Journal of Information System Research (JOSH)
Volume 6, No. 1, Oktober 2024, pp 23−33
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v6i1.5682

Implementation and Analysis of Profiling Mechanism for Anonymity and Privacy on Whonix Operating System

Yana J.S Batunanggar*, Adityas Widjajarto, M Tegoeh Kurniawan

Faculty of Industrial Engineering, Information System, Telkom University, Bandung
Jl. Telekomunikasi. 1, Terusan Buahbatu - Bojongsoang, Telkom University, Sukapura, Kec. Dayeuhkolot, Kabupaten Bandung, Jawa Barat, Indonesia
Email: [1,*]yanajsbatunanggar@student.telkomuniversity.ac.id, [2]adtwjrt@telkomuniversity.ac.id, [3]teguhkurniawan@telkomuniversity.ac.id
Correspondence Author Email: yanajsbatunanggar@student.telkomuniversity.ac.id
Submitted: **25/07/2024;** Accepted: **05/09/2024;** Published: **13/10/2024**

Abstract−This research will implement anonymity using the Whonix operating system. This research seeks to analyze the features of the Whonix operating system that can support anonymity and privacy profiling, the function of anonymity and privacy profiling on the operating system, and the character of the operating system capable of maintaining anonymity and privacy. Features owned by the Whonix operating system that support anonymity and privacy profiling on Whonix are application, network, and operating system aspects, as well as analyzing anonymity and privacy functions with metrics. This research produces metrics on each aspect. The application aspect obtained metrics of data encryption, metadata protection, and privacy by design by analyzing profiling experiments on KeePassXC and GnuPG applications. The network aspect uses Tor compatibility, IP Address obfuscation, and logging policy metrics by analyzing profiling experiments on Wireguard and DNSLeakTest. While the operating system aspect uses data encryption, logging and monitoring, and access control metrics by analyzing profiling experiments with fingerprinting and backup and restore scenarios. The results of this study obtained scoring profiling of the Whonix operating system, application aspect profiling scenarios with a score of 1o, network aspects with a total score of 11, and operating system aspects with a total score of 10. So it is obtained from the results of this study that all aspects of the application, network, and operating system were successful by 97% as measured based on the measurement metrics of each aspect.

Keywords: Anonymity; Privacy; Profiling; The Onion Router (TOR); Digital

1. INTRODUCTION

The urgency of the cybersecurity domain is directly proportional to the dependence of aspects of life on digital activities. Today, cybersecurity safeguards this data from unauthorized access, theft, or manipulation, ensuring the privacy and security of individuals and organizations[1]. Cybersecurity focuses on protecting the confidentiality, integrity, and availability of assets known as CIA: confidentiality, integrity, and availability [2]. These aspects are protected because attackers commonly utilize them to gather activities to target for attack and exploitation. As a user on digital activities, it cannot detect the aspects that will be used by the attacker. Therefore, users can utilize the concept of anonymity, which is a condition where the user's identity is hidden so that it cannot be identified or traced [3]. Many methods can implement anonymity, such as using privacy networks, controlling digital footprints, and The Onion Router (Tor) network. Tor provides a service with multiple layers of encryption, preventing anyone from tracking the pages a user visits [4]. This research will implement anonymity in digital activities using the Whonix operating system. Whonix is a Debian distro that supports anonymity and privacy when exploring digital activities [3][5]. Whonix utilizes the Tor network, which allows users to explore digitalization anonymously[5].

Whonix is an operating system specifically designed to ensure the privacy and anonymity of its users [5]. It consists of two main virtual machines: Whonix Gateway is internal virtual network interface which serves as the Tor connection manager [6]. While Whonix Workstation, where users run applications and perform daily activities [7]. By separating these functions, Whonix offers higher security as attacks on the workstation will not reveal the user's true identity. This research focuses on profiling the Whonix operating system in maintaining privacy and anonymity. Profiling is the process of collecting data and analyzing how a system behaves or how a feature works [4], [8]. In this context, profiling is done using application features that are successfully implemented and grouped into three aspects: applications, networks, and operating systems. Profiling is done to evaluate whether this operating system truly supports privacy and anonymity in digital activities.

The problem formulation that is the reference of this research is as follows: How can operating system features support profiling anonymity and privacy in digital activities? How does profiling anonymity and privacy function on the operating system? And how is the character of the operating system able to maintain anonymity and privacy in digital activities?

To answer the formulation of the problem, this research aims to identify features owned by the Whonix operating system that support profiling anonymity and privacy in digital activities, analyze aspects that need to be maintained in digital activities as a function of profiling anonymity and privacy in Whonix, and analyze Whonix into an operating system to maintain anonymity and privacy in digital activities. The limitations of this research are: This research is based on experimental and simulation results on the Whonix operating system; the profiling aspects carried out are applications, networks, and operating systems; and simulations are carried out in virtual machines where there are possible configuration differences with the operating system installed on the hardware.

Journal of Information System Research (JOSH)
Volume 6, No. 1, Oktober 2024, pp 23−33
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v6i1.5682

With these limitations, the research will be more focused and the results obtained are more accurate in the context of using Whonix in a controlled environment.

The benefits obtained by this research can be divided into two categories, namely theoretical benefits and practical benefits. Theoretically, this research adds insight into operating systems that can be used for anonymity and privacy and recognizes the characters that must be owned by the operating system to support anonymity and privacy. This is important because researchers also act as users who explore digitalization, so a deep understanding of operating systems such as Whonix will be very useful.

Practically, this research can measure the effectiveness of the Whonix operating system in supporting anonymity and privacy. By testing the features and mechanisms in Whonix, researchers can determine how well this operating system protects user identity and data. In addition, this research can also help other users in utilizing the features owned by the Whonix operating system in exploring digitalization more safely and anonymously.

Thus, this research makes a significant contribution both in terms of scientific development in the field of cybersecurity and in practical applications to protect user privacy and anonymity. The results of this research are expected to be a reference for users and operating system developers in developing and using technologies that support privacy and anonymity. Profiling the Whonix operating system will provide a clear picture of how this system works and how effective it is in protecting users from digital threats.

