draft-ietf-dprive-start-tls-for-dns-01

IETF 93, Prague

July 24, 2015

Changes since -00

- Incorporated a number of suggestions and comments from Daniel Kahn Gillmor, Sara Dickinson, and others.
- Removed a discussion question on utility of the TO in a UDP message. There was no input from the working group on this point.
- When a client receives TO=0 in response to TO=1 query, the client MAY (was SHOULD) use the established connection for unencrypted queries.
- Clarify that when TLS handshake fails, both sides must close the connection.

Changes since -00

- Rewrote the "established connection" section.
- This document no longer makes specific recommendations on idle timeouts. It defers to other documents.
- Added reference to TLS fast session resumption and mention of TLS false start work-in-progress.
- Added an "implementation status" section.

Strong TLS Profile

- We will add reference to RFC 7525 (BCP 195), Recommendations for Secure Use of TLS and DTLS.

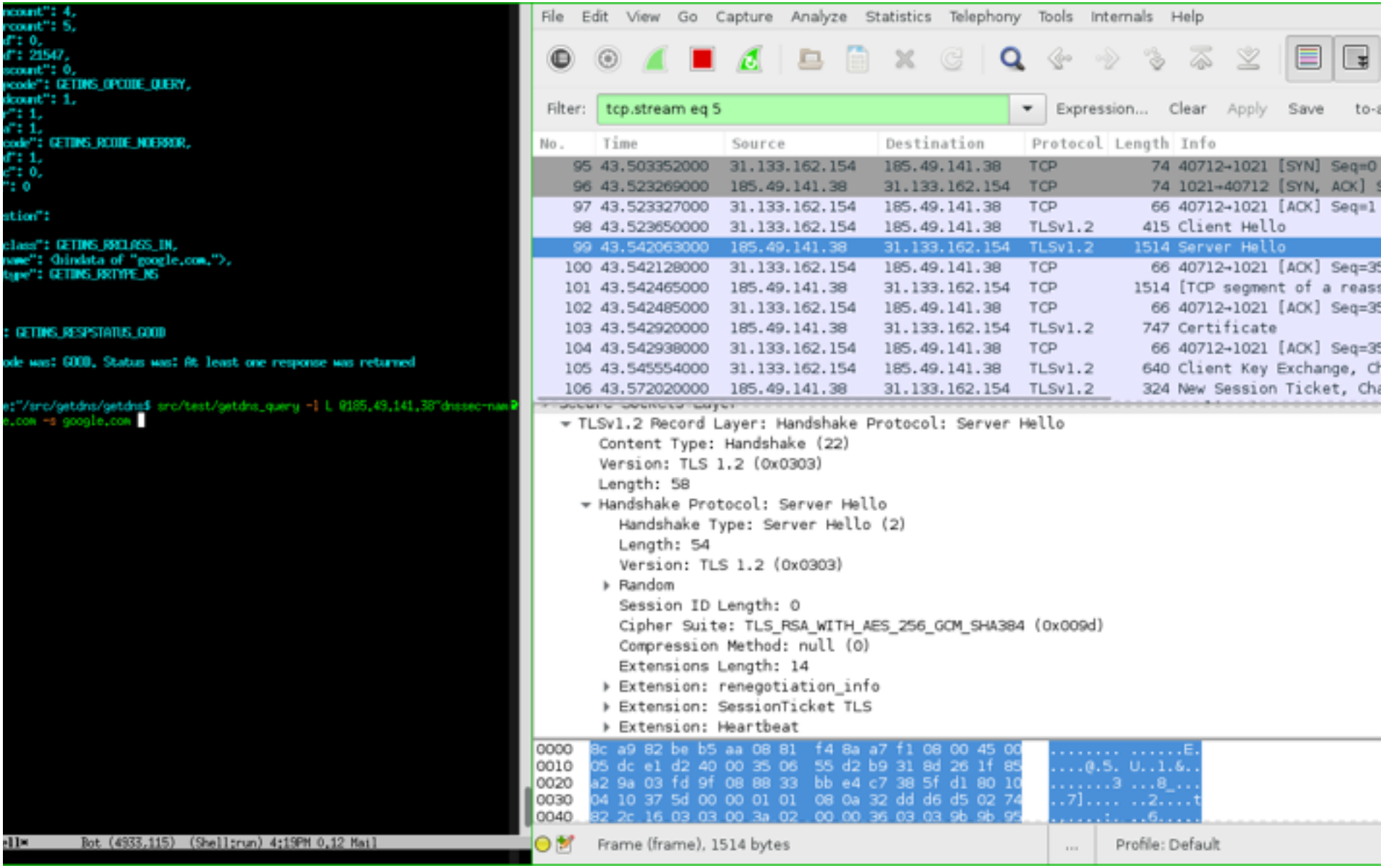
Discussion: Upgrade vs. Port

- Authors heard working group desire to eliminate “STARTTLS” upgrade approach from the draft.
- Would simplify implementations.
- We have asked the chairs to request RFC 7120 early allocation of port.

Implementation Status

- Unbound
  - supports port-based DNS-over-TLS since 1.4.14
  - upgrade-based patch for 1.5.1
- ldns & drill
  - port-based and upgrade-based patch
- digit (USC/ISI tool)
  - supports both port- and upgrade-based
- getdns (client)
  - port-based and upgrade-based
  - new: certificate authentication (hackathon!)

Hackathon Screenshot



Q & A