SSL/TLS

SSL (Secure Socket Layer)

- Protocolo entre capa 4 y 5 sobre TCP del modelo DoD

SSL

Es responsable de:

- Fragmentar el flujo de datos en paquetes SSL.
- Comprimir los paquetes antes de cifrarlos.
- Autenticar al servidor y/o cliente SSL.
- Cifrar los paquetes.
- Se puede usar para ofrecer servicios de seguridad a diversas aplicaciones (no sólo HTTP).

Versiones

- SSLv1
  - Diseñado por Netscape.
  - Mientras se presentaba el protocolo en una conferencia, asistentes a la conferencia lo rompieron antes que terminara la presentación.
- SSLv2
  - Diseñado por Netscape.
  - Incorporado a Netscape Navigator 1.0
  - Vulnerable al ataque MITM.
- SSLv3
  - Internet Draft producido por Netscape (11/96).
  - Nunca se estandarizó, sólo existe como draft.
  - Propuesto como estándar para la IETF.

Requerimientos

Cuando un cliente y un servidor SSL quieren comunicarse, deben:

1. Ponerse de acuerdo en la versión de SSL.
2. Ponerse de acuerdo en los algoritmos criptográficos.
3. Autenticarse mutuamente (opcional).
4. Usar un algoritmo de llave pública para generar secretos compartidos.

Pasos

ClientHello (C → S)
Dispongo de: RSA + RC4/128 + MD5
Este es mi número aleatorio (Rc).
ServerHello (S → C)
Acepto RSA + RC4/128 + MD5
Este es mi número aleatorio (Rs).
(opc. S → C) Certificate o ServerKeyExchange
Este es mi certificado SSL o mi secreto Diffie-Hellman.
(opcional S → C) CertificateRequest
Requiero un certificado de cliente.
ServerHelloDone (S → C)

Generando la llave

- Si el servidor mandó un CertificateRequest el cliente debe mandar su certificado en un mensaje Certificate e indicarle que no tiene certificado.
- Si el servidor le mandó al cliente su certificado SSL el cliente cifra una llave secreta aleatoria con la llave pública del servidor y se la manda en un ClientKeyExchange.
- Si el servidor le mandó al cliente un secreto Diffie-Hellman el cliente genera su secreto DH y se lo manda en un ClientKeyExchange.
- Ahora ambos tienen una llave secreta compartida.

Características SSL

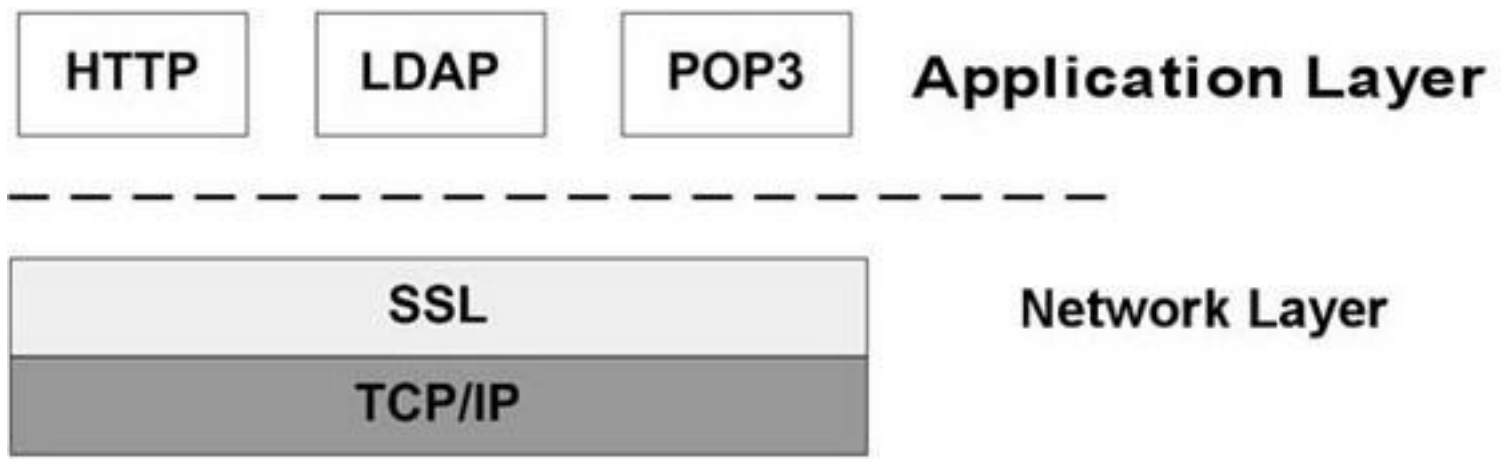
- Confidencialidad de los datos.
- Autenticación y no repudiación de cliente y servidor mediante firmas digitales.
- Integridad de los datos mediante códigos de autenticación de mensajes.
- Protocolo adaptativo.

Largo de llave

- El cliente es el que determina el largo de la llave de cifrado.
- El servidor se adapta a lo que el cliente soporte.

Captura de tráfico

Source	Destination	Protocol	Info
10.12.56.71	10.12.38.7	SSLv2	Client Hello
10.12.38.7	10.12.56.71	SSLv2	Server Hello
10.12.56.71	10.12.38.7	SSLv2	Client Master Key
10.12.38.7	10.12.56.71	SSLv2	Encrypted Data



SET (Secure Electronic Transaction)

- Es un protocolo desarrollado por Visa y Mastercard y que utiliza el estándar SSL.
- SET se basa en el uso de una firma electrónica del comprador y una transacción que involucra, no sólo al comprador y al vendedor, sino también a sus respectivos bancos.
- Desde Septiembre de 1999 en Chile.

Chilean credit card transaction central sorting system Transbank, Chilean systems integrator Adexus and Chile's ISP Entel Internet will launch an Ecommerce pilot project implementing the Secure Electronic Transaction (SET) protocol in September. Chilean record store Feria del Disco will participate as a "guinea-pig" and sell their records using the SET protocol.\r\n

¿Cómo funciona SET?

- Los datos del cliente son enviados al servidor del vendedor, pero dicho vendedor sólo recibe la orden.
- Los números de la tarjeta del banco se envían directamente al banco del vendedor, quien podrá leer los detalles de la cuenta bancaria del comprador y contactar con el banco para verificarlos en tiempo real.

Ventajas de SET

- Autentifica todas las partes implicadas (banco, compañía de tarjetas de Crédito, comerciante y cliente), las cuales disponen de un Certificado Digital, facilitando de modo jerárquico las "relaciones de confianza".
- Confidencialidad e integridad.

Payment Card Industry Data Security Standard

Las compañías que procesan, guardan o transmiten datos de tarjetas deben cumplir con el estándar o arriesgan la pérdida de sus permisos para procesar las tarjetas de crédito y débito (Perdida de franquicias), enfrentar auditorías rigurosas o pagos de multas.

CORREOS CHILE

PCI DSS COMPLIANT

https://latinamerica.mastercard.com/es-region-lac/comerciantes/seguridad-y-proteccion/requisitos-y-recomendaciones-de-seguridad/proteccion-de-datos-del-sito-y-pci.html

TLS (Transport Layer Security)

- Sucesor de SSL
- TLS 1.0 (enero de 1999).
- Soportado desde Internet Explorer 5.0.
- Puede ser visto como SSL v3.1

Source	Destination	Protocol	Info
192.168.1.107	168.143.172.53	SSL	Client Hello
168.143.172.53	192.168.1.107	TLSv1	Server Hello
168.143.172.53	192.168.1.107	TLSv1	Certificate, Server Key Exchange, Server Hello Done
192.168.1.107	168.143.172.53	TLSv1	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
168.143.172.53	192.168.1.107	TLSv1	Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake Message

	SSL	TLS
Versión	3.0	1.0
Suite Cipher	Admite Fortezza (algoritmo)	No es compatible con Fortezza
Criptografía secreta	Utiliza el resumen del mensaje del secreto premaster para crear el secreto maestro.	Utiliza una función pseudoaleatoria para crear un secreto maestro.
Protocolo de grabación	Utiliza MAC (Código de Autenticación de Mensaje)	Utiliza HMAC (Hashed MAC)
Protocolo de alerta	Se incluye el mensaje de alerta "Sin certificado".	Elimina la descripción de alerta (sin certificado) y agrega una docena de otros valores.
Autenticación de mensaje	Ad hoc	Estándar
Autentificación	Ad hoc	Función pseudoaleatoria
Certificado verificar	Complejo	Sencillo
Terminado	Ad hoc	Función pseudoaleatoria

TLS 1.2 (SSL 3.3)

- En Agosto de 2008 se publica la versión 1.2.
- Recomienda el uso de PKCS#1 versión 2.1, en vez de versiones más antiguas.
- La razón de dicho cambio es para protegerse contra ataques descubiertos por Daniel Bleichenbacher que podían lanzarse contra servidores TLS 1.0, usando PKCS#1 versión 1.5

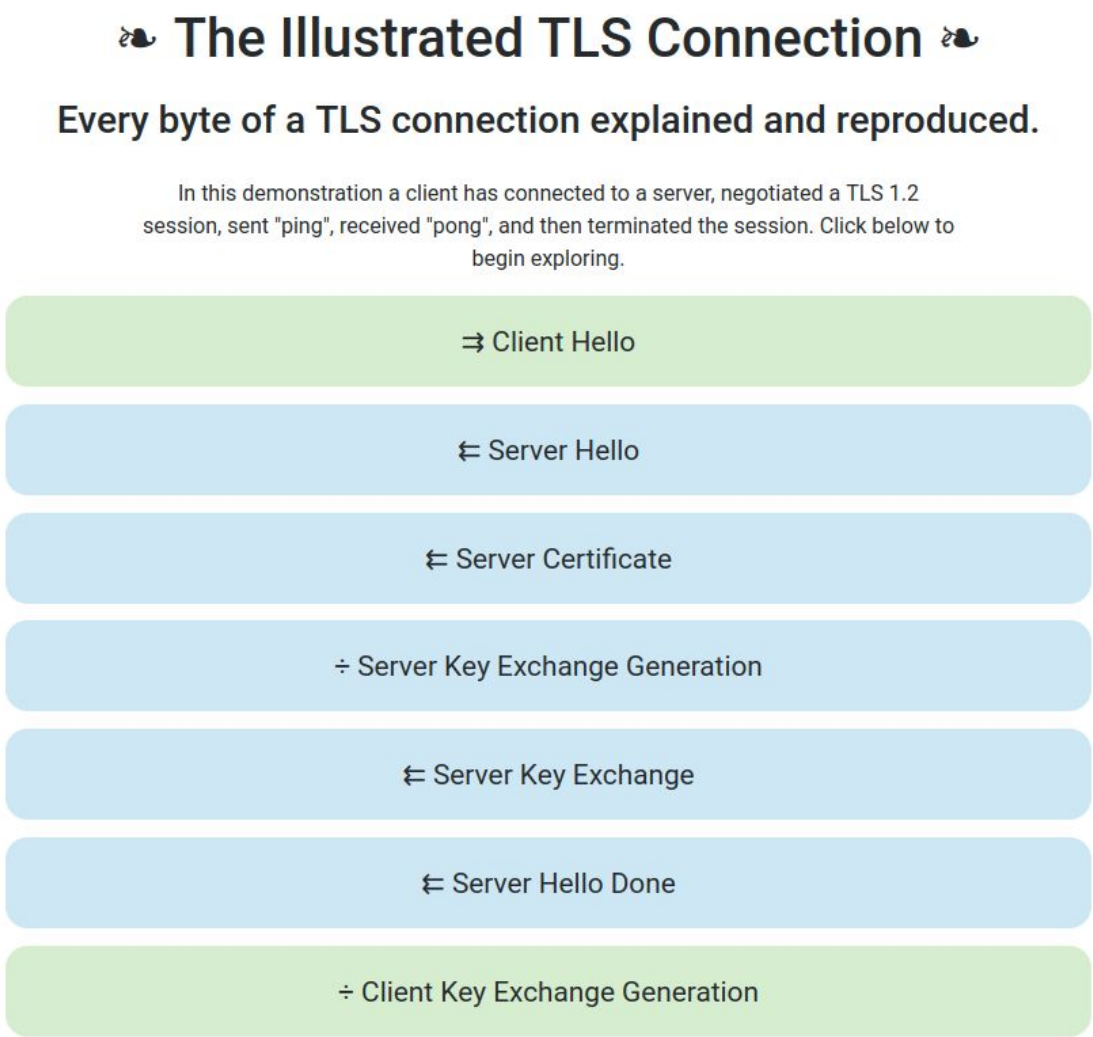
http://tools.ietf.org/html/rfc5246

PKCS

- En criptografía PKCS se refiere a un grupo de estándares de criptografía, de clave pública concebidos y publicados por los laboratorios de RSA en California. A RSA Security se le asignaron los derechos de licenciamiento para la patente del algoritmo de clave asimétrica RSA y adquirió los derechos de licenciamiento para muchas otras patentes de claves.

http://www.rsa.com/rsalabs/node.asp?id=2124

Ilustración de TLS



https://tls.ulfheim.net/

¿Qué versión usaba Firefox 4?

Opera 12

Security Protocols

- [x] Enable SSL 3
- [x] Enable TLS 1
- [x] Enable TLS 1.1
- [x] Enable TLS 1.2

Details <<

Select ciphers to enable

Version	Cipher
SSL 3/TLS 1	☐ 0 bit Authentication Only (RSA/SHA)
SSL 3/TLS 1	☐ 0 bit Authentication Only (RSA/SHA-256)
SSL 3/TLS 1	☑ 168 bit 3-DES (Anonymous DH/SHA)
SSL 3/TLS 1	☑ 128 bit AES (Anonymous DH/SHA-256)
SSL 3/TLS 1	☑ 256 bit AES (Anonymous DH/SHA-256)
SSL 3/TLS 1	☑ 168 bit 3-DES (RSA/SHA)
SSL 3/TLS 1	☑ 168 bit 3-DES (DH_RSA/SHA)
SSL 3/TLS 1	☑ 168 bit 3-DES (DHE_RSA/SHA)
SSL 3/TLS 1	☑ 168 bit 3-DES (DH_DSS/SHA)
SSL 3/TLS 1	☑ 168 bit 3-DES (DHE_DSS/SHA)
SSL 3/TLS 1	☑ 128 bit ARC4 (RSA/MD5)
SSL 3/TLS 1	☑ 128 bit ARC4 (RSA/SHA)
SSL 3/TLS 1	☑ 128 bit AES (RSA/SHA)

Help Cancel OK

Certificados

- La Autoridad de Certificación ofrece diferentes tipos de certificados que se diferencian por el nivel de confianza que ofrecen.
- Este nivel de confianza depende del procedimiento que se observa para verificar la identidad del solicitante del Certificado.

Entidades Certificadoras

Global TLS certificate

DigiCert has exhibited strong market leadership in its growth, supporting the adoption of new standards and continually innovating with the industry's best, most modern PKI (Public Key Infrastructure) technology

In addition to the strength in the TLS/SSL market, the company is also focused on new security technologies, such as protecting devices in the IoT and developing implementations of post-quantum cryptography

CA en Chile

- E-CertChile

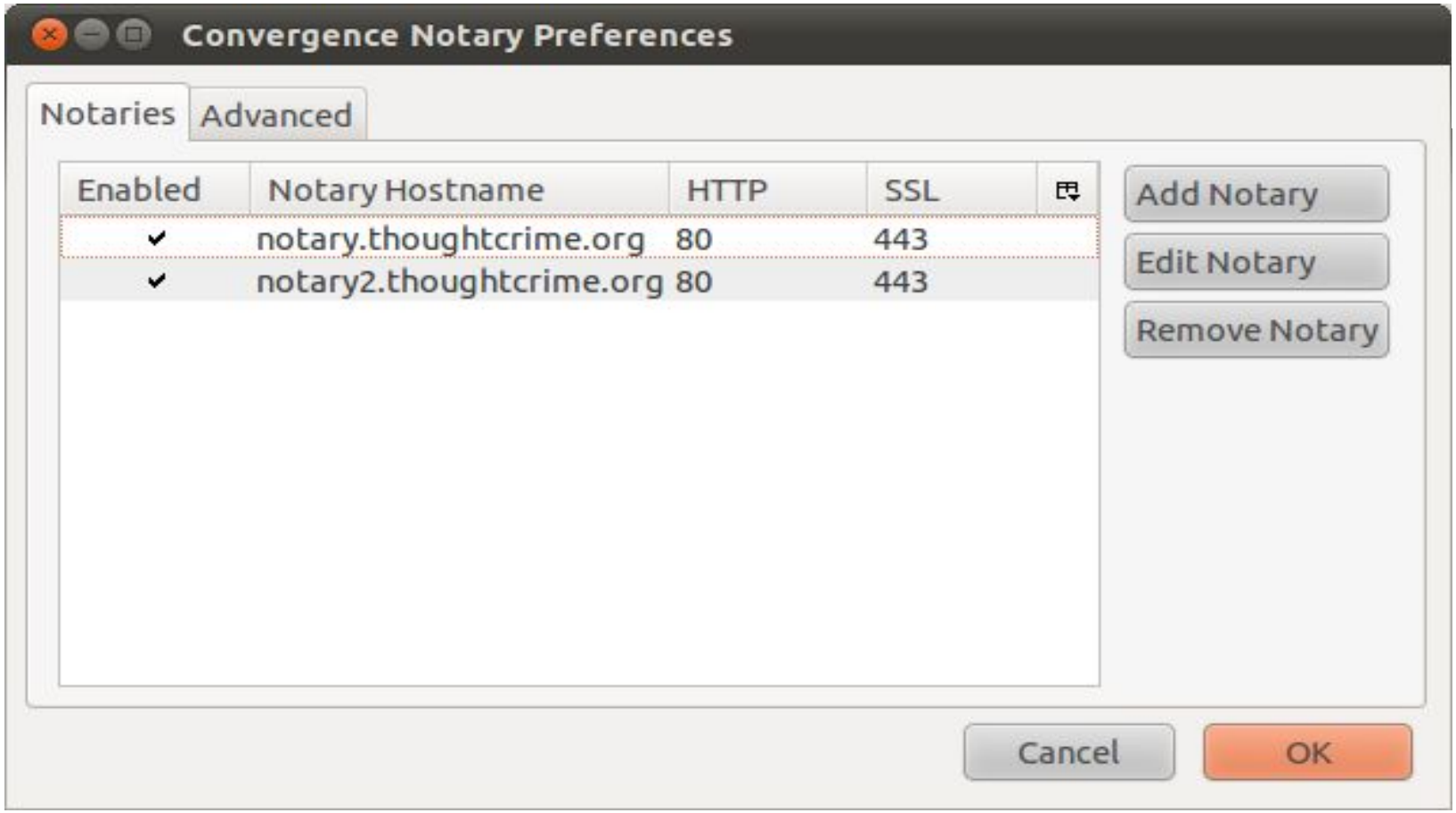
¿Cuáles son las CA a nivel mundial?

http://www.securitybydefault.com/2012/01/en-manos-de-quien-esta-la-seguridad-de.html

Alternativa

CONVERGENCE Beta

- Notario que certifica elegido por el usuario



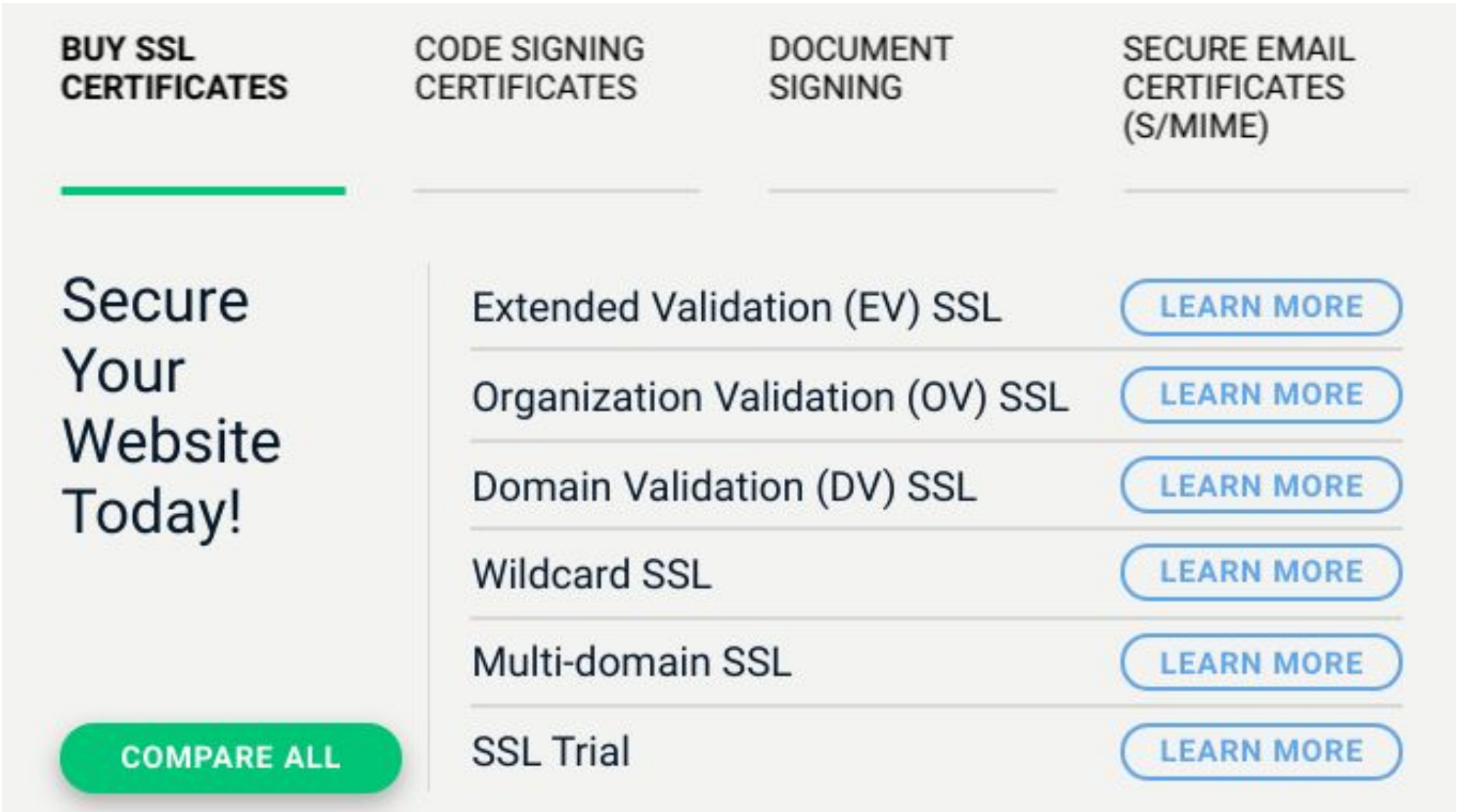
https://github.com/moxie0/Convergence

Extended Validation SSL Certificate

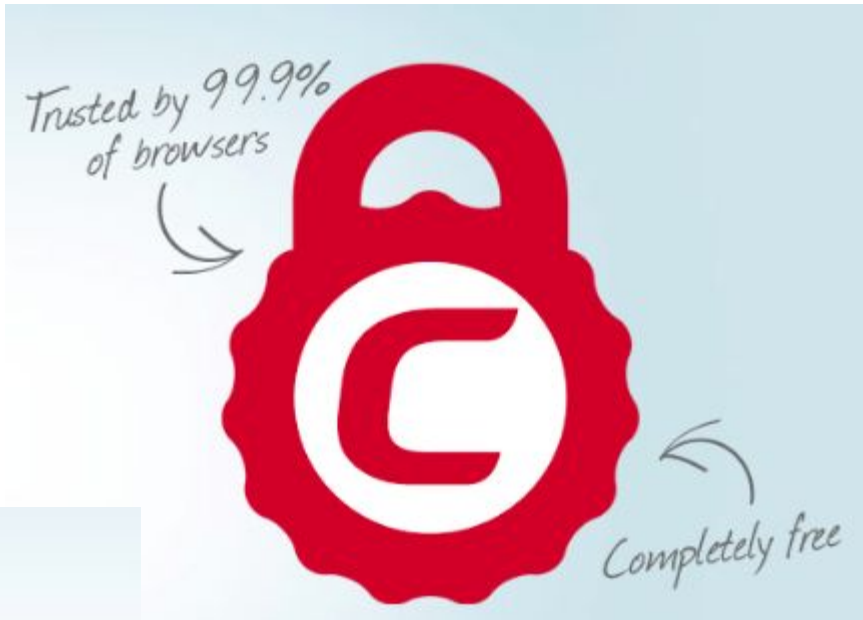
An Extended Validation Certificate (EV) is a certificate conforming to X.509 that proves the legal entity of the owner and is signed by a Certificate Authority key that can issue EV certificates.

