

Unikanie rejestrowania czynności użytkownika: TOR, Linux Tails

podkom. Sylwester Panasewicz¹

¹ Laboratorium Kryminalistyczne Komendy Wojewódzkiej Policji w Białymstoku, sylwester.panasewicz@bk.policja.gov.pl

Streszczenie

Sieć TOR (The Onion Router) jest wirtualną siecią komputerową zapewniającą anonimizację oraz dostęp do często nielegalnych danych lub dla unikających cenzury. Linux Tails (The Amnesic Incognito Live System) stanowi natomiast system operacyjny bootowany wyłącznie z nośnika przenośnego (np.: pendrive, karty pamięci czy też płyty DVD) lub uruchamiany w sposób zwirtualizowany. Tails jako jedno z narzędzi oferuje dostęp do sieci TOR, zapewniając ponadto dalece wyszukane mechanizmy służące do unikania pozostawienia śladów cyfrowych na maszynie, z której korzysta użytkownik. Mimo innych intencji twórców obu omawianych powyżej narzędzi stały się one ulubionym pakietem olbrzymiej grupy przestępców na całym świecie. Autor w niniejszej publikacji skupia się na omówieniu zarówno obszarów powstawania śladów cyfrowych użytkownika TOR oraz Tails, jak i na możliwościach badawczych oraz możliwościach wnioskowania na ich podstawie. W pierwszej części artykułu opisany został mechanizm działania anonimizującej sieci TOR. Następnie autor zapoznaje czytelnika ze środowiskiem Linux Tails oraz odnosi się do faktycznych przypadków użycia.

Słowa kluczowe: anonimizacja, TOR, Tails, Linux, trasowanie, wirtualny

Jeszcze niedawno sen z oczu włamywacza spędzał problem, w jaki sposób pozostawić możliwie niewiele śladów na miejscu przestępstwa. Dziś, w dobie cyfrowej, sprawcy korzystają z różnorodnych narzędzi, by uzyskać nieuprawniony dostęp, fałszywą tożsamość lub dokonać innych działań, praktycznie nie pozostawiając śladów innych niż cyfrowe. Próbuje ukryć się w cieniu zwykłego ruchu sieciowego, maskując swoją działalność, szyfrując dane stanowiące dowody cyfrowe. Niekiedy mogą wręcz powrócić na miejsce przestępstwa i kontynuować zacieranie śladów lub weryfikować ich istnienie bez wiedzy organów ścigania. Choć idea sieci anonimizujących czy elastycznych systemów operacyjnych typu live nie powstała z myślą o świecie przestępczym, jej owoce coraz częściej stają się takimi narzędziami. Skłoniło to autora do opisanego w niniejszym artykule systemu operacyjnego Linux Tails, w charakterze narzędzia i zawartych w nim programów anonimizujących m.in. korzystających z sieci TOR, w kontekście kryminalistycznych badań informacyjnych. Trzeba pamiętać jednak, że tego typu narzędzia są używane również m.in. przez ludzi żyjących w systemach autorytarnych lub osoby chcące zachować swoją prywatność. Czytelnicy, którzy mieli okazję

zapoznać się z książką *Pamięć nieulotna* autorstwa Edwarda Snowdena, wiedzą, że podczas jego pracy dla NSA w kontakcie z prasą korzystał z systemu operacyjnego Tails. I co najważniejsze – nie został na tym przyłapany, co stanowi szczególną rekomendację.

Sieć TOR (The Onion Router) jest wirtualną siecią komputerową, w której zaimplementowano trasowanie cebulowe drugiej generacji, co zapobiega analizie ruchu sieciowego i zapewnia jej użytkownikom prawie anonimowy dostęp do zasobów Internetu.

Projekt TOR był początkowo sponsorowany przez laboratorium badawcze Marynarki Wojennej Stanów Zjednoczonych (U.S. Naval Research Laboratory) i rozwijany jako projekt militarny w celu ochrony komunikacji wywiadowczej USA w Internecie. Miał maskować działalność agentów wywiadu w sieci.

Inicjatorami sieci TOR byli programiści Roger Dingledine, Nick Mathewson oraz Paul Syverson, którzy przy wsparciu Centrum Badawczego Marynarki Wojennej USA rozpoczęli w 2002 r. pracę nad projektem. W 2004 roku na 13. Sympozjum Bezpieczeństwa Stowarzyszenia USENIX przedstawili pracę *Tor: The Second-Generation Onion Router*. W czasie od końca 2004 r. do listopada 2005 r. stał się on projektem

firmowanym przez Electronic Frontier Foundation (EFF). Obecnie rozwojem oprogramowania TOR zajmuje się Tor Project – niedochodowa organizacja non-profit o charakterze badawczo-edukacyjnym z siedzibą w Stanach Zjednoczonych, wspomagana przez wolontariuszy i użytkowników sieci na całym świecie. Projekt aktualnie funkcjonuje na licencji BSD, ale cały czas jest pośrednio sponsorowany przez Marynarkę Wojenną Stanów Zjednoczonych (Mider, 2019).

The Onion Router został udostępniony do użytku cywilnego w 2003 r. Serwery tworzące sieć TOR w początkowym okresie jej działania były umiejscowione jedynie w Stanach Zjednoczonych oraz Niemczech.

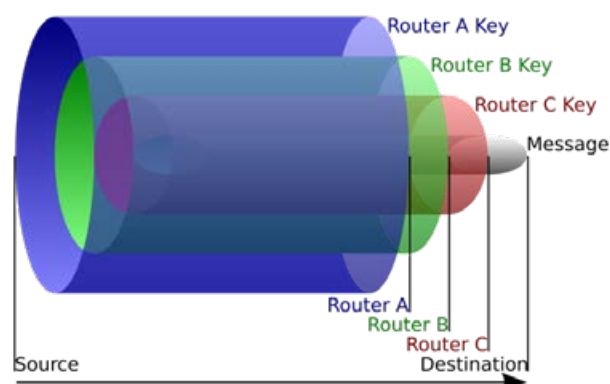
Nazwa sieci TOR jest skrótem od The Onion Router (router cebulowy). Pochodzi od techniki polegającej na wysłaniu niezależnych i wielowarstwowo szyfrowanych pakietów, stąd określenie „trasowanie cebulowe”. Tworzące tę sieć urządzenia realizują proces zwany trasowaniem cebulowym, odmiennym od klasycznego trasowania przez routery wykorzystujące model TCP/IP (Mider, 2019; Casad, 2017).

W sieci TOR dane są wysyłane zaszyfrowanymi warstwami, analogicznie do warstw cebuli. Zaszyfrowane w ten sposób dane są przesyłane przez serię węzłów sieciowych (routery cebulowe, ang. *onion routers*), z których każdy usuwa („odrywa”) pojedynczą warstwę, odsłaniając kolejny cel przesyłanych danych. Gdy ostatnia warstwa zostanie odszyfrowana, dane docierają do miejsca docelowego. Nadawca pozostaje anonimowy, ponieważ każdy węzeł zna tylko lokalizację bezpośrednio poprzedzających i następujących węzłów. Router w każdej warstwie „wie” tylko to, co jest mu niezbędne do działania. Adresy IP wszystkich zapytań i odpowiedzi zmieniają się w każdym węźle (Ortega, 2022).

Trasowanie cebulowe jest strukturą danych utworzoną przez enkapsulowanie („zawijanie”) danych w kolejne warstwy szyfrowania, które mogą być odszyfrowane przez tyle komputerów pośredniczących, ile jest warstw, zanim dotrą do miejsca docelowego. Połączenia pomiędzy każdym węzłem (serwerem proxy) jest szyfrowane. Pierwotne dane (i ich nadawca) pozostają ukryci, ponieważ dane są przesyłane pomiędzy węzłami pośrednimi, a żaden pośredni węzeł nie „zna” zarówno miejsca pochodzenia, jak i miejsca docelowego danych, dzięki czemu nadawca pozostaje anonimowy. Obserwacja takiego ruchu sieciowego nie pozwala stwierdzić, co jest w nim przesyłane.

Sieć TOR zapewnia anonimowość z wykorzystaniem protokołu TCP przy stosunkowo małym opóźnieniu i wysokiej przepustowości. Mechanizmy zaimplementowane w protokole sieci TOR nakładają warstwę anonimowości na warstwę TCP i tworzą ścieżkę

(domyślnie minimum) trzypunktową, przez którą routery sieci TOR szyfrują warstwowo. Informacja o trasach jest przesyłana przez grupę autorytatywnych serwerów. W uproszczeniu: cała komunikacja TCP użytkownika jest tunelowana w jednym węźle, rotującym w czasie, a w celu zapewnienia niskich opóźnień sieć TOR nie wymusza retransmisji zgubionych pakietów.



Ryc. 1. Mechanizm trasowania cebulowego: źródło wysyła dane do routera A, który usuwa warstwę szyfrowania, aby dowiedzieć się tylko, gdzie wysłać je dalej i skąd pochodzą (choć nie „wie”, czy nadawca jest źródłem, czy tylko innym węzłem). Router A wysyła je do routera B, który odszyfrowuje kolejną warstwę, aby poznać następne miejsce docelowe danych. Router B wysyła dane do routera C, który usuwa ostatnią warstwę szyfrowania i przesyła oryginalną wiadomość do miejsca przeznaczenia

Z perspektywy prywatności sieć TOR ma dwa cele:

1. Ukrywanie lokalizacji użytkowników korzystających z Internetu – wyśledzenie używanych przez nich adresów IP i lokalizacji ma być niemożliwe.
2. Szyfrowanie przesyłanych danych – sieć TOR szyfrując dane i przesyłając je routingiem cebulowym, ukrywa adresy IP użytkowników i przesyłane dane oraz ukrywa adresy IP operatorów ISP, poprzez których użytkownicy łączą się z siecią TOR (Ortega, 2022).

Węzły tworzące sieć TOR mają różne zadania i w zależności od charakterystyki i konfiguracji, różniemy:

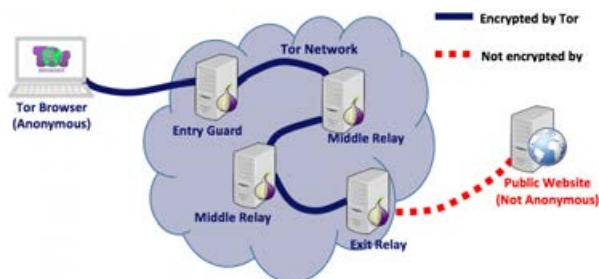
1. Węzły strażnicze (ang. *guard relays*) – komunikujące się z użytkownikami, połączone z resztą sieci TOR. Wykorzystywane od długiego czasu. Mają duże przepustowości.
2. Węzły przekaźnikowe (ang. *middle relays*) – komunikujące się wyłącznie z innymi węzłami. Dane, które z nich wychodzą, nie opuszczają sieci TOR.
3. Węzły wyjściowe (ang. *exit relays*) – punkty końcowe (brzegowe) sieci TOR. Odbierają żądania,

przesyłają je do odbiorców, odbierają odpowiedzi i wysyłają je w sieć w kierunku nadawcy.

4. Węzły pomostowe (ang. *bridge relays*) – będące węzłami, o których nie ma informacji w jawnym katalogu węzłów sieci TOR, które znacznie trudniej jest zablokować. Korzysta się z nich, gdy operator ISP blokuje sieć TOR. Lista ta jest dostępna na stronie <https://bridges.torproject.org> (Ortega, 2022).

Korzystanie z sieci TOR wygląda następująco:

1. Host łączący się z siecią TOR pobiera listę dostępnych węzłów i wybiera trzy z nich: strażniczy, przekąźnikowy i wyjściowy.
2. Dane przeznaczone do wysłania przez sieć TOR są najpierw szyfrowane. Tylko węzeł wyjściowy zna adres żądanej usługi sieciowej i ma wgląd w przesyłane pakiety danych, ale ich pochodzenie nie jest mu znane, co zapewnia prywatność użytkownikowi.
3. Zasyfrowane dane są ponownie szyfrowane i tylko węzeł przekąźnikowy wie, do którego węzła wyjściowego ma je przesłać. Dzięki podwójnemu szyfrowaniu tylko węzeł strażniczy wie, gdzie znajduje się węzeł przekąźnikowy (Ortega, 2022).



