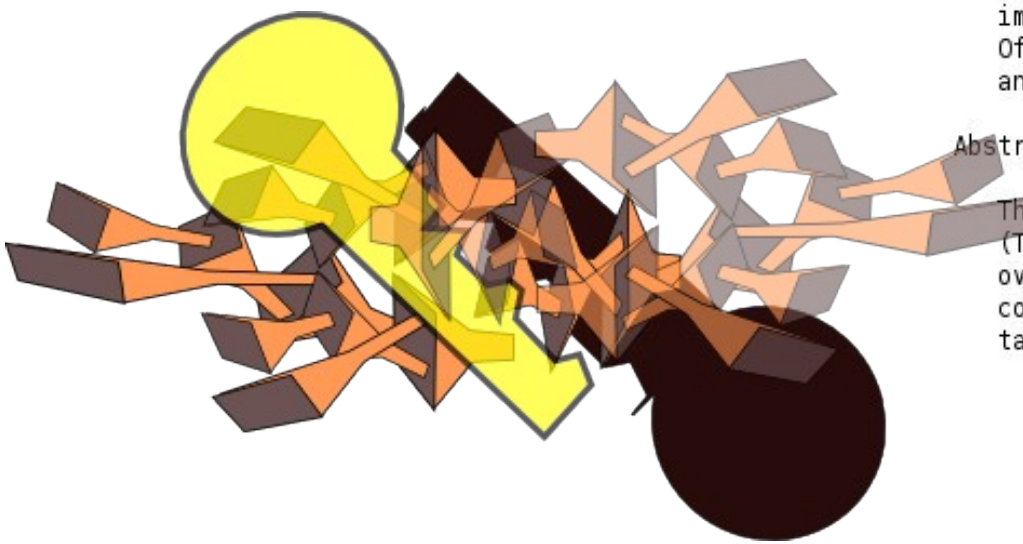
Autour de SSL/TLS
La sécurité par le petit s de https



Updated by: 5746, 5878 — PROPOSED STANDARD
Errata Exist

Network Working Group — T. Dierks
Request for Comments: 5246 — Independent
Obsoletes: 3268, 4346, 4366 — E. Rescorla
Updates: 4492 — RTFM, Inc.
Category: Standards Track — August 2008

The Transport Layer Security (TLS) Protocol Version 1.2

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Abstract

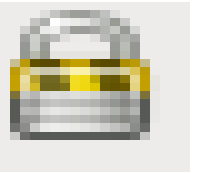
This document specifies Version 1.2 of the Transport Layer Security (TLS) protocol. The TLS protocol provides communications security over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.

Les acteurs...

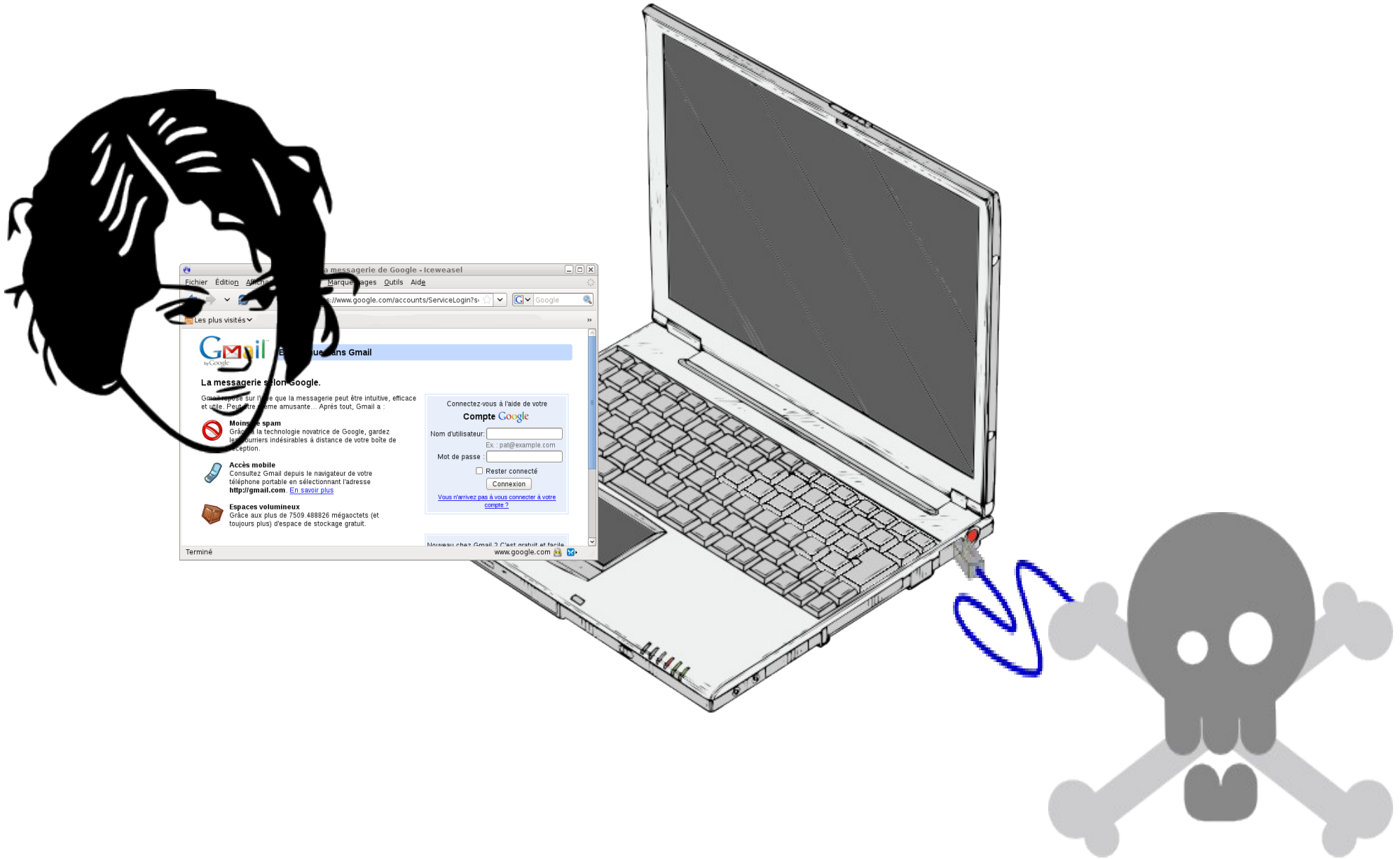
- Alice
- Bob
- Eve
- Mallory
- Le « S » de https



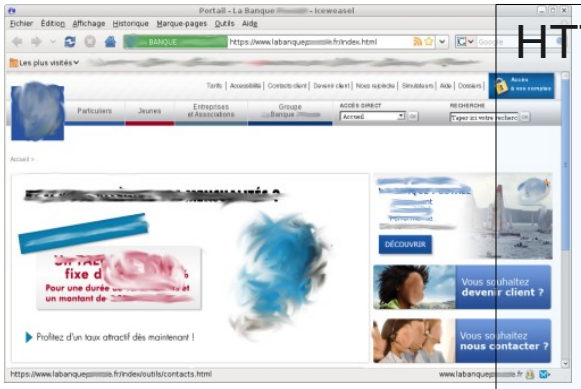




Pourquoi TCP/IP seul n'est pas suffisant ?



Pourquoi HTTP seul n'est pas suffisant ?



HTTP

TCP/IP

Mon identifiant: 6719719
Mon code : 6789

Mon identifiant: 6719719
Mon code : 6789

Mon identifiant: 6719719
Mon code : 6789

Mon identifiant: 6719719
Mon code : 6789

Et HTTPS fait quoi de mieux ?

- la communication s'effectue avec le bon intervenant. **Identification / Authentification**
- la **confidentialité** est respectée
- Le contenu des informations n'est pas altéré, **l'intégrité** est respectée.

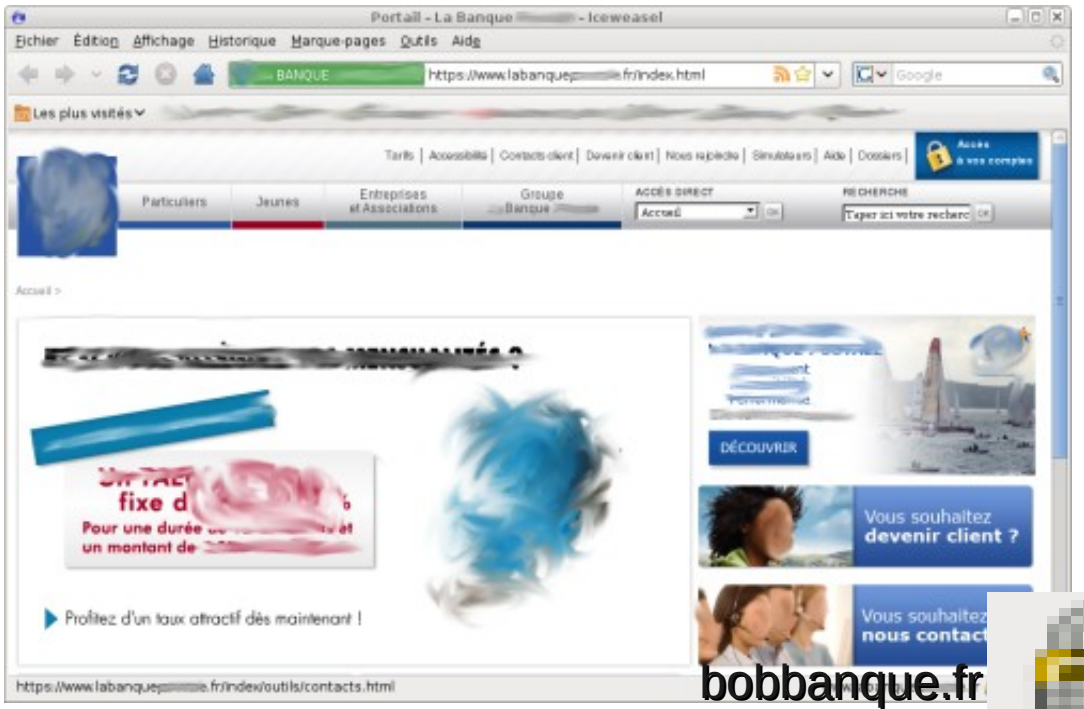
Comment s'assurer que le site web est bien celui de ma banque ?

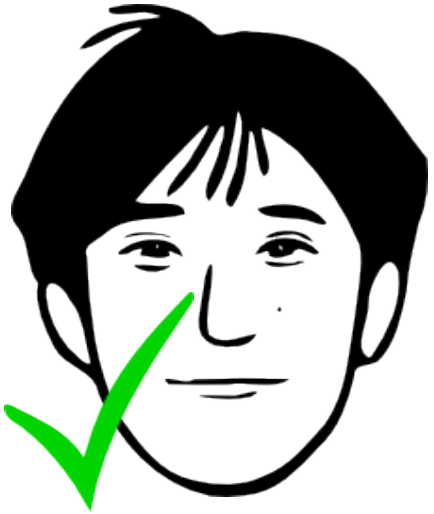
C'est le nom de la banque qui apparaît dans l'url

Comment s'assurer que le site web est bien celui de ma banque ?

L'url commence par https

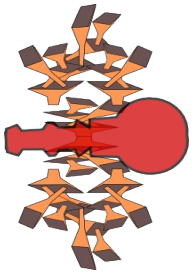
Comment s'assurer que le site web est bien celui de ma banque ?

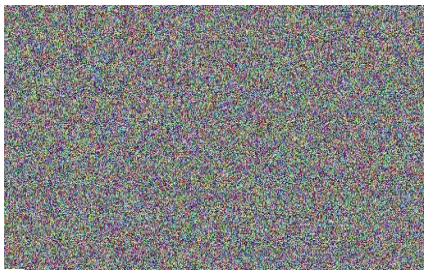


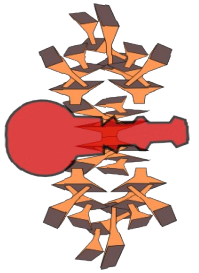


Il y a un cadenas **en bas** indiquant la validité du site

Confidentialité / Chiffrement

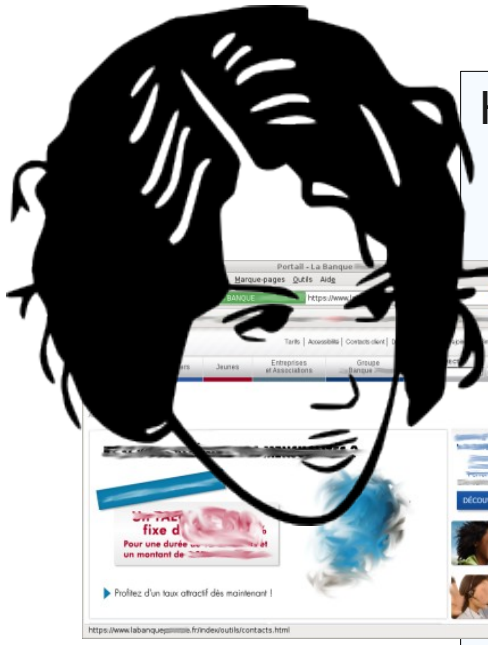






En Clair — Chiffre — Chiffré — Déchiffre — En Clair

PlainText — Encipher/Encrypt — CipherText — Decipher/Decrypt — PlainText

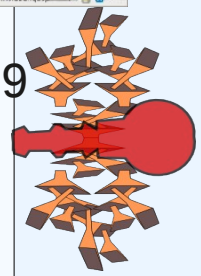


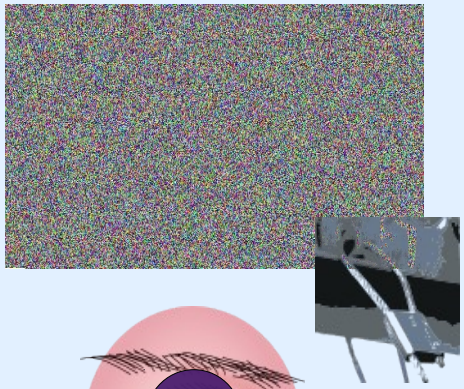
HTTPS

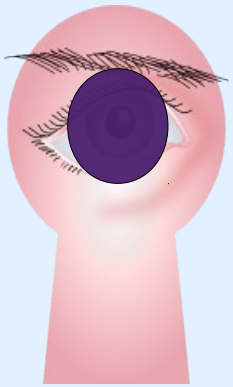
TLS

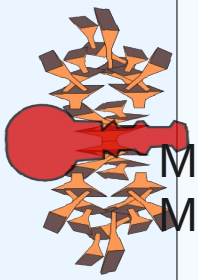
TCP/IP

Mon identifiant: 6719719
Mon code : 6789







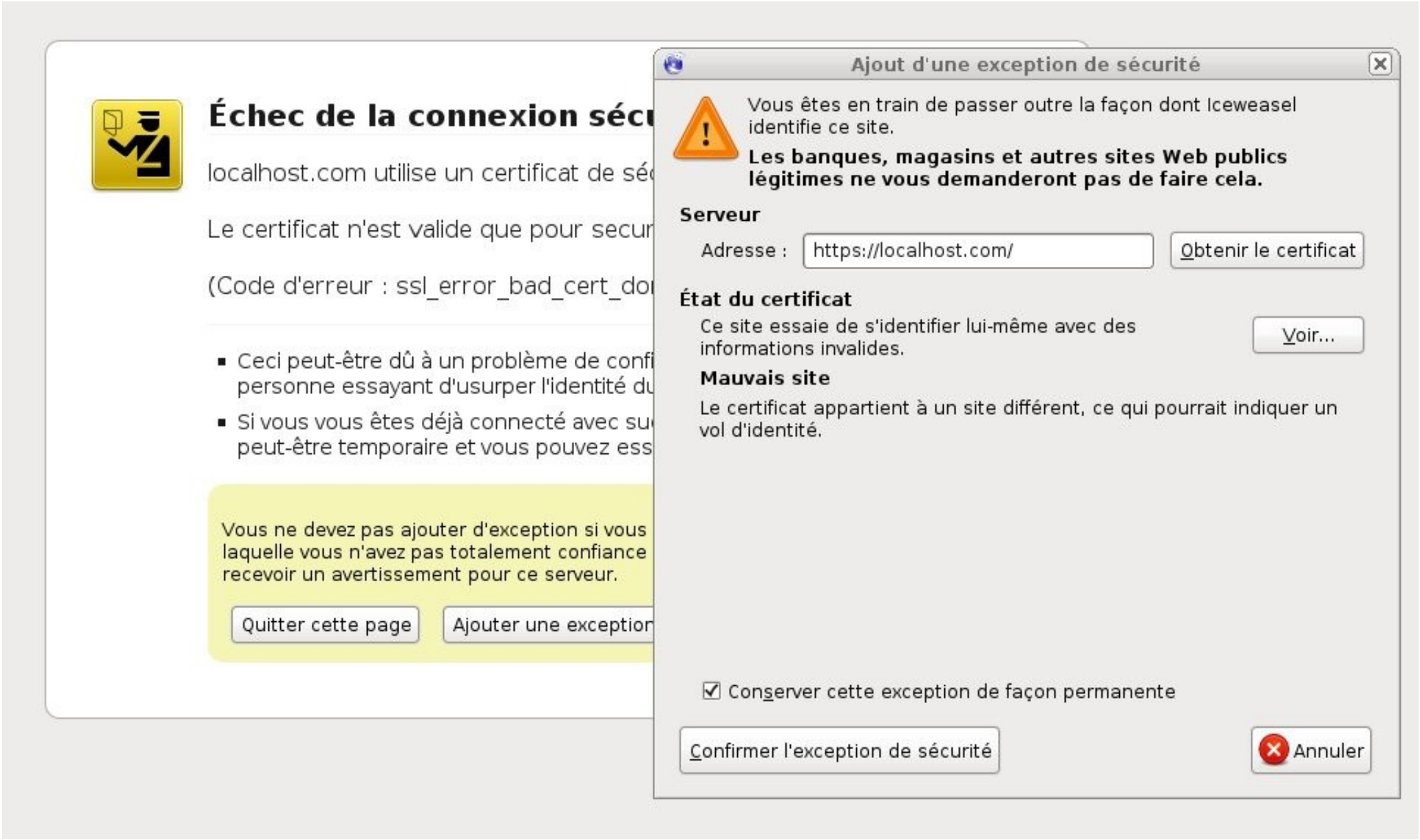


Mon identifiant: 6719719
Mon code : 6789

Pourquoi tous les sites ne sont pas en HTTPS ?

- Parce que cela coûte cher :
  - En CPU (la crypto à clé publique est un gouffre)
  - En certificats : chaque site web doit payer
- Parce que c'est plus lent
- D'ailleurs certains sites ne sécurisent que la partie transaction financière en https
  - Cela pose aussi des problèmes de sécurité...

Le maillon faible



TLS : Le protocole n'est pas secret

Updated by: 5746, 5878 — PROPOSED STANDARD
Errata Exist

Network Working Group — T. Dierks
Request for Comments: 5246 — Independent
Obsoletes: 3268, 4346, 4366 — E. Rescorla
Updates: 4492 — RTFM, Inc.
Category: Standards Track — August 2008

The Transport Layer Security (TLS) Protocol
Version 1.2

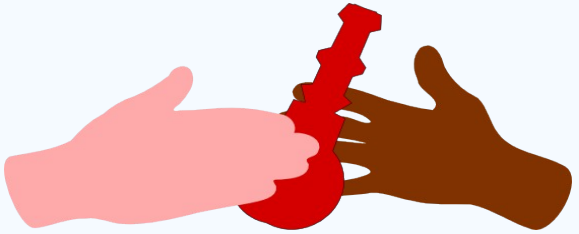
Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

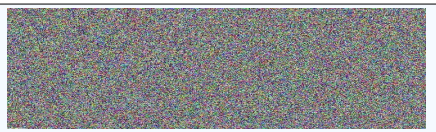
Abstract

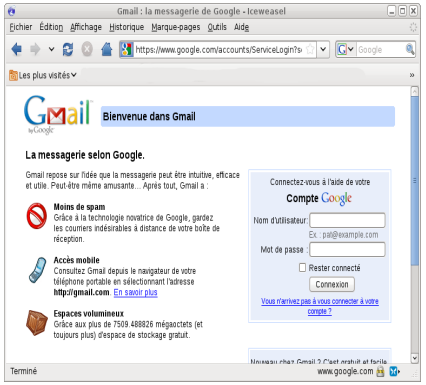
This document specifies Version 1.2 of the Transport Layer Security (TLS) protocol. The TLS protocol provides communications security over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.

C'est très simple...

