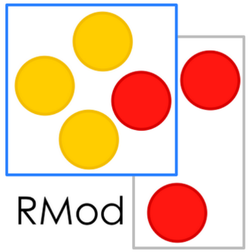


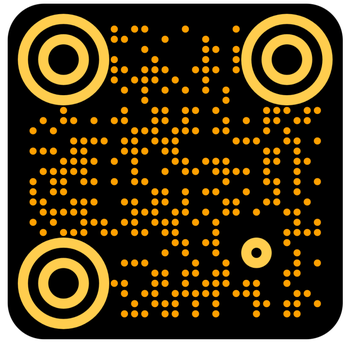
Inria

Université de Lille

cnrs

IMT Nord Europe
École Mines-Télécom
IMT-Université de Lille

CRIStAL
Centre de Recherche en Informatique, Signal et Automatique de Lille

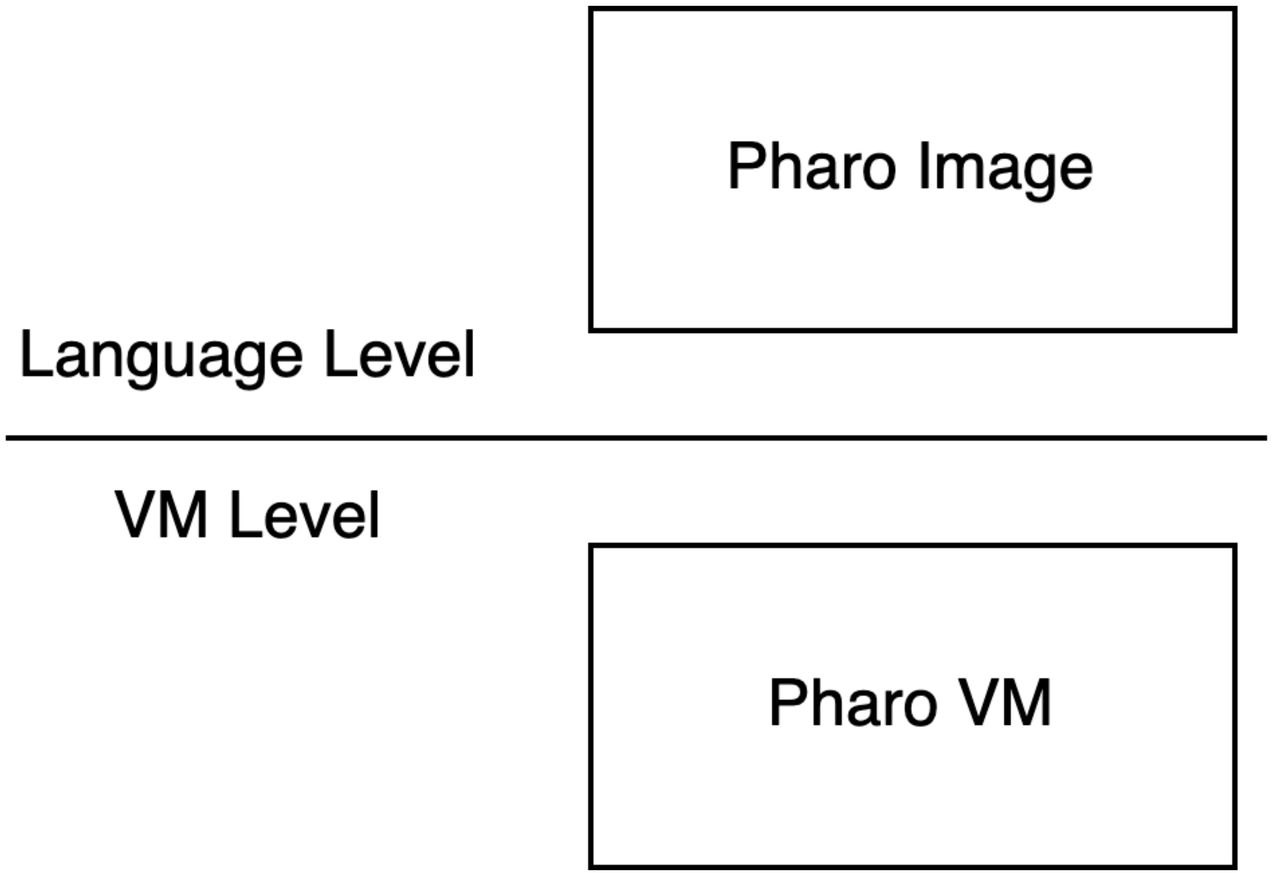


Polyphemus
Ease Virtual Machine Level Tooling

Pierre Misse-Chanabier
Theo Rogliano

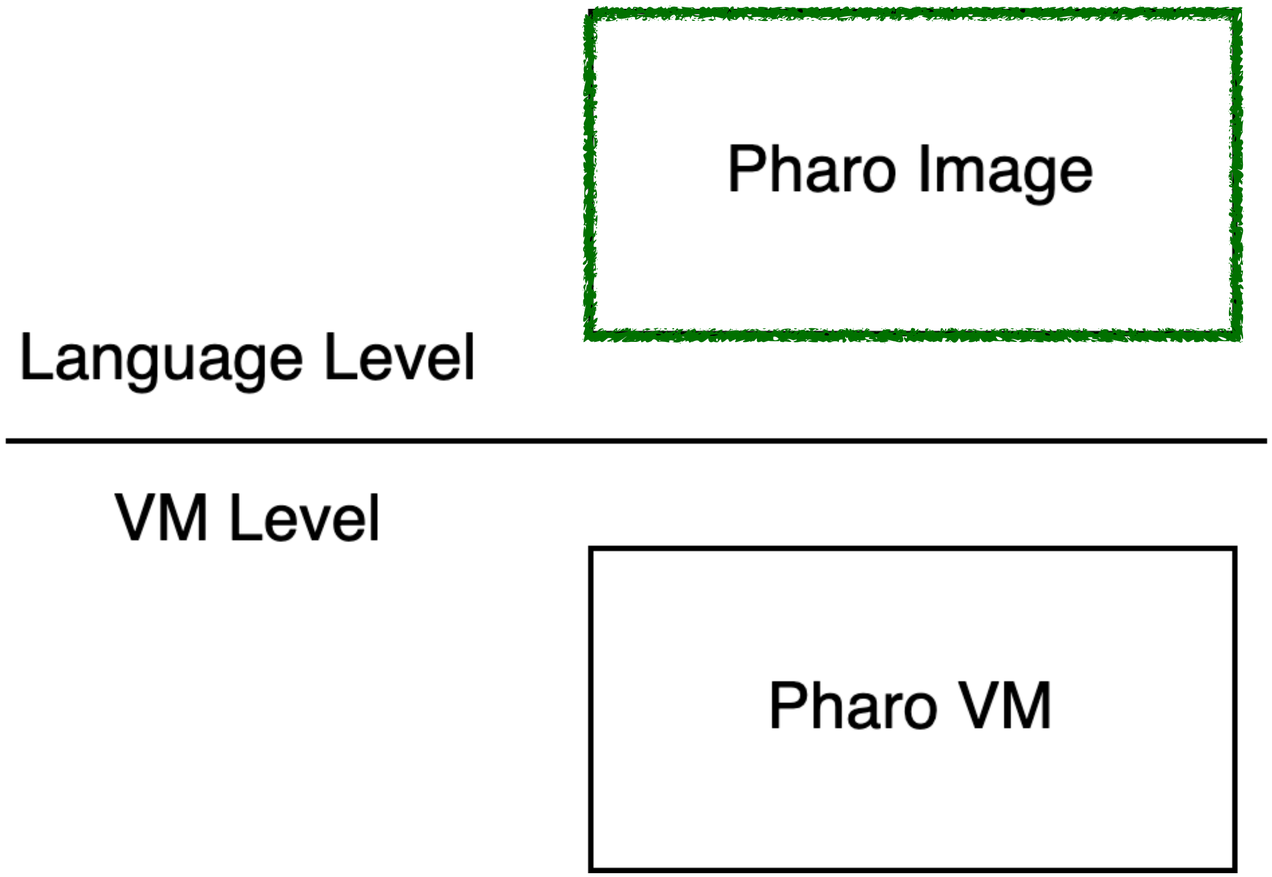
Who Does Not Love Tools ?

