Computer forensics suites

Technology, Information Technology

Computer Forensics

Research has proved that every year there is a significant rise of criminal activities performed using computers. Most of the culprits are driven to the criminal activities by factors that include; intellectual gain, financial gain, sexual impulses, thrill-seeking, and addiction, just to mention but a few (Eoghan 2011). However, with the advanced technology, the scientists improvised Computer Forensics suites that have been used in the pursuit of curbing the criminal activities. This paper discusses Online Digital Forensic suite as the most efficient suite in investigating computer forensics cases, and cyber crime activities.

Online Digital forensics Suite assists administrators and investigators in collecting a wide variable data from the suspected machines. This tool does not require installation of an agent on the targeted machine. Online Digital Forensics Suite enables rapid and sound examination of the targeted computer without disrupting the current operations of a given premises (Martin 2006). It offers an extensive functional framework for the investigators, and captures volatile and consistent data from the target under examination. The suite saves time in collection of data, therefore, enabling a fast and reliable response to an intrusion or crime act. Handling of the suite is very simplified. It does necessarily need technical training. The suite enables a visual display of images and an automatic storing of data needed form the targeted computer (Ibrahim 2010). No software is needed to be preloaded on the target. This makes it cheap to implement and use. Additionally, the tool uses power sparingly as compared to the available suites.

Online Digital Forensic Suite is basically browser based. The browser based interface enables the conducting investigator to connect to Online Digital Forensic Suite and manage investigation from any given location. This is enabled by the use of a wide variety of browsers and Organizing System platforms. The connection is protected by https and all information or data sent crosswise is encrypted. Data analysis with the suite is forensically sound. It employs best and accepted practices that preserve the integrity and validity of evidence (Ibrahim 2010).

Online Digital Forensic Suite enables live forensics. It captures volatile information sent from running systems that can be lost if the systems are powered down. This permits conventional analysis of the forensic data. The crucial volatile data and information includes listening to the servers, running processes, network connection, open ports and memory. Files with strange names and strange location arouse suspicion forensic examination. This tool gathers information from a running system that cannot be retrieved by any other way.

Personally, I would suggest that the local law enforcement agency consider purchasing the Online Digital Forensic Suite. The suite enables non-invasive live and rapid data analysis. The suite is easy to use and does not call for added cost of training as compared to the rest of the available suites. The suite enables extensive investigation due to the use of the web browsers (John 2005). This tool enhances capture of persistent and volatile data from the systems under examination. The suite has proved to be efficient in investigation, basing my argument on the past conducted investigation on the suite usage. Many illegal deals have been stopped by the agencies using

this forensic suite. Notably, the suite employs acceptable practices that preserve the integrity and validity of the evidence. Therefore, the evidence compiled from this tool can be used in the courts of law as evidence.

References

Eoghan, C. (2011). Digital Evidence and Computer Crime: Forensic Science. Massachusetts: Academic Press

Ibrahim, B. (2010). Digital Forensic and Cyber Crime. Berlin: Springer Publishers

John, R. (2005). Computer Crime Scene Investigation. Stamford: Cengage Learning

Martin, O. (2006). Advanced Forensics II: International On Digital Forensic. Berlin: Springer

Publishers