VeriSign®

How do validating caches deal with spoofed responses?

Duane Wessels

VeriSign Labs

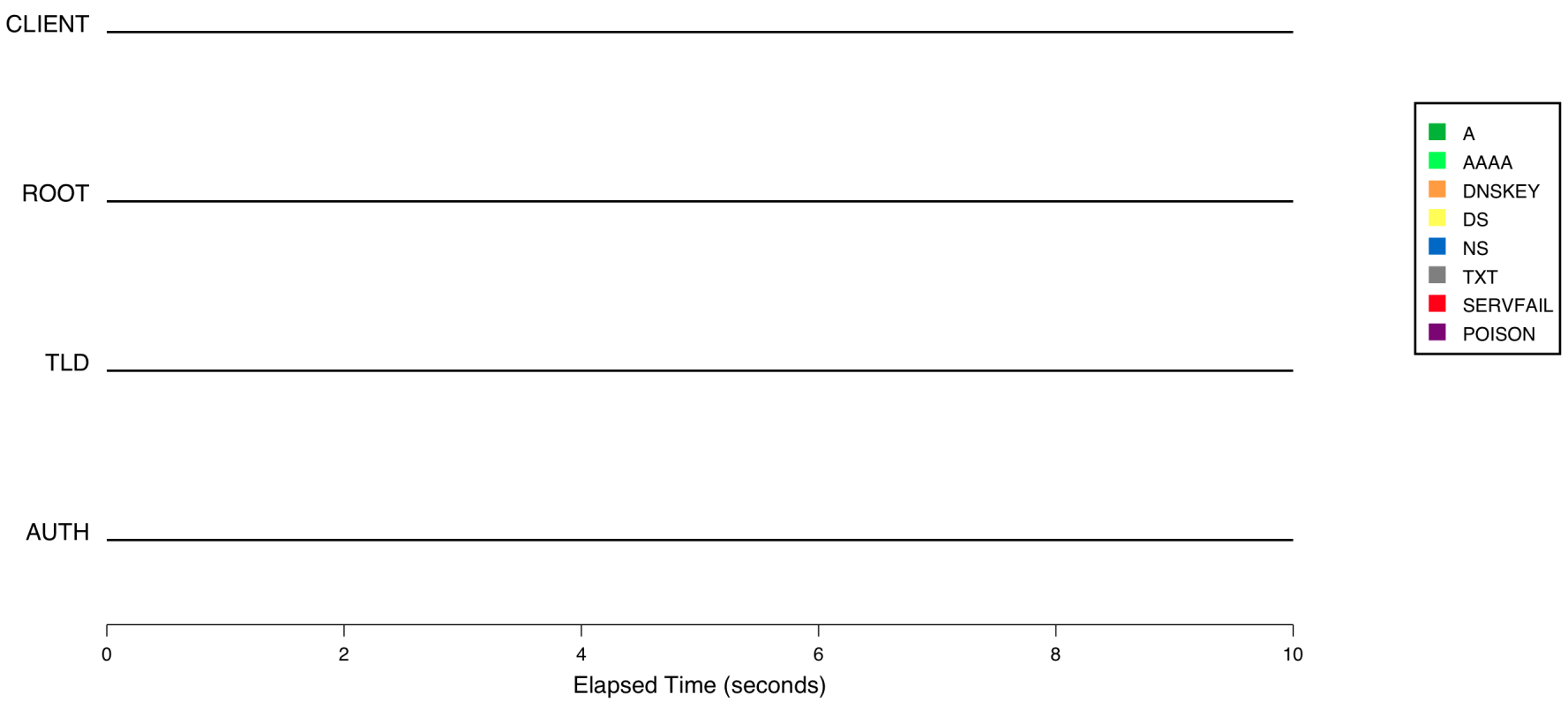
DNSSEC and Spoofing

- DNSSEC prevents spoofing
  - if spoofed zone is signed
  - and chain-of-trust exists
- And by “spoofing” I mean falsified or unsigned response data.
- How does a validating resolver behave when responses are spoofed?

Some Tests

- We ran some controlled tests
- Using BIND-9.7.0-P2
- Using Unbound-1.4.4
- And a few “spoofing” scenarios we could think of
  - answers for www.facebook.com from a root server
  - answer with a bad signature
  - NXdomain for a TLD
  - a DS response that never arrives
- Note: Caches always start empty