Tooling Levels



Who Does Not Love Tools ?

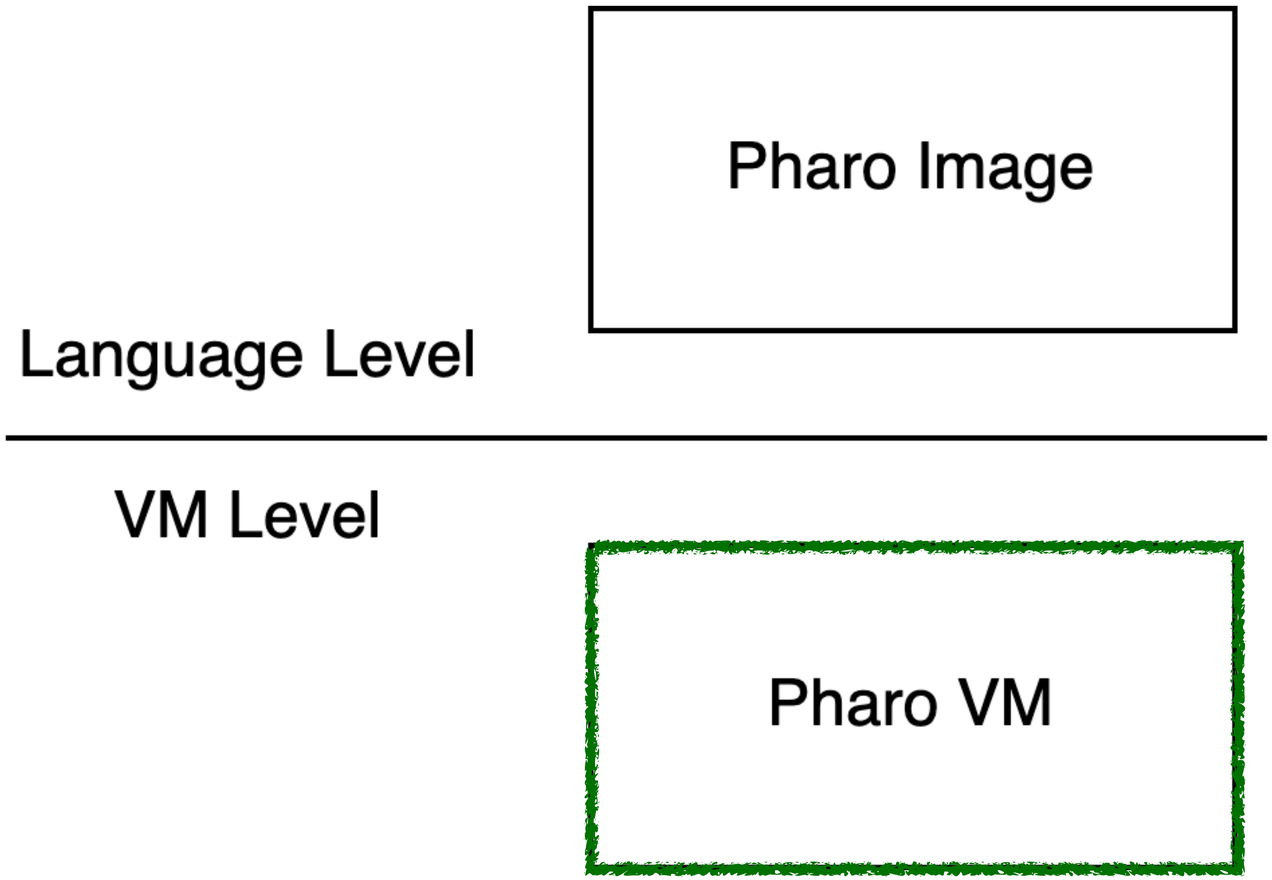
Tools at the Language Level

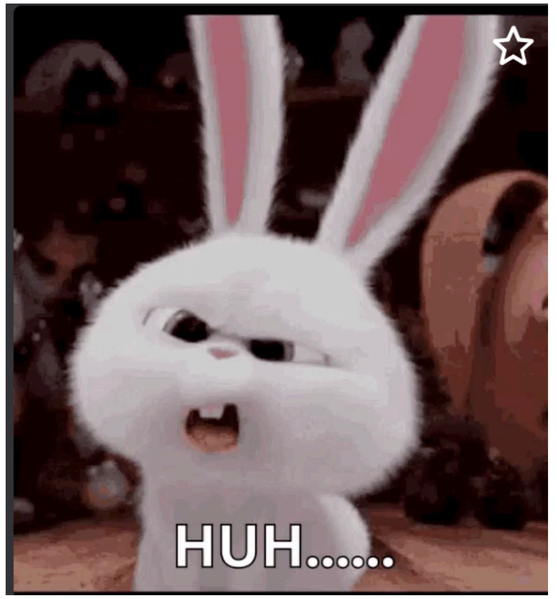


NewTools, Moose, Roassal,
Calypso, SUnit, Iceberg, Refactoring, Epicea
... ...

