Joseph Thornton

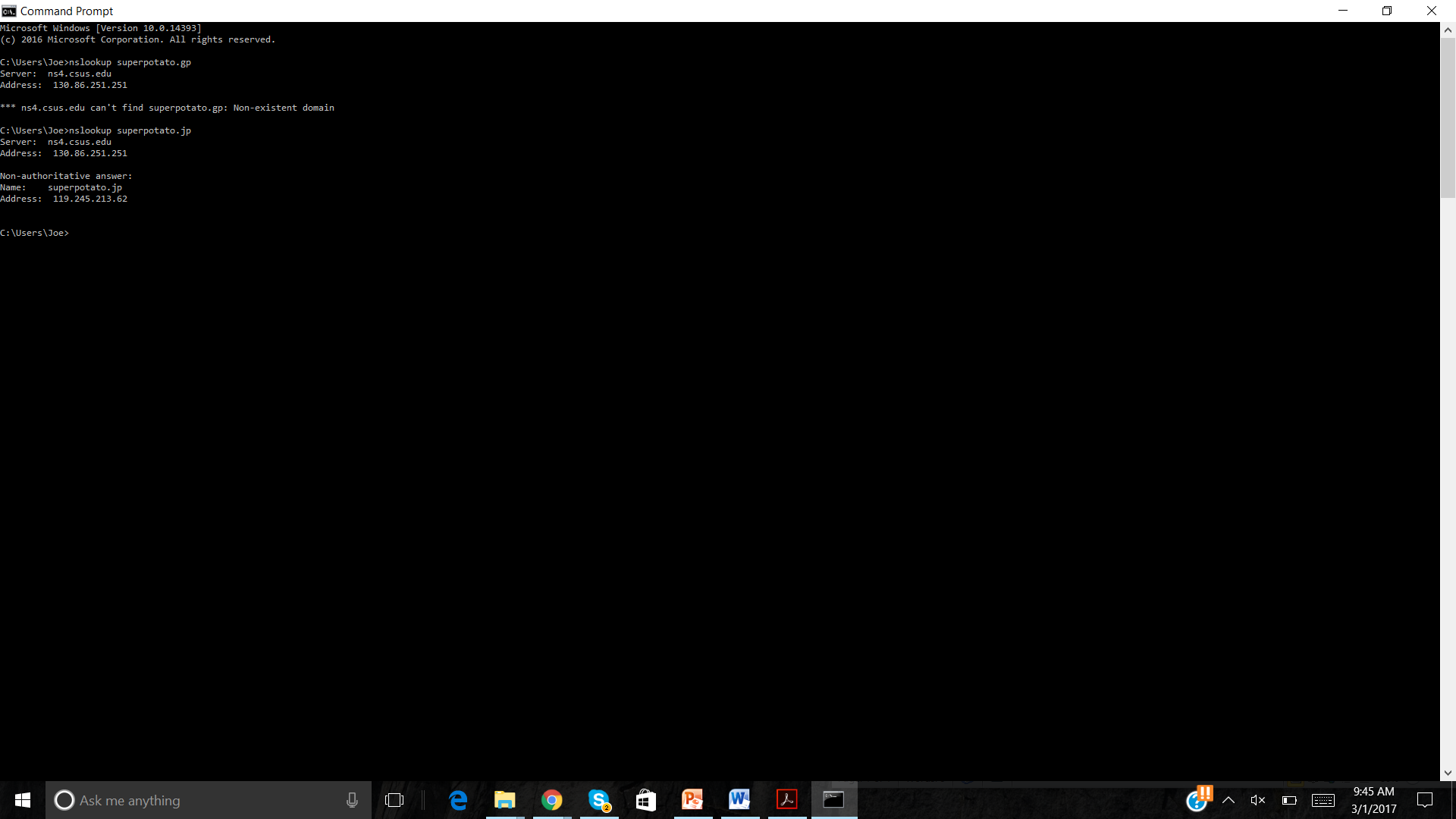
Professor Gansah

CPE 138

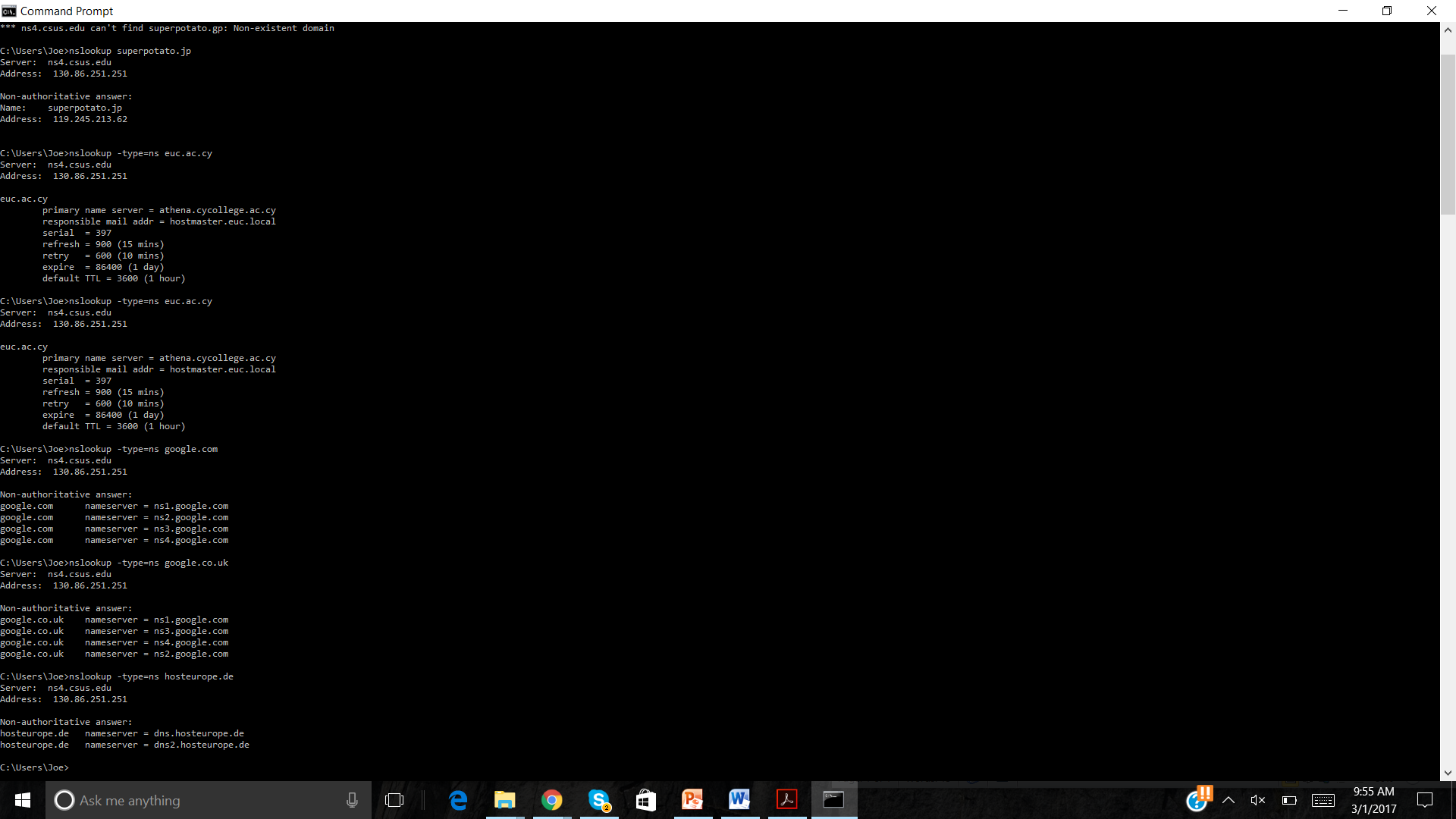
