World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:13, No:01, 2019

Rapid Evidence Remote Acquisition in High-Availability Server and Storage System for Digital Forensic to Unravel Academic Crime

Authors : Bagus Hanindhito, Fariz Azmi Pratama, Ulfah Nadiya

Abstract : Nowadays, digital system including, but not limited to, computer and internet have penetrated the education system widely. Critical information such as students' academic records is stored in a server off- or on-campus. Although several countermeasures have been taken to protect the vital resources from outsider attack, the defense from insiders threat is not getting serious attention. At the end of 2017, a security incident that involved academic information system in one of the most respected universities in Indonesia affected not only the reputation of the institution and its academia but also academic integrity in Indonesia. In this paper, we will explain our efforts in investigating this security incident where we have implemented a novel rapid evidence remote acquisition method in high-availability server and storage system thus our data collection efforts do not disrupt the academic information system and can be conducted remotely minutes after incident report has been received. The acquired evidence is analyzed during digital forensic by constructing the model of the system in an isolated environment which allows multiple investigators to work together. In the end, the suspect is identified as a student (insider), and the investigation result is used by prosecutors to charge the suspect as an academic crime.

Keywords : academic information system, academic crime, digital forensic, high-availability server and storage, rapid evidence remote acquisition, security incident
Conference Title : ICDFCI 2019 : International Conference on Digital Forensics and Cybercrime Investigation
Conference Location : Bali, Indonesia
Conference Dates : January 14-15, 2019