TLS = Privacy. What?

Dirk Wetter (d0rk)

@drwetter

about:me

- **Independent security consultant**
  - > 20yrs of profession
  - pentests / defense+hardening / concepts / training / PM / (C)ISO
  - → Privacy: important to me
- **Community involvements**
  - OWASP
  - GUUG
- **My pet (project):** 
  - testssl.sh

about:whatis

- **Motivation**
  - Over-reaction privacy + TLS
  - Clean up fundamental misconception
    - Little clue about CIA triad
      - confidentialy, integrity, availability
    - Often confuse confidentiality @ transport with privacy
  - Different angles

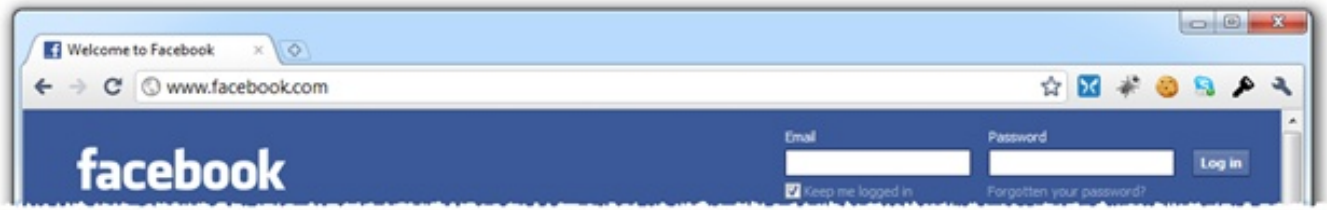
beyond:own_nose

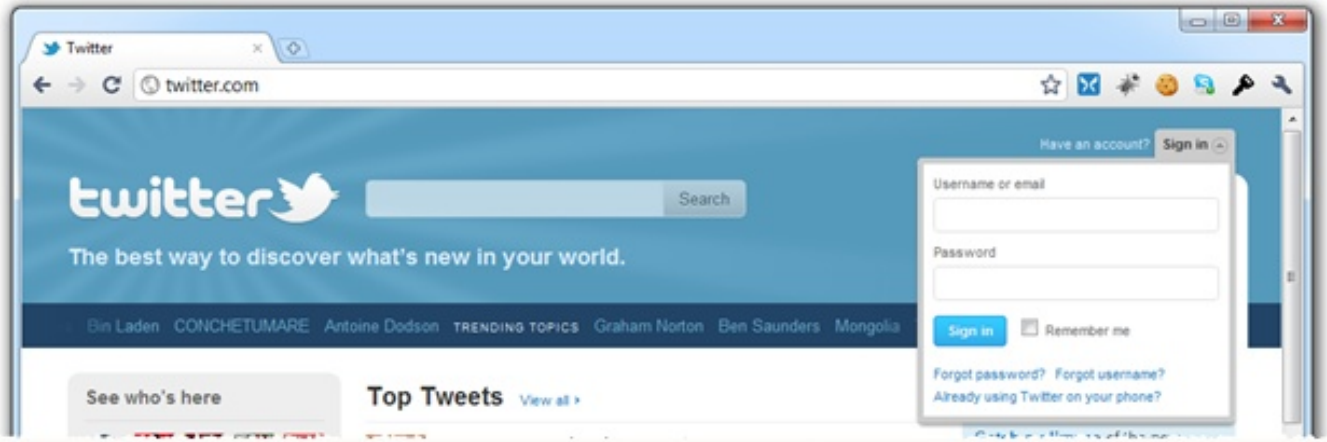
- **HTTP+TLS** commonly known as **HTTPS**
- **see beyond one's own TLS nose**
  - SMTP+STARTTLS
    - ~60% encrypted, ½ of it (~30%) only have proper certificate validation
    - configured MTA sender to hard fail?
  - IMAP/POP: (STARTTLS: 45-50%, pure IMAPS/POPS: 54-65%)
  - Jabber: C2S: ~3% (!), S2S < 1%
  - VoIP, GSM: keep on dreaming ;-)
  - DNS – oh well
- **Also: compare privacy values**
  - Can't think when Jabber, SMTP etc. is not privacy related

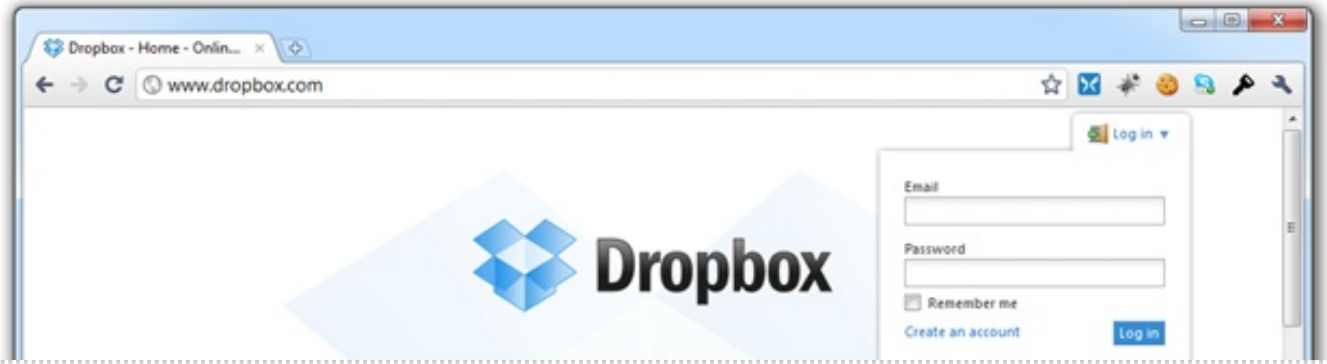
- **And now**

  HTTP+TLS commonly known as **HTTPS**

nottalking:about

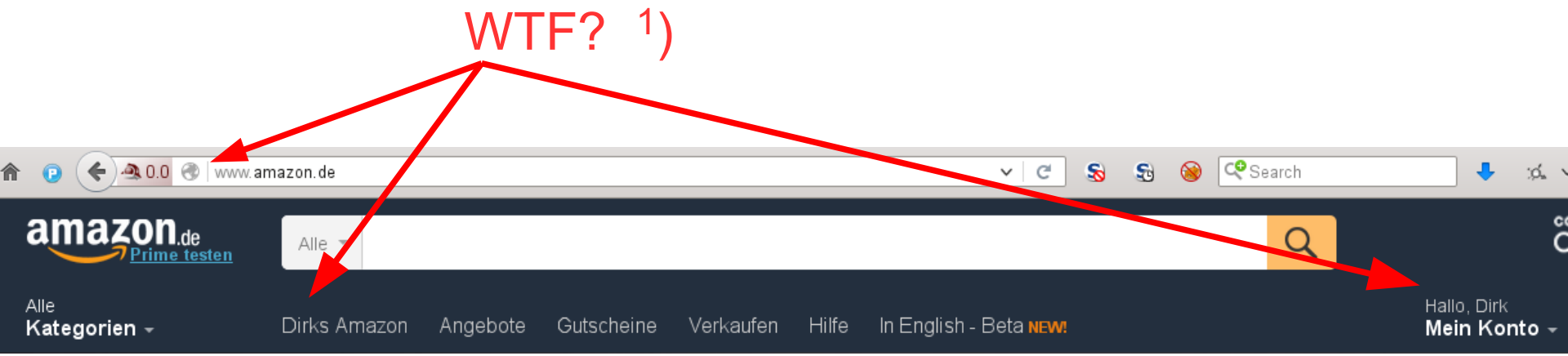






Troy Hunt 2011 @ https://www.troyhunt.com/ssl-is-not-about-encryption/

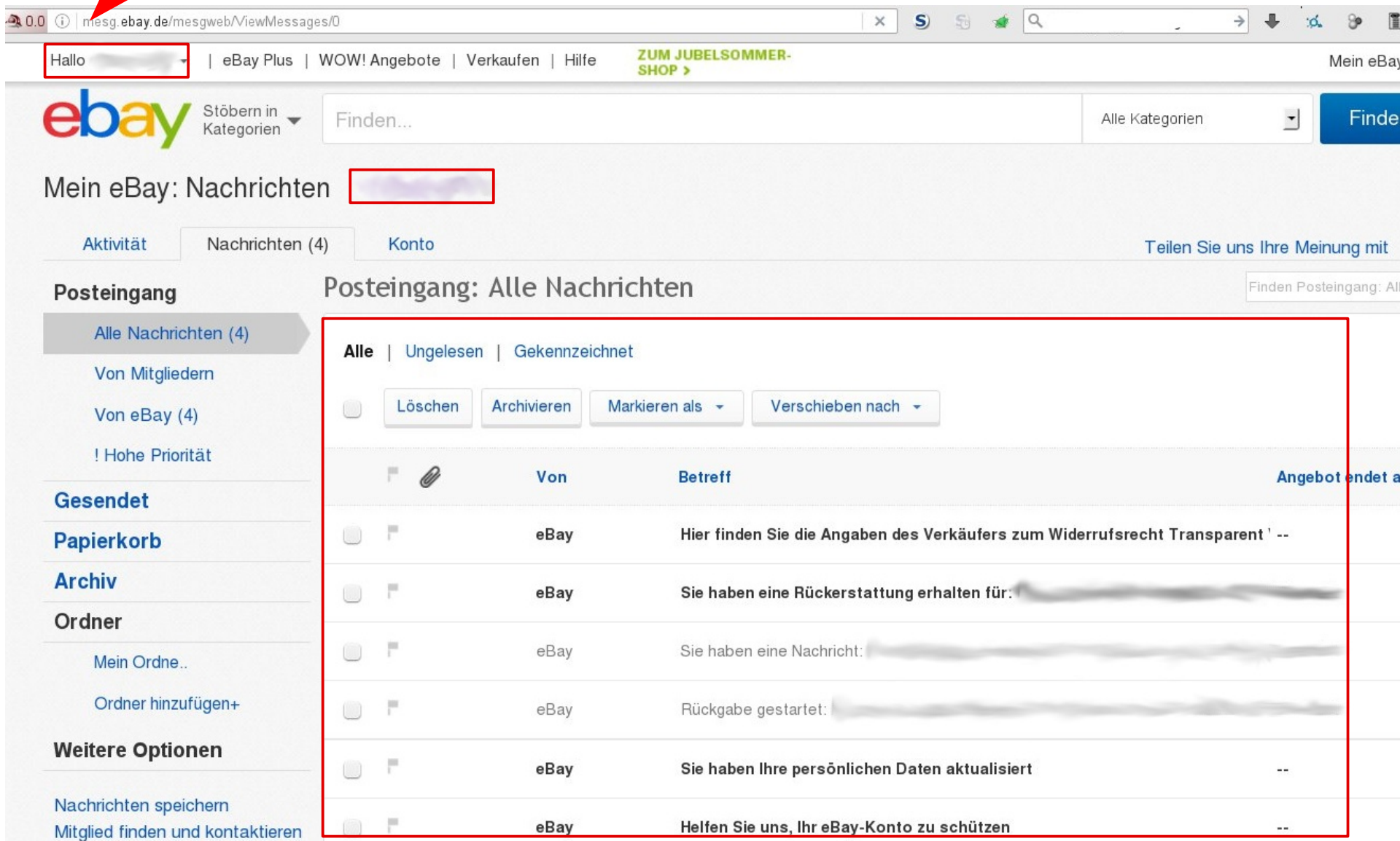
nottalking:about



1) German site until ~Q1/2016

WTF?

