# 14-741: Homework 4

## Assigned: Monday November 23, 2015

**Due: Monday December 7, 2015**

**Name: Vishruta Rudresh**

**Andrew ID: vrudresh**

**Scores**

**Problem 1 (70 pts max):**

**Problem 2 (30 pts max):**

**Total (100 pts max):**

**Guidelines**

* Be neat and concise in your explanations.
* Use the assignment template for written answers.
* Please check your English. You won’t be penalized for using incorrect grammar, but you will get penalized if we can’t understand what you are writing.
* Proofs (including mathematical proofs) get full credit. Statements without proof or argumentation get no credit.
* There is an old saying from one of my math teachers in college: “In math, anything that is only partially right is totally wrong.” While I am not as loathe to give partial credit, please check your derivations.
* **This is not a group assignement. Feel free to discuss the assignment in general terms with other people, but the answers must be your own.** Our academic integrity policy strictly follows http://www.ini. cmu.edu/ini\_files/docs/policies/MS25\_INIStudentHandbook.pdf, section IV-C.
* Write a report using your favorite editor, and submit it using Blackboard before class on the due date. Late submissions incur penalties as described on the syllabus (first you use up grace credits, then you lose points). **Only PDF submissions will be graded.**
* Post any clarifications or questions regarding this homework in Piazza.
* Good luck!

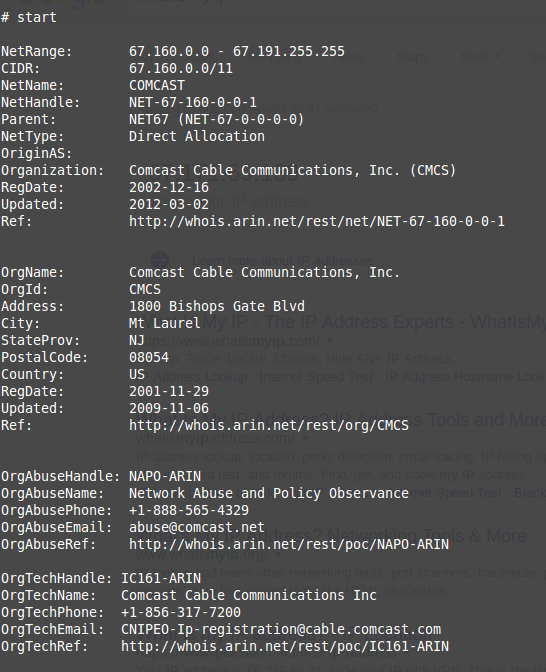
# Using Tor (70 pts)

## Preliminaries

1. (5 pts) (Before starting Tor) What is your public IP address? Show the output of a whois query on that address.

**Public IP address: 67.171.69.139**

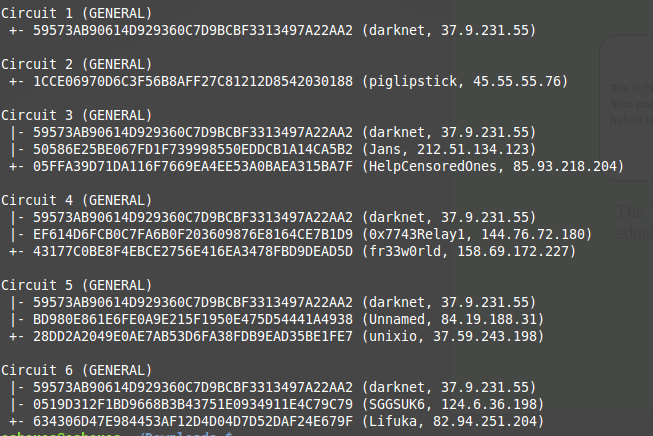
**Output of whois query**



2. (10 pts) Provide a Python script that, using the Stem library, displays:

