Universidad de La Laguna

Práctica de Laboratorio #13. Análisis Forense

En esta práctica vamos a realizar dos ejercicios de **Análisis Forense**, que fueron presentados en elhacker.net como dos retos de análisis forense. Siguiendo los análisis realizados en ambos casos aprenderemos a utilizar las herramientas básicas en análisis forense de sistemas informáticos.

Ejercicios

Reto 1

La Brigada Especial de Delitos Informáticos ha sido requerida por la Policía. Ésta, llevaba 2 meses detrás de una red de narcotraficantes, consiguiendo averiguar que en unos pocos días iba a tener lugar uno de los intercambios de cocaína más importantes de los últimos tiempos.

En el momento oportuno atraparon a uno de los integrantes de la banda residente en el país, el cual llevaba en su poder un pendrive con información que se piensa puede ser muy valiosa para el desmantelamiento de ambas bandas y del intercambio. En este caso te ha tocado a ti investigar el caso, una gran responsabilidad, pero a la vez una gran oportunidad, serás capaz de estar a la altura??

Los "expertos" de la policía han hecho sus propios hallazgos antes de entregarte el pendrive:

- Sistema de Archivos: ext2
- Información de utilidad en el penDrive: fecha, hora y lugar del intercambio (se lo consiguieron sonsacar al detenido, así como el conocimiento de que todo lo que se pueda necesitar en un momento dado, está igualmente en el pendrive) Por desgracia parece ser que los delincuentes fueron precavidos, y tomaron ciertas medidas para que esta información no sea evidente a primera vista...

Tu misión será hacer un análisis exhaustivo de la situación para conseguir sacar todos los datos posibles: Fecha y hora de la entrega, nombre del jefe de la banda, lugar del intercambio...

SOLUCIÓN AL RETO

C/ Padre Herrera s/n
38207 La Laguna
Santa Cruz de Tenerife. España

T: 900 43 25 26

ull.es

Reto 2

La Brigada Especial de Delitos Informáticos ha sido requerida por la Policía nuevamente.

Esta vez andan detrás de un grupo de narcos que han fundado un nuevo laboratorio en la zona para cortar la cocaína y después sacarla al mercado.

Uno de los mochileros de la banda fue interceptado, siéndole incautado 1 Kg de cocaína cortada y un pendrive. No fue posible sonsacarle nada al individuo, por miedo de este a las posibles represalias de la banda, pero se sospecha que dentro del pendrive llevaba información sobre dónde está el nuevo laboratorio clandestino de la organización.

Por desgracia parece ser que los delincuentes fueron precavidos, y tomaron ciertas medidas para que esta información no sea evidente a primera vista...

Tu misión será hacer un análisis exhaustivo de la situación para conseguir la dirección del laboratorio y así desarticular la banda entera.

SOLUCIÓN AL RETO

Escribir un informe pormenorizado de los pasos realizados en ambos análisis y las herramientas utilizadas. Explicar en cada caso cómo se ha asegurado la cadena de custodia en el acceso a la información cuando se ha estado realizando el análisis.