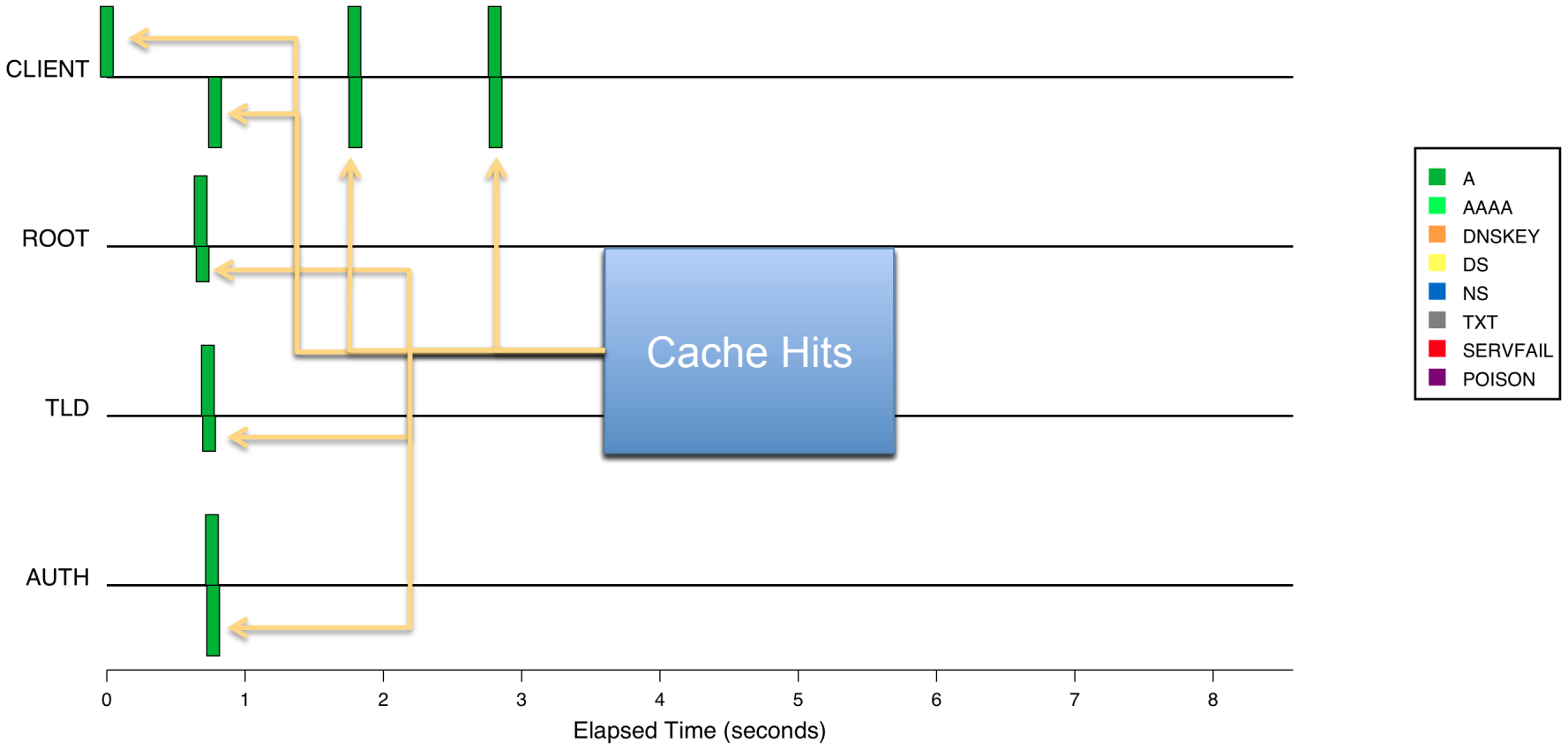
Visualizing DNS Traffic



Running on Slow Hardware

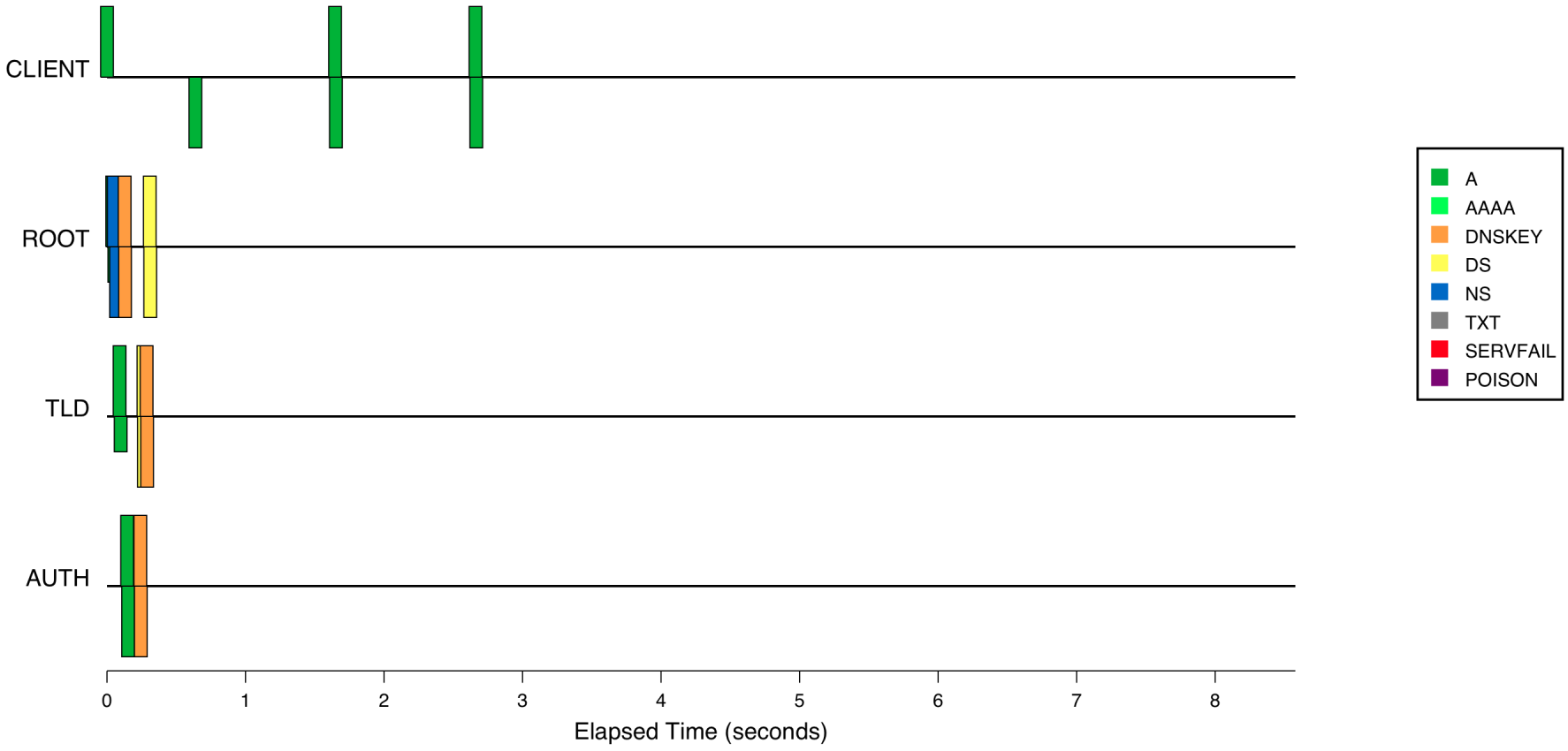
This is not a performance test, so ignore the time-axis values.

