

00001160	8d eb 6b 46 bf e2 2b 0e	13 f5 5e 93 85 9c 1f da	00001180	30 00 41 28 00 00 00 61	65 61 62 69 00 01 1e 00	l0.A(. . .seabi.
00001170	83 c3 e8 1e 16 46 89 d4	79 13 07 1e 4d f4 63 c7	00001190	00 00 05 35 54 45 00 06	04 08 01 09 01 12 04 14	[.5TE.
00001180	99 b1 90 61 96 46 89 d4	33 4f 07 0c 1b aa 0e 85	00001200	01 15 01 17 03 18 01 19	01 1a 02 00 2e 73 68 73	[.ash.
00001190	61 08 a1 9e 99 5e d9 19	fc 81 ba 54 55 05 92 8d	00001210	74 72 74 61 62 00 2e 69	64 75 64 75 70 00 2e 68	[.tntab.
000011a0	fb 21 24 c2 b9 26 0d 02	22 9a 8e aa 76 2e 1c 8f	00001220	61 73 68 00 2e 64 79 6e	73 79 6d 00 2e 64 79 6e	[.lstr.
000011b0	b4 03 1d 7d 12 3f 0f 6e	54 37 57 c6 4b 76 36 cf	00001230	73 74 72 00 2e 72 65 6c	2e 70 6c 74 00 2e 74 65	[.lstr.
000011c0	8d 45 94 9f 47 4b be da	55 c7 63 c0 99 ce 45 77	00001240	78 74 00 2e 72 6f 64 61	74 61 00 2e 70 72 65 69	[.lstr.
000011d0	43 38 ff 2e 50 89 c0 92	1 f2 e a4 af 96 44 4f 8f	00001250	6e 69 74 5f 61 72 72 61	79 00 2e 69 6e 69 74 5f	[.lstr.
000011e0	49 96 61 61 66 c6 40 e8	Fe 6a 44 2c 54 af 87 d8 6f	00001260	61 72 72 61 79 00 2e 66	69 6e 69 5f 61 72 72 61	[.lstr.
000011f0	17 aa c1 92 7e 9b 4c f8	05 67 19 f3 0c 06 0f	00001270	79 00 2e 63 74 6f 72 73	00 2e 64 79 6e 61 6d 69	[.lstr.
00001200	cf b4 0d 33 46 8e da 73	49 0d 05 ef 9d 9e fc 0c	00001280	83 00 2e 67 6f 74 00 2e	62 73 73 00 2e 63 6f 69	[.lstr.
00001210	a3 93 e5 b5 38 79 96 f0	22 43 7f 5c f8 da 12 b6	00001290	6d 65 6e 74 00 2e 41 52	4d 2e 61 74 74 72 69 62	[.lstr.
00001220	de 67 3b 6b 02 b3 70 4a	90 18 04 86 03 20 01 1e	00001300	75 74 65 73 00 00 00 00	00 00 00 00 00 00 00 00	[.lstr.
00001230	76 29 3c 26 e6 ee 85 32	02 11 35 a4 a4 1f 3a 78	00001310	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	[.lstr.
00001240	36 42 f1 5a 24 86 1f 9e	33 c5 5f 82 b3 06 d5 2e	00001320	0b 00 00 00 01 00 00 00	02 00 00 00 d4 80 0e 00	[.lstr.
00001250	ea b6 f6 20 c4 b2 44 8d	1f 90 c0 f4 a8 02 2f 8f	00001330	04 00 00 00 13 00 00 00	00 00 00 00 00 00 00 00	[.lstr.
00001260	1e 89 92 ef c5 25 25 25	9d 0d 05 ef 9d 9e fc 0c	00001340	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	[.lstr.
00001270	03 27 d1 a5 8f 57 57 57	9d 0d 05 ef 9d 9e fc 0c	00001350	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	[.lstr.
00001280	f4 57 3a 13 6d 1f 8f	9d 0d 05 ef 9d 9e fc 0c	00001360	19 00 00 00 0b 00 00 00	02 00 00 00 b4 81 00 00	[.lstr.
00001290	df 9e 38 04 9c fc 2c 73	42 73 42 62 c2 39 72	00001370	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	[.lstr.
000012a0	f5 0a 83 b4 3a b5 de 83	68 32 4d 50 c3 b6 9a de	00001380	b4 01 00 00 02 00 00 04	04 00 00 00 01 00 00 00	[.lstr.
000012b0	0c 24 e7 68 23 75 83 83	1e 8a e2 ad c5 17 ac 56	00001390	04 00 00 00 10 00 00 00	21 00 00 00 03 00 00 00	[.lstr.
000012c0	1a 17 83 0e b6 9c 17 0c	84 ad 3c 2d 03 ff 1a 82	00001400	00 00 00 b4 83 00 00 00	b4 03 00 00 05 01 00 00	[.lstr.
000012d0	f1 e9 f9 c9 fb e6 2e a5	66 97 71 99 f4 6e c3 88	00001410	00 00 00 00 00 00 00 00	01 00 00 00 00 00 00 00	[.lstr.
000012e0	8b 3a b4 33 8e 07 9a 81	af ab f8 14 56 1d 40 82	00001420	29 00 00 00 09 00 00 00	02 00 00 00 bc 84 00 00	[.lstr.