Ryc. 2. Diagram pokazujący typowy scenariusz działania klienta sieci TOR uzyskującego dostęp do publicznej strony w sieci Internet

Dane są szyfrowane, zanim opuszczą komputer użytkownika:

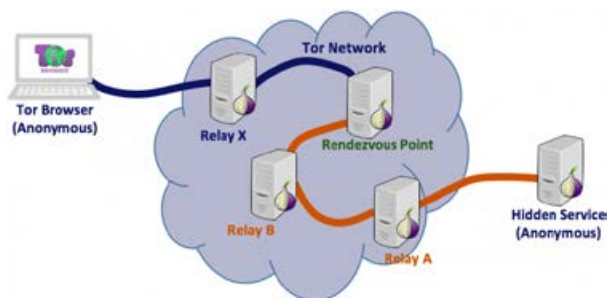
1. Jeśli istnieje system monitorujący połączenie internetowe (może to zrobić ISP), widzi on tylko zasyfrowane dane wymieniane z węzłem strażniczym.
2. Tylko węzeł strażniczy widzi IP użytkownika i wie, gdzie znajduje się węzeł przekąźnikowy.
3. Tylko węzeł przekąźnikowy wie, gdzie są węzły strażniczy i wyjściowy. Nie wie jednak, gdzie jest użytkownik ani żądana strona internetowa (lub inna usługa sieciowa). Węzły przekąźnikowe nie znają swoich miejsc w sieci.
4. Węzeł wyjściowy wie, gdzie jest żądana strona internetowa (lub inna usługa sieciowa) i węzeł przekąźnikowy. Ale nie wie, gdzie jest użytkownik i węzeł strażniczy (Ortega, 2022).



Ryc. 3. Diagram pokazujący jak wiadomość będzie podróżować poprzez sieć TOR dopóki nie dotrze do publicznej witryny internetowej. Klient sieci TOR (przeglądarka Tor Browser) dodaje tyle warstw, ile jest przekąźników w łańcuchu

Niektóre sieci blokują ruch wychodzący na porcie TCP 9050 używanym przez sieć TOR, a nawet dynamicznie wciągają na czarną listę wszystkie węzły sieci TOR, uniemożliwiając korzystanie z tej sieci. Ograniczenie to można ominąć, używając tzw. mostków sieciowych, czyli węzłów sieci TOR niewidocznych w publicznym katalogu sieci (Allsopp, 2017).

Oprócz łączenia się z usługami w Internecie sieć TOR umożliwia korzystanie z tzw. ukrytych usług (*hidden services*), świadczonych na całkowicie anonimowych serwerach sieciowych zamkniętych w ekosystemie sieci TOR i widocznych tylko w niej, które korzystają z własnego rozproszonego systemu adresowania (Allsopp, 2017).



Ryc. 4. Diagram przedstawiający mechanizm uzyskiwania dostępu do serwera WWW ukrytego w sieci TOR (ukrytej usługi): (1) jeden serwer Tor Relay (przekąźnik) zostanie wybrany jako (przekąźnik) Rendezvous Point; (2) tworzone są dwa połączenia: jeden od klienta sieci Tor do węzła Rendezvous Point, a drugi od ukrytego serwera w sieci Tor do węzła Rendezvous Point. Autor uważam, że czytelnikowi pozostawia pod rozwagę, czy Hidden Service na powyższym diagramie nie powinien być objęty obszarem obrazowej chmury Tor Network

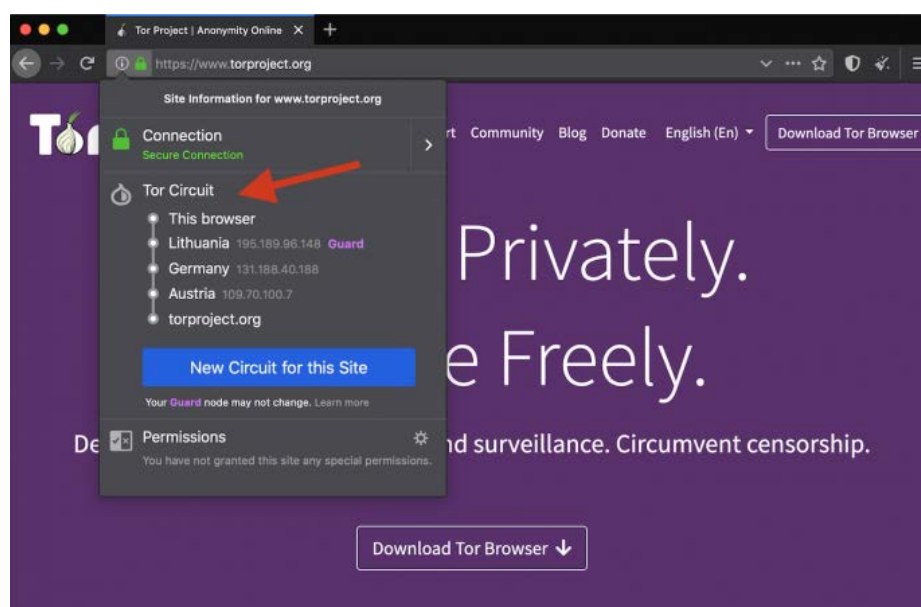
W przeciwieństwie do zwykłych stron internetowych, do których uzyskuje się dostęp za pomocą ich adresów URL, dostęp do ukrytych usług uzyskuje się za pomocą specjalnego typu adresów *onion*, zawierających losowy, niemnemoniczny ciąg znaków i niebędących

częścią typowego systemu DNS w Internecie. Losowe znaki w adresie witryny w sieci TOR (np.: https://zqkltwi-4fecvo6ri.onion/wiki/index.php/Main_Page) dodatkowo utrudniają znalezienie odpowiedniej witryny – dostęp mają osoby, które wiedzą, jak ich szukać.

Najpopularniejszym programem do przeglądania sieci TOR jest Tor Browser Bundle, który jest zintegrowany z przeglądarką internetową Mozilla Firefox. Program zapewnia ochronę użytkownikowi, jeśli korzysta on wyłącznie z wbudowanej przeglądarki Firefox. Po połączeniu z siecią TOR można swobodnie przeglądać strony internetowe, a także prowadzić rozmowy za pomocą komunikatorów. Program ma ogromną ilość różnych opcji konfiguracyjnych, za pomocą których możemy ustawić połączenie z siecią TOR i ustanowić nowe połączenie TCP, wpisując inny adres IP. Przeglądarka Tor Browser zapewnia bezpieczeństwo na trzech poziomach, a każdy z nich możemy w każdym momencie samodzielnie ustawić. Poziomy te to: *standardowy* (wszystkie funkcje przeglądarki TOR i stron są włączone); *bezpieczniejszy* (obsługa skryptów JavaScript na stronach bez HTTPS jest wyłączona, podobnie niektóre czcionki i symbole, media HTML5 (audio i video) uruchamiają się dopiero po naszym kliknięciu) oraz *najbezpieczniejszy* (ustawienie HTML5 jak wyżej, a także domyślnie wyłączony JavaScript na wszystkich stronach, tak samo niektóre czcionki, symbole i obrazki).

Jak można się dowiedzieć z powyższej analizy działania sieci wirtualnej Tor, do jej obsługi niezbędne jest specjalistyczne oprogramowanie. Bezpieczeństwo użytkownika wzrasta, gdy działa ono w środowisku minimalizującym powstawanie artefaktów cyfrowych. Najlepszym takim środowiskiem jest system operacyjny, który działa, opierając się wyłącznie na pamięci operacyjnej komputera lub systemie wirtualnym. Opisany w dalszej części artykułu system Tails nie jest jedyną dystrybucją Linux przeznaczoną do podobnych celów. Wśród popularnych można wymienić także: Qubes OS, minimalistyczny Alpine Linux, IprediaOS, Whonix oraz Kodachi Linux, jednakże autor skupił się na omawianej dystrybucji z uwagi na jej popularność w przekazywanym do badań materiale dowodowym.

The Amnesic Incognito Live System, czyli w skrócie TAILS, to oparta na Debianie i środowisku graficznym Gnome dystrybucja Linux przeznaczona wyłącznie do użytkowania w formie Live USB, Live DVD lub dla środowiska wirtualnego. Pierwsza wersja tego systemu operacyjnego została stworzona w 2009 przez deweloperów „The Tails project” z myślą o bezpieczeństwie, zachowaniu prywatności i anonimowości użytkownika. Do wersji 5.2 z 12 lipca 2022 roku, której funkcjonalności w tej części artykułu zostaną omówione (autor skupia się w swoim opracowaniu na funkcjonalnościach szczególnie istotnych dla cyfrowej analizy śledczej, w związku



BLOCK TRACKERS

Tor Browser isolates each website you visit so third-party trackers and ads can't follow you. Any cookies

Ryc. 5. Okno przeglądarki Tor Browser z widocznymi adresami węzłów sieci TOR oraz opcjami zmiany obwodu

z tym nie zawiera ono pełnego opisu systemu Linux Tails 5.2), projekt przeszedł imponującą ewolucję, która znacząco wpływała również na *modus operandi* użytkowników go przestępców. Szczególnie istotna, z punktu widzenia informatyka śledczego, wydaje się ewolucja polityki twórców systemu dotyczącej metod dostępu do obszaru udostępnionego dla zapisu danych.

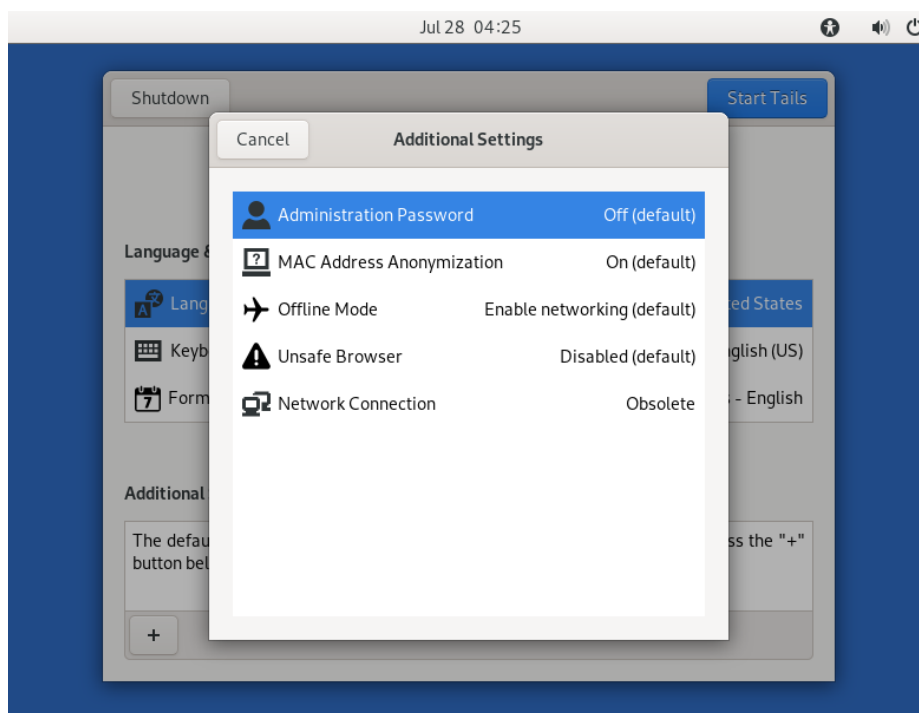
Aktualnie według dystrybutora TAILS jest systemem skierowanym do użytkowników takich jak: aktywiści, dziennikarze oraz ich źródła, osoby doświadczające nadmiernej kontroli w swoim środowisku oraz wszelkie osoby potrzebujące prywatności w świecie cyfrowym. Jest to oprogramowanie darmowe na licencji GNU/GPL, zatem źródłem finansowania wspomnianej grupy deweloperów są m.in. sponsorzy, wśród których szczególnie znamienna jest obecność organizacji takich jak: U.S. Department of State (powyżej 100 000 dolarów); ProtonMail, RIPE NCC (po 50 000–99 999 dolarów) czy też TOR.

