Cristian Cortez

ID: if2482

CS 471: Security & Info Assurance

Assignment 7

Abstract

In this assignment, we use Tails OS to run a Tor Browser that is connected to a Tor network. The prupose of this assignment is to understand how Tails OS and Tor provide a user with Data Confidentiality through data encryption. Tails OS is run through a VM without persistant storage. Tor Browser is used to generate traffic. "Tcpdump" is used to capture packets while Wireshark is used for analysis. Packet analysis shows how a user is anonymous during data transmission as well as hidden packet content that provides privacy.

Introduction

A Tails system will be used to connect to the Tor Network via a Tor browser session. Tcpdump will be used to capture packets. Wireshark will be used to analyze packets after capture. An encrypted text file will be created and shared via OnionShare as well as donloaded and decrypted.

Commands used:

NIX GENERAL

```
// create a text file with a message.
echo "All work and no play makes Cristian a dull boy." >> Desktop/secrets.txt

// copy the file to the Tor Browser directory
cp Desktop/secrets.txt.gpg 'Tor Browser'

//change permissions on pcap file
sudo chown amnesia:amnesia Desktop/packets.pcap

// copy the pcap file to the Tor Browser for cloud upload
cp Desktop/packets.pcap 'Tor Browser'
```

GPG

```
// encrypt with symmetric encryption.
gpg --symmetric Desktop/secrets.txt
```

TCPDUMP

```
// start packet capture with tcpdump
sudo tcpdump -i any -s 65535 -w Desktop/packets.pcap
```

WIRESHARK : FILTERS

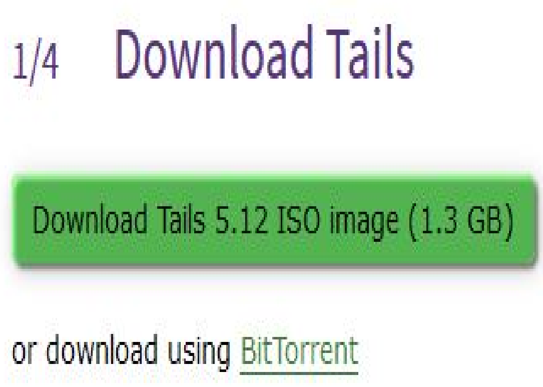
```
// filter the packets for only those that contain tcp
tcp

// filter packets with ip address loopback
ip.addr == 127.0.0.1
```

Summary of Results

A: Create Tails OS in a Virtual Box

1. Download the Tail iso

Download the Tails OS iso here


1/4 Download Tails
Download Tails 5.12 ISO image (1.3 GB)
or download using BitTorrent

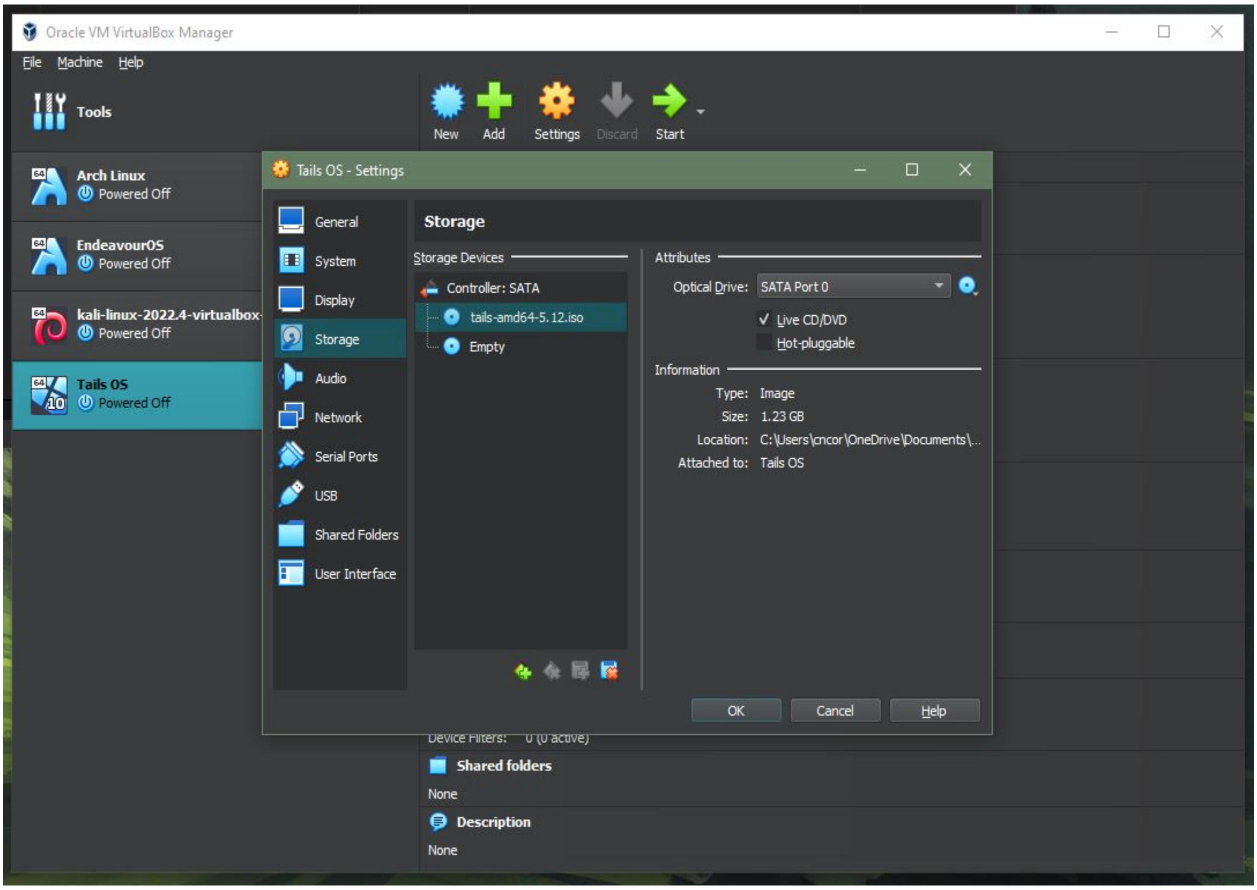
2. Create a Virtual Box

Create a Virtual Box named "Tails OS" with no hard drive. Add the iso image as a new optical drive in Virtual Box.

Go to:

```
Tails OS -> Settings -> Storage -> Controller SATA -> "Add Optical Drive" ->
select Tails iso
```

Next, select "Live CD/DVD".



Storage

Storage Devices

Controller: SATA
- tails-amd64-5.12.iso
- Empty

Attributes

Optical Drive: SATA Port 0

☑ Live CD/DVD

□ Hot-pluggable

Information

Type: Image
Size: 1.23 GB
Location: C:\Users\cncor\OneDrive\Documents\...
Attached to: Tails OS

Device Filters: 0 (0 active)

Shared folders: None

Description: None

3. Run Tails for the First Time

Run the newly created VM.

Be sure to set the sudo password to "letmein". This is very important.

Go to:

```
Welcome to Tails! -> Additional Settings -> Admin Password -> "letmein" -> Add
```

Then go ahead and start Tails!

B: Pre-packet Capture: Tor Connect and Plaintext File Encryption

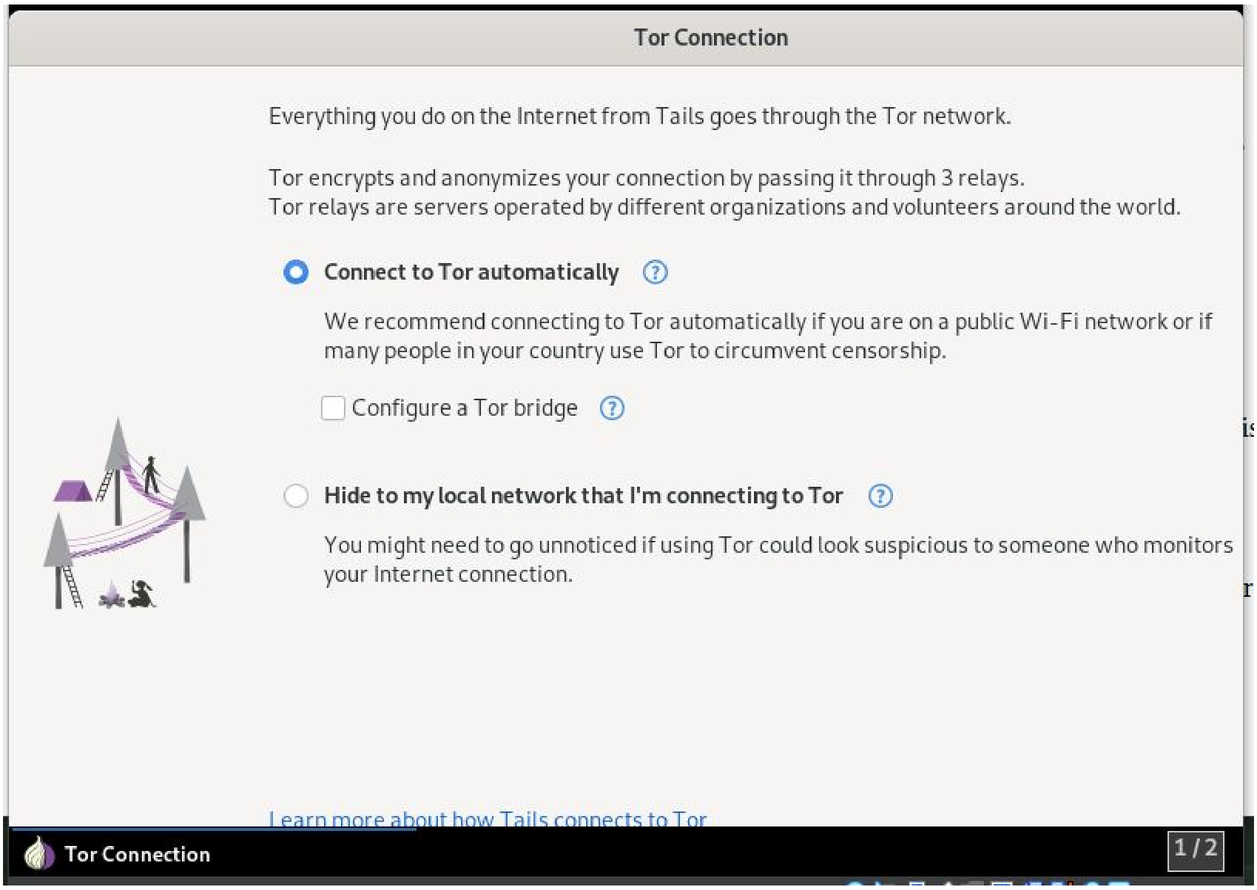
1. Tor Connection

After starting Tails, a new window will ask to set up a Tor Connection.

Select:

```
"Connect to Tor Automatically"
```

Do not Configure a Tor bridge.



Tor Connection

Everything you do on the Internet from Tails goes through the Tor network.

Tor encrypts and anonymizes your connection by passing it through 3 relays.
Tor relays are servers operated by different organizations and volunteers around the world.

● Connect to Tor automatically

We recommend connecting to Tor automatically if you are on a public Wi-Fi network or if many people in your country use Tor to circumvent censorship.

□ Configure a Tor bridge

○ Hide to my local network that I'm connecting to Tor

You might need to go unnoticed if using Tor could look suspicious to someone who monitors your Internet connection.

Learn more about how Tails connects to Tor

Then select:

```
"Connect to Tor"
```

This process will take a few seconds.

NOTE: this option maybe hidden behind the VM window. Increase the size of the VM window and youll see it.

