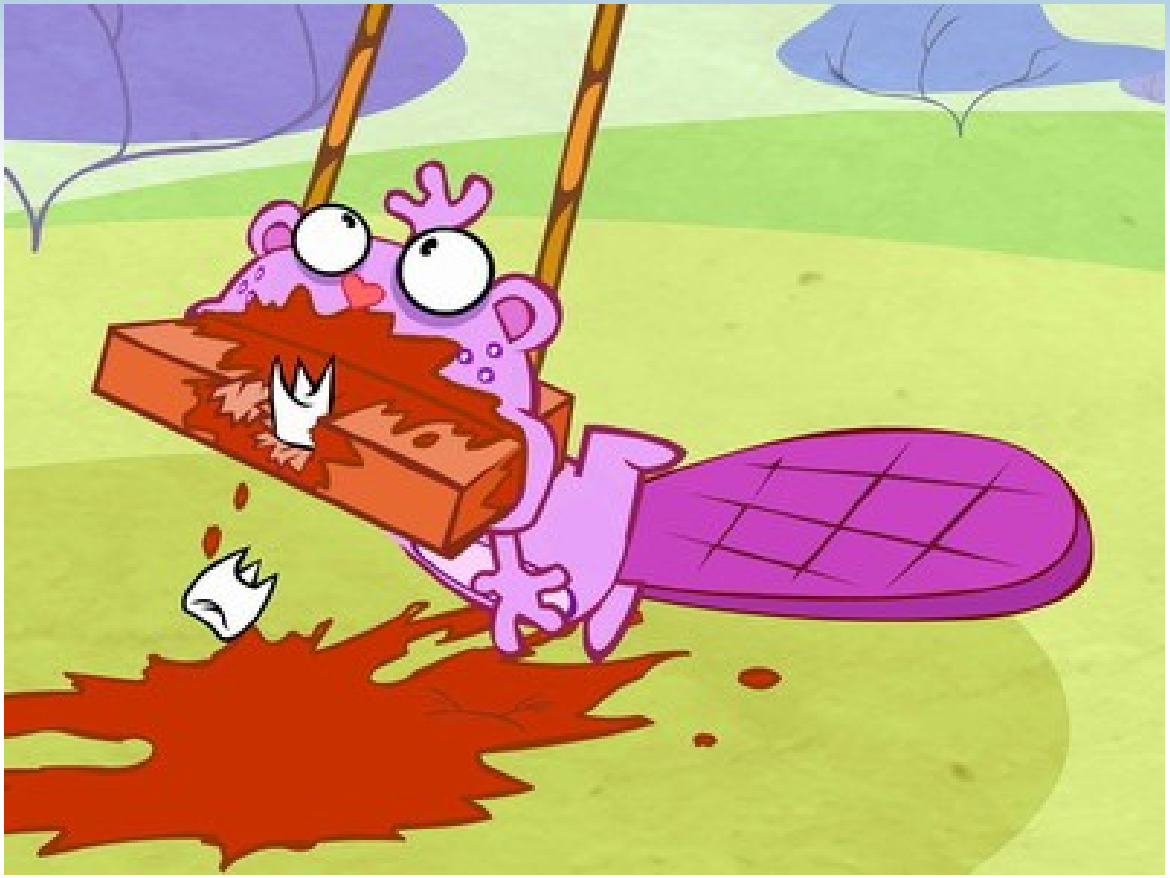
What is SWF ?

