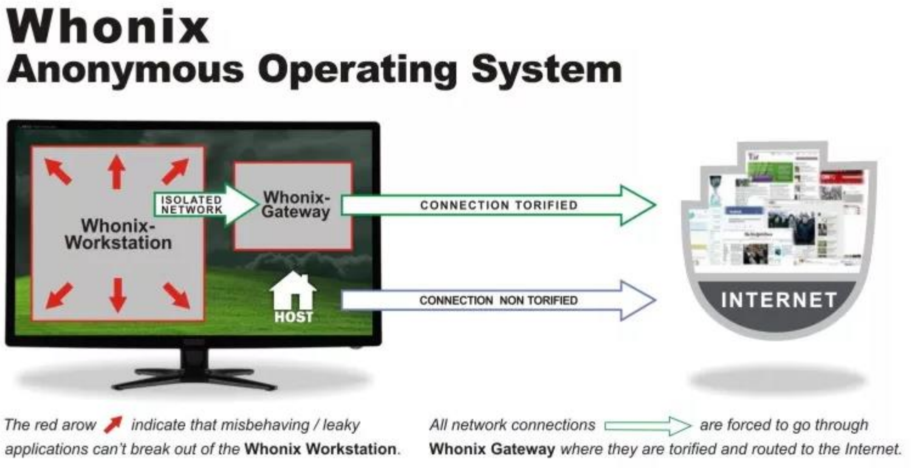
Lab – Anonymize Kali Using Whonix

Overview

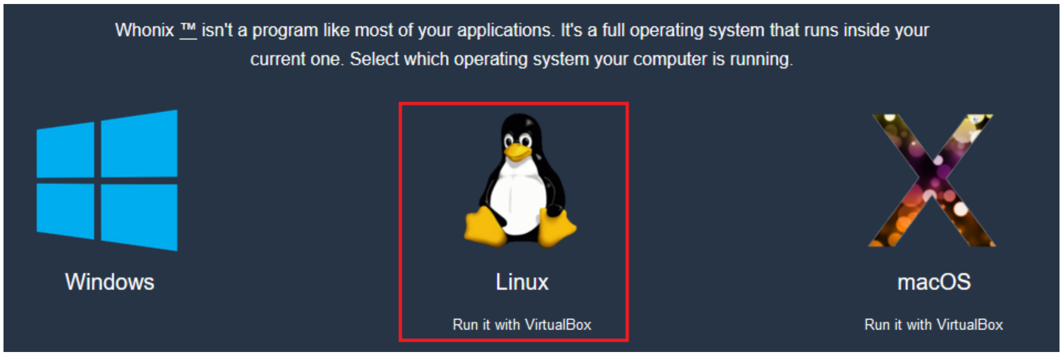
In this lab, you will learn how to remain fully anonymous using the Whonix Gateway while Kali Linux on the Internet. Running Kali Linux as a virtual machine can be an ideal hacking platform for launching attacks, but Kali is only as anonymous as the connection it uses.

Tor is an effective traffic obfuscation network, and while the Tor Browser alone cannot support a hacker's behavior, when combined with Whonix, Kali traffic is wholly anonymized and safe from a Man-In-The-Middle Attack.


Whonix
Anonymous Operating System
ISOLATED NETWORK
Whonix-Gateway
Whonix-Workstation
HOST
CONNECTION TORIFIED
CONNECTION NON TORIFIED
INTERNET
The red arow indicate that misbehaving / leaky applications can't break out of the Whonix Workstation.
All network connections are forced to go through Whonix Gateway where they are torified and routed to the Internet.

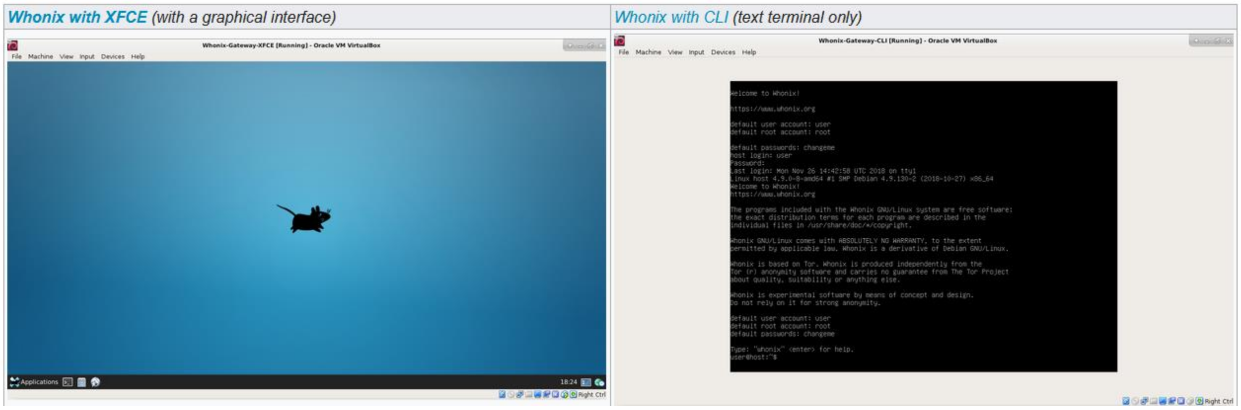
Begin the Lab!

We first need to download the OVA file for Whoinx. The download for the Whonix can be downloaded using the following link Download Whonix or by pointing your browser to https://www.whonix.org/



Whonix ™ isn't a program like most of your applications. It's a full operating system that runs inside your current one. Select which operating system your computer is running.

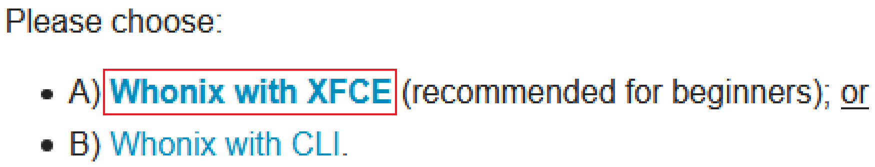
Whonix downloads as an OVA file. Once the importation of the OVA into VirtualBox is complete, you will have two virtual machines.


