

**ANALISIS PEMANFAATAN OSINT DALAM MENGIDENTIFIKASI  
SERANGAN PHISING PADA MEDIA SOSIAL**

**SKRIPSI**

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana  
Program Studi Teknik Komputer



disusun oleh

**ARIZKA WAHYU SATRIA ANGGARA**

**22.83.0802**

Kepada

**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS AMIKOM**

**YOGYAKARTA YOGYAKARTA**

**2026**

**ANALISIS PEMANFAATAN OSINT DALAM MENGIDENTIFIKASI  
SERANGAN PHISING PADA MEDIA SOSIAL**

**SKRIPSI**

untuk memenuhi salah satu syarat mencapai derajat Sarjana  
Program Studi Teknik Komputer



disusun oleh

**ARIZKA WAHYU SATRIA ANGGARA**

**22.83.0802**

Kepada

**FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM  
YOGYAKARTA YOGYAKARTA  
2026**

# **HALAMAN PERSETUJUAN**

## **SKRIPSI**

### **ANALISIS PEMANFAATAN OSINT DALAM MENGIDENTIFIKASI SERANGAN PHISING PADA MEDIA SOSIAL**

yang disusun dan diajukan oleh

**Arizka Wahyu Satria Anggara**

**22.83.0802**

telah disetujui oleh Dosen Pembimbing Skripsi  
pada tanggal 29 September 2025

**Dosen Pembimbing,**

**Dr. Donv Arjvus, S.S., M.Kom**

**NIK. 190302128**

## HALAMAN PENGESAHAN

### SKRIPSI

ANALISIS PEMANFAATAN OSINT DALAM MENGIDENTIFIKASI SERANGAN PHISING  
PADA MEDIA SOSIAL

yang disusun dan diajukan oleh

**Arizka Wahyu Satria Anggara**

22.83.0802

Telah dipertahankan di depan Dewan Penguji  
pada tanggal <tanggal ujian>

#### Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

**Alva Hendi Muhammad, A.Md., S.T., M.Eng., Ph.D**  
NIK. 190302493

**Wahid Miftahul Ashari, S.Kom., M.T.**  
NIK. 190302452

**Dr. Dony Ariyus, S.S., M.Kom.**  
NIK. 190302128

Skripsi ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer  
Tanggal 23 Febuari 2026

**DEKAN FAKULTAS ILMU KOMPUTER**



**Prof. Dr. Kusriini, M.Kom.**  
NIK. 190302106

## HALAMAN PERNYATAAN KEASLIAN SKRPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Arizka Wahyu Satria Anggara

NIM : 22.83.0802

Menyatakan bahwa Skripsi dengan judul berikut:

Analisis Pemanfaatan OSINT Dalam Mengidentifikasi Serangan Pada Media Sosial

Dosen Pembimbing : Dr. Dony Ariyus, S.S., 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, 14 Mei 2026

Yang Menyatakan,



Arizka Wahyu Satria Anggara

## HALAMAN PERSEMBAHAN

Skripsi ini saya persembahkan dengan penuh rasa syukur dan hormat kepada:

1. Kedua Orang Tuaku Tercinta, Terima kasih yang tak terhingga atas segala doa yang tak pernah putus, kasih sayang, dan pengorbanan luar biasa untuk mendukung pendidikan saya hingga tahap ini. Karya ini adalah bukti kecil bakti ananda untuk membalas segala kebaikan Bapak dan Ibu.
2. Bapak Dr. Dony Ariyus, S.S., M.Kom selaku Dosen Pembimbing. Terima kasih yang sebesar-besarnya atas waktu, kesabaran, dan ilmu yang telah Bapak/Ibu curahkan dalam membimbing saya. Terima kasih telah menjadi pelita yang mengarahkan saya saat tersesat dalam penyusunan skripsi ini hingga tuntas.
3. Kakakku Nanda Pasa.W. Terima kasih telah menjadi penasihat, pendengar keluh kesah, dan pendukung setia di setiap langkah perjuangan ini.
4. Teman-teman Seperjuangan dan Tongkrongan. Terima kasih atas kebersamaan, diskusi, dan semangat yang kalian berikan. Sukses untuk kita semua.

## KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh. Selamat pagi/siang dan salam sejahtera untuk kita semua.

Yang saya hormati, Bapak/Ibu **Dr. Dony Ariyus, S.S., M.Kom** selaku Dosen Pembimbing yang telah membimbing saya hingga tahap ini.