Omawiany system operacyjny do działania potrzebuje 64-bitowego procesora oraz co najmniej 2 GB pamięci operacyjnej a producent deklaruje kompatybilność z większością komputerów osobistych produkowanych po 2006 roku. Jak wspomniano wcześniej, uruchamiany jest na komputerze przy użyciu nośnika USB lub płyty DVD z pominięciem użycia rodzimego systemu operacyjnego, gwarantując jednocześnie dostęp do zamontowanych nośników pamięci w trybie jedynie „do odczytu”. Już na tym etapie działania

użytkownika nie powstają na komputerze artefakty wskazujące na użycie TAILS, ponieważ jedynym niestandardowym poleceniem podczas rozruchu jest skorzystanie z interfejsu wyboru nośnika bootowania i, jak potwierdza praktyka autora artykułu, na większości testowanych oraz przedstawionych do badań w toku realizacji postanowień o powołaniu dowodu z opinii biegłego urzędzeń operacja ta nie wymaga trwałej modyfikacji ustawień systemu BIOS.

Po wybraniu standardowego trybu uruchomienia użytkownik ma możliwość prekonfiguracji parametrów, m.in. wpływających istotnie na bezpieczeństwo.

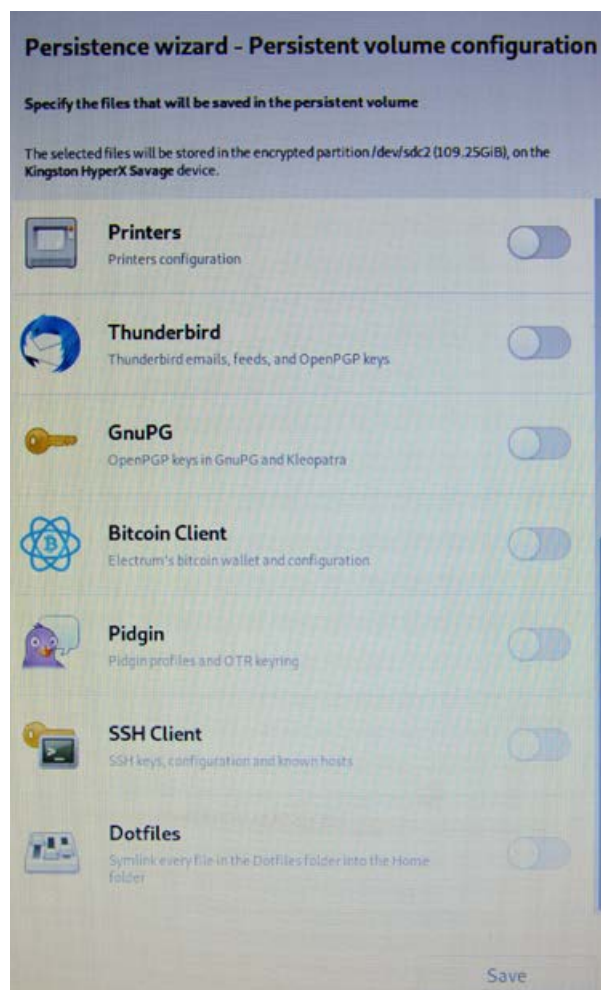
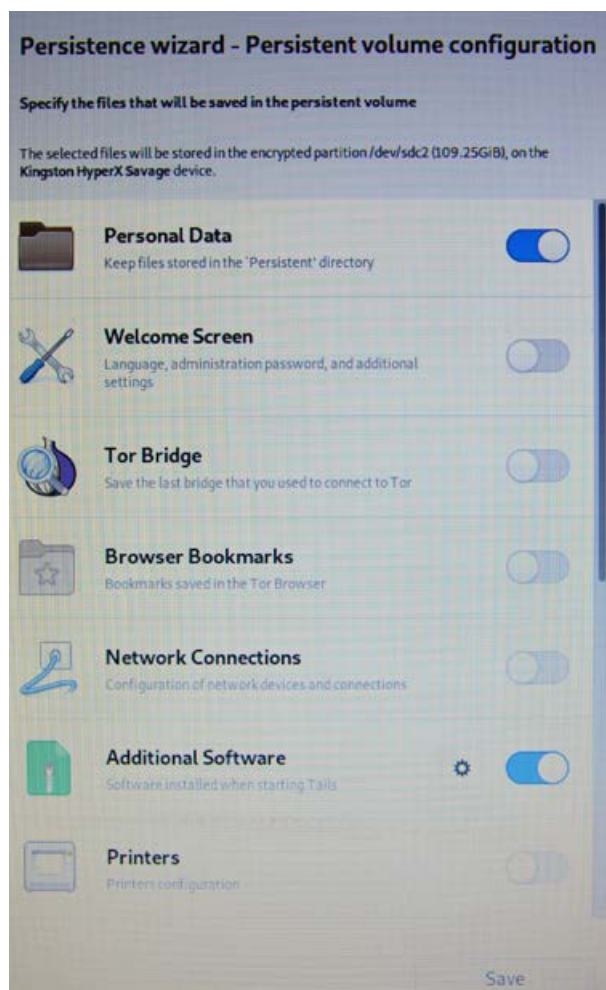
Do ustawień tych należy możliwość określenia hasła administracyjnego. Pominięcie tego kroku znacząco ogranicza pewne funkcjonalności, dając jednocześnie mniej zaawansowanemu użytkownikowi większą gwarancję uniknięcia powstania artefaktów o charakterze dowodu cyfrowego. Kolejnymi opcjami prekonfiguracyjnymi, o których warto wspomnieć, są: możliwość automatycznego anonimizowania adresu fizycznego MAC interfejsów sieciowych, wymuszony tryb offline, udostępnienie funkcji tzw. Unsafe Browser, czyli przeglądarki internetowej z możliwością użytkowania sieci Internet z pominięciem TOR, której działanie ze względów bezpieczeństwa domyślnie jest zablokowane. Poprzednie wersje rozwojowe Linux Tails na poziomie prekonfiguracji oferowały m.in. nawet kamuflaż w postaci graficznego interfejsu przypominającego pulpit MS Windows.



Ryc. 6. Widok okien wyboru panelu prekonfiguracyjnego sesji Linux Tails wykonany w formie zrzutu ekranu sesji na maszynie wirtualnej

System operacyjny Linux Tails uruchomiony z użyciem parametrów opisanych powyżej, jak wspomniano wcześniej, umożliwia dostęp do zamontowanych nośników pamięci w trybie „tylko do odczytu”. Prawidłowe działanie softwarowej blokady zapisu systemu TAILS potwierdziły liczne testy autora polegające na montowaniu różnych nośników, zarówno pamięci przenośnej, jak i dysków zainstalowanych w badanych jednostkach, przeglądaniu ich zawartości, prób zapisu na tych nośnikach z wykorzystaniem oprogramowania z interfejsem graficznym dystrybuowanego z kompilacją live USB LinuX Tails 5.2 oraz pracy bieżącej tego systemu, a następnie weryfikowaniu ich wartości funkcji skrótu SHA-1 oraz MD5. Należy zauważyć, że dla systemów plików innych niż oparte na GNU/Linux wbudowana przeglądarka plików automatycznie ignoruje ograniczenia uprawnień dostępu do przeglądania zawartości nośników danych. W przypadku braku szyfrowania możliwe jest zatem uzyskanie dostępu do wszelkich plików użytkownika komputera osobistego, odczytanie ich zawartości lub wykonanie kopii, nawet

jeśli natywny system operacyjny jest zabezpieczony przed nieuprawnionym dostępem (Prostym sposobem ochrony przed nieuprawnionym uruchomieniem systemu TAILS na komputerze jest zabezpieczenie panelu wyboru źródła bootowania hasłem z poziomu BIOS). Ponadto nie obserwuje się powstania artefaktów o charakterze dowodu cyfrowego związanych z tym faktem na użytkowanym komputerze. Operacje wykonywane są co prawda z użyciem pamięci RAM, jednakże architektura systemu TAILS ma wbudowany mechanizm, który po zakończeniu procesu natychmiast nadpisuje przydzielony mu obszar, system blokuje również standardowe metody wykonania zrzutu pamięci RAM. Wykonanie takiego zrzutu możliwe jest np. za pomocą oprogramowania AVML, jednakże z uwagi na ograniczenie możliwości zapisu wyniku wyłącznie w obszarze Persistent Storage (patrz dalsza część artykułu) lub za pomocą interfejsu sieciowego stanowi, obok samej analizy treści zrzutu, ciekawy i ważny do rozwiązania w toku dalszych analiz własnych autora problem badawczy. Ponadto w przypadku prawidłowego zakończenia pracy



Ryc. 7. Zdjęcia okna konfiguracyjnego Persistent Storage

z systemem TAILS następuje nadpisanie całości pamięci ulotnej, co czyni go niewrażliwym na zastosowanie śledcze metod *cold boot attack*.

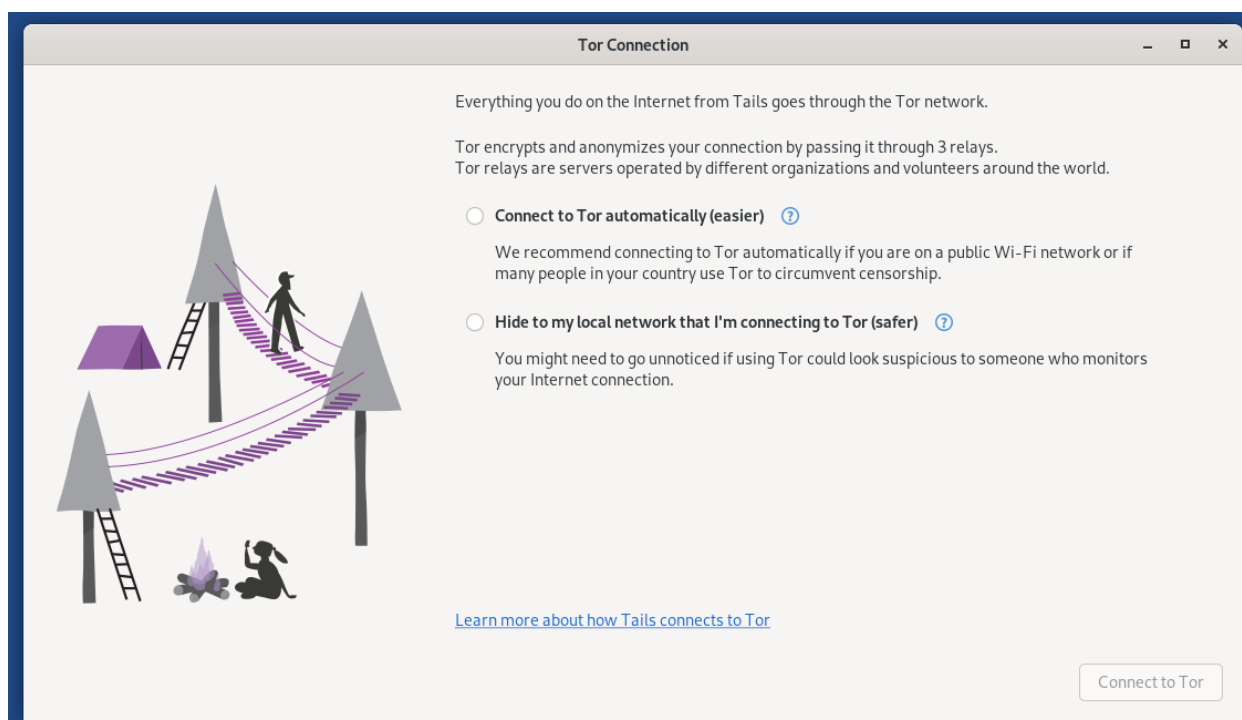
We wcześniejszych wersjach rozwojowych Linux Tails średnio zaawansowany użytkownik mógł zamontować nośniki pamięci w trybie *read-write*, a więc do opisanych powyżej możliwości dodać można było zdolność do ingerencji w dane. W opisywanej wersji 5.2 z poziomu standardowych ustawień systemu oraz załączonych aplikacji brak jest takiej funkcjonalności, co mimo podniesienia poziomu poufności użytkownika powoduje istotne utrudnienie tzn. brak magazynu na dane wytworzone w trakcie pracy. Deweloperzy m.in. w tym celu zaimplementowali funkcjonalność o nazwie: Persistent Storage – zaszyfowaną pamięć trwałą. Funkcja ta dostępna jest do skonfigurowania z poziomu uruchomionego z nośnika USB Linux Tails. Za jej pomocą użytkownik w obszarze wolnej pamięci nośnika (Persistent Storage można jedynie zainstalować na nośniku z systemem Linux Tails) zakłada partycję szyfrowaną standardem Linux LUKS. Podczas kolejnego uruchomienia systemu Live partycja zostaje rozpoznana i po podaniu hasła w trybie *read-write* udostępniona zostaje szyfrowana przestrzeń, gdzie oprócz plików użytkownika mogą być m.in. zainstalowane aplikacje lub przechowywane ustawienia konfiguracyjne TAILS.

