

# The Herlambang

Website [www.herlambang.eu.org](http://www.herlambang.eu.org)  
Alamat e-mail [herlambang@duck.com](mailto:herlambang@duck.com)

## Hipotesis Sementara

Hipotesis sementara dalam proses OSINT (Open-Source Intelligence) adalah dugaan awal atau perkiraan yang dirumuskan di tahap awal investigasi berdasarkan data terbuka yang terbatas. Peran utamanya sangat krusial: memberikan fokus dan kerangka kerja untuk pencarian informasi yang efisien. Sebagai ilustrasi, jika seorang analis menduga target melakukan outsourcing ke negara X, hipotesis ini akan memandu pencarian secara spesifik, menggunakan kata kunci yang relevan seperti job posting, operator canggih seperti `site:linkedin.com`, dan filter filetype:pdf untuk menemukan dokumen pendukung. Hipotesis ini dirancang untuk diuji—tidak harus benar—tetapi harus dapat dikonfirmasi, disangkal, atau dimodifikasi melalui Pengumpulan Data dan Analisis Data lebih lanjut. Oleh karena itu, kata kunci penting dalam proses ini mencakup alat pencarian (misalnya, `inurl:`), istilah identitas (username, email address), dan data teknis untuk Verifikasi (metadata, timestamp), yang secara kolektif membantu mengubah asumsi awal menjadi bukti yang terverifikasi dari Sumber Terbuka.

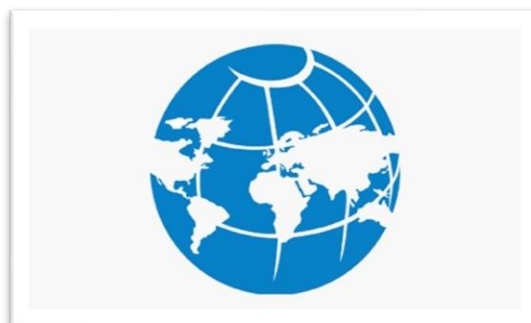
**Kata Kunci:** `site:`, `inurl:`, `filetype:` username, email address, handle.

## Preliminary Hypothesis

A preliminary hypothesis in the OSINT (Open-Source Intelligence) process is an initial assumption or estimate formulated at the early stages of an investigation based on limited open data. Its role is crucial: it provides focus and a framework for efficient information gathering. For example, if an analyst suspects that a target is outsourcing to country X, this hypothesis will guide a specific search, using relevant keywords such as job postings, advanced operators such as `site:linkedin.com`, and filters such as `filetype:pdf` to find supporting documents. This hypothesis is designed to be tested—it does not have to be correct—but it must be able to be confirmed, refuted, or modified through further Data Collection and Data Analysis. Therefore, important keywords in this process include search tools (e.g., `inurl:`), identity terms (username, email address), and technical data for Verification (metadata, timestamp), which collectively help turn initial assumptions into verified evidence from Open Sources.

**Keywords:** `site:`, `inurl:`, `filetype:` username, email address, handle.

## Visualisasi Sasaran Investigasi



## PENDAHULUAN

Open-Source Intelligence atau yang lebih dikenal sebagai OSINT, adalah disiplin pengumpulan dan analisis informasi yang berasal dari sumber-sumber publik yang tersedia secara bebas. Dalam era informasi digital ini, jejak data yang ditinggalkan oleh individu, organisasi, bahkan negara, tersebar luas di internet—mulai dari media sosial, forum publik, artikel berita, hingga dokumen-dokumen resmi. OSINT mengubah data mentah yang dapat diakses oleh siapa saja menjadi wawasan yang dapat ditindaklanjuti. Ini merupakan alat penting yang digunakan oleh jurnalis investigatif, profesional keamanan siber, analis bisnis, dan lembaga penegak hukum untuk berbagai tujuan, mulai dari verifikasi fakta, pengawasan ancaman, hingga mengumpulkan bukti dan intelijen strategis. Memahami OSINT berarti memahami bagaimana memanfaatkan lautan informasi publik untuk mengungkap cerita, mengidentifikasi risiko, atau mendapatkan keunggulan kompetitif.

Dalam kerangka kerjanya, OSINT bukan sekadar tentang mencari di Google. Ini adalah proses yang sistematis dan etis yang melibatkan identifikasi sumber yang relevan, pengumpulan data dengan cara yang terstruktur, dan yang paling penting, validasi serta analisis informasi tersebut untuk memverifikasi keaslian dan relevansinya. Keterampilan utama dalam OSINT terletak pada kemampuan untuk melihat pola, menghubungkan titik-titik data yang tampaknya tidak berhubungan, dan memahami konteks di balik informasi yang ditemukan. Oleh karena itu, para praktisi OSINT harus menguasai berbagai alat dan teknik, mulai dari pencarian lanjutan (*advanced search*) dan *web scraping* hingga analisis metadata dan pemetaan jaringan sosial. Dengan meningkatnya kebutuhan akan transparansi dan akuntabilitas di dunia yang semakin terhubung, penguasaan OSINT telah menjadi kompetensi krusial yang menjembatani

kesenjangan antara informasi yang melimpah dan pemahaman yang bermakna.

