Digital Forensics: Current Scenario and Future Challenges

Sonal LAKADE
Digital and Cyber Forensic Department, Institute of Forensic Science, Mumbai, Maharashtra, India
sonal.lakade73@gmail.com

Abstract

A major challenge to digital forensic analysis is the ongoing growth in the volume of data seized and presented for analysis. This is a result of the continuing development of storage technology, including increased storage capacity in consumer devices and cloud storage services, and an increase in the number of devices seized per case. The information technology is a double-edged sword, consistently presenting us with advantages and disadvantages. The increasing opportunities for knowledge gaining, high -productivities, efficiency and worldwide faster communications are the outcomes of cyber world. In other side, the various crimes emerging out of the internet are hacking, cyber terrorism, spamming, Trojan horse attacks, denial of service attacks, pornography, cyber stalking etc. However, the present article has the specific and minimum scope of focusing the issues in Cyber Stalking such as, integration of some definitions of cyber stalking, methods used to stalk the victim in online, stalkers' and victims' characteristics, magnitude of the problem in this information world, reason for stalking and in final to conclude with some suggestions for prevention of cyber stalking. On the whole, the aspiring aim of this article is to create a basic awareness on current situation and challenges.

Index terms: victim, digital forensics, open source tools, proprietary tools

References:

[1]. T. Abraham, “Event sequence mining to develop profiles for computer forensic investigation purposes” in ACSW frontiers '06: proceedings of the 2006 Australasian workshops on grid computing and research; 2006. p. 145-53.

[2]. R. Al-Zaidy, B.C.M. Fung, A.M. Youssef, F. Fortin, Mining criminal networks from unstructured text documents, Digit Investig 2012;8:147-60.

[3]. M. Alzaabi, A. Jones, T.A. Martin, An ontology-based forensic analysis tool, Digit Forensics, Secur Law 2013;(2013 Conference Suppl.):121-135.

[4]. D. Quick, K.R. Choo, Impacts of increasing volume of digital forensic data: A survey and future research challenges Digital Investigation 11 (2014) 273-294.

[5]. S. Garfinkel , Digital forensics research: The next 10 years , Digital Investigation (2010) S64 -S73.

[6]. S. Garfinkel, D. Cox, Finding and archiving the internet footprint, February 9-11 2009.

[7]. M.M. Nasreldin, M. El-Hennawy, H.K. Aslan and A. El-Hennawy, IJCSI International Journal of Computer Science Issues, Volume 12, Issue 1, No 1, January 2015.

[8]. P.S. Bogawar, K.K. Bhoyar, Email Mining: A Review, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 1, 2012.

[9]. P. Jungheum, C. Hyunji, L. Sangjin, Forensic analysis techniques for fragmented flash memory pages in smartphones, Digital Investigation 9 (2012) 109–118.

[10]. L, Pan, L.M. Batten, Robust performance testing for digital forensic tools, Digital Investigation 6(2009).

[11]. M. Meyers, M. Rogers, Computer forensics: the need for standardization and certification, International Journal of Digital Evidence 2004;3(2).

[12]. J.T. McDonald, Y.C. Kim, A. Yasinsac, Software issues in digital forensics. SIGOPS Operating Systems Review 2008; 42(3):29-40.