03/08/2017

Lab 2

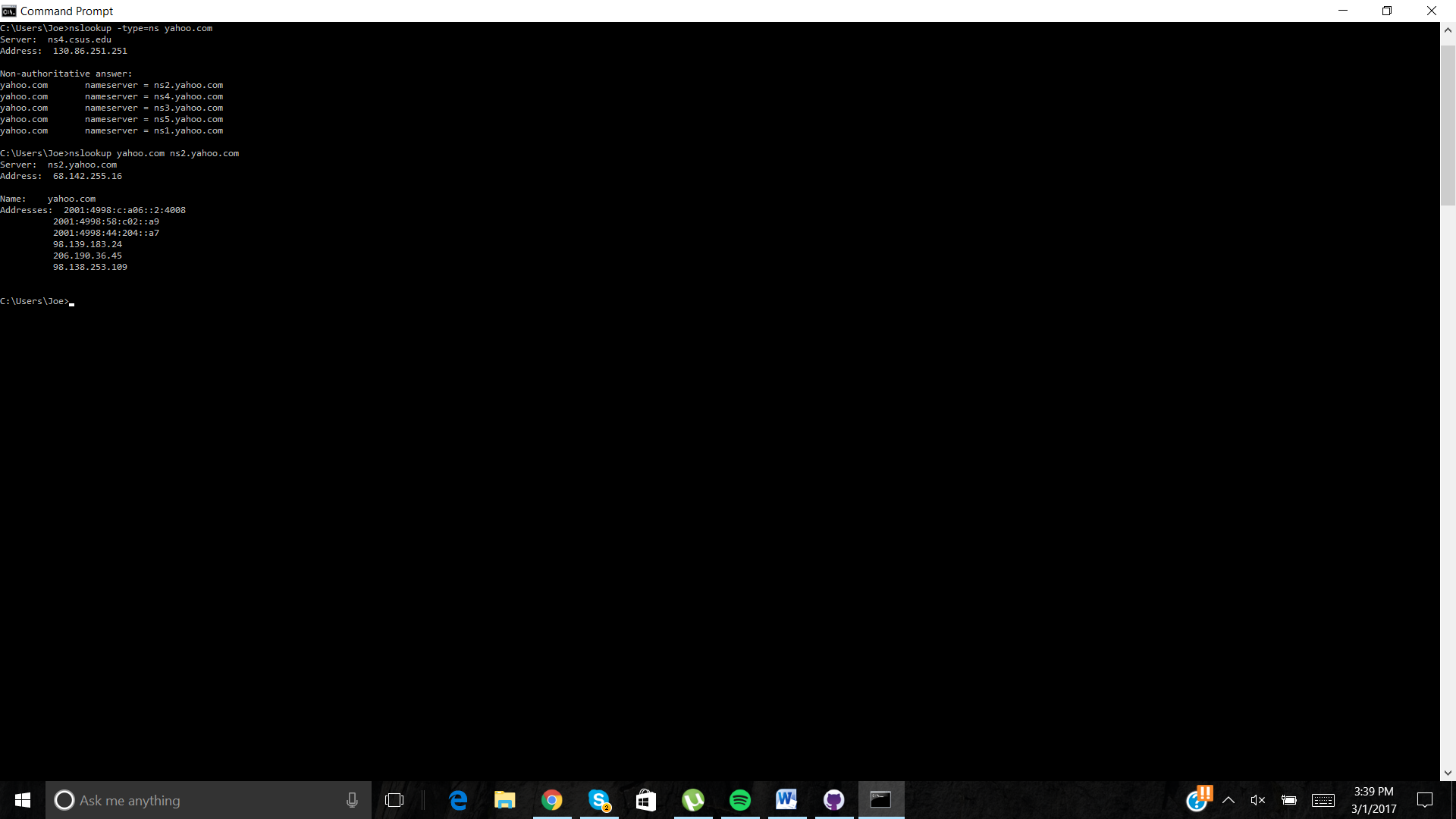
1. nslookup
   1. Super potato.jp/ip: 119.245.213.62



