

Messing with binary formats

44CON



Ange Albertini
2013/09/13

London, England



reverse engineering & visual documentations

<http://corkami.com>





DOS_HEADER

e_magic

MZ

e_lfanew

40h

NT_HEADERS

Signature

PE\0\0

FILE

HEADER

Machine

14Ch

Characteristics

102h

OPTIONAL

HEADER

```
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
```




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



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

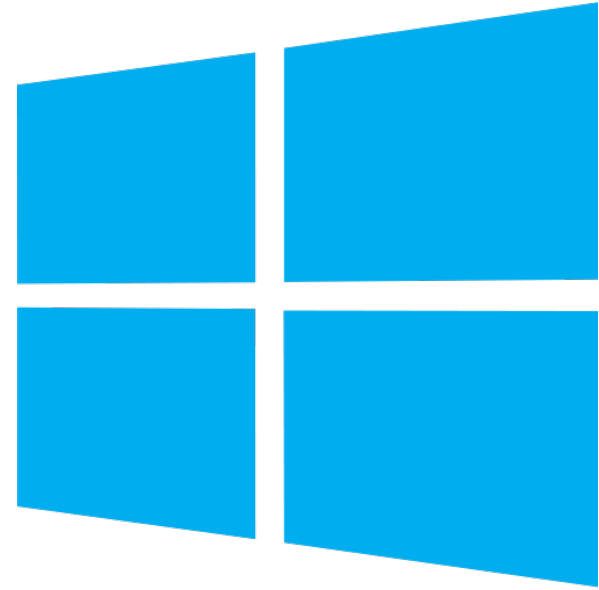


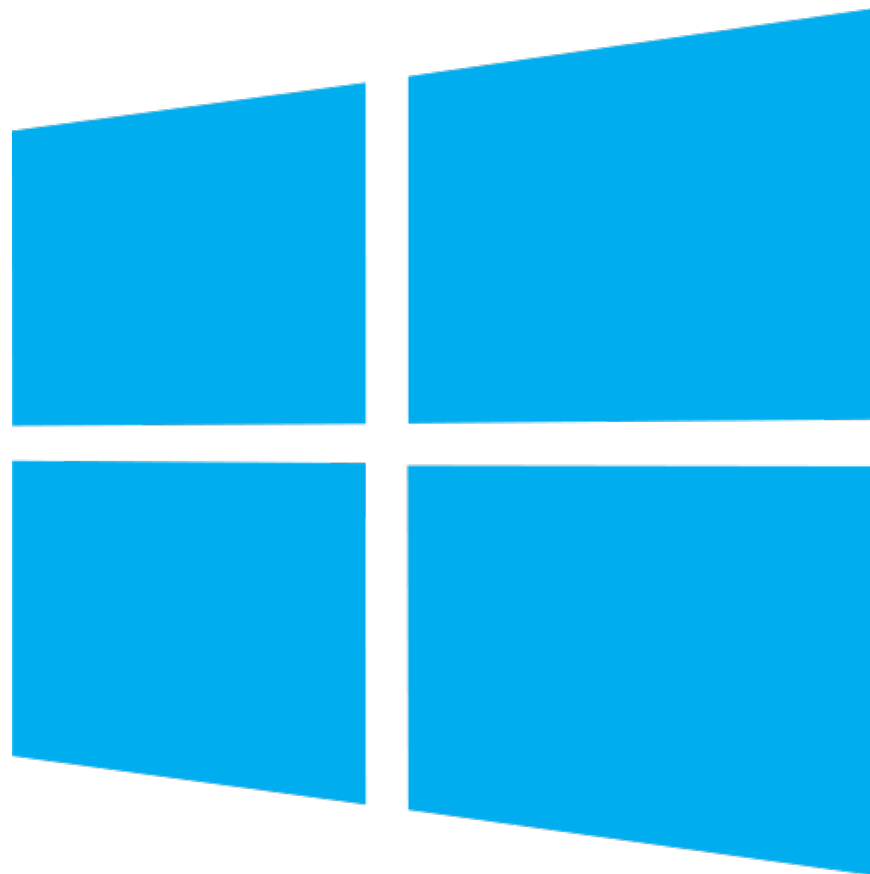
COMPUTER
PROBLEMS CAUSED
BY VIRUSES

HTML



Java





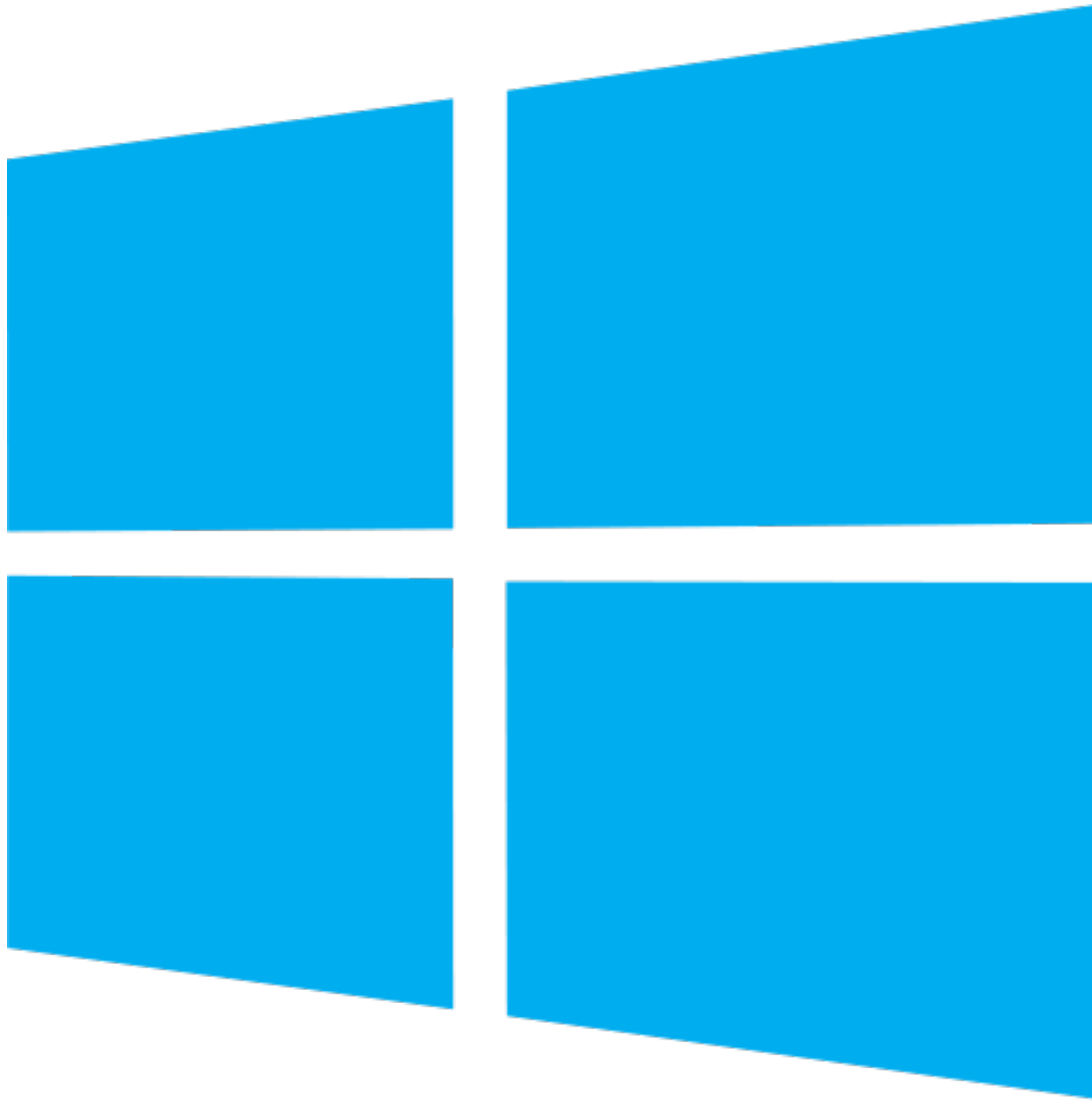


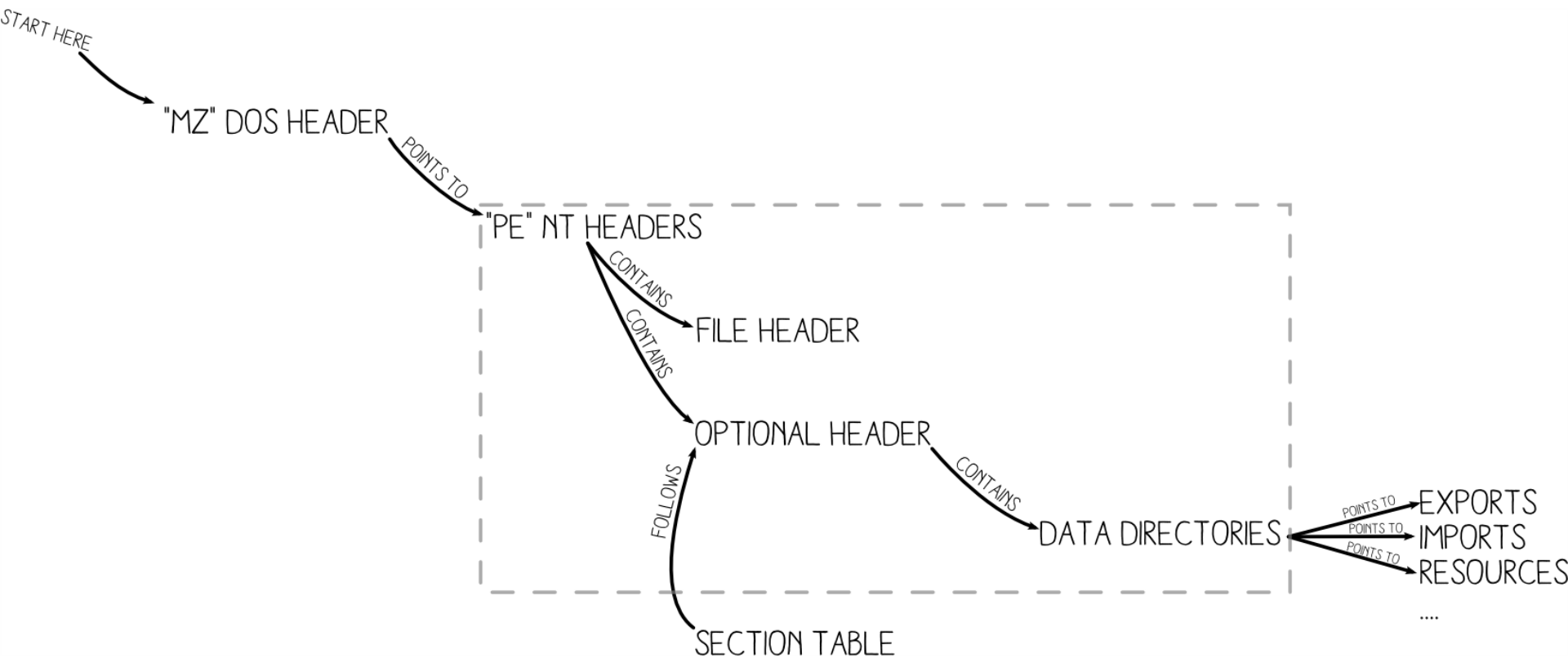
MZ

HTML









Header

MZ

DOS header

since IBM PC-DOS 1.0 (1981)

PE (or NE/LE/LX/...)

