**DNSSEC Implementation :**

The first step for resolving a domain using DNSSEC is to validate the root Servers.The root servers are validated using signed DS record **root_dsList** taken from http://data.iana.org/root-anchors/root-anchors.xml . To validate the root servers a hash is generated for root using 'sha256' algorithm and the hash is compared with records in root_dsList.If the hash matches with a record in a root_dsList,the root server is validated and we get a top level domain.In my code resolve(tokens)[line 113-123] is executing this part of code.

After we get a top level domain(TLD), we will generate next level servers as we go down the domain hierarchy.This is done by querying the parent server to get RRSet,the ds records for the child ,the encryption algorithm for the child and a boolean flag which represents whether the current flag is Authoritative name server or not.This part of DNSSEC resolver is taken care by **getNextServers(query_servers, domain, isFetchZSK).**This function has a boolean flag isFetchZSK and if this flag is true,this method will return RRSet,RRsig and ZSK.ZSK is the ds record of the parent zone.

The RRset,RRSig and ZSK fetched from the parent Zone using **getNextServers()** method is validated in the **validateZSKandKSK()** method.This method has two parts,in first part it validates the RRSet record we got from the parent.This is done by using a python API (dns.dnssec.validate).In the second part,the DS record from the parent zone is compared with the hash generated in child zone.If both parts return true then the **validateZSKandKSK()** method will return true and a chain of trust is established between parent and child zone.

I iteratively validated each zone using the validateZSKandKSK**() method** and generated subdomain servers starting from the root servers till the last subdomain in the bottom of the hierarchy is reached.**resolve(tokens)** method is responsible to perform this part of execution.Once I reach at the last domain,I simply query the resolved served with 'A' domain type to generate the output.