UJI PERFORMA ANALISIS STATIS DAN DINAMIS DALAM INVESTIGASI FORENSIK MALWARE PADA *PLATFORM* ANDROID

SKRIPSI

UIN SUNAN AMPEL
S U R A B A Y A

Disusun Oleh :

MUHAMMAD SHOFIUDIN
09020620036

PROGRAM STUDI SISTEM INFORMASI
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SUNAN AMPEL
SURABAYA
2024

LEMBAR PERNYATAAN KEASLIAN

Saya yang bertanda tangan di bawah ini,

Nama	:	Muhammad Shofiudin
NIM	:	09020620036
Program Studi	:	Sistem Informasi
Angkatan	:	2020

Menyatakan bahwa saya tidak melakukan plagiasi dalam penulisan skripsi saya yang berjudul : "UJI PERFORMA ANALISIS STATIS DAN DINAMIS DALAM INVESTIGASI FORENSIK *MALWARE* PADA *PLATFORM* ANDROID". Apabila suatu saat nanti terbukti saya melakukan tindakan plagiat, maka saya bersedia menerima sanksi yang telah ditetapkan.

Demikian pernyataan keasLian ini saya buat dengan sebenar-benarnya.

Surabaya, 05 Juni 2024

Yang menyatakan,

(Muhammad Shofiudin)

NIM. 09020620036

LEMBAR PERSETUJUAN PEMBIMBING

Skripsi oleh

NAMA	:	MUHAMMAD SHOFIUDIN
NIM	:	09020620036
JUDUL	:	UJI PERFORMA ANALISIS STATIS DAN DINAMIS DALAM INVESTIGASI FORENSIK *MALWARE* PADA *PLATFORM* ANDROID

ini telah diperiksa dan disetujui untuk diujikan.

Surabaya, 05 Juni 2024

Dosen Pembimbing 1	Dosen Pembimbing 2
Muhammad Andik Izzuddin, M.T	Mujib Ridwan, S.Kom., M.T
NIP. 198403072014031001	NIP. 198604272014031004

LEMBAR PENGESAHAN TIM PENGUJI SKRIPSI

Skripsi Muhammad Shofiudin ini telah dipertahankan
di depan tim penguji skripsi
di Surabaya, 11 Juni 2024

Mengesahkan,
Dewan Penguji

Dosen Penguji I

Dr. Achmad Teguh Wibowo, MT., MTCNA
NIP. 198810262014031003

Dosen Penguji II

Noor Wahyudi, M.Kom
NIP. 198403232014031002

Dosen Penguji III

Muhammad Andik Izzuddin, M.T
NIP. 198403072014031001

Dosen Penguji IV

Mujib Ridwan, S.Kom, M.T
NIP. 198604272014031004

Mengetahui,
Dekan Fakultas Sains dan Teknologi
UIN Sunan Ampel Surabaya

Dr. Saepul Hamdani, M.Pd
NIP. 196507312000031002

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN AMPEL SURABAYA
PERPUSTAKAAN
Jl. Jend. A. Yani 117 Surabaya 60237 Telp. 031-8431972 Fax.031-8413300
E-Mail: perpus@uinsby.ac.id

LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI
KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademika UIN Sunan Ampel Surabaya, yang bertanda tangan di bawah ini, saya:

Nama	:	MUHAMMAD SHOFIUDIN
NIM	:	09020620036
Fakultas/Jurusan	:	SAINS DAN TEKNOLOGI / SISTEM INFORMASI
E-mail address	:	shofiudinmuh@gmail.com

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Perpustakaan UIN Sunan Ampel Surabaya, Hak Bebas Royalti Non-Eksklusif atas karya ilmiah :

■ Skripsi ☐ Tesis ☐ Desertasi ☐ Lain-lain (.....)

yang berjudul :

UJI PERFORMA ANALISIS STATIS DAN DINAMIS DALAM INVESTIGASI FORENSIK *MALWARE* PADA *PLATFORM* ANDROID

beserta perangkat yang diperlukan (bila ada). Dengan Hak Bebas Royalti Non-Ekslusif ini Perpustakaan UIN Sunan Ampel Surabaya berhak menyimpan, mengalih-media/format-kan, mengelolanya dalam bentuk pangkalan data (database), mendistribusikannya, dan menampilkan/mempublikasikannya di Internet atau media lain secara ***fulltext*** untuk kepentingan akademis tanpa perlu meminta ijin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan atau penerbit yang bersangkutan.

