HUNCHLY

DARK WEB INVESTIGATION

GUIDE

Contents

1. Introduction 3

2. Setting up Chrome for Dark Web Access 5

3. Setting up Virtual Machines for Dark Web Access 9

4. Starting Points for Tor Investigations 20

5. Technical Clues for De-Anonymizing Hidden Services 22

- 5.1 Censys.io SSL Certificates 23
- 5.2 Searching Shodan for Hidden Services 24
- 5.3 Checking an IP Address for Tor Usage 24
- 5.4 Additional Resources 25

6. Conclusion 26

1. Introduction

1 Introduction

There is a lot of confusion about what the dark web is vs. the deep web. The dark web is part of the Internet that is not accessible through traditional means. It requires that you use a technology like Tor (The Onion Router) or I2P (Invisible Internet Project) in order to access websites, email or other services.

The deep web is slightly different. The deep web is made of all the webpages or entire websites that have not been crawled by a search engine. This could be because they are hidden behind paywalls or require a username and password to access.

We are going to be setting up access to the dark web with a focus on the Tor network. We are going to accomplish this in two different ways.

The first way is to use the Tor Browser to get Google Chrome connected to the the Tor network. This is the less private and secure option, but it is the easiest to set up and use and is sufficient for accessing material on the dark web.

The second way is to use a virtual machine setup to create a much more secure environment to perform investigations. Don't be afraid of the terminology, this is pretty straightforward. It's also a bit more resource intensive, but that shouldn't be a problem as long as your computer is reasonably modern.

The reason we focus on Chrome is that we hope you are going to take Hunchly along for the ride so that you can automatically capture hidden service pages, extract EXIF metadata from photos, and leverage some of the investigative tools in Hunchly to make your life easier.

Let's get started!

WARNING

This is important. This guide is **NOT** a guide on how to remain hidden, anonymous or how to perform undercover operations online. This goes for the dark web or otherwise.

This guide is here to help you get setup using Google Chrome to access Tor resources, and how to leverage Hunchly to capture evidence while you do it.

There are numerous references online that you can find that will help you with staying hidden. This is not one of them.

2. Setting up Chrome for Dark Web Access

Setting up Chrome for Dark Web Access

2

Setting Up Chrome to Access Tor

Sometimes you need to quickly refer to a resource on the dark web and your anonymity is less of a concern. The following steps will show you how you can use Tor Browser to proxy Chrome connections and easily access Tor hidden services. It is worth noting that using the Buscador virtual machine (shown later) allows you to open Chrome and browse to hidden services directly without any additional configuration.

Be warned this is the least secure method for accessing Tor with Chrome but I often use it for quick hidden service checks.

Step 1

Download and install Tor Browser: https://www.torproject.org/download/download

Step 2

Download and install Google Chrome: https://www.google.com/chrome/

Step 3

Start Tor browser and leave it running. This will provide our connection to Tor for us.

Step 4

Now we need to get Chrome to proxy its traffic through Tor. The setup is slightly different for each operating system:

Windows

1. You should have a Chrome shortcut on your desktop. Right-click on it and select **Copy**.
2. Right-click on your desktop and select **Paste**.
3. Rename the new shortcut to **Chrome Tor**.
4. Right-click on the Chrome Tor shortcut and select **Properties**.

Setting up Chrome for Dark Web Access

2

Step 4

continued...

5. In the target field add the following after the chrome.exe part:

```
--proxy-server="socks5://localhost:9150" --host-resolverrules="MAP *
~NOTFOUND , EXCLUDE localhost"
```

6. Click the **Apply** button and then click **OK**.

7. Make sure you have all Chrome windows closed and then double click your Chrome Tor **shortcut**.

8. You should see Chrome open and you can now proceed to **step 5** below to verify for your connection.

Mac OS X

1. If Chrome is open, close it (right-click on Chrome in the dock and select **Quit**).

2. Open your **/Applications** folder and go to **Utilities**.

3. Double-click on **Terminal**.

4. Copy and paste this command into the Terminal window, and press **Enter**:

4.
```
/Applications/Google\ Chrome.app/Contents/MacOS/Google\ Chrome --proxy-
server="socks5://localhost:9150" --host-resolverrules="MAP * ~NOTFOUND ,
EXCLUDE localhost"/Applications/Google\ Chrome.app/Contents/MacOS/Google\
Chrome --proxy-server="socks5://localhost:9150" --host-resolverrules="MAP *
~NOTFOUND , EXCLUDE localhost"
```

5. Chrome should open and you can now proceed to **step 5** below to verify for your connection.

Linux

Generally Chrome will be installed as google-chrome and can be accessed from anywhere in your terminal. As Linux installs vary greatly we are going to assume this is the case.