000012f0	ef 28 b7 3c 8d c1 a0 08	b7 be 8b fd a2 86 96 73	00001430	bc 04 00 00 98 00 00 00	03 00 00 00 06 00 00 00	[.lstr.
00001300	b2 c3 87 58 07 9a 9c 81	07 f9 4a 85 94 92 2b 67	00001440	04 00 00 00 08 00 00 00	20 00 00 00 01 00 00 00	[.lstr.
00001310	04 b7 46 ea ef 9a 17 04	47 09 ed 97 d5 95 1e cf	00001450	06 00 00 00 54 85 00 00	54 05 00 00 f8 00 00 00	[.lstr.
00001320	e2 74 73 f4 0a 33 ca c2	4e 10 65 bd b2 09 d2 25	00001460	00 00 00 00 00 00 00 04	04 00 00 00 04 00 00 00	[.lstr.
00001330	64 1b ec dd b8 ab 1e 12	50 a3 4a 65 17 86 15 63	00001470	32 00 00 00 01 00 00 00	06 00 00 00 50 86 00 00	[.lstr.
00001340	8f 59 1b 80 4a c7 d8 69	bb 41 48 e2 e8 63 6b 8a	00001480	50 06 00 00 e8 02 00 00	00 00 00 00 00 00 00 00	[.lstr.
00001350	85 a7 1c 32 55 24 de d1	e2 84 cc cb b9 1e 7d 91 de	00001490	00 00 00 00 00 00 00 00	38 00 00 00 01 00 00 00	[.lstr.
00001360	a5 55 9f 5e 0a 9a c8 3e	62 84 21 61 62 16 d6 d6	00001500	00 00 00 00 38 89 00 00	38 09 00 00 e0 02 00 00	[.lstr.
00001370	df 6f cf 51 ee 1d 9b c8	32 15 2b 09 42 c5 53 91	00001510	00 00 00 00 00 00 00 00	04 00 00 00 01 00 00 00	[.lstr.
00001380	01 09 2a c2 9e 1e 89 93	32 f9 e5 ef 16 7d 20 29	00001520	40 00 00 00 10 00 00 00	03 00 00 00 00 90 00 00	[.lstr.
00001390	4b 06 1c d8 cb f2 7f 66	54 aa a3 84 91 45 f7 95	00001530	00 10 00 00 08 00 00 00	00 00 00 00 00 00 00 00	[.lstr.
000013a0	5e 1f 5a f6 fc bd 05 60	fd d5 6f 4f 6e bc 1a fe	00001540	01 00 00 00 00 00 00 00	4f 00 00 00 0e 00 00 00	[.lstr.
000013b0	1a 17 83 0e b6 9c 17 0c	84 ad 3c 2d 03 ff 1a 82	00001550	03 00 00 00 08 90 00 00	08 10 00 00 08 00 00 00	[.lstr.
000013c0	93 ed 67 fc 55 ed 0a ba	6e 40 58 08 bf 09 77 8b	00001560	00 00 00 00 00 00 00 00	01 00 00 00 00 00 00 00	[.lstr.
000013d0	e1 dd 66 6d 77 27 1e d5	22 4f 4c b5 66 95 79 b6	00001570	5b 00 00 00 0f 00 00 00	03 00 00 00 10 90 00 00	[.lstr.
000013e0	0e 3a 48 71 28 81 d6 11	74 48 5e a1 f3 e4 e9 27	00001580	10 10 00 00 08 00 00 00	00 00 00 00 00 00 00 00	[.lstr.
000013f0	6d 8e 44 52 ea bb c4 42	aa 5a 9e cf 68 1e f5 ab	00001590	04 00 00 00 00 00 00 00	67 00 00 00 01 00 00 00	[.lstr.
00001400	3a 17 83 0e b6 9c 17 0c	84 ad 3c 2d 03 ff 1a 82	00001600	03 00 00 00 18 90 00 00	18 10 00 00 08 00 00 00	[.lstr.
00001410	ff c9 33 80 03 3b 30 33	ce bc 0c 0c 0c 0c d7 d7	00001610	00 00 00 00 00 00 00 00	01 00 00 00 00 00 00 00	[.lstr.
00001420	4d 21 47 c5 af 73 bd e0	8a 2e 8c 9c 10 c7 d8 d7	00001620	00 00 00 00 00 00 00 00	03 00 00 00 20 90 00 00	[.lstr.
00001430	48 f9 9e 18 d8 e8 26 b9	f7 aa 0e 47 01 5c d2 43	00001630	20 10 00 00 c8 00 00 00	04 00 00 00 00 00 00 00	[.lstr.
00001440	fd 57 0f ca ee cc c3 6f	d2 59 95 15 31 55 0d 51	00001640	04 00 00 00 08 00 00 00	77 00 00 00 01 00 00 00	[.lstr.
00001450	04 b7 46 ea ef ab 9a 17	4d 09 ed 97 d5 95 1e cf	00001650	03 00 00 00 e8 90 00 00	e8 10 00 00 58 00 00 00	[.lstr.
00001460	4c 8d 75 fc 6c 36 f7	d9 66 a5 ad 66 8b e1 8d	00001660	00 00 00 00 00 00 00 00	04 00 00 00 04 00 00 00	[.lstr.
00001470	a5 7b 93 a7 07 03 04 08	05 05 8d 8d b7 03 c8 0e	00001670	7e 00 00 00 08 00 00 00	03 00 00 00 00 00 00 00	[.lstr.

