ANALISIS FORENSIK DIGITAL TERHADAP PERDAGANGAN DATA PRIBADI DI *DARK WEB* MENGGUNAKAN *OSINT & THREAT INTELLIGENCE*

SKRIPSI

DISUSUN OLEH

AHMAD AL QODRI AZIZI DALIMUNTHE

NPM. 2109020031

PROGRAM STUDI TEKNOLOGI INFORMASI

FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI

UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA

MEDAN

2025

ANALISIS FORENSIK DIGITAL TERHADAP PERDAGANGAN DATA PRIBADI DI *DARK WEB* MENGGUNAKAN *OSINT & THREAT INTELLIGENCE*

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer (S.Kom) dalam Program Studi Teknologi Informasi pada Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Muhammadiyah Sumatera Utara

AHMAD AL QODRI AZIZI DALIMUNTHE
NPM. 2109020031

PROGRAM STUDI TEKNOLOGI INFORMASI
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
MEDAN
2025

LEMBAR PENGESAHAN

Judul Skripsi	:	Analisis Forensik Digital Terhadap Perdagangan Data Pribadi Di *Dark Web* Menggunakan *OSINT* & *Threat Intelligence*
Nama Mahasiswa	:	Ahmad Al Qodri Azizi Dalimunthe
NPM	:	2109020031
Program Studi	:	Teknologi Informasi

Menyetujui
Komisi Pembimbing

Mulkan Azhari S.Kom., M.Kom.
NIDN. 0108129402

Ketua Program Studi
Teknologi Informasi

Fatma Sari Hutagalung S.Kom., M.Kom.
NIDN. 0117019301

Dekan

Dr. Al-Khowarizmi, S.Kom., M.Kom.
NIDN. 0127099201

i

PERNYATAAN ORISINALITAS

ANALISIS FORENSIK DIGITAL TERHADAP PERDAGANGAN DATA PRIBADI DI DARK WEB MENGGUNAKAN OSINT & THREAT INTELLIGENCE

SKRIPSI

Saya menyatakan bahwa karya tulis ini adalah hasil karya sendiri, kecuali beberapa kutipan dan ringkasan yang masing-masing disebutkan sumbernya.

Medan, Juli 2025

Yang membuat pernyataan

Ahmad Al Qodri Azizi Dalimunthe

NPM. 2109020031

ii

PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademika Universitas Muhammadiyah Sumatera Utara, saya bertanda tangan dibawah ini:

Nama	: Ahmad Al Qodri Azizi Dalimunthe
NPM	: 2109020031
Program Studi	: Teknologi Informasi
Karya Ilmiah	: Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Muhammadiyah Sumatera Utara Hak Bedas Royalti Non-Eksekutif *(Non-Exclusive Royalty free Right)* atas penelitian skripsi saya yang berjudul:

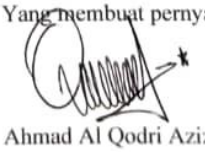
ANALISIS FORENSIK DIGITAL TERHADAP PERDAGANGAN DATA PRIBADI DI DARK WEB MENGGUNAKAN OSINT & THREAT INTELLIGENCE

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksekutif ini, Universitas Muhammadiyah Sumatera Utara berhak menyimpan, mengalih media, memformat, mengelola dalam bentuk database, merawat dan mempublikasikan Skripsi saya ini tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis dan sebagai pemegang dan atau sebagai pemilik hak cipta.

Demikian pernyataan ini dibuat dengan sebenarnya.

Medan, Juli 2025

Yang membuat pernyataan



Ahmad Al Qodri Azizi Dalimunthe

NPM. 2109020031

iii

RIWAYAT HIDUP

DATA PRIBADI

Nama Lengkap	: Ahmad Al Qodri Azizi Dalimunthe
Tempat dan Tanggal Lahir	: Medan, 31 Oktober 2003
Alamat Rumah	: Jalan Karya Gg Wakaf No. 11
Telepon/Faks/HP	: 081280978017
E-mail	: ahmadalqodridalimunthe@gmail.com
Instansi Tempat Kerja	: -
Alamat Kantor	: -

DATA PENDIDIKAN

SD	: SD Negeri 060849	TAMAT: 2015
SMP	: SMP Negeri 7 Medan	TAMAT: 2018
SMA	: SMA Negeri 3 Medan	TAMAT: 2021

KATA PENGANTAR

Assalamualaikum Warrahmatullahi Wabarakatuh

Alhamdulillah, Puji dan syukur penulis panjatkan kehadirat Allah SWT yang telah memberikan penulis kesehatan dan kesempatan khususnya kepada penulis dalam menyelesaikan penyusunan skripsi ini dengan judul "Analisis Forensik Digital Terhadap Perdagangan Data Pribadi di *Dark Web* menggunakan *OSINT* dan *Threat Intelligence*" sebagai salah satu syarat kelulusan untuk memperoleh gelar Sarjana pada Program Studi Teknologi Informasi, Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Muhammadiyah Sumatera Utara.

Penulis tentunya berterima kasih kepada berbagai pihak dalam dukungan serta doa dalam penyelesaian skripsi. Penulis juga mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. Agussani, M.AP., Rektor Universitas Muhammadiyah Sumatera Utara (UMSU)
2. Bapak Dr. Al-Khowarizmi, S.Kom., M.Kom. Dekan Fakultas Ilmu Komputer dan Teknologi Informasi (FIKTI) UMSU.
3. Ibu Fatma Sari Hutagaulung S.Kom., M.Kom. Ketua Program Studi Teknologi Informasi.
4. Bapak Muhammad Basri S.Kom., M.Kom. Sekretaris Program Studi Teknologi Informasi

5. Bapak Mulkan Azhari S.Kom., M.Kom. selaku dosen pembimbing yang telah dengan sabar membimbing, mengarahkan, dan memberikan masukan yang sangat berharga dalam proses penyusunan skripsi ini
6. Seluruh dosen dan staf akademik khususnya di Program Studi Teknologi Informasi yang telah memberikan ilmu, pengetahuan, dan pengalaman selama masa studi.
7. Kedua orang tua tercinta saya yaitu Bapak Muhammad Khaidir Dalimunthe dan Ibu Suriatik yang selalu memberikan doa, motivasi, dan dukungan moral maupun material.
8. Kedua Saudari saya yaitu Nur Khumairah Dalimunthe dan Thohirah Al Fajri Dalimunthe S.Bns yang juga turut ikut memberikan doa, motivasi, dan masukan kepada saya.
9. Miranda Dewi selaku pasangan yang telah menemani saya dari mulai awal perkuliahan sampai dengan saat ini yang juga selalu memberikan saran dan masukan kepada saya.
10. Teman-teman "Punyaku Grup" yaitu Yoga, Gatot, Rifqi, Anggi, Farhan, Ikhsan, dan Mubarton yang selalu berdiskusi bersama terkait dengan akademik yang kami jalani selama 8 semester di Universitas Muhammadiyah Sumatera Utara.
11. Semua pihak yang terlibat langsung ataupun tidak langsung yang tidak dapat penulis ucapkan satu-persatu yang telah membantu penyelesaian skripsi ini.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Oleh karena itu, kritik dan saran yang membangun sangat penulis harapkan demi perbaikan di masa yang akan datang. Semoga skripsi ini dapat memberikan manfaat bagi pembaca dan dapat menjadi referensi bagi penelitian selanjutnya dan saya sangat berharap skripsi saya bisa menjadi landasan pendidikan terkait dengan ilmu Cyber Security khususnya Digital Forensik yang cukup jarang dibahas secara mendalam.

Medan, Juli 2025

Penulis

ANALISIS FORENSIK DIGITAL TERHADAP PERDAGANGAN DATA PRIBADI DI *DARK WEB* MENGGUNAKAN *OSINT* & *THREAT INTELLIGENCE*

ABSTRAK

Kebocoran data pribadi yang diperjualbelikan di Dark Web menjadi isu yang semakin mengkhawatirkan, terutama setelah kasus yang menimpa Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi (Kemendikbudristek) pada tahun 2024. Penelitian ini bertujuan untuk menganalisis pola perdagangan data pribadi di Dark Web dengan pendekatan forensik digital yang didukung oleh metode Open Source Intelligence (OSINT) dan Threat Intelligence. Penelitian dilakukan dengan studi kasus terhadap data yang dibagikan oleh akun “grepcn” di forum LeakBase dan disebarkan ulang oleh akun “knox” di DarkForums. Proses investigasi dilakukan melalui pemantauan pasif, analisis struktur data dengan tools seperti Python dan NetworkX, serta validasi email menggunakan platform OSINT seperti HaveIBeenPwned dan IntelX. Hasilnya menunjukkan bahwa data pribadi diperjualbelikan dalam format SQL dan disembunyikan di balik sistem berbayar menggunakan mata uang kripto. Sebagian besar data yang dianalisis terbukti valid dan pernah mengalami kebocoran. Penelitian ini menunjukkan bahwa pendekatan gabungan OSINT dan Threat Intelligence dapat digunakan secara efektif untuk mendeteksi dan menganalisis aktivitas perdagangan data pribadi di Dark Web, serta memberikan gambaran awal mengenai ancaman siber yang semakin berkembang.

Kata Kunci: Dark Web, Forensik Digital, OSINT, Threat Intelligence, Kebocoran Data

DIGITAL FORENSIC ANALYSIS OF PERSONAL DATA TRADING ON THE DARK WEB USING OSINT & THREAT INTELLIGENCE

ABSTRACT

The illicit trade of personal data on the Dark Web has become an increasingly concerning issue, especially following the 2024 data breach incident involving Indonesia's Ministry of Education, Culture, Research, and Technology. This research aims to analyze the patterns of personal data trading on the Dark Web using a digital forensic approach combined with Open Source Intelligence (OSINT) and Threat Intelligence methods. The study is based on a case involving data leaked by a user named "grepcn" on LeakBase and re-shared by "knox" on DarkForums. The investigation involved passive monitoring, data structure analysis using tools such as Python and NetworkX, and email validation using OSINT platforms like HaveIBeenPwned and IntelX. The results show that the personal data was distributed in SQL format and hidden behind paid content systems using cryptocurrency. Most of the data analyzed was confirmed to be valid and previously breached. This study demonstrates that combining OSINT and Threat Intelligence can effectively support the detection and analysis of personal data trading activities on the Dark Web, while also providing insights into the growing landscape of cyber threats.

Keywords: Dark Web, Digital Forensics, OSINT, Threat Intelligence, Data Breach

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Dalam era digital, perkembangan teknologi informasi dan komunikasi telah membawa perubahan besar dalam kehidupan manusia. Dalam prosesnya, data pribadi menjadi semakin penting dan sensitif karena banyak aktivitas yang dilakukan secara *online*. Data pribadi mencakup informasi seperti nama, alamat, nomor identitas, informasi finansial, riwayat kesehatan, dan informasi sensitif lainnya yang berkaitan dengan individu (Anggen Suari & Sarjana, 2023).

Kebocoran data terjadi karena sistem informasi mempunyai kerentanan yang dapat dieksploitasi di mana biasanya berasal dari kurangnya akan kesadaran keamanan informasi atau kesalahan mendasar dalam konfigurasi sistem. Ketika terjadi insiden kebocoran data, seringkali penyebab dan pelaku kejadian tidak diketahui sehingga diperlukan investigasi untuk mendapatkan informasi mengenai pelaku dan penyerangannya. Salah satu kerugian yang terjadi adalah penyalahgunaan data pribadi akibat kebocoran data yang telah tersebar luas secara terbuka di dunia maya (Risman Saputra & Arizal, 2023).

Dalam banyak kasus, pelanggaran data bukan hanya disebabkan oleh serangan eksternal (external threat), tetapi juga karena adanya individu di dalam organisasi yang secara sengaja maupun tidak sengaja membocorkan informasi sensitif. Menurut IBM pada tahun 2024, 83% organisasi melaporkan mengalami setidaknya satu serangan dari dalam (*insider attack*) dalam 12 bulan terakhir (IBM, 2024)

Salah satu bagian dari *Deep web* adalah *Dark Web*, bagian internet yang satu ini tidak dapat ditemukan menggunakan *search engine* seperti Google, Yahoo atau sejenisnya. Dikarenakan hal tersebut maka kejahatan siber sering kali terjadi pada bagian internet ini, situs-situs yang melakukan transaksi ilegal bisa ditemukan jika memiliki alamat url dari situsnya yang berbeda dari url pada *Surface web* dikarenakan situs situs *Dark Web* menggunakan domain dot onion. Karena sulit dilacak, *Dark Web* sering digunakan sebagai tempat komunikasi yang anonim, khususnya oleh pelaku aktivitas ilegal. *Software* yang paling umum digunakan adalah PGP (*Pretty Good Privacy*) sebagai layanan enkripsi (Nugranto & Koprawi, 2024).

Dark Web adalah bagian tersembunyi dari internet yang sering dikaitkan dengan aktivitas ilegal. Berbeda dengan *Surface Web* yang dapat diindeks oleh mesin pencari seperti Google dan Bing, *Dark Web* tidak dapat diakses menggunakan *browser* biasa. Untuk mengaksesnya, diperlukan perangkat lunak khusus seperti TOR. Darknet sendiri menjadi wadah bagi berbagai layanan tersembunyi, yang kerap dimanfaatkan untuk aktivitas ilegal, seperti perdagangan narkoba dan penjualan senjata. Tingkat anonimitas yang tinggi di *Dark Web* menjadikannya tempat yang menarik bagi pelaku kejahatan, sehingga menimbulkan tantangan besar bagi aparat penegak hukum dan pakar keamanan siber (Reddy Gopireddy, 2020).

Pada September 2024, Indonesia kembali diguncang oleh insiden kebocoran data berskala besar yang menimpa salah satu instansi yaitu Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi (Kemendikbudristek), di mana data

internal mereka termasuk nama lengkap, alamat IP, alamat email, lokasi pengguna, hingga informasi akun pengguna terekspos dan diperjualbelikan secara bebas di *Dark Web*.

Data tersebut dibocorkan oleh seorang aktor siber dengan nama samaran @grepcn melalui forum *LeakBase*, salah satu komunitas perdagangan data ilegal yang populer di *Dark Web*, yang menjadi pengganti dari *BreachForums* setelah ditutup oleh FBI. Kasus ini bukan hanya menyoroti lemahnya infrastruktur keamanan siber nasional, tetapi juga menunjukkan bagaimana forum-forum tersembunyi digunakan sebagai sarana perdagangan data sensitif yang bersifat strategis.

Insiden ini dilaporkan oleh *Communication & Information System Security Research Center* (CISSReC) sebagai bagian dari rangkaian serangan siber besar sepanjang tahun 2024, dengan total kerugian dari berbagai insiden mencapai ratusan miliar rupiah (Rachmatunnisa, 2024). Oleh karena itu, dibutuhkan pendekatan investigasi forensik digital yang mendalam berbasis *Open Source Intelligence (OSINT)* dan *Threat Intelligence* untuk mengungkap struktur data, pola perdagangan, serta aktor ancaman yang terlibat dalam ekosistem *Dark Web*.

Penjualan data hasil pelanggaran keamanan (*data breach*) di forum-forum *Dark Web* telah menjadi perhatian serius dalam dunia keamanan siber. Forum-forum ini berfungsi sebagai platform bagi pelaku kejahatan siber untuk memperdagangkan informasi rahasia dan produk ilegal. Sebuah penelitian mengembangkan model tanpa pengawasan untuk mengidentifikasi dan mengkarakterisasi forum-forum *Dark Web*, menunjukkan bahwa forum-forum ini

secara signifikan dieksploitasi untuk perdagangan informasi rahasia dan produk ilegal oleh para kriminal (Nazah et al., 2021).

Dalam mendukung proses investigasi forensik digital terhadap kebocoran data pribadi, teknik *Open Source Intelligence* (*OSINT*) digunakan untuk mengumpulkan informasi dari sumber terbuka seperti media sosial, forum diskusi, situs web, dan berbagai repositori data publik. *OSINT* tidak hanya digunakan untuk memperoleh informasi terkait suatu insiden keamanan siber, tetapi juga dapat membantu dalam profiling pelaku serangan, mengidentifikasi infrastruktur yang digunakan oleh penyerang, serta melacak pergerakan data curian di berbagai platform digital. Dengan kemampuannya dalam mengekstrak informasi dari berbagai sumber terbuka, *OSINT* menjadi alat penting dalam investigasi pasca-insiden, terutama dalam kasus *phishing*, serangan *ransomware*, kebocoran data, dan ancaman *Advanced Persistent Threats* (APT).

Selain itu, *Threat Intelligence* memainkan peran penting dalam mendeteksi, mengantisipasi, dan mencegah serangan siber dengan cara menganalisis pola serangan yang berkembang secara global. *Threat Intelligence* memungkinkan organisasi untuk memahami karakteristik serangan, mengenali indikator kompromi *(Indicators of Compromise/IoC),* serta memprediksi potensi ancaman di masa depan dengan memanfaatkan data dari berbagai sumber. Dengan memanfaatkan *Threat Intelligence Platform* (TIP), organisasi dapat mengklasifikasikan ancaman berdasarkan teknik dan taktik yang digunakan oleh penyerang. Selain itu, dengan adanya pemodelan ancaman yang tepat, organisasi dapat mempercepat waktu respons terhadap insiden siber serta mengurangi dampak dari serangan yang terjadi.

Dalam konteks penelitian ini, integrasi antara Digital Forensik, *OSINT*, dan *Threat Intelligence* akan menjadi fokus utama dalam menganalisis dan mengevaluasi metode yang paling efektif untuk investigasi pasca-insiden siber. Penelitian ini akan membahas bagaimana *OSINT* dapat mendukung proses pengumpulan bukti digital dengan lebih efisien, bagaimana *Threat Intelligence* dapat meningkatkan kemampuan deteksi ancaman serta strategi mitigasi, serta bagaimana analisis forensik digital dapat membantu mengungkap jejak serangan secara lebih mendalam. Dengan memahami keterkaitan ketiga aspek ini, penelitian ini bertujuan untuk memberikan kontribusi dalam pengembangan strategi keamanan siber yang lebih efektif, khususnya dalam menghadapi tantangan serangan siber yang semakin kompleks dan terstruktur.

1.2. Rumusan Masalah

Penelitian ini merumuskan sejumlah permasalahan utama, yaitu sejauh mana *Open Source Intelligence (OSINT)* mampu mendeteksi dan memperoleh informasi terkait kebocoran data pribadi yang terjadi di *Dark Web*, serta bagaimana pola perdagangan data pribadi berlangsung di dalamnya. Selain itu, penelitian ini juga berupaya mengevaluasi efektivitas metode *OSINT* dalam mendukung proses investigasi kebocoran data, menganalisis bagaimana pendekatan digital forensik dapat digunakan untuk mengidentifikasi bukti-bukti digital yang relevan, serta mengeksplorasi bagaimana penerapan *Threat Intelligence* dapat membantu dalam mengantisipasi, mendeteksi secara dini, dan merespons berbagai ancaman keamanan siber akibat aktivitas perdagangan data pribadi di *Dark Web*.

1.3. Batasan Masalah

Penelitian ini memiliki batasan sebagai berikut:

1. Fokus pada satu kasus kebocoran data Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi (Kemendikbudristek) tahun 2024 yang diperjualbelikan di forum *Dark Web.*
2. Sumber Data: Fokus pada data yang diperjualbelikan di *Dark Web* yaitu *LeakBase*, forum kejahatan siber, dan *marketplace* illegal seperti *LeakBase* yang dapat diakses menggunakan teknik *OSINT*.
3. Batasan Waktu: Penelitian dilakukan berdasarkan data yang ditemukan selama rentang waktu penelitian berlangsung.
4. Tidak ada transaksi atau pembelian data ilegal yang dilakukan. Semua data yang dianalisis berasal dari sampel yang dipublikasikan secara terbuka oleh penjual di forum *Dark Web*.

1.4. Tujuan Penelitian

Penelitian ini bertujuan untuk:

1. Mengumpulkan dan menganalisis dataset kebocoran data menggunakan *OSINT*.
2. Mengidentifikasi pola perdagangan data pribadi di *Dark Web*.
3. Mengevaluasi efektivitas *OSINT* dalam mendeteksi kebocoran data berdasarkan keterjangkauan dan relevansi informasi yang ditemukan.
4. Penelitian ini juga bertujuan untuk merumuskan pendekatan investigasi terstruktur berbasis *OSINT* dan *Threat Intelligence* terhadap kasus perdagangan data pribadi di *Dark Web*, yang dapat digunakan sebagai kerangka awal dalam penelitian lanjutan maupun implementasi kebijakan keamanan data.

1.5. Manfaat Penelitian

1.5.1 Manfaat Akademik

Penelitian ini diharapkan dapat menjadi kontribusi bagi literatur akademik dalam bidang *Digital Forensik* dan *Threat Intelligence*. Selain itu, penelitian ini dapat menjadi referensi bagi penelitian selanjutnya yang membahas metodologi deteksi kebocoran data menggunakan *OSINT*.

1.5.2 Manfaat Praktis

Dari sisi praktis, hasil penelitian ini dapat digunakan oleh pemerintah, perusahaan teknologi, perbankan, serta individu dalam memahami pola kebocoran data dan meningkatkan langkah-langkah mitigasi keamanan siber.

1.5.3 Manfaat Sosial

Penelitian ini juga dapat meningkatkan kesadaran masyarakat mengenai bahaya kebocoran data pribadi dan bagaimana langkah-langkah yang dapat diambil untuk melindungi informasi pribadi mereka di era digital saat ini.

BAB II

LANDASAN TEORI

2.1. Studi Terdahulu

Tabel 2.1 Studi Terdahulu

No	Penulis (Tahun)	Judul Penelitian	Hasil Penelitian
1	Handika Fajar Nugranto & Muhammad Koprawi (2023)	Investigasi Kejahatan Siber pada *Surface Web* dan *Deep Web* Menggunakan Metode NIST	Menunjukkan efektivitas metode NIST dalam investigasi kejahatan siber di *Surface Web* dan *Deep Web*. Ditemukan bahwa kejahatan yang paling umum di *Surface Web* adalah *hacking* (49%), kebocoran data (36%), dan pornografi (15%), sementara di *Deep Web* lebih beragam, termasuk *hacking* (31%), transaksi narkoba (29%), kebocoran data (26%), dan pornografi (7%)

2	Saiba Nazah et al. (2020)	*Evolution of Dark Web Threat Analysis and Detection: A Systematic Approach*	Studi sistematis tentang ancaman kejahatan di *Dark Web*, mengidentifikasi berbagai metode deteksi seperti analisis *hash*, monitoring lalu lintas jaringan, scraping *marketplace*, dan analisis exit node TOR. Studi ini juga menekankan pentingnya analisis pasar kripto dan forum diskusi untuk investigasi forensik.
3	Dendi Risman Saputra et al. (2023)	*Investigasi Insiden Kebocoran Data Menggunakan Integrasi Melalui Pendekatan Open Source Intelligence dan Detection Maturity Level Model*	Menggunakan *OSINT* yang diintegrasikan dengan *Detection Maturity Level* (DML) Model untuk investigasi kebocoran data. Hasilnya menunjukkan bahwa integrasi ini dapat mengidentifikasi pelaku kejahatan siber lebih efektif.
4	Philipp Kühn, Kyra	*Navigating the Shadows: Manual and*	- Menganalisis *Dark Web* sebagai sumber *Open Source*

	Wittorf, Christian Reuter (2024)	*Semi-Automated Evaluation of the Dark Web for Cyber Threat Intelligence*	*Intelligence (OSINT)* untuk *Cyber Threat Intelligence (CTI).* - Meneliti 65 forum *Dark Web*, 7 toko vendor tunggal, dan 72 *marketplace*. - Menemukan bahwa 88% *marketplace* dan 53% forum mengandung informasi yang relevan dengan keamanan siber. - Mengidentifikasi tantangan dalam pengambilan data seperti *CAPTCHA* dan interaksi manual yang diperlukan.
5	Jyri Rajamäki, Iiro Lahti, Johanna Parviainen (2022)	*OSINT on the Dark Web: Child Abuse Material Investigations*	- Membahas penggunaan *OSINT* dalam investigasi materi eksploitasi anak di *Dark Web.* - Mengidentifikasi tantangan utama dalam investigasi LEA (*Law Enforcement Agencies*), seperti penyimpanan data dan

			aspek hukum. - Menyarankan pendekatan otomatisasi *OSINT* untuk mengurangi paparan terhadap konten ilegal.

