Hani Mebar, **Assignment 6**
Haaga-Helia University of Applied Sciences
ICT4HM103-3004
07/12/2022

H6 Onion

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".

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

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

- search engine for onion sites
- marketplace
- fraud
- forum

c) In your own words, how does anonymity work in TOR? (e.g. how does it use: public keys, encryption, what algorithms?)

d) What kind of the treath models could TOR fit?

Answers

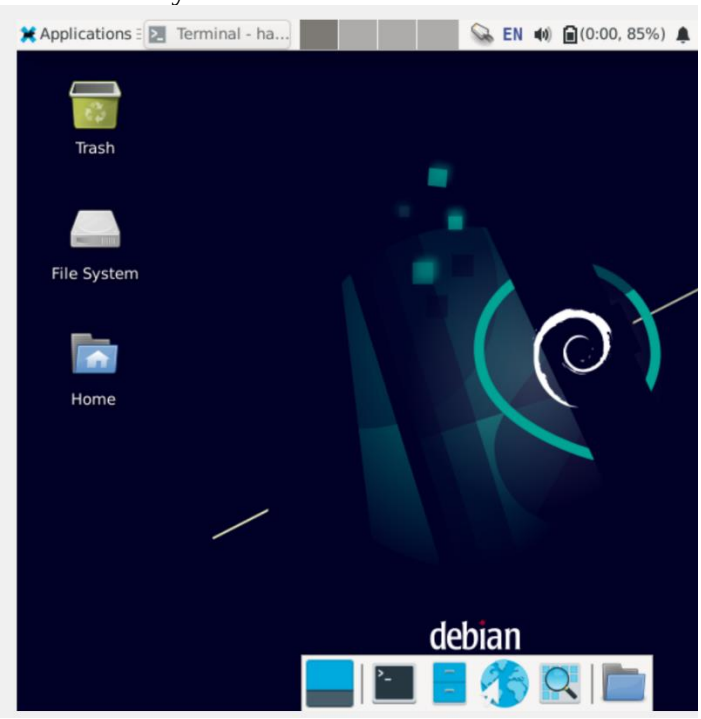
x)

- The book is about showing how covert communication is used in order to understand it better especially if a crime was committed using these techniques. So if you know the 'what' you can figure out the 'how'.
- The intended use of the Tor browser is for anonymous communication. It was created by the US government but is not under any control and can be update by anyone with a technical know-how.
- It can be used for virtuous reasons, like whistleblowing when something is being hidden by governments. It can help people communicate outside the detection of oppressive regimes and governments.
- Sensitive information that help bring justice to those in need can use Tor to communicate with open societies who bring their plight to the world.
- Where there is secrecy, there will be crime as well. Tor is used to sell drugs, weapons, services that include murder for hire, and for human trafficking.
- Tor (or the Onion Router) is a system that cannot be beaten, or at least it's very difficult. The way it works is that it removes a layer of encryption, appears like 3 (an entry, middle and exit) before it reaches the final recipient. If you want to find out where it came from you can't trace it because the nodes change every ten minutes.

- You cannot find browsing history on Tor especially when it's closed. Even if you happen across a computer with Tor browser open, you have a very short time to see where the user has been browsing.
- Biggest weakness in Tor is the human user who especially if they decide to customise their browser settings. Any change can leak information out including simple things like updating or adding a driver or add-on to be able to play a video (because it will need the real IP and therefore captures it).
- Attacks to deanonymize tor users include gaining control in as many entry points as possible, doing a middle man capture service attack (but even whole nations cannot do this),
- Only way to solve crime committed using Tor is with some form of luck or a 'break' in the case.