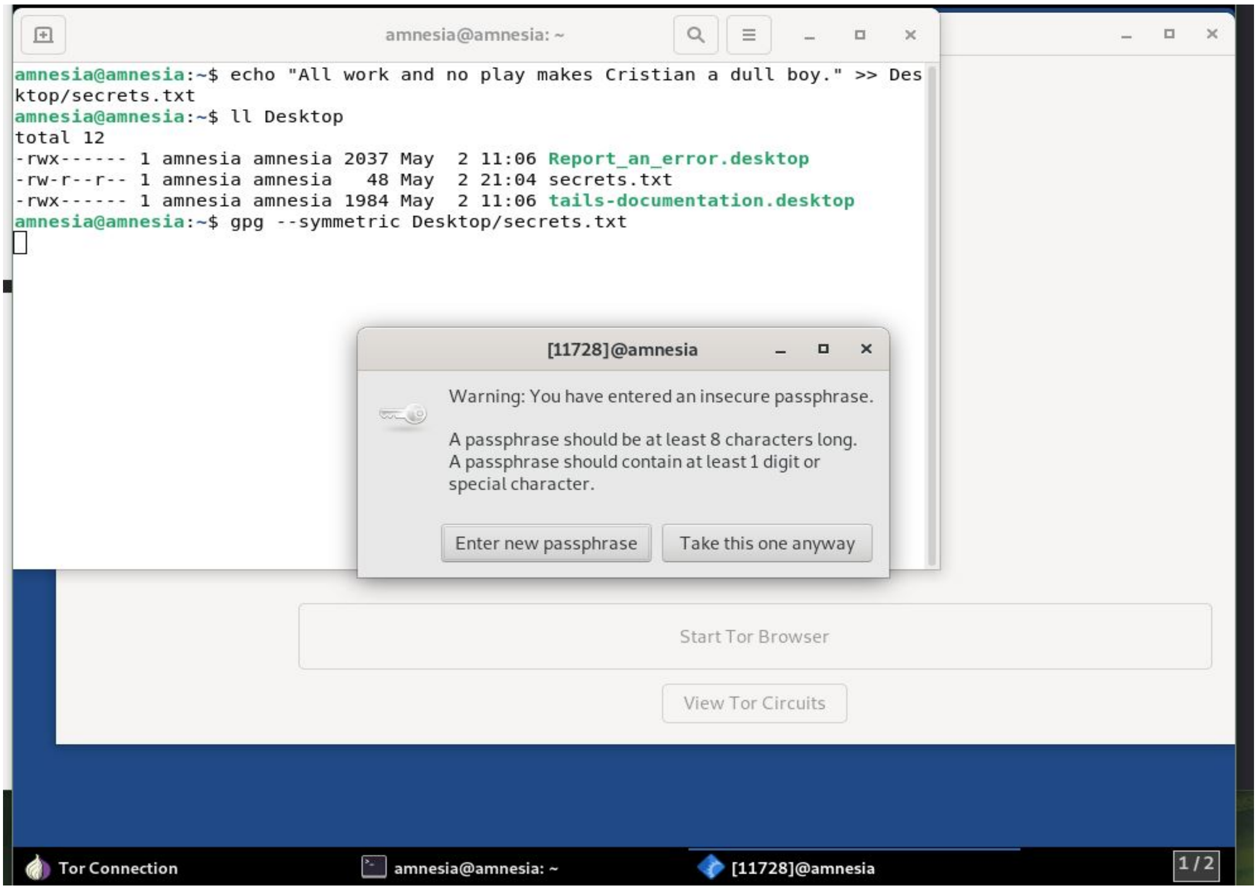
Do not start the browser yet.

2. Plaintext file ecnryption

We will need an encrypted file to upload to the *Onionshare* service. We will use "gpg" command tool to symmetrically encrypt the file. Ensure to use the password "letmein"; this is important.

Use commands:

```
// create a text file with a message.
echo "All work and no play makes Cristian a dull boy." >> Desktop/secrets.txt

// encrypt with symmetric encryption.
gpg --symmetric Desktop/secrets.txt

// copy the file to the Tor Browser directory
cp Desktop/secrets.txt.gpg 'Tor Browser'
```



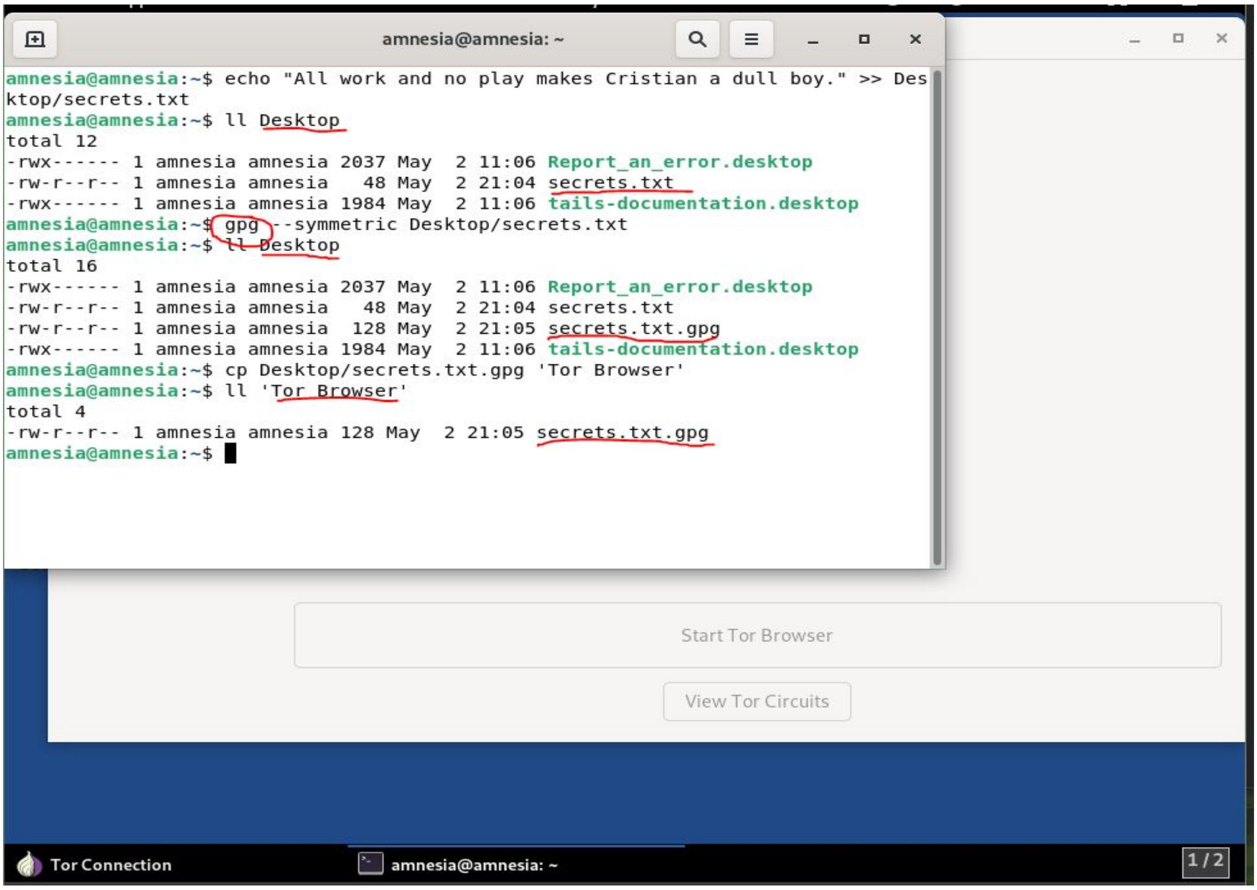
```
amnesia@amnesia:~$ echo "All work and no play makes Cristian a dull boy." >> Desktop/secrets.txt
amnesia@amnesia:~$ ll Desktop
total 12
-rwx------ 1 amnesia amnesia 2037 May  2 11:06 Report_an_error.desktop
-rw-r--r-- 1 amnesia amnesia   48 May  2 21:04 secrets.txt
-rwx------ 1 amnesia amnesia 1984 May  2 11:06 tails-documentation.desktop
amnesia@amnesia:~$ gpg --symmetric Desktop/secrets.txt
```

[11728]@amnesia

Warning: You have entered an insecure passphrase.

A passphrase should be at least 8 characters long.
A passphrase should contain at least 1 digit or special character.

Once created, this encrypted file will need to be copied to the 'Tor Browser' folder. Tor browser only has permission to access this folder an no other.



```
amnesia@amnesia:~$ echo "All work and no play makes Cristian a dull boy." >> Desktop/secrets.txt
amnesia@amnesia:~$ ll Desktop
total 12
-rwx------ 1 amnesia amnesia 2037 May  2 11:06 Report_an_error.desktop
-rw-r--r-- 1 amnesia amnesia   48 May  2 21:04 secrets.txt
-rwx------ 1 amnesia amnesia 1984 May  2 11:06 tails-documentation.desktop
amnesia@amnesia:~$ gpg --symmetric Desktop/secrets.txt
amnesia@amnesia:~$ ll Desktop
total 16
-rwx------ 1 amnesia amnesia 2037 May  2 11:06 Report_an_error.desktop
-rw-r--r-- 1 amnesia amnesia   48 May  2 21:04 secrets.txt
-rw-r--r-- 1 amnesia amnesia  128 May  2 21:05 secrets.txt.gpg
-rwx------ 1 amnesia amnesia 1984 May  2 11:06 tails-documentation.desktop
amnesia@amnesia:~$ cp Desktop/secrets.txt.gpg 'Tor Browser'
amnesia@amnesia:~$ ll 'Tor Browser'
total 4
-rw-r--r-- 1 amnesia amnesia 128 May  2 21:05 secrets.txt.gpg
amnesia@amnesia:~$
```

C: Pack Capture: Tor Browser, DuckDuckGo, Onion Address, Unsafe Browser, Onion Share

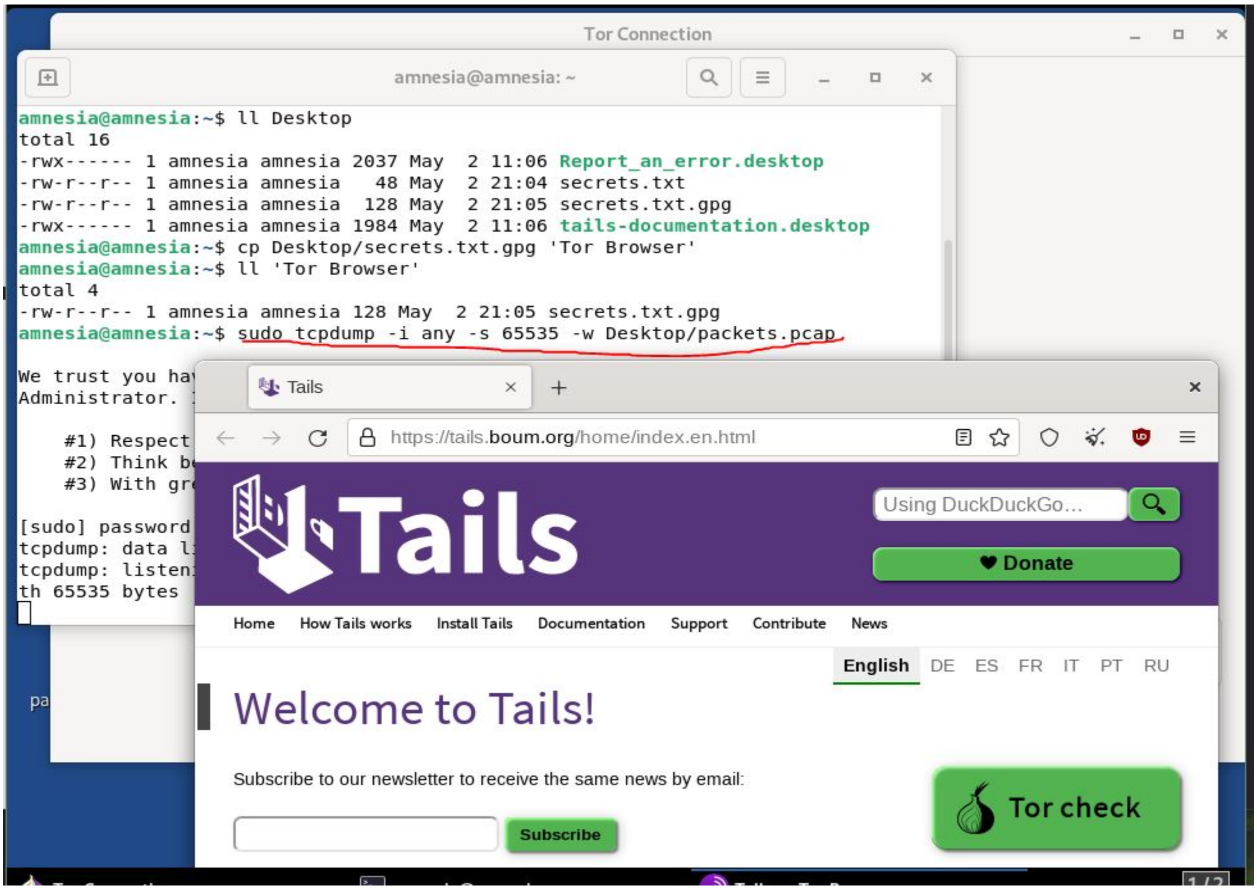
1. Start Packet Capture

In this assignment, we will use the "tcpdump" command instead of Wireshark to conduct the packet capture.