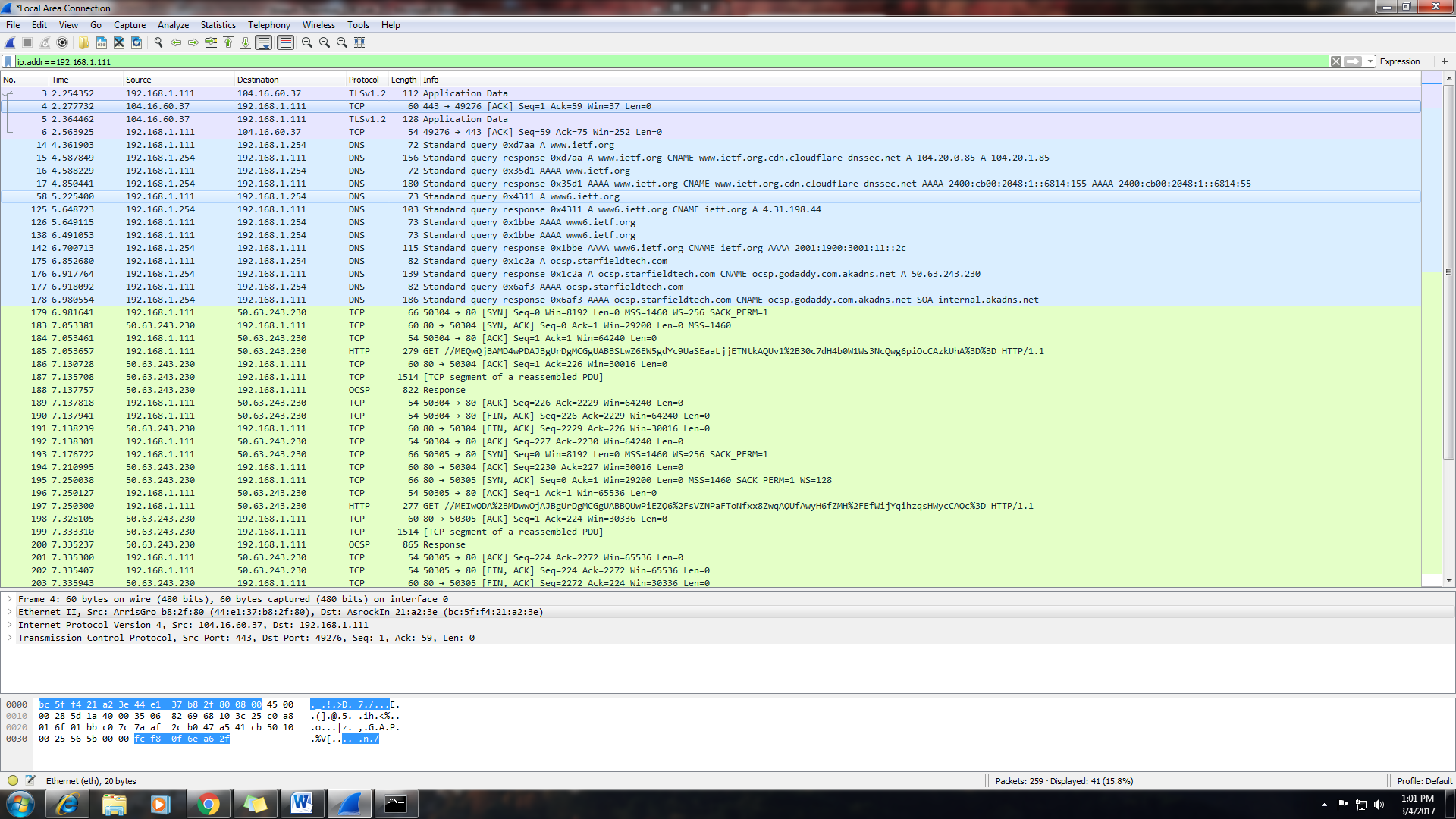
* 1. **Dns.hosteurope.de**



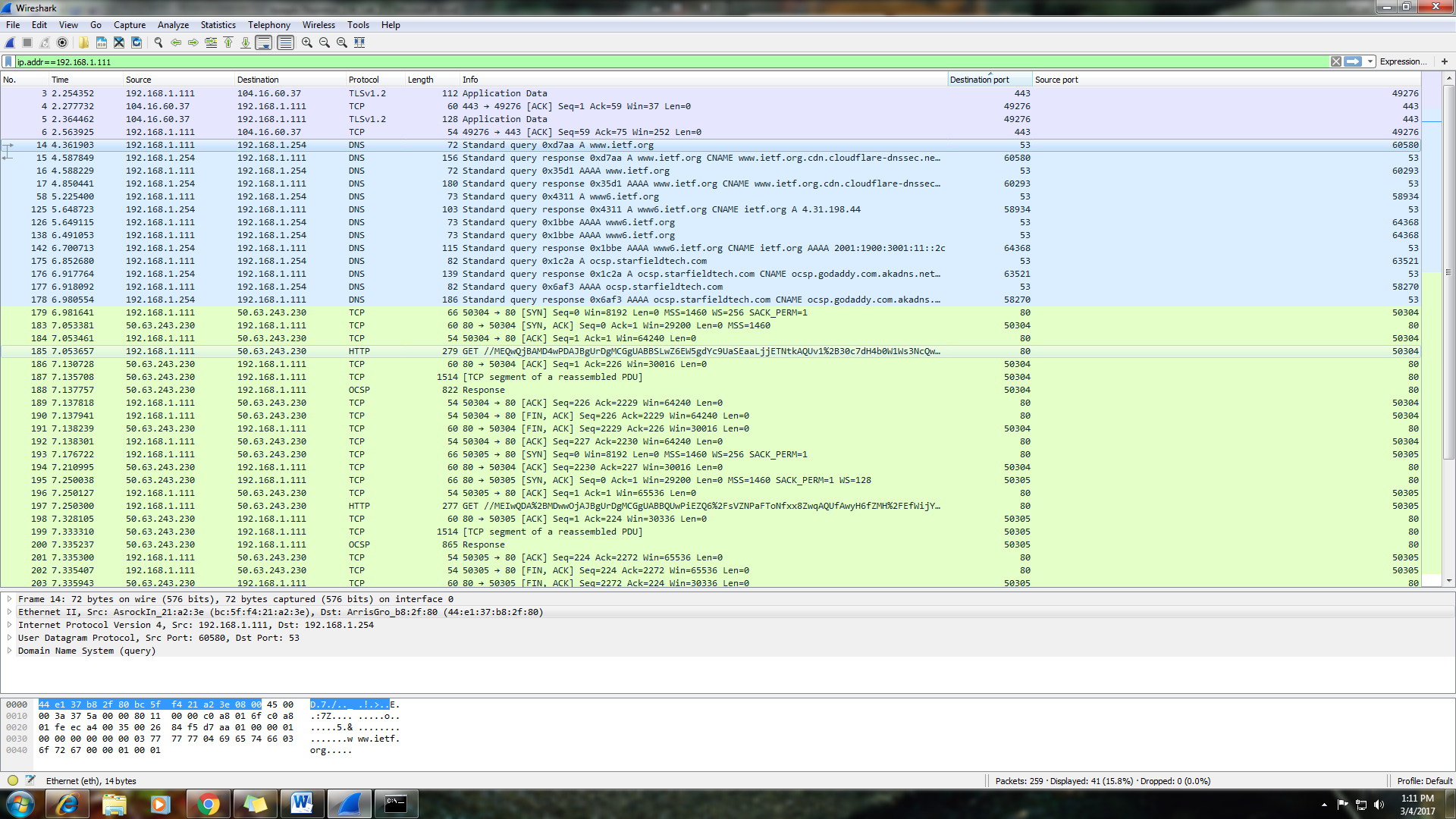
* 1. **68.142.255.16**