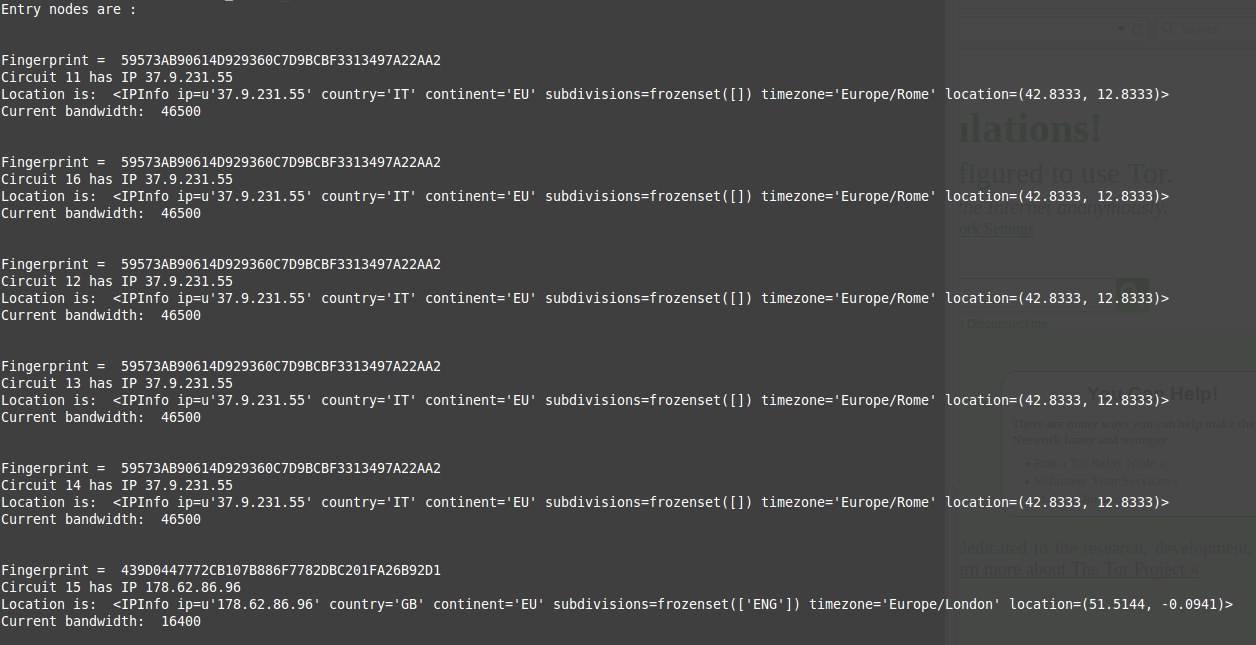
(a)A list of all Tor circuits your machine currently uses, as specified by the list of three Tor relays. An entry should look like “entry node–middle node–exit node.”

