

# Polyphemos

## Ease Virtual Machine Level Tooling



**Pierre Misse-Chanabier**  
**Theo Rogliano**



# Who Does Not Love Tools ?

## Tooling Levels



Pharo Image

Language Level

VM Level

Pharo VM

# Who Does Not Love Tools ?

## Tools at the Language Level

Pharo Image

Language Level

VM Level

Pharo VM

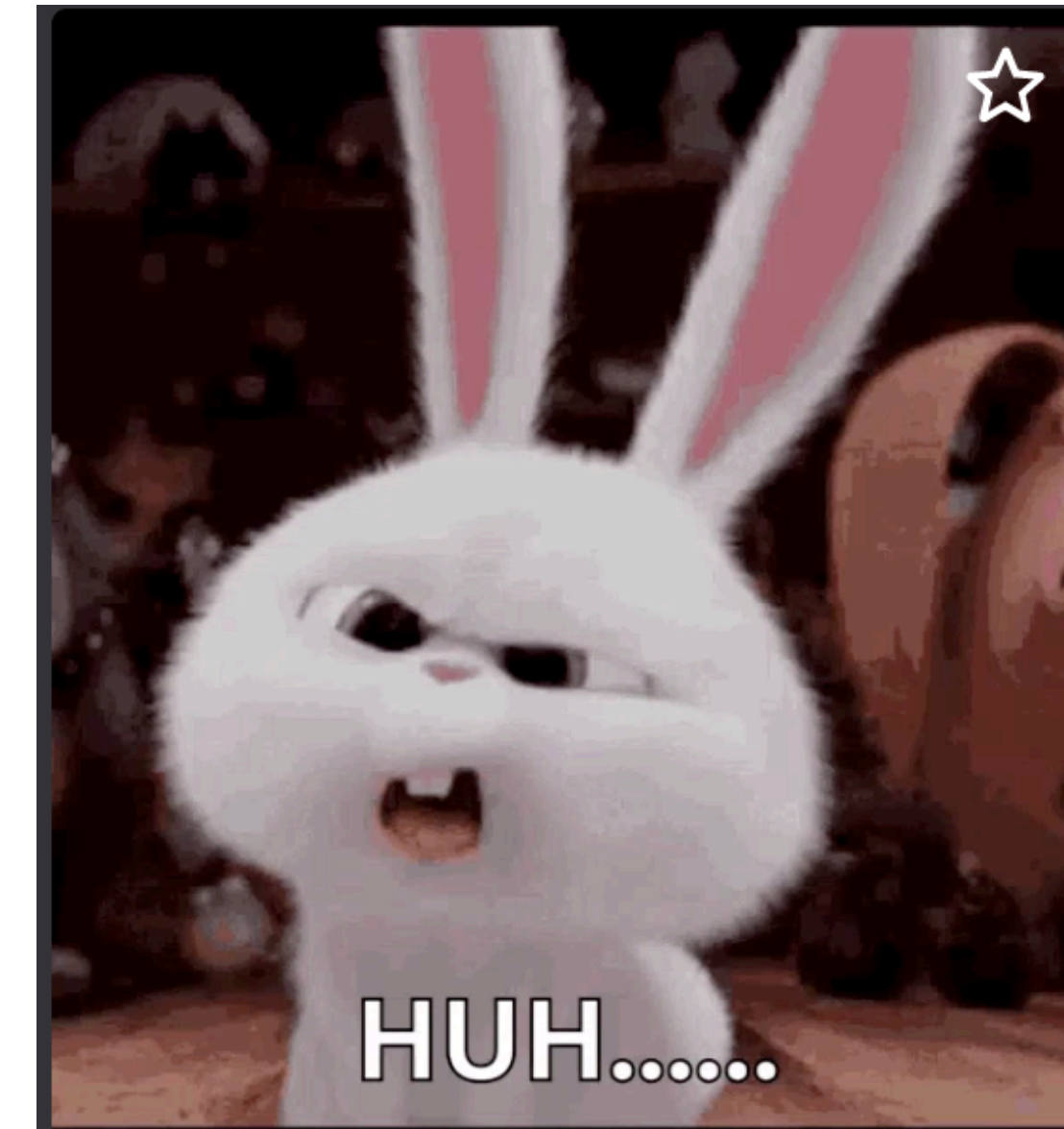
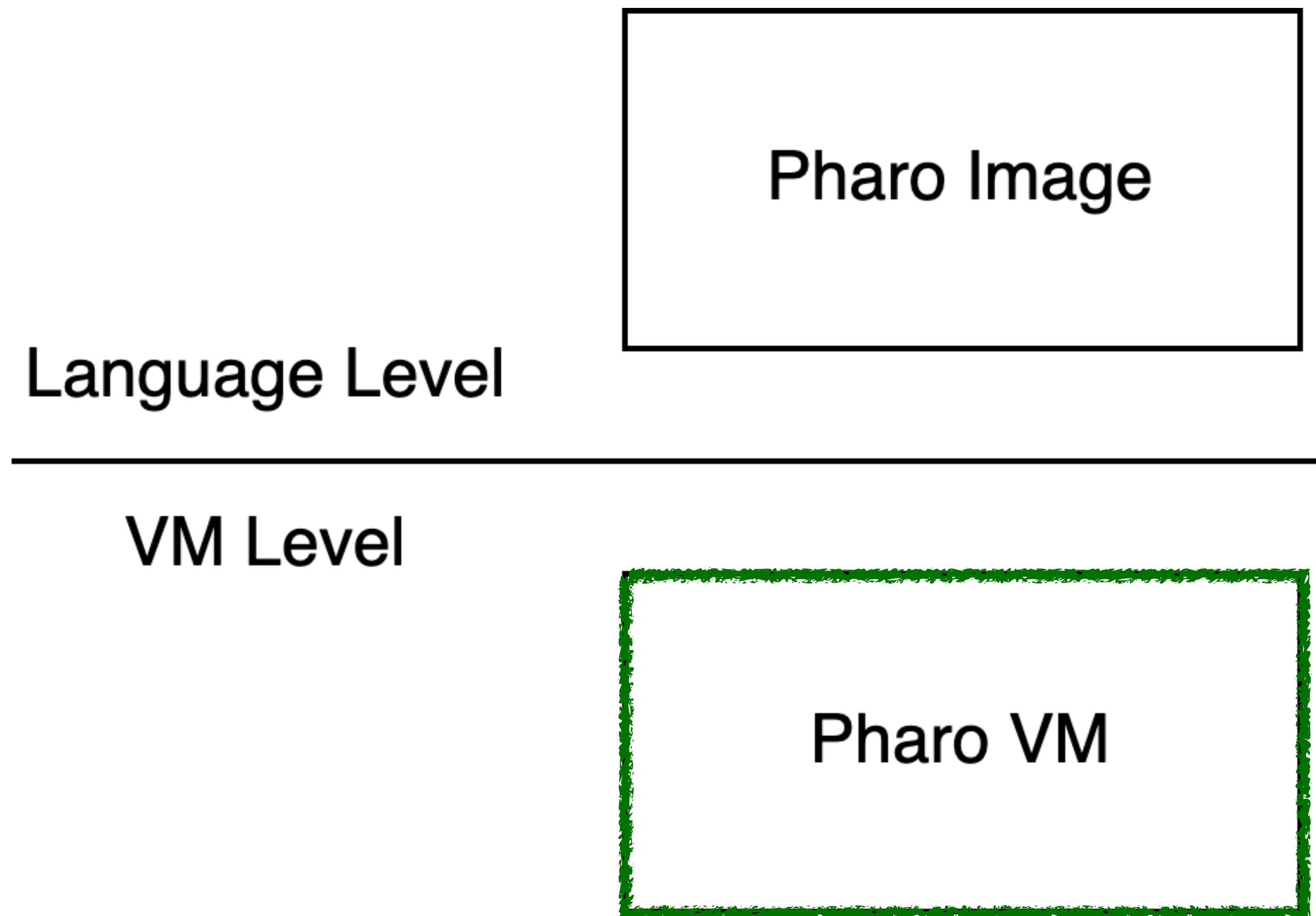
NewTools, Moose, Roassal,  
Calypso, SUnit, Iceberg, Refactoring, Epicea

