ANALISIS FORENSIK MOBILE TROJAN METASPLOIT DENGAN PENDEKATAN NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

SKRIPSI

OLEH :
PUTRA OSAMA
09011282025049

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2024

ANALISIS FORENSIK MOBILE TROJAN METASPLOIT DENGAN PENDEKATAN NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH :
PUTRA OSAMA
09011282025049

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2024

HALAMAN PENGESAHAN

ANALISIS FORENSIK MOBILE TROJAN METASPLOIT DENGAN PENDEKATAN NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH :
PUTRA OSAMA
09011282025049

Indralaya, 2 Juli 2024

Mengetahui,
Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.
NIP. 196612032006041001

Pembimbing Tugas Akhir

Prof. Deris Stiawan, M.T., Ph.D.
NIP. 197806172006041002

AUTHENTICATION PAGE

FORENSIC ANALYSIS OF MOBILE TROJAN METASPLOIT USING THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) APPROACH

THESIS

Submitted To Ful fill One of The Requirements
To Obtain a Bachelor's Degree in Computer Science

By :
PUTRA OSAMA
09011282025049

Indralaya, 22 *July* 2024

Acknowledge,
Head of Computer System Department

Dr. Ir. Sukemi, M.T.
NIP. 196612032006041001

Final Project Advisor

Prof. Deris Stiawan, M.T., Ph.D.
NIP. 197806172006041002

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Kamis

Tanggal : 4 Juli 2024

Tim Penguji :

1. **Ketua** : **Sarmayanta Sembiring, M.T.**
2. **Sekretaris** : **Nurul Afifah, M.Kom.**
3. **Penguji** : **Dr. Ahmad Zarkasi, M.T.**
4. **Pembimbing** : **Prof. Deris Stiawan, M.T., Ph.D.**

Mengetahui, 22/7/24

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama	: Putra Osama
NIM	: 09011282025049
Program Studi	: Sistem Komputer
Judul	: Analisis Forensik *Mobile Trojan Metasploit* dengan Pendekatan *National Institute of Standards and Technology* (NIST)

Hasil pengecekan *Software* (*iThenticate/Turnitin*) : 5%

Menyatakan bahwa laporan tugas akhir/skripsi saya merupakan hasil karya sendiri dan bukan hasil plagiasi/duplikasi dari penelitian orang lain. Apabila ditemukan unsur plagiasi/duplikasi dari penelitian orang lain, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian, pernyataan ini saya buat dengan sebenar-benarnya dan tanpa adanya paksaan.

Indralaya, 17 Juli 2024

Penulis

Putra Osama

NIM. 09011282025049

KATA PENGANTAR

Alhamdulillahirabbil'alamin. Puji dan syukur penulis panjatkan atas kehadirat Allah SWT. yang mana berkat karunia dan rahmat-Nya, sehingga penulis dapat menyelesaikan penulisan tugas akhir ini. Sholawat serta salam tak lupa pula penulis ucapkan kepada junjungan dan panutan kita Nabi Muhammad SAW., kepada keluarganya, para sahabatnya, dan semoga kita tergolong pada orang-orang ahli surga, *Aamiin*.

Pada kesempatan ini, terwujudlah bagi penulis sebuah karya ilmiah atau tugas akhir untuk melengkapi salah satu syarat memperoleh gelar sarjana komputer (S.Kom) pada Fakultas Ilmu Komputer Univeristas Sriwijaya dengan judul ***"Analisis Forensik Mobile Trojan Metasploit dengan Pendekatan National Institute of Standards and Technology (NIST)"***.

Pada penyusunan tugas akhir ini, penulis banyak sekali mendapat bantuan dan dorongan dari berbagai pihak. Semoga Allah SWT. memberikan balasan yang setimpal. Oleh karena itu, penulis ingin menyampaikan ucapan terima kasih yang sebesar-besarnya kepada :

