fidélitas
Virtual

Computación Forense

Técnicas Antiforenses

Clase 2b

Profesor: Ing. Alex Araya Rojas, MT

CISSP, CISM

Técnicas Anti Forenses

- **Qué son las Técnicas Anti Forenses?**

  - Son actividades que se ejecutan para prevenir que los procesos forenses tengan éxito.
  - Su objetivo es reducir la cantidad y calidad de la evidencia y esconder los elementos que permitan la trazabilidad de un hecho.
  - Son también utilizadas para comprometer la confidencialidad de un reporte forense.

Técnicas Anti Forenses

- **Algunos ejemplos de Técnicas Anti Forenses?**

  - Borrado de datos: archivos, directorios, etc.
  - Protección por contraseña
  - Esteganografía
  - Esconder archivos en estructuras de archivos del sistema
  - Borrado de artefactos maliciosos
  - Sobreescritura de datos y metadatos

Técnicas Anti Forenses

- **Algunos ejemplos de Técnicas Anti Forenses? (cont.)**

  - Encriptación de archivos
  - Utilización de protocolos de encriptados
  - Rootkits
  - Explotación de bugs en las mismas herramientas forenses
  - Detección de actividades de herramientas forenses

Técnicas Anti Forenses

- **Qué ocurre cuando borramos un archivo de un sistema FAT?**

  - El sistema operativo reemplaza la primera letra del nombre del archivo borrado con un byte de control que indica que ha sido borrado (E5 en hexadecimal)

  - El clúster correspondiente en donde se ubica el archivo en FAT es marcado como libre, para que pueda ser reutilizado más adelante, sin embargo, sigue teniendo información.

  - En NTFS es similar, solo que se marca como borrado en la tabla maestra de archivos MFT y el clúster se marca como libre también.

Técnicas Anti Forenses

- **Protecciones por Contraseña**
  - Los archivos protegidos por contraseñas son comunes, para ellos, el investigador forense debe utilizar herramientas de password cracking.
  - En los laboratorios de esta semana encontraremos ejercicios de este tipo y algunos tips!!
  - Recuerde que la evaluación de la escena muchas veces nos puede ayudar con la generación de los diccionarios y ataques de fuerza bruta, sea observador!!!

Técnicas Anti Forenses

- **Archivos ocultos en las estructuras del sistema operativo y en otros medios**

  - En uno de los laboratorios de la semana 1 utilizamos el registry reaper, que nos permitió obtener grandes detalles del registro de Windows e identificar unidades de almacenamiento que han sido utilizadas en el equipo así como archivos ejecutados recientemente que nos pueden dar pistas de interés.

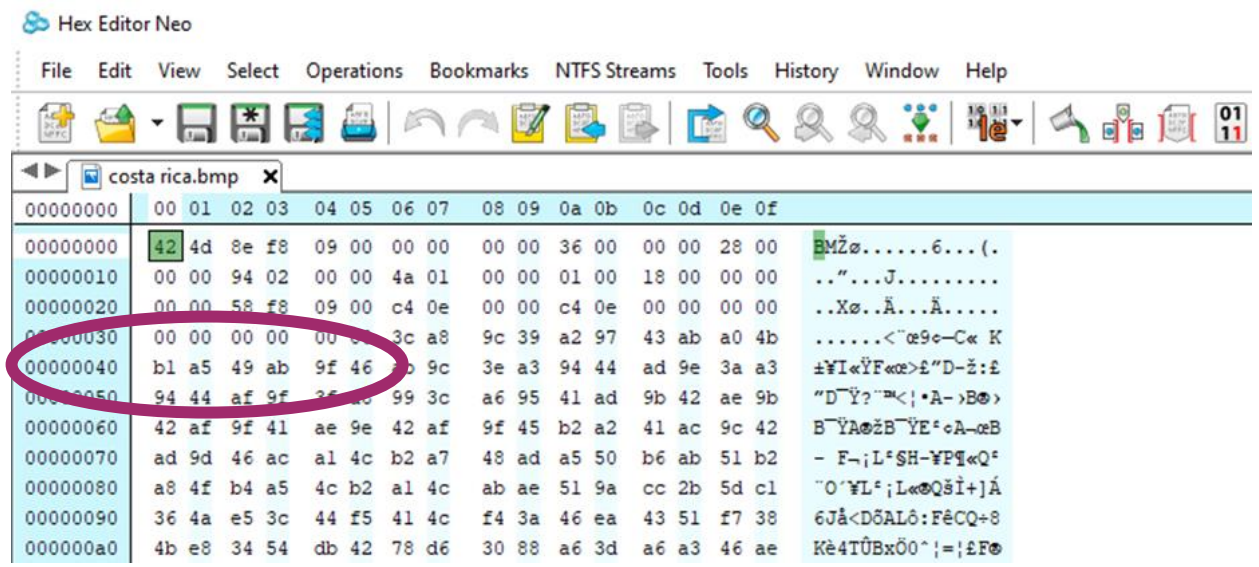
  - Una técnica comúnmente utilizada es la esteganografía, método mediante el cual podemos esconder un archivo de interés en una fotografía, video o audio. Inclusive podemos habilitar cifrado y contraseñas para complicar la labora forense.

