DAFTAR PUSTAKA

Annaby, M. H., Mahmoud, M. E., Abdusalam, H. A., Ayad, H. A., & Rushdi, M. A. (2024). On 3D encryption schemes based on chaotic permutations and rotations with geometric stability. *Optik*, *300*. https://doi.org/10.1016/j.ijleo.2024.171680

Asaad, R. R., & Saeed, V. A. (2022). A Cyber Security Threats, Vulnerability, Challenges and Proposed Solution. *Applied computing Journal*, 227–244. https://doi.org/10.52098/acj.202260

Berbecaru, D. G., & De Santo, M. (2026). Detecting TLS Protocol Anomalies Through Network Monitoring and Compliance Tools. *Future Internet*, *18*(1). https://doi.org/10.3390/fi18010062

Botacin, M., Galhardo Moia, V. H., Ceschin, F., Amaral Henriques, M. A., & Grégio, A. (2021). Understanding uses and misuses of similarity *hashing* functions for malware detection and family clustering in actual scenarios. *Forensic Science International: Digital Investigation*, *38*, 301220. https://doi.org/10.1016/j.fsidi.2021.301220

Burgetová, I., Matoušek, P., & Ryšavý, O. (2025). Towards identification of network applications in encrypted traffic. *Annals of Telecommunications*, *80*(11–12), 1015–1032. https://doi.org/10.1007/s12243-025-01114-z

Bushehri, A. S., Balboul, A., Belkhiri, A., Keivanpour, S., Nicolescu, G., & Dagenais, M. (2025). NOProbe: A NOP-based Dynamic Binary Instrumentation Framework Using Binary Rewriting on x86. *IEEE Transactions on Dependable and Secure Computing*. https://doi.org/10.1109/TDSC.2025.3641055

Fleming, M., & Olukoya, O. (2024). A temporal analysis and evaluation of *fuzzy hashing* algorithms for Android malware analysis. *Forensic Science International: Digital Investigation*, *49*, 301770. https://doi.org/10.1016/j.fsidi.2024.301770

Hassan, M., Haque, M. E., Tozal, M. E., Raghavan, V., & Agrawal, R. (2022). Intrusion Detection Using Payload Embeddings. *IEEE Access*, *10*, 4015–4030. https://doi.org/10.1109/ACCESS.2021.3139835

Heino, J., Hakkala, A., & Virtanen, S. (2023). Categorizing TLS traffic based on JA3 pre-hash values. *Procedia Computer Science*, *220*, 94–101. https://doi.org/10.1016/j.procs.2023.03.015

Jakobs, C., Mahr, A., Lambertz, M., Rybalka, M., & Plohmann, D. (2025). *Byte*wise approximate matching: Evaluating common scenarios for executable files. *Forensic Science International: Digital Investigation*, *53*, 301927. https://doi.org/10.1016/j.fsidi.2025.301927

Martín-Pérez, M., Rodríguez, R. J., & Balzarotti, D. (2021). Pre-processing memory dumps to improve similarity score of Windows modules. *Computers & Security*, *101*, 102119. https://doi.org/10.1016/j.cose.2020.102119

Mun, H. W., Huh, J. W., & Han, D. G. (2026). Fault injection attack against deep neural network-parameter exposure in random Bits-flip model. *Connection Science*, *38*(1). https://doi.org/10.1080/09540091.2026.2622884

Oh, C., Ha, J., & Roh, H. (2021a). A Survey on TLS-Encrypted Malware Network Traffic Analysis Applicable to Security Operations Centers. *Applied Sciences*, *12*(1), 155. https://doi.org/10.3390/app12010155

Oh, C., Ha, J., & Roh, H. (2021b). A Survey on TLS-Encrypted Malware Network Traffic Analysis Applicable to Security Operations Centers. *Applied Sciences*, *12*(1), 155. https://doi.org/10.3390/app12010155

Onieva, J. A., Pérez Jiménez, P., & López, J. (2024). Malware similarity and a new *fuzzy* hash: Compound Code Block Hash (CCBHash). *Computers & Security*, *142*, 103856. https://doi.org/10.1016/j.cose.2024.103856

Pan, Y., Lin, W., He, Y., & Zhu, Y. (2022). Coverage-guided differential testing of TLS implementations based on syntax mutation. *PLoS ONE*, *17*(1 1). https://doi.org/10.1371/journal.pone.0262176

Qureshi, S., Tunio, S., Akhtar, F., Wajahat, A., Nazir, A., & Ullah, F. (2021). Network Forensics: A Comprehensive Review of Tools and Techniques. *International Journal of Advanced Computer Science and Applications*, *12*(5). https://doi.org/10.14569/IJACSA.2021.01205103

Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. *ICISSP 2018 - Proceedings of the 4th International Conference on Information Systems Security and Privacy*, *2018-January*, 108–116. https://doi.org/10.5220/0006639801080116

Thomson, A., Maglaras, L., & Moradpoor, N. (2024). *A novel TLS-based Fingerprinting approach that combines feature expansion and similarity mapping*. http://arxiv.org/abs/2410.03817

Yu, L., Tao, J., Xu, Y., Sun, W., & Wang, Z. (2024). TLS fingerprint for encrypted malicious traffic detection with attributed graph kernel. *Computer Networks*, *247*, 110475. https://doi.org/10.1016/j.comnet.2024.110475

Zhang, Y., Huang, L., Gao, P., Song, F., Sun, J., & Dong, J. S. (2025). Verification of Bit-Flip Attacks against Quantized Neural Networks. *Proceedings of the ACM on Programming Languages*, *9*(OOPSLA1). https://doi.org/10.1145/3720471