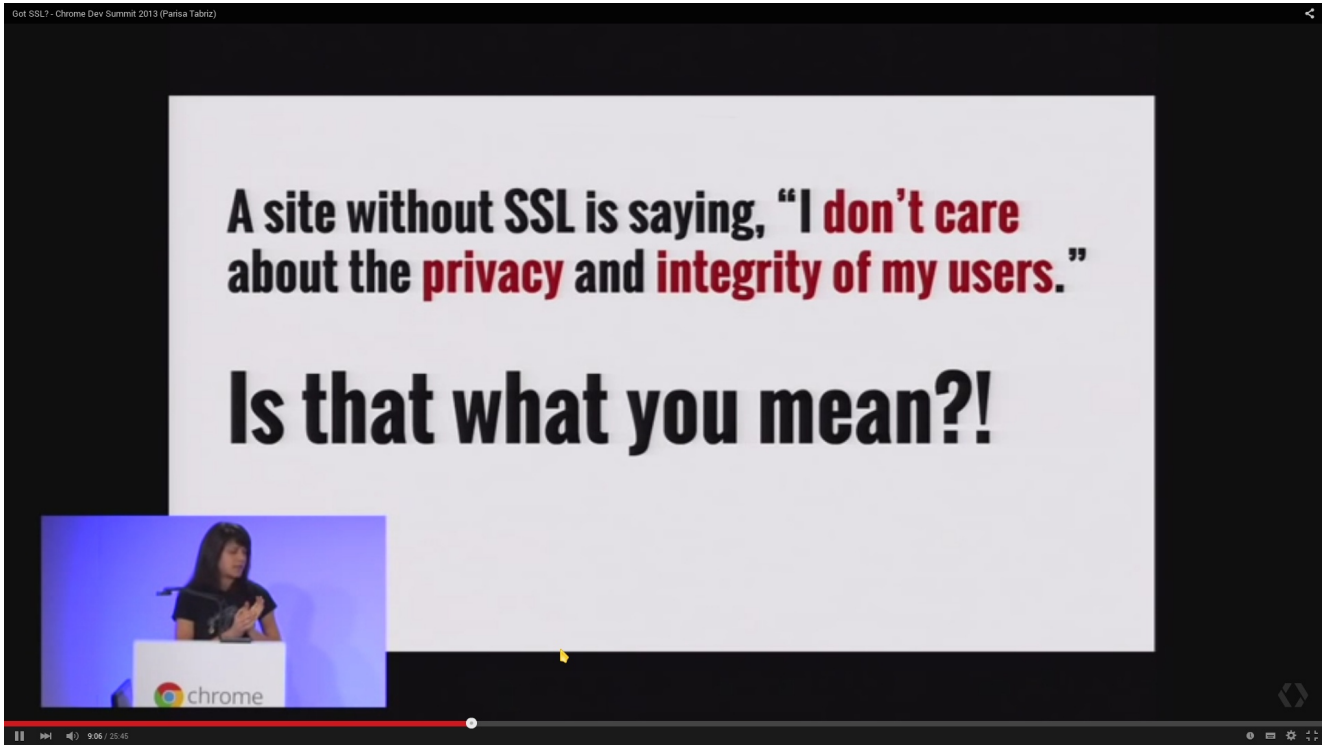
nottalking:about



(Personally taken)

talking:about

- **HTTPS**
  - 2013: Google @ Chrome Dev Summit



Got SSL? - Chrome Dev Summit 2013 (Parisa Tabriz) https://www.youtube.com/watch?v=sJ8EX61fFWQ

talking:about

- **HTTPS**
  - 2013: Google @ Chrome Dev Summit
  - 8/2014: Google's power

Google | Webmaster Central Blog

HTTPS as a ranking signal

For these reasons, over the past few months we've been running tests taking into account whether sites use secure, encrypted connections as a signal in our search ranking algorithms. We've seen positive results, so we're starting to use HTTPS as a ranking signal. For now it's only a very lightweight signal — affecting fewer than 1% of global queries, and carrying less weight than other signals such as high-quality content — while we give webmasters time to switch to HTTPS. But over time, we may decide to strengthen it, because we'd like to encourage all website owners to switch from HTTP to HTTPS to keep everyone safe on the web.

Safe? From what??

http://googlewebmastercentral.blogspot.com.au/2014/08/https-as-ranking-signal.html

talking:about

- **HTTPS**
  - 2013: Google @ Chrome Dev Summit
  - 8/2014: Google's power
  - 6/2015: „HTTPS everywhere for IETF“

https://www.chromium.org/Home/chromium-security/marking-http-as-non-secure

talking:about

- “The IETF has recognised that the act of accessing public information required for routine tasks can be **privacy sensitive** and can benefit from using a **confidentiality service,** such as is provided by TLS. [BCP188] The IETF in its normal operation publishes a significant volume of public data (such as Internet-drafts), **to which this argument applies**.”

talking:about

- „HTTPS everywhere for IETF“

Tony Hain: *While I don't object to making the IETF content available via https/tls, this proposed statement reads as political knee-jerk BS that is both unnecessary and uncalled for. What the statement MUST focus on is 'data integrity', and SHOULD NOT stop to fear mongering over 'privacy'. "It is public data ..."*

