

**IDENTIFIKASI BUKTI DIGITAL WHATSAPP
PADA SMARTPHONE ANDROID
DENGAN MENGGUNAKAN
METODE ANDROID BACKUP
APPLICATION PACKAGE KIT (APK) DOWNGRADE**



TESIS

Oleh :

Deny Sulisdyantoro

55420110025

**UNIVERSITAS
MERCU BUANA**

MAGISTER TEKNIK ELEKTRO

FAKULTAS TEKNIK

UNIVERSITAS MERCU BUANA

JAKARTA

2022

PENGESAHAN TESIS

Judul : IDENTIFIKASI BUKTI DIGITAL WHATSAPP PADA
SMARTPHONE ANDROID DENGAN
MENGUNAKAN METODE ANDROID BACKUP
APPLICATION PACKAGE KIT (APK) DOWNGRADE

Nama : DENY SULISDYANTORO

NIM : 55420110025

Program Studi : MAGISTER TEKNIK ELEKTRO

Tanggal : 4 Agustus 2022

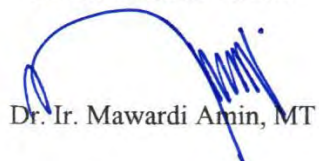
Pembimbing



Dr. Marza Ihsan Marzuki, MT

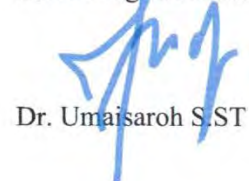
Mengesahkan:

Dekan Fakultas Teknik



Dr. Ir. Mawardi Amin, MT

Ketua Program Studi



Dr. Umairah S.ST

PERNYATAAN SIMILARITY CHECK

Saya yang bertanda tangan di bawah ini menyatakan bahwa karya ilmiah yang ditulis oleh :

Nama : Deny Sulisdyantoro
NIM : 55420110025
Program Studi : Magister Teknik Elektro

Dengan judul

“ IDENTIFIKASI BUKTI DIGITAL WHATSAPP PADA SMARTPHONE ANDROID DENGAN MENGGUNAKAN METODE ANDROID BACKUP APPLICATION PACKAGE KIT (APK) DOWNGRADE “,

Telah dilakukan pengecekan *similarity* dengan sistem Turnitin pada tanggal 28 Juli 2022, didapatkan nilai persentase sebesar 22%.

Jakarta, Agustus 2022

Administrator Turnitin



Miyono, S.Kom

PERNYATAAN

Saya yang bertanda tangan di bawah ini menyatakan dengan sebenar-benarnya bahwa semua pernyataan dalam Tesis ini :

Judul : Identifikasi Bukti Digital WhatsApp pada Smartphone
Android dengan menggunakan Metode Android Backup
Application Package Kit (APK) Downgrade

Nama : Deny Sulisdyantoro

NIM : 55420110025

Program Studi : Magister Teknik Elektro

Tanggal : 29 Juli 2022

Merupakan hasil studi pustaka, penelitian lapangan dan karya saya sendiri dengan bimbingan Dosen Pembimbing yang ditetapkan dengan Surat Tugas Ketua Program Studi Magister Teknik Elektro nomor 09-4/660/F-STT/V/2021 tanggal 22 Mei 2021.

Karya Ilmiah ini belum pernah diajukan untuk memperoleh gelar kesarjanaan pada program sejenis di perguruan tinggi lain. Semua informasi, data, hasil pengolahannya yang digunakan, telah dinyatakan secara jelas sumbernya dan dapat diperiksa kebenarannya.

Jakarta, 1 Agustus 2022



The image shows a 10,000 Indonesian Rupiah postage stamp. The stamp features the Garuda Pancasila emblem and the text 'SEPULUH RIBU RUPIAH', '10000', 'METERA TEMPEL', and 'E2EAJX897562407'. A handwritten signature in black ink is written over the stamp.

Deny Sulisdyantoro

KATA PENGANTAR

Puji syukur kehadirat Allah swt., atas segala limpahan rahmat dan karunia-Nya, sehingga Tesis ini dapat diselesaikan tepat pada waktunya. Shalawat serta Salam kepada Nabi Besar Rasulullah Muhammad saw, yang telah membawa cahaya Iman dan Islam dari jaman kegelapan sehingga di Hari Akhir nanti kita akan mendapat syafa'atnya, aamiin ya Robbal 'Alamin.