Ensure to save the file with a Wireshark compatiable extension i.e. ".pacp"

Use Commands:

```
// start packet capture
sudo tcpdump -i any -s 65535 -w Desktop/packets.pcap
```



```
amnesia@amnesia:~$ ll Desktop
total 16
-rwx------ 1 amnesia amnesia 2037 May  2 11:06 Report_an_error.desktop
-rw-r--r-- 1 amnesia amnesia   48 May  2 21:04 secrets.txt
-rw-r--r-- 1 amnesia amnesia  128 May  2 21:05 secrets.txt.gpg
-rwx------ 1 amnesia amnesia 1984 May  2 11:06 tails-documentation.desktop
amnesia@amnesia:~$ cp Desktop/secrets.txt.gpg 'Tor Browser'
amnesia@amnesia:~$ ll 'Tor Browser'
total 4
-rw-r--r-- 1 amnesia amnesia 128 May  2 21:05 secrets.txt.gpg
amnesia@amnesia:~$ sudo tcpdump -i any -s 65535 -w Desktop/packets.pcap

We trust you ha
Administrator. 

    #1) Respect
    #2) Think b
    #3) With gr

[sudo] password
tcpdump: data l
tcpdump: listen
th 65535 bytes
```

Welcome to Tails!

Subscribe to our newsletter to receive the same news by email:

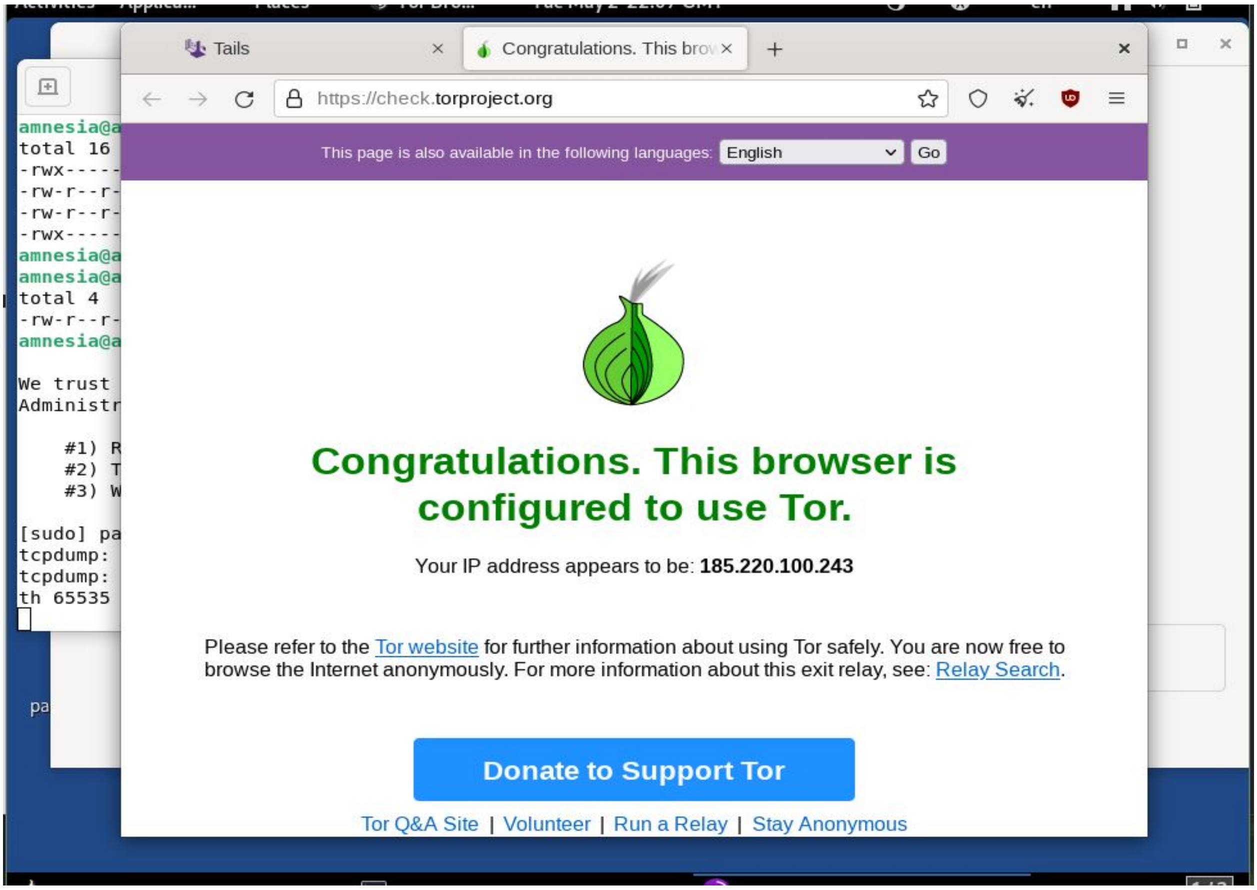
Then start the Tor Browser from the still open "Tor Connection" window.

2. Check Tor Browser Configuration

To check if the Tor Browser is correctly configured, navigate to

https://check.torproject.org/

This will check the browser config.



```
amnesia@a
total 16
-rwx-----
-rw-r--r-
-rw-r--r-
-rwx-----
amnesia@a
amnesia@a
total 4
-rw-r--r-
amnesia@a

We trust
Administr

    #1) R
    #2) T
    #3) W

[sudo] pa
tcpdump:
tcpdump:
th 65535
```

This page is also available in the following languages: English Go

Congratulations. This browser is configured to use Tor.

Your IP address appears to be: **185.220.100.243**

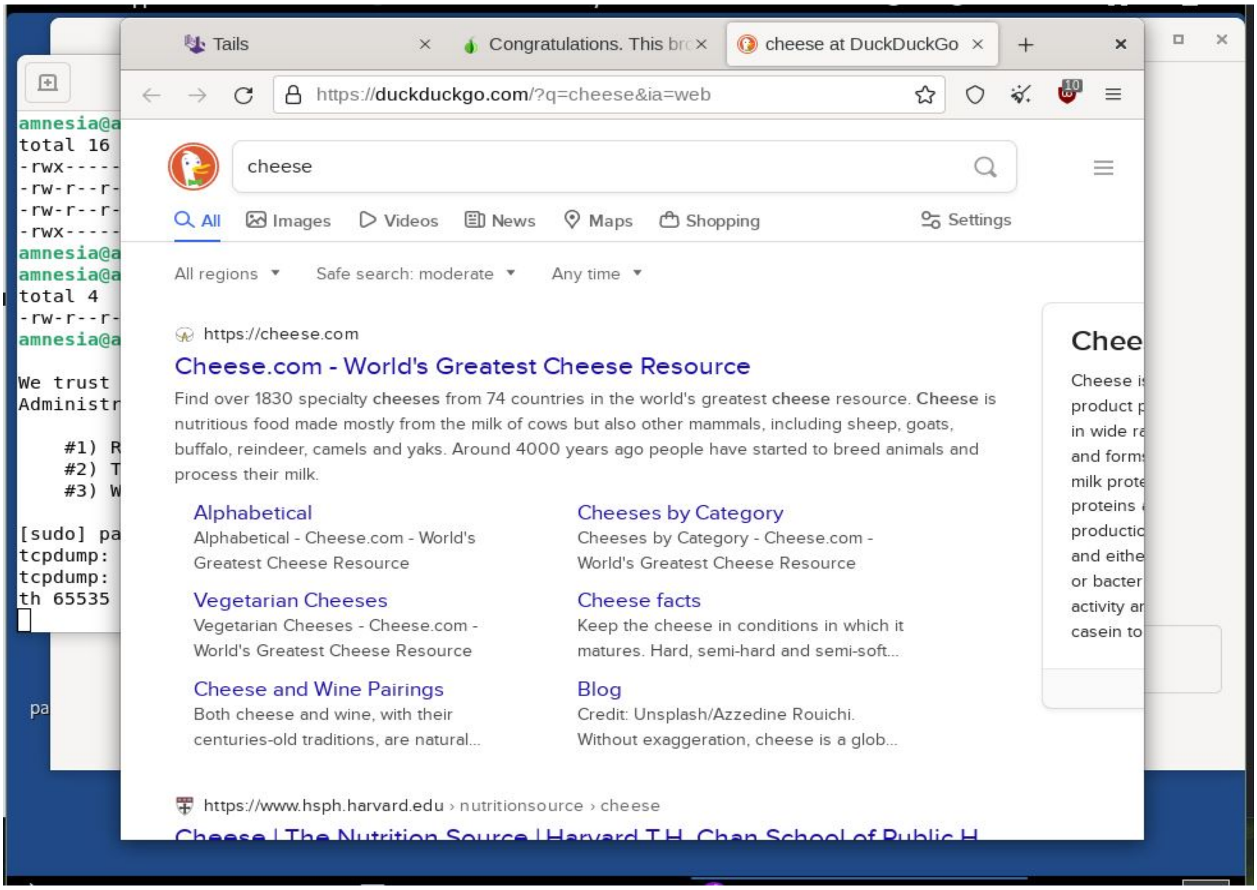
Please refer to the Tor website for further information about using Tor safely. You are now free to browse the Internet anonymously. For more information about this exit relay, see: Relay Search.

Donate to Support Tor

Tor Q&A Site | Volunteer | Run a Relay | Stay Anonymous

3. Tor Browser, DuckDuckGo, Unsafe Browser

From the Tor browser, do some basic web searches. For example, search duckduckgo for "cheese".



```
amnesia@a
total 16
-rwx-----
-rw-r--r-
-rw-r--r-
-rwx-----
amnesia@a
amnesia@a
total 4
-rw-r--r-
amnesia@a

We trust
Administr

    #1) R
    #2) T
    #3) W

[sudo] pa
tcpdump:
tcpdump:
th 65535
```

https://cheese.com

Cheese.com - World's Greatest Cheese Resource

Find over 1830 specialty **cheeses** from 74 countries in the world's greatest **cheese** resource. **Cheese** is nutritious food made mostly from the milk of cows but also other mammals, including sheep, goats, buffalo, reindeer, camels and yaks. Around 4000 years ago people have started to breed animals and process their milk.

Alphabetical
Alphabetical - Cheese.com - World's Greatest Cheese Resource

Cheeses by Category
Cheeses by Category - Cheese.com - World's Greatest Cheese Resource

Vegetarian Cheeses
Vegetarian Cheeses - Cheese.com - World's Greatest Cheese Resource

Cheese facts
Keep the cheese in conditions in which it matures. Hard, semi-hard and semi-soft...

Cheese and Wine Pairings
Both cheese and wine, with their centuries-old traditions, are natural...