Setting up Chrome for Dark Web Access

2

Step 4

continued...

1. If Chrome is open, close it.
2. Open your terminal application.
3. Copy and paste the following command into the terminal window:

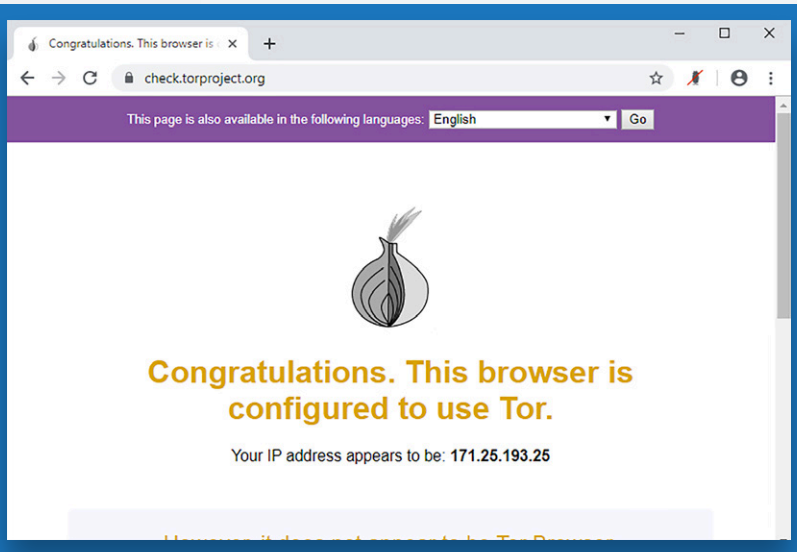
```
google-chrome --proxy-server="socks5://localhost:9150" --host-resolverrules="MAP * ~NOTFOUND , EXCLUDE localhost"/Applications/Google\ Chrome.app/Contents/MacOS/Google\ Chrome --proxy-server="socks5://localhost:9150" --host-resolverrules="MAP * ~NOTFOUND , EXCLUDE localhost"
```

4. You should see Chrome open and you can now proceed to **step 5** below to verify for your connection.

Step 5

Now we need to verify that everything is working. In your Chrome Tor browser window head to: https://check.torproject.org

You should see a message that you are connected to Tor but not using a Tor Browser. This indicates that you have set everything up successfully.



Validating that we are connected to Tor.

3. Setting up Virtual Machines for Dark Web Access

Setting up Virtual Machines for Dark Web Investigations

A far more secure method for performing your dark web investigations is to use virtual machines to both protect you on a network level and at a host level. We will setup two virtual machines, one that will be your investigative machine and one that will forward all of your Internet traffic through Tor. All of the software used is free, and setting it all up is not as hard as it may sound.

We will use Buscador, an OSINT-focused virtual machine by David Westcott and Michael Bazzell, for our investigation virtual machine. The gateway virtual machine that will forward all traffic will use Whonix.

One awesome thing with Buscador is that it is configured to automatically allow you to browse both Tor and I2P by default. So you may wonder to yourself: well why go through all of the trouble of setting up these two virtual machines? The answer is that with our setup, we will route all traffic through Tor. This means any command line tools or additional software on Buscador will also use Tor and not just your web browser.

If you don't feel like setting up the full "paranoid" version, you can stop after getting Buscador imported and starting it up, and skip all of the networking / Whonix parts.

Downloading the Prerequisites

Step 1

Download and install Virtual Box for your operating system here:
https://www.virtualbox.org/wiki/Downloads

Step 2

Download the Buscador virtual machine:
https://inteltechniques.com/buscador/

Step 3

Download the Whonix Gateway virtual machine (only the gateway is required):
https://www.whonix.org/wiki/VirtualBox/CLI

