Jordan University of Science and Technology

Utilizing data lifetime of TCP buffers in digital forensics: Empirical study

Authors: Mohammed I. Al-Saleh and Ziad A. Al-Sharif

Abstract: Digital Forensics (DF) is vital for providing digital evidence of computer crimes and security violations. As the Internet community grows in size, many individuals are actively and continually committing cyber crimes such as stealing private information, credit card numbers, copyrighted material, and even threatening innocent people. Locating criminals and proving them guilty might involve tracing their IP addresses, identifying their physical locations, and investigating their machines to look for evidence. Inspecting hard drives and solid state disks has been proven useful in DF because they can keep information permanently. Much of information, though, is not stored on permanent storage devices instead are temporarily kept in the physical memory (or RAM). The RAM, though volatile, can also be inspected for evidence. In this paper, we present a study that helps investigators make use of the valuable, stealthy TCP Connections' Artifacts (TCPCA) that sit in the RAM for a while even after the connection is torn down. We show different scenarios and present our results. Even though dumping and inspecting the RAM for evidence extraction is not new in literature, to the best of our knowledge, we are the first to study the behavior and the possibility of using TCPCA in the RAM for DF.