JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER

p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 254-269
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.400

Analisis Forensik Digital Terhadap Perdagangan Data Pribadi Di Dark Web Menggunakan Osint & Threat Intelligence

Ahmad Al Qodri Azizi Dalimunthe[1,*], Mulkan Azhari[1]

[1]Ilmu Komputer dan Teknologi Informasi, Teknologi Informasi, Universitas Muhammadiyah SumateraUtara, Kota Medan, Indonesia
Email: [1]ahmadalqodridalimunthe@gmail.com, [2]mulkan@umsu.ac.id
(*Email Corresponding Author: ahmadalqodridalimunthe@gmail.com)
Received: 22 Juni 2025. | Revision: 26 Juni 2025 | Accepted: 26 Juni 2025

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

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*

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah menyebabkan meningkatnya ketergantungan masyarakat terhadap sistem digital, khususnya dalam pengelolaan data pribadi. Data pribadi kini menjadi aset digital yang sangat sensitif, mencakup informasi seperti nama lengkap, alamat, nomor identitas, hingga informasi keuangan dan kesehatan [1]. Ketika sistem informasi memiliki kerentanan, potensi kebocoran data pun meningkat. Kebocoran ini tidak hanya berasal dari serangan eksternal, tetapi juga dari serangan internal atau insider threat, sebagaimana dilaporkan oleh IBM (2024), yang menyatakan bahwa 83% organisasi mengalami serangan dari dalam dalam 12 bulan terakhir [2]. Salah satu medium utama dalam penyebaran data hasil kebocoran adalah Dark Web, yakni bagian tersembunyi dari internet yang hanya dapat diakses dengan jaringan terenkripsi seperti TOR. Karakteristik utama dari Dark Web adalah tingkat anonimitas yang tinggi, menjadikannya tempat populer bagi aktivitas ilegal seperti perdagangan data pribadi [3]. Forum-forum seperti LeakBase dan DarkForums kini menjadi tempat utama transaksi data sensitif yang mencakup identitas warga, akun pemerintahan, hingga jejak digital lembaga resmi. Insiden besar yang mengguncang Indonesia terjadi pada September 2024, ketika data internal milik Kemendikbudristek dilaporkan bocor dan diperjualbelikan oleh aktor siber di Dark Web [4]. Data tersebut mencakup nama lengkap, alamat email, IP address, nomor telepon, dan institusi asal. Hal ini menjadi indikasi lemahnya perlindungan data oleh instansi pemerintah dan pentingnya pengembangan metode investigasi yang mampu mendeteksi dan menganalisis peredaran data secara proaktif. Untuk menjawab tantangan tersebut, pendekatan Open Source Intelligence (OSINT) dan Threat Intelligence (TI) dinilai efektif dalam mendukung investigasi kebocoran data. OSINT merupakan metode pengumpulan data dari sumber terbuka seperti forum, media sosial, dan arsip publik, yang dapat digunakan untuk mengidentifikasi ancaman dan pelaku serangan [5][6]. Sementara itu, Threat Intelligence berperan dalam memberikan konteks, indikator kompromi (IoC), serta pola serangan yang dapat digunakan untuk mitigasi ancaman secara sistematis [7].

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 254-269
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.400

Penelitian terdahulu telah banyak membahas analisis Dark Web dari sisi teknis maupun hukum. Misalnya, Nazah (2020) menyoroti teknik pendeteksian seperti hash analysis dan exit node monitoring, sementara Nugranto & Koprawi (2024) menerapkan metode NIST untuk investigasi kejahatan siber secara umum. Namun, studi-studi tersebut belum mengintegrasikan pendekatan OSINT dan Threat Intelligence secara langsung dalam konteks kebocoran data di Indonesia [8] [9]. Oleh karena itu, penelitian ini menawarkan pendekatan yang lebih terintegrasi dan aplikatif dengan menggabungkan kerangka kerja NIST SP 800-86 dan Threat Intelligence Lifecycle untuk menganalisis satu studi kasus kebocoran data yang nyata. 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. OSINT memungkinkan pihak berwenang untuk mengakses, mengumpulkan, dan menganalisis data terbuka dari berbagai sumber, seperti media sosial, forum daring, berita, hingga metadata dari situs web. Melalui pendekatan ini, instansi terkait dapat melakukan deteksi dini terhadap potensi ancaman, memetakan jaringan pelaku, serta mengidentifikasi kerentanan pada infrastruktur kritis yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab.Hal ini menunjukkan bagaimana OSINT dapat digunakan dalam proses hukum dan investigasi keamanan digital [10].

Selain aspek teknis dan investigatif, kebocoran data pribadi juga merupakan pelanggaran hukum yang diatur dalam Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Dalam pasal-pasalnya, UU ini menegaskan bahwa setiap penyelenggara sistem elektronik wajib melindungi data pribadi pengguna, dan setiap penyebaran tanpa izin dapat dikenai sanksi pidana dan administratif. Hal ini menegaskan bahwa investigasi kebocoran data tidak hanya penting dari sisi forensik, tetapi juga untuk mendukung penegakan hukum yang berbasis bukti digital. Dengan demikian, penelitian ini bertujuan untuk memberikan kontribusi praktis dan akademik dalam pengembangan metode investigasi kebocoran data pribadi, khususnya yang terjadi di ekosistem Dark Web. Selain itu, penelitian ini juga diharapkan menjadi referensi dalam penguatan kebijakan keamanan informasi nasional yang berbasis pada analisis aktual dan pendekatan forensik digital yang terstruktur.