'modern' headers

since Windows NT 3.1 (1993)

OFFSET 0

DOS Header

IMAGE_DOS_HEADER

00+2 e_magic MZ

02+2 e_cblp

04+2 e_cp exe size

06+2 e_crlc

08+2 e_cparhdr exe start

0a+2 e_minalloc

0c+2 e_maxalloc

0e+2 e_ss initial ss

10+2 e_sp initial sp

12+2 e_csum

14+2 e_ip

16+2 e_cs

18+2 e_lfarlc

1a+2 e_ovno

1c+2 e_res[4]

24+2 e_oemid

26+2 e_oeminfo

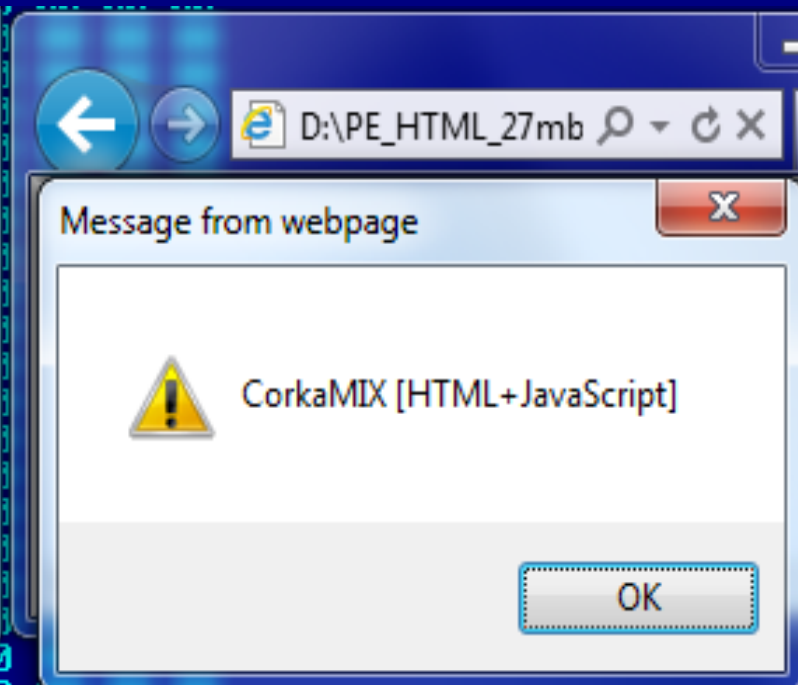
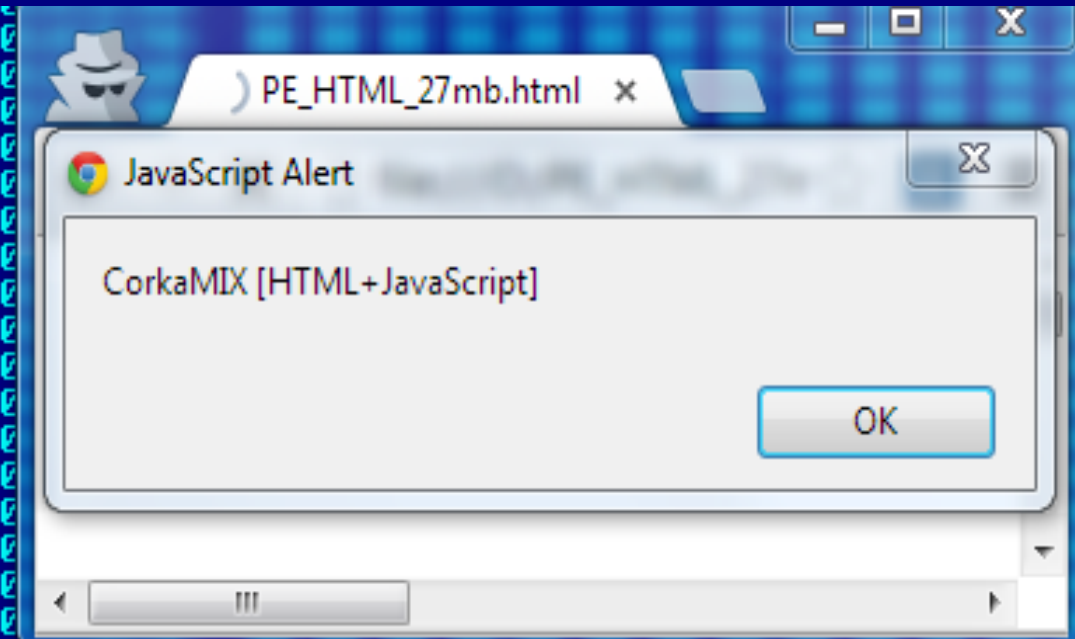
28+2 e_res2[10]

3c+4 e_lfanew

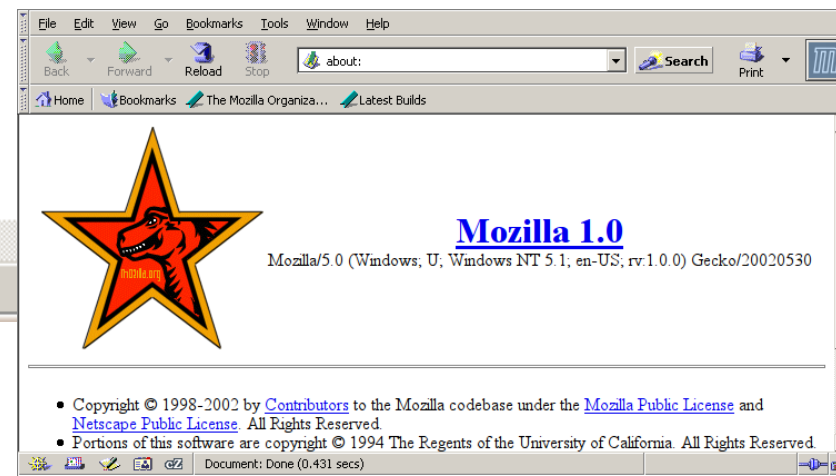
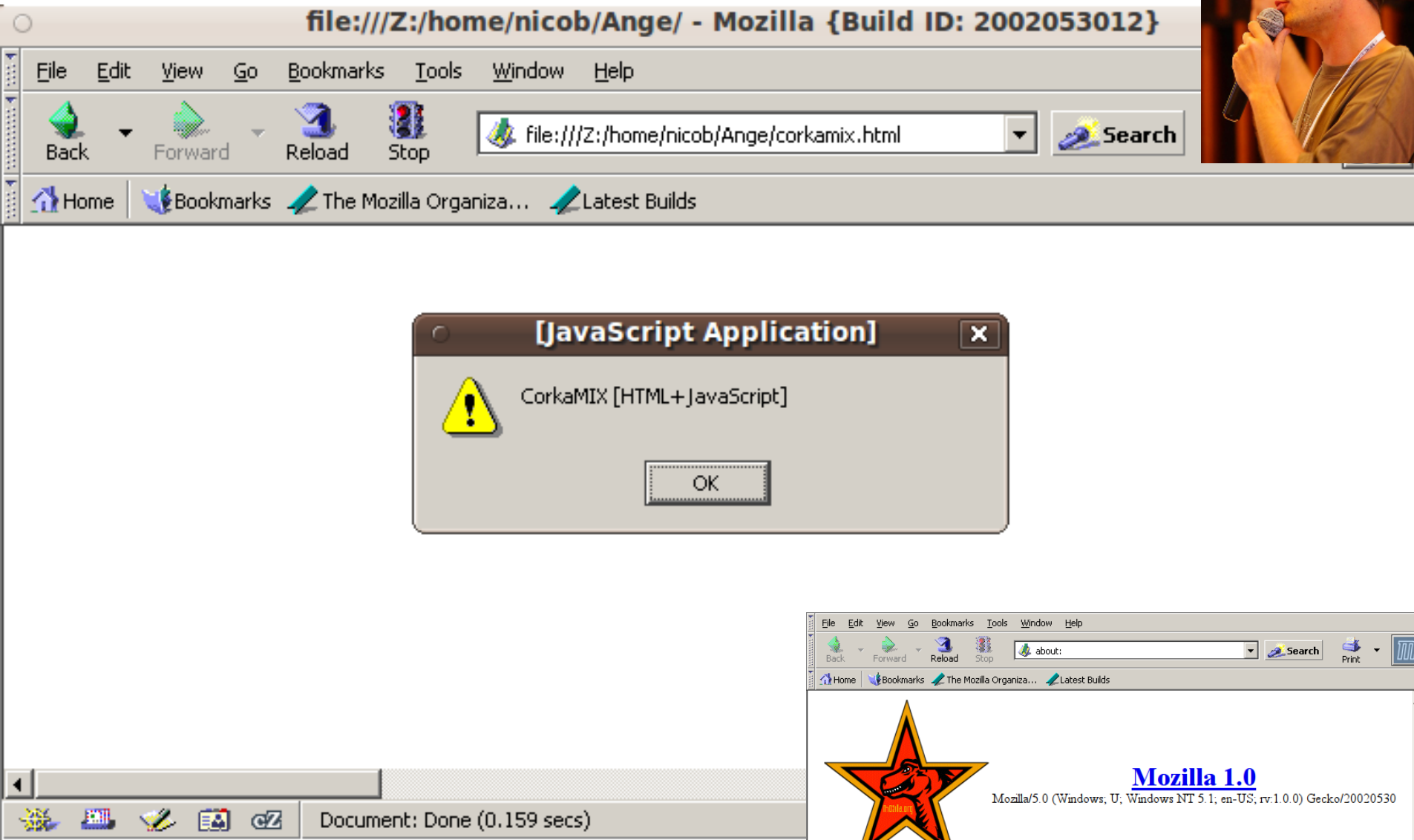
000004A80:	69	74	20	63-6F	64	65	0D-0A	00	49	6E-66	6F	3A	20	code error: 700
000004A90:	36	34	20	62-69	74	73	20-6E	6F	74	20-73	75	70	70	it code Info:
000004AA0:	6F	72	74	65-64	0D	0A	00-00	00	00	00-00	00	00	00	64 bits not supp
000004AB0:	50	45	00	00-4C	01	00	00-D3	F6	5E	81-B1	0F	CB	06	orted
000004AC0:	36	06	E7	32-08	01	0F	01-0B	01	8E	AF-96	D3	5E	A6	PE L@ u: ^ü *r
000004AD0:	ED	48	81	8B-EE	CB	6E	38-00	00	00	00-A8	1D	DA	96	6r2 O*O3Oä>U^
000004AE0:	9B	D5	36	CF-00	00	FD	7E-01	00	00	00-01	00	00	00	8HüiE7m8 i+rü
000004AF0:	C4	5E	A2	35-58	44	C8	EF-04	00	E5	A5-00	00	00	00	ç f6 ± ²~@ @
000004B00:	D6	4B	00	00-D5	4B	00	00-18	E7	A9	01-03	00	70	9A	-^ó5XDLn♦ σÑ
000004B10:	C7	BD	12	00-A8	1A	00	00-06	9E	12	00-23	01	00	00	K FK ↑r-@♥ pü
000004B20:	A5	2B	4A	CE-6D	43	B9	B2-10	26	00	00-68	A8	1A	57	W↑ i→ R↑ #@
000004B30:	B8	24	00	00-26	81	CD	27-00	00	00	00-78	EA	0B	F5	N+JmC!& hç→W
000004B40:	63	0F	2B	56-0C	31	BE	17-8B	67	C2	18-0B	64	F5	D8	q\$ &ü=' xΩδJ
000004B50:	C0	27	00	00-14	00	00	00-08	CA	8D	9A-00	00	00	00	c*+Uq1d iigT↑δdJ÷
000004B60:	61	F5	9F	CE-CE	B3	CF	BA-83	3E	46	89-5D	1D	1E	F9	L' ¶ iü
000004B70:	FC	00	00	00-02	A1	E7	60-00	00	00	00-E9	88	52	8D	aJf ÷ â>Fël+▲·
000004B80:	00	00	00	00-34	DD	53	D4-88	24	00	00-B9	01	00	00	" 0i r' 0êRi
000004B90:	7C	4F	57	9E-CB	D2	98	DC-00	00	00	00-A6	59	CD	93	4 S ê\$ i @
000004BA0:	E2	D1	5E	B4-95	25	BB	0B-FF	35	FC	02-FD	7E	E8	2D	LOWRmÿ ðY=ô
000004BB0:	B7	FF	FF	C3-00	00	00	00-00	00	00	00-00	00	00	00	r_T^ 0%ñδ 5"0²~ö-
000004BC0:	0D	0A	00	FF-25	90	24	FD-7E	00	00	00-00	00	00	00	¶
000004BD0:	FF	25	94	24-FD	7E	-	-	-	-	-	-	-	-	J@ %É\$²~
														%ö\$²~

