

Check if file exists:

MobileSubstrate.dylib

```
loc_100193060:
ldr    x0, [sp, #0x6a0 + var_1E0] ; argument "instance" for method imp___stubs__objc_msgSend, CODE XREF=__T07DVIA_v232JailbreakDetectionViewControllerC20jailbreakTest4TappedyypF+276
adrp   x8, #0x100437000 ; 0x100437f50@PAGE
add    x8, x8, #0xf50 ; 0x100437f50@PAGEOFF, &@selector(defaultManager)
ldr    x1, [x8] ; argument "selector" for method imp___stubs__objc_msgSend, "defaultManager",@selector(defaultManager)
bl    imp___stubs__objc_msgSend ; objc_msgSend
mov    fp, fp
bl    imp___stubs__objc_retainAutoreleasedReturnValue ; objc_retainAutoreleasedReturnValue
adrp   x8, #0x10035d000 ; 0x10035d8c0@PAGE
add    x8, x8, #0x8c0 ; 0x10035d8c0@PAGEOFF, "/Library/MobileSubstrate/MobileSubstrate.dylib"
mov    w3, #0xae
mov    x1, x9
orr    w2, wzr, #0x1
str    x0, [sp, #0x6a0 + var_1E8]
mov    x0, x8
bl    imp___stubs__T0S25Bp21_builtinStringLiteral_Bw17utf8CodeUnitCountBi1_7isASCIIItcfC ; Swift.String.init(_builtinStringLiteral: Builtin.RawPointer, utf8CodeUnitCount: Builtin.W
str    x2, [sp, #0x6a0 + var_1F0]
bl    imp___stubs__T0SS10FoundationE19_bridgeToObjectiveCs08NSStringCyF ; (extension in Foundation):Swift.String._bridgeToObjectiveC() -> __C.NSString
ldr    x1, [sp, #0x6a0 + var_1F0]
str    x0, [sp, #0x6a0 + var_1F8]
mov    x0, x1 ; argument "instance" for method imp___stubs__swift_unknownRelease
bl    imp___stubs__swift_unknownRelease ; swift_unknownRelease
adrp   x8, #0x100438000 ; 0x100438250@PAGE
add    x8, x8, #0x258 ; 0x100438250@PAGEOFF, &@selector(fileExistsAtPath:)
ldr    x1, [x8] ; argument "selector" for method imp___stubs__objc_msgSend, "fileExistsAtPath:",@selector(fileExistsAtPath:)
ldr    x0, lsp, #0xc00 + var_1F8
ldr    x2, [sp, #0x6a0 + var_1E8]
str    x0, [sp, #0x6a0 + var_200]
mov    x0, x2 ; argument "instance" for method imp___stubs__objc_msgSend
ldr    x2, [sp, #0x6a0 + var_200]
bl    imp___stubs__objc_msgSend ; objc_msgSend
ldr    x1, [sp, #0x6a0 + var_1F8]
str    w0, [sp, #0x6a0 + var_204]
mov    x0, x1 ; argument "instance" for method imp___stubs__objc_release
bl    imp___stubs__objc_release ; objc_release
ldr    x0, [sp, #0x6a0 + var_1E8] ; argument "instance" for method imp___stubs__objc_release
bl    imp___stubs__objc_release ; objc_release
ldr    w9, [sp, #0x6a0 + var_204]
tbz    w9, 0x0, loc_100193108
```

Check if file exists:

Cydia.app

```
loc_100192f98:
ldr    x0, [sp, #0x6a0 + var_1B0] ; argument "instance" for method imp___stubs__objc_msgSend, CODE XREF=__T07DVIA_v232JailbreakDetectionViewControllerC20j
adrp   x8, #0x100437000 ; 0x100437f50@PAGE
add    x8, x8, #0xf50 ; 0x100437f50@PAGEOFF, &@selector(defaultManager)
ldr    x1, [x8] ; argument "selector" for method imp___stubs__objc_msgSend, "defaultManager",@selector(defaultManager)
bl    imp___stubs__objc_msgSend ; objc_msgSend
mov    fp, fp
bl    imp___stubs__objc_retainAutoreleasedReturnValue ; objc_retainAutoreleasedReturnValue
adrp   x8, #0x10035d000 ; 0x10035d8a0@PAGE
add    x8, x8, #0x8a0 ; 0x10035d8a0@PAGEOFF, "/Applications/Cydia.app"
mov    w9, #0x17
mov    x1, x9
orr    w2, wzr, #0x1
str    x0, [sp, #0x6a0 + var_1B8]
mov    x0, x8
bl    imp___stubs__T0S25Bp21_builtinStringLiteral_Bw17utf8CodeUnitCountBi1_7isASCIIItcfC ; Swift.String.init(_builtinStringLiteral: Builtin.RawPointer, u
str    x2, [sp, #0x6a0 + var_1C0]
bl    imp___stubs__T0SS10FoundationE19_bridgeToObjectiveCs08NSStringCyF ; (extension in Foundation):Swift.String._bridgeToObjectiveC() -> __C.NSString
ldr    x1, [sp, #0x6a0 + var_1C0]
str    x0, [sp, #0x6a0 + var_1C8]
mov    x0, x1 ; argument "instance" for method imp___stubs__swift_unknownRelease
bl    imp___stubs__swift_unknownRelease ; swift_unknownRelease
adrp   x8, #0x100438000 ; 0x100438250@PAGE
add    x8, x8, #0x258 ; 0x100438250@PAGEOFF, &@selector(fileExistsAtPath:)
ldr    x1, [x8] ; argument "selector" for method imp___stubs__objc_msgSend, "fileExistsAtPath:",@selector(fileExistsAtPath:)
ldr    x0, lsp, #0x6a0 + var_1C8
ldr    x2, [sp, #0x6a0 + var_1B8]
str    x0, [sp, #0x6a0 + var_1D0]
mov    x0, x2 ; argument "instance" for method imp___stubs__objc_msgSend
ldr    x2, [sp, #0x6a0 + var_1D0]
bl    imp___stubs__objc_msgSend ; objc_msgSend
ldr    x1, [sp, #0x6a0 + var_1C8]
str    w0, [sp, #0x6a0 + var_1D4]
mov    x0, x1 ; argument "instance" for method imp___stubs__objc_release
bl    imp___stubs__objc_release ; objc_release
ldr    x0, [sp, #0x6a0 + var_1B8] ; argument "instance" for method imp___stubs__objc_release
bl    imp___stubs__objc_release ; objc_release
ldr    w9, [sp, #0x6a0 + var_1D4]
tbz    w9, 0x0, loc_100193040
```

Check if file exists:

Bash

```

loc_100193128:
ldr    x0, [sp, #0x6a0 + var_210] ; argument "instance" for method imp___stubs___objc_msgSend, CODE XREF=__T07DVIA_v232JailbreakDetectionViewControllerC2
adrp   x8, #0x100437000 ; 0x100437f50@PAGE
add    x8, x8, #0xf50 ; 0x100437f50@PAGEOFF, &@selector(defaultManager)
ldr    x1, [x8]      ; argument "selector" for method imp___stubs___objc_msgSend, "defaultManager",@selector(defaultManager)
bl     imp___stubs___objc_msgSend ; objc_msgSend
mov    fp, fp
bl     imp___stubs___objc_retainAutoreleasedReturnValue ; objc_retainAutoreleasedReturnValue
x8, #0x10035b000 ; 0x10035b107@PAGE
adrp   x8, x8, #0x107 ; 0x10035b107@PAGEOFF, "/bin/bash"
mov    w9, #0x9
mov    x1, x9
orr    w2, wzr, #0x1
str    x0, [sp, #0x6a0 + var_218]
mov    x0, x8
bl     imp___stubs___T0$2$Bp21_builtinStringLiteral_Bw17utf8CodeUnitCountBi1_7isASCIIItcfC ; Swift.String.init(_builtinStringLiteral: Builtin.RawPointer,
str    x2, [sp, #0x6a0 + var_220]
bl     imp___stubs___T0$1$0$FoundationE19_bridgeToObjectiveCSo8NSStringCyF ; (extension in Foundation):Swift.String._bridgeToObjectiveC() -> __C.NSString
ldr    x1, [sp, #0x6a0 + var_220]
str    x0, [sp, #0x6a0 + var_228]
mov    x0, x1      ; argument "instance" for method imp___stubs___swift_unknownRelease
bl     imp___stubs___swift_unknownRelease ; swift_unknownRelease
adrp   x8, #0x100438000 ; 0x100438258@PAGE
add    x8, #0x258 ; 0x100438258@PAGEOFF, &@selector(fileExistsAtPath:)
ldr    x1, [x8]      ; argument "selector" for method imp___stubs___objc_msgSend, "fileExistsAtPath:",@selector(fileExistsAtPath:)
ldr    x0, [sp, #0x6a0 + var_228]
ldr    x2, [sp, #0x6a0 + var_218]
str    x0, [sp, #0x6a0 + var_230]
mov    x0, x2      ; argument "instance" for method imp___stubs___objc_msgSend
ldr    x2, [sp, #0x6a0 + var_230]
bl     imp___stubs___objc_msgSend ; objc_msgSend
ldr    x1, [sp, #0x6a0 + var_228]
str    w0, [sp, #0x6a0 + var_234]
mov    x0, x1      ; argument "instance" for method imp___stubs___objc_release
bl     imp___stubs___objc_release ; objc_release
ldr    x0, [sp, #0x6a0 + var_218] ; argument "instance" for method imp___stubs___objc_release
bl     imp___stubs___objc_release ; objc_release
ldr    w9, [sp, #0x6a0 + var_234]
tbz    w9, 0x0, loc_1001931d0