... ..



# Who Does Not Love Tools ?

## Tools at the VM Level



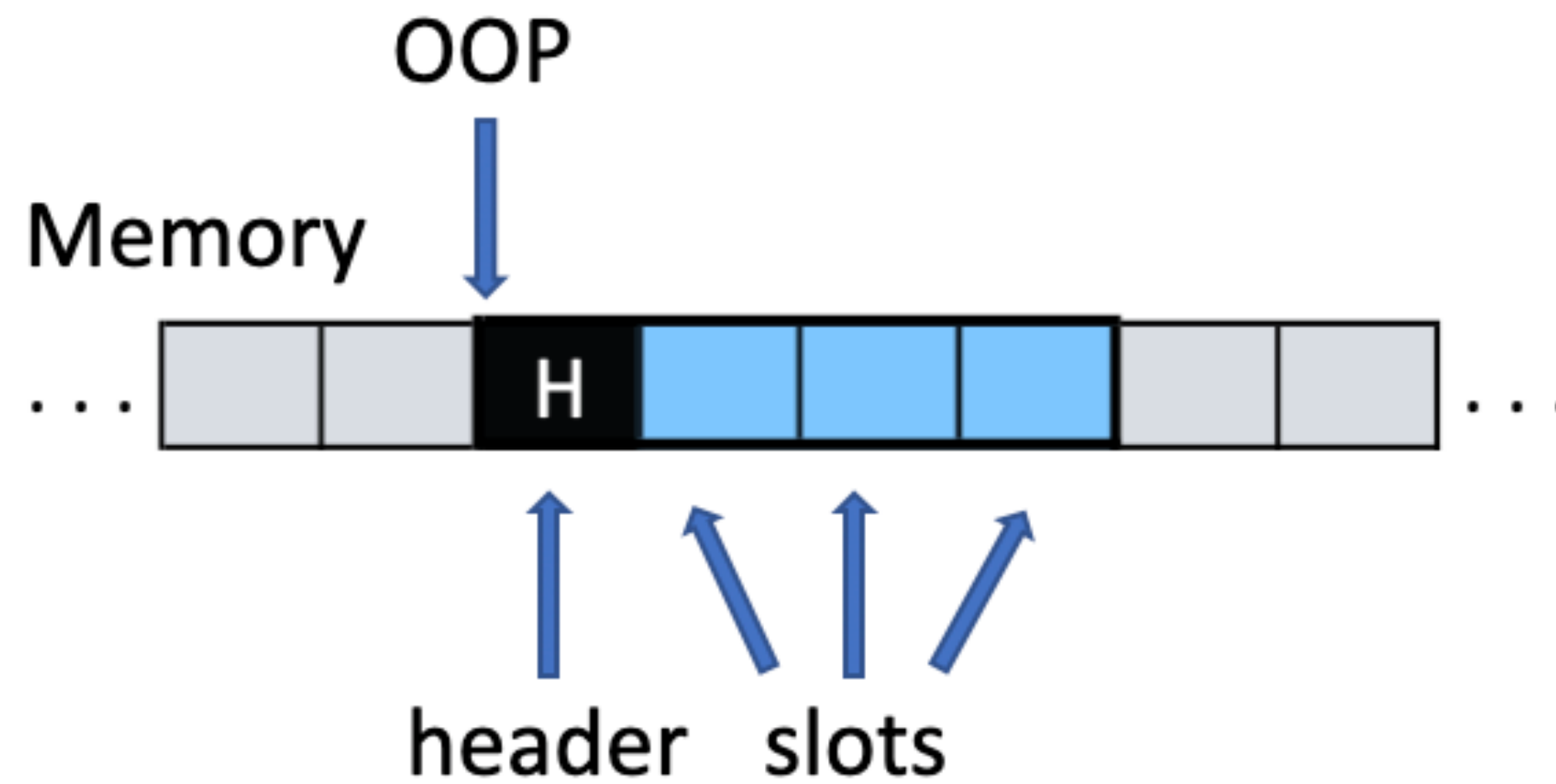
Bootstrap, VM machine code debugger  
Others ?

Not many things a Pharo developer cares about !



# Let's Code VM Level Tools !

## What's an Ordinary Object Pointer (OOP)



# Who Does Not Love Tools ?

## Why Should we Care About VM Level Tools ?

```
Form >> #scaledByDisplayScaleFactor
self halt.
^ self scaledToSize: self extent * self currentWorld displayScaleFactor.
```

# Who Does Not Love Tools ?

Don't Close the Image !



**Form** >> #scaledByDisplayScaleFactor

self halt.

^ self scaledToSize: self extent \* self currentWorld displayScaleFactor.



