Jordan University of Science and Technology

Utilizing Program's Execution Data for Digital Forensics

Authors: Ziad A. Al-Sharif

Abstract: Criminals use computers and software to perform their crimes or to cover their misconducts. Main memory or RAM encompasses vibrant information about a system including its active processes. Program's variables data and value vary in their scope and duration in RAM. This paper exploits program's execution state and its dataflow to obtain evidence of the software usage. It extracts information left by program execution in support for legal actions against perpetrators. Our investigation model assumes no information is provided by the operating system; only raw RAM dumps. Our methodology employs information from the target program source code. This paper targets C programs that are used on Unix based systems. Several experiments are designed to show that scope and storage information of various source code variables can be used to identify program's activities. Results show that investigators have good chances locating various variables' values even after the process is stopped.