2. RESEARCH METHODOLOGY

2.1 Research Stages

The stages carried out in this study include 6 stages, namely: Initial Stage, Hypothesis, Experiment Design Stage, Experiment Stage, Analysis Stage, and Final Stage.

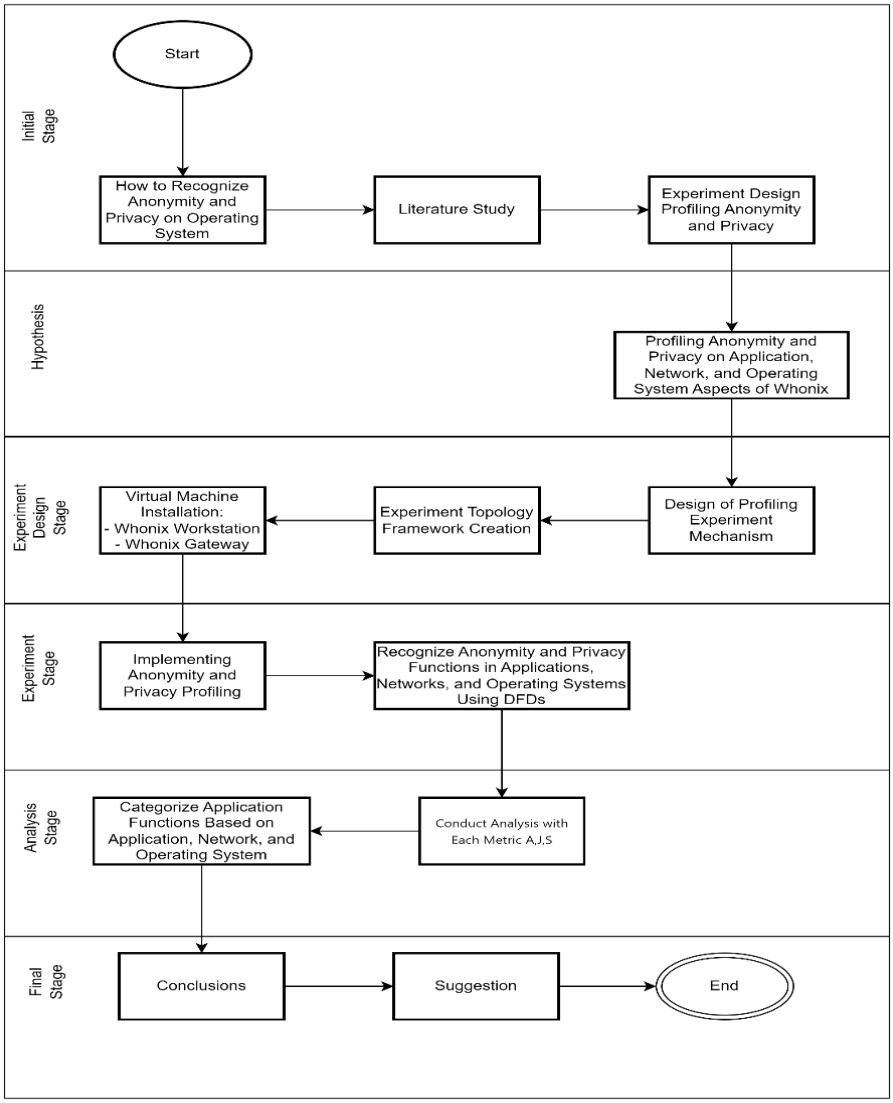

Figure 1. Research Stages

Journal of Information System Research (JOSH)
Volume 6, No. 1, Oktober 2024, pp 23−33
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v6i1.5682

Figure 1 represents the stages of research that begin at the initial stage, namely the profiling stage of anonymity and privacy in Whonix. Then a summary of the literature study is carried out to make guidelines, followed by compiling a profiling experiment design and continued by installing Whonix. Then the second stage is the hypothesis stage, which is declaring the conditions before the profiling experiment is carried out. The third stage of experimental design is by drafting the profiling experiment mechanism, drafting the experimental topology framework, and installing the operating system. Furthermore, in the fourth stage of the experimental stage, namely taking notes before, during, and after the implementation of anonymity and privacy profiling. The fifth stage is the analysis stage, which compares the results by measuring the profiling aspects of anonymity and privacy with metrics. The sixth stage is the final stage by summarizing the results of the analysis and drawing conclusions from the experimental results and making suggestions for further research guidelines.

2.2 Conceptual Framework

A conceptual framework is a visual representation that provides an abstract picture of the structure, components and relationships of the elements involved in the research or development [9], [10]. In this context, the concept of a model can also be understood as a diagram that depicts the relationship between certain factors, as explained [10]. The conceptual framework in this study is as follows:

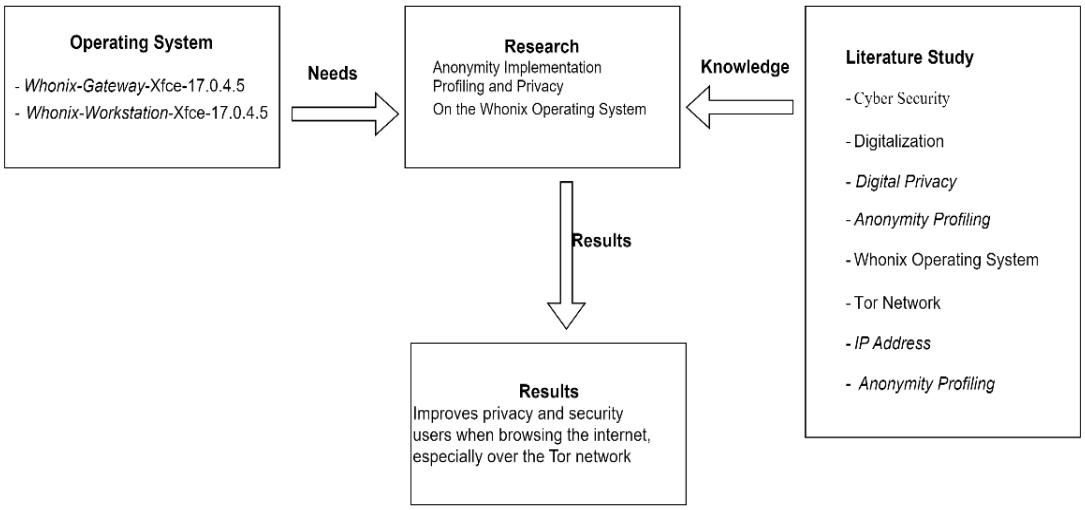

Figure 2. Conceptual Framework

Figure 2 explains that the conceptual model in this study is divided into 3 parts, namely requirements, research, and theoretical basis. In the requirements there are operating systems, namely Whonix-Workstation-Xfce and Whonix-Gateway-Xfce. Whonix is a Linux distribution designed to increase user privacy and security when browsing the Internet by utilizing the Tor network. Whonix is based on Debian. Whonix is divided into 2 separate virtual machines: one for the environment (Workstation) and for the Tor network service (Gateway). This gateway functions as a router that directs Tor traffic. While the Workstation serves as the environment where applications and Internet activities take place. In the research section, there are artifacts of the results produced, namely, to Improve user privacy and security when browsing the Internet, especially through the Tor network. Followed by the theoretical basis used to obtain the expected output as stated in the conceptual framework above.

2.3 Data Collection

The focus is on the implementation of profiling on the Whonix operating system with the aim of analyzing the operating system that supports the implementation of anonymity and privacy. The collected data will be categorized based on experimental aspects, namely applications, networks, and operating systems.

2.4 Data Processing

Data processing is done by comparing data conditions before and after profiling implementation. Analysis is carried out based on the size of the metric by considering the impact on the features owned by the application installed on Whonix. The resulting data will be analyzed using the metric categories of each aspect that have been defined in the profiling testing framework.

2.5 Evaluation Method

The evaluation method in profiling anonymity and privacy on Whonix Linux is based on the aspect of influence on the features of the applications installed on Whonix. The evaluation is carried out with reference to the profiling testing framework, and the results are used to determine the extent to which Whonix can support the desired level of anonymity and privacy.

Journal of Information System Research (JOSH)
Volume 6, No. 1, Oktober 2024, pp 23−33
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v6i1.5682

3. RESULT AND DISCUSSION

In this chapter, the process of analyzing the results of anonymity profiling testing on the three aspects of applications, networks, and operating systems is carried out. The purpose of this analysis is to represent Whonix's ability to do profiling. The experimental scenario includes conditions, namely experiments when Tor is disabled.

3.1 Application Profiling

3.1.1 Analysis of KeePassXC Anonymity/Privacy Function Mechanism

KeePassXC is an open-source password manager used to securely store and manage passwords [11]. The following is the Data Flow Diagram (DFD) profiling the KeePassXC application:

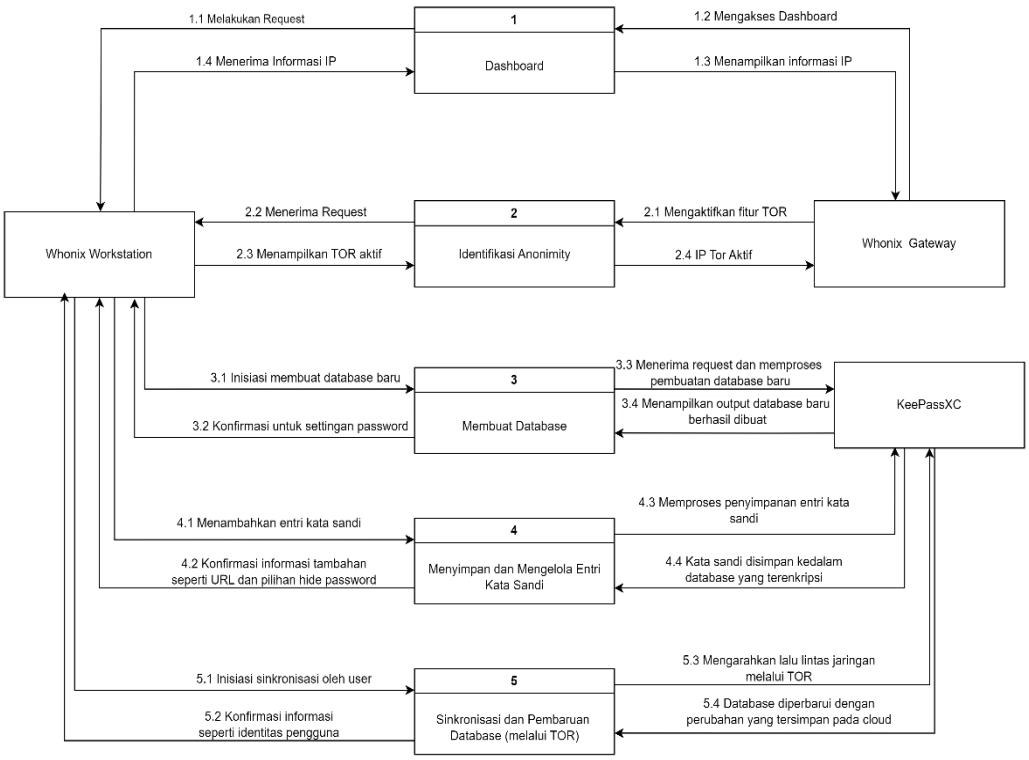

Figure 3. KeePassXC Function Mechanism

Figure 3 explains KeePassXC uses strong mechanisms to maintain the anonymity and privacy of its users. The use of Tor to manipulate network traffic ensures that the user's identity and activities remain hidden. A strict encryption process ensures that the password data stored in the database remains secure and inaccessible to unauthorized parties. This mechanism guarantees that every step from database creation to synchronization is done with a high level of security and privacy.

3.1.2 KeePassXC Profiling Results

The k-anonymity method is a technique that transforms data so that the published dataset has at least k tuples with the same attributes and values[12]. KeePassXC profiling uses scoring K-Anonymity standards.: 0 representing No, 1 representing Partially, and 2 representing Yes.