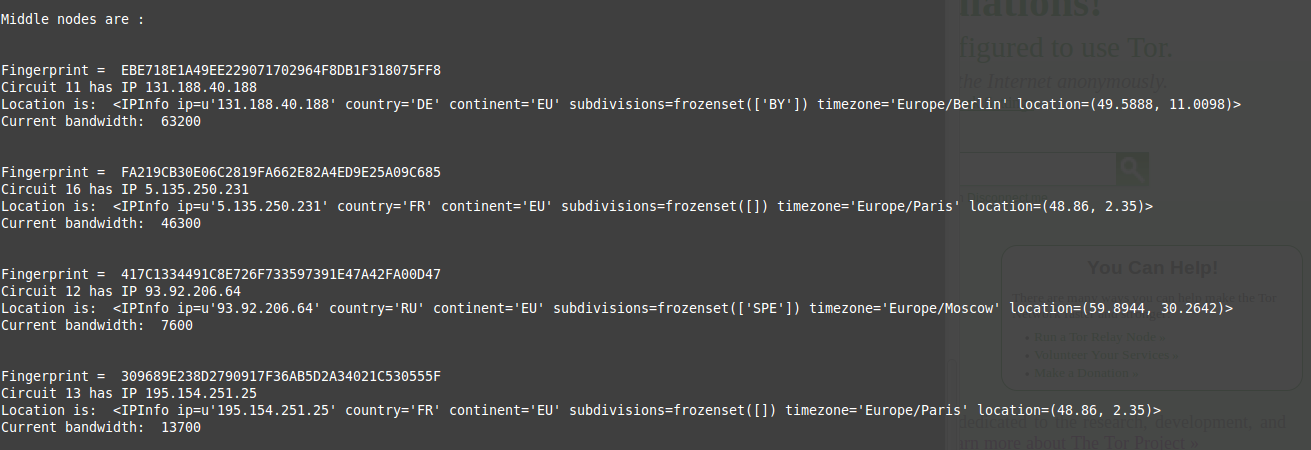
**Output: python q\_112a.py**

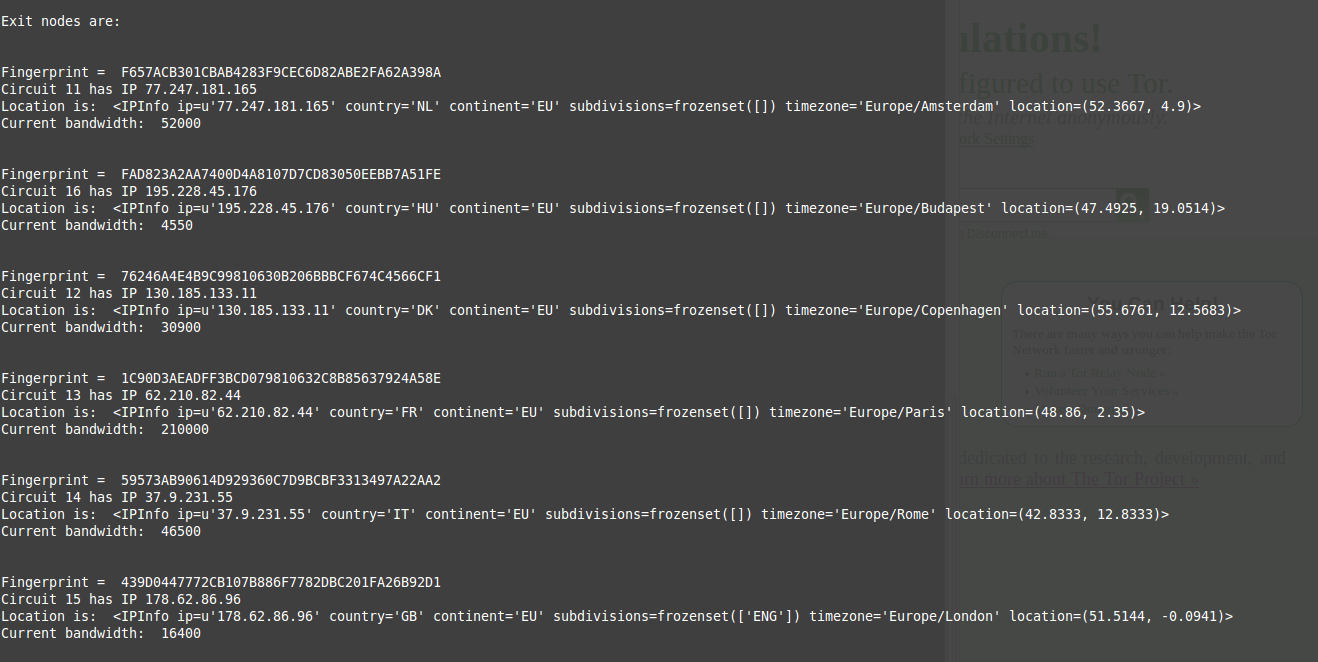


* + 1. For each circuit:
       - The IP address of each relay in the circuit
       - The location (country) of each relay
       - The current bandwidth of each relay Provide both your python script **and** its output.

**Output: python q\_112b.py**



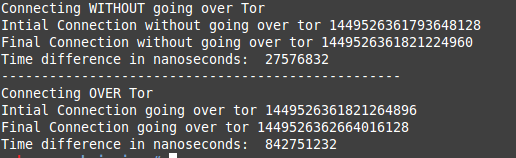




## Measuring latencies

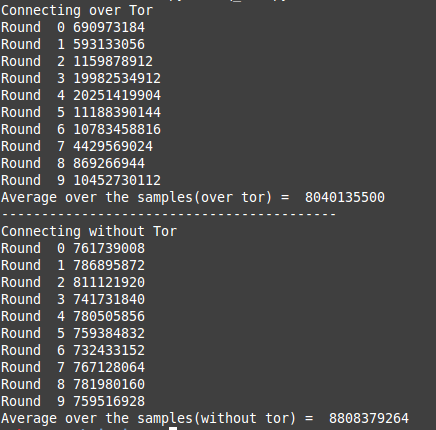
1.(10 pts) Write a small toy program in Python that 1) directly connects to a webserver without going over Tor, and then 2) connects to the same webserver but going over Tor, and 3) measures the difference between response times. Please include the source of your program in your handout.

