TLS als Beruhigungspille?

Dirk Wetter

@drwetter

about:me

- **Unabhängiger IT Security Consultant**
  - > 20 Jahre Berufserfahrung
  - Sicherheitsüberprüfungen (Web, Software, Systeme, Netze) / Verteidigung+Härtungen / Konzepte / Training / PM / (C)ISO
  - ► Datenschutz / Privatsphäre: wichtig für mich!

- **Mein Projekt**
  - testssl.sh

- **Involviert in**
  - OWASP
  - GUUG

https://drwetter.eu/

about:whatis

- **Motivation**
  - Überreaktion
  - Protagonisten: „Security“, „Privacy“ „safe“
  - Wenig Reflektion

    C)onfidentiality, I)ntegrity, A)vailability

- Bemerkenswert: Nur **HTTPS = HTTP+TLS**

- **Tellerrand**
  - SMTP+STARTTLS
    - ~60% encrypted, Hälfte (=~30%) haben vernünftige Zertifikatsvalidierung
      - MTA sender → hard fail?
    - Nicht-Opportunistisch?
  - IMAP/POP: (STARTTLS: 45-50%, pure IMAPS/POPS: 54-65%)
  - Jabber: C2S: ~3% (!), S2S < 1%
  - VoIP, GSM: träum weiter ;-)

- **Privacy-Werte Protokoll**
  - Höher als HTTP?!

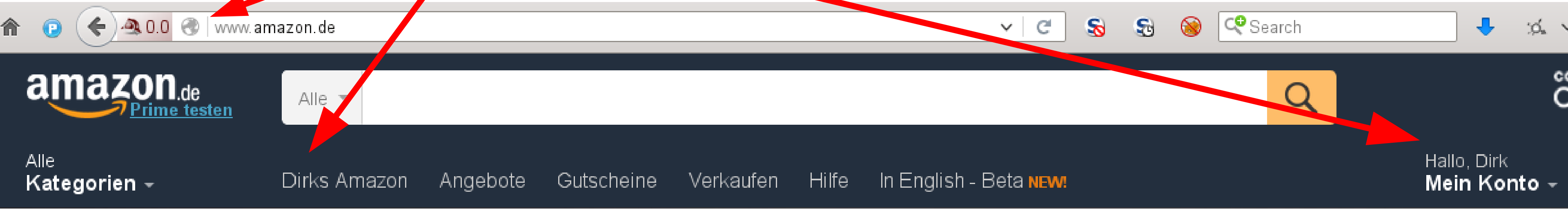
- **Umschalten…**

auf **HTTP+TLS** — commonly known as **HTTPS**

Frank. C Müller https://de.wikipedia.org/wiki/Datei:Lichtleitung_1_fcm.jpg CC4-BY-SA

nottalking:about

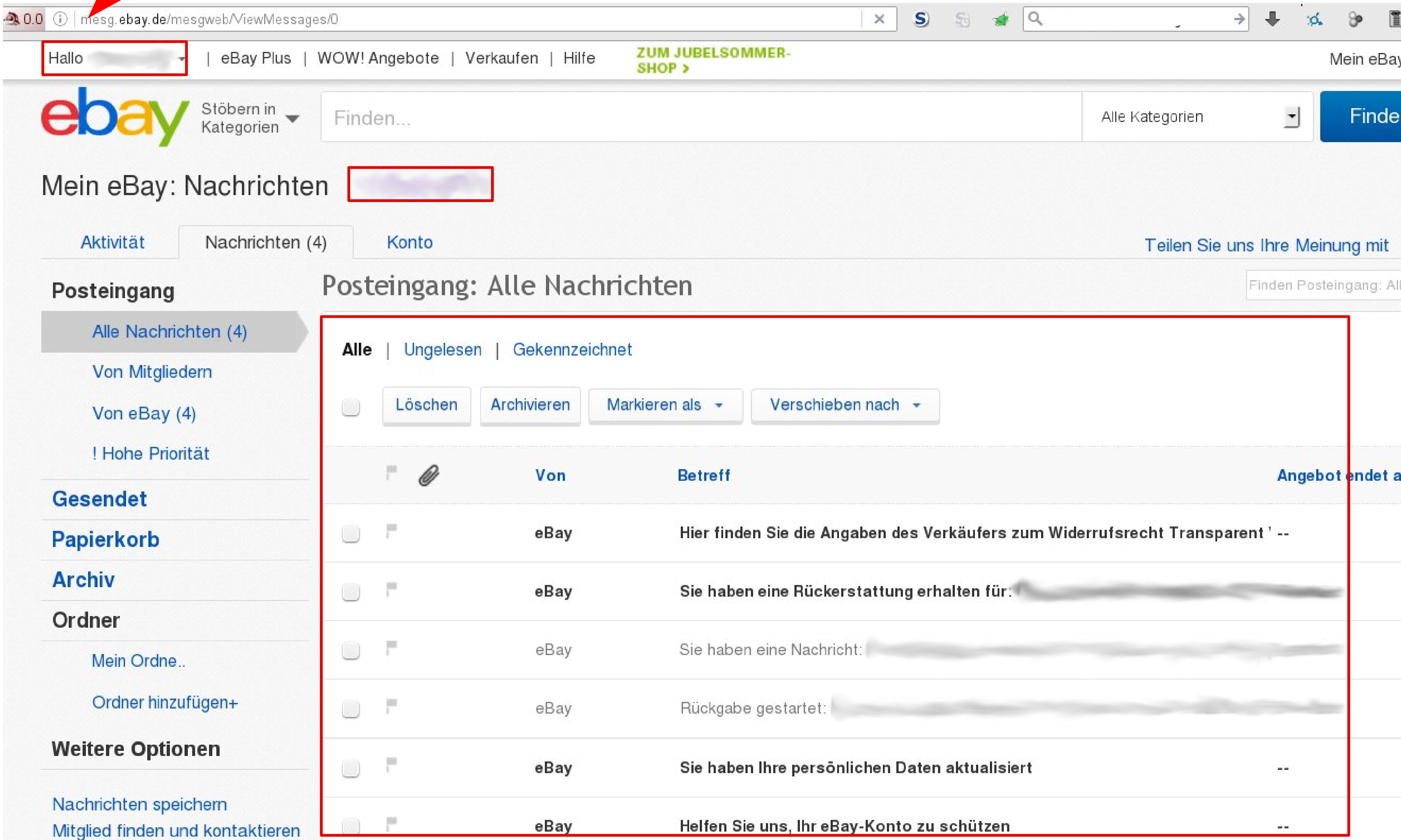
WTF? [1]



[1] Vor ~ einem Jahr

nottalking:about

WTF?



mesg.ebay.de/mesgweb/ViewMessages/0

Hallo [redacted] | eBay Plus | WOW! Angebote | Verkaufen | Hilfe

ZUM JUBELSOMMER-SHOP ›

Mein eBay

Stöbern in Kategorien

Finden...

Alle Kategorien

Finde

Mein eBay: Nachrichten [redacted]

Aktivität | Nachrichten (4) | Konto

Teilen Sie uns Ihre Meinung mit

Posteingang

- Alle Nachrichten (4)
- Von Mitgliedern
- Von eBay (4)
- ! Hohe Priorität

Gesendet

Papierkorb

Archiv

Ordner

- Mein Ordne..
- Ordner hinzufügen+

Weitere Optionen

- Nachrichten speichern
- Mitglied finden und kontaktieren

Posteingang: Alle Nachrichten

Finden Posteingang: All

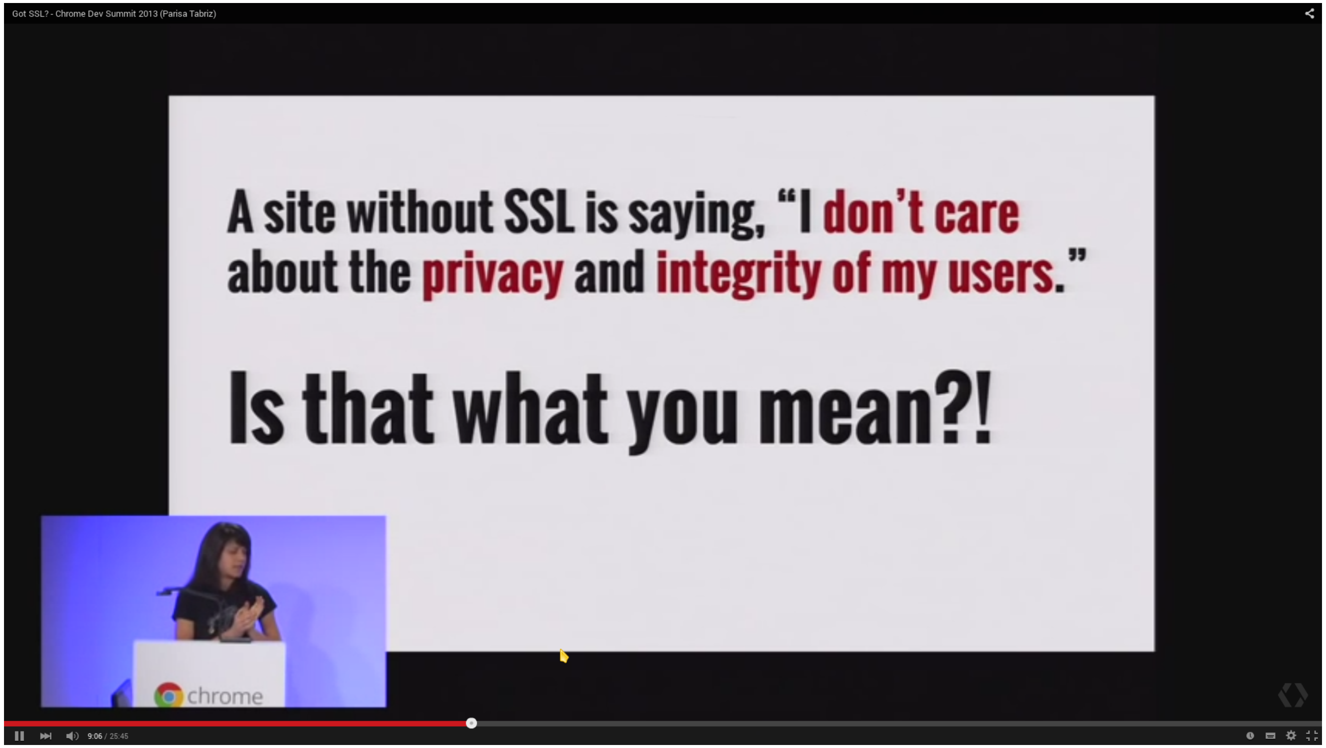
Alle | Ungelesen | Gekennzeichnet

□ Löschen | Archivieren | Markieren als ▾ | Verschieben nach ▾

	Von	Betreff	Angebot endet a
□	eBay	Hier finden Sie die Angaben des Verkäufers zum Widerrufsrecht Transparent '	--
□	eBay	Sie haben eine Rückerstattung erhalten für: [redacted]	
□	eBay	Sie haben eine Nachricht: [redacted]	
□	eBay	Rückgabe gestartet: [redacted]	
□	eBay	Sie haben Ihre persönlichen Daten aktualisiert	--
□	eBay	Helfen Sie uns, Ihr eBay-Konto zu schützen	--

(Personally taken)

- **HTTPS**
  - 11/2013: Google @ Chrome Dev Summit

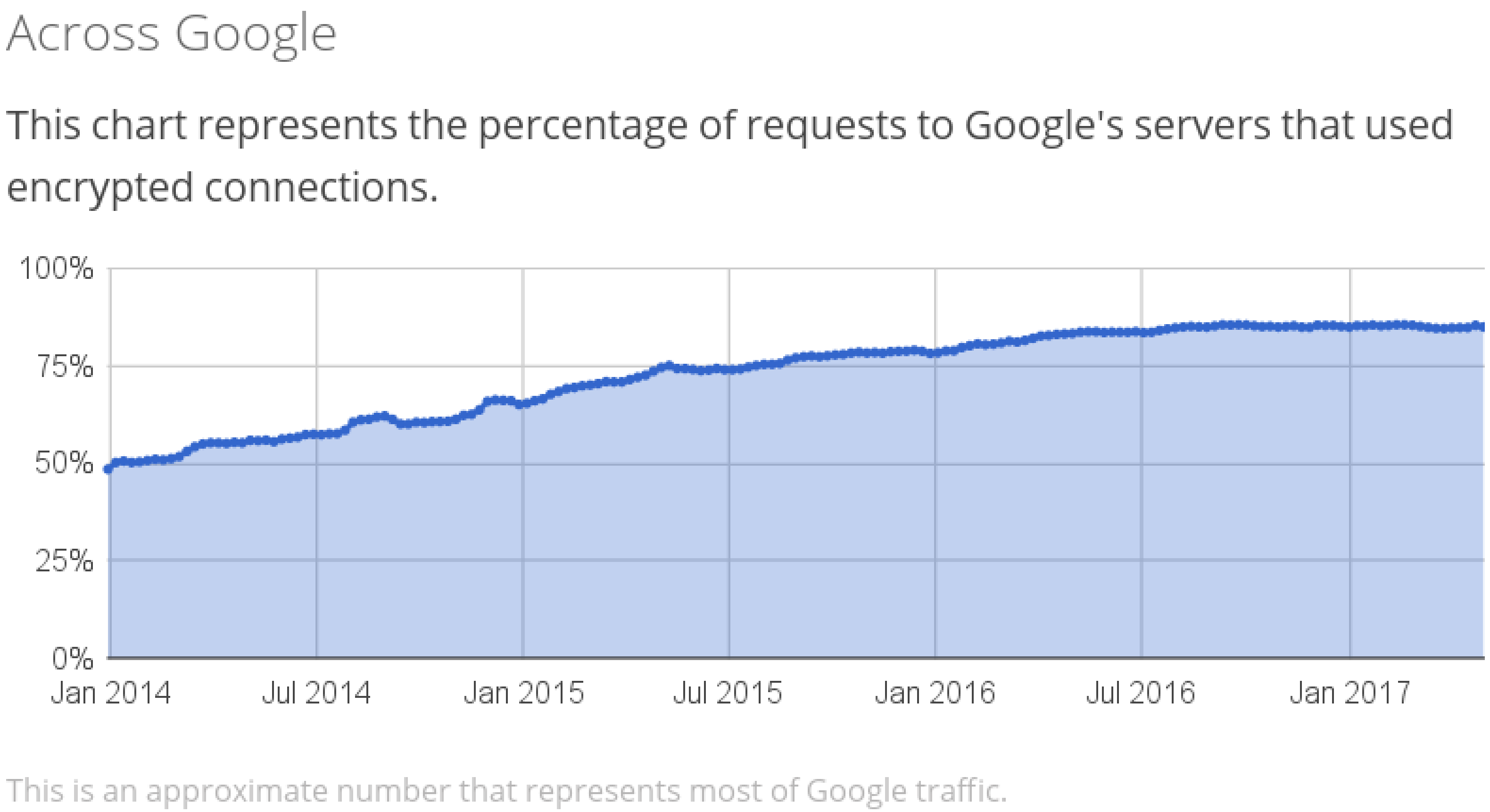


A site without SSL is saying, “I don’t care about the privacy and integrity of my users.”

Is that what you mean?!

