Network Security Challenge 10 - Hard

In this challenge we will test your knowledge of DNSSEC very thoroughly. The server will give you traces of DNS resolutions resolving different domains. [1] Your job is to verify if the traces are valid and send `True` or `False` to the server. If you do it correctly every time for `HARDNESS` times, you get a flag. If you don't to it correctly every time, the server will give you the amount of correct traces and for debugging purposes the index of the first incorrect answer. [2]
You can assume the following:

1. The trace is always from a query for an A record. The result can be either an A record or NSEC3.
2. The trace has all the information you need for the verification. If not, you should respond that the trace is invalid.
3. The attacker can delete, edit or add any information.

Good luck!

Exercise 10–2 is hosted at `netsec.net.in.tum.de` at port 20210.
The client script provided via Moodle already handles all communication with the server.
We recommend connecting to the server using `netcat (man nc)` first.
It is advisable to have a Linux system at hand for the challenges. Our servers and clients are written in python.

[1] The output looks similar to `dig +trace somedomain.com`, with info like `DNSKEY` records interlaced. You can also save the traces and inspect them manually.
[2] This challenge is well-tested. Still, if you reach >90% and cannot solve the challenge and are sure that we have made a mistake, you can mail your code to `mailto:netsec@net.in.tum.de`. **We will only help you if you reach >90%!**