# DoT or DoH: Intro to DNS Privacy

Sheryl (Shane) Hermoso
Network Operations Engineer, APNIC

# DNS Privacy Risks

- “DNS is public data”

- **DNS requests** contain fields that are considered private
  - Source IP address
  - QNAME
  - (any personally identifiable information or PII)

- **DNS caches** in the servers
  - Query logs
  - “your recursive server knows a lot about you”

- The lack of privacy protection in DNS is actively exploited

# Privacy is an issue

“Pervasive Monitoring is an attack.” (RFC7258)

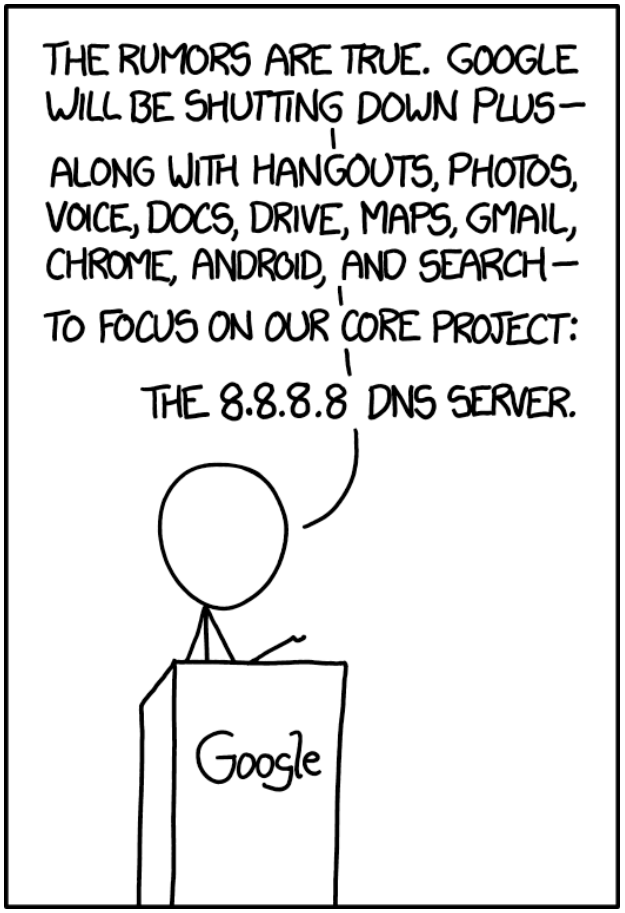
- widespread (and often covert) surveillance through intrusive gathering of protocol artefacts, including application content, or protocol metadata such as headers.

# DNS cloud providers

There has been a rise in DNS cloud providers

**Why do we use them?**

- Free and generally fast
- Avoid surveillance and blocking
- Don’t trust your ISP
- Focus on privacy