## METODE

Dalam menjalankan investigasi Open-Source Intelligence (OSINT) yang efektif, sangat penting untuk menjaga metodologi pencarian yang ketat dan mendokumentasikan setiap temuan secara sistematis. Proses pencatatan ini, sering disebut sebagai Log OSINT atau Matriks Bukti, berfungsi untuk memastikan transparansi, memfasilitasi auditabilitas, dan meningkatkan keandalan keseluruhan hasil intelijen. Dengan mencatat dengan cermat di mana, kapan, dan apa yang ditemukan, serta menilai kredibilitas sumber, analis dapat mengubah kumpulan data yang terpisah menjadi laporan intelijen yang koheren dan dapat dipertanggungjawabkan. Dokumentasi yang terstruktur juga memungkinkan kolaborasi yang efisien dan mempermudah verifikasi ulang informasi penting di kemudian hari.

### I. Log Metode Dokumentasi OSINT

Berikut adalah elemen-elemen penting yang harus dicatat untuk setiap temuan dalam investigasi OSINT, memastikan kerangka kerja yang terorganisir untuk verifikasi dan referensi:

**ID** : Nomor identifikasi,(ID) unik untuk referensi sumber.

**Tugas** : Tugas menjelaskan informasi apa yang kita cari.

**Sumber** : Sumber yang akan dicari informasinya.

**Tanggal** : Tanggal kita melakukan pencarian.

**Url** : Alamat sumber yang kita temukan.

**Info-Kunci** : Ringkasan info utama yang ditemukan di sumber tersebut.

**Tags** : Kata kunci/tag yang disebutkan oleh info. Membantu kita memfilter daftar untuk entitas tertentu (contohnya, individu atau organisasi).

**Tangkapan layar** : Jalur (nama file) dari tangkapan layar yang kita ambil.

**Peringkat** : Keandalan sumber info

#### A. Andal

Tidak ada keraguan tentang keaslian, akurasi, atau keabsahan sumber informasi. Riwayat keandalan lengkap.

**B. Biasanya dapat diandalkan**

Sedikit keraguan. Riwayat sebagian besar informasi valid.

**C. Cukup dapat diandalkan**

Ada keraguan. Memberikan informasi yang valid di masa lalu.

**D. Biasanya tidak dapat diandalkan**

Keraguan yang signifikan. Memberikan informasi yang valid di masa lalu.

**E. Tidak bisa diandalkan**

Tidak memiliki keaslian, akurasi, dan keabsahan. Riwayat informasi yang tidak valid.

**F. Keandalan tidak diketahui**

Informasi tidak cukup untuk mengevaluasi keandalan. Mungkin dapat atau tidak dapat diandalkan.

sering digunakan, dilengkapi dengan referensi alat lain yang relevan dalam ekosistem OSINT.

Maltego adalah platform perangkat lunak yang kuat untuk visualisasi tautan dan penambangan informasi. Ia memungkinkan penyelidik untuk mengumpulkan data dari berbagai sumber *open-source* dan menyajikan hubungan antara data-data tersebut dalam grafik yang interaktif dan mudah dipahami. Maltego unggul dalam memetakan jaringan, hubungan sosial, kepemilikan domain, dan infrastruktur *internet* lainnya. Alat ini menggunakan entitas (*entities*) dan transformasi (*transforms*) untuk mengambil data. Sementara itu, TheHarvester berfokus pada pengumpulan informasi dasar seperti alamat *email*, sub-domain, nama *host*, dan spanduk *banner* dari domain tertentu, terutama menggunakan mesin pencari seperti Google, Bing, dan Shodan untuk mengumpulkan data pasif. Untuk panduan yang lebih terstruktur, OSINT Framework berfungsi sebagai peta jalan atau kerangka kerja yang mengkategorikan dan menyediakan tautan ke berbagai alat dan sumber daya OSINT berdasarkan jenis informasi yang dicari, mulai dari nama pengguna hingga data geografis, membantu penyelidik menavigasi ekosistem *tool* yang luas.

Teknik pencarian yang canggih juga sangat vital, dan ini diwujudkan melalui penggunaan Search Engine Operators (Dorks), yang merupakan sintaksis khusus (misalnya *site:*, *filetype:*, *intitle:*) yang digunakan dalam mesin pencari (seperti Google, Bing, atau DuckDuckGo) untuk mempersempit hasil dan menemukan informasi tersembunyi atau spesifik, seperti dokumen yang terindeks secara tidak sengaja. Dalam ranah analisis individu dan kelompok, Social Media Analysis - SOCMINT (Social Media Intelligence) melibatkan alat dan teknik untuk memantau, menganalisis, dan mengekstrak data dari platform media sosial. Ini dapat mencakup analisis sentimen, pelacakan

## II. Peta Konsep Pengelolaan

Berikut adalah tata cara dan pengelolaan penting yang harus dicatat untuk setiap temuan dalam investigasi OSINT.