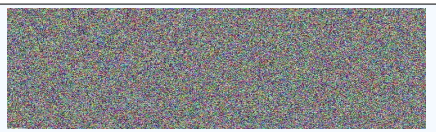


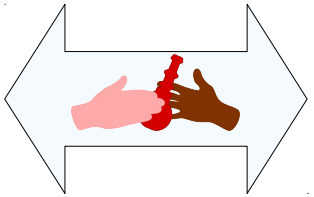
TLS



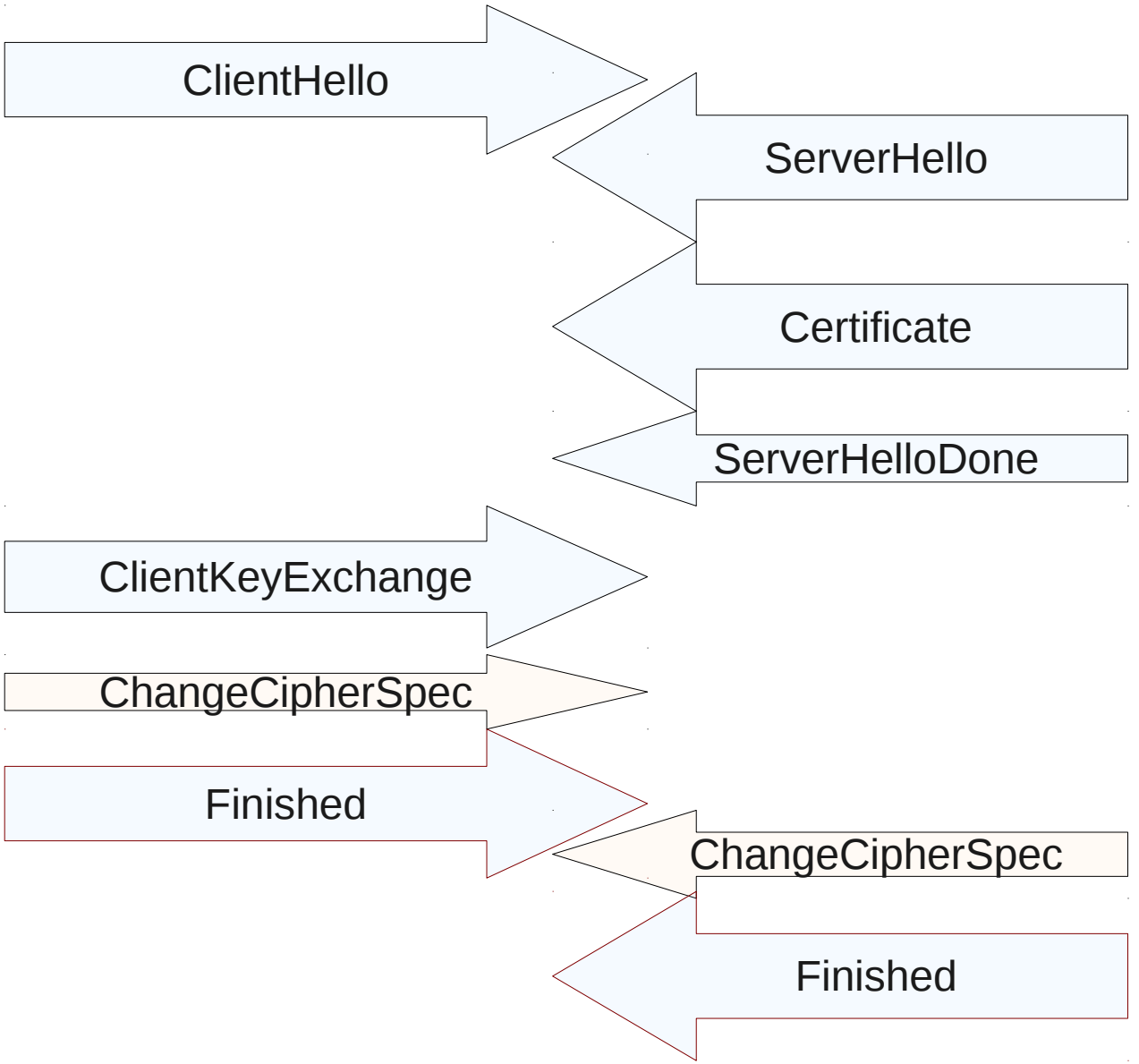


- Réutilsation -

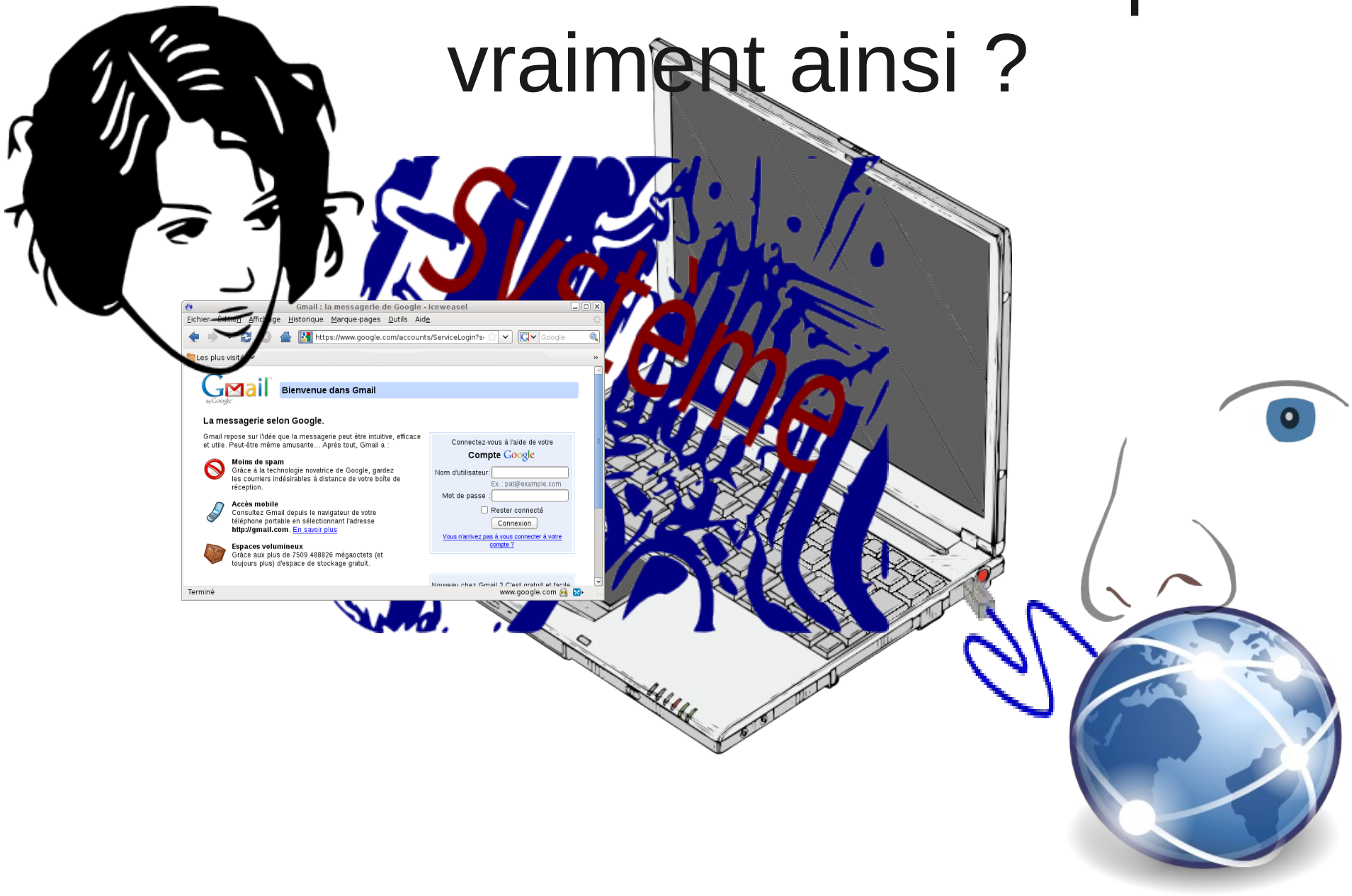




Handshake

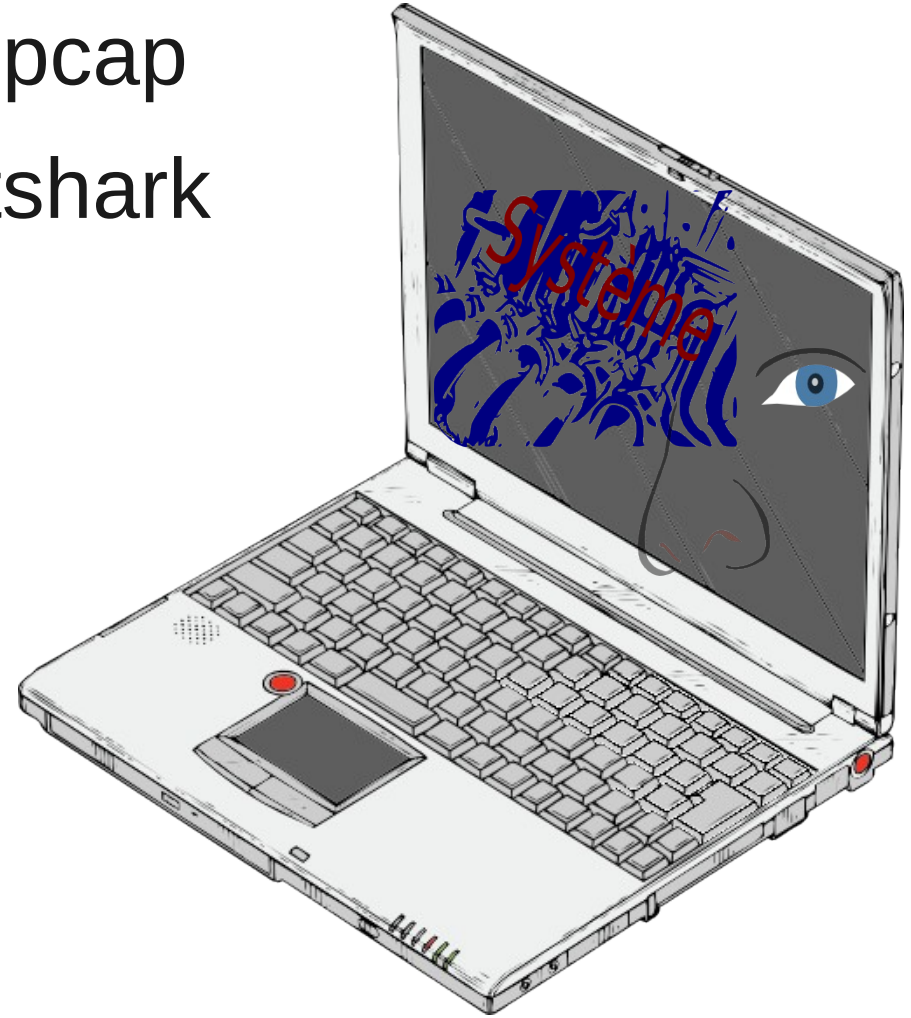

ClientHello
ServerHello
Certificate
ServerHelloDone
ClientKeyExchange
ChangeCipherSpec
Finished
ChangeCipherSpec
Finished

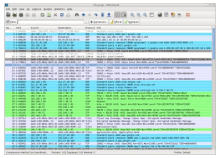
Comment savoir si cela se passe vraiment ainsi ?



Analyser le protocole

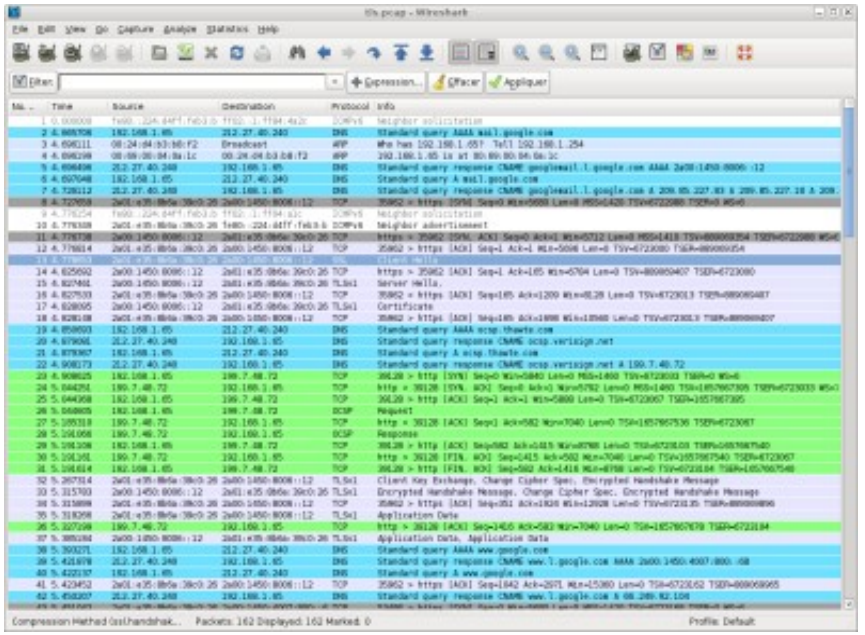
- Tcpdump -i eth0 -s0 -w eth0capture.pcap
- Wireshark eth0capture.pcap
- Ou en mode console : tshark

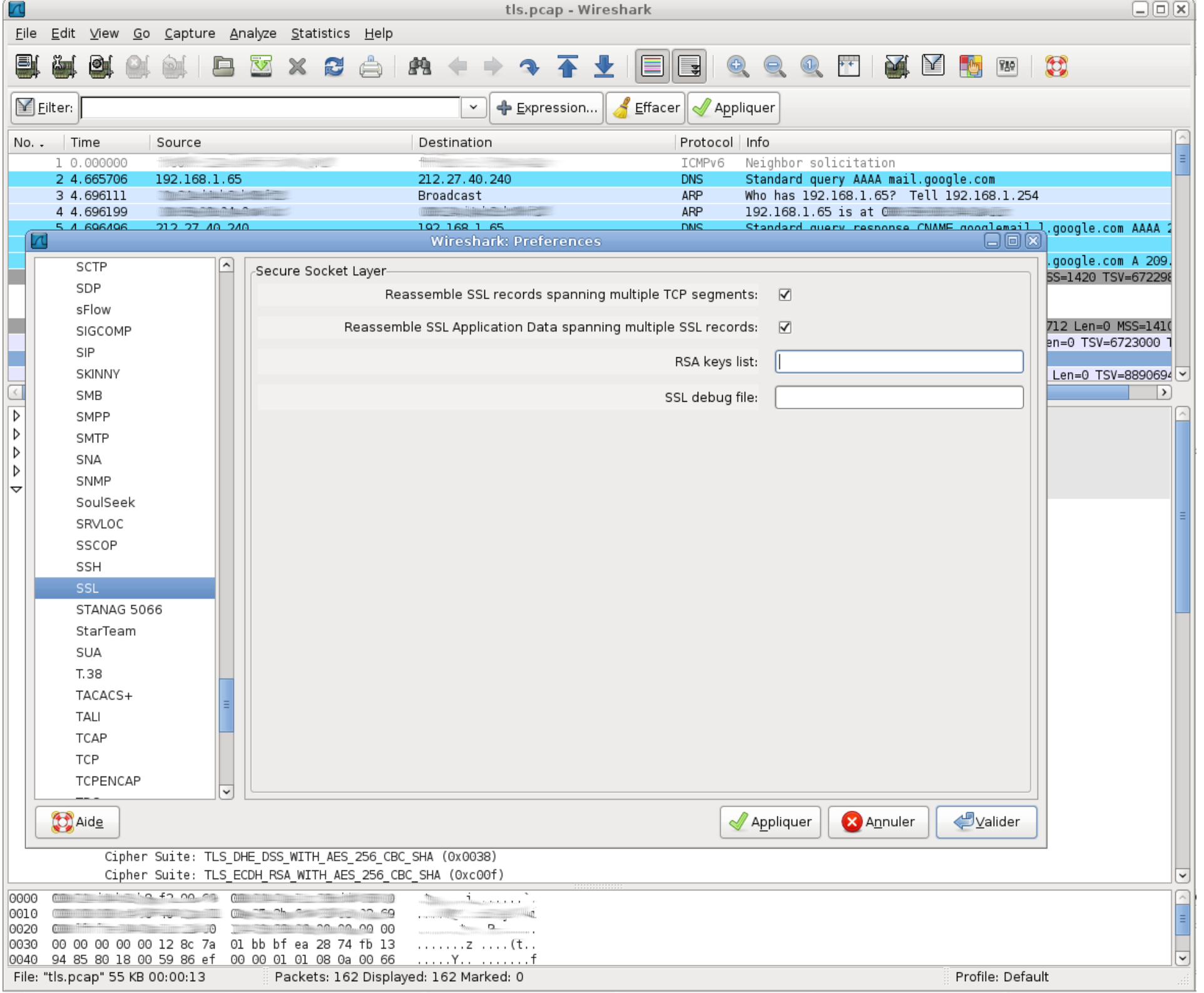


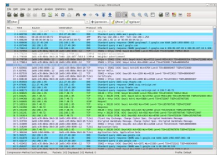


Wireshark

- Super ! Des lignes en couleur ...




tls.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Effacer Appliquer
No. Time Source Destination Protocol Info
1 0.000000 ICMPv6 Neighbor solicitation
2 4.665706 192.168.1.65 212.27.40.240 DNS Standard query AAAA mail.google.com
3 4.696111 Broadcast ARP Who has 192.168.1.65? Tell 192.168.1.254
4 4.696199 ARP 192.168.1.65 is at
Wireshark: Preferences
SCTP
SDP
sFlow
SIGCOMP
SIP
SKINNY
SMB
SMPP
SMTP
SNA
SNMP
SoulSeek
SRVLOC
SSCOP
SSH
SSL
STANAG 5066
StarTeam
SUA
T.38
TACACS+
TALI
TCAP
TCP
TCPENCAP
Secure Socket Layer
Reassemble SSL records spanning multiple TCP segments:
Reassemble SSL Application Data spanning multiple SSL records:
RSA keys list:
SSL debug file:
Aide
Appliquer
Annuler
Valider
Cipher Suite: TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)
Cipher Suite: TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
0030 00 00 00 00 00 12 8c 7a 01 bb bf ea 28 74 fb 13 .....z ....(t..
0040 94 85 80 18 00 59 86 ef 00 00 01 01 08 0a 00 66 .....Y.. .....f
File: "tls.pcap" 55 KB 00:00:13
Packets: 162 Displayed: 162 Marked: 0
Profile: Default



Connection...

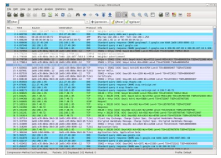
- Chaque ligne est une trame ethernet entrée ou sortie par l'interface de capture (ici eth0)

Avant

Emetteur Recepteur

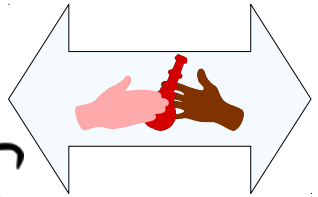
No.	Time	Source	Destination	Protocol	Info
1	0.000000	[redacted]	[redacted]	ICMPv6	Neighbor solicitation
2	4.665706	192.168.1.65	212.27.40.240	DNS	Standard query AAAA mail.google.com
3	4.696111	[redacted]	Broadcast	ARP	Who has 192.168.1.65? Tell 192.168.1.254
4	4.696199	[redacted]	[redacted]	ARP	192.168.1.65 is at 00:69:00:04:0a:1c
5	4.696496	212.27.40.240	192.168.1.65	DNS	Standard query response CNAME googlemail.l.google.com AAAA 2a00:1450:8006::12
6	4.697048	192.168.1.65	212.27.40.240	DNS	Standard query A mail.google.com
7	4.726112	212.27.40.240	192.168.1.65	DNS	Standard query response CNAME googlemail.l.google.com A 209.85.227.83 A 209.85.227.18 A
8	4.727659	2a01:e35:8b6a:39c0:26	2a00:1450:8006::12	TCP	35962 > https [SYN] Seq=0 Win=5680 Len=0 MSS=1420 TSV=6722988 TSER=0 WS=6
9	4.776154	[redacted]	[redacted]	ICMPv6	Neighbor solicitation
10	4.776349	2a01:e35:8b6a:39c0:26	[redacted]	ICMPv6	Neighbor advertisement
11	4.776738	2a00:1450:8006::12	2a01:e35:8b6a:39c0:26	TCP	https > 35962 [SYN, ACK] Seq=0 Ack=1 Win=5712 Len=0 MSS=1410 TSV=889069354 TSER=6722988
12	4.776814	2a01:e35:8b6a:39c0:26	2a00:1450:8006::12	TCP	35962 > https [ACK] Seq=1 Ack=1 Win=5696 Len=0 TSV=6723000 TSER=889069354
13	4.778653	2a01:e35:8b6a:39c0:26	2a00:1450:8006::12	SSL	Client Hello

Après

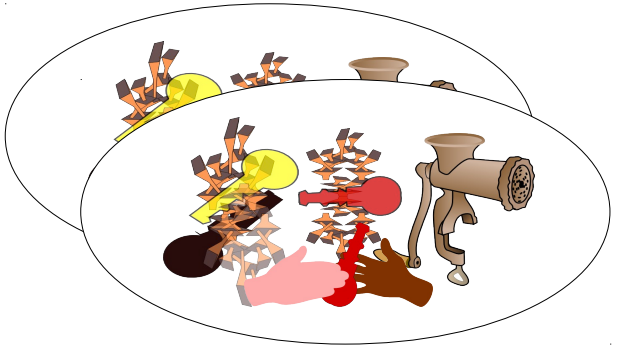


Détail de paquet Ipv6

```
▷ Internet Protocol Version 6
▷ Transmission Control Protocol, Src Port: 35962 (35962), Dst Port: https (443), Seq: 1, Ack: 1, Len: 164
▽ Secure Socket Layer
  ▽ TLSv1 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 159
    ▽ Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 155
        Version: TLS 1.0 (0x0301)
      ▽ Random
          gmt_unix_time: Oct 16, 2010 16:11:54.000000000
          random_bytes: B639BCE044162267662991D67D2826989D3DB46641D6AD99...
        Session ID Length: 0
        Cipher Suites Length: 68
      ▷ Cipher Suites (34 suites)
        Compression Methods Length: 1
      ▽ Compression Methods (1 method)
          Compression Method: null (0)
        Extensions Length: 46
      ▷ Extension: server_name
      ▷ Extension: elliptic_curves
      ▷ Extension: ec_point_formats
      ▷ Extension: SessionTicket TLS
```

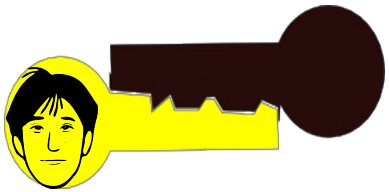


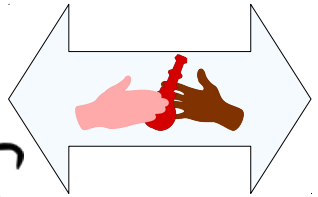
ClientHello



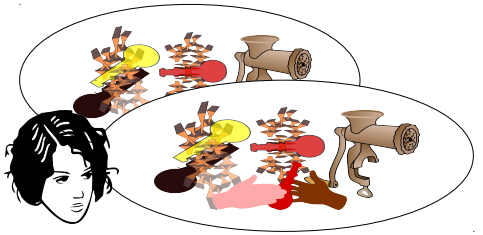
ClientHello

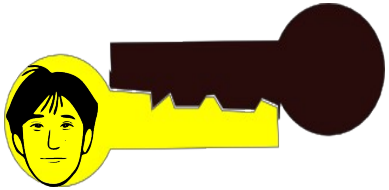
NULL

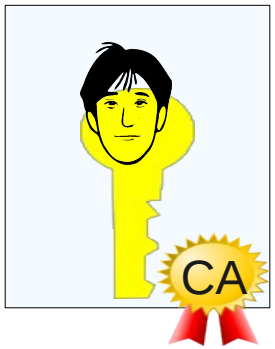




ClientHello



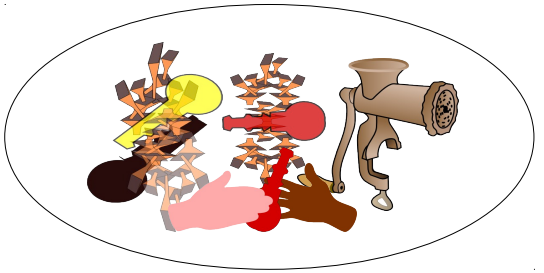




Hasard

- Le hasard est une base de la sécurité
- Entropie
- Determinisme
- Générateur pseudo-aléatoire
- Distribution uniforme

CipherSuite

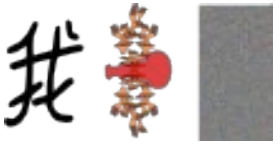


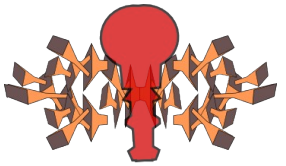
TLS_DH_DSS_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_RC4_128_SHA

Authentification

Echange de clés

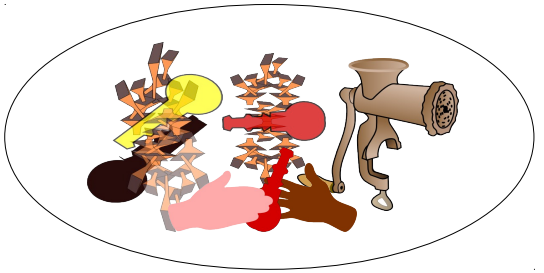
Chiffrage



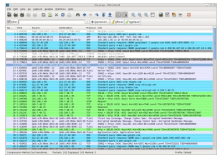


Intégrité

CipherSuite



TLS_KRB5_EXPORT_WITH_DES_CBC_40_MD5	0x00	0x29
TLS_KRB5_EXPORT_WITH_RC2_CBC_40_MD5	0x00	0x2A
TLS_KRB5_EXPORT_WITH_RC4_40_MD5	0x00	0x2B
TLS_GOSTR341094_WITH_28147_CNT_IMIT	0x00	0x80
TLS_GOSTR341001_WITH_28147_CNT_IMIT	0x00	0x81
TLS_GOSTR341094_WITH_NULL_GOSTR3411	0x00	0x82
TLS_GOSTR341001_WITH_NULL_GOSTR3411	0x00	0x83
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	0x00	0x41
TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA	0x00	0x42
TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA	0x00	0x43
TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	0x00	0x44
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	0x00	0x45
TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA	0x00	0x46
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	0x00	0x84
TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA	0x00	0x85
TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA	0x00	0x86
TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	0x00	0x87
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	0x00	0x88
TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA	0x00	0x89
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256	0x00	0xBA
TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA256	0x00	0xBB
TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA256	0x00	0xBC
TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256	0x00	0xBD
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	0x00	0xBE
TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256	0x00	0xBF
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256	0x00	0xC0
TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA256	0x00	0xC1
TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA256	0x00	0xC2
TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256	0x00	0xC3
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256	0x00	0xC4
TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256	0x00	0xC5



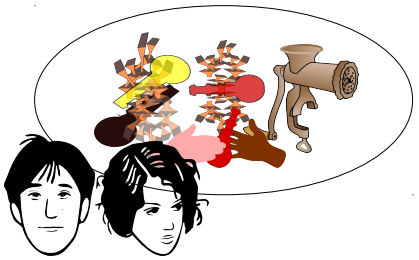
13	4.778653	[redacted]:39c0:26	[redacted]:12	SSL	Client Hello
14	4.825692	[redacted]:12	[redacted]:39c0:26	TCP	https > 35962 [ACK] Seq=1 Ack=165 Win=6784 Len=0 TSV=889069407 TSER=6723000
15	4.827461	[redacted]:12	[redacted]:39c0:26	TLSv1	Server Hello,
16	4.827533	[redacted]:39c0:26	[redacted]:12	TCP	35962 > https [ACK] Seq=165 Ack=1209 Win=8128 Len=0 TSV=6723013 TSER=889069407
17	4.828095	[redacted]:12	[redacted]:39c0:26	TLSv1	Certificate
18	4.828148	[redacted]:39c0:26	[redacted]:12	TCP	35962 > https [ACK] Seq=165 Ack=1698 Win=10560 Len=0 TSV=6723013 TSER=889069407
19	4.850693	192.168.1.65	212.27.40.240	DNS	Standard query AAAA ocsp.thawte.com

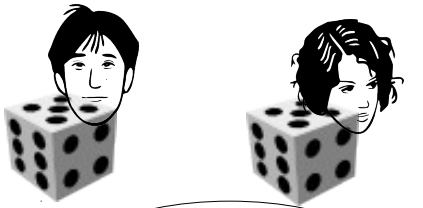
Secure Socket Layer

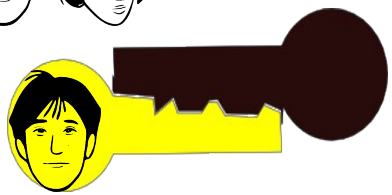
- TLSv1 Record Layer: Handshake Protocol: Server Hello
  - Content Type: Handshake (22)
  - Version: TLS 1.0 (0x0301)
  - Length: 52
  - Handshake Protocol: Server Hello
    - Handshake Type: Server Hello (2)
    - Length: 48
    - Version: TLS 1.0 (0x0301)
    - Random
      - gmt_unix_time: Oct 16, 2010 16:11:54.000000000
      - random_bytes: C0BC3311C476CB3640AEA0492C97FA870E1C4ABBCC033287...
    - Session ID Length: 0
    - Cipher Suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)
    - Compression Method: null (0)
    - Extensions Length: 8
    - Extension: server_name
      - Type: server_name (0x0000)
      - Length: 0
      - Data (0 bytes)
    - Extension: SessionTicket TLS
      - Type: SessionTicket TLS (0x0023)
      - Length: 0
      - Data (0 bytes)

