**PROGRAM STUDI TEKNIK KOMPUTER**

# ANALISIS FORENSIK DALAM PENELUSURAN IDENTITAS, KEASLIAN DAN *MALWARE* DARI *EMAIL* MASUK

**KARYA AKHIR**


**MUHAMMAD DIMAS PUTRA**

**221220014**


**PROGRAM DIPLOMA III**

**FAKULTAS VOKASI**

**UNIVERSITAS BINA DARMA**

**PALEMBANG**

**2025**

# HALAMAN PENGESAHAN

## ANALISIS FORENSIK DALAM PENELUSURAN IDENTITAS, KEASLIAN DAN *MALWARE* DARI *EMAIL* MASUK

**MUHAMMAD DIMAS PUTRA**

**221220014**

**Telah diterima sebagai salah satu syarat untuk memperoleh gelar Ahli Madya pada Program Studi Teknik Komputer**

**Palembang, 6 Agustus 2025**
**Fakultas Vokasi**
**Universitas Bina Darma**

**Pembimbing,**

**Rahmat Novrianda Dasmen, S.T., M.Kom**

**Dekan,**

**Prof. Dr. Edi Surya Negara, M.Kom.**

# HALAMAN PERSETUJUAN KOMISI PENGUJI

Karya akhir yang berjudul "ANALISIS FORENSIK DALAM PENELUSURAN IDENTITAS, KEASLIAN DAN MALWARE DARI EMAIL MASUK" oleh Muhammad Dimas Putra, telah dipertahankan di depan Komisi penguji pada hari Kamis tanggal 6 Agustus 2025.

## KOMISI PENGUJI

1. Rahmat Novrianda Dasmen, S.T., M.Kom. — Ketua Penguji
2. Misinem, S.Kom., M.Kom — Anggota Penguji 1 ( )
3. Irwansyah, M.M., M.Kom — Anggota Penguji 2 ( )

Palembang, 6 Agustus 2025

Program Studi Teknik Komputer

Fakultas Vokasi

Universitas Bina Darma

Ketua,

Universitas Bina Darma
Fakultas Vokasi

Timur Dali Purwanto, M.Kom.

# SURAT PERNYATAAN

Saya bertanda tangan dibawah ini :

Nama : Muhammad Dimas Putra

Nim : 221220014

Dengan ini menyatakan bahwa :

1) Karya tulis saya ini adalah hasil dan belum pernah diajukan untuk mendapatkan gelar akademik Diploma di Universitas Bina Darma.
2) Karya tulis ini murni gagasan, rumusan dan penelitian saya sendiri dengan arahan dari tim pembimbing.
3) Di dalam karya tulis ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas kutip dengan mencantumkan nama pengarang dan memasukan dalam daftar rujukan atau daftar pustaka.
4) Saya bersedia karya tulis ini di cek keasliannya menggunakan plagiarism cheeker serta diunggah ke internet, sehingga dapat diakses public secara online
5) Surat pernyataan ini saya tulis dengan sungguh-sungguh dan apabila terbukti melakukan penyimpangan atau ketidakbenaran dalam pernyataan ini maka saya bersedia menerima sanksi sesuai dengan peraturan perundang-undangan yang berlaku ssat ini.

Dengan surat pernyataan ini saya buat agar dapat dipergunakan sebagaimana mestinya.

Palembang, 6 Agustus 2025
Yang membuat pernyataan,


Muhammad Dimas Putra
Nim: 221220014

# MOTTO DAN PERSEMBAHAN

**“**Maka sesungguhnya bersama kesulitan itu ada kemudahan.
Sesungguhnya bersama kesulitan itu kemudahan”
(Q.S Al-insyirah: 5-6)

“Dan tidaklah mungkin Allah membebani sesorang melainkan sesuai dengan kesanggupannya”
(Q.S Al-Baqarah 286)

KUPERSEMBAHKAN KEPADA:

- Allah SWT, Dzat Maha Mengetahui, yang senantiasa membukakan jalan dalam setiap kebuntuan dan menenangkan hati saat logika tak lagi mampu menjelaskan. Segala puji dan syukur hanya untuk-Mu.
- Yang teristimewa kedua orangtua tercinta yang telah memberikan kasih sayang, nasehat, motivasi, memenuhi kebutuhan penulis, dukungan serta doa yang tiada henti dalam setiap langkahku, ada doa kalian yang diam-diam mengetuk langit. Terima kasih atas peluh, restu, dan cinta yang tak terhitung nilainya.
- Adiku dan keluarga besarku yang selalu menghadirkan rasa hangat dan arti pulang yang sesungguhnya. Terima kasih atas doa-doa yang mengalir dalam senyap dan dukungan yang tak pernah absen, walau tak selalu dalam kata.
- Dosen pembimbing dan para pengajar, yang telah menjadi lentera dalam gelap, membagikan ilmu, membuka pikiran, dan menanamkan rasa ingin tahu yang tak pernah padam.
- Sahabat seperjuangan Teknik Komputer yang tetap solid dari awal sampai akhir dan rekan magang , yang telah menjadi bahu saat beban terasa berat dan tawa saat hari terasa penat. Kalian bukan hanya teman belajar, tapi juga penyejuk dalam perjalanan akademik ini.

- Karya ini saya persembahkan untuk diri saya sendiri,sebagai bentuk penghargaan atas setiap usaha, ketekunan, dan kesabaran dalam melalui proses panjang penyusunan karya akhir ini. Semoga pencapaian ini menjadi langkah awal menuju masa depan yang lebih baik.

# ABSTRACT

*The Directorate of Innovation and Business Incubator (DIIB) at Bina Darma University is a center for innovation and business that frequently receives emails from external parties. This opens up the possibility of receiving suspicious emails that could potentially carry viruses, malware, or phishing attempts. This study uses the DFRWS method with the stages of Identification, Preservation, Collection, Examination, Analysis, and Presentation. The tools used include MXToolbox for header analysis, WhoisLookup and Talos for email reputation and identity, Sucuri for domain verification, and VirusTotal for scanning attachments. Three suspicious emails were examined, and the results showed that two of them failed SPF, DKIM, and DMARC authentication and used public domains such as Gmail and Yahoo, indicating potential spoofing and phishing. Although the attachment scan results showed no active malware, contextual analysis revealed suspicious communication patterns and high phishing indicators. This study underscores the importance of email forensics in detecting hidden threats.*

***Keywords:*** *DIIB, Email, DFRWS, Malware, Tools*

# ABSTRAK

Direktorat Inovasi dan Inkubator Bisnis (DIIB) di Universitas Bina Darma merupakan pusat inovasi dan bisnis yang sering menerima email dari pihak eksternal. Hal ini membuka kemungkinan penerimaan email mencurigakan yang berpotensi membawa virus, malware, atau upaya phishing. Penelitian ini menggunakan metode DFRWS dengan tahapan Identifikasi, Preservasi, Pengumpulan, Pemeriksaan, Analisis, dan Presentasi. Tools yang digunakan antara lain MXToolbox untuk analisis header, WhoisLookup dan Talos untuk reputasi email dan identitas , Sucuri untuk verifikasi domain, dan VirusTotal untuk memindai attachment. Tiga email yang mencurigakan diperiksa, dan hasilnya menunjukkan bahwa dua di antaranya gagal dalam otentikasi SPF, DKIM, dan DMARC serta menggunakan domain publik seperti Gmail dan Yahoo, yang mengindikasikan berpotensi melakukan spoofing dan phishing. Meskipun hasil pemindaian lampiran menunjukkan tidak ada malware yang aktif, analisis kontekstual mengungkapkan pola komunikasi yang mencurigakan dan indikator phishing yang tinggi. Penelitian ini menggarisbawahi pentingnya forensik email dalam mendeteksi ancaman tersembunyi.

