RubyTSK

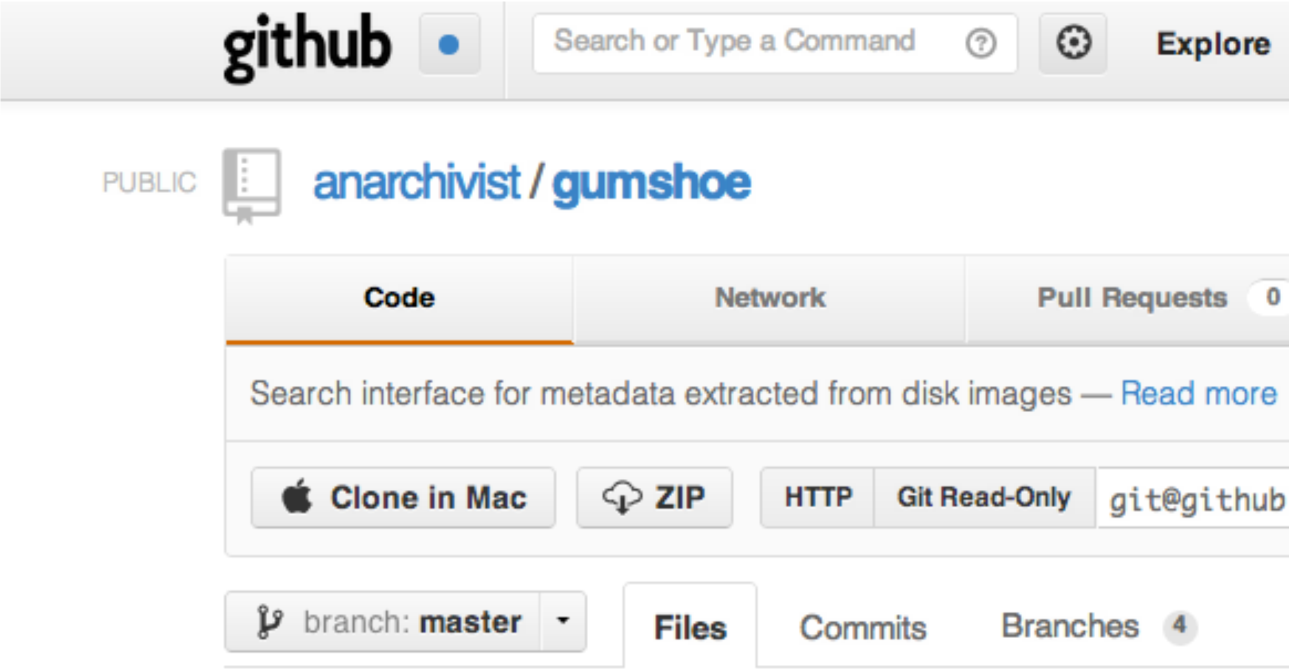
A Ruby Binding for the SleuthKit

Matthew Stephens, UVA Library

About me

- Sustaining Digital Scholarship @ UVA Library
- Legacy code & data specialist
- Ruby shop
- Custodian for orphaned data & apps
- Next door to an archive!

Inspiration?



PUBLIC anarchivist / gumshoe

Search interface for metadata extracted from disk images — Read more

Ideal Ruby SleuthKit API

- Fidelity

Ideal Ruby SleuthKit API

- Fidelity
- Flexibility

Ideal Ruby SleuthKit API

- Fidelity
- Flexibility
- Easy to use

Ideal Ruby SleuthKit API

- Fidelity
- Flexibility
- Easy to use
- Accessible to C && Ruby developers

The Dream

- `Require ‘sleuthkit’`

The Dream

- Require ‘sleuthkit’
- image=Sleuthkit.new(‘path/to/my.iso’)

