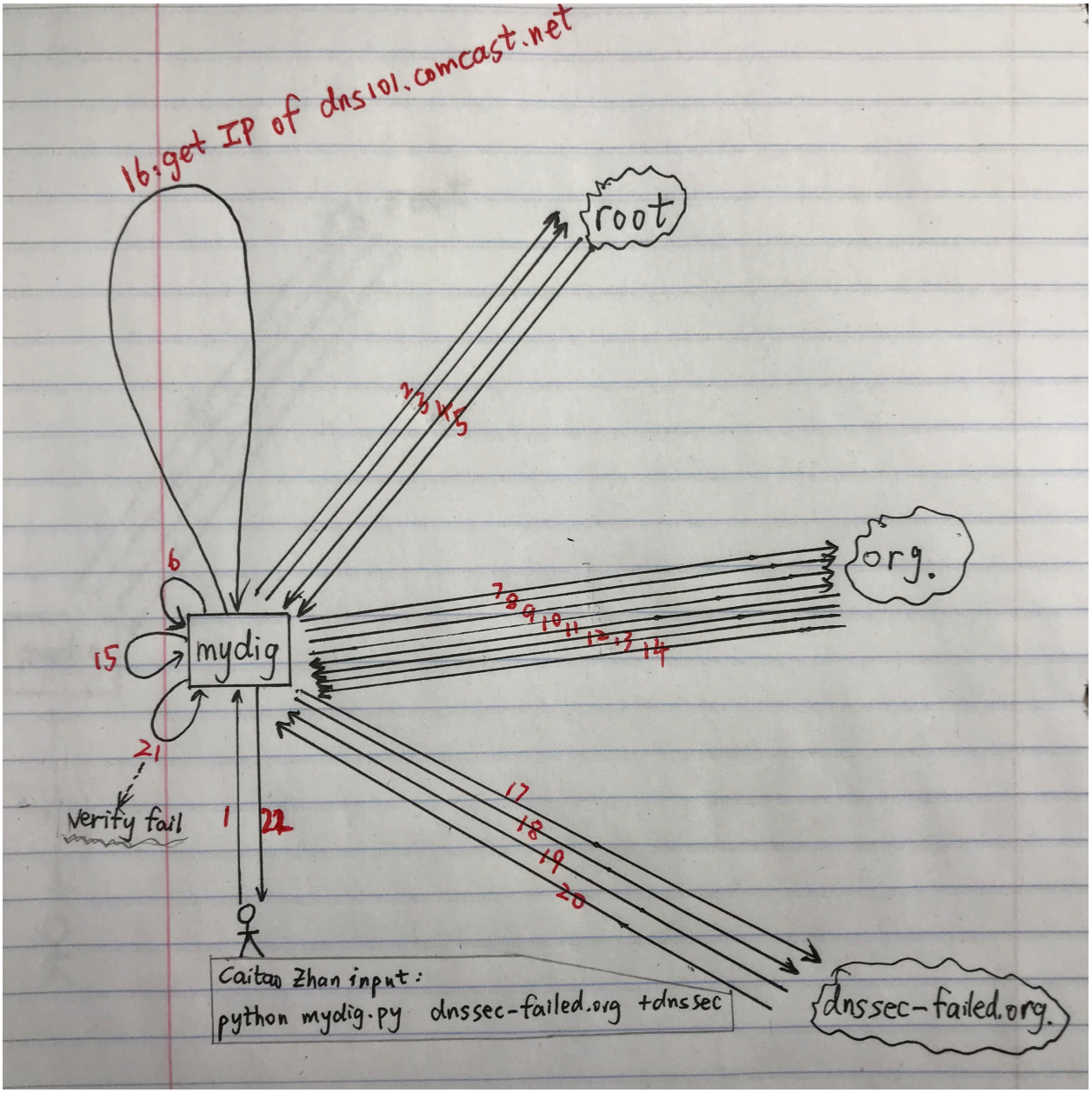
DNSSEC Implementation

In a nutshell, **I implemented my DNS resolver with DNSSEC *exactly the way it should be*.**

My two main references are: https://www.cloudflare.com/dns/dnssec/how-dnssec-works/ and https://www.youtube.com/watch?v=_8M_vuFcdZU. The YouTube video is extraordinary, and I followed every single step in the video.

When using the test case **dnssec-failed.org**, getting the **right output** with **right intermediate steps** is not easy. The following figure shows all the right steps.



I will show my DNSSEC implementation by explaining the example above, 22 steps in total.

1. User input: python mydig.py dnssec-failed.org A +dnssec
2. Single_iterative_query (**dnssec-failed.org**, type A, root_ip, want_dnssec=True)
3. Single_iterative_query (**root**, type DNSKEY, root_ip, want_dnssec=True)
4. Step 2 response with org's DS, and IP of org TLD NS.
5. Step 3 response with root's DNSKEY and its RRSIG
6. Verify the root. Success!
7. Single_iterative_query (**dnssec-failed.org**, type A, org_ip, want_dnssec=True)
8. Single_iterative_query (**org**, type DNSKEY, org_ip, want_dnssec=True)
9. **Step 8 returns nothing**. There may be some issues with the org TLD NS. I found out that I can only get the DNSKEYs and their RRSIGs by querying them **separately**. Also, there are 4 DNSKEYs for org, but I **cannot get all four of them at once**. I need to query **many** times until you can all four. Single_iterative_query (org, type DNSKEY, org_ip, want_dnssec=**False**) $\times N$. By experiment, **expected value of N is 4**.
10. Single_iterative_query (**org**, type RRSIG, org_ip, want_dnssec=**False**). Get org's RRSIG of DNSKEY. Note that this query occasionally returns nothing.
11. Step 7 response with dnssec-failed.org's DS. **However, IP for its authoritative NS is not found.** This leads to step 16.
12. Step 8 response which is empty. Suppose to be org's DNSKEYs and their RRSIG.
13. Step 9 response. Actually, is the **union of many responses** so that all four org's DNSKEYs is fetched.
14. Step 10 response with org's RRSIG of DNSKEYs.
15. Verify the org zone. Success!
16. Get the IP address of dnssec-failed.org's authoritative NS (for example, dns101.comcast.net). *Use the Part-A of homework-1 to do this.*
17. Single_iterative_query (**dnssec-failed.org**, type A, root_ip, want_dnssec=True)
18. Single_iterative_query (**dnssec-failed.org**, type DNSKEY, root_ip, want_dnssec=True)
19. Step 17 response with dnssec-failed.org's IP address and its RRSIG
20. Step 18 response with dnssec-failed.org's DNSKEYS
21. Verify dnssec-failed.org zone. Failure!
22. Recursively return the outputs to user.

The above 22 steps take around **700~800 msec**. If unluckily a timeout occurred somewhere, then it will take more than one second.

The output of those 22 steps are:

```
Congrats! . DNSKEYs are verified
Congrats! org. DS is verified
Congrats! Root verified
Congrats! org. DNSKEYs are verified
Congrats! dnssec-failed.org. DS is verified
Congrats! Zone org. verified
Congrats! dnssec-failed.org. DNSKEYs are verified
Congrats! A records are verified
Sorry! None of the 2 public key signing keys of dnssec-failed.org. can be verified by its DS in parent's zone! Thus, zone dnssec-failed.org. is NOT verified

Query time: 726 msec
WHEN: Mon Feb 19 12:28:24 2018

DNSSec Verification failed
```

Note that the **cnn.com and palpay.com have fewer steps**. These two don't have to do step 9 and 10 because their step 8 return the desired DNSKEYS and RRSIG. Also, they are lucky and don't need to do step 16.