

**ANALISIS KEBOCORAN DATA SENSITIF PERSEORANGAN
MENGUNAKAN *OSINT (OPEN SOURCE
INTELLIGENCE)***

SKRIPSI

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



disusun oleh

RAFLI ILHAM PRASETYO

22.83.0907

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2025**

**ANALISIS KEBOCORAN DATA SENSITIF PERSEORANGAN
MENGUNAKAN *OSINT (OPEN SOURCE
INTELLIGENCE)***

SKRIPSI

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



disusun oleh

RAFLI ILHAM PRASETYO

22.83.0907

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2025

HALAMAN PERSETUJUAN

SKRIPSI

ANALISIS KEBOCORAN DATA SENSITIF PERSEORANGAN
MENGGUNAKAN *OSINT (OPEN SOURCE INTELLIGENCE)*

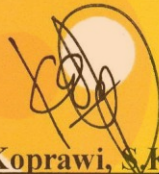
yang disusun dan diajukan oleh

Rafli Ilham Prasetyo

22.83.0907

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 20 November 2025

Dosen Pembimbing,



Muhammad Kopravi, S.Kom., M.Eng.
NIK. 190302454

HALAMAN PENGESAHAN
SKRIPSI
ANALISIS KEBOCORAN DATA SENSITIF PERSEORANGAN
MENGUNAKAN *OSINT (OPEN SOURCE INTELLIGENCE)*

yang disusun dan diajukan oleh

Rafli Ilham Prasetyo

22.83.0907

Telah dipertahankan di depan Dewan Penguji
pada tanggal 20 November 2025

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Melwin Syafrizal, S.Kom., M.Eng., Ph.D.
NIK. 190302105

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

Muhammad Koprari, S.Kom., M.Eng.
NIK. 1903022454



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 20 November 2025

DEKAN FAKULTAS ILMU KOMPUTER



Prof. Dr. Kusriani, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : RAFLI ILHAM PRASETYO
NIM : 22.83.0907

Menyatakan bahwa Skripsi dengan judul berikut:

ANALISIS KEBOCORAN DATA SENSITIF PERSEORANGAN MENGUNAKAN *OSINT (OPEN SOURCE INTELLIGENCE)*

Dosen Pembimbing : Muhammad Kopravi, 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, 20 November 2025

Yang Menyatakan,



Rafli Ilham Prasetyo

HALAMAN MOTTO

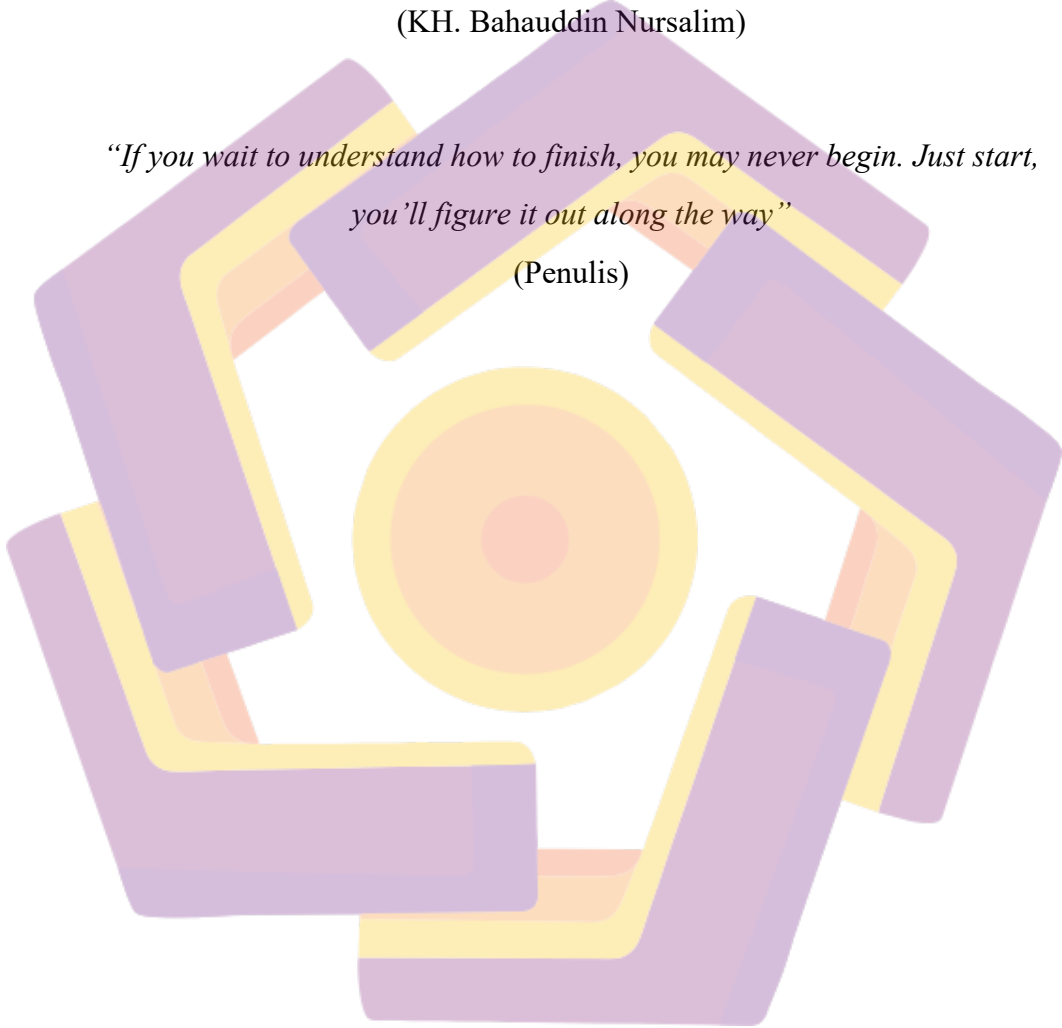
“You’ll Never Walk Alone”

