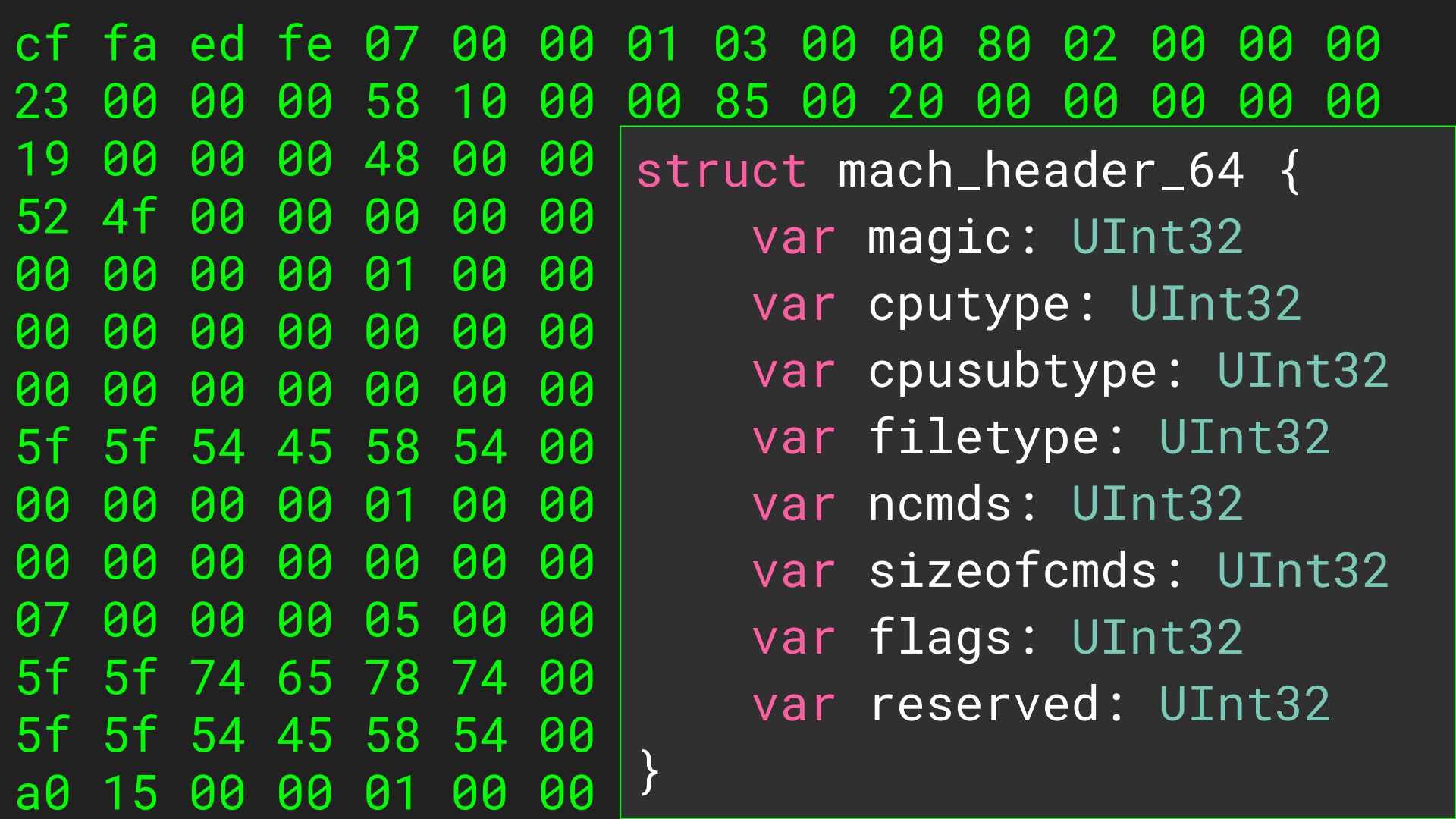
try! Swift

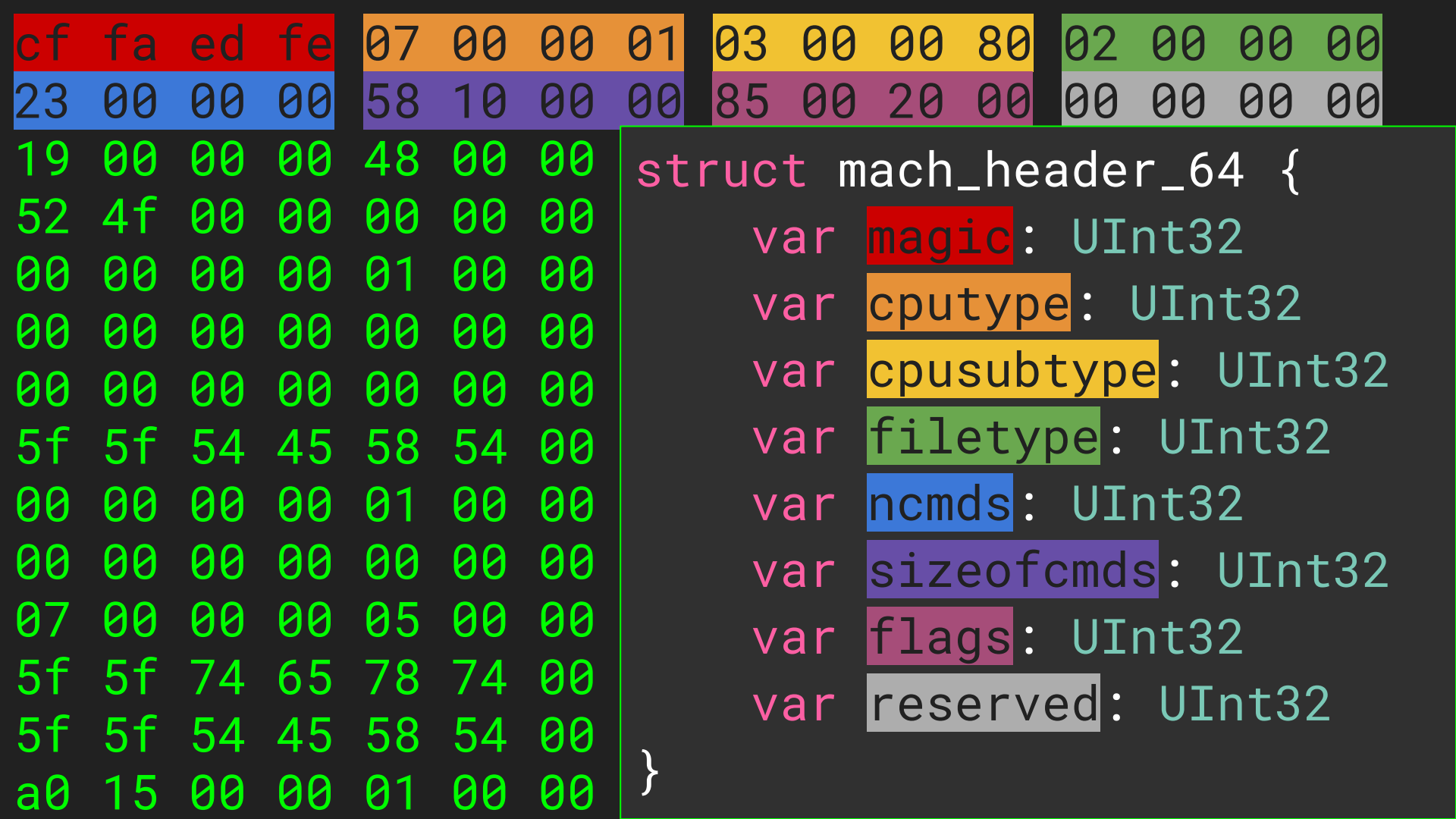
MachObfuscator

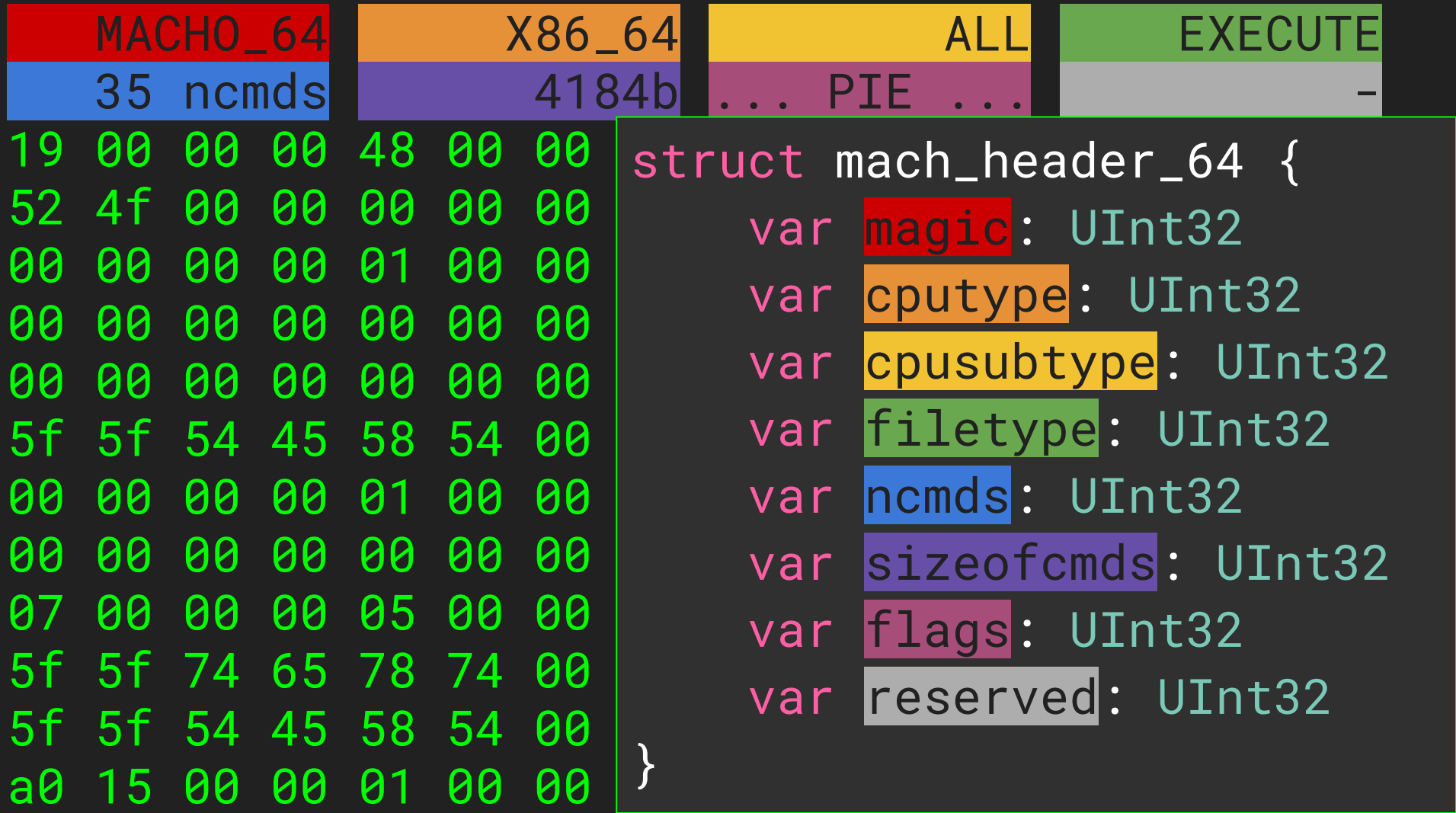
Kamil Borzym
@kam800

Section9

```
cf fa ed fe 07 00 00 01 03 00 00 80 02 00 00 00
23 00 00 00 58 10 00 00 85 00 20 00 00 00 00 00
19 00 00 00 48 00 00 00 5f 5f 50 41 47 45 5a 45
52 4f 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 01 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 00 00 00 00 00 00 00 19 00 00 00 f8 04 00 00
5f 5f 54 45 58 54 00 00 00 00 00 00 00 00 00 00
00 00 00 00 01 00 00 00 00 50 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 50 00 00 00 00 00 00
07 00 00 00 05 00 00 00 0f 00 00 00 00 00 00 00
5f 5f 74 65 78 74 00 00 00 00 00 00 00 00 00 00
5f 5f 54 45 58 54 00 00 00 00 00 00 00 00 00 00
a0 15 00 00 01 00 00 00 7a 26 00 00 00 00 00 00
```


cf fa ed fe 07 00 00 01 03 00 00 80 02 00 00 00
23 00 00 00 58 10 00 00 85 00 20 00 00 00 00 00
19 00 00 00 48 00 00
52 4f 00 00 00 00 00
00 00 00 00 01 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
5f 5f 54 45 58 54 00
00 00 00 00 01 00 00
00 00 00 00 00 00 00
07 00 00 00 05 00 00
5f 5f 74 65 78 74 00
5f 5f 54 45 58 54 00
a0 15 00 00 01 00 00
struct mach_header_64 {
var magic: UInt32
var cputype: UInt32
var cpusubtype: UInt32
var filetype: UInt32
var ncmds: UInt32
var sizeofcmds: UInt32
var flags: UInt32
var reserved: UInt32
}


cf fa ed fe 07 00 00 01 03 00 00 80 02 00 00 00
23 00 00 00 58 10 00 00 85 00 20 00 00 00 00 00
19 00 00 00 48 00 00
52 4f 00 00 00 00 00