Who Does Not Love Tools ?

Tools at the VM Level



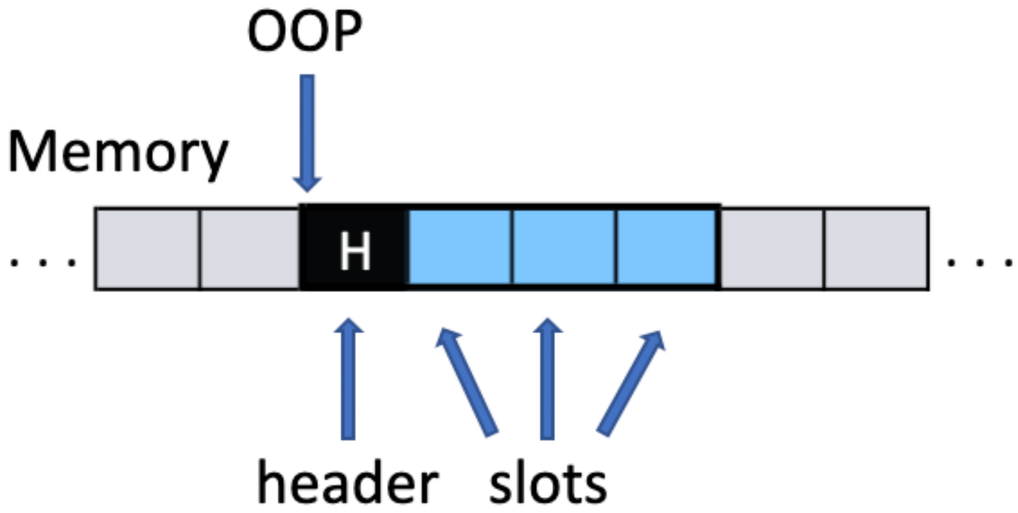


Bootstrap, VM machine code debugger
Others ?

