

00001160	8d eb 6b 46 bf e2 2b 0e	13 f5 5e 93 85 9c 1f da	.kF.+...x...	00001160	30 00 41 28 00 00 00 61	65 61 62 69 00 01 1e 00	0.A(...seabi...
00001170	5e 83 e8 1b c3 cc d2 86	78 13 07 1e 4b f4 63 c7	N...x...M.c.	00001160	00 00 05 35 54 45 00 06	04 08 01 09 01 12 04 14	...5TE...
00001180	99 b1 90 b6 9e 46 89 d0	33 4f ad 0c 1b aa 0e 85	a...FY.30...	00001170	01 15 01 17 03 18 01 19	01 1a 02 00 2e 73 68 73	tntab...interp...h
00001190	61 08 a1 9e 99 5e d9 19	7c 81 ba 54 55 05 92 8d	/S...v...	00001180	74 72 74 61 62 00 2e 69	64 74 65 72 70 00 2e 68	tash...dynsym...dyn
000011a0	fb 21 24 c2 b9 26 0d 02	22 9a 8a aa 76 2e 1c 8f	...?..nT7M.Kv6..	00001190	61 73 68 00 2e 64 79 6e	73 79 6d 00 2e 64 79 6e	str...rel.plt...tel
000011b0	b4 03 1d 7d 12 3f 0f 6e	54 37 57 c6 4b 76 36 cf	...[G...U.c...Ew	000011a0	73 74 72 00 2e 72 65 6c	2e 70 6c 74 20 7e 74 65	xt...rodatab...prei
000011c0	8d 45 94 9f 47 4b be da	55 c7 63 c0 99 ce 45 77	...[C8...P...Do	000011b0	78 74 00 2e 72 6f 64 61	74 61 00 2e 70 72 65 69	nit...array...init
000011d0	43 38 f7 2e 50 89 c0 92	1 f f2 ae af af 96 44 4f	...[.af..B...jD.T...	000011c0	6e 69 74 5f 61 72 72 61	71 79 00 2e 69 6e 69 74 5f	ash...ctors...dynami
000011e0	49 96 c2 61 66 c6 40 e8	Fe 6a 4a 2c 54 88 87 d8	...[...F...sl...g...S...	000011d0	61 72 72 61 79 00 2e 66	69 6e 69 5f 61 72 72 61	ment...ARM.attrib
000011f0	17 aa c1 92 7e 9b 4c f8	05 67 19 53 0c 06 0f	...[...Bu...C...	000011e0	79 00 2e 63 74 6f 72 73	00 2e 64 79 6e 61 6d 69	utes...
00001200	cf b4 0d 33 46 8e da 7d	49 0d 05 ef 9e 9e fc 0c	...[gk...p.j...	00001200	63 00 2e 67 6f 74 00 2e	62 73 73 00 2e 63 6f 69	...5TE...
00001210	a3 93 e5 b5 38 75 9e f0	22 43 7f 5c f8 da 12 b6	v)<R...Z...:x	00001210	6d 65 6e 74 00 2e 41 52	4d 2e 61 74 74 72 69 62	...
00001220	de 67 3b 6b 02 b3 70 4a	90 18 04 86 03 20 01 1e	6B.Z...35...	00001220	75 74 65 73 00 00 00 00	00 00 00 00 00 00 00 00	...
*					00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00001240	76 29 3c 26 e6 ee 85 32	02 11 35 4f a4 1f 3a 78	...[...D...l...g...S...	00001240	0b 00 00 00 01 01 00 00	02 00 00 00 d4 80 00 00	...
00001250	36 42 f1 5a 24 86 1f 9e	33 e5 ff 82 b3 06 d5 2e	...[...F...l...g...S...	00001250	04 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00001260	ea b6 f6 20 c4 b2 44 8d	1f 90 c0 f4 a8 d2 2f 7f	...[...Kp...K.X...	00001260	04 00 00 00 13 00 00 00	00 00 00 00 00 00 00 00	...
00001270	1e 89 92 ef c5 25 70 ff	9d d6 fb 4b a9 58 c4 b2	...[...M.p...S...	00001270	01 00 00 00 00 00 00 00	13 00 00 00 05 00 00 00	...
00001280	03 27 d1 a5 8f 57 d3 70	b2 88 d5 5e 5e 00 39 b4	...[...U...S...	00001280	02 00 00 e8 80 00 00 00	e8 00 00 cc 00 00 00 00	...
00001290	f4 57 3a 13 8c 8c 8c 8c	8c 8c 8c 8c 8c 8c 8c 8c	...[...f...q...n...	00001290	00 00 00 00 00 00 00 00	04 00 00 00 00 00 00 00	...
000012a0	df 9e 38 84	7c 7c 7c 7c 7c 7c 7c 7c	...[...g...V...	000012a0	29 00 00 09 00 00 00 00	02 00 00 bc 84 00 00 00	...
000012b0	f5 0a 83 b4	8c 8c 8c 8c 8c 8c 8c 8c	...[...X...J...+...g...	000012b0	04 00 00 98 00 00 00 00	03 00 00 06 00 00 00 00	...
000012c0	c0 24 e7 68 23 75 83 83	1e 8a e2 ad c5 17 ac 56	...[...F...T...E...	000012c0	00 00 00 00 00 00 00 00	07 00 00 00 00 00 00 00	...
000012d0	1a 17 83 0e b6 9c 17 0c	84 ad 3c 2d 03 ff 1a 82	...[...U...n...X...w...	000012d0	06 00 00 00 54 85 00 00	54 05 00 00 f8 00 00 00	...
000012e0	f1 e9 f9 c f b e 2e a5	66 97 71 99 d4 6e c3 88	...[...kmu...K.L.f.y...	000012e0	00 00 00 00 00 00 00 00	04 00 00 04 00 00 00 00	...