ClientHello

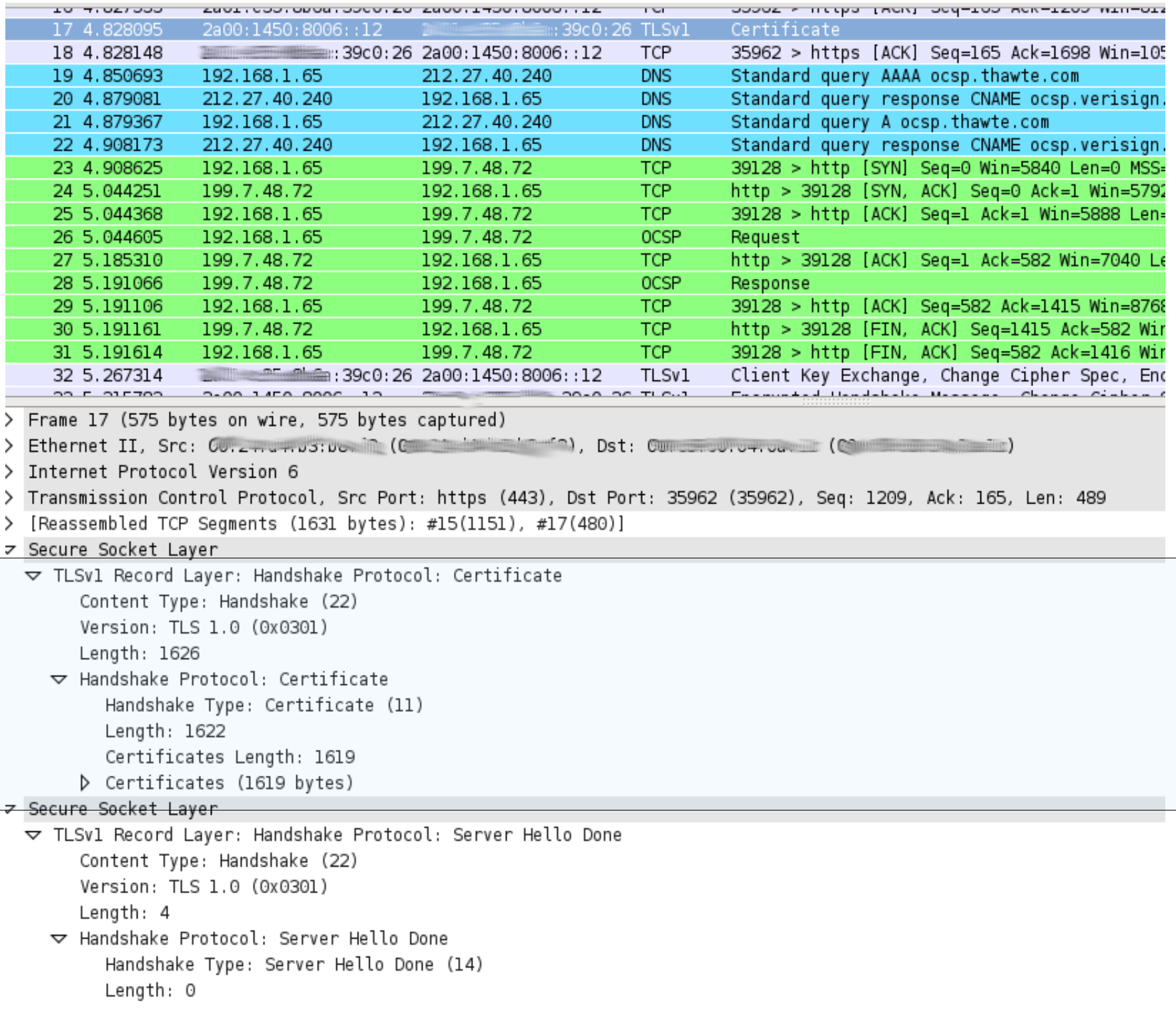
ServerHello







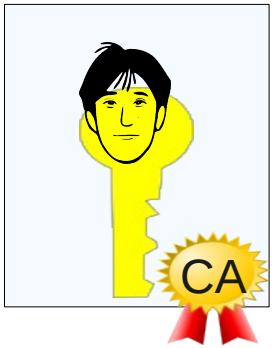
ServerHello


17 4.828095 2a00:1450:8006::12 :39c0:26 TLSv1 Certificate
18 4.828148 :39c0:26 2a00:1450:8006::12 TCP 35962 > https [ACK] Seq=165 Ack=1698 Win=105
19 4.850693 192.168.1.65 212.27.40.240 DNS Standard query AAAA ocsp.thawte.com
20 4.879081 212.27.40.240 192.168.1.65 DNS Standard query response CNAME ocsp.verisign.
21 4.879367 192.168.1.65 212.27.40.240 DNS Standard query A ocsp.thawte.com
22 4.908173 212.27.40.240 192.168.1.65 DNS Standard query response CNAME ocsp.verisign.
23 4.908625 192.168.1.65 199.7.48.72 TCP 39128 > http [SYN] Seq=0 Win=5840 Len=0 MSS=
24 5.044251 199.7.48.72 192.168.1.65 TCP http > 39128 [SYN, ACK] Seq=0 Ack=1 Win=5792
25 5.044368 192.168.1.65 199.7.48.72 TCP 39128 > http [ACK] Seq=1 Ack=1 Win=5888 Len=
26 5.044605 192.168.1.65 199.7.48.72 OCSP Request
27 5.185310 199.7.48.72 192.168.1.65 TCP http > 39128 [ACK] Seq=1 Ack=582 Win=7040 Le
28 5.191066 199.7.48.72 192.168.1.65 OCSP Response
29 5.191106 192.168.1.65 199.7.48.72 TCP 39128 > http [ACK] Seq=582 Ack=1415 Win=8768
30 5.191161 199.7.48.72 192.168.1.65 TCP http > 39128 [FIN, ACK] Seq=1415 Ack=582 Win
31 5.191614 192.168.1.65 199.7.48.72 TCP 39128 > http [FIN, ACK] Seq=582 Ack=1416 Win
32 5.267314 :39c0:26 2a00:1450:8006::12 TLSv1 Client Key Exchange, Change Cipher Spec, Enc
Frame 17 (575 bytes on wire, 575 bytes captured)
Ethernet II, Src:
Dst:
Internet Protocol Version 6
Transmission Control Protocol, Src Port: https (443), Dst Port: 35962 (35962), Seq: 1209, Ack: 165, Len: 489
[Reassembled TCP Segments (1631 bytes): #15(1151), #17(480)]
Secure Socket Layer
TLSv1 Record Layer: Handshake Protocol: Certificate
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 1626
Handshake Protocol: Certificate
Handshake Type: Certificate (11)
Length: 1622
Certificates Length: 1619
Certificates (1619 bytes)
Secure Socket Layer
TLSv1 Record Layer: Handshake Protocol: Server Hello Done
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 4
Handshake Protocol: Server Hello Done
Handshake Type: Server Hello Done (14)
Length: 0

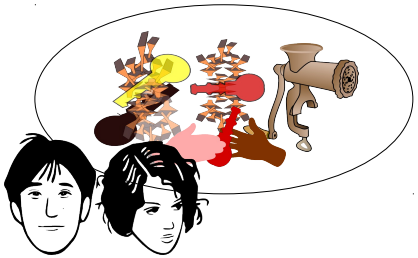
ClientHello

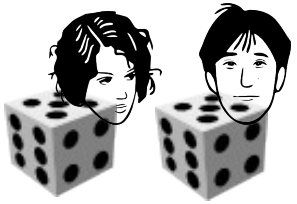
ServerHello

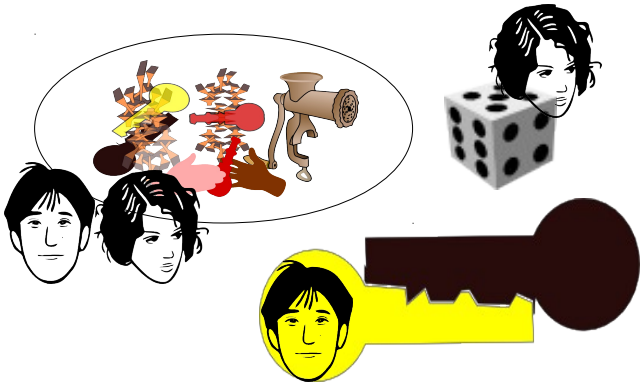
Certificate

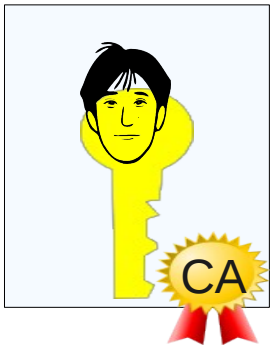


Certificate

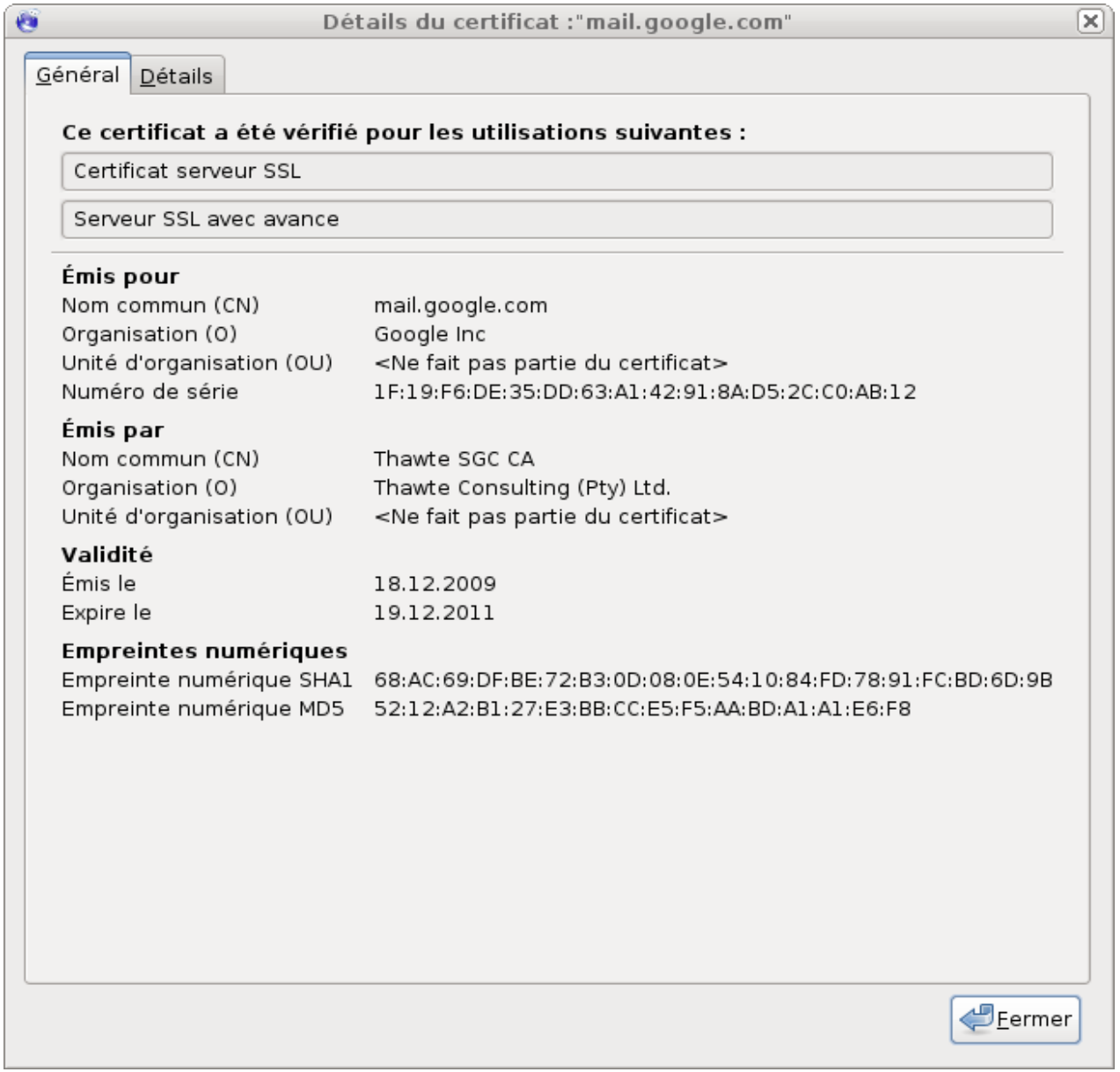




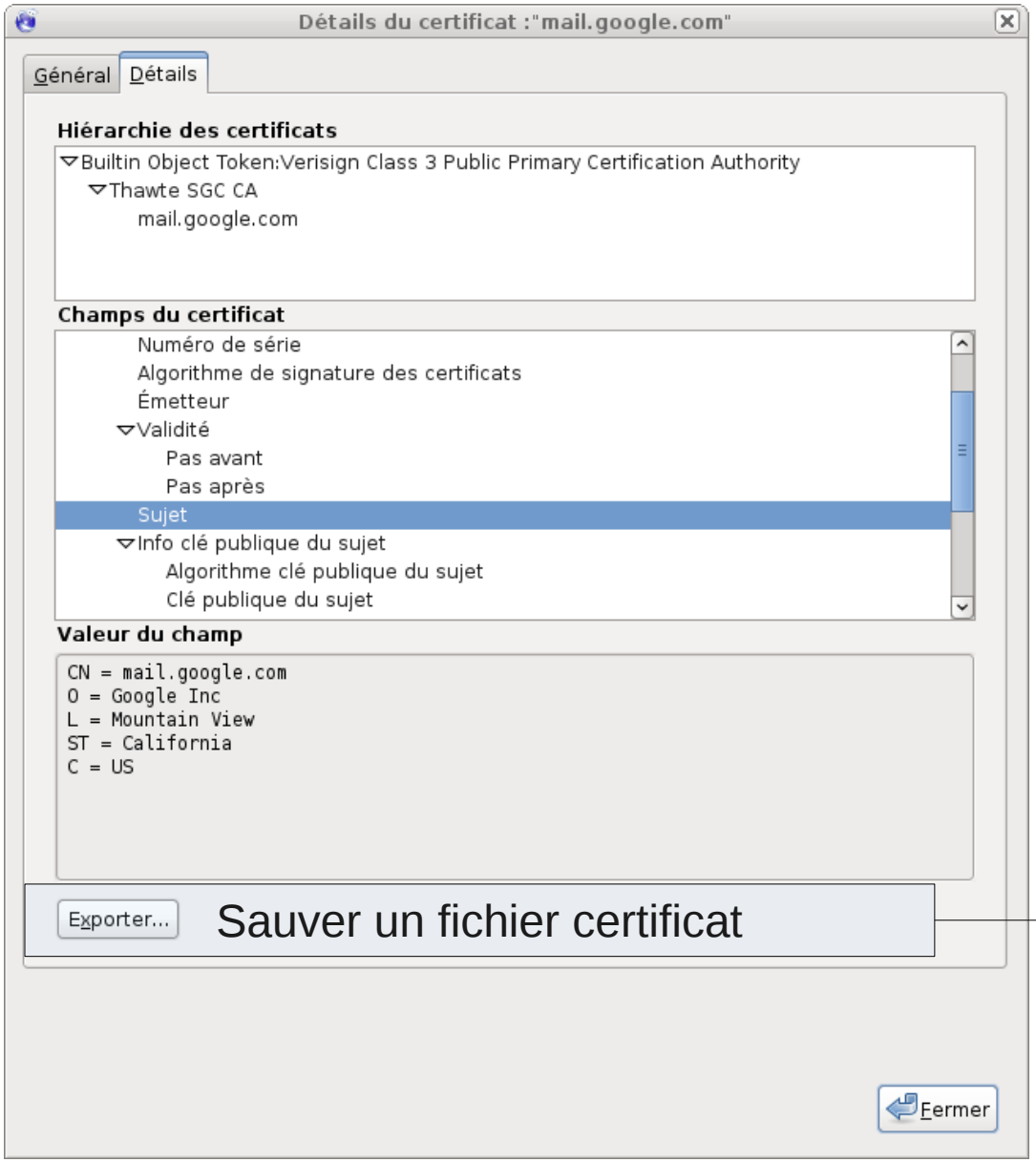




Les Certificats X509



Fichier certificat au format PEM



gmail.cert

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIQL9+89q6RUm0PmqPfQDQ+mjANBgkqhkiG9w0BAQUFADBM
MQswCQYDVQQGEwJaQTElMCMGA1UEChMcVGhhd3RlIENvbnN1bHRpbmcgKFB0eSkg
THRkLjEWMBQGA1UEAxMNVGhhd3RlIFNHQyBDQTAeFw0wOTEyMTgwMDAwMDBaFw0x
MTEyMTgyMzU5NTlaMGgxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlh
MRYwFAYDVQQHFA1Nb3VudGFpbiBWaWV3MRMwEQYDVQQKFApHb29nbGUgSW5jMRcw
FQYDVQQDFA53d3cuZ29vZ2xlLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkC
gYEA6PmGD5D6htffvXImttdEAoN4c9kCKO+IRTn7EOh8rqk41XXGOOsKFQebg+jN
gtXj9xVoRaELGYW84u+E593y17iYwqG7tcFR39SDAqc9BkJb4SLD3muFXxzW2k6L
05vuuWciKh0R73mkszeK9P4Y/bz5RiNQl/Os/CRGK1w7t0UCAwEAAaOB5zCB5DAM
BgNVHRMBAf8EAjAAMDYGA1UdHwQvMC0wK6ApoCeGJWh0dHA6Ly9jcmwudGhhd3Rl
LmNvbS9UaGF3dGVTR0NDQS5jcmwwKAYDVR0lBCEwHwYIKwYBBQUHAwEGCCsGAQUF
BwMCBglghkgBhvhCBAEwcgYIKwYBBQUHAQEEZjBkMCIGCCsGAQUFBzABhhZodHRw
Oi8vb2NzcC50aGF3dGUuY29tMD4GCCsGAQUFBzAChjJodHRwOi8vd3d3LnRoYXd0
ZS5jb20vcmVwb3NpdG9yeS9UaGF3dGVfU0dDX0NBLmNydDANBgkqhkiG9w0BAQUF
AAOBgQCfQ89bxFApsb/isJr/aiEdLRLDLE5a+RLizrmCUi3nHX4adpaQedEkUjh5
u2ONgJd8IyAPkU0Wueru9G2Jysa9zCRo1kNbzipYvzwY4OA8Ys+EWASDLD04se6
z5nRUP8pJcA2NhUzUnC+MY+f6H/nEQyNv4SgQhqAibAxWEEHXw==
-----END CERTIFICATE-----
```

Base64

PEM

Base64

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIQL9+89q6RUm0PmqPfQDQ+mjANBgkqhkiG9w0BAQUFADBM
MQswCQYDVQQGEwJaQTElMCMGA1UEChMcVGhhd3RlIENvbnN1bHRpbmcgKFB0eSkg
THRkLjEWMBQGA1UEAxMNVGhhd3RlIFNHQyBDQTAeFw0wOTEyMTgwMDAwMDBaFw0x
MTEyMTgyMzU5NTlaMGgxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlh
MRYwFAYDVQQHFA1Nb3VudGFpbiBWaWV3MRMwEQYDVQQKFApHb29nbGUgSW5jMRcw
FQYDVQQDFA53d3cuZ29vZ2xlLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkC
gYEA6PmGD5D6htffvXImttdEAoN4c9kCKO+IRTn7EOh8rqk41XXGOOsKFQebg+jN
gtXj9xVoRaELGYW84u+E593y17iYwqG7tcFR39SDAqc9BkJb4SLD3muFXxzW2k6L
05vuuWciKh0R73mkszeK9P4Y/bz5RiNQl/Os/CRGK1w7t0UCAwEAAaOB5zCB5DAM
BgNVHRMBAf8EAjAAMDYGA1UdHwQvMC0wK6ApoCeGJWh0dHA6Ly9jcmwudGhhd3Rl
LmNvbS9UaGF3dGVTR0NDQS5jcmwwKAYDVR0lBCEwHwYIKwYBBQUHAwEGCCsGAQUF
BwMCBglghkgBhvhCBAEwcgYIKwYBBQUHAQEEZjBkMCIGCCsGAQUFBzABhhZodHRw
Oi8vb2NzcC50aGF3dGUuY29tMD4GCCsGAQUFBzAChjJodHRwOi8vd3d3LnRoYXd0
ZS5jb20vcmVwb3NpdG9yeS9UaGF3dGVfU0dDX0NBLmNydDANBgkqhkiG9w0BAQUF
AAOBgQCfQ89bxFApsb/isJr/aiEdLRLDLE5a+RLizrmCUi3nHX4adpaQedEkUjh5
u2ONgJd8IyAPkU0Wueru9G2Jysa9zCRo1kNbzipYvzwY4OA8Ys+WAi0oR1A04Se6
z5nRUP8pJcA2NhUzUnC+MY+f6H/nEQyNv4SgQhqAibAxWEEHXw==
-----END CERTIFICATE-----
```

openssl base64 -d -in gmail.cert | hexdump -C

```
00000000  30 82 03 21 30 82 02 8a  a0 03 02 01 02 02 10 2f  |0..!0........../|
00000010  df bc f6 ae 91 52 6d 0f  9a a3 df 40 34 3e 9a 30  |.....Rm....@4>.0|
00000020  0d 06 09 2a 86 48 86 f7  0d 01 01 05 05 00 30 4c  |...*.H........0L|
00000030  31 0b 30 09 06 03 55 04  06 13 02 5a 41 31 25 30  |1.0...U....ZA1%0|
00000040  23 06 03 55 04 0a 13 1c  54 68 61 77 74 65 20 43  |#..U....Thawte C|
00000050  6f 6e 73 75 6c 74 69 6e  67 20 28 50 74 79 29 20  |onsulting (Pty) |
00000060  4c 74 64 2e 31 16 30 14  06 03 55 04 03 13 0d 54  |Ltd.1.0...U....T|
00000070  68 61 77 74 65 20 53 47  43 20 43 41 30 1e 17 0d  |hawte SGC CA0...|
00000080  30 39 31 32 31 38 30 30  30 30 30 30 5a 17 0d 31  |091218000000Z..1|
00000090  31 31 32 31 38 32 33 35  39 35 39 5a 30 68 31 0b  |11218235959Z0h1.|
000000a0  30 09 06 03 55 04 06 13  02 55 53 31 13 30 11 06  |0...U....US1.0..|
000000b0  03 55 04 08 13 0a 43 61  6c 69 66 6f 72 6e 69 61  |.U....California|
000000c0  31 16 30 14 06 03 55 04  07 14 0d 4d 6f 75 6e 74  |1.0...U....Mount|
000000d0  61 69 6e 20 56 69 65 77  31 13 30 11 06 03 55 04  |ain View1.0...U.|
000000e0  0a 14 0a 47 6f 6f 67 6c  65 20 49 6e 63 31 17 30  |...Google Inc1.0|
000000f0  15 06 03 55 04 03 14 0e  77 77 77 2e 67 6f 6f 67  |...U....www.goog|
00000100  6c 65 2e 63 6f 6d 30 81  9f 30 0d 06 09 2a 86 48  |le.com0..0...*.H|
00000110  86 f7 0d 01 01 01 05 00  03 81 8d 00 30 81 89 02  |............0...|
00000120  81 81 00 e8 f9 86 0f 90  fa 86 d7 df bd 72 26 b6  |.............r&.|
00000130  d7 44 02 83 78 73 d9 02  28 ef 88 45 39 fb 10 e8  |.D..xs..(..E9...|
00000140  7c ae a9 38 d5 75 c6 38  eb 0a 15 07 9b 83 e8 cd  ||..8.u.8........|
00000150  82 d5 e3 f7 15 68 45 a1  0b 19 85 bc e2 ef 84 e7  |.....hE.........|
00000160  dd f2 d7 b8 98 c2 a1 bb  b5 c1 51 df d4 83 02 a7  |..........Q.....|
00000170  3d 06 42 5b e1 22 c3 de  6b 85 5f 1c d6 da 4e 8b  |=.B[."..k._...N.|
00000180  d3 9b ee b9 67 22 2a 1d  11 ef 79 a4 b3 37 8a f4  |....g"*...y..7..|
00000190  fe 18 fd bc f9 46 23 50  97 f3 ac fc 24 46 2b 5c  |.....F#P....$F+\|
000001a0  3b b7 45 02 03 01 00 01  a3 81 e7 30 81 e4 30 0c  |;.E........0..0.|
000001b0  06 03 55 1d 13 01 01 ff  04 02 30 00 30 36 06 03  |..U.......0.06..|
000001c0  55 1d 1f 04 2f 30 2d 30  2b a0 29 a0 27 86 25 68  |U.../0-0+.).'.%h|
000001d0  74 74 70 3a 2f 2f 63 72  6c 2e 74 68 61 77 74 65  |ttp://crl.thawte|
000001e0  2e 63 6f 6d 2f 54 68 61  77 74 65 53 47 43 43 41  |.com/ThawteSGCCA|
000001f0  2e 63 72 6c 30 28 06 03  55 1d 25 04 21 30 1f 06  |.crl0(..U.%.!0..|
00000200  08 2b 06 01 05 05 07 03  01 06 08 2b 06 01 05 05  |.+.........+....|
00000210  07 03 02 06 09 60 86 48  01 86 f8 42 04 01 30 72  |.....`.H...B..0r|
00000220  06 08 2b 06 01 05 05 07  01 01 04 66 30 64 30 22  |..+........f0d0"|
00000230  06 08 2b 06 01 05 05 07  30 01 86 16 68 74 74 70  |..+.....0...http|
00000240  3a 2f 2f 6f 63 73 70 2e  74 68 61 77 74 65 2e 63  |://ocsp.thawte.c|
00000250  6f 6d 30 3e 06 08 2b 06  01 05 05 07 30 02 86 32  |om0>..+.....0..2|
00000260  68 74 74 70 3a 2f 2f 77  77 77 2e 74 68 61 77 74  |http://www.thawt|
00000270  65 2e 63 6f 6d 2f 72 65  70 6f 73 69 74 6f 72 79  |e.com/repository|
00000280  2f 54 68 61 77 74 65 5f  53 47 43 5f 43 41 2e 63  |/Thawte_SGC_CA.c|
00000290  72 74 30 0d 06 09 2a 86  48 86 f7 0d 01 01 05 05  |rt0...*.H.......|
000002a0  00 03 81 81 00 9f 43 cf  5b c4 50 29 b1 bf e2 b0  |......C.[.P)....|
000002b0  9a ff 6a 21 1d 2d 12 c3  2c 4e 5a f9 12 e2 ce b9  |..j!.-..,NZ.....|
000002c0  82 52 2d e7 1d 7e 1a 76  96 90 79 d1 24 52 38 79  |.R-..~.v..y.$R8y|
000002d0  bb 63 8d 80 97 7c 23 20  0f 91 4d 16 b9 ea ee f4  |.c...|# ..M.....|
000002e0  6d 89 ca c6 bd cc 24 68  d6 43 5b ce 2a 58 bf 3c  |m.....$h.C[.*X.<|
000002f0  18 e0 e0 3c 62 cf 96 02  2d 28 47 50 34 e1 27 ba  |...<b...-(GP4.'.|
00000300  cf 99 d1 50 ff 29 25 c0  36 36 15 33 52 70 be 31  |...P.)%.66.3Rp.1|
00000310  8f 9f e8 7f e7 11 0c 8d  bf 84 a0 42 1a 80 89 b0  |...........B....|
00000320  31 58 41 07 5f                                    |1XA._|
00000325
```

