Dinos Stamou
Evaggelos Balaskas
Nikos Roussos

Encrypted Neutral DNS

Dinos Stamou
Operations / IT Security Engineer
@dinosrc

Evaggelos Balaskas
Cloud Platform Operations
@ebalaskas

Nikos Roussos
Technical Lead
@comzeradd

DNS: the problem

- Hierarchical (eg. .org TLD)
- Clear text UDP (Sniffing, Hijacking, Poisoning, MITM)
- Heavily centralized by ISPs (eg. CPEs)
- Vulnerable to State censorship

Let’s get Legal

- Νόμος 2121/1993 και 4481/2017
  - Προβλέπει το μπλοκάρισμα ιστοσελίδων από τους ISPs
  - Ολιγομελής (3 άτομα) επιτροπή με απόλυτη εξουσία
  - Επιτροπή για τη Διαδικτυακή Προσβολή Δικαιωμάτων Πνευματικής Ιδιοκτησίας και Συγγενικών Δικαιωμάτων (ΕΔΠΠΙ)
- ISPs: DNS blocking/hijacking

ΑΡΙΘΜΟΣ ΑΠΟΦΑΣΗΣ 3/2018

Η Επιτροπή για τη Διαδικτυακή Προσβολή της Πνευματικής Ιδιοκτησίας συνεδρίασε μυστικά την

Censorship

- Κανονισμός 2015/2120
  - Net Neutrality

3) Οι πάροχοι υπηρεσιών πρόσβασης στο διαδίκτυο δεν εφαρμόζουν μέτρα διαχείρισης της κίνησης που υπερβαίνουν αυτά που ορίζονται στο δεύτερο εδάφιο και, κυρίως, **δεν παρεμποδίζουν**, **επιβραδύνουν**, **αλλοιώνουν, περιορίζουν, εισάγουν παρεμβολές, υποβαθμίζουν ή επιβάλλουν διακρίσεις έναντι συγκεκριμένου περιεχομένου**, εφαρμογών ή υπηρεσιών ή συγκεκριμένων κατηγοριών αυτών, **εκτός αν αυτό είναι αναγκαίο** και **μόνο για όσο διάστημα είναι αναγκαίο**, ούτως ώστε:

α) να συμμορφωθούν με τις ενωσιακές νομοθετικές πράξεις ή την εθνική νομοθεσία που συμμορφώνεται με το ενωσιακό δίκαιο, στην οποία υπάγεται ο πάροχος υπηρεσιών πρόσβασης στο διαδίκτυο, ή με τα μέτρα που συμμορφώνονται με το ενωσιακό δίκαιο που θέτει σε εφαρμογή τις εν λόγω ενωσιακές νομοθετικές πράξεις ή εθνική νομοθεσία, μεταξύ άλλων και με τις αποφάσεις δικαστηρίων ή δημόσιων αρχών που διαθέτουν τις σχετικές αρμοδιότητες·

Censorship

- Body of European Regulators for Electronic Communications (BEREC)
- BEREC Net Neutrality Regulatory Assessment Methodology

4.1.3 DNS manipulation

DNS manipulation refers to a situation where a DNS reply is received (on an A or AAAA request) which falsely indicates that the domain is unknown or where an incorrect IP address is returned. The result of this manipulation is that the client is redirected to a different address.

DNS manipulation can be detected by analysing the responses to DNS requests on known targets (e.g. DNS records of specific domains under the control of the NRA).

Note that end user environment (especially firewalls) may affect the results. However, in the case of a crowdsourcing approach it may be possible to compare thousands of results from different end users and using different DNS resolvers which could solve the problem.