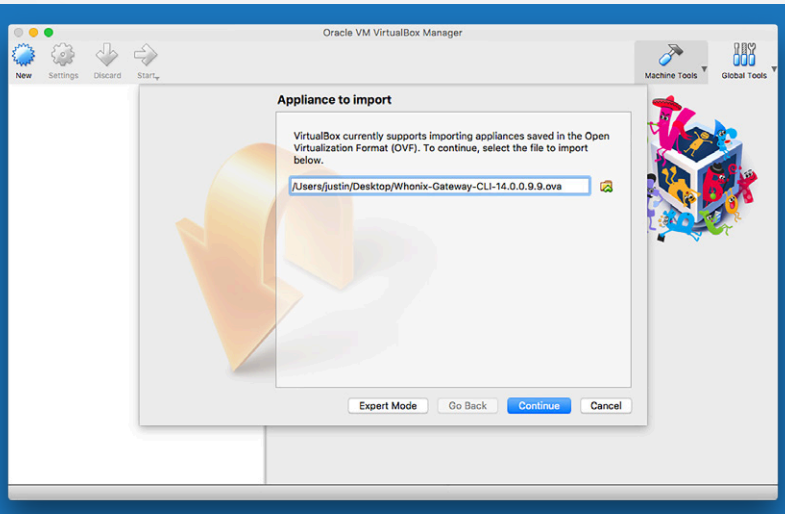
Once you have all three downloaded and Virtual Box installed we can now begin importing the virtual machines. First we will import the Whonix Gateway.

Setting up Virtual Machines for Dark Web Access

3

Step 4

From the **File Menu** select **Import Appliance**. On the next screen click the folder icon and browse to the location where you stored the **Whonix Gateway** download:



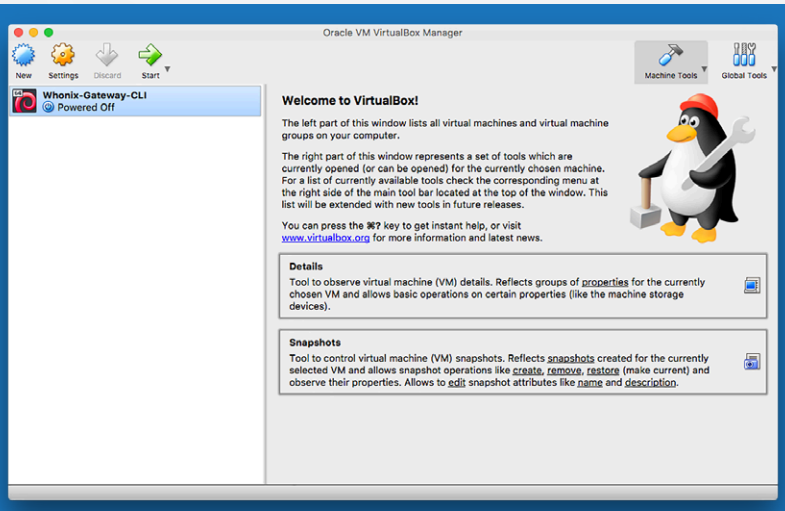
Specifying the path to the Whonix Gateway.

Step 5

Click the **Continue** button and on the resulting screen click **Import** and then **Agree**.

Step 6

The import can take a few seconds to a few minutes depending on your computer hardware. When it is finished you should see the virtual machine in the left hand panel of virtual box as shown below.



Whonix gateway successfully imported.

Step 7

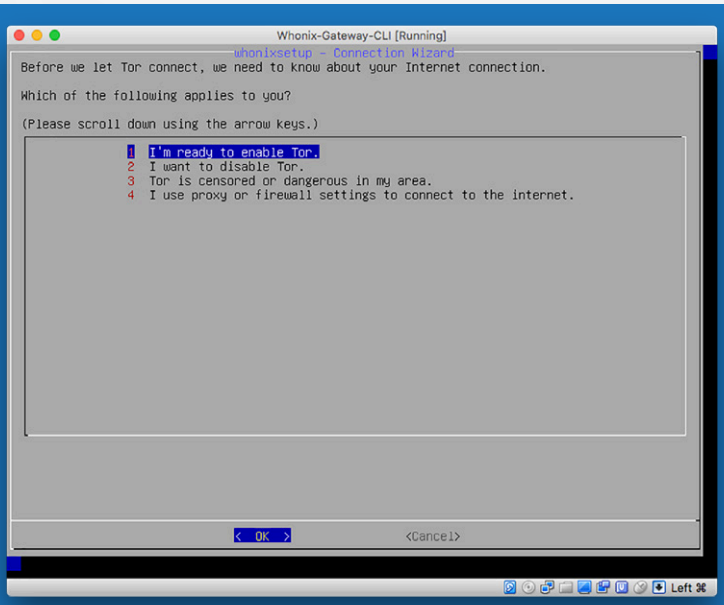
Click on the Whonix gateway virtual machine and then click the **Start** button above it. You will see a new window open with the **Whonix Gateway** starting up.

Setting up Virtual Machines for Dark Web Access

3

Step 8

Now you can login by using the user **“root”** and the password **“changeme”.** This should kickoff the Whonix setup. If you do not see the setup screen shown below, simply type: **whonixsetup** and hit **Enter** on your keyboard.



