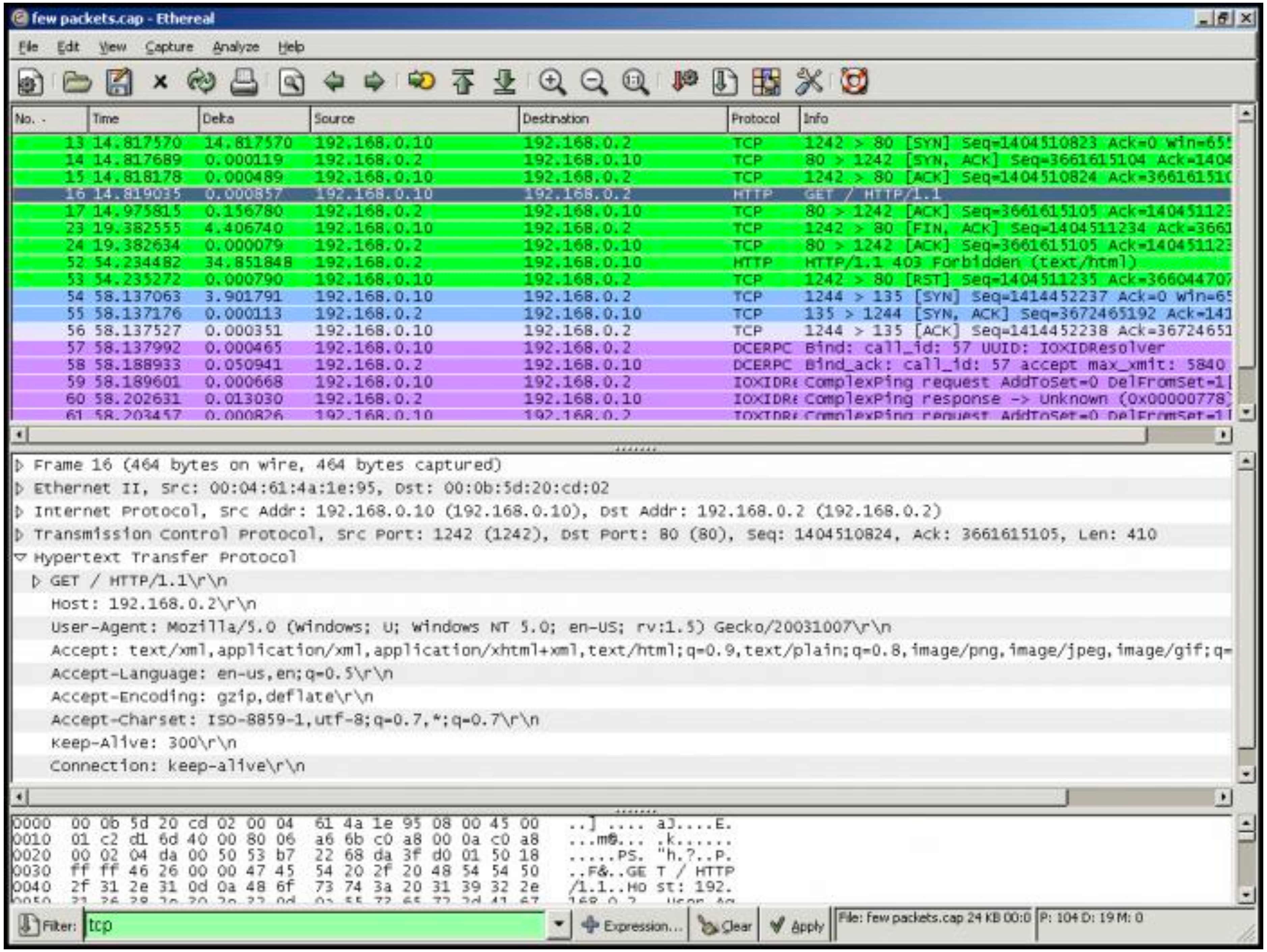
Winning At

HTTPS

WHY?

NATIONAL SECURITY AGENCY
PEEPING WHILE YOU'RE SLEEPING
The NSA
The only part of government that actually listens.

Why?



```
No. -  Time       Delta      Source        Destination   Protocol Info
    13 14.817570  14.817570  192.168.0.10  192.168.0.2   TCP      1242 > 80 [SYN] Seq=1404510823 Ack=0 Win=65
    14 14.817689  0.000119   192.168.0.2   192.168.0.10  TCP      80 > 1242 [SYN, ACK] Seq=3661615104 Ack=1404
    15 14.818178  0.000489   192.168.0.10  192.168.0.2   TCP      1242 > 80 [ACK] Seq=1404510824 Ack=36616151
    16 14.819035  0.000857   192.168.0.10  192.168.0.2   HTTP     GET / HTTP/1.1
    17 14.975815  0.156780   192.168.0.2   192.168.0.10  TCP      80 > 1242 [ACK] Seq=3661615105 Ack=14045112
    23 19.382555  4.406740   192.168.0.10  192.168.0.2   TCP      1242 > 80 [FIN, ACK] Seq=1404511234 Ack=3661
    24 19.382634  0.000079   192.168.0.2   192.168.0.10  TCP      80 > 1242 [ACK] Seq=3661615105 Ack=14045112
    52 54.234482  34.851848  192.168.0.2   192.168.0.10  HTTP     HTTP/1.1 403 Forbidden (text/html)
    53 54.235272  0.000790   192.168.0.10  192.168.0.2   TCP      1242 > 80 [RST] Seq=1404511235 Ack=36604470
    54 58.137063  3.901791   192.168.0.10  192.168.0.2   TCP      1244 > 135 [SYN] Seq=1414452237 Ack=0 Win=65
    55 58.137176  0.000113   192.168.0.2   192.168.0.10  TCP      135 > 1244 [SYN, ACK] Seq=3672465192 Ack=141
    56 58.137527  0.000351   192.168.0.10  192.168.0.2   TCP      1244 > 135 [ACK] Seq=1414452238 Ack=36724651
    57 58.137992  0.000465   192.168.0.10  192.168.0.2   DCERPC   Bind: call_id: 57 UUID: IOXIDResolver
    58 58.188933  0.050941   192.168.0.2   192.168.0.10  DCERPC   Bind_ack: call_id: 57 accept max_xmit: 5840
    59 58.189601  0.000668   192.168.0.10  192.168.0.2   IOXIDRe  ComplexPing request AddToSet=0 DelFromSet=1[
    60 58.202631  0.013030   192.168.0.2   192.168.0.10  IOXIDRe  ComplexPing response -> Unknown (0x00000778)
    61 58.203457  0.000826   192.168.0.10  192.168.0.2   IOXIDRe  ComplexPing request AddToSet=0 DelFromSet=1[
```

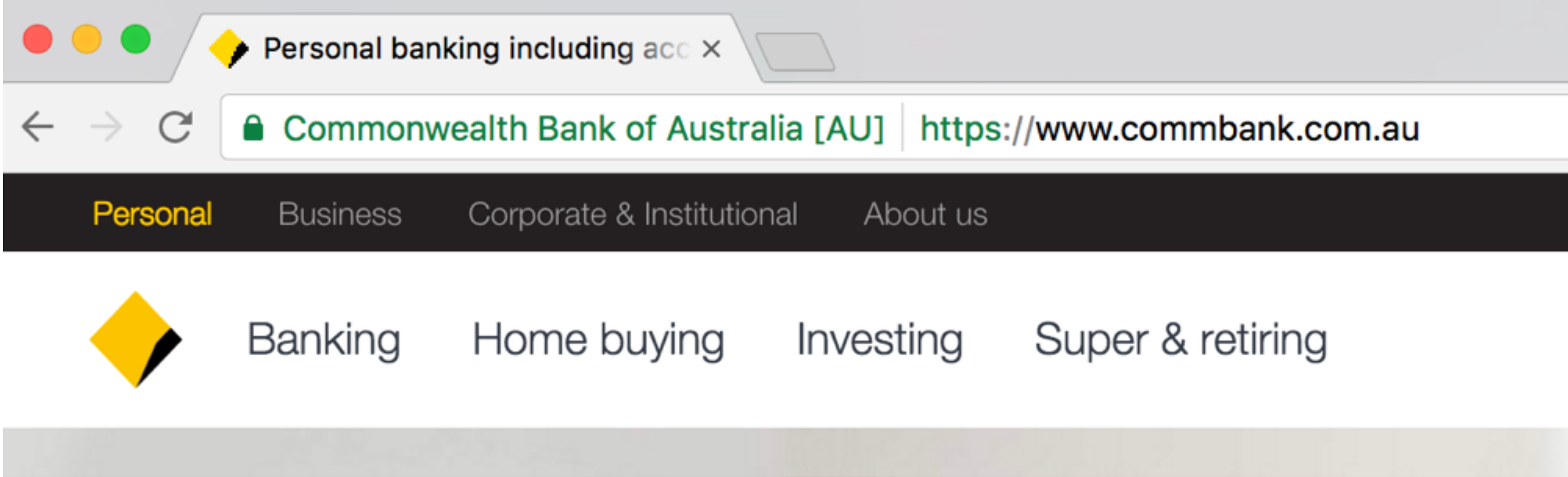
```
▷ Frame 16 (464 bytes on wire, 464 bytes captured)
▷ Ethernet II, Src: 00:04:61:4a:1e:95, Dst: 00:0b:5d:20:cd:02
▷ Internet Protocol, Src Addr: 192.168.0.10 (192.168.0.10), Dst Addr: 192.168.0.2 (192.168.0.2)
▷ Transmission Control Protocol, Src Port: 1242 (1242), Dst Port: 80 (80), Seq: 1404510824, Ack: 3661615105, Len: 410
▽ Hypertext Transfer Protocol
  ▷ GET / HTTP/1.1\r\n
    Host: 192.168.0.2\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.0; en-US; rv:1.5) Gecko/20031007\r\n
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,image/jpeg,image/gif;q=
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
```

```
0000   00 0b 5d 20 cd 02 00 04   61 4a 1e 95 08 00 45 00    ..] .... aJ....E.
0010   01 c2 d1 6d 40 00 80 06   a6 6b c0 a8 00 0a c0 a8    ...m@... .k......
0020   00 02 04 da 00 50 53 b7   22 68 da 3f d0 01 50 18    .....PS. "h.?..P.
0030   ff ff 46 26 00 00 47 45   54 20 2f 20 48 54 54 50    ..F&..GE T / HTTP
0040   2f 31 2e 31 0d 0a 48 6f   73 74 3a 20 31 39 32 2e    /1.1..Ho st: 192.
0050   31 36 38 2e 30 2e 32 0d   0a 55 73 65 72 2d 41 67    168.0.2. .User-Ag
```

