DAFTAR PUSTAKA

Aditya, H. N., Widiyasono, N., & Rahmatulloh, A. (2024). Analisis Malware Aquvaprn.exe Untuk Investigasi Sistem Operasi Dengan Metode Memory Forensics. *Jurnal Teknik Informatika dan Sistem Informasi*, *10*(2), 161–172. https://doi.org/10.28932/jutisi.v10i2.6562

Amdani, R. T., Hafidudin, S. T., & Iqbal, M. (2021). ANALISIS DAN DETEKSI MALWARE POISON IVY DENGAN METODE MALWARE ANALISIS DINAMIS DAN MALWARE ANALISIS STATIS. *Jurnal Elektro Telekomunikasi Terapan*, *7*, 178–191.

Anugerah, C. A., Cahyani, N. D. W., & Jadied, E. M. (2024). Comparative Impact Analysis of Ransomware using Dynamic AnalysisTechniques on Windows 10. *International Journal on Information and Communication Technology (IJoICT)*, *10*(1), 90–99. https://doi.org/10.21108/ijoict.v10i1.940

Aslan, O., & Samet, R. (2020). A Comprehensive Review on Malware Detection Approaches. Dalam *IEEE Access* (Vol. 8, hlm. 6249–6271). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2019.2963724

Azzery, Y., Dwi Mulyanto, N., & Hidayat, T. (2022). MEMORY FORENSIC DEVELOPMENT AND CHALLENGES IN IDENTIFYING DIGITAL CRIME : A REVIEW. *TEKNOKOM*, *5*(1), 96–102. https://doi.org/10.31943/teknokom.v5i1.73

Damodaran, A., Di Troia, F., Corrado, V. A., Austin, T. H., & Stamp, M. (2022). A Comparison of Static, Dynamic, and Hybrid Analysis for Malware Detection. *arXiv*, 1–23. https://doi.org/10.1007/s11416-015-0261-z

Daniswara, D. A., Budiyono, A., & Almaarif, A. (2019). ANALISIS DETEKSI MALICIOUS ACTIVITY MENGGUNAKAN METODE ANALISIS MALWARE DINAMIS BERBASIS ANOMALI. *e-Proceeding of Engineering*, *6*, 7796–7803.

Das, P. P. (2022). Malware Analysis Using Memory Forensics. *International Journal for Research in Applied Science and Engineering Technology*, *10*(10), 488–495. https://doi.org/10.22214/ijraset.2022.47021

Devi, D. M., K.S., S., & Kumar, Rs. (2021). MALWARE ANALYSIS IN WINDOWS SYSTEM. Dalam *International Journal of Advanced Trends in Engineering* (Nomor 3). www.ijatest.org

Djenna, A., Bouridane, A., Rubab, S., & Marou, I. M. (2023). Artificial Intelligence-Based Malware Detection, Analysis, and Mitigation. *Symmetry*, *15*(3). https://doi.org/10.3390/sym15030677

Eze, A. O., & Chukwunonso, C. (2018). Malware Analysis and Mitigation in Information Preservation. *IOSR Journal of Computer Engineering (IOSR-JCE)*, *20*(4), 53–62. https://doi.org/10.9790/0661-2004015362

Gupta, S., Lu, F., Barlow, A., Raff, E., Ferraro, F., Matuszek, C., Nicholas, C., & Holt, J. (2024). Living off the Analyst: Harvesting Features from Yara Rules for Malware Detection. *2024 IEEE International Conference on Big Data (BigData)*. http://arxiv.org/abs/2411.18516

Jadhav, B., & Jadhav, M. (2024). Malware Detection and Analysis Using YARA Tool. *International Journal of Advanced Research in Science, Communication and Technology*, 161–166. https://doi.org/10.48175/IJARSCT-22623

Kusuma, G. H. A. (2023). Implementasi Volatility dalam Mengalanalisa Malware pada Memory Dump. *Journal of Informatics and Advanced Computing*, *4*, 36–43.

Mishra, A., & Bagade, P. (2023). MalDicom: A Memory Forensic Framework for Detecting Malicious Payload in DICOM Files. *arXiv*. http://arxiv.org/abs/2312.00483

Mujtaba, A., Zulfiqar, M., Azhar, M. U., Ali, S., Ali, A., & Khan, H. (2025). ML-based Fileless Malware Threats Analysis for the Detection of Cyber security

Attack based on Memory Forensics: A Survey. *The Asian Bulletin of Big Data Management*, *5*(1), 1–14. https://doi.org/10.62019/abbdm.v5i1.289

Naik, N., Jenkins, P., Savage, N., Yang, L., Boongoen, T., Iam-On, N., Naik, K., & Song, J. (2021). Embedded YARA rules: strengthening YARA rules utilising fuzzy hashing and fuzzy rules for malware analysis. *Complex and Intelligent Systems*, *7*(2), 687–702. https://doi.org/10.1007/s40747-020-00233-5

Naik, N., Jenkins, P., Savage, N., Yang, L., Naik, K., & Song, J. (2020). Embedding Fuzzy Rules with YARA Rules for Performance Optimisation of Malware Analysis. *2020 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*.