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.
```

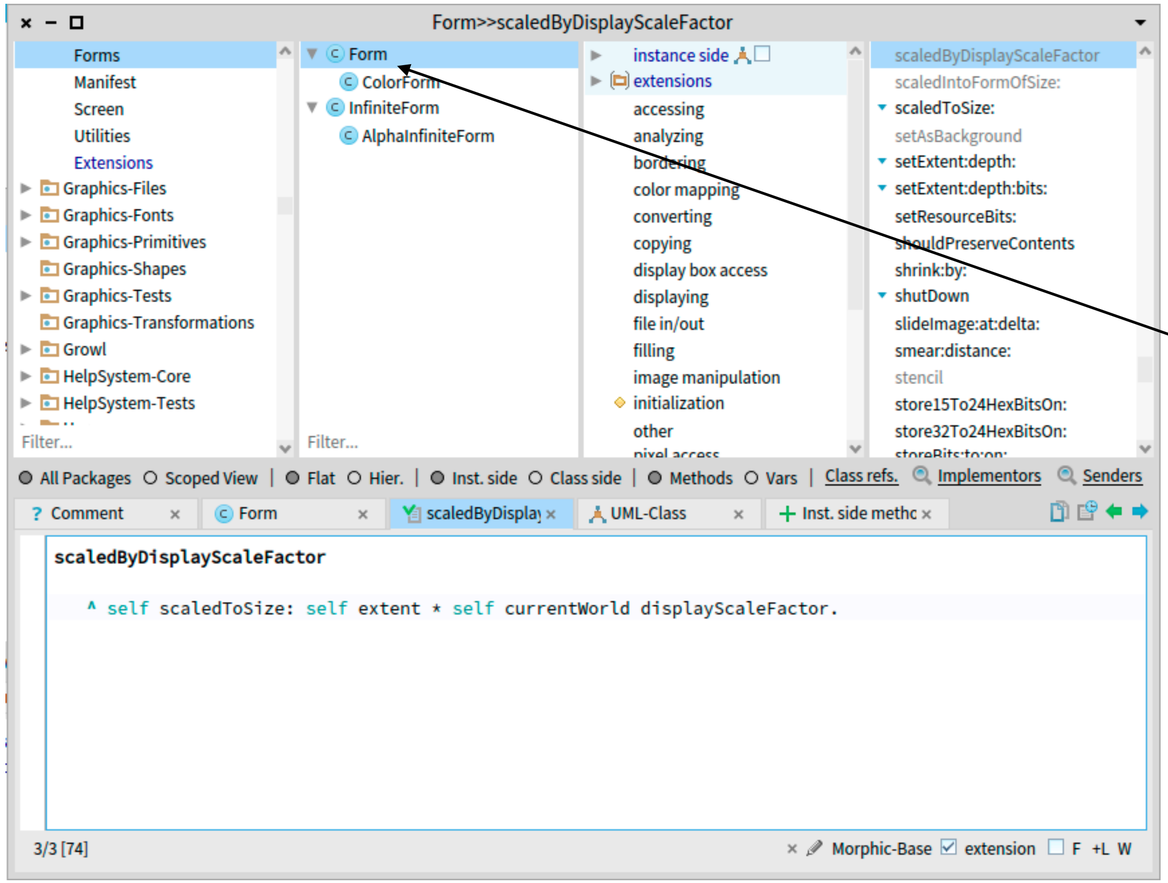
Who Does Not Love Tools ?

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 AbstractWorldRenderer
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 !

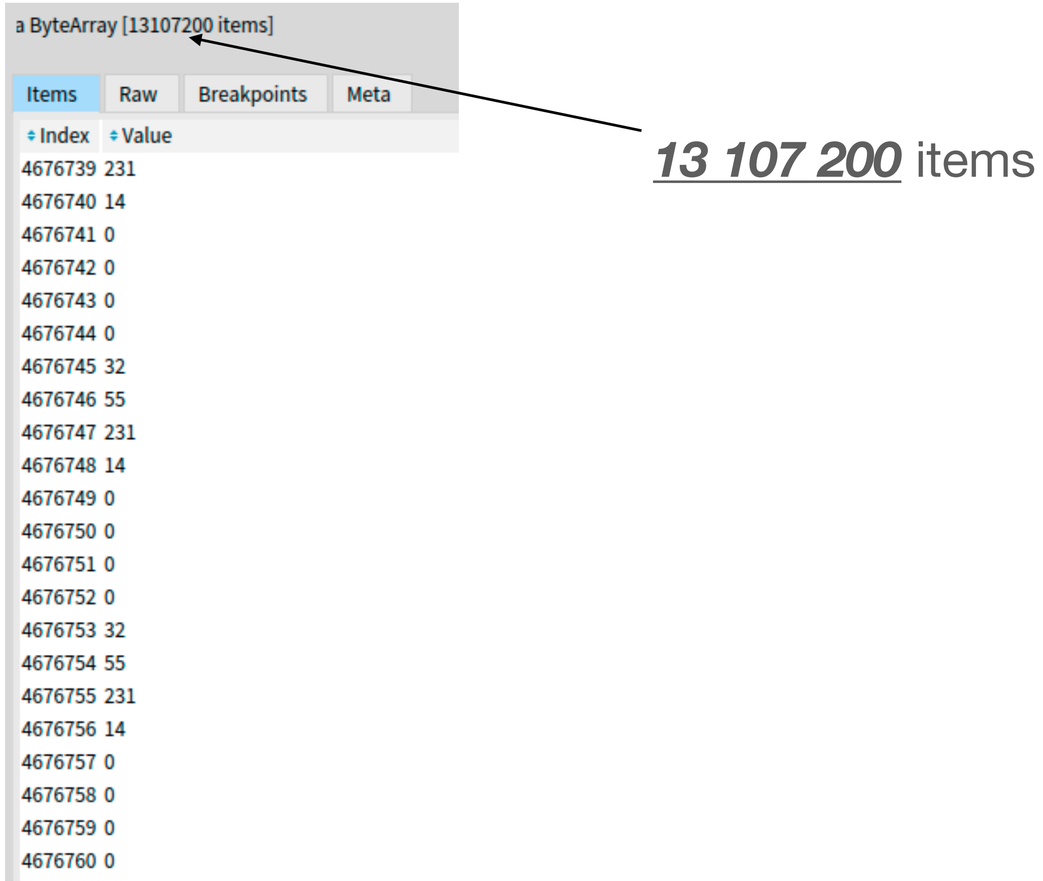
Let’s Find the Class Form …



Found it !

Let’s Code VM Level Tools !

Let’s Find The Class Form … But at the VM Level …



13 107 200 items

Let’s Code VM Level Tools !

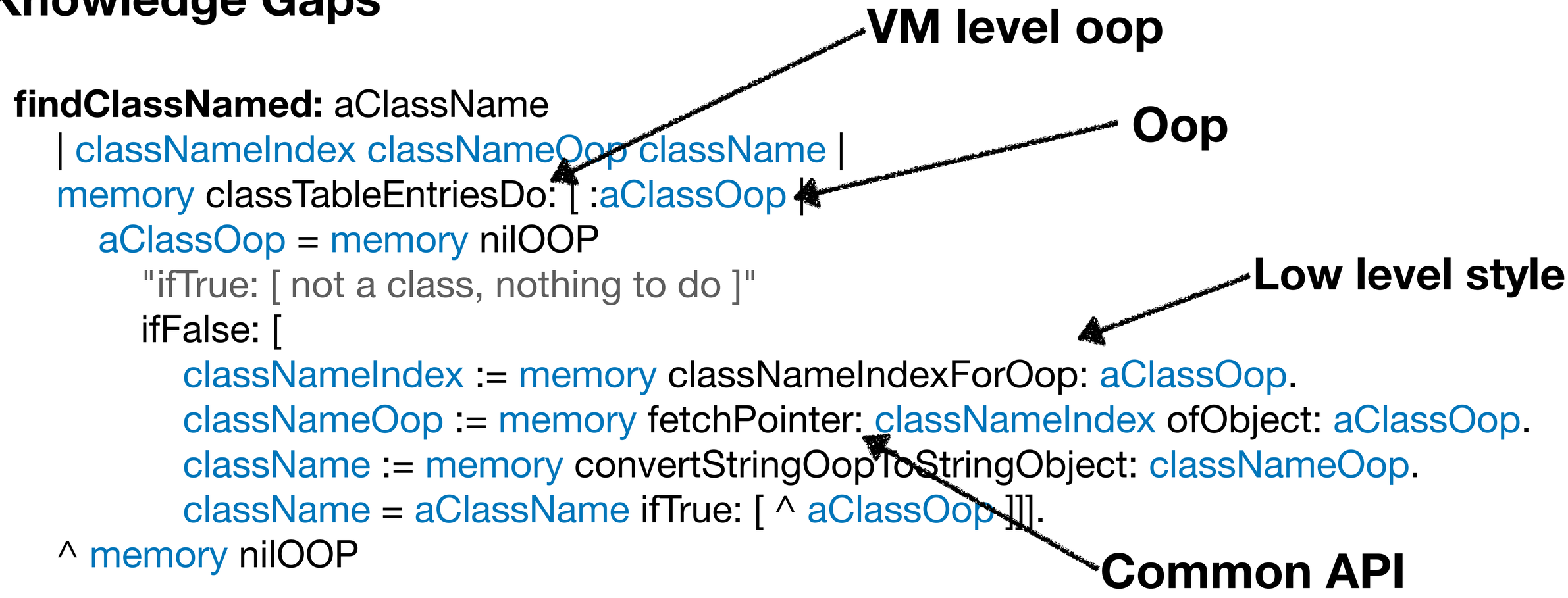
With the Help of the Simulator

```
findClassNamed: 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 findClassNamed: Form >>> 406749864

Let’s Code VM Level Tools !

Knowledge Gaps




```
findClassNamed: 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
```

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	Solutions
• Ordinary Object Pointers (OOP)	• Objects
• Common API	• Specialized API & Polymorphism
• VM level information	• 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

Pharo Object

self	Form
superclass	DisplayMedium
methodDict	a MethodDictionary [206 items] (size 206)
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

