. login adresse mot de passe

. select inbox

. fetch numéro\_mail body[ ]

.store 1 +flags (\Deleted)  
  
Le message n'apparaît plus sur le Webmail. Mais en fait il n'est pas supprimé

→

.store 1 -flags (\Deleted)

. create archive2

. select inbox

. copy 1 archive2

. store 1 +flags (\Deleted)

. expunge

. CLOSE

. LOGOUT

1.2

nslookup -type=MX grenoble-inp.org

grenoble-inp.org mail exchanger = 10 etu3.viallet.grenoble-inp.fr.

grenoble-inp.org mail exchanger = 5 etu.viallet.grenoble-inp.fr.

grenoble-inp.org mail exchanger = 20 etu4.viallet.grenoble-inp.fr.

10, 5 et 20. Numéro priorité  
  
HELO Nom  
MAIL FROM:

RCPT TO:

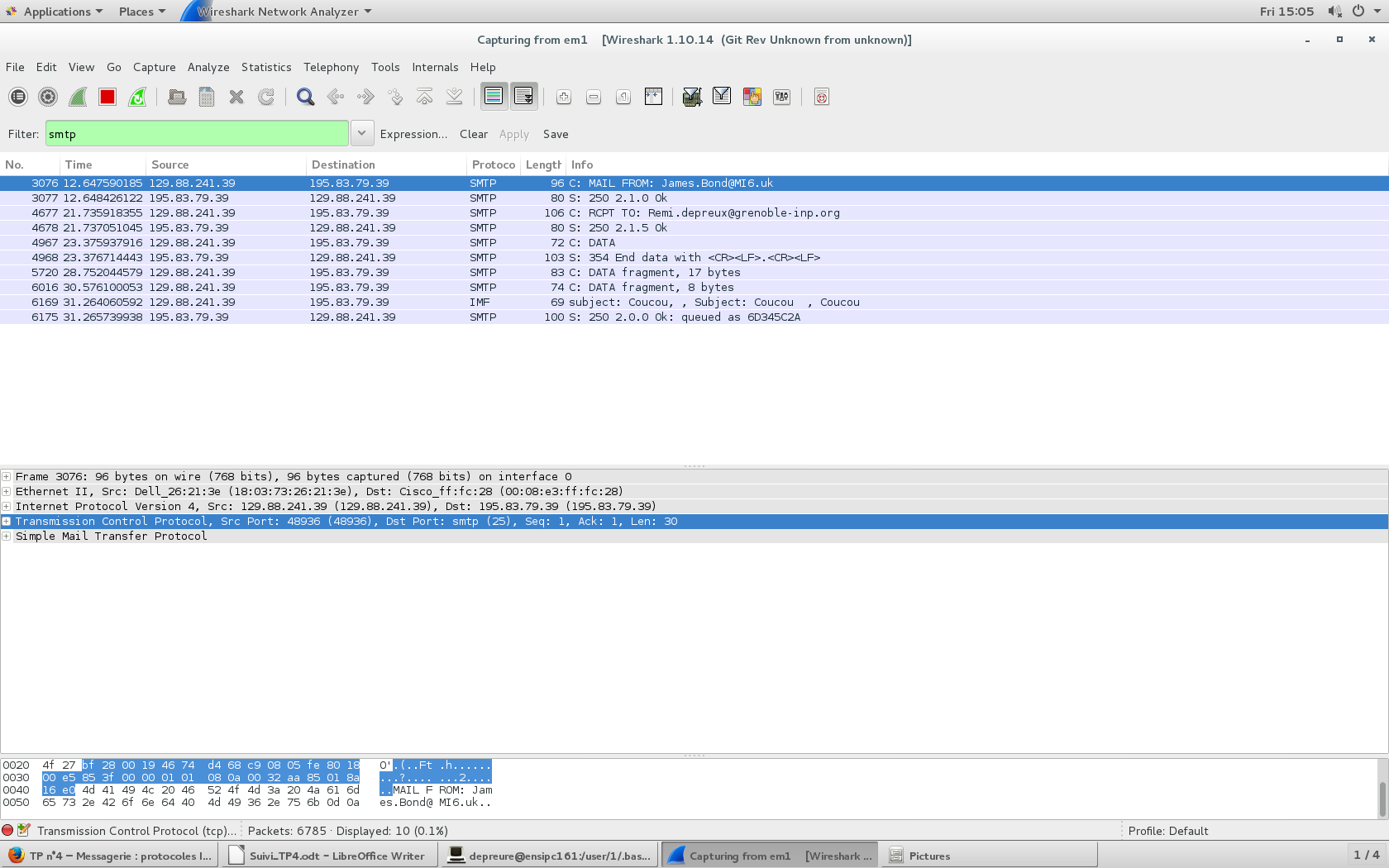
DATA

éventuellement

Subject: [insérer objet]

….

.



La communication n'est pas sécurisée

IMF rassemble tous les fragments

STARTTLS : 3 requêtes non chiffrées dont EHLO puis ouais on chiffre frère?  
  
Quand on essaie avec Grenoble-inp.org en openssl

openssl s\_client -starttls smtp -connect etu.viallet.grenoble-inp.fr:25

ça affiche

CONNECTED(00000003)

didn't found starttls in server response, try anyway...

140664014165920:error:140770FC:SSL routines:SSL23\_GET\_SERVER\_HELLO:unknown protocol:s23\_clnt.c:794:

---

no peer certificate available

---

No client certificate CA names sent

---

SSL handshake has read 232 bytes and written 324 bytes

---

New, (NONE), Cipher is (NONE)

Secure Renegotiation IS NOT supported

Compression: NONE

Expansion: NONE

No ALPN negotiated

