Tor LAB

LAB 6

Josiah Smythe

March 25, 2019

Dr. Lehrfeld -Information Security and Assurance

East Tennessee State University

1. Purpose

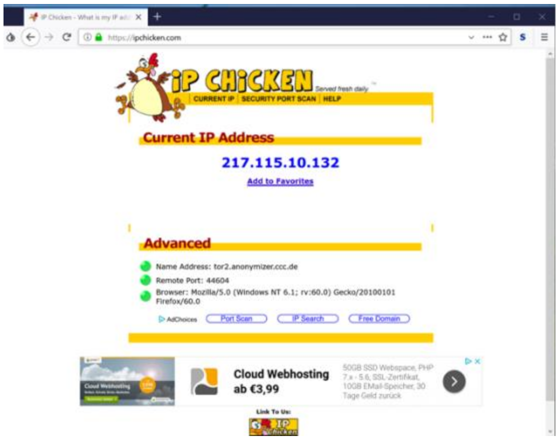
This exercise will illustrate several different methods of browsing the internet anonymously. This process will show how the anonymity of an internet connection can be created and utilized in real word situations.

2. Materials

This lab was completed within the virtual machine environment Windows 10 Consumer. This system was running in the virtual machine hosting application VMware Fusion Professional, Version 11.0.2. VMware Fusion was being supported by Mac OS Mojave on a MacBook Pro 2015 15” with 16 GB of DDR3 Ram and an Intel i7-4770HQ running 2.2GHz. The procedures implemented in this project were completed according to the instructions in the document “tor - Lab.dox” provided by Prof. Lehrfeld and was also supported by personal class notes.

3. Procedures and Results

To begin evaluating these methods of spoofing by simulating anonyms signature the Virtual Machine application VMware Fusion was launched. The virtual machine Windows 10 Consumer was launched from VMware Fusion and the process of downloading the Tor bundle was begin. The Tor suite can be found at the website https://www.torproject.org and because it is an open source software it is free to download and install. The default installation questions were accepted when the Tor installer prompted for a choice. After the installation process had completed, the application Mozilla Firefox was terminated to ensure that no issues would arise between the Tor version of Firefox and the original.



Current IP Address

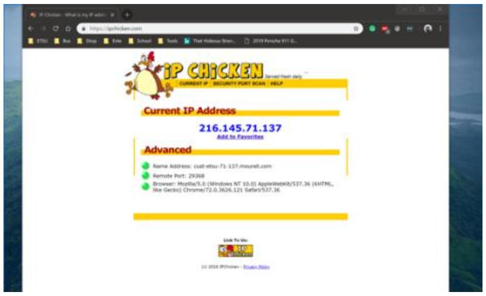
217.115.10.132

Advanced

- Name Address: tor2.anonymizer.ccc.de
- Remote Port: 44604
- Browser: Mozilla/5.0 (Windows NT 6.1; rv:60.0) Gecko/20100101 Firefox/60.0

Ipchicken.com Tor, image #1

The next step taken was to launch the Tor browser from the desktop of the windows 10 system where it was installed to. This is done by opening the folder called Tor Browser and navigating to the icon called “Start Tor Browser”. As inferred by the name this link will initialize the application Tor Browser that was downloaded and installed previously. When the application is up and running it will look similar to Mozilla Firefox, but it will display an onion in the top left corner of the browser right below the first tab. To evaluate the current digital signature via the currently broadcasted iPaddress the website ipchicken.com was accessed. The result of this step is shown on the right in screenshot #1. As shown the iPaddress is “217.115.10.132”. To follow up with the previous discovery of the ipaddres being spoofed the application Google Chrome was opened in the same Windows 10 environment and the website ipchicken.com was navigated to. The results of this second ipchicken.com