Nicolas Cannasse
http://ncannasse.fr
FFK 2009

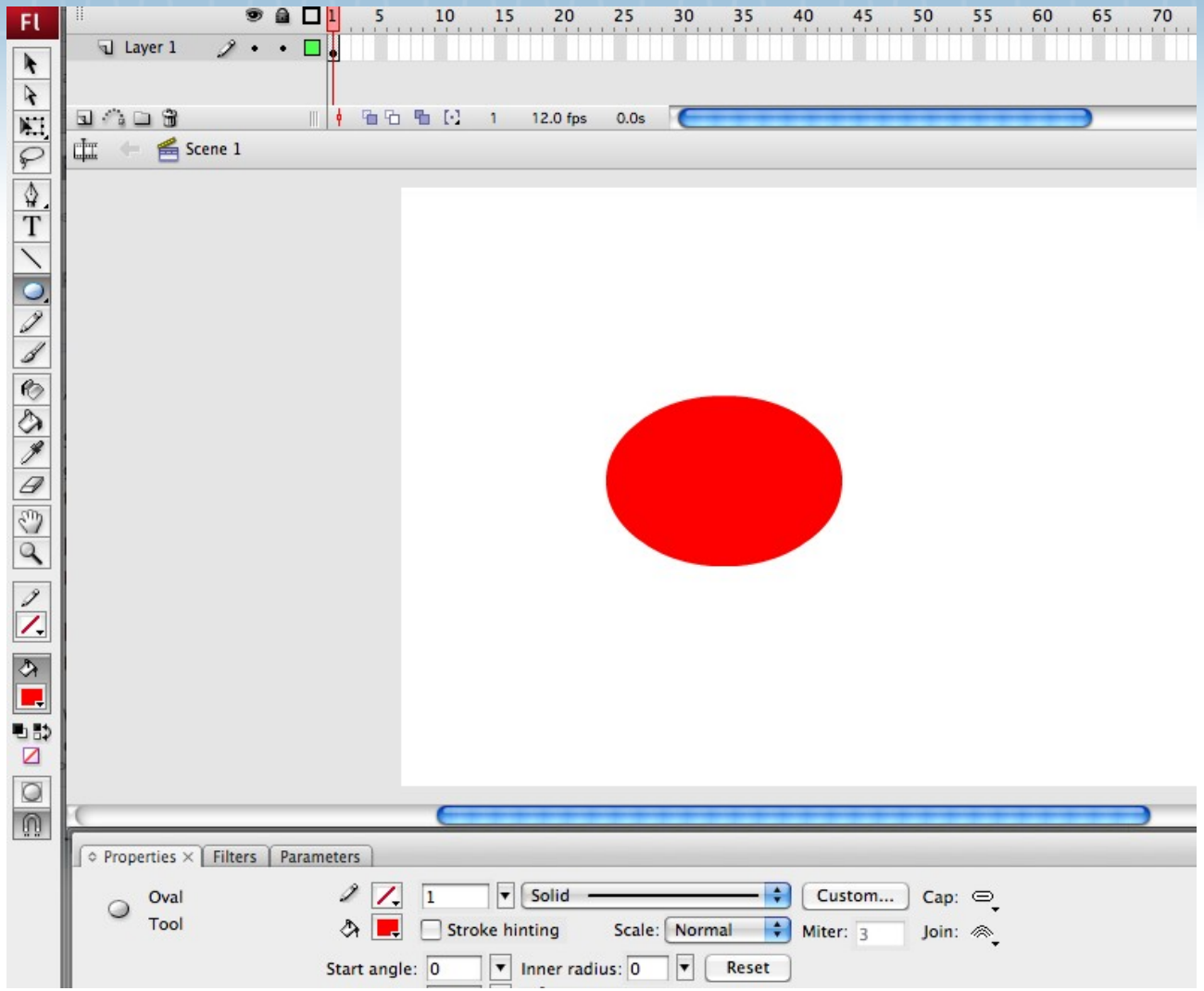
What is SWF ?



What is SWF ?


imagination
Show me your imagination instead.
imagination
imagination

What is SWF ?


Fl
Layer 1
1
5
10
15
20
25
30
35
40
45
50
55
60
65
70
1
12.0 fps
0.0s
Scene 1
Properties
Filters
Parameters
Oval
Tool
1
Solid
Custom...
Cap:
Stroke hinting
Scale:
Normal
Miter:
3
Join:
Start angle:
0
Inner radius:
0
Reset

What's inside ?

