

Etude du logiciel CAMOUFLAGE

Free File Camouflage
v1.25

CHAHER Somia

M2 - SSI -

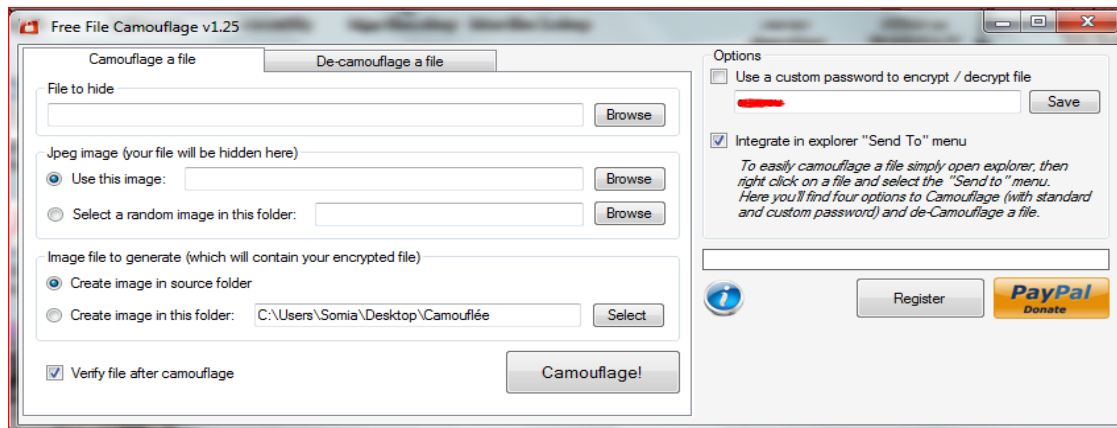
Université de Lorraine _ Metz



Sommaire

Présentation du logiciel.....	3
Installation du logiciel "Camouflage"	4
Sous Windows	4
Sous Linux	7
Etude du logiciel	8
Sous Windows	8
Sous Linux	21

Présentation du logiciel



Camouflage est un logiciel qui permet de cacher et ainsi protéger tous types de fichier dans une image "jpeg".

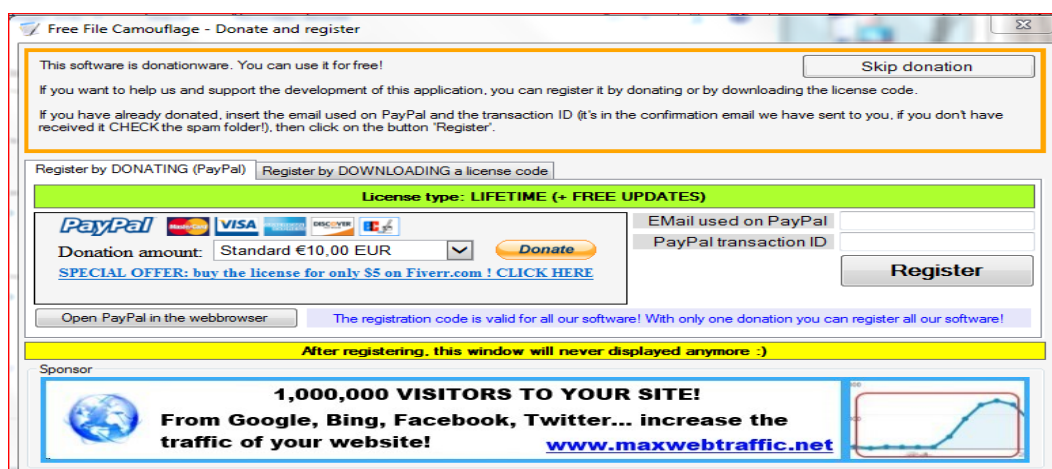
Il permet aussi de récupérer le fichier caché à partir de l'image.

Selon la page officiel du logiciel www.myportablesoftware.com, tous les fichiers sont chiffrés avec AES et cachés à l'intérieur d'une image.

Le logiciel est également utile pour envoyer des programmes ".exe" par mail. Car actuellement, de nombreux fournisseurs de messagerie ne permettent pas cela !

Le site officiel assure que tous les logiciels qui proposent dans leur site sont faits par eux et sont tous originaux. Le site assure aussi que les logiciels ne contiennent ni spyware, ni adware, ni virus !

Le logiciel est complètement gratuit et peut être utilisé partout (maison, travail, école), toutefois le site fait appel à des donations, pour les gens qui veulent les aider et soutenir le développement des applications étant donné que le site propose une panoplie de logiciels gratuits.



Le logiciel peut être utilisé sous les environnements suivants : Windows XP, VISTA, 7, 8 (32 & 64 bit)

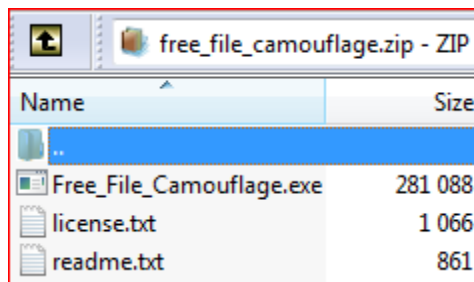
Néanmoins, on a essayé de l'installer sur une machine ubuntu (Linux), on détaillera cela par la suite.

Installation du logiciel "Camouflage"

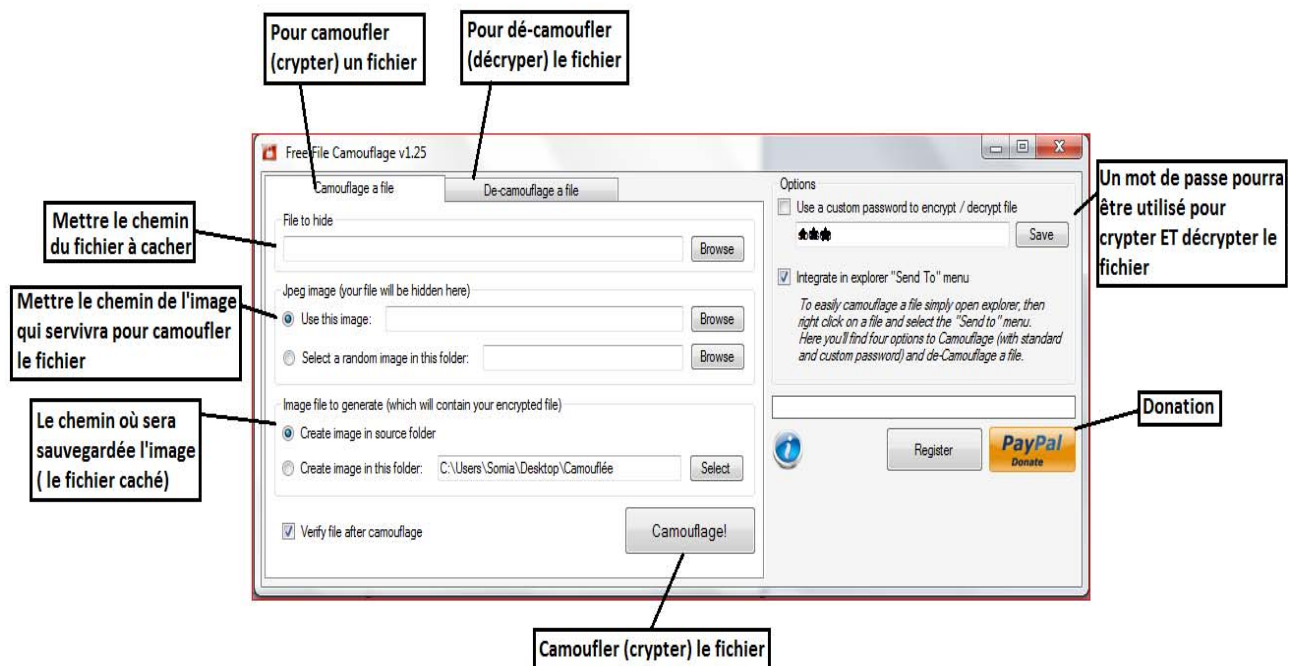
Sous Windows

Le logiciel doit être installé sous les environnements suivants : Windows XP, VISTA, 7, 8 (32 & 64 bit).

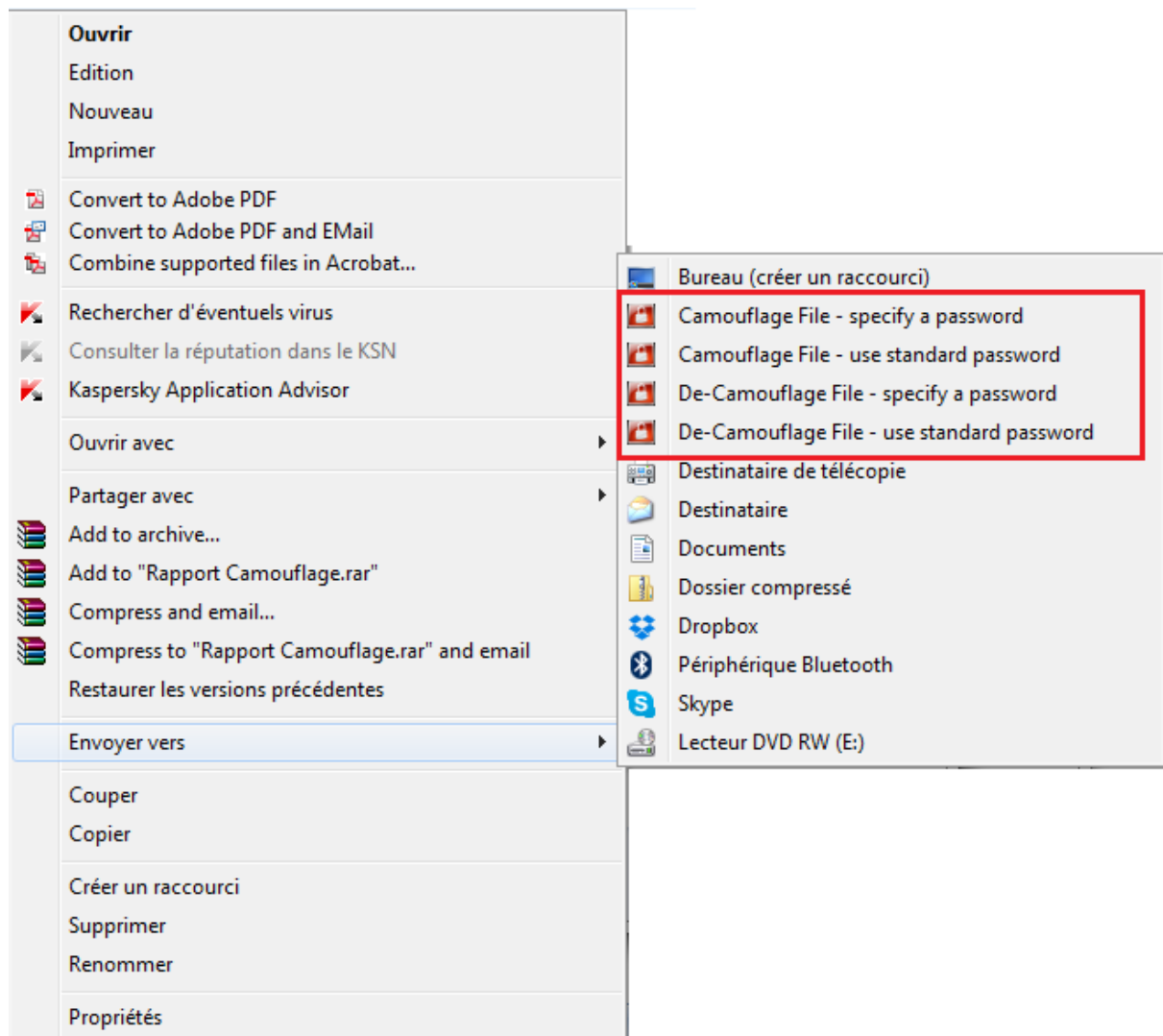
Il suffit de télécharger le logiciel du site www.myportablesoftware.com, il sera téléchargé sous format zip 'free_file_camouflage.zip', il faudra ensuite le dé-zipper. Une fois dé-zipper, un répertoire sera créé avec comme nom 'free_file_camouflage' contenant à l'intérieur le logiciel 'Free_File_Camouflage.exe' ainsi que deux fichiers texte : licence et readme



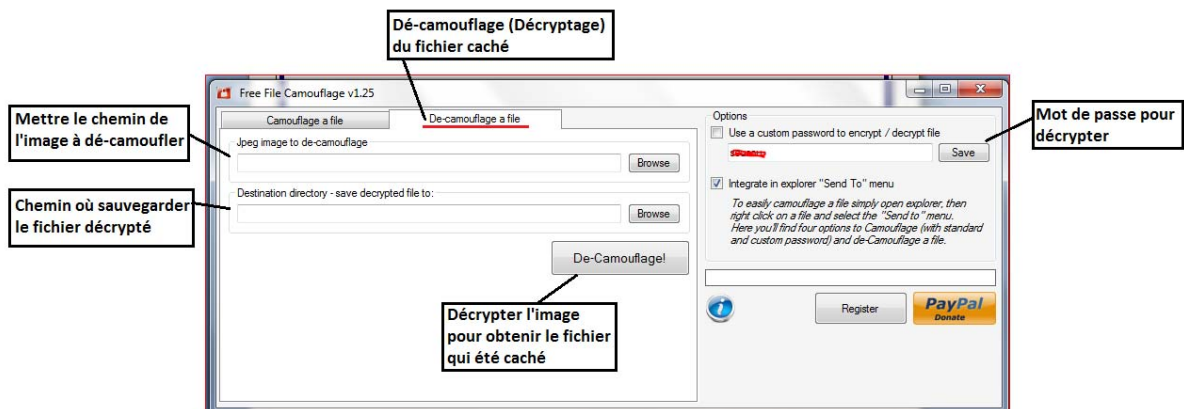
Pour le lancer, cliquer sur Free_File_Camouflage.exe



On remarque aussi qu'après le lancement du logiciel et en cliquant droit sur n'importe quel fichier sur l'ordinateur ensuite sur "Envoyer vers", on trouve la possibilité de camoufler un fichier avec un mot de passe spécifique, camoufler un fichier avec le mot de passe standard, dé-camoufler le fichier avec un mot de passe spécifique et dé-camoufler le fichier avec le mot de passe standard, comme il est montré dans l'image ci-dessous.



