

dprive
Internet-Draft
Updates: [1035](#), [7230](#) (if approved)
Intended status: Informational
Expires: November 18, 2017

D. Gillmor
ACLU
May 17, 2017

Demultiplexing Streamed DNS from HTTP/1.x
draft-dkg-dprive-demux-dns-http-03

Abstract

DNS over TCP and HTTP/1.x are both stream-oriented, client-speaks-first protocols. They can both be run over a stream-based security protocol like TLS. A server accepting a stream-based client can distinguish between a valid stream of DNS queries and valid stream of HTTP/1.x requests by simple observation of the first few octets sent by the client. This can be done without any external demultiplexing mechanism like TCP port number or ALPN.

Implicit multiplexing of the two protocols over a single listening port can be useful for obscuring the presence of DNS queries from a network observer, which makes it relevant for DNS privacy.

Widespread adoption of the described approach could constrain evolution of the stream-based variants of both DNS ([[RFC1035](#)]) and HTTP/1.x ([[RFC7230](#)]) by ossifying existing distinguishing bit patterns in early octets sent by the client. However, this draft explicitly rules out multiplexing in this form with HTTP/2, so it should place no constraints on it or any higher version of HTTP.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on November 18, 2017.

Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	3
1.1.	Terminology	4
2.	Scoping	4
2.1.	Distinguish only at the start of a stream	4
2.2.	HTTP/2 is not always client-speaks-first	4
2.3.	Avoid multiplexing in the clear	5
2.4.	Avoid mixing with other demultiplexing	5
2.5.	Heavily-restricted network environments	5
2.6.	Why not ALPN?	5
3.	Overview of initial octets	6
3.1.	DNS stream initial octets	6
3.2.	HTTP/1.x initial octets	7
3.2.1.	HTTP/0.9	7
3.2.2.	HTTP/1.0 and HTTP/1.1	8
4.	Specific octets	9
4.1.	octets 0 and 1	9
4.2.	octets 2 and 3	9
4.3.	octet 4	10
4.4.	octet 5	10
4.5.	octets 6 and 7	11
4.6.	octets 8 through 11	11
4.7.	octets 12 and 13	11
5.	Combinations of octets	11
5.1.	Proof: a valid DNS message cannot be an HTTP/1.x query	12
6.	Guidance for Demultiplexing Servers	13
6.1.	Without supporting HTTP/0.9	13

6.2.	Supporting archaic HTTP/0.9 clients	13
6.3.	Signaling demultiplexing capacity	14
7.	Guidance for DNS clients	15
7.1.	Interpreting failure	16
8.	Guidance for HTTP clients	16

9.	Security Considerations	16
10.	Privacy Considerations	16
11.	IANA Considerations	17
12.	Document Considerations	17
13.	References	17
13.1.	Normative References	17
13.2.	Informative References	18
	Author's Address	19

[1.](#) Introduction

DNS and HTTP/1.x are both client-speaks-first protocols capable of running over stream-based transport like TCP, or as the payload of a typical TLS [[RFC5246](#)] session.

There are some contexts where it is useful for a server to be able to decide what protocol is used by an incoming TCP stream, to choose dynamically between DNS and HTTP/1.x on the basis of the stream itself (rather than a port designation or other explicit demultiplexing).

For example, a TLS terminator listening on port 443 and receiving either no ALPN token at all, or the "http/1.1" ALPN token might be willing to serve DNS-over-TLS [[RFC7858](#)] as well as HTTPS.

A simple demultiplexing server should do this demuxing based on the first few bytes sent by the client on a given stream; once a choice has been established, the rest of the stream is committed to one or the other interpretation.

This document provides proof that a demultiplexer can robustly distinguish HTTP/1.x from DNS on the basis of the content of the first few bytes of the client's stream alone.

A DNS client that knows it is talking to a server which is this position (e.g. trying to do DNS-over-TLS on TCP port 443 with no ALPN

token, used traditionally only for HTTPS) might also want to be aware of network traffic patterns that could confuse such a server. This document presents explicit mitigations that such a DNS client MAY decide to use.