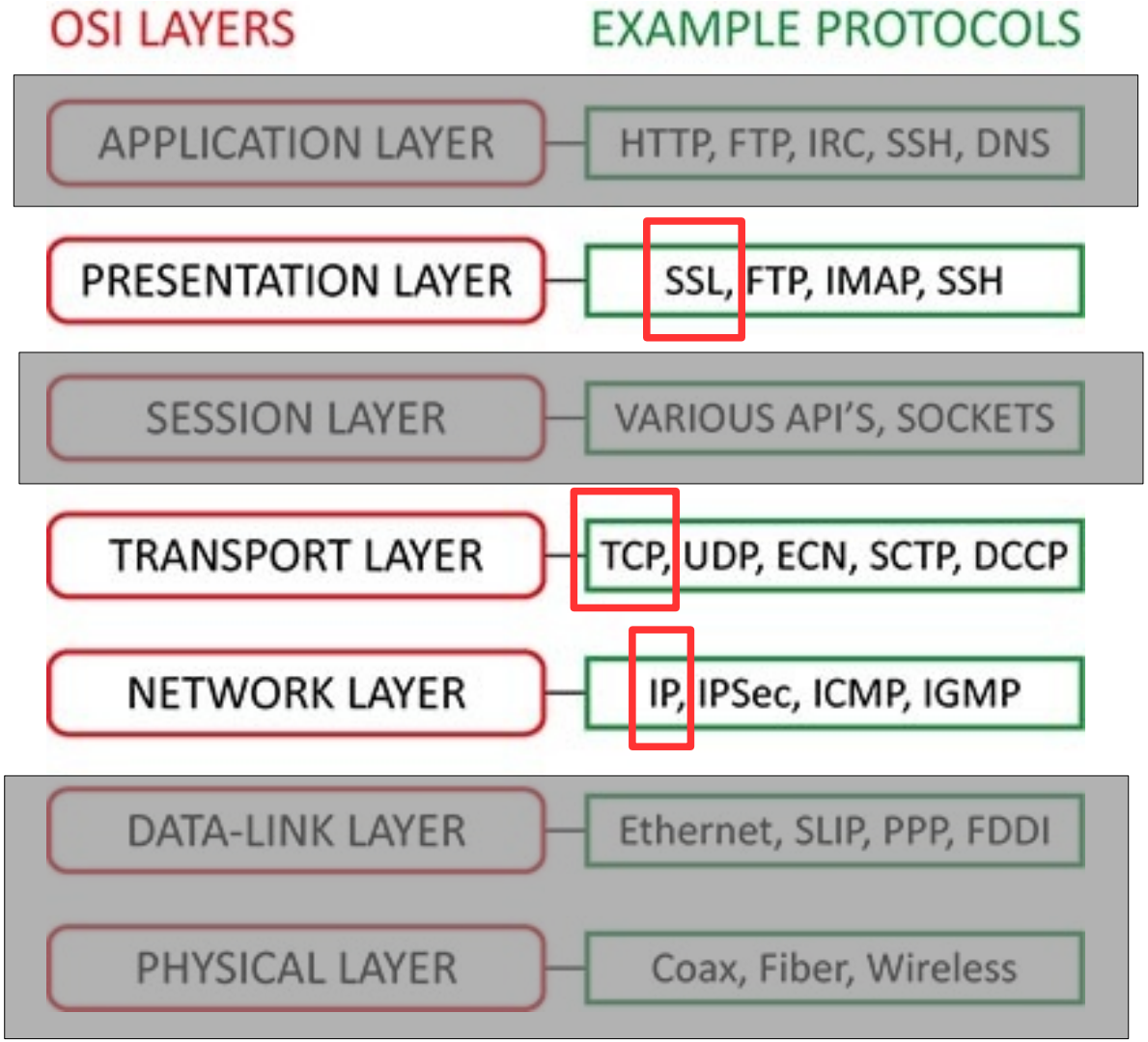
talking:about

- „HTTPS everywhere for IETF“

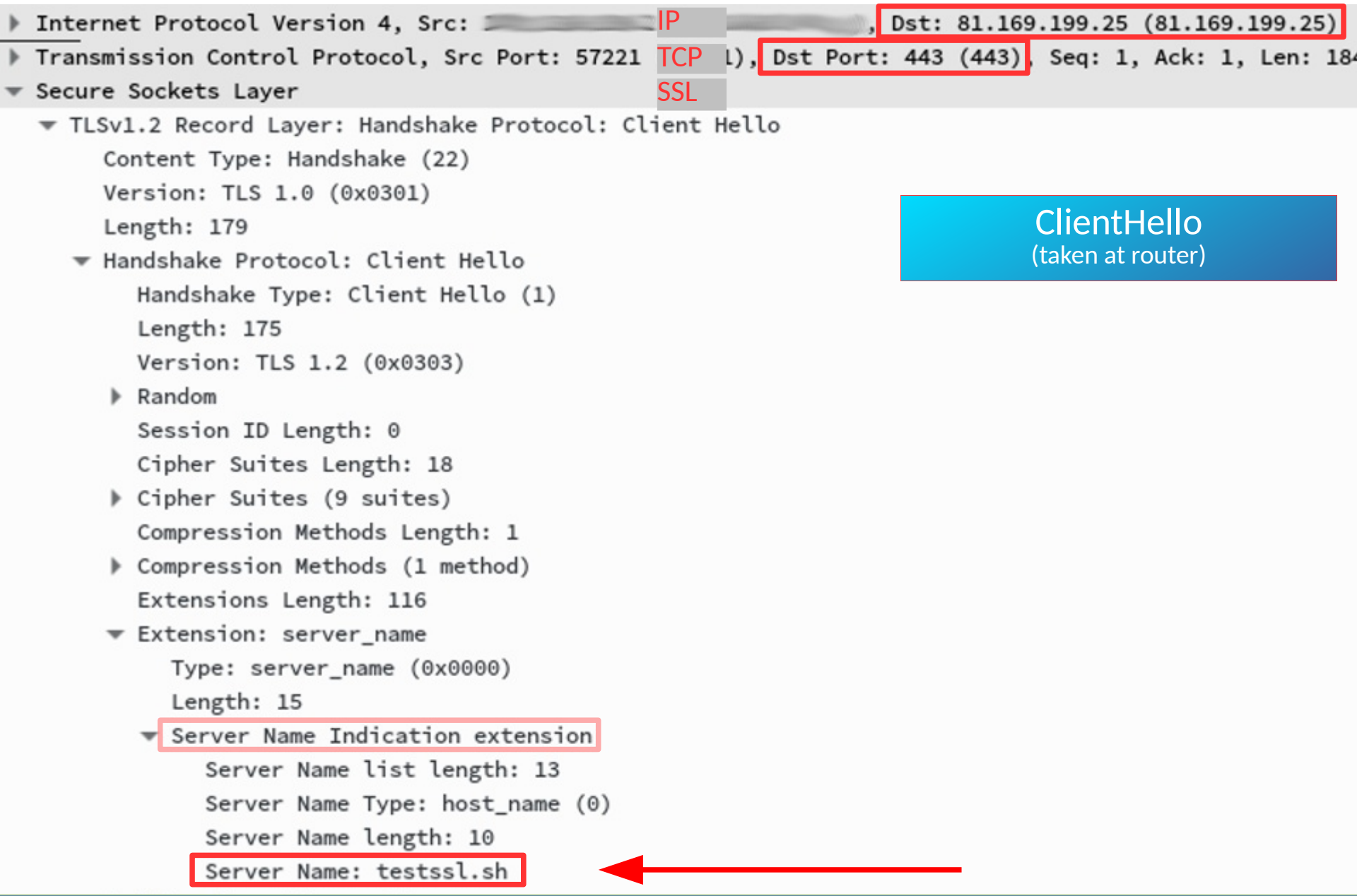
Tony Hain: *While I don't object to making the IETF content available via https/tls, this proposed statement reads as political knee-jerk BS that is both unnecessary and uncalled for. What the statement MUST focus on is 'data integrity', and SHOULD NOT stop to fear mongering over 'privacy'. "It is public data ..."*

Roy Fielding: *Browsers don't send singular messages containing anonymous information. They send a complex sequence of messages to multiple parties with an interaction pattern and communication state.*

network:layers

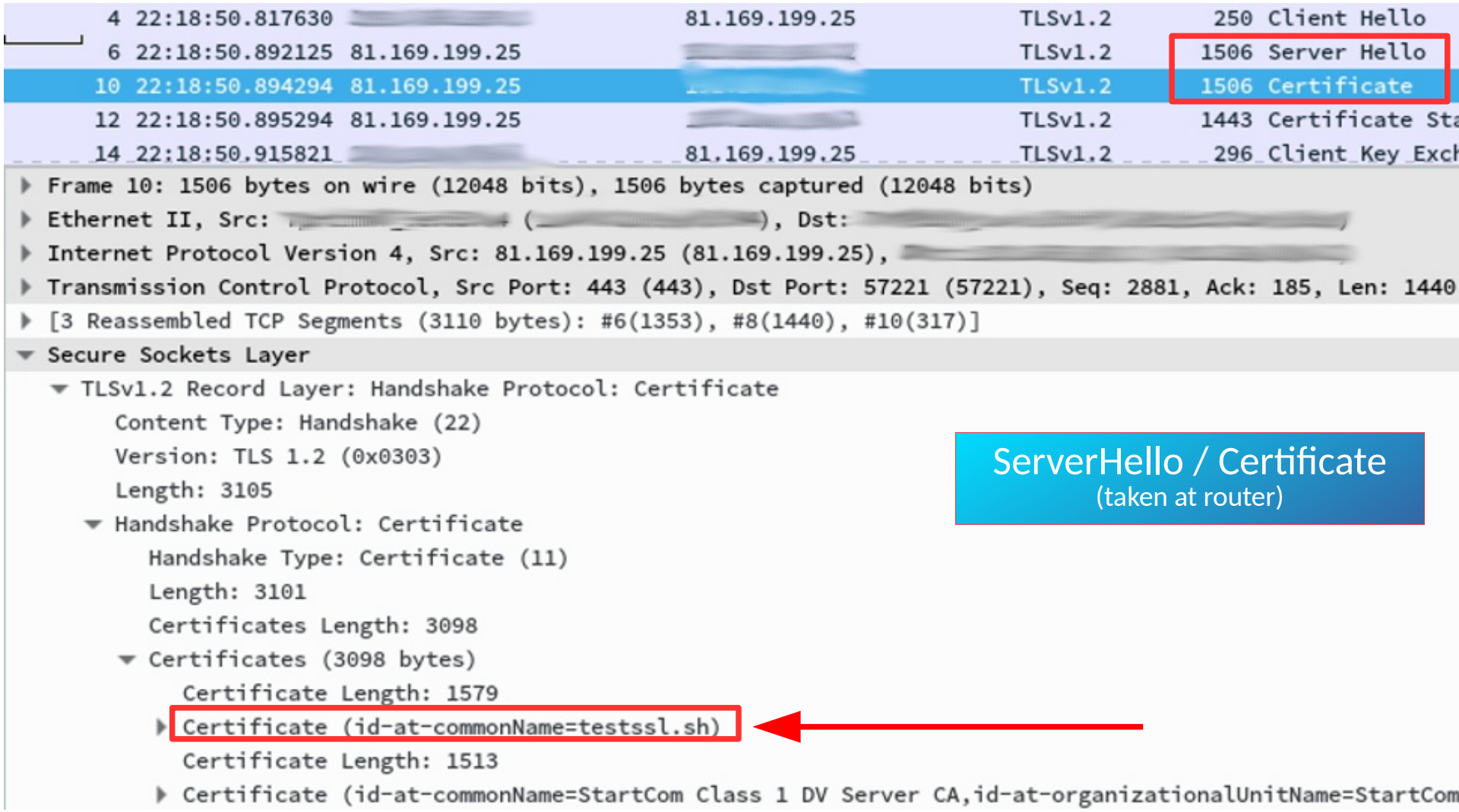


layers:{IP,TCP,TLS}



ClientHello
(taken at router)

layers:{IP,TCP,TLS}



ServerHello / Certificate
(taken at router)

browser:before

- **Not the first obvious request**
  - DNS (clear text)

Source	Destination	Protocol	Length	Info
[redacted]	[redacted]	DNS	70	Standard query 0x36db A testssl.sh
[redacted]	[redacted]	DNS	221	Standard query response 0x36db A 81.169.199.25
[redacted]	[redacted]	DNS	70	Standard query 0xc37d AAAA testssl.sh
[redacted]	[redacted]	DNS	121	Standard query response 0xc37d

  - 3rd party involvement!

browser:before

- Not the first obvious request
  - DNS
  - OCSP (if not stapled)

http://ocsp.godaddy.com/

```
Host: ocsp.godaddy.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:47.0) [..]
Accept: text/html,application/xhtml+xml,application/xml [..]
Accept-Language: en-US,en
Accept-Encoding: gzip, deflate
Content-Length: 75
Content-Type: application/ocsp-request
Connection: keep-alive

<DER encoded OCSPRequest>
```

browser:before

- Not the first obvious request
  - DNS
  - OCSP (if not stapled)
    - 3rd party involvement!
    - RFC 6960
      - 4.1.1. ASN.1 Specification of the OCSP Request

```
CertID  ::=  SEQUENCE {
   hashAlgorithm        AlgorithmIdentifier,
   issuerNameHash       OCTET STRING, -- Hash of issuer's DN
   issuerKeyHash        OCTET STRING, -- Hash of issuer's public key
   serialNumber         CertificateSerialNumber }
```

browser:TLS layer

ClientHellos
(sniffed from router)

Firefox

```
Handshake Protocol: Client Hello
  Handshake Type: Client Hello (1)
  Length: 185
  Version: TLS 1.2 (0x0303)
▸ Random
  Session ID Length: 0
  Cipher Suites Length: 26
▸ Cipher Suites (13 suites)
  Compression Methods Length: 1
▸ Compression Methods (1 method)
  Extensions Length: 118
▸ Extension: server_name
▸ Extension: Unknown 23
▸ Extension: renegotiation_info
▸ Extension: elliptic_curves
▸ Extension: ec_point_formats
▸ Extension: SessionTicket TLS
▸ Extension: next_protocol_negotiation
▸ Extension: Application Layer Protocol Ne
▸ Extension: status_request
▸ Extension: signature_algorithms
```

Chrome

```
Handshake Protocol: Client Hello
  Handshake Type: Client Hello (1)
  Length: 192
  Version: TLS 1.2 (0x0303)
▸ Random
  Session ID Length: 0
  Cipher Suites Length: 34
▸ Cipher Suites (17 suites)
  Compression Methods Length: 1
▸ Compression Methods (1 method)
  Extensions Length: 117
▸ Extension: renegotiation_info
▸ Extension: server_name
▸ Extension: Unknown 23
▸ Extension: SessionTicket TLS
▸ Extension: signature_algorithms
▸ Extension: status_request
▸ Extension: signed_certificate_timestamp
▸ Extension: Application Layer Protocol Negotiatio
▸ Extension: Unknown 30032
▸ Extension: ec_point_formats
▸ Extension: elliptic_curves
▸ Extension: Unknown 24
```

browser:TLS layer

ClientHellos
(sniffed from router)

