

Lab-5: DNS tricks

- Share

-

- 1



-

CHANGED 3 MONTHS AGO Like Bookmark

Subscribed

0

Lab-5: DNS tricks

tep 0: Check the IP Addresses for Two Different Websites

Open up an RDP connection to Ubuntu.

In your Ubuntu machine, open a terminal prompt. You can do so by navigating to Applications -> Terminal Emulator. Terminal Prompt in Applications dropdown

We will first be using the ping command, which we will use to send out a message (in the form of a packet of information) to Google's servers. If the server is available, it will send a reply back to us. If it's not, we'll see that show as well as a response in the terminal output.

Type ping www.google.com in the terminal. Once you hit enter, you'll see the pings start. Let it continue until you've captured about four (4) pings, and then type Control + C in order to stop the command.

Let's analyze this information! In parenthesis, you'll see the website's IP address. The IP address is the unique number that has been assigned to the website (usually by an Internet Service Provider) and identifies it on the internet. Note the IP address that is reflected for www.google.com in the pings:

www.google.com

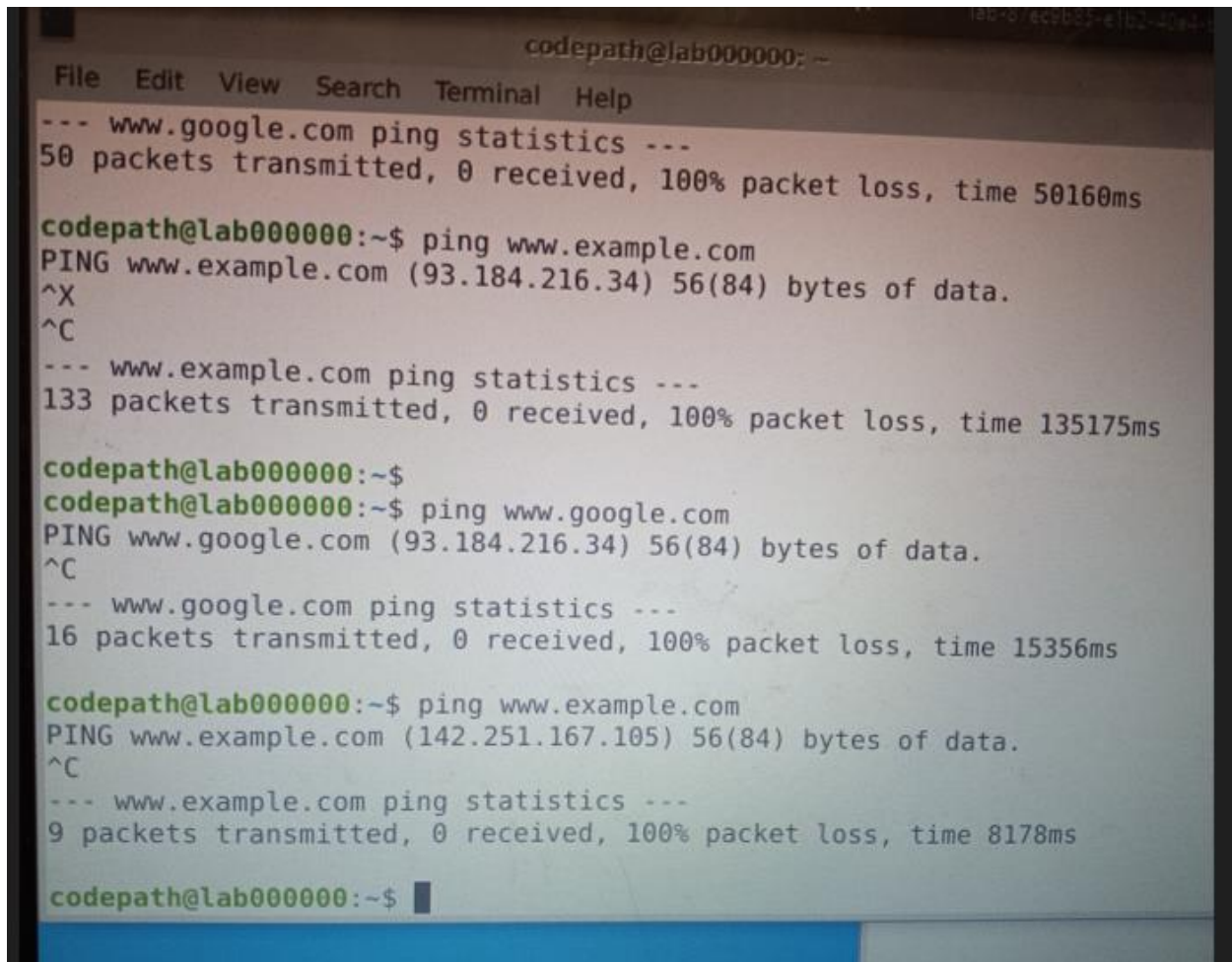
Next, in the same terminal, type ping www.example.com. Note the IP address that is reflected for www.example.com in the pings:

