Maestría en

CIBERSEGURIDAD

Trabajo previo a la obtención de título de Magister en Ciberseguridad

AUTOR/ES:

Ascencio Moreno Luis Javier

Granizo Fonseca Fernando Andrés

Jami Jami Sandra Isabel

Montenegro Salazar Manuel Felipe

TUTOR/ES:

Iván Reyes Chacón

Alejandro Cortés López

Análisis Forense de Registros de Videollamadas de Microsoft Teams para la Resolución de Casos de Ciberacoso

REINVENTEMOS EL FUTURO

RESUMEN

El presente trabajo aborda un caso simulado de ciberacoso laboral en entornos digitales, específicamente utilizando la plataforma Microsoft Teams como escenario principal. El objetivo fue demostrar la viabilidad de aplicar técnicas de análisis forense digital para identificar, extraer y preservar evidencia relacionada con actos de acoso en contextos corporativos virtuales. Para ello, se diseñó un entorno controlado que replicó una reunión en línea entre cuatro colaboradores de una empresa ficticia, donde uno de los participantes adopta un rol de agresor frente a otro compañero.

Los resultados evidencian que es técnicamente posible obtener información de valor forense desde los dispositivos utilizados, incluso cuando se trata de plataformas en la nube como Teams. Se lograron recuperar mensajes eliminados, registros de archivos compartidos y referencias a carpetas ofensivas, todo lo cual respalda el incidente reportado en el escenario planteado. Este ejercicio valida el uso de metodologías forenses en entornos de colaboración digital y demuestra que, con las herramientas adecuadas, es factible generar evidencia sólida que sirva de sustento en investigaciones internas o procesos legales.

Palabras clave: análisis forense digital, Microsoft Teams, ciberacoso laboral, memoria RAM, Autopsy, Volatility, evidencia digital, captura de memoria, ciberseguridad empresarial, investigación forense.

ABSTRACT

This project explores a simulated case of digital workplace harassment, using Microsoft Teams as the primary platform for interaction. The main objective was to demonstrate the feasibility of applying digital forensic techniques to identify, extract, and preserve evidence related to online harassment incidents within professional environments. To achieve this, a controlled scenario was created, replicating a virtual meeting among four employees from a fictitious company, where one participant played the role of the aggressor toward another.

The results show that it is technically possible to obtain valuable forensic information from the devices used, even when dealing with cloud-based platforms like Teams. Deleted messages, shared file logs, and references to offensive folders were successfully recovered, supporting the reported scenario. This exercise validates the use of forensic methodologies in digital collaboration environments and demonstrates that, with the right tools, it is feasible to generate solid evidence to support internal investigations or legal proceedings.

Keywords: digital forensics, Microsoft Teams, workplace cyberbullying, RAM memory, Autopsy, Volatility, evidence, dump, corporate cybersecurity, forensic investigation.