Maestría en

CIBERSEGURIDAD

Trabajo previo a la obtención de título de
Magister en Ciberseguridad

AUTORES:

Miguel F. Lema

Mireya D. Álvarez

Ángel E. Gaona

Katherine E. Vera

TUTOR:

Ing. Iván Reyes

Análisis Forense de Videollamadas en Sistemas Operativos

Quito - Ecuador

Junio– 2025

REINVENTEMOS EL FUTURO

RESUMEN

En el presente trabajo se realiza un análisis forense digital basado en la plataforma de videoconferencias Zoom, ejecutadas en los sistemas operativos Windows y Linux. El objetivo principal es realizar un análisis forense comparativo en la plataforma de videollamadas Zoom bajo sistemas operativos Windows y Linux, con el fin de identificar evidencias digitales relevantes para procesos de investigación.

A través de la creación de escenarios controlados, se recopilaron evidencias antes y después de reuniones virtuales utilizando imágenes forenses de disco, volcado de memoria y herramientas de análisis como Wireshark, FTK Imager, Guymager, Belkasoft Live RAM Capture, LiME (Linux Memory Extractor), Autopsy, Belkasoft Evidence Center X, DB Browser for SQLite, Python con Volatility, y técnicas de extracción de artefactos. Se analizaron directorios específicos como *AppData*, *Documents\Zoom* y registros del sistema para identificar archivos relevantes como zoomus.db, zoomus.enc.db y logs de ejecución.

Los resultados evidencian diferencias significativas en la persistencia y tipo de evidencias según la versión de Zoom utilizada y el sistema operativo, siendo más accesibles en Windows que en Linux, y más completas en versiones de pago. Asimismo, se destacan aspectos relacionados con la seguridad, la privacidad de los datos, y la dificultad de recuperación en entornos cifrados.

Este trabajo contribuye al campo de la informática forense al ofrecer una guía práctica, permitiendo una mejor preparación frente a incidentes que involucren herramientas de videocomunicación en contextos empresariales o judiciales.

Palabras clave: análisis forense, Zoom, videollamadas, artefactos digitales, Windows, Linux, privacidad, cifrado.

ABSTRACT

This research presents a digital forensic analysis based on the Zoom videoconferencing platform, executed on both Windows and Linux operating systems. The primary objective is to perform a comparative forensic examination of Zoom across these systems, aiming to identify digital evidence relevant to investigative procedures.

Through the creation of controlled scenarios, evidence was collected before and after virtual meetings using disk forensic images, memory dumps, and analysis tools such as Wireshark, FTK Imager, Guymager, Belkasoft Live RAM Capturer, LiME (Linux Memory Extractor), Autopsy, Belkasoft Evidence Center X, DB Browser for SQLite, and Python with Volatility, alongside artifact extraction techniques. Specific directories such as AppData, Documents\Zoom, and system registry entries were analyzed to identify relevant files such as zoomus.db, zoomus.enc.db and execution logs.

The results reveal significant differences in the persistence and type of digital evidence depending on the Zoom version and operating system, with data being more accessible in Windows environments than in Linux, and more comprehensive in paid versions of the platform. Additionally, key issues related to data security, user privacy, and the challenges of recovery in encrypted environments are highlighted.

This work contributes to the field of digital forensics by offering a practical guide that enhances preparedness for incidents involving videoconferencing tools in corporate or judicial contexts.

Keywords: forensic analysis, Zoom, videoconferencing, digital artifacts, Windows, Linux, privacy, encryption.