00 00 00 00 01 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
5f 5f 54 45 58 54 00
00 00 00 00 01 00 00
00 00 00 00 00 00 00
07 00 00 00 05 00 00
5f 5f 74 65 78 74 00
5f 5f 54 45 58 54 00
a0 15 00 00 01 00 00
struct mach_header_64 {
var magic: UInt32
var cputype: UInt32
var cpusubtype: UInt32
var filetype: UInt32
var ncmds: UInt32
var sizeofcmds: UInt32
var flags: UInt32
var reserved: UInt32
}


MACHO_64
X86_64
ALL
EXECUTE
35 ncmds
4184b
... PIE ...
-
19 00 00 00 48 00 00
52 4f 00 00 00 00 00
00 00 00 00 01 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
5f 5f 54 45 58 54 00
00 00 00 00 01 00 00
00 00 00 00 00 00 00
07 00 00 00 05 00 00
5f 5f 74 65 78 74 00
5f 5f 54 45 58 54 00
a0 15 00 00 01 00 00
struct mach_header_64 {
var magic: UInt32
var cputype: UInt32
var cpusubtype: UInt32
var filetype: UInt32
var ncmds: UInt32
var sizeofcmds: UInt32
var flags: UInt32
var reserved: UInt32
}

```
extension Data {
  func getStruct<T>(at offset: Int) -> T {
    return withUnsafeBytes {
      (ptr: UnsafePointer<UInt8>) in
        ptr.advanced(by: offset)
           .withMemoryRebound(to: T.self,
                              capacity: 1,
                              { $0.pointee })
    }
  }
}
```

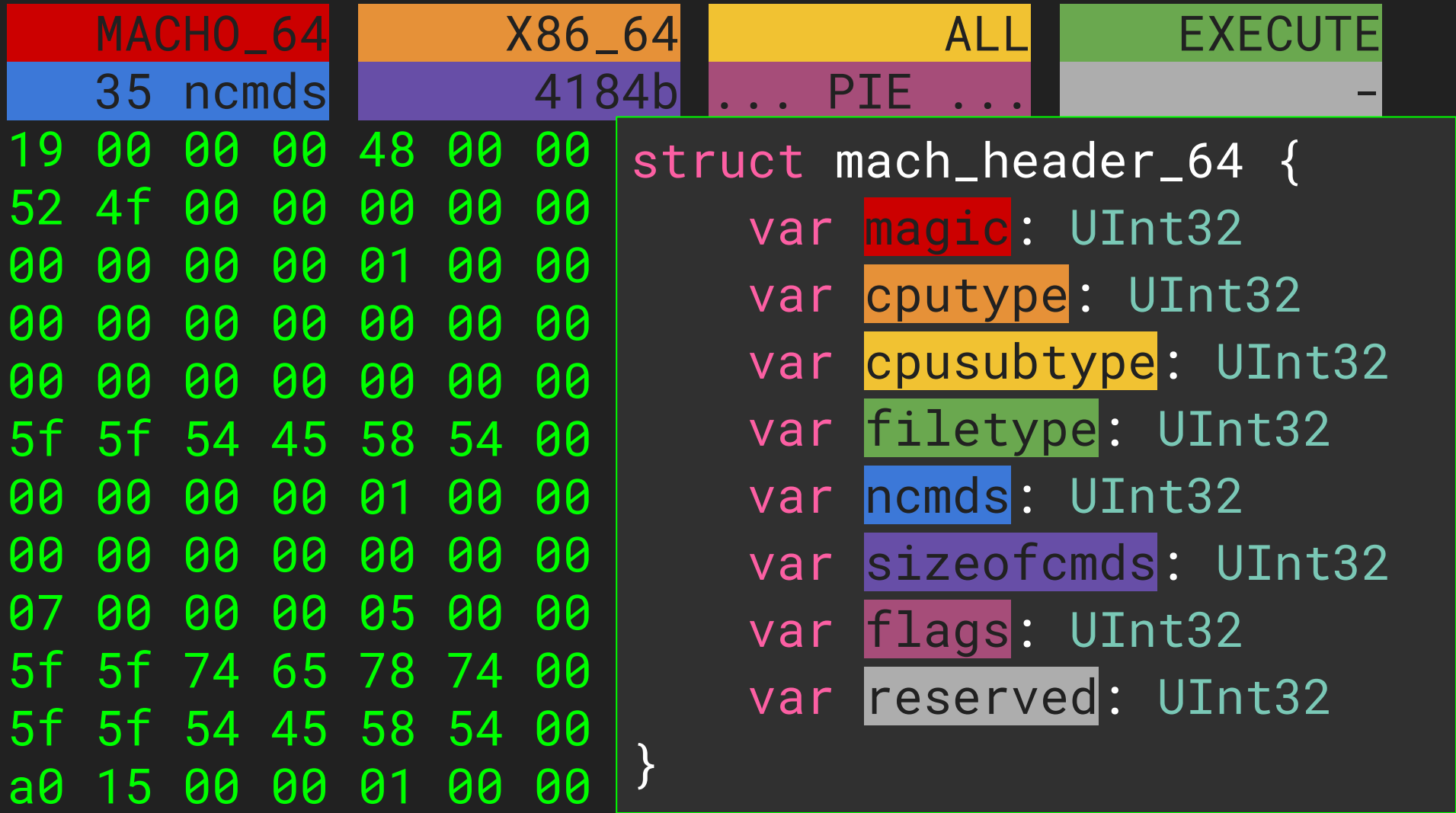
```
extension Data {
  func getStruct<T>(at offset: Int) -> T {
    return withUnsafeBytes {
      (ptr: UnsafePointer<UInt8>) in
        ptr.advanced(by: offset)
           .withMemoryRebound(to: T.self,
                              capacity: 1,
                              { $0.pointee })
    }
  }
}
```