Playing Hide and Seek with Dalvik Executables

Axelle Aprille

Hack.Lu, October 2013



whoami

```
#!/usr/bin/perl -w
my $self = {
    realname => 'Axelle Apvrille',
    nickname => 'Crypto Girl',
    twitter => '@cryptax',
    job => 'Malware Analyst and Researcher',
    # reverse engineering of incoming mobile malware
    # research and tools in related areas
    title => 'Senior', # white hair
    company => 'Fortinet, FortiGuard Labs',
    before => 'Security software eng.: protocols, crypto...',
    languages => 'French, English, Hexadecimal :)'
};
```

Quick background

Android mobile phone

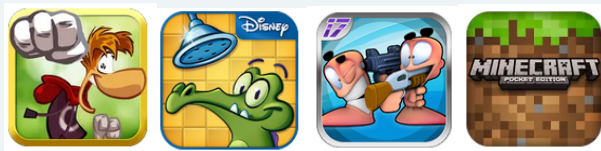


Quick background

Android mobile phone



Applications: APK

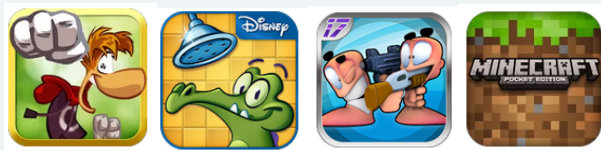


Quick background

Android mobile phone



Applications: APK



Inside the APK: DEX

Dalvik Executable with Dalvik bytecode

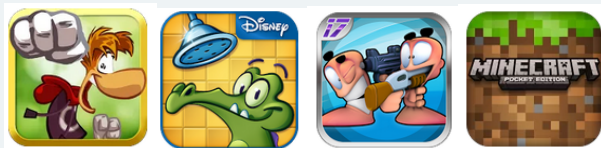
```
dex.035.V..d..$g
```

Quick 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

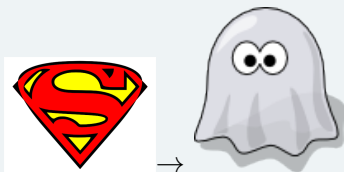
```
'bytes', '** I am Mr Hyde **', '<init>'...
```