- Graphics
  - Vectorized
  - Bitmaps (jpeg, png...)
- Sound
  - Mp3, wav...
- Code
  - compiled as2 or as3 or haXe or ...
- Everything together is a **SWF FILE**

What's inside ?

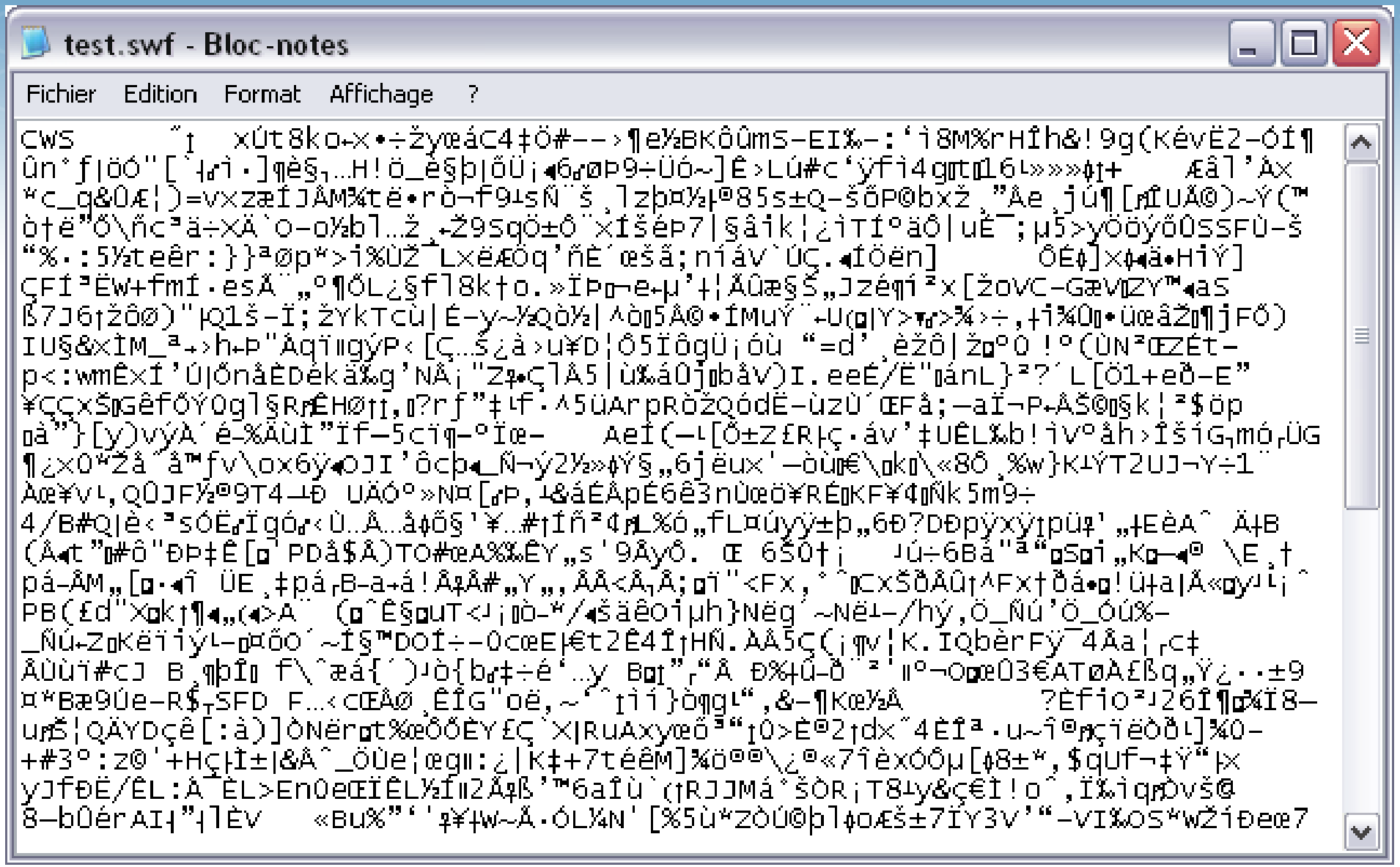
- What is a File ?
  - Array of Byte (saved on disk)
- What is a Byte ?
  - 8 bits
  - 2 x 2 x 2 x 2 x 2 x 2 x 2 = 256
  - a value between 0 and 255
  - 256 = 16 x 16 = 2 hexadecimal values
  - a value between 00 and FF (in hex)

