DNS Privacy - Current Work

This page describes at a high level the progress in various areas of DNS Privacy work (most recent activity at the top) mainly focussed on DNS-over-TLS.

See past DNS Privacy work

October 2019

- Comcast begin a phase one of a DoH public beta: https://doh.xfinity.com/dns-query and a DoT public beta: dot.xfinity.com
- ICANN OCTO document including evaluation of encrypted DNS: Local and Internet Policy Implications of Encrypted DNS
- Mozilla release FAQ on DoH: DNS over HTTPS FAQs.
- DNSCrypt implements a scheme similar in concept to Oblivious DNS ANONYMIZED DNSCRYPT
- Nice article on DNS Security: Threat Modeling DNSSEC, DoT, and DoH from netmeister.org
- Netherlands National Cyber Security Centre publishes a factsheet on DNS monitoring Factsheet DNS monitoring will get-harder
- Opera announces experimental support fro DoH on an opt-in basis.

September 2019

- Another blog from Bert Hubert: Centralised DoH is bad for privacy in 2019 and beyond
- IMC Paper: An Empirical Study of the Cost of DNS-over-HTTPs
- And today the Encrypted DNS Deployment Initiative launches: " a collaborative effort to ensure the smooth global adoption and reliable operation of DNS encryption technology. "
- Chrome announces experiment to upgrade to DoH with existing DNS provider
- OpenBSD has disabled DoH in their Firefox packages
- Firefox announce rollout of DoH by default in the USA during September.... and it will use Cloudflare
    - And a non-standard method to disable it.....
    - And details of how to do this in BIND
- And.... some reaction about the Firefox DoH announcement...
    - CircleID - http://www.circleid.com/posts/20190906_dns_over_https_the_privacy_and_security_concerns/
    - ISP Review - https://www.ispreview.co.uk/index.php/2019/09/headache-for-uk-isps-as-firefox-adopt-dns-over-https-by-default.html
    - Think Broadband - https://www.thinkbroadband.com/news/8525-doh-on-its-way-to-firefox-for-usa-users-first
    - ZDNet - https://www.zdnet.com/article/mozilla-to-gradually-enable-dns-over-https-for-firefox-us-users-later-this-month/
    - Computer Business Review - https://www.cbronline.com/news/firefox-dns-over-https
    - Engadget - https://www.engadget.com/2019/09/07/firefox-dns-over-https-by-default/
    - Forbes - https://www.forbes.com/sites/zakdoffman/2019/09/08/firefox-announces-major-new-encryption-default-to-protect-millions-of-users/#2ee8308518c0
    - MenaFN - https://menafn.com/1098979803/India-Soon-Firefox-will-encrypt-domain-name-requests-by-default

August 2019

- Great study on fingerprinting websites based on Encrypted DNS Queries encrypted-dns-privacy-a-traffic-analysis-perspective
- BIND announce future support for DoT in their annual report ISC annual report
- Various of opinion pieces on DoH/DoT
    - InfoBlox Blog 'DoT DoH and the DNS Last Mile Security Problem'
    - Nice article from Stacie Hoffman on 'Recalibrating the doh debate'
- UK Internet Watch Foundation writes to the UK secretary of State about DoH.
- Experimental support for DoH in Knot Resolver

July 2019

- IETF DPRIVE WG: New/updated drafts of using TLS for Zone transfers: DNS Zone Transfer over TLS and DNS Zone Transfer using DNS Stateful Operations
- ANRW Paper: Analyzing the Costs (and Benefits) of DNS, DoT, and DoH for the Modern Web
- Hackathon @ Africa Internet Summit 2019 results include measurement of DoH traffic Africa Hackathon results
- Enterprises openly discussing blocking DoH endpoints, and publishing lists of IPs
- Big twitter debates over the pros and cons of DoH to Cloudflare including
    - Declaration of the 'Streisand effect' happening
    - Allegations of the first malware using DoH
- UK ISPA announces finalists for 2019 Internet Villains, including Mozilla its for 'DoH by default' plans, then backs down but with detailed explanation because
- Mozilla finally make a clear statement about their Firefox DoH plans in the UK: 'We have no current plans to enable DoH by default in the UK', but they don't rule out other European countries.