https://www.mrdomain.com/products/ssl/green-bar/

$e paga por separado

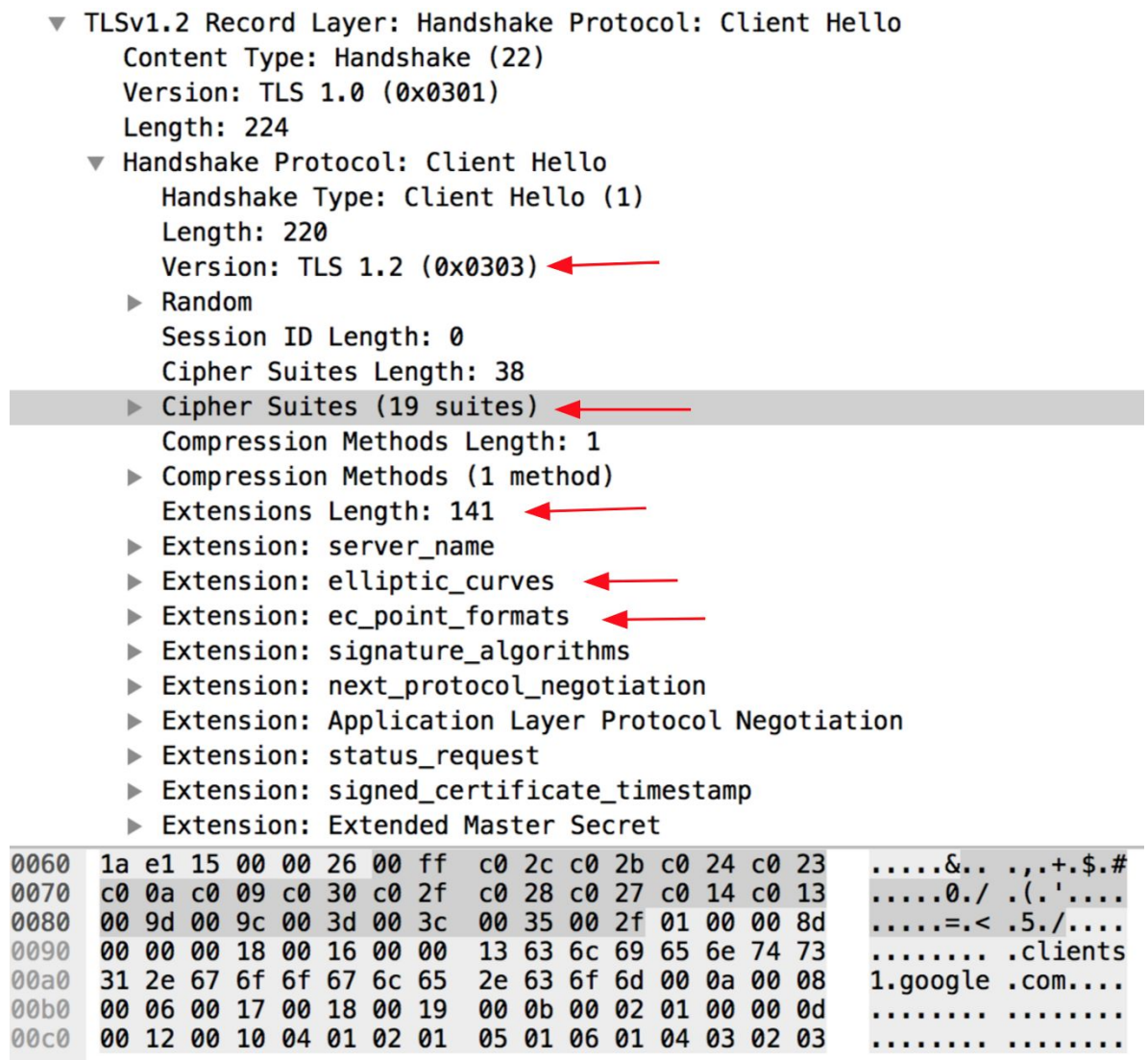


Certificado gratuito por 90 días



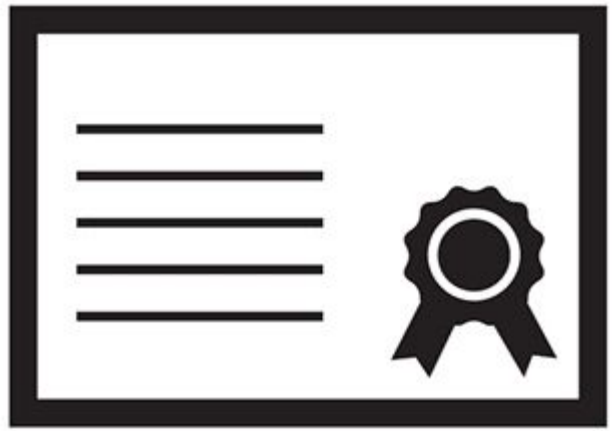
TLS Fingerprint

JA3 fingerprints the way that a client application communicates over TLS and JA3S fingerprints the server response.



https://engineering.salesforce.com/tls-fingerprinting-with-ja3-and-ja3s-247362855967

X.509



X.509

- El protocolo X.509 fue publicado como una recomendación de la ITU llamada ITU-T X.509
- X.509 (Versión 1) fue expuesto en 1988 para servicios de directorio y se basa en un sistema jerárquico donde los principales entes son autoridades certificadoras (Salt AC) que emiten certificados digitales de identificación.
- Caso contrario al PGP que consiste en un modelo de confianza y autenticación a través de la web, donde cualquiera puede firmar y garantizar la validez de la llave pública de otro.
- X.509 (Versión 2) aparece en 1993.

X.509

- X.509 (Versión 3) define el formato para extensiones de los certificados utilizados para almacenar información adicional referente al propietario y define el uso del mismo.
- El término X.509 se refiere a la última versión publicada del estándar a menos que se indique otra cosa.

http://tools.ietf.org/html/rfc5280

¿Cómo funciona?

- X.509 es un sistema mediante el cual la autoridad certificadora emite un certificado, dando una llave pública única. La autenticidad de un certificado y una entidad certificadora es dependiente del certificado raíz, el cual es la base primordial de la cadena de certificaciones del modelo X.509.
- Los certificados raíz son confiados implícitamente, y el mejor ejemplo es que muchos programas como navegadores, y lectores de correo vienen con muchos de ellos preinstalados.
- El sistema X.509 también incluye el método para CRL (certificate revocation list).

Protocolos que soportan X.509

- SSL/TLS
- IPSec
- S/MIME
- Smartcard
- SSH
- HTTPS
- XMMP
- muchos más

X.509 codifications

PEM codifica certificados en Base64 / ASCII, incluyendo encabezado y pie de página. Generalmente se utilizan para certificados digitales X.509 v3 y servidores web.

```
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
```

DER, es utilizada para codificar, de forma binaria, extensiones PEM y es frecuentemente usado por JAVA y software de escritorio como navegadores de Internet.

X.509 extensions

CRT utilizada para certificados. Los certificados pueden ser codificados en binarios DER o como PEM. Es la extensión más utilizada en sistemas *nix, como Linux o Unix.

CER extensión alternativa a la CRT pero siguiendo las convenciones de Microsoft.

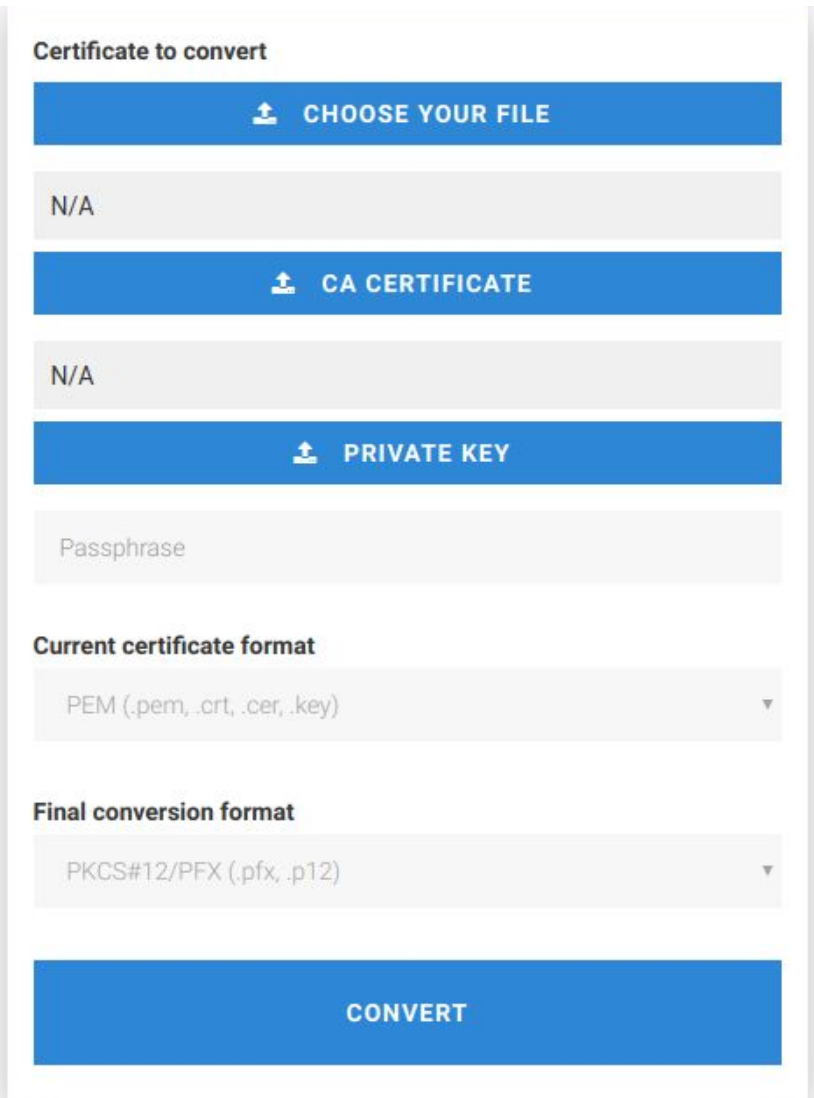
KEY extensión utilizada tanto para la clave pública como la privada de PKCS. Estas claves pueden estar codificadas en formato binario DER o PEM.

X.509 PKCS format

PKCS#7 y P7B está codificado en Base64 / ASCII. Solo contiene certificados y strings, pero no la llave privada. Generalmente se utiliza en Windows y servidores basados en Java como Tomcat. Utiliza la extensión .p7b y .p7c

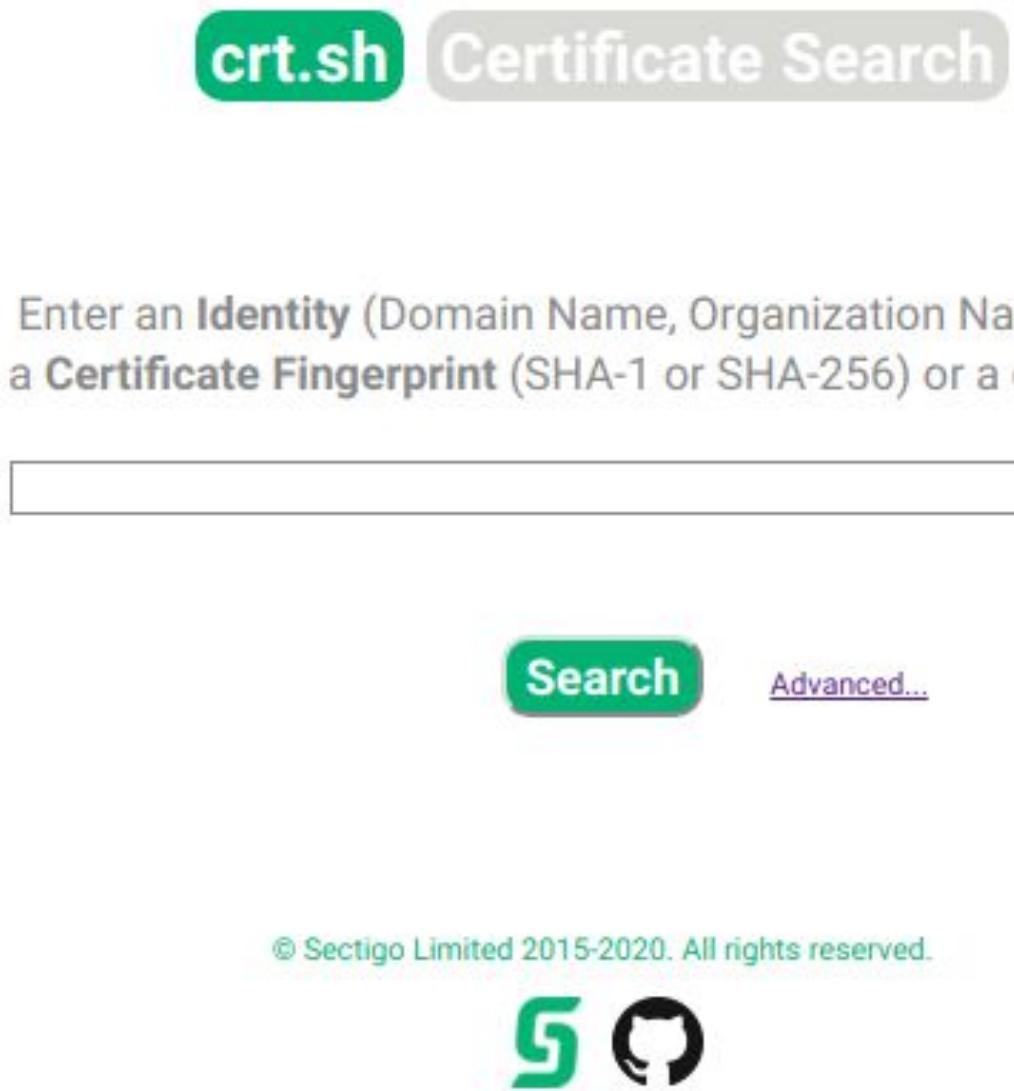
PKCS#12 y PFX está codificado en binario. Almacena el certificado del servidor y la llave privada en un archivo encriptado. Los archivos con extensión .p12, .pksc#12 o .pfx, son idénticos. Generalmente utilizado en servidores Microsoft.

Certificate Conversion



https://www.httpcs.com/en/ssl-converter

Certificate transparency log search engine



Searching subdomains

crt.sh ID	Logged At ⇧	Not Before	Not After	Matching Identities	Issuer Name
2977779749	2020-06-19	2020-06-19	2020-09-17	bitacoraindulto.titulodigital.udp.cl www.bitacoraindulto.titulodigital.udp.cl	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
2977779506	2020-06-19	2020-06-19	2020-09-17	bitacoraindulto.titulodigital.udp.cl www.bitacoraindulto.titulodigital.udp.cl	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
2977779547	2020-06-19	2020-06-19	2020-09-17	cpanel.titulodigital.udp.cl cpcalendars.titulodigital.udp.cl cpcontacts.titulodigital.udp.cl mail.titulodigital.udp.cl titulodigital.udp.cl webdisk.titulodigital.udp.cl webmail.titulodigital.udp.cl www.titulodigital.udp.cl	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
2977779520	2020-06-19	2020-06-19	2020-09-17	lafamilia.titulodigital.udp.cl www.lafamilia.titulodigital.udp.cl	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
2977779587	2020-06-19	2020-06-19	2020-09-17	cpanel.titulodigital.udp.cl cpcalendars.titulodigital.udp.cl	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"

https://blog.segu-info.com.ar/2018/03/ctfr-y-crtsh-para-extraer-subdominios.html

Subdomains attacks

¿Qué hacer si se deja de usar un subdominio asociado a un sitio de un tercero?

https://blog.segu-info.com.ar/2020/06/el-peligro-de-los-subdominios.html

HTTP/S in one command line

```
python -m SimpleHTTPServer
python3 -m http.server
```

```
pip install ext_http_server
openssl req -new -x509 -days 365 -nodes -out cert.pem
-keyout cert.pem
ext_http_server --cert cert.pem -d . -a user:password
```

https://github.com/bboe/extended_http_server

Certificate Revocation Systems

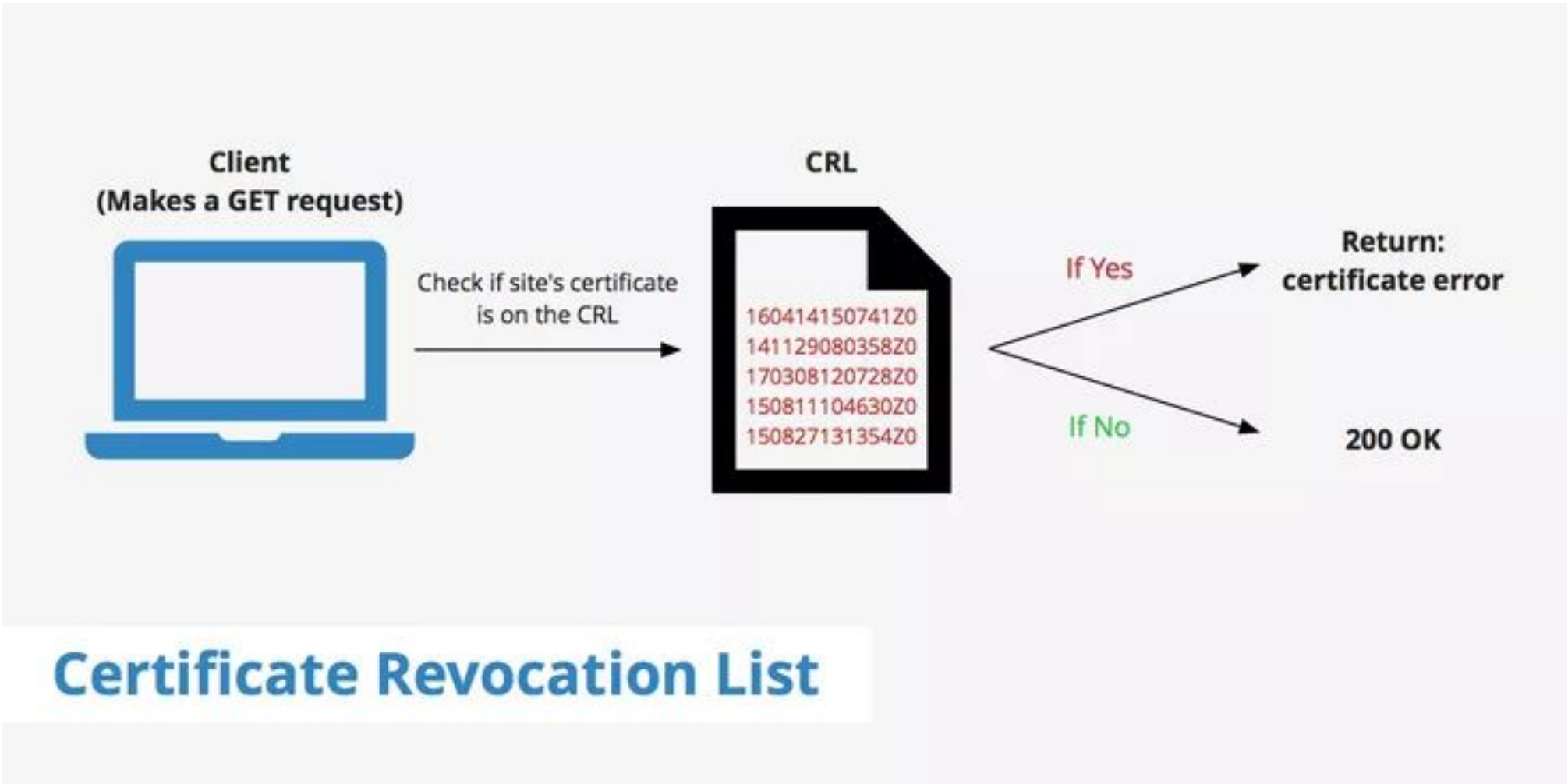
- Certificate Revocation Lists (CRL)
- Online Certificate Status Protocol (OCSP)
- Soft-fail behavior
- OCSP Stapling
- Must-staple extension
- Chrome CRLset and Firefox OneCRL

https://medium.com/@alexeysamoshkin/how-ssl-certificate-revocation-is-broken-in-practice-af3b63b9cb3

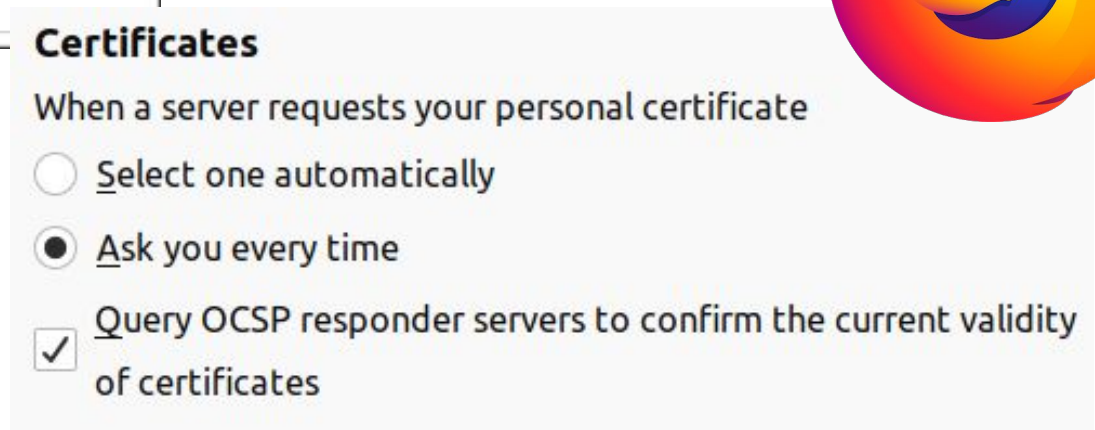
Certificate Revocation Lists

- CRL se almacena en el equipo local.
- La CRL puede quedar obsoleta, al igual que un antivirus, si no se mantiene actualizada todo el tiempo.