1. **Ipconfig**
2. **Tracing DNS with Wireshark**
   1. **TCP**



* 1. **Source : 53 destination: 60500**

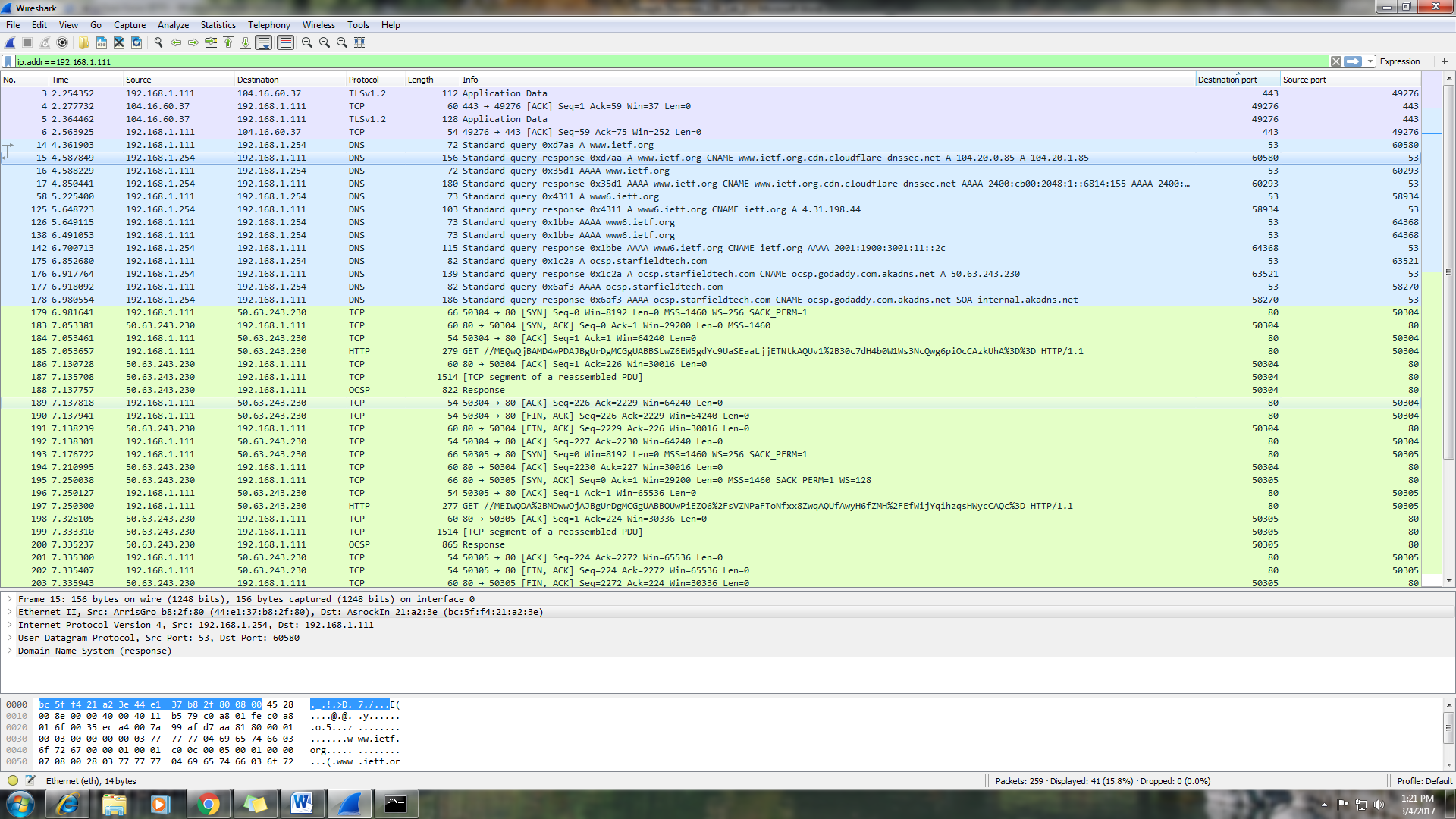


* + 1. **14 4.361903 192.168.1.111 192.168.1.254 DNS 72 Standard query 0xd7aa A www.ietf.org 53 60580**

