DAFTAR PUSTAKA

Afonso, V. M., de Amorim, M. F., Grégio, A. R., Junquera, G. B., & de Geus, P. L. (2015). Identifying Android Malware Using Dynamically Obtained Features. *Journal of Computer Virology and Hacking Techniques*, 9-17.

Alamsyah, R. S. (2016). Analisis Deteksi Spyware pada Platform Android.

Alghamdi, R., Alfalqi, K., & Waqdan, M. (2015). Android Platform Malware Analysis. *(IJACSA) International Journal of Advanced Computer Science and Applications*, 140-146.

Almarri, S., & Sant, P. (2014). Optimised Malware Detection in Digital Forensics. *International Journal of Network Security & Its Applications (IJNSA),* 1-15.

Alzaylaee, M. K., Yerima, S. Y., & Sezer, S. (2017). EMULATOR vs REAL PHONE: Android Malware Detection Using Machine Learning. *Centre for Secure Information Technologies (CSIT)*, 65-72.

Android. (2019, 2 15). *Manifest.permission | Android Developers*. Retrieved from Android Developers: https://developer.android.com/reference/android/Manifest.permission.html

Bacci, A., Bartoli, A., Martinelli, F., Medvet, E., Mercaldo, F., & Visaggio, C. A. (2013). Impact of Code Obfuscation on Android Malware Detection based on Static and Dynamic Analysis Machine Learning-based malware detection.

Gadhiya, S., & Bhavsar, K. (2013). Techniques for Malware Analysis. *International Journal of Advanced Research in Computer Science and Software Engineering*, 972-975.

Herlambang, S. (2018). *Deteksi Malware Android Berdasarkan System Call Menggunakan Algoritma Support Vector Machine*. Malang: UMM.

Infoblox. (2018). *Infoblox Administrator Guide*. California: Infoblox Technical Publication.

Kirat, D., & Vigna, G. (2015). MalGene : Automatic Extraction of Malware Analysis Evasion Signature. *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security - CCS '15*, 769-780.

Kunang, Y. N. (2014). Analisis Forensik Malware pada Platform Android. *Konferensi Nasional Ilmu Komputer (KONIK)*, 141-148.

Lengyel, T. K., Maresca, S., Payne, B. D., Webster, G. D., Vogl, S., & Kiayias, A. (2014). Scalability, Fidelity and Stealth in the DRAKVUF Dynamic

Malware Analysis System. *Proceedings of the 30th Annual Computer Security Applications Conference on - ACSAC '14*, 386-395.

Maulana, A. F. (2018). Reverse Engineering dan Analisis Malware Ahmyth pada Perangkat Android.

McAfee Inc. (2018). *McAfee Mobile Threat Report Q1, 2018.* California: McAfee Inc.

Meier, R., & Lake, I. (2018). *Professional Android, 4th Edition.* Indianapolis: John Wiley & Sons, Inc.

Nakamura, M., & Gargenta, M. (2014). *Learning Android, 2nd Edition.* California: O'Reilly Media, Inc.

StatCounter. (2018). *Mobile Operating System Market Share Worldwide*. Retrieved from StatCounter Global Stats: http://gs.statcounter.com/os-market-share/mobile/worldwide

Wandera. (2017). *The current state of mobile malware.* San Francisco: Wandera.

Wardhana, R. S. (2015). Analisa Hybrid untuk Sistem Deteksi Malware Otomatis dengan Support Vector Model Classifier. 1-10.

Yuan, Z., Lu, Y., Wang, Z., & Xue, Y. (2014). Droid-Sec : Deep Learning in Android Malware Detection. *Sigcomm 2014*, 371-372.

Zalavadiya, N., & Sharma, P. D. (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*(2), 5042-5054.