R2¢ΘИ 2Ø2I

r2frida Kung-Fu

Better Together

Álex Soler
@as0ler

OCT 2021

$ whoami ALEX SOLER

SECURITY RESEARCHER @ ATTACKIQ

Mobile enthusiastic, specially iOS

R2Frida Trainer

Radare2 Fanboy

Twitter: @as0ler
Github: https://github.com/as0ler

Agenda

1. What is r2frida
2. r2frida 101
3. r2f plugins
4. r2flutch
5. Q&A

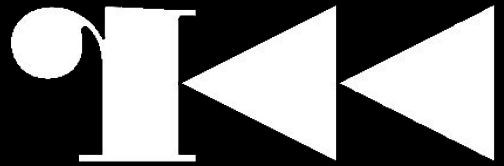
What is R2frida

What is radare2?

- Advanced free/open/libre hexadecimal editor with disassembler, debugger, ...
- Multi-platform, multi-architecture, works on any POSIX system and Windows
- Provides libraries, apis, bindings and scripting to use all the features
- Command-line interface (with visual and embedded web server interfaces)
- Each module can be extended with plugins
- r2pipe is the recommended way to script r2 from ANY language
- Easy to integrate with existing tools

R2pm

- r2pm is the package manager



https://github.com/radareorg/radare2

What is Frida?

- A world-class dynamic instrumentation toolkit
  - Debug live processes
- Scriptable
  - Execute your own debug scripts inside another process
- Multi-platform
  - Windows, macOS, Linux, iOS, Android, QNX
- Highly modular, interacted with via JavaScript API
- Open Source

FRIDA

https://frida.re

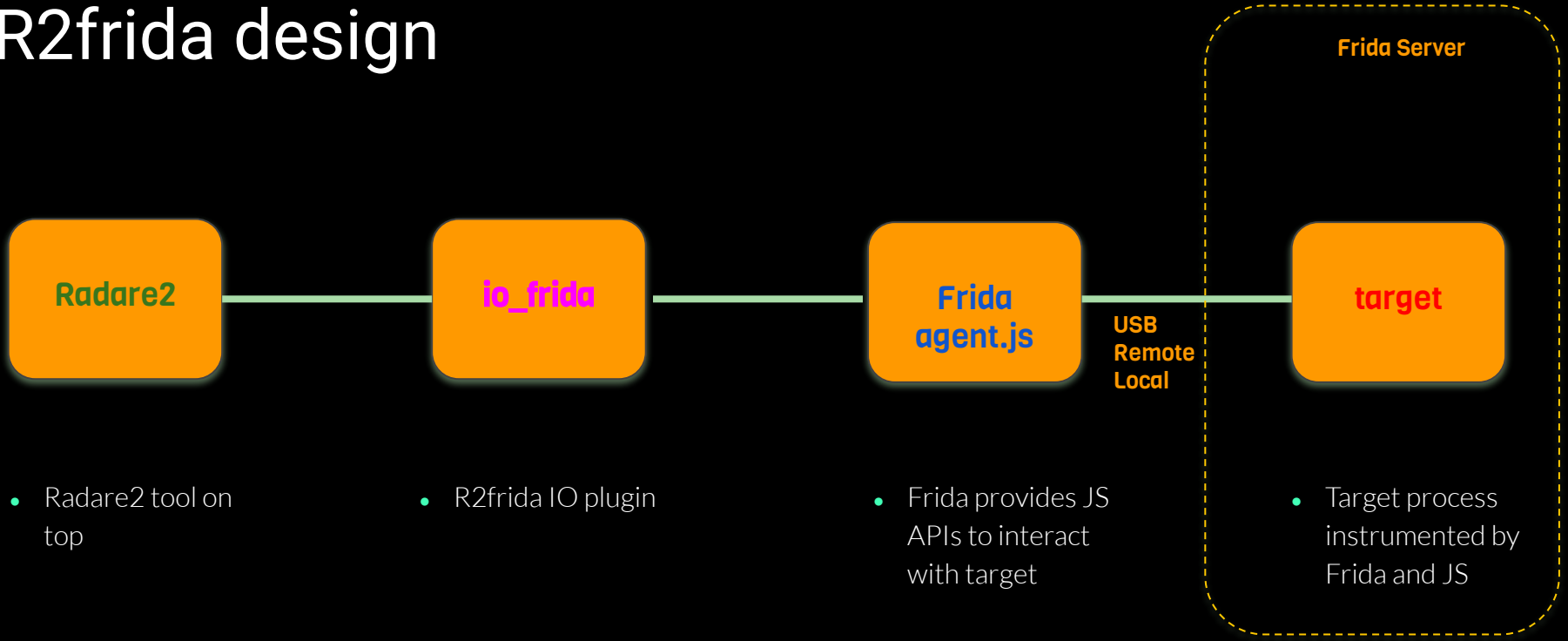
Why not leverage the power of both?

R2Frida

- Radare2 IO plugin to use Frida from r2 shell
- Combines the power of **static** (Radare2) & **dynamic analysis** (Frida)
- Attach to (or spawn) any local or remote process (USB, TCP)
- Ability to read and write memory from target process
  - f.ex to analyze/disassemble the app in memory.
- Frida information loaded into r2 flags
  - maps, symbols, imports, class, methods, fields, …
- Flexibility to build your own r2frida plugins
- Written in C/JavaScript (Open Source)

https://github.com/nowsecure/r2frida

R2frida design



- Radare2 tool on top
- R2frida IO plugin
- Frida provides JS APIs to interact with target
- Target process instrumented by Frida and JS

```
$ r2 frida://attach/usb//re.target.app
[0x00000000]> :?
```