- Base64 : permet de faire tenir dans un texte des données numériques.
- 65 caractères <-> 6 bits
- Pour openssl il faut que chaque ligne fasse moins de 80 caractères

Openssl

- Un outil en ligne de commande (openssl <commande> <arguments...>)
  - Administrateur système / sécurité : génération des clés, demande de Certificats
  - Mise en place d'un serveur Web sécurisé (ex: apache avec mod_ssl).
- Une librairie de fonctions pour la sécurité
  - Développement d'une application nécessitant une sécurité particulière
  - D'autres librairies existent : NSS, GnuTLS ...
- Licence BSD like

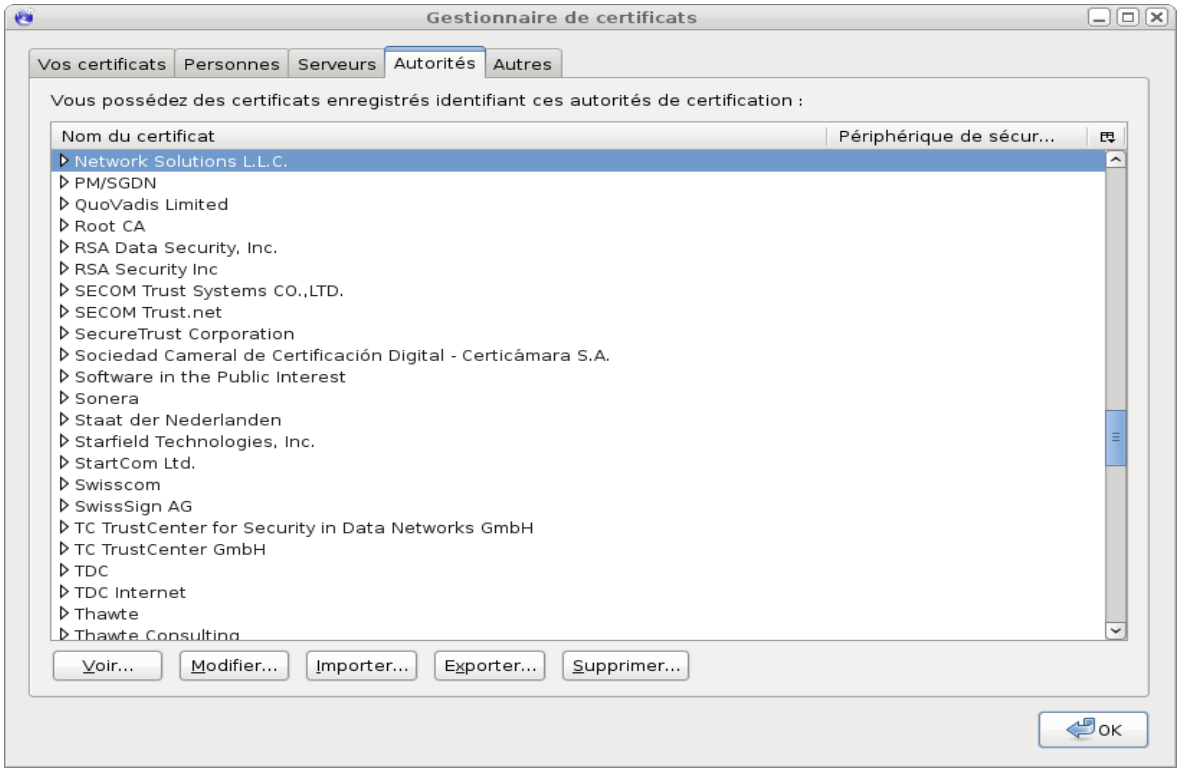
Certificat Texte

openssl x509 -text -in gmail.cert

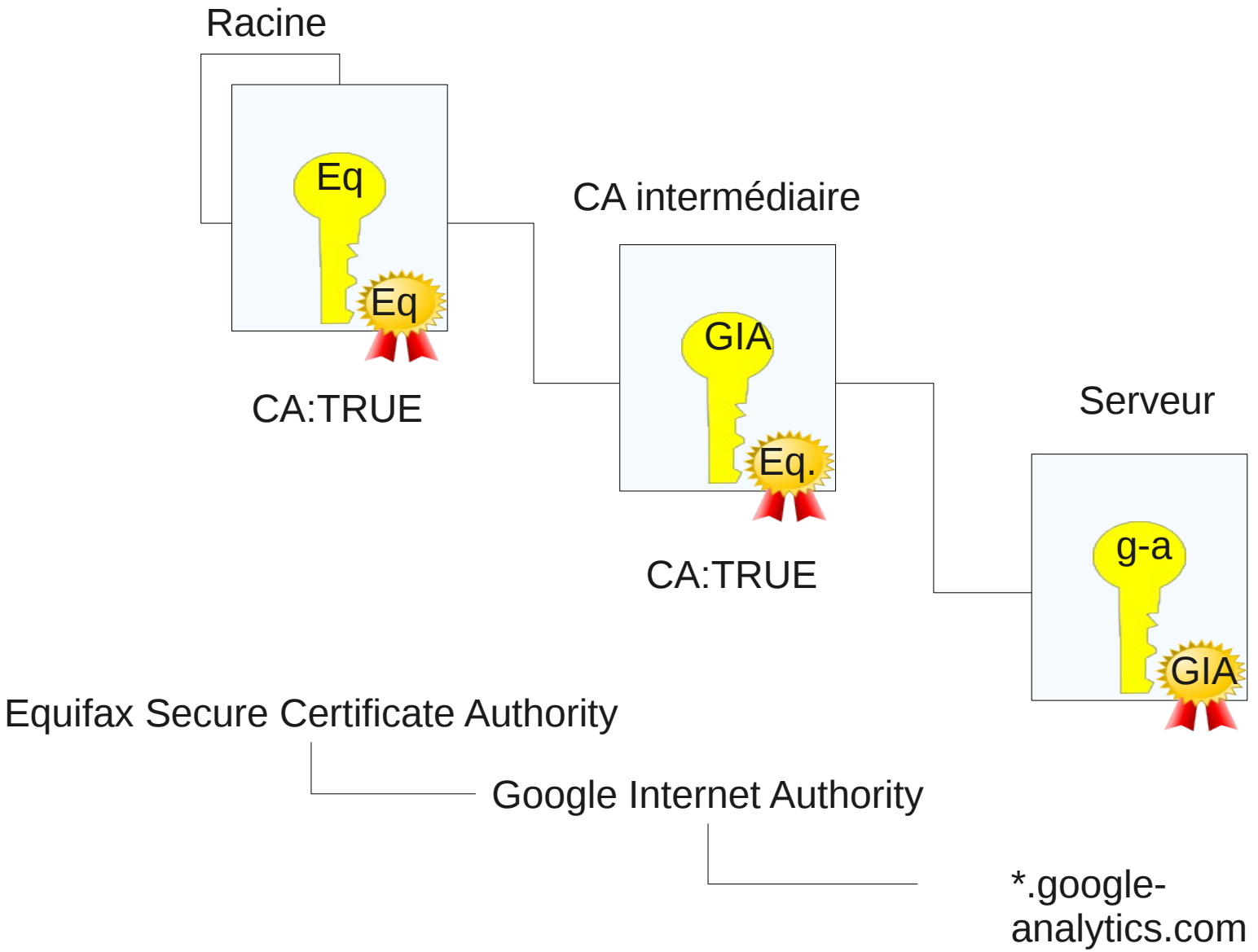
```
    Data:
        Version: 3 (0x2)
        Serial Number: 2f:df:bc:f6:ae:91:52:6d:0f:9a:a3:df:40:34:3e:9a
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=ZA, O=Thawte Consulting (Pty) Ltd., CN=Thawte SGC CA
        Validity
            Not Before: Dec 18 00:00:00 2009 GMT
            Not After : Dec 18 23:59:59 2011 GMT
        Subject: C=US, ST=California, L=Mountain View, O=Google Inc, CN=www.google.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 CRL Distribution Points:
                URI:http://crl.thawte.com/ThawteSGCCA.crl
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication, Netscape Server Gated Crypto
            Authority Information Access:
                OCSP - URI:http://ocsp.thawte.com
                CA Issuers - URI:http://www.thawte.com/repository/Thawte_SGC_CA.crt
    Signature Algorithm: sha1WithRSAEncryption
        9f:...07:5f
```

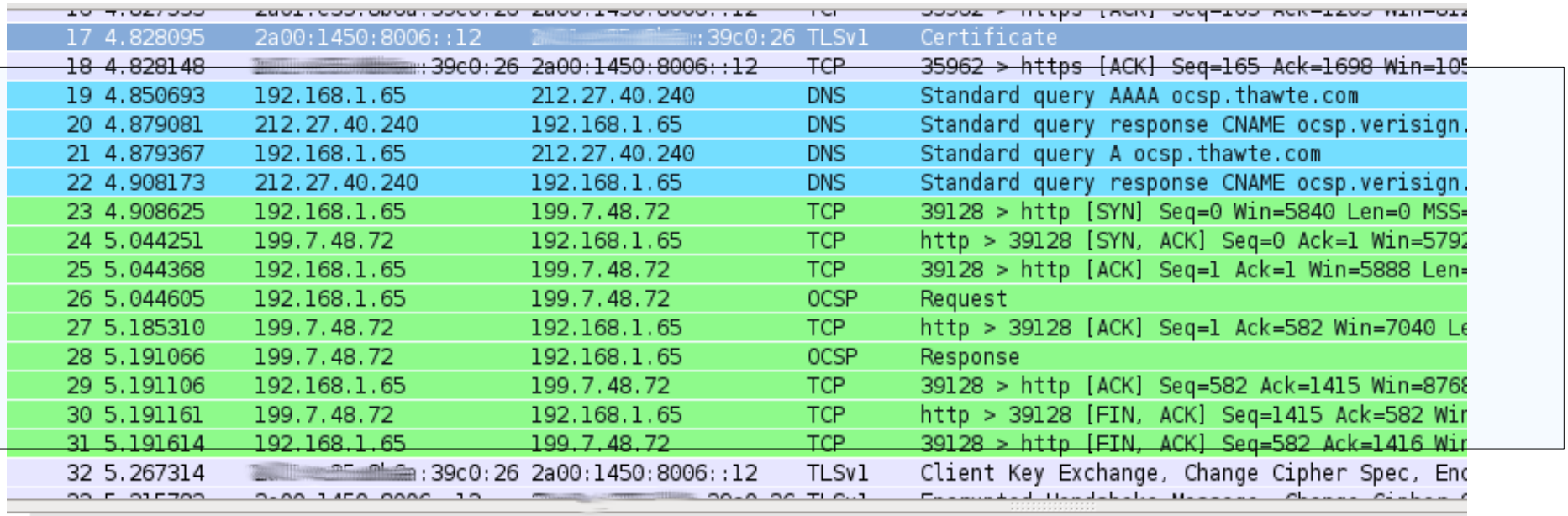
Autorité de Certification

wget http://www.thawte.com/repository/Thawte_SGC_CA.crt
openssl x509 -inform der -in Thawte_SGC_CA.crt -out Thawte_SGC_CA.crt.pem
openssl verify -CAfile Thawte_SGC_CA.crt.pem -purpose any gmail.cert
gmail.cert: OK



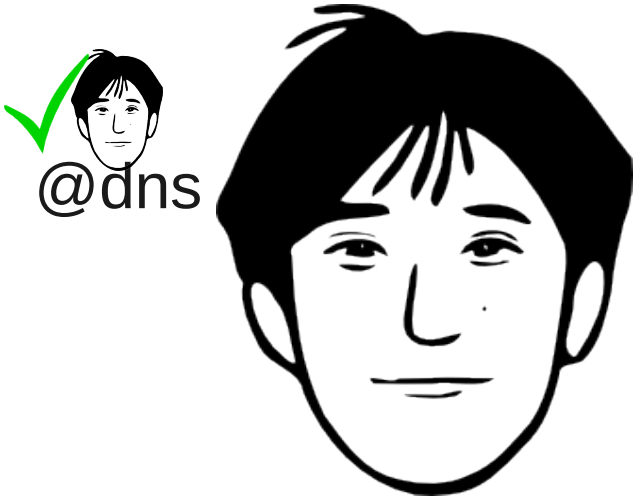
Chaine de confiance

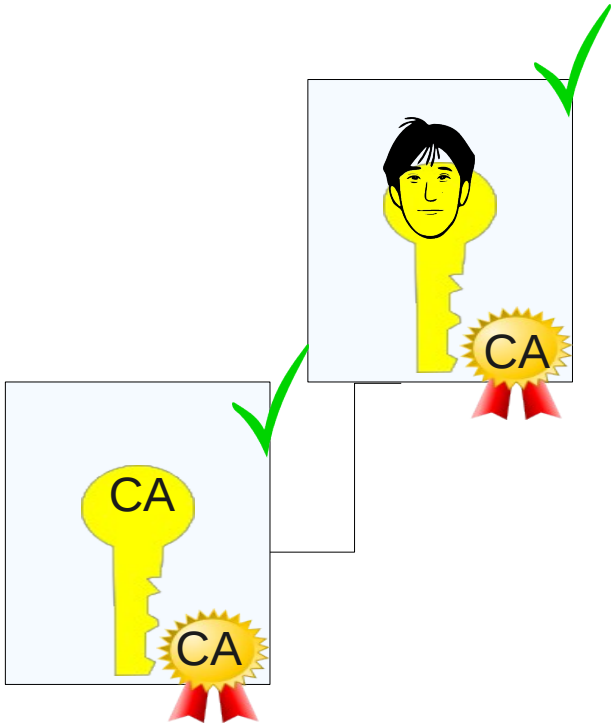




17	4.828095	2a00:1450:8006::12	[redacted]:39c0:26	TLSv1	Certificate
18	4.828148	[redacted]:39c0:26	2a00:1450:8006::12	TCP	35962 > https [ACK] Seq=165 Ack=1698 Win=105
19	4.850693	192.168.1.65	212.27.40.240	DNS	Standard query AAAA ocsp.thawte.com
20	4.879081	212.27.40.240	192.168.1.65	DNS	Standard query response CNAME ocsp.verisign.
21	4.879367	192.168.1.65	212.27.40.240	DNS	Standard query A ocsp.thawte.com
22	4.908173	212.27.40.240	192.168.1.65	DNS	Standard query response CNAME ocsp.verisign.
23	4.908625	192.168.1.65	199.7.48.72	TCP	39128 > http [SYN] Seq=0 Win=5840 Len=0 MSS=
24	5.044251	199.7.48.72	192.168.1.65	TCP	http > 39128 [SYN, ACK] Seq=0 Ack=1 Win=5792
25	5.044368	192.168.1.65	199.7.48.72	TCP	39128 > http [ACK] Seq=1 Ack=1 Win=5888 Len=
26	5.044605	192.168.1.65	199.7.48.72	OCSP	Request
27	5.185310	199.7.48.72	192.168.1.65	TCP	http > 39128 [ACK] Seq=1 Ack=582 Win=7040 Le
28	5.191066	199.7.48.72	192.168.1.65	OCSP	Response
29	5.191106	192.168.1.65	199.7.48.72	TCP	39128 > http [ACK] Seq=582 Ack=1415 Win=8768
30	5.191161	199.7.48.72	192.168.1.65	TCP	http > 39128 [FIN, ACK] Seq=1415 Ack=582 Win
31	5.191614	192.168.1.65	199.7.48.72	TCP	39128 > http [FIN, ACK] Seq=582 Ack=1416 Win
32	5.267314	[redacted]:39c0:26	2a00:1450:8006::12	TLSv1	Client Key Exchange, Change Cipher Spec, Enc

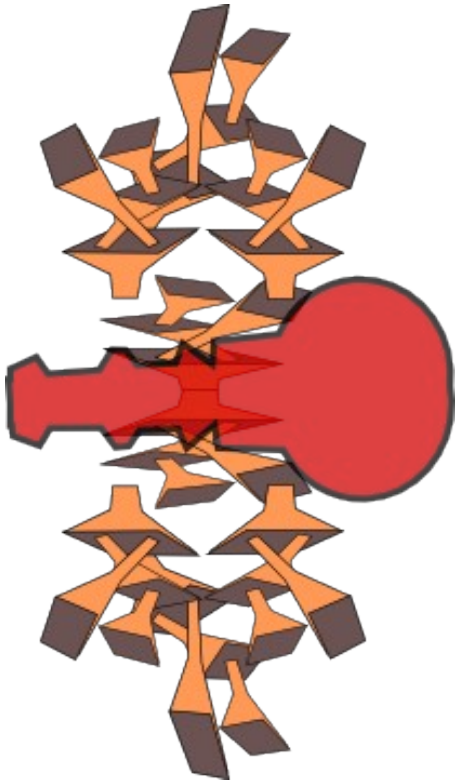
```
> Frame 17 (575 bytes on wire, 575 bytes captured)
> Ethernet II, Src: [redacted], Dst: [redacted]
> Internet Protocol Version 6
> Transmission Control Protocol, Src Port: https (443), Dst Port: 35962 (35962), Seq: 1209, Ack: 165, Len: 489
> [Reassembled TCP Segments (1631 bytes): #15(1151), #17(480)]
v Secure Socket Layer
  v TLSv1 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 1626
    v Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 1622
        Certificates Length: 1619
      > Certificates (1619 bytes)
v Secure Socket Layer
  v TLSv1 Record Layer: Handshake Protocol: Server Hello Done
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 4
    v Handshake Protocol: Server Hello Done
        Handshake Type: Server Hello Done (14)
        Length: 0
```

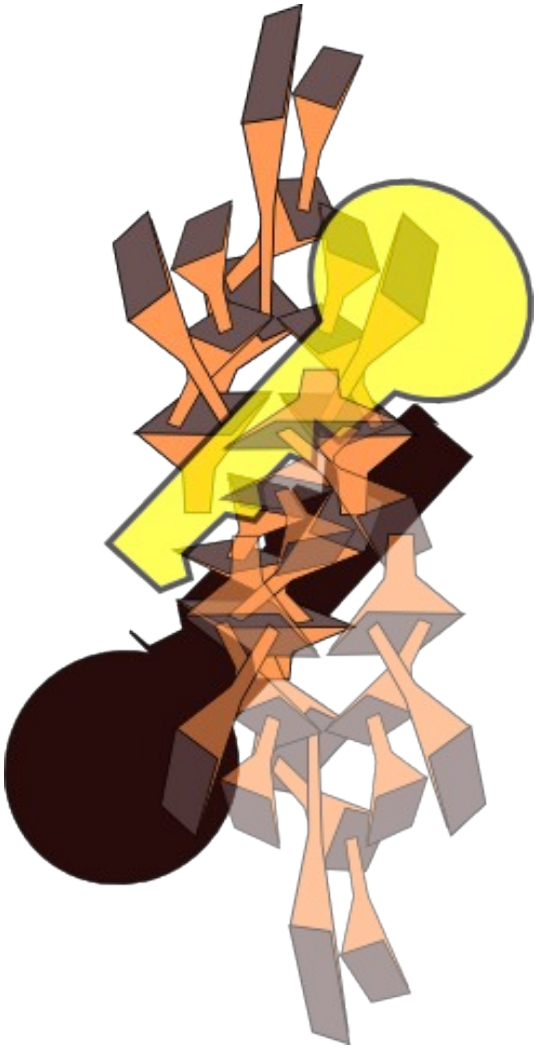

@dns


CA
CA

Echange de clés ... Pas si simple

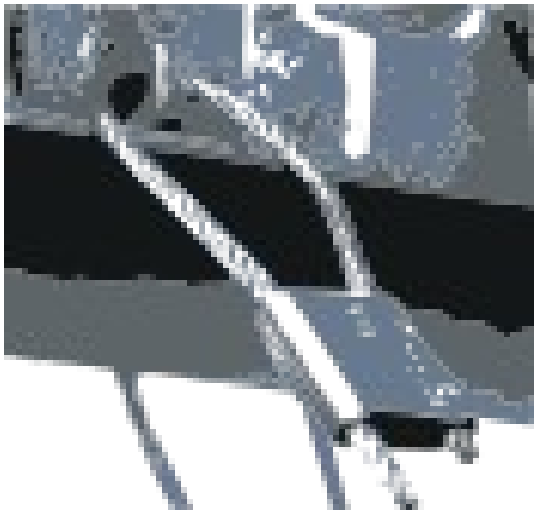
Matériel cryptographique





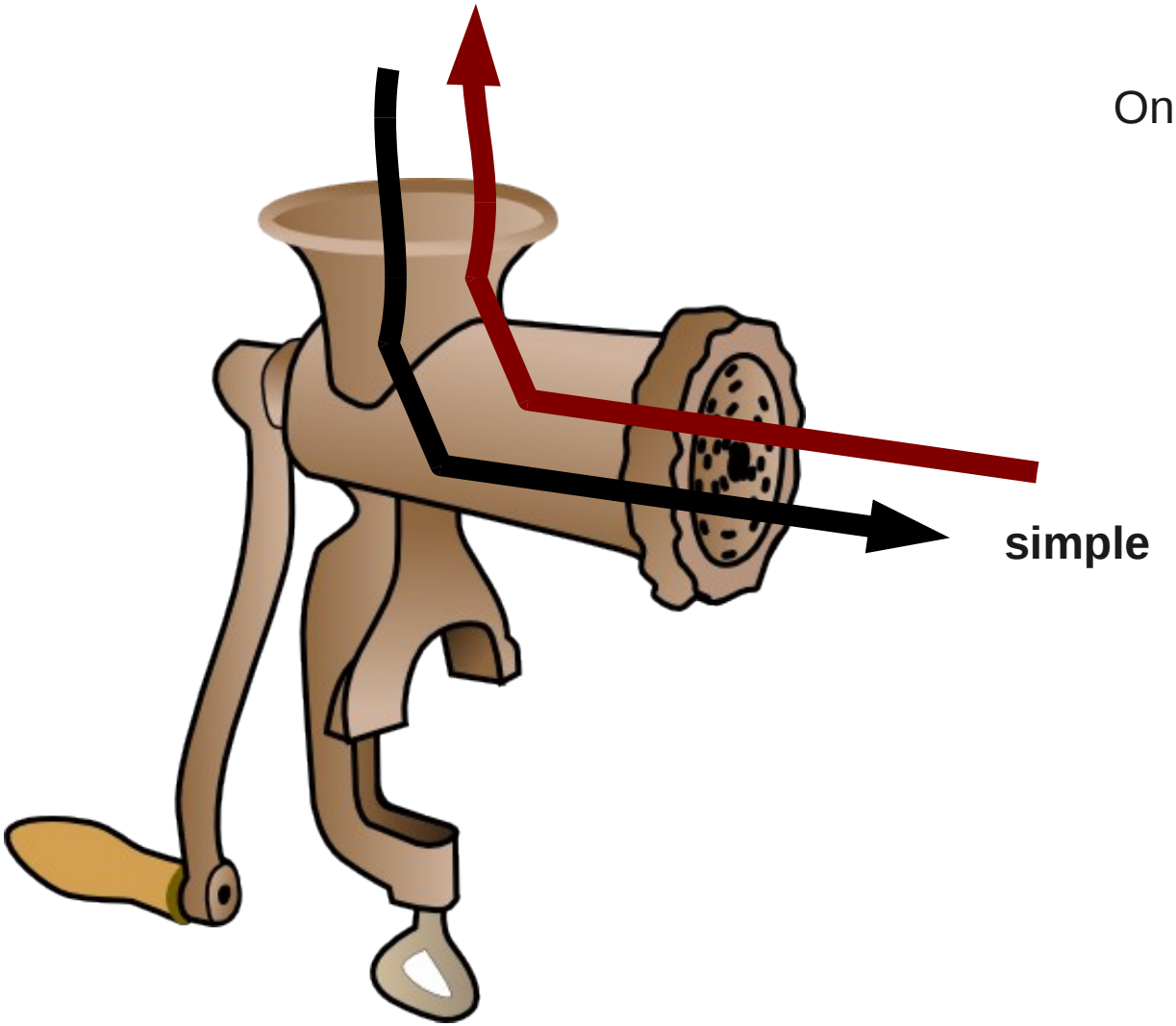
Fonctions de Hachage

- SHA256
- SHA1
- MD5



Irreversible

Extrêmement difficile / long



simple

One-Way function

Dispersif

Openssl sha1 -c <who.jpeg

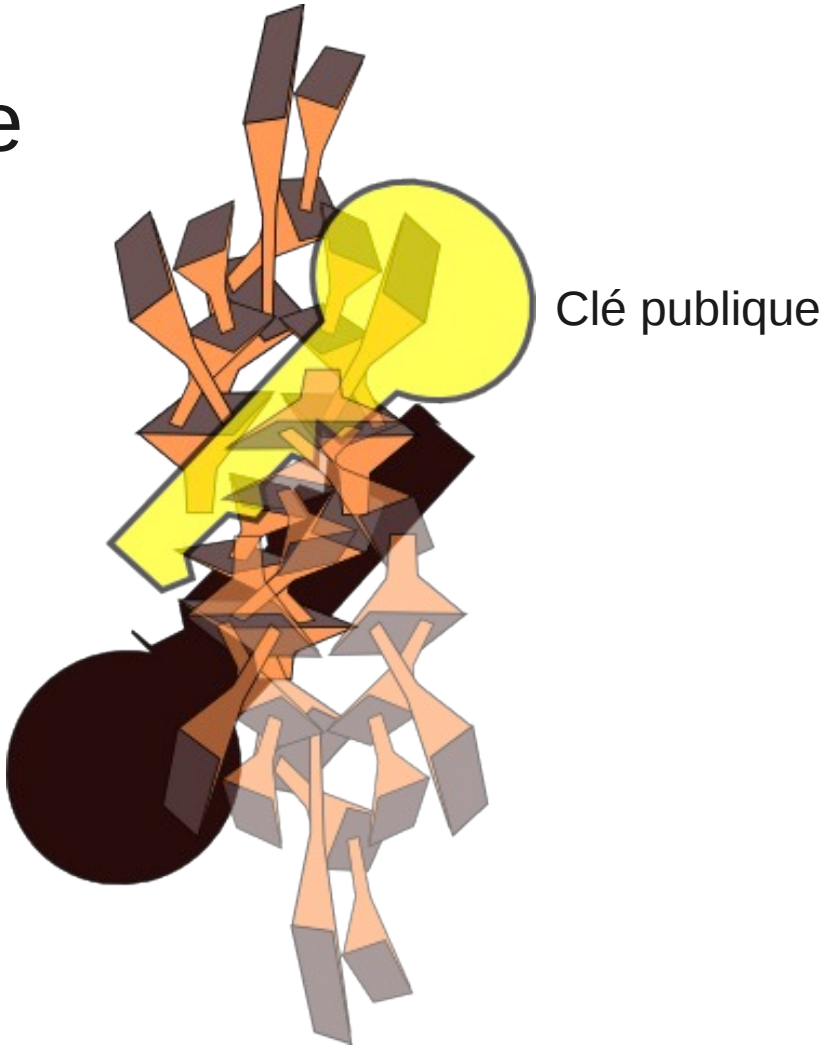
fa:45:5c:49:ac:
27:4f:b8:ee:d1:
8d:68:b5:4e:d9:
94:34:8f:a0:4c

