DAFTAR PUSTAKA

[1] S. Rheno Widianto and I. Abdullah Azzam, "Analisis Upaya Peretasan Web Application Firewall dan Notifikasi Serangan Menggunakan Bot Telegram pada Layanan Web Server," *Elektra*, vol. 3, no. 2, pp. 19–28, 2018.

[2] N. Provos, D. Mcnamee, P. Mavrommatis, K. Wang, and N. Modadugu, "The Ghost In The Browser Analysis of Web-based Malware," *Proc. first Conf. First Work. Hot Top. Underst. Botnets*, vol. 462, p. 4, 2007, doi: 10.1038/nature08624.

[3] A. Moser, C. Kruegel, and E. Kirda, "Exploring multiple execution paths for malware analysis," *Proc. - IEEE Symp. Secur. Priv.*, pp. 231–245, 2007, doi: 10.1109/SP.2007.17.

[4] B. Raharjo, "Sekilas Mengenai Forensik Digital," *J. Sosioteknologi*, vol. 12, no. 29, pp. 384–387, 2013, doi: 10.5614/sostek.itbj.2013.12.29.3.

[5] E. Akbal, F. Güneş, and A. Akbal, "Digital Forensic Analyses of Web Browser Records," *J. Softw.*, vol. 11, no. 7, pp. 631–637, 2016, doi: 10.17706/jsw.11.7.631-637.

[6] T. Rochmadi, "Live Forensik Untuk Analisa Anti Forensik Pada Web Browser Studi Kasus Browzar," *Indones. J. Bus. Intell.*, vol. 1, no. 1, p. 32, 2019, doi: 10.21927/ijubi.v1i1.878.

[7] T. A. Cahyanto, "Investigasi Forensika Pada Log Web Server untuk Menemukan Bukti Digital Terkait dengan Serangan Menggunakan Metode Hidden Markov Models," pp. 15–19, 2014.

[8] V. Sahfitri, M. Universitas, B. Darma, D. Universitas, and B. Darma, "Analisis Forensik Malware Pop-Up Ads Iklan Pada Platform Android," no. 03, 2015.

[9] G. Hendita, A. Kusuma, and Y. Fadhilah, "Analisis Forensik Digital E-Commerce pada Website Rental Mobil Menggunakan Metode NIST," *Pros. Semin. Nas. SISFOTEK*, vol. 3, no. 1, pp. 228–234, 2019.

[10] Y. A. Utomo *et al.*, "Membangun Sistem Analisis Malware Pada Aplikasi Android Dengan Metode Reverse Engineering Menggunakan Remnux," vol. 4, no. 3, pp. 2000–2012, 2018.

[11] D. R. Septiani, N. Widiyasono, and H. Mubarok, "Investigasi Serangan Malware Njrat Pada PC," *J. Edukasi dan Penelit. Inform.*, vol. 2, no. 2, pp. 123–128, 2016, doi: 10.26418/jp.v2i2.16736.

[12] L. Gitleman, *済無No Title No Title No Title*. 2014.

[13] S. Peisert, M. Bishop, S. Karin, and K. Marzullo, "Principles-Driven Forensic

Analysis," pp. 85–93, 2006.

[14] V. S. Pai, P. Druschel, and W. Zwaenepoel, "Flash: An efficient and portable Web server," *Proc. 1999 USENIX Annu. Tech. Conf.*, 1999.

[15] K. T. Dave, "Brute-Force Attack 'Seeking but Distressing,'" *Int. J. Innov. Eng. Technol.*, vol. 2, no. 3, pp. 75–77, 2013.

[16] N. Kumar, "Investigations in Brute Force Attack on Cellular Security Based on Des and Aes," *IJCEM Int. J. Comput. Eng. Manag.*, vol. 14, no. October, pp. 2230–7893, 2011, [Online]. Available: www.IJCEM.orgIJCEMwww.ijcem.org.

[17] S. T. Y, "Kali Linux - The BackTrack Successor," *Pentest Mag.*, vol. 2013, no. 16, p. 7, 2013.

[18] H. Loi and A. Olmsted, "Low-cost detection of backdoor malware," *2017 12th Int. Conf. Internet Technol. Secur. Trans. ICITST 2017*, no. August, pp. 197–198, 2018, doi: 10.23919/ICITST.2017.8356377.

[19] Q. Aini, I. Handayani, and C. A. Seto, "Content Management System Zpreneur in Support of Entrepreneurship Ilearning At Perguruan Tinggi Raharja," *CCIT J.*, vol. 8, no. 3, pp. 233–245, 2015, doi: 10.33050/ccit.v8i3.351.