**Output**: python q\_1121.py

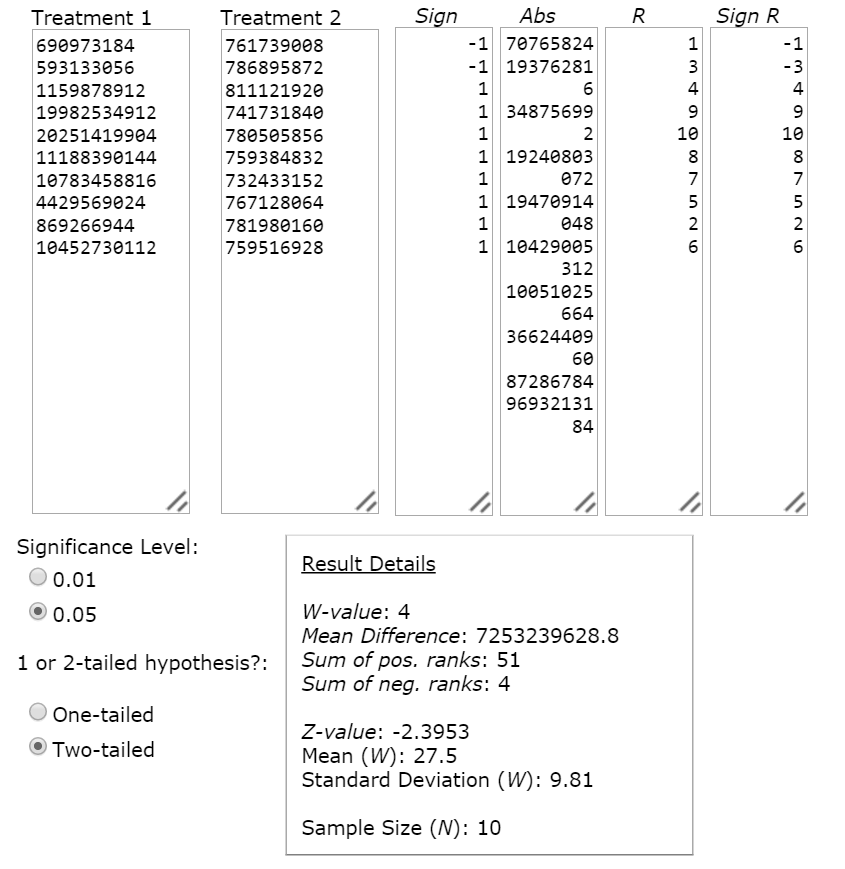


1. (10 pts) Give an estimate figure of how much overhead in latency Tor generates on a given connection using the above program. Run the above experiment 10 times, changing Tor identities (and thus, circuits) but connecting to the same website for each of the 10 runs, and provide a table summarizing the results. Do you see statistical significance (use an appropriate, non-parametric statistical test and report critical values)?

**Output: python p\_1122.py**



**Statistical significance as calculated over the sample space provided above and using the website: http://www.socscistatistics.com/tests/signedranks/Default2.aspx**



*Result 1 - Z-value*

The Z-value is -2.3953. The p-value is 0.0164. The result is significant at p≤ 0.05.

*Result 2 - W-value*

The W-value is 4. The critical value of *W* for *N* = 10 at p≤ 0.05 is 8. Therefore, the result is significant at p≤ 0.05.

