

## DAFTAR PUSTAKA

- Akamai. (2019, Mei 15). *Akamai Blog | Bots Tampering with TLS to Avoid Detection*. <https://www.akamai.com/blog/security/bots-tampering-with-tls-to-avoid-detection>
- Akram, M., Barker, W. C., Clatterbuck, R., Dodson, D., Everhart, B., Gilbert, J., Haag, W., Johnson, B., Kapasouris, A., Lam, D., Pleasant, B., Raguso, M., Souppaya, M., Symington, S., Turner, P., & Wilson, C. (2020). *Securing web transactions TLS server certificate management*. <https://doi.org/10.6028/NIST.SP.1800-16>
- Anderson, B., & McGrew, D. (2016). Identifying encrypted malware traffic with contextual flow data. *AISec 2016 - Proceedings of the 2016 ACM Workshop on Artificial Intelligence and Security, co-located with CCS 2016*, 35–46. <https://doi.org/10.1145/2996758.2996768>
- Benjamin, D. (2020). *RFC 8701: Applying Generate Random Extensions And Sustain Extensibility (GREASE) to TLS Extensibility*. <https://www.rfc-editor.org/info/rfc8701>
- BlackBerry Research. (2023). *Global Threat Intelligence Report*.
- Breitinger, F., Baier, H., & White, D. (2014). On the database lookup problem of approximate matching. *Proceedings of the Digital Forensic Research Conference, DFRWS 2014 EU*, S1–S9. <https://doi.org/10.1016/j.diin.2014.03.001>
- Brzuska, C., Delignat-Lavaud, A., Egger, C., Fournet, C., Kohbrok, K., & Kohlweiss, M. (2022). *Key-schedule Security for the TLS 1.3 Standard*.
- Buruaga, J. S., Méndez, R. B., Brito, J. P., & Martin, V. (2025). Hybrid Quantum-Safe integration of TLS in SDN networks. *Computer Networks*, 267. <https://doi.org/10.1016/j.comnet.2025.111355>
- Chapman, P., & Evans, D. (2011). Automated black-box detection of side-channel vulnerabilities in web applications. *Proceedings of the ACM Conference on Computer and Communications Security*, 263–274. <https://doi.org/10.1145/2046707.2046737>
- Dowling, B., Fischlin, M., Günther, F., & Stebila, D. (2021). A Cryptographic Analysis of the TLS 1.3 Handshake Protocol. *Journal of Cryptology*, 34(4). <https://doi.org/10.1007/s00145-021-09384-1>
- Frolov, S., & Wustrow, E. (2019). The use of TLS in Censorship Circumvention. *26th Annual Network and Distributed System Security Symposium, NDSS 2019*. <https://doi.org/10.14722/ndss.2019.23511>
- Han, J., Kamber, M., & Pei, J. (2012). *Data Mining Data Mining Concepts and Techniques Third Edition*.
- Heino, J., Hakkala, A., & Virtanen, S. (2022). Study of methods for endpoint aware inspection in a next generation firewall. *Cybersecurity*, 5(1). <https://doi.org/10.1186/s42400-022-00127-8>
- John Althouse. (2017). *TLS Fingerprinting with JA3 and JA3S - Salesforce Engineering Blog*. <https://engineering.salesforce.com/tls-fingerprinting-with-ja3-and-ja3s-247362855967/>

- Jurafsky, D., & Martin, J. H. (2026). *Speech and Language Processing An Introduction to Natural Language Processing, Computational Linguistics, and Speech Recognition with Language Models Third Edition draft*.
- Kaddouri, M., Bouhdadi, M., Kaddouri, Z., Guerchi, D., & Echandouri, B. (2019). New Transport Layer Security using Metaheuristics and New Key Exchange Protocol. Dalam *IJACSA) International Journal of Advanced Computer Science and Applications* (Vol. 10, Nomor 8). [www.ijacsa.thesai.org](http://www.ijacsa.thesai.org)
- Kalka, M., & Kirejczyk, M. (2024). *A Comprehensive Review of TLSNotary Protocol*. <http://arxiv.org/abs/2409.17670>
- Kornblum, J. (2006). Identifying almost identical files using context triggered piecewise hashing. *Digital Investigation*, 3(SUPPL.), 91–97. <https://doi.org/10.1016/j.diin.2006.06.015>
- Kotzias, P., Paterson, K. G., Razaghpanah, A., Vallina-Rodriguez, N., Amann, J., & Caballero, J. (2018). Coming of age: A longitudinal study of TLS deployment. *Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC*, 415–428. <https://doi.org/10.1145/3278532.3278568>
- Levenshtein. (1965). *Binary Codes Capable of Correcting Deletions, Insertions and Reversals*.
- Liu, Z. (2022). *DeepTLS: comprehensive and high-performance feature extraction for encrypted traffic*. <http://arxiv.org/abs/2208.03862>
- McKay, K. A., & Cooper, D. A. (2019). *Guidelines for the selection, configuration, and use of Transport Layer Security (TLS) implementations*. <https://doi.org/10.6028/NIST.SP.800-52r2>
- Oliver, J., Cheng, C., & Chen, Y. (2013). *TLSH-A Locality Sensitive Hash*. [https://www.academia.edu/9768744/On\\_Attacking\\_Locality\\_Sensitive\\_Hashes\\_and\\_Similarity\\_Digests](https://www.academia.edu/9768744/On_Attacking_Locality_Sensitive_Hashes_and_Similarity_Digests)
- Rescorla. (2018). *The Transport Layer Security (TLS) Protocol Version 1.3*.
- Roussev, V. (2010). *Chapter 8 DATA FINGERPRINTING WITH SIMILARITY DIGESTS*.
- Schulz, K. U., & Mihov, S. (2003). Fast string correction with Levenshtein automata. *International Journal on Document Analysis and Recognition*, 5(1), 67–85. <https://doi.org/10.1007/s10032-002-0082-8>
- Sikeridis, D., Kampanakis, P., & Devetsikiotis, M. (2020). Post-Quantum Authentication in TLS 1.3: A Performance Study. *27th Annual Network and Distributed System Security Symposium, NDSS 2020*. <https://doi.org/10.14722/ndss.2020.24203>
- Sokolova, M., & Lapalme, G. (2009). A systematic analysis of performance measures for classification tasks. *Information Processing and Management*, 45(4), 427–437. <https://doi.org/10.1016/j.ipm.2009.03.002>
- Wickramasinghe, N., Shaghaghi, A., Tsudik, G., & Jha, S. (2025). *SoK: Decoding the Enigma of Encrypted Network Traffic Classifiers*. <https://doi.org/10.1109/SP61157.2025.00165>