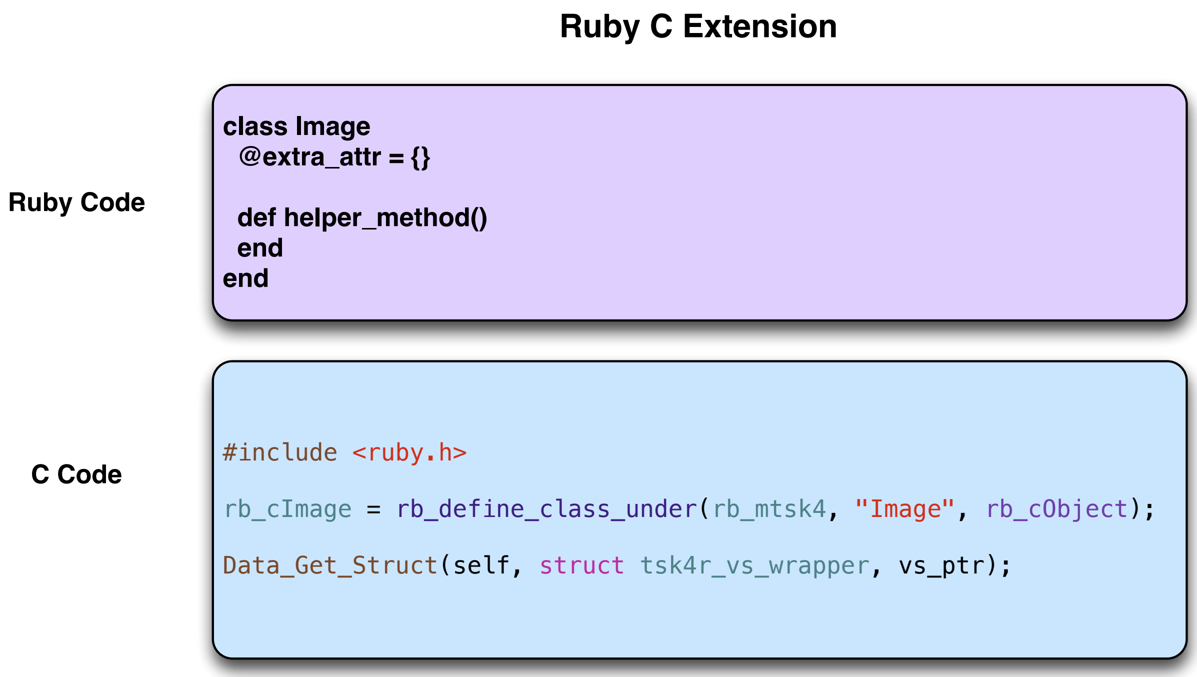
The Dream

- Require ‘sleuthkit’
- image=Sleuthkit.new(‘path/to/my.iso’)
- …

The Dream

- `Require ‘sleuthkit’`
- `image=Sleuthkit.new(‘path/to/my.iso’)`
- …
- cavort

C wrapped in Ruby



Ruby C Extension

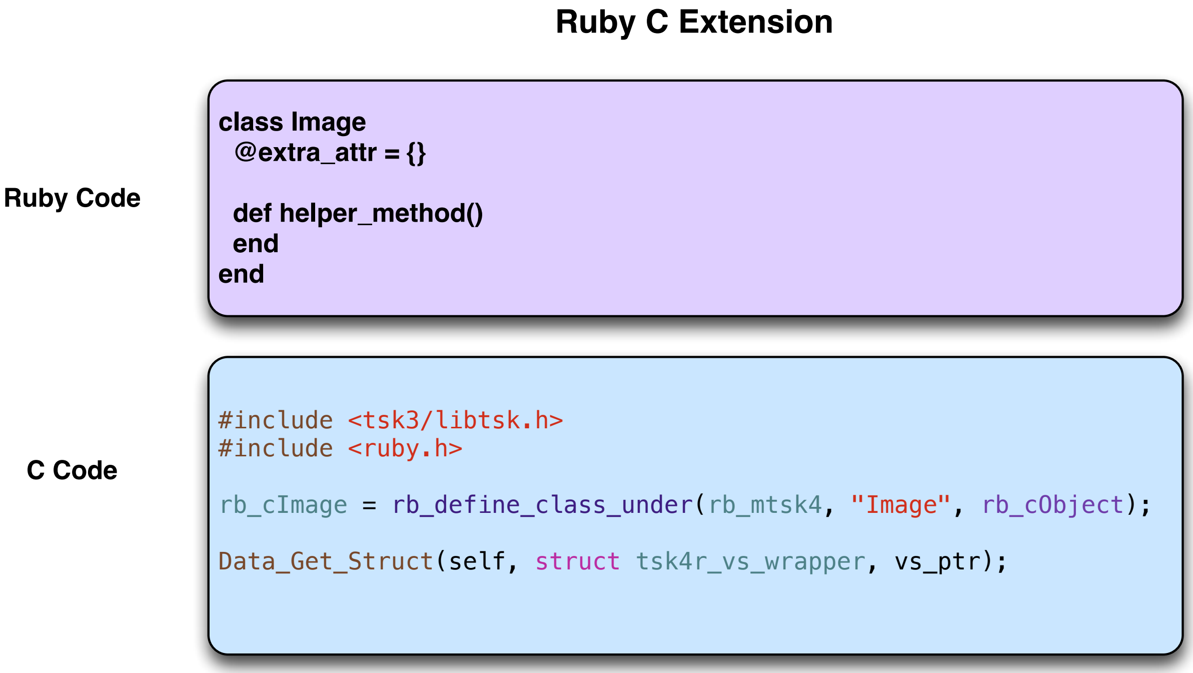
Ruby Code

```ruby
class Image
  @extra_attr = {}

  def helper_method()
  end
end
```

C Code

```c
#include <ruby.h>

rb_cImage = rb_define_class_under(rb_mtsk4, "Image", rb_cObject);

Data_Get_Struct(self, struct tsk4r_vs_wrapper, vs_ptr);
```

C wrapped in Ruby



Ruby C Extension

Ruby Code

```ruby
class Image
  @extra_attr = {}

  def helper_method()
  end
end
```

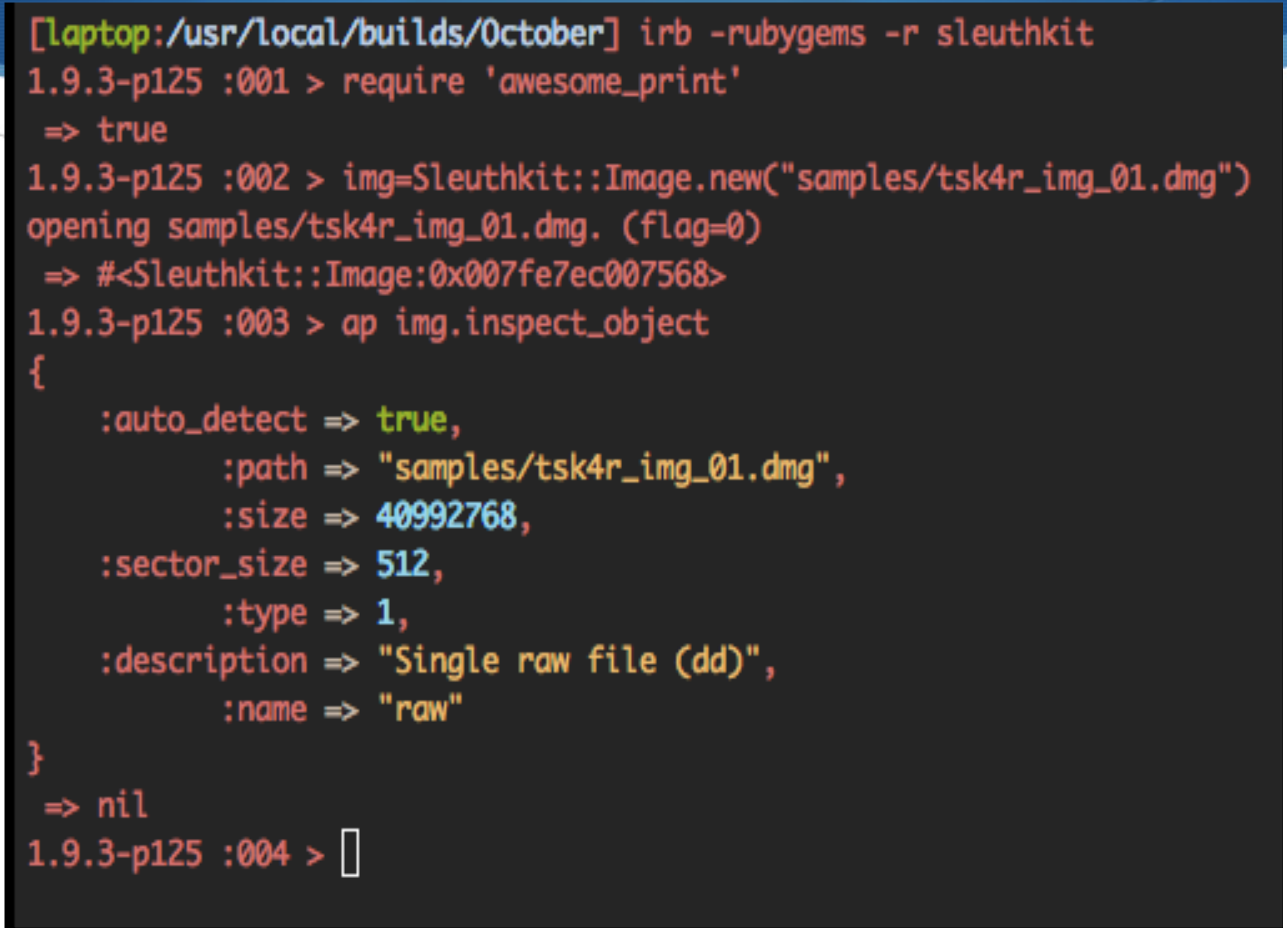
C Code

```c
#include <tsk3/libtsk.h>
#include <ruby.h>

rb_cImage = rb_define_class_under(rb_mtsk4, "Image", rb_cObject);

Data_Get_Struct(self, struct tsk4r_vs_wrapper, vs_ptr);
```

