First I have queried the root server and extracted the RRSets from the obtained response. Then for each of the RRSets, I have extracted the signatures to get the signer and footprint of the respective RRSet. Then I have queried the signer for the DNSKEY record and extracted the data from the RRSets of the answer section from the obtained response. From the data, I have looked for the DNSKEY which had the footprint same as obtained above and if they matched, I have saved the key as the DNSKEYRecord. Then I have verified the rrset and the corresponding RRSig record with the obtained key and if it doesn't give any error then KSK key has been verified. Then the Zonal RRSet and the SIGRecord have been verified and if it doesn't give any error then the ZSK has also been verified. Then a DS query with the zonal RRset is sent to the zonal signer and some keys are obtained and these keys are then verified with the above obtained keys and if any of them match then the DS is also verified.