Chrome 51

```
Cipher Suites (17 suites)
  Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
  Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
  Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
  Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
  Cipher Suite: Unknown (0xcca9)
  Cipher Suite: Unknown (0xcca8)
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcc14)
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcc13)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
```

Firefox 47

```
Cipher Suites (13 suites)
  Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
  Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
  Cipher Suite: Unknown (0xcca9)
  Cipher Suite: Unknown (0xcca8)
  Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
  Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
  Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
  Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
  Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
  Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
  Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
  Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
  Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
```

```
Elliptic curves (3 curves)
    Elliptic curve: secp256r1 (0x0017)
    Elliptic curve: secp384r1 (0x0018)
    Elliptic curve: secp521r1 (0x0019)
```

```
Extension: elliptic_curves
  Type: elliptic_curves (0x000a)
  Length: 8
  Elliptic Curves Length: 6
  Elliptic curves (3 curves)
    Elliptic curve: Unknown (0x001d)
    Elliptic curve: secp256r1 (0x0017)
    Elliptic curve: secp384r1 (0x0018)
```

browser:TLS layer

ClientHellos
(sniffed from router)

Firefox 47

```
Cipher Suites (13 suites)
  Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
  Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
  Cipher Suite: Unknown (0xcca9)
  Cipher Suite: Unknown (0xcca8)
  Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
  Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
  Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
  Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
  Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
  Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
  Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
  Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
  Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
```

Firefox 50

```
14 suites)
 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
 Unknown (0xcca9)
 Unknown (0xcca8)
 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
 TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
 TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
```

browser:TLS layer

- **Browser TLS fingerprinting on the wire**
  - SSLlabs Client API (mod_sslhaf)
    https://api.dev.ssllabs.com/api/v3/getClients
  - 

    github.com/LeeBrotherston/tls-fingerprinting/

    https://blog.squarelemon.com/tls-fingerprinting/

```
prompt~:$ tls-fingerprinting/fingerprintls./fingerprintls -i <NW IF>
```

browser:TLS layer

- **Browser TLS fingerprinting on the wire**
  - Time skew (past, kind of….)

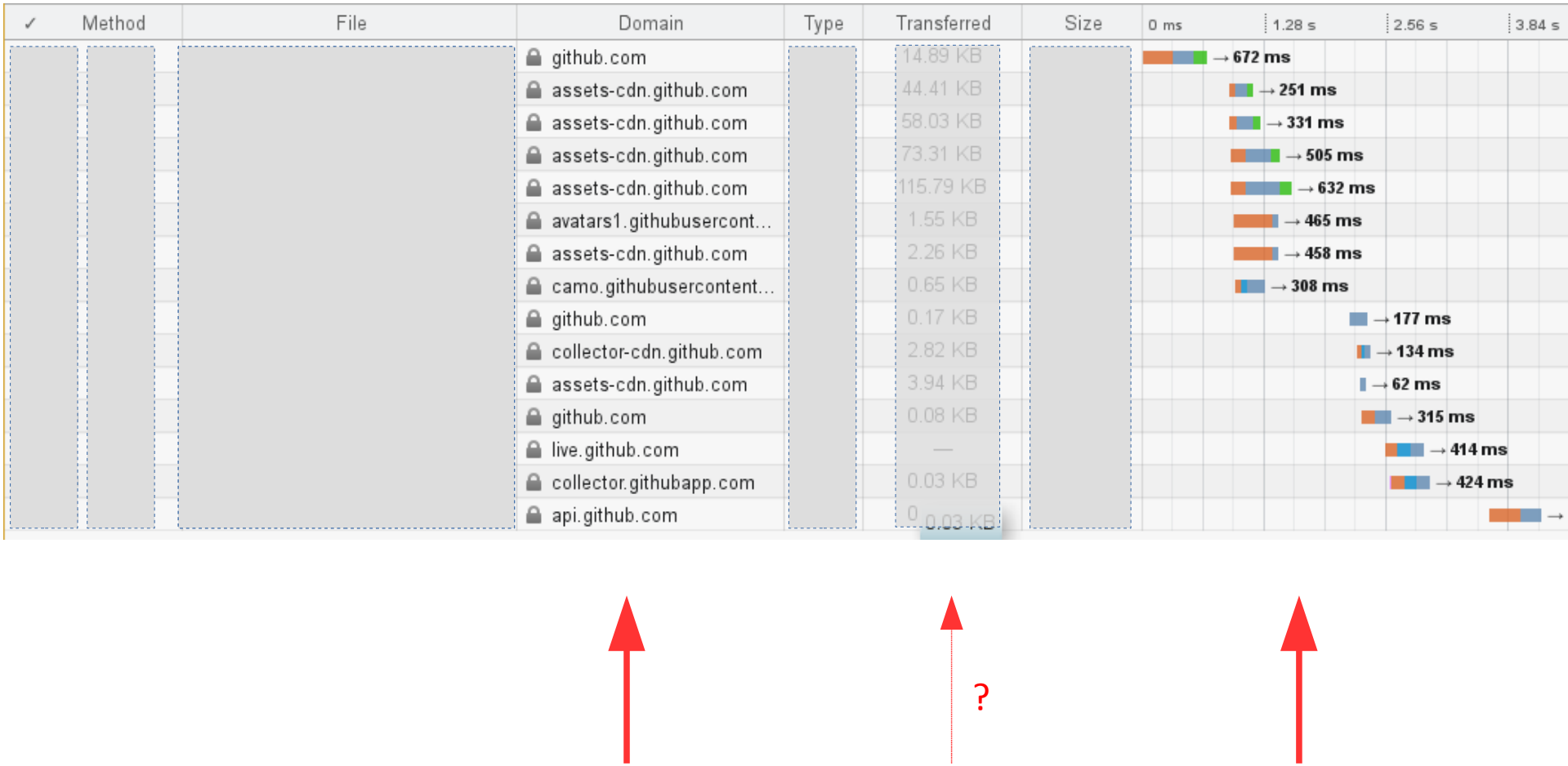
```
▾ Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 170
    Version: TLS 1.2 (0x0303)
  ▾ Random
      GMT Unix Time: Jun 26, 2016 15:22:24.000000000 CEST
      Random Bytes: 90f7cbf829e58feff7c534656155a7507db13e39543164db...
    Session ID Length: 0
    Cipher Suites Length: 52
  ▸ Cipher Suites (26 suites)
```

gmt_unix_time [ms]

```
▼ Random
      gmt_unix_time: Sep 12, 2089 03:04:57.000000000 CEST
      random_bytes: 5dd1e62fa2d5340e8384a06fb2dbef076ba0966cc34589c7...
```

