JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 3, September 2025, Pp. 2355-2365

ANALISIS PENILAIAN METRIK *ANONYMITY* DAN *PRIVACY* PADA KODACHI LINUX

Irvan Sihaloho*[1)], Adityas Widjajarto[2)], M. Teguh Kurniawan[3)]
1. Telkom University, Indonesia
2. Telkom University, Indonesia
3. Telkom University, Indonesia

Article Info
Kata Kunci: Kodachi Linux, *Anonymity*, *Privacy*, TOR, VPN

Keywords: KodachiLinux, *Anonymity*, *Privacy*, TOR, VPN

Article history:
Received 15 August 2024
Revised 6 September 2024
Accepted 2 October 2024
Available online 1 September 2025

DOI :
https://doi.org/10.29100/jipi.v10i3.6437

* Corresponding author.
Irvan Sihaloho
E-mail address:
irvanloho@student.telkomuniversity.ac.id

ABSTRAK
Penelitian ini berfokus pada penerapan profil dan analisis *anonymity* dan *privacy* dalam sistem operasi Kodachi Linux pada penerapan teknologi seperti TOR dan VPN untuk menjaga kerahasiaan identitas. Metodologi penelitian ini meliputi *profiling* dan analisis dari berbagai skenario berdasarkan kondisi *anonymity* dan *privacy* yang diaktifkan pada aspek jaringan, aplikasi, dan *storage*. Hasil menunjukkan Kodachi Linux menyediakan perlindungan yang signifikan untuk *anonymity* dan *privacy*, dengan nilai tertinggi sebesar 5 pada layanan jaringan yang memenuhi kelima metrik, tetapi saat fitur *anonymity* dan *privacy* diaktifkan terjadi penggunaan RAM sebesar 40%. Aplikasi yang menempati peringkat teratas termasuk Speeekchat, Pidgin *Internet* , Onion Share, Kodachi Ghacks Browser: TOR, Kodachi Loaded Browser: TOR, Kodachi Browser with Proxychains: TOR, dan TOR Browser, Veracrypt, dan Zulucrypt, memiliki *score* tertinggi sebesar 5 memenuhi kelima metrik. *Score* tertinggi dalam layanan *storage* terdapat pada Nuke System dan *non-persistent* yang mewujudkan fungsi *anonymity* dan *privacy* dengan *score* 5 dari kelima klasifikasi metrik. Kesimpulan penelitian Kodachi Linux mencapai fungsi *anonymity* dan *privacy* dalam layanan jaringan, aplikasi, dan *storage*, tetapi menjadi batasan dalam penggunaan RAM untuk layanan jaringan dan pilihan aplikasi yang terbatas untuk fungsi *anonymity* dan *privacy*. Enkripsi keamanan data dan Nuke System kurang fleksibel dalam manajemen data.

ABSTRACT
This research focuses on the application of *anonymity* and *privacy profiling* and analysis in the Kodachi Linux operating system on the application of technologies such as TOR and VPN to maintain confidentiality of identity. The research methodology included field testing and data analysis in various system usage scenarios, depicted in Data Flow Diagrams based on *anonymity* and *privacy* conditions enabled based on service profile aspects such as *network*, application, and *storage*. The results show that Kodachi Linux provides a significant layer of protection for *anonymity* and *privacy*, with the highest *score* of 5 on *network* services meeting all metrics, but facing limitations when *anonymity* and *privacy* features are enabled with 40% RAM usage. Top ranked apps include Speeekchat, Pidgin *Internet*, Onion Share, Kodachi Ghacks Browser: TOR, Kodachi Loaded Browser: TOR, Kodachi Browser with Proxychains: TOR, and TOR Browser, Veracrypt, and Zulucrypt, had the highest *score* of 5 meeting all metrics. The highest *score* in *storage* services is in Nuke System and *non-persistent* which realize the function of *anonymity* and *privacy* with a *score* of 5 from all five metric classifications. In conclusion, Kodachi Linux achieves *anonymity* and *privacy* functions in *network*, application, and *storage* services, but is limited in RAM usage for *network* services and limited application choices for *anonymity* and *privacy* functions. Data security *encryption* and Nuke System lack flexibility in data management.

.

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 3, September 2025, Pp. 2355-2365

I. PENDAHULUAN

KEAMANAN siber berperan bagi individu dan organisasi yang menjaga dan melindungi kerahasiaan (*Confidential*), integritas (*Integrity*), dan ketersediaan (*Availability*) [1] . *Anonymity* dan *privacy* menjadi terancam karena kurangnya penerapan teknologi yang tepat [2]. Pengguna yang peduli terhadap *privacy* terbatas oleh pengawasan dan pelacakan *internet* yang digunakan oleh perusahaan atau penyedia layanan *Internet* [1]. *Anonymity* dan *privacy* memiliki peranan penting dalam meningkatkan keamanan *privacy* pada era digitalisasi. *Anonymity* bertujuan untuk melindungi informasi identitas pengguna seperti nama asli, lokasi, dan *IP address (Internet Protocol)* [3]. *Privacy* untuk memastikan tidak ada tindakan kejahatan mengumpulkan atau menyimpan informasi pribadi, tanpa sepengetahuan pengguna [4]. Sistem teknologi informasi merupakan infrastruktur yang mencakup *hardware*, *software*, data, dan jaringan yang digunakan pada proses komunikasi informasi. Perlindungan sistem teknologi informasi penting, karena sebagai dasar operasi pada organisasi atau perusahaan. Masalah yang dihadapi adalah kurangnya penerapan keamanan pada sistem operasi yang secara khusus dirancang untuk melindungi *anonymity* dan *privacy*. Oleh sebab itu, keamanan *privacy* diperlukan fungsi sistem operasi yang mendukung *anonymity* dan *privacy*. Salah satu fungsi penerapan *anonymity* dan *privacy* adalah Kodachi Linux.
Kodachi Linux merupakan sistem operasi yang dirancang dengan kemudahan beroperasi dengan menggunakan *Virtual Machine*, USB, atau DVD [5]. Salah satu fungsi Kodachi yaitu dapat merahasiakan identitas menggunakan teknologi anonim seperti TOR (*The Onion Router*) *network* dan VPN (*Virtual Private Network*) yang mendukung *anonymity* dan *privacy*.