2. METODOLOGI PENELITIAN

2.1 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. 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 [11].

2.2 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.

Tabel 1. Tools yang digunakan dalam penelitian

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.

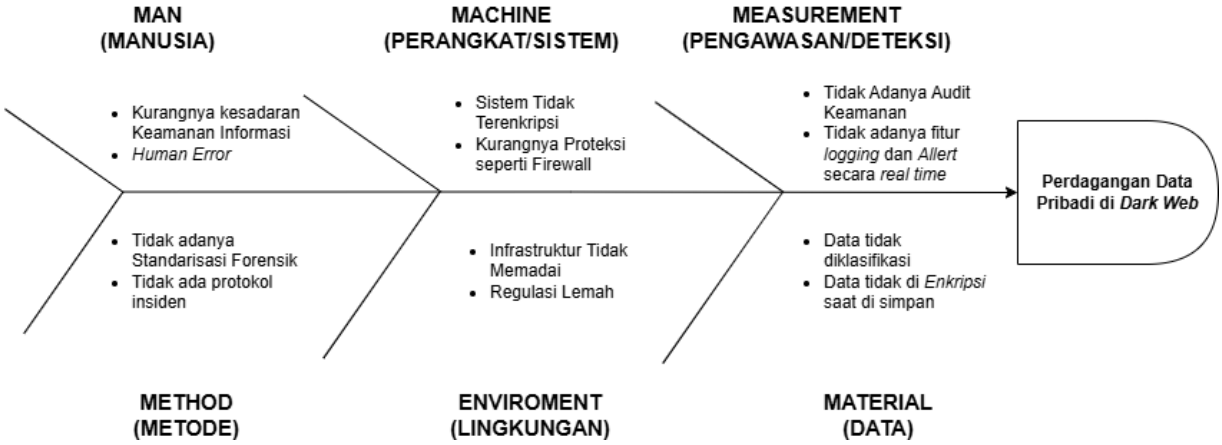
JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 254-269
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.400

Tabel 2. Perangkat yang digunakan

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

2.3 Fishbone Diagram

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* [12].

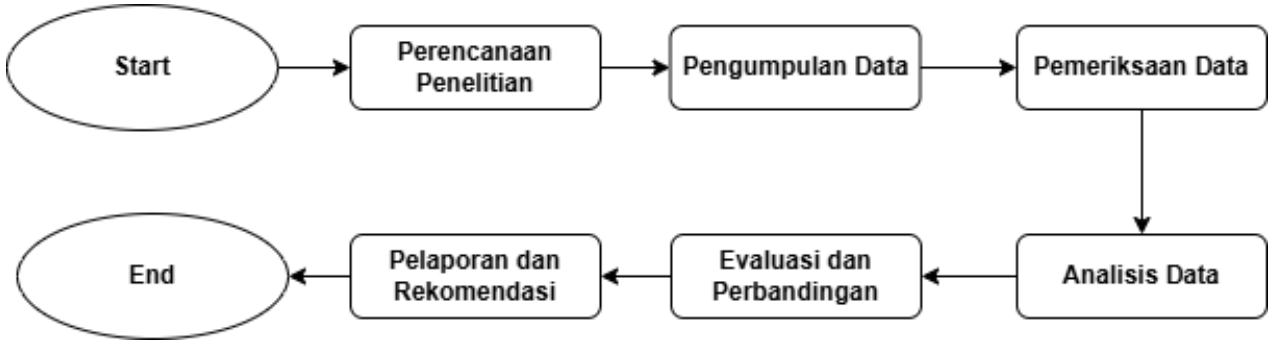


Gambar 1. *Fishbone Diagram*

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 [13].

2.4 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 2. Visualisasi Alur Penelitian

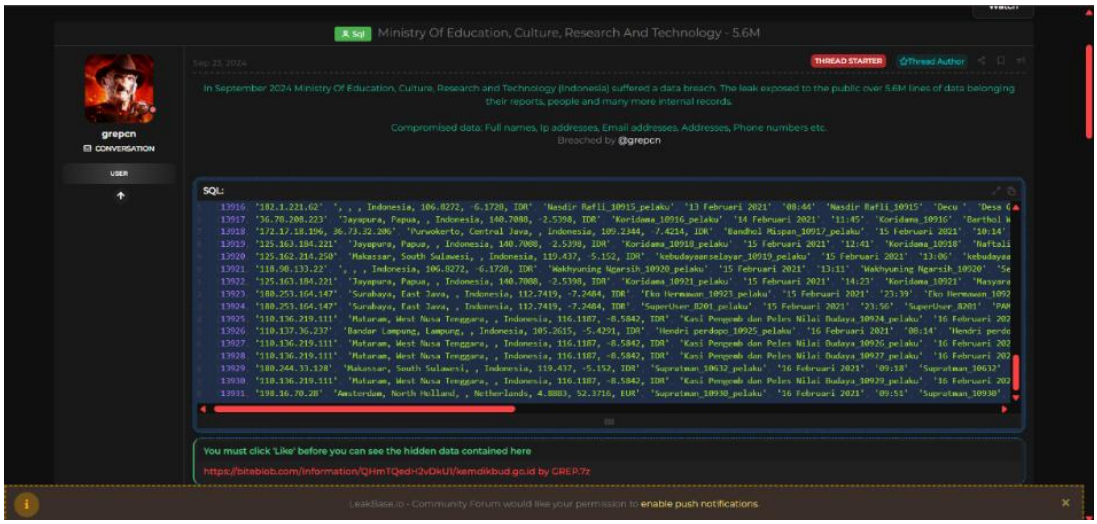
JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 254-269
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.400