```

Check if file exists:

sshd

```

loc_1001931f0:
ldr    x0, [sp, #0x6a0 + var_240] ; argument "instance" for method imp___stubs___objc_msgSend, CODE XREF=__T07DVIA_v232JailbreakDetectionViewControllerC2
adrp   x8, #0x100437000 ; 0x100437f50@PAGE
add    x8, x8, #0xf50 ; 0x100437f50@PAGEOFF, &@selector(defaultManager)
ldr    x1, [x8]      ; argument "selector" for method imp___stubs___objc_msgSend, "defaultManager",@selector(defaultManager)
bl     imp___stubs___objc_msgSend ; objc_msgSend
mov    fp, fp
bl     imp___stubs___objc_retainAutoreleasedReturnValue ; objc_retainAutoreleasedReturnValue
x8, #0x10035b000 ; 0x10035b111@PAGE
add    x8, x8, #0x111 ; 0x10035b111@PAGEOFF, "/usr/sbin/sshd"
orr    w9, wzr, #0xe
mov    x1, x9
orr    w2, wzr, #0x1
str    x0, [sp, #0x6a0 + var_248]
mov    x0, x8
bl     imp___stubs___T0$2$Bp21_builtinStringLiteral_Bw17utf8CodeUnitCountBi1_7isASCIIItcfC ; Swift.String.init(_builtinStringLiteral: Builtin.RawPointer,
str    x2, [sp, #0x6a0 + var_250]
bl     imp___stubs___T0$1$0$FoundationE19_bridgeToObjectiveCSo8NSStringCyF ; (extension in Foundation):Swift.String._bridgeToObjectiveC() -> __C.NSString
ldr    x1, [sp, #0x6a0 + var_250]
str    x0, [sp, #0x6a0 + var_258]
mov    x0, x1      ; argument "instance" for method imp___stubs___swift_unknownRelease
bl     imp___stubs___swift_unknownRelease ; swift_unknownRelease
adrp   x8, #0x100438000 ; 0x100438258@PAGE
add    x8, #0x258 ; 0x100438258@PAGEOFF, &@selector(fileExistsAtPath:)
ldr    x1, [x8]      ; argument "selector" for method imp___stubs___objc_msgSend, "fileExistsAtPath:",@selector(fileExistsAtPath:)
ldr    x0, [sp, #0x6a0 + var_258]
ldr    x2, [sp, #0x6a0 + var_248]
str    x0, [sp, #0x6a0 + var_260]
mov    x0, x2      ; argument "instance" for method imp___stubs___objc_msgSend
ldr    x2, [sp, #0x6a0 + var_260]
bl     imp___stubs___objc_msgSend ; objc_msgSend
ldr    x1, [sp, #0x6a0 + var_258]
str    w0, [sp, #0x6a0 + var_264]
mov    x0, x1      ; argument "instance" for method imp___stubs___objc_release
bl     imp___stubs___objc_release ; objc_release
ldr    x0, [sp, #0x6a0 + var_248] ; argument "instance" for method imp___stubs___objc_release
bl     imp___stubs___objc_release ; objc_release
ldr    w9, [sp, #0x6a0 + var_264]
tbz    w9, 0x0, loc_100193298

