MOBIB Avenger forensics

Plot

- June 2011: anonymous video on Youtube

  MOBIBAvenger claims to have broken MOBIB and promise free ride to everybody, as revenge against the (real) privacy concerns of MOBIB card
- Lame answer from STIB
  “all systems can be hacked, that's life”

Goal of this forensics game

REAL or FAKE?

Bonus question:
Who is MOBIBAvenger?

A few facts on MOBIB

- Calypso standard
- Smartcard ISO14443-4B with file structure
- (obviously nothing to do with MIFARE Classic)
- Privacy nightmare... ask Gildas

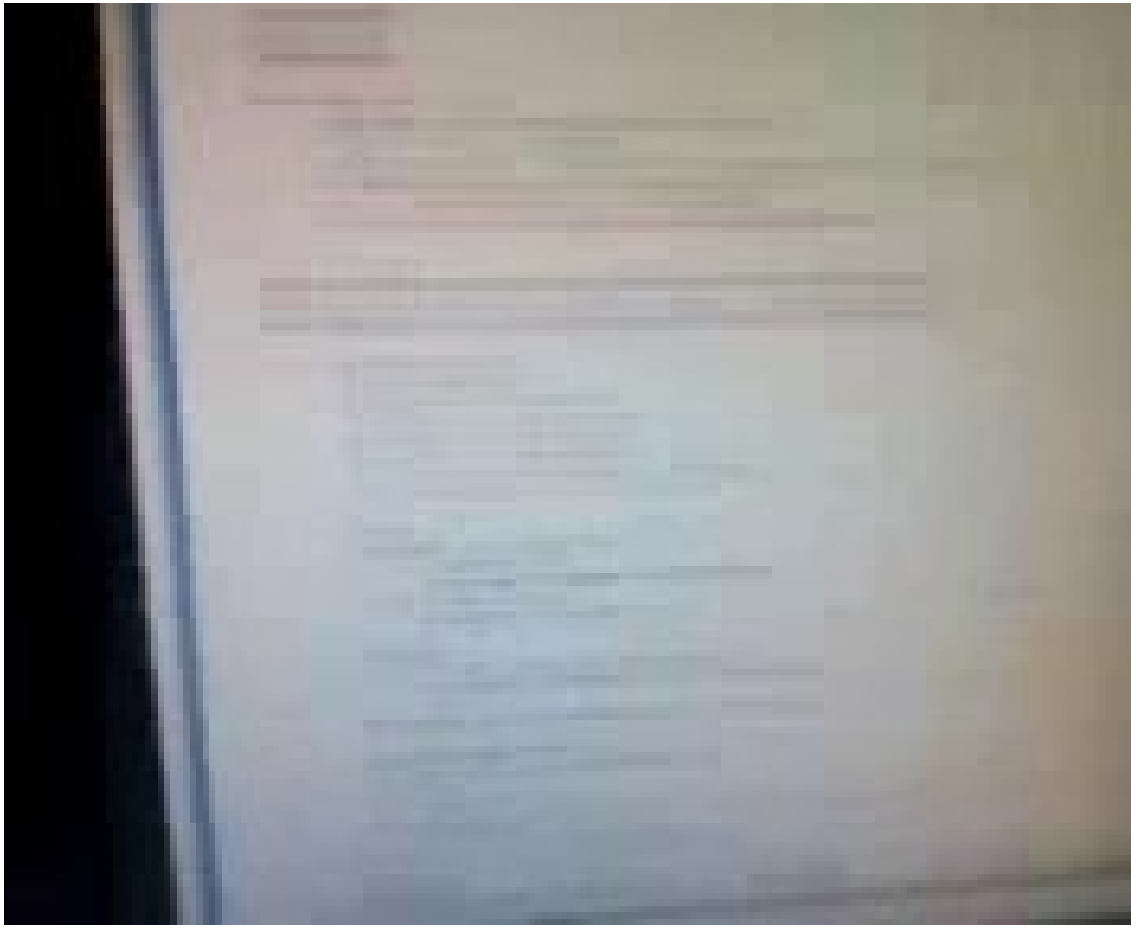
Forensics time

Did you find incoherences?

The easy ones :-)

What's this Open MOBIB software?

Well actually...