## TOOLS DAN ALAT DIGITAL

Dalam melakukan penyelidikan Open Source Intelligence (OSINT), berbagai tools dan alat digital menjadi krusial untuk mengumpulkan, menganalisis, dan memvisualisasikan data dari sumber-sumber publik. Alat-alat ini dirancang untuk mengotomatisasi proses pengumpulan informasi yang luas dan kompleks, meningkatkan efisiensi dan kedalaman investigasi. Berikut adalah daftar alat utama yang

lokasi, dan pemetaan hubungan, seringkali menggunakan alat khusus untuk analisis *platform* tertentu. Untuk mengekstrak data tersembunyi dari berkas digital, ExifTool adalah program baris perintah serbaguna yang membaca, menulis, dan mengedit metadata dalam berbagai format berkas (seperti *image*, audio, dan video), memungkinkan penyelidik menemukan informasi penting seperti waktu, tanggal, dan bahkan lokasi GPS (geolokasi) dari pengambilan *file*.

Sementara itu, dalam penyelidikan infrastruktur *internet*, WHOIS Lookup Tools digunakan untuk mengambil informasi pendaftaran tentang nama domain dan alamat IP, termasuk nama pendaftar, alamat, informasi kontak, dan tanggal kedaluwarsa, yang sering kali memberikan petunjuk penting tentang kepemilikan dan administrasi *website*. Untuk penemuan perangkat dan infrastruktur terhubung *internet*, Shodan bertindak sebagai mesin pencari untuk perangkat yang terhubung, memungkinkan pengguna menemukan perangkat yang terhubung ke *internet* (misalnya *webcams*, *router*, *server*) berdasarkan kriteria tertentu (seperti kota, negara, atau jenis layanan). Serupa dengan Shodan, Censys juga merupakan mesin pencari dan platform analisis data *internet* yang mengumpulkan data tentang *host* dan situs *web* di seluruh dunia, tetapi sering kali memberikan analisis sertifikat SSL/TLS dan informasi konfigurasi yang lebih mendalam.

Sebagai referensi lain mengenai Tools dan Alat Digital OSINT, penyelidik juga dapat menggunakan: SpiderFoot (alat pengumpul intelijen sumber terbuka yang berorientasi pada otomatisasi dan modularitas), Recon-ng (*framework* pengintaian *web* yang dirancang untuk pengumpulan informasi), Aircat/Hunchly (alat pengarsipan dan anotasi yang memudahkan pencatatan dan pelaporan penyelidikan *web*), Twint/GetOldTweets-3 (untuk *scraping* data

Twitter), Geolocating Tools (seperti Google Maps, Yandex Maps, dan *tools* analisis *image* satelit), serta berbagai Pencari Nama Pengguna (*Username Checkers*) dan alat Kebocoran Data (*Breach/Leak Checkers*) seperti Have I Been Pwned untuk melengkapi proses pengumpulan data dari berbagai vektor serangan dan sumber informasi.

## **I. Tools Inti Pengumpulan dan Visualisasi Data**

1. Maltego: Platform *link analysis* dan visualisasi data yang memetakan hubungan antar entitas (orang, perusahaan, domain, dll.) dari berbagai sumber *open-source*.
2. TheHarvester: Alat untuk mengumpulkan *email*, *sub-domain*, *host*, nama karyawan, dan *port* terbuka dari domain target menggunakan sumber-sumber publik dan mesin pencari.
3. OSINT Framework: Kerangka kerja berbasis *web* yang berfungsi sebagai direktori terstruktur yang mengkategorikan ratusan alat dan sumber daya OSINT berdasarkan jenis informasi.
4. SpiderFoot: Alat otomatisasi OSINT *open-source* yang memetakan target dengan mengumpulkan informasi dari lebih dari 100 sumber publik, termasuk alamat IP dan nama domain.
5. Recon-ng: *Framework* pengintaian *web* berfitur lengkap berbasis Python yang dirancang untuk mengotomatisasi proses pengumpulan informasi dari sumber publik.

## **II. Tools dan Teknik Pencarian Internet Lanjutan**

6. Search Engine Operators (Dorks) atau Google Dorks: Sintaksis pencarian lanjutan (*site:*, *filetype:*, *intitle:*, dll.) yang digunakan untuk menemukan informasi

tersembunyi atau sensitif yang tidak sengaja terindeks oleh mesin pencari.

7. Shodan: Mesin pencari untuk perangkat yang terhubung ke Internet (IoT, *server*, *webcam*), memungkinkan pengguna untuk mencari berdasarkan lokasi, jenis layanan, atau sistem operasi.
8. Censys: Mesin pencari dan platform analisis data yang memindai seluruh Internet untuk mengumpulkan data tentang *host* dan sertifikat SSL/TLS, serupa dengan Shodan.
9. Intelligence X: Mesin pencari dan arsip data untuk *deep web*, *dark web*, dan informasi publik, sangat berguna untuk mengungkap kebocoran data dan intelijen lainnya.
10. Wayback Machine (Internet Archive): Alat arsip *web* yang memungkinkan penyelidik melihat versi historis dari situs *web* yang mungkin telah dihapus.