LLOOP

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

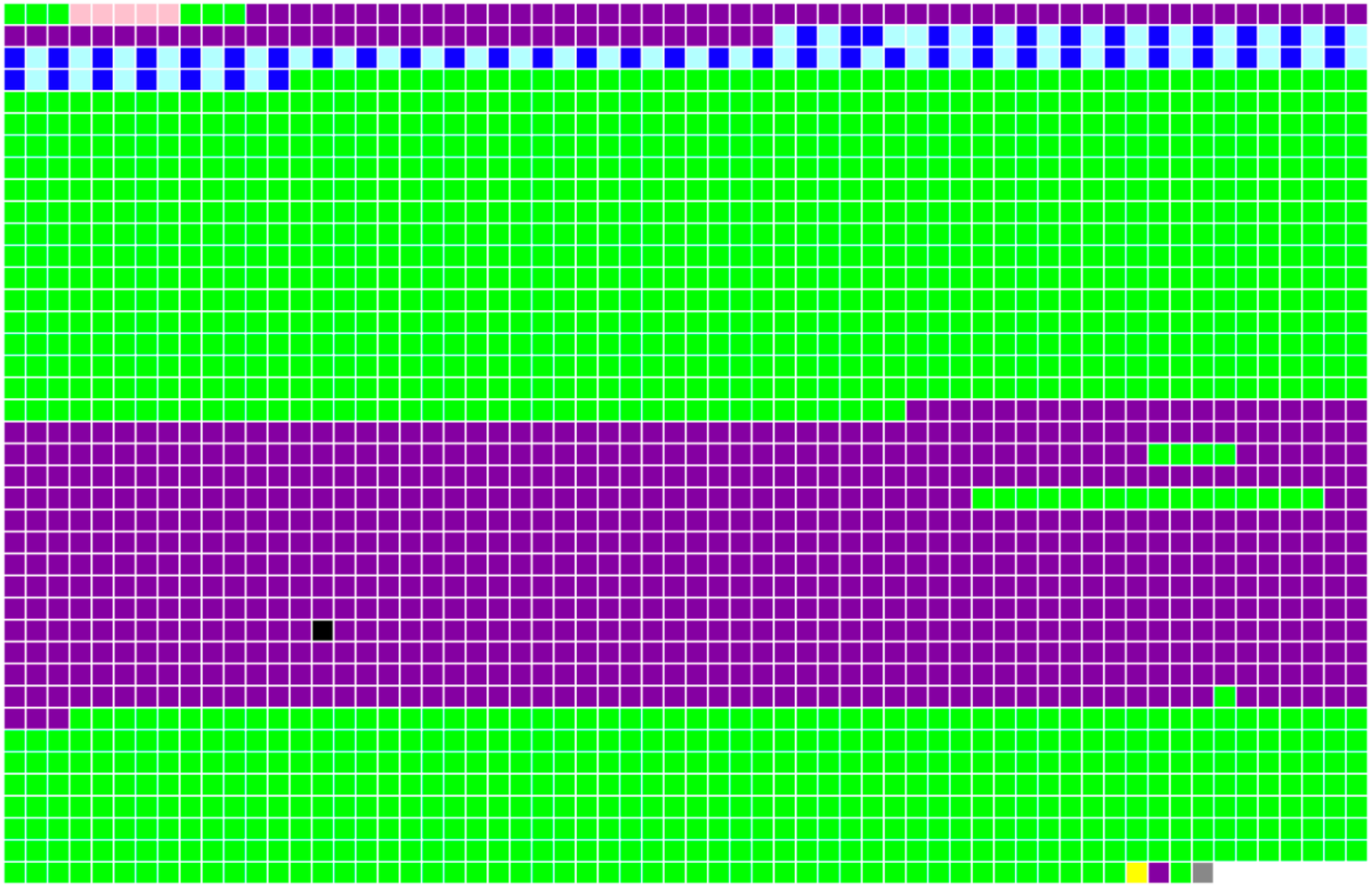
Inspectors #2

Compiled Method

address	8685808
printString	PCMessage >> #arguments
header	10100000000000000000000000001111100000000000010000011011
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