“Kita harus yakin seyakini-yakinnya, bahwa semua kemungkinan itu mungkin”

(KH. Bahauddin Nursalim)

*“If you wait to understand how to finish, you may never begin. Just start,
you’ll figure it out along the way”*

(Penulis)



HALAMAN PERSEMBAHAN

Dengan menyebut nama Allah SWT, segala puji dan syukur kami haturkan atas rahmat, petunjuk, dan kemudahan yang selalu menyertai. Segala upaya, waktu, dan perjuangan yang tercurah dalam proses penulisan skripsi ini akhirnya membuahkan hasil, berkat izin dan karunia-Nya. Oleh karena itu, skripsi ini saya persembahkan secara istimewa bagi:

1. Kedua Orang Tua Tercinta, Bapak Ismuhani dan Ibu Dede Handayani, yang kasih sayangnya tak terbatas. Terima kasih atas setiap lantunan doa, dukungan tanpa henti, fasilitas terbaik yang diberikan, serta segala pengorbanan dan jerih payah yang telah dicurahkan demi mewujudkan masa depan anakmu ini.
2. Bapak Muhammad Koprari, S.Kom., M.Eng., Selaku Dosen Pembimbing yang terhormat. Penghargaan setinggi-tingginya atas kesabaran, arahan, bimbingan, serta waktu yang telah diluangkan hingga skripsi ini dapat tersusun dengan baik dan tuntas.
3. Teman Seperjuangan, Semua rekan dan sahabat terbaik yang telah menjadi bagian tak terpisahkan dari perjalanan perkuliahan. Terima kasih telah berbagi tawa dan duka, serta memberikan motivasi dan semangat hingga detik penyelesaian skripsi ini.

KATA PENGANTAR

Puji dan Syukur kehadirat Allah Subhanahu Wa Ta'ala, karena atas segala berkat rahmat, karunia, dan hidayah-Nya, yang senantiasa memberikan kekuatan, kesehatan, dan kelancaran sehingga penulis dapat menyelesaikan skripsi yang berjudul **“Analisis Kebocoran Data Sensitif Perseorangan Menggunakan OSINT (Open Source Intelligence)”**, yang disusun sebagai salah satu syarat untuk mencapai derajat Sarjana Komputer pada Program Studi Teknik Komputer, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta.

Dengan segala kerendahan hati dan ketulusan, shalawat dan salam yang terindah kita sanjungkan kehadirat junjungan agung kita, Nabi Muhammad SAW, beserta seluruh keluarga dan keturunan beliau yang mulia. Beliau adalah sumber cahaya ilmu yang menerangi kegelapan kebodohan, sebuah petunjuk agung yang sempurna. Melalui risalah dan sunahnya, kita dijamin memperoleh keselamatan yang menyeluruh, baik dalam menata kehidupan di dunia fana ini maupun saat meraih kebahagiaan sejati di kehidupan akhirat kelak.