Whonix setup ready to run.

Step 9

Hit **Enter** with the **OK** button highlighted, and in the next screen hit **Enter** again. You should see a message that Tor has been successfully enabled. Hit **OK** and you can now minimize the window.

NOTE: to get your mouse out of the virtual machine you hit **CTRL+ALT** on your keyboard (**CTRL+COMMAND** on Mac).

Step 10

Now we’ll import the Buscador virtual machine. Click **File** - **Import Appliance**, then select the location of your Buscador download and click **Import**.

Step 11

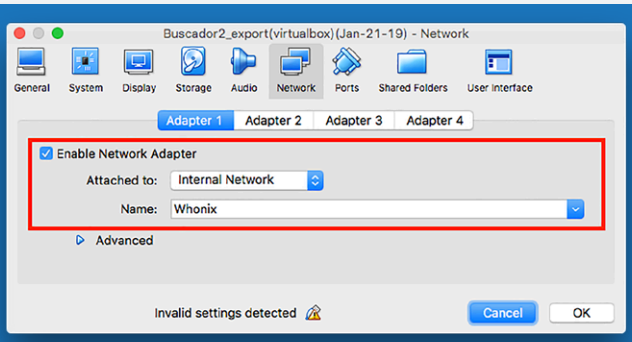
Once it is successfully imported we need to change its network configuration to force all traffic out of our Whonix gateway. Select the Buscador virtual machine and click the **Settings** button.

Setting up Virtual Machines for Dark Web Access

3

Step 12

Click on the **Network** tab and set Interface 1 to connect to the internal network Whonix as shown below.



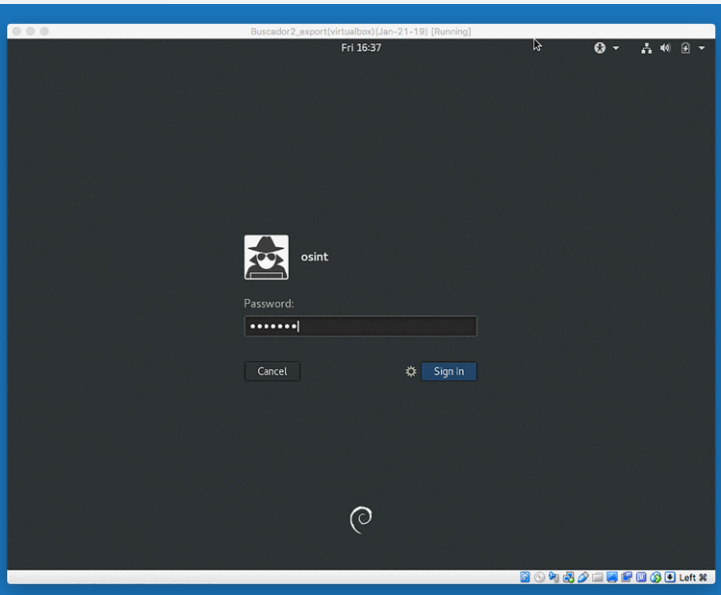
Setting the Buscador network interface.

Step 13

Click the **OK** button which will close the Settings panel. Now select the Buscador virtual machine and click **Start**.

Step 14

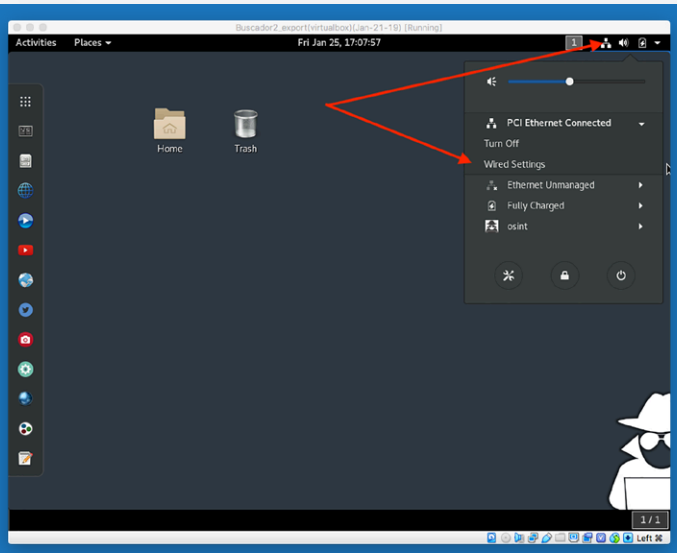
Once the virtual machine has started the password is: **osint** to login to the machine.



Buscador login screen.