Penelitian ini berfokus pada analisis efektivitas Kodachi Linux dalam mewujudkan fungsi *anonymity* dan pengguna, dengan penekanan pada aspek perlindungan data dalam layanan jaringan, aplikasi, dan *storage*. Dengan fokus pada Kodachi Linux, penelitian ini akan menguji dan menganalisis fitur-fitur dan aspek sistem operasi seperti jaringan, aplikasi dan *storage* dalam mewujudkan fungsi *anonymity* dan *privacy*. Penelitian ini akan memberikan panduan komprehensif mengenai bagaimana sistem operasi mendukung *anonymity* dan *privacy*, dengan fokus utama pada Kodachi Linux. Fitur-fitur yang ada akan diuji dan dianalisis berdasarkan standar klasifikasi seperti K-*anonymity* dan *Entropy Anonymity Degree (EAD)* untuk mengukur sejauh mana sistem operasi ini mendukung kedua fungsi tersebut. [6]. Melalui pengujian dan *profiling* fitur *anonymity* dan *privacy*, penelitian ini bertujuan untuk memberikan dokumentasi yang sistematis terkait hasil analisis fungsi *anonymity* dan *privacy*. Data yang dikumpulkan akan diolah menjadi diagram aliran data *Data Flow Diagram* (DFD), yang menjelaskan alur data selama proses *profiling*. Analisis lebih lanjut akan dilakukan untuk menentukan metrik-metrik yang terkait untuk mengukur fungsi *anonymity* dan *privacy*, yang dapat digunakan sebagai indikator keberhasilan implementasi fitur-fitur tersebut pada sistem operasi.

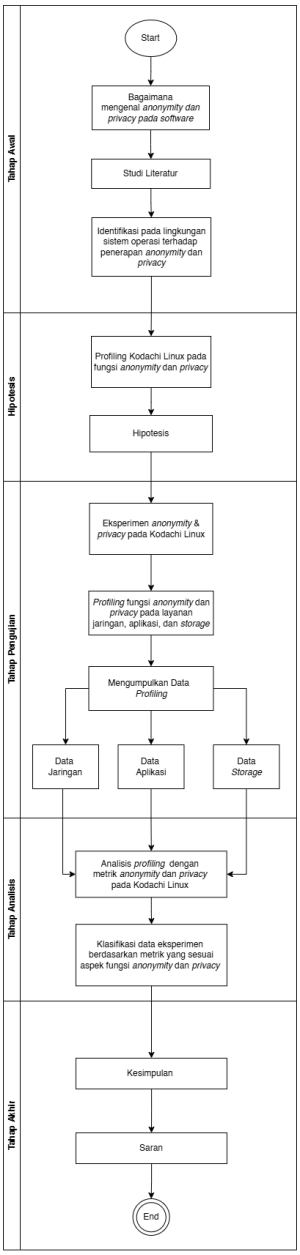
Penelitian implementasi dari fungsi *anonymity* dan *privacy* pada sistem operasi terhadap pengujian *profiling* untuk dianalisis menjadi hasil akhir berupa dokumentasi *profiling* dan pengumpulan data yang diklasifikasi untuk menentukan metrik-metrik yang mewujudkan fungsi *anonymity* dan *privacy* pada aspek layanan sistem operasi. Pengujian *profiling* dilakukan pada aspek layanan jaringan, aplikasi, dan *storage* dengan berdasarkan dua kondisi yaitu pada saat fitur *anonymity* dan *privacy* diaktifkan dan maupun tidak. Pada analisis, dilakukan klasifikasi hasil data *profiling* berdasarkan metrik-metrik yang dirumuskan sesuai fungsi *anonymity* dan *privacy* yang diwujudkan.

Kontribusi utama penelitian ini adalah memberikan wawasan mengenai efektivitas sistem operasi, khususnya Kodachi Linux dalam melindungi *anonymity* dan *privacy* dalam bidang keamanan siber tentang implementasi efektif dari teknologi anonim dalam melindungi *privacy* pengguna di lingkungan digital dan lingkup sistem operasi.

II. METODE PENELITIAN

Sistematika penyelesaian masalah pada tahapan penelitian berguna untuk memecahkan masalah yang dirumuskan adalah penyelesaian masalah secara sistematika. Sebelum eksperimen *profiling* pada Kodachi Linux, implementasi *profiling*, dan analisis metrik *anonymity* dan *privacy*, dibentuk mekanisme penyelesaian masalah. Penelitian ini terdapat kerangka lima tahapan untuk menyelesaikan masalah yaitu: tahap awal, hipotesis, tahap pengujian, tahap analisis, dan tahap akhir terdapat pada Gambar. 1 Sistematika Penyelesaian Masalah.

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 3, September 2025, Pp. 2355-2365



Gambar. 1 Sistematika Penyelesaian Masalah

1. Tahap Awal

Tahap awal penelitian dimulai dengan melakukan identifikasi bagaimana tahapan implementasi *profiling anonymity* dan *privacy* pada Kodachi Linux sebagai objek. Kodachi Linux dipilih sebagai objek penelitian karena karakteristik uniknya yang dirancang untuk mendukung *anonymity* dan *privacy*. Sistem operasi ini mengintegrasikan teknologi keamanan seperti TOR dan VPN untuk memastikan penjelajahan internet yang anonim dan perlindungan data pribadi. Kodachi Linux juga menyediakan antarmuka ramah pengguna, dapat dijalankan dari media portabel seperti USB, serta dilengkapi dengan layanan aplikasi dan *storage* yang dirancang khusus untuk keamanan *anonymity* dan *privacy*. Aplikasi enkripsi, manajemen kata sandi, dan penyimpanan terenkripsi memastikan data tetap aman dari akses tidak sah, menjadikan Kodachi Linux relevan sebagai objek penelitian dalam konteks perlindungan *privacy* dan keamanan data. Kemudian, studi literatur dilakukan untuk memastikan bahwa masalah penelitian ini memiliki kesesuaian dan memungkinkan dilakukan dengan memperdalam teori mengenai tahapan implementasi *profiling* pada Kodachi Linux. Dari tahapan implementasi *profiling* dilaksanakan identifikasi pada lingkungan sistem operasi terhadap penerapan *anonymity* dan *privacy*.

2. Tahap Hipotesis

Tahapan hipotesis sebagai rancangan untuk menghasilkan acuan kemungkinan terhadap hipotesis yang berkaitan dengan hubungan antara karakter Kodachi Linux dengan *profiling anonymity* dan *privacy*. Pada tahapan ini dilakukan *profiling* Kodachi Linux terhadap fungsi *anonymity* dan *privacy*.