HTML





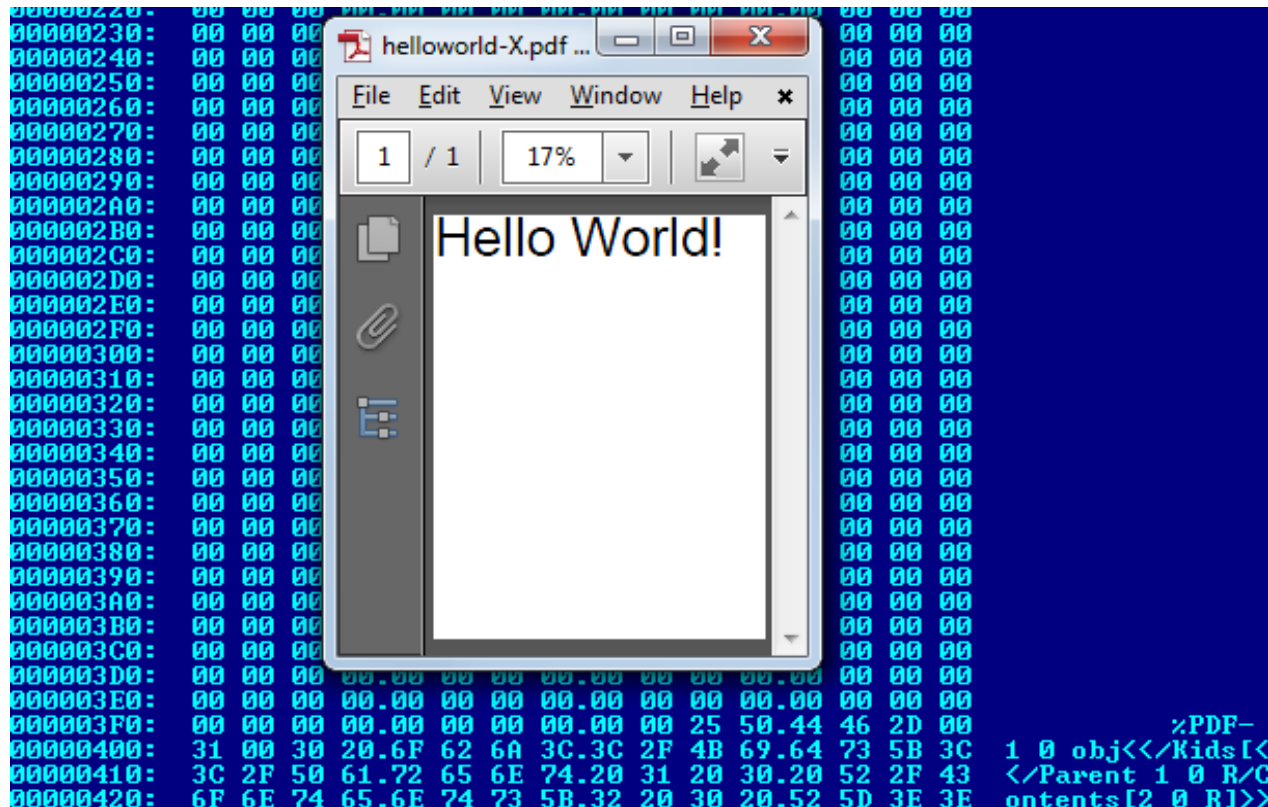
```
01A5B2A0: 00 00 00 00.00 00 00 00.00 00 00 00.00 00 00 00.00
01A5B2B0: 00 00 00 00.00 00 00 00.00 00 00 00.00 00 00 00.00
01A4B2C0: 3C 68 74 6D.6C 3E 0D 0A.3C 62 6F 64.79 3E 3C 73
01A4B2D0: 74 79 6C 65.3E 62 6F 64.79 20 7B 20.76 69 73 69
01A4B2E0: 62 69 6C 69.74 79 3A 68.69 64 64 65.6E 3B 7D 20
01A4B2F0: 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>Jf<body><s
tyle>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><!--
```



7.5.2 File Header

The first line of a PDF file shall be a *header* consisting of the 5 characters `%PDF-` followed by a version number of the form 1.N, where N is a digit between 0 and 7.



3.4.1, "File Header"

13. Acrobat viewers require only that the header appear somewhere within the first 1024 bytes of the file.

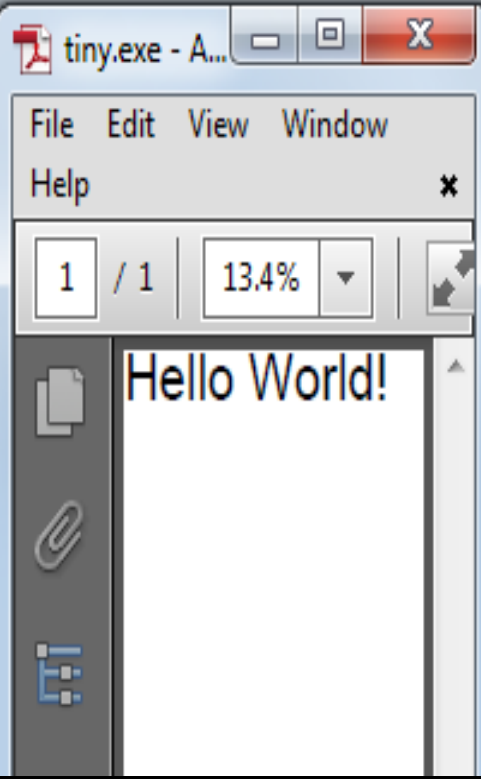
contactenation PE PDF

```
>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
```



The screenshot shows a Windows XP desktop with three windows open. The background window is a Notepad instance titled 'Hiew: NOTEPAD.EXE' displaying a hex dump of a file named 'NOTEPAD.EXE'. The hex dump shows various byte sequences, including 'MZ', 'PE', and 'stream'. Overlaid on this is a Notepad window titled 'NOTEPAD.EXE - Adobe Reader' which is displaying a PDF document. The PDF content includes the title 'Zythom', the subtitle 'Dans la peau d'un informaticien expert judiciaire', and 'Tome 1'. Below this, there is a quote in French: '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 conscience.' The third window in the foreground is a small Notepad window titled 'Untitled - Notepad' which is empty.



```
>yasm -o test.jar zip.asm
```

```
>unzip -lv test.jar
```