Whonix-Gateway-XFCE [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications
18:24
Right Ctrl
Whonix-Gateway-CLI [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

Whonix with XFCE (*with a graphical interface*)

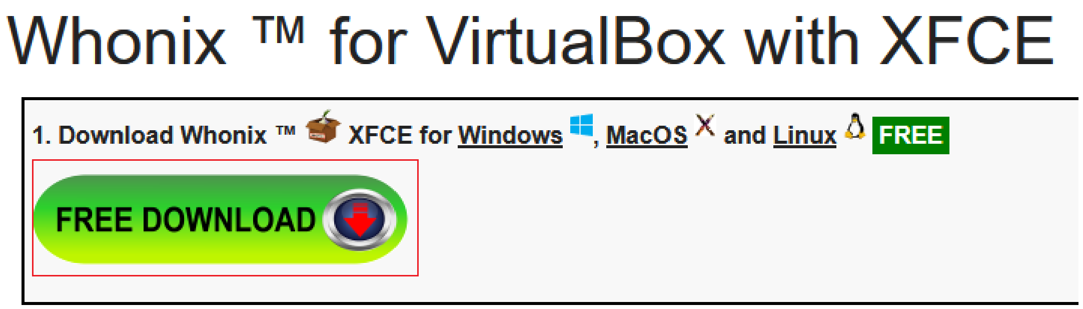
Whonix with CLI (*text terminal only*)

```
Welcome to Whonix!

https://www.whonix.org

default user account: user
default root account: root

default passwords: changeme
host login: user
Password:
Last login: Mon Nov 26 14:42:58 UTC 2018 on tty1
Linux host 4.9.0-8-amd64 #1 SMP Debian 4.9.130-2 (2018-10-27) x86_64
Welcome to Whonix!
https://www.whonix.org

The programs included with the Whonix GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Whonix GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law. Whonix is a derivative of Debian GNU/Linux.

Whonix is based on Tor. Whonix is produced independently from the
Tor (r) anonymity software and carries no guarantee from The Tor Project
about quality, suitability or anything else.

Whonix is experimental software by means of concept and design.
Do not rely on it for strong anonymity.

default user account: user
default root account: root
default passwords: changeme

Type: "whonix" <enter> for help.
user@host:~$
```



Please choose:

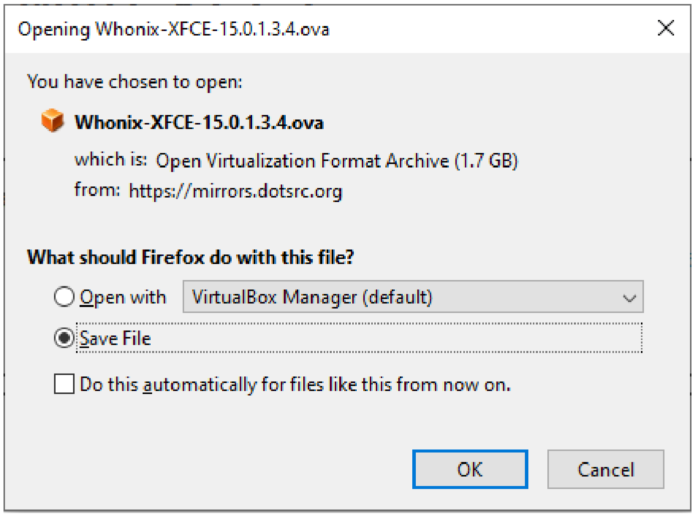
- A) Whonix with XFCE (recommended for beginners); or
- B) Whonix with CLI.



Whonix ™ for VirtualBox with XFCE

1. Download Whonix ™ XFCE for Windows, MacOS and Linux FREE

Save the OVA to a location on your local machine. Remember where you saved it.



Opening Whonix-XFCE-15.0.1.3.4.ova

You have chosen to open:

Whonix-XFCE-15.0.1.3.4.ova

which is: Open Virtualization Format Archive (1.7 GB)
from: https://mirrors.dotsrc.org

What should Firefox do with this file?

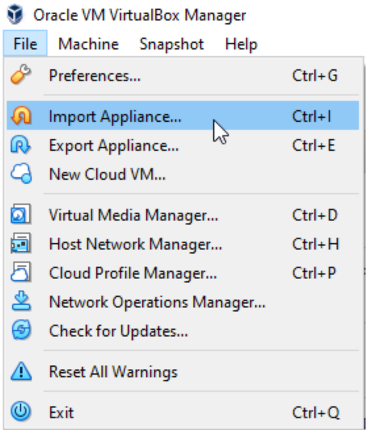
○ Open with VirtualBox Manager (default)

● Save File

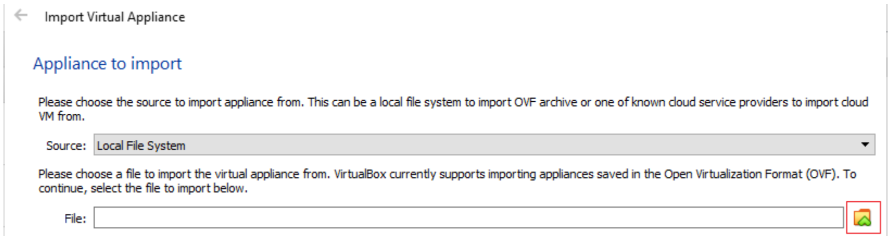
☐ Do this automatically for files like this from now on.

For this lab, we will use the VirtualBox Management console to import and create our two virtual machines.

Inside of VirtualBox, click on File, and from the context menu, select Import appliance.