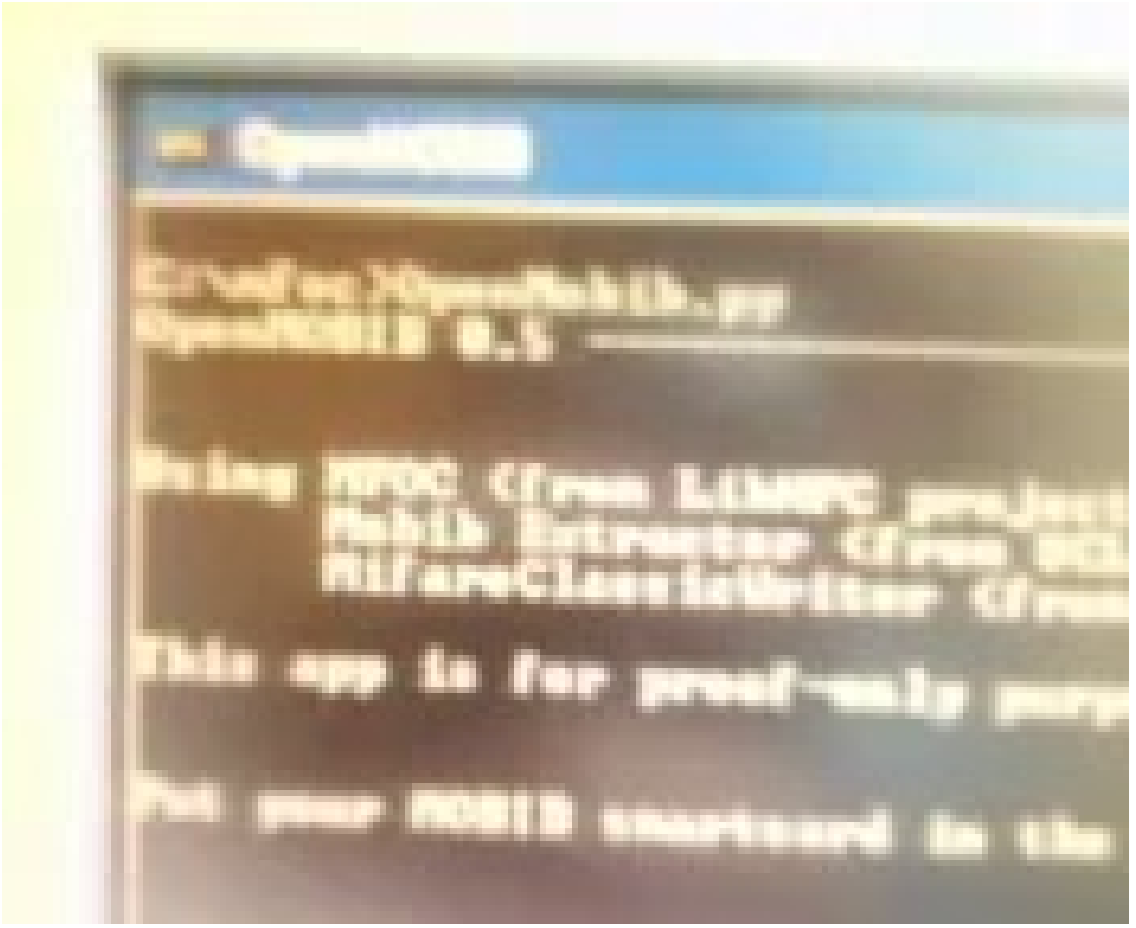


It's MOBIBextractor by UCL

```
334         ##############
335         ## Load Log ##
336         ##############
337
338         def processLoadLog (self):
339                 tmp_hexa = self.load_logs[0] + self.load_logs[1]
340                 tmp_bin = hex_to_bin(tmp_hexa)
341                 self.purchase_card = find_date(int(bin_to_number(tmp_bin[2:len(tmp_bin)])))
342                 if self.purchase_card == "NO TRAVEL REGISTERED":
343                         self.purchase_card = "UNKNOWN DATE"
344                 print "Date of the card purchase : %s"%self.purchase_card
345
346
347         ###########################################################################
348         ## Find Name + Birthdate + Post code + Card number + Remaining travels ##
349         ###########################################################################
350
351         def processHolder (self):
352                 # self.holder1 has :
353                 # - bytes 0-1 : unknown data
354                 # - bytes 2-11 : the card number
355                 # - bytes 12-20 : unknown data
356                 # - bytes 21-24 : the birthday
357                 # - bytes 24-28 : the begining of the name
358                 # self.holder2 has the end of the name
359
360                 ## Name
361                 hexa_name = self.holder1[25][1]
362                 for i in range(26, 29):
363                         hexa_name = hexa_name + self.holder1[i]
364                 for a in (self.holder2):
365                         hexa_name = hexa_name + a
366
367                 bin_name = ''
368                 for i in range(0,len(hex_to_bin(hexa_name))):
369                         bin_name = bin_name + hex_to_bin(hexa_name)[i]
```