000012f0	8b 3a b4 33 88 67 8a 84	af ab f8 14 56 1d 40 82	...[...Hq...h...	000012f0	00 00 00 00 00 00 00 00	06 00 00 00 50 86 00 00	...
00001300	ef 28 bf 3c 8d c1 a0 08	b7 be 8b fd a2 86 96 73	...[...I...*...Y...J...	00001300	32 00 00 00 38 89 00 00	38 09 00 00 01 02 00 00	...
00001310	e2 c3 87 58 0f 9a 9c 81	07 f9 4a b5 94 92 2b 67	...[...I...G...p...	00001310	00 00 00 00 00 00 00 00	04 00 00 00 01 00 00 00	...
00001320	04 b7 46 ae af 9a 17 0d	47 09 ed 97 d5 95 1e cf	...[...H...k...G...A...C	00001320	40 00 00 10 00 00 00 00	03 00 00 00 00 90 00 00	...
00001330	e2 74 73 f4 0a 33 ca c2	4e 10 65 bd b2 09 d2 25	...[...I...G...p...	00001330	00 10 00 00 08 00 00 00	00 00 00 00 00 00 00 00	...
00001340	64 1b ec dd b8 ab 1e 12	50 a3 a4 65 17 86 15 63	...[...U...n...X...w...	00001340	01 00 00 00 00 00 00 00	4f 00 00 00 0e 00 00 00	...
00001350	8f 59 1b 80 4a c7 d8 69	bb 41 48 d2 e8 63 6b 8a	...[...kmu...K.L.f.y...	00001350	03 00 00 00 08 90 00 00	08 10 00 00 08 00 00 00	...
00001360	85 a7 1c 32 55 24 de d1	e2 84 cc b9 1e 7d 91 de	...[...Hq...h...	00001360	00 00 00 00 00 00 00 00	01 00 00 00 00 00 00 00	...
00001370	a5 55 9f 5e 00 9a c8 3e	89 64 21 61 62 f6 de d6	...[...I...G...p...	00001370	5b 00 00 00 0f 00 00 00	03 00 00 00 10 90 00 00	...
00001380	df 6f cf 51 ee 1d 9b c8	32 15 2b 09 42 c5 53 91	...[...H...k...G...A...C	00001380	10 10 00 00 08 00 00 00	00 00 00 00 00 00 00 00	...
00001390	01 09 2a c2 9e 1e 89 93	55 99 e5 cf 18 7d 20 29	...[...I...G...p...	00001390	04 00 00 00 00 00 00 00	07 00 00 00 01 00 00 00	...
000013a0	4b 06 1c d8 cb f2 7f 66	54 aa a3 84 91 45 7f 95	...[...I...G...p...	000013a0	00 10 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
000013b0	5e 1f 5a f6 fc fb 05 60	fd d5 6f 4f 6e cb 1a fe	...[...H...k...G...A...C	000013b0	01 00 00 00 00 00 00 00	4f 00 00 00 0e 00 00 00	...
000013c0	1a 17 83 0e b6 9c 17 0c	84 ad 3c 2d 03 ff 1a 82	...[...I...G...p...	000013c0	03 00 00 00 08 90 00 00	08 10 00 00 08 00 00 00	...
000013d0	93 e2 77 ca 55 ed 0a b5	6e 40 58 08 bf 09 77 8b	...[...U...n...X...w...	000013d0	00 00 00 00 00 00 00 00	01 00 00 00 00 00 00 00	...
000013e0	ex dd 6b 67 77 27 1e da	2e 4f 4c b5 66 95 79 b6	...[...kmu...K.L.f.y...	000013e0	00 00 00 00 00 00 00 00	03 00 00 00 10 90 00 00	...
000013f0	0e 3a 48 71 28 81 d6 11	74 48 5e a1 f3 ea e9 27	...[...Hq...h...	000013f0	10 10 00 00 08 00 00 00	00 00 00 00 00 00 00 00	...
00001400	6d 8e 44 52 e4 bb c4 42	85 ba 9e c7 68 6e 6e 6e	...[...I...G...p...	00001400	04 00 00 00 00 00 00 00	07 00 00 00 01 00 00 00	...
00001410	3a 17 83 0e b6 9c 17 0c	84 ad 3c 2d 03 ff 1a 82	...[...H...k...G...A...C	00001410	00 00 00 00 00 00 00 00	18 10 00 00 08 00 00 00	...
00001420	ff c9 33 80 73 3b 30 33	ce bc 0c 0c 0c 67 da 4c	...[...I...G...p...	00001420	00 00 00 00 00 00 00 00	01 00 00 00 00 00 00 00	...
00001430	da 21 47 c5 af 03 2e e0	8a 2e 8c 91 70 48 db da	...[...H...k...G...A...C	00001430	06 00 00 00 06 00 00 00	03 00 00 00 20 90 00 00	...
00001440	48 f9 9e 18 d8 e8 26 b9	f7 aa 0e 47 01 5c d2 43	...[...I...G...p...	00001440	20 10 00 00 c8 00 00 00	04 00 00 00 00 00 00 00	...
00001450	fd 57 0f ca ee cc c3 df	b2 59 95 15 31 55 0d 51	...[...U...n...X...w...	00001450	04 00 00 00 08 00 00 00	77 00 00 00 01 00 00 00	...
00001460	04 b7 46 ae af 9a 17 0d	47 09 ed 97 d5 95 1e cf	...[...Hq...h...	00001460	03 00 00 00 e8 90 00 00	e8 10 00 00 58 00 00 00	...
00001470	4c 8d 75 fc 6c 36 f7	99 66 a5 ad 66 8e e1 8d	...[...I...G...p...	00001470	00 00 00 00 00 00 00 00	04 00 00 00 04 00 00 00	...