Pour décrypter ou dé-camoufler un fichier est aussi simple que le cryptage ; il suffit d'introduire le chemin de l'image contenant le fichier caché et le chemin d'où on veut sauvegarder le fichier une fois décrypter, introduire le mot de passe utilisé pour le cryptage de ce fichier (dans le cas d'utilisation d'un mot de passe) et finalement cliquer sur le bouton "De-Camouflage !", comme il est montré dans l'image ci dessous

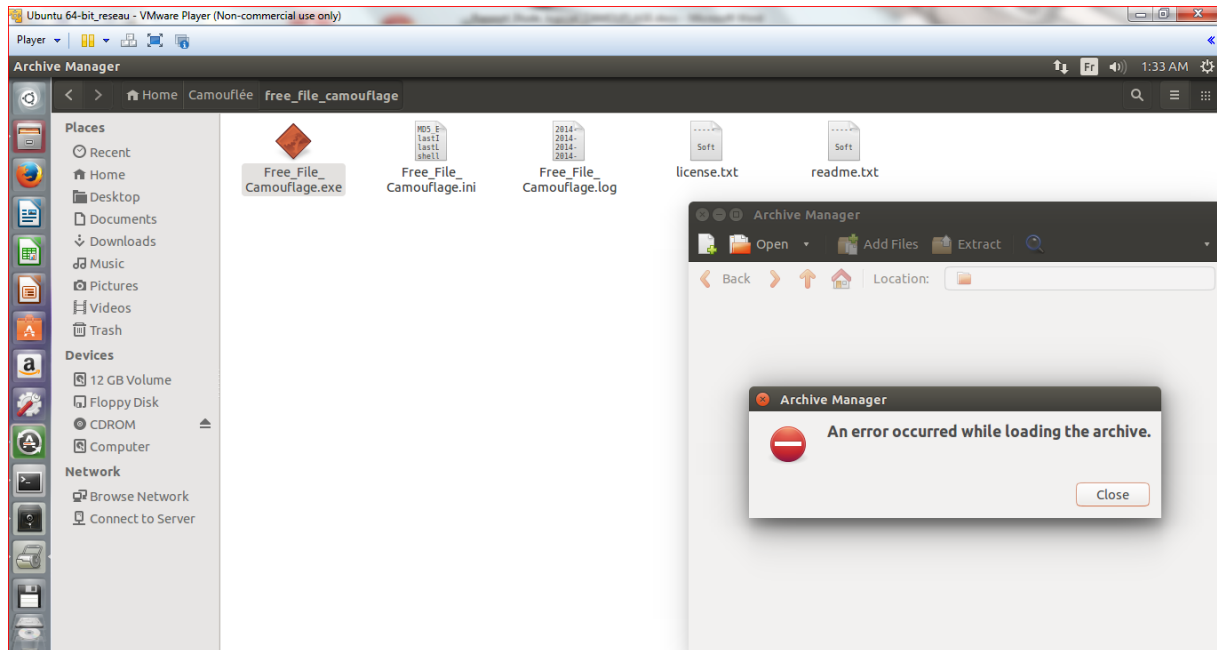


Une fois crypter un fichier, on s'aperçoit de la création d'un fichier dans le dossier "free_file_camouflage" qui est : Free_File_Camouflage.ini, contenant des informations sur la dernière utilisation du logiciel, la version du logiciel utilisé et d'autres informations.

```
Free_File_Camouflage.ini - Bloc-notes
Fichier  Edition  Format  Affichage  ?
MD5_EXE=jFCwMwMn6aUEFAjt7R5XaA==
lastInstalledVer=1.25
lastLaunched=2015-02-27
shellIntegration=Y
destDirCustom=C:\Users\Somia\Desktop\Camouflée
use_custom_PWD=N
custom_PWD=MRM7wizeZ40ubXLwRe3Ctw==
```

Sous Linux

Tout simplement sous Linux, le logiciel ne fonctionne pas.



Bien entendu y a d'autre méthode pour l'installer ; il existe des outils qui font fonctionner des programmes sous linux qui sont initialement conçu pour windows et vis versa.

Etude du logiciel

Sous Windows

L'étude a été faite sous une machine virtuelle hébergeant un windows server 2008 :

Ouvrir une fenêtre cygwin64 terminal et aller au répertoire contenant le logiciel free_file_camouflage

```
/cygdrive/c/Users/Administrator/Downloads/free_file_camouflage
Administrator@WIN-RSII2T1HA2E /cygdrive/c/Users/Administrator/Downloads/free_file_camouflage
$ ls
FFC_Windows Internals.001.jpg  Free_File_Camouflage.ini  readme.txt
Free_File_Camouflage.exe      license.txt                test.txt
```

- On essaie d'avoir les informations sur les sections en exécutant la commande : `objdump -h Free_File_Camouflage.exe`

`-h, --[section-]headers` Display the contents of the section headers

```
Administrator@WIN-RSII2T1HA2E /cygdrive/c/Users/Administrator/Downloads/free_file_camouflage
$ objdump -h Free_File_Camouflage.exe

Free_File_Camouflage.exe:      file format pei-i386

Sections:
Idx Name          Size      VMA       LMA       File off  Algn
  0 .text          00049c24  00402000  00402000  00000400  2**2
    CONTENTS, ALLOC, LOAD, READONLY, CODE
  1 .sdata         000000a3  0044c000  0044c000  0004a200  2**2
    CONTENTS, ALLOC, LOAD, DATA
  2 .rsrc          000013b8  0044e000  0044e000  0004a400  2**2
    CONTENTS, ALLOC, LOAD, READONLY, DATA
  3 .reloc         0000000c  00450000  00450000  0004b800  2**2
    CONTENTS, ALLOC, LOAD, READONLY, DATA
```

- Trouver les DLL requises pour le programme en tapant la commande : `objdump -x Free_File_Camouflage.exe`

`-x, --all-headers` Display the contents of all headers


```

/cygdrive/c/users/Administrator/Downloads/Free_file_camouflage
Administrator@WIN-RSII2T1HA2E /cygdrive/c/users/Administrator/Downloads/Free_file_camouflage
$ objdump -x Free_File_Camouflage.exe

Free_File_Camouflage.exe:      file format pei-i386
Free_File_Camouflage.exe
architecture: i386, flags 0x0000012f:
HAS_RELOC, EXEC_P, HAS_LINENO, HAS_DEBUG, HAS_LOCALS, D_PAGED
start address 0x0044bc1e

Characteristics 0x102
      executable
      32 bit words

Time/Date      Mon Nov  3 13:28:08 2014
Magic          010b      (PE32)
MajorLinkerVersion  8
MinorLinkerVersion  0
SizeOfCode        00049e00
SizeOfInitializedData 00001800
SizeOfUninitializedData 00000000
AddressOfEntryPoint 0004bc1e
BaseOfCode        00002000
BaseOfData        0004c000
ImageBase         00400000
SectionAlignment  00002000
FileAlignment     00000200
MajorOSSystemVersion  4
MinorOSSystemVersion  0
MajorImageVersion    0
MinorImageVersion    0
MajorSubsystemVersion 4
MinorSubsystemVersion 0
Win32Version        00000000
SizeOfImage        00052000
SizeOfHeaders      00000400
Checksum          00000000
Subsystem         00000002      (Windows GUI)
DllCharacteristics  00008540
SizeOfStackReserve 00100000
SizeOfStackCommit  00001000
SizeOfHeapReserve   00100000
SizeOfHeapCommit    00001000
LoaderFlags        00000000
NumberOfRvaAndSizes 00000010

```

```

The Data Directory
Entry 0 00000000 00000000 Export Directory [.edata (or where ever we found it)]
Entry 1 0004bbd0 0000004b Import Directory [parts of .idata]
Entry 2 0004e000 000013b8 Resource Directory [.rsrc]
Entry 3 00000000 00000000 Exception Directory [.pdata]
Entry 4 00000000 00000000 Security Directory
Entry 5 00050000 0000000c Base Relocation Directory [.reloc]
Entry 6 0004c000 0000001c Debug Directory
Entry 7 00000000 00000000 Description Directory
Entry 8 00000000 00000000 Special Directory
Entry 9 00000000 00000000 Thread Storage Directory [.tls]
Entry a 00000000 00000000 Load Configuration Directory
Entry b 00000000 00000000 Bound Import Directory
Entry c 00002000 00000008 Import Address Table Directory
Entry d 00000000 00000000 Delay Import Directory
Entry e 00002008 00000048 CLR Runtime Header
Entry f 00000000 00000000 Reserved

```

There is an import table in .text at 0x44bbd0

The Import Tables (interpreted .text section contents)

vma:	Hint Table	Time Stamp	Forward Chain	DLL Name	First Thunk
0004bbd0	0004bbf8	00000000	00000000	0004bc0e	00002000

DLL Name: mscoree.dll

vma:	Hint/Ord	Member-Name	Bound-To
4bc00	0	_CorExeMain	

0004bbe4	00000000	00000000	00000000	00000000	00000000
----------	----------	----------	----------	----------	----------

PE File Base Relocations (interpreted .reloc section contents)

```

Virtual Address: 0004b000 Chunk size 12 (0xc) Number of fixups 2
reloc 0 offset c20 [4bc20] HIGHLOW
reloc 1 offset 0 [4b000] ABSOLUTE

```

There is a debug directory in .sdata at 0x44c000

Type	Size	Rva	Offset
2	CodeView 00000087	0004c01c	0004a21c

(format RSDS signature ccdd829b7c1c4c1f8958725a8fadd45c age 1)

```

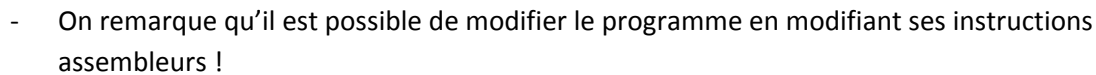
The .rsrc Resource Directory section:
000 Type Table: Char: 0, Time: 00000000, Ver: 0/0, Num Names: 0, IDs: 4
010 Entry: ID: 0x000003, Value: 0x80000030
030 Name Table: Char: 0, Time: 00000000, Ver: 0/0, Num Names: 0, IDs: 1
040 Entry: ID: 0x000002, Value: 0x80000090
090 Language Table: Char: 0, Time: 00000000, Ver: 0/0, Num Names: 0, IDs: 1
0a0 Entry: ID: 00000000, Value: 0x0000f0
0f0 Leaf: Addr: 0x04e508, Size: 0x000ca8, Codepage: 0
018 Entry: ID: 0x00000e, Value: 0x80000048
048 Name Table: Char: 0, Time: 00000000, Ver: 0/0, Num Names: 0, IDs: 1
058 Entry: ID: 0x007f00, Value: 0x800000a8
0a8 Language Table: Char: 0, Time: 00000000, Ver: 0/0, Num Names: 0, IDs: 1
0b8 Entry: ID: 00000000, Value: 0x000100
100 Leaf: Addr: 0x04f1b0, Size: 0x000014, Codepage: 0
020 Entry: ID: 0x000010, Value: 0x80000060
060 Name Table: Char: 0, Time: 00000000, Ver: 0/0, Num Names: 0, IDs: 1
070 Entry: ID: 0x000001, Value: 0x800000c0
0c0 Language Table: Char: 0, Time: 00000000, Ver: 0/0, Num Names: 0, IDs: 1
0d0 Entry: ID: 00000000, Value: 0x000110
110 Leaf: Addr: 0x04e130, Size: 0x0003d4, Codepage: 0
028 Entry: ID: 0x000018, Value: 0x80000078
078 Name Table: Char: 0, Time: 00000000, Ver: 0/0, Num Names: 0, IDs: 1
088 Entry: ID: 0x000001, Value: 0x800000d8
0d8 Language Table: Char: 0, Time: 00000000, Ver: 0/0, Num Names: 0, IDs: 1
0e8 Entry: ID: 00000000, Value: 0x000120
120 Leaf: Addr: 0x04f1c8, Size: 0x0001ea, Codepage: 0
Resources start at 508x

Sections:
Idx Name          Size      VMA      LMA      File off  Algn
  0 .text          00049c24 00402000 00402000 00000400 2**2
  1 .sdata         000000a3 0044c000 0044c000 0004a200 2**2
  2 .rsrc          000013b8 0044e000 0044e000 0004a400 2**2
  3 .reloc         0000000c 00450000 00450000 0004b800 2**2
                CONTENTS, ALLOC, LOAD, READONLY, DATA
SYMBOL TABLE:
no symbols

