# ANALISIS FORENSIK TERHADAP DATABASE SQLITE PADA APLIKASI MICHAT BERBASIS ANDROID

**SKRIPSI**


Disusun oleh:

**M. HAZRI**
**17.83.0009**



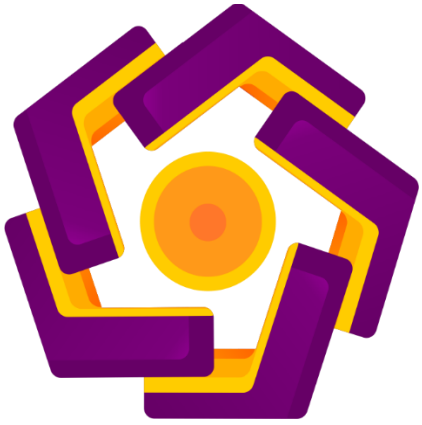
**PROGRAM SARJANA**
**PROGRAM STUDI TEKNIK KOMPUTER**
**FAKULTAS ILMU KOMPUTER**
**UNIVERSITAS AMIKOM YOGYAKARTA**
**YOGYAKARTA**


**2022**

# ANALISIS FORENSIK TERHADAP DATABASE SQLITE PADA APLIKASI MICHAT BERBASIS ANDROID

## SKRIPSI

Diajukan kepada Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta
untuk memenuhi salah satu syarat memperoleh gelar Sarjana Komputer
Pada Jenjang Program Sarjana – Program Studi Teknik Komputer




Disusun oleh:

**M. HAZRI**
**17.83.0009**


**PROGRAM SARJANA**
**PROGRAM STUDI TEKNIK KOMPUTER**
**FAKULTAS ILMU KOMPUTER**
**UNIVERSITAS AMIKOM YOGYAKARTA**
**YOGYAKARTA**
**2022**

# HALAMAN PERSETUJUAN

## SKRIPSI

**ANALISIS FORENSIK TERHADAP DATABASE SQLITE PADA APLIKASI MICHAT BERBASIS ANDROID**

yang dipersiapkan dan disusun oleh

**M. HAZRI**

**17.83.0009**

Telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 09 Desember 2020

**Dosen Pembimbing,**

**Melwin Syafrizal, S.Kom., M.Eng.**
**NIK. 190302105**

# HALAMAN PENGESAHAN

## SKRIPSI

### ANALISIS FORENSIK TERHADAP DATABASE SQLITE PADA APLIKASI MICHAT BERBASIS ANDROID

yang dipersiapkan dan disusun oleh

**M. HAZRI**

**17.83.0009**

Telah dipertahankan di depan Dewan Penguji
pada tanggal 23 Juni 2022

**Susunan Dewan Penguji**

| **Nama Penguji** | **Tanda Tangan** |
|---|---|
| **Melwin Syafrizal, S.Kom., M.Eng.**<br>**NIK. 190302105** | |
| **Wahid Miftahul Ashari, S.Kom., M.T**<br>**NIK. 190302452** | |
| **Rini Indrayani, ST, M.Eng**<br>**NIK. 190302417** | |

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 23 Juni 2022

**DEKAN FAKULTAS ILMU KOMPUTER**

**Hanif Al Fatta,S.Kom., M.Kom.**
**NIK. 190302096**

## HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

**Nama mahasiswa : M. HAZRI**
**NIM : 17.83.0009**

Menyatakan bahwa Skripsi dengan judul berikut:

**ANALISIS FORENSIK TERHADAP DATABASE SQLITE PADA APLIKASI MICHAT BERBASIS ANDROID**

Dosen Pembimbing : Melwin Syafrizal, S.Kom., M.Eng.

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, Kamis 23 Juni 2022

Yang Menyatakan,


M. HAZRI

## HALAMAN MOTTO

"Jika kamu tidak sanggup menahan lelahnya belajar maka kamu harus sanggup menahan perihnya kebodohan"

**(Imam Syafi'i)**

"Do not pray for an easy life, pray for the strength to endure a difficult one"

**(Bruce Lee)**

## HALAMAN PERSEMBAHAN

Segala puji bagi Allah SWT atas limpahan rahmat dan hidayah serta karunia-Nya sehingga skripsi ini selesai dengan sebaik-baiknya. Skripsi ini saya persembahkan untuk :

