Masaryk University
Faculty of Informatics

Operating systems for privacy and anonymity: a survey

Bachelor's Thesis

Andrej Hulina

Brno, Fall 2020

Masaryk University
Faculty of Informatics

Operating systems for privacy and anonymity: a survey

Bachelor's Thesis

Andrej Hulina

Brno, Fall 2020

This is where a copy of the official signed thesis assignment and a copy of the Statement of an Author is located in the printed version of the document.

Declaration

Hereby I declare that this paper is my original authorial work, which I have worked out on my own. All sources, references, and literature used or excerpted during elaboration of this work are properly cited and listed in complete reference to the due source.

Andrej Hulina

Advisor: RNDr. Lukáš Němec

Acknowledgements

I would like to thank my advisor RNDr. Lukáš Němec for his help, patience and suggestions, and also my family and friends for their support during my entire studies.

Abstract

The present thesis is set to explore the operating systems focused on the user's privacy and anonymity. The first part of the thesis describes such properties of operating systems, on which operating system they should be built, which anonymous network should be used, and which features they should contain. Furthermore, the thesis includes a brief description of nine operating systems with such focus. Three of them, Whonix, Tails OS, and Kodachi Linux, are described in detail in the next part. All three systems are tested for everyday use, such as searching the Internet, sending messages via instant messenger, and sending emails. The systems are compared in the last part of the thesis.

Keywords

operating system, anonymity, privacy, security, Tor, users, Whonix, Tails, Kodachi

Contents

Introduction **1**

1 Properties of the operating systems for privacy and anonymity **2**
1.1 Tor anonymity network . . . 3
1.1.1 The Tor Browser . . . 3
1.1.2 OnionShare . . . 4
1.1.3 Tor stream isolation . . . 4
1.2 Features . . . 4
1.2.1 AppArmor . . . 5
1.2.2 Keystroke Anonymization . . . 5
1.2.3 Metadata cleaning . . . 5

2 A survey of operating systems for privacy and anonymity **6**
2.1 Tails OS . . . 6
2.2 Whonix . . . 6
2.3 Kodachi Linux . . . 7
2.4 Parrot OS . . . 7
2.5 Subgraph OS . . . 8
2.6 Ipredia OS . . . 8
2.7 MOFO Linux . . . 8
2.8 Heads OS . . . 9
2.9 Robolinux . . . 9

3 Whonix **10**
3.1 Whonix-Gateway . . . 11
3.2 Whonix-Workstation . . . 12
3.3 Features . . . 14
3.4 Tests . . . 15

4 Tails OS **16**
4.1 Encrypted Persistent Storage . . . 17
4.2 Applications . . . 18
4.3 Features . . . 19
4.4 Tests . . . 20

5 Kodachi Linux **22**

5.1 Applications 23
5.2 Features 24
5.3 Tests 25

6 Comparison **27**

7 Conclusion **30**

Bibliography **31**

List of Tables

6.1 Overall properties 27
6.2 Features 28
6.3 Applications 29

List of Figures

1.1 How Tor works 3
3.1 Lynis in Whonix 16
4.1 Lynis in Tails 21
5.1 Lynis in Kodachi 26

Introduction

Gone are the days when everyone thought people were private on the Internet. The internet users should already know that nobody is 100 percent protected against the companies trying to gain as much information about every user as possible [1]. Every visited website collects some data about the users. Almost all the free applications and websites have the same rule. When the user does not pay, he becomes the product. Most websites contain advertisements, trackers, and people are being tracked on almost every website [2].

People who care about humans' inalienable rights to privacy and freedom of expression try to help others defeat all methods of internet surveillance and censorship, which corporations, internet service providers, and governments use [3]. They try to create all types of software to keep privacy and stay anonymous on the Internet. Globally, there are many different applications with such intent. However, even the best application can not ensure the highest anonymity and privacy if installed on a flawed operating system that can not be trusted. That is why it is also necessary to have an operating system designed to increase users' anonymity and privacy on the Internet [4].

The thesis focuses on operating systems that take users' anonymity and privacy as the primary goal, even at the cost of lower usability or slower connection. In the first chapter, the properties of such operating systems are described. Part of the chapter is devoted to Tor, the most common anonymity network. Proper operating systems with such intent should come with several features, which increase all the abilities. Few commonly used features increasing security, anonymity, and privacy are also mentioned and briefly described.

In the next chapter, nine operating systems for anonymity and privacy are briefly introduced. Three of them, Whonix, Tails OS, and Kodachi Linux, are described in detail. All three systems are tested for every day user activities and tested with Lynis, a testing security tool that provides a health scan of the system to support compliance and system hardening [5]. The sixth chapter compares the overall properties, features, and applications of these three operating systems.

1 Properties of the operating systems for privacy and anonymity

There are many operating systems globally, but only some focus on privacy and anonymity. They are not created by the enormous companies, but by people who often only want to help others, even without any ambitions for profit. That is why the developers use the cornerstone on which the entire operating system is built, the Linux distributions like Debian that are free and open-source. However, these Linux distributions come with versatility and usability as their primary goals. For this reason, operating systems with such scope are heavily modified to emphasize security, anonymity, and privacy over all else.

In the digital world, there is no single way to protect a system from all types of attacks successfully. That is why many operating systems use defense in depth. Defense in depth means that a series of security mechanisms are layered to protect the system's data. If one layer fails, another immediately steps up to thwart an attack. [6]

Operating systems for anonymity and privacy should be easy to run and easy to destroy, as the system can get compromised by a simple mistake that the users make on the Internet. When the system is compromised, it is necessary to destroy it and use a new clean version. The easiest way to create such an operating system is a live system. The live operating system can be booted on to USB, CD, or SD card, from where it always launches as a new, untouched system. After the system shuts down, everything is wiped out, leaving no trace, which solves the compromised system's problem. However, this type of operating system is not persistent.

Another way how can be such an operating system designed is a virtual machine. The operating system running as a virtual machine can be easily installed and run as a persistent system. Such an operating system should provide full hardware isolation, so the hardware and host OS are protected when the system is compromised. When it happens, the virtual machine can be destroyed by one click and installed again [7].

1.1 Tor anonymity network

For the highest anonymity and privacy, operating systems are using anonymity networks. The most common is the Tor network. Tor stands for The Onion Router and is often used as a building block for creating new tools or operating systems focused on privacy and anonymity. Commonly, only connections through the Tor network are available in such operating systems to ensure the highest anonymity. Tor is a traffic analysis resistance tool. It does not prevent data collection. However, it makes it so that whatever data is collected cant be meaningfully deciphered and utilize for whatever purpose by anyone.

The Tor software is an open network designed to give all of its users the same identity. Tor hides the user's location by relaying the traffic through three random places globally and encrypting the traffic with a triple layer of encryption to ensure nobody can follow the Tor circuit back to its origin [8, 9, 10].

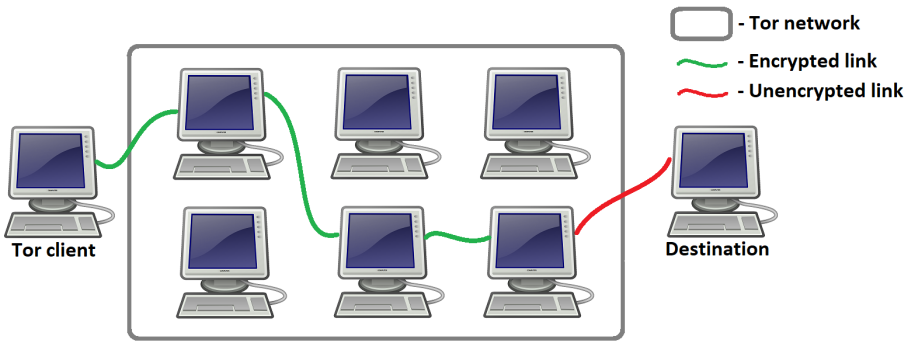

Figure 1.1: How Tor works

1.1.1 The Tor Browser

The easiest way to access the Tor network is the Tor Browser, a modified Mozilla Firefox version. The Tor Browser works like a regular browser, but besides, it is optimized for anonymity, and all the browsing data are encrypted. All traffic from the browser is routed through the Tor

network. Every visited website is isolated, which is a protection against the follow by advertisements and third-party trackers, which allows the users even to increase the security. The browser also automatically clears the browsing history and cookies when it shuts down.

