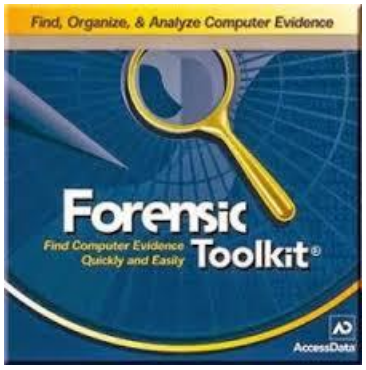
Herramientas de interfaz gráfica de usuario para la Informática Forense



Informática forense es un campo cada vez mayor en la aplicación de la ley y la industria privada. Analistas forenses responden a los delitos informáticos o mal uso de entregar un informe detallado de la actividad del usuario en un sistema. Hay muchas de línea de comandos y GUI herramientas (Graphical User Interface) que los examinadores profesionales forenses utilizan para recopilar información. Herramientas forenses más gráficas son multiplataforma, u operan en más de un sistema operativo. Alrededor de la mitad de las herramientas forenses GUI comunes utilizados en el año 2010 son de código abierto (libre) para uso no comercial.

EnCase Forensic Suite de EnCase es un conjunto de herramientas de análisis forense utilizados por los EE.UU. militares y varias agencias locales de aplicación de la ley para llevar a cabo investigaciones penales. El software, que se distribuye sólo a la policía y los usuarios del gobierno, incluye una interfaz gráfica de usuario completa, la fabricación de herramientas poderosas disponibles para para copiar, analizar y buscar archivos de destino en un sistema informático. EnCase sólo es útil para las investigaciones fuera de línea de los discos duros y medios extraíbles que no están en los sistemas de destino en vivo o memoria volátil.

Helix Forense LiveCD es una compilación de herramientas de código abierto comunes utilizados por los investigadores forenses independientes y comerciales. Hasta 2009, el Helix LiveCD estaba disponible para su descarga gratuita , ya está a la venta por la corporación eFence . El kit de herramientas incluye Helix copiadoras de disco , talladores de archivos , búsqueda de cadena y herramientas de examen de meta-datos para prácticamente cualquier formato de disco duro . Además , Helix también se puede instalar en una unidad USB y se utiliza para analizar los anfitriones vivos y la memoria volátil.

MacForensicsLab software y hardware incluido es un conjunto de herramientas forenses multiplataforma diseñado para ayudar a la policía en las investigaciones , proteger a los usuarios contra el robo de identidad, y ayudar a las empresas en las auditorías del uso apropiado de los documentos digitales . Tanto la versión de software de este paquete ofrecen capacidades GUI de hardware y , con las versiones de hardware que también proporciona la captura de datos volátiles y análisis de cualquier sistema que ejecute o dormir.

Autopsy la autopsia es un equipo forense de la suite de gestión basado en navegador, que mantiene un registro de toda la actividad de auditoría en un sistema. Autopsia combina varias herramientas de línea de comandos, como dd (copiadora de datos sin procesar) y la galleta (la actividad del navegador auditor) , para proporcionar un módulo de administración gráfica común para las investigaciones de plataforma cruzada . Muchos investigadores independientes usan Autopsia de investigaciones privadas, recuperación de datos, y los casos de abuso de la informática de negocios. La autopsia está disponible para los sistemas Linux, y es completamente de código abierto.

FUNDAMENTOS DE LA ESTEGANOGRAFIA

**** Esta actividad es de tipo INDIVIDUAL**

El **estego-algoritmo** es el algoritmo esteganográfico que indica cómo realizar el procedimiento de incorporación del **mensaje esteganográfico** en el portador para obtener el **estego-mensaje**. Según el tipo de estego-algoritmo podemos distinguir entre dos tipos de esteganografía:[5] Esteganografía pura y esteganografía de clave secreta.

OBJETIVOS

· Analizar ficheros sospechosos mediante la técnica de Esteganografía.

PRACTICA:

1. Lea el documento esteganografia.pdf -→ Realizar mapa conceptual CMAP TOOLS, donde se plasmen los aspectos más importantes y terminología relacionada con los temas vistos en este 2° corte, debe tener su nombre en la parte inferior del documento, guardar como MC-nombrecompleto.PDF:
   - **Herramientas de interfaz gráfica de usuario para la informática forense**
   - **Análisis forense entornos Windows (presentación y explicación en clase /** marzo 16**)**
   - **Fundamentos de la Esteganografía**

2. Descargar los programas y tutoriales que se utilizaran para el encriptamiento de archivos en ficheros de imágenes desde la dirección:
   https://www.dropbox.com/s/omwjrqzg9eipbyr/programas_tutoriales.zip?dl=0
   https://www.dropbox.com/s/4mh6xxv9anfalw6/programas_tutoriales.zip?m=

3. Instalar software para reconocimiento, realice los tutoriales de los programas AdaStegano tanto para el modo consola y gráfico y el de Xiao_Stenography.. (pantallazos y explicación de los procesos realizados). guardar como Practica-nombrecompleto.PDF

4. Utilizando el programa AdaStegano mediante el modo consola encripte los siguientes documentos: imagen del logo CUN y su **ESTADO DE NOTAS** en un archivo PDF .
   - El documento PDF es válido únicamente si aparece su documento de identificación y nombre.
   - Única clave válida de encriptación: **IFCUN,** método de encriptación **cesar.**
   - Nombrar el archivo alterado con su nombre + A1, ejemplo: **FernandoJimA1.bmp**

5. Cree un documento en Word que contenga una imagen escaneada de un documento personal (licencia de conducción, cedula, carne estudiantil), guardelos como DI Luego encripte el documento en una imagen diferente a la anterior.coloque como contraseña **CUN2** y cifre en modo serpent. Nombrar el archivo alterado con su nombre + A2, ejemplo: **FernandoJimA2.jpg**

6. Utilizando el programa Xiao_Stenography encripte los siguientes documentos:
   - Elige la imagen o fichero de sonido donde ocultarás la información, selecciona los ficheros que quieres ocultar y ajusta después las opciones de configuración necesarias: algoritmo de encriptación, contraseña, etc. Descargue una imagen .bmp, allí encripte el documento creado en el numeral 4 (PDF). sin clave de encriptación. Nombrar el archivo alterado con su nombre + A3, ejemplo: **FernandoJimA3.bmp**

PRODUCTO A ENTREGAR = (3) 45%

Contenido

CARPETA COMPRIMIDA .RAR…con nombre NOMBRE COMPLETO- PRACTICA2, esta debe contener:

1. Documento en PDF donde este el mapa conceptual insertado como imagen
2. Documento en PDF Práctica realizada que contenga pantallazos y explicación de las mismas, sobre el proceso de instalación y manipulación de archivos = técnica de Esteganografía de los puntos 4, 5 y 6 de la práctica realizada en su equipo, debe aparecer su nombre en las imágenes adjuntas.
3. Carpeta con las imágenes estenográficas creadas según nombres e indicaciones dadas

INDICACIONES PARA LA PRESENTACIÓN

- Los archivos deben tener exactamente los formatos y nombres especificados.
- Formato de entrega FINAL : Carpeta comprimida .RAR o .ZIP
- **Envio: Hasta Domingo 29 de Marzo**