Data protection in web development *made easy*

Amelia Andersdotter & Anders Jensen-Urstad

DrupalCamp Baltics
August 28, 2015

“Our freedom is built on what others do not know of our existences.”
—ALEKSANDR SOLZHENITSYN

dataskydd.net

“Everyone has the right to respect for his private and family life, his home and his correspondence.”

—EUROPEAN CONVENTION ON HUMAN RIGHTS, ARTICLE 8

Data protection

A collection of tools for achieving privacy.

Data security

When procedures work as foreseen.

How to be excellent to each other

~~How we defeat NSA/GCHQ/whoever~~

Do your visitors have an obligation to help you or your client out?

Right to *know* ❧

Right to *consent*

User-centric

Data minimization

Effective sanctions

Right to *know*

Right to *consent* ❧

User-centric

Data minimization

Effective sanctions

Right to *know*

Right to *consent*

User-centric ❧

Data minimization

Effective sanctions

Right to *know*

Right to *consent*

User-centric

Data minimization

Effective sanctions

Right to *know*

Right to *consent*

User-centric

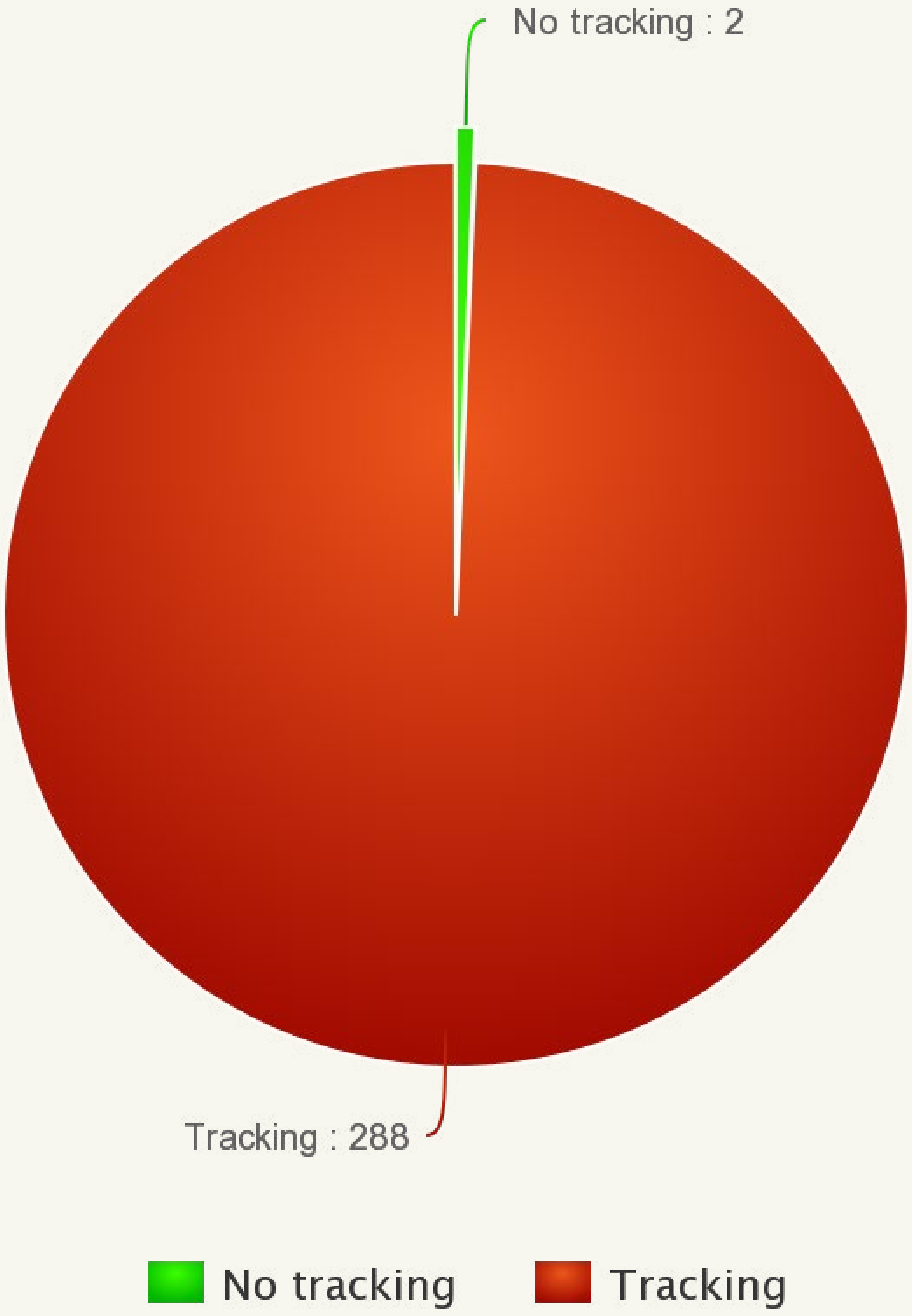
Data minimization

Effective sanctions ❧

Public sector websites

Private visits

Governing vs. *governance*



99% of Swedish municipalities use either…

- third-party trackers
- tracking cookies
- third-party service behaviors

European Union Law

Present:

Directive 2002/48/EC *E-Privacy. Art 5(3): "cookie law"*

Directive 1995/46/EC *Data Protection*

Directive 2014/53/EU *Radio Equipment Standardisation*

Member State laws on public administration

Coming:

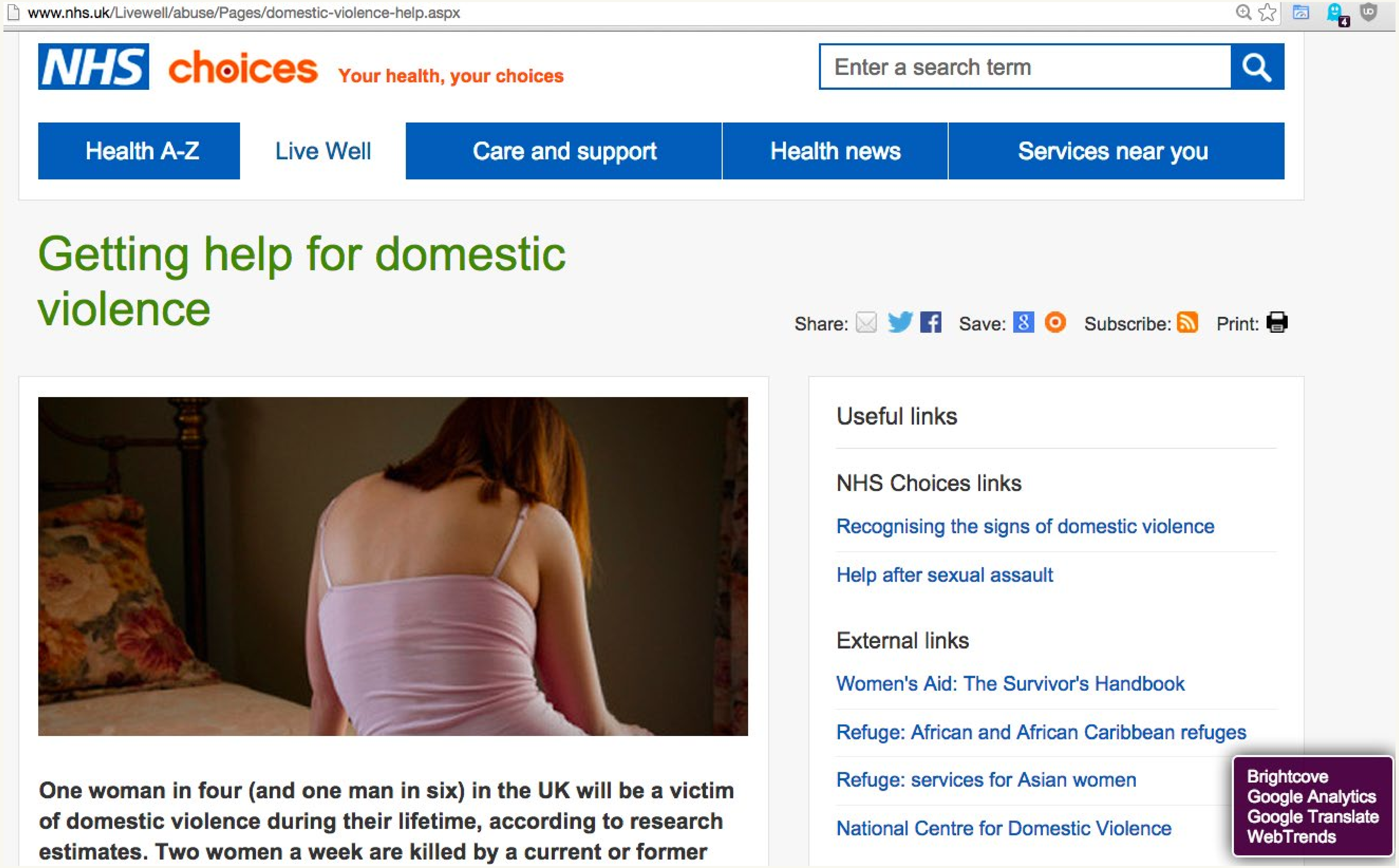
General Data Protection Regulation (GDPR)

Law Enforcement Data Protection Directive

So what to do?

1. Encrypt *all* the things.
2. Don’t expose your visitors to others.

    (At least not without consent!)



www.nhs.uk/Livewell/abuse/Pages/domestic-violence-help.aspx

Getting help for domestic violence

One woman in four (and one man in six) in the UK will be a victim of domestic violence during their lifetime, according to research estimates. Two women a week are killed by a current or former

Useful links

NHS Choices links

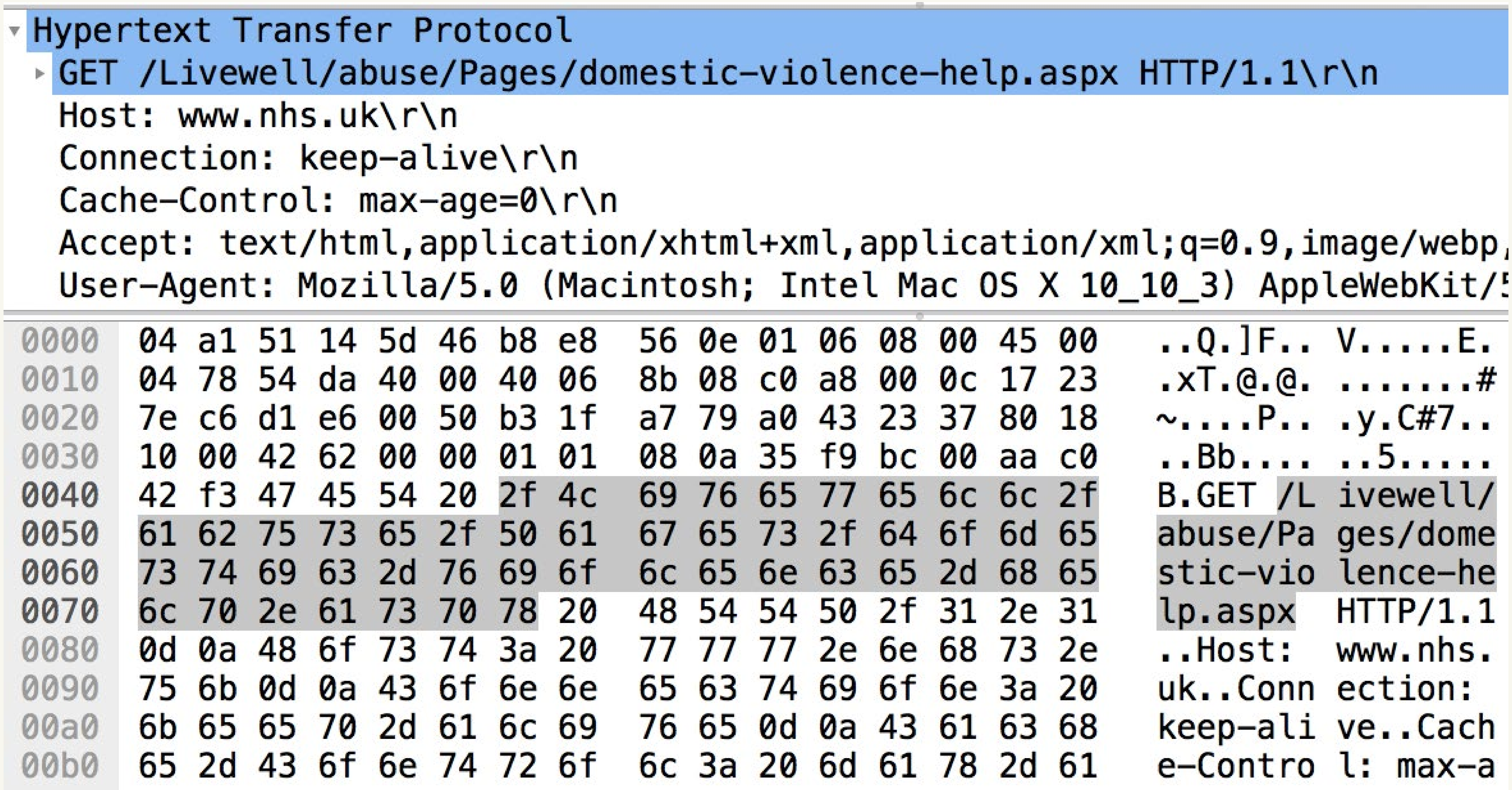
- Recognising the signs of domestic violence
- Help after sexual assault