Oracle VM VirtualBox Manager
File
Machine
Snapshot
Help
Preferences... Ctrl+G
Import Appliance... Ctrl+I
Export Appliance... Ctrl+E
New Cloud VM...
Virtual Media Manager... Ctrl+D
Host Network Manager... Ctrl+H
Cloud Profile Manager... Ctrl+P
Network Operations Manager...
Check for Updates...
Reset All Warnings
Exit Ctrl+Q

On the first page of the import wizard, use the browse option to find your OVA file and x2 click to import the appliance. Click next.



Import Virtual Appliance

Appliance to import

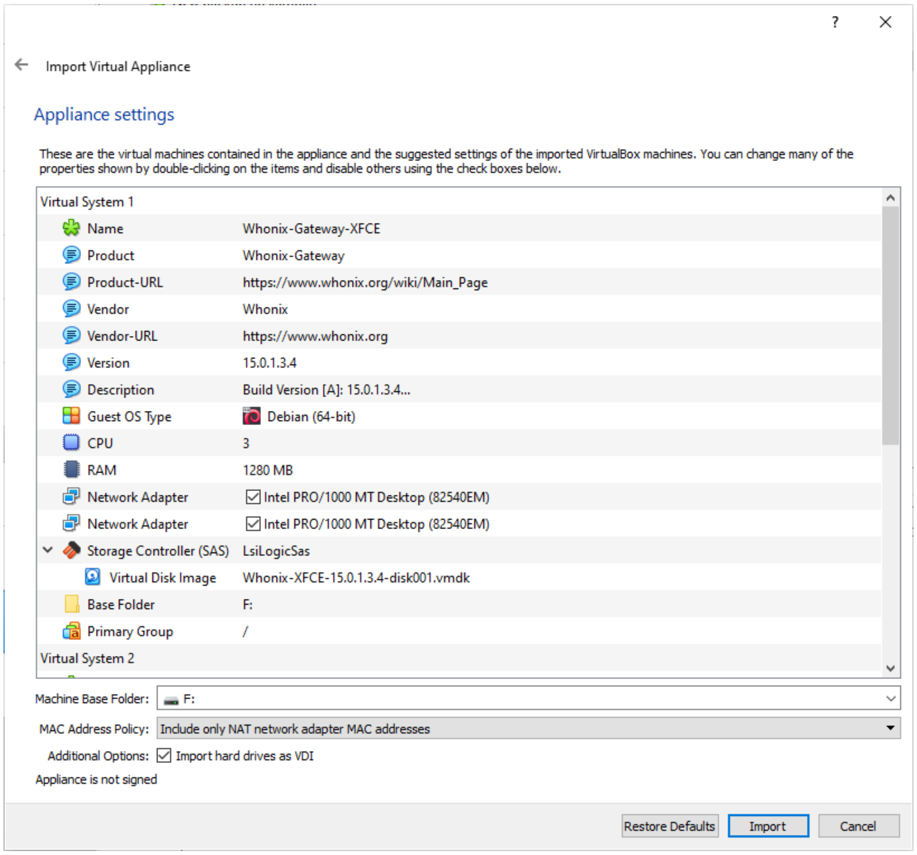
Please choose the source to import appliance from. This can be a local file system to import OVF archive or one of known cloud service providers to import cloud VM from.

Source: Local File System

Please choose a file to import the virtual appliance from. VirtualBox currently supports importing appliances saved in the Open Virtualization Format (OVF). To continue, select the file to import below.

File:

On the next page, accept the defaults and click install.



Import Virtual Appliance

Appliance settings

These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.

Virtual System 1	
Name	Whonix-Gateway-XFCE
Product	Whonix-Gateway
Product-URL	https://www.whonix.org/wiki/Main_Page
Vendor	Whonix
Vendor-URL	https://www.whonix.org
Version	15.0.1.3.4
Description	Build Version [A]: 15.0.1.3.4...
Guest OS Type	Debian (64-bit)
CPU	3
RAM	1280 MB
Network Adapter	☑ Intel PRO/1000 MT Desktop (82540EM)
Network Adapter	☑ Intel PRO/1000 MT Desktop (82540EM)
Storage Controller (SAS)	LsiLogicSas
Virtual Disk Image	Whonix-XFCE-15.0.1.3.4-disk001.vmdk
Base Folder	F:
Primary Group	/
Virtual System 2	

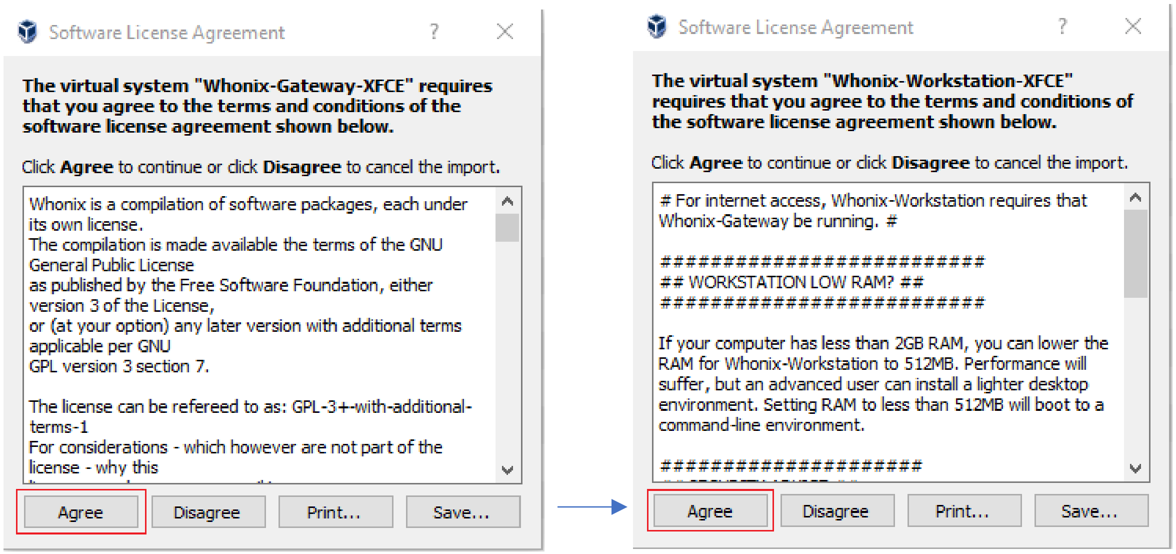
Machine Base Folder: F:

MAC Address Policy: Include only NAT network adapter MAC addresses

Additional Options: ☑ Import hard drives as VDI

Appliance is not signed

Agree to the license agreement.