This document limits its discussion to HTTP/1.x over TCP or TLS or some other classical stream-based protocol (it excludes HTTP over QUIC, for example, and HTTP/2 [[RFC7540](#)] or later). Likewise, it considers only the TCP variant of DNS (and excludes DNS over UDP or any other datagram transport).

[1.1.](#) Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[RFC2119](#)].

[2.](#) Scoping

[2.1.](#) Distinguish only at the start of a stream

A server which attempts to distinguish DNS queries from HTTP/1.x requests individually might consider using these guidelines in the middle of a running stream (e.g. at natural boundaries, like the end of an HTTP/1.1 request, or after a DNS message), but this document focuses specifically on a heuristic choice for the whole stream, based on the initial few octets sent by the client.

While it's tempting to consider distinguishing at multiple points in the stream, the complexities of determining the specific end of an HTTP/1.x request body and handling HTTP/1.x error cases make this more difficult to implement on the side of a DNS client configured to talk to such a server. Interleaving the responses themselves on a stream with multiple data elements is also challenging. So do not use this technique anywhere but at the beginning of a stream!

If being able to interleave DNS queries with HTTP requests on a single stream is desired, a strategy like [[I-D.hoffman-dns-over-https](#)] or [[I-D.ietf-dnsop-dns-wireformat-http](#)]

is recommended instead.

[2.2.](#) HTTP/2 is not always client-speaks-first

While this demultiplexing technique functions for HTTP/1.0 and HTTP/1.1, it does not work for HTTP/2 [[RFC7540](#)] because HTTP/2 is not guaranteed to be a client-speaks-first protocol. In particular, many HTTP/2 servers prefer to send a SETTINGS frame immediately without waiting for data from the client, if they already know they're speaking HTTP/2. In the event that HTTP/2 is to be transported over TLS, the ALPN token negotiated in the TLS handshake is "h2", which allows the server to know as soon as the handshake is complete that it can start pushing data to the client.

A standard DNS-over-TLS client connecting to a server that might be multiplexing DNS with HTTP on the same listener MUST NOT indicate an intent to speak HTTP/2 that could prompt this unsolicited first flight from the server. Concretely, a DNS client connecting over TLS

on TCP port 443 expecting to speak standard DNS-over-TLS [[RFC7858](#)] MUST NOT offer or accept the "h2" ALPN token.

If use of DNS in the same channel as HTTP/2 is desired, a strategy like [[I-D.hoffman-dns-over-https](#)] is recommended instead.

[2.3.](#) Avoid multiplexing in the clear

The widespread deployment of transparent HTTP/1.x proxies makes it likely that any attempt to do this kind of multiplexing/demultiplexing on a cleartext channel that normally carries HTTP/1.x (e.g. TCP port 80) will fail or trigger other "interesting" behaviors. The approach described in this draft should be done only in channels sufficiently obscured that a transparent proxy would not try to interpret the resultant stream.

[2.4.](#) Avoid mixing with other demultiplexing

Some other (non-IETF) systems (e.g. [[HAPROXY](#)]) take a similar approach with multiplexing data on top of HTTP/1.x by taking advantage of bitpatterns that are presumed to not be present in normal HTTP/1.x requests.

Use of the approach described in this draft in conjunction with these other approaches is not advisable. Doing so safely would require explicit and detailed review of all three (or more) protocols involved.

[2.5.](#) Heavily-restricted network environments

Some network environments are so tightly constrained that outbound connections on standard TCP ports are not accessible. In some of these environments, an explicit HTTP proxy is available, and clients must use the HTTP CONNECT pseudo-method to make https connections. While this multiplexing approach can be used in such a restrictive environment, it would be necessary to teach the DNS client how to talk to (and through) the HTTP proxy. These details are out of scope for this document. A DNS client capable of this additional layer of complexity may prefer to pursue a strategy like [\[I-D.hoffman-dns-over-https\]](#) instead.

[2.6.](#) Why not ALPN?

If this is done over TLS, a natural question is whether the client should simply indicate its preferred protocol in the TLS handshake's ALPN [\[RFC7301\]](#) extension (e.g. with some new ALPN token "dns").

