Implementasi Dan Analisa *Profiling Anonymity* Dan *Privacy* Pada *Operating System* Tails

1st Maya Angelia Br Surbakti
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
maysbkti@student.telkomuniversity.ac.id

2nd Adityas Widjajarto
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
adtwjrt@telkomuniversity.ac.id

3rd M. Teguh Kurniawan
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
teguhkurniawan@telkomuniversity.ac.id

***Abstrak* —Tails adalah sistem operasi berbasis Debian dalam keluarga Linux, dirancang untuk menyediakan anonymity dan privacy bagi pengguna melalui jaringan Tor. Penelitian ini bertujuan mengevaluasi dan menganalisis kemampuan Tails OS dalam menjaga anonymity dan privacy melalui profiling aplikasi, jaringan, dan system storage. Studi ini melibatkan identifikasi fitur software yang mendukung anonymity dan privacy, serta pengukuran metrik relevan untuk mengevaluasi fungsionalitasnya. Hasil dari penelitian ini menunjukkan Tails memiliki fitur-fitur yang mendukung penerapan anonymity dan privacy yang diilustrasikan melalui data flow diagram dan metrik yang disusun berdasarkan hasil profiling. Hasil metrik yang secara penuh mewujudkan dan terpenuhi pada profiling anonymity dan privacy pada aspek aplikasi adalah Onion Share, Pidgin OTR, KeePassXc, Thunderbird dan Tor Browser dengan menyatakan skor Yes sebanyak 5 dari hasil ke-5 metrik pada aspek aplikasi. Hasil metrik yang tidak sepenuhnya mewujudkan anonymity dan privacy terdapat pada social media yang di akses melalui Tor Browser dengan hasil menyatakan skor Yes sebanyak 3 dari hasil ke-5 metrik. Hasil metrik yang tidak mewujudkan anonymity dan privacy terdapat pada Unsafe Browser dengan hasil menyatakan skor Yes sebanyak 2 dari hasil ke-5 metrik. Hasil yang secara penuh mewujudkan dan terpenuhi pada profiling anonymity dan privacy pada aspek networking adalah Tor dan Dnsleaktest dengan hasil skor Yes sebanyak 4 dari hasil ke-4 metrik, kemudian Hasil metrik yang tidak mewujudkan anonymity dan privacy adalah VPN dengan hasil skor Yes 0 dari ke-4 metrik. Pada aspek system storage yang memenuhi anonymity dan privacy adalah Persisten Storage dengan hasil skor Yes sebanyak 4 dari ke-4 metrik, sedangkan LUKS dengan hasil skor Yes sebanyak 2 dari ke-4 metrik menyatakan bahwa LUKS tidak sepenuhnya anonymity dan privacy. Kesimpulan dari penelitian ini adalah bahwa metrik yang digunakan dalam profiling aplikasi, jaringan, dan system storage di Tails OS secara komprehensif menunjukkan bahwa sistem operasi ini menyediakan lingkungan layanan yang mendukung anonymity dan privacy**.

***Kata kunci*— *Anonymity*, Privacy, Tor, *Profiling*, Fungsi, Metrik**

I. PENDAHULUAN

Ilmuwan sosial, filsuf, dan pengacara telah mempertanyakan *privacy* sebagai masalah hukum dan sosial. *Privacy* adalah hak asasi manusia yang penting, seperti yang diakui oleh Deklarasi Hak Asasi Manusia PBB, Konvensi Internasional tentang Hak Sipil dan Politik (PI/EPIC Privacy International, Electronic Privacy Information Center, 1999). Dalam demokrasi, *privacy* harus dihargai. Pengetahuan tentang teknik komunikasi dan informasi modern telah menempatkan *privacy* dalam bahaya (Stefanos Gritzalis, 2004).

Anonymity dan *privacy* dalam era *digital* saat ini menjadi relevan dan penting. *Privacy* merupakan hak seseorang untuk mengontrol informasi pribadi dan menentukan sejauh mana seseorang tersebut bersedia berbagi informasi dengan orang lain. Sementara itu, *anonymity* dapat diartikan sebagai ketiadaan identitas yang terkait dengan tindakan tertentu. Setiap tindakan *online* dapat meninggalkan jejak *digital*, seperti IP *address* dan data pribadi dan lainnya. Oleh karena itu, menjaga *privacy* dan *anonymity* dalam aktivitas *online* merupakan tantangan yang kompleks (Yuwinanto, n.d.-a). Dalam konteks ini, munculnya sistem operasi bernama Tails (*The Amnesic Incognito Live System*), Tails adalah sistem operasi *portable* berbasis Debian yang berfokus pada menjaga *anonymity* dan *privacy* pengguna. Salah satu fitur dari Tails OS adalah memiliki kemampuan untuk beroperasi dari *drive DVD* atau *USB*. Sistem operasi ini memanfaatkan teknologi *anonymous* seperti jaringan Tor dan berbagai fitur keamanan yang kuat bagi pengguna (Hulina, 2020).

Dalam penelitian ini bertujuan untuk menganalisis fitur-fitur dan fungsi yang terdapat pada Tails OS melalui proses *profiling*. Hasil dari penelitian ini diharapkan memberikan pemahaman dan gambaran mengenai perlindungan *privacy* di era *digital*.

II. KAJIAN TEORI

A. Cyber Security

Keamanan Siber (cyber security) merupakan teknologi yang bertujuan melindungi aset digital dari akses yang tidak sah, dapat dimanfaatkan, dan disalahgunakan oleh pihak yang tidak bertanggung jawab. Bidang in menangani upaya pelindungan sistem digital ataupun informasi dari segala jenis akses yang tidak sah. Fokus utama cyber securtity adalah menjaga kerahasiaan, integritas, dan ketersediaan aset dan

data digital, yang dikenal sebagai CIA (confidentiality, integrity, availability) (Hamdani et al., 2022).

B. *Digital Privacy*

Digital *privacy* adalah kemampuan individu atau kelompok orang untuk menjaga kehidupan pribadi dan urusan personal dari public, termasuk dalam penggunaan layanan *online*, pemantauan lalu lintas *internet*, akses ke pusat data bahkan penyimpanan profil pribadi (Yuwinanto - PRIVASI ONLINE DAN KEAMANAN DATA.Pdf, n.d.).

C. *Anonymity*

Anonymity atau anonimitas berasal dari kata Yunani (*anonymia*) yang merupakan tanpa identitas. *Anonymity* mencakup informasi tentang identitas seseorang yang tidak diketahui. Menurut Pfitzman & Kohntopp dan Joinson *anonymity* dapat dikelompokkan dalam skala fungsional; less anonymous hingga *fully anonymous* (Lilis Nosiva Rini, Rouli Manalu n.d.).

D. TOR

Tor atau "*The Onion Router*" merupakan lapisan tambahan yang beroperasi pada *internet*, dirancang untuk memberikan tingkat *anonymity end-to-end* yang lebih tinggi melalui desain Onion Routing. Cara data dienkripsi dan diteruskan melalui lapisan. Proses ini melibatkan penghapusan header paket yang berisi informasi pengirim, kemudian mengenkripsi sisa informasi. Selama proses ini diulang beberapa kali, setiap relay hanya memiliki kunci untuk enkripsi dan mengetahui IP tujuan dari relay berikutnya (Abraham et al., n.d.).

E. Tails OS

Tails atau *The Amnesiac Incognito Live System* adalah operasi bersifat *open-source* dan gratis, dirancang untuk fokus pada keamanan dalam menjaga *privacy* dan *anonymity*, Tails juga sistem operasi berbasis debian. Tails hanya mengimplementasikan beberapa fitur keamanan lain sebagai bagian dari kernel dasar Debian (Hulina, 2020).

F. IP Address

Ip address merupakan suatu cara pemberian identifikasi pada jaringan komputer dengan memberikan deretan angka pada perangkat komputer (host), router dan peralatan jaringan lainnya. IP (*Internet Protocol*) dirancang untuk menghubungkan sistem komunikai komputer pada jaringan switched dimana setiap komputer diidentifikasi melalui alamat IP yang unik, sehingga setiap alamatnya berbeda satu sama lain. Tujuannya untuk mencegah kesalahan pada saat transfer data (Wardoyo et al., 2014).