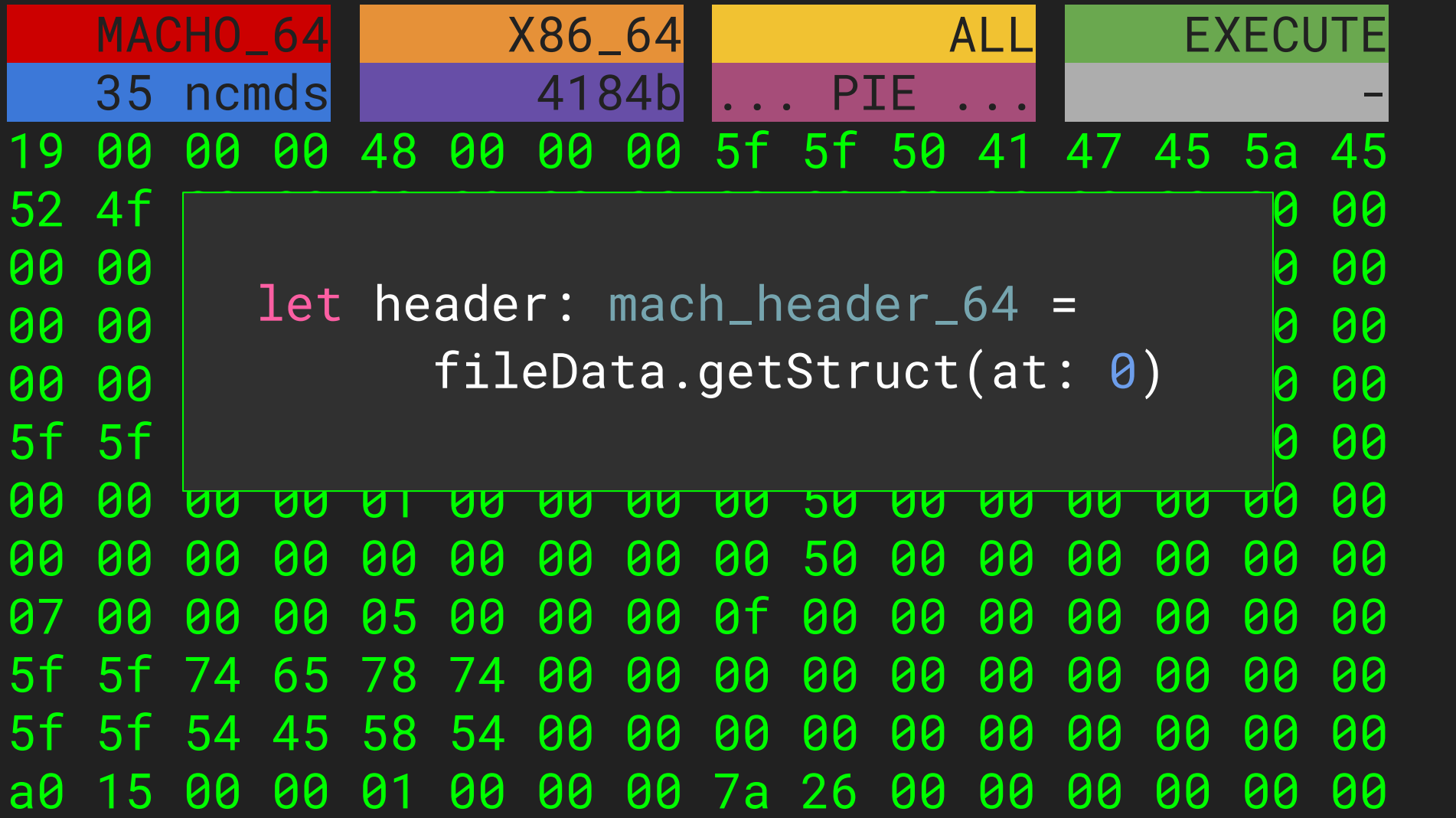
```
extension Data {
  func getStruct<T>(at offset: Int) -> T {
    return withUnsafeBytes {
      (ptr: UnsafePointer<UInt8>) in
        ptr.advanced(by: offset)
           .withMemoryRebound(to: T.self,
                              capacity: 1,
                              { $0.pointee })
    }
  }
}
```

```
extension Data {
  func getStruct<T>(at offset: Int) -> T {
    return withUnsafeBytes {
      (ptr: UnsafePointer<UInt8>) in
        ptr.advanced(by: offset)
           .withMemoryRebound(to: T.self,
                              capacity: 1,
                              { $0.pointee })
    }
  }
}
```

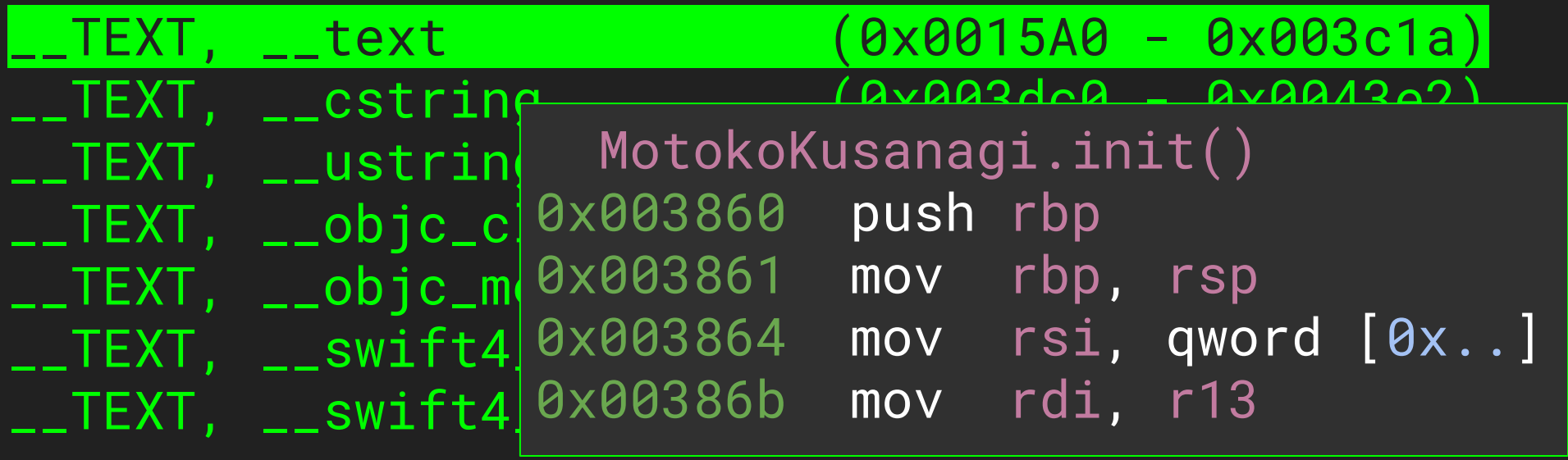
```
extension Data {
  func getStruct<T>(at offset: Int) -> T {
    return withUnsafeBytes {
      (ptr: UnsafePointer<UInt8>) in
        ptr.advanced(by: offset)
           .withMemoryRebound(to: T.self,
                              capacity: 1,
                              { $0.pointee })
    }
  }
}
```

```
extension Data {
  func getStruct<T>(at offset: Int) -> T {
    return withUnsafeBytes {
      (ptr: UnsafePointer<UInt8>) in
        ptr.advanced(by: offset)
           .withMemoryRebound(to: T.self,
                              capacity: 1,
                              { $0.pointee })
    }
  }
}
```