Blog
Credit: Unsplash/Azzedine Rouichi. Without exaggeration, cheese is a glob...

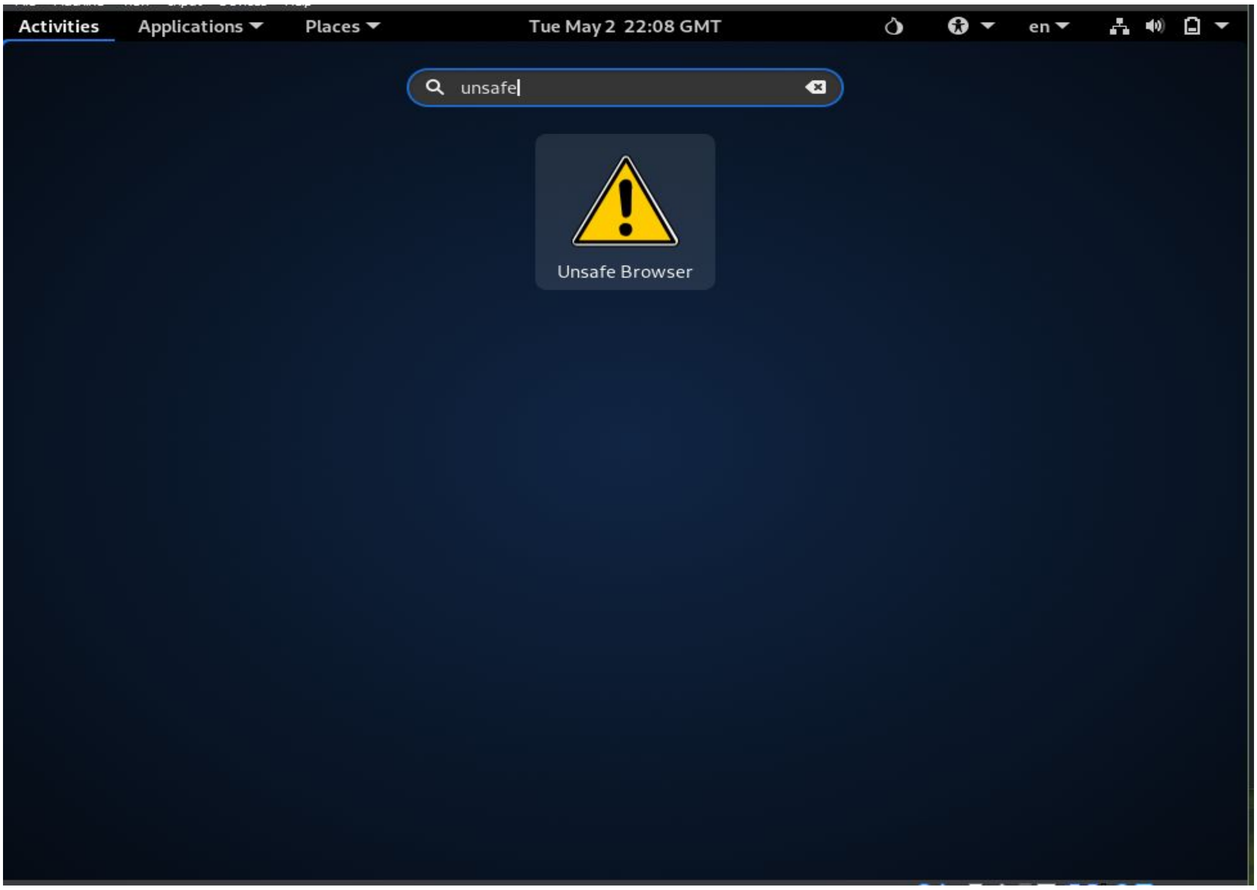
https://www.hsph.harvard.edu › nutritionsource › cheese

Cheese | The Nutrition Source | Harvard T.H. Chan School of Public H

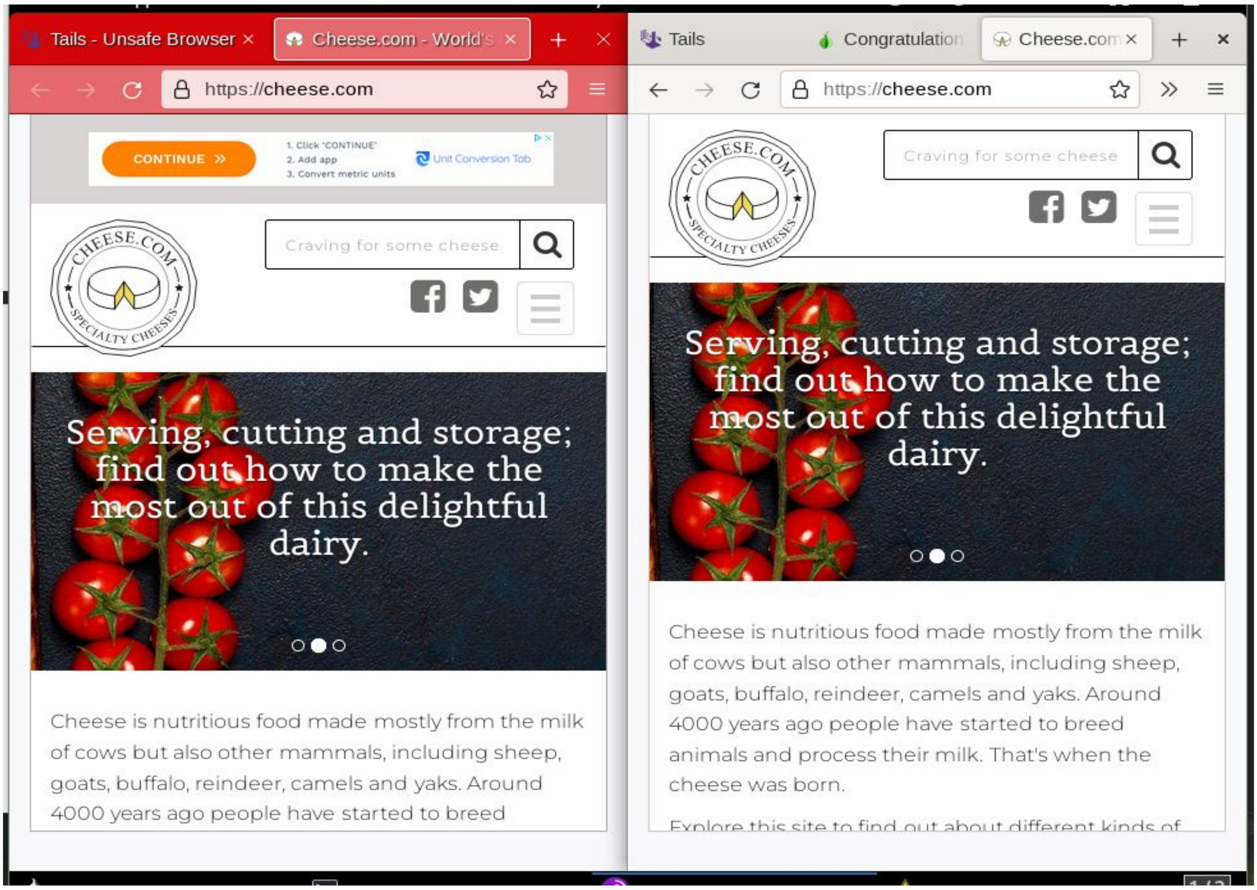
Chee
Cheese i
product p
in wide ra
and form
milk prote
proteins
productic
and eithe
or bacter
activity ar
casein to

Now start the unsafe browser. Do this by searching for it:

```
super key -> "unsafe"
```



Notice, if we enter "cheese.com" in both browsers, the unsafe browser contains an ad banner at the top of the page. No such banner exists in the Tor Browser.



Serving, cutting and storage; find out how to make the most out of this delightful dairy.

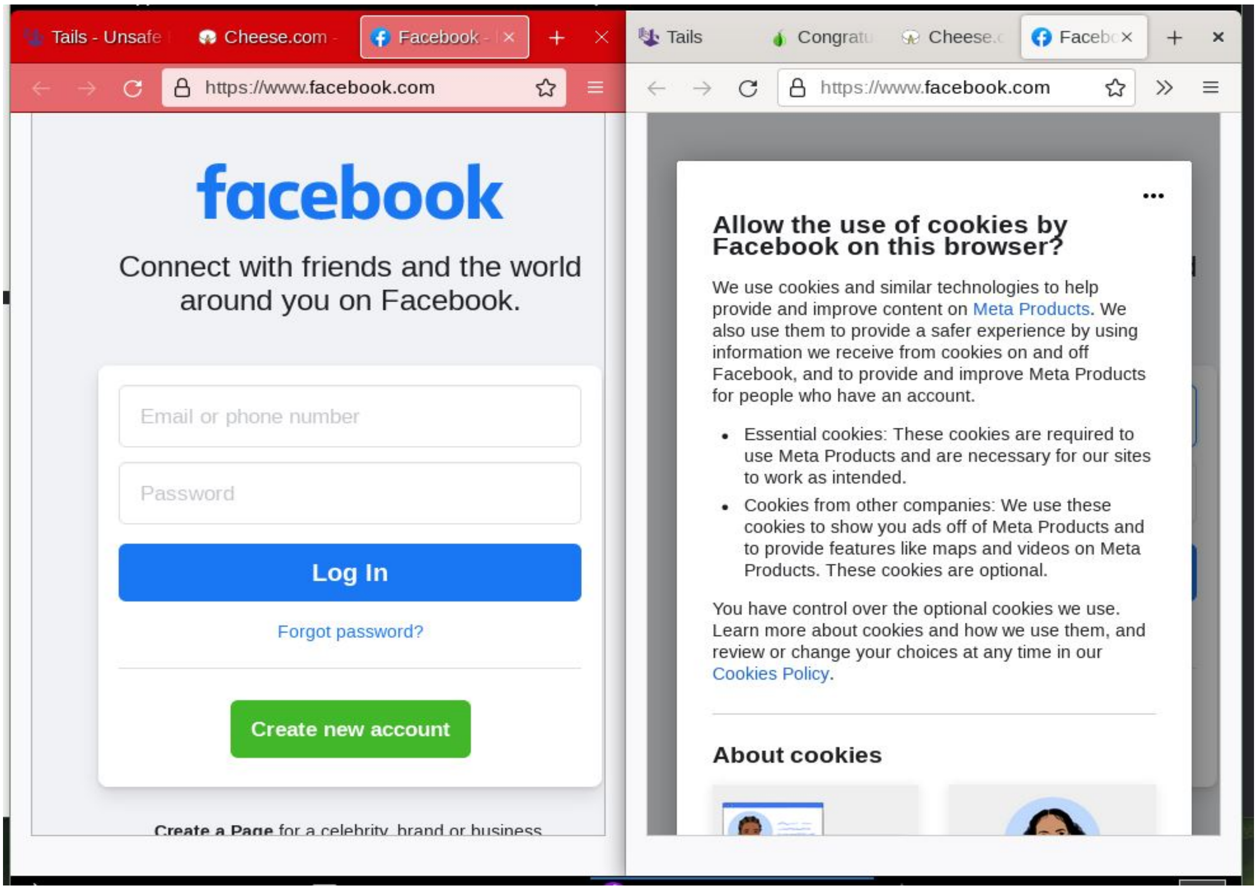
Cheese is nutritious food made mostly from the milk of cows but also other mammals, including sheep, goats, buffalo, reindeer, camels and yaks. Around 4000 years ago people have started to breed

Serving, cutting and storage; find out how to make the most out of this delightful dairy.

Cheese is nutritious food made mostly from the milk of cows but also other mammals, including sheep, goats, buffalo, reindeer, camels and yaks. Around 4000 years ago people have started to breed animals and process their milk. That's when the cheese was born.

Explore this site to find out about different kinds of

Try this with another site. I tried "facebook.com". This resulted in Tor issuing a popup window asking my about cookies for facebook.com, whereas the unsafe browser sent me straight to login.



