

DNS-over-TLS clients

- `getdns`
- LDNS (drill) 1.6.17
- Digit 1.4

`getdns` is currently the most feature rich client for DNS-over-TCP and DNS-over-TLS features. See the [DNS Privacy daemon - Stubby](#) web page for how to use it as a local DNS Privacy stub resolver.

getdns

- **Website:** <https://getdnsapi.net/>
 - `getdns` supports multiple features related to DNS privacy including persistent connections, strict and opportunistic privacy profiles and TLS authentication by hostname or SPKI pinset
- **API spec:** <https://getdnsapi.net/spec.html>
- **Source:** <https://github.com/getdnsapi/getdns>
 - See the first few sections on the [DNS Privacy daemon - Stubby](#) page for instructions on how to install and build `getdns` as a local stub resolver with TLS support from source.
- **API:** Use the api directly via C or any of the available [language bindings](#) (Python, Java, nodejs, PHP)
- **getdns_query:** Use API directly, or use with the wrapper script `getdns_query` (run 'make getdns_query' then `getdns_query` is found in the test directory):
 - `getdns_query @<serverIP> -s -a -A -I T` (Pipelined TCP queries)
 - `getdns_query @<serverIP> -s -a -A -I L` (Pipelined TLS queries)
 - `getdns_query @<serverIP> -s -a -A -I LT` (Pipelined TLS queries with fallback to TCP)
 - `getdns_query @<serverIP>~<hostname> -s -a -A -I L -m` (Pipelined TLS queries in strict mode using server hostname for authentication)
- **Daemon mode:** see the [DNS Privacy daemon - Stubby](#) page

LDNS (drill) 1.6.17

- **Source:** `ldns 1.6.17` source code available from this link to NLNet Labs: [ldns-1.6.7](#)
- **Patch:** Grab and apply the [patch to ldns-1.6.17](#) from our git repository. Also see the notes [here](#).
- **Query:** 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 @<serverIP> <query name>` (to see TCP query)
 - `drill -I -p1021 @<serverIP> <query name>` (to see TLS query)
 - `drill -C @<serverIP> <query name>` (to see STARTTLS query)
 - `drill -C -D @<serverIP> <query name>` (to do a DNSSEC lookup using STARTTLS)

Digit 1.4

- **Source:** Grab the digit client DNS-over-TLS tool from the ISI website: <http://www.isi.edu/ant/software/tdns/index.html>
- **Query:** Build digit with `openssl`:
 - create a file called *queries* containing a query name
 - `./digit -f queries -r <serverIP> -V -t tcp` (to see TCP query)
 - `./digit -f queries -r <serverIP> -V -t ssl` (to see DNS-over-TLS query)