Proses penyusunan skripsi ini tidak terlepas dari dukungan, doa, masukan, dan bantuan dari berbagai pihak yang berperan penting dalam setiap tahap perjalanan akademik penulis. Dengan penuh kerendahan hati, penulis menyampaikan ucapan terimakasih yang sebesar-besarnya kepada :

1. Bapak dan Ibu tercinta yang senantiasa selalu mendoakan, menasehati, mendidik, dan menyemangati penulis hingga dapat menyelesaikan skripsi ini.
2. Adik dan seluruh keluarga besar yang selalu hadir dengan kasih sayang, doa, dan dukungan diawal hingga akhir masa studi penulis di Universitas Amikom Yogyakarta.
3. Bapak Prof. Dr. M. Suyanto, M.M, Selaku Rektor Universitas Amikom Yogyakarta.
4. Ibu Prof. Dr. Kusri, M.Kom., Selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.

5. Bapak Dr. Dony Ariyus, S.S., M.Kom., selaku Kepala Prodi Teknik Komputer Universitas Amikom Yogyakarta.
6. Bapak Muhammad Koprari, S.Kom., M.Eng., selaku dosen pembimbing yang senantiasa memberikan ilmunya dengan sabar dan ikhlas selama proses pengerjaan skripsi ini, sehingga penulis dapat menyelesaikannya dengan baik dan tepat waktu.
7. Ibu Senie Destya, M.Kom, selaku dosen wali atas arahan dan motivasi yang diberikan selama masa perkuliahan.
8. Seluruh dosen Universitas Amikom Yogyakarta, yang telah memberikan ilmu, pengetahuan, dukungan dan arahnya selama penulis menempuh pendidikan di Universitas Amikom Yogyakarta.
9. Teman-teman Teknik Komputer Angkatan 22 terutama 22TK03 yang menjadi bagian dari perjalanan masa studi ini, berbagai canda dan tawa, susah senang, semangat, dan dukungan disetiap langkahnya.
10. Kepada teman-teman RB (Rumah Bujang) dan JB (Jaga Bumi) yang senantiasa memberikan dukungan, motivasi, dan semangat kepada penulis sedari awal hingga akhir masa studi ini. Tanpa kalian saya bukan apa-apa!
11. Semua pihak yang telah memberikan dukungan, semangat, dan bantuan berupa moril ataupun materil sepanjang proses penyusunan skripsi ini.

Sesungguhnya segala kebenaran dan kesempurnaan yang termuat di dalamnya adalah semata-mata atas rahmat dan kehendak Allah SWT.

Oleh karena itu, penulis mempersilakan para pembaca untuk mengambil manfaat sebesar-besarnya dari penelitian ini, namun apabila terdapat kesalahan atau kekeliruan, maka hal itu murni berasal dari keterbatasan dan kekhilafan penulis pribadi, dan penulis memohon agar kekeliruan tersebut dapat dimaafkan dan ditinggalkan

