

Polyglottes binaires

et

implications



SSTIC, Rennes, France

Anglicismes en approche

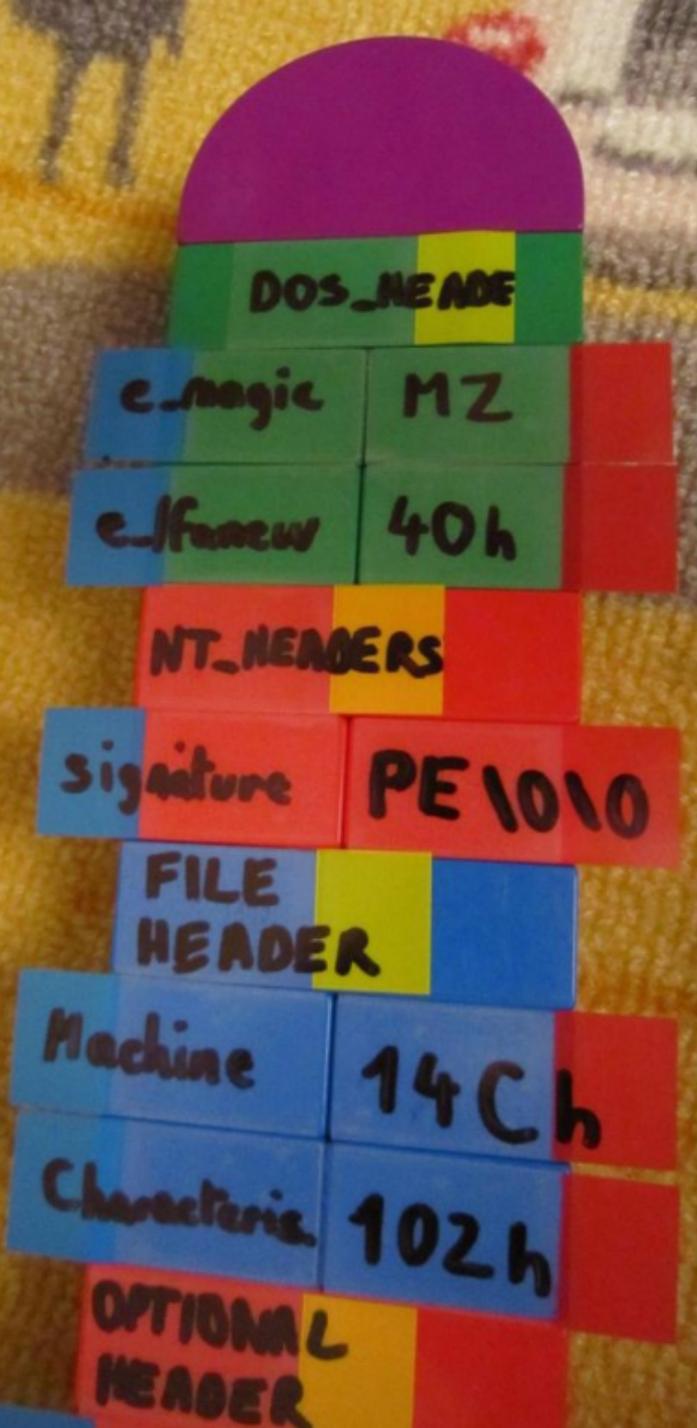
rétro-conception & documentations visuelles

<http://corkami.com>





brique par brique



```
istruc IMAGE_DOS_HEADER
    at IMAGE_DOS_HEADER.e_magic, db 'MZ'
    at IMAGE_DOS_HEADER.e_lfanew, dd NT_Signature - IMAGEBASE
iend
NT_Signature:
istruc IMAGE_NT_HEADERS
    at IMAGE_NT_HEADERS.Signature, db 'PE', 0, 0
iend
istruc IMAGE_FILE_HEADER
    at IMAGE_FILE_HEADER.Machine, dw IMAGE_FILE_MACHINE_I386
    at IMAGE_FILE_HEADER.Characteristics, dw IMAGE_FILE_EXECUTABLE_IMAGE
iend
istruc IMAGE_OPTIONAL_HEADER32
```



un exécutable *complet*

IMAGEBASE equ 400000h
org IMAGEBASE

```
istruc IMAGE_DOS_HEADER
    at IMAGE_DOS_HEADER.e_magic, db 'MZ'
    at IMAGE_DOS_HEADER.e_lfanew, dd NT_Signature - IMAGEBASE
iend
```

```
NT_Signature:
istruc IMAGE_NT_HEADERS
    at IMAGE_NT_HEADERS.Signature, db 'PE', 0, 0
iend
```

```
istruc IMAGE_FILE_HEADER
    at IMAGE_FILE_HEADER.Machine, dw IMAGE_FILE_MACHINE_I386
    at IMAGE_FILE_HEADER.Characteristics, dw IMAGE_FILE_EXECUTABLE_IMAGE
iend
```

```
istruc IMAGE_OPTIONAL_HEADER32
    at IMAGE_OPTIONAL_HEADER32.Magic, dw IMAGE_NT_OPTIONAL_HDR32_MAGIC
    at IMAGE_OPTIONAL_HEADER32.AddressOfEntryPoint, dd EntryPoint - IMAGEBASE ; not strictly required
    at IMAGE_OPTIONAL_HEADER32.ImageBase, dd IMAGEBASE ; not required under XP
    at IMAGE_OPTIONAL_HEADER32.SectionAlignment, dd 1
    at IMAGE_OPTIONAL_HEADER32.FileAlignment, dd 1
    at IMAGE_OPTIONAL_HEADER32.MajorSubsystemVersion, dw 4
    at IMAGE_OPTIONAL_HEADER32.SizeOfImage, dd SIZEOFIMAGE
    at IMAGE_OPTIONAL_HEADER32.SizeOfHeaders, dd SIZEOFIMAGE - 1 ; required for XP
    at IMAGE_OPTIONAL_HEADER32.Subsystem, dw IMAGE_SUBSYSTEM_WINDOWS_CUI
iend
```

```
istruc IMAGE_DATA_DIRECTORY_16
iend
```

```
EntryPoint:
    push 42
    pop eax
    ret
```

le problème





COMPUTER PROBLEMS
THAT MAKE PEOPLE SAY
"MAYBE IT HAS A VIRUS?"