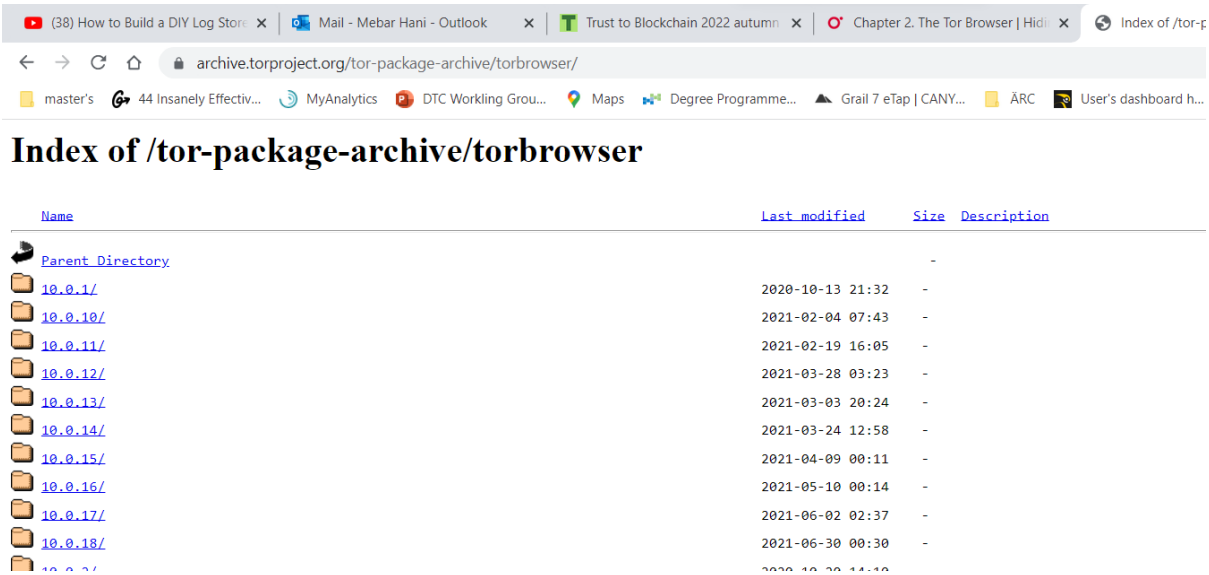
Installing Tor browser

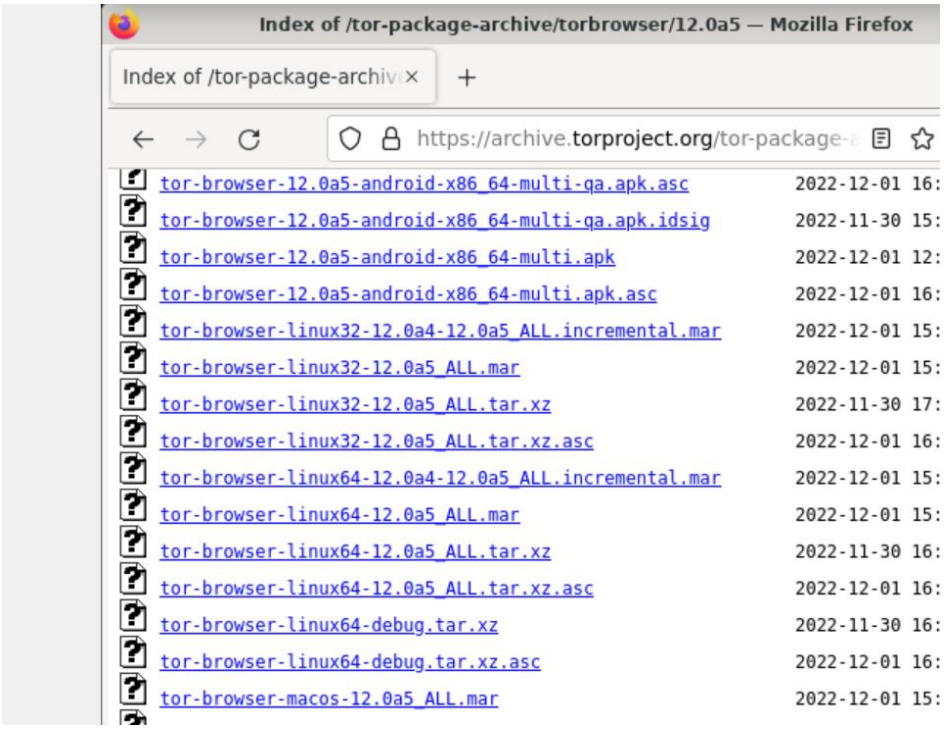
I went into my virtual machine first



Then I used the website which showed archived versions of Tor browsers which was in the book:
https://archive.torproject.org/tor-package-archive/torbrowser/

