Volatile Memory Forensics: A Legal Perspective

International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 155
-
Number 3

Year of Publication: 2016

Authors:

Harnoor Kaur Mann, Gurpal Singh Chhabra

Abstract

In today's world of fast changing technology where everything is governed by Internet directly or indirectly, the trend of crime has undergone a dramatic change over the past few years. Today, one can commit a crime with just a click of a button on laptop or computer and enjoy the garb of anonymity and impunity to a great extent. In such a scenario, it has become imperative to throw some light on the emerging issue of tackling cybercrimes in 21st century. This paper describes the extraction and analysis of volatile data that is available in computer's RAM that is in a running state on windows operating systems and shows the utility of RAM in Computer Forensics that is often neglected while crime scenario with running system is encountered. Keeping in view this necessity, it is essential to consider the issues of digital evidence and their collection, preservation, and admissibility in the court of law.

References

1. Remzi H. Arpaci-Dusseau, Andrea C. Arpaci-Dusseau, Operating Systems: Three Easy
7. https://forensicswiki.org/wiki/Memory_analysis

Index Terms

Computer Science  Information Sciences

Keywords

Read Only Memory (ROM), Acquisition, Seizing, Verifying, imaging, Random Access Memory (RAM), Integrity, Authenticity, Address Resolution Protocol (ARP), Man-In-The-Middle Attack.