Creating a SWF

Test.hx

```
1  // haxe -swf9 test.swf -main Test
2
3  class Test {
4
5      static function main() {
6          flash.Lib.trace("Hello World !");
7      }
8
9  }
```

Opening a SWF



Opening a SWF in Binary

.... 3188 bytes

```
43 57 53 09 98 12 00 00  78 DA 74 38 6B 6F 1B D7  CWS.▌...xÚt8ko.×
95 F7 9E 79 9C E1 43 34  87 D6 23 96 2D 9B B6 65  ▌÷▌y▌áC4▌Ö#▌-▌¶e
BD 42 4B F4 FB 6D 53 96  45 49 89 2D 3A 91 EC 38  ½BKôûmS▌EI▌-:´ì8
4D 25 72 48 CE 68 26 21  39 0A 67 28 4B E9 76 CB  M%rHÎh&!9.g(KévË
32 AD D3 CD B6 FB 6E B0  1F 83 05 F6 D3 22 5B 60  2-ÓÍ¶ûn°.▌.öÓ"[`
17 0B EC B7 5D 14 E8 A7  02 85 48 21 F6 5F E8 A7  ..ì·].è§.▌H!ö_è§
FE 05 F5 DC A1 1E 11 36  0B F8 DE 39 F7 DC F3 7E  þ.õÜ¡..6.øÞ9÷Üó~
5D CA 9B 4C FA 23 63 91  FF 66 EC 34 67 8F 74 8D  ]Ê▌Lú#c´ÿfì4g▌t▌
31 36 03 BB BB BB 0F 12  2B 09 C6 E2 6C 92 C1 D7  16.»»»»..+.Æâl´Á×
2A 63 5F 71 26 DB C6 A6  29 3D 76 D7 7A E6 CD 4A  *c_q&ÛÆ¦)=v×zæÍJ
C5 4D BE 74 EB 95 72 F2  AC 66 39 15 73 D1 A8 9A  ÅM¾të▌rò¬f9.sÑ¨▌
B8 6C 7A FE A4 BD 19 AE  38 35 73 B1 51 2D 9A F5  ¸lzþ¤½.®85s±Q-▌õ
50 A9 62 78 9E B8 94 C5  65 B8 6A FA B6 5B 0E CE  P©bx▌¸▌Åe¸jú¶[.Î
55 C3 A9 29 7E DD 28 99  F2 86 EB 94 D5 5C F1 63  UÃ©)~Ý(▌ò▌ë▌Õ\ñc
```

8 First Bytes

43 57 53 09 98 12 00 00

8 First Bytes

43 57 53 09 98 12 00 00

C W S

8 First Bytes

43 57 53 **09** 98 12 00 00

Version

8 First Bytes

43 57 53 09 **98 12 00 00**

0x00001298

= 4760 ?