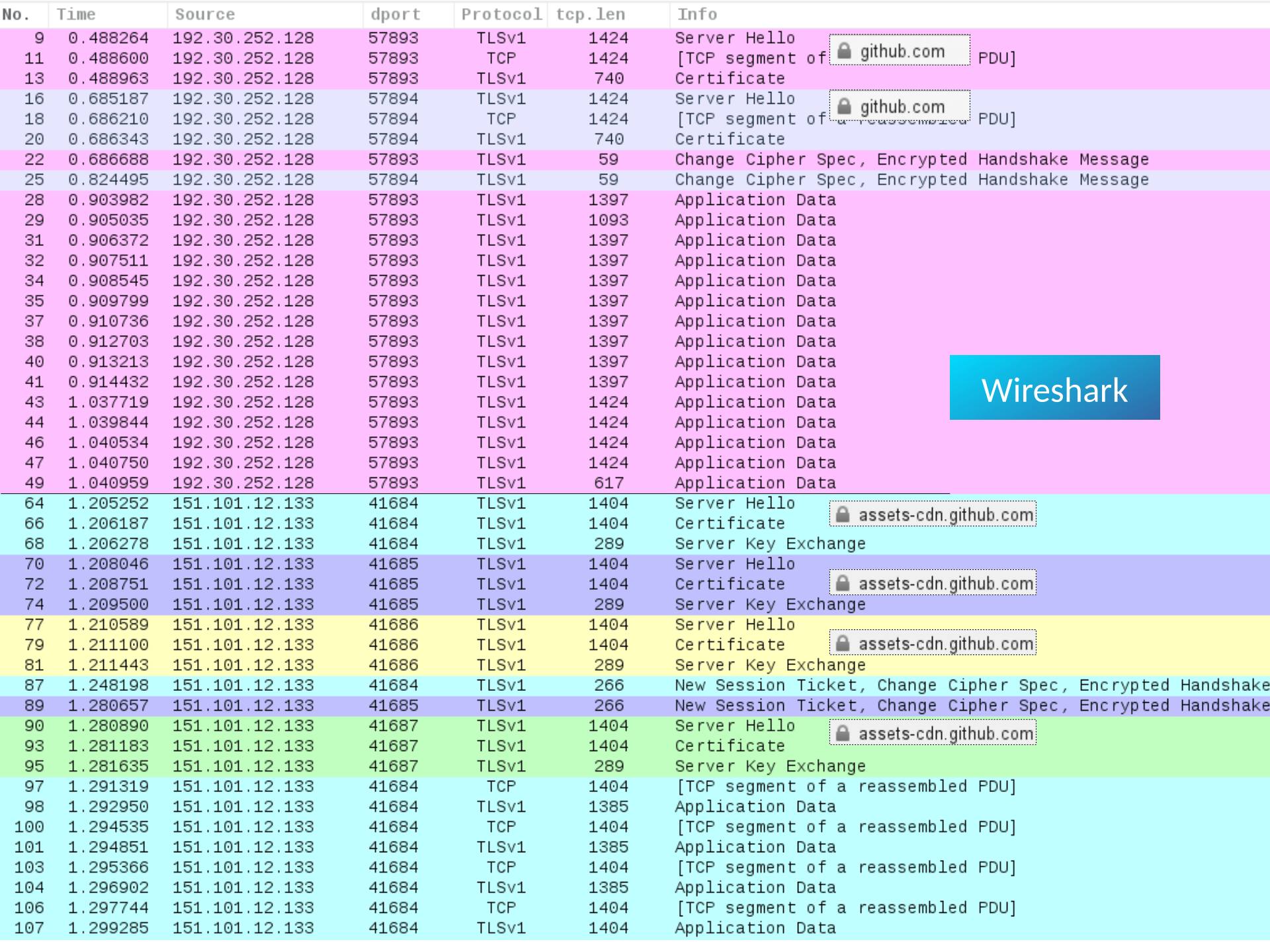
browser:getting worse

- **At the console**



No.	Time	Source	Protocol	tcp.len	Info
9	0.488264	192.30.252.128	TLSv1	1424	Server Hello
11	0.488600	192.30.252.128	TCP	1424	[TCP segment of a reassembled PDU]
13	0.488963	192.30.252.128	TLSv1	740	Certificate
16	0.685187	192.30.252.128	TLSv1	1424	Server Hello
18	0.686210	192.30.252.128	TCP	1424	[TCP segment of a reassembled PDU]
20	0.686343	192.30.252.128	TLSv1	740	Certificate
22	0.686688	192.30.252.128	TLSv1	59	Change Cipher Spec, Encrypted Handshake Message
25	0.824495	192.30.252.128	TLSv1	59	Change Cipher Spec, Encrypted Handshake Message
26	0.829847	192.30.252.128	TCP	0	https→57893 [ACK] Seq=3648 Ack=699 Win=18 Len=0 TSval=1703186353 TSec
28	0.903982	192.30.252.128	TLSv1	1397	Application Data
29	0.905035	192.30.252.128	TLSv1	1093	Application Data
31	0.906372	192.30.252.128	TLSv1	1397	Application Data
32	0.907511	192.30.252.128	TLSv1	1397	Application Data
34	0.908545	192.30.252.128	TLSv1	1397	Application Data
35	0.909799	192.30.252.128	TLSv1	1397	Application Data
37	0.910736	192.30.252.128	TLSv1	1397	Application Data
38	0.912703	192.30.252.128	TLSv1	1397	Application Data
40	0.913213	192.30.252.128	TLSv1	1397	Application Data
41	0.914432	192.30.252.128	TLSv1	1397	Application Data
43	1.037719	192.30.252.128	TLSv1	1424	Application Data
44	1.039844	192.30.252.128	TLSv1	1424	Application Data
46	1.040534	192.30.252.128	TLSv1	1424	Application Data
47	1.040750	192.30.252.128	TLSv1	1424	Application Data
49	1.040959	192.30.252.128	TLSv1	617	Application Data
64	1.205252	151.101.12.133	TLSv1	1404	Server Hello
66	1.206187	151.101.12.133	TLSv1	1404	Certificate
68	1.206278	151.101.12.133	TLSv1	289	Server Key Exchange
70	1.208046	151.101.12.133	TLSv1	1404	Server Hello
72	1.208751	151.101.12.133	TLSv1	1404	Certificate
74	1.209500	151.101.12.133	TLSv1	289	Server Key Exchange
77	1.210589	151.101.12.133	TLSv1	1404	Server Hello
79	1.211100	151.101.12.133	TLSv1	1404	Certificate
81	1.211443	151.101.12.133	TLSv1	289	Server Key Exchange
87	1.248198	151.101.12.133	TLSv1	266	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
89	1.280657	151.101.12.133	TLSv1	266	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
90	1.280890	151.101.12.133	TLSv1	1404	Server Hello
93	1.281183	151.101.12.133	TLSv1	1404	Certificate
95	1.281635	151.101.12.133	TLSv1	289	Server Key Exchange
97	1.291319	151.101.12.133	TCP	1404	[TCP segment of a reassembled PDU]
98	1.292950	151.101.12.133	TLSv1	1385	Application Data
100	1.294535	151.101.12.133	TCP	1404	[TCP segment of a reassembled PDU]
101	1.294851	151.101.12.133	TLSv1	1385	Application Data
103	1.295366	151.101.12.133	TCP	1404	[TCP segment of a reassembled PDU]
104	1.296902	151.101.12.133	TLSv1	1385	Application Data
106	1.297744	151.101.12.133	TCP	1404	[TCP segment of a reassembled PDU]
107	1.299285	151.101.12.133	TLSv1	1404	Application Data

No.	Time	Source	dport	Protocol	tcp.len	Info
9	0.488264	192.30.252.128	57893	TLSv1	1424	Server Hello
11	0.488600	192.30.252.128	57893	TCP	1424	[TCP segment of github.com PDU]
13	0.488963	192.30.252.128	57893	TLSv1	740	Certificate
16	0.685187	192.30.252.128	57894	TLSv1	1424	Server Hello
18	0.686210	192.30.252.128	57894	TCP	1424	[TCP segment of github.com PDU]
20	0.686343	192.30.252.128	57894	TLSv1	740	Certificate
22	0.686688	192.30.252.128	57893	TLSv1	59	Change Cipher Spec, Encrypted Handshake Message
25	0.824495	192.30.252.128	57894	TLSv1	59	Change Cipher Spec, Encrypted Handshake Message
28	0.903982	192.30.252.128	57893	TLSv1	1397	Application Data
29	0.905035	192.30.252.128	57893	TLSv1	1093	Application Data
31	0.906372	192.30.252.128	57893	TLSv1	1397	Application Data
32	0.907511	192.30.252.128	57893	TLSv1	1397	Application Data
34	0.908545	192.30.252.128	57893	TLSv1	1397	Application Data
35	0.909799	192.30.252.128	57893	TLSv1	1397	Application Data
37	0.910736	192.30.252.128	57893	TLSv1	1397	Application Data
38	0.912703	192.30.252.128	57893	TLSv1	1397	Application Data
40	0.913213	192.30.252.128	57893	TLSv1	1397	Application Data
41	0.914432	192.30.252.128	57893	TLSv1	1397	Application Data
43	1.037719	192.30.252.128	57893	TLSv1	1424	Application Data
44	1.039844	192.30.252.128	57893	TLSv1	1424	Application Data
46	1.040534	192.30.252.128	57893	TLSv1	1424	Application Data
47	1.040750	192.30.252.128	57893	TLSv1	1424	Application Data
49	1.040959	192.30.252.128	57893	TLSv1	617	Application Data
64	1.205252	151.101.12.133	41684	TLSv1	1404	Server Hello
66	1.206187	151.101.12.133	41684	TLSv1	1404	Certificate
68	1.206278	151.101.12.133	41684	TLSv1	289	Server Key Exchange
70	1.208046	151.101.12.133	41685	TLSv1	1404	Server Hello
72	1.208751	151.101.12.133	41685	TLSv1	1404	Certificate
74	1.209500	151.101.12.133	41685	TLSv1	289	Server Key Exchange
77	1.210589	151.101.12.133	41686	TLSv1	1404	Server Hello
79	1.211100	151.101.12.133	41686	TLSv1	1404	Certificate
81	1.211443	151.101.12.133	41686	TLSv1	289	Server Key Exchange
87	1.248198	151.101.12.133	41684	TLSv1	266	New Session Ticket, Change Cipher Spec, Encrypted Handshake
89	1.280657	151.101.12.133	41685	TLSv1	266	New Session Ticket, Change Cipher Spec, Encrypted Handshake
90	1.280890	151.101.12.133	41687	TLSv1	1404	Server Hello
93	1.281183	151.101.12.133	41687	TLSv1	1404	Certificate
95	1.281635	151.101.12.133	41687	TLSv1	289	Server Key Exchange
97	1.291319	151.101.12.133	41684	TCP	1404	[TCP segment of a reassembled PDU]
98	1.292950	151.101.12.133	41684	TLSv1	1385	Application Data
100	1.294535	151.101.12.133	41684	TCP	1404	[TCP segment of a reassembled PDU]
101	1.294851	151.101.12.133	41684	TLSv1	1385	Application Data
103	1.295366	151.101.12.133	41684	TCP	1404	[TCP segment of a reassembled PDU]
104	1.296902	151.101.12.133	41684	TLSv1	1385	Application Data
106	1.297744	151.101.12.133	41684	TCP	1404	[TCP segment of a reassembled PDU]
107	1.299285	151.101.12.133	41684	TLSv1	1404	Application Data



browser:getting worse

- **Network difficult:**
  - length not visible (MTU)
    - HTTP/1.1: pipelining
      - But: source port TCP
    - Keepalive
    - 304
  - SSL session ID / TLS session tickets

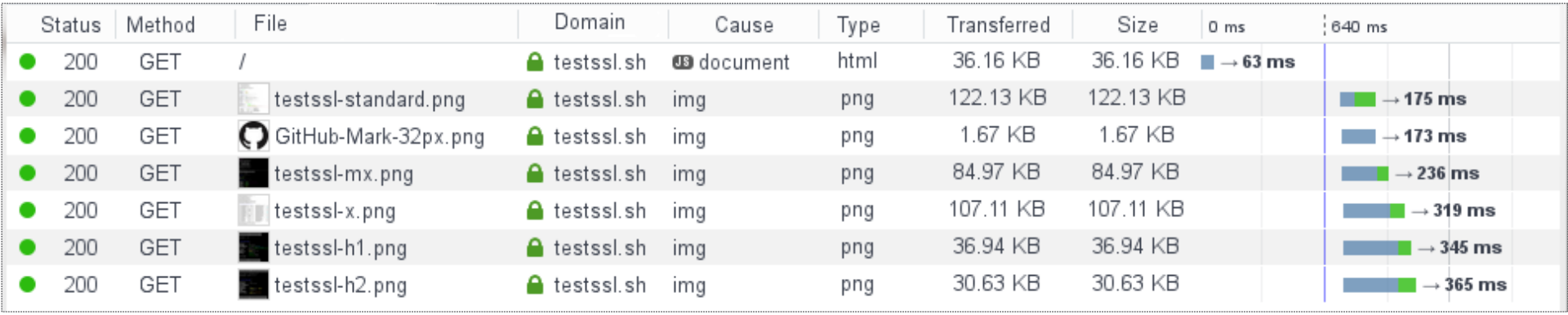
Wireshark

browser:slightlybetter

- **HTTP/2**
  - Not that widespread yet (no github e.g.)
    - Internet traffic: 11.1% in 12/2016 (w3techs.com)
    - Per host count (trends.builtwith.com) 12/2016
      - 345k (< 0.1%)
      - 1652 (0.2% of top 1 mio)