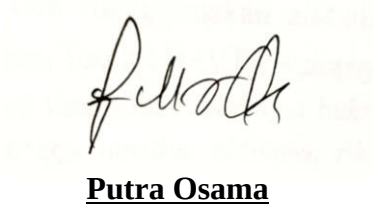
1. Kedua Orang Tua tercinta atas kasih sayang, doa, motivasi, serta dukungan moril, materil, dan spiritual.
2. Kakak Perempuan yang juga selalu memberikan motivasi dan dukungan moril maupun materil.
3. Bapak Prof. Dr. Erwin, S.Si, M. Si., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. Sukemi, M.T., selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Prof. Deris Stiawan, M.T., Ph.D., selaku Dosen Pembimbing Tugas Akhir, yang telah memberikan bimbingan, saran, dan motivasi.
6. Bapak Dr. Rossi Passarella, M.Eng., selaku Dosen Pembimbing Akademik Jurusan Sistem Komputer.
7. Kak Angga, selaku Admin Jurusan Sistem Komputer, atas bantuannya dalam administrasi tugas akhir.

8. Arya, Hafidz, Bintang, Afif, dan Iyas, selaku rekan penulis dalam riset tugas akhir yang banyak membantu dan memberikan saran.
9. Grup Riset COMNETS sebagai wadah belajar, dan lab COMNETS sebagai tempat penulis belajar dan menulis tugas akhir.
10. Seluruh teman seperjuangan angkatan 2020 dan kakak tingkat, yang menjadi panutan di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

Penulis mengharapkan dan membuka diri untuk segala kritik dan saran yang membangun dari semua pihak sebagai acuan untuk penulisan tugas akhir yang lebih baik lagi. Akhir kata penulis berharap, semoga tugas akhir ini memberikan manfaat dan berguna bagi kita semua.

Indralaya, 17 Juli 2024

Penulis,



Putra Osama

NIM. 09011282025049

ANALISIS FORENSIK MOBILE TROJAN METASPLOIT DENGAN PENDEKATAN NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

Putra Osama (09011282025049)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer
Universitas Sriwijaya
E-mail : putraosamaid@gmail.com

ABSTRAK

Peningkatan jumlah APK dalam teknologi *mobile* dari tahun ke tahun sering kali disertai dengan munculnya APK yang mengandung *malware*. Dengan menggunakan kerangka kerja *Metasploit*, *threat actor* dapat menyisipkan *payload* pada APK jinak. Untuk menanggapi serangan semacam ini, perlu dilakukan investigasi forensik pada perangkat *mobile*. Penelitian ini bertujuan untuk melakukan analisis forensik pada perangkat Android yang terinfeksi APK Trojan, dengan menerapkan metodologi NIST SP 800-101 dan menggunakan alat-alat forensik seperti Magnet ACQUIRE, Mobile Verification Toolkit (MVT), Autopsy, dan SQLite DB Browser. Hasil penelitian mencakup identifikasi berbagai bukti digital seperti file APK Trojan, *database* WhatsApp, *timeline* aktivitas, *file* terhapus, dan dataset *network traffic*. Penelitian ini memberikan pemahaman tentang mekanisme serangan dan strategi mitigasi potensial untuk melindungi perangkat Android dari ancaman serupa di masa depan.

Kata Kunci : *Mobile Forensic*, APK, *Trojan*, *Metasploit*, NIST SP 800-101.

Mengetahui,

Ketua Jurusan Sistem Komputer	**Pembimbing Tugas Akhir**
Dr. Ir. Sukemi, M.T.	**Prof. Deris Stiawan, M.T., Ph.D.**
NIP. 196612032006041001	**NIP. 197806172006041002**

FORENSIC ANALYSIS OF MOBILE TROJAN METASPLOIT USING THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) APPROACH

Putra Osama (09011282025049)

Dept. of Computer System, Faculty of Computer Science

Sriwijaya University

E-mail : putraosamaid@gmail.com

ABSTRACT

The increasing number of APKs in mobile technology each year often coincides with the emergence of APKs containing malware. Through the Metasploit framework, threat actors are able to embed payloads into benign APKs. To address this issue, forensic investigation on mobile devices becomes crucial. This research aims to conduct forensic analysis on Android devices infected with Trojan APKs, applying NIST SP 800-101 methodology and utilizing forensic tools such as Magnet ACQUIRE, Mobile Verification Toolkit (MVT), Autopsy, and SQLite DB Browser. The research results include the identification of various digital evidence such as Trojan APK files, WhatsApp databases, activity timelines, deleted files, and network traffic datasets. This study provides deep insights into attack mechanisms and potential mitigation strategies to protect Android devices from similar threats in the future.