3. HASIL DAN PEMBAHASAN

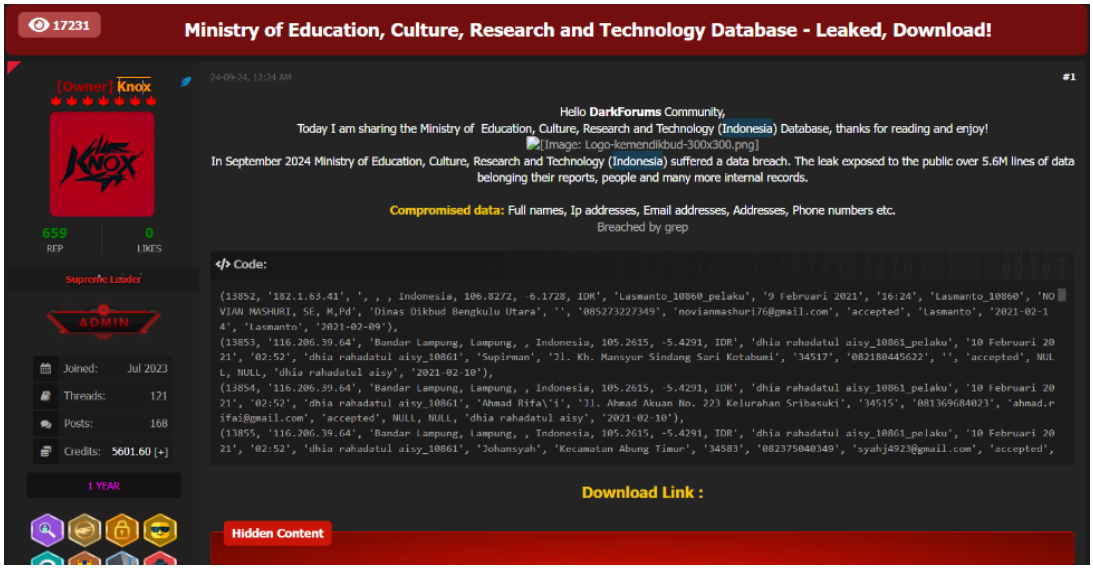
3.1 Deskripsi Umum Insiden dan Sumber Data

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.

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 3 Gambar Forum Penjualan *LeakBase* oleh grepcn



Gambar 4 Gambar Forum Penjualan *DarkForums* oleh Knox

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 254-269
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.400

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.

3.2 Analisis Struktur dan Pola Perdagangan Data

Proses investigasi dilakukan dengan mengikuti tahapan NIST SP 800-86, dimulai dari pengumpulan data (collection) secara pasif menggunakan Tor Browser. Data tersebut kemudian diperiksa dan diolah dengan Python untuk mempermudah analisis. Dari total 80 data sampel, ditemukan 65 nama valid, 34 IP address valid, dan 17 email valid. Data diperoleh dalam bentuk *preview* berbasis teks yang ditampilkan langsung di *thread* unggahan pelaku yang menggunakan nama akun seperti "@grepcn" dan "@Knox".

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. Hasil ataupun output dari kode program python tersebut berbentuk file .csv dan xlxs. Dari hasil *examination* data sampel yang telah dilakukan terdapat total 80 data pribadi yang bocor disampel tersebut diantaranya meliputi:

Tabel 3. 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 3, 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.

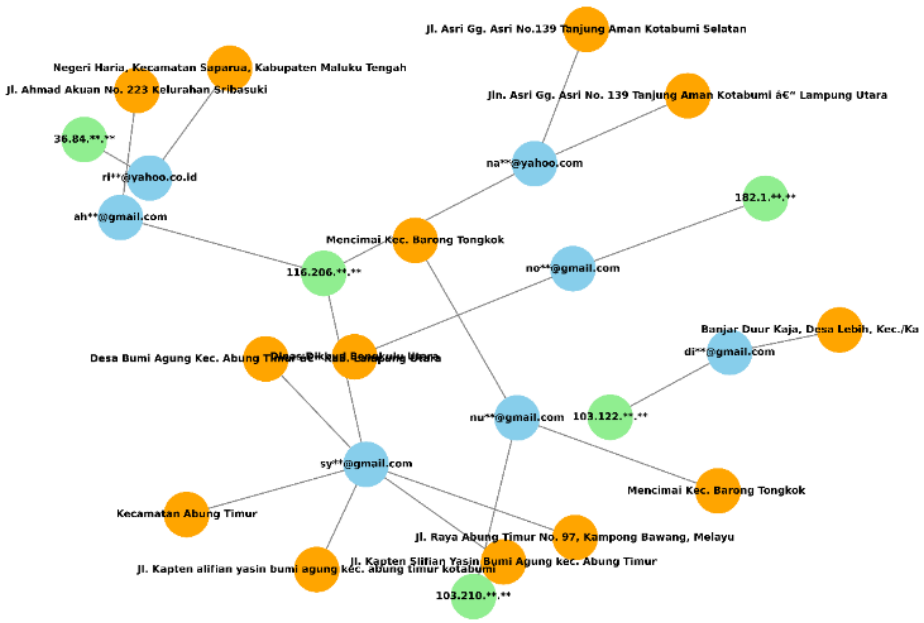
3.3 Validasi dan Temuan Utama

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.