```

On remarque que l'application utilise une DLL : mscoree.dll

- Ouvrir le programme avec le logiciel "OllyDbg"



Dans cette section, on peut remarquer tous les registres ainsi que leurs contenus

```

Registers (FPU)
EAX 6F53510B MSCOREE.6F53510B
ECX 6F550065 ASCII "lCanUnLoadNowInternal"
EDX 6F53510A UNICODE "ersion"
EBX 7EFD0000
ESP 0030F724
EBP 0030F7AC
ESI 6F535108 UNICODE "Version"
EDI 00000000
EIP 6F53488B MSCOREE.6F53488B
C 0 ES 002B 32bit 0(FFFFFFFF)
P 0 CS 0023 32bit 0(FFFFFFFF)
A 0 SS 002B 32bit 0(FFFFFFFF)
Z 0 DS 002B 32bit 0(FFFFFFFF)
S 0 FS 0053 32bit 7EFD0000(FFF)
T 0 GS 002B 32bit 0(FFFFFFFF)
D 0
O 0 LastErr 00000000 ERROR_SUCCESS
EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)
ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 (GT)
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1
Last cmd 0000:00000000
VMX 0 0 0 0 0 0 0 0

```

- Là, on peut voir les modules exécutables

Base	Size	Entry	Name	Type	File version	Static links	Path
77D00000	00100000		ntdll		6.1.7600.16385		C:\Windows\SysWOW64\
77310000	00110000	773235C8	KERNEL32		6.1.7600.17179		C:\Windows\syswow64\
012F0000	00052000	0133BC1E	Free_File_Camou	.NET	1.25.0.0		C:\Users\Administrat
75070000	00040000	75072E54	MSCOREE		4.0.31106.0 (Ma		C:\Windows\SYSTEM32\
77160000	00047000	771674B1	KERNELBASE		6.1.7600.17179		C:\Windows\syswow64\
75000000	???		Mod_7500	Hidden			
752F0000	???		Mod_752F	Hidden			
75360000	???		Mod_7536	Hidden			
77B20000	???		Mod_77B2	Hidden			

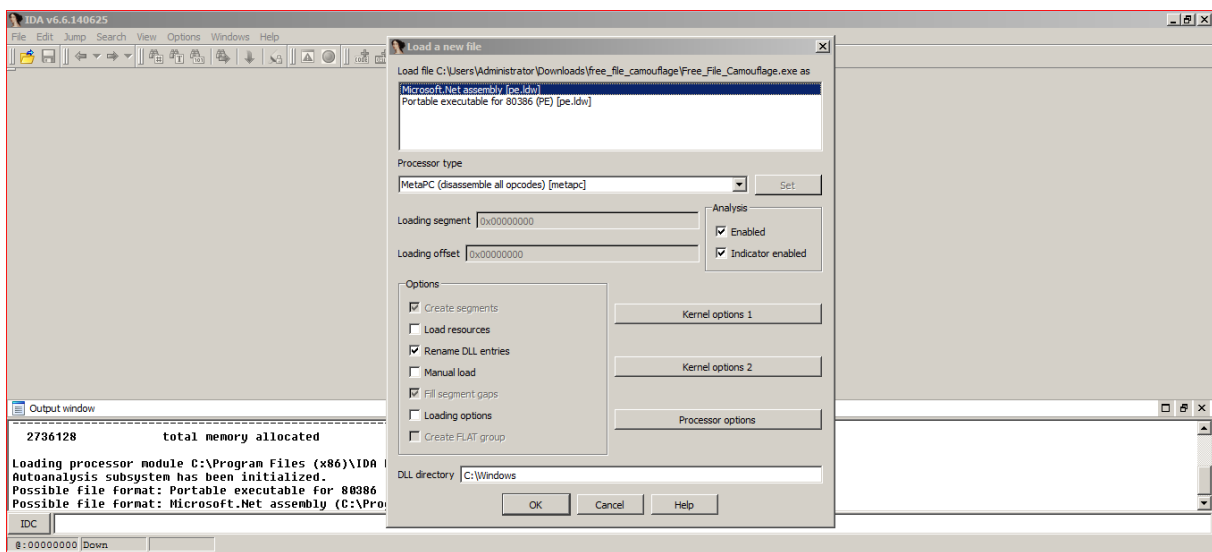
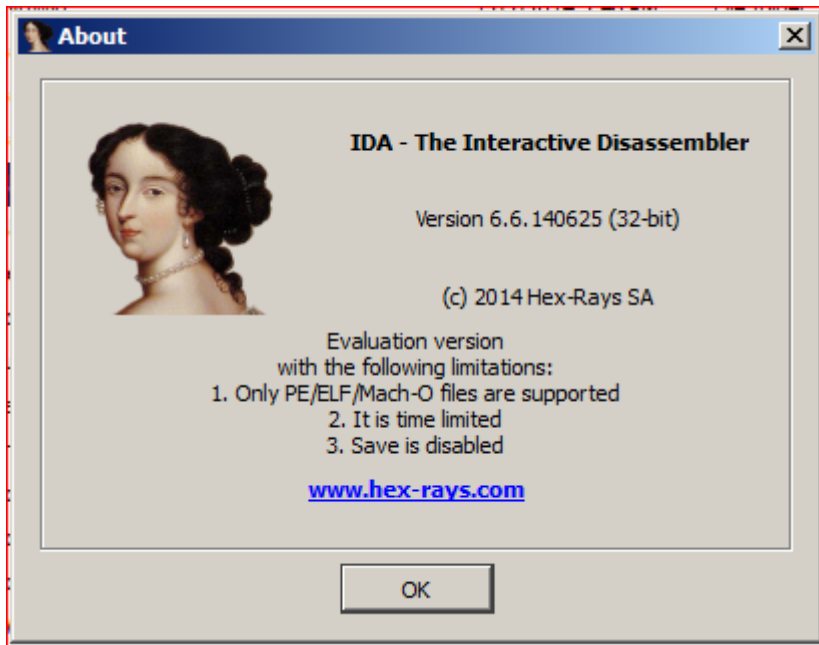
- L'exécution du programme à partir d'OllyDbg a commencé mais s'est arrêtée avec une erreur disant Exception E0434F4D et on remarque que cette valeur été dans le registre EBX !

OllyDbg - Free_File_Camouflage.exe - [CPU - main thread, module KERNELBASE]

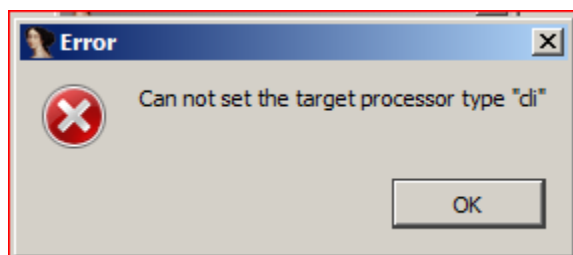
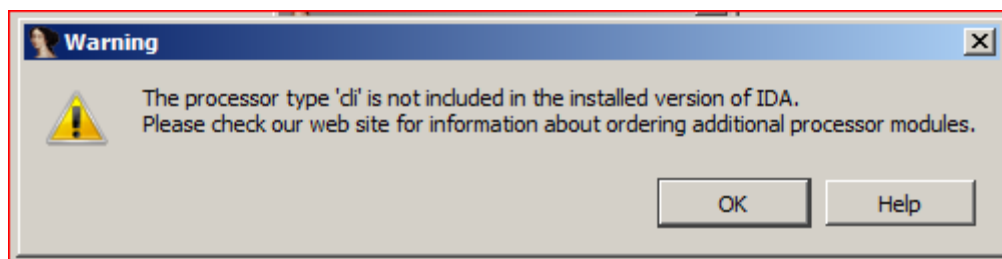
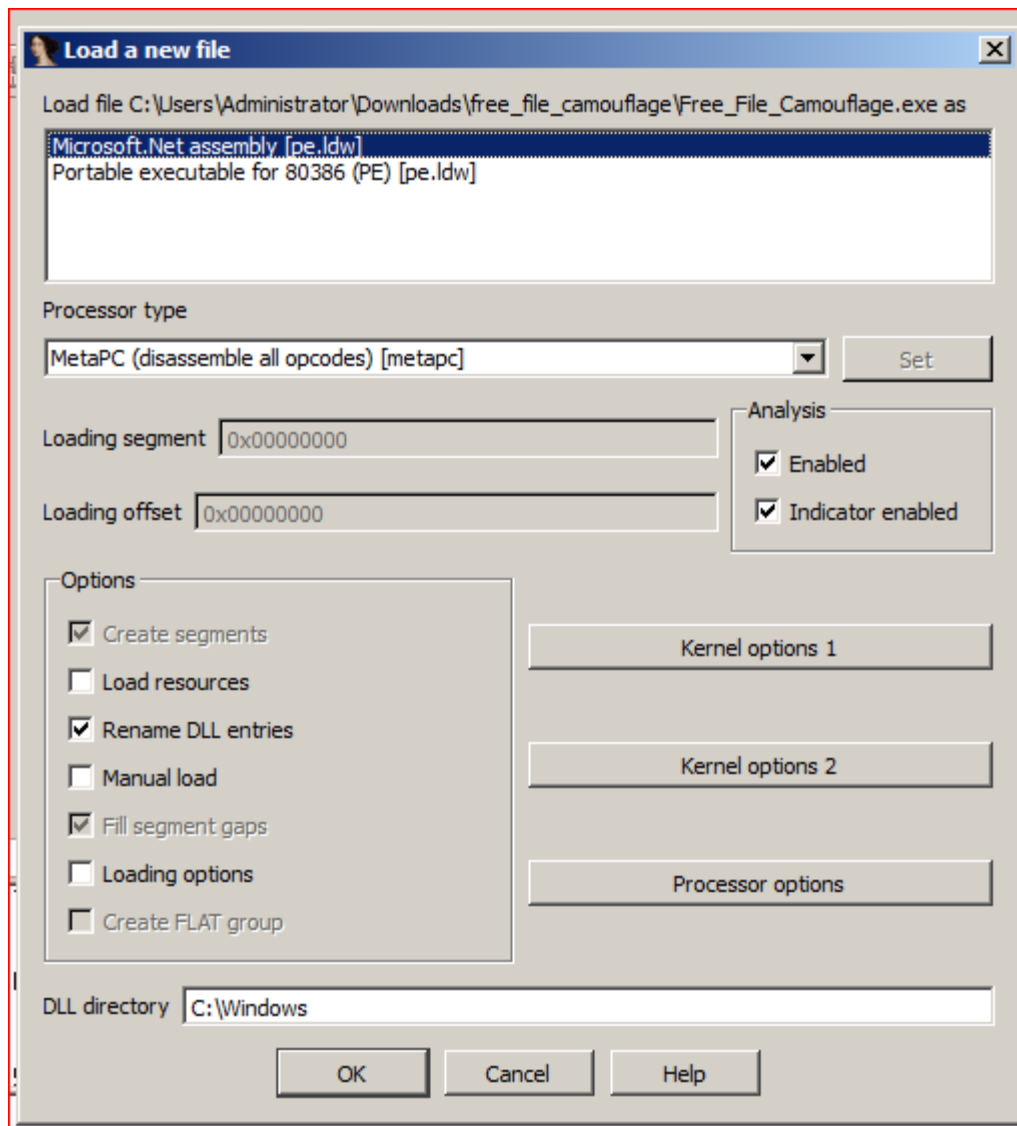
File View Debug Trace Plugins Options Windows Help

