# PERBANDINGAN PERFORMA *TOOLS LIVE FORENSIC* PADA SISTEM OPERASI WINDOWS MENGGUNAKAN METODE *NIST*

**SKRIPSI**


Disusun oleh:

**Alfat Yanuar Fitriyansyah**
**17.83.0022**

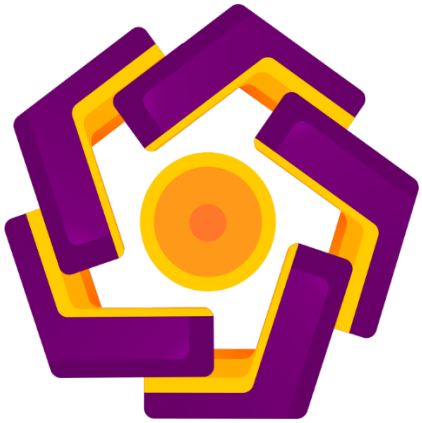


**PROGRAM SARJANA**
**PROGRAM STUDI TEKNIK KOMPUTER**
**FAKULTAS ILMU KOMPUTER**
**UNIVERSITAS AMIKOM YOGYAKARTA**
**YOGYAKARTA**
**2021**

# PERBANDINGAN PERFORMA *TOOLS LIVE FORENSIC* PADA SISTEM OPERASI WINDOWS MENGGUNAKAN METODE *NIST*

## 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:

**Alfat Yanuar Fitriyansyah**
**17.83.0022**


**PROGRAM SARJANA**
**PROGRAM STUDI TEKNIK KOMPUTER**
**FAKULTAS ILMU KOMPUTER**
**UNIVERSITAS AMIKOM YOGYAKARTA**
**YOGYAKARTA**
**2021**

# HALAMAN PERSETUJUAN
## HALAMAN PERSETUJUAN

## SKRIPSI

**PERBANDINGAN PERFORMA *TOOLS LIVE FORENSIC* PADA SISTEM OPERASI WINDOWS MENGGUNAKAN METODE NIST**

yang dipersiapkan dan disusun oleh

**Alfat Yanuar Fitriyansyah**

**17.83.0022**

Telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 6 Juni 2021

**Dosen Pembimbing,**

**Joko Dwi Santoso, M.Kom**
**NIK. 190302181**

# HALAMAN PENGESAHAN

## HALAMAN PENGESAHAN

## SKRIPSI

**PERBANDINGAN PERFORMA *TOOLS LIVE FORENSIC* PADA SISTEM OPERASI WINDOWS MENGGUNAKAN METODE NIST**

yang dipersiapkan dan disusun oleh

**Alfat Yanuar Fitriyansyah**

**17.83.0022**

Telah dipertahankan di depan Dewan Penguji
pada tanggal 22 Juni 2021

**Susunan Dewan Penguji**

| Nama Penguji | Tanda Tangan |
|---|---|
| **Joko Dwi Santoso, M.Kom**<br>**NIK. 190302181** | _____ |
| **Banu Santoso, S.T., M.Eng**<br>**NIK. 190302327** | _____ |
| **Wahyu Sukestyastama Putra, S.T., M.Eng**<br>**NIK. 190302328** | _____ |

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 22 Juni 2021

**DEKAN FAKULTAS ILMU KOMPUTER**

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

## HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

**Nama mahasiswa : Alfat Yanuar Fitriyansyah**
**NIM : 17.83.0022**

Menyatakan bahwa Skripsi dengan judul berikut:

**Perbandingan Performa *Tools Live Forensic* Pada Sistem Operasi Windows Menggunakan Metode NIST**
Dosen Pembimbing : Joko Dwi Santoso, M.Kom

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, 22 Juni 2021

Yang Menyatakan,


Alfat Yanuar Fitriyansyah

## HALAMAN MOTTO

"Usaha dan keberanian tidak cukup tanpa tujuan dan arah perencanaan."
**(JOHN F. KENNEDY)**

"Hidup itu bukan soal menemukan diri Anda sendiri, hidup itu membuat diri Anda sendiri."
**(GEORGE BERNARD SHAW)**