Filter: tcp

File: few packets.cap 24 KB 00:0 | P: 104 D: 19 M: 0

Wireshark, TCPDump, Ethereal… etc



Personal banking including acc ×

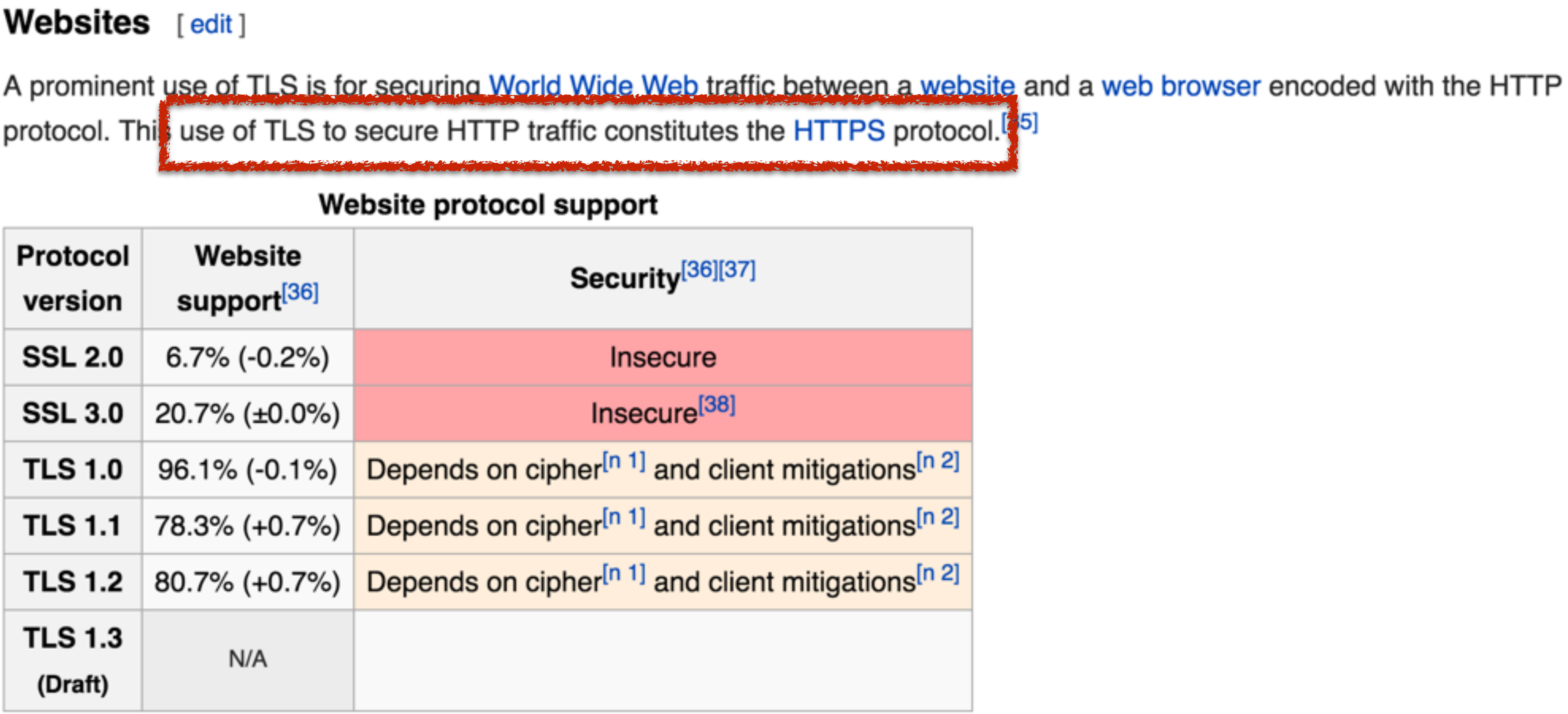
Commonwealth Bank of Australia [AU] https://www.commbank.com.au

Personal Business Corporate & Institutional About us

Banking Home buying Investing Super & retiring

Google

WHAT?

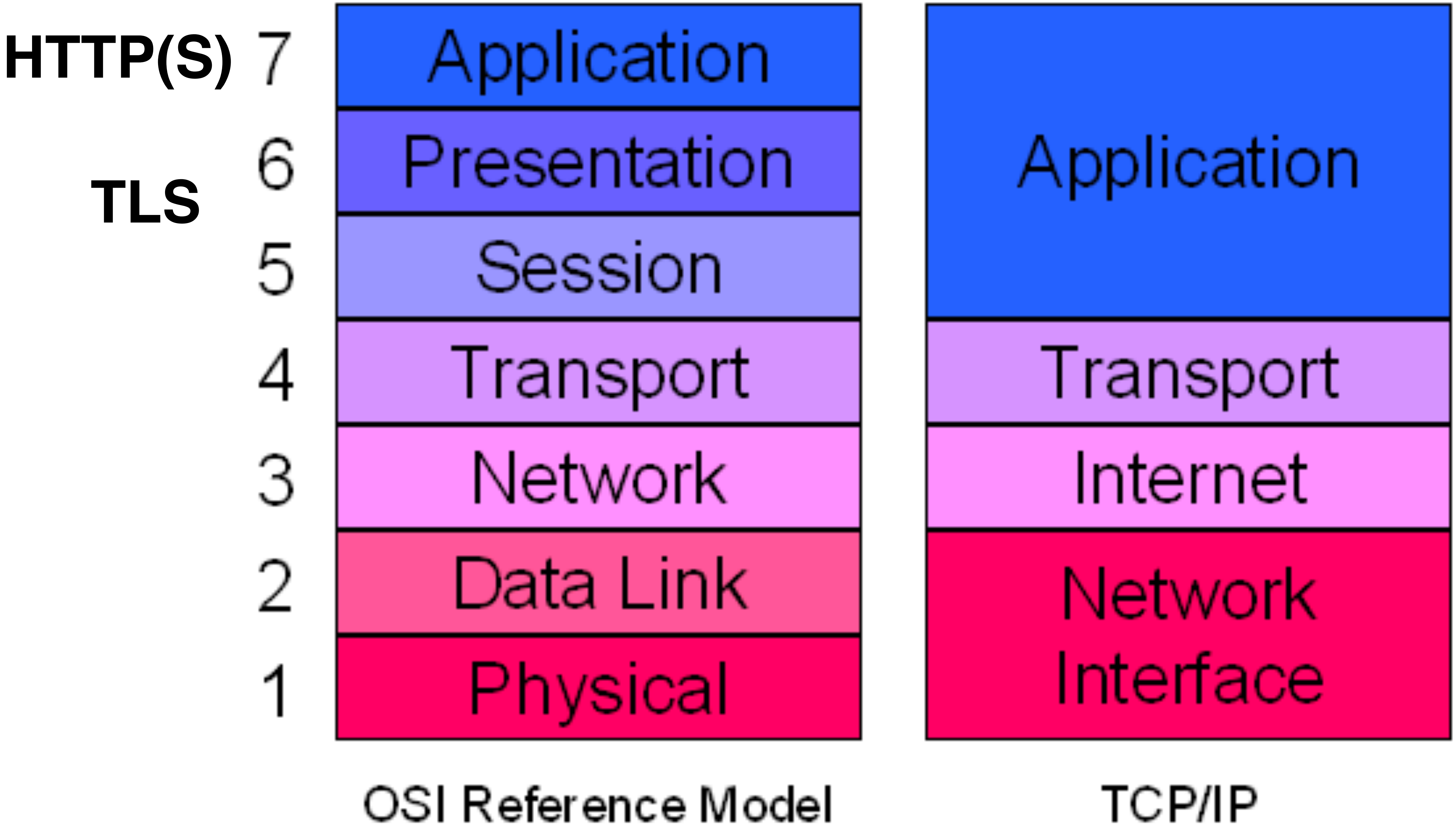


Websites [edit]

A prominent use of TLS is for securing World Wide Web traffic between a website and a web browser encoded with the HTTP protocol. This use of TLS to secure HTTP traffic constitutes the HTTPS protocol.[35]

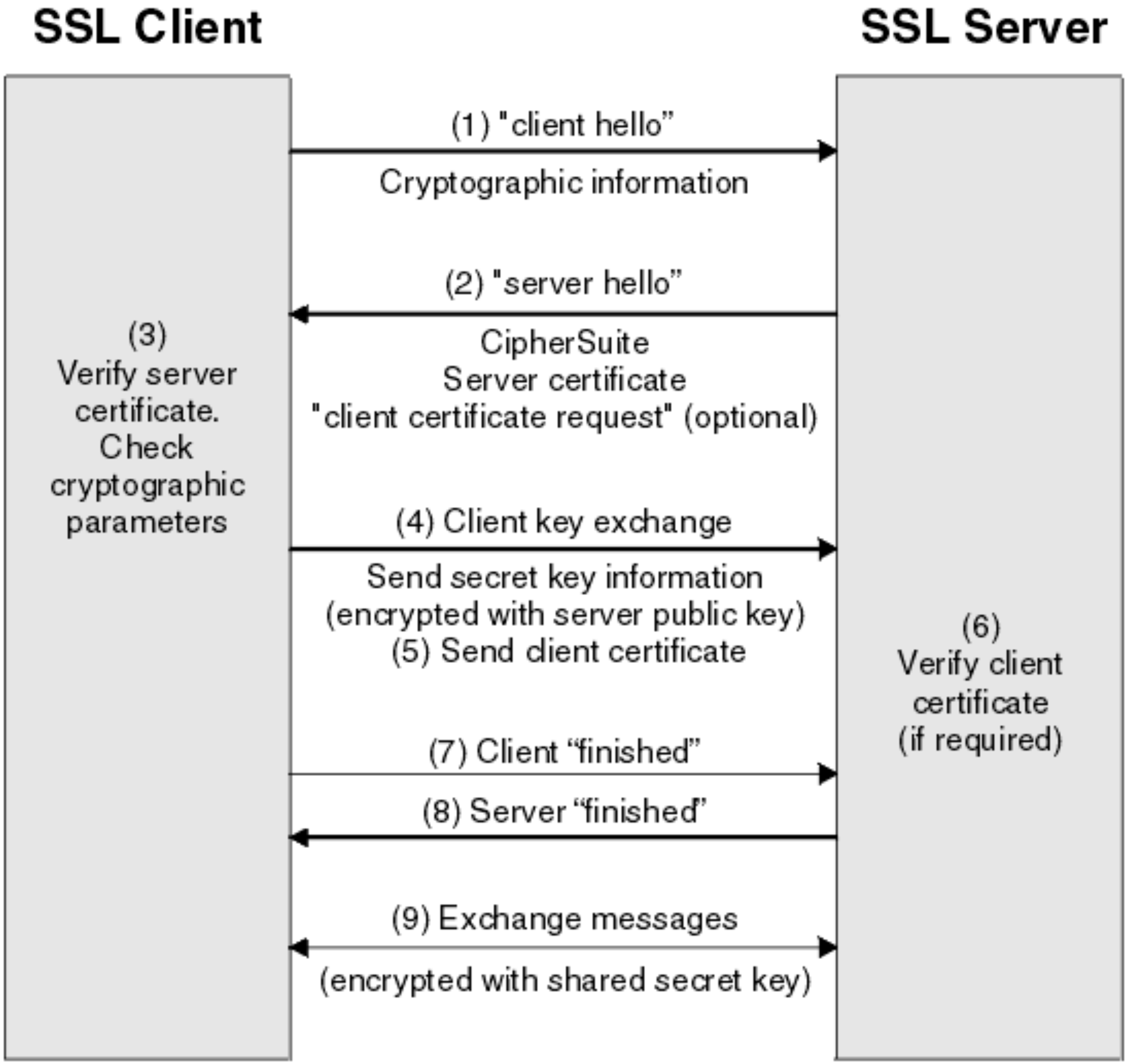
Website protocol support

Protocol version	Website support[36]	Security[36][37]
SSL 2.0	6.7% (-0.2%)	Insecure
SSL 3.0	20.7% (±0.0%)	Insecure[38]
TLS 1.0	96.1% (-0.1%)	Depends on cipher[n 1] and client mitigations[n 2]
TLS 1.1	78.3% (+0.7%)	Depends on cipher[n 1] and client mitigations[n 2]
TLS 1.2	80.7% (+0.7%)	Depends on cipher[n 1] and client mitigations[n 2]
TLS 1.3 (Draft)	N/A	