Table 1. KeePassXC profiling results

No	Aspects	Score
1	Data Encryption	2
2	Metadata Protection	1
3	Privacy by Design	2
	Total Score	**5**

In Table 1 KeePassXC profiling results represents scoring through implementation results as follows:

a. Data Encryption: 2 (Yes)
   KeePassXC uses the Advanced Encryption Standard (AES) encryption algorithm with a 256-bit key size. AES is a highly secure encryption standard that is widely recognized in the information security industry. Any data entered into the KeePassXC database, including usernames, passwords, notes, and attachment files, is encrypted using AES-256. [13]

Journal of Information System Research (JOSH)
Volume 6, No. 1, Oktober 2024, pp 23−33
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v6i1.5682

b. Metadata Protection: 1 (Partially)
Although the content in the KeePassXC database is encrypted, metadata such as the database file name and file size are not encrypted. This information remains accessible and can be used for specific purposes. KeePassXC does not have any special features to encrypt or hide metadata. However, using KeePassXC in a Tor/Whonix network environment can help protect identities anonymously during transmission over the Tor network.

c. Privacy By Design: 2 (Yes)
KeePassXC was designed with privacy in mind from the start.This includes the use of strong encryption (AES-256) and minimization of data collection. KeePassXC does not collect or store user data apart from the encrypted database stored locally. KeePassXC has features such as clipboard clearing and auto-lock to minimize user footprint and prevent unauthorized access.

3.1.3 Mechanism Analysis of GnuPG Anonymity/Privacy Function

GnuPG (GNU Privacy Guard) is a cryptographic tool used to encrypt and decrypt data before it is sent as well as to sign and verify digital signatures [14].
The following is the Data Flow Diagram (DFD) profiling the GnuPG application:

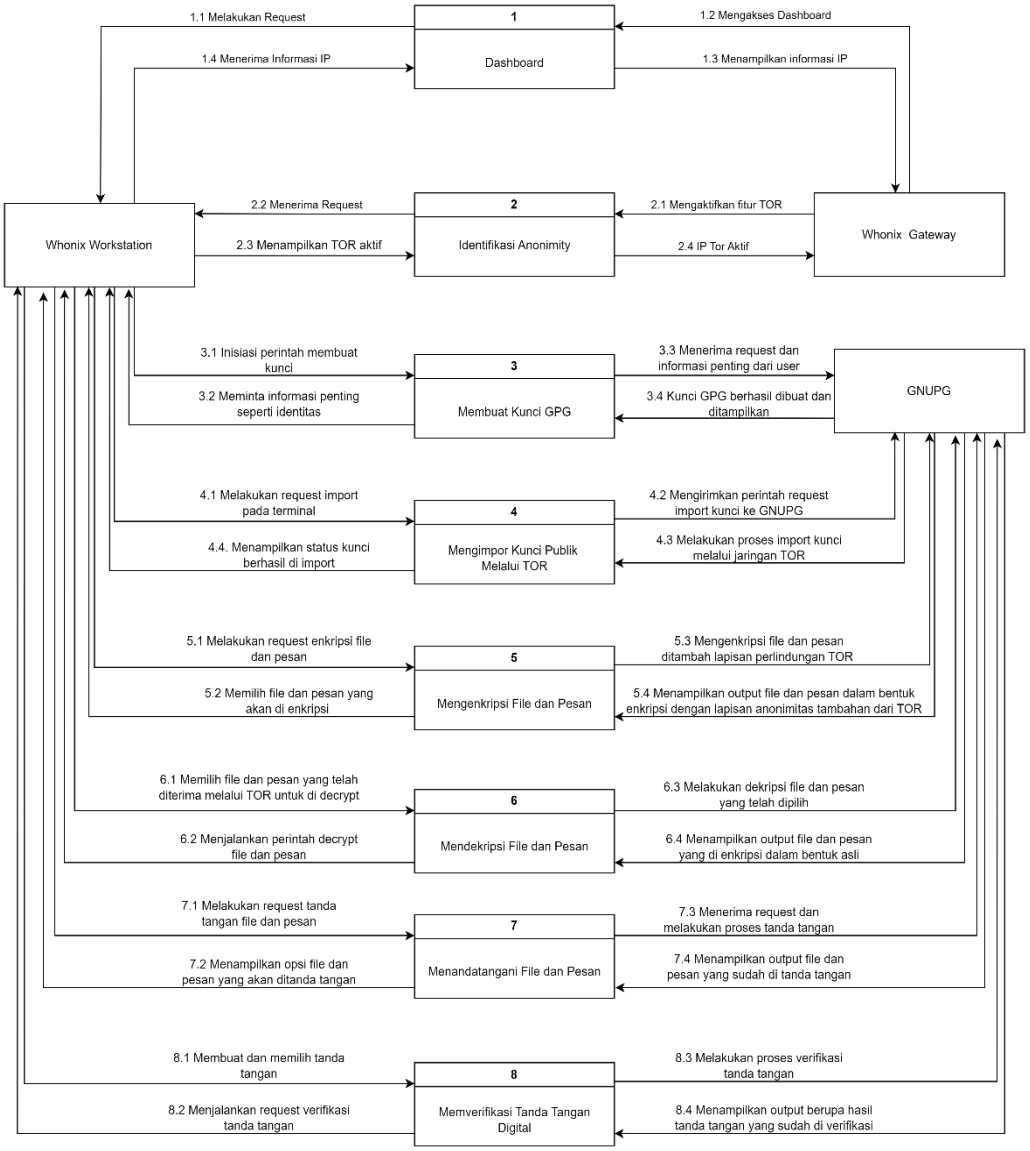

Figure 4. GnuPG Function Mechanism

Figure 4 respresents anonymity and privacy function mechanism in GnuPG with Tor enabled ensures that any cryptographic activities, such as key generation, public key import, message encryption and decryption, and digital signature signing and verification, are performed with anonymity protection through the Tor network. As such, all communications and data processed remain encrypted and protected from prying eyes, and the identity

Journal of Information System Research (JOSH)
Volume 6, No. 1, Oktober 2024, pp 23−33
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v6i1.5682

of the user remains anonymous thanks to Tor's use of obfuscated IP addresses. This adds an additional layer of security, preserving user privacy at every stage of the cryptographic process.