Openssl sha1 -c <whodot.jpeg

12:d1:ce:26:5e:
50:d7:e9:e5:2d:
72:95:b9:0b:ac:
25:42:93:ee:9c

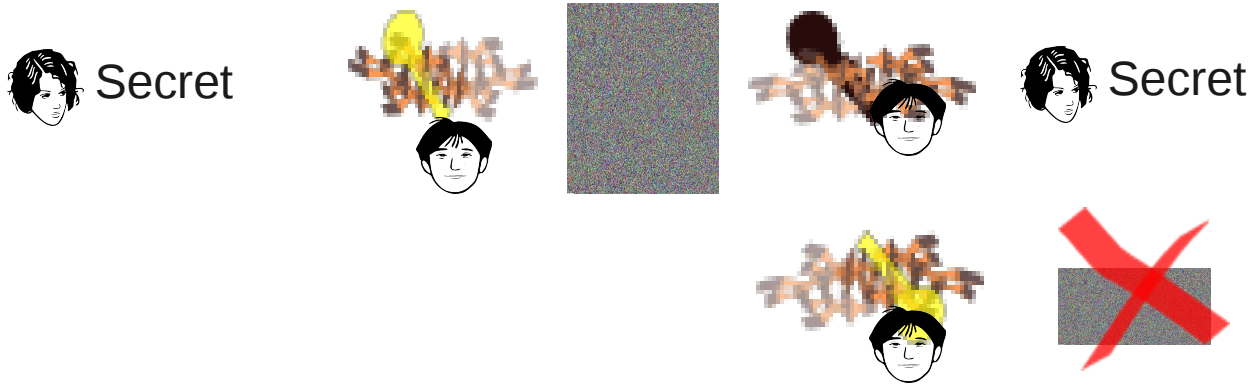
Crypto à clés asymétriques

- Crypto à clé publique
  - RSA
  - El Gamal
  - DSS/DSA
    - signature

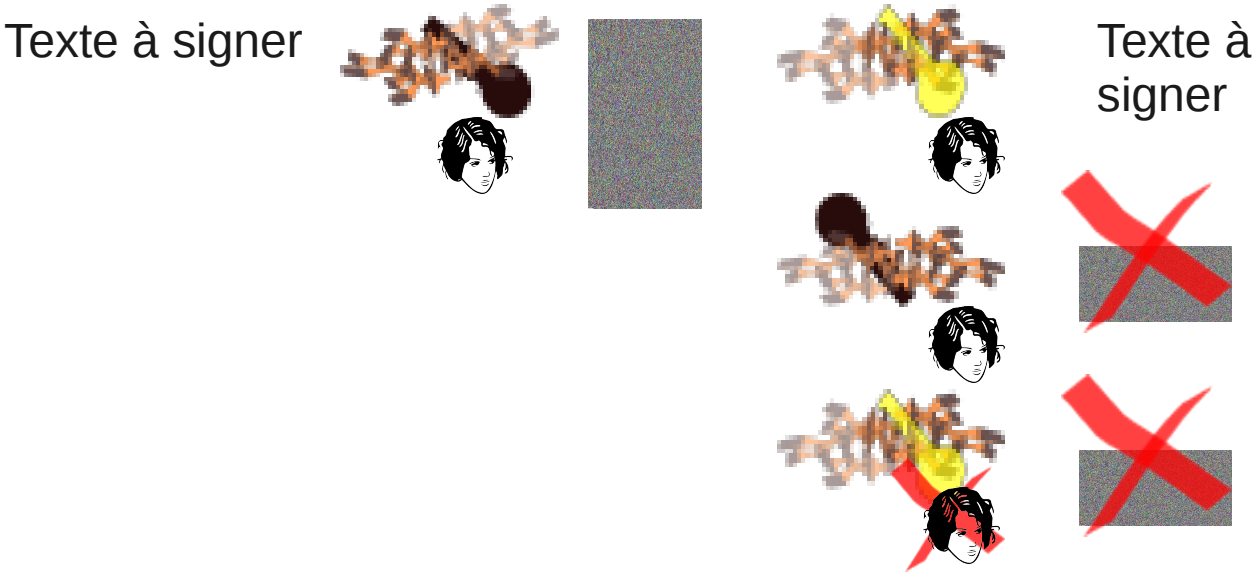


Utilisations

Chiffrement, échange de clefs



signature



RSA

openssl genrsa

```
Generating RSA private key, 512 bit long modulus
e is 65537 (0x10001)

-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAMBW/JaWqIoqAzouvlsqL4mlt4rc4JfOMfvs+8wUG0CljhFLIRzC
9AyWnEN2dKfNvcO23KRkC/pKOl1ZERDnP80CAwEAAQJBAL5WltoTN7CayNzQGzKu
eaK26v6xfFTeCZrsN3YKw7lhI59625lmordLyBVPzfzx0iNWcrTfgm89cJLxbxiG
KAECIQDw3K4OW/mDOa4nR3ia8CQ5jcTBPyLzrV7uRvVN/CEiAQIhAMxtnTkSdnoC
aVNqmjRX/jZu4v4lH0cIfGE3NhB6tQXNAiAsvfGfPTqWQ8q0BTTEI0O3ZTxdYWsO
tO/jd07uE53cAQIhAI+KNAg754a6JLyWsJoqYuxTpf0vkaut0K/uNX8SugLNAiBs
ef1pKItH+8rB/FgY9Bz7om344BFVFyOX/vjCl/NQLg==
-----END RSA PRIVATE KEY-----
```

$C \equiv M^e \pmod n$

$M \equiv C^d \pmod n$

openssl rsa -inform pem -in rsa.key -pubout

```
writing RSA key
-----BEGIN PUBLIC KEY-----
MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAN5caTj/aJ1EV44o+ba5bIlf9Ef7AsJ9
8EnAR7sTWhrpofzgzhHpt0kpD2kzNpZ4xdW3nYLaSMiQwCpvwSH1BJkCAwEAAQ==
-----END PUBLIC KEY-----
```

openssl rsa -text -inform pem -in rsa.pub -pubin

Modulus (512 bit):

00:de:5c:69:38:ff:68:9d:44:57:8e:28:f9:b6:b9:
6c:89:5f:f4:47:fb:02:c2:7d:f0:49:c0:47:bb:13:
5a:1a:e9:a1:fc:e0:ce:11:e9:b7:49:29:0f:69:33:
36:96:78:c5:d5:b7:9d:82:da:48:c8:90:c0:2a:6f:
c1:21:f5:04:99

Exponent: 65537 (0x10001)

openssl rsa -inform pem -text -in rsa.key

Private-Key: (512 bit)

modulus:

00:de:5c:69:38:ff:68:9d:44:57:8e:28:f9:b6:b9:
6c:89:5f:f4:47:fb:02:c2:7d:f0:49:c0:47:bb:13:
5a:1a:e9:a1:fc:e0:ce:11:e9:b7:49:29:0f:69:33:
36:96:78:c5:d5:b7:9d:82:da:48:c8:90:c0:2a:6f:
c1:21:f5:04:99

publicExponent: 65537 (0x10001)

privateExponent:

5e:85:05:ad:56:d4:4f:55:87:aa:44:3c:b1:b1:6c:
33:90:f8:33:c8:bd:49:93:63:1a:d6:83:27:40:78:
a2:cb:36:21:6a:74:1a:d7:d6:e7:0a:23:5f:fb:29:
24:32:bd:d8:fb:d1:5f:6a:af:24:be:53:c1:4c:5a:
9b:7a:39:21

prime1:

00:fa:2d:47:3e:86:32:a3:e5:24:0d:ec:3f:bb:e4:
3b:91:7c:40:57:63:6d:96:6b:3c:98:33:27:b7:49:
70:04:25

prime2:

00:e3:89:63:12:56:2d:87:bd:54:e0:75:c7:44:85:
65:45:26:7c:61:46:84:1b:38:b9:08:8f:4f:93:1e:
97:3a:65

exponent1:

7f:f6:02:d7:cf:2a:3d:bc:69:49:99:ca:2b:9f:9c:
7c:58:92:4c:60:75:e0:17:2f:a2:25:a0:2d:d6:a9:
2d:e5

exponent2:

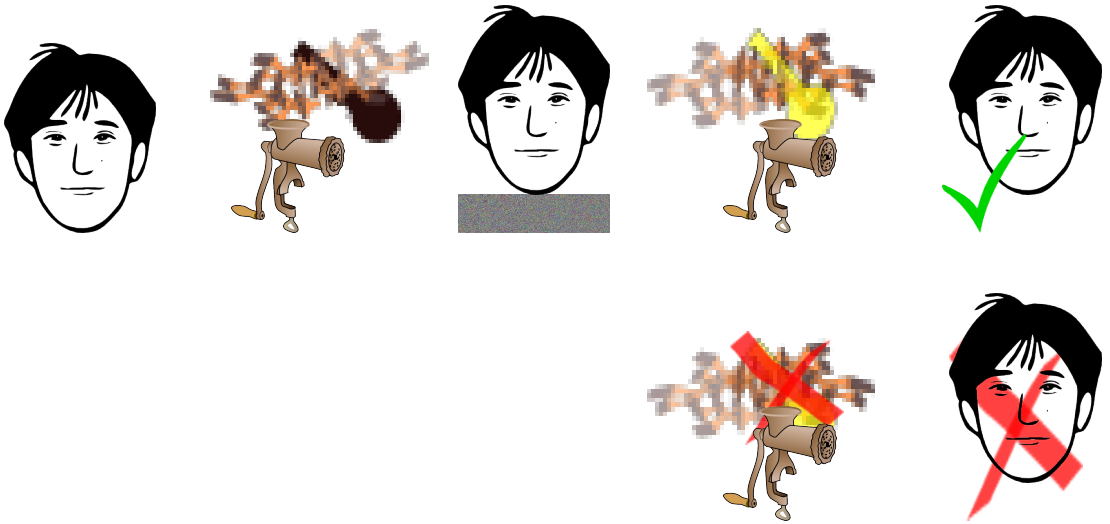
00:d4:be:34:1f:84:eb:f5:2a:95:1d:79:81:e3:13:
46:68:ad:5f:46:24:84:88:5f:34:c2:48:1c:82:d5:
eb:57:f1

coefficient:

00:a4:f0:22:13:4a:37:d6:c1:16:d2:8c:36:89:8b:
6e:76:df:cc:78:4a:4d:fd:c1:e6:9f:4b:72:f3:95:
45:f8:33

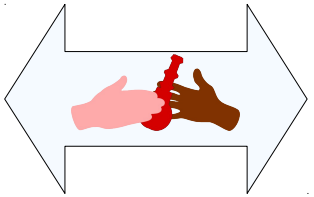
DSA

- Plus lent que RSA
- Uniquement pour vérifier les signatures

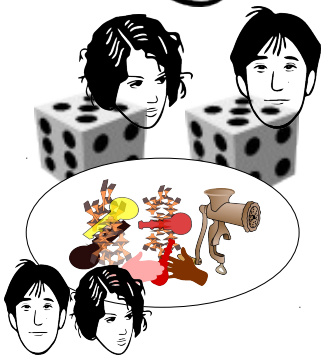


Diffie Hellman...

- Où comment fournir de la confidentialité anonyme
- Perfect Forward Secrecy
  - Une fois la clé de cryptage perdue il n'y a aucun moyen de relire le résulat.

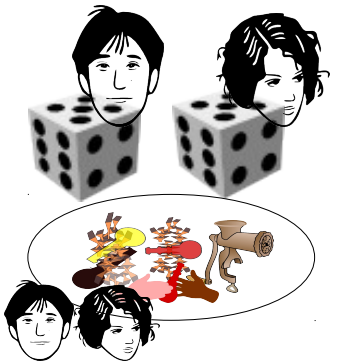


Handshake



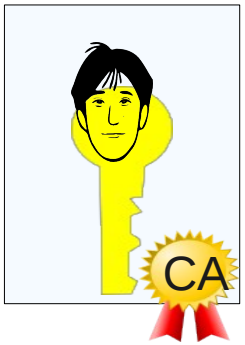
ClientHello

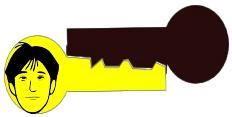
ServerHello

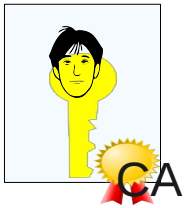


Certificate

ServerHelloDone

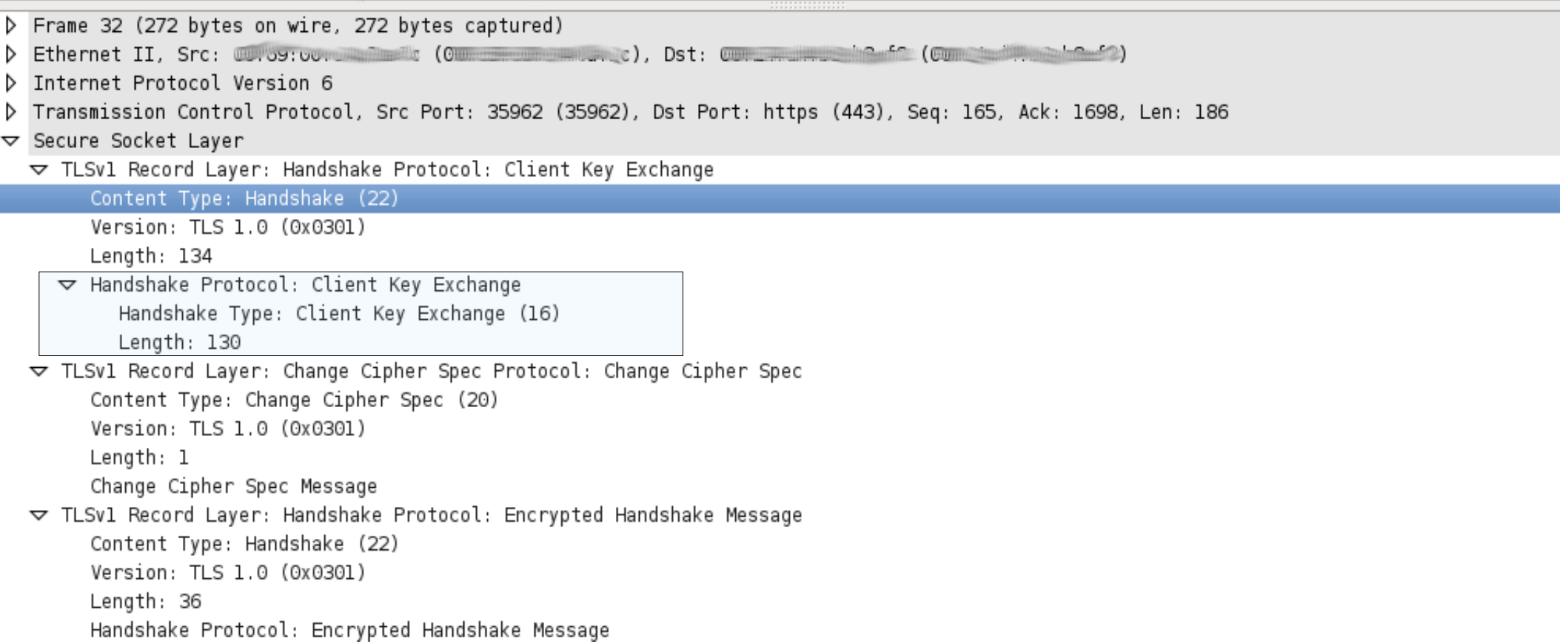




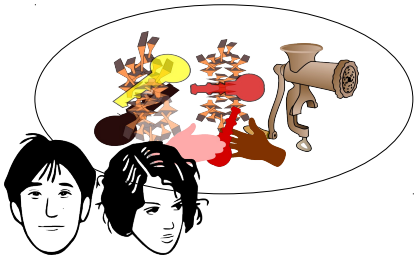


ClientKeyExchange

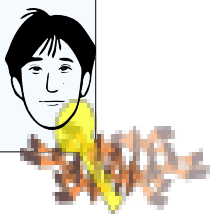

15 4.827461 :12 :39c0:26 TLSv1 Server Hello,
16 4.827533 :39c0:26 ::12 TCP 35962 > https [ACK] Seq=165 Ack=1209 Win=8128 Len=0 TSV=6723013 TSE
17 4.828095 :12 :39c0:26 TLSv1 Certificate
18 4.828148 :39c0:26 ::12 TCP 35962 > https [ACK] Seq=165 Ack=1698 Win=10560 Len=0 TSV=6723013 TSE
32 5.267314 :39c0:26 :12 TLSv1 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
33 5.315783 :12 :39c0:26 TLSv1 Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake
34 5.315899 :39c0:26 :8006::12 TCP 35962 > https [ACK] Seq=351 Ack=1924 Win=12928 Len=0 TSV=6723135 TSE
35 5.318266 :39c0:26 :8006::12 TLSv1 Application Data

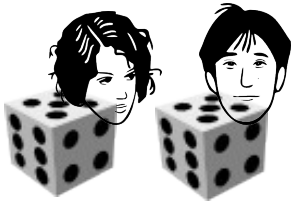

Frame 32 (272 bytes on wire, 272 bytes captured)
Ethernet II, Src:
Internet Protocol Version 6
Transmission Control Protocol, Src Port: 35962 (35962), Dst Port: https (443), Seq: 165, Ack: 1698, Len: 186
Secure Socket Layer
TLSv1 Record Layer: Handshake Protocol: Client Key Exchange
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 134
Handshake Protocol: Client Key Exchange
Handshake Type: Client Key Exchange (16)
Length: 130
TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
Content Type: Change Cipher Spec (20)
Version: TLS 1.0 (0x0301)
Length: 1
Change Cipher Spec Message
TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 36
Handshake Protocol: Encrypted Handshake Message