Tor browser has three security levels. The default level is Standard, which does not disable any website features. The middle-way, Safer level disables the most common dangerous website features. On all the non-HTTPS websites, it also disables Javascript. The Safest security level allows only website features that are required for basic services and static websites. Images, media, and scripts are affected. It also disables Javascript on all websites [11, 12].

1.1.2 OnionShare

OnionShare is an open-source tool that allows sharing files of any size over the Tor network anonymously and securely. The users need to drag and drop files into the OnionShare and start sharing, which will generate an unguessable address. This address needs to be sent to the receiver, who does not need OnionShare to download the file. The file can be downloaded by opening the address in the Tor browser [13].

1.1.3 Tor stream isolation

Stream isolation creates a new circuit and isolates the stream as much as possible, which prevents attacks on the users' anonymity. Before the stream isolation implementation, it was very likely that multiple streams would select the same circuit, which could lead to a combination of unrelated transmissions and compromising users' anonymity [14].

1.2 Features

Anonymity, security, and privacy are complex problems with many issues beyond the IP address masking necessary for users' privacy protection. Every operating system includes many different features. However, some of them should be part of every operating system as another security and anonymity layer.

1.2.1 AppArmor

AppArmor is a Linux kernel security module whose functionality allows the system administrator to use per-program profiles (AppArmor profiles), designed to restrict specific high-risk applications from unintentionally releasing information on the Internet. Profiles restrict which system recourses applications can access. The most common are capabilities for network access and raw socket access and permissions for reading, writing, and executing files on specific paths. For some applications like Tor, some profiles are enforced by default [15].

1.2.2 Keystroke Anonymization

The newest keystroke biometric algorithms can uniquely fingerprint users based on soft biometric characteristics like typing speed, error frequency, length of pauses in typing, and many others [16]. These algorithms generate a primary pattern for users, which are compared in the future. Every user produces keystrokes as specific as signature or handwriting. However, typing styles can differ depending on the user's energy or mood situation. Adversaries might likely have samples of keystroke fingerprinting from everyday users' online activities, which can be compared with "anonymous" samples. It is a privacy risk, and users who care about their privacy should not type straight into browsers with enabled Javascript. Recommended is using an offline text editor for writing and copying the text into the web interface. Operating systems might come with some specific Keystroke Anonymization Tool [17, 18].

1.2.3 Metadata cleaning

Metadata is data about data. Almost every file contains metadata, and it should be cleaned for privacy. One file can be embedded information like the users and computer name, date and time of the creation and last update, location, and many others. If the operating system for anonymity and privacy does not provide any metadata cleaning, it should at least come with an additional feature, which allows the users to clean all metadata from the files [19].

2 A survey of operating systems for privacy and anonymity

In this section, nine operating systems focused on anonymity, and privacy will be briefly introduced.

2.1 Tails OS

Its name is a shortcut for The Amnesiac Incognito Live System. Tails is a portable Debian-based OS focused on preserving privacy and anonymity designed to run with full functionality from a DVD or USB thumb drive and can also run in the virtual machine.

The whole system runs independently from the other operating system and does not write anything to the hard disk. It runs only from the computer's memory, so it leaves no trace on the computer. When the system shuts down, it deletes memory with all files unless explicitly asked not to do so.

Tails uses Tor as its default networking application to protect users' privacy online. The system blocks all the applications attempting to access the Internet directly without Tor [20].

2.2 Whonix

Whonix is an open-source operating system focused on anonymity, privacy, and security while connected to the web. Based on security-hardened Debian derivative calls Kicksecure, Tor, and the principle of protection by isolation.

The system consists of two virtual machines, the Whonix-Gateway and the Whonix-Workstation, installed on a user-provided host operating system and connected through an isolated network. Both have their own IPs, which make it impossible to track activity back to its original user. The Whonix-Workstation runs applications on a completely isolated network and can only talk to the Whonix-Gateway. The Whonix-Gateway runs as Tor processes and acts as a gateway. It means that only connections through the Tor are permitted. This security

by isolation configuration averts many malware threats, misbehaving applications, and users' error [21].

2.3 Kodachi Linux

Kodachi Linux is a live operating system based on Debian that can boot from a DVD, USB stick, or SD card. The entire OS is functional from the host's temporary memory RAM. The system cleans up after itself, so no trace is left behind once it is shut down. Users can install it on any PC, but this is not recommended as it will save all the settings on the hard drive.

Kodachi provides full anonymity and privacy. When the operating system starts, it automatically starts VPN and TOR network service. All traffic runs through a VPN, after that through the Tor network with DNS encryption. Free VPN is part of the pre-configured toolset. The system has its browser based on the Tor Browser, from which some problematic Tor modules have been cut off. It also offers I2P, GNUNET, and a custom VPN [22].

2.4 Parrot OS

Parrot OS is a privacy-hardened GNU/Linux distribution based on Debian, which comes in two major versions: Parrot OS Home and Parrot OS Security. It can be dual-booted with other operating systems or run on Docker or Virtual Box.

Parrot Home is a lightweight and always updated system designed for daily use. It is focused on regular users who care about their privacy but do not need special security tools. It includes Tor Browser, Firefox with preset extension HTTPS Everywhere, and other programs to increase users' privacy and anonymity. The system comes with Anon Surf, which routes all the traffic and packets through Tor.

Parrot Security is made for professional use, and it comes as a complete all-in-one environment for cloud pen testing, computer forensics, reverse engineering, hacking, cryptography, privacy, and anonymity. This version also has pre-installed security and anonymity tools like Tor, I2P, or Anonsurf [23].

2.5 Subgraph OS

Subgraph OS is a lightweight Debian-based distribution that uses the Gnome desktop environment. Although it looks like a modern OS, it is still in the Alpha version. The system is designed to be difficult to attack. It is accomplished by the proactive, ongoing focus on security and attack resistance and also by the kernel hardened with Grsecurity, the best set of Linux kernel security enhancements available.

The applications run in sandbox environments, known as Oz, unique to this OS. Oz is designed to isolate applications from each other and the rest of the system. Access to system resources is only granted to applications that need them. For example, the PDF viewer and the image viewer do not have access to any network interface in the sandbox they are configured to run in. The communication of applications is restricted so that they use the Tor network exclusively. Applications should connect through the Tor network via the Metaproxy application [24].

2.6 Ipredia OS

IprediaOS is a Fedora-based privacy-oriented operating system, which can be run in live mode or installed to the users' hard drive. It uses the I2P anonymizing network instead of the Tor network. I2P does not act as Tor, so not as a gateway to the standard Internet. Because of this, the system cannot browse regular websites, only i2p websites. Anonymous email, bit torrent, and IRC clients, which provide an anonymous internet experience, are pre-installed. IprediaOS is no longer maintained [25].

2.7 MOFO Linux

MOFO Linux is an Ubuntu-based operating system focused on providing users with a complete toolset for roaming around the Internet safely with absolute freedom. The toolset includes OpenVPN, I2P, Softether, Freenet, Tor, Tor Browser, and other tools that provide an anonymous and secure connection to the Internet. Internet history and usage tracks are destroyed on every shutdown. This OS is de-

signed for easy usage on every computer type. The system has no documentation.

It contains office, multimedia, and internet applications enabling web browsing, productivity, and entertainment. It can run directly from a CD or USB, but the users can install it on HDD or SSD. It might also run in a virtual machine [26].

2.8 Heads OS

Heads is a free and open-source Linux distro born to answer Tails since Tails uses systemd as an init system and contains non-free software. By default, Heads offers Openbox as its graphical window manager. The system uses a hardened Linux kernel with grsecurity. Grsecurity helps to protect the system against zero-day[1] attacks and other known attacks on the Linux kernel.