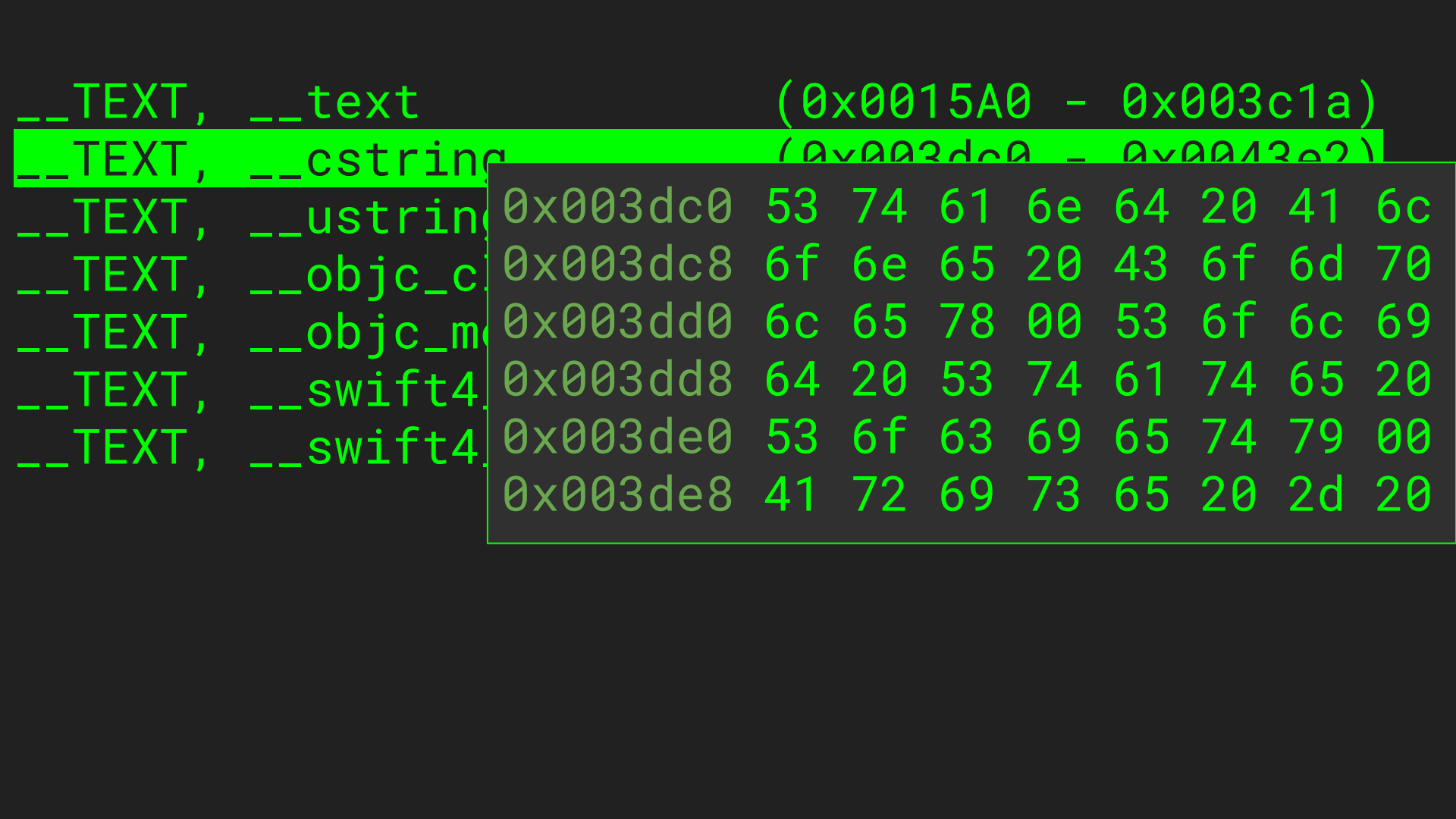

MACHO_64
X86_64
ALL
EXECUTE
35 ncmds
4184b
... PIE ...
-
19 00 00 00 48 00 00
52 4f 00 00 00 00 00
00 00 00 00 01 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
5f 5f 54 45 58 54 00
00 00 00 00 01 00 00
00 00 00 00 00 00 00
07 00 00 00 05 00 00
5f 5f 74 65 78 74 00
5f 5f 54 45 58 54 00
a0 15 00 00 01 00 00
struct mach_header_64 {
var magic: UInt32
var cputype: UInt32
var cpusubtype: UInt32
var filetype: UInt32
var ncmds: UInt32
var sizeofcmds: UInt32
var flags: UInt32
var reserved: UInt32
}

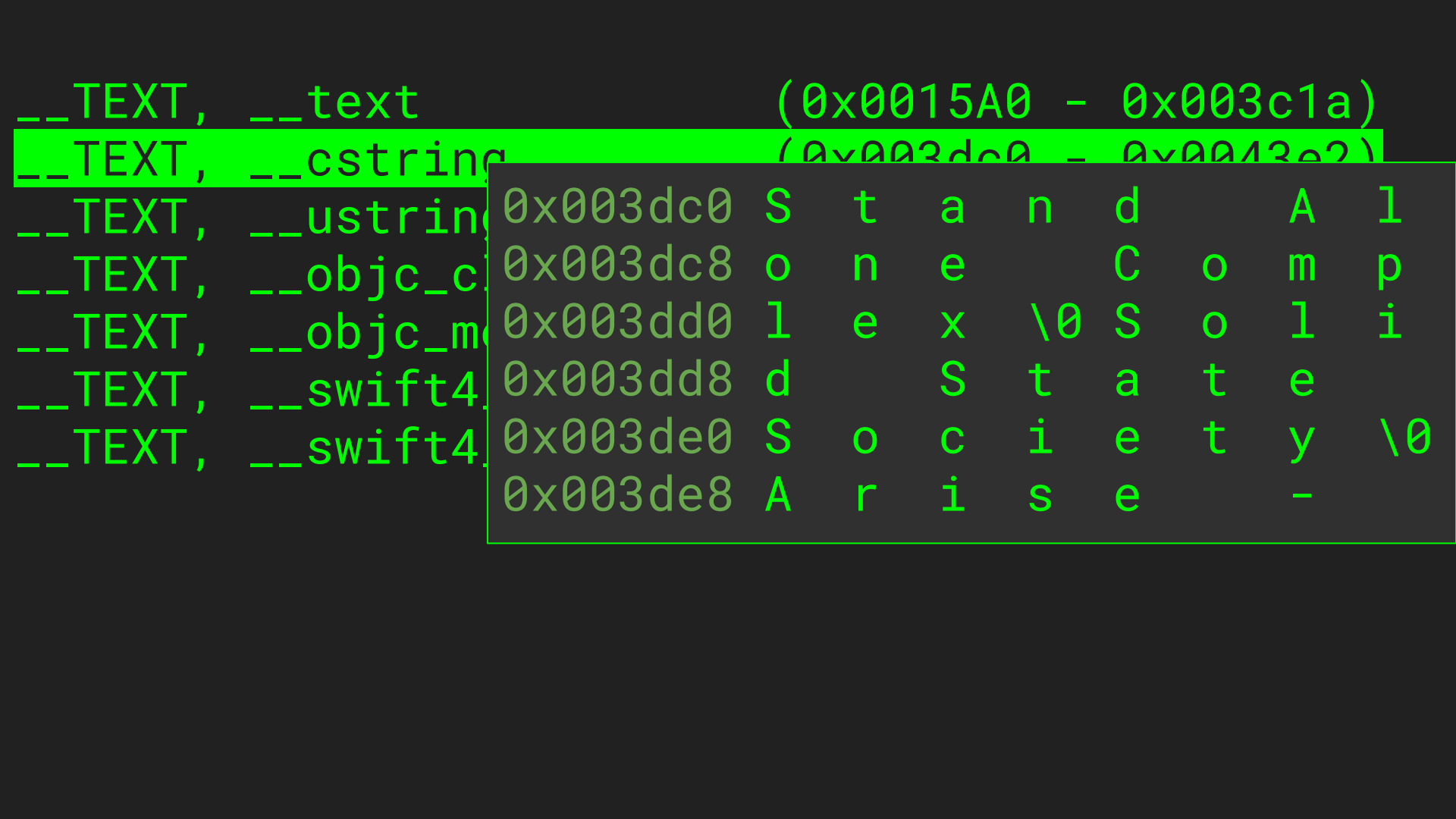

MACHO_64
X86_64
ALL
EXECUTE
35 ncmds
4184b
... PIE ...
-
19 00 00 00 48 00 00 00 5f 5f 50 41 47 45 5a 45
52 4f
00 00
00 00
00 00
5f 5f
00 00
00 00 00 00 00 00 00 00 50 00 00 00 00 00 00
07 00 00 00 05 00 00 00 0f 00 00 00 00 00 00 00
5f 5f 74 65 78 74 00 00 00 00 00 00 00 00 00 00
5f 5f 54 45 58 54 00 00 00 00 00 00 00 00 00 00
a0 15 00 00 01 00 00 00 7a 26 00 00 00 00 00 00
let header: mach_header_64 =
fileData.getStruct(at: 0)

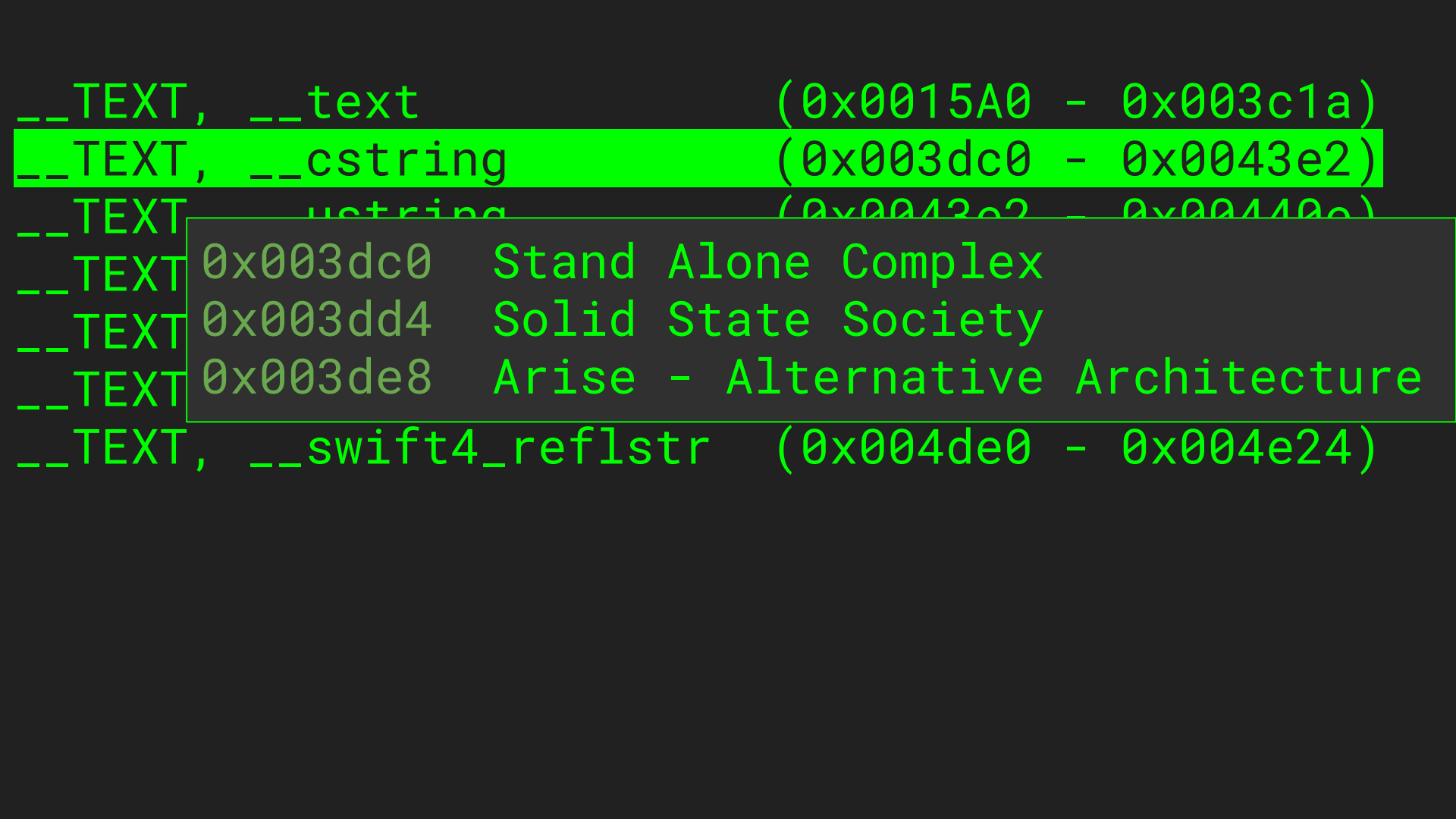
```
__TEXT, __text                (0x0015A0 - 0x003c1a)
__TEXT, __cstring             (0x003dc0 - 0x0043e2)
__TEXT, __ustring             (0x0043e2 - 0x00440e)
__TEXT, __objc_classname      (0x00440e - 0x004434)
__TEXT, __objc_methname       (0x004434 - 0x004b09)
__TEXT, __swift4_typeref      (0x004cbc - 0x004d38)
__TEXT, __swift4_reflstr      (0x004de0 - 0x004e24)
```