Censorship

- Αποφάσεις Ελληνικών Δικαστηρίων
  - 13478/2014 Μον. Πρωτοδικείο Αθηνών
  - 10452/2015 Μον. Πρωτοδικείο Αθηνών
- DNS Filtering περιορίζει/παραβιάζει:
  - Την ελευθερία πληροφόρησης
  - Τη συμμετοχή στην ΚτΠ
  - Την προστασία προσωπικών δεδομένων
  - Το απόρρητο της ελεύθερης ανταπόκρισης και επικοινωνίας
  - Τη διαδικτυακή ουδετερότητα
- Κρίση περιορισμού δικαιωμάτων από μια επιτροπή (μη εφαρμογή αρχή αναλογικότητας)

μελών των αιτούντων νομικών προσώπων (που αφορούν όλο και λιγότερο τους ίδιους τους δημιουργούς και περισσότερο τα συμφέροντα των ίδιων των εταιρειών της πολιτιστικής βιομηχανίας), στο σύνολό τους, συνιστούν περιορισμούς των κατωτέρω αναφερομένων δικαιωμάτων, οι οποίοι, όμως, δεν είναι συμβατοί με την αρχή της αναλογικότητας και με το απαραβίαστο : (α) της ελευθερίας της πληροφόρησης (άρθρο 5 α παρ. 1 Σ), (β) του δικαιώματος συμμετοχής στην κοινωνία της πληροφορίας (άρθρο 5 α παρ. 2 Σ), ως αναγκαίας προϋπόθεσης για την ισότιμη συμμετοχή των ατόμων στην κοινωνική, πολιτική και οικονομική ζωή καθώς και για τηνμε ουσιαστικό τρόπο ενάσκηση των θεμελιωδών δικαιωμάτων τους, (γ) του δικαιώματος προστασίας από τη συλλογή, επεξεργασία και χρήση των προσωπικών δεδομένων (άρθρο 9 α Σ), (δ) του απορρήτου της ελεύθερης ανταπόκρισης και επικοινωνίας (άρθρο 19 Σ), δεδομένου ότι μέσω αυτών καταστέλλονται, αδιακρίτως, όχι μόνον παράνομες αλλά και νόμιμες πράξεις και ως εκ τούτου συνιστούν ανεπίτρεπτη επέμβαση στις τελευταίες, που ενώ δεν σχετίζονται με την διακίνηση

ΕΠΙΤΡΟΠΗ ΓΙΑ ΤΗ ΔΙΑΔΙΚΤΥΑΚΗ ΠΡΟΣΒΟΛΗ ΤΗΣ ΠΝΕΥΜΑΤΙΚΗΣ ΙΔΙΟΚΤΗΣΙΑΣ

του άρθρου 66Ε του νόμου 2121/1993

Η πρόσβαση στη σελίδα που προσπάθησες να επισκεφθείς έχει διακοπεί με απόφαση της ΕΔΠΠΙ

γιατί παρείχε πρόσβαση παράνομα σε έργα που προστατεύονται με δικαίωμα πνευματικής ιδιοκτησίας

Σκέψου ότι επιλέγοντας την πρόσβαση σε περιεχόμενο από νόμιμες πηγές, συνεισφέρεις στην καλλιτεχνική δημιουργία, στη βελτίωση του πολιτιστικού προϊόντος και στην ανάπτυξη της οικονομίας

Interception

```
$ dig +short @212.205.212.205 libgen.is
  83.235.64.18

$ dig -x 83.235.64.18
  edppi.otenet.gr.

$ curl -I libgen.is
  HTTP 302 Moved Temporarily
```

Censorship

- Turkey (social media, Wikipedia)
- Egypt (social media, news sites)
- Spain (Catalonia referendum sites)