		OSI Reference Model	TCP/IP
HTTP(S)	7	Application	Application
TLS	6	Presentation	
	5	Session	
	4	Transport	Transport
	3	Network	Internet
	2	Data Link	Network Interface
	1	Physical	

:443



SSL Client

SSL Server

(1) "client hello"

Cryptographic information

(2) "server hello"

CipherSuite
Server certificate
"client certificate request" (optional)

(3)
Verify server
certificate.
Check
cryptographic
parameters

(4) Client key exchange

Send secret key information
(encrypted with server public key)
(5) Send client certificate

(6)
Verify client
certificate
(if required)

(7) Client "finished"

(8) Server "finished"

(9) Exchange messages

(encrypted with shared secret key)

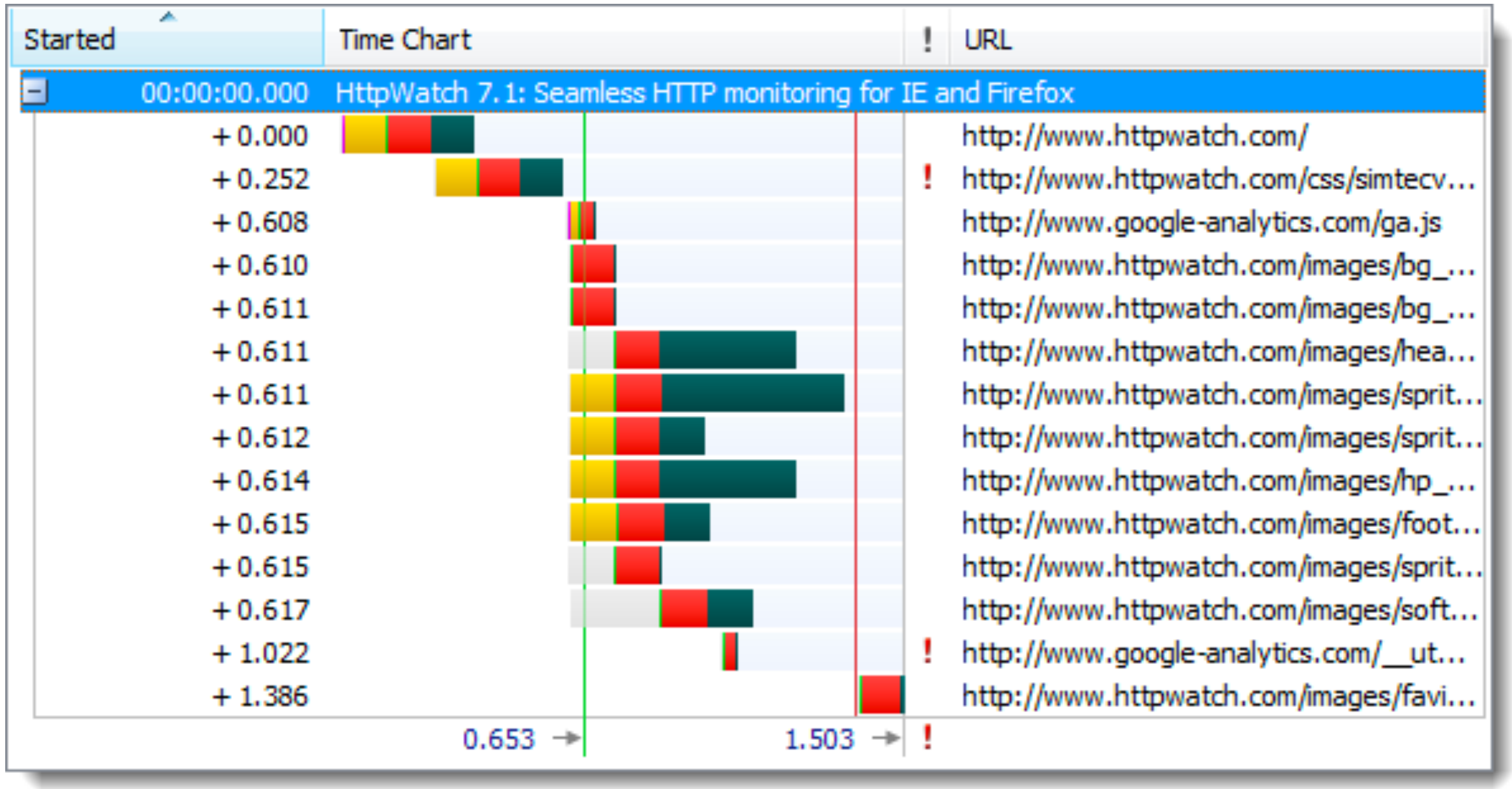
FAQ

Is HTTPS cached??

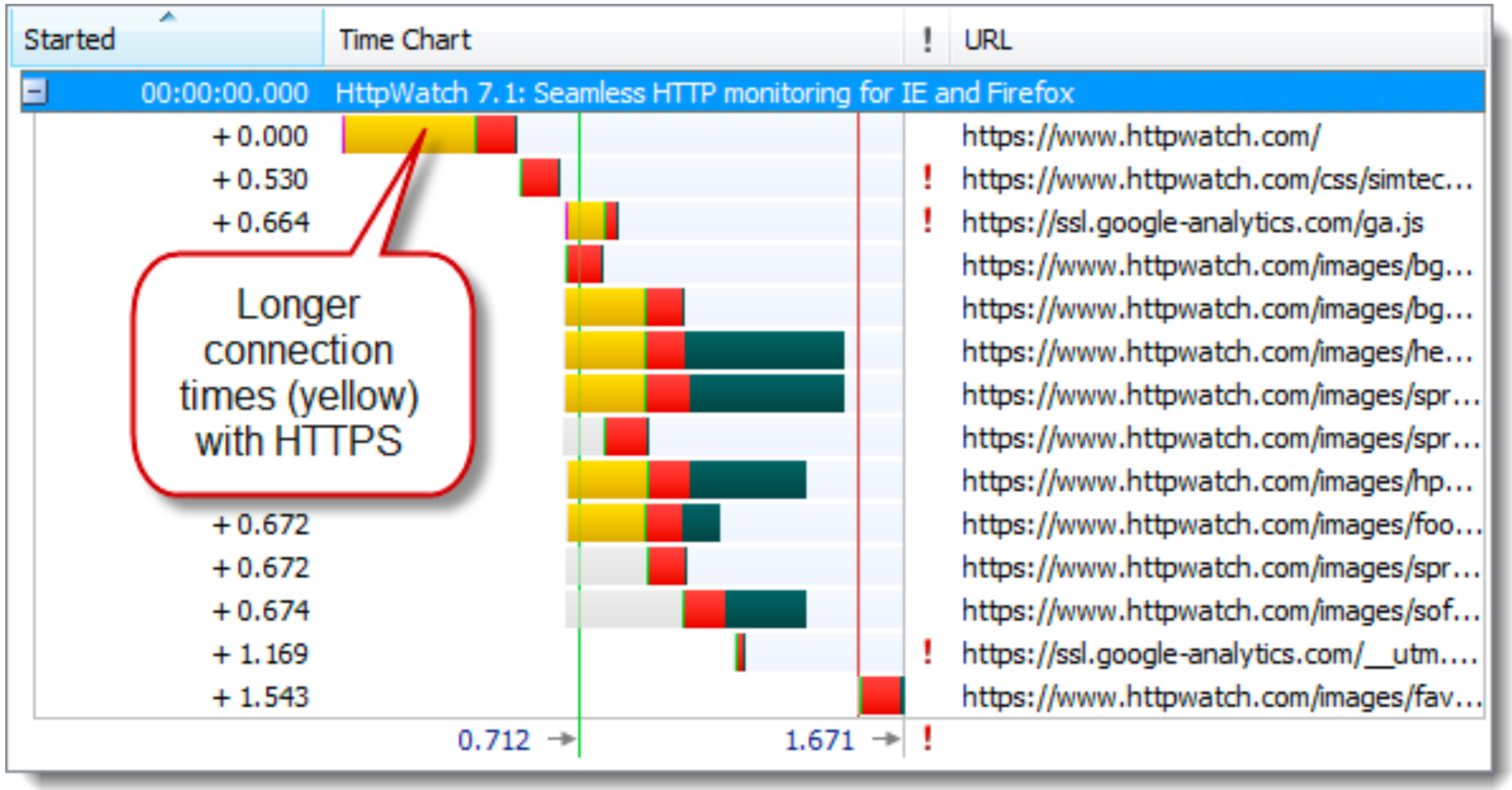
HTTPS hides metadata?

True or False

Are requests slower?

