draft-dkg-dprive-demux-dns-http

Daniel Kahn Gillmor <dkg@fifthhorseman.net>
ACLU
AMERICAN CIVIL LIBERTIES UNION

DPRIVE
IETF 99

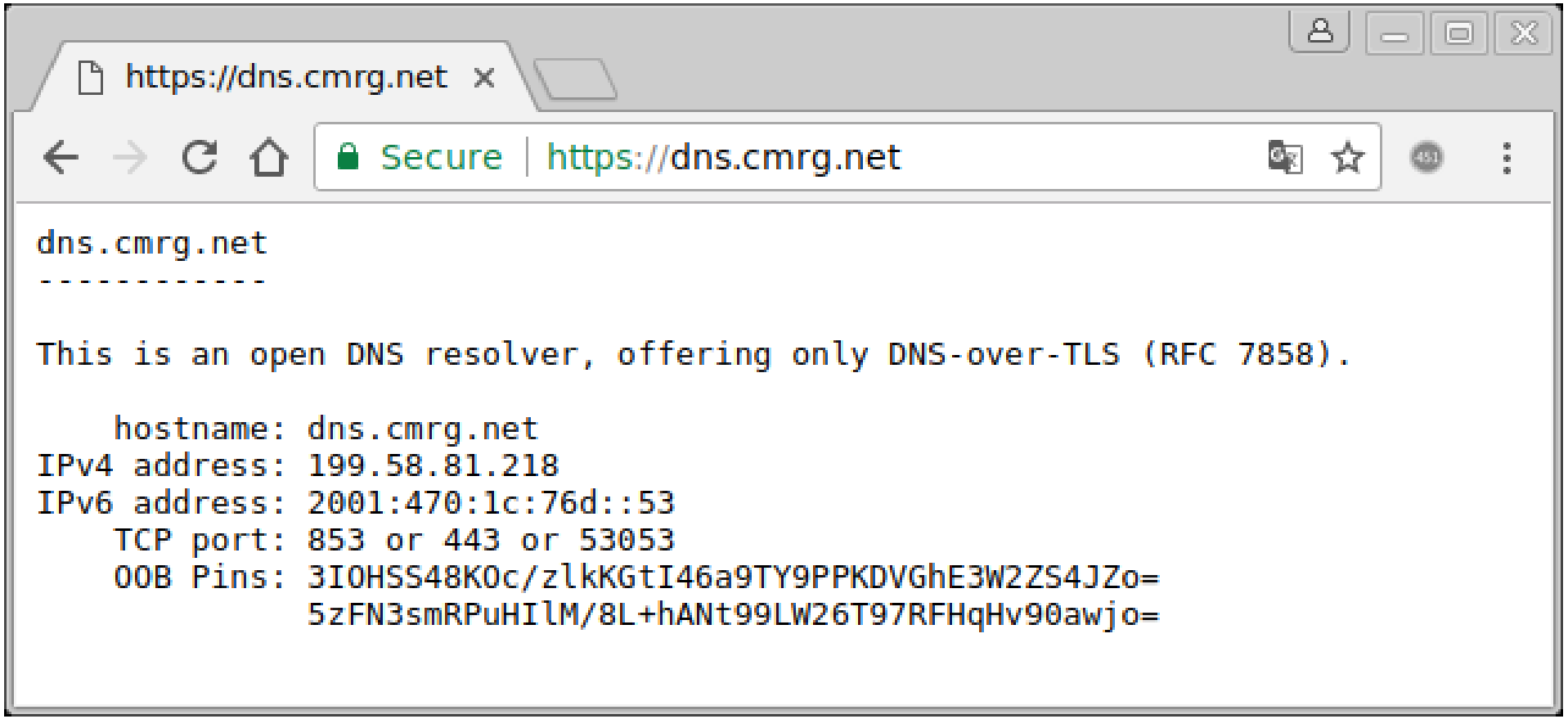
Tunneled TLS Protocols

Protocol	Inner Protocol	TCP port
HTTPS	HTTP	443
DNS-over-TLS	DNS(tcp)	853

WWTNAD?