Open Observatory of Network Interference
ooni.torproject.org

DNS over HTTPS

RFC 8484

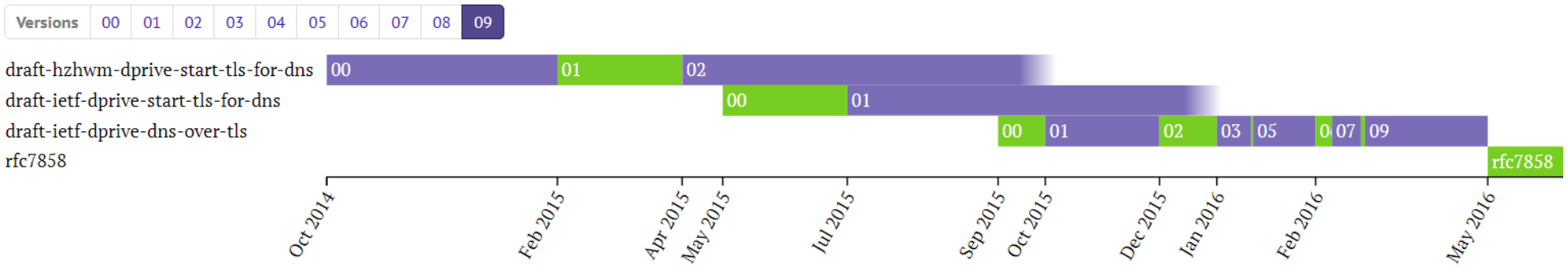

```
The first example request uses GET to request "www.example.com".

:method = GET
:scheme = https
:authority = dnsserver.example.net
:path = /dns-query?dns=AAABAAABAAAAAAAAA3d3dwdleGFtcGxlA2NvbQAAAQAB
accept = application/dns-message
```

DNS over TLS

Specification for DNS over Transport Layer Security (TLS)

RFC 7858

Status | IESG evaluation record | IESG writeups | Email expansions | History



- Initiation of DNS over TLS is very straightforward. By establishing a connection over a well-known port, clients and servers expect and agree to negotiate a TLS session to secure the channel.
- DNS clients and servers MUST NOT use port 853 to transport **cleartext** DNS messages.
- By default, a DNS server that supports DNS over TLS MUST listen for and accept TCP connections on port 853, unless it has mutual agreement with its clients to use a port other than 853 for DNS over TLS.

Demo

“Here we are now, entertain us”

~ Kurt Cobain

https://vimeo.com/377333902

Building Blocks

- **Let’s Encrypt**

  letsencrypt.org

- **dnsdist**

  dnsdist.org

- **dns-over-https**

  github.com/m13253/dns-over-https

- **nginx**

  nginx.org

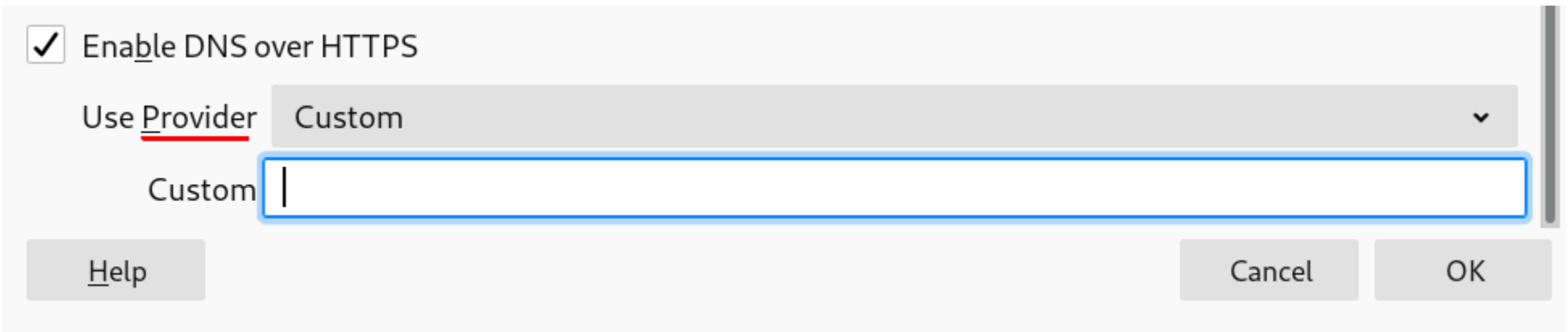
- **PowerDNS Recursor**

  powerdns.com

https://vimeo.com/377388498

DoH: Firefox

- General --> Network Settings --> Settings
- Enable DNS over HTTPS
- Pick provider



DoT: Systemd

/etc/systemd/resolved.conf

```
[Resolve]
DNS=___.___.___.____
DNSOverTLS=yes
```

Critical Engineering

The Critical Engineer considers any technology depended upon to be both a challenge and a threat. The greater the dependence on a technology the greater the need to study and expose its inner workings, regardless of ownership or legal provision.