External links

- Women's Aid: The Survivor's Handbook
- Refuge: African and African Caribbean refuges
- Refuge: services for Asian women
- National Centre for Domestic Violence

Brightcove
Google Analytics
Google Translate
WebTrends

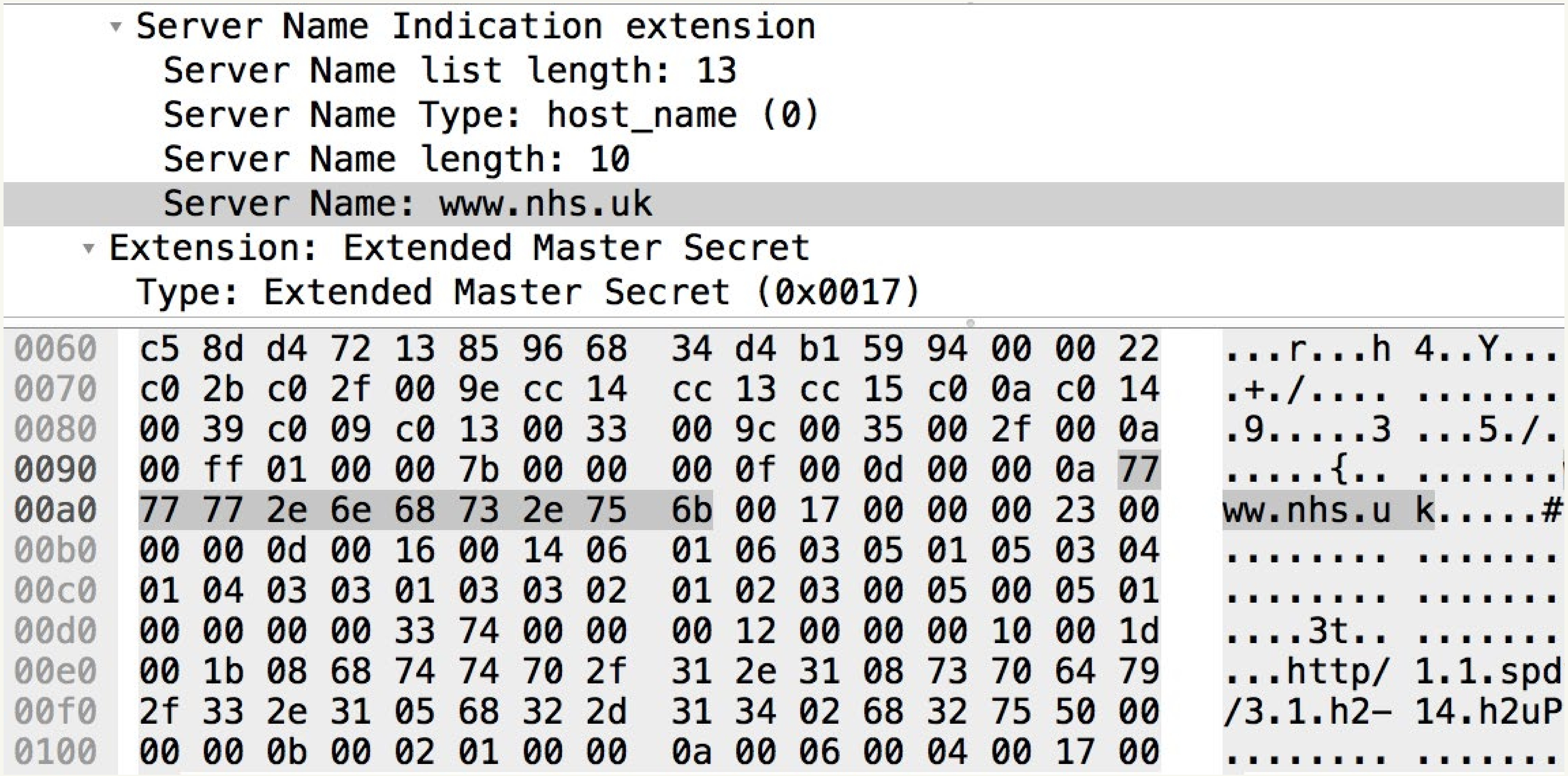
HTTP



```
▾ Hypertext Transfer Protocol
  ▸ GET /Livewell/abuse/Pages/domestic-violence-help.aspx HTTP/1.1\r\n
    Host: www.nhs.uk\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_3) AppleWebKit/5
```

```
0000  04 a1 51 14 5d 46 b8 e8  56 0e 01 06 08 00 45 00   ..Q.]F.. V.....E.
0010  04 78 54 da 40 00 40 06  8b 08 c0 a8 00 0c 17 23   .xT.@.@. .......#
0020  7e c6 d1 e6 00 50 b3 1f  a7 79 a0 43 23 37 80 18   ~....P.. .y.C#7..
0030  10 00 42 62 00 00 01 01  08 0a 35 f9 bc 00 aa c0   ..Bb.... ..5.....
0040  42 f3 47 45 54 20 2f 4c  69 76 65 77 65 6c 6c 2f   B.GET /L ivewell/
0050  61 62 75 73 65 2f 50 61  67 65 73 2f 64 6f 6d 65   abuse/Pa ges/dome
0060  73 74 69 63 2d 76 69 6f  6c 65 6e 63 65 2d 68 65   stic-vio lence-he
0070  6c 70 2e 61 73 70 78 20  48 54 54 50 2f 31 2e 31   lp.aspx  HTTP/1.1
0080  0d 0a 48 6f 73 74 3a 20  77 77 77 2e 6e 68 73 2e   ..Host:  www.nhs.
0090  75 6b 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20   uk..Conn ection: 
00a0  6b 65 65 70 2d 61 6c 69  76 65 0d 0a 43 61 63 68   keep-ali ve..Cach
00b0  65 2d 43 6f 6e 74 72 6f  6c 3a 20 6d 61 78 2d 61   e-Contro l: max-a
```