Znamiennym jest, że omawiany system operacyjny nie wymusza utworzenia hasła o wysokim stopniu skomplikowania (dopuszcza nawet jeden dowolny znak jako hasło dostępu), co czyni utworzoną partycję

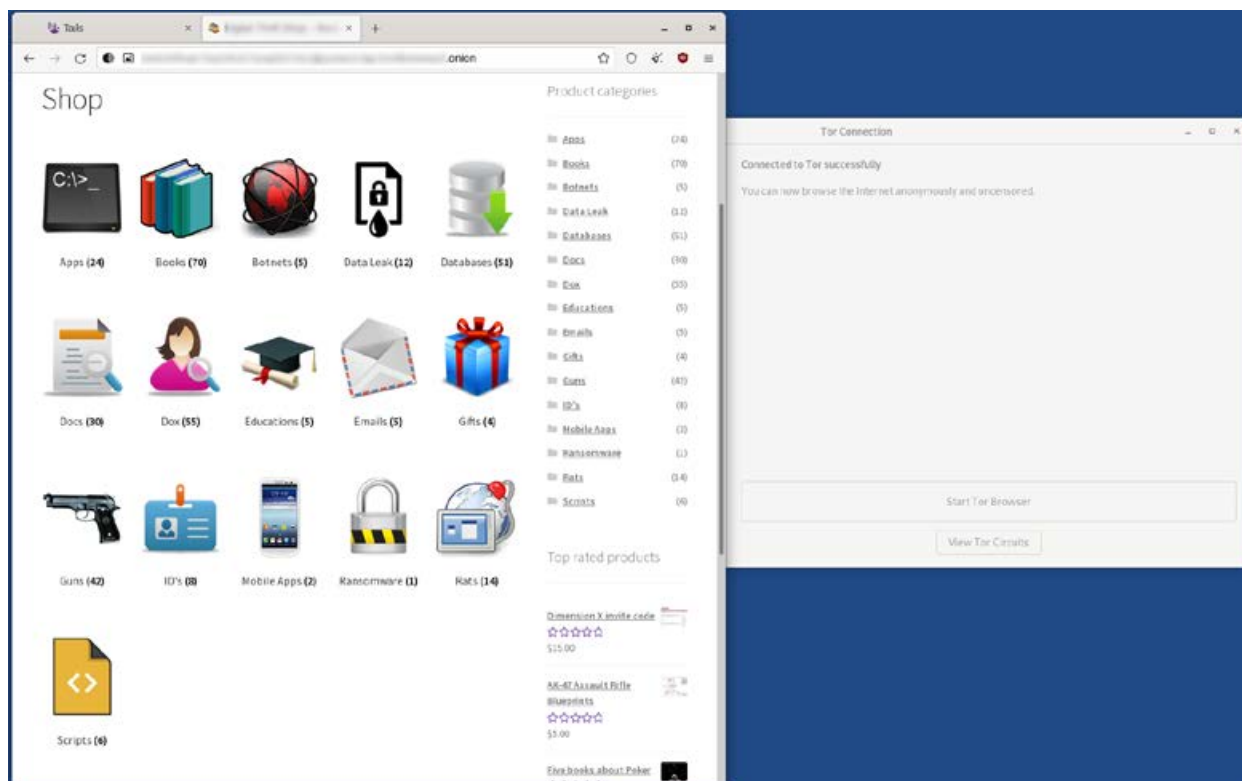
podatną na ataki słownikowe czy też *brute force* z wykorzystaniem m.in. oprogramowania takiego jak Password Kit Forensics. Ponadto standard szyfrowania LUKS pozwala na odczyt zaszyfowanej partycji z użyciem znanego hasła dostępu na dowolnym komputerze wyposażonym w stosowne oprogramowanie. Czynność ta może łatwo doprowadzić do powstania w systemie operacyjnym użytego komputera artefaktów zawierających np.: miniatury lub kopie zawartości multimedialnych, indeksy plików oraz ich metadane mające znaczenie śladów cyfrowych.

Kolejną warstwą użyteczności systemu Linux Tails jest interfejs sieciowy. Jak opisano wcześniej, przeglądarka Unsafe Browser dostępna jest jedynie na wyraźne żądanie użytkownika. W innym przypadku całość komunikacji z siecią Internet lub ukrytymi usługami w sieci TOR realizowana jest za pośrednictwem sieci TOR. Ponadto system oferuje zastosowanie tzw. Tor bridge, czyli specjalistycznych przekaźników ukrywających ruch, jak opisano we wcześniejszej części niniejszego artykułu. Metoda ta umożliwia również uzyskanie dostępu do sieci TOR za pomocą punktów dostępowych, gdzie takie połączenie z Internetem jest zablokowane, lub ukrycie takiej działalności.

Przy dodatkowym założeniu stosowania VPN, braku powstawania na komputerze artefaktów innych niż ulotne, które związane są z użytkowaniem sieci, szyfrowaniu pakietów danych oraz ich metadanych, braku bezpośredniego dostępu śledczych do użytkownika komputera z otwartą sesją TAILS, analiza ruchu



Ryc. 8. Widok okna konfiguracji połączenia z TOR wykonany w formie zrzutu ekranu sesji na maszynie wirtualnej



Ryc. 9. Widok okna przeglądarki z uruchomioną poglądowo witryną dostępną jedynie z poziomu TOR wykonany w formie zrzutu ekranu sesji na maszynie wirtualnej

sieciowego oraz jego śledzenie stają się wyjątkowo trudne i pracochłonne, a wręcz niemożliwe. Należy jednak pamiętać, że istnieją narzędzia bazujące na analizie anomalii w ruchu sieciowym pozwalające na typowanie użytkowników stosujących opisane techniki.

Opisywana wersja 5.2 ma również wbudowanego klienta poczty Thunderbird z funkcją obsługi szyfrowanych wiadomości e-mail, aplikację KeePassXC wspomagającą tworzenie i przechowywanie haseł dostępowych, pakiet biurowy LibreOffice, bardzo ciekawą aplikację OnionShare wspierającą przesyłanie plików za pomocą sieci TOR, pakiet narzędzi do obróbki grafiki i dźwięku oraz inne programy użytkowe, w tym diagnostyczne.

Na uwagę zasługuje również fakt potwierdzającej się w wyniku testów oraz analiz materiałów przekazywanych do badań zadowolającej stabilności pracy systemu. Jednocześnie w przypadku nagłego usunięcia z portu USB nośnika zawierającego uruchomioną sesję Linux Tails 5.2 następuje natychmiastowe wyłączenie interfejsu graficznego i po krótkim wylistowaniu błędów oraz kilku procesów systemowych komputer zostaje wyłączony. Znaczenie opisanego powyżej mechanizmu dla organów ścigania autor pozwala sobie pozostawić ocenie czytelnika. Ponadto TAILS stabilnie pracuje w środowisku wirtualnym np. VMware Workstation, gdzie jedynym ograniczeniem funkcjonalności jest brak obsługi Persistent Storage (według dystrybutora

pełna funkcjonalność na maszynie jest dostępna w aplikacji *virt-manager* działającej w środowisku Linux).

W praktyce biegłego z zakresu badań informatycznych spotkać można pomysłowe połączenia wyrafinowanych narzędzi utrudniających przeprowadzenie analizy danych, takich jak Linux Tails, oraz różnorodnych fizycznych modyfikacji sprzętu mających za zadanie dodatkowo zabezpieczyć dane przed czynnościami organów ścigania. Materiałem dostarczonym do badań w jednej z takich spraw był komputer przenośny, w którym wycięto część obudowy, tak by ułatwić szybki demontaż dysku twardego, natomiast w czytniku nośników optycznych ujawniona została jedna z dystrybucji TAILS nagrana na płycie DVD, co przedstawiono poglądowo na poniższych zdjęciach:



Ryc. 10. Widok czytnika wraz z nośnikiem Linux Tails



Ryc. 11. Widok modyfikacji w obudowie komputera przedstawionego na zdjęciu powyżej

W kolejnym, bardziej wymagającym analitycznie przypadku autor mimo szczegółowych badań m.in. za pomocą oprogramowania X-Ways Forensics, Magnet AXIOM czy też wirtualizacji systemu operacyjnego zainstalowanego na przekazanej do badań jednostce komputerowej nie ujawnił zgodnie z pytaniem prowadzącego: dokumentacji, wpisów historii przeglądania stron internetowych czy też treści korespondencji dotyczącej wprowadzania do obrotu pewnych nielegalnych substancji. Mimo że historia ujawniona w pamięci przeglądarek internetowych oraz treści plików nie wskazywała nawet na zainteresowanie użytkownika przedmiotowymi zagadnieniami, stała się ona kluczowa dla wskazania dalszego toku postępowania w tej sprawie. Szczegółowa analiza historii wyszukiwania fraz w sieci Internet wskazała bowiem na nagle i objawiające się w krótkim czasie zainteresowanie użytkownika narzędziami do anonimizacji oraz dostępu do sieci TOR. Stwierdzono również obecność śladów cyfrowych wskazujących na pobranie z sieci Internet jednej z dystrybucji Linux Tails. W toku wcześniejszej analizy na partycji odpowiedzialnej za bootowanie systemu MS Windows (na takiej partycji dostęp do zapisu z poziomu użytkownika systemu MS Windows jest zablokowany) ujawniono również obecność nietypowego pliku tekstowego. Korelacja znaczników czasowych opisanych powyżej zbiorów artefaktów wskazała na kolejność działań opisaną poniżej. Użytkownik w pierwszym kroku wyszukał, a następnie pobrał i zainstalował Linux Tails na nośniku wymiennym. W celu ukrycia wrażliwych dla siebie danych zapisał je w pliku tekstowym umieszczonym, jak wspomniano powyżej, na niewidocznej z poziomu użytkownika MS Windows partycji dysku systemowego (operacja zapisu nie byłaby możliwa dla średniozaawansowanego użytkownika, gdyby użyto nowszych dystrybucji TAILS, takich jak wersja 5.2. Fakt ten może tłumaczyć, dlaczego w przypadkach rozpatrywanych w ramach aktualnych zleceń w materiale dowodowym znajdują się starsze wersje rozwojowe systemu). W istocie

przedmiotowy plik zawierał adres witryny sieci TOR, który z uwagi na składnię charakteryzującą się wysoką entropią znaków, jak wspomniano wcześniej (np.: https://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page), jest trudny do zapamiętania. Wspomniany adres prowadził do spersonalizowanej strony użytkownika na witrynie specjalizującej się w obrocie nielegalnymi substancjami. W tym substancjami, których dotyczyło zlecenie badań. Polityka transparentności wspomnianej witryny pozwalała na pisanie publicznych informacji zwrotnych poszczególnym użytkownikom. Ustalono zatem, że na podstawie skarg odbiorców (związanych z zerwaniem kontaktu i niewywiązaniem się dostarczenia zakupionego towaru) przedmiotowa spersonalizowana strona została zablokowana zaraz po dacie czynności związanych z zabezpieczeniem sprzętu przekazanego do badań. Ponadto autor pragnie zwrócić uwagę, że o ile obecność ujawnionego adresu w obszarze dostępnym użytkownikowi MS Windows można spróbować wytłumaczyć nawet procesami geologii cyfrowej, np. związanymi z *cache* przeglądarek internetowych, to pojawienie się pliku w opisanym obszarze nośnika pamięci wskazuje na zachowanie intencjonalne i to z użyciem niespecyficznym, profesjonalnych narzędzi.