1. Kedua orang tua, Bapak Abdul Azam dan Ibu Husnayani yang selalu mendoa'kan, memberi dukungan, fasilitas serta memberikan hasil kerja kerasnya kepada saya.
2. Bapak Melwin Syafrizal, S.Kom., M.Eng. Selaku dosen pembimbing yang telah membantu dalam penyusunan skripsi ini.
3. Kepada kakak saya Nizamuddin yang selalu memberikan semangat dan dukungan.
4. Kepada istri saya Widiatul Islamiyah yang selalu memberikan dukungan mental, semangat serta selalu sabar menemani dalam menyelesaikan skripsi saya.
5. Kepada sahabat dan teman-teman yang ada disaat suka maupun duka selama masa perkuliahan saya.

## KATA PENGANTAR

Puji dan syukur kami panjatkan kehadirat Tuhan Yang Maha Esa atas karunia yang telah dianugerahkan kepada penulis, sehingga penulis dapat menyelesaikan skripsi yang berjudul "Analisis Forensik Terhadap Database Sqlite Pada Aplikasi Michat Berbasis Android".

Skripsi ini disusun sebagai syarat memperoleh gelar Sarjana Komputer pada program Studi S1 Teknik Komputer Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.

Penulis menyadari bahwa tanpa bantuan dan bimbingan dari berbagai pihak, skripsi ini tidak mungkin dapat terselesaikan. Oleh karena itu, penulis menyampaikan terima kasih kepada :

1. Allah SWT karena atas karunia-Nya, sehingga penulis dapat menyelesaikan skripsi ini dengan baik dan semoga dapat memberikan mamfaat di kemudian hari.
2. Bapak Prof. Dr. M. Suyanto, M.M. selaku Rektor Universitas AMIKOM Yogyakarta.
3. Bapak Dony Ariyus, M.Kom. selaku Ketua Program Studi S1 Teknik Komputer Universitas AMIKOM Yogyakarta.
4. Bapak Melwin Syafrizal, S.Kom., M.Eng. selaku Dosen Pembimbing yang telah bersedia memberikan pengarahan dan bimbingan dalam penyususnan Skripsi ini.
5. Segenap Dosen, Staff, dan Karyawan Universitas AMIKOM Yogyakarta yang telah memberikan ilmu kepada penulis di bangku kuliah dan juga membantu penulis dalam kelancaran administrasi sampai terselesaikannya Skripsi ini.
6. Orang tua, saudara-saudara beserta keluarga yang selalu mendoakan dan memberikan dukungan penuh kepada penulis.
7. Serta kepada semua pihak yang telah membantu dalam penyusunan Skripsi ini yang tidak dapat penulis sebutkan satu per satu.

Penulis berharap semoga skripsi ini dapat bermamfaat bagi semua pihak yang terkait dalam penulisan ini. Dalam penulisan skripsi ini penulis menyadari masih banyak kekurangan karena terbatasnya pengetahuan dan pengalaman penulis. Karena itu, dengan lapang hati penulis mengharapkan kritik dan saran yang membangun guna menyempurnakan skripsi ini.

Yogyakarta, Kamis 23 Juni 2022

Penulis

**DAFTAR ISI**

HALAMAN JUDUL ..... ii
HALAMAN PERSETUJUAN ..... iii
HALAMAN PENGESAHAN ..... iv
HALAMAN MOTTO ..... vi
HALAMAN PERSEMBAHAN ..... vii
KATA PENGANTAR ..... viii
DAFTAR ISI ..... x
DAFTAR TABEL ..... xii
DAFTAR GAMBAR ..... xiii
INTISARI ..... xiv
*ABSTRACT* ..... xv
BAB I PENDAHULUAN ..... 1
1.1 Latar Belakang Masalah ..... 1
1.2 Rumusan Masalah ..... 2
1.3 Batasan Masalah ..... 2
1.4 Tujuan Penelitian ..... 2
1.5 Sistematika Penulisan ..... 3
BAB II LANDASAN TEORI ..... 4
2.1 Tinjauan Pustaka ..... 4
*2.2 Smartphone Android* ..... 6
*2.3 Mobile Forensic* ..... 8
2.4 Akuisisi ..... 9
2.5 Bukti Digital ..... 9
2.6 Standard Operating Procedure (SOP) ..... 10
2.7 Hashing ..... 11
2.8 SQLite ..... 11
2.9 Aplikasi MiChat ..... 13
2.10 *Cybercrime* ..... 15
2.11 NIST ..... 15
2.12 ADB ..... 16
2.13 DD ..... 17
2.14 Root ..... 17
2.15 DB Browser ..... 17
2.16 File *Carving* ..... 18
2.17 *Foremost* ..... 18
BAB III METODOLOGI PENELITIAN ..... 19
3.1 Deskripsi Objek ..... 19