Saya bersedia untuk menanggung secara pribadi, tanpa melibatkan pihak Perpustakaan UIN Sunan Ampel Surabaya, segala bentuk tuntutan hukum yang timbul atas pelanggaran Hak Cipta dalam karya ilmiah saya ini.

Demikian pernyataan ini yang saya buat dengan sebenarnya.

Surabaya, 22 Juni 2024

Penulis

(MUHAMMAD SHOFIUDIN)

ABSTRAK

UJI PERFORMA ANALISIS STATIS DAN DINAMIS DALAM INVESTIGASI FORENSIK *MALWARE* PADA PLATFORM ANDROID

Oleh :

Muhammad Shofiudin

Perkembangan teknologi informasi yang semakin pesat membawa dampak yang sangat signifikan. Semakin canggih inovasi yang dilakukan, semakin besar pula ancaman yang muncul. Total serangan *malware* yang terjadi pada tahun 2023 tercatat sebanyak 5,46 miliyar yang mana pada tahun sebelumnya sebanyak 5,38 miliyar. Data ini menunjukkan bahwa serangan *malware* terus mengalami peningkatan, termasuk pula di Indonesia. Penelitian ini akan melakukan uji performa metode analisis statis dan dinamis untuk menemukan metode yang lebih efektif dalam analisis *malware* sebagai bentuk langkah penanggulanan serangan yang dilakukan. Penelitian menggunakan *software* MobSF sebagai alat analisis statis dan VirusTotal sebagai alat analisis dinamis dengan menggunakan kerangka kerja yang disediakan oleh NIST *Special Publication* 800-83. Sampel *malware* yang digunakan adalah file Cek Foto Paket JNE Express.apk. Hasil dari investigasi menggunakan NIST SP 800-83 menunjukkan bahwa hasil yang diperoleh analisis dinamis dapat memberikan informasi yang lebih detail tentang perilaku *malware.* Dari perbandingan hasil yang diperoleh, analisis dinamis memperoleh 16 temuan terkait informasi *malware.* Sedangkan analisis statis memperoleh 11 temuan terkait informasi *malware.* Analisis dinamis memiliki keunggulan dalam kemampuan untuk mengidentifikasi *malware* yang bersembunyi, memberikan informasi lebih rinci, dan memiliki tingkat kesulitan yang lebih rendah. Sedangkan analisis statis memiliki keunggulan dalam keamanan sistem ketika proses analisis dilakukan.

Kata kunci : Uji Performa, Analisis Statis, Analisis Dinamis, *Malware,* MobSF, VirusTotal, NIST SP 800-83

ABSTRACT

STATIC AND DYNAMIC ANALYSIS PERFORMANCE TEST IN MALWARE FORENSIC INVESTIGATION ON THE ANDROID PALTFORM

By:

Muhammad Shofiudin

The rapid development of information technology has had a very significant impact. The more advanced the innovations, the greater the threats that arise. The total number of malware attacks in 2023 was recorded at 5.46 billion, compared to 5.38 billion in the previous year. This data indicates that malware attacks continue to increase, including in Indonesia. This research aims to test the performance of static and dynamic analysis methods to find the most effective method for malware analysis as a step towards mitigating these attacks. The research uses MobSF software for static analysis and VirusTotal for dynamic analysis, following the framework provided by NIST Special Publication 800-83. The malware sample used is the Cek Foto Paket JNE Express.apk file. The results of the investigation using NIST SP 800-83 show that dynamic analysis provides more detailed information about malware behavior. From the comparison of the results obtained, dynamic analysis yielded 16 findings related to malware information, while static analysis yielded 11 findings. Dynamic analysis has advantages in identifying hidden malware, providing more detailed information, and having a lower level of difficulty. On the other hand, static analysis has advantages in system security during the analysis process.