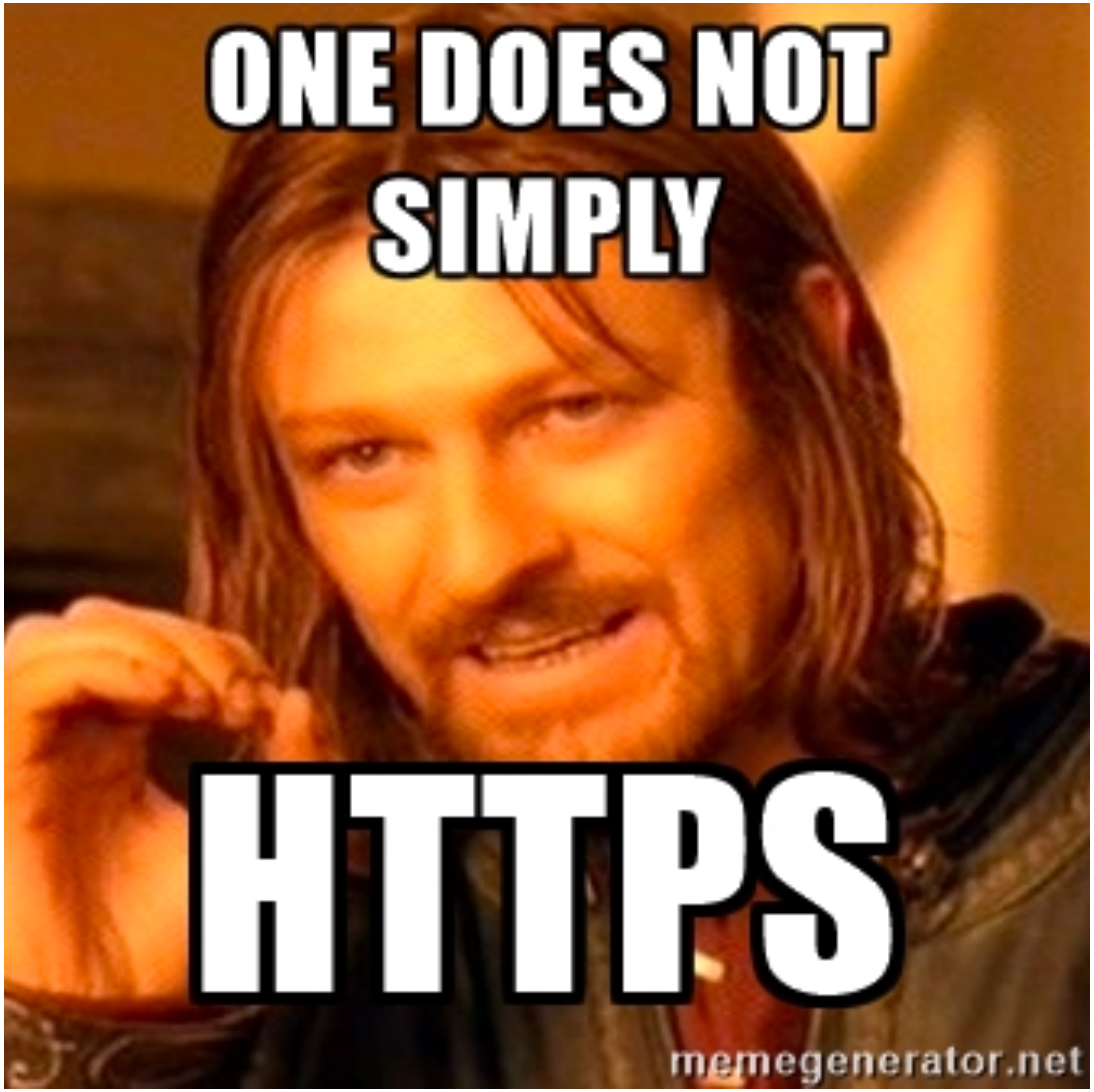


Started	Time Chart	!	URL
00:00:00.000	HttpWatch 7.1: Seamless HTTP monitoring for IE and Firefox		
+ 0.000			http://www.httpwatch.com/
+ 0.252		!	http://www.httpwatch.com/css/simtecv…
+ 0.608			http://www.google-analytics.com/ga.js
+ 0.610			http://www.httpwatch.com/images/bg_…
+ 0.611			http://www.httpwatch.com/images/bg_…
+ 0.611			http://www.httpwatch.com/images/hea…
+ 0.611			http://www.httpwatch.com/images/sprit…
+ 0.612			http://www.httpwatch.com/images/sprit…
+ 0.614			http://www.httpwatch.com/images/hp_…
+ 0.615			http://www.httpwatch.com/images/foot…
+ 0.615			http://www.httpwatch.com/images/sprit…
+ 0.617			http://www.httpwatch.com/images/soft…
+ 1.022		!	http://www.google-analytics.com/__ut…
+ 1.386			http://www.httpwatch.com/images/favi…
	0.653 → 1.503 →	!	



Started	Time Chart	!	URL
00:00:00.000	HttpWatch 7.1: Seamless HTTP monitoring for IE and Firefox		
+ 0.000			https://www.httpwatch.com/
+ 0.530		!	https://www.httpwatch.com/css/simtec…
+ 0.664		!	https://ssl.google-analytics.com/ga.js
			https://www.httpwatch.com/images/bg…
			https://www.httpwatch.com/images/bg…
			https://www.httpwatch.com/images/he…
			https://www.httpwatch.com/images/spr…
			https://www.httpwatch.com/images/spr…
			https://www.httpwatch.com/images/hp…
+ 0.672			https://www.httpwatch.com/images/foo…
+ 0.672			https://www.httpwatch.com/images/spr…
+ 0.674			https://www.httpwatch.com/images/sof…
+ 1.169		!	https://ssl.google-analytics.com/__utm.…
+ 1.543			https://www.httpwatch.com/images/fav…
	0.712 → 1.671 →	!	

Longer connection times (yellow) with HTTPS


ONE DOES NOT SIMPLY
HTTPS
memegenerator.net

Setup

Single name

mydomain.com

www.mydomain.com

Let’s Encrypt

certbot

Wildcard

*.bandcamp.com

$100-1000s

Multi-Domain SAN

mydomain.com

www.mydomain.com

random.com

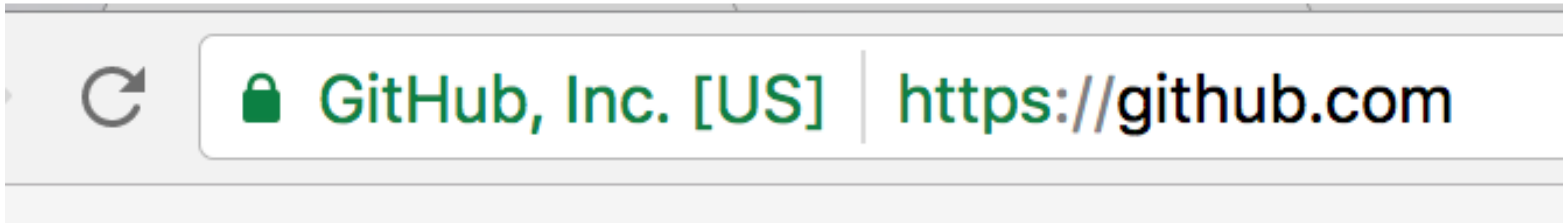
www.random.com

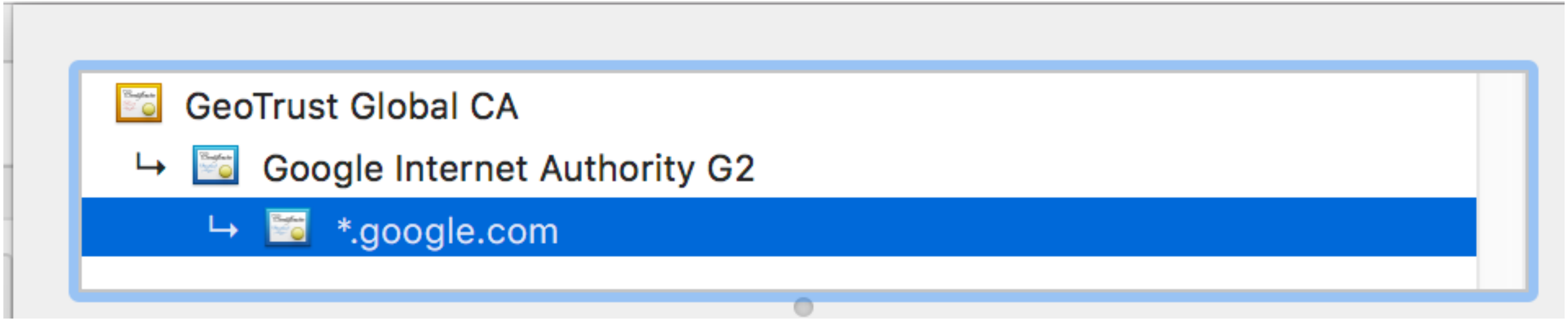
sub.random.com

$100-1000s

Validation Types

- Self Signed
- Domain Validated
- Organisation Validated
- EV (Extended Validation)