HTTPS



```
▾ Server Name Indication extension
    Server Name list length: 13
    Server Name Type: host_name (0)
    Server Name length: 10
    Server Name: www.nhs.uk
▾ Extension: Extended Master Secret
    Type: Extended Master Secret (0x0017)

0060  c5 8d d4 72 13 85 96 68  34 d4 b1 59 94 00 00 22   ...r...h 4..Y...
0070  c0 2b c0 2f 00 9e cc 14  cc 13 cc 15 c0 0a c0 14   .+./.... .......
0080  00 39 c0 09 c0 13 00 33  00 9c 00 35 00 2f 00 0a   .9.....3 ...5./.
0090  00 ff 01 00 00 7b 00 00  00 0f 00 0d 00 00 0a 77   .....{.. .......
00a0  77 77 2e 6e 68 73 2e 75  6b 00 17 00 00 00 23 00   ww.nhs.u k.....#
00b0  00 00 0d 00 16 00 14 06  01 06 03 05 01 05 03 04   ........ .......
00c0  01 04 03 03 01 03 03 02  01 02 03 00 05 00 05 01   ........ .......
00d0  00 00 00 00 33 74 00 00  00 12 00 00 00 10 00 1d   ....3t.. .......
00e0  00 1b 08 68 74 74 70 2f  31 2e 31 08 73 70 64 79   ...http/ 1.1.spd
00f0  2f 33 2e 31 05 68 32 2d  31 34 02 68 32 75 50 00   /3.1.h2- 14.h2uP
0100  00 00 0b 00 02 01 00 00  0a 00 06 00 04 00 17 00   ........ .......
```

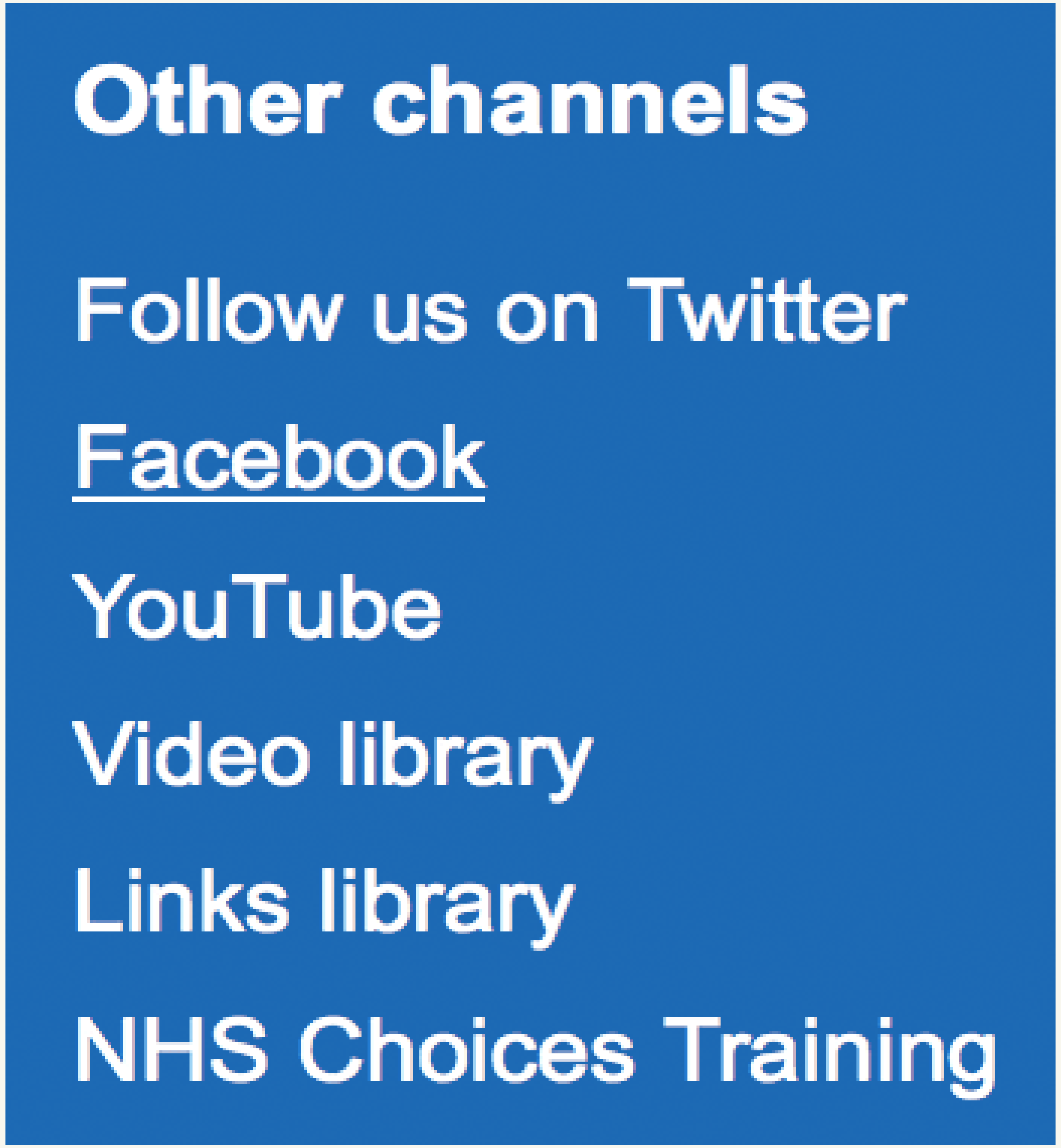
- SSL certificates are cheap
- Let's Encrypt (letsencrypt.org) will make them free and automated:

```
  $ sudo apt-get install lets-encrypt
  $ lets-encrypt example.com
```

- Use HTTP Strict Transport Security (HSTS)

(Bonus: HTTPS now used as a ranking signal by Google.)