Keywords : Performance Test, Static Analysis, Dynamic Analysis, Malware, MobSF, VirusTotal, NIST SP 800-83

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

DAFTAR PUSTAKA

A. Ofori, Y. (2020) 'Digital Forensics Investigation Jurisprudence: Issues Of Admissibility Of Digital Evidence', *Journal of Forensic, Legal & Investigative Sciences*, 6(1), pp. 1–8. Available at: https://doi.org/10.24966/FLIS-733X/100045.

Abdul Kadir, A.F., Habibi Lashkari, A. and Daghmehchi Firoozjaei, M. (2024) 'Android Operating System', in *Understanding Cybersecurity on Smartphones: Challenges, Strategies, and Trends*. Cham: Springer Nature Switzerland, pp. 25–42. Available at: https://doi.org/10.1007/978-3-031-48865-8_2.

Ahdiat, A. (2023) '67% Penduduk Indonesia Punya Handphone pada 2022', *Databoks*, 8 March.

Akhtar, M.S. and Feng, T. (2023) 'Evaluation of Machine Learning Algorithms for Malware Detection', *Sensors*, 23(2), p. 946. Available at: https://doi.org/10.3390/s23020946.

Alenezi, M. and Almomani, I. (2017) 'Abusing Android permissions: A security perspective', in *2017 IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT)*. *2017 IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT)*, Aqaba: IEEE, pp. 1–6. Available at: https://doi.org/10.1109/AEECT.2017.8257772.

Alenezi, M.N. *et al.* (2022) 'Evolution of Malware Threats and Techniques: a Review', *International Journal of Communication Networks and Information Security (IJCNIS)*, 12(3). Available at: https://doi.org/10.17762/ijcnis.v12i3.4723.

Ali, M. *et al.* (2022) 'Profile Hidden Markov Model Malware Detection and API Call Obfuscation':, in *Proceedings of the 8th International Conference on Information Systems Security and Privacy*. *6th International Special Session on FORmal methods for Security Engineering*, Vienna, Austria: SCITEPRESS - Science and Technology Publications, pp. 688–695. Available at: https://doi.org/10.5220/0011005800003120.

Almomani, I.M. and Khayer, A.A. (2020) 'A Comprehensive Analysis of the Android Permissions System', *IEEE Access*, 8, pp. 216671–216688. Available at: https://doi.org/10.1109/ACCESS.2020.3041432.

Alsharabi, N., Alshammari, M.F. and Alharbi, Y. (2023) 'Analysis of Ransomware Using Reverse Engineering Techniques to Develop Effective Countermeasures', *Journal of Advances in Information Technology*, 14(2), pp. 284–294. Available at: https://doi.org/10.12720/jait.14.2.284-294.

Aravazhi, M.S. (2020) 'Understanding Cyber Crime and Cyber Laundering: Threat and Solution', *EPRA International Journal of Research & Development (IJRD)* [Preprint].

Cahyanto, T.A., Wahanggara, V. and Ramadana, D. (2017) 'Analisis dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis dan Malware Analisis Statis', 2(1).

Chen, S. *et al.* (2016) 'StormDroid: A Streaminglized Machine Learning-Based System for Detecting Android Malware', *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*. Xi'an, China:

Association for Computing Machinery. Available at: https://doi.org/10.1145/2897845.2897860.

Cichonski, P. *et al.* (2012) *Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology*. NIST SP 800-61r2. National Institute of Standards and Technology, p. NIST SP 800-61r2. Available at: https://doi.org/10.6028/NIST.SP.800-61r2.

Coban, O. and Ozel, S. (2019) 'Adapting Text Categorization for Manifest based Android Malware Detection', *Computer Science*, 20(3), p. 383. Available at: https://doi.org/10.7494/csci.2019.20.3.3285.

Damodaran, A. *et al.* (2017) 'A Comparison of Static, Dynamic, and Hybrid Analysis for Malware Detection', *Journal of Computer Virology and Hacking Techniques*, 13(1), pp. 1–12. Available at: https://doi.org/10.1007/s11416-015-0261-z.