Nigam, P. (2020). Malware Detection and Signature Generation. *International Journal of Engineering Trends and Applications (IJETA)*, *7*, 15. www.ijetajournal.org

Patil, V., M, N. K., M, P. S., & Singh, A. (2025). Effectively Writing YARA Rules to Detect Malware. *International Journal for Research in Applied Science and Engineering Technology*, *13*(1), 1265–1273. https://doi.org/10.22214/ijraset.2025.66535

Penmatsa, R. K. V., Kalidindi, A., & Kumar Reddy Mallidi, S. (2020). Feature reduction and optimization of malware detection system using ant colony optimization and rough sets. *International Journal of Information Security and Privacy*, *14*(3), 95–114. https://doi.org/10.4018/IJISP.2020070106

Qomariah, N., Alwi, E. I., & Asis, M. A. (2023). Analisis Malware Hummingbad Dan Copycat Pada Android Menggunakan Metode Hybrid. *CyberSecurity dan Forensik Digital*, *6*(2), 39–47.

Rabia Mehmood. (2024). Live Memory Forensic: Capture and Analyzing Volatile Data. *International Journal for Electronic Crime Investigation*, *8*(3). https://doi.org/10.54692/ijeci.2024.0803208

Rudd, E. M., Rozsa, A., Günther, M., & Boult, T. E. (2017). A Survey of Stealth Malware Attacks, Mitigation Measures, and Steps Toward Autonomous Open World Solutions. Dalam *IEEE Communications Surveys and Tutorials* (Vol. 19, Nomor 2, hlm. 1145–1172). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/COMST.2016.2636078

Rughani, V., & Rughani, P. H. (2017). AUMFOR: Automated Memory Forensics for Malware Analysis. *Asian Journal of Engineering and Applied Technology*, *6*(2), 36–39. https://doi.org/10.51983/ajeat-2017.6.2.2781

Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. Dalam *Sensors* (Vol. 23, Nomor 16). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/s23167273

Sajan, P. P., Mohan, M., & Kuriakose, B. J. (2025). Yara-Based Emotet Malware Scanner-A Factual Analysis. Dalam *Communications on Applied Nonlinear Analysis* (Vol. 32, Nomor 2s). https://internationalpubls.com

Saurabh. (2018). Advance Malware Analysis Using Static and Dynamic Methodology. *2018 International Conference on Advanced Computation and Telecommunication (ICACAT)*.

Schelenz, L., & Pawelec, M. (2022). Information and Communication Technologies for Development (ICT4D) critique. *Information Technology for Development*, *28*(1), 165–188. https://doi.org/10.1080/02681102.2021.1937473

Shehab, R., s.alismail, A., Amin Almaiah, Dr. M., Alkhdour, Dr. T., AlWadi, Dr. B. M., & Alrawad, Dr. M. (2024). Assessment of Cybersecurity Risks and threats on Banking and Financial Services. *Journal of Internet Services and Information Security*, *14*(3), 167–190. https://doi.org/10.58346/jisis.2024.i3.010

Shree, R., Kant Shukla, A., Prakash Pandey, R., Shukla, V., & Bajpai, D. (2021). Memory forensic: Acquisition and analysis mechanism for operating systems. *Materials Today: Proceedings*, *51*, 254–260. https://doi.org/10.1016/j.matpr.2021.05.270

Sihwail, R., Omar, K., Ariffin, K. A. Z., & Al Afghani, S. (2019). Malware detection approach based on artifacts in memory image and dynamic analysis. *Applied Sciences (Switzerland)*, *9*(18). https://doi.org/10.3390/app9183680

Triantoro, A., Widiyasono, N., & Gunawan, R. (2021). Hack.exe Malware Analysis and Investigation Using Memory Forensics. *International Journal of Engineering and Emerging Technology*, *6*(2). https://any.run/

Yousuf, M. I., Anwer, I., Riasat, A., Zia, K. T., & Kim, S. (2023). Windows malware detection based on static analysis with multiple features. *PeerJ Computer Science*, *9*. https://doi.org/10.7717/PEERJ-CS.1319

Zalavadiya, N., & Sharma, 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), 5042–5054. https://doi.org/10.15680/IJIRCCE.2017