Penelitian sebelumnya oleh Nugranto & Koprawi (2024b) meneliti efektivitas metode NIST dalam investigasi kejahatan siber pada *Surface Web* dan *Deep Web*. Studi ini menemukan bahwa *Surface Web* didominasi oleh kejahatan hacking (49%), kebocoran data (36%), dan pornografi (15%), sementara di *Deep Web* lebih bervariasi, termasuk transaksi narkoba dan jual beli senjata. Namun, penelitian ini hanya menekankan pada metode NIST sebagai *framework* utama, tanpa mengintegrasikan pendekatan *Threat Intelligence Lifecycle* yang dapat memberikan perspektif lebih luas mengenai siklus ancaman dan mitigasinya. Sebaliknya, penelitian ini mengombinasikan NIST SP 800-86 dengan *Threat Intelligence Lifecycle*, yang tidak hanya mencakup investigasi bukti digital tetapi juga mencakup bagaimana informasi ancaman diproses, dianalisis, dan digunakan untuk mencegah serangan di masa depan.

Selanjutnya, penelitian oleh Nazah et al. (2020) menyoroti ancaman dan metode deteksi di *Dark Web* melalui pendekatan sistematis. Studi ini berfokus pada berbagai teknik seperti analisis *hash*, monitoring lalu lintas jaringan, *scraping marketplace*, serta analisis *exit node* TOR. Meskipun memberikan wawasan yang kuat dalam analisis ancaman di *Dark Web*, penelitian ini lebih menitikberatkan pada deteksi teknis berbasis machine learning dan monitoring jaringan tanpa

menghubungkannya secara eksplisit dengan metodologi investigasi forensik seperti NIST SP 800-86. Dalam hal ini, penelitian saya menambahkan kerangka kerja investigasi forensik yang lebih struktural, sehingga tidak hanya mendeteksi ancaman tetapi juga menyediakan metodologi yang lebih komprehensif untuk memvalidasi bukti digital dan merancang strategi respons ancaman.

Penelitian lainnya oleh Risman Saputra & Arizal (2023) berfokus pada investigasi kebocoran data menggunakan *Open Source Intelligence* (*OSINT*) yang dikombinasikan dengan *Detection Maturity Level* (*DML*) Model. Hasil penelitian ini menunjukkan bahwa pendekatan *OSINT-DML* efektif dalam mengidentifikasi pelaku dan metode serangan dalam insiden kebocoran data. Namun, penelitian ini masih terbatas pada investigasi kebocoran data dan tidak secara eksplisit membahas bagaimana metode ini dapat diintegrasikan dengan *framework* forensik yang lebih luas, seperti NIST SP 800-86 yang digunakan dalam penelitian ini. Oleh karena itu, penelitian saya menawarkan pendekatan yang lebih holistik dengan menggabungkan forensik digital dan *intelligence lifecycle*, memungkinkan deteksi yang lebih proaktif dan investigasi yang lebih mendalam terhadap berbagai bentuk ancaman siber.

Penelitian yang dilakukan oleh Kuhn et al. (2024) dalam jurnal berjudul *Navigating the Shadows: Manual and Semi-Automated Evaluation of the Dark Web for Cyber Threat Intelligence* lebih berfokus pada eksplorasi *Dark Web* sebagai sumber *Cyber Threat Intelligence (CTI)* secara umum. Penelitian ini mengkaji berbagai forum dan *marketplace* di *Dark Web* untuk mengidentifikasi informasi yang berkaitan dengan keamanan siber, seperti *malware*, layanan peretasan, dan eksploitasi kerentanan sistem. Salah satu temuan penting dari penelitian ini adalah

bahwa 88% *marketplace* dan 53% forum di *Dark Web* mengandung informasi relevan dengan keamanan siber. Selain itu, penelitian ini juga menyoroti tantangan dalam mengumpulkan data dari *Dark Web*, seperti *CAPTCHA*, interaksi manual yang diperlukan, dan mekanisme *anti-crawling*. Namun, penelitian ini tidak secara spesifik membahas perdagangan data pribadi, melainkan lebih berfokus pada bagaimana *Dark Web* dapat menjadi sumber intelijen bagi keamanan siber secara keseluruhan. Sementara itu, penelitian saya memiliki cakupan yang lebih spesifik, yaitu menganalisis perdagangan data pribadi di *Dark Web* serta bagaimana *OSINT* dan *Threat Intelligence* dapat digunakan untuk mendeteksi, melacak, dan menganalisis pola perdagangan tersebut.

Selanjutnya, penelitian oleh Rajamäki (2022) dalam jurnal *OSINT on the Dark Web: Child Abuse Material Investigations* lebih menitikberatkan pada penggunaan *OSINT* dalam investigasi eksploitasi anak di *Dark Web*. Penelitian ini mengidentifikasi tantangan utama yang dihadapi oleh Lembaga Penegak Hukum (LEA) dalam mengumpulkan bukti digital terkait konten ilegal, terutama dalam hal penyimpanan data dan keterbatasan akses terhadap konten yang sifatnya ilegal. Selain itu, penelitian ini juga membahas bagaimana *OSINT* dapat digunakan untuk menargetkan situs atau pengguna yang terkait dengan aktivitas ilegal tersebut tanpa harus mengekspos peneliti terhadap konten berbahaya. Meskipun penelitian ini memberikan wawasan yang relevan dalam konteks investigasi *Dark Web*, fokus utamanya adalah pada eksploitasi anak, bukan perdagangan data pribadi. Penelitian saya, di sisi lain, lebih berorientasi pada bagaimana data pribadi diperjualbelikan di *Dark Web*, termasuk metode yang digunakan oleh pelaku, jenis data yang diperdagangkan, serta bagaimana *OSINT* dan *Threat Intelligence* dapat

dimanfaatkan untuk mendeteksi dan menganalisis pola aktivitas perdagangan data pribadi ini.

Secara keseluruhan, penelitian saya memiliki fokus yang lebih spesifik dibandingkan penelitian sebelumnya, yaitu menyelidiki perdagangan data pribadi di *Dark Web* menggunakan *OSINT* dan *Threat Intelligence*. Sementara studi terdahulu lebih menyoroti keamanan siber secara umum dan kejahatan eksploitasi anak di *Dark Web*, penelitian saya lebih menekankan pada bagaimana data pribadi diperdagangkan, siapa saja aktornya, bagaimana cara transaksi dilakukan, dan bagaimana metode investigasi digital dapat digunakan untuk mengungkap pola perdagangan tersebut. Oleh karena itu, penelitian ini diharapkan dapat memberikan kontribusi dalam mengisi celah penelitian yang belum banyak dikaji sebelumnya, khususnya dalam konteks forensik digital terhadap perdagangan data pribadi di *Dark Web*

2.2. Forensik Digital

Digital forensik adalah cabang dari forensik yang berkaitan dengan identifikasi, pengumpulan, analisis, dan pelestarian bukti digital yang ditemukan dalam perangkat elektronik untuk digunakan dalam investigasi hukum dan keamanan siber. Secara lebih spesifik, digital forensik bertujuan untuk mendapatkan bukti yang sah, memastikan integritas data, serta mengungkap motif, pelaku, dan metode dalam suatu insiden kejahatan digital.

Menurut Hariyadi et al. (2022), Forensik Digital merupakan cabang ilmu bedah atau forensik yang berkaitan dengan barang bukti elektronik dan bukti digital dengan tujuan melakukan identifikasi terkait barang bukti tersebut dalam rangka melakukan pengungkapan fakta-fakta sebagai upaya penegakan hukum atau

peraturan perundangan yang berlaku. Penggunaan perangkat elektronik secara tidak etis sehingga menyebabkan terganggunya sistem komputer dan jaringan dapat dikategorikan sebagai tindak kejahatan digital atau *cybercrime*.

NIST *(National Institute of Standards and Technology)* mendefinisikan digital forensik sebagai bidang ilmu forensik yang berfokus pada pemulihan dan investigasi materi yang ditemukan di perangkat digital, sering kali dalam kaitannya dengan kejahatan komputer. Menurut NIST, digital forensik mencakup serangkaian prosedur standar untuk mengumpulkan, menganalisis, dan mempresentasikan bukti digital. NIST juga menekankan pentingnya penggunaan kerangka kerja yang terstruktur, seperti yang tercantum dalam NIST SP 800-86, untuk memastikan integritas bukti dan validitas investigasi.

2.3. Dark Web

Dark Web adalah bagian kecil dari *Deep Web* (web terdalam) yang sengaja disembunyikan dan hanya dapat diakses melalui jaringan khusus yang menggunakan protokol enkripsi seperti Tor (*The Onion Router*), I2P, atau *Freenet*. Berbeda dengan *Surface Web* (web permukaan) yang terindeks oleh mesin pencari, *Dark Web* memerlukan tools dan konfigurasi khusus untuk mengaksesnya (Nugranto & Koprawi, 2024).

Dark Web adalah bagian dari internet yang tidak dapat diakses menggunakan mesin pencari konvensional seperti Google atau Bing dan memerlukan perangkat lunak khusus, seperti *The Onion Router* (TOR), untuk mengaksesnya. *Dark Web* merupakan subbagian dari *Deep Web*, yaitu bagian internet yang tidak terindeks oleh mesin pencari dan hanya dapat diakses melalui autentikasi tertentu.

Salah satu karakteristik utama dari *Dark Web* adalah anonimitas, yang memungkinkan penggunanya untuk berkomunikasi dan bertukar informasi tanpa identitas mereka dapat dengan mudah dilacak. Hal ini dimungkinkan melalui teknologi enkripsi dan penggunaan jaringan seperti TOR dan I2P yang mengaburkan identitas pengguna dengan merutekan lalu lintas internet melalui beberapa lapisan server sebelum mencapai tujuan akhirnya.

2.3.1. Perbedaan antara *Surface Web, Deep Web,* dan *Dark Web*

Gambar 2.1 *Surface Web, Deep Web, dan Darkweb*

Sumber: https://data-ox.com/surface-web-dark-web-and-deep-web

Internet terdiri dari tiga lapisan utama, yaitu *Surface Web, Deep Web,* dan *Dark Web*. Meskipun *Surface Web* dan *Deep Web* umumnya dimanfaatkan untuk keperluan yang legal, *Dark Web* sering kali menjadi tempat bagi pelaku kejahatan siber untuk melakukan aktivitas ilegal atau tidak etis. Untuk mengakses *Dark Web,* diperlukan peramban khusus seperti Tor,

yang menawarkan tingkat anonimitas tinggi melalui mekanisme enkripsi yang kompleks, sehingga memungkinkan pengguna termasuk pelaku kejahatan untuk menyembunyikan identitas mereka. Internet secara umum dapat dikategorikan ke dalam tiga bagian utama yaitu :

a. Surface Web

Surface Web atau *Visible Web* adalah bagian dari internet yang dapat diakses secara publik dan diindeks oleh mesin pencari seperti Google, Bing, atau Yahoo. Konten pada *Surface Web* mencakup situs web, blog, forum, dan platform media sosial yang dapat diakses tanpa memerlukan autentikasi khusus. Diperkirakan, *Surface Web* hanya mencakup sekitar 4-5% dari keseluruhan konten yang ada di internet.

Contoh: Wikipedia, Facebook, dan situs berita.

b. Deep Web

Deep Web adalah bagian dari internet yang tidak diindeks oleh mesin pencari dan tidak dapat diakses secara langsung melalui pencarian standar. Konten pada *Deep Web* mencakup *database*, arsip, halaman web yang dilindungi kata sandi, dan informasi yang memerlukan autentikasi untuk diakses. *Deep Web* mencakup sekitar 90-95% dari keseluruhan konten internet.

Contoh: basis data akademik, email, akun perbankan online.z

c. Dark Web

Dark Web merupakan lapisan terdalam dari internet yang bersifat tersembunyi dan tidak dapat diakses menggunakan peramban biasa. Untuk mengaksesnya, diperlukan peramban khusus seperti Tor, yang dirancang

untuk melindungi anonimitas pengguna. *Dark Web* tidak diindeks oleh mesin pencari dan menggunakan sistem enkripsi yang memungkinkan penggunanya tetap anonim sepenuhnya. Meskipun dapat digunakan untuk berbagai tujuan, *Dark Web* sering dimanfaatkan oleh pelaku kejahatan siber untuk aktivitas ilegal, seperti perdagangan narkoba, penyebaran konten terlarang, serta transaksi menggunakan mata uang kripto guna menghindari pelacakan.

Perbedaan ini dapat digambarkan dalam bentuk piramida, di mana *Surface Web* hanya mencakup sekitar 4-5% dari total internet, sementara *Deep Web* mencakup mayoritas informasi yang tidak terindeks, dan *Dark Web* merupakan bagian kecil dari *Deep Web* yang hanya dapat diakses melalui jaringan terenkripsi (Davies, 2020).

Berikut merupakan perbandingan singkat antara *Surface Web, Deep Web,* dan *Dark Web* :

Tabel 2.2 Perbandingan *Suface Web*,*Deep Web*,dan *Dark Web*

Aspek	***Surface Web***	***Deep Web***	***Dark Web***
Aksebilitas	Terbuka untuk umum	Memerlukan autentikasi atau izin khusus	Memerlukan perangkat lunak khusus (misalnya, TOR)
Pengindeksan	Diindeks oleh mesin pencari	Tidak diindeks oleh mesin pencari	Tidak diindeks dan disembunyikan

Konten	Informasi publik, berita, media sosial	Data sensitif, basis data, arsip pemerintah	Aktivitas anonim, pasar gelap, forum tersembunyi
Keamanan	Rentan terhadap pelacakan dan monitoring	Lebih aman, namun tetap rentan jika tidak dilindungi	Menawarkan anonimitas tinggi, namun sering digunakan untuk aktivitas ilegal

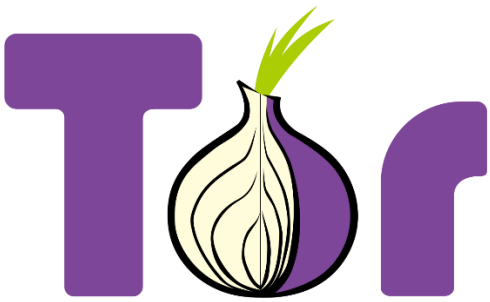
2.3.2. Sejarah dan Perkembangan *Dark Web*

Konsep jaringan anonim pertama kali dikembangkan pada tahun 1990-an oleh *Naval Research Laboratory* Amerika Serikat, yang menciptakan TOR sebagai alat komunikasi rahasia untuk militer dan intelijen. Pada tahun 2004, kode TOR dirilis secara terbuka sebagai proyek *open-source*, memungkinkan siapa saja untuk menggunakannya demi anonimitas di internet.

Sejak saat itu, *Dark Web* berkembang menjadi ekosistem yang kompleks, digunakan oleh berbagai kelompok, termasuk jurnalis, aktivis, serta pelaku kejahatan siber. Salah satu kasus terkenal yang mengangkat perhatian publik terhadap *Dark Web* adalah penutupan Silk Road pada tahun 2013, sebuah pasar gelap daring yang digunakan untuk perdagangan narkotika, senjata, dan data pribadi yang dicuri.

Dark Web terus berkembang dengan munculnya teknologi baru yang meningkatkan anonimitas dan keamanan pengguna, serta meningkatnya upaya penegakan hukum untuk mengawasi dan mengendalikan aktivitas ilegal di dalamnya.

2.3.3. TOR (*The Onion Router*)



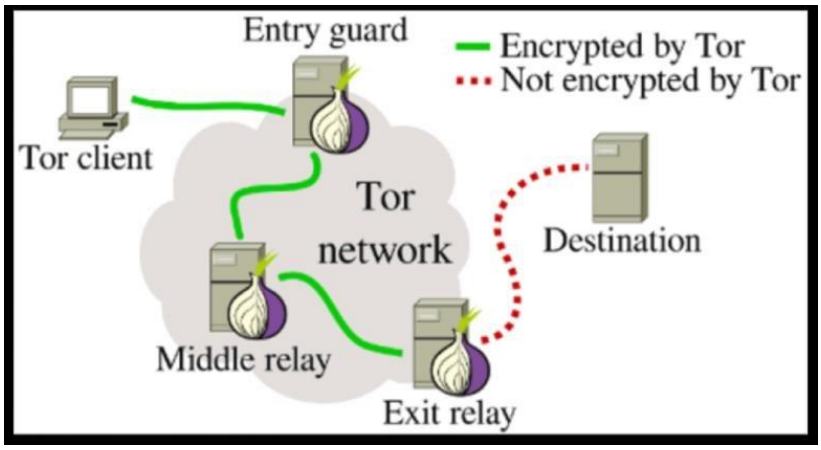
Gambar 2.2 Tor Browser

Sumber : https://www.torproject.org/

Menurut Sanjaya et al. (2020) Tor Browser adalah peramban web yang dirancang khusus untuk melindungi anonimitas penggunanya. Peramban ini banyak digunakan oleh individu yang ingin menjaga privasi mereka serta menghindari sensor saat menjelajahi internet. Seiring dengan perkembangan teknologi, Tor Browser terus mengalami peningkatan signifikan dalam hal keamanan, stabilitas, dan kecepatan akses. Pembaruan yang berkelanjutan memastikan bahwa pengguna dapat menjelajahi web dengan tingkat anonimitas yang lebih baik, sekaligus meminimalkan risiko pelacakan dan pengawasan.

TOR (*The Onion Router*) pertama kali dikembangkan oleh Laboratorium Penelitian Angkatan Laut Amerika Serikat pada pertengahan 1990-an sebagai proyek penelitian untuk menciptakan komunikasi yang anonim di internet. Proyek ini kemudian diadopsi oleh *Electronic Frontier*

Foundation (EFF) dan komunitas *open-source*, yang mengembangkan TOR menjadi jaringan anonimisasi yang dapat digunakan oleh publik. TOR resmi dirilis ke publik pada tahun 2002 dan sejak saat itu menjadi alat utama bagi pengguna yang ingin menjaga privasi mereka di internet.



Gambar 2.3 Simulasi Jaringan TOR

Sumber : Sanjaya et al. (2020)

Jaringan Tor dirancang untuk memberikan anonimitas bagi penggunanya dengan cara meneruskan lalu lintas internet melalui serangkaian server yang disebut sebagai *relay* atau *node*. Relay ini bekerja sama untuk menyembunyikan identitas pengguna dan tujuan komunikasi mereka. Tor menggunakan teknik yang dikenal sebagai *Onion Routing*, di mana data dienkripsi dalam beberapa lapisan sebelum dikirim melalui serangkaian node. Proses ini terdiri dari tiga jenis relay utama:

A. *Entry/Guard Relay* (Relay Masuk/Penjaga)

Relay ini berfungsi sebagai pintu masuk ke jaringan Tor. Ketika pengguna mengakses Tor, mereka akan terhubung terlebih dahulu ke *relay* ini. Meskipun *entry relay* mengetahui alamat IP asli pengguna, *relay* ini tidak

mengetahui tujuan akhir komunikasi karena informasi tersebut dienkripsi. *Entry relay* hanya meneruskan paket data ke *middle relay*.

Pentingnya *entry relay* dalam keamanan:

a. *Entry relay* dipilih dengan hati-hati oleh klien dan biasanya tetap sama selama periode waktu tertentu (*guard relay*) untuk mengurangi risiko serangan *traffic correlation attack*.
b. Jika seorang penyerang mengontrol *entry relay*, mereka dapat mencatat alamat IP pengguna dan berpotensi melakukan serangan *deanonymization* (pengungkapan identitas).

B. *Middle Relay* (Relay Tengah)

Middle relay bertindak sebagai perantara antara *entry relay* dan *exit relay*. Perannya sangat penting karena:

a. *Middle relay* hanya mengetahui bahwa data berasal dari *entry relay* dan akan diteruskan ke *exit relay*, tanpa mengetahui sumber atau tujuan akhir data.
b. Karena *middle relay* tidak pernah terhubung langsung ke pengguna atau ke internet publik, relay ini relatif aman dari ancaman hukum dibandingkan dengan *entry* atau *exit relay*.
c. *Middle relay* memperkuat anonimitas dengan mencegah korelasi antara pengguna dan aktivitas mereka di internet.

C. *Exit Relay* (Relay Keluar)

Exit relay adalah titik terakhir dalam jaringan Tor sebelum data mencapai tujuan akhir (misalnya, situs web yang dikunjungi). Karena *exit relay* adalah node terakhir yang berkomunikasi dengan server tujuan, alamat

IP dari exit relay terlihat oleh server tersebut. Ini memiliki beberapa konsekuensi:

a. **Risiko hukum**: Karena *exit relay* yang berinteraksi langsung dengan internet publik, operatornya sering menghadapi tuduhan penyalahgunaan jaringan, seperti penyebaran malware atau aktivitas ilegal lainnya. Banyak penyedia layanan internet (ISP) memblokir *exit relay* karena alasan ini.
b. **Keamanan pengguna**: Jika *exit relay* dikendalikan oleh aktor jahat (*malicious exit node*), mereka bisa melakukan serangan seperti *Man-in-the-Middle (MitM)* atau *SSL stripping* untuk mencuri informasi sensitif yang tidak terenkripsi.
c. **Kebijakan exit node**: Beberapa *exit relay* menerapkan kebijakan ketat tentang lalu lintas yang mereka izinkan untuk mengurangi kemungkinan penyalahgunaan.