Podsumowując powyższą analizę, autor pragnie zwrócić uwagę, że narzędzie Linux Tails w wersji 5.2 stanowi system minimalizujący powstawanie geologicznych dowodów cyfrowych (Altheide, 2014, s. 18), a więc takich, które związane są z autonomiczną pracą systemu komputerowego i powstającą automatycznie oraz nieintencjonalnie. Jednocześnie ilość artefaktów o charakterze archeologii cyfrowej (Altheide, 2014, s. 18), a więc powstających intencjonalnie w wyniku działań użytkownika zbiorów danych, zależy w tym przypadku od jego samoświadomości oraz charakteru i poziomu skomplikowania wykonywanych operacji. W odniesieniu do zastosowań przestępczych kluczowym problemem użytkownika jest żmudność wykonywania niekiedy zwyczajowo prostych operacji, a zatem pokusa do rezygnowania z pewnych zasad bezpieczeństwa. Zachowania takie stanowią pole do wykorzystania najcenniejszych umiejętności informatyka śledczego, jakimi obok wiedzy specjalnej są umiejętności analitycznego myślenia i korelacji faktów, bez których nawet coraz bardziej zaawansowane oprogramowanie *forensics* wciąż będzie bezużyteczne.

Szczególne podziękowania za wymianę myśli naukowej składam Panom: Rafałowi Czechowi, Marcinowi Napiórkowskiemu oraz Krzysztofowi Turowskiemu.

Autor

Bibliografia:

1. Allsopp, W. (2017). *Testy penetracyjne dla zaawansowanych. Hakowanie najlepiej zabezpieczonych sieci na świecie*. Wydawnictwo Helion.
2. Altheide, C., Carvey, H. (2014). *Informatyka śledcza. Przewodnik po narzędziach open source*. Wydawnictwo Helion.
3. Casad, J. (2017). *TCP/IP w 24 godziny. Wydanie VI*. Wydawnictwo Helion.
4. Ciborski, T. (2015). *Ukryta tożsamość. Jak się obronić przed utratą prywatności*. Wydawnictwo Helion.
5. Flow, S. (2022). *Hakuj jak duch. Łamanie zabezpieczeń środowisk chmurowych*. Wydawnictwo Helion.
6. Hayes, D.R. (2021). *Informatyka w kryminalistyce. Praktyczny przewodnik*. Wydanie II. Gliwice. Wydawnictwo Helion.
7. Krawetz N. (2008). *Hacking Ubuntu. Konfiguracja i optymalizacja*. Gliwice. Wydawnictwo Helion.
8. Mider D. (2019). *Czarny i czerwony rynek w sieci The Onion Router – analiza funkcjonowania darkmarketów*, „Przegląd Bezpieczeństwa Wewnętrznego” 21/19.
9. Muniz J, Lakhani A. (2014). *Kali Linux. Testy penetracyjne*. Gliwice. Wydawnictwo Helion.
10. Ortega J. M. (2022). *Bezpieczeństwo sieci w Pythonie. Rozwiązywanie problemów za pomocą skryptów i bibliotek*. Wydanie II. Gliwice. Wydawnictwo Helion.
11. Petreley N., Bacon J. (2005). *100 sposobów na Linux*. Gliwice. Wydawnictwo Helion.
12. Sokół R. (2014). *Jak pozostać anonimowym w sieci*. Gliwice. Wydawnictwo Helion.
3. Hosting Anonymous Website on Tor Network, Abed Samhuri, <https://medium.com/axon-technologies/hosting-anonymous-website-on-tor-network-3a82394d7a01> (dostęp: 28.07.2022).
4. Jak zainstalować i poprawnie skonfigurować przeglądarkę Tor 8.0, Ewelina Stój, PurePC, <https://www.purepc.pl/jak-zainstalowac-i-poprawnie-skonfigurowac-przegladarke-tor-8-0> (dostęp: 27.07.2022).
5. Narzędzia anonimizujące działania w Internecie jako instrumentarium do prowadzenia operacji informacyjnych w ramach wojny hybrydowej, Przegląd Bezpieczeństwa Wewnętrznego Wydanie Specjalne, Kamil Kucharski, <https://www.abw.gov.pl/download/1/1923/kucharski.pdf> (dostęp: 28.07.2022).
6. Sieć TOR – wszystko, co trzeba o niej wiedzieć, Bitdefender, <https://bitdefender.pl/siec-tor-wszystko-co-trzeba-o-niej-wiedziec/> (dostęp: 28.07.2022).
7. Signing in to a network using a captive portal, https://tails.boum.org/doc/anonymous_internet/tor/index.en.html#hiding (dostęp: 26.07.2022).
8. Tor Browser Bundle, dobreprogramy, <https://www.dobreprogramy.pl/tor-browser-bundle,program,windows,6628600948791425> (dostęp: 28.07.2022).
9. Tor Browser 9.0 już dostępny do pobrania, Sekurak, <https://sekurak.pl/tor-browser-9-0-juz-dostepny-do-pobrania/> (dostęp: 28.07.2022).
10. Tor (sieć anonimowa), Wikipedia, [https://pl.wikipedia.org/wiki/Tor_\(sie%C4%87_anonimowa\)](https://pl.wikipedia.org/wiki/Tor_(sie%C4%87_anonimowa)) (dostęp: 28.07.2022).
11. Tails – Accessing the internal hard disk, https://tails.boum.org/doc/advanced_topics/internal_hard_disk/index.en.html (dostęp: 26.07.2022).
12. Tails – Memory erasure, https://tails.boum.org/contribute/design/memory_erasure/ (dostęp: 26.07.2022).
13. Tails – Sponsors, <https://tails.boum.org/sponsors/index.en.html> (dostęp: 26.07.2022).
14. Trasowanie cebulowe, Wikipedia, https://pl.wikipedia.org/wiki/Trasowanie_cebulowe (dostęp: 28.07.2022).
15. Zarys historyczny sieci Darknet oraz aspekty legalnego i nielegalnego wykorzystania technologii Tor, Przegląd Nauk Stosowanych nr 19, Politechnika Opolska Wydział Ekonomii i Zarządzania, Rafał Kokot, Tomasz Turba, https://pns.po.opole.pl/images/PNS_19/PNS19-IX.pdf (dostęp: 28.07.2022).
16. Z systemem Tails nikt nie będzie śledził cię w internecie, <https://www.benchmark.pl/aktualnosci/system-tails-gwarantuje-prawdziwa-anonimowosc-w-sieci.html> (dostęp: 29.07.2022).

Źródła rycin:

Ryc. 1: Trasowanie cebulowe, Wikipedia, https://pl.wikipedia.org/wiki/Trasowanie_cebulowe.

Ryc. 2, 3, 4: Hosting Anonymous Website on Tor Network, Abed Samhuri, <https://medium.com/axon-technologies/hosting-anonymous-website-on-tor-network-3a82394d7a01>.

Ryc. 5: Tor Browser 9.0 już dostępny do pobrania, Sekurak, <https://sekurak.pl/tor-browser-9-0-juz-dostepny-do-pobrania/>.

Ryc. nr 6, 7, 8, 9, 10, 11: opracowanie własne autora.

Internet:

1. BridgeDB, Tor Project, <https://bridges.torproject.org/bridges?transport=obfs4> (dostęp: 28.07.2022).
2. GitHub – microsoft/avml: AVML – Acquire Volatile Memory for Linux, <https://github.com/microsoft/avml> (dostęp: 26.07.2022).

Avoiding recording user activities: TOR, Linux Tails

second lieutenant Sylwester Panasewicz¹

¹ Forensic Laboratory of the Provincial Police Headquarters in Białystok, sylwester.panasewicz@bk.policja.gov.pl

Abstract

The Tor (The Onion Router) network is a virtual computer network that provides anonymisation and access to often illegal data or for those avoiding censorship. Linux Tails (The Amnesic Incognito Live System), on the other hand, is an operating system bootable only from a removable media (e.g.: flash drive, memory card or DVD) or run in a virtualized manner. Tails, as one of the tools, offers access to the Tor network providing, in addition, far sophisticated mechanisms to avoid leaving digital traces on the user's machine. Despite the different intentions of the developers of the two tools discussed above, they have also become the favorite package of a huge group of criminals around the world. In this publication, the author focuses on discussing both the areas of formation of digital traces of Tor and Tails usage, as well as the research possibilities and inference possibilities based on them. The first part of the article describes the mechanism of the Tor anonymizing network. The author then introduces the reader to the Linux Tails environment and refers to actual use cases.

Keywords: anonymisation, Tor, Tails, Linux, routing, virtual

Until recently, the burglar's sleep was spent on the problem of how to leave as few traces as possible at the scene of the crime. Today, in the digital age, perpetrators use a variety of tools to gain unauthorized access, fake identities or perform other actions, leaving virtually no traces other than digital. They try to hide in the shadows of ordinary network traffic, mask their activities, and encrypt data that constitutes digital evidence. Sometimes they may even return to the crime scene and continue to obliterate traces or verify their existence without the knowledge of law enforcement. Although the idea of anonymizing networks or flexible live operating systems did not originate with the criminal world in mind, its fruits are increasingly becoming such tools. This prompted the author to describe in this article the Linux Tails operating system as a tool and the anonymizing programs it contains, including those using the Tor network in the context of computer forensics. However, it is important to remember that these types of tools are also used by, among others, people living in authoritarian systems, or people who want to maintain their privacy. All readers who have had the opportunity to read the book „Non-Volatile Memory” by Edward Snowden know that during his work for the NSA, he used the Tails operating system to contact the press. And most importantly, he was not caught at it, which is a special recommendation.

The Tor (The Onion Router) network is a virtual computer network that implements second-generation onion routing, which prevents network traffic analysis and provides its users with almost anonymous access to Internet resources.

The Tor project was initially sponsored by the U.S. Naval Research Laboratory and developed as a military project to protect U.S. intelligence communications on the Internet. It was meant to mask the activities of intelligence agents on the Internet.

The initiators of the Tor network were programmers Roger Dingledine, Nick Mathewson and Paul Syverson, who began work on the project in 2002 with the support of the US Naval Research Center. In 2004 at the 13th. Security Symposium of the USENIX Association presented the paper „Tor: The Second-Generation Onion Router”. In late 2004 to November 2005, it became a project branded by the Electronic Frontier Foundation (EFF). Today, Tor software development is handled by the Tor Project, a non-profit research and education organisation based in the United States, supported by volunteers and network users around the world. The project currently operates under a BSD license, but has been indirectly sponsored by the US Navy all along (Mider, 2019).

The Onion Router was made available for civilian use in 2003. The servers making up the Tor network

in its early days were located only in the United States and Germany.

The name of the Tor network is an acronym for „The Onion Router“. It is derived from a technique that involves sending independent and multilayered encrypted packets, hence the term „onion routing“. The devices that make up this network, perform a process called onion routing, different from classic routing by routers using the TCP/IP model (Mider, 2019; Casad, 2017).

In the Tor network, data is sent in encrypted layers, analogous to the layers of an onion. The data thus encrypted is sent through a series of network relays (onion routers, or onion routers), each of which removes („peels off“) a single layer, revealing the next destination of the transmitted data. Once the last layer is decrypted, the data arrives at its destination. The sender remains anonymous, as each relay only knows the location of the immediately preceding and following relays. The router at each layer knows only what it needs to operate. The IP addresses of all requests and responses change at each relay (Ortega, 2022).

Onion routing is a data structure created by encapsulating („wrapping“) data in successive layers of encryption, which can be decrypted by as many intermediary computers as there are layers before it reaches its destination. The connection between each relay (proxy server) is encrypted. The original data (and its sender) remain hidden because the data is transmitted between intermediate relays, and no intermediate relay knows both the origin and destination of the data, so the sender remains anonymous.

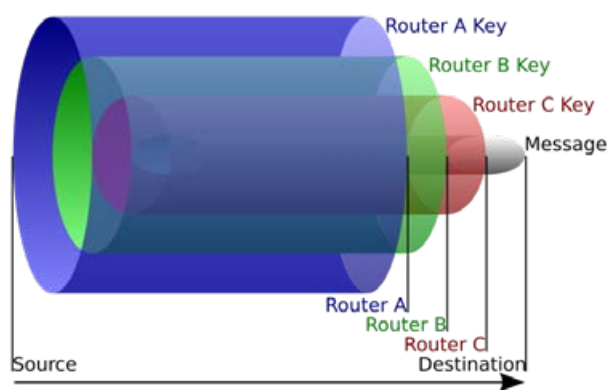


Fig. 1. Onion routing mechanism: the source sends data to Router A, which removes the encryption layer to find out just where to send it next and where it came from (although it doesn't know if the sender is the source or just another relay). Router A sends it to router B, which decrypts the next layer to learn its next data destination. Router B sends the data to Router C, which removes the last layer of encryption and sends the original message to its destination

Observation of such network traffic makes it impossible to tell what is being transmitted in it.

