Security Assignment 3: Internet Privacy

Chris Low

November 20, 2025

1 Methodology (unencrypted DNS)

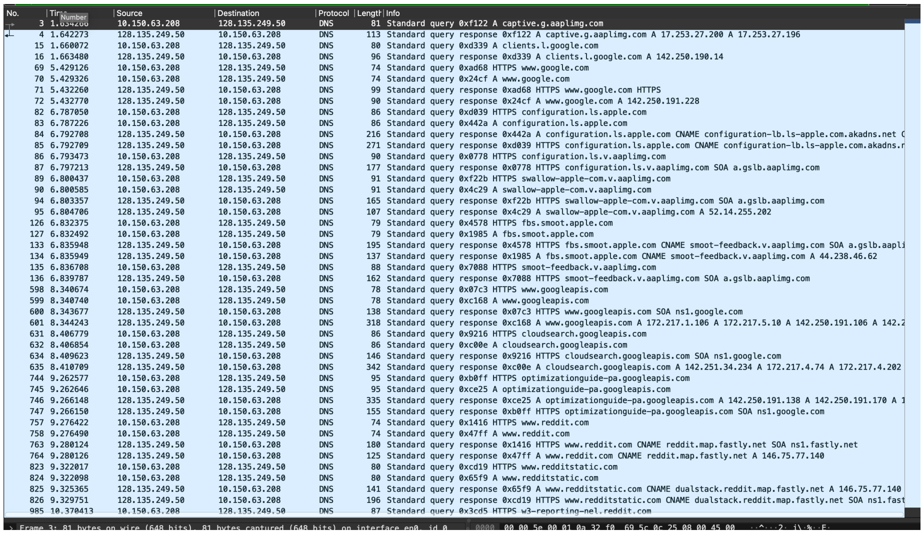
I ran this experiment on the UChicago WiFi network using a Mac laptop. Before visiting Reddit, I closed other browser tabs and cleared the cache in Chrome so that the page load would look as fresh as possible.

I then started Wireshark on the active interface and set a display filter of

```
dns
```

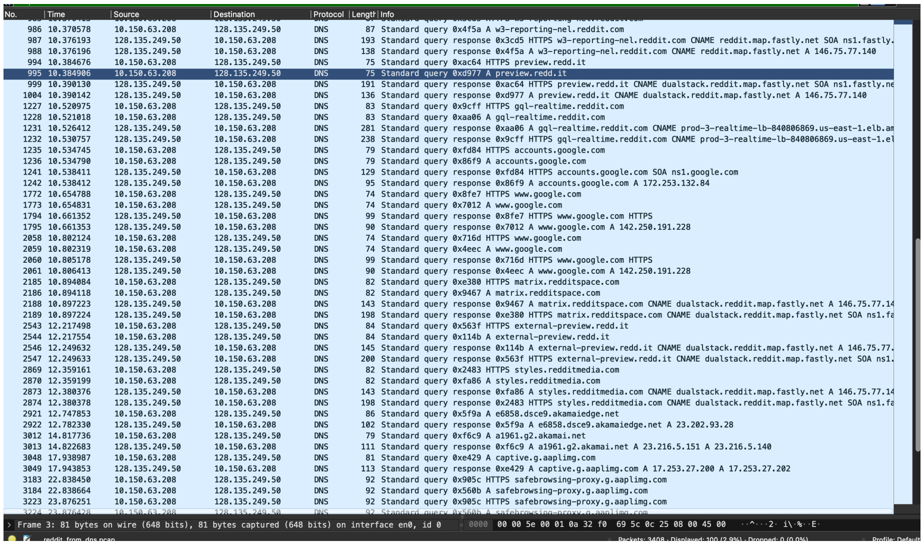
so only DNS packets would be shown. With the capture running, I typed `https://www.reddit.com` in the address bar and waited for the front page to finish loading. After the bursts of DNS traffic died down, I stopped the capture and saved it as a pcap file that contained only DNS packets.