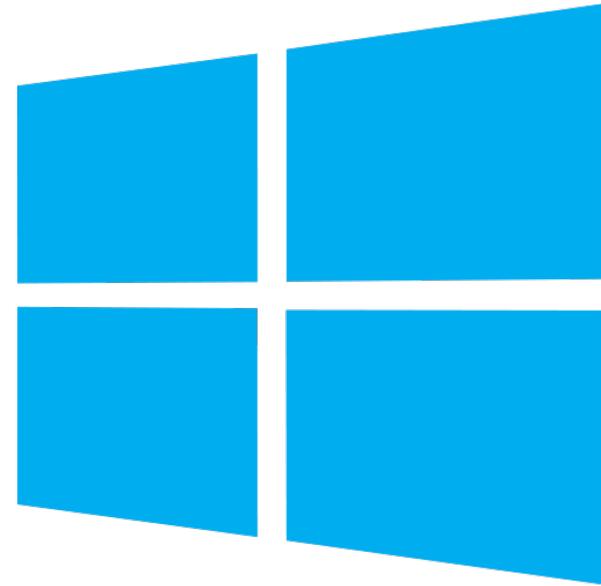
COMPUTER
PROBLEMS CAUSED
BY VIRUSES

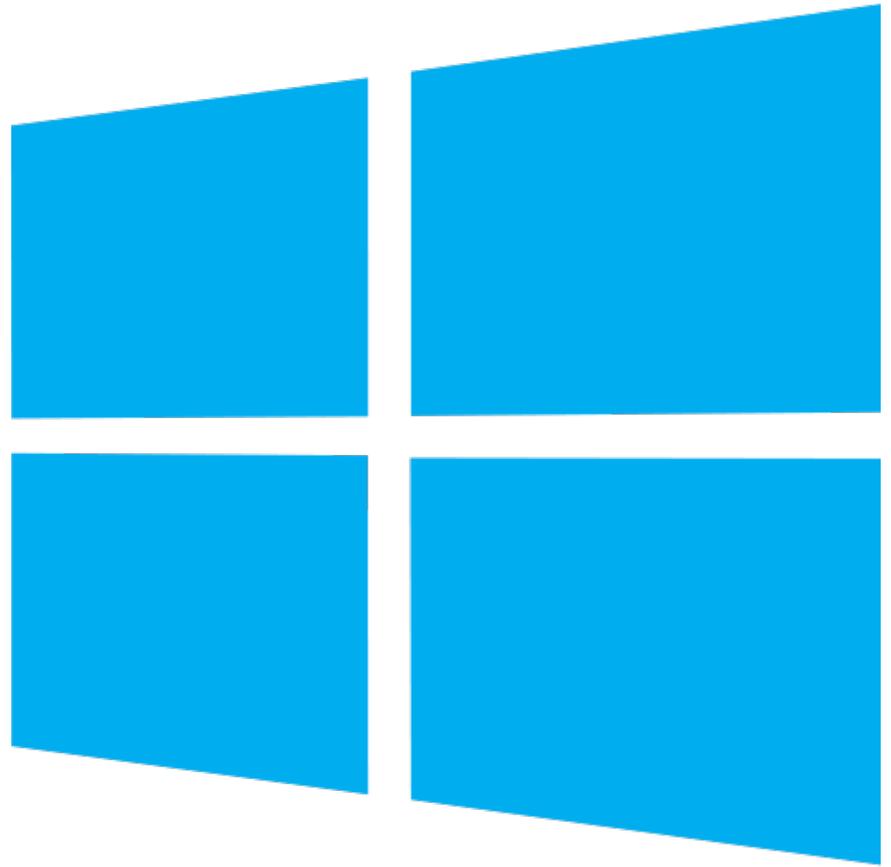
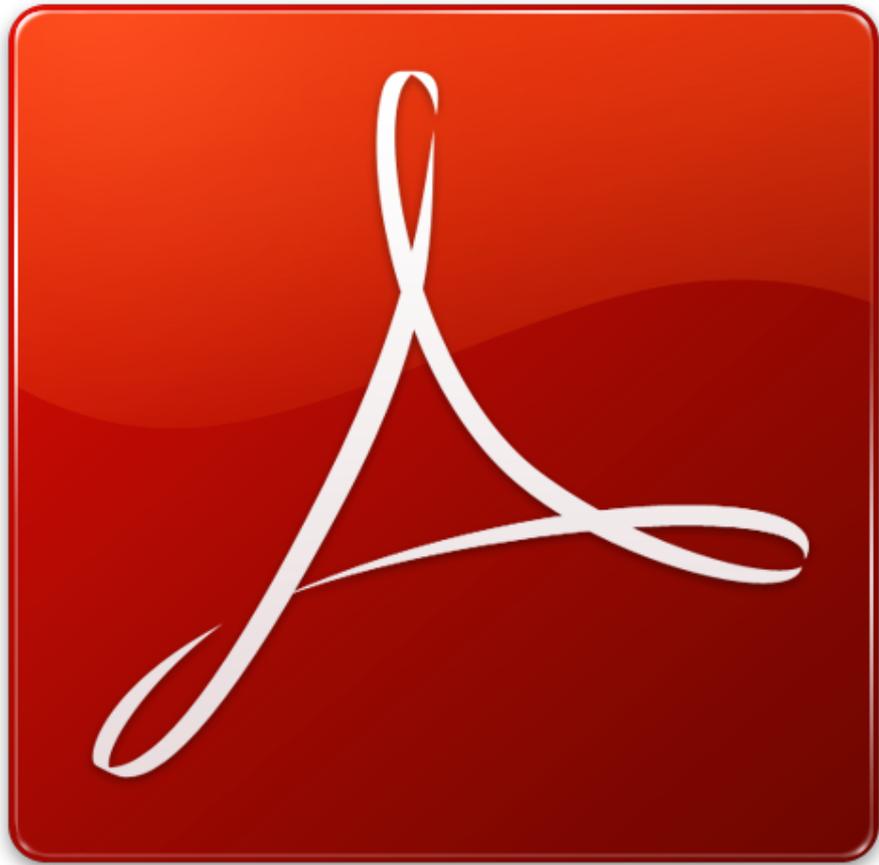