A Normal Transaction



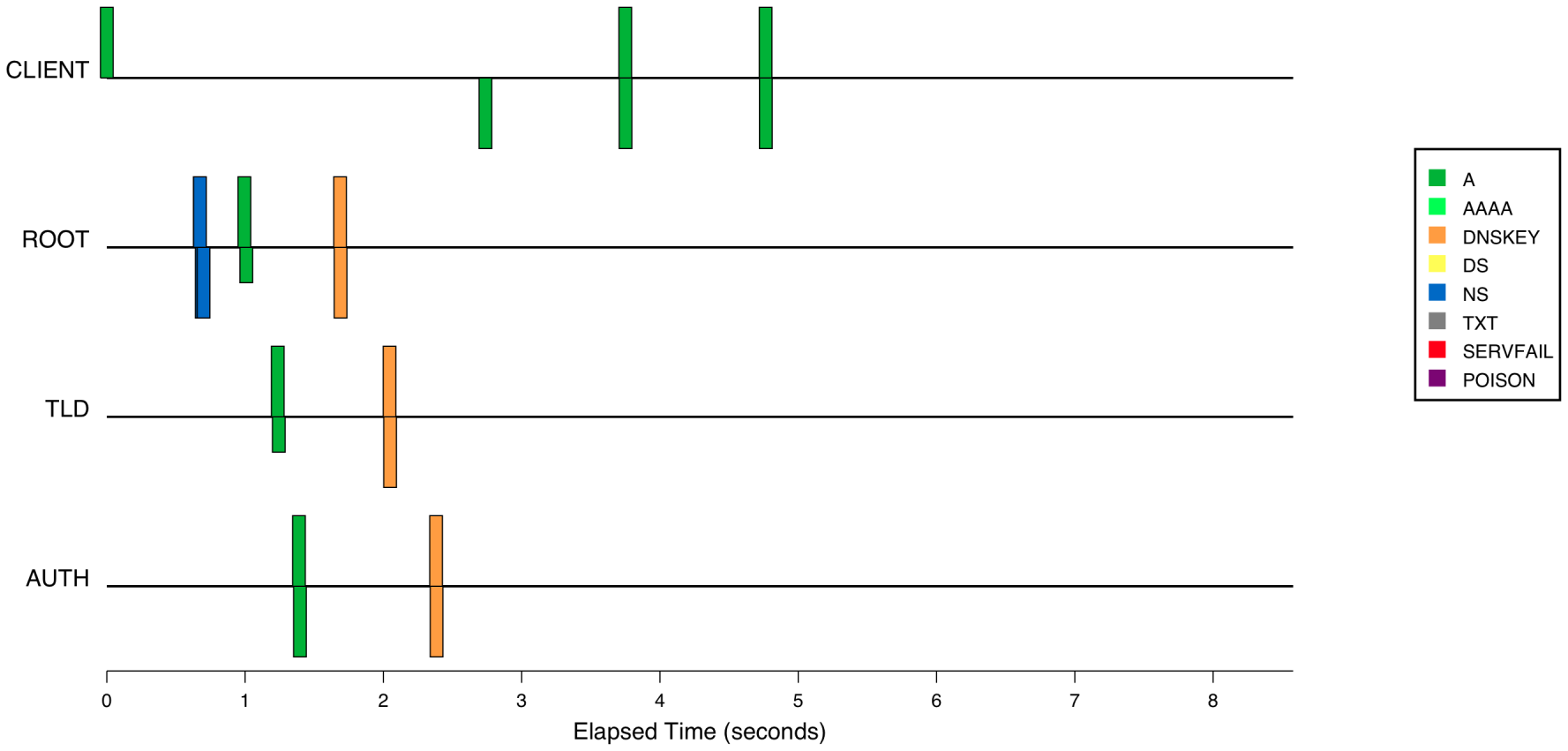
A normal transaction. You can see referral following from the Root, TLD, and then Authoritative namservers. After the initial request there are two cache hits. Note there is some delay between the client's query and its receipt at the Root because of a user-level process that decides whether or not to spoof.

BIND: With Trust Anchor



Here the resolver is configured with a Root trust anchor and issues DS and DNSKEY queries to the other nameservers.

Unbound: With Trust Anchor

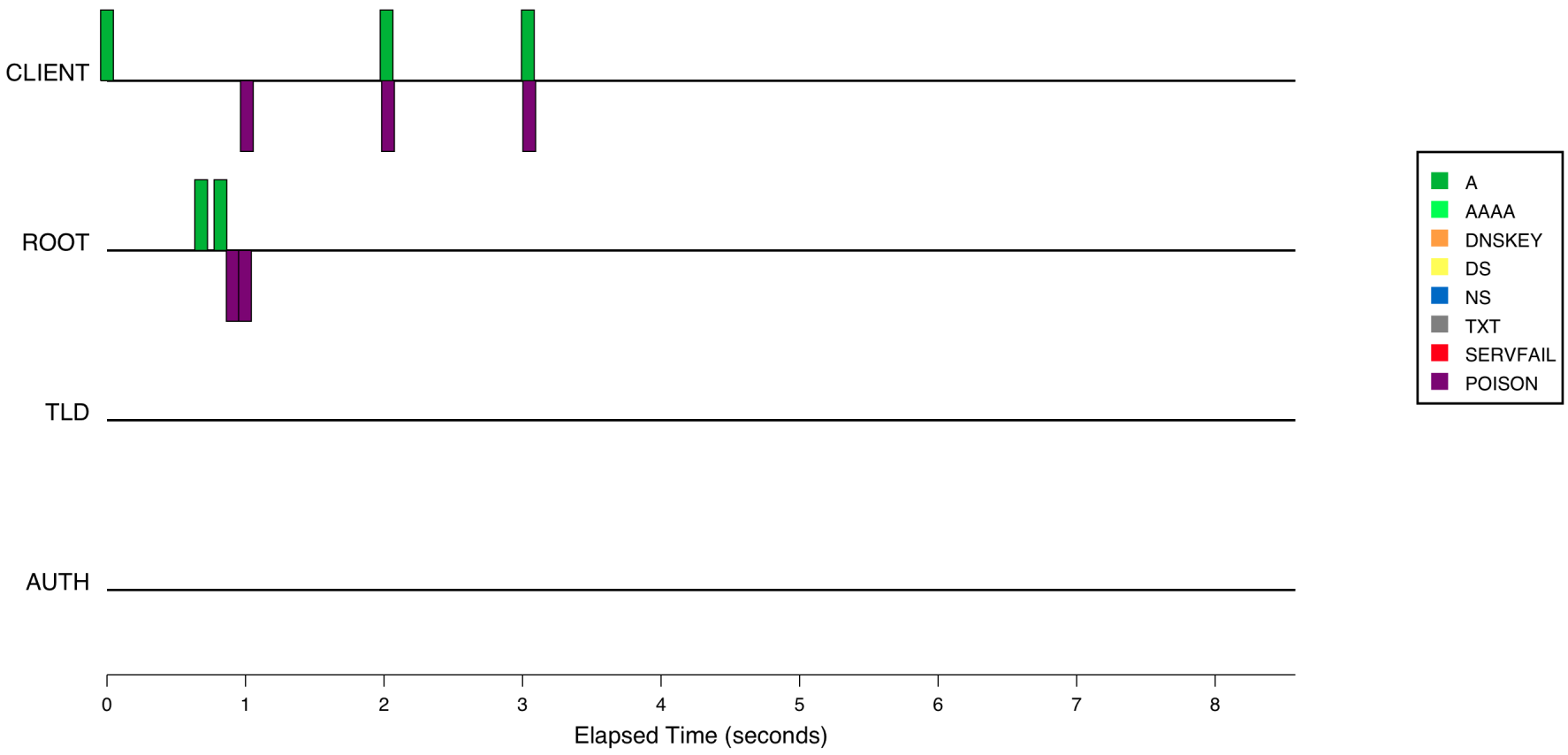


Note no separate DS queries – they are in the referrals.