__TEXT, __text (0x0015A0 - 0x003c1a)
__TEXT, __cstring
__TEXT, __ustring
__TEXT, __objc_c
__TEXT, __objc_m
__TEXT, __swift4_
__TEXT, __swift4_
MotokoKusanagi.init()
0x003860 push rbp
0x003861 mov rbp, rsp
0x003864 mov rsi, qword [0x..]
0x00386b mov rdi, r13

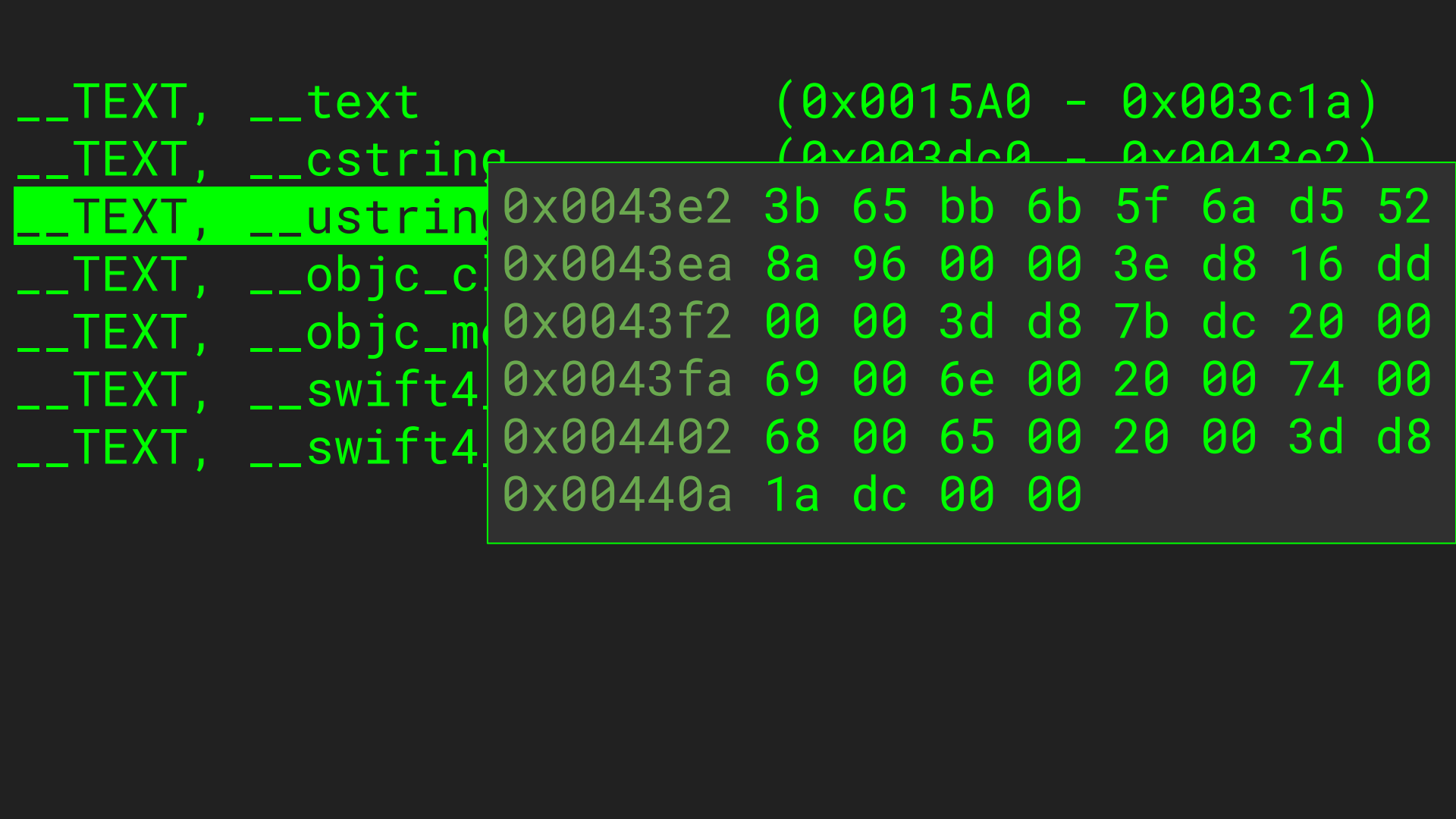
```
__TEXT, __text                (0x0015A0 - 0x003c1a)
__TEXT, __cstring             (0x003dc0 - 0x0043e2)
__TEXT, __ustring             (0x0043e2 - 0x00440e)
__TEXT, __objc_classname      (0x00440e - 0x004434)
__TEXT, __objc_methname       (0x004434 - 0x004b09)
__TEXT, __swift4_typeref      (0x004cbc - 0x004d38)
__TEXT, __swift4_reflstr      (0x004de0 - 0x004e24)
```

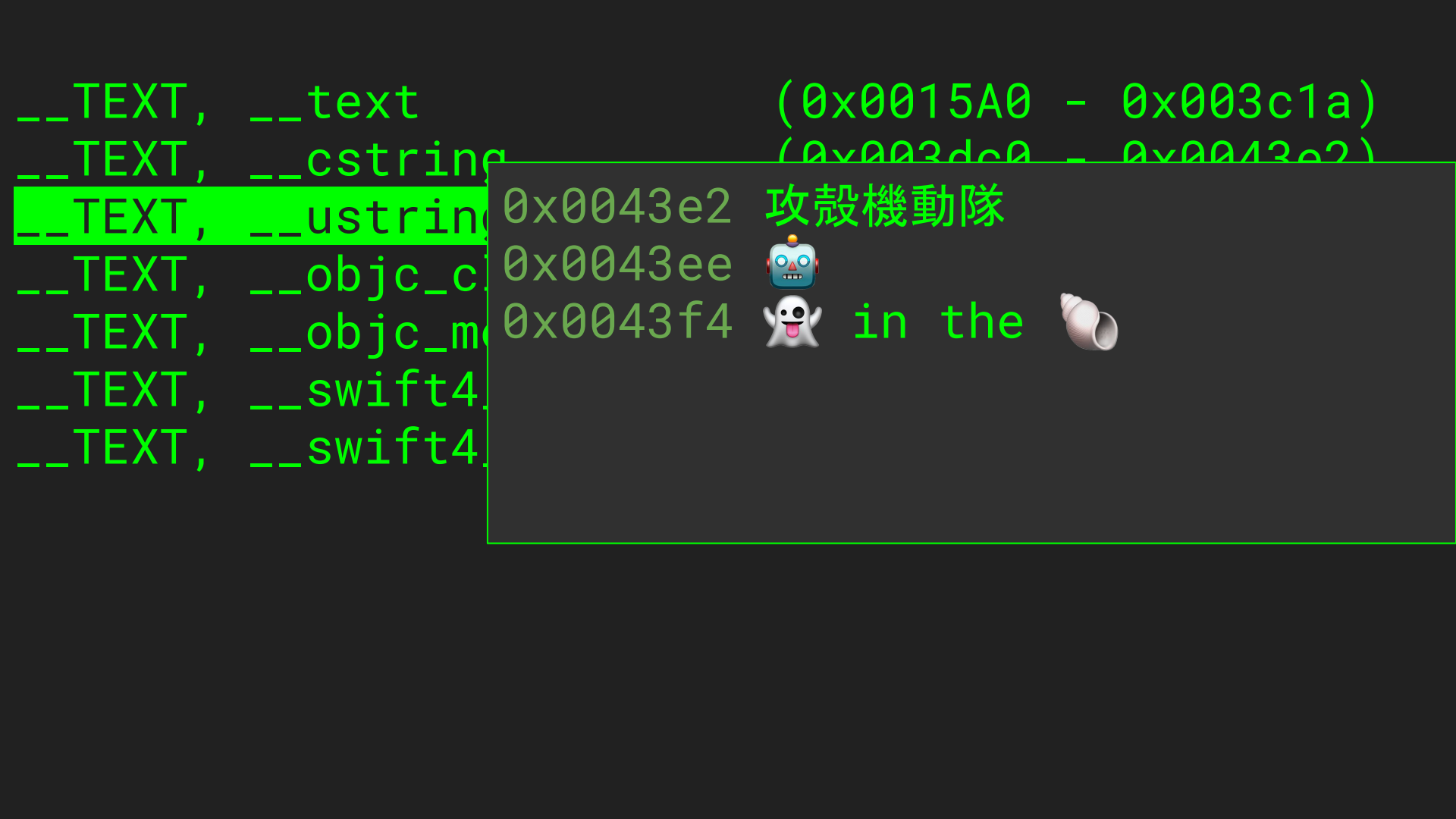

__TEXT, __text (0x0015A0 - 0x003c1a)
__TEXT, __cstring
__TEXT, __ustring
__TEXT, __objc_c
__TEXT, __objc_m
__TEXT, __swift4
__TEXT, __swift4
0x003dc0 53 74 61 6e 64 20 41 6c
0x003dc8 6f 6e 65 20 43 6f 6d 70
0x003dd0 6c 65 78 00 53 6f 6c 69
0x003dd8 64 20 53 74 61 74 65 20
0x003de0 53 6f 63 69 65 74 79 00
0x003de8 41 72 69 73 65 20 2d 20