HTML

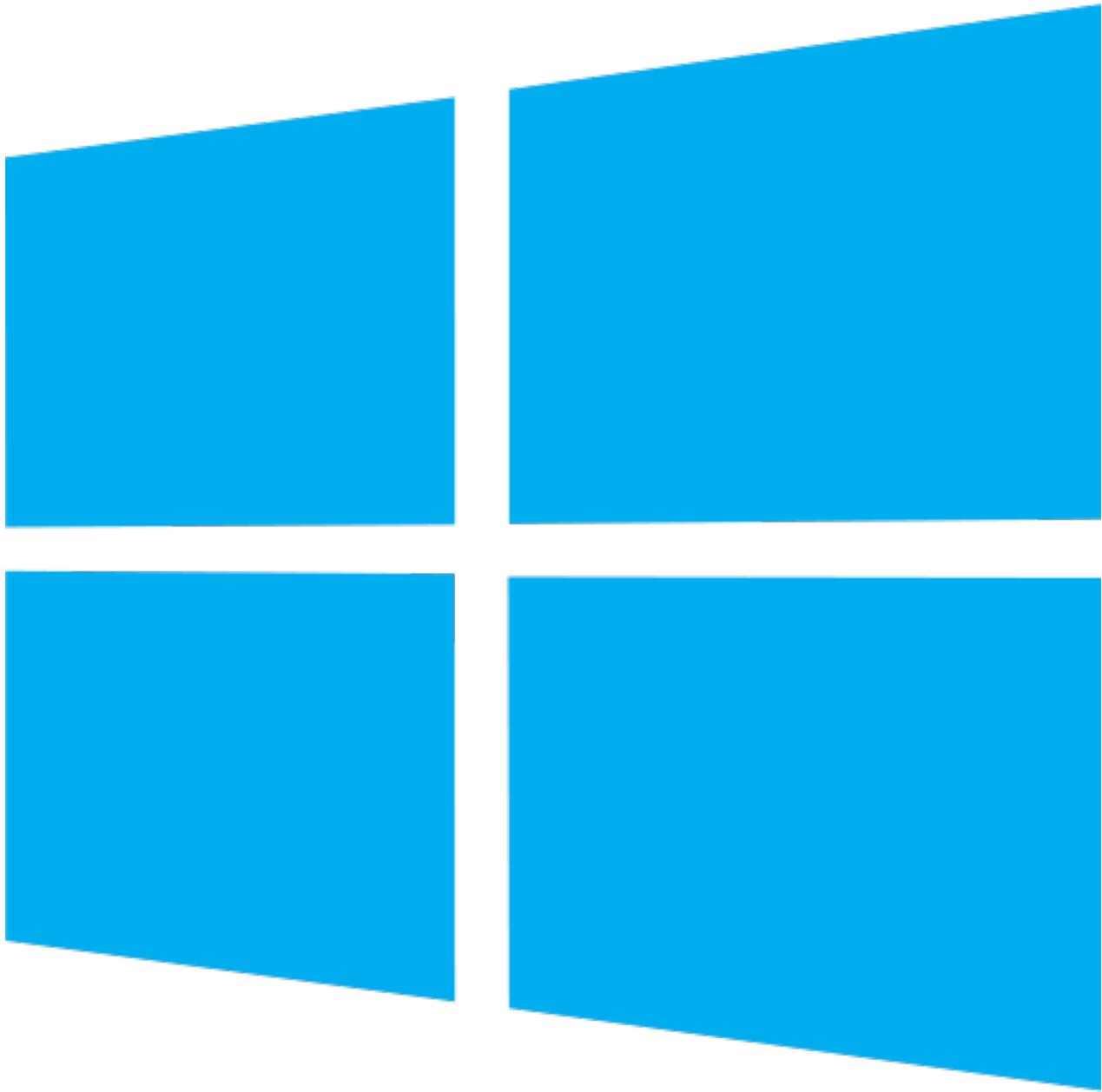


Java









en-tête

MZ

en-tête DOS

depuis IBM PC-DOS 1.0 (1981)

PE (ou NE/LE/LX/VZ/...)

en-têtes 'modernes'

depuis Windows NT 3.1 (1993)



offset 0

IMAGE_DOS_HEADER

0x00 dw e_magic MZ

0x02 dw e_cblp

0x04 dw e_cp exe size

0x06 dw e_crhc

0x08 dw e_cparhdr exe start

0x0a dw e_minalloc

0x0c dw e_maxalloc

0x0e dw e_ss

0x10 dw e_sp

0x12 dw e_csum

0x14 dw e_ip

0x16 dw e_cs

0x18 dw e_lfantr

0x1a dw e_ovno

0x1c dw e_res[4]

0x24 dw e_oemid

0x26 dw e_oeminfo

0x28 dw e_res2[10]

0x3c dd e_lfanew  offset to PE Header



HTML



PE_HTML_27mb.html x

JavaScript Alert

CorkaMIX [HTML+JavaScript]

OK

D:\PE_HTML_27mb

Message from webpage



CorkaMIX [HTML+JavaScript]

OK

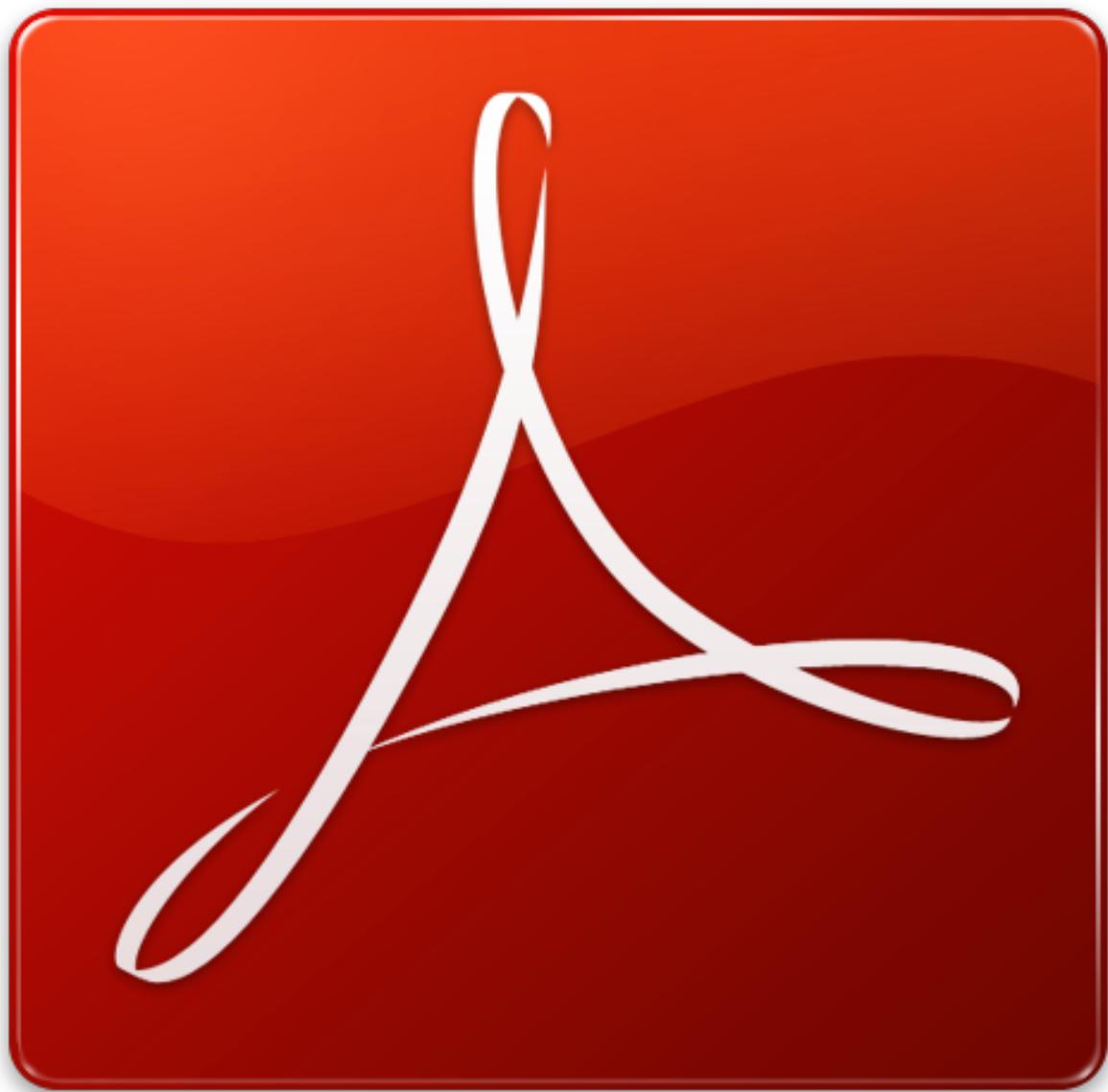
```

01A5B2A0: 00 00 00 00.00 00 00 00.00 00 00 00.00
01A5B2B0: 00 00 00 00.00 00 00 00.00 00 00 00.00
01A4B2C0: 3C 68 74 6D.6C 3E 0D 0A.3C 62 6F 64.79 3E 3C 73
01A4B2D0: 74 79 6C 65.3E 62 6F 64.79 20 7B 20.76 69 73 69
01A4B2E0: 62 69 6C 69.74 79 3A 68.69 64 64 65.6E 3B 7D 20
01A4B2F0: 2E 6E 20 7B.20 76 69 73.69 62 69 6C.69 74 79 3A
01A4B300: 20 76 69 73.69 62 6C 65.3B 20 70 6F.73 69 74 69
01A4B310: 6F 6E 3A 20.61 62 73 6F.6C 75 74 65.3B 20 70 61
01A4B320: 64 64 69 6E.67 3A 20 30.20 31 65 78.20 30 20 31
01A4B330: 65 78 3B 20.6D 61 72 67.69 6E 3A 20.30 3B 20 74
01A4B340: 6F 70 3A 20.30 3B 20 6C.65 66 74 3A.20 30 3B 20
01A4B350: 7D 20 68 31.20 7B 20 6D.61 72 67 69.6E 2D 74 6F
01A4B360: 70 3A 20 30.2E 34 65 78.3B 20 6D 61.72 67 69 6E
01A4B370: 2D 62 6F 74.74 6F 6D 3A.20 30 2E 38.65 78 3B 20
01A4B380: 7D 3C 2F 73.74 79 6C 65.3E 3C 64 69.76 20 63 6C
01A4B390: 61 73 73 3D.6E 3E 3C 73.63 72 69 70.74 20 74 79
01A4B3A0: 70 65 3D 27.74 65 78 74.2F 6A 61 76.61 73 63 72
01A4B3B0: 69 70 74 27.3E 61 6C 65.72 74 28 27.43 6F 72 6B
01A4B3C0: 61 4D 49 58.20 5B 48 54.4D 4C 2B 4A.61 76 61 53
01A4B3D0: 63 72 69 70.74 5D 27 29.3B 3C 2F 73.63 72 69 70
01A4B3E0: 74 3E 3C 21.2D 2D
  
