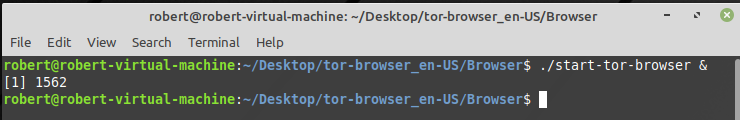
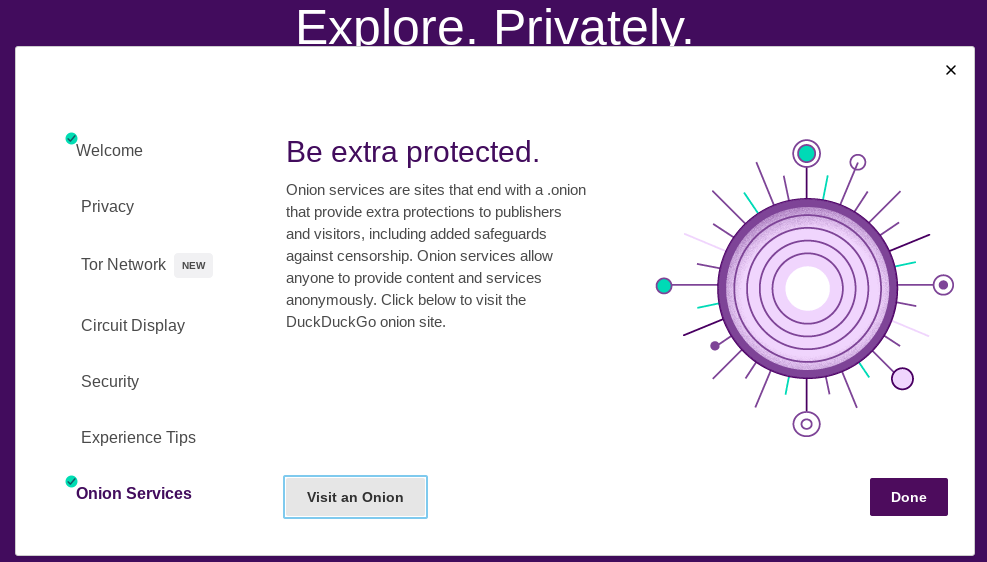
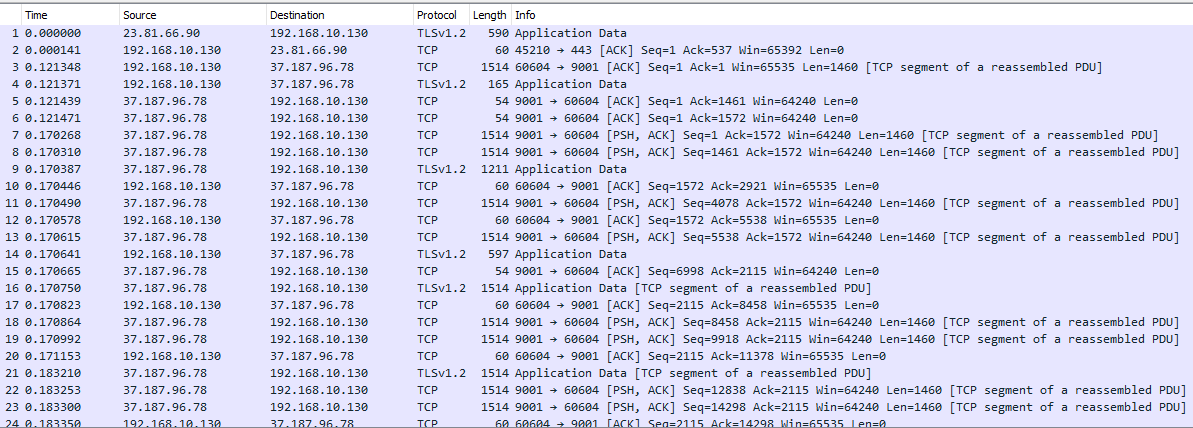
Step 1) Installing TOR in my virtual machine