Keamanan dan Tantangan Jaringan Tor

a. Lapisan Enkripsi: Setiap *relay* dalam jaringan hanya mengetahui node sebelum dan sesudahnya, bukan sumber atau tujuan akhirnya. Hal ini membuat sulit bagi pengamat jaringan untuk melacak komunikasi pengguna.
b. Daftar Publik: Semua relay Tor terdaftar dalam daftar publik sehingga siapa pun bisa mengetahui IP address dari node yang tersedia. Ini memungkinkan sensor internet untuk memblokir akses ke Tor dengan memfilter lalu lintas ke alamat-alamat ini.

c. Serangan terhadap Tor: Beberapa serangan seperti *Traffic Analysis* dan *Correlation Attacks* dapat digunakan untuk mencoba mendekripsi jalur komunikasi Tor, terutama jika penyerang mengontrol beberapa relay dalam jaringan.

2.4. Pencurian Data Pribadi

Pencurian data pribadi adalah tindakan memperoleh informasi pribadi seseorang tanpa izin dengan tujuan tertentu, seperti penipuan, pencurian identitas, atau kejahatan siber lainnya. Data yang dicuri dapat mencakup nama lengkap, alamat, nomor identitas (KTP, SIM, paspor), informasi keuangan, kredensial *login*, dan bahkan riwayat medis. Tindakan ini sering terjadi melalui teknik seperti *phishing*, *hacking*, *skimming*, atau eksploitasi celah keamanan sistem elektronik(Anugerah, 2021).

Beberapa faktor utama yang menyebabkan maraknya pencurian data pribadi di internet meliputi:

a. Banyak masyarakat belum memahami pentingnya menjaga keamanan data pribadi mereka. Misalnya, mereka dengan mudah memberikan informasi pribadi di me dia sosial atau mengklik tautan yang tidak jelas keamanannya.
b. Banyak organisasi, termasuk perusahaan dan lembaga pemerintah, masih memiliki sistem keamanan yang rentan. Kebocoran data sering terjadi karena lemahnya proteksi terhadap akses ilegal ke database mereka.
c. Banyak pelaku pencurian data menjual informasi pribadi di *Dark Web* atau menggunakannya untuk aktivitas ilegal seperti *fraud*, *scamming*, dan pencucian uang. Informasi pribadi bernilai tinggi di pasar gelap digital.

d. Banyak individu tidak menggunakan *password* yang kuat atau menggantinya secara berkala. Selain itu, kebiasaan membagikan informasi sensitif di internet tanpa perlindungan yang memadai juga menjadi penyebab utama.

2.5. Open Source Intelligence (OSINT)

Menurut Dokman & Ivanjko (2020) *Open Source Intelligence (OSINT)* adalah metode pengumpulan informasi dari sumber yang terbuka dan dapat diakses oleh siapa saja. Data yang dikumpulkan masih dalam bentuk mentah, kemudian dianalisis dan diolah menjadi informasi yang berguna. Hasil analisis ini disebut sebagai produk intelijen, yang berperan penting dalam kegiatan intelijen untuk mendukung pengambilan keputusan.

Selain itu, menurut Kumar (2024) *Open Source Intelligence (OSINT*) adalah metode pengumpulan informasi yang memanfaatkan sumber daya yang tersedia secara publik untuk menghasilkan intelijen yang dapat digunakan dalam berbagai konteks, termasuk keamanan nasional, penegakan hukum, dan pengambilan keputusan bisnis. *OSINT* memanfaatkan data dari berbagai sumber seperti media sosial, artikel berita, laporan pemerintah, dan publikasi akademis.

OSINT memiliki peran penting dalam mendeteksi ancaman siber, termasuk peretasan data dan aktivitas ilegal di *Dark Web*. Dengan meningkatnya jumlah informasi yang tersedia di internet, *OSINT* memungkinkan penggunanya untuk mengidentifikasi pola dan tren yang mengindikasikan ancaman potensial sebelum menjadi insiden yang lebih besar (Puyvelde & Rienzi, 2025).

OSINT memiliki peran penting dalam *cybersecurity* dan investigasi kriminal. Data yang diperoleh dari sumber terbuka, seperti media sosial dan

database publik, sering digunakan dalam identifikasi ancaman siber, termasuk peretasan data dan aktivitas ilegal di *Dark Web*. Salah satu contoh nyata adalah kasus investigasi FBI pada tahun 2020, di mana *OSINT* digunakan untuk mengidentifikasi seorang tersangka di Philadelphia yang terlibat dalam pembakaran kendaraan polisi selama demonstrasi (Szymoniak & Foks, 2024). Hal ini menunjukkan bagaimana *OSINT* dapat digunakan dalam proses hukum dan investigasi keamanan digital.

Di Indonesia, pemanfaatan *OSINT* telah digunakan dalam beberapa sektor, seperti mendukung pertahanan negara dan mendeteksi ancaman terorisme. Penelitian menunjukkan bahwa *OSINT* dapat membantu mengurangi kerentanan terhadap serangan dengan melakukan analisis proaktif terhadap ancaman dan infrastruktur kritis (Lavinia et al. 2023).

Salah satu tantangan utama dalam penggunaan *OSINT* adalah validitas dan reliabilitas informasi yang diperoleh dari sumber terbuka. Banyak data yang tersedia di internet belum tentu akurat, sehingga memerlukan metode verifikasi yang kuat agar informasi yang digunakan dalam investigasi dapat dipertanggungjawabkan (Samad et al., 2024)

Menurut penelitian yang dilakukan oleh Prasetyo et al. (2023), *OSINT* juga memiliki keterbatasan dalam hal cakupan data yang dapat diakses. Meskipun mampu mengumpulkan informasi dari berbagai sumber, *OSINT* tetap memiliki keterbatasan dalam mendapatkan data dari jaringan tertutup atau data yang telah dienkripsi. Oleh karena itu, *OSINT* perlu dikombinasikan dengan teknik investigasi lainnya agar lebih efektif dalam mendeteksi ancaman digital.

Dengan demikian, *OSINT* terus berkembang sebagai salah satu metode utama dalam forensik digital dan investigasi keamanan siber, terutama dalam mendeteksi perdagangan data ilegal dan aktivitas mencurigakan di *Dark Web* (Szymoniak & Foks, 2024).

2.6. Threat Intelligence

Threat Intelligence (TI) adalah proses memahami ancaman terhadap suatu organisasi berdasarkan data yang tersedia, yang tidak hanya sebatas pengumpulan informasi, tetapi juga memastikan bahwa data tersebut relevan dan dapat digunakan untuk mengambil keputusan strategis. TI merupakan pengetahuan berbasis bukti mengenai ancaman dengan tujuan untuk mencegah serangan atau mempersingkat waktu antara penetrasi dan deteksi (Aljuhami & Bamasoud, 2021).

Selain itu, TI mencakup informasi seperti konteks, mekanisme, indikator, implikasi, serta rekomendasi tindakan terhadap suatu risiko yang sedang berlangsung atau baru muncul. Informasi ini dapat digunakan untuk merespons ancaman dengan lebih efektif. Sumber data TI dapat berasal dari berbagai kanal, baik dari sumber teknis seperti sensor lokal maupun dari sumber manusia seperti diskusi di forum rahasia atau komunikasi dengan pihak lain. Dengan demikian, TI menyediakan wawasan yang mencakup indikator teknis, konteks ancaman, mekanisme serangan, dampak potensial, serta langkah-langkah yang dapat diambil untuk menghadapi ancaman saat ini maupun yang mungkin muncul di masa depan (Aljuhami & Bamasoud, 2021).

Threat Intelligence mencakup berbagai aspek penting, antara lain:

- Konteks Ancaman**:** Informasi yang memberikan pemahaman lebih dalam mengenai ancaman, termasuk siapa pelakunya, bagaimana mereka beroperasi, dan target mereka.
- Indikator Ancaman (*IoC - Indicators of Compromise*): Data spesifik yang menunjukkan adanya ancaman, seperti alamat IP mencurigakan, domain berbahaya, atau *hash* malware.
- Analisis Tren dan Pola: Mengidentifikasi pola serangan siber yang muncul berdasarkan data historis dan prediksi ancaman di masa depan.
- Rekomendasi Tindakan: Langkah-langkah mitigasi yang dapat diambil untuk mencegah atau mengurangi dampak dari ancaman yang teridentifikasi

Menurut Paranjape (2020), integrasi *Cyber Threat Intelligence* (CTI) dalam sistem keamanan siber memungkinkan proses deteksi dan mitigasi ancaman dilakukan secara lebih efisien dan proaktif. Dalam penelitian mereka, dijelaskan bahwa pengumpulan dan analisis data ancaman yang bersumber dari berbagai kanal – seperti *threat feed*, *dark web*, dan sistem internal organisasi – dapat membantu dalam mengenali pola serangan dan mendeteksi indikator kompromi (*Indicators of Compromise/IoC*).

2.7. Linux

Gambar 2.4 Sistem Operasi Linux

Sumber : https://www.vexels.com/png-svg/preview/140692/linux-logo

Linux adalah sistem operasi berbasis *open source* yang dikembangkan dari kernel Unix. Sistem ini memungkinkan pengguna untuk mengakses, memodifikasi, dan mendistribusikan kode sumbernya secara bebas. Linux menjadi populer karena kestabilan, fleksibilitas, dan keamanan yang lebih tinggi dibandingkan dengan sistem operasi komersial lainnya.

Linux merupakan sistem operasi berbasis Unix yang bersifat *open-source* dan banyak digunakan dalam bidang keamanan siber, termasuk digital forensik, *OSINT* (*Open Source Intelligence),* dan *Threat Intelligence*. Keunggulan utama Linux dalam digital forensik terletak pada fleksibilitas, keamanan, serta ketersediaan berbagai alat analisis yang mendukung investigasi terhadap perdagangan data pribadi di *Dark Web*.

Linux terdiri dari beberapa komponen utama:

1. Kernel: Inti dari sistem operasi yang mengelola *hardware* dan sumber daya komputer.

2. *Shell*: *Interface* yang memungkinkan pengguna untuk berinteraksi dengan sistem operasi melalui perintah.
3. *File System*: Struktur direktori yang digunakan untuk mengorganisir data dan file dalam sistem.
4. *Library dan Utilities*: Perangkat lunak tambahan yang membantu dalam menjalankan berbagai aplikasi.

Dalam konteks investigasi digital forensik, Linux sering kali menjadi pilihan utama karena kemampuannya dalam melakukan analisis sistem file, ekstraksi data dari berbagai sumber, serta aksesibilitas terhadap alat-alat khusus yang dikembangkan untuk investigasi forensik dan intelijen siber.

Berbagai distribusi (distro) Linux telah dikembangkan secara khusus untuk kebutuhan digital forensik, *OSINT*, dan *Threat Intelligence*. Berikut merupakan disto linux yang akan digunakan dalam proses penelitian yang akan dipakai oleh peneliti:

2.7.1. CSI Linux

CSI Linux merupakan distribusi Linux yang dirancang khusus untuk investigasi digital forensik dan *OSINT*. Distro ini dilengkapi dengan berbagai alat untuk analisis *Dark Web*, pengumpulan data intelijen dari sumber terbuka, serta pemrosesan bukti digital yang terkait dengan kejahatan siber (CSI LINUX, 2023).

1. Fitur dan Keunggulan CSI Linux

Beberapa keunggulan CSI Linux yang menjadikannya pilihan ideal untuk penelitian forensik dan *OSINT* adalah:

a. *Pre-installed OSINT Tools*: CSI Linux menyediakan lebih dari 100 *tools OSINT* yang siap digunakan, sehingga peneliti tidak perlu repot menginstal satu per satu.
b. Isolasi Aman dalam *Virtual Machine*: CSI Linux dirancang untuk berjalan secara optimal di dalam virtualisasi seperti VirtualBox, sehingga proses investigasi dilakukan dalam lingkungan terisolasi dan aman.
c. Integrasi dengan Tor dan VPN: Memberikan akses anonim dan aman untuk menjelajahi *Dark Web* tanpa mengekspos identitas pengguna.
d. *Workflow Investigatif* yang Terstruktur: CSI Linux memiliki pendekatan modular, dengan *Desktop Investigator, Gateway*, dan *SIEM Console* yang memisahkan antara pengumpulan, analisis, dan dokumentasi.

2. *Tool-Tool Open Source* dalam CSI Linux

Berikut adalah beberapa tools penting yang tersedia dalam CSI Linux dan dapat digunakan dalam penelitian untuk mendukung proses analisis data pribadi di *Dark Web* menggunakan *OSINT* dan *Threat Intelligence*:

1. Tor Browser & Tor Service
    a. Memberikan akses ke jaringan .onion (*Dark Web)* secara anonim.
    b. CSI Linux menyediakan shortcut langsung untuk menjelajahi *Dark Web* melalui Tor secara aman dari dalam VM.
2. *OSINT Framework* (dalam bentuk browser navigasi)
    a. Menu navigasi yang memudahkan investigasi sesuai kategori: akun sosial media, domain, email, data breach, dsb.
    b. Membantu menelusuri jalur investigasi yang sistematis.

2.8. Virtual Box

Gambar 2.5 Oracle *Virtual Box*

VirtualBox adalah perangkat lunak virtualisasi *open-source* yang memungkinkan pengguna menjalankan beberapa sistem operasi (OS) secara simultan pada satu komputer fisik. Dengan *VirtualBox*, pengguna dapat membuat dan mengelola mesin virtual (VM) yang beroperasi di atas sistem operasi host, sehingga memfasilitasi pengujian, pengembangan, dan penggunaan aplikasi lintas platform tanpa memerlukan perangkat keras tambahan (Method Karamagi et al., 2020).

2.8.1. Konsep Dasar Virtualisasi

Virtualisasi adalah teknologi yang memungkinkan pembuatan representasi virtual dari sumber daya komputer, seperti perangkat keras, sistem operasi, penyimpanan, atau jaringan. Tujuan utama virtualisasi adalah meningkatkan efisiensi dan fleksibilitas dalam pengelolaan sumber daya IT. Dengan memisahkan perangkat keras fisik dari sistem operasi dan aplikasi yang berjalan di atasnya, virtualisasi memungkinkan:

a. Isolasi Lingkungan: Setiap VM berjalan secara independen, sehingga kegagalan atau perubahan pada satu VM tidak mempengaruhi VM lainnya.
b. Penggunaan Sumber Daya yang Efisien: Beberapa VM dapat berbagi sumber daya fisik yang sama, mengoptimalkan penggunaan CPU, memori, dan penyimpanan.
c. Kemudahan Pengelolaan dan Pengujian: Administrator dapat dengan mudah membuat, menghapus, atau memodifikasi VM sesuai kebutuhan tanpa mengganggu sistem utama .

2.8.2. Fitur Utama VirtualBox

- Dukungan *Multi-Platform*: VirtualBox dapat diinstal pada berbagai sistem operasi *host*, termasuk Windows, macOS, Linux, dan Solaris.
- Kompatibilitas Luas: Mendukung berbagai sistem operasi *guest*, seperti Windows, Linux, Solaris, dan lainnya.
- Manajemen Perangkat Keras Virtual: Memungkinkan konfigurasi komponen virtual seperti CPU, memori, penyimpanan, dan perangkat jaringan sesuai kebutuhan.
- Fitur Snapshot: Memungkinkan pengguna untuk menyimpan status VM pada titik tertentu dan mengembalikannya nanti, memfasilitasi pengujian dan pemulihan sistem.
- Integrasi dengan *Host*: Menyediakan fitur seperti folder bersama dan *clipboard* bersama antara *host* dan *guest* untuk mempermudah transfer data (Wikipedia, 2025)

BAB III

METODOLOGI PENELITIAN

3.1. Pendekatan dan Metode Penelitian

Penelitian ini menggunakan pendekatan mixed methods, yang menggabungkan pendekatan kualitatif dan kuantitatif untuk memperoleh pemahaman komprehensif mengenai perdagangan data pribadi di *Dark Web*. Pendekatan ini memungkinkan eksplorasi mendalam terhadap fenomena yang kompleks serta pengukuran objektif terhadap variabel yang relevan.

3.1.1. Pendekatan Kualitatif

Pendekatan kualitatif digunakan untuk mengeksplorasi secara mendalam dinamika perdagangan data pribadi di *Dark Web*. Metode ini melibatkan analisis konten terhadap forum-forum dan platform di *Dark Web* yang digunakan untuk transaksi data ilegal.

Data kualitatif dikumpulkan melalui:

a. Observasi partisipatif di berbagai forum dan pasar gelap di *Dark Web*.
b. Analisis dokumen digital, seperti thread diskusi dan listing penjualan data pribadi.
c. Studi kasus dari kebocoran data pribadi yang telah terjadi sebelumnya.

Pendekatan ini memungkinkan pemahaman lebih dalam mengenai motif, pola, dan strategi yang digunakan oleh pelaku kejahatan siber dalam memperdagangkan data pribadi.

3.1.2. Pendekatan Kuantitatif

Pendekatan kuantitatif diterapkan untuk mengukur sejauh mana data pribadi diperjualbelikan di *Dark Web* serta untuk mengidentifikasi tren dan pola statistik terkait aktivitas tersebut.

Data kuantitatif dikumpulkan melalui:

a. Teknik *Open Source Intelligence (OSINT)* dengan alat seperti *HaveIBeenPwned?* dan Intelligence X.
b. *Threat Intelligence* Platforms seperti VirusTotal, dan lainnya.

Hasil analisis digunakan untuk mengidentifikasi jumlah dan jenis data pribadi yang diperjualbelikan, frekuensi transaksi, serta harga yang ditawarkan. Pendekatan ini memanfaatkan analisis statistik untuk menemukan korelasi dan tren yang signifikan dalam perdagangan data pribadi (Lubis, 2023).

3.1.3. Penggabungan Pendekatan Kualitatif dan Kuantitatif

Dengan menggabungkan kedua pendekatan ini, penelitian ini diharapkan dapat memberikan gambaran yang komprehensif mengenai perdagangan data pribadi di *Dark Web*.

a. Pendekatan kualitatif memberikan wawasan mendalam mengenai konteks dan mekanisme perdagangan.
b. Pendekatan kuantitatif memberikan data empiris untuk mengukur skala dan tren fenomena tersebut.

Pendekatan *mixed methods* juga memungkinkan validasi silang antara temuan kualitatif dan kuantitatif, sehingga meningkatkan validitas dan reliabilitas hasil penelitian (Hukom & Setiadi, 2025).

3.2. Alat dan Sumber Data

Dalam penelitian ini, peneliti menggunakan berbagai alat bantu yang dikelompokkan ke dalam dua kategori utama, yaitu *Open Source Intelligence (OSINT) dan Threat Intelligence Platform (TIP)*. Semua alat yang digunakan merupakan perangkat lunak open-source atau versi gratis terbatas (*freemium*), yang tersedia secara legal dan dapat diakses oleh publik.

Penggunaan alat-alat ini bertujuan untuk mendukung proses investigasi digital forensik terhadap perdagangan data pribadi di *Dark Web*, baik dalam hal pengumpulan data, eksplorasi entitas, hingga analisis indikator kompromi *(Indicators of Compromise / IoC).*

Tabel 3. 1 *Tools* Investigasi yang Digunakan

No	Tools	Deskripsi
1	Tor Browser	Digunakan untuk mengakses forum dan marketplace ilegal di Dark Web secara anonim.
2	Intelligence X	Mesin pencari intelijen sumber terbuka untuk memverifikasi kebocoran data (email, domain, file dump) dari berbagai sumber termasuk Dark Web.
3	HaveIBeenPwned	Platform untuk mengecek apakah email/domain korban telah terlibat dalam insiden kebocoran data yang tercatat secara publik.
4	Python + NetworkX	Digunakan untuk parsing data bocor dan memvisualisasikan relasi antar entitas seperti email, IP address, dan institusi korban.

5	VirusTotal	Digunakan untuk memverifikasi reputasi domain atau link eksternal yang disebarkan oleh pelaku di forum, termasuk indikasi malware atau phising.

Tabel 3.2 Perangkat dan Lingkungan Penelitian

No	Komponen	Spesifikasi
1	Laptop Peneliti	Lenovo ThinkPad X280 – Intel Core i7 Gen 8, RAM 16 GB
2	Sistem Operasi	Windows 11 Pro 64 bit
3	Virtual Machine	CSI Linux (dijalankan di VirtualBox), digunakan untuk OSINT dan investigasi aman

Sumber data yang digunakan dalam penelitian ini diperoleh melalui metode observasi pasif di forum-forum Dark Web, khususnya dari:

a. LeakBase.io

Forum yang memuat unggahan akun “@grepcn” yang membagikan data hasil kompromi terhadap instansi pemerintah Indonesia.

b. DarkForums.st

Forum yang memperlihatkan re-upload data oleh akun “Knox”, yang memuat file dalam format SQL dump.

c. Data Sampel Preview yang Dipublikasikan Secara Terbuka

Seluruh data yang dianalisis berupa cuplikan (preview) yang dibagikan secara terbuka oleh pelaku di thread forum — tanpa transaksi atau pembobolan

sistem. Data mencakup seperti nama lengkap, Email, IP address, Instansi, Nomor telepon.

3.3. Model Investigasi Forensik

Penelitian ini mengadopsi model investigasi forensik digital yang disarankan oleh NIST *Special Publication* 800-86, yang terdiri dari empat tahap utama: Pengumpulan (*Collection*), Pemeriksaan (*Examination*), Analisis (*Analysis*), dan Pelaporan (*Reporting*). Model ini memberikan kerangka kerja sistematis untuk mengintegrasikan teknik forensik ke dalam respons insiden keamanan informasi.

Gambar 3.1 NIST SP 800-86

1. Pengumpulan (*Collection*)
   A. Deskripsi: Tahap ini melibatkan identifikasi, pengumpulan, dan pencatatan data yang relevan dari berbagai sumber, termasuk sistem komputer, jaringan, dan perangkat penyimpanan.
   B. Implementasi dalam Penelitian:

a. Mengumpulkan data dari *Dark Web* menggunakan alat seperti Tor Browser.
b. Menggunakan alat *OSINT* untuk mengidentifikasi jejak digital terkait perdagangan data pribadi.

2. Pemeriksaan (*Examination*)

A. Deskripsi: Tahap ini fokus pada pemrosesan dan penyaringan data yang telah dikumpulkan untuk mengidentifikasi informasi yang signifikan, sambil menjaga integritas data.

3. Analisis (*Analysis*)

A. Deskripsi: Tahap ini melibatkan evaluasi data yang telah diperiksa untuk menarik kesimpulan yang berkaitan dengan insiden atau aktivitas yang sedang diselidiki.
B. Implementasi dalam Penelitian:
   a. Menganalisis pola perdagangan data pribadi di *Dark Web* untuk mengidentifikasi tren yang digunakan oleh pelaku.
   b. Menggunakan teknik analisis konten untuk memahami konteks dan signifikansi data yang diperoleh.

4. Pelaporan (*Reporting*)

A. Deskripsi: Tahap akhir ini mencakup dokumentasi temuan, metodologi yang digunakan, dan rekomendasi untuk tindakan selanjutnya.
B. Implementasi dalam Penelitian:
   a. Menyusun laporan forensik yang mendetail yang mencakup temuan utama, metodologi investigasi, dan rekomendasi untuk mitigasi ancaman di masa depan.