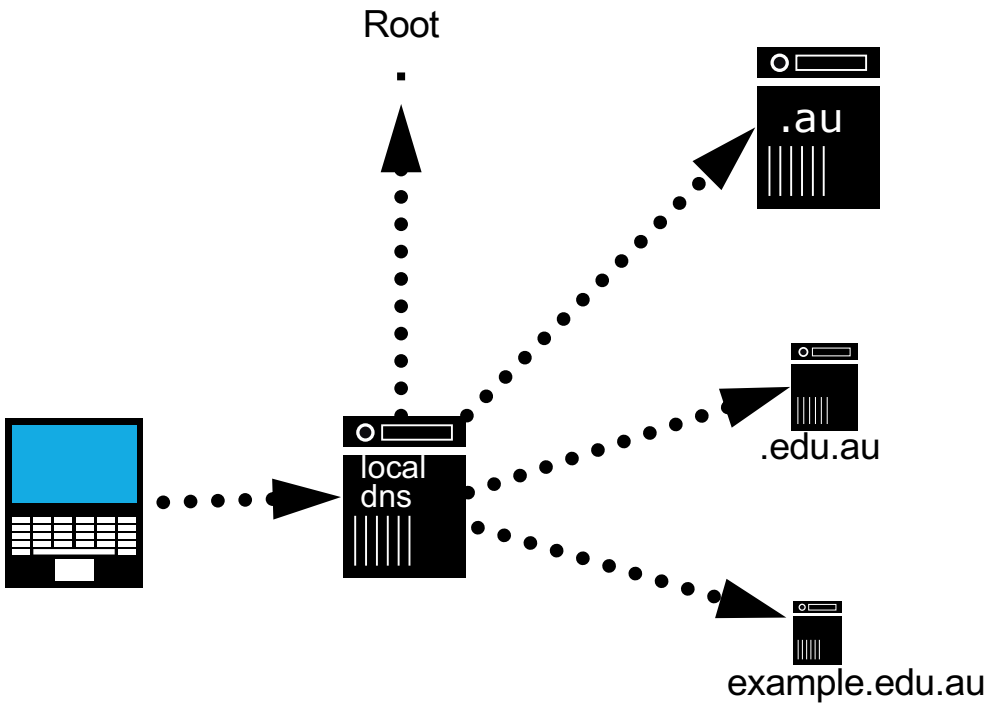
# Improving DNS Privacy

- DNS Privacy Considerations (RFC7626)

- Secure DNS transactions
  - Between stub resolver to recursive DNS server
  - Between recursive server to authoritative server

- Query Name Minimisation

- Encryption
  - DNS over TLS
  - DNS over DTLS
  - DNS over HTTPS



# DNS over TLS (DoT)

- RFC 7858
- Uses port 853
- DNS queries are sent over TLS-encrypted TCP connections
- Avoids spoofing, eavesdropping and DNS-based filters
- Two profiles (RFC8310)
  - Strict
    - Requires an encrypted and authenticated to a privacy-enabling DNS server and creates TLS connections
    - Failure to establish connection results to no service
  - Opportunistic
    - Desires privacy when possible
    - DNS server may be obtained by DHCP or an untrusted source

# Using Stubby DNS with DoT

- Stubby is a local DNS privacy stub resolver that
  - Runs as a daemon
  - Listens on loopback and sends out queries via TLS
  - Uses *Strict* privacy profile
- Simple setup

```
brew install stubby
vi /usr/local/etc/stubby/stubby.yml
/usr/local/sbin/stubby
```

```
# stubby.yml
# The getdnsapi.net server
  - address_data: 185.49.141.37
    tls_auth_name: "getdnsapi.net"
    tls_pubkey_pinset:
      - digest: "sha256"
        value:
foxZRnIh9gZpWnl+zEiKa0EJ2rdCGroMWm02
gaxSc9Q=
```

https://github.com/getdnsapi/stubby

# DoT Support - Servers

Servers

| Mode | | Load Balancer | Recursive | | | | | Auth | | |
|---|---|---|---|---|---|---|---|---|---|---|
| *Software* | | dnsdist | Unbound | BIND | Knot Res | CoreDNS[e] | Tenta[e] | NSD | BIND | Knot Auth |
| General | QNAME minimisation | n/a | ✓ | ✓ | ✓ | | | | | |
| *TCP/TLS Features* | TCP fast open[b] | ✓ | ✓ | ✓ | ✓ | | | | ✓ | ✓ |
| | Process Pipelined queries | ✓ | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✓ |
| | Provide OOOR | (g) | ✓ | ✓ | ✓ | | | n/a | n/a | n/a |
| | EDNS0 Keepalive[c] | | ✓ | ✓ | ✓ | | | | ✓ | |
| *TLS Features* | TLS encryption (Port 853) | ✓ | ✓ | (d) | ✓ | ✓ | ✓ | | | |
| | Provide TLS auth credentials | ✓ | ✓ | (d) | ✓ | ✓ | ✓ | | | |
| | EDNS0 Padding (basic) | | | ✓ | ✓ | | | | ✓ | |
| | TLS DNSSEC Chain Extension[h] | | | | | | | | | |

https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Implementation+Status

# DNS over HTTPS (DoH)

- RFC 8484
- DNS queries done securely over HTTPS
  - prevents on-path devices from interfering with DNS operations
  - allows web applications to access DNS information via existing browser APIs
- Client follows a URI template to construct the URL to use for resolution
  - Uses the "`application/dns-message`" type