3.3.1. 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.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 254-269
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.400



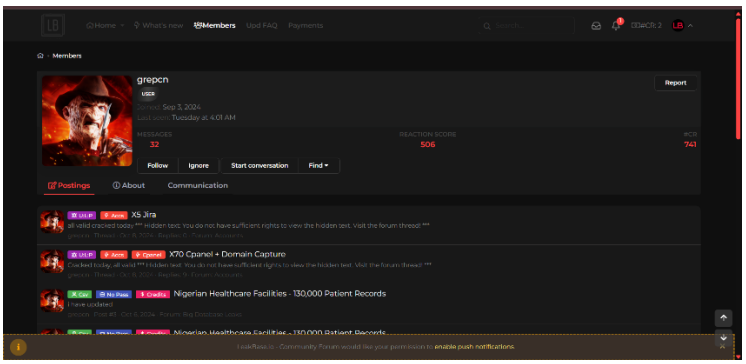
Gambar 5. Visualisasi Relasi dari 20 Data Sampel

Visualisasi graf menggunakan NetworkX menunjukkan hubungan yang kompleks antar entitas korban kebocoran data, dengan email dan alamat IP yang telah disamarkan demi menjaga privasi. Ditemukan bahwa beberapa alamat IP digunakan oleh lebih dari satu email, mengindikasikan akses dari jaringan bersama seperti sekolah atau kantor. Seluruh email menggunakan domain umum seperti @gmail.com, namun berdasarkan keterkaitan dengan entitas geografis, sebagian korban diduga berasal dari wilayah masyarakat umum seperti Kecamatan Abung Timur dan Desa Bumi Agung. Selain itu, terdapat akun email yang terhubung ke lebih dari satu instansi, yang mungkin menunjukkan peran administratif lintas lembaga. Hasil visualisasi ini memperkuat proses analisis dengan mengidentifikasi simpul pusat (central nodes), pola distribusi, dan jalur relasi antar korban secara menyeluruh.

3.3.2. 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. Profil Pelaku Utama

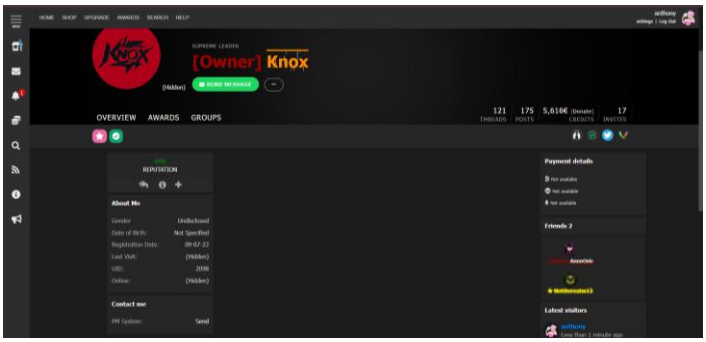
No	Deskripsi	Keterangan
1.	Gambar	

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 254-269
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.400

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

Pada tabel 4 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 5. Profil "Knox"

No	Deskripsi	Keterangan
1.	Gambar	
2.	*Forum*	DarkForums.st
3.	*Username*	knox
4.	*Level*	Owner
5.	Tanggal bergabung	9 Juli 2023
6.	Total Post	168
7.	*Threat*	121
8.	Reputasi	659

Pada tabel 5 dijelaskan bahwa akun dengan *username* "Knox" diduga sebagai *owner* dari forum DarkForums. Knox adalah aktor yang melakukan *re-upload* 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.

3.3.3 Analisis Pola Distribusi dan Penjualan

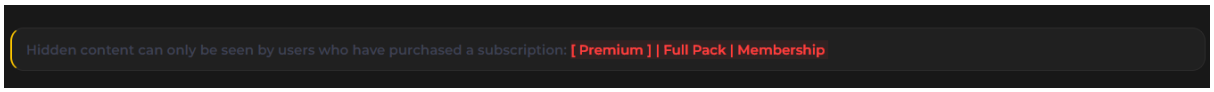
Pola perdagangan data yang ditemukan memiliki struktur dan strategi pemasaran yang menyerupai sistem *e-commerce* gelap. Berdasarkan observasi terhadap tiga aktor di atas, pola distribusi dapat diringkas sebagai berikut:

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 254-269
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.400

Tabel 6. Model Distribusi

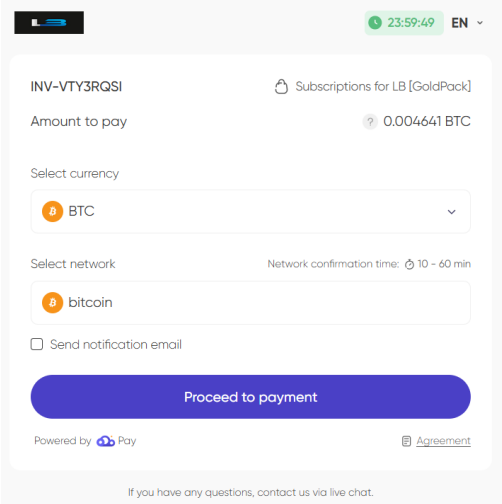
No	Tahap	Aktor	Peran
2.	*Leaker*	grepcn	Upload data kebocoran dengan data sampel.
3.	*Reuploader*	knox	Menyebarkan ulang ke forum lain dengan monetisasi langsung

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 3 sebagai temuan utama.