Connect with friends and the world around you on Facebook.

Create a Page for a celebrity, brand or business.

Allow the use of cookies by Facebook on this browser?

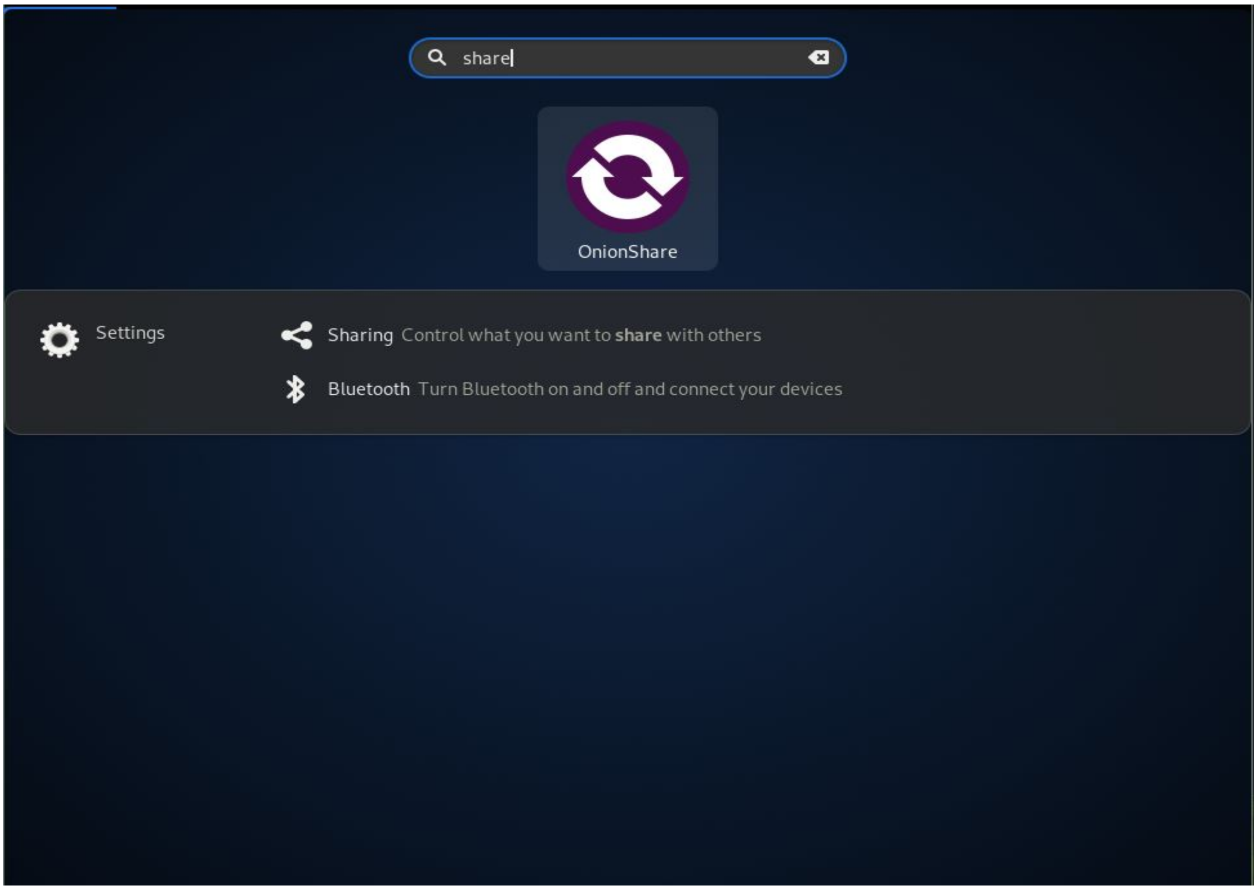
We use cookies and similar technologies to help provide and improve content on Meta Products. We also use them to provide a safer experience by using information we receive from cookies on and off Facebook, and to provide and improve Meta Products for people who have an account.

- Essential cookies: These cookies are required to use Meta Products and are necessary for our sites to work as intended.
- Cookies from other companies: We use these cookies to show you ads off of Meta Products and to provide features like maps and videos on Meta Products. These cookies are optional.

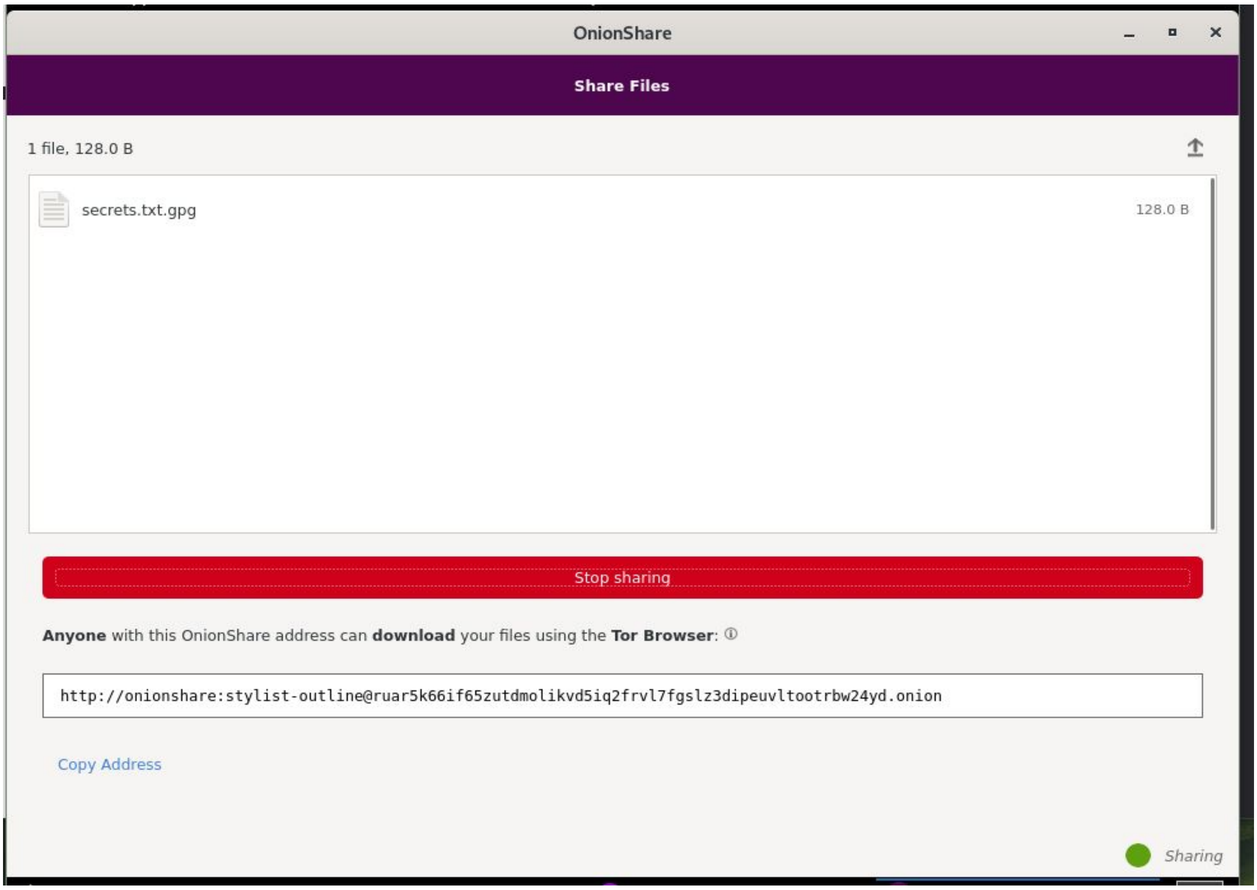
You have control over the optional cookies we use. Learn more about cookies and how we use them, and review or change your choices at any time in our Cookies Policy.

Now, let share the encrypted file over the "OnionShare" service.

```
super key -> "share"
```


share
OnionShare
Settings
Sharing Control what you want to share with others
Bluetooth Turn Bluetooth on and off and connect your devices

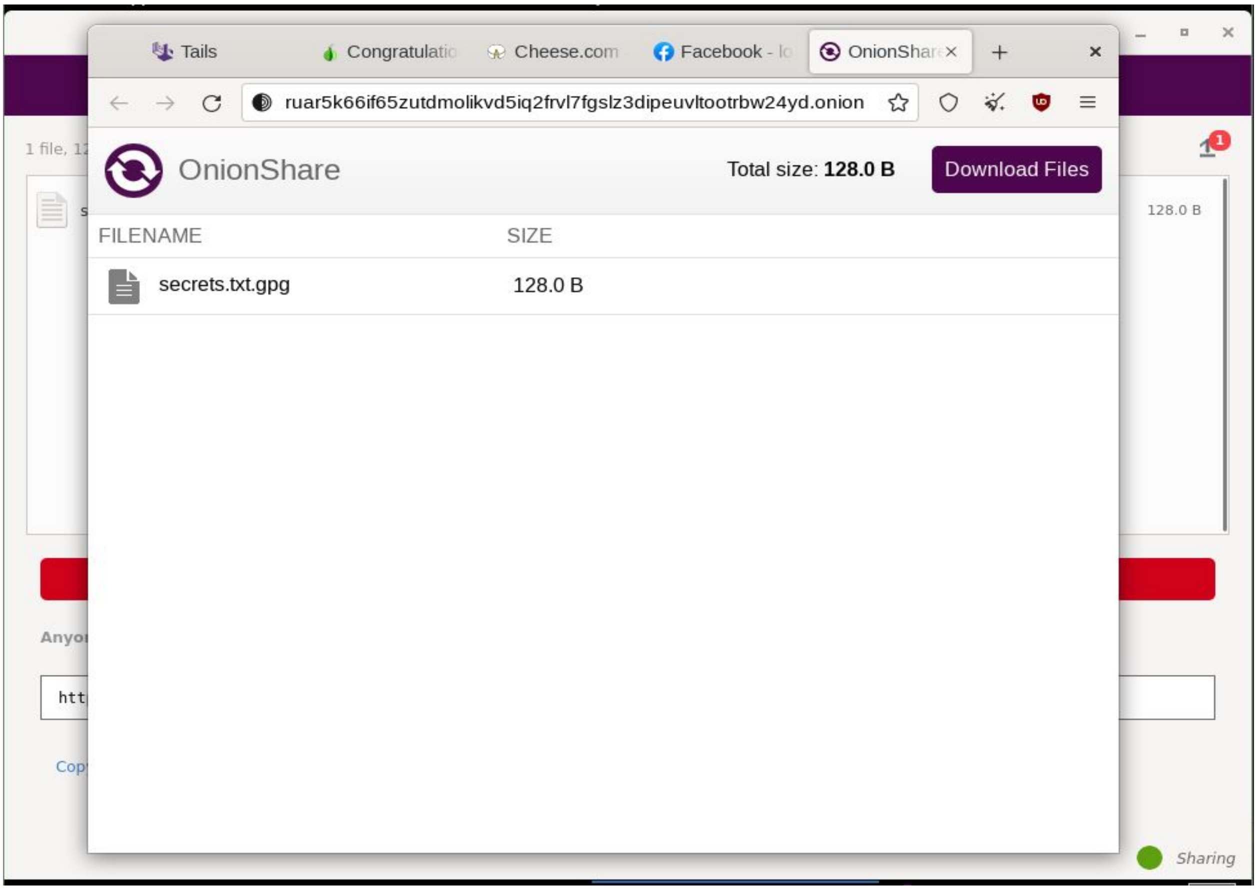
Within the OnionShare client, navigate to the 'Tor Browser' folder and select the encrypted text file to share. Begin the share.



Anyone with this OnionShare address can **download** your files using the **Tor Browser**:

```
http://onionshare:stylist-outline@ruar5k66if65zutdmolikvd5iq2frvl7fgslz3dipeuvltootrbw24yd.onion
```

This will generate a link. Copy this link and use it to access the OnionShare service from the Tor Browser.

