Maestría en

CIBERSEGURID

Trabajo de investigación previo a la obtención del título de

Magíster en Ciberseguridad

AUTORES:

Ing. Kevin Bolívar Lascano Sánchez

Ing. Víctor Hugo Ponce Chamorro

Ing. David Leandro Chipantiza Chacha

Ing. Carlos Andrés Narváez Tello

TUTORES:

Ing. Iván Reyes

Ing. Alejandro Cortés

TEMA:

Extracción y análisis de datos de dispositivos iOS con un enfoque forense para abogados de la ciudad de Puyo.

Quito – Ecuador

Octubre 2024

RESUMEN

El presente trabajo se centra en la extracción y análisis de datos de dispositivos iOS con un enfoque forense, dirigido a abogados en la ciudad de Puyo. Se busca establecer un marco teórico sólido sobre el análisis forense digital, enfatizando las técnicas de extracción de datos críticos. Se adoptaron metodologías reconocidas, como el modelo Digital Forensic Research Workshop (DFRWS) y el modelo Association of Chief Police Officers (ACPO), para garantizar la integridad de la evidencia digital a lo largo del proceso.

La metodología aplicada se desglosa en varias etapas: preservación, donde se asegura la integridad de la evidencia; recolección, utilizando herramientas especializadas como Magnet Axiom y Cellebrite; examen y análisis, enfocado en identificar patrones y datos relevantes; y documentación y reporte, que garantiza la transparencia en los hallazgos. Estos pasos garantizan que el proceso se alinee con las mejores prácticas en la disciplina forense.

Se llevaron a cabo dos casos ficticios, diseñados exclusivamente para fines educativos: la filtración de documentos confidenciales y el hurto y venta de un automotor, ambos utilizando un dispositivo Apple iPhone 7. Los resultados de la investigación destacan la importancia de herramientas forenses efectivas, identificando a Magnet Axiom, Cellebrite UFED y Cellebrite Physical Analyzer como esenciales para el análisis de datos críticos. Esto proporciona a los abogados de Puyo recursos valiosos para la gestión de casos que involucren dispositivos móviles, asegurando la validez y fiabilidad de la información obtenida.

Palabras clave: Análisis forense, dispositivos iOS, extracción de datos, Magnet Axiom, Cellebrite, evidencia digital, DFRWS, ACPO.

ABSTRACT

This study focuses on the extraction and analysis of data from iOS devices with a forensic approach, aimed at lawyers in the city of Puyo. It seeks to establish a solid theoretical framework on digital forensic analysis, emphasizing critical data extraction techniques. Recognized methodologies such as the Digital Forensic Research Workshop (DFRWS) model and the Association of Chief Police Officers (ACPO) model were adopted to ensure the integrity of digital evidence throughout the process.

The applied methodology is divided into several stages: preservation, ensuring the integrity of the evidence; collection, utilizing specialized tools such as Magnet Axiom and Cellebrite; examination and analysis, focused on identifying patterns and relevant data; and documentation and reporting, which ensures transparency in findings. These steps ensure that the process aligns with best practices in the forensic discipline.

Two fictitious cases were carried out, designed exclusively for educational purposes: the leakage of confidential documents and the theft and sale of a motor vehicle, both using an Apple iPhone 7. The research results highlight the importance of effective forensic tools, identifying Magnet Axiom, Cellebrite UFED, and Cellebrite Physical Analyzer as essential for analyzing critical data. This provides lawyers in Puyo with valuable resources for managing cases involving mobile devices, ensuring the validity and reliability of the obtained information.

Keywords: Forensic analysis, iOS devices, data extraction, Magnet Axiom, Cellebrite, digital evidence, DFRWS, ACPO.