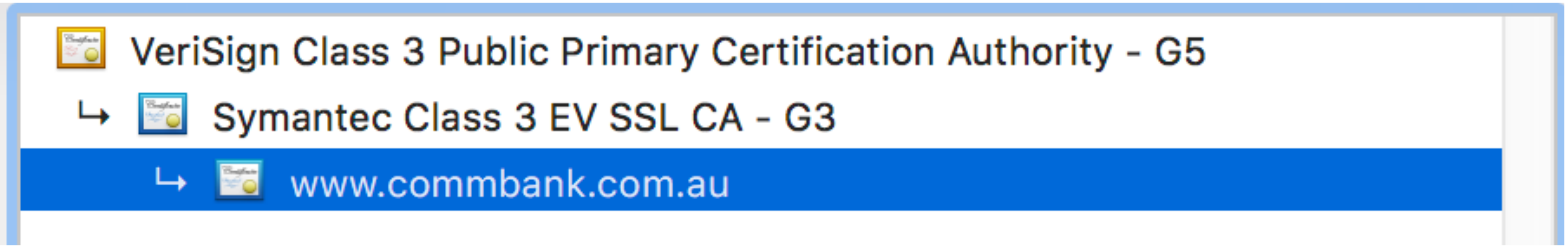




GeoTrust Global CA

↳ Google Internet Authority G2

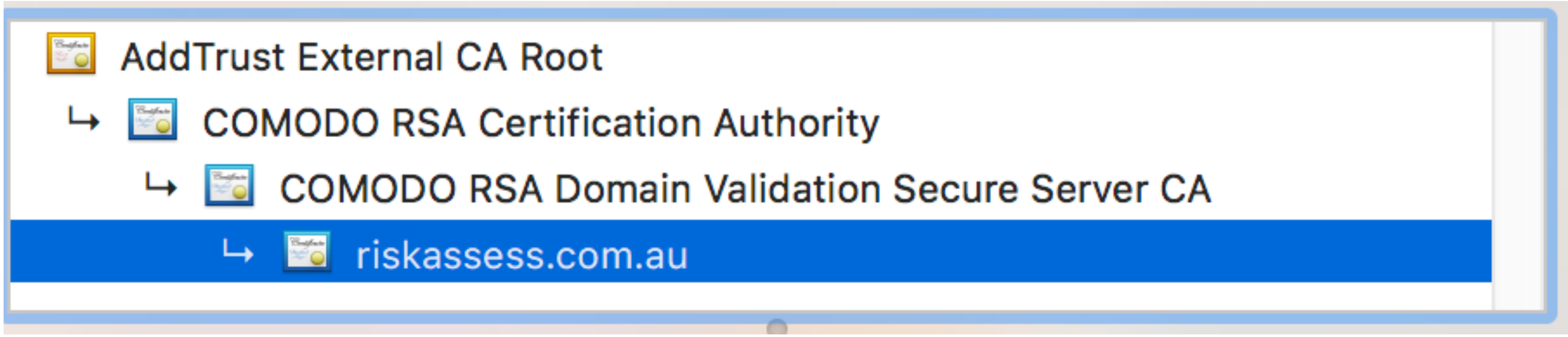
↳ *.google.com



VeriSign Class 3 Public Primary Certification Authority - G5

↳ Symantec Class 3 EV SSL CA - G3

↳ www.commbank.com.au



AddTrust External CA Root

↳ COMODO RSA Certification Authority

↳ COMODO RSA Domain Validation Secure Server CA

↳ riskassess.com.au

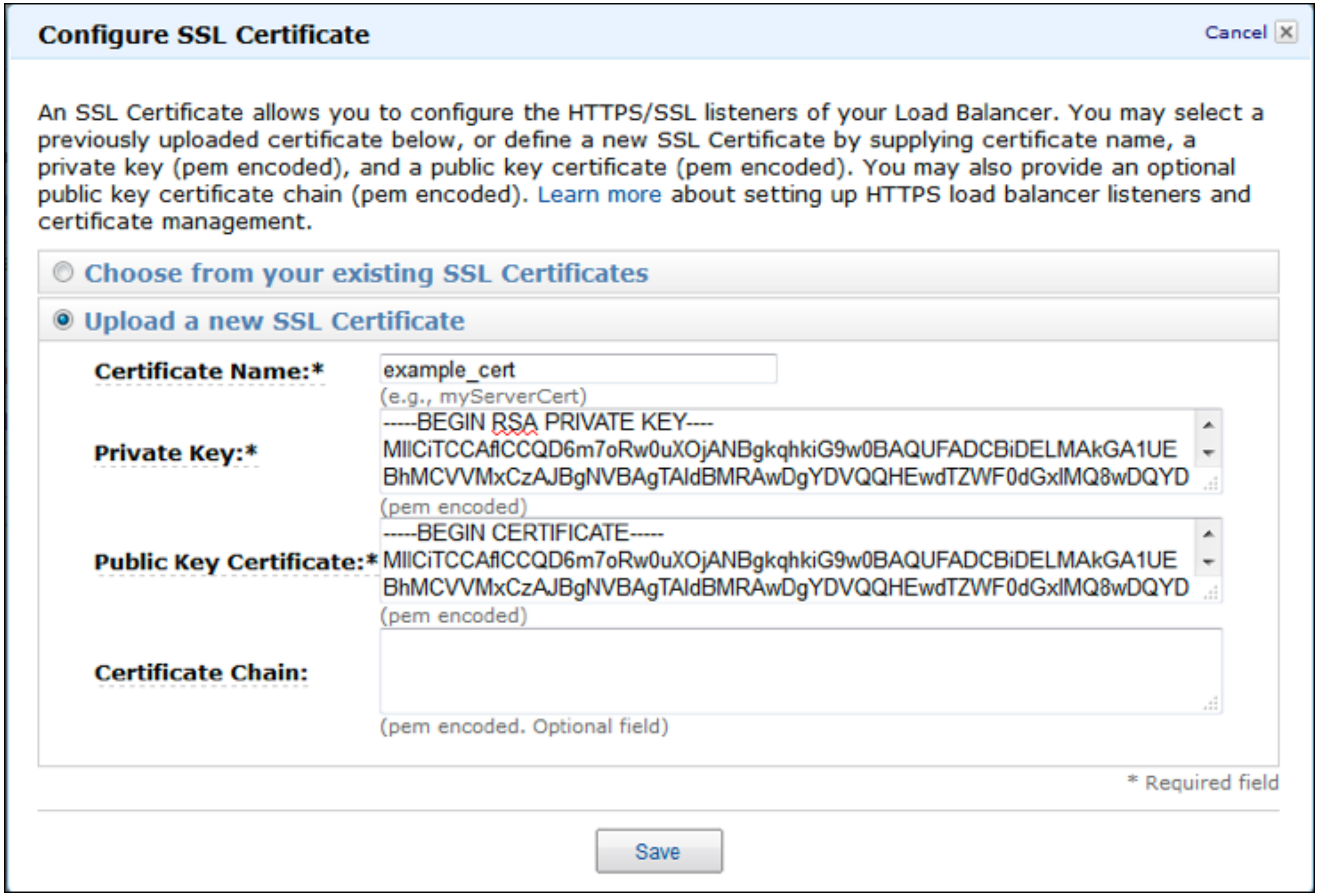
```
openssl req \
       -newkey rsa:2048 -nodes -keyout domain.key \
       -out domain.csr
```

```
Generating a 2048 bit RSA private key
...........................................+++
.....................................+++
writing new private key to 'domain.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:NSW
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:My Company
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:mydomain.com
Email Address []:james@crispdesign.net

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Domain Validation

- Upload file
- cname / txt DNS record
- Email sent to contacts on domain



An SSL Certificate allows you to configure the HTTPS/SSL listeners of your Load Balancer. You may select a previously uploaded certificate below, or define a new SSL Certificate by supplying certificate name, a private key (pem encoded), and a public key certificate (pem encoded). You may also provide an optional public key certificate chain (pem encoded). Learn more about setting up HTTPS load balancer listeners and certificate management.

