Tyler Kim

CS-3710

**Explore TOR**

IPv4 before Tor: 68.100.13.93

IPv4 after Tor: 192.42.116.25

Links:

<http://6nhmgdpnyoljh5uzr5kwlatx2u3diou4ldeommfxjz3wkhalzgjqxzqd.onion/>

<http://s4k4ceiapwwgcm3mkb6e4diqecpo7kvdnfr5gg7sph7jjppqkvwwqtyd.onion/>

<http://jgwe5cjqdbyvudjqskaajbfibfewew4pndx52dye7ug3mt3jimmktkid.onion/>

**Packet-Sniffing**

1. Encoded Websites

* Ebay.com
* Wikimedia.org
* Cnn.com
* W3.org
* 1e100.net
* Facebook.com
* Slashdot.org
* Akamaitechnologies.com
* Google.com
* Gstatic.com
* Wikipedia.org
* Fbcdn.net
* Turner.com
* Gstatic.com

1. Types of files
   * text
     1. html
     2. css
     3. javascript
   * image
     1. jpeg
     2. png
     3. gif
     4. x-icon
   * application
     1. json
     2. x-www-form-urlencoded
2. Network Ports Accessed
   * 8080
   * 53
   * 853
   * 139
   * 2896
   * 443
   * 80
   * 22
   * 3389
   * 5353
3. get username(s) and password(s)
   1. location: gemini.cs.virginia.edu
   2. usernames
      1. aaron
      2. asb2t
   3. password
      1. rhubarb
4. I cannot get the e-bay password because it seems to be handled on e-bay’s side and the actual text seems to be encrypted.
5. Application and transport layer protocols
   1. TCP
   2. UDP
   3. IP
   4. ICMP