Step 15

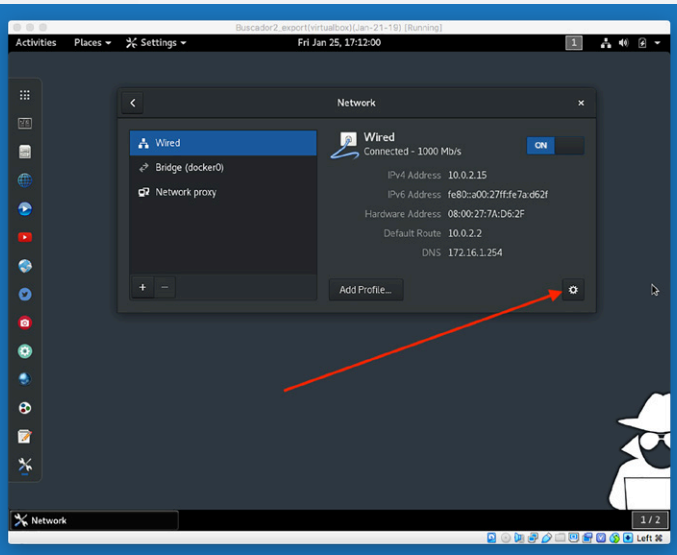
Now we need to reconfigure the Buscador VM so that it will route all of its traffic through our Whonix gateway. Click the **Network** icon shown below, and select the **PCI Ethernet Connected** item to expand it and then click **Wired Settings**.



Selecting the network interface to configure.

Step 16

In the next view click the **Gear** icon in the bottom right as shown below.



Click the gear icon to see the properties page.

Setting up Virtual Machines for Dark Web Access

3

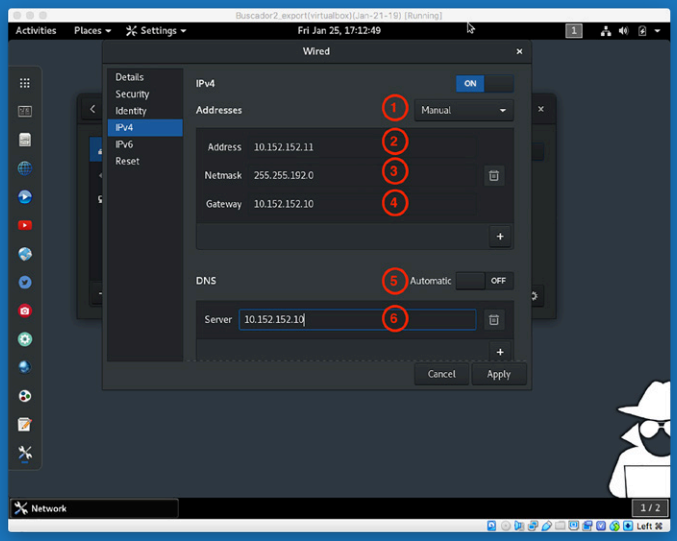
Step 17

Click the **OK** button which will close the Settings panel. Now select the Buscador virtual machine and click **Start**.

Step 18

In the properties screen we need to make a number of adjustments, and each are labelled in the figure below. When you are done, click the **Apply** button.

1. Switch the first dropdown from “Automatic (DHCP)” to **Manual**.
2. In the address field enter: **10.152.152.11**
3. In the netmask field enter: **255.255.192.0**
4. In the gateway field enter: **10.152.152.10**
5. Switch the DNS Automatic toggle to: **OFF**
6. In the Server field enter: **10.152.152.10**



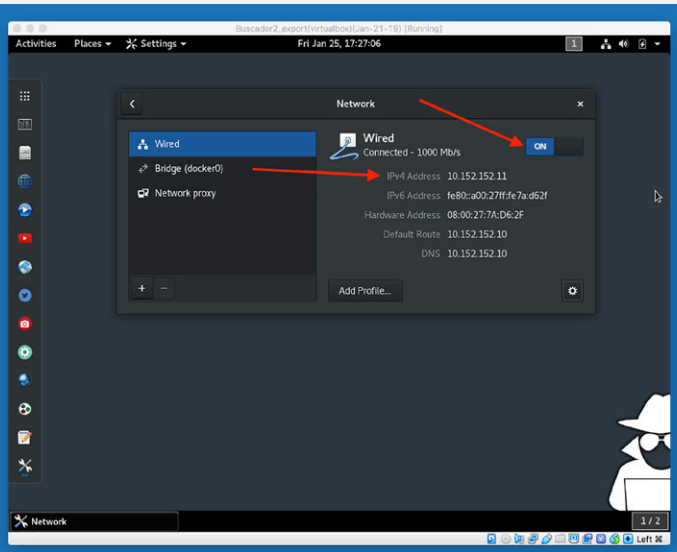
Setting the network adapter properties in Buscador.