Yogyakarta, 20 November 2025

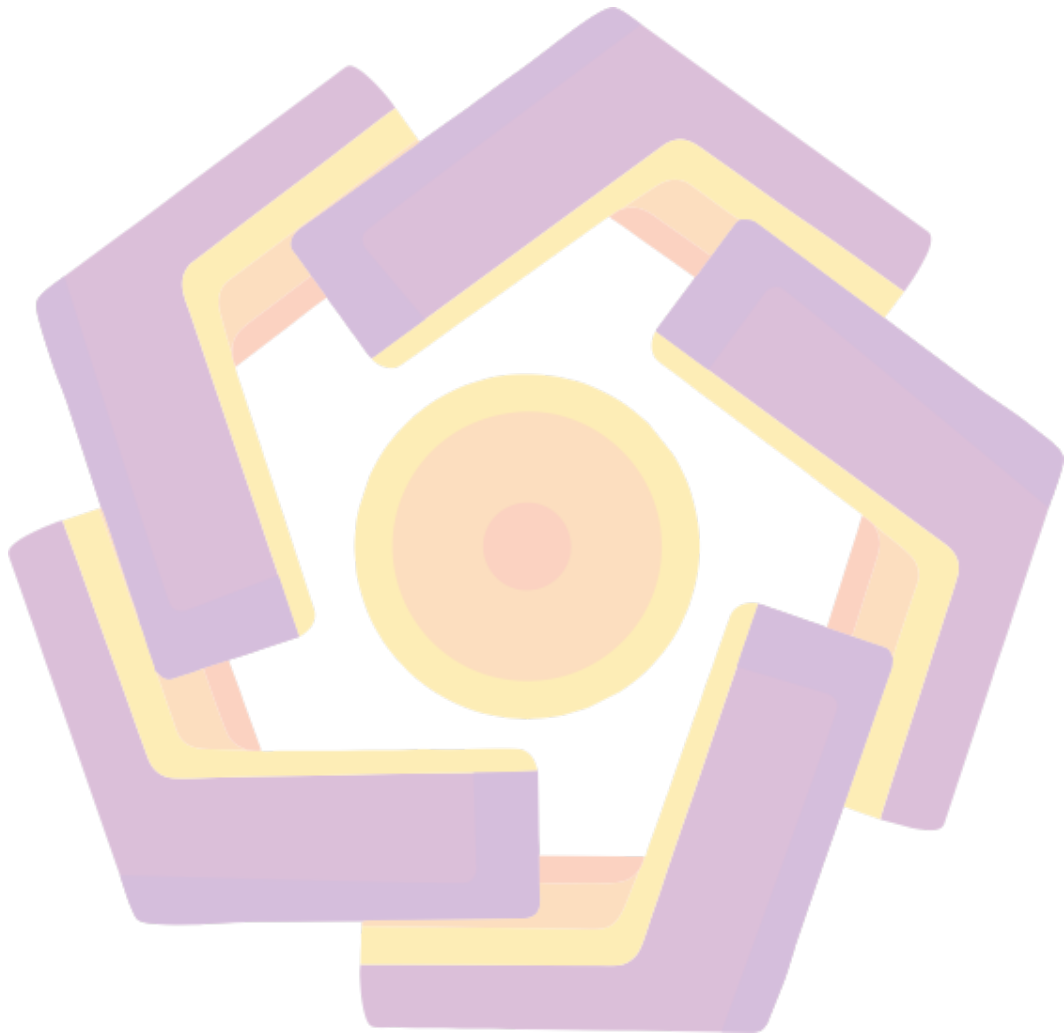
Penulis

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN	ii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI	Error! Bookmark not defined.
HALAMAN MOTTO	v
HALAMAN PERSEMBAHAN	vi
KATA PENGANTAR	vii
DAFTAR ISI.....	ix
DAFTAR TABEL.....	xii
DAFTAR GAMBAR.....	xiii
DAFTAR LAMPIRAN.....	xvi
DAFTAR SINGKATAN	xvii
INTISARI	xviii
<i>ABSTRACT</i>	xix
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	4
1.6 Sistematika Penulisan	4
BAB II TINJAUAN PUSTAKA	5
2.1 Studi Literatur	5