Keywords : Mobile Forensic, APK, Trojan, Metasploit, NIST 800-101.

Acknowledge,

Head of Computer System Department

Dr. Ir. Sukemi, M.T.
NIP. 196612032006041001

Final Project Advisor

Prof. Deris Stiawan, M.T., Ph.D.
NIP. 197806172006041002

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1. Latar Belakang

Pada tahun 2023, *data* statistik menunjukan jumlah unduhan aplikasi *mobile* mencapai 257 milliar [1]. Seiring dengan perkembangan teknologi *mobile* dan peningkatan jumlah aplikasi yang dipublikasikan di *app store* dan *play store*, infeksi *mobile malware* semakin meningkat [2]. Oleh karena itu, perangkat *mobile* menjadi sumber bukti penting bagi penyidik forensik.

National Institute of Standards and Technology (NIST), melalui *Information Technology Laboratory* (ITL) telah memainkan peran kunci dalam menghadirkan pedoman dan standar untuk melakukan forensik pada perangkat *mobile*, seperti yang digunakan dan disebutkan pada penelitian [3]. Pedoman tersebut mencakup prosedur dan metode yang dapat membantu penyidik forensik dalam menghadapi tantangan yang berkaitan dengan perangkat *mobile*.

Menurut [4], meskipun *mobile forensic* masih relatif baru, telah terjadi peningkatan dalam jumlah penelitian yang dilakukan dalam *domain* ini. Tantangan utama yang dihadapi oleh penyidik *mobile forensic* dapat dikelompokan menajadi dua kategori utama, yakni tantangan pengumpulan *data* dan tantangan selama analisis *data*. Hal ini menunjukan bahwa selain kompleksitas teknis dari *mobile malware*, penyidik juga perlu mengatasi kendala operasional selama proses forensik.

Pada penelitian terdahulu [5], sudah mencoba melakukan proses investigasi forensik dengan memberikan panduan menggunakan pendekatan atau prosedur forensik NIST terhadap proses investigasi aplikasi *blockchain,* khususnya *web3 wallet* dan berhasil mendapatkan artefak berupa *log* dan *file cache web* yang dapat menjadi sumber bukti penting. Penelitian tersebut menyoroti potensi keamanan dan privasi dari aplikasi yang diteliti dan memberikan panduan detail bagi peneliti untuk menganalisis *mobile forensic*.

Pada penelitian lainnya [6], juga telah mencoba melakukan analisis forensik dengan pendekatan NIST dengan bantuan forensik *tools* terhadap perangkat *mobile* Samsung Galaxy S4 dan Samsung Galaxy A3 untuk mendapatkan artefak

pada aplikasi Whatsapp. Hasilnya, *tools* yang dipakai yaitu Oxygen Forensics dan Magnet AXIOM dinilai unggul dan berhasil dalam mengakuisisi artefak Whatsapp. Penelitian tersebut juga memberikan penduan detail tentang prosedur forensik dengan pendekatan NIST dan sekaligus penggunaan *tools* forensik dalam prosedurnya.

Dengan mempertimbangkan kompleksitas dan evolusi ancaman dalam ekosistem *mobile,* penelitian ini bertujuan untuk memberikan kontribusi pada pemahaman lebih lanjut mengenai analisis forensik terhadap *Trojan Metasploit.* Dengan merangkul pendekatan yang telah ditetapkan oleh NIST, diharapkan penelitian ini dapat memberikan kerangka kerja yang kuat untuk menghadapi tantangan-tantangan terkini dalam mengumpulkan dan menganalisis bukti forensik dari perangkat *mobile* yang tereksploitasi.

1.2. Rumusan Masalah

1. Bagaimana menganalisis *mobile forensic Trojan Metasploit* dengan pendekatan NIST?
2. Bagaimana tingkat keberhasilan dan tantangan menerapkan pendekatan NIST pada analisis *mobile forensic Trojan Metasploit*?
3. Bagaimana bukti yang didapatkan dengan pendekatan NIST?
4. Bagaimana karakteristik APK *Trojan Metasploit*?