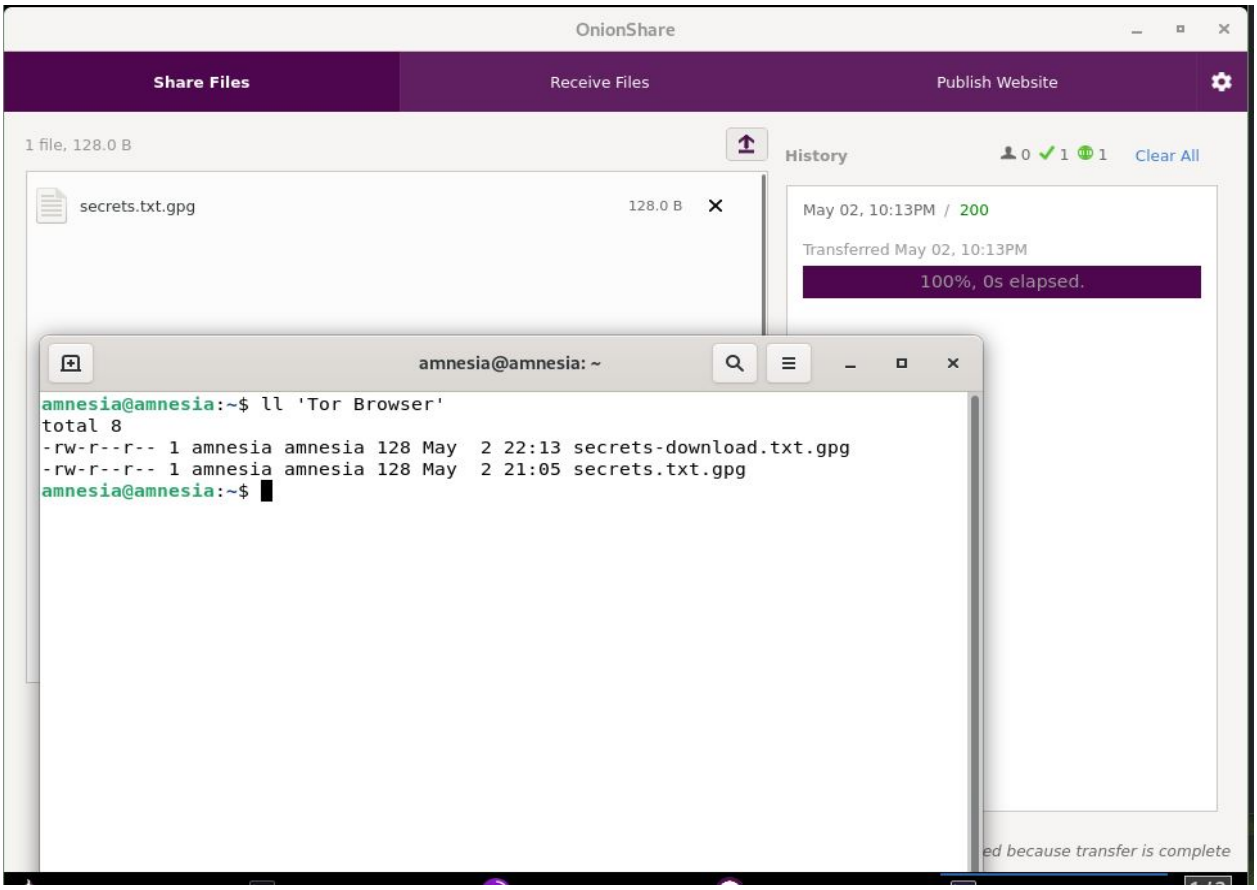


ruar5k66if65zutdmolikvd5iq2frvl7fgslz3dipeuvltootrbw24yd.onion

Total size: **128.0 B**

FILENAME	SIZE
secrets.txt.gpg	128.0 B

Inside the Share service, download the encrypted file. We will decrypt it later.



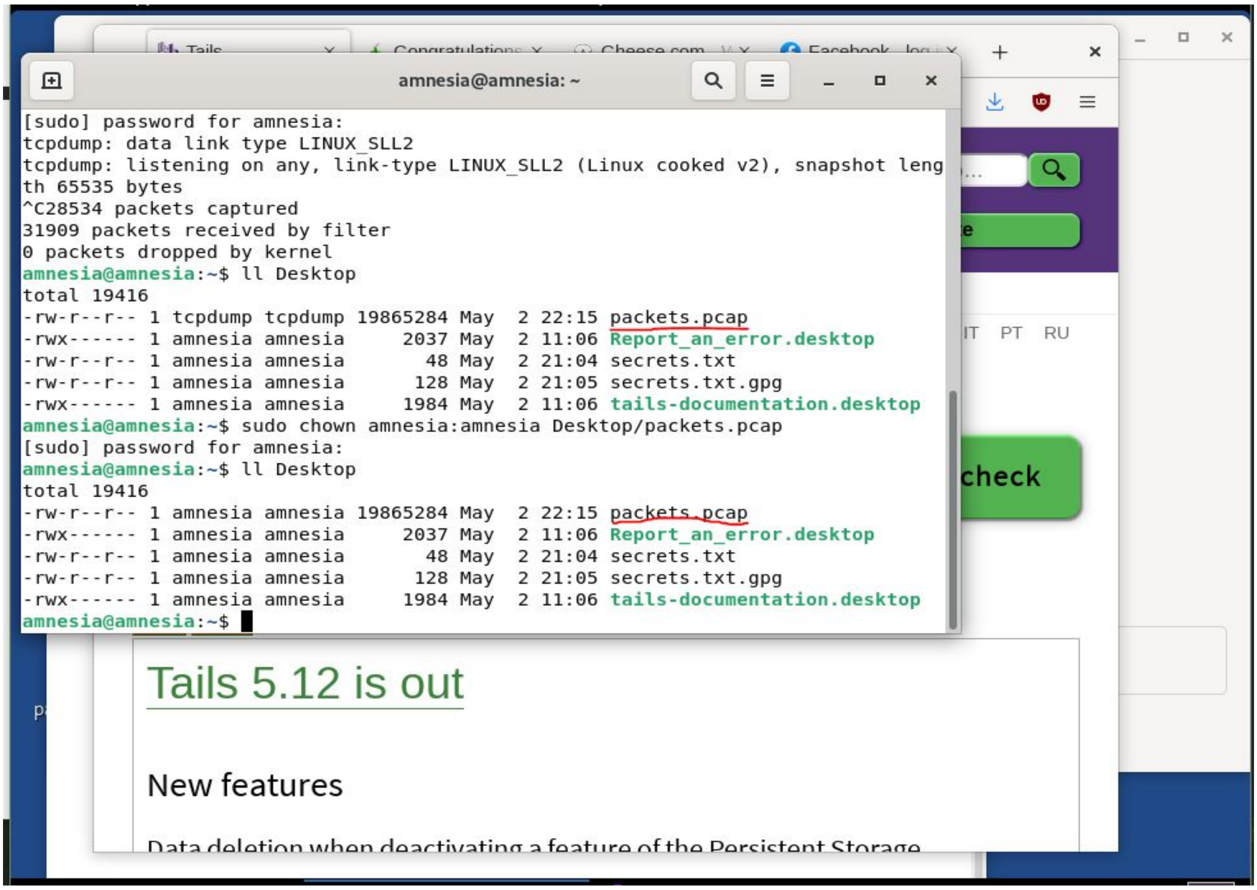
```
amnesia@amnesia:~$ ll 'Tor Browser'
total 8
-rw-r--r-- 1 amnesia amnesia 128 May  2 22:13 secrets-download.txt.gpg
-rw-r--r-- 1 amnesia amnesia 128 May  2 21:05 secrets.txt.gpg
amnesia@amnesia:~$ 
```

Stop the packet capture. You will need to change perimssions on the pcap file.

You will also need a way to copy it from Tails OS. I did this through google drive. When using an online service, ensure the file is located within the 'Tor Browser' folder so that web browser is able to access it.

Use Commands:

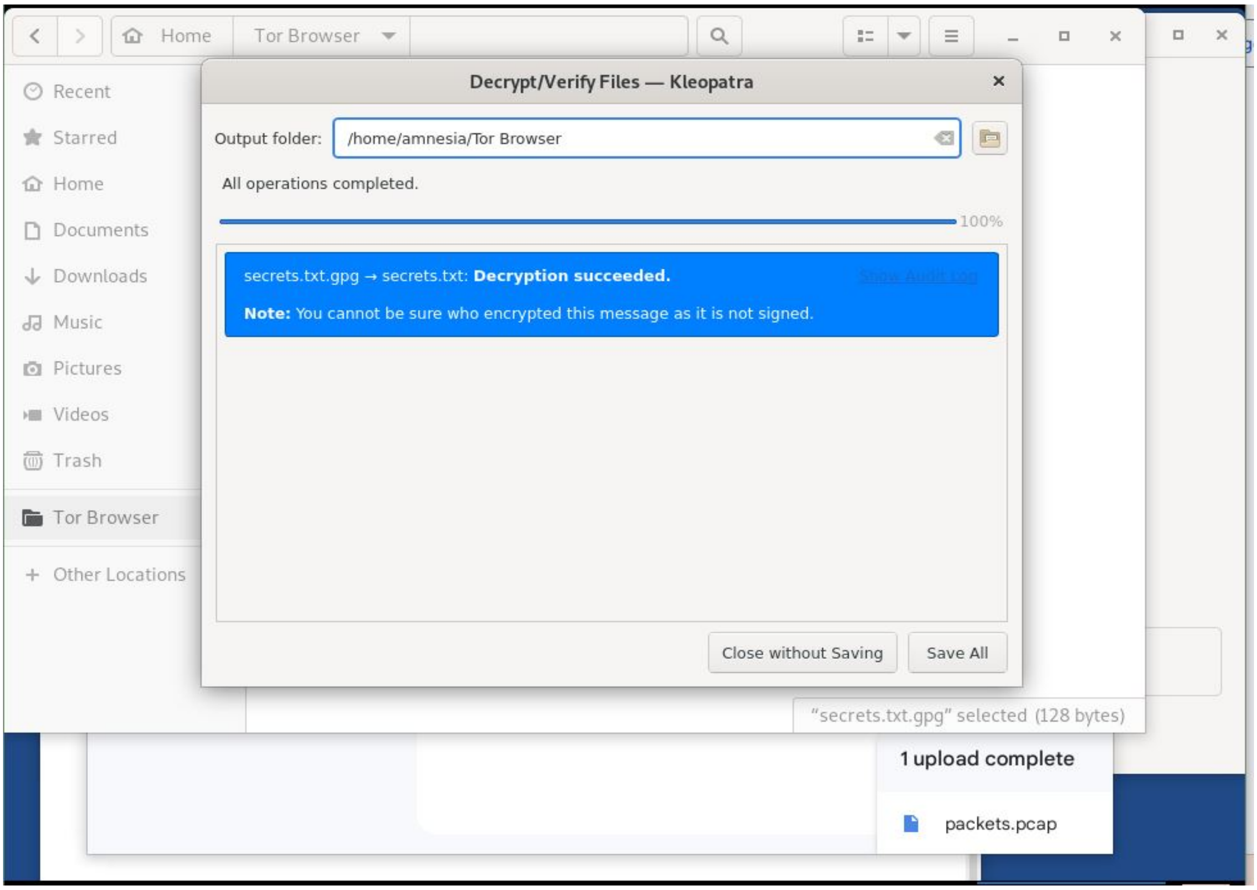
```
//change permissions on pcap file
sudo chown amnesia:amnesia Desktop/packets.pcap

// copy the pcap file to the Tor Browser for cloud upload
cp Desktop/packets.pcap 'Tor Browser'
```


amnesia@amnesia: ~
Tails 5.12 is out
New features
Data deletion when deactivating a feature of the Persistent Storage
check

```
[sudo] password for amnesia:
tcpdump: data link type LINUX_SLL2
tcpdump: listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot leng
th 65535 bytes
^C28534 packets captured
31909 packets received by filter
0 packets dropped by kernel
amnesia@amnesia:~$ ll Desktop
total 19416
-rw-r--r-- 1 tcpdump tcpdump 19865284 May  2 22:15 packets.pcap
-rwx------ 1 amnesia amnesia     2037 May  2 11:06 Report_an_error.desktop
-rw-r--r-- 1 amnesia amnesia       48 May  2 21:04 secrets.txt
-rw-r--r-- 1 amnesia amnesia      128 May  2 21:05 secrets.txt.gpg
-rwx------ 1 amnesia amnesia     1984 May  2 11:06 tails-documentation.desktop
amnesia@amnesia:~$ sudo chown amnesia:amnesia Desktop/packets.pcap
[sudo] password for amnesia:
amnesia@amnesia:~$ ll Desktop
total 19416
-rw-r--r-- 1 amnesia amnesia 19865284 May  2 22:15 packets.pcap
-rwx------ 1 amnesia amnesia     2037 May  2 11:06 Report_an_error.desktop
-rw-r--r-- 1 amnesia amnesia       48 May  2 21:04 secrets.txt
-rw-r--r-- 1 amnesia amnesia      128 May  2 21:05 secrets.txt.gpg
-rwx------ 1 amnesia amnesia     1984 May  2 11:06 tails-documentation.desktop
amnesia@amnesia:~$
```

D: Decryption

Within the 'Tor Browser' folder, locate the downloaded encrypted text file shared with OnionShare. Double click it to decrypt it.