```

```

<html>f[<body><st
yle>body { visi
bility:hidden;}
.n < visibility:
visible; positi
on: absolute; pa
dding: 0 1ex 0 1
ex; margin: 0; t
op: 0; left: 0;
> h1 < margin-to
p: 0.4ex; margin
-bottom: 0.8ex;
></style><div cl
ass=n><script ty
pe='text/javascr
ipt'>alert('Cork
aMIX [HTML+JavaS
cript]');</scrip
t><!--
  
```





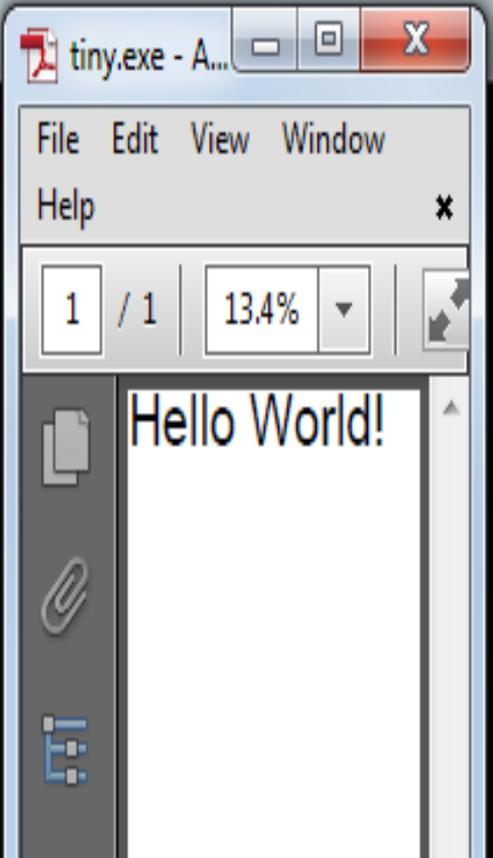
contactenation PE PDF

```
>ls -l
total 2
-rw-rw-rw- 1 user      group    191 Mar 10  2011 helloworld.pdf
-rwxrwxrwx 1 user      group    268 Sep  7 11:29 tiny.exe
```

```
>copy tiny.exe+helloworld.pdf
tiny.exe
helloworld.pdf
        1 file(s) copied.
```

```
>tiny.exe
* 268b universal tiny PE (XP-W7x64)
```

```
>ls -l
total 2
-rw-rw-rw- 1 user      group    191 Mar 10  2011 helloworld.pdf
-rwxrwxrwx 1 user      group    460 Sep 20 10:37 tiny.exe
```



C:\ Hiew: NOTEPAD.EXE

d:\NOTEPAD.EXE ↓FRO ----- PE .01000002 | Hiew 8.22 (c)SEN

```
01000000: 4D 5A 0A 25-50 44 46 2D-31 2E 34 0A-6F 62 6A 3C MZ%PDF-1.4obj<
01000010: 3C 3E 3E 73-74 72 65 61-6D 0A 00 00-00 00 00 00 <>>stream
01000020: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
01000030: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
```

C:\ Hiew: NOTEPAD.EXE

d:\NOTEPAD.

```
010139C0: 00
010139D0: 00
010139E0: 00
010139F0: 6E
00010E00: 25
00010E10: 0A
00010E20: 65
00010E30: 32
00010E40: 29
00010E50: 74
00010E60: 66
00010E70: 3E
00010E80: 5B
00010E90: 6E
00010EA0: 31
00010EB0: 6E
00010EC0: 29
00010ED0: 68
00010EE0: 2E
00010EF0: 74
00010F00: 66
00010F10: 4D
00010F20: 74
00010F30: 35
00010F40: 64
```

NOTEPAD.EXE - Adobe Reader

File Edit View Window Help

1 / 180 47% Tools

Zythom

Dans la peau d'un informaticien
expert judiciaire

Tome 1
L'âge d'or est devant nous

"Je jure, d'apporter mon concours à la Justice, d'accomplir ma mission, de faire mon rapport, et de donner mon avis en mon honneur et en ma conscience."

Seulement utilisé en Cours d'appel sur l'Expert judiciaire.

139EF | Hiew 8.22 (c)SEN

```
00 00
00 00
00 35
0A ndstreamendobj
0D %PDF-1.4%
70 [ 0 obj
20 e/Catalog/Pages
52 2 0 R/Lang(fr-FR
6F ) /StructTreeRoot
6E t 764 0 R/MarkIn
65 fo<</Marked true
73 >>/OutputIntents
```

Untitled - Notepad

File Edit Format View Help

Ln 1, C

```
0 35 tOutputProfile 5
4 61 528 0 R>>] /Meta
5 0D 4+~ EF20 0 D\P
```





Java



récapitulons



Structure

1. début

- Signature PE
 - i. %PDF + début d'objet

2. suite

- PE (suite)
- HTML
- PDF (suite)