MIFOC <> MFOC

Actually his “sw” credits a few ones

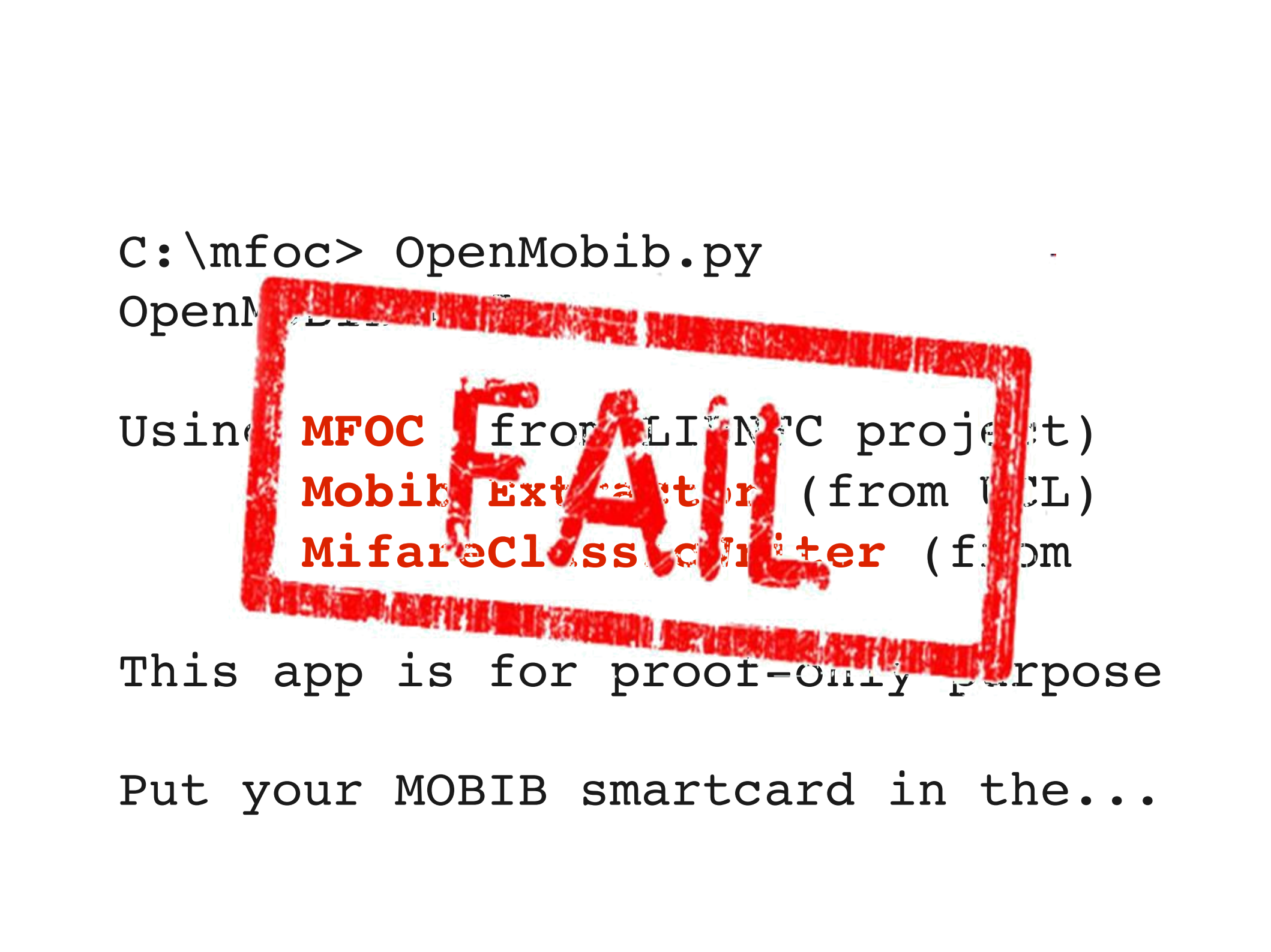


```
C:\mfoc> OpenMobib.py
OpenMOBIB 0.5

Using MFOC (from LIBNFC project)
      Mobib Extractor (from UCL)
      MifareClassicWriter (from

This app is for proof-only purpose

Put your MOBIB smartcard in the...
```