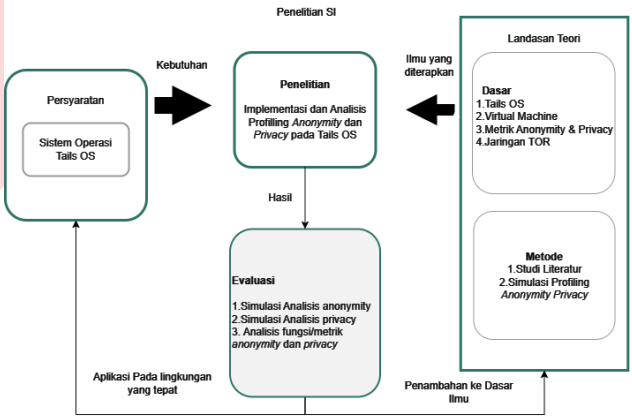
G. Implementasi *Anonymity* Profiling

Profiling anonymity mengacu pada penggunaan data pribadi untuk mengevaluasi beberapa aspek pribadi yang terkait dengan seseorang, khususnya untuk menganalisis atau memprediksi aspek-aspek yang berkaitan dengan kinerja seseorang di tempat kerja, situasi ekonomi, kesehatan, preferensi pribadi, minat, perilaku, lokasi, atau pergerakan seseorang. *Profiling anonymity* dapat dilakukan melalui pemrosesan otomatis data pribadi, periklanan, dan bidang lainnya untuk menargetkan individu atau kelompok tertentu. Penggunaan *profiling anonymity* menimbulkan kekhawatiran privasi, karena dapat mengakibatkan diskriminasi atau konsekuensi negatif lainnya bagi individu. Oleh karena itu, penting untuk mengatur penggunaan profil anonimitas dan memastikan bahwa individu memiliki kontrol atas data pribadi.

III. METODE

A. Model Konseptual

Model konseptual adalah representasi suatu diagram atauvisual dari suatu konsep atau ide. Model ini bertujuan mengilustrasikan dan mempermudah pemahaman konsep secara menyeluruh dan difokuskan pada stuktur hubungan inti dari konsep yang diwakili. Berikut adalah gambaran model konseptual yang diterapkan dalam Tugas Akhir:



GAMBAR 1
(Metodologi Penelitian)

Gambar diatas *Menjelaskan rincian sebagai berikut*

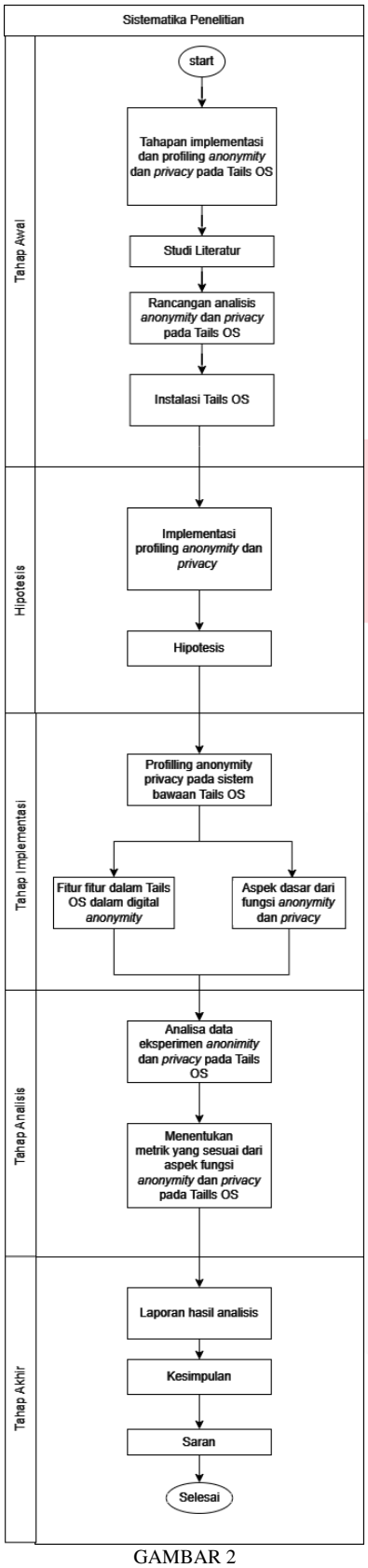
1.Bagian Persyaratan terdapat sistem operasi Tails Tails, adalah sistem operasi berbasis Linux, diciptakan dengan fokus pada perlindungan *privacy* pengguna. Tails memanfaatkan teknologi enkripsi untuk mengamankan semua data penyimpanan, memanfaatkan jaringan Tor untuk melindungi *privacy* pengguna dengan mengenkripsi lalu lintas *internet* dan menyembunyikan alamat IP.

2.Bagian Penelitian SI terdiri dari penelitian dan evaluasi. Pada Penelitian menghasilkan implementasi dan analisis profiling *anonymity* dan *privacy* pada Tails OS. Kemudian pada bagian lingkup Evaluasi, terdisi dari simulasi *anonymity*, simulasi *privacy* dan analisis fugsi atau metrik *anonymity* dan *privacy*

3.Bagian Dasar Ilmu terdiri dari dasar teori dan metode. Bagian teori terdiri dari Tails OS, virtual machine, metrik *anonymity* dan *privacy*, jaringan TOR.

B. Sistematika Penyelesaian Masalah

Sistematika penyelesaian masalah adalah suatu pendekatan atau urutan proses yang terlibat dalam menganalisis, mengidentifikasi, dan menyelesaikan masalah. Tujuannya adalah memberikan kerangka kerja terstruktur. Sistematika penyelesaian masalah dibagai 5 tahap yaitu: tahap awal, hipotesis, tahap implemetasi, tahap analisis, dan tahap akhir.



GAMBAR 2
(Sistematika penyelesaian)

1. Tahap Awal

Tahap awal penelitian dimulai dengan melakukan bagaimana tahapan implementasi profiling *anonymity* dan *privacy* pada Tails OS. Dilanjutkan dengan melalukan riset dengan studi literatur. Studi literatur perlu dilakukan untuk memastikan bahwa masalah yang dibahas sesuai dengan tahapan implementasi terhadap profiling.

2. Tahap Hipotesis

Pada tahap ini melakukan hipotesis yang mengarah pada pernyataan awal terkait implementasi teknologi keamanan *anonymity* dan *privacy*.

3. Tahap Implementasi

Pada tahap ini akan dilakukan proses profilling *anonymity privacy* pada sistem bawaan Tails OS. Setelah profiling dilakukan, maka akan menghasilkan fitur yang terdapat pada Tails OS dalam digital *anonymity* dan aspek dasar dari fungsi *anonymity* dan *privacy*

4. Tahap Analisis

Tahap analisis ini dilakukan proses analisis dari hasil yang didapatkan pada implementasi yang sudah dilakukan. Hasil analisis berupa Analisa data simulasi *anonymity* dan *privacy* pada Tails OS. Setelah itu menentukan metrik yang sesuai dari aspek fungsi *anonymity* dan *privacy*.

5. Tahap Akhir

Tahap akhir dari penelitian adalah tahap pelaporan hasil penelitian. Pada tahap ini, hasil analisis yang telah dilakukan disusun secara sistematis, kemudian diringkas dalam bentuk kesimpulan dan saran.

C. Pengumpulan Data

Pengumpulan data dilakukan berdasarkan kerangka kerja yang tergambar dalam bentuk diagram di atas. Pengumpulan data dalam implementasi profiling pada sistem operasi Tails bertujuan untuk mengevaluasi tingkat dukungan sistem operasi tersebut mendukung penerapan *anonymity* dan *privacy*. Data akan diklasifikasikan berdasarkan fitur fitur dan aspek dasar fungsi *anonymity* dan *privacy* yang terdapat pada Tails OS

D. Pengolahan Data

Pengolahan data diatur dengan melakukan perbandingan antara hasil pengujian profiling dan karateristik fitur-fitur Tails OS berdasarkan ukuran metrik dari aplikasi bawaan yang telah terinstal. Data yang diperoleh akan dievaluasi dengan menggunakan klasifikasi metrik sesuai dengan kerangka kerja pengujian profiling.

E. Metode Evaluasi

Pengujian profiling terhadap implementasi *anonymity* dan *privacy* pada Tails OS berfokus pada dampak terhadap fitur-fitur dan aplikasi sistem operasi, serta aplikasi pihak ketiga yang diinstal.

IV. IMPLEMENTASI DAN SKENARIO PENGUJIAN

Pada bab ini, akan dibahas eksperimen implementasi sistem operasi Tails yang terdiri dari tiga kelompok yaitu aplikasi, networking dan system storage. Eksperimen ini dibuat dalam tiga aspek

1. Aplikasi

Dalam aspek ini dilakukan profiling pada aplikasi Onion Share, Pidgin OTR, Thunderbird, KeePassXC, Tor Browser, Unsafe Browser, Server Gmail, Server Whatsapp, Server Youtube, Server Instagram, dan Server Facebook.

2. Networking

Bagian ini melakukan profiling jaringan pada Tails dengan skenario penggunaan Tor Network, DNS leak test, dan VPN

3. System Storage

Bagian ini melakukan profiling pada system storage yang terdapat pada sistem operasi Tails.

