



Tails Os

SYSTEM OPERACYJNY

Maria Budziło, Ivasenko Kateryna

WYDZIAŁ INŻYNIERII MATERIAŁOWEJ I FIZYKI Politechnika Krakowska im.
Tadeusza Kościuszki

Grudzień 17, 2020

Plan

WPROWADZENIE

ZNACZENIE

TAILS: THE AMNESIC INCOGNITO LIVE SYSTEM
UŻYWAJ GO WSZĘDZIE NIE POZOSTAWIAJĄC ŚLADÓW
ANONIMOWOŚĆ ONLINE Z TOR

TAILS OS

GNOME DESKTOP

ZGODNOŚĆ SPRZĘTU

INSTALACJA

NETWORKING

OPROGRAMOWANIE NIE ZAWARTE W TAILS

INNE KWESTIE BEZPIECZEŃSTWA



WPROWADZENIE

- Tails to system operacyjny, taki jak Windows lub Mac OS, ale specjalnie zaprojektowany, aby zachować anonimowość i prywatność
- Tails lub The Amnesic Incognito Live System to skoncentrowana na bezpieczeństwie dystrybucja Linuksa
- Bezpieczeństwo połączeń wychodzących zapewnia Tor



WPROWADZENIE

- Tails to system operacyjny, taki jak Windows lub Mac OS, ale specjalnie zaprojektowany, aby zachować anonimowość i prywatność
- Tails lub The Amnesic Incognito Live System to skoncentrowana na bezpieczeństwie dystrybucja Linuksa
- Bezpieczeństwo połączeń wychodzących zapewnia Tor



WPROWADZENIE

- Tails to system operacyjny, taki jak Windows lub Mac OS, ale specjalnie zaprojektowany, aby zachować anonimowość i prywatność
- Tails lub The Amnesic Incognito Live System to skoncentrowana na bezpieczeństwie dystrybucja Linuksa
- Bezpieczeństwo połączeń wychodzących zapewnia Tor

ZNACZENIE

1. TAILS: THE AMNESIC INCOGNITO LIVE SYSTEM
2. UŻYWAJ GO WSZĘDZIE NIE POZOSTAWIAJĄC ŚLADÓW
3. ANONIMOWOŚĆ ONLINE Z TOR
4. NARZĘDZIA DO SZYFROWANIA



ZNACZENIE

1. TAILS: THE AMNESIC INCOGNITO LIVE SYSTEM
2. UŻYWAJ GO WSZĘDZIE NIE POZOSTAWIAJĄC ŚLADÓW
3. ANONIMOWOŚĆ ONLINE Z TOR
4. NARZĘDZIA DO SZYFROWANIA



ZNACZENIE

1. TAILS: THE AMNESIC INCOGNITO LIVE SYSTEM
2. UŻYWAJ GO WSZĘDZIE NIE POZOSTAWIAJĄC ŚLADÓW
3. ANONIMOWOŚĆ ONLINE Z TOR
4. NARZĘDZIA DO SZYFROWANIA



ZNACZENIE

1. TAILS: THE AMNESIC INCOGNITO LIVE SYSTEM
2. UŻYWAJ GO WSZĘDZIE NIE POZOSTAWIAJĄC ŚLADÓW
3. ANONIMOWOŚĆ ONLINE Z TOR
4. NARZĘDZIA DO SZYFROWANIA





TAILS: THE AMNESIC INCOGNITO LIVE SYSTEM

1. Umożliwia prawie anonimowe korzystanie z Internetu wszędzie online i na dowolnym komputerze, ale nie pozostawia śladu tego, co zrobiłeś, chyba że chcesz
2. Tails to system działający na żywo
3. Jest on darmowym oprogramowaniem opartym na systemie Debianie
4. Tails jest dostarczany z aplikacjami, które zostały skonfigurowane z myślą o bezpieczeństwie



TAILS: THE AMNESIC INCOGNITO LIVE SYSTEM

1. Umożliwia prawie anonimowe korzystanie z Internetu wszędzie online i na dowolnym komputerze, ale nie pozostawia śladu tego, co zrobiłeś, chyba że chcesz
2. Tails to system działający na żywo
3. Jest on darmowym oprogramowaniem opartym na systemie Debianie
4. Tails jest dostarczany z aplikacjami, które zostały skonfigurowane z myślą o bezpieczeństwie