“fakebook”: A spoofed Root Server Response

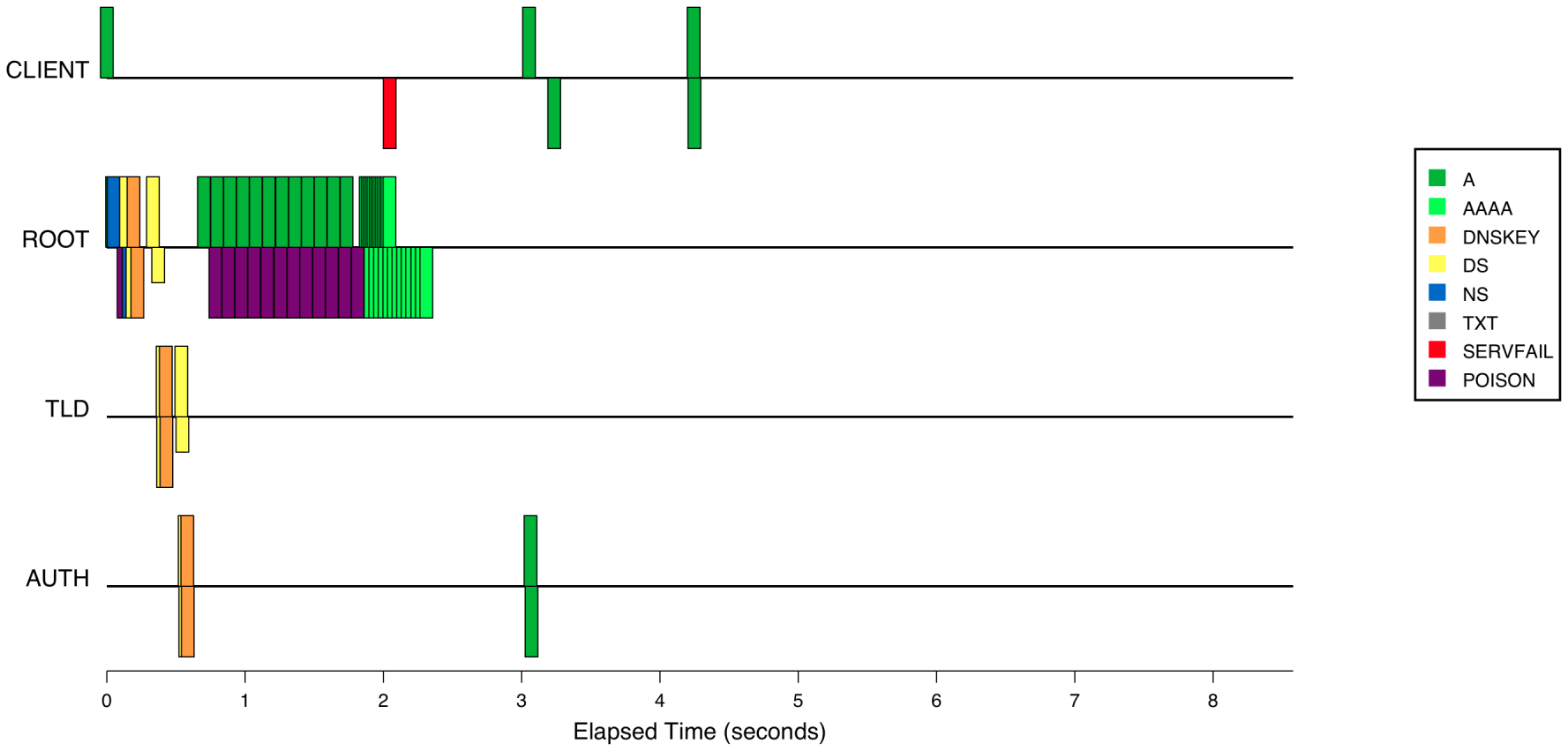
- Client issues query for www.facebook.net
- facebook.net zone is signed (as is net and root)
- All 13 root servers return a falsified, unsigned response
- Qname = facebook.net queries are not spoofed

Spoofed Answer, no Trust Anchor



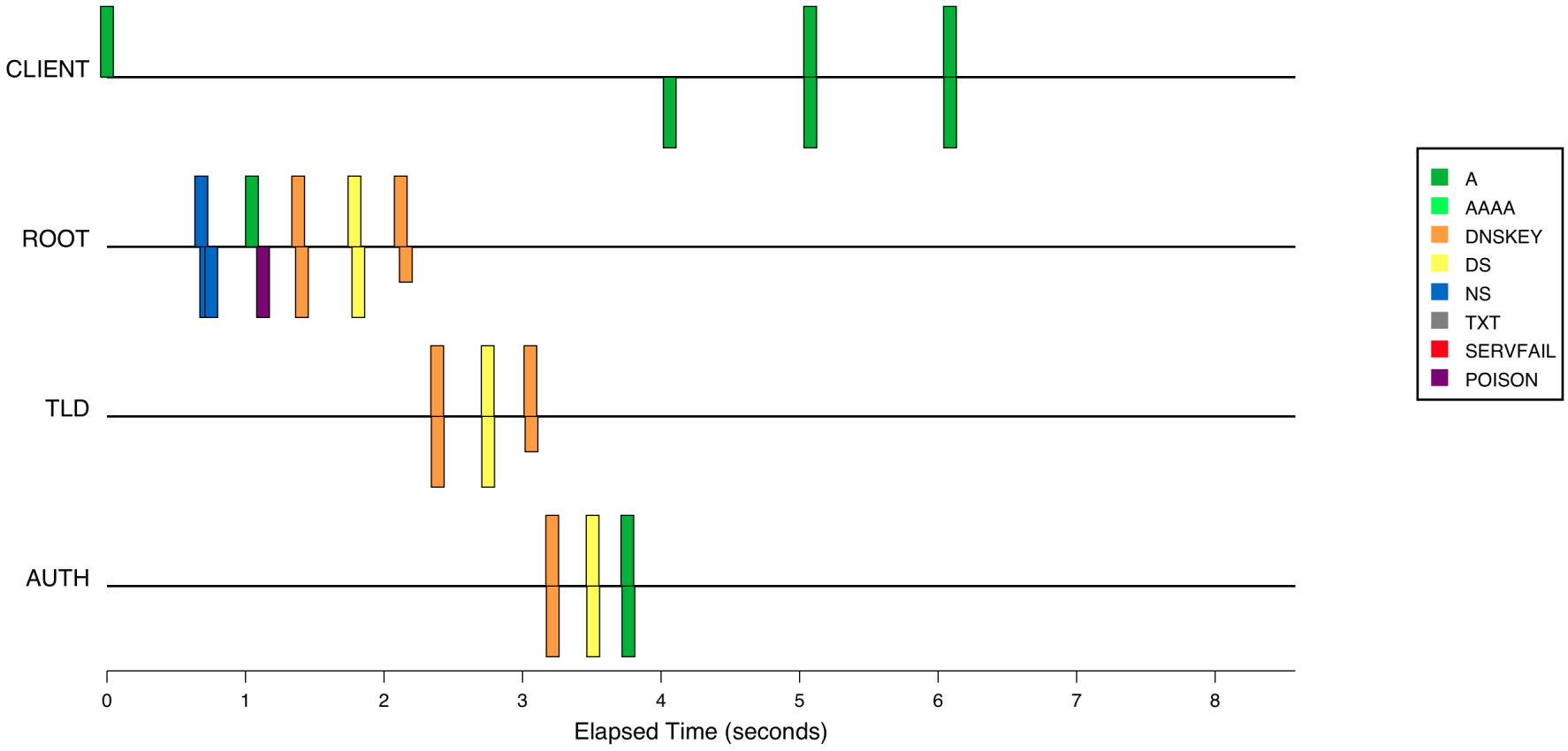
In this case the resolver receives a “bad” response that appears to come from a Root server IP address. The response is trusted and returned to the client. (It seems the resolver was impatient waiting for a response and sent two queries.)