In this trace the client IP is `10.150.63.208`, and the main DNS resolver is `128.135.249.50`, which belongs to UChicago. There are several dozen DNS queries and responses in total. Screenshots of the packet capture is shown below, but you can also find them in the file `reddit_from_dns.pcap`.



No.	Time	Source	Destination	Protocol	Length	Info
3	1.634266	10.150.63.208	128.135.249.50	DNS	81	Standard query 0xf122 A captive.g.aaplimg.com
4	1.642273	128.135.249.50	10.150.63.208	DNS	113	Standard query response 0xf122 A captive.g.aaplimg.com A 17.253.27.200 A 17.253.27.196
15	1.660072	10.150.63.208	128.135.249.50	DNS	80	Standard query 0xd339 A clients.l.google.com
16	1.663480	128.135.249.50	10.150.63.208	DNS	96	Standard query response 0xd339 A clients.l.google.com A 142.250.190.14
69	5.429126	10.150.63.208	128.135.249.50	DNS	74	Standard query 0xad68 HTTPS www.google.com
70	5.429326	10.150.63.208	128.135.249.50	DNS	74	Standard query 0x24cf A www.google.com
71	5.432260	128.135.249.50	10.150.63.208	DNS	99	Standard query response 0xad68 HTTPS www.google.com HTTPS
72	5.432770	128.135.249.50	10.150.63.208	DNS	90	Standard query response 0x24cf A www.google.com A 142.250.191.228
82	6.787050	10.150.63.208	128.135.249.50	DNS	86	Standard query 0xd039 HTTPS configuration.ls.apple.com
83	6.787226	10.150.63.208	128.135.249.50	DNS	86	Standard query 0x442a A configuration.ls.apple.com
84	6.792708	128.135.249.50	10.150.63.208	DNS	216	Standard query response 0x442a A configuration.ls.apple.com CNAME configuration-lb.ls-apple.com.akadns.net C
85	6.792709	128.135.249.50	10.150.63.208	DNS	271	Standard query response 0xd039 HTTPS configuration.ls.apple.com CNAME configuration-lb.ls-apple.com.akadns.r
86	6.793473	10.150.63.208	128.135.249.50	DNS	90	Standard query 0x0778 HTTPS configuration.ls.v.aaplimg.com
87	6.797213	128.135.249.50	10.150.63.208	DNS	177	Standard query response 0x0778 HTTPS configuration.ls.v.aaplimg.com SOA a.gslb.aaplimg.com
89	6.800437	10.150.63.208	128.135.249.50	DNS	91	Standard query 0xf22b HTTPS swallow-apple-com.v.aaplimg.com
90	6.800585	10.150.63.208	128.135.249.50	DNS	91	Standard query 0x4c29 A swallow-apple-com.v.aaplimg.com
94	6.803357	128.135.249.50	10.150.63.208	DNS	165	Standard query response 0xf22b HTTPS swallow-apple-com.v.aaplimg.com SOA a.gslb.aaplimg.com
95	6.804706	128.135.249.50	10.150.63.208	DNS	107	Standard query response 0x4c29 A swallow-apple-com.v.aaplimg.com A 52.14.255.202
126	6.832375	10.150.63.208	128.135.249.50	DNS	79	Standard query 0x4578 HTTPS fbs.smoot.apple.com
127	6.832492	10.150.63.208	128.135.249.50	DNS	79	Standard query 0x1985 A fbs.smoot.apple.com
133	6.835948	128.135.249.50	10.150.63.208	DNS	195	Standard query response 0x4578 HTTPS fbs.smoot.apple.com CNAME smoot-feedback.v.aaplimg.com SOA a.gslb.aapli
134	6.835949	128.135.249.50	10.150.63.208	DNS	137	Standard query response 0x1985 A fbs.smoot.apple.com CNAME smoot-feedback.v.aaplimg.com A 44.238.46.62
135	6.836708	10.150.63.208	128.135.249.50	DNS	88	Standard query 0x7088 HTTPS smoot-feedback.v.aaplimg.com