Terima kasih tak terhingga juga penulis ucapkan kepada berbagai pihak, yaitu :

1. Rektor Universitas Mercu Buana, Bapak Prof. Dr. Ngadino Surip, MS yang telah memberikan kesempatan kepada penulis untuk belajar dan berjuang di Universitas Mercu Buana.
2. Dekan Fakultas Teknik Universitas Mercu Buana, Bapak Dr. Ir. Mawardi Amin, MT yang telah memberikan sarana dan prasarana untuk belajar dan berjuang.
3. Ketua Program Studi Pascasarjana Magister Teknik Elektro Universitas Mercu Buana, Ibu Dr. Umairah, S.ST. dengan segala kebijaksanaan.
4. Dosen Pembimbing Tesis, Bapak Dr. Marza Ihsan Marzuki, MT atas segala arahan, pencerahan, bimbingan, support, motivasi, ilmu, kesabaran dan kebaikannya.
5. Belahan Jiwaku miumiu mylopelope, Aisyah Belajam, atas curahan cinta dan kasih sayangnya.
6. Para Jagoanku, MS.Riyadh, MS.Izzat dan MZ.Fayyadh agar menjadi motivasi kalian untuk terus belajar dan berjuang.
7. Alm. Ananda MS.Walid, yang telah mendahului kami dalam Jannah-NYA.

8. Serta seluruh keluarga baik Ibu, Bapak, dan adik serta para pihak yang tidak dapat penulis sebutkan satu per satu, namun tidak mengurangi rasa hormat penulis karena telah mencurahkan segenap perhatian dan dukungan baik moril maupun materil.

Penulis sangat mengharapkan saran, pencerahan, kritikan dan masukan yang membangun dari semua pihak guna mendekati sempurnanya tesis ini. Akhir kata, penulis sampaikan terima kasih tak terhingga kepada semua pihak yang telah berkontribusi dalam penyusunan Tesis ini dari awal hingga akhir.

Bogor, Agustus 2022

dsulisdyantoro



UNIVERSITAS
MERCU BUANA

DAFTAR ISI

PENGESAHAN TESIS	i
PERNYATAAN SIMILARITY CHECK.....	ii
PERNYATAAN.....	iii
KATA PENGANTAR	iv
DAFTAR ISI.....	vi
DAFTAR GAMBAR	viii
DAFTAR TABEL.....	xi
ABSTRACT.....	xii
ABSTRAK	xiii
BAB I	1
A. Latar Belakang	1
B. Rumusan Masalah	7
C. Tujuan Penelitian	8
D. Sasaran dan Kontribusi Penelitian	8
E. Batasan Masalah.....	9
BAB II.....	10
A. Penelitian Terdahulu	10
B. Forensik Digital.....	15
C. Mobile Forensic	17
D. Sistem Operasi Android.....	19
E. Aplikasi WhatsApp.....	21
F. Struktur File dan <i>Database</i> WhatsApp.....	23
G. Ekstraksi <i>file system</i>	26
H. Metode Android Backup.....	27
I. Metode Android Backup APK Downgrade.....	28
J. Nilai Hash.....	29
BAB III	32
A. Studi Pustaka.....	32
B. Metodologi Rujukan NIST.....	32

C. Model Penelitian	36
D. Penyusunan Skenario	37
E. Akuisisi.....	38
F. Analisis	39
BAB IV	40
A. Simulasi.....	40
B. Tahapan <i>Collection</i>	40
C. Tahapan Examination.....	42
D. Tahapan Analysis.....	47
E. Tahapan Reporting	63
F. Pembuktian Nilai Hash.....	66
G. Recovery file/data yang dihapus.....	67
BAB V.....	69
A. Kesimpulan	69
B. Saran.....	70
DAFTAR PUSTAKA	72
LAMPIRAN.....	74
Laporan Hasil Akuisisi dan Ekstraksi	74