How to install it

Clean previous installations

```
$ r2pm -c r2frida
```

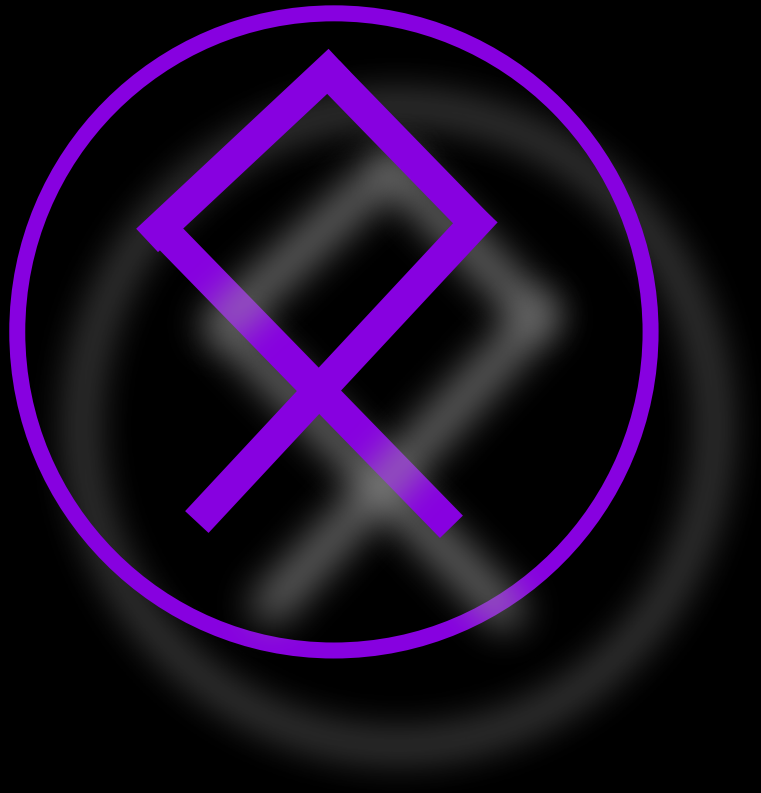
Install latest released version

```
$ r2pm -i r2frida
```

Development environment

```
$ git clone
https://github.com/nowsecure/r2frida
$ cd r2frida
$ make
$ make user-install
```

R2frida 101



Starting up

- Listing devices:
  - r2 frida://usb//

```
~ ▷ r2 frida://usb//
Id                                              Type Name
------------------------------------------------------
d4c30369c116d30e3823298e30468ba67cec90ca     usb iPhone
local                                       local Local System
socket                                     remote Local Socket
```

- Listing running processes:
  - r2 frida://attach/usb/<device>/
  - r2 frida://attach/usb//

- Listing applications:
  - r2 frida://spawn/usb//
  - r2 frida://launch/usb//

```
~ ▷ r2 frida://launch/usb//
PID              Name Identifier
------------------------------
-          AimHarder com.aimharder.mainapp
-           Among Us com.innersloth.amongus
-              Books com.apple.iBooks
-       Burger King®e es.burgerking.burgerking-iphone
-         Calculator com.apple.calculator
-           Calendar com.apple.mobilecal
-              Clock com.apple.mobiletimer
1810          Safari com.apple.mobilesafari
2078    Epic Race 3D com.gym.racegame
```

Starting up

- Attach to an application
  - r2 frida://attach/usb//<App Name>
  - r2 frida://attach/usb//<PID>
- Spawn an application (Process paused)
  - r2 frida://spawn/usb//<package name>
  - Should be resumed using ':dc'
- Launch an application (Process resumed)
  - r2 frida://launch/usb//<package name>

```
~ ▷ r2 frida://attach/usb//"Among
Us"
 -- Everything up-to-date.
[0x00000000]>
```

```
~ ▷ r2 frida://attach/usb//
PID   Name
----------
1     launchd
[...]
23887 Among Us
~ ▷ r2 frida://attach/usb//23887
-- Now 8-bit clean with better ASCII!
[0x00000000]>
```

```
~ ▷ r2 frida://spawn/usb//com.innersloth.amongus
resumed spawned process.
 -- command not found: calc.exe
[0x00000000]>
```

```
~ ▷ r2 frida://spawn/usb//com.innersloth.amongus
 -- I accidentally radared my filesystem today.
[0x00000000]> :dc
resumed spawned process.
```

R2frida Handlers

- If you wanna use R2frida, use these command handlers:
  - **:**
  - **=!**

⚠️ Previous `\` r2f command prefix has been deprecated.

- Asking for help:
  - **:?**
  - **=!?**
- Check Frida Version:
  - **\?V**

```
[0x00000000]> :?
r2frida commands are prefixed with `=!` or `:`.
:. script                   Run script
:  frida-expression         Run given expression inside the agent
/[x|j] <string|hexpairs>    Search hex/string pattern in memory ranges (see search.in=?)
:/v[1248][j] value          Search for a value honoring `e cfg.bigendian` of given width
:/w[j] string               Search wide string
:<space> code..             Evaluate Cycript code
:?                          Show this help
:?e message                 Show message like ?e but from the agent
:?E title message           Show UIAlert dialog with given title and message
:?V                         Show target Frida version
:chcon file                 Change SELinux context (dl might require this)
:d.                         Start the chrome tools debugger
:db (<addr>|<sym>)          List or place breakpoint
:db- (<addr>|<sym>)|*       Remove breakpoint(s)
:dc                         Continue breakpoints or resume a spawned process
:dd[j-][fd] ([newfd])       List, dup2 or close filedescriptors (ddj for JSON)
:di[0,1,-1] [addr]          Intercepts and replace return value of address without calling the function
:dif[0,1,-1] [addr]         Intercepts return value of address after calling the function
:dk ([pid]) [sig]           Send specific signal to specific pid in the remote system
:dkr                        Print the crash report (if the app has crashed)
:dl libname                 Dlopen a library (Android see chcon)
:dl2 libname [main]         Inject library using Frida's >= 8.2 new API
:dlf path                   Load a Framework Bundle (iOS) given its path
:dlf- path                  Unload a Framework Bundle (iOS) given its path
:dm[.|j|*]                  Show memory regions
:dma <size>                 Allocate <size> bytes on the heap, address is returned
```

```
[0x00000000]> :?V
{"version":"15.1.1"}
```

