REFERENCES

Asad, H., Adhikari, S., & Gashi, I. (2024). "A perspective–retrospective analysis of diversity in signature-based open-source network intrusion detection systems," *International Journal of Information Security*, vol. 23, no. 2, pp. 1331–1346. Available at: https://doi.org/10.1007/s10207-023-00794-9.

Balfanz, D., Bhargavan, K., Cheval, V., & Wood, C.A. (2019). "The Case for Encrypted Client Hello: A New Approach to Privacy in TLS Handshakes," presented at the *ACM Conference on Computer and Communications Security (CCS)*, Los Angeles, CA, USA.

Benjamin, D. (2020). *Applying Generate Random Extensions And Sustain Extensibility (GREASE) to TLS Extensibility*, RFC 8701, Internet Engineering Task Force. Available at: https://doi.org/10.17487/RFC8701.

Chai, Z., Ghafari, A., & Houmansadr, A. (2019). "On the Importance of Encrypted-SNI (ESNI) to Censorship Circumvention," *9th USENIX Workshop on Free and Open Communications on the Internet (FOCI 19)*, Santa Clara, CA. USENIX Association.

Cohen, J. (1988). *Statistical Power Analysis for the Behavioral Sciences*. 2nd edn. Lawrence Erlbaum Associates.

Dierks, T. & Rescorla, E. (2008). *The Transport Layer Security (TLS) Protocol Version 1.2*, RFC 5246, Internet Engineering Task Force. Available at: https://doi.org/10.17487/RFC5246.

Dodiya, B. & Singh, U.K. (2022). "Malicious traffic analysis using Wireshark by collection of indicators of compromise," *International Journal of Computer Applications*, vol. 183, no. 53, pp. 1–6. Available at: https://www.ijcaonline.org/archives/volume183/number53/32286-2022921876/ (Accessed: 20 October 2024).

Dong, H., Zhang, Y., Lee, H., Huque, S., & Sun, Y. (2024). "Deciphering the Digital Veil: Exploring the Ecosystem of DNS HTTPS Resource Records," *arXiv*, 22 March.

"Encrypted DNS: The good, the bad and the moot." (n.d.). Available at: https://doi.org/10.12968/S1361-3723(22)70572-6.

Efron, B. & Tibshirani, R. J. (1994). *An Introduction to the Bootstrap*. Chapman & Hall/CRC.

Glass, E. B. (1949). "Note on rank biserial correlation," *Educational and Psychological Measurement*, vol. 9, no. 3, pp. 407–410. Available at: https://doi.org/10.1177/001316444900900310.

Hoang, N.P., Polychronakis, M., & Gill, P. (2022). "Measuring the Accessibility of Domain Name Encryption and Its Impact on Internet Filtering," *arXiv*, 1 February.

"HTTPS encryption on the web – Google Transparency Report." (n.d.). Available at: https://transparencyreport.google.com/https/overview?hl=en (Accessed: 28 April 2024).

Huitema, C. (2020). *Issues and Requirements for Server Name Identification (SNI) Encryption in TLS*, RFC 8744, RFC Editor. Available at: https://doi.org/10.17487/RFC8744.

Huitema, C. & Kuehlewind, M. (2020). "Encrypted Client Hello: A New Approach to Privacy in TLS Handshakes," in *Proceedings of the ACM Conference on Computer and Communications Security*.

Jain, G. & Anubha. (2021). "Application of SNORT and Wireshark in Network Traffic Analysis," *IOP Conference Series: Materials Science and Engineering*, vol. 1119, no. 1, p. 012007. Available at: https://doi.org/10.1088/1757-899X/1119/1/012007.

Kampourakis, V., Kambourakis, G., Chatzoglou, E., & Zaroliagis, C. (2022). "Revisiting man-in-the-middle attacks against HTTPS," *Network Security*, vol. 2022, no. 3, pp. S1353-4858(22)70028–1. Available at: https://doi.org/10.12968/S1353-4858(22)70028-1.

Khandkar, V.S., Hanawal, M.K., & Kulkarni, S.G. (2022). "Challenges in Adapting ECH in TLS for Privacy Enhancement over the Internet," *arXiv*, 5 July.

Kumar, V. & Sangwan, D.O.P. (2012). "Signature Based Intrusion Detection System Using SNORT," *International Journal of Computer Applications*.

Levene, H. (1960). "Robust tests for equality of variances," in *Contributions to Probability and Statistics: Essays in Honor of Harold Hotelling*. Stanford: Stanford University Press, pp. 278–292.

"Let's Encrypt Stats - Let's Encrypt." (n.d.). Available at: https://letsencrypt.org/stats/ (Accessed: 28 April 2024).

