

Cours PLURITAL 2012-2013

Jean-François Perrot & Marie-Anne Moreaux

Examen écrit du mardi 15 janvier 2013

Durée 3h, tous documents autorisés

Les trois questions que voici sont sans rapport entre elles. Traitez-les dans l'ordre de votre choix.

Veillez à toujours motiver vos décisions...

1. Cryptographie

Lorsqu'un éditeur de textes ouvre un fichier en se trompant d'encodage, le résultat peut être surprenant.

1. Quand vous lisez (attention ! les 'Ã' sont des LATIN CAPITAL LETTER A WITH TILDE) :

Ã+a, c'Ã©tait mon frÃ¨re RenÃ© (Ã gauche, prÃ`s de la fenÃªtre)
et Ãsa c'Ã©tait ma sÃªur IÃªs.

que concluez-vous sur

- le codage original du fichier
- le réglage de l'éditeur

?

2. Et si vous lisez ceci (avec un autre éditeur) :

√aa, c'√©tait mon fr√©re Ren√© (√ gauche, pr√s de la fen√ªtre)
et √sa c'√©tait ma s√ªur I√ªs.

que concluez-vous ?

3. Comment expliquez-vous la différence entre la situation 1 ci-dessus et celle-ci :

Ã[Ã]a, c'Ã©tait mon frÃ¨re RenÃ© (Ã gauche, prÃ`s de la fenÃªtre)
et Ãsa c'Ã©tait ma sÃª[Ã]ur IÃªs.

et avec cette autre ?

Ã[Ã]a, c'Ã©tait mon frÃªre RenÃ© (Ã gauche, prÃªs de la fenÃªtre)
et Ãsa c'Ã©tait ma sÃª[Ã]ur IÃªs.

N.B. Le signe '[Ã]' ne désigne pas un caractère, mais la place occupée par un caractère de contrôle.

4. Dans tous ces exemples, la persistance des caractères ASCII à travers les différents codages rend le texte déchiffrable (pour un francophone). Un texte qui ne contient point d'ASCII devient très mystérieux... On envisage donc d'exploiter ce phénomène pour crypter des messages supposés écrits en UTF-8 avec des systèmes non-latins.
- L'idée est de sauvegarder le texte avec un codage sur 8 bits qui utilise tous les octets au-delà de 128, de transmettre le message ainsi codé dans son codage 8 bits, puis d'ouvrir le fichier transmis en UTF-8.
- Pourquoi cette restriction sur le choix du codage ?
 - Voici un exemple de message codé

```

EiE^E^EΣEΩEΠE∫œåœÇ EüœÄE>E±EΩEΠœÉE°œåœÇ
ESœÖœÄEøœÄEøEΣœÉEΣœÇ

```

Comment faire pour le déchiffrer ?

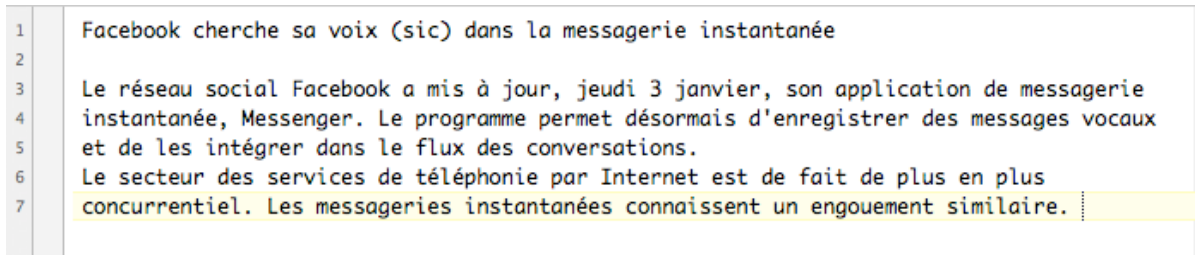
2. Tentatives d'hameçonnage

J'ai soigneusement découpé des exemples de messages bizarres en vue de composer un sujet d'examen, mais un coup de vent a dispersé mes papiers. Je me retrouve avec 6 fiches (en-têtes, déclarations MIME, corps du message) extraites de deux messages différents. Pouvez-vous reconstituer ces deux messages ?