__TEXT, __text (0x0015A0 - 0x003c1a)
__TEXT, __cstring
__TEXT, __ustring
__TEXT, __objc_c
__TEXT, __objc_m
__TEXT, __swift4_
__TEXT, __swift4_
0x003dc0 S t a n d A l
0x003dc8 o n e C o m p
0x003dd0 l e x \0 S o l i
0x003dd8 d S t a t e
0x003de0 S o c i e t y \0
0x003de8 A r i s e -

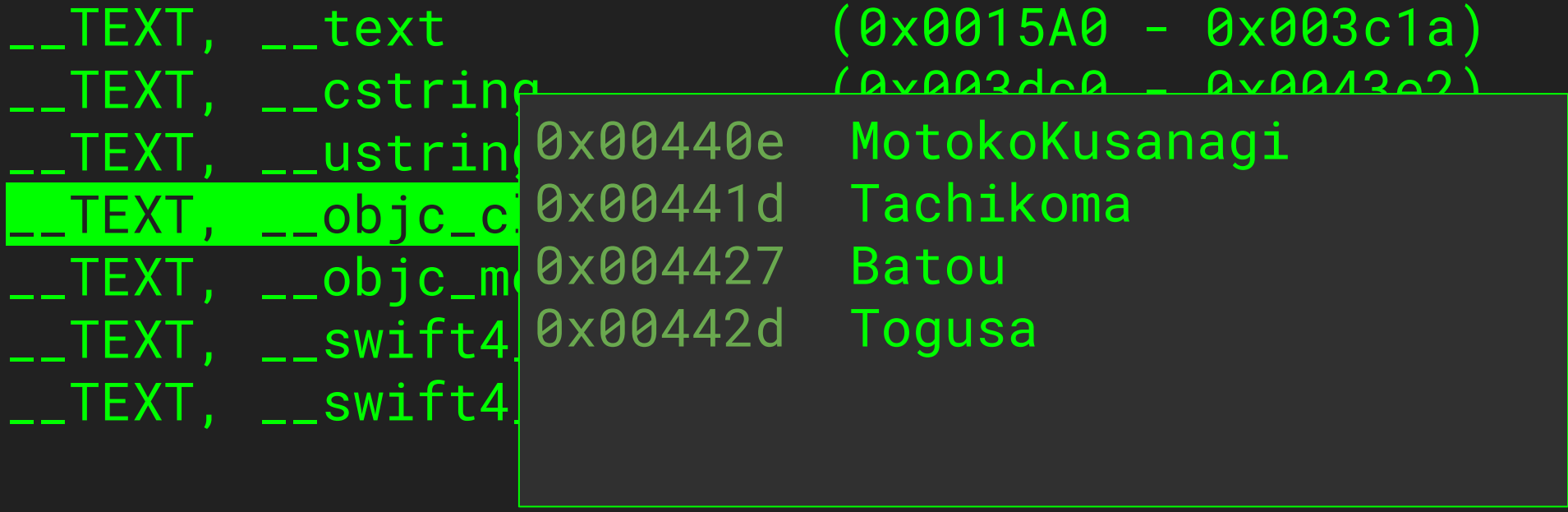

__TEXT, __text (0x0015A0 - 0x003c1a)
__TEXT, __cstring (0x003dc0 - 0x0043e2)
__TEXT
__TEXT
__TEXT
__TEXT
0x003dc0 Stand Alone Complex
0x003dd4 Solid State Society
0x003de8 Arise - Alternative Architecture
__TEXT, __swift4_reflstr (0x004de0 - 0x004e24)

```
__TEXT, __text                (0x0015A0 - 0x003c1a)
__TEXT, __cstring             (0x003dc0 - 0x0043e2)
__TEXT, __ustring             (0x0043e2 - 0x00440e)
__TEXT, __objc_classname      (0x00440e - 0x004434)
__TEXT, __objc_methname       (0x004434 - 0x004b09)
__TEXT, __swift4_typeref      (0x004cbc - 0x004d38)
__TEXT, __swift4_reflstr      (0x004de0 - 0x004e24)
```

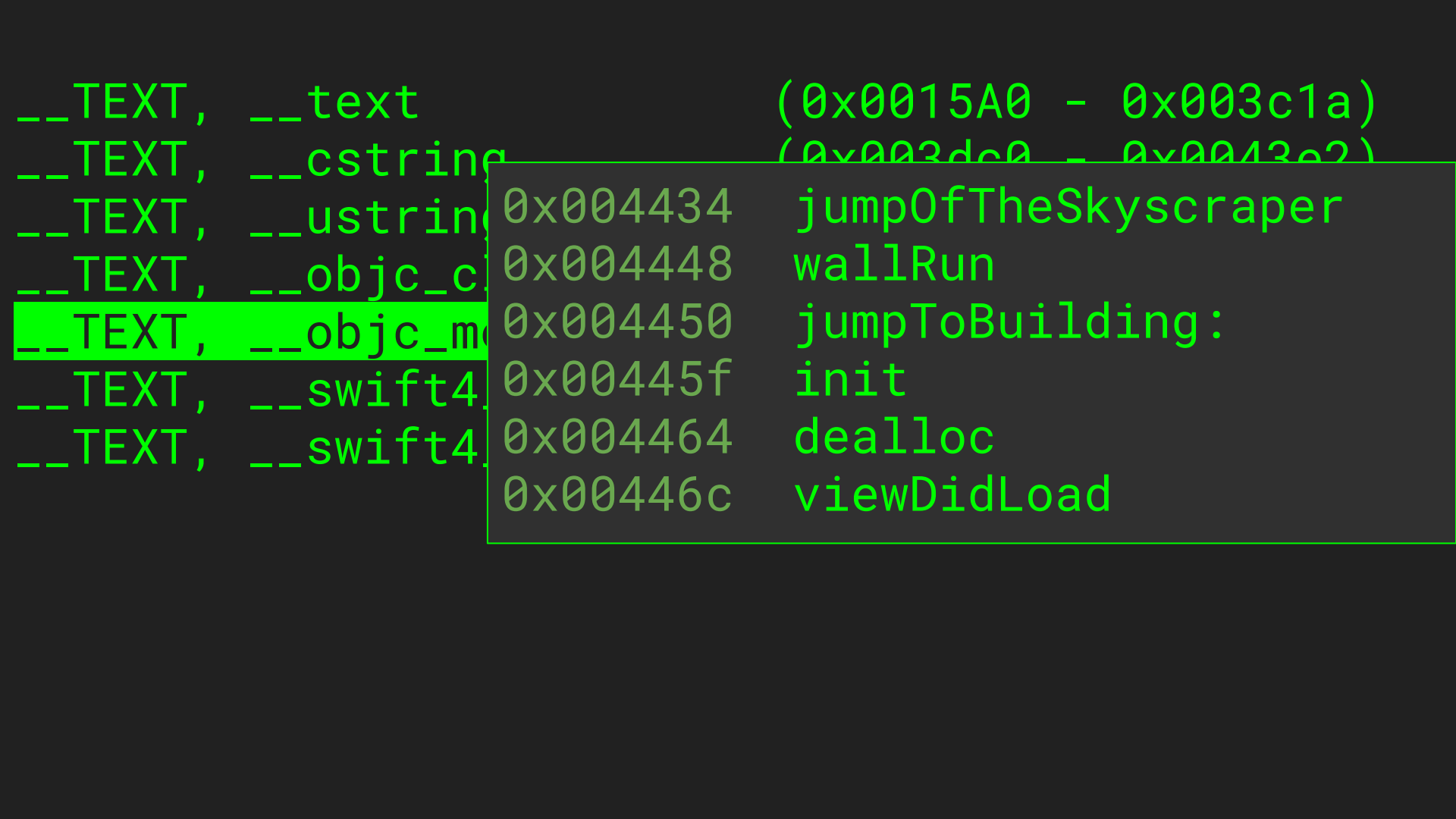

__TEXT, __text (0x0015A0 - 0x003c1a)
__TEXT, __cstring
__TEXT, __ustring
__TEXT, __objc_c
__TEXT, __objc_m
__TEXT, __swift4
__TEXT, __swift4
0x0043e2 3b 65 bb 6b 5f 6a d5 52
0x0043ea 8a 96 00 00 3e d8 16 dd
0x0043f2 00 00 3d d8 7b dc 20 00
0x0043fa 69 00 6e 00 20 00 74 00
0x004402 68 00 65 00 20 00 3d d8
0x00440a 1a dc 00 00


__TEXT, __text (0x0015A0 - 0x003c1a)
__TEXT, __cstring
__TEXT, __ustring
__TEXT, __objc_c
__TEXT, __objc_m
__TEXT, __swift4_
__TEXT, __swift4_
0x0043e2 攻殻機動隊
0x0043ee 🤖
0x0043f4 👻 in the 🐚

