

The Amnesiac Incognito System and Tor Project: Anonymity in Times of Mass Surveillance

Guilherme O. Santos¹

¹Instituto de Ciências Exatas e Aplicadas – Universidade Federal de Ouro Preto (UFOP)
Caixa Postal 24 - 35.930-970 - João Monlevade - MG - Brazil

Abstract. *In an era of unprecedented global surveillance and threats to digital privacy, tools that empower individuals to maintain anonymity and security online have become crucial. Tails, a Linux-based operating system tailored for privacy, and the Tor Project, the organization behind the widely-used Tor anonymity network, have emerged as cornerstones of secure online communication. This article delves into the features, strengths, and limitations of both Tails and the Tor network, analyzing their symbiotic relationship and their collective impact on defending democracy, protecting human rights, and enabling freedom of expression.*

Resumo. *Em uma era de vigilância global sem precedentes e ameaças à privacidade digital, ferramentas que permitem aos indivíduos manter anonimato e segurança online tornaram-se indispensáveis. O Tails, um sistema operacional baseado em Linux projetado para privacidade, e o Tor Project, a organização responsável pela amplamente utilizada rede de anonimato Tor, emergem como pilares da comunicação segura na internet. Este artigo explora os recursos, pontos fortes e limitações de ambos, analisando sua relação simbiótica e impacto coletivo na defesa da democracia, proteção dos direitos humanos e promoção da liberdade de expressão.*

1. Introduction

The digital age has brought about advancements but also significant challenges, particularly concerning online privacy and security. Surveillance by governments and corporations has reached unprecedented levels, threatening not only individual privacy but also fundamental rights such as freedom of expression and access to information. In this context, tools that provide robust anonymity and privacy are vital.

This article focuses on the synergy between Tails (The Amnesic Incognito Live System), a Linux-based operating system specifically designed to preserve privacy, and the Tor Project, the non-profit organization that develops the widely-used Tor anonymity network. Both tools share a mission of enabling secure, anonymous communication in an era of mass surveillance and censorship.

1.1. Objectives

The objective of this paper is to analyze Tails and Tor strengths, limitations, security flaws, also how the impact with the merge between them can lead to new fight for freedom and democracy.

1.2. The right of anonymity

The right to privacy is essential for various reasons, not only for individuals but also for private companies and government entities, all of which rely on different levels of confidentiality. Journalists must protect their sources, private companies need to safeguard their technological innovations to prevent economic losses, and governments often collect sensitive data for national security purposes, which must be protected to avoid catastrophic data breaches. A prime example of such a breach occurred Brazil in 2021, in the midst of the coronavirus pandemic when the personal data of 223 million Brazilians was exposed in a massive leak [G1].

The issues of surveillance and espionage have always been present, but they have become more complex with time. For example, [O Globo] article discusses the National Security Agency (NSA) espionage activities targeting Brazilian citizens and companies, a case revealed through classified documents leaked by Edward Snowden. These disclosures highlighted the NSA's extensive surveillance practices, including monitoring communications of Brazilian officials, corporations like Petrobras, and even then-President Dilma Rousseff. Another example it was Linus Torvalds disclosing that the NSA requested a backdoor in the Linux operating system [Greenwald 2014].

2. The Tor Project

Today, Tor has thousands of volunteer-run relays and millions of users around the world. It is a vital tool for privacy and online freedom [The Tor Project Docs]. In this section, we will talk about Tor history, how it was created and modified over the years, briefly mention what its functionality is like and its Limitations.

2.1. History

In the 1990s, people realized that the internet was not secure and could be used for surveillance [The Tor Project Docs]. In 1995, researchers at the U.S. Naval Research Lab (NRL) began working on a way to create anonymous internet connections. Their solution was called "onion routing," where internet traffic is sent through multiple servers and encrypted at each step [Archive].

In the early 2000s, [Dingledine], joined the project and renamed it **Tor** (The Onion Routing). The goal of Tor was a creation of a circuit-based low-latency anonymous communication service. This second-generation Onion Routing system addresses limitations in the original design by adding perfect forward secrecy, congestion control, directory servers, integrity checking, configurable exit policies, and a practical design for location-hidden services via rendezvous points. In 2002, the Tor network was launched with its code released for free.