However, ALPN tokens requested by the client are visible to a network observer (and the ALPN token selected by the server is visible to a network observer in TLS 1.2 and earlier), so a network controller attempting to confine the user's DNS traffic to a limited set of servers could use the ALPN extension as a signal to block DNS-specific streams.

Another alternative could be an ALPN token that indicates potentially-multiplexed traffic (e.g. "http/1.1-or-dns"). This has a comparable problem when confronted with a network adversary that intends to penalize or hamper DNS-over-TLS. Existing HTTP clients will not send this token, and even if some start to offer it, it will provide less cover for DNS-over-TLS clients.

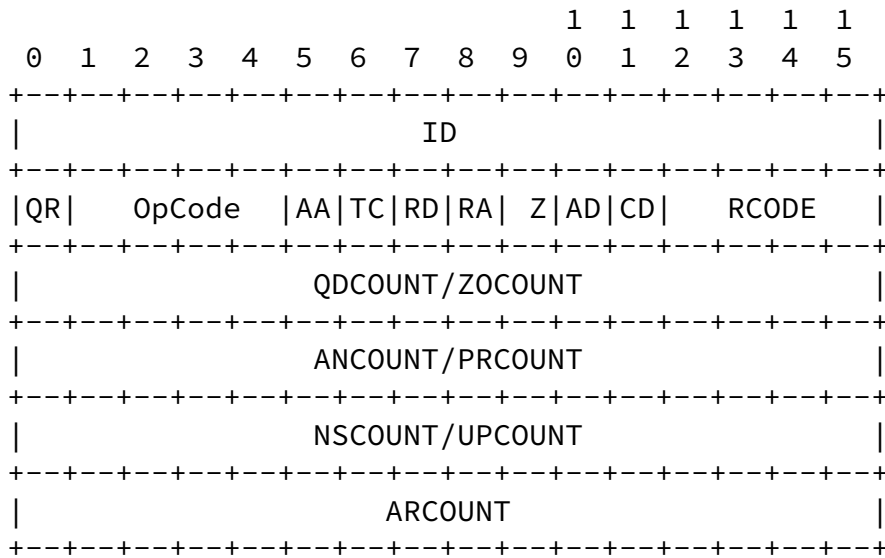
[3.](#) Overview of initial octets

3.1. DNS stream initial octets

[RFC1035] [section 4.2.2](#) ("TCP Usage") shows that every stream-based DNS connection starts with a DNS message, preceded with a 2-octet message length field:

The message is prefixed with a two byte length field which gives the message length, excluding the two byte length field.

[RFC6895] [section 2](#) represents the DNS message header section, which is the first part of the DNS message on the wire (after the message length).



So in a DNS over TCP stream, the interpretation of the initial 14 octets are fixed based on information about the first query sent on the stream:

- o 0,1: length of initial DNS message
- o 2,3: DNS Transaction ID
- o 4,5: DNS opcode, flags, and response code
- o 6,7: Question count (or Zone count in UPDATE)

- o 8,9: Answer count (or Prerequisite count in UPDATE)
- o 10,11: Authority count (or Update count in UPDATE)
- o 12,13: Additional RR count

All DNS streams sent over TCP start with at least these 14 octets.

[3.2.](#) HTTP/1.x initial octets

In an HTTP stream before HTTP/2, the first octets sent from the client are either the so-called "Simple-Request" (for HTTP/0.9) or the "Request-Line" (for HTTP/1.0 and HTTP/1.1). The data in this initial stream has variable characteristics.

Most servers may wish to ignore the oldest of these, HTTP/0.9.

[3.2.1.](#) HTTP/0.9

[RFC1945] [section 4.1](#) says that HTTP/0.9 queries (that is, HTTP queries from before HTTP/1.0 was formalized) use this form:

Simple-Request = "GET" SP Request-URI CRLF

Note that HTTP/0.9 clients send this string and only this string, nothing else (no request body, no subsequent requests). The "Request-URI" token is guaranteed to start with a printable ASCII character, and cannot contain any members of the CTL class (values 0x00 through 0x1F) but due to loose early specifications, it might sometimes contain high-valued octets (those with the most-significant bit set - 0x80 or above).