Referrers



Other channels

Follow us on Twitter

Facebook

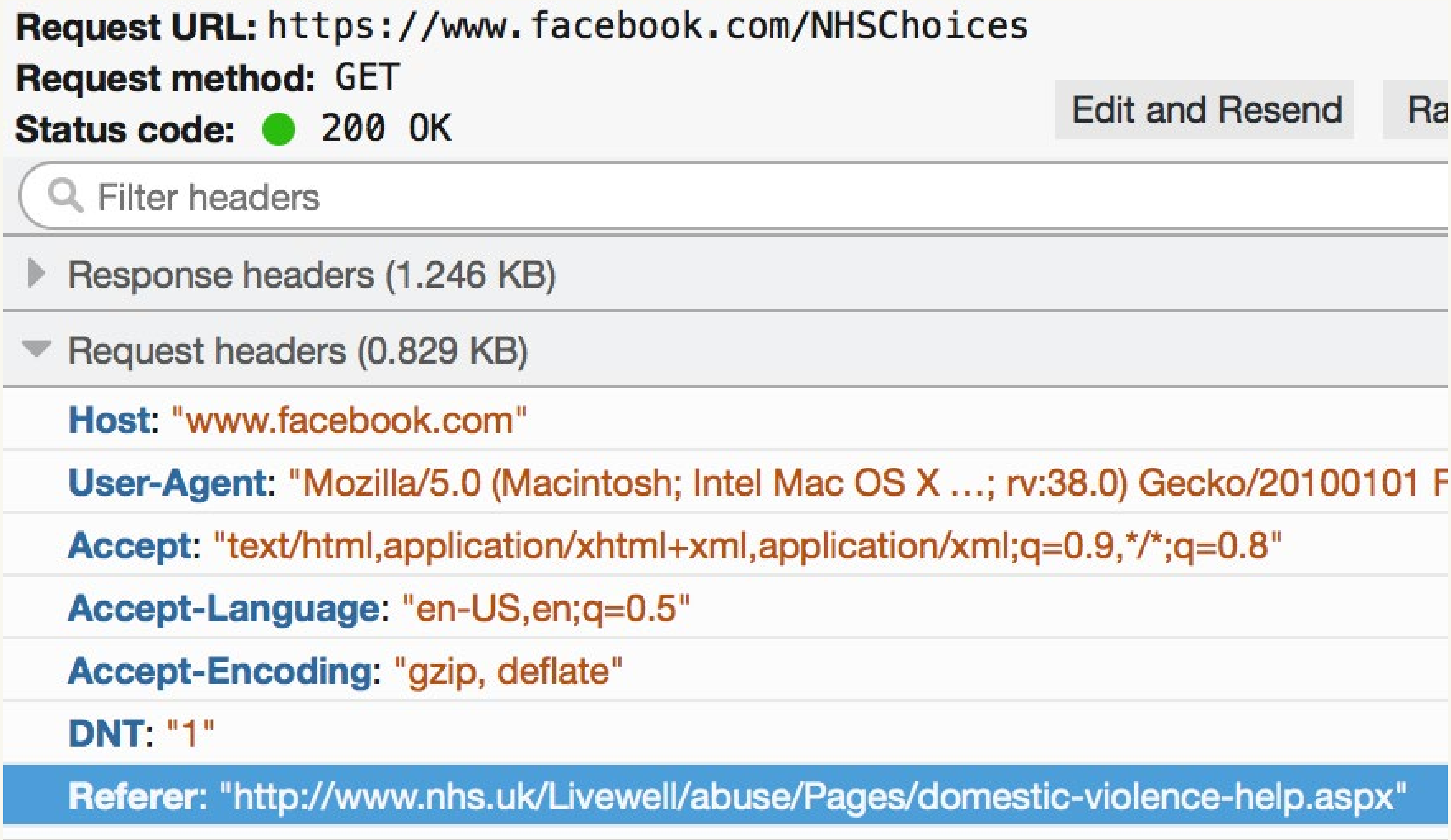
YouTube

Video library

Links library

NHS Choices Training

click



Request URL: https://www.facebook.com/NHSChoices

Request method: GET

Status code: ● 200 OK

Response headers (1.246 KB)

Request headers (0.829 KB)

Host: "www.facebook.com"

User-Agent: "Mozilla/5.0 (Macintosh; Intel Mac OS X …; rv:38.0) Gecko/20100101 F

Accept: "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8"

Accept-Language: "en-US,en;q=0.5"

Accept-Encoding: "gzip, deflate"

DNT: "1"

Referer: "http://www.nhs.uk/Livewell/abuse/Pages/domestic-violence-help.aspx"

Don’t tell other websites about your visitors

```
<a href="http://foo.bar" rel="noreferrer">
I don’t leak referrer information.
</a>
```

W3C HTML5 Recommendation, 4.8.4.8

(Plugin: https://drupal.org/project/noreferrer)