The virtual system "Whonix-Gateway-XFCE" requires that you agree to the terms and conditions of the software license agreement shown below.

Click **Agree** to continue or click **Disagree** to cancel the import.

Whonix is a compilation of software packages, each under its own license.
The compilation is made available the terms of the GNU General Public License
as published by the Free Software Foundation, either version 3 of the License,
or (at your option) any later version with additional terms applicable per GNU
GPL version 3 section 7.

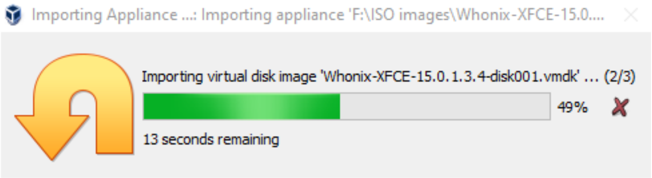
The license can be refereed to as: GPL-3+-with-additional-terms-1
For considerations - which however are not part of the license - why this

The virtual system "Whonix-Workstation-XFCE" requires that you agree to the terms and conditions of the software license agreement shown below.

Click **Agree** to continue or click **Disagree** to cancel the import.

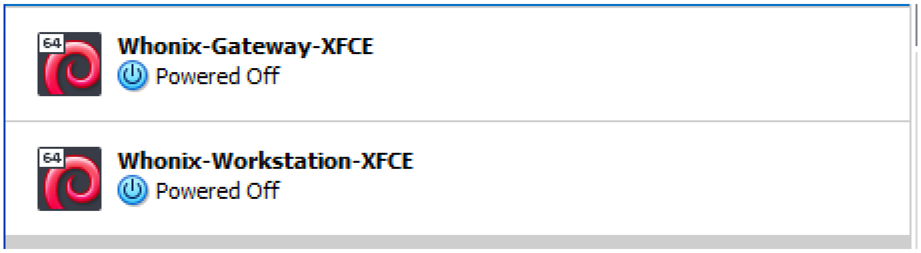
```
# For internet access, Whonix-Workstation requires that Whonix-Gateway be running. #

##########################
## WORKSTATION LOW RAM? ##
##########################

If your computer has less than 2GB RAM, you can lower the RAM for Whonix-Workstation to 512MB. Performance will suffer, but an advanced user can install a lighter desktop environment. Setting RAM to less than 512MB will boot to a command-line environment.

#####################
```

The OVA file begins with the import process.


Importing Appliance ...: Importing appliance 'F:\ISO images\Whonix-XFCE-15.0....

Importing virtual disk image 'Whonix-XFCE-15.0.1.3.4-disk001.vmdk' ... (2/3)
49%
13 seconds remaining

Once the install is complete, you will have two virtual machines installed. One is the Whonix Gateway, and the other is the Whonix workstation.

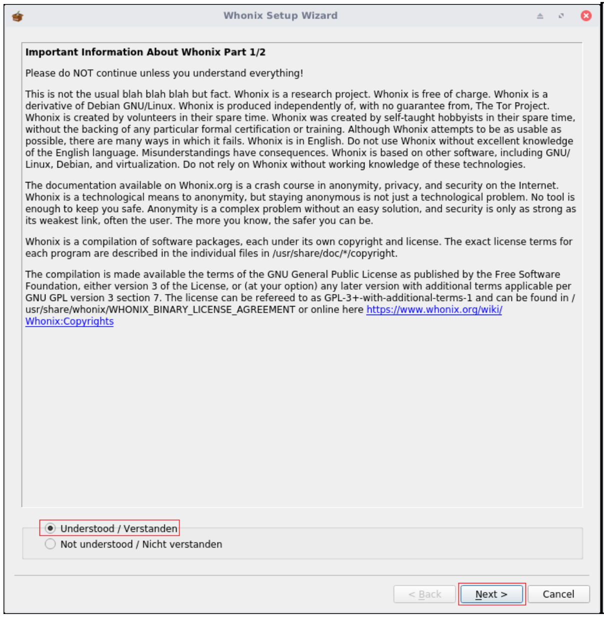


Whonix-Gateway-XFCE
Powered Off

Whonix-Workstation-XFCE
Powered Off

Launch the Whonix Gateway

Launch the Whonix Gateway. When you first access the Gateway, you will be greeted with some information you will need to acknowledge.



Important Information About Whonix Part 1/2

Please do NOT continue unless you understand everything!

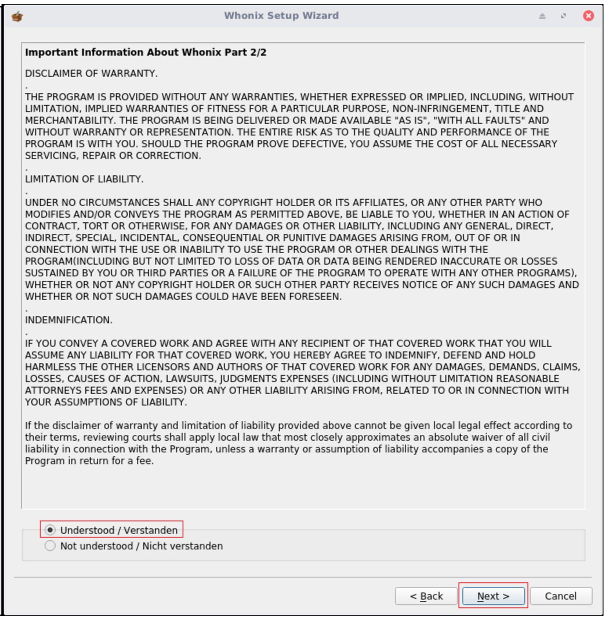
This is not the usual blah blah blah but fact. Whonix is a research project. Whonix is free of charge. Whonix is a derivative of Debian GNU/Linux. Whonix is produced independently of, with no guarantee from, The Tor Project. Whonix is created by volunteers in their spare time. Whonix was created by self-taught hobbyists in their spare time, without the backing of any particular formal certification or training. Although Whonix attempts to be as usable as possible, there are many ways in which it fails. Whonix is in English. Do not use Whonix without excellent knowledge of the English language. Misunderstandings have consequences. Whonix is based on other software, including GNU/Linux, Debian, and virtualization. Do not rely on Whonix without working knowledge of these technologies.