# Who Does Not Love Tools ?

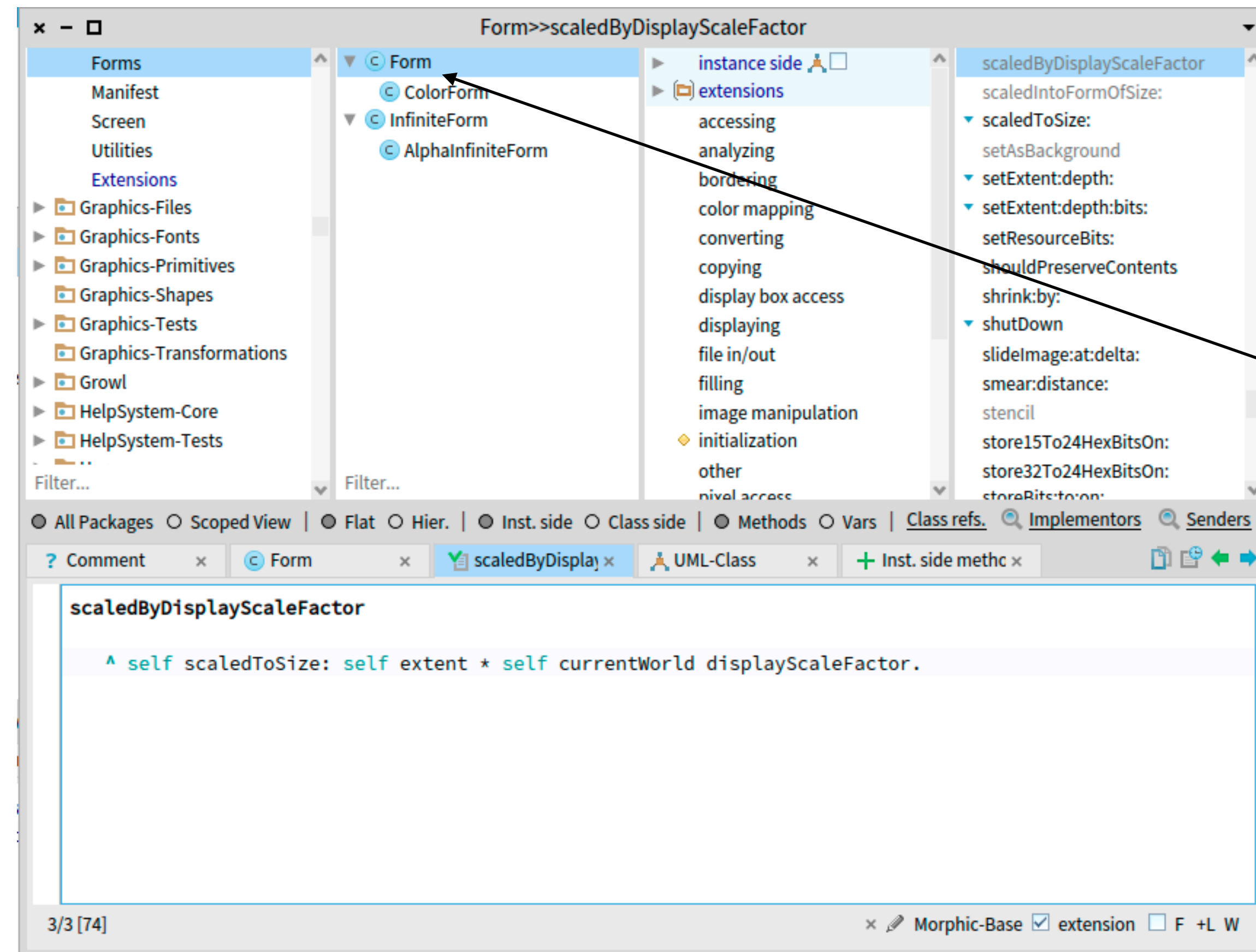
Too Late !

```
Halt
SmallInteger(Object)>>haltOnce
Form>>scaledByDisplayScaleFactor
ThemeIcons>>iconNamed:
MorphicRootRenderer(Object)>>iconNamed:
MorphicRootRenderer(OSWorldRenderer)>>setAttributesDefault
MorphicRootRenderer class(OSWorldRenderer class)>>forWorld:
[ :arg5 | tmp2 := arg5 forWorld: arg1 ] in AbstractWorldRenderere
FullBlockClosure(BlockClosure)>>cull:
[ :arg4 | (arg1 value: arg4) ifTrue: [ ^ arg2 cull: arg4 ] ] in
  arg2 cull...etc...
OrderedCollection>>do:
OrderedCollection(Collection)>>detect:ifFound:ifNone:
OrderedCollection(Collection)>>detect:ifFound:
AbstractWorldRenderer class>>detectCorrectOneForWorld:
```



# Let's Code VM Level Tools !

Let's Find the Class Form ...



Found it !

# Let's Code VM Level Tools !

Let's Find The Class Form ... But at the VM Level ...

a ByteArray [13107200 items]

| Items   | Raw   | Breakpoints | Meta |
|---------|-------|-------------|------|
| Index   | Value |             |      |
| 4676739 | 231   |             |      |
| 4676740 | 14    |             |      |
| 4676741 | 0     |             |      |
| 4676742 | 0     |             |      |
| 4676743 | 0     |             |      |
| 4676744 | 0     |             |      |
| 4676745 | 32    |             |      |
| 4676746 | 55    |             |      |
| 4676747 | 231   |             |      |
| 4676748 | 14    |             |      |
| 4676749 | 0     |             |      |
| 4676750 | 0     |             |      |
| 4676751 | 0     |             |      |
| 4676752 | 0     |             |      |
| 4676753 | 32    |             |      |
| 4676754 | 55    |             |      |
| 4676755 | 231   |             |      |
| 4676756 | 14    |             |      |
| 4676757 | 0     |             |      |
| 4676758 | 0     |             |      |
| 4676759 | 0     |             |      |
| 4676760 | 0     |             |      |

13 107 200 items

# Let's Code VM Level Tools !

## With the Help of the Simulator

```
findClassName: aClassName
| classNameIndex classNameOop className |
memory classTableEntriesDo: [ :aClassOop |
    aClassOop = memory nilOOP
    "ifTrue: [ not a class, nothing to do ]"
    ifFalse: [
        classNameIndex := memory classNameIndexForOop: aClassOop.
        classNameOop := memory fetchPointer: classNameIndex ofObject: aClassOop.
        className := memory convertStringOopToStringObject: classNameOop.
        className = aClassName ifTrue: [ ^ aClassOop ]]].
^ memory nilOOP
```

memory findClassName: Form >>> 406749864

# Let's Code VM Level Tools !

## Knowledge Gaps

```
findClassName: aClassName
| classNameIndex classNameOop className |
memory classTableEntriesDo: [ :aClassOop |
  aClassOop = memory nilOOP
  "ifTrue: [ not a class, nothing to do ]"
  ifFalse: [
    classNameIndex := memory classNameIndexForOop: aClassOop.
    classNameOop := memory fetchPointer: classNameIndex ofObject: aClassOop.
    className := memory convertStringOopToStringObject: classNameOop.
    className = aClassName ifTrue: [ ^ aClassOop ]].
^ memory nilOOP
```

**VM level oop** (points to `classNameOop`)

**Oop** (points to `aClassOop`)

**Low level style** (points to `classNameIndex`)

**Common API** (points to `className`)

# Let's Code VM Level Tools !

## Knowledge gaps recaps

### Issues

- Ordinary Object Pointers (OOP)
- Common API
- VM level information



# Polyphemus

## Introducing LLOOPs

### Language level OOPs

#### Issues

- Ordinary Object Pointers (OOP)
- Common API
- VM level information

#### Solutions

- Objects
- Specialized API & Polymorphism
- VM and Language level information

# Polyphemus

## Tooling the OOPs Using LLOOPs

- Object specific behavior
  - Inspectors
  - Memory visualisation
  - Naming entities
- 
- Depends on your imagination !