Referrer Policy, W3C draft

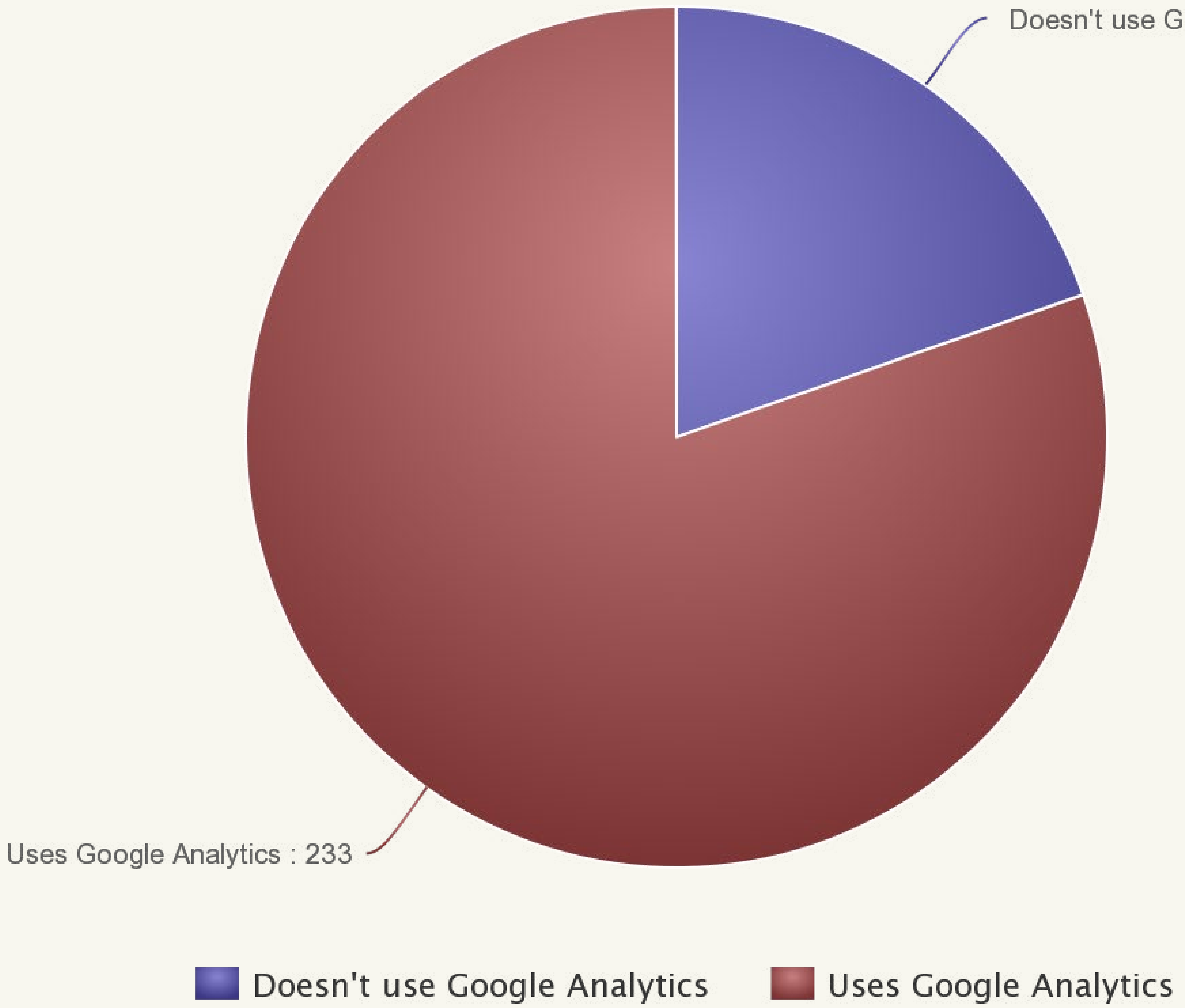
Firefox, Chrome, Safari, Microsoft Edge:

```
<meta name="referrer" content="never" />
```

Soon:

```
<a href="http://whitelist.me"
referrerpolicy="unsafe-url">Send referrer, always</a>
```

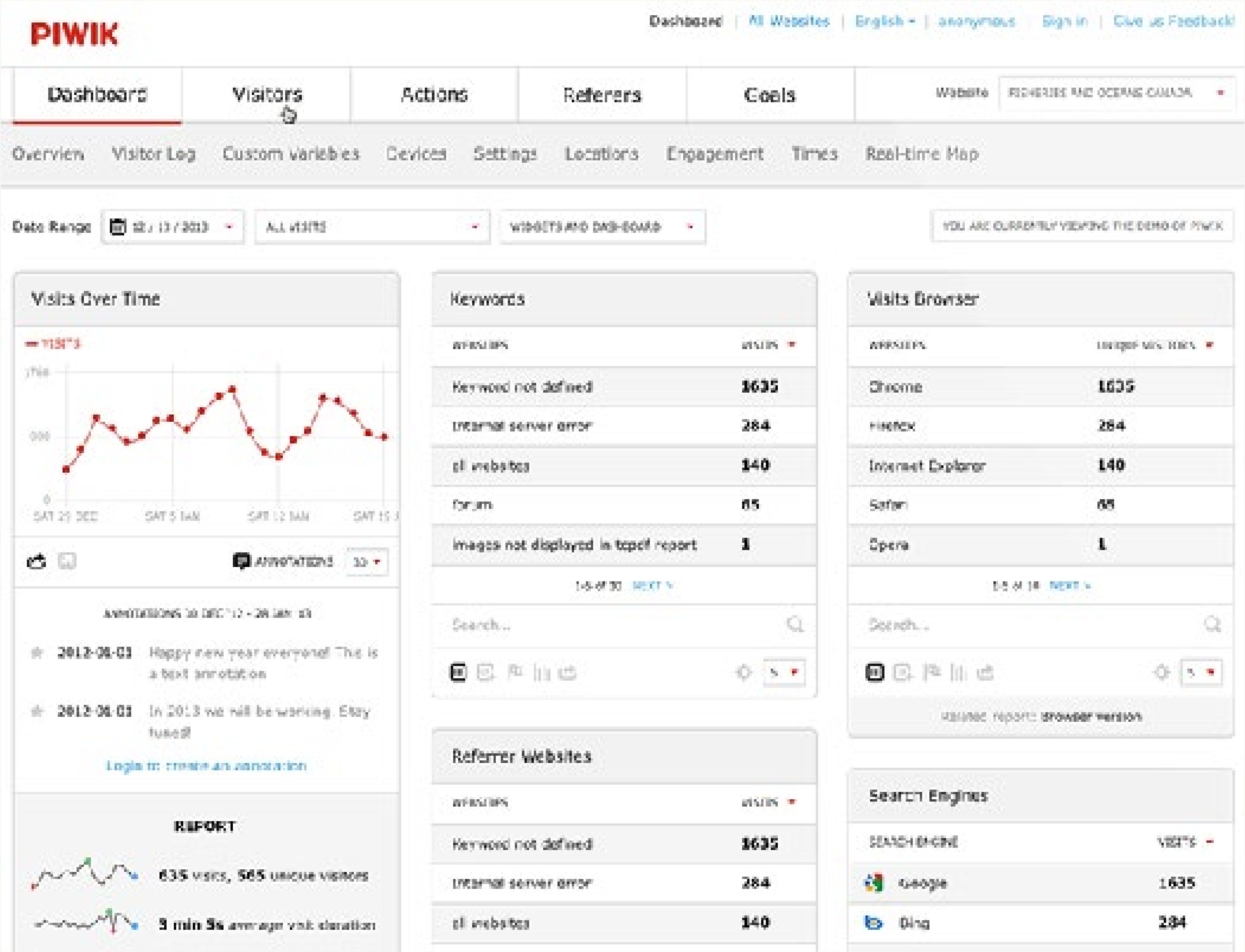
No More Shall We Third-Party



Google Analytics usage among Swedish municipalities

Piwik

- Open source, PHP + MYSQL
- *You* own the data
- Various privacy options
- Can be used without cookies



ANNOTATIONS 30 DEC '12 - 28 JAN '13

☆ 2012-01-01 Happy new year everyone! This is a text annotation

☆ 2012-01-01 In 2013 we will be working. Stay tuned!