Let’s begin with something easy

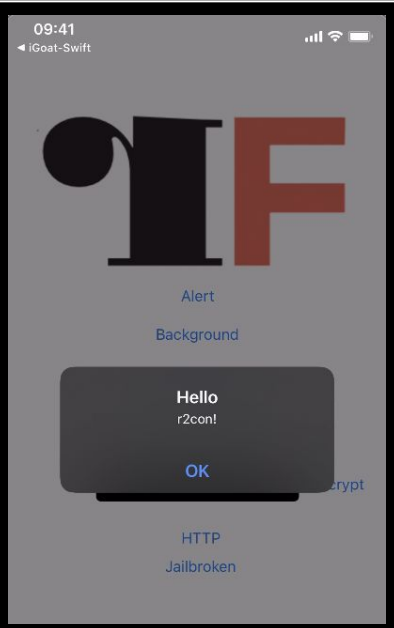
Process info:

```
[0x00000000]> :i
arch                arm
bits                64
os                  darwin
pid                 42421
uid                 501
objc                true
runtime             QJS
swift               false
java                false
mainLoop            true
pageSize            16384
pointerSize         8
codeSigningPolicy   optional
isDebuggerAttached  false
cwd                 /
bundle              me.murphy.demo-objc-app
exename             demo_objc_app
appname
appversion          1.0
appnumversion       16809984
homedir             /var/mobile/Containers/Data/Application/B198DA52-0192-4A38-9F60-2C32A92EC6AF
tmpdir              /private/var/mobile/Containers/Data/Application/B198DA52-0192-4A38-9F60-2C32A92EC6AF/tmp/
bundledir           /private/var/containers/Bundle/Application/2657BA53-9CB1-48B2-93D8-D41E3F23DB1A/demo_objc_app.app
minOS               12.0
```

Let’s begin with something easy

Send messages to the Agent:

```
[0x00000000]> :?E Hello r2con!
```



Execute Frida Code

```
[0x00000000]> :eval Process.arch
arm64
```

Execute Frida Script

```
[0x00000000]> :. ./frida.js
This is a Frida Script. Platform: darwin
```

R2f output can be converted to...

- JSON (using j)

```
[0x00000000]> :ij
{"arch":"arm","bits":64,"os":"darwin","pid":424
21,"uid":501,"objc":true,"runtime":"QJS","swift
":false,"java":false,"mainLoop":true,"pageSize"
:16384,"pointerSize":8,"codeSigningPolicy":"opt
ional","isDebuggerAttached":false,"cwd":"/","bu
ndle":"me.murphy.demo-objc-app","exename":"demo
_objc_app","appname":"","appversion":"1.0","app
numversion":"16809984","homedir":"/var/mobile/C
ontainers/Data/Application/B198DA52-0192-4A38-9
F60-2C32A92EC6AF","tmpdir":"/private/var/mobile
/Containers/Data/Application/B198DA52-0192-4A38
-9F60-2C32A92EC6AF/tmp/","bundledir":{"handle":
"0x283964700"},"minOS":"12.0"}
```

- r2 commands (using *)

```
[0x00000000]> :i*
e asm.arch=arm
e asm.bits=64
e asm.os=darwin
[0x00000000]> .:i*
```

Getting Process Information (:i[liEs])

Library info:

- **:il**
- **:il***
- **.:il***

```
[0x10285c000]> :il
0x000000010285c000 demo_objc_app
0x00000001a48da000 Security
0x000000019ebbf000 Foundation
0x00000001b16ec000 libobjc.A.dylib
0x00000001cc162000 libSystem.B.dylib
0x000000019d8e4000 CoreFoundation
0x00000001cfcd0000 UIKit
0x00000001b642d000 libsqlite3.dylib
...
```

Import info:

- **:ii**
- **:ii libname**
- **.:ii***

```
[0x1046f0000]> :ii
0x1f533de60 v OBJC_METACLASS_$_NSObject
/usr/lib/libobjc.A.dylib
0x1f533de60 v OBJC_METACLASS_$_NSObject
/usr/lib/libobjc.A.dylib
0x1f533de60 v OBJC_METACLASS_$_NSObject
/usr/lib/libobjc.A.dylib
...
```

Export info:

- **:iE**
- **:iE libname**
- **.:iE***

```
[0x10285c000]> :iE
0x10285c000 v _mh_execute_header
0x102861980 f main
0x10286be10 v kRNCryptorAES256Settings
0x10286be78 v kRNCryptorFileVersion
0x10286c2a8 v kRNCryptorErrorDomain
0x10286f198 v OBJC_CLASS_$_MainViewController
...
```

Symbol info:

- **:is**
- **:is libname**
- **.:is***

```
[0x10285c000]> :is
0x102860a6c s -[MainViewController viewDidLoad]
0x102860ab4 s -[MainViewController
changeBgWithColor:]
0x102860e50 s -[MainViewController showAlert]
0x102860f80 s __31-[MainViewController
showAlert]_block_invoke
...
```

Initialize the r2 session

- Check r2 evaluable vars

```
[0x00000000]> :init

e dbg.backend =io
e anal.autoname=true
e cmd.fcn.new=aan
.=!ie*
.=!il*
m /r2f io 0
s entry0
```

- Autoset r2 evaluable vars into the session.
- Seeks to app entrypoint.

```
[0x00000000]> .:init

Mounted io on /r2f at 0x0

[0x104acd790]>
```

Getting Class Information (:ic / :icw)

- List all classes from the app:

```
[0x00000000]> :ic
NSLeafProxy
Object
__NSGenericDeallocHandler
_NSZombie_
__NSMessageBuilder
...
```

- Search for an specific class:

```
[0x102861870]> :ic~Main
WebMainThreadInvoker
NEFileHandleMaintainer
AudioComponentMainRegConnection
MainViewController
```