Length	Method	Size	Ratio	Date	Time	CRC-32	Name
0	Stored	0	0%	00/00/80	00:00	00000000	META-INF/
35	Stored	35	0%	00/00/80	00:00	deadbeef	META-INF/MANIFEST.MF
299	Stored	299	0%	00/00/80	00:00	0badbabe	test.class
334		334	0%				3 files

```
>unzip -t test.jar
```

```
Archive: test.jar
```

```
testing: META-INF/
```

```
OK
```

```
testing: META-INF/MANIFEST.MF
```

```
bad CRC
```

```
8391c53a
```

```
<should be deadbeef>
```

```
testing: test.class
```

```
bad CRC
```

```
7846a510
```

```
<should be 0badbabe>
```

```
At least one error was detected in test.jar.
```

```
>java -jar test.jar
```

```
Java: Working! <with wrong CRCs>
```

```
>
```

Structure

1. start

- PE Signature
 - %PDF + fake *obj* start
 - HTML comment start

2. next

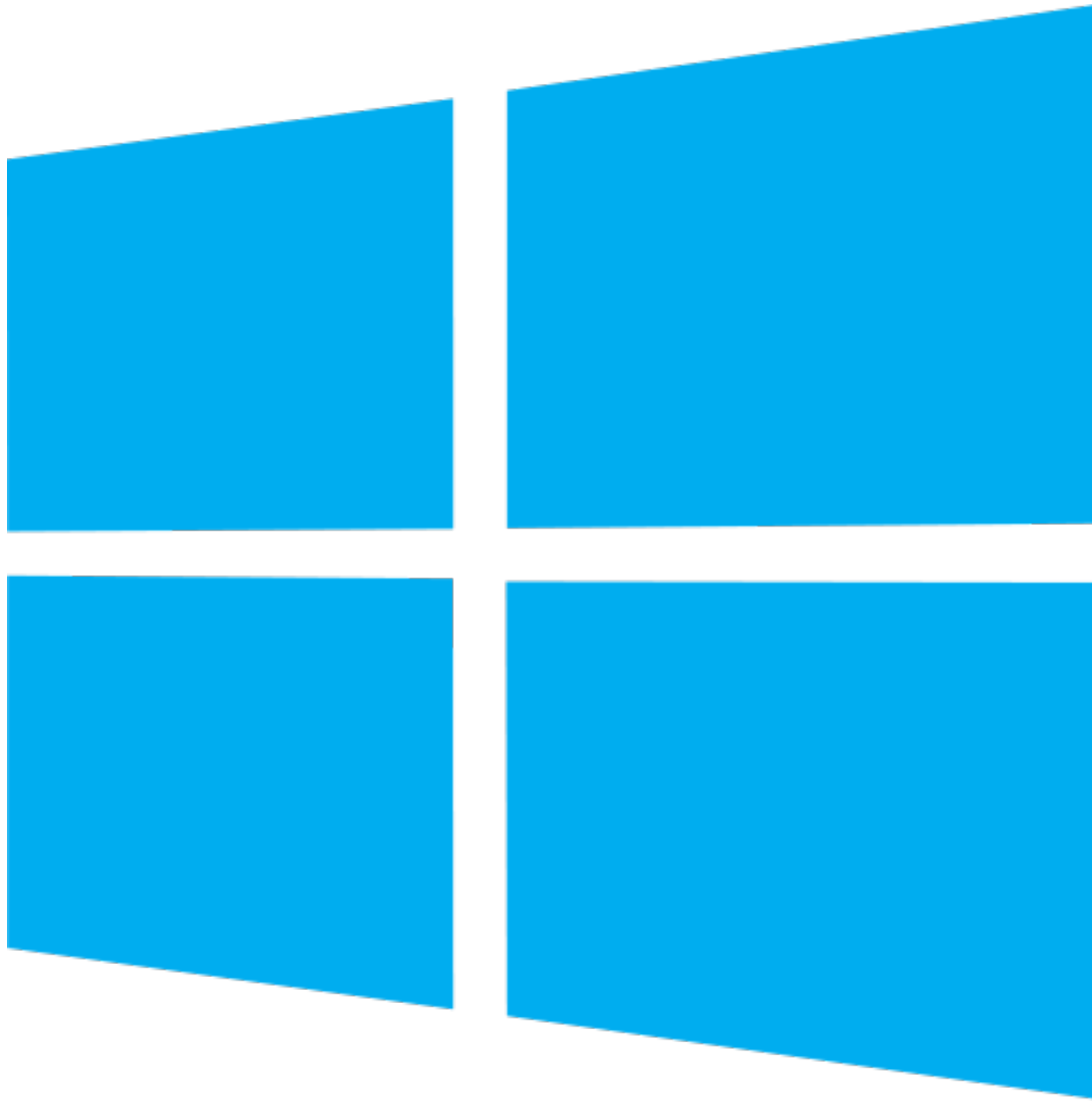
- PE (next)
- HTML
- PDF (next)

