ANALISIS FORENSIK DIGITAL ADWARE PADA APLIKASI UC BROWSER DAN SNACK VIDEO PADA PERANGKAT ANDROID DENGAN METODE NATIONAL INSTITUTE OF JUSTICE (NIJ)

SKRIPSI

UIN SUNAN AMPEL
S U R A B A Y A

Disusun Oleh:

ALMAR'ATUS SHOLEKAH

09040620046

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 : ALMAR'ATUS SHOLEKAH

NIM : 09040620046

Program Studi : SISTEM INFORMASI

Angkatan : 2020

Menyatakan bahwa saya tidak melakukan plagiat dalam penulisann skripsi saya yang berjudul " ANALISIS FORENSIK DIGITAL ADWARE PADA APLIKASI UC BROWSER DAM SNACK VIDEO PADA PERANGKAT ANDROID DENGAN METODE NATIONAL INSTITUTE OF JUSTICE (NIJ)". Apabila suatu saat nanti terbukti saya melakukan tindakan plagiasi, maka saya bersedia menerima sanksi yang telah ditetapkan.

Demikian pernyataan keaslian ini saya buat dengan sebenar-benarnya.

Surabaya, 13 Desember 2024

Yang menyatakan,

Almar'atus Sholekah

09040620046

LEMBAR PERSETUJUAN TIM PEMBIMBING

LEMBAR PERSETUJUAN PEMBIMBING

Skripsi oleh

NAMA	:	ALMAR'ATUS SHOLEKAH
NIM	:	09040620046
JUDUL	:	ANALISIS FORENSIK DIGITAL ADWARE PADA APLIKASI UC BROWSER DAN SNACK VIDEO PADA PERANGKAT ANDROID DENGAN METODE NATIONAL INSTITUTE OF JUSTICE (NIJ)

Ini telah diperiksa dan disetujui untuk diujikan.

Surabaya, 12 Desember 2024

Dosen Pembimbing 1	Dosen Pembimbing 2
Muhammad Andik Izzuddin, MT	**Faris Mushlihul Amin, M. Kom**
NIP. 198403072014031001	NIP. 198808132014031001

LEMBAR PENGESAHAN TIM PENGUJI SKRIPSI

LEMBAR PENGESAHAN TIM PENGUJI SKRIPSI

Skirpsi Almar'atus Sholekah ini telah dipertahankan

didepan tim penguji skripsi

di Surabaya, 24 Desember 2024

Mengesahkan

Dewan Penguji

Penguji I	Penguji II
Dr.Eng. Anang Kunaefi, M. Kom	**Noor Wahyudi, M.Kom**
NIP. 197911132014031001	NIP. 198403232014031002

Penguji III	Penguji IV
Muhammad Ardik Izzuddin, MT	**Faris Mushlihul Amin, M. Kom**
NIP. 198403072014031001	NIP. 198808132014031001

Mengetahui

Dekan Fakultas Sains dan Teknologi

UIN Sunan Ampel Surabaya

Dr. A. Saepul Hamdani, M.Pd

LEMBAR PERSETUJUAN PUBLIKASI KARYA ILMIAH

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 : ALMAR'ATUS SHOLEKAH
NIM : 090406 20096
Fakultas/Jurusan : SAINS DAN TEKNOLOGI / SISTEM INFORMASI
E-mail address : alma16339@gmail.com

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Perpustakaan UIN Sunan Ampel Surabaya, Hak Bebas Royalti Non-Eksklusif atas karya ilmiah :
☒ Sekripsi ☐ Tesis ☐ Desertasi ☐ Lain-lain (.....)
yang berjudul :

ANALISIS FORENSIK DIGITAL ADWARE PADA APLIKASI CLC BROWSER DAN SNACK VIDEO PADA PERANGKAT ANDROID DENGAN METODE NATIONAL INSTITUTE OF JUSTICE (NIJ)

beserta perangkat yang diperlukan (bila ada). Dengan Hak Bebas Royalti Non-Eksklusif 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, 14 Januari 2025