Setting up Virtual Machines for Dark Web Access

3

Step 19

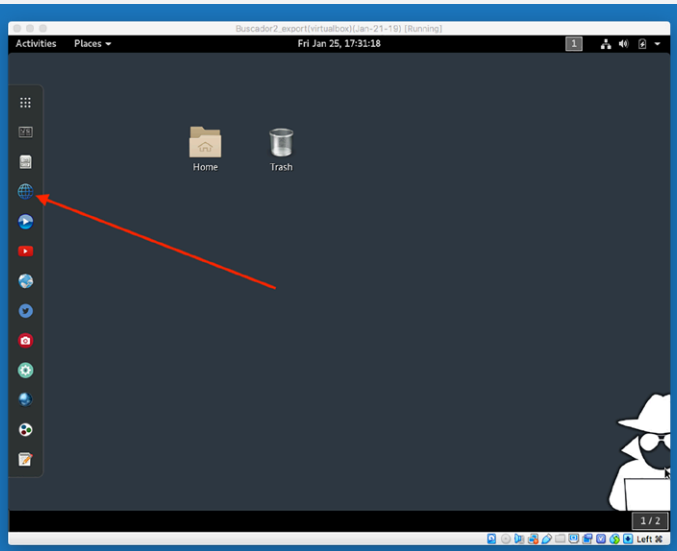
Once you have clicked **Apply** toggle the interface off and then on for it to pick up your new settings. You should see your IP address be set to **10.152.152.11** as shown below.



Toggle network interface to pick up newly configured IP address.

Step 20

Awesome, now we can test that our connection is going out through Tor. Click the **Browsers** shortcut in the left hand toolbar in Buscador and double click the **Google Chrome** icon. Once Chrome starts browse to: https://check.torproject.org



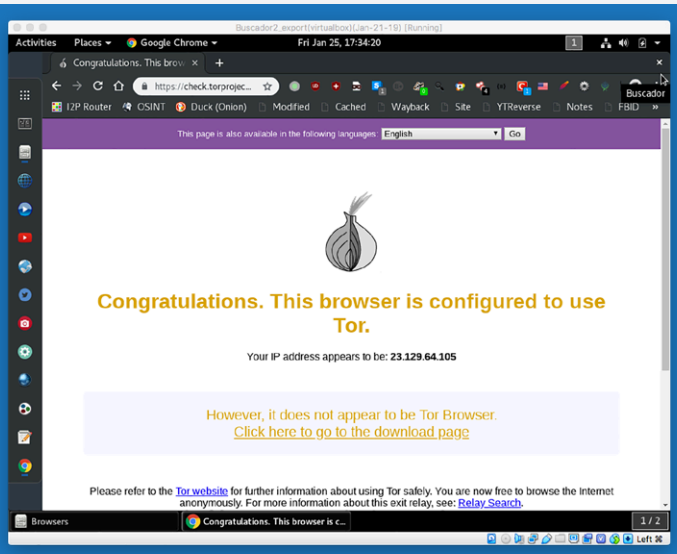
The Browsers shortcut in the Buscador toolbar.

Setting up Virtual Machines for Dark Web Access

3

Step 21

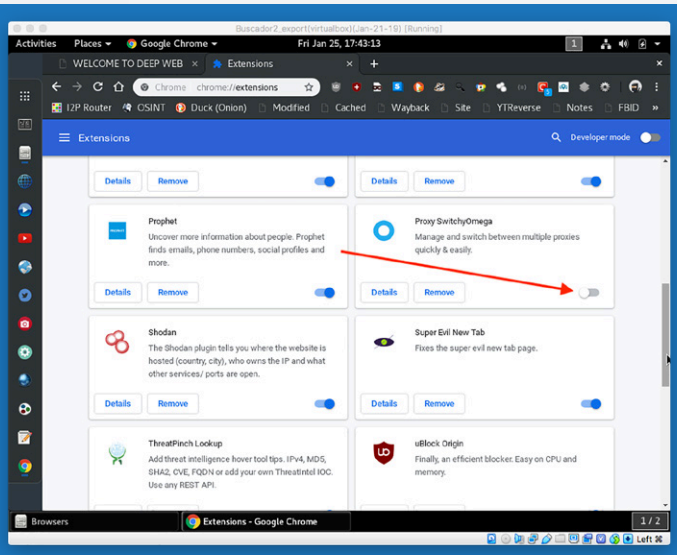
If all goes well you should see a message similar to the one below that indicates you are connected to the Tor network.