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

- **HTTPS**
  - Einschub https://www.google.com/transparencyreport/https/

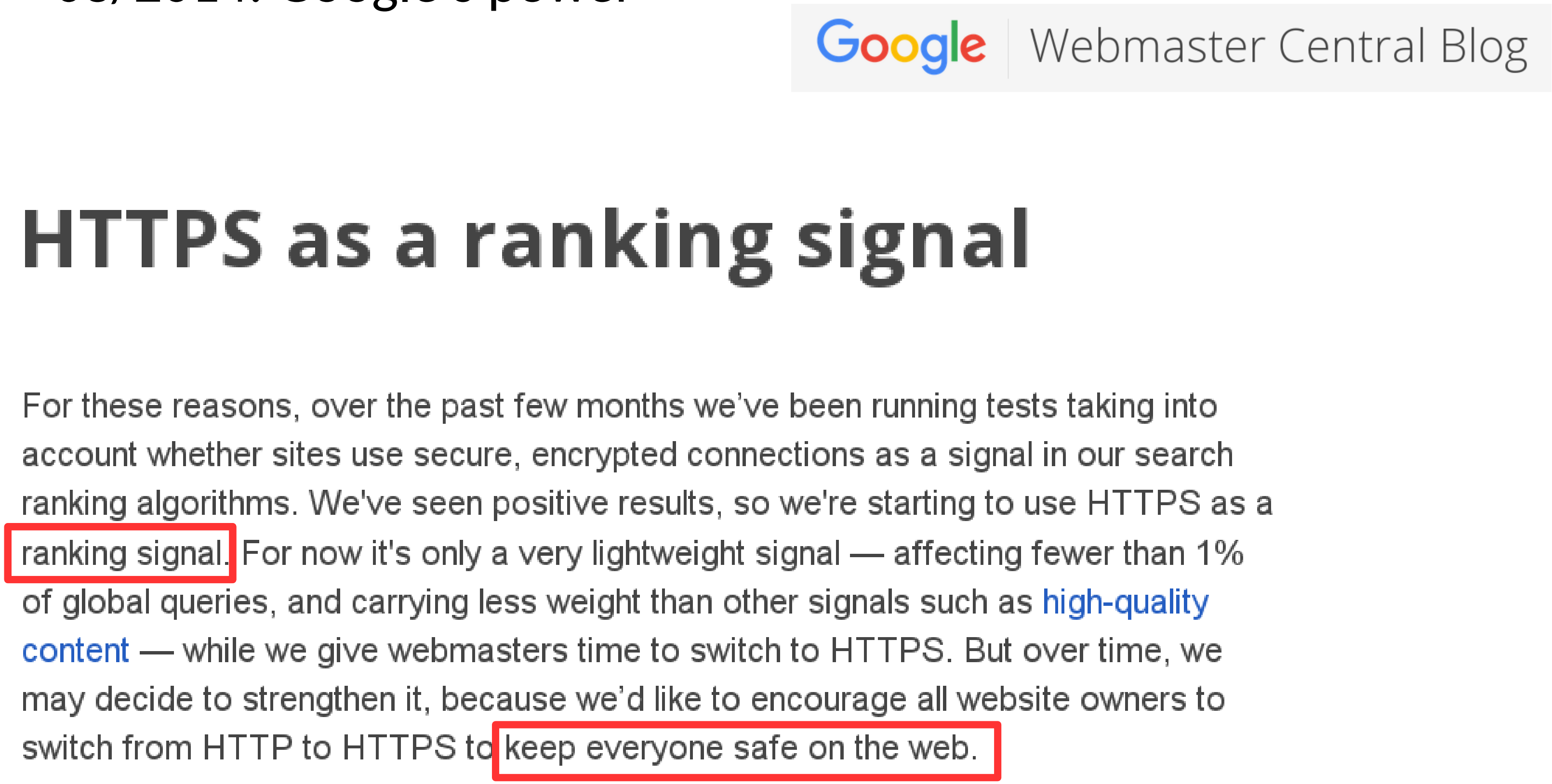


Across Google

This chart represents the percentage of requests to Google's servers that used encrypted connections.

This is an approximate number that represents most of Google traffic.

- **HTTPS**
  - 11/2013: Google @ Chrome Dev Summit
  - 08/2014: 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

- **HTTPS**
  - 11/2013: Google @ Chrome Dev Summit
  - 08/2014: Google's power
  - 06/2015: „HTTPS everywhere for IETF“

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

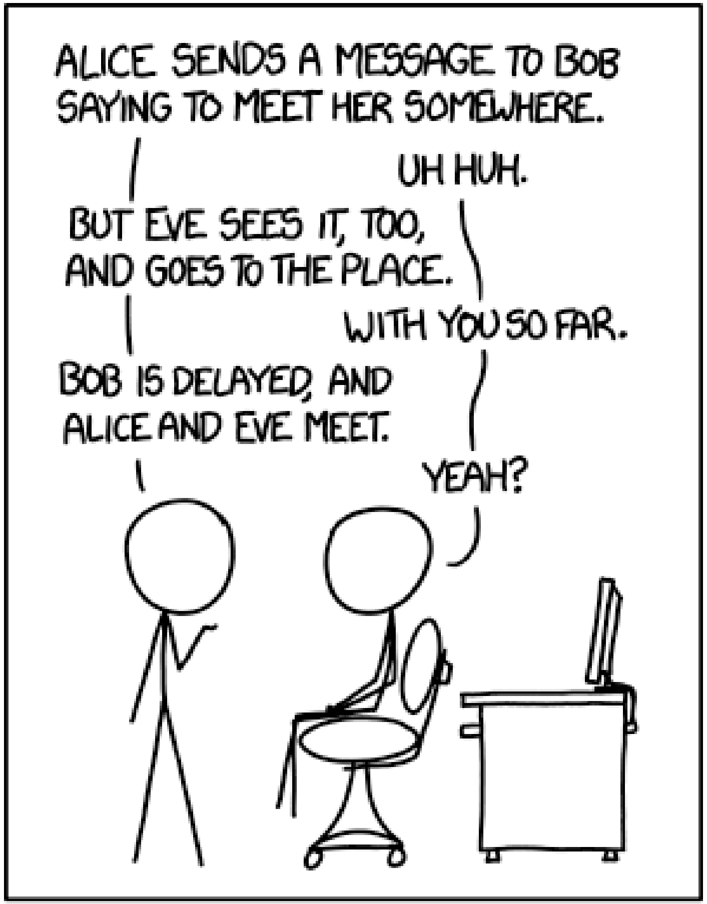
talking:about

- “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**.”

https://trac.tools.ietf.org/group/iesg/trac/wiki/HttpsEverywhere

talking:about

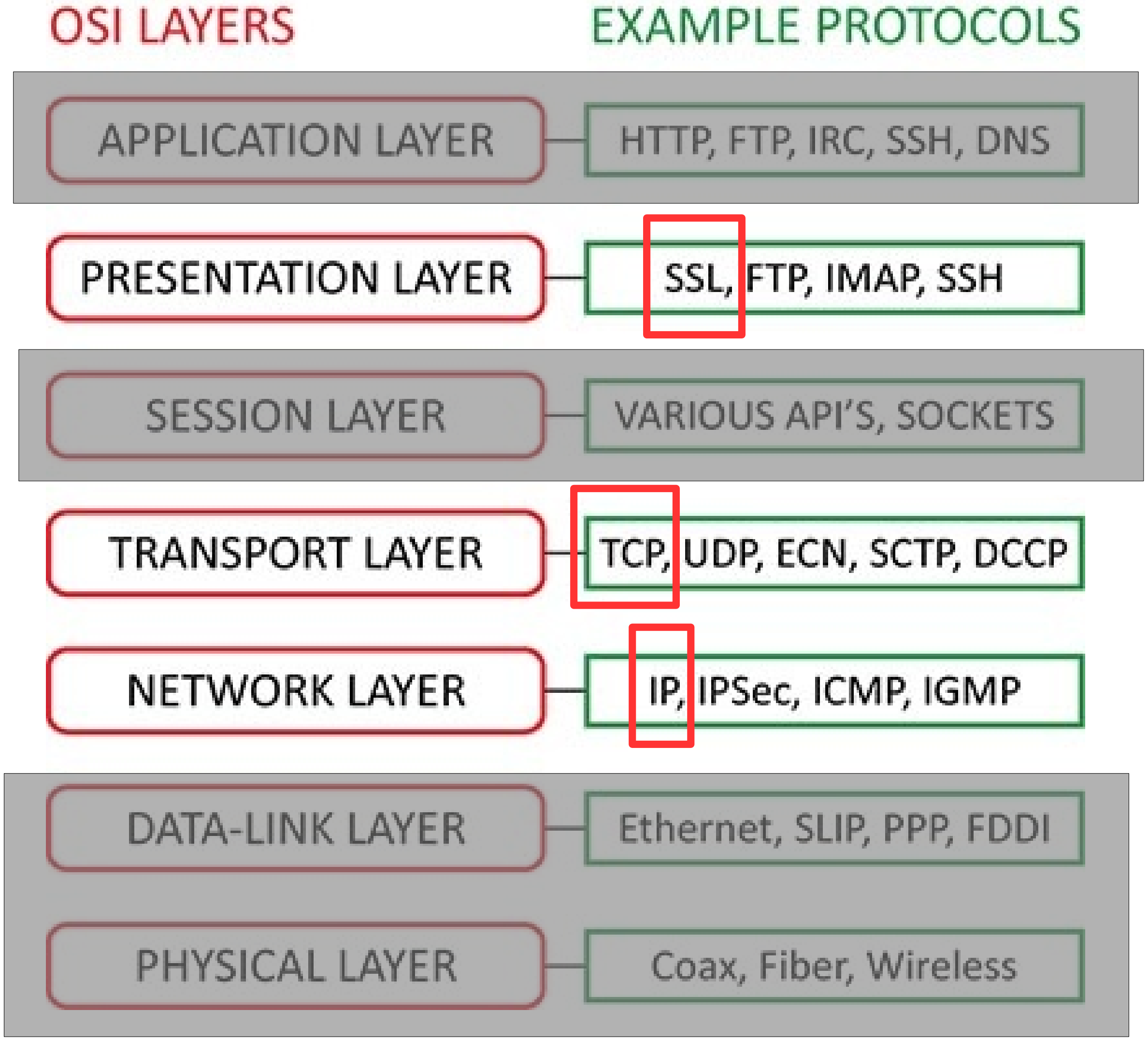
- **HTTPS 100%**
  - Was sieht ~~Eve~~ NSA im Netz?


ALICE SENDS A MESSAGE TO BOB SAYING TO MEET HER SOMEWHERE.
UH HUH.
BUT EVE SEES IT, TOO, AND GOES TO THE PLACE.
WITH YOU SO FAR.
BOB IS DELAYED, AND ALICE AND EVE MEET.
YEAH?

I'VE DISCOVERED A WAY TO GET COMPUTER SCIENTISTS TO LISTEN TO ANY BORING STORY.

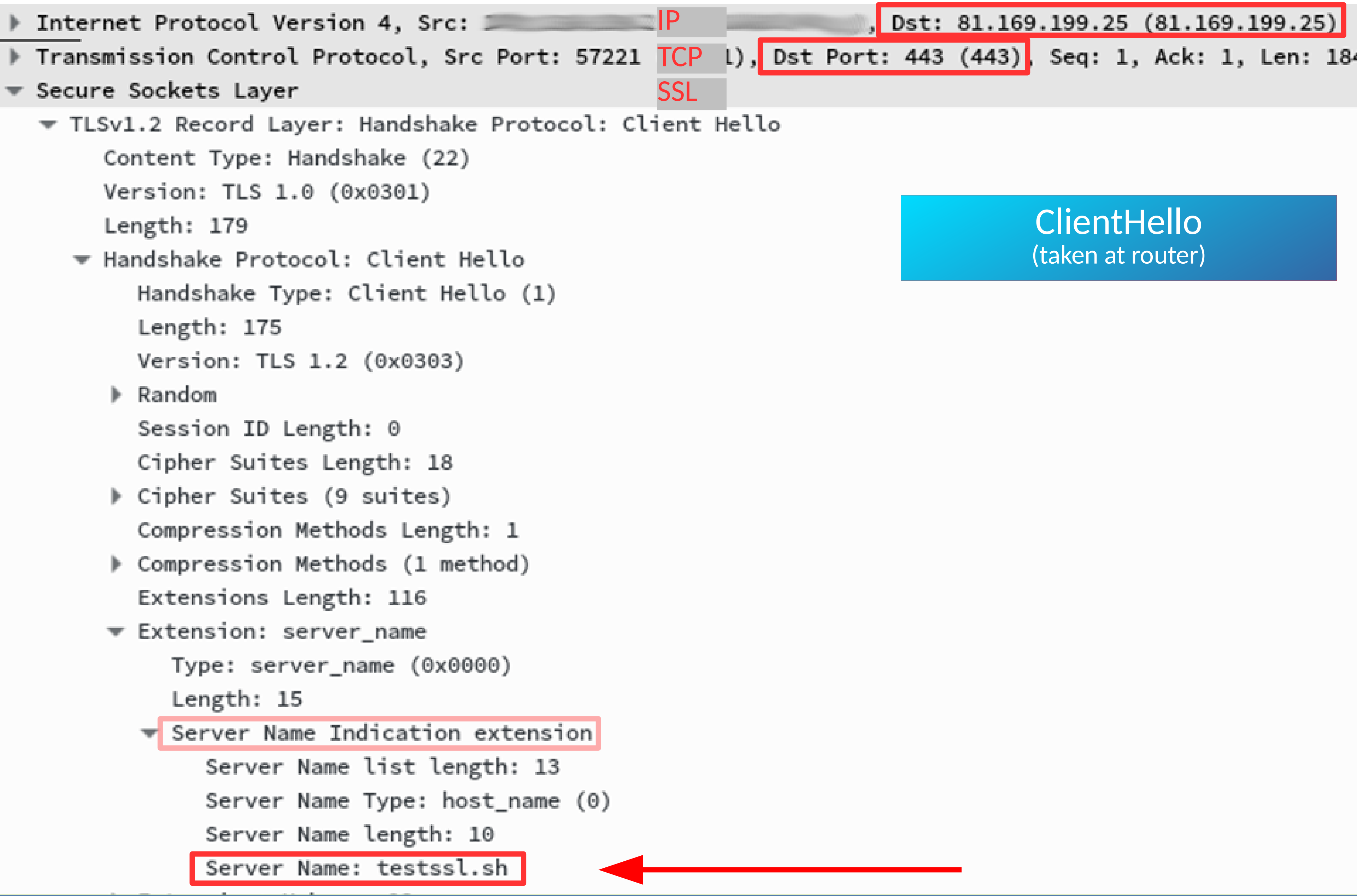
https://xkcd.com/1323/

network:layers



OSI LAYERS	EXAMPLE PROTOCOLS
APPLICATION LAYER	HTTP, FTP, IRC, SSH, DNS
PRESENTATION LAYER	SSL, FTP, IMAP, SSH
SESSION LAYER	VARIOUS API'S, SOCKETS
TRANSPORT LAYER	TCP, UDP, ECN, SCTP, DCCP
NETWORK LAYER	IP, IPSec, ICMP, IGMP
DATA-LINK LAYER	Ethernet, SLIP, PPP, FDDI
PHYSICAL LAYER	Coax, Fiber, Wireless

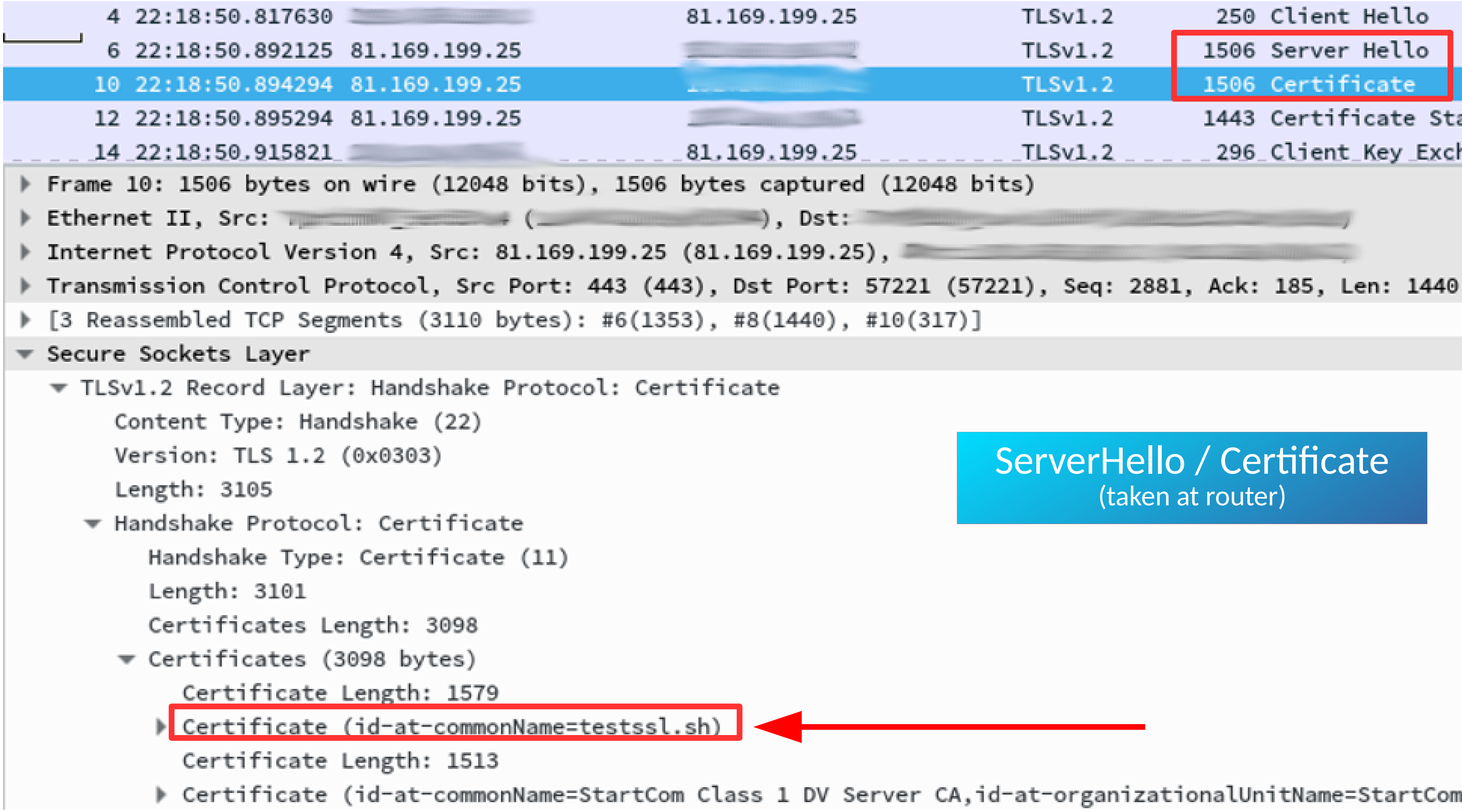
layers:{IP,TCP,TLS}



```
▸ Internet Protocol Version 4, Src: [redacted], Dst: 81.169.199.25 (81.169.199.25)
▸ Transmission Control Protocol, Src Port: 57221 l), Dst Port: 443 (443), Seq: 1, Ack: 1, Len: 18
▾ Secure Sockets Layer
  ▾ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 179
    ▾ Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 175
        Version: TLS 1.2 (0x0303)
      ▸ Random
        Session ID Length: 0
        Cipher Suites Length: 18
      ▸ Cipher Suites (9 suites)
        Compression Methods Length: 1
      ▸ Compression Methods (1 method)
        Extensions Length: 116
      ▾ Extension: server_name
          Type: server_name (0x0000)
          Length: 15
        ▾ Server Name Indication extension
            Server Name list length: 13
            Server Name Type: host_name (0)
            Server Name length: 10
            Server Name: testssl.sh
```