- List methods of an specific class:

```
[0x102861870]> :ic MainViewController
0x0000000102861870 - isJailbroken
0x0000000102860fd0 - alertBtnPressed:
...
```

- Disassemble an specific method:

```
[0x00000000]> .:ic* MainViewController
[0x00000000]> s sym.objc.MainViewController.isJailbroken
[0x10467d870]> afr
[0x10467d870]> pdf
```

- Get defined classes into the app:

```
[0x10066977c]> :icw~demo
/private/var/containers/Bundle/Application/E2A48562-3B66-4CCA-92E5-
BE479C57AC51/demo_objc_app.app/demo_objc_app MainViewController
/private/var/containers/Bundle/Application/E2A48562-3B66-4CCA-92E5-
BE479C57AC51/demo_objc_app.app/demo_objc_app KeychainManager
/private/var/containers/Bundle/Application/E2A48562-3B66-4CCA-92E5-
BE479C57AC51/demo_objc_app.app/demo_objc_app TransportLayerManager
/private/var/containers/Bundle/Application/E2A48562-3B66-4CCA-92E5-
BE479C57AC51/demo_objc_app.app/demo_objc_app FileManager
/private/var/containers/Bundle/Application/E2A48562-3B66-4CCA-92E5-
BE479C57AC51/demo_objc_app.app/demo_objc_app RNCryptor
/private/var/containers/Bundle/Application/E2A48562-3B66-4CCA-92E5-
BE479C57AC51/demo_objc_app.app/demo_objc_app RNEncryptor
...
```

Mount Remote FS

- Mounts remote filesystem.
- iOS Support
- Allows to access Device Filesystem
  - AppHome: data app container.
  - Device: root fs.
  - AppBundle: application content.

```
[0x00000000]> .:init
Mounted io on /r2f at 0x0
[0x104125924]> ms
[/]> ls
m r2f
[/]> ls r2f
d AppHome
d AppBundle
d Device
[/]>
```

- Allows to download content from the device.

```
[/]> ls /r2f/AppBundle
f r2f-better-together.png
d Base.lproj
d _CodeSignature
f Default-568h@2x.png
d META-INF
f r2frida-icon-120-120.png
f Info.plist
f r2frida.png
f r2frida-icon-180-180.png
f PkgInfo
f Assets.car
f embedded.mobileprovision
f demo_objc_app
f AppIcon60x60@2x.png
[/]> cd /r2f/AppBundle/
[/r2f/AppBundle]> get Info.plist
[/r2f/AppBundle]>
```

Use Case 1: Analyzing iOS method in Memory

- analysis.r2

```
e emu.str = true
e anal.nopskip = false
.:init
.:ii*
.:iE*
.:ic* MainViewController
S
```

- R2 commands:

```
[0x000000000]> . analysis.r2
[0x10093d924]> s sym.objc.MainViewController.isJailbroken
[0x10093d77c]> afr
[0x10093d77c]> pdg
[0x10093d77c]> :e/
[0x10093d77c]> aac;aaef;aa
[0x1009447c8]> s fcn.100944768
[0x100944768]> afn dlsym
```

```
undefined sym.objc.MainViewController.isJailbroken(int64_t arg1, int64_t arg2)

{
    int32_t iVar1;
    code *pcVar2;
    undefined auStack208 [148];
    int32_t iStack60;
    undefined8 uStack56;
    undefined8 uStack48;
    int64_t iStack40;
    int64_t iStack32;
    undefined uStack17;

    uStack48 = 0x1006727cd;
    uStack56 = 0x1006727e5;
    iStack40 = arg2;
    iStack32 = arg1;
    iStack60 = sub.access_100670768(0x1006727cd, 0);
    if (iStack60 == 0) {
        uStack17 = 1;
    }
    else {
        pcVar2 = (code *)sub.dlsym_1006707c8(0xfffffffffffffffd, 0x1006727fa);
        iVar1 = (*pcVar2)(uStack56, auStack208);
        if (iVar1 < 0) {
            uStack17 = 0;
        }
        else {
            uStack17 = 1;
        }
    }
    return uStack17;
}
```

```
[0x10066977c]> ps @ 0x1006727e5
/private/var/lib/apt
[0x10066977c]> ps @ 0x1006727cd
/Applications/Cydia.app
[0x10066977c]> ps @ 0x1006727fa
lstat
[0x10066977c]>
```

Calling the code (:dxo)

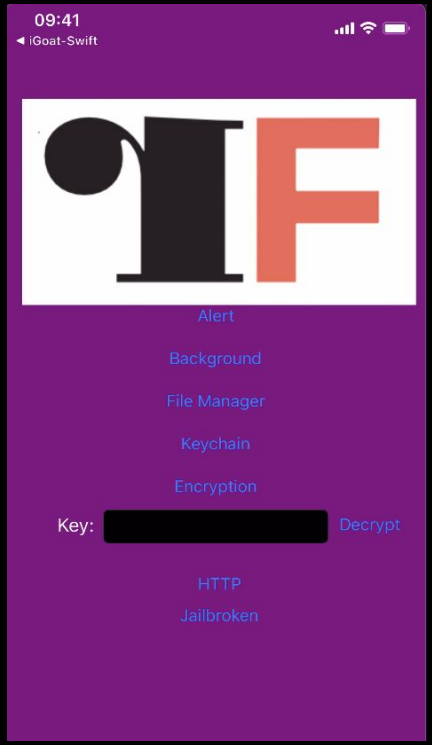
- Only iOS Support
- Allows to call an ObjC method from the application.