Bab ini memiliki sistematika profiling sebagai berikut:

a. Rancangan Sistem: bagian ini berisi pengunaan hardware dan software pada eksperimen.
b. Skenario Percobaan: berisi gambaran langkah-langkah penggunaan aspek aplikasi, jaringan, dan system storage.
c. Implementasi Eksperimen: berisi data penggunaan implmentasi dengan data berupa gambar screenshot pada saat melakukan eksperimen

Data Hasil Eksperimen: Berisi data hasil yang berkaitan dengan implementasi eksperimen dan dipresentasikan dengan tabel input dan output sebagai perbandingan kondisi.

A. Rancangan Sistem

Implementasi profiling *anonymity* pada sistem operasi Tails memerlukan perancangan sistem untuk pengujian. Pengujian ini dilakukan dengan melakukan *booting* dari USB *Flashdrive*. Sistem operasi ini tidak meninggalkan jejak di komputer yang digunakan untuk menjaga *privacy* pengguna. Hasil pengujian ini akan dianalisis untuk mengetahui efektivitas implementasi profiling *anonymity* dan *privacy*.

1. Spesifikasi Hardware

Penelitian ini menjelaskan spesifikasi hardware pada laptop MSI GF63 Thin 10SC yang digunakan selama proses penelitian dan analisis. Berikut adalah rincian perangkat keras yang digunakan terlampir dalam tabel IV.1 berikut:

Tabel 1
(Spesifikasi *Hardware)*

Komponen	Informasi	
Core Hardware Specification	*Processor*	Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz (12 CPUs), ~2.6GHz
	Memory	16384MB RAM
	Hard Disk	477 GB SSD
	System Type	64 - Bit
	Operating System	Windows 11 Home 64-bit (10.0, Build 22621) (22621.ni_release.220506-1250)
	Eksternal Memory	*USB Flashdrive* 64 GB

2. Spesifikasi Software

Penelitian ini menjelaskan spesifikasi software atau perangkat lunak yang digunakan dalam proses *anonymity* and *privacy* profiling. Berikut adalah rincian software yang digunakan:

Tabel 2
(Operating System Information)

Komponen	Nama	*Requirment*	
Core Software Specification	*Operating System*	*Name*	Tails
		Version	6.1
		Processor	64-bit x86-64 *compatible processor*
		Memory	4 GB
		System Type	64-bit
		Operating System	*Debian-based Linux distribution (live system)*
	Eksternal Aplication	*Aplication*	*BalenaEtcher*

Spesifikasi yang digunakan menurut tabel 1 pada penelitian dan analisis, pada bagian ini akan dijelaskan fungsi dari *software* yang digunakan sebagai berikut:

a. Operating System

Tails

Operating System Tails (*The amnesic Incognito Live System*) adalah sistem operasi portabel yang sangat aman, yang melindungi *privacy online* pengguna melalui *tor network* sebagai aplikasi jaringan default. Tails tidak menggunakan hard disk, sehingga tidak ada data yang disimpan di sistem. Semua aktivitas pengguna disimpan di memori utama dan dihapus saat sistem dimatikan.

b. Memory

USB Flashdrive

*USB (*Universal Serial Bus*) Flashdrive* pada penelitian ini digunakan sebagai sistem operasi yang portable dan terintegrasi dan dapat dijalankan secara langsung. Sistem operasi ini diinstal pada *flasdrive* kemudian system ini dirancang untuk boot dari media *hardware*.

c. Eksternal *Aplication*

BalenaEtcher

BalenaEtcher pada penelitian ini digunakan untuk memflash file image pada sistem operasi seperti ISO dan IMG ke media eksternal *memory* seperti *USB flashdrive,* sehingga memudahkan untuk membuat media instalasi bootable untuk menjalankan sistem operasi Tails.

3. Spesifikasi Software

Penelitian ini menjelaskan spesifikasi *software* terkait aspek aplikasi, *networking,* dan *system storage* pada Tails OS yang digunakan dalam proses *anonymity and privacy profiling*. Berikut adalah rincian *software* yang digunakan:

Tabel IV 1 Spesifikasi *Software*

Aspek	Nama Software	Versi
Aplikasi	Onion Share	2.2
	Pidgin dan OTR	2.14.12
	Tor Browser	13.5.1
	Unsafe Browser	13.0.15
	KeePassXC	2.7.4
	Thunderbird	115.10.1

	Layanan Gmail	Layanan 2024
	Layanan WhatsApp	Layanan 2024
	Layanan YouTube	Layanan 2024
	Layanan Instagram	Layanan 2024
	Layanan Facebook	Layanan 2024
Networking	Tor *network*	Layanan 2024
	DNS leak test	Layanan 2024
	VPN	Layanan 2024
System Storage	Persistent Storage	Layanan 2024
	LUKS	Layanan 2024

Tabel IV 3 memberikan rincian tentang perangkat lunak dan versi layanan yang digunakan dalam sistem yang fokus pada *anonymity* dan *privacy*. Versi terbaru dari setiap perangkat lunak dan layanan (layanan 2024) menunjukkan bahwa sistem ini diatur dengan menggunakan teknologi terbaru.

4. Daftar IP Address

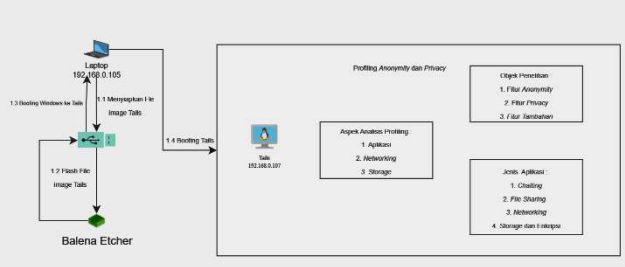
IP address (Internet Protocol Address) merupakan angka yang digunakan untuk mengidentifikasi perangkat dalam jaringan komputer. Fungsi IP address sebagai identifikasi perangkat dan sebagai komunikasi antar perangkat. Berikut merupakan daftar Ip address yang digunakan dalam profiling;

TABEL IV 3
(Daftar IP *address)*

Komponen	Sistem Operasi	*Ip Address*	*Gateaway*	*Subnet Mask*
Host	Tails	192.168.0.107	192.168.0.1	/24
Host	Windows	192.168.0.105	N/A	/24

5. Platform Eksperimen

Rancangan penelitian ini bertujuan untuk memberikan rancangan secara sistematis terkait kebutuhan perangkat yang digunakan dalam implementasi profiling *anonymity* dan *privacy*. Mekanisme ini membantu dalam menjalankan prosedur yang diterapkan dalam menjaga *anonymity* dan *privacy* pengguna. Berikut gambar dari platform eksperimen:



GAMBAR IV 1
(Mekasnisme Eksperimen)

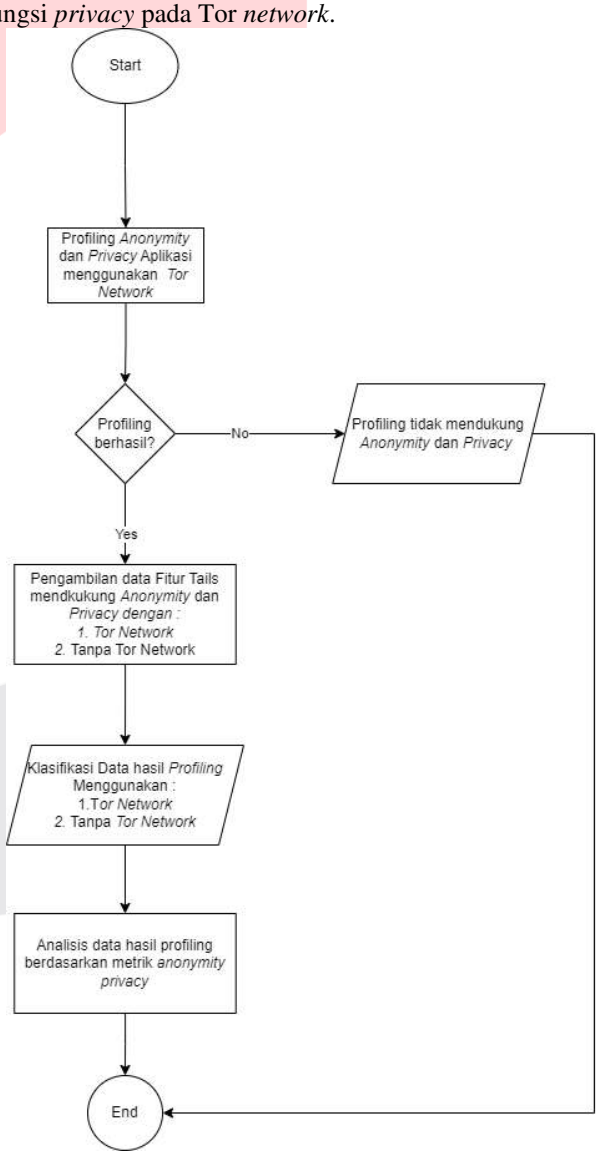
Pada Gambar IV 1 Proses dimulai dengan menyediakan *USB Flashdrive* kemudian menggunakan aplikasi *open-source* Balena Etcher untuk membuat image file dari sistem operasi Tails yang fungsinya untuk membuat media *bootable* pada perangkat eksperimen yang digunakan. Tails digunakan dalam eksperimen profiling *anonymity* dan *privacy* dalam aspek seperti aplikasi, *network,* dan Sistem enkripsi, kemudian objek eksperimen terdiri dari fitur *anonymity*, fitur *privacy* dan fitur tambahan dan jenis aplikasi yang digunakan dalam penelitian ini menggunakan aplikasi *default* pada Tails. Jenis aplikasi yang digunakan yaitu aplikasi *chatting, file sharing, networking*, dan sistem operasi pada Tails.