○ Choose from your existing SSL Certificates

● Upload a new SSL Certificate

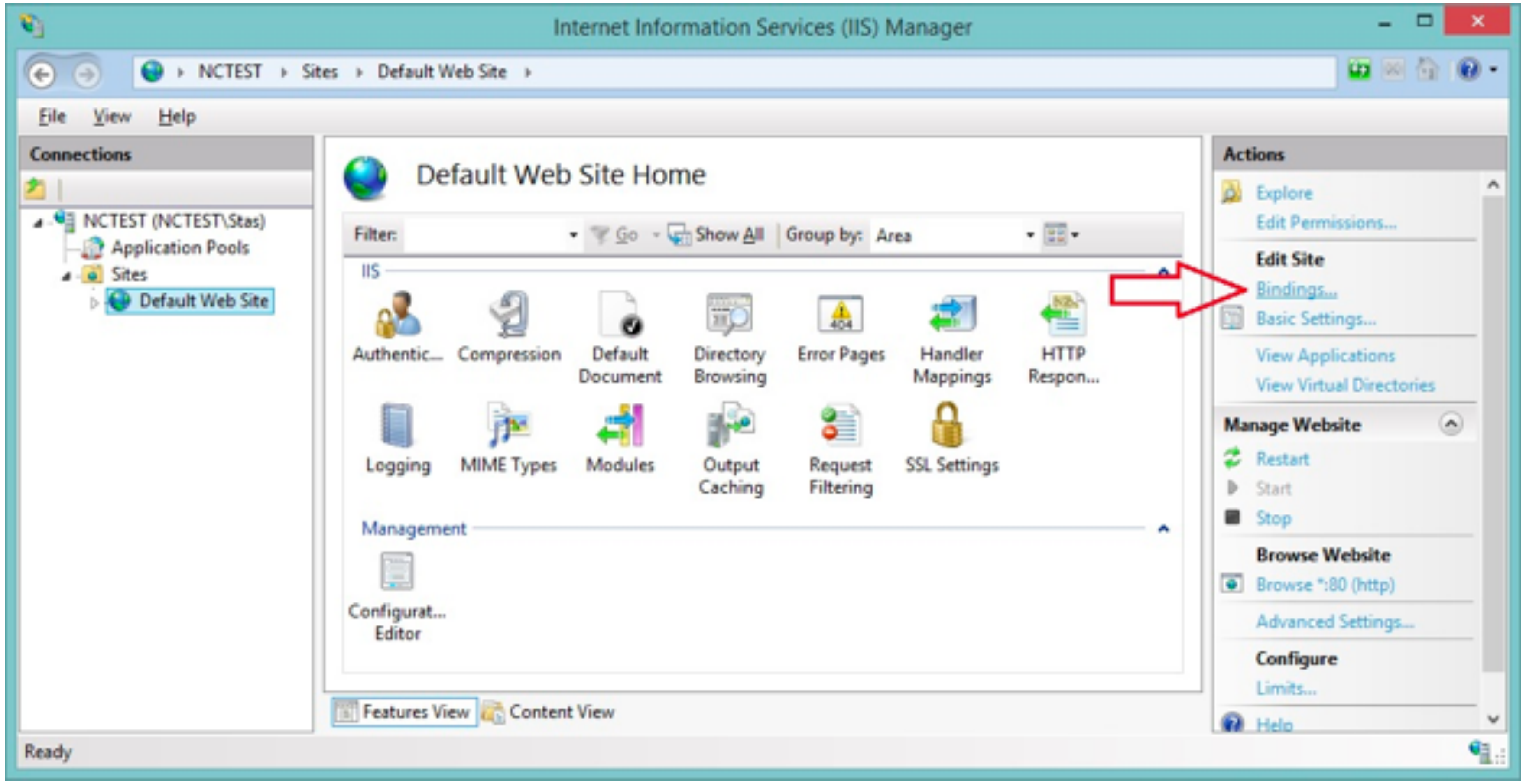
Certificate Name:* example_cert
(e.g., myServerCert)

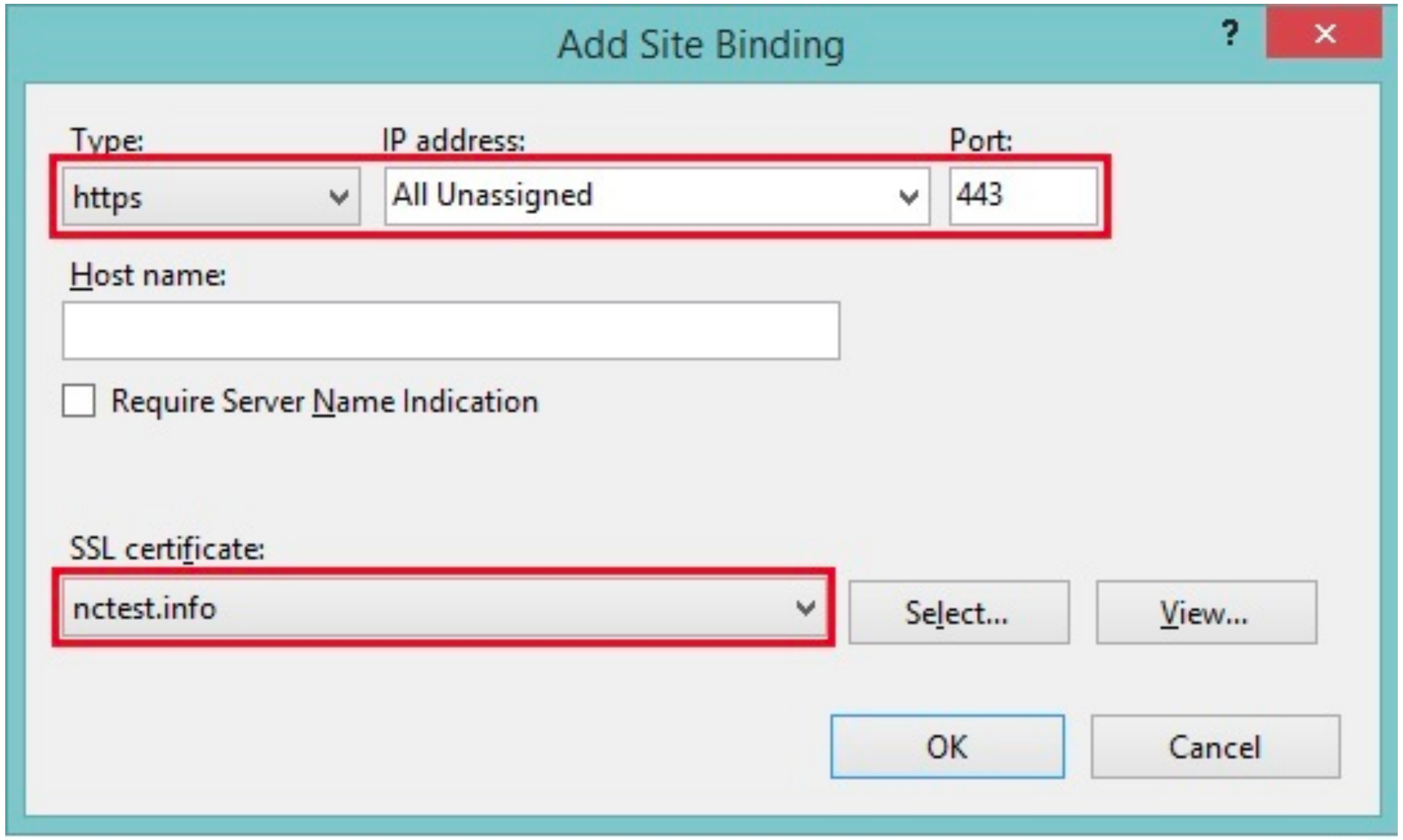
Private Key:*
```
-----BEGIN RSA PRIVATE KEY----
MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UE
BhMCVVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYD
```
(pem encoded)

Public Key Certificate:*
```
-----BEGIN CERTIFICATE-----
MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UE
BhMCVVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYD
```
(pem encoded)

Certificate Chain:
(pem encoded. Optional field)

* Required field





Type: https

IP address: All Unassigned

Port: 443

Host name:

□ Require Server Name Indication

SSL certificate: nctest.info

Apache

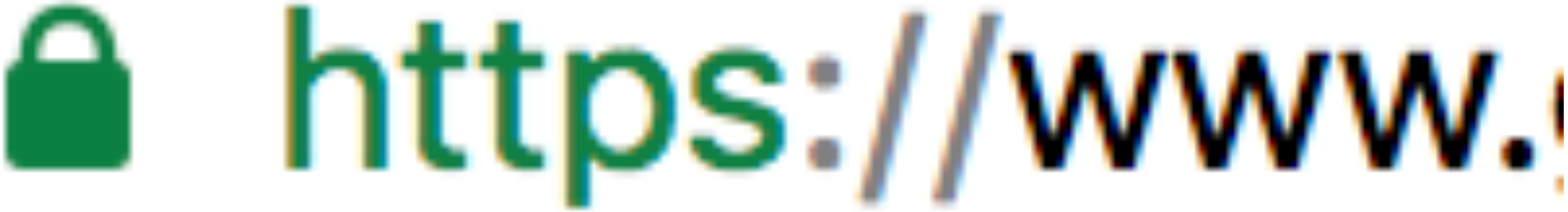
```
SSLEngine On
SSLCertificateFile /etc/apache2/ssl/server.crt
SSLCertificateKeyFile /etc/apache2/ssl/server.key
SSLCertificateChainFile /etc/apache2/ssl/server.ca-bundle
```

web.config

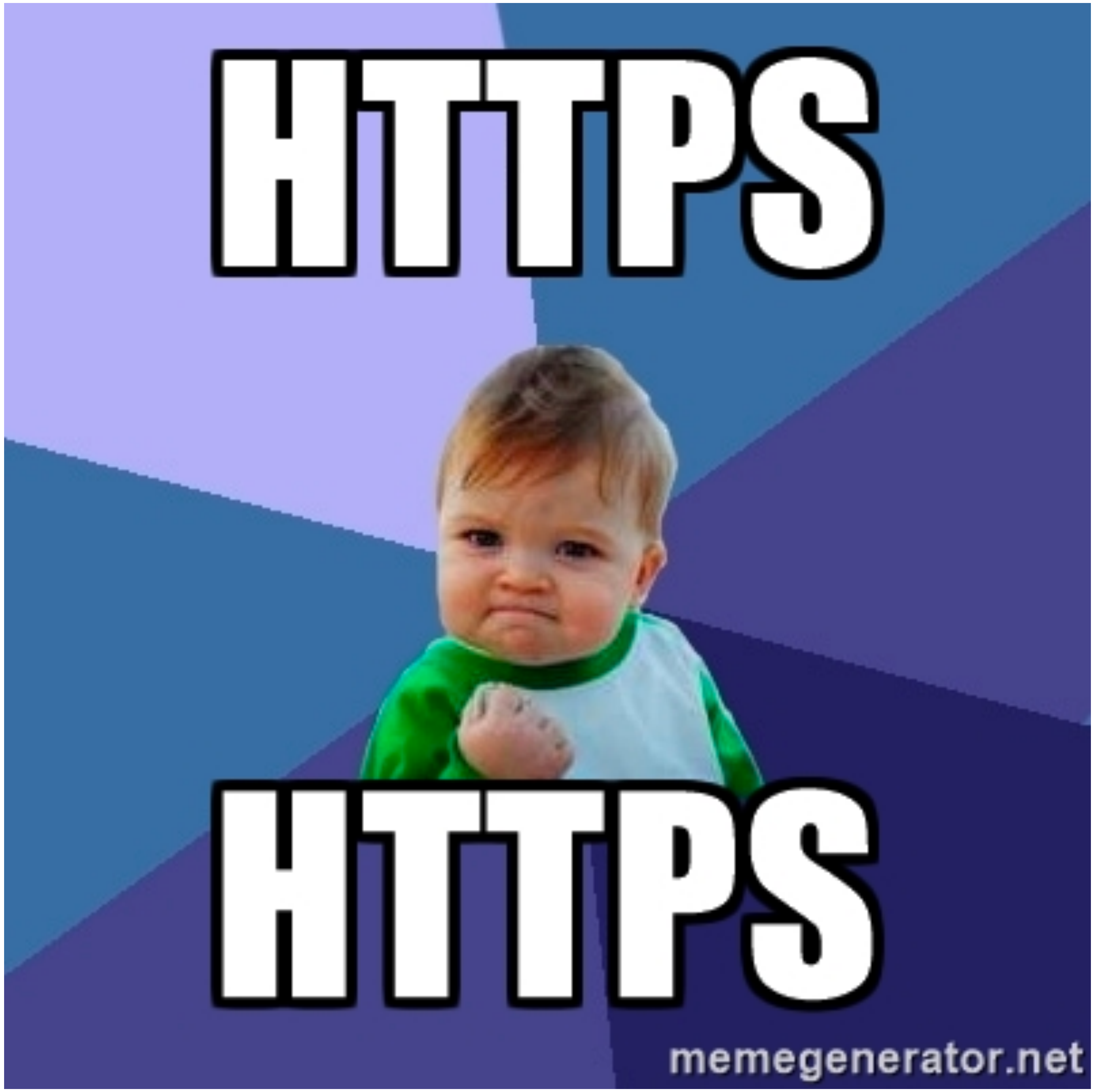
```
<rule name="Force WWW and SSL" enabled="true" stopProcessing="true">
  <match url="(.*)" />
  <conditions logicalGrouping="MatchAny">
      <add input="{HTTP_HOST}" pattern="^[^www]" />
      <add input="{HTTPS}" pattern="off" />
  </conditions>
  <action type="Redirect" url="https://www.zzz.com/{R:1}" appendQueryString="true"
redirectType="Permanent" />
</rule>
```

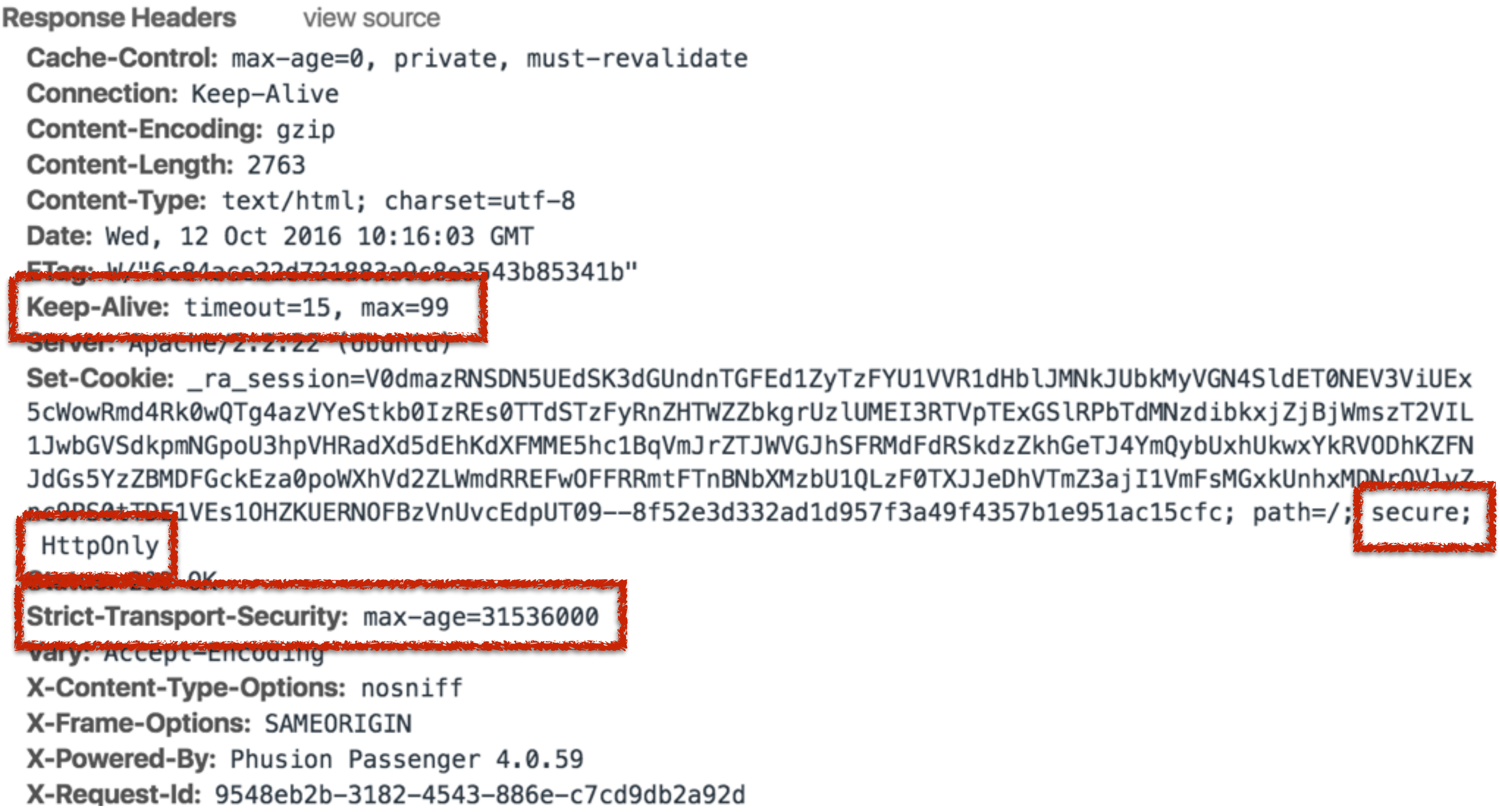
Apache Rewrite Rule