3.4. Penerapan *Threat Intelligence Lifecycle*

Gambar 3.2 Threat Intelligence Lifecycle

Sumber : https://threat.media/definition/what-is-the-threat-intelligence-lifecycle/

Penerapan siklus intelijen ancaman yang efektif memungkinkan organisasi untuk secara proaktif mengidentifikasi dan menanggapi ancaman keamanan siber sebelum mereka berkembang menjadi insiden yang merugikan (Mishardila, 2020). Dalam penelitian ini, penerapan *Threat Intelligence Lifecycle* berperan penting untuk memberikan wawasan yang sistematis dan dapat ditindaklanjuti dalam mendeteksi serta menganalisis aktivitas perdagangan data pribadi di *Dark Web*. Model ini terdiri dari enam tahapan utama yang bersifat siklikal dan berkesinambungan, yaitu: *Planning & Direction, Collection, Processing, Analysis, Dissemination,* dan *Feedback.*

Masing-masing tahapan ini dijelaskan sebagai berikut:

1. *Planning & Direction* (Perencanaan dan Arahan)

Tahap pertama ini merupakan fondasi utama dari siklus intelijen ancaman. Perencanaan yang matang dibutuhkan untuk menetapkan kebutuhan informasi, aset yang ingin dilindungi, serta jenis ancaman yang akan dipantau.

Implementasi dalam penelitian:

a. Mengidentifikasi data pribadi yang rawan diperjualbelikan di *Dark Web* seperti email, nomor induk kependudukan (NIK), dan data finansial.
b. Menentukan fokus intelijen terhadap platform dan entitas yang paling banyak terlibat dalam aktivitas ilegal tersebut.
c. Menyusun rencana strategi pengumpulan dan metode analisis data dari sumber *Dark Web*.

2. *Collection* (Pengumpulan Data)

Tahap ini berkaitan dengan pengumpulan informasi dari berbagai sumber intelijen, baik secara manual maupun otomatis. Informasi dikumpulkan dari forum-forum *Dark Web, Threat Intelligence Feeds*, *Data Breach Archives*, dan sumber *OSINT* lainnya.

Implementasi dalam penelitian:

a. Memanfaatkan tools seperti Intelligence X untuk menelusuri data terbuka.
b. Mengakses forum *Dark Web* menggunakan Tor Browser dan alat pemantauan.

3. *Processing* (Pemrosesan Data)

Setelah data dikumpulkan, tahap ini berfungsi untuk mengorganisir, membersihkan, dan menyaring informasi mentah menjadi data yang siap untuk dianalisis.

Implementasi dalam penelitian:

a. Membersihkan data dari noise atau duplikasi agar relevan dengan kebutuhan investigasi.
b. Menstandarisasi format data untuk keperluan klasifikasi (misalnya: tipe data pribadi, frekuensi kemunculan).
c. Melakukan *hash verification* menggunakan SHA-256 untuk menjamin integritas data forensik.

4. *Analysis* (Analisis)

Pada tahap ini, data yang telah diproses dianalisis secara mendalam untuk mengidentifikasi ancaman yang nyata. Proses ini melibatkan interpretasi terhadap pola serangan, entitas yang terlibat, dan dampaknya terhadap sistem atau organisasi. Implementasi dalam penelitian:

a. Menganalisis percakapan, listing, dan struktur forum *Dark Web* untuk mendeteksi pola perdagangan data pribadi.
b. Mengidentifikasi teknik yang digunakan oleh *threat actors* dan IoC *(Indicators of Compromise).*
c. Menggunakan teknik *content analysis* dan *network mapping* untuk menelusuri hubungan antar pelaku.

5. *Dissemination* (Diseminasi Intelijen)

Diseminasi merupakan tahap distribusi hasil analisis intelijen ke pihak yang berkepentingan. Laporan intelijen harus mudah dipahami, relevan, dan tepat waktu. Implementasi dalam penelitian:

a. Menyusun laporan hasil analisis dalam format yang ringkas, analitis, dan dapat digunakan untuk rekomendasi kebijakan keamanan.

b. Membagikan laporan kepada pembimbing akademik serta pihak lain yang relevan dengan kebijakan perlindungan data.

6. *Feedback* (Umpan Balik)

Tahap ini menjadi penutup sekaligus penghubung untuk siklus selanjutnya. Evaluasi dilakukan untuk mengetahui apakah hasil intelijen sebelumnya efektif dalam mendeteksi dan memitigasi ancaman.

Implementasi dalam penelitian:

a. Melakukan refleksi terhadap proses analisis dan hasil investigasi, serta menentukan area yang perlu ditingkatkan.
b. Menyesuaikan kembali strategi pengumpulan dan fokus intelijen berdasarkan temuan sebelumnya dan perubahan ancaman.

3.5. Teknik Pengumpulan Data

Teknik pengumpulan data dalam penelitian ini dilakukan melalui beberapa metode berikut:

1. Observasi Pasif di *Dark Web*
    a. Mengakses forum dan *marketplace* ilegal dengan menggunakan Tor Browser.
    b. Mengamati aktivitas jual beli data pribadi tanpa melakukan interaksi langsung.
2. Analisis Data dari Forum
    a. Menganalisis daftar harga, jenis data yang diperjualbelikan, serta metode pembayaran yang digunakan.

3. Analisis *OSINT* dan *Threat Intelligence*
    a. Menggunakan alat *OSINT* untuk menelusuri jejak digital dari kebocoran data.
    b. Menganalisis laporan *threat intelligence* untuk memahami pola serangan dan aktor ancaman.

3.6. Teknik Analisis Data

Analisis data dilakukan dengan metode content analysis dan statistical analysis:

1. *Content Analysis* (Analisis Konten)
    a. Menganalisis isi percakapan di forum *Dark Web* untuk memahami motif dan pola perdagangan data.
    b. Mengklasifikasikan tipe data pribadi yang diperjualbelikan berdasarkan kategori tertentu.
2. *Statistical Analysis* (Analisis Statistik)
    a. Menghitung jumlah dan tren transaksi perdagangan data pribadi dari berbagai *marketplace* ilegal.
    b. Menggunakan data *visualization* untuk menyajikan pola perdagangan data pribadi dalam bentuk grafik dan tabel.

3.7. Metode Evaluasi dan Perbandingan

Evaluasi dalam penelitian ini dilakukan melalui pendekatan studi komparatif dan pengukuran efektivitas teknik investigasi yang diterapkan. Penilaian difokuskan pada efektivitas metode *Open Source Intelligence (OSINT)* dan *Threat Intelligence* dalam mendeteksi serta menganalisis aktivitas perdagangan data pribadi di *Dark Web*. Evaluasi ini bertujuan untuk mengukur seberapa baik pendekatan dan alat yang digunakan mampu mengungkap pola kebocoran data

secara akurat, relevan, dan tepat waktu. Evaluasi Keefektifan *OSINT* & *Threat Intelligence.*

3.7.1. Evaluasi Keefektifan *OSINT* dan *Threat Intelligence*

Penelitian ini menggunakan sejumlah indikator evaluasi untuk mengukur efektivitas metode investigasi yang digunakan, antara lain:

a. Akurasi Deteksi

   Mengukur seberapa besar data yang ditemukan melalui *OSINT* dan *Threat Intelligence* dapat diverifikasi sebagai data yang benar-benar bocor berdasarkan sumber valid (seperti HaveIBeenPwned dan Intelligence X).

b. Kelengkapan Informasi

   Menilai jumlah dan keberagaman atribut data (misalnya: NIK, nama, email, nomor telepon, instansi, dll) yang tersedia dalam sampel yang ditemukan di forum-forum *Dark Web*.

c. Relevansi Kontekstual

   Menganalisis keterkaitan antara data yang ditemukan dengan kasus kebocoran data yang sudah terjadi, seperti kesesuaian domain email, nama institusi, atau pola waktu kebocoran.

d. Waktu Deteksi

   Mengukur rentang waktu antara tanggal kebocoran data pertama kali diketahui publik (misalnya dari media atau lembaga keamanan siber) dengan waktu peneliti berhasil menemukan data tersebut melalui teknik *OSINT*.

e. Kemudahan Akses & Efisiensi Tools

Menilai pengalaman penggunaan tools dalam hal efisiensi waktu, kemudahan pengoperasian, dan kemampuan dalam mendeteksi informasi valid.

3.7.2. Perbandingan dengan Studi Kasus Sebelumnya

Peneliti juga akan melakukan komparasi dengan beberapa studi kebocoran data yang telah terdokumentasi sebelumnya, guna menilai sejauh mana temuan dalam penelitian ini memiliki kesamaan atau perbedaan, baik dari sisi jenis data yang bocor, struktur forum perdagangan, hingga taktik threat actor.

Sumber-sumber pembanding meliputi:

a. Penelitian akademik sebelumnya yang mengulas kebocoran data di Indonesia maupun internasional
b. Repository publik kebocoran data seperti HaveIBeenPwned dan Intelligence X

3.8. Kerangka Waktu Penelitian

Tabel 3.3 Waktu Penelitian

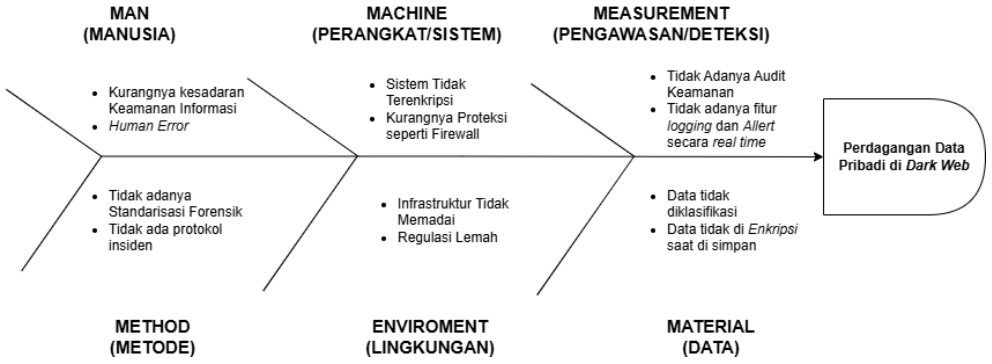
No	Uraian Kegiatan	Maret				April				Mei				Juni				Juli			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1.	Tahap Persiapan Penelitian	■	■	■																	
2.	Tahap Penyusunan Proposal				■	■	■	■	■												
3.	Seminar Proposal									■											
3.	Tahap Pelaksanaan Penelitian										■	■	■	■	■						

4.	Tahap Penyusunan Laporan dan Revisi																					
5.	Ujian Skripsi																					

3.9. Fishbone Diagram

Untuk mengidentifikasi faktor-faktor penyebab terjadinya kebocoran data pribadi yang berujung pada perdagangan data di *dark web*, peneliti menggunakan pendekatan *Fishbone Diagram* atau dikenal juga sebagai *Cause-and-Effect Diagram*. Model ini efektif untuk melakukan identifikasi akar permasalahan (*root cause analysis*) secara sistematis, terutama dalam kasus yang kompleks dan melibatkan berbagai dimensi risiko seperti insiden kebocoran data.

Fishbone diagram pada penelitian ini mengadopsi pendekatan *5M+1E* yang terdiri dari lima kategori utama: *Man* (Manusia), *Machine* (Perangkat/Sistem), *Method* (Metode), *Measurement* (Pengawasan dan Deteksi), *Material (Data)*, serta *Environment* (Lingkungan). Setiap kategori memetakan penyebab potensial yang berkontribusi terhadap kebocoran data dan perdagangannya di *dark web* (Alshaikh, 2020).



Gambar 3.3 Fishbone Diagram

a. *Man* (Manusia): Rendahnya kesadaran terhadap pentingnya keamanan informasi, kesalahan individu dalam mengelola data pribadi, serta minimnya edukasi publik terkait perlindungan data menjadi penyebab signifikan.
b. *Machine* (Perangkat/Sistem): Kelemahan teknis seperti kesalahan konfigurasi, tidak adanya sistem proteksi seperti *firewall* dan *Intrusion Detection System (IDS)*, serta penggunaan perangkat lunak usang membuka celah terhadap serangan.
c. *Method* (Metode): Tidak diterapkannya standar seperti enkripsi data atau protokol tanggap insiden dan forensik digital mengakibatkan lemahnya perlindungan data.
d. *Measurement* (Pengawasan dan Deteksi): Kurangnya *real-time monitoring*, belum digunakannya *Threat Intelligence Platform (TIP)*, serta ketiadaan sistem audit menyebabkan lambatnya deteksi kebocoran.
e. *Material* (Data): Data sensitif (NIK, alamat, nomor HP, dsb.) diperlakukan sama seperti data biasa dan Data pribadi disimpan dalam bentuk plaintext, sangat mudah dicuri.
f. *Environment* (Lingkungan): Infrastruktur keamanan yang belum memadai, lemahnya regulasi perlindungan data, dan tingginya aktivitas *underground forum* menjadi katalisator yang memperbesar risiko kebocoran data.

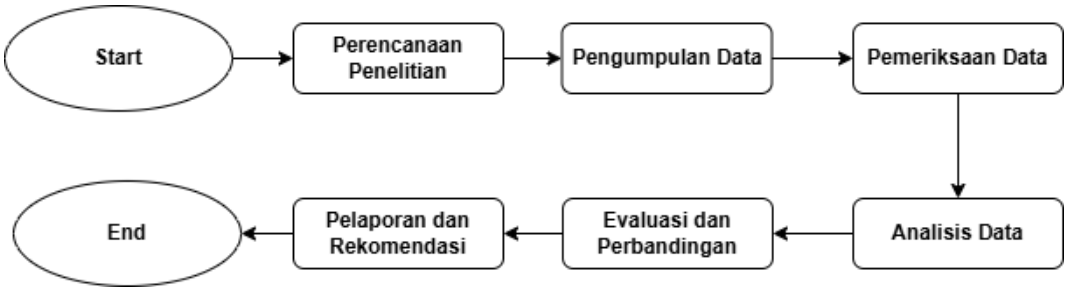
Penggunaan *Fishbone Diagram* dalam penelitian ini didasarkan pada tujuan untuk:

a. Mengidentifikasi akar penyebab kebocoran data pribadi secara sistematis dan menyeluruh;
b. Menyusun strategi forensik dan mitigasi yang tepat berdasarkan analisis akar masalah;
c. Menjadi landasan logis dalam penyusunan alur investigasi berbasis *Open Source Intelligence (OSINT)* dan *Threat Intelligence*.

Fishbone diagram telah terbukti sebagai alat yang efektif dalam menganalisis akar masalah dalam sistem keamanan informasi, karena dapat memberikan visualisasi yang jelas terhadap berbagai sumber penyebab insiden yang bersifat kompleks dan multidimensi (Ring et al., 2021).

3.10. Visualisasi Alur Penelitian

Untuk memperjelas tahapan-tahapan dalam proses penelitian ini, berikut disajikan *flowchart* yang menggambarkan alur kerja mulai dari perencanaan hingga pelaporan. Visualisasi ini mengintegrasikan langkah-langkah *OSINT*, *Threat Intelligence*, dan digital forensik berdasarkan framework NIST SP 800-86 serta *Threat Intelligence Lifecycle*.



Gambar 3.4 *Flowchart* Penelitian

Berikut merupakan penjelasan dari *Flowchart* penelitian skripsi mulai dari *Start* sampai dengan *End*.

1. Mulai

Penelitian dimulai dengan identifikasi masalah, penyusunan rumusan masalah, serta perumusan tujuan dan batasan penelitian.

2. Perencanaan Penelitian

Menentukan studi kasus yang digunakan, merancang pendekatan metode, memilih tools investigasi, serta menyiapkan lingkungan forensik.

3. Pengumpulan Data

Pengumpulan data dilakukan melalui observasi pasif di forum *Dark Web* dan pencarian data bocor menggunakan *tools OSINT*. Hanya sampel publik yang digunakan.

4. Pemeriksaan Data

Data sampel yang diperoleh diperiksa dari sisi struktur, kelengkapan atribut, serta dilakukan proses hashing dan pembersihan terhadap data duplikat atau tidak relevan.

5. Analisis Data

Tahap ini mencakup analisis pola perdagangan data, *profiling threat actor*, serta validasi data menggunakan *Threat Intelligence tools* seperti VirusTotal. Teknik kuantitatif seperti statistik deskriptif juga diterapkan untuk mengukur volume data dan tren peredarannya.

6. Evaluasi dan Perbandingan

Evaluasi dilakukan terhadap efektivitas pendekatan *OSINT* dan TI berdasarkan indikator akurasi, kelengkapan, dan relevansi. Hasil data juga dibandingkan dengan data makro untuk validasi struktur.

7. Pelaporan dan Rekomendasi

Hasil investigasi didokumentasikan dalam laporan forensik, dilengkapi dengan visualisasi dan saran mitigasi keamanan siber bagi instansi terkait.

8. Selesai

Tahapan akhir menandakan selesainya proses investigasi dan penyusunan dokumen skripsi.

BAB IV

HASIL DAN PEMBAHASAN

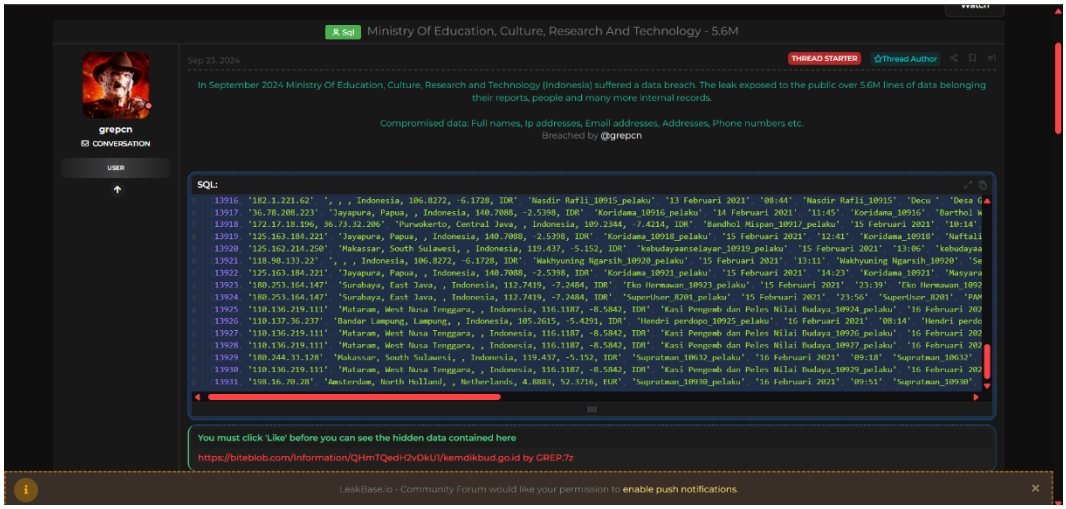
4.1. Deskripsi Kasus

Penelitian ini didasarkan pada data yang diperoleh dari dua forum, yakni *LeakBase* dan *DarkForums*. Sumber utama berasal dari akun dengan nama samaran "@grepcn" yang mempublikasikan unggahan berisi *preview file* yang diklaim sebagai hasil kompromi data dari sistem internal milik Kementerian Pendidikan dan Kebudayaan, Riset, dan Teknologi. Data tersebut mencakup informasi pribadi seperti nama lengkap, alamat email, alamat instansi, nomor ponsel, *IP address*, dan identitas organisasi asal.

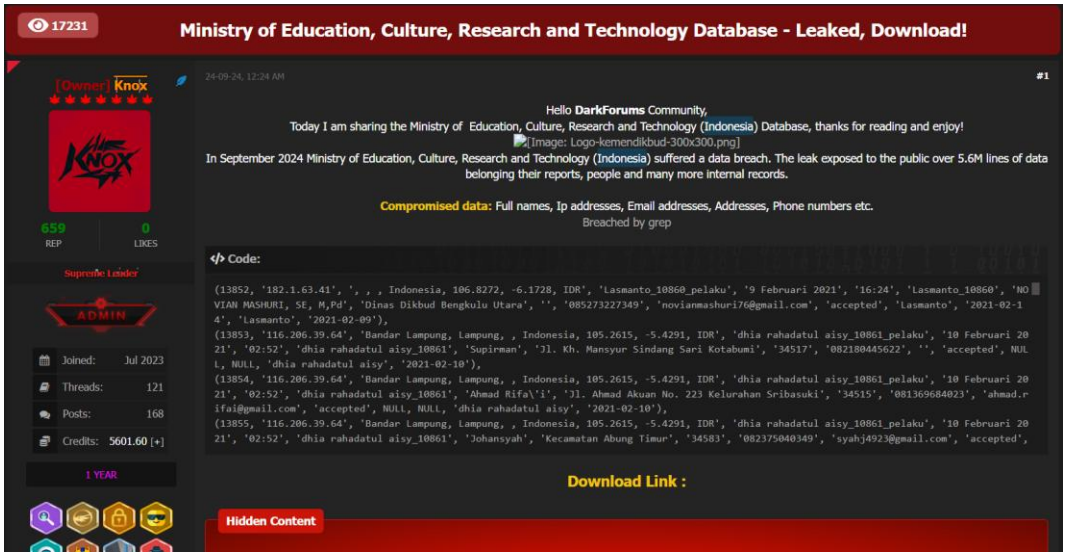
Keberadaan data tersebut tidak hanya terbatas pada satu forum, tetapi juga ditemukan kembali di forum lain seperti *DarkForums*, yang mengindikasikan bahwa data tersebut telah tersebar luas dan kemungkinan besar merupakan bagian dari *dump* asli. Konsistensi struktur data di kedua forum dan kemunculannya di kanal distribusi yang berbeda menunjukkan tingkat kredibilitas yang tinggi.

Berikut merupakan hasil capture dari kedua forum tersebut yaitu *Leakbase* dan *DarkForums.* Terlihat bahwa sumber utama yaitu “grepcn” mengunggah file preview data pribadi milik Kemendikbudristek yang diduga bocor pada September 2024 yang disebarluaskan di *Leakbase*. Lalu file yang sama disebarkan lagi oleh di forum lain yaitu *DarkForums* yang disebarkan oleh “Knox” yang dimana adalah admin dari forum tersebut. Terlihat bahwa sumber file itu bersumber dari “grepcn”

yang dimana yaitu diduga oleh peneliti sebagai pelaku utama dalam insiden kebocoran data pribadi tersebut.



Gambar 4.1 Gambar Forum Penjualan *LeakBase* oleh grepcn



Gambar 4.2 Gambar Forum Penjualan *DarkForums* oleh Knox

Karakteristik Umum Data Kebocoran Data yang dianalisis dalam penelitian ini mencakup kombinasi informasi pribadi dan metadata institusional yang terdapat pada kedua forum tersebut yang dimana sebagai data sampel. Elemen data utama meliputi:

a. Nama lengkap individu
b. Alamat email
c. IP address
d. Instansi atau lembaga asal
e. Nomor telepon
f. Tanggal entri data

Karakteristik ini menunjukkan bahwa data kemungkinan besar berasal dari sistem internal yang digunakan secara nasional dalam lingkup Kementerian Pendidikan dan Kebudayaan. Hal ini memberikan alasan kuat untuk menduga bahwa kebocoran terjadi akibat kelemahan dalam pengamanan sistem informasi milik kementerian tersebut.

