DAFTAR PUSTAKA

[1] L. M. Ibrahim, "Detection of Zeus Botnet in Computers Networks and Internet," 2012, pp. 84-89.

[2] A. Kurniawan and Y. Prayudi, "Teknik Live Forensics Pada Aktivitas Zeus *Malware* Untuk Mendukung Investigasi *Malware* Forensics," Hacking And Digital Forensics Expose, 2014.

[3] A. Flaglien, "Cross-computer *Malware* Detection in Digital Forensics," 2010.

[4] M. Brand, "Analysis Avoidance Techniques of Malicious Software," November, 2010.

[5] G. Kaur and B. Nagpal, "Exploring the *Malware* Analysis Landscape for Forensic Investigation," 2012, pp. 1-6.

[6] R. Karen, "Computer Forensics – We've Had an Incident, Who Do We Get to Investigate?," *SANS* , 2002.

[7] M. Lessing and B. v. Solms, Live Forensics Acquisition as Alternative to Traditional Forensic Processes, Johannesburg, 2008.

[8] H. Bintoro, "Analisis Kinerja Metode Live Forensics untuk Investigasi Random Acess Memory pada Sistem Operasi Microsoft Windows XP", Bandung: IT Telkom, 2012.

[9] T. Sukardi, "Forensik Komputer Prinsip-Prinsip Dasar," 2012, pp. 1-21.

[10] J. Sammons, The Basic of Digital Forensic "The Primer for Getting Started in Digital Forensic", USA: Syngress, 2012.

[11] J. Milletary, "*Citadel* Trojan *Malware* Analysis," Dell SecureWorks, 2012.

[12] P. Schwartz, "Setup and Analysis of ZeuS Banking Trojan V 2.0.8.9 w/ Volatility and LibVMI in a Virtualized Lab," 2014.

[13] H.-Y. Lock, "Using IOC (Indicators of Compromise) in *Malware* Forensics," *SANS Institute,* pp. 4-7, 2013.

[14] M. H. Ligh, A. Case, J. Levy and A. Walters, "The Art of Memory Forensics", Indiana: WILEY, 2014.