x) Read and summarize (briefly, e.g. with some bullets)

**Shavers & Bair 2016: [Hiding Behind the Keyboard: The Tor Browser €](#);
subchapters: "Introduction", "History and Intended Use of The Onion Router",
"How The Onion Router Works", "Tracking Criminals Using TOR".**

- Tor browser is just modified Firefox browser

- Tor allows everyone without technical knowledge to use internet anonymously.

- Initially developed by US government, but then used mostly by anyone who
  legitimately wants to stay hidden online

- Tor makes the connection anonymous through random relays which add their
  own layer of encryption (like layers of "onion")

- Despite the protection that Tor provides, there are several cases where the
  anonymity when using Tor has been compromised

- The anonymity can be broken with man in the middle attacks, geolocation,
  comparing timestamps and other metadata and using vulnerabilities in
  documents, html etc.

**Quintin 2014: [7 Things You Should Know About Tor](#)**

- According to the article Tor is still very relevant when trying to stay
  anonymous online

- Tor is totally legit and not used only by criminals. No one has been prosecuted
  when maintaining a Tor relay

- Even though fast and easy to use, Tor is not foolproof

**a) Install [TOR browser](#) and access TOR network (.onion addresses). (Explain in
detail how you installed it, and how you got access to TOR).**

- I already had TOR installed on several devices. but if I would've done it on my
  Kali linux machine I would've followed this documentation:
  https://www.kali.org/docs/tools/tor/

## b) Browse TOR network, find, take screenshots and comment

First I connect to Torch search engine:
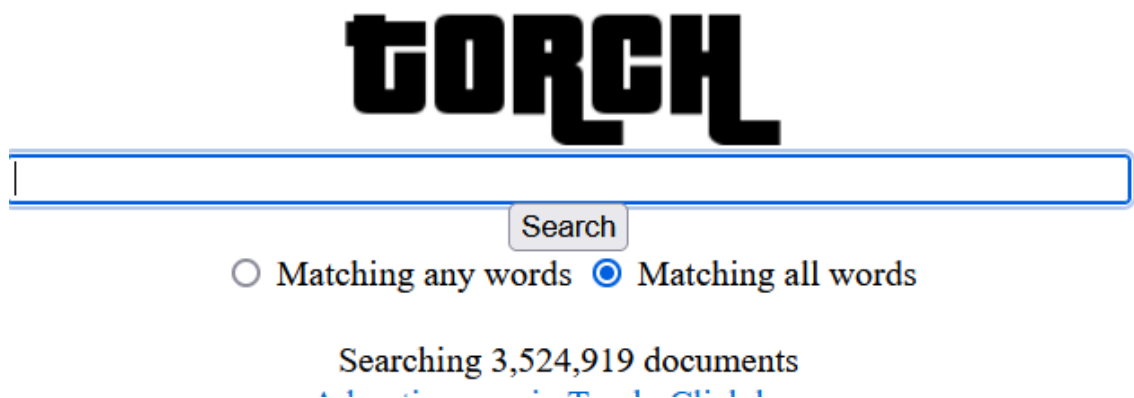
I've read many times that buying drugs from darknet is easy and available for anyone disregarding age or technical skills. I heard about this site called "tsätti" that's used for these purposes and I easily found the link to it from "normal internet" (torch couldn't help with this one). I connected to the site and saw indeed illegal substances being advertised:

I also visited a technology focused Wizardry and Steamworks forum:
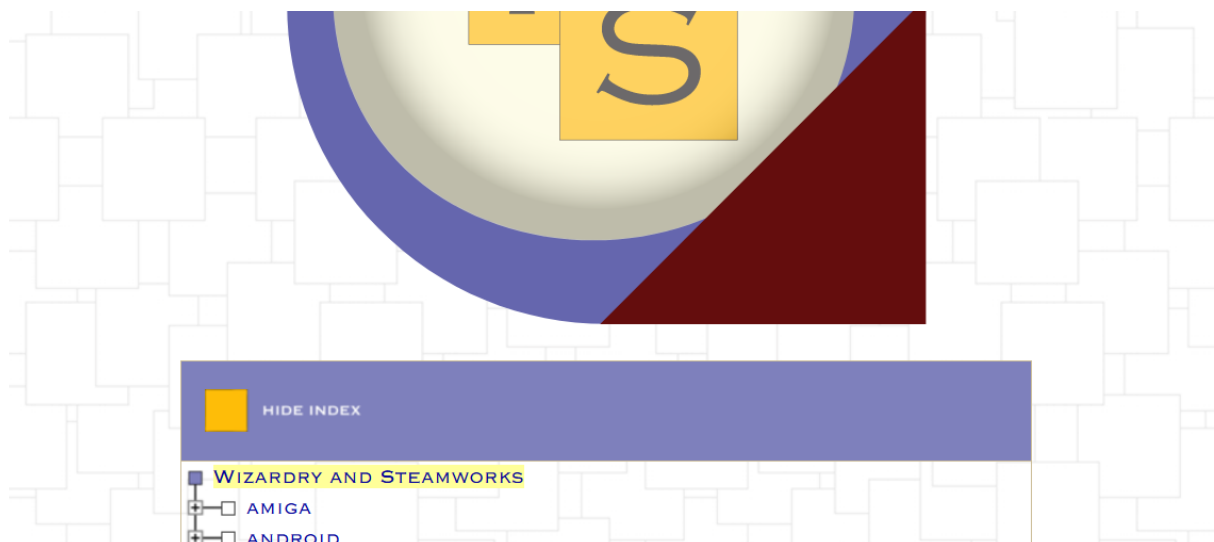
I visited WikiLeaks organisation page, didn't whistleblow anyone though:

c) In your own words, how does anonymity work in TOR? (e.g. how does it use: public keys, encryption, what algorithms? This subtask does not require tests with a computer.)

The anonymity when using TOR comes from the multi-layered encryption and the randomly chosen route of different relays that add these layers. All the relays that the connection passes through, only knows the previous relay and where the massage is being sent to.

Public key encryption is being used in the relays that have public and private keys. The data is encrypted with relays public keys and only they can decrypt the added encryption with matching private keys.

d) What kind of the threat models could TOR fit? (This subtask does not require tests with a computer.)

TOR is fitting technology to protect yourself against surveillance and location privacy. You can anonymise yourself from anyone who tries to track your internet usage.

Because of this it's also good technology for conducting sensitive activities that has to be hidden from bad governments or other malicious and corrupted institutions.

When using public networks or untrusted networks, TOR is a great tool for hiding your tracks.