ClientHello
(taken at router)

layers:{IP,TCP,TLS}



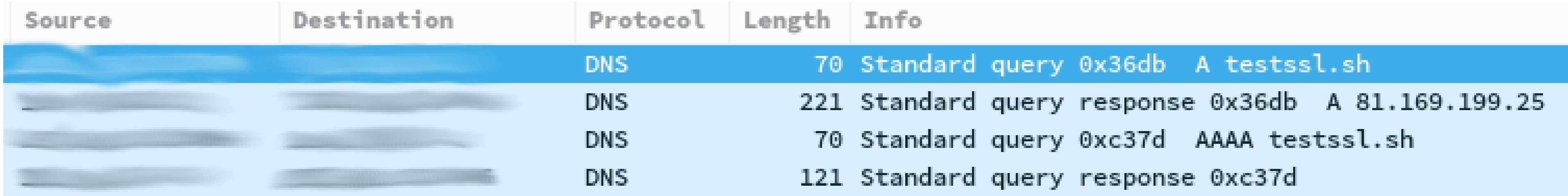
```
    4 22:18:50.817630 [redacted]        81.169.199.25      TLSv1.2      250 Client Hello
    6 22:18:50.892125 81.169.199.25     [redacted]         TLSv1.2     1506 Server Hello
   10 22:18:50.894294 81.169.199.25     [redacted]         TLSv1.2     1506 Certificate
   12 22:18:50.895294 81.169.199.25     [redacted]         TLSv1.2     1443 Certificate Sta
   14 22:18:50.915821 [redacted]        81.169.199.25      TLSv1.2      296 Client Key Exch
▸ Frame 10: 1506 bytes on wire (12048 bits), 1506 bytes captured (12048 bits)
▸ Ethernet II, Src: [redacted] ([redacted]), Dst: [redacted]
▸ Internet Protocol Version 4, Src: 81.169.199.25 (81.169.199.25), [redacted]
▸ Transmission Control Protocol, Src Port: 443 (443), Dst Port: 57221 (57221), Seq: 2881, Ack: 185, Len: 1440
▸ [3 Reassembled TCP Segments (3110 bytes): #6(1353), #8(1440), #10(317)]
▾ Secure Sockets Layer
  ▾ TLSv1.2 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 3105
    ▾ Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 3101
        Certificates Length: 3098
      ▾ Certificates (3098 bytes)
          Certificate Length: 1579
        ▸ Certificate (id-at-commonName=testssl.sh)
          Certificate Length: 1513
        ▸ Certificate (id-at-commonName=StartCom Class 1 DV Server CA,id-at-organizationalUnitName=StartCom
```

ServerHello / Certificate

(taken at router)

browser:before

- **Vor Aufruf der Webseite...**
  - DNS (Klartext)



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

- **Vor Aufruf der Webseite...**
  - DNS
  - OCSP

```
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

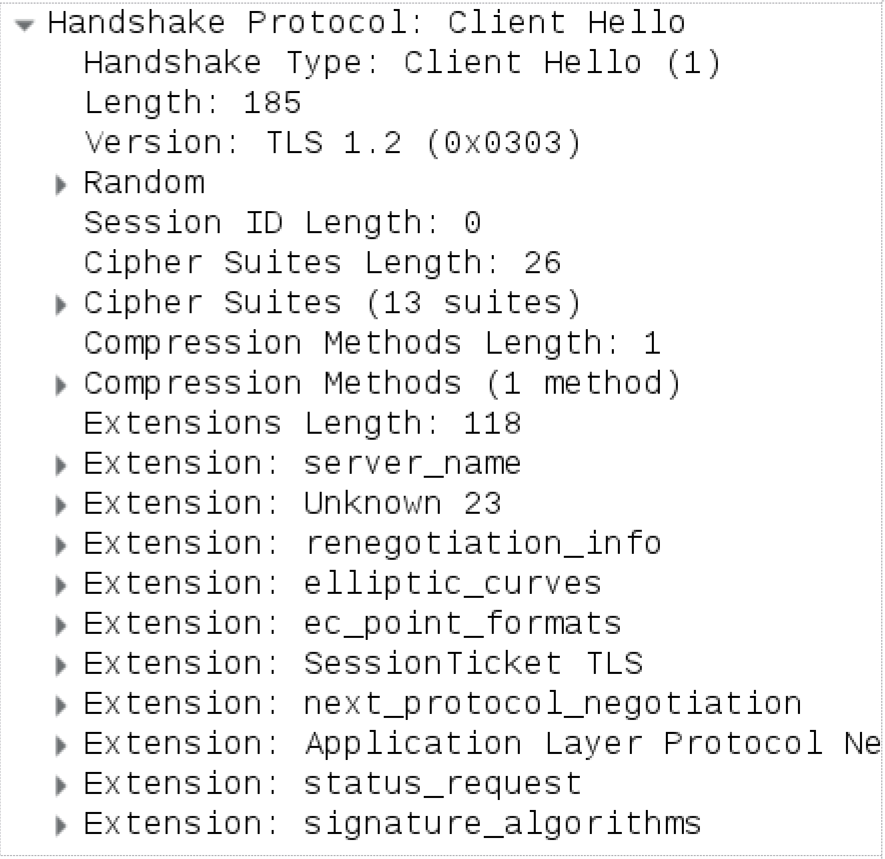
- **Vor Aufruf der Webseite…**
  - DNS
  - OCSP
    - 3rd party involvement!
    - RFC 6960
      - 4.1.1. ASN.1 Specification of the OCSP Request

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

browser:TLS layer

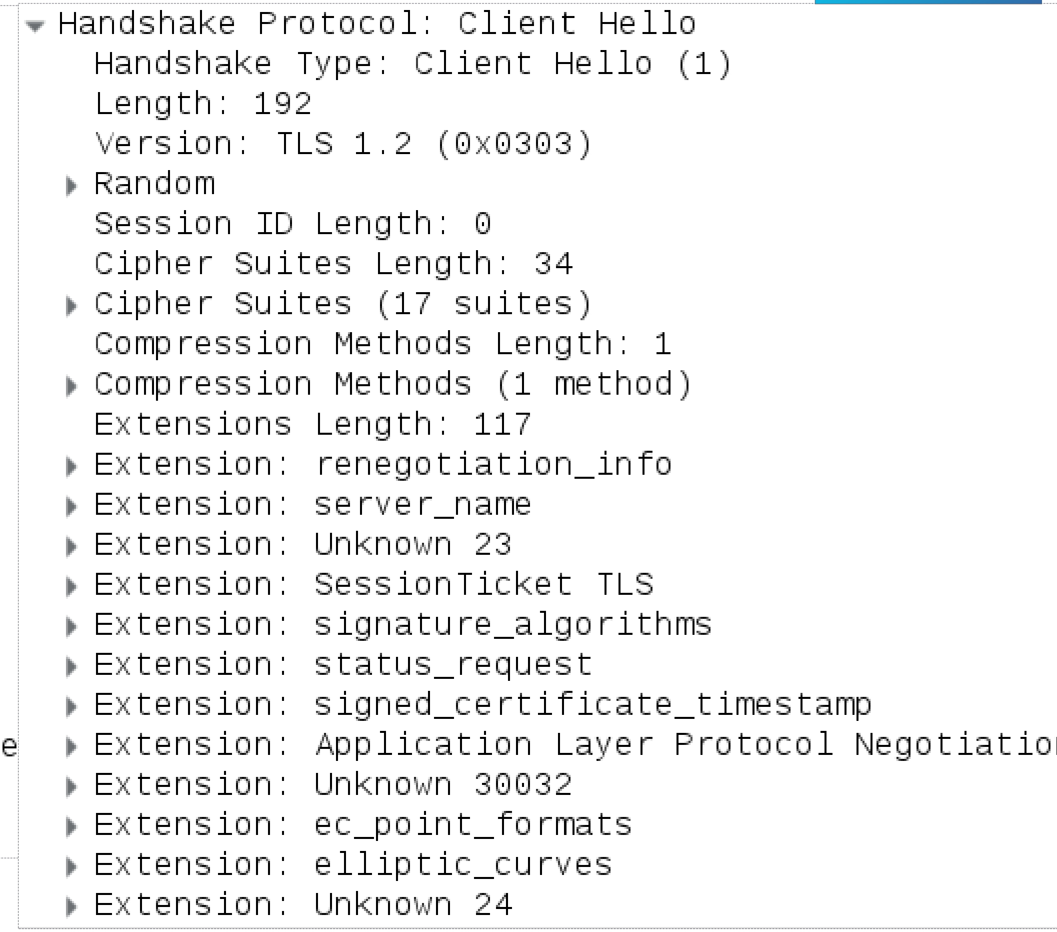
ClientHellos
(sniffed from router)

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
```

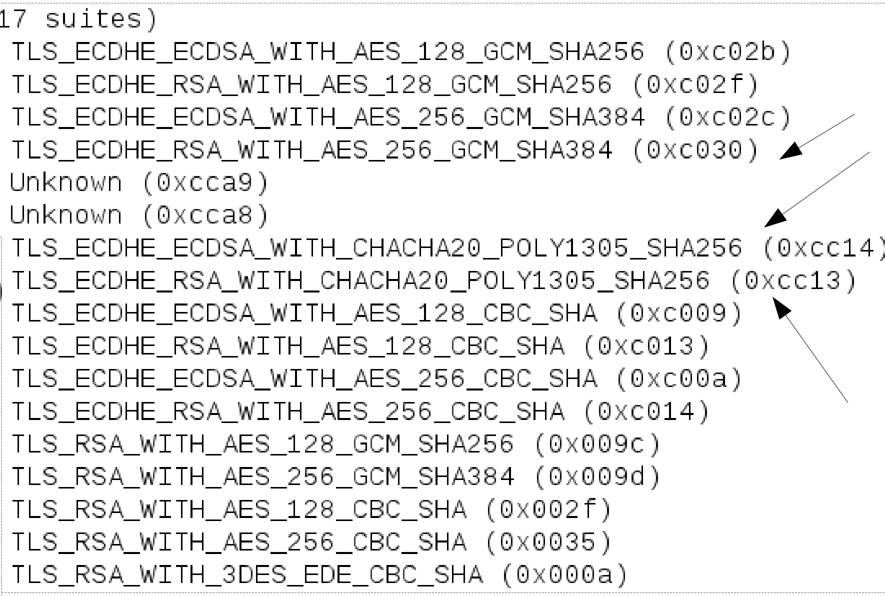
Chrome



```
▼ 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
```

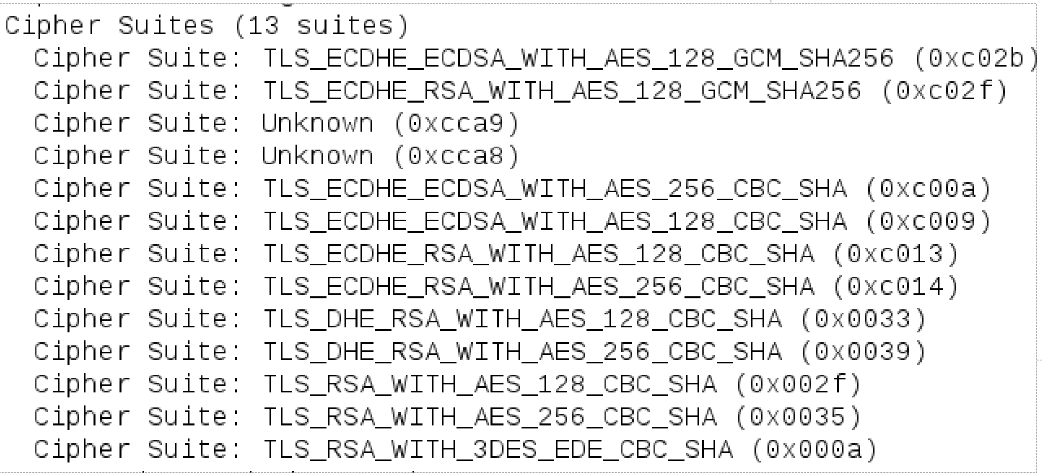
ClientHellos
(sniffed from router)

Chrome 51

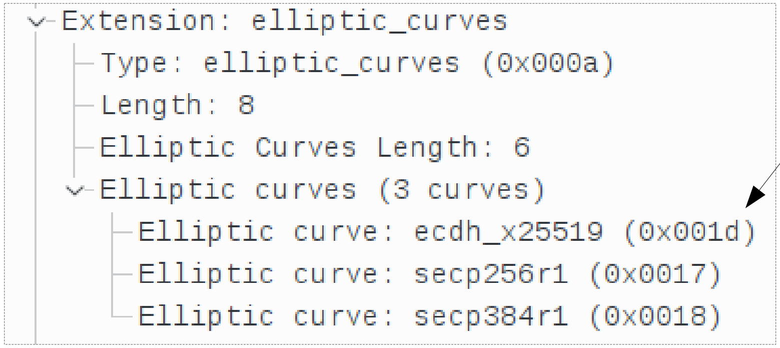


```
Cipher Suites (17 suites)
  Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
  Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
  Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
  Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
  Cipher Suite: 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)
```

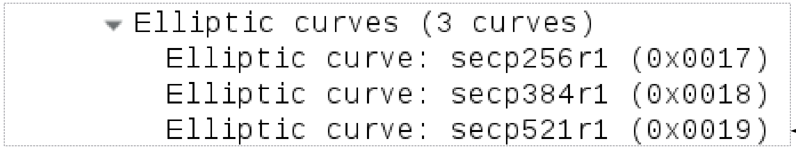
Firefox 47



```
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)
```



```
Extension: elliptic_curves
  Type: elliptic_curves (0x000a)
  Length: 8
  Elliptic Curves Length: 6
  Elliptic curves (3 curves)
    Elliptic curve: ecdh_x25519 (0x001d)
    Elliptic curve: secp256r1 (0x0017)
    Elliptic curve: secp384r1 (0x0018)
```