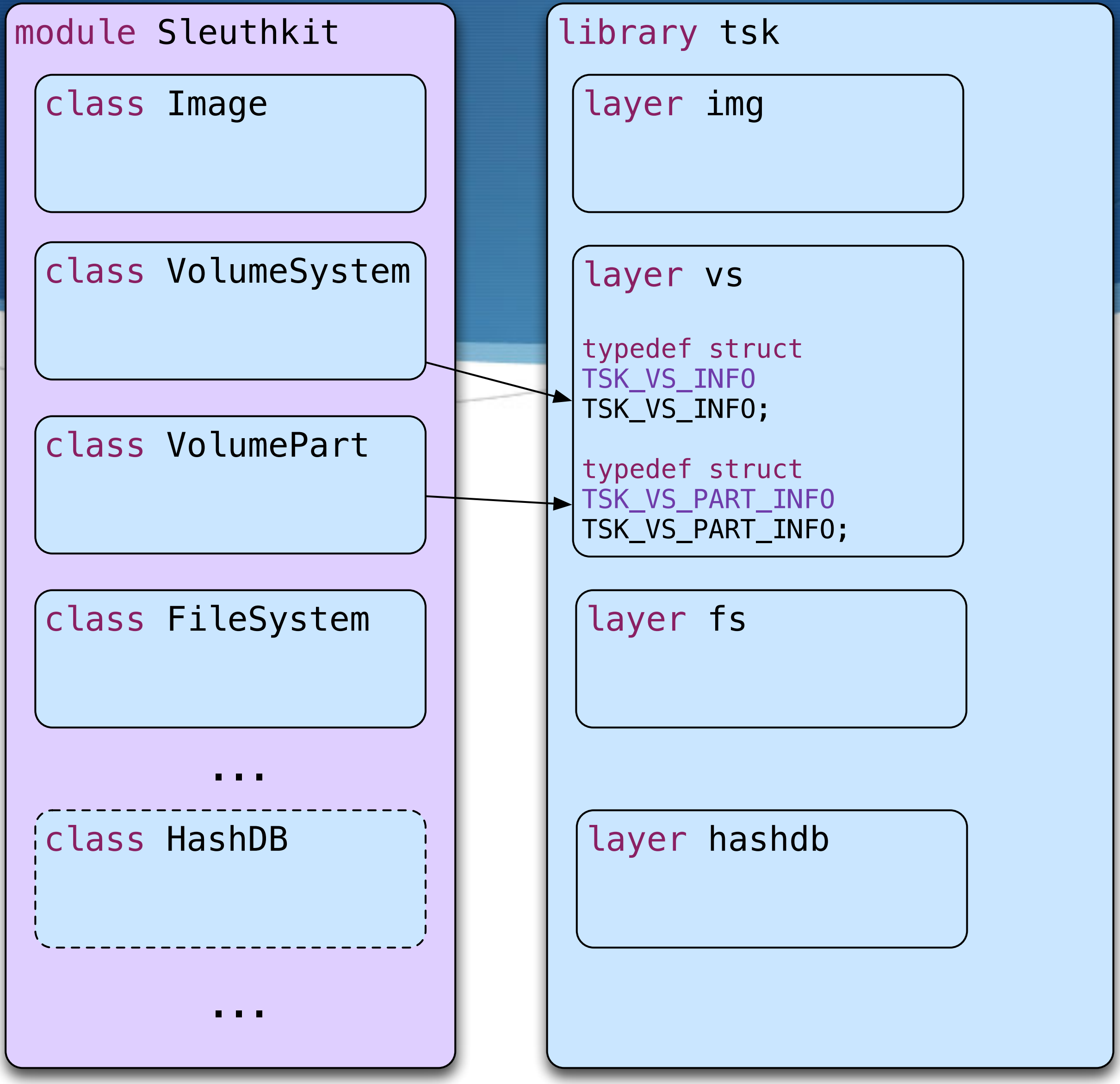
The wrapper

```
#include <tsk3/libtsk.h>

// Sleuthkit::Image struct-in-ruby-object
struct tsk4r_img_wrapper {
  TSK_IMG_INFO * image;
};

// Sleuthkit::Image function declarations
VALUE allocate_image(VALUE klass);
void  deallocate_image(struct tsk4r_img_wrapper * ptr);
VALUE initialize_disk_image(int argc, VALUE *args, VALUE self);
```

1st Result: Ruby Objects



```
[laptop:/usr/local/builds/October] irb -rubygems -r sleuthkit
1.9.3-p125 :001 > require 'awesome_print'
 => true
1.9.3-p125 :002 > img=Sleuthkit::Image.new("samples/tsk4r_img_01.dmg")
opening samples/tsk4r_img_01.dmg. (flag=0)
 => #<Sleuthkit::Image:0x007fe7ec007568>
1.9.3-p125 :003 > ap img.inspect_object
{
    :auto_detect => true,
           :path => "samples/tsk4r_img_01.dmg",
           :size => 40992768,
    :sector_size => 512,
           :type => 1,
    :description => "Single raw file (dd)",
           :name => "raw"
}
 => nil
1.9.3-p125 :004 >
```



module Sleuthkit

class Image

class VolumeSystem

class VolumePart

class FileSystem

...