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 3, September 2025, Pp. 2355-2365

3. Tahap Pengujian

Pada tahapan ini akan dilakukan eksperimen *anonymity* dan *privacy* pada Kodachi Linux dengan pengujian *profiling* pada layanan jaringan, aplikasi, dan *storage.* Selanjutnya hasil data *profiling* mengumpulkan data *profiling* berdasarkan fungsi *anonymity* dan *privacy* terwujud dengan data yang dihasilkan antara lain:

1) Data hasil *profiling* jaringan
2) Data hasil *profiling* aplikasi
3) Data hasil *storage profiling*

Pada pengujian dilakukan berdasarkan beberapa variabel yang dikendalikan dalam penelitian in termasuk faktor eksternal seperti kondisi jaringan, perangkat keras yang digunakan, dan lingkungan pengujian, bertujuan untuk memastikan bahwa tidak ada faktor lain yang mempengaruhi hasil *profiling*. Dalam konteks penelitian ini, pengendalian variabel dilakukan dengan memastikan bahwa semua pengujian dilakukan dalam kondisi yang berupa konfigurasi sistem yang serupa,kondisi jaringan pengaturan fitur on-off dan pengujian yang dilakukan secara berskala, yang menggunakan konfigurasi jaringan yang konsisten seperti kombinasi VPN, TOR, DNSCrypt, dan TORDNS, serta *hardware* yang sama selama pengujian. Selain itu, pengujian dilakukan dengan memperhitungkan skenario di mana fitur *anonymity* dan *privacy* diaktifkan dan dinonaktifkan, sehingga perbandingan hasil dapat dilakukan secara valid dan reliabel. Selain itu pengendalian variabel tersebut diterapkan pada layanan aplikasi dan *storage*, yaitu untuk layanan aplikasi seperti *chatting, sharing file*, dan *browser* pengujian dilakukan dengan skenario fitur *anonymity* dan *privacy* diaktifkan dan dinonaktifkan, kemudian aplikasi *encryption*, faktor-faktor seperti versi perangkat lunak, konfigurasi awal, dan metode penggunaan harus distandarkan variabel yang mempengaruhi hasil pengujian. Demikian pula, untuk layanan *storage*, variabel seperti jenis media penyimpanan, metode enkripsi yang digunakan, dan kapasitas penyimpanan. Pengendalian ini memastikan bahwa hasil penelitian secara akurat mencerminkan keandalan dan keamanan layanan jaringan, aplikasi, dan *storage.* Kodachi Linux tanpa dipengaruhi oleh faktor eksternal yang tidak terkait dengan sistem operasinya. Setelah hasil pada kondisi *anonymity* dan *privacy* diketahui maka dilanjutkan pada tahapan analisis.

4. Tahap Analisis

Pada tahap ini akan dilakukan analisis *profiling* dengan metrik *anonymity* dan *privacy* yang ditentukan berdasarkan hasil data *profiling* [6]. Hasil analisis ini akan menunjukkan karakteristik Kodachi Linux pada metrik yang berkaitan dengan *anonymity* dan *privacy* [7]. Selanjutnya, akan dilakukan klasifikasi data akan berdasarkan metrik sesuai fungi *anonymity* dan *privacy*. Metrik yang digunakan pada tahap analisis berdasarkan layanan jaringan, aplikasi, dan *storage* pada Tabel. 1 Metrik penelitian.

TABEL. I
METRIK PENELITIAN

Layanan	Metrik	Fungsi	Referensi
Jaringan	Usability TOR	Digunakan untuk menyamarkan identitas atau lokasi sebenarnya pada sistem operasi	[8]
	IP Address masking	Menunjukkan kejadian penyamaran identitas pada *IP Address* yang terhubung pada perangkat	[9]
	Security privacy	Mengacu pada implementasi keamanan dari VPN dan akses pihak ketiga.	[10]
	Encryption Compability	Kemampuan dalam menerapkan berbagai algoritma dan protokol enkripsi	[11]
	Leak Shield	Kemampuan untuk melindungi data dari kebocoran informasi sensitif.	[12]
Aplikasi *Chatting* Aplikasi *Sharing File* Aplikasi *Browser*	*Usability* TOR	Berfungsi pada kemampuan aplikasi dapat terhubung pada TOR *network*.	[13]
	Peering communication	Kemampuan aplikasi yang berkomunikasi pada jaringan yang sama, sehingga membatasi kebocoran komunikasi.	[14]
	Disguising Identity	Kemampuan menyembunyikan identitas tanpa membutuhkan identitas yang spesifik pada membuat akun	[15]
	External Tracking	Kemampuan mendukung penerapan komunikasi tanpa pelacakan hak yang tidak sah.	[8]
	Data Scrubbing	kemampuan aplikasi yang menghapus jejak komunikasi.	[16]
Aplikasi *Encryption*	*Encryption Compablity*	Kemampuan melakukan *encryption* pada Disk atau volume dengan algoritma *encryption*	[17]
	Key management	Mendukung penguncian otomatis volume	[10]
	Plausible Deniability	Kemampuan volume tersembunyi keberadaan data terenkripsi.	[18]
	Secure erase	Proses menghapus data dari perangkat penyimpanan tanpa dapat dipulihkan	[11]
	Auto lock	Kemampuan mengunci akses pada sistem atau volume terenkripsi	[17]
Storage	*Encryption Compability*	Kemampuan melakukan *encryption* pada Disk atau volume dengan algoritma *encryption*	[19]
	Access Control	Mengukur efektivitas sistem dalam membatasi akses ke sumber daya hanya untuk pengguna	[20]

Plausible Deniability	Kemampuan sistem untuk menyembunyikan eksistensi data atau komunikasi	[18]
Secure Erase	Proses menghapus data dari perangkat penyimpanan tanpa dapat dipulihkan	[11]
Privacy Policy	Kemampuan mengevaluasi efektivitas dan tingkat perlindungan *privacy* data.	[21]

5. Tahap Akhir

Tahap ini adalah tahap terakhir dari penelitian dengan kesimpulan terkait *profiling* yang menghasilkan data akhir untuk analisis mengenai karakter Kodachi Linux berdasarkan metrik *anonymity* dan *privacy* pada layanan jaringan, aplikasi, dan *storage* kemudian pemberian saran akan dituliskan pada laporan hasil penelitian.

III. HASIL DAN PEMBAHASAN

A. *Rancangan Sistem*

Pada penelitian ini dilakukan rancangan dalam implementasi *profiling* dengan melibatkan instrumen penelitian berupa *Hardware* dan *Software*. Pengujian yang akan dirancang berdasarkan aspek aplikasi, jaringan, dan *storage* pada sistem operasi.