- **:dxo <className> <MethodName> <args>**

```
[0x00000000]> :ic MainViewController~changeBg
0x00000001044189c0 - changeBgWithColor:
[0x00000000]> :dxo MainViewController setBackground: 6
```

- Enables to get the function signature
  - **:afs**
    - trace: can be an address or symbol name.
    - Registry: a list of registers.

```
[0x00000000]> :afs MainViewController changeBgWithColor:
void (pointer, pointer, int);
```



Tracing the code (:dt[f,r])

- Enables tracing functions with format.
- **:dtf [addr] [format]**
  - Allows to print argument values

```
[0x00000000]>:dtf?
Usage: dtf [format] || dtf [addr] [fmt]
  ^  = trace onEnter instead of onExit
  +  = show backtrace on trace
 p/x = show pointer in hexadecimal
  c  = show value as a string (char)
  i  = show decimal argument
  z  = show pointer to string
  h  = hexdump from pointer (optional length, h16 to dump 16
bytes)
  H  = hexdump from pointer (optional position of length
argument, H1 to dump args[1] bytes)
  s  = show string in place
  O  = show pointer to ObjC object
```

- Enables tracing functions, obtaining registry values.
  - **:dtr**
    - trace: can be an address or symbol name.
    - Registry: a list of registers.

```
[0x00000000]> :dtr?
 dtr   trace regs
[0x00000000]> :dtr CCKeyDerivationPBKDF x0 x1 x2
```

- Lookup address of a defined symbol.
  - **:isa <name>**

```
[0x00000000]> :isa CCKeyDerivationPBKDF
0x1e5af8e1c
```

Tracing the code (:dt[f,r])

```
[0x00000000]> :dtf CCKeyDerivationPBKDF xz
true
[0x00000000]> [dtf onLeave][Mon Sep 27 2021 19:43:33 GMT+0200] CCKeyDerivationPBKDF@0x1e5af8e1c - args: 0x2, "S3cretPassw0rd!ute", Retval: 0x0 backtrace: 0x10415ac7c
orPassword:salt:settings:],0x10415f1e4 demo_objc_app!-[RNEncryptor initWithSettings:password:IV:encryptionSalt:HMACSalt:handler:],0x10415eee0 demo_objc_app!-[RNEncry
handler:],0x10415e148 demo_objc_app!+[RNEncryptor encryptData:withSettings:password:error:],0x104159ac0 demo_objc_app!-[EncryptionManager encryptData:WithPassword:],
nViewController encryptionBtnPressed:],0x1a029bf2c UIKitCore!-[UIApplication sendAction:to:from:forEvent:],0x19fc2c408 UIKitCore!-[UIControl sendAction:to:forEvent:]
```

```
[0x00000000]> :dtr CCKeyDerivationPBKDF x0 x1 x2
[0x00000000]> [dtr][Mon Sep 27 2021 19:45:08 GMT+0200] 0x1e5af8e1c - registers: {"x0":"0x2","x1":"0x2824e9ac0 (S3cretPassw0rd!)","x2":"0xf"} backtrace: 0x10415ac7c dem
Password:salt:settings:],0x10415f1e4 demo_objc_app!-[RNEncryptor initWithSettings:password:IV:encryptionSalt:HMACSalt:handler:],0x10415eee0 demo_objc_app!-[RNEncryptor
ndler:],0x10415e148 demo_objc_app!+[RNEncryptor encryptData:withSettings:password:error:],0x104159ac0 demo_objc_app!-[EncryptionManager encryptData:WithPassword:],0x10
iewController encryptionBtnPressed:],0x1a029bf2c UIKitCore!-[UIApplication sendAction:to:from:forEvent:],0x19fc2c408 UIKitCore!-[UIControl sendAction:to:forEvent:],0x1
```

- For iOS
  - **:dtf objc: [ClassName]. [MethodName]**

```
[0x00000000]> :dtf objc:MainViewController.isJailbroken
true
[0x00000000]> [dtf onLeave][Mon Sep 27 2021 19:51:10 GMT+0200] objc:MainViewController.isJailbroken@0x10415977c - args: . Retval: 0x1 backtrace: 0x104159608 demo_objc_
breakBtnPressed:],0x1a029bf2c UIKitCore!-[UIApplication sendAction:to:from:forEvent:],0x19fc2c408 UIKitCore!-[UIControl sendAction:to:forEvent:],0x19fc2c748 UIKitCore!
ents:withEvent:],0x19fc2b098 UIKitCore!-[UIControl touchesEnded:withEvent:],0x1a02d6564 UIKitCore!-[UIWindow _sendTouchesForEvent:],0x1a02d7e4c UIKitCore!-[UIWindow se
re!-[UIApplication sendEvent:],0x1a0336e54 UIKitCore!__dispatchPreprocessedEventFromEventQueue,0x1a033b678 UIKitCore!__processEventQueue,0x1a0332964 UIKitCore!__eventF
```