The documentation available on Whonix.org is a crash course in anonymity, privacy, and security on the Internet. Whonix is a technological means to anonymity, but staying anonymous is not just a technological problem. No tool is enough to keep you safe. Anonymity is a complex problem without an easy solution, and security is only as strong as its weakest link, often the user. The more you know, the safer you can be.

Whonix is a compilation of software packages, each under its own copyright and license. The exact license terms for each program are described in the individual files in /usr/share/doc/*/copyright.

The compilation is made available the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version with additional terms applicable per GNU GPL version 3 section 7. The license can be refereed to as GPL-3+-with-additional-terms-1 and can be found in /usr/share/whonix/WHONIX_BINARY_LICENSE_AGREEMENT or online here https://www.whonix.org/wiki/Whonix:Copyrights

● Understood / Verstanden
○ Not understood / Nicht verstanden



Important Information About Whonix Part 2/2

DISCLAIMER OF WARRANTY.

.

THE PROGRAM IS PROVIDED WITHOUT ANY WARRANTIES, WHETHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, TITLE AND MERCHANTABILITY. THE PROGRAM IS BEING DELIVERED OR MADE AVAILABLE "AS IS", "WITH ALL FAULTS" AND WITHOUT WARRANTY OR REPRESENTATION. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

.

LIMITATION OF LIABILITY.

.

UNDER NO CIRCUMSTANCES SHALL ANY COPYRIGHT HOLDER OR ITS AFFILIATES, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, FOR ANY DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL, DIRECT, INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL OR PUNITIVE DAMAGES ARISING FROM, OUT OF OR IN CONNECTION WITH THE USE OR INABILITY TO USE THE PROGRAM OR OTHER DEALINGS WITH THE PROGRAM(INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), WHETHER OR NOT ANY COPYRIGHT HOLDER OR SUCH OTHER PARTY RECEIVES NOTICE OF ANY SUCH DAMAGES AND WHETHER OR NOT SUCH DAMAGES COULD HAVE BEEN FORESEEN.

.

INDEMNIFICATION.

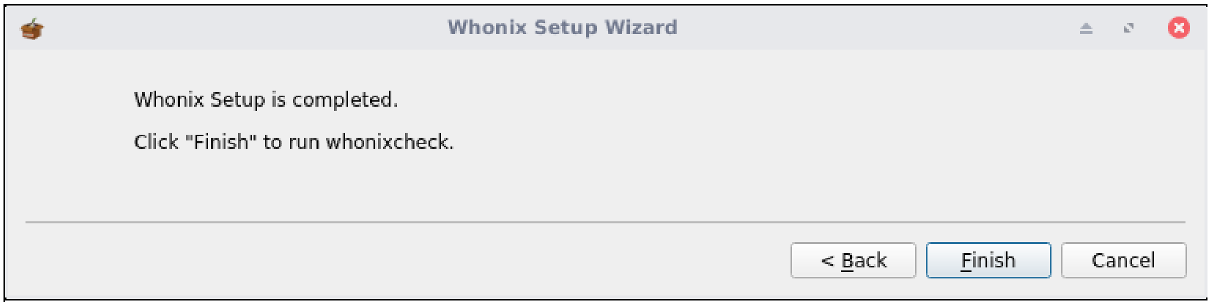
.

IF YOU CONVEY A COVERED WORK AND AGREE WITH ANY RECIPIENT OF THAT COVERED WORK THAT YOU WILL ASSUME ANY LIABILITY FOR THAT COVERED WORK, YOU HEREBY AGREE TO INDEMNIFY, DEFEND AND HOLD HARMLESS THE OTHER LICENSORS AND AUTHORS OF THAT COVERED WORK FOR ANY DAMAGES, DEMANDS, CLAIMS, LOSSES, CAUSES OF ACTION, LAWSUITS, JUDGMENTS EXPENSES (INCLUDING WITHOUT LIMITATION REASONABLE ATTORNEYS FEES AND EXPENSES) OR ANY OTHER LIABILITY ARISING FROM, RELATED TO OR IN CONNECTION WITH YOUR ASSUMPTIONS OF LIABILITY.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

● Understood / Verstanden
○ Not understood / Nicht verstanden

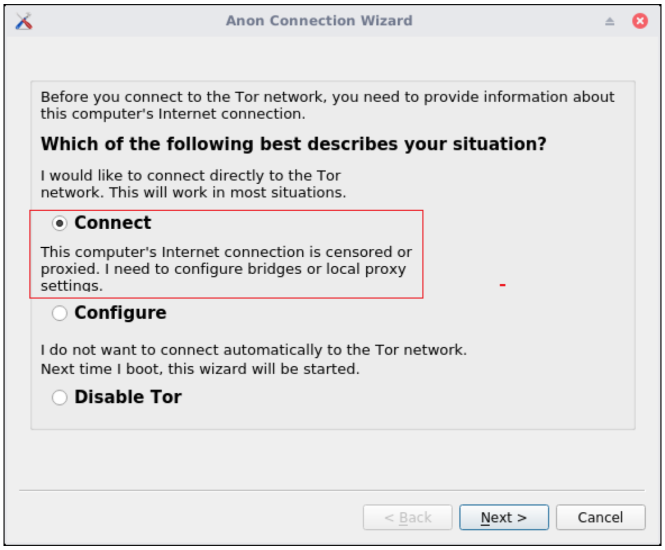
You will have to agree that you understand one more time, and finally, on the last page, you can click finish.