BIND: Trust Anchor and Spoofed Root Response



BIND tried all 13 roots (and all 13 return bad answers), then returns SERVFAIL. Note, however, that BIND was able to talk to the Authority before it re-tried the Roots. Subsequent client queries are successful because the proper delegations are in the cache.

Unbound: Trust Anchor and Spoofed Root Reponse

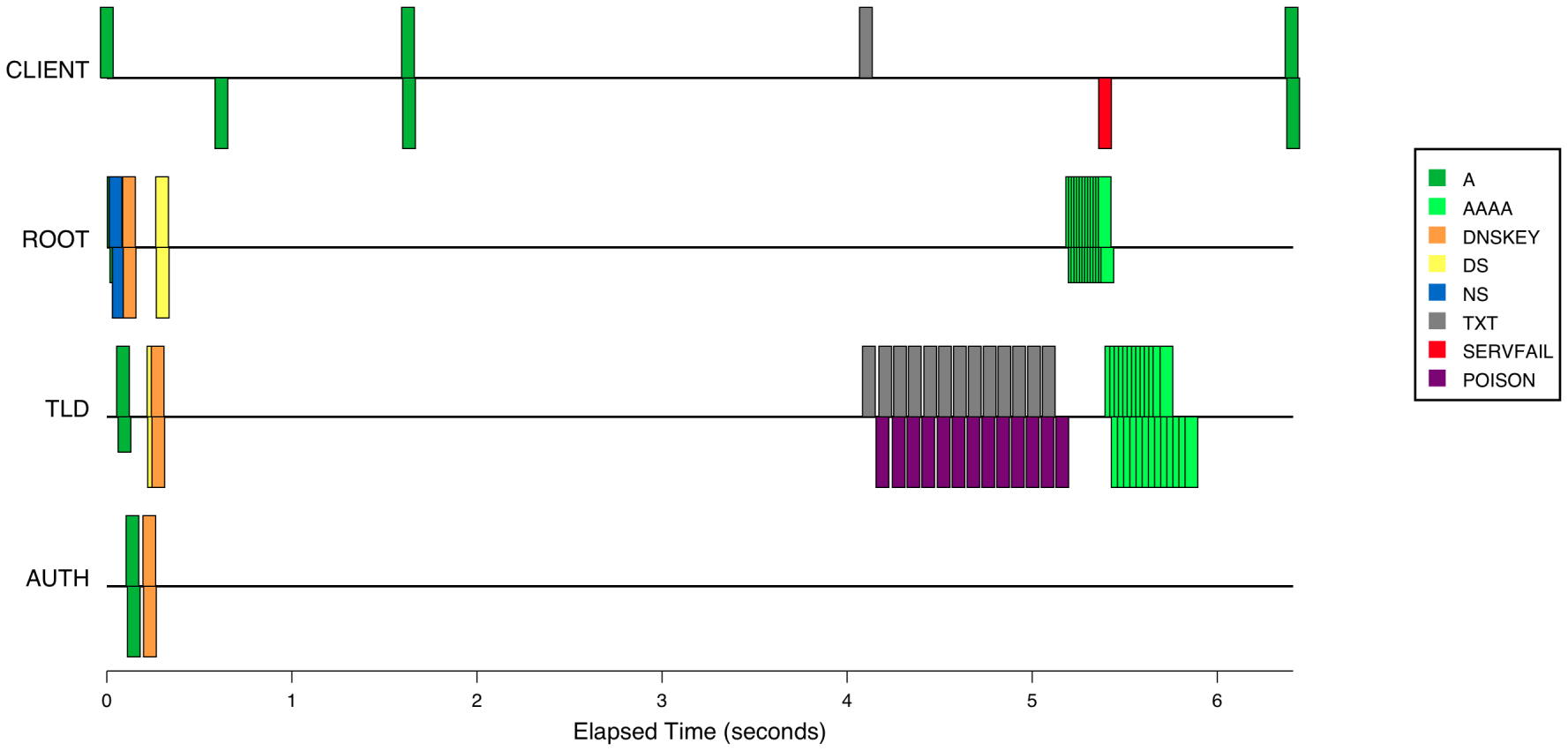


Unbound receives the poisoned response, then follows delegations for DNSKEY/ DS queries, and finally sends query to Authority. No SERVFAIL.