class HashDB

...

library tsk

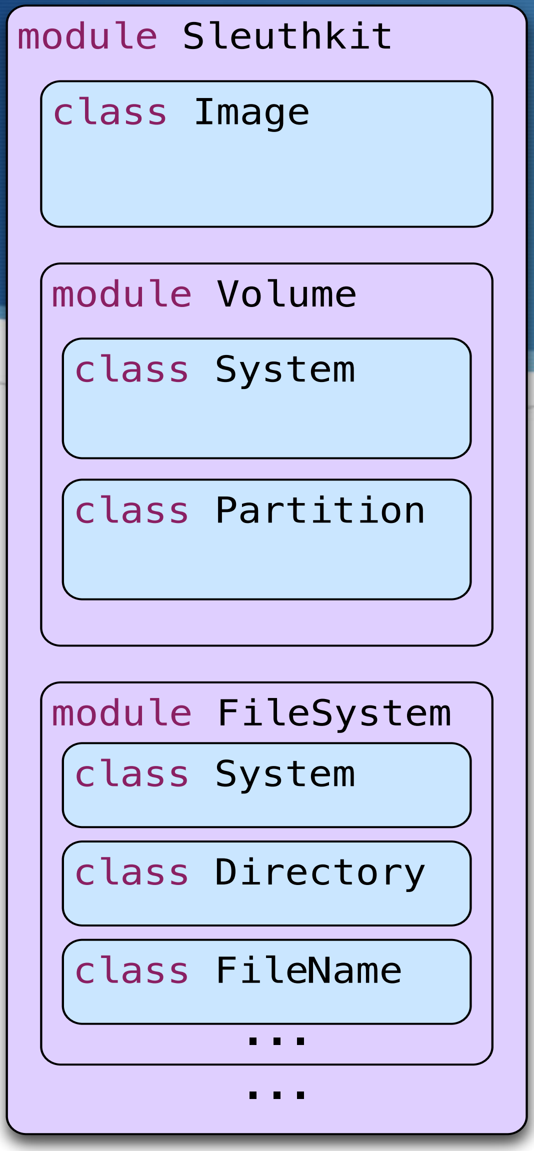
layer img

layer vs

```
typedef struct
TSK_VS_INFO
TSK_VS_INFO;

typedef struct
TSK_VS_PART_INFO
TSK_VS_PART_INFO;
```

layer fs

layer hashdb



module Sleuthkit

class Image

module Volume

class System

class Partition

module FileSystem

class System

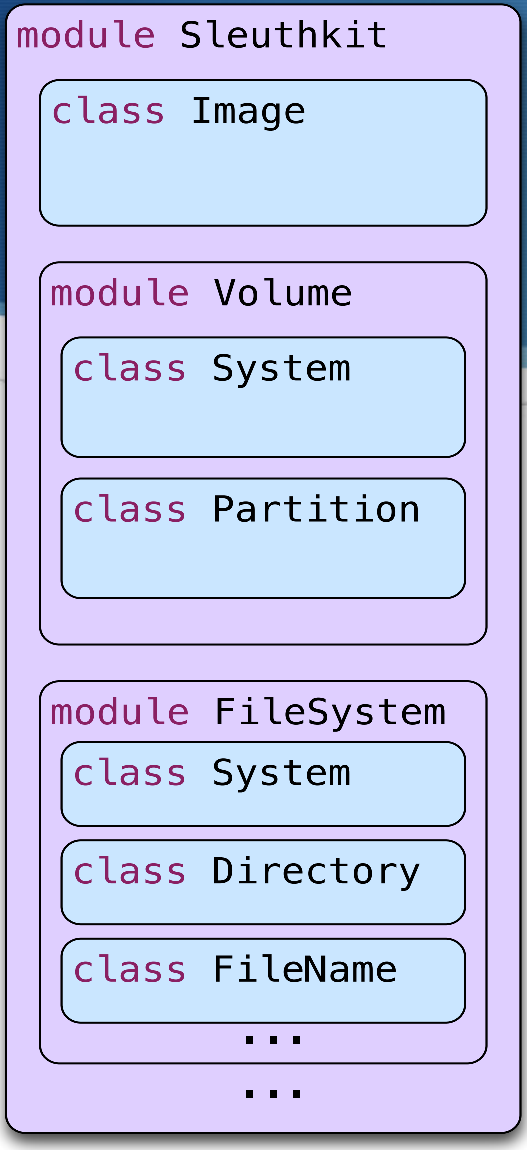
class Directory

class FileName

...

...