Current IP Address

216.145.71.137

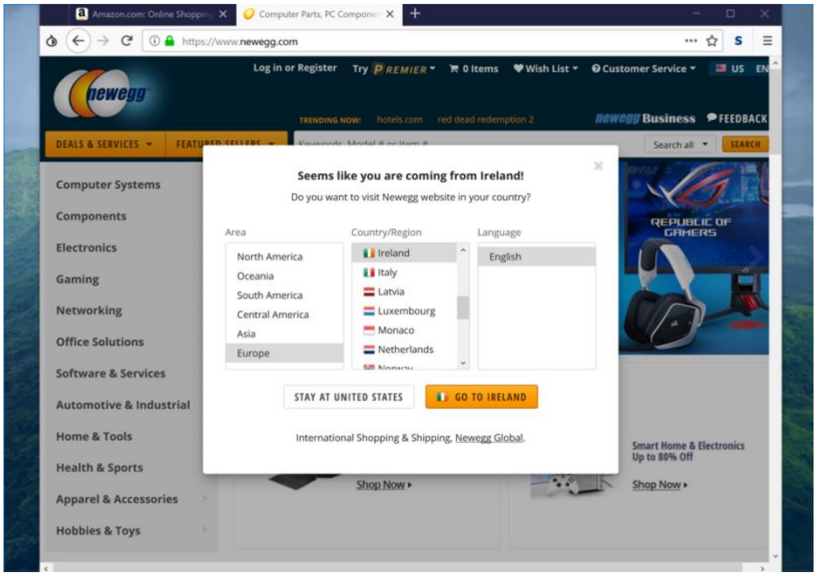
Advanced

- Name Address: cust-etsu-71-137.mounet.com
- Remote Port: 29368
- Browser: Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36

Ipchicken.com Google Chrome, image #2

connection are shown in image #2. The physical address of the Google Chrome displayed by ipchicken is Cust-etsu-71-137.mounet.com. This shows that ipchicken can see the user-specific information about this connection but also that the Tor browser was spoffing the ipaddress. After this step, the application Tor browser was again opened, and the onion was selected. This will display a dropdown and one of the options will be "new identity" and that option was selected. This selection will require the browser to restart, and when it does it will have acquired a new iPaddress and it was 83.71.173.24.

Within the Tor browser, the website Newegg.com was navigated to. This provided an explicit representation of how well this application does its job. The results of this step of navigating to Newegg.com are shown by image #3. The browser thinks that the windows 10 system is coming from Ireland, but in reality it is operating in a computer lab in northeast Tennessee.


https://www.newegg.com

Seems like you are coming from Ireland!

Do you want to visit Newegg website in your country?

Area: North America, Oceania, South America, Central America, Asia, Europe

Country/Region: Ireland, Italy, Latvia, Luxembourg, Monaco, Netherlands

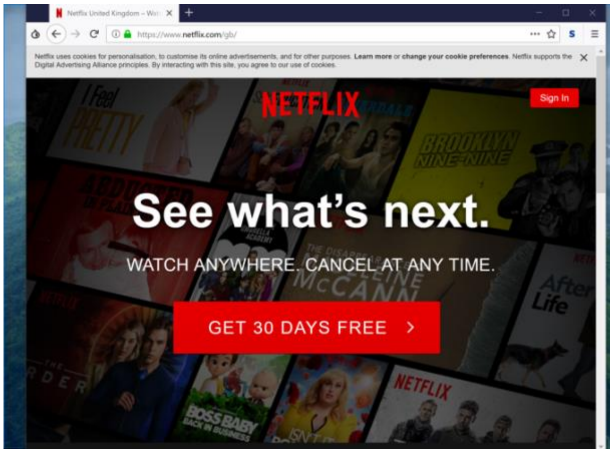
Language: English

STAY AT UNITED STATES | GO TO IRELAND

International Shopping & Shipping, Newegg Global.

Newegg.com Tor Browser, image #3

In a similar manner to how Tor confused Amazon.com, Tor was also able to confuse Bing.com, Netflix.com, and Apple.com by spoofing the ipaddress. This results of browsing to these three different websites are shown by images # 4, 5, and 6. In all three of these situations, the websites showed prompts for the interface language to be changed to fit the supposed area, this is shown in the top of the browsers in each image.

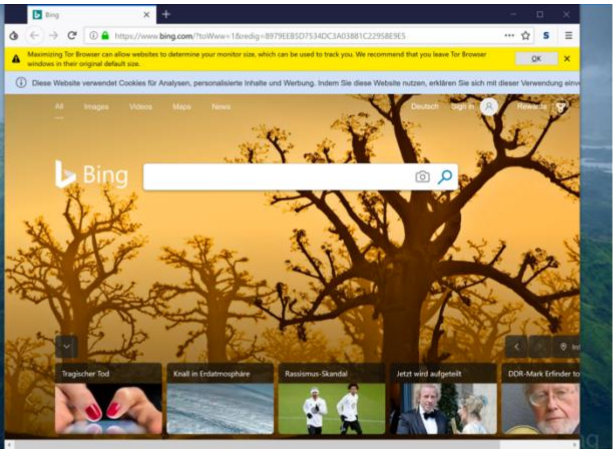

https://www.netflix.com/gb/

Netflix uses cookies for personalisation, to customise its online advertisements, and for other purposes. Learn more or change your cookie preferences. Netflix supports the Digital Advertising Alliance principles. By interacting with this site, you agree to our use of cookies.

See what's next.

WATCH ANYWHERE. CANCEL AT ANY TIME.