Application source code

```
public void thisishidden(boolean ismrhyde) {
    Log.i("HideAndSeek",
        "In thisishidden(): set mrhyde="
        +ismrhyde);
    try {
        File dir;
        if (context !=null) {
            ...
        }
    }
}
```

Method thisishidden(): hidden to disassemblers

- ▶ Baksmali does not see it
- ▶ dex2jar does not see it
- ▶ IDA Pro does not see it
- ▶ Androguard does not see it



Demo

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



Demo

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

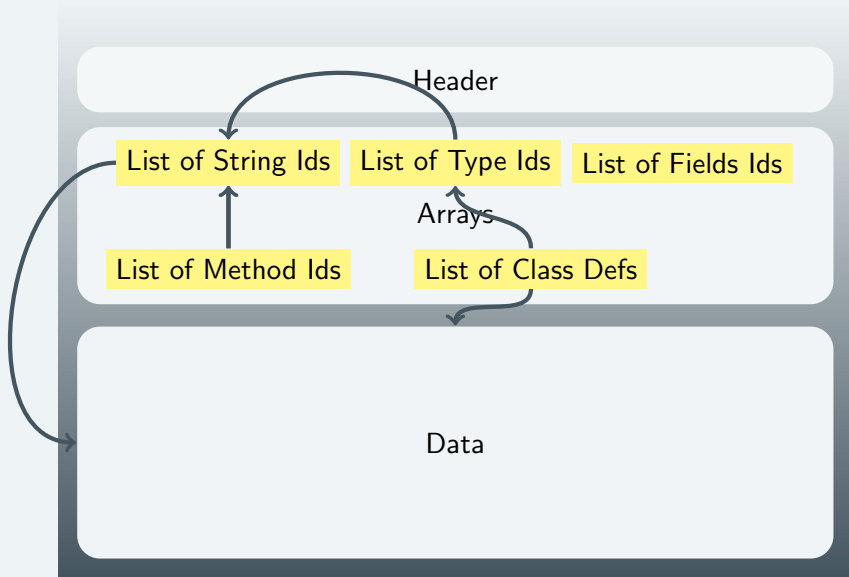
A diagram showing the structure of a DEX file. It consists of three stacked, rounded rectangular boxes. The top box is labeled 'Header', the middle box is labeled 'Arrays', and the bottom box is labeled 'Data'. The boxes are separated by thin horizontal lines and are contained within a larger, dark grey rounded rectangle.

Header

Arrays

Data

Format of a DEX file



encoded_method

- ▶ **access_flags:**
ACC_PUBLIC,
ACC_PRIVATE,
ACC_STATIC...
- ▶ **code_off:** offset to
code from
beginning of DEX
file
- ▶ **method_idx_diff:**
increment to
method indexes

Header

class_def_item

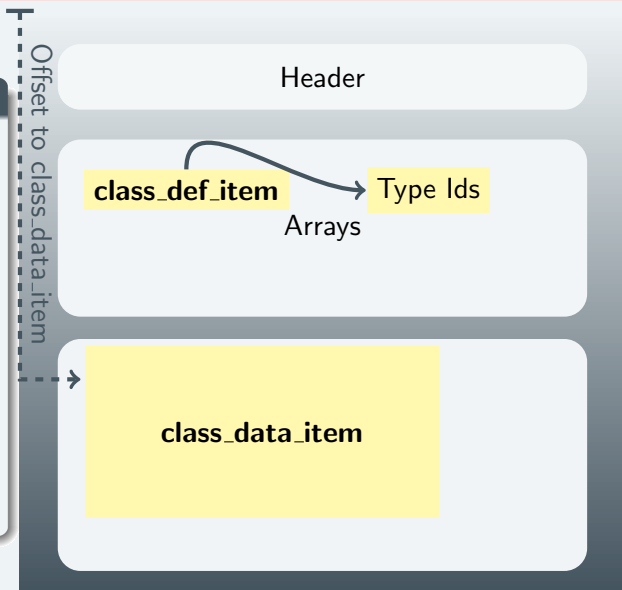
Arrays

Data

Inside the list of class definitions

encoded_method

- ▶ **access_flags:**
ACC_PUBLIC,
ACC_PRIVATE,
ACC_STATIC...
- ▶ **code_off:** offset to
code from
beginning of DEX
file
- ▶ **method_idx_diff:**
increment to
method indexes