www.example.com IP address

Other pieces to note here in the console is that you'll see the size of the data packets that have been sent for each request (in this case, 64 bytes), as well as the time it took for the response to come back for each one (measured in milliseconds).

At the bottom of each ping for the web address you'll see a summary of this information (statistics) printed out for you in the console.

ping statistics summary

A screenshot of a terminal window with a dark background and light-colored text. The terminal shows a series of ping commands and their results. The prompt is 'codepath@lab0000000: ~'. The first command is 'ping www.google.com', which results in '50 packets transmitted, 0 received, 100% packet loss, time 50160ms'. The second command is 'ping www.example.com', which results in '133 packets transmitted, 0 received, 100% packet loss, time 135175ms'. The third command is 'ping www.google.com', which results in '16 packets transmitted, 0 received, 100% packet loss, time 15356ms'. The fourth command is 'ping www.example.com', which results in '9 packets transmitted, 0 received, 100% packet loss, time 8178ms'. The terminal window has a menu bar at the top with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'.

```
codepath@lab0000000: ~
File Edit View Search Terminal Help
--- www.google.com ping statistics ---
50 packets transmitted, 0 received, 100% packet loss, time 50160ms

codepath@lab0000000:~$ ping www.example.com
PING www.example.com (93.184.216.34) 56(84) bytes of data.
^X
^C
--- www.example.com ping statistics ---
133 packets transmitted, 0 received, 100% packet loss, time 135175ms

codepath@lab0000000:~$
codepath@lab0000000:~$ ping www.google.com
PING www.google.com (93.184.216.34) 56(84) bytes of data.
^C
--- www.google.com ping statistics ---
16 packets transmitted, 0 received, 100% packet loss, time 15356ms

codepath@lab0000000:~$ ping www.example.com
PING www.example.com (142.251.167.105) 56(84) bytes of data.
^C
--- www.example.com ping statistics ---
9 packets transmitted, 0 received, 100% packet loss, time 8178ms

codepath@lab0000000:~$
```

Step 1: Install Falkon Browser

You may already have Falkon browser installed on your Ubuntu Linux box from the Unit 2 lab Ubuntu machine setup. In case you don't have it already, please install with the following command:

```
sudo apt install -y falkon
```

You can check to see if it is installed by going to the top left menu under Applications -> Internet -> Falkon (as shown below):

Falkon Browser Application

Step 2: Navigate to Hosts File

Now, we will take a look at the hosts file.

In the RDP connection in your Ubuntu machine, open up another terminal prompt using the same steps as you did for the first one (Applications -> Terminal Emulator). In the top bar of your Ubuntu window, you should now see that there are two prompts open in the menu, and you'll be able to switch back and forth between these two windows.

uxterm Two Instances Launched

In the new open terminal window, type `pwd`. This command is short for print working directory, which will let you know the full path of the directory you are currently in. You should see `/home/azureuser` as listed below:

Print Working Directory Home Folder

From here, you can type `ls` to see the files that are in this directory. `ls` is short for list.