B. Skenario Percobaan

Skenario eksperimen berfungsi sebagai perencanaan dalam menyiapkan serangkaian metode yang memungkinkan dalam aspek profiling *anonymity* dan *privacy* pada Tails. Skenario eksperimen ini memiliki alur dalam perumusan dan hasil profiling *anonymity* dan *privacy* berdasarkan penggunaan Tor Network dan fitur Tails lainnya berdasarkan activity diagram.

1. Skenario Eksperimen Aplikasi

Skenario eksperimen aplikasi berfungsi sebagai landasan terhadap profiling *anonymity* dan *privacy*. Pada tahap ini dilakukan proses profiling *anonymity* dan *privacy* dengan menggunakan tor network pada aplikasi Tails. Dalam penelitian ini menguji apakah aplikasi tersebut memiliki fungsi *privacy* pada Tor *network*.



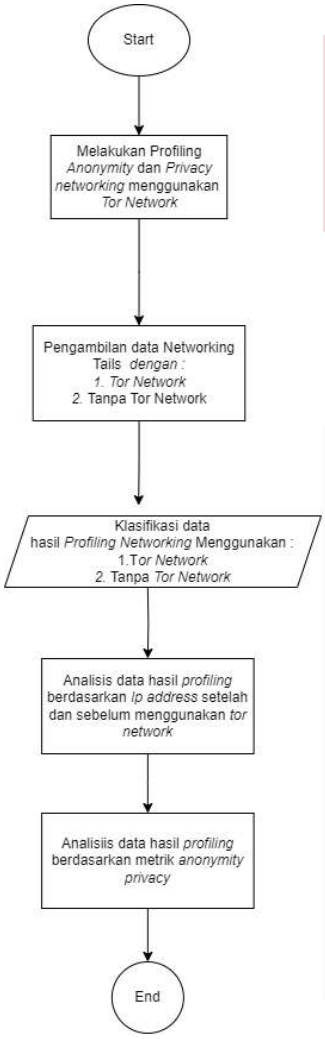
GAMBAR IV.1
(Skenario Eksperimen Aplikasi)

Pada Gambar IV.2 menjelaskan alur proses profiling. Pertama tama proses dilakukan dengan melakukan *profiling* aplikasi dengan menggunakan *tor network.* Setelah proses

profiling berhasil kemudian dilakukan dengan mengambil data fitur Tails yang mendukung *anonymity* dan *privacy* dengan menggunakan *tor network* dan tanpa *tor network*. Lalu data data yang diperoleh diklasifikasikan berdasarkan *Tor network* dan tanpa *tor network.* Data hasil *profiling* tersebut dilakukan dengan analisis berdasarkan metrik *anonymity* dan *privacy.*

2. Skenario Eksperimen *Networking*

Pada tahap ini akan dilakukan pengujian difokuskan pada implementasi *tor network* dalam Tails. Tujuan utama eksperimen ini untuk melihat kinerja dan tingkat *anonymity* yang diberikan oleh Tor. Alur skenario eksperimen akan dijelaskan menggunakan gambar *diagram* yang dapat dilihat pada gambar IV.3 dibawah ini:

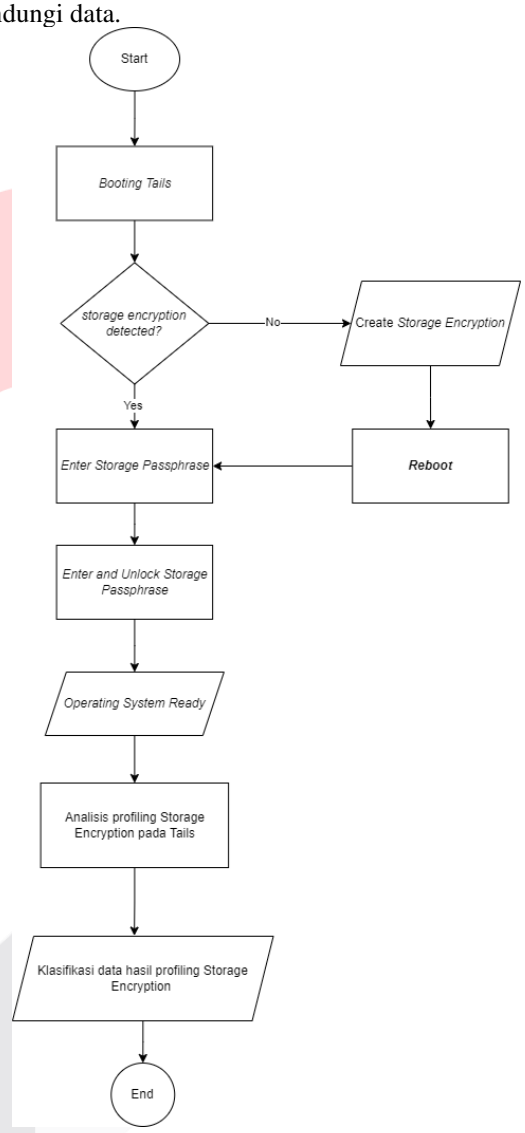


GAMBAR IV.2
(Diagram Skenario Eksperimen Networking)

Pada Gambar IV.3 menjelaskan tentang alur proses profiling *tor network.* Pada tahap pertama melakukan konfigurasi *Tor Network* pada Tails. Kemudian pengambilan data networking menggunakan Tor *network* dan tanpa *Tor network*. Pengambilan data ini bersifat kualitatif dengan menggunakan Tor Browser dan Unsafe Browser pada Tails. Setelah pengambilan data dilakukan maka akan diklasifikasikan data networking yang menggunakan *Tor Network* dan tidak menggunakan *Tor Network.* Kemudian setelah klasifikasi data selesai, maka dilanjutkan dengan analisis hasil profiling berdasarkan *Ip address* setelah dan sebelum menggunakan *Tor Network.* Setelah melakukan analisis data hasil dilanjutkan dengan analisis data hasil *profiling* berdasarkan metrik *anonymity* dan *privacy*

3. Skenario Eksperimen *Encryption System Storage*

Pada bagian ini dilakukan membuat skenario implementasi penyimpanan enkripsi pada Tails. Tujuan utama dari eksperimen ini untuk memahami proses konfigurasi dan keamanan penyimpanan yang diberikan oleh Tails dalam melindungi data.



GAMBAR IV.3
(Skenario Eksperimen System Storage Encryption)

Pada Gambar IV.4 menjelaskan alur proses eksperimen *system storage encryption* pada *system operating* Tails dimulai dengan *booting* Tails. Setalah selesai *booting* Tails, maka akan diarahkan ke user administrasi yang dimana Tails akan men-*detect storage encryption* dalam kondisi ini ketika storage encryption terdeteksi maka Tails akan meminta user memasukkan password *passphrase* dan kemudian *unlock passphrase.* Di kondisi ini ketika user belum memiliki *storage encryption* maka dapat membuat *storage encryption* yang tersedia di Tails. Setelah selesai *unlock storage encryption*, Tails akan memulai tampilan awal, setelah itu melakukan analisis *profiling storage encryption* yang tersedia pada Tails, terakhir melakukan klasifikasikan data

hasil *profiling* penyimpanan enkripsi dan analisis data hasil profiling dengan metrik *anonymity* dan *privacy.*

C. Implementasi Percobaan

Untuk mendapatkan hasil eksperimen, dilakukan implementasi dengan menggunakan Tor Network dan tanpa Tor Network. Dalam tahap ini melakukan implementasi percobaan profiling terdiri dari aplikasi, networking, dan storage encryption yang tersedia pada Tails yang memiliki *anonymity* dan *privacy* pada Tails. Tor Network dalam Tails hanya memiliki fitur *connect to* Tor dan tidak memiliki fitur untuk menonaktifkan Tor, sehingga terdapat beberapa aplikasi yang tidak menggunakan Tor aplikasi tersebut langsung diakses tanpa membutuhkan akses Tor Connection pada Tails. Berikut merupakan implementasi percobaan profiling yang dilakukan:

1. Implementasi Percobaan *profiling* pada Aplikasi

Implementasi ini berisikan data yang mewakili saat melakukan profiling aplikasi dengan menggunakan *Tor Network* dan tanpa *Tor Network*. Beberapa aplikasi yang berdasarkan server *website* pada implementasi ini diakses dengan Tor Browser dan Unsafe Browser.