Li, F., Razaghpanah, A., Kakhki, A.M., Niaki, A.A., Choffnes, D., Gill, P., & Mislove, A. (2017). "lib•erate, (n): a library for exposing (traffic-classification) rules and avoiding them efficiently," in *Proceedings of the 2017 Internet Measurement Conference*, ACM, London, United Kingdom, pp. 128–141. Available at: https://doi.org/10.1145/3131365.3131376.

Mann, H. B. & Whitney, D. R. (1947). "On a test of whether one of two random variables is stochastically larger than the other," *The Annals of Mathematical Statistics*, vol. 18, no. 1, pp. 50–60. Available at: https://doi.org/10.1214/aoms/1177730491.

Nguyen, V., Mohammed, D., Omar, M., & Dean, P. (2020). "Net Neutrality Around the Globe: A Survey," in *2020 3rd International Conference on Information and Computer Technologies (ICICT)*, IEEE, San Jose, CA, USA, pp. 480–488. Available at: https://doi.org/10.1109/ICICT50521.2020.00083.

Nir, Y., Salz, R., & Sullivan, N. (2024). "Transport Layer Security (TLS) Parameters." Available at: https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml (Accessed: 29 April 2024).

Nir, Y., Salz, R., & Sullivan, N. (n.d.). "Transport Layer Security (TLS) Extensions." Available at: https://www.iana.org/assignments/tls-extensiontype-values/tls-extensiontype-values.xhtml (Accessed: 29 April 2024).

Neyman, J. (1937). "Outline of a theory of statistical estimation based on the classical theory of probability," *Philosophical Transactions of the Royal Society of London. Series A, Mathematical and Physical Sciences*, vol. 236, no. 767, pp. 333–380. Available at: https://doi.org/10.1098/rsta.1937.0005.

Rescorla, E. & Modadugu, N. (2018). *The Transport Layer Security (TLS) Protocol Version 1.3*, RFC 8446, Internet Engineering Task Force. Available at: https://doi.org/10.17487/RFC8446.

Rescorla, E. (2018). *The Transport Layer Security (TLS) Protocol Version 1.3*, RFC 8446, Internet Engineering Task Force. Available at: https://doi.org/10.17487/RFC8446.

Rescorla, E., Oku, K., Sullivan, N., & Wood, C.A. (2022). *TLS Encrypted Client Hello*, Internet Draft no. draft-ietf-tls-esni-14, Internet Engineering Task Force.

Sanders, C. (n.d.). *Practical Packet Analysis, 3rd Edition [Book]*. Available at: https://www.oreilly.com/library/view/practical-packet-analysis/9781492020356/ (Accessed: 30 April 2024).

Schwartz, B.M., Bishop, M., & Nygren, E. (2023). *Service Binding and Parameter Specification via the DNS (SVCB and HTTPS Resource Records*, RFC 9460, Internet Engineering Task Force. Available at: https://doi.org/10.17487/RFC9460.

Shamsimukhametov, D., Kurapov, A., Liubogoshchev, M., & Khorov, E. (2022). "Is Encrypted ClientHello a Challenge for Traffic Classification?" *IEEE Access*, vol. 10, pp. 77883–77897. Available at: https://doi.org/10.1109/ACCESS.2022.3191431.

Shapiro, S. S. & Wilk, M. B. (1965). "An analysis of variance test for normality (complete samples)," *Biometrika*, vol. 52, no. 3/4, pp. 591–611. Available at: https://doi.org/10.2307/2333709.

"Snort Frequently Asked Questions." (n.d.). Available at: https://www.snort.org/faq (Accessed: 30 April 2024).

Student (1908). "The probable error of a mean," *Biometrika*, vol. 6, no. 1, pp. 1–25. Available at: https://doi.org/10.2307/2331554.

Tsiatsikas, Z., Karopoulos, G., & Kambourakis, G. (2023). "Measuring the Adoption of TLS Encrypted Client Hello Extension and Its Forebear in the Wild," in Katsikas, S., Cuppens, F., Kalloniatis, C., Mylopoulos, J., Pallas, F., Pohle, J., & Sasse, M.A., et al. (Eds.), *Computer Security. ESORICS 2022 International Workshops*, vol. 13785, Springer International Publishing, Cham, pp. 177–190. Available at: https://doi.org/10.1007/978-3-031-25460.

Tsiknas, K., Taketzis, D., Demertzis, K., & Skianis, C. (2021). "Cyber Threats to Industrial IoT: A Survey," 5 February. Available at: https://doi.org/10.20944/preprints202102.0148.v1.

Yu, S. & Won, Y. (2022). "A survey of methods for encrypted network traffic fingerprinting," *Mathematical Biosciences and Engineering*, vol. 20, no. 2, pp. 2183–2202. Available at: https://doi.org/10.3934/mbe.2023101.