7716C3F5 JBE SHORT 7716C3FA
7716C3F7 POP EAX
7716C3F9 MOV DWORD PTR SS:[EBP+40],EAX
7716C3FD C1EB 02 SHL EBX,2
7716C400 JBE SHORT 7716C401
7716C401 PUSH DWORD PTR SS:[EBP+14]
7716C404 LEA EDI,[EBP+3C]
7716C407 PUSH EAX
7716C409 MOV ESP,EIP
7716C40B CALL Jmp.tntdll.nency
7716C40D JBE SHORT 7716C410
7716C410 JMP SHORT 7716C415
7716C412 MOV DWORD PTR SS:[EBP+40],EAX
7716C415 LEA EDI,[EBP+60]
7716C418 PUSH EAX
7716C419 CDB 00000000
7716C41B CDB 00000000
7716C41D CDB 00000000
7716C41F CDB 00000000
7716C421 CDB 00000000
7716C423 CDB 00000000
7716C425 CDB 00000000
7716C427 CDB 00000000
7716C429 CDB 00000000
7716C42B CDB 00000000
7716C42D CDB 00000000
7716C42F CDB 00000000
7716C431 CDB 00000000
7716C433 CDB 00000000
7716C435 CDB 00000000
7716C437 CDB 00000000
7716C439 CDB 00000000
7716C43B CDB 00000000
7716C43D CDB 00000000
7716C43F CDB 00000000
7716C441 CDB 00000000
7716C443 CDB 00000000
7716C445 CDB 00000000
7716C447 CDB 00000000
7716C449 CDB 00000000
7716C44B CDB 00000000
7716C44D CDB 00000000
7716C44F CDB 00000000
7716C451 CDB 00000000
7716C453 CDB 00000000
7716C455 CDB 00000000
7716C457 CDB 00000000
7716C459 CDB 00000000
7716C45B CDB 00000000
7716C45D CDB 00000000
7716C45F CDB 00000000
7716C461 CDB 00000000
7716C463 CDB 00000000
7716C465 CDB 00000000
7716C467 CDB 00000000
7716C469 CDB 00000000
7716C46B CDB 00000000
7716C46D CDB 00000000
7716C46F CDB 00000000
7716C471 CDB 00000000
7716C473 CDB 00000000
7716C475 CDB 00000000
7716C477 CDB 00000000
7716C479 CDB 00000000
7716C47B CDB 00000000
7716C47D CDB 00000000
7716C47F CDB 00000000
7716C481 CDB 00000000
7716C483 CDB 00000000
7716C485 CDB 00000000
7716C487 CDB 00000000
7716C489 CDB 00000000
7716C48B CDB 00000000
7716C48D CDB 00000000
7716C48F CDB 00000000
7716C491 CDB 00000000
7716C493 CDB 00000000
7716C495 CDB 00000000
7716C497 CDB 00000000
7716C499 CDB 00000000
7716C49B CDB 00000000
7716C49D CDB 00000000
7716C49F CDB 00000000
7716C4A1 CDB 00000000
7716C4A3 CDB 00000000
7716C4A5 CDB 00000000
7716C4A7 CDB 00000000
7716C4A9 CDB 00000000
7716C4AB CDB 00000000
7716C4AD CDB 00000000
7716C4AF CDB 00000000
7716C4B1 CDB 00000000
7716C4B3 CDB 00000000
7716C4B5 CDB 00000000
7716C4B7 CDB 00000000
7716C4B9 CDB 00000000
7716C4BB CDB 00000000
7716C4BD CDB 00000000
7716C4BF CDB 00000000
7716C4C1 CDB 00000000
7716C4C3 CDB 00000000
7716C4C5 CDB 00000000
7716C4C7 CDB 00000000
7716C4C9 CDB 00000000
7716C4CB CDB 00000000
7716C4CD CDB 00000000
7716C4CF CDB 00000000
7716C4D1 CDB 00000000
7716C4D3 CDB 00000000
7716C4D5 CDB 00000000
7716C4D7 CDB 00000000
7716C4D9 CDB 00000000
7716C4DB CDB 00000000
7716C4DD CDB 00000000
7716C4DF CDB 00000000
7716C4E1 CDB 00000000
7716C4E3 CDB 00000000
7716C4E5 CDB 00000000
7716C4E7 CDB 00000000
7716C4E9 CDB 00000000
7716C4EB CDB 00000000
7716C4ED CDB 00000000
7716C4EF CDB 00000000
7716C4F1 CDB 00000000
7716C4F3 CDB 00000000
7716C4F5 CDB 00000000
7716C4F7 CDB 00000000
7716C4F9 CDB 00000000
7716C4FB CDB 00000000
7716C4FD CDB 00000000
7716C4FF CDB 00000000
7716C501 CDB 00000000
7716C503 CDB 00000000
7716C505 CDB 00000000
7716C507 CDB 00000000
7716C509 CDB 00000000
7716C50B CDB 00000000
7716C50D CDB 00000000
7716C50F CDB 00000000
7716C511 CDB 00000000
7716C513 CDB 00000000
7716C515 CDB 00000000
7716C517 CDB 00000000
7716C519 CDB 00000000
7716C51B CDB 00000000
7716C51D CDB 00000000
7716C51F CDB 00000000
7716C521 CDB 00000000
7716C523 CDB 00000000
7716C525 CDB 00000000
7716C527 CDB 00000000
7716C529 CDB 00000000
7716C52B CDB 00000000
7716C52D CDB 00000000
7716C52F CDB 00000000
7716C531 CDB 00000000
7716C533 CDB 00000000
7716C535 CDB 00000000
7716C537 CDB 00000000
7716C539 CDB 00000000
7716C53B CDB 00000000
7716C53D CDB 00000000
7716C53F CDB 00000000
7716C541 CDB 00000000
7716C543 CDB 00000000
7716C545 CDB 00000000
7716C547 CDB 00000000
7716C549 CDB 00000000
7716C54B CDB 00000000
7716C54D CDB 00000000
7716C54F CDB 00000000
7716C551 CDB 00000000
7716C553 CDB 00000000
7716C555 CDB 00000000
7716C557 CDB 00000000
7716C559 CDB 00000000
7716C55B CDB 00000000
7716C55D CDB 00000000
7716C55F CDB 00000000
7716C561 CDB 00000000
7716C563 CDB 00000000
7716C565 CDB 00000000
7716C567 CDB 00000000
7716C569 CDB 00000000
7716C56B CDB 00000000
7716C56D CDB 00000000
7716C56F CDB 00000000
7716C571 CDB 00000000
7716C573 CDB 00000000
7716C575 CDB 00000000
7716C577 CDB 00000000
7716C579 CDB 00000000
7716C57B CDB 00000000
7716C57D CDB 00000000
7716C57F CDB 00000000
7716C581 CDB 00000000
7716C583 CDB 00000000
7716C585 CDB 00000000
7716C587 CDB 00000000
7716C589 CDB 00000000
7716C58B CDB 00000000
7716C58D CDB 00000000
7716C58F CDB 00000000
7716C591 CDB 00000000
7716C593 CDB 00000000
7716C595 CDB 00000000
7716C597 CDB 00000000
7716C599 CDB 00000000
7716C59B CDB 00000000
7716C59D CDB 00000000
7716C59F CDB 00000000
7716C5A1 CDB 00000000
7716C5A3 CDB 00000000
7716C5A5 CDB 00000000
7716C5A7 CDB 00000000
7716C5A9 CDB 00000000
7716C5AB CDB 00000000
7716C5AD CDB 00000000
7716C5AF CDB 00000000
7716C5B1 CDB 00000000
7716C5B3 CDB 00000000
7716C5B5 CDB 00000000
7716C5B7 CDB 00000000
7716C5B9 CDB 00000000
7716C5BB CDB 00000000
7716C5BD CDB 00000000
7716C5BF CDB 00000000
7716C5C1 CDB 00000000
7716C5C3 CDB 00000000
7716C5C5 CDB 00000000
7716C5C7 CDB 00000000
7716C5C9 CDB 00000000
7716C5CB CDB 00000000
7716C5CD CDB 00000000
7716C5CF CDB 00000000
7716C5D1 CDB 00000000
7716C5D3 CDB 00000000
7716C5D5 CDB 00000000
7716C5D7 CDB 00000000
7716C5D9 CDB 00000000
7716C5DB CDB 00000000
7716C5DD CDB 00000000
7716C5DF CDB 00000000
7716C5E1 CDB 00000000
7716C5E3 CDB 00000000
7716C5E5 CDB 00000000
7716C5E7 CDB 00000000
7716C5E9 CDB 00000000
7716C5EB CDB 00000000
7716C5ED CDB 00000000
7716C5EF CDB 00000000
7716C5F1 CDB 00000000
7716C5F3 CDB 00000000
7716C5F5 CDB 00000000
7716C5F7 CDB 00000000
7716C5F9 CDB 00000000
7716C5FB CDB 00000000
7716C5FD CDB 00000000
7716C5FF CDB 00000000
7716C601 CDB 00000000
7716C603 CDB 00000000
7716C605 CDB 00000000
7716C607 CDB 00000000
7716C609 CDB 00000000
7716C60B CDB 00000000
7716C60D CDB 00000000
7716C60F CDB 00000000
7716C611 CDB 00000000
7716C613 CDB 00000000
7716C615 CDB 00000000
7716C617 CDB 00000000
7716C619 CDB 00000000
7716C61B CDB 00000000
7716C61D CDB 00000000
7716C61F CDB 00000000
7716C621 CDB 00000000
7716C623 CDB 00000000
7716C625 CDB 00000000
7716C627 CDB 00000000
7716C629 CDB 00000000
7716C62B CDB 00000000
7716C62D CDB 00000000
7716C62F CDB 00000000
7716C631 CDB 00000000
7716C633 CDB 00000000
7716C635 CDB 00000000
7716C637 CDB 00000000
7716C639 CDB 00000000
7716C63B CDB 00000000
7716C63D CDB 00000000
7716C63F CDB 00000000
7716C641 CDB 00000000
7716C643 CDB 00000000
7716C645 CDB 00000000
7716C647 CDB 00000000
7716C649 CDB 00000000
7716C64B CDB 00000000
7716C64D CDB 00000000
7716C64F CDB 00000000
7716C651 CDB 00000000
7716C653 CDB 00000000
7716C655 CDB 00000000
7716C657 CDB 00000000
7716C659 CDB 00000000
7716C65B CDB 00000000
7716C65D CDB 00000000
7716C65F CDB 00000000
7716C661 CDB 00000000
7716C663 CDB 00000000
7716C665 CDB 00000000
7716C667 CDB 00000000
7716C669 CDB 00000000
7716C66B CDB 00000000
7716C66D CDB 00000000
7716C66F CDB 00000000
7716C671 CDB 00000000
7716C673 CDB 00000000
7716C675 CDB 00000000
7716C677 CDB 00000000
7716C679 CDB 00000000
7716C67B CDB 00000000
7716C67D CDB 00000000
7716C67F CDB 00000000
7716C681 CDB 00000000
7716C683 CDB 00000000
7716C685 CDB 00000000
7716C687 CDB 00000000
7716C689 CDB 00000000
7716C68B CDB 00000000
7716C68D CDB 00000000
7716C68F CDB 00000000
7716C691 CDB 00000000
7716C693 CDB 00000000
7716C695 CDB 00000000
7716C697 CDB 00000000
7716C699 CDB 00000000
7716C69B CDB 00000000
7716C69D CDB 00000000
7716C69F CDB 00000000
7716C6A1 CDB 00000000
7716C6A3 CDB 00000000
7716C6A5 CDB 00000000
7716C6A7 CDB 00000000
7716C6A9 CDB 00000000
7716C6AB CDB 00000000
7716C6AD CDB 00000000
7716C6AF CDB 00000000
7716C6B1 CDB 00000000
7716C6B3 CDB 00000000
7716C6B5 CDB 00000000
7716C6B7 CDB 00000000
7716C6B9 CDB 00000000
7716C6BB CDB 00000000
7716C6BD CDB 00000000
7716C6BF CDB 00000000
7716C6C1 CDB 00000000
7716C6C3 CDB 00000000
7716C6C5 CDB 00000000
7716C6C7 CDB 00000000
7716C6C9 CDB 00000000
7716C6CB CDB 00000000
7716C6CD CDB 00000000
7716C6CF CDB 00000000
7716C6D1 CDB 00000000
7716C6D3 CDB 00000000
7716C6D5 CDB 00000000
7716C6D7 CDB 00000000
7716C6D9 CDB 00000000
7716C6DB CDB 00000000
7716C6DD CDB 00000000
7716C6DF CDB 00000000
7716C6E1 CDB 00000000
7716C6E3 CDB 00000000
7716C6E5 CDB 00000000
7716C6E7 CDB 00000000
7716C6E9 CDB 00000000
7716C6EB CDB 00000000
7716C6ED CDB 00000000
7716C6EF CDB 00000000
7716C6F1 CDB 00000000
7716C6F3 CDB 00000000
7716C6F5 CDB 00000000
7716C6F7 CDB 00000000
7716C6F9 CDB 00000000
7716C6FB CDB 00000000
7716C6FD CDB 00000000
7716C6FF CDB 00000000
7716C701 CDB 00000000
7716C703 CDB 00000000
7716C705 CDB 00000000
7716C707 CDB 00000000
7716C709 CDB 00000000
7716C70B CDB 00000000
7716C70D CDB 00000000
7716C70F CDB 00000000
7716C711 CDB 00000000
7716C713 CDB 00000000
7716C715 CDB 00000000
7716C717 CDB 00000000
7716C719 CDB 00000000
7716C71B CDB 00000000
7716C71D CDB 00000000
7716C71F CDB 00000000
7716C721 CDB 00000000
7716C723 CDB 00000000
7716C725 CDB 00000000
7716C727 CDB 00000000
7716C729 CDB 00000000
7716C72B CDB 00000000
7716C72D CDB 00000000
7716C72F CDB 00000000
7716C731 CDB 00000000
7716C733 CDB 00000000
7716C735 CDB 00000000
7716C737 CDB 00000000
7716C739 CDB 00000000
7716C73B CDB 00000000
7716C73D CDB 00000000
7716C73F CDB 00000000
7716C741 CDB 00000000
7716C743 CDB 00000000
7716C745 CDB 00000000
7716C747 CDB 00000000
7716C749 CDB 00000000
7716C74B CDB 00000000
7716C74D CDB 00000000
7716C74F CDB 00000000
7716C751 CDB 00000000
7716C753 CDB 00000000
7716C755 CDB 00000000
7716C757 CDB 00000000
7716C759 CDB 00000000
7716C75B CDB 00000000
7716C75D CDB 00000000
7716C75F CDB 00000000
7716C761 CDB 00000000
7716C763 CDB 00000000
7716C765 CDB 00000000
7716C767 CDB 00000000
7716C769 CDB 00000000
7716C76B CDB 00000000
7716C76D CDB 00000000
7716C76F CDB 00000000
7716C771 CDB 00000000
7716C773 CDB 00000000
7716C775 CDB 00000000
7716C777 CDB 00000000
7716C779 CDB 00000000
7716C77B CDB 00000000
7716C77D CDB 00000000
7716C77F CDB 00000000
7716C781 CDB 00000000
7716C783 CDB 00000000
7716C785 CDB 00000000
7716C787 CDB 00000000
7716C789 CDB 00000000
7716C78B CDB 00000000
7716C78D CDB 00000000
7716C78F CDB 00000000
7716C791 CDB 00000000
7716C793 CDB 00000000
7716C795 CDB 00000000
7716C797 CDB 00000000
7716C799 CDB 00000000
7716C79B CDB 00000000
7716C79D CDB 00000000
7716C79F CDB 00000000
7716C7A1 CDB 00000000
7716C7A3 CDB 00000000
7716C7A5 CDB 00000000
7716C7A7 CDB 00000000
7716C7A9 CDB 00000000
7716C7AB CDB 00000000
7716C7AD CDB 00000000
7716C7AF CDB 00000000
7716C7B1 CDB 00000000
7716C7B3 CDB 00000000
7716C7B5 CDB 00000000
7716C7B7 CDB 00000000
7716C7B9 CDB 00000000
7716C7BB CDB 00000000
7716C7BD CDB 00000000
7716C7BF CDB 00000000
7716C7C1 CDB 00000000
7716C7C3 CDB 00000000
7716C7C5 CDB 00000000
7716C7C7 CDB 00000000
7716C7C9 CDB 00000000
7716C7CB CDB 00000000
7716C7CD CDB 00000000
7716C7CF CDB 00000000
7716C7D1 CDB 00000000
7716C7D3 CDB 00000000
7716C7D5 CDB 00000000
7716C7D7 CDB 00000000
7716C7D9 CDB 00000000
7716C7DB CDB 00000000
7716C7DD CDB 00000000
7716C7DF CDB 00000000
7716C7E1 CDB 00000000
7716C7E3 CDB 00000000
7716C7E5 CDB 00000000
7716C7E7 CDB 00000000
7716C7E9 CDB 00000000
7716C7EB CDB 00000000
7716C7ED CDB 00000000
7716C7EF CDB 00000000
7716C7F1 CDB 00000000
7716C7F3 CDB 00000000
7716C7F5 CDB 00000000
7716C7F7 CDB 00000000
7716C7F9 CDB 00000000
7716C7FB CDB 00000000
7716C7FD CDB 00000000
7716C7FF CDB 00000000
7716C801 CDB 00000000
7716C803 CDB 00000000
7716C805 CDB 00000000
7716C807 CDB 00000000
7716C809