Tor Browser dalam percobaan ini diharuskan menggunakan Tor Network dikarenakan Tor Browser dapat diakses ketika Tor Aktif, sedangkan Unsafe Browser dapat diakses ketika menggunakan Tor Network dan tanpa Tor Network. Implementasi ini dijelaskan dengan menggunakan hasil percobaan dan penjelasan percobaan.

Tor *network* pada Tails merupakan sebuah jaringan *anonymn* yang membantu melindungi *privacy* pengguna dengan megenkripsi koneksi internet saat menjelajah internet. Jaringan ini bekerja dengan merutekan traffic *internet* melalui rangkaian server yang disebut “relays”. Setiap relay mengenkripsi traffic data melalui tiga relay yang berbeda.

1. Cara Kerja Tor Network Pada *Tails OS*

a. *Tunnels* (Node Acak)

Tor membuat jalur yang terdiri dari beberapa node acak melalui jaringan tor. Setiap node hanya mengetahui node sebelumnya dan node berikutnya, sehingga mempersulit pelacakan jalur dari pengguna ke tujuan akhir

b. *Relay Nodes*

Pada *relay node* akan merutekan traffic internet dengan 3 rangkaian *relay nodes* yaitu;

Entry Node (Guard) sebagai titik pertama yang dikenal oleh pengguna untuk masuk ke jaringan tor.

Middle Relay sebagai node perantara yang meneruskan lalu lintas dari *entry node* ke *exit node.*

Exit Node Sebagai node terakhir yang mengirimkan lalu lintas ke internet public dan tempat enkripsi terakhir dihapus.

c. *Encryption Layer*

Setiap lapisan *relay* menambahkan lapisan enkripsi atau menghapus lapisan enkripsi untuk menjaga data tetap aman dan *anonymn*.

2. Fungsi Tor Network Pada *Tails OS*

Adapun beberapa fungsi dan fitur yang tedapat pada *Tails OS* yaitu:

d. Menyembunyikan *Ip address*: Tor network menyembunyikan *Ip address* yang sebenarnya dengan merutekan *traffic* melalui jaringan *relay* yang kompleks. Dalam hal ini akan mempersulit pelacakan aktivitas *online* ke perangkat

e. Menyembunyikan Lokasi: Tor network membuat data lokasi yang berbeda dari Ip yang telah dienkripsi

f. Keamanan: Dengan menggunakan Tor, pengguna dapat menghindari *surveilans, censorship*, dan *virus.*

3. Keterbatasan Tor Network Pada *Tails OS*

Tor Network pada Tails OS memiliki beberapa keterbatasan yang penting untuk diperhatikan oleh pengguna yang mengandalkan sistem *anonymity* dan *privacy*. Berikut adalah beberapa keterbatasan Tor *network* pada Tails:

1. Kecepatan yang Lambat: Karena lalu lintas *internet* melalui tiga *relay* (*node*), kecepatan browsing dan pengunduhan bisa menjadi lambat dibandingkan dengan koneksi *internet* biasa. Ini karena setiap relay menambah latensi dan bandwith jaringan Tor terbatas.

4. Penyalahgunaan Jaringan Tor

Beberapa pengguna menyalahgunakan penggunaan jaringan tor, misalnya melalukan serangan *DDoS* atau penggunaan perangkat lunak *peer-to-peer* melalui jaringan tor dapat memperlambat jaringan.

D. Data Eksperimen

1. Hasil data Eksperimen Aplikasi

a. Onion Share

TABEL IV.4
Hasil Data Eksperimen Onion Share Menggunakan *Tor Network*

Browser	*Software*	*Input*	*Output*
Tor Browser	Onion Share	Add file yang ingin di *sharing*	Onion share menerima file yang di *add*
		Memilih *start sharing* seperti Gambar IV.7	Dikarenakan *start sharing* menggunakan Tor, *link sharing* dapat dibentuk dapat diakses menggunakan tor browser.
		Link yang dibentuk merupakan links yang berisikan file seperti Gambar IV.5	Link yang dibentuk kemudian diakses, hasil akses pada *link* tersebut merupakan file yang telah di *add* dan kemudian file tersebut dapat di *download* seperti Gambar IV.6, sehingga implementasi Onion Share ini memiliki fungsi *anonymity* dan *privacy*
		Link yang dibentuk pada Gambar IV.5 diakses	*Link* kemudian di copy pada Unsafe browser kemudian

		melalui unsafe browser.	dijalankan, hasil dari percobaan *link* tersebut terlihat hasil pada Gambar IV.8
Unsafe Browser		*Link* yang dibentuk pada Gambar IV.5 diakses melalui unsafe browser.	*Link* kemudian di copy pada Unsafe browser kemudian dijalankan, hasil dari percobaan *link* tersebut terlihat hasil pada Gambar IV.8

b. Pidgin OTR

TABEL IV 2
Hasil Data Eksperimen Pidgin dan OTR Menggunakan *Tor Network*

Software	*Input*	*Output*
Pidgin OTR	Membuat *buddy account* dengan menggunakan protokol XMPP seperti Gambar IV.9	Verifikasi *account* seperti *username*, *password*, dan captca.
	Account buddy berhasil dibuat.	*Account buddy* yang berhasil dibuat akan menampilkan status a*vailable*
	Komunikasi dapat dilakukan dengan memilih *new instant message*, *join chat,* dan atau *buddies* lain duluan melakukan chat. Seperti gambar IV.10	Komunikasi terjalin dengan cybesec@jabber.calyxinstitute.org dengan menggunakan *Tor network* seperti Gambar IV.10

c. Thunderbird

TABEL IV 3
Hasil Data Eksperimen Thunderbird Menggunakan Tor Network

Software	*Input*	*Output*
Thunderbird	Percobaan dilakukan dengan membuat kunci OpenPGP pada *sender* dan *receiver.*	Kunci OpenPGP yang dibuat dibentuk oleh Thunderbird, dan menunjukkan hasil kunci OpenPGP dan expired juga tertera seperti Gambar IV.12.
	Sender mengirim pesan enkripsi yang dimana receiver juga memiliki kunci OpenPGP.	Pesan yang dikirim berhasil dan pesan tersebut memiliki *manage security* seperti Gambar IV.14, *sender* dan *receiver* dapat membuka data *manage security* tersebut.

KeePassXC

TABEL IV 4
Hasil Data Eksperimen KeePassXC

Software	*Input*	*Output*
KeePassXC	Membuat *database*	Database dapat dibuat dengan beberapa langkah seperti membuat nama database, format yang digunakan, dan password database yang terlampir pada Gambar IV.16
	Membuat isi database dengan menambahkan data dengan menggunakan Entry pada KeePassXC, kemudian mengisi data seperti *title, username, password* untuk data, *URL*, *tags, expires*, dan *notes* seperti Gambar IV.17	Isi data yang berhasil dibuat dan disimpan pada KeePassXC, data tersebut ditampilkan pada KeePassXC seperti Gambar IV.18

d. Tor Browser

TABEL IV 5
Hasil Data Eksperimen Tor Browser

Software	*Input*	*Output*
Tor Browser	Konfigurasi Tor Network	Konfigurasi Tor Network berhasil, pengguna dapat membuka Tor browser dan dapat melakukan *browsing.*
	Mengakses uBlock Origin	Meskipun pada Tor browser tetap memblokir iklan pada halaman *web*, Tails menambahkan fitur uBlock Origin sesuai kebutuhan pengguna untuk mengakses *web*

		dengan *privacy* dan *anonymity*.
	Mengakses layanan *website* yang diblokir	Akses layanan berhasil dibuka, biasanya layanan yang diblokir dapat dilihat pada browsing di internet "The Hidden Wiki" terdapat beberapa kategori seperti Gambar IV.19. Contoh website yang diakses tersebut berada pada Gambar IV.23

e. Unsafe Browser

TABEL IV 6
Hasil Data Eksperimen Unsafe Browser

Software	*Input*	*Output*
Unsafe Browser	Tidak memerlukan konfigurasi Tor	Unsafe browser dapat dibuka ketika menggunakan dan tidak menggunakan *Tor network*
	Akses Layanan *website* secara langsung	Unsafe browser merespon ketika pengguna menggunakan alamat website yang benar seperti www.instagram.com, www.gmail.com
	Check history browsing	Unsafe browser menyertakan history browsing seperti Gambar IV.25, meskipun ketika Tails OS dimatikan history tersebut akan hilang tetapi tidak menjamin *anonymity* dan *privacy*.