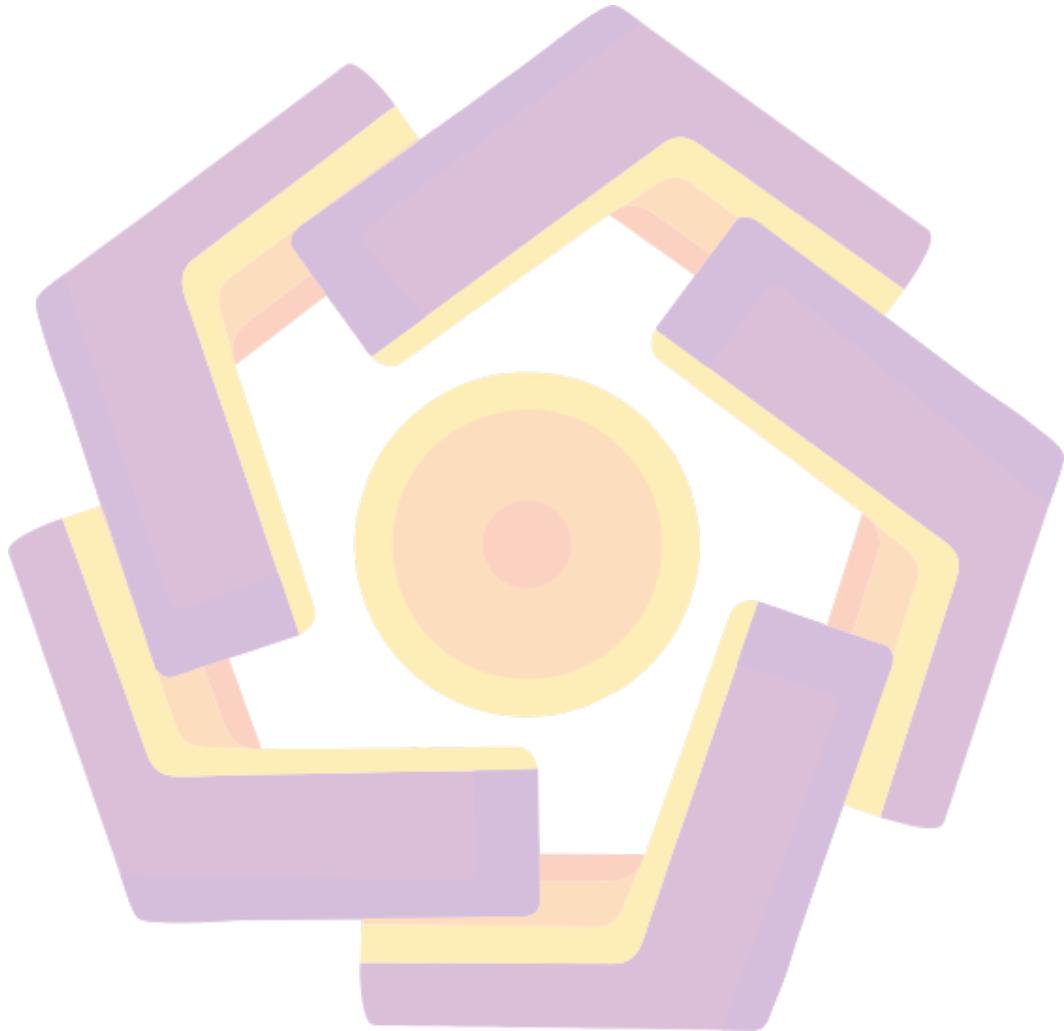
2.2	Dasar Teori.....	18
2.2.1	Data Sensitif Perseorangan	18
2.2.2	Metodologi OSINT & Teknik.....	21
2.2.3	Ancaman & Eksploitasi	28
BAB III METODE PENELITIAN		33
3.1	Objek Penelitian.....	33
3.1.1	Justifikasi Pemilihan Objek Penelitian	33
3.1.2	Batasan Etika Penelitian	33
3.2	Analisis Masalah.....	34
3.3	Solusi Masalah	35
3.4	Alur Penelitian	35
3.5	Pemetaan Alur Kerja Investigasi.....	37
3.5.1	Fase Pre-Engagement (Penetapan Tujuan dan Batasan).....	37
3.5.2	Fase Information Gathering (Pengumpulan Data).....	38
3.5.3	Fase Analysis, Processing & Correlation (Pengolahan dan Korelasi Data).....	39
3.5.4	Fase Reporting & Production (Penyajian Hasil dan Risiko).....	39
3.6	Alat dan Bahan.....	40
BAB IV HASIL DAN PEMBAHASAN		44
4.1	Sock Puppets	44
4.2	Data Collection (Pengumpulan Data)	44
4.3	Data Processing & Validation.....	65
4.4	Risk Analysis & Production.....	84
BAB V PENUTUP		93
5.1	Kesimpulan	93

5.2	Saran	93
REFERENSI		95
LAMPIRAN.....		100



DAFTAR TABEL

Tabel 2. 1 Keaslian Penelitian	9
Tabel 3. 1 Kebutuhan Alat dan Bahan.....	40
Tabel 4. 1 Ringkasan Profil Risiko Target	85