So the first 5 octets are all constrained to be no less than 0x20 (SP) and no more than 0x7F (DEL), and all subsequent octets sent from the client have a value at least 0x0A (LF).

The shortest possible HTTP/0.9 client request is:

char:	G	E	T	SP	/	CR	LF
index:	0	1	2	3	4	5	6

The lowest possible HTTP/0.9 client request (sorted ASCIIbetically)

is:

```
char: G   E   T   SP +   :   CR LF
index: 0   1   2   3   4   5   6   7
```

[3.2.2.](#) HTTP/1.0 and HTTP/1.1

The request line format for HTTP/1.1 matches that of HTTP/1.0 (HTTP/1.1 adds protocol features like pipelining, but doesn't change the request form itself). But unlike HTTP/0.9, the initial verb (the "method") can vary.

[RFC7230] [section 3.1.1](#) says that the first line of an HTTP/1.1 request is:

```
request-line  = method SP request-target SP HTTP-version CRLF
method        = token
```

and [\[RFC7230\] section 3.2.6](#) says:

```
token          = 1*tchar

tchar          = "!" / "#" / "$" / "%" / "&" / "'" / "*"
                / "+" / "-" / "." / "^" / "_" / "`" / "|" / "~"
                / DIGIT / ALPHA
                ; any VCHAR, except delimiters
```

and VCHAR is defined in [\[RFC5234\] appendix B.1](#) as:

```
VCHAR          = %x21-7E
```

"request-target" itself cannot contain 0x20 (SP) or any CTL characters, or any characters above the US-ASCII range (> 0x7F).

And the "HTTP-version" token is either the literal string "HTTP/1.0" or the literal string "HTTP/1.1", both of which are constrained to the same printable-ASCII range.

The ASCIIbetically-lowest shortest possible HTTP/1.0 or HTTP/1.1 request is:

```
char: !   SP /   SP H   T   T   P   /   1   .   0   CR LF CR LF
index: 0   1   2   3   4   5   6   7   8   9   0   a   b   c   d   e
```

In any case, no HTTP/1.0 or HTTP/1.1 request line can include any values lower than 0x0A (LF) or greater than 0x7F (DEL) in the first 15 octets.

However, [\[RFC7230\] section 3.1.1](#) also says:

In the interest of robustness, a server that is expecting to receive and parse a request-line SHOULD ignore at least one empty line (CRLF) received prior to the request-line.

So we should also consider accepting an arbitrary number of repeated CRLF sequences before the request-line as a potentially-valid HTTP client behavior.

[4.](#) Specific octets

The sections below examine likely values of specific octet positions in the stream. All octet indexes are 0-based.

[4.1.](#) octets 0 and 1

Any DNS message less than 3338 octets sent as the initial query over TCP can be reliably distinguished from any version of HTTP/1.x by the first two octets of the TCP stream alone.

3338 is 0x0D0A, or the ASCII string CRLF, which some HTTP/1.x clients might send before an initial request. No HTTP/1.x client can legitimately send anything lower than this.

Most DNS queries are easily within this range automatically.

[4.2.](#) octets 2 and 3

In a DNS stream, octets 2 and 3 represent the client-chosen message ID. The message ID is used to bind messages with responses. Over connectionless transports like UDP, this is an important anti-spoofing measure, as well as a distinguishing measure for clients reusing the same UDP port for multiple outstanding queries. Standard DNS clients already explicitly randomize this value.

For the connection-oriented streaming DNS discussed here, the anti-spoofing characteristics are not relevant (the connection itself provides anti-spoofing), so the client is free to choose arbitrary values.

With a standard DNS client which fully-randomizes these values, only 25% of generated queries will have the high bits of both octets set to 0. 100% of all HTTP/1.x requests will have the high bits of both of these octets cleared. Similarly, some small percentage of randomly-generated DNS queries will have values here lower than 0x0A,

while no HTTP/1.x clients will ever send these low values.