1.3. Batasan Masalah

1. Analisis *mobile forensic* berfokus pada perangkat *mobile victim*.
2. Analisis akan terfokus pada *mobile Trojan Metasploit* dalam bentuk APK.
3. *Tools* forensik menggunakan Mobile Verification Toolkit (MVT) dan Autopsy dengan ketersediaan *open-source* dan Magnet ACQUIRE dengan ketersediaan *freeware*.

1.4. Tujuan

Adapun tujuan dari penelitian ini, yaitu :

1. Menerapkan pendekatan *National Institute of Standards and Technology* (NIST) dalam proses *mobile forensic*.

2. Meningkatkan pemahaman tentang karakteristik yang berkaitan dengan serangan APK *Trojan Metasploit.*

1.5. Manfaat

Adapun manfaat didapatkan dari penelitian ini, yaitu :

1. Menyediakan panduan praktis bagi para penelitian dimasa depan tentang keamanan informasi dalam menerapkan pendekatan NIST pada analisis *mobile forensik*.
2. Memperkaya literatur keamanan informasi dengan penelitian khusus dalam analisis *mobile forensic.*
3. Memberikan pemahaman lebih mendalam tentang ancaman keamanan *mobile* dan meningkatkan kesadaran akan perlunya langkah-langkah mitigasi yang efektif.

1.6. Metodologi Penelitian

Metodologi yang digunakan dalam penulisan tugas akhir ini dirancang dengan cermat untuk memastikan kelancaran dan ketepatan dalam analisis forensik pada perangkat *mobile*. Metodologi ini melewati beberapa tahapan yang terperinci untuk mencapai tujuan penelitian yang telah ditetapkan sebagai berikut :

1. Tahap Pertama (Studi Pustaka/Literatur)

   Tahap ini dilakukan sesuai dengan kerelevanan penelitian sebelumnya yang mengacu banyaknya artikel, *paper*¸ jurnal dan buku yang berhubungan dengan penelitian ini yang berjudul "Analisis Forensik *Mobile Trojan Metasploit* dengan Pendekatan *National Institute of Standards and Technology* (NIST)".

2. Tahap Kedua (Perancangan Sistem)

   Tahap ini ialah perancangan sistem yang akan digunakan dalam analisis forensik pada perangkat *mobile*. Dalam tahap ini, mulai merancang topologi untuk menjalankan skenario *attacking*, termasuk pembuatan dan persiapan APK *Trojan*. Selain itu, tahap ini juga mencakup persiapan kebutuhan perangkat keras, serta instalasi maupun konfigurasi perangkat lunak.

3. Tahap Ketiga (Pengujian)

   Tahap ini merupakan kelanjutan dari proses perancangan sebelumnya. Pada tahap ini, dilakukan skenario *attacking* yang akan dijadikan dasar pengujian forensik. Selain itu, mulai diterapkan pendekatan atau metode forensik yang sesuai. Tahap ini juga mencakup rincian langkah-langkah pengujian, termasuk jenis serangan yang dilakukan dalam skenario dan proses pengumpulan *data* forensik.