TABEL. II
SPESIFIKASI *HARDWARE*

Komponen	Informasi	Komponen
Spesifikasi Main OS	*Processor*	AMD Ryzen 5 4500U with Radeon Graphics
	Memory	8192 MB RAM
	Hard Disk	477 GB SSD
	System type	64-bit
	Operating System	Windows 11 Home Single Langueage 64-bit

TABEL. III
SPESIFIKASI *CORE SOFTWARE*

Komponen	Informasi	Komponen
Spesifikasi *Core Software*	*Virtual Machine*	Vmware Workstation – version 16.2.5
	Operating System	Kodachi Linux-8.27-64-kernel-6.2
	Memory	2048 MB RAM
	System type	64 bit
	Processor	64-bit x 86-64

Pada Tabel. 3 Spesifikasi *Core Software* menunjukkan terkait informasi spesifikasi *Software* yang digunakan yaitu *Virtual Machine*, dan *Operating System*. Kedua *software* tersebut digunakan sebagai instrumen pengujian *anonymity* dan *privacy*. Berikut rincian spesifikasi *software*:

1) *Virtual Machine*

Pada pengujian ini menggunakan Vmware Workstation yang berperan sebagai *software* virtual untuk menjalankan sistem operasi secara bersamaan pada satu *device*. Oleh sebab itu, Vmware Workstation pada penelitian ini berfungsi untuk instalasi dan menjalakan Kodachi Linux.

2) *Operating* System

Kodachi Linux merupakan sistem operasi yang mendukung teknologi *privacy* dan *anonymity*. Kodachi Linux sebagai objek pengujian yang berkaitan dengan tujuan penelitian ini. Dalam pengujian ini, dilakukan *profiling* pada tipe sistem Kodachi Linux. Pertama, Kodachi *live* dijalankan pada *Virtual Machine* dari media eksternal tanpa perlu terinstal pada *harddisk*. Kedua, Kodachi *Booting* yaitu di mana sistem operasi terinstal secara permanen dan tersimpan pada RAM *harddisk* dan dijalankan melalui media penyimpanan saat komputer aktif.

TABEL. IV
SPESIFIKASI *SOFTWARE*

Aspek	Nama *Software*	Versi
Aplikasi *Chatting*	Pidgin *Internet*	4.0.2-2
	Element	1.11.23
	Tox	3.13.2-2
	Speekchat	1.6.0
Aplikasi *Sharing File*	Onion Share	0.9.2-1
	Localsend	1.14.0
	Sharik	V3.1
	QRCP	0.11.2

	Portal	V1.2.3
Aplikasi *Browser*	Firefox Unsafe	113.0.2
	Kodachi Lite *Browser*	3.4.1
	Kodachi Loaded *Browser*: TOR	3.4.1
	Kodachi Ghacks *Browser*: TOR	3.4.1
	Kodachi *Browser* with Proxichains: TOR	3.4.1
	TOR *Browser*	0.2.9-2
Aplikasi *Encryption*	Veracrypt	1.25.9
	Zulucrypt	5.4.0
	Picocrypt	1.39

Pada Tabel. 4 Spesifikasi *Software* memberikan informasi mengenai *software* beserta versi yang digunakan dalam Kodachi Linux berdasarkan aplikasi *chatting*, aplikasi *sharing file*, aplikasi *browser*, dan aplikasi *encryption* dalam pengujian fungsi *anonymity* dan *privacy*.

B. Analisis Pengukuran Anonymity dan Privacy

Pengukuran hasil *profiling* dilakukan klasifikasi pada penggunaan metrik fungsi *anonymity* dan *privacy* pada layanan jaringan, aplikasi, dan *storage* bertujuan mengetahui dan pemahaman klasifikasi pada penerapan *anonymity* dan *privacy*. Analisis pengukuran aspek layanan jaringan, aplikasi dan *storage* berdasarkan klasifikasi metrik yang dirumuskan dengan memberikan nilai di mana 1 dikatakan *Yes*, dan 0 dikatakan *No*. Penilaian klasifikasi metrik direpresentasikan berdasarkan pengukuran *K-anonymity* dan *Entropy Anonymity Degree (EAD),* dengan penjelasan sebagai berikut.

1) *K-anonymity* digunakan dengan tujuan untuk menggambarkan penilaian fungsi *anonymity* dan *privacy* dan sebagai acuan dalam klasifikasi metrik dari layanan jaringan, aplikasi, dan *storage*.
2) *Entropy Anonymity Degree (EAD)* bertujuan sebagai acuan dalam memberikan klasifikasi metrik dan *scoring* dalam menentukan fungsi *anonymity* dan *privacy* yang tinggi dan rendah pada layanan jaringan, aplikasi, dan *storage.*

C. Analisis Pengukuran Layanan Jaringan

Dalam analisis pengukuran layanan jaringan menggunakan metrik *anonymity* dan *privacy* yang berhubungan untuk mengevaluasi sejauh mana fungsi *anonymity* dan *privacy* diwujudkan. Penentuan metrik berdasarkan data *profiling* yang dikumpulkan, dengan hasil pengukuran fungsi *anonymity* dan *privacy* layanan jaringan Tabel. *5* Pengukuran Metrik Layanan Jaringan.

TABEL. V
PENGUKURAN METRIK LAYANAN JARINGAN

No	Struktur jaringan	*Usability* TOR	*IP Address masking*	*Security privacy*	*Encryption compability*	*Leak shield*	Total *Score*
1	ISP + DN*Scrypt*	No	No	No	No	No	0
2	ISP + VPN + DN*Scrypt*	No	No	Yes	Yes	Yes	3
3	ISP + VPN + TOR + DN*Scrypt*	Yes	Yes	Yes	Yes	Yes	5
4	ISP + VPN + Torify + TORDNS	Yes	Yes	Yes	Yes	Yes	5

Pada Tabel. 5 Pengukuran Metrik Layanan Jaringan menunjukkan hasil jaringan ditunjukkan fungsi *anonymity* dan *privacy* pada jaringan ISP + VPN + TOR + DNScrypt dan ISP + VPN + Torify + TORDNS dengan hasil sebagai berikut.

1) *Usability* TOR: (Yes)
   Penggunaan TOR pada Kodachi Linux berfungsi dengan kemudahan dan konfigurasi yang baik dalam layanan jaringan untuk memastikan terbentuk fungsi *anonymity*, di mana lalu lintas jaringan pada aktivitas digital dan sistem operasi diarahkan pada koneksi TOR. Selain itu adanya penggunaan TOR yang mengarahkan setiap permintaan DNS akan melalui TOR *network*, ditunjukkan dengan IP TOR dan IP TORDNS yang teralokasi pada sistem.
2) *IP Address masking: (Yes)*
   Konektivitas TOR yang terjadi memberikan karakteristik penyamaran identitas melalui bentuk *IP Address* yang anonim. Ketika terhubung TOR, *IP Address* yang terhubung bukan *IP Address* asli, tetapi *IP Address* dari proses TOR node. Oleh sebab itu, terjadinya *IP Address* yang disembunyikan dan dilindungi pada fungsi *anonymity* dan *privacy.*
3) *Security Privacy*: (Yes)

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 3, September 2025, Pp. 2355-2365

Keamanan yang ditunjukkan oleh penggunaan teknologi VPN, TOR, dan DNS *System* dapat secara efektif melindungi *privacy* dari berbagai ancaman keamanan. VPN melindungi data saat transit, TOR memastikan *anonymity* dengan menyembunyikan identitas dan lokasi, sementara DN*Scrypt* melindungi *privacy* permintaan DNS dari pengawasan. Secara keseluruhan, kombinasi ini memberikan tingkat perlindungan yang tinggi terhadap data dan *privacy*.