136	6.839787	128.135.249.50	10.150.63.208	DNS	162	Standard query response 0x7088 HTTPS smoot-feedback.v.aaplimg.com SOA a.gslb.aaplimg.com
598	8.340674	10.150.63.208	128.135.249.50	DNS	78	Standard query 0x07c3 HTTPS www.googleapis.com
599	8.340740	10.150.63.208	128.135.249.50	DNS	78	Standard query 0xc168 A www.googleapis.com
600	8.343677	128.135.249.50	10.150.63.208	DNS	138	Standard query response 0x07c3 HTTPS www.googleapis.com SOA ns1.google.com
601	8.344243	128.135.249.50	10.150.63.208	DNS	318	Standard query response 0xc168 A www.googleapis.com A 172.217.1.106 A 172.217.5.10 A 142.250.191.106 A 142.2
631	8.406779	10.150.63.208	128.135.249.50	DNS	86	Standard query 0x9216 HTTPS cloudsearch.googleapis.com
632	8.406854	10.150.63.208	128.135.249.50	DNS	86	Standard query 0xc00e A cloudsearch.googleapis.com
634	8.409623	128.135.249.50	10.150.63.208	DNS	146	Standard query response 0x9216 HTTPS cloudsearch.googleapis.com SOA ns1.google.com
635	8.410709	128.135.249.50	10.150.63.208	DNS	342	Standard query response 0xc00e A cloudsearch.googleapis.com A 142.251.34.234 A 172.217.4.74 A 172.217.4.202
744	9.262577	10.150.63.208	128.135.249.50	DNS	95	Standard query 0xb0ff HTTPS optimizationguide-pa.googleapis.com
745	9.262646	10.150.63.208	128.135.249.50	DNS	95	Standard query 0xce25 A optimizationguide-pa.googleapis.com
746	9.266148	128.135.249.50	10.150.63.208	DNS	335	Standard query response 0xce25 A optimizationguide-pa.googleapis.com A 142.250.191.138 A 142.250.191.170 A 1
747	9.266150	128.135.249.50	10.150.63.208	DNS	155	Standard query response 0xb0ff HTTPS optimizationguide-pa.googleapis.com SOA ns1.google.com
757	9.276422	10.150.63.208	128.135.249.50	DNS	74	Standard query 0x1416 HTTPS www.reddit.com
758	9.276490	10.150.63.208	128.135.249.50	DNS	74	Standard query 0x47ff A www.reddit.com
763	9.280124	128.135.249.50	10.150.63.208	DNS	180	Standard query response 0x1416 HTTPS www.reddit.com CNAME reddit.map.fastly.net SOA ns1.fastly.net
764	9.280126	128.135.249.50	10.150.63.208	DNS	125	Standard query response 0x47ff A www.reddit.com CNAME reddit.map.fastly.net A 146.75.77.140
823	9.322017	10.150.63.208	128.135.249.50	DNS	80	Standard query 0xcd19 HTTPS www.redditstatic.com
824	9.322098	10.150.63.208	128.135.249.50	DNS	80	Standard query 0x65f9 A www.redditstatic.com
825	9.325365	128.135.249.50	10.150.63.208	DNS	141	Standard query response 0x65f9 A www.redditstatic.com CNAME dualstack.reddit.map.fastly.net A 146.75.77.140
826	9.329751	128.135.249.50	10.150.63.208	DNS	196	Standard query response 0xcd19 HTTPS www.redditstatic.com CNAME dualstack.reddit.map.fastly.net SOA ns1.fast
985	10.370413	10.150.63.208	128.135.249.50	DNS	87	Standard query 0x3cd5 HTTPS w3-reporting-nel.reddit.com

```
> Frame 3: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface en0, id 0
0000  00 00 5e 00 01 0a 32 f0  69 5c 0c 25 08 00 45 00   ··^···2· i\·%··E·
```



```
No.   Time       Source          Destination     Protocol Length Info
  986 10.370578  10.150.63.208   128.135.249.50  DNS       87 Standard query 0x4f5a A w3-reporting-nel.reddit.com