All Internet traffic is always routed through the Tor network, but with an option to turn it off. The Tor protocol is designed to encrypt the traffic so that users are anonymized on the Internet. Web sites and services will not know from where the traffic comes [28].

2.9 Robolinux

Robolinux is a Debian-based operating system that can be installed on a hard drive, bootable media, or a virtual machine. The system loads with no logs VPN calls Private Internet Access, which is charged. The users can add other privacy tools like Tor, I2P, Bleachbit, Enigmail, and the JonDo browser.

Robolinux is unique with its integration between Windows and Linux, on which it places a heavy emphasis. Every Robolinux version runs regular Windows programs flawlessly and natively inside its desktop, which increases the speed with which the users operate with a computer. Besides, the system is not affected by any Microsoft Windows viruses and malware. Also, it runs many times faster than any other Windows OS [29].

1. Zero-day attack is an attack exploiting vulnerabilities of the software that have not been disclosed publicly [27].

3 Whonix

Whonix is an open-source operating system focusing on security, anonymity, and privacy. The system is being up to this day regularly updated, and currently, 15.0.1.5.4 is the newest version released on December 1, 2020.

Whonix is based on Kick Serure, a security-hardened derivative of Debian. To make the system as secure as possible, Kick Secure uses the kernel hardening settings standards, recommended by the Kernel Self Protection Project known as the KSPP. The project covers, among other things, active detection of attack attempts or removal of entire classes of bugs [30].

To ensure online anonymity, Whonix is built on Tor, which it uses as a default anonymization network. All the rerouting and encryption functions of Tor are applied to all applications that need a network connection. All connections, applications, and traffic are forced through Tor. Otherwise, they are blocked. Since all the Tor traffic is going through several servers worldwide before it reaches the destination, it is almost impossible to connect the Whonix users to their internet activity [31].

For the best security, Whonix comes with isolation. It runs as two virtual machines, Whonix-Gateway, and Whonix-Workstation, isolated but connected through an isolated network. Currently, few options for Whonix virtualization and hardware configuration, which significantly affect Whonix's usability and security, are available.

The most common configuration consists of two virtual machines installed on a single host system. Virtual machines can be installed in VirtualBox VM, Qubes OS, or Linux KVM. Both of them run on the host hardware but can not interact with the host OS. They are completely isolated. Any dangerous malware, unwanted connections, or any other threats can not leave Whonix. Neither the applications nor websites can read any information about the host hardware. For example, if a virus were to bypass the Tor browser, it would just end up inside a virtual machine and not in the host machine. A virtual machine can be easily destroyed and recreated. It gives the users the advantage of this OS's protection features without rebooting or installing a new operating system.

Whonix-Gateway and Whonix-Workstation can also be physically isolated on two separate host systems. The Whonix-Gateway can run on its physical device run either directly on the hardware or inside a virtual machine. The latter is recommended. The Whonix-Workstation should always run in a Virtual Machine. If both software is installed directly on physical devices, it does not provide any protection against hardware fingerprints. It is also difficult to install and recommended only for advanced users [32].

3.1 Whonix-Gateway

Whonix-Gateway is software designed to run Tor processes and act as a gateway for the other virtual machine. This virtual machine has two virtual network interfaces. Through the first one is connected to the Internet. It is getting a connection from the host and communicates with Tor relays. The second one is connected to the virtual LAN, which runs entirely inside the host. It connects the Gateway with the Workstation, usually, Whonix-Workstation.

Whonix-Gateway also supports the torification of other operating systems, Microsoft Windows, Android, and other GNU/Linux. However, using a default Whonix-Workstation is the most secure and most comfortable way. Whonix-Custom-Workstation is recommended only for advanced users [33].

Whonix-Gateway is not designed for regular users' activity. It creates and prevents Tor connections, there should be no Internet activity, and it should not be used as a distribution for Linux. It is necessary to keep it always updated. Tools like Stop Tor, Reload Tor, and Restart Tor GUI, which do precisely what their name says, are pre-installed along with others like Nyx-Status Monitor for Tor, Anon connection wizard, Tor Control Panel, Global Firewall Settings, Reload Firewall, and others. Since Whonix is a Linux derivative, it also contains a Terminal [34].

Nyx is a terminal monitor for Tor, which provides detailed real-time information about the user's relay, such as relay detail, IP, connection types, CPU and memory usage, bandwidth graphs, event logs, interpreter, and much more.

Tor Control Panel is a Tor controller, the quality and suitability of which is not guaranteed by The Tor Project, from which it is independently produced. It allows the users to check Tor status, stop, restart, or configure Tor, showing the logs. It also comes with the utilities for displaying Tor circuits and streams and setting a new identity, which can only be done if the system is connected to the Tor network [35].

Anon connection wizard is an application that helps the users to configure the Tor bridge or a proxy before connecting to Tor. The users can connect directly to the Tor network, but some countries do not allow them to use Tor, as it is illegal. These users need to configure Tor bridges, which hide the fact that the system connects to Tor from the internet service provider. As a next step, the users can also configure a proxy. Bridge and proxy can be configured at the same time. The Tor network can also be disabled. However, without the Tor network, the users are not able to do any internet activity [36].

WhonixCheck is a bash script responsible for checking essential system variables. It verifies if the operating system is up-to-date or if IP forwarding is disabled on Whonix-Gateway. It also checks if networking is configured correctly and notifies about the Tor network. In addition to these, WhonixCheck provides many other checks. It runs automatically after the first boot, but the users can start it also manually [37].

The firewall features of Whonix-Gateway include stream isolation, optional Tor relay, optional VPN-Firewall, and others. The firewall should not be removed. Users can modify them using User Firewall Settings or access the preset rule with the Global Firewall Settings. Both are pre-installed [38].

Web Browser is not allowed to be run on the Gateway. Browsing the Internet is not secure on the Gateway.

3.2 Whonix-Workstation

The second virtual machine calls Whonix-Workstation, is the one that should be actively used by users. It runs applications, which should all be launched only in the Workstation, not in the Gateway. Unlike the Gateway, the Workstation is connected only to the internal virtual LAN, which allows it to communicate only with the Gateway. It is

isolated from the host system. All traffic coming from the Workstation is forced to pass through the Tor network. Only IP addresses on the internal LAN, which are the same in every installation of Whonix, are available for the Workstation. No application, not even malware with root privileges, can see the host's real IP address but only the anonymized Whonix IP addresses. It makes IP address and DNS leaks impossible, which reduces the users' risk of being tracked by anyone.

Applications can also not connect to the unsecured Internet and can communicate only over the encrypted Tor network. Since the Workstation is not connected to the network directly but to the pre-anonymized Gateway's network, it is impossible to establish an Internet connection on the Workstation when the Gateway is turned off, or Tor does not work [39].

Whonix-Workstations comes with a few pre-installed and pre-configured applications with safety in mind, making them ready for use with minimal user input.

Since Whonix ensures anonymity and privacy by using Tor, the Tor browser is the system's default and the only recommended web browser. Tor Browser was already described in the section 1.1 at the page 3, and Whonix modifies the regular Tor Browser Bundle just slightly. It disables the Tor Circuit View function for security reasons and Open Network Settings. Together with other small changes, Whonix changes the default landing page of the browser.

For communication, Whonix comes with two open-source applications, XChat, and qTox. The former one uses IRC and the latter one Tox protocol [40].

As the default password manager, Whonix uses KeePassXC. The system also has pre-installed applications like VLC, Xpdf, or Ristretto Image Viewer. For cryptocurrency, Whonix offers two options, Monero GUI for Monero and Electrum Wallet for Bitcoin. Few applications like WhonixCheck, Firewall settings, or Terminal are also pre-installed on the Workstation and work similarly to the Gateway applications.

For Keystroke Anonymization has Whonix pre-installed application called Kloak, which intercepts the user's keyboard input before it reaches the driver and randomizes it [41].