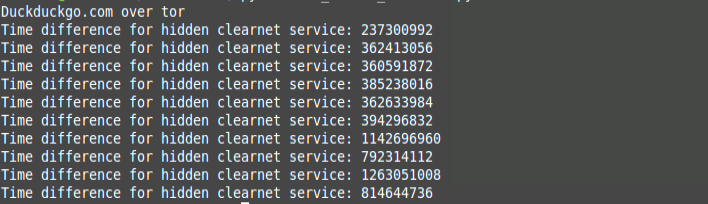
3. (10 pts) Now, connect to the Tor hidden service [http://3g2upl4pq6kufc4m.onion/,](http://3g2upl4pq6kufc4m.onion/) and measure the latency of connecting to that website. Compare it to the latency to its “clearnet” version https:

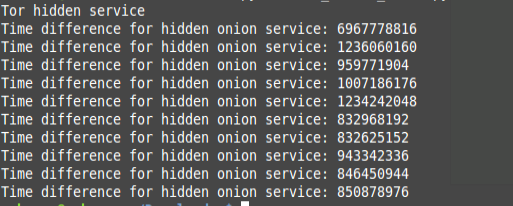
//duckduckgo.com/ using the Tor network, and bypassing the Tor network.

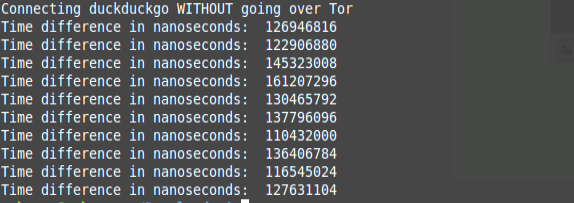
Run that experiment 10 times with ten different identities and report the following results.

**Output**:

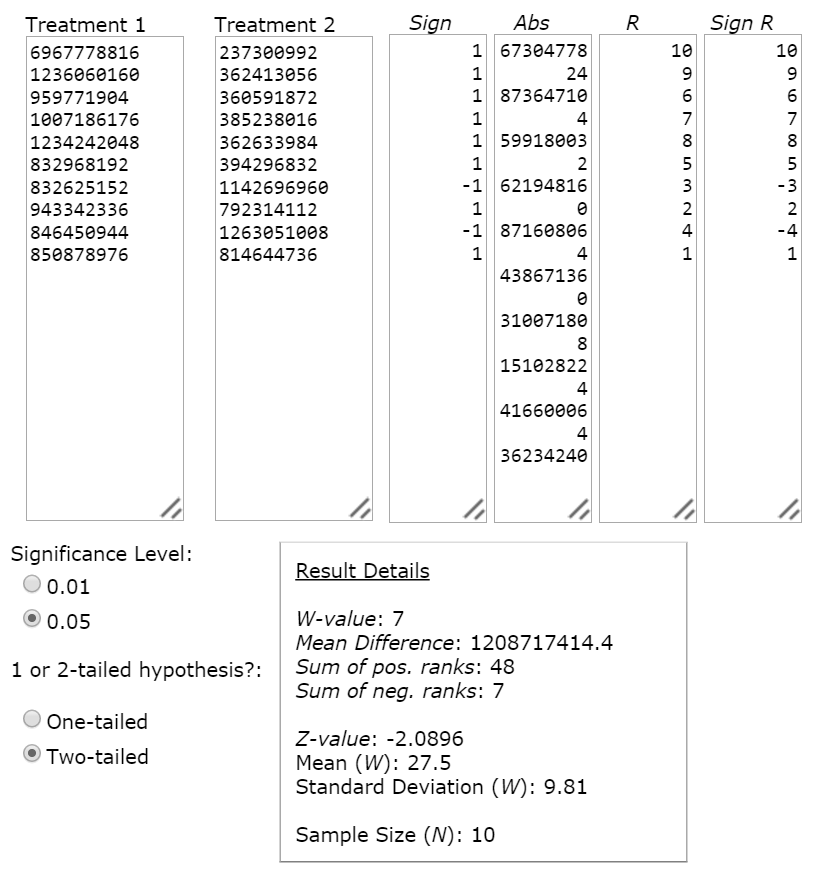
1. Python over\_tor\_duck.py
2. Python tor\_hidden\_onion.py
3. Python not\_over\_tor\_duck.py







Do you observe a statistical difference between latencies to the hidden service, and latencies to the same webserver in the clearnet going over Tor? - Yes, Hidden services is on the left column and the duckduckgo site over tor on the right column