4. Tahap Keempat (Analisis)

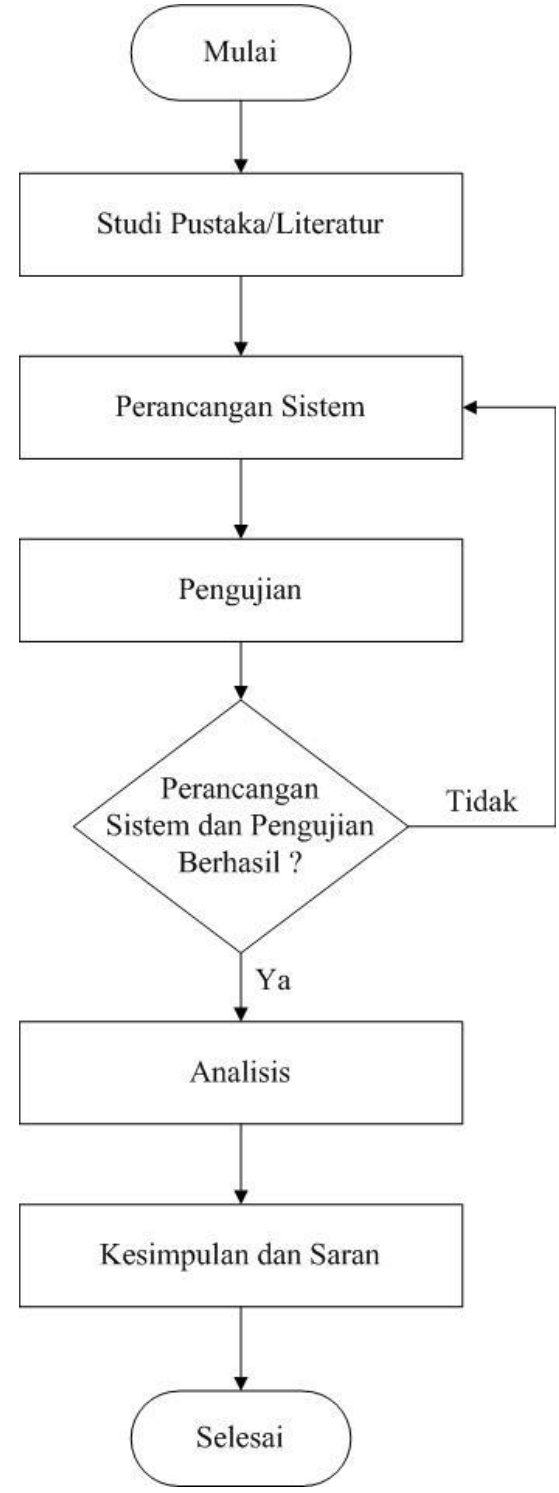
   Tahap ini dilakukan ketika tahap kedua yaitu perancangan sistem dan tahap ketiga yaitu pengujian sudah berhasil dilakukan. Pada tahap ini, yang dilakukan adalah memeriksa dan menganalisis hasil pengumpulan *data* forensik dari tahap ketiga yaitu tahap pengujian yang bertujuan untuk mengungkap bukti-bukti *digital* dan nilai pembuktian terhadap skenario serangan sebelumnya.

5. Tahap Kelima (Kesimpulan dan Saran)

   Tahap ini akan dirumuskan suatu kesimpulan berdasarkan permasalahan, studi pustaka, metodologi penelitian, dan analisis hasil membuat beberapa saran yang dapat dijadikan penelitian selanjutnya.

Dengan demikian, tahapan yang telah dilalui dalam metodologi penulisan tugas akhir ini memberikan landasan yang kokoh dalam menjalankan analisis forensik terhadap *Trojan Metasploit* pada perangkat *mobile*. Kesimpulan dan saran yang dihasilkan dari metodologi ini diharapkan dapat memberikan kontribusi yang berharga bagi penelitian selanjutnya dalam bidang *mobile forensic*.

Pada Gambar 1.1 berikut, ditampilkan gambaran proses penelitian dalam bentuk diagram alir.



Gambar 1.1. Diagram Alir Metodologi Penelitian

1.7. Sistematika Penulisan

Demi meningkatkan kemudahan penyusunan tugas akhir ini dan memberikan penjelasan yang lebih terperinci mengenai substansi setiap bab yang terdapat didalamnya, maka dibuatlah suatu sistematika penulisan sebagai berikut :

BAB I PENDAHULUAN

Pada Bab I akan menjelaskan latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat, metodologi penelitian, dan sistematika penulisan yang mengacu pada landasan topik penelitian.

BAB II TINJAUAN PUSTAKA

Pada Bab II akan berisi mengenai studi literatur penelitian terdahulu, dasar teori *mobile forensic*, *mobile Trojan Metasploit*, dan mengenal pendekatan *mobile forensic* oleh *National Institute of Standards and Tecnology* (NIST)

BAB III METODOLOGI PENELITIAN

Pada Bab III akan memberikan penjelasan secara sistematis mengenai bagaimana proses penelitian dilakukan, tahapan perancangan, dan penerapan pendekatan atau metode penelitian.

BAB IV HASIL DAN ANALISIS

Pada Bab IV akan menjelaskan hasil penelitian yang dilakukan serta analisis dari hasil *data* yang didapatkan.

BAB V KESIMPULAN DAN SARAN

Pada Bab V berisi kesimpulan dari hasil penelitian yang dilakukan, menjawab rumusan masalah serta mencapai tujuan dari Bab I (Pendahuluan), dan saran untuk penelitian selanjutnya.