Chrome working through the Tor network.

Step 22

Now we just have one more slight thing to change in Chrome to enable us to browse to hidden services. By default Buscador will allow you to visit .onion addresses through a Tor proxy. We need to disable this extension by going to: **chrome://extensions** in your Chrome URL bar. Find the **Proxy SwitchyOmega** extension and toggle it **off** as shown below.



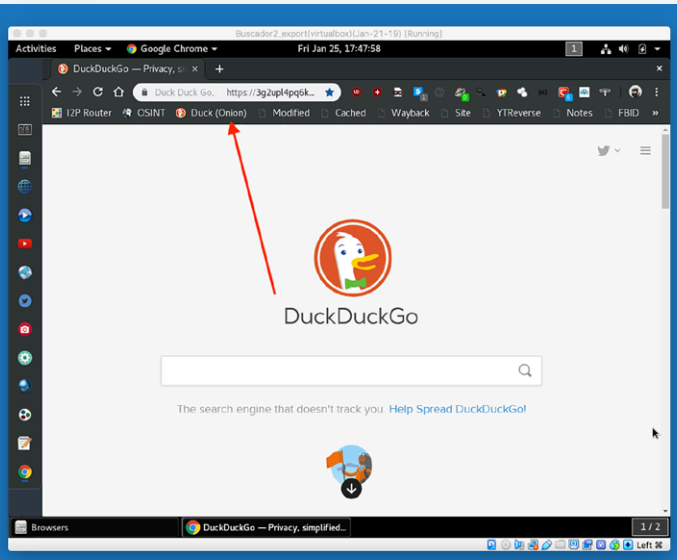
Disabling the Proxy SwitchyOmega extension.

Setting up Virtual Machines for Dark Web Access

3

Step 23

Great! Now we can test that we can reach hidden services by clicking the **Duck (Onion)** bookmark as shown. If DuckDuckGo (the hidden service) loads up for you then you are done with your setup and you can begin doing some investigations on Tor!



Viewing the DuckDuckGo hidden service.

OPTIONAL

Improve your Dark Web Investigations with Hunchly

HUNCHLY

Hunchly has a number of tools that can really enhance your investigations both on the surface web and the dark web. We might be a bit biased but we strongly suggest you take it with you when you go on those dark web deep dives.

Grab your free 30-day trial today at https://hunch.ly/try-it-now!

4. Starting Points for Tor Investigations

Starting Points for Tor Investigations

4

Often first-time dark web investigators are faced with the immediate problem of finding a starting point to begin dipping their toes in. There are a few resources that you can tap into that can help create a starting point for your investigations.

1 Hunchly Daily Dark Web Report

We offer a free service that emails a spreadsheet of hidden services each day. It will tell you any new hidden services discovered, and a historical listing of hidden services that are currently up or down.

2 Reddit/r/onions

This is a good place where Reddit contributors are discussing hidden services on Tor and can sometimes yield good starting points for investigations.

3 DeepDotWeb.com

This is a news site for all things dark web, and they also include up to date information on dark web marketplaces on Tor. Definitely a site to watch or use as a jumping off point.

Using any one of these resources will give you a place to start accessing Tor hidden services and start to see how they operate. You'll be pleasantly surprised that they work exactly like surface websites.

5. Technical Clues for De-Anonymizing Hidden Services

Technical Clues for De-Anonymizing Hidden Services 5

Technical Tips for Investigations on Tor

Often there are subtle clues that a hidden service exposes that might help you track down where it lives for “real” on the Internet. This can vary from misguided hidden service administrators setting up SSL certificates to server headers that you can examine in Shodan and other sites.