Whonix Setup is completed.

Click "Finish" to run whonixcheck.

On the next screen, you can tell Whonix how you want the Gateway configured. Accept the default setting.



Before you connect to the Tor network, you need to provide information about this computer's Internet connection.

Which of the following best describes your situation?

I would like to connect directly to the Tor network. This will work in most situations.

● **Connect**

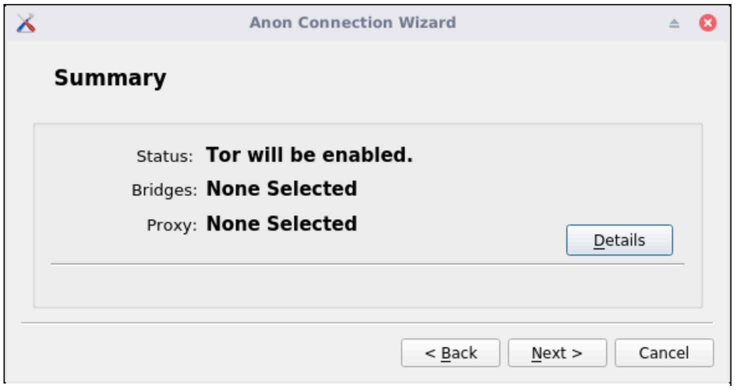
This computer's Internet connection is censored or proxied. I need to configure bridges or local proxy settings.

○ **Configure**

I do not want to connect automatically to the Tor network. Next time I boot, this wizard will be started.

○ **Disable Tor**

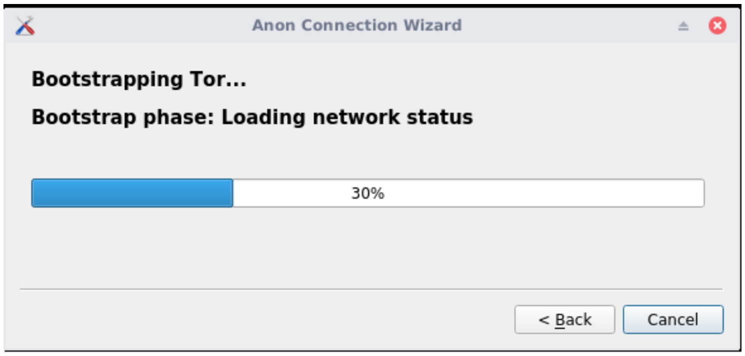
The next screen is a summary of your selection. Click next.



Summary

Status: Tor will be enabled.
Bridges: None Selected
Proxy: None Selected

The next screen starts the connection to the Tor network.

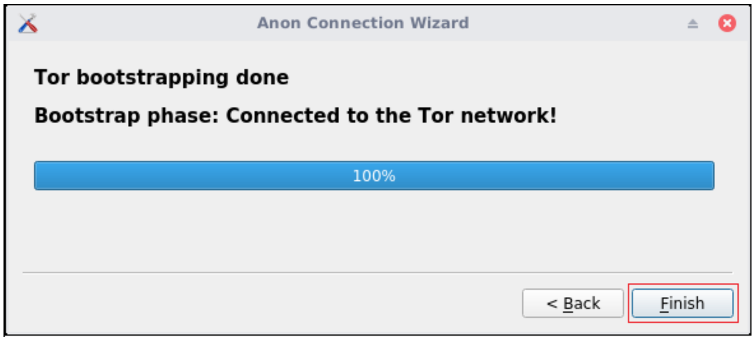


Bootstrapping Tor...

Bootstrap phase: Loading network status

30%

On the last screen, you can click finish.

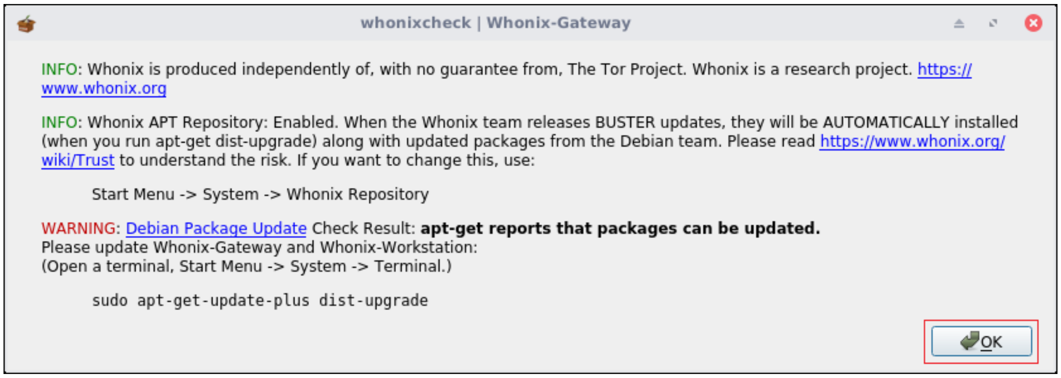


Tor bootstrapping done

Bootstrap phase: Connected to the Tor network!

