DAFTAR PUSTAKA

Adenansi, R. and Novarina, L.A. (2017) ‘Malware dynamic’, *Jurnal of Education and Information Communication Technology*, 1(1), pp. 37–43.

Almarri, S. and Sant, P. (2014) ‘Optimised Malware Detection in Digital Forensics’, *International Journal of Network Security & Its Applications*, 6(1), pp. 01–15. doi:10.5121/ijnsa.2014.6101.

Bahtiar, F., Widiyasono, N. and Aldya, A.P. (2018) ‘Memory Volatile Forensik Untuk Deteksi Malware Menggunakan Algoritma Machine Learning’, *Jurnal Teknik Informatika dan Sistem Informasi*, 4, pp. 242–253.

Fadli, M.R. (2021) ‘Memahami desain metode penelitian kualitatif’, *Humanika*, 21(1), pp. 33–54. doi:10.21831/hum.v21i1.38075.

Hadi, S. (2016) ‘Pemeriksaan Keabsahan Data Penelitian Kualitatif Pada Skripsi [Examination of the Validity of Qualitative Research Data on Thesis]’, *Ilmu Pendidikan*, 22(1), pp. 21–22.

Nugroho, H.A. and Prayudi, Y. (2014) ‘Penggunaan Teknik Reverse Engineering Pada Malware Analysis Untuk Identifikasi Serangan’, *Knsi*, pp. 27–28.

Rathnayaka, C. and Jamdagni, A. (2017) ‘An efficient approach for advanced malware analysis using memory forensic technique’, *Proceedings - 16th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 11th IEEE International Conference on Big Data Science and Engineering and 14th IEEE International Conference on Embedded Software and Systems, Trustcom/BigDataSE/ICESS 2017*, pp. 1145–1150.

doi:10.1109/Trustcom/BigDataSE/ICESS.2017.365.

Septiani, D.R., Widiyasono, N. and Mubarok, H. (2016) 'Investigasi Serangan Malware Njrat Pada PC', *Jurnal Edukasi dan Penelitian Informatika (JEPIN)*, 2(2), pp. 123–128. doi:10.26418/jp.v2i2.16736.

Triantoro, A., Widiyasono, N. and Gunawan, R. (2021) 'Hack. exe Malware Analysis and Investigation Using Memory Forensics', *Ojs.Unud.Ac.Id*, 6(2), pp. 94–99. Available at: https://ojs.unud.ac.id/index.php/ijeet/article/download/IJEET.2021.v06.i01.p16/39911.

Uppal, D., Mehra, V. and Verma, V. (2014) 'Basic survey on Malware Analysis, Tools and Techniques', *International Journal on Computational Science & Applications*, 4(1), pp. 103–112. doi:10.5121/ijcsa.2014.4110.

YusirwanS, S., Prayudi, Y. and Riadi, I. (2015) 'Implementation of Malware Analysis using Static and Dynamic Analysis Method', *International Journal of Computer Applications*, 117(6), pp. 11–15. doi:10.5120/20557-2943.

Zalavadiya, N. and Sharma, D.P. (2017) 'A Methodology of Malware Analysis, Tools and Technique for *Windows* platform – RAT Analysis', *International Journal of Innovative Research in Computer and Communication Engineering*, 5(3), pp. 5042–5054. doi:10.15680/IJIRCCE.2017.

Adenansi, R. dan Novarina, L.A. (2017) "Malware dynamic," *Jurnal of Education and Information Communication Technology*, 1(1), hal. 37–43.

Almarri, S. dan Sant, P. (2014) "Optimised Malware Detection in Digital Forensics," *International Journal of Network Security & Its Applications*, 6(1),

hal. 01–15. Tersedia pada: https://doi.org/10.5121/ijnsa.2014.6101.

Bahtiar, F. *dkk* (2018) "Memory Volatile Forensik Untuk Deteksi Malware Menggunakan Algoritma Machine Learning," *Jurnal Teknik Informatika dan Sistem Informasi*, 4, hal. 242–253.

Cahyanto, T.A. dkk (2017) "Analisis dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis dan Malware Analisis Statis," *Justindo, Jurnal Sistem & Teknologi Informasi Indonesia*, 2(1), hal. 19–30.

Ciptohartono, C.C. dan Dermawan, M.K. (2019) "Pencegahan Viktimisasi Pencurian Data Pribadi," 3(2), hal. 157–169.

Fadli, M.R. (2021) "Memahami desain metode penelitian kualitatif," *Humanika*, 21(1), hal. 33–54. Tersedia pada: https://doi.org/10.21831/hum.v21i1.38075.

Hadi, S. (2016) "Pemeriksaan Keabsahan Data Penelitian Kualitatif Pada Skripsi [Examination of the Validity of Qualitative Research Data on Thesis]," *Ilmu Pendidikan*, 22(1), hal. 21–22.

Megira, S. dkk (2018) "Malware Analysis and Detection Using Reverse Engineering Technique," *Journal of Physics: Conference Series*, 1140(1). Tersedia pada: https://doi.org/10.1088/1742-6596/1140/1/012042.

Nugroho, H.A. dan Prayudi, Y. (2014) "Penggunaan Teknik Reverse Engineering Pada Malware Analysis Untuk Identifikasi Serangan," *Knsi*, hal. 27–28.

Rathnayaka, C. dan Jamdagni, A. (2017) "An efficient approach for advanced malware analysis using memory forensic technique," *Proceedings - 16th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 11th IEEE International Conference on Big Data Science*

and Engineering and 14th IEEE International Conference on Embedded Software and Systems, hal. 1145–1150. Tersedia pada: https://doi.org/10.1109/Trustcom/BigDataSE/ICESS.2017.365.

Septiani, D.R. dkk (2016) "Investigasi Serangan Malware Njrat Pada PC," *Jurnal Edukasi dan Penelitian Informatika (JEPIN)*, 2(2), hal. 123–128. Tersedia pada: https://doi.org/10.26418/jp.v2i2.16736.

Triantoro, A. dkk (2021) "Hack. exe Malware Analysis and Investigation Using Memory Forensics," *Ojs.Unud.Ac.Id*, 6(2), hal. 94–99. Tersedia pada: https://ojs.unud.ac.id/index.php/ijeet/article/download/IJEET.2021.v06.i01.p16/39911.

Uppal, D. dkk (2014) "Basic survey on Malware Analysis, Tools and Techniques," *International Journal on Computational Science & Applications*, 4(1), hal. 103–112. Tersedia pada: https://doi.org/10.5121/ijcsa.2014.4110.

Yusirwan, S. dkk (2015) "Implementation of Malware Analysis using Static and Dynamic Analysis Method," *International Journal of Computer Applications*, 117(6), hal. 11–15. Tersedia pada: https://doi.org/10.5120/20557-2943.

Zalavadiya, N. dan Sharma, D.P. (2017) "A Methodology of Malware Analysis, Tools and Technique for *Windows* platform – RAT Analysis," *International Journal of Innovative Research in Computer and Communication Engineering*, 5(3), hal. 5042–5054. Tersedia pada: https://doi.org/10.15680/IJIRCCE.2017.