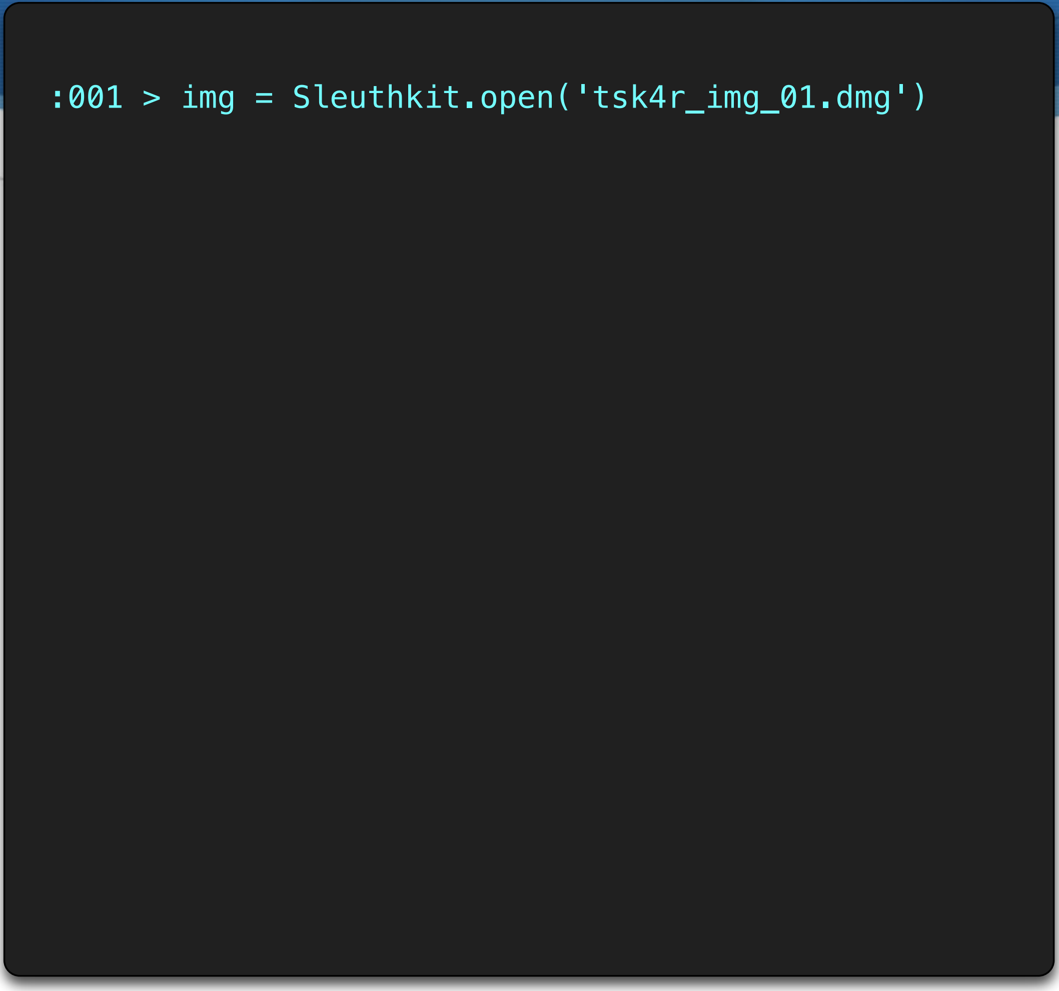
```
SleuthKit::Image.new()
```



```
module Sleuthkit
  class Image
  module Volume
    class System
    class Partition
  module FileSystem
    class System
    class Directory
    class FileName
    ...
  ...
```

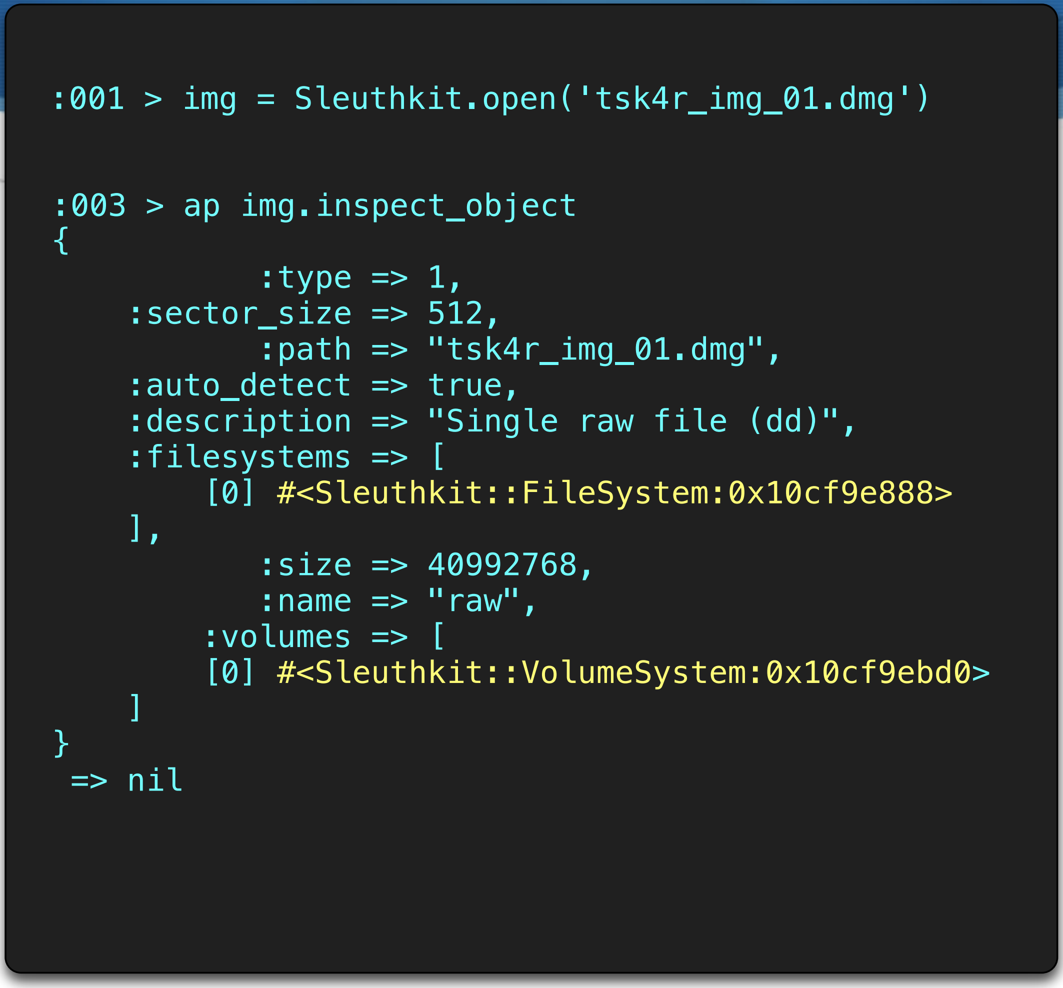
```
SleuthKit::Image.new()
SleuthKit::Volume::Partition.new()
SleuthKit::FileSystem::System.new()
```

Module helper methods!