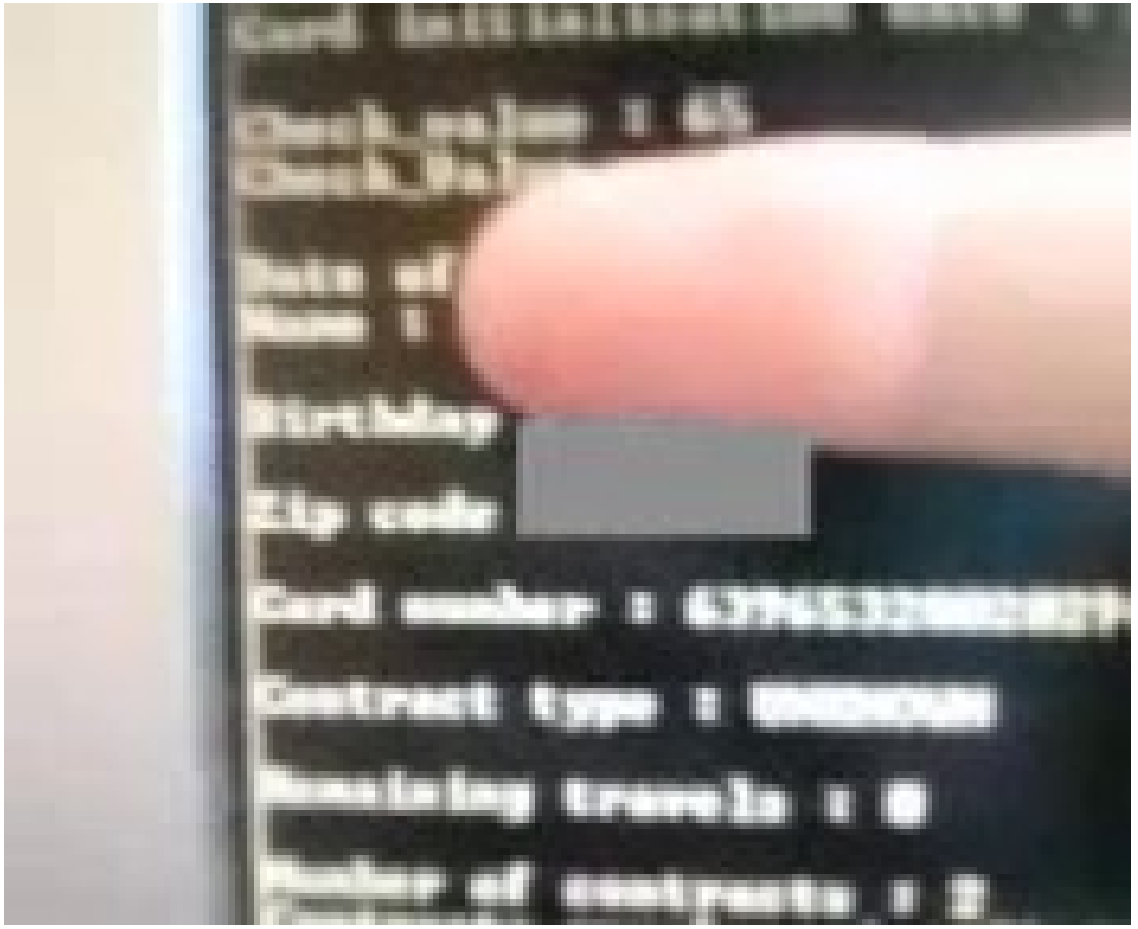

C:\mfoc> OpenMobib.py
MFOC
Mobib Extractor
MifareClassicWriter
FAIL
This app is for proof-only purpose