# Dalvik Executable (DEX) Trick: Hidex

Axelle Aprille

Insomni'Hack March 2014



## whoami

```
#!/usr/bin/perl -w # recently converting to Python!  
my $self = {  
    realname => 'Axelle Apvrille',  
    nickname => 'Crypto Girl',  
    twitter => '@cryptax',  
    job => 'Malware Analyst and Researcher',  
    focus => 'Misc malware = mobile, Internet of Things...',  
    title => 'Senior', # white hair  
    company => 'Fortinet, FortiGuard Labs',  
    before => 'Security software eng.: protocols, crypto...',  
    languages => 'French, English, Hexadecimal :)'  
};
```

# Quick Android background

## Android mobile phone

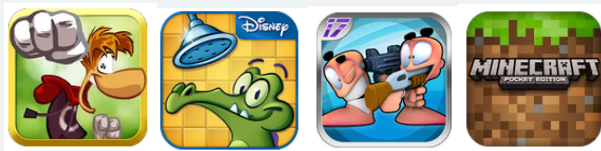


# Quick Android background

Android mobile phone



Applications: APK

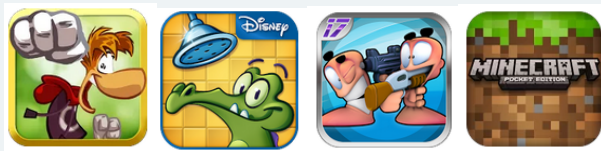


# Quick Android background

## Android mobile phone



## Applications: APK



## Inside the APK: DEX

Dalvik Executable with Dalvik bytecode

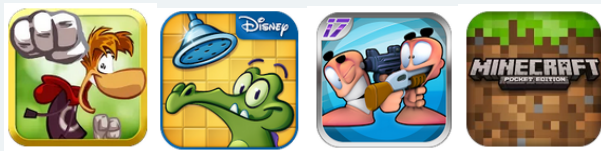
```
dex.035.V..d..$g
```

# Quick Android background

## Android mobile phone



## Applications: APK



### Inside the APK: DEX

Dalvik Executable with Dalvik bytecode

```
dex.035.V..d..$g
```

### Inside the DEX

Classes, methods, fields, strings

```
'bytes', '** I am Mr Hyde **', '<init>'...
```



### Goal

1. Write an app
2. Hide a given *method* of the app to disassemblers



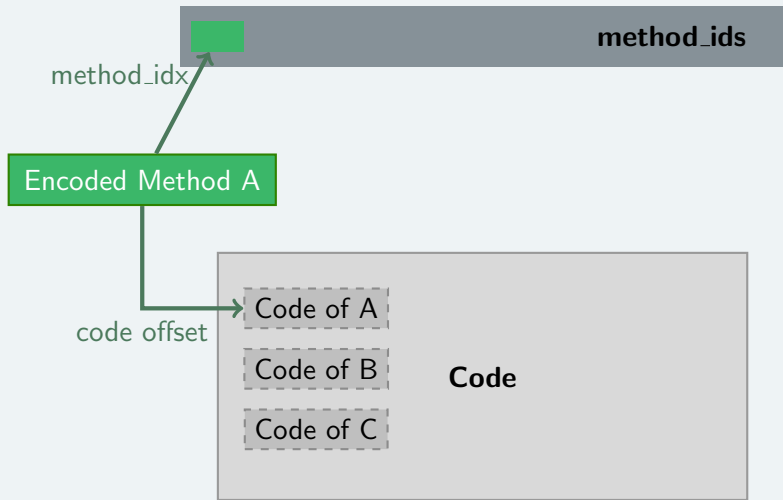
## Goal

1. Write an app
2. Hide a given *method* of the app to disassemblers

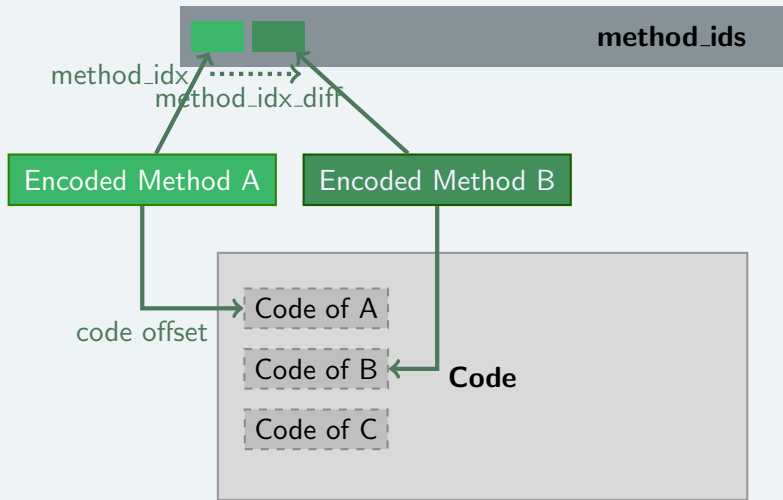
## Demo - source code:

<https://github.com/cryptax/dextools>

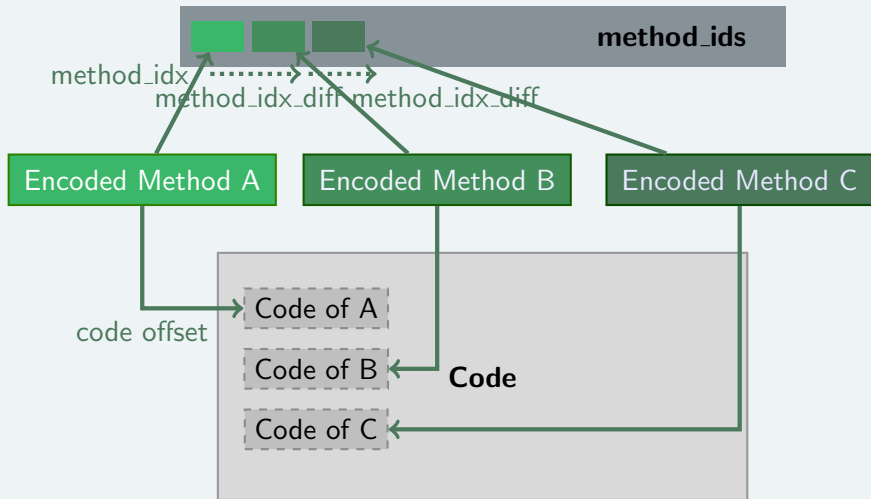
1. Example method **thisishidden()**:
  - ▶ Logs "In thisishidden(): set mrhyde=" etc
  - ▶ Accesses file "identity" in app dir
  - ▶ Exact prototype: `public void thisishidden(boolean ismrhyde)`
2. Hide **thisishidden()**: Baksmali, dex2jar, Androguard, JEB, IDA Pro do not see it!
3. Back: reveal **thisishidden()**