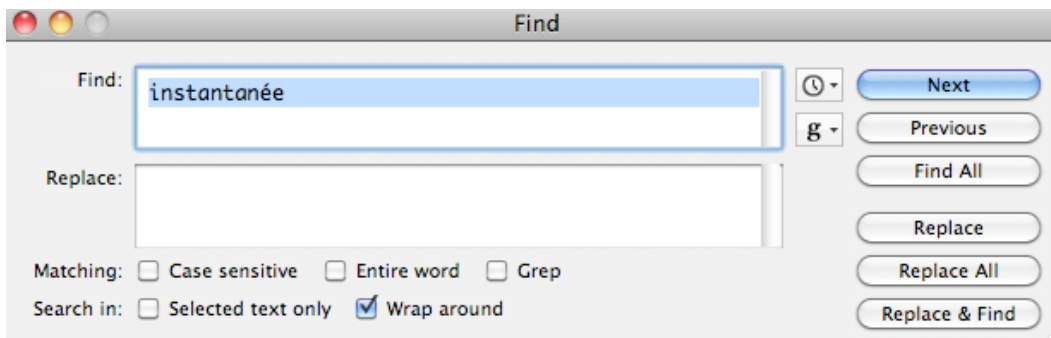
- From: Mohammad Ahmed <mahmad@squ.edu.om>
Date: Fri, 11 Jan 2013 13:30:23 +0400
Subject: =?iso-8859-1?Q?administrateur_du_syst=E8me?=>
- Date: Wed, 9 Jan 2013 20:21:13 +0100 (CET)
From: "serveurs-mail@libero.it" <serveurs-mail@libero.it>
Reply-To: "serveurs-mail@libero.it" <serveurs-mail@libero.it>
Subject: =?UTF-8?Q?SERVEUR*/-_(G00GLE!!-_:AVIS_DE?=
=?UTF-8?Q?_DESACTIVATION_DE_COMPTE--MAIL=E2=80=8F?=>
- MIME-Version: 1.0
Content-Type: text/plain; charset="UTF-8"
Content-Transfer-Encoding: quoted-printable
- MIME-Version: 1.0
Content-Type: text/plain; charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
- Les abonn=C3=A9s aux services *Google* (Compte Gmail!) sont tenus de se faire identifier par l'=C3=A9quipe de notification afin d'=C3=A9viter la mise en r=C3=A9ception de votre compte et de toujours b=C3=A9n=C3=A9ficier = de nos services. En passant imp=C3=A9rativement le texte ci-dessous.
- Am=E9liorez votre QUOTA BO=CETE AUX LETTRES
Votre bo=E9te de r=E9ception a presque d=E9pass=E9 sa limite de stockage.
Il ne sera pas en mesure d'envoyer et de recevoir des e-mails en cas de d=E9passement de la limiter
Et votre compte e-mail sera supprim=E9 de nos serveurs.

3. Disparition

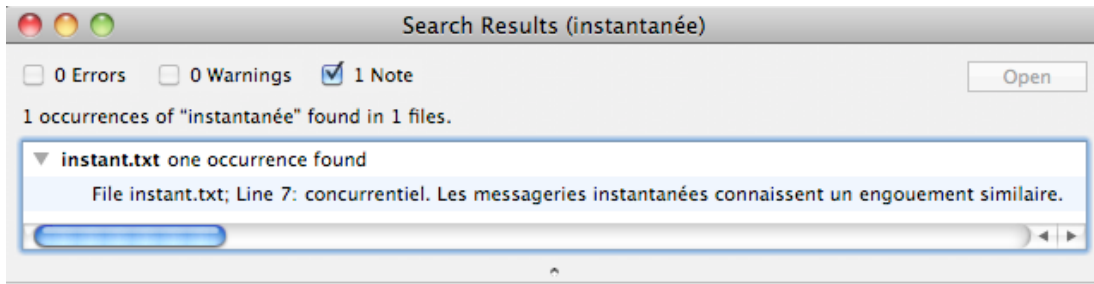
En travaillant sur un texte de journal...



on demande toutes les occurrences du mot `instantanée`, par l'option *find all* du logiciel de recherche "plein texte" :



avec un résultat inattendu :



Avez-vous une interprétation de ce résultat ?