f. Gmail

TABEL IV 7
Hasil Data Eksperimen Gmail Menggunakan Tor network

Browser	*Software*	*Input*	*Output*
Tor Browser	*Server* Gmail	Login gmail	Gmail dapat dibuka saat menggunakan Tor Browser seperti Gambar IV.26 yang memungkinkan bahwa Tor tidak membatasi penggunaan gmail saat menggunakan *Tor Network.*
		Kirim pesan melalui gmail	Kirim pesan juga dapat dilakukan ketika menggunakan tor browser seperti Gambar IV.26, letak *privacy* dan *anonymity* ini memungkinkan ketika pengguna mengakses gmail melalui Tor Network sehingga tidak akan mudah dalam pelacakan oleh pihak ketiga.
Unsafe Browser		Login Gmail	Login dapat dilakukan ketika mengakses gmail, tetapi penggunaan gmail pada unsafe browser tidak menjamin pengguna menjadi *anonymity* seperti gambar IV.27

g. Whatsapp

TABEL IV 8
Hasil Data Eksperimen Whatsapp

Browser	*Software*	*Input*	*Output*
Tor Browser	*Server Web* Whatsapp	Login whatsapp mengunakan scan barcode	Whatsapp web tidak membentuk *barcode* yang akan di *scan* sehingga tidak dapat dilakukan seperti Gambar IV.28, memungkinkan hal ini dikarenakan Whatsapp memblokir penggunaan Tor.
		Login whatsapp mengunakan *scan barcode*	Whatsapp web membentuk barcode kemudian di scan dari perangkat *gadget* merujuk pada Gambar IV.29
Unsafe Browser		Mengirim Pesan	Menampilkan pesan dan mensinkronisasikan pesan dari perangkat

			Gadget, sehingga dapat melakukan komunikasi seperti Gambar IV.29

h. Facebook

TABEL IV 9
Hasil Data Eksperimen Facebook

Browser	*Software*	*Input*	*Output*
Tor Browser	*Server Web* Facebook	Login Facebook	Menampilkan perizinan penggunaan *cookies.*
			Menampilkan beranda facebook, dan mencoba mengirim pesan seperti Gambar IV.30
Unsafe Browser		Login Facebook	Pada Unsafe Browser tidak menampilkan perizinan penggunaan *cookies.* Facebook juga menampilkan halaman beranda sama seperti pada Tor Browser setelah melakukan *login* merujuk pada Gambar IV.31

i. Instagram

TABEL IV 10
Hasil Data Eksperimen Instagram

Browser	*Software*	*Input*	*Output*
Tor Browser	*Server Web* Instagram	Login Instagram	Menampilkan perizinan penggunaan *cookies.*
			Menampilkan beranda Instagram seperti Gambar IV.34
Unsafe Browser		Login Instagram	Tidak menampilkan perizinan penggunaan *cookies,* dan juga menampilkan beranda Instagram seperti

			Gambar IV.35

j. Youtube

TABEL IV 11
Hasil Data Eksperimen Youtube

Browser	*Software*	*Input*	*Output*
Tor Browser	*Server Web* Youtube	Akses halaman Youtube	Menampilkan halaman youtube tanpa perlu *login* akun seperti Gambar IV.31.
Unsafe Browser		Akses halaman Youtube	Menampilkan halaman youtube tanpa perlu *login* akun seperti Gambar IV.32

2. Hasil data Eksperimen Networking

a. Tor Network

Hasil eksperimen ini menunjukkan hasil perbandingan server yang membentuk jaringan Ip yang dirutekan atau dienkripsi oleh Tor melalui tiga rute yaitu *entry node*, *middle relay*, dan *exit node*.

TABEL IV 12
Hasil Data Eksperimen Tor Network

Server	*Entry Node (Guard)*	*Middle Relay*	*Exit Node*
Tails.net (Gambar IV.37)	116.202.237.212 (Germany)	178.17.179.254 (Moldova)	185.241.208.206 (Poland)
Dnsleaktest.com (Gambar IV.38)	94.23.172.32 (Czechia)	148.251.136.16 (Germany)	54.36.209.254 (France)

b. DNS Leak Test

TABEL IV 13
Hasil Data Eksperimen DNS Leak Test

Browser	*Server*	*Input*	*Output*
Tor Browser	DNS Leak Test	*Check Ip address*	*Ip address*: 54.36.209.254 (*Exit Node Tor*, Gambar IV.38) *Location*: France
Unsafe Browser	DNS Leak Test	*Check Ip address*	*Ip address: 182.253.194.45* Gambar IV.39 Location: Bandung, Indonesia

c. VPN

TABEL IV 14
Hasil Data Eksperimen VPN

Browser	VPN	*Server*	*Input*	*Output*
Tor Browser	Proton VPN Server: Jepang	DNS Leak Test	*Check Ip address*	*Ip address*: 77.91.86.95 *Location*: Sweden, Stockholm

	VPN on			
	Proton VPN Server: Jepang VPN off	DNS Leak Test	*Check Ip address*	*Ip address: 77.91.86.95 Location*: Sweden, Stockholm
Unsafe Browser	Proton VPN Server: Jepang VPN on	DNS Leak Test	*Check Ip address*	*Ip address: 182.253.194.45 Location*: Bandung, Indonesia
	Proton VPN Server: Jepang VPN off	DNS Leak Test	*Check Ip address*	*Ip address:182.253.194.45 Location*: Bandung, Indonesia

IV.4.1 Hasil data Eksperimen *Storage Encryption*

1. Persistent Storage

TABEL IV 15
Hasil Data Eksperimen Persisten Storage

Fitur	Input	Output
Persistent Storage	File dan dokumen	Teks, gambar, dokomen LibreOffice
	Configuration system	*Turn on, turn off configuration (Personal document, system setting, network, application)*
	Additional Software	Aplikasi yang memiliki konfigurasi diinstal melalui terminal, menambahkan beberapa package untuk aplikasi eksternal
	Persistent Folder	Persistent, Tor Browser (persistent), Dotfiles, Tor Browser

2. LUKS (*Linux Unified Key Setup*)

TABEL IV 16
Hasil Data Eksperimen LUKS

Fitur	Input	Output
Membuat LUKS Volume	Menggunakan *system disk* (*USB Flashdrive*), menambahkan *volume name, type*, create password	LUKS *Created* dan dilindungi oleh *passphrase* (*password*) Gambar IV.46
Akses Direktori LUKS	Menggunakan File manager, Input Password	Menampilkan direktori file seperti gambar IV.45

V. ANALISA

A. Analisa Profiling

Pada bab ini akan dibahas dan dianalisis hasil dari eksperimen dan implementasi yang telah dilakukan yaitu profiling *anonymity* dan *privacy* berdasarkan tiga aspek yaitu aplikasi, *networking*, dan *storage*. Analisis ini mencakup evaluasi efektivitas penggunaan berbagai fitur *anonymity* dan *privacy* pada Tails. Analisa ini mencakup dua kondisi eksperimen yaitu ketiga menggunakan Tor, tanpa menggunakan tor, dan eksperimen server website menggunakan Tor Browser dan Unsafe Browser.

1. *Profiling* Aplikasi

Dalam skenario membutuhkan beberapa langkah langkah yang dilakukan untuk mewujudkan *profiling*. Pengujian ini berdasarkan perumusan analisis *profiling* yang akan divisualisasikan menggunakan *data flow diagram* untuk memberikan informasi secara visual.

B. Metrik Profiling

Metrik *profiling* dilakukan untuk mengidentifikasi ketiga aspek dari aplikasi, jaringan, dan *system storage* yang mempengaruhi aspek *anonymity* dan *prvacy*. Hasil *profiling* ini di buat berdasarkakn hasil implementasi *profiling* yang dilakukan dan sebagai penentu metrik yang digunakan.