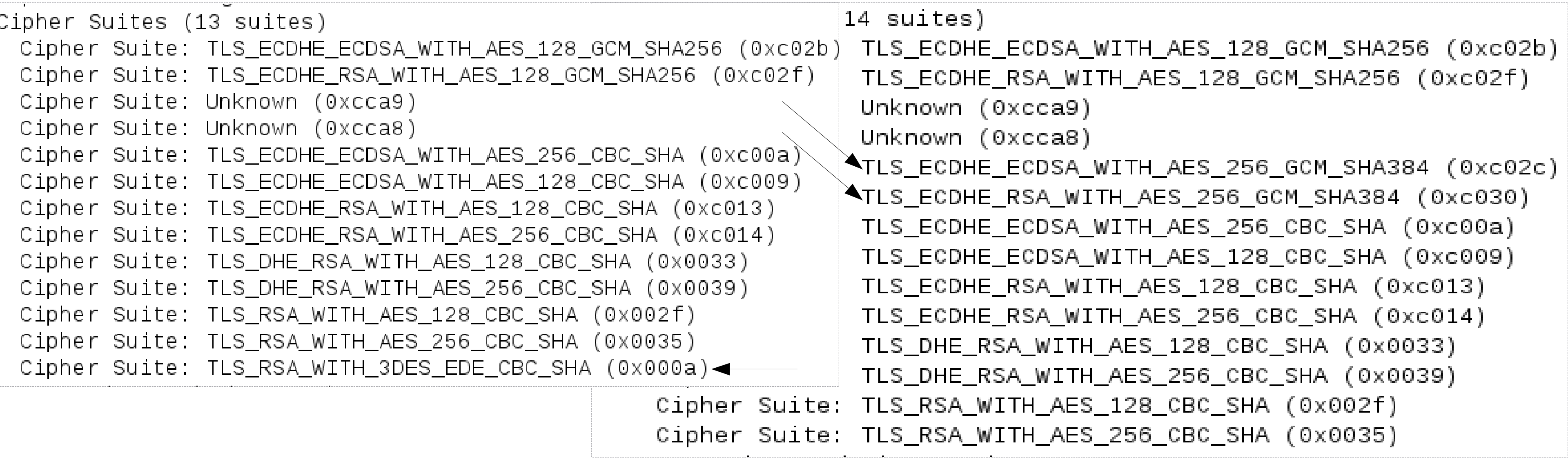
```
Elliptic curves (3 curves)
  Elliptic curve: secp256r1 (0x0017)
  Elliptic curve: secp384r1 (0x0018)
  Elliptic curve: secp521r1 (0x0019)
```

browser:TLS layer

ClientHellos
(sniffed from router)

Firefox 47

Firefox 52



```
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)
```

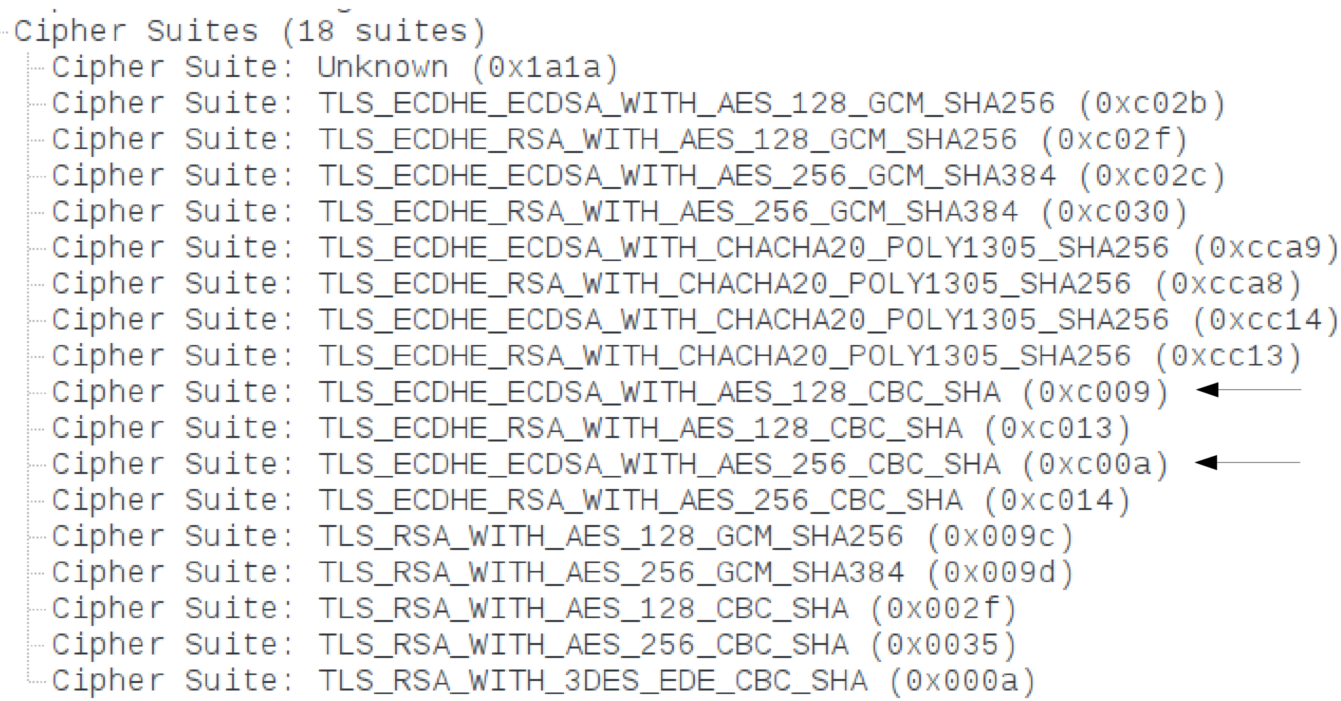
```
14 suites)
 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
 Unknown (0xcca9)
 Unknown (0xcca8)
 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (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

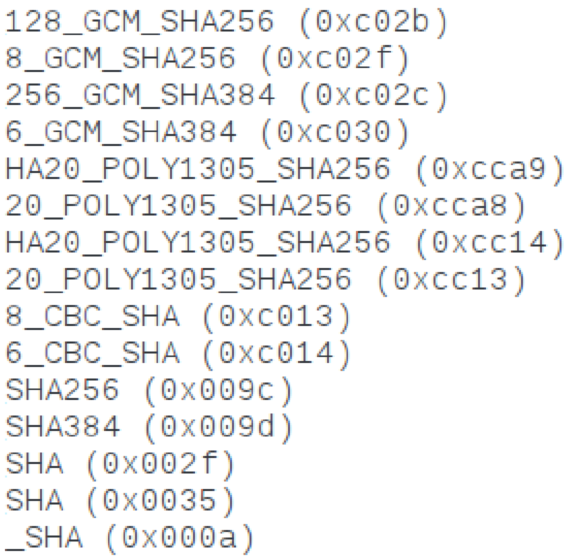
ClientHellos
(sniffed from router)

Chrome 55

Chrome 56

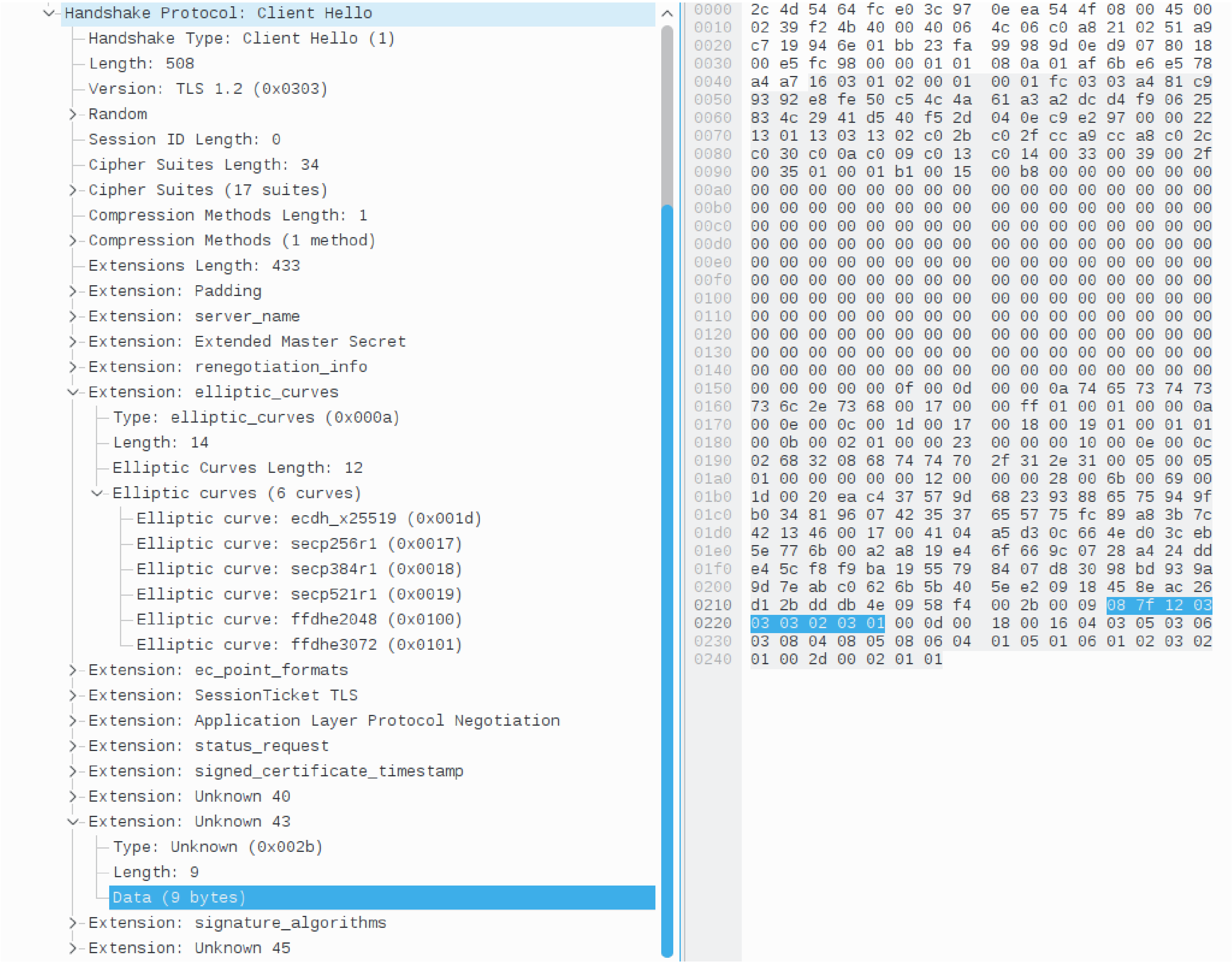


```
Cipher Suites (18 suites)
    Cipher Suite: Unknown (0x1a1a)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
    Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcc14)
    Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcc13)
    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_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
    Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
    Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
    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)
```



```
128_GCM_SHA256 (0xc02b)
8_GCM_SHA256 (0xc02f)
256_GCM_SHA384 (0xc02c)
6_GCM_SHA384 (0xc030)
HA20_POLY1305_SHA256 (0xcca9)
20_POLY1305_SHA256 (0xcca8)
HA20_POLY1305_SHA256 (0xcc14)
20_POLY1305_SHA256 (0xcc13)
8_CBC_SHA (0xc013)
6_CBC_SHA (0xc014)
SHA256 (0x009c)
SHA384 (0x009d)
SHA (0x002f)
SHA (0x0035)
_SHA (0x000a)
```

browser:TLS layer



```
Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 508
    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: 433
  > Extension: Padding
  > Extension: server_name
  > Extension: Extended Master Secret
  > Extension: renegotiation_info
  v Extension: elliptic_curves
        Type: elliptic_curves (0x000a)
        Length: 14
        Elliptic Curves Length: 12
      v Elliptic curves (6 curves)
            Elliptic curve: ecdh_x25519 (0x001d)
            Elliptic curve: secp256r1 (0x0017)
            Elliptic curve: secp384r1 (0x0018)
            Elliptic curve: secp521r1 (0x0019)
            Elliptic curve: ffdhe2048 (0x0100)
            Elliptic curve: ffdhe3072 (0x0101)
  > Extension: ec_point_formats
  > Extension: SessionTicket TLS
  > Extension: Application Layer Protocol Negotiation
  > Extension: status_request
  > Extension: signed_certificate_timestamp
  > Extension: Unknown 40
  v Extension: Unknown 43
        Type: Unknown (0x002b)
        Length: 9
        Data (9 bytes)
  > Extension: signature_algorithms
  > Extension: Unknown 45
```

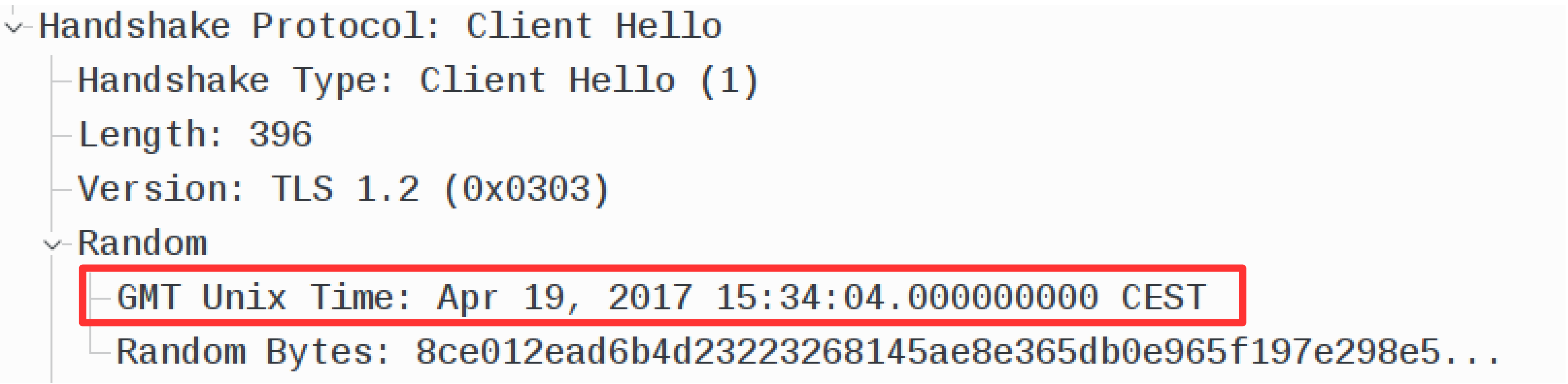
```
0000  2c 4d 54 64 fc e0 3c 97  0e ea 54 4f 08 00 45 00
0010  02 39 f2 4b 40 00 40 06  4c 06 c0 a8 21 02 51 a9
0020  c7 19 94 6e 01 bb 23 fa  99 98 9d 0e d9 07 80 18
0030  00 e5 fc 98 00 00 01 01  08 0a 01 af 6b e6 e5 78
0040  a4 a7 16 03 01 02 00 01  00 01 fc 03 03 a4 81 c9
0050  93 92 e8 fe 50 c5 4c 4a  61 a3 a2 dc d4 f9 06 25
0060  83 4c 29 41 d5 40 f5 2d  04 0e c9 e2 97 00 00 22
0070  13 01 13 03 13 02 c0 2b  c0 2f cc a9 cc a8 c0 2c
0080  c0 30 c0 0a c0 09 c0 13  c0 14 00 33 00 39 00 2f
0090  00 35 01 00 01 b1 00 15  00 b8 00 00 00 00 00 00
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0110  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0120  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0130  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0140  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0150  00 00 00 00 00 0f 00 0d  00 00 0a 74 65 73 74 73
0160  73 6c 2e 73 68 00 17 00  00 ff 01 00 01 00 00 0a
0170  00 0e 00 0c 00 1d 00 17  00 18 00 19 01 00 01 01
0180  00 0b 00 02 01 00 00 23  00 00 00 10 00 0e 00 0c
0190  02 68 32 08 68 74 74 70  2f 31 2e 31 00 05 00 05
01a0  01 00 00 00 00 00 12 00  00 00 28 00 6b 00 69 00
01b0  1d 00 20 ea c4 37 57 9d  68 23 93 88 65 75 94 9f
01c0  b0 34 81 96 07 42 35 37  65 57 75 fc 89 a8 3b 7c
01d0  42 13 46 00 17 00 41 04  a5 d3 0c 66 4e d0 3c eb
01e0  5e 77 6b 00 a2 a8 19 e4  6f 66 9c 07 28 a4 24 dd
01f0  e4 5c f8 f9 ba 19 55 79  84 07 d8 30 98 bd 93 9a
0200  9d 7e ab c0 62 6b 5b 40  5e e2 09 18 45 8e ac 26
0210  d1 2b dd db 4e 09 58 f4  00 2b 00 09 08 7f 12 03
0220  03 03 02 03 01 00 0d 00  18 00 16 04 03 05 03 06
0230  03 08 04 08 05 08 06 04  01 05 01 06 01 02 03 02
0240  01 00 2d 00 02 01 01
```

Firefox 52
(TLS 1.3)

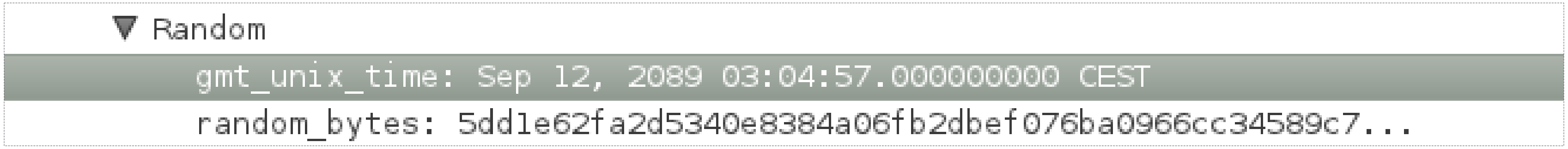
browser:TLS layer

- **Microsoft?**
  - Epoch (bis incl. IE 11 + Edge!)

#LOL!