List command

We can see all of the folders show up in the blue colors. Let's navigate into the Documents folder by typing `cd Documents`:

Navigating to Documents directory

Type `pwd` again. This should now list the path as `/home/azureuser/Documents`:

Print Working Directory Documents Folder

Type `ls` to list the files in the Documents directory. For this Ubuntu machine, there are no files here, yet if you may have some that you've saved in this location, and you'll see them listed here.

List command Documents Folder

In the new open terminal window, type `cd ~`. This command will always take you to your home directory in case you might be in a different place in the file system. Tilde command

Type `pwd`. This should now list `/home/azureuser` (your home directory).

Print Working Directory Home Folder

Type `cd ..` to go up one directory. This is called the parent directory to the one we were just in.

Change to parent directory

Type `pwd`. We can confirm that we are in the `/home` folder now. Notice how the terminal prompt also matches and prints this out as well.

Print Working Directory Home Folder

Type `ls`. Here we see our `azureuser`.

List command to see user folder

Type `cd ..` to go up one more directory.

Change to parent directory

Type `pwd`. We can confirm that we are in the `/home` folder now. Notice how the terminal prompt also matches and prints this out as well.

Print Working Directory Root Folder

Type `ls`. Here we are able to see the `/etc` folder in the list.

List Command to See Root Folder

We will navigate to the `etc` folder from here – change directory into the `etc` folder.

`cd etc`

Change to `etc` folder

Type `pwd`. Here you will be able to confirm that you navigated into the `/etc` folder.

Print Working Directory `etc` Folder

If we type `ls`, we will see all the contained files. Here we will find the `hosts` file in the list.

List the files, find the `host` file

`cd ~` to go to the home directory,

`pwd` to print the working directory,

`ls` to list the contents of the current directory,

`cd <folder>` to navigate into a directory,

`cd ..` to go up one directory (parent directory), and

`nano` to open up a file in a text editor.

These commands will be ones that you will use often when working in the command line. Feel free to refer to this section whenever you need a refresher! tada

Step 3: Examine the `Hosts` file

Let's take a look at this file! In order to open it, we can use `nano` text editor. Type:
`nano hosts`

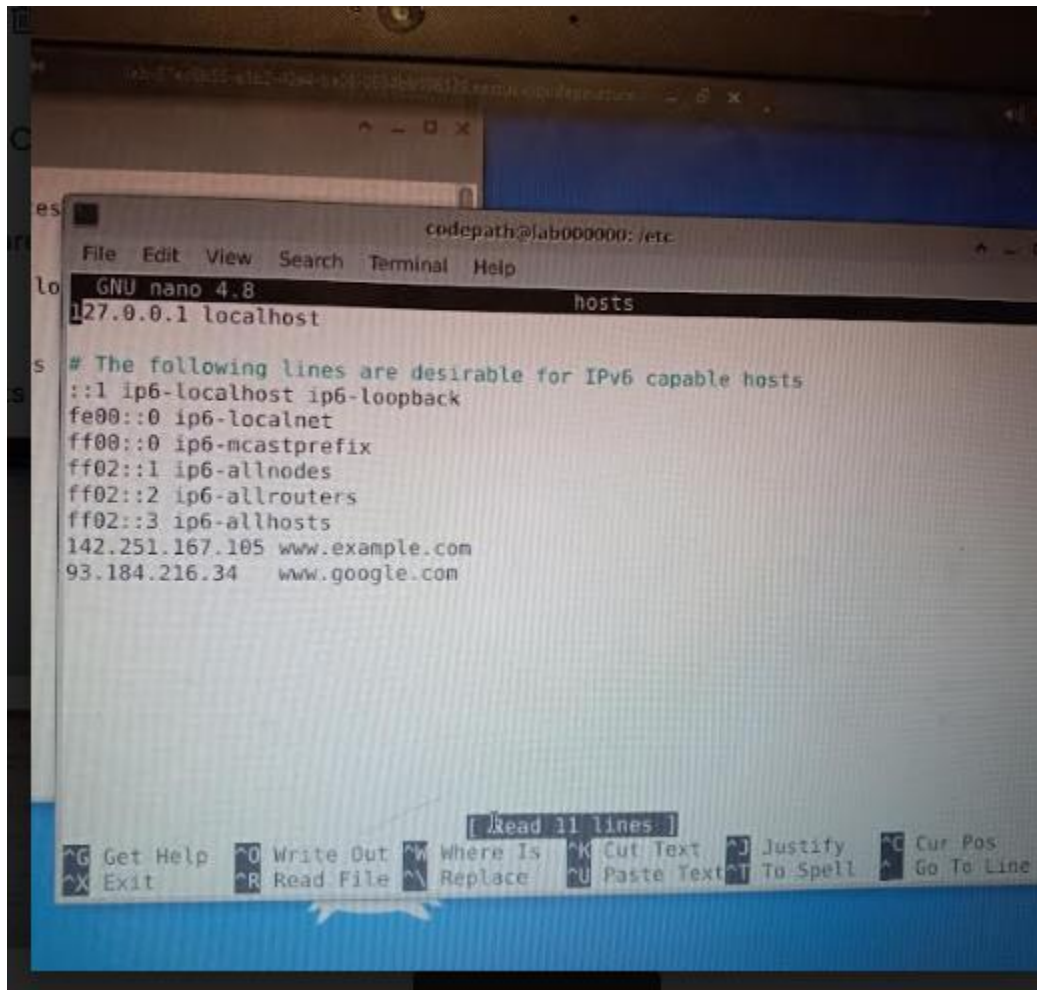
Press enter. Here you will see the file open up, and it will look something similar to this.