Devi, P.G., Chandana, S. and Sathish, P. (2021) 'Design and Development of Android Application for Virtual Birthday Present', in *2021 6th International Conference on Communication and Electronics Systems (ICCES)*. *2021 6th International Conference on Communication and Electronics Systems (ICCES)*, Coimbatre, India: IEEE, pp. 752–757. Available at: https://doi.org/10.1109/ICCES51350.2021.9489255.

Gong, L. *et al.* (2022) 'Overlay-Based Android Malware Detection at Market Scales: Systematically Adapting to the New Technological Landscape', *IEEE Transactions on Mobile Computing*, 21(12), pp. 4488–4501. Available at: https://doi.org/10.1109/TMC.2021.3079433.

Gronli, T.-M. *et al.* (2014) 'Mobile Application Platform Heterogeneity: Android vs Windows Phone vs iOS vs Firefox OS', in *2014 IEEE 28th International Conference on Advanced Information Networking and Applications*. *2014 IEEE 28th International Conference on Advanced Information Networking and Applications (AINA)*, Victoria, BC, Canada: IEEE, pp. 635–641. Available at: https://doi.org/10.1109/AINA.2014.78.

Hanifurohman, C. and Hutagalung, D.D. (2020) 'Analisis Statis Menggunakan Mobile Security Framework untuk Pengujian Keamanan Aplikasi Mobile E-Commerce Berbasis Android', *Sebatik*, 24(1), pp. 22–28. Available at: https://doi.org/10.46984/sebatik.v24i1.920.

Haritsah, M., Widjajarto, A. and Almaarif, A. (2023) 'Analisis Karakteristik Antivirus Berdasarkan Aktivitas Malware menggunakan Analisis Dinamis', *Journal of Information System Research (JOSH)*, 4(2), pp. 693–700. Available at: https://doi.org/10.47065/josh.v4i2.2908.

Hariyadi, D. (2022) *Buku Panduan Dasar Digital Forensik*. 1st edn. Yogyakarta: Baskara Media.

Hatika, L.K., Budiyono, A. and Almaarif, A. (2019) 'Analisis Ketepatan Deteksi Malware Pada Software Antivirus Menggunakan Metode Analisis Statis', 6(2), pp. 7812–7819.

Hyder, M.F. and Ismail, M.A. (2021) 'Securing Control and Data Planes From Reconnaissance Attacks Using Distributed Shadow Controllers, Reactive and Proactive Approaches', *IEEE Access*, 9, pp. 21881–21894. Available at: https://doi.org/10.1109/ACCESS.2021.3055577.

Jamal, N. (2017) 'Model-Model Integrasi Keilmuan Perguruan Tinggi Keagamaan Islam', *KABILAH : Journal of Social Community*, 2(1), pp. 83–101. Available at: https://doi.org/10.35127/kbl.v2i1.3088.

Jaramillo, L.E.S. (2018) 'Malware Detection and Mitigation Techniques: Lessons Learned from Mirai DDOS Attack', *Journal of Information Systems Engineering & Management*, 3(3). Available at: https://doi.org/10.20897/jisem/2655.

Jaramillo, L.E.S. (2019) 'Malware Threats Analysis and Mitigation Techniques for Compromised Systems', *Journal of Information Systems Engineering & Management*, 4(1). Available at: https://doi.org/10.29333/jisem/5742.

Jensen, K., Tazi, F. and Das, S. (2021) 'Multi-Factor Authentication Application Assessment: Risk Assessment of Expert-Recommended MFA Mobile Applications', *Social Science Research Network* [Preprint].

Joyce, R.E. (2021) 'Instruction For Secret National Security Systems Public Key Infrastructure X.509 Certificate Policy'.

Kapratwar, A., Troia, F.D. and Stamp, M. (2017) 'Static and Dynamic Analysis of Android Malware'.