https://tools.ietf.org/html/rfc8484

# DNS Query using JSON

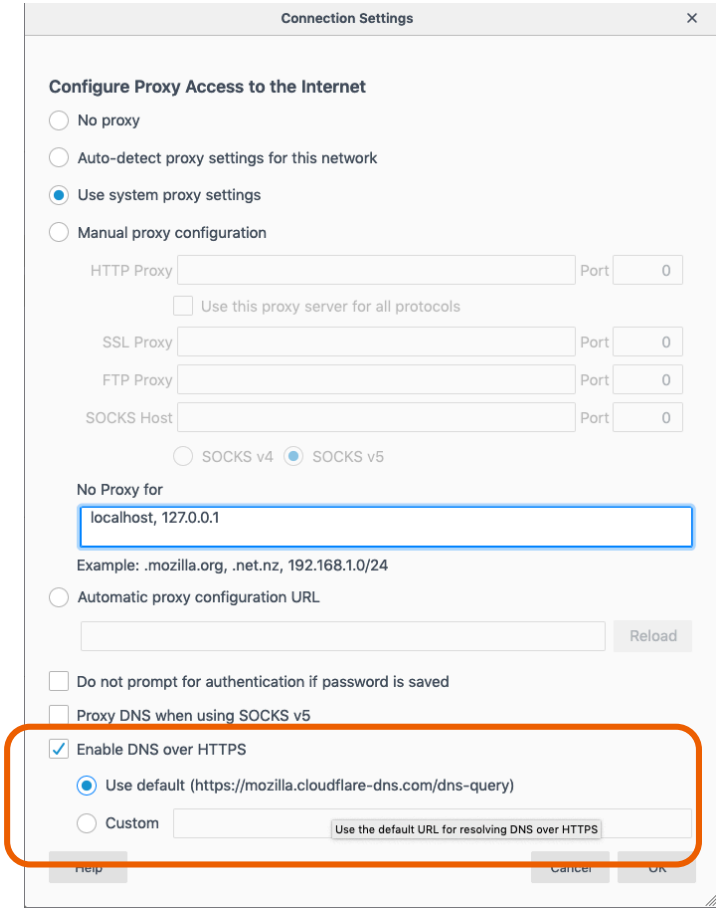
```
curl -s -H 'accept: application/dns+json' \
            'https://dns.google.com/resolve?name=www.apnic.net&type=A' | jq
{
 "Status": 0,
  "TC": false,
  "RD": true,
  "RA": true,
  "AD": true,
  "CD": false,
  "Question": [
    {
      "name": "www.apnic.net.",
      "type": 1
    }
  ],
……
```

# DNS Response using JSON

```
"Answer": [
    {
      "name": "www.apnic.net.",
      "type": 1,
      "TTL": 299,
      "data": "203.119.101.73"
    }
  ],
  "Comment": "Response from 202.12.31.53."
}
```