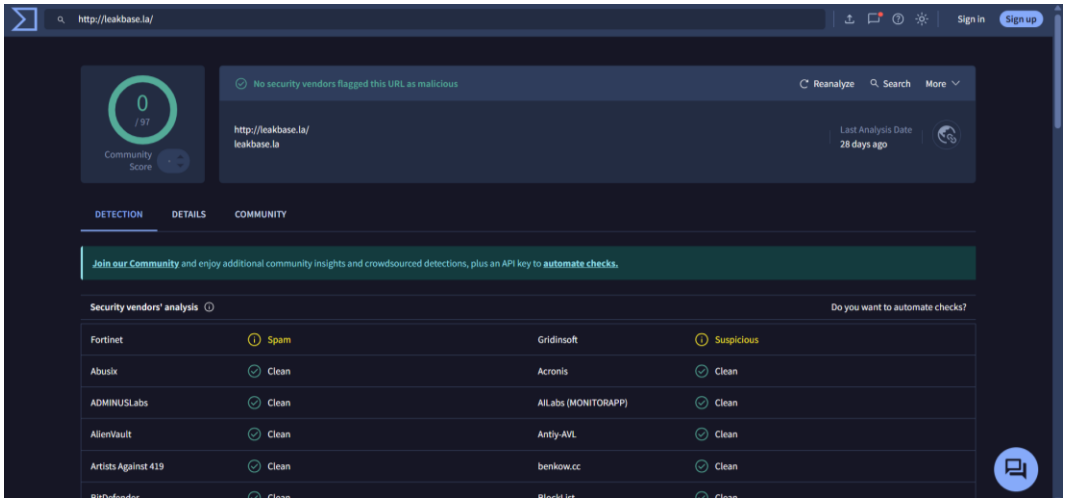
4.2. Proses Akuisisi Data (*Collection*)

Tahapan pertama dalam proses investigasi forensik digital adalah pengumpulan data atau *collection*. Pada penelitian ini, data dikumpulkan secara pasif dari dua sumber utama, yaitu forum *LeakBase* dan *DarkForums*. Data diperoleh dalam bentuk *preview* berbasis teks yang ditampilkan langsung di thread unggahan pelaku yang menggunakan nama akun seperti "@grepcn" dan "@Knox".

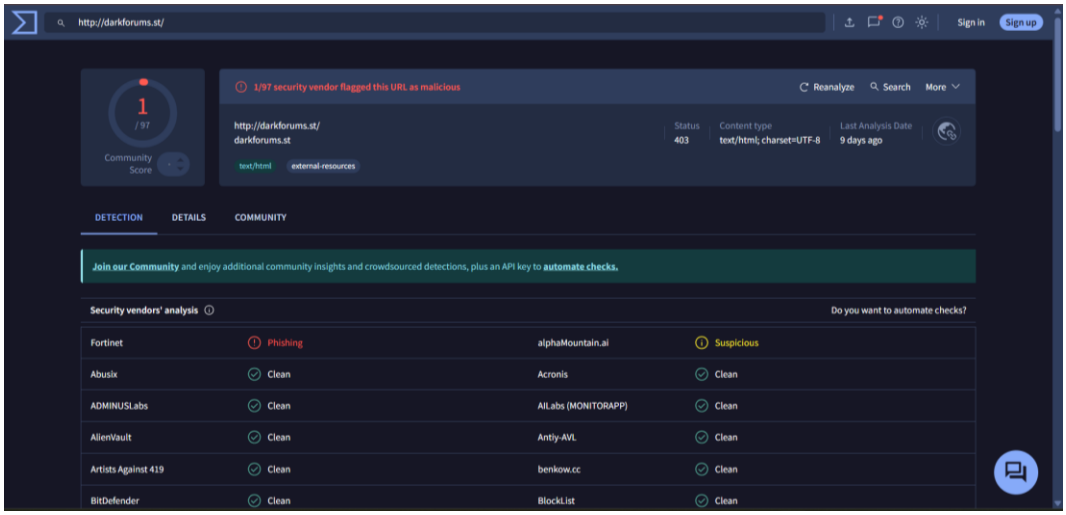
Akses dilakukan melalui browser Tor untuk menjamin kerahasiaan identitas dan integritas proses pengumpulan data. Tidak ada transaksi atau komunikasi langsung yang dilakukan dengan pelaku, melainkan hanya pengunduhan file yang telah tersedia secara publik atau *preview* yang dibagikan secara terbuka oleh pelaku. Proses ini dilakukan sesuai dengan prinsip etika penelitian digital dan bertujuan untuk menjaga legalitas serta objektivitas investigasi.

Berikut merupakan proses akuisisi data (*Collection*) dari kedua forum yang melakukan penjualan data tersebut :

a. Sebelum mengakses forum tersebut peneliti melakukan cek keamanan kedua forum tersebut terlebih dahulu untuk memastikan keamanan data peneliti dikarenakan forum ini sangat rawan untuk diakses dijaringan bebas. Berikut merupakan hasil pengecekan forum leakbase.la dan darkforums.st menggunakan tools VirusTotal.



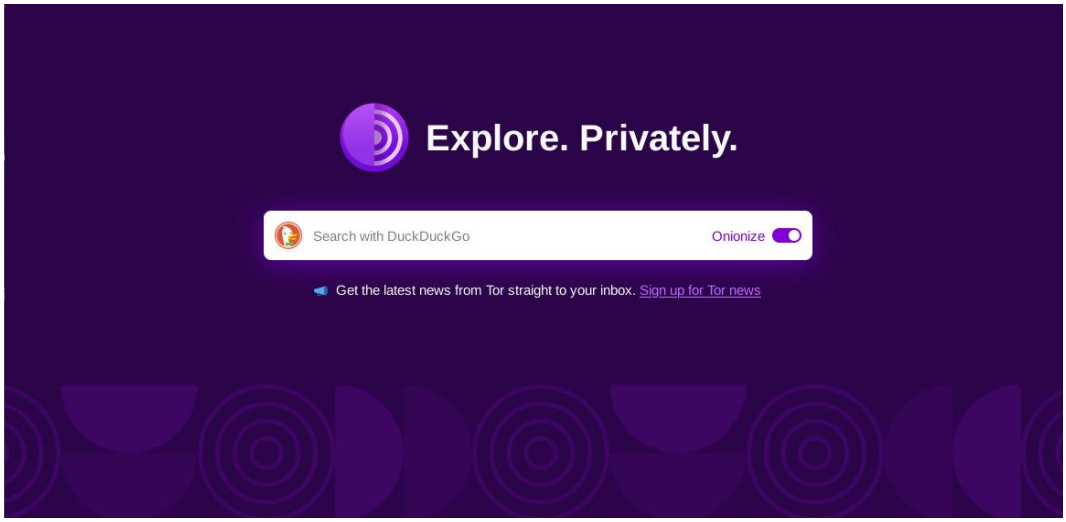
Gambar 4. 3 Hasil Pengecekan forum Leakbase.la menggunakan VirusTotal



Gambar 4. 4 Hasil Pengecekan forum DarkForums.st menggunakan VirusTotal

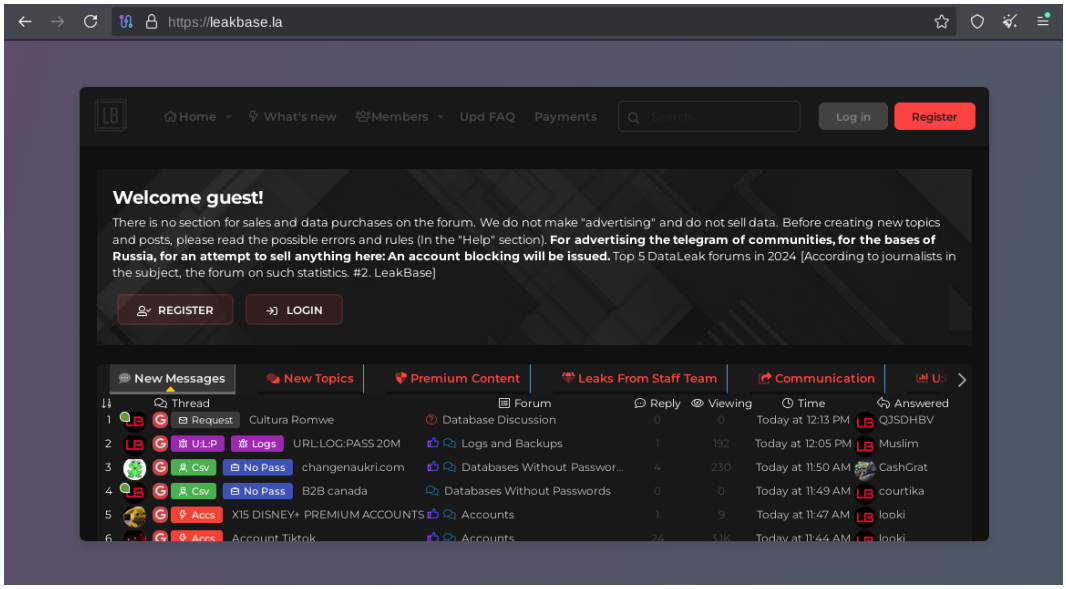
Dari hasil pengecekkan menunjukkan bahwa kedua forum tersebut terdapat laporan sebagai "*Suspicious*" yang dimana forum *Leakbase* terdeteksi sebagai "spam" dan forum *Darkforums* terdeteksi mengandung "*Phising*".

b. Peneliti masuk menggunakan jaringan tor untuk menjaga identitas agar tetap anonim dalam melakukan penelitian. Hal ini dilakukan karena terdeteksi adanya "*Suspicious*" dengan *tools* VirusTotal.

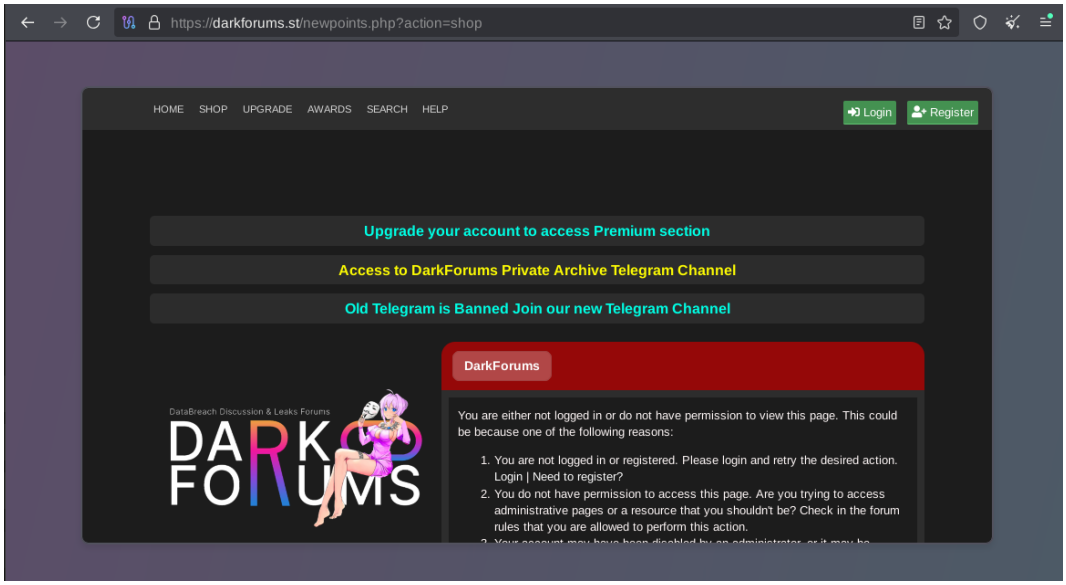


Gambar 4. 5 Gambar Tor Browser

c. Setelah itu saya mengakses forum leakbase.la dan darkforums.st dengan tor browser untuk menjaga agar tetap *anonim*.



Gambar 4. 6 Tampilan Forum Leakbase.la



Gambar 4. 7 Gambar Forum DarkForums.st

d. Setelah melakukan penelitian dari kedua forum tersebut didapatkanlah kasus kebocoran data pribadi yang menjadi pemfokusan penelitian ini seperti yang tertera pada Gambar 4.1 dan Gambar 4.2.

4.3. Pemeriksaan Struktur Data (*Examination*)

Tahapan ini bertujuan untuk melakukan inspeksi awal terhadap struktur dan integritas data yang telah diperoleh. Pemeriksaan dilakukan dengan membuka file hasil akuisisi data dari forum *Leakbase* dan *DarkForums* dan mengekstrak kolom-kolom utama seperti nama, email, IP address, dan instansi. Berikut merupakan proses *examination data* sebagai validasi dan memudahkan dalam proses penelitian selanjutnya. Dalam konteks penelitian ini, penulis memperoleh data mentah dalam bentuk teks semi-terstruktur yang merepresentasikan hasil kebocoran data dari forum.

Data tersebut kemudian melalui proses *parsing* menggunakan bahasa pemrograman Python. *Parsing* ini bertujuan untuk mengonversi format teks mentah menjadi struktur data yang terorganisasi (dalam hal ini tabel data), sehingga dapat dianalisis lebih lanjut pada tahap berikutnya.

```
import cs v
import io
import pandas as pd


raw_data = """
(Data Mentah dari Proses Acquisisi Data di Forum Leakbase dan DarkForum)
"""


# === Preprocessing ===
lines = raw_data.strip().split('\n')
clean_lines = [line.strip()[1:-1] for line in lines if line.strip().startswith('(')]
```

```
csv_data = "\n".join(clean_lines)


# === Parsing CSV-style ===
reader = csv.reader(io.StringIO(csv_data), quotechar='"', skipinitialspace=True)
data = list(reader)


# === Kolom  ===
columns = [
    "ID", "IP", "Lokasi", "Akun", "Tanggal", "Waktu", "Username",
    "Nama", "Alamat/Instansi", "Kode Pos", "No HP", "Email", "Status",
    "Validator", "Tanggal Validasi", "Operator", "Tanggal Input"
]
# === Buat DataFrame dan simpan ===
df = pd.DataFrame(data, columns=columns)


# Simpan ke file
df.to_csv("hasil_data.csv", index=False)
df.to_excel("hasil_data.xlsx", index=False)


print("Data berhasil diparsing dan disimpan ke 'hasil_data.csv' dan
'hasil_data.xlsx'")
print(df.head())
```

Validasi dilakukan untuk memisahkan data yang valid dengan data yang tidak relevan, seperti *placeholder*, *field* kosong, atau data *dummy*. Data yang lolos tahap pemeriksaan ini akan diproses lebih lanjut dalam tahap analisis. Alat bantu seperti spreadsheet editor, script Python (pandas), dan visualisasi tabel digunakan dalam tahap ini untuk menyusun dan memfilter data.

Hasil ataupun output dari kode program python tersebut berbentuk file .csv dan xlxs. Berikut merupakan *preview* dari hasil *examination* dari data sampel tersebut

Nama	Alamat/Instansi	Kode Pos	No HP	Email	Status
NOVIAN MASHURI, SE, M,Pd	Dinas Dikbud Bengkulu Utara		085273227349	novianmashuri76@gmail.com	accepted
Supirman	Jl. Kh. Mansyur Sindang Sari Kotabumi	34517	082180445622		accepted
Ahmad Rifai'	Jl. Ahmad Akuan No. 223 Kelurahan Sribasuki	34515	081369684023	ahmad.rifai@gmail.com	accepted
Johansyah	Kecamatan Abung Timur	34583	082375040349	syahj4923@gmail.com	accepted
SYAHRI SUTAN TURUNAN MIGO	Desa Bumi Agung Kec. Abung Timur â€" Kab. Lampung Utara	34583	085383002876	syahri.kobum@gmail.com	accepted
Syahri Sutan Turunan Migo	Jl. Kapten Slifian Yasin Bumi Agung kec. Abung Timur	34583	085383002876	syahri.kobum@gmail.com	accepted
Johansyah	Jl. Raya Abung Timur No. 97, Kampong Bawang, Melayu	34583	082375040349	syahj4923@gmail.com	accepted
Nani Rahayu	Jl. Asri Gg. Asri No.139 Tanjung Aman Kotabumi Selatan	34511	08127913420	nanirahayutari@yahoo.com	accepted
Saiful Darmawan	Jl. Raya Kota Alam Kotabumi	34519	082182913969		accepted
SYAHRI SUTAN TURUNAN MIGO	Desa Bumi Agung Kec. Abung Timur â€" Kab. Lampung Utara	34583	085383002876	syahri.kobum@gmail.com	accepted
SYAHRI SUTAN TURUNAN MIGO	Desa Bumi Agung Kec. Abung Timur â€" Kab. Lampung Utara	34583	085383002876	syahri.kobum@gmail.com	accepted
Dekeng Sembiring	Kabanjahe Gg Bakti	22113	085261155704	a	accepted
Simpei Sinulingga	Desa Lingga	22150	081376319931	a	accepted
Emanuel	Mencimai Kec. Barong Tongkok	75576	085245009471	nuelema753@gmail.com	accepted
Dekeng Sembiring	Kabanjahe Gg Bakti	22113	085261155704	a	accepted
Dekeng Sembiring	Kabanjahe Gg Bakti	22113	085261155704	a	accepted
Emanuel	Mencimai Kec. Barong Tongkok	75576	085245009471	nuelema753@gmail.com	accepted
Dekeng Sembiring	Kabanjahe Gg Bakti	22113	085261155704	a	accepted
Emanuel	Mencimai Kec. Barong Tongkok	75576	085245009471	nuelema753@gmail.com	accepted
Emanuel	Mencimai Kec. Barong Tongkok	75576	085245009471	nuelema753@gmail.com	accepted
Emanuel	Mencimai Kec. Barong Tongkok	75576	085245009471	nuelema753@gmail.com	accepted
Emanuel	Mencimai Kec. Barong Tongkok	75576	085245009471	nuelema753@gmail.com	accepted
KAMARULLAH	Desa Allakuang Kabupaten Sidenreng Rappang	91611	082335555780	-	accepted
SYAHRI SUTAN TURUNAN MIGO	Desa Bumi Agung Kec. Abung Timur â€" Kab. Lampung Utara	34583	085383002876	syahri.kobum@gmail.com	accepted
Masri	Jl. Lintas Bengkulu, Pekon Way Nukak, Kecamatan Karya Penggawa Kabupaten Pesisir Barat.	34878	085267447683		accepted
Siti Zairoh	Jl. Lintas Barat, Pekon Sukajadi, Kecamatan Krui Selatan, Kabupaten Pesisir Barat	34874	081272460490		accepted

Gambar 4. 8 Hasil *Examination* data sampel menggunakan Python

Dari hasil *examination* data sampel yang telah dilakukan terdapat total 80 data pribadi yang bocor disampel tersebut diantaranya meliputi

Tabel 4. 1 Tabel Total Data keseluruhan

No	Item	Jumlah
1.	Total seluruh data sampel	80
2.	Jumlah Email Valid	17
3.	Jumlah IP Valid	34
4.	Jumlah nama valid	65

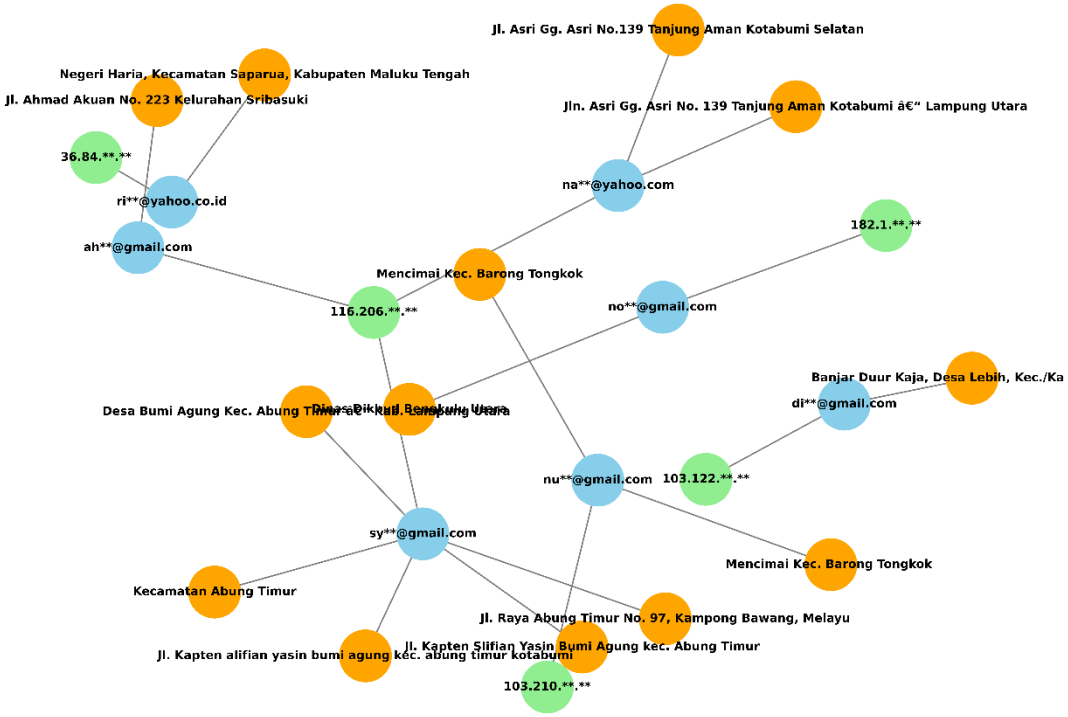
Berdasarkan Tabel 4.1, terdapat sebanyak 80 data sampel yang dianalisis. Dari jumlah tersebut, sebanyak 17 data teridentifikasi memiliki alamat email valid, 34 data memiliki IP address valid, serta 65 data mengandung nama valid. Validitas data tersebut ditentukan berdasarkan kriteria tertentu, seperti format penulisan yang sesuai standar dan keterbacaan informasi. Hal ini menunjukkan bahwa sebagian besar data mengandung nama yang dapat dikenali, sedangkan email valid masih tergolong sedikit dikarenakan banyak entry data email yang kosong pada data sampel yang ditemukan.

4.4. Analisis Hasil Temuan (*Analysis*)

Setelah data dibersihkan, tahap selanjutnya adalah analisis mendalam untuk menemukan keterkaitan antar entitas serta pola distribusi data. Dalam penelitian ini, pendekatan yang digunakan adalah analisis graf (*graph analysis*) menggunakan NetworkX, lalu ada profiling actor dan analisis pola distribusi dan penjualan data tersebut.

4.4.1 Analisis Relasi Entitas (*Entity Graph Analysis*)

Entitas seperti *IP address*, alamat email, dan instansi ditampilkan sebagai node, sementara keterhubungan antar elemen dianalisis berdasarkan relasi yang terekam dalam dump. Hasil analisis menunjukkan adanya beberapa node pusat (*central nodes*) seperti *IP address* yang muncul pada lebih dari satu entri atau alamat email yang digunakan oleh lebih dari satu individu.