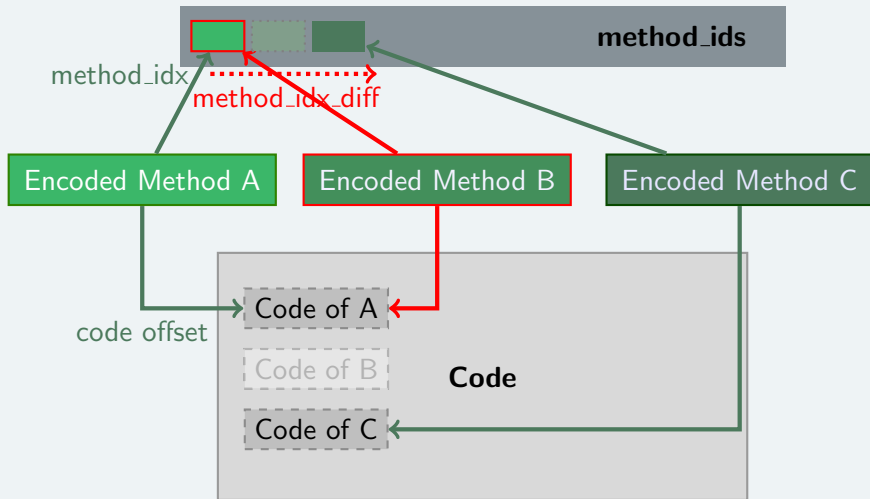
# How it works / inside class\_data items



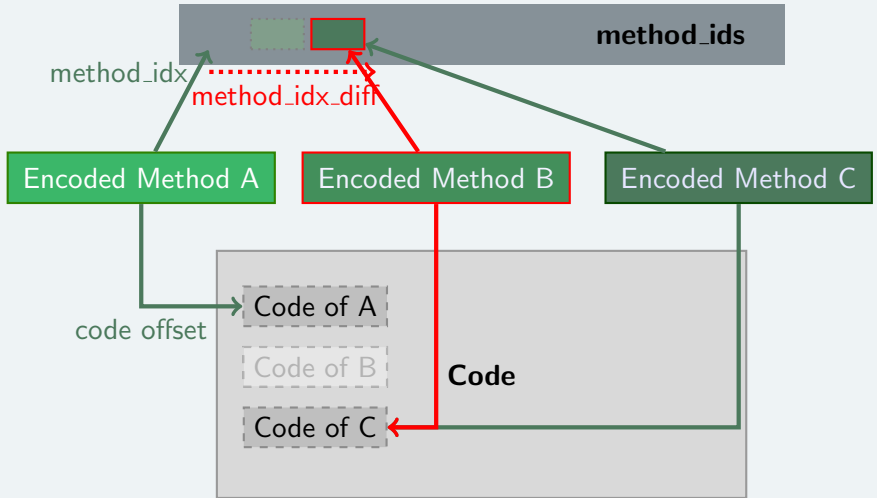
# How it works / inside class\_data items



# How it works / inside class\_data items



# How it works / inside class\_data items



## Access flags

You *may* modify it

but must remain with the same category of methods:

- ▶ direct methods: static, private, constructors
- ▶ virtual methods: others ;)

## Single method to hide?

In `class_data_item`, set `direct_methods_size` (or `virtual_methods_size`)

+ nullify `encoded_method`

3980h:	81 80 04 80 23 05 01 06 00 10 1A 01 0A 01 0A 02	.e.e#.....
3990h:	1A 01 09 13 02 1C 88 80 04 98 23 01 81 80 04 A4	.....^e."#..e.x
39A0h:	3C 01 00 00 00 00 00 00 00 00 00 00 00 00 00	<..à<...>..È>..
39B0h:	31 00 00 00 00 00 00 00 00 00 00 00 00 00 00	?.....
39C0h:	01 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....ö...

## Build a valid DEX

- ▶ Compute the SHA-1 of the new DEX → Write to header
- ▶ Compute the checksum of the new DEX → Write to header
- ▶ hidex or dexrehash in  
<https://github.com/cryptax/dextools>

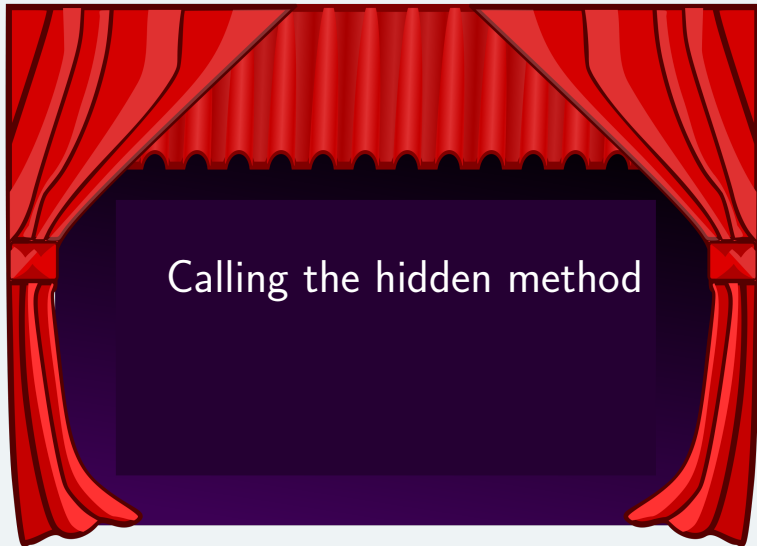
## Re-package: easy

- ▶ In original APK, replace DEX with new one
- ▶ Zip, sign package (jarsigner)

## Did you know?

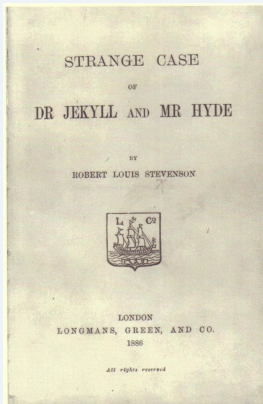
You can write a .dex 'manually' using Yasm - thanks @angealbertini  
Hello World: 695 bytes





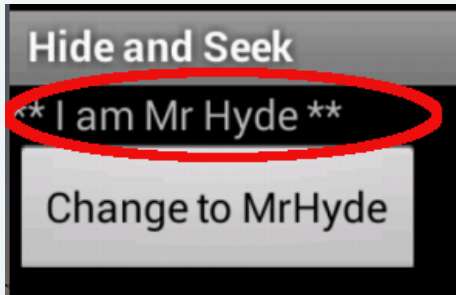
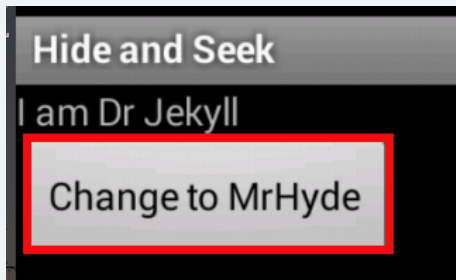
### calling `this.isHidden()`

- ▶ The method is hidden to disassemblers
- ▶ ... but it can be run!