June 2019

- IETF ADD BoF: Plans announced to hold a BoF at IETF 105 in Montreal for 'Applications doing DNS'
- IETF DNSOP WG: Latest version of a mechanism to discover recursive resolver information including DoT/DoH: DNS Resolver Information Self-publication
- Google officially launches its Public DoH service
- A flurry of opinion papers, meetings and media discussion about DoH/DoT
    - ICANN 65 (Policy Forum): Policy Aspects of DNS over HTTPS (DoH), DNS over TLS (DoT) and Related Issues
    - Eurodig 2019: 'DNS over HTTPS – What is it, and why should you care?'
    - The Open Rights Group Report
    - CENTR position paper on DoH
- NSD 4.2 supports DoT - first open source authoritative server to do this!

May 2019

- Interesting analysis of the current DoT/DoH software picture: https://doh.defaultroutes.de/implementations.html
- UK House of Lords Agenda for 14th May includes a Question on DoH. This follows much media coverage in the UK e.g.
    - The Times article "Warning over Google Chrome browser's new threat to children"
    - Daily Mail "Google's plans for new encrypted Chrome web browser could make it harder for UK government to stop computer users watching porn online"
        - "Crisis talks are being held on May 8 by the National Cyber Security Centre (NCSC), part of GCHQ, to discuss the risks the new encrypted browser will present, "
    - PC Pro article on DoH
- Much discussion of DoH at 2019 the ICANN DNS Symposium (including a panel in the afternoon session)
    - Good talk on the DoH Dilema by Vittorio Bertola
    - ISP centric view of DoH by Andy Fidler of British Telecom
    - And the view of Paul Vixie on Benefits and Hazards of Non- Local DNS Resolution
    - Panel on DoH (1hr 50 mins into this recording)
- Interesting.... https://www.nextdns.io: "The next-generation DNS", a hosted, private DNS resolver with DoT and DoH support and blocklists.
- Quad9 have launched their own mobile app "Quad9 Connect" for Android
    - Along with a statement they will never host web content on the same IP as a DoH endpoint.
- The ISP Internet Initiative Japan (IIJ) launches a Beta trail of DoT and DoH (article is in Japanese)

April 2019

- Mozilla statement on their DoH TRR policy requirements.
- Knot resolver adds experimental DoH in 4.0.0!
- Latest results from Mozilla on their Firefox DoH testing

March 2019

- So much discussion of DoT/DoH at IETF 104:
    - The DoH WG is still discussing the ins and outs of a proposed discovery mechanism: https://datatracker.ietf.org/doc/draft-ietf-doh-resolver-associated-doh/
    - Statement from Mozilla on future deployment plans: https://mailarchive.ietf.org/arch/msg/doh/po6GCAJ52BAKuyL-dZiU91v6hLw
    - Also a statement from Google Chrome on their DoH plans: https://mailarchive.ietf.org/arch/msg/dnsop/GE8v2Yz6zsl28clDvlshGh3rYlc
    - Side meeting on 'DoH/DoT deployment models and centralisation of DNS services' produced much discussion if no conclusions or concrete actions....
    - DPRIVE WG discussed the Future requirements, The DNS Privacy Operator BCP, DNS Privacy Application policy, Authentication of Authoritative servers and Bootstrapping mechanisms!
- The Stubby chocolatey package is now accepted and has the name stubby (thanks to the chocolatey folks - the previous stubby package was renamed!).
- A trio of drafts discussing DoH deployment issues causing much discussion on the IETF DOH/DPRIVE/DNSOP mailing lists:
    - https://datatracker.ietf.org/doc/draft-livingood-doh-implementation-risks-issues/
    - https://datatracker.ietf.org/doc/draft-reid-doh-operator/
    - https://datatracker.ietf.org/doc/draft-bertola-bcp-doh-clients/

- Nice intro to DNS Privacy from ISOC
- Work has started on a chocolatey package for Stubby: https://chocolatey.org/packages/stubby-dns/0.2.5.0 It is submitted and waiting for moderation (the name 'stubby' was already taken!)
- New Windows Installer for Stubby available (v0.2.5 stubby/v1.5.1 getdns/V1.1.1b OpenSSL). There have been changes to versioning and file installation. Please see the release notes at Windows Installer for Stubby.