The Tor network provides TCP-based anonymity with relatively low latency and high bandwidth. The mechanisms implemented in the Tor network protocol impose a layer of anonymity on the TCP layer and create a (default minimum) three-point path through which Tor network routers layer encryption. Routing information is sent by a group of authoritative servers. In simple terms: all of a user's TCP communications are tunneled into a single relay, rotating in time, and to ensure low latency, the Tor network does not force retransmission of lost packets.

From a privacy perspective, the Tor network has two purposes:

1. hiding the location of users accessing the Internet – tracing the IP addresses and locations they use is supposed to be impossible;
2. encryption of transmitted data – the Tor network, by encrypting data and sending it via onion routing, hides the IP addresses of users and transmitted data, and hides the IP addresses of the ISPs through which users connect to the Tor network (Ortega, 2022).

The relays that make up the Tor network have different tasks, and depending on their characteristics and configuration, we distinguish:

1. guard relays – communicating with users, connected to the rest of the Tor network. Used for a long time. They have large throughputs;
2. middle relays – which communicate only with other relays. The data that comes out of them does not leave the Tor network;
3. exit relays – the end (edge) points of the Tor network. They receive the requests, send them to the recipients, receive the responses and send them across the network toward the sender;
4. bridge relays – which are relays about which there is no information in the public directory of Tor network relays, which are much more difficult to block. They are used when the ISP blocks the Tor network. The list is available at <https://bridges.torproject.org> (Ortega, 2022).

The use of the Tor network is as follows:

1. A host connecting to the Tor network retrieves a list of available relays and selects three of them: guard, relay and output;
2. The data to be sent over the Tor network is first encrypted. Only the originating relay knows the address of the requested network service and has insight into the data packets being transmitted, but

their origin is not known to it, thus providing privacy to the user;

3. The encrypted data is re-encrypted and only the relay relay knows which output relay to send it to. With double encryption, only the guard relay knows where the relay relay is located (Ortega, 2022).



Fig. 2. Diagram showing a typical scenario of a Tor client accessing a public site on the Internet

The data is encrypted before it leaves the user's computer:

1. If there is a system that monitors the Internet connection (the ISP may do so), it only sees the encrypted data exchanged with the watchdog relay;
2. Only the guard relay sees the user's IP and knows where the relay relay is located;
3. Only the relay relay knows where the guard and output relays are. However, it does not know where the user is or the requested website (or other web service). Relay relays do not know their places in the network;
4. The output relay knows where the requested website (or other web service) and relay relay are. But it doesn't know where the user and the guard relay are (Ortega, 2022).



Fig. 3. A diagram showing how a message travels through the Tor network until it reaches a public website. The Tor network client (Tor Browser) adds as many layers as there are relays in the chain

Some networks block outbound traffic on the TCP port 9050 used by the Tor network, and even dynamically

blacklist all Tor network relays, making it impossible to use the network. This restriction can be circumvented by using so-called network bridges, i.e. Tor network relays that are not visible in the public Tor network directory (Allsopp, 2017).

In addition to connecting to services on the Internet, the Tor network enables the use of so-called hidden services, provided on completely anonymous web servers, locked into and visible only within the Tor network ecosystem, which use their own distributed addressing system (Allsopp, 2017).

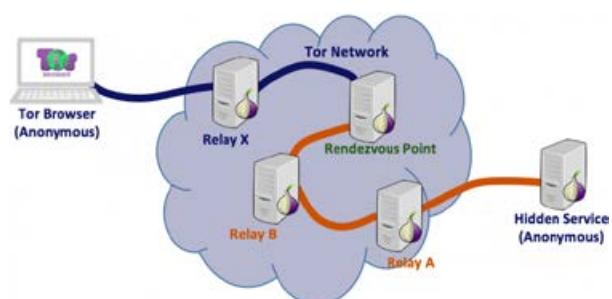


Fig. 4. Diagram showing the mechanism for accessing a web server hidden in the Tor network (hidden service): (1) one Tor Relay (relay) server will be selected as (relay) Rendezvous Point; (2) two connections are established: one from the Tor network client to the Rendezvous Point relay, and the other from a hidden server in the Tor network to the Rendezvous Point relay. The author leaves it to the attentive reader to consider whether the „Hidden Service“ in the diagram above should not be covered by the „Tor Network“ image cloud area

Unlike regular websites, which are accessed via their URLs, hidden services are accessed via a special type of onion address that contains a random, non-mnemonic string and is not part of the Internet's typical DNS system. Random characters in the address of a site on the TOR network (e.g.: https://zqkltwi4fecvo6ri.onion/wiki/index.php/Main_Page) make it even more difficult to find the right site - access is available to those who know how to look for them.

The most popular program for browsing the Tor network is the Tor Browser Bundle, integrated into the Mozilla Firefox web browser. The program provides protection to the user if he only uses the built-in Firefox browser. Once you are connected to the Tor network, you can freely browse the web, as well as chat using instant messaging. The program has a huge number of different configuration options, with which we can set up a connection to the Tor network and establish a new TCP connection by entering a different IP address. Tor Browser provides security at three levels, which we can set ourselves at any time. These levels are: Standard (all Tor browser and page features are

enabled); Safer (JavaScript support on pages without HTTPS is disabled, likewise some fonts and symbols, HTML5 media (audio and video) run only after we click) and Safest (same situation with HTML5 as above, and JavaScript disabled by default on all pages, likewise some fonts, symbols and images).

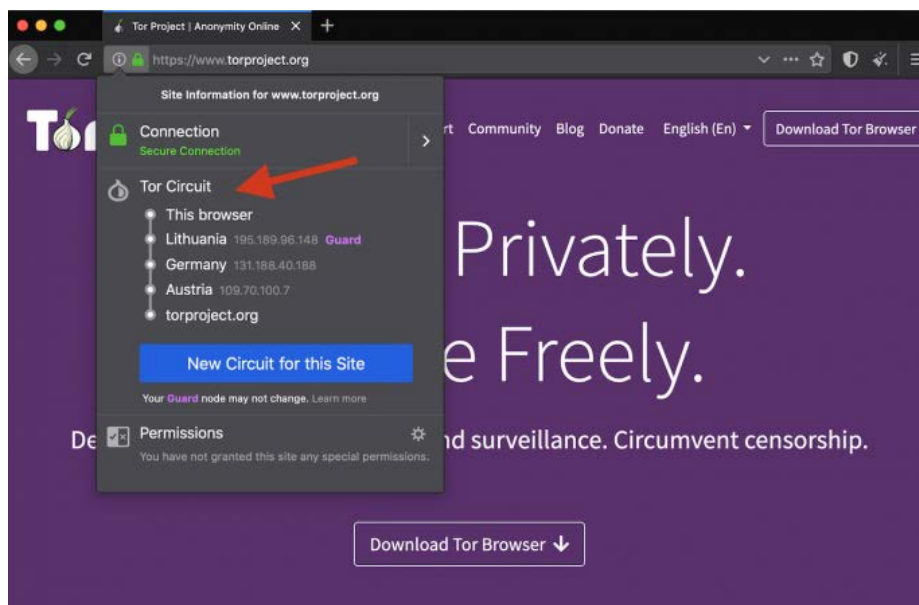
As you can learn from the above analysis of the operation of the Tor virtual network, specialized software is required to operate it. User safety increases when it operates in an environment that minimizes the creation of digital artifacts. The best such environment is a computer memory-only operating system or a virtual system. The Tails system described later in this article is not the only Linux distribution designed for similar purposes. Among the popular ones can also be mentioned: Qubes OS, minimalist Alpine Linux, IprediaOS, Whonix and Kodachi Linux, however, the author focused on the distribution in question due to its popularity in the evidence submitted for the study.

„The Amnesic Incognito Live System”, or Tails for short, is a Debian-based Linux distribution based on Debian and the Gnome desktop environment designed exclusively for use as a Live USB, Live DVD or for a virtual environment. The first version of this operating system was created in 2009 by the developers of „The Tails project” with security, privacy and user anonymity in mind. Up to version 5.2 on July 12, 2022,

the functionality of which will be discussed in this part of the article (the author’s paper focuses on functionality particularly relevant to digital forensics and therefore does not include a full description of Linux Tails 5.2), the project has undergone an impressive evolution that has also significantly affected the modus operandi of the criminals using it. Of particular relevance from the point of view of a computer forensic investigator seems to be the evolution of the system developers’ policy on methods of accessing the area made available for data recording.

Currently, according to the distributor, Tails is a system aimed at users such as activists, journalists and their sources, people experiencing excessive scrutiny in their environment, and anyone in need of privacy in the digital world. It is free software under the GNU/GPL license, so the source of funding for the aforementioned group of developers includes sponsors among whom the participation of organisations such as: U. S. Department of State (over \$100,000); ProtonMail, RIPE NCC (\$50,000-\$99,999 each) or Tor.

The operating system in question needs a 64-bit processor and at least 2 GB of RAM to operate and the manufacturer claims compatibility with most personal computers manufactured after 2006. As mentioned earlier, using a USB flash drive or DVD, it runs on the computer bypassing the use of the native



BLOCK TRACKERS

Tor Browser isolates each website you visit so third-party trackers and ads can't follow you. Any cookies

Fig. 5. Tor Browser window with visible addresses of Tor network relays and options for changing the circuit

operating system while guaranteeing read-only access to the mounted storage media. Even at this stage of the user's action, no artifacts indicating the use of Tails are created on the computer, since the only non-standard command during startup is the use of the boot media selection interface, and as the practice of the article's author confirms, on most of the devices tested and submitted for testing in the course of the implementation of the provisions for the expert opinion, this operation does not require permanent modification of the BIOS settings.

After selecting the standard startup mode, the user has the option to preconfigure parameters, among others that significantly affect security.

These settings include the ability to specify an administrative password. Skipping this step significantly limits certain functionality while giving the less sophisticated user a greater guarantee of avoiding digital evidence artifacts. Other pre-configuration options worth mentioning are the ability to automatically anonymize the physical MAC address of network interfaces, enforced offline mode, provision of the so-called Unsafe Browser function, i.e. a web browser with the ability to use the Internet bypassing Tor, which is blocked by default for security reasons. Previous development versions of Linux Tails at the pre-configuration level even offered, at a minimum, camouflage in the form of a graphical interface resembling the MS Windows desktop.