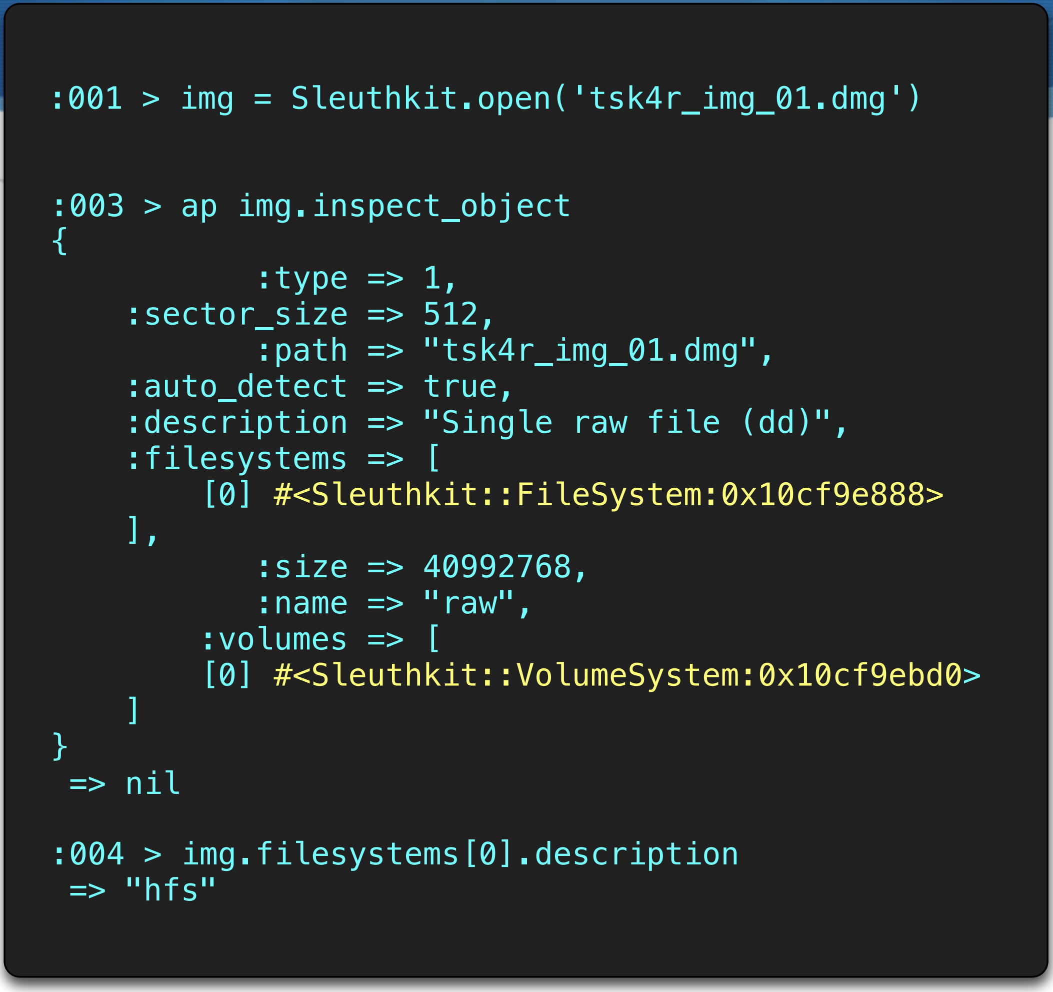
```
:001 > img = Sleuthkit.open('tsk4r_img_01.dmg')
```

Module helper methods!



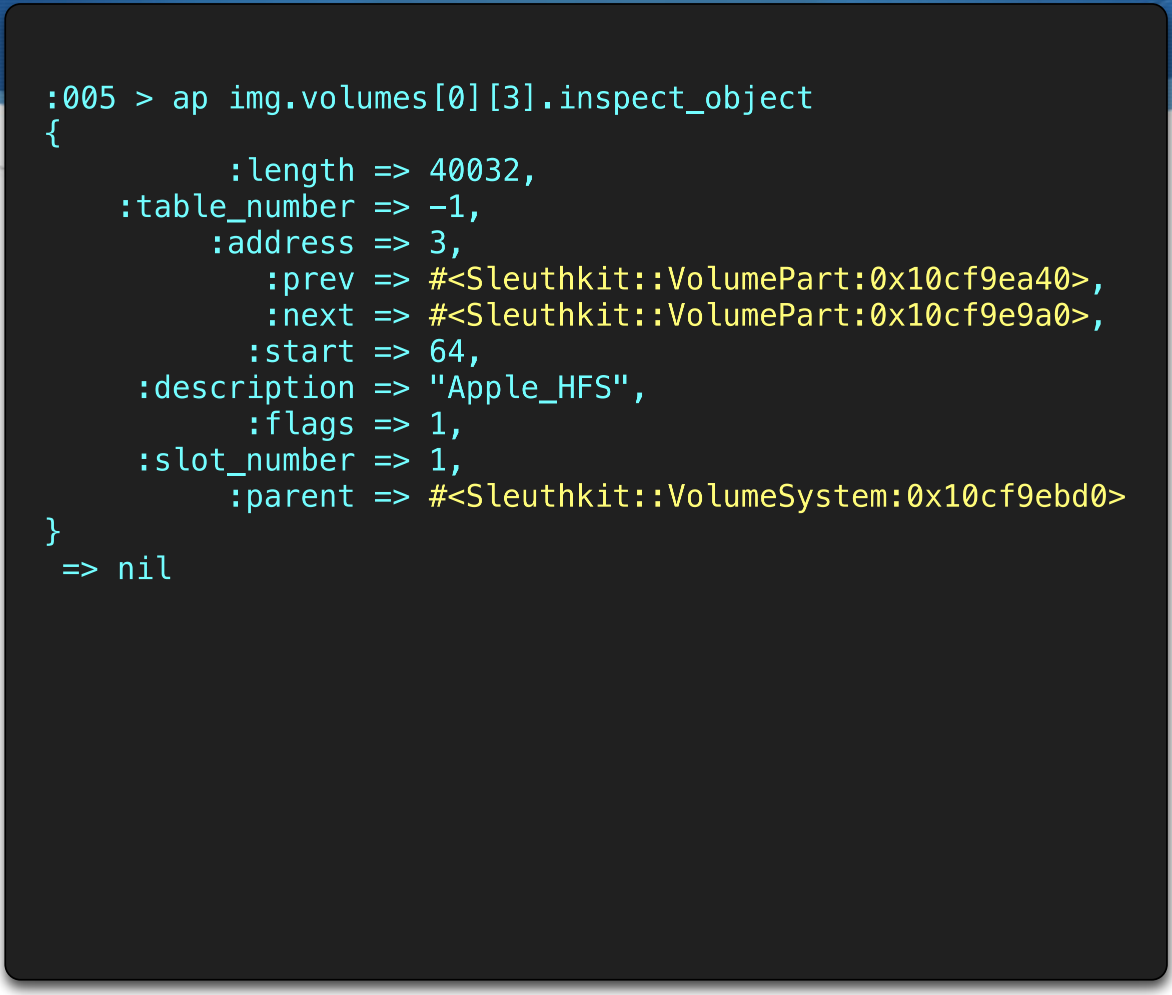
```
:001 > img = Sleuthkit.open('tsk4r_img_01.dmg')


:003 > ap img.inspect_object
{
           :type => 1,
    :sector_size => 512,
           :path => "tsk4r_img_01.dmg",
    :auto_detect => true,
    :description => "Single raw file (dd)",
    :filesystems => [
        [0] #<Sleuthkit::FileSystem:0x10cf9e888>
    ],
           :size => 40992768,
           :name => "raw",
        :volumes => [
        [0] #<Sleuthkit::VolumeSystem:0x10cf9ebd0>
    ]
}
 => nil
```