3.1.4 GnuPG Profiling Results

The k-anonymity method is a technique that transforms data so that the published dataset has at least k tuples with the same attributes and values[12]. GnuPG profiling uses scoring 0 representing No/, 1 representing Partially, and 2 representing Yes.

Table 2. GnuPG profiling results

No	Aspects	Score
1	Data Encryption	2
2	Metadata Protection	2
3	Privacy by Design	1
	Total Score	**5**

In Table 2. GnuPG profiling resuls represents scoring through implementation results as follows:

a. Data Encryption: 2 (Yes)
   GnuPG supports very strong OpenPGP (RFC4880) encryption for email and file transmission needs [15]. This ensures that encrypted data is only accessible to the recipient. With Tor on, GnuPG data encryption remains unaffected but gains an additional layer of security from the Tor anonymizing network.
b. Metadata Protection: 2 (Partially)
   GnuPG protects the contents of messages and files, but metadata such as sender, recipient, and time of delivery are not explicitly encrypted. With Tor on, network metadata (such as IP address and location) becomes harder to trace, although metadata related to the message itself can still be exposed.
c. Privacy by Design: 1(Partially)
   GnuPG is designed with user privacy in mind, but the implementation of this privacy depends on the proper use of the tool by the user. With Tor enabled, the use of GnuPG in the message encryption and decryption process will help maintain user privacy, especially when communicating over the secure and anonymous Tor network.

3.2 Network Profiling

3.2.1 Anonymity/Privacy Wireguard Function Mechanism Analysis

WireGuard can be defined as a new open-source secure tunneling VPN protocol [16]. Wireguard designed to be faster, simpler and more efficient [17]. Wireguard gave better results during the latency test with an average latency of 28.56 ms [18]. Here is the Data Flow Diagram (DFD) of Wireguard profiling with Tor active:

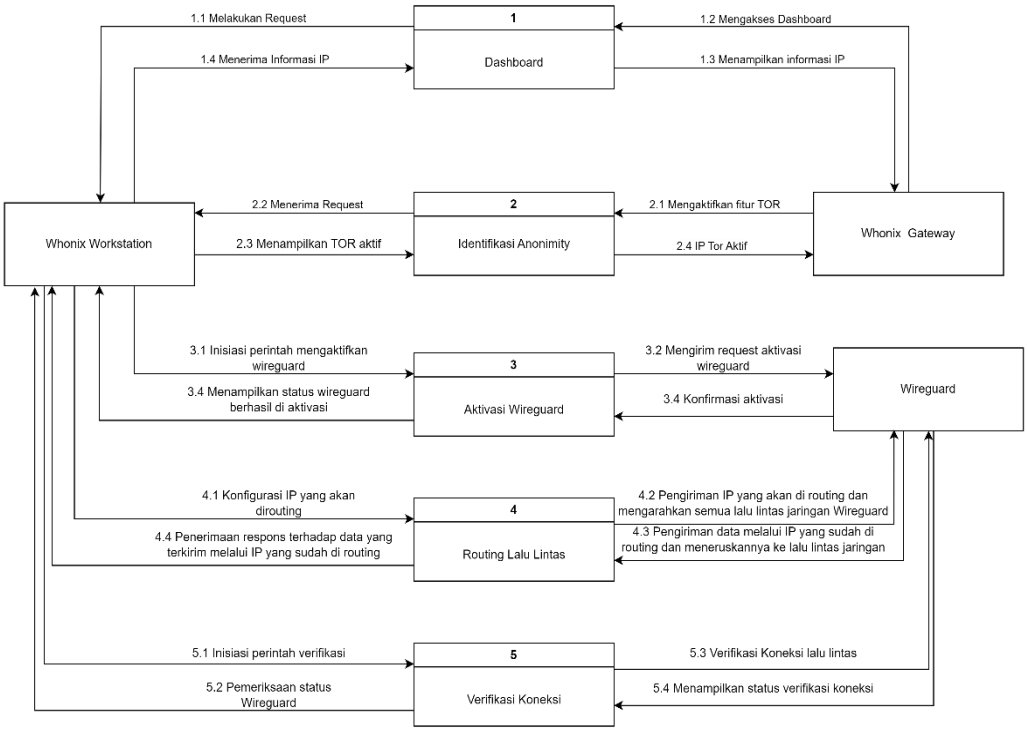

Figure 5. Wireguard Function Mechanism

Journal of Information System Research (JOSH)
Volume 6, No. 1, Oktober 2024, pp 23−33
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v6i1.5682

Figure 5 represents WireGuard's anonymity and privacy function mechanisms ensure that all network communications made through this VPN protocol remain encrypted and protected from prying eyes. By using modern cryptographic keys, WireGuard hides the original user's IP address and maintains the privacy of data sent over the network. This provides additional anonymity, ensuring that the user's identity and data remain secure in every connection made.

3.2.2 Wireguard Profiling Results

The k-anonymity method is a technique that transforms data so that the published dataset has at least k tuples with the same attributes and values[12]. Wireguard profiling uses scoring 0 representing No, 1 representing Partially, and 2 representing Yes. The following is a table of Wireguard profiling measurements:

Table 3. Wireguard profiling results

No	Aspects	Score
1	Tor Compatibility	2
2	IP Address Obfuscation	2
3	Logging Policy	2
	Total Score	**6**

In Table 3. Wireguard Profiling Results represents scoring through implementation results as follows:

a. Tor Compatibility: 2 (Yes)
   Wireguard can be used with Tor in Whonix. In the correct configuration, Wireguard can work alongside Tor, ensuring all traffic through Wireguard runs through the Tor network. Whonix is designed to route all network traffic through Tor, including VPN traffic, which makes Wireguard compatible with Tor within a Whonix environment.
b. IP Address Obfuscation: 2 (Yes)
   Wireguard is not specifically designed to hide user IP addresses from end nodes. However, when properly configured inside a Whonix that uses Tor, a user's real IP address can be hidden. This requires additional configuration to ensure that the real IP address is not visible to Wireguard nodes. The use of Tor within Whonix can hide the original IP address, but this requires technical settings that are not readily available in the standard Wireguard configuration.
c. Logging Policy: 2 (Yes)
   Wireguard has no explicit logging policy, but its minimalist design means there is no logging of user activity by default. However, logging policies may vary depending on the specific implementation and VPN service provider using Wireguard. The use of Wireguard within Whonix with Tor adds an additional layer of protection, reducing the risk of logging that could reveal info to users.

