# ANALISA PERBANDINGAN EFEKTIFITAS LIVE FORENSIC DAN DISK FORENSIK PADA INVESTIGASI BUKTI DIGITAL WHATSAPP WEB

**SKRIPSI**

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer


Disusun oleh:

**RACHMAT WAHYUDI**

**18.83.0233**


Kepada


**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS AMIKOM YOGYAKARTA**

**YOGYAKARTA**


**2024**

# ANALISA PERBANDINGAN EFEKTIFITAS LIVE FORENSIC DAN DISK FORENSIK PADA INVESTIGASI BUKTI DIGITAL WHATSAPP WEB

**SKRIPSI**

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi S1 Teknik Komputer


disusun oleh

**RACHMAT WAHYUDI**

**18.83.0233**


Kepada


**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS AMIKOM YOGYAKARTA**

**YOGYAKARTA**


**2024**

## HALAMAN PERSETUJUAN

# SKRIPSI

## ANALISA PERBANDINGAN EFEKTIFITAS LIVE FORENSIC DAN DISK FORENSIK PADA INVESTIGASI BUKTI DIGITAL WHATSAPP WEB

Yang disusun dan diajukan oleh

Rachmat Wahyudi

18.83.0233

telah disetujui oleh Dosen Pembimbing Skripsi

pada tanggal 21 Februari 2024

**Dosen Pembimbing,**

**Banu Santoso, S.T., M.Eng.**

**NIK. 190302327**

## HALAMAN PENGESAHAN

## SKRIPSI

### ANALISA PERBANDINGAN EFEKTIFITAS LIVE FORENSIC DAN DISK FORENSIK PADA INVESTIGASI BUKTI DIGITAL WHATSAPP WEB

yang disusun dan diajukan oleh

**Rachmat Wahyudi**

**18.83.0233**

Telah dipertahankan di depan Dewan Penguji
pada tanggal 21 Februari 2024

**Susunan Dewan Penguji**

| Nama Penguji | Tanda Tangan |
|---|---|
| **Jeki Kuswanto, M.Kom**<br>**NIK. 190302456** | |
| **Joko Dwi Santoso, M.Kom**<br>**NIK. 190302181** | |
| **Banu Santoso, S.T., M.Eng**<br>**NIK. 190302327** | |

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 21 Februari 2024

**DEKAN FAKULTAS ILMU KOMPUTER**

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

## HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

**Nama mahasiswa : Rachmat Wahyudi**
**NIM : 18.83.0233**

Menyatakan bahwa Skripsi dengan judul berikut:
**Analisa Perbandingan Efektifitas Live Forensic dan Disk Forensic pada Investigasi Bukti Digital Whatsapp Web**

Dosen Pembimbing : Banu Santoso, S.T., 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, 21 Februari 2024

Yang Menyatakan,


Rachmat Wahyudi

## 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. Orang tua saya, yang selalu mendoa'kan, memberi dukungan, fasilitas serta memberikan hasil kerja kerasnya kepada saya.
2. Bapak, Banu Santoso, S.T., M.Eng. Selaku dosen pembimbing yang telah membantu dalam penyusunan skripsi ini.
3. Kepada sahabat dan teman-teman yang ada disaat suka maupun duka selama masa perkuliahan saya.

## KATA PENGANTAR

Puji dan syukur dipanjatkan kehadirat Tuhan Yang Maha Esa atas karunia yang telah dianugerahkan kepada penulis, sehingga penulis dapat menyelesaikan skripsi yang berjudul "Investigasi Anti Forensic Terhadap Bukti Digital USB Flashdisk dengan Metode NIST". Skripsi ini disusun sebagai syarat memperoleh gelar Sarjana Komputer pada program Studi S1 Teknik Komputer Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.

