

RESUMEN EJECUTIVO

En la actualidad el mundo se encuentra en medio de una nueva Era Digital, la tecnología avanza tanto que ha llegado a formar parte de nuestro día a día en actividades como, ocio, educación, comunicación, salud, negocios, etc. Sin embargo conjuntamente con estos avances también la delincuencia ha buscado la forma de adaptarse al medio, y recientemente en la última década, la informática forense ha tomado gran importancia a nivel mundial, los gobiernos han implementado leyes que castiguen este tipo de delitos pero al igual que en cualquier delito se necesita pruebas, un análisis minucioso y a fondo que permita encontrar un culpable, como se llevó a cabo el delito y poder tomar acciones preventivas en base a estos casos. En el mercado se puede encontrar muchas herramientas válidas para este tipo de tareas sin embargo hablando de Windows 8 que es un sistema privativo, muchas de estas herramientas son privadas y para su uso se debe adquirir una licencia por un lapso de tiempo establecido. El presente trabajo de titulación desarrolla una propuesta para el uso de herramientas Open Source aplicando adecuadamente las fases de un análisis forense y basado teóricamente en las mejores prácticas de la informática forense.

Palabras Clave

INFORMÁTICA FORENSE

OPEN SOURCE

WINDOWS 8

CADENA DE CUSTODIA

CYBER-CRIMEN

ABSTRACT

Nowadays the world is in the middle of a new digital era, technology advances so much that has become part of our day to day activities such as entertainment, education, communication, health, business, etc. Nevertheless together with these advances also crime has found new ways to adapt to the environment, and recently in the last decade, computer forensics took importance globally, governments have implemented laws that punish such crimes but any crime needs evidence, and a meticulous and thoroughly analysis which help to find the guilty, how it was done and take corrective and preventive actions on the basis of these cases. In the market you can find many valid tools for these tasks however talking about Windows 8 which is a proprietary system, many of these tools are private and for use must acquire a license for a set time period. This thesis develops a proposal for the use of Open Source tools properly applying the phases of a forensic analysis and theoretical based on the best practices of computer forensics.

Key Words

COMPUTER FORENSICS

OPEN SOURCE

WINDOWS 8

CHAIN OF CUSTODY

CYBER-CRIME