4) *Encryption Compabilty*: (Yes)
Penggunaan algoritma *encryption* pada konektivitas VPN dan TOR, keduanya berfungsi meningkatkan keamanan data. *Encryption* yang terjadi pada perlindungan lalu lintas terjadi antara perangkat dan server. Pada VPN menggunakan algoritma *encryption* AES. Sedangkan pada TOR, *encryption* terjadi pada lalu lintas melalui TOR *network*, melibatkan *encryption* pada proses TOR *node*. Sehingga memastikan data terlindungi pada pengawasan dan pelacakan eksternal.

5) *Leak Shield: (Yes)*
Konektivitas TOR yang dapat terhubung mampu memberikan keamanan melindungi tidak terjadinya kebocoran data, yang ditunjukkan pada fitur DNS dan TOR yang menyembunyikan identitas *IP Address*.

Dari klasifikasi metrik layanan jaringan, terlihat bahwa konfigurasi jaringan pada Kodachi Linux yang melibatkan VPN, TOR, dan DNScrypt atau TORDNS menunjukkan efektivitas dalam melindungi aspek keamanan dan *privacy*. Namun, aktivasi fitur *anonymity* dan *privacy* ini meningkatkan penggunaan RAM hingga 40%, yang dapat menjadi batasan dan mempengaruhi performa sistem secara signifikan. Pada sistem dengan kapasitas RAM terbatas, peningkatan penggunaan RAM ini dapat menyebabkan penurunan kecepatan, gangguan *multitasking*, dan bahkan gangguan dalam menjalankan aplikasi. Oleh karena itu, penting memastikan spesifikasi *hardware* yang digunakan cukup tinggi agar fitur *anonymity* dan *privacy* dapat berjalan efisien tanpa menurunkan performa sistem. Selain itu, konfigurasi ISP + DNScrypt yang rentan terhadap pelacakan dan pengungkapan identitas menunjukkan kelemahan dalam menjaga *anonymity* dan *privacy*, sehingga tidak aman untuk situasi yang memerlukan tingkat *privacy* tinggi. Konfigurasi jaringan dengan *score* 3 menunjukkan adanya peningkatan keamanan, tetapi masih memiliki risiko kebocoran identitas, sehingga kurang cocok untuk skenario yang membutuhkan *anonymity* dan *privacy* yang kuat. Hal ini menunjukkan bahwa konfigurasi tersebut tidak memadai untuk situasi yang memerlukan perlindungan kuat terhadap pelacakan dan pengawasan layanan jaringan.

D. Analisis Pengukuran Layanan Aplikasi

Pengukuran pada layanan aplikasi berdasarkan hasil data *profiling* untuk memberikan pengukuran pada fungsi *anonymity* dan *privacy* pada layanan aplikasi dalam melindungi data, dan untuk menghasilkan himpunan aplikasi yang dikategorikan dari penerapan *anonymity* dan *privacy*. Pengukuran metrik pada layanan aplikasi Tabel. 6 Pengukuran Metrik Aplikasi *Chatting*.

TABEL. VI
PENGUKURAN METRIK APLIKASI *CHATTING*

Aplikasi *Chatting*	**Metrik**					**Total *Score***
	***Usability* TOR**	***Peering Communication***	***Disguising Identity***	***External Tracking***	***Data Scrubbing***	
Pidgin *Internet*	Yes	Yes	Yes	Yes	Yes	5
Element	Yes	No	Yes	Yes	No	3
Speekchat	Yes	Yes	Yes	Yes	Yes	5
Tox	Yes	No	Yes	Yes	No	3
Instagram	No	No	No	No	No	0
Whatsapp	No	No	No	No	No	0
Gmail	No	No	No	No	No	0

Pada Tabel. 6 Pengukuran Metrik Aplikasi *Chatting* menunjukkan klasifikasi pada aplikasi *chatting* memiliki kemampuan dalam mewujudkan *anonymity* dan *privacy* terdapat pada aplikasi Speekchat dan Pidgin Internet memiliki *score* memenuhi klasifikasi metrik *Usability* TOR, *Peering Communication, Disguising Identity, External Tracking,* dan *Data Scrubbing*. Pada Element dan Tox memiliki *score* 3 karena tidak memenuhi metrik *Peering Communcation* dan *Data Scrubbing*, menunjukkan kurangnya dukungan untuk komunikasi peer-to-peer atau data scrubbing menandakan fungsi *anonymity* tidak sepenuhnya terlindungi atau tidak cocok untuk situasi di mana *anonymity* dan *privacy*. Sedangkan pada aplikasi Instagram, Whatsapp, dan Gmail tidak mendukung *anonymity* dan *privacy* menunjukkan aplikasi tersebut tidak mendukung TOR, tidak menyamarkan identitas, dan tidak memiliki mekanisme perlindungan dari pelacakan eksternal atau pembersihan data. Ini berarti aplikasi-aplikasi ini tidak mendukung untuk digunakan dalam konteks yang membutuhkan *privacy* tinggi, seperti komunikasi sensitif atau aktivitas digital di lingkungan yang represif. Hasil analisis menunjukkan Kodachi Linux pada layanan aplikasi

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 3, September 2025, Pp. 2355-2365

yang dapat mewujudkan *anonymity* dan *privacy* secara tinggi pada aplikasi tertentu, namun menjadi batasan pada aplikasi yang tidak mendukung fungsi *anonymity* dan *privacy* yang menimbulkan risiko signifikan, terutama bagi yang memerlukan *privacy* tinggi dalam aktivitas digital.