```
RewriteCond %{HTTPS} off
RewriteCond %{HTTP_HOST} ^(www.)*([a-z.]+)$ [NC]
RewriteRule ^/(.*)$ https://www.%2/$1 [R=301,L]
```



🔒 https://www.


HTTPS
HTTPS
memegenerator.net



Response Headers   view source

```
Cache-Control: max-age=0, private, must-revalidate
Connection: Keep-Alive
Content-Encoding: gzip
Content-Length: 2763
Content-Type: text/html; charset=utf-8
Date: Wed, 12 Oct 2016 10:16:03 GMT
ETag: W/"6c84ace22d721883a9c8e3543b85341b"
Keep-Alive: timeout=15, max=99
Server: Apache/2.2.22 (Ubuntu)
Set-Cookie: _ra_session=V0dmazRNSDN5UEdSK3dGUndnTGFEd1ZyTzFYU1VVR1dHblJMNkJUbkMyVGN4SldET0NEV3ViUEx
5cWowRmd4Rk0wQTg4azVYeStkb0IzREs0TTdSTzFyRnZHTWZZbkgrUzlUMEI3RTVpTExGSlRPbTdMNzdibkxjZjBjWmszT2VIL
1JwbGVSdkpmNGpoU3hpVHRadXd5dEhKdXFMME5hc1BqVmJrZTJWVGJhSFRMdFdRSkdzZkhGeTJ4YmQybUxhUkwxYkRVODhKZFN
JdGs5YzZBMDFGckEza0poWXhVd2ZLWmdRREFwOFFRRmtFTnBNbXMzbU1QLzF0TXJJeDhVTmZ3ajI1VmFsMGxkUnhxMDNrOVlvZ
nc9PS0tTDE1VEs1OHZKUERNOFBzVnUvcEdpUT09--8f52e3d332ad1d957f3a49f4357b1e951ac15cfc; path=/; secure;
 HttpOnly
Status: 200 OK
Strict-Transport-Security: max-age=31536000
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Powered-By: Phusion Passenger 4.0.59
X-Request-Id: 9548eb2b-3182-4543-886e-c7cd9db2a92d
```

HSTS

```
Strict-Transport-Security: max-age=31536000;
includeSubDomains
```

chrome://net-internals/#hsts

IE11+, Edge, FF, Chrome, Safari

Engineering a Reversible HTTPS Migration

- 302 “temporary” redirect in rewrite rules
- Don’t set HSTS!
- Change to 301 and set HSTS once it’s all OK

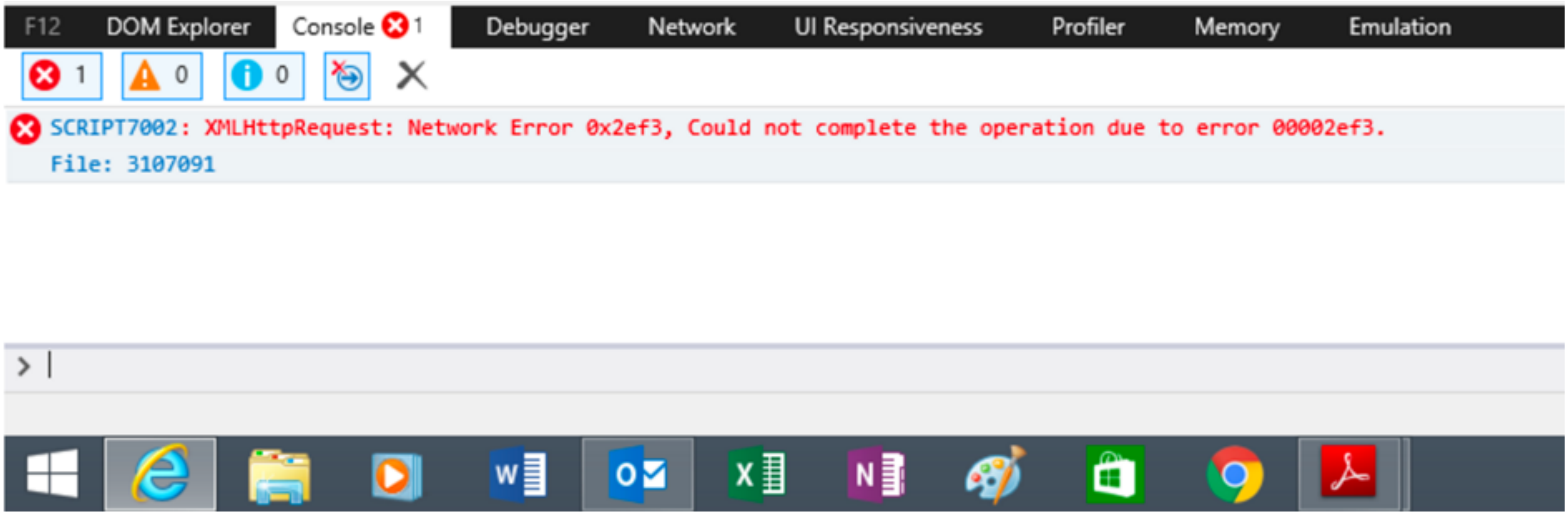
OH NOES
WAI U DO DIS
ICANHASCHEEZBURGER.COM

Tips & Gotchas

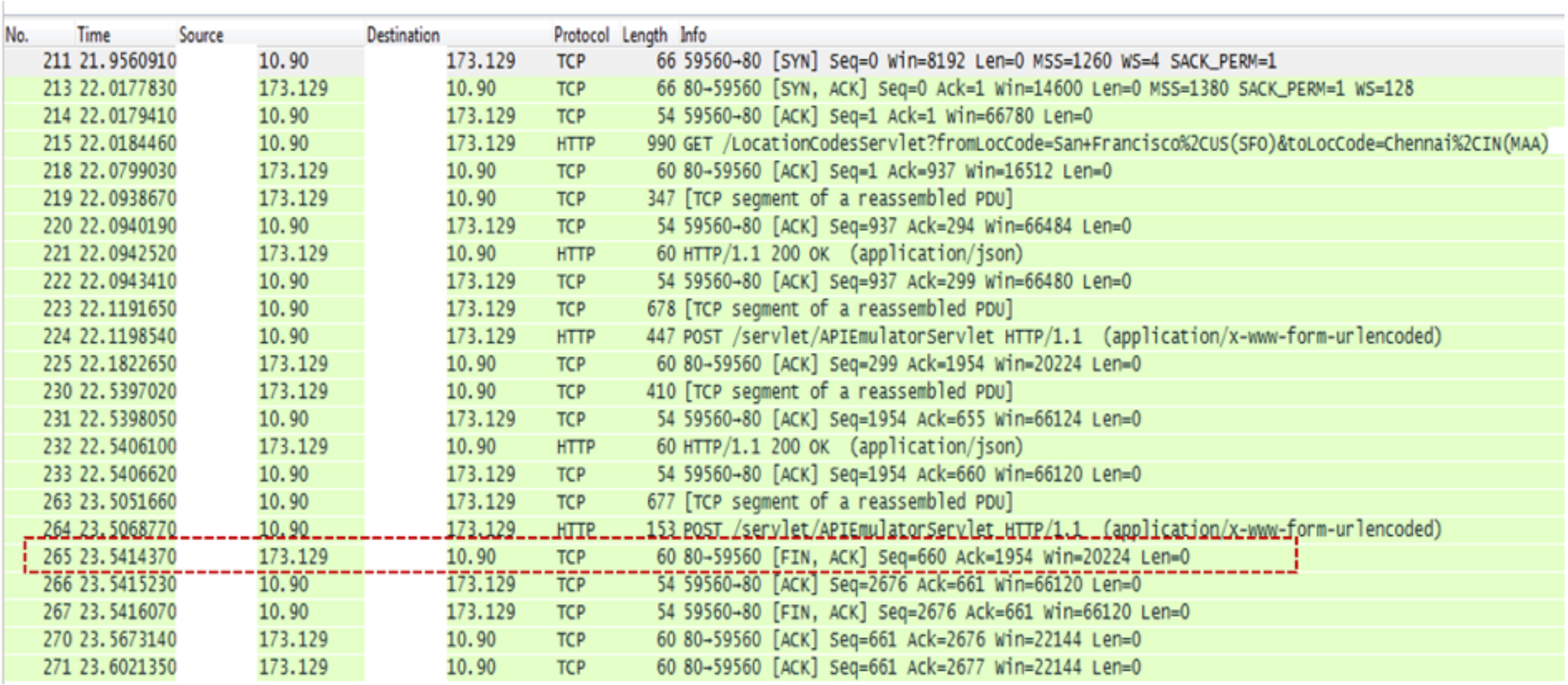
- Mixed mode sites HTTP/HTTPS
- With invalid certificate, Chrome only caches images, not JS or CSS

KeepAlive

Short KeepAlive can cause IE problems on slow connections



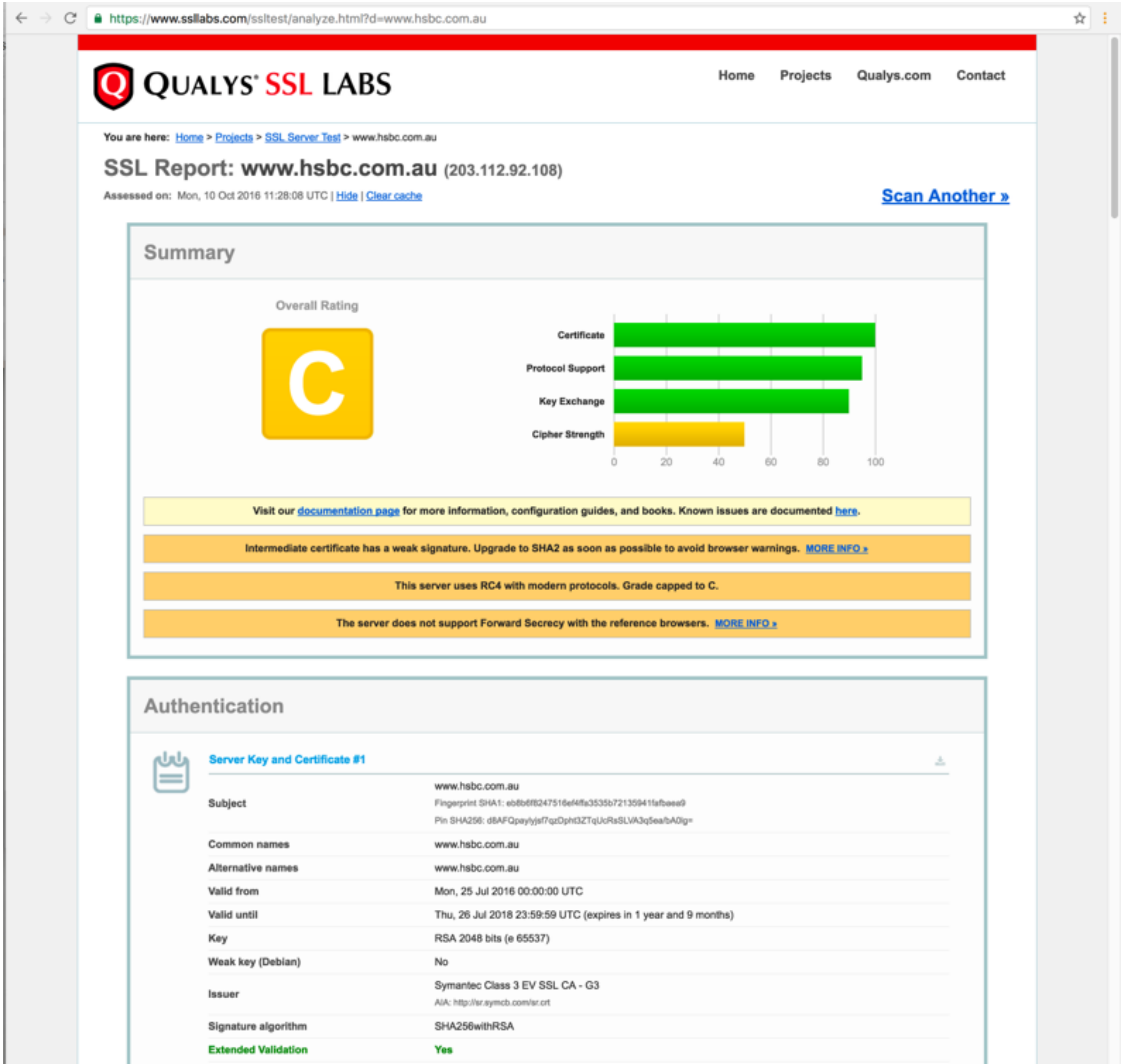
```
SCRIPT7002: XMLHttpRequest: Network Error 0x2ef3, Could not complete the operation due to error 00002ef3.
File: 3107091
```