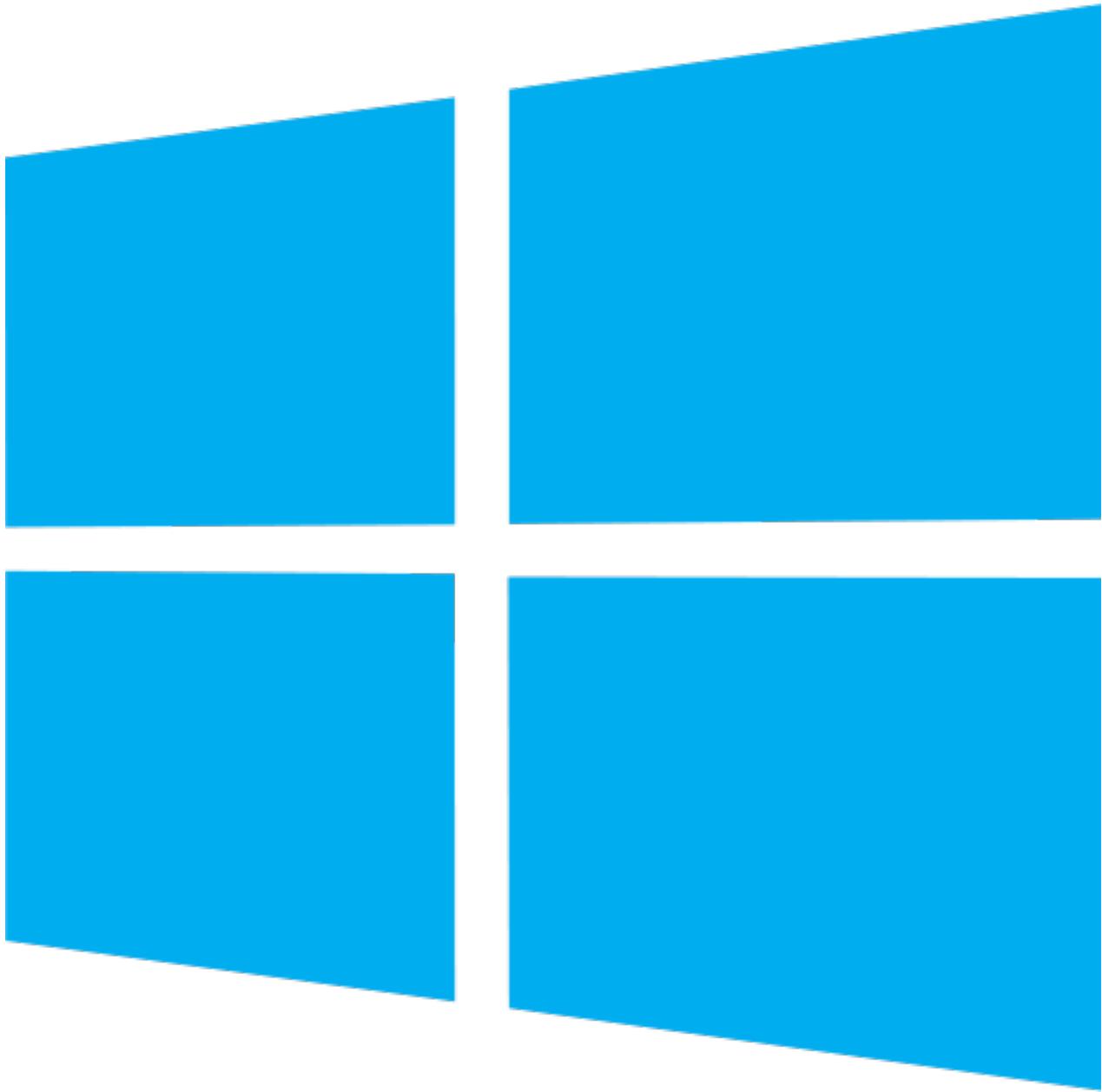
3. fin

- ZIP



ça manque de sel...
(et de plantages)





IMAGE_IMPORT_DESCRIPTOR

IMAGE_THUNK_DATA

00 dd AddressOfData
00000000

0c dd Name

10 FirstThunk

terminator

msvcrt.dll, 0

IMAGE_IMPORT_BY_NAME

00 dw Hint: 0

02 db Name: printf, 0

10 FirstThunk 00000000



Preparing import...

Import: Invalid data



Warning



The imports segment seems to be destroyed. This MAY mean that the file was packed or otherwise modified in order to make it more difficult to analyze. If you want to see the imports segment in the original form, please reload it with the 'make imports section' checkbox cleared.

OK

Don't display this message again



Table A-2. One-byte Opcode Map: (00H – F7H) *

	0	1	2	3	4	5	6	7
D	Eb, 1 <small>64</small>	Ev, 1 <small>64</small>	Eb, CL <small>64</small>	Ev, CL <small>64</small>	AAM ⁶⁴ lb	AAD ⁶⁴ lb		XLAT/ XLATB

Table A-3. Two-byte Opcode Map: 08H – 7FH (First Byte is 0FH) *

	pxf	8	9	A	B	C	D	E	F
0		INVD	WBINVD		2-byte Illegal Opcodes UD2 ^{1B}		NOP Ev		
1		Prefetch ^{1C} (Grp 16 ^{1A})							NOP Ev
		vmovans	vmovans	cvtni2ns	vmovntns	cvftns2ni	cvftns2ni	vucomiss	vcomiss



Table A-1. One-Byte Opcodes, Low Nibble 0–7h

Nibble ¹	0	1	2	3	4	5	6	7
D	Eb, 1	Ev, 1	Eb, CL	Ev, CL	AAM ³	AAD ³	SALC ³	XLAT

Table A-4. Second Byte of Two-Byte Opcodes, Low Nibble 8–Fh

Prefix	Nibble ¹	8	9	A	B	C	D	E	F
n/a	0	INVD	WBINVD	invalid	UD2	invalid	Group P ² PREFETCH	FEMMS	3DNow! See "3DNow! TM Opcodes" on page 351
n/a	1	Group 16 ²	NOP ³	NOP ³	NOP ³				