The Linux Tails operating system running with the parameters described above, as mentioned earlier, allows access to mounted storage media in „read-only” mode. The correct operation of the Tails system's software write blocker was confirmed by the author's numerous tests, which consisted of mounting various media, both removable memory and disks installed in the tested units, reviewing their contents, attempting to write to these media using GUI software distributed with the live USB compilation Linux Tails 5.2 and running this system, and then verifying their SHA-1 and MD5 hash function values. It should be noted that for file systems other than those based on GNU/Linux, the built-in file viewer automatically ignores access permission restrictions to view the contents of storage media. Thus, in the absence of encryption, it is possible to access, read or make copies of any personal computer user's files, even if the native operating system is protected from unauthorized access (A simple way to prevent unauthorized booting of Tails on a computer is to protect the boot source selection panel with a BIOS-level password). In addition, no digital evidence artifacts related to this fact are observed on the computer in use. Although the operations are performed using RAM, however, the Tails system architecture has a built-in mechanism that immediately overwrites the allocated area when the process finishes, the system also blocks the standard methods of performing a RAM dump. The execution of such a snapshot is

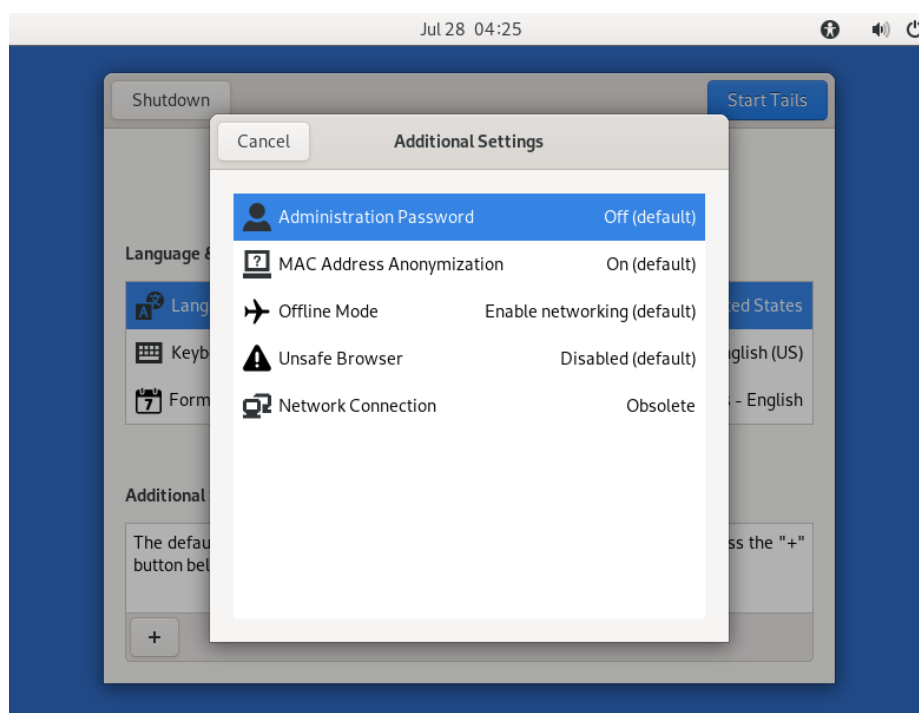


Fig. 6. View of Linux Tails session pre-configuration panel selection windows taken as a screenshot of a session on a virtual machine

possible, for example, with the help of AVML software, however, due to the limitation of the possibility of saving the result only in the „Persistent Storage” area (See the further part of the article) or with the help of a web interface, it represents, besides the analysis of the content of the snapshot itself, an interesting and important research problem to be solved in the course of further author’s own analysis. In addition, when Tails is properly terminated, all of its ephemeral memory is overwritten, making it invulnerable to the use of investigative „cold boot attack” methods.

In earlier development versions of Linux Tails, an intermediate user could mount storage media in „read-write” mode, so to the capabilities described above, the ability to tamper with data could be added. In the described version 5.2 from the level of standard system settings and attached applications, there is no such functionality, which, despite the increase in the level of confidentiality of use, causes a significant hindrance, i.e. no storage for data produced during the work. Among other things, the developers have implemented a feature called: „Persistent Storage” – encrypted permanent

storage. This feature is available to configure from Linux Tails, which is running from a USB stick. With its help, the user sets up a partition encrypted with the Linux LUKS standard in the free storage area of the carrier („Persistent Storage” can only be installed on the carrier with Linux Tails’. During the next boot of the Live system, the partition is recognized and, after entering the password in read-write mode, an encrypted space is made available, where, in addition to user files, applications can be installed or Tails configuration settings stored, among other things.

It is telling that the operating system in question does not force the creation of a password of high complexity (it even allows one arbitrary character as an access password), which makes the created partition vulnerable to dictionary or „brute force” attacks using mini-software such as „Passware Kit Forensics”. In addition, the LUKS encryption standard allows the encrypted partition to be read with a known access password on any computer with the appropriate software. This activity can easily lead to artifacts in the operating system of the computer used, containing, for

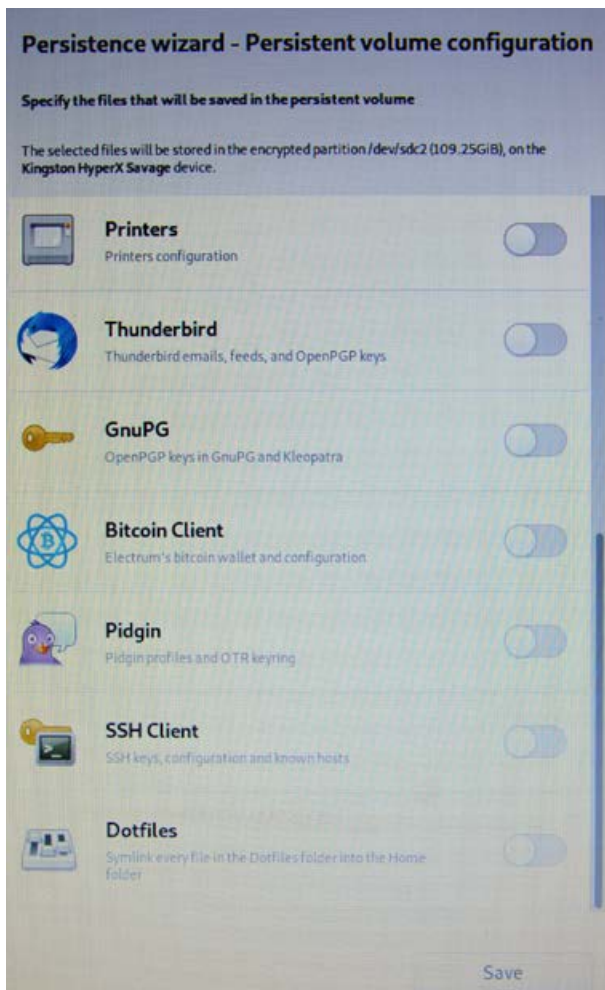
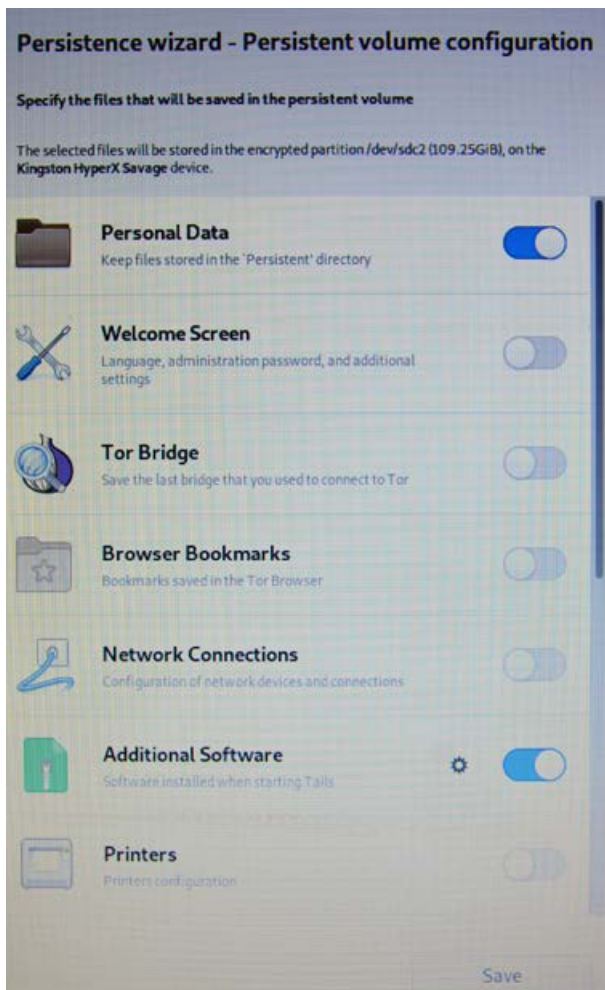


Fig. 7. Images of the „Persistent Storage” configuration window

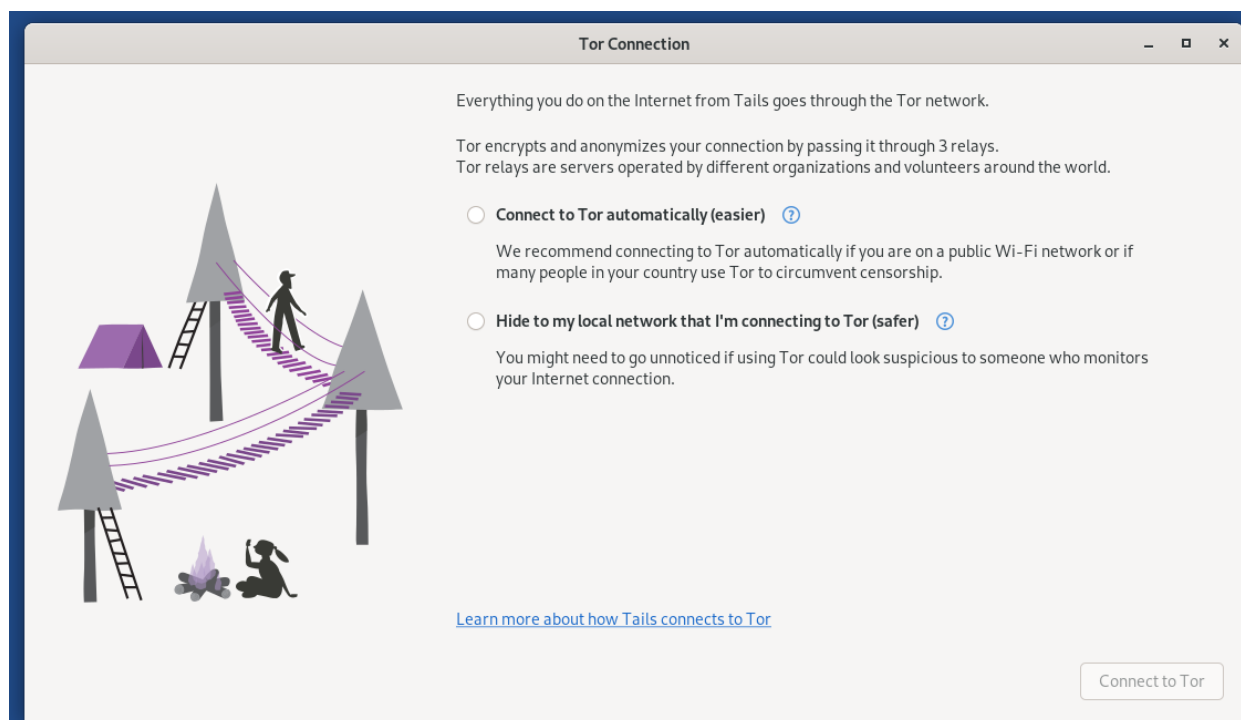


Fig. 8. View of the Tor connection configuration window taken as a screenshot of a session on a virtual machine

example: thumbnails or copies of multimedia content, file indexes and their metadata, having the meaning of digital traces.

Another layer of usability for Linux Tails is the web interface. As described earlier, the „Unsafe Browser” is available only upon explicit request by the user. Otherwise, all communication with the Internet or hidden services on the Tor network is carried out via the Tor network. In addition, the system offers the use of „Tor bridge”, or specialized relays that hide traffic as described earlier in this article. This method also makes it possible to access the Tor network through access points where such Internet connection is blocked or to hide such activity.

With the additional assumption of the use of a VPN, the absence of the creation of non-fleeting artefacts on the computer that are associated with network usage, the encryption of data packets and their metadata, the lack of direct access by investigators to the computer in use with an open Tails session, the analysis of network traffic and its tracking becomes extremely difficult and laborious, not to say impossible. However, it should be noted that there are tools based on analysis of anomalies in network traffic that allow typing users who use the described techniques.

The described version 5.2 also has a built-in „Thunderbird” mail client with support for encrypted e-mails, a „KeePassXC” application supporting the creation and storage of access passwords, the „LibreOffice” office suite, a very interesting „OnionShare” application

supporting file transfer via the Tor network, a suite of graphics and sound processing tools, and other utility programs, including diagnostics.

Also noteworthy is the fact, confirmed by tests and analysis of materials submitted for testing, of satisfactory stability of system operation. At the same time, if the media containing a running session of Linux Tails 5.2 is suddenly removed from the USB port, the GUI is immediately shut down and, after a brief listing of errors and several system processes, the computer shuts down. The significance of the mechanism described above for law enforcement agencies, the author allows himself to leave to the reader’s free thought. In addition, Tails works stably in a virtual environment such as VMware Workstation, where the only limitation of functionality is the lack of support for „Persistent Storage”(according to the distributor, full functionality on the machine is available in the „virt-manager” application running in a Linux environment).