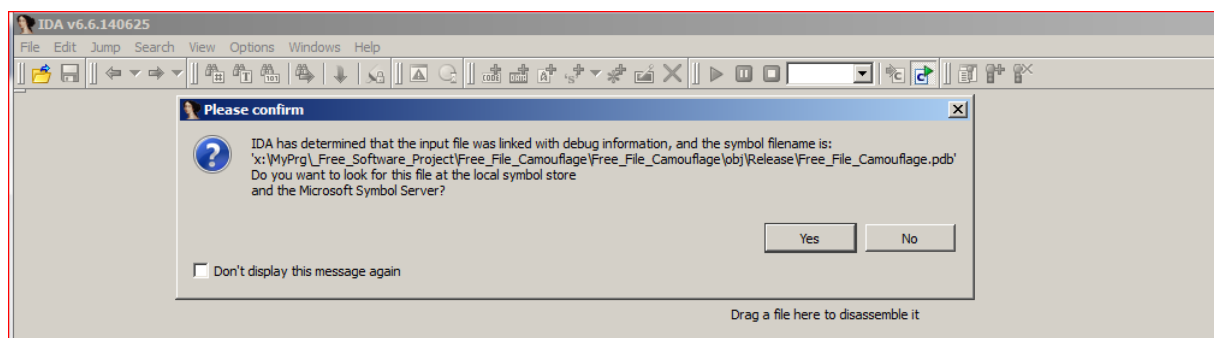
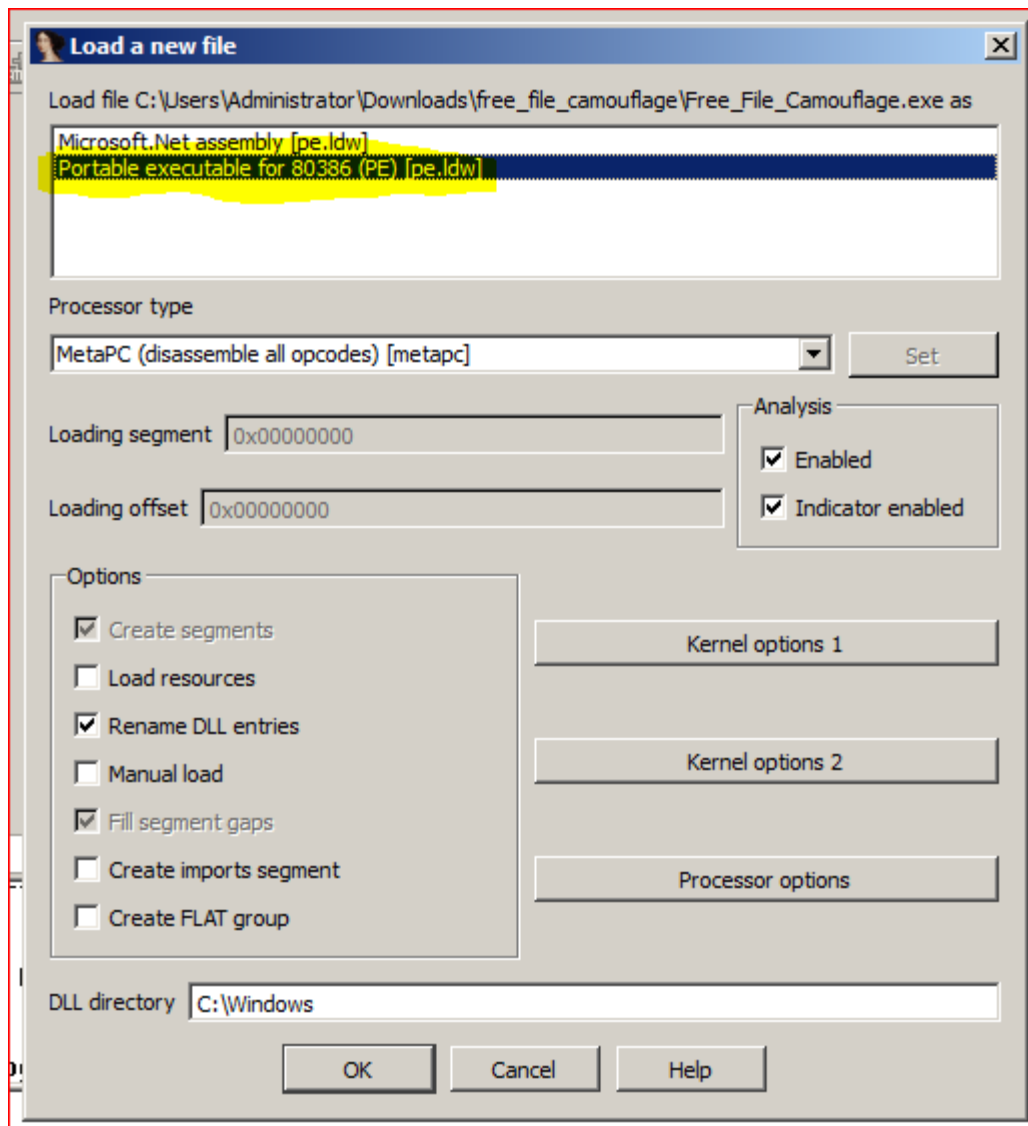
- Ouvrir le programme avec le logiciel "IDA Demo v6.6"

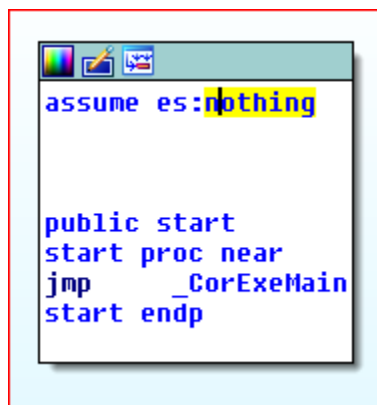
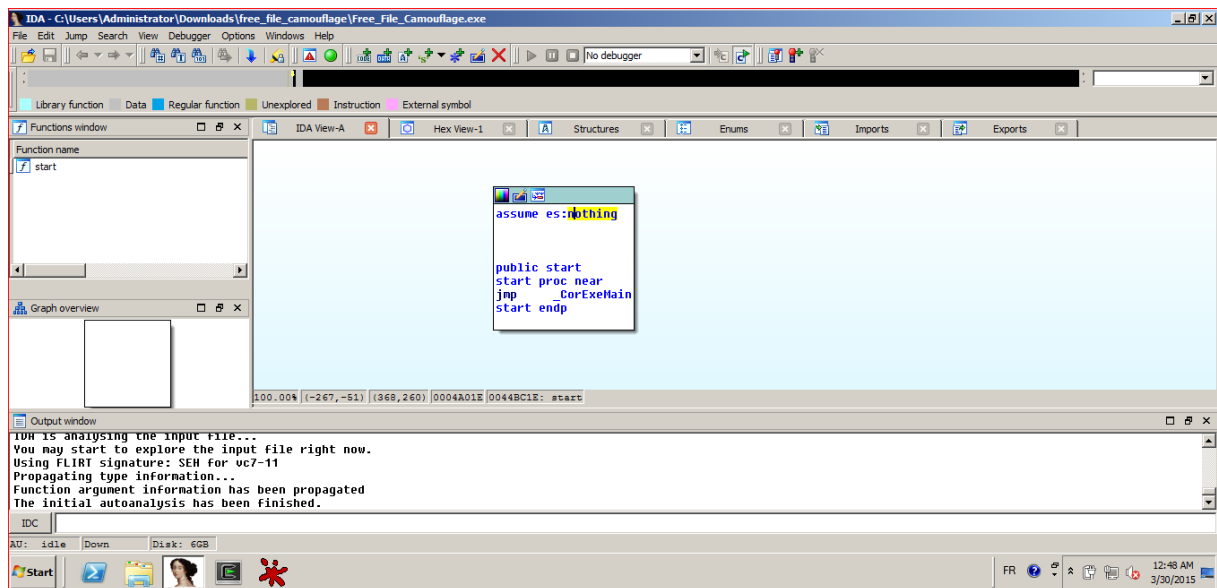


Le lancement du programme avec IDA Demo comme étant « Microsoft.Net assembly » n'a pas fonctionné, et affiche un message d'erreur comme il est mentionné ci dessous