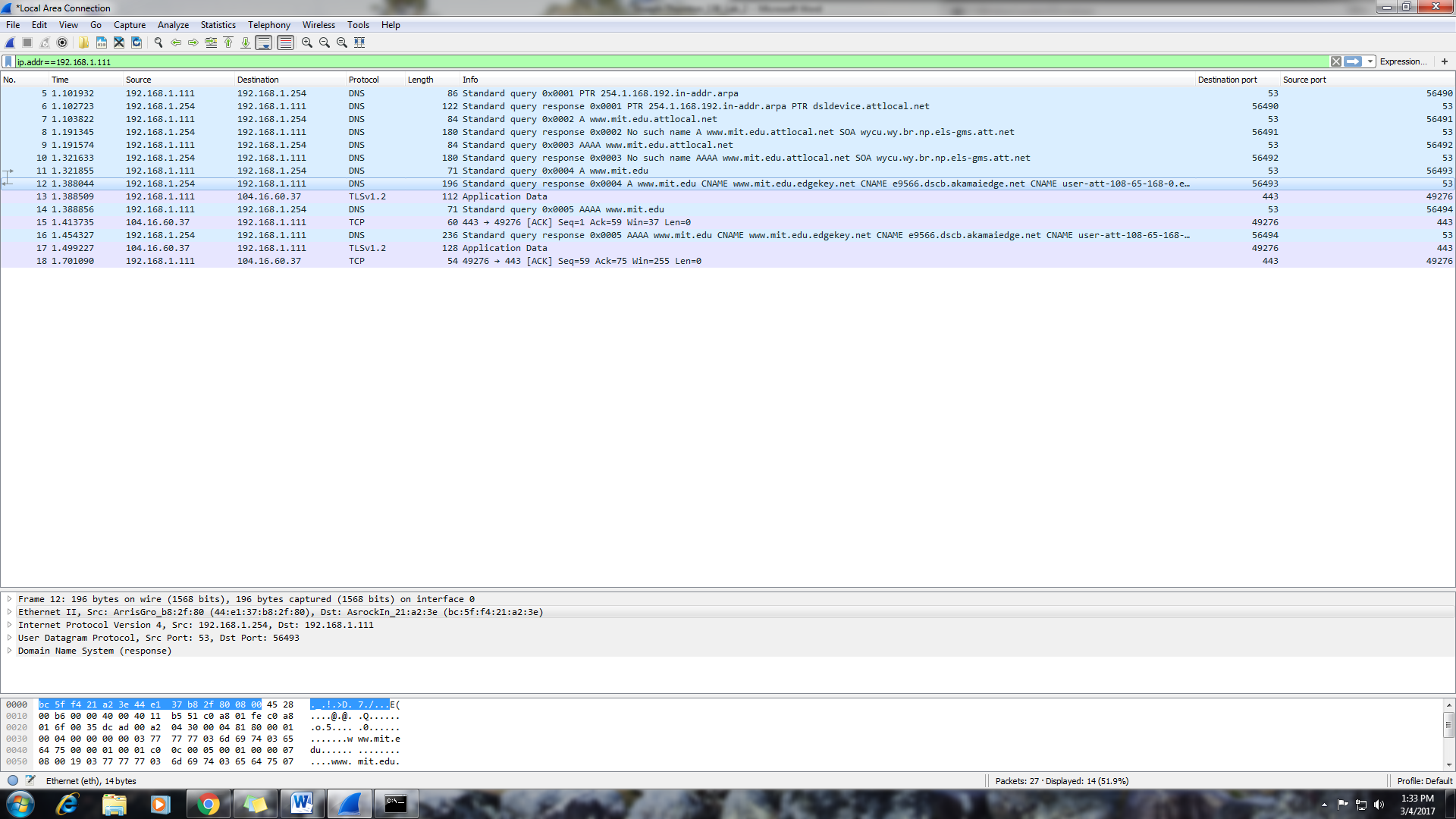
**This is the local router ip address this means that the router is the thing that decides what dns will be used.,**

* + 1. **Yes they are the same.**

* 1. **Standard Query and it answers what the address for the desired name is in this example 4.31.198.44 and many other responses from server**
  2. **It has 4 “answers” (seen below”) they contain multiple answers to the same query they return ipv4 answers and ipv6 answers as well as alternate ip addresses.**