3.2.3 Analysis of DNSLeakTest Anonymity/Privacy Function Mechanism

DNSLeakTest is a testing process to ensure that DNS (Domain Name System) requests made by the operating system do not leak to unwanted DNS servers. DNS requests made by user while browsing the internet are possibly exposed to the ISP [19]. The following is the Data Flow Diagram (DFD) of DNSLeakTest profiling with Tor active:

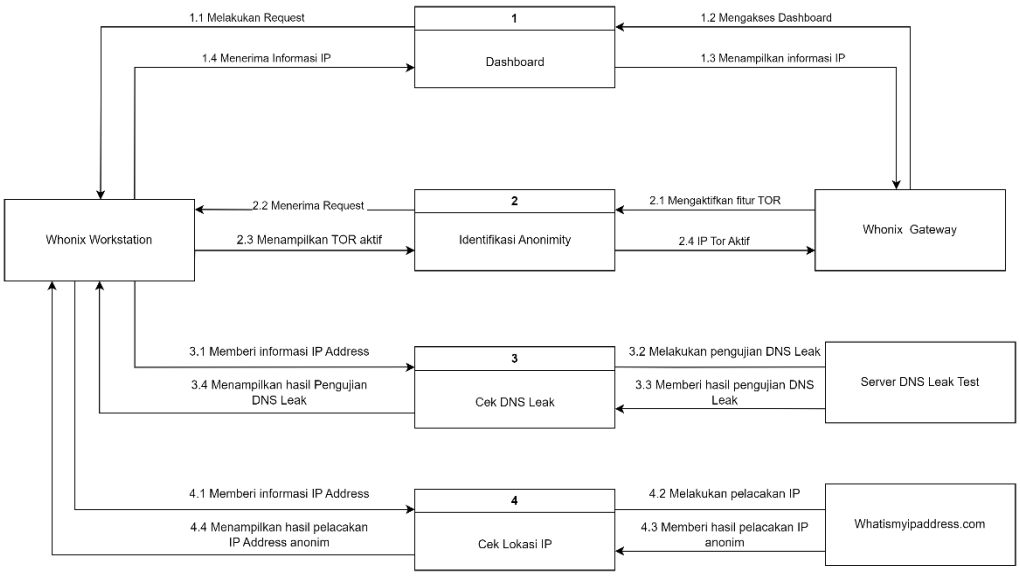

Figure 6. DNSLeakTest Function Mechanism

Journal of Information System Research (JOSH)
Volume 6, No. 1, Oktober 2024, pp 23−33
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v6i1.5682

Figure 6 explains DNSLeakTest Function Mechanism. DNSLeakTest is a testing process to ensure that DNS requests made by the operating system do not leak to unwanted DNS servers. DNSLeakTest profiling with Tor active consists of four main activities. First, on the dashboard activity, it starts with accessing the Whonix Workstation dashboard which displays the user's IP information. Second, anonymity identification, involves activating the Tor feature on the Whonix Gateway and verifying the Tor connection which displays the active Tor IP. Third, DNS Leak check, tests for DNS leaks using the DNSLeakTest server, where the test results show a random IP address from Tor. Finally, the IP location check, involves IP tracking through the Whatismyipaddress server to display the IP location masked by the Tor network, ensuring user anonymity and privacy is maintained. This process ensures that the user's real IP is not visible and all DNS requests remain anonymous and encrypted.

3.2.4 DNSLeakTest Profiling Results

The k-anonymity method is a technique that transforms data so that the published dataset has at least k tuples with the same attributes and values[12]. DnsLeakTest profiling uses scoring 0 represents No, 1 represents Partially, and 2 represents Yes.

Table 4. DNSLeakTest profiling results

No	Aspects	Score
1	Tor Compatibility	2
2	IP Address Obfuscation	2
3	Logging Policy	1
	Total Score	**5**

In Table 4 DNSLeakTest profiling results represents scoring through implementation results as follows:

a. Tor Compatibility: 2 (Yes)
   DNSLeakTest can function properly in the Tor environment, ensuring that DNS leak testing can be performed without technical problems. Whonix routes all network traffic through Tor, including DNS requests, so DNSLeakTest can evaluate DNS leaks in the context of the anonymized network provided by Tor. Tor Compatibility ensures that DNSLeakTest can be used with Tor without requiring complex additional configuration.
b. IP Address Obfuscation: 2 (Yes)
   Tor hides the user's real IP address and server location by routing traffic through multiple nodes before reaching the final destination. When running DNSLeakTest with Tor, only the IP address of the Tor exit node is visible to the DNSLeakTest server. This ensures that the user's identity remains anonymous, and the real IP address is not exposed, providing strong protection against IP tracking.
c. Logging Policy: 1 (Partially)
   DNSLeakTest has a logging policy that varies depending on the service provider. Some services like dnsleaktest.com commit to keeping no logs, while others may keep minimal logs for analysis and service improvement purposes. When used with Tor, the user's real IP address is not visible to DNSLeakTest, reducing the risk of personal data being logged. However, since DNSLeakTest is open.