February 2019

- Write up by Bert Hubert giving a good overview of the FOSDEM DNS privacy panel discussions
- New Windows Installer for Stubby available (v0.2.5 stubby/v1.5.1 getdns/V1.1.1a OpenSSL)
- Lots of action at FOSDEM surrounding DoH:
    - DNS Privacy Panel with Bert Hubert, Daniel Stenberg and Stéphane Bortzmeyer
    - The DoH Dilemma by Vittorio Bertola
    - DNS over HTTPS - the good, the bad and the ugly by Daniel Stenberg

January 2019

- More details on support for Stubby in Asuswrt-Merlin
- Adguard servers added to the DNS Privacy Public Resolvers page.
- Google launch a DoT service! Credentials are added to Stubby in the 0.2.5 release.
- Some nice articles by Fernando Gont of ISOC on DoH support in Firefox and Issues with DoT in systemd
- Unbound version 1.8.3 now supports EDNS(0) Keepalive and TCP connection management

Nov 2018

- A write up of our most recent Benchmarking work is now available: Follow-up Performance Measurements (Q4 2108)
- Interesting APNIC blog on 'Opinion: consolidation, centralization, and the Internet architecture' by Jari Arkko
- Privacy advocate Senator Wyden urges DHS to adopt encrypted DNS
- Interesting work on DoH monitoring by the HPRC group at the IETF 103 Hackathon

October 2018

- DoH becomes a RFC: RFC8484 - 'DNS Queries over HTTPS (DoH)'
- White paper at PETS on traffic analysis of DoH traffic: 'DNS Privacy not so private: the traffic analysis perspective'
- Recent talks on DoT/DoH:
    - OARC 29: Where will encrypted DNS transports push DNS operators?- Slides, Video
    - OARC 29: Operational experience for DNS over HTTPS (DoH) and DNS over TLS (DoT)- Slides, Video
    - RIPE 77: It's DNS Jim, But Not as We Know It - Slides, Video
    - RIPE 77 DNS WG: DNS Privacy measurements (Benchmarking DoT) - Slides, Video
    - RIPE 77 BCOP TF: Implications of DNS over anything but UDP - Slides, Video
- Thanks to Jonathan Underwood for all his work on Stubby in OpenWRT!
- Chrome is working on exposing DoH via a user configuration option with a drop down list and user defined option.
- Quad9 announce support for DoH!
- More dual DoT & DoH servers thanks to DNS Warden!

Sept 2018

- Video of a UKNOF presentation on considerations for operators of encrypted DNS.
- More testing of Firefox+Cloudflare in Firefox Beta, but also no clear statement on future plans.
- Adding CleanBrowsing and Tenta servers to the Test Servers page.
- New draft proposing a way to (insecurely) discover a DoH server on your local network.
- Great blog by Bert Hubert of PowerDNS on using third party DNS providers.

Aug 2018

- Firefox announces the results of its DoH experiment but still no work on the future default config options.
- Thanks to john9527 for stubby support in his Asuswrt-Merlin LTS fork.
- And Firefox nightly now has a UI for configuration of the DoH server
- The awesome folks at PowerDNS have an experimental DoH service and are working to add DoH to dnsdist - details in this mail post.
- Android Pie 9 includes Opportunistic DNS-over-TLS - woot!
- I-D draft-dickinson-dprive-bcp-op has been adopted by the DPRIVE WG
- Many thanks to BlahDNS for setting up a DNS-over-TLS service. Servers in both Germany and Japan!

Jul 2018

- Lots of interesting discussion at IETF 102 on DRIU (DNS Resolver Identification and Use) and 'Resolverless DNS'
- Centr interview "The DNS community brought DNS over HTTPS on itself"
- Great work at the IETF 102 Hackathon on Oblivious DNS, DoT for recursive to authoritative and DoH!
- Talk from the ICANN DNS Symposium on 'Where's my DNS?' (video)- questions about current and future DNS resolution on end user devices including the current status of DoH.
- Many thanks to Fondation RESTENA (the NREN for Luxembourg and the registry for the .lu ccTLD) for setting up a DNS-over-TLS privacy server!