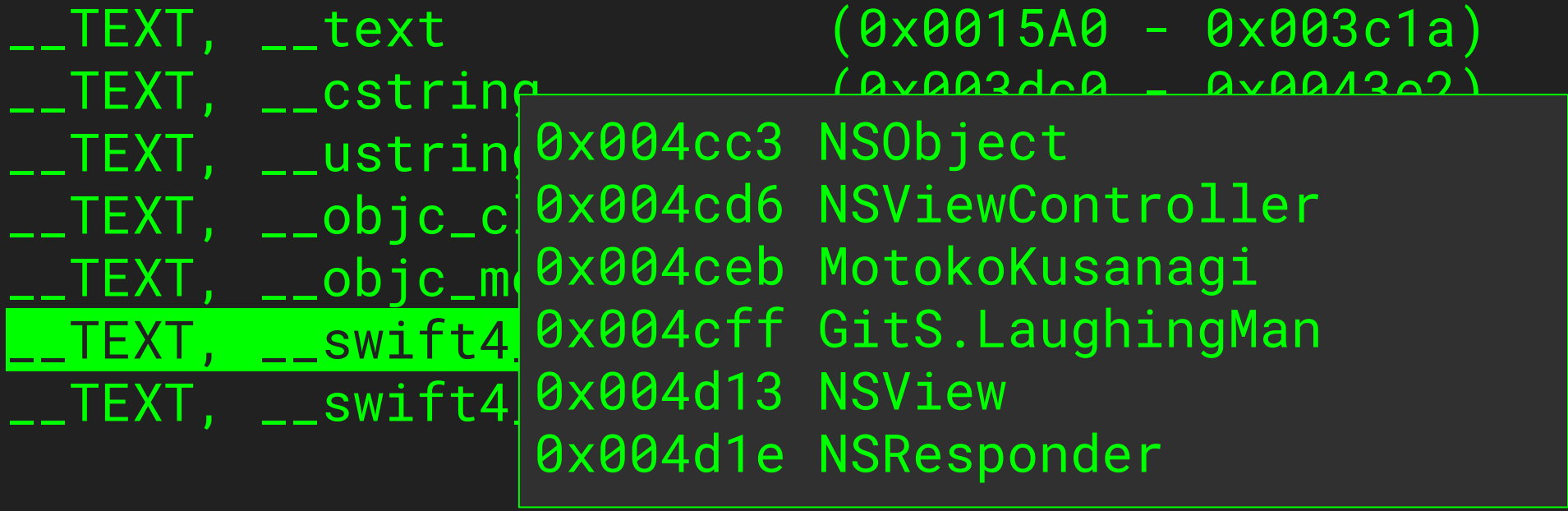
```
__TEXT, __text                (0x0015A0 - 0x003c1a)
__TEXT, __cstring             (0x003dc0 - 0x0043e2)
__TEXT, __ustring             (0x0043e2 - 0x00440e)
__TEXT, __objc_classname      (0x00440e - 0x004434)
__TEXT, __objc_methname       (0x004434 - 0x004b09)
__TEXT, __swift4_typeref      (0x004cbc - 0x004d38)
__TEXT, __swift4_reflstr      (0x004de0 - 0x004e24)
```


__TEXT, __text (0x0015A0 - 0x003c1a)
__TEXT, __cstring
__TEXT, __ustring
__TEXT, __objc_c
__TEXT, __objc_m
__TEXT, __swift4_
__TEXT, __swift4_
0x00440e MotokoKusanagi
0x00441d Tachikoma
0x004427 Batou
0x00442d Togusa

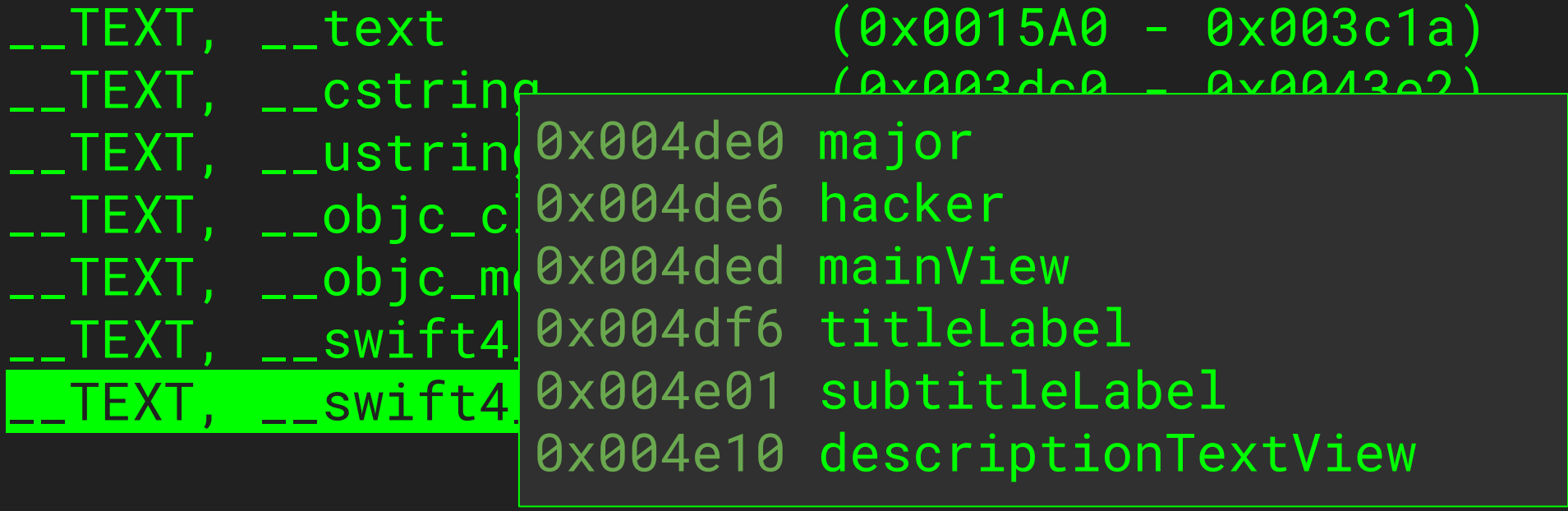
```
__TEXT, __text                (0x0015A0 - 0x003c1a)
__TEXT, __cstring             (0x003dc0 - 0x0043e2)
__TEXT, __ustring             (0x0043e2 - 0x00440e)
__TEXT, __objc_classname      (0x00440e - 0x004434)
__TEXT, __objc_methname       (0x004434 - 0x004b09)
__TEXT, __swift4_typeref      (0x004cbc - 0x004d38)
__TEXT, __swift4_reflstr      (0x004de0 - 0x004e24)
```

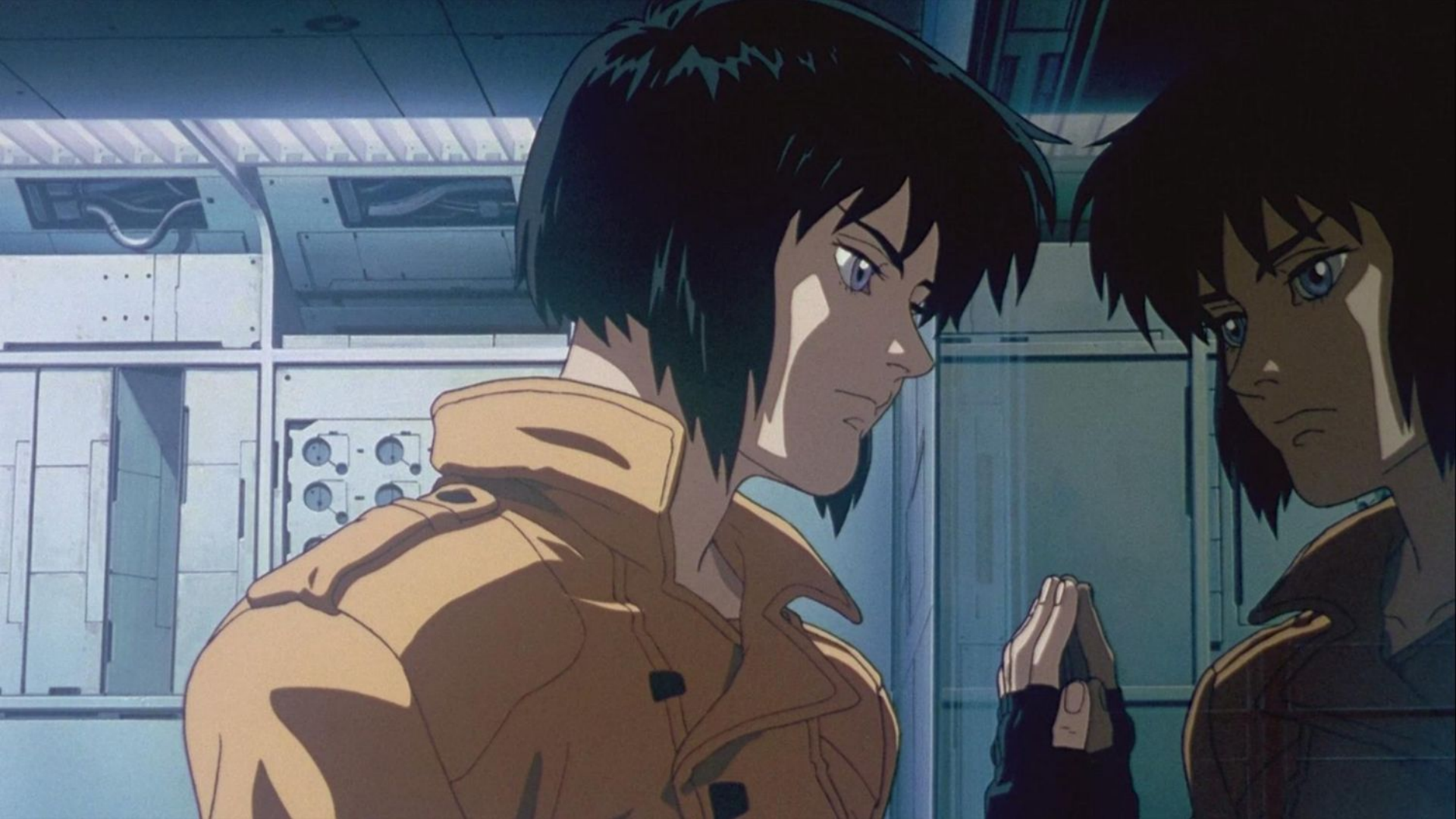

__TEXT, __text (0x0015A0 - 0x003c1a)
__TEXT, __cstring
__TEXT, __ustring
__TEXT, __objc_c
__TEXT, __objc_m
__TEXT, __swift4
__TEXT, __swift4
0x004434 jumpOfTheSkyscraper
0x004448 wallRun
0x004450 jumpToBuilding:
0x00445f init
0x004464 dealloc
0x00446c viewDidLoad

```
__TEXT, __text                (0x0015A0 - 0x003c1a)
__TEXT, __cstring             (0x003dc0 - 0x0043e2)
__TEXT, __ustring             (0x0043e2 - 0x00440e)
__TEXT, __objc_classname      (0x00440e - 0x004434)
__TEXT, __objc_methname       (0x004434 - 0x004b09)
__TEXT, __swift4_typeref      (0x004cbc - 0x004d38)
__TEXT, __swift4_reflstr      (0x004de0 - 0x004e24)
```