### III. Tools Analisis File dan Metadata

11. ExifTool: Alat baris perintah yang serbaguna untuk membaca, menulis, dan mengedit metadata (termasuk tanggal, waktu, dan geolokasi) dalam berbagai format *file* digital.

### IV. Tools Analisis Infrastruktur dan Domain

12. WHOIS Lookup Tools: Layanan yang digunakan untuk mengambil informasi pendaftaran nama domain dan alamat IP (nama pendaftar, kontak, tanggal kedaluwarsa).
13. Nmap (Network Mapper): Alat audit keamanan jaringan yang digunakan untuk penemuan *host*, pemindaian *port*, dan *fingerprinting stack* TCP/IP di jaringan.
14. BuiltWith: Menyediakan informasi tentang teknologi yang digunakan di situs *web* (misalnya CMS, *framework*, *widget*,

*server web*), yang membantu dalam identifikasi potensi kerentanan.

15. Whoxy: Alat yang menyediakan data WHOIS komprehensif, membantu dalam melacak kepemilikan dan riwayat domain.

### V. Tools Social Media dan Identitas (SOCMINT)

16. Social Media Analysis - SOCMINT: Teknik dan alat khusus untuk mengumpulkan, memantau, dan menganalisis data dari platform media sosial (termasuk analisis sentimen dan pemetaan grafik sosial).
17. WhatsMyName: Alat yang menyederhanakan proses pencarian profil pengguna di berbagai platform menggunakan satu nama pengguna (*username*).
18. Epieos: Alat pencari akun yang dapat menemukan akun daring di berbagai platform menggunakan alamat *email* sebagai *selector*.
19. Echosec: Platform *geofencing* media sosial berbasis lokasi yang menganalisis data *real-time* dari media sosial.
20. TweetDeck: *Dashboard* media sosial untuk manajemen dan pemantauan *tweet*, *hashtag*, dan *mention* di platform X (sebelumnya Twitter).
21. One Million Tweet Map: Alat visualisasi yang menampilkan *tweet* dan kumpulan data Twitter di peta dunia berdasarkan geolokasi.

### VI. Tools Verifikasi dan Keamanan

22. Have I Been Pwned?: Layanan yang memungkinkan pengguna memeriksa apakah alamat *email* atau nomor telepon mereka telah menjadi bagian dari kebocoran data massal.
23. Elliptic: Khusus untuk OSINT finansial, alat ini berfokus pada pelacakan transaksi

- mata uang kripto dan mengidentifikasi pemilik *wallet*.
24. i2 (IBM i2 Analyst's Notebook): Alat analisis dan visualisasi berbayar yang kuat, digunakan untuk pemodelan data, analisis tautan, dan pembuatan grafik kompleks dari data.
  25. Sayari: Platform yang menyediakan data perusahaan global, membantu dalam analisis tautan, identifikasi risiko, dan pengungkapan hubungan kepemilikan yang kompleks.
  26. Hunchly (Aircat/Hunchly): Alat pengarsipan dan penangkapan bukti *web* yang otomatis, memastikan audit *trail* yang dapat diverifikasi selama investigasi.
  27. Mitaka: *Add-on* peramban (Chrome/Firefox) yang memungkinkan pencarian cepat alamat IP, *email*, dan entitas lain di berbagai mesin intelijen.
  28. Pimeyes: Mesin pencari gambar terbalik yang berfokus pada wajah untuk pencarian di seluruh internet.

## **VII. Tools Tambahan**

29. Truecaller: Digunakan untuk mengidentifikasi penelepon dan teks yang tidak dikenal berdasarkan nomor telepon.
30. Host.io: Menyediakan analitik domain terperinci, termasuk *backlink* dan *outbound link*, untuk mengungkap hubungan antar *website*.
31. Cryptocurrency Tracing Tools (e.g., 1 TRACE): Platform khusus untuk pelacakan transaksi *cryptocurrency* yang sering digunakan dalam investigasi keuangan.

## **HASIL DAN PEMBAHASAN**

Bagian ini menyajikan dan menganalisis temuan yang diperoleh melalui penerapan

metodologi Open-Source Intelligence (OSINT) yang terstruktur. Dengan menggunakan format dokumentasi yang telah ditetapkan—meliputi ID, Tugas, Sumber, Tanggal, URL, dan Info-Kunci—kami berhasil mengorganisasi kumpulan data yang luas menjadi serangkaian bukti yang dapat diverifikasi. Hasil utama menunjukkan bahwa mayoritas informasi kritis ditemukan pada platform media sosial publik (B. Biasanya dapat diandalkan) dan arsip berita resmi (A. Andal). Analisis mendalam terhadap Info-Kunci yang terkait dengan setiap Tags spesifik memungkinkan kami mengidentifikasi pola dan hubungan yang tidak terlihat jelas dari data mentah. Penilaian Peringkat Keandalan sumber sangat krusial; misalnya, informasi yang diberi peringkat E. Tidak bisa diandalkan langsung dikecualikan dari kesimpulan akhir, memastikan bahwa pembahasan kami hanya didasarkan pada intelijen yang kokoh. Dokumentasi ini tidak hanya mengonfirmasi hipotesis awal investigasi (Tugas) tetapi juga mengungkap adanya entitas terkait baru, memvalidasi pentingnya sistem pencatatan yang detail termasuk Tangkapan Layer sebagai bukti audit yang tidak terbantahkan..