Uncompressed SWF

```
46 57 53 09 97 12 00 00  70 00 0F A0 00 00 BB 80  FWS.▌...p.. ..»▌
00 1E 01 00 44 11 08 00  00 00 43 02 FF FF FF 3F  ....D.....C.ÿÿÿ?
12 5D 12 00 00 10 00 2E  00 02 A0 06 00 00 96 01  .]........ ...▌.
00 04 68 61 78 65 03 4C  6F 67 0D 48 65 6C 6C 6F  ..haxe.Log.Hello
20 77 6F 72 6C 64 20 21  08 66 69 6C 65 4E 61 6D   world !.fileNam
65 07 54 65 73 74 2E 68  78 0A 6C 69 6E 65 4E 75  e.Test.hx.lineNu
6D 62 65 72 09 63 6C 61  73 73 4E 61 6D 65 04 54  mber.className.T
65 73 74 0A 6D 65 74 68  6F 64 4E 61 6D 65 04 6D  est.methodName.m
61 69 6E 05 74 72 61 63  65 04 76 6F 69 64 06 4F  ain.trace.void.O
62 6A 65 63 74 0D 66 6C  61 73 68 2E 64 69 73 70  bject.flash.disp
6C 61 79 09 4D 6F 76 69  65 43 6C 69 70 07 63 75  lay.MovieClip.cu
72 72 65 6E 74 0B 66 6C  61 73 68 2E 75 74 69 6C  rrent.flash.util
73 08 67 65 74 54 69 6D  65 72 03 69 6E 74 06 53  s.getTimer.int.S
74 72 69 6E 67 01 2E 21  68 74 74 70 3A 2F 2F 61  tring..!http://a
```

SWF Structure

- Documented in « SWF File Format Spec. »
- Header :
  - `CWS` / `FWS`
  - Player Version
  - File Size
  - Width & Height
  - Frames Per Sec
  - Total Number of Frames
- List of « Tags »