TABEL. VII
PENGUKURAN METRIK APLIKASI *SHARING FILE*

Aplikasi *Sharing*	**Metrik**					**Total *Score***
	***Usability* TOR**	***Peering Communication***	***Disguising Identity***	***Usability* TOR**	***Peering Communication***	
Onion Share	Yes	Yes	Yes	Yes	Yes	5
QRCP	No	Yes	No	No	Yes	2
Portal	No	Yes	No	No	Yes	2
Localsend	No	Yes	No	No	No	1
Sharik	No	Yes	No	No	No	1

Pada Tabel. 7 Pengukuran Metrik Aplikasi *Sharing File* menunjukkan aplikasi sharing yang tepat bergantung pada kebutuhan spesifik terhadap *privacy* dan *anonymity*. Onion Share memiliki tingkat *anonymity* dan *privacy* yang tinggi karena memenuhi kelima metrik klasifikasi pengukuran *anonymity* dan *privacy,* namun menjadi karakter dimana Onion Share bergantung pada konektivitas TOR agar dapat terjadi *sharing file*. Untuk kebutuhan yang moderat, QRCP dan Portal memiliki *score* 2 karena tidak memenuhi metrik *Usability* TOR, *Disguising Identity*, dan *External Tracking* yang tidak terjadinya penyembunyian identitas pada aktivitas digital, dan pelacakan pada pihak yang tidak sah. Sementara Localsend dan Sharik tidak mendukung fungsi *anonymity* dan *privacy* pada klasifikasi metrik karena terhubung menggunakan jaringan lokal yang tidak menyembunyikan identitas pengguna dan lebih rentan terhadap intersepsi dan pelacakan oleh pihak ketiga.

TABEL. VIII
PENGUKURAN METRIK APLIKASI *BROWSER*

Aplikasi *Browser*	**Metrik**					**Total *Score***
	***Usability* TOR**	***Peering Communication***	***Disguising Identity***	***Usability* TOR**	***Peering Communication***	
Firefox unsafe	Yes	Yes	Yes	Yes	No	4
TOR *Browser*	Yes	Yes	Yes	Yes	Yes	5
Kodachi lite *Browser*	Yes	Yes	Yes	Yes	No	4
Kodachi Loaded *Browser*: TOR	Yes	Yes	Yes	Yes	Yes	5
Kodachi Ghakcs *Browser*: TOR	Yes	Yes	Yes	Yes	Yes	5

Pada Tabel. 8 Pengukuran Metrik Aplikasi *Browser* menunjukkan karakter aplikasi Browser dalam mewujudkan fungsi *anonymity* dan *privacy*. TOR Browser, Kodachi Loaded Browser: TOR, dan Kodachi Ghacks Browser: TOR mendukung semua metrik, termasuk *Usability* TOR, *Peering Commnuncation, Disguising Identity, External Tracking*, dan *Data Scrubbing*. Firefox unsafe dan Kodachi Lite Browser mendukung memenuhi metrik *Usability* TOR, *Peering Commnuncation, Disguising Identity, External Tracking*, tetapi tidak *Data Scrubbing*. Secara keseluruhan, TOR Browser, Kodachi Loaded Browser: TOR, dan Kodachi Ghacks Browser: TOR menawarkan perlindungan *privacy* dan *anonymity* yang paling komprehensif, sementara Firefox Unsafe dan Kodachi Lite Browser menawarkan perlindungan yang kurang lengkap karena tidak mendukung pembersihan data. Risiko utama dari browser dengan *score* tinggi adalah potensi kerentanan dalam ketergantungan jaringan TOR. Browser dengan *score* 4, yaitu Firefox Unsafe dan Kodachi Lite Browser, tidak memenuhi metrik *Data Scrubbing* meningkatkan peluang data, seperti *cookies* dan *cache*, tetap tersimpan di perangkat, yang dapat dimanfaatkan oleh penyerang Kekurangan ini membuat lebih rentan terhadap pengawasan jangka panjang dan pengumpulan data oleh pihak ketiga, terutama di lingkungan di mana perangkat dapat diakses secara fisik.

TABEL. IX
PENGUKURAN METRIK APLIKASI *ENCRYPTION*

Aplikasi *Encryption*	**Metrik**					**Total *Score***
	Encryption Compability	***Key management***	***Plausible Deniability***	***Secure erase***	***Auto Lock***	
Veracrypt	Yes	Yes	Yes	Yes	Yes	5
Zulucrypt	Yes	Yes	Yes	Yes	Yes	5
Picocrypt	Yes	Yes	No	Yes	Yes	4
Sirikali	Yes	Yes	No	Yes	Yes	4

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 3, September 2025, Pp. 2355-2365

Pada Tabel. 9 Pengukuran Metrik *Aplikasi Encryption* menunjukkan karakter aplikasi *encryption* dalam mewujudkan fungsi keamanan data. Veracrypt dan zulucrypt mendukung kelima metrik *Encryption Compability, Key Management, Plausible Deniability, Secure Erase*, dan *Auto Lock*. Sirikali mendukung *Encryption Compability, Key Management, Secure Erase*, dan *Auto Lock*, tetapi tidak mendukung *Plausible Deniability*. Secara keseluruhan, Veracrypt dan Zulucrypt menawarkan perlindungan keamanan data yang komprehensif di antara aplikasi *encryption*, sementara Picocrypt dan Sirikali menawarkan perlindungan yang kurang lengkap karena tidak mendukung *Plausible Deniability*. Aplikasi enkripsi dengan *score* tinggi, seperti Veracrypt dan Zulucrypt, menawarkan perlindungan data yang komprehensif dengan mendukung semua metrik penting, termasuk *Plausible Deniability* dan *Secure Erase*. Ini menjadikan ideal untuk skenario berisiko tinggi, seperti penyimpanan informasi sensitif atau rahasia yang memerlukan keamanan berlapis dan kemampuan menyembunyikan eksistensi data yang terenkripsi. Namun, aplikasi seperti Picocrypt dan Sirikali memiliki keterbatasan karena tidak mendukung *Plausible Deniability*, yang memungkinkan pengguna untuk menyangkal keberadaan volume terenkripsi jika melakukan akses secara paksa. Meski tetap efektif untuk enkripsi dasar, mungkin kurang aman untuk digunakan dalam konteks di mana perlu perlindungan data.

E. Pengukuran Metrik Layanan Storage

Pada Analisis pengukuran layanan *storage*, metrik *anonymity* dan *privacy* digunakan untuk mengevaluasi fungsi *anonymity* dan *privacy* diwujudkan. Metrik ini mencakup *Encryption Compability, Access Control, Plausible Deniability, Secure Erase,* dan *Privacy Policy* [17]. Penentuan metrik ini berdasarkan data *profiling* yang dikumpulkan, dengan hasil pada Tabel. 10 Pengukuran Metrik Layanan *Storage*.