The Electronic Frontier Foundation (EFF) supported Tor's development starting in 2004, and in 2006, the Tor Project, Inc. was founded to maintain the software. Over time, Tor grew in popularity, especially among activists, and Tor Browser was created to make Tor easier to use.

Tor gained significant attention during the 2010 Arab Spring, where it helped protect activists' identities and bypass censorship [The Tor Project Docs]. Its importance grew further, showing that Tor could not easily be cracked.

2.2. How it works

Tor is a network of virtual tunnels that allows you to improve your privacy and security on the Internet. Tor works by sending your traffic through three random servers (also known as relays) in the Tor network. The last relay in the circuit (the "exit relay") then sends the traffic out into the public Internet. The more people who use the Tor network, the better it works for keeping everyone anonymous.

"It's easier to hide in a large crowd than to stand out in a smaller one."
- [Cardenas-Haro and Dawson 2017]"

It's important not only to protect the content of our conversations but also who we talk to and when. To keep this safe, we need encryption and random routing of data. The Figure 1 illustrates a user browsing a website over Tor, and the Figure 2 show in details how setup begins with the OP selecting an entry OR and exchanging keys. Once the entry OR replies with "created" the OP extends the circuit hop by hop until complete. Then, the OP sends a begin command with the destination address, initiating a TCP handshake with the website before transmitting data (e.g., a GET request) [Basyoni et al. 2023].

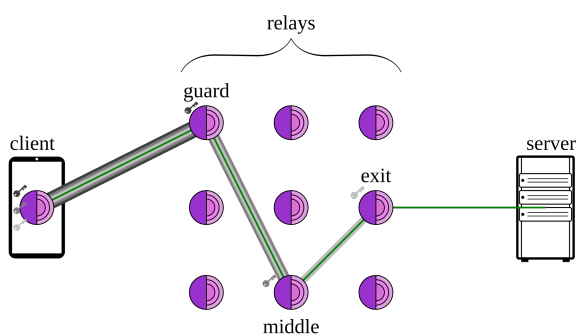


Figura 1. Example of how Tor works [The Tor Project Docs].

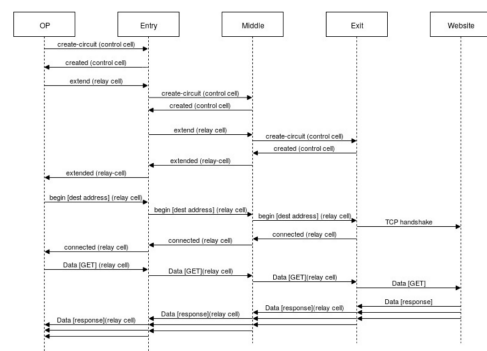


Figura 2. Tor circuit creation [Basyoni et al. 2023]

2.3. Attacks and Limitations

Like all software, Tor's protections have limitations, and Tor's implementation or design have been vulnerable to attacks at various points throughout its history.

[Mandela et al. 2023] conducted a forensic analysis of the unencrypted layer in the Tor network to evaluate how network traffic analysis could uncover user online activities for criminal investigations. The study demonstrated the feasibility of de-anonymizing Tor users and identifying their online actions by analyzing the unencrypted headers of their network packets. These findings highlight that, although the Tor network serves as a vital tool for online privacy and security, it is not without vulnerabilities, emphasizing the need for users to implement additional measures to safeguard their privacy and security.

According to [Basyoni et al. 2023], a commonly adopted threat model for many attacks involves the presence of one or more malicious Tor relays, either compromised by the attacker or operated by them from the outset.

[Le Blond et al. 2011] carried out an attack on BitTorrent users by targeting clients that established connections both through Tor and without it, and then correlating other connections that shared the same Tor circuit.

3. The Amnesic Incognito Live System

In this section, we explore Tails and its role in ensuring digital privacy and anonymity, its history, the significant 2024 merger with the Tor Project, and its core functionalities.

3.1. History

Tails was first released on June 23, 2009. It is the next iteration of development on Incognito, a discontinued Gentoo-based Linux distribution [Gray 2011]. The Tor Project provided financial support for its development in the beginnings of the project [Finances 2013]. In 2023, the Tails Project approached the Tor Project to merge operations. The merger was completed on September 26, 2024, stating that:

”By bringing these two organizations together, we’re not just making things easier for our teams, but ensuring the sustainable development and advancement of these vital tools. Working together allows for faster, more efficient collaboration, enabling the quick integration of new features from one tool to the other. This collaboration strengthens our mission and accelerates our ability to respond to evolving threats.”