3.3 Features

Some of the features, like Tor, were already described in the section 1.1 at the page 3. Whonix implements stream isolation and some pre-installed applications like Tor Browser or HexChat are configured to use different SocksPort, which means that every application with dedicated SockPort takes a different path through the Tor network.

The system does not perform automatic metadata cleaning of files, but the system comes bundled with MAT2, which can be used for manual metadata cleaning. It is a shortcut for the Metadata Anonymization toolkit, and it supports almost every standard file formats. MAT does not delete the file with removable metadata. Instead, it creates a new clean file with the .cleaned extension. It does not anonymize the files' content, nor can it handle any custom metadata field, steganography, or watermarking. It just removes metadata from the file. To ensure the best anonymity, using file formats with no metadata is highly recommended [42].

By default, Whonix runs in a persistent mode. However, since version 15, Whonix can also be run as a live system. VM Live Mode ensures that everything written to the virtual drive is forgotten after the system is powered off. A virtual machine in live mode is not amnestic by itself. Even though live mode writes everything to the RAM, core dumps, swap files, malware, or other configuration can bypass it. Therefore, it is highly recommended to configure a read-only hard mode as a prevention against malware from remounting the hard drive as read-write. In Host Live Mode runs the entire host operating system in live mode, only available for the OS based on Debian. All the writes are redirected to the RAM, which is massive prevention against malware gaining persistence. Highly recommended is also a correct implementation of a write protection switch [43].

Timekeeping is essential for security, anonymity, and privacy. Therefore Whonix does not use the host's system clock and time synchronization mechanism and leaves them untouched. It also disables most time synchronization features from the virtualizers.

Whonix comes with a sdwdate, which is a security time synchronization. Sdwdate sets the systems clock by communicating with Tor onion webservers via end-to-end encrypted TCP.

Whonix also uses Boot Clock Randomization, which randomly moves the system clock between 0 and 180 seconds into the future or past during boot. It improves anonymity and privacy by prevention of time-based fingerprinting and linkability issues [44].

3.4 Tests

Whonix-Gateway should always be started first, and its first start should be in persistent mode. It allows Tor Entry Guards for Tor. When the Gateway is first launching, the Tor network has to be set up. After the first launch, Whonix-Gateway can also run in a live mode. The first boot of Whonix-Workstation is very similar to Whonix-Gateway, except that the Tor network does not have to be set up. Both of the machines have to be regularly updated.

Every system boot after the first boot up takes only a few minutes, even though two virtual machines have to be started. The time mainly depends on the host machine. The system runs smoothly, and it is automatically connected to the Internet if the host is connected. Internet connection is a bit slower, as everything is forced through the Tor network. Tor browser is pre-installed, and no additional settings are needed.

Web browsing is slower than at the host OS, but still fast enough. It all depends on the internet service provider.

The first instant messenger, HexChat, includes all the IRC client functions and has only one server, the secure version of the OFTC. All other servers have been removed. HexChat launches quickly and is simple to use. It allows one-on-one communication with private messaging and file sharing.

Another instant messenger, qTox, is also simple to use. It uses the Tox protocol to communicate with other users. Tox is a peer-to-peer video-calling and instant-messaging protocol. Currently is Tox, the only VoIP solution compatible with Tor. QTox also allows adding a friend by the Tox ID, which is different for every user.

Whonix does not come with any mail application pre-installed, but any application available on Debian can be installed.

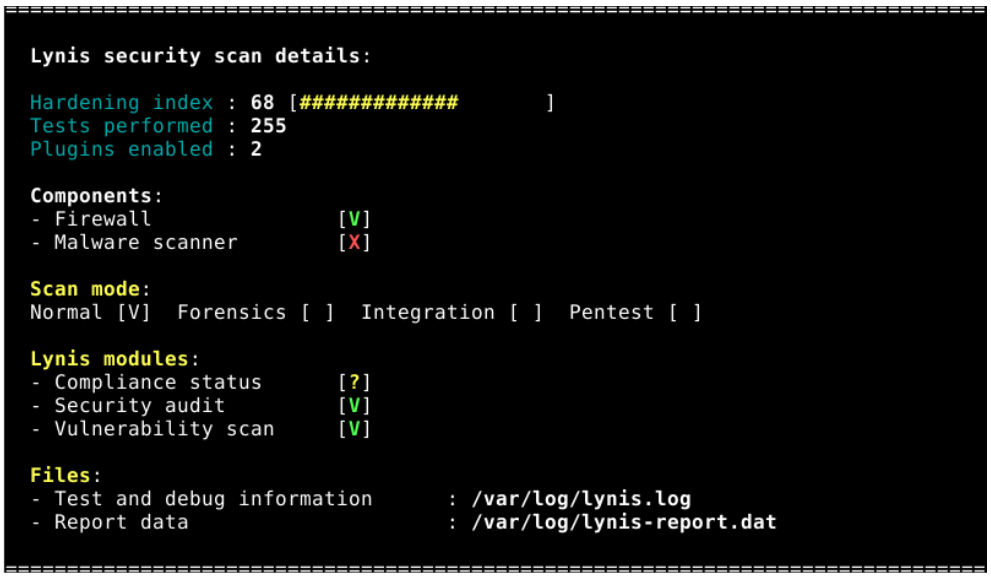

Figure 3.1: Lynis in Whonix

4 Tails OS

The Amnestic Incognito Live System is an open-source and free security-hardened operating system based on Debian, which aims to preserve privacy and anonymity. Tails is being regularly updated, and the new version is released almost every month. Currently, 4.14 is the newest version released on December 15, 2020.

Debian has already integrated most kernel-level security features. Tails kernel has only a few other security features implemented as the base Debian kernel. Several kernel parameters like $vsyscal = none$, $mce = 0$, $slub\_debug = FZP$, and a few more have been passed to the Tails boot command line and /proc/sys. These parameters increase security against kernel exploits [45].

Like many other operating systems focused on anonymity and privacy, Tails achieves its anonymity using Tor as its default networking application. All outgoing and incoming connections are forced to go through Tor, which encrypts and anonymizes online activity. All pre-installed software is configured to make a connection only

via Tor. When an application tries to make a direct connection to the Internet, it is automatically blocked. It also blocks all non-anonymous connections. A website without any encryption is not allowed either. Tails comes with the Tor applications like Tor Browser, OnionShare, and others already pre-installed. Tor Project also provides financial support for Tails development [46].

Tails is designed to be a portable, live operating system. The operating system can be installed on DVD, USB, or SD card from which can quickly run. It can also run as a virtual machine but was initially created to run as a live system, which is still recommended. It gives the users the ability to run Tails on every computer and stay anonymous even outside the home in a public place. It runs independently of the host machine. Everything is uploaded only to the RAM, so it does not leave any trace on the host SSD or HDD. When the system shuts down, browser history, downloaded files, and everything that has not been pre-installed are deleted, making it almost impossible to track down the users. For the users, who would like to store some files and settings, Tails comes with Encrypted Persistent Storage. Since the system runs in a Live mode and always starts in the clean mode, Tails is not recommended as a permanent operating system [47].

4.1 Encrypted Persistent Storage

Encrypted Persistent Storage allows users, which run Tails from the USB Stick to store some data in the USB's free space to keep the data persistent. All the stored data are encrypted by default, but not everything can be stored. Users can configure the storage by using the tool called Configure Persistent Volume, which can be found in Tails Tab in the Applications list. The first step of persistent volume creation is to set the password, which will be used to unlock the storage after every boot. Tails will then create a persistent volume on the USB stick. The USB stick must be at least 8 GB. After the persistent volume is successfully created, the users can specify the features, which will be stored in it.

When the configuration is finished, it is necessary to reboot the system. Until the reboot, nothing will change. After it, Tails starts with Welcome to Tails as usual, but now with to option to unlock the

Encrypted Persistent Storage with the chosen password. All data of the selected features of the Persistent Storage are automatically available. Personal data can be stored in a directory called Persistent. When the system is started without the unlocked storage, it starts without this directory in the clean mode without any saved configuration. Not only files, but the additional applications can be stored and are installed every time Tails starts. Every pre-installed application in Tails is tested for security, and the additional applications could be a security threat. Network Connections, Browser Bookmarks, Printer Settings, and many others can be stored in the Encrypted Persistent Storage.