```

Check if file exists:

apt

```

loc_1001932b8:
ldr    x0, [sp, #0x6a0 + var_270] ; argument "instance" for method imp___stubs___objc_msgSend, CODE XREF=__T07DVIA_v232JailbreakDetectionViewControllerC20j
adrp  x8, #0x100437000 ; 0x100437f500PAGE
add   x8, x8, #0xff50 ; 0x100437f500PAGEOFF, &@selector(defaultManager)
ldr   x1, [x8] ; argument "selector" for method imp___stubs___objc_msgSend, "defaultManager",@selector(defaultManager)
bl    imp___stubs___objc_msgSend ; objc_msgSend
mov   fp, fp
bl    imp___stubs___objc_retainAutoreleasedReturnValue ; objc_retainAutoreleasedReturnValue
x8, #0x10035d000 ; 0x10035d8f80PAGE
add   x8, x8, #0x8f8 ; 0x10035d8f80PAGEOFF, "/etc/apt"
orr   w9, wzr, #0x8
mov   x1, x9
orr   w2, wzr, #0x1
str   x0, [sp, #0x6a0 + var_278]
mov   x0, x8
bl    imp___stubs___T0S2Bp21_builtinStringLiteral_Bw17utf8CodeUnitCountBi1_7isASCIIItcfC ; Swift.String.init(_builtinStringLiteral: Builtin.RawPointer, utf8CodeUnitCount: Builtin.Int32) -> _C.NSString
str   x2, [sp, #0x6a0 + var_280]
bl    imp___stubs___T0S10FoundationE19_bridgeToObjectiveCSo8NSStringCyF ; (extension in Foundation):Swift.String._bridgeToObjectiveC() -> _C.NSString
ldr   x1, [sp, #0x6a0 + var_280]
str   x0, [sp, #0x6a0 + var_288]
mov   x0, x1 ; argument "instance" for method imp___stubs___swift_unknownRelease
bl    imp___stubs___swift_unknownRelease ; swift_unknownRelease
adrp  x8, #0x100438000 ; 0x1004382580PAGE
add   x8, x8, #0x258 ; 0x1004382580PAGEOFF, &@selector(fileExistsAtPath:)
ldr   x1, [x8] ; argument "selector" for method imp___stubs___objc_msgSend, "fileExistsAtPath:",@selector(fileExistsAtPath:)
ldr   x0, [sp, #0x6a0 + var_288]
ldr   x2, [sp, #0x6a0 + var_278]
str   x0, [sp, #0x6a0 + var_290]
mov   x0, x2 ; argument "instance" for method imp___stubs___objc_msgSend
ldr   x2, [sp, #0x6a0 + var_290]
bl    imp___stubs___objc_msgSend ; objc_msgSend
ldr   x1, [sp, #0x6a0 + var_288]
str   w0, [sp, #0x6a0 + var_294]
mov   x0, x1 ; argument "instance" for method imp___stubs___objc_release
bl    imp___stubs___objc_release ; objc_release
ldr   x0, [sp, #0x6a0 + var_278] ; argument "instance" for method imp___stubs___objc_release
bl    imp___stubs___objc_release ; objc_release
ldr   w9, [sp, #0x6a0 + var_294]
tba   w9, 0xb, loc_10019335c