Kayani, A.K. and Saeed, M.Q. (2021) 'Comparative Analysis of Anti-Virus Evasion Malware Creator Tools of Kali Linux, with Proposed Model for Obfuscation', in *2021 International Conference on Cyber Warfare and Security (ICCWS)*. *2021 International Conference on Cyber Warfare and Security (ICCWS)*, Islamabad, Pakistan: IEEE, pp. 24–29. Available at: https://doi.org/10.1109/ICCWS53234.2021.9702944.

Kohli, N. and Mohaghegh, M. (2020) 'Security Testing Of Android Based Covid Tracer Applications', in *2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*. *2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*, Gold Coast, Australia: IEEE, pp. 1–6. Available at: https://doi.org/10.1109/CSDE50874.2020.9411579.

Le, D.T. *et al.* (2023) 'Exploring Common Malware Persistence Techniques on Windows Operating Systems (OS) for Enhanced Cybersecurity Management', in El-Latif, A. A. A. et al., *Cybersecurity Management in Education Technologies*. 1st edn. New York: CRC Press, pp. 107–149. Available at: https://doi.org/10.1201/9781003369042-7.

Lebbie, M., Prabhu, S.R. and Agrawal, A.K. (2022) 'Comparative Analysis of Dynamic Malware Analysis Tools', in M. Dua et al. (eds) *Proceedings of the International Conference on Paradigms of Communication, Computing and Data Sciences*. Singapore: Springer Singapore (Algorithms for Intelligent Systems), pp. 359–368. Available at: https://doi.org/10.1007/978-981-16-5747-4_31.

Makridakis, S. (2017) 'The forthcoming Artificial Intelligence (AI) revolution: Its impact on society and firms', *Futures*, 90, pp. 46–60. Available at: https://doi.org/10.1016/j.futures.2017.03.006.

May (2022) 'Waspada Penipuan Berkedok Kurir Paket Kirim File APK Berujung Saldo Rekening', *Viva*, 5 December. Available at: https://www.viva.co.id/berita/nasional/1551670-waspada-penipuan-berkedok-kurir-paket-kirim-file-apk-berujung-saldo-rekening-ludes (Accessed: 28 September 2023).

Mazurczyk, W. and Caviglione, L. (2021) ‘Cyber reconnaissance techniques’, *Communications of the ACM*, 64(3), pp. 86–95. Available at: https://doi.org/10.1145/3418293.

Mell, P., Kent, K.A. and Nusbaum, J. (2005) *Guide to malware incident prevention and handling*. 0 edn. NIST SP 800-83. Gaithersburg, MD: National Institute of Standards and Technology, p. NIST SP 800-83. Available at: https://doi.org/10.6028/NIST.SP.800-83.

Monnappa, K.A. (2018) *Learning Malware Analysis Explore the concepts, tools, and techniques to analyze and investigate Windoes malware*. Birmingham, UK: Packt Publishing Ltd.

Muhtadi, A.F. and Almaarif, A. (2020) ‘Analysis ofMalware Impact on Network Traffic using Behavior-based Detevtion Technique’, *International Journal of Advances in Data and Information Systems*, 1(1), pp. 17–25. Available at: https://doi.org/10.25008/ijadis.v1i1.14.

Mustajab, R. (2023) ‘Ada 5,46 Mialiar Serangan Malware di Dunia Pada 2022’, *DataIndonesia*, 30 May. Available at: https://dataindonesia.id/internet/detail/ada-546-miliar-serangan-malware-di-dunia-pada-2022 (Accessed: 29 September 2023).

Nasirudin, N., Sunardi, S. and Riadi, I. (2020) ‘Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express’, *Jurnal Informatika Universitas Pamulang*, 5(1), p. 89. Available at: https://doi.org/10.32493/informatika.v5i1.4578.

Naway, A. and Li, Y. (2018) ‘Android Malware Detection Using Autoencoder’, *International Journal of Computer Engineering and Applications*, 12(12).

Nugroho, A. and cyberthread.id, A.N. (2022) *Viral File Android Berkedok J&T Express, BSSN: Ini Malware SMS Stealer Kategori Dangerous*, *cyberthreat.id*. Available at: https://cyberthreat.id/read/14999/Viral-File-Android-Berkedok-JT-Express-BSSN-Ini-Malware-SMS-Stealer-Kategori-Dangerous (Accessed: 12 February 2024).