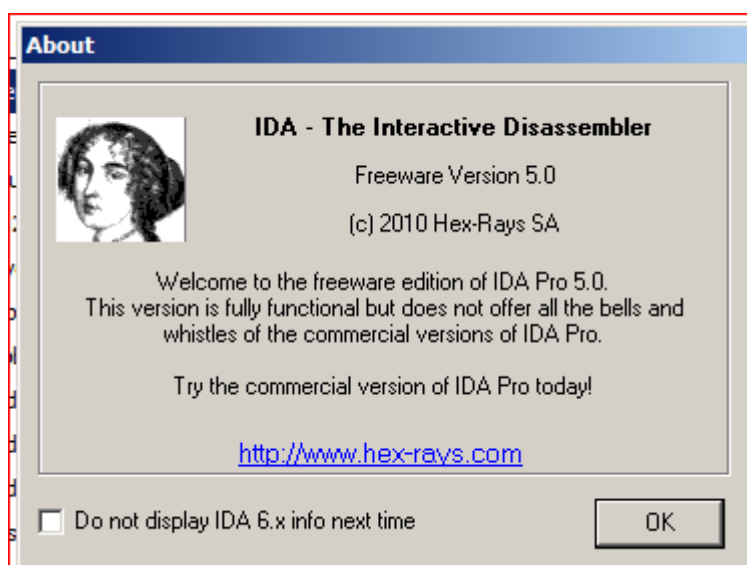


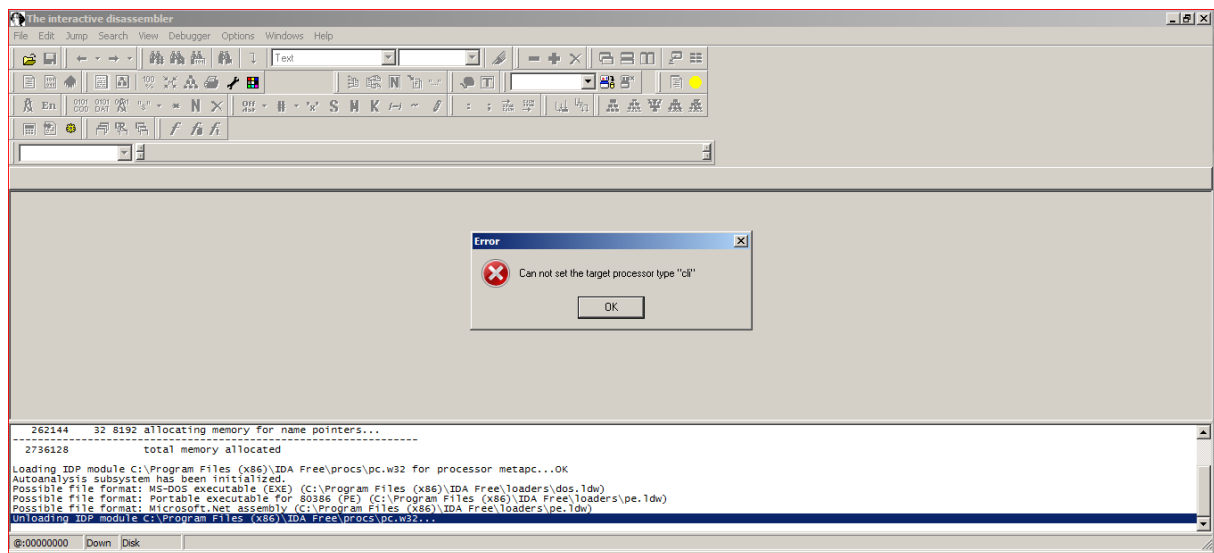
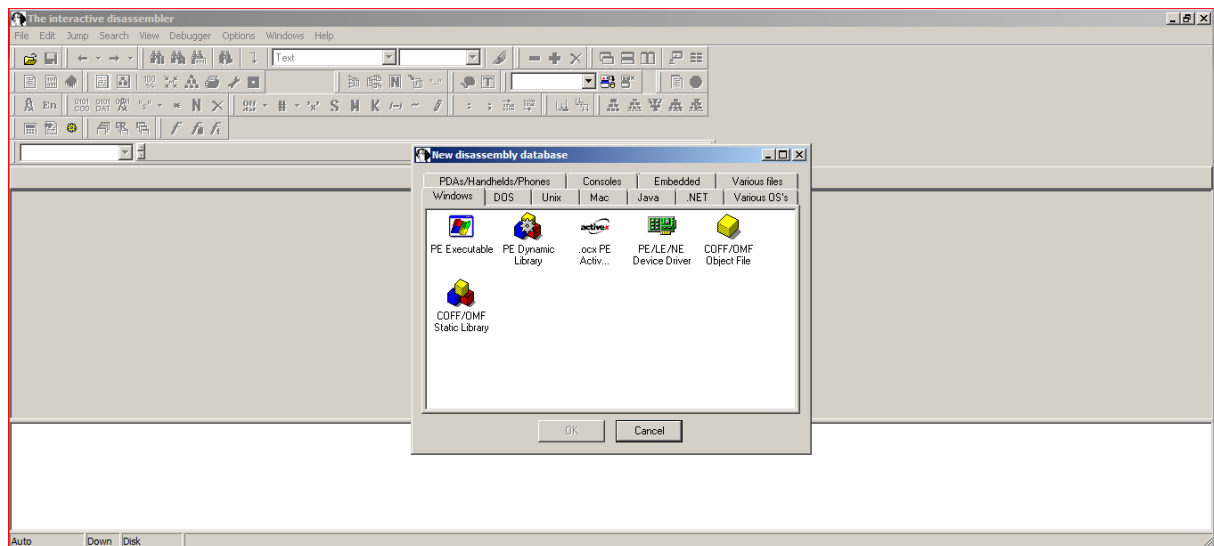
Mais en choisissant le mode "Portable executable for 80386 (PE)" comme il est montré dans l'image ci-dessous, le programme a marché



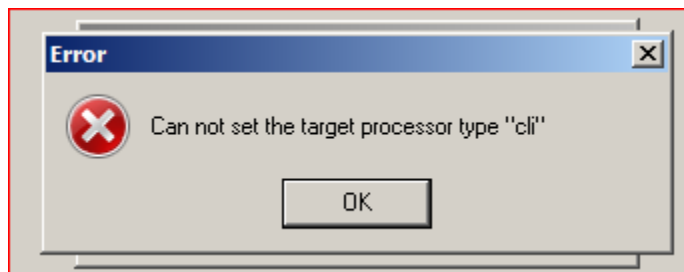
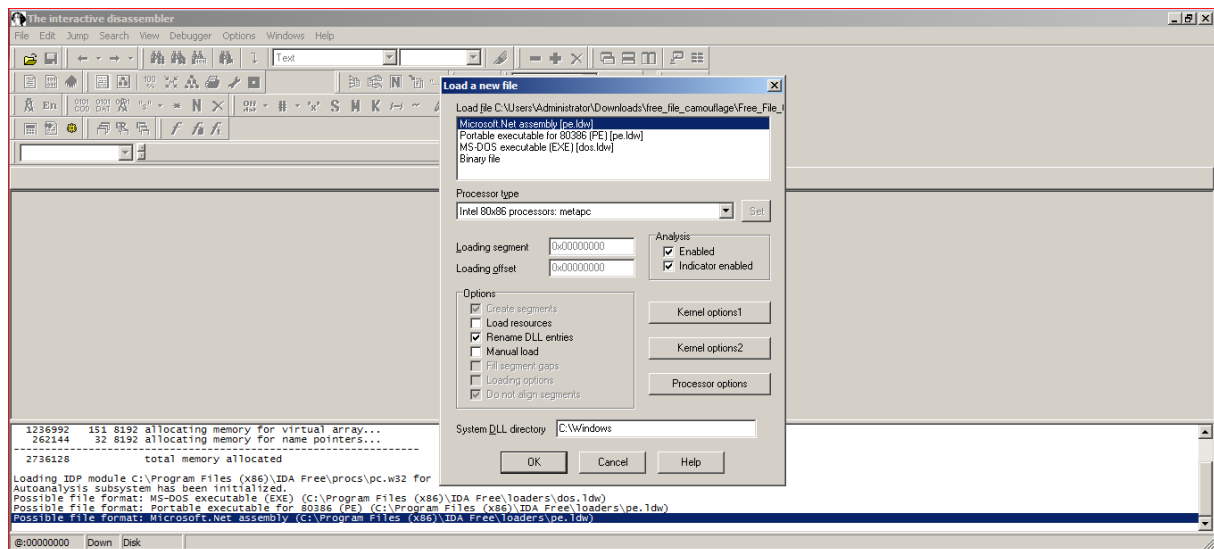


- Ouvrir le programme avec « IDA Pro Free »

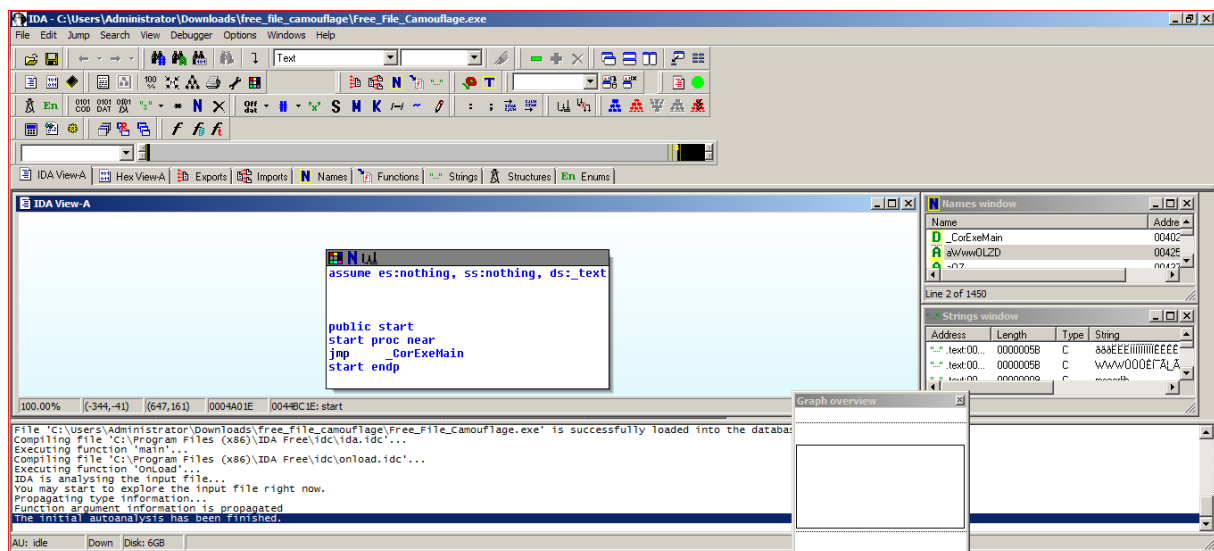




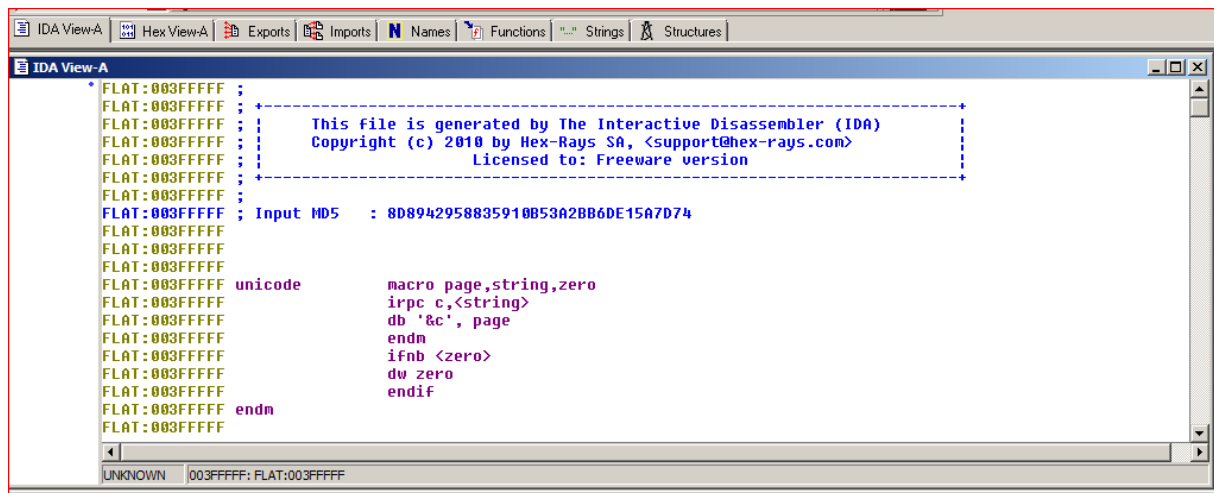
Même chose que tout à l'heure, le lancement du programme comme étant « Microsoft.Net assembly » n'a pas fonctionné, et affiche un message d'erreur comme il est mentionné ci dessous



Mais en choisissant « Portable executable for 80386 », ça fonctionne



Ce que j'ai put faire à partir de là, c'est récupérer tous le code « le programme désassemble »



Le code est en pièce jointe nommé « IDA_programme »

Sous Linux

Malgré que le programme ne marche pas sous linux, ceci dit, on est resté sous linux pour effectuer les opérations suivantes essayant de comprendre au mieux le logiciel.

En premier lieu, on a camouflé un fichier .pdf sous une image s'appelant 'FFC_images.jpg', on a téléchargé du net la même image (mais sans le document caché à l'intérieur bien entendu) image_google_1.jpg et image_google_2.jpg; on a mis le tous le même répertoire

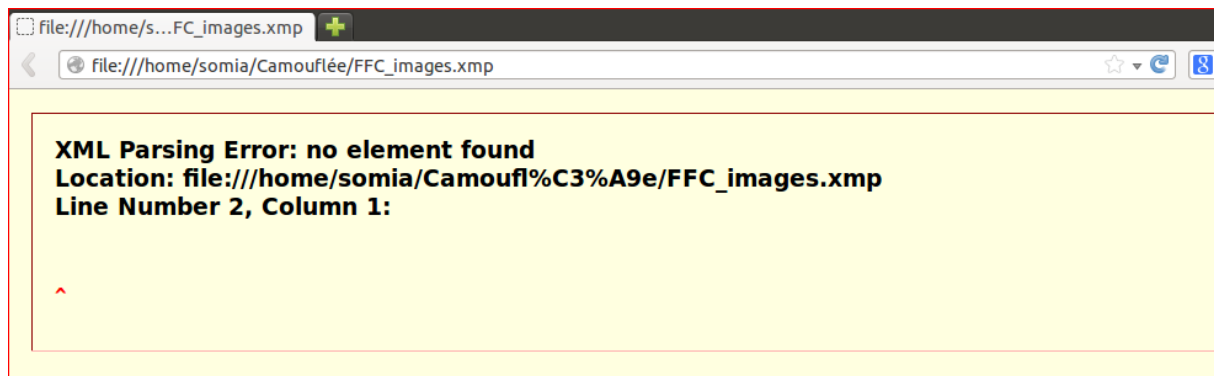
- Exiv2 *.jpg : affiche un sommaire à propos des informations Exif concernant toutes les images qui sont dans le répertoire

```
somia@ubuntu: ~/Camouflée
examples.desktop  PcapClassifier  Templates
git               Pictures        test
somia@ubuntu:~$ cd Camouflée/
somia@ubuntu:~/Camouflée$ ls
1-Information-Security_intro-2014_UNIV.pdf  image_google_1.jpg
FFC_images.jpg                               image_google_2.jpg
tree File camouflage
somia@ubuntu:~/Camouflée$ exiv2 *.jpg
FFC_images.jpg      File name       : FFC_images.jpg
FFC_images.jpg      File size       : 1762753 Bytes
FFC_images.jpg      MIME type       : image/jpeg
FFC_images.jpg      Image size      : 228 x 152
FFC_images.jpg: No Exif data found in the file
image_google_1.jpg  File name       : image_google_1.jpg
image_google_1.jpg  File size       : 2877 Bytes
image_google_1.jpg  MIME type       : image/jpeg
image_google_1.jpg  Image size      : 182 x 121
image_google_1.jpg: No Exif data found in the file
image_google_2.jpg  File name       : image_google_2.jpg
image_google_2.jpg  File size       : 2981 Bytes
image_google_2.jpg  MIME type       : image/jpeg
image_google_2.jpg  Image size      : 182 x 121
image_google_2.jpg: No Exif data found in the file
somia@ubuntu:~/Camouflée$
```