D:\corkamix.exe - WinDbg:6.12.0002.633 X86

File Edit View Debug Window Help

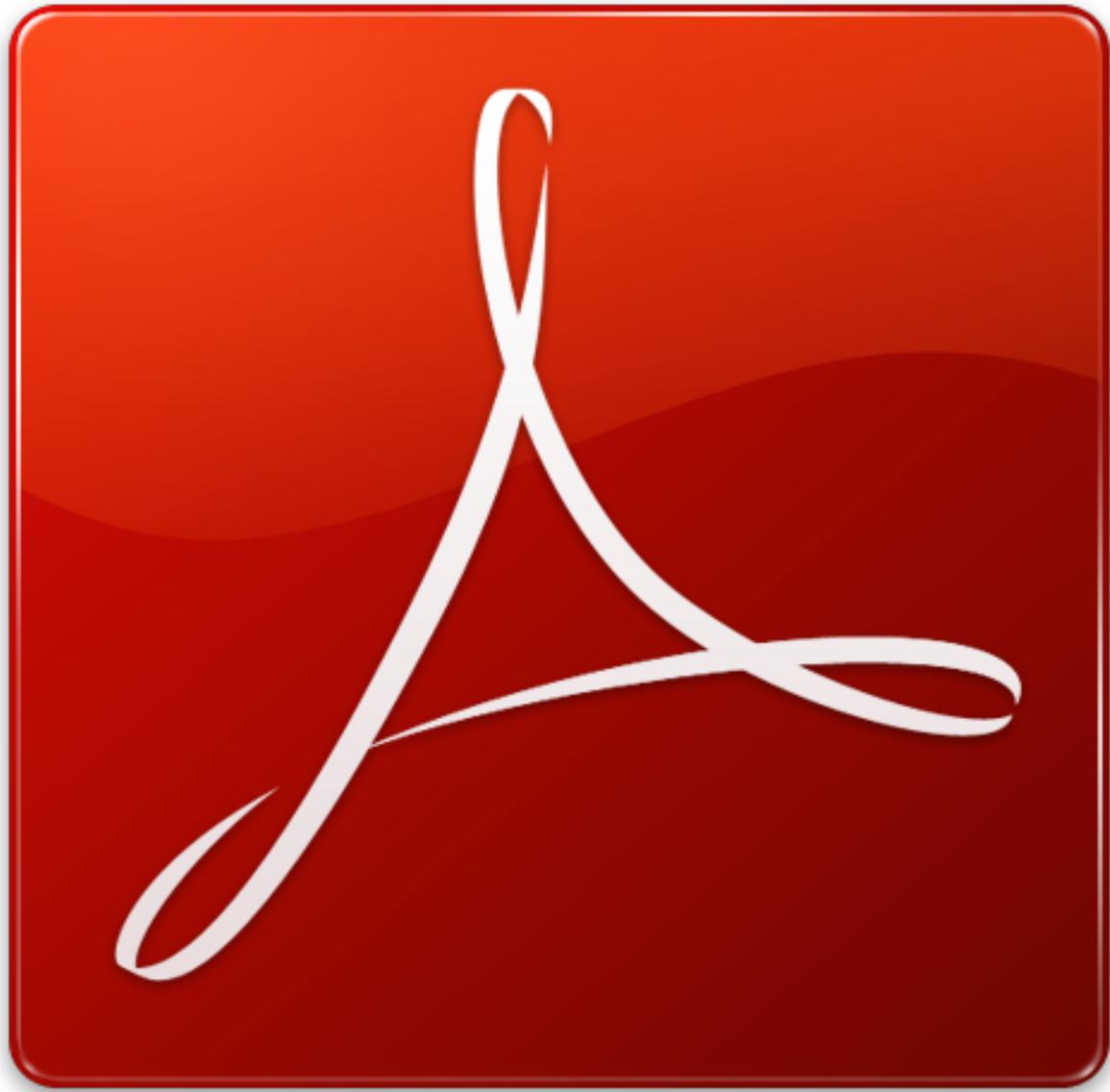
Command

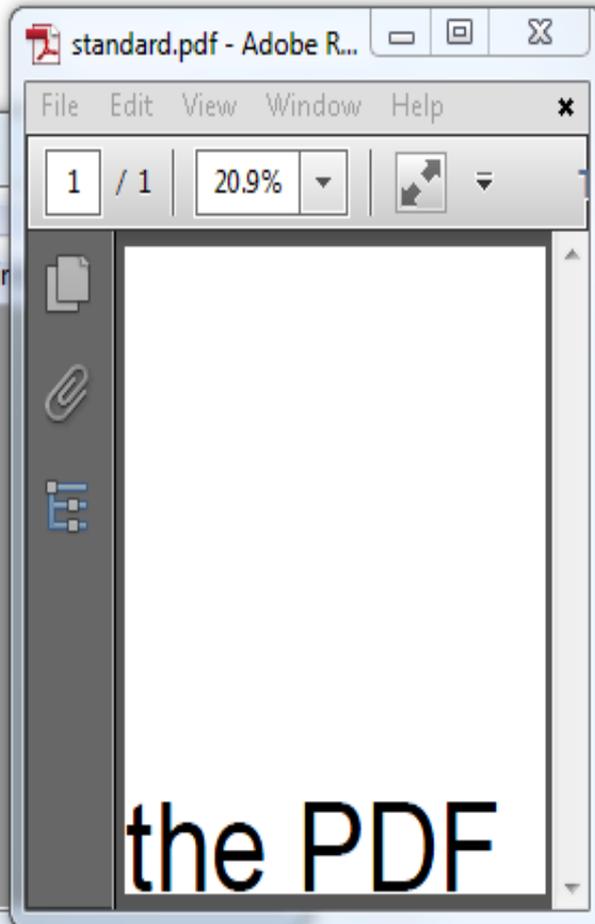
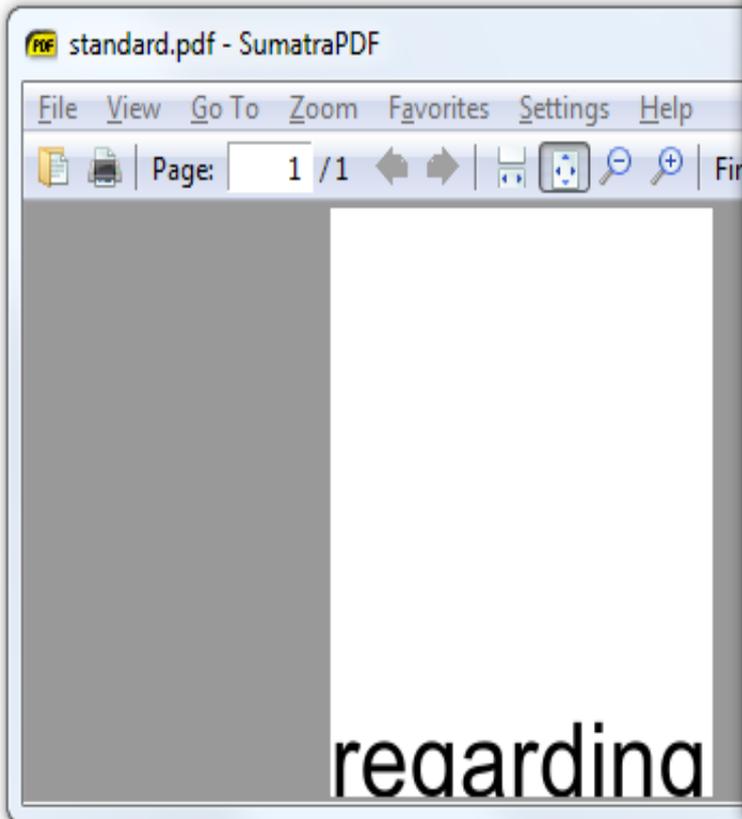
```
0:000> u
image00400000+0x138:
00400138 0f          ???
00400139 1838       sbb      byte ptr [eax],bh
0040013b 685a004000 push    offset image00400000+0x5a (0040005a)
00400140 ff154b014000 call    dword ptr [image00400000+0x14b (0040014b)]
00400146 d6         ???
00400147 83c404     add     esp,4
0040014a c3         ret
0040014b b9c5037700 mov     ecx,7703C5h
```

0:000>

Ln 0, Col 0 Sys 0:<Local> Proc 000:51c Thrd 000:d00 ASM OVR CAPS NUM







```

10 0 obj
<<

  /Count 0
  /Kids [<<

    /Contents 11 0 R
    /Resources <<
      /Font <<
        /F1 <<
          /BaseFont /Arial
        >>
      >>
    >>
  >>]
>>

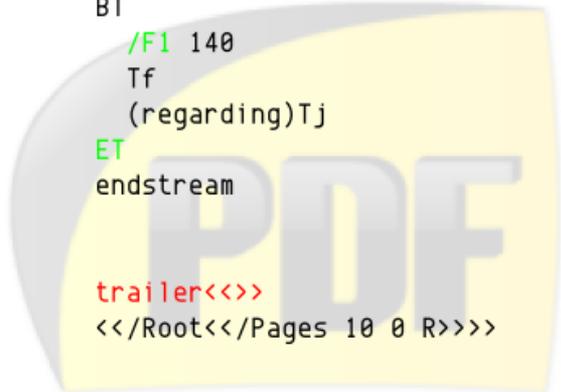
```

```

11 0 obj
<< >>
stream
BT
  /F1 140
  Tf
  (regarding)Tj
ET
endstream

trailer<<>>
<</Root<</Pages 10 0 R>>>>