Default `Hosts` File

For our purposes, all we need to know is that these four (4) lines and settings are all needed in the `hosts` file as default so that communication can happen to translate the host names we search for into an IP address. The first one is our `localhost`, and is the way that the Ubuntu machine knows how to talk to itself. If you're curious and would like to read more about what each of these different addresses mean, please take a look at this [Understanding Ubuntu's Hosts File](#) article.

You may also see a message in the terminal window that says File '`hosts`' is unwritable. This is because when we opened the file using `nano hosts`, we opened it in viewing mode, which will not allow us to make edits. We don't have to worry

about this for now since we are only examining the file, yet we'll use a different command when we want to edit it later.



```
codepath@lab0000000: /etc
File Edit View Search Terminal Help
GNU nano 4.8 hosts
127.0.0.1 localhost

# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
142.251.167.105 www.example.com
93.184.216.34 www.google.com

[ Read 11 lines ]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell ^_ Go To Line
```

Type Control-X to exit this screen and go back to the terminal prompt.

Step 4: View the Web Pages in the Browser

Now, we'll take a look at each of these websites in the browser. We'll want to verify it's what we're expecting to see when we go to them directly.

Open the Falkon browser (by navigating to Applications -> Internet -> Falkon) and open a new browser window.Falkon Browser Application

Falkon Browser Window

Let's first take a look at Google's Search Engine site. In the address bar at the top, type www.google.com.Type www.google.com

Press enter in the address bar. It will navigate to www.google.com. In case it gives a prompt to "Sign in to Google", click on "No thanks".Navigate to www.google.com.

The web page should show up the same as we saw before, as shown in the image below, and the url will show as <https://www.google.com>.Google.com url in Address

Bar

Next, let's take a look at the [Example.com](http://www.example.com) site. In the address bar at the top, type www.example.com. Type www.example.com

Press enter in the address bar. It will navigate to www.example.com. Note the url in the address bar that is shown. In this case, it's

showing <https://www.example.com/.Example.com> url in Address Bar

Step 5: Edit the Browser Settings

Before we make any edits to our hosts file, since we went to the website in our browser, we'll need to clear any history and traces of us visiting them so that we can be sure that we'll be accessing the correct info from the hosts file. Let's change some settings in the browser.

