Dnssec Implementation:

In DNS, at each point of time, we send a single request and get the response of it and use that response to loop through in finding the final IP address. We used a dnspython module to implement this.
The DNSSec was implemented to verify each response from the server so that we can prevent man in the middle attack. To implement DNSSEC, we send two requests from the localhost to the root server. The initial request will be sent with rdatatype.DNSKEY and the want_dnsec=True option. The next request will be sent with the appropriate DNS query type. This would tell the root server that we are requesting for the Delegators Signature and RRSIG of the Delegators Signature. If the input fails to return the answer section for the first request, we understand that the “Dnssec is not supported” for the particular request
The second request could help us in fetching the recordset(rrset) and record signature(rrsig). We use the rrset,rrsig, and DS and pass it to dns.dnsec.validate(). When it fails, we return “DnsSec Verification Failed”.

The second part of the verification would be to check whether the key that we get from the initial request is valid or not. To do this, we get the Key Signing key of the child and find the appropriate algorithm(SHA-1, SHA256, SHA384) used by parent Delegators Signature(DS) and hash the child using the algorithm and check if it returns the DS of the parent. If it does not, our key has been compromised and we can state that “DnsSec Verification Failed”.

Examples:
1. python dnssec.py verisigninc.com A

verisigninc.com. 3600 IN A 72.13.63.55
verisigninc.com. 3600 IN RRSIG A 8 2 3600 20201022161123 20200922161123 63484 verisigninc.com. Xg2CopWpAvfWDOa/gnn3xVSlEzJGBVh4 54G4gA865++HFeeSlOogmjgXMN9Rtak9 PdCIJBiImmVve8tyUStUUqIP3HqCPjLC jOI5QIqh1CEd51Fd0GLRpFS7YGn/tUdl mxXXuN7TqpTXa08RliJFHg0CCap3hjYc gxVlgCXtsFY=

Here, the keys were validated and hence we resolved the IP address for the data type requested.

2. python dnssec.py www.dnssec-failed.org A

DNSSec verification failed

Here, during the verification of the final step, the hashing verification fails the DNSSec.

3. python dnssec.py Amazon.com A

DNSSEC not supported.