- Exiv2 -eiX FFC_images.xmp

```
somia@ubuntu:~/Camouflée$ exiv2 -eiX FFC_images.jpg
```

Après avoir exécuté la commande, un fichier s'est créé dans le répertoire ('FFC_images.xmp'), après avoir fait un double click la dessus, ci-dessous le résultat



- File *

```
somia@ubuntu:~/Camouflée$ file *
1-Information-Security_intro-2014_UNIV.pdf: PDF document, version 1.5
FFC_images.jpg: JPEG image data, JFIF standard 1.01
FFC_images.xmp: XML document text
free_file_camouflage: directory
image_google_1.jpg: JPEG image data, JFIF standard 1.01
image_google_2.jpg: JPEG image data, JFIF standard 1.01
somia@ubuntu:~/Camouflée$
```

- Hexdump -C image_google_1.jpg

```
somia@ubuntu:~/Camouflée$ hexdump -C image_google_1.jpg
00000000 ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 |.....JFIF.....|
00000010 00 01 00 00 ff db 00 84 00 09 06 07 12 12 12 12 |.....|
00000020 10 0f 14 0f 15 10 15 14 10 10 10 10 14 14 15 10 |.....|
00000030 15 16 0f 15 14 16 16 14 14 14 17 18 1c 28 20 18 |.....( .|
00000040 1a 26 1c 15 14 21 3d 2d 26 29 2b 2e 2e 2e 18 1f |.&...!=&)+....|
00000050 22 20 25 2e 27 20 2e 2e 2e 01 00 00 00 0d 00 |305 7/
```

Concernant l'image téléchargée d'internet, après l'exécution de la commande hexdump -C, on a vu que c'est une (JFIF) ce qui signifie que le stockage de l'image est en binaire.

Idem pour l'image_google_2.jpg téléchargée elle aussi d'internet

```
somia@ubuntu:~/Camouflée$ hexdump -C image_google_2.jpg
00000000 ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 |.....JFIF.....|
00000010 00 01 00 00 ff db 00 84 00 09 06 06 14 0f 10 15 |.....|
00000020 10 10 14 12 10 15 14 14 14 10 10 10 14 10 18 15 |.....|
00000030 18 14 0f 14 10 15 15 14 10 12 17 17 1e 26 1e 17 |.....&..|
00000040 19 25 19 15 15 1f 2f 22 23 27 35 2c 2e 2c 15 20 |.%.../"#'5,.,. |
```

Concernant l'image camouflée, c'est la même chose mais on s'aperçoit que le résultat est nettement plus grand que les deux précédents

```
somia@ubuntu:~/Camouflée$ hexdump -C FFC_images.jpg | more
00000000 ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 |.....JFIF.....|
00000010 00 01 00 00 ff db 00 84 00 09 06 07 10 12 10 14 |.....|
00000020 0f 10 10 0f 10 10 0f 10 10 0f 10 0f 0f 10 10 |.....|
00000030 0f 0d 15 14 14 17 16 16 14 15 15 18 1c 28 20 1a |.....( .|
00000040 1a 25 1c 14 15 21 31 22 25 29 2d 2e 2e 2e 17 1f |.%....!1"%)-.....|
```

J'ai essayé de trouver le mot de passe avec lequel le fichier a été crypté mais pas de résultat

```
somia@ubuntu:~/Camouflée$ hexdump -C FFC_images.jpg | grep sousou
somia@ubuntu:~/Camouflée$
somia@ubuntu:~/Camouflée$ hexdump -C FFC_images.jpg | grep password
somia@ubuntu:~/Camouflée$
somia@ubuntu:~/Camouflée$ hexdump -C FFC_images.jpg | grep PWD
00025ce0 2f 48 59 70 31 50 57 44 4c 70 68 50 69 6d 6f 54 |/HYp1PwDLphPimoT|
0003f1f0 5a 48 73 32 35 6f 44 69 56 34 63 41 71 50 57 44 |ZHs25oDiV4cAqPWD|
00066c30 74 4b 4b 69 42 39 79 50 57 44 73 48 4e 49 6f 67 |tKKiB9yPwDsHNIog|
00094160 50 6d 4d 42 76 71 37 57 35 42 50 57 44 61 56 63 |PmMBvq7W5BPwDaVc|
00174f20 4e 53 76 71 39 50 57 44 6e 6f 6c 6b 33 4b 57 43 |NSvq9PwDno1k3KWC|
somia@ubuntu:~/Camouflée$ hexdump -C FFC_images.jpg | grep pwd
00013800 70 36 66 6b 2b 63 43 6c 70 77 64 6d 39 37 59 67 |p6fk+cClpwdm97Yg|
00013f90 37 79 66 50 77 51 6c 77 74 79 47 70 77 64 72 51 |7yfPwQlwtYGpwrQ|
00022ad0 70 77 64 43 77 33 78 4d 59 39 32 47 69 64 6e 6b |pwdCw3xMY92Gidnk|
0002d620 70 77 64 51 62 52 34 51 73 7a 73 47 64 37 37 49 |pwdQbR4QszsGd77I|
000a31f0 45 37 2f 46 79 70 77 64 73 34 41 53 49 63 63 4f |E7/Fypwds4ASicc0|
000bb970 70 77 64 63 77 4f 45 61 31 49 53 45 46 47 53 36 |pwdcw0Ea1IIEFGS6|
somia@ubuntu:~/Camouflée$
```

- Exiftool image_google_1.jpg

Exiftool n'étant pas installé alors pour l'avoir, on a installé libimage-exiftool-perl

```
somia@ubuntu:~/Camouflée$ exiftool image_google_1.jpg
The program 'exiftool' is currently not installed. You can install it by typing:
sudo apt-get install libimage-exiftool-perl
somia@ubuntu:~/Camouflée$ sudo apt-get install libimage-exiftool-perl
[sudo] password for somia:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  libimage-exiftool-perl
0 upgraded, 1 newly installed, 0 to remove and 527 not upgraded.
Need to get 2,154 kB of archives.
After this operation, 11.6 MB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu/ trusty/universe libimage-exiftool-per
l all 9.46-1 [2,154 kB]
Fetched 2,154 kB in 4s (440 kB/s)
Selecting previously unselected package libimage-exiftool-perl.
(Reading database ... 170049 files and directories currently installed.)
Preparing to unpack .../libimage-exiftool-perl_9.46-1_all.deb ...
Unpacking libimage-exiftool-perl (9.46-1) ...
Processing triggers for man-db (2.6.7.1-1) ...
Setting up libimage-exiftool-perl (9.46-1) ...
somia@ubuntu:~/Camouflée$
```



```
somia@ubuntu:~/Camouflée$ exiftool image_google_1.jpg
ExifTool Version Number      : 9.46
File Name                    : image_google_1.jpg
Directory                   : .
File Size                    : 2.8 kB
File Modification Date/Time   : 2015:01:24 01:33:26-08:00
File Access Date/Time        : 2015:03:30 01:37:30-07:00
File Inode Change Date/Time   : 2015:01:24 01:38:09-08:00
File Permissions             : rwxrw-rw-
File Type                    : JPEG
MIME Type                    : image/jpeg
JFIF Version                 : 1.01
Resolution Unit              : None
X Resolution                  : 1
Y Resolution                  : 1
Image Width                  : 182
Image Height                  : 121
Encoding Process              : Baseline DCT, Huffman coding
Bits Per Sample               : 8
Color Components              : 3
Y Cb Cr Sub Sampling         : YCbCr4:2:0 (2 2)
Image Size                   : 182x121
somia@ubuntu:~/Camouflée$
```

```
somia@ubuntu:~/Camouflée$ exiftool image_google_2.jpg
ExifTool Version Number      : 9.46
File Name                    : image_google_2.jpg
Directory                   : .
File Size                    : 2.9 kB
File Modification Date/Time   : 2015:01:24 01:33:47-08:00
File Access Date/Time        : 2015:03:30 01:37:37-07:00
File Inode Change Date/Time   : 2015:01:24 01:38:09-08:00
File Permissions             : rwxrw-rw-
File Type                    : JPEG
MIME Type                    : image/jpeg
JFIF Version                 : 1.01
Resolution Unit              : None
X Resolution                  : 1
Y Resolution                  : 1
Image Width                  : 182
Image Height                  : 121
Encoding Process              : Baseline DCT, Huffman coding
Bits Per Sample               : 8
Color Components              : 3
Y Cb Cr Sub Sampling         : YCbCr4:2:0 (2 2)
Image Size                   : 182x121
somia@ubuntu:~/Camouflée$
```



```
somia@ubuntu:~/Camouflée$ exiftool FFC_images.jpg
ExifTool Version Number      : 9.46
File Name                    : FFC_images.jpg
Directory                   : .
File Size                   : 1721 kB
File Modification Date/Time  : 2014:10:15 02:29:08-07:00
File Access Date/Time       : 2015:03:30 01:37:24-07:00
File Inode Change Date/Time  : 2015:01:24 01:38:09-08:00
File Permissions             : rwxrwx-rw-
File Type                   : JPEG
MIME Type                   : image/jpeg
JFIF Version                : 1.01
Resolution Unit              : None
X Resolution                 : 1
Y Resolution                 : 1
Image Width                  : 228
Image Height                 : 152
Encoding Process             : Baseline DCT, Huffman coding
Bits Per Sample              : 8
Color Components             : 3
Y Cb Cr Sub Sampling        : YCbCr4:2:0 (2 2)
Image Size                   : 228x152
somia@ubuntu:~/Camouflée$
```

Après avoir exécuté le exiftool sur les 3 images, on remarque qu'il n'y a que la taille 'File size' qui change !

- dd

```
somia@ubuntu:~/Camouflée$ dd if=FFC_images.jpg bs=1 count=1024
1024+0 records in
1024+0 records out
1024 bytes (1.0 kB) copied, 0.0126648 s, 80.9 kB/s
somia@ubuntu:~/Camouflée$
```

```
somia@ubuntu:~/Camouflée$ dd if=FFC_images.jpg skip=4048 bs=1 of=out  
1758705+0 records in  
1758705+0 records out  
1758705 bytes (1.8 MB) copied, 7.64706 s, 230 kB/s  
somia@ubuntu:~/Camouflée$
```

Après avoir exécuté cette commande, un fichier 'out' a été créé.

```
somia@ubuntu:~/Camouflée$ file *  
1-Information-Security_intro-2014_UNIV.pdf: PDF document, version 1.5  
FFC_images.jpg: JPEG image data, JFIF standard 1.01  
FFC_images.xmp: XML document text  
free_file_camouflage: directory  
image_google_1.jpg: JPEG image data, JFIF standard 1.01  
image_google_2.jpg: JPEG image data, JFIF standard 1.01  
out: ISO-8859 text, with very long lines,  
with CRLF line terminators  
somia@ubuntu:~/Camouflée$
```

Après avoir fait un 'more' du fichier 'ou', on remarque que c'est un fichier encodé en base64.