Gambar 4. 9 Visualisasi Relasi dari 20 Data Sampel

Untuk menjaga privasi individu, seluruh email dan alamat IP dalam visualisasi telah disamarkan sebagian (misalnya ab**@gmail.com, 123.45.**.**). Visualisasi ini membantu peneliti memetakan relasi antar korban dan mengidentifikasi simpul yang berperan penting dalam jaringan penyebaran data. Hasil dari analisis visualisasi dengan networkx memperlihatkan beberapa temuan penting:

a. Terdapat beberapa alamat IP yang digunakan oleh lebih dari satu email, misalnya 18.206.**.**. Hal ini mengindikasikan bahwa para korban kemungkinan besar mengakses sistem dari jaringan yang sama, seperti lingkungan sekolah atau kantor, yang menggunakan koneksi publik atau *shared network.*

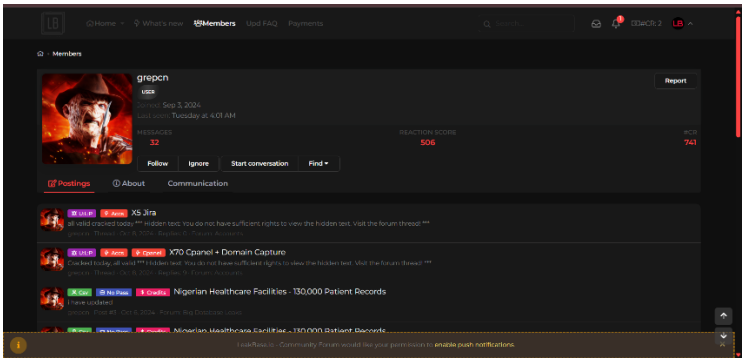
b. Email yang bocor seluruhnya menggunakan domain umum seperti @gmail.com, Namun, dari keterkaitan dengan entitas lokasi seperti alamat jalan, desa, atau kecamatan, dapat diasumsikan bahwa sebagian korban berasal dari lingkungan masyarakat umum, termasuk wilayah administratif seperti Kecamatan Abung Timur, Banjar Duur Kaja, dan Desa Bumi Agung.
c. Beberapa email terhubung ke lebih dari satu instansi, yang dapat menjadi indikasi bahwa akun tersebut memiliki akses lintas lembaga atau memiliki peran administratif yang luas.

Visualisasi graf ini secara langsung mendukung tahap *Analysis* dengan memberikan gambaran menyeluruh mengenai hubungan antar entitas, node pusat (*central nodes*), dan potensi jalur distribusi data. Dengan adanya node-node yang memiliki koneksi lebih dari satu arah, peneliti dapat mengidentifikasi sumber data dominan, pola hubungan antar korban, serta pola penggunaan alamat IP yang berulang.

4.4.2. Profiling Pelaku (*Actor Profiling*)

Berdasarkan investigasi pada forum *LeakBase*, ditemukan akun bernama “grepcn” yang memiliki aktivitas aktif dalam mendistribusikan data hasil kebocoran, termasuk database Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi (Kemdikbudristek) 2024. Berikut untuk hasil data lengkapnya :

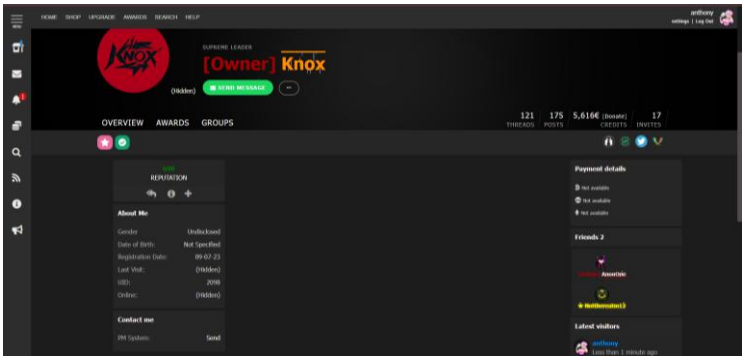
Tabel 4. 2 Profil Pelaku Utama

Gambar	
Forum	Leakbase.la
Username	grepcn
Level	*user*
Tanggal bergabung	3 September 2024
Total Post	32
Reaction Score	506
Followers	8 *User*
Following	1 *User* yaitu Chuky *(Owner LeakBase*)

Pada tabel 4.2 dijelaskan bahwa akun yang bernama “grepcn” terduga menjadi aktor utama pada kebocoran data Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi (Kemendikbud). Akun ini memublikasikan *dump* dengan deskripsi teknis terperinci, termasuk metadata geografis, nama lengkap, alamat email, *IP address*, nomor telepon, dan timestamp aktivitas. Gaya penulisan yang digunakan bersifat teknikal dan sistematis, menunjukkan bahwa pelaku memiliki

kemampuan teknis dalam melakukan data *extraction* dan *SQL formatting*. Terlihat pada postingan kebocoran data Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi (Kemendikbud) dan beberapa postingan lainnya yang menggunakan format data yang diunggah dalam bentuk *sql dump*.

Tabel 4. 3 Profil "Knox"

Gambar	
Forum	DarkForums.st
Username	knox
Level	Owner
Tanggal bergabung	9 Juli 2023
Total Post	168
Threat	121
Reputasi	659

Pada tabel 4.3 dijelaskan bahwa akun dengan *username* "Knox" diduga sebagai *owner* dari forum DarkForums. Knox adalah aktor yang melakukan *re-upl oad* di *platform* lain, kemungkinan dengan tujuan monetisasi ulang. Data yang

sama kemudian didistribusikan ulang oleh akun lain bernama Knox di forum *DarkForum*s, lengkap dengan tampilan sampel SQL yang berisikan data pribadi korban.

Berdasarkan temuan tersebut dapat disimpulkan bahwa :

a. Grepcn bertindak sebagai penyedia utama data (*original leaker*).
b. Knox adalah aktor yang melakukan *re-upload* di *platform* lain, kemungkinan dengan tujuan monetisasi ulang.

4.4.3. Analisis Pola Distribusi dan Penjualan

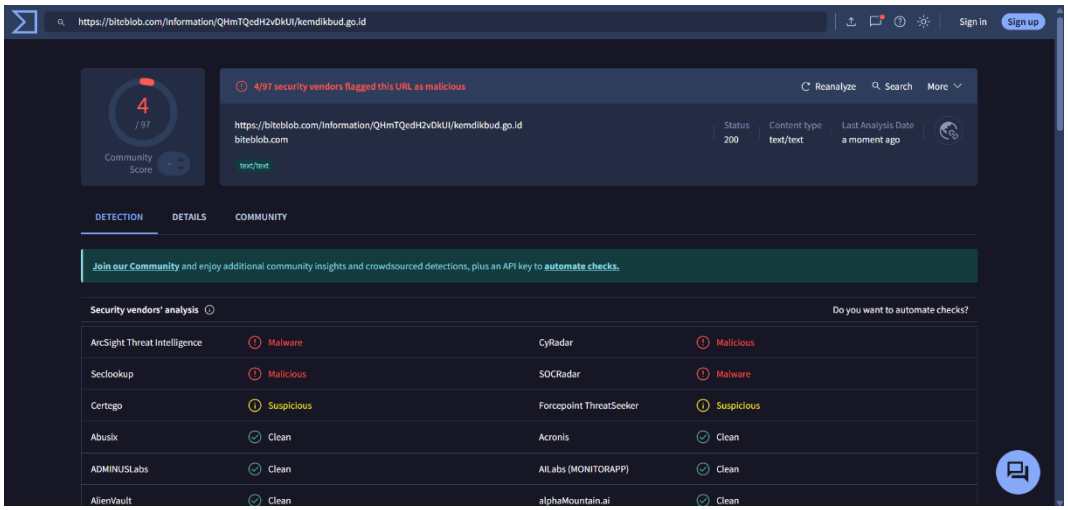
Pola perdagangan data yang ditemukan memiliki struktur dan strategi pemasaran yang menyerupai sistem *e-commerce* gelap. Berdasarkan observasi terhadap tiga aktor di atas, pola distribusi dapat diringkas sebagai berikut:

Tabel 4. 4 Model Distribusi

No	Tahap	Aktor	Peran
1.	*Leaker*	grepcn	Upload data kebocoran dengan data sampel.
2.	*Reuploader*	knox	Menyebarkan ulang ke forum lain dengan monetisasi langsung

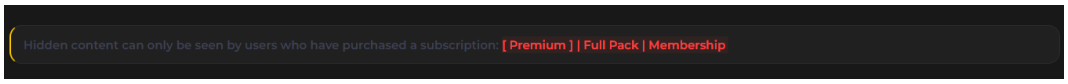
Sosok utama dalam penyebaran data ini adalah akun bernama grepcn, yang pertama kali membagikan dump data dalam *thread* di forum *LeakBase*. Menariknya, grepcn tidak langsung menjual data tersebut. Ia justru membagikannya secara terbuka, lengkap dengan file .7z yang diunggah ke situs pihak ketiga: biteblob.com seperti yang tertera pada gambar 4.1 sebagai temuan utama.

Tidak sampai disitu, penulis juga melakukan investigasi dan mencoba menganalisis situs tersebut bukan dari mengaksesnya langsung tetapi mengecek kredibilitas *link* tersebut dengan *tools* virustotal



Gambar 4. 10 Hasil Pendeteksian menggunakan virustotal

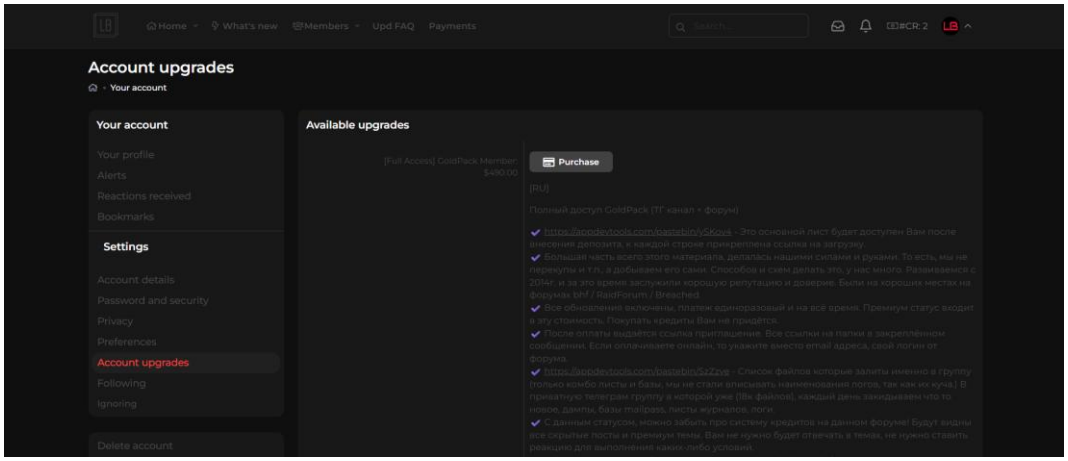
Hasil analisis dari virustotal menunjukkan ada total 4 vendor yang menandai sebagai berbahaya diantaranya yaitu *ArcSight Threat Intelligence* menandai sebagai *Malware*, Seclookup menandai sebaga *Malicious*, CyRadar menandai sebagai *Malicious*, SOCRadar menandai sebagai *malware*. Ini menandai bahwa situs tersebut tidak aman untuk diakses secara langsung dikarenakan mengandung malware yang cukup berbahaya untuk diakses.



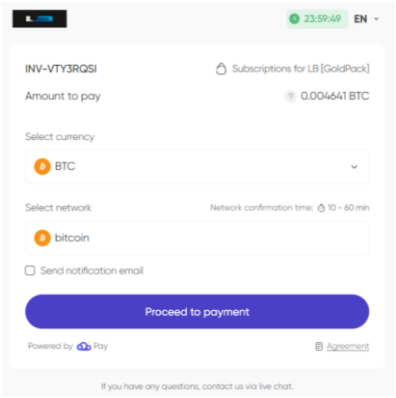
Gambar 4. 11 *Hidden Content Leakbase*

Setelah analisis mendalam, pada forum *Leakbase* juga terlihat bahwa ada beberapa unggahan dengan "*Hidden Content"* yang mengharuskan pengguna melakukan *upgrade subscription* membership. Untuk mendapatkan akses ke "*Hidden Content" user* harus membayar subcription yang beragam harga

membershipnya. Untuk metode pembayaran menggunakan *cryptocurrency* seperti Bitcoin dan yang lainnya seperti pada gambar dibawah ini.

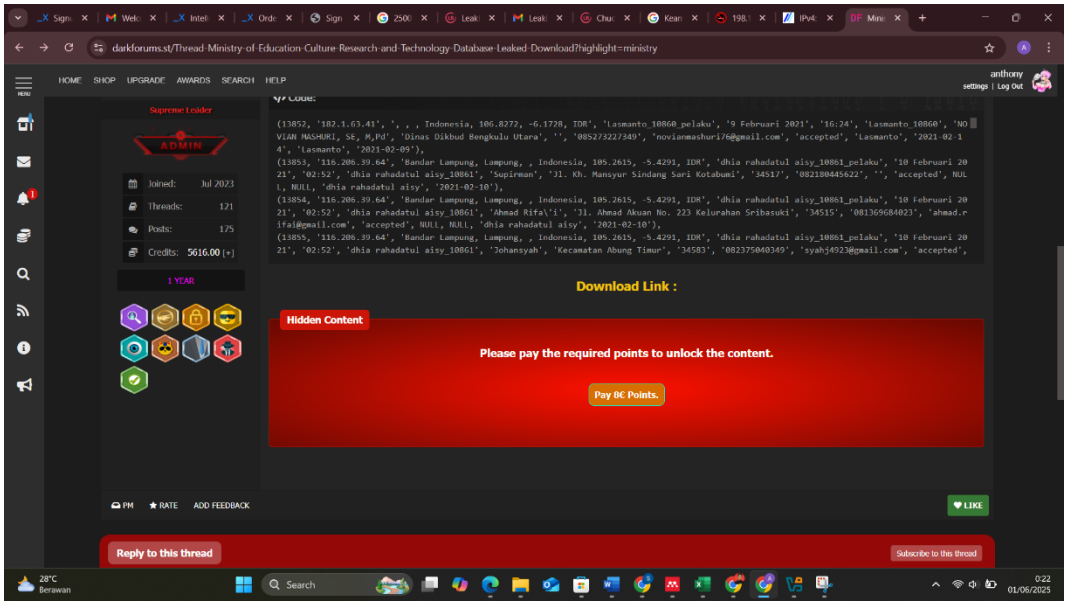


Gambar 4. 12 *Upgrade* akun *membership* di *Leakbase*



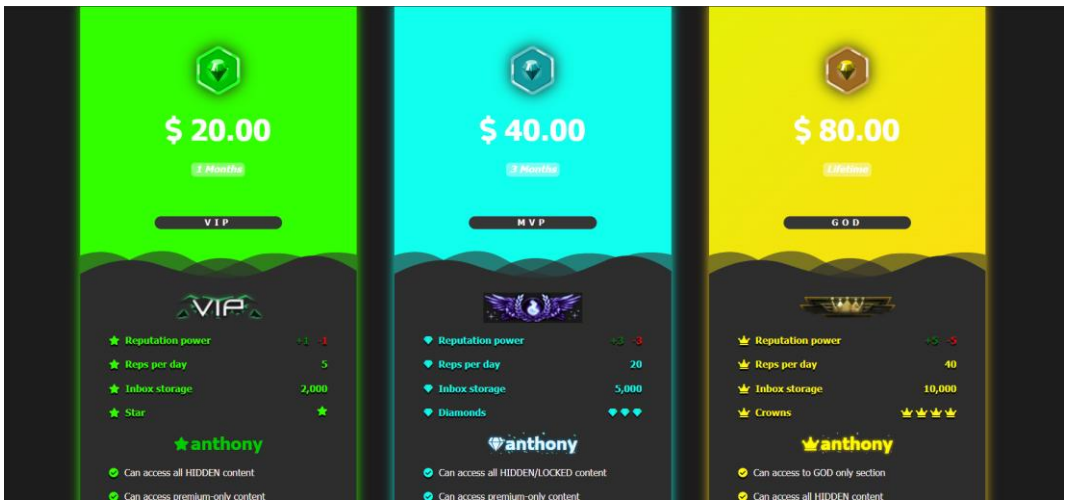
Gambar 4. 13 Metode Pembayaran

Setelah data kebocoran Kemdikbud 2024 pertama kali diunggah oleh akun grepcn di forum *LeakBase*, muncul kembali distribusi ulang dari file yang sama di platform berbeda, yakni *DarkForums*, oleh akun bernama Knox. Aksi reupload ini menunjukkan adanya rantai distribusi lintas-forum, yang sering terjadi dalam ekosistem perdagangan data pribadi.



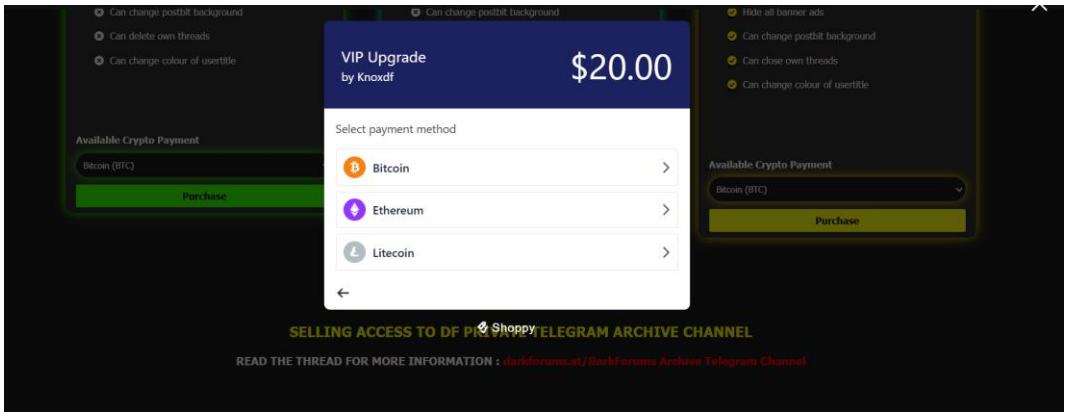
Gambar 4. 14 Pola perdagangan oleh Knox

Terlihat pada gambar 4.10 berbeda dari grepcn yang langsung memberikan akses melalui *link* biteblob.com, Knox menyematkan file unduhan di balik sistem "*Hidden Content*" yang hanya bisa dibuka setelah melakukan pembayaran (dibanderol seharga €9). *Link* langsung disembunyikan, tidak tersedia untuk *user* publik atau tidak terverifikasi.



Gambar 4. 15 *Upgrade* layanan di DarkForums

Untuk mendapatkan akses ke *hidden content* tersebut, pengguna harus mengupgrade layanan di *DarkForums* yang dimana ada 3 jenis layanan yaitu “VIP, MVP dan GOD” dengan masing masing harga yang ditawarkan. Untuk metode pembayaran menggunakan *cryptocurrency* yang dimana ada Bitcoin, Etherium, dan Litecoin yang dapat dilihat pada gambar 4.11 dibawah ini.



Gambar 4. 16 Metode pembayaran DarkForums

4.5. Validasi data sampel menggunakan *OSINT Tools*

Setelah melakukan analisis terhadap struktur data dan pola distribusi yang ditemukan dalam *dump* kebocoran, langkah selanjutnya adalah melakukan validasi terhadap data sampel seperti alamat email menggunakan *tools OSINT*. Validasi ini bertujuan untuk mengonfirmasi apakah email yang ditemukan benar-benar terlibat dalam insiden kebocoran sebelumnya dan apakah terdapat bukti pendukung dari platform pihak ketiga yang memiliki indeks kebocoran data.

Dua *tools* berbasis *OSINT* yang digunakan dalam tahap ini adalah:

- *Have I Been Pwned (HIBP)*, yang menyediakan informasi mengenai data-data yang pernah terlibat dalam insiden breach global secara publik.
- *IntelX*, sebuah mesin pencari intelijen sumber terbuka yang mencakup indeks pastebin, dump *dark web*, dan forum-forum kebocoran data.

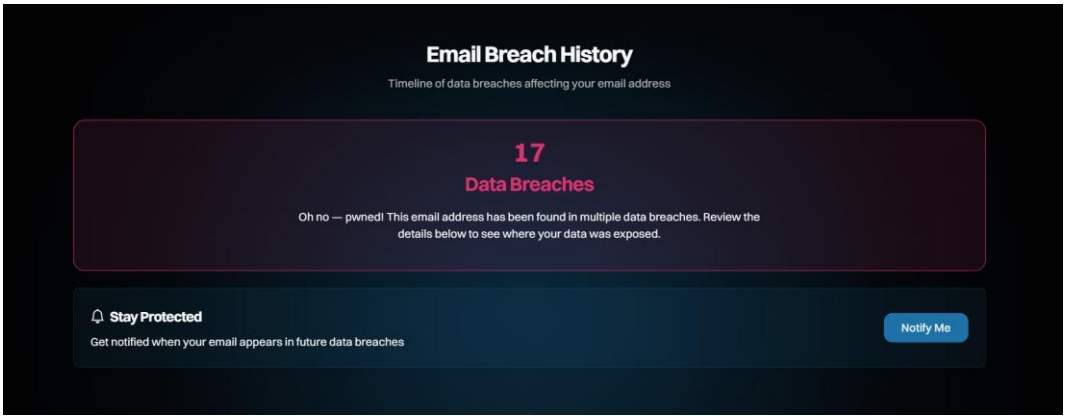
Berikut merupakan hasil pengujian menggunakan HIBP (*HaveIBeenPwned?*) dan IntelligenceX

Tabel 4. 5 Hasil pengujian dengan HIBP dan IntelX

No	Email	HIBP	IntelX
1.	ahmad.rifai@gmail.com	Terdeteksi	Terdeteksi
2.	artefakpapua@gmail.com	Terdeteksi	Terdeteksi
3.	dianpurnamis12@gmail.com	-	Terdeteksi
4.	dikbudlotimbidangkebudayaan@gmail.com	-	Terdeteksi
5.	dinporabudpar@banyumaskab.go.id	-	Terdeteksi
6.	disparbudtrenggalek@gmail.com	Terdeteksi	Terdeteksi
7.	ilhambrk@gmail.com	Terdeteksi	Terdeteksi
8.	nanirahayutari@yahoo.com	-	Terdeteksi
9.	nasdir70@gmail.com	-	Terdeteksi
10.	novianmashuri76@gmail.com	-	Terdeteksi
11.	nuelema753@gmail.com	-	Terdeteksi
12.	ridwansamal@yahoo.co.id	-	Terdeteksi
13.	syahj4923@gmail.com	-	Terdeteksi
14.	syahri.kobum@gmail.com	-	Terdeteksi
15.	tebatrasau@gmail.com	-	Terdeteksi
16.	yermin68@gmail.com	-	Terdeteksi
17.	yongkimahendra24@gmail.com	Terdeteksi	Terdeteksi

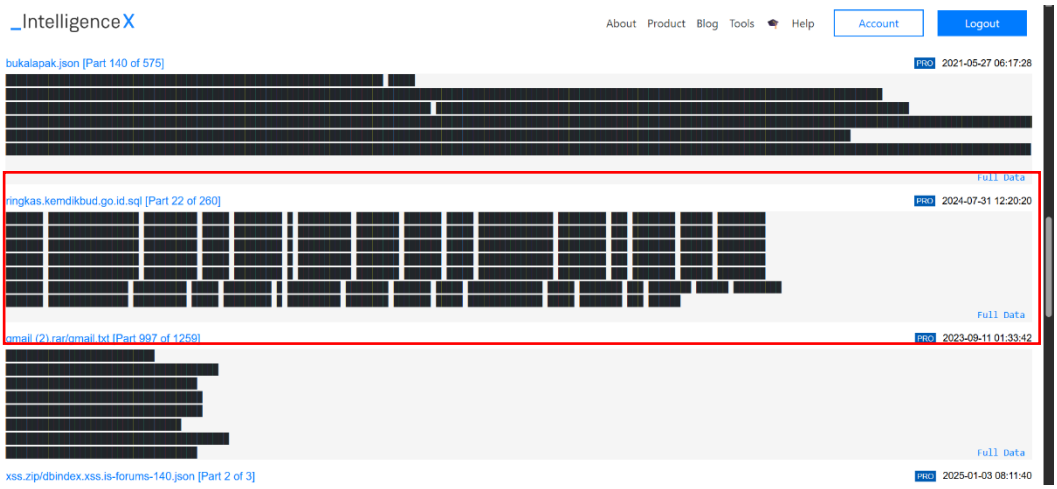
Berikut merupakan penjelasan terkait hasil pengujian menggunakan HIBP dan Intelx

a. HIBP hanya mendeteksi 5 dari 17 email (±29%) sebagai bagian dari breach yang pernah terjadi.