– Isabela Fernandes, Executive Director, The Tor Project.

Other security-focused operating systems that make or made extensive use of Tor include Linux From Scratch (LFS), Liberté Linux, Qubes OS, Subgraph, Parrot OS, Tor-ramdisk, and Whonix.

3.2. Why tails ?

The Tails Linux distribution gained significant recognition after being revealed as the operating system used by Snowden, the whistleblower who exposed the PRISM surveillance program to The Guardian and The Washington Post [Franceschi-Bicchierai 2020], [Greenwald 2014].

As Snowden himself emphasized:

”If you look at the way post-2013 whistleblowers have been caught, it is clear the absolute most important thing you can do to maintain your anonymity is reduce the number of places in your operational activity where you can make mistakes. Tor and Tails still do precisely that.”

— Edward Snowden, [Tails Team Docs 2024].

Unlike the operating systems mentioned above, tails has unique peculiarities. It operates entirely from removable media, such as a USB stick or DVD, and ensures that all data is erased upon reboot, leaving no traces behind. For secure file deletion, Tails includes the Nautilus Wipe tool, which completely removes files, unlike conventional systems that may leave residual data.

A old feature of Tails was its ability to camouflage its interface to resemble Windows operating systems, enabling discreet use in public spaces without drawing attention. This built-in feature has been discontinued because the developer which worked on it no longer contributes to the project. But users can still install it from other open source sources. For instance, Figure 3 depicts an camouflage mimicking Windows XP, while Figure



Figura 3. Tails Windows XP Camouflage

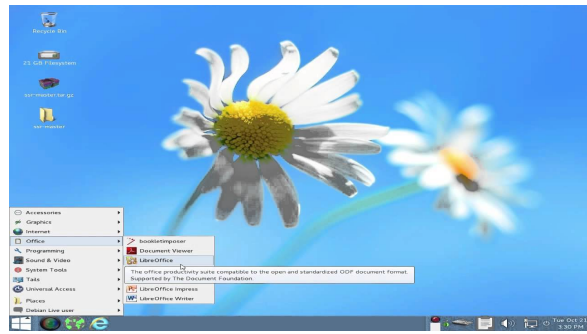


Figura 4. Tails Windows 8 Camouflage

4 illustrates a camouflage styled after Windows 8, including similar icons and interface elements to enhance its believability.

All network traffic in Tails is routed through the Tor network, ensuring anonymity and privacy. Media Access Control (MAC) spoofing is implemented to prevent tracking based on the physical address of wireless or Ethernet network cards. This process assigns randomized MAC addresses to network interfaces, as illustrated in Figure 5. Tails also optionally supports the Invisible Internet Project (I2P), an anonymous network layer that facilitates peer-to-peer communication. Together, these mechanisms ensure that users avoid leaving any digital footprint.

```
3: veth-tbb@if2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu
  link/ether 1a:77:39:ec:10:86 brd ff:ff:ff:ff:ff:ff
5: veth-onioncircs@if4: <BROADCAST,MULTICAST,UP,LOWER_UP>
  link/ether 76:86:9e:b0:2a:44 brd ff:ff:ff:ff:ff:ff
7: veth-tca@if6: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu
  link/ether 6e:0a:7f:7d:5a:53 brd ff:ff:ff:ff:ff:ff
9: veth-onionshare@if8: <BROADCAST,MULTICAST,UP,LOWER_UP>
  link/ether c2:61:31:2f:79:2c brd ff:ff:ff:ff:ff:ff
11: veth-clearnet@if10: <BROADCAST,MULTICAST,UP,LOWER_UP>
  link/ether 06:ea:96:0d:ab:16 brd ff:ff:ff:ff:ff:ff
12: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500
  link/ether 60:c7:XXXXXXXXXX brd ff:ff:ff:ff:ff:ff
13: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500
  link/ether 04:ec:XXXXXXXXXX brd ff:ff:ff:ff:ff:ff
```

Figura 5. Example of various MAC addresses generated by Tails.