Gambar 6. *Hidden Content Leakbase*

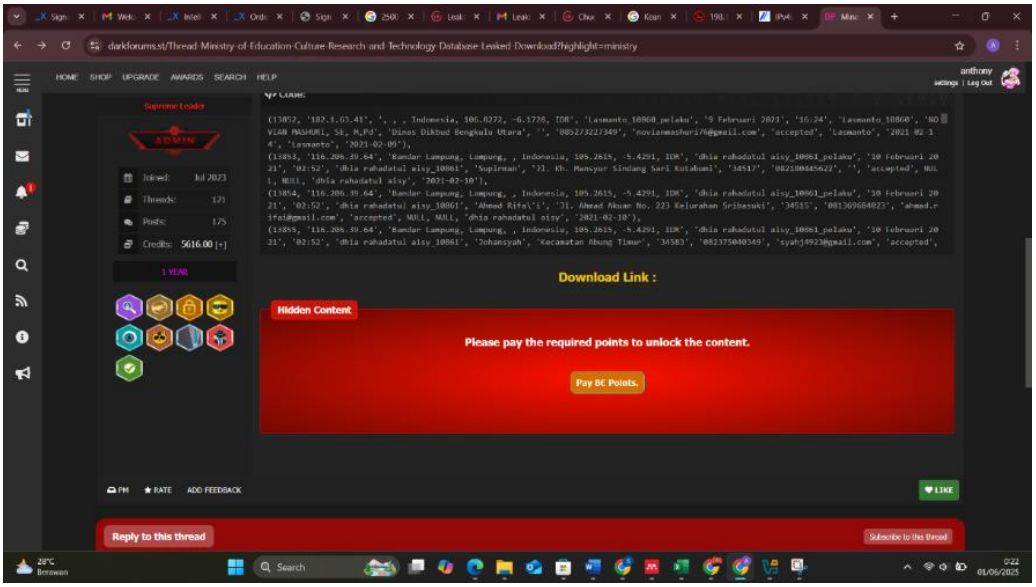
Setelah analisis mendalam, pada forum *Leakbase* juga terlihat bahwa ada beberapa unggahan dengan "*Hidden Content"* yang mengharuskan pengguna melakukan *upgrade subscription* membership. Untuk mendapatkan akses ke "*Hidden Content" user* harus membayar subcription yang beragam harga membershipnya. Untuk metode pembayaran menggunakan *cryptocurrency* seperti Bitcoin dan yang lainnya seperti pada gambar dibawah ini.



Gambar 7. Metode Pembayaran

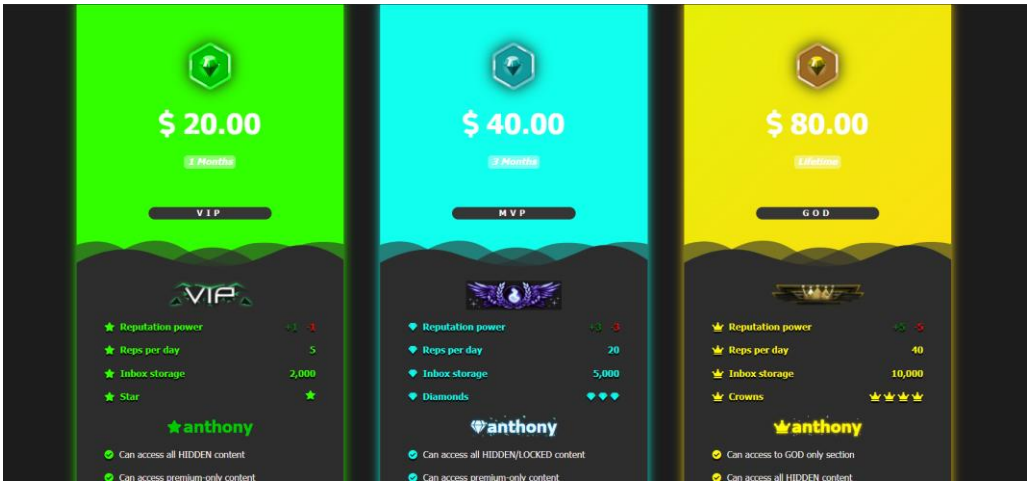
Setelah data kebocoran Kemdikbud 2024 pertama kali diunggah oleh akun grepcn di forum *LeakBase*, muncul kembali distribusi ulang dari file yang sama di platform berbeda, yakni *DarkForums*, oleh akun bernama Knox. Aksi reupload ini menunjukkan adanya rantai distribusi lintas-forum, yang sering terjadi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

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 254-269
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.400