Perkenalkan, nama saya **Arizka Wahyu Satria Anggra** dengan NIM **22.83.0802**

Pada kesempatan yang berharga ini, izinkan saya mempresentasikan hasil penelitian skripsi saya yang berjudul:

**'ANALISIS PEMANFAATAN *OPEN SOURCE INTELLIGENCE* (OSINT) DALAM MENGIDENTIFIKASI SERANGAN *PHISING* PADA MEDIA SOSIAL'.**

Penelitian ini dilatarbelakangi oleh fenomena pergeseran serangan siber, di mana media sosial—khususnya Facebook—kini menjadi sarang utama penyebaran tautan *phishing*. Masalah utamanya bukan hanya pada link yang berbahaya, tetapi sulitnya melacak siapa identitas asli di balik akun penyebar tersebut.

Oleh karena itu, penelitian ini hadir untuk menguji efektivitas metode OSINT dalam dua hal: mendeteksi infrastruktur phishing dan melakukan atribusi identitas pelaku.

Yogyakarta, 15 Desember 2025



Arizka Wahyu Satria Anggr

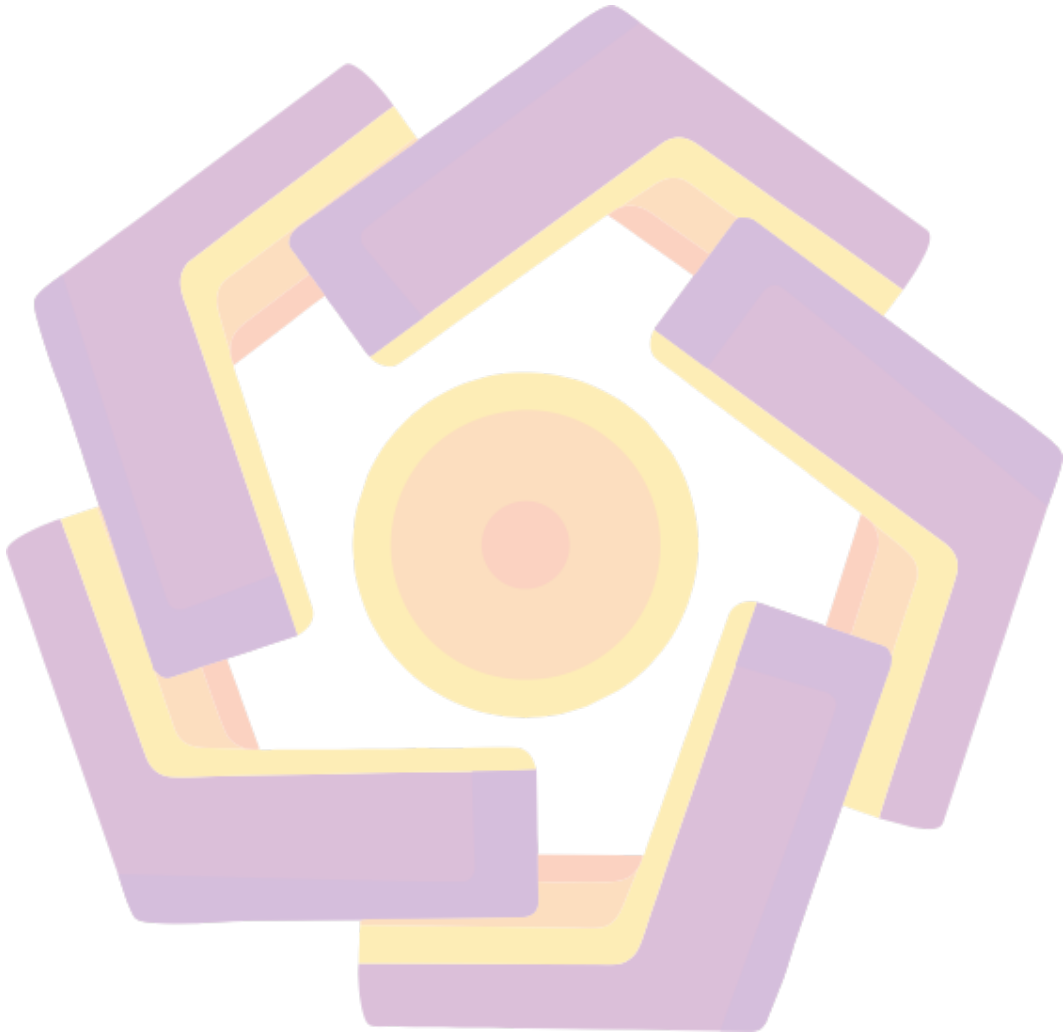
## DAFTAR ISI

|                                                           |     |
|-----------------------------------------------------------|-----|
| HALAMAN JUDUL.....                                        | i   |
| HALAMAN PERSETUJUAN.....                                  | i   |
| HALAMAN PENGESAHAN.....                                   | iii |
| HALAMAN PERNYATAAN KEASLIAN SKRPSI.....                   | iv  |
| HALAMAN PERSEMBAHAN.....                                  | v   |
| KATA PENGANTAR.....                                       | vi  |
| DAFTAR ISI.....                                           | vii |
| DAFTAR TABEL.....                                         | ix  |
| DAFTAR GAMBAR.....                                        | x   |
| INTISARI.....                                             | xi  |
| <i>ABSTRACT</i> .....                                     | xii |
| BAB I PENDAHULUAN.....                                    |     |
| 1.1 Latar Belakang.....                                   | 1   |
| 1.2 Rumusan Masalah.....                                  | 2   |
| 1.3 Batasan Masalah.....                                  | 2   |
| 1.4 Tujuan Penelitian.....                                | 3   |
| 1.5 Manfaat Penelitian.....                               | 4   |
| 1.6 Sistematika Penulisan.....                            | 4   |
| BAB II                                                    |     |
| TINJAUAN PUSTAKA.....                                     | 6   |
| 2.1 Studi Literatur.....                                  | 6   |
| 2.2 Dasar Teori.....                                      | 11  |
| 2.2.1 Phishing.....                                       | 11  |
| 2.2.2 OSINT.....                                          | 12  |
| 2.2.3 Virus Totaal.....                                   | 13  |
| 2.2.4 Instant Data Scraper.....                           | 14  |
| 2.2.5 Data Leak Api.....                                  | 15  |
| 2.2.6 Facebook.....                                       | 15  |
| 2.2.7 Observasi.....                                      | 17  |
| BAB III                                                   |     |
| METODE PENELITIAN.....                                    | 18  |