Put your MOBIB smartcard in the...

Oh BTW... which RFID reader?

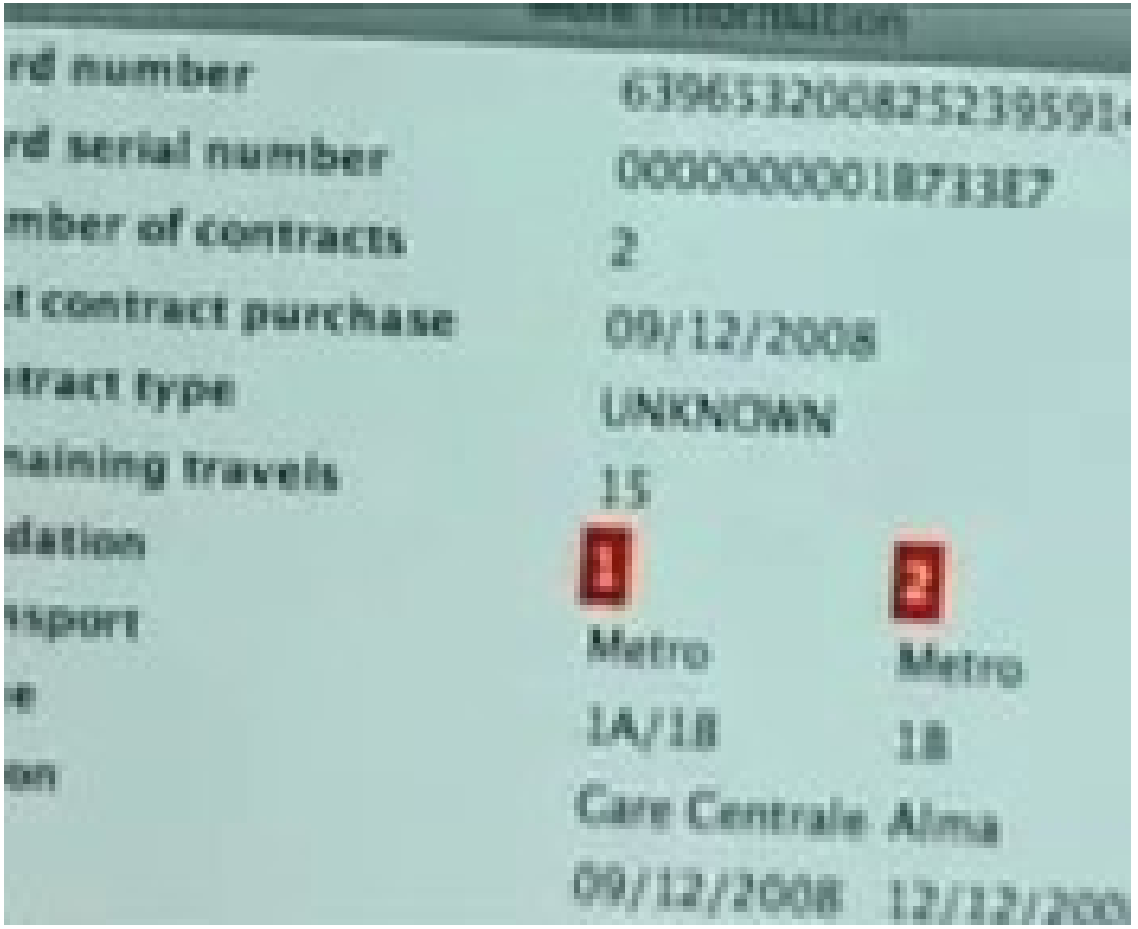
Microsoft Wireless Receiver (for keyboard / mouse)