Gambar 8. Pola perdagangan oleh Knox

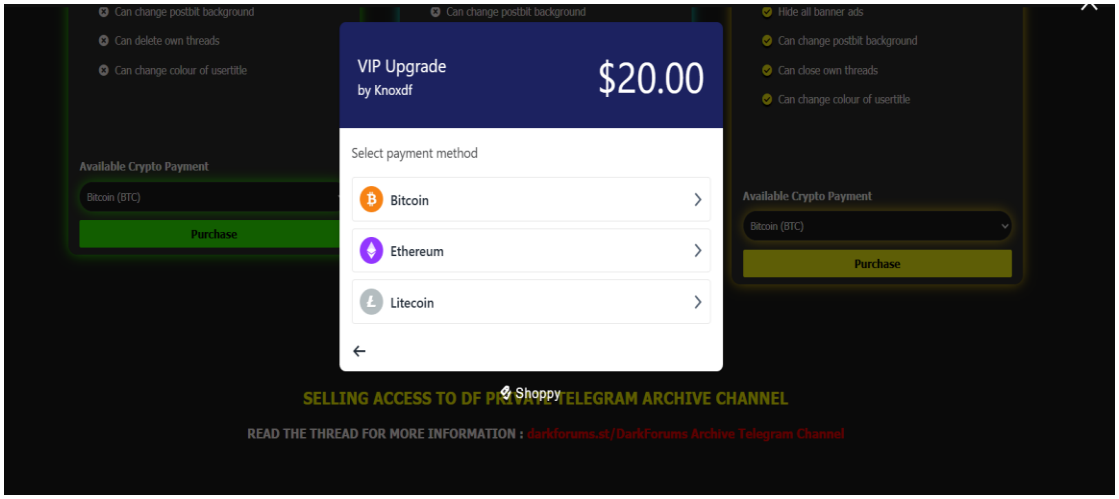
Terlihat pada gambar 8 berbeda dari grepcn yang langsung memberikan akses melalui *link* biteblob.com, Knox menyematkan file unduhan di balik sistem "*Hidden Content*" yang hanya bisa dibuka setelah melakukan pembayaran (dibanderol seharga €9). *Link* langsung disembunyikan, tidak tersedia untuk *user* publik atau tidak terverifikasi.



Gambar 9. *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 10 dibawah ini.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 254-269
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.400



Gambar 10. Metode pembayaran DarkForums

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

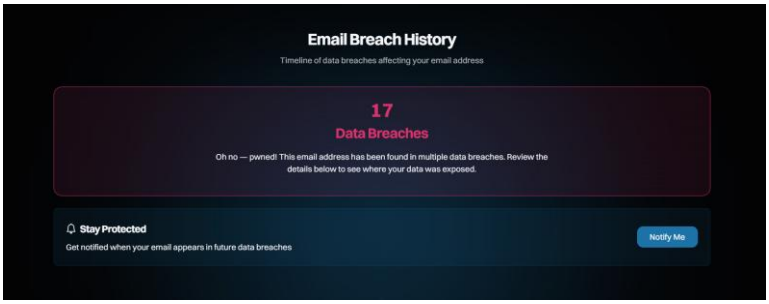
Tabel **7.** Hasil pengujian dengan HIBP dan IntelX

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

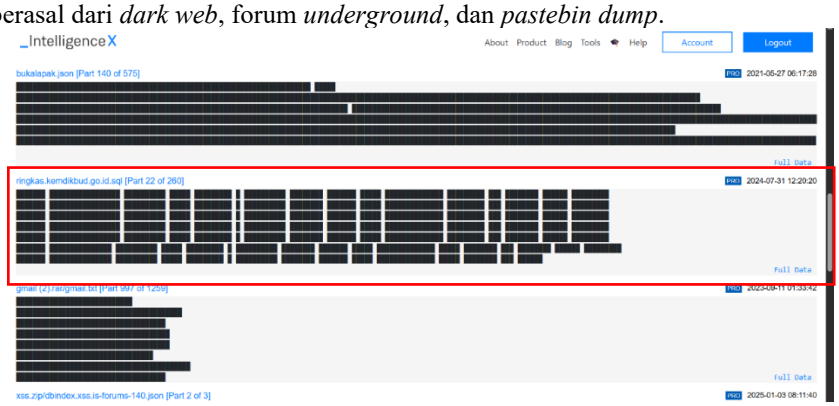
a. HIBP hanya mendeteksi 5 dari 17 email (±29%) sebagai bagian dari breach yang pernah terjadi.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 254-269
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.400



Gambar 11 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 12 Hasil deteksi menggunakan IntelX

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 11 terdapat 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 12 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.

3.4 Evaluasi Metodologi dan Implikasi

Selanjutnya, validasi dilakukan dengan dua tools OSINT: **HaveIBeenPwned** dan **IntelX**. Hasilnya, IntelX mampu mendeteksi semua email (100%) sebagai bagian dari insiden kebocoran, sedangkan HIBP hanya mendeteksi 5 email (29%). Hal ini menunjukkan bahwa data yang diperoleh memang benar-benar bocor dan sesuai dengan insiden Kemendikbudristek 2024.

Dari hasil observasi, ditemukan bahwa forum-forum ini menggunakan sistem hidden content dan mata uang kripto untuk mengakses file, layaknya sistem e-commerce gelap. File yang diunggah *grepcn* dapat diakses secara gratis melalui link eksternal, namun pada versi *knox*, file disembunyikan dan hanya bisa dibuka setelah membayar. Situs tempat file diunggah, yaitu *biteblob.com*, juga terdeteksi sebagai berbahaya oleh VirusTotal.