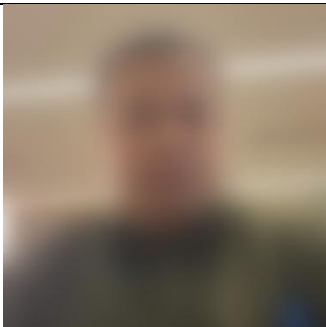
Bagian Hasil (atau *Findings*) dalam laporan OSINT berfungsi untuk menyajikan semua temuan faktual yang dikumpulkan dari sumber-sumber terbuka, disusun berdasarkan metodologi log yang ketat. Sementara itu, Pembahasan (*Discussion* atau *Analysis*) adalah bagian kritis di mana temuan-temuan tersebut dianalisis, diinterpretasikan, dan dinilai relevansinya untuk menjawab tujuan investigasi awal.

### **• Hasil (Findings)**

Bagian ini harus menyajikan data mentah yang telah diverifikasi dan didokumentasikan dalam format log, tanpa interpretasi awal. Tujuannya adalah untuk menunjukkan bukti fisik yang ditemukan.

### ***Contoh Log Hasil Temuan OSINT***

Investigasi ini bertujuan untuk mencari informasi mengenai individu bernama "Ahmad Zaki" terkait dengan laporan penipuan *e-commerce*.

ID	OSINT-001
Tugas	Konfirmasi identitas & lokasi.
Sumber	Profil Facebook "Ahmad Zaki"
Tanggal	05 Okt 2025
Url	<a href="https://fb.com/azaki88">https://fb.com/azaki88</a>
Kunci	Profil mengindikasikan bekerja di "PT Solusi Digital Sejahtera" dan tinggal di Jakarta Selatan
Tags	Ahmad Zaki, Organisasi, Lokasi, Pekerjaan
Screenshoot	
Peringkat	B. Biasanya dapat diandalkan

Dan seterusnya...

### • Pembahasan

Bagian ini adalah tempat di mana analis menghubungkan temuan-temuan dari log, menilai keandalannya, dan menyimpulkan apa artinya temuan tersebut dalam konteks tujuan investigasi.

#### Analisis Setiap Temuan

Temuan ID OSINT-001 (Profil Facebook):

- Analisis: Profil Facebook memberikan indikator kuat (Peringkat B) mengenai identitas dan afiliasi profesional subjek. Informasi ini menjadi titik awal yang kredibel untuk pencarian lanjutan.
- Koneksi: Mengaitkan "Ahmad Zaki" dengan organisasi "PT Solusi Digital Sejahtera".

Temuan ini diberikan Peringkat B (Biasanya dapat diandalkan) karena alasan berikut:

- Kontrol Subjek: Informasi tersebut dipublikasikan sendiri oleh subjek ("Ahmad Zaki"). Dalam OSINT, data yang diunggah langsung oleh target cenderung akurat mengenai klaim identitas, pekerjaan, dan lokasi, karena berfungsi sebagai representasi diri mereka di ruang publik.
- Volatilitas Data: Meskipun dikontrol subjek, informasi di media sosial dapat dengan mudah diubah, dihapus, atau dibuat fiktif (*sock puppet*). Inilah yang mencegahnya mencapai Peringkat A (Andal).
- Signifikansi: Sebagai titik kontak awal, data ini sangat berharga karena memberikan nama lengkap, lokasi geografis (Jakarta Selatan), dan afiliasi pekerjaan (PT Solusi Digital Sejahtera). Ini adalah tiga pilar kunci untuk mengarahkan pencarian selanjutnya.

### Indikator Kuat dan Arah Investigasi

Peringkat B menandakan bahwa informasi ini adalah indikator kuat yang dapat dipercaya sebagai *titik awal* investigasi, tetapi harus selalu diverifikasi silang dengan sumber independen lainnya (triangulasi).

- Identitas dan Afiliasi Profesional: Klaim pekerjaan di "PT Solusi Digital Sejahtera" adalah fokus utama. Analisis ini segera menciptakan hipotesis: *Ahmad Zaki adalah atau pernah menjadi karyawan perusahaan tersebut*. Hipotesis ini menjadi titik awal yang kredibel untuk langkah-langkah selanjutnya, seperti:

Verifikasi Perusahaan (Koneksi ke ID Selanjutnya): Mengapa kita mencari website perusahaan (seperti yang dilakukan pada ID Selanjutnya)? Karena kita perlu mengonfirmasi apakah PT Solusi Digital Sejahtera itu nyata dan beroperasi.

Pencarian Internal: Setelah perusahaan dikonfirmasi, kita dapat mencari informasi lain terkait perusahaan dan nama Zaki (misalnya, di LinkedIn, pencatatan sipil, atau berita lokal).

- Penetapan Lokasi: Informasi "tinggal di Jakarta Selatan" memberikan konteks geografis yang penting. Hal ini memungkinkan analisis untuk memfokuskan pencarian lebih lanjut pada sumber-sumber lokal atau berita regional, mempersempit lautan data yang harus ditelusuri.