```
Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 396
    Version: TLS 1.2 (0x0303)
    Random
        GMT Unix Time: Apr 19, 2017 15:34:04.000000000 CEST
        Random Bytes: 8ce012ead6b4d23223268145ae8e365db0e965f197e298e5...
```



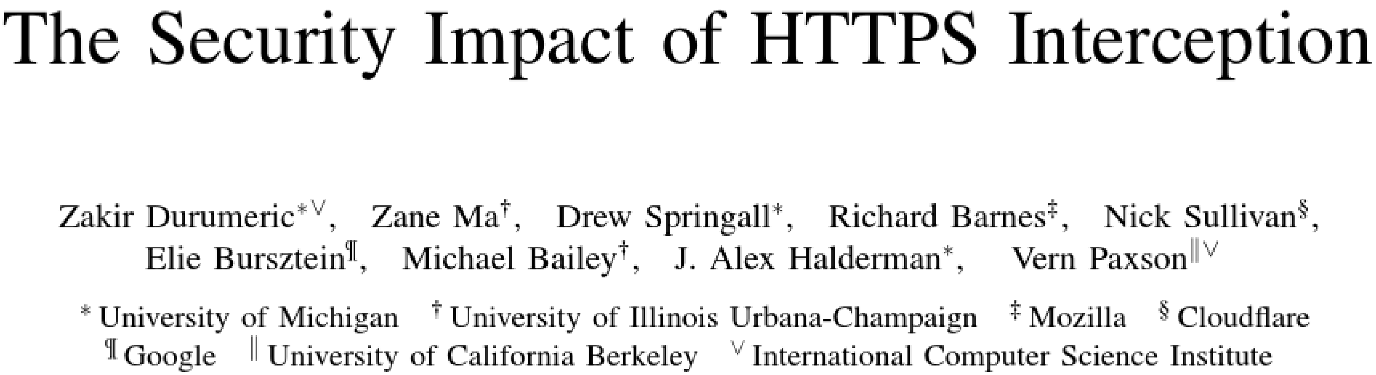
```
▼ Random
      gmt_unix_time: Sep 12, 2089 03:04:57.000000000 CEST
      random_bytes: 5dd1e62fa2d5340e8384a06fb2dbef076ba0966cc34589c7...
```

browser:TLS layer

- **Microsoft?**
  - Epoch (bis incl. IE 11 + Edge)
  - SChannel:
    - IE+Edge → OS-Bestandteil
    - Patchlevel!

browser:TLS layer

- **Microsoft?**
  - Epoch (bis incl. IE 11 + Edge)
  - SChannel
  - Schlimmer: AV!



The Security Impact of HTTPS Interception

Zakir Durumeric[*∨], Zane Ma[†], Drew Springall[*], Richard Barnes[‡], Nick Sullivan[§],
Elie Bursztein[¶], Michael Bailey[†], J. Alex Halderman[*], Vern Paxson[‖∨]

[*] University of Michigan [†] University of Illinois Urbana-Champaign [‡] Mozilla [§] Cloudflare
[¶] Google [‖] University of California Berkeley [∨] International Computer Science Institute

Network and Distributed System Security Symposium 2017

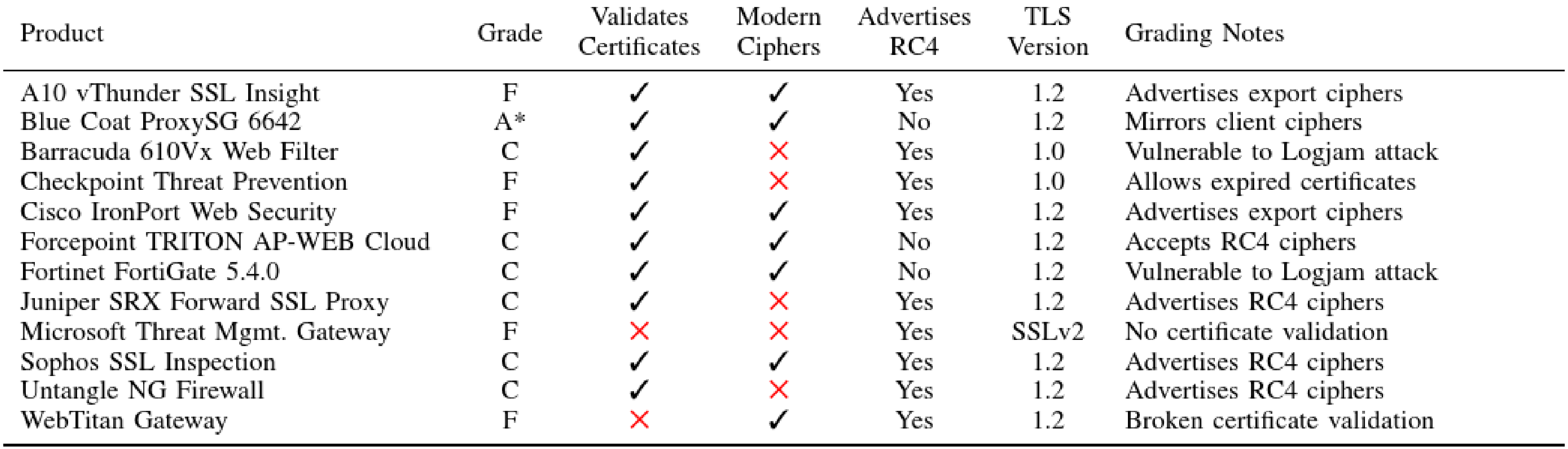
Product	OS	Browser MITM				Grade	Validates Certificates	Modern Ciphers	TLS Version	Grading Notes
		IE	Chrome	Firefox	Safari					
Avast …										
AV 11	Win	●	○	○		A*	✓	✓	1.2	Mirrors client ciphers
AV 11.7	Mac		●	●	●	F	✓	✓	1.2	Advertises DES
AVG …										
Internet Security 2015–6	Win	●	●	○		C	✓	✓	1.2	Advertises RC4
Bitdefender …										
Internet Security 2016	Win	●	●	●		C	✓	○	1.2	RC4, 768-bit D-H
Total Security Plus 2016	Win	●	●	●		C	✓	○	1.2	RC4, 768-bit D-H
AV Plus 2015–16	Win	●	●	●		C	✓	○	1.2	RC4, 768-bit D-H
Bullguard …										
Internet Security 16	Win	●	●	●		A*	✓	✓	1.2	Mirrors client ciphers
Internet Security 15	Win	●	●	●		F	✓	✗	1.0	Advertises DES
CYBERsitter …										
CYBERsitter 11	Win	●	●	●		F	✗	✗	1.2	No cert. validation, DES
Dr. Web …										
Security Space 11	Win	●	●	●		C	✓	○	1.2	RC4, FREAK
Dr. Web 11 for OS X	Mac		●	●	●	F	✓	✗	1.0	Export ciphers, DES, RC2
ESET …										
NOD32 AV 9	Win	●	●	●		F	○	○	1.2	Broken cert. validation
Kaspersky …										
Internet Security 16	Win	●	●	●		C	✓	✓	1.2	CRIME vulnerability
Total Security 16	Win	●	●	●		C	✓	✓	1.2	CRIME vulnerability
Internet Security 16	Mac		●	●	●	C	✓	✓	1.2	768-bit D-H
KinderGate …										
Parental Control 3	Win	●	●	●		F	○	✗	1.0	Broken cert. validation
Net Nanny …										
Net Nanny 7	Win	●	●	●		F	✓	✓	1.2	Anonymous ciphers
Net Nanny 7	Mac		●	●	●	F	✓	✓	1.2	Anonymous ciphers
PC Pandora …										
PC Pandora 7	Win	●	◐	◐		F	✗	✗	1.0	No certificate validation
Qustodio …										
Parental Control 2015	Mac		●	●	●	F	✓	✓	1.2	Advertises DES

Interception:
○ No Interception (conn. allowed)
◐ Connections Blocked
● Connections Intercepted

Certificate Validation:
✗ No Validation
○ Broken Validation
✓ Correct Validation

Modern Ciphers:
✗ No Support
○ Non-preferred Support
✓ Preferred Support

Fig. 4: **Security of Client-side Interception Software**—We evaluate and fingerprint popular antivirus and client-side security products, finding that products from twelve vendors intercept connections.[5] In all but two cases, products degrade TLS connection



Product	Grade	Validates Certificates	Modern Ciphers	Advertises RC4	TLS Version	Grading Notes
A10 vThunder SSL Insight	F	✓	✓	Yes	1.2	Advertises export ciphers
Blue Coat ProxySG 6642	A*	✓	✓	No	1.2	Mirrors client ciphers
Barracuda 610Vx Web Filter	C	✓	✗	Yes	1.0	Vulnerable to Logjam attack
Checkpoint Threat Prevention	F	✓	✗	Yes	1.0	Allows expired certificates
Cisco IronPort Web Security	F	✓	✓	Yes	1.2	Advertises export ciphers
Forcepoint TRITON AP-WEB Cloud	C	✓	✓	No	1.2	Accepts RC4 ciphers
Fortinet FortiGate 5.4.0	C	✓	✓	No	1.2	Vulnerable to Logjam attack
Juniper SRX Forward SSL Proxy	C	✓	✗	Yes	1.2	Advertises RC4 ciphers
Microsoft Threat Mgmt. Gateway	F	✗	✗	Yes	SSLv2	No certificate validation
Sophos SSL Inspection	C	✓	✓	Yes	1.2	Advertises RC4 ciphers
Untangle NG Firewall	C	✓	✗	Yes	1.2	Advertises RC4 ciphers
WebTitan Gateway	F	✗	✓	Yes	1.2	Broken certificate validation

Fig. 3: **Security of TLS Interception Middleboxes**—We evaluate popular network middleboxes that act as TLS interception proxies. We find that nearly all reduce connection security and five introduce severe vulnerabilities. *Mirrors browser ciphers.

Certificate Validation:

✗ No Validation

○ Broken Validation

✓ Correct Validation

browser:TLS layer

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

    (benutzt testssl.sh!)
  -

    This repository Search

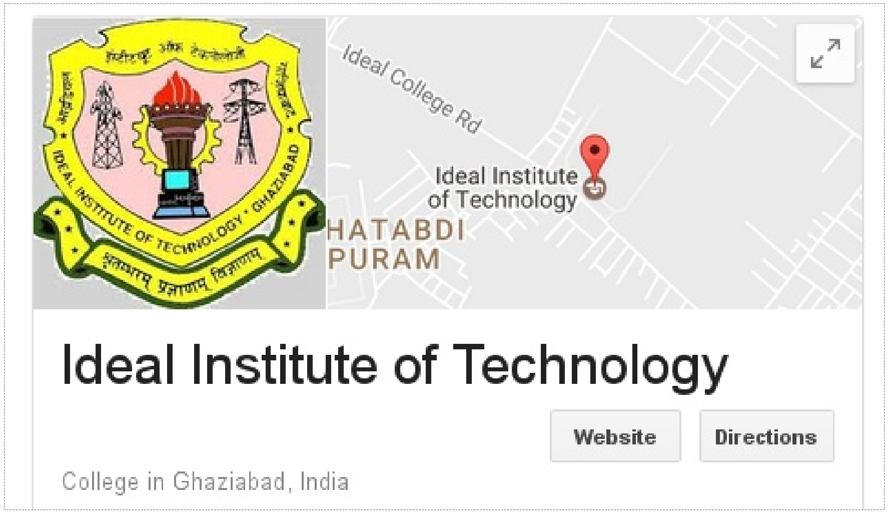
    LeeBrotherston / tls-fingerprinting

    github.com/LeeBrotherston/tls-fingerprinting/

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

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

- **War: Idealbild**

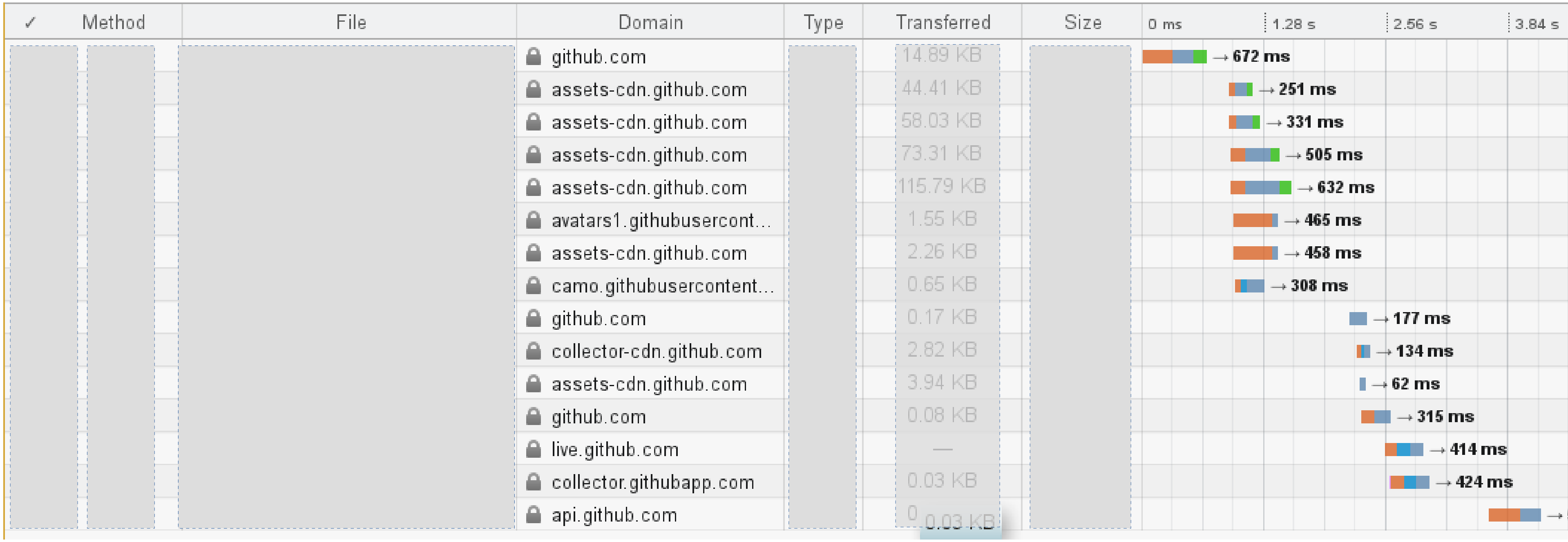


Ideal Institute of Technology

College in Ghaziabad, India

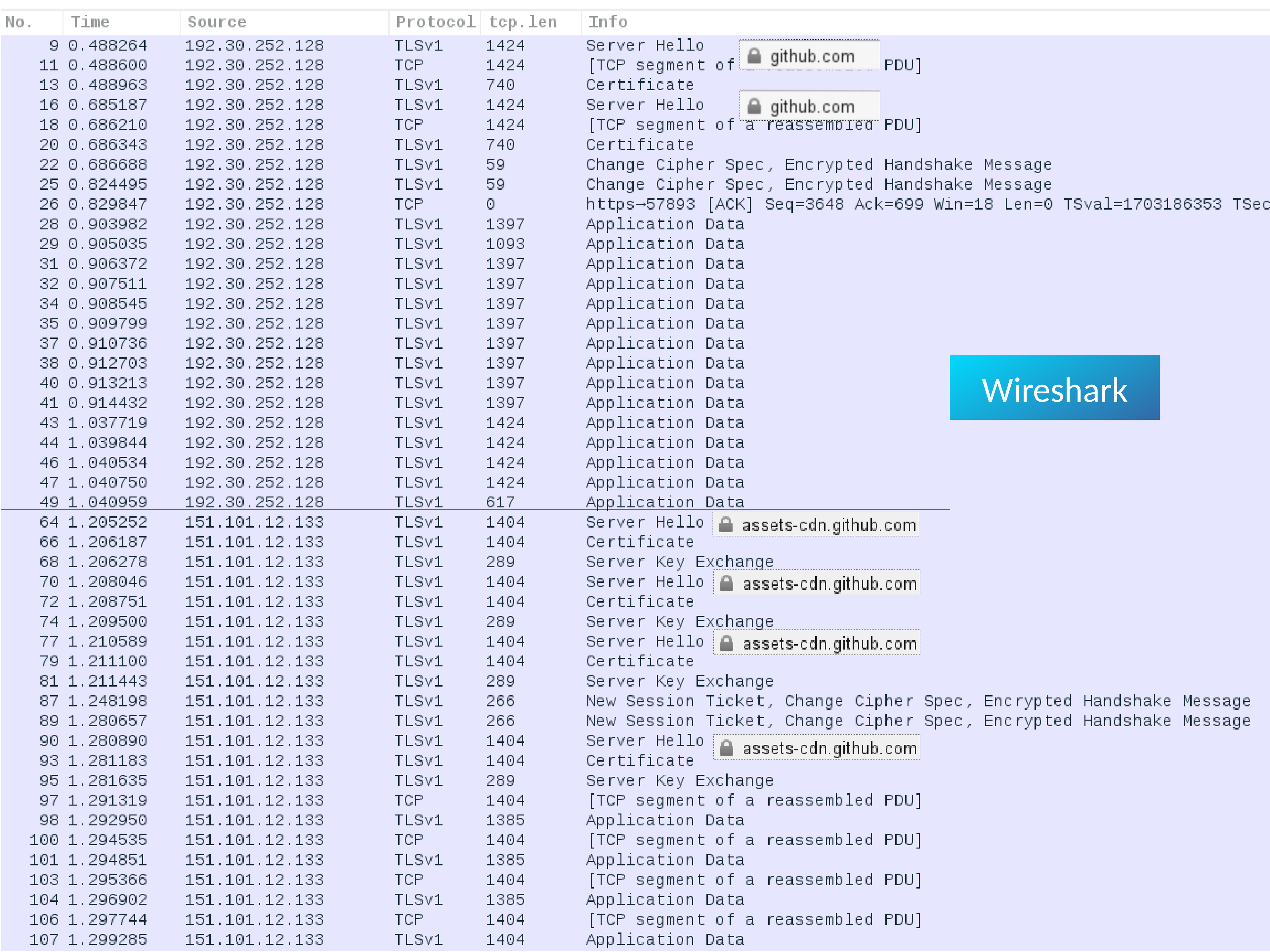
browser:getting worse

- **Developer-Konsole**

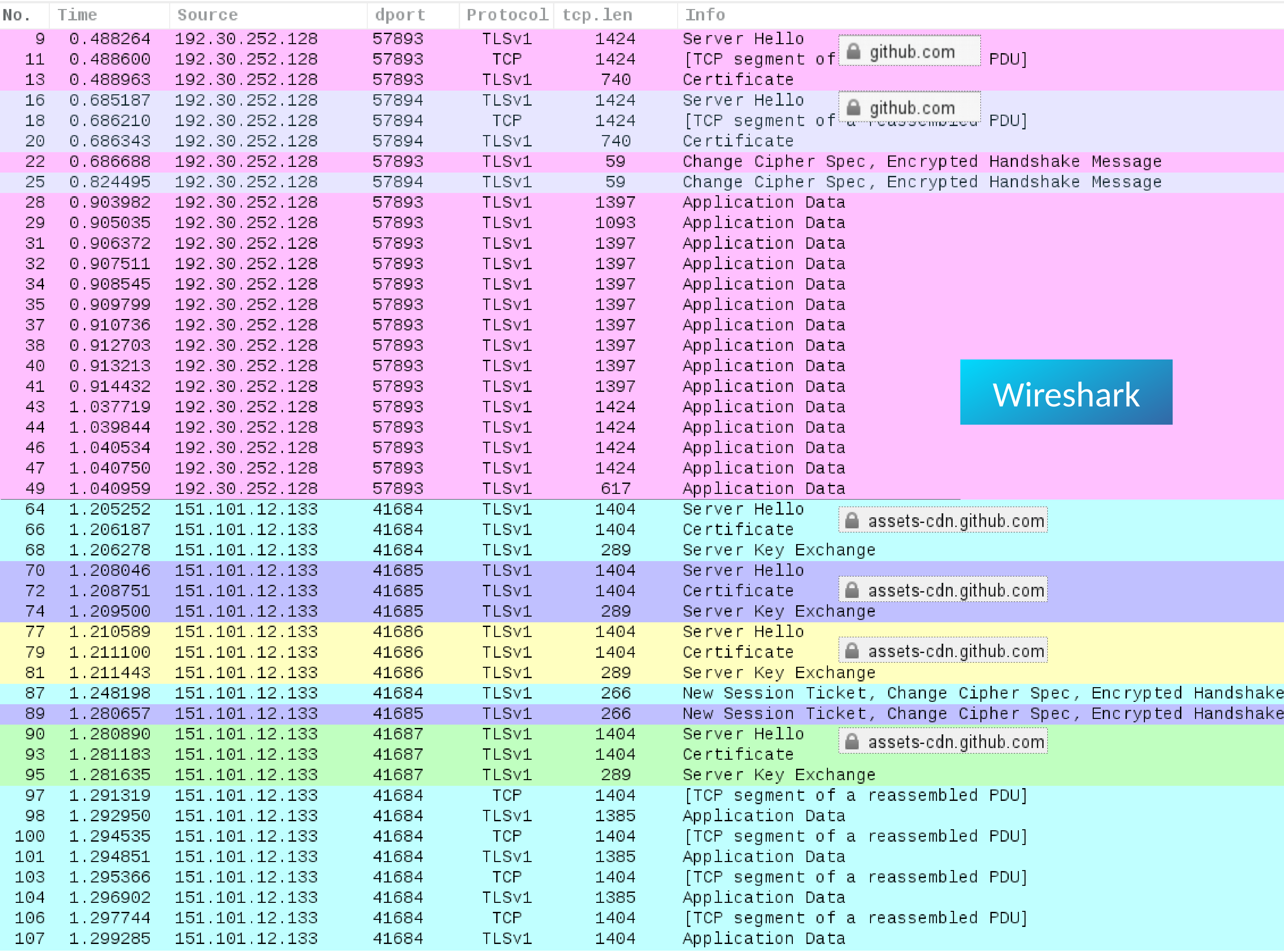


✓	Method	File	Domain	Type	Transferred	Size	0 ms 1.28 s 2.56 s 3.84 s
[redacted]	[redacted]	[redacted]	🔒 github.com	[redacted]	14.89 KB	[redacted]	→ 672 ms
[redacted]	[redacted]	[redacted]	🔒 assets-cdn.github.com	[redacted]	44.41 KB	[redacted]	→ 251 ms
[redacted]	[redacted]	[redacted]	🔒 assets-cdn.github.com	[redacted]	58.03 KB	[redacted]	→ 331 ms
[redacted]	[redacted]	[redacted]	🔒 assets-cdn.github.com	[redacted]	73.31 KB	[redacted]	→ 505 ms
[redacted]	[redacted]	[redacted]	🔒 assets-cdn.github.com	[redacted]	115.79 KB	[redacted]	→ 632 ms
[redacted]	[redacted]	[redacted]	🔒 avatars1.githubusercont...	[redacted]	1.55 KB	[redacted]	→ 465 ms
[redacted]	[redacted]	[redacted]	🔒 assets-cdn.github.com	[redacted]	2.26 KB	[redacted]	→ 458 ms
[redacted]	[redacted]	[redacted]	🔒 camo.githubusercontent...	[redacted]	0.65 KB	[redacted]	→ 308 ms
[redacted]	[redacted]	[redacted]	🔒 github.com	[redacted]	0.17 KB	[redacted]	→ 177 ms
[redacted]	[redacted]	[redacted]	🔒 collector-cdn.github.com	[redacted]	2.82 KB	[redacted]	→ 134 ms
[redacted]	[redacted]	[redacted]	🔒 assets-cdn.github.com	[redacted]	3.94 KB	[redacted]	→ 62 ms
[redacted]	[redacted]	[redacted]	🔒 github.com	[redacted]	0.08 KB	[redacted]	→ 315 ms
[redacted]	[redacted]	[redacted]	🔒 live.github.com	[redacted]	—	[redacted]	→ 414 ms
[redacted]	[redacted]	[redacted]	🔒 collector.githubapp.com	[redacted]	0.03 KB	[redacted]	→ 424 ms
[redacted]	[redacted]	[redacted]	🔒 api.github.com	[redacted]	0 0.03 KB	[redacted]	→

?



