World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:14, No:10, 2020

A Unified Approach for Digital Forensics Analysis

Authors : Ali Alshumrani, Nathan Clarke, Bogdan Ghite, Stavros Shiaeles

Abstract : Digital forensics has become an essential tool in the investigation of cyber and computer-assisted crime. Arguably, given the prevalence of technology and the subsequent digital footprints that exist, it could have a significant role across almost all crimes. However, the variety of technology platforms (such as computers, mobiles, Closed-Circuit Television (CCTV), Internet of Things (IoT), databases, drones, cloud computing services), heterogeneity and volume of data, forensic tool capability, and the investigative cost make investigations both technically challenging and prohibitively expensive. Forensic tools also tend to be siloed into specific technologies, e.g., File System Forensic Analysis Tools (FS-FAT) and Network Forensic Analysis Tools (N-FAT), and a good deal of data sources has little to no specialist forensic tools. Increasingly it also becomes essential to compare and correlate evidence across data sources and to do so in an efficient and effective manner enabling an investigator to answer high-level questions of the data in a timely manner without having to trawl through data and perform the correlation manually. This paper proposes a Unified Forensic Analysis Tool (U-FAT), which aims to establish a common language for electronic information and permit multi-source forensic analysis. Core to this approach is the identification and development of forensic analyses that automate complex data correlations, enabling investigators to investigate cases more efficiently. The paper presents a systematic analysis of major crime categories and identifies what forensic analyses could be used. For example, in a child abduction, an investigation team might have evidence from a range of sources including computing devices (mobile phone, PC), CCTV (potentially a large number), ISP records, and mobile network cell tower data, in addition to third party databases such as the National Sex Offender registry and tax records, with the desire to auto-correlate and across sources and visualize in a cognitively effective manner. U-FAT provides a holistic, flexible, and extensible approach to providing digital forensics in technology, application, and data-agnostic manner, providing powerful and automated forensic analysis.

Keywords : digital forensics, evidence correlation, heterogeneous data, forensics tool
Conference Title : ICDFI 2020 : International Conference on Digital Forensics and Investigations
Conference Location : Los Angeles, United States
Conference Dates : October 29-30, 2020