Inside the list of class definitions

encoded_method

- ▶ **access_flags:**
ACC_PUBLIC,
ACC_PRIVATE,
ACC_STATIC...
- ▶ **code_off:** offset to
code from
beginning of DEX
file
- ▶ **method_idx_diff:**
increment to
method indexes

Offset to class_data_item

Header

class_def_item

Type Ids

Arrays

List of fields

Direct methods:

encoded_method

class_data_item

Virtual methods:

encoded_method

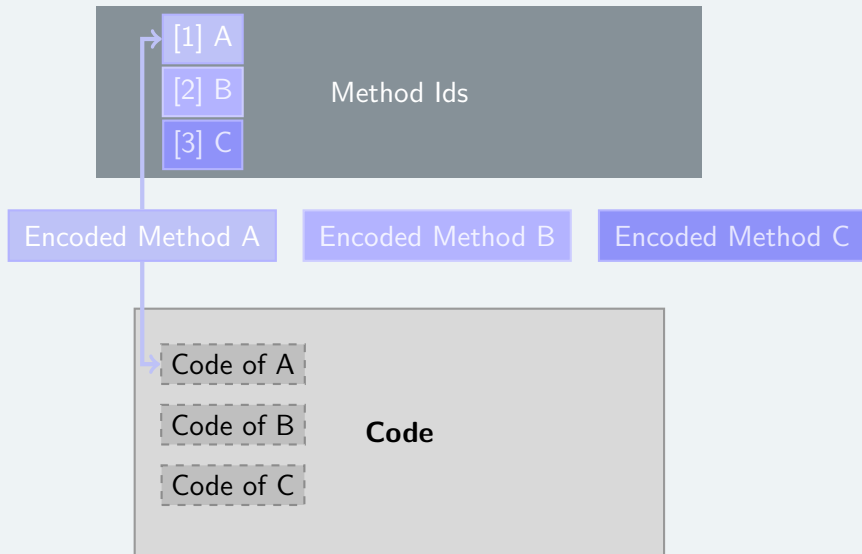
Trick

Modify the chaining of methods and skip the hidden method
The info for the hidden method is still there, but won't be read

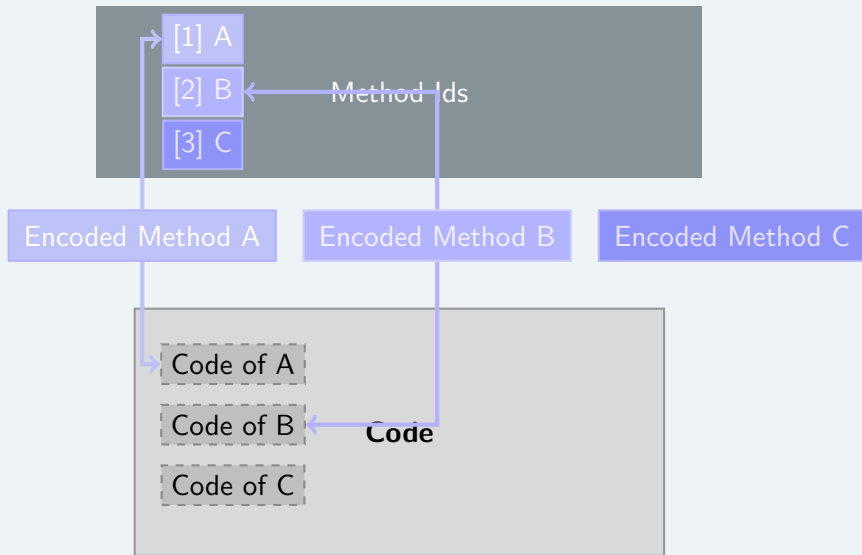
Implementation

- ▶ **method_idx_diff:**
 - ▶ modify for hidden method
 - ▶ + modify for the *'other'* method
- ▶ **code_off:** refer the other method
- ▶ **access_flags:** nothing to do
- ▶ **direct_methods_size** (or **virtual_methods_size**): nothing to do