DAFTAR GAMBAR

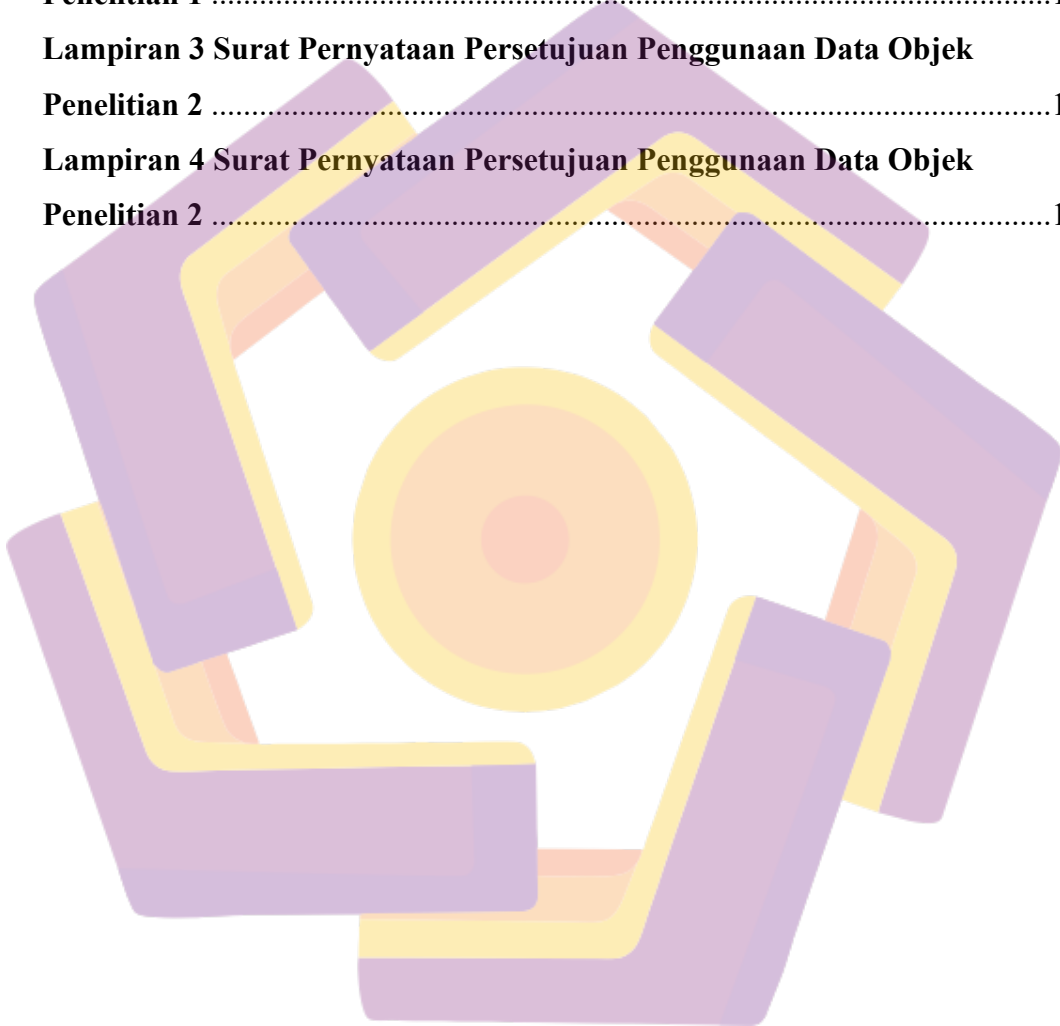
Gambar 2. 1 Kategori <i>Personally Identifiable Information</i> Sensitif[12].....	18
Gambar 2. 2 Klasifikasi Digital Footprint: Active dan Passive[20]	22
Gambar 2. 3 Google Dorking <i>Commands</i> [23].....	23
Gambar 2. 4 Kategori Data yang Dapat Dikumpulkan[25].....	25
Gambar 2. 5 Beberapa Modus <i>Social Engineering</i> [29].	29
Gambar 2. 6 Vektor Utama Terjadinya Pencurian Identitas[33]	31
Gambar 3. 1 Alur Penelitian	37
Gambar 4. 1 Akun <i>Sock Puppets</i>	44
Gambar 4. 2 Penggunaan Kueri Dorking.....	45
Gambar 4. 3 Riwayat Donasi	45
Gambar 4. 4 Riwayat Pendidikan (SMA).....	46
Gambar 4. 5 Pendataan Fasilitas Pelayanan Kesehatan	46
Gambar 4. 6 Leak Nomor Telepon.....	47
Gambar 4. 7 <i>Feed</i> Instagram 1	47
Gambar 4. 8 <i>Feed</i> Instagram 2	48
Gambar 4. 9 Kueri Dorking dengan Hasil File PDF	48
Gambar 4. 10 Ucapan dari Sahabat.....	49
Gambar 4. 11 Temuan Riwayat Pendidikan	49
Gambar 4. 12 Isi dari Temuan Riwayat Pendidikan	50
Gambar 4. 13 Riwayat Pendidikan	50
Gambar 4. 14 Temuan Riwayat Vaksin.....	51
Gambar 4. 15 Isi dari Riwayat Temuan Vaksin	51
Gambar 4. 16 File Kelompok.....	52
Gambar 4. 17 Isi dari File Kelompok.....	52
Gambar 4. 18 Kueri Dorking dengan Hasil File Document.....	53
Gambar 4. 19 Kueri Dorking dengan Hasil File XLSX	54
Gambar 4. 20 Kueri Dorking dengan Hasil File PPT.....	54
Gambar 4. 21 Riwayat Pendidikan pada PDDIKTI.....	55