In the practice of expert IT investigators, one encounters ingenious combinations of sophisticated tools that make data analysis difficult, such as Linux Tails, and a variety of physical hardware modifications designed to further secure data from law enforcement access. The material provided for testing in one such case was a laptop computer in which part of the case had been cut out to facilitate quick removal of the hard drive, while the optical media reader revealed one of the Tails distributions recorded on a DVD, as illustrated in the photos below:

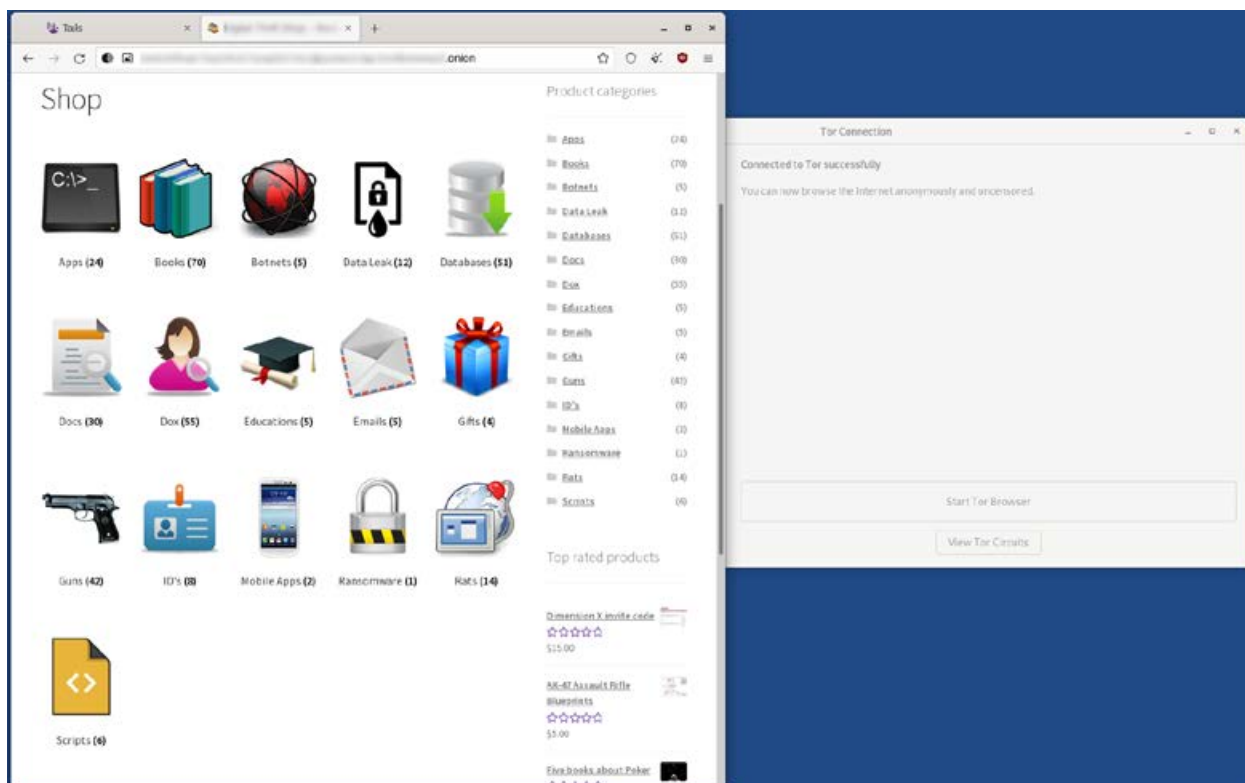


Fig. 9. View of a browser window with a preview site running, accessible only from Tor, taken as a screenshot of a session on a virtual machine

In another more analytically challenging case, the author, despite detailed research using X-Ways Forensics software, Magnet AXIOM or virtualisation of the operating system installed on the computer unit submitted for testing, failed to reveal, according to the investigator's question: documentation, web browsing history entries or the contents of correspondence regarding the marketing of certain illegal substances. Although the history revealed in the memory of the web browsers and the contents of the files did not even indicate the user's interest in the issues in question, they became crucial in pointing out the further course of the case. This is because a detailed analysis of search history for phrases on the Internet indicated that the user's interest in anonymisation tools and access to the Tor network was sudden and ran over a short period of time. Digital traces indicating the download of one of the Linux Tails distributions from the Internet were also found. An earlier analysis on the partition responsible for booting MS Windows (write access from the MS Windows user level is blocked on such a partition) also revealed the presence of an unusual text file. Correlation of the timestamps of the artifact sets described above indicated the order of operations described below. As a first step, the user searched for and then downloaded and installed Linux Tails on removable media. In order to hide the data that was sensitive to him, he saved it in a text file placed, as mentioned

above, on a system disk partition invisible from the MS Windows user (the save operation would not have been possible (for an intermediate user) if newer Tails distributions such as version 5.2 had been used. This fact may explain why cases considered under current test orders are able to contain older development versions of the system in evidence). In fact, the file in question contained the address of a TOR network site, which, due to a syntax characterized by high character entropy, as mentioned earlier (e.g.: https://zqkltwi4fecvo6ri.onion/wiki/index.php/Main_Page), is cumbersome to remember. The address in question led to a personalized user page on a site specializing in the trafficking of illegal substances. Including the substances involved in the study order. The transparency policy of the said



Fig. 10. View of the reader with the Linux Tails carrier



Fig. 11. View of modifications to the computer case pictured above

site allowed individual users to write public feedback. Thus, it was established that based on complaints from recipients (related to the breaking of contact and failure to deliver the purchased goods), the personalized site in question was blocked immediately after the date of activities related to securing the equipment submitted for testing. In addition, the author would like to point out that while the presence of the disclosed address in the area accessible to the MS Windows user can be tried to explain even by processes of digital geology, e.g. related to the „cache” of Internet browsers, the appearance of the file in the described area of the storage medium, indicates intentional behavior, and this with the use of non-specific professional tools.

Summarizing the above analysis, the author would like to point out that the Linux Tails tool version 5.2 is a system that minimizes the emergence of geological digital evidence (Altheide, 2014, 18), i.e. that which is related to the autonomous operation of the computer system and arises automatically and unintentionally. At the same time, the amount of artifacts of the nature of digital archaeology (Altheide, 2014, 18), that is, those created intentionally as a result of the user's actions of the datasets depends in this case on the user's self-awareness and the nature and level of complexity of the operations performed. With regard to criminal applications, a key user concern is the tediousness of performing sometimes habitually simple operations, and thus the temptation to abandon certain security principles. Such behavior provides a field for the use of the computer forensic scientist's most valuable skills, which, in addition to special knowledge, are the ability to think analytically and correlate facts, without which even increasingly sophisticated forensics software will still be useless.

My special appreciation for the exchange of scientific ideas go to: Rafał Czech, Marcin Napiórkowski and Krzysztof Turowski.

Author

References:

1. Allsopp, W. (2017). *Advanced Penetration Testing: Hacking the World's Most Secure Networks* (in Polish). Wydawnictwo Helion.
2. Altheide, C., Carvey, H. (2014). *Digital Forensics with Open Source Tools* (in Polish). Wydawnictwo Helion.
3. Casad, J. (2017). *TCP/IP in 24 hours. Issue VI* (in Polish). Wydawnictwo Helion.
4. Ciborski, T. (2015). *Ukryta tożsamość. Jak się obronić przed utratą prywatności* (*Hidden Identity. How to protect yourself from loss of privacy*). Wydawnictwo Helion.
5. Flow, S. (2022). *How To Hack Like A Ghost. Breaching the Cloud* (in Polish) Wydawnictwo Helion.
6. Hayes, D. R. (2021). *Practical Guide to Computer Forensics Investigations. Issue II* (in Polish). Gliwice Wydawnictwo Helion.
7. Krawetz N. (2008). *Hacking Ubuntu: Serious Hacks Mods and Customizations* (in Polish). Gliwice Wydawnictwo Helion.
8. Mider D. (2019). *Czarny i czerwony rynek w sieci The Onion Router – analiza funkcjonowania darkmarketów* (Black and red markets in The Onion Router network – an analysis of how dark markets work), *Przegląd Bezpieczeństwa Wewnętrznego* 21/19
9. Muniz J, Lakhani A. (2014). *Kali Linux. Penetration tests*. Gliwice Wydawnictwo Helion.
10. Ortega J. M. (2022). *Mastering Python for Networking and Security. Leverage Python scripts and libraries to overcome networking and security issues. Issue II* (in Polish). Gliwice Helion Publishing
11. Sokół R. (2014). *Jak pozostać anonimowym w sieci* (How to stay anonymous online). Gliwice Wydawnictwo Helion.
12. Petreley N, Bacon J. (2005). *Linux Desktop Hacks* (in Polish). Gliwice Wydawnictwo Helion.

Source of figures:

Fig. 1. Onion routing, Wikipedia, https://pl.wikipedia.org/wiki/Trasowanie_cebulowe

Fig. no. 2, 3, 4: Hosting Anonymous Website on Tor Network, Abed Samhuri, <https://medium.com/axon-technologies/hosting-anonymous-website-on-tor-network-3a82394d7a01>

Fig. 5. Tor Browser 9.0 now available for download, Sekurak, <https://sekurak.pl/tor-browser-9-0-juz-dostepny-do-pobrania/>

Fig. no. 6, 7, 8, 9, 10, 11: author

Internet Sources:

1. BridgeDB, Tor Project, <https://bridges.torproject.org/bridges?transport=obfs4> (date of access: July 28, 2022).

2. GitHub – microsoft/avml: AVML – Acquire Volatile Memory for Linux, <https://github.com/microsoft/avml> (date of access: 26 July 2022).
3. Hosting Anonymous Website on Tor Network, Abed Samhuri, <https://medium.com/axon-technologies/hosting-anonymous-website-on-tor-network-3a82394d7a01> (date of access: July 28, 2022).
4. How to install and properly configure the Tor 8.0 browser, Ewelina Stój, PurePC, <https://www.purepc.pl/jak-zainstalowac-i-poprawnie-skonfigurowac-prze-gladarke-tor-8-0> (date of access: 27 July 2022).
5. Tools for anonymizing online activities as an instrumentality for information operations in hybrid warfare, Przegląd Bezpieczeństwa Wewnętrznego, Special Issue, Kamil Kucharski, <https://www.abw.gov.pl/download/1/1923/kucharski.pdf> (date of access: 28 July 2022).
6. TOR network – everything you need to know about it, Bitdefender, <https://bitdefender.pl/siektor-wszystko-co-trzeba-o-niej-wiedziec/> (date of access: July 28, 2022).
7. Signing in to a network using a captive portal, https://tails.boum.org/doc/anonymous_internet/tor/index.en.html#hiding (date of access: 26 July 2022).
8. Tor Browser Bundle, goodprograms, <https://www.dobreprogramy.pl/tor-browser-bundle,program,windows,6628600948791425> (date of access: July 28, 2022).
9. Tor Browser 9.0 now available for download, Sekurak, <https://sekurak.pl/tor-browser-9-0-juz-dostepny-do-pobrania/> (date of access: July 28, 2022).
10. Tor (anonymous network), Wikipedia, [https://pl.wikipedia.org/wiki/Tor_\(sie%C4%87_anonymous\)](https://pl.wikipedia.org/wiki/Tor_(sie%C4%87_anonymous)) (date of access: July 28, 2022).
11. Tails – Accessing the internal hard disk, https://tails.boum.org/doc/advanced_topics/internal_hard_disk/index.en.html (date of access: 26 July 2022).
12. Tails – Memory erasure, https://tails.boum.org/contribute/design/memory_erasure/ (date of access: 26 July 2022).
13. Tails – Sponsors, <https://tails.boum.org/sponsors/index.en.html> (date of access: 26 July 2022).
14. Onion routing, Wikipedia, https://pl.wikipedia.org/wiki/Trasowanie_cebulowe (date of access: July 28, 2022).
15. Historical Outline of the Darknet and Aspects of Legal and Illegal Use of Tor Technology, Review of Applied Sciences No. 19, Opole University of Technology Faculty of Economics and Management, Rafał Kokot, Tomasz Turba, https://pns.po.opole.pl/images/PNS_19/PNS19-IX.pdf (date of access: 28 July 2022).