DAFTAR PUSTAKA

[1] Statista.com, "Number of mobile app downloads worldwide from 2016 to 2023," *TechCrunch*. https://www.statista.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads (accessed Apr. 10, 2024).

[2] M. Ashawa and S. Morris, "Analysis of Mobile Malware: A Systematic Review of Evolution and Infection Strategies," *J. Inf. Secur. Cybercrimes Res.*, vol. 4, no. 2, pp. 103–131, 2021, doi: 10.26735/krvi8434.

[3] D. Sudiana, C. H. Nuruddin, M. Rizkinia, and D. Husna, "Forensic Analysis of WhatsApp Disappearing Message on Unrooted Android Using Mobile Device Forensics Methodology NIST SP 800-101r1," *Evergreen*, vol. 11, no. 1, pp. 516–524, 2024.

[4] H. Alatawi, K. Alenazi, S. Alshehri, S. Alshamakhi, M. Mustafa, and A. Aljaedi, "Mobile Forensics: A Review," *2020 Int. Conf. Comput. Inf. Technol. ICCIT 2020*, vol. 02, pp. 1–6, 2020, doi: 10.1109/ICCIT-144147971.2020.9213739.

[5] M. M. Mirza, A. Ozer, and U. Karabiyik, "Mobile Cyber Forensic Investigations of Web3 Wallets on Android and iOS," *Appl. Sci.*, vol. 12, no. 21, 2022, doi: 10.3390/app122111180.

[6] G. M. Zamroni and I. Riadi, "Mobile Forensic Tools Validation and Evaluation for Instant Messaging," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 10, no. 5, pp. 1860–1866, 2020, doi: 10.18517/ijaseit.10.5.7499.

[7] A. S. Putra, N. Aisyah, and V. H. Valentino, "Analysis of nist methods on facebook messenger for forensic evidence," *J. Innov. Res. Knowl.*, vol. 1, no. 8, pp. 695–702, 2022.

[8] S. Sharma, C. R. Krishna, and R. Kumar, "RansomDroid: Forensic analysis and detection of Android Ransomware using unsupervised machine learning technique," *Forensic Sci. Int. Digit. Investig.*, vol. 37, p. 301168, 2021.

[9] A. Menahil, W. Iqbal, M. Iftikhar, W. Bin Shahid, K. Mansoor, and S. Rubab, “Forensic Analysis of Social Networking Applications on an Android Smartphone,” *Wirel. Commun. Mob. Comput.*, vol. 2021, 2021, doi: 10.1155/2021/5567592.

[10] A. N. Ichsan and I. Riadi, “Mobile Forensic on Android-based IMO Messenger Services using Digital Forensic Research Workshop (DFRWS) Method,” *Int. J. Comput. Appl.*, vol. 174, no. 18, pp. 34–40, 2021, doi: 10.5120/ijca2021921076.

[11] K. D. O. Mahendraa and I. K. A. Mogia, “Digital Forensic Analysis of Michat Applications on Android as Digital Proof in Handling Online Prostitution Cases,” *J. Elektron. Ilmu Komput. Udayana p-ISSN*, vol. 2301, p. 5373, 2021.

[12] I. G. N. G. Wicaksanaa and I. K. G. Suhartanaa, “Forensic Analysis of Telegram Desktop-based Applications using the National Institute of Justice (NIJ) Method,” *J. Elektron. Ilmu Komput. Udayana p-ISSN*, vol. 2301, p. 5373, 2020.

[13] M. Moreb, “Forensic Investigations of Popular Applications on Android and iOS Platforms,” in *Practical Forensic Analysis of Artifacts on iOS and Android Devices: Investigating Complex Mobile Devices*, Springer, 2022, pp. 109–149.

[14] A. Al-Dhaqm, S. A. Razak, R. A. Ikuesan, V. R. Kebande, and K. Siddique, “A review of mobile forensic investigation process models,” *IEEE Access*, vol. 8, pp. 173359–173375, 2020, doi: 10.1109/ACCESS.2020.3014615.

[15] X. Q. Chow and N. H. Ab Rahman, “A Mobile Forensic Visualization Tool For Android Data Partition,” *Appl. Inf. Technol. Comput. Sci.*, vol. 2, no. 2, pp. 37–52, 2021.

