SOFTWARE PARA RECOLECCIÓN DE EVIDENCIAS DIGITALES RÁPIDAS EN SISTEMAS WINDOWS

UNIVERSIDAD NACIONAL DEL NORDESTE

Autores: Lic. Marcos Adrián Monti, Dr. David Luis La Red Martínez / Facultad de Ciencias Exactas y Naturales y Agrimensura / Universidad Nacional del

RESUMEN

La necesidad de análisis de evidencia digital forense comprende ciertos desafíos en cuanto a escasez de herramientas de software disponibles, los altos costos y sobre todo los tiempos requeridos para llevar a cabo estos análisis, los cuales dependen en gran manera de la capacidad de los equipos involucrados. Resulta conveniente disponer de la capacidad de capturar información en el lugar del hecho utilizando las herramientas de software disponibles de manera inteligente de modo que sea posible discernir, cuando exista un gran volumen de equipos, cuáles podrían ser de interés a la causa judicial y cuáles no.

CONTEXTO

La Problemática se desarrolla en el contexto del análisis forense de evidencias digitales en el Poder Judicial, uno de los organismos públicos de la Provincia de Formosa. La informática forense o el cómputo forense es el uso de métodos y técnicas científicas probadas, con el fin de identificar, preservar, validar, analizar, interpretar, documentar y presentar evidencia digital obtenida a partir de fuentes de información digital, con el propósito de facilitar la reconstrucción de hechos en una investigación legal, o ayudar a anticipar o prevenir acciones en contra de la ley. De esta manera la Informática Forense actúa como una rama de la Informática que provee un complementario a la Criminalística clásica, enfocándose en el análisis de las evidencias digitales, que pudiesen existir, en cualquier escena del hecho.

FaCENA
FACULTAD DE CIENCIAS EXACTAS Y NATURALES Y AGRIMENSURA

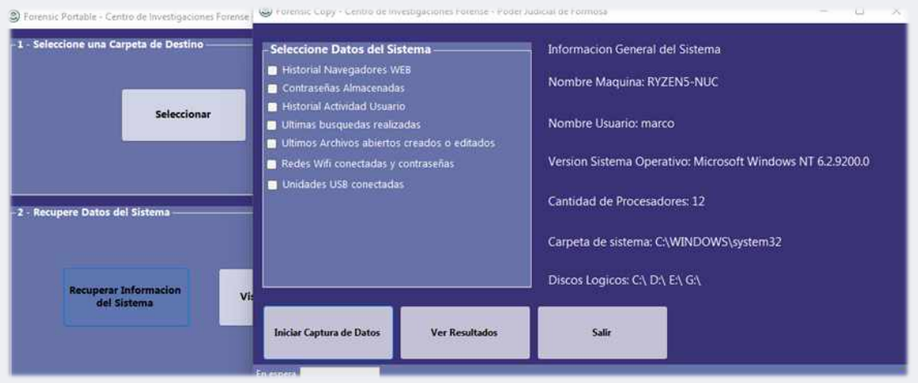
LINEAS DE INVESTIGACION Y DESARROLLO

Los objetivos del trabajo consistieron en el estudio, recopilación y análisis de datos que son factibles de recuperar en sistemas que ejecutan el sistema operativo Microsoft Windows sobre la actividad de el/los usuario/s del mismo, con el objetivo de desarrollar herramientas de software que permitan automatizar las tareas de captura de información.

RESULTADOS OBTENIDOS

Se ha obtenido como resultado una aplicación de tipo portable capaz de ejecutarse en sistemas Windows desde cualquier dispositivo o unidad de disco portátil. Sus modulos principales son:

- Modulo de recuperacion de datos del sistema: Desde aquí es posible obtener información de uso del sistema



- Módulo de Copia Forense: En este modulo tendremos la posibilidad de realizar una copia forense de todos los archivos que resulten de interés.