GET 30 DAYS FREE

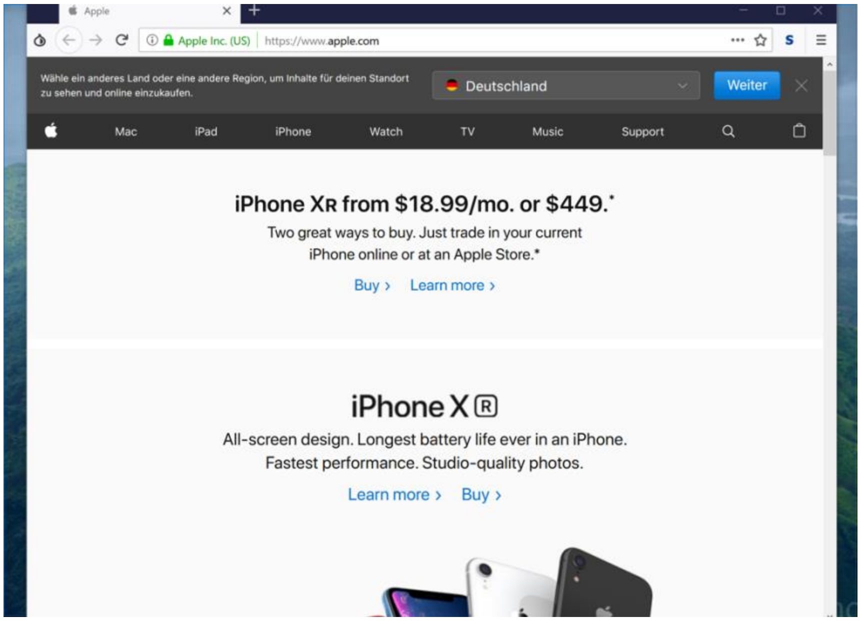

https://www.bing.com/?toWww=1&redig=8979EEB5D7534DC3A03881C22958E9E5

Maximizing Tor Browser can allow websites to determine your monitor size, which can be used to track you. We recommend that you leave Tor Browser windows in their original default size.

Diese Website verwendet Cookies für Analysen, personalisierte Inhalte und Werbung. Indem Sie diese Website nutzen, erklären Sie sich mit dieser Verwendung einv

Netflix.com Tor Browser, image #4

Bing.com Tor Browser, image #5



Wähle ein anderes Land oder eine andere Region, um Inhalte für deinen Standort zu sehen und online einzukaufen.

iPhone XR from $18.99/mo. or $449.*

Two great ways to buy. Just trade in your current iPhone online or at an Apple Store.*

Buy › Learn more ›

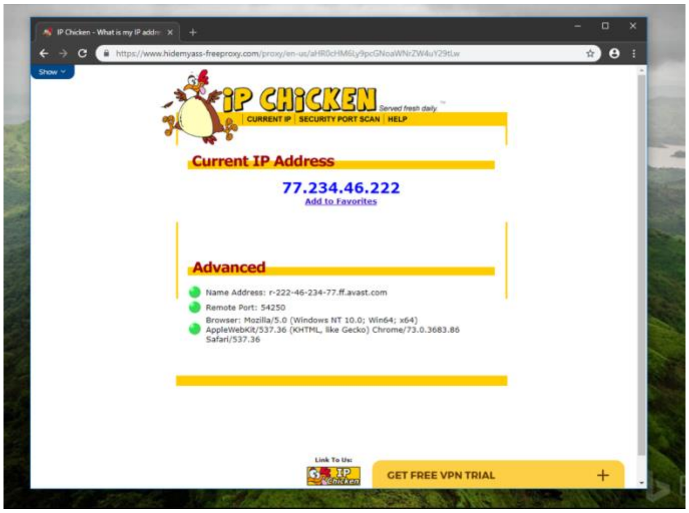
iPhone XR

All-screen design. Longest battery life ever in an iPhone. Fastest performance. Studio-quality photos.

Learn more › Buy ›

Apple.com Tor Browser, image #6

After considering the affects that Tor was able to have on the internet sites by spoofing the ipaddress, a comparison between the Tor browser and the internet proxy hide.me was completed. This test was designed to look for differences achieved by implementing one privacy measure over the other. This test was done by navigating to the site hide.me within google chrome and then within hide.me's proxy to ipchicken.com. Image #7 shows how the proxy was also able to change the ipaddress.