It is highly recommended not to store any sensitive data in persistent storage, as anyone can steal the USB stick and hack into the Tails because the storage is visible to anyone who gains access to the USB stick. It can even be opened in another operating system.

When one feature is turned off, data is no longer available but is still stored in the Encrypted Persistent Storage. It is necessary to navigate to */live/persistence/TailsData*"_"*unlocked* with nautilus command execute with root rights and delete a specific folder of the feature.

To delete everything stored in the Persistent Storage, Tails also comes with a Delete Persistent Volume tool. It is necessary to keep the storage locked after the boot. Storage can not be deleted when it is unlocked. Current data recovery techniques can recover files even from a deleted Persistent Storage. It is a security threat, so it is recommended to format the USB stick for a complete cleanup [48, 49].

4.2 Applications

As a proper Operating system, Tails comes with the most necessary applications already pre-installed. All the applications are tested for security, and the system provides application isolation for some applications with AppArmor.

Tor Browser with HTTPS Everywhere, No Script, New identity, and other features is the Tails' default browser. Besides, to protect the data and the system from the attacks against Tor Browser, Tails confined the Tor Browser with AppArmor, which allows the Tor Browser to write to and read-only from a limited number of folders [50].

For communication, Tails includes Pidgin Instant Messenger. Pidgin is an open-source chat program that allows users to connect to multiple different chat networks and have more accounts connected at once. Currently, for security reasons, only IRC and XMPP protocols can be used in Tails. Pidgin contains a list of plug-ins. One of the plug-ins is Off-The-Record Messaging, which provides encryption, authentication, deniability, and perfect forward secrecy. It all allows users to have a private conversation over instant messaging [51].

As a default email-client, Tails uses Thunderbird, which comes preinstalled. Thunderbird has built-in support of OpenPGP and S/MIME, which are encryption standards. Besides, in Tails, it is configured for additional anonymity and privacy. Only secure protocols are allowed. Insecure protocols are disabled. From the emails' header are removed the information that could identify a Tails users. All the technologies that could be used for trackings, like Javascript or cookies, are disabled [52].

Same as Whonix, Tails uses KeePassXC as its default password manager.

Additionally, all the applications available for Debian can be easily installed on Tails.

4.3 Features

Tails comes with several features that support privacy and encryption.

Tails does not provide any data encryption, except Encrypted Persistent Storage. However, Tails comes with GnuPG, an open implementation of OpenPGP, and provides document encryption. Tails also includes OpenPGP Applet, which allows manipulating text using OpenPGP. It can use the passphrase encryption of OpenPGP to encrypt text with a passphrase. Applet can also use OpenPGP's public key encryption, allowing users to encrypt text and decrypt encrypted text. Users can also sign text with OpenPGP and verify such a text. It is recommended not to type any confidential text directly into the browser, but encrypt the text written to a text application using OpenPGP Applet and paste the encrypted text into the browser [53, 54].

The system comes with LUKS, which is the standard method for encryption of Linux hard disk. VeraCrypt, another disk encryption

tool, is also supported. Both LUKS and VeraCrypt are used to create an encrypted partition, but VeraCrypt works not only on Linux but also on Windows and macOS. It is recommended to encrypt all the files for Tails and Linux with LUKS and files, which are supposed to be shared across different operating systems with VeraCrypt [55].

Tails does not provide any metadata cleaning, but it comes with MAT, which is similar to MAT2, and also contains PDF Redact Tools, which is used to strip and redact metadata from the documents.

Tails does not do any keystroke anonymization, but Gnome's screen keyboard can be used for protection against keyloggers.

4.4 Tests

Even though Tails can also run inside the virtual machine, it is created to run as a live system from a USB stick, and that is how it is tested.

The system launches fast, the same as every standard operating system, but it mostly depends on the host machine. Since the system erases all the settings after it shuts, it must always be connected to the Internet. It takes approximately one minute to start the Tor after the network connection is established. Overall, it takes maximally 4 minutes till the system is ready for use.

The system is based on Debian, which is by itself a user-friendly operating system, and Tails does not change anything. All the pre-installed applications are wisely separated into blocks and all launch without any delay.

The default browser, Tor browser, works without any complications. Everything downloaded via Tor Browser must be saved to the Tor Browser folder. The files have to be copied to this folder before uploading them via Tor Browser.

Pidgin Instant Messenger comes with a user-friendly interface, which allows users to start conversations quickly. It is translated almost into ninety languages, so even people who do not speak English can use it without any restrictions.

Mozilla Thunderbird, the mail application in Tails, is also straightforward and easy to use. The users need to access their email, and Thunderbird contains an assistant that guides the users to access it

when starting. Thunderbird in Tails comes with many security utilities, which were already described.

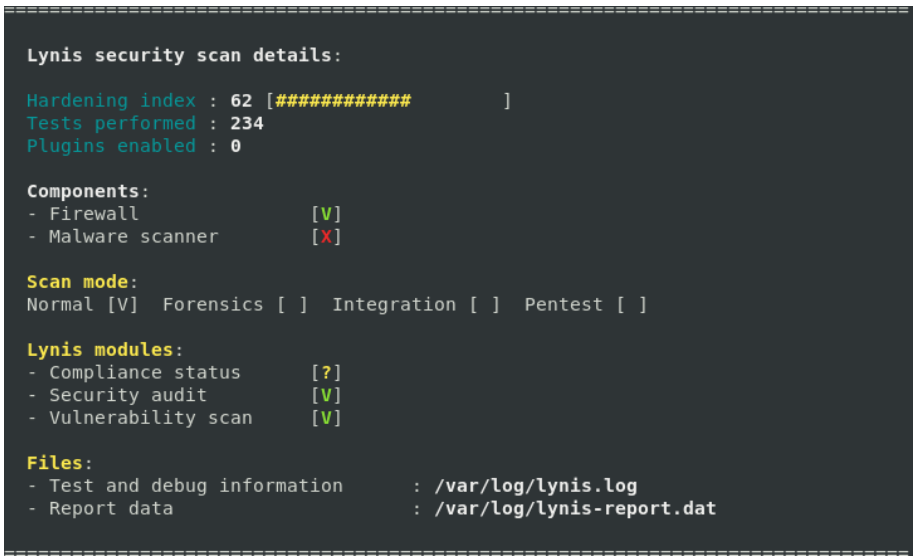

Figure 4.1: Lynis in Tails

5 Kodachi Linux

Kodachi Linux is a free operating system designed to be secure, anonymous, and anti-forensic. The system is based on Xubuntu 18.04.5, which is a Ubuntu derivative. The difference is that Ubuntu uses Gnome as its desktop environment, but Xubuntu uses customized Xfce. Hence the name, Ubuntu + Xfce. An IT company calls Eagle Eye Digital Solutions is developing it. The company is based in Oman and focuses on preserving computer anonymity and privacy. There are three ways to use Kodachi. The developer's first and most recommended way is to boot up the Kodachi's ISO file using a virtual machine inside the host machine. The developer recommends using VMware. By default, the system runs in a live mode, ensuring that all the memory is wiped down after every shutdown. However, the system can also be installed inside the virtual machine, which will allow the users to store the files. The second option is to have the ISO file burned on a USB stick, DVD, or SD card and run it in live mode. Even though everything is deleted when the system shuts down, some files can also be saved across different sessions and do not have to wipe completely. Kodachi offers to create persistent storage on USB, which can be encrypted or unencrypted. The last option is to install Kodachi on the hard drive of the host PC. Installation can be done from the desktop of running Kodachi in a live mode, where are two installation files available. One provides online installation and the second offline installation. Both of the installations allow the users to install Kodachi anytime. The offline installation installs all the packages, which are verified with PGP, from an ISO file. The online installation installs everything from the Internet. Another option for how to install Kodachi on the hardware is to install it from the boot menu. The primary purpose of Kodachi was to be an anti-forensic operating system. So with the installation, it loses its main purpose, and it is not anti-forensic anymore. It is only recommended to use it as a live system. However, even installed Kodachi can be secured. It has to be installed as encrypted, and the main OS has to be encrypted as well if it is installed inside the virtual machine [22].