# Polyphemus

## Object Specific Behavior

- aClass subclasses
- aClassTablePage indexInClassTable
- anIndexableObject numberOfSlots

# Polyphemus

## Inspectors

LLOOP

Pharo Object

|                      |  |
|----------------------|--|
| self                 | Form   |
| superclass           | DisplayMedium  |
| { } methodDict       | a MethodDictionary [206 items] (size 206)                    |
| Σ format             | 65541  |
| layout               | a FixedLayout  |
| organization         | a ClassOrganization  |
| commentSourcePointer | nil  |
| { } subclasses       | an Array [6 items] (ColorForm Cursor DisplayScreen GlyphForm |
| name                 | Form   |
| { } classPool        | a Dictionary [1 item] (#FloodFillTolerance->nil )            |
| sharedPools          | nil  |
| { } environment      | a SystemDictionary [10453 items]                             |
| category             | Graphics-Display Objects-Forms                               |

| Key          | Value   |
|--------------|---|
| address      | 406749864   |
| printString  | Form  |
| header       | 10110000000000000111001100100000000100000000000011100110001 |
| class        | Form class  |
| oopClassTag  | 1841  |
| format       | Non Indexable (1)   |
| hash         | 1842  |
| pinned       | false   |
| space        | Old Space   |
| immutable    | false   |
| numSlots     | 11  |
| superclass   | DisplayMedium   |
| methodDict   | Instance of MethodDictionary                                |
| format       | 65541   |
| layout       | Instance of FixedLayout                                     |
| organization | Instance of ClassOrganization                               |
| subclasses   | Instance of Array   |
| name         | Form  |
| classPool    | Instance of Dictionary                                      |
| sharedPools  | nilObject   |
| environment  | Instance of SystemDictionary                                |
| category     | Graphics-Display Objects-Forms                              |

# Polyphemus

## Inspectors #2

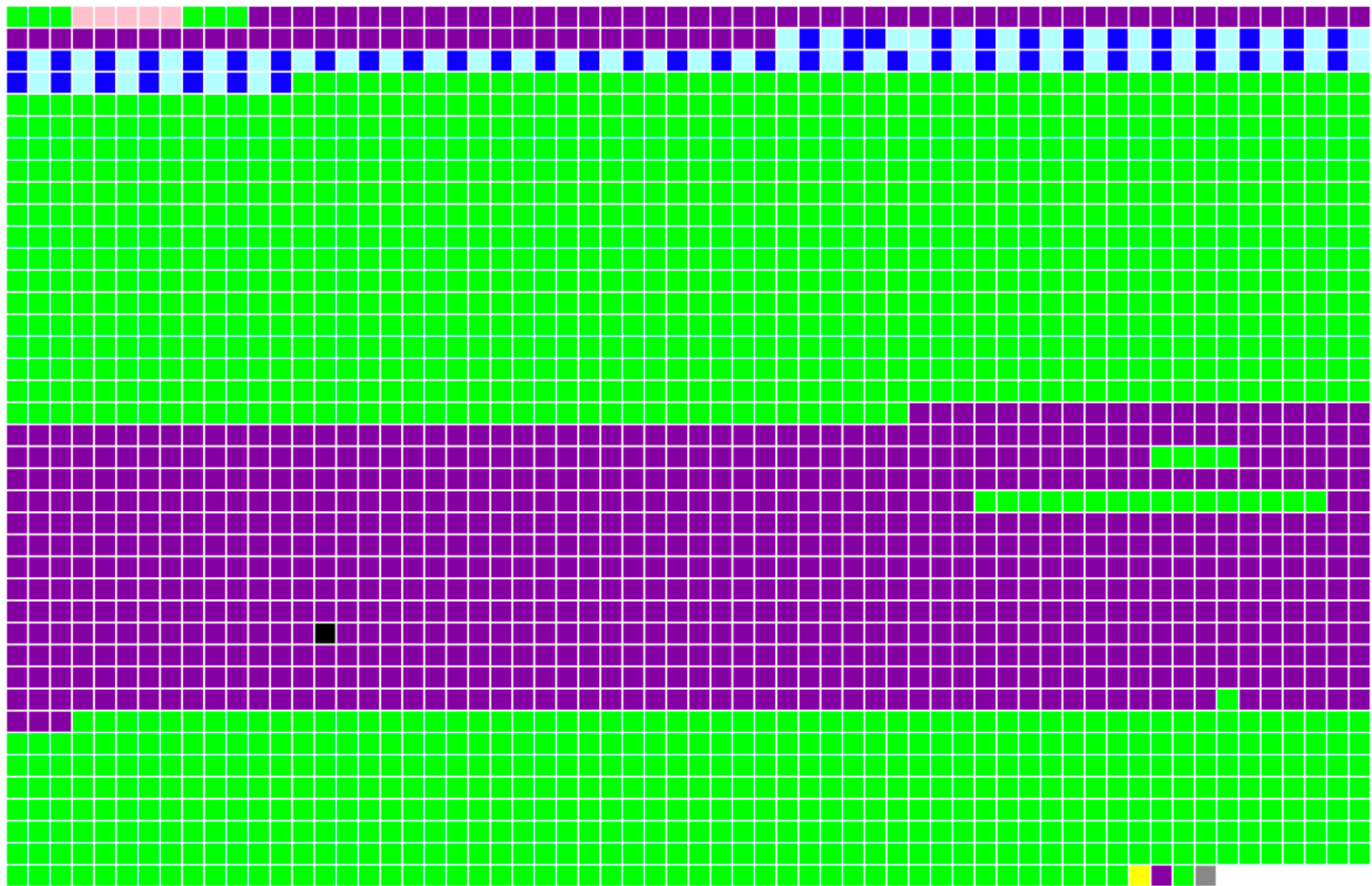
### Compiled Method

|             |   |
|-------------|---|
| address     | 8685808   |
| printString | PCMessage >> #arguments   |
| header      | 101000000000000000000000000000000111110000000000000010000011011 |
| class       | PCCompiledMethod  |
| oopClassTag | 1051  |
| format      | Compiled method (31)  |
| hash        | 0   |
| pinned      | false   |
| space       | Old Space   |
| immutable   | false   |
| selector    | arguments   |
| methodClass | PCMessage   |
| numLiterals | 2   |
| literal 1   | arguments   |
| literal 2   | Instance of PCAssociation                                       |