Use Case 2: iOS HTTP Network Monitor

- ios_http_intercept.r2

```
:dtf objc:NSURL.^URLWithString:$ 000
:dtf `:ic NSMutableURLRequest~setHTTPBody:0[0]` 000
:dtf objc:NSURLSession.^uploadTaskWithRequest:fromData:completionHandler:$ 00000
:dtf objc:NSURLSession.^downloadTaskWithRequest:completionHandler:$ 0000
:dtf objc:NSURLSession.^dataTaskWithRequest:completionHandler:$ 0000
:dtf objc:NSURLSession.^dataTaskWithRequest:$ 000
:dtf objc:NSURLSession.^dataTaskWithURL:completionHandler:$ 0000
:dtf objc:NSURLSession.^dataTaskWithURL:$ 000
:e hook.output=json
:e hook.backtrace=false
```


```
[0x00000000]> {"source":"dtf","name":"objc:NSURL.^URLWithString:$","address":"0x19ebcd330","timestamp":"2021-09-28T15:03:14.181Z","values":["NSURL: \"NSURL\"","URLWithString:","nil"],"retval":"0x0"}
{"source":"dtf","name":"objc:NSURL.^URLWithString:$","address":"0x19ebcd330","timestamp":"2021-09-28T15:03:14.182Z","values":["NSURL: \"NSURL\"","URLWithString:","__NSCFString: \"es.burgerking.burgerking-iphone://google/link/?dismiss=1&is_weak_match=1\""],"retval":"0x280662700"}
{"source":"dtf","name":"objc:NSURLSession.^dataTaskWithRequest:$","address":"0x19dfea4e4","timestamp":"2021-09-28T15:03:14.371Z","values":["__NSURLSessionLocal: \"<__NSURLSessionLocal: 0x111e59110>\"","dataTaskWithRequest:","NSMutableURLRequest: \"<NSMutableURLRequest: 0x282ac5750> { URL: https://api.airtouchbk.es/api/v1/news?geocode=08&key=3RtSwmF8KAelm98PaNJJYrRpP7iGONJJuOIlXef9w29Psb3Ue6Lzquu9TrKY39i6&language=en }\""],"retval":"0x111e668b0"}
{"source":"dtf","name":"0x000000019dfef504","address":"0x19dfef504","timestamp":"2021-09-28T15:03:14.372Z","values":["NSMutableURLRequest: \"<NSMutableURLRequest: 0x282afbf90> { URL: https://api.airtouchbk.es/api/v1/news?geocode=08&key=3RtSwmF8KAelm98PaNJJYrRpP7iGONJJuOIlXef9w29Psb3Ue6Lzquu9TrKY39i6&language=en }\"","setHTTPBody:"],"retval":"0x2814f4788"}
{"source":"dtf","name":"objc:NSURL.^URLWithString:$","address":"0x19ebcd330","timestamp":"2021-09-28T15:03:14.376Z","values":["NSURL: \"NSURL\"","URLWithString:","__NSCFString: \"https://api.airtouchbk.es\""],"retval":"0x2803e7c60"}
{"source":"dtf","name":"objc:NSURLSession.^dataTaskWithRequest:$","address":"0x19dfea4e4","timestamp":"2021-09-28T15:03:14.414Z","values":["__NSURLSessionLocal: \"<__NSURLSessionLocal: 0x1119abd80>\"","dataTaskWithRequest:","NSMutableURLRequest: \"<NSMutableURLRequest: 0x282afb3e0> { URL: https://api.airtouchbk.es/api/v1/promotions?geocode=08&key=3RtSwmF8KAelm98PaNJJYrRpP7iGONJJuOIlXef9w29Psb3Ue6Lzquu9TrKY39i6&language=en }\""],"retval":"0x1119aca90"}
{"source":"dtf","name":"objc:NSURLSession.^dataTaskWithRequest:$","address":"0x19dfea4e4","timestamp":"2021-09-28T15:03:14.415Z","values":["__NSURLSessionLocal: \"<__NSURLSessionLocal: 0x11195eb90>\"","dataTaskWithRequest:","NSMutableURLRequest: \"<NSMutableURLRequest: 0x282afb6a0> { URL: https://api.airtouchbk.es/api/v1/coupons?geocode=08&key=3RtSwmF8KAelm98PaNJJYrRpP7iGONJJuOIlXef9w29Psb3Ue6Lzquu9TrKY39i6&language=en }\""],"retval":"0x1119ad580"}
{"source":"dtf","name":"0x000000019dfef504","address":"0x19dfef504","timestamp":"2021-09-28T15:03:14.415Z","values":["NSMutableURLRequest: \"<NSMutableURLRequest: 0x282af4c40> { URL: https://api.airtouchbk.es/api/v1/promotions?geocode=08&key=3RtSwmF8KAelm98PaNJJYrRpP7iGONJJuOIlXef9w29Psb3Ue6Lzquu9TrKY39i6&language=en }\"","setHTTPBody:"],"retval":"0x2814eb488"}
{"source":"dtf","name":"0x000000019dfef504","address":"0x19dfef504","timestamp":"2021-09-28T15:03:14.416Z","values":["NSMutableURLRequest: \"<NSMutableURLRequest: 0x282af4ba0> { URL: https://api.airtouchbk.es/api/v1/coupons?geocode=08&key=3RtSwmF8KAelm98PaNJJYrRpP7iGONJJuOIlXef9w29Psb3Ue6Lzquu9TrKY39i6&language=en }\"","setHTTPBody:"],"retval":"0x2814eb288"}
{"source":"dtf","name":"objc:NSURL.^URLWithString:$","address":"0x19ebcd330","timestamp":"2021-09-28T15:03:14.417Z","values":["NSURL: \"NSURL\"","URLWithString:","__NSCFString: \"https://api.airtouchbk.es\""],"retval":"0x2803e7330"}
{"source":"dtf","name":"objc:NSURL.^URLWithString:$","address":"0x19ebcd330","timestamp":"2021-09-28T15:03:14.419Z","values":["NSURL: \"NSURL\"","URLWithString:","__NSCFString: \"https://api.airtouchbk.es\""],"retval":"0x2803e9c00"}
```

Modifying behaviours (:di and :dif)

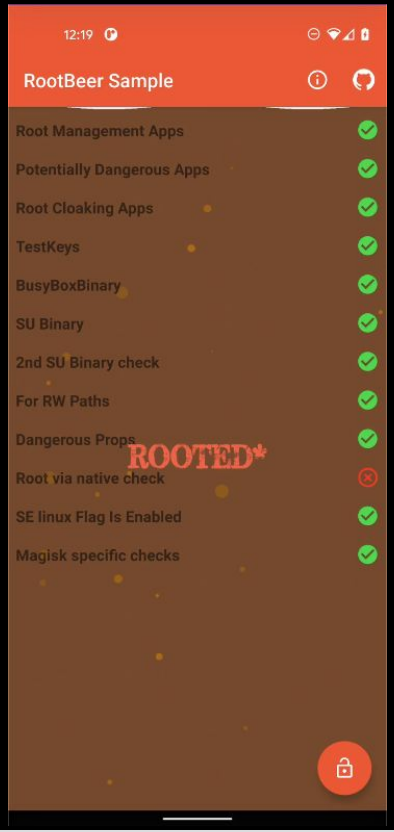
- Allows to modify return values.
- Both methods have support of **objc:** and **java:** method helpers.
- **:dif[0,1,-1] [addr]**
  - Modifies the return value [0,1,-1] after calling the original method.
- **:di[0,1,-1] [addr]**
  - Modifies the return value [0,1,-1] without calling the original method.
- **:dii [addr] [int]**
  - Modifies the return value with the defined int without calling the original method.
- **:dis [addr] [string ptr]**
  - Modifies the return value with the defined string without calling the original method.

```
[0x00000000]> :di?
 di    intercept help
 di-1  intercept ret_1
 di0   intercept ret0
 di1   intercept ret1
 dif   intercept fun help
 dif-1 intercept fun ret_1
 dif0  intercept fun ret0
 dif1  intercept fun ret1
 difi  intercept fun ret int
 difs  intercept fun ret string
 dii   intercept ret int
 dis   intercept ret string
```