3. bottom

- ZIP



DEMO



MZ

PE LO

8

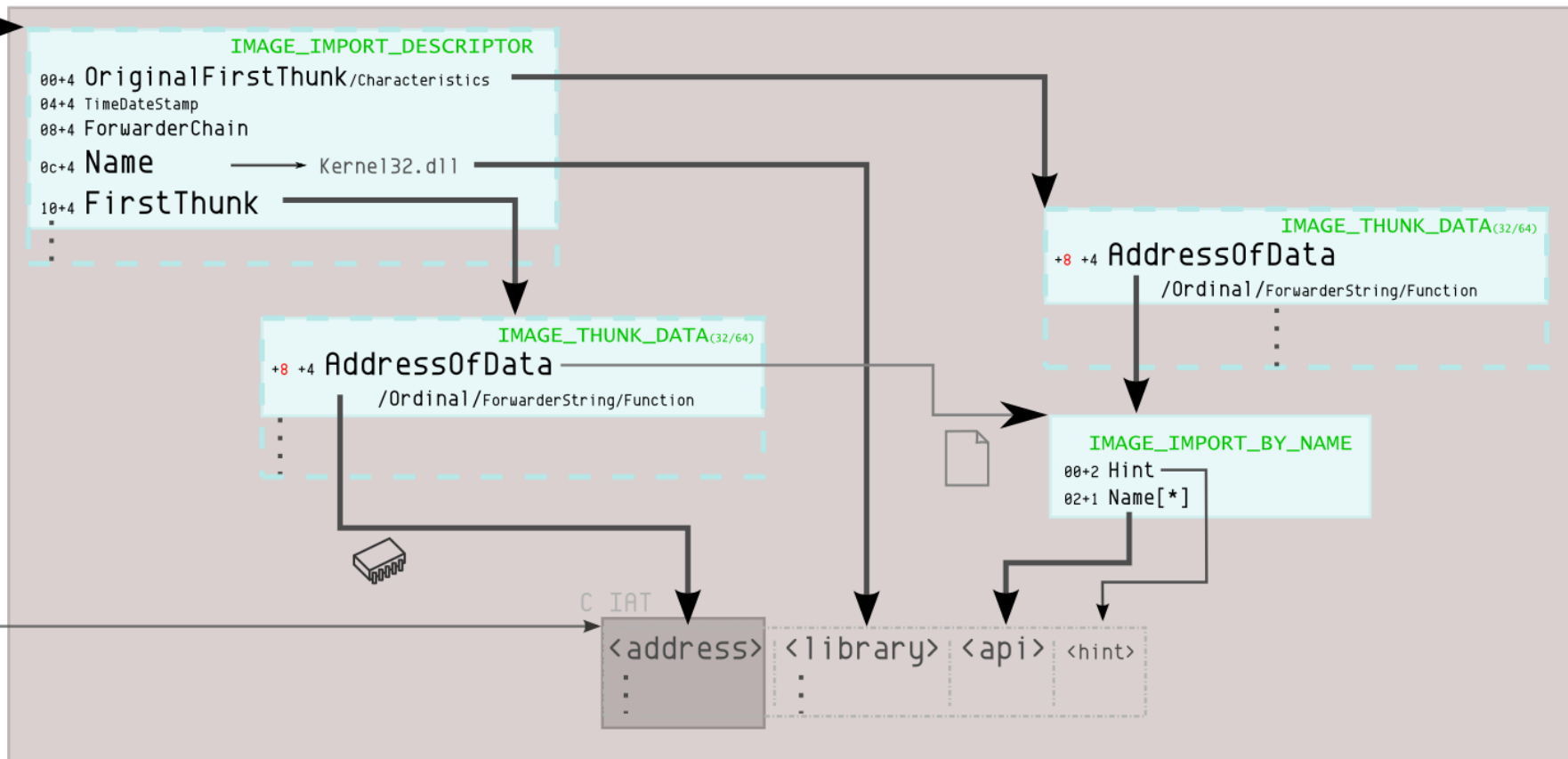
H

li*x t

```

    00000000  7f 45 34 76 5a 52 51 50 4f 4e 4d 4c 4b 4a 49 48  .ZE v
    00000010  47 46 45 44 43 42 41 40 3f 3e 3d 3c 3b 3a 39 38  .
    00000020  37 36 35 34 33 32 31 30 2f 2e 2d 2c 2b 2a 29 28  .
    00000030  27 26 25 24 23 22 21 20 1f 1e 1d 1c 1b 1a 19 18  .
    00000040  17 16 15 14 13 12 11 10 0f 0e 0d 0c 0b 0a 09 08  .
    00000050  07 06 05 04 03 02 01 00 ff fd fb fa f9 f8 f7 f6  .
    00000060  f5 f4 f3 f2 f1 f0 e7 e6 e5 e4 e3 e2 e1 e0 d7 d6  .
    00000070  d5 d4 d3 d2 d1 d0 c7 c6 c5 c4 c3 c2 c1 c0 b7 b6  .
    00000080  b5 b4 b3 b2 b1 b0 a7 a6 a5 a4 a3 a2 a1 a0 97 96  .
    00000090  95 94 93 92 91 90 87 86 85 84 83 82 81 80 77 76  .
    000000a0  75 74 73 72 71 70 67 66 65 64 63 62 61 60 57 56  .
    000000b0  55 54 53 52 51 50 47 46 45 44 43 42 41 40 37 36  .
    000000c0  35 34 33 32 31 30 27 26 25 24 23 22 21 20 17 16  .
    000000d0  15 14 13 12 11 10 07 06 05 04 03 02 01 00 ff fd  .
    000000e0  fb fa f9 f8 f7 f6 f5 f4 f3 f2 f1 f0 e7 e6 e5 e4  .
    000000f0  e3 e2 e1 e0 d7 d6 d5 d4 d3 d2 d1 d0 c7 c6 c5 c4  .
    00000100  c3 c2 c1 c0 b7 b6 b5 b4 b3 b2 b1 b0 a7 a6 a5 a4  .
    00000110  a3 a2 a1 a0 97 96 95 94 93 92 91 90 87 86 85 84  .
    00000120  83 82 81 80 77 76 75 74 73 72 71 70 67 66 65 64  .
    00000130  63 62 61 60 57 56 55 54 53 52 51 50 47 46 45 44  .
    00000140  43 42 41 40 37 36 35 34 33 32 31 30 27 26 25 24  .
    00000150  23 22 21 20 17 16 15 14 13 12 11 10 07 06 05 04  .
    00000160  03 02 01 00 ff fd fb fa f9 f8 f7 f6 f5 f4 f3 f2  .
    00000170  f1 f0 e7 e6 e5 e4 e3 e2 e1 e0 d7 d6 d5 d4 d3 d2  .
    00000180  d1 d0 c7 c6 c5 c4 c3 c2 c1 c0 b7 b6 b5 b4 b3 b2  .
    00000190  b1 b0 a7 a6 a5 a4 a3 a2 a1 a0 97 96 95 94 93 92  .
    000001a0  91 90 87 86 85 84 83 82 81 80 77 76 75 74 73 72  .
    000001b0  71 70 67 66 65 64 63 62 61 60 57 56 55 54 53 52  .
    000001c0  51 50 47 46 45 44 43 42 41 40 37 36 35 34 33 32  .
    000001d0  31 30 27 26 25 24 23 22 21 20 17 16 15 14 13 12  .
    000001e0  11 10 07 06 05 04 03 02 01 00 ff fd fb fa f9 f8  .
    000001f0  f7 f6 f5 f4 f3 f2 f1 f0 e7 e6 e5 e4 e3 e2 e1 e0  .
    00000200  d7 d6 d5 d4 d3 d2 d1 d0 c7 c6 c5 c4 c3 c2 c1 c0  .
    00000210  b7 b6 b5 b4 b3 b2 b1 b0 a7 a6 a5 a4 a3 a2 a1 a0  .
    00000220  97 96 95 94 93 92 91 90 87 86 85 84 83 82 81 80  .
    00000230  77 76 75 74 73 72 71 70 67 66 65 64 63 62 61 60  .
    00000240  57 56 55 54 53 52 51 50 47 46 45 44 43 42 41 40  .
    00000250  37 36 35 34 33 32 31 30 27 26 25 24 23 22 21 20  .
    00000260  17 16 15 14 13 12 11 10 07 06 05 04 03 02 01 00  .
    00000270  ff fd fb fa f9 f8 f7 f6 f5 f4 f3 f2 f1 f0 e7 e6  .
    00000280  e5 e4 e3 e2 e1 e0 d7 d6 d5 d4 d3 d2 d1 d0 c7 c6  .
    00000290  c5 c4 c3 c2 c1 c0 b7 b6 b5 b4 b3 b2 b1 b0 a7 a6  .
    000002a0  a5 a4 a3 a2 a1 a0 97 96 95 94 93 92 91 90 87 86  .
    000002b0  85 84 83 82 81 80 77 76 75 74 73 72 71 70 67 66  .
    000002c0  65 64 63 62 61 60 57 56 55 54 53 52 51 50 47 46  .
    000002d0  45 44 43 42 41 40 37 36 35 34 33 32 31 30 27 26  .
    000002e0  25 24 23 22 21 20 17 16 15 14 13 12 11 10 07 06  .
    000002f0  05 04 03 02 01 00 ff fd fb fa f9 f8 f7 f6 f5 f4  .
    00000300  f3 f2 f1 f0 e7 e6 e5 e4 e3 e2 e1 e0 d7 d6 d5 d4  .
    00000310  d3 d2 d1 d0 c7 c6 c5 c4 c3 c2 c1 c0 b7 b6 b5 b4  .
    00000320  b3 b2 b1 b0 a7 a6 a5 a4 a3 a2 a1 a0 97 96 95 94  .
    00000330  93 92 91 90 87 86 85 84 83 82 81 80 77 76 75 74  .
    00000340  73 72 71 70 67 66 65 64 63 62 61 60 57 56 55 54  .
    00000350  53 52 51 50 47 46 45 44 43 42 41 40 37 36 35 34  .
    00000360  33 32 31 30 27 26 25 24 23 22 21 20 17 16 15 14  .
    00000370  13 12 11 10 07 06 05 04 03 02 01 00 ff fd fb fa  .
    00000380  f9 f8 f7 f6 f5 f4 f3 f2 f1 f0 e7 e6 e5 e4 e3 e2  .
    00000390  e1 e0 d7 d6 d5 d4 d3 d2 d1 d0 c7 c6 c5 c4 c3 c2  .
    000003a0  c1 c0 b7 b6 b5 b4 b3 b2 b1 b0 a7 a6 a5 a4 a3 a2  .
    000003b0  a1 a0 97 96 95 94 93 92 91 90 87 86 85 84 83 82  .
    000003c0  81 80 77 76 75 74 73 72 71 70 67 66 65 64 63 62  .
    000003d0  61 60 57 56 55 54 53 52 51 50 47 46 45 44 43 42  .
    000003e0  41 40 37 36 35 34 33 32 31 30 27 26 25 24 23 22  .
    000003f0  21 20 17 16 15 14 13 12 11 10 07 06 05 04 03 02  .
    00000400  01 00 ff fd fb fa f9 f8 f7 f6 f5 f4 f3 f2 f1 f0  .
    00000410  e7 e6 e5 e4 e3 e2 e1 e0 d7 d6 d5 d4 d3 d2 d1 d0  .
    00000420  c7 c6 c5 c4 c3 c2 c1 c0 b7 b6 b5 b4 b3 b2 b1 b0  .
    00000430  a7 a6 a5 a4 a3 a2 a1 a0 97 96 95 94 93 92 91 90  .
    00000440  87 86 85 84 83 82 81 80 77 76 75 74 73 72 71 70  .
    00000450  67 66 65 64 63 62 61 60 57 56 55 54 53 52 51 50  .
    00000460  47 46 45 44 43 42 41 40 37 36 35 34 33 32 31 30  .
    00000470  27 26 25 24 23 22 21 20 17 16 15 14 13 12 11 10  .
    00000480  07 06 05 04 03 02 01 00 ff fd fb fa f9 f8 f7 f6  .
    00000490  f5 f4 f3 f2 f1 f0 e7 e6 e5 e4 e3 e2 e1 e0 d7
```

1 Imports



IMAGE_IMPORT_DESCRIPTOR

IMAGE_THUNK_DATA

00 dd AddressOfData
00000000

0c dd Name

10 FirstThunk

terminator

'msvcrt.d11',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>40 A</small>	Shift Grp 2 ^{1A} Ev, 1 <small>40 A</small>		Eb, CL <small>40 A</small>	Ev, CL <small>40 A</small>	AAM ⁱ⁶⁴ lb	AAD ⁱ⁶⁴ 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
		vmmovs	vmmovs	cutps2ps	vmmovps	cutps2pi	cutps2pi	vmmovss	vmmovss

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

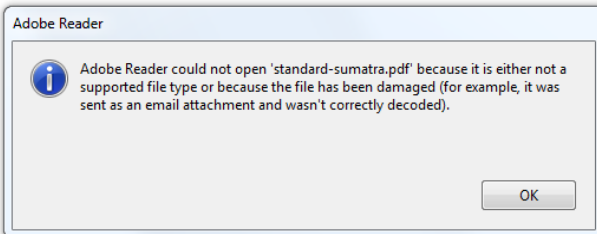
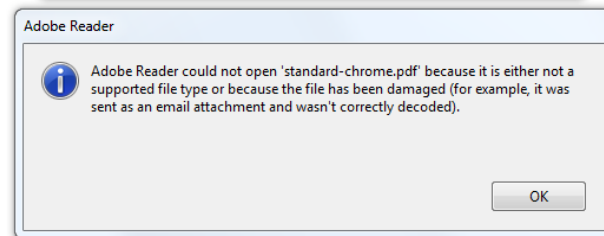
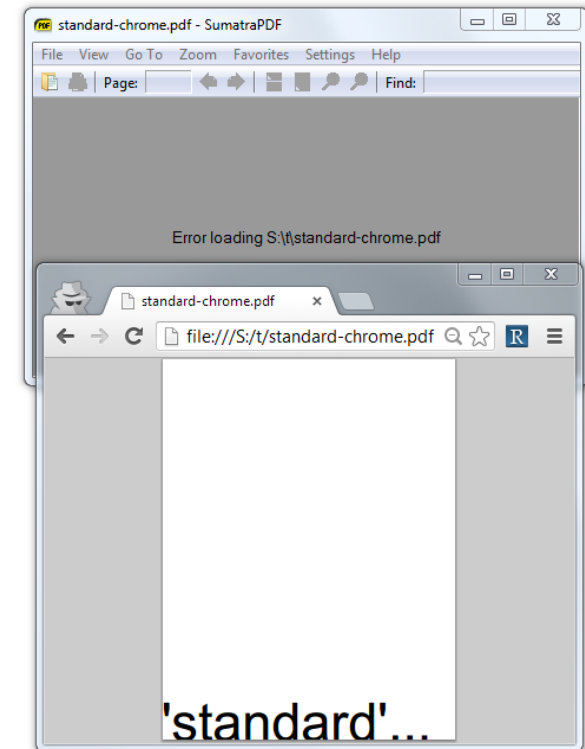
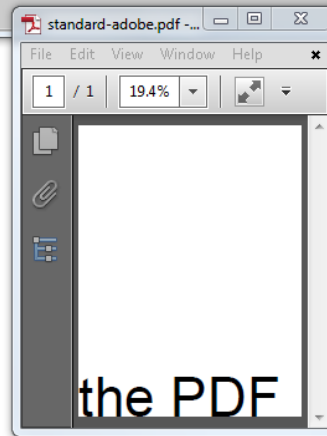
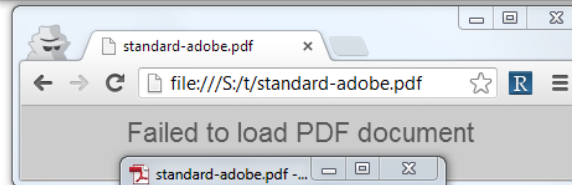
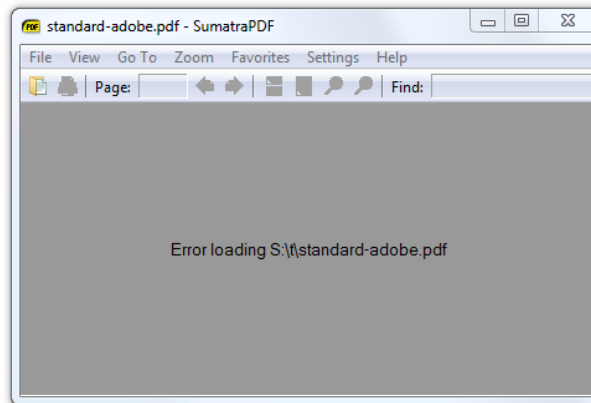
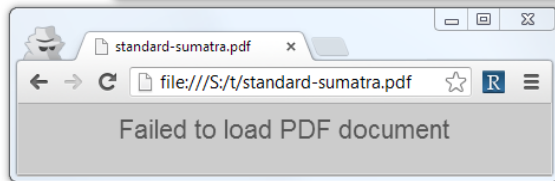
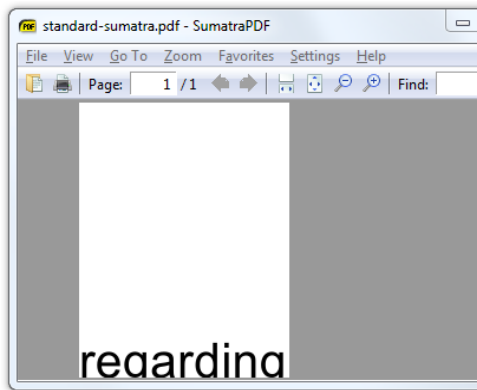
ASM