Who's MOBIB Avenger?

For sure he's shy



From his card number?

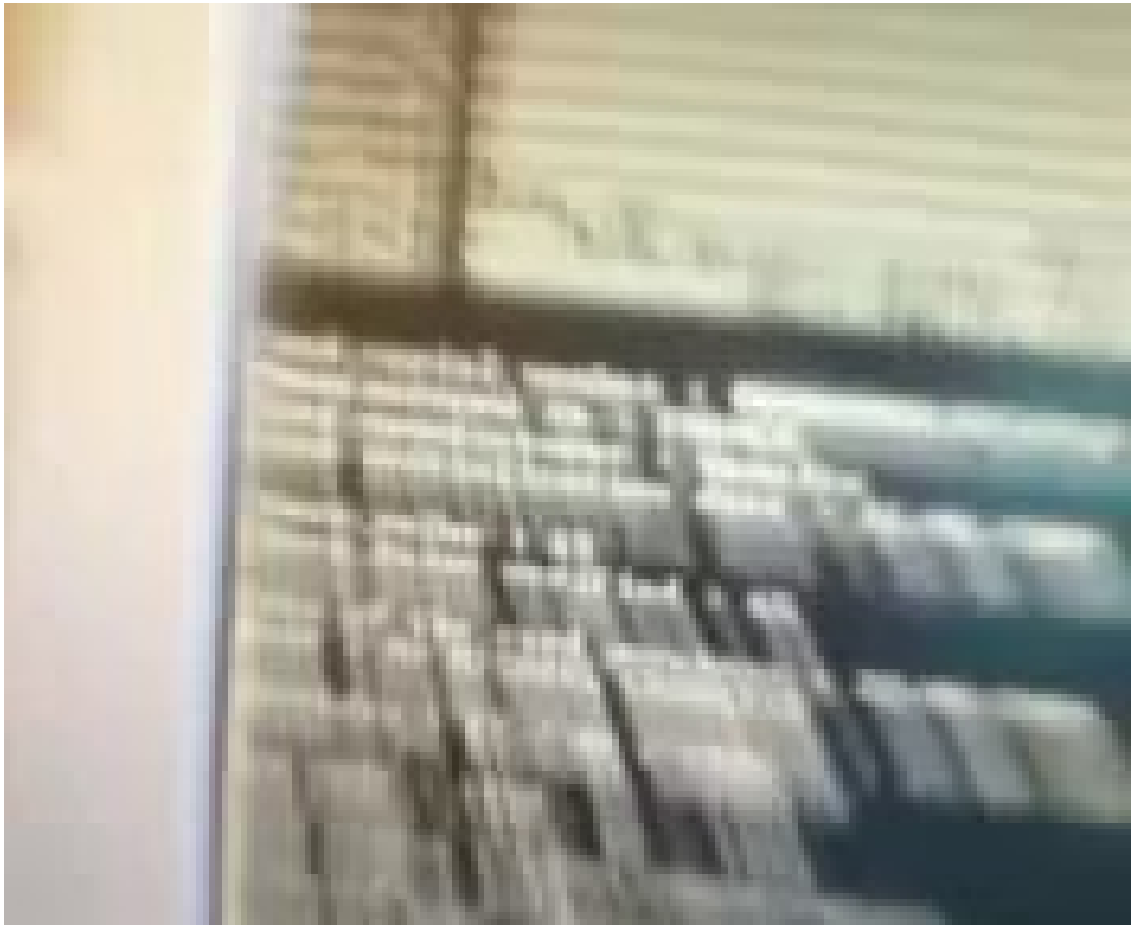


Actually that's even not his card

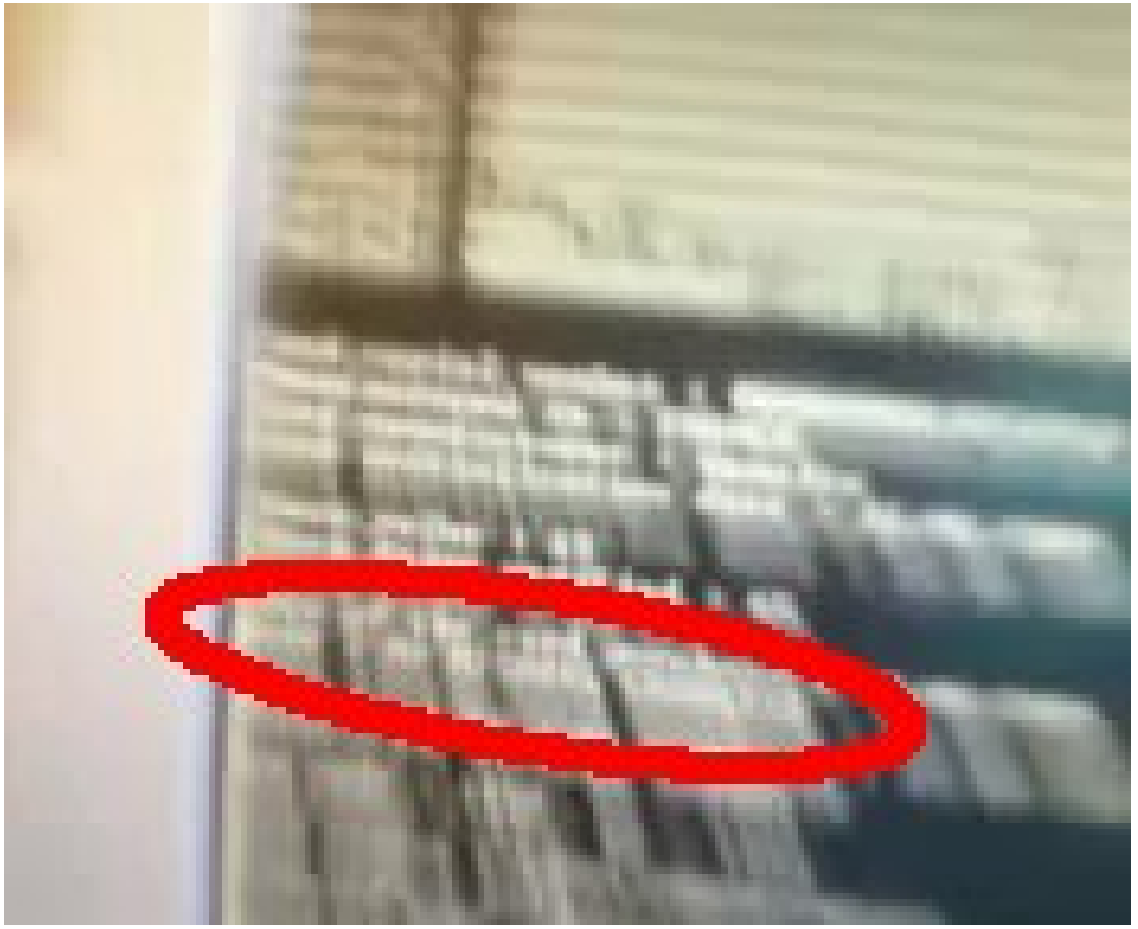
But the card of one of Gildas' colleagues

Captured from TV news reportage
(remember it was about privacy concerns)

