una buena práctica en su investigación, aplicando el ciclo de calidad: PHVA - Planear, Hacer, Verificar y Actuar, y de esta manera incrementar la confiabilidad de las técnicas aplicadas en la práctica de esta disciplina

APLICACIÒN DE TÈCNICAS DE ANÀLISIS SOBRE LOS DATOS ADQUIRIDOS



Una vez se tiene hecha la identificación, se hace una copia o imagen que sea igual al contenido de la evidencia, además se debe asignar un código único el cual corresponde a una serie de bytes que se convierten en el total del medio que se está analizando; dicho código debe ser suficientemente seguro y complejo como para evitar que pueda ser verificado por personal no autorizado, desde este punto se empieza a tener una cadena de custodia eficiente. A partir de este punto se pueden hacer copias de la imagen para que el personal que corresponda pueda acceder a la información.

APLICACIÒN DE TÈCNICAS DE ANÀLISIS SOBRE LOS DATOS ADQUIRIDOS

La etapa 1 de esta fase corresponde a hacer copias de la evidencia obtenida, esto se hace por medio de diversos métodos y se emplean funciones como MD5 o SHA1, esta firmas se deben incluir en la etiqueta de cada copia que se haga, debe incluir fecha y hora en que se ha creado la copia y se deben distinguir como copia 1 y copia 2 por ejemplo. Se debe tener especial cuidado con los discos duros por temas de temperatura y condiciones climáticas con el fin de preservarlos.

APLICACIÒN DE TÈCNICAS DE ANÀLISIS SOBRE LOS DATOS ADQUIRIDOS

La etapa 2 hace referencia a la cadena de custodia donde se establecen responsables y controles sobre la evidencia. El acceso a la evidencia debe ser muy restrictivo con el fin de evitar manipulaciones incorrectas.

APLICACIÒN DE TÈCNICAS DE ANÀLISIS SOBRE LOS DATOS ADQUIRIDOS

Debemos tener en cuenta : Gestión de datos de investigación, en un estudio realizado después de los datos obtenidos en una investigación por un ataque cibernético se logro concluir y es para tener en cuenta:

Es fundamental el uso de contraseñas seguras:

Al pensar en mecanismos que contribuyan a la seguridad de los datos, es muy importante utilizar contraseñas robustas, capaces de resistir ataques informáticos. Un software para descubrir contraseñas de forma automatizada es capaz de probar millones de combinaciones en minutos, por lo que no debe subestimarse la función que juega una buena contraseña en proteger nuestros datos.

APLICACIÒN DE TÈCNICAS DE ANÀLISIS SOBRE LOS DATOS ADQUIRIDOS

Algunas claves para crear contraseñas seguras:

Crear contraseñas largas. Algunos sistemas solicitan un mínimo de 7 u 8 caracteres. Para mayor seguridad, pueden utilizarse 15 caracteres o más, especialmente para proteger aquellos servicios que se consideran críticos

Utilizar mayúsculas, minúsculas, signos de puntuación y caracteres no alfabéticos

Utilizar contraseñas únicas para cada servicio. Por ejemplo, no utilizar una misma clave para proteger datos almacenados en un servidor institucional y en un servicio de almacenamiento en la nube.

APLICACIÒN DE TÈCNICAS DE ANÀLISIS SOBRE LOS DATOS ADQUIRIDOS

- **Evitar errores comunes**, tales como:
  - Utilizar palabras de diccionario, aún si están en otros idiomas
  - Utilizar datos personales, tales como números de identificación, teléfonos o direcciones
  - Utilizar referencias a la cultura popular, tales como nombres de libros, personajes, canciones, bandas musicales, etc.
- Puede utilizarse el **enfoque XKCD**, que consiste en utilizar cuatro palabras escogidas al azar. Para fortalecer la contraseña, sustituir algunas de las letras por signos y números, utilizando mayúsculas y minúsculas.
- Otro enfoque es **utilizar un gestor de contraseñas**, software que genera y maneja contraseñas únicas y encriptadas, ofreciendo mayores garantías de seguridad y evitando el problema de crear y recordar múltiples contraseñas

Y por supuesto, deben tomarse las precauciones que se recomiendan para la protección de cualquier contraseña, como **evitar ingresar a cuentas desde conexiones públicas o en espacios inseguros**.