browser:slightlybetter

- **HTTP/2!**
  - Also privacy-wise: Change for the better



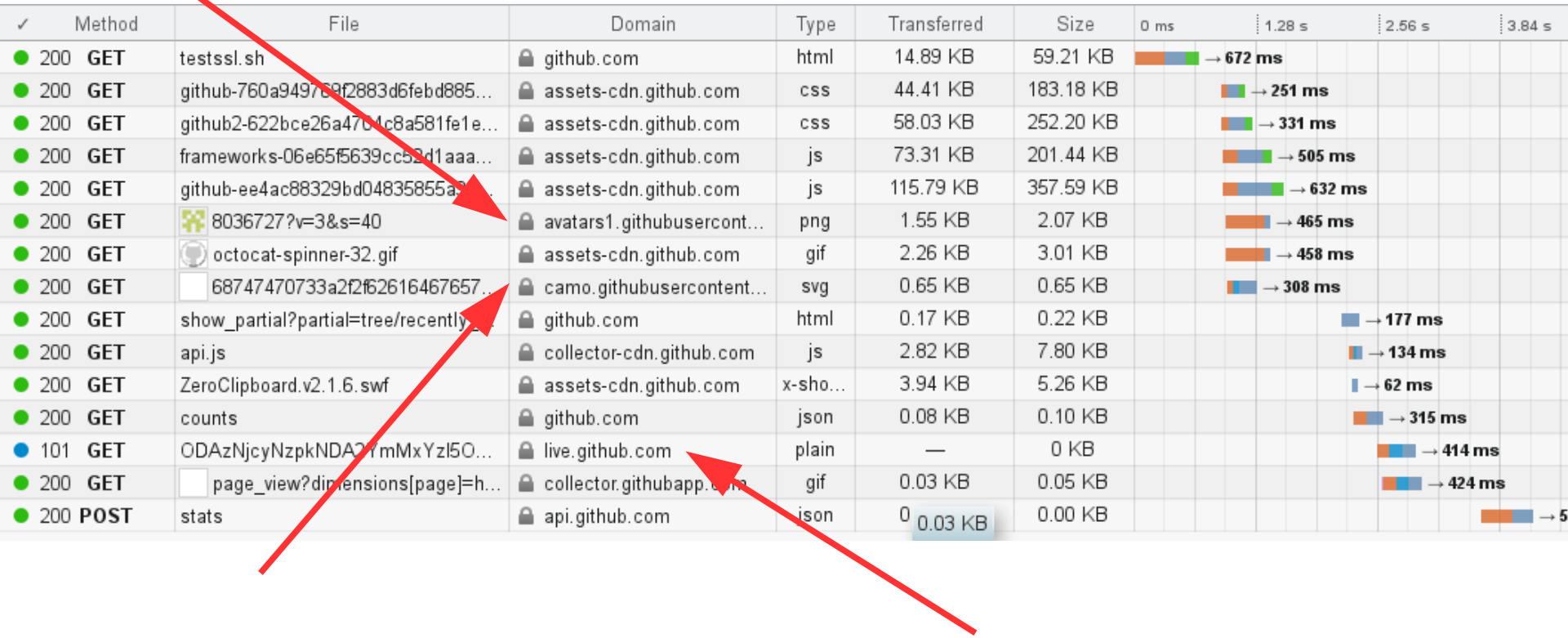
Status	Method	File	Domain	Cause	Type	Transferred	Size	0 ms	640 ms
200	GET	/	testssl.sh	document	html	36.16 KB	36.16 KB	→ 63 ms	
200	GET	testssl-standard.png	testssl.sh	img	png	122.13 KB	122.13 KB		→ 175 ms
200	GET	GitHub-Mark-32px.png	testssl.sh	img	png	1.67 KB	1.67 KB		→ 173 ms
200	GET	testssl-mx.png	testssl.sh	img	png	84.97 KB	84.97 KB		→ 236 ms
200	GET	testssl-x.png	testssl.sh	img	png	107.11 KB	107.11 KB		→ 319 ms
200	GET	testssl-h1.png	testssl.sh	img	png	36.94 KB	36.94 KB		→ 345 ms
200	GET	testssl-h2.png	testssl.sh	img	png	30.63 KB	30.63 KB		→ 365 ms

No.	Time	Source	Destination	dport	Protocol	Length	Info
6	0.105836000	81.169.199.25	192.168.1.5	50194	TLSv1.2	1506	Server Hello
8	0.108323000	81.169.199.25	192.168.1.5	50194	TCP	1506	[TCP segment of a reassembled PDU]
10	0.109915000	81.169.199.25	192.168.1.5	50194	TLSv1.2	2811	Certificate
14	0.148408000	81.169.199.25	192.168.1.5	50194	TCP	66	443→50194 [ACK] Seq=5626 Ack=346 Win=15552 Len=0 TSval=127859
15	0.149913000	81.169.199.25	192.168.1.5	50194	TLSv1.2	324	New Session Ticket, Change Cipher Spec, Encrypted Handshake M
16	0.149925000	81.169.199.25	192.168.1.5	50194	TLSv1.2	135	Application Data
19	0.150438000	81.169.199.25	192.168.1.5	50194	TLSv1.2	104	Application Data
21	0.188334000	81.169.199.25	192.168.1.5	50194	TCP	66	443→50194 [ACK] Seq=5991 Ack=803 Win=17696 Len=0 TSval=127859
22	0.215167000	81.169.199.25	192.168.1.5	50194	TCP	1506	[TCP segment of a reassembled PDU]
23	0.215896000	81.169.199.25	192.168.1.5	50194	TCP	2946	[TCP segment of a reassembled PDU]
25	0.216602000	81.169.199.25	192.168.1.5	50194	TCP	1506	[TCP segment of a reassembled PDU]
26	0.217551000	81.169.199.25	192.168.1.5	50194	TCP	1506	[TCP segment of a reassembled PDU]
28	0.219914000	81.169.199.25	192.168.1.5	50194	TLSv1.2	1445	Application Data
29	0.221871000	81.169.199.25	192.168.1.5	50194	TCP	1506	[TCP segment of a reassembled PDU]
31	0.226756000	81.169.199.25	192.168.1.5	50194	TCP	2946	[TCP segment of a reassembled PDU]
33	0.227672000	81.169.199.25	192.168.1.5	50194	TCP	1506	[TCP segment of a reassembled PDU]
34	0.249377000	81.169.199.25	192.168.1.5	50194	TCP	1506	[TCP segment of a reassembled PDU]
36	0.252546000	81.169.199.25	192.168.1.5	50194	TLSv1.2	2946	Application Data
38	0.255128000	81.169.199.25	192.168.1.5	50194	TCP	1506	[TCP segment of a reassembled PDU]
39	0.256251000	81.169.199.25	192.168.1.5	50194	TCP	1506	[TCP segment of a reassembled PDU]
41	0.257079000	81.169.199.25	192.168.1.5	50194	TCP	1506	[TCP segment of a reassembled PDU]
42	0.258202000	81.169.199.25	192.168.1.5	50194	TCP	1506	[TCP segment of a reassembled PDU]
44	0.259621000	81.169.199.25	192.168.1.5	50194	TLSv1.2	1506	Application Data
45	0.260671000	81.169.199.25	192.168.1.5	50194	TCP	1506	[TCP segment of a reassembled PDU]
47	0.261578000	81.169.199.25	192.168.1.5	50194	TCP	1506	[TCP segment of a reassembled PDU]
48	0.282169000	81.169.199.25	192.168.1.5	50194	TCP	1506	[TCP segment of a reassembled PDU]
50	0.283281000	81.169.199.25	192.168.1.5	50194	TCP	2946	[TCP segment of a reassembled PDU]
52	0.284229000	81.169.199.25	192.168.1.5	50194	TLSv1.2	1506	Application Data
53	0.285369000	81.169.199.25	192.168.1.5	50194	TCP	1506	[TCP segment of a reassembled PDU]
55	0.286245000	81.169.199.25	192.168.1.5	50194	TCP	1506	[TCP segment of a reassembled PDU]
56	0.286915000	81.169.199.25	192.168.1.5	50194	TLSv1.2	356	Application Data
64	0.794699000	81.169.199.25	192.168.1.5	50194	TCP	1506	[TCP segment of a reassembled PDU]
65	0.795925000	81.169.199.25	192.168.1.5	50194	TCP	1506	[TCP segment of a reassembled PDU]
67	0.797563000	81.169.199.25	192.168.1.5	50194	TCP	1506	[TCP segment of a reassembled PDU]
68	0.798478000	81.169.199.25	192.168.1.5	50194	TCP	1506	[TCP segment of a reassembled PDU]
70	0.799642000	81.169.199.25	192.168.1.5	50194	TCP	1506	[TCP segment of a reassembled PDU]
71	0.800642000	81.169.199.25	192.168.1.5	50194	TCP	1506	[TCP segment of a reassembled PDU]
73	0.802724000	81.169.199.25	192.168.1.5	50194	TCP	1506	[TCP segment of a reassembled PDU]
74	0.803486000	81.169.199.25	192.168.1.5	50194	TCP	1506	[TCP segment of a reassembled PDU]
76	0.804361000	81.169.199.25	192.168.1.5	50194	TCP	1506	[TCP segment of a reassembled PDU]
77	0.805140000	81.169.199.25	192.168.1.5	50194	TCP	1506	[TCP segment of a reassembled PDU]
79	0.806218000	81.169.199.25	192.168.1.5	50194	TCP	1506	[TCP segment of a reassembled PDU]
80	0.806986000	81.169.199.25	192.168.1.5	50194	TCP	66	443→50194 [ACK] Seq=59500 Ack=1054 Win=17696 Len=0 TSval=1278
81	0.807785000	81.169.199.25	192.168.1.5	50194	TCP	66	443→50194 [ACK] Seq=59500 Ack=1211 Win=17696 Len=0 TSval=1278
82	0.830459000	81.169.199.25	192.168.1.5	50194	TLSv1.2	1506	Application Data
84	0.831816000	81.169.199.25	192.168.1.5	50194	TCP	1506	[TCP segment of a reassembled PDU]
85	0.832666000	81.169.199.25	192.168.1.5	50194	TCP	1506	[TCP segment of a reassembled PDU]
87	0.833802000	81.169.199.25	192.168.1.5	50194	TCP	1506	[TCP segment of a reassembled PDU]
88	0.834825000	81.169.199.25	192.168.1.5	50194	TCP	1506	[TCP segment of a reassembled PDU]
90	0.835746000	81.169.199.25	192.168.1.5	50194	TCP	1506	[TCP segment of a reassembled PDU]
91	0.838552000	81.169.199.25	192.168.1.5	50194	TCP	1506	[TCP segment of a reassembled PDU]