In the top bar in the Falkon browser is an icon on the top left with three (3) vertical lines (this is often called a hamburger menu icon). Click on it and navigate to History -> Show All History.

Show All History Falkon Browser Settings

This will open up a Library menu, which will show the browser history. Click the arrow dropdown menu icon to expand and see more for Today. You should see the websites we have just visited on this list, Example and Google, as shown below:

Click Today Dropdown to See All History

Next, click on the Clear All History button:

Click on Clear All History

It will prompt you with a message that says "Are you sure you want to delete all history?". Click on Yes.

Click on Yes to Confirm to Clear All History

You should now see all of the history cleared in the menu. This will remove some traces of us having visited the web pages before in the browser. Click the X at the top of the menu to close it.

History Cleared in Menu

Next, we'll change a few of the browser settings to clear more of the information that's been stored about the pages we visited.

In the hamburger menu, navigate to Preferences:

Navigate to Preferences in Falkon Menu

The Preferences Menu will pop up, and you'll be taken to the General section. Here, we will change the "After Launch" settings.

Launch Settings

In the drop down menu, choose "Open homepage". This will open the default home page, which is set to falkon:start (which we saw earlier).

Open homepage Preference in Falkon General Settings

Once that is selected, click on the "Apply" button to set this setting.

Apply Launch settings to open homepage

Next, click on the Browsing section on the left. In the Local Storage tab, we will be changing a few settings.

Uncheck the Allow storing network cache on disk.

Uncheck Allow saving history.

Uncheck Allow local storage of HTML5 web content.

Click the Delete Now button next to the Delete locally stored HTML5 web content on close.

Setting Local Storage Settings

Your Browsing Settings should look like the image below. After you are done changing these settings, click on the "Apply" button.

Applying Local Storage Settings

The last setting we will set will be under the "Privacy" section. In the "Manage Cookies" setting, click on the "Cookies Manager" button.

Click on Cookies Manager button

Under the Cookies Menu, click on the "Remove all cookies". This will delete all the cookies the browser currently has saved.

Remove all cookies

It will prompt you to confirm that you want to delete all the cookies on your computer. Click on the "Yes" button.

Confirm deleting all cookies

The cookies will be cleared! After you are done, click on the "Settings" tab:

Cleared Cookies

☐ Uncheck the "Allow storing of cookies" setting.

Uncheck Allow storing of cookies

After you are done, click on the "Close" button.

Close Cookie Settings Menu

Back in the Privacy Preferences menu, click on the "Apply" button. After you click on "Apply", click the "Ok" button to close the Preferences menu.

Apply Privacy Settings

The very last thing we will do is to clear the recent history. In the hamburger menu, go to Tools -> Clear Recent History:

Clear Recent History Setting

Make sure that these settings are as follows:

Visited pages history from: should be set to "All". This will clear page histories from any time period.

Web databases, Local storage, Cache, and Cookies are all checked.

Once you have modified these settings, click on the "Clear" button. The button will change to "Done" and the popup window will close itself.

Clear Recent History on Falkon

Close the browser window once you are done with all the changes.

Step 6: Edit the Hosts file

Back in our terminal window where we opened the hosts file, we'll start to make some edits. take a look at this file! In order to open it, we can use nano text editor again with one slight change. Type:

```
sudo nano hosts
```

Adding sudo in front of the command we used before will allow us to modify this file. It should no longer show the warning from before when the file opens:Open hosts file

Move your cursor to the bottom of the file by using the down arrow on your keyboard (place it after the line that has ff02::2). You should see the white cursor as shown below.