Use Case 3: Android AntiRoot Bypass

- Java Checks bypass:

```
[0x000000000]>:di0 java:com.scottyab.rootbeer.RootBeer.checkSuExists
[0x000000000]>:di0 java:com.scottyab.rootbeer.RootBeer.checkForSuBinary
[0x000000000]>:di0 java:com.scottyab.rootbeer.RootBeer.checkForRWPaths
[0x000000000]>:di0
java:com.scottyab.rootbeer.RootBeer.checkForMagiskBinary
[0x000000000]>
[JAVA TRACE][Tue Sep 28 2021 12:17:37 GMT+0200] Intercept return for
com.scottyab.rootbeer.RootBeer:checkForSuBinary with 0
[JAVA TRACE][Tue Sep 28 2021 12:17:37 GMT+0200] Intercept return for
com.scottyab.rootbeer.RootBeer:checkSuExists with 0
[JAVA TRACE][Tue Sep 28 2021 12:17:37 GMT+0200] Intercept return for
com.scottyab.rootbeer.RootBeer:checkForRWPaths with 0
[JAVA TRACE][Tue Sep 28 2021 12:17:37 GMT+0200] Intercept return for
com.scottyab.rootbeer.RootBeer:checkForMagiskBinary with 0
```



Use Case 3: Android AntiRoot Bypass

- Native Checks bypass:

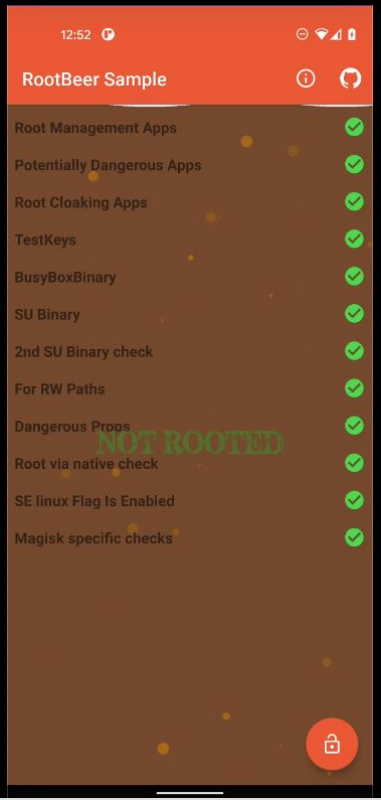
```
[0x71642ee000]> s sym.fun._Z6existsPKc
[0x71642eea18]> afr
[0x71642eea18]> aaef
[0x71642eea18]> aan
[0x71642eea18]> pdg

// WARNING: [r2ghidra] Var arg_30h is stack pointer based, which is not supported for decompilation.

undefined4 sym.fun._Z6existsPKc(int64_t arg1)

{
    int64_t iVar1;
    undefined4 uStack20;

    iVar1 = sub.fopen_71642ee970(arg1, 0x71642eec97);
    if (iVar1 == 0) {
        if (*(int32_t *)0x71642f1000 != 0) {
            sub.__android_log_print_71642ee940(4, 0x71642eec90, 0x71642eecbb, arg1);
        }
        uStack20 = 0;
    }
    else {
        if (*(int32_t *)0x71642f1000 != 0) {
            sub.__android_log_print_71642ee940(4, 0x71642eec90, 0x71642eec99, arg1);
        }
        sub.fclose_71642ee920(iVar1);
        uStack20 = 1;
    }
    return uStack20;
}
[0x71642eea18]>
```