criticalengineering.org

Organize

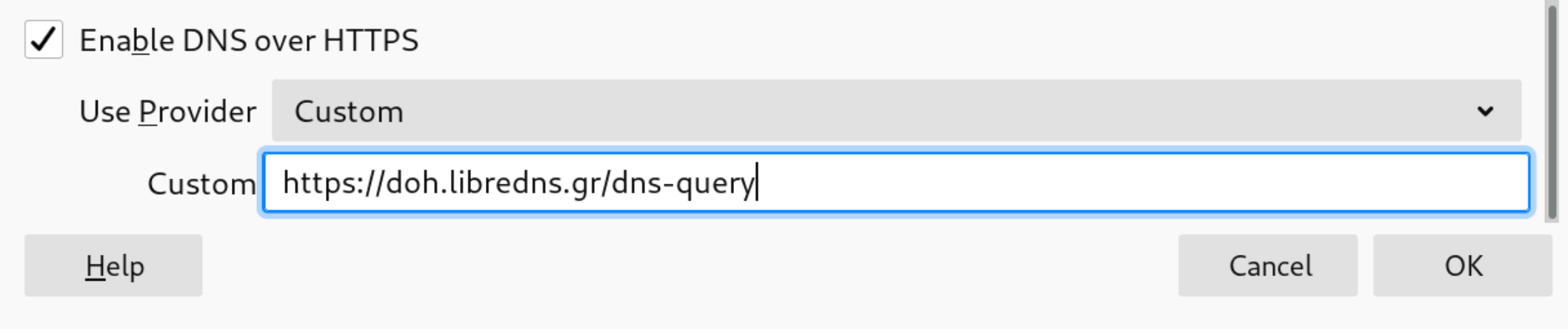
Many hackers around the world are (re-)decentralizing the net. **This is our part**, offering distributed, free (as in freedom) services to the world. Always based on Free Open Source Software.

