RESUMEN

El análisis Forense es un área de la seguridad informática que surge a raíz de problemas de incidentes de seguridad. La tecnología avanzado aceleradamente así como también la forma en que se operan y se almacenan los medios informáticos. La idea principal de este proyecto es desarrollar una guía metodológica, que en base a la utilización de herramientas se obtiene la réplica o imagen del disco óptico donde reside la evidencia para una recolección, análisis digital y el análisis forense. La guía metodológica utilizada es: Preparar, identificar, recolectar, preservar, analizar e informar, proporcionando un marco teórico que sustente la investigación y análisis forense. Se utiliza la herramienta de distribución de Linux forense llamado Caine (Computer Aided Investigative Environment), el mismo que cuenta con una serie de utilidades y herramientas para: el estudio preliminar, recolección de la evidencia, análisis de la evidencia.

Palabras Claves

CAINE
FORENSE
AUTOPSY
EVIDENCIA

ABSTRACT

Forensic analysis is an area of computer security that arises as a result of problems of security incidents. Technology advanced rapidly as well as also the form in which they operate, and the resources are stored. The main idea of this project is to develop a methodological guide, which gets the replica or image of the optic disc resides for a collection, digital analysis and forensic evidence based on the use of tools. The methodological guide used is: prepare, identify, collect, preserve, analyze, and report, providing a framework that supports the research and forensic analysis. Using the Linux distribution forensic named Caine (Computer Aided Investigative Environment), which features a series of utilities and tools for: the preliminary study, evidence collection and analysis of evidence.

KeyWords

CAINE
FORENSE
AUTOPSY
EVIDENCE