100%

Once the Tor network starts, a check will be run and to see if any updates are available.



whonixcheck | Whonix-Gateway

INFO: Whonix is produced independently of, with no guarantee from, The Tor Project. Whonix is a research project. https://www.whonix.org

INFO: Whonix APT Repository: Enabled. When the Whonix team releases BUSTER updates, they will be AUTOMATICALLY installed (when you run apt-get dist-upgrade) along with updated packages from the Debian team. Please read https://www.whonix.org/wiki/Trust to understand the risk. If you want to change this, use:

Start Menu -> System -> Whonix Repository

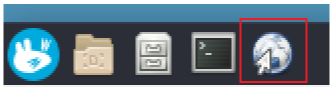
WARNING: Debian Package Update Check Result: **apt-get reports that packages can be updated.**
Please update Whonix-Gateway and Whonix-Workstation:
(Open a terminal, Start Menu -> System -> Terminal.)

```
sudo apt-get-update-plus dist-upgrade
```

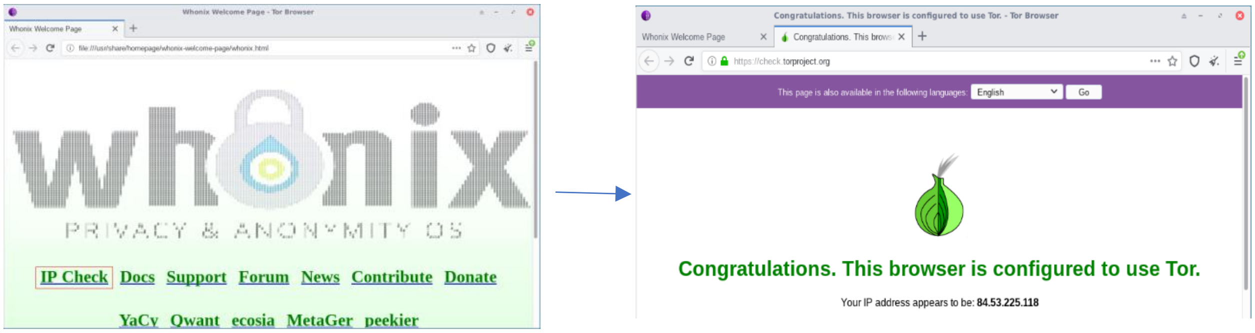
Launch the Whonix Workstation

You can now launch your Whonix Workstation. You will have to agree to the same three-part understanding. The Whonix Workstation is preconfigured to work with the Whonix Gateway, so there will be nothing to configure. The Workstation has loaded, it will conduct a connection check. Once the connection check completes, you will see the same info messages you had to acknowledge with the Gateway.

Once the connection check has been completed, you can check your Tor connection by launching the Tor browser and conducting an IP check.



When the TOR browser opens, click on the IP Check option to see if you are on the Tor network.



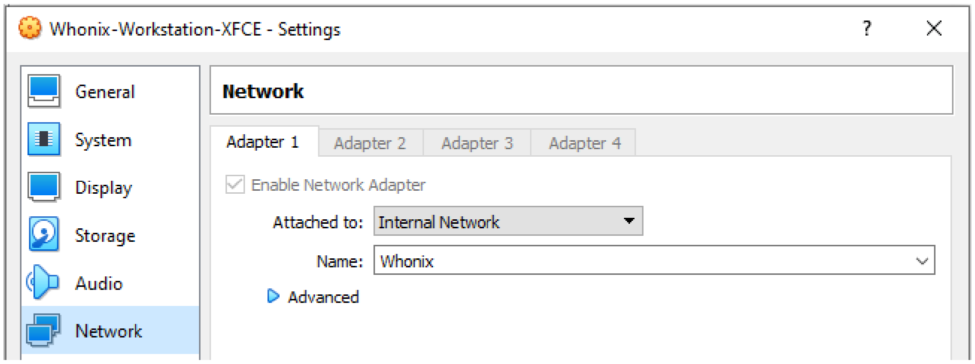
Whonix Welcome Page - Tor Browser
Whonix Welcome Page
file:///usr/share/homepage/whonix-welcome-page/whonix.html
whonix
PRIVACY & ANONYMITY OS
IP Check
Docs
Support
Forum
News
Contribute
Donate
YaCy
Qwant
ecosia
MetaGer
peekier
Congratulations. This browser is configured to use Tor. - Tor Browser
Congratulations. This brows
https://check.torproject.org
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: **84.53.225.118**

You can power off the Whonix Workstation as we will not need it for the remainder of this lab.

The big take away about the Whonix Workstation is that you can use it for anonymous browsing in conjunction with the Whonix Gateway much the same way you would use any workstation. The Workstations VirtualBox connection is set to communicate through the Gateway using the VirtualBox Internal Network adapter.



Network

☑ Enable Network Adapter

Attached to: Internal Network

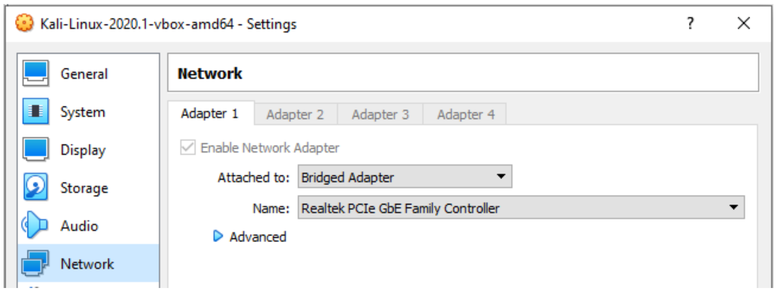
Name: Whonix

Configure your Kali Linux

The configuring of Kali to route its connection through the Whonix Gateway is quite simple.

Currently, Kali is configured to use DHCP, but we will need to set the wired network connection with a static IPv4 address required to find and communicate with the Whonix Gateway.

Ensure that your VirtualBox network adapter for Kali is set to NAT or Bridged Networking.



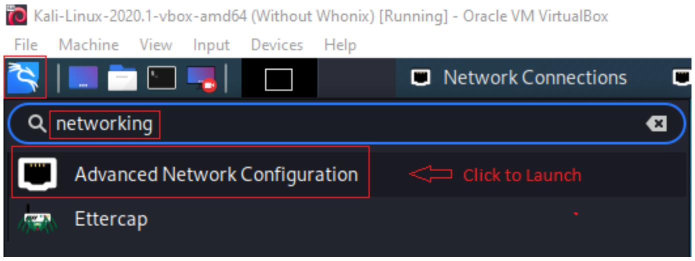
Network

☑ Enable Network Adapter

Attached to: Bridged Adapter

Name: Realtek PCIe GbE Family Controller

To begin, click on the Kali application icon and in the search window type networking, and from the results, click on Advanced Network Configuration.