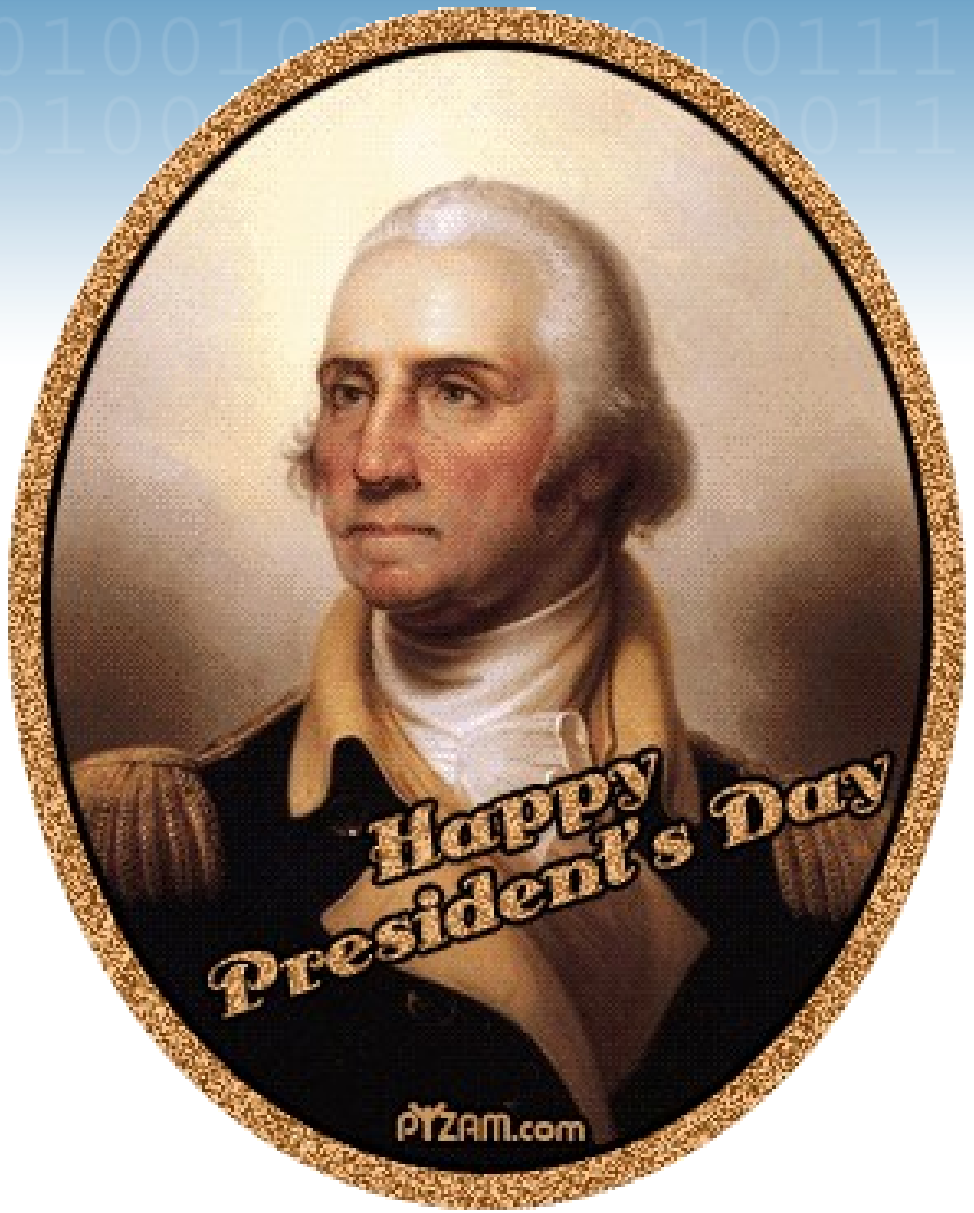
SWF Tag

- ID + Custom Data

- 2 bytes (16 bits) header
  - 10 bits tag ID
  - 6 bits data length (0-63)
- Large tags = 63
  - 32 bits data length

- Custom tag data

Graphics



SWF Graphics Tags

- Bitmap
- Shape
- MovieClip
- MovieClip Timeline :
  - 16-bits unique ID
  - Put #45 at Depth 52
  - Move #58 to (7.1 , -2.3)
  - Remove #3
  - Show Frame

Example

Good-old Flash 7 gfx.swf

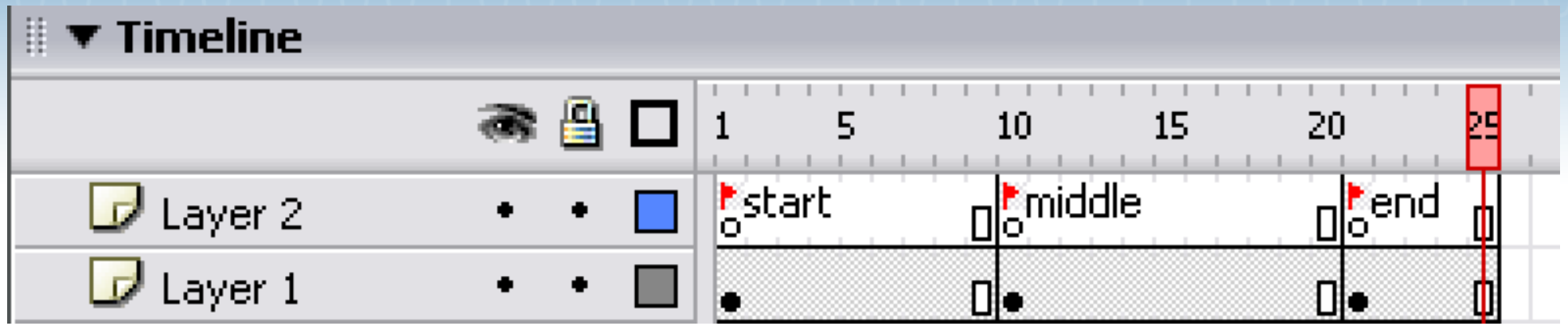
Listing Tags

```haxe
// haxe -lib format -x DisplayTags

class DisplayTags {

    static function main() {
        var f = neko.io.File.read("test.swf",true);
        var swf = new format.swf.Reader(f).read();
        neko.Lib.println( "Header : "+swf.header );
        for( tag in swf.tags )
            neko.Lib.println( format.swf.Tools.dumpTag(tag,16) );
    }

}
```

