Part 1: Explore Tor

IP Address (before Tor): 199.111.225.130

IP Address (after Tor): 185.246.188.67, 2a0b:f4c2::13, 192.42.116.218

Website: https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion/

Part 2: Packet Sniffing

fcrackzip -l 6-6 -u -c a tcpdump.zip
pw == abcdez

What websites were visited that encoded the data using gzip?

ebay.com
wikimidedia.org.www
cn.com.www
slashdot.org
facebook.com
1e100.net.www

What types of files were transferred?

text/html
text/css
application/json
text/javascript

What network ports were accessed?

8080, 22

What is the username(s) and password(s) were used when logging in? Where were they used to log in to?

asb2t, rhubarb were used to log into pegasus

Can you determine my ebay password? Why or why not?

No, the information is encrypted.

What other network-level and transport-level protocols were used, other than TCP?

DDP, UDP