Daftar Pustaka

Arifah, D. A. (2011). Kasus Cybercrime Di Indonesia. *Jurnal Bisnis Dan Ekonomi*, *18*(2), 185–195.

Choudhary, R., & Khurana, M. (2017). Exploitation of PDF Reader Vulnerabilities using Metasploit Tool. *I.J Education and Management Engineering*, (September), 23–34. https://doi.org/10.5815/ijeme.2017.05.03

Gupta, H., & Kumar, R. (2015). Protection against penetration attacks using Metasploit. *2015 4th International Conference on Reliability, Infocom Technologies and Optimization: Trends and Future Directions, ICRITO 2015*, 2–5. https://doi.org/10.1109/ICRITO.2015.7359226

Hausknecht, K., Foit, D., & Burić, J. (2015). RAM data significance in digital forensics. *2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2015 - Proceedings*, (May), 1372–1375. https://doi.org/10.1109/MIPRO.2015.7160488

Hermaduanti, N., & Riadi, I. (2016). Automation framework for rogue access point mitigation in ieee 802.1X-based WLAN. *Journal of Theoretical and Applied Information Technology*, *93*(2), 287–296.

Ionut, A. (2015). An Introduction to Nmap with a Focus on Information Gathering.

Kurniawan, A., & Prayudi, Y. (2014). Teknik Live Forensics Pada Aktivitas Zeus Malware Untuk Mendukung Investigasi Malware Forensics. *HADFEX (Hacking and Digital Forensics Exposed)*, (JUNE 2014), 1–5.

Logen, S., Höfken, H., & Schuba, M. (2012). Simplifying RAM forensics: A GUI and extensions for the volatility framework. *Proceedings - 2012 7th International Conference on Availability, Reliability and Security, ARES 2012*, 620–624. https://doi.org/10.1109/ARES.2012.12

Mazdadi, M. I., Riadi, I., & Luthfi, A. (2017). Live Forensics on RouterOS using API Services to Investigate Network Attacks. *International Journal of Computer Science and Information Security (IJCSIS)*, *15*(2), 406–410.

Munif, A. (2013). *Sistem Operasi Teknologi Informasi Dan Komunikasi*. (Wismanu, Ed.).

Podile, A., Gottumukkala, K., & Sastry Pendyala, K. (2015). Digital Forensic Analysis Of Malware Infected Machine-Case Study. *International Journal of Scientific & Technology Research*, *4*(09). Retrieved from www.ijstr.org

Rochmadi, T. (2017). *Analisis Anti Forensik pada Portable Web Browser Mode Private*

Menggunakan Metode Live Forensik.

Thantilage, R., & Jeyamohan, N. (2017). A volatile memory analysis tool for retrieval of social media evidence in windows 10 OS based workstations. *2017 National Information Technology Conference (NITC)*, 86–88. https://doi.org/10.1109/NITC.2017.8285664

Thomas, S., Sherly, K. K., & Dija, S. (2013). Extraction of memory forensic artifacts from windows 7 RAM image. *2013 IEEE Conference on Information and Communication Technologies, ICT 2013*, (Ict), 937–942. https://doi.org/10.1109/CICT.2013.6558230

Timalsina, U., & Gurung, K. (2017). Metasploit Framework with Kali Linux, (April 2015), 0–8. https://doi.org/10.13140/RG.2.2.12377.93284

Umar, R., Yudhana, A., & Faiz, M. N. (2017). Analisis Kinerja Metode Live Forensics Untuk Investigasi Random Access Memory Pada Sistem Proprietary, (April).

Wadner, K. (2014). An Analysis of Meterpreter during Post-Exploitation.

Yudhistira, D. S. (2018). Metode Live Forensics Untuk Analisis Random Access Memory Pada Perangkat Laptop.