Penulis

(Almar'atus Sholekah)
nama terang dan tanda tangan

ABSTRAK

ANALISIS FORENSIK DIGITAL ADWARE PADA APLIKASI UC BROWSER DAN SNACK VIDEO PADA PERANGKAT ANDROID DENGAN METODE NATIONAL INSTITUTE OF JUSTICE (NIJ)

Penelitian ini bertujuan untuk menganalisis perilaku *adware* pada aplikasi UC Browser dan Snack Video pada perangkat *Android* dengan menggunakan metode *National Institute of Justice* (NIJ). *Adware,* sebagai salah satu bentuk *malware,* berpotensi mengganggu performa perangkat, menampilkan iklan tidak diinginkan, serta mengumpulkan data pribadi tanpa izin. Aplikasi UC Browser dan Snack Video dipilih sebagai objek penelitian karena popularitasnya yang tinggi dan potensinya dalam menjadi target ancaman *adware*. Metode NIJ digunakan untuk memberikan kerangka sistematis yang mencakup lima tahapan: *identification*, *collection, examination, analysis,* dan *reporting*. *Tools* seperti APK Tool, Tinycore, PCAPdroid, dan VirusTotal digunakan untuk mendeteksi dan menganalisis *adware* yang terintegrasi dalam kedua aplikasi tersebut. Hasil penelitian ini diharapkan dapat meningkatkan kesadaran pengguna *Android* tentang pentingnya keamanan digital dalam menggunakan aplikasi dari sumber terpercaya.

Kata kunci: Adware, UC Browser, Snack Video, Forensik Digital, National Institute of Justice (NIJ).

ABSTRACT

DIGITAL FORENSIC ANALYSIS OF ADWARE ON UC BROWSER AND SNACK VIDEO APPLICATIONS ON ANDROID DEVICES USING THE NATIONAL INSTITUTE OF JUSTICE (NIJ) METHOD

This study aims to analyze the behavior of adware on UC Browser and Snack Video applications on Android devices using the National Institute of Justice (NIJ) method. Adware, as a form of malware, has the potential to disrupt device performance, display unwanted advertisements, and collect personal data without permission. The UC Browser and Snack Video applications were chosen as research objects because of their high popularity and potential to be targets of adware threats. The NIJ method is used to provide a systematic framework that includes five stages: identification, collection, examination, analysis, and reporting. Tools such as APK Tool, Tinycore, PCAPdroid, and VirusTotal are used to detect and analyze adware integrated into both applications. The results of this study are expected to increase Android users' awareness of the importance of digital security in using applications from trusted sources.

Keywords: *Adware, UC Browser, Snack Video, Digital Forensics, National Institute of Justice (NIJ).*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

DAFTAR PUSTAKA

Abdiati, A. D., Setiawan, S., & Supendar, H. (2021). Pemilihan Web Browser Pada Mobile Menggunakan Metode Analytical Hierachy Process. *Jurnal Infortech*, *3*(1), Article 1. Https://Doi.Org/10.31294/Infortech.V3i1.10298

Agustin, P. A., & Nuryana, I. K. D. (2022). Analisa Perbandingan Pengguna Aplikasi Tiktok Dengan Snack Video Menggunakan Metode Utaut Dan Eucs. *Journal Of Emerging Information System And Business Intelligence (Jeisbi)*, *3*(4), 80–90.

Anton Kivva. (2023). *Smartphone Malware Statistics, Q2 2023*. Https://Securelist.Com/It-Threat-Evolution-Q2-2023-Mobile-Statistics/110427/

Aplikasi Android Di Google Play. (2024). From Https://Play.Google.Com/Store/Games?Hl=Id

Arenas, Á., Ray, G., Hidalgo, A., & Urueña, A. (2024). How To Keep Your Information Secure? Toward A Better Understanding Of Users Security Behavior. *Technological Forecasting And Social Change*, *198*, 123028. Https://Doi.Org/10.1016/J.Techfore.2023.123028

Ashawa, M., Morris, S., & The Society Of Digital Information And Wireless Communication. (2019). Analysis Of Android Malware Detection Techniques: A Systematic Review. *International Journal Of Cyber-Security And Digital Forensics*, *8*(3), 177–187. Https://Doi.Org/10.17781/P002605

