www.eysglobal.com

MÓDULO 1
TEMA 10:METODOLOGÌA DE TRABAJO PARTE 1

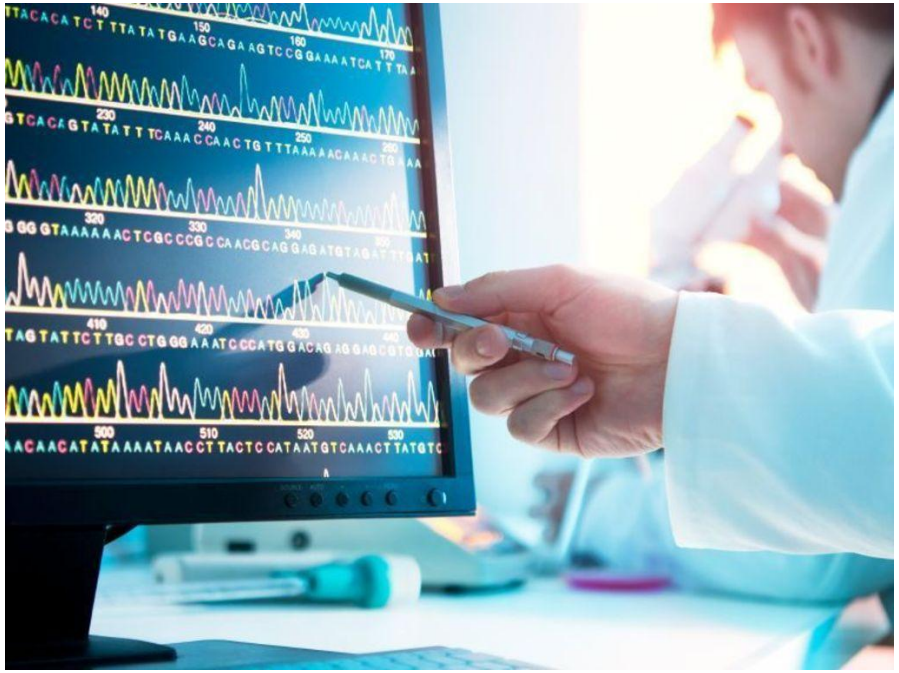
IDENTIFICACIÒN

Esta clase describe el método por el cual el investigador es notificado de un posible incidente. Se determinan ítems, componentes y datos posiblemente asociados con el incidente.

METODOLOGIA DE TRABAJO

METODOLOGIA DE TRABAJO : IDENTIFICACIÒN

aquí será primordial seleccionar la evidencia, en tiempo y forma, y ajustada al escenario de la investigación. Definiendo guías para priorizar la selección de la evidencia a analizar (modelos de triage) que faciliten una primera identificación de lo importante, y abandonando las prácticas de «copiar todo».



METODOLOGIA DE TRABAJO : ADQUISICIÓN

habrá casos en los que la evidencia ya no será absoluta (en términos de completitud) y no será posible, técnica o metodológicamente, realizar una tradicional imagen completa «bit a bit». En estas situaciones, habrá que utilizar los **procedimientos de priorización** o triage de la fase de identificación, para determinar qué parte de la evidencia será necesario copiar. Por lo que cobrará especial importancia justificar y documentar apropiadamente las razones y los métodos utilizados para copiar una u otra parte de la evidencia, de forma que se pueda garantizar su integridad y validez como fuente de prueba.

METODOLOGIA DE TRABAJO : PRESERVACIÓN/CUSTODIA

Preservar la evidencia de forma segura y cumpliendo con los requisitos legales, requerirá una inversión en **laboratorios forenses** apropiados al volumen de los casos a tratar. Además de contar con actores externos e independientes que garanticen la inalterabilidad de la prueba en el tiempo, como se hace actualmente con los depósitos notariales o incorporando nuevas formas como el uso de la firma electrónica o, en un futuro, los modelos basados en **blockchain**.

METODOLOGIA DE TRABAJO: ANÁLISIS

Incorporar nuevas técnicas de análisis basadas en el uso de aplicaciones de **Big Data**, la **Inteligencia Artificial** o el **Machine Learning**, requerirá contar con recursos humanos con dichas habilidades, así como con nuevas herramientas capaces de entender y evaluar los algoritmos que hay detrás de los datos.

METODOLOGIA DE TRABAJO: PRESENTACIÓN DE RESULTADOS

Los informes, además del contenido tradicional de alcance, objetivos, análisis y resultados, tendrán que incorporar una completa evaluación de las herramientas y métodos de análisis utilizados. Más aún cuando la volatilidad de los datos o la imposibilidad de hacer una copia completa de los mismos, impida garantizar la repetición de los procesos.

METODOLOGIA DE TRABAJO.
Mayores Desafíos en la Informática Forense Digital

Técnicos. Estar actualizado es el mayor problema. La tecnología digital evoluciona constantemente. Enormes cantidades de información, tiempos de mercados cada vez más pequeños, inseguridad en las herramientas y la falta de experiencia y entrenamiento destacan claramente el problema.

- Procedural: Los analistas forenses deben recolectar cualquier evidencia que los guíe o les provea soporte en su investigación. No obstante, los procedimientos analíticos y los protocolos no están estandarizados ni tampoco la terminología utilizada.
- Social: La incertidumbre acerca de la exactitud y eficacia de las técnicas actuales provocan que la información recolectada sea almacenada por períodos de tiempo extremadamente largos, utilizando recursos que podrían ser aprovechados en la solución de problemas reales más que en almacenamiento

METODOLOGIA DE TRABAJO

• Legal: Se puede crear la tecnología más avanzada posible, pero si no cumple con la ley, su utilidad es discutible.

Foco de Investigación: Es necesario incorporar aspectos forenses en herramientas en lugar de producir soluciones puntuales. Es necesario que la tecnología no sea tan fácilmente comprometida. Para comenzar a responder el problema del entrenamiento y la experiencia, es necesario mucho más esfuerzo en producir interfaces de usuario que trate las deficiencias en niveles de destreza que siempre estarán presentes y serán peores cuando los problemas crezcan.

METODOLOGIA DE TRABAJO:
Técnicas anti-forenses

Durante la actividad forense, es posible encontrarse con algunas situaciones en la que la aplicación de métodos tradicionales puede verse opacada. Estas técnicas son llamadas generalmente técnicas anti-forenses y se pueden clasificar en cuatro grandes categorías:

METODOLOGIA DE TRABAJO:
Técnicas anti-forenses

- ✓ Data hiding. El objetivo es ocultar la información de manera que sea difícil encontrarla y además, mantenerla accesible para usos futuros. Algunas técnicas son: encriptación, esteganografía, otros.
- ✓ Artifact wiping. El objetivo es eliminar definitivamente archivos o sistemas completos. Algunas técnicas son: herramientas software de limpieza de discos; herramientas software de limpieza de archivos (más rápidos); “disk degaussing” que consiste en dispositivos hardware capaces de aplicar un campo electromagnético sobre el dispositivo de almacenamiento digital eliminando la información contenida en él; destrucción física del dispositivo

METODOLOGIA DE TRABAJO:
Técnicas anti-forenses

- ✓ Trail obfuscation. El objetivo es alterar información con el objetivo de confundir y desorientar el proceso de análisis forense. Algunas técnicas son: limpiadores de logs, spoofing, falta de información, modificar metadata de archivos, cuentas falsas, etc..
- ✓ Attacks against computer forensics. El objetivo es inutilizar reconocidas técnicas de análisis forense.