Wireshark
testssl.sh

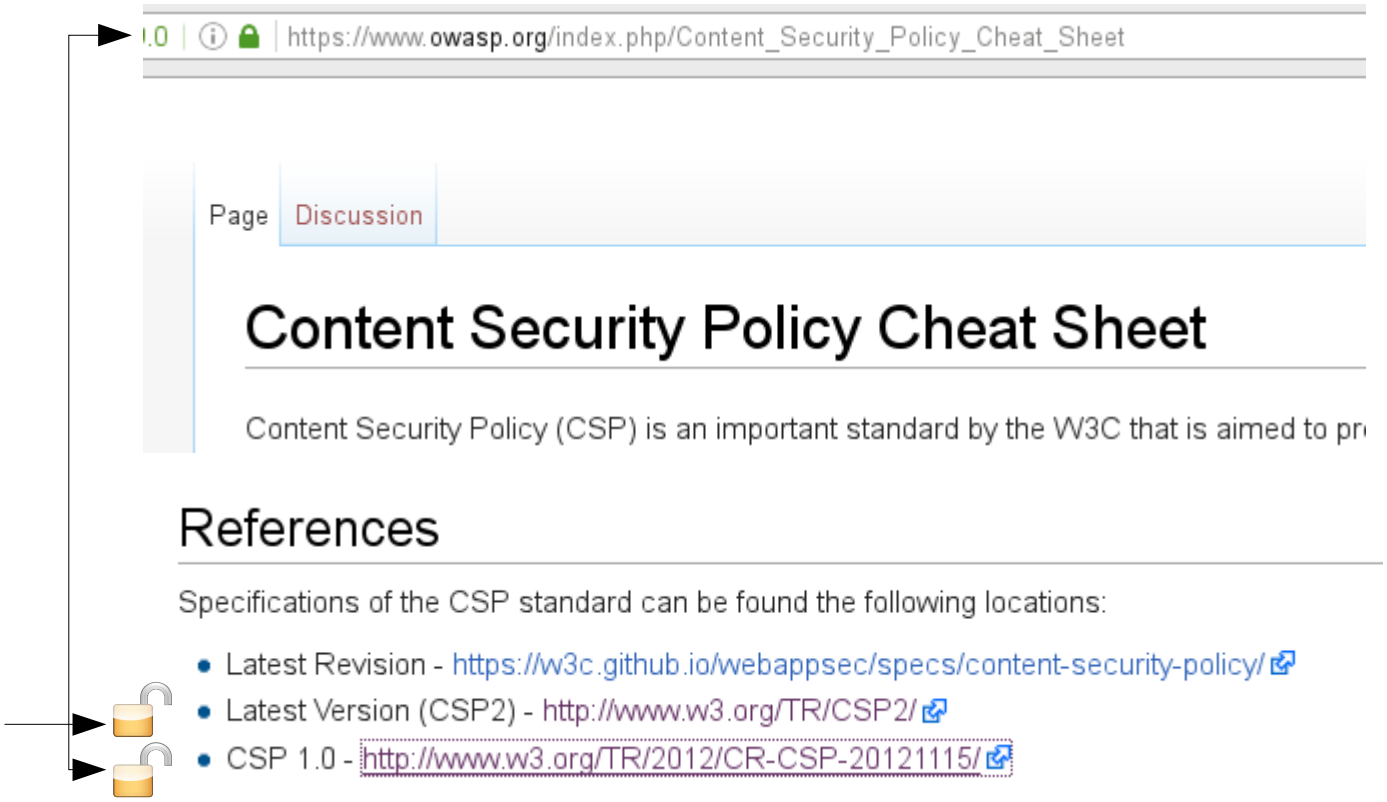
browser:TLS layer

- **connection to 3rd parties (back to HTTP/1.1)**



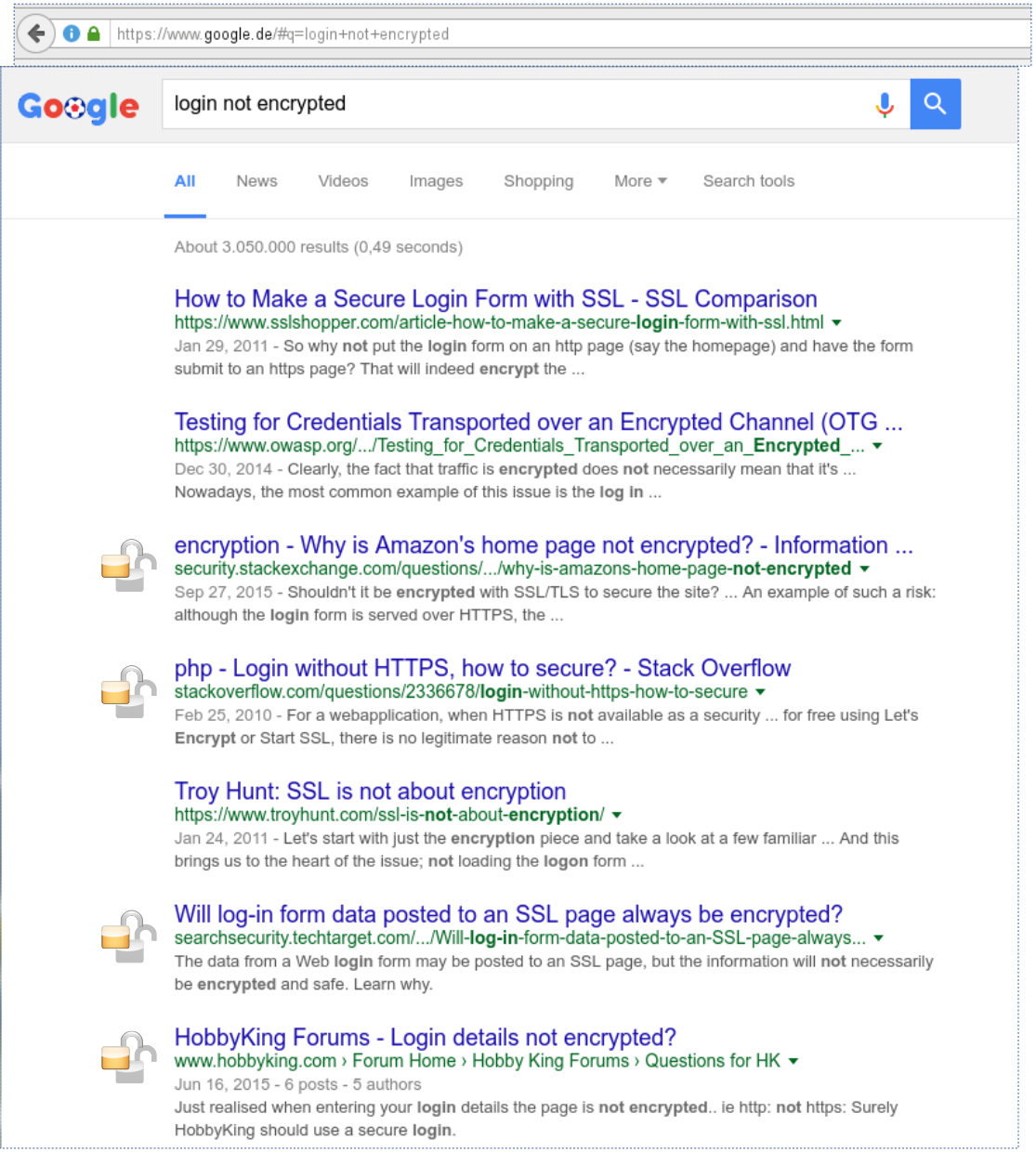
✓	Method	File	Domain	Type	Transferred	Size	0 ms / 1.28 s / 2.56 s / 3.84 s
200	GET	testssl.sh	github.com	html	14.89 KB	59.21 KB	→ 672 ms
200	GET	github-760a9497[illegible]f2883d6febd885…	assets-cdn.github.com	css	44.41 KB	183.18 KB	→ 251 ms
200	GET	github2-622bce26a47[illegible]c8a581fe1e…	assets-cdn.github.com	css	58.03 KB	252.20 KB	→ 331 ms
200	GET	frameworks-06e65f5639cc5[illegible]d1aaa…	assets-cdn.github.com	js	73.31 KB	201.44 KB	→ 505 ms
200	GET	github-ee4ac88329bd04835855a[illegible]	assets-cdn.github.com	js	115.79 KB	357.59 KB	→ 632 ms
200	GET	8036727?v=3&s=40	avatars1.githubusercont…	png	1.55 KB	2.07 KB	→ 465 ms
200	GET	octocat-spinner-32.gif	assets-cdn.github.com	gif	2.26 KB	3.01 KB	→ 458 ms
200	GET	68747470733a2f2f62616467657…	camo.githubusercontent…	svg	0.65 KB	0.65 KB	→ 308 ms
200	GET	show_partial?partial=tree/recently[illegible]	github.com	html	0.17 KB	0.22 KB	→ 177 ms
200	GET	api.js	collector-cdn.github.com	js	2.82 KB	7.80 KB	→ 134 ms
200	GET	ZeroClipboard.v2.1.6.swf	assets-cdn.github.com	x-sho…	3.94 KB	5.26 KB	→ 62 ms
200	GET	counts	github.com	json	0.08 KB	0.10 KB	→ 315 ms
101	GET	ODAzNjcyNzpkNDA2YmMxYzl5O…	live.github.com	plain	—	0 KB	→ 414 ms
200	GET	page_view?dimensions[page]=h…	collector.githubapp.[illegible]	gif	0.03 KB	0.05 KB	→ 424 ms
200	POST	stats	api.github.com	json	0 0.03 KB	0.00 KB	→ 5

browser:referer



RFC 2616

browser:referer



- **Major search engines**
  - HTTP landing page:

    internal POST before GET

server:URL

- **Scary research**
  - WF = website fingerprinting! (or WFP)

    Website fingerprinting (WFP) attack is a special case of traffic analysis. Performed by an eavesdropper, it tries to infer which webpage a client is viewing by identifying patterns in network traffic
  - (sometimes disputed)
  - HTTP/1.1 only

server:URL

Privacy Vulnerabilities in Encrypted HTTP Streams

George Dean Bissias, Marc Liberatore, David Jensen, and Brian Neil Levine

University of Massachusetts, Amherst, MA 01003, USA
{gbiss,liberato,jensen,brian}@cs.umass.edu

Abstract. Encrypting traffic does not prevent an attacker from performing some types of traffic analysis. We present a straightforward traffic analysis attack against encrypted HTTP streams that is surprisingly effective in identifying the source of the traffic. An attacker starts by creating a profile of the statistical characteristics of web requests from interesting sites, including distributions of packet sizes and inter-arrival times. Later, candidate encrypted streams are compared against these profiles. In our evaluations using real traffic, we find that many web sites are subject to this attack. With a training period of 24 hours and a 1 hour delay afterwards, the attack achieves only 23% accuracy. However, an attacker can easily pre-determine which of trained sites are easily identifiable. Accordingly, against 25 such sites, the attack achieves 40% accuracy;

server:URL

Touching from a Distance: Website Fingerprinting Attacks and Defenses

Xiang Cai
Stony Brook University
xcai@cs.stonybrook.edu

Xin Cheng Zhang
Stony Brook University
xinczhan@gmail.com

Brijesh Joshi
Stony Brook University
sunjosh17@hotmail.com

Rob Johnson
Stony Brook University
rob@cs.stonybrook.edu

ABSTRACT

We present a novel web page fingerprinting attack that is able to defeat several recently proposed defenses against traffic analysis attacks, including the application-level defenses HTTPOS [15] and randomized pipelining over Tor [18]. Regardless of the defense scheme, our attack was able to guess which of 100 web pages a victim was visiting at least 50% of the time and, with some defenses, over 90% of the time. Our attack is based on a simple model of network behavior and out-performs previously proposed ad hoc attacks. We then build a web *site* fingerprinting attack that is able to identify whether a victim is visiting a particular web site with over 90% accuracy in our experiments.