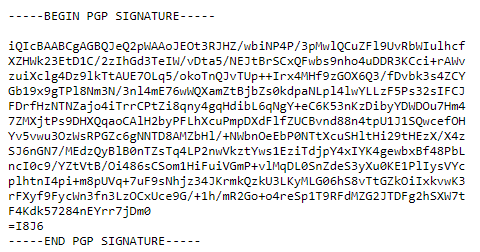


Step 2) Examining the TOR is package using Wireshark



TOR is using the port 9001 and the IP is 37.187.96.78, in which is locate in France.

Step 3) Check the Signature



Questions:

**What are signatures?**

Signatures or digital signatures refers to authentication of a file, text, email etc.

**Why do companies use them?**

It’s important for companies because files over the internet can be altered for malicious intentions. If a file is altered the authentication method fails. It allows companies to detect whether a file was corrupted or not.

**Why would you need to check a signature before downloading and installing a program?**

It’s important to check the digital signature of a program to see if the application comes from the original source. If the authentication method fails as I mentioned, it means that the file was altered by an unknow individual.

**What is a tor?**

TOR is a browser that allows us to surf the web anonymous. When we use web browsers such as Google Chrome and Internet Explorer, we leave traces behind. Such data is important for third companies to study our algorithms in the internet. TOR hides our traces and blocks cookies for a more secure way to surf the web.

**Why is it used?**

When we use search engines as “Google” or when we visit a website, our activity is recorded. With such information, they target us with advertisement, or they may sell our private information to third party companies without our concern. However, TOR is a browser that blocks incoming “cookies” from websites trying to collect our information. It allows us to navigate the internet anonymous by using P2P encrypted connection.

**How is a tor different than a VPN?**

TOR hops between three or more nodes, and the final node (which is the exit node) reveals the host IP. A VPN is faster because it hops to one single node and then assign the host a different IP. However, TOR is more unanimous than a VPN. A VPN knows your real IP and it’s up to the user to trust the company. TOR is just for browsing actibity, while a VPN encrypted our entire connection.

**What happened when you installed the TOR?**

When I used TOR for the first time, I noticed that some website was denying me the access of their contents because TOR was blocking their cookies policy.

**What is your traffic doing now?**

When I use TOR the port 9001 or 597 opens, and a random IP 37.187.96.78 is in use



**Are you protected?**

Using TOR adds another layer of protection to our activity when surfing the web. However, I don’t feel fully protected. The end node can still see the host activity.

**Do you still need to be careful while browsing the Internet?**

Yes, I need to be careful while browsing the internet, A VPN or using TOR doesn’t guaranteed full protection. The best way to be protected is to not use the internet at all.

**Can you do secure transactions (such as paying a credit card) safely from anywhere if you're connected while using the TOR?**

No, because TOR is a P2P network-oriented network, and you don’t know who’s behind the other end.

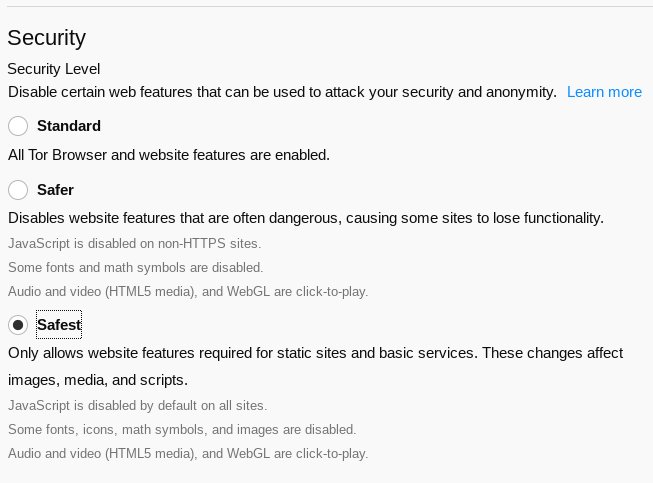
**Why do you need to use the browser bundle?**