libreops.cc

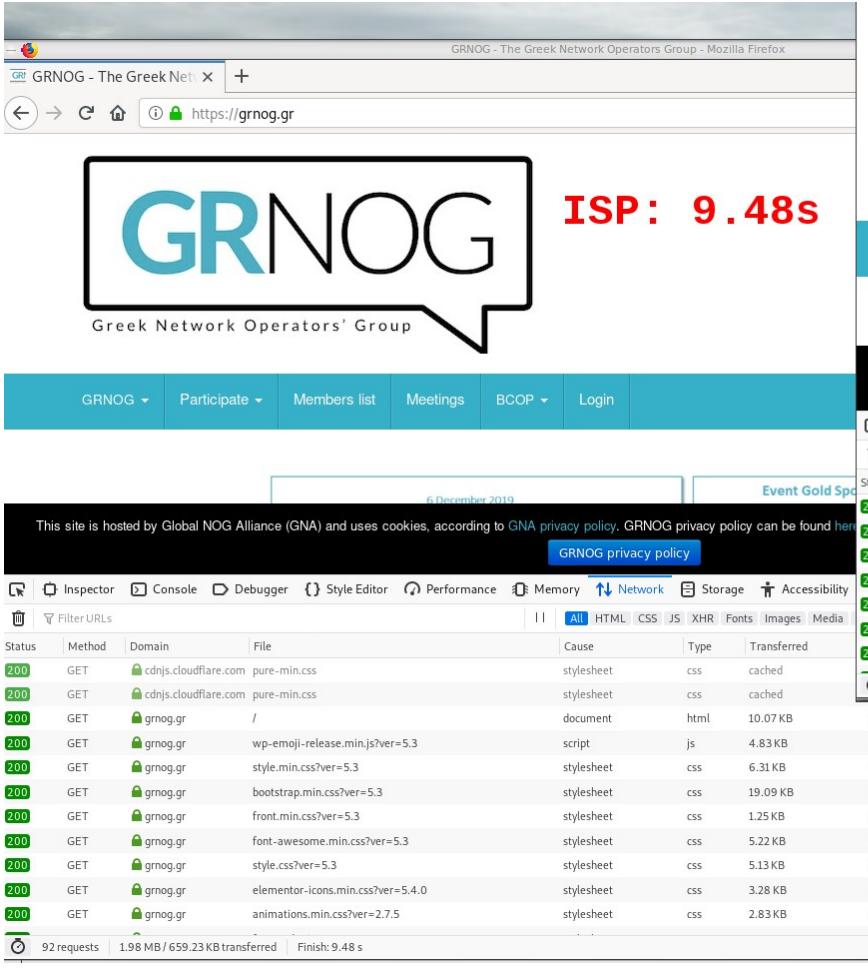
LibreDNS

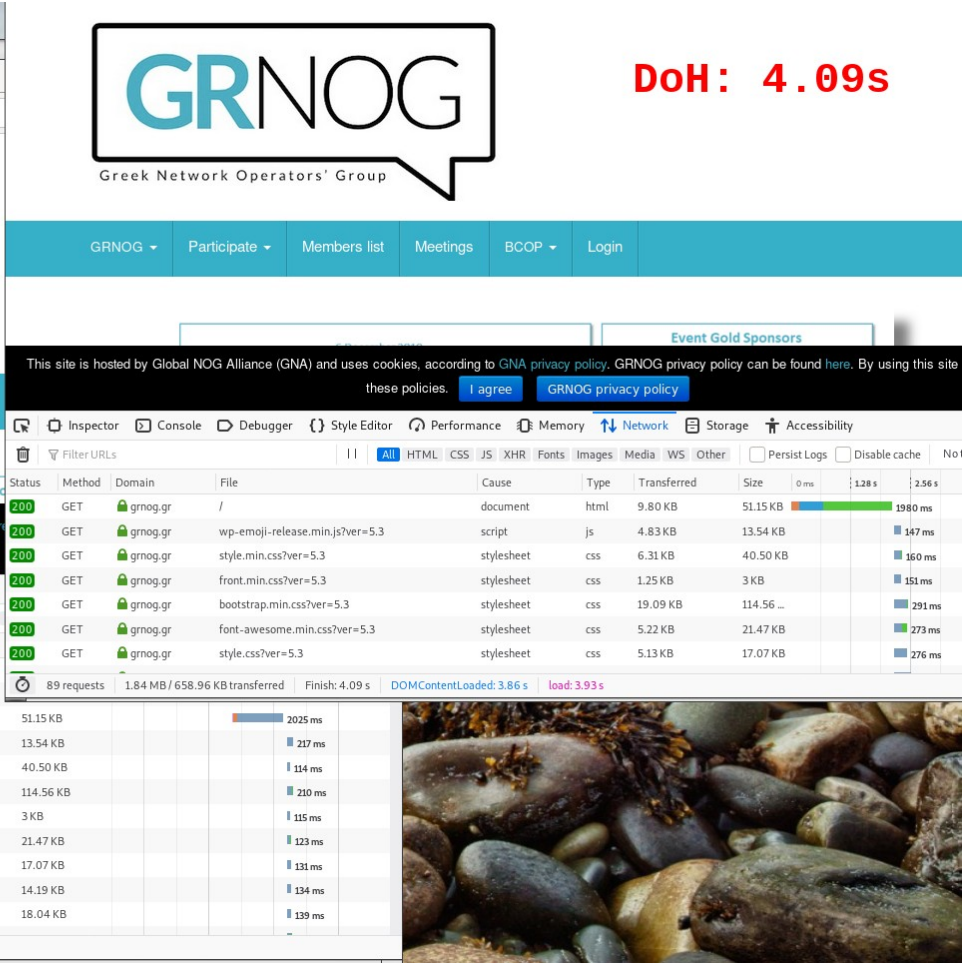
A public encrypted DNS service, that people can use, to maintain secrecy of their DNS traffic, but also circumvent censorship.

libredns.gr



Metrics


GRNOG - The Greek Network Operators Group - Mozilla Firefox
https://grnog.gr
GRNOG
Greek Network Operators' Group
ISP: 9.48s
GRNOG
Participate
Members list
Meetings
BCOP
Login
This site is hosted by Global NOG Alliance (GNA) and uses cookies, according to GNA privacy policy. GRNOG privacy policy can be found here
GRNOG privacy policy
Inspector
Console
Debugger
Style Editor
Performance
Memory
Network
Storage
Accessibility
92 requests
1.98 MB / 659.23 KB transferred
Finish: 9.48 s