"Apa yang kita pikirkan menentukan apa yang akan terjadi pada kita. Jadi jika kita ingin mengubah hidup kita, kita perlu sedikit mengubah pikiran kita."
**(WAYNE DYER)**

"Tidak apa-apa untuk merayakan kesuksesan tapi lebih penting untuk memperhatikan pelajaran tentang kegagalan."
**(BILL GATES)**

"Kebahagiaan adalah disaat apa yang ada pikirkan, apa yang anda katakan, dan apa yang anda lakukan berada dalam satu keharmonian."
**(MAHATMA GANDHI)**

"Kesuksesan bukanlah kunci dari kebahagiaan. Sebaliknya kebahagiaan adalah kunci dari kesuksesan.
**(BOB DYLAN)**

## 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 Priono dan Ibu Rini Retna Ningsih yang selalu mendoa'kan, memberi dukungan, fasilitas serta memberikan hasil kerja kerasnya kepada saya.
2. Bapak Joko Dwi Santoso, M.kom. Selaku dosen pembimbing yang telah membantu dalam penyusunan skripsi ini.
3. Kepada adik saya yang selalu memberikan semangat dan dukungan.
4. 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 “Perbandingan Performa Tools Live Forensic Pada Sistem Operasi Windows Menggunakan 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 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 Joko Dwi Santoro, M.kom. 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, 4 Maret 2021

Penulis

**DAFTAR ISI**

# DAFTAR TABEL

## DAFTAR GAMBAR

# INTISARI

Salah satu teknik bidang digital forensik dalam proses mengumpulkan bukti-bukti untuk mengungkap sebuah kasus *cybercrime* yakni *live forensic*. Berbeda dengan teknik tradisional forensik, teknik *live forensic* memungkinkan investigator memperoleh data *Volatile* yang tersimpan pada memori sistem (RAM). Terdapat banyak artefak sensitif dapat diperoleh menggunakan teknik live forensic.

Pada penelitian ini, penulis akan menganalisis berbagai bukti potensial yang terdapat pada RAM dengan skenario yang sudah dibuat menggunakan metodologi *National Institute of Standards Technology (NIST).* Metodologi ini dipilih karena kerangka prosedur yang cocok untuk diterapkan pada penanganan insiden secara lebih efektif dalam banyak kasus *live forensic*. Penelitian ini berfokus pada evaluasi perbandingan performa 3 *tool open-source live forensic* dalam menganalisis beberapa bukti yang telah ditemukan.

Proses akuisisi serta imaging memori RAM menggunakan tool *FTK imager* dan sudah dilakukan perbandingan md5 checksum untuk menjaga keaslian bukti digital. Terdapat berbagai hasil yang diperoleh dari berbagai perbandingan tools tersebut, mulai Volatility mampu menemukan artefak 90%, Rekall 70% dan Redline 45%.

**Kata kunci:** *Live Forensic, Digital Forensic, Cybercrime, NIST*

## ABSTRACT

*One of the techniques in the field of digital forensics in the process of collecting evidence to uncover a case of cybercrime that is live forensic. Unlike traditional forensic techniques, live forensic techniques allow investigators to obtain Volatile data stored on system memory (RAM). There are many sensitive artifacts that can be obtained using live forensic techniques.*

*In this study, the authors will analyze various potential evidence contained in RAM with scenarios that have been created using the methodology of the National Institute of Standards Technology (NIST). This methodology was chosen because of the framework of procedures suitable for applying to incident handling more effectively in many live forensic cases. This study focuses on evaluating the performance comparison of 3 live forensic open-source tools in analyzing some of the evidence that has been found.*

*The acquisition and imaging process of RAM memory uses the FTK imager tool and an md5 checksum comparison has been carried out to maintain the authenticity of digital evidence. There are various results obtained from various comparisons of these tools, starting with Volatility being able to find 90% artifacts, 70% Rekall and 45% Redline.*

***Keyword:*** *Live Forensic, Digital Forensic, Cybercrime, NIST*