Nurhalim, S. (2022) ‘Waspada! Modus Penipuan Baru Mengaku Kurir Kirim Foto File APK’, *Detik.com*, 6 December.

Olesen, D. *et al.* (2016) ‘GNSS Software Receiver for UAVs’, in. Available at: https://api.semanticscholar.org/CorpusID:56296321.

Or-Meir, O. *et al.* (2020) ‘Dynamic Malware Analysis in the Modern Era—A State of the Art Survey’, *ACM Computing Surveys*, 52(5), pp. 1–48. Available at: https://doi.org/10.1145/3329786.

Ozcan, A. *et al.* (2023) ‘A hybrid DNN–LSTM model for detecting phishing URLs’, *Neural Computing and Applications*, 35(7), pp. 4957–4973. Available at: https://doi.org/10.1007/s00521-021-06401-z.

Pamungkas, C. *et al.* (2023) ‘Analysis of Brute Force Attacks Using National Institute Of Standards And Technology (NIST) Methods on Routers’, *Journal of Informatics Information System Software Engineering and Applications (INISTA)*, 5(2), pp. 115–125. Available at: https://doi.org/10.20895/inista.v5i2.1039.

Peng, P. *et al.* (2019) ‘Opening the Blackbox of VirusTotal: Analyzing Online Phishing Scan Engines’, in *Proceedings of the Internet Measurement Conference*. *IMC ’19: ACM Internet Measurement Conference*, Amsterdam

Netherlands: ACM, pp. 478–485. Available at: https://doi.org/10.1145/3355369.3355585.
Prahara, S. (2022) *Pembuktian Elektronik dan Digital Forensik di Indonesia*. 1st edn. Padang: LPPM Universitas Bung Hatta.
Prawira, Y. (2022) 'Live Forensics Analysis Of Malware Identified Email Crimes To Increase Evidence Of Cyber Crime', *Digital Zone Jurnal Teknologi Informasi dan Komunikasi*, 13(2), pp. 111–124.
Pribadi, B., Rosdiana, S. and Arifin, S. (2023) 'Digital forensics on facebook messenger application in an android smartphone based on NIST SP 800-101 R1 to reveal digital crime cases', *Procedia Computer Science*, 216, pp. 161–167. Available at: https://doi.org/10.1016/j.procs.2022.12.123.
Qiao, Q. *et al.* (2022) 'Multi-label Classification for Android Malware Based on Active Learning', *IEEE Transactions on Dependable and Secure Computing*, pp. 1–18. Available at: https://doi.org/10.1109/TDSC.2022.3213689.
Raodia, R. (2019) 'Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (Cybercrime)', *Jurisprudentie*, 6(2), p. 39. Available at: https://doi.org/10.24252/jurisprudentie.v6i2.11399.
Riskiyadi, M., Anggono, A., and Tarjo (2021) 'Cybercrime dan Cybersecurity pada Fintech: Sebuah Tinjauan Pustaka Sistematis', *Jurnal Manajemen dan Organisasi*, 12(3), pp. 239–251. Available at: https://doi.org/10.29244/jmo.v12i3.33528.
Rizaty, M.A. (2023) 'Pengguna Internet di Indonesia Sentuh 212 Juta pada 2023', *DataIndonesia*, 3 February. Available at: https://dataindonesia.id/internet/detail/pengguna-internet-di-indonesia-sentuh-212-juta-pada-2023 (Accessed: 26 September 2023).
Salfati, E. and Pease, M. (2022) *Digital Forensics and Incident Response (DFIR) framework for Operational Technology (OT)*. NIST IR 8428. Gaithersburg, MD: National Institute of Standards and Technology (U.S.), p. NIST IR 8428. Available at: https://doi.org/10.6028/NIST.IR.8428.
Sarnita, S. (2023) 'Sebanyak 67,88% Penduduk RI Gunakan Telepon Genggam pada 2022', *DataIndonesia*, 12 June. Available at: https://dataindonesia.id/telekomunikasi/detail/sebanyak-6788-penduduk-ri-gunakan-telepon-genggam-pada-2022 (Accessed: 15 November 2023).
Sharma, Y. and Arora, A. (2024) 'A comprehensive review on permissions-based Android malware detection', *International Journal of Information Security* [Preprint]. Available at: https://doi.org/10.1007/s10207-024-00822-2.
Shijo, P.V. and Salim, A. (2015) 'Integrated Static and Dynamic Analysis for Malware Detection', *Procedia Computer Science*, 46, pp. 804–811. Available at: https://doi.org/10.1016/j.procs.2015.02.149.
Sihwail, R., Omar, K. and Zainol Ariffin, K.A. (2018) 'A Survey on Malware Analysis Techniques: Static, Dynamic, Hybrid and Memory Analysis', *International Journal on Advanced Science, Engineering and Information Technology*, 8(4–2), pp. 1662–1671. Available at: https://doi.org/10.18517/ijaseit.8.4-2.6827.
Sindoni, A. (2023) *Toward a methodology for malware analysis and characterization for Machine Learning application*. Politecnico Di Torino.