Gambar 4. 17 Hasil deteksi menggunakan HIBP

b. Sementara itu, IntelX mendeteksi ke-17 email (100%) telah muncul dalam indeks publik kebocoran data, termasuk yang berasal dari *dark web*, forum *underground*, dan *pastebin dump*.



Gambar 4. 18 Hasil deteksi menggunakan IntelligenX

Temuan ini memperkuat dugaan bahwa entitas digital pada dataset yang dianalisis memang telah terlibat dalam kebocoran data dan memiliki jejak digital dalam arsip *underground*, baik sebagai korban langsung maupun sebagai bagian dari dataset yang dijual atau dibagikan secara bebas. Terlihat pada gambar 4.13 ada

total 5/17 email terdeteksi pernah terjadi kebobolan data dan tersebar di *Darkweb*. Tetapi HIBP kurang efektif dikarenakan hanya terdapat total 5 email dan untuk kepastian data itu dibobol pada kasus "Kemdikbudristek 2024" belum memadai. Sedangkan pada hasil pendeteksi IntelX terlihat jelas bahwa total 17 email dari data sampel tersebut pernah terjadi kebobolan pada kasus "Kemdikbudristek 2024" yang terlihat jelas pada gambar 4.14 yaitu ada kebocoran data "ringkas.kemdikbud.go.id" dan terlihat jelas bahwa file itu berformat "SQL". Ini menandai bahwa data sampel yang disebarluaskan dari kedua forum tersebut dinyatakan valid pernah terjadi kebobolan pada tahun 2024.

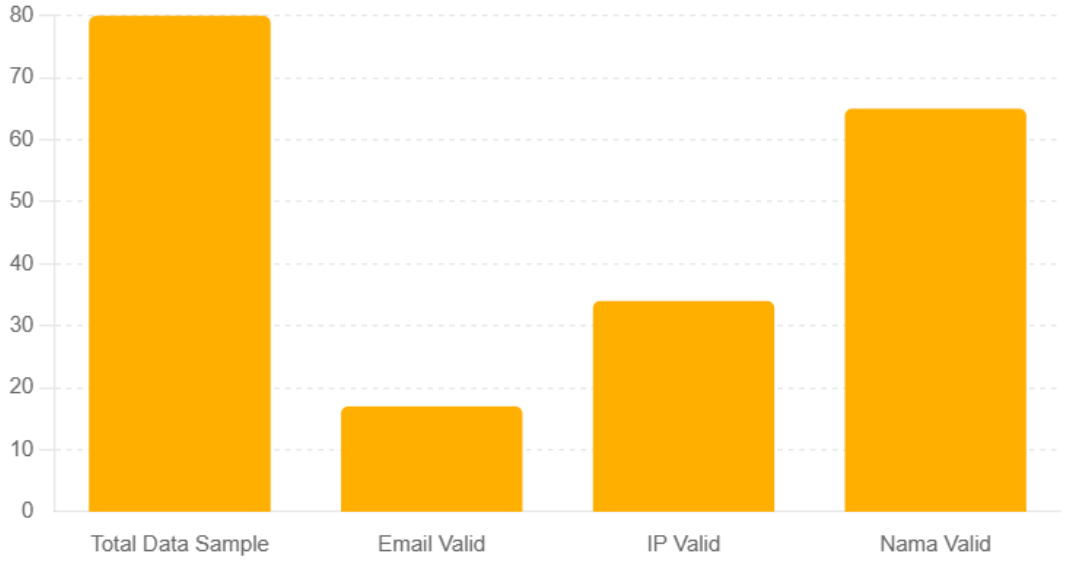
4.6. Penyajian dan Pelaporan Temuan (*Dissemination & Reporting*)

Berikut adalah format pelaporan akhir dari hasil investigasi forensik digital terhadap kasus perdagangan data pribadi yang diduga berasal dari sistem internal Kemdikbudristek dan diperjualbelikan di forum *Leakbase* dan *DarkForums*. Penyajian ini disusun berdasarkan kerangka NIST SP 800-86 dan *Threat Intelligence Lifecycle* yang telah diimplementasikan secara sistematis.

Tabel 4. 6 Hasil Temuan Utama

No	Komponen	Deskripsi
1.	Sumber Data Bocor	ringkas.kemdikbud.go.id (tervertifikasi di IntelX)
2.	Aktor Penjualan Data	Grepcn (*leaker*) & knox (*Re-uploader)*
3.	Deskripsi Kebocoran Data	*In September 2024 Ministry Of Education, Culture, Research and Technology (Indonesia) suffered a data breach. The leak exposed to the public over 5.6M lines of data belonging their*

		reports, people and many more internal records. *Compromised data: Full names, Ip addresses, Email addresses, Addresses, Phone numbers etc.* *Breached by @grepcn*
4.	Tanggal Kebocoran Data	Diunggah pada 23 September 2024 (*Leakbase* by grepcn) Disebarkan pada 24 September 2024 (*DarkForums* by Knox)
4.	Forum Distribusi	*LeakBase* (oleh grepcn) dan *DarkForums* (oleh knox)
5.	Format File	SQL *Dump*, diunggah via biteblob.com
6.	Jumlah Sampel Terverifikasi	80 entri data
7.	Data Valid	65 nama valid, 34 IP valid, 17 email valid
8.	Tipe Data	Nama, email, instansi, IP, nomor HP, timestamp
9.	Hasil Validasi Sampel	IntelX (100% terdeteksi), HIBP (29% terdeteksi)
10.	Metode Penjualan	*Hidden Content* berbayar via *cryptocurrency*



Gambar 4. 19 Visualisasi Jumlah Data yang terverifikasi

Pada Gambar 4.19 menunjukkan hasil verifikasi terhadap data pribadi yang diperoleh dari dump kebocoran Kemendikbudristek 2024. Dari total 80 data sampel yang dianalisis, sebanyak 65 data mengandung nama lengkap yang valid (81,25%), 34 data memuat alamat IP valid (42,5%), dan hanya 17 data yang memiliki alamat email valid (21,25%). Visualisasi ini menegaskan bahwa sebagian besar data yang bocor mengandung informasi identitas dasar seperti nama dan IP address, sementara data email memiliki tingkat validitas yang lebih rendah karena banyak entri yang tidak lengkap atau kosong.

Tabel 4. 7 Prediksi Penyebab Kebocoran Data

No	**Fakta Temuan Penelitian**	**Prediksi Penyebab**
1.	Data berbentuk SQL *dump*, berisi struktur tabel, field lengkap	Kemungkinan diambil dari akses langsung database (*internal access*)
2.	Banyak data *plaintext*, tanpa enkripsi	Tidak diterapkan *enkripsi* atau proteksi data *level field*

3.	Data bocor dan diperjual belikan di forum	Tidak adanya sistem deteksi kebocoran data (*leak monitoring*)
4.	Email dan IP instansi bocor secara spesifik	Tidak adanya pembatasan akses berdasarkan kredensial atau IP
5.	Distribusi data dilakukan oleh aktor teknis (grepcn) dengan deskripsi sistematis dengan format SQL yang bisa dilihat dari data sampel yang disebarkan.	Akses langsung ke database oleh pihak internal atau eksploitasi kredensial admin. Biasanya ini terjadi antara kelalaian dalam menentukan kredensial admin atau kemungkinan bisa juga serangan dari dalam (*Insider Threat)*

Tabel 4. 8 Tabel Solusi Mitigasi Berbasis Fishbone

No	**Kategori**	**Solusi Rekomendasi**
1.	*Man* (*Insider Threat*)	Implementasi sistem deteksi aktivitas mencurigakan oleh internal *(Insider Threat Detection)* seperti monitoring *file-access log* oleh admin sistem.
2.	*Machine*	Menerapkan enkripsi pada database (*field-level encryption*) dan membatasi akses query dengan sistem *whitelist*.
3.	*Method*	Menyusun prosedur audit log internal dan menerapkan teknik honeytoken untuk mendeteksi aktivitas eksfiltrasi data

4.	*Measurement*	Mengintegrasikan platform *Threat Intelligence* untuk pemantauan indikator kompromi (IoC) secara *real-time*.
5.	*Material*	Menerapkan masking atau hashing untuk data pribadi sensitif seperti NIK, email, dan nomor HP, serta menghapus data tidak relevan dari sistem cadangan publik.
6.	*Enviroment*	Membangun sistem pemantauan kata kunci internal yang mendeteksi indikasi kebocoran melalui indeks publik seperti IntelX dan leak archive lainnya.

4.7. Evaluasi dan Perbandingan Hasil Penelitian

Evaluasi dan perbandingan hasil penelitian ini disusun untuk membahas sejauh mana metode dan pendekatan yang dilakukan ini secara efektif dan efisien. Evaluasi dilakukan berdasarkan pengalaman implementasi selama proses investigasi, mulai dari pengumpulan data, analisis, hingga pelaporan. Selain itu, bagian ini juga membandingkan hasil penelitian dengan beberapa studi sebelumnya yang relevan, guna melihat kontribusi, perbedaan pendekatan, serta keunikan yang ditawarkan oleh penelitian ini dalam konteks pengembangan keilmuan di bidang forensik digital dan keamanan informasi.

4.7.1. Evaluasi Internal terhadap Proses Penelitian

Evaluasi terhadap proses investigasi dilakukan dengan pendekatan analisis deskriptif kuantitatif yang didukung oleh pemanfaatan berbagai *tools open-source*. Tujuannya adalah untuk mengukur sejauh mana metode dan alat bantu yang

digunakan dalam penelitian ini mampu menghasilkan temuan yang akurat dan relevan terhadap kasus kebocoran data Kemdikbudristek tahun 2024.

Evaluasi dilakukan menggunakan pendekatan analisis deskriptif kuantitatif, dibantu oleh tools open-source seperti *Intelligence* X, *HaveIBeenPwned*, dan VirusTotal. Beberapa indikator utama yang digunakan dalam evaluasi efektivitas metode *OSINT* dan *Threat Intelligence* dalam penelitian ini meliputi:

a. Akurasi Deteksi: IntelX berhasil mendeteksi seluruh 17 sampel email (100%) sebagai bagian dari kebocoran yang terkait dengan domain ringkas.kemdikbud.go.id, sedangkan HIBP hanya mendeteksi 5 dari 17 email (29%). Hal ini menunjukkan bahwa IntelX lebih unggul dalam jangkauan indeks data kebocoran dari sumber underground.
b. Kelengkapan Atribut Data: Dari total 80 entri data, sebanyak 65 data mengandung nama valid, 34 IP valid, dan 17 email valid. Ini menunjukkan tingkat kelengkapan informasi yang cukup tinggi, mendukung analisis entitas dengan visualisasi graf.
c. Relevansi Kontekstual: Data yang diperoleh memiliki struktur SQL dump, lengkap dengan metadata institusional dan timestamp yang cocok dengan deskripsi kebocoran oleh aktor bernama @grepcn di LeakBase.
d. Efisiensi Tools: Penggunaan CSI Linux sebagai platform terpadu memungkinkan analisis dilakukan secara aman dalam lingkungan virtual. NetworkX juga memberikan hasil visualisasi relasi antar entitas yang efektif dalam mendeteksi pola distribusi data.
e. Evaluasi Risiko Akses: Tools VirusTotal digunakan untuk mengecek keamanan forum dan file yang ditautkan. Hasil menunjukkan bahwa link

biteblob.com ditandai sebagai berbahaya oleh beberapa vendor, sehingga peneliti dapat menghindari potensi infeksi malware selama proses pengumpulan data.

Dari hasil evaluasi di atas, dapat disimpulkan bahwa metode dan tools yang digunakan dalam penelitian ini memberikan hasil yang akurat, relevan, dan aman, sesuai dengan prinsip etika dan metodologi forensik digital.

4.7.2. Perbandingan dengan Penelitian Sebelumnya

Dari hasil penelitian yang sudah saya lakukan, berikut merupakan beberapa perbandingan antara penelitian saya dengan penelitian yang terdahulu telah dilakukan

Tabel 4. 9 Tabel Hasil Perbandingan

No	Penulis (Tahun)	Fokus Penelitian	Metode yang Digunakan	Kelebihan	Kelemahan
1	Nugranto & Koprawi (2023)	Investigasi umum kejahatan di Surface dan Deep Web	NIST SP 800-86	Menggunakan framework forensik terstruktur	Tidak mengintegrasikan Threat Intelligence; tidak fokus pada perdagangan data
2	Nazah et al. (2020)	Deteksi ancaman Dark Web secara teknis	Analisis hash, traffic, scraping, node TOR	Teknik deteksi Dark Web bervariasi	Tidak menggunakan pendekatan forensik NIST dan OSINT

3	Risman Saputra et al. (2023)	Investigasi kebocoran data secara umum	OSINT + Detection Maturity Level (DML)	Efektif untuk identifikasi pelaku	Tidak menggunakan framework forensik seperti NIST
4	Kühn et al. (2024)	Evaluasi Dark Web untuk Cyber Threat Intelligence	Manual dan semi-otomatis scraping forum & marketplace	Menyediakan analisis luas pada Dark Web	Tidak fokus pada data pribadi; tantangan teknis tinggi
5	Rajamäki et al. (2022)	Investigasi eksploitasi anak di Dark Web	OSINT	Fokus pada tantangan hukum dan teknis dalam investigasi LEA	Tidak relevan langsung dengan perdagangan data pribadi
6	Penelitian saya (2025)	Perdagangan data pribadi di Dark Web (kasus Kemendikbudristek 2024)	Integrasi NIST SP 800-86, Threat Intelligence Lifecycle, OSINT, Validasi HIBP & IntelX, Visualisasi Python	Spesifik pada perdagangan data, integrasi framework lengkap, visualisasi aktor dan relasi, solusi mitigasi berbasis fishbone	Fokus pada satu kasus, terbatas pada sampel yang dipublikasikan di forum

BAB V

PENUTUP

5.1. Kesimpulan

Penelitian ini dilakukan untuk menyelidiki praktik perdagangan data pribadi di Dark Web, dengan mengambil kasus kebocoran data pada Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi (Kemendikbudristek) pada tahun 2024 sebagai studi utama. Proses investigasi dilakukan dengan menggabungkan pendekatan forensik digital berbasis kerangka NIST SP 800-86 dan pendekatan intelijen siber melalui Threat Intelligence Lifecycle, serta didukung oleh penggunaan berbagai tools Open Source Intelligence (OSINT).

Berdasarkan hasil penelitian yang dilakukan terhadap kasus kebocoran data Kemdikbudristek 2024 yang diperjualbelikan di forum LeakBase dan DarkForums, dapat disimpulkan bahwa:

a. OSINT dan Threat Intelligence terbukti efektif digunakan dalam investigasi digital forensik terhadap perdagangan data pribadi di Dark Web. Teknik ini mampu mengidentifikasi struktur data, memprofilkan aktor pelaku, serta memverifikasi keaslian data bocor melalui platform seperti IntelX dan HIBP.
b. Validasi data menggunakan OSINT menunjukkan tingkat keberhasilan yang tinggi, khususnya pada platform IntelX yang mendeteksi 100% sampel email sebagai bagian dari kebocoran. Hal ini menunjukkan bahwa data yang dianalisis valid dan relevan dengan insiden kebocoran Kemdikbudristek 2024.

c. Pola perdagangan data di Dark Web menyerupai sistem e-commerce tersembunyi, di mana data dijual dalam format SQL dump melalui skema hidden content dan mata uang kripto. Aktor utama seperti "grepcn" dan "Knox" berperan dalam penyebaran lintas forum.
d. Penerapan model NIST SP 800-86 dan Threat Intelligence Lifecycle secara bersamaan memberikan pendekatan yang holistik, mulai dari proses pengumpulan, pemeriksaan, analisis, hingga pelaporan. Pendekatan gabungan ini mampu menggambarkan alur investigasi secara terstruktur dan dapat direplikasi untuk studi kasus serupa.
e. Penyebab kebocoran data kemungkinan besar berasal dari kelalaian sistem internal, baik karena absennya proteksi enkripsi, lemahnya deteksi kebocoran, atau potensi insider threat. Hal ini diperkuat oleh format data yang terstruktur rapi dalam SQL dump dan indikasi akses langsung ke database.
f. Kelemahan penelitian ini terletak pada beberapa aspek, yaitu data yang dianalisis hanya terbatas pada cuplikan (*preview*) yang dipublikasikan secara terbuka sehingga belum merepresentasikan keseluruhan dataset, penggunaan tools masih terbatas pada versi freemium sehingga detail analisis tidak sepenuhnya dapat diakses, fokus penelitian hanya pada satu kasus kebocoran (Kemendikbudristek 2024) sehingga generalisasinya masih terbatas, serta penelitian ini bersifat observasi pasif tanpa keterlibatan langsung dalam transaksi sehingga analisis hanya bergantung pada bukti digital yang tersedia di ruang publik.

5.2. Saran

Berdasarkan temuan dan kesimpulan dari penelitian ini, penulis memberikan beberapa saran berikut:

1. Untuk Instansi Pemerintah dan Organisasi Pemilik Data:
    a. Terapkan enkripsi data pada tingkat field dalam database untuk melindungi data sensitif.
    b. Implementasikan sistem monitoring aktivitas internal *(insider threat detection*) dan *real-time threat intelligence*.
    c. Lakukan audit berkala dan simulasi insiden keamanan untuk meningkatkan kesiapsiagaan terhadap kebocoran data.
2. Untuk Peneliti Selanjutnya:
    a. Disarankan memperluas cakupan dengan membandingkan lebih dari satu kasus kebocoran untuk melihat tren nasional maupun global.
    b. Mengembangkan sistem deteksi otomatis berbasis machine learning untuk mengidentifikasi kebocoran data sejak dini dari forum-forum *Dark Web*.
    c. Menyertakan wawancara atau kerja sama dengan institusi keamanan siber untuk validasi hasil secara lebih menyeluruh.
3. Untuk Masyarakat Umum:
    a. Tingkatkan kesadaran akan pentingnya perlindungan data pribadi di internet.
    b. Hindari penggunaan kredensial yang sama pada berbagai platform dan manfaatkan layanan verifikasi kebocoran data secara berkala seperti HIBP.

Penelitian ini diharapkan dapat memberikan kontribusi praktis dan akademis dalam pengembangan strategi keamanan data di era digital yang semakin kompleks, serta menjadi pijakan awal bagi studi lanjutan dalam bidang forensik digital, OSINT, dan intelijen ancaman siber.

DAFTAR PUSTAKA

Aljuhami, A. M., & Bamasoud, D. M. (2021). Cyber Threat Intelligence in Risk Management A Survey of the Impact of Cyber Threat Intelligence on Saudi Higher Education Risk Management. In *IJACSA) International Journal of Advanced Computer Science and Applications* (Vol. 12, Issue 10). www.ijacsa.thesai.org

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers and Security*, *98*. https://doi.org/10.1016/j.cose.2020.102003

Anggen Suari, K. R., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *6*(1), 132–142. https://doi.org/10.38043/jah.v6i1.4484

Anugerah, F. (2021). *PENCURIAN DATA PRIBADI DI INTERNET DALAM PERSPEKTIF KRIMINOLOGI*. https://ejournal.undiksha.ac.id/index.php/jkh

Davies, G. (2020). Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers. *Journal of Criminal Law*, *84*(5), 407–426. https://doi.org/10.1177/0022018320952557

Dokman, T., & Ivanjko, T. (2020). Open Source Intelligence (OSINT): issues and trends. *INFuture2019: Knowledge in the Digital Age*. https://doi.org/10.17234/infuture.2019.23

FFaizal, A., & Luthfi, A. (2024). Comparison Study of NIST SP 800-86 and ISO/IEC 27037 Standards as A Framework for Digital Forensic Evidence Analysis. *Journal of Information Systems and Informatics*, *6*(2), 701–718. https://doi.org/10.51519/journalisi.v6i2.717

Hariyadi, D., Sadewo, B., Munajat, K., & Pratama, D. (2022). *Buku Panduan Dasar Forensik Digital*. https://www.researchgate.net/publication/365993681

Hukom, R., & Setiadi, M. H. (2025). Pengaruh Media Sosial terhadap Pola Kejahatan di Era Digital: Studi Kriminologi dengan Pendekatan Netnografi. *Perkara : Jurnal Ilmu Hukum Dan Politik*, *3*(1), 750–768. https://doi.org/10.51903/perkara.v3i1.2353

Kuhn, P., Wittorf, K., & Reuter, C. (2024). Navigating the Shadows: Manual and Semi-Automated Evaluation of the Dark Web for Cyber Threat Intelligence. *IEEE Access*, *12*, 118903–118922. https://doi.org/10.1109/ACCESS.2024.3448247

Kumar, N. (2024). OSINT (OPEN SOURCE INTELLIGENCE) Exploring the Power of Open Source Intelligence in Modern Decision-Making. *INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT*, *08*(05), 1–5. https://doi.org/10.55041/IJSREM34025

Lavinia, N., & Puspitasari. (2023). URGENSI PEMANFAATAN OPEN SOURCE INTELLIGENT (OSINT) DALAM UPAYA PENCEGAHAN AKSI TERORISME DI INDONESIA. *Jurnal Sosial Humaniora Terapan*, *6*(1). https://doi.org/10.7454/jsht.v6i1.1105

Lubis, S. (2023). *SERANGAN CYBER DAN KEBOCORAN DATA PADA LEMBAGA KEUANGAN SYARIAH PRA DAN PASCA UU NO. 27 TAHUN 2022 TENTANG PELINDUNGAN DATA PRIBADI DAN UU NO. 4 TAHUN 2023 TENTANG PENGEMBANGAN DAN PENGUATAN SEKTOR KEUANGAN*.