**Kata Kunci:** DIIB, Email, DFRWS, Malware, Tools

# DAFTAR RIWAYAT HIDUP

*CURICULUM VITAE*

**Muhammad Dimas Putra, A.Md.**

**Fresh Graduate, Computer Engineering of Universitas Bina Darma**

**PALEMBANG, SOUTH SUMATERA** 30319 - 0895-3018-9156 -Email : muhammaddimas090704@gmail.com

## PERSONAL INFORMATION

Date Of Birt : Palembang, December, 9th, 2004

Address : Komp. Griya Kencana Indah, RT.027/RW.0.12, Lebung Gajah, Sematang Borang, Palembang

Nationality : Indonesia

Marital Status : Single

## EDUCATION BACKGROUND

**2019 – 2022** **SMA Negeri 18 Palembang**

**2022 – 2025** **Universitas Bina Darma**

Vocational Faculty, Computer Enginnering Associate's degree

## AWARD

**2025** **Participant of Management Day Expo (Enterpreneurship Competition)**

**2025** **Participant of kenali lebih dekat Digital Marketing & Content Creator**

**2025** **Presenter of Seminar of Nasionsal FORTEI Regional I Sumatera**

# KATA PENGANTAR

بِسْمِ اللهِ الرَّحْمٰنِ الرَّحِيْمِ

Alhamdullilah, puji syukur penulis panjatkan ke hadirat Allah SWT yang telah memberikan kesehatan, ketekunan, dan pertolongannya hingga akhrinya Karya akhir yang berjudul "Implementasi teknik komputer forensik dalam penelusuran identitas, keaslian, dan *malware* dari *email* masuk". laporan akhir ini disusun untuk memenuhi syarat dalam menyelesaikan salah satu syarat untuk memperoleh gelar Ahli Madya (A.Md.) pada program studi DIII – Teknik Komputer Fakultas Vokasi Universitas Bina Darma.

Dalam penyusunan Karya akhir, penulis mendapatkan banyak dukungan dari berbagai pihak. Baik berupa bimbingan, motivasi, arahan, saran, informasi, maupun data-data baik secara tertulis maupun lisan.

Oleh karena itu, penulis mengucapkan terima kasih kepada :

1) Prof. Dr. Edi Surya Negara, S.Kom., M.Kom. Selaku Plt Rektor Universitas Bina Darma sekaligus Dekan Fakultas Vokasi Universitas Bina Darma.
2) Bapak Timur Dali Purwanto, M.Kom. Selaku Ketua Program Studi Teknik Komputer Universitas Bina Darma.
3) Bapak Rahmat Novrianda Dasmen, S.T., M.Kom. Selaku dosen pembimbing yang telah memberikan arahan, saran, masukan, dan bimbingan dalam proses untuk menyelesaikan tugas akhir ini.

4) Ibu Misinem, S.Kom., M.Kom dan Bapak Irwansyah, M.M., M.Kom selaku Dosen penguji yang telah memberikan masukan, kritik, dan saran yang membangun demi penyempurnaan Karya akhir ini.
5) Seluruh dosen yang telah memberikan ilmu dan mengajarkan saya dalam menempuh pendidikan pada Universitas Bina Darma
6) Buat keluarga tercinta, terima kasih atas doa, dukungan, dan kasih sayang yang tak pernah putus, memberikan dukungan dan motivasi hingga aku menjadi orang yang berkarakter baik.
7) Rekan-rekan seperjuangan dan tim DIIB, atas diskusi saran dan masukan yang diberikan.

Akhir kata, penulis membuka diri terhadap segala bentuk kritik dan saran yang membangun sebagai bahan evaluasi dan perbaikan demi penyempurnaan karya akhir ini di masa mendatang.

Palembang, 6 Agustus 2025

Muhammad Dimas Putra

# DAFTAR ISI

# DAFTAR TABEL

# DAFTAR GAMBAR

# DAFTAR LAMPIRAN