Jordan University of Science and Technology

Towards the Memory Forensics of MS Word Documents

Authors: Ziad A. Al-Sharif, Hasan Bagci, Toqa' Abu Zaitoun and Aseel Asad

Abstract: Memory forensics plays a vital role in digital forensics. It provides important information about user?s activities on a digital device. Various techniques can be used to analyze the RAM and locate evidences in support for legal procedures against digital perpetrators in the court of law. This paper investigates digital evidences in relation to MS Word documents. Our approach utilizes the XML representation used internally by MS Office. Different documents are investigated. A memory dump is created while each of these documents is being viewed or edited and after the document is closed. Used documents are decompressed and the resulting folders and XML files are analyzed. Various unique parts of these extracted files are successfully located in the consequent RAM dumps. Results show that several portions of the MS Word document formats and textual data can be successfully located in RAM and these portions would prove that the document is/was viewed or edited by the perpetrator.