```
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 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 a reassembled 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

🔒 github.com

🔒 github.com

Wireshark

🔒 assets-cdn.github.com

🔒 assets-cdn.github.com

🔒 assets-cdn.github.com

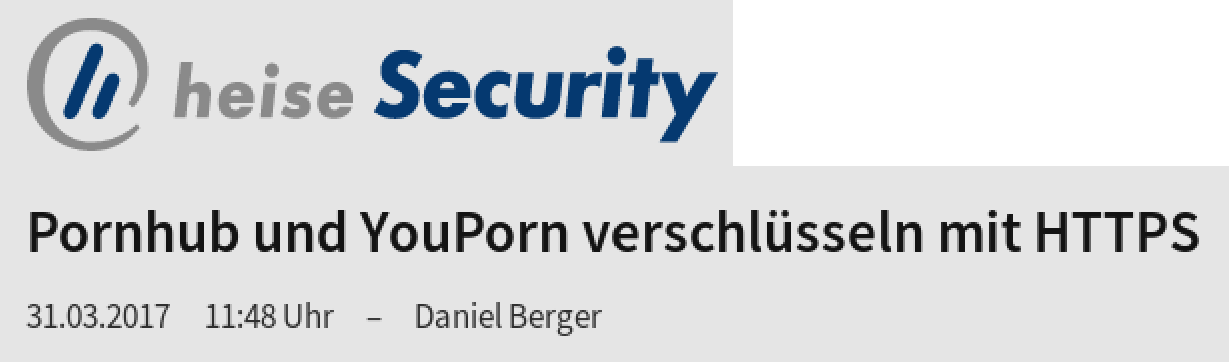
🔒 assets-cdn.github.com

browser:getting worse

- **Im Netz jedoch**
  - Länge sieht man nicht (MTU)
    - HTTP/1.1: pipelining
      - But: source port TCP
    - Keepalive
    - 304
    - Bzw....
  - SSL session ID / TLS session tickets

browser:getting worse

- **Im Netz jedoch**



heise Security

Pornhub und YouPorn verschlüsseln mit HTTPS

31.03.2017 11:48 Uhr – Daniel Berger

Der Besuch der Seite bleibe dank HTTPS "streng vertraulich". [..] Trotz HTTPS erfahren die Provider zwar weiterhin, ob ihre Kunden täglich Pornhub besuchen. Verborgen bleibt aber, was genau sie sich auf der Seite angeschaut haben.

- HTTP Layer: 206
  - TLS: Eine Verbindung
  - ∑ (Paketlängen-Overhead) = Nettolänge des Videos

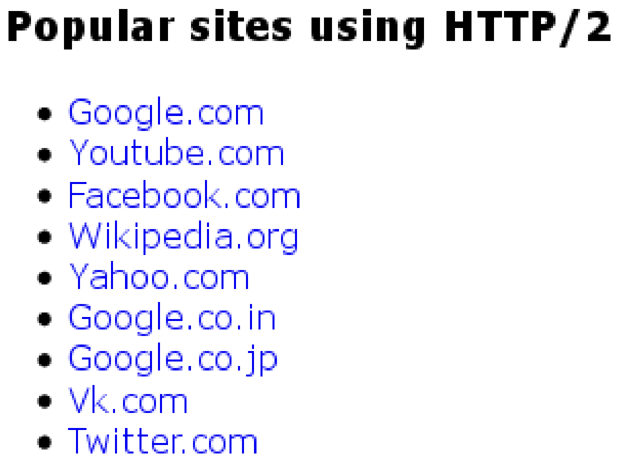
https://www.heise.de/security/meldung/Pornhub-und-YouPorn-verschluesseln-mit-HTTPS-3672189.html

browser:getting worse

- **Im Netz jedoch**
  - Länge sieht man nicht (MTU)
    - HTTP/1.1: pipelining
      - But: source port TCP
    - Keepalive
    - 304
    - Aber: HTTP 206-Problem
  - SSL session ID / TLS session tickets

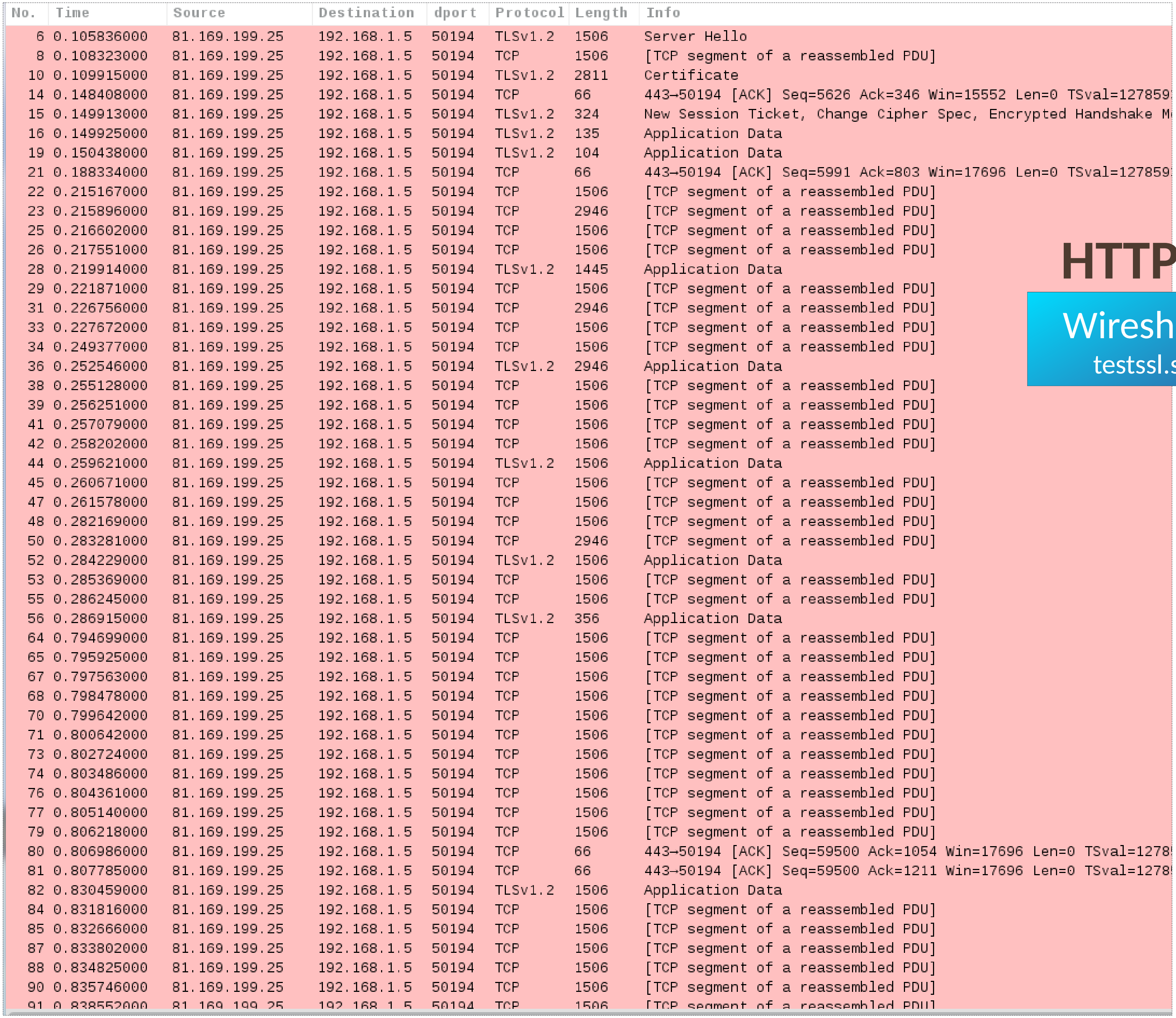
browser:slightlybetter

- **HTTP/2**
  - Leider noch wenig verbreitet
    - Internet traffic: 14.4% in 5/2017 (w3techs.com)
    - Per host count (trends.builtwith.com) 5/2017
      - 386k (~0.1%)
      - Top 100k: 165 (0.2%)



Popular sites using HTTP/2

- Google.com
- Youtube.com
- Facebook.com
- Wikipedia.org
- Yahoo.com
- Google.co.in
- Google.co.jp
- Vk.com
- Twitter.com



```
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]
```

HTTP/2!