| 3.1 Objek Penelitian.....                                 | 18  |
| 3.1.1 Platform Media Sosial Facebook.....                 | 18  |
| 3.1.2 Aktivitas Serangan Phishing dan Link Berbahaya..... | 19  |
| 3.1.3 Identitas Digital dan Atribusi Pelaku.....          | 19  |
| 3.2 Alur Penelitian.....                                  | 20  |
| 3.3 Alat dan Bahan.....                                   | 21  |

|                                                                        |    |
|------------------------------------------------------------------------|----|
| BAB IV                                                                 |    |
| HASIL DAN PEMBAHASAN.....                                              | 24 |
| 4.1. Hasil Penelitian.....                                             | 24 |
| 4.1.1 Pngumpulan data.....                                             | 24 |
| 1. Persiapan dan Instalasi.....                                        | 24 |
| 2. Menentukan Target Data.....                                         | 24 |
| 3. Aktivasi Ekstensi.....                                              | 25 |
| 4. Konfigurasi Navigasi (Infinite Scroll atau Pagination).....         | 25 |
| 5. Proses Crawling (Start Crawling).....                               | 26 |
| 4.1.3.1 Penggunaan VirusTotal untuk Menganalisis Domain.....           | 28 |
| 1. Mengakses Layanan.....                                              | 28 |
| 2. Memasukkan URL Target.....                                          | 29 |
| 3. Analisis Hasil Pemindaian (Detection).....                          | 29 |
| 4.2. Pembahasan.....                                                   | 30 |
| 4.2.1. Efektivitas Tahapan Penerapan OSINT.....                        | 31 |
| 4.2.2. Karakteristik Serangan Phishing di Facebook.....                | 31 |
| 4.3 Cara Kerja Bot Telegram untuk Pencarian Identitas (OSINT).....     | 31 |
| 4.4. Pencarian Identitas Pelaku penyebaran Phishing.....               | 34 |
| 4.4.1. Analisis Investigasi Target 1 (Akun Perdi Wahyu Pratama).....   | 34 |
| 4.4.2 Analisis Investigasi Target 2 (Akun Aldy Pranata).....           | 36 |
| 4.4.3 Analisis Investigasi Target 3 (Akun Putry Cantika).....          | 38 |
| 4.4.4 Analisis Investigasi Target 4 (Akun Fahry Fanny Aryo Surya)..... | 40 |
| 4.4.5 Analisis Investigasi Target 5 (Akun Megi Kurniawan).....         | 42 |
| 4.5 Peran OSINT dalam Deteksi Dini (Early Detection).....              | 44 |
| BAB VPENUTUP.....                                                      |    |
| 45                                                                     |    |
| 5.1 Kesimpulan.....                                                    | 45 |
| REFERENSI.....                                                         | 47 |

## DAFTAR TABEL

|                                                    |    |
|----------------------------------------------------|----|
| Tabel 2.1 Keaslian Penelitian.....                 | 7  |
| Tabel 3.3 Merupakan Tabel Alat Yang Digunakan..... | 22 |
| Tabel 4.1.2 Tabel Hasil Pengumpulan Data.....      | 27 |
| Tabel 4.1.3 Hasil Reputasi Data.....               | 29 |