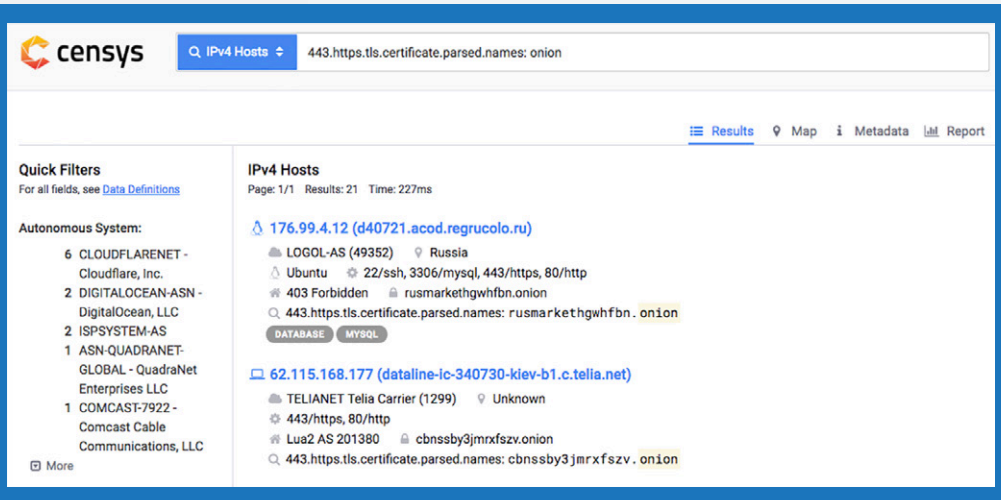
5.1 Censys.io SSL Certificates

It is always interesting when a Tor hidden service has an associated SSL certificate deployed to their server. The traffic within Tor is already encrypted so this is largely not needed, however, sometimes you will find that someone has made the mistake of setting one up.

You can actually search through Censys.io for these tidbits of information. For example, to find all surface web sites that have a .onion SSL certificate (meaning they are already de-anonymized potentially):

```
443.https.tls.certificate.parsed.names: onion
```

This should give you a list of IP addresses where there were SSL certificates that had hidden service addresses in them.



Censys.io search for SSL certificates with onion in their name.

5.2 Searching Shodan for Hidden Services

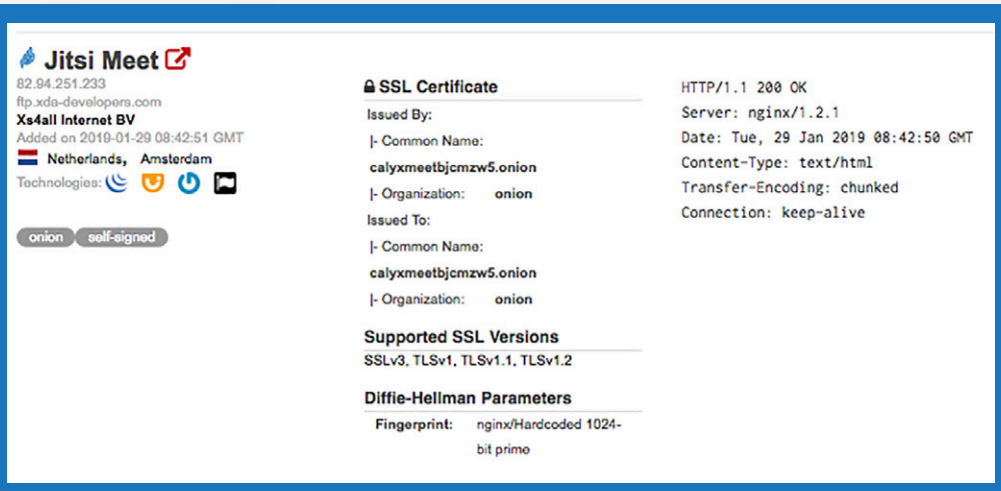
Using much the same technique, we can actually search Shodan for .onions either by doing an SSL certificate search, or just a general query. You can also substitute the .onion with the full address of the hidden service you are interested in as well.

```
ssl:".onion"
```

For a general query you can simply do:

```
".onion"
```

By examining the results you can spot any sites that may be misconfigured that may indicate where they are located.



Shodan result showing a hidden service and its IP address.

5.3 Checking an IP Address for Tor Usage

Sometimes you will be on the opposite end of an investigation where you have an IP address and you aren't sure if the user was on Tor or not. The Tor Project makes a handy tool that allows you to determine whether an IP address was connected to Tor on a particular date.

You can use the tool here: https://metrics.torproject.org/exonerator.html

5.4 Additional Resources

There are some excellent articles, blog posts and tools for investigating hidden services on Tor. Here are some personal favourites:

- Finding the Real Origin IPs Hiding Behind CloudFlare or Tor - SecJuice
- Securing a Web Hidden Service
- Investigating Using the Dark Web (Presentation)
- OnionScan (tool)

6. Conclusion

6 Conclusion

Dark web investigations are not as scary as one might think, but it is important to have your investigation goals set out before you start poking around. Think about your target, the risk of you being discovered, and ultimately what you are trying to glean.

The rest of it is just simply applying all of your investigative knowledge like you would any other investigation. Look for email addresses, try to spot patterns, and more than anything be tenacious.

If you need a hand with anything or have any questions please just send me a note: justin@hunch.ly

Happy hunting!

Justin Seitz

www.hunch.ly