Arms Race

- DNS-over-TLS defender: squat 443
- But users type the service name into their browsers

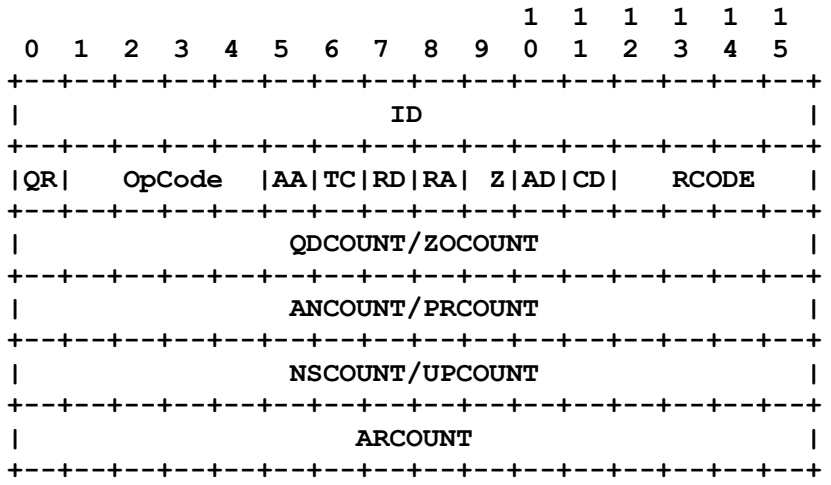


Why not both?

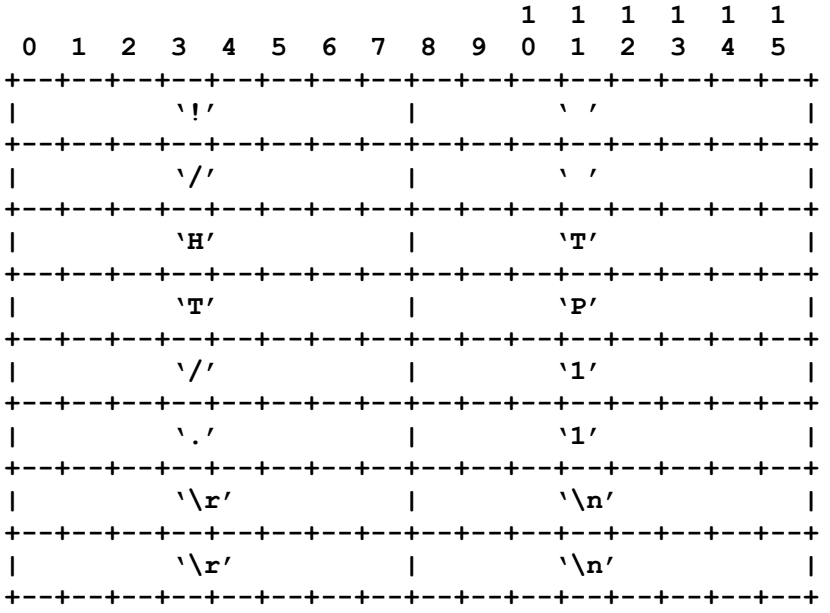
```
0 dkg@dirk:~$ dig @dns.cmrg.net#443 +tls +tls-ca +tls-hostname=dns.cmrg.net www.ietf.org
;; TLS session (TLS1.2)-(ECDHE-RSA-SECP256R1)-(AES-256-GCM)
;; ->>HEADER<<- opcode: QUERY; status: NOERROR; id: 29739
;; Flags: qr rd ra; QUERY: 1; ANSWER: 3; AUTHORITY: 0; ADDITIONAL: 1

;; EDNS PSEUDOSECTION:
;; Version: 0; flags: ; UDP size: 4096 B; ext-rcode: NOERROR

;; QUESTION SECTION:
;; www.ietf.org.                  IN      A

;; ANSWER SECTION:
www.ietf.org.           1269    IN      CNAME   www.ietf.org.cdn.cloudflare.net.
www.ietf.org.cdn.cloudflare.net. 69     IN      A       104.20.0.85
www.ietf.org.cdn.cloudflare.net. 69     IN      A       104.20.1.85

;; Received 149 B
;; Time 2017-07-17 18:46:01 EDT
;; From 199.58.81.218@443(TCP) in 42.0 ms
0 dkg@dirk:~$
```

The difference (inside TLS)