  987 10.376193  128.135.249.50  10.150.63.208   DNS      193 Standard query response 0x3cd5 HTTPS w3-reporting-nel.reddit.com CNAME reddit.map.fastly.net SOA ns1.fastly.
  988 10.376196  128.135.249.50  10.150.63.208   DNS      138 Standard query response 0x4f5a A w3-reporting-nel.reddit.com CNAME reddit.map.fastly.net A 146.75.77.140
  994 10.384676  10.150.63.208   128.135.249.50  DNS       75 Standard query 0xac64 HTTPS preview.redd.it
  995 10.384906  10.150.63.208   128.135.249.50  DNS       75 Standard query 0xd977 A preview.redd.it
  999 10.390130  128.135.249.50  10.150.63.208   DNS      191 Standard query response 0xac64 HTTPS preview.redd.it CNAME dualstack.reddit.map.fastly.net SOA ns1.fastly.ne
 1004 10.390142  128.135.249.50  10.150.63.208   DNS      136 Standard query response 0xd977 A preview.redd.it CNAME dualstack.reddit.map.fastly.net A 146.75.77.140
 1227 10.520975  10.150.63.208   128.135.249.50  DNS       83 Standard query 0x9cff HTTPS gql-realtime.reddit.com
 1228 10.521018  10.150.63.208   128.135.249.50  DNS       83 Standard query 0xaa06 A gql-realtime.reddit.com
 1231 10.526412  128.135.249.50  10.150.63.208   DNS      281 Standard query response 0xaa06 A gql-realtime.reddit.com CNAME prod-3-realtime-lb-840806869.us-east-1.elb.am
 1232 10.530757  128.135.249.50  10.150.63.208   DNS      238 Standard query response 0x9cff HTTPS gql-realtime.reddit.com CNAME prod-3-realtime-lb-840806869.us-east-1.el
 1235 10.534745  10.150.63.208   128.135.249.50  DNS       79 Standard query 0xfd84 HTTPS accounts.google.com
 1236 10.534790  10.150.63.208   128.135.249.50  DNS       79 Standard query 0x86f9 A accounts.google.com
 1241 10.538411  128.135.249.50  10.150.63.208   DNS      129 Standard query response 0xfd84 HTTPS accounts.google.com SOA ns1.google.com
 1242 10.538412  128.135.249.50  10.150.63.208   DNS       95 Standard query response 0x86f9 A accounts.google.com A 172.253.132.84
 1772 10.654788  10.150.63.208   128.135.249.50  DNS       74 Standard query 0x8fe7 HTTPS www.google.com
 1773 10.654831  10.150.63.208   128.135.249.50  DNS       74 Standard query 0x7012 A www.google.com
 1794 10.661352  128.135.249.50  10.150.63.208   DNS       99 Standard query response 0x8fe7 HTTPS www.google.com HTTPS
 1795 10.661353  128.135.249.50  10.150.63.208   DNS       90 Standard query response 0x7012 A www.google.com A 142.250.191.228
 2058 10.802124  10.150.63.208   128.135.249.50  DNS       74 Standard query 0x716d HTTPS www.google.com
 2059 10.802319  10.150.63.208   128.135.249.50  DNS       74 Standard query 0x4eec A www.google.com
 2060 10.805178  128.135.249.50  10.150.63.208   DNS       99 Standard query response 0x716d HTTPS www.google.com HTTPS
 2061 10.806413  128.135.249.50  10.150.63.208   DNS       90 Standard query response 0x4eec A www.google.com A 142.250.191.228
 2185 10.894084  10.150.63.208   128.135.249.50  DNS       82 Standard query 0xe380 HTTPS matrix.redditspace.com
 2186 10.894118  10.150.63.208   128.135.249.50  DNS       82 Standard query 0x9467 A matrix.redditspace.com