```



```

%PDF-1.

30 0 obj
<<

  /Kids [<<
    /Parent 30 0 R
    /Contents 31 0 R
    /Resources <<>>
  >>]
>>

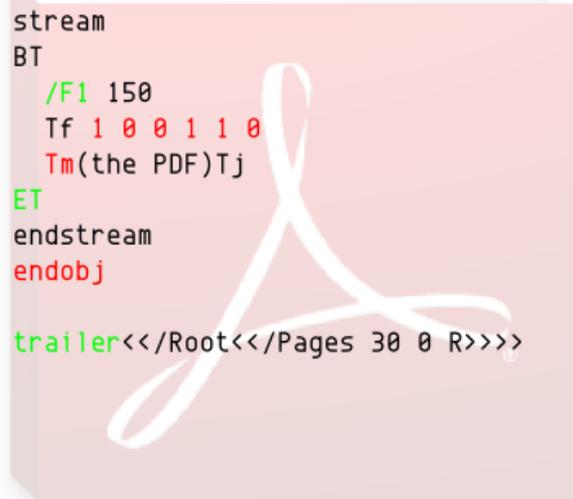
```

```

31 0 obj
<< >>
stream
BT
  /F1 150
  Tf 1 0 0 1 1 0
  Tm(the PDF)Tj
ET
endstream
endobj

trailer<</Root<</Pages 30 0 R>>>>

```



```

%PDF

20 0 obj
<<
  /Pages <<

    /Kids [<<

      /Contents -4294967275 4294967296 R
    >>]
>>
>>

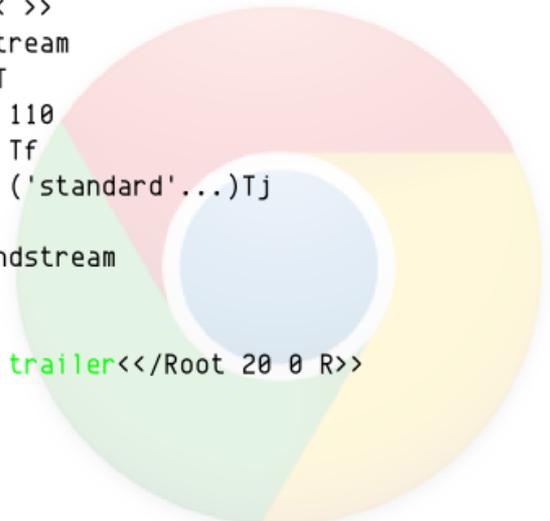
```

```

21 0 obj
<< >>
stream
BT
  110
  Tf
  ('standard'...)Tj
endstream

% trailer<</Root 20 0 R>>

```



```

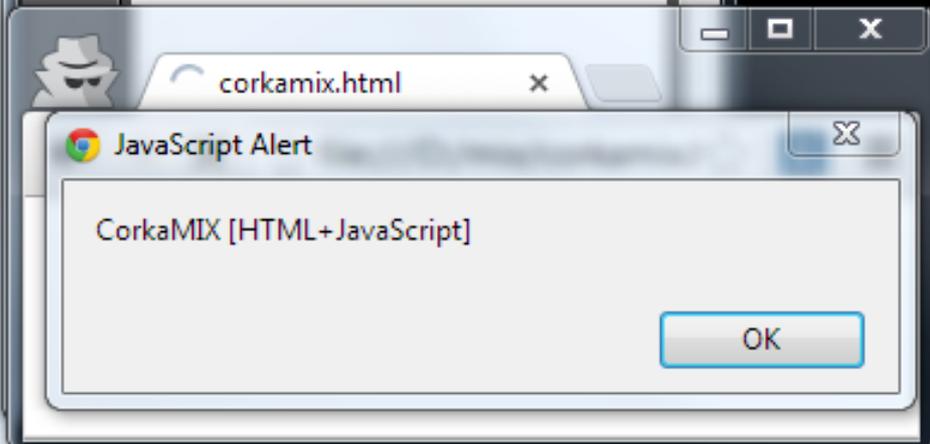
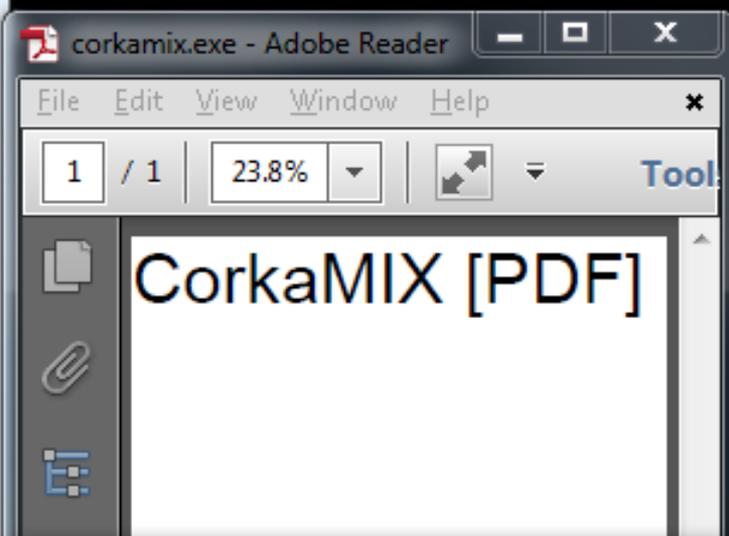
>corkamix.exe
CorkaMIX [PE]
>java -jar corkamix.exe
CorkaMIX [Java CLASS in JAR]

>cmp -b corkamix.exe corkamix_1b.exe
cmp: EOF on corkamix.exe

>python corkamix_1b.exe
CorkaMIX [python]

>copy corkamix.exe corkamix.html
1 file(s) copied.

```



```

db 'MZ'
; [...]
db '%PDF-1.', 0ah
db 'obj<<>>stream', 0ah

db '<html>'
; [...]
    at IMAGE_NT_HEADERS.Signature, db 'PE',0,0
; [...]
    db 0fh, 018h, 111b << 3
    push msg
    call [__imp__printf]
    salc
; [...]
header:
    db 'PK', 3, 4
    dw 0ah ; version_needed
; [...]
_dd 0CAFEBABEh ; signature
_dw 3          ; major version
_dw 2dh       ; minor version
; [...]
    _dd 9 ; length of bytecode
    GETSTATIC 8
    LDC 14
    INVOKEVIRTUAL 16
    RETURN
    _dw 0 ; exceptions_count
    _dw 0 ; attributes_count
; [...]