Azis Kuba. (2024). *43 Juta Pengguna Aktif Per Bulan, Snackvideo Jadi Platform Video Peringkat 2 Di Indonesia—Herald Id*. Https://Herald.Id/2024/03/08/43-Juta-Pengguna-Aktif-Per-Bulan-Snackvideo-Jadi-Platform-Video-Peringkat-2-Di-Indonesia/

Choo, E., Nabeel, M., De Silva, R., Yu, T., & Khalil, I. (2022). *A Large Scale Study And Classification Of Virustotal Reports On Phishing And Malware Urls* (Arxiv:2205.13155). Arxiv. Http://Arxiv.Org/Abs/2205.13155

Cuomo, R., D'agostino, D., & Ianulardo, M. (2022). Mobile Forensics: Repeatable And Non-Repeatable Technical Assessments. *Sensors*, *22*(18), Article 18. Https://Doi.Org/10.3390/S22187096

Elahi, H., Wang, G., & Chen, J. (2020). Pleasure Or Pain? An Evaluation Of The Costs And Utilities Of Bloatware Applications In Android Smartphones. *Journal Of Network And Computer Applications*, *157*, 102578. Https://Doi.Org/10.1016/J.Jnca.2020.102578

Eric Wolkstein, S. M. M. At R. (2024). *Online Security And Cybersecurity Trends 2024 | Reasonlabs*. Https://Reasonlabs.Com/Research/Cybersecurity-Trends-2024

Hariyadi, D. (2022). *Buku Panduan Dasar Forensik Digital*.

Katutwa, K., Banda, D. E., & Shabani, J. (2022). Detection Of Android Adware Using Transfer Learning With Computer Vision. *Computer Science And Engineering*, *12*(1), 30–38.

Kusuma, G. H. A. (2023). *Implementasi Volatility Dalam Mengalanalisa Malware Pada Memory Dump*. *4*.

Mualfah, D., Viransa, A., & Amran, H. F. (2021). Akuisisi Bukti Digital Pada Aplikasi Tamtam Messenger Menggunakan Metode National Institute Of Justice. *Journal Of Software Engineering And Information Systems*, *3*(1). Https://Doi.Org/10.37859/Seis.V3i1.4548

Mubarok, M. S. H., Dasmen, R. N., Pranata, V., & Ary, M. (2024). *Digital Analysis Of Forensic Data Recovery On Flash Drive Using National Institute Of Justice (Nij) Method*. *12*(01).

Nasirudin, N., Sunardi, S., & Riadi, I. (2020). Analisis Forensik Smartphone Android Menggunakan Metode Nist Dan Tool Mobiledit Forensic Express. *Jurnal Informatika Universitas Pamulang*, *5*(1), 89. Https://Doi.Org/10.32493/Informatika.V5i1.4578

Nurul Qomariah, Erick Irawadi Alwi, & Muhammad Arfah Asis. (2024). Analisis Malware Hummingbad Dan Copycat Pada Android Menggunakan Metode Hybrid. *Cyber Security Dan Forensik Digital*, *6*(2), 39–47. Https://Doi.Org/10.14421/Csecurity.2023.6.2.4180

Onero. (2023). *Memahami Apk: Pengertian, Manfaat, Dan Cara Kerjanya*. Onero Solutions : It Solutions & Digital Marketing Jakarta. Https://Onero.Id/Insight/Detail/Memahami-Apk-Pengertian-Manfaat-Dan-Cara-Kerjanya/

Pcapdroid. (2024). Pcapdroid. From Https://Emanuele F.Github.Io/Pcapdroid/Quick_Start.Html

Prawira, Y. (2022). *Live Forensics Analysis Of Malware Identified Email Crimes To Increase Evidence Of Cyber Crime*.