3.3 Operating System Profiling

3.3.1 Analysis of Anonymity/Privacy Fingerprinting Function Mechanism

Profiling fingerprinting aims to identify and analyze techniques used to collect unique system or user information. Fingerprinting can be used by attackers or trackers to distinguish between different users or systems, even if they try to remain anonymous. Here is the Data Flow Diagram (DFD) of profiling fingerprinting with Tor active:

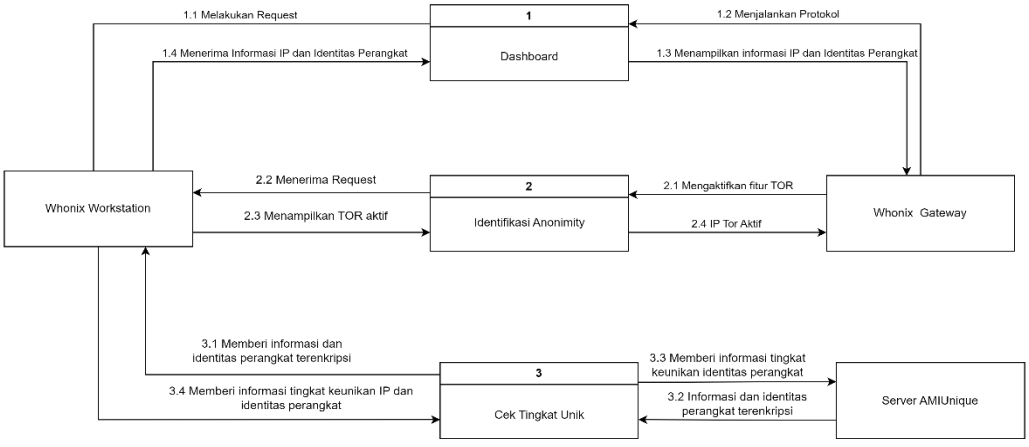

Figure 7. Fingerprinting Function Mechanism

Journal of Information System Research (JOSH)
Volume 6, No. 1, Oktober 2024, pp 23−33
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v6i1.5682

Figure 7 represents mechanism of anonymity and privacy functions in fingerprinting with Tor enabled aims to minimize unique information that can be used to track users. By enabling Tor, Whonix Workstation ensures that every request and device information sent to external servers, such as amiunique, is encrypted and anonymous. This reduces the possibility of collecting user identity data and obscuring real IP addresses, thus preserving user privacy and anonymity against fingerprinting techniques that could potentially uniquely distinguish and track systems or users.

3.3.2 Fingerprinting Profiling Results

The k-anonymity method is a technique that transforms data so that the published dataset has at least k tuples with the same attributes and values[12]. Whonix operating system profiling uses scoring 0 representing No, 1 representing Partially, and 2 representing Yes. The following is the fingerprinting profiling results table:

Table 5. Fingerprinting profiling results

No	Aspects	Score
1	Data Encryption	2
2	Logging and Monitoring	1
3	Access Control	2
	Total Score	**5**

In Table 5 profiling results of the fingerprinting represents scoring through the following implementation results:

a. Data Encryption: 2 (Yes)
   Data transferred through Whonix is encrypted via the Tor network, ensuring that data remains secure from external parties. In addition, Whonix supports full disk encryption to protect data at rest.
b. Logging and Monitoring: 1 (Partially)
   Whonix minimizes logging to maintain privacy. While some logging remains for basic troubleshooting and security purposes, it is designed to not store sensitive information that could identify the user's identity.
c. Access Control: 2 (Yes)
   Whonix uses strict access control and privilege management. Root access is restricted and requires additional authentication via sudo. Regular users have minimum access rights, in accordance with the principle of least privilege security.

3.3.3 Analysis of Anonymity/Privacy Backup and Restore Function Mechanism

Backup is the process of making a copy of data from the system to ensure that data can be recovered in the event of loss or damage. While restore is the process of returning data that has been backed up to the original system or a new system after loss or damage occurs. Here is the Data Flow Diagram (DFD) of Backup and Restore:

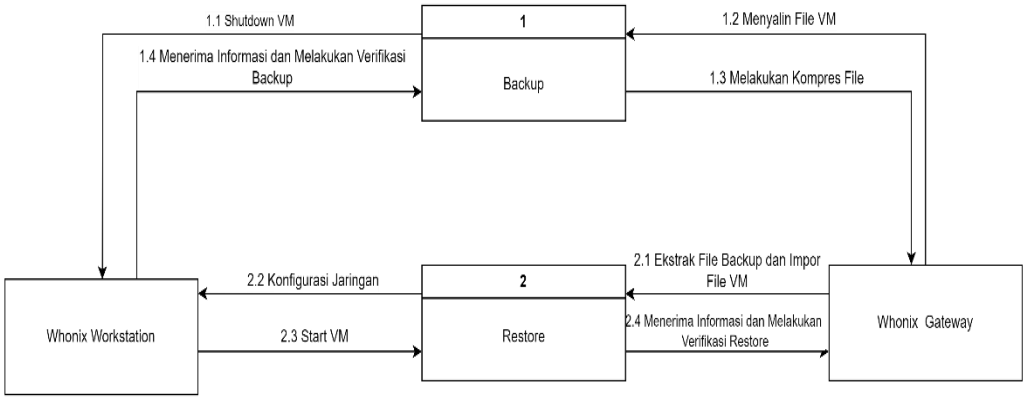

Figure 8. Backup dan Restore Function Mechanism

Figure 8 explains anonymity/privacy function mechanism in the backup and restore process is important to ensure that the data backed up and restored does not degrade the level of confidentiality and anonymity. The backup process starts with shutting down the VM to ensure data consistency, followed by file compression to reduce size and maintain data integrity. On restore, steps include file extraction and reconfiguration of the VM to ensure that network settings and functionality remain as previously required, as well as verification to ensure that data and applications function properly without compromising the privacy and anonymity of the system.

3.3.4 Backup and Restore Profiling Results

The k-anonymity method is a technique that transforms data so that the published dataset has at least k tuples with the same attributes and values[12]. Whonix operating system profiling backup and restore uses scoring 0 representing No/No, 1 representing Partially, and 2 representing Yes/Yes.

Journal of Information System Research (JOSH)
Volume 6, No. 1, Oktober 2024, pp 23−33
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v6i1.5682

Table 6. Backup and restore profiling results

No	Aspects	Score
1	Data Encryption	2
2	Logging and Monitoring	2
3	Access Control	1
	Total Score	**5**

In Table 6 Backup and restore profiling results represents scoring through the following implementation results:

a. Data Encryption: 2 (Yes)
   Data transferred through Whonix is encrypted via the Tor network. Tor network ensuring to protect the connection[20] . In addition, Whonix supports full disk encryption to protect data at rest.
b. Logging and Monitoring: 1 (Partially)
   Whonix minimizes logging to maintain privacy. While some logging remains for basic troubleshooting and security purposes, it is designed to not store sensitive information that could identify the user's identity.
c. Access Control: 2 (Yes)
   Whonix uses strict access control and privilege management. Root access is restricted and requires additional authentication via sudo. Regular users have minimum access rights, in accordance with the principle of least privilege security.