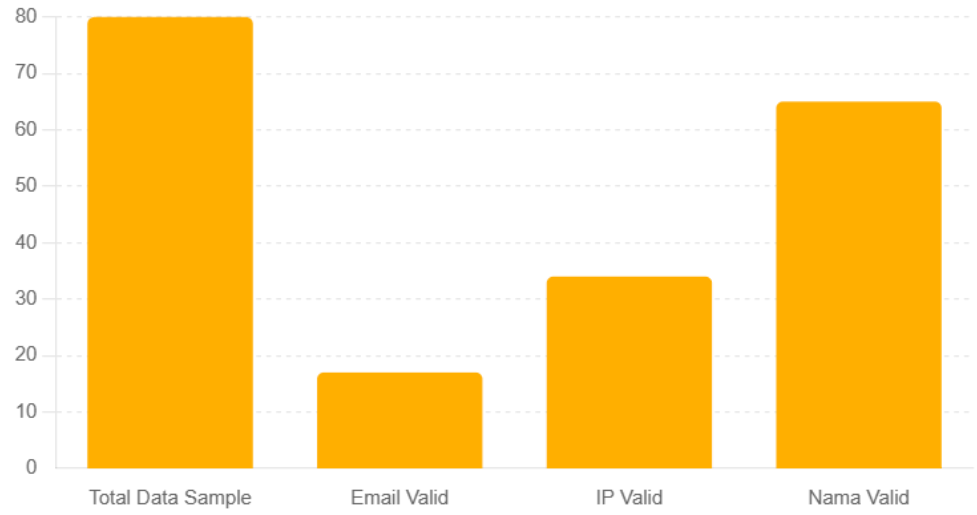
Berikut adalah format pelaporan akhir dari hasil investigasi forensik digital terhadap kasus perdagangan data pribadi yang diduga berasal dari sistem internal Kemdikbudristek dan diperjualbelikan di forum *Leakbase* dan *DarkForums*. Penyajian ini disusun berdasarkan kerangka NIST SP 800-86 dan *Threat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

Tabel 8. 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)*

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 254-269
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.400

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 13. Visualisasi Jumlah Data yang terverifikasi

Pada Gambar 13 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 9. 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*)

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 254-269
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.400

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 10. 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.

Berdasarkan hasil evaluasi yang disusun menggunakan kerangka kerja NIST SP 800-86 dan Threat Intelligence Lifecycle, dapat disimpulkan bahwa metode dan tools yang digunakan dalam penelitian ini terbukti mampu menghasilkan temuan yang akurat, relevan, dan aman. Validasi terhadap data sampel yang diperoleh dari forum LeakBase dan DarkForums menunjukkan tingkat keberhasilan yang signifikan, dengan lebih dari 80 entri data berhasil diverifikasi, serta dukungan dari platform OSINT seperti IntelX (100%) dan HaveIBeenPwned (29%). Hasil ini memperkuat bahwa pendekatan berbasis OSINT dan Threat Intelligence efektif dalam mengungkap jejak digital perdagangan data pribadi.

Selain itu, analisis mendalam terhadap pola kebocoran data, aktor pelaku, dan struktur distribusi data mengindikasikan adanya potensi kuat bahwa kebocoran berasal dari akses internal yang tidak terproteksi secara optimal. Prediksi penyebab kebocoran menunjuk pada kelemahan dalam enkripsi database, lemahnya pengawasan kredensial admin, serta tidak adanya sistem monitoring kebocoran data secara real-time.

Dalam konteks mitigasi, penelitian ini juga menyusun solusi berdasarkan pendekatan Fishbone Diagram yang mengidentifikasi faktor-faktor risiko dari sisi manusia, mesin, metode, dan lingkungan. Rekomendasi seperti implementasi field-level encryption, penerapan audit log dan honeytoken, serta integrasi platform Threat Intelligence menjadi langkah penting dalam membangun sistem pertahanan yang responsif dan berlapis.

Secara keseluruhan, proses investigasi telah dilakukan sesuai dengan prinsip-prinsip forensik digital yang menjunjung integritas data, transparansi proses, serta kepatuhan terhadap aspek etika dan hukum. Hasil ini diharapkan dapat memberikan kontribusi nyata bagi penguatan kebijakan perlindungan data pribadi dan strategi keamanan siber nasional di masa mendatang.

Tabel 11. Tabel Hasil Perbandingan

No	Penulis (Tahun)	Judul Penelitian	Fokus Penelitian	Metode yang Digunakan	Kelebihan	Kelemahan

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 254-269
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.400

1	Nugranto & Koprawi (2023) [9]	Investigasi Kejahatan Siber pada Surface Web dan Deep Web Menggunakan Metode NIST	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) [8]	Evolution of Dark Web Threat Analysis and Detection	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) [14]	Investigasi Kebocoran Data Menggunakan OSINT dan DML	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) [15]	Navigating the Shadows	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) [16]	OSINT on the Dark Web: Child Abuse Material Investigations	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)	Analisis Forensik Digital terhadap Perdagangan Data Pribadi di Dark Web Menggunakan OSINT & Threat Intelligence	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