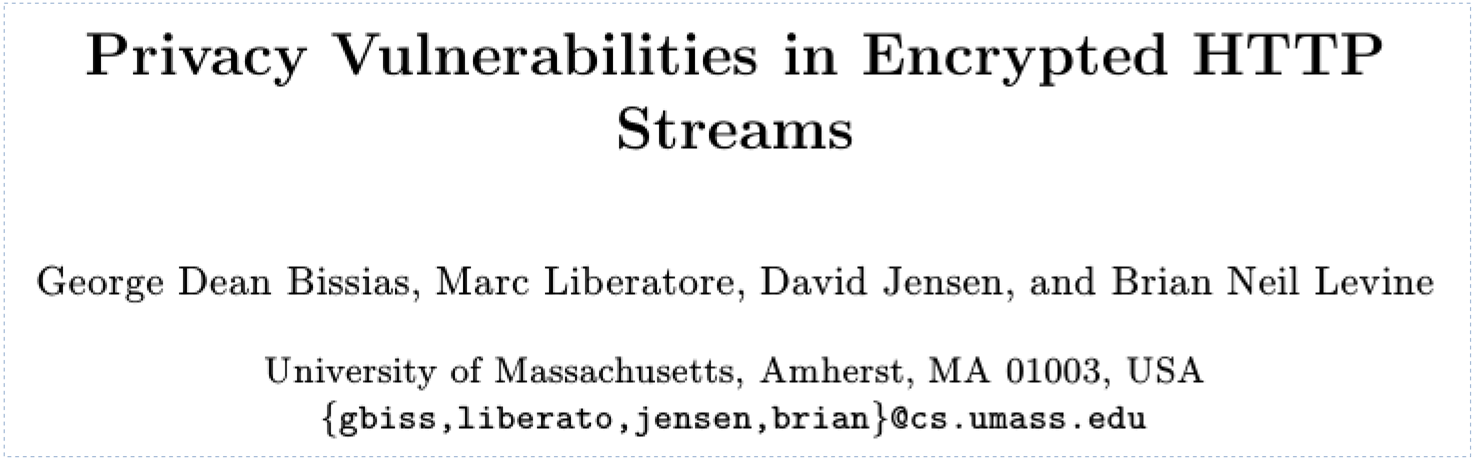
Wireshark
testssl.sh

server:URL

- **Forschung**
  - WF / WPF = website fingerprinting!

    Wikipedia: *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*
  - Zuverlässigkeit Gegenstand von Diskussionen
  - HTTP/1.1 only

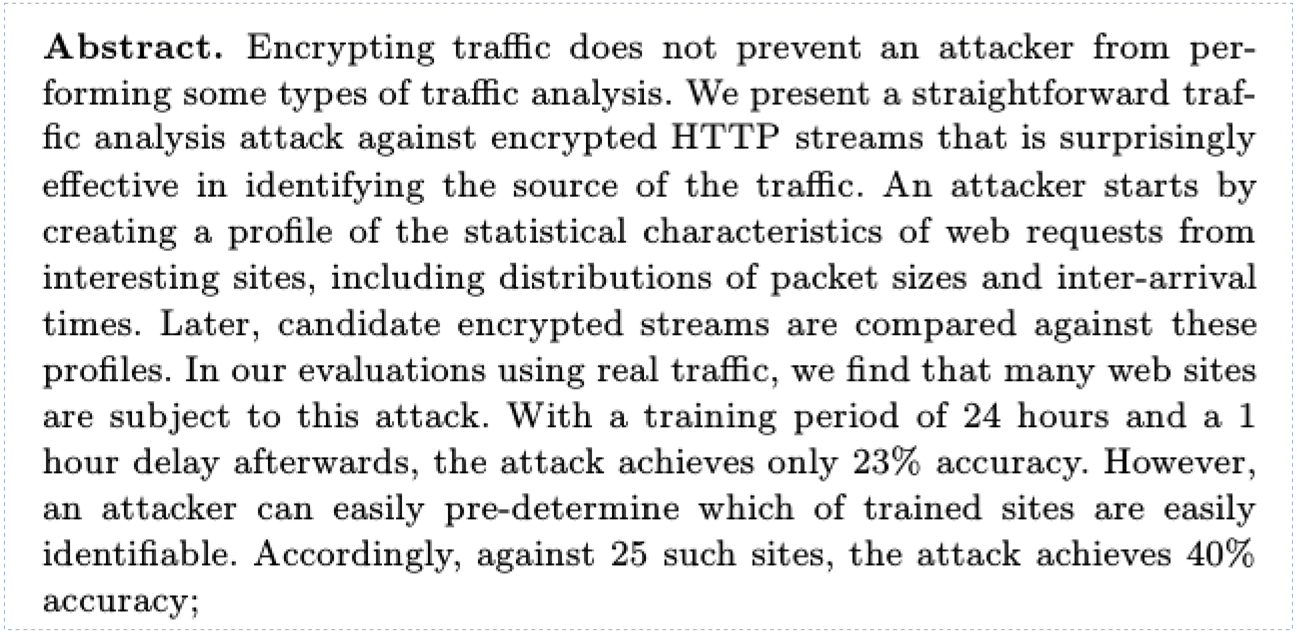
server:URL



Privacy Vulnerabilities in Encrypted HTTP Streams

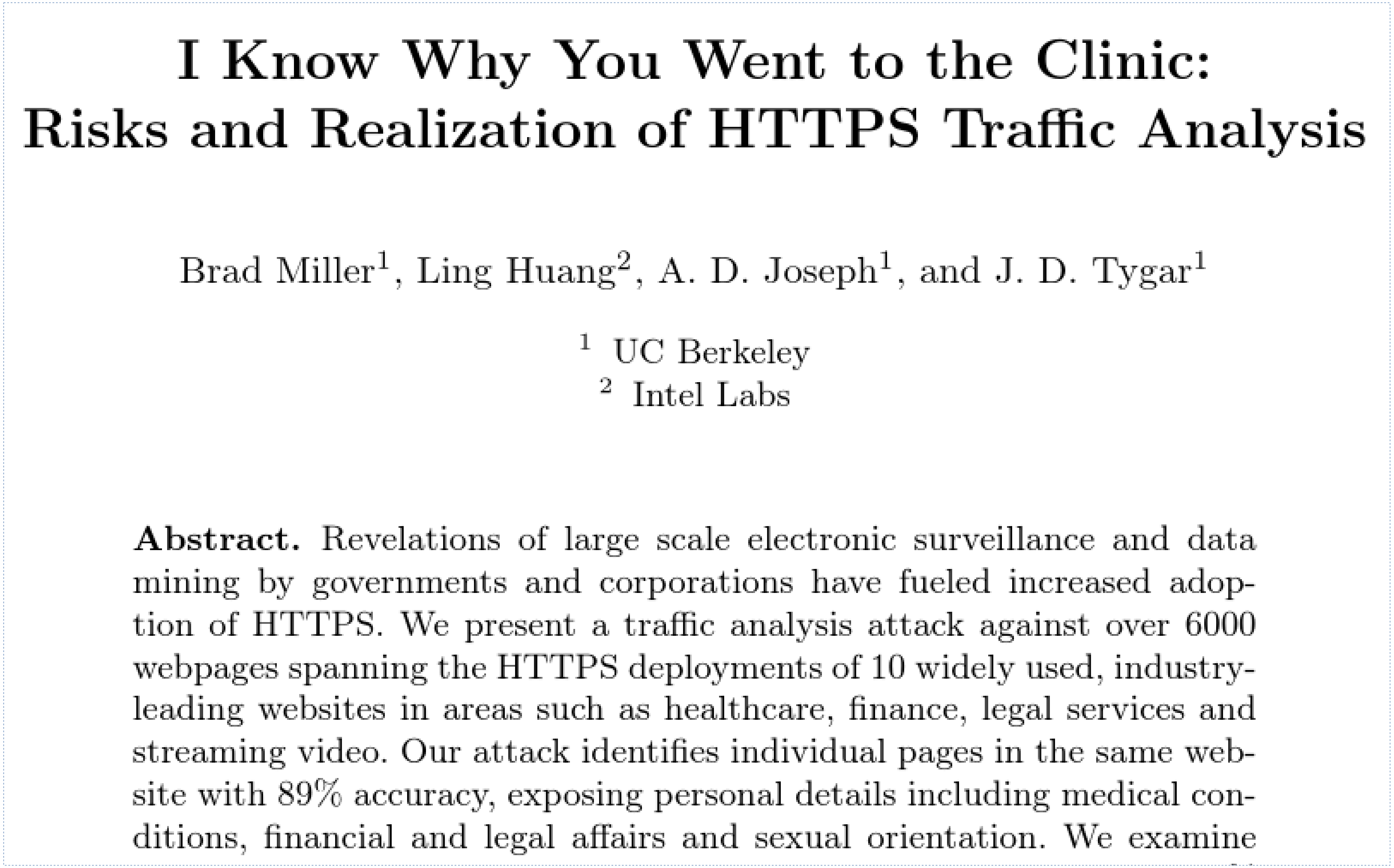
George Dean Bissias, Marc Liberatore, David Jensen, and Brian Neil Levine

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



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

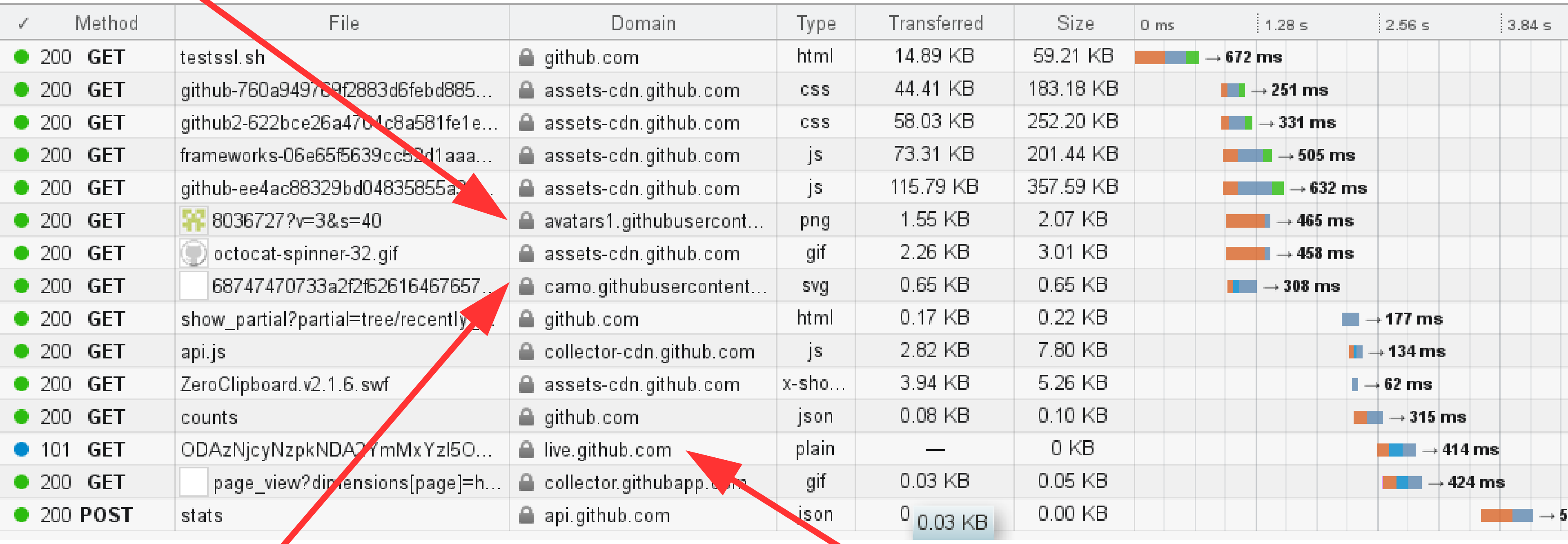
Brad Miller[1], Ling Huang[2], A. D. Joseph[1], and J. D. Tygar[1]

[1] UC Berkeley
[2] Intel Labs

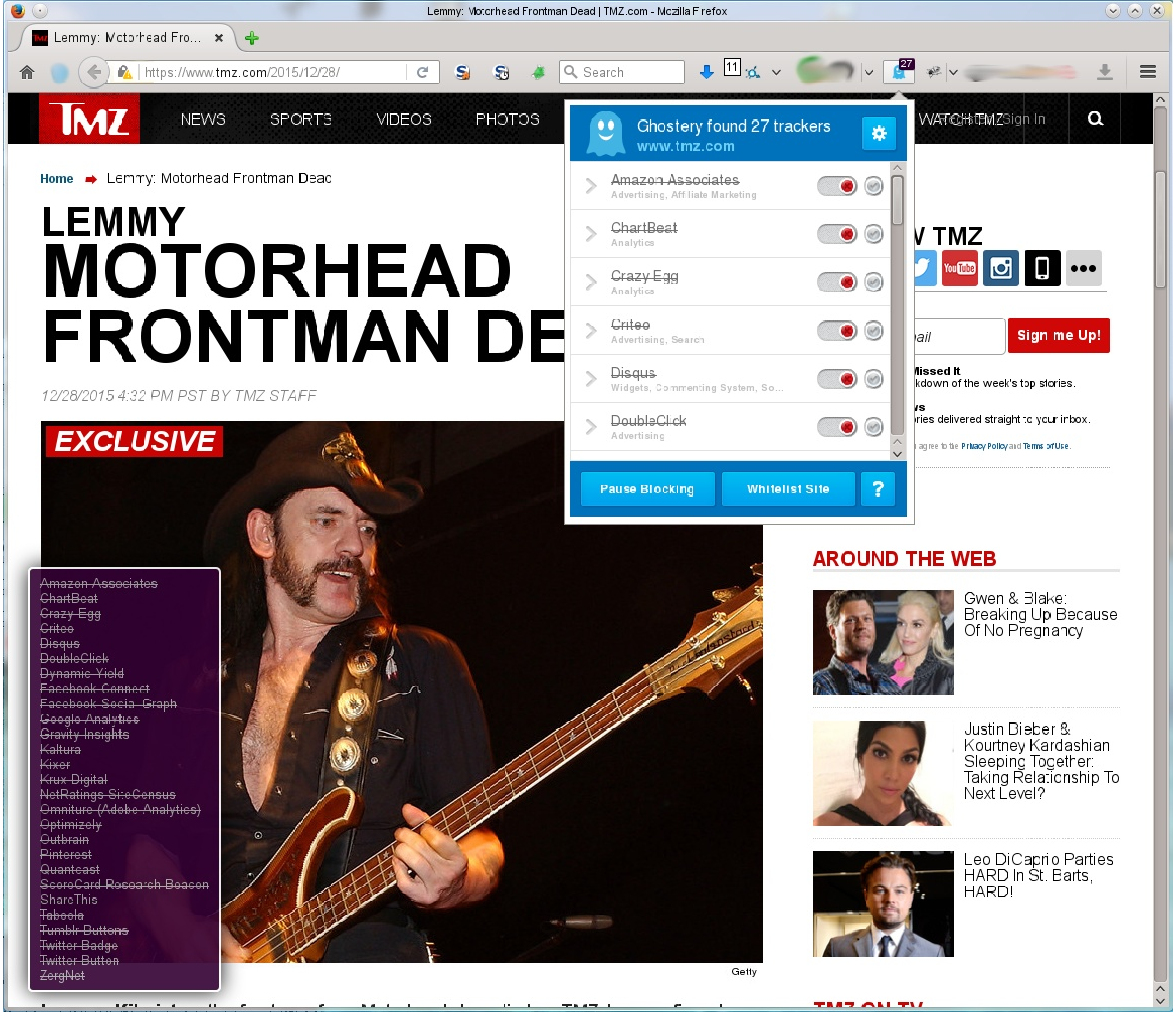
Abstract. Revelations of large scale electronic surveillance and data mining by governments and corporations have fueled increased adoption of HTTPS. We present a traffic analysis attack against over 6000 webpages spanning the HTTPS deployments of 10 widely used, industry-leading websites in areas such 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

browser:TLS layer

- **Dritte**



✓	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-760a949769f2883d6febd885…	assets-cdn.github.com	css	44.41 KB	183.18 KB	→ 251 ms
● 200	GET	github2-622bce26a4704c8a581fe1e…	assets-cdn.github.com	css	58.03 KB	252.20 KB	→ 331 ms
● 200	GET	frameworks-06e65f5639cc52d1aaa…	assets-cdn.github.com	js	73.31 KB	201.44 KB	→ 505 ms
● 200	GET	github-ee4ac88329bd04835855a3…	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_…	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	ODAzNjcyNzpkNDA2YmMxYzI5O…	live.github.com	plain	—	0 KB	→ 414 ms
● 200	GET	page_view?dimensions[page]=h…	collector.githubapp.com	gif	0.03 KB	0.05 KB	→ 424 ms
● 200	POST	stats	api.github.com	json	0 0.03 KB	0.00 KB	→ 5



Lemmy: Motorhead Frontman Dead | TMZ.com - Mozilla Firefox
Lemmy: Motorhead Fro...
https://www.tmz.com/2015/12/28/
Search
27
NEWS
SPORTS
VIDEOS
PHOTOS
WATCH TMZ
Sign In

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

Home ➡ Lemmy: Motorhead Frontman Dead

LEMMY
MOTORHEAD
FRONTMAN DE

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

~~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~~

Missed It
kdown of the week's top stories.
rs
ries delivered straight to your inbox.
agree to the Privacy Policy and Terms of Use.