```

Check if cydia can be opened:

```

loc_1001935e0:
ldr   x0, [sp, #0x6a0 + var_348] ; argument "instance" for method imp___stubs___objc_msgSend, CODE XREF=__T07DVIA_v232JailbreakTest4TappedyypF+1
adrp  x8, #0x100438000 ; 0x100438cfcf80PAGE
add   x8, x8, #0xfc8 ; 0x100438cfcf80PAGEOFF, &@selector(sharedApplication)
ldr   x1, [x8] ; argument "selector" for method imp___stubs___objc_msgSend, "sharedApplication",@selector(sharedApplication)
bl    imp___stubs___objc_msgSend ; objc_msgSend
mov   fp, fp
bl    imp___stubs___objc_retainAutoreleasedReturnValue ; objc_retainAutoreleasedReturnValue
adrp  x8, #0x10035d000 ; 0x10035d9380PAGE
add   x8, x8, #0x938 ; 0x10035d9380PAGEOFF, "cydia://package/com.example.package"
mov   w0, #0x23
mov   x1, x9
orr   w2, wzr, #0x1
str   x0, [sp, #0x6a0 + var_350]
mov   x0, x8
bl    imp___stubs___T0S2Bp21_builtinStringLiteral_Bw17utf8CodeUnitCountBi1_7isASCIIItcfC ; Swift.String.init(_builtinStringLiteral: Builtin.RawPointer, utf8CodeUnitCount: Builtin.Int32) -> _C.NSString
bl    imp___stubs___T010Foundation3URLVACgSS6string_tcfC ; Foundation.URL.init(string: Swift.String) -> Foundation.URL
str   x0, [sp, #0x6a0 + var_358]
cbz   x0, loc_100193634

```

```

loc_100193670:
ldr      x0, [sp, #0x6a0 + var_360] ; CODE XREF=__T07DVIA_v232JailbreakDetectionViewControllerC20jailbreakTest4TappedyypF+
str      x0, [sp, #0x6a0 + var_368]
bl       imp___stubs___T010Foundation3URLV19_bridgeToObjectiveCSo5NSURLCyF ; Foundation.URL._bridgeToObjectiveC() -> __C.N
ldr      lr, [sp, #0x6a0 + var_368]
str      x0, [sp, #0x6a0 + var_370]
mov      x0, lr      ; argument "instance" for method imp___stubs__objc_release
bl       imp___stubs__objc_release ; objc_release
adrp   x0, #0x100439000 ; 0x1004396e0@PAGE
add    x0, x0, #0x6e0 ; 0x1004396e0@PAGEOFF, &@selector(canOpenURL:)
ldr      x1, [x0]      ; argument "selector" for method imp___stubs__objc_msgSend, "canOpenURL:",@selector(canOpenURL:)
ldr      x0, [sp, #0x6a0 + var_370]
ldr      lr, [sp, #0x6a0 + var_350]
str      x0, [sp, #0x6a0 + var_378]
mov      x0, lr      ; argument "instance" for method imp___stubs__objc_msgSend
ldr      x2, [sp, #0x6a0 + var_378]
bl       imp___stubs__objc_msgSend ; objc_msgSend
ldr      x1, [sp, #0x6a0 + var_370]
str      w0, [sp, #0x6a0 + var_37C]
mov      x0, x1      ; argument "instance" for method imp___stubs__objc_release
bl       imp___stubs__objc_release ; objc_release
ldr      x0, [sp, #0x6a0 + var_350] ; argument "instance" for method imp___stubs__objc_release
bl       imp___stubs__objc_release ; objc_release
ldr      w8, [sp, #0x6a0 + var_37C]
tbz      w8, 0x0, loc_1001936dc

```

Successfully bypass jailbreak detection:

```

PROBLEMS   OUTPUT   DEBUG CONSOLE   TERMINAL   PORTS
○ evdaezez@evdaezs-Mac-mini scripts % frida -U -l ./jb4.js DVIA-v2
/---|  Frida 16.1.3 - A world-class dynamic instrumentation toolkit
| _ | |
> | Commands:
/_|_| help      -> Displays the help system
. . . object?   -> Display information about 'object'
. . . exit/quit -> Exit
. . .
. . . More info at https://frida.re/docs/home/
. . .
. . . Connected to iPhone (id=dbf1d4c5f4a1dc91993f0d23e966bd3192655422)

[iPhone::DVIA-v2 ]-> fileExistsAtPath: bypassing /Applications/Cydia.app
fileExistsAtPath: bypassing /bin/bash
fileExistsAtPath: bypassing /usr/sbin/sshd
fileExistsAtPath: bypassing /etc/apt
canOpenURL: cydia://package/com.example.package was successful with: 0x1, bypassing.
|
```