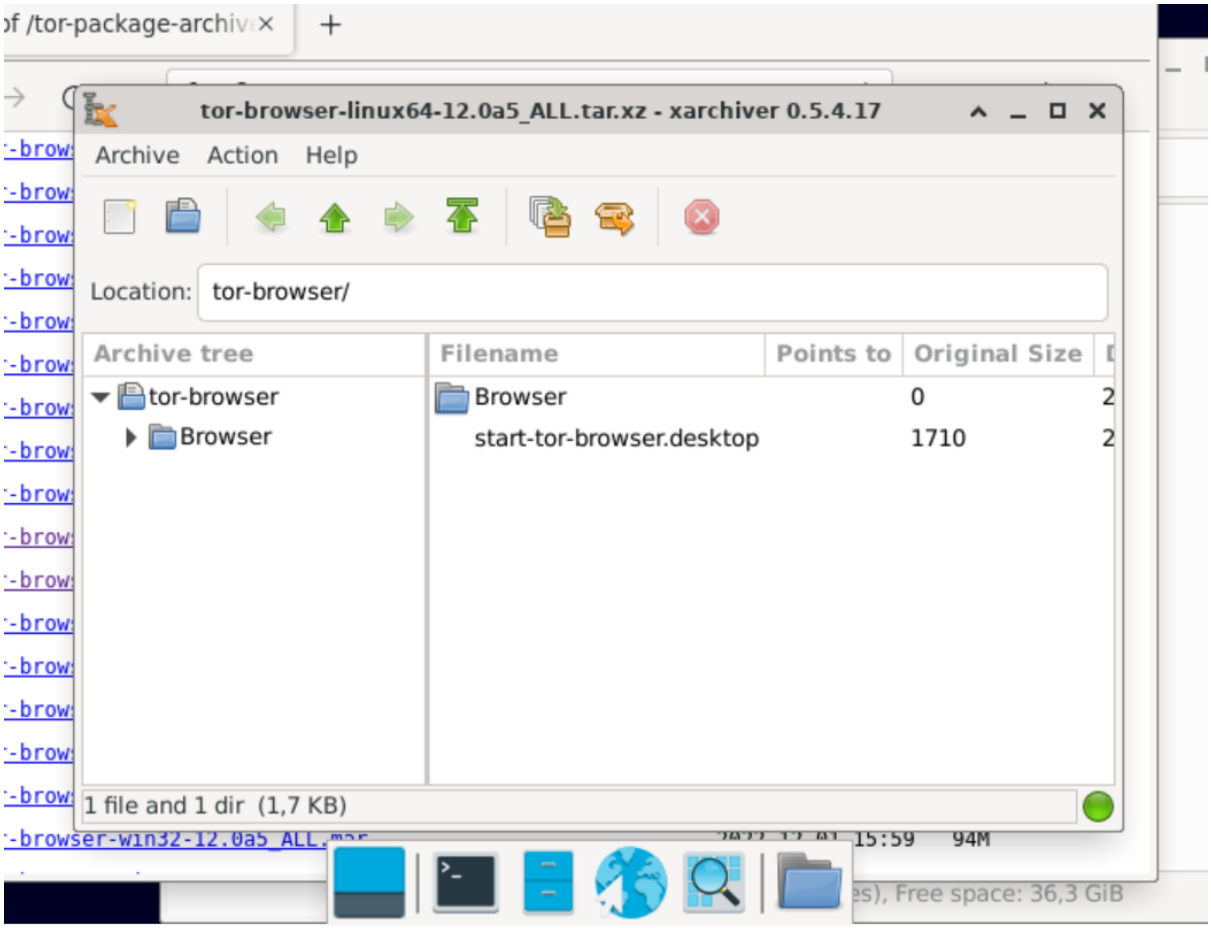
Hani Mebar, **Assignment 6**
Haaga-Helia University of Applied Sciences
ICT4HM103-3004
07/12/2022





I looked for the install file and selected the install 12-0a5_tar.xz file on the virtual machine which gave the below image

Hani Mebar, **Assignment 6**
Haaga-Helia University of Applied Sciences
ICT4HM103-3004
07/12/2022



I couldn't get it to open this way so I decided to check how to do it via apt-get in GUI.

First I ran sudo apt-get update then I installed with command sudo apt get tor -y

```
hanim@classVirtualMachine:~$ sudo apt-get update
[sudo] password for hanim:
Hit:1 http://deb.debian.org/debian bullseye InRelease
Get:2 http://deb.debian.org/debian bullseye-updates InRelease [44,1 kB]
Get:3 http://security.debian.org/debian-security bullseye-security InRelease
[48,4 kB]
Get:4 http://security.debian.org/debian-security bullseye-security/main Sour
es [172 kB]
Get:5 http://security.debian.org/debian-security bullseye-security/main amd6
 Packages [209 kB]
Get:6 http://security.debian.org/debian-security bullseye-security/main Tran
lation-en [135 kB]
Fetched 609 kB in 1s (669 kB/s)
Reading package lists... Done
hanim@classVirtualMachine:~$ sudo apt-get install tor -y
Reading package lists... Done
Building dependency tree... Done
```

but I still had no idea where the app was and how to run it, so unfortunately I just gave up on tasks a) and b) as I didn't want to run tor on my regular daily computer.

Hani Mebar, **Assignment 6**
Haaga-Helia University of Applied Sciences
ICT4HM103-3004
07/12/2022

c) in my own words, Tor is like that game at the parties where there would be an item (the message or file) is placed inside a box which gets wrapped in a layer of gift wrap (encryption). Then you keep adding many layers of the gift wrapping (hashes and more encryption) with every layer. During the party (the transferring of the message or file), you hand the big bundle of gifts with no idea how many layers of wrapping is on it (goes to many different nodes, or people at the party are tor network nodes). The music plays and you pass the wrapped gift around, and everytime the music stops you peel one layer off (this represents the message stopping at each node and removing one layer of encryption). Eventually a person gets the last layer removed and has the gift. Only difference is that no one would be able to see the gift and the number of players is much much larger so chances of the gift going to the same hands would be impossible or minimal.

D) I think 'threat' was misspelt because I could not find anything call treath. One possibility is like the recent case in Germany with fascist groups organizing to over-throw the government[i] , they can do this by remaining invisible to the police and commit their crime. Tor can be used as a way to share malicious codes between attackers anonymously globally or even locally, which could then be used and released on the intended target. Ransomware can be sold online. Drugs, even the bad ones, can be sold only anonymously.

[i] BBC, 2022, URL https://www.bbc.com/news/world-europe-63885028, accessed 07 December 2022