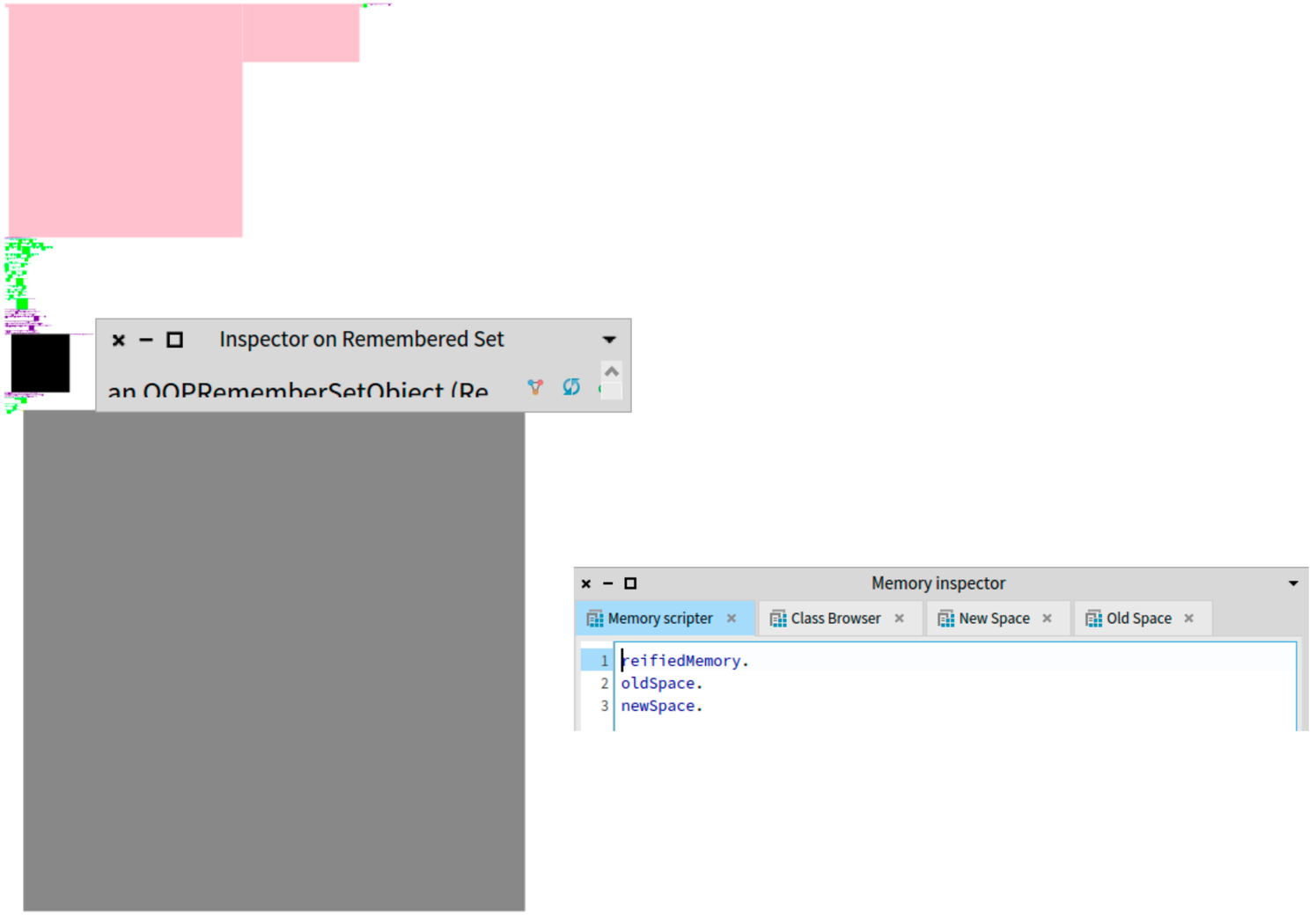
1 free chunk

1468 regular object

51 metaclass

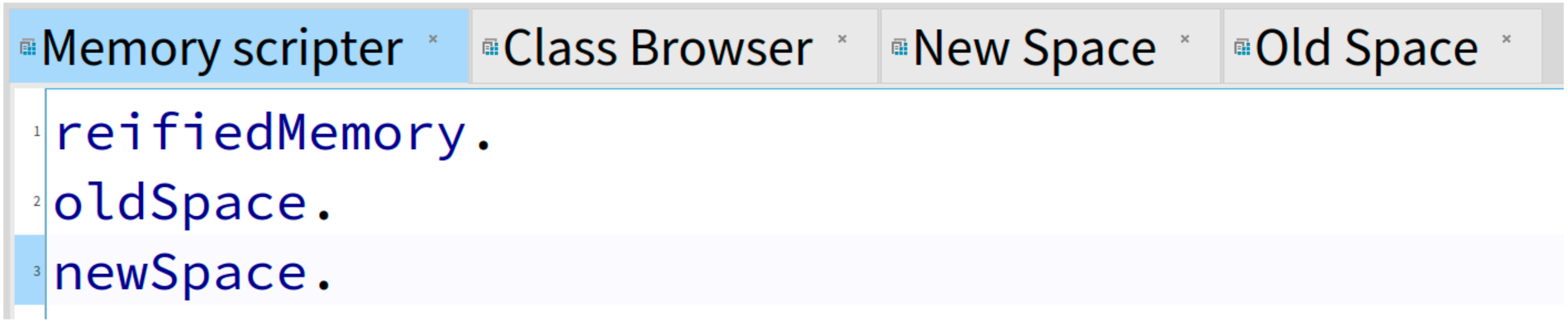
Polyphemus

What's That ?