SSL-Session:

Protocol : TLSv1.2

Cipher : 0000

Session-ID:

Session-ID-ctx:

Master-Key:

Key-Arg : None

Krb5 Principal: None

PSK identity: None

PSK identity hint: None

Start Time: 1520605452

Timeout : 300 (sec)

Verify return code: 0 (ok)

L'image est véhiculée en chiffrée

Les données sont codées avec ma clef privée, j'suppose.

[depreure@ensipc161 home]$ openssl x509 -text -in certificat.crt

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

86:be:99:7e:ec:1d:46:a2:ba:e0:95:f0:9e:9a:bb:42

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO RSA Client Authen

tication and Secure Email CA

Validity

Not Before: Mar 9 00:00:00 2018 GMT

Not After : Mar 9 23:59:59 2019 GMT

Subject: emailAddress=remi.depreux@grenoble-inp.org

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

00:c4:32:47:fe:b3:9b:f5:a7:94:63:e2:91:38:f5:

7c:c6:29:c4:a2:a9:bd:67:3f:28:8a:48:ac:72:43:

b3:ce:b5:93:30:20:64:c7:e0:0a:60:99:84:ff:98:

53:32:f4:4f:a5:a1:99:64:1b:4b:1b:ca:d2:68:31:

4b:f9:9c:bb:67:8f:b9:4b:1c:e4:fa:87:72:6c:26:

8f:b0:e7:83:7f:c4:5f:50:75:a0:29:35:50:d0:7b:

9b:a0:da:8a:ce:f6:bf:e0:67:e9:90:72:a1:d1:1b:

32:0c:24:e0:fb:c5:3a:5a:04:66:2f:98:66:00:e7:

78:7f:4b:50:73:9f:95:a5:bd:17:fa:d1:84:8f:6a:

06:b6:8a:54:66:02:55:8e:86:cf:b7:e0:05:f6:03:

32:96:9e:36:b2:fe:5d:d7:33:6f:55:99:2e:ca:15:

4e:27:da:87:f7:f6:87:f5:ed:4a:70:f3:4f:c4:31:

70:2e:9b:39:9c:c2:bf:ee:63:17:66:26:13:76:0a:

71:1b:cd:c5:0c:da:66:1e:17:d9:49:55:43:c3:cb:

6a:8e:6c:c3:6f:68:b8:6b:1c:60:b5:40:01:a5:73:

86:c2:dd:fd:47:f0:a4:5e:7c:12:d5:28:0e:43:68:

f0:de:6d:60:d8:88:7b:72:2c:a0:fe:8b:79:9e:05:

f3:03

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Authority Key Identifier:

keyid:82:AF:6C:8C:F8:C5:FE:96:61:7C:E8:1F:3D:2B:71:48:5E:C4:8B:C0

X509v3 Subject Key Identifier:

38:B6:FF:EF:29:C9:E3:1B:70:92:37:6E:E8:E5:15:B5:36:22:83:AB

X509v3 Key Usage: critical

Digital Signature, Key Encipherment

X509v3 Basic Constraints: critical

CA:FALSE

X509v3 Extended Key Usage:

E-mail Protection, 1.3.6.1.4.1.6449.1.3.5.2

Netscape Cert Type:

S/MIME

X509v3 Certificate Policies:

Policy: 1.3.6.1.4.1.6449.1.2.1.1.1

CPS: https://secure.comodo.net/CPS

X509v3 CRL Distribution Points:

Full Name:

URI:http://crl.comodoca.com/COMODORSAClientAuthenticationandSecureEmailCA.crl

Authority Information Access:

CA Issuers - URI:http://crt.comodoca.com/COMODORSAClientAuthenticationandSecureEmailCA.c

rt

OCSP - URI:http://ocsp.comodoca.com

X509v3 Subject Alternative Name:

email:remi.depreux@grenoble-inp.org

Signature Algorithm: sha256WithRSAEncryption

41:e6:74:2c:1c:20:a3:42:66:65:e9:6f:c8:4a:da:ee:b7:b6:

94:f5:61:47:95:9e:bc:49:47:81:2a:02:70:bb:21:6a:2a:74:

d1:dd:64:8b:48:f2:1c:23:a6:37:eb:c3:f1:2c:d1:88:0c:ba:

93:77:24:01:5c:a8:7d:89:40:72:1c:0d:bb:71:37:c4:4f:db:

6e:d5:ef:4d:24:c0:b3:9f:c4:43:b4:c4:d8:a8:f6:21:1d:42:

9f:52:fc:ad:42:72:cc:cb:54:ce:4c:53:c6:ba:c9:29:16:b6:

85:3f:5d:69:67:6a:19:97:ce:95:5a:85:27:82:02:84:fd:d2:

d7:56:25:94:7a:90:80:2a:a3:a7:de:89:67:d8:58:99:31:53:

82:2b:64:ee:05:f4:a6:e9:22:58:c8:38:3d:bd:0a:2a:39:55:

ec:b4:06:f4:6f:99:e3:59:0a:86:65:3a:43:36:f0:81:15:3a:

66:4e:75:1d:62:59:62:3c:ad:09:42:a4:ce:6e:1b:23:9a:69:

c9:f9:06:98:25:cd:ed:b3:f7:73:4f:c1:3a:59:3f:21:0a:7c:

f5:f4:ad:89:d3:ac:e2:9f:f2:ab:9e:6a:81:20:74:1a:91:48:

44:7b:b4:bb:c9:5d:28:5b:e8:f2:70:63:f7:c0:69:31:6a:0b:

d3:1b:f7:f5

-----BEGIN CERTIFICATE-----

MIIFRjCCBC6gAwIBAgIRAIa+mX7sHUaiuuCV8J6au0IwDQYJKoZIhvcNAQELBQAw

gZcxCzAJBgNVBAYTAkdCMRswGQYDVQQIExJHcmVhdGVyIE1hbmNoZXN0ZXIxEDAO

BgNVBAcTB1NhbGZvcmQxGjAYBgNVBAoTEUNPTU9ETyBDQSBMaW1pdGVkMT0wOwYD

VQQDEzRDT01PRE8gUlNBIENsaWVudCBBdXRoZW50aWNhdGlvbiBhbmQgU2VjdXJl

IEVtYWlsIENBMB4XDTE4MDMwOTAwMDAwMFoXDTE5MDMwOTIzNTk1OVowLjEsMCoG

CSqGSIb3DQEJARYdcmVtaS5kZXByZXV4QGdyZW5vYmxlLWlucC5vcmcwggEiMA0G

CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDEMkf+s5v1p5Rj4pE49XzGKcSiqb1n