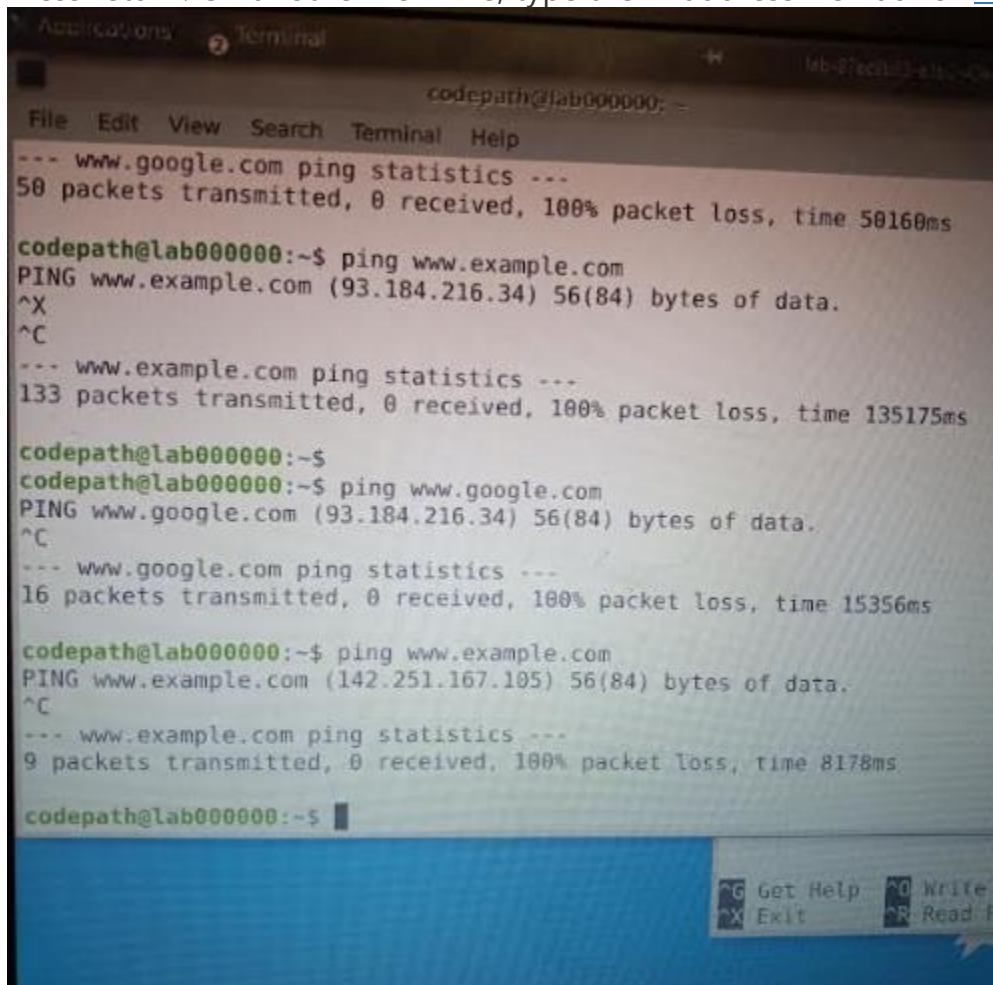
White cursor in file

Now, we'll start adding entries to our hosts file for the websites we are testing.

On the new line, type the IP address we had for www.google.com.

On the same line, type the website we want to direct it to instead, which is www.example.com.Type new IP address for www.example.com

Press return. On another new line, type the IP address we had for www.example.com.

A terminal window titled 'Terminal' with a menu bar (File, Edit, View, Search, Terminal, Help) and a title bar (Applications, Terminal, lab-27ecb03-31b0-40a4). The prompt is 'codepath@lab0000000: ~\$'. The terminal shows the following commands and output:

```
--- www.google.com ping statistics ---
50 packets transmitted, 0 received, 100% packet loss, time 50160ms

codepath@lab0000000:~$ ping www.example.com
PING www.example.com (93.184.216.34) 56(84) bytes of data.
^X
^C
--- www.example.com ping statistics ---
133 packets transmitted, 0 received, 100% packet loss, time 135175ms

codepath@lab0000000:~$
codepath@lab0000000:~$ ping www.google.com
PING www.google.com (93.184.216.34) 56(84) bytes of data.
^C
--- www.google.com ping statistics ---
16 packets transmitted, 0 received, 100% packet loss, time 15356ms

codepath@lab0000000:~$ ping www.example.com
PING www.example.com (142.251.167.105) 56(84) bytes of data.
^C
--- www.example.com ping statistics ---
9 packets transmitted, 0 received, 100% packet loss, time 8178ms

codepath@lab0000000:~$
```

On the same line, type Google's Search Engine website url www.google.com.