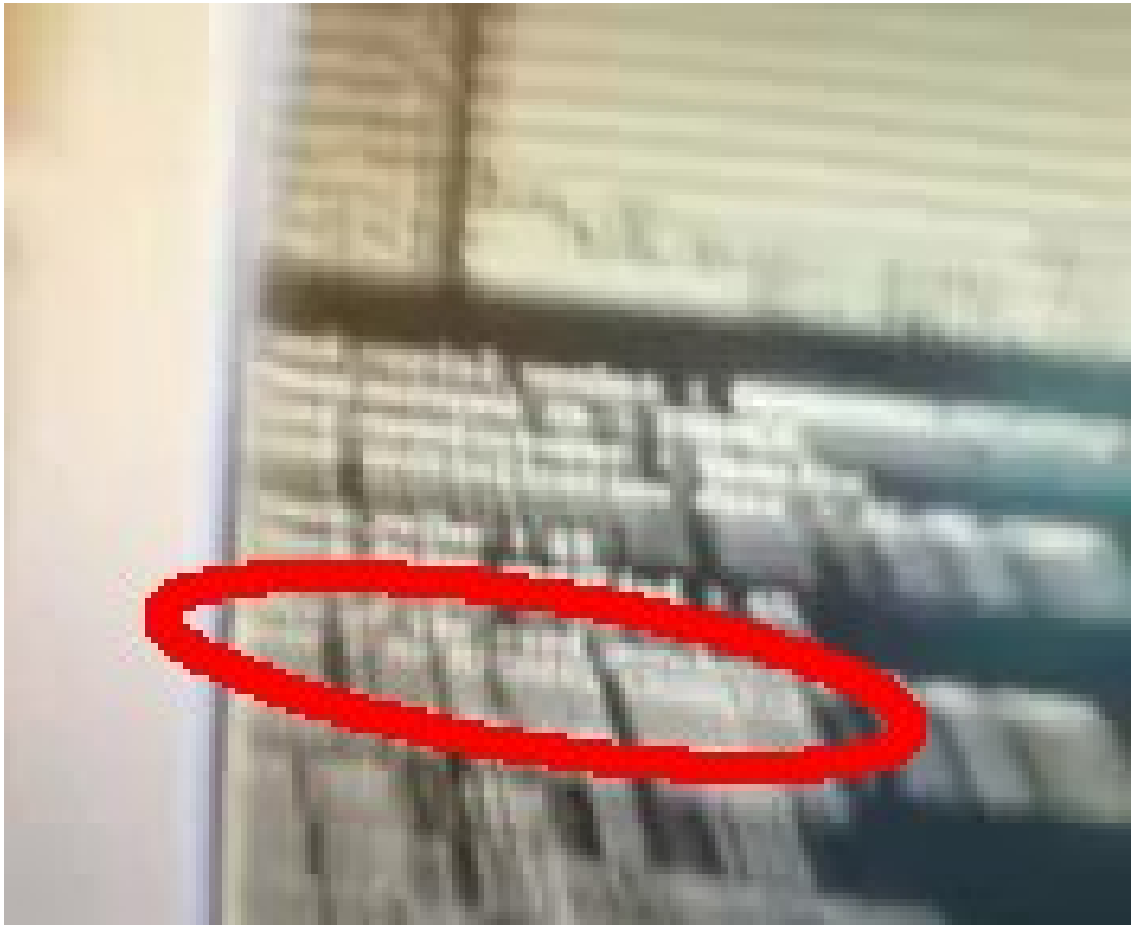
Let's look closer to the mem dump



Let's look closer to the mem dump

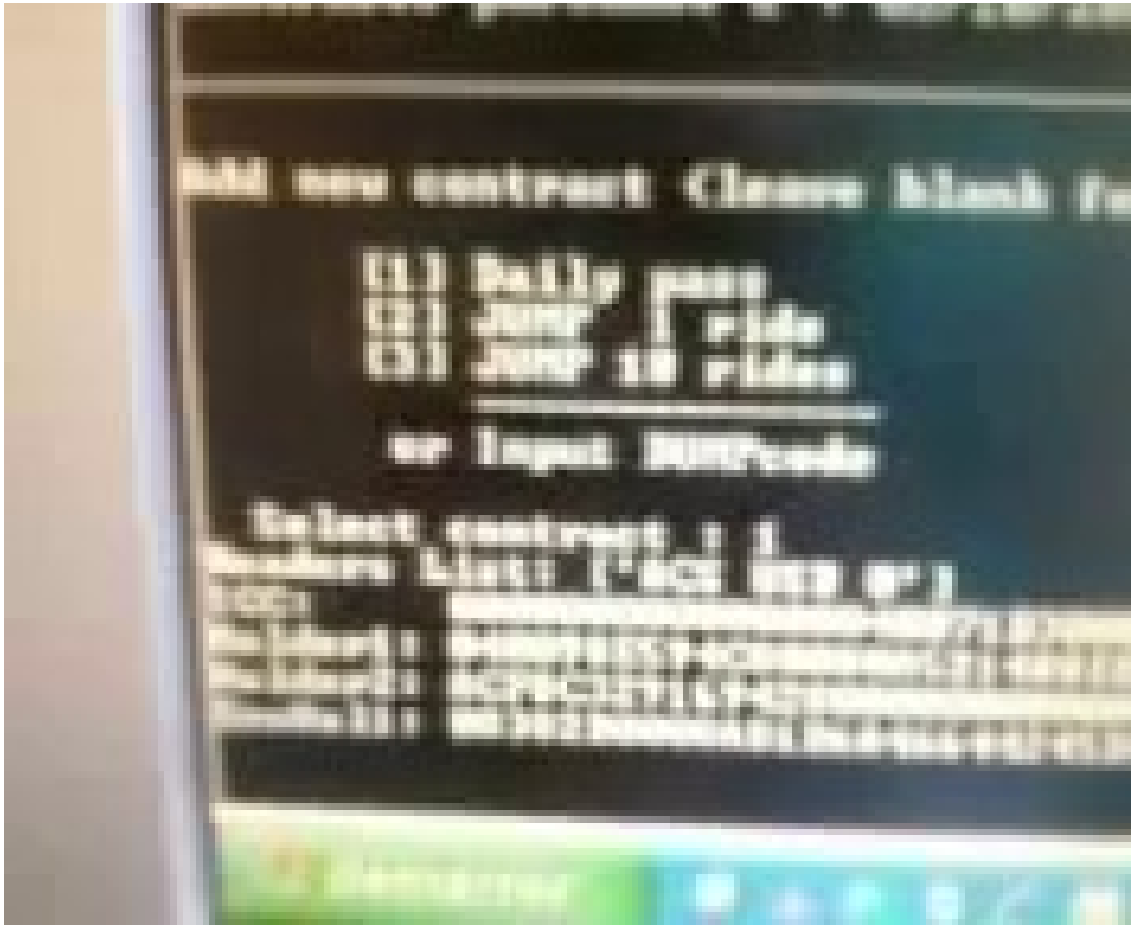


Let's look closer to the mem dump



=> MICHAEL ...?

His name was hidden...
But not the raw memory dump



```
Holder1: 040098...?
Holder2: ACF8C32...
```

MOBIB coding: 8 to 5 bits

```
Holder2: ACF8C3271694230?
         ACF8C3291694280?
```

```
AC       F8       C3       27       16       94       28       0
                           29                          23
10101100 11111000 11000011 00100111 00010110 10010100 00101000
                           00101001                    00100011
   01100 11111 00011 00001 10010 01110  00101 10100 10100 00101 0
                                 10010                 00100 01100
   L     _     C     A     R     N/R    E     T     T     E/DL
```

=> Michael Carnette/Carrette?

Let's ask our big ~~friend~~ brother

michael + carrette + mobib

facebook

Inscription Pour un monde plus ouvert.

Michaël Carrette ▶ **NON A MOBIB (stib)**

4 décembre 2011, 09:37 ·

Votez pour "MOBIB" sur www.bigbrotherawards.be

www.bigbrotherawards.be

Depuis janvier 2008 la STIB a introduit une nouvelle carte de transport : la carte MoBIB. Basée sur la technologie « sans contact » ou RFID, la carte MoBIB, désormais

J'aime · Commenter

Hello Mr Carrette

Michael Carrette

PORTFOLIO

HOME | ABOUT ME | WEBSITE | SOFTWARE | VIDEO

En construction

Curriculum Vitae
au format PDF

Michaël CARRETTE
Rue A. Bracke, 38
1950 Kraainem

tel : +32472/20.26.70
mail : info@miccarr.com

Michaël CARRETTE
Rue A. Bracke, 38
1950–Kraainem
Tel. : 02 / 720.83.21
G.S.M. : 0472 / 20.26.70
E-mail : micradio@gmail.com

Curriculum Vitæ

Parcours Scolaire

- *En cours de 1e BA cinématographie à la HELB-INRACI de Foret ;*
