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

Anti-Forensic Countermeasure: An Examination and Analysis Extended Procedure for Information Hiding of Android SMS Encryption Applications

Authors : Ariq Bani Hardi

Abstract : Empowerment of smartphone technology is growing very rapidly in various fields of science. One of the mobile operating systems that dominate the smartphone market today is Android by Google. Unfortunately, the expansion of mobile technology is misused by criminals to hide the information that they store or exchange with each other. It makes law enforcement more difficult to prove crimes committed in the judicial process (anti-forensic). One of technique that used to hide the information is encryption, such as the usages of SMS encryption applications. A Mobile Forensic Examiner or an investigator should prepare a countermeasure technique if he finds such things during the investigation process. This paper will discuss an extension procedure if the investigator found unreadable SMS in android evidence because of encryption. To define the extended procedure, we create and analyzing a dataset of android SMS encryption application. The dataset was grouped by application characteristics related to communication permissions, as well as the availability of source code and the documentation of encryption scheme. Permissions indicate the possibility of how applications exchange the data and keys. Availability of the source code and the encryption scheme documentation can show what the cryptographic algorithm specification is used, how long the key length, how the process of key generation, key exchanges, encryption/decryption is done, and other related information. The output of this paper is an extended or alternative procedure for examination and analysis process of android digital forensic. It can be used to help the investigators while they got a confused cause of SMS encryption during examining and analyzing. What steps should the investigator take, so they still have a chance to discover the encrypted SMS in android evidence?

Keywords : anti-forensic countermeasure, SMS encryption android, examination and analysis, digital forensic
Conference Title : ICDFCI 2019 : International Conference on Digital Forensics and Cybercrime Investigation
Conference Location : Bali, Indonesia
Conference Dates : January 14-15, 2019