[4.3.](#) octet 4

In a DNS stream, octet 4 combines several fields:

```

  0  1  2  3  4  5  6  7
+--+--+--+--+--+--+--+
|QR|  Opcode  |AA|TC|RD|
+--+--+--+--+--+--+--+
```

In a standard DNS query sent over a streaming interface, QR, Opcode, AA, and TC are all set to 0. The least-significant bit (RD - Recursion Desired) is set when a packet is sent from a stub to a recursive resolver. The value of such an octet is 0x01. This value never occurs in octet 4 of a legitimate HTTP/1.x client.

But under DNS UPDATE ([\[RFC2136\]](#)), Opcode is set to 5 and all the option bits are cleared, which means this value would have 0x40 (ASCII '@'), which could legitimately occur in some HTTP/1.x requests at this position.

[4.4.](#) octet 5

In a DNS stream, octet 5 also combines several fields:

```

  0  1  2  3  4  5  6  7
+--+--+--+--+--+--+--+
|RA| Z|AD|CD|  RCODE  |
+--+--+--+--+--+--+--+
```

In some DNS messages sent from a client, all these bits are 0. However, [section 5.7 of \[RFC6840\]](#) suggests that queries may wish to set the AD bit to indicate a desire to learn from a validating resolver whether the resolver considers the contents to be Authentic Data.

[RFC6840] also suggests that:

validating resolvers SHOULD set the CD bit on every upstream query.

So many queries, particularly from DNSSEC-validating DNS clients, are likely to set bits 2 and 3, resulting in a value 0x30 (ASCII '0'). This is usually a legitimate value for octet 5 in an HTTP/1.x request.

[4.5.](#) octets 6 and 7

In DNS, octets 6 and 7 represent the query count. Most DNS clients will send one query at a time, which makes this value 0x0001. As long as the number of initial queries does not exceed 0x0A0A (2570), then at least one of these octets will have a value less than 0x0A. No HTTP/1.x client sends an octet less than 0x0A in positions 6 or 7.

In DNS UPDATE, octets 6 and 7 represent the zone count. Entries in the Zone section of the DNS UPDATE message are structured identically to entries in the Query section of a standard DNS message.

[4.6.](#) octets 8 through 11

In streaming DNS, octets 8 through 11 represent answer counts and authority counts in normal DNS queries, or Prerequisite and Update counts in DNS UPDATE. Standard DNS queries will set them both 0. DNS UPDATE queries are likely to include some records in these sections, so they won't be all zero, but as long as no more than 2570 Prerequisite records and no more than 2570 Update records are sent, at least one octet will have value less than 0x0A. But no HTTP/1.x client sends an octet less than 0x0A in these positions.

[4.7.](#) octets 12 and 13

In streaming DNS, octets 12 and 13 represent the number of Additional RRs. When a DNS query is sent with EDNS(0), the OPT RR is accounted for here. So this is often either 0x0000 or 0x0001. In a Secure DNS UPDATE [[RFC3007](#)], the SIG(0) or TSIG record is also found in this section, which could increase the values of these octets to 0x0002. No HTTP/1.x client will send octets with these low values at these positions.

[5.](#) Combinations of octets

In a DNS message, each Question in the Question section (or Zone in the Zone section for DNS UPDATE) is at least 5 octets (1 octet for zero-length QNAME + 2 octets for QTYPE + 2 octets for QCLASS), and each RR (in the Answer, Authority, and Additional sections for normal DNS queries; or in the Prerequisite, Update, and Additional sections for DNS UPDATE) is at least 11 octets. And the header itself is 12 octets.

So we know that for a valid DNS stream, the first message has a size of at least:

```
min_first_msg_size = 12 + 5 * (256*o[6] + o[7]) +  
                    11 * (256*(o[8] + o[10] + o[12]) +  
                        o[9] + o[11] + o[13])
```

It's possible to compare this value with the expected first query size:

```
first_msg_size = 256 * o[0] + o[1]
```

if "first_query_size" is less than "min_first_query_size" we can be confident that the stream is not DNS.