# Polyphemus

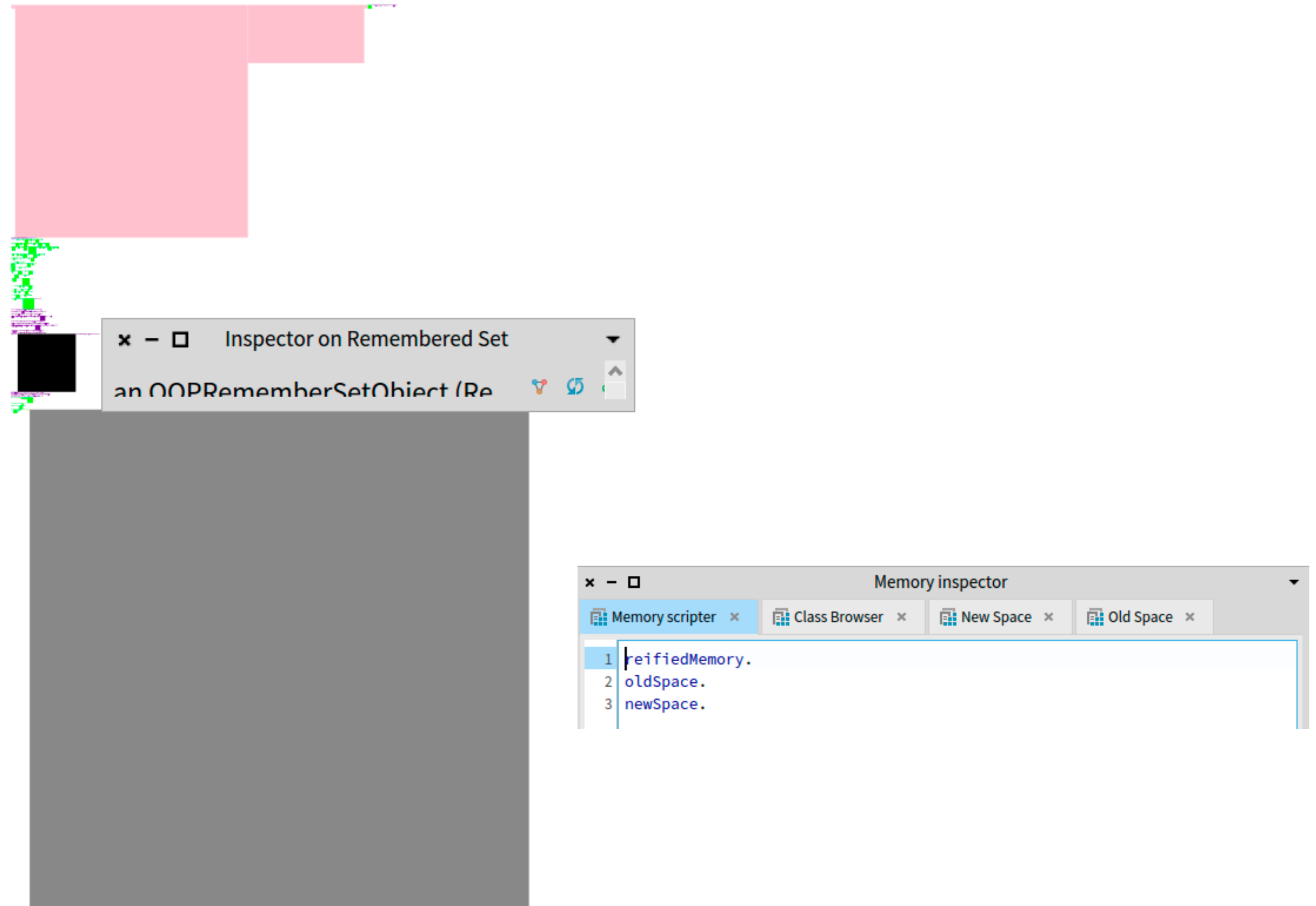
## Memory visualisation



- 1 pinned object
- 895 compiled method
- 51 class
- 5 special object
- 1 context
- 1 free chunk
- 1468 regular object
- 51 metaclass