 2188 10.897223  128.135.249.50  10.150.63.208   DNS      143 Standard query response 0x9467 A matrix.redditspace.com CNAME dualstack.reddit.map.fastly.net A 146.75.77.14
 2189 10.897224  128.135.249.50  10.150.63.208   DNS      198 Standard query response 0xe380 HTTPS matrix.redditspace.com CNAME dualstack.reddit.map.fastly.net SOA ns1.fa
 2543 12.217498  10.150.63.208   128.135.249.50  DNS       84 Standard query 0x563f HTTPS external-preview.redd.it
 2544 12.217554  10.150.63.208   128.135.249.50  DNS       84 Standard query 0x114b A external-preview.redd.it
 2546 12.249632  128.135.249.50  10.150.63.208   DNS      145 Standard query response 0x114b A external-preview.redd.it CNAME dualstack.reddit.map.fastly.net A 146.75.77.
 2547 12.249633  128.135.249.50  10.150.63.208   DNS      200 Standard query response 0x563f HTTPS external-preview.redd.it CNAME dualstack.reddit.map.fastly.net SOA ns1.
 2869 12.359161  10.150.63.208   128.135.249.50  DNS       82 Standard query 0x2483 HTTPS styles.redditmedia.com
 2870 12.359199  10.150.63.208   128.135.249.50  DNS       82 Standard query 0xfa86 A styles.redditmedia.com
 2873 12.380376  128.135.249.50  10.150.63.208   DNS      143 Standard query response 0xfa86 A styles.redditmedia.com CNAME dualstack.reddit.map.fastly.net A 146.75.77.14
 2874 12.380378  128.135.249.50  10.150.63.208   DNS      198 Standard query response 0x2483 HTTPS styles.redditmedia.com CNAME dualstack.reddit.map.fastly.net SOA ns1.fa
 2921 12.747853  10.150.63.208   128.135.249.50  DNS       86 Standard query 0x5f9a A e6858.dsce9.akamaiedge.net
 2922 12.782330  128.135.249.50  10.150.63.208   DNS      102 Standard query response 0x5f9a A e6858.dsce9.akamaiedge.net A 23.202.93.28
 3012 14.817736  10.150.63.208   128.135.249.50  DNS       79 Standard query 0xf6c9 A a1961.g2.akamai.net
 3013 14.822683  128.135.249.50  10.150.63.208   DNS      111 Standard query response 0xf6c9 A a1961.g2.akamai.net A 23.216.5.151 A 23.216.5.140
 3048 17.938987  10.150.63.208   128.135.249.50  DNS       81 Standard query 0xe429 A captive.g.aaplimg.com
 3049 17.943853  128.135.249.50  10.150.63.208   DNS      113 Standard query response 0xe429 A captive.g.aaplimg.com A 17.253.27.200 A 17.253.27.202
 3183 22.838450  10.150.63.208   128.135.249.50  DNS       92 Standard query 0x905c HTTPS safebrowsing-proxy.g.aaplimg.com
 3184 22.838664  10.150.63.208   128.135.249.50  DNS       92 Standard query 0x560b A safebrowsing-proxy.g.aaplimg.com
 3223 23.876251  10.150.63.208   128.135.249.50  DNS       92 Standard query 0x905c HTTPS safebrowsing-proxy.g.aaplimg.com
 3224 23.876428  10.150.63.208   128.135.249.50  DNS       92 Standard query 0x560b A safebrowsing-proxy.g.aaplimg.com
> Frame 3: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface en0, id 0   0000  00 00 5e 00 01 0a 32 f0  69 5c 0c 25 08 00 45 00   ··^···2· i\·%··E·
reddit_from_dns.pcap                              Packets: 3408 · Displayed: 100 (2.9%) · Dropped: 0 (0.0%)      Profile: Default
```