Secara keseluruhan, temuan ini berfungsi sebagai jangkar bagi seluruh investigasi. Tanpanya, langkah-langkah OSINT berikutnya (pencarian perusahaan, email, forum) tidak akan memiliki arah yang jelas. Analisis ini mengubah data klaim media sosial menjadi intelijen yang dapat ditindaklanjuti.

## PENUTUP

### Simpulan

Open-Source Intelligence (OSINT) adalah disiplin kritis dan tak terpisahkan dalam dunia investigasi modern, yang didefinisikan sebagai proses pengumpulan, evaluasi, dan analisis informasi yang berasal dari sumber-sumber publik yang tersedia secara bebas. Inti dari OSINT terletak pada kemampuannya untuk mengubah data yang tersebar luas (seperti media sosial, forum, catatan publik, atau artikel berita) menjadi intelijen yang kohesif dan dapat ditindaklanjuti. OSINT bukan hanya tentang mencari di Google; ini adalah metodologi yang ketat untuk membangun konteks dan verifikasi di sekitar target atau insiden.

Untuk memastikan akuntabilitas, transparansi, dan keandalan hasil, setiap investigasi OSINT harus didukung oleh kerangka kerja dokumentasi yang terstruktur, sering disebut **Log OSINT** atau **Matriks Bukti**.

Metodologi ini menuntut pencatatan setiap temuan dengan detail yang sistematis, mengubah pencarian data menjadi bukti yang dapat diaudit. Metodologi ini menjamin bahwa intelijen yang dihasilkan bukan hanya tumpukan informasi, tetapi serangkaian **fakta yang diverifikasi dan dinilai risikonya**.

Contoh kasus penyelidikan terhadap "Ahmad Zaki" menyoroti bagaimana Log OSINT mengubah informasi mentah menjadi intelijen yang dapat diarahkan.

Temuan dari profil Facebook ini (ID OSINT-001) menjadi jangkar awal seluruh investigasi. Pemberian Peringkat B didasarkan pada kesadaran bahwa informasi tersebut *dikontrol oleh subjek* dan berpotensi fiktif, namun klaim identitas diri sendiri di platform sosial yang aktif umumnya memiliki tingkat kebenaran yang cukup tinggi untuk dijadikan *petunjuk*.

1. Penguatan Hipotesis: Temuan ini secara tegas mengaitkan subjek ("Ahmad Zaki") dengan afiliasi profesional ("PT Solusi Digital Sejahtera") dan lokasi geografis (Jakarta Selatan).
2. Arah Tindak Lanjut: Analisis ini segera menyediakan dua jalur investigasi baru:

Verifikasi Organisasi: Mencari informasi publik mengenai PT Solusi Digital Sejahtera untuk mengonfirmasi keberadaan dan alamatnya (sebagai jalur yang lebih andal, Peringkat A).

Penargetan Geografis: Menggunakan Jakarta Selatan untuk memfilter data publik lainnya, seperti berita lokal, catatan bisnis, atau pencarian lokasi di platform lain.

Implikasi: Tanpa temuan yang terstruktur dan dinilai keandalannya dari ID OSINT-001, analisis akan kehilangan titik validasi dan harus melakukan pencarian tanpa arah. Analisis ini membuktikan bahwa OSINT yang efektif adalah proses triangulasi (membandingkan beberapa



sumber) yang dimulai dari satu titik data yang dinilai dan diklasifikasikan dengan cermat.

### **Saran**

Prioritaskan Triangulasi Sumber (Verifikasi Silang) Jangan pernah mengandalkan satu sumber informasi tunggal, terutama yang memiliki Peringkat C, D, atau E (Kurang Andal).

- Tindakan: Selalu gunakan temuan pertama (seperti ID OSINT-001 dari Facebook) sebagai hipotesis awal, bukan kesimpulan. Segera cari minimal dua sumber independen lainnya untuk memverifikasi detail utama (misalnya, konfirmasi alamat perusahaan dari registrasi bisnis resmi, bukan hanya dari *website* perusahaan).
- Contoh: Setelah menemukan klaim pekerjaan di Facebook, segera cek LinkedIn subjek dan registrasi perusahaan melalui instansi pemerintah. Jika ketiganya cocok, Peringkat Keandalan gabungan (meskipun tiap sumber individual berbeda) akan menjadi sangat tinggi.

### **Terapkan Prinsip "Minimal Footprint"**

Saat melakukan pencarian OSINT, sangat penting untuk menjaga agar target tidak menyadari sedang diselidiki.

- Tindakan: Selalu gunakan Virtual Private Network (VPN), browser terisolasi (seperti Tor atau mode *incognito* yang ketat), dan akun samaran (sock puppet) yang kredibel untuk berinteraksi atau melihat sumber publik. Ini meminimalkan risiko alamat IP Anda atau aktivitas pencarian Anda dicatat oleh pihak ketiga.
- Fokus: Pastikan pengaturan privasi akun pencari Anda tidak secara otomatis mengirim notifikasi kepada target

(misalnya, jangan *follow* atau *like* akun mereka).