TABEL. X
PENGUKURAN METRIK LAYANAN *STORAGE*

Fitur layanan *storage*	**Metrik**					**Total *Score***
	Encryption Compability	***Key management***	***Plausible Deniability***	***Secure erase***	***Auto Lock***	
Persistent	Yes	Yes	No	No	Yes	3
Non-persistent	Yes	No	No	Yes	Yes	3
Nuke *System*	Yes	Yes	Yes	Yes	Yes	5
Kodachi *encryption file*	Yes	Yes	Yes	No	Yes	4

Pada Tabel. 10 Pengukuran Metrik Layanan *Storage* menunjukkan karakter fitur layanan *storage* dalam mewujudkan fungsi keamanan data. *Persistent* mendukung *Encryption Compability, Access Control, dan Privacy Policy*, tetapi tidak mendukung *Plausible deniability* dan *Secure Erase*. *Non-persistent* mendukung *Encryption Compability, Secure Erase*, dan *Privacy* Policy, tetapi tidak mendukung *Access Control* dan *Plausible Deniability*. Nuke System mendukung semua metrik, termasuk *Encryption Compability*, *Access Control, Plausible Deniability, Secure Erase*, dan *Privacy* Policy. Kodachi *Encryption File* memenuhi metrik *Encryption Compability, Access Control, Plausible Deniability,* dan *Privacy* Policy tetapi tidak mendukung *Secure Erase*. Secara keseluruhan, Nuke System menawarkan perlindungan keamanan data yang paling komprehensif di antara fitur layanan *storage* yang disebutkan, sementara *Persistent* dan Kodachi *Encryption File* menawarkan perlindungan yang kurang lengkap karena tidak mendukung beberapa metrik seperti *Secure Erase dan Plausible Deniability*. *Non-persistent* juga memberikan perlindungan yang kurang lengkap karena tidak mendukung *Access Control* dan *Plausible Deniability*. Oleh karena itu, layanan *storage* pada Kodachi Linux menunjukkan keterbatasan pada terbatas akan penyimpanan data, karena penggunaan keamanan data enkripsi dan fitur Nuke *system* yang menghapus semua data secara cepat dan menyeluruh ketika diaktifkan, yang membatasi fleksibilitas dalam pengelolaan data. Sehingga tingkat akan penggunaan sistem operasi menjadi sensitif, dan membutuhkan potensi pemahaman yang tinggi dalam menggunakan Kodachi Linux pada *storage* dan pengelolaan data.

F. Perbandingan Kodachi Linux

Perbandingan Kodachi Linux dengan sistem operasi lain yaitu Whonix, dan Tails yang mendukung *anonymity* dan *privacy*, menunjukkan keunggulan pada Kodachi Linux dalam *anonymity*, *privacy*, dan keamanan data [5]. Perbandingan Kodachi Linux dengan sistem operasi atau aplikasi serupa penting untuk menilai kinerja, dan kekuatan dalam fungsi *anonymity* dan *privacy*, dengan standar atau hasil pengujian dari alternatif lain, maka memperoleh konteks yang jelas mengenai efektivitas Kodachi Linux, mengidentifikasi fitur-fitur unggulan, serta memberikan informasi tentang penggunaan Kodachi Linux. Hasil perbandingan berdasarkan fitur-fitur yang

dimiliki sistem operasi dalam mewujudkan fungsi *anonymity* dan *privacy*, yang disajikan pada Tabel. 11 Perbandingan Kodachi Linux.

TABEL. XI
PERBANDINGAN KODACHI LINUX

Features	Tails	Whonix	Kodachi Linux
Tor starts automatically	Yes	Yes	Yes
Combines multiple anonymity tools	No	Yes	Yes
Encrypted DNS	No	No	Yes
Nuke Feature	No	No	Yes
Persistence and Non-persistence	Yes	Yes	Yes
Auto-wipe data	Yes	No	Yes

Pada Tabel. 11 Perbandingan Kodachi Linux, Kodachi Linux menawarkan beberapa keunggulan signifikan dibandingkan dengan Tails dan Whonix. Pertama, Kodachi Linux menyediakan enkripsi DNS, yang melindungi *privacy* pengguna dengan menyembunyikan permintaan DNS dari pihak ketiga, sebuah fitur yang tidak tersedia di Tails atau Whonix. Selain itu, Kodachi Linux dilengkapi dengan fitur nuke yang melakukan penghapusan data secara cepat dan aman dalam situasi darurat, serta kemampuan auto-wipe data untuk memastikan data tidak tertinggal setelah *booting* yang juga dimiliki Tails namun perbedaan yang dimiliki Kodachi Linux adanya enkripsi data pada penggunaan LUKS *encryption*, tetapi tidak ada di Whonix. Terakhir, Kodachi Linux mengintegrasikan berbagai alat *anonymity* lebih luas dibandingkan Whonix, yang hanya menggunakan Tor. Dengan kombinasi fitur-fitur ini, Kodachi Linux memberikan perlindungan dan keamanan fungsi *anonymity* dan *privacy* yang terwujud dari sistem operasi lain.

Dari hasil penelitian tentang efektivitas Kodachi Linux dalam melindungi *anonymity* dan *privacy*, terdapat beberapa rekomendasi untuk implementasi lebih lanjut. Pertama, optimalisasi penggunaan RAM diperlukan mengingat peningkatan penggunaan memori hingga 40% saat fitur *anonymity* dan *privacy* diaktifkan, yang memerlukan spesifikasi *hardware* tinggi agar fungsi ini dapat berjalan secara optimal. Disarankan untuk selalu mengaktifkan fitur *anonymity* dan *privacy* serta mengikuti panduan yang disediakan untuk memaksimalkan perlindungan data. Selain itu, penggunaan kombinasi VPN dan TOR dapat meningkatkan lapisan keamanan, sehingga pemahaman tentang cara kerja kedua teknologi ini penting untuk memastikan kinerja maksimal dari fungsi *anonymity* dan *privacy*. Penting juga untuk melakukan *backup* data secara berkala, terutama untuk data sensitif, guna menghindari potensi kehilangan data. Kontribusi terhadap peningkatan keamanan dan *privacy* dapat dilakukan melalui *profiling* pengukuran yang lebih rinci, mengaitkan pengaruhnya pada penggunaan *storage* dan fungsionalitas sistem operasi. Penelitian lanjutan juga dapat menggunakan aplikasi yang lebih bervariasi dan melakukan *profiling* serta pengukuran yang lebih luas dengan pendekatan kuantitatif untuk mendapatkan pemahaman yang lebih mendalam dan bervariasi tentang fungsi *anonymity* dan *privacy*..