Output folder: /home/amnesia/Tor Browser

All operations completed.

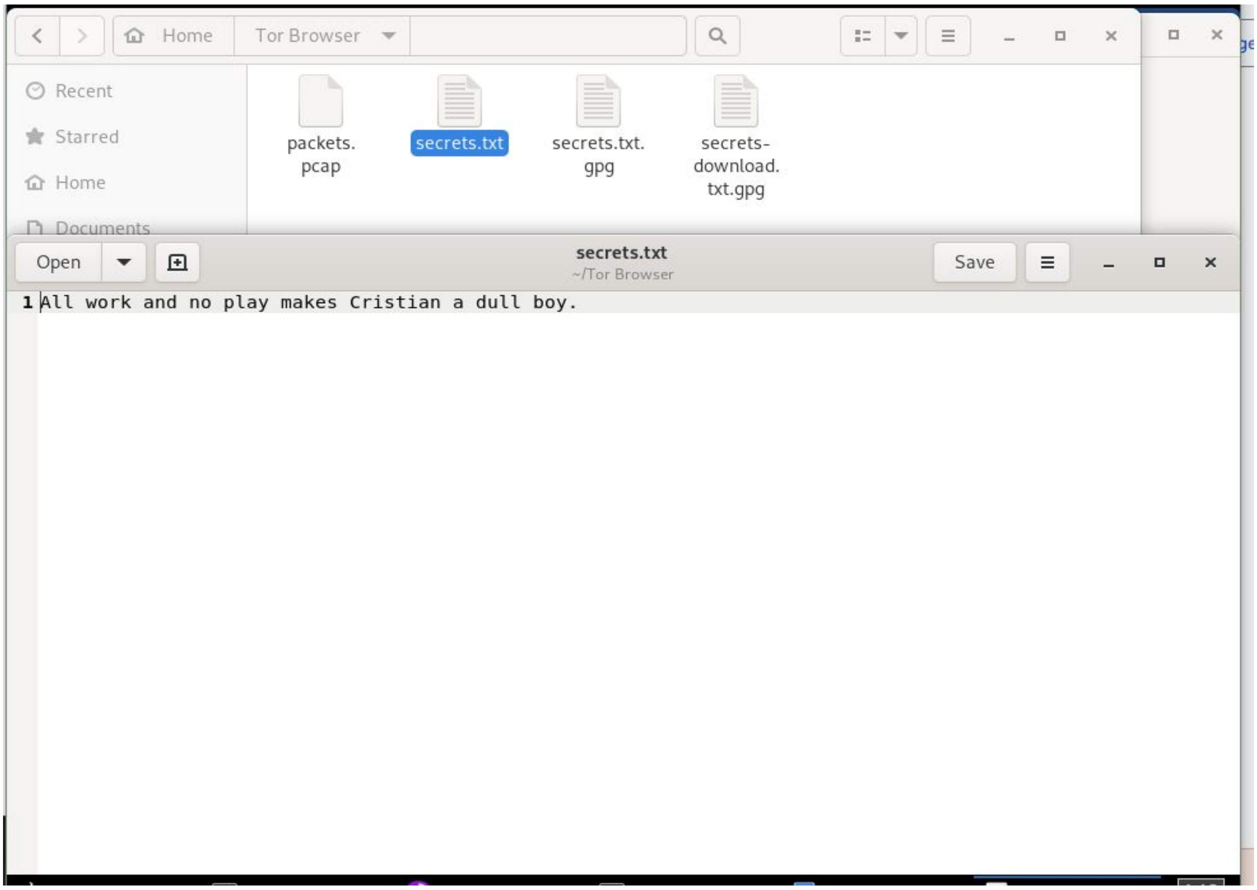
100%

secrets.txt.gpg → secrets.txt: **Decryption succeeded.**

Note: You cannot be sure who encrypted this message as it is not signed.

“secrets.txt.gpg” selected (128 bytes)

Enter in the password to view the message.



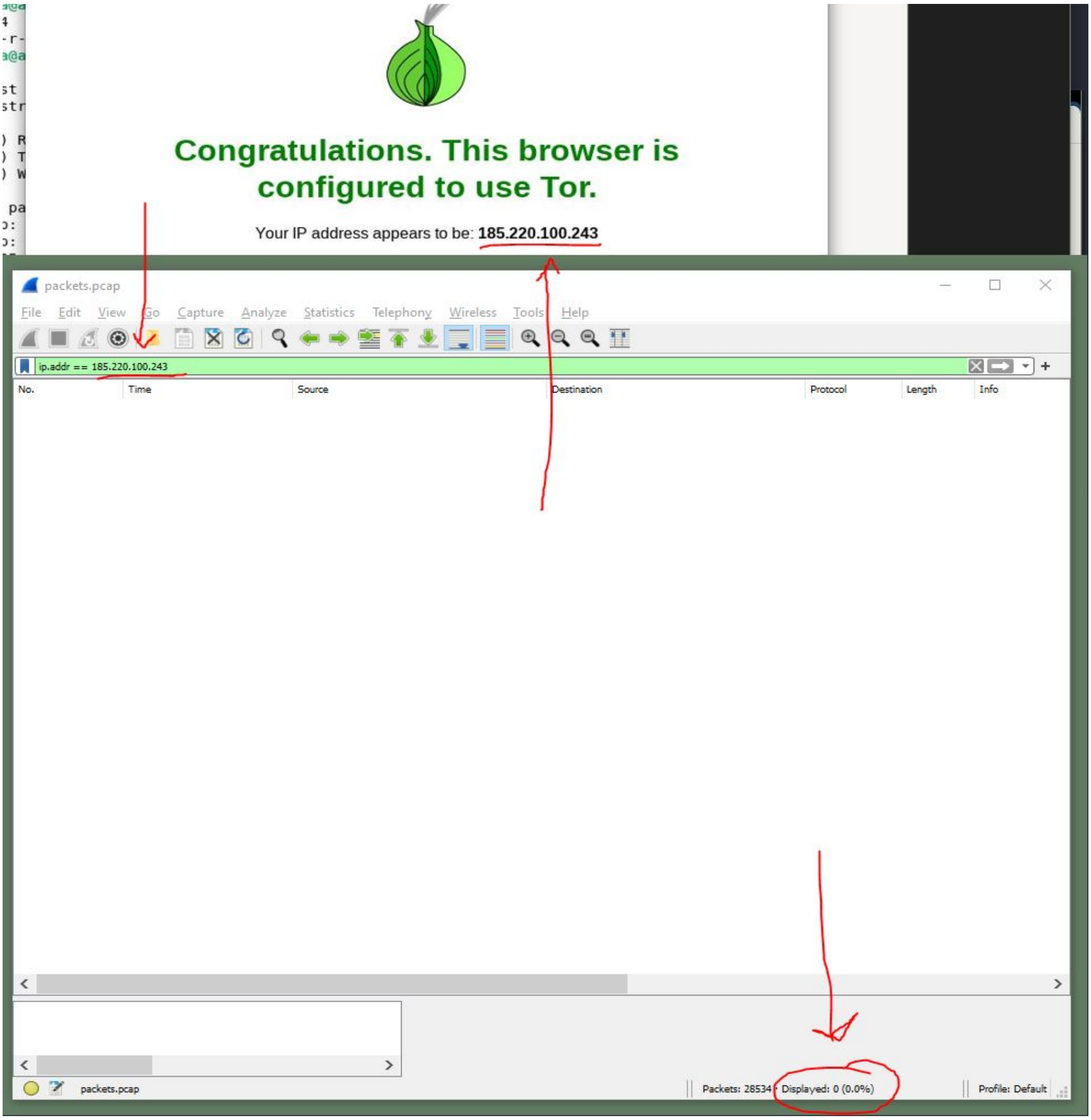
```
All work and no play makes Cristian a dull boy.
```

Analysis

Packets

Analysis for this assignment is conducted on the numerous packets that were captured when using the Tor Browser, the unsafe browser and OnionShare.

The first step would be to filter the packets for the IP address of our machine. Expectedly, this resulted in zero packets.



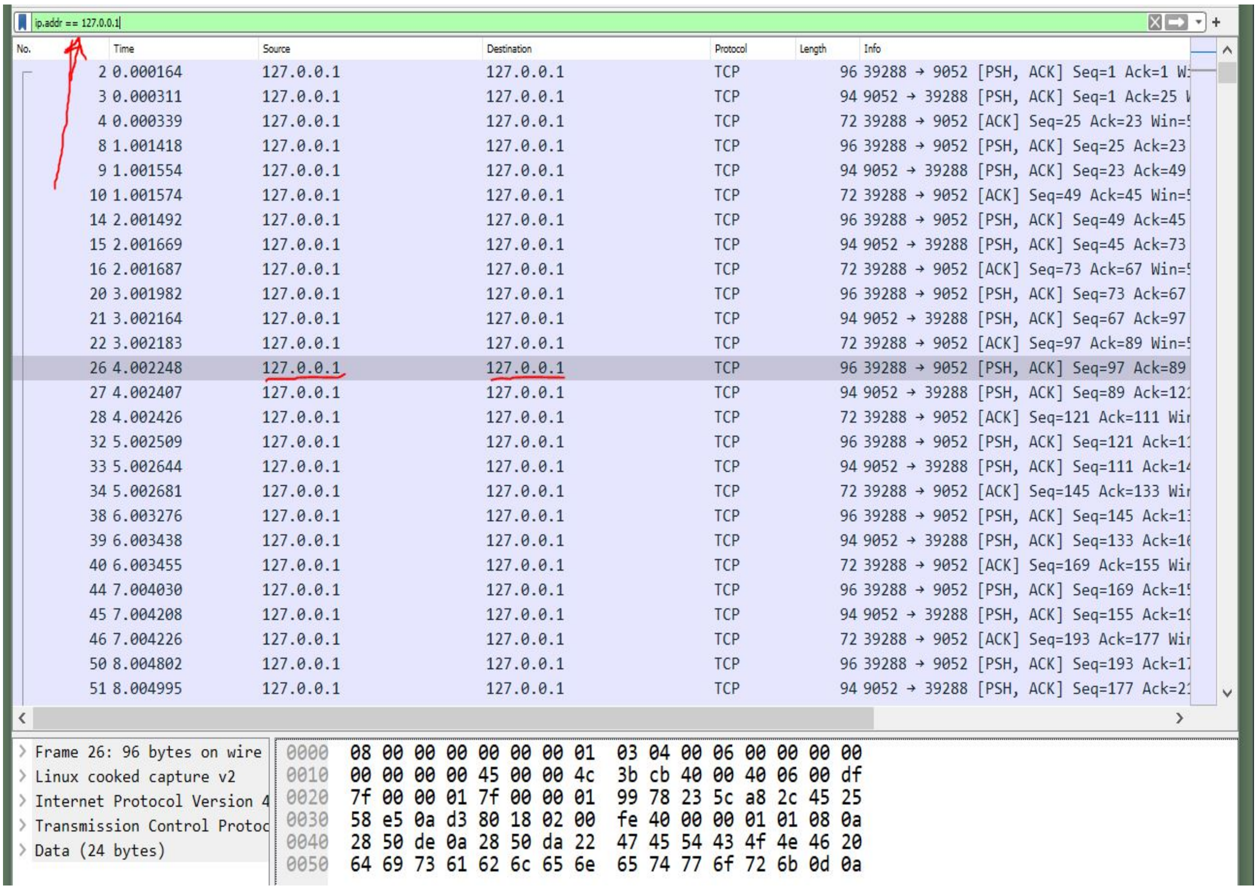
Congratulations. This browser is configured to use Tor.