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

-
<</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
    >>]
  >>
>>

```

```

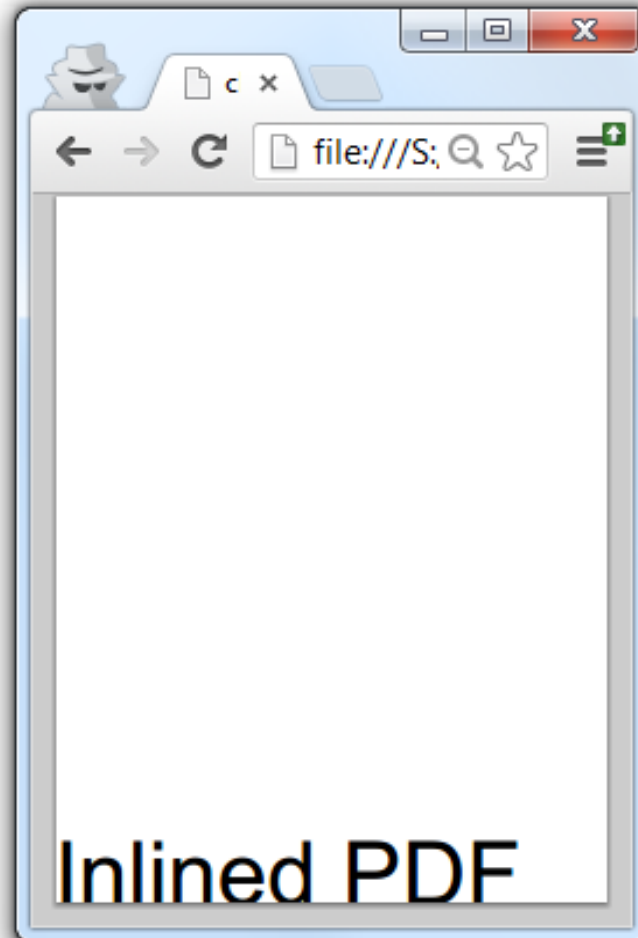
21 0 obj
<< >>
stream
BT
110
Tf
('standard'...)Tj
endstream

% trailer
<</Root 20 0 R>>

```

All streams must be indirect objects (see Section 3.2.9, “Indirect Objects”) and the stream dictionary must be a direct object. The keyword **stream** that follows the stream dictionary should be followed by an end-of-line marker consisting of either a carriage return and a line feed or just a line feed, and not by a carriage

```
%PDF*****
1 0 obj
<<
  /Size 2
  /W[[1/]]
  /Root 1 0 R
  /Pages<<
    /Kids[<<
      /Contents<<>>
      stream
      BT{99
      Tf{Td(Inlined PDF)'}
      endstream
    >>]
  >>
>>
stream
*
endstream
startxref%*****
```



```

%PDF-1.1
1 0 obj
<<
%      /Type /Catalog
...
>>
endobj

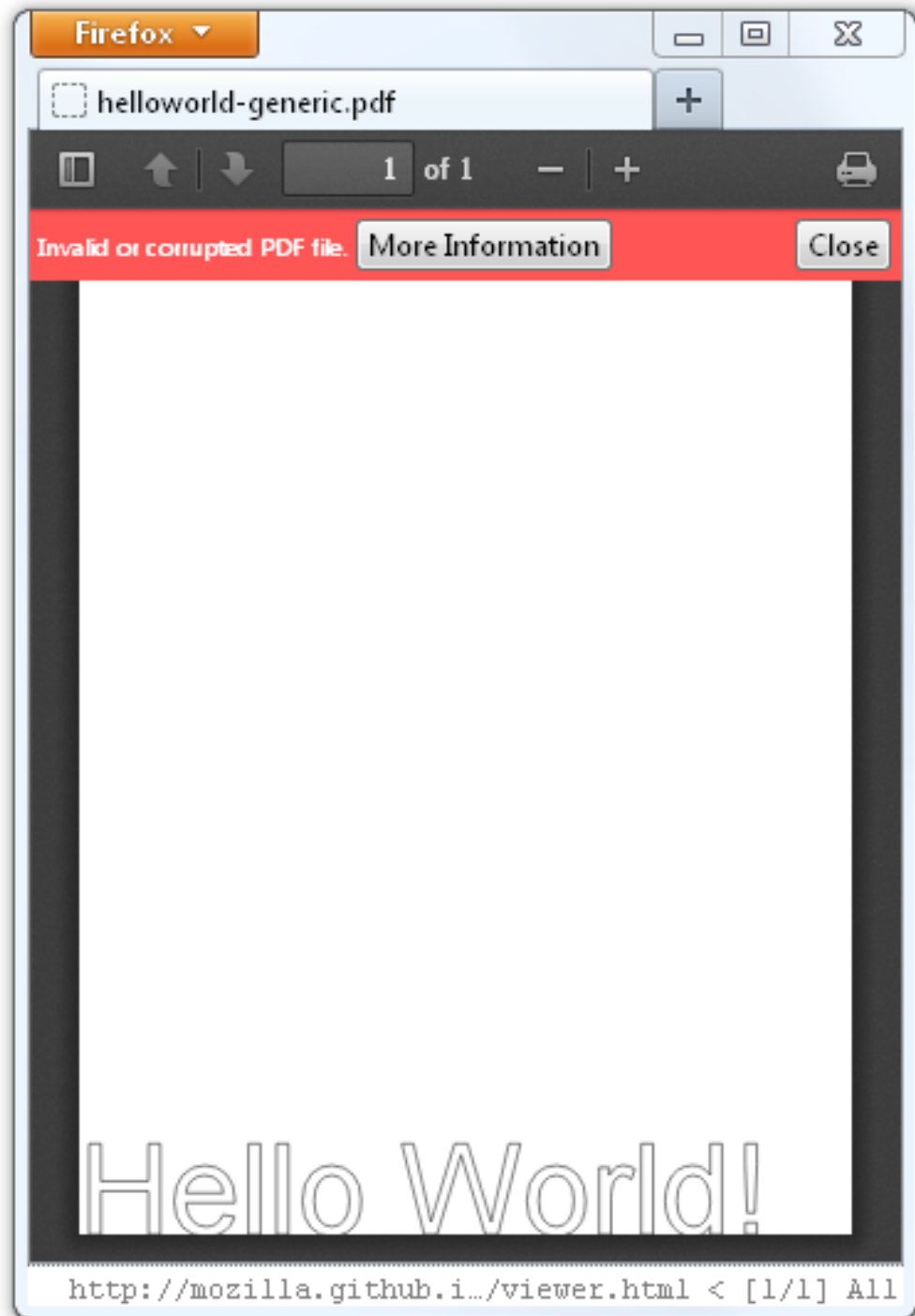
2 0 obj
<<
      /Type /Pages
...
>>
endobj

