Enabling DNSSEC validation with the root trust anchor in Unbound

You need to log in to your resolver (cache) machine, i.e. for group 1, you would use resolv.grp1.dns.nsrc.org, as you did in the unbound config exercise

1. Grab the root key

   NOTE: This is only for the purpose of this lab - on the Internet, you would simply use "unbound-anchor" to download the real root.key, and set "auto-trust-anchor-file:" in unbound.conf, and let unbound update the key when necessary.

   In this lab, ask your instructor if we are using the "RZM" or not.

   ### With RZM

   Go to https://rzm.dnssek.org/, and copy the trust-anchor statement (the ENTIRE line) from this page and paste it into a file, /usr/local/etc/unbound/root.key

   ### Without RZM

   Grab the key from the root server:

   ```
   # scp sysadm@a.root-servers.net:root.key  /usr/local/etc/unbound/root.key
   ```

   Edit the /usr/local/etc/unbound/unbound.conf file:

   Find the "trust-anchor-file:" line, and change it from:

   ```
   # trust-anchor-file: ""
   ```

   to

   ```
   trust-anchor-file: "/usr/local/etc/unbound/root.key"
   ```

2. Reload the nameserver

   ```
   # service unbound restart
   ```

3. dig @localhost +dnssec mytld. SOA

   What do you notice ?