GRNOG
Greek Network Operators' Group
DoH: 4.09s
GRNOG
Participate
Members list
Meetings
BCOP
Login
Event Gold Sponsors
This site is hosted by Global NOG Alliance (GNA) and uses cookies, according to GNA privacy policy. GRNOG privacy policy can be found here. By using this site
these policies.
I agree
GRNOG privacy policy
Inspector
Console
Debugger
Style Editor
Performance
Memory
Network
Storage
Accessibility
89 requests
1.84 MB / 658.96 KB transferred
Finish: 4.09 s
DOMContentLoaded: 3.86 s
load: 3.93 s

Metrics

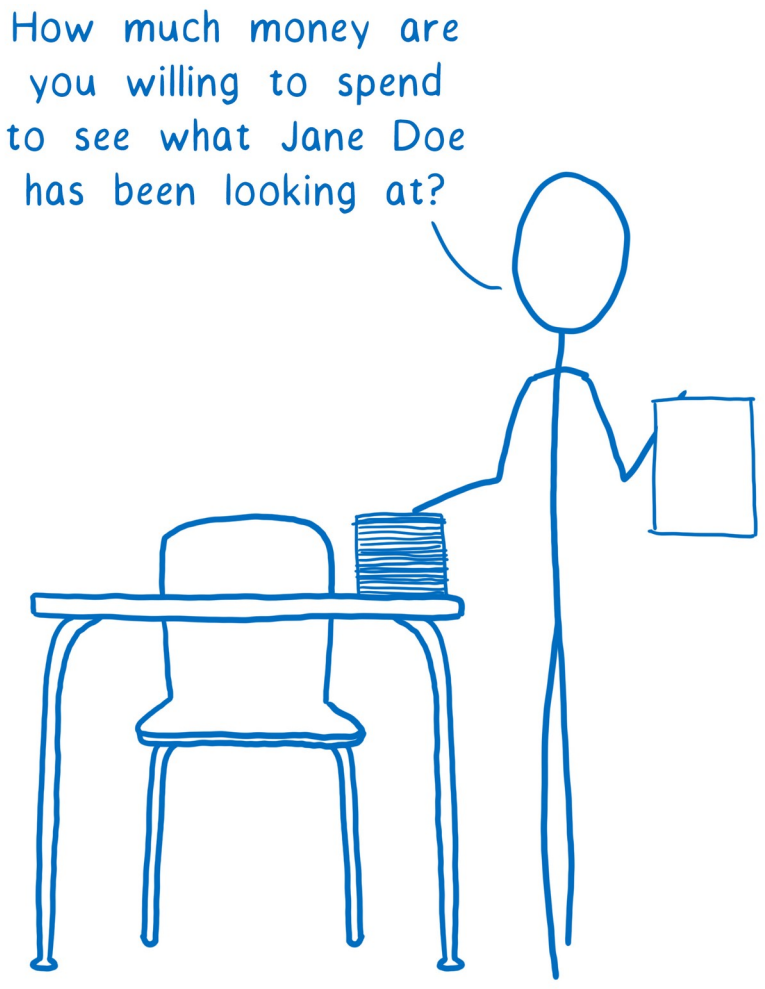
```
$ dig grnog.gr
Query time: 26 msec

$ /bin/time -f %E  curl -s https://doh.libredns.gr/dns-query?name=grnog.gr
0:00.52

$ /bin/time -f %E  curl -s https://mozilla.cloudflare-dns.com/dns-query?name=grnog.gr
0:00.46

$ dig grnog.gr @8.8.8.8|grep time
  Query time: 57 msec

$ dig grnog.gr @1.1.1.1|grep time
  Query time: 20 msec

$ dig grnog.gr @9.9.9.9|grep time
  Query time: 138 msec
```

Resources

- LibreDNS source code

  gitlab.com/libreops/libredns

Questions?


How much money are you willing to spend to see what Jane Doe has been looking at?