World Academy of Science, Engineering and Technology
International Journal of Law and Political Sciences
Vol:16, No:03, 2022

WormHex: Evidence Retrieval Tool of Social Media from Volatile Memory

Authors : Norah Almubairik, Wadha Almattar, Amani Alqarni

Abstract : Social media applications are increasingly being used in our everyday communications. These applications utilise end-to-end encryption mechanisms, which make them suitable tools for criminals to exchange messages. These messages are preserved in the volatile memory until the device is restarted. Therefore, volatile forensics has become an important branch of digital forensics. In this study, the WormHex tool was developed to inspect the memory dump files of Windows and Mac-based workstations. The tool supports digital investigators to extract valuable data written in Arabic and English through web-based WhatsApp and Twitter applications. The results verify that social media applications write their data into the memory regardless of the operating system running the application, with there being no major differences between Windows and Mac.

Keywords : volatile memory, REGEX, digital forensics, memory acquisition
Conference Title : ICDFFE 2022 : International Conference on Digital Forensics and Forensic Evidence
Conference Location : Miami, United States
Conference Dates : March 11-12, 2022