DAFTAR PUSTAKA

[1] B. H. Jung, S. Il Bae, C. Choi, and E. G. Im, "Packer identification method based on byte sequences," *Concurr Comput*, vol. 32, no. 8, pp. 1–11, 2020, doi: 10.1002/cpe.5082.

[2] S. Sibi Chakkaravarthy, D. Sangeetha, and V. Vaidehi, "A Survey on malware analysis and mitigation techniques," *Comput Sci Rev*, vol. 32, pp. 1–23, 2019, doi: 10.1016/j.cosrev.2019.01.002.

[3] H. D. Menéndez, S. Bhattacharya, D. Clark, and E. T. Barr, "The arms race: Adversarial search defeats entropy used to detect malware," *Expert Syst Appl*, vol. 118, pp. 246–260, 2019, doi: 10.1016/j.eswa.2018.10.011.

[4] A. Mohanta and A. Saldanha, *Malware Analysis Lab Setup*. 2020. doi: 10.1007/978-1-4842-6193-4_2.

[5] Rhonda Johnson, "Creating Awareness of Anti- Forensic Deceptions Used by Cyber-Criminals," *eForensicMagazine*.

[6] H. Majed, H. N. Noura, and A. Chehab, "Overview of Digital Forensics and Anti-Forensics Techniques," *8th International Symposium on Digital Forensics and Security, ISDFS 2020*, 2020, doi: 10.1109/ISDFS49300.2020.9116399.

[7] X. Li, Z. Shan, F. Liu, Y. Chen, and Y. Hou, "A consistently-executing graph-based approach for malware packer identification," *IEEE Access*, vol. 7, pp. 51620–51629, 2019, doi: 10.1109/ACCESS.2019.2910268.

[8] A. H. Muhammad, G. Mandar, and M. Hamid, "Analisis Penggunaan Packer Perangkat Lunak Berbahaya(Malware) Menggunakan Teknik Reverse Engineering," *Jurnal Teknik Informatika (J-Tifa)*, vol. 5, no. 1, pp. 6–10, Mar. 2021, doi: 10.52046/j-tifa.v5i1.1400.

[9] S. S. Lad and A. C. Adamuthe, "Improved Deep Learning Model for Static PE Files Malware Detection and Classification," *International Journal of Computer Network and Information Security*, vol. 14, no. 2, pp. 14–26, Apr. 2022, doi: 10.5815/ijcnis.2022.02.02.

[10] J. Singh and J. Singh, "Challenges of Malware Analysis: Obfuscation Techniques."

[11] J. Kävrestad, *Fundamentals of Digital Forensics*. 2018. doi: 10.1007/978-3-319-96319-8.

[12] D. Paul Joseph and J. Norman, "An analysis of digital forensics in cyber security," in *Advances in Intelligent Systems and Computing*, Springer Verlag, 2019, pp. 701–708. doi: 10.1007/978-981-13-1580-0_67.

[13] M. A. Wani, W. A. Bhat, and A. Dehghantanha, "An analysis of anti-forensic capabilities of B-tree file system (Btrfs)," *Australian Journal of Forensic Sciences*, vol. 52, no. 4, pp. 371–386, 2020, doi: 10.1080/00450618.2018.1533038.

[14] H. Majed, H. N. Noura, and A. Chehab, “Overview of Digital Forensics and Anti-Forensics Techniques,” *8th International Symposium on Digital Forensics and Security, ISDFS 2020*, 2020, doi: 10.1109/ISDFS49300.2020.9116399.

[15] “Jurnal The Science and Military,” vol. 17, no. 1, p. 355, 2022.

[16] S. YusirwanS, Y. Prayudi, and I. Riadi, “Implementation of Malware Analysis using Static and Dynamic Analysis Method,” *Int J Comput Appl*, vol. 117, no. 6, pp. 11–15, May 2015, doi: 10.5120/20557-2943.

[17] Y. Ilhamdi and Y. N. Kunang, “ANALISIS MALWARE PADA SISTEM OPERASI WINDOWS MENGGUNAKAN TEKNIK FORENSIK,” *Bina Darma Conference on Computer Science*.

[18] N. Maleki, M. Bateni, and H. Rastegari, “An Improved Method for Packed Malware Detection using PE Header and Section Table Information,” *International Journal of Computer Network and Information Security*, vol. 11, no. 9, pp. 9–17, Sep. 2019, doi: 10.5815/ijcnis.2019.09.02.

[19] S. Malik Animesh Kumar Agrawal, “Multi Pronged Approach For Ransomware Analysis.” [Online]. Available: https://ssrn.com/abstract=4017025

[20] B. Denham and D. R. Thompson, “Ransomware and Malware Sandboxing Ransomware and Malware Sandboxing Ransomware and Malware Sandboxing,” 2022. [Online]. Available: https://scholarworks.uark.edu/csceuht/98

[21] “Building A Home Malware Analysis Lab.”

[22] Y. Dwi *et al.*, “Analisis Malware Menggunakan Metode Analisis Statis dan Dinamis untuk Pembuatan IOC Berdasarkan STIX Versi 2.1.”