CRL


Client
(Makes a GET request)
Check if site's certificate
is on the CRL
CRL
160414150741Z0
141129080358Z0
170308120728Z0
150811104630Z0
150827131354Z0
If Yes
Return:
certificate error
If No
200 OK
Certificate Revocation List

CRL



https://github.com/agl/crlset-tools
https://www.keycdn.com/support/certificate-revocation-list

¿Qué info contienen los CRL?

openssl crl -inform DER -in FILENAME.crl -text -noout

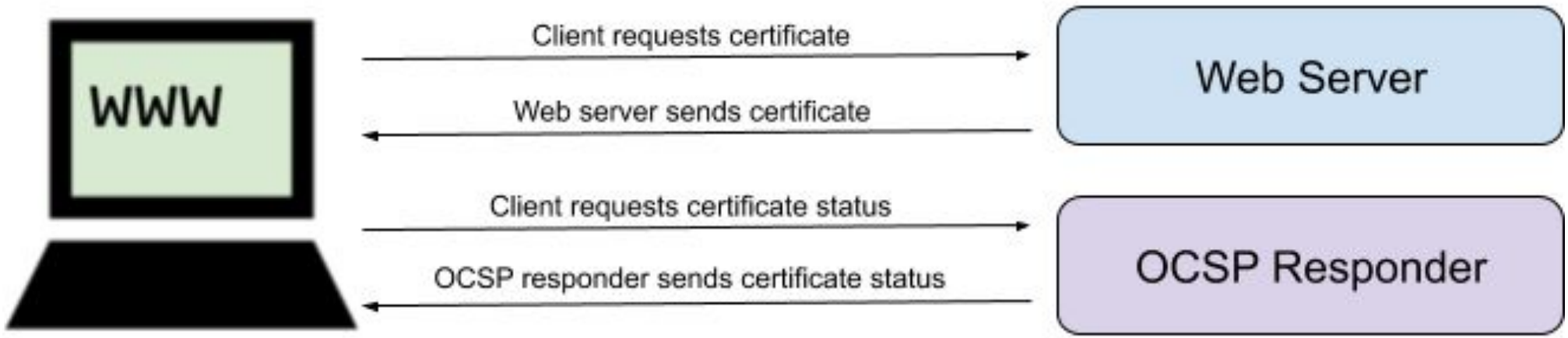
```
openssl crl -inform DER -in fcpca.crl -text -noout

Certificate Revocation List (CRL):
        Version 2 (0x1)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, O = U.S. Government, OU = FPKI, CN = Federal Common Policy CA
        Last Update: Oct 17 08:30:11 2019 GMT
        Next Update: Oct 18 02:30:00 2019 GMT
        CRL extensions:
            X509v3 CRL Number:
                6552
            X509v3 Authority Key Identifier:
                keyid:AD:0C:7A:75:5C:E5:F3:98:C4:79:98:0E:AC:28:FD:97:F4:E7:02:FC

Revoked Certificates:
    Serial Number: 5C84
        Revocation Date: May  7 14:33:41 2018 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Privilege Withdrawn
    Serial Number: 019A
        Revocation Date: Mar  5 15:11:10 2019 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Superseded
```

https://fpki.idmanagement.gov/crls/

Online Certificate Status Protocol

- Es un método para determinar el estado de vigencia de un certificado digital X.509 usando otros medios que no sean el uso de CRL (Listas de Revocación de Certificados). Este protocolo se describe en el RFC6960 y está en el registro de estándares de Internet.
- Analiza el número de serie del certificado.
- Si la comprobación no es posible, el certificado se considera inválido.

OCSP


WWW
Client requests certificate
Web server sends certificate
Web Server
Client requests certificate status
OCSP responder sends certificate status
OCSP Responder

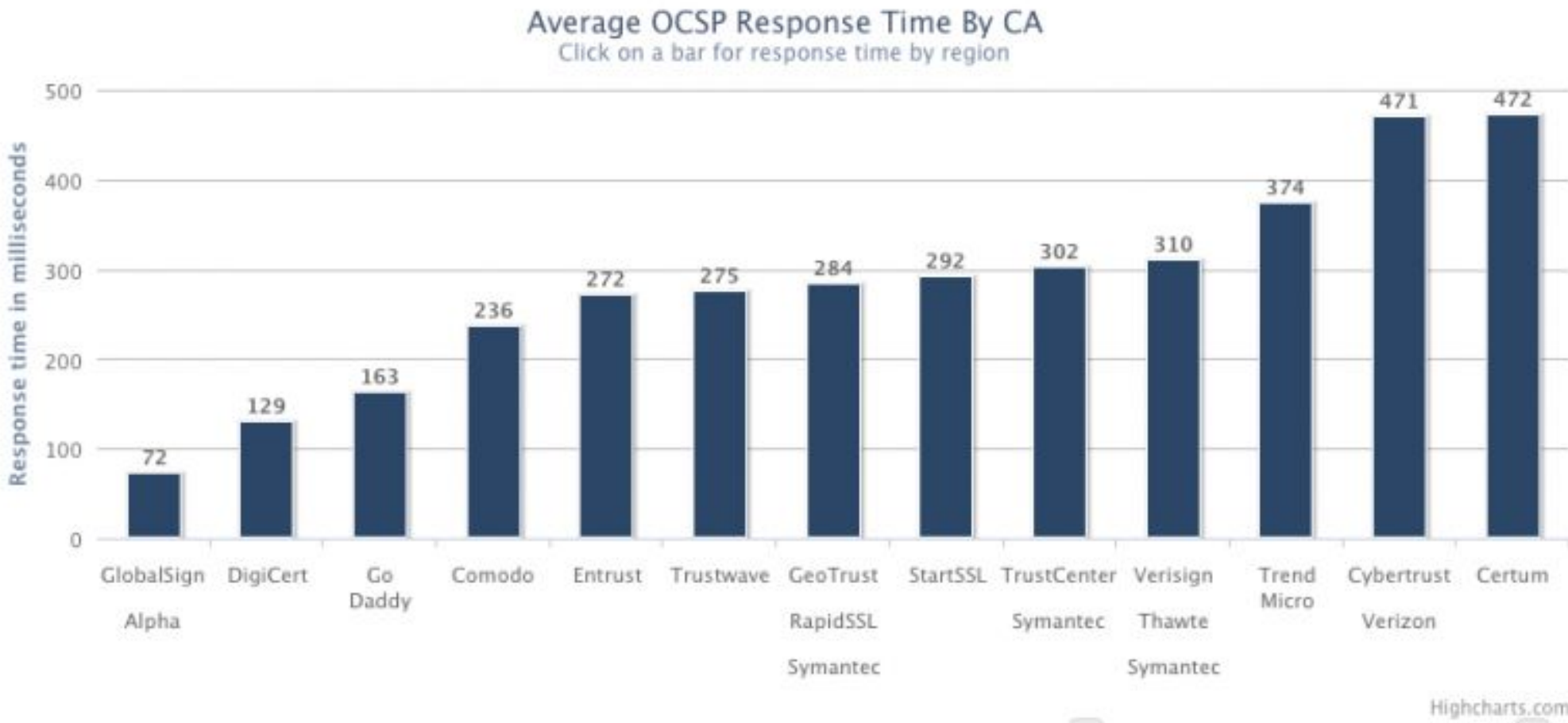
OCSP Responder

```
openssl s_client -connect akamai.com:443 2>&1
 < /dev/null | sed -n '/-----BEGIN/,/-----END/p' > cer
t.pem
openssl x509 -in cert.pem -noout -ocsp_uri


http://ocsp.digicert.com
```

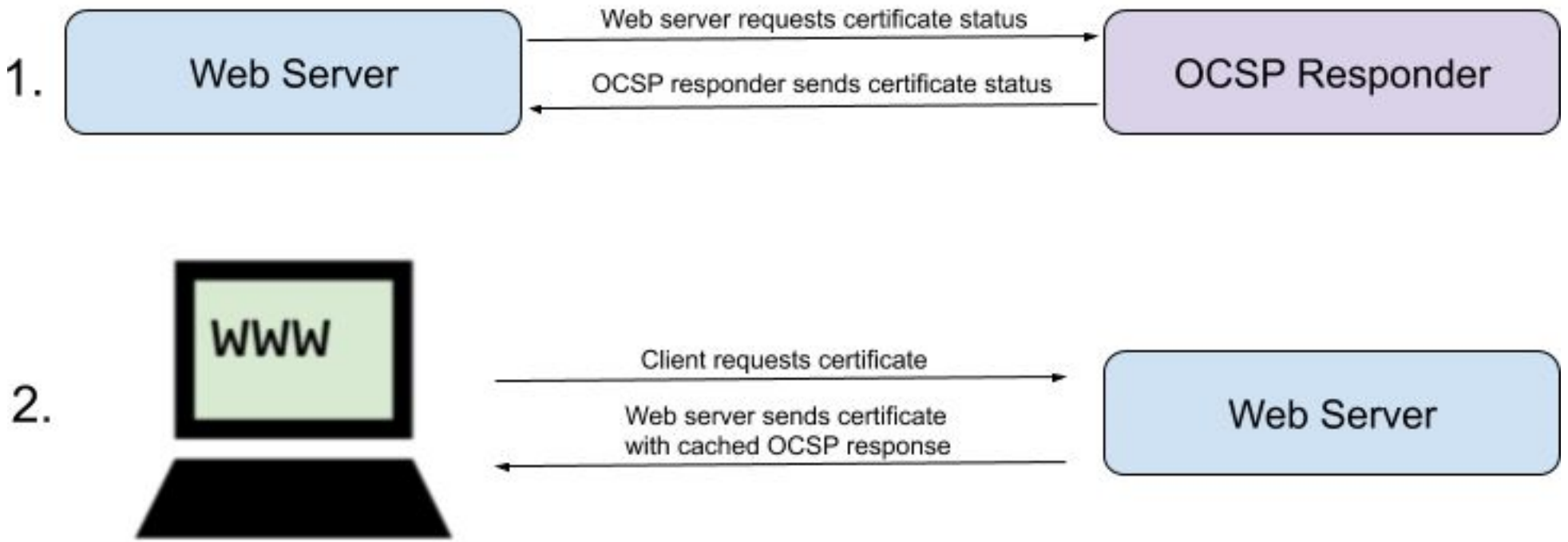
https://akshayranganath.github.io/OCSP-Validation-With-Openssl/

https://www.freecodecamp.org/news/openssl-command-cheatsheet-b441be1e8c4a/

OCSP


Average OCSP Response Time By CA
Click on a bar for response time by region
Response time in milliseconds
500
400
300
200
100
0
72
129
163
236
272
275
284
292
302
310
374
471
472
GlobalSign
Alpha
DigiCert
Go
Daddy
Comodo
Entrust
Trustwave
GeoTrust
RapidSSL
Symantec
StartSSL
TrustCenter
Symantec
Verisign
Thawte
Symantec
Trend
Micro
Cybertrust
Verizon
Certum
Highcharts.com

OCSP Stapling



https://www.ssl.com/faqs/what-is-ocsp-online-certificate-status-protocol/

Certificates Revoked per Day

https://isc.sans.edu/crls.html

OneCRL

Audit details

Disclosed via the CCADB

Auditor	Standard Audit	BR Audit	EV SSL Audit	Documents	CCADB	Owner / Certificate
LSTI	ETSI EN 319 411: 2019-12-18 (2018-11-23 to 2019-10-18)	ETSI EN 319 411: 2019-12-18 (2018-11-23 to 2019-10-18)	ETSI EN 319 411: 2019-12-18 (2018-11-23 to 2019-10-18)	CP CPS	0011J00001FB3O0QAL	Root CA: Dhimyotis / Certigna This CA: Dhimyotis / Certigna

Revocation

Report a problem with this certificate to the CA

Mechanism	Provider	Status	Revocation Date	Last Observed in CRL	Last Checked (Error)
OCSP	The CA	Check	?	n/a	?
CRL	The CA	Revoked	2020-03-10 11:44:47 UTC	2020-03-10 16:16:48 UTC	2020-06-20 20:10:20 UTC
CRLSet/Blacklist	Google	Not Revoked	n/a	n/a	n/a
disallowedcert.stl	Microsoft	Not Revoked	n/a	n/a	n/a
OneCRL	Mozilla	Revoked [by Issuer Name, Serial Number]	Unknown	n/a	n/a

https://crt.sh/mozilla-onecrl

¿Cómo acelerarlo?

Acelerador SSL

- Un servidor SSL debe cifrar, descifrar, calcular hash, verificar firma digital, etc. de cada sesión SSL de algún cliente.
- Un servidor SSL de alto tráfico (un Banco, una tienda virtual) puede tener la CPU al 100 % en cálculos de algoritmos criptográficos.
- El costo de tener un cluster de servidores puede ser prohibitivo.
- Un Acelerador SSL es hardware especializado que se encarga de la criptografía.

Tarjetas Aceleradoras SSL

- Tarjetas que implementan todos los algoritmos criptográficos de SSL en hardware.
- Tienen una API criptográfica que se puede integrar con servidores Web.
- Funcionan sólo con determinados servidores Web y depende de la arquitectura y sistema operativo.
- Todo el protocolo SSL lo maneja la tarjeta y el servidor sólo se encarga del HTTP “puro”.

Hardware SSL

SPECIFICATIONS	i15800/i15800-N
Intelligent Traffic Processing:	L7 requests per second: 10M L4 connections per second: 4.2M L4 HTTP requests per second: 35M Maximum L4 concurrent connections: 300M Throughput: 320 Gbps/160 Gbps L4/L7
Hardware Offload SSL/TLS:	ECC†: 100K TPS (ECDSA P-256) RSA: 160K TPS (2K keys) 50 Gbps bulk encryption*
FIPS SSL:	N/A
Hardware Compression:	60 Gbps
Hardware DDoS Protection:	210M SYN cookies per second

Nomenclatura

- TPS (Transactions Per Second)
- CPS (Connection Per Second)
- FIPS (Federal Information Processing Standards) 140: Certifica distintos niveles de seguridad en criptografía.

SSL Bandwidth Table		
Link Type	**Link Speed**	**SSL Connection Rate**
T1	1.5 Mbps	8.5 TPS
Ethernet	10 Mbps	56.8 TPS
DS3	45 Mbps	255.7 TPS
Fast Ethernet	100 Mbps	568.1 TPS
OC3	155 Mbps	880.7 TPS
Gigabit Ethernet	1,000 Mbps	5681.8 TPS

http://csrc.nist.gov/publications/PubsDrafts.html#FIPS-140--3

Firewalls NG

Vendor	512b Cipher Performance Loss	1024b Cipher Performance Loss	2048b Cipher Performance Loss
Juniper SRX3600	34%	13%	36%
Stonesoft 3202	54%	60%	76%
Palo Alto Networks PA-5020	66%	78%	79%
SourceFire 8250	77%	78%	83%
Check Point 12600	87%	87%	87%
Dell SonicWall E10800	84%	85%	94%
Fortinet 3600C	93%	93%	94%
SourceFire 8290	94%	94%	96%
Vendor	**512b Cipher Transactions Per Second**	**1024b Cipher Transactions Per Second**	**2048b Cipher Transactions Per Second**
Juniper SRX3600	8,400	8,400	8,000
SourceFire 8250	18,000	17,800	6,800
SourceFire 8290	18,000	17,800	6,800
Palo Alto Networks PA-5020	5,098	4,662	3,767
Dell SonicWall E10800	15000	12200	2600
Stonesoft 3202	7,500	6,250	2,000
Check Point 12600	1,500	1,500	1,500
Fortinet 3600C	1,516	1,424	1,294

Figure 1 – SSL Performance Impacts on Bandwidth and Transaction per Second Loss

https://www.nsslabs.com/

Juniper SRX 3600

http://www.cdw.com/shop/

¿Dónde se usa FIPS 140?

Momentus® Laptop Hard Drives

Seagate® Momentus® hard drives deliver high capacity and performance along with innovative technology, such as self-encryption and free-fall sensors. If you require feature-rich, reliable, robust and secure laptop storage, Momentus drives are for you. Now with FIPS 140-2 Validated models available.**

Capacity

Options ?

Interface

Cache

Spin Speed (RPM)

Model ST9750423AS | SATA 3Gb/s | 750GB | 16MB | 5400 |

IronKey FIPS 140-2 LEVEL 3 CERTIFIED D200 MLC USB & Flash Drives (8 GB) (D2-D200-S08-3FIPS)

$102.00 10 stores

No reviews yet.
Be the first!

Type: USB Flash Drive

Capacity: 8 GB

See more features

Add to list Price Alert Share

OpenSSL w/FIPS 140-2 certificate

The OpenSSL certification is special because this type of certificate usually applies to ready-to-use, executable program packages; in this case, NIST has certified the source code. The certificate, however, is only valid if executable code is generated from the validated, unchanged source code according to a precisely documented method.

http://openssl.org/docs/fips/UserGuide-2.0.pdf

Operative System with FIPS 140-2

Blackberry 10 ahora tiene certificación FIPS 140-2.
Su objetivo es validar que los procedimientos de cifrado en transmisiones sean lo bastante seguros como para ser utilizados por Instituciones y empresas relacionadas con el gobierno.

http://bizblog.blackberry.com/

¿Cuándo empezó el boom SSL?

twitter blog

Making Twitter more secure: HTTPS

Tuesday, March 15, 2011

Tweet Privacy

☐ Protect my tweets

Only let people whom I approve follow my tweets.
If this is checked, your future tweets will not be available publicly. Tweets posted previously may still be publicly visible in some places.

HTTPS Only

☑ Always use HTTPS.

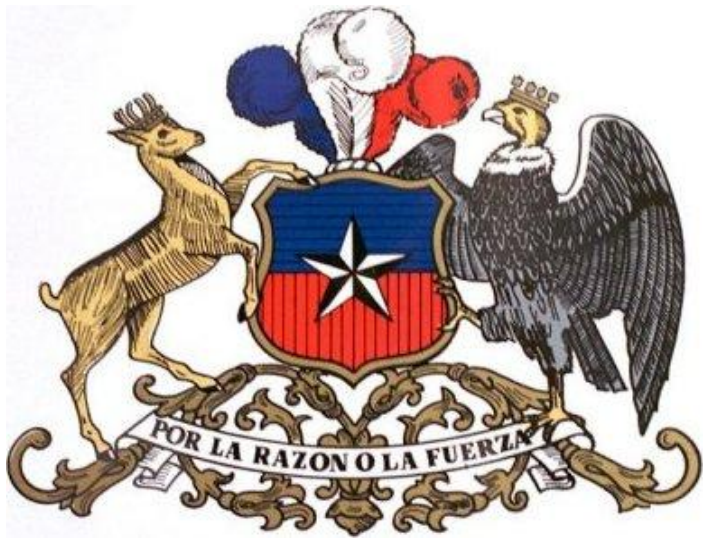
Save

Deactivate my account.

@twitterglobalpr
Twitter Comms

We suggest using HTTPS for improved security. We're starting to turn this on by default for some users. More here: support.twitter.com/articles/48195...

23 Aug by RachaelRad via web



un año después...

Securing your Twitter experience with HTTPS

Monday, February 13, 2012

Last year, we added the option to always use HTTPS when accessing Twitter.com on the web. This setting makes your Twitter experience more secure by protecting your information, and it's especially helpful if you use Twitter over an unsecured Internet connection like a public wi-fi network.

Now, HTTPS will be on by default for all users, whenever you sign in to Twitter.com. If you prefer not use it, you can turn it off on your Account Settings page. HTTPS is one of the best ways to keep your account safe and it will only get better as we continue to improve HTTPS support on our web and mobile clients.

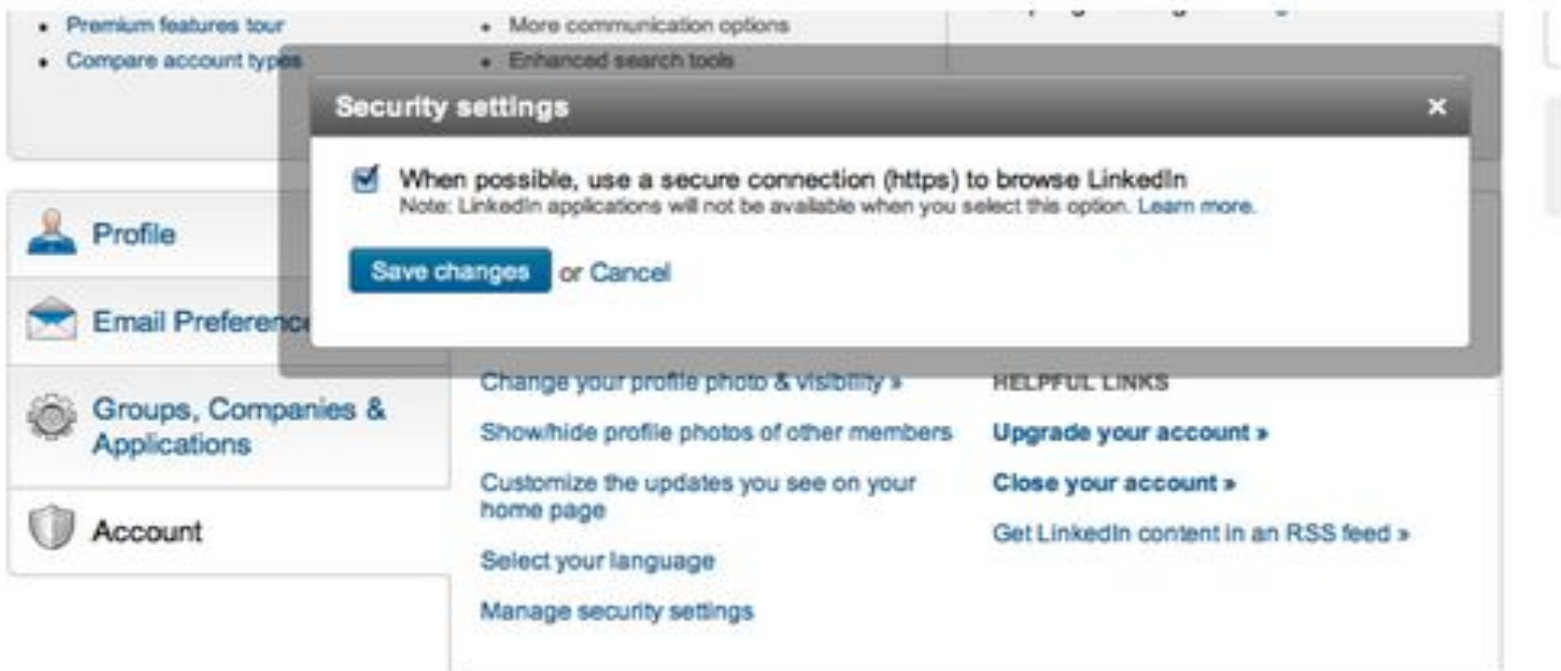
http://blog.twitter.com/

Linkedin

A More Secure LinkedIn Browsing Experience

Arvind Mani, February 7, 2012

We are happy to announce LinkedIn now supports *https* for your browsing experience. This is currently an "opt in" feature that will be rolled out gradually in the next coming weeks to all of our members. Serving our site over *https* is a key step to enhance the security for all of you, especially for those of you using public networks such as open WiFi hotspots.



http://blog.linkedin.com/2012/02/07/linkedin-ssl/

El blog de Facebook

A Continued Commitment to Security

por Alex Rice el miércoles, 26 de enero de 2011 a las 10:13

This Friday is Data Privacy Day, an international effort by governments, businesses and advocacy groups to raise awareness about the importance of staying in control of personal information. A key part of controlling information has always been protecting it from security threats like viruses, malware and hackers.