ClientKeyExchange

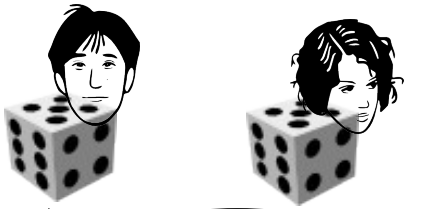


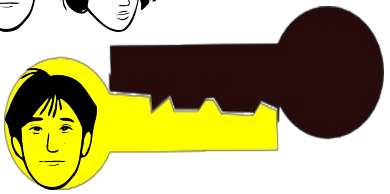
Pre master secret

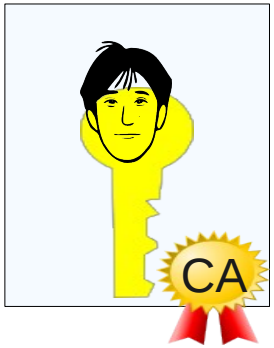




ClientKeyExchange

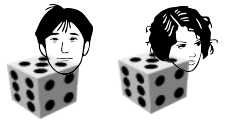


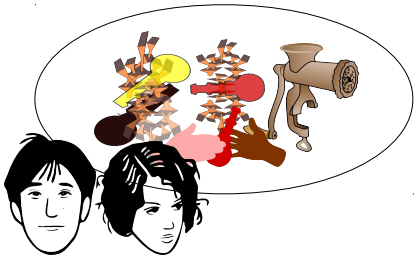




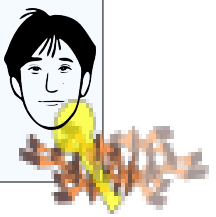
ClientKeyExchange

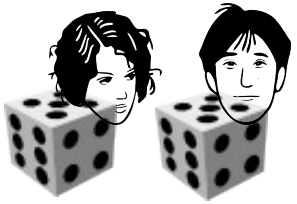
@dns

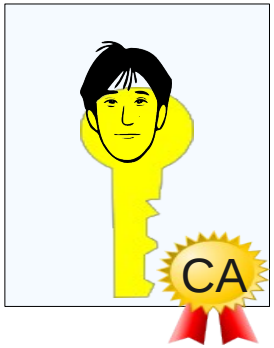


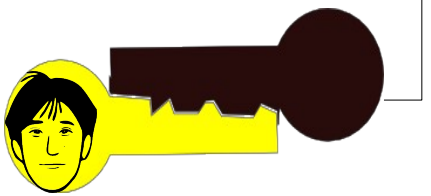


Pre master secret

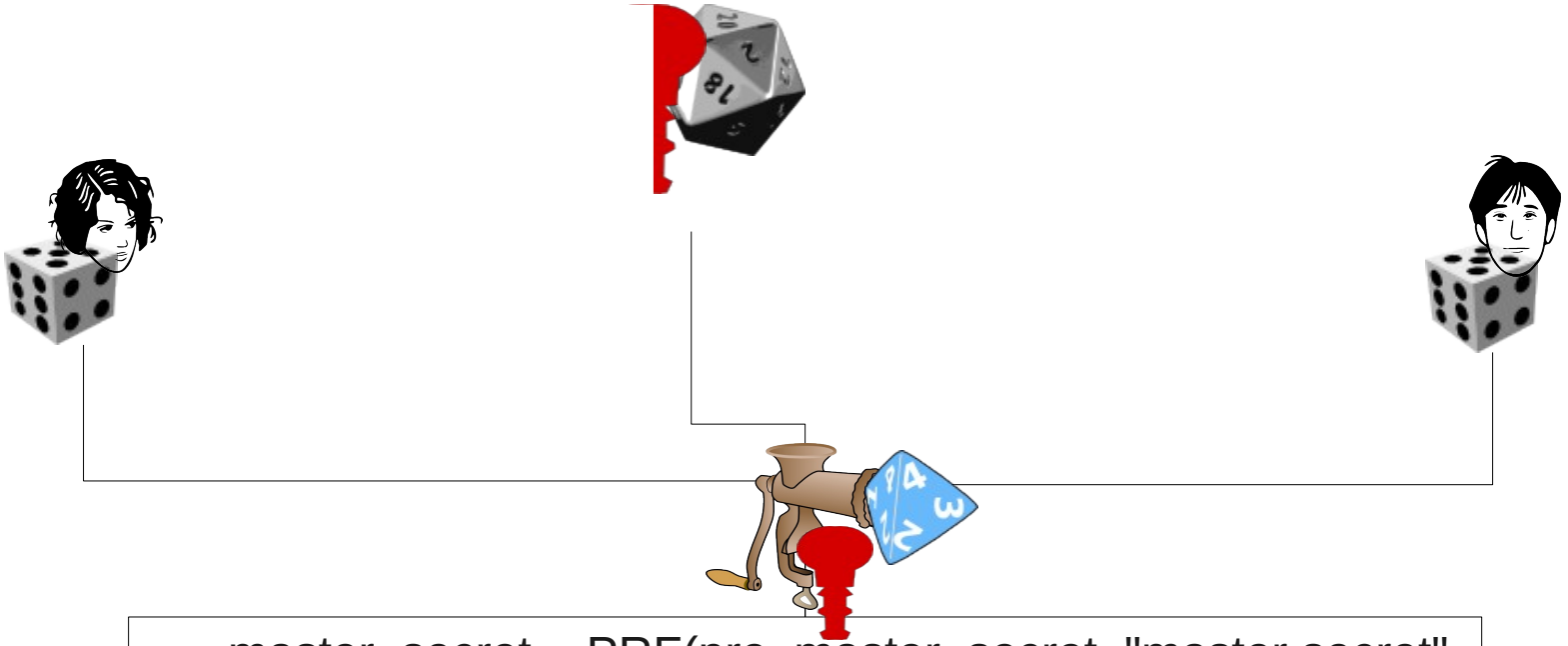








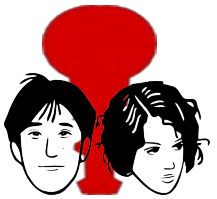
Pre-master Secret



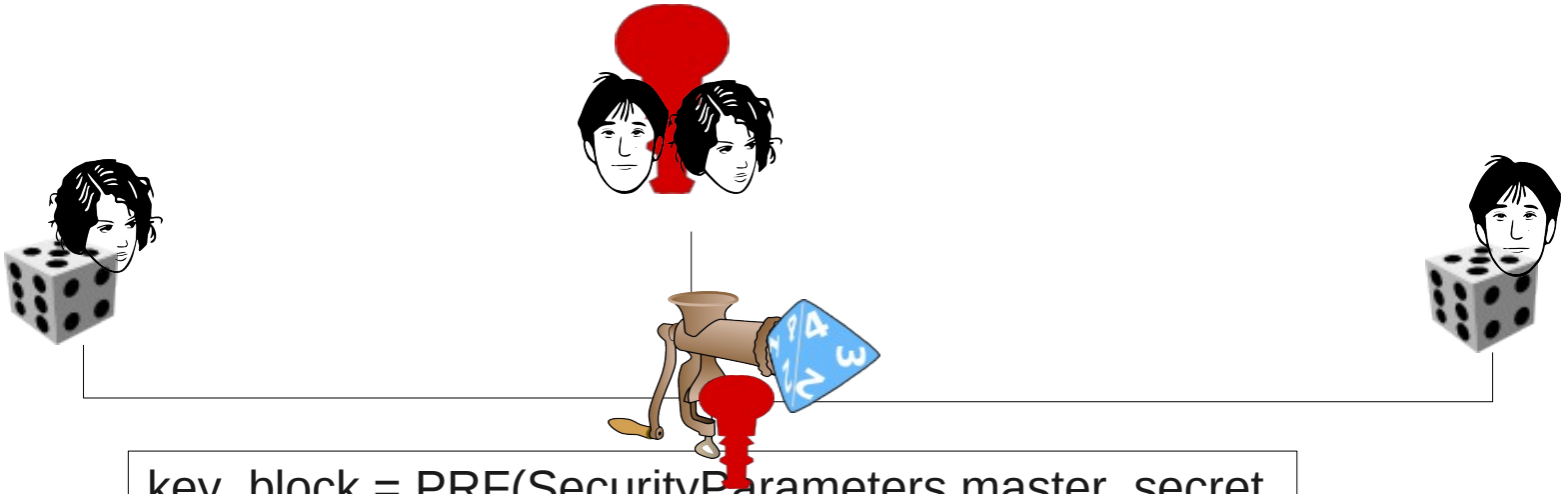
master_secret = PRF(pre_master_secret, "master secret",
ClientHello.random + ServerHello.random)
[0..47];

(*) différent pour SSLv3 qui n'utilise pas un HMAC

Master Secret

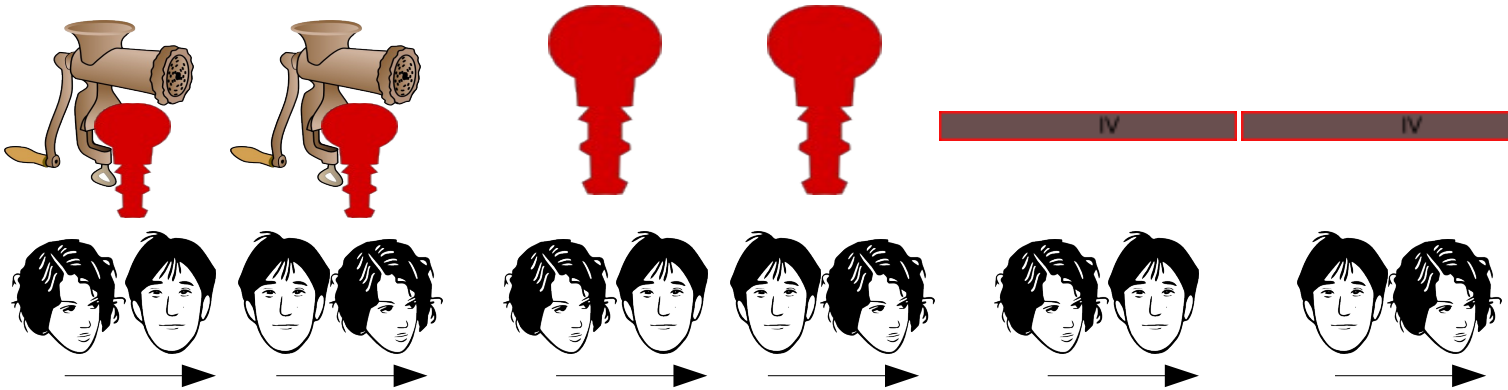


Master Secret



```
key_block = PRF(SecurityParameters.master_secret,
                "key expansion",
                SecurityParameters.server_random +
                SecurityParameters.client_random);
```

Key Block



PRF

TLS < 1.2 PRF P_MD5 xor P_SHA1

TLS = 1.2 PRF P_SHA256

PRF : Pseudo-Random Function

P_hash(secret, seed) = HMAC_hash(secret, A(1) + seed) + HMAC_hash(secret, A(2) + seed) +...

A(0) = seed
A(i) = HMAC_hash(secret, A(i-1))

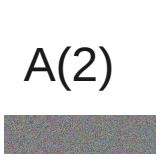
P_hash

A(0)

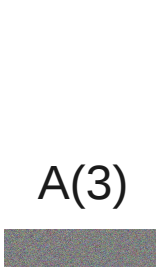
graine

A(1)

A(2)



A(3)



secret

HMAC (hash)

Hash :

MD5, SHA1, SHA256...

(...)

A(1)

graine

A(2)

graine

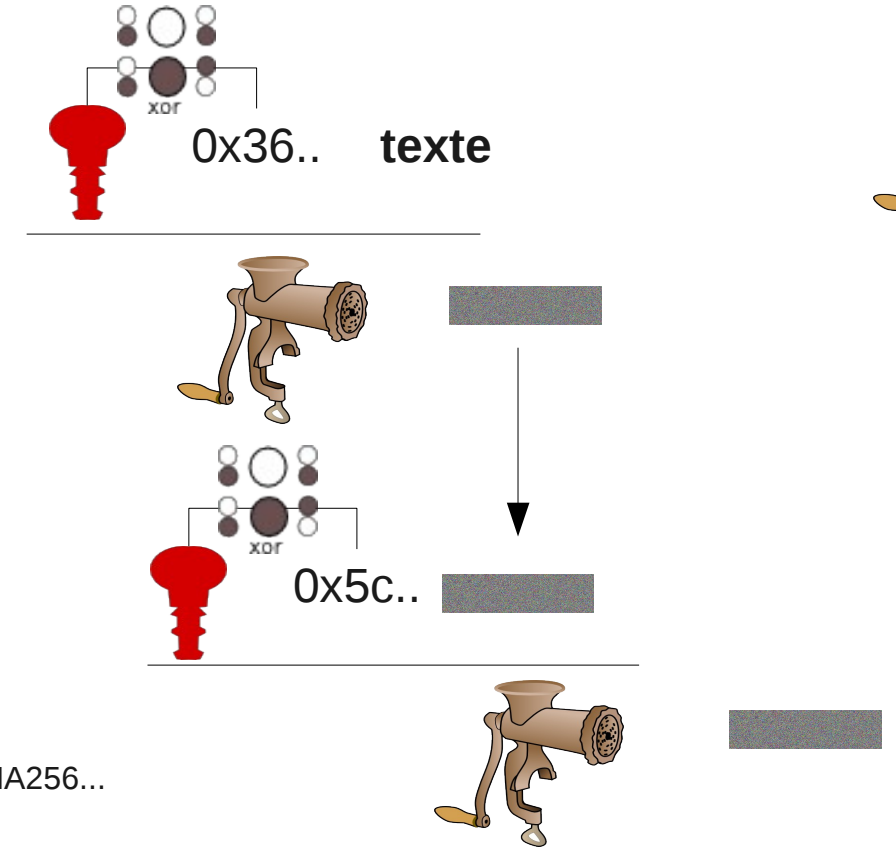
A(3)

graine

(...)

HMAC

http://tools.ietf.org/html/rfc2104



H(K XOR opad, H(K XOR ipad, text))

Frame 32 (272 bytes on wire, 272 bytes captured)

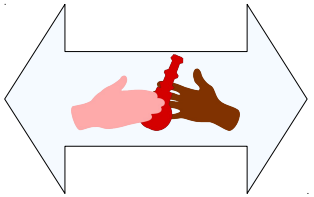
Ethernet II, Src: [redacted], Dst: [redacted]

Internet Protocol Version 6

Transmission Control Protocol, Src Port: 35962 (35962), Dst Port: https (443), Seq: 165, Ack: 1698, Len: 186

Secure Socket Layer

- TLSv1 Record Layer: Handshake Protocol: Client Key Exchange
  - Content Type: Handshake (22)
  - Version: TLS 1.0 (0x0301)
  - Length: 134
  - Handshake Protocol: Client Key Exchange
    - Handshake Type: Client Key Exchange (16)
    - Length: 130
- TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
  - Content Type: Change Cipher Spec (20)
  - Version: TLS 1.0 (0x0301)
  - Length: 1
  - Change Cipher Spec Message
- TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
  - Content Type: Handshake (22)
  - Version: TLS 1.0 (0x0301)
  - Length: 36
  - Handshake Protocol: Encrypted Handshake Message



Handshake

ClientHello

ServerHello

Certificate

ServerHelloDone

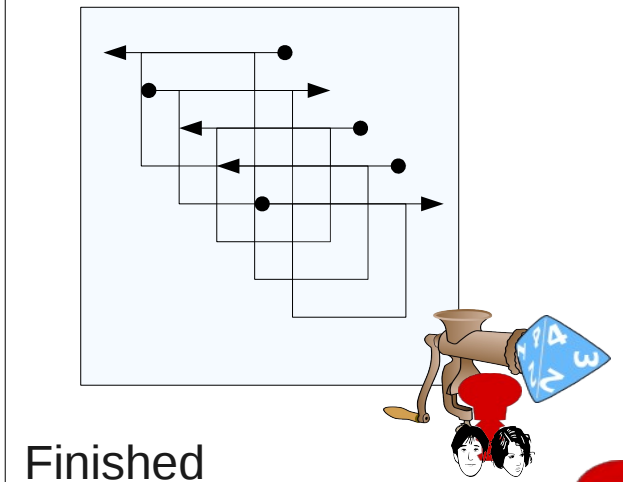
ClientKeyExchange

ChangeCipherSpec

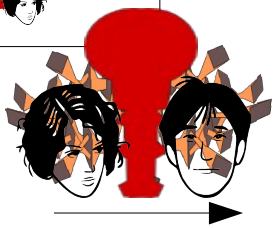
Finished

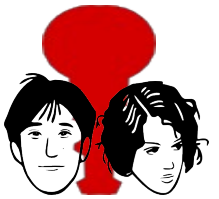
@dns

Finished

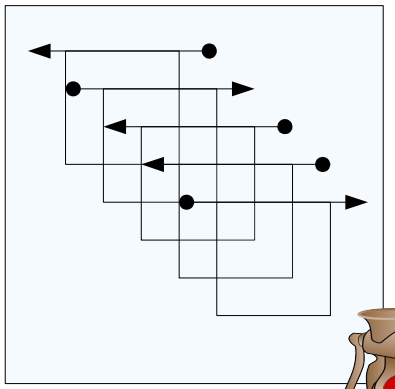


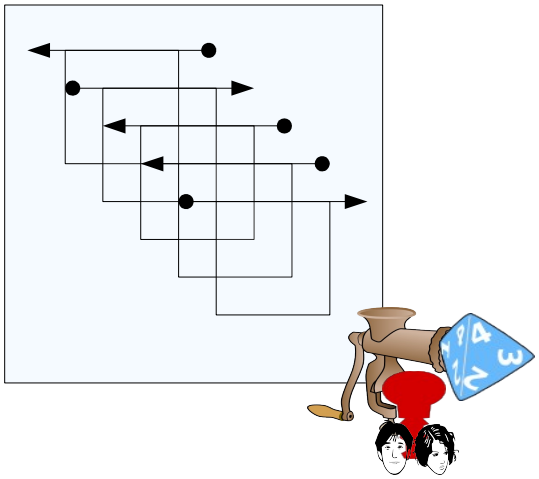
Finished



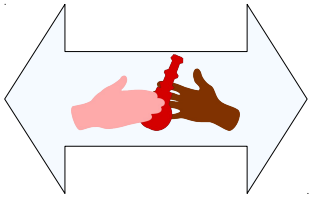


@dns





= ? :



Handshake

ClientHello

ServerHello

Certificate

ServerHelloDone

ClientKeyExchange

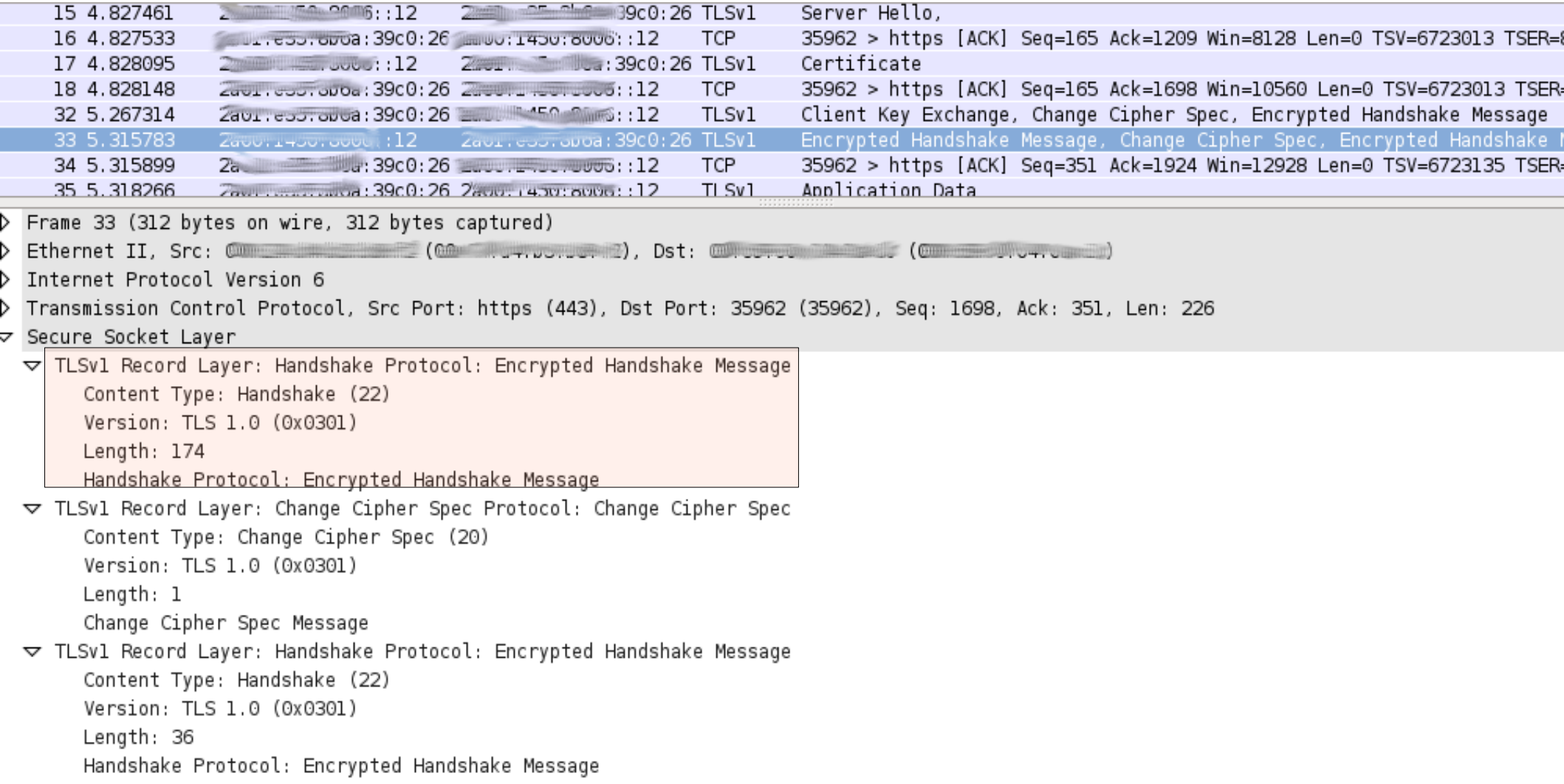
ChangeCipherSpec

Finished

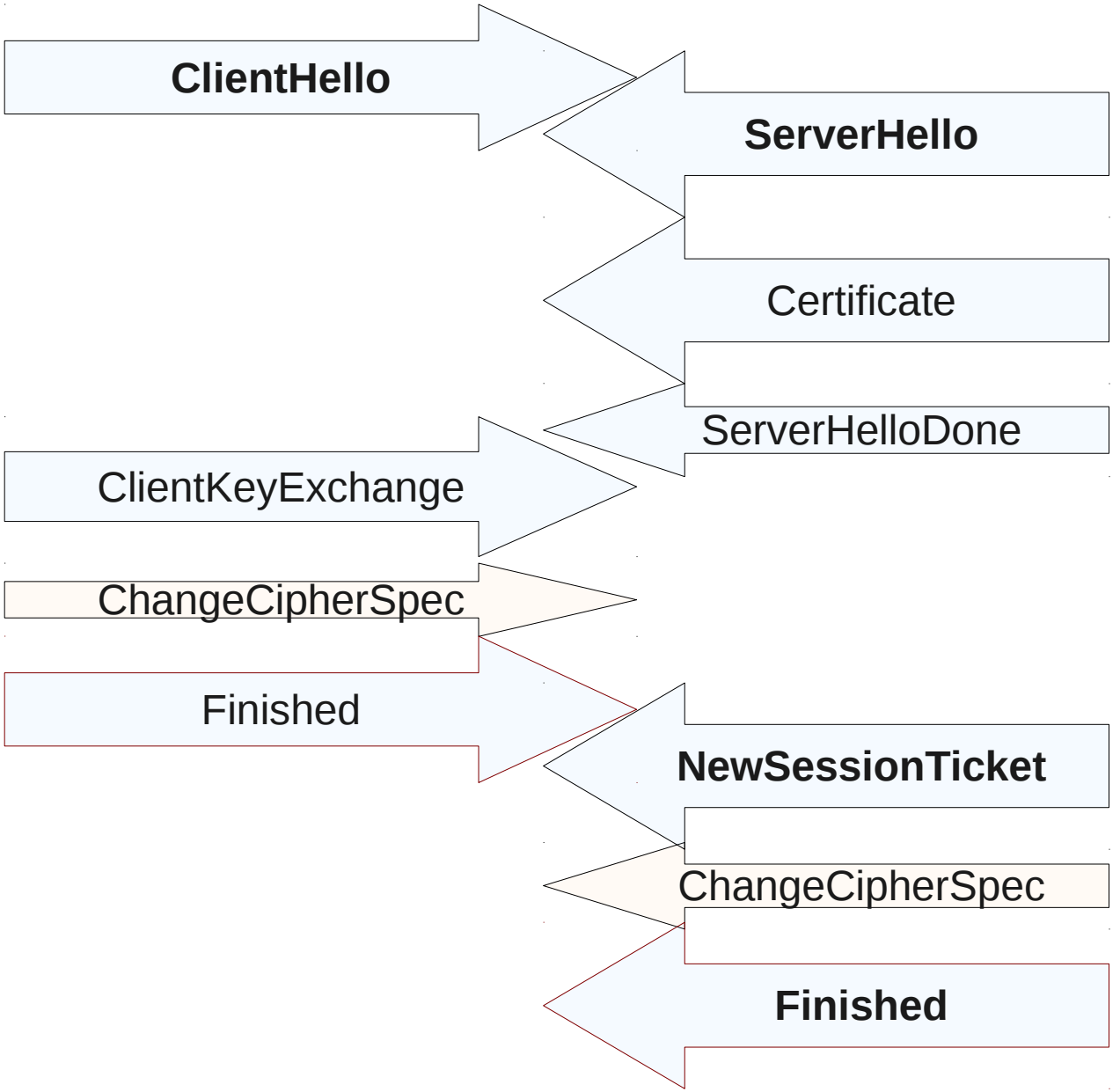
ChangeCipherSpec

Finished

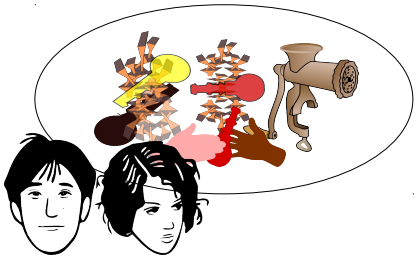
La réalité trahit la théorie ?