5.1 Applications

Even though Kodachi was created to be an anti-forensic and live system, it can also be used daily. All the applications like media players, video and audio editing applications, image viewers, all Libre office applications, text editors, and many others are pre-installed.

The default web browser is the Kodachi Browser, which is a standard Firefox enhanced to perform better. The Kodachi browser comes in three versions. The first is for people who care about privacy but are not paranoid. It has several plug-ins, and when it launches, it automatically uses the host VPN IP.

The second option, also called Loaded Kodachi Browser, is more secure and has more plug-ins and configurations. After the launch, it automatically connects through Tor and uses the Tor IP.

The third one, Kodachi Ghacks Browser, is the most secure. It is similar to the previous one, but with advanced Ghacks scripting. Most of the visited sites are broken and might look like a mess because Javascript is disabled. The system also comes with Tor Browser and Sphere Tor Browser, a secure browser protected with a password. However, the users can also use the default Firefox, which is an unsafe browser.

Kodachi comes with a few instant messengers pre-installed. Session Messenger is the one most recommended by the developer because of its high security. Nevertheless, users can choose from secure messengers like Element, Signal, Wire, Pidgin, CoyIM, or Bettegram.

The system does not automatically change the MAC address. It is so because some network cards lose their connection when their MAC address changes. Nevertheless, Kodachi comes with a tool to change the MAC address manually. Kodachi does not provide any metadata cleaning, but it comes with MAT, Metadata Anonymization Toolkit like MAT2.

It is recommended to use multiple layers of encryption. That is why Kodachi comes with more encryption utilities, VeraCrypt, ZuluCrypt, and SiriKali. For the users who do not want to use VPN or Tor but connect to the internet service providerdirectly, Kodachi comes with a tool calls Noisy Crawler. Noisy Crawler generates HTTP/DNS traffic noise that looks like more people are browsing the web from the system. Internet service providerwould see queries of websites that

the users did not visit. Since the users do not use any VPN or Tor, the destination IP is leaked. However, it makes the data less valuable for extra obscurity and selling.

Kodachi includes two filesharing tools. The first one, OnionShare, was already described in the section 1.1.2 at the page 4. The second one, which does not rely on the Tor network, calls Syncthing. It runs inside the web browser, so it automatically launches the web browser with the Syncthing web page after the start. The system also comes with KeePassXC and Password and Keys pre-installed. Both of the applications are password managers.

On the desktop are shown information about CPU, disks, VPN, Tor, or Security score. Security score shows how the system is secure. The system comes with a Security Evaluation tool, which helps the users reach the maximum score of 100 [56, 57].

5.2 Features

Kodachi is pre-configured to use VPN, Tor, and DNScrypt to ensure privacy and anonymity.

It also uses AppArmor for application security. When the system starts, Kodachi's VPN, which Kodachi's developer pays, automatically starts. He does not want any user to misuse his VPN bandwidth by downloading huge files like movies or torrent files, killing the VPN's bandwidth. That is why the users can get banned from using it. The banned users need to write an email to the developer and ask him for an unban. To download any stuff without getting banned, the users have to use another VPN. Kodachi comes with another free VPN, VPN Gate, but it is recommended to use Kodachi's VPN, which is more secure. Users can also use Mullvad, NordVPN, Proton, HideMe, or other paid VPNs, which are pre-configured or set up their VPN, which is simple in Kodachi.

The system allows users to stop the VPN. However, when the VPN runs, the users can ensure that the traffic is forced through the VPN. Kodachi comes with two scripts called Force Traffic via VPN, ensuring that all the Internet traffic is blocked when the VPN connection is lost. No packet is allowed to leave the machine when some of the predefined attributes are changed. The first option checks only one

attribute, the IP. The second one also stops the connection when port, interface, or protocol are changed. These scripts do not allow any connections without a VPN, so the real IP will never leak.

Tor also starts automatically after the system's start. Tor can be enabled even without the VPN, but it is not recommended. The users can also torify the entire system, ensuring that no packet leaves the system without entering the TOR network. The system can run only a torified shell, without the whole system being torified. The users can specify one exit node country from the predefined countries or let the system randomly select the exit node country.

With VPN and Tor, Kodachi automatically launches DNScrypt, which is secure and very fast. Another encrypted option is Tor DNS, which is much slower but, on the other hand, much more secure because it is decentralized. Even though DNScrypt is centralized, the developer predefined several properly tested nodes in the config file. One of the nodes is always randomly picked to prevent the IP leak. Kodachi also allows other DNS providers like Open Nic, Mullvad, or Nord DNS, and the users can also set up their DNS.

5.3 Tests

Kodachi can be used in more options. The live mode is the most recommended, so tests are provided in Kodachi running in a virtual machine as a live system.

The system can be used from the first start without any additional settings. The virtual machine takes only a few minutes to start, it depends on the host. Same as Whonix, Kodachi is automatically connected to the Internet if the host is connected. VPN, Tor, and DNScrypt start automatically but can be turned off or changed using predefined scripts that handle each change with a single click.

Kodachi runs smoothly and takes only a few seconds to launch every application. All applications are reasonably divided into tool blocks like Web browsers, Tor tools, System apps, or Security apps.

All browsers start fast. The ones that work with Tor are slower than those without Tor, but it all depends on the internet service provider. If it is fast, then all the browsers in Kodachi are also fast enough. All three versions of the default Kodachi Browser come with many security add-

ons and bookmarks with many websites for security check, DNS check, or proxies, making the browsers even more user-friendly.

By the developer, Session Messenger is the most recommended messenger but currently does not work. All other seven messengers launch pretty fast and are globally commonly used, which is why they are pre-installed in Kodachi. It is needed to create an account to use them, which is straightforward, as the messengers are user-friendly and overall simple to use.

Mozilla Thunderbird is the only one mail application in Kodachi. It is installed in default settings, but the users can easily add any extensions like EnigMail, which adds OpenPGP authentication and message encryption to Thunderbird. Thunderbird is globally used and has a user-friendly interface, intuitive even for common users with low IT skills.

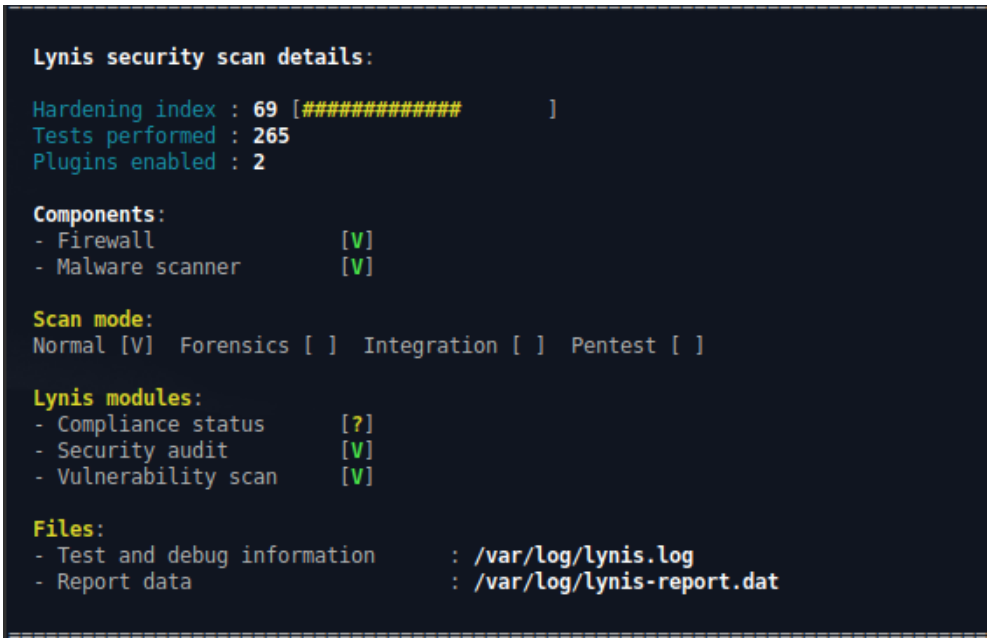

Figure 5.1: Lynis in Kodachi

6 Comparison

All three operating systems are designed for the same, anonymity and privacy, but each achieves it differently.