PyiKSKxyQ7POtZMwIGTH4ApgmYT/mFMy9E+loZlkG0sbytJoMUv5nLtnj7lLHOT6

h3JsJo+w54N/xF9QdaApNVDQe5ug2orO9r/gZ+mQcqHRGzIMJOD7xTpaBGYvmGYA

53h/S1Bzn5WlvRf60YSPaga2ilRmAlWOhs+34AX2AzKWnjay/l3XM29VmS7KFU4n

2of39of17Upw80/EMXAumzmcwr/uYxdmJhN2CnEbzcUM2mYeF9lJVUPDy2qObMNv

aLhrHGC1QAGlc4bC3f1H8KRefBLVKA5DaPDebWDYiHtyLKD+i3meBfMDAgMBAAGj

ggHzMIIB7zAfBgNVHSMEGDAWgBSCr2yM+MX+lmF86B89K3FIXsSLwDAdBgNVHQ4E

FgQUOLb/7ynJ4xtwkjdu6OUVtTYig6swDgYDVR0PAQH/BAQDAgWgMAwGA1UdEwEB

/wQCMAAwIAYDVR0lBBkwFwYIKwYBBQUHAwQGCysGAQQBsjEBAwUCMBEGCWCGSAGG

+EIBAQQEAwIFIDBGBgNVHSAEPzA9MDsGDCsGAQQBsjEBAgEBATArMCkGCCsGAQUF

BwIBFh1odHRwczovL3NlY3VyZS5jb21vZG8ubmV0L0NQUzBaBgNVHR8EUzBRME+g

TaBLhklodHRwOi8vY3JsLmNvbW9kb2NhLmNvbS9DT01PRE9SU0FDbGllbnRBdXRo

ZW50aWNhdGlvbmFuZFNlY3VyZUVtYWlsQ0EuY3JsMIGLBggrBgEFBQcBAQR/MH0w

VQYIKwYBBQUHMAKGSWh0dHA6Ly9jcnQuY29tb2RvY2EuY29tL0NPTU9ET1JTQUNs

aWVudEF1dGhlbnRpY2F0aW9uYW5kU2VjdXJlRW1haWxDQS5jcnQwJAYIKwYBBQUH

MAGGGGh0dHA6Ly9vY3NwLmNvbW9kb2NhLmNvbTAoBgNVHREEITAfgR1yZW1pLmRl

cHJldXhAZ3Jlbm9ibGUtaW5wLm9yZzANBgkqhkiG9w0BAQsFAAOCAQEAQeZ0LBwg

o0JmZelvyEra7re2lPVhR5WevElHgSoCcLshaip00d1ki0jyHCOmN+vD8SzRiAy6

k3ckAVyofYlAchwNu3E3xE/bbtXvTSTAs5/EQ7TE2Kj2IR1Cn1L8rUJyzMtUzkxT

xrrJKRa2hT9daWdqGZfOlVqFJ4IChP3S11YllHqQgCqjp96JZ9hYmTFTgitk7gX0

pukiWMg4Pb0KKjlV7LQG9G+Z41kKhmU6QzbwgRU6Zk51HWJZYjytCUKkzm4bI5pp

yfkGmCXN7bP3c0/BOlk/IQp89fStidOs4p/yq55qgSB0GpFIRHu0u8ldKFvo8nBj

98BpMWoL0xv39Q==

-----END CERTIFICATE-----

Échange de mails signés avec les certificats puis on peut encrypter

S\MIME ENCRYPTED MESSAGE  
  
Sur WEBMAIL on ne reçoit pas le message