Jun 2018

- Great news - the latest systemd-resolvd release now supports DNS-over-TLS!
- Interesting work by the folks at Bromite (a privacy focused fork of Chromium that runs on Android). They just enabled the Chromium DoH implementation by exposing configure options (via chrome://flags). See this user guide.
    - Oh, and they do a neat fingerprint detection page to see what your browser sends about you in HTTP headers!
- Awesome tutorial by linuxbabe.com about using Stubby on Ubuntu Desktop!
- The DoH draft is in WGLC and is getting significant discussion!

    - The amazing folks at dnsdist are working on implementing DoH and finding important issues with the draft
- Mozilla have been blogging about their plans for using DoH
    - Here's the details of how it works and how to configure it
    - Heres a blog in their general strategy

May 2018

- DPRIVE WG at IETF just re-chartered to cover adding confidentiality to recursive to authoritative exchanges.
- Interesting presentations from the DNS WG @ RIPE 76
    - Measurements on DNS Privacy (DNS-over-TCP and TLS benchmarking)
    - High Performance DNS-over-TCP
    - A Survey on DNS Privacy
    - Deploying DNS-over-TLS at RIPE
    - BCOP WG - DNS Privacy PCP
    - Dude, where's my DNS? (subtitle 'DNS-over-HTTPS is coming!')
- The Stubby Windows installer and macOS GUI App are both updated to use the getdns 1.4.2rc1 and stubby 0.2.3rc1 releases.
- Unbound 1.7.1 now supports authentication of DNS-over-TLS using PKIX certificates!

April 2018

- Thanks to Matthew Vance for a docker image combining Stubby and Unbound.
- Android announcement about the DNS-over-TLS support in Android P Developer preview.
- We are excited about the new proposal for for Oblivious DNS to hide queries from resolver operators
- Cloudflare now running an open recursive resolver with DNS-over-TLS and DNS-over-HTTPS! Details on the Test Servers page.
- The latest release of dnsdist includes support for DNS-over-TLS - thanks PowerDNS folks!
- RFC8310 is now published: Usage Profiles for DNS over TLS and DNS over DTLS
- Write up of the IETF101 Hackathon work on DoH.

March 2018

- First version of Recommendations for DNS Privacy Operators is now published as a IETF draft for review.
- Videos from the DNS Privacy Workshop 2018 are now available on You Tube on the DNS Privacy Project Channel
- ISC announce the next version of BIND 9 will include QNAME minimisation
- Also, 3 of the dnsovertls(N).sinodun.com servers are running BIND 9.12 and are now padding responses!

February 2018

- Live traffic for a subset of Test servers now available
- Interactive map of the DNS Privacy test server locations now available
- Another new test server using Knot resolver - thanks the folks at dns.neutopia.org
- Nice talks at FOSDEM yesterday from Stephane Bortzmeyer on DNS Privacy and Willem Toorop on Stub resolvers
- The getdns and stubby packages are now available in LEDE OpenWRT!
- Latest release of Knot Resolver does TLS forwarding upstream!

January 2018

- We are now using a new and improved getdns based monitoring plugin for our Test Server Monitoring dashboard which can test more server capabilities!
- Two more Test servers now listen on port 443: dnsovertls.sinodun.com and dnsovertls1.sinodun.com
- Thanks to the Knot Resolver folks for quick fixes to some issues with DNS-over-TLS support - the latest release (1.5.1) seems much more stable!
- We note that dnscrypt.org is now re-directed to this site due to changes in the DNSCrypt project status
- We also have additional documentation on automating certificate renewal