TAILS: THE AMNESIC INCOGNITO LIVE SYSTEM

1. Umożliwia prawie anonimowe korzystanie z Internetu wszędzie online i na dowolnym komputerze, ale nie pozostawia śladu tego, co zrobiłeś, chyba że chcesz
2. Tails to system działający na żywo
3. Jest on darmowym oprogramowaniem opartym na systemie Debianie
4. Tails jest dostarczany z aplikacjami, które zostały skonfigurowane z myślą o bezpieczeństwie

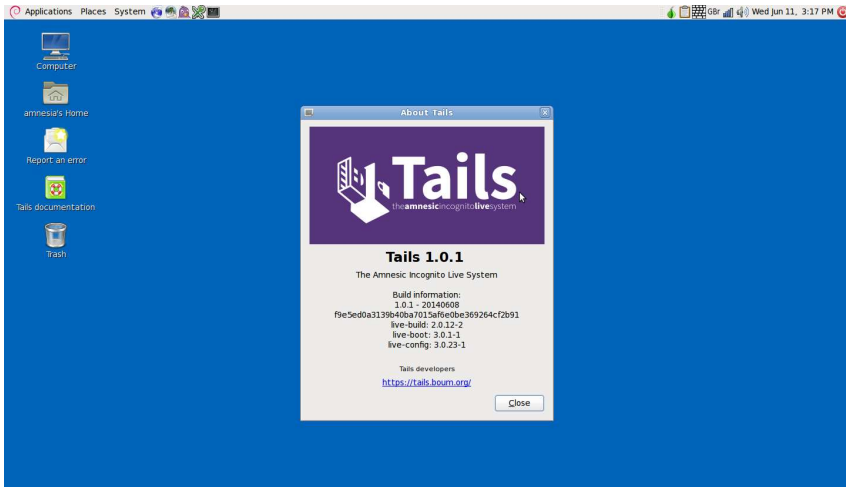


TAILS: THE AMNESIC INCOGNITO LIVE SYSTEM

1. Umożliwia prawie anonimowe korzystanie z Internetu wszędzie online i na dowolnym komputerze, ale nie pozostawia śladu tego, co zrobiłeś, chyba że chcesz
2. Tails to system działający na żywo
3. Jest on darmowym oprogramowaniem opartym na systemie Debianie
4. Tails jest dostarczany z aplikacjami, które zostały skonfigurowane z myślą o bezpieczeństwie



THE AMNESIC INCOGNITO LIVE SYSTEM





UŻYWAJ GO WSZĘDZIE NIE POZOSTAWIAJĄC ŚLADÓW

- Możesz go używać w domu, u znajomego lub w lokalnej bibliotece



UŻYWAJ GO WSZĘDZIE NIE POZOSTAWIAJĄC ŚLADÓW

- Umożliwia pracę nad poufnym plikiem na dowolnym komputerze i zapobiega odzyskiwaniu danych po wyłączeniu komputera.



ANONIMOWOŚĆ ONLINE Z TOR

1. Tails polega na sieciach Tor, aby chronić prywatność w Internecie
2. Całe oprogramowanie jest skonfigurowane do łączenia się przez Tor



ANONIMOWOŚĆ ONLINE Z TOR

1. Tails polega na sieciach Tor, aby chronić prywatność w Internecie
2. Całe oprogramowanie jest skonfigurowane do łączenia się przez Tor



TAILS OS

Ogólne cechy charakterystyczne Tails

Obsługiwany sprzęt	x86 i / lub maszyny wirtualne
Oparty na	Tor, Debian
Bramka i torify dowolnego systemu operacyjnego	Nie torifying Bramka.
Odpowiedzialny za budowanie obwodów Tora (sieci) na stacji roboczej	Klient Tor działający
Stacja robocza nie musi ufać bramie	To nie jest brama
Szyfrowanie dysku lokalnego	Tak, dla trwałego USB.
Ochrona przed atakiem zimnego rozruchu	Tak

GNOME DESKTOP

Tails wspierany jest przez graficzne środowisko GNOME. Główną wadą GNOME jest to, że do prawidłowego działania wymaga sporo zasobów, ale ma też wiele zalet.



Zgodność sprzętu

1

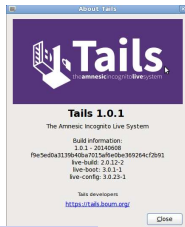
Tails automatycznie wykrywa typ procesora komputera i odpowiednio ładuje jądro 32- lub 64-bitowe.