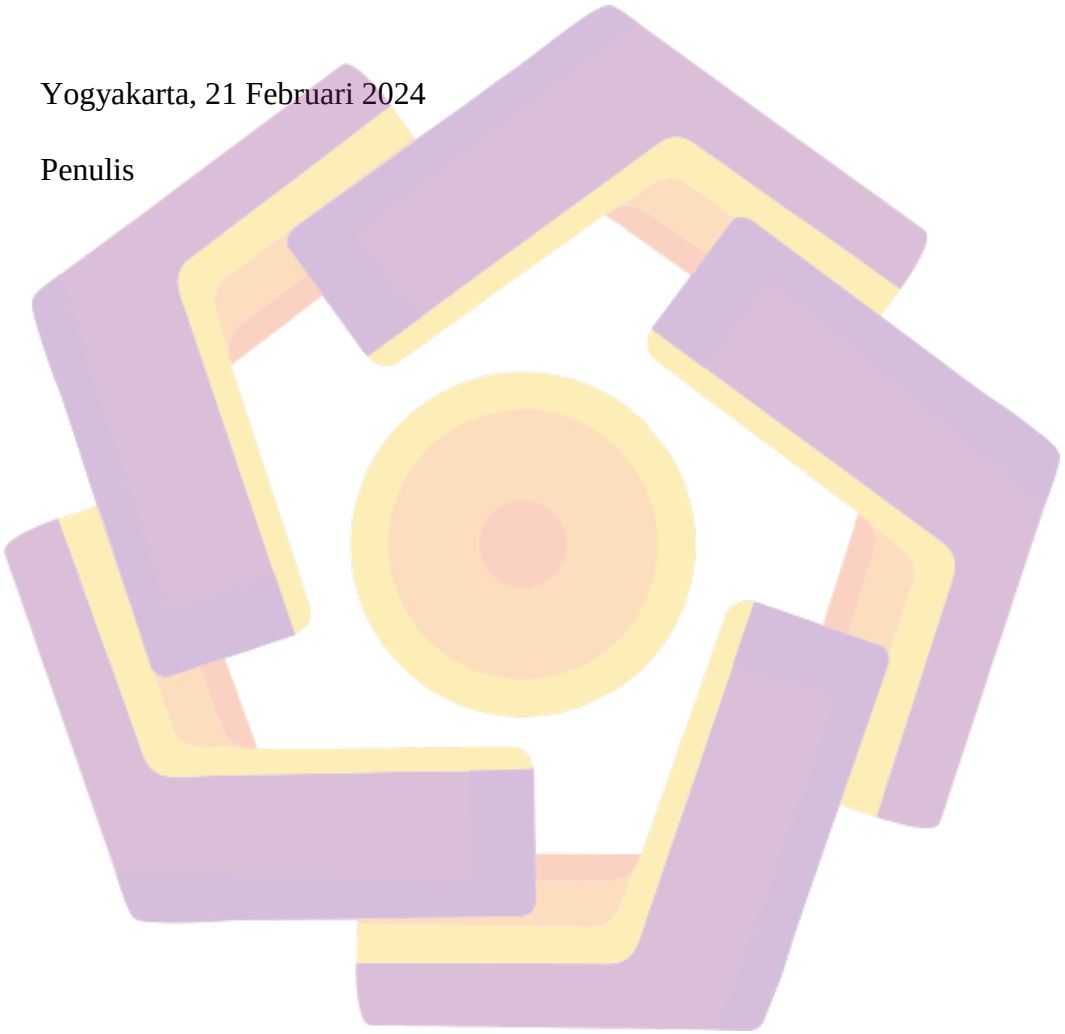
Penulis menyadari bahwa tanpa bantuan dan bimbingan dari berbagai pihak, skripsi ini tidak mungkin dapat terselesaikan. Oleh karena itu, penulis menyampaikan terima kasih kepada :

1. Allah SWT karena atas karunia-Nya, sehingga penulis dapat menyelesaikan skripsi ini dengan baik dan semoga dapat memberikan manfaat 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. Banu Santoso, S.T., 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, 21 Februari 2024

Penulis



# DAFTAR ISI

## DAFTAR TABEL

## DAFTAR GAMBAR

# INTISARI

Internet tidak hanya memberikan manfaat bagi masyarakat, namun juga dapat menimbulkan dampak negatif. Salah satunya yaitu kejahatan dunia maya. Sosial media yang sering digunakan oleh masyarakat dapat disalahgunakan untuk dijadikan sebagai media kejahatan. Salah satunya melalui sosial media yang popular di Indonesia, yaitu Whatsapp. Kasus peredaran narkoba melalui aplikasi Whatsapp sering terjadi di Indonesia, sehingga memerlukan penanganan lebih lanjut agar kasus kejahatan tersebut dapat diselesaikan dan pelaku dapat mempertanggungjawabkan perbuatannya.

Salah satu teknik nya adalah live forensic, dimana dengan teknik ini investigator memungkinkan mendapat data volatile yang tersimpan pada ram, pagefile ataupun hibernation file. Data pada memori ram menjadi sumber bukti digital yang sangat sensitif karena menyimpan banyak informasi penting ketika sistem dalam keadaan hidup (real time) seperti program yang berjalan, chat logs, network connections atau bahkan cryptographic keys. Tidak hanya live forensik, penelitian ini juga menggabungkan analisa disk forensik sebagai acuan perbandingan efektifitas. Fokus penelitian ini akan mengevaluasi dan menganalisis bukti potensial memori ram dan disk menggunakan metode National Institute of Justice (NIJ). Hasil penelitian ini adalah pembuktian temuan berbagai artefak penting dari skenario dan eksperimen sehingga dapat menjadi bukti digital yang valid dalam proses mengungkap tindak kejahatan. Berdasarkan teknik analisa live forensic dan disk forensic, hasil akhir yang diperoleh peneliti mampu membuktikan scenario aktivitas tersebut.

**Kata kunci:** *Digital Forensic, Disk Forensic, Live Forensic, Whatsapp Forensic*

## *ABSTRACT*

*The internet not only provides benefits to society, but can also have negative impacts. One of them is cyber crime. Social media that is often used by the public can be misused to be used as a medium for crime. One of them is through the popular social media in Indonesia, namely Whatsapp. Cases of drug trafficking through the Whatsapp application often occur in Indonesia, so that further handling is required so that these crime cases can be resolved and the perpetrators can be held accountable for their actions.*

*One of the techniques is live forensic, where with this technique it is possible for investigators to obtain volatile data stored in RAM, pagefile or hibernation file. Data in RAM memory is a very sensitive source of digital evidence because it stores a lot of important information when the system is on (real time) such as running programs, chat logs, network connections or even cryptographic keys. Not only live forensics, this study also incorporates disk forensic analysis as a reference for comparing effectiveness. The focus of this research will be to evaluate and analyze the potential evidence of ram and disk memory using the National Institute of Justice (NIJ) method. The result of this research is to prove the findings of various important artifacts from scenarios and experiments so that they can become valid digital evidence in the process of uncovering crimes. Based on live forensic and disk forensic analysis techniques, the final results obtained by the researcher are able to prove the activity scenario.*



***Keyword:*** *Digital Forensic, Disk Forensic, Anti Forensic*