Method Karamagi, R., Said, A., & Karamagi, R. M. (2020). *Implementation of Inter-Networking with Host Internet in Oracle® VirtualBox Guest Virtual Machines*. https://doi.org/10.36648/computer-science-engineering-survey.08.02.10

Mishardila, G. (2020). *Penerapan siklus intelijen ancaman yang efektif memungkinkan organisasi untuk secara proaktif mengidentifikasi dan menanggapi ancaman keamanan siber sebelum mereka berkembang menjadi insiden yang merugikan*.

Nazah, S., Huda, S., Abawajy, J. H., & Hassan, M. M. (2021). An Unsupervised Model for Identifying and Characterizing Dark Web Forums. *IEEE Access*, *9*, 112871–112892. https://doi.org/10.1109/ACCESS.2021.3103319

Nazah, S., Huda, S., Abawajy, J., & Hassan, M. M. (2020). Evolution of dark web threat analysis and detection: A systematic approach. *IEEE Access*, *8*, 171796–171819. https://doi.org/10.1109/ACCESS.2020.3024198

Nugranto, H. F., & Koprawi, M. (2024a). Investigasi Kejahatan Siber pada Surface Web dan Deep Web Menggunakan Metode NIST. *Julyxxxx, x, No.x*, 1–5. https://doi.org/https://doi.org/10.35957/jatisi.v11i1.3245

Nugranto, H. F., & Koprawi, M. (2024b). Investigasi Kejahatan Siber pada Surface Web dan Deep Web Menggunakan Metode NIST. *Julyxxxx, x, No.x*, 1–5. https://doi.org/https://doi.org/10.35957/jatisi.v11i1.3245

Paranjape, H. (2020). Cyber Threat Intelligence: How to Collect and Analyse Data to Detect, Prevent and Mitigate Cyber Threats Aryendra Dalal Manager Application Security Engineer-Deloitte LLP. In *International Journal on*

Recent and Innovation Trends in Computing and Communication. http://www.ijritcc.org

Prasetyo, D., Sebayang, N., Dillianto, B., & Staff dan Komando TNI Angkatan Laut, S. (2023). *Pemanfaatan Open Source Intelligence dalam Membantu Tugas TNI untuk Melindungi Pertahanan Negara*. http://Jiip.stkipyapisdompu.ac.id

Puyvelde, D. Van, & Rienzi, F. T. (2025). The rise of open-source intelligence. *European Journal of International Security*. https://doi.org/10.1017/eis.2024.61

Rajamäki, J. (2022). OSINT on the Dark Web: Child Abuse Material Investigations. *Information & Security: An International Journal*, *53*, 21–32. https://doi.org/10.11610/isij.5302

Reddy Gopireddy, R. (2020). Dark Web Monitoring: Extracting and Analyzing Threat Intelligence. *International Journal of Science and Research (IJSR)*, *9*(3), 1693–1696. https://doi.org/10.21275/SR24801072234

Ring, M., Schlör, D., Wunderlich, S., Landes, D., & Hotho, A. (2021). Malware detection on windows audit logs using LSTMs. *Computers and Security*, *109*. https://doi.org/10.1016/j.cose.2021.102389

Risman Saputra, D., & Arizal, A. (2023). *Investigasi Insiden Kebocoran Data Menggunakan Integrasi Melalui Pendekatan Open Source Intelligence dan Detection Maturity Level Model*.

Samad, M. Y., Ningtiyas, B. K., Fiqih, Rosny, F., & Permatasari, D. A. (2024). Anticipating Cyber Espionage: Open Source Intelligence (OSINT)

Investigation and Cyber Counterintelligence. *Journal of Students' Research in Computer Science*, *5*(2), 167–184. https://doi.org/10.31599/288ab341

Sanjaya, W., Sugiantoro, B., & Prayudi, Y. (2020). A Metode Offline Forensik Untuk Analisis Digital Artefak Pada TOR Browser Di Sistem Operasi Linux. *JITU : Journal Informatic Technology And Communication*, *4*(2), 41–51. https://doi.org/10.36596/jitu.v4i2.345

Szymoniak, S., & Foks, K. (2024). Open Source Intelligence Opportunities and Challenges – A Review. *Advances in Science and Technology Research Journal*, *18*(3), 123–139. https://doi.org/10.12913/22998624/186036

CSI LINUX. (2023). *Cyber Investigation Operating System*. Retrieved Maret 18, 2025, from CSI Linux: https://csilinux.com/

Kali linux Documentation. (2023). *Kali Linux Tools Listing.* Retrieved Maret 18, 2025, from Kali Linux: https://www.kali.org/docs/

Rachmatunnisa. (2024). *Rangkuman Serangan Siber 2024 CISSReC: Darurat Judi Online hingga PDNS Lumpuh*. (DetikInet) Retrieved March 5, 2025, from https://inet.detik.com/security/d-7711614/rangkuman-serangan-siber-2024-cissrec-darurat-judi-online-hingga-pdns-lumpuh?form=MG0AV3

Wikipedia. (2025, 3 4). *VirtualBox*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/VirtualBox?

IBM. (2024, November 26). *83% of organizations reported insider attacks in 2024*. Retrieved from IBM: https://www.ibm.com/think/insights/83-percent-organizations-reported-insider-threats-2024

LAMPIRAN

Lampiran 1 SK-2 Penetapan Dosen Pembimbing

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UMSU Terakreditasi A Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 89/SK/BAN-PT/Akred/PT/III/2019
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003
umsumedan umsumedan umsumedan umsumedan

PENETAPAN DOSEN PEMBIMBING
PROPOSAL/SKRIPSI MAHASISWA
NOMOR : 439/II.3-AU/UMSU-09/F/2025

Assalamu'alaikum Warahmatullahi Wabarakatuh

Dekan Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Muhammadiyah Sumatera Utara, berdasarkan Persetujuan permohonan judul penelitian Proposal / Skripsi dari Ketua / Sekretaris.

Program Studi	**: Teknologi Informasi**
Pada tanggal	**: 26 Februari 2025**

Dengan ini menetapkan Dosen Pembimbing Proposal / Skripsi Mahasiswa.

Nama	**: Ahmad Al Qodri Azizi Dalimunthe**
NPM	**: 2109020031**
Semester	**: VII (Tujuh)**
Program studi	**: Teknologi Informasi**
Judul Proposal / Skripsi	**: Analisis Forensik Digital terhadap Perdagangan Data Pribadi di Dark Web Menggunakan OSINT dan Threat Intelligence**
Dosen Pembimbing	**: Mulkan Azhari, S.Kom, M.Kom.**

Dengan demikian di izinkan menulis Proposal / Skripsi dengan ketentuan

1. Penulisan berpedoman pada buku panduan penulisan Proposal / Skripsi Fakultas Ilmu Komputer dan Teknologi Informasi UMSU
2. Pelaksanaan Sidang Skripsi harus berjarak 3 bulan setelah dikeluarkannya Surat Penetapan Dosen Pembimbing Skripsi.
3. **Proyek Proposal / Skripsi** dinyatakan " **BATAL** " bila tidak selesai sebelum Masa Kadaluarsa tanggal : **26 Februari 2026**
4. Revisi judul……..

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Ditetapkan di : Medan
Pada Tanggal : 27 Sya'ban 1446 H
26 Februari 2025 M

Dekan

Dr. Al-Khowarizmi, M.Kom.
NIDN : 0127099201

Cc. File

Lampiran 2 *Letter Of Acceptance Journal*

JURNAL KOMPUTER TEKNOLOGI INFORMASI DAN SISTEM INFORMASI (JUKTISI)
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
e-ISSN : 2963-7104 | p-ISSN : 2962-3022

SURAT BUKTI TERIMA
(*Letter of Acceptance*)
Nomor: JUKTISI/95/VI/2025

Yang bertanda tangan dibawah ini :

Publisher	:	LKP KARYA PRIMA KURSUS
Alamat	:	Jl. Gurilla No. 2 Sidorejo Medan
Jurnal	:	Jurnal Komputer Teknologi Informasi dan Sistem Informasi (JUKTISI)
ISSN	:	e-ISSN : 2961-7286 | p-ISSN : 2962-3677

Menerangkan bahwa setelah dilakukan proses review dan revisi, maka tim redaksi (Editorial Team) **menerima paper/artikel** dengan identitas sebagai berikut :

Penulis	:	Ahmad Al Qodri Azizi Dalimunthe, Mulkan Azhari
Judul	:	Analisis Forensik Digital Terhadap Perdagangan Data Pribadi Di Dark Web Menggunakan Osint& Threat Intelligence

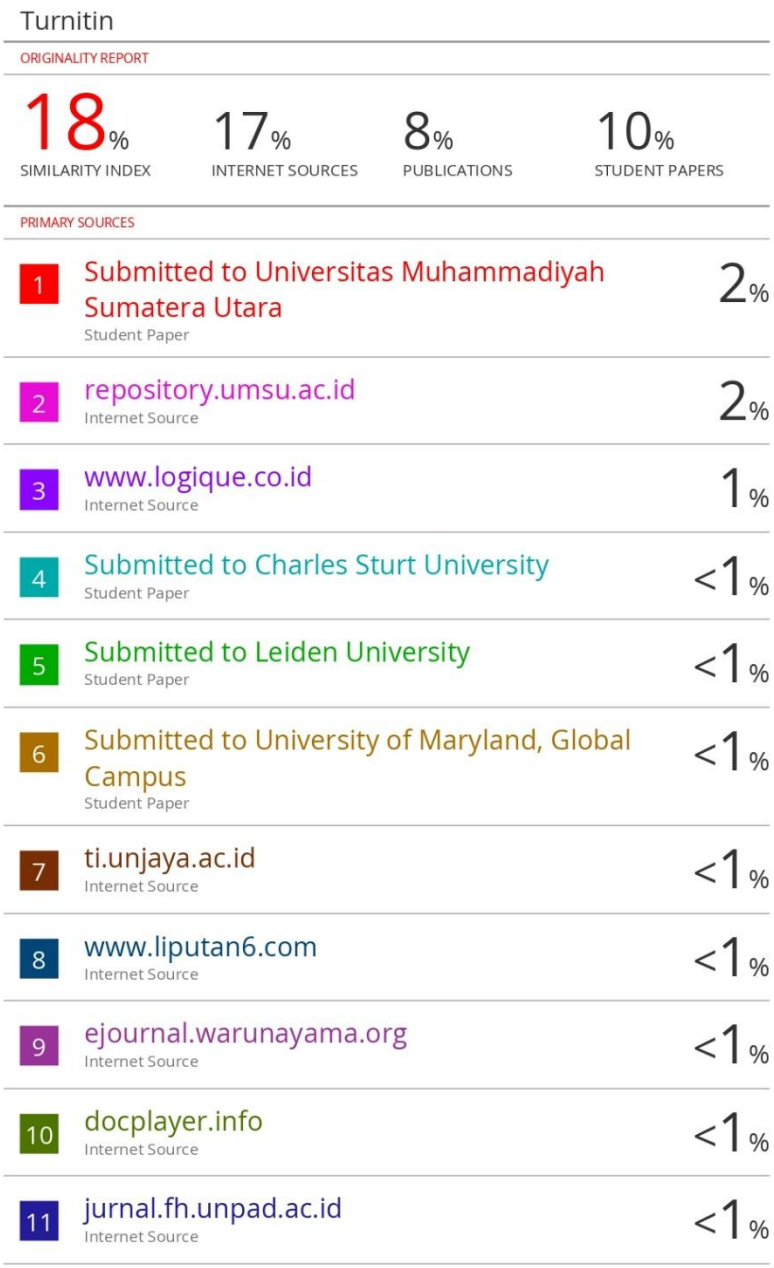
Akan dipublikasikan pada periode terbit Volume 4 No. 1 Juni 2025. Demikian Surat Bukti Terima (*Letter of Acceptance*) ini diperbuat untuk dipergunakan sebagaimana mestinya.

Medan, 26 Juni 2025
Editor in Chief : JUKTISI

Tim Editor

Silahkan SCAN untuk Download SK ISSN JUKTISI dari : https://issn.lipi.go.id/

Lampiran 3 Turnitin



Turnitin

ORIGINALITY REPORT

18%	17%	8%	10%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Universitas Muhammadiyah Sumatera Utara Student Paper	2%
2	repository.umsu.ac.id Internet Source	2%
3	www.logique.co.id Internet Source	1%
4	Submitted to Charles Sturt University Student Paper	<1%
5	Submitted to Leiden University Student Paper	<1%
6	Submitted to University of Maryland, Global Campus Student Paper	<1%
7	ti.unjaya.ac.id Internet Source	<1%
8	www.liputan6.com Internet Source	<1%
9	ejournal.warunayama.org Internet Source	<1%
10	docplayer.info Internet Source	<1%
11	jurnal.fh.unpad.ac.id Internet Source	<1%

12	journal.stekom.ac.id Internet Source	<1 %
13	www.journal-isi.org Internet Source	<1 %
14	repository.bsi.ac.id Internet Source	<1 %
15	ojs.upsi.edu.my Internet Source	<1 %
16	www.ejournal-jp3.com Internet Source	<1 %
17	eprints.amikom.ac.id Internet Source	<1 %
18	Submitted to Liberty University Student Paper	<1 %
19	Submitted to Queen's University of Belfast Student Paper	<1 %
20	Submitted to Open University of Cyprus Student Paper	<1 %
21	123dok.com Internet Source	<1 %
22	digilib.uinsgd.ac.id Internet Source	<1 %
23	Submitted to Adtalem Global Education Student Paper	<1 %
24	dspace.uii.ac.id Internet Source	<1 %
25	Amelia Pertiwi, Ayu Amelia Pertiwi. "IMPLEMENTASI OWNCLOUD PADA UBUNTU 24.04 MENGGUNAKAN VIRTUALBOX",	<1 %

	PROSISKO: Jurnal Pengembangan Riset dan Observasi Sistem Komputer, 2025 Publication	
26	repository.up.ac.za Internet Source	<1 %
27	www.ijana.in Internet Source	<1 %
28	aiya.org.au Internet Source	<1 %
29	www.ijritcc.org Internet Source	<1 %
30	Submitted to Southern New Hampshire University - Continuing Education Student Paper	<1 %
31	Submitted to Asia Pacific University College of Technology and Innovation (UCTI) Student Paper	<1 %
32	repository.unair.ac.id Internet Source	<1 %
33	Submitted to The Robert Gordon University Student Paper	<1 %
34	inet.detik.com Internet Source	<1 %
35	Friska Yulanda Pratiwi, Fajar Rachmad Dwi Miarsa. "Urgensi Edukasi Publik dalam Menangkal Penyalahgunaan Data Pribadi", RIGGS: Journal of Artificial Intelligence and Digital Business, 2025 Publication	<1 %
36	okhovvat.com Internet Source	<1 %

37	Submitted to Universitas Pamulang Student Paper	<1 %
38	blogseger.com Internet Source	<1 %
39	repository.uam.ac.id Internet Source	<1 %
40	Tri Ginanjar Laksana, Sri Mulyani. "PENGETAHUAN DASAR IDENTIFIKASI DINI DETEKSI SERANGAN KEJAHATAN SIBER UNTUK MENCEGAH PEMBOBOLAN DATA PERUSAHAAN", Jurnal Ilmiah Multidisiplin, 2024 Publication	<1 %
41	fikti.umsu.ac.id Internet Source	<1 %
42	jiip.stkipyapisdompu.ac.id Internet Source	<1 %
43	www.scribd.com Internet Source	<1 %
44	journalstories.ai Internet Source	<1 %
45	repository.iaknambon.ac.id Internet Source	<1 %
46	repository.tudelft.nl Internet Source	<1 %
47	www.alinea.id Internet Source	<1 %
48	etd.umy.ac.id Internet Source	<1 %

49	file.scirp.org Internet Source	<1 %
50	Submitted to Sriwijaya University Student Paper	<1 %
51	rifqimulyawan.com Internet Source	<1 %
52	text-id.123dok.com Internet Source	<1 %
53	"Potensi Ancaman Penggunaan OSINT Menyebabkan Kegagalan Pengambilan Keputusan Akibat Informasi Hoax", Jurnal Kajian Stratejik Ketahanan Nasional, 2023 Publication	<1 %
54	Submitted to Western Illinois University Student Paper	<1 %
55	repository.mercubuana.ac.id Internet Source	<1 %
56	scholar.ui.ac.id Internet Source	<1 %
57	Submitted to Fakultas Ekonomi Universitas Indonesia Student Paper	<1 %
58	T. Mariprasath, Kumar Reddy Cheepati, Marco Rivera. "Practical Guide to Machine Learning, NLP, and Generative AI: Libraries, Algorithms, and Applications", River Publishers, 2024 Publication	<1 %
59	Submitted to Technological University Dublin Student Paper	<1 %
60	lib.unnes.ac.id Internet Source	

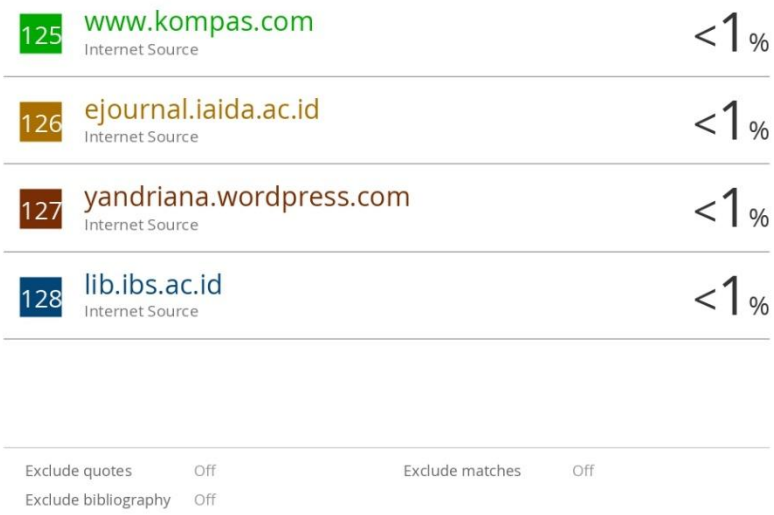
		<1 %
61	link.springer.com Internet Source	<1 %
62	ojs.unikom.ac.id Internet Source	<1 %
63	repositori.uma.ac.id Internet Source	<1 %
64	repository-feb.unpak.ac.id Internet Source	<1 %
65	repository.dinamika.ac.id Internet Source	<1 %
66	"URGENSI PEMANFAATAN OPEN SOURCE INTELLIGENT (OSINT) DALAM UPAYA PENCEGAHAN AKSI TERORISME DI INDONESIA", Jurnal Sosial Humaniora Terapan, 2023 Publication	<1 %
67	artikelpendidikan.id Internet Source	<1 %
68	daeyynala.blogspot.com Internet Source	<1 %
69	dinastirev.org Internet Source	<1 %
70	ejournal.unhi.ac.id Internet Source	<1 %
71	mafiadoc.com Internet Source	<1 %
72	repository.bakrie.ac.id Internet Source	<1 %

73	repository.its.ac.id Internet Source	<1 %
74	repository.usu.ac.id Internet Source	<1 %
75	Abu S. S. M. Barkat Ullah, Al-Sakib Khan Pathan. "Security Analytics for the Internet of Everything", CRC Press, 2020 Publication	<1 %
76	Joceline Eloysa Halim, Timotius F.C.W. Sutrisno, Anak Agung Ayu Puty Andrina. "ANALISIS FAKTOR PENENTU NIAT PENGGUNAAN E-COMMERCE DI KALANGAN GENERASI Z: STUDI PADA UBIQUITOUS CONNECTIVITY, INFORMATION TRANSPARENCY, DAN INFORMATION OVERLOAD", JMBI UNSRAT (Jurnal Ilmiah Manajemen Bisnis dan Inovasi Universitas Sam Ratulangi)., 2024 Publication	<1 %
77	e-campus.iainbukittinggi.ac.id Internet Source	<1 %
78	eprints.pancabudi.ac.id Internet Source	<1 %
79	eprints.walisongo.ac.id Internet Source	<1 %
80	fe.ekasakti.org Internet Source	<1 %
81	indofakta.com Internet Source	<1 %
82	la.mathworks.com Internet Source	<1 %

83	pdffox.com Internet Source	<1 %
84	redasamudera.id Internet Source	<1 %
85	repositori.usu.ac.id Internet Source	<1 %
86	www.gentaandalas.com Internet Source	<1 %
87	www.ijraset.com Internet Source	<1 %
88	www.indobic.or.id Internet Source	<1 %
89	blogwoke.wordpress.com Internet Source	<1 %
90	boedimanagoes.wordpress.com Internet Source	<1 %
91	ciprutimut.blogspot.com Internet Source	<1 %
92	core.ac.uk Internet Source	<1 %
93	datadosen.com Internet Source	<1 %
94	downloadtesismanajemen.blogspot.com Internet Source	<1 %
95	ejurnal.kampusakademik.co.id Internet Source	<1 %
96	etheses.uin-malang.ac.id Internet Source	<1 %

97	findpdf.net Internet Source	<1 %
98	munthe14.wordpress.com Internet Source	<1 %
99	nasional.sindonews.com Internet Source	<1 %
100	network.bepress.com Internet Source	<1 %
101	penelitikomunikasi.blogspot.com Internet Source	<1 %
102	repository.uin-suska.ac.id Internet Source	<1 %
103	repository.unj.ac.id Internet Source	<1 %
104	repository.unsoed.ac.id Internet Source	<1 %
105	repository.unsri.ac.id Internet Source	<1 %
106	ruanglaptop.com Internet Source	<1 %
107	support.google.com Internet Source	<1 %
108	www.jatit.org Internet Source	<1 %
109	www.theseus.fi Internet Source	<1 %
110	Submitted to Universidad Privada del Norte Student Paper	<1 %

111	dasar-hacking.blogspot.com Internet Source	<1 %
112	digilib.uns.ac.id Internet Source	<1 %
113	dlib.uni-svishtov.bg Internet Source	<1 %
114	es.scribd.com Internet Source	<1 %
115	id.123dok.com Internet Source	<1 %
116	id.scribd.com Internet Source	<1 %
117	isij.eu Internet Source	<1 %
118	jkm.my.id Internet Source	<1 %
119	kumparan.com Internet Source	<1 %
120	repositorio.ug.edu.ec Internet Source	<1 %
121	repository.unugiri.ac.id:8443 Internet Source	<1 %
122	ssp.jst.go.jp Internet Source	<1 %
123	webdesign.tutsplus.com Internet Source	<1 %
124	www.brilio.net Internet Source	<1 %


125 www.kompas.com
Internet Source
<1%
126 ejournal.iaida.ac.id
Internet Source
<1%
127 yandriana.wordpress.com
Internet Source
<1%
128 lib.ibs.ac.id
Internet Source
<1%
Exclude quotes Off
Exclude matches Off
Exclude bibliography Off