Gambar 4. 22 Penggunaan Kueri <i>Dorking</i> – 2	56
Gambar 4. 23 Penggunaan Kueri <i>Dorking</i> lanjutan - 2	56
Gambar 4. 24 Temuan kebocoran data COB.....	57
Gambar 4. 25 Riwayat Pendidikan objek penelitian 2	58
Gambar 4. 26 Temuan kebocoran <i>database</i>	58
Gambar 4. 27 Riwayat Pendidikan objek penelitian 2	59
Gambar 4. 28 Postingan Instagram yang Terindeks	59
Gambar 4. 29 Kueri <i>Dorking</i> dengan Hasil File Document.....	60
Gambar 4. 30 Kueri <i>Dorking</i> dengan Hasil File PPT	60
Gambar 4. 31 Kueri <i>Dorking</i> dengan Hasil File XLSX	61
Gambar 4. 32 Akun Instagram Objek Penelitian	61
Gambar 4. 33 Postingan Instagram yang akan dianalisis	62
Gambar 4. 34 <i>Snap Story</i>	63
Gambar 4. 35 Akun Instagram Kedua dan Ketiga Objek Penelitian	64
Gambar 4. 36 Akun Instagram objek penelitian 2	64
Gambar 4. 37 Akun LinkedIn Objek Penelitian 1	65
Gambar 4. 38 Akun LinkedIn Objek Penelitian 1	66
Gambar 4. 39 Validasi Postingan Instagram yang akan dianalisis	67
Gambar 4. 40 Validasi <i>Snap Story</i>	68
Gambar 4. 41 Profil Akun <i>Get Contact</i> Objek Penelitian 1	69
Gambar 4. 42 Alamat Rumah Objek Penelitian 1	69
Gambar 4. 43 Pencarian 6 digit awal NIK Objek Penelitian 1	70
Gambar 4. 44 Input Validasi NIK	70
Gambar 4. 45 Output Validasi NIK	71
Gambar 4. 46 Riwayat Pendidikan S1	71
Gambar 4. 47 Riwayat Pendidikan Profesi	72
Gambar 4. 48 Validasi dengan Alat Ekstraksi Data (<i>Bot Telegram</i>)	73
Gambar 4. 49 Temuan Data Bocor menggunakan Alat Ekstraksi Data	74
Gambar 4. 50 Cek Kebocoran Data Email 1 dan 2	74
Gambar 4. 51 Cek Kebocoran Data Email 3	75
Gambar 4. 52 <i>Email Lookup</i> 1	76

Gambar 4. 53 Riwayat Ulasan Email 1	77
Gambar 4. 54 <i>Email Lookup 2</i>	77
Gambar 4. 55 <i>Email Lookup 3</i>	78
Gambar 4. 56 Riwayat Ulasan Email 3	79
Gambar 4. 57 Validasi NIK Objek Penelitian 2	79
Gambar 4. 58 Riwayat Pendidikan (2)	80
Gambar 4. 59 Validasi dengan Alat Ekstaksi Data (<i>Bot Telegram</i>)	81
Gambar 4. 60 Profil Akun <i>Get Contact</i> Objek Penelitian 2	82
Gambar 4. 61 Alamat Rumah Objek Penelitian 2	83
Gambar 4. 62 Nomer Rekening Objek Penelitian 2	84
Gambar 4. 63 Simulasi <i>Spear Phising Financial</i>	87
Gambar 4. 64 Simulasi Serangan <i>Fraudster</i>	88
Gambar 4. 65 Simulasi <i>Doxing</i>	89
Gambar 4. 66 Simulasi Serangan COD Palsu	90
Gambar 4. 67 Permohonan Informasi Nomor KK	91

DAFTAR LAMPIRAN

Lampiran 1 Surat Pernyataan Persetujuan Penggunaan Data Objek	
Penelitian 1	100
Lampiran 2 Surat Pernyataan Persetujuan Penggunaan Data Objek	
Penelitian 1	101
Lampiran 3 Surat Pernyataan Persetujuan Penggunaan Data Objek	
Penelitian 2	102
Lampiran 4 Surat Pernyataan Persetujuan Penggunaan Data Objek	
Penelitian 2	103



DAFTAR SINGKATAN



OSINT	<i>Open Source Intelligence</i>
GEOINT	<i>Geospatial Intelligence</i>
INTs	<i>Intelligence Disciplines</i>
HUMINT	<i>Human Intelligence</i>
SIGINT	<i>Signals Intelligence</i>
MASINT	<i>Measurement and Signature Intelligence</i>
SOCMINT	<i>Social Media Intelligence</i>
DML	<i>Detection Maturity Level Model</i>
SOCENG	<i>Social Engineering</i>
GDPR	<i>General Data Protection Regulation</i>
PDP	<i>Perlindungan Data Pribadi</i>

INTISARI

Pesatnya perkembangan teknologi informasi dan meningkatnya penggunaan internet di Indonesia telah menimbulkan tantangan serius dalam perlindungan data pribadi sensitif. Kebocoran data tidak hanya terjadi melalui peretasan sistem, tetapi juga melalui jejak digital pasif yang terindeks secara publik tanpa disadari oleh pemiliknya. Kondisi ini menimbulkan dampak signifikan, mulai dari ancaman terhadap privasi individu, potensi pencurian identitas, hingga risiko sosial dan finansial akibat penyalahgunaan data. Oleh karena itu, penelitian ini berangkat dari urgensi untuk memahami bagaimana data pribadi dapat terekspos secara terbuka, serta bagaimana metode investigasi berbasis *Open Source Intelligence* (OSINT) dapat digunakan untuk mengidentifikasi dan menganalisis kerentanan tersebut.