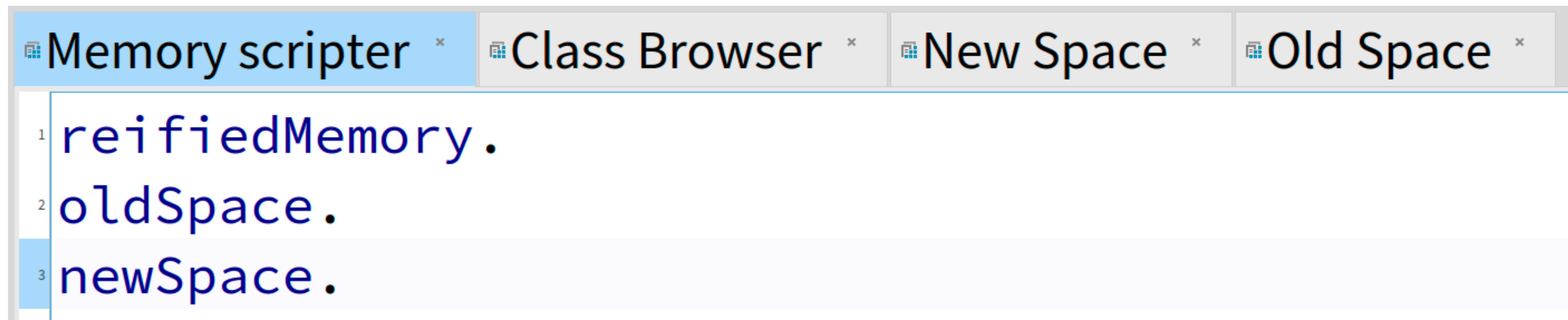
# Polyphemus

## What's That ?



# Polyphemus

## Scripter

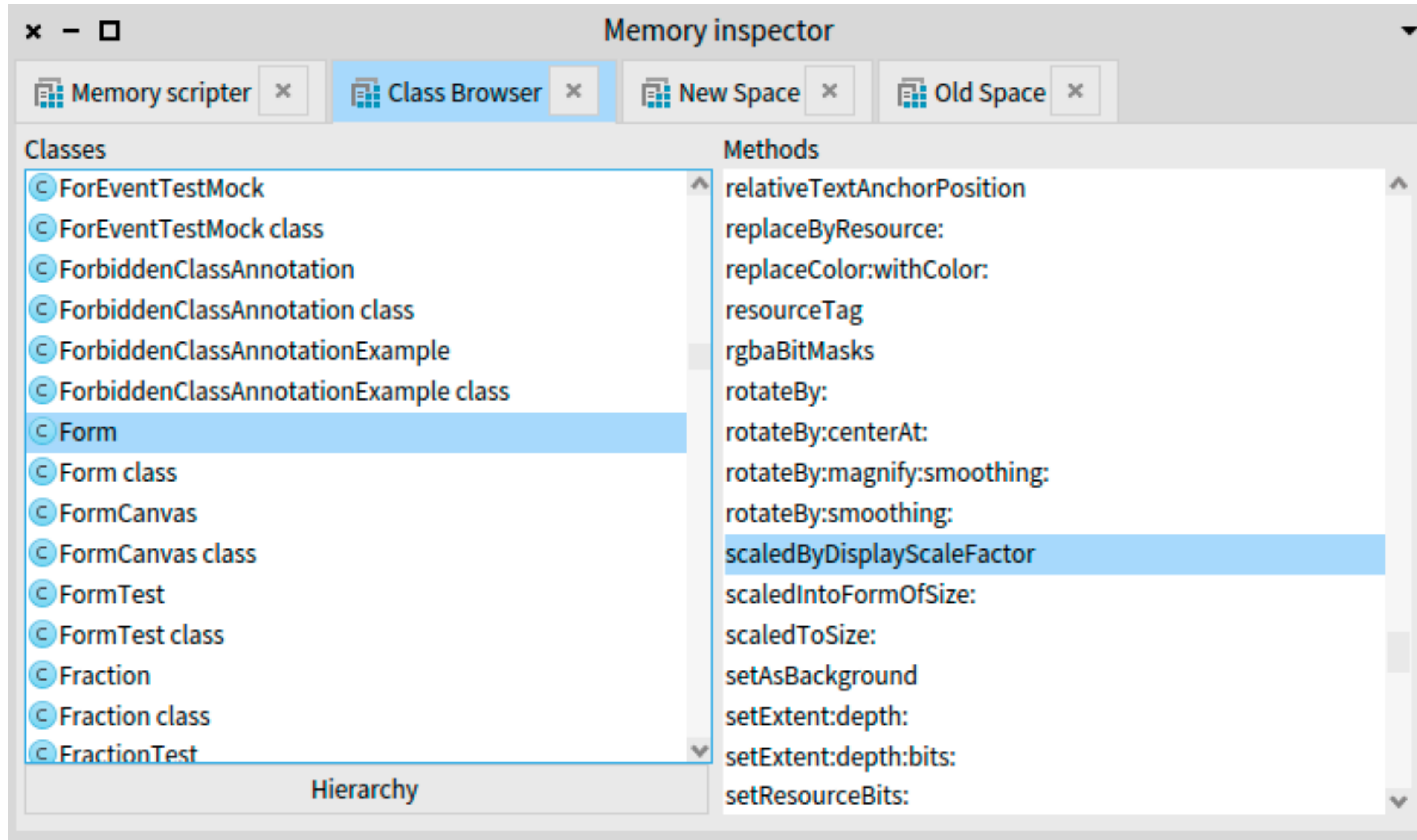


The screenshot shows the Polyphemus Scripter interface. At the top, there is a tab bar with four tabs: "Memory scripter" (active, highlighted in blue), "Class Browser", "New Space", and "Old Space". Below the tabs is a code editor with three lines of JavaScript code:

```
1 reifiedMemory.  
2 oldSpace.  
3 newSpace.
```

# Polyphemus

## Memory Visualisation #2



# Real World Bug Fix #1

Remember This ?



**Form** >> #scaledByDisplayScaleFactor

self halt.

^ self scaledToSize: self extent \* self currentWorld displayScaleFactor.





# Real World Bug Fix #1

## A Meta-Error Fix

Inspector on Form >> #scaledByDisplayScaleFactor

an OOPCompiledMethod (Form ...)

Oop Raw Breakpoints Meta

| Key         | Value                               |
|-------------|-------------------------------------|
| address     | Form >> #scaledByDisplayScaleFactor |
| header      | 10100001000001100011011111010001100 |
| class       | CompiledMethod                      |
| oopClassTag | 3101                                |
| format      | Compiled method (24)                |
| hash        | 1074045                             |
| pinned      | false                               |
| space       | Old Space                           |
| immutable   | false                               |
| selector    | scaledByDisplayScaleFactor          |
| methodClass | Form                                |
| numLiterals | 7                                   |
| literal 1   | haltOnce                            |
| literal 2   | extent                              |
| literal 3   | currentWorld                        |
| literal 4   | displayScaleFactor                  |
| literal 5   | scaledToSize:                       |
| literal 6   | Instance of AdditionalMethodState   |
| literal 7   | Instance of GlobalVariable          |

```
1 self allBytecodes
2 "#(81 128 216 76 76 129 76 130 131 104 148 92 36 159 7
  253)"
```

Inspector on Form >> #scaledByDisplayScaleFactor

an OOPCompiledMethod (Form ...)