- *Obtention du diplôme de qualification technique en Informatique au Collège Technique St Jean de Wavre;*
- *Secondaires passés au Collège Technique St Jean de Wavre (2003-2009);*
- *Maternelles et Primaires passés à l'école chapelle-aux-champs de Woluwé St-Lambert avec obtention du CEB.*

Actually he contacted Gildas in the past to get info on the system

Je ne cherche pas a pirater le système, mais bien en faire un sujet de travail de fin d'année.

Merci,

Michaël CARRETTE

Conclusions?

- Many incoherences:
  - MIFOC ≠ MFOC
  - Calypso ≠ MIFARE
  - RFID reader ≠ wireless keyboard station
  - Roel's video misuse
  - Gildas' video misuse
- Chance for him that STIB didn't go to the police... as his identity could be revealed

But remember

- MOBIB extractor is real (ok, hard to find...)
- It shows unprotected personal data
- This video only brings confusion between debunked allegations and real privacy problems

Images

Carte mobib

Mots clés

Internet, Police, Politique, Technologies, Transport, STIB

La carte MoBIB de la STIB a remporté jeudi soir le prix du jury lors de la seconde cérémonie des Big Brother's Awards organisée par la Ligue des droits de l'Homme. Ce prix a été emporté dans la catégorie Entreprises et concerne les questions en matière de sécurité des données personnelles et d'anonymat que pose la carte MoBIB.

Objectif de ces Awards : dénoncer "le meilleur du pire" en matière d'atteinte à la vie privée en Belgique.

Le jury a remis un Award à 3 acteurs, répartis en 3 catégories, afin de pointer les problèmes et interrogations que pose leur (in)action en matière respect de la vie privée.

Last minute update

STIB announced this Monday that anonymous cards are now available

Still remains (probably) the last 3 rides issue