```



```
demo
$yasm -o corkaminux elf.asm
$java -jar corkaminux
CorkaMInuX [Java]
$chmod +x corkaminux
$./corkaminux
CorkaMInuX [ELF]
$cp corkaminux corkaminux-test.html
$firefox corkaminux-test.html 2> /dev/null &
[1] 24462
$cp corkaminux corkaminux-test.pdf
$vince corkaminux-test.pdf 2> /dev/null &
[2] 24511
$
```

Mozilla Firefox

Connecting...

file:/// ☆ ×

Goog

CorkaMInuX [HTML+JavaScript]

OK

corkaminux-test.pdf

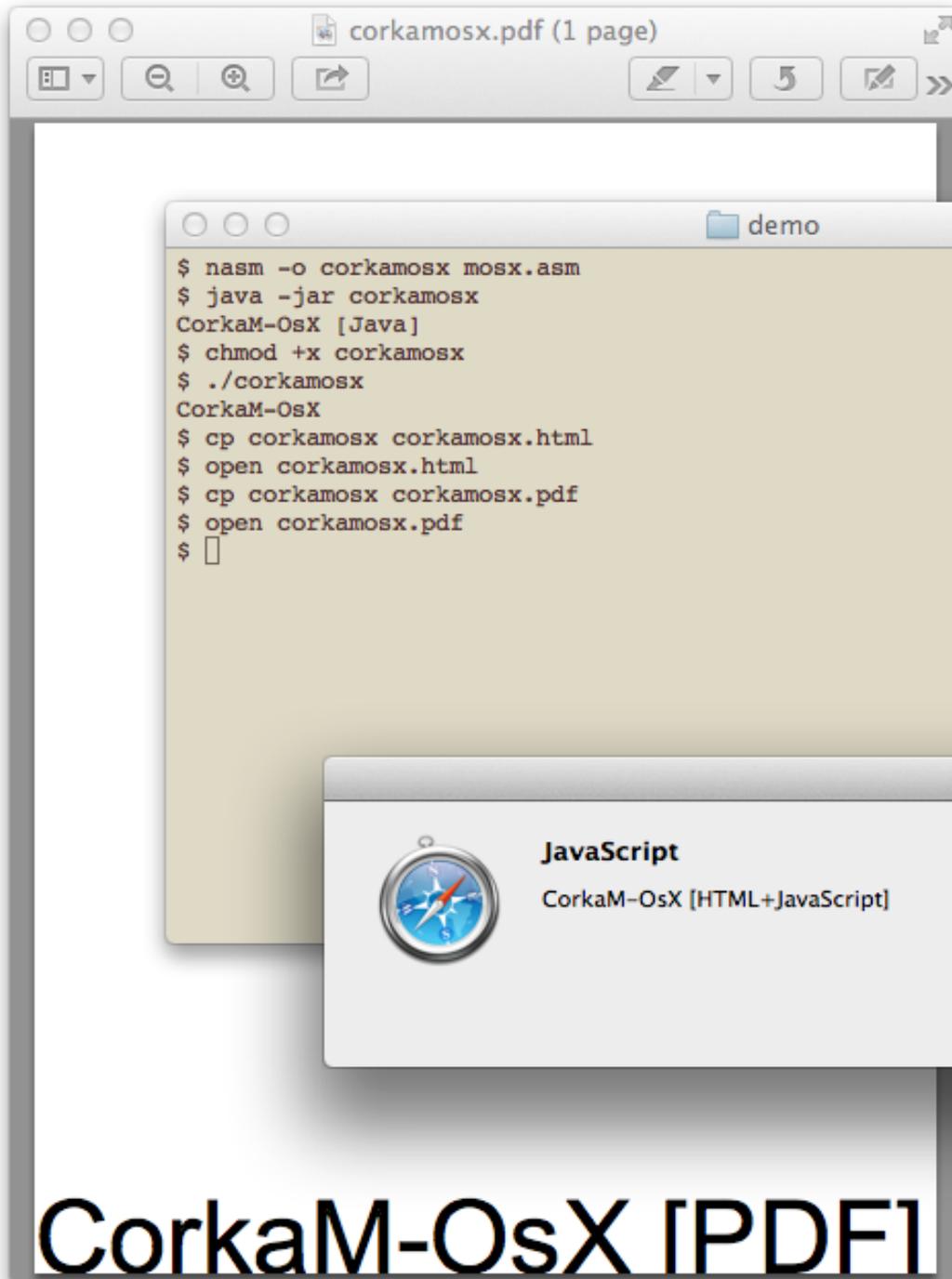
Previous Next 1 (1 of 1)

Thumbnails

CorkaMInuX [PDF] 1

CorkaMInuX [PDF]





CorkaM-OsX [PDF]



l'intérêt?





LOST





SHA256: 2a9c7a16cdb3c3f2285afaf61072dd5e7cc022e97f351cad6234a13e5216f389

SHA1: e27faaa006229f8e4ab97fba7019dc9f2797f84d

MD5: 88cad2b56ab67b43794a0f7a4e690fd5

File size: 1.5 KB (1530 bytes)

File name: corkamix.exe

File type: PDF

Tags: pdf



JEAN
SEBERG
JEAN-PAUL
BELMONDO



un film de
JEAN-LUC CODARD

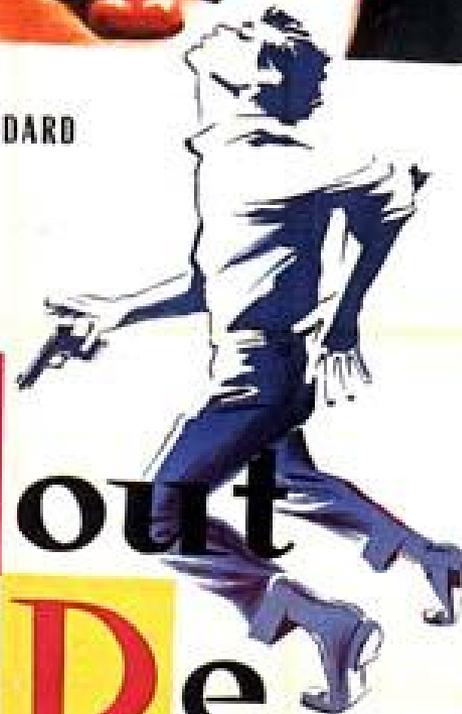


out

De



ouffle...



Scénario original de FRANCIS TRUFFAUT

Scénario adapté de CLAUDE CHABROL

Monté par Henri-Jacques HUIE Liliiane DAYO Claude MANARD VAN DODDE Daniel BOULANGER

Musique de MARTIN SPOELI éditeur Harmonia photographie de René COSTARD

montage GUYBERT DE BOUQUILLON



INTERDIT AUX MOINS DE 18 ANS



Faiblesses

- contourner
 - filtres → exfiltration
 - *same origin policy*
 - détection
 - ex: PE sain mais PDF/HTML/... malveillant
 - faire abandonner
 - déplacer la frontière sain <> corrompu
- déni de service



Conclusion



Conclusion

- la confusion de type, c'est le mal
 - les documentations succinctes, aussi
 - les logiciels laxistes, pareil
- aller plus loin que la documentation
 - Adobe: bien / Sumatra: pas bien
- suggestions
 - + de contrôle sur les extensions
 - isolation des fichiers téléchargés
 - un type = une signature (longue) au dép. 0



Merci à *VOUS* !

(et particulièrement à Olivier et Axel)

Questions ?



http://

rétroconception.échangedepile.fr ;)

reverseengineering

.stackexchange.com

@angealbertini



ange@corkami.com