Login to create an annotation

REPORT

635 visits, **565** unique visitors

3 min 5s average visit duration

Keywords

WEBSITES	VISITS ▾
Keyword not defined	**1635**
internal server error	**284**
all websites	**140**
forum	**65**
images not displayed in tcpdf report	**1**

1-5 of 30 NEXT ›

Visits Browser

WEBSITES	UNIQUE VISITORS ▾
Chrome	**1635**
Firefox	**284**
Internet Explorer	**140**
Safari	**65**
Opera	**1**

1-5 of 18 NEXT ›

Related reports: **browser version**

Referrer Websites

WEBSITES	VISITS ▾
Keyword not defined	**1635**
internal server error	**284**
all websites	**140**

Search Engines

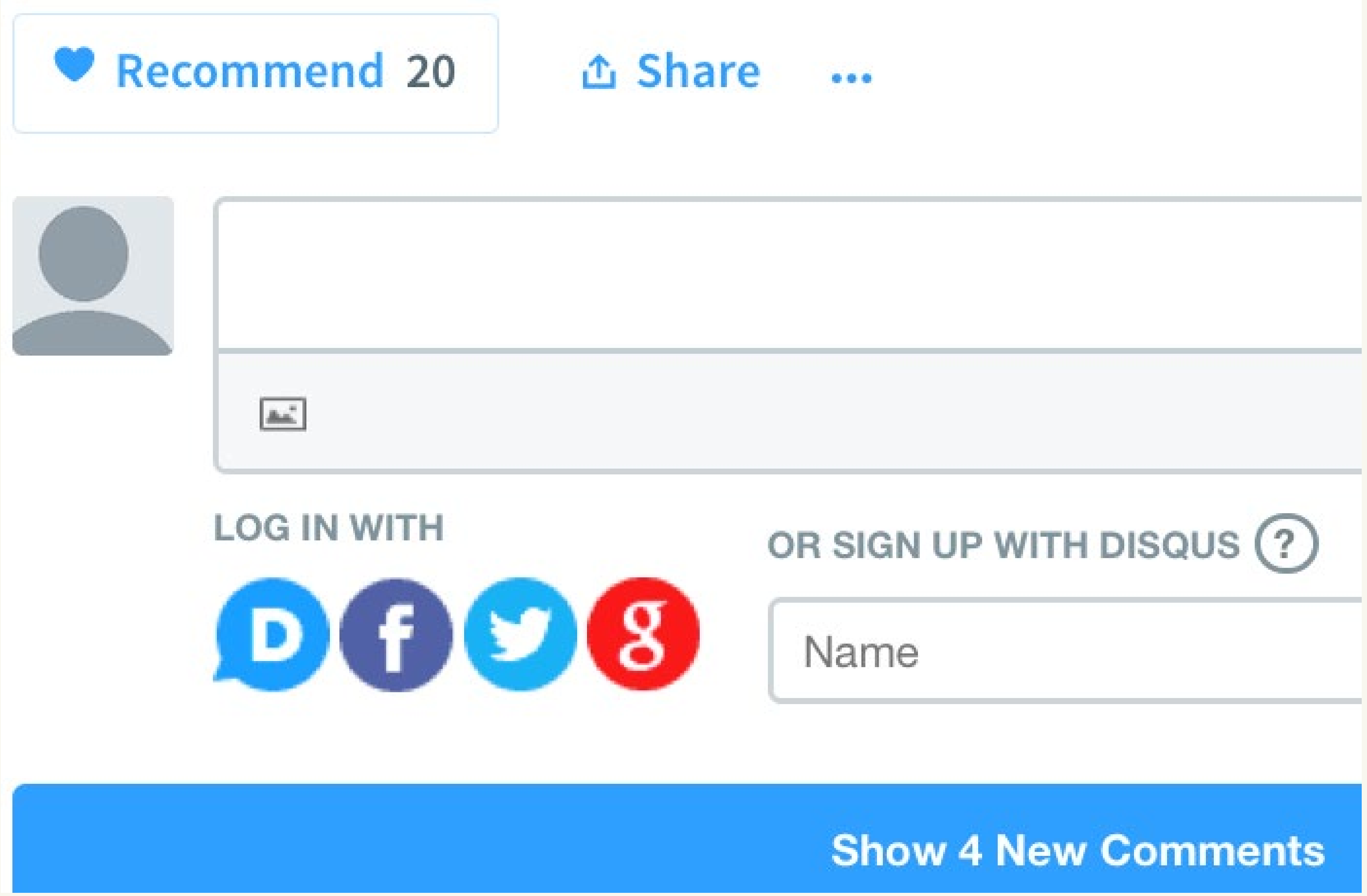
SEARCH ENGINE	VISITS ▾
Google	1635
Bing	**284**

Totally *radical* alternative: don’t track.

