Try DNS-over-TLS

If you want to try out DNS-over-TLS then instructions are listed below.

Alternatively

- Use Stubby as your local DNS-over-TLS resolver
- watch a short video demonstrating TCP connection re-use, pipelining, TCP Fast Open and DNS-over-TLS: DNS-over-TLS demo video

Try DNS-over TLS

Grab a DNS-over-TLS client tool:

- Grab the latest version of getdns or
- Grab the patch to ldns-1.6.17
  https://portal.sinodun.com/stash/projects/TDNS/repos/dns-over-tls_patches/browse/ldns-1.6.17_dns-over-tls.patch

Query a public NSD server patched to support DNS-over-TLS:

- Verisign Labs are kindly hosting a zone on a server running NSD patched to support DNS-over-TLS for testing purposes.
  - The zone is named starttls.verisignlabs.com and it has A, AAAA, and TXT records for names from 'A' to 'Z'.
  - The IP address of the server is currently 173.255.254.151 - it might change so check for yourself.

- To query with getdns, run 'make getdns_query' to generate the getdns_query wrapper script in the test *directory* then
  - getdns_query @<serverIP> -s -a -A -l L (Pipelined TLS queries)
  - getdns_query @<serverIP> -s -a -A -l LT (Pipelined TLS queries with fallback to TCP)
  - getdns_query @<serverIP>~<hostname> -s -a -A -l L -m (Pipelined TLS queries in strict mode using server hostname for authentication)

- To query this with drill use: (the IP address is used here simply to stop the server name resolution falling back to TCP because your local resolver doesn't support DNS-over-TLS).
  - drill -t @173.255.254.151 b.starttls.verisignlabs.com (to see TCP query)
  - drill -C @173.255.254.151 b.starttls.verisignlabs.com (to see DNS-over-TLS query)
  - drill -C -D @173.255.254.151 b.starttls.verisignlabs.com (to do a DNSSEC lookup using DNS-over-TLS)

Decode in Wireshark

- If you want to decode the DNS packets in Wireshark (use 1.12.1 or later)
  - download the server key file: nsd.key
  - configure the key in wireshark in Edit->Preferences
    - open the protocol list in the right hand menu and select SSL from the list
    - Click on the RSA keys list 'Edit' box and then click on 'New' in the dialog that appears
      - Enter '173.255.254.151' for the IP addresss, '53' for the port and 'http' or 'spdy' for the protocal (DNS is not yet available here).
      - Use the Key File selector to choose the nds.key file you downloaded
    - Save this by hitting OK, OK and Apply.
    - Back in the main window use the Analyze->Decode as... option to choose to decode as SSL
    - Click on one of the packets labelled 'Application data' and you should see an additional tab appear in the Packet bytes view window of wireshark labelled "Decrypted SSL data".

- The starttls.verisign.com zone is signed
- The verisignlab.com server also supports TCP Fast open, as do both drill and digit.