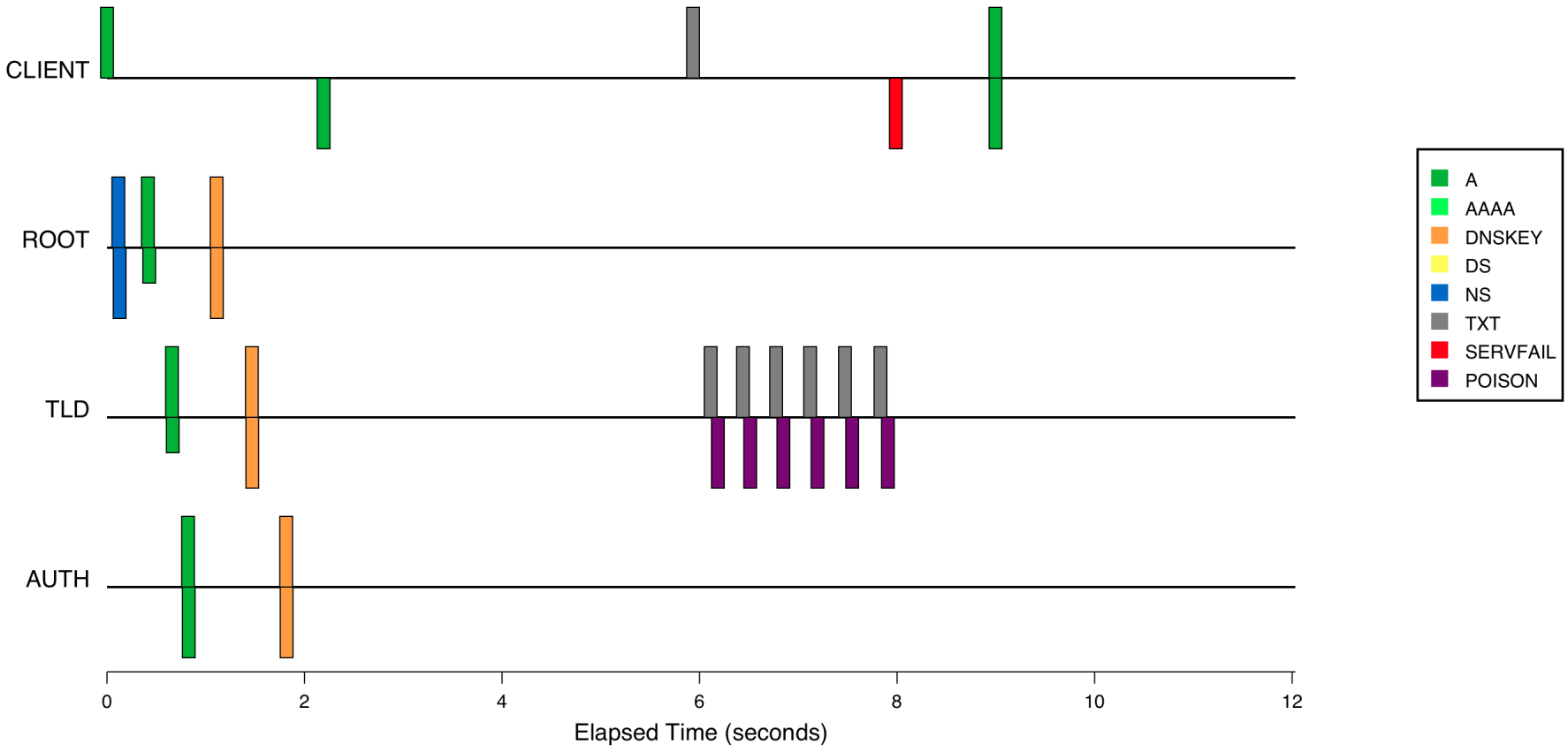
.NET NXDomain

- First, a successful query for www.example.net
- Then, a TXT query for “net” which results in a spoofed NXDomain response
- Then another normal query for www.example.net