# DoH - Firefox (1/2)

- Preferences > Network Settings

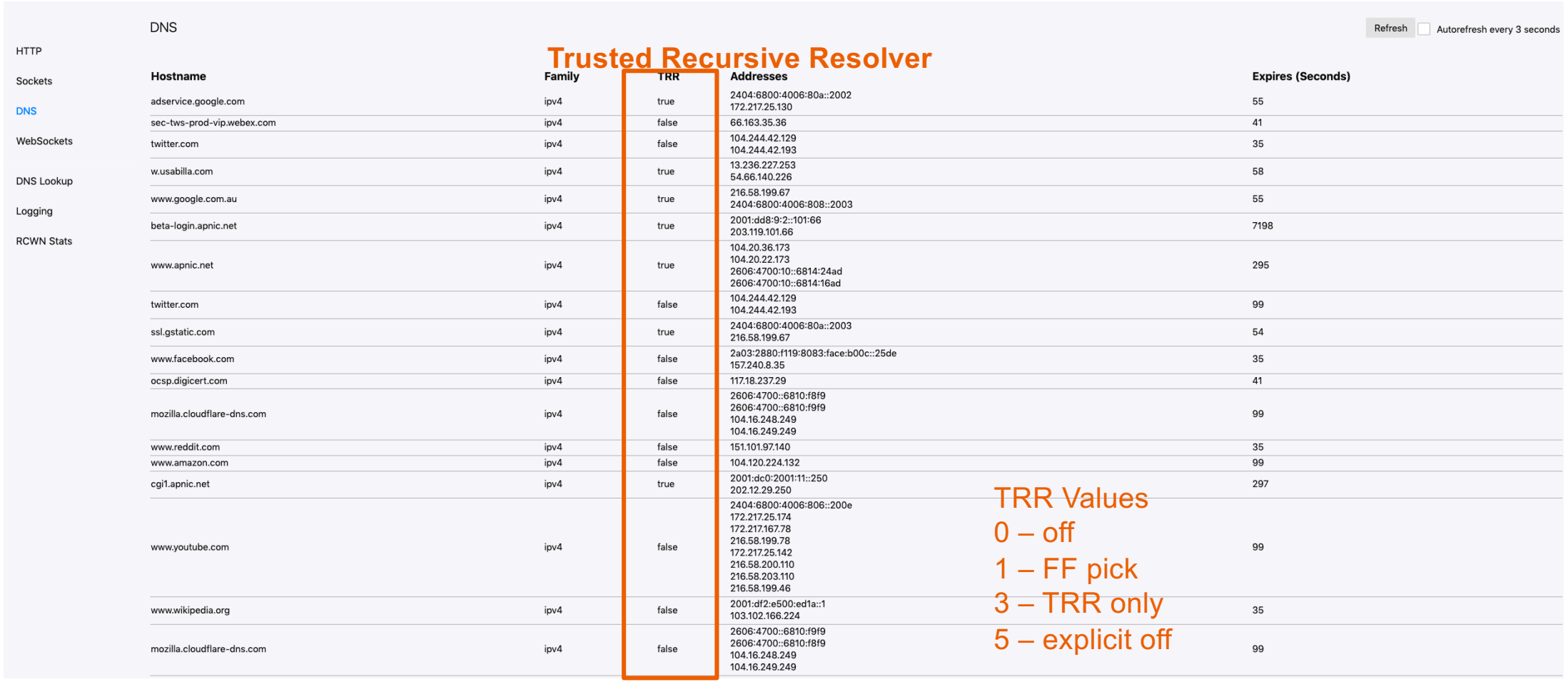



**about:config**

| Preference Name | Status | Type | Value |
|---|---|---|---|
| network.trr.allow-rfc1918 | default | boolean | false |
| network.trr.blacklist-duration | default | integer | 60 |
| network.trr.bootstrapAddress | default | string | |
| network.trr.confirmationNS | default | string | example.com |
| network.trr.credentials | default | string | |
| network.trr.custom_uri | default | string | |
| network.trr.disable-ECS | default | boolean | true |
| network.trr.early-AAAA | default | boolean | false |
| network.trr.max-fails | default | integer | 5 |
| network.trr.mode | default | integer | 0 |
| network.trr.request-timeout | default | integer | 1500 |
| network.trr.uri | default | string | https://mozilla.cloudflare-dns.com/dns-query |
| network.trr.useGET | default | boolean | false |
| network.trr.wait-for-portal | default | boolean | true |

# DoH - Firefox (2/2)

about:networking#dns



# DoH – Cloudflared

- simple setup

```
# Install on MAC
brew install cloudflare/cloudflare/cloudflared
cloudflared - version

# Run
sudo cloudflared proxy-dns
INFO[0000] Adding DNS upstream                           url="https://1.1.1.1/dns-query"
INFO[0000] Starting metrics server                       addr="127.0.0.1:51291"
INFO[0000] Adding DNS upstream                           url="https://1.0.0.1/dns-query"
INFO[0000] Starting DNS over HTTPS proxy server          addr="dns://localhost:53"
```