2 Who can see that I visited Reddit from unencrypted DNS

Because these DNS packets are unencrypted, several parties can see the domain names in clear text.

Campus DNS resolver and local network

All DNS queries in the trace go from `10.150.63.208` (my machine) to `128.135.249.50`. This means the UChicago recursive DNS resolver sees every domain that I look up. The resolver can easily tell that I visited Reddit from queries such as:

- `www.reddit.com`
- `www.redditstatic.com`
- `i.redd.it`
- `preview.redd.it`
- `styles.redditmedia.com`
- `matrix.redditspace.com`
- `w3-reporting-nel.reddit.com` and `w3-reporting-csp.reddit.com`

Any administrator who operates this resolver, or who can monitor the UChicago internal network, can link those names to my client IP and to the time of the visit.

If the campus resolver forwards queries to an upstream ISP or another provider, that upstream resolver would also see the same domain names and could draw the same conclusion.

Authoritative DNS and hosting providers

Authoritative DNS servers for Reddit and for its infrastructure providers also see some information. For example, the trace includes queries for Akamai domains such as

- `a1961.g2.akamai.net`
- `e6858.dsce9.akamaiedge.net`

These belong to Akamai, which provides Reddit with static assets and media upon some Google search. The authoritative name servers for these domains receive the DNS queries and can see that a UChicago address is trying to reach hosts that serve Reddit content.

Unlike the campus resolver, they do not see the full set of sites I visit, but they do see that I am contacting infrastructure that belongs to Reddit.

3 Other entities that know I visited Reddit

Even if we ignore the DNS layer, other parties learn about my visit as part of normal web operation. I grouped the domains in the trace by company, based on the hostnames visible in the DNS packets.

Reddit

Reddit related domains in the capture include:

- `www.reddit.com` (main site)
- `i.redd.it`, `preview.redd.it` (images and link previews)
- `www.redditstatic.com`, `styles.redditmedia.com` (static assets and styles)
- `gql-realtime.reddit.com`, `matrix.redditspace.com`
- `w3-reporting-nel.reddit.com`, `w3-reporting-csp.reddit.com` (reporting endpoints)

Once the DNS lookup succeeds, my browser opens HTTPS connections to these hosts. Reddit therefore knows that someone at a UChicago address visited the front page, which APIs were used, and which images and scripts were loaded. If I had been logged in, Reddit could tie this to my account.

Google

Several Google owned domains appear in the trace:

- safebrowsing.googleapis.com
- www.google.com and accounts.google.com
- encrypted-tbn0.gstatic.com
- optimizationguide-pa.googleapis.com
- clients4.google.com and other googleapis.com hostnames

Chrome uses Google Safe Browsing to check URLs against a phishing and malware list, so contacting safebrowsing.googleapis.com tells Google that the browser is checking a new site. Some of the other googleapis.com and gstatic.com hostnames serve fonts, static files or browser services. If Reddit embeds any Google services or if Chrome talks to Google while the page loads, Google can infer that the browser just loaded Reddit, even though the page itself is hosted elsewhere.

Apple

The trace includes several Apple hostnames, for example:

- captive.g.aaplimg.com
- configuration.ls.apple.com
- swallow-apple.com, fbs.smoot.apple.com, smoot-feedback.v.aaplimg.com
- safebrowsing-proxy.g.aaplimg.com

These are not caused directly by Reddit. They come from macOS itself. For instance, captive.g.aaplimg.com is used to detect captive portals and to check internet connectivity. Apple therefore learns that this Mac is online and periodically making these checks. When combined with timing and other signals, Apple could correlate this with general browsing activity.