December 2017

- Check out the interesting privacy work and products coming out of the Tenta project - in particular their Tenta browser, open source DNS resolver and comparison of DNS-over-TLS vs DNSCrypt!
- 2 new test servers:
    dnsovertls3.sinodun.com**which supports TLS 1.3** and TLS 1.2 (thanks again to Surfnet for hosting)!
        - Version 1.3.0 of getdns (to be release Dec 21st) will support TLS 1.3 when linked against OpenSSL 1.1.1, so build stubby against that to that if you want to test out TLS 1.3!
    - dns.bitgeek.in based in India - many thanks Sairam Kunala!
- Windows Installer is updated to use the getdns 1.2.1rc-1 and Stubby 0.2.0 releases!
- We now have an alpha release of a prototype StubbyManager GUI for macOS. This is a work in progress!
- Quad9 is now added to the Test servers pages

November 2017

- Excellent blog post by Stephane Bortzmeyer about the new Quad9 service. (Note that Quad9 have not themselves announced official DNS-over-TLS support)
- Also a blog post from Alex Band on configuring Stubby with Quad9.
- Work at the IETF Hackathon on DANE verification of DNS-over-TLS servers. Congrats to the DNS team who won overall best contribution!
- Check out a new docker image providing Stubby using Quad9

October 2017

- We have three new test servers added during October - thanks to Lars de Bruin and Gerold Krötlinger!
- The first release of a Windows installer for the Stubby CLI tool is announced. Please test! (A GUI is on the way.....)
- The DNS Privacy Workshop will again be co-located with NDSS in San Diego - February 2018.
- We have a new DNS Privacy server in South America - Thank you NIC Chile!
- We talked at OARC 27 about DNS Privacy clients. You tube video available.

September 2017

- Jan Zorz has written an excellent article about his experience trying to set up DNS Privacy. We got lots of useful feedback from him and are working on the issues he found! Thanks Jan.

August 2017

- We are very pleased to announce that the OTF is now generously funding work by dnsprivacy.net!
- We are pleased to announce that there is now an official Homebrew formula for Stubby!
- Stubby now has its own source code repository.

July 2017

- The IETF EDU Privacy Tutorial is happening again at IETF 99! Slides are here: DNS Privacy Tutorial.
- We have a new DNS Privacy server in Asia!! See Experimental DNS-over-TLS Servers
- We are talking on 6th July about getdns, Stubby and DNS Privacy at AFNIC JCSA!
- Here is our presentation from RMLL!

June 2017

- **NEW!** We now have live monitoring of the Experimental DNS Privacy servers
- A short video on our work at the IETF Hackathons is now available!
- We have several new Experimental DNS-over-TLS servers now
- The DNS Privacy Tutorial is going to be given again at IETF 99 in Prague

May 2017

- Here's a presentation on DNS-over-QUIC from OARC (slides, video - got to 8:04 hrs in)
- Here's our presentations on dnsprivacy.net at OARC (slides, video - go to 6:45 hrs in) and RIPE (slides, video)
- The dnsprivacy.org website content has now been migrated to its own server after being hosted on portal.sinodun.com.

April 2017

- New Internet Draft on DNS in dedicated QUIC Connections and lots of interesting drafts around DNS over HTTP getting discussion
- Latest 1.1.0 release of getdns includes Stubby!
- The DNS Privacy team is highlighted in the IETF Hackathon Videos
- We'll be talking at both the RMLL conference (5th July) and at JCSA in Paris (6th July) about DNS Privacy
- We are proud to add Salesforce as supporters of the DNS Privacy project!

March 2017

- Great work at the IETF 98 Hackathon on DNS Privacy. In particular see Stephane Borztmeyer's blog on his DNS-over-TLS monitoring plug-in.
- Proceedings from the NDSS DNS Privacy workshop are available here.
- Thanks to Matthew Ford from ISOC for a great write up of the workshop.
- We'll be talking at OARC about dnsprivacy.net

February 2017

- We are very pleased to announce a new donation from NLnet Foundation to support work on Stubby. Thank you for your generous support!!
- Preliminary agenda published for NDSS DNS Privacy Workshop (26th Feb, San Diego)
- DNS Privacy will be a topic at the IETF 98 Hackathon - please come along!