## DAFTAR GAMBAR

|                                                                         |    |
|-------------------------------------------------------------------------|----|
| Gambar 2.1 Laporan kasus phishing.....                                  | 11 |
| Gamabar 2.2.4 Tampilan Instan data Scraper.....                         | 14 |
| Gambar 2.2.6 Tampilan Halaman Grup Facebook.....                        | 16 |
| Gambar 3.2.1 Alur Penelitian identifikasi Phishing.....                 | 20 |
| Gambar 4.1.1.....                                                       | 24 |
| Gambar 4.1.1.....                                                       | 25 |
| Gambar 4.1.1.....                                                       | 26 |
| Gambar 4.1.1.....                                                       | 26 |
| Gambar 4.1.3.1.....                                                     | 28 |
| Gambar 4.1.3.1.....                                                     | 29 |
| Gambar 4.3 Tampilan dari outpus atau hasil dari investigasi.....        | 33 |
| Gambar 4.4.1 Postingan peyebaran link phishing Predi Wahyu Pratama..... | 34 |
| Gambar 4.4.1 Hasil Penyelidikan Identitas.....                          | 35 |
| Gambar 4.4.2 Postingan peyebaran link phishing.....                     | 36 |
| Gambar 4.4.2 Hasil Penyelidikan Identitas:.....                         | 37 |
| Gambar 4.4.3 Postingan peyebaran link phishing Putry Cantika.....       | 38 |
| Gambar 4.4.3 Hasil Penyelidikan Identitas D.....                        | 39 |
| Gambar 4.3.4 Postingan peyebaran link phishing Surya Aryo.....          | 40 |
| Gambar 4.4.4 Hasil Penyelidikan Identitas D:.....                       | 41 |
| Gambar 4.3.5 Postingan peyebaran link phishing:.....                    | 43 |

## INTISARI

Serangan *phishing* di media sosial Facebook terus meningkat dengan teknik rekayasa sosial yang semakin kompleks, sehingga membutuhkan metode deteksi yang lebih proaktif dan mendalam. Penelitian ini bertujuan untuk menganalisis efektivitas teknik *Open Source Intelligence* (OSINT) dalam mengidentifikasi kampanye *phishing* dan mengungkap identitas digital asli pelaku. Metodologi yang digunakan adalah studi kasus investigatif dengan memanfaatkan berbagai perangkat OSINT, antara lain *Instant Data Scraper* untuk pengumpulan data, VirusTotal untuk validasi tautan berbahaya, serta bot Telegram yang terintegrasi dengan *API Leak Checker* untuk atribusi pelaku. Hasil penelitian menunjukkan bahwa penggunaan instrumen OSINT mampu memetakan karakteristik teknis serangan secara akurat dan berhasil mengungkap data pribadi (*Personally Identifiable Information*) dari lima target pelaku, meliputi Nomor Induk Kependudukan (NIK), alamat fisik, e-mail asli, hingga data registrasi kendaraan. Kesimpulan dari penelitian ini menegaskan bahwa integrasi berbagai sumber data terbuka dan alat investigasi digital dapat menjadi kerangka kerja yang efektif dalam proses deteksi dini dan atribusi ancaman siber di media sosial, serta memberikan kontribusi bagi strategi pertahanan siber yang lebih preventif.

**Kata kunci:** OSINT, Phishing, Facebook, Investigasi Siber, Atribusi, API Leak Checker.

## ***ABSTRACT***

*Phishing is a common type of cyberattack that exploits users' vulnerabilities by Phishing attacks on Facebook social media continue to increase with increasingly complex social engineering techniques, requiring more proactive and in-depth detection methods. This study aims to analyze the effectiveness of Open Source Intelligence (OSINT) techniques in identifying phishing campaigns and uncovering the real digital identities of the perpetrators. The methodology used is an investigative case study utilizing various OSINT tools, including Instant Data Scraper for data collection, VirusTotal for malicious link validation, and Telegram bots integrated with API Leak Checkers for perpetrator attribution. The results show that the use of OSINT instruments can accurately map the technical characteristics of attacks and successfully reveal the Personally Identifiable Information (PII) of five targeted perpetrators, including National Identification Numbers (NIK), physical addresses, original e-mails, and vehicle registration data. The conclusion of this study emphasizes that the integration of various open data sources and digital investigation tools can be an effective framework in the early detection and attribution process of cyber threats on social media, as well as contributing to a more preventive cyber defense strategy.*

**Keyword:** *OSINT, Phishing, Facebook, Cyber Investigation, Attribution, API Leak Checker*