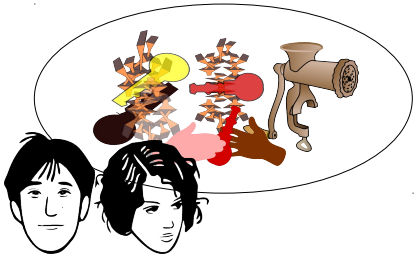


Session Ticket Extension



NewSessionTicket

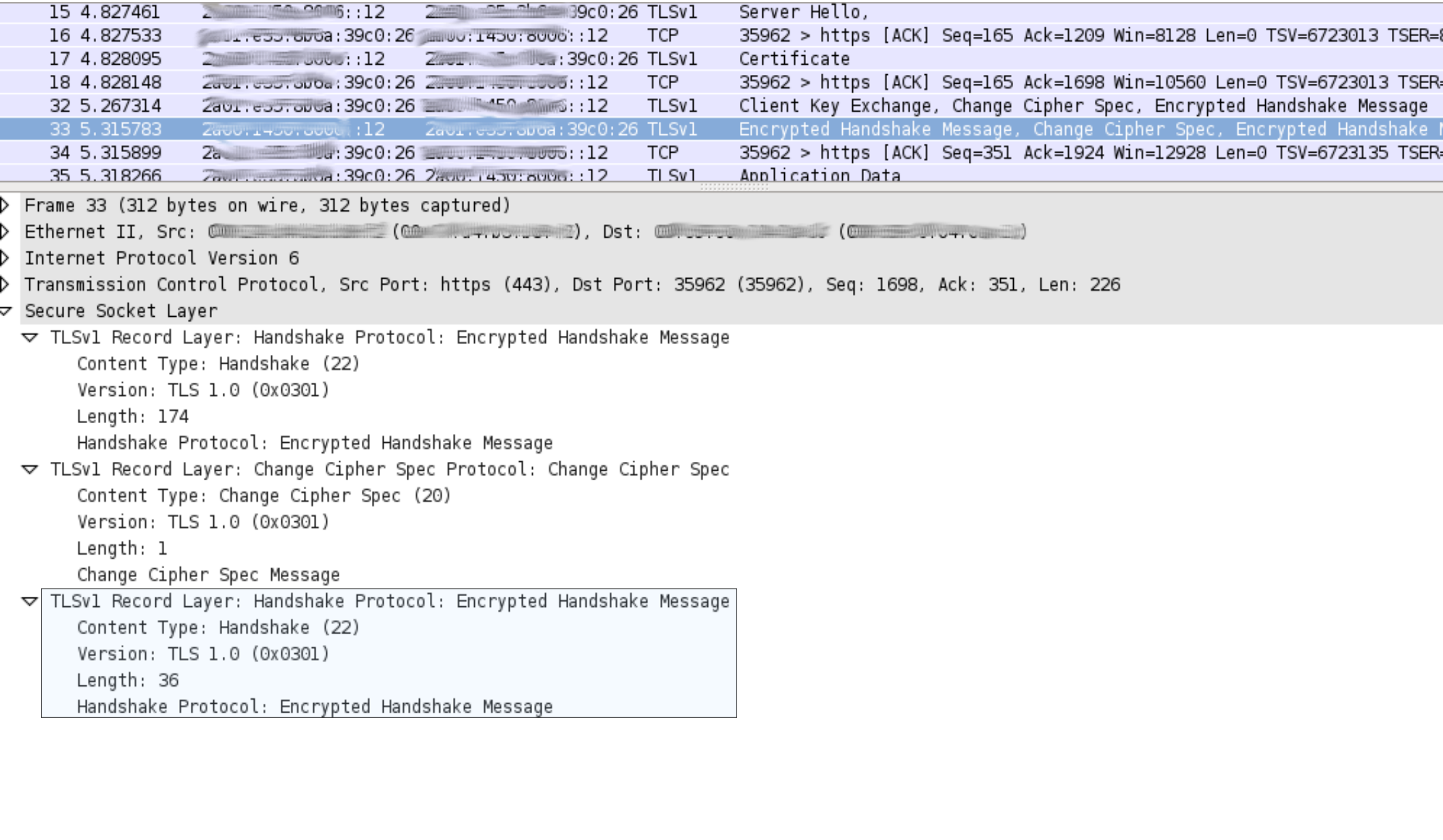




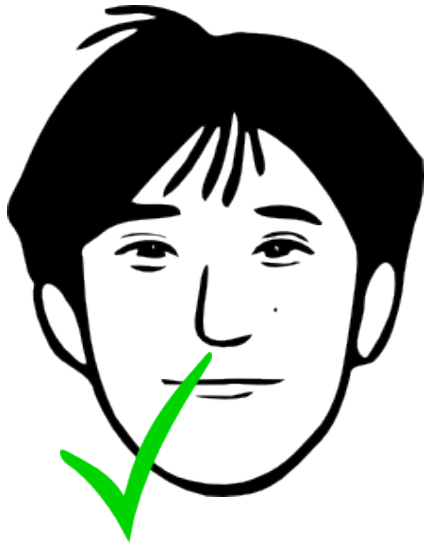
Durée de vie ticket

Ticket
(opaque)

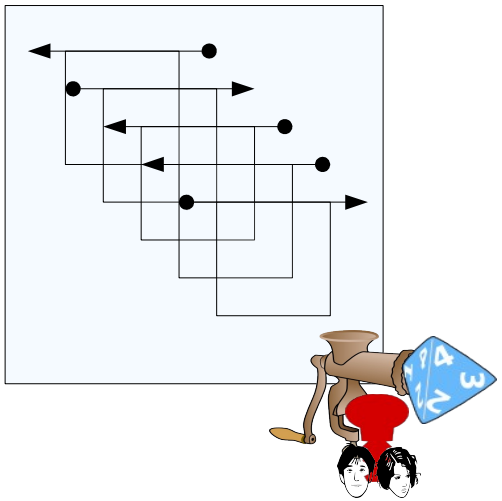
NewSessionTicket

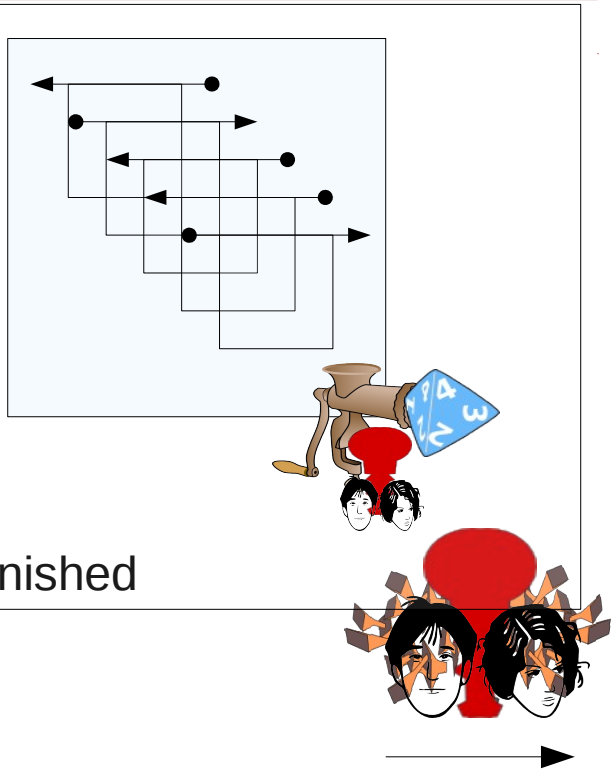

15 4.827461 TLSv1 Server Hello,
16 4.827533 TCP 35962 > https [ACK] Seq=165 Ack=1209 Win=8128 Len=0 TSV=6723013 TSER=
17 4.828095 TLSv1 Certificate
18 4.828148 TCP 35962 > https [ACK] Seq=165 Ack=1698 Win=10560 Len=0 TSV=6723013 TSER=
32 5.267314 TLSv1 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
33 5.315783 TLSv1 Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake
34 5.315899 TCP 35962 > https [ACK] Seq=351 Ack=1924 Win=12928 Len=0 TSV=6723135 TSER=
35 5.318266 TLSv1 Application Data
Frame 33 (312 bytes on wire, 312 bytes captured)
Ethernet II, Src:
Dst:
Internet Protocol Version 6
Transmission Control Protocol, Src Port: https (443), Dst Port: 35962 (35962), Seq: 1698, Ack: 351, Len: 226
Secure Socket Layer
TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 174
Handshake Protocol: Encrypted Handshake Message
TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
Content Type: Change Cipher Spec (20)
Version: TLS 1.0 (0x0301)
Length: 1
Change Cipher Spec Message
TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 36
Handshake Protocol: Encrypted Handshake Message

@dns



Finished



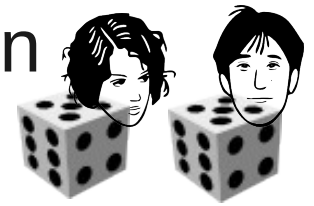


Finished

= ? :

Protection Replay-Attack

- Rejouer des paquets chiffrés sans posséder la clé.
- Pour s'en protéger on combine deux techniques :
  - Nonces : les paquets sont marqués avec un identifiant qui ne doit pas être réutilisé



  - Contrôle d'intégrité : on vérifie que le flux n'est pas altéré.

Hanshake Finished !

ClientHello

ServerHello

Certificate

ServerHelloDone

ClientKeyExchange

ChangeCipherSpec

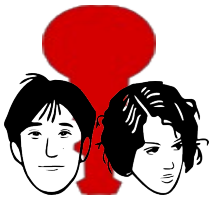
Finished

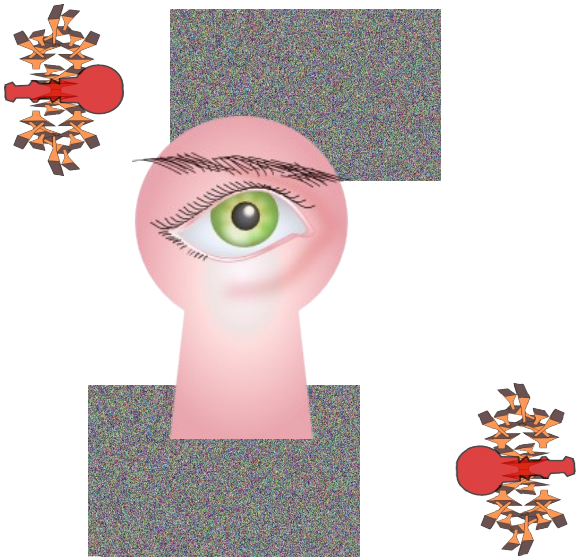
NewSessionTicket

ChangeCipherSpec

Finished

Ticket
(opaque)





Informations sur la page - https://mail.google.com/mail/?shva=1#inbox

Général | Médias | Flux | Permissions | Sécurité

Identité du site Web

Site Web : **mail.google.com**

Propriétaire : **Ce site Web ne fournit pas d'informations concernant son identité.**

Vérifiée par : **Thawte Consulting (Pty) Ltd.**

Ce site Web fournit un certificat pour vérifier son identité. [Afficher le certificat]

Vie privée et historique

Ai-je déjà visité ce site Web auparavant ? **Oui, 1 289 fois**

Ce site Web collecte-t-il des informations (cookies) sur mon ordinateur ? **Oui** [Voir les cookies]

Ai-je un mot de passe enregistré pour ce site Web ? **Non** [Voir les mots de passe enregistrés]

Détails techniques

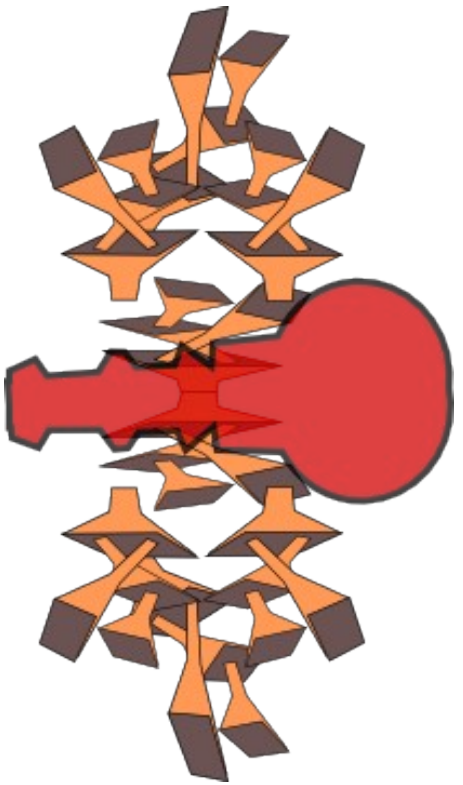
Connexion chiffrée : chiffrement de haut niveau (RC4 128 bit)

La page que vous voyez a été chiffrée avant sa transmission sur Internet.

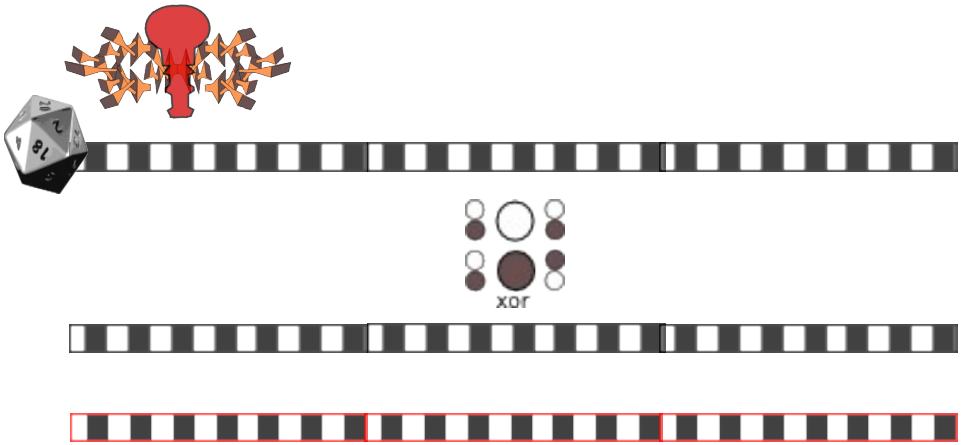
Le chiffrement rend très difficile aux personnes non autorisées la visualisation de la page durant son transit entre ordinateurs. Il est donc très improbable que quelqu'un puisse lire cette page durant son transit sur le réseau.

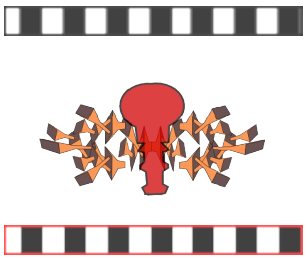
Crypto Symétrique

- 3DES : bloc
- AES (Rijndael) : bloc
- RC4 : flot

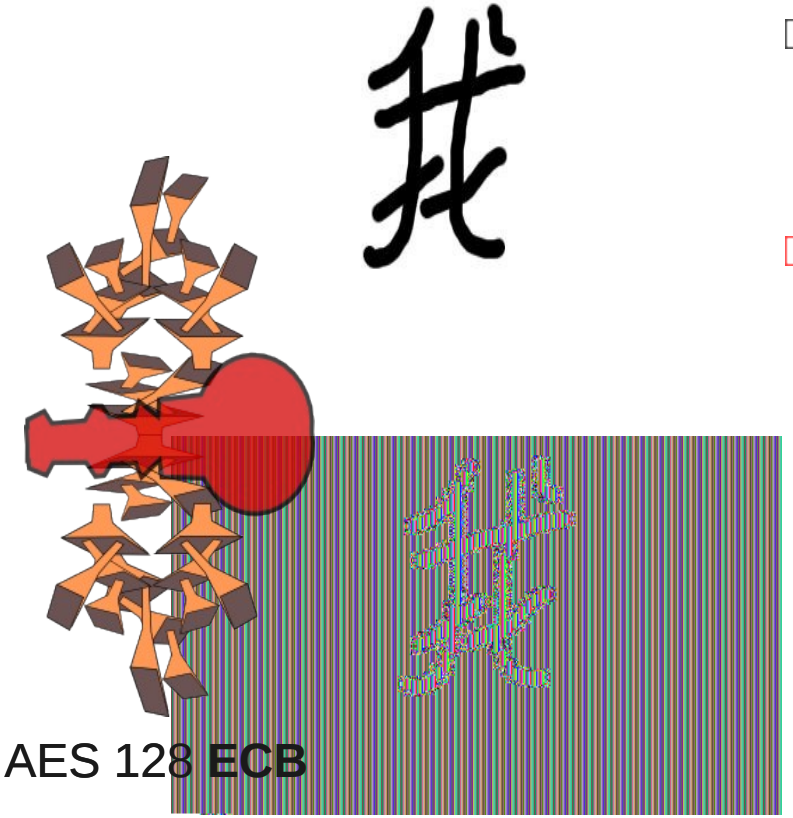


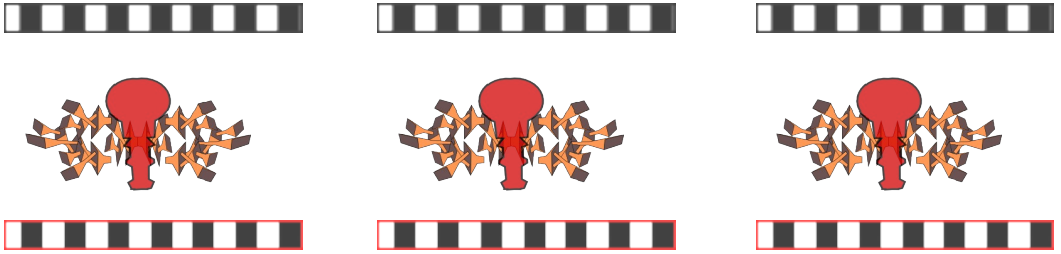
Flot ou Bloc





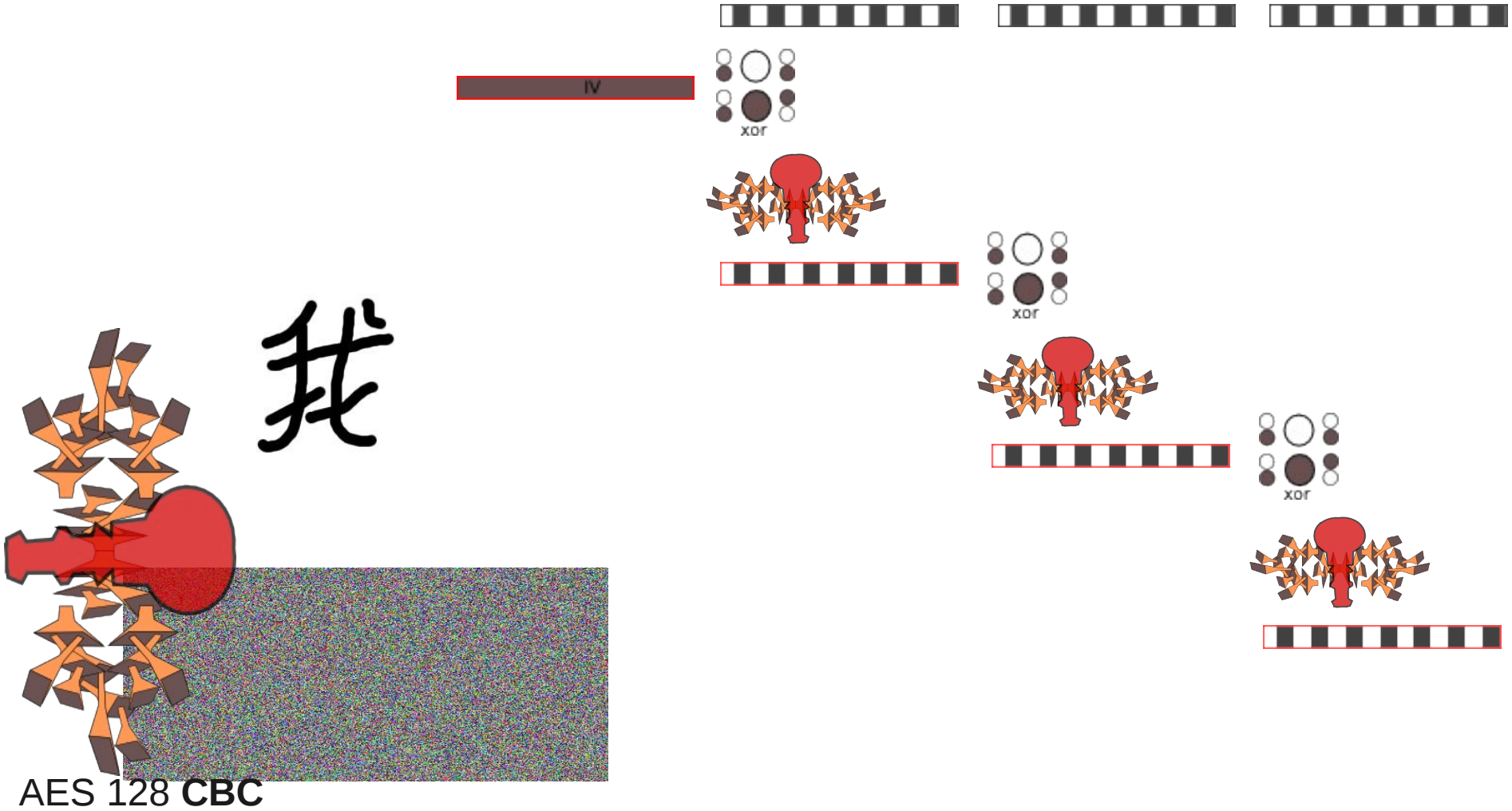
Electronic Codebook ECB





Openssl aes-128-ecb -e -in who.bmp -out whoaes.bmp -k password

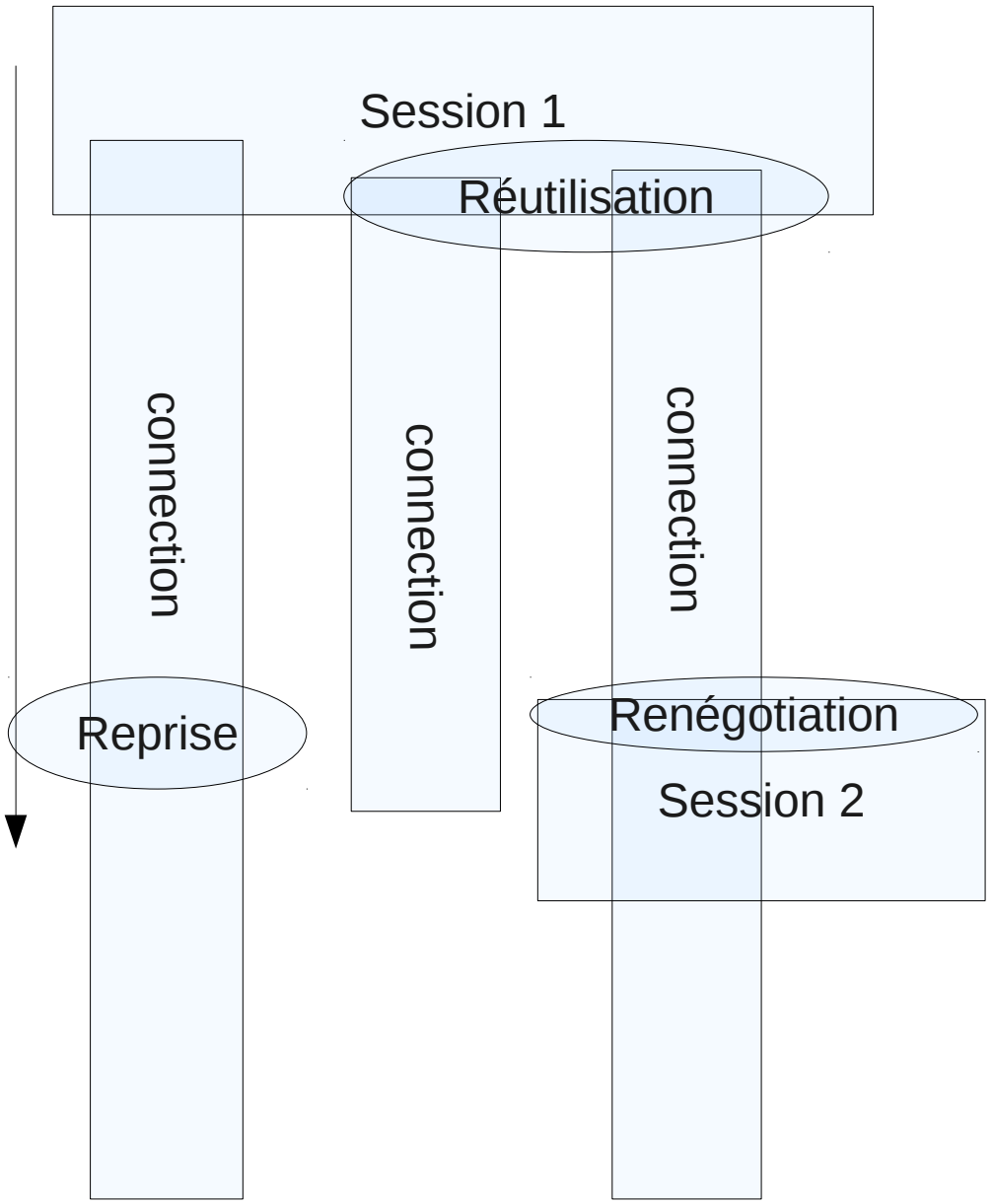
Cipher Block Chaining CBC



AES 128 **CBC**

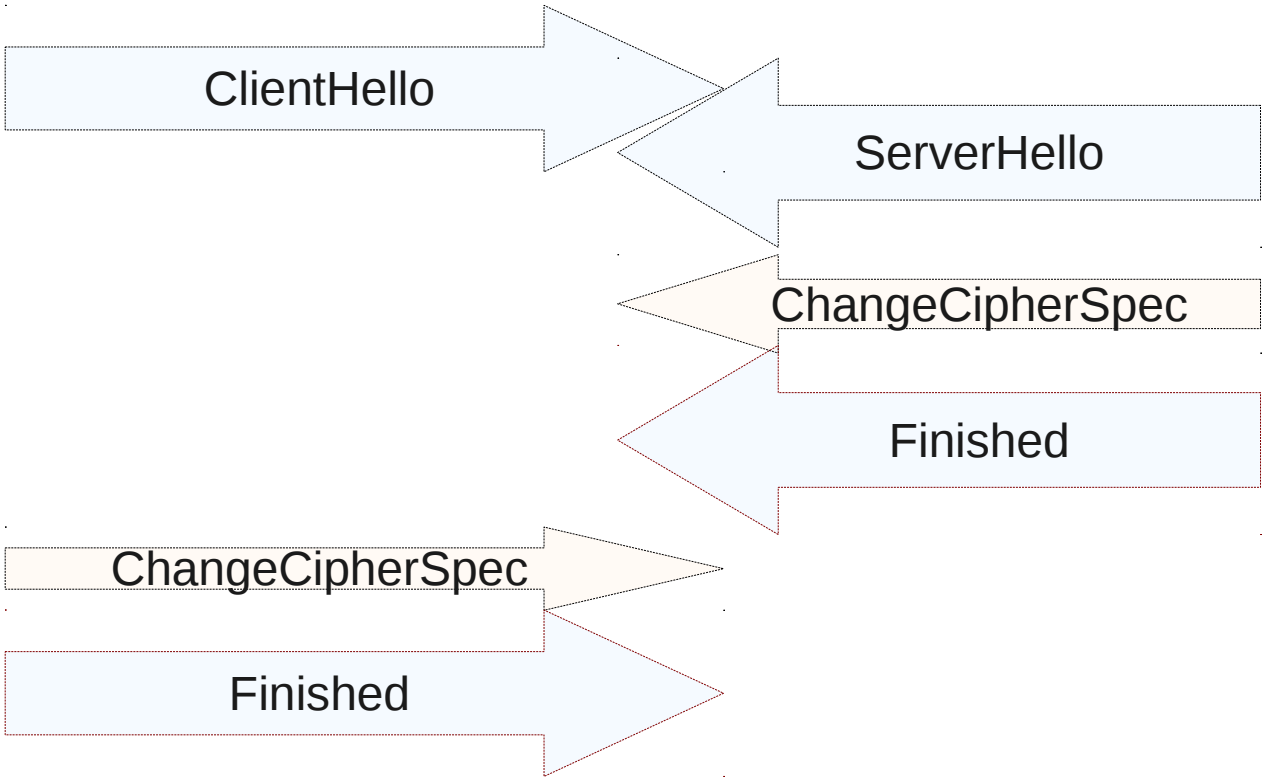
Openssl aes-128-cbc -e -in who.bmp -out whoaes.bmp -k password