[5.1.](#) Proof: a valid DNS message cannot be an HTTP/1.x query

For any a valid, stream-based DNS message:

- o If there are fewer than 0x0A00 Questions then octet 6 < 0x0A.
- o If there are fewer than 0x0A00 Answer RRs, then octet 8 < 0x0A.
- o If there are fewer than 0x0A00 Authority RRs, then octet 10 < 0x0A.
- o If there are fewer than 0x0A00 Additional RRs, then octet 12 < 0x0A.

If any of these four inequalities hold, then the packet is clearly DNS, not HTTP/1.x.

if none of them hold, then there are at least $0x0A00$ (2560) Questions and $3 \times 2560 == 7680$ RRs. But:

$$12 + 5 \times 2560 + 11 \times 7680 == 97292$$

So the smallest possible DNS message where none of these four inequalities hold is 97292 octets. But a DNS message is limited in size to 65535 octets.

Therefore at least one of these inequalities holds, and one of the first 14 octets of a DNS stream is $< 0x0A$.

But in a standard HTTP/1.x request, none of the first 14 octets can have a value $< 0x0A$, so a valid DNS message cannot be mistaken for an HTTP/1.x request.

[6.](#) Guidance for Demultiplexing Servers

Upon receiving a connection stream that might be either DNS or HTTP/1.x, a server can inspect the initial octets of the stream to decide where to send it.

[6.1.](#) Without supporting HTTP/0.9

A server that doesn't care about HTTP/0.9 can simply wait for the first 14 octets of the client's request to come in. Then the algorithm is:

```
bytestream = read_from_client(14)
for x in bytestream:
    if (x < 0x0A) or (x > 0x7F):
        return `DNS`
return `HTTP`
```

[6.2.](#) Supporting archaic HTTP/0.9 clients

A server that decides to try to support HTTP/0.9 clients has a slightly more challenging task, since some of them may send fewer octets than the initial DNS message, and the server shouldn't block waiting for data that will never come.

```
bytestream = read_from_client(5)
for x in bytestream[0:5]:
    if (x < 0x0A) or (x > 0x7F):
        return `DNS`
if (bytestream[0:4] != 'GET '):    # not HTTP/0.9
    bytestream += read_from_client(9)
    for x in bytestream[5:14]:
        if (x < 0x0A) or (x > 0x7f):
            return `DNS`
    return `HTTP`
else:
    # maybe HTTP/0.9
```

```

seen_sp = False
seen_high = False
while (len(bytestream) < 14):
    if (seen_sp and seen_high):
        return `DNS`
    x = read_from_client(1)
    bytestream += x
    if (x > 0x7F):
        seen_high = True
    elif (x < 0x0A):
        return `DNS`
    elif (x == 0x20):
        seen_sp = True           # SP found before CRLF, not HTTP/0.9
    elif (x == 0x0A):
        return `HTTP`
return `HTTP`

```

Note that if `read_from_client()` ever fails to read the number of requested bytes (e.g. because of EOF), then the stream is neither valid HTTP nor valid DNS, and can be discarded.

[6.3.](#) Signaling demultiplexing capacity

This document assumes that clients can learn out-of-band which listening service they can connect to. For example, the administrator of a machine can configure a local forwarding stub resolver to use DNS-over-TLS on port 443 of some specific server. This explicit configuration carries with it some level of trust – the client is choosing to trust the configured server with its DNS queries.

In some circumstances, it might be useful for a listener to signal to a client that it is willing and capable of handling both DNS and HTTP/1.x traffic. While such signalling could be useful for dynamic discovery, it opens questions of trust (which servers should the client be willing to rely on for DNS resolution?) and is out-of-scope for this draft.

[7.](#) Guidance for DNS clients

Consider a DNS client that connects to a server that might be interested in answering HTTP/1.x requests on the same address/port

(or other channel identifier). The client wants to send traffic that is unambiguously DNS traffic to make it easy for the server to distinguish it from inbound HTTP/1.x requests. Fortunately, this is trivial to do. In fact, any sensibly-implemented DNS-over-TLS client can use this approach without modification, just by adjusting the port number of the upstream recursive resolver from 853 to 443.