UNIVERSITAS
MERCU BUANA

DAFTAR GAMBAR

Gambar 1.1 Statistik Pengguna WhatsApp

Gambar 2.1 Diagram Venn penelitian terdahulu

Gambar 2.2 Arsitektur Android

Gambar 2.3 Struktur File/Folder WhatsApp

Gambar 2.4 File/folder Backups pada WhatsApp

Gambar 2.5 File/folder Media pada WhatsApp

Gambar 2.6 File/folder *Databases* pada WhatsApp

Gambar 2.7 Struktur *Database* WhatsApp

Gambar 3.1 Metodologi Digital Forensic NIST

Gambar 3.2 Skenario dalam investigasi bukti digital WhatsApp

Gambar 3.3 Model Penelitian Forensik Digital pada WhatsApp Android

Gambar 4.1 Deteksi Awal Smartphone Samsung Galaxy Note 9

Gambar 4.2 Proses Akuisisi dan Ekstraksi pada smartphone Android Samsung

Gambar 4.3 Setting Parameter pada Smartphone Android

Gambar 4.4 Proses Akuisisi dengan Metode Android Backup

Gambar 4.5 File list hasil akuisisi Metode Android Backup

Gambar 4.6 Proses Temporary Downgrading WhatsApp

Gambar 4.7 File list hasil akuisisi Metode Android Backup APK Downgrade

Gambar 4.8 Nilai Hash akuisisi Metode Android Backup

Gambar 4.9 Nilai Hash akuisisi Metode Android Backup APK Downgrade

Gambar 4.10 Proses Downgrading APK WhatsApp dengan FINALExtractor

Gambar 4.11 Hasil Akuisisi dengan Metode Android Backup

Gambar 4.12 Hasil Akuisisi dengan Metode Android Backup APK Downgrade

Gambar 4.13 File System hasil ekstraksi WhatsApp.db

Gambar 4.14 Kontak WhatsApp pada Hexview

Gambar 4.15 Percakapan WhatsApp pada Hexview

Gambar 4.16 Analisis Data pada kategori Call Log

Gambar 4.17 Analisis Data pada kategori Chats

Gambar 4.18 Analisis Data pada kategori Contacts

Gambar 4.19 Analisis Data pada kategori Cookies

Gambar 4.20 Analisis Data pada kategori Device Locations

Gambar 4.21 Analisis Data pada kategori Installed Applications

Gambar 4.22 Analisis Data pada kategori Searched Items

Gambar 4.23 Analisis Data pada kategori User Accounts

Gambar 4.24 Analisis Data pada kategori Web History

Gambar 4.25 Analisis Data pada kategori Applications

Gambar 4.26 Analisis Data pada kategori Archives

Gambar 4.27 Analisis Data pada kategori Audio

Gambar 4.28 Analisis Data pada kategori *Databases*

Gambar 4.29 Analisis Data pada kategori Documents

Gambar 4.30 Analisis Data pada kategori Exchange

Gambar 4.31 Analisis Data pada kategori Images

Gambar 4.32 Analisis Data pada kategori Text

Gambar 4.33 Analisis Data pada kategori Uncategorized

Gambar 4.34 Analisis Data pada kategori Videos

Gambar 4.35 Deleted data

Gambar 4.36 Grafik perbandingan hasil ekstraksi

Gambar 4.37 Report Dataset dengan metode Android Backup

Gambar 4.38 Report Dataset dengan metode Android Backup APK Downgrade

Gambar 4.39 Chat WhatsApp dalam bentuk tautan file.txt

Gambar 4.40 Cuplikan Chat WhatsApp dalam PDF Report

Gambar 4.41 Timestamp file video

Gambar 4.42 Nilai hash file video

Gambar 4.43 Timestamp dan nilai hash file pdf dokumen

Gambar 4.44 Recovery data komunikasi teks WhatsApp

Gambar 4.45 File dokumen komunikasi WhatsApp yang gagal direcovery



UNIVERSITAS
MERCU BUANA

DAFTAR TABEL

Tabel 1. Perbandingan Penelitian Terdahulu

Tabel 2. Perangkat Simulasi

Tabel 3. Evidence Penelitian

Tabel 4. Perbandingan hasil akuisisi dan ekstraksi

Tabel 5. Persentase hasil akuisisi dan ekstraksi