3.2 Alat Dan Bahan Penelitian ..... 20
3.3 Perancangan Skenario ..... 21
3.4 Metode Penelitian ..... 22
3.5 Alur investigasi ..... 23
3.6 Teknik Analasis ..... 24
3.6.1 Analasis menggunakan DB Browser ..... 24
3.6.2 Analisis dengan Teknik File *Carving* ..... 24
BAB IV PEMBAHASAN ..... 25
4.1 Persiapan ..... 25
4.1.1 Persiapan *Smartphone* Pelaku ..... 25
4.1.2 Persiapan PC Investigator ..... 28
4.1.3 Implementasi Skenario ..... 31
*4.1.3.1 Collections* ..... 32
*4.1.3.2 Examination* ..... 36
*4.1.3.3 Analysis* ..... 37
*4.1.3.4 Reporting* ..... 43
BAB V PENUTUP ..... 46
5.1 Kesimpulan ..... 46
5.2 Saran ..... 46
DAFTAR PUSTAKA ..... 47

# DAFTAR TABEL

Tabel 2.1 Penelitian Terdahulu ..... 5
Tabel 2.1 Penelitian Terdahulu (lanjutan)..... 6
Tabel 3.1 Spesifikasi *Smartphone* Pelaku..... 20
Tabel 3.2 Informasi alat untuk proses root..... 20
Tabel 3.3 Kebutuhan Perangkat Lunak..... 21
Tabel 4.1 Hasil Akuisisi..... 34
Tabel 4.2 Nilai Hash Bukti Digital ..... 36
Tabel 4.3 Direktori pada aplikasi Michat..... 36
Tabel 4.4 Detail Kontak pada *Smartphone* Pelaku ..... 39
Tabel 4.5 Riwayat chat yang berhasil ditemukan ..... 41
Tabel 4.6 Temuan Barang Bukti ..... 45

## DAFTAR GAMBAR

Gambar 2.1 Arsitektur Android ..... 7
Gambar 2.2 Arsitektur SQLite ..... 12
Gambar 2.3 MiChat di Playstore ..... 13
Gambar 2.4 Informasi Tambahan dari aplikasi MiChat ..... 14
Gambar 2.5 Metode NIST ..... 15
Gambar 3.1 Putusan Mahkamah Agung Republik Indonesia Tahun 2021 ..... 19
Gambar 3.2 Tahap Persiapan Lingkungan Penelitian ..... 21
Gambar 3.3 Skenario Penelitian ..... 21
Gambar 3.4 Penelitian Metode NIST ..... 22
Gambar 3.5 Alur Investigasi ..... 23
Gambar 3.6 Analisis menggunakan DB Browser ..... 24
Gambar 3.7 Teknik Analisa file *carving* ..... 24
Gambar 4.1 Aplikasi Root *Smartphone* ..... 25
Gambar 4.2 USB Debugging dan Unlock Bootloader Aktif ..... 26
Gambar 4.3 Proses instalasi custom recovery ..... 26
Gambar 4.4 Proses Instalasi Lazyflasher ..... 27
Gambar 4.5 Proses instalasi Magisk ..... 27
Gambar 4.6 Root Checker ..... 28
Gambar 4.7 FTK Imager berhasil terinstal ..... 28
Gambar 4.8 Pengaturan path environment ..... 29
Gambar 4.9 Executable tool dd ..... 29
Gambar 4.10 Windows subsystem for linux ..... 30
Gambar 4.11 Kali linux on Windows ..... 30
Gambar 4.12 Instalasi tool *foremost* ..... 31
Gambar 4.13 Transaksi antara Bandar dan Pemakai ..... 31
Gambar 4.14 Akuisisi microSD ..... 32
Gambar 4.15 Pengaturan lokasi penyimpanan dan output file akuisisi ..... 33
Gambar 4.16 Proses akusisi berlangsung ..... 33
Gambar 4.17 File hasil Akuisisi ..... 33
Gambar 4.18 Proses Duplikat Data Image Menggunakan Tool dd ..... 35
Gambar 4.19 File Hasil Imaging Data Image ..... 35
Gambar 4.20 Hasil Nilai Hash pada File asli dan Duplikat ..... 35
Gambar 4.21 Hasil Ekstraksi Barang Bukti Digital ..... 36
Gambar 4.22 Isi dari direktori *Databases* ..... 37
Gambar 4.23 Struktur database file 5164791249075200social.db ..... 38
Gambar 4.24 Tabel Account ..... 39
Gambar 4.25 Daftar Kontak pada Hp Pelaku ..... 39
Gambar 4.26 Tabel Messages ..... 40
Gambar 4.27 Tabel *Uploaded Contacs* ..... 41
Gambar 4.28 Ekstraksi *Carving* Menggunakan Tool *Foremost* ..... 42
Gambar 4.29 Hasil Ekstraksi Menggunakan Tool *Foremost* ..... 42
Gambar 4.30 File Gambar yang diperoleh dengan *Carving* ..... 43
Gambar 4.31 Hasil *Report* Tool FTK Imager ..... 44