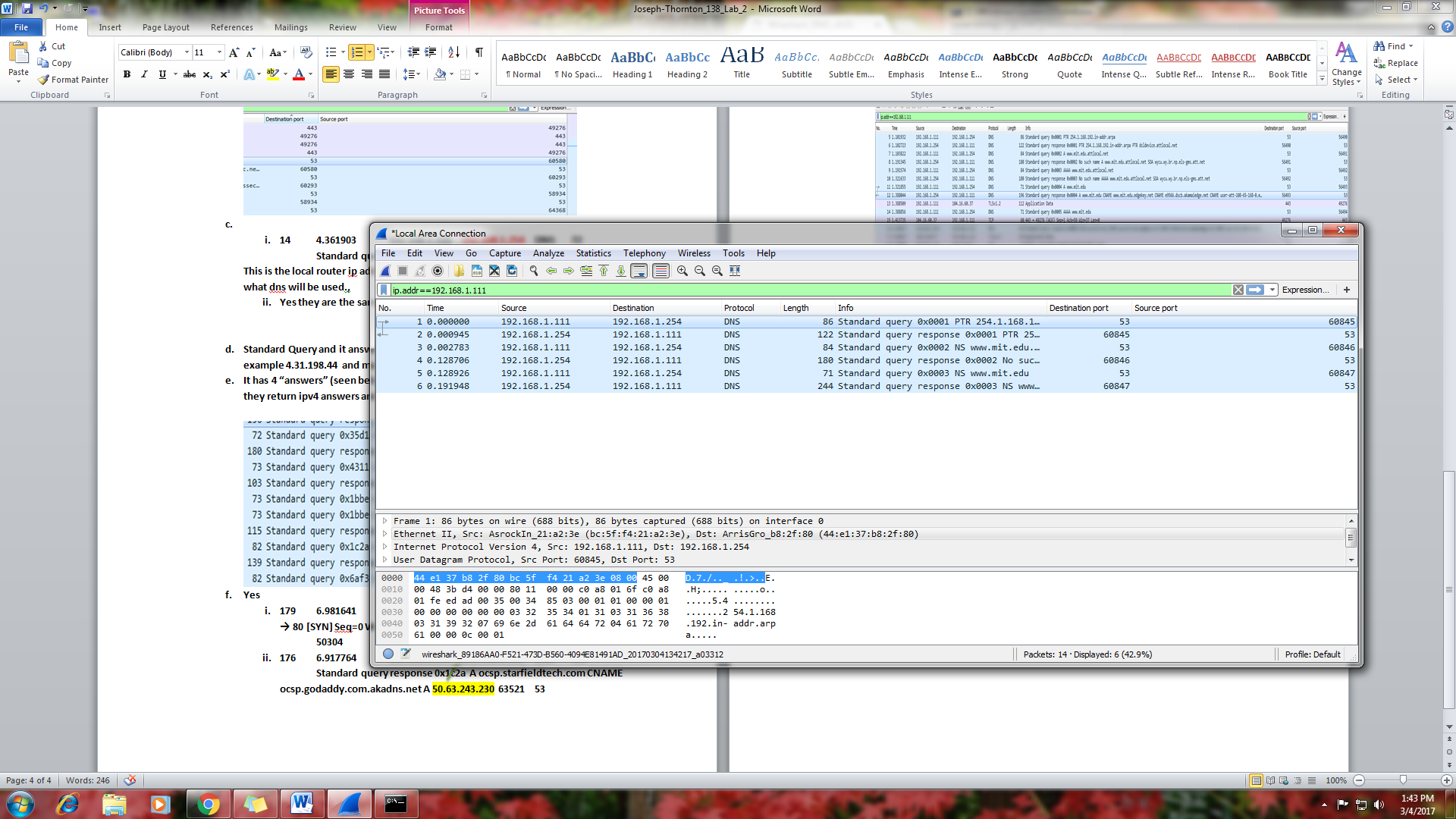


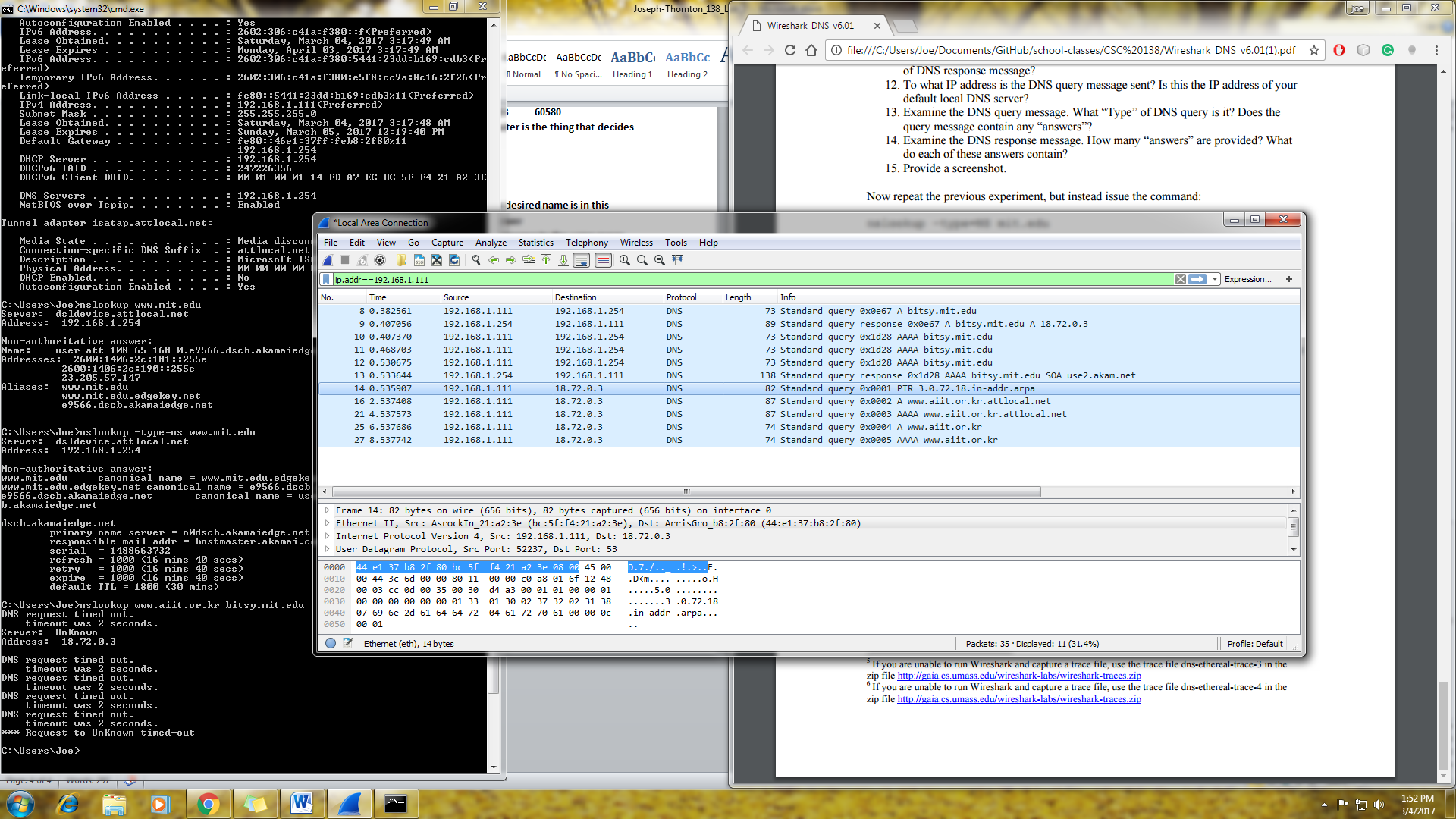
* 1. **Yes**
     1. **179 6.981641 192.168.1.111 50.63.243.230 TCP 66 50304 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK\_PERM=1 80 50304**
     2. **176 6.917764 192.168.1.254 192.168.1.111 DNS 139 Standard query response 0x1c2a A ocsp.starfieldtech.com CNAME ocsp.godaddy.com.akadns.net A 50.63.243.230 63521 53**
  2. **Source Port: 53, Destination port: 56493**



* 1. **Yes 192.168.1.254== Linksys router that handles the DNS.**
  2. **Yes** 
     1. **12 1.388044 192.168.1.254 192.168.1.111 DNS 196 Standard query response 0x0004 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net CNAME user-att-108-65-168-0.e9566.dscb.akamaiedge.net A 23.205.57.147 56493 53**
  3. **It contains 5 and they have the information about first the name server that was asked and theyn subsequent response has the ip address for the site given**

**Screenshot Above**

* 1. **Yes: 192.168.1.254**
  2. 
  3. **Yes, 2 0.000945 192.168.1.254 192.168.1.111 DNS 122 Standard query response 0x0001 PTR 254.1.168.192.in-addr.arpa PTR dsldevice.attlocal.net 60845 53**
  4. **It provides 3 and yes it does provide name servers**
  5. **6 0.191948 192.168.1.254 192.168.1.111 DNS 244 Standard query response 0x0003 NS www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net CNAME user-att-108-65-168-0.e9566.dscb.akamaiedge.net SOA n0dscb.akamaiedge.net 60847 53**
  6. **No ip 18.72.0.3 it corresponds to name server bitsy.mit.edu name server**



* 1. **Does not contain answers site must be down or out dated.**
     1. **14 0.535907 192.168.1.111 18.72.0.3 DNS 82 Standard query 0x0001 PTR 3.0.72.18.in-addr.arpa 53 52237**
  2. **No answers server is out of date**
  3. **Screen Shot Above**