Classwork 8

50.520: Systems Security

Anonymity and Privacy

Question 1

Install and configure the Tor software on your system.
For 50 randomly selected websites download the main pages using a console tool (e.g., wget or curl)

- with Tor, and
- without Tor (just native Internet connection).

Report observed latencies (min, max, average, and median) and draw a conclusion what is the latency introduced by the Tor network.
Show an evidence that your application is communicating via Tor (one screenshot from Wireshark is enough).

Question 2

Tor software is sometimes misconfigured such that applications use native Internet connections to conduct DNS resolutions and then Tor to communicate with servers. What kind of anonymity and privacy risks (and under what adversary model) such a misconfiguration introduces?

Question 3

Read about the PANOPTICLICK project (https://panopticlick.eff.org).
Test it with three browsers (selected by you), conducting the tracking test with the standard view and private/incognito view. Report obtained results.
Briefly describe how the most *secure* browser protects from tracking techniques? If there are some techniques that it does not protect from, please propose how the browser vendor could fix it.