### The strange case of Dr Jekyll and Mr Hyde – R. Stevenson

- ▶ Split personalities: Dr Jekyll or Mr Hyde
- ▶ Only one way to change into MrHyde: call `this.isHidden()`
- ▶ Current personality displayed in main activity

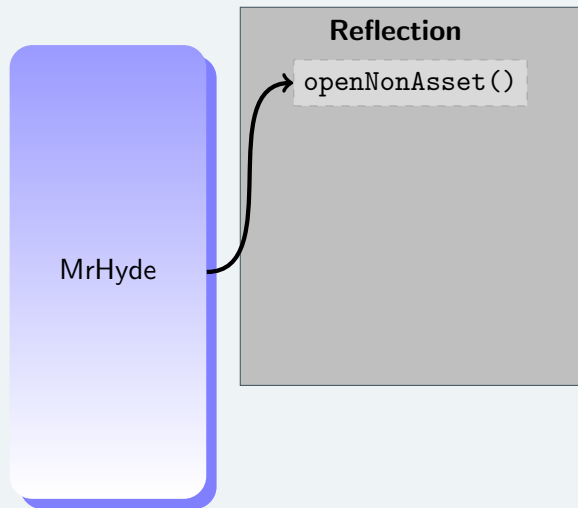


```
I/HideAndSeek( 851): invoking thisishidden() with arg=true
I/HideAndSeek( 851): In thisishidden(): set mrhyde=true
I/HideAndSeek( 851): thisishidden(): context=android.app.Applic
I/HideAndSeek( 851): thisishidden(): dir=/data/data/com.fortigu
I/HideAndSeek( 851): thisishidden(): file: /data/data/com.forti
I/HideAndSeek( 851): thisishidden(): done
```

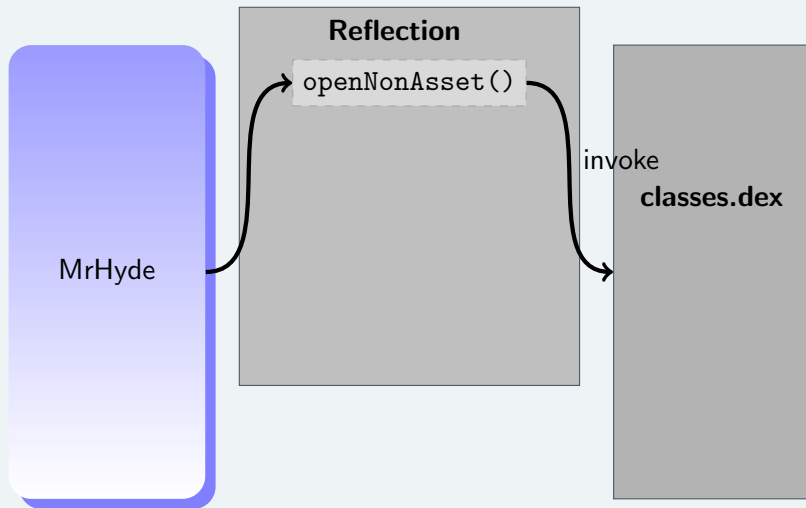
Implementation... technical but illustrated ;)



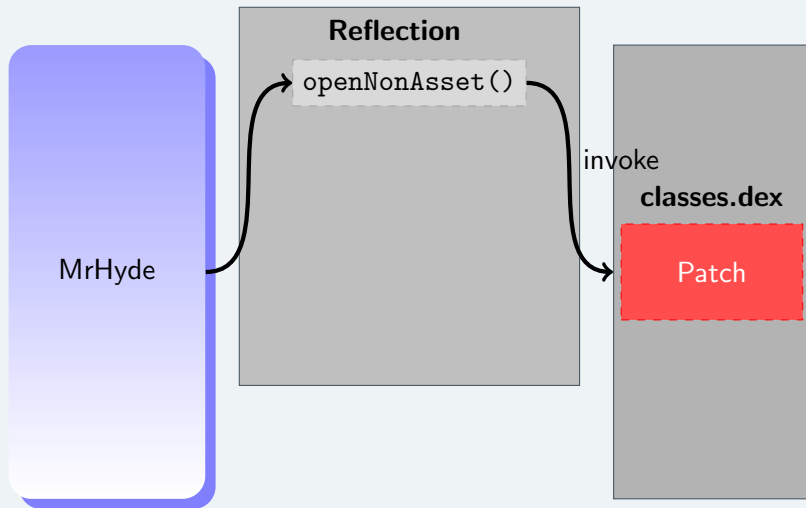
MrHyde



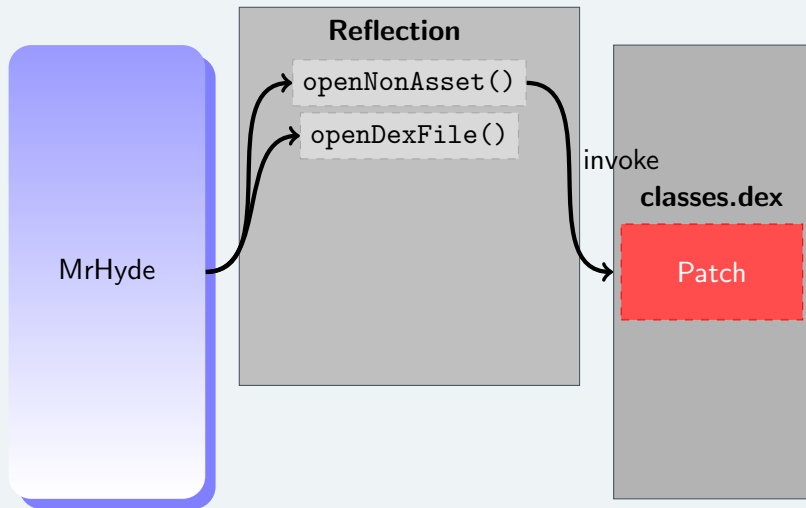
# Implementation... technical but illustrated ;)