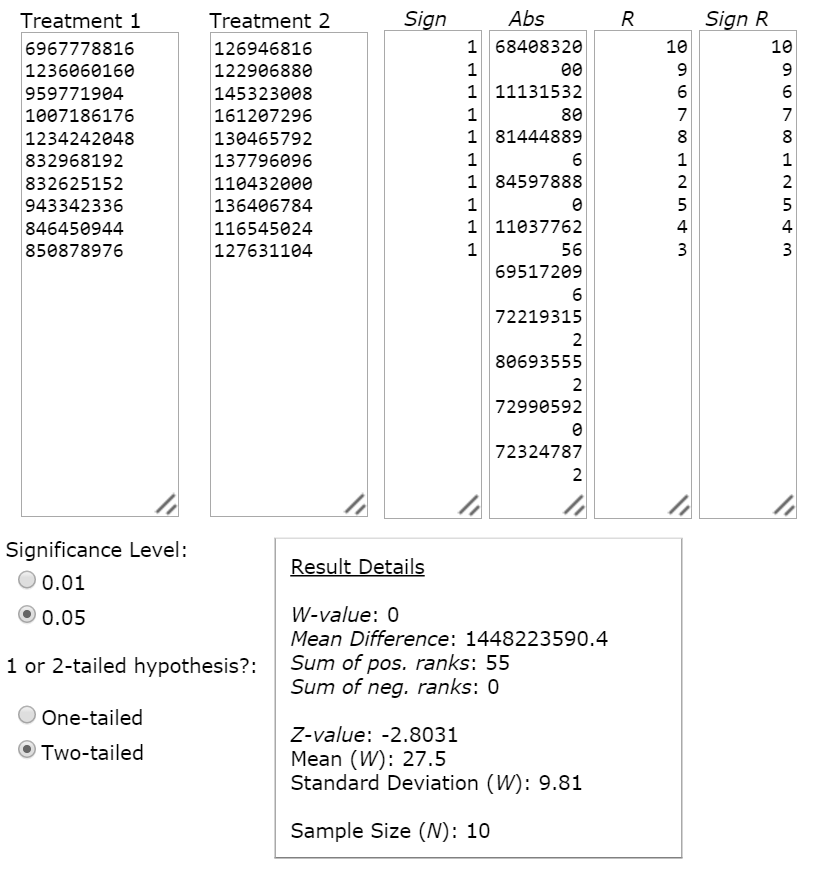
*Result 1 - Z-value*

The Z-value is -2.0896. The p-value is 0.03662. The result is significant at p≤ 0.05.

*Result 2 - W-value*

The W-value is 7. The critical value of *W* for *N* = 10 at p≤ 0.05 is 8. Therefore, the result is significant at p≤ 0.05.

Between latencies to the hidden service and latencies to the same server in the clearnet not going over Tor? - Yes, Tor hidden services on the left column and duckduckgo site not going over tor on the right hand column



*Result 1 - Z-value*

The Z-value is -2.8031. The p-value is 0.00512. The result is significant at p≤ 0.05.

*Result 2 - W-value*

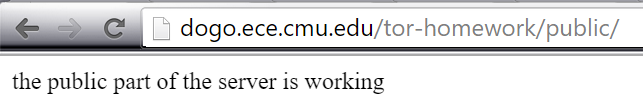
The W-value is 0. The critical value of *W* for *N* = 10 at p≤ 0.05 is 8. Therefore, the result is significant at p≤ 0.05.

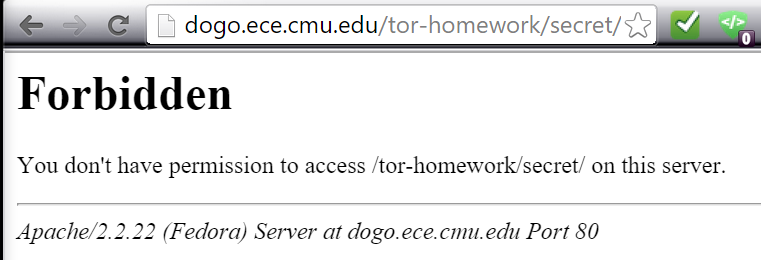
Finally, explain why the hidden service address does not use https: the probably reasons include:

1. The need for https does not arise as Tor hidden services encrypts traffic end-to-end, similar to that of https.
2. Tor hidden services contains a hash of the server public key and hence, there is no dependency on a certificate authority, an authority https is reliant on. Hence, tor hidden services does not need or use https.
3. https are reliant on DNS servers and are hence susceptible to DNS attack. Tor hidden services do not need DNS server as they are anonymous networks that relay across the network node by node, hence Tor hidden services do not use https and hence are also not susceptible to DNS attacks.