J'ai essayé de le décodé mais ceci n'a pas fonctionné

```
somia@ubuntu:~/Camouflée$ sudo base64 -d out  
base64: invalid input  
somia@ubuntu:~/Camouflée$
```

Là on a fait un file * du répertoire contenant le logiciel

```
somia@ubuntu:~/Camouflée/free_file_camouflage$ file *  
Free_File_Camouflage.exe: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for  
MS Windows  
Free_File_Camouflage.ini: UTF-8 Unicode text, with CRLF line terminators  
Free_File_Camouflage.log: UTF-8 Unicode text, with CRLF line terminators  
license.txt: UTF-8 Unicode (with BOM) text, with CRLF line terminators  
readme.txt: UTF-8 Unicode (with BOM) text, with CRLF line terminators  
somia@ubuntu:~/Camouflée/free_file_camouflage$
```

```
somia@ubuntu:~/Camouflée$ sudo base64 -d out.64 | file -  
base64: invalid input  
/dev/stdin: no read permission  
somia@ubuntu:~/Camouflée$
```

```
somia@ubuntu:~/Camouflée$ sudo base64 -d | file -f out.64
```

```
CjidVyf2GushnUDQUpcwzfHGGf7o24KQ0mxemlhDUBaGfVJ+Xr5RJULRW3srFvyjpWQXQ05Nj0ogBJCOvKhb
A1acr/iNAMAPy766xbepvdBwAXdbuc6C89K428tyj6GqZhzw0LtNuV4/i444pUwrJkPvFPCsvDZUIxs0Lu
hc59qQ2Ru6mux8+KcaWvaRyYsLrgaIfkuh70lvGu7maFJm8tA3+izVxLiVIPFKyJmP1sF0u3oSo/FBEdCaRY
PgoyfaYnFuVDMqnn9dM5fq9U0RvLZzbQMTmPcvR0rZ1oGfVVLcmYtWzEzw+HujV25CwLSm2GcYtI2F+koia7E
CjvNWACm9FcF79VImUY33y6ekX++ZZdrHkhVG8+dmDChfQPcti2/tPtkXuvFLf2Y/Hhza4AZtpQ6TQ3nXy/7
HczbaCr0p5047cYdreYhbB6BMMYz+PGYNGNh161HNxUabU7DkE5T/BLXeq65CZqBAa75reIek70FtcShRg8C
m0gwxUMZjdhdDj/KpNkPPCtVa5tzZa5xEGlL0wQmbt1w5IyLikqsZL41S6MdE9858x0+Rx4nPmPmRskD/His
xWET43+wU8jVz/r4WrBm1DqauPGtStVSpLW95DekZwj7mqjJekY32gRaAxllACzUV3qb/HKh03s4qbx50ULR
wJ/z7boEqJ2gRHA0lCs1Rpnmj9sOXyEHkH1cpYLE6/BqyK0jZW4gHS05tsCphIXvExHGCPdEiuBe9BFpjBbx
Rf4efyuCKclWNk7U3ouh+ctYeQB1u8/Avgpj7aNorZKqPYWljxRksB/VPtzj1JzK0xDESb520tCh4tWIKyo0
Xs3FJwdk2cJMbghR6yCY9Ja7Sm4cHoZPKMvXoKI30DitWTVOKfxLQ38HixDAqFJigjb99Gx7Pcd/6fpykmns
9w0eIBjdjpd+4lbaeI7Q0XtdZWKH611eNYGR+9Q4CjwNj3zFOTujLEA0LvhnQuDukXpjbGTCSD72vE02GNjL
jhy7p09gdIhdLHAObIKoy0eek2HB3i3U4JrjHw0YAy/OHswb8JeP/ODZ0/R59G6/s7xKa205eYiQkmtPyd3
ycPBC8YTxe4rmp8Zu0HATiUzzNAInH0+DNTq8HctFMFIIOhxEnVQLNLUYbGMhDmzqcXLPMMe+nLHlTW0AR4L
0PIrRuIDSShd+InHATTBWU3M489Evr1aHbN1QNS/aUzG405ty/0AM4ijCYetUAARIZSCHDCmdK55c1vum4k
ZtTV5J1cKSN0QvTU00Gqs40ZJoZn1fWY5MSXAKQILfB2aE1zu/gD7tCD+jdUk441zvKFntkTTIzVVR4Eil4gG
P9BvGZiKOW+17dGX0qXcW1nkWfgw71kAGK7QtXkw3dHfM2inXe3FhXGCD45yvmMyj4dQqODVNS9PmpgIoI/P
KwUhbpHwsQ2wtg5r87CmQcEnepPCFmpMZ2nMup+RfkIRgnrVtEVxH8vmMZv98FShSASxh/szjP/bY9zbUgry
7hWQYN+6tA5P2/i0nWfiJv1GCPWxu0QUANt27WVeKohPkLqqxcJ4MLYEnLF4Eka5IXCZCcyd0aFBhP+uz4A0
xvzmzWnxrcqX0Vp+KJWPiscU9nGGEKaDIEqgtCfLrnUNWk7PbsWm5hE7jqjR5WCudf8DKv22VqTUIBBn0e+W
AWyegLEK57IjV4ZpidD1KMrPkwc2npybYFv7n+FXetS3gDY7L8K2RwcbFu16hKM++Rzn9a8j75GnPGEWCU
oUGl3vReffCL0h+YSCGLZC0pyIQmNIhs/+CMnGv+9AjeS17+YvXvYyFH3vbktA6AkctypLPkREyaKGaIsnP
s6H/9Tr6++n+rHNCOSQFGqwwV8oSo0NCSG79VDBUV+paMtPAeuzflg3Ez+I0S/Rr9xfXwae3k2EEGsn4Xesk
MhyJICNFNZoI+GMVERLNVmPESQesvS+lc5tH19KVfF8w9A3gPbD5Z4q+zZCh298I8nK4m7FQMLI96ZCXgsj
cd++QU/6/Q00jXsSzCY0Mz8JkFaXWaj5gSs8EACHDq01w20Ve52JpvGDyDp2VNLqzh6jITnsyLL+4A3p+pC1
VYg+Ate5my89PVbI+jzMf5bvvgLtsPjd1J6wn0fJE6H//0Q30AZnJBru6gf33+ItYqkUuTh9sbaufmOCpna
dFuG2RPLmacryPbczbxKXUZ0fT2JIRI7lzaBUqzcEqMevf1mFM2w7xpA1KjUStofYKjXm07JUzRwsSkvzXTx
Qdrs4eKooI4/J8wMfMznjGGZvcefchmh0rUjD7ZkSzYo02h6bht2bC2dreK1XSozQrv0NrLj6xvCTIH22nT
NzfC38NkP5hJY4uLQWmWdtYoRDwYWOu47RWrcEh0ex0Hh1aaLDaxs1DezPjKHkmrvxChFBKupBTvxsZx9VhV
TYYe7tbgTzFFPPKImhorhgG+6QsUv+qsg2YJjle2TbMwRXlCNVCv1irKTKAWEA1IhXgw8CT01aPgARELHrym
Uc/9sXxNu8hW6MW6VkfF3zTmM9vqjEx/o5wcPFREXkjysgGnfmaNXvJRkzqgWklU+ZfGXwcopaPwokHzidt
7oldopFcghQ30y/aC8iQhpN1cX1MwBw1xVA7Ji0phRicNMGHK4CRJA4Lzw8Aq2GVQ00DJLABuPTX+jfPp7CM
' (File name too long)vyCiChh9SQ3qBSaV7YhVqsSFDqlpbDg=
```

- imagemagick

```
somia@ubuntu:~/Camouflée$ cat image_google_1.jpg | convert -strip - - | md5sum
The program 'convert' can be found in the following packages:
* imagemagick
* graphicsmagick-imagemagick-compat
Try: sudo apt-get install <selected package>
d41d8cd98f00b204e9800998ecf8427e -
somia@ubuntu:~/Camouflée$ sudo apt-get install imagemagickl
```

- wine ! L'outil a été téléchargé pour pouvoir tester et le logiciel camouflage.exe et aussi pour pouvoir installer 'idag.exe' et l'exécuter

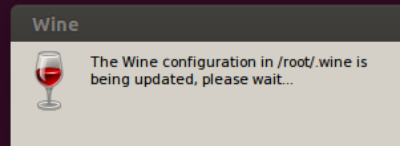
```
somia@ubuntu:~/Camouflée$ sudo apt-get install wine
```

```
somia@ubuntu: ~  
Package configuration  
  
Configuring ttf-mscorefonts-installer  
  
TrueType core fonts for the Web EULA  
  
END-USER LICENSE AGREEMENT FOR MICROSOFT SOFTWARE  
  
IMPORTANT-READ CAREFULLY: This Microsoft End-User License Agreement  
("EULA") is a legal agreement between you (either an individual or a  
single entity) and Microsoft Corporation for the Microsoft software  
accompanying this EULA, which includes computer software and may include  
associated media, printed materials, and "on-line" or electronic  
documentation ("SOFTWARE PRODUCT" or "SOFTWARE"). By exercising your  
rights to make and use copies of the SOFTWARE PRODUCT, you agree to be  
bound by the terms of this EULA. If you do not agree to the terms of  
this EULA, you may not use the SOFTWARE PRODUCT.  
  
<Ok>
```

```
somia@ubuntu: ~  
Package configuration  
  
Configuring ttf-mscorefonts-installer  
  
In order to install this package, you must accept the license terms, the  
"TrueType core fonts for the Web EULA ". Not accepting will cancel the  
installation.  
  
Do you accept the EULA license terms?  
  
      <Yes>      <No>
```

Après la fin de l'installation de 'wine', on a essayé de lancer « wine free_File_Camouflage.exe » mais ceci n'a pas marché


```
somia@ubuntu:~/Camouflée/free_file_camouflage$ sudo wine Free_File_Camouflage.exe
wine: '/home/somia' is not owned by you, refusing to create a configuration directory there
somia@ubuntu:~/Camouflée/free_file_camouflage$ sudo su
root@ubuntu:/home/somia/Camouflée/free_file_camouflage# wine Free_File_Camouflage.exe
wine: created the configuration directory '/root/.wine'
```



```
err:msi:cabinet_copy_file failed to create L"C:\\windows\\mono\\mono-2.0\\lib\\mono\\gac\\Accessibili
ty\\2.0.0.0_b03f5f7f11d50a3a\\Accessibility.dll" (error 3)
err:msi:extract_cabinet_stream FDICopy failed
err:msi:ACTION_InstallFiles Failed to extract cabinet: L"#image.cab"
err:msi:ITERATE_Actions Execution halted, action L"InstallFiles" returned 1603
err:appwizcpl:install_file MsiInstallProduct failed: 1603
fixme:storage:create_storagefile Storage share mode not implemented.
err:mscoree:LoadLibraryShim error reading registry key for installroot
err:mscoree:LoadLibraryShim error reading registry key for installroot
err:mscoree:LoadLibraryShim error reading registry key for installroot
err:mscoree:LoadLibraryShim error reading registry key for installroot
fixme:iphlpapi:NotifyAddrChange (Handle 0x114e2b8, overlapped 0x114e2d0): stub
fixme:storage:create_storagefile Storage share mode not implemented.
err:mscoree:LoadLibraryShim error reading registry key for installroot
err:mscoree:LoadLibraryShim error reading registry key for installroot
err:mscoree:LoadLibraryShim error reading registry key for installroot
err:mscoree:LoadLibraryShim error reading registry key for installroot
err:msi:cabinet_copy_file failed to create L"C:\\windows\\syswow64\\gecko\\2.21\\wine_gecko\\dictiona
ries\\en-US.dic" (error 3)
err:msi:extract_cabinet_stream FDICopy failed
err:msi:ACTION_InstallFiles Failed to extract cabinet: L"#winegecko.cab"
err:msi:ITERATE_Actions Execution halted, action L"InstallFiles" returned 1603
err:appwizcpl:install_file MsiInstallProduct failed: 1603
Could not load wine-gecko. HTML rendering will be disabled.
wine: configuration in '/root/.wine' has been updated.
wine: Install Mono for Windows to run .NET applications.
```

```
root@ubuntu:/home/somia/Camouflée/free_file_camouflage# wine Free_File_Camouflage.exe
wine: Install Mono for Windows to run .NET applications.
root@ubuntu:/home/somia/Camouflée/free_file_camouflage#
```

- objdump

```
root@ubuntu:/home/somia/Camouflée/free_file_camouflage# objdump -d Free_File_Camouflage.exe >> objdump_Free-File-Camouflage.txt
```

```
root@ubuntu:/home/somia/Camouflée/free_file_camouflage# objdump -d Free_File_Camouflage.exe >> objdump_Free-File-Camouflage.txt
```

J'ai ensuite fait un grep du 'main' sur ce fichier, mais aucun résultat n'y apparaît !

```
root@ubuntu:/home/somia/Canouflée/free_file_camouflage# ls
Free_File_Camouflage.exe  Free_File_Camouflage.ini  Free_File_Camouflage.log  license.txt  objdump_Free-File-Camouflage.txt  readme.txt
root@ubuntu:/home/somia/Canouflée/free_file_camouflage# less objdump_Free-File-Camouflage.txt | grep main
root@ubuntu:/home/somia/Canouflée/free_file_camouflage# less objdump_Free-File-Camouflage.txt | grep main
root@ubuntu:/home/somia/Canouflée/free_file_camouflage# more objdump_Free-File-Camouflage.txt | grep main
root@ubuntu:/home/somia/Canouflée/free_file_camouflage#
```

L'idée été de pouvoir trouver soit le mot de passe ou un indice pour remonter au mot de passe et ainsi pouvoir décrypter le fichier.

C'est-à-dire en trouvant où dans le programme il fait le test pour voir si le mot de passe est correct alors il va faire le décryptage ; ce test là, je voulais le changer pour que le test soit toujours vrai. C'est-à-dire avec ou sans le bon mot de passe, le fichier se décryptera toujours.

Si j'avais trouvé l'emplacement, la prochaine étape été d'installer « ghex » qui est un éditeur hexadécimal pour pouvoir modifier le test en question et permettre le décryptage quelque soit le mot de passe.

J'ai aussi fait exécuter le logiciel Free_File_Camouflage.exe tout en ayant wireshark en exécution, ainsi j'ai obtenu un fichier pcap, qui est aussi joint à ce fichier, et ce afin de pouvoir étudier le fichier pcap, pour voir lors de l'exécution du programme, est ce qu'il se connecte à internet (il s'est avéré que oui), en se connectant à internet, il fait quoi, etc.