Kali-Linux-2020.1-vbox-amd64 (Without Whonix) [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Network Connections
networking
Advanced Network Configuration
Click to Launch
Ettercap

When the configuration wizard loads, click on IPv4 Settings. Under addresses, click the Add button.

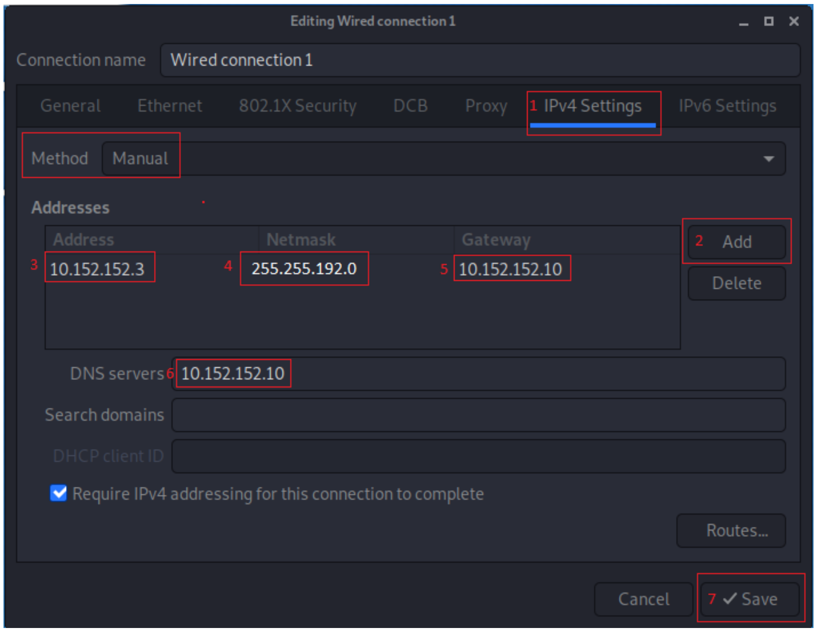
In the Addresses window type the following IP address information.

Address: 10.152.152.3

Netmask: 255.255.192.0

Gateway: 10.152.152.10

DNS servers: 10.152.152.10



Connection name: Wired connection 1

Method: Manual

Addresses

Address	Netmask	Gateway
3 10.152.152.3	4 255.255.192.0	5 10.152.152.10

DNS servers 6 10.152.152.10

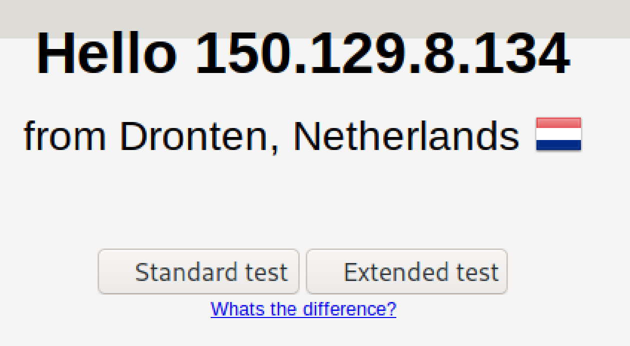
Search domains

DHCP client ID

☑ Require IPv4 addressing for this connection to complete

You can now open your Kali browser and attempt to access the Internet. To see your assigned Tor IP address and your location, you can go to www.dnsleaktest.com to confirm you are using the Whonix Gateway.

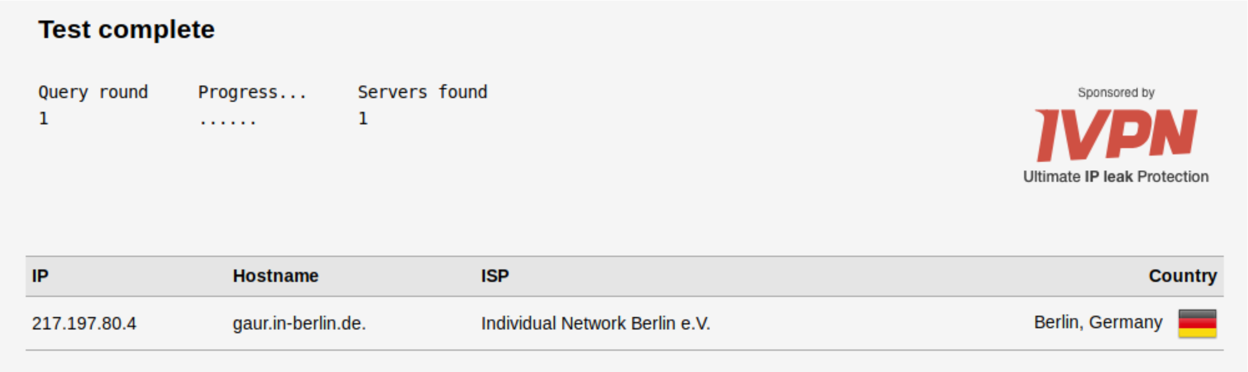
My IP address and location are shown as being in the Netherlands.



Hello 150.129.8.134

from Dronten, Netherlands

My DNS server is in Berlin, Germany.



Test complete

```
Query round     Progress...     Servers found
1               ......          1
```

IP	Hostname	ISP	Country
217.197.80.4	gaur.in-berlin.de.	Individual Network Berlin e.V.	Berlin, Germany

Looking good!

Summary –

In this lab, you learned how to work anonymously with Kali using the Whonix Gateway. Whonix uses the Tor network to ensure your data stays encapsulated. Though there is no 100% sure way to ensure complete anonymous browsing, the Whonix Gateway is about as close as we can get. When we add in a commercial VPN, we add in still another layer of anonymity.

End of the lab!