That's why we've developed a number of complex systems that operate behind the scenes to keep you secure on Facebook. In addition, we've created some advanced features you can use to help protect yourself even more, such as remote logout and one-time passwords. These features are especially useful when you're uncertain whether your network or computer is secure. Today, we're announcing two new such features.

A Secured Connection

If you've ever done your shopping or banking online, you may have noticed a small "lock" icon

n. This indicates that your
th the website and ensure that
HTTPS whenever your
to help keep your data even

Seguridad de la cuenta Ocultar

Configura la navegación segura (https) y las alertas de inicio de sesión.

Navegación segura (https)

☑ Usar Facebook mediante una conexión segura (https) cuando sea posible

Cuando un dispositivo móvil o una computadora nueva entre en esta cuenta:

☑ Enviarme un mensaje de correo electrónico

Guardar

¿Seguridad o Xperia?

https://blog.hboeck.de/archives/754-Playing-with-the-EFF-SSL-Observatory.html

ELECTRONIC FRONTIER FOUNDATION

ENCRYPT THE WEB:
INSTALL HTTPS
EVERYWHERE

https://www.eff.org/https-everywhere

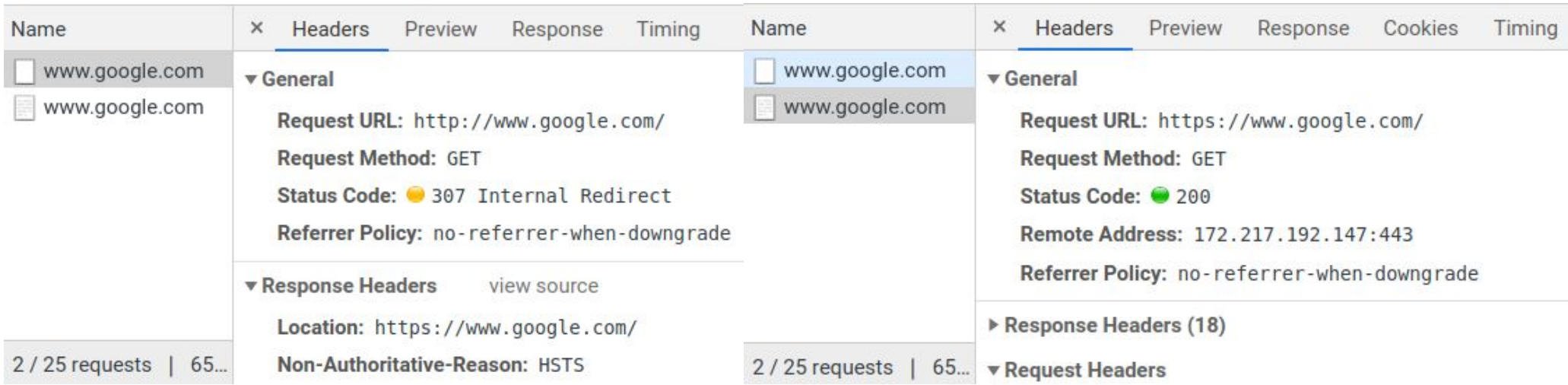
HTTP Strict Transport Security (HSTS)

- Impide que las páginas se carguen si no están protegidas por SSL.

```
# load module (example using [RHEL])
LoadModule headers_module modules/mod_headers.so

# Use HTTP Strict Transport Security to force client to use secure connections only
Header always set Strict-Transport-Security "max-age=500; includeSubDomains"

# redirect all HTTP to HTTPS
<VirtualHost *:80>
	ServerAlias *
	RewriteEngine On
	RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [redirect=301]
</VirtualHost>
```

http://tools.ietf.org/

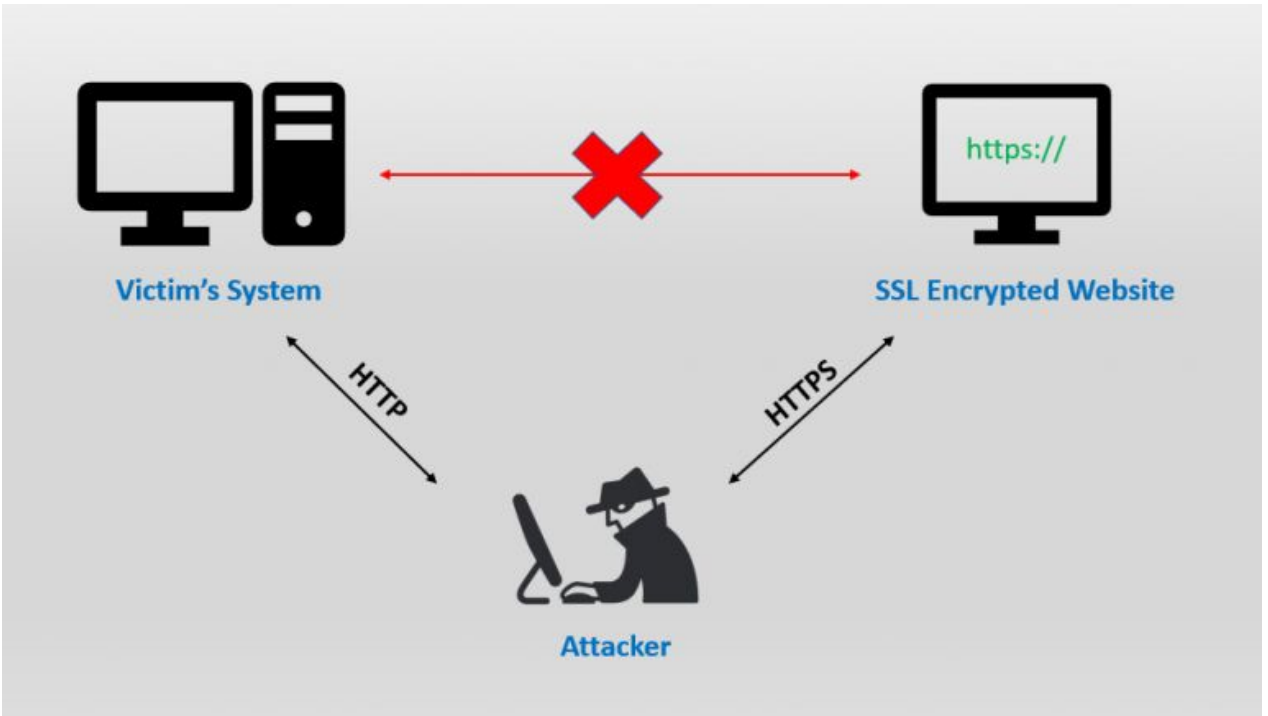
HSTS Aprobado!



https://httpsnow.org/

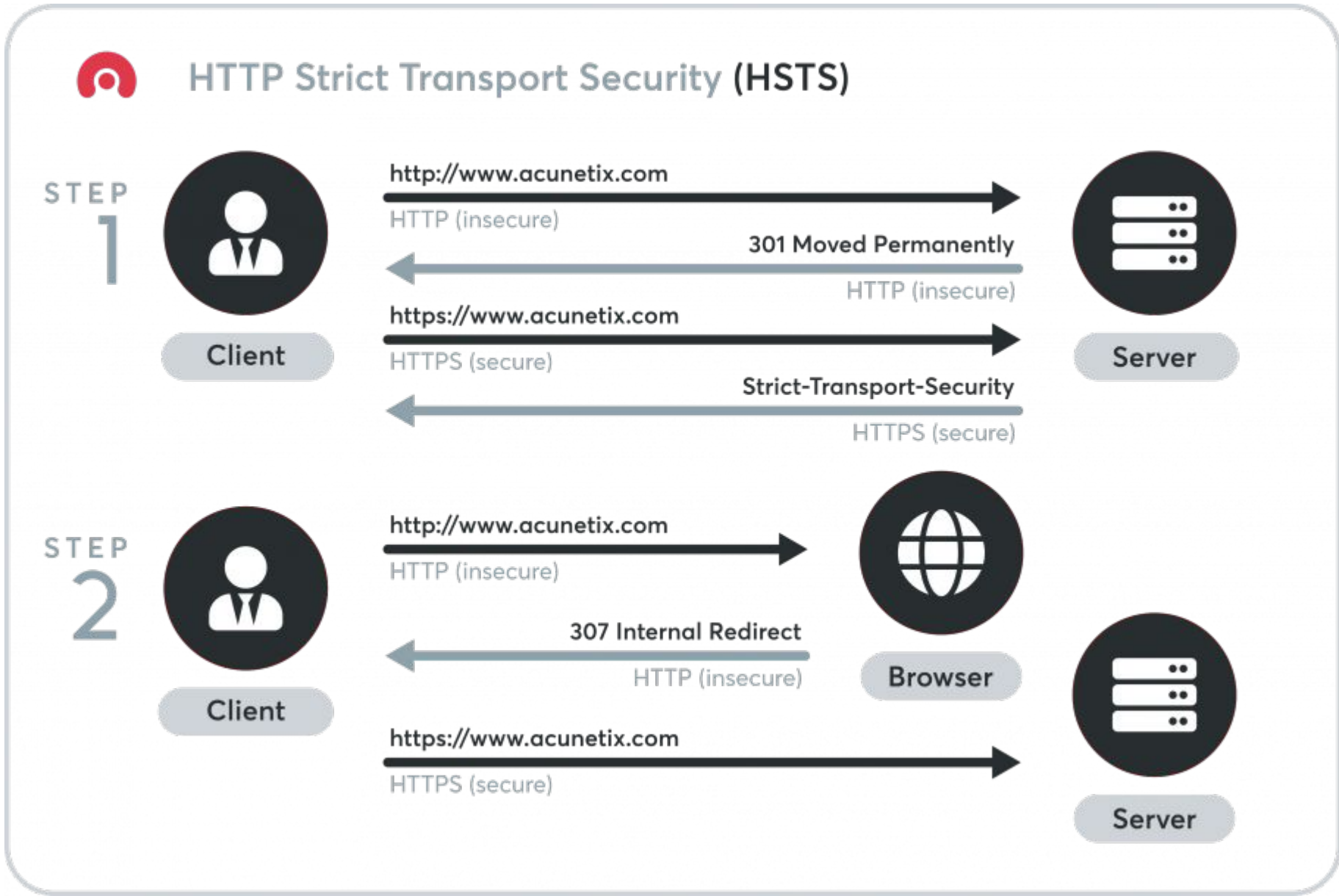
Atacando HSTS

Consultas previas por HTTP
NTP
MiTMF



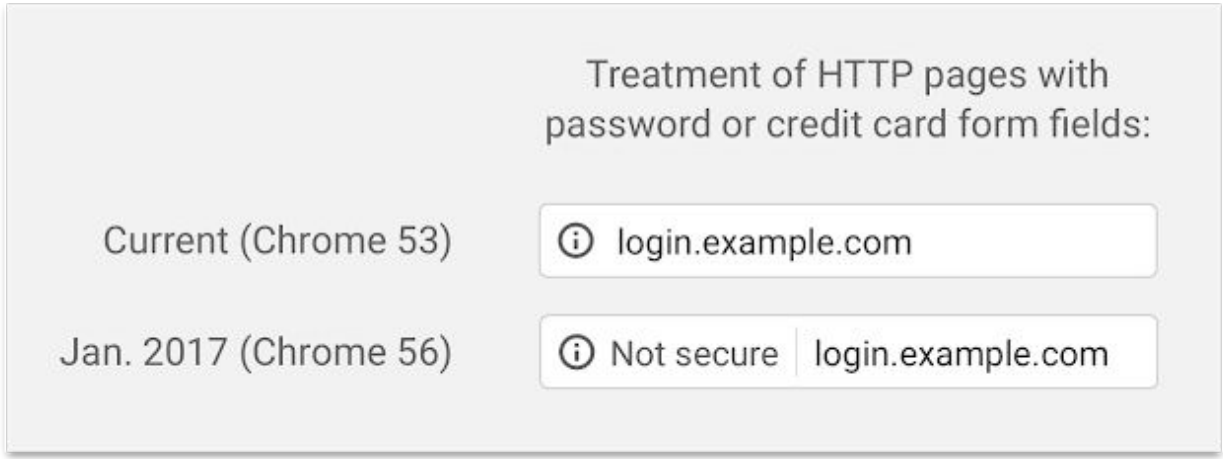
https://www.elladodelmal.com/2016/03/ataques-man-in-middle-hsts-sslstrip-2.html

¿Cómo funciona HSTS?



HTTP sites as “not secure”

En enero de 2017 Chrome 56 empezó a notificar como inseguros los sitios que enviaban la password o tarjetas de crédito en texto plano.
A partir de Julio de 2018, Chrome 68 empezó a notificar que todos los sitios sin SSL/TLS son inseguros.



https://security.googleblog.com/2018/02/a-secure-web-is-here-to-stay.html

Tiempo máximo de validez

En el 2018 se pasó de 3 años a tan solo 2 años como periodo máximo de validez.

https://www.ssls.com/blog/changes-ssl-certificate-validity-period/

Seguridad o negocio?

The CA/Browser Forum propuso que en marzo de 2020 pasen a tener una validez máxima de 13 meses.

https://blog.segu-info.com.ar/2019/08/quieren-reducir-los-certificados-https.html

Safari sólo permitirá hasta 1 año

Dean Coclin
@chosensecurity

Today's big news: One year max public TLS certs are coming, starting 1 Sept 2020, if you want to be trusted in Safari.

7:10 PM · Feb 19, 2020 · Twitter Web App

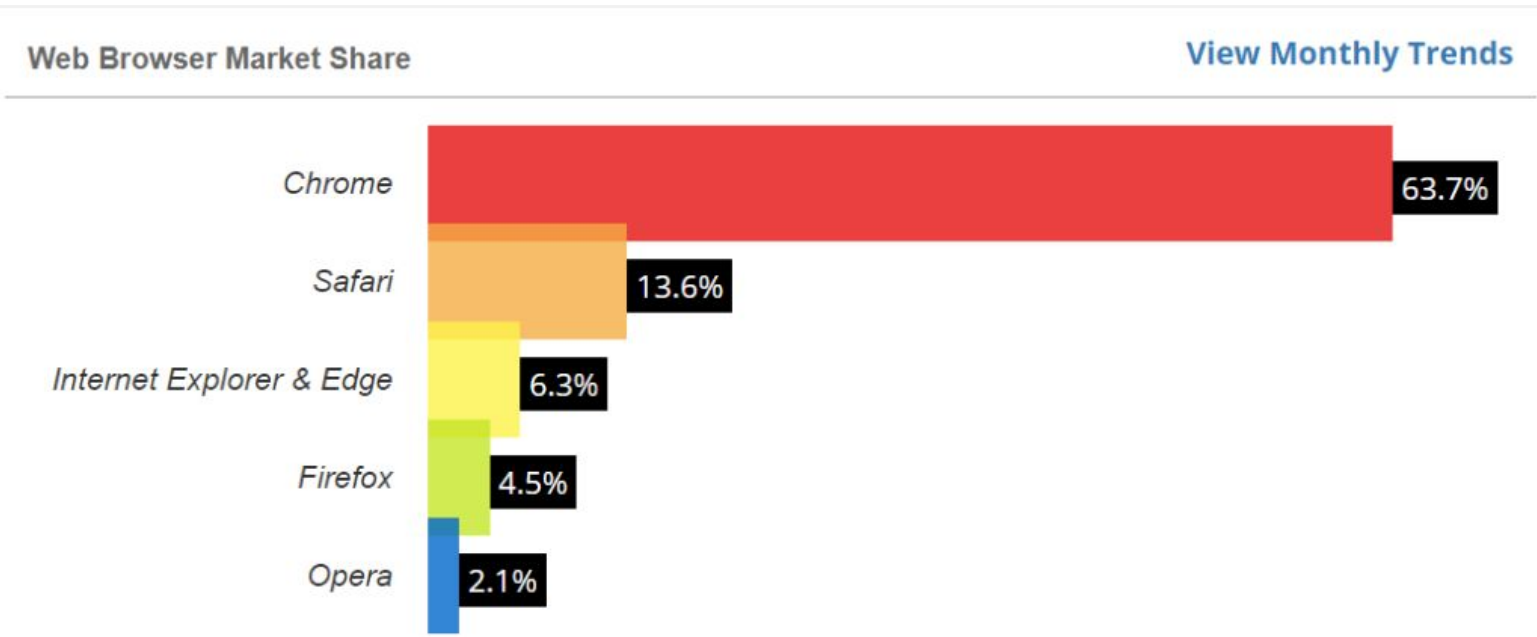
https://wwwhatsnew.com/2020/02/24/safari-rechazara-certificados-https-con-validez-de-mas-de-13-meses/

Chrome se le une

Dean Coclin
@chosensecurity

Chrome joins Apple in limiting public TLS certificates to 398 days starting Sept 1st.

4:45 PM · Jun 10, 2020 · Twitter Web App

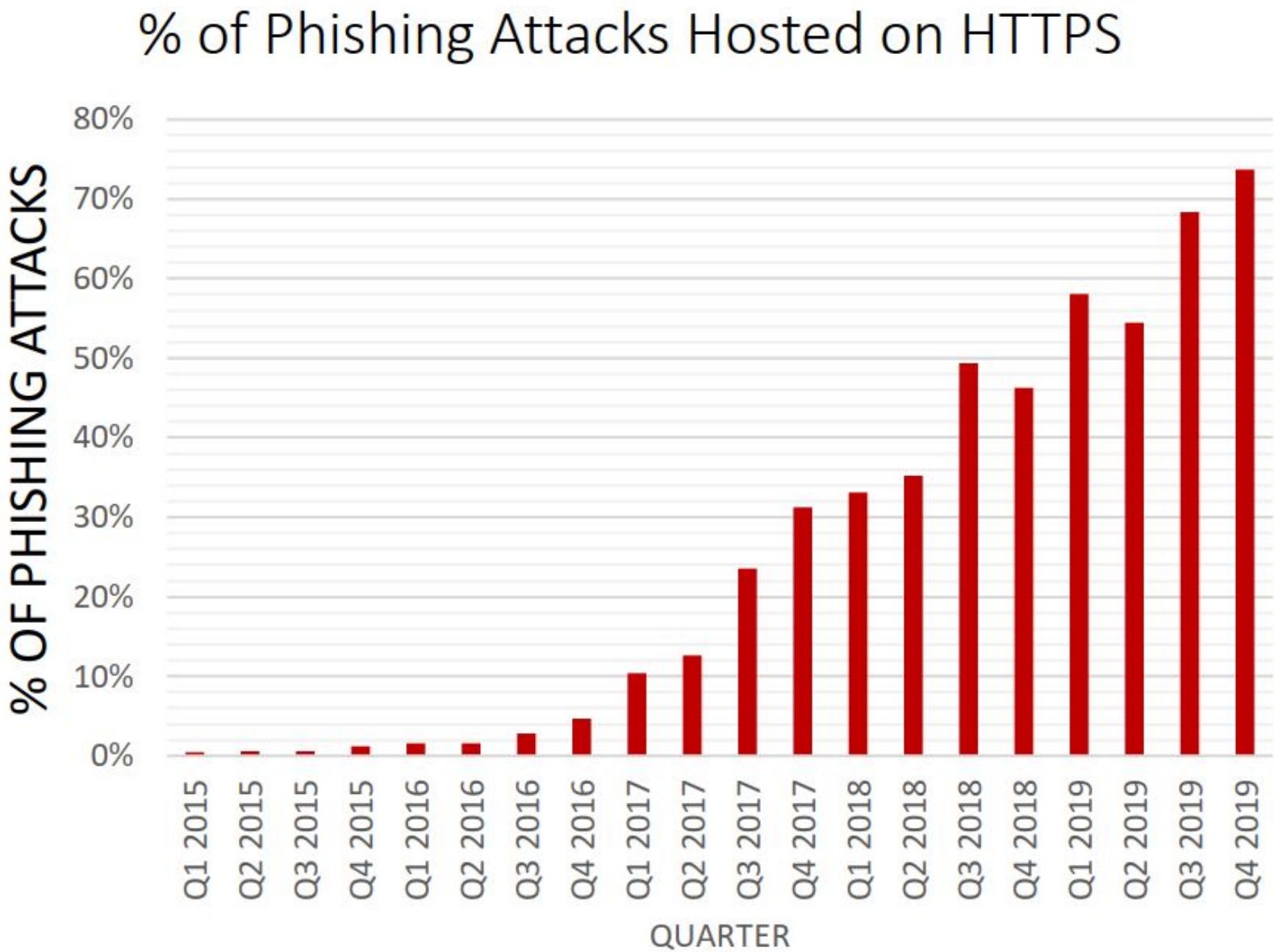


SSL for 5 years!

Sectigo Subscription SSL permite renovar automáticamente el certificado hasta por 5 años.

https://www.helpnetsecurity.com/2019/10/25/sectigo-subscription-ssl/

Phishing


% of Phishing Attacks Hosted on HTTPS
% OF PHISHING ATTACKS
80%
70%
60%
50%
40%
30%
20%
10%
0%
Q1 2015
Q2 2015
Q3 2015
Q4 2015
Q1 2016
Q2 2016
Q3 2016
Q4 2016
Q1 2017
Q2 2017
Q3 2017
Q4 2017
Q1 2018
Q2 2018
Q3 2018
Q4 2018
Q1 2019
Q2 2019
Q3 2019
Q4 2019
QUARTER

Ataques

Ataque Comodo

COMODO BR
Criando Confiança na Web

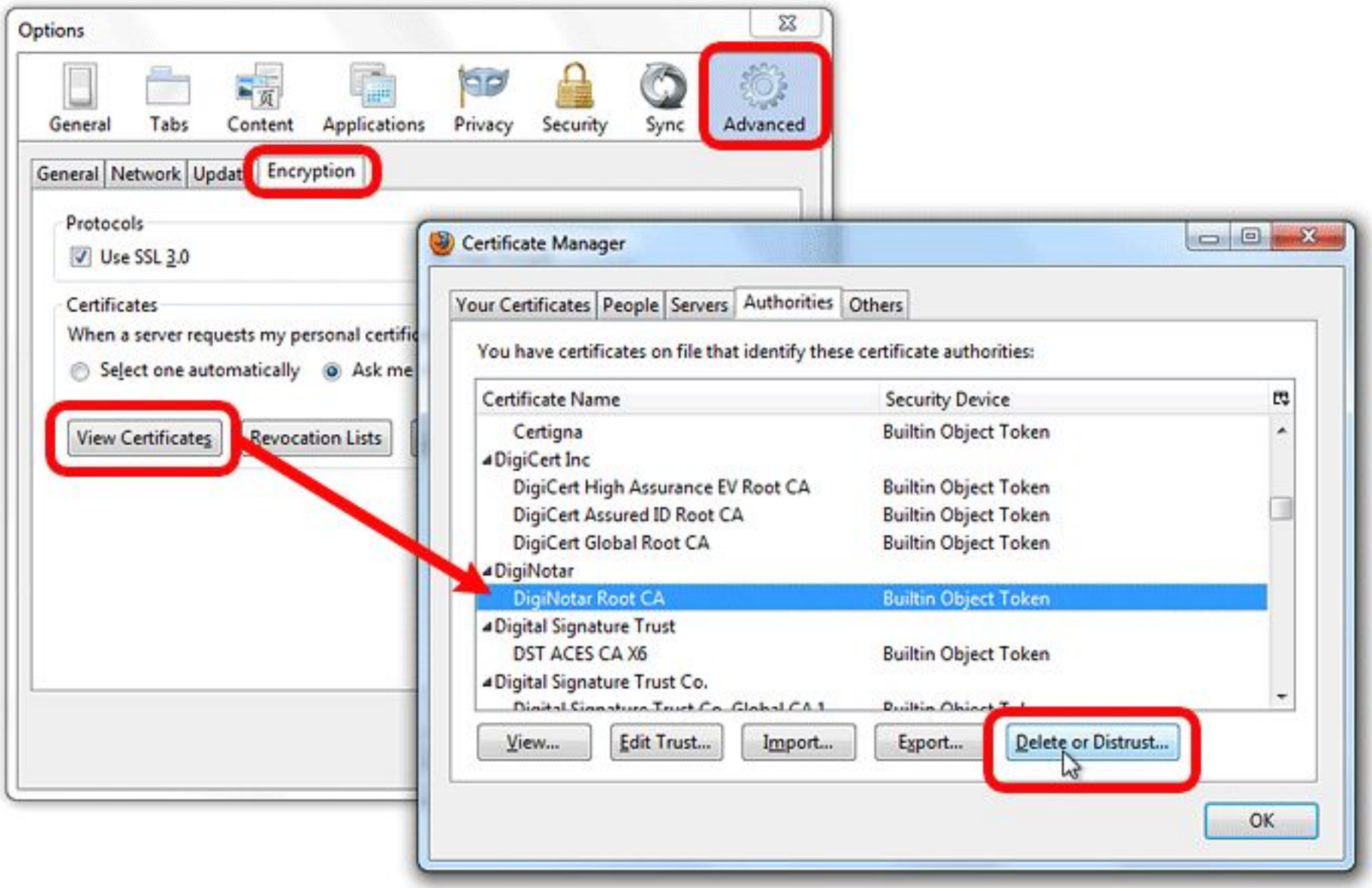
- A través de Inyección SQL

https://www.infosecurity-magazine.com/news/comodo-admits-two-more-registration-authorities-16986/

Ataque DigiNotar

- El certificado falso de google está disponible en: http://pastebin.com/ff7Yg663

Banned forever



Acciones...