BIND: .NET NXDomain



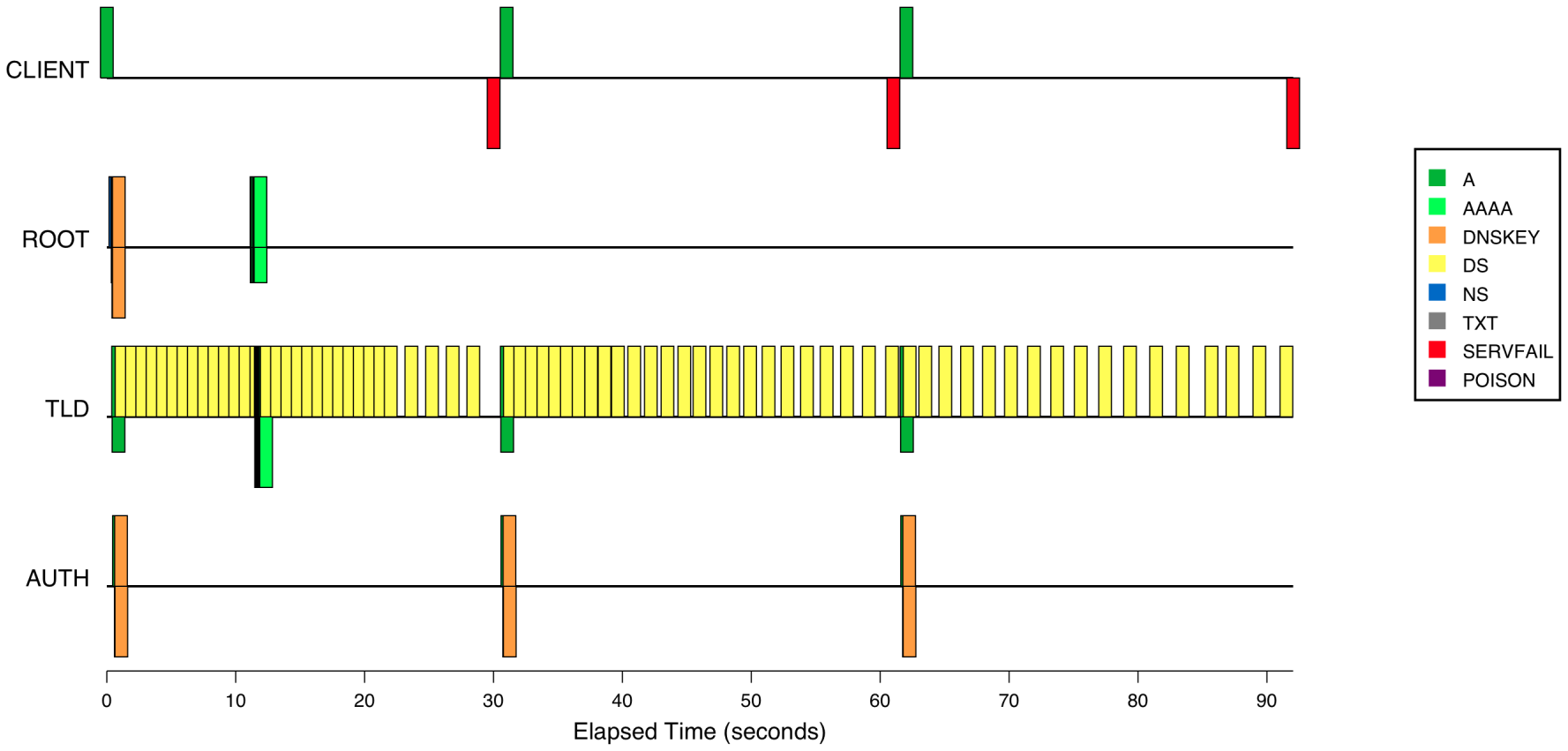
Unbound: .NET NXDomain



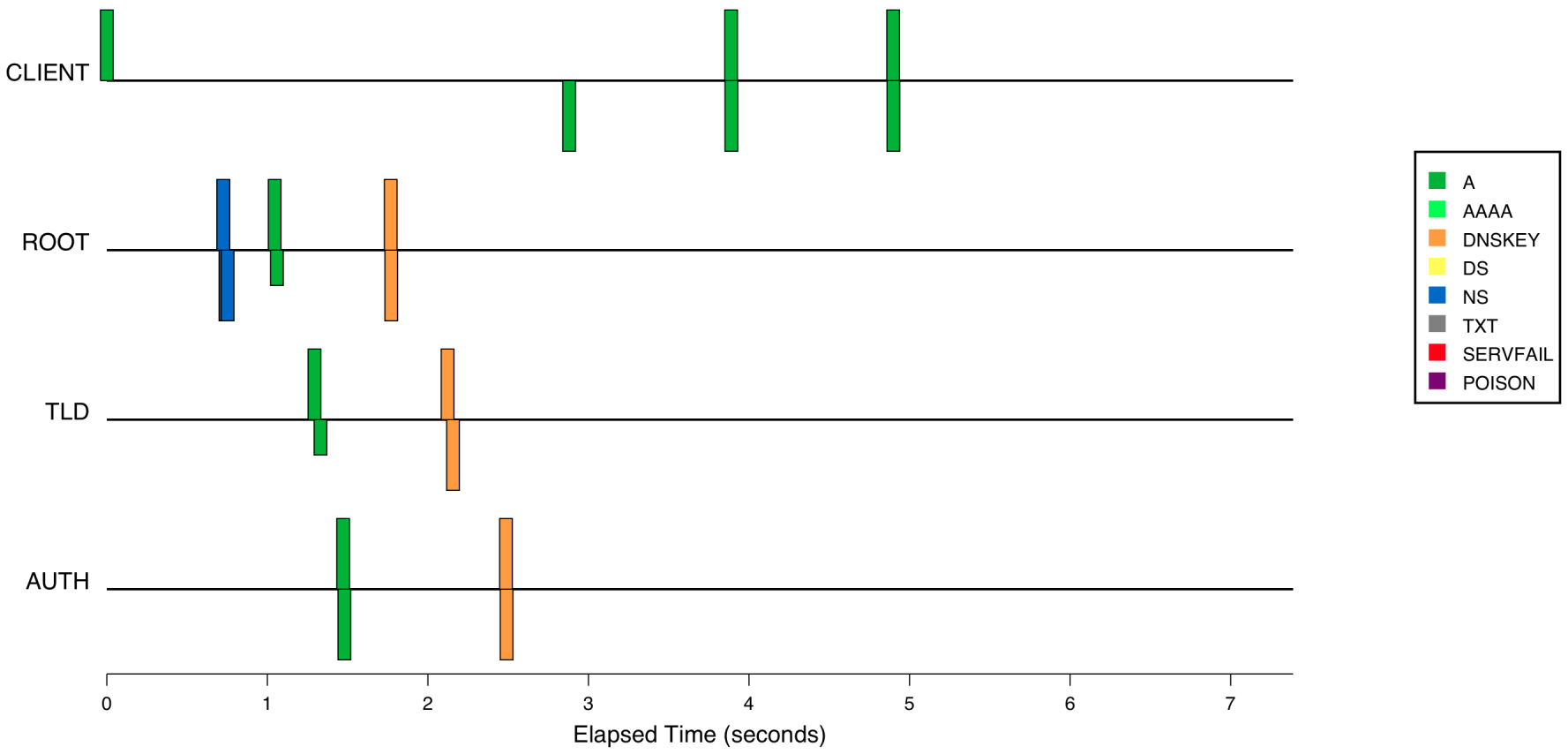
DS Timeout

- Resolver never receives a DS response from a TLD nameserver
  - Maybe it gets fragmented
  - Or there is buggy middleware
  - Or worse

