Jordan University of Science and Technology

RAM Forensics against Cyber Crimes Involving Files

Authors: Mohammed Al-Saleh and Ziad Al-Sharif

Abstract: Cyber crimes are explosively increasing as a result of the wide deployment of the Internet. Breaking into others? machines to steal their valuable information (such as credit card numbers) or execute unwanted code, threatening innocent people, pirating copyrighted software, and distributing malicious software are examples of such crimes. Digital Forensics (DF) techniques are utilized to accuse cyber criminals and prove them guilty. This paper observes that many different violations explicitly or implicitly involve files . A file is a logical entity that might occupy different physical locations in the system. Explicit actions that involve files include directly downloading them from the Internet resources or copying them from external storage devices. On the other hand, viewing some entities (such as pictures, audios, videos, etc.) in web browsers might implicitly involve files. Using peer-to-peer networks (e.g., BitTorrent), however, requires partitioning a file into different pieces and distributing them among the participating peers. The requesting peer can download the pieces from the other peers. In this case, the involved file is physically partitioned and downloaded from different locations . Finding files in criminals? machines can be used as an evidence against them. This paper shows that, in many cases, violators? actions can be thought of as if they are involving files. We design different experiments and examine the state of the physical memory (RAM) after an activity that explicitly or implicitly involves a file. We show that all or some portions of the files can be found in the RAM memory. This research considers the way the Operating System (OS) manages the RAM memory and how it loads data into it. Furthermore, because the OS allocates memory spaces for processes in a page granularity, this paper shows that searching for files can be effectively and efficiently conducted in a page granularity. Finally, this paper sho