Such a client should follow these guidelines:

- o Send the DNS message size (a 16-bit integer) together in the same packet with the full header of the first DNS message so that the recipient can review as much as possible of the frame at once. This is a best practice for efficient stream-based DNS anyway.

If the client is concerned about stream fragmentation that it cannot control, and it is talking to a server that might be expecting HTTP/0.9 clients, then the server might not be willing to wait for the full initial 14 octets to make a decision.

Note that this fragmentation is not a concern for streams wrapped in TLS when using modern AEAD ciphersuites. In this case, the client gets to choose the size of the plaintext record, which is either recovered by the server in full (unfragmented) or the connection fails.

If the client does not have such a guarantee from the transport, it MAY also take one of the following mitigating actions relating to the first DNS message it sends in the stream [explanation of what the server gets to see in the fragmented stream case are in square brackets after each mitigation]:

- o Ensure the first message is marked as a query (QR = 0), and it uses opcode 0 ("Standard Query"). [bytestream[4] < 0x08]
- o Ensure that the first message has RA = 0, Z = 0, and RCODE = 0. [bytestream[5] == 0x00]
- o Ensure that the high bit of the first octet of the message ID of the first message is set. [bytestream[2] > 0x7F]
- o Send an initial short Server Status DNS message ahead of the otherwise intended initial DNS message. [bytestream[0] == 0x00]

- o Use the EDNS(0) padding option [[RFC7830](#)] to pad the first message to a multiple of 256 octets. [bytestream[1] == 0x00]

[7.1.](#) Interpreting failure

FIXME: A DNS client that does not already know that a server is willing to carry both types of traffic SHOULD expect a transport connection failure of some sort. Can we say something specific about what it should expect?

[8.](#) Guidance for HTTP clients

HTTP clients SHOULD NOT send HTTP/0.9 requests, since modern HTTP servers are not required to support HTTP/0.9. Sending an HTTP/1.0 request (or any later version) is sufficient for a server to be able to distinguish the two protocols.

[9.](#) Security Considerations

FIXME: Clients should locally validate DNSSEC (servers may still be able to omit some records)

FIXME: if widely deployed, consider amplification for DDoS against authoritative servers?

FIXME: consider DNSSEC transparency

FIXME: consider TLS session resumption - this counts as a new stream boundary, so the multiplexing decision need not persist across resumption.

FIXME: consider 0-RTT

FIXME: consider X.509 cert validation

FIXME: what other security considerations should clients take?

FIXME: what other security considerations should servers take?

[10.](#) Privacy Considerations

FIXME: DNS queries and HTTP requests can reveal potentially sensitive information about the sender.

FIXME: consider DNS and HTTP traffic analysis - how should requests or responses be padded, aggregated, or delayed given that streams are multiplexed?

Internet-Draft Demultiplexing Streamed DNS from HTTP/1.x

May 2017

FIXME: any other privacy considerations?

11. IANA Considerations

This document does not ask IANA to make any changes to existing registries.

However, it does update the DNS and HTTP specifications, to reflect the fact that services using this demultiplexing technique may be constrained in adoption of future versions of either stream-based DNS or HTTP/1.x if those future versions modify either protocol in a way that breaks with the distinctions documented here.

In particular, this draft assumes that all future stream-based versions of HTTP/1.x should have the following properties:

- o the client will speak first
- o the client will send at least 14 octets before expecting a response from the server.
- o none of those first 14 octets will be below 0x0A (LF) or above 0x7F (DEL).

Future extensions to stream-based DNS or HTTP/1.x should take this demultiplexing technique into consideration.

12. Document Considerations

[RFC Editor: please remove this section before publication]

This document is currently edited as markdown. Minor editorial changes can be suggested via merge requests at <https://gitlab.com/dkg/hddemux> or by e-mail to the author. Please direct all significant commentary to the public IETF DNS Privacy mailing list: dns-privacy@ietf.org or to the IETF HTTP WG mailing list: ietf-http-wg@w3.org

13. References

13.1. Normative References

- [RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, [RFC 1035](#), DOI 10.17487/RFC1035, November 1987, <<http://www.rfc-editor.org/info/rfc1035>>.