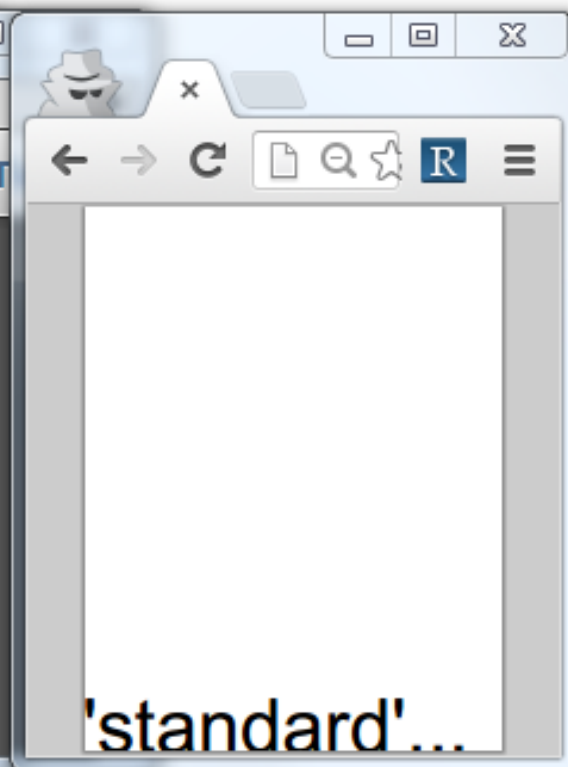
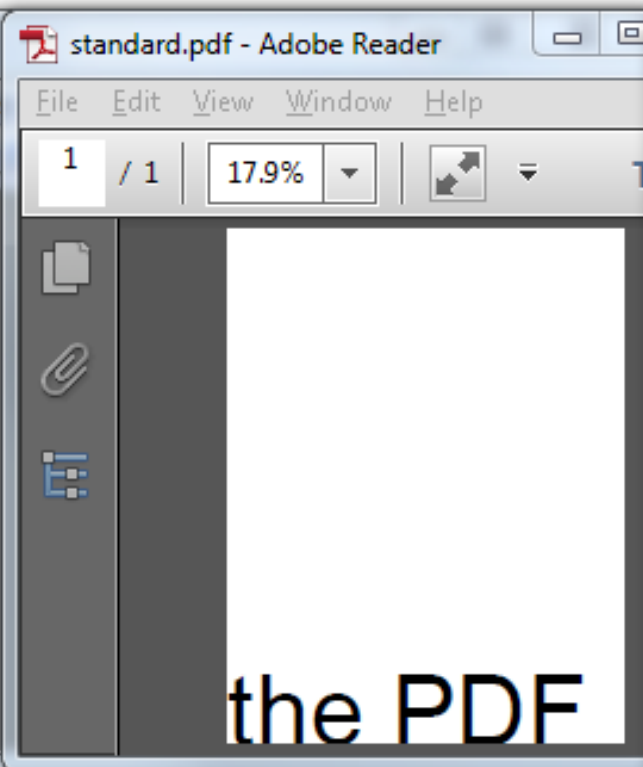
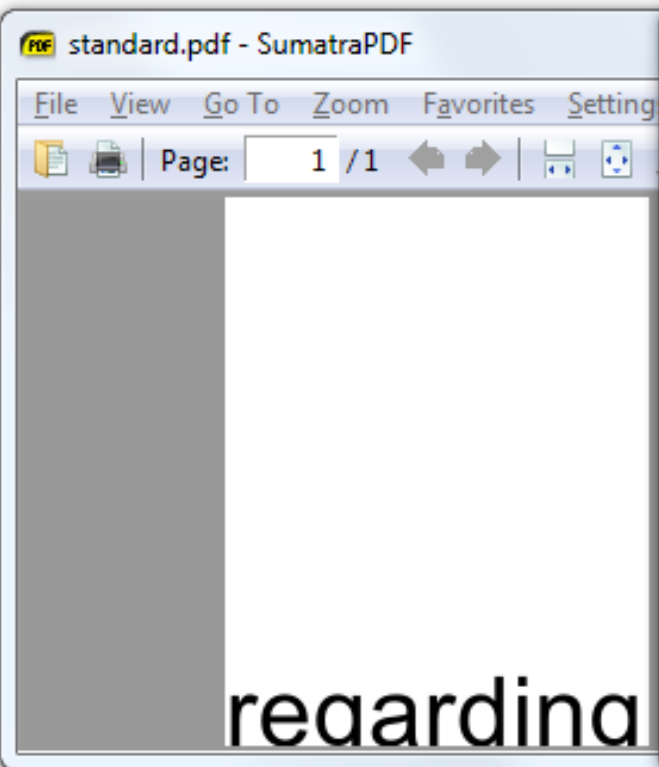
3 0 obj
<<
      /Type /Page
      /Resources <<
        /Font <<
          /F1 <<
            /Type /Font
            /Subtype
/Type1
...
          >>
        >>
      >>
    >>
endobj

4 0 obj
<< /Length 47>>
stream
...

xref
0 1
0000000000 65535 f
0000000010 00000 n
...

```





alternate

REALITY
DEMO


```

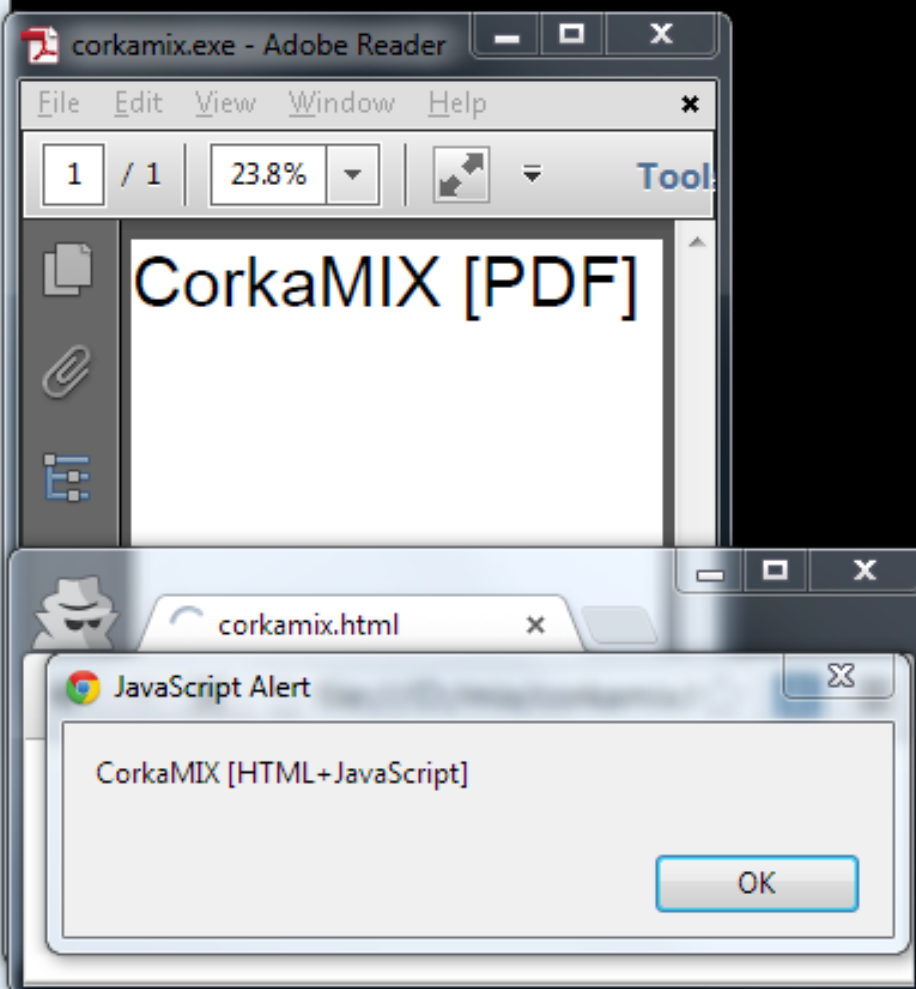
>corkamix.exe
CorkaMIX [PE]
>java -jar corkamix.exe
CorkaMIX [Java CLASS in JAR]

>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
; [...]