Type new IP address for www.example.com

In order to save our changes, we'll type the command Control+O. This is the Write Out command, which will write these changes to the hosts file. When it asks what "File Name to Write:", leave it as "hosts".

Write out changes to hosts file

You'll see a message print out that shows that you wrote some lines! This confirms that the changes you wrote were saved to the file.

Message showing file changes written

To close the file, type Control+X. This should exit the file and take you back to the terminal prompt. Terminal prompt after writing file

Step 7: Check the Pings in the Terminal For Changes

In the same terminal window, ping www.google.com. Notice how the IP address is now different than before, and it's being redirected to the IP address

for www.example.com:

www.google.com is redirected to www.example.com IP address- [] Try pinging `www.example.com`. Notice how the IP address is now different than before, and it's being redirected to the IP address for `www.google.com`: `www.example.com` is redirected to www.google.com IP address the hosts file! Now, we'll want to check what kind of behavior we'll see in the browser.

Step 8: Check the Browser For Changes

Open a new Falkon browser window. It should take you to the falkon: start page based on the settings we set before.

Open a new Falkon Browser window

Since we cleared all of the local data for the browser, we should be able to check each of the sites from scratch, and it should be referencing our modified `hosts file.

Type www.google.com in the address bar and hit Return.

Type www.google.com in the Address Bar

A 404 - Not Found page should display. Check the url – this will still show www.google.com.

404 Error for Example page

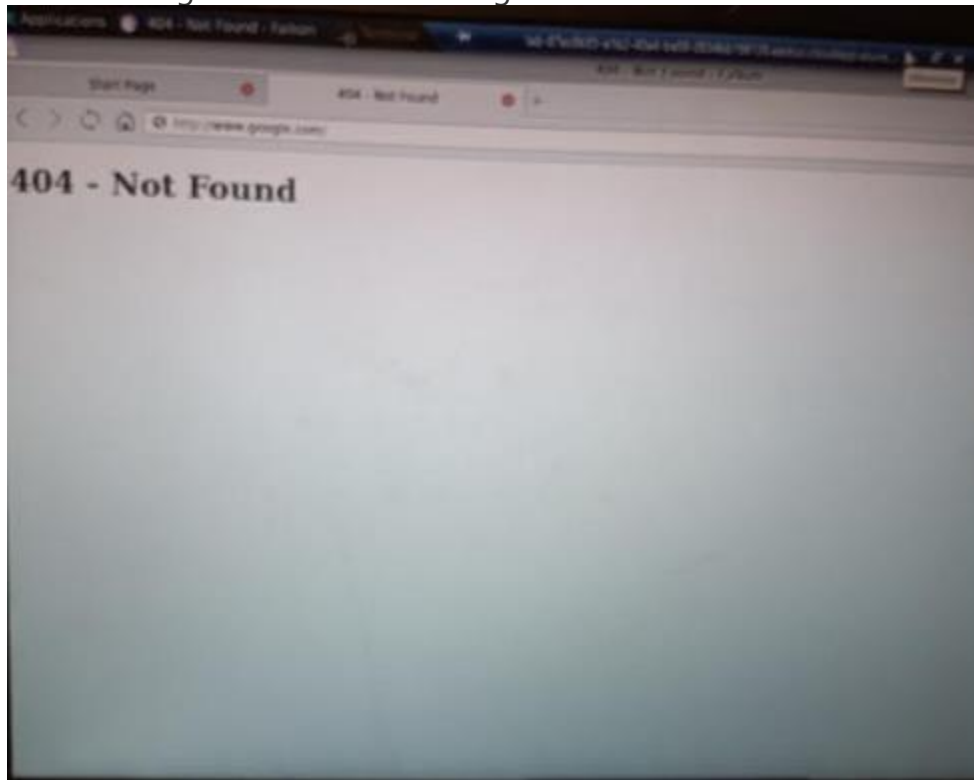
Now, try typing www.example.com in the address bar.