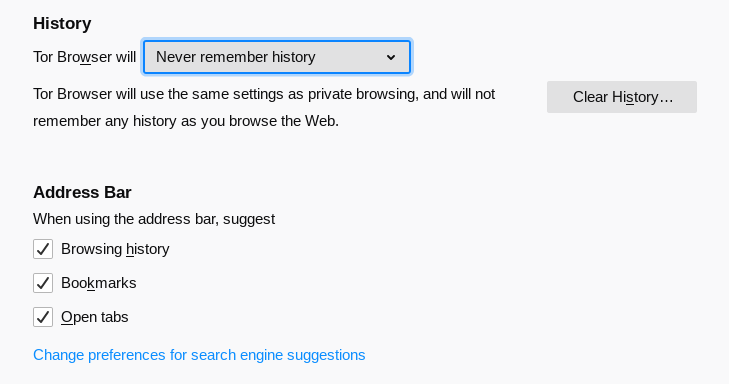
The browser bundle is a portable TOR browser that can be install in a USB. It’s useful if you want to surf the web anonymous without using your main pc or if you want to navigate the web in a public Wi-Fi connection.

PRIVATE BROWSING

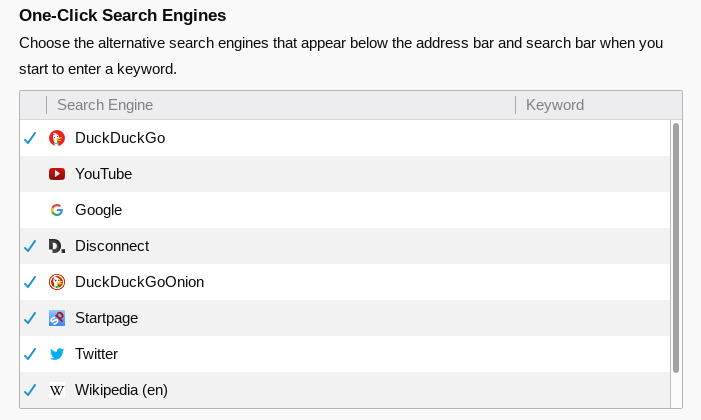
**Name at least 3 changes you could make to your browser/configuration/preferences/etc that would make you more anonymous online.**

First thing I did was to change the security level to the ‘Safest’.



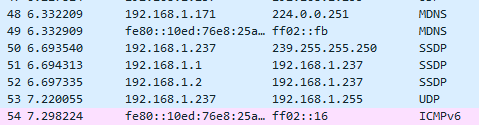
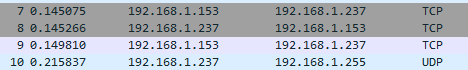
2) I choose the option to “Never Remember History” 

3) I disabled Google as an alternative search engine



Wireshark:

**1. List up to 10 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.**



**2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet listing window is the amount of time, in seconds, since Wireshark tracing began.**



According to the picture 426.209365 - 426.203219 = **0.006146 seconds**

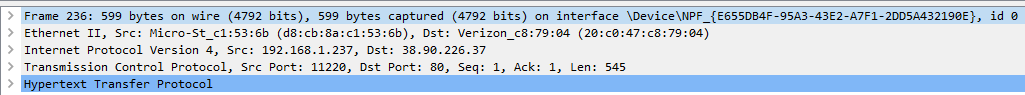
**3. What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.cs.umass.edu)? What is the Internet address of your computer?**



According to the picture the address of gaia.cs.umass.edu is **128.119.245.12**

My internet address 192.168.1.237

**Print the two HTTP messages displayed in step 9 above. To do so, select Print from the Wireshark File command menu, and select “Selected Packet Only” and “Print as displayed” and then click OK**.

Get: 

OK: 

