Jordan University of Science and Technology

Towards Carving PDF Files in the Main Memory

Authors: Ziad A. Al-Sharif, Dana N. Odeh and Mohammad I. Al-Saleh

Abstract: Digital forensics concerns about extracting and analyzing the contents of digital devices. It is used to locate digital evidences in order to support legal actions against criminals in the court of law. This paper utilizes file carving techniques to extract digital evidences in the RAM about opened PDF files. This paper observes that PDF files consist of objects. Each object is marked with special indicators that mark its start and end. These indicators are used to locate and extract the objects of a PDF file from the RAM. We design several experiments and show that carving PDF files from the RAM is possible even after closing the PDF file viewer.