Daftar Pustaka

Ah, M. Z. (2009). Fakultas teknik program teknik komputer depok desember 2009.

Al-Dalky, R. (2014). *Accelerating Snort NIDS Using NetFPGA-bassed Bloom Filter*. Khalifa University of Science. *International Journal of Computer Science and Security. Retrived from:*

http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6906470&queryText=snort&newsearch=true

Al-Azhar, M. N. (2012). Digital Forensic : Panduan Praktis Investigasi Komputer. Salemba Infotek.

Cahyanto, T. A., & Prayudi, Y. (2014). Investigasi Forensika Pada Log Web Server untuk Menemukan Bukti Digital Terkait dengan Serangan Menggunakan Metode Hidden Markov Models. *Snati*, 15–19.

Charles, T., & Pollock, M. (2015). Digital forensic investigations at universities in South Africa. *2015 Second International Conference on Information Security and Cyber Forensics (InfoSec)*, 53–58. https://doi.org/10.1109/InfoSec.2015.7435506

Design & Deployment Of Testbed Based On ICMPv6 Flooding Attack. (2014), *64*(3), 795–801.

Franke, K. (n.d.). Computa (onal Forensics : Trends and Challenges in Applying Ar (ficial Intelligence Methodologies to Digital Forensics Impact of Computa * onal Science, 1–66.

Guide to Integrating Forensic Techniques into Incident Response. (n.d.).

Indra, A. (2010). Intrusion Detection Tools and Techniques – A Survey, *2*(6).

Introduction to Snort A . Sniffer Mode. (n.d.), 1–11.

Iswardani, A., & Riadi, I. (2016). Denial Of Service Log Analysis Using Density K-Means Method, *83*(2), 299–302.

Khamphakdee, N. (2014). Improving Intrusion Detection System Based on Snort Rules for Network Probe Attack Detection, 69–74.

Lanke, N. M., & Jacob, C. H. R. (2014). Detection of DDOS Attacks Using Snort Detection, *2*(9), 13–17.

Lipeng, D., Xingyuan, C., Huilin, T., & Wang, S. (2013). A Generation Framework of Multiple

Evasions on IDS. *2013 Third International Conference on Instrumentation, Measurement, Computer, Communication and Control*, 549–552. https://doi.org/10.1109/IMCCC.2013.124

McAfee Labs Threats Report. (2016), (March).

Nguyen, K., Tran, D., Ma, W., & Sharma, D. (2014). An Approach to Detect Network Attacks Applied for Network Forensics, 655–660.

Server, K., & Aktivitas, D. (2013). Implementasi honeypot untuk meningkatkan sistem keamanan server dari aktivitas serangan.

Shah, V., & Aggarwal, A. K. (2015). Heterogeneous fusion of IDS alerts for detecting DOS attacks. *Proceedings - 1st International Conference on Computing, Communication, Control and Automation, ICCUBEA 2015*, 153–158. https://doi.org/10.1109/ICCUBEA.2015.35

Sindhu, K. K., & Meshram, B. B. (2012). Digital Forensics and Cyber Crime Datamining, *2012*(July), 196–201.

Snort.org. 2016. Retrived form, http//:Snort.org.download.

Stiawan, D., Yaseen, A. L. A., Shakhatreh, I., Idris, M. Y., Bakar, K. A. B. U., & Abdullah, A. H. (2012). Intrusion Prevention System: A Survey, *40*(1), 44–54.

Studi, P., Informatika, T., Sains, F., Teknologi, D. A. N., & Kalijaga, U. I. N. S. (2015). Investigasi Forensik Jaringan Dari Serangan DDoS Menggunakan Metode Naive Bayes.

Suteva, N., Mileva, A., & Loleski, M. (2014). Computer Forensic Analisys of Some Web Attacks, 42–47.

Utami Putri, R., & Istiyanto, J. E. (2012). Analisis Forensik Jaringan Studi Kasus Serangan SQL Injection pada Server Universitas Gadjah Mada. *International Journal of Computer Science and Security*, *6*(2). Retrieved from http://journal.ugm.ac.id/index.php/ijccs/article/view/2157

Wireshark.org.2016. Retrived from, http//:Wireshark.org.download.