Type	MAC Address
Ethernet	60:c7:XX:XX:XX:XX
Wi-Fi	04:ec:XX:XX:XX:XX
Spoofed MAC 1	1a:77:39:ec:10:86
...	...
Spoofed MAC 5	06:ea:96:0d:ab:16

Tabela 1. MAC addresses, based on Figure 5.

The system employs advanced cryptographic tools to secure files, emails, and messages. For instance, it uses LUKS (Linux Unified Key Setup) for disk encryption. Figure 6 demonstrates the creation of an encrypted partition by Tails, allocating 6.5 GB to `/dev/sdb2` for the persistent storage feature, while the operating system resides on `/dev/sdb1`.

Figure 7 provides a closer look at the structure of the encrypted partition, highlighting its directories and files:

- `.` and `..`: Represent the current directory (`.`) and the parent directory (`..`), standard in Unix-like systems.
- `apt/`: Stores APT package management data, enabling Tails users to persist software installation preferences.

- `dont-ask-again/`: Contains user preferences or configurations to suppress prompts for specific actions or warnings.
- `live-additional-software.conf`: A configuration file specifying additional software packages to load at startup or retain in persistent storage.
- `lost+found/`: A directory automatically created on ext-based filesystems for recovering corrupted or lost files.
- `persistence.conf`: The configuration file defining the data to be stored persistently and encrypted in Tails.
- `Persistent/`: A secure and encrypted space within the partition, enabling users to retain specific files, configurations, and settings across sessions. This feature is particularly valuable for securely storing documents, encryption keys, and custom application settings without compromising the system's ephemeral nature.

```
sdb                8:16  1  14,5G  0 disk
├─sdb1             8:17  1    8G   0 part
└─sdb2             8:18  1   6,5G  0 part
    └─luks-896b171f-aaa9-43c4-ae7-66d6c8eb5fd6
```

Figura 6. Encrypted Partition with LUKS

```
total 40
drwxrwx---+ 6 root  root  4096 dez  2 12:54 .
drwxr-x---+ 3 root  root   60 dez  3 08:29 ..
drwx----- 4 root  root  4096 nov 28 22:46 apt
drwx----- 2 olive1r4 olive1r4 4096 nov 28 22:46 dont-ask-again
-rw-r--r--  1 115   122    3 dez  2 10:30 live-additional-software.conf
drwx----- 2 root  root 16384 nov 28 22:44 lost+found
-rw-----  1 115   122   120 dez  2 12:54 persistence.conf
drwx----- 5 olive1r4 olive1r4 4096 dez  3 08:02 Persistent
```

Figura 7. Contents of /dev/sdb2

Forced HTTPS for all website communications, and OpenPGP for email encryption are also built-in features. Tails also supports Off-the-Record messaging for secure, deniable chat. Its features include tools for metadata anonymization, a virtual keyboard to avoid keyloggers, and the “Shamir’s Secret Sharing” algorithm for encrypted message decryption by multiple participants.

The system includes security measures like automatic RAM clearing on shutdown to prevent cold boot attacks, the AppArmor security module to limit program resource access, updates to address security vulnerabilities and is built entirely with open-source software for trust and transparency [Cardenas-Haro and Dawson 2017].

3.3. Weakness, Limitations and Security incidents

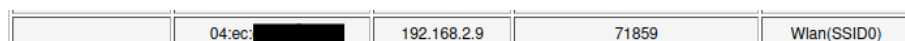
Like any system, Tails has its limitations. Being a Debian-based system, it is designed to minimize vulnerabilities, so the chances of a flaw affecting the entire system are rare. However, since Tails integrates multiple tools, any weakness in one could still compromise the system. Moreover, effectively using Tails requires a certain level of technical knowledge, as many of its tools are not specifically tailored for ease of use [Cardenas-Haro and Dawson 2017].

According to [Basyoni et al. 2023], in 2017, the FBI used malicious code developed by Facebook, identifying sexual extortionist and Tails user Buster Hernandez through a zero-day vulnerability in the default video player. The exploit was never explained to or discovered by the Tails developers, but it is believed that the vulnerability was patched in a later release of Tails.

A important factor that needs close attention is the metadata. Tails does not clear it for us, but it provides the tools necessary for the removal of information that can help to

identify us from the metadata, before sending any of the files. In the case of e-mails even if we encrypt the contents, the subject and other headers remain understandable.