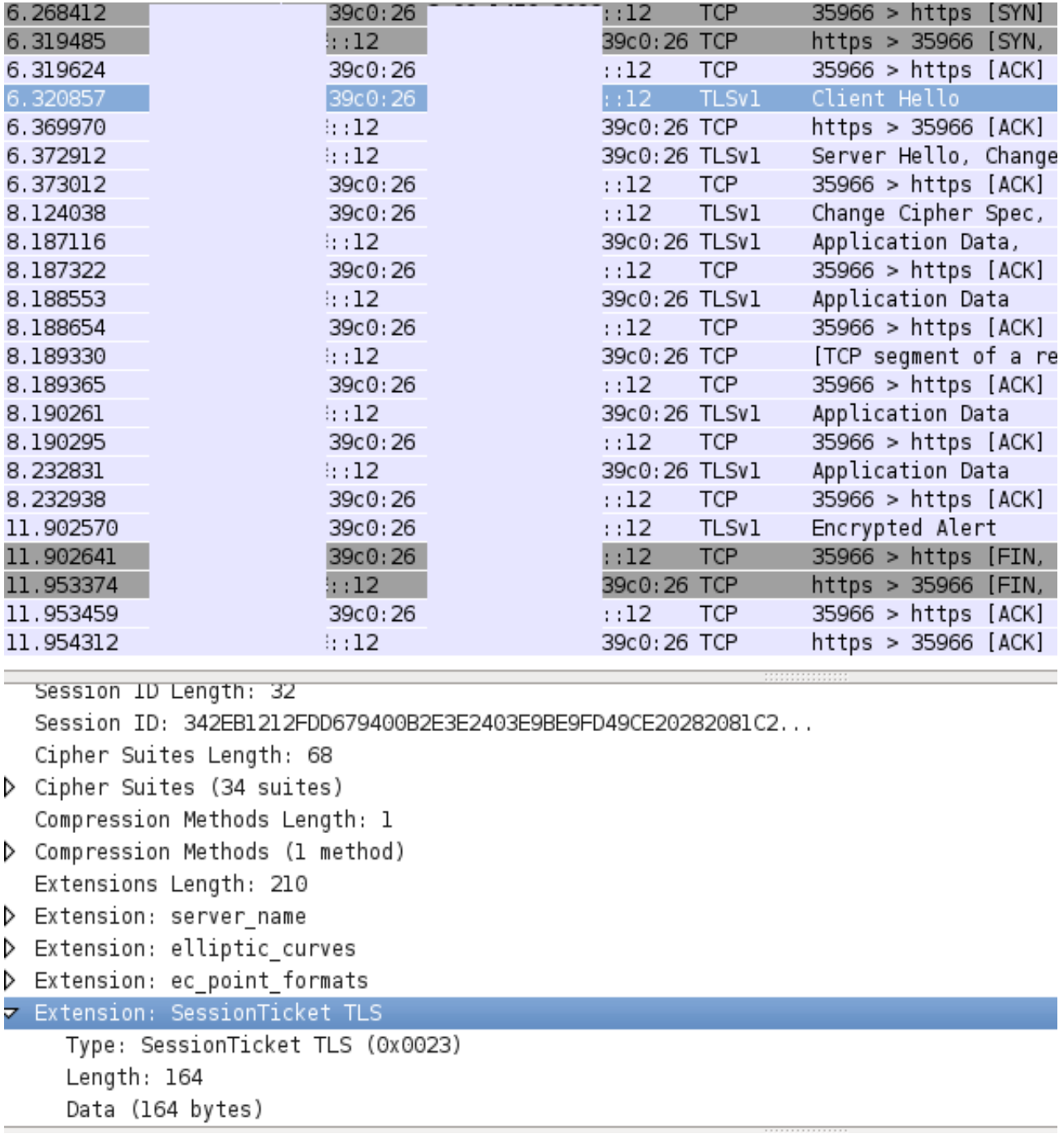
Session



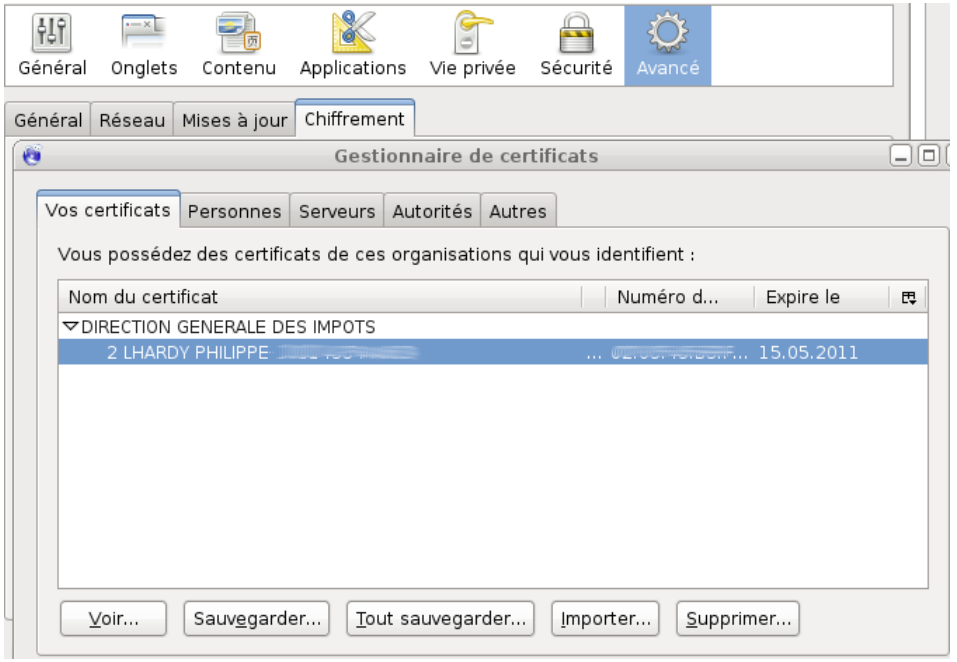

```
struct {
      ProtocolVersion protocol_version;
      CipherSuite cipher_suite;
      CompressionMethod compression_method;
      opaque master_secret[48];
      ClientIdentity client_identity;
      uint32 timestamp;
  } StatePlaintext;

  enum {
     anonymous(0),
     certificate_based(1),
     psk(2)
  } ClientAuthenticationType;

  struct {
      ClientAuthenticationType client_authentication_type;
      select (ClientAuthenticationType) {
          case anonymous: struct {};
          case certificate_based:
              ASN.1Cert certificate_list<0..2^24-1>;
          case psk:
              opaque psk_identity<0..2^16-1>;   /* from [RFC4279] */
      };
   } ClientIdentity;
```

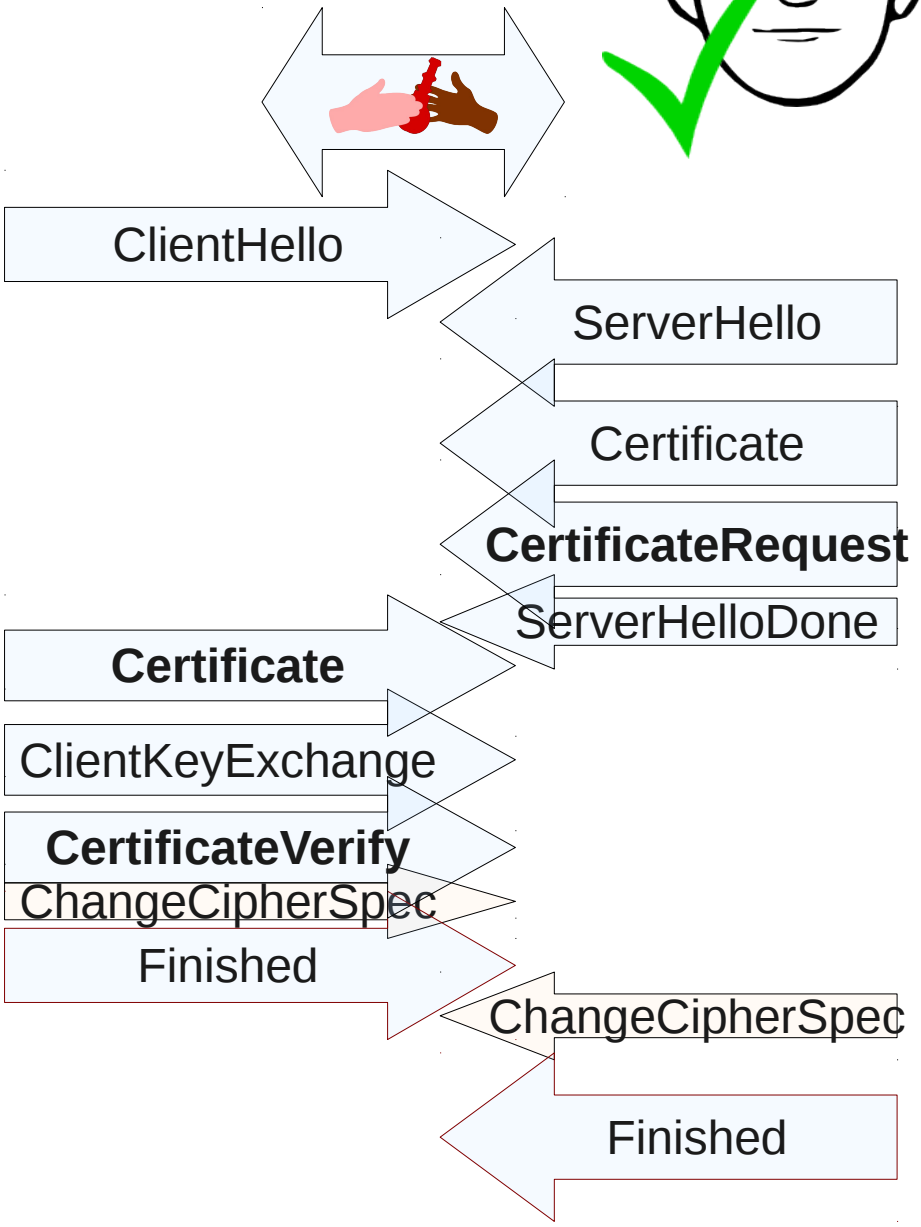
Réutilisation ou reprise de session




6.268412 39c0:26 ::12 TCP 35966 > https [SYN]
6.319485 ::12 39c0:26 TCP https > 35966 [SYN,
6.319624 39c0:26 ::12 TCP 35966 > https [ACK]
6.320857 39c0:26 ::12 TLSv1 Client Hello
6.369970 ::12 39c0:26 TCP https > 35966 [ACK]
6.372912 ::12 39c0:26 TLSv1 Server Hello, Change
6.373012 39c0:26 ::12 TCP 35966 > https [ACK]
8.124038 39c0:26 ::12 TLSv1 Change Cipher Spec,
8.187116 ::12 39c0:26 TLSv1 Application Data,
8.187322 39c0:26 ::12 TCP 35966 > https [ACK]
8.188553 ::12 39c0:26 TLSv1 Application Data
8.188654 39c0:26 ::12 TCP 35966 > https [ACK]
8.189330 ::12 39c0:26 TCP [TCP segment of a re
8.189365 39c0:26 ::12 TCP 35966 > https [ACK]
8.190261 ::12 39c0:26 TLSv1 Application Data
8.190295 39c0:26 ::12 TCP 35966 > https [ACK]
8.232831 ::12 39c0:26 TLSv1 Application Data
8.232938 39c0:26 ::12 TCP 35966 > https [ACK]
11.902570 39c0:26 ::12 TLSv1 Encrypted Alert
11.902641 39c0:26 ::12 TCP 35966 > https [FIN,
11.953374 ::12 39c0:26 TCP https > 35966 [FIN,
11.953459 39c0:26 ::12 TCP 35966 > https [ACK]
11.954312 ::12 39c0:26 TCP https > 35966 [ACK]
Session ID Length: 32
Session ID: 342EB1212FDD679400B2E3E2403E9BE9FD49CE20282081C2...
Cipher Suites Length: 68
Cipher Suites (34 suites)
Compression Methods Length: 1
Compression Methods (1 method)
Extensions Length: 210
Extension: server_name
Extension: elliptic_curves
Extension: ec_point_formats
Extension: SessionTicket TLS
Type: SessionTicket TLS (0x0023)
Length: 164
Data (164 bytes)

Identification Client





Autres Handshakes

- Le handshake est encore différent
- Diffie Hellman
- Kerberos
-
- Mais ce sera pour une autre présentation...

Ce qu'il faut retenir

- La sécurité fournie par TLS dépend de la façon dont l'application l'utilise.
- Avec RSA et sans Diffie Hellman c'est la clé privé du serveur qui protège tout. Un fois décrypté la clé... tout le trafic est en clair.
- La clé publique est dans tous les certificats, par contre la clé privée doit être protégée, par un mot de passe si possible voir mieux.
- Une autorité de certification doit faire autorité.

Implémentations

- NSS
  - **libnss3-1d : Ensemble de bibliothèques conçues pour supporter le développement multi-plates-formes d'applications clientes et serveurs sécurisées. Il supporte les certificats SSLv2 et v4, TLS, PKCS #5, #7, #11, #12, S/MIME, X.509 v3 et d'autres standards de sécurité.**
- OpenSSL
- GnuTls
  - GnuTls est l'implémentation GPL de TLS. OpenSSL a une licence BSD like qui n'est pas GPL.
- Java + BouncyCastle
- ... fermées, propriétaires ..

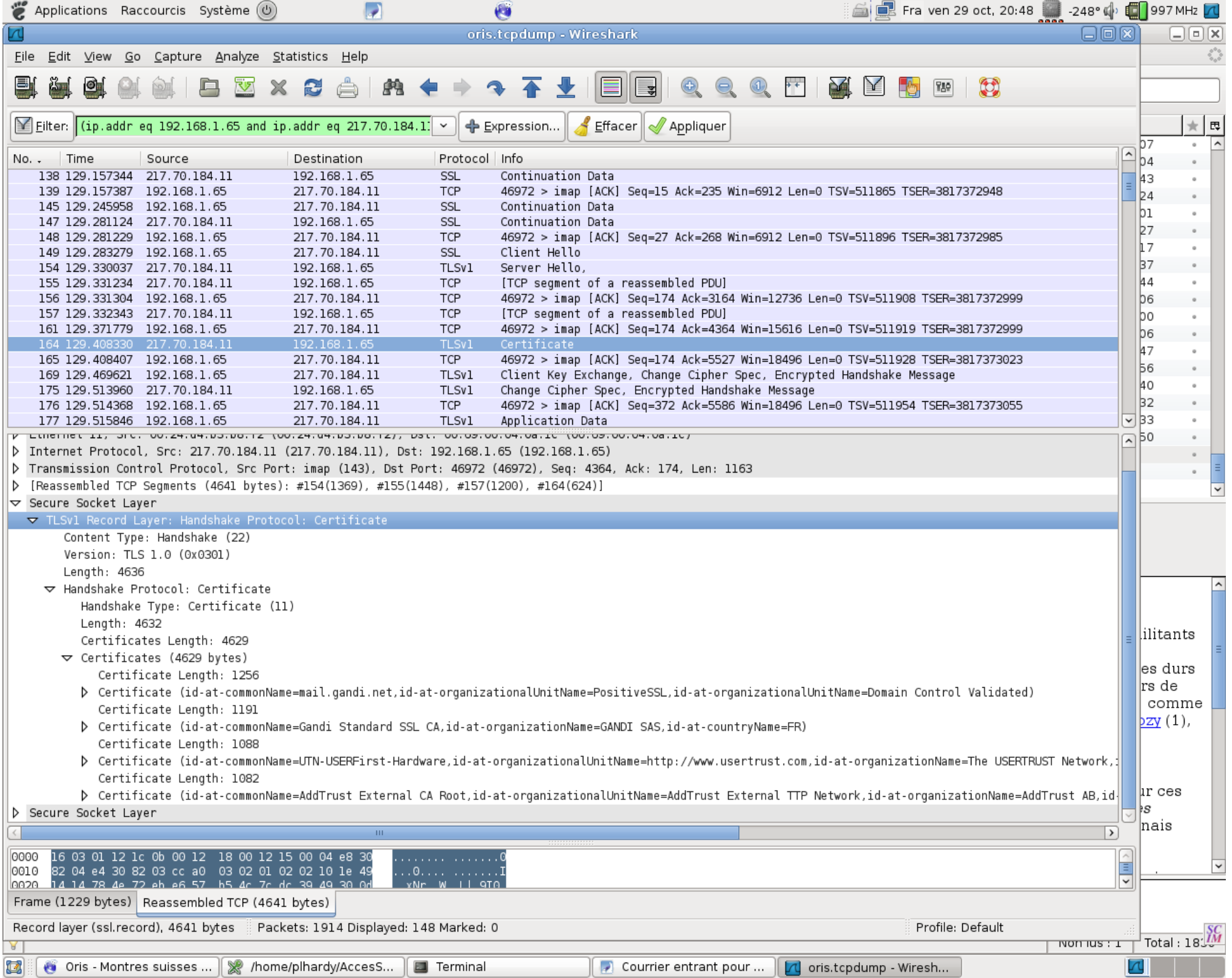
Utilisations

- Https
- Toute application qui désire s'assurer qu'elle communique bien avec la bonne entité.
- Https + Proxy Web
- RPV (VPN)
  - OpenVPN = openssl + tun(IP) | tap(Ethernet)
- Des protocoles existants se sont vu ajouter STARTTLS pour avoir un surcouche TLS.

Le S de ... LDAPS SMTP over TLS

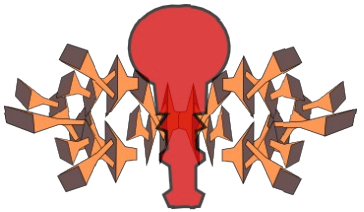
- LDAPS
  - ldap over TLS qui nécessite un port 636 dédié et qui peut fonctionner avec un ldap v2 bind. C'est le plus classique
  - Ldaps qui fonctionne soit en ldap clair ou au dessus de TLS par l'utilisation d'une commande STARTTLS
- SNMP-S
- IMAP+TLS – POPS – NNTP - XMPP
- Wifi : EAP/TLS PEAP TTLS ...
- Mais pas SFTP ou SCP(tunnel ssh)

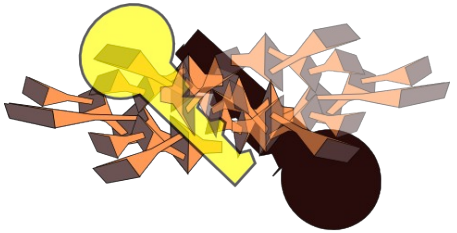
"SNMP over DTLS over UDP" and "SNMP over TLS over TCP" (RFC5953)


Applications Raccourcis Système
Fra ven 29 oct, 20:48
-248°
997 MHz
oris.tcpdump - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: (ip.addr eq 192.168.1.65 and ip.addr eq 217.70.184.11
Expression... Effacer Appliquer
No. Time Source Destination Protocol Info
138 129.157344 217.70.184.11 192.168.1.65 SSL Continuation Data
139 129.157387 192.168.1.65 217.70.184.11 TCP 46972 > imap [ACK] Seq=15 Ack=235 Win=6912 Len=0 TSV=511865 TSER=3817372948
145 129.245958 192.168.1.65 217.70.184.11 SSL Continuation Data
147 129.281124 217.70.184.11 192.168.1.65 SSL Continuation Data
148 129.281229 192.168.1.65 217.70.184.11 TCP 46972 > imap [ACK] Seq=27 Ack=268 Win=6912 Len=0 TSV=511896 TSER=3817372985
149 129.283279 192.168.1.65 217.70.184.11 SSL Client Hello
154 129.330037 217.70.184.11 192.168.1.65 TLSv1 Server Hello,
155 129.331234 217.70.184.11 192.168.1.65 TCP [TCP segment of a reassembled PDU]
156 129.331304 192.168.1.65 217.70.184.11 TCP 46972 > imap [ACK] Seq=174 Ack=3164 Win=12736 Len=0 TSV=511908 TSER=3817372999
157 129.332343 217.70.184.11 192.168.1.65 TCP [TCP segment of a reassembled PDU]
161 129.371779 192.168.1.65 217.70.184.11 TCP 46972 > imap [ACK] Seq=174 Ack=4364 Win=15616 Len=0 TSV=511919 TSER=3817372999
164 129.408330 217.70.184.11 192.168.1.65 TLSv1 Certificate
165 129.408407 192.168.1.65 217.70.184.11 TCP 46972 > imap [ACK] Seq=174 Ack=5527 Win=18496 Len=0 TSV=511928 TSER=3817373023
169 129.469621 192.168.1.65 217.70.184.11 TLSv1 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
175 129.513960 217.70.184.11 192.168.1.65 TLSv1 Change Cipher Spec, Encrypted Handshake Message
176 129.514368 192.168.1.65 217.70.184.11 TCP 46972 > imap [ACK] Seq=372 Ack=5586 Win=18496 Len=0 TSV=511954 TSER=3817373055
177 129.515846 192.168.1.65 217.70.184.11 TLSv1 Application Data
Internet Protocol, Src: 217.70.184.11 (217.70.184.11), Dst: 192.168.1.65 (192.168.1.65)
Transmission Control Protocol, Src Port: imap (143), Dst Port: 46972 (46972), Seq: 4364, Ack: 174, Len: 1163
[Reassembled TCP Segments (4641 bytes): #154(1369), #155(1448), #157(1200), #164(624)]
Secure Socket Layer
TLSv1 Record Layer: Handshake Protocol: Certificate
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 4636
Handshake Protocol: Certificate
Handshake Type: Certificate (11)
Length: 4632
Certificates Length: 4629
Certificates (4629 bytes)
Certificate Length: 1256
Certificate (id-at-commonName=mail.gandi.net,id-at-organizationalUnitName=PositiveSSL,id-at-organizationalUnitName=Domain Control Validated)
Certificate Length: 1191
Certificate (id-at-commonName=Gandi Standard SSL CA,id-at-organizationName=GANDI SAS,id-at-countryName=FR)
Certificate Length: 1088
Certificate (id-at-commonName=UTN-USERFirst-Hardware,id-at-organizationalUnitName=http://www.usertrust.com,id-at-organizationName=The USERTRUST Network,
Certificate Length: 1082
Certificate (id-at-commonName=AddTrust External CA Root,id-at-organizationalUnitName=AddTrust External TTP Network,id-at-organizationName=AddTrust AB,id-
Secure Socket Layer
0000 16 03 01 12 1c 0b 00 12 18 00 12 15 00 04 e8 30 0
0010 82 04 e4 30 82 03 cc a0 03 02 01 02 02 10 1e 49 ...0.... I
Frame (1229 bytes)
Reassembled TCP (4641 bytes)
Record layer (ssl.record), 4641 bytes
Packets: 1914 Displayed: 148 Marked: 0
Profile: Default
Oris - Montres suisses ...
/home/plhardy/AccesS...
Terminal
Courrier entrant pour ...
oris.tcpdump - Wiresh...

Taille des clefs

- Ne pas comparer des clefs symétriques avec des paires de clefs publiques/privées
- Au minimum :
  - >= 128 symétrique
  - >= 1024 clé publique RSA (cela dépend de l'algo).





A chaque couche ses protocoles

Application	Application openssl
Présentation	PGP/GnuPG S/Mime
Session	SSH
Transport	TLS
	TCP – UDP -SCTP
Réseau	IPSec
Liaison	WEP WPA 802.1x
Physique	Cryptographie Quantique

Ipsec vs SSL/TLS

- (+) multi-protocoles, tout ce qui passe sur IP peut être sécurisé par Ipsec
- (<>) Echange des clefs par un protocole hors bande (ISAKMP/IKE)
- (<>) chaque sens de trafic est indépendant
- Principalement utilisé pour les réseaux privés virtuels d 'entreprises
  - (=) Difficile à mettre en place.
  - (+) au même niveau qu'IP il n'altère pas la gestion des flux de données. Par exemple pour les protocoles de VoIP.
- - Sensible à la modification des adresses IP
  - (-) traverse les réseaux personnels avec difficulté

SSH vs SSL/TLS

- Sécurisation d'un accès au shell distant
  - Systèmes unix
  - A remplacé les telnet et r (login,...) commandes
- SSH est au shell unix ce que SSL/TLS est service web.
- Tunnel de protocoles
  - (=) tunnel TCP, UDP et même IP moyennant l'utilisation d'encapsulation IP/IP.
- Transitivité
  - (+) permet de traverser plusieurs systèmes avec la même identité

PGP/GnuPG != S/Mime

- Principalement utilisé pour les courriers
- Ce n'est pas un protocole réseau, il s'utilise avant envoi et après réception des données, quelquesoit la façon dont elles sont transmises, pourvu quelles ne soient pas altérées.
- PGP/GnuPG N'utilise pas les PKI X509 la chaine de confiance est gérée par chacun des participants
- S/Mime Utilise les certificats X509

Références Bibliographiques

- IETF : TLS 1.2 rfc5246 (+ rfc5747, rfc5878)
- SSL and TLS « Designing and Building Secure Systems » Eric Rescorla ADDISON-WESLEY
- Network Security with OpenSSL John Viega, Matt Messier & Pravir Chandra
- « Applied Cryptography » Bruce Schneier John Wiley & Sons,Inc
- Divers
  - W. Richard Stevens. UNIX Network Programming, Volume 2: Inter-process Communications. Prentice-Hall, 1999.

Bruce Schneier

- Bruce Schneier...
- ...Parce qu'il ne peut y avoir de présentation autours de la cryptographie sans une mention à Bruce Schneier :-)