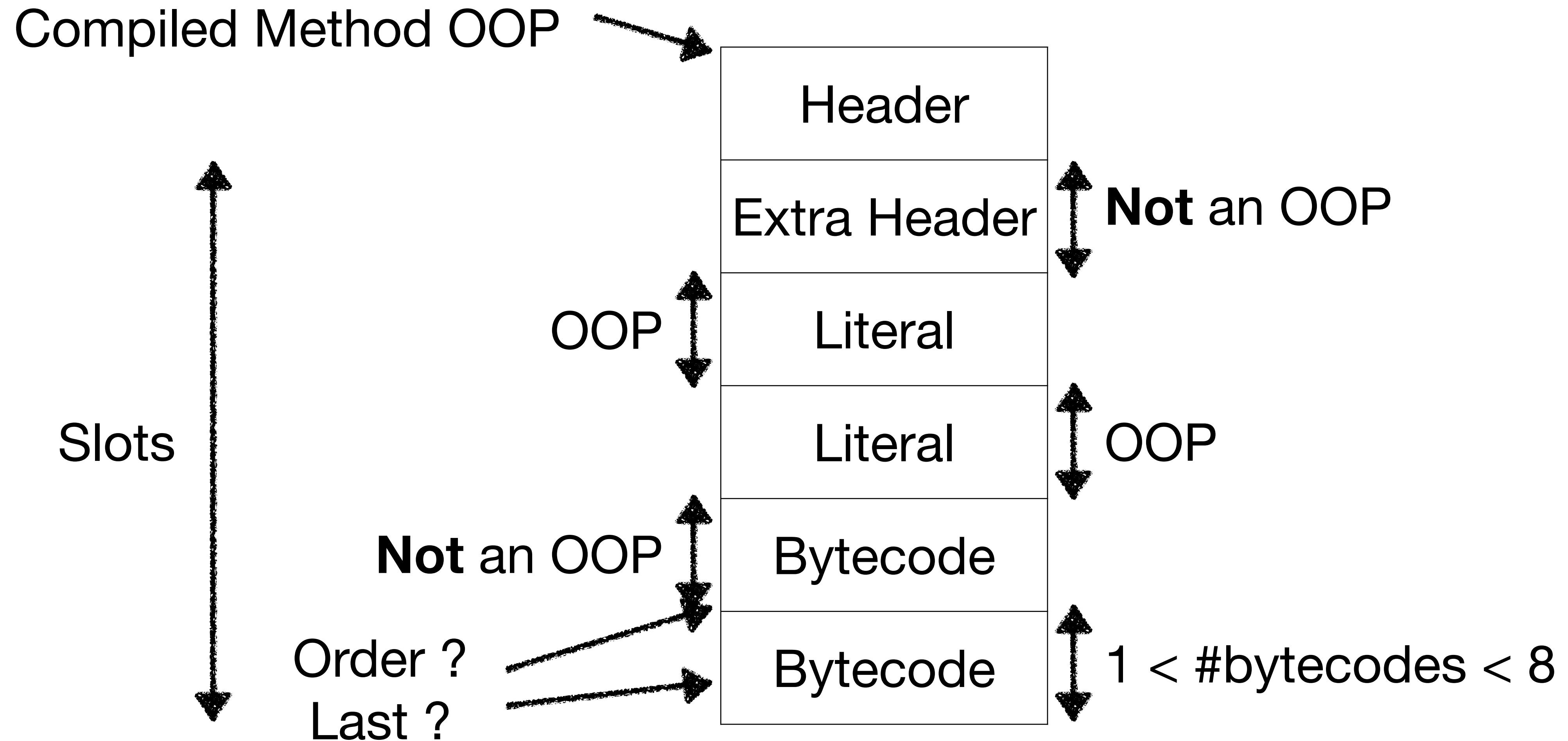
Oop Raw Breakpoints Meta

| Key         | Value                                 |
|-------------|---------------------------------------|
| address     | Form >> #scaledByDisplayScaleFactor   |
| header      | 1001000000101100011101111011000110110 |
| class       | CompiledMethod                        |
| oopClassTag | 3101                                  |
| format      | Compiled method (27)                  |
| hash        | 182139                                |
| pinned      | false                                 |
| space       | Old Space                             |
| immutable   | false                                 |
| selector    | scaledByDisplayScaleFactor            |
| methodClass | Form                                  |
| numLiterals | 6                                     |
| literal 1   | extent                                |
| literal 2   | currentWorld                          |
| literal 3   | displayScaleFactor                    |
| literal 4   | scaledToSize:                         |
| literal 5   | scaledByDisplayScaleFactor            |
| literal 6   | Instance of GlobalVariable            |

```
1 self allBytecodes
2 "#(76 76 128 76 129 130 104 147 92 16 152 150 252)"
3
```

# Real World Bug Fix #1

## A Meta-Error Fix Analysis



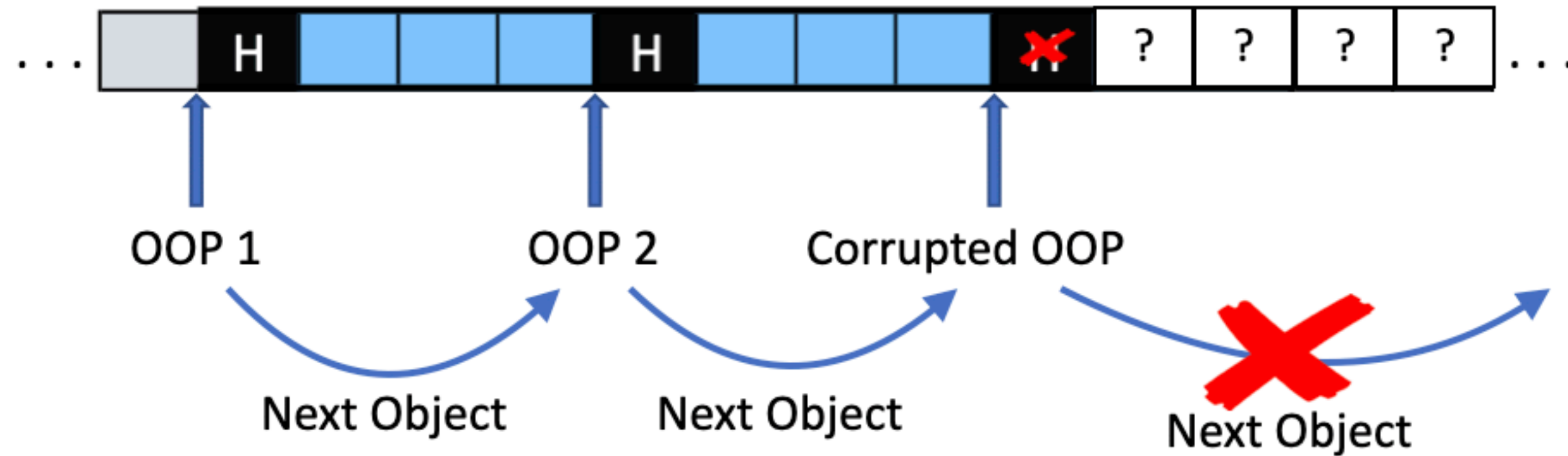
# Real World Bug Fix #2

## A Memory Corruption

Oop Oop Oop Oop ?