Another vulnerability lies in network-level tracking. Network administrators can still view the real MAC address of a device through a router's management interface, even when using Tails. This exposes users to potential privacy and security risks, particularly when connecting to open or untrusted wireless networks. Figure 8 illustrates how a router can display the real MAC address of a user, despite the safeguards implemented by Tails.



04:ec: [redacted]	192.168.2.9	71859	Wlan(SSID0)
-------------------	-------------	-------	-------------

Figura 8. Real MAC address of a machine running Tails as seen on a network router

4. Conclusions

The right to privacy is a cornerstone of democracy and a fundamental human right, yet it faces significant challenges from unreasonable searches, mass surveillance, and corporate exploitation of personal data. Encryption and privacy-focused technologies play a dual role: while they may complicate law enforcement's work, they are essential for protecting individuals' freedoms and safeguarding against abuse.

Through this study, we emphasize that tools like Tails Linux and Tor are not merely technologies; they are instruments of resistance against surveillance and a means of upholding privacy. The continued use and development of such tools are vital in ensuring the fundamental rights of individuals in the digital age.

Open-source technologies such as Linux, Tails, Tor, and privacy-centric cryptocurrencies like Monero empower users to operate beyond the reach of government overreach and corporate control. These tools, often mischaracterized as enablers of criminal activity, are indispensable for journalists, activists, dissidents, and law enforcement agents working under oppressive regimes. The prevalence of mass surveillance by governments and corporations poses a severe threat to democracy, eroding trust and curtailing personal autonomy.

Referências

- Archive, T. O. R. Archives. <https://www.onion-router.net/Archives.html>. Accessed: 2024-11-30.
- Basyoni, L., Fetais, N., Erbad, A., Mohamed, A., and Guizani, M. (2023). Traffic analysis attacks on tor: A survey. *Kindi Center for Computing Research, Qatar University*. Emails: lamiaa@qu.edu.qa, n.almarri@qu.edu.qa, aerbada@qu.edu.qa, amrm@qu.edu.qa, mguizani@qu.edu.qa.
- Cardenas-Haro, J. A. and Dawson, M. (2017). Tails linux operating system: The amnesiac incognito system in times of high surveillance, its security flaws, limitations, and strengths in the fight for democracy. In Dawson, M. et al., editors, *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications*, pages 260–271. IGI Global.
- Dingledine, R. Tor: The second-generation onion router. <https://css.csail.mit.edu/6.858/2022/readings/tor-design.pdf>. Accessed: 2024-12-01.
- Finances, T. (2013). Finances. <https://tails.boum.org>. Archived from the original on March 29, 2019. Retrieved May 13, 2013.
- Franceschi-Bicchierai, L. (2020). Facebook helped the fbi hack a child predator. *Vice*. Archived from the original on June 13, 2020. Retrieved June 12, 2020.
- G1. Vazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber. <https://shorturl.at/bkHdV>. Accessed: 2024-11-30.
- Gray, J. (2011). The tails project's the amnesiac incognito live system (tails). *Linux Journal*. Archived from the original on August 13, 2019. Retrieved August 12, 2012.
- Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State*. Macmillan.
- Le Blond, S., Manils, P., Chaabane, A., Kaafar, M. A., Castelluccia, C., Legout, A., and Dabbous, W. (2011). One bad apple spoils the bunch: Exploiting p2p applications to trace and profile tor users. In *4th USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET '11)*. National Institute for Research in Computer Science and Control. Archived (PDF) from the original on April 27, 2011. Retrieved April 13, 2011.
- Mandela, N., Mahmoud, A. A. S., and Agrawal, A. K. (2023). A forensic analysis of the tor network in tails operating system. In *2023 10th International Conference on Computing for Sustainable Global Development (INDIACom)*, pages 546–551.
- O Globo. Relembra caso de espionagem da nsa a cidadãos e empresas no brasil. <https://shorturl.at/z4tVB>. Accessed: 2024-12-02.
- Tails Team Docs (2024). Tails documentation. <https://tails.net/doc/>. Accessed: 2024-11-30.
- The Tor Project Docs. History of tor. <https://www.torproject.org/about/>. Accessed: 2024-11-27.