Pribadi, B., Rosdiana, S., & 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*, 161–167. Https://Doi.Org/10.1016/J.Procs.2022.12.123

Priharsari, D. (2022). Systematic Literature Review Di Bidang Sistem Informasi Dan Ilmu Komputer. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *9*(2), 263. Https://Doi.Org/10.25126/Jtiik.2022923884

Rahmawati, A. (2022). *Apa Itu Bloatware? Ini Cara Menghapusnya*. Dosenit.Com. Https://Dosenit.Com/Software/Bloatware

Riadi, I., Yudhana, A., & Galih Pramuja Inngam Fanani. (2023). Comparative Analysis Of Forensic Software On Android-Based Michat Using Acpo And Dfrws Framework. *Jurnal Resti (Rekayasa Sistem Dan Teknologi Informasi)*, *7*(2), 286–292. Https://Doi.Org/10.29207/Resti.V7i2.4547

Sahfitri, & Kom, S. (2018). *Analisis Forensik Malware Pop-Up Ads Iklan Pada Platform Android*.

Seraj, S., Pavlidis, M., Trovati, M., & Polatidis, N. (2024). Maddroid: Malicious Adware Detection In Android Using Deep Learning. *Journal Of Cyber Security Technology*, *8*(3), 163–190. Https://Doi.Org/10.1080/23742917.2023.2247197

Silvia. (2022). *Pengertian Adware, Jenis, Dan Cara Menghindarinya*. Https://Www.Jetorbit.Com/Blog/Pengertian-Adware-Dan-Cara-Menghindarinya/

Sinambela, S., Pangestu, A. R., & Feriyanto, R. (2020). Analisis Aplikasi Malware Pada Android Dengan Metode Statik. *Jurnal Ilmiah Ilkominfo - Ilmu Komputer & Informatika*, *3*(2). Https://Doi.Org/10.47324/Ilkominfo.V3i2.101

Situmorang, S., Lubis, H., & Manullang, J. (2022). *Analysis Of Malware Methods Using Dynamic Analysis In Detecting Malware*. *6*(36).

Sixo Online Apk Analyzer | Sisik. (2024). From Https://Sisik.Eu/Apk-Tool

Sulistiowati, F. (2019). *Usability Testing Aplikasi Play Store Menggunakan Smartpls*. Https://Doi.Org/10.13140/Rg.2.2.26963.73767

Symu, A. (2021). Uc Browser Umumkan Laporan Tren Tahunan 2020. *Tabloidpulsa.Id*. Https://Tabloidpulsa.Id/Uc-Browser-Umumkan-Laporan-Tren-Tahunan-2020/

Tim. (2024). *33,8 Juta Serangan Siber Sasar Pengguna Hp Sepanjang 2023*. Teknologi. Https://Www.Cnnindonesia.Com/Teknologi/20240301114357-185-1069174/338-Juta-Serangan-Siber-Sasar-Pengguna-Hp-Sepanjang-2023

Universitas Indonesia, Wirara, A., Hardiawan, B., & Salman, M. (2020). Identifikasi Bukti Digital Pada Akuisisi Perangkat Mobile Dari Aplikasi Pesan Instan "Whatsapp." *Teknoin*, *26*(1), 66–74. Https://Doi.Org/10.20885/Teknoin.Vol26.Iss1.Art7

Valencia, V. N. G. A. P. (2022). *21 Distro Linux Terbaik Dan Terpopuler*. Dosenit.Com. Https://Dosenit.Com/Software/Distro-Linux

Vigne, N. L. (2024). *National Institute Of Justice*.

Wikipedia. (2024). Android (Operating System). In *Wikipedia*. Https://En.Wikipedia.Org/W/Index.Php?Title=Android_(Operating_System)&Oldid=1222725713

Wikipedia. (2024). Uc Browser. In *Wikipedia Bahasa Indonesia, Ensiklopedia Bebas*. Https://Id.Wikipedia.Org/W/Index.Php?Title=Uc_Browser&Oldid=25613492

Yessy. (2024). *Mengenal Aplikasi Bloatware, Bawaan Dari Ponsel*. Fortuneidn.Com. From Https://Www.Fortuneidn.Com/Tech/Yessy/Aplikasi-Bloatware-Adalah

Yuliana, D., Yuniati, T., & Parga Zen, B. (2023). Analisis Forensik Terhadap Kasus Cyberbullying Pada Instagram dan Whatsapp Menggunakan Metode National Institute Of Justice (Nij). *Cyber Security Dan Forensik Digital*, *5*(2), 52–59. Https://Doi.Org/10.14421/Csecurity.2022.5.2.3734