Your IP address appears to be: 185.220.100.243

```
ip.addr == 185.220.100.243
```

Packets: 28534 · Displayed: 0 (0.0%)

This was expected. The IP address in the above screenshot is a "fake" address generated by the Tor network. This address is actually a pseudonym for the loopback address. Loopback addresses are used to provide intercommunicatons between the Tor client and the Tor proxy running on the same computer.



```
ip.addr == 127.0.0.1

No.  Time      Source      Destination  Protocol  Length  Info
 2 0.000164   127.0.0.1   127.0.0.1    TCP       96 39288 → 9052 [PSH, ACK] Seq=1 Ack=1 Wi
 3 0.000311   127.0.0.1   127.0.0.1    TCP       94 9052 → 39288 [PSH, ACK] Seq=1 Ack=25 W
 4 0.000339   127.0.0.1   127.0.0.1    TCP       72 39288 → 9052 [ACK] Seq=25 Ack=23 Win=
 8 1.001418   127.0.0.1   127.0.0.1    TCP       96 39288 → 9052 [PSH, ACK] Seq=25 Ack=23
 9 1.001554   127.0.0.1   127.0.0.1    TCP       94 9052 → 39288 [PSH, ACK] Seq=23 Ack=49
10 1.001574   127.0.0.1   127.0.0.1    TCP       72 39288 → 9052 [ACK] Seq=49 Ack=45 Win=
14 2.001492   127.0.0.1   127.0.0.1    TCP       96 39288 → 9052 [PSH, ACK] Seq=49 Ack=45
15 2.001669   127.0.0.1   127.0.0.1    TCP       94 9052 → 39288 [PSH, ACK] Seq=45 Ack=73
16 2.001687   127.0.0.1   127.0.0.1    TCP       72 39288 → 9052 [ACK] Seq=73 Ack=67 Win=
20 3.001982   127.0.0.1   127.0.0.1    TCP       96 39288 → 9052 [PSH, ACK] Seq=73 Ack=67
21 3.002164   127.0.0.1   127.0.0.1    TCP       94 9052 → 39288 [PSH, ACK] Seq=67 Ack=97
22 3.002183   127.0.0.1   127.0.0.1    TCP       72 39288 → 9052 [ACK] Seq=97 Ack=89 Win=
26 4.002248   127.0.0.1   127.0.0.1    TCP       96 39288 → 9052 [PSH, ACK] Seq=97 Ack=89
27 4.002407   127.0.0.1   127.0.0.1    TCP       94 9052 → 39288 [PSH, ACK] Seq=89 Ack=12
28 4.002426   127.0.0.1   127.0.0.1    TCP       72 39288 → 9052 [ACK] Seq=121 Ack=111 Win
32 5.002509   127.0.0.1   127.0.0.1    TCP       96 39288 → 9052 [PSH, ACK] Seq=121 Ack=1
33 5.002644   127.0.0.1   127.0.0.1    TCP       94 9052 → 39288 [PSH, ACK] Seq=111 Ack=14
34 5.002681   127.0.0.1   127.0.0.1    TCP       72 39288 → 9052 [ACK] Seq=145 Ack=133 Win
38 6.003276   127.0.0.1   127.0.0.1    TCP       96 39288 → 9052 [PSH, ACK] Seq=145 Ack=1
39 6.003438   127.0.0.1   127.0.0.1    TCP       94 9052 → 39288 [PSH, ACK] Seq=133 Ack=16
40 6.003455   127.0.0.1   127.0.0.1    TCP       72 39288 → 9052 [ACK] Seq=169 Ack=155 Win
44 7.004030   127.0.0.1   127.0.0.1    TCP       96 39288 → 9052 [PSH, ACK] Seq=169 Ack=15
45 7.004208   127.0.0.1   127.0.0.1    TCP       94 9052 → 39288 [PSH, ACK] Seq=155 Ack=19
46 7.004226   127.0.0.1   127.0.0.1    TCP       72 39288 → 9052 [ACK] Seq=193 Ack=177 Win
50 8.004802   127.0.0.1   127.0.0.1    TCP       96 39288 → 9052 [PSH, ACK] Seq=193 Ack=17
51 8.004995   127.0.0.1   127.0.0.1    TCP       94 9052 → 39288 [PSH, ACK] Seq=177 Ack=2

> Frame 26: 96 bytes on wire       0000  08 00 00 00 00 00 00 01  03 04 00 06 00 00 00 00
> Linux cooked capture v2          0010  00 00 00 00 45 00 00 4c  3b cb 40 00 40 06 00 df
> Internet Protocol Version 4      0020  7f 00 00 01 7f 00 00 01  99 78 23 5c a8 2c 45 25
> Transmission Control Protoc      0030  58 e5 0a d3 80 18 02 00  fe 40 00 00 01 01 08 0a
> Data (24 bytes)                  0040  28 50 de 0a 28 50 da 22  47 45 54 43 4f 4e 46 20
                                   0050  64 69 73 61 62 6c 65 6e  65 74 77 6f 72 6b 0d 0a
```

Tor Relays

Loopback addresses are also used during the tranmission on the Tor relay. When a Tor browser connects to the Tor network, a three layered relay is provided for communications. The components of the relay are:

1. Entry Node
2. Middle Node
3. Exit Node

Encryption is used to hide the ip addresses of every node in the relay. When packets are recieved by a node, each node must decrypt the address and encrypt the address before transmission (except in the Exit node that keeps the destination IP decrypted). This creates a large overhead on the Tor relays that are not present in normal web browsing.

This is something I noticed; the Tor browser was somewhat slower than normal web browsing. Factors that produce slower speeds with Tor than web rbowsing include:

- large encryption layers
- multiple hops in the relay
- unequal computational power amongst nodes
- geographical location of nodes

Exit nodes are those that have the direct connection with the service requested by the tranmission. For example, "cheese.com" would only have the IP address of the exit node and not of the other nodes in the relay nor the user computer. In this way, relays are the "layers" of the Onion Router and encryption provides the privacy.

Packet Expectations

Packet analysis could show some information about the traffic but would not explicitly show contents or identity. Kinds of information include:

1. IP addresses of exit node:

   Ip addresses are encrypted during the Tor relay. However, they are decrypted for the destination IP, leaving the exit node (last node in the relay) exposed to the requested service.

2. Protocol Information:

   The kinds of protocols within the packets are not encrypted. For example, we can see the majority of the packets collected are for the TCP protocol.

3. Traffic Patterns, Size and Timing:

   We can infer services based on the way traffic was recieved. For example, if Tor networks are used to provide a DDOS attack, we could infer that from the way packets are sized (like a maximum size to eat bandwidth) and there timings (alot of various packets spaced far enough apart to go undected.)

Tails's Unsafe Browser

The unsafe browser is a Tails OS built-in web browser that does not connect to a Tor Network to provide privacy through Onion Routing. Instead, the Unsafe Browser uses a regular standard connection between a client and a server. This browser is considered "unsafe" because it does not use the Tor network. This is helpful because a website might not be compatiable with Tor, so this would allow a user to visit such sites. However, these connections are not private so are subject to potential spying by ISPs, Admins, attackers, etc.

First thing to note about the Unsafe Browser is that there is no search engine. Websites must be entered in manually (DNS). I think the reason for this is to provide some level privacy without using the Tor network. Search engines tend to collect data on activity for any number of possible reasons. Someone who has gone the effort to use Tails OS, who is then forced to use Unsafe Browser would still like to get some privacy, otherwise whats the point.

Tails OS Permant Storage

Privacy is the main concern for Tails and Tor users. These services are meant to provide privacy even at the cost of typical user experiences, such as persistant storage. In this way, permamnt storage is seen as inherently un-private. Cold storage of data is typically always at risk of undisclosed access, especially if it sits unencrypted. Removing persistant storage as a base feature in Tails means that Tails leaves no trace on the computer that runs it. Especailly since Tails is designed to be run off a live USB drive.

Conclusion

In this assignment, we used Tails OS to browse the web through the Tor Browser connected to the Tor network. Tails Os was installed in VM without persistant storage. "tcpdump" was used to capture traffic during the Tor browser session. Wireshark was used to analyze the packets.

Packet analysis of the traffic generated by the Tor browser reavealed very little about the kinds of content that was being transmitted as well as how IP addresses are hidden across the relay nodes. It showed how Tor connections rely on loopback addresses within Tor relay nodes to communicate between the clients and proxies. Overall, traffic generateed with Tor is hard to analyze. It would require extensive research and probing to determine what kinds of content is being transmitted across a Tor network.

Tor with Tails is better and Tor without Tails. Firsdtly, Tails provides a preconfigured Tor browser that needs no tinkering to provide full privacy. Tails also ships with various Tor clients including Onionshare. More so, Tails has many built in privacy gurads that work with Tor to provide the user confidentiality such as non-persistant storage.

Before describing how each tool used in this assignment provides or does not provide the X.800 Secuirty Services, lets take a brief moment to define them.

1. *Authentication*: ensures that all parties involved in a data access or connection are who they say they are.
2. *Access Control*: the ability to limit and control access to system resouces through secuirty policies and mechanisms.
3. *Data Confidentiality*: prevents unauthorized data acess.
4. *Data-Integrity*: provides assurance that total data streams remain unchanged by unauthorized entities.
5. *Non-repuditation*: protects against denial of involvement within a connection.

TAILS OS : Access Control, Data Confidentiality

Tails OS provides a user with tight privacy and anonymity through encryption and non-persistant storage. In this way, Tails provides the security services of Access Control and Data Confidentilaity.

Tails provides ***Access Control*** through the use of firewalls. While this is not the tightest of access control, firewalls do serve as a network filter which can protect against data access. I would also say that Tails built-in non-persistant storage is a form access control in that data that is not stored has no potential for illegal access.

Tails provides ***Data Confidentiality*** through the use of a heavy encryption layer of all traffic generated with a Tor browser. Tails also provides an "unsafe browser" that does not have a built in search engine, which would otherwise collect data on a users searches.

TOR ONION BROWSER : Access Control, Data Confidentiality

Tor Browser provides a user with a large encryption layer over traffic. Tor Browser also uses a Tor relay generated from a Tor network that provides the user several layers of separation from them and the service they are requesting from. Tor browser uses various loopback address of the various nodes on the relay to communicate between clients and proxies. In this way, Tor provides Data Confidentiality as well as Access Control.

Tor Provides ***Access Control*** through the use of proxies that can be configured to connect to the next node in the relay. As we saw in our packet analysis, a proxy was using the loopback address to communicate with the entry node of the relay.

Tor provides ***Data Confidentaility*** through the use of an encryption layer that is provided by the Tor network. At each stage of the relay, IP addresses are decrypted and encrypted to ensure that nodes can only talk with each other and not with the start or end points. In this way, a user is anonymous during the transmission.