[16] “About NIST,” *The National Institute of Standards And Technology*, 2022. https://www.nist.gov/about-nist (accessed Jan. 11, 2024).

[17] "What ITL Does," *The National Institute of Standards and Technology*, 2023. https://www.nist.gov/itl (accessed Jan. 11, 2024).

[18] P.-C. Cristian, T.-C. Hernan, G.-Q. Rene, A.-P. Francisco, and N.-G. Cristian, "Methodologies and Forensic Analysis Tools on Android Mobile Devices: A Systematic Literature Review," in *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*, 2020, pp. 1–7.

[19] R. Ayers, S. Brothers, and W. Jansen, "Guidelines on Mobile Device Forensics." Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD. doi: https://doi.org/10.6028/NIST.SP.800-101r1.

[20] V. Sihag, M. Vardhan, and P. Singh, "A survey of android application and malware hardening," *Comput. Sci. Rev.*, vol. 39, p. 100365, 2021.

[21] Statista.com, "Mobile operating systems targeted by developers worldwide in 2022 and 2023," *JetBrains*. https://www.statista.com/statistics/1078678/software-development-operating-system-mobile/ (accessed Apr. 10, 2024).

[22] C. A. E. Vásquez, W. Fuertes, and A. R. S. Cárdenas, "An implementation of a Virus Focuses on Mobile Devices with Android. An Ethical Hacking Event.," *Latin-American J. Comput.*, vol. 7, no. 2, pp. 78–91, 2020.

[23] S. Raj and N. K. Walia, "A Study on Metasploit Framework: A Pen-Testing Tool," *2020 Int. Conf. Comput. Perform. Eval. ComPE 2020*, pp. 296–302, 2020, doi: 10.1109/ComPE49325.2020.9200028.

[24] A. R. Damanik, H. B. Seta, and T. Theresiawati, "Analisis Trojan Dan Spyware Menggunakan Metode Hybrid Analysis," *J. Ilm. Matrik*, vol. 25, no. 1, pp. 89–97, 2023.

[25] A. F. Muhtadi and A. Almaarif, "Analysis of Malware Impact on Network Traffic using Behavior-based Detection Technique," *Int. J. Adv. Data Inf. Syst.*, vol. 1, no. 1, pp. 17–25, 2020, doi: 10.25008/ijadis.v1i1.14.

[26] M. A. H. Nasution and A. T. Laksono, “Investigasi Serangan Backdoor Remote Access Trojan (RAT) Terhadap Smartphone,” *JURIKOM (Jurnal Ris. Komputer)*, vol. 7, no. 4, pp. 505–510, 2020.

[27] Z. Wang, L. Sun, and H. Zhu, “Defining Social Engineering in Cybersecurity,” *IEEE Access*, vol. 8, pp. 85094–85115, 2020.

[28] M. Hijji and G. Alam, “A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats during the COVID-19 Pandemic: Challenges and Prospective Solutions,” *IEEE Access*, vol. 9, 2021.

[29] A. Fukami, R. Stoykova, and Z. Geradts, “A new model for forensic data extraction from encrypted mobile devices,” *Forensic Sci. Int. Digit. Investig.*, vol. 38, p. 301169, 2021.

[30] Amnesty International Security Lab, “Mobile Verification Toolkit,” *MVT Project Developers*, 2021. https://docs.mvt.re/en/latest/ (accessed Mar. 10, 2024).

[31] H. Jawale, P. Kamble, H. Sen, D. K. Singh, and S. Khedikar, “Unveiling the Pegasus Payload: Functionality and Implications of a Sophisticated Data Capture Framework,” *Int. Res. J. Innov. Eng. Technol.*, vol. 7, no. 10, p. 648, 2023.

[32] M. T. Shaamood, “Represent The Date Value In 2 Bytes,” *Iraqi J. Humanit. Soc. Sci. Res.*, vol. 3, no. 10, 2023.

[33] S. Qureshi, S. Tunio, F. Akhtar, A. Wajahat, A. Nazir, and F. Ullah, “Network Forensics: A Comprehensive Review of Tools and Techniques,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 5, 2021.

[34] D. Clark and B. P. Turnbull, “Interactive 3D Visualization of Network Traffic in Time for Forensic Analysis.,” in *VISIGRAPP (3: IVAPP)*, 2020, pp. 177–184.