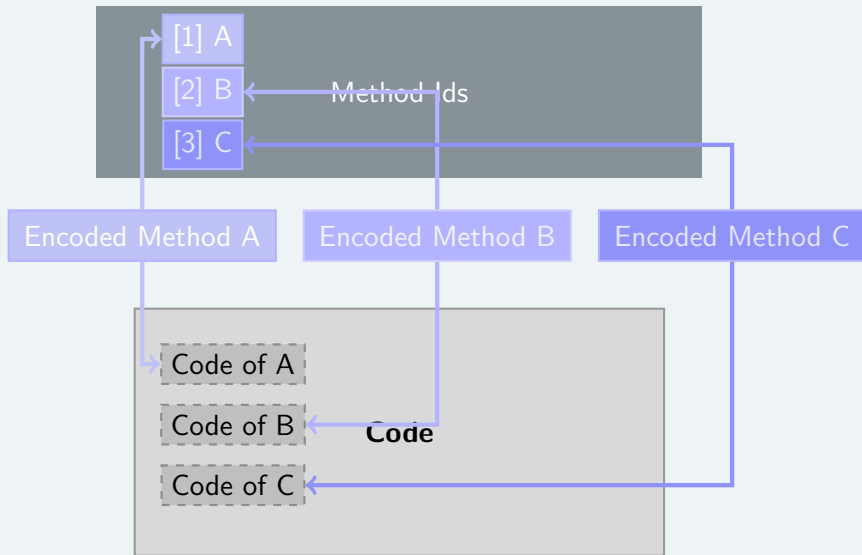
Visual representation of chaining



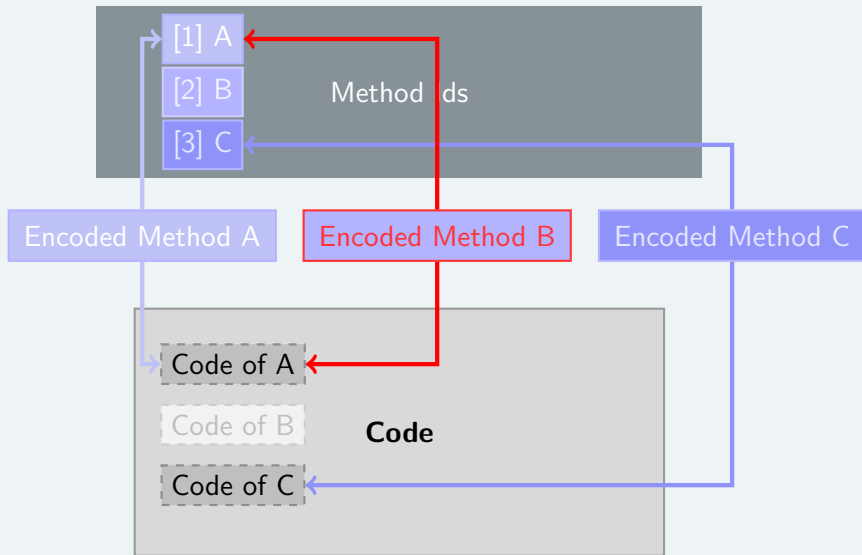
Visual representation of chaining



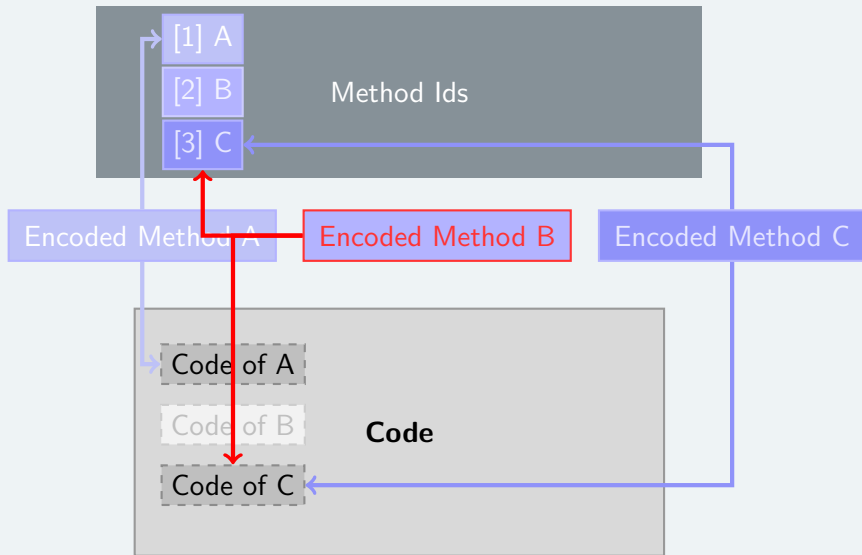
Visual representation of chaining



Visual representation of chaining



Visual representation of chaining





Some more tricks

- ▶ **Access flags:** you *may* modify but must choose a flag within *direct* methods or *virtual* methods
- ▶ **Single method?** Set *direct_methods_size* (or *virtual_methods_size*) and 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 01 01 04 3E 01 09 C8 3E 01 09 B8  <..à<...>..È>..
39B0h: 31 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ?.....
39C0h: 01 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00  .....
```

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

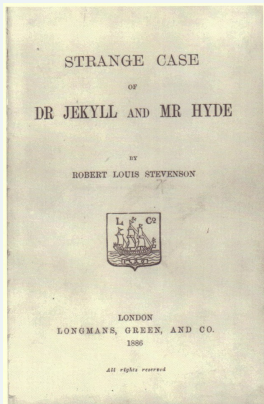
Re-build APK

- ▶ Unzip original APK: retrieve manifest, resources...
- ▶ Zip new APK with new DEX + same manifest and resources
- ▶ Sign package (jarsigner)

Part 2: calling the hidden method

calling thisishidden()

- ▶ 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 thisishidden()
- ▶ Current personality displayed in main activity



DEMO :)



Load the current DEX file

`openNonAsset()` not directly accessible → use reflection

```
// get AssetManager class via reflection
Class localClass = Class.forName("...AssetManager");
Class[] arrayOfClass = new Class[1];
arrayOfClass[0] = String.class;
// get openNonAsset method
Method localMethod = localClass.getMethod("openNonAsset", ...
AssetManager localAssetManager = this.context.getAssets();
Object[] arrayOfObject = new Object[1];
arrayOfObject[0] = paramString;
// invoke method
InputStream localInputStream = (InputStream)localMethod.invoke(...);
```



Patch the DEX

Undo what we did - re-chain the hidden method, re-hash and checksum the DEX

```
int patch_index = 0x2c99;
dex[patch_index++] = 1; // method_idx_diff
dex[patch_index++] = 1; // access flag
dex[patch_index++] = (byte)0xcc; // code offset
dex[patch_index++] = (byte)0x28;
dex[patch_index++] = 1;
```



Open the modified DEX

- ▶ use reflection to call `openDexFile()`
`native private static int
openDexFile(byte[] fileContents);`
- ▶ returns a cookie = pointer to internal struct for DEX
- ▶ load modified class using `defineClass()`