IV. KESIMPULAN

Berdasarkan analisis yang dilakukan pada penelitian, menghasilkan kesimpulan bahwa identifikasi fungsi *anonymity* dan *privacy* dengan *profiling* pada aspek jaringan, aplikasi, dan *storage* disusun pada *Data Flow Diagram*. Hasil pengukuran metrik fungsi *anonymity* dan *privacy* pada Kodachi Linux yaitu berpengaruh pada layanan jaringan, Kodachi Linux mendukung penggunaan teknologi VPN, TOR, DNSscrypt, dan TORDNS dalam mewujudkan fungsi *anonymity* dan *privacy*, dengan *score* sebesar 5 yang diklasifikasikan berdasaraan memenuhi kelima metrik yang digunakan, tetapi menjadi batasan saat mengaktifkan fitur *anonymity* dan *privacy* dalam situasi penggunaan RAM sebesar 40%. Pada layanan aplikasi menempati posisi tertinggi terdapat Speeekchat, Pidgin *Internet*, Onion Share, Kodachi Ghacks *Browser*: TOR, Kodachi Loaded *Browser*: TOR, Kodachi *Browser* with Proxychains: TOR, dan TOR *Browser* dengan *score* 5 memenuhi kelima metrik. Kemudian pada aplikasi *encryption* memenuhi fungsi *anonymity* dan *privacy* tertinggi pada Veracrypt dan Zulucrypt dengan *score* 5 memenuhi kelima metrik. Hasil pengukuran tertinggi pada layanan *storage* penggunaan Nuke *System* dan *non-persistent* dalam menerapkan fungsi *anonymity* dan *privacy* dengan *score* 5 memenuhi kelima metrik Kesimpulan penelitian ini adalah Kodachi Linux mewujudkan fungsi *anonymity* dan *privacy* pada aspek layanan jaringan, aplikasi, dan *storage.*

DAFTAR PUSTAKA

[1] S. W. A. Hamdani *et al.*, "Cybersecurity Standards in the Context of Operating System," *ACM Comput. Surv.*, vol. 54, no. 3, 2021, doi: 10.1145/3442480.
[2] D. Hellwig, G. Karlic, and A. Huchzermeier, "Privacy and Anonymity," *Manag. Prof.*, vol. Part F433, pp. 99–121, 2020, doi: 10.1007/978-3-030-

40142-9_5.
[3] D. L. Huete Trujillo and A. Ruiz-Martínez, "Tor Hidden Services: A Systematic Literature Review," *J. Cybersecurity Priv.*, vol. 1, no. 3, pp. 496–518, 2021, doi: 10.3390/jcp1030025.
[4] A. K. Jadoon, "Forensic Analysis of Tor Browser: A Case Study for Privacy and Anonymity on the Web," *ScienceDirect*, vol. 299, pp. 59–73, 2019, [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0379073819301082
[5] A. Hulina, "Operating systems for privacy and anonymity: a survey," 2020, [Online]. Available: https://scholar.googleusercontent.com/scholar?q=cache:1klDeFImsO0J:scholar.google.com/+operating+systems+anonymity&hl=en&as_sdt=0,5
[6] D. J. Kelly, R. O. Baldwin, R. A. Raines, M. R. Grimaila, and B. E. Mullins, "A survey of state-of-the-art in anonymity metrics," *Proc. ACM Conf. Comput. Commun. Secur.*, pp. 31–39, 2008, doi: 10.1145/1456441.1456453.
[7] K. Chatzikokolakis and T. Chothia, "Calculating probabilistic anonymity from sampled data," *Manuscript*, 2007, [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.164.897&rep=rep1&type=pdf
[8] K. Kenny, K. Gunadi, and L. W. Santoso, "Implementasi The Onion Router (Tor) Berbasis Virtual Private Network (VPN) pada Raspberry Pi," *J. Infra*, vol. 5, no. 2, pp. 125–129, 2017, [Online]. Available: http://publication.petra.ac.id/index.php/teknik-informatika/article/view/5769/5266
[9] A. Afzal, M. Hussain, S. Saleem, M. K. Shahzad, A. T. S. Ho, and K. H. Jung, "Encrypted network traffic analysis of secure instant messaging application: A case study of signal messenger app," *Appl. Sci.*, vol. 11, no. 17, 2021, doi: 10.3390/app11177789.
[10] D. L. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," *Commun. ACM*, vol. 24, no. 2, pp. 84–90, 1981, doi: 10.1145/358549.358563.
[11] G. Wang, J. Chen, and L. T. Yang, *and Anonymity in Computation, Communication, and Storage*, vol. 1. 2018. doi: 10.1007/978-3-030-24900-7.
[12] D. McCoy, K. Bauer, D. Grunwald, T. Kohno, and D. Sicker, "Shining light in dark places: Understanding the tor network," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 5134 LNCS, pp. 63–76, 2008, doi: 10.1007/978-3-540-70630-4_5.
[13] M. R. Nosouhi, S. Yu, K. Sood, and M. Grobler, "HSDC-Net: Secure anonymous messaging in online social networks," *Proc. - 2019 18th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. IEEE Int. Conf. Big Data Sci. Eng. Trust. 2019*, pp. 350–357, 2019, doi: 10.1109/TrustCom/BigDataSE.2019.00054.
[14] J. Zhang, H. Duan, W. Liu, and J. Wu, "Anonymity analysis of P2P anonymous communication systems," *Comput. Commun.*, vol. 34, no. 3, pp. 358–366, 2011, doi: 10.1016/j.comcom.2010.06.022.
[15] N. F. Abbas and R. Al-bahrani, "INTERNATIONAL JOURNAL OF HUMANITIES AND CULTURAL STUDIES ISSN 2356-5926 The Search for Identity in Online Chat," no. September 2015, 2016.
[16] Y. J. Park, "Digital Literacy and Privacy Behavior Online," *Communic. Res.*, vol. 40, no. 2, pp. 215–236, 2013, doi: 10.1177/0093650211418338.
[17] T. ČIERNIKOVÁ, "Selected open tools supporting security and privacy protection for regular end-users," *Is.Muni.Cz*, 2022, [Online]. Available: https://is.muni.cz/th/h7qfk/thesis.pdf
[18] E. Anzuoni and T. Gagliardoni, "Shufflecake: Plausible Deniability for Multiple Hidden Filesystems on Linux," *CCS 2023 - Proc. 2023 ACM SIGSAC Conf. Comput. Commun. Secur.*, pp. 3033–3047, 2023, doi: 10.1145/3576915.3623126.
[19] J. Caesar, "Cryptographic Key Management A Beginner's Guide".
[20] M. F. Safitra, M. Lubis, and A. Widjajarto, "Security Vulnerability Analysis using Penetration Testing Execution Standard (PTES): Case Study of Government's Website," *ACM Int. Conf. Proceeding Ser.*, no. August, pp. 139–145, 2023, doi: 10.1145/3592307.3592329.
[21] I. Wagner and D. Eckhoff, "Technical privacy metrics: A systematic survey," *ACM Comput. Surv.*, vol. 51, no. 3, pp. 1–45, 2018, doi: 10.1145/3168389.