4. KESIMPULAN

Hasil penelitian menunjukkan bahwa pendekatan forensik digital berbasis NIST SP 800-86 yang dikombinasikan dengan siklus Threat Intelligence, serta didukung oleh tools OSINT seperti IntelX dan HIBP, terbukti efektif dalam mengungkap praktik perdagangan data pribadi di Dark Web.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. Studi kasus pada insiden kebocoran data Kemendikbudristek 2024 mengungkap bahwa seluruh sampel email yang dianalisis valid, dengan struktur data rapi dalam format SQL dump. Proses investigasi juga berhasil memetakan identitas pelaku, termasuk akun seperti "grepcn" dan "Knox", serta memverifikasi aktivitas perdagangan lintas forum yang menyerupai sistem e-commerce tersembunyi. Penerapan gabungan antara NIST dan Threat Intelligence Lifecycle memungkinkan alur investigasi yang menyeluruh, mulai dari identifikasi insiden hingga pelaporan hasil. Pola kebocoran mengindikasikan adanya kelemahan sistem internal, seperti tidak adanya enkripsi, lemahnya deteksi kebocoran, dan potensi ancaman dari dalam (insider threat). Dengan demikian, pendekatan ini tidak hanya dapat

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 254-269
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.400

direplikasi untuk kasus serupa, tetapi juga menjadi acuan bagi penguatan sistem keamanan siber instansi pemerintah di masa depan.

REFERENCES

[1] K. R. Anggen Suari and I. M. Sarjana, "Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia," *Jurnal Analisis Hukum*, vol. 6, no. 1, pp. 132–142, Apr. 2023, doi: 10.38043/jah.v6i1.4484.

[2] IBM, "83% of organizations reported insider attacks in 2024." Accessed: Apr. 22, 2025. [Online]. Available: https://www.ibm.com/think/insights/83-percent-organizations-reported-insider-threats-2024

[3] R. Reddy Gopireddy, "Dark Web Monitoring: Extracting and Analyzing Threat Intelligence," *International Journal of Science and Research (IJSR)*, vol. 9, no. 3, pp. 1693–1696, Mar. 2020, doi: 10.21275/SR24801072234.

[4] Rachmatunnisa, "Rangkuman Serangan Siber 2024 CISSReC: Darurat Judi Online hingga PDNS Lumpuh." Accessed: Mar. 05, 2025. [Online]. Available: https://inet.detik.com/security/d-7711614/rangkuman-serangan-siber-2024-cissrec-darurat-judi-online-hingga-pdns-lumpuh?form=MG0AV3

[5] T. Dokman and T. Ivanjko, "Open Source Intelligence (OSINT): issues and trends," in *INFuture2019: Knowledge in the Digital Age*, Faculty of Humanities and Social Sciences, University of Zagreb Department of Information and Communication Sciences, FF press, 2020. doi: 10.17234/infuture.2019.23.

[6] D. Van Puyvelde and F. T. Rienzi, "The rise of open-source intelligence," *European Journal of International Security*, 2025, doi: 10.1017/eis.2024.61.

[7] A. M. Aljuhami and D. M. Bamasoud, "Cyber Threat Intelligence in Risk Management A Survey of the Impact of Cyber Threat Intelligence on Saudi Higher Education Risk Management," 2021. [Online]. Available: www.ijacsa.thesai.org

[8] S. Nazah, S. Huda, J. Abawajy, and M. M. Hassan, "Evolution of dark web threat analysis and detection: A systematic approach," *IEEE Access*, vol. 8, pp. 171796–171819, 2020, doi: 10.1109/ACCESS.2020.3024198.

[9] H. F. Nugranto and M. Koprawi, "Investigasi Kejahatan Siber pada Surface Web dan Deep Web Menggunakan Metode NIST," *Julyxxxx*, vol. x, No.x, pp. 1–5, Mar. 2024, doi: https://doi.org/10.35957/jatisi.v11i1.3245.

[10] N. Lavinia and Puspitasari, "URGENSI PEMANFAATAN OPEN SOURCE INTELLIGENT (OSINT) DALAM UPAYA PENCEGAHAN AKSI TERORISME DI INDONESIA," *Jurnal Sosial Humaniora Terapan*, vol. 6, no. 1, Dec. 2023, doi: 10.7454/jsht.v6i1.1105.

[11] R. Hukom and M. H. Setiadi, "Pengaruh Media Sosial terhadap Pola Kejahatan di Era Digital: Studi Kriminologi dengan Pendekatan Netnografi," *Perkara : Jurnal Ilmu Hukum dan Politik*, vol. 3, no. 1, pp. 750–768, Mar. 2025, doi: 10.51903/perkara.v3i1.2353.

[12] M. Alshaikh, "Developing cybersecurity culture to influence employee behavior: A practice perspective," *Comput Secur*, vol. 98, Nov. 2020, doi: 10.1016/j.cose.2020.102003.

[13] M. Ring, D. Schlör, S. Wunderlich, D. Landes, and A. Hotho, "Malware detection on windows audit logs using LSTMs," *Comput Secur*, vol. 109, Oct. 2021, doi: 10.1016/j.cose.2021.102389.

[14] D. Risman Saputra and A. Arizal, "Investigasi Insiden Kebocoran Data Menggunakan Integrasi Melalui Pendekatan Open Source Intelligence dan Detection Maturity Level Model," Dec. 2023.

[15] P. Kuhn, K. Wittorf, and C. Reuter, "Navigating the Shadows: Manual and Semi-Automated Evaluation of the Dark Web for Cyber Threat Intelligence," *IEEE Access*, vol. 12, pp. 118903–118922, 2024, doi: 10.1109/ACCESS.2024.3448247.

[16] J. Rajamäki, "OSINT on the Dark Web: Child Abuse Material Investigations," *Information & Security: An International Journal*, vol. 53, pp. 21–32, 2022, doi: 10.11610/isij.5302.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER

p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 254-269
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.400