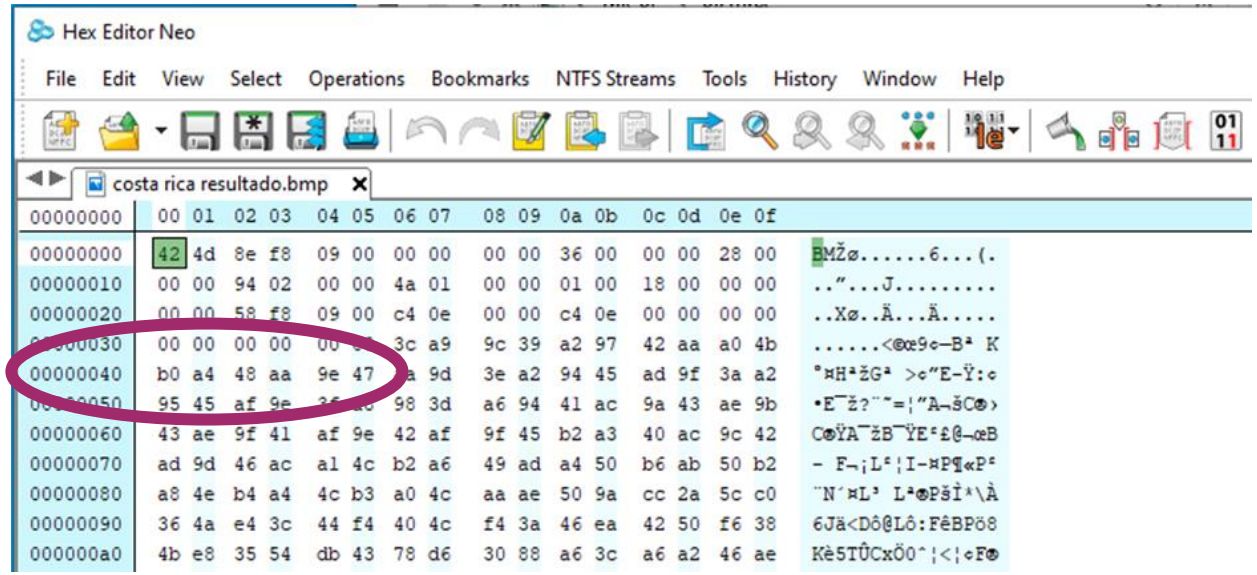
Técnicas Anti Forenses

fidélitas Virtual

Técnicas Anti Forenses

fidélitas Virtual





Técnicas Anti Forenses

- **Spoofing de Direccion IP**

  - Cambiar nuestra dirección IP y ocultarnos a la hora de generar un ataque es sencillo y existen múltiples formas de hacerlo.

  - Una de las más conocidas es TOR, que permite con tan solo descargar el navegador cambiar nuestra identidad múltiples veces y pasar por una serie de equipos que hacen muy complicado que se logre determinar una traza real.

  - Vamos a realizar un Laboratorio de este tema también para aprender esta técnica antiforense y cómo podemos detectar su utilización como peritos forenses.

fidélitas
Virtual

Gracias