Module helper methods!



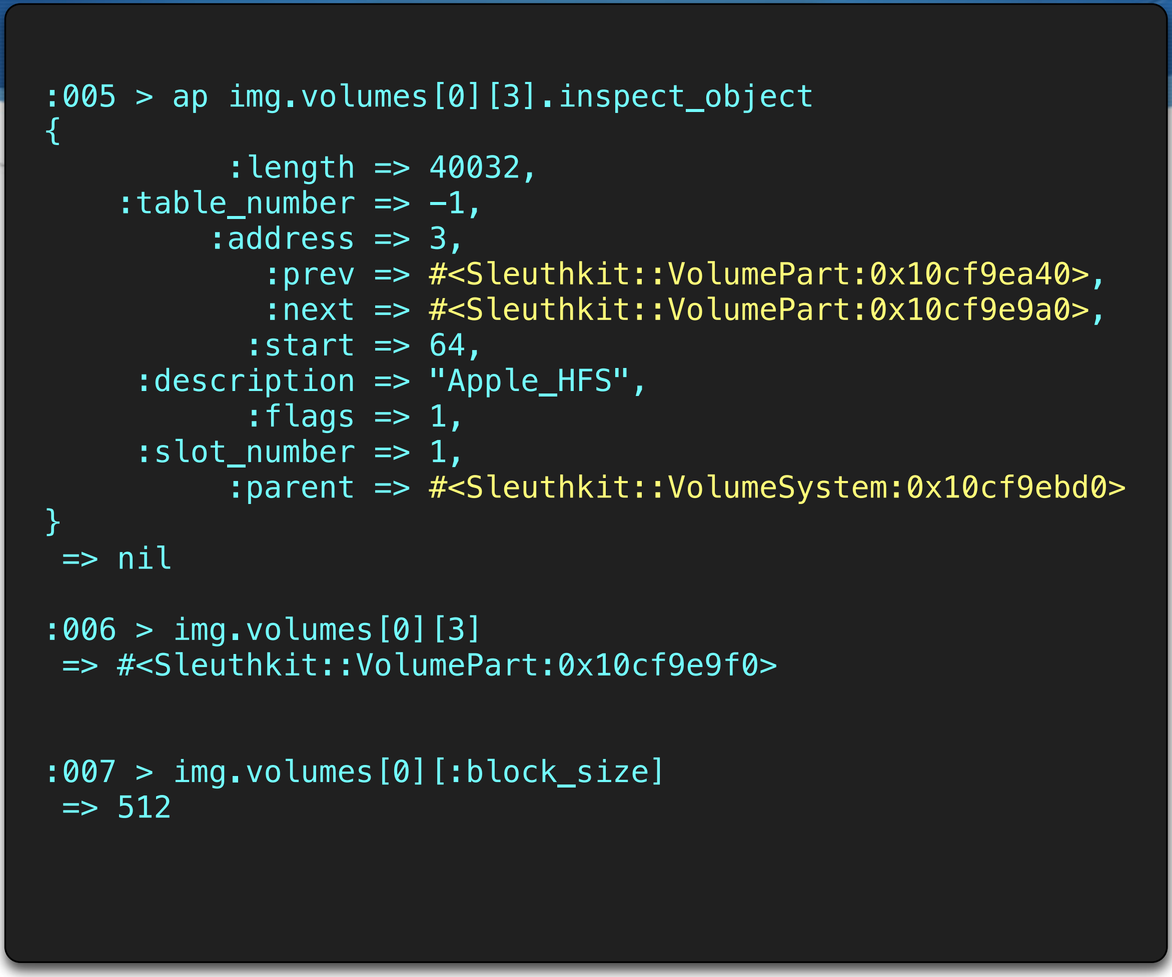
```
:001 > img = Sleuthkit.open('tsk4r_img_01.dmg')


:003 > ap img.inspect_object
{
           :type => 1,
    :sector_size => 512,
           :path => "tsk4r_img_01.dmg",
    :auto_detect => true,
    :description => "Single raw file (dd)",
    :filesystems => [
        [0] #<Sleuthkit::FileSystem:0x10cf9e888>
    ],
           :size => 40992768,
           :name => "raw",
        :volumes => [
        [0] #<Sleuthkit::VolumeSystem:0x10cf9ebd0>
    ]
}
 => nil

:004 > img.filesystems[0].description
 => "hfs"
```

Module helper methods!



```
:005 > ap img.volumes[0][3].inspect_object
{
          :length => 40032,
    :table_number => -1,
         :address => 3,
            :prev => #<Sleuthkit::VolumePart:0x10cf9ea40>,
            :next => #<Sleuthkit::VolumePart:0x10cf9e9a0>,
           :start => 64,
     :description => "Apple_HFS",
           :flags => 1,
     :slot_number => 1,
          :parent => #<Sleuthkit::VolumeSystem:0x10cf9ebd0>
}
 => nil
```

Module helper methods!



```
:005 > ap img.volumes[0][3].inspect_object
{
          :length => 40032,
    :table_number => -1,
         :address => 3,
            :prev => #<Sleuthkit::VolumePart:0x10cf9ea40>,
            :next => #<Sleuthkit::VolumePart:0x10cf9e9a0>,
           :start => 64,
     :description => "Apple_HFS",
           :flags => 1,
     :slot_number => 1,
          :parent => #<Sleuthkit::VolumeSystem:0x10cf9ebd0>
}
 => nil

:006 > img.volumes[0][3]
 => #<Sleuthkit::VolumePart:0x10cf9e9f0>


:007 > img.volumes[0][:block_size]
 => 512
```