Les explications fournies par *hexdump* vous satisfont-elles ?

```
jfp% hexdump -C instant.txt
00000000  46 61 63 65 62 6f 6f 6b 20 63 68 65 72 63 68 65 |Facebook cherche|
00000010  20 73 61 20 76 6f 69 78 20 28 73 69 63 29 20 64 | sa voix (sic) d|
00000020  61 6e 73 20 6c 61 20 6d 65 73 73 61 67 65 72 69 |ans la messageri|
00000030  65 20 69 6e 73 74 61 6e 74 61 6e 65 cc 81 65 0a |e instantane..e.|
00000040  0a 4c 65 20 72 c3 a9 73 65 61 75 20 73 6f 63 69 |.Le r..seau soci|
00000050  61 6c 20 46 61 63 65 62 6f 6f 6b 20 61 20 6d 69 |al Facebook a mi|
00000060  73 20 c3 a0 20 6a 6f 75 72 2c 20 6a 65 75 64 69 |s .. jour, jeudi|
00000070  20 33 20 6a 61 6e 76 69 65 72 2c 20 73 6f 6e 20 | 3 janvier, son |
00000080  61 70 70 6c 69 63 61 74 69 6f 6e 20 64 65 20 6d |application de m|
00000090  65 73 73 61 67 65 72 69 65 0a 69 6e 73 74 61 6e |essenger.instan|
000000a0  74 61 6e 65 cc 81 65 2c 20 4d 65 73 73 65 6e 67 |tane..e, Messeng|
000000b0  65 72 2e 20 4c 65 20 70 72 6f 67 72 61 6d 6d 65 |er. Le program|
000000c0  20 70 65 72 6d 65 74 20 64 c3 a9 73 6f 72 6d 61 | permet d..sorma|
000000d0  69 73 20 64 27 65 6e 72 65 67 69 73 74 72 65 72 |is d'enregistrer|
000000e0  20 64 65 73 20 6d 65 73 73 61 67 65 73 20 76 6f | des messages vo|
000000f0  63 61 75 78 20 0a 65 74 20 64 65 20 6c 65 73 20 |caux .et de les |
00000100  69 6e 74 c3 a9 67 72 65 72 20 64 61 6e 73 20 6c |int..grer dans l|
```

| | | | |
|----------|-------------------------|-------------------------|-------------------|
| 00000110 | 65 20 66 6c 75 78 20 64 | 65 73 20 63 6f 6e 76 65 | e flux des conve |
| 00000120 | 72 73 61 74 69 6f 6e 73 | 2e 0a 4c 65 20 73 65 63 | rsations..Le sec |
| 00000130 | 74 65 75 72 20 64 65 73 | 20 73 65 72 76 69 63 65 | teur des service |
| 00000140 | 73 20 64 65 20 74 c3 a9 | 6c c3 a9 70 68 6f 6e 69 | s de t..l..phoni |
| 00000150 | 65 20 70 61 72 20 49 6e | 74 65 72 6e 65 74 20 65 | e par Internet e |
| 00000160 | 73 74 20 64 65 20 66 61 | 69 74 20 64 65 20 70 6c | st de fait de pl |
| 00000170 | 75 73 20 65 6e 20 70 6c | 75 73 20 0a 63 6f 6e 63 | us en plus .concl |
| 00000180 | 75 72 72 65 6e 74 69 65 | 6c 2e 20 4c 65 73 20 6d | urrentiel. Les m |
| 00000190 | 65 73 73 61 67 65 72 69 | 65 73 20 69 6e 73 74 61 | essageries insta |
| 000001a0 | 6e 74 61 6e c3 a9 65 73 | 20 63 6f 6e 6e 61 69 73 | ntan..es connais |
| 000001b0 | 73 65 6e 74 20 75 6e 20 | 65 6e 67 6f 75 65 6d 65 | sent un engoueme |
| 000001c0 | 6e 74 20 73 69 6d 69 6c | 61 69 72 65 2e 20 | nt similaire. |
| 000001ce | | | |