__TEXT, __text (0x0015A0 - 0x003c1a)
__TEXT, __cstring
__TEXT, __ustring
__TEXT, __objc_c
__TEXT, __objc_m
__TEXT, __swift4
__TEXT, __swift4
0x004cc3 NSObject
0x004cd6 NSViewController
0x004ceb MotokoKusanagi
0x004cff GitS.LaughingMan
0x004d13 NSView
0x004d1e NSResponder

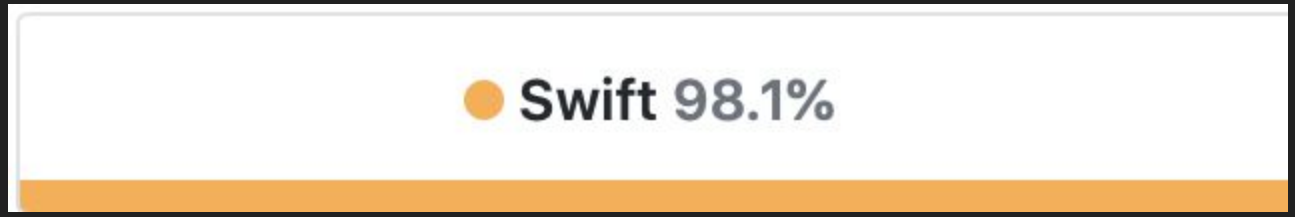
```
__TEXT, __text                (0x0015A0 - 0x003c1a)
__TEXT, __cstring             (0x003dc0 - 0x0043e2)
__TEXT, __ustring             (0x0043e2 - 0x00440e)
__TEXT, __objc_classname      (0x00440e - 0x004434)
__TEXT, __objc_methname       (0x004434 - 0x004b09)
__TEXT, __swift4_typeref      (0x004cbc - 0x004d38)
__TEXT, __swift4_reflstr      (0x004de0 - 0x004e24)
```

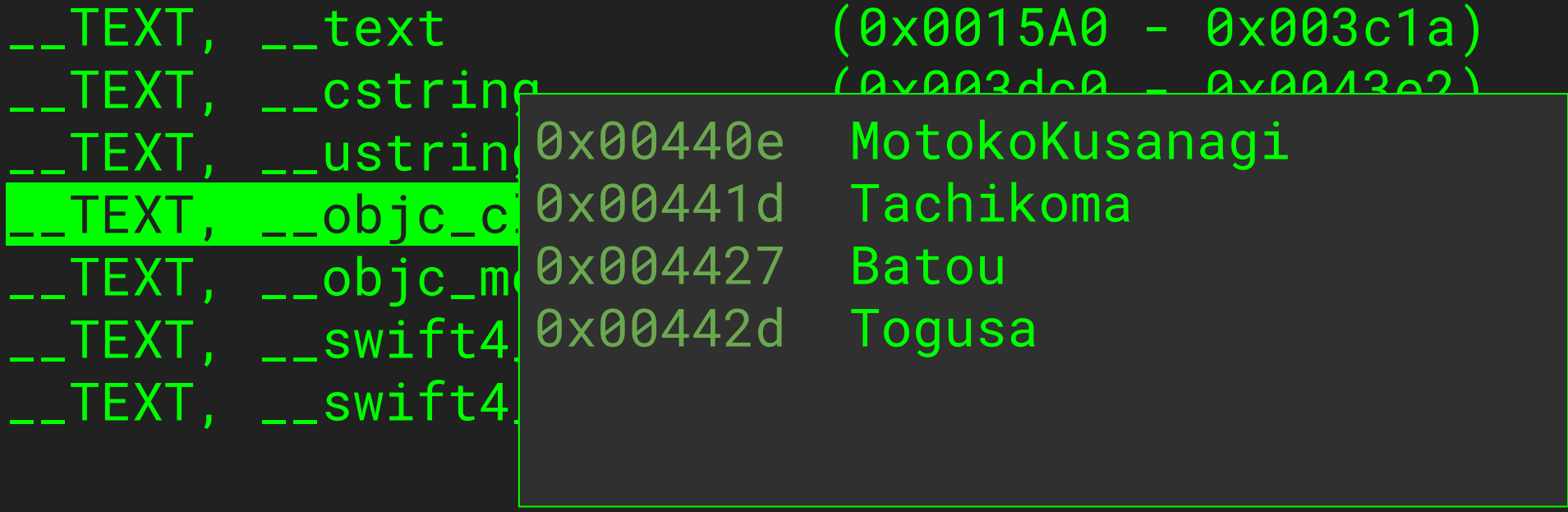

__TEXT, __text (0x0015A0 - 0x003c1a)
__TEXT, __cstring
__TEXT, __ustring
__TEXT, __objc_c
__TEXT, __objc_m
__TEXT, __swift4
__TEXT, __swift4
0x004de0 major
0x004de6 hacker
0x004ded mainView
0x004df6 titleLabel
0x004e01 subtitleLabel
0x004e10 descriptionTextView

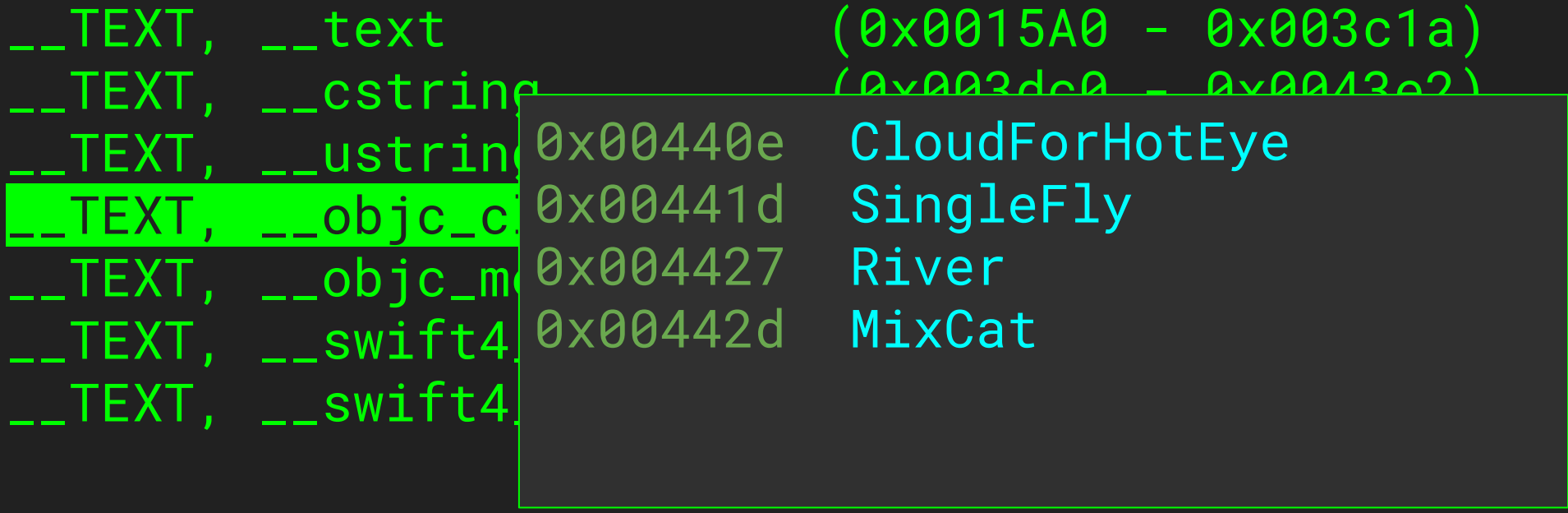


github.com/kam800/MachObfuscator

github.com/kam800/MachObfuscator




__TEXT, __text (0x0015A0 - 0x003c1a)
__TEXT, __cstring
__TEXT, __ustring
__TEXT, __objc_c
__TEXT, __objc_m
__TEXT, __swift4_
__TEXT, __swift4_
0x00440e MotokoKusanagi
0x00441d Tachikoma
0x004427 Batou
0x00442d Togusa


__TEXT, __text (0x0015A0 - 0x003c1a)
__TEXT, __cstring
__TEXT, __ustring
__TEXT, __objc_c
__TEXT, __objc_m
__TEXT, __swift4_
__TEXT, __swift4_
0x00440e CloudForHotEye
0x00441d SingleFly
0x004427 River
0x00442d MixCat

Kamil Borzym

@kam800

kam800/MachObfuscator

allegro