2

Tails jest dostępny tylko na architekturach x86 i x86₆₄

3

Tails nie działa w architekturze ARM



Zgodność sprzętu

1

Tails automatycznie wykrywa typ procesora komputera i odpowiednio ładuje jądro 32- lub 64-bitowe.

2

Tails jest dostępny tylko na architekturach x86 i x86₆₄

3

Tails nie działa w architekturze ARM



Zgodność sprzętu

1

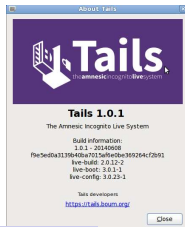
Tails automatycznie wykrywa typ procesora komputera i odpowiednio ładuje jądro 32- lub 64-bitowe.

2

Tails jest dostępny tylko na architekturach x86 i x86_64

3

Tails nie działa w architekturze ARM





INSTALACJA

1. Tails jako system na żywo powinien być instalowany z zewnętrznego dysku. Jest to zabieg celowy ułatwiający wykorzystanie docelowych funkcji Tails
2. Tails dostarcza aktualizacje co 6 tygodni
3. Nie zaleca się przeprowadzania samodzielnych aktualizacji, np. za pomocą `apt get` lub Synaptic



INSTALACJA

1. Tails jako system na żywo powinien być instalowany z zewnętrznego dysku. Jest to zabieg celowy ułatwiający wykorzystanie docelowych funkcji Tails
2. Tails dostarcza aktualizacje co 6 tygodni
3. Nie zaleca się przeprowadzania samodzielnych aktualizacji, np. za pomocą `apt get` lub Synaptic



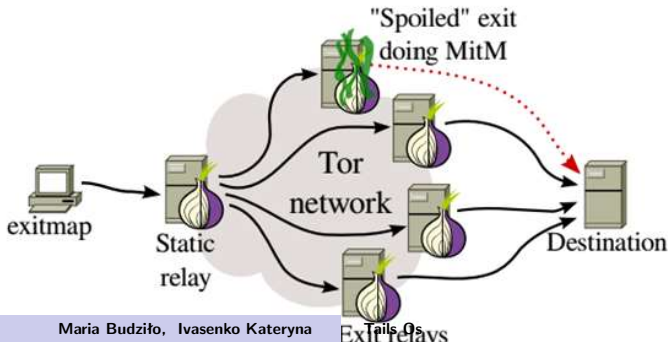
INSTALACJA

1. Tails jako system na żywo powinien być instalowany z zewnętrznego dysku. Jest to zabieg celowy ułatwiający wykorzystanie docelowych funkcji Tails
2. Tails dostarcza aktualizacje co 6 tygodni
3. Nie zaleca się przeprowadzania samodzielnych aktualizacji, np. za pomocą `apt get` lub Synaptic

NETWORKING

KORZYSTANIE Z VPN ZAMIAST TOR

Podstawowym założeniem Tails jest zmuszanie całego ruchu wychodzącego do korzystania z sieci anonimowych, takich jak Tor czy I2P. VPN nie są natomiast sieciami anonimowymi, co całkowicie daje Tor.



NETWORKING

cont

KORZYSTANIE Z VPN DO POŁĄCZENIA Z TOR (VPN PRZED TOR)

Obecnie nie jest możliwe łącznie się za pomocą VPN z Internetem, jednak odpowiednie mosty Tor, są przydatne do ominięcia ograniczeń związanych z wymuszeniem korzystania z VPN.





NETWORKING

cont

ŁĄCZENIE SIĘ Z VPN ZA POMOCĄ TOR (VPN PO TOR)

Niestety możliwość łączenia z VPN przez Tor w celu np. uzyskania dostępu do usług bądź zasobów dostępnych tylko w sieci VPN między innymi w firmach czy uczelnia, jest obecnie niełatwa przy użyciu Tails.

OPROGRAMOWANIE NIE ZAWARTE W TAILS

To oprogramowanie jest już dostępne w Debianie, ponieważ jest to wymóg dołączenia do Tails i ma ono wiele zalet.



INNE KWESTIE BEZPIECZEŃSTWA

Tails w zainfekowanym systemie

- Tails działa niezależnie od systemu operacyjnego zainstalowanego na komputerze. Co jest niesamowitą zaletą w przypadku, kiedy oryginalny system operacyjny zostanie zaatakowany przez na przykład wirusa, z Tails można nadal bezpiecznie korzystać, pomimo naruszenia głównego OS.





Tails Official Website

<https://tails.boum.org/>



Wikimedia Commons

https://commons.wikimedia.org/wiki/Main_page/

Dziękujemy za uwagę