January 2017

- Planning under way for the NDSS DNS Privacy workshop on 26th February in San Diego
- https://datatracker.ietf.org/doc/draft-ietf-dprive-dtls-and-tls-profiles/ has cleared WGLC
- 1.0.0 release of getdns (which supports DNS-over-TLS)
- Knot resolver 1.2.0 released with improved DNS-over-TLS support
- Warren Kumari has provided a Docker container for easy deployment of a DNS-over-TLS server!

December 2016

- Improved usability for Stubby planned for the 1.1.0-alpha3 release
- The content of this site is now available via the dnsprivacy.org site.
- CoreDNS now offers DNS-over-HTTPS (as well as DNS-over-TLS). Also see dingo if interested in DNS-over-HTTPS clients.

November 2016

- IETF 97 EDU team held a DNS Privacy Tutorial, which got coverage in both Heise and two articles in The Register: The_Register_22Nov, The_Register_6Dec
- More work at the Hackathon on Knot Resolver DNS Privacy implementation, TCP support in BIND and Stubby. A further DNS Privacy test server made available thanks to dkg.
- DPRIVE working group discussed a possible re-charter to focus work on the Resolver to Authoritative problem.
- DNS-over- HTTP(S) BOF held

October 2016

- 2 more test DNS Privacy resolvers made available (Thanks to Surfnet for resources!)
- getdns version 1.1.02-alpha released with a prototype implementation of Stubby - a DNS Privacy stub resolver
- https://datatracker.ietf.org/doc/draft-ietf-dprive-dtls-and-tls-profiles/ moved into Working Group Last Call
- https://datatracker.ietf.org/doc/draft-mayrhofer-dprive-padding-profile/ was published to propose specific policies for padding DNS packets
- https://datatracker.ietf.org/doc/draft-ietf-dnssd-privacy/ adopted by the DNS-SD working group

September 2016

- https://datatracker.ietf.org/doc/draft-ietf-dprive-dnsodtls/ passed WGLC with status 'Experimental' and was submitted to IESG for review

August 2016

- WGLC starts for https://datatracker.ietf.org/doc/draft-ietf-dprive-dnsodtls/

July 2016

- https://datatracker.ietf.org/doc/draft-bortzmeyer-dprive-step-2/ was published as a first step in describing the Resolver to Authoritative problem

June 2016

- OARC made a test DNS Privacy server available - many thanks!

May 2016

- Presentation in the RIPE DNS working group on experimental deployments of DNS Privacy servers.
- RFC7858 Published: Specification for DNS over Transport Layer Security (TLS)

April 2016

- Work at the IETF Hackathon in Buenos Aires to start implementing TLS in Knot resolver

March 2016

- getdns 1.0.0b1 release!
- RFC7816 Published: DNS Query Name Minimisation to Improve Privacy

February 2016

- EDNS0 Keepalive draft approved for publication as RFC7828

January 2016

- 5966bis draft approved for publication as RFC7766
- *Authentication and (D)TLS Profile for DNS-over-TLS and DNS-over-DTLS* draft adopted by DPRIVE
- Testing of FreeBSD implementation of TCP Fast Open. Reported bug in linux client implementation of TFO (now fixed) and made feature request to OpenSSL to support client side TFO.
- Started work on Unbound patch to support TFO on Linux, FreeBSD and OS X.

December 2015

- Produced first version of *Authentication and (D)TLS Profile for DNS-over-TLS and DNS-over-DTLS* draft for submission to DPRIVE working group
- Client side EDNS0 keepalive option implemented in getdns
- SPKI pinset TLS authentication available in getdns

November 2105

- Attended IETF 94.
    - Participated in Hackathon including getdns implementation of EDNS0 Padding option
    - Last call review of DNS-over-TLS
    - Agreed to start work on combined draft for (D)TLS Authentication mechanisms

October 2015

- Attended OARC Fall Workshop. Presentationed onUsing TLS for DNS privacy in practice.
- Attended ICANN in Dublin, presented on *DNSSEC for Legacy applications* including discussing DNS privacy features of getdns.