# Implementation... technical but illustrated ;)

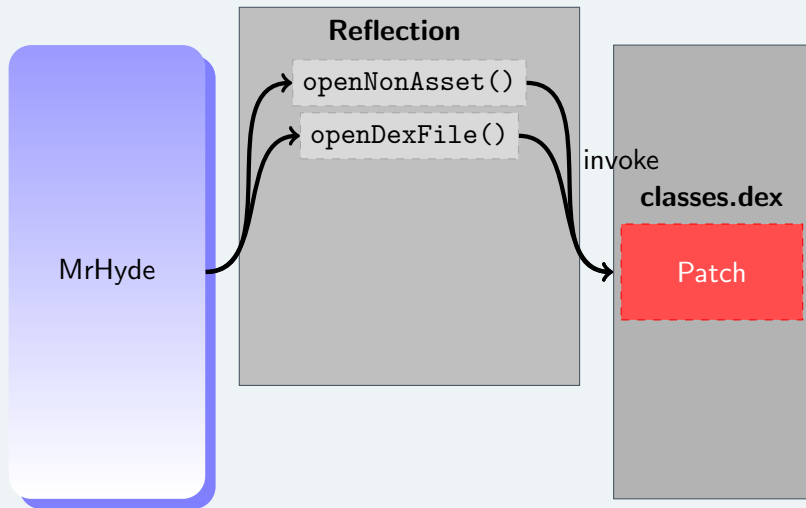


# Implementation... technical but illustrated ;)

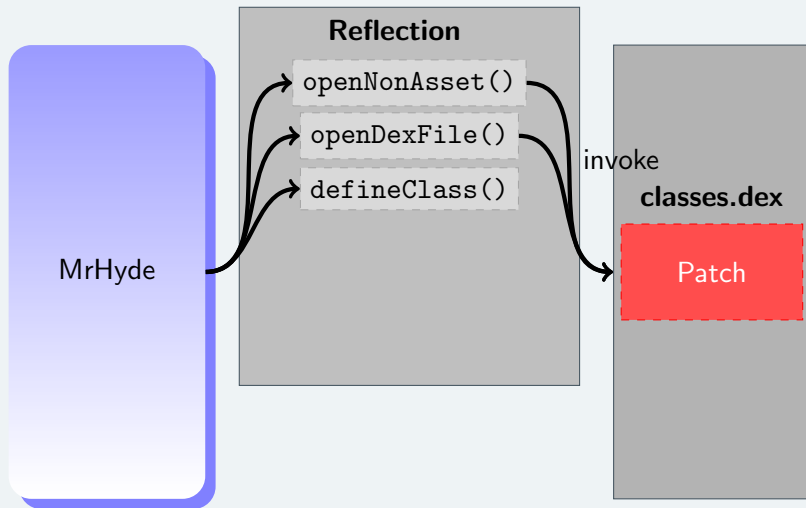




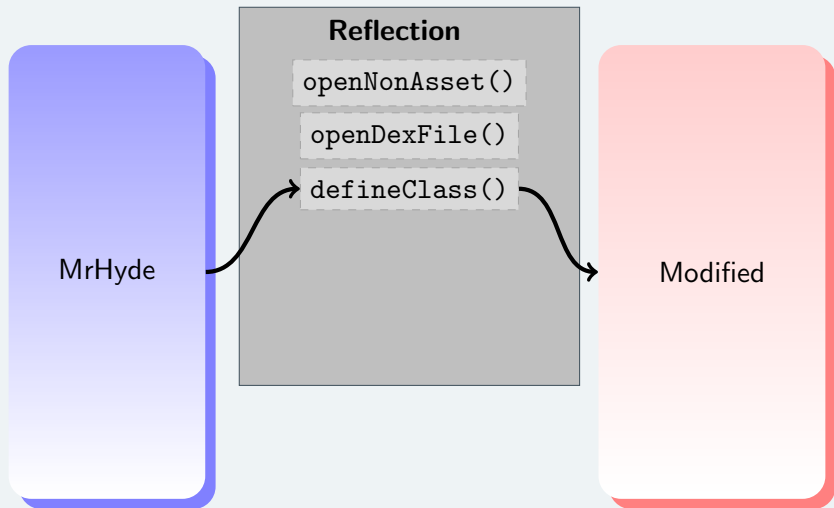
# Implementation... technical but illustrated ;)