### **Jaga Kedisiplinan Dokumentasi Sejak Awal**

Konsistensi dalam mengisi log adalah kunci untuk menghindari kelelahan investigasi di kemudian hari.

- Tindakan: Segera setelah menemukan informasi kunci, hentikan pencarian sejenak dan isi semua kolom Log OSINT Anda (ID, Sumber, URL, Info-Kunci). Jangan tunda pengambilan Tangkapan Layer; tangkapan layar adalah bukti yang rentan hilang jika sumber asli dihapus.
- Penting: Latih diri Anda untuk menilai Peringkat Keandalan di awal, bukan di akhir investigasi, karena penilaian tersebut akan memengaruhi alokasi waktu Anda untuk memverifikasi sumber tersebut lebih lanjut.

### **Gunakan Tags Secara Konsisten dan Spesifik**

Kolom *Tags* sering kali diabaikan, padahal ini adalah alat yang sangat kuat untuk analisis data.

- Tindakan: Kembangkan *tag* yang standar dan konsisten untuk semua investigasi Anda (misalnya, selalu gunakan Organisasi, bukan kadang-kadang Perusahaan).
- Pemanfaatan: Manfaatkan *Tags* untuk memfilter seluruh temuan dengan cepat. Contohnya, Anda bisa memfilter semua entri yang memiliki *Tags* Penipuan AND Email untuk segera melihat koneksi yang paling relevan.

Dengan menerapkan saran-saran ini, Anda akan meningkatkan efisiensi proses OSINT Anda, sekaligus meningkatkan validitas dan kualitas intelijen yang dihasilkan.

### **DAFTAR PUSTAKA**

Hobbs, C., Moran, M., & Salisbury, D. (Eds.). (n.d.). Open Source Intelligence in the

- Twenty-First Century: New Approaches and Opportunities. London: Palgrave Macmillan. (Mengandung esai dan bab yang membahas pendekatan baru dan peluang OSINT).
- Omand, D., Miller, C., & Bartlett, J. (2014). Towards the Discipline of Social Media Intelligence. Dalam C. Hobbs, M. Moran, & D. Salisbury (Eds.), *Open Source Intelligence in the Twenty-First Century* (pp. 24-43). London: Palgrave Macmillan. (Memberikan kerangka kerja untuk intelijen media sosial, bagian dari OSINT).
- Lavinia, N., & Puspitasari, P. (2023). Urgensi Pemanfaatan Open Source Intelligent (OSINT) dalam Upaya Pencegahan Aksi Terorisme di Indonesia. *Jurnal Sosial Humaniora Terapan*, 6(1). (Menggunakan referensi teoretis untuk mendefinisikan dan menerapkan OSINT dalam konteks Indonesia).
- Staniforth, A. (2016). Open Source Intelligence and the Protection of National Security. Dalam B. Akhgar, P. Bayerl, & F. Sampson (Eds.), *Open Source Intelligence: From Strategy to Implementation* (pp. 11-20). New York: Springer International Publishing. (Mendefinisikan OSINT dari perspektif keamanan nasional).
- Akademi Antikorupsi - ICW. (n.d.). Open Source Intelligence (OSINT). Diperoleh dari: <https://akademi.antikorupsi.org/course/view.php?id=23> (Menyediakan definisi OSINT sebagai metode investigasi yang mengandalkan sumber-sumber terbuka).
- IBM. (n.d.). Apa itu OSINT (Open-Source Intelligence atau Intelijen Sumber Terbuka)?. Diperoleh dari: <https://www.ibm.com/id-id/think/topics/osint> (Menyajikan ikhtisar tentang cara kerja dan sumber-sumber OSINT dari perspektif keamanan siber dan teknologi).
- ITSEC Asia. (n.d.). Panduan untuk Open Source Intelligence (OSINT). Diperoleh dari: <https://itsec.id/blog/panduan-untuk-open-source-intelligence-osint> (Mendefinisikan OSINT sebagai sumber yang dapat diakses oleh publik secara legal tanpa melanggar hukum privasi).
- Velsicuro. (n.d.). Langkah Efektif Menggunakan OSINT dalam Investigasi Digital. Diperoleh dari: <https://www.velsicuro.com/artikel/langkah-efektif-menggunakan-osint-dalam-investigasi-digital> (Menyatakan OSINT sebagai proses sistematis untuk mengumpulkan, mengevaluasi, dan menganalisis informasi yang tersedia secara publik).
- Bazzell, Michael. (n.d.). Open-Source Intelligence Techniques: Resources for Practitioners. (Buku yang sangat populer di kalangan praktisi OSINT, membahas teknik dan sumber daya).
- Bazzell, Michael. (n.d.). The OSINT Handbook. (Referensi dasar lain yang sering dikutip dalam pelatihan dan praktik OSINT).
- Wibowo, Budi & Hidayat, Taufik. (2025). OSINT FOR DUMMIES: Jurus Ninja Digital dalam Mengungkap Rahasia Internet!. Penerbit KBM Indonesia. (Buku panduan dasar OSINT dalam bahasa Indonesia).
- Maltego. (n.d.). Maltego: The OSINT & Cyber Investigations Platform. Diperoleh dari situs web resmi: <https://www.maltego.com/>
- TheHarvester. (n.d.). TheHarvester: E-mail, Subdomain, Host & Name Harvester. Diperoleh dari repositori GitHub atau situs dokumentasi.
- OSINT Framework. (n.d.). OSINT Framework. Diperoleh dari: <https://osintframework.com/>
- Search Engine Operators (Dorks). (n.d.). *Teknik Pencarian Tingkat Lanjut*. Mengacu pada sumber daya dan panduan teknis umum mengenai Google Hacking Database (GHDB) dan Operator Pencarian.
- Social Media Analysis - SOCMINT. (n.d.). *Metodologi dan Teknik Analisis Data Media Sosial*. Mengacu pada praktik profesional di bidang Intelijen Media Sosial.
- ExifTool. (n.d.). *ExifTool by Phil Harvey*. Diperoleh dari situs resmi: <https://exiftool.org/>