# dnscrypt-proxy

- Simple setup

```
cp example-dnscrypt-proxy.toml
dnscrypt-proxy.toml
./dnscrypt-proxy
```

```
[2019-06-24 06:01:47] [NOTICE] Source [public-resolvers.md] loaded
[2019-06-24 06:01:47] [NOTICE] dnscrypt-proxy 2.0.19
[2019-06-24 06:01:47] [NOTICE] Now listening to 127.0.0.1:53 [UDP]
[2019-06-24 06:01:47] [NOTICE] Now listening to 127.0.0.1:53 [TCP]
[2019-06-24 06:01:47] [NOTICE] Now listening to [::1]:53 [UDP]
[2019-06-24 06:01:47] [NOTICE] Now listening to [::1]:53 [TCP]
[2019-06-24 06:01:49] [NOTICE] [doh.appliedprivacy.net] OK (DoH) - rtt:
397ms
[2019-06-24 06:01:50] [NOTICE] [arvind-io] OK (crypto v2) - rtt: 407ms
[2019-06-24 06:01:50] [NOTICE] [bottlepost-dns-nl] OK (crypto v2) - rtt:
352ms
[2019-06-24 06:01:50] [NOTICE] [charis] OK (crypto v2) - rtt: 358ms
[2019-06-24 06:01:51] [NOTICE] [cloudflare] OK (DoH) - rtt: 59ms
[2019-06-24 06:01:51] [NOTICE] [cpunks-ru] OK (crypto v1) - rtt: 387ms
[2019-06-24 06:01:51] [NOTICE] [cs-ch] OK (crypto v2) - rtt: 408ms
[2019-06-24 06:01:52] [NOTICE] [cs-swe] OK (crypto v2) - rtt: 408ms
[2019-06-24 06:01:52] [NOTICE] [cs-nl] OK (crypto v2) - rtt: 408ms
[2019-06-24 06:01:53] [NOTICE] [cs-nl2] OK (crypto v2) - rtt: 408ms
[2019-06-24 06:01:53] [NOTICE] [cs-fi] OK (crypto v2) - rtt: 408ms
[2019-06-24 06:01:53] [NOTICE] [cs-pl] OK (crypto v2) - rtt: 408ms
[2019-06-24 06:01:54] [NOTICE] [cs-dk] OK (crypto v2) - rtt: 415ms
…
[2019-06-24 06:02:38] [NOTICE] [ventricle.us] OK (crypto v2) - rtt: 288ms
[2019-06-24 06:02:38] [NOTICE] [opennic-R4SAS] OK (crypto v2) - rtt: 385ms
[2019-06-24 06:02:38] [NOTICE] Server with the lowest initial latency:
quad9-dnscrypt-ip4-nofilter-alt (rtt: 53ms)
[2019-06-24 06:02:38] [NOTICE] dnscrypt-proxy is ready - live servers: 75
```


Ref: https://github.com/jedisct1/dnscrypt-proxy

# DoH Public Available Servers

https://github.com/curl/curl/wiki/DNS-over-HTTPS

| | | |
|---|---|---|
| Google | https://dns.google.com/experimental | |
| Cloudflare | https://cloudflare-dns.com/dns-query | Supports both -04 and -13 content-types |
| Quad9 | Recommended: https://dns.quad9.net/dns-query<br>Secured: https://dns9.quad9.net/dns-query<br>Unsecured: https://dns10.quad9.net/dns-query | Secured provides: Security blocklist, DNSSEC, no EDNS Client-Subnet<br>Unsecured provides: No security blocklist, no DNSSEC, no EDNS Client-Subnet<br>Recommend is currently identical to secure. |
| CleanBrowsing | https://doh.cleanbrowsing.org/doh/family-filter/ | anycast DoH server with parental control (restricts access to adult content + enforces safe search) |
| @chantra | https://dns.dnsoverhttps.net/dns-query | "toy server" which runs doh-proxy |
| @jedisct1 | https://doh.crypto.sx/dns-query | a server which runs another project called doh-proxy, written in Rust. |
| PowerDNS | https://doh.powerdns.org | Based on dnsdist-doh branch |

# Some issues

- DNS centralisation
  - cloud DNS providers have majority of the market share
- Privacy issues
  - Your DNS data will not be be subject to local privacy laws
- Debugging and protection
  - DoH can be used for data exfiltration
  - ISPs can’t localise DNS filters
  - Who handles troubleshooting?


Questions