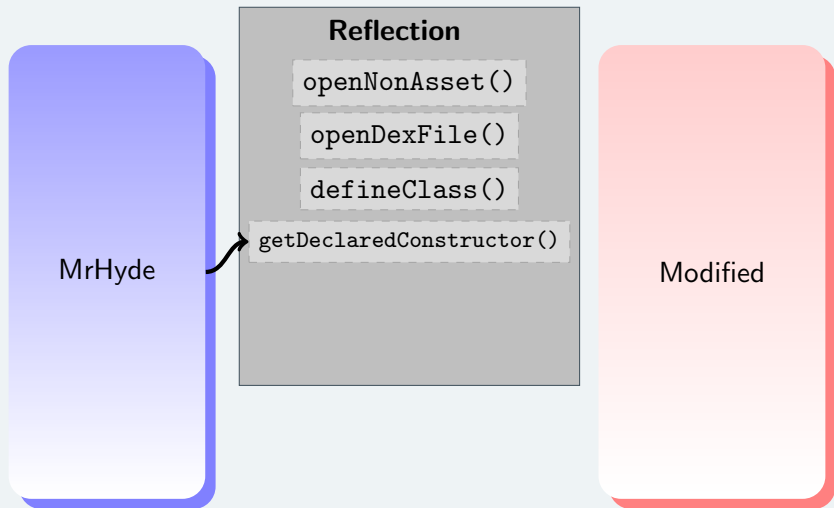


# Implementation... technical but illustrated ;)

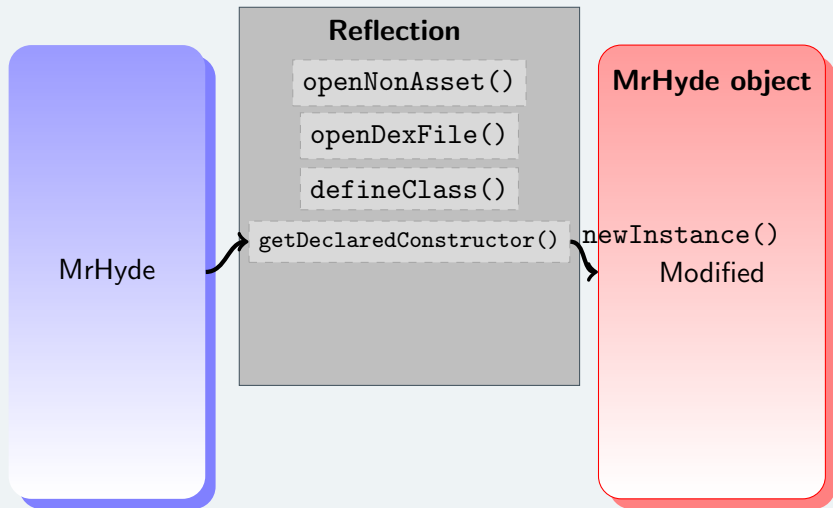


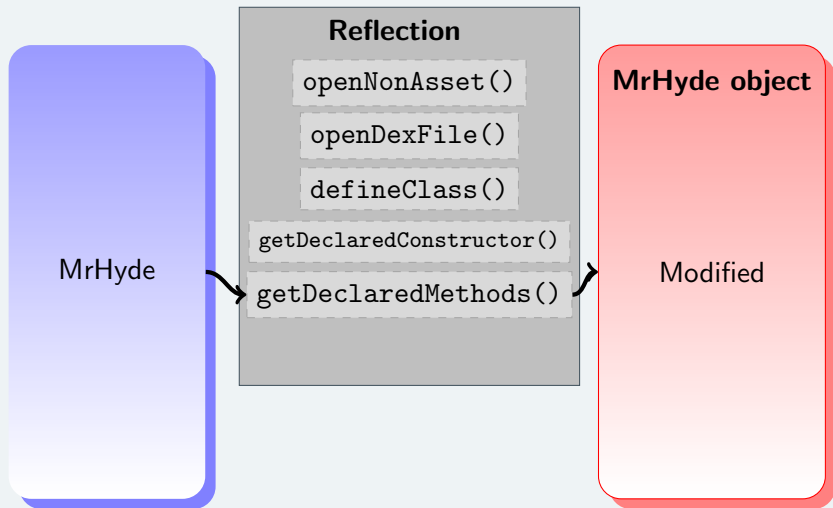
# Implementation... technical but illustrated ;)

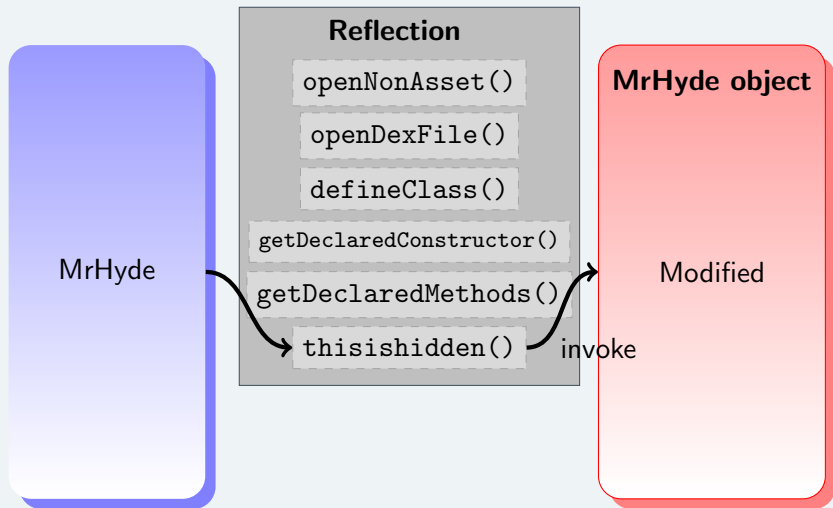


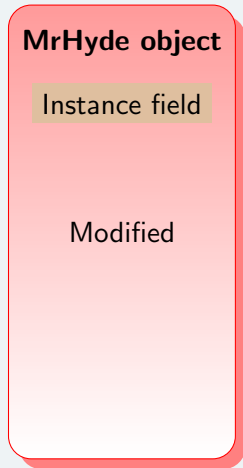
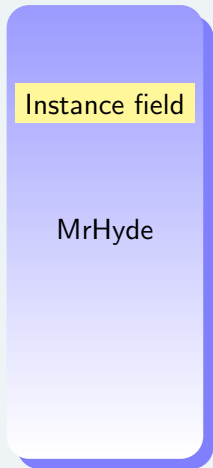


