I have implemented dnssec in top-down approach. That is I am starting my verification from root servers.

Verifying root server's key signing key with the trust anchor present at http://data.iana.org/root-anchors/root-anchors.xml (KeyDigest id="Klajeyz"). The hash value of key signing key matches with the digest record in trust-anchor.

Program queries root server for DNSKEYs and get Three DNSKEYs. Out of which one is Key Signing Key and other two are ZSKs. The response also contains the RRSIG record for DNSKEYS. The RRSIG records of these DNSKEY gets verified by KSK.

Now the program queries top level domains for their DNSKEYs as per the input query. We get a set of KSK and ZSK. The program now request parent server for DS records. The hash value of KSK is same as digest in DS record. This way we can establish trust between child and parent zone. The RRSIG DS records gets validated with parent ZSK. The program now queries the server for DNS records and verifies the RRSIG records using ZSK of TLD.

The chain goes on till the input gets fully resolved.

In my program following stages of verification are working fine in DNS hierarchy.
DNSKEY verification
Transfer trust from parent zone to child zone.
DNS records verification

For google.com the DS record is not present on .com tld and DNSKEYs are also not available, so for google.com the dnssec is not implemented on google.com.

If the whole process comes out without error the dnssec is implemented for that site.

If there is key verification error in any of the above three verification dnssec verification fails

The code may not work for record type other than A.