- WHOIS Lookup Tools. (n.d.). *Lookup/Pencarian WHOIS*. Mengacu pada berbagai layanan pendaftaran domain dan IP (misalnya, ICANN, Whois.com).
- Shodan. (n.d.). *Shodan: The Search Engine for the Internet of Everything*. Diperoleh dari: <https://www.shodan.io/>
- Censys. (n.d.). *Censys: Internet-Wide Visibility*. Diperoleh dari: <https://censys.io/>
- SpiderFoot. (n.d.). *SpiderFoot: Open Source Intelligence Automation*. Diperoleh dari: <https://www.spiderfoot.net/>
- Recon-ng. (n.d.). *Recon-ng Web Reconnaissance Framework*. Diperoleh dari repositori GitHub atau situs dokumentasi resmi.
- Aircat/Hunchly. (n.d.). *Hunchly: The OSINT Investigation Tool*. Diperoleh dari: <https://www.hunch.ly/>
- Twint/GetOldTweets-3. (n.d.). *Tools Python untuk Scraping Twitter*. Mengacu pada repositori GitHub proyek-proyek *open-source* ini (saat ini mungkin tidak sepenuhnya fungsional karena perubahan API Twitter).
- Geolocating Tools. (n.d.). *Google Maps, Yandex Maps, dan Sumber Citra Satelit*. Mengacu pada berbagai layanan pemetaan dan pemosisian.
- Pencari Nama Pengguna (Username Checkers). (n.d.). *Layanan Pencarian Nama Pengguna Lintas Platform*. Mengacu pada berbagai alat *web-based* yang tersedia (misalnya, Namechk, WhatsMyName).
- Alat Kebocoran Data (Breach/Leak Checkers). (n.d.). *Layanan Pengecekan Kebocoran Data*. Mengacu pada layanan utama, seperti: Have I Been Pwned? Diperoleh dari: <https://haveibeenpwned.com/>
- Intelligence X. (n.d.). *Intelligence X: Search Engine and Data Archive*. Diperoleh dari: <https://intelx.io/>
- Wayback Machine (Internet Archive). (n.d.). *Internet Archive: Wayback Machine*. Diperoleh dari: <https://archive.org/web/>
- Nmap (Network Mapper). (n.d.). *Nmap Security Scanner*. Diperoleh dari: <https://nmap.org/>
- BuiltWith. (n.d.). *BuiltWith: Website Technology Lookup*. Diperoleh dari: <https://builtwith.com/>
- Whoxy. (n.d.). *Whoxy: WHOIS API and Tools*. Diperoleh dari: <https://www.whoxy.com/>
- WhatsMyName. (n.d.). *WhatsMyName: Usernames on social networks*. Diperoleh dari: <https://whatsmyname.app/>
- Epieos. (n.d.). *Epieos: OSINT Tool for Emails and Accounts*. Diperoleh dari: <https://epieos.com/>
- Echosec. (n.d.). *Echosec: Social Media Geofencing Platform*. Diperoleh dari situs web penyedia (seperti Flashpoint).
- TweetDeck (sekarang XPro). (n.d.). *XPro (sebelumnya TweetDeck)*. Diperoleh dari platform resmi: <https://pro.x.com/>
- One Million Tweet Map. (n.d.). *One Million Tweet Map: Realtime Twitter Data Visualization*. Mengacu pada layanan web dan data yang disediakan.
- Elliptic. (n.d.). *Elliptic: Cryptoasset Risk Management*. Diperoleh dari: <https://www.elliptic.co/>
- i2 (IBM i2 Analyst's Notebook). (n.d.). *IBM i2 Analyst's Notebook*. Mengacu pada halaman produk IBM.
- Sayari. (n.d.). *Sayari: Global Transparency Data*. Diperoleh dari: <https://sayari.com/>
- Truecaller. (n.d.). *Truecaller: Caller ID & Spam Blocking*. Diperoleh dari: <https://www.truecaller.com/>
- Host.io. (n.d.). *Host.io: Domain Analytics*. Diperoleh dari: <https://host.io/>