# Implementation... technical but illustrated ;)



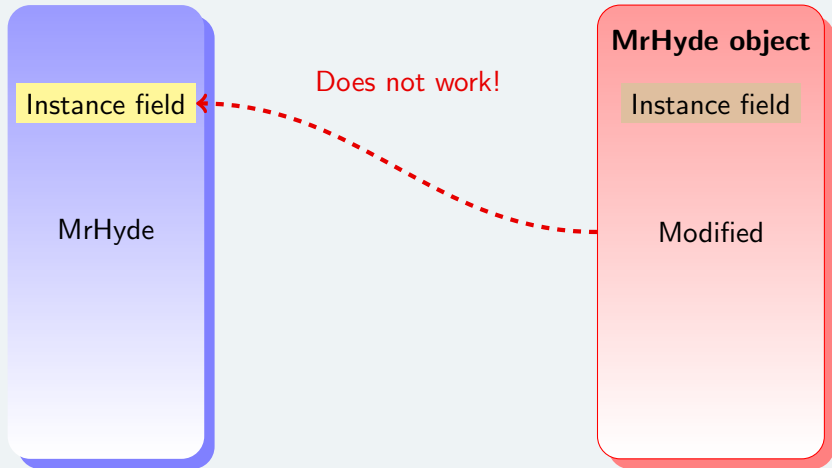




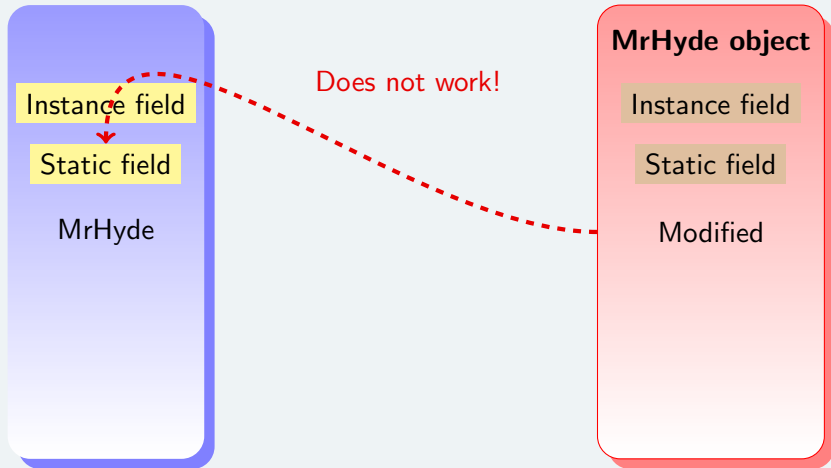




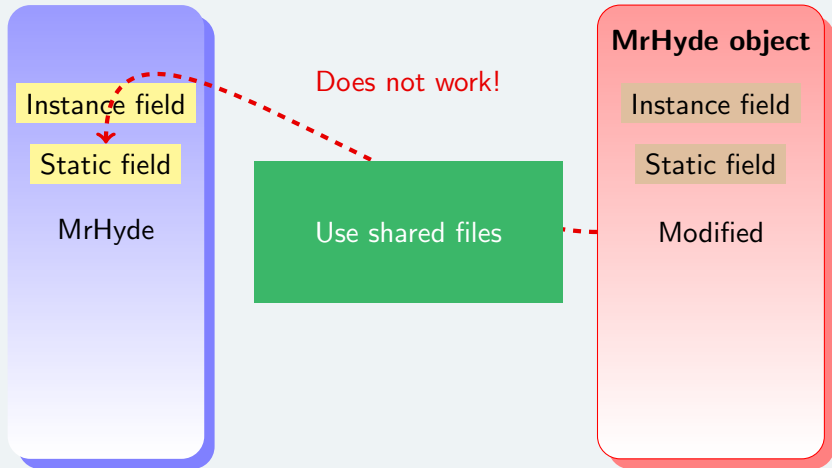
# Implementation... technical but illustrated ;)



# Implementation... technical but illustrated ;)



# Implementation... technical but illustrated ;)





It works :)

- ▶ Dex manipulation: working on all versions
- ▶ Calling hidden method: < 4.4.2.  
Prototypes for `openDexFile` and `defineClass` changed
  - ▶ minor modif for `defineClass`
  - ▶ `openDexFile` no longer works on `byte[]`

**Work in progress: looks feasible.**

- ▶ Android Security Team notified in June 2013

# Detecting hidden methods

How? Use '--detect' option in hidex.pl

```
$ ./hidex.pl --input classes.dex | grep -B 1 "WARNING"  
$ ./nonreferenced-methods.sh classes.dex
```

- ▶ null code offset: just a hint
- ▶ null or negative method\_idx\_diff
- ▶ code offset or method\_id already referenced
- ▶ method\_id never referenced: beware, there are valid methods not implemented in the DEX.

Something is wrong with openNonAsset()

```
Class: Lcom../MrHyde; Method: openNonAsset Position: 0x2C99  
WARNING: Code offset 0x13D8 ALREADY REFERENCED  
Class: Lcom../MrHyde; Method: openNonAsset Position: 0x2C99  
WARNING: method_idx_diff <= 0 detected  
Class: Lcom../MrHyde; Method: openNonAsset Position: 0x2C99  
WARNING: METHOD_IDX 22 ALREADY REFERENCED
```

# Non Referenced Methods Detection results

```
Method Landroid/annotation/SuppressLint;->value is never used  
Method Landroid/annotation/TargetApi;->value is never used
```

→ abstract methods indeed never used.

```
Method Lcom/fortiguard/hideandseek/MrHyde;->thisishidden is never used
```

→ hidden method!

```
Method Ljava/io/File;->delete is never used  
Method Ljava/io/File;->exists is never used  
Method Ljava/io/FileOutputStream;-><init> is never used  
Method Ljava/io/FileOutputStream;->close is never used  
Method Ljava/io/FileOutputStream;->write is never used  
Method Ljava/lang/Object;->toString is never used
```

→ methods used only by the hidden method!

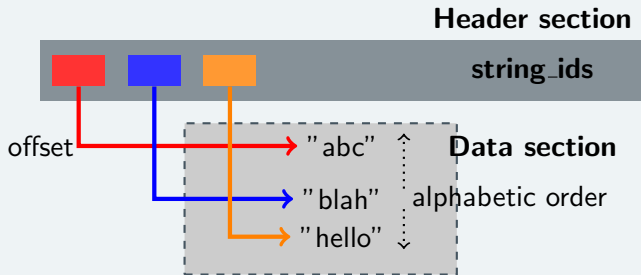
## Fixing

- ▶ Implement `method_idx_diff` check?
- ▶ Implement code or `method_id` duplicate references check?

## Working around

- ▶ Unpatch the DEX: `hidex.pl`
- ▶ Disassemble bytecode at a given location: `androdis.py`

# How about hiding strings?



- ▶ **No idx\_diff.** No chaining.
- ▶ **String as byte []** → not in strings list but visible in hex (e.g strings Unix command)
- ▶ **Encode, encrypt, obfuscate string** → possible - nothing new.



# Thank You !

Where's the source code?

<https://github.com/cryptax/dextools>

FortiGuard Labs

Follow us on twitter: **@FortiGuardLabs**

or on our blog <http://blog.fortinet.com>

Me: **@cryptax** or aapvrille at fortinet dot com

Useless/shameless/stupid speaker challenge

I told @angealbertini I could keep it under 20 slides ;)



Are those PowerPoint slides? No way! It's L<sup>A</sup>T<sub>E</sub>X + TikZ + Beamer + [Lobster](#)