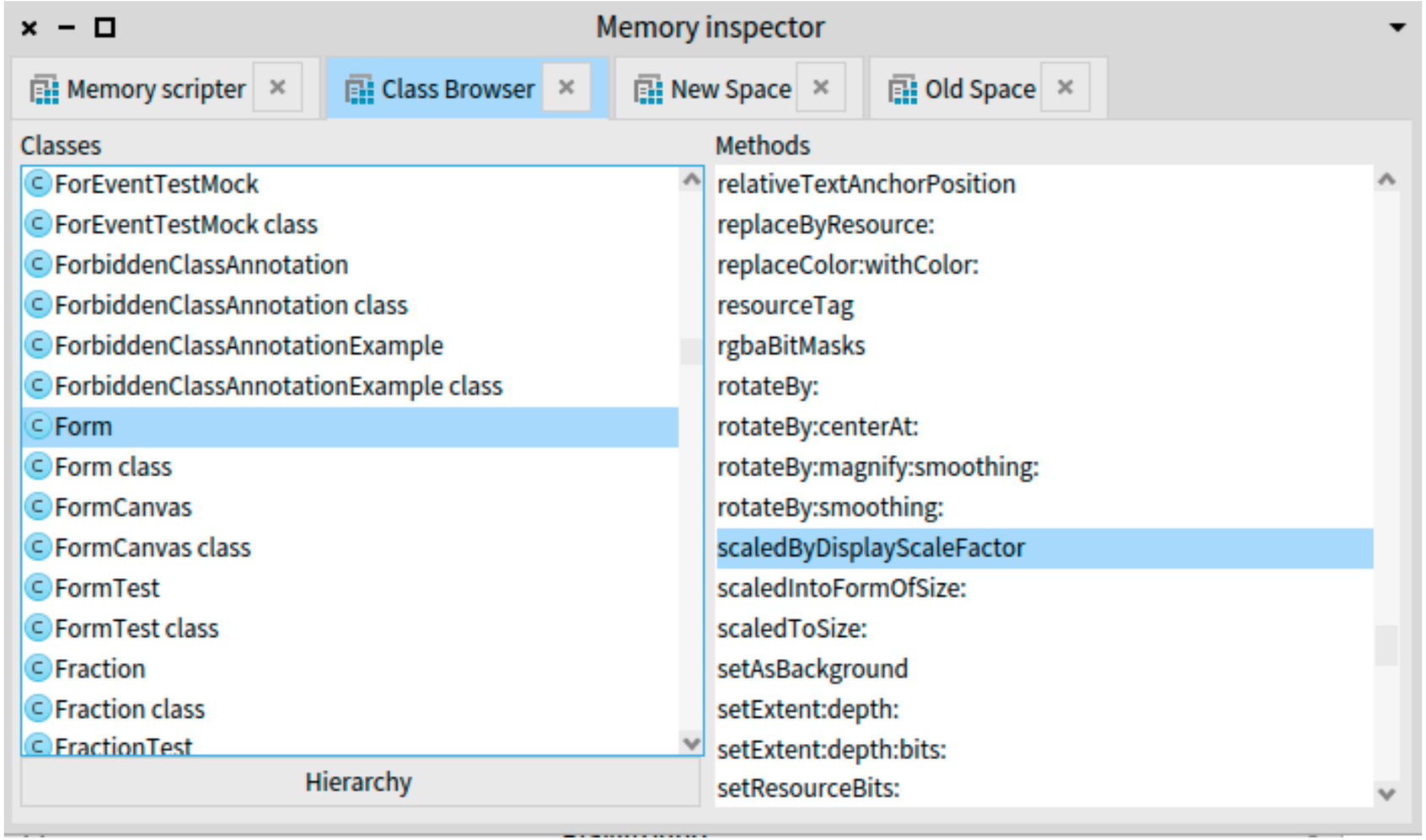
Polyphemus

Scripter



Polyphemus

Memory Visualisation #2



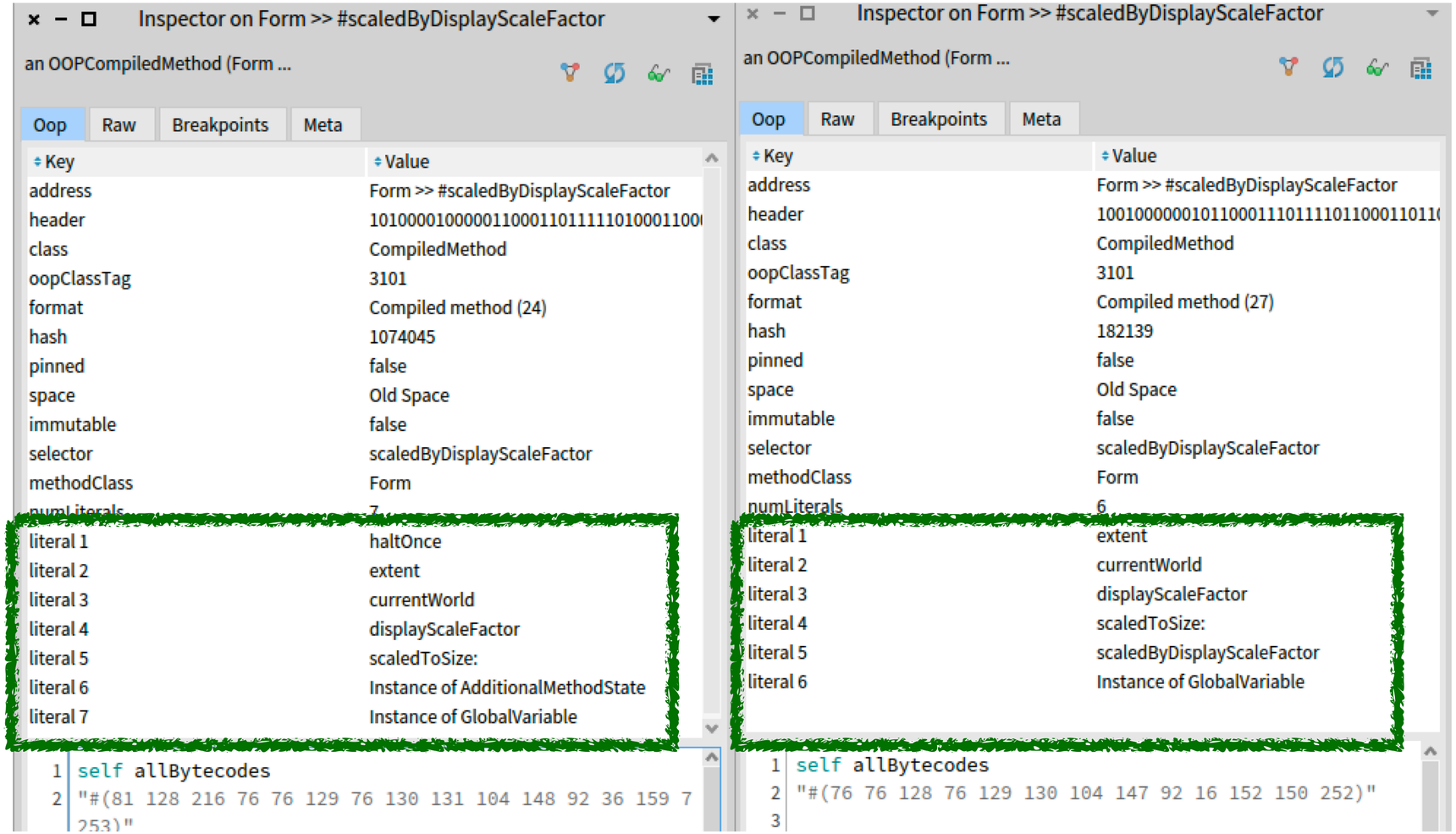
Real World Bug Fix #1

Remember This ?