Gillmor

Expires November 18, 2017

[Page 17]

Internet-Draft Demultiplexing Streamed DNS from HTTP/1.x

May 2017

- [RFC1945] Berners-Lee, T., Fielding, R., and H. Frystyk, "Hypertext Transfer Protocol -- HTTP/1.0", [RFC 1945](#), DOI 10.17487/RFC1945, May 1996, <<http://www.rfc-editor.org/info/rfc1945>>.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.
- [RFC2136] Vixie, P., Ed., Thomson, S., Rekhter, Y., and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", [RFC 2136](#), DOI 10.17487/RFC2136, April 1997, <<http://www.rfc-editor.org/info/rfc2136>>.
- [RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, [RFC 5234](#), DOI 10.17487/RFC5234, January 2008, <<http://www.rfc-editor.org/info/rfc5234>>.
- [RFC7230] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing", [RFC 7230](#), DOI 10.17487/RFC7230, June 2014, <<http://www.rfc-editor.org/info/rfc7230>>.

13.2. Informative References

- [HAPROXY] Tarreau, W., "The Proxy protocol", March 2017, <<https://www.haproxy.org/download/1.8/doc/proxy-protocol.txt>>.
- [I-D.hoffman-dns-over-https]
Hoffman, P. and P. McManus, "DNS Queries over HTTPS",

[draft-hoffman-dns-over-https-00](#) (work in progress), May 2017.

[I-D.ietf-dnsop-dns-wireformat-http]

Song, L., Vixie, P., Kerr, S., and R. Wan, "DNS wire-format over HTTP", [draft-ietf-dnsop-dns-wireformat-http-01](#) (work in progress), March 2017.

[RFC3007] Wellington, B., "Secure Domain Name System (DNS) Dynamic Update", [RFC 3007](#), DOI 10.17487/RFC3007, November 2000, <<http://www.rfc-editor.org/info/rfc3007>>.

Gillmor

Expires November 18, 2017

[Page 18]

Internet-Draft Demultiplexing Streamed DNS from HTTP/1.x

May 2017

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", [RFC 5246](#), DOI 10.17487/RFC5246, August 2008, <<http://www.rfc-editor.org/info/rfc5246>>.

[RFC6840] Weiler, S., Ed. and D. Blacka, Ed., "Clarifications and Implementation Notes for DNS Security (DNSSEC)", [RFC 6840](#), DOI 10.17487/RFC6840, February 2013, <<http://www.rfc-editor.org/info/rfc6840>>.

[RFC6895] Eastlake 3rd, D., "Domain Name System (DNS) IANA Considerations", [BCP 42](#), [RFC 6895](#), DOI 10.17487/RFC6895, April 2013, <<http://www.rfc-editor.org/info/rfc6895>>.

[RFC7301] Friedl, S., Popov, A., Langley, A., and E. Stephan, "Transport Layer Security (TLS) Application-Layer Protocol Negotiation Extension", [RFC 7301](#), DOI 10.17487/RFC7301, July 2014, <<http://www.rfc-editor.org/info/rfc7301>>.

[RFC7540] Belshé, M., Peon, R., and M. Thomson, Ed., "Hypertext Transfer Protocol Version 2 (HTTP/2)", [RFC 7540](#), DOI 10.17487/RFC7540, May 2015, <<http://www.rfc-editor.org/info/rfc7540>>.

[RFC7830] Mayrhofer, A., "The EDNS(0) Padding Option", [RFC 7830](#), DOI 10.17487/RFC7830, May 2016,

<<http://www.rfc-editor.org/info/rfc7830>>.

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D.,
and P. Hoffman, "Specification for DNS over Transport
Layer Security (TLS)", [RFC 7858](#), DOI 10.17487/RFC7858, May
2016, <<http://www.rfc-editor.org/info/rfc7858>>.

Author's Address

Daniel Kahn Gillmor
American Civil Liberties Union
125 Broad St.
New York, NY 10004
USA

Email: dkg@fifthhorseman.net