Type www.example.com in the Address Bar

A 404 - Not Found page should display. Check the url – this will still

show www.example.com, yet is showing a Google server error page, so we know that

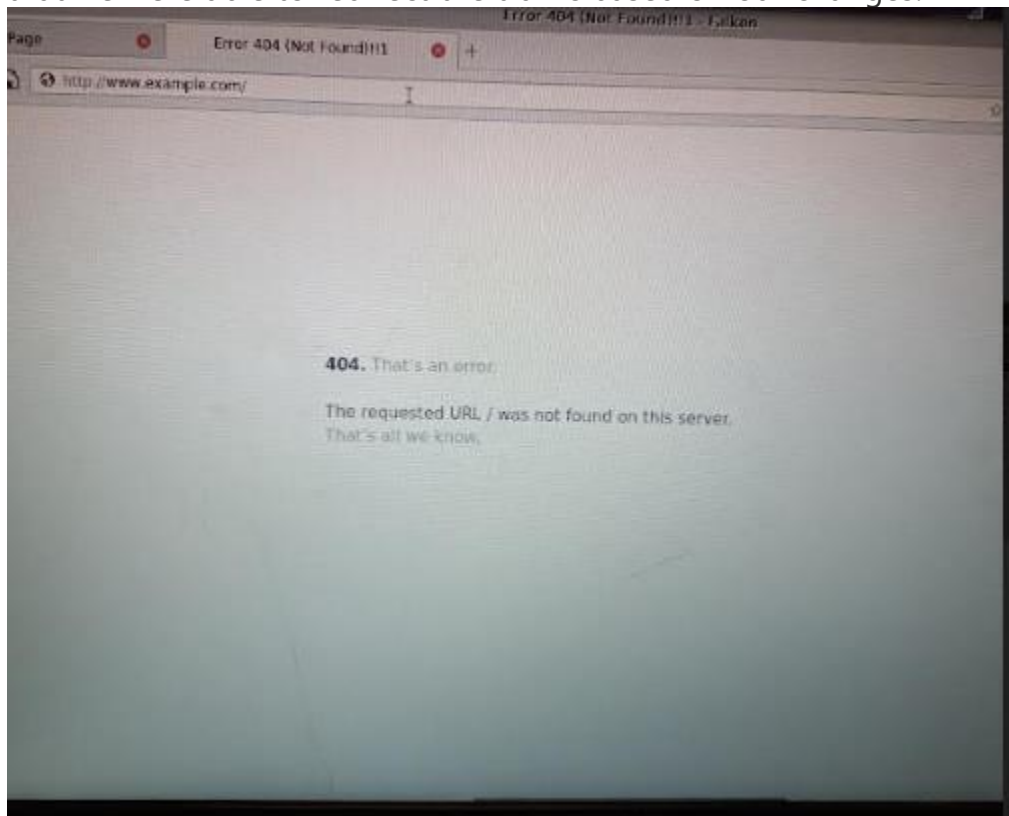
we are being redirected to a Google server.



404 Error for Google page

One thing to note is that we were not able to see the actual pages being spoofed in the browser. The reason we could only see the error messages show is because there are more advanced security features in the browser that will prevent us from showing the actual page, yet our pings and error messages have helped us verify

that we were able to redirect the traffic based on our changes.



Step 9: Restore your Hosts file to normal!

Use `sudo nano hosts` to edit your hosts file again. This time, remove all those extra lines you added... that way Google works in future projects!

[Expand all](#)[Back to top](#)[Go to bottom](#)

Select a repo

Edit Note Details

Change note title, set tags, cover photos, and other metadata here.

[Skip](#)[Next](#)