Metode penelitian menggunakan pendekatan OSINT hibrida, yang menggabungkan teknik *Google Dorking* untuk menelusuri dokumen digital terindeks publik dan *Social Media Intelligence* (SOCMINT) untuk memprofilkan informasi dari media sosial. Alat yang digunakan meliputi operator pencarian lanjutan Google, validasi melalui *bot* ekstraksi data, serta analisis jejak digital dari platform seperti Instagram dan LinkedIn. Proses penelitian mengikuti tahapan sistematis: *Pre-Engagement* (penetapan tujuan dan batasan), *Information Gathering* (pengumpulan data), *Analysis & Correlation* (pengolahan dan korelasi data), hingga *Reporting* (penyajian hasil dan risiko). Pendekatan ini memastikan bahwa proses investigasi dapat direplikasi oleh peneliti lain dengan tetap memperhatikan batasan etika dan regulasi perlindungan data pribadi.

Hasil penelitian menunjukkan bahwa data sensitif yang paling sering terekspos meliputi nama lengkap, Nomor Induk Kependudukan (NIK), nomor telepon, alamat rumah, serta riwayat pendidikan. Kebocoran ini sebagian besar berasal dari dokumen lama yang terindeks mesin pencari dan unggahan media sosial yang tidak terlindungi. Penelitian ini berkontribusi dalam memberikan pemahaman mendalam mengenai efektivitas OSINT dalam mengidentifikasi kebocoran data, sekaligus menegaskan potensi ancaman *doxing* dan penipuan berbasis rekayasa sosial. Hasil penelitian dapat dimanfaatkan oleh akademisi, praktisi keamanan siber, maupun masyarakat umum untuk meningkatkan kesadaran terhadap manajemen jejak digital. Selain itu, penelitian lanjutan direkomendasikan untuk mengintegrasikan OSINT dengan teknologi *machine learning* dan analitik big data, sehingga deteksi kebocoran data dapat dilakukan secara lebih cepat, adaptif, dan komprehensif di masa depan.

Kata kunci: OSINT, Google Dorking, Kebocoran Data, Data Pribadi Sensitif, *Doxing*.

ABSTRACT

The rapid development of information technology and increasing internet usage in Indonesia have posed serious challenges to the protection of sensitive personal data. Data leaks occur not only through system hacking but also through passive digital footprints that are publicly indexed without the owner's knowledge. This situation has significant impacts, ranging from threats to individual privacy, potential identity theft, to social and financial risks resulting from data misuse. Therefore, this research is motivated by the urgency of understanding how personal data can be publicly exposed, and how Open Source Intelligence (OSINT)-based investigative methods can be used to identify and analyze these vulnerabilities.

The research method uses a hybrid OSINT approach, combining Google Dorking techniques to search publicly indexed digital documents and Social Media Intelligence (SOCMINT) to profile information from social media. The tools used include advanced Google search operators, validation through data extraction bots, and digital footprint analysis from platforms like Instagram and LinkedIn. The research process followed a systematic process: Pre-Engagement (determining objectives and limitations), Information Gathering (data collection), Analysis & Correlation (data processing and correlation), and Reporting (presenting results and risks). This approach ensures that the investigation process can be replicated by other researchers while adhering to ethical constraints and personal data protection regulations.

The results show that the most frequently exposed sensitive data includes full names, National Identification Numbers (NIK), telephone numbers, home addresses, and educational histories. These leaks primarily originate from old documents indexed by search engines and unprotected social media posts. This research contributes to a deeper understanding of the effectiveness of OSINT in identifying data leaks, while also highlighting the potential threats of doxing and social engineering-based fraud. The research findings can be utilized by academics, cybersecurity practitioners, and the general public to raise awareness of digital footprint management. Furthermore, further research is recommended to integrate OSINT with machine learning technology and big data analytics, enabling faster, more adaptive, and more comprehensive data leak detection in the future.

Keyword: OSINT, Google Dorking, Data Leaks, Sensitive Personal Data, Doxing.