Third-parties: Comment platforms

Disqus:

- ~~Anonymity~~
- ~~Control~~
- ~~Rights~~
- ~~Privacy~~

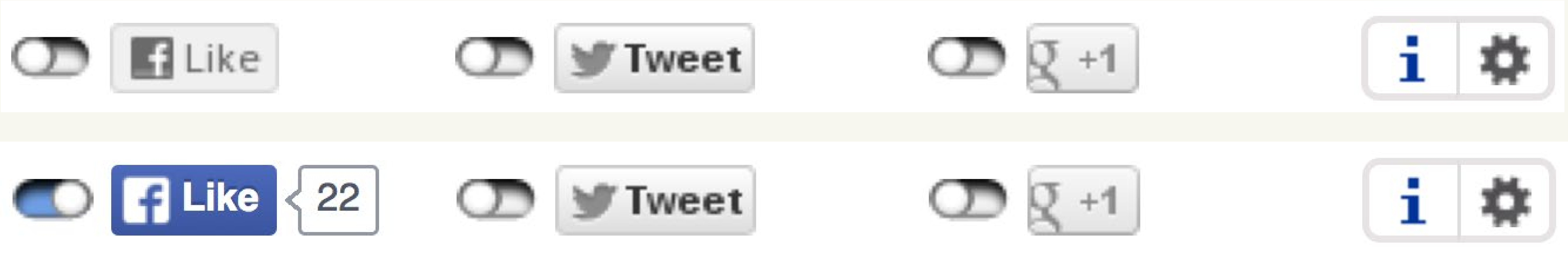


The Quest for a Disqus alternative

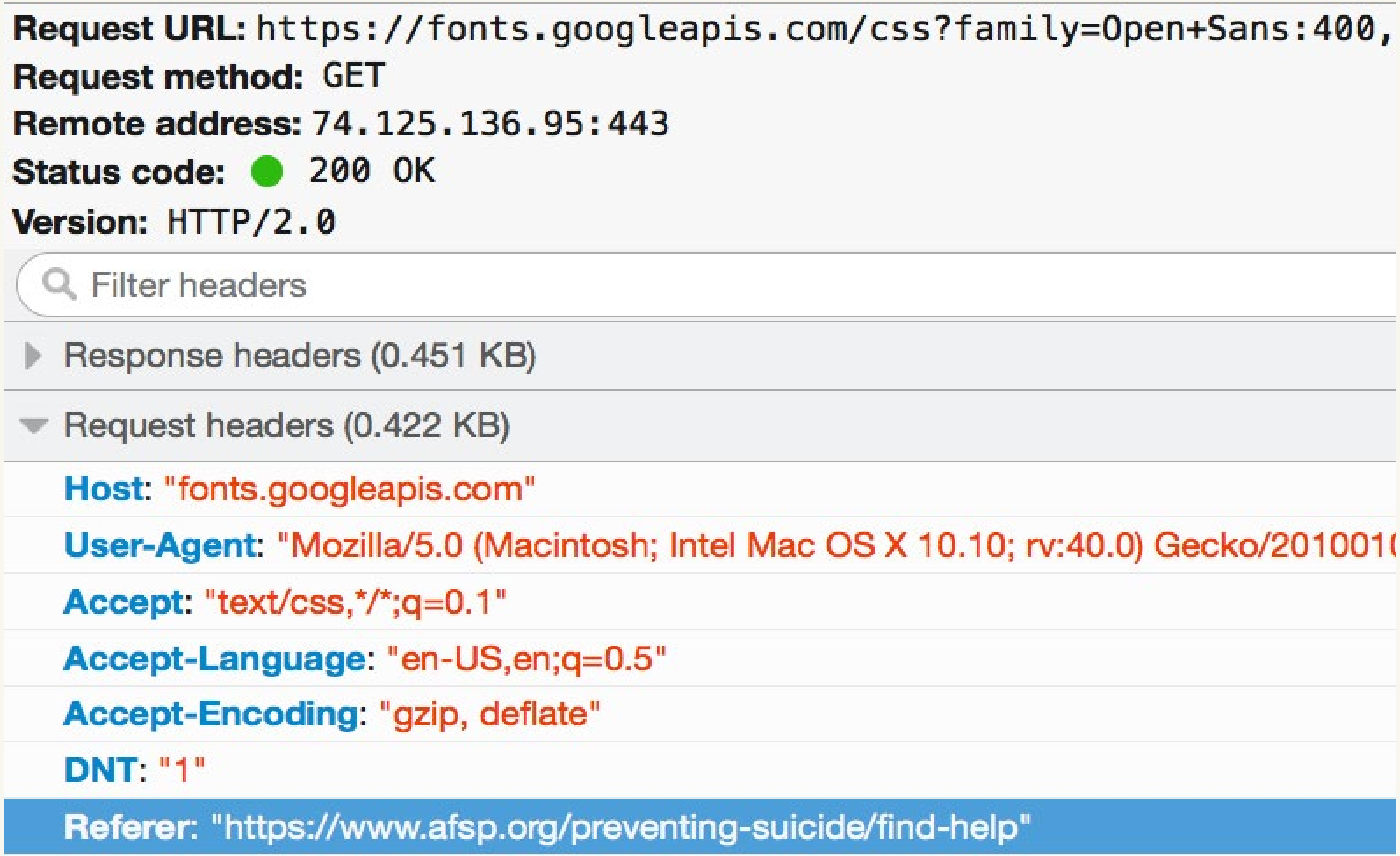
- Plain ol' built-in comment system
- Self-hosted open-source Disqus-like software (e.g., Isso, HashOver)
- Integration with forum software (e.g., Discourse, Vanilla Forums)

Third-parties: Social media

- Vendor-provided embedded like/share buttons track people
- Use locally hosted images/fonts instead!
- *Or*… two-click solution:



Third-parties: Fonts



Request URL: `https://fonts.googleapis.com/css?family=Open+Sans:400,`

Request method: `GET`

Remote address: `74.125.136.95:443`

Status code: ● `200 OK`

Version: `HTTP/2.0`

▸ Response headers (0.451 KB)

▾ Request headers (0.422 KB)

Host: "fonts.googleapis.com"

User-Agent: "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:40.0) Gecko/201001

Accept: "text/css,*/*;q=0.1"

Accept-Language: "en-US,en;q=0.5"

Accept-Encoding: "gzip, deflate"

DNT: "1"

Referer: "https://www.afsp.org/preventing-suicide/find-help"

Once More, with Feeling

Use HTTPS.

Don’t leak referrers.

No third-party resources without consent. *Self-host* when possible.

https://dataskydd.net/dcbaltics2015

In conclusion...

Individuals matter.

It's possible to protect privacy.

Join us! ❦

Amelia Andersdotter
amelia@andersdotter.cc
@teirdes
ameliaandersdotter.eu

Anders Jensen-Urstad
anders@unix.se
@ndrsju
anders.unix.se

Slides, references, code, etc.:
https://dataskydd.net/dcbaltics2015

DRUPALCAMP · BALTICS

2015

AUGUST 28TH

TALLINN

THANK YOU!

Q&A

www.drupalcampbaltics.com

EXOVE veebimajutus.ee ZONE.EE wunderkraut KWD druid.fi