server:URL

I Know Why You Went to the Clinic: Risks and Realization of HTTPS Traffic Analysis

Brad Miller[1], Ling Huang[2], A. D. Joseph[1], and J. D. Tygar[1]

[1] UC Berkeley
[2] Intel Labs

Abstract. Revelations of large scale electronic surveillance and data mining by governments and corporations have fueled increased adoption of HTTPS. We present a traffic analysis attack against over 6000 webpages spanning the HTTPS deployments of 10 widely used, industry-leading websites in areas such as healthcare, finance, legal services and streaming video. Our attack identifies individual pages in the same website with 89% accuracy, exposing personal details including medical conditions, financial and legal affairs and sexual orientation. We examine

Lemmy: Motorhead Frontman Dead | TMZ.com - Mozilla Firefox

Lemmy: Motorhead Fro...

https://www.tmz.com/2015/12/28/

Search

TMZ NEWS SPORTS VIDEOS PHOTOS WATCH TMZ Sign In

Home ➡ Lemmy: Motorhead Frontman Dead

LEMMY MOTORHEAD FRONTMAN DE

12/28/2015 4:32 PM PST BY TMZ STAFF

Getty

Ghostery found 27 trackers
www.tmz.com

- ~~Amazon Associates~~ — Advertising, Affiliate Marketing
- ~~ChartBeat~~ — Analytics
- ~~Crazy Egg~~ — Analytics
- ~~Criteo~~ — Advertising, Search
- ~~Disqus~~ — Widgets, Commenting System, So...
- ~~DoubleClick~~ — Advertising

Pause Blocking | Whitelist Site | ?

~~Amazon Associates~~
~~ChartBeat~~
~~Crazy Egg~~
~~Criteo~~
~~Disqus~~
~~DoubleClick~~
~~Dynamic Yield~~
~~Facebook Connect~~
~~Facebook Social Graph~~
~~Google Analytics~~
~~Gravity Insights~~
~~Kaltura~~
~~Kixer~~
~~Krux Digital~~
~~NetRatings SiteCensus~~
~~Omniture (Adobe Analytics)~~
~~Optimizely~~
~~Outbrain~~
~~Pinterest~~
~~Quantcast~~
~~ScoreCard Research Beacon~~
~~ShareThis~~
~~Taboola~~
~~Tumblr Buttons~~
~~Twitter Badge~~
~~Twitter Button~~
~~ZergNet~~

V TMZ

Sign me Up!

Missed It
kdown of the week's top stories.

ries delivered straight to your inbox.

agree to the Privacy Policy and Terms of Use.

AROUND THE WEB


Gwen & Blake: Breaking Up Because Of No Pregnancy


Justin Bieber & Kourtney Kardashian Sleeping Together: Taking Relationship To Next Level?


Leo DiCaprio Parties HARD In St. Barts, HARD!

pest:oftheinternet

```
✖ Blocked loading mixed active content "http://w.sharethis.com/button/buttons.js" [Learn More]
✖ Blocked loading mixed active content "http://ll-assets.tmz.com/fonts/tmz/liberation-mono/regular.ttf" [Learn More]
✖ Blocked loading mixed active content "http://tmz.vo.llnwd.net/o28/fonts/woff/RobotoCondensed-Regular1.woff" [Learn More]
✖ Blocked loading mixed active content "http://tmz.vo.llnwd.net/o28/fonts/ttf/RobotoCondensed-Regular1.ttf" [Learn More]
✖ Blocked loading mixed active content "http://tmz.vo.llnwd.net/o28/fonts/woff/Roboto-Regular1.woff" [Learn More]
✖ Blocked loading mixed active content "http://tmz.vo.llnwd.net/o28/fonts/ttf/Roboto-Regular1.ttf" [Learn More]
✖ Blocked loading mixed active content "http://ll-assets.tmz.com/fonts/tmz/roboto-condensed/light.ttf" [Learn More]
⚠ Loading mixed (insecure) display content "http://tmz.vo.llnwd.net/o28/assets/svg/social_2015/white_f_facebook.svg" on a secure page [Learn More
⚠ Loading mixed (insecure) display content "http://tmz.vo.llnwd.net/o28/assets/svg/social_2015/white_tbird_twitter.svg" on a secure page [Learn M
⚠ Loading mixed (insecure) display content "http://tmz.vo.llnwd.net/o28/assets/svg/social_2015/white_comment_tmz.svg" on a secure page [Learn Mor
✖ Blocked loading mixed active content "http://tmz.vo.llnwd.net/o28/fonts/woff/SourceSansPro-Bold.otf.woff" [Learn More]
✖ Blocked loading mixed active content "http://tmz.vo.llnwd.net/o28/fonts/ttf/SourceSansPro-Bold.ttf" [Learn More]
✖ Blocked loading mixed active content "http://cdn.kixer.com/ad/load.js" [Learn More]
✖ Blocked loading mixed active content "http://www.zergnet.com/zerg.js?id=34754" [Learn More]
✖ Blocked loading mixed active content "http://cdn.api.twitter.com/1/urls/count.json?url=http%3A%2F%2Fwww.tmz.com%2F2015%2F12%2F28%2Flemmy-motorh
  _=1451412906818" [Learn More]
⚠ Loading mixed (insecure) display content "http://tmz.vo.llnwd.net/o28/assets/svg/social_2015/icon-facebook.svg" on a secure page [Learn More]
⚠ Loading mixed (insecure) display content "http://tmz.vo.llnwd.net/o28/assets/svg/social_2015/icon-twitter.svg" on a secure page [Learn More]
⚠ Loading mixed (insecure) display content "http://tmz.vo.llnwd.net/o28/assets/svg/social_2015/icon-youtube.svg" on a secure page [Learn More]
⚠ Loading mixed (insecure) display content "http://tmz.vo.llnwd.net/o28/assets/svg/social_2015/icon-instagram.svg" on a secure page [Learn More]
```

- **Statistics**
  - 249 GET requests (!) to 81 Hosts
  - 49 x Mixed content blocked
  - 15 x loaded

- **Mixed Content**
  - State of the (small) disaster:

- **Mixed Content**
  - State of the (bigger) desasters:

Mixed Content Tests	Webkit @ Android 5.0.1		IE 11 + Y to question	Android 4.0.3 and FF < 23
Images	Passive	Yes	Yes	Yes
CSS	Active	No	Yes	Yes
Scripts	Active	No	Yes	Yes
XMLHttpRequest	Active	Yes	No	Yes
WebSockets	Active	Test failed	No	N/A
Frames	Active	No	No	Yes

remember:snowden

- **Remember**
  - **GCHQ/NSA piggybacking e.g. google tracking**

    According to the documents, the NSA and its British counterpart, GCHQ, are using the small tracking files or "cookies" that advertising networks place on computers to identify people browsing the Internet. The intelligence agencies have found particular use for a part of a Google-specific tracking mechanism known as the “PREF” cookie. These cookies typically don't contain personal information, such as someone's name or e-mail address, but they do contain numeric codes that enable Web sites to uniquely identify a person's browser.

https://www.washingtonpost.com/news/the-switch/wp/2013/12/10/nsa-uses-google-cookies-to-pinpoint-targets-for-hackin

take:aways

- **Bottom line**
  - Information security values matter!!1!
    - C)onfidentiality, I)ntegrity, A)vailability
  - **Content** is being ~protected via HTTPS
  - You improve C,I and privacy using encryption, but:
    - HTTP/1.1 + HTTP2: **Metadata leakage**:
      - IP address, port, hostname!!
    - Client side:
      - Browser + Browser version (TLS fingerprinting)
      - Website fingerprinting: HTTP2 vs. HTTP/1.1
    - Server side:
      - Online trackers!

take:aways

- **Bottom line, server-part**
  - Server:
    - Properly rotate away & anonymize logs
    - Use OCSP stapling
    - Use HTTP/2 in combination with TLS
    - Don't use 3rd party trackers

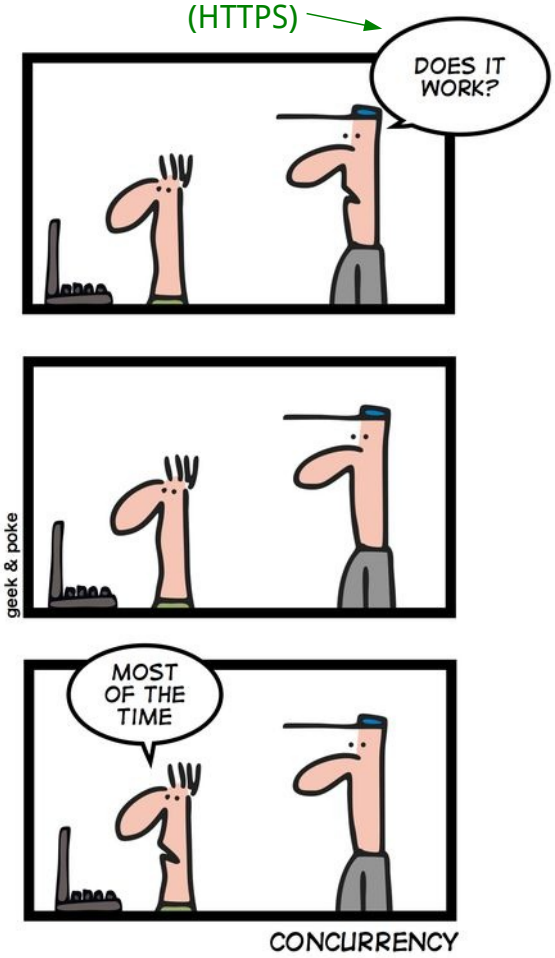
And If you need to: be honest and DO NOT talk about privacy!

- **Danke**

  dirk at

  - drwetter eu
  - testssl sh

@drwetter



Geek & Poke (Oliver Widder)