GFX Dump

```
Header :
  width=550,height=400,cmp=true,
  ver=7,fps=1.0,frames=4

Tags :
  TBackgroundColor(FFFFFF)
  TShape(id:1,data:722D2CD2987498900100FF000...)
  TPlaceObject2(cid:1,depth:1)
  TShowFrame()
  TShape(id:5,data:5C147D1003F5A610...)
  TPlaceObject2(cid:5,depth:2,x:2900,y:2700)
  TShowFrame()
  TPlaceObject2(move:true,depth:2,x:7980,y:5957)
  TShowFrame()
  TRemoveObject2(depth:1)
  TShowFrame()
```

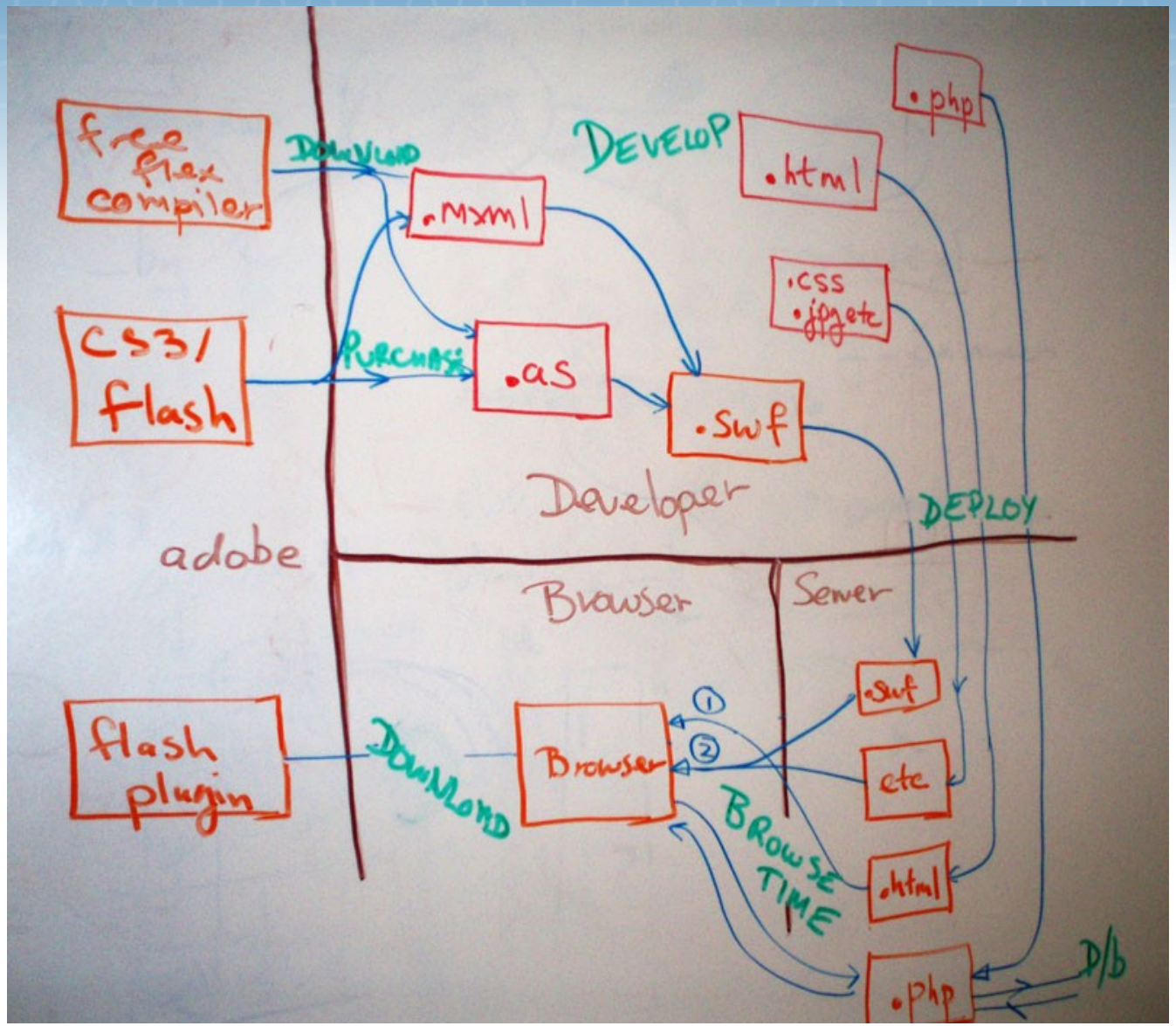
MovieClip Timeline



- 3 keyframes
- start : gotoAndStop("end")
- end : gotoAndStop("middle")

Hacking the Timeline

Code


free flex compiler
DOWNLOAD
.mxml
DEVELOP
.html
.php
.css
.jpg etc
CS3/ flash
PURCHASE
.as
.swf
Developer
DEPLOY
adobe
Browser
Server
flash plugin
DOWNLOAD
Browser
.swf
etc
.html
.php
BROWSE TIME
D/b

SWF Code Tags

- What is « Bytecode » ?
  - everything you need to run the program
  - produced by the compiler
  - also called « assembler »
  - either Flash6-8 (AS1+AS2) or Flash9 (AS3)
  - Array of OpCode
- What is an « Opcode » ?
  - a simple operation
  - numerical (add, sub, ...)
  - logical (call, jump-if , ...)

Numerical Operation (AS3)

```
var x : int = 5;

var y : int = x + 3;

---------
  smallint 5
  setreg 1              r1 := 5
  reg 1
  smallint 3
  add                   s0 := add r1 3
  toint                 s0 := int s0
  setreg 2              r2 := s0
```

Numerical Operation (haXe)

```
var x = 5;

var y = x + 3;

---------
  smallint 5
  setreg 1                r1 := 5
  reg 1
  smallint 3
  iadd                    s0 := iadd r1 3
  setreg 2                r2 := s0
```