IP Chicken - What is my IP addr
https://www.hidemyass-freeproxy.com/proxy/en-us/aHR0cHM6Ly9pcGNoaWNrZW4uY29tLw
Show
IP CHICKEN
Served fresh daily
CURRENT IP
SECURITY PORT SCAN
HELP
Add to Favorites
Link To Us:
GET FREE VPN TRIAL

Current IP Address

77.234.46.222

Advanced

- Name Address: r-222-46-234-77.ff.avast.com
- Remote Port: 54250
- Browser: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.86 Safari/537.36

ipchicken.com in the proxy hide.me, image #7

4. Observations

"The Onion Browser", better known by the abbreviation Tor, provides an internet browser with the primary purpose of keeping the user's data anonymous. This feature of providing an avenue for secure private communications between computers assists individuals in numerous ways. Tor is utilized by journalists, spies and also a host of dark web corporations. This browser provides unique opportunities for each group mentioned above and it attracts the different people for verifying reasons.

Tor provides an avenue for reporters to communicate with the outside world without coming under the scrutiny of their oppressive governments. This happens in several countries there are very restrictive laws about the publication of news articles. Reporters under these kinds of oppressive leadership have started creating news sites on Tor to release news about the current situations of the country with the provided anonymous capabilities gained through The Onion Browser.

This anonymous browser is also used by some government agencies to track down acts of cybercrime by infecting Tor web pages adds with malware and then using that to track down the users. This type of infiltration of Tor would likely be done by large government security agencies like the FBI, and NSA. This use case is out of the standard purpose of the Tor browser, but it is none the less a valid use of the application.

And there is obviously the use of this anonymous browser for illegal or "Dark Web" actions that individuals or organizations would like to participate in without being exposed. This may be the most known use of Tor and similarly, it is one of the primary reasons that people would consider an application like Tor, but contrary to that popular belief only about 4% of Tor users are doing shady or illegal things on the browser. This was highlighted by The Tor Project in a lecture called "Understanding Tor Onion Services and Their Use Cases - HOPE XI 2016".

Although Tor does provide internet privacy through anonymous connections it has several serious weaknesses. As noted above Tor users are vulnerable malware infections from government security organizations that are trying to track down suspects. This is a huge vulnerability of Tor because it breaks one of the browser primary purposes and that is concealing and protecting the users with anonyms measures. Another vulnerability was discovered with Tor by MIT researchers that discovered a way to crack the algorithms that the data is encrypted by. This is noted by Darrow, Barb in his article about how the browser Tor may be losing its anonymity. In this article MIT researchers discovered that by analyzing the internet traffic with machine learning they were able to determine what traffic belonged to the Tor servers and also whether it was "ordinary Web-browsing circuit, an introduction-point circuit, or a rendezvous-point circuit." (Darrow 1) This means that Tor is vulnerable to BGP attacks as of numerous kinds if the data is accessible like the MIT researchers have found.

Internet proxy's and the Tor browser both provide security measures for internet traffic, but this section will determine which provides the fullest security. To accurately determine which service is more secure an evaluation of pros will be made for both solutions. After considering the security measures provided by each service, a judgment will be made as to which is the most secure.

Firstly, the application Tor will be considered for its security benefits. The basis for the anonymity that Tor provides is based on the feature of routing and encrypting user data that it accomplishes. This process of routing user data is done by Tor servers connecting in a chain of three between the user and the internet server that they are accessing. The security measures gained by Tor come into play at this point for the fact that there is encryption happening between every server communication throughout a Tor system. This means that all the data at each point of the communication sequence is encrypted and therefore is unreadable without the decryption key and also untracable. This point to point strategy of encryption and rerouting the data through all the different servers provides secure anonymity for the user.

Secondly, internet proxy's supply numerous features that allow for greater user security. Proxy's provide filtering and protection similar to that a firewall would on all data that is forwarded through them. This feature gives the user the security of a basic firewall. An internet proxy, similar to Tor, changes the users ipaddress to provide security and a level of anonymity. What makes the ipaddressing of a proxy different than that of Tor is that a proxy actually changes the ipaddress and passes it on to the web server, whereas the Tor spoofing just passes it along in an encrypted and unreadable way. Like the Tor Browser proxy servers encrypt all the data that travels through them which also provides another level of security.

Both of these options provide measures of security and protection, but it is evident that an internet proxy server provides security features that surpass the abilities of the Tor. A proxy server supports the ability to change the ipaddress instead of just spoofing it the way Tor does. The feature of a basic firewall protection provided by an internet proxy again overwhelms the security provided by Tor. For these reasons and by the clear explanations a internet proxy server provides greater security then the Tor browser.

5. References

The Tor Project, *Understanding Tor Onion Services and Their Use Cases - HOPE XI 2016*, Web May 27, 2018, accessed March 25, 2019. https://darkwebnews.com/anonymity-tools/tor/understanding-tor-onion-services-use-cases/

Darrow, Barb. *Vulnerability could make Tor, the anonymous network, less anonymous*, July 2015. Web accessed March 25, 2019. http://fortune.com/2015/07/29/tor-vulnerability/