Akamai and other CDNs

As mentioned above, Akamai appears through domains such as a1961.g2.akamai.net and e6858.dsce9.akamaiedge.net. These hosts serve static assets for Reddit. When my browser loads images, style sheets or JavaScript from Akamai, Akamai sees my IP address, the Reddit related hostnames, and the time of access. Even if they do not see DNS for www.reddit.com itself, they can still see that they are serving Reddit content to a client at UChicago.

Slack and other background services

There are DNS queries for `slack.com` as well. These are almost certainly from the Slack desktop app running in the background, not from Reddit itself. They still show up in the capture because Wireshark is recording all DNS traffic on the interface. This illustrates that a DNS trace taken on a real machine often contains noise from other applications.

4 Privacy concerns by company

The privacy risks are different for each of these parties.

UChicago DNS and any upstream ISP

The campus resolver at `128.135.249.50` sees every domain that my machine looks up, in clear text, along with timestamps and my client IP. Over time this data can reveal a very detailed picture of my browsing habits and daily routine. Policies at a university are usually more benign than at a commercial ISP, but technically the capability is the same. Logs could be kept for troubleshooting, but they could also be used for monitoring or handed over if requested.

Reddit

Reddit needs to know which pages I visit, otherwise it cannot serve the site. Still, Reddit can log all of my page views, the subreddits I look at, my interactions, and my approximate location from IP. If I am logged in, this history can be tied to my account and used for recommendations, content ranking or targeted advertising. If the logs are ever breached or shared, this could reveal a lot about my interests.

Google

Because Chrome and some page components talk to Google services during the visit, Google can often infer that I am on Reddit, even though I am not on a Google website. Google already has search history, YouTube watch history and other signals. Adding another source of browsing data lets Google build a more complete profile that can be used for ads or other personalization. The concern here is cross site tracking and the concentration of data in one company.

Akamai and other CDNs

Akamai mainly sees requests for static resources. On its own, this is less sensitive than full page content, but Akamai serves a very large fraction of the web. If it wanted to, it could correlate traffic from the same IP across different customer sites and learn which large services someone uses. Even if the company does not do this in practice, the potential is there because unencrypted DNS and hostnames in HTTPS requests leak quite a bit of information.

Apple

Apple learns that the device is online and that it is contacting Apple network check and feedback services. This is not specific to Reddit, but it adds to the general telemetry Apple has about the device. The concern is less about this one site, and more about the accumulation of many small signals from different services on the system.

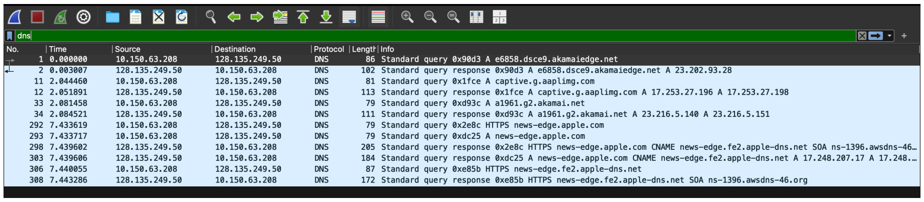
Other background services

Queries from Slack and similar apps are a reminder that DNS captures reflect the whole device, not just one browser tab. Any service that runs in the background can add entries to the trace and can also be logged by the DNS resolver. This widens the amount of information that a network operator or DNS provider can collect about a user.

Overall, the unencrypted DNS trace for a single visit to `reddit.com` exposes not only that I visited Reddit, but also which third party services and infrastructure providers were involved, and which other applications on my machine were active at the same time.