```
Class patchedHyde = null;  
Log.i("HideAndSeek", "retrieving patched MrHyde class");  
if (defineClassMethod != null) {  
    patchedHyde = (Class) defineClassMethod.invoke(  
        dexFileClass, params);  
}
```

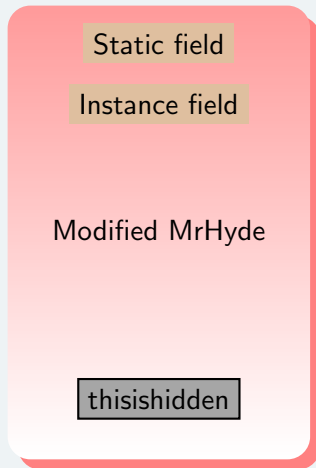
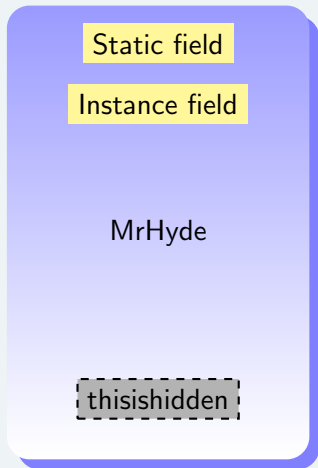


Invoke the hidden method

- ▶ Search for the hidden method (`getDeclaredMethods()`)
- ▶ Instantiate an object
- ▶ Call `thisishidden()`

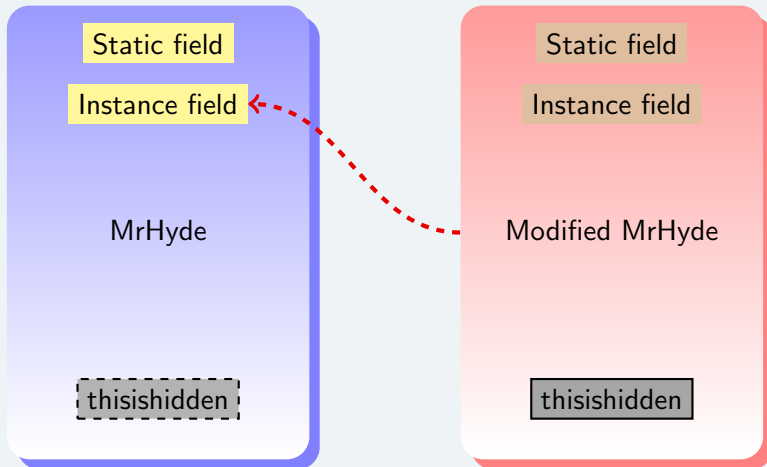
```
Object obj = patchedHyde.getDeclaredConstructor(Context.class)
    .newInstance(context);
Log.i("HideAndSeek", "after new Instance");
arg[0] = Boolean.valueOf(true);
Log.i("HideAndSeek", "invoking thisishidden()..");
thisishiddenMethod.invoke(obj, arg);
```

It's two different classes

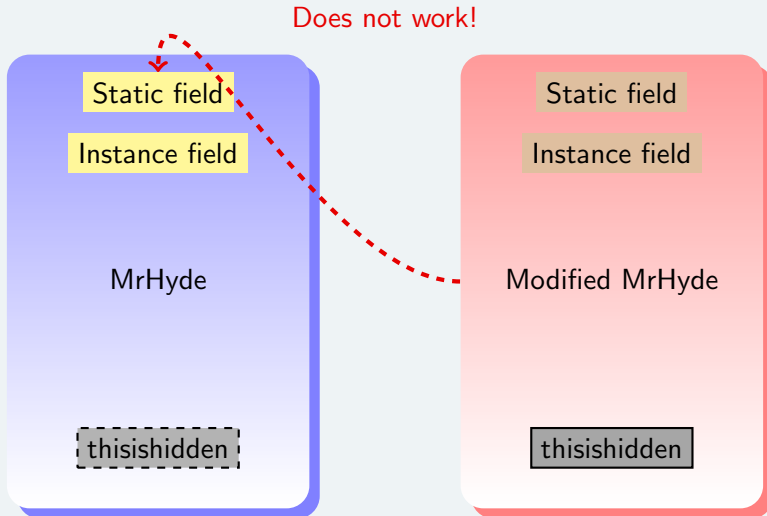


It's two different classes

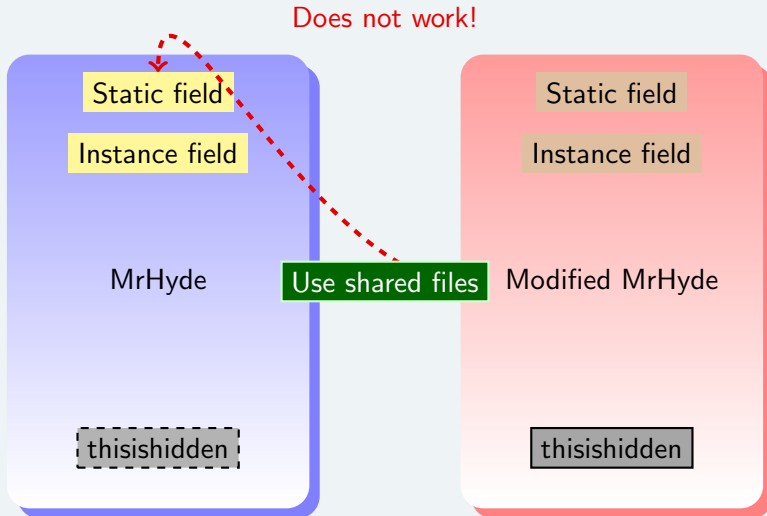
Does not work!



It's two different classes



It's two different classes



Dangers

It can be used to hide some malicious feature

Detection

The strings are not hidden

The bytecode is there

Solutions

- ▶ Use my patch/unpatch tool: `hidex.pl`
- ▶ Disassemble bytecode at a given location: `androdix.py`
- ▶ Fix Android: verify consistency of `encoded_method`
- ▶ Google notified in June 2013

Thank You !

Thanks!

to **@pof** ... and for your attention!

FortiGuard Labs

Follow us on twitter: **@FortiGuardLabs**

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

Me

twitter: **@cryptax**

e-mail: aapvrille at fortinet dot com

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



Are those PowerPoint slides? No way! It's \LaTeX + TikZ + Beamer + [Lobster](#)