```
No.  Time        Source        Destination    Protocol Length Info
 211 21.9560910       10.90         173.129   TCP        66 59560→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1260 WS=4 SACK_PERM=1
 213 22.0177830       173.129       10.90     TCP        66 80→59560 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1380 SACK_PERM=1 WS=128
 214 22.0179410       10.90         173.129   TCP        54 59560→80 [ACK] Seq=1 Ack=1 Win=66780 Len=0
 215 22.0184460       10.90         173.129   HTTP      990 GET /LocationCodesServlet?fromLocCode=San+Francisco%2CUS(SFO)&toLocCode=Chennai%2CIN(MAA)
 218 22.0799030       173.129       10.90     TCP        60 80→59560 [ACK] Seq=1 Ack=937 Win=16512 Len=0
 219 22.0938670       173.129       10.90     TCP       347 [TCP segment of a reassembled PDU]
 220 22.0940190       10.90         173.129   TCP        54 59560→80 [ACK] Seq=937 Ack=294 Win=66484 Len=0
 221 22.0942520       173.129       10.90     HTTP       60 HTTP/1.1 200 OK  (application/json)
 222 22.0943410       10.90         173.129   TCP        54 59560→80 [ACK] Seq=937 Ack=299 Win=66480 Len=0
 223 22.1191650       10.90         173.129   TCP       678 [TCP segment of a reassembled PDU]
 224 22.1198540       10.90         173.129   HTTP      447 POST /servlet/APIEmulatorServlet HTTP/1.1  (application/x-www-form-urlencoded)
 225 22.1822650       173.129       10.90     TCP        60 80→59560 [ACK] Seq=299 Ack=1954 Win=20224 Len=0
 230 22.5397020       173.129       10.90     TCP       410 [TCP segment of a reassembled PDU]
 231 22.5398050       10.90         173.129   TCP        54 59560→80 [ACK] Seq=1954 Ack=655 Win=66124 Len=0
 232 22.5406100       173.129       10.90     HTTP       60 HTTP/1.1 200 OK  (application/json)
 233 22.5406620       10.90         173.129   TCP        54 59560→80 [ACK] Seq=1954 Ack=660 Win=66120 Len=0
 263 23.5051660       10.90         173.129   TCP       677 [TCP segment of a reassembled PDU]
 264 23.5068770       10.90         173.129   HTTP      153 POST /servlet/APIEmulatorServlet HTTP/1.1  (application/x-www-form-urlencoded)
 265 23.5414370       173.129       10.90     TCP        60 80→59560 [FIN, ACK] Seq=660 Ack=1954 Win=20224 Len=0
 266 23.5415230       10.90         173.129   TCP        54 59560→80 [ACK] Seq=2676 Ack=661 Win=66120 Len=0
 267 23.5416070       10.90         173.129   TCP        54 59560→80 [FIN, ACK] Seq=2676 Ack=661 Win=66120 Len=0
 270 23.5673140       173.129       10.90     TCP        60 80→59560 [ACK] Seq=661 Ack=2676 Win=22144 Len=0
 271 23.6021350       173.129       10.90     TCP        60 80→59560 [ACK] Seq=661 Ack=2677 Win=22144 Len=0
```

HTTPS links/assets

- Relative urls “/users/edit” “/public/img.svg”
- HTTPS urls
- Protocol relative urls
  eg, <script src=“//ajax.microsoft.com/ajax/jquery/jquery-1.3.2.min.js”>



You are here: Home > Projects > SSL Server Test > www.hsbc.com.au

SSL Report: www.hsbc.com.au (203.112.92.108)

Assessed on: Mon, 10 Oct 2016 11:28:08 UTC | Hide | Clear cache

Scan Another »

Summary

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

Intermediate certificate has a weak signature. Upgrade to SHA2 as soon as possible to avoid browser warnings. MORE INFO »

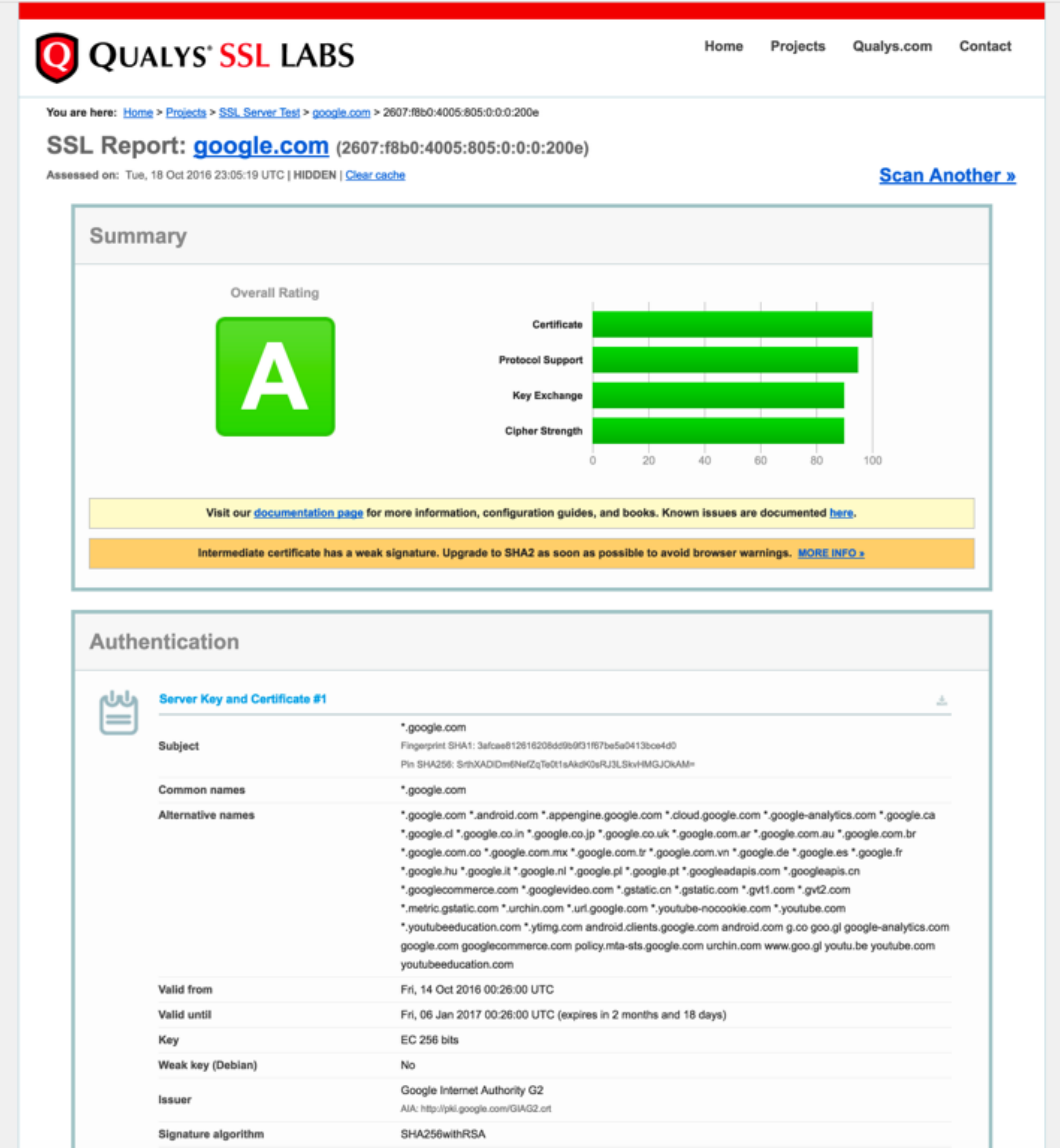
This server uses RC4 with modern protocols. Grade capped to C.

The server does not support Forward Secrecy with the reference browsers. MORE INFO »

Authentication

Server Key and Certificate #1

Subject	www.hsbc.com.au Fingerprint SHA1: eb8b6f8247516ef4ffa3535b72135941fafbaea9 Pin SHA256: d8AFQpaylyjsf7qzDpht3ZTqUcRsSLVA3q5ea/bA0lg=
Common names	www.hsbc.com.au
Alternative names	www.hsbc.com.au
Valid from	Mon, 25 Jul 2016 00:00:00 UTC
Valid until	Thu, 26 Jul 2018 23:59:59 UTC (expires in 1 year and 9 months)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Symantec Class 3 EV SSL CA - G3 AIA: http://sr.symcb.com/sr.crt
Signature algorithm	SHA256withRSA
Extended Validation	Yes



QUALYS® SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > google.com > 2607:f8b0:4005:805:0:0:0:200e

SSL Report: google.com (2607:f8b0:4005:805:0:0:0:200e)

Assessed on: Tue, 18 Oct 2016 23:05:19 UTC | **HIDDEN** | Clear cache

Scan Another »

Summary

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

Intermediate certificate has a weak signature. Upgrade to SHA2 as soon as possible to avoid browser warnings. MORE INFO »

Authentication

Server Key and Certificate #1

Subject	*.google.com Fingerprint SHA1: 3afcae812616208dd9b9f31f67be5a0413bce4d0 Pin SHA256: SrthXADIDm6NefZqTe0t1sAkdK0sRJ3LSkvHMGJOkAM=
Common names	*.google.com
Alternative names	*.google.com *.android.com *.appengine.google.com *.cloud.google.com *.google-analytics.com *.google.ca *.google.cl *.google.co.in *.google.co.jp *.google.co.uk *.google.com.ar *.google.com.au *.google.com.br *.google.com.co *.google.com.mx *.google.com.tr *.google.com.vn *.google.de *.google.es *.google.fr *.google.hu *.google.it *.google.nl *.google.pl *.google.pt *.googleadapis.com *.googleapis.cn *.googlecommerce.com *.googlevideo.com *.gstatic.cn *.gstatic.com *.gvt1.com *.gvt2.com *.metric.gstatic.com *.urchin.com *.url.google.com *.youtube-nocookie.com *.youtube.com *.youtubeeducation.com *.ytimg.com android.clients.google.com android.com g.co goo.gl google-analytics.com google.com googlecommerce.com policy.mta-sts.google.com urchin.com www.goo.gl youtu.be youtube.com youtubeeducation.com
Valid from	Fri, 14 Oct 2016 00:26:00 UTC
Valid until	Fri, 06 Jan 2017 00:26:00 UTC (expires in 2 months and 18 days)
Key	EC 256 bits
Weak key (Debian)	No
Issuer	Google Internet Authority G2 AIA: http://pki.google.com/GIAG2.crt
Signature algorithm	SHA256withRSA

Questions?