Part 2: Encrypted DNS Results

After switching Chrome to use Cloudflare (1.1.1.1) for secure DNS, the DNS traffic in Wireshark changed sharply. In the unencrypted trace, there were many DNS packets for Reddit domains and for several third party services. In contrast, the encrypted DNS trace contained almost no DNS queries from the browser. The only DNS packets that appeared were from macOS background services, such as Apple network checks, and a small number of CDN related lookups. No Reddit related domain names appeared in the capture, as shown:



dns

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.150.63.208	128.135.249.50	DNS	86	Standard query 0x90d3 A e6858.dsce9.akamaiedge.net
2	0.003007	128.135.249.50	10.150.63.208	DNS	102	Standard query response 0x90d3 A e6858.dsce9.akamaiedge.net A 23.202.93.28
11	2.044460	10.150.63.208	128.135.249.50	DNS	81	Standard query 0x1fce A captive.g.aaplimg.com
12	2.051891	128.135.249.50	10.150.63.208	DNS	113	Standard query response 0x1fce A captive.g.aaplimg.com A 17.253.27.196 A 17.253.27.198
33	2.081458	10.150.63.208	128.135.249.50	DNS	79	Standard query 0xd93c A a1961.g2.akamai.net
34	2.084521	128.135.249.50	10.150.63.208	DNS	111	Standard query response 0xd93c A a1961.g2.akamai.net A 23.216.5.140 A 23.216.5.151
292	7.433619	10.150.63.208	128.135.249.50	DNS	79	Standard query 0x2e8c HTTPS news-edge.apple.com
293	7.433717	10.150.63.208	128.135.249.50	DNS	79	Standard query 0xdc25 A news-edge.apple.com
298	7.439602	128.135.249.50	10.150.63.208	DNS	205	Standard query response 0x2e8c HTTPS news-edge.apple.com CNAME news-edge.fe2.apple-dns.net SOA ns-1396.awsdns-46…
303	7.439606	128.135.249.50	10.150.63.208	DNS	184	Standard query response 0xdc25 A news-edge.apple.com CNAME news-edge.fe2.apple-dns.net A 17.248.207.17 A 17.248.…
306	7.440055	10.150.63.208	128.135.249.50	DNS	87	Standard query 0xe85b HTTPS news-edge.fe2.apple-dns.net
308	7.443286	128.135.249.50	10.150.63.208	DNS	172	Standard query response 0xe85b HTTPS news-edge.fe2.apple-dns.net SOA ns-1396.awsdns-46.org

Who can still see that I visited Reddit

Encrypted DNS removes visibility from the campus network and anyone else watching local DNS traffic. UChicago's resolver no longer receives my DNS queries, and the domain names are no longer exposed on the wire.

The new party that gains visibility is Cloudflare, since Chrome now sends its DNS lookups directly to Cloudflare over an encrypted connection. Cloudflare can see every domain the browser resolves, including all of the Reddit related names that were visible to UChicago in the first trace.

Other types of entities still see my activity even with encrypted DNS. **Reddit** sees the visit through my HTTPS connections to its servers. Its **CDNs, such as Akamai or Fastly,** still see requests for images, scripts, and other static files. These connections reveal that I am loading Reddit content even though the DNS lookups do not appear in Wireshark.

Privacy tradeoffs

Encrypted DNS shifts who can observe my browsing. It prevents the campus network, local administrators, and passive observers on the WiFi from reading my DNS queries. This removes one of the easiest ways to monitor which sites I visit.

However, it does not hide my activity from every party. **The DNS resolver I choose, in this case Cloudflare, now receives all of my browser's DNS traffic.** Cloudflare can build the same type of browsing profile that UChicago could build in the unencrypted case, although Cloudflare may have different policies about logging and retention.

Encrypted DNS also does not hide information from the sites I connect to. Reddit still sees my HTTPS requests. Its CDNs still see that my browser is fetching Reddit assets. These services can infer that I am visiting Reddit from the hostnames inside the encrypted HTTPS requests.

In summary, encrypted DNS protects my traffic from local observers but moves trust to the DNS provider and does not prevent the destination sites or their CDNs from seeing that I visited them.