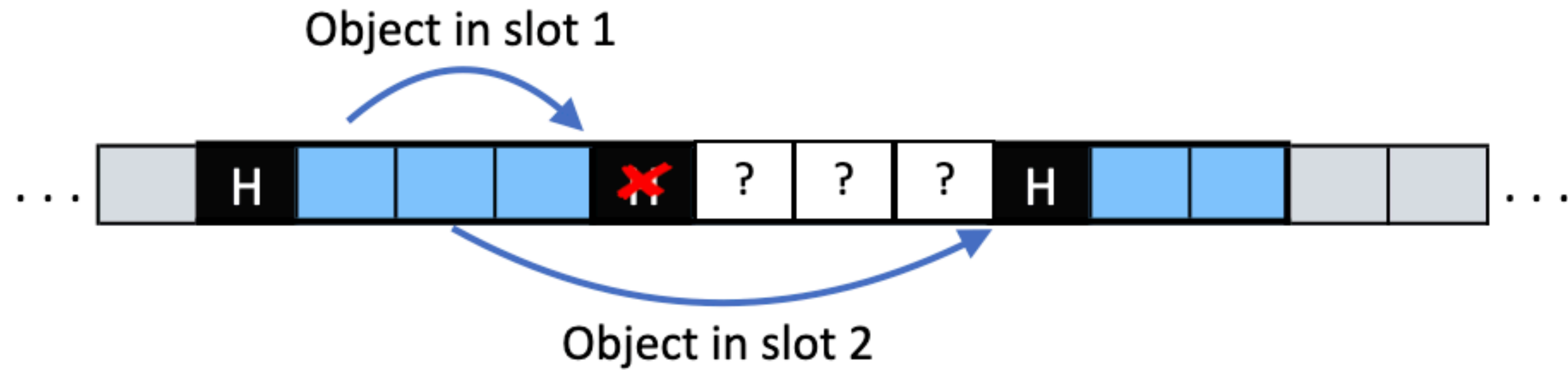
# Real World Bug Fix #2

## Iterating the Corrupted Memory



# Real World Bug Fix #2

## Recovering Objects





# Real World Bug Fix #2

## Cleansing The Corruption

|     |     |     |     |     |     |     |     |     |     |     |     |     |     |
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| Oop | Oop | Oop | Oop | F   | Oop | Oop | Oop | Oop | Oop | Oop | Oop | Oop | Oop |
| F   | Oop | Oop | F   | Oop | F   | Oop | Oop | F   | Oop | Oop | Oop | Oop | Oop |
| Oop | Oop | Oop | Oop | Oop | F   | Oop | Oop | Oop | Oop | Oop | Oop | Oop | Oop |
| Oop | Oop | Oop | F   | Oop | Oop | Oop | Oop | Oop | Oop | Oop | Oop | Oop | Oop |

# Real World Bug Fix #2

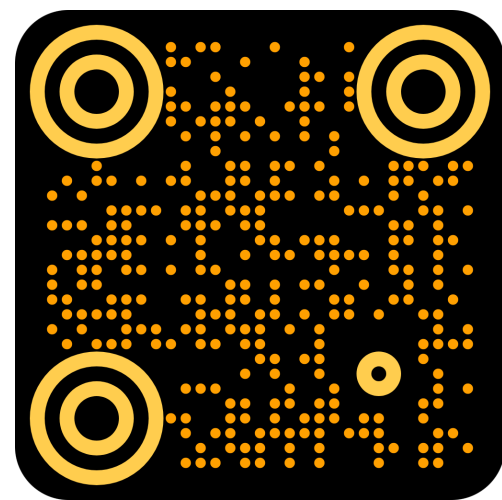
## Corruption Cleansing Analysis

- Objects' slots iteration
- Reference patching
- Re-computation of the free lists/tree
- Focus on learning rather than how to look



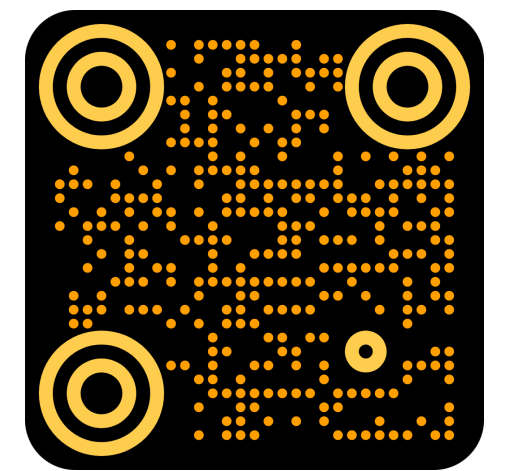
# Conclusion

# Github

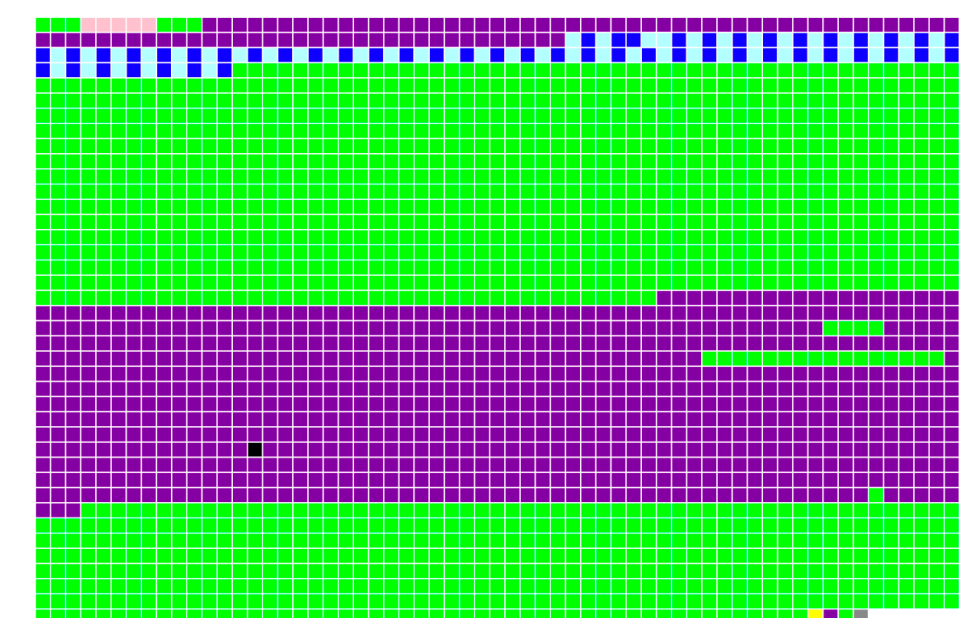


- Tooling at the VM level **was** hard
- LLOOP eases VM level tooling
- Validated with multiple custom tools
- Zombie Pharo images are now a thing

VMIL Paper  
preprint



## Visualization



- 1 pinned object
- 895 compiled method
- 51 class
- 5 special object
- 1 context
- 1 free chunk
- 1468 regular object
- 51 metaclass

|              |  |
|--------------|--|
| * Key        | * Value  |
| address      | 406749864  |
| printString  | Form   |
| header       | 1011000000000000000111001100100000000100000000000000111001100001 |
| class        | Form class   |
| oopClassTag  | 1841   |
| format       | Non Indexable (1)  |
| hash         | 1842   |
| pinned       | false  |
| space        | Old Space  |
| immutable    | false  |
| numSlots     | 11   |
| superclass   | DisplayMedium  |
| methodDict   | Instance of MethodDictionary                                     |
| format       | 65541  |
| layout       | Instance of FixedLayout  |
| organization | Instance of ClassOrganization                                    |
| subclasses   | Instance of Array  |
| name         | Form   |
| classPool    | Instance of Dictionary   |
| sharedPool   | nilObject  |
| environment  | Instance of SystemDictionary                                     |
| category     | Graphics-Display Objects-Forms                                   |



Pierre Misse-Chanabier  
[pierre\\_misse25@msn.com](mailto:pierre_misse25@msn.com)  
[github.com/hogoww](https://github.com/hogoww)  
Discord tag: hogo#8547