Firefox 6.0.2 removes trust to DigiNotar CA

Posted on 07 September 2011.

BOOKMARK ...

Mozilla released Firefox 6.0.2 that removes trust exceptions for certificates issued by Staat der Nederlanden and therefore offers additional protection against fraudulent DigiNotar certificates.

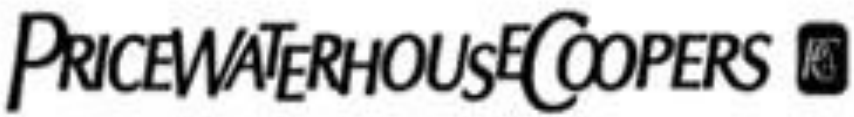
¿Cuándo un CA es válido?

- La CA debe completar una auditoría y enviar los resultados a Microsoft cada 4 meses.
- Windows deja de confiar en certificados SHA-1 a partir del 1 de enero de 2017.

https://docs.microsoft.com/en-us/security/trusted-root/program-requirements

¿Quién certificó a DigiNotar?

Date of issuance: November 1, 2010
Date of expiration: November 1, 2013



https://www.helpnetsecurity.com/2011/09/15/is-this-the-end-of-the-line-for-diginotar/

Caso La Polar

Hasta 2011, PwC era la auditora externa de 12 de las 40 empresas del Índice de Precio Selectivo de Acciones (IPSA), las que más transan en la bolsa. Sólo la superaba Ernst & Young, que auditaba a 13 de las grandes compañías. Deloitte estaba contratada por nueve y KPMG por seis.
Luego del escándalo de La Polar la mayoría de los clientes de PwC se cambiaron a Deloitte.

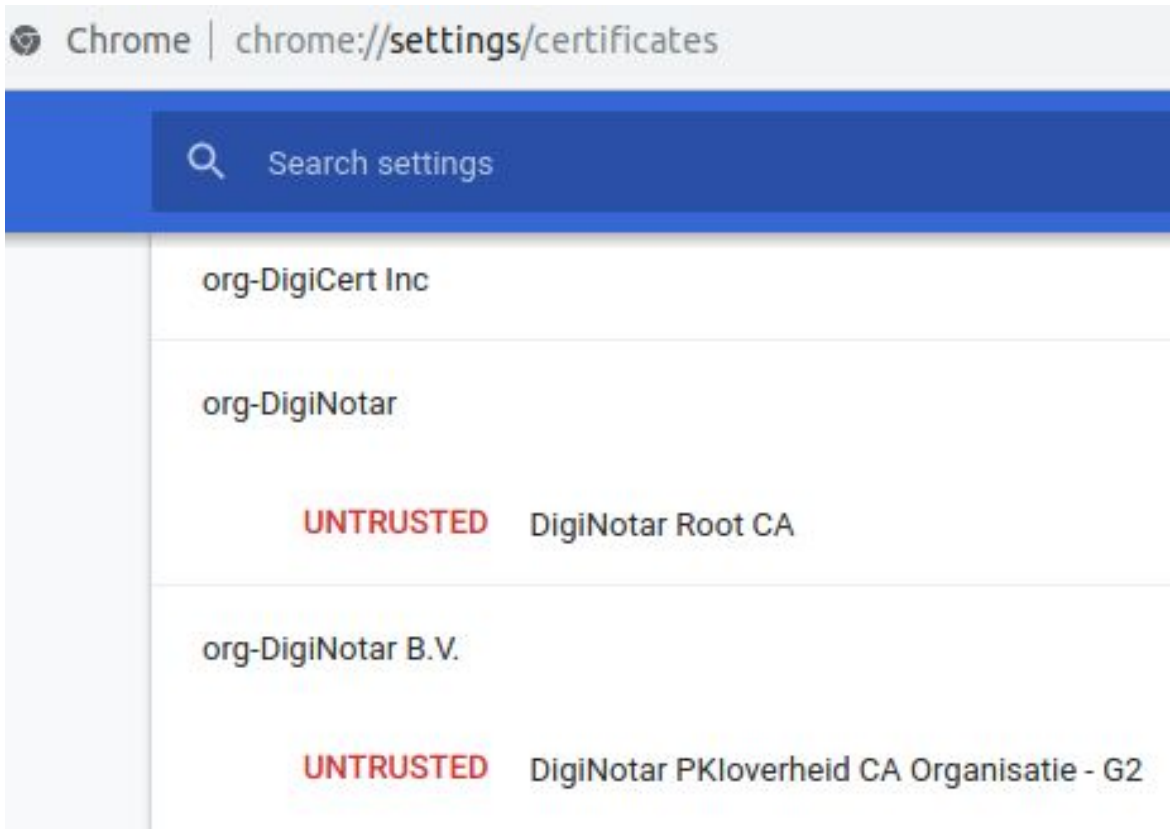
http://ciperchile.cl

Bankruptcy

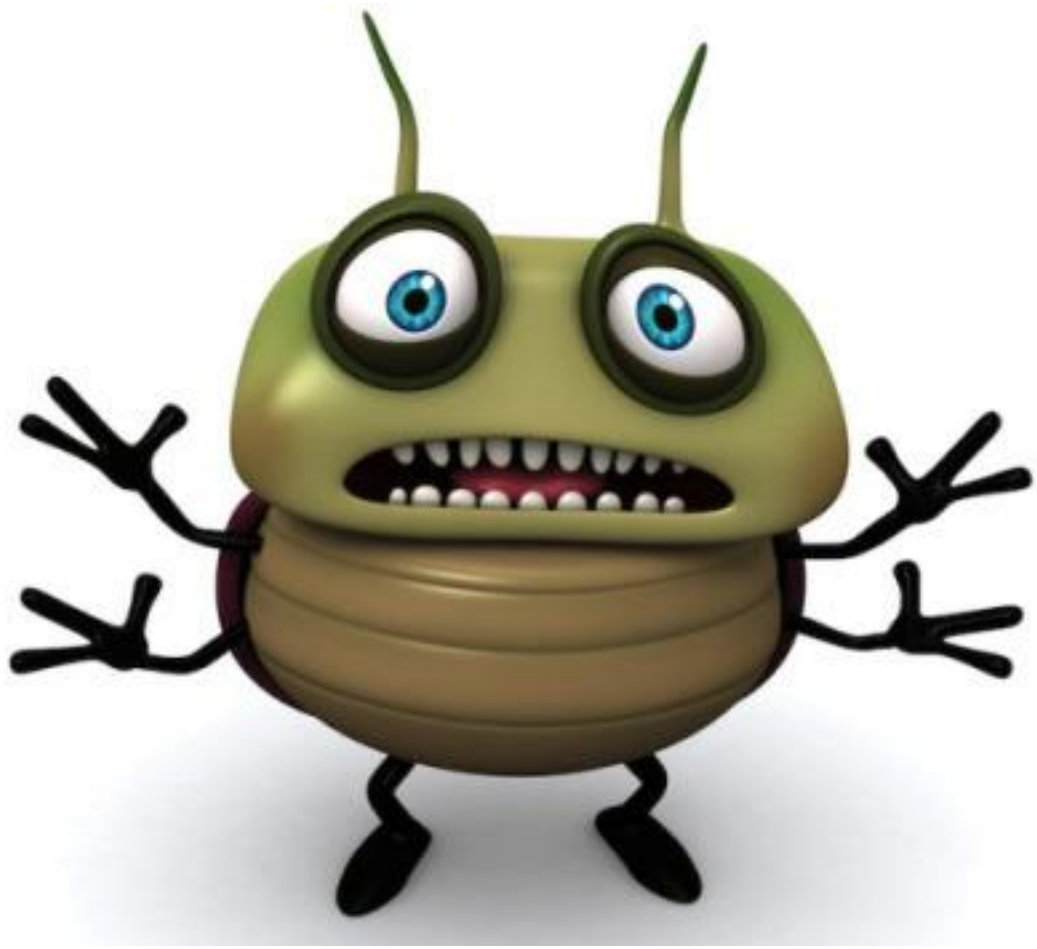
- El 20 de Septiembre del 2011, Vasco declara a Diginotar en bancarrota.

http://www.vasco.com/

Gestión de certificados...



RSA 512 it's a bug



https://bugzilla.mozilla.org/show_bug.cgi?id=360126

años atrás...

- **June 30, 2011** – Mozilla will stop accepting MD5 as a hash algorithm for intermediate and end-entity certificates. After this date software published by Mozilla will return an error when a certificate with an MD5-based signature is used.
  - This change is being tracked in Bugzilla #590364.

- **December 31, 2013** – Mozilla will disable or remove all root certificates with RSA key sizes smaller than 2048 bits.

https://wiki.mozilla.org/CA:MD5and1024

RSA 1024 bits

The CA/Browser Forum and leading browser vendors officially ended support for 1024-bit RSA keys after 2013.

Certification Authority/Browser (CA/B) Forum

Los estándares de la industria a través de CA/B Forum requiere que los certificados expedidos después del 1 de enero 2014 deben ser al menos de 2048 bits.

https://www.cabforum.org/Baseline_Requirements_V1.pdf

SSL upgrade

Todos los certificados SSL de google se actualizarán a llaves de 2048 bits para finales de 2013.

http://googleonlinesecurity.blogspot.se

ECDSA

- Se descubre vulnerabilidad en las firmas que usan Elliptic Curve Digital Signature Algorithm (ECDSA).
- Permite revelar la llave privada del servidor TLS.

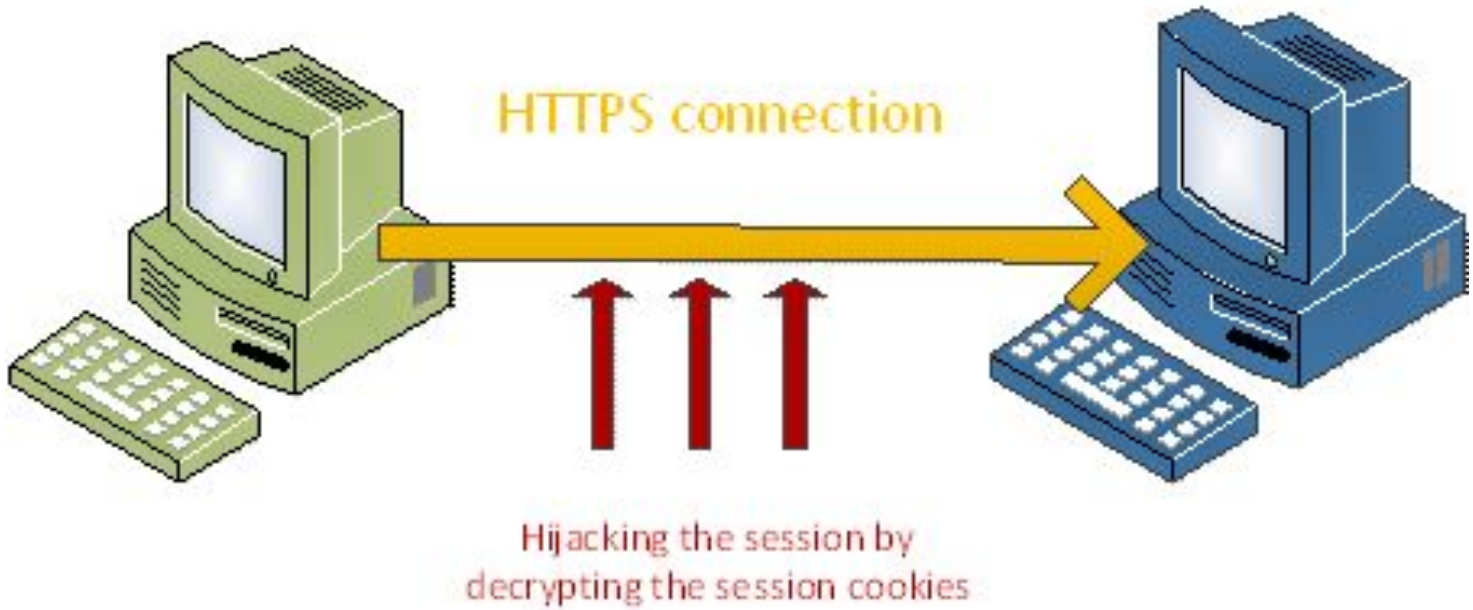
http://eprint.iacr.org/2011/232.pdf

Browser Exploit Against SSL / TLS

- Exploit formado por código Javascript y un sniffer de red que captura y desencripta los tokens de autenticación o las cookies de un usuario que accede a un sitio web seguro.
- BEAST permite crackear una cookie cifrada de PayPal en menos de 10 minutos.
- La única manera de estar totalmente seguro, es desactivar TLS 1.0, SSL 2.0 e incluso SSL 3.0, y usar las versiones 1.1 y 1.2 de TLS.

http://citeseerx.ist.psu.edu/

The Crime Attack



http://www.hackplayers.com/2012/09/CRIME-ataque-SSL-TLS-sucesor-BEAST.html

Heartbleed CVE-2014-0160

DOMAIN	VULNERABLE SITES	SAFE SITES	TOTAL NO. OF SITES USING SSL	TOTAL NO. OF SITES	PERCENTAGE
KR	57	45	102	2839	56%
JP	534	661	1195	17852	45%
RU	2708	3590	6298	38573	43%
CN	66	98	164	10430	40%
GOV	26	43	69	829	38%
BR	866	1782	2648	16328	33%
AU	553	1190	1743	7911	32%
UK	1073	2692	3765	19062	28%
DE	1544	4780	6324	34275	24%
FR	594	2474	3068	13033	19%
IN	611	2851	3462	13204	18%
Total	8632	20206	28838	174336	30%

https://www.us-cert.gov/ncas/alerts/TA14-098A

Sitios vulnerables ¿Aún lo serán?

demandafacil.cl
bysconsultora.cl
impocore.cl
activapatagonia.cl
ignaciomoragapropiedades.cl
vocesdelatierra.cl
powelec.cl
tradingmaipo.cl
cultivosm.cl
myomainstitute.cl
azafrangourmet.cl
safetree.cl
cuatroptos.cl

inviertepatagonia.cl
regaloslaesperanza.cl
celltek.cl

https://safeweb.norton.com/heartbleed

POODLE

Padding Oracle On Downgraded Legacy Encryption

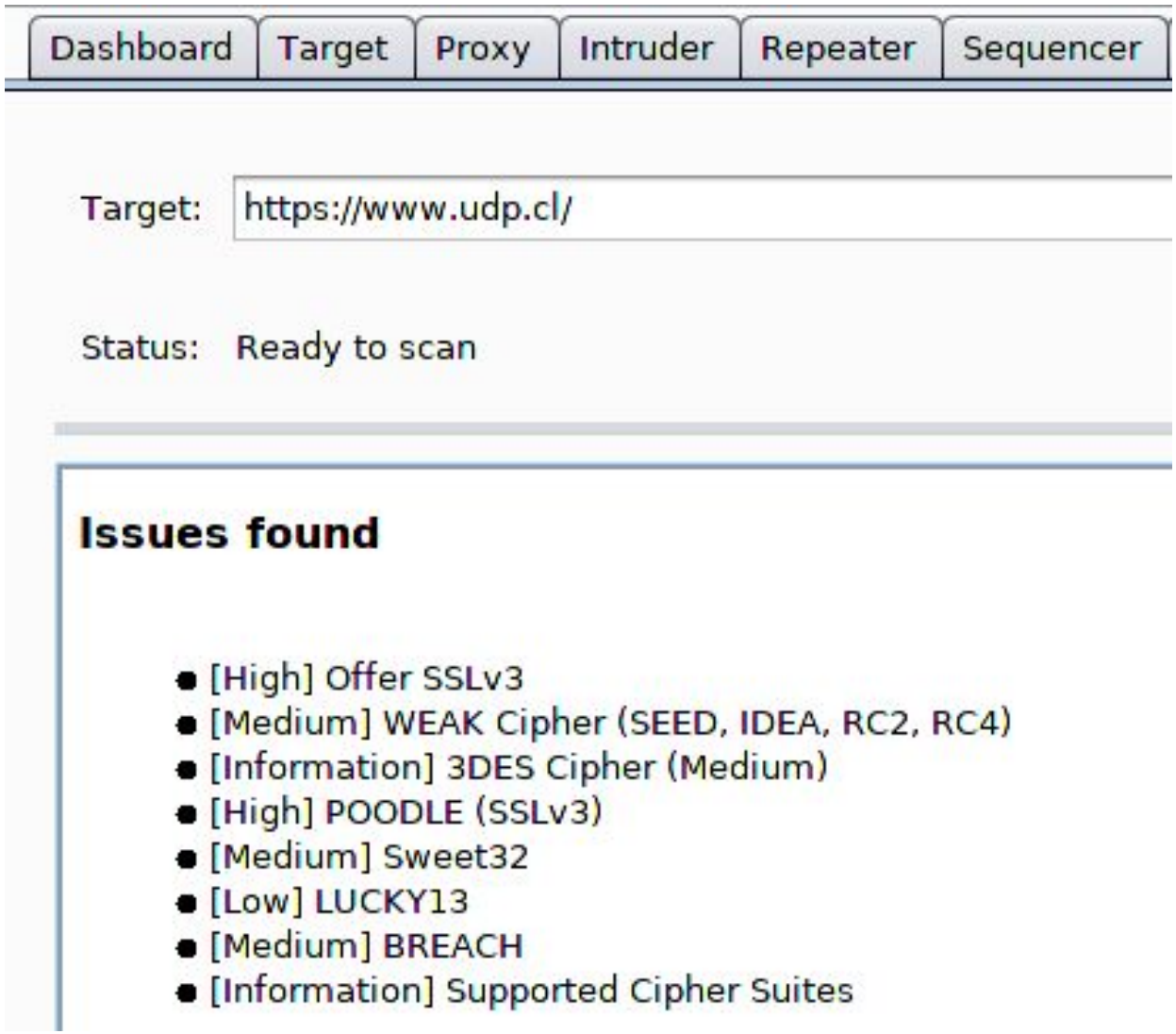
CVE-2014-3566

Poodle PoC?

https://asciinema.org/a/174901

https://github.com/mpgn/poodle-PoC

SSL Scanner

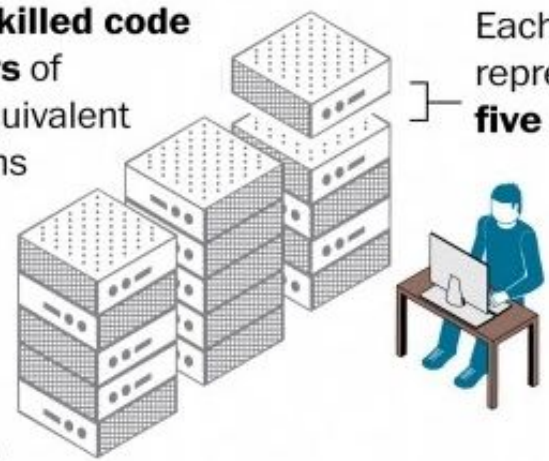

Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Target: https://www.udp.cl/
Status: Ready to scan
Issues found
[High] Offer SSLv3
[Medium] WEAK Cipher (SEED, IDEA, RC2, RC4)
[Information] 3DES Cipher (Medium)
[High] POODLE (SSLv3)
[Medium] Sweet32
[Low] LUCKY13
[Medium] BREACH
[Information] Supported Cipher Suites

FREAK

Factoring attack on RSA-EXPORT Keys
Similar a POODLE y afecta a máquinas Apple y Google.

512-bit encryption code

Researchers first broke a 512-bit key in 1999. Doing so today requires **a skilled code breaker** about **seven hours** of computing time from the equivalent of **75 computers,** said Johns Hopkins University cryptographer Matthew D. Green. That much computing power can be rented from a cloud provider for less than $100.



[CVE-2015-0204]

Logjam

Explota vulnerabilidad de DH.
Expertos creen que un ataque exitoso podría dejar al 18% del principal millón de dominios HTTPS en la web abiertos a la escucha e intercepción de información.