BIND: DS Timeout



Unbound: DS Timeout

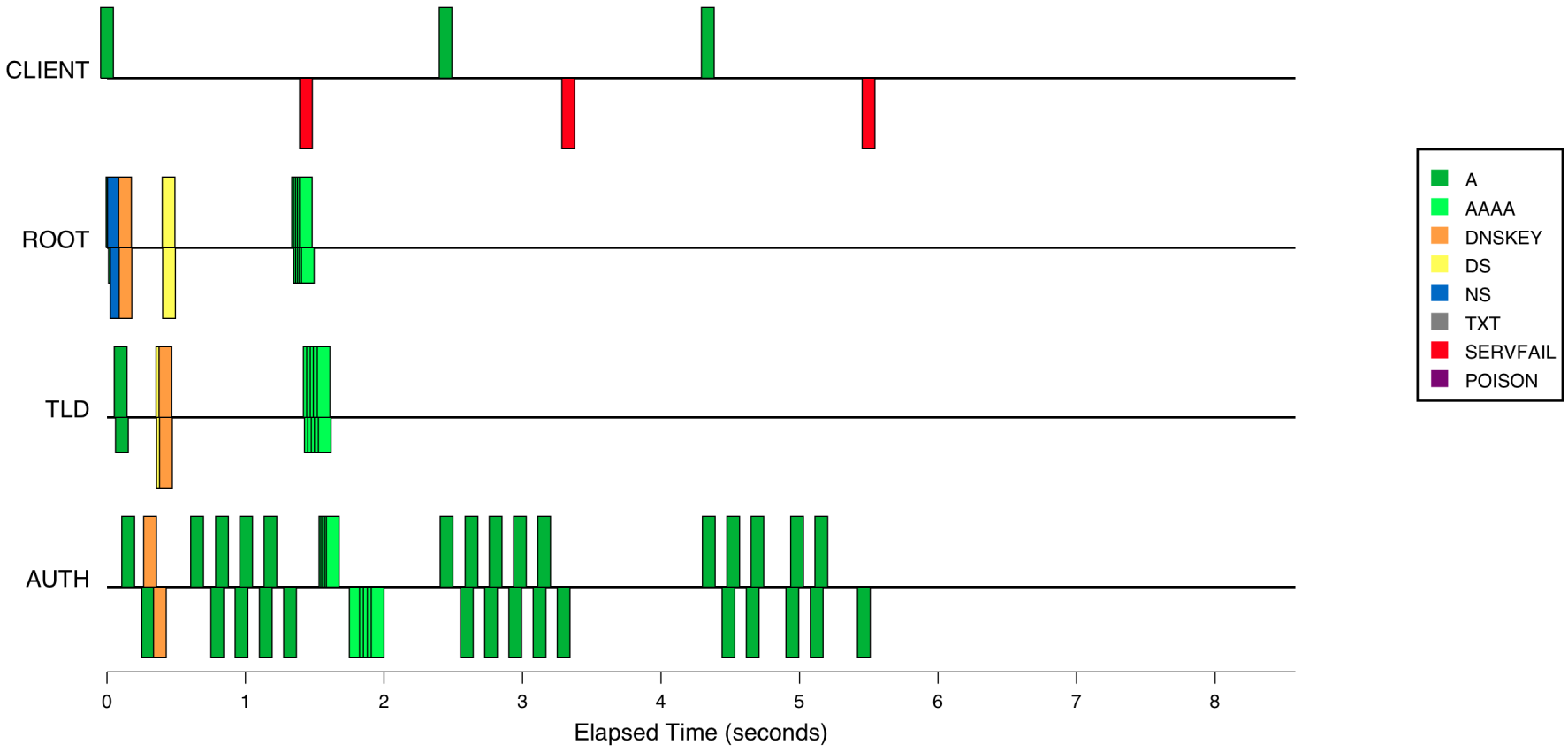


Unbound seems to be happy with DS records in the referrals and never issues queries of type DS.

Bad Signature

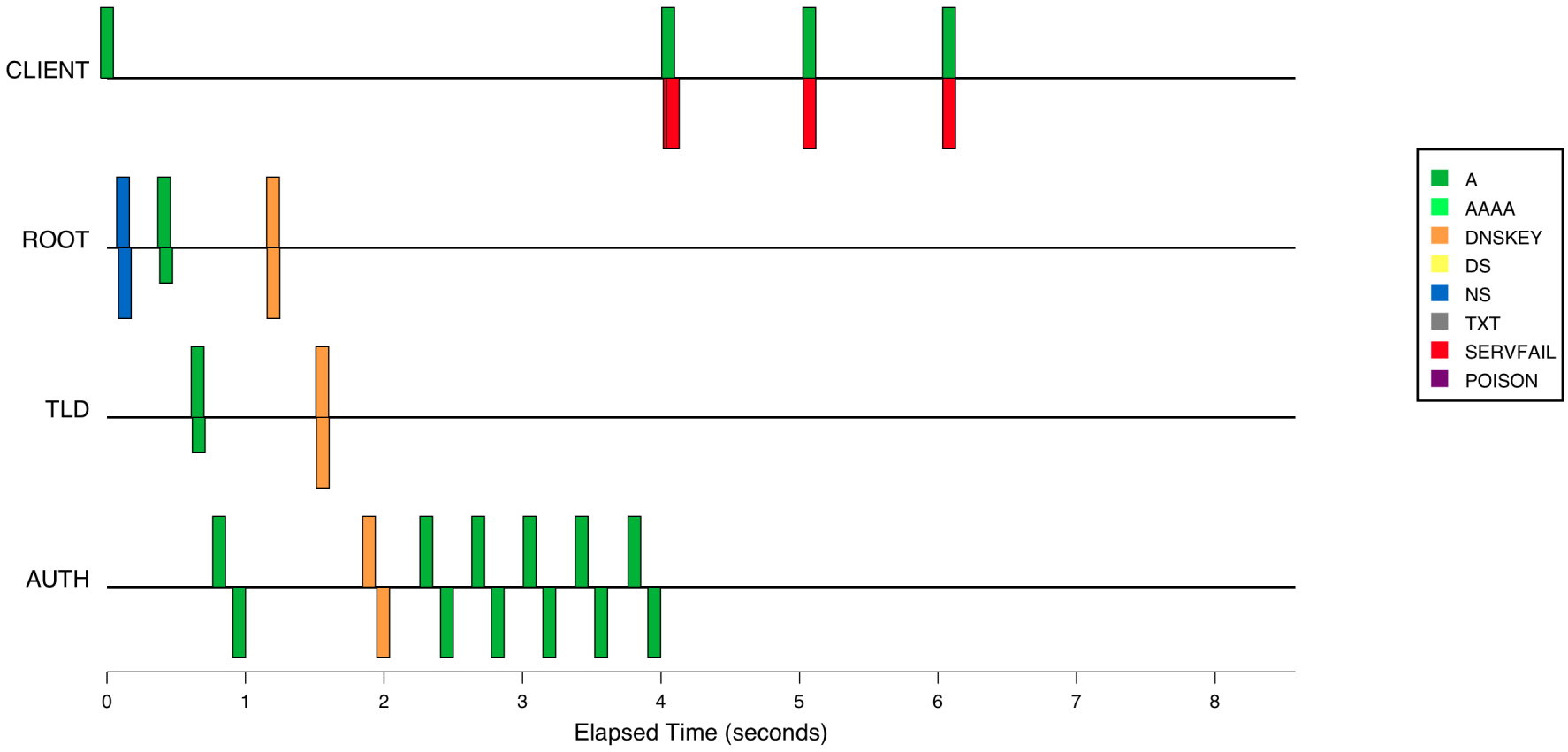
- Client issues queries for www.example.net
- Resolver receives spoofed response with a bad RRSIG
- (Resolver never receives response with good RRSIG)

BIND: Bad RRSIG



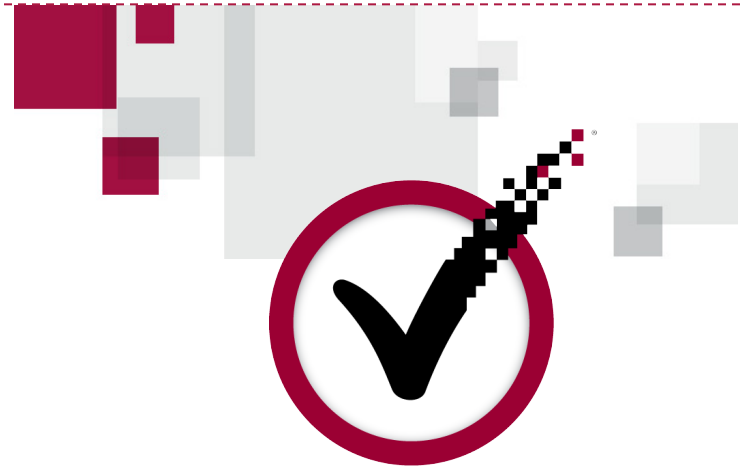
BIND does not cache the failure – subsequent queries result in more queries to the authority server.

Unbound: Bad RRSIG



Note Unbound adds the validation failure to the “bad cache” and does not forward subsequent queries.

VeriSign®



Questions?

Duane Wessels

dwessels@verisign.com