Table 6.1: Overall properties

	Whonix	Tails	Kodachi
General purpose	Persistent system	Live system	Live system
Based on	Debian	Debian	XUbuntu
Default Desktop	Xfce	Gnome	Xfce
Persistence	Yes	Yes, but it is not recommended	Yes, but it is not recommended
Live mode	Yes	Yes	Yes
Lynis - Hardening Index	68	62	69
hline **Documentation**	Extensive wiki	Extensive documentation on the website	Small documentation on the website
Usability	User-friendly interface and easy to use for everyone	User-friendly interface and easy to use for everyone	User-friendly interface, but it is harder to use for people without knowledge of Linux

Whonix was created to run in a persistent mode and can also run as a live system and has an isolated Workstation from the Gateway for the best security. On the other site, Kodachi and Tails were created to run as live systems, and they do not come with isolation. However,

Kodachi can be installed, and in Tails, Encrypted Persistent Storage allows users to store the files. None of this is recommended.

Whonix has an extensive wiki page where everything about this system is described in detail. It contains complete manuals even for more advanced settings. Tails also offers significant documentation that helps users set up the Encrypted Persistent Storage, or create an email account. However, Kodachi has only small documentation on the main website, which only describes how the system works and how users can increase its security.

All three systems come with a user-friendly interface, which helps users to achieve the highest anonymity and privacy on the Internet. However, Kodachi includes many more applications, and only with small documentation, it can be hard to use for the users with a little Linux knowledge. Whonix and Tails are straightforward, with not too many applications and much better documentation.

Table 6.2: Features

	Whonix	Tails	Kodachi
Tor starts automatically	Yes	Yes	Yes
Built-in VPN	No	No	Yes
Encrypted DNS	Tor DNS	Tor DNS	DNScrypt, Tor DNS
Stream Isolation	Yes	Yes	No
AppArmor	Yes	Yes	Yes
KeyStroke Anonymization	Yes	No	No

Some of the features have all the systems similar. Tor starts automatically when the system connects to the Internet, and all the traffic is forced through the Tor. Nevertheless, Kodachi also comes with another anonymous network, I2P. The users can switch between Tor and I2P, even though Tor is the recommended one. VPN is set up by default only in Kodachi. However, Whonix and Tails both have small documentation of how VPNs can be set up. Even though keyloggers

are becoming still a more significant threat, only Whonix provides KeyStroke Anonymization. None of the systems require any other settings and can be used straight after it launches.

Table 6.3: Applications

	Whonix	Tails	Kodachi
Default Browser	Tor Browser	Tor Browser	Kodachi Browser
Pre-installed Email client	None	ThunderBird	ThunderBird
Pre-installed Instant messenger	HexChat, qTox	Pidgin	Session and 7 other applications
Pre-installed Cryptocurrency wallet	Monero GUI and Electrum	Electrum	Electrum

Whonix and Tails come with a wide selection of pre-installed applications. However, Kodachi comes with many more applications than Whonix or Tails. It includes more than one application for almost every application type, as the developer wants to satisfy everyone. Not all the applications in Kodachi come with the best security.

7 Conclusion

The thesis aimed to provide a survey of the operating systems for anonymity and privacy. There is no single way to design such a system. Every system can be built on different Linux distribution, use a different anonymity network. It depends on the users what they prefer. Some users might prefer anonymity and privacy over usability, and others might need the system to be user-friendly and easy to use, although it may not be as secure.

The most commonly used anonymity network is Tor, and several operating systems are based on it. Some of the operating systems do not use and do not recommend using any VPN. However, others come with VPN built-in, as their developers believe it increases anonymity and privacy.

Although there are many operating systems for anonymity and privacy, as described in the second chapter, not all are regularly updated, and some have not been updated for more than a year. However, three in detail described operating systems are being regularly updated and currently belong to the most used systems for such intent.

There is no one best operating system for everybody, whereas every system is useful for different people and situations. Whonix is designed to run mainly as a persistent system in a virtual machine. It is simple to run this system. However, the host machine needs to be started first, which might take some time. On the other hand, Tails and Kodachi are designed to run as live systems. Tails from USB, CD, or SD card, and Kodachi also in a virtual machine. Tails useful for people who want to use operating system for anonymity and privacy in some public place, as it boots fast and does not leave any traces on the host machine. Kodachi works the same, although it launches slower because it contains many more applications. Nevertheless, Kodachi can also be installed on the hard disk and used as a persistent operating system. From these three operating systems, Kodachi is the one with the most possibilities of use but is also the hardest to use, as it has many features and applications but almost no documentation.

Bibliography

1. GRITZALIS, Stefanos. Enhancing web privacy and anonymity in the digital era. *Information Management & Computer Security*. 2004.
2. BORST, Karl Joseph; BRAUND, Stephen. *Website with activities triggered by clickable ads*. Google Patents, 2011. US Patent App. 12/893,430.
3. MENDEL, Toby; PUDDEPHATT, Andrew; WAGNER, Ben; HAWTIN, Dixie; TORRES, Natalia. *Global survey on Internet privacy and freedom of expression*. UNESCO, 2012.
4. KRAIJAK, Surapon; TUWANUT, Panwit. A survey on internet of things architecture, protocols, possible applications, security, privacy, real-world implementation and future trends. In: *2015 IEEE 16th International Conference on Communication Technology (ICCT)*. 2015, pp. 26–31.
5. GUNAWAN, Teddy Surya; LIM, Muhammad Kassim; ZULKURNAIN, Nurul Fariza; KARTIWI, Mira. On the Review and Setup of Security Audit Using Kali Linux. *Indonesian Journal of Electrical Engineering and Computer Science*. 2018, vol. 11, no. 1, pp. 51–59.
6. KUIPERS, David; FABRO, Mark. *Control systems cyber security: Defense in depth strategies*. 2006. Tech. rep. Idaho National Laboratory (INL).
7. VON HAGEN, William. *Through the Web, Darkly: Privacy, Anonymity, and the Dark Web*. Pittsburg: William Von Hagen, 2019. ISBN 978-0-578-56194-3.
8. SYVERSON, Paul; DINGLEDINE, Roger; MATHEWSON, Nick. Tor: The secondgeneration onion router. In: *Usenix Security*. 2004, pp. 303–320.
9. HUANG, Hsiao-Ying; BASHIR, Masooda. The onion router: Understanding a privacy enhancing technology community. *Proceedings of the Association for Information Science and Technology*. 2016, vol. 53, no. 1, pp. 1–10.

10. *Tor* [online]. The Tor Project, 2014/2020 [visited on 2020-12-27]. Available from: `https://2019.www.torproject.org/about/overview.html.en`.

11. JADOON, Abid Khan; IQBAL, Waseem; AMJAD, Muhammad Faisal; AFZAL, Hammad; BANGASH, Yawar Abbas. Forensic analysis of Tor browser: a case study for privacy and anonymity on the web. *Forensic science international*. 2019, vol. 299, pp. 59–73.

12. *Tor Browser* [online]. The Tor Project, 2014/2020 [visited on 2020-12-27]. Available from: `https://tb-manual.torproject.org/about/`.

13. HASSAN, Nihad A; HIJAZI, Rami. Online Anonymity. In: *Digital Privacy and Security Using Windows*. Springer, 2017, pp. 123–194.