DNS



HTTP/1.1



DNS and HTTP/1.1 requests are disjoint

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

Implementation Status

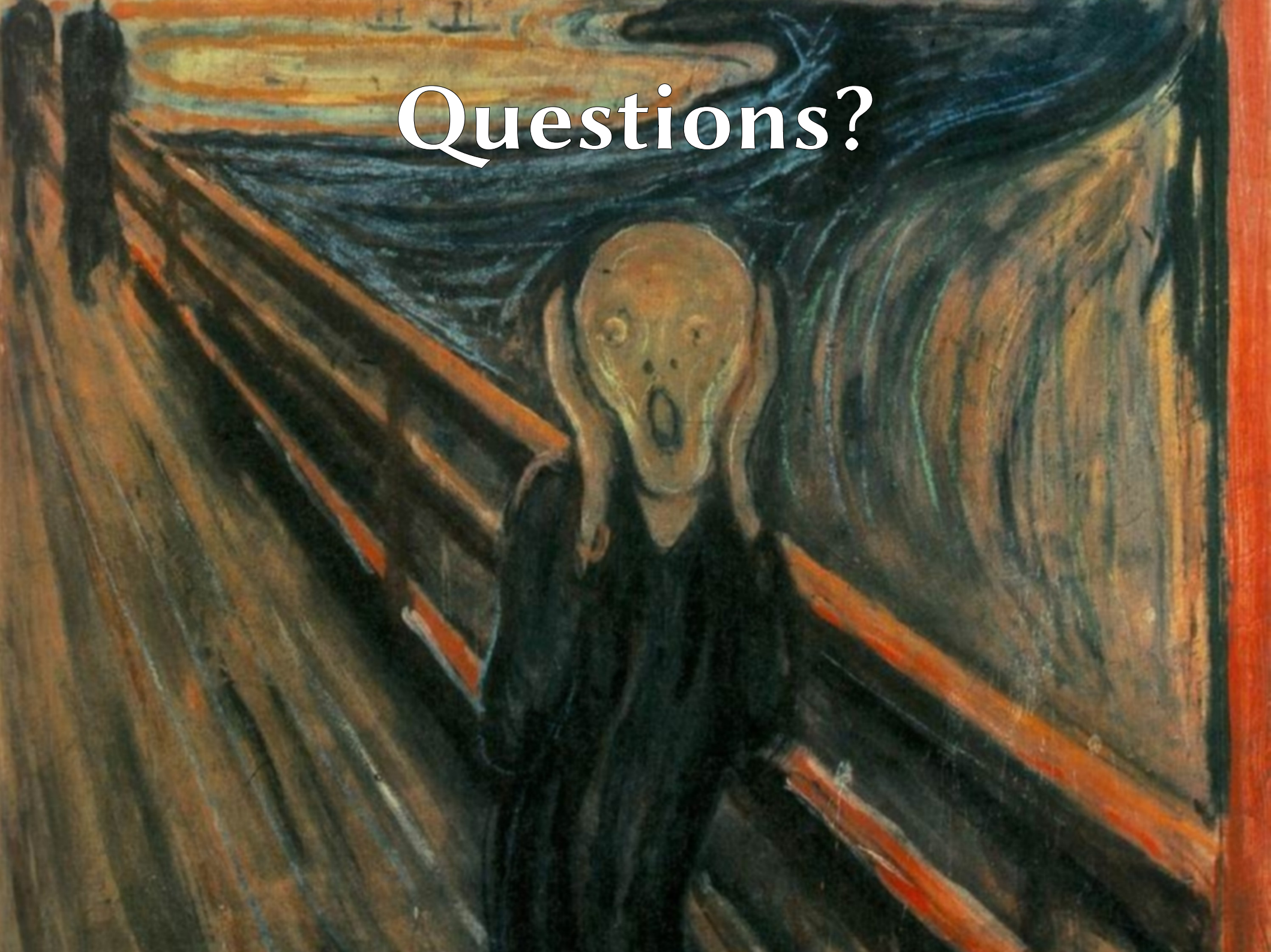
- https://gitlab.com/dkg/hddemux/
- In Debian testing
- Works fine with unmodified clients

  (DNS and HTTP/1.1)

Caveats

- Per-TLS connection
- HTTP/1.1 only (client-speaks-first)
- For multiplexing inside H2, see:

  `draft-hoffman-dns-over-http`
- Might constrain future development of stream-oriented DNS (and HTTP/1.1?)
- Combining with other multiplexing approaches unclear


Questions?