# INTISARI

Kebutuhan internet pada saat sekarang ini terbilang sangat tinggi. Apalagi pada masa pandemi Covid-19 ini memaksa orang-orang untuk tidak keluar rumah, baik untuk bekerja, kuliah, ataupun berkumpul dengan kerabat jauh. Sosial media adalah salah satu sarana untuk bisa berinteraksi dengan orang lain tanpa harus bertatap muka langsung kapanpun dan dimanapun selama masih ada koneksi internet. *Instant Messaging* adalah proses pengiriman atau bertukar pesan dari perangkat seluler satu ke yang lainnya melalui jaringan internet. Investigator forensik sering melakukan analisis terhadap aplikasi *instant messaging* pada perangkat seluler.

Pada tugas akhir ini akan berfokus melakukan analisis forensik *instant messaging* terhadap aplikasi MiChat berbasis android. Pengujian akan dilakukan menggunakan sebuah *smartphone* Xiaomi Redmi Note 4X yang disimulasikan sebagai barang bukti. Skenario yang dibuat dengan memasangkan aplikasi MiChat pada *smartphone* android dan melakukan pengiriman pesan teks, gambar dan audio. Penelitian akan dimulai dari proses *Collection* atau pengumpulan data, selanjutnya dilakukan proses *examination* atau pengolahan data, kemudian dilanjutkan dengan proses analisis data dan yang terakhir proses *reporting* atau membuat laporan dari data yang sudah di analisis. Metode *collection, examination, analysis* dan *reporting* merupakan rekomendasi dari NIST yang menggunakan 4 langkah kegiatan *forensic*.

Hasil pengujian dan anlisa yang dilakukan peneliti pada database sqlite aplikasi Michat berhasil memperoleh bukti digital berupa riwayat chat menggunakan tool DB Browser dan dengan teknik *carving* menggunakan tool foremost peneliti juga berhasil memeperoleh barang bukti berupa file gambar (jpg, png, gif) dan audio.

**Kata kunci :** forensik, android, instant messenger, michat

## *ABSTRACT*

*The need for the internet at this time is very high. Especially during the Covid-19 pandemic, forcing people not to leave the house, either to work, study, or gather with distant relatives. Social media is a means to be able to interact with other people without having to meet face to face anytime and anywhere as long as there is an internet connection. Instant Messaging is the process of sending or exchanging messages from one mobile device to another via the internet. Forensic investigators often perform analysis of instant messaging applications on mobile devices.*

*This final project will focus on analyzing instant messaging forensics on the Android-based MiChat application. The test will be carried out using a simulated Xiaomi Redmi Note 4X smartphone as evidence. A scenario created by installing the MiChat application on an android smartphone and sending text, image and audio messages. The research will start from the collection process or data collection, then the examination process or data processing is carried out, then continued with the data analysis process and finally the reporting process or making a report from the data that has been analyzed. The method of collection, examination, analysis and reporting is a recommendation from NIST which uses 4 steps of forensic activities.*

*The results of testing and analysis carried out by researchers on the sqlite database of the Michat application succeeded in obtaining digital evidence in the form of chat history using the DB Browser tool and with carving techniques using the foremost tool, the researchers also succeeded in obtaining evidence in the form of image files (jpg, png, gif) and audio.*


***Keyword:*** *forensic, android, instant messanging, michat*