1.*Report profiling*

TABEL V 1
Report *profiling*

Aplikasi	Menggunakan Tor	Tanpa Tor	Browser
Onion Share	✓	×	Hasil Link Sharing hanya dapat diakses pada Tor Browser
Pidgin dan OTR	✓	×	-
Tor Browser	✓	×	Tor Browser
Unsafe Browser	✓	✓	Unsafe Browser
Thunderbird	✓	✓	-
Gmail	✓	✓	Tor Browser, Unsafe Browser
Whatsapp	×	✓	Tor Browser, Unsafe Browser
Youtube	✓	✓	Tor Browser, Unsafe Browser
Instagram	✓	✓	Tor Browser, Unsafe Browser
Facebook	✓	✓	Tor Browser, Unsafe Browser

Pada Tabel V.1 merupakan tabel yang menunjukkan kemampuan aplikasi-aplikasi tertentu berfungsi dengan baik ketika menggunakan atau tidak menggunakan jaringan Tor. Tabel ini menunjukkan bahwa penggunaan jaringan Tor sangat penting untuk aplikasi-aplikasi yang membutuhkan

tingkat *anonymity* dan *privacy* yang tinggi. OnionShare, Pidgin OTR, dan Tor Browser hanya berfungsi optimal atau eksklusif melalui jaringan Tor karena kebutuhan *anonimity* dan keamanan.

Aplikasi seperti Thunderbird, Gmail, YouTube, Instagram, dan Facebook berfungsi baik dengan maupun tanpa Tor, tetapi penggunaan Tor memberikan lapisan tambahan privasi dengan menyembunyikan alamat IP pengguna. Namun, WhatsApp tidak mendukung penggunaan dengan jaringan Tor, yang menunjukkan keterbatasan dalam integrasi beberapa layanan dengan jaringan Tor.

Penggunaan browser juga bervariasi, di mana beberapa aplikasi lebih baik diakses melalui Tor Browser untuk menjaga privasi dan anonimitas, sementara yang lain dapat diakses melalui Unsafe Browser dengan risiko privasi lebih besar.

Secara keseluruhan, tabel ini menggarisbawahi pentingnya penggunaan Tor untuk aplikasi yang memprioritaskan anonimitas dan keamanan, meskipun beberapa aplikasi masih dapat berfungsi tanpa Tor dengan kompromi tertentu pada privasi.

C. Analisis Hasil Metrik Profiling

Analisis hasil metrik *profiling* ini didapatkan berdasarkan metrik *profiling* pada setiap aplikasi, *networking,* dan *storage*. Hasil analisis metrik dari tiga aspek tersebut pada penelitian ini berdasarkan hasil percobaan atau hasil eksperimen yang dilakukan. Hasil implementasi direpresentasikan dalam bentuk angka dan pernyataan yaitu 0 (No), dan 1 (Yes). Pengkuran yang direpresentasikan ini menggunakan *K-Anonymity* dan *Entropy Anonymity Degree (EAD)* pada jurnal "**A Survey of State-of-the-Art in Anonymity Metrics**" (Kelly et al., 2008).

g. K-*Anonymity* digunakan untuk tujuan menggambarkan penilaian fitur-fitur dan fungsi *anonymity* dan *privacy* sebagai acuan klasifikasi metrik pada tiga aspek; aplikasi, *networking,* dan *system storage.*
h. Entropy *Anonymity* Degree (EAD) digunakan untuk tujuan memberikan klasifikasi metrik dan *scoring* dalam menentukan fitur-fitur dan fungsi *anonymity* dan *privacy* yang tinggi dan rendah pada tiga aspek; aplikasi, *networking,* dan *system storage.*

D. Ringkasan Hasil Analisa Metrik Profiling

Ringkasan hasil analisa metrik profiling ini akan dijabarkan menjadi kesimpulan pada setiap tiga aspek yang berdasarkan hasil eksperimen atau hasil percobaan. Berikut merupakan hasil ringkasan:

V.4.1 Ringkasan Analisa Metrik Aplikasi

1. Onion Share: Berdasarkan Tabel V.5 bahwa hasil metrik yang terdapat pada Onion Share berdasarkan *profiling* terdapat metrik yang digunakan adalah *Metadata Control (Yes) Peering Communication on Tor (Yes), Essential functionality (Yes), Digital Trace (Yes), Registration Require (Yes)*
2. Pidgin OTR: Berdasarkan Tabel V.6 bahwa hasil metrik yang terdapat pada Pidgin OTR berdasarkan *profiling* terdapat metrik yang dapat digunakan adalah *Metadata Control (Yes) Peering Communication on Tor (Yes), Essential functionality (Yes), Digital Trace (Yes), Registration Require (Yes)*
3. Thunderbird: Berdasarkan Tabel V.7 bahwa hasil metrik yang terdapat pada Thunderbird berdasarkan *profiling* terdapat metrik yang dapat digunakan adalah *Metadata Control (Yes) Peering Communication on Tor (Yes), Essential functionality (Yes), Digital Trace (Yes), Registration Require (Yes)*
4. KeePassXC: Berdasarkan Tabel V.8 bahwa hasil metrik yang terdapat pada KeePassXC berdasarkan *profiling* terdapat metrik yang dapat digunakan adalah *Metadata Control (Yes) Peering Communication on Tor (Yes), Essential functionality (Yes), Digital Trace (Yes), Registration Require (Yes)*
5. Tor Browser: Berdasarkan Tabel V.9 bahwa hasil metrik yang terdapat pada Tor Browser berdasarkan *profiling* terdapat metrik yang dapat digunakan adalah *Metadata Control (Yes) Peering Communication on Tor (Yes), Essential functionality (Yes), Digital Trace (Yes), Registration Require (Yes)*
6. Unsafe Browser: Berdasarkan Tabel V.10 bahwa hasil metrik yang terdapat pada Unsafe Browser berdasarkan *profiling* terdapat metrik yang dapat digunakan adalah *Essential functionality (Yes), Registration Require (Yes)*
7. Layanan Gmail pada Tor Browser: Berdasarkan Tabel V.11 bahwa hasil metrik yang terdapat pada layanan Gmail berdasarkan *profiling* terdapat metrik yang dapat digunakan adalah *Peering Communication on Tor (Yes), Essential functionality (Yes), Digital Trace (Yes).*
8. Layanan WhatsApp pada Tor Browser: Berdasarkan Tabel V.12 bahwa hasil metrik yang terdapat pada layanan Gmail berdasarkan *profiling* terdapat metrik yang dapat digunakan adalah *Digital Trace (Yes)*
9. Layanan Facebook pada Tor Browser: Berdasarkan Tabel V.13 bahwa hasil metrik yang terdapat pada layanan Facebook berdasarkan *profiling* terdapat metrik yang dapat digunakan adalah *Peering Communication on Tor (Yes), Essential functionality (Yes), Digital Trace (Yes).*
10. Layanan YouTube pada Tor Browser: Berdasarkan Tabel V.14 bahwa hasil metrik yang terdapat pada layanan YouTube berdasarkan *profiling* terdapat metrik yang dapat digunakan adalah *Peering Communication on Tor (Yes), Essential functionality (Yes), Digital Trace (Yes).*
11. Layanan Instagram pada Tor Browser: Berdasarkan Tabel V.15 bahwa hasil metrik yang terdapat pada layanan Instagram berdasarkan *profiling* terdapat metrik yang dapat digunakan adalah *Peering Communication on Tor (Yes), Essential functionality (Yes), Digital Trace (Yes).*

V.4.2 Ringkasan Analisa Metrik Networking

1.Tor *Network*: Berdasarkan Tabel V.16 bahwa hasil metrik yang terdapat pada Tor *network* berdasarkan *profiling* terdapat metrik yang dapat digunakan adalah *Compatibility Tor (Yes), Tor Circuit (Yes), Essential functionality (Yes), Digital Trace (Yes)*
2. Dnsleaktest: Berdasarkan Tabel V.17 bahwa hasil metrik yang terdapat pada Dnsleaktest berdasarkan *profiling* terdapat metrik yang dapat digunakan adalah *Compatibility Tor (Yes), Tor Circuit (Yes), Essential functionality (Yes), Digital Trace (Yes)*
3.VPN: Berdasarkan Tabel V.18 bahwa hasil metrik yang terdapat pada Dnsleaktest berdasarkan *profiling* terdapat metrik yang dapat digunakan adalah *Digital Trace (No)*

V.4.3 Ringkasan Analisa Metrik *System Storage*

1. Persistent Storage: Berdasarkan Tabel V.19 bahwa hasil metrik yang terdapat pada Persistent Storage berdasarkan *profiling* terdapat metrik yang dapat digunakan adalah *System*

Encryption (yes), Backup data (Yes), User Access Control (Yes), Compability with Other Tools (*Yes*).