## Using exits to circumvent censorship

1. (5 pts) Try to connect to <http://dogo.ece.cmu.edu/tor-homework/public/> and http:// dogo.ece.cmu.edu/tor-homework/secret/ using a regular browser. How different are the results?





1. (10 pts) To circumvent this “block,” you will attempt to force the use of specific exit nodes. Write a Stem script to constrain Tor to specific exits in different countries. Provide your Python/Stem script in your handout.

Answer: python test.py

1. (10 pts) Use your script to find as many countries as possible in which the website [http://dogo.ece.](http://dogo.ece/) cmu.edu/tor-homework/secret/ is *not* blocked. Provide a list of these countries, as well as the exact date/time at which you made each request verifying that each of these countries was not blocked.

Answer: Fr, HU, NL, DK

Important note: we are logging all requests to the server and have reasonably good fingerprinting techniques. So, we can probably tell whether or not you are cheating on the exercise... so don’t cheat! (One program per person, and don’t run your program for friends...) Also try to be considerate of others and do not flood the server with requests. (Attempting to hack into the server, it goes without saying, would be a major academic integrity offense, and would be treated as such.)

# WikiLeaks and anonymity (30 pts)

**Answer:**

My stance is for not banning the design and use of anonymous networks. Anonymous networks tend to provide the privacy that everyone desires. It is true that anonymous networks brews cybercrime and cyber-criminal activities, such as child pornography, selling of drugs online (silk route) , human trafficking and other illegal activities and that the anonymity makes it all the more difficult for government law agencies to catch these criminals, but the benefits of an anonymous network outweighs this tradeoff.

Firstly, the world we live in is conservative and does not support and could be dangerous to make certain statements, or have certain opinions or lifestyles. Hence, anonymity becomes important for discussions involving sexual abuse, minority issues, harassment, sex lives, and many other things. Additionally, anonymity is useful for people who want to ask technical questions that they don't want to admit they don't know the answer to, report illegal activities without fear of retribution, and many other things. Hence, anonymity uploads the sanctity of witness protection programs, child protection services by allowing users to anonymously report crime and violence alike. Imagine, if the identity of the user is revealed to the criminal whom the user reported, the user’s life could be in danger. The reporting user’s family and friends could be in danger. Anonymous network helps prevent such situations.

Secondly, it is also encouraged by doctors, for patients to communicate to someone about their illness or how they feel about it so as to relieve them of their tension or distress. However, such patients are usually reluctant to communicate openly and publicly for the fear of being judged and ridiculed and hence would prefer to communicate anonymously. Therefore, anonymous networks would be a huge boon to people who would prefer to communicate anonymously, patients and the elderly alike. If not for communication, people in general could use anonymous networks for voting online. One’s political stance need not be revealed to anyone.

Thirdly, Anonymity is a basic necessity to uphold “freedom of speech” without being subjected to ridicule, censorships, abuse and social intolerance. One example that proves this point is the Charlie Hebdo attack, where 12 people were shot dead by an apparent militant Islamist group in Paris. Charlie Hebdo is a French satirical magazine that voiced its opinion on a Middle Eastern way of living and worship. To this, an Islamist group took offence and sought revenge by gunning down the editor and few other cartoonists working for the magazine stating that they have avenged their lord, the Prophet Muhammad. It is to be noted that, such incidents would have not occurred if such opinions were voiced anonymously. The Islamist group could not have targeted anyone or avenged anyone if the cartoonists were anonymous.

Lastly, but not the least, anonymity is the core for national intelligence communication, gathering and execution. Sensitive information regarding national security cannot be made public and if it is, it should be anonymous and should not come from the nation state as that would instill fear in the minds of the general populace of the nation state. Also, armed forces’ critical missions as spying on nation states, or terrorists should be kept a secret, because if revealed, it could lead to war between two nation states or a retaliation from the terrorist group. Sensitive information exchanged between parties in these critical missions need to be anonymous and secure. Hence, banning the design and use of anonymous network would be a huge burden to a lot of people.