	Vulnerable if most common 1024-bit group is broken
HTTPS — Top 1 Million Domains	17.9%
HTTPS — Browser Trusted Sites	6.6%
SSH — IPv4 Address Space	25.7%
IKEv1 (IPsec VPNs) — IPv4 Address Space	66.1%

https://weakdh.org/

Irán bloquea el tráfico https

- El gobierno decidió censurar todos los SMS que contuviesen la palabra dólar en un extraño intento de frenar la devaluación de su moneda.
- Para “celebrar” la revolución iraní de 1979, el gobierno ha decidido bloquear todo el tráfico SSL de servicios que estén ubicados fuera del país.

https://elpais.com/tecnologia/2012/02/10/actualidad/1328873270_653423.html

Kill SSL3 & RC4 Junio 2015

RFC7568

http://disablessl3.com/

Symantec CA deprecation (2018)

Symantec™

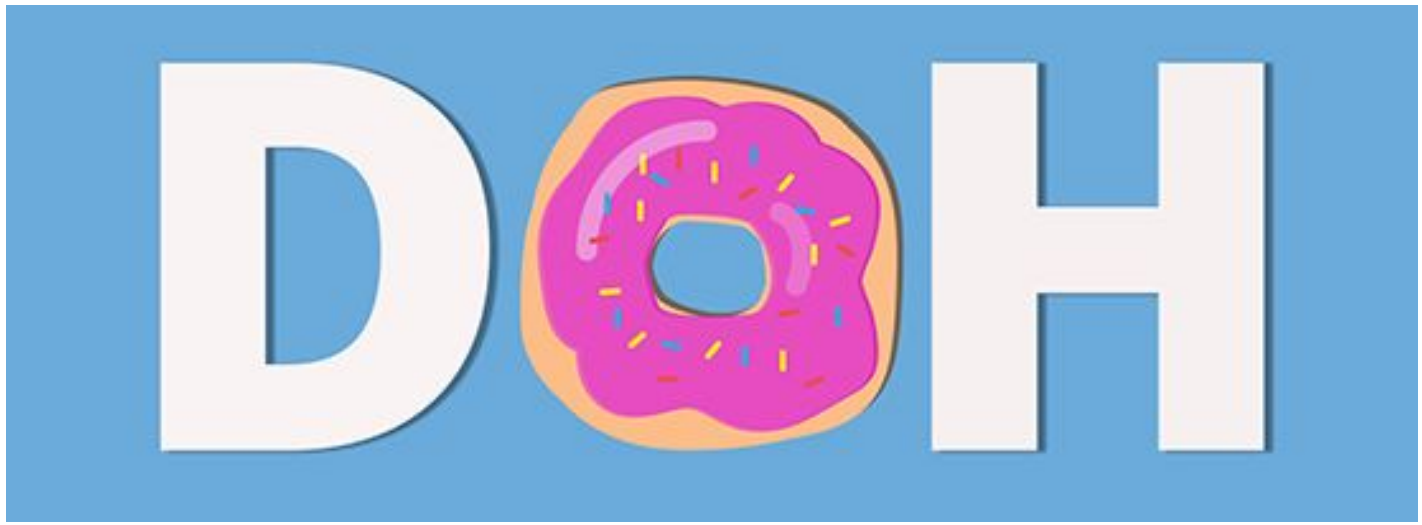
digicert®

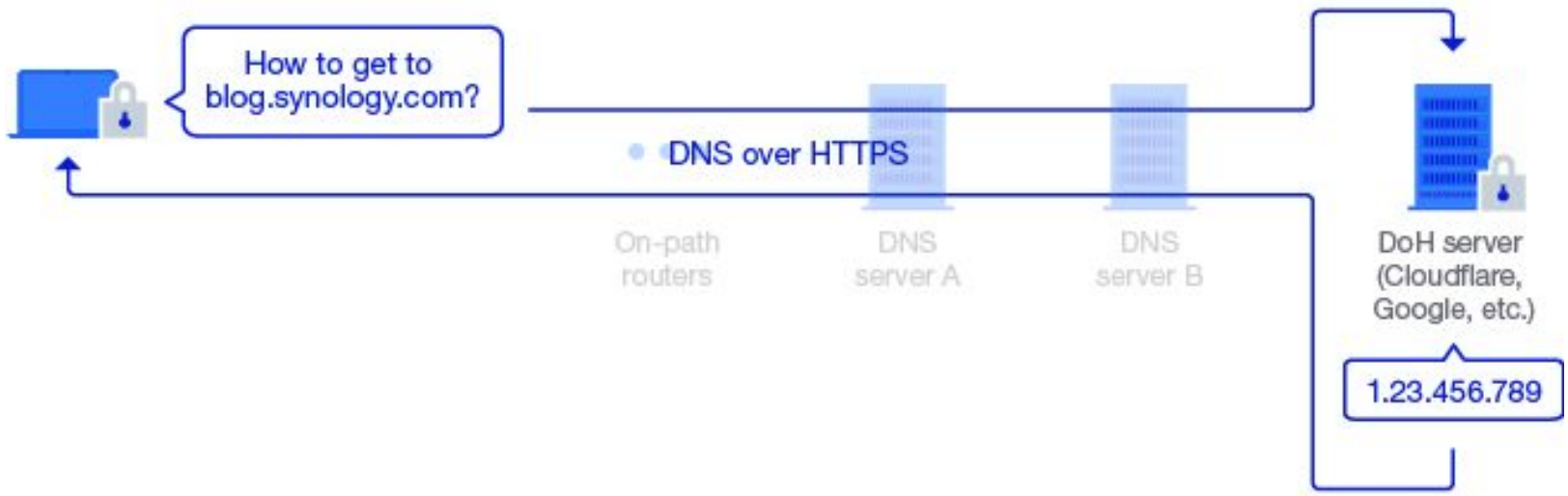
https://www.thesslstore.com/blog/final-distrust-symantec-ssl-certificates/

Burp addon to kill SSL

- SSLv2 and SSLv3 connectivity
- Heartbleed
- CCS Injection
- TLS_FALLBACK_SCSV support
- POODLE (SSLv3)
- Sweet32
- DROWN
- FREAK
- LUCKY13
- CRIME (TLS Compression)
- BEAST
- Check for weak ciphers
- BREACH
- Logjam

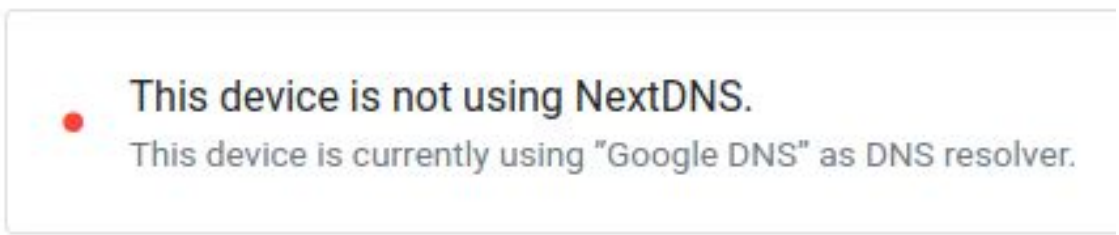
https://portswigger.net/bappstore/474b3c575a1a4584aa44dfefc70f269d


DOH



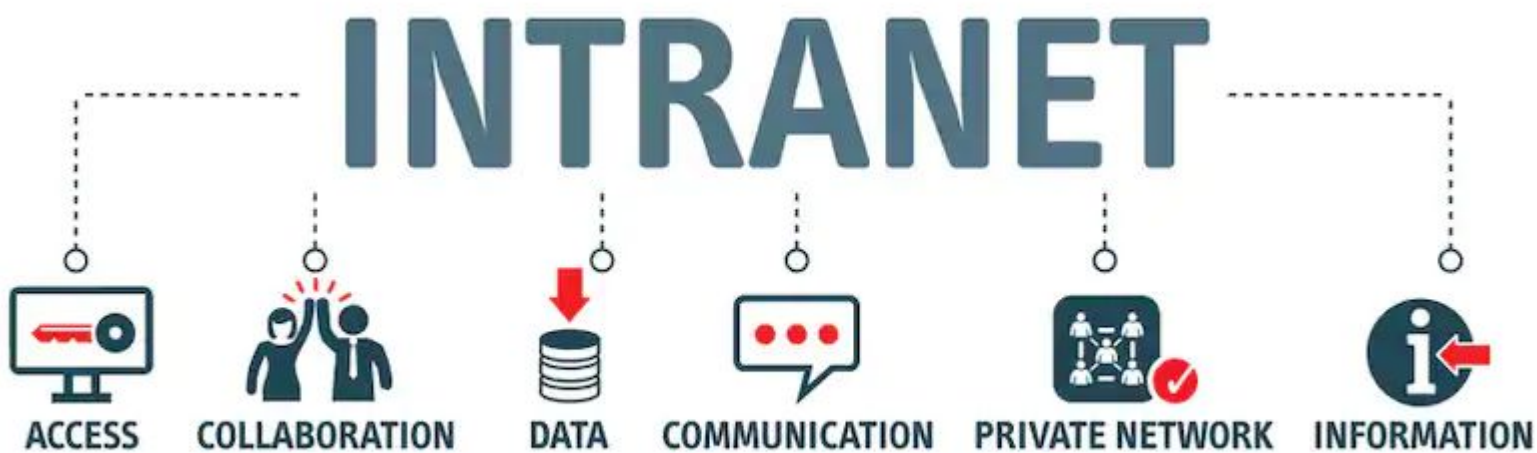
https://blog.apnic.net/2018/10/12/doh-dns-over-https-explained/

Firefox 72



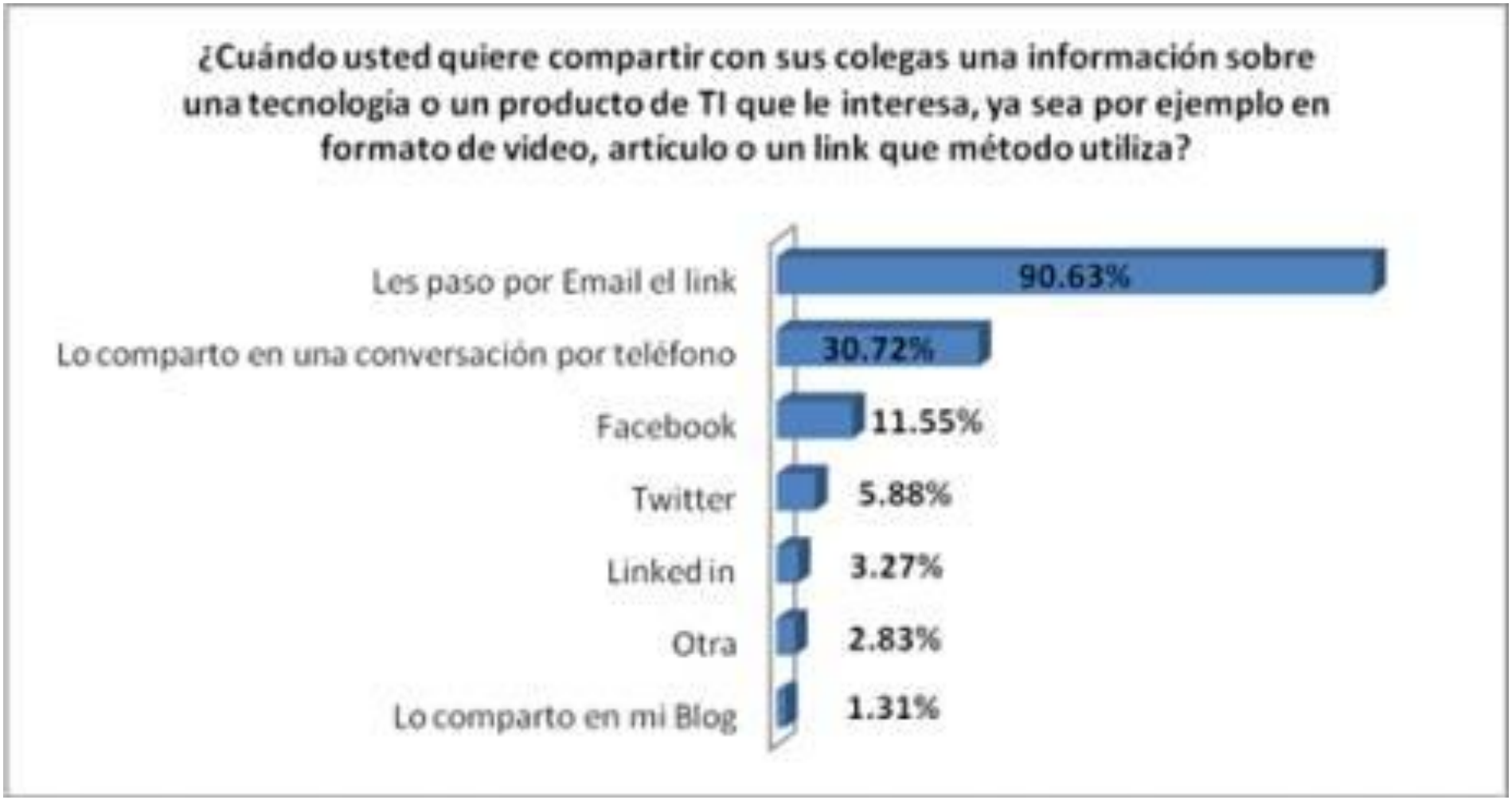
https://www.redeszone.net/tutoriales/seguridad/deshabilitar-dns-over-https-mozilla-firefox-red-local-dnsmasq/

Intranet udp



S/MIME

¿Se usará tanto el mail en TI?



Fuente: Latin America IT Investment Trends 2H10 - IDC Latin America, Noviembre 2010

S/MIME (Secure MIME o Secure Multipurpose Mail Extension)

- Es un proceso de seguridad utilizado para el intercambio de correo electrónico que hace posible garantizar la confidencialidad y el reconocimiento de autoría de los mensajes electrónicos.
- El S-MIME está basado en el estándar MIME, cuyo objetivo es permitir a los usuarios adjuntar a sus mensajes electrónicos archivos diferentes a los archivos de texto ASCII. Por lo tanto, el estándar MIME hace posible que podamos adjuntar todo tipo de archivos a nuestros correos electrónicos.

¿Cómo funciona S-MIME?

- El estándar S-MIME se basa en el principio de cifrado de clave pública.
- Cada una de las diversas secciones de un mensaje electrónico, codificado de acuerdo al estándar MIME, se cifra utilizando una clave de sesión.
- La clave de sesión se inserta en cada encabezado de la sección y se cifra utilizando la clave pública del destinatario.

FossaGuard_Pro: Encrypt Gmail with S/MIME

Offered by: Fossa Team

Fossa Guard enables end-to-end S/MIME encryption on top of Gmail® complementing it with industry standard privacy

Secure e-mailing with Gmail becomes easy on Desktop and Android. Encrypt and Sign your Gmail messages with industry standard - S/MIME using Chrome, Yandex or Firefox browsers.

Fossa Server and Fossa Guard web extension provide secure mailing solution on top of Gmail (TM) following S/MIME specification.

Fossa Guard generates key pair within your browser then Fossa Server securely supplies you with personal X.509 certificate upon Certificate Signing Request (CSR) so that your private key always stays with you.

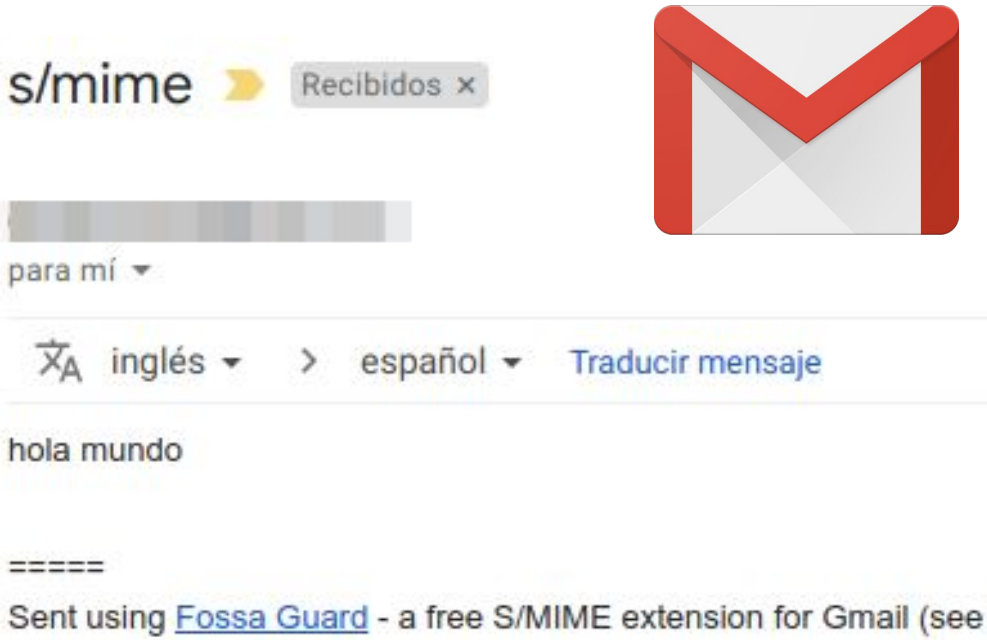
Use Fossa Guard extension to sign or to encrypt your email with X.509 certificate. The certificate is free and stays valid for 3 months (beta phase limitation).

	Fossa Guard
S/MIME certificate	Fossa only
Sign & Encrypt email	✔
Certificate Management	✔
S/MIME certificate registry	✔
Multiple private keys	
Send mail as	

Free Chrome version

Free Firefox version

S/MIME for Gmail



PKCS #7 MIME Files

Los archivos en formato P7M son responsables de almacenar mensajes de correo electrónico cifrados (o firmados digitalmente). En dicho archivo, se almacenan el contenido y el archivo adjunto.

Thunderbird®

https://superuser.com/questions/1489546/mozilla-thunderbird-not-opening-p7m-attachment-of-encrypted-emails

RFC 5581

Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification. Abril 2019

https://tools.ietf.org/html/rfc8551

Cómo se implementa?

¿Cómo se implementa SSL?


```
<VirtualHost *:443>
    ServerName www.example.com
    ServerAlias example

    SSLEngine on
    SSLCertificateFile    /etc/apache2/ssl.crt/server.crt
    SSLCertificateKeyFile /etc/apache2/ssl.crt/server.key
```

http://httpd.apache.org/docs/2.0/mod/mod_ssl.html

SSL Configuration Generator

https://ssl-config.mozilla.org/

Let’s Encrypt

https://letsencrypt.org/

Un problema con los certificados TLS/SSL de Let's Encrypt implica revocar 3 de los 116 millones que están en uso.

https://www.microsiervos.com/archivo/seguridad/problema-certificados-tls-ssl-lets-encrypt-revocar.html

https://certbot.eff.org/lets-encrypt/ubuntubionic-apache


GET INSPIRED
BY THESE
EXAMPLES!

This Connection is Untrusted

You have asked Firefox to connect securely to **www.participemos.gob.cl**, but we can't confirm that your connection is secure.

Technical Details

www.participemos.gob.cl uses an invalid security certificate.

The certificate is not trusted because no issuer chain was provided.
The certificate is only valid for intranet.msgg.gov.cl
The certificate expired on 02/02/2011 08:59 PM. The current time is 10/06/2011 03:18 PM.

https://www.participemos.gob.cl/

www.participemos.gov.cl | 443 | CHECK SSL

(ex: www.ibm.com) port (443 is HTTPS default)

SSL Server Certificate

Common Name: intranet.msgg.gov.cl
Issuing CA: VeriSign Trust Network
Organization: Ministerio Secretaria General de Gobierno
Valid from February 02, 2010 to February 02, 2011
Key Size: 1024 bits

GEOCERTS SSL™
SSL Made Simple

Certificate Expiraton

This certificate has expired.

Certificate Common Name (CN) and Hostname Match?

The hostname (www.participemos.gov.cl) does NOT match the Common Name in the certificate (intranet.msgg.gov.cl). This certificate is currently invalid for this host.

DNS, etc.

www.participemos.gov.cl resolves to 163.247.56.106.
Server type: Apache

Certificate Chain Complete?

A valid Root CA Certificate could not be located, the certificate will likely display browser warnings.

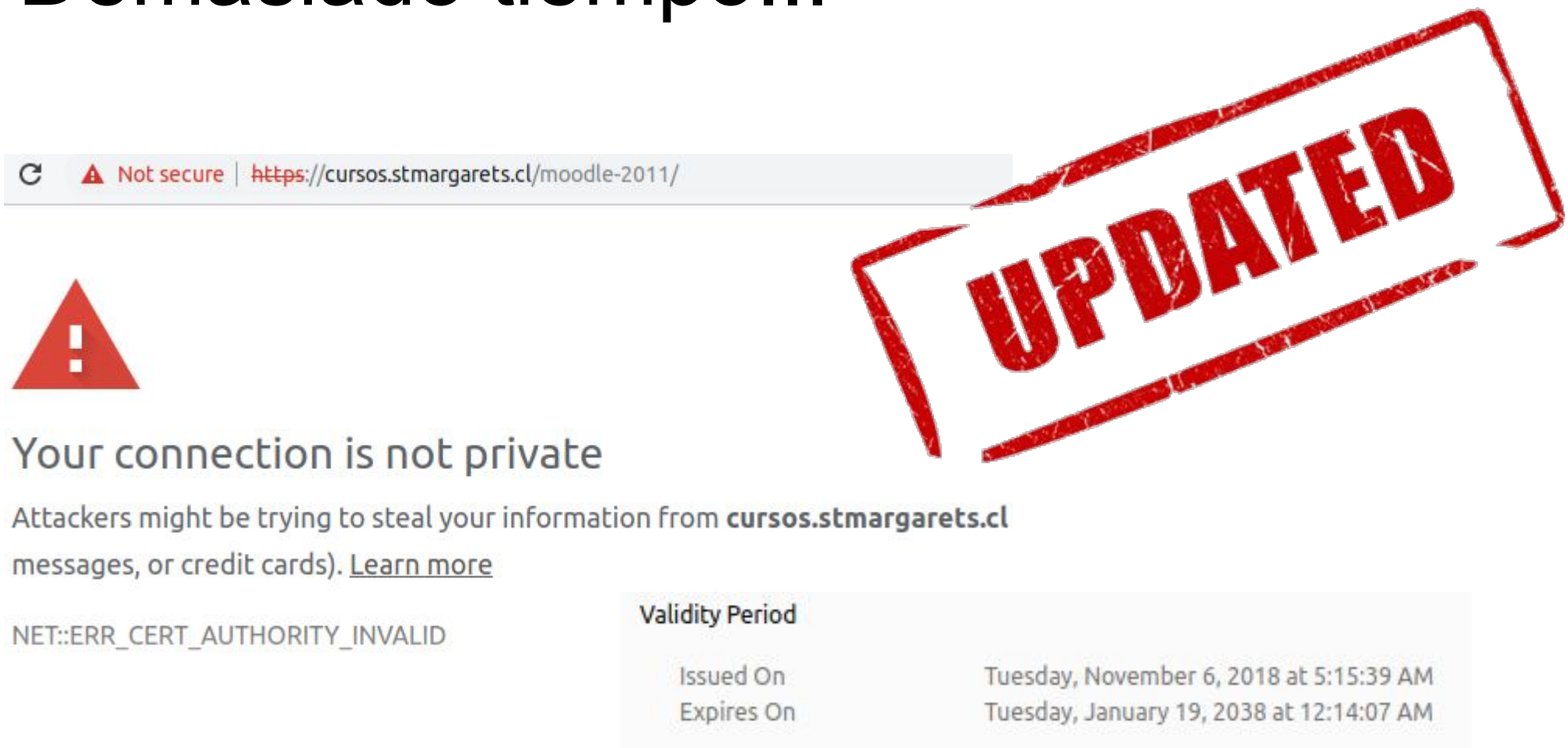
http://www.geocerts.com/ssl_checker


Not secure | https://www.participemos.gob.cl
Testing 123..
operation of the Apache HTTP server
read this page it means that this site
erver is powered by CentOS.
Certificate Viewer: localhost.localdomain
General
Details
This certificate has been verified for the following usages:
Issued To
Common Name (CN) localhost.localdomain
Organization (O) SomeOrganization
Organizational Unit (OU) SomeOrganizationalUnit
Issued By
Common Name (CN) localhost.localdomain
Organization (O) SomeOrganization
Organizational Unit (OU) SomeOrganizationalUnit
Validity Period
Issued On Tuesday, November 6, 2018 at 1:30:26 PM
Expires On Wednesday, November 6, 2019 at 1:30:26 PM

Poco tiempo...

https://cursos.stmargarets.cl/moodle-2011/

Demasiado tiempo...