2. LUKS: Berdasarkan Tabel V.20 bahwa hasil metrik yang terdapat pada LUKS berdasarkan *profiling* terdapat metrik yang dapat digunakan adalah *System Encryption (Yes), User Access Control (Yes).*

VI. KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan tiga aspek *profiling* aplikasi*, networking,* dan *storage Tails* berikut kesimpulan yang didapatkan:

1. *Data Flow Diagram*

Data flow diagram disusun berdasarkan implementasi *profiling* dan merupakan hasil tahapan profiling anonymity dan privacy pada Tails OS. Pada layanan aplikasi Tails OS terdapat aplikasi yang bergantung pada jaringan Tor untuk dapat digunakan seperti aplikasi Onion Share (*sharing file*), Pidgin (aplikasi *chatting*), Thunderbird (pesan enkripsi). Pada aplikasi *browser* seperti Tor Browser dan beberapa layanan aplikasi yang diakses secara *online,* tidak sepenuhnya menerapkan fungsi *anonymity* dan *privacy* karena pengguna hanya *anonymous* dalam bentuk identitas IP yang dienkripsi oleh Tor. Pilihan aplikasi ini diharapkan disesuaikan dengan kebutuhan pengguna dalam menjaga *anonymity* dan *privacy* dalam digitalisasi. Pada *networking* terdapat jaringan Tor yang telah diuji yang menerapkan pengguna menjadi *anonymity* dan *privacy* dan pada layanan Dnsleaktest membantu dalam menguji pada kebocoran jaringan Tor. Pada aplikasi KeePassXC yang tidak memerlukan jaringan Tor dapat membantu pengguna untuk menyimpan dan mengelola berbagai password *database* dan informasi penting lainnya dalam satu tempat yang aman.

2. Metrik yang digunakan

Secara keseluruhan, metrik yang digunakan dalam penelitian ini memberikan gambaran yang komprehensif tentang fungsi aplikasi, *networking*, dan *system storage* dalam menjaga *anonymity* dan *privacy.* Dari hasil metrik yang didapatkan pada metrik aplikasi terdapat aplikasi seperti Onion Share, Pidgin OTR, dan layanan aplikasi browser seperti Tor Browser yang memiliki fungsi *anonymity* dan *privacy* seperti metrik sedangkan *profiling* berdasarkan layanan Facebook, YouTube, Instagram, Gmail tidak sepenuhnya memikili fungsi *anonymity* dan *privacy* Hasil *profiling* yang tidak mewujudkan *anonymity* dan *privacy* terdapat pada Unsafe Browser. Metrik pada *networking* yang mewujudkan *anonymity* dan *privacy* terletak pada Tor *network* dan Dnsleaktest karena tidak adanya *digital trace* sehingga pengguna menjadi *full anonymous.* Metrik *system storage* yang mewujudkan *anonymity* dan *privacy* adalah Persistent Storage dan LUKS tidak sepenuhnya mewujudkan *anonymity* dan *privacy*.

3. Aplikasi, *networking, system storage*

Tiga kategori aplikasi, *networking, system storage* yang memiliki kategori *anonymity* dan *privacy* pada Tails OS seperti sistem yang menggunakan jaringan terenkripsi, sistem yang mengelola data penting tanpa memerlukan jaringan terenkripsi, ketiga aspek ini dapat digunakan pada Tails OS untuk menghasilkan lingkungan sistem yang lengkap dengan *anonymity* dan *privacy.*

i. Metrik yang relevan pada *profiling anonymity* dan *privacy* terhadap aspek aplikasi yaitu:

Hasil metrik yang secara penuh mewujudkan dan terpenuhi pada profiling *anonymity* dan *privacy* pada aspek aplikasi adalah Onion Share, Pidgin OTR, KeePassXc, Thunderbird dan Tor Browser dengan menyatakan skor Yes sebanyak 5 dari hasil ke-5 metrik yaitu adalah *Metadata Control, Peering Communication on Tor, Essential functionality, Digital Trace,* dan *Registration Require.* Hasil metrik yang tidak sepenuhnya mewujudkan *anonymity* dan *privacy* terdapat pada social media yang di akses melalui Tor Browser dengan hasil menyatakan skor Yes sebanyak 3 dari hasil ke-5 metrik yaitu *Peering Communication on Tor, Essential functionality, Digital Trace.* Hasil metrik yang tidak mewujudkan *anonymity* dan *privacy* terdapat pada Unsafe Browser dengan hasil menyatakan skor Yes sebanyak 2 dari hasil ke-5 metrik yaitu *Essential functionality,* dan *Registration Require.*

j. Metrik yang relevan mewujudkan *anonymity* dan *privacy* terhadap aspek *networking* yaitu:

Hasil yang secara penuh mewujudkan dan terpenuhi pada *profiling anonymity* dan *privacy* pada aspek *networking* adalah Tor dan Dnsleaktest dengan hasil skor Yes sebanyak 4 dari hasil ke-4 metrik yaitu *Compatibility Tor, Tor Circuit, Essential functionality,* dan *Digital Trace.* Hasil metrik yang tidak mewujudkan *anonymity* dan *privacy* adalah VPN dengan hasil skor Yes 0 dari ke-4 metrik.

k. Metrik yang relevan mewujudkan *anonymity* dan *privacy* terhadap aspek *system storage* yaitu:

Pada aspek system storage yang memenuhi *anonymity* dan *privacy* adalah Persisten Storage dengan hasil skor Yes sebanyak 4 dari ke-4 metrik yaitu *System Encryption, Backup data, User Access Control, Compatibility with other Tools*.

Sedangkan LUKS dengan hasil skor Yes sebanyak 2 dari ke-4 metrik yaitu *System Encryption,* dan *User Access Control* bahwa LUKS tidak sepenuhnya *anonymity* dan *privacy*. Tambahan yang mewujudkan pengguna menjadi *anonymity* dan *privacy* pada lingkungan Tails OS ini juga terdapat pada penggunaan sistem operasi dengan menggunakan *USB Flashdrive* atau *DVD.*

B. Saran

Sebagai saran yang dapat digunakan sebagai masukan lanjutan dari penelitian ini adalah sebagai berikut

1. Potensi penelitian lanjutan untuk pengembangan Tails OS, pemgembangan pada repositori sehingga banyak aplikasi memiliki ketergantungan yang tidak ada di repositori Tails, sehingga pengguna sulit dalam menginstal aplikasi eksternal.
2. Penelitian lebih lanjut terkait jaringan Tor, karena aspek pada kecepatan akses ketika menggunakan Tor lebih lambat saat melakukan pengunduhan dan *browsing internet.*
3. Penelitian terkait dengan rincian metrik dalam bentuk kuantitatif dengan aspek tambahan terkait kerentanan dan *threat* seperti eksploitasi pada fungsi Tails OS.

REFERENSI

Rini, L. N., & Manalu, R. (n.d.). Memahami penggunaan dan motivasi akun anonim Instagram di kalangan remaja. Program Studi S1 Ilmu Komunikasi, Fakultas Ilmu Sosial dan

Ilmu Politik, Universitas Diponegoro*29570-63288-1-SM.pdf*. (n.d.).

Abraham, S., Silva, T., Decourcy, R., & Cardon, J. (n.d.). *... and other tools for Safeguarding Online Activities*.

Hamdani, S. W. A., Abbas, H., Janjua, A. R., Shahid, W. B., Amjad, M. F., Malik, J., Murtaza, M. H., Atiquzzaman, M., & Khan, A. W. (2022). Cybersecurity Standards in the Context of Operating System: Practical Aspects, Analysis, and Comparisons. *ACM Computing Surveys*, *54*(3), 1–36. https://doi.org/10.1145/3442480

Hulina, A. (2020). *Operating systems for privacy and anonymity: A survey*.

Kelly, D. J., Raines, R. A., Grimaila, M. R., Baldwin, R. O., & Mullins, B. E. (2008). A survey of state-of-the-art in anonymity metrics. *Proceedings of the 1st ACM Workshop on Network Data Anonymization*, 31–40. https://doi.org/10.1145/1456441.1456453

Meiliana, L. C. D. (2012). *ANALISIS DAN PERANCANGAN APLIKASI SPESIFIKASI METRIK*.

Stefanos Gritzalis. (2004). Enhancing Web privacy and anonymity in the digital era. *Information Management & Computer Security*, *12*(3), 255–287. https://doi.org/10.1108/09685220410542615

Wardoyo, S., Ryadi, T., & Fahrizal, R. (2014). ANALISIS PERFORMA FILE TRANSPORT PROTOCOL PADA PERBANDINGAN METODE IPv4 MURNI, IPv6 MURNI DAN TUNNELING 6to4 BERBASIS ROUTER MIKROTIK. *Jurnal Nasional Teknik Elektro*, *3*(2).

Yuwinanto, H. P. (n.d.-b). *PRIVASI ONLINE DAN KEAMANAN DATA*.

Dawson, M., & Cárdenas-Haro, J. A. (2017). Tails Linux operating system. *International Journal of Hyperconnectivity and the Internet of Things*, *1*(1), 47-55. https://doi.org/10.4018/ijhiot.2017010104