IMPLEMENTASI CUSTOM RECOVERY BOOT SEBAGAI SOLUSI FORENSIK DIGITAL UNTUK EKSTRAKSI DATA PADA PERANGKAT ANDROID YANG TERKUNCI

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

disusun oleh

NUR WAHID ROBIANSYAH

19.83.0355

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

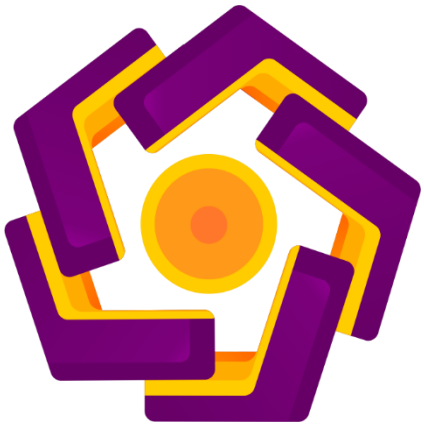
2025

IMPLEMENTASI CUSTOM RECOVERY BOOT SEBAGAI SOLUSI FORENSIK DIGITAL UNTUK EKSTRAKSI DATA PADA PERANGKAT ANDROID YANG TERKUNCI

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer



disusun oleh

NUR WAHID ROBIANSYAH

19.83.0355

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2025

HALAMAN PERSETUJUAN

SKRIPSI

IMPLEMENTASI CUSTOM RECOVERY BOOT SEBAGAI SOLUSI FORENSIK DIGITAL UNTUK EKSTRAKSI DATA PADA PERANGKAT ANDROID YANG TERKUNCI

yang disusun dan diajukan oleh

NUR WAHID ROBIANSYAH

19.83.0355

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 19 Februari 2025

Dosen Pembimbing,

M. RUDYANTO ARIEF, S.T, M.T
NIK. 190302098

HALAMAN PENGESAHAN

SKRIPSI

IMPLEMENTASI CUSTOM RECOVERY BOOT SEBAGAI SOLUSI FORENSIK DIGITAL UNTUK EKSTRAKSI DATA PADA PERANGKAT ANDROID YANG TERKUNCI

yang disusun dan diajukan oleh

NUR WAHID ROBIANSYAH

19.83.0355

Telah dipertahankan di depan Dewan Penguji
pada tanggal 19 Februari 2025

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Donni Prabowo, S.Kom., M.Kom **NIK. 190302253**	
Melwin Syafrizal, S.Kom., M.Eng., Ph.D. **NIK. 190302105**	
Muhammad Rudyanto Arief, S.T., M.T **NIK. 190302098**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 12 Juni 2025

DEKAN FAKULTAS ILMU KOMPUTER

Prof. Dr. Kusrini, S.Kom., M.Kom.
NIK. 190302106

iii

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : NUR WAHID ROBIANSYAH
NIM : 19.83.0355

Menyatakan bahwa Skripsi dengan judul berikut:

IMPLEMENTASI CUSTOM RECOVERY BOOT SEBAGAI SOLUSI FORENSIK DIGITAL UNTUK EKSTRAKSI DATA PADA PERANGKAT ANDROID YANG TERKUNCI

Dosen Pembimbing : M. RUDYANTO ARIEF, S.T, M.T

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 19 Februari 2025

Yang Menyatakan,

NUR WAHID ROBIANSYAH

HALAMAN PERSEMBAHAN

Pertama saya ucapkan rasa sykur kepada Allah Swt atas selesainya naskah skripsi ini dengan baik dan lancer. Dan skripsi ini saya persembahkan untuk :

1. Orang tua saya Bapak Sugeng dan Ibu Sri Sulastri yang senantiasa memberikan dukungan kasih sayang, mendoakan, serta dukungan moral dan materi tanpa henti. Terima kasih atas segala pengorbanan dan semangat yang telah diberikan selama ini.
2. Adik saya Abimanyu Adi Pamungkas yang memberi dorongan semangat kepada saya dalam mengerjakan skripsi ini.
3. Bapak Dosen Muhammad Rudyanto Arief, S.T, M.T. selaku Dosen pembimbing saya yang dengan sabar berbagi ilmu, memberikan bimbingan, serta membentuk saya menjadi pribadi yang lebih baik dalam memahami bidang ilmu ini.
4. Seluruh dosen prodi TEKNIK KOMPUTER yang telah memberi ilmu serta mengarahkan saya hingga di titik sekarang.
5. Tommy Frenlie Boseren, Aliyudi Risal, Afra Nida Ahnaf, Angga Ardiakto, Atiqah Suci Ramadhanti, serta teman-teman lainnya yang tidak bisa saya sebutkan satu persatu yang sudah memberikan arahan serta dukungan untuk menyelesaikan skripsi ini.

KATA PENGANTAR

Puji dan syukur ke hadirat Allah Swt atas rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan skripsi yang berjudul "Meningkatkan Investigasi Forensik Digital dalam Serangan Buffer Overflow pada Database Situs Web : Pendekatan Forensik Langsung " sebagai salah satu syarat untuk memperoleh gelar Sarjana pada Prodi S1 Teknik Komputer, Universitas AMIKOM Yogyakarta.