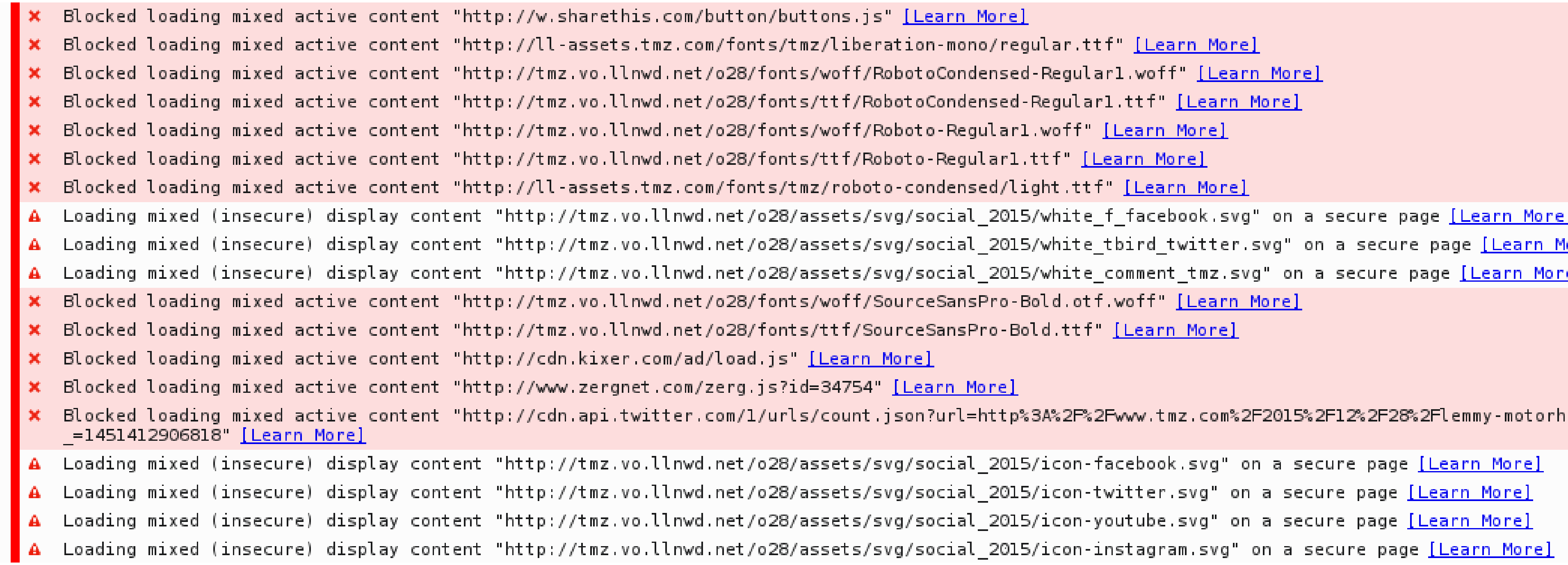
AROUND THE WEB

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!

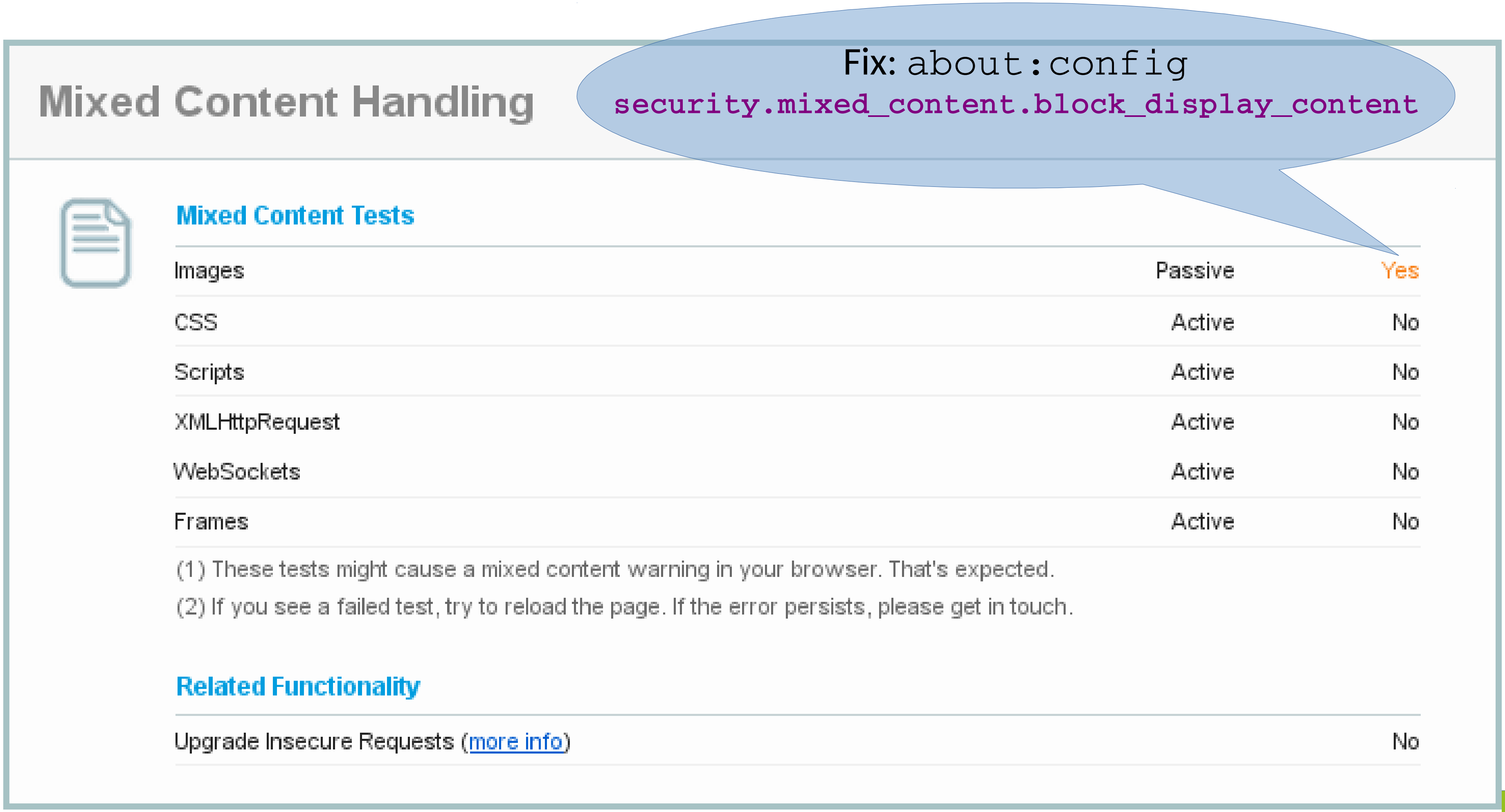
pest:oftheinternet



```
✖  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 Mo
⚠  Loading mixed (insecure) display content "http://tmz.vo.llnwd.net/o28/assets/svg/social_2015/white_comment_tmz.svg" on a secure page [Learn More
✖  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:



Fix: `about:config` `security.mixed_content.block_display_content`

Mixed Content Handling

Mixed Content Tests

Images	Passive	Yes
CSS	Active	No
Scripts	Active	No
XMLHttpRequest	Active	No
WebSockets	Active	No
Frames	Active	No

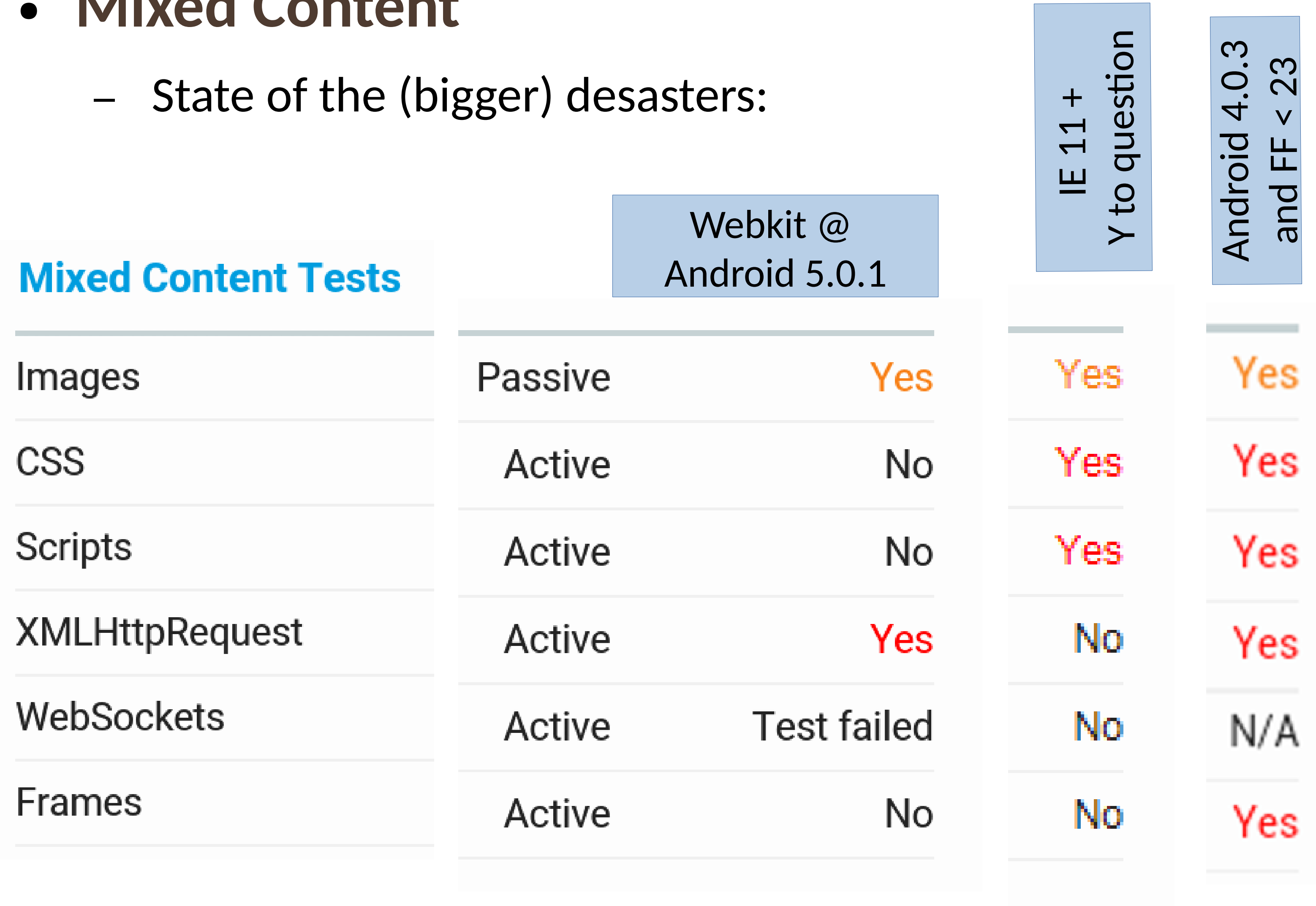
(1) These tests might cause a mixed content warning in your browser. That's expected.

(2) If you see a failed test, try to reload the page. If the error persists, please get in touch.

Related Functionality

Upgrade Insecure Requests (more info)	No

- **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:xkeyscore

- **Anteil TLS / Klartext für HTTP**
  - Keine 100% (EFF: gut 50% in 2/2017)

  - Klartext grundsätzlich schlimmer
    - User-Agent

      [..] Android 7.0; SM-G935F Build/NRD90M [..] Chrome/58.0.3029.83 [..]
    - Plugins
    - Canvas Size
    - Mobile Sensoren
      - Fingerabdruck, Kamera, Mikro, GPS, Barometer, Temperatur (2-4x), Luftfeuchte, Beschleunigung, Gyroskop, Magnetfeld, Kompass, Schall, ...

- **Eve: Korrelation TLS/Klartext**

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

take:aways

- **Bottom line**
  - **Dinge sind komplizierter, als man denkt…**
  - Verschlüssele wegen
    - C)onfidentiality, I)ntegrity, A)vailability
    - Kann nicht schaden auch wegen Privatsphäre
  - Aber: **HTTPS ist kein VPN**
    - Eve sieht immer Metadaten
    - Eve kann mehr
      - Welche Pornos
      - Tracker
      - Mixed Content
      - Web site fingerprinting
    - Korreliert mit unverschlüsseltem Traffic

take:aways

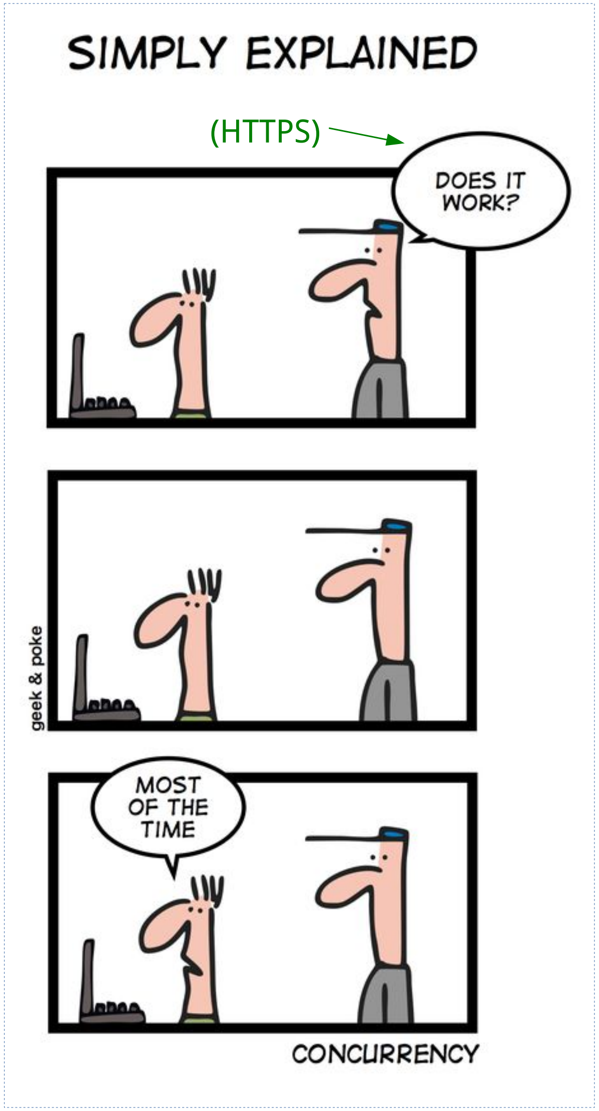
- **Bottom line, cont‘d**
  - Server:
    - Properly rotate away & anonymize logs
    - Benutze OCSP stapling
    - HTTP/2 in Kombination mit TLS
    - Benutze keine Tracker von Dritten

- **Danke**

  dirk at

  - drwetter eu
  - testssl sh

@drwetter



Geek & Poke (Oliver Widder)