14. KIRAN, Kumar; CHALKE, Saurabh S; USMAN, Mohammad; SHENOY, PraDeepa; VENUGOPAL, KR. Anonymity and Performance Analysis of Stream Isolation in Tor Network. In: *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. 2019, pp. 1–6.

15. GRUENBACHER, Andreas; ARNOLD, Seth. *AppArmor Technical Documentation*. 2007.

16. KILLOURHY, Kevin S; MAXION, Roy A. Comparing anomaly-detection algorithms for keystroke dynamics. In: *2009 IEEE/IFIP International Conference on Dependable Systems & Networks*. 2009, pp. 125–134.

17. MIGDAL, Denis; ROSENBERGER, Christophe. Keystroke Dynamics Anonymization System. In: *ICETE (2)*. 2019, pp. 448–455.

18. MONACO, John V; TAPPERT, Charles C. Obfuscating keystroke time intervals to avoid identification and impersonation. *arXiv preprint arXiv:1609.07612*. 2016.

19. ZENG, Marcia Lei. *Metadata*. Neal-Schuman Publishers, Inc., 2008.

20. *Tails* [online]. Tails, 2011/2020 [visited on 2020-12-01]. Available from: `https://tails.boum.org/index.en.html`.

21. *Whonix* [online]. Whonix, 2011/2020 [visited on 2020-11-01]. Available from: https://www.whonix.org/wiki/Main_Page.

22. *Kodachi* [online]. Warith Al Maawali, 2013/2020 [visited on 2020-12-15]. Available from: https://www.digi77.com/linux-kodachi/.

23. *Parrot OS* [online]. Parrot Security, 2013/2020 [visited on 2020-10-20]. Available from: https://www.parrotsec.org/.

24. *Subgraph OS* [online]. Subgraph, 2014/2020 [visited on 2020-10-20]. Available from: https://subgraph.com/.

25. *Ipredia OS* [online]. Ipredia, 2015/2020 [visited on 2020-10-20]. Available from: https://www.ipredia.org/.

26. *Mofolinux* [online]. Mofolinux, 2015/2020 [visited on 2020-10-20]. Available from: https://mofolinux.com.

27. BILGE, Leyla; DUMITRAŞ, Tudor. Before we knew it: an empirical study of zero-day attacks in the real world. In: *Proceedings of the 2012 ACM conference on Computer and communications security*. 2012, pp. 833–844.

28. *Heads OS* [online]. Heads, 2013/2020 [visited on 2020-10-20]. Available from: https://heads.dyne.org/.

29. *Robolinux* [online]. John Martinson, 2013/2020 [visited on 2020-10-20]. Available from: https://robolinux.org/about.html.

30. *KickSecure* [online]. Whonix, 2013/2020 [visited on 2020-11-05]. Available from: https://www.whonix.org/wiki/Kicksecure.

31. *Whonix and Tor* [online]. Whonix, 2013/2020 [visited on 2020-11-06]. Available from: https://www.whonix.org/wiki/Whonix_and_Tor.

32. *Whonix - Stream Isolation* [online]. Whonix, 2013/2020 [visited on 2020-11-08]. Available from: https://www.whonix.org/wiki/Stream_Isolation.

33. *Whonix - Other Operating Systems* [online]. Whonix, 2013/2020 [visited on 2020-11-07]. Available from: https://www.whonix.org/wiki/Other_Operating_Systems.

34. *Whonix - Gateway* [online]. Whonix, 2013/2020 [visited on 2020-11-07]. Available from: https://www.whonix.org/wiki/Whonix-Gateway.

35. *Whonix - Tor Controller* [online]. Whonix, 2013/2020 [visited on 2020-11-07]. Available from: https://www.whonix.org/wiki/Tor_Controller#Arm.

36. *Whonix - Anon Connection Wizard* [online]. Whonix, 2013/2020 [visited on 2020-11-07]. Available from: https://www.whonix.org/wiki/Anon_Connection_Wizard.

37. *Whonix - WhonixCheck* [online]. Whonix, 2013/2020 [visited on 2020-11-07]. Available from: https://www.whonix.org/wiki/Whonixcheck.

38. *Whonix - Gateway Firewall* [online]. Whonix, 2013/2020 [visited on 2020-11-07]. Available from: https://www.whonix.org/wiki/Whonix-Gateway_Firewall.

39. *Whonix - Workstation* [online]. Whonix, 2013/2020 [visited on 2020-11-07]. Available from: https://www.whonix.org/wiki/Whonix-Workstation.

40. *Whonix - Instant Messenger Chat* [online]. Whonix, 2013/2020 [visited on 2020-11-06]. Available from: https://www.whonix.org/wiki/Chat.

41. *Whonix - Software* [online]. Whonix, 2013/2020 [visited on 2020-11-08]. Available from: https://www.whonix.org/wiki/Software.

42. VOISIN, Julien; GUYEUX, Christophe; BAHI, Jacques M. The metadata anonymization toolkit. *arXiv preprint arXiv:1212.3648*. 2012.

43. *Whonix - Live Mode* [online]. Whonix, 2013/2020 [visited on 2020-11-06]. Available from: https://www.whonix.org/wiki/VM_Live_Mode.

44. *Whonix - Dev/TimeSync* [online]. Whonix, 2013/2020 [visited on 2020-11-06]. Available from: https://www.whonix.org/wiki/Dev/TimeSync.

45. *Tails - Kernel hardening* [online]. Tails, 2011/2020 [visited on 2020-12-09]. Available from: https://tails.boum.org/contribute/design/kernel_hardening/.

46. *Tails - Tor* [online]. Tails, 2011/2020 [visited on 2020-12-09]. Available from: https://tails.boum.org/doc/about/tor/index.en.html.

47. *Tails - How it works* [online]. Tails, 2011/2020 [visited on 2020-12-09]. Available from: https://tails.boum.org/about/index.en.html.

48. *Tails - Persistence* [online]. Tails, 2011/2020 [visited on 2020-12-09]. Available from: https://tails.boum.org/contribute/design/persistence/.

49. *Tails - Encrypted Persistence Storage* [online]. Tails, 2011/2020 [visited on 2020-12-09]. Available from: https://tails.boum.org/doc/first_steps/persistence/configure/index.en.html.

50. *Tails - Tor Browser* [online]. Tails, 2011/2020 [visited on 2020-12-10]. Available from: https://tails.boum.org/doc/anonymous_internet/Tor_Browser/index.en.html.

51. *Pidgin* [online]. Pidgin, 2011/2020 [visited on 2020-12-10]. Available from: https://www.pidgin.im/.

52. *Tails - Thunderbird* [online]. Tails, 2011/2020 [visited on 2020-12-11]. Available from: https://tails.boum.org/doc/anonymous_internet/thunderbird/index.en.html.

53. WINTER, Brenno de; MOLLARD, Michael Fischer v. Gnu Privacy Guard (GnuPG) Mini Howto. *retrieved from the Internet: http://www. gnupg. org/documentation/howtos. en. html, version 0.1*. 2003, vol. 4.

54. *Tails - OpenPGP Applet* [online]. Tails, 2011/2020 [visited on 2020-12-11]. Available from: https://tails.boum.org/doc/encryption_and_privacy/gpgapplet/index.en.html.

55. *Tails - LUKS* [online]. Tails, 2011/2020 [visited on 2020-12-12]. Available from: https://tails.boum.org/doc/encryption_and_privacy/encrypted_volumes/index.en.html.

56. *Interview by the Russian OSINT and Linux Kodach 7.1 Walk through - E16* [online]. Tech and Crypto Vibes, 2020-07-10 [visited on 2020-12-15]. Available from: https://www.youtube.com/watch?v=dVVqiuWxdjs&ab_channel=TechandCryptoVibes.

57. *Linux Kodachi 4.0 security OS x Full walk around and how to install it - E13* [online]. Tech and Crypto Vibes, 2018-10-05 [visited on 2020-12-16]. Available from: https://www.youtube.com/watch?v=tZiH1jmN3WE&ab_channel=TechandCryptoVibes.