August 2015

- Addition of TLS authentication using hostname to getdns

July 2015

- IETF 93
    - Work on getnds TLS authentication during Hackathon
    - Working group presentations on 59966-bis draft and https://tools.ietf.org/html/draft-ietf-dnsop-edns-tcp-keepalive-02
- 0.3 release of getdns including
    - New transport list options allowing user to flexibly specify an ordered list of accepted transport options from TLS, STARTTLS, TCP, UDP
    - Ability to configure idle timeout associated with TCP connections

May 2015

- 0.2 release of getdns including STARTTLS

April 2015

- Release of version 0.1.8 of getdns including TLS and TLS with fallback to TCP

March 2015

- Work started in getdns to implement dns-over-tls - Demo given at IETF92 in Dallas of proof-of-concept code.
- Publication of updated set of patches in the dns-over-tls repository
- Publication of https://tools.ietf.org/html/draft-ietf-dnsop-5966bis-01

January 2015

- Changed to using DNS-over-TLS instead of T-DNS
- Extend LDNS and NSD patches to include options to use the TO bit (for experimental inter-op testing)
- Publish LDNS code into repository for review
- getdns work put on hold, instead start work on Unbound server patch

November 2014

- Presenting at IETF 91
- Started work on T-DNS in getdns

October 2014

- Implementation of TCP Fast open support (linux only) in getdn for stub mode in 0.1.5 release.
- Testing of 0.1.5 getdns codebase which implements TCP pipelining.
- POC implementation of TCP Fast Open in ldns, Unbound and NSD.
- Patch released to implement STARTTLS in NSD.
- Released patch to ldns for connection re-use.

September 2014

- Continued helping to implement switch to ldns for stub mode in getdns.
    - Basic support for synchronous API implemented and per query namespaces also supported. (Note DNSSEC stub validation is still done by unbound at this point....)
- Creating patch for ldns/drill to support connection reuse for TCP. Using this from synchronous stub mode in getdns to demonstrate connection re-use.
- Work on TCP related drafts

August 2014

- Working on getnds
    - Added a new test to verify which transport queries are actually sent over
    - Helping to implement the switch to ldns for stub mode
    - Working on support for pipelining of TCP queries

July 2014

- Attended IETF 90 in Toronto and gave a demo of sending queries from drill to Unbound using T-DNS
- Started looking at pipelining multiple queries from drill to Unbound
- Extending test framework to test multiple scenarios for drill <-> Unbound
- Finished patch to drill to add extra options:
    - -l will send a single query over TLS
    - -L will send a single query over TLS after negotiating an upgrade using a STARTTLS/CH/TXT query
- Finished patch to Unbound to support 'upgrade_tls' configure option. This enables unbound to receive a a STARTTLS/CH/TXT query, send a STARTTLS/CH/TXT response when configured properly, upgrade to SSL and then receive a query over SSL.

June 2014

- Started work on Unbound <-> NSD hop
- Completing implementation in Unbound to get drill <-> Unbound hop working
- Implemented a patch to drill to support T-DNS for a single DNS query
- Discussions on the class to be used for the dummy query. The resolver -> authoritative hop might be better implemented with a IN class query.
- Start work on Unbound - understand current SSL-upstream implementation

- From Willem: LDNS does not have support for asynchronous operation so in the short term it will probably be used in getdns just in synchronous mode so that the implementation of TDNS can continue.
- Further work on test framework

May 2014

- Current getdns stub implementation cannot support sending of CH class queries as it uses libunbound which denies the query and never sends it onwards. Discussed in getnds meeting 19th May that further implementation of T-DNS in getdns will have to wait until libunbound is replaced with ldns for the stub mode. Current understanding is that Willem is going to tackle this in the next few weeks.
- Identified need to support CH class in getdns for dummy STARTTLS query. Start on implementation of this.
    - This implementation highlighted the need for getdns to gracefully handle refused queries that have no associated data.
- Created test harness to create a dummy STARTTLS query
- Agreed that initial implementations will use the dummy CH class query (not the TO bit)
- Forked getdns. Familiarisation with getdns code base - get it to install and run!
- Kick off meetings with T-DNS and getdns teams
- Creation of project issue tracker and wiki site
- Reading of relevant drafts and documentation - capture any early technical questions