Moving back & forth

Ruby calling function written in C

```
VALUE call_tsk_fsstat(VALUE self, VALUE io);
```

Moving back & forth

Ruby calling function written in C

```
VALUE call_tsk_fsstat(VALUE self, VALUE io);
```

```
def print_tsk_fsstat(report = "")

  if report.kind_of?( IO )
   self.call_tsk_fsstat(report)
  end
end
```

Moving back & forth

Can C see Ruby?

```ruby
def parse_opts(h={})
  opts = h || Hash.new
  return opts
end
```

Moving back & forth

Can C see Ruby?

```ruby
def parse_opts(h={})
  opts = h || Hash.new
  return opts
end
```

```c
opts = rb_funcall(self, rb_intern("parse_opts"), 1, opts);
```

C && Ruby example
flexible call to function pointer

```
:015 > s=String.new
=> ""
:016 > filesys=fs
=> #<Sleuthkit::FileSystem:0x10cf9e888>
:017 >
:017 > s=String.new
=> ""
:018 > filesys.print_tsk_fsstat(s)
=> "FILE SYSTEM INFORMATION\n--------------------------------------------\nFile System Type: HFS+\nFile
System Version: HFS+\n\nVolume Name: Partition 1\nVolume Identifier: ff83fbdcb863d7d8\n\nLast Mounted By:
Mac OS X, Journaled\nVolume Unmounted Properly\nMount Count: 53\n\nCreation
:019 > puts s
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: HFS+
File System Version: HFS+

Volume Name: Partition 1
Volume Identifier: ff83fbdcb863d7d8

Last Mounted By: Mac OS X, Journaled
Volume Unmounted Properly
Mount Count: 53
```

Road Map

- Flesh out API at file system layer & hashdb

Road Map

- Flesh out API at file system layer & hashdb
- Wrap higher-level functions

Road Map

- Flesh out API at file system layer & hashdb
- Wrap higher-level functions
- FFI (libffi)

Road Map

- Flesh out API at file system layer & hashdb
- Wrap higher-level functions
- FFI (libffi)
- More Ruby, less C

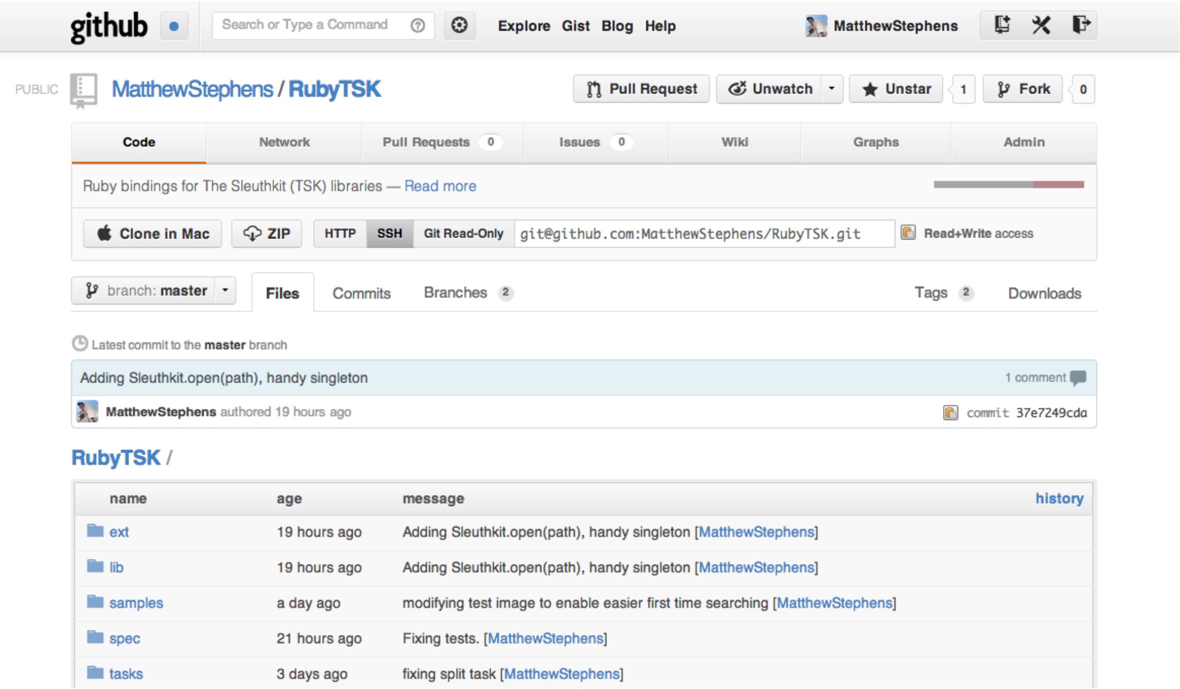
Road Map

- Flesh out API at file system layer
- Wrap higher-level functions
- FFI (libffi)
- More Ruby, less C
- Testing on many platforms & ruby versions

Development Tools

- Rake
- Bundler & rvm
- Rspec, ruby-debug
- https://github.com/MatthewStephens/RubyTSK

Development Repo



MatthewStephens / RubyTSK

Ruby bindings for The Sleuthkit (TSK) libraries — Read more

git@github.com:MatthewStephens/RubyTSK.git

Latest commit to the **master** branch

Adding Sleuthkit.open(path), handy singleton — 1 comment

MatthewStephens authored 19 hours ago — commit 37e7249cda

RubyTSK /

name	age	message	history
ext	19 hours ago	Adding Sleuthkit.open(path), handy singleton [MatthewStephens]	
lib	19 hours ago	Adding Sleuthkit.open(path), handy singleton [MatthewStephens]	
samples	a day ago	modifying test image to enable easier first time searching [MatthewStephens]	
spec	21 hours ago	Fixing tests. [MatthewStephens]	
tasks	3 days ago	fixing split task [MatthewStephens]	

Come Visit!
(excuse the mess)

- Git: https://github.com/MatthewStephens/RubyTSK
- Twitter: @beesharp4
- Email: matthew.stephens@virginia.edu

Thanks very much!