4. CONCLUSION

Profiling is performed on three aspects using the Whonix operating system: application, network, and operating system. Identification of anonymity and privacy is done using basic application functions based on Data Flow Diagram (DFD). Characters in the application, network, and operating system aspects that support anonymity and privacy can be organized by metrics, namely: Application: data encryption, metadata protection, and privacy by design. Network: tor compatibility, IP Address obfuscation, and logging policy. Operating System: data encryption, logging and monitoring, and access control. Based on the measurements taken on these three aspects, the category with the highest score is the network aspect. So Whonix supports the anonymity and privacy aspects with the highest metrics as well. Whonix is designed using two virtual machines (Gateway and Workstation): This operating system architecture separates network activities and user applications so that each virtual machine has specific functions to maximize features and performance. Whonix Workstation can be replaced with an environment using another operating system by pointing the network interface to Whonix Gateway so that the environment can also use an anonymous network with Tor provided by Whonix Gateway. Based on the profiling experiments conducted, Whonix does not support VPN by default. However, it provides a secure and anonymous environment for users. The integration of Tor, the unique architecture with two virtual machines, and the focus on isolation and security make Whonix capable of supporting anonymizing scenarios.

REFERENCES

[1] M. Hlatshwayo, “CYBERSECURITY IN THE DIGITAL SPACE,” Oct. 2023, [Online]. Available: https://www.researchgate.net/publication/375115830
[2] L. Kim, “Cybersecurity: Ensuring Confidentiality, Integrity, and Availability of Information,” Jan. 2022, doi: 10.1007/978-3-030-91237-6_26.
[3] B. Lundgren, “Beyond the concept of anonymity: what is really at stake.” Big data and democracy. 2020.
[4] H. Barstad and C. Li, “Deanonymizing communications on The Onion Router (TOR) network with Deep Learning,” 2021. [Online]. Available: https://github.com/HallyB96/TOR-Deep-Fingerprinting-Master-Thesis.
[5] A. Hulina, “Operating systems for privacy and anonymity: a survey B,” Brno, 2020.
[6] M. B. Betel de Robles, J. C. Anthony Hermocilla, and J. P. Pabico, “Characterization and Classification of Malware Traffic over the Tor Network,” Computing Society of the Philippines, Inc, 2020.
[7] P. Choorod and G. Weir, “Tor Traffic Classification Based on Encrypted Payload Characteristics,” in Proceedings - 2021 IEEE 4th National Computing Colleges Conference, NCCC 2021, Institute of Electrical and Electronics Engineers Inc., Mar. 2021. doi: 10.1109/NCCC49330.2021.9428874.
[8] J. Perno and C. W. Probst, “Human Aspects of Information Security, Privacy and Trust,” T. Tryfonas, Ed., in Lecture Notes in Computer Science. Cham: Springer International Publishing, 2017. doi: 10.1007/978-3-319-58460-7.
[9] O. Eriksson and P. J. Ågerfalk, “Speaking things into existence: Ontological foundations of identity representation and management,” Information Systems Journal, vol. 32, no. 1, pp. 33–60, Jan. 2022, doi: 10.1111/isj.12330.
[10] F. M. Purba, P. Warih, and M. Saputra, “Design Of Enterprise Resource Planning System In Inventory Management Module Using Odoo Application With Quickstart Method In Pharmacy Room Of Puskesmas III Denpasar Utara,” 2021.
[11] A. Master, “Password Managers: Secure Passwords the Easy Way,” Center for Education and Research in Information Assurance and Security (CERIAS), 2022, doi: 10.5703/1288284317618.
[12] W. Mahanan, W. A. Chaovalitwongse, and J. Natwichai, “Data privacy preservation algorithm with k-anonymity,” World Wide Web, vol. 24, no. 5, pp. 1551–1561, Sep. 2021, doi: 10.1007/s11280-021-00922-2.

Journal of Information System Research (JOSH)
Volume 6, No. 1, Oktober 2024, pp 23−33
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v6i1.5682

[13] T. Oesch, "An Analysis of Modern Password Manager Security and Usage on An Analysis of Modern Password Manager Security and Usage on Desktop and Mobile Devices Desktop and Mobile Devices," Information Security Commons, Other Computer Engineering Commons, 2021.
[14] A. Z. Mardiansyah, A. Zubaidi, A. H. Jatmika, and R. B. Huwae, "Implementation of GNU Privacy Guard (GPG) Hybrid Encryption to Improve Information Security in Electronic Signature (E-Sign) Services at the University of Mataram," 2024.
[15] K. Nair, P. Maitreyi, E. Sushma, and A. H. M, "Providing Security for a Chat Application using RSA Encryption with GPG," International Conference for Innovation in Technology (INOCON), pp. 1–5, 2024, doi: 10.1109/INOCON60754.2024.10511348.
[16] A. Anbarje, M. Sabbagh, and D. P. Palacin, "Evaluation of WireGuard and OpenVPN," Dissertation, 2020.
[17] P. A. Wu supervised by Tanja Lange Jacob Appelbaum Jason Donenfeld, "Analysis of the WireGuard protocol," 2019.
[18] V. Johansson, "A COMPARISON OF OPENVPN AND WIREGUARD ON ANDROID," Computer Science, 2024.
[19] A. M. Taib, "Securing Network Using Raspberry Pi by Implementing VPN, Pi-Hole, and IPS (VPiSec)," International Journal of Advanced Trends in Computer Science and Engineering, vol. 9, no. 1.3, pp. 457–464, Jun. 2020, doi: 10.30534/ijatcse/2020/7291.32020.
[20] Jr. Jonathan A. Goohs, "CULR_Fall_Journal_Apr_Revision," COLUMBIA UNDERGRADUATE LAW REVIEW, vol. XVIII, no. 1, pp. 133–134, 2021.