Penulisan skripsi ini bertujuan untuk memberikan wawasan mengenai Forensik Digital. Penulis menyadari bahwa penyusunan skripsi ini tidak terlepas dari bantuan dan dukungan berbagai pihak. Oleh karena itu, penulis ingin menyampaikan terima kasih kepada:

1. Prof. Dr. M. Suyanto, M.M, selaku Rektor Universitas Amikom Yogyakarta.
2. Dr. Dony Ariyus, S.S, M.Kom, selaku Kaprodi Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.
3. Muhammad Rudyanto Arief, S.T, M.T, selaku pembimbing yang telah memberikan bimbingan, arahan, dan masukan selama proses penyusunan skripsi ini.
4. Segenap Dosen Fakultas Ilmu Komputer yang telah mendidik dan memberikan ilmu selama masa kuliah dan seluruh staf yang selalu sabar dan melayani segala administrasi selama proses penelitian ini.
5. Semua pihak yang telah membantu dan tidak dapat disebutkan satu persatu.

Semoga segala kebaikan dan pertolongan semuanya mendapat berkah dari Allah Swt. Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Oleh karena itu, segala saran dan kritik yang membangun sangat diharapkan demi perbaikan di masa mendatang. Semoga penelitian ini dapat memberikan manfaat bagi pembaca dan pengembangan ilmu di bidang Digital Forensik.

Yogyakarta, 16 Februari 2025

Nur Wahid Robiansyah

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Investigasi forensik digital menghadapi tantangan besar akibat tingginya biaya serta keterbatasan lisensi alat forensik komersial. Selain itu, fitur keamanan pada perangkat Android modern, seperti enkripsi data dan Factory Reset Protection (FRP), semakin menyulitkan proses ekstraksi data dari perangkat yang terkunci. Penelitian ini bertujuan untuk mengembangkan metode alternatif dalam pengambilan data forensik menggunakan custom recovery boot (TWRP) sebagai solusi untuk mengakses dan memperoleh data dari perangkat Android tanpa bergantung pada alat forensik berbayar.

Metode penelitian ini berbasis simulasi dengan mempertimbangkan berbagai keterbatasan teknis, seperti kerusakan port micro-USB, tombol fisik yang tidak berfungsi, serta penguncian layar dan FRP. Proses penelitian melibatkan flashing TWRP, pengambilan file cadangan (backup), serta analisis integritas data melalui verifikasi nilai hash. Hasil penelitian menunjukkan keberhasilan pemulihan data sebesar 1,95GB, yang terdiri dari 685 foto (748MB), 48 video (652MB), 57 dokumen (226MB), dan 71 file audio (324MB). Beberapa foto,video dan audio yang berhasil dipulihkan mengandung bukti penting terkait kejadian yang terjadi dua hari sebelum dugaan tindak kejahatan, termasuk keberadaan individu yang terakhir terlihat bersama korban.

Penelitian ini memberikan kontribusi dalam bidang forensik digital mobile dengan menyediakan metode alternatif untuk mengakses perangkat Android yang terkunci tanpa menggunakan perangkat lunak komersial yang mahal. Selain itu, penelitian ini memastikan keabsahan data melalui verifikasi nilai hash, yang menjaga integritas barang bukti digital. Hasil penelitian ini dapat dimanfaatkan oleh peneliti forensik independen, lembaga penegak hukum, akademisi dalam bidang keamanan siber, serta profesional forensik digital dalam menangani kasus-kasus investigasi mobile tanpa keterbatasan alat komersial. Dengan metode yang lebih ekonomis dan efektif ini, diharapkan forensik digital dapat lebih mudah diakses dan diterapkan dalam berbagai skenario investigasi.

Kata kunci : *Forensik digital, TWRP, Factory Reset Protection (FRP), ekstraksi data, keamanan Android.*

ABSTRACT

Digital forensic investigations face major challenges due to the high cost and license limitations of commercial forensic tools. In addition, security features on modern Android devices, such as data encryption and Factory Reset Protection (FRP), further complicate the process of data extraction from locked devices. This research aims to develop an alternative method for forensic data retrieval using custom recovery boot (TWRP) as a solution to access and obtain data from Android devices without relying on paid forensic tools.

The research method is simulation-based, taking into account various technical limitations, such as micro-USB port damage, non-functional physical buttons, and screen and FRP locking. The research process involved flashing TWRP, retrieving backup files, and analyzing data integrity through hash value verification. The results showed successful recovery of 1.95GB of data, consisting of 685 photos (748MB), 48 videos (652MB), 57 documents (226MB) and 71 audio files (324MB). Some of the recovered photos,videos, and audio contained important evidence related to events that occurred two days prior to the alleged crime, including the whereabouts of individuals last seen with the victim.

This research contributes to the field of mobile digital forensics by providing an alternative method to access locked Android devices without using expensive commercial software. In addition, this research ensures data validity through hash value verification, which maintains the integrity of digital evidence. The results of this research can be utilized by independent forensic researchers, law enforcement agencies, academics in the field of cybersecurity, and digital forensics professionals in handling mobile investigation cases without the limitations of commercial tools. With this more economical and effective method, it is expected that digital forensics can be more accessible and applied in various investigation scenarios.

Keyword : *Digital forensics, TWRP, Factory Reset Protection (FRP), data extraction, Android security.*