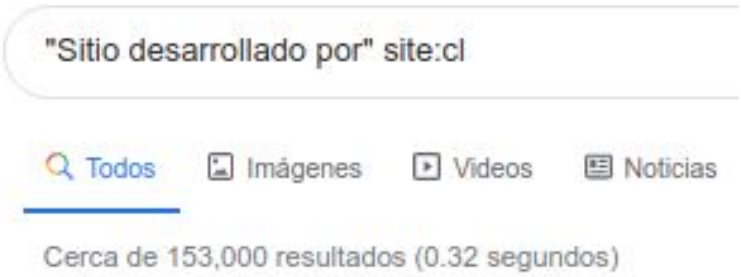


Sitio 100% Chilenos

Lista de nuevos dominios .cl

https://www.nic.cl/registry/Ultimos.do?t=1m

Desarrolladores web en Chile



Outdated List 2012-1

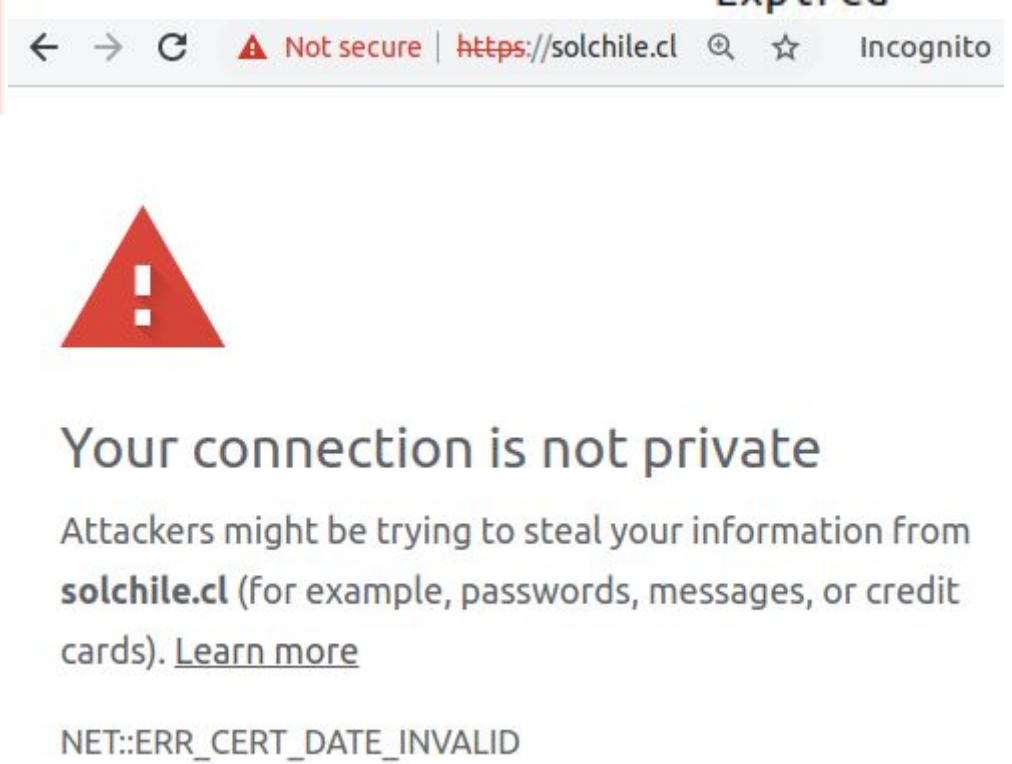
lan.com:443:Expired
vtr.cl:443:Expired
vtr.com:443:Expired
cam4.com:443:Expired
redgol.cl:443:Expired
reclamos.cl:443:Expired
zmart.cl:443:Expired
zancada.com:443:Expired
puntovital.cl:443:Expired
integramedica.cl:443:Expired
acciontrabajo.cl:443:Expired
laguiachile.cl:443:Expired
dailymail.co.uk:443:Expired

ssl -check

Host	Status	Expires	Days
www.lan.com:443	Valid	Jan 11 2020	87
www.vtr.cl:443	Valid	Dec 12 2019	57
www.vtr.com:443	Valid	Dec 12 2019	57
cam4.com:443	Valid	Oct 10 2021	725
redgol.cl:443	Valid	Jan 24 2020	100
reclamos.cl:443	Valid	Jul 31 2020	289
zmart.cl:443	Valid	Jan 10 2020	86
zancada.com:443	Valid	Aug 23 2020	312
puntovital.cl:443	Valid	Feb 24 2020	131
integramedica.cl:443	Valid	Apr 12 2020	179
acciontrabajo.cl:443	Valid	Apr 11 2020	178
laguiachile.cl:443	Valid	Jan 7 2020	83
dailymail.co.uk:443	Valid	Dec 29 2019	74

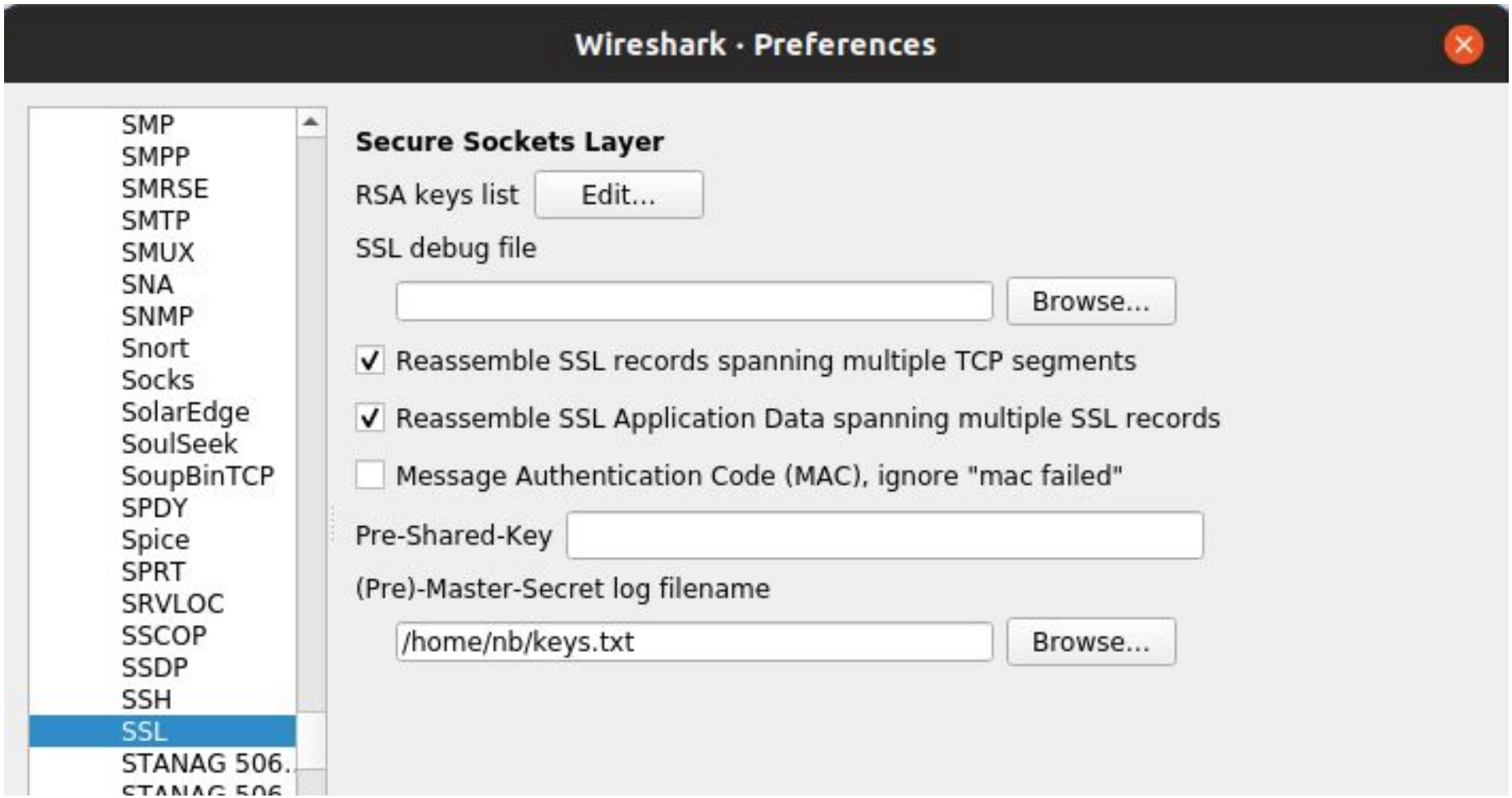
Outdated List 2019-2

```
ssl-cert-check -f tarea1s

Host                                                Status       Expires      Days
--------------------------------------------------- ------------ ------------ ----
solchile.cl:443                                     Expired      May 17 2019  -152
globalelectronica.cl:443                            Expired      May 28 2015  -1602
diarioeldia.cl:443                                  Expired      Apr 28 2019  -171
solchile.cl:443                                     Expired      May 17 2019  -152
casamarilla.cl:443                                  Expired      Aug 22 2019  -55
easy.cl:443                                         Expired      Oct 9 2019   -7
```

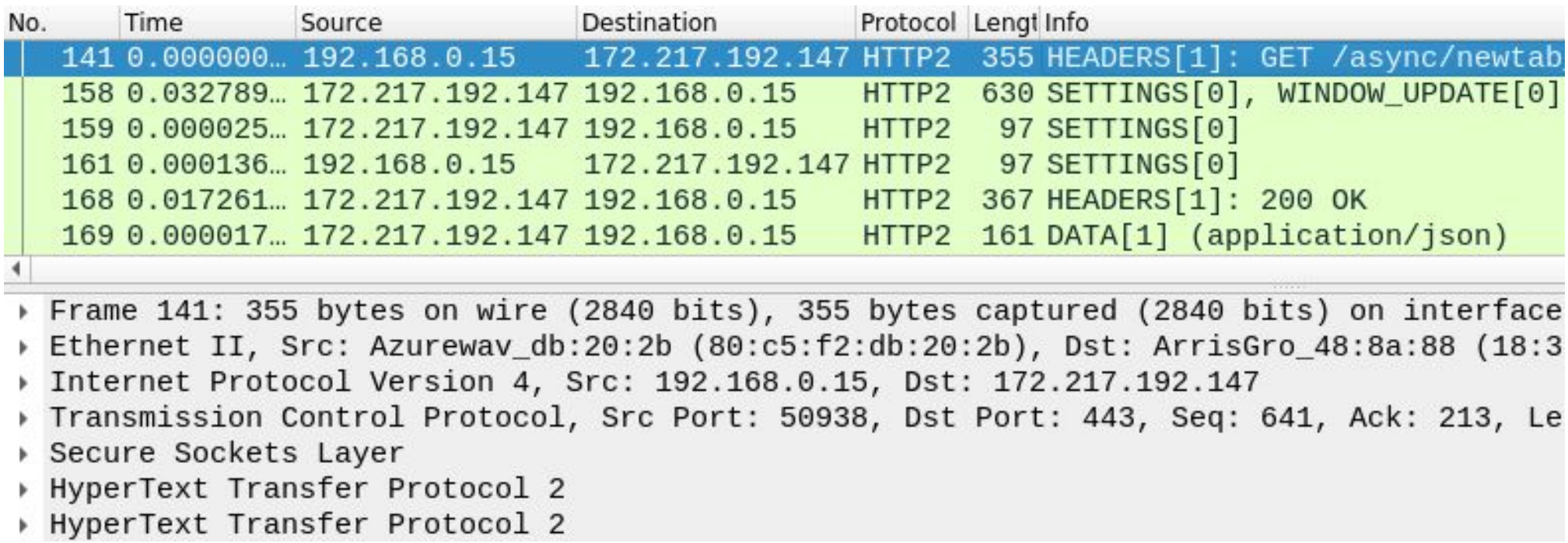


Decrypt SSL w/Wireshark

SSLKEYLOGFILE="$PWD/keys.txt" google-chrome --user-data-dir=/tmp/cr



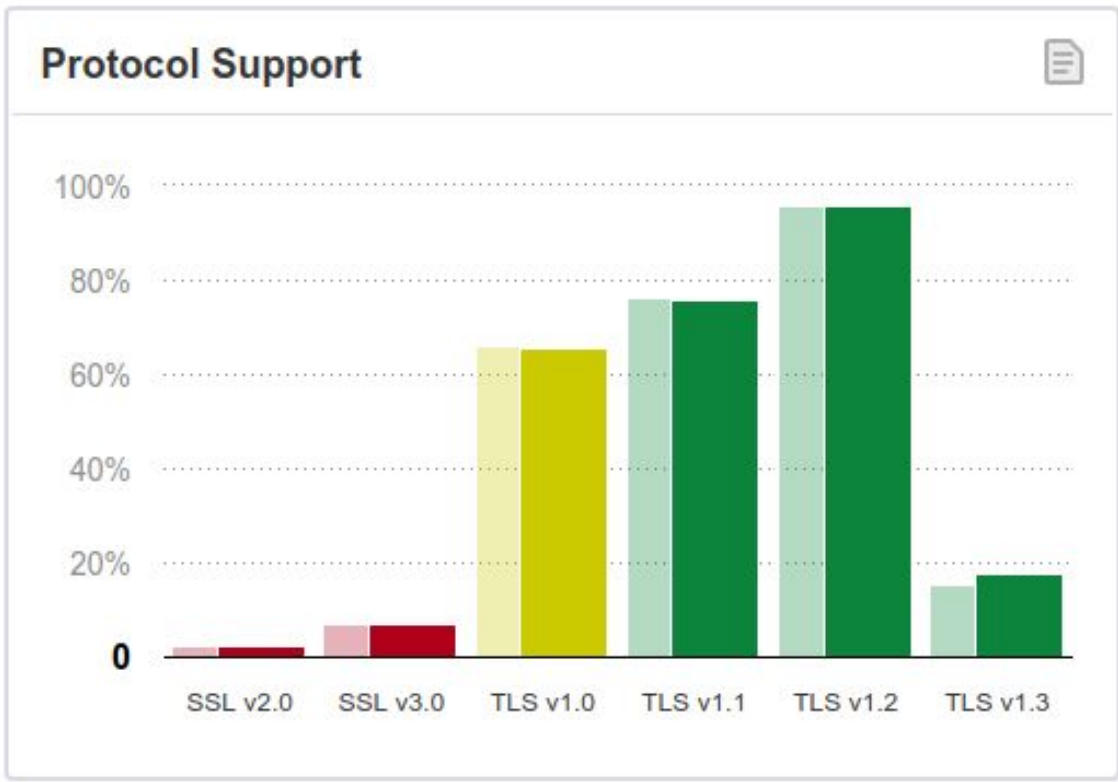
HTTP2 Protocol decoded

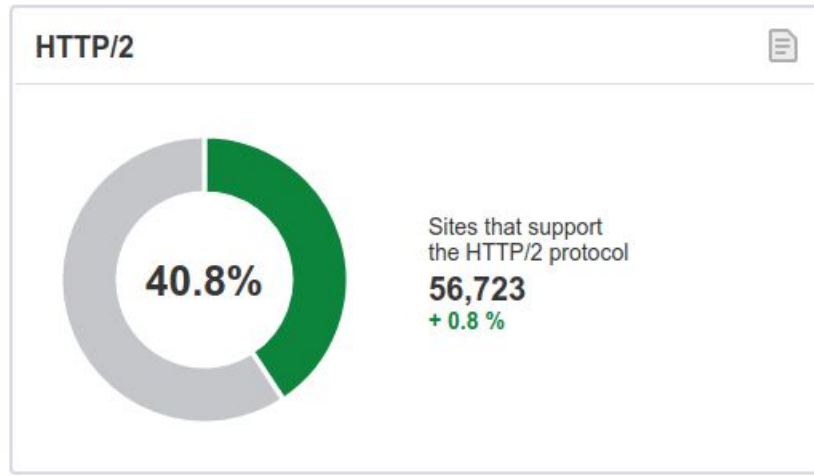


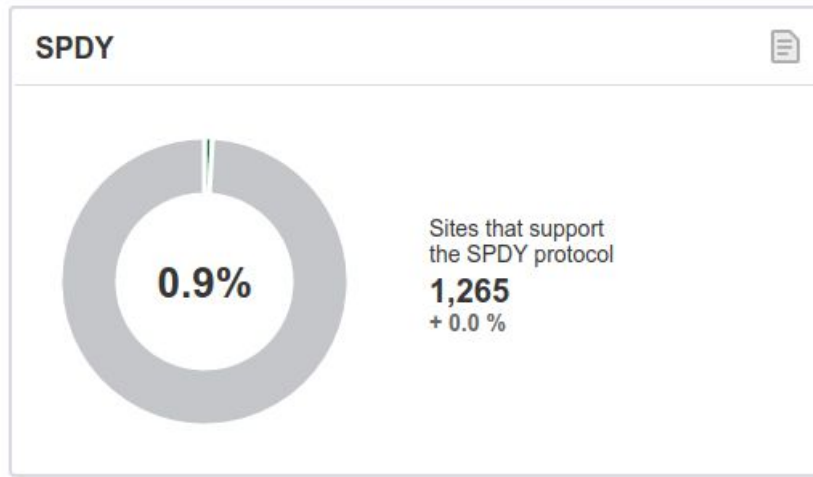
No.	Time	Source	Destination	Protocol	Lengt	Info
141	0.000000…	192.168.0.15	172.217.192.147	HTTP2	355	HEADERS[1]: GET /async/newtab
158	0.032789…	172.217.192.147	192.168.0.15	HTTP2	630	SETTINGS[0], WINDOW_UPDATE[0]
159	0.000025…	172.217.192.147	192.168.0.15	HTTP2	97	SETTINGS[0]
161	0.000136…	192.168.0.15	172.217.192.147	HTTP2	97	SETTINGS[0]
168	0.017261…	172.217.192.147	192.168.0.15	HTTP2	367	HEADERS[1]: 200 OK
169	0.000017…	172.217.192.147	192.168.0.15	HTTP2	161	DATA[1] (application/json)

```
▸ Frame 141: 355 bytes on wire (2840 bits), 355 bytes captured (2840 bits) on interface
▸ Ethernet II, Src: Azurewav_db:20:2b (80:c5:f2:db:20:2b), Dst: ArrisGro_48:8a:88 (18:3
▸ Internet Protocol Version 4, Src: 192.168.0.15, Dst: 172.217.192.147
▸ Transmission Control Protocol, Src Port: 50938, Dst Port: 443, Seq: 641, Ack: 213, Le
▸ Secure Sockets Layer
▸ HyperText Transfer Protocol 2
▸ HyperText Transfer Protocol 2
```

SSL Pulse







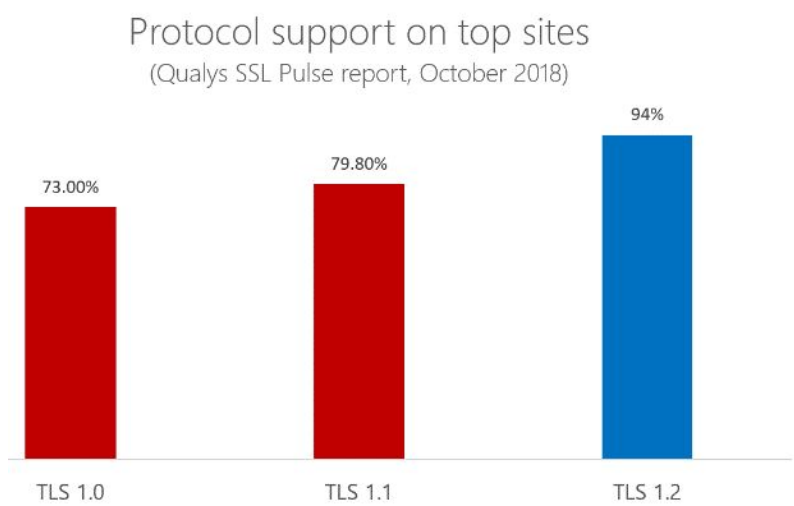
https://www.ssllabs.com/ssl-pulse/

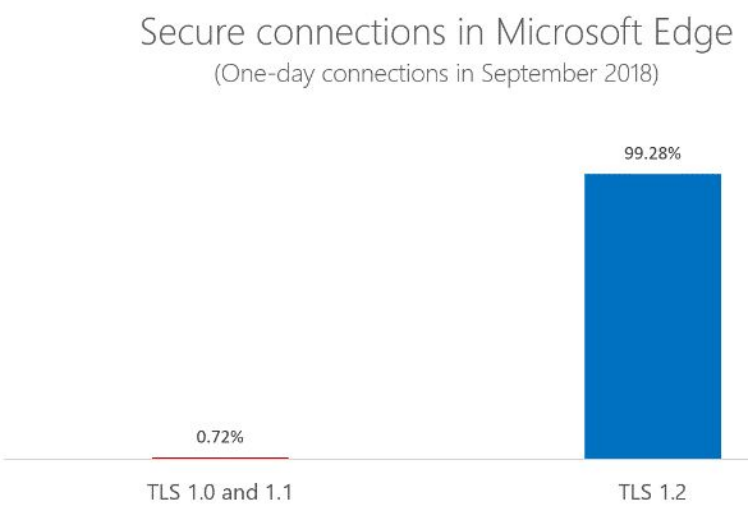
¿Qué trae el futuro?