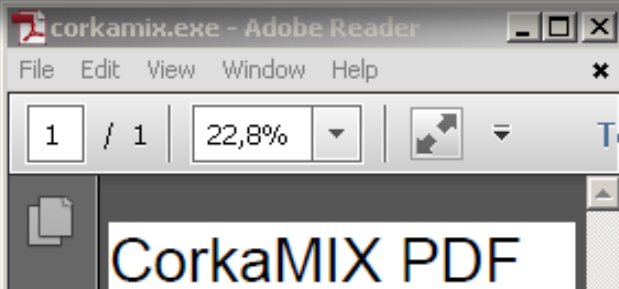
    _dd 9 ; length of bytecode
    GETSTATIC 8
    LDC 14
    INVOKEVIRTUAL 16
    RETURN
    _dw 0 ; exceptions_count
    _dw 0 ; attributes_count
; [...]

```

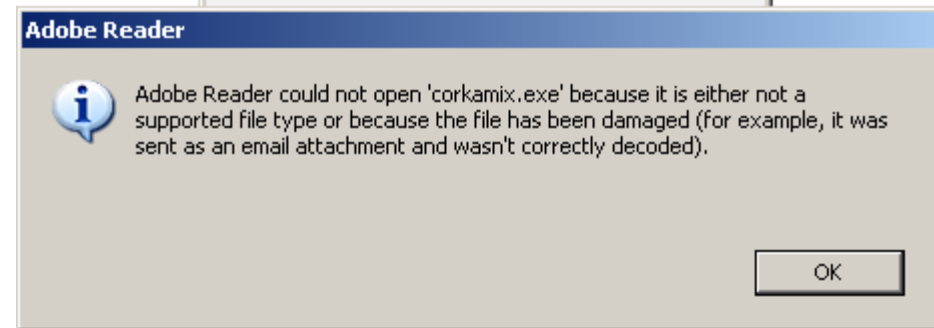
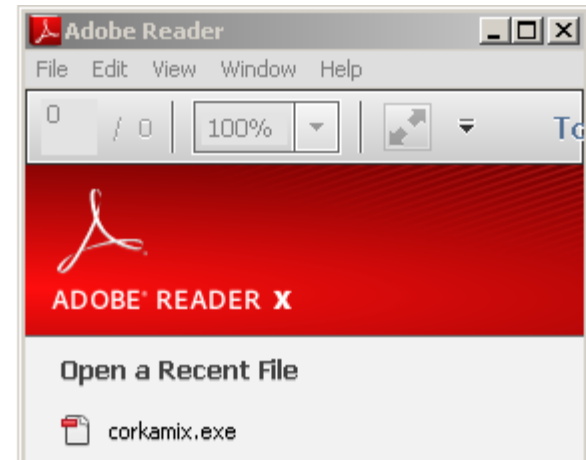
Portions copyright Right Hemisphere, Inc.

Version 10.1.4

Legal

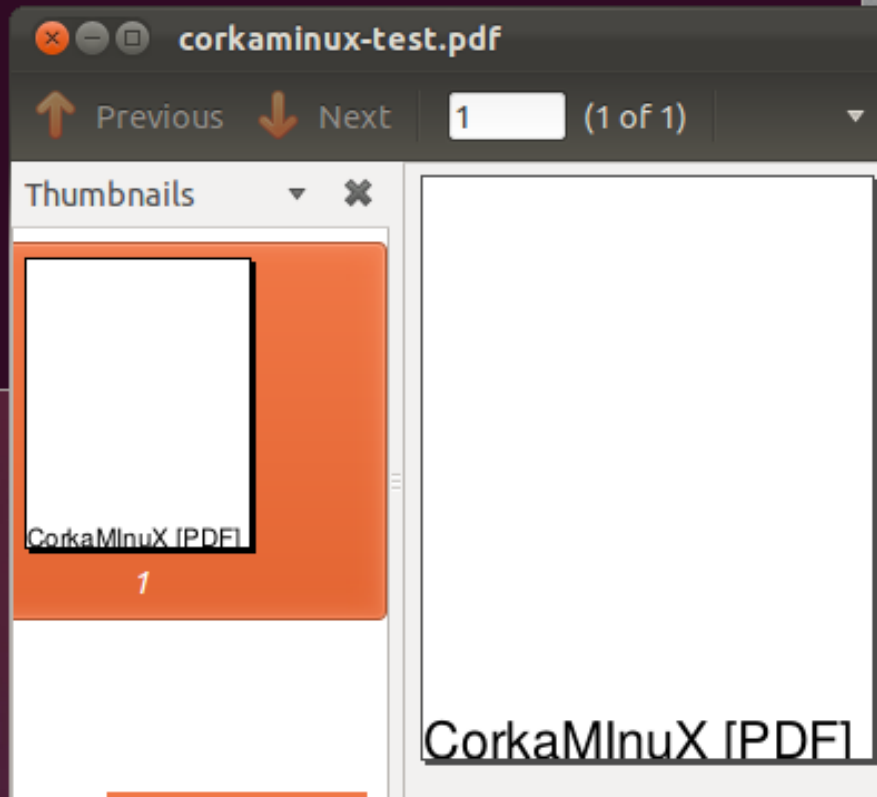
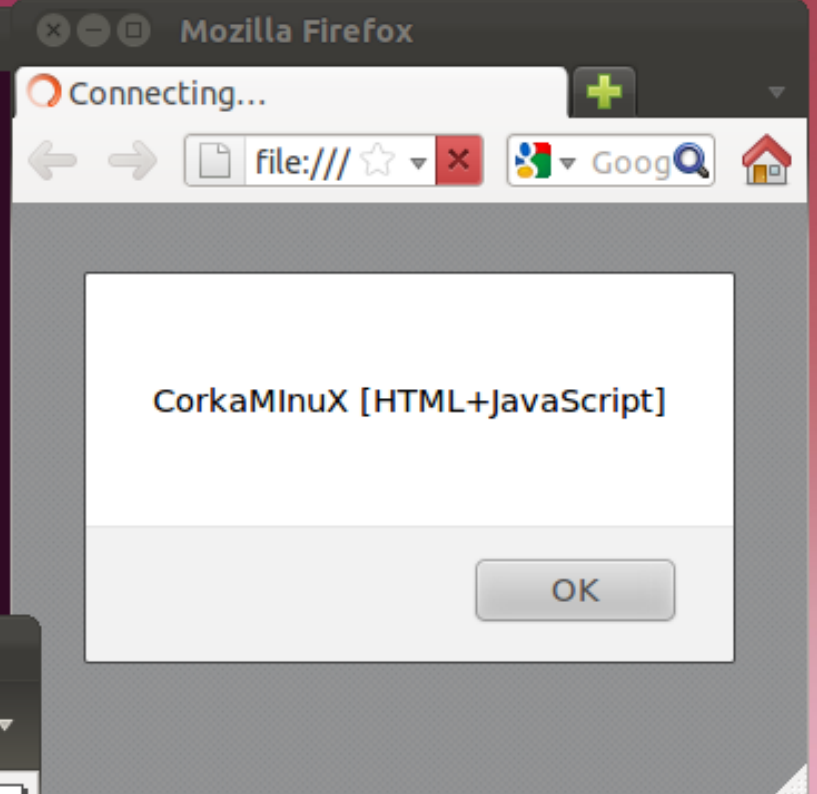


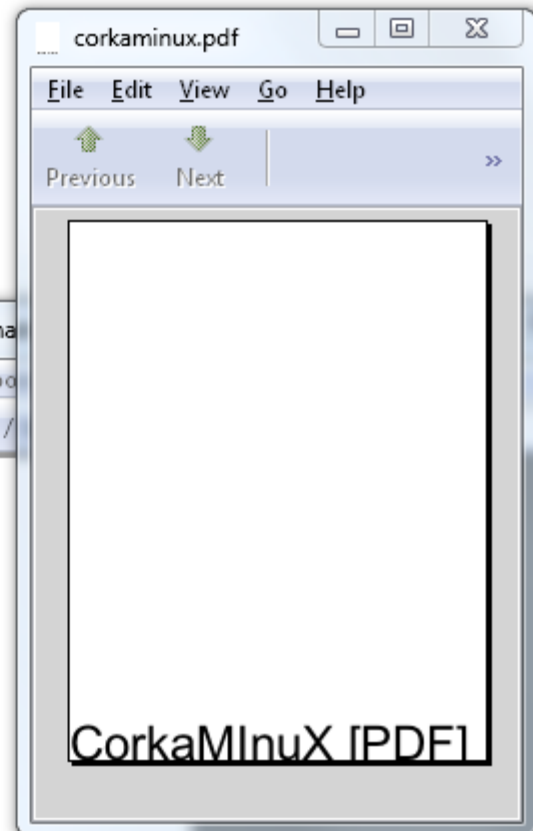
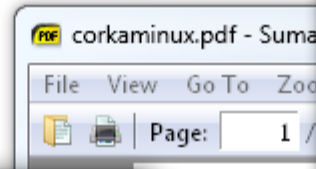
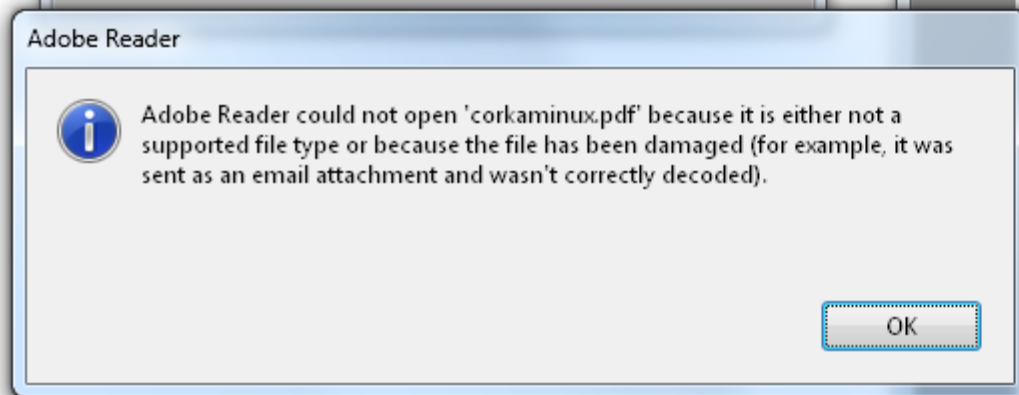
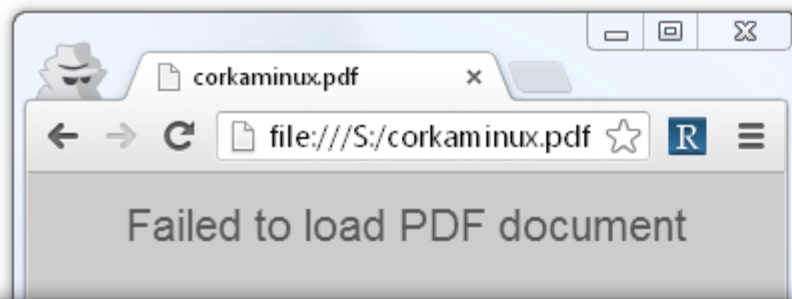
10.1.4



10.1.5

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





corkamosx.pdf (1 page)

```
$ nasm -o corkamosx mosx.asm
$ java -jar corkamosx
CorkaM-OsX [Java]
$ chmod +x corkamosx
$ ./corkamosx
CorkaM-OsX
$ cp corkamosx corkamosx.html
$ open corkamosx.html
$ cp corkamosx corkamosx.pdf
$ open corkamosx.pdf
$
```

JavaScript
CorkaM-OsX [HTML+JavaScript]

OK

CorkaM-OsX [PDF]





LOST





SHA256: 2a9c7a16cdb3c3f2285afaf61072dd5e7cc022e97f351cad6234a13e5216f389

SHA1: e27faaa006229f8e4ab97fba7019dc9f2797f84d

MD5: 88cad2b56ab67b43794a0f7a4e690fd5

File size: 1.5 KB (1530 bytes)

File name: corkamix.exe

File type: PDF

Tags: pdf

— Studio Canal Collection —



A FILM BY
JEAN-LUC GODARD

BREATHLESS

JEAN SEBERG
JEAN-PAUL BELMONDO
ORIGINAL SCREENPLAY BY **FRANÇOIS TRUFFAUT**
ARTISTIC ADVISOR **CLAUDE CHABROL**



Weaknesses

- evasion
 - filters → exfiltration
 - *same origin policy*
 - detection
 - ex: clean PE but malicious PDF/HTML/...
 - exhaust checks
 - pretend to be corrupt
- DoS

Conclusion

Conclusion

- type confusion is bad
 - succinct docs too
 - lazy softwares as well
- go beyond the specs
 - Adobe: good
- suggestions
 - more extensions checks
 - isolate downloaded files
 - enforce magic signature at offset 0

thank YOU !

Questions ?

http://

reverseengineering

.stackexchange.com

@angealbertini



ange@corkami . com

Bonus

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii	
00000000	47	49	46	38	39	61	2F	2A	0A	00	00	FF	00	2C	00	00	GIF89a/*.....,..	<-Format data
00000010	00	00	2F	2A	0A	00	00	02	00	3B	2A	2F	3D	31	3B	61	../*.....;*/=1;a	<-Format data - For...
00000020	6C	65	72	74	28	22	48	65	6C	6C	6F	20	57	6F	72	6C	lert("Hello.Worl	<-Foreign data
00000030	64	5C	6E	28	66	72	6F	6D	20	61	20	47	49	46	20	66	d\n(from.a.GIF.f	
00000040	69	6C	65	29	22	29	3B										ile)");	

gifjs.html

view-source:file:///S:/gif/gifjs.html

```

1 <html><body>
2 
3 <script src="gifjs.gif"></script>
4 </body></html>

```

gifjs.html

file:///S:/gif/gifjs.html

JavaScript Alert

Hello World
(from a GIF file)

OK