While Loop

```
var x = 50;
while( x > 0 )
   x--;
```

```
--------
  0 smallint 50
  1 toint
  2 setreg 1                    r1 := 50
  3 jump +3                     go 6
  4 label
  5 decrireg 1                  r1 := r1 - 1
  6 reg 1
  7 smallint 0
  8 jump-gt -4                  if( r1 > 0 ) go 4
```

test.swf

Test.hx

```
1  // haxe -swf9 test.swf -main Test
2
3  class Test {
4
5      static function main() {
6          flash.Lib.trace("Hello World !");
7      }
8
9  }
```

Code Dump

```
Header :
  width=400,height=300,cmp=false,ver=9,fps=7680,frames=1

Tags :
  TSandBox(8)
  TBackgroundColor(FFFFFF)
  TActionScript3(context:null,data:[4601 bytes])
  TSymbolClass([{ className => flash.Boot, cid => 0 }])
  TShowFrame()
```

Code Dump

```
class Test extends Object {
   function construct() : void
   static final function main() : void
}

function construct :
  0 this
  1 scope
  2 retvoid

function main :
  0 getlex flash.Lib
  1 string "Hello world !"
  2 callpropvoid trace 1
  3 retvoid
```

Code Security

- Human-readable :
  - Classes
  - Fields
  - Method names
  - Strings
- They can't be « protected » !
- ... but they can be renamed (Obfuscation)

Code Speed

- Fast :
  - numerical operations (except div)
  - field access
- Slow :
  - Math functions
  - static function calls
  - array access
  - cast
  - « new »

Code Speed

The star system experiment

What is SWF ?

- « just » a technology
- every technology has its limits
- learn the technology to bypass these limits
- content matters the most
- it's up to you !

What is SWF ?

Thank you !

http://ncannasse.fr