TLS 1.3, DTLS 1.3, mejoras en el performance del tráfico

Los navegadores deshabilitarán versiones inseguras de TLS en 2020

Como consecuencia de este anuncio, TLS 1.0 y 1.1 se deshabilitarán en Chrome 81, mientras que Firefox lo hará a lo largo del mes de marzo de 2020, lo mismo que Safari.





https://blog.segu-info.com.ar/2018/10/los-navegadores-deshabilitaran.html

Deprecating TLSv1.0 and TLSv1.1

https://datatracker.ietf.org/doc/draft-ietf-tls-oldversions-deprecate/

TLS 1.0 ha muerto

https://blog.segu-info.com.ar/2020/02/ultimo-aviso-tls-v10-esta-muerto.html

Slack

El 19 de febrero de 2020, Slack dejará de admitir las versiones 1.0 y 1.1 del protocolo de seguridad de la capa de transporte.

https://api.slack.com/changelog/2019-07-deprecate-early-tls-versions

Deprecating MD5 and SHA-1 in TLSv1.2

https://datatracker.ietf.org/doc/draft-ietf-tls-md5-sha1-deprecate/

NIST Special Publication 800-57

- Through 2010 (minimum of 80 bits of strength)
  - FFC (e.g., DSA, D-H) Minimum: L=1024; N=160
  - IFC (e.g., RSA) Minimum: k=1024
  - ECC (e.g. ECDSA) Minimum: f=160
- Through 2030 (minimum of 112 bits of strength)
  - FFC (e.g., DSA, D-H) Minimum: L=2048; N=224
  - IFC (e.g., RSA) Minimum: k=2048
  - ECC (e.g. ECDSA) Minimum: f=224
- Beyond 2030 (minimum of 128 bits of strength)
  - FFC (e.g., DSA, D-H) Minimum: L=3072; N=256
  - IFC (e.g., RSA) Minimum: k=3072
  - ECC (e.g. ECDSA) Minimum: f=256

Recomendaciones NIST

Algorithm	Usage
RSA 3072-bit or larger	Key Establishment, Digital Signature
Diffie-Hellman (DH) 3072-bit or larger	Key Establishment
ECDH with NIST P-384	Key Establishment
ECDSA with NIST P-384	Digital Signature
SHA-384	Integrity
AES-256	Confidentiality

https://cryptome.org/2016/01/CNSA-Suite-and-Quantum-Computing-FAQ.pdf

All with TLS

Google Chrome comenzará a bloquear todo el contenido que no esté cifrado con TLS, comenzando con Chrome 79 (Diciembre 2019).

https://www.genbeta.com/navegadores/google-chrome-comenzara-a-bloquear-carga-todas-imagenes-videos-audio-que-no-usen-https

Support for TLS 1.3

Various Implementation Support for TLS 1.3

Implementation	TLS 1.0 RFC 2246	TLS 1.1 RFC 4346	TLS 1.2 RFC 5246	TLS 1.3 RFC 8446
wolfSSL	Yes	Yes	Yes	Yes
BoringSSL	Yes	Yes	Yes	Up to draft 23
GnuTLS	Yes	Yes	Yes	Up to draft 26
MatrixSSL	Yes	Yes	Yes	No
OpenSSL	Yes	Yes	Yes	Yes
rustls	No	No	Yes	Up to draft 22

https://www.wolfssl.com/docs/tls13/

TLS 1.3

Lanzada la versión final en Agosto de 2018 por la RFC8446
Remueve características obsoletas de TLS 1.2 tales como:

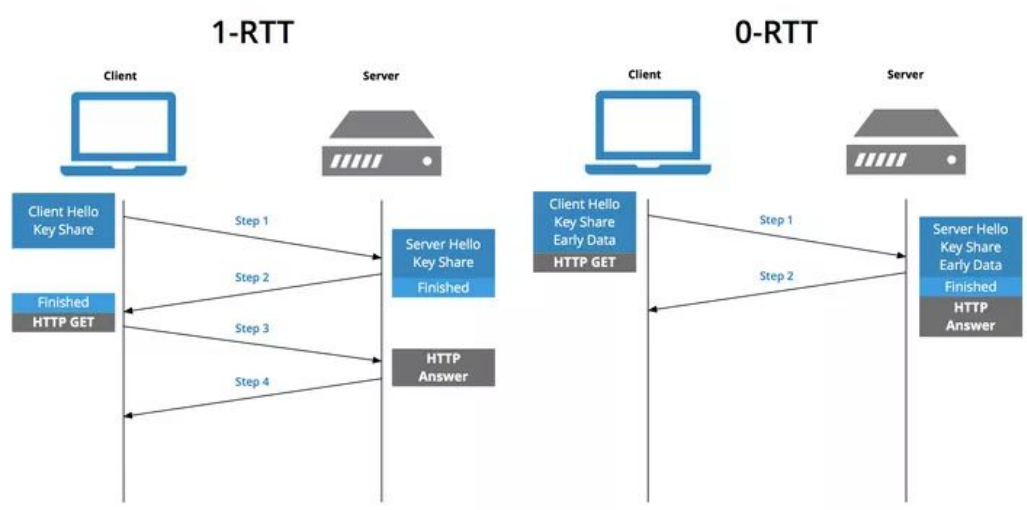
- SHA-1
- RC4
- DES
- 3DES
- AES-CBC
- MD5
- Grupos Diffie-Hellman arbitrarios – CVE-2016-0701
- EXPORT- claves de fuerza – Responsable de FREAK y LogJam

https://tools.ietf.org/html/draft-ietf-tls-tls13-28

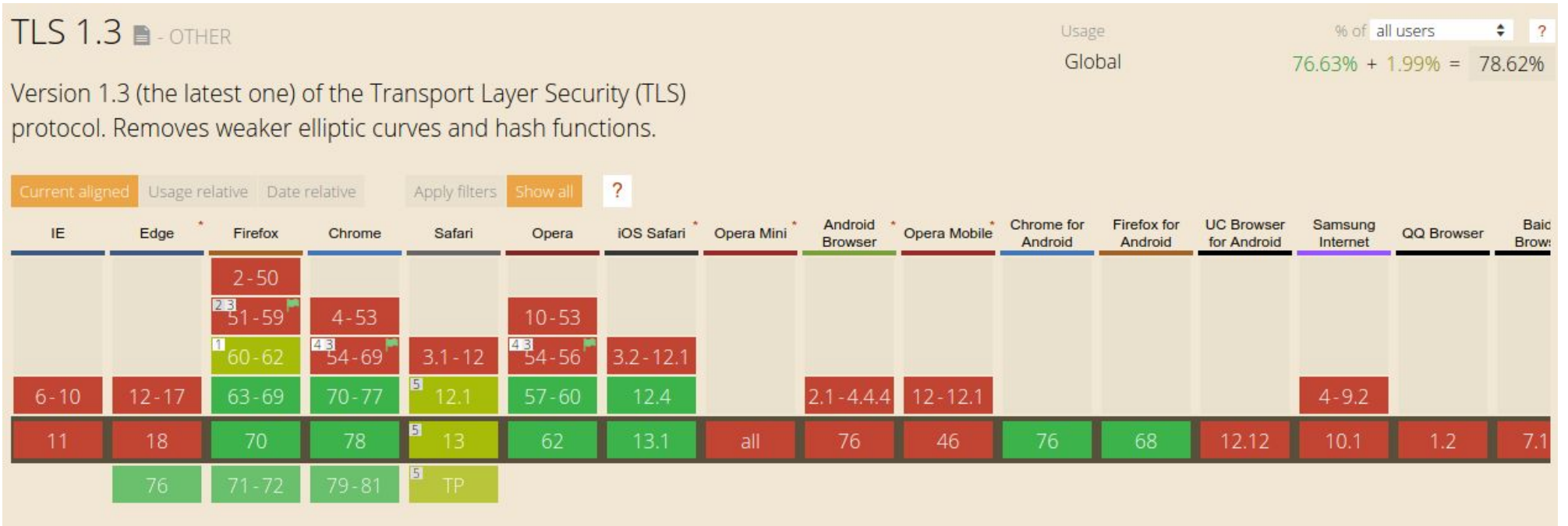
TLS Handshake differences

TLS 1.3 0-RTT

La reanudación de sesión de TLS 1.2 mediante tickets o identificadores de sesión está deprecada en TLS 1.3. Ambos métodos se sustituyen por una clave precompartida (PSK). Cuando se requiere reanudar la sesión con TLS 1.3, se ahorra un RTT.

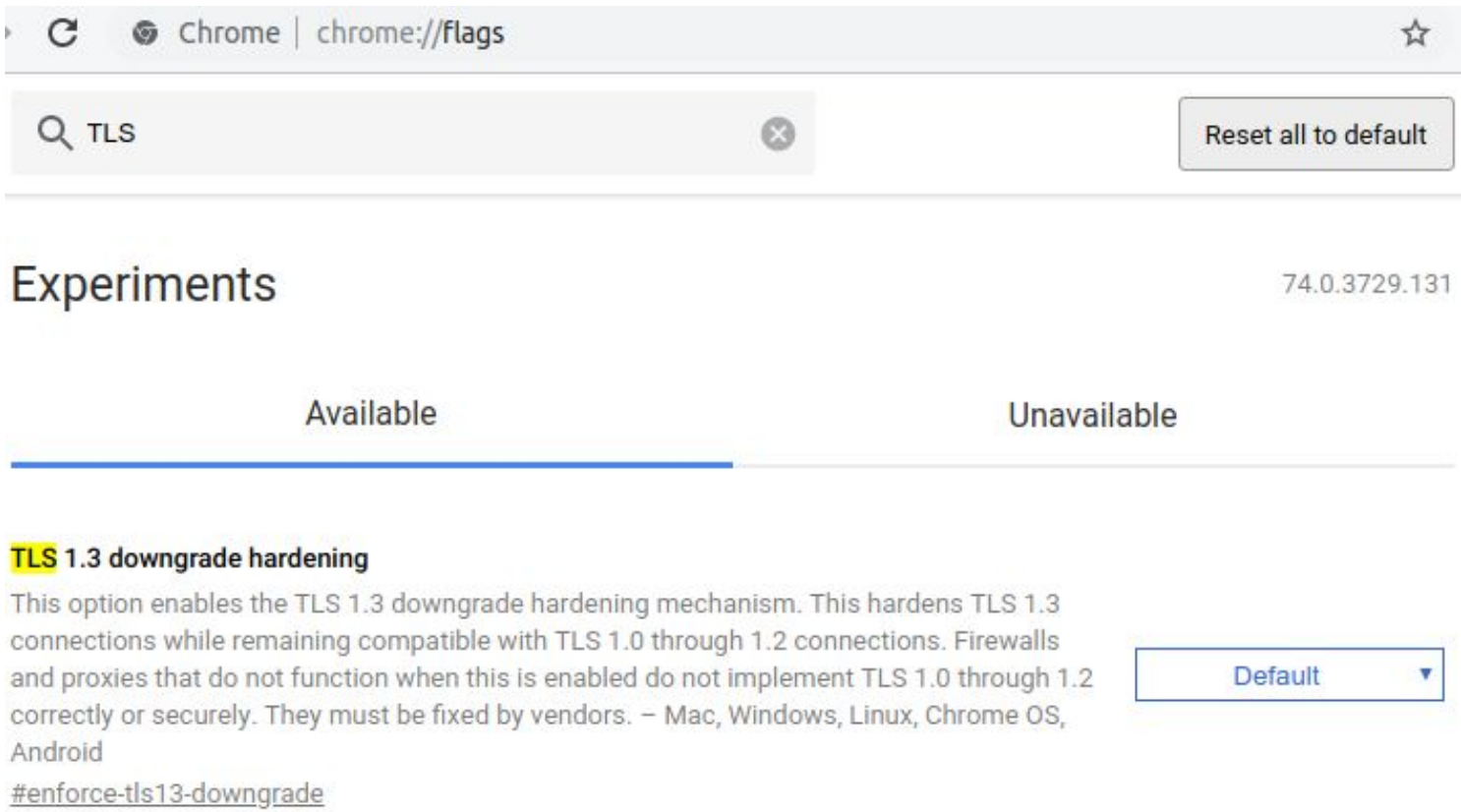


Browser compatibility



https://caniuse.com/#feat=tls1-3

Downgrade hardening



The GnuTLS Transport Layer Security Library

GnuTLS is a secure communications library implementing the SSL, TLS and DTLS protocols and technologies around them. It provides a simple C language application programming interface (API) to access the secure communications protocols as well as APIs to parse and write X.509, PKCS #12, and other required structures.

https://gnutls.org/

DTLS 1.3

Versión TLS 1.3 implementada en datagramas, cuya versión release podría estar lista para Abril de 2020.

Library support for DTLS

Implementation	DTLS 1.0[1]	DTLS 1.2[2]
Botan	Yes	Yes
GnuTLS	Yes	Yes
Java Secure Socket Extension	Yes	Yes
LibreSSL	Yes	No
libsystools[6]	Yes	No
MatrixSSL	Yes	Yes
mbed TLS (previously PolarSSL)	Yes[7]	Yes[7]
Network Security Services	Yes[8]	Yes[9]
OpenSSL	Yes	Yes[10]
PyDTLS[11][12]	Yes	Yes
Python3-dtls[13][14]	Yes	Yes
SChannel 7/2008R2, 8/2012, 8.1/2012R2, 10	Yes[15]	No[15]
SChannel 10 (1607), 2016	Yes	Yes[16]
Secure Transport OS X 10.8–10.10 / iOS 5–8	Yes[17]	No
tinydtls [18]	No	Yes
Waher.Security.DTLS [19]	No	Yes
wolfSSL (previously CyaSSL)	Yes	Yes
@nodertc/dtls [20][21]	No	Yes
java-dtls[22]	Yes	Yes
pion/dtls[23] (Go)	No	Yes
Implementation	**DTLS 1.0**	**DTLS 1.2**

https://tools.ietf.org/html/draft-ietf-tls-dtls13-33

Performance

- HTTP/2
- Brotli Compression
- HPACK Compression
- OCSP Stapling
- Use a CDN

https://wp-rocket.me/blog/https-affects-website-performance/

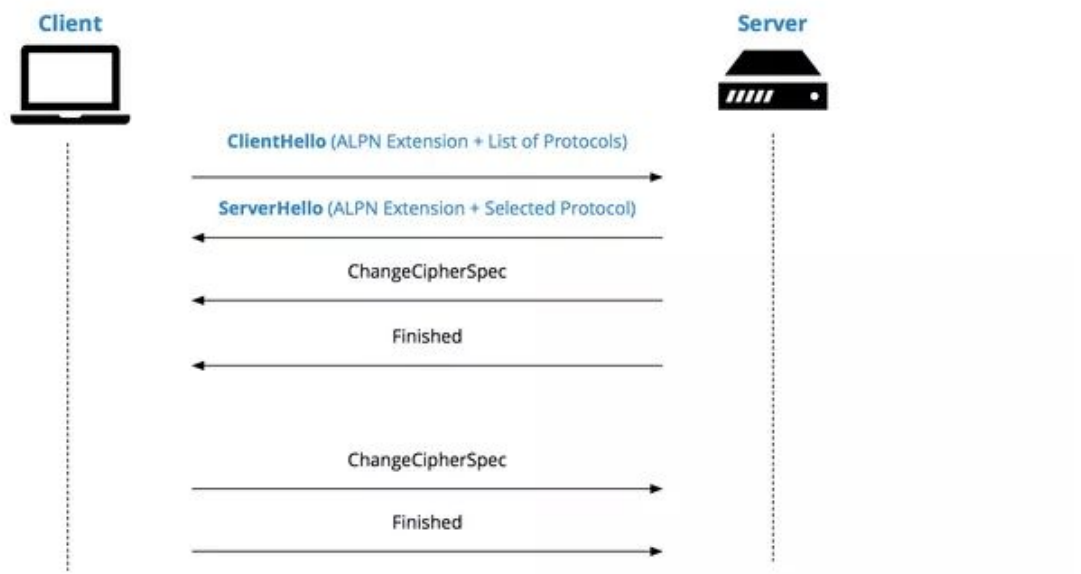
Beneficios HTTP2 sobre HTTP1.1

- Multiplexed streams
- Server push
- HEADERS compression
- Binary format

https://medium.com/@factoryhr/http-2-the-difference-between-http-1-1-benefits-and-how-to-use-it-38094fa0e95b

Application-Layer Protocol Negotiation ALPN

Según la RFC 7301, con ALPN el cliente enviará una lista de protocolos de aplicación soportados al servidor como parte del mensaje TLS ClientHello (HTTP 1.1, HTTP 2.0, etc). La lista de protocolos de soporte se envía al servidor en el primer mensaje, minimizando así la cantidad de RTT necesarios.



HTTP/2 Test

VERIFY HTTP/2 SUPPORT

www.google.com

HTTP/2 protocol is supported.

ALPN extension is supported.

https://tools.keycdn.com/http2-test

HTTP/3

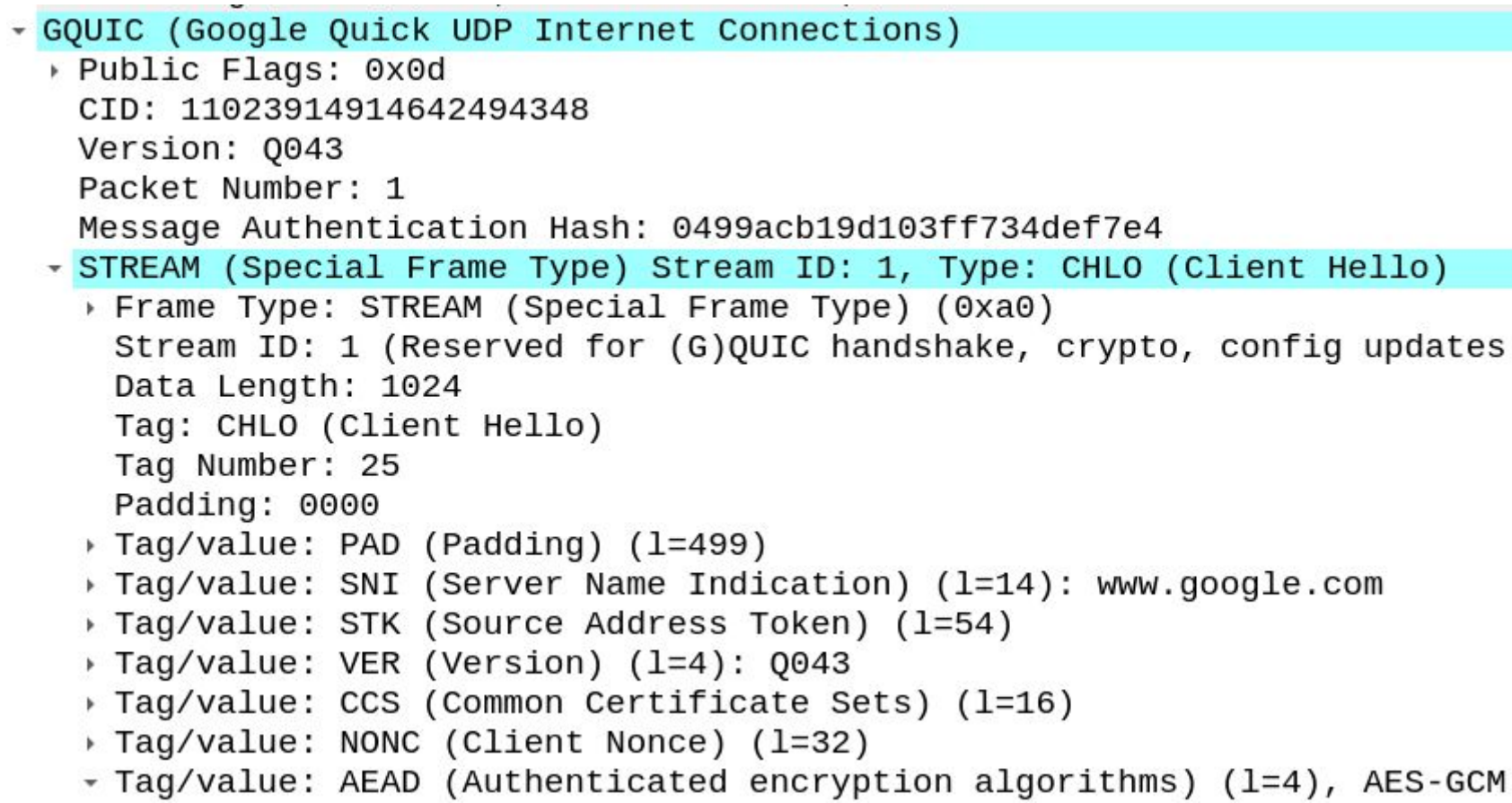
Al igual que DTLS 1.3, HTTP/3 aún está por definirse la versión release, que podría ser en Marzo de 2020.
Es la evolución de QUIC, protocolo desarrollado por Google (HTTP2 sobre UDP)

https://www.thewebmaster.com/hosting/2015/dec/14/what-is-http2-and-how-does-it-compare-to-http1-1/

GQUIC

192.168.1.127	172.20.85.12	DNS	85	Standard query 0x6920 A www.google.com OPT
172.20.85.12	192.168.1.127	DNS	181	Standard query response 0x6920 A www.google.com
192.168.1.127	172.217.192.106	GQUIC	1392	Client Hello, PKN: 1, CID: 11023914914642494348
172.217.192.106	192.168.1.127	GQUIC	1392	Payload (Encrypted), PKN: 1
192.168.1.127	172.217.192.106	GQUIC	81	Payload (Encrypted), PKN: 2, CID: 1102391491464
192.168.1.127	172.217.192.106	GQUIC	70	Payload (Encrypted), PKN: 3, CID: 1102391491464
172.217.192.106	192.168.1.127	GQUIC	62	Payload (Encrypted), PKN: 2
192.168.1.127	172.217.192.106	GQUIC	1392	Client Hello, PKN: 1, CID: 40361719635540774 96
192.168.1.127	172.217.192.106	GQUIC	529	Payload (Encrypted), PKN: 2, CID: 403617196355 4
172.217.192.106	192.168.1.127	GQUIC	1392	Payload (Encrypted), PKN: 1
172.217.192.106	192.168.1.127	GQUIC	62	Payload (Encrypted), PKN: 2
192.168.1.127	172.217.192.106	GQUIC	83	Payload (Encrypted), PKN: 3, CID: 403617196355 4
192.168.1.127	172.217.192.106	GQUIC	70	Payload (Encrypted), PKN: 4, CID: 403617196355 4
172.217.192.106	192.168.1.127	GQUIC	1043	Payload (Encrypted), PKN: 3
172.217.192.106	192.168.1.127	GQUIC	60	Payload (Encrypted), PKN: 4
192.168.1.127	172.217.192.106	GQUIC	70	Payload (Encrypted), PKN: 5, CID: 403617196355 4
192.168.1.127	172.217.192.106	GQUIC	970	Payload (Encrypted), PKN: 4, CID: 1102391491464
172.217.192.106	192.168.1.127	GQUIC	582	Payload (Encrypted), PKN: 3
172.217.192.106	192.168.1.127	GQUIC	122	Payload (Encrypted), PKN: 4
192.168.1.127	172.217.192.106	GQUIC	70	Payload (Encrypted), PKN: 5, CID: 1102391491464
192.168.1.127	172.217.192.106	GQUIC	193	Payload (Encrypted), PKN: 6, CID: 1102391491464
172.217.192.106	192.168.1.127	GQUIC	244	Payload (Encrypted), PKN: 5
172.217.192.106	192.168.1.127	GQUIC	273	Payload (Encrypted), PKN: 6

GQUIC Detail



Compression

Brotli es un algoritmo de compresión de código abierto sin pérdidas desarrollado por Google como una alternativa a Gzip, Zopfli y Deflate que reduce el consumo de ancho de banda y ayuda a cargar el contenido más rápidamente alcanzando un 20-26% más de compresión que Zopfli con menos uso de CPU.

https://opensource.googleblog.com/2015/09/introducing-brotli-new-compression.html

Perfect Forward Secrecy

Se trata de un sistema de seguridad basado en la utilización de distintas claves privadas para encriptar cada conexión de los usuarios a sus servicios. De esta forma, cada conexión tiene una clave, que se borra cada cierto tiempo.

http://www.cs.bu.edu/~itkis/pap/forward-secure-survey.pdf

	Session identifiers	Session tickets	OCSP stapling	Dynamic record sizing	ALPN	Forward secrecy	HTTP/2	TLS 1.3	TLS 1.3 0-RTT
Apache	yes	yes	yes	yes	yes	yes	yes	yes	no
ATS	yes	yes	yes	dynamic	yes	yes	yes	yes	no
Caddy	yes	yes	yes	yes	yes	yes	yes	yes	no
F5 BIG-IP	yes	yes	yes	yes	yes	yes	yes	yes	no
H2O	yes	yes	yes	dynamic	yes	yes	yes	yes	yes
HAProxy	yes	yes	yes	dynamic	yes	yes	yes	yes	yes
Hitch	yes	yes	yes	no	yes	yes	yes	yes	no
IIS	yes	yes	yes	no	yes	yes	yes	no	no
Citrix ADC	yes	yes	yes	no	yes	yes	yes	yes	no
NGINX	yes	yes	yes	static (16k)	yes	yes	yes	yes	yes
node.js	yes	yes	optional	optional	yes	yes	yes	yes	no
Go	yes	yes	optional	yes	yes	yes	yes	yes	no
nghttpx	yes	yes	yes	dynamic	yes	yes	yes	yes	yes

How HTTPS works ...in a comic! 🌈 🎉 🍕

Dissecting an SSL certificate

https://jvns.ca/blog/2017/01/31/whats-tls/


Fin.