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

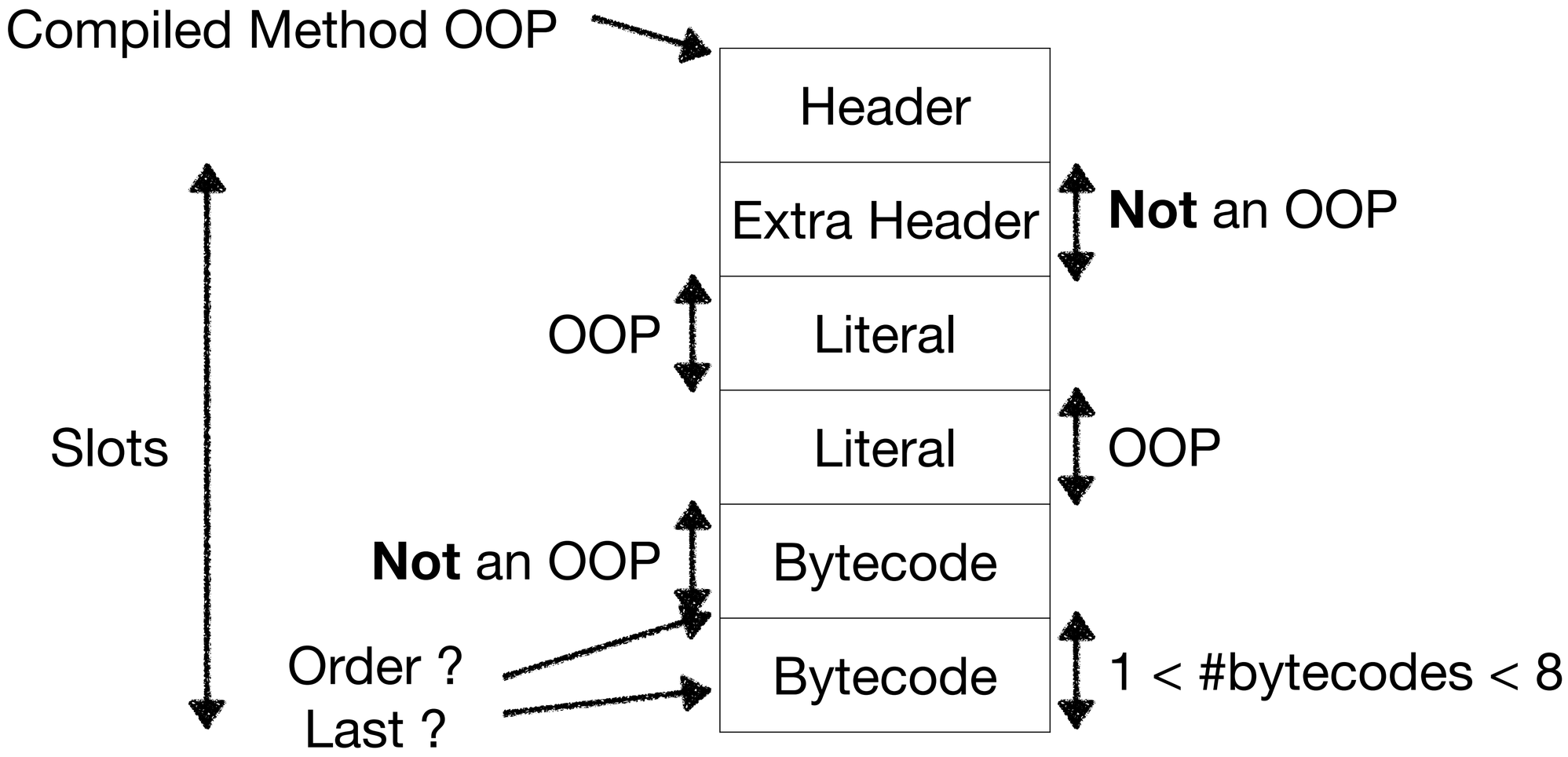
Real World Bug Fix #1

A Meta-Error Fix



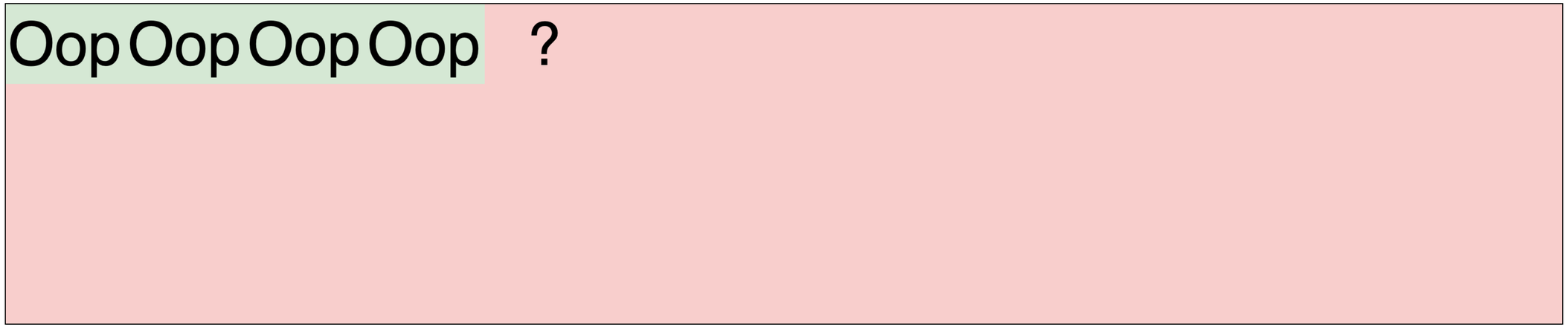
Real World Bug Fix #1

A Meta-Error Fix Analysis



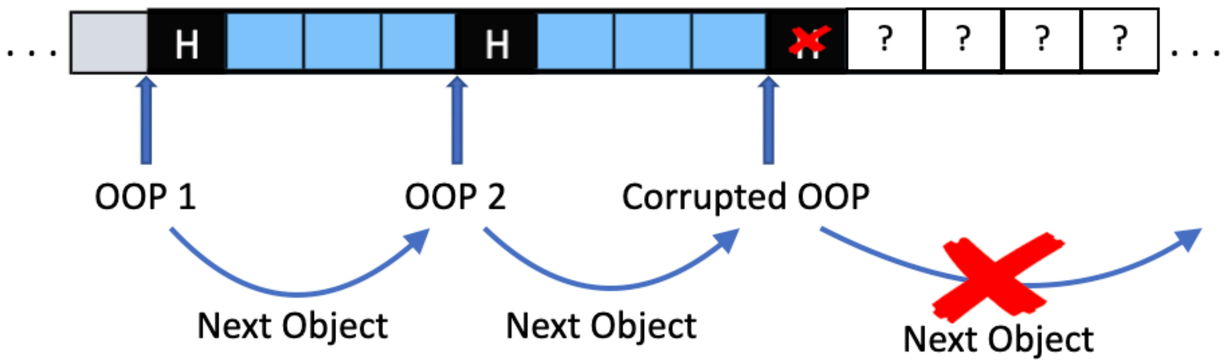
Real World Bug Fix #2

A Memory Corruption



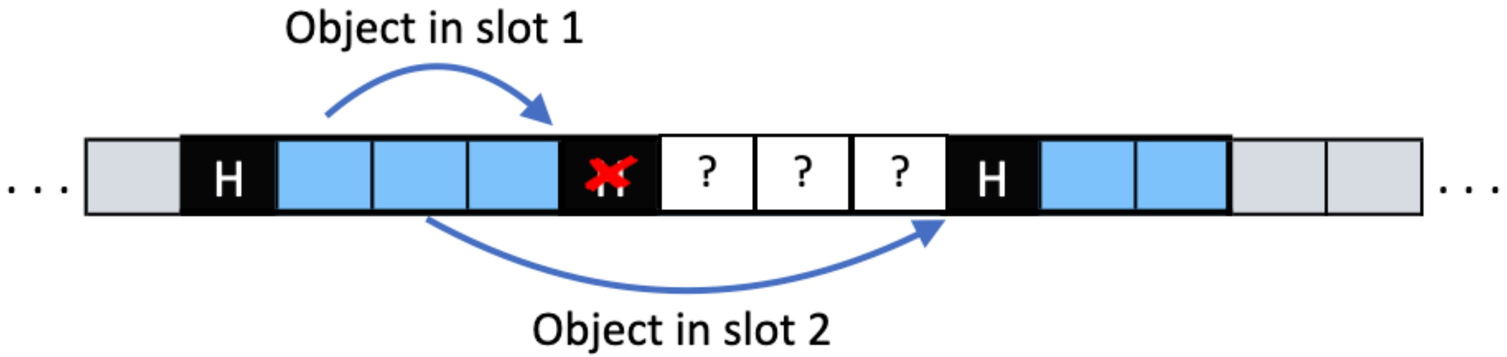
Real World Bug Fix #2

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
F	Oop	Oop	F	Oop	F	Oop	Oop	F	Oop	Oop	Oop	Oop
Oop	Oop	Oop	Oop	Oop	F	Oop	Oop	Oop	Oop	Oop	Oop	Oop
Oop	Oop	Oop	F	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

Pierre Misse-Chanabier
pierre_misse25@msn.com
github.com/hogoww
Discord tag: hogo#8547

Visualization