Souppaya, M. and Scarfone, K. (2013) *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*. NIST SP 800-83r1. National Institute of Standards and Technology, p. NIST SP 800-83r1. Available at: https://doi.org/10.6028/NIST.SP.800-83r1.

Statista, D.P. (2023) 'Market share of mobile operating systems in Indonesia from January 2019 to August 2023'. https://www.statista.com/statistics/262205/market-share-held-by-mobile-operating-systems-in-indonesia/.

Surendran, R. and Thomas, T. (2022) 'Detection of malware applications from centrality measures of syscall graph', *Concurrency and Computation: Practice and Experience*, 34(10), p. e6835. Available at: https://doi.org/10.1002/cpe.6835.

Syaputra, R. (2020) 'Studi Literatur Analisis Malware Menggunakan Metode Analisis Dinamis dan Statis', 01(01), pp. 14–24.

Umam, M.K. (2024) 'Analisis Forensik Malware pada Perangkat Android Menggunakan Framework D4I'.

Wajahat, A. *et al.* (2024) 'Securing Android IoT devices with GuardDroid transparent and lightweight malware detection', *Ain Shams Engineering Journal*, p. 102642. Available at: https://doi.org/10.1016/j.asej.2024.102642.

Waliulu, R.F. and Iskandar Alam, T.H. (2018) 'Reverse Engineering Analysis Forensic Malware WEBC2-DIV', *Journal of Informatics, Informations System, Software Engineering and Applications*, 1(1). Available at: https://doi.org/10.30865/komik.v2i1.902.

Wang, Y. (2022) 'Vulnerability analysis and improvement of RASP technology', in *2022 International Symposium on Advances in Informatics, Electronics and Education (ISAIEE)*. *2022 International Symposium on Advances in Informatics, Electronics and Education (ISAIEE)*, Frankfurt, Germany: IEEE, pp. 266–272. Available at: https://doi.org/10.1109/ISAIEE57420.2022.00061.

Wijaya, D.C. *et al.* (2021) 'An Implementation and Evaluation of Basic Data Storage Topic for Content Provider Stage in Android Programming Learning Assistance System', in *2021 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*. *2021 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, Zallaq, Bahrain: IEEE, pp. 328–333. Available at: https://doi.org/10.1109/3ICT53449.2021.9581767.

Yonamine, S., Taenaka, Y. and Kadobayashi, Y. (2022) 'Tamer: A Sandbox for Facilitating and Automating IoT Malware Analysis with Techniques to Elicit Malicious Behavior':, in *Proceedings of the 8th International Conference on Information Systems Security and Privacy*. *6th International Special Session on FORmal methods for Security Engineering*, Vienna, Austria: SCITEPRESS - Science and Technology Publications, pp. 677–687. Available at: https://doi.org/10.5220/0010968300003120.

Zhu, S. *et al.* (2020) 'Measuring and Modeling the Label Dynamics of Online Anti-Malware Engines', in *Proceeding of the 29th USENIX Security Symposium*.

29th USENIX Security Symposium, USENIX the Advanced Computing Systems Association.