Use Case 3: Android AntiRoot Bypass

- Native Bypass:

```
[0x000000000]>.:il*
[0x000000000]>s `:il~check`
[0x7103bcc000]>.:ii*
[0x7103bcc000]>.:iE*
[0x7103bcc000]>:e hook.output=json
[0x7103bcc000]>:e hook.backtrace=false
[0x7103bcc000]>:dtf `:iE~exist:0[0]` z
[0x7103bcc000]>:di0 `:iE~exist:0[0]`
```


```
[0x7103bcc000]> {"source":"java","class":"com.scottyab.rootbeer.RootBeer","method":"checkForSuBinary","returnValue":0,"timestamp":"2021-09-28T10:52:17.393Z"}
{"source":"java","class":"com.scottyab.rootbeer.RootBeer","method":"checkSuExists","returnValue":0,"timestamp":"2021-09-28T10:52:17.393Z"}
{"source":"java","class":"com.scottyab.rootbeer.RootBeer","method":"checkForRWPaths","returnValue":0,"timestamp":"2021-09-28T10:52:17.394Z"}
{"source":"dtf","name":"0x7103bcca18","address":"0x7103bcca18","timestamp":"2021-09-28T10:52:17.429Z","values":["\"/data/local/su\""],"retval":"0x0"}
{"source":"dtf","name":"0x7103bcca18","address":"0x7103bcca18","timestamp":"2021-09-28T10:52:17.429Z","values":["\"/data/local/bin/su\""],"retval":"0x0"}
{"source":"dtf","name":"0x7103bcca18","address":"0x7103bcca18","timestamp":"2021-09-28T10:52:17.429Z","values":["\"/data/local/xbin/su\""],"retval":"0x0"}
{"source":"dtf","name":"0x7103bcca18","address":"0x7103bcca18","timestamp":"2021-09-28T10:52:17.429Z","values":["\"/sbin/su\""],"retval":"0x0"}
{"source":"dtf","name":"0x7103bcca18","address":"0x7103bcca18","timestamp":"2021-09-28T10:52:17.429Z","values":["\"/su/bin/su\""],"retval":"0x0"}
{"source":"dtf","name":"0x7103bcca18","address":"0x7103bcca18","timestamp":"2021-09-28T10:52:17.429Z","values":["\"/system/bin/su\""],"retval":"0x0"}
{"source":"dtf","name":"0x7103bcca18","address":"0x7103bcca18","timestamp":"2021-09-28T10:52:17.430Z","values":["\"/system/bin/.ext/su\""],"retval":"0x0"}
{"source":"dtf","name":"0x7103bcca18","address":"0x7103bcca18","timestamp":"2021-09-28T10:52:17.430Z","values":["\"/system/bin/failsafe/su\""],"retval":"0x0"}
{"source":"dtf","name":"0x7103bcca18","address":"0x7103bcca18","timestamp":"2021-09-28T10:52:17.430Z","values":["\"/system/sd/xbin/su\""],"retval":"0x0"}
{"source":"dtf","name":"0x7103bcca18","address":"0x7103bcca18","timestamp":"2021-09-28T10:52:17.430Z","values":["\"/system/usr/we-need-root/su\""],"retval":"0x0"}
{"source":"dtf","name":"0x7103bcca18","address":"0x7103bcca18","timestamp":"2021-09-28T10:52:17.430Z","values":["\"/system/xbin/su\""],"retval":"0x0"}
{"source":"dtf","name":"0x7103bcca18","address":"0x7103bcca18","timestamp":"2021-09-28T10:52:17.430Z","values":["\"/cache/su\""],"retval":"0x0"}
{"source":"dtf","name":"0x7103bcca18","address":"0x7103bcca18","timestamp":"2021-09-28T10:52:17.430Z","values":["\"/data/su\""],"retval":"0x0"}
{"source":"dtf","name":"0x7103bcca18","address":"0x7103bcca18","timestamp":"2021-09-28T10:52:17.430Z","values":["\"/dev/su\""],"retval":"0x0"}
{"source":"dtf","name":"0x7103bcca18","address":"0x7103bcca18","timestamp":"2021-09-28T10:52:17.430Z","values":["\"/product/bin/su\""],"retval":"0x0"}
{"source":"dtf","name":"0x7103bcca18","address":"0x7103bcca18","timestamp":"2021-09-28T10:52:17.430Z","values":["\"/apex/com.android.runtime/bin/su\""],"retval":"0x0"}
{"source":"dtf","name":"0x7103bcca18","address":"0x7103bcca18","timestamp":"2021-09-28T10:52:17.430Z","values":["\"/apex/com.android.art/bin/su\""],"retval":"0x0"}
{"source":"dtf","name":"0x7103bcca18","address":"0x7103bcca18","timestamp":"2021-09-28T10:52:17.430Z","values":["\"/system_ext/bin/su\""],"retval":"0x0"}
{"source":"dtf","name":"0x7103bcca18","address":"0x7103bcca18","timestamp":"2021-09-28T10:52:17.430Z","values":["\"/odm/bin/su\""],"retval":"0x0"}
{"source":"dtf","name":"0x7103bcca18","address":"0x7103bcca18","timestamp":"2021-09-28T10:52:17.430Z","values":["\"/vendor/bin/su\""],"retval":"0x0"}
{"source":"dtf","name":"0x7103bcca18","address":"0x7103bcca18","timestamp":"2021-09-28T10:52:17.431Z","values":["\"/vendor/xbin/su\""],"retval":"0x0"}
{"source":"java","class":"com.scottyab.rootbeer.RootBeer","method":"checkForMagiskBinary","returnValue":0,"timestamp":"2021-09-28T10:52:17.431Z"}
```

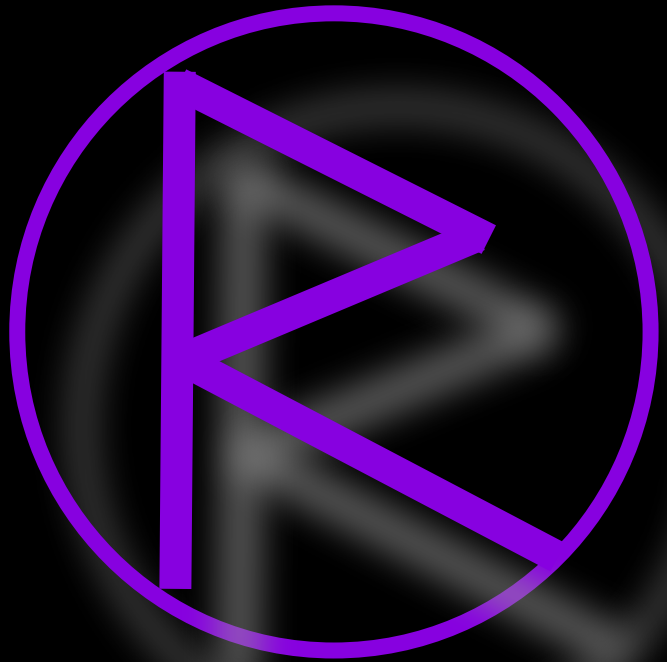
Use Case 3: Android AntiRoot Bypass

- Monitoring open system calls:

```
[0x00000000]>:dtf open z
```

```
[0x71610e5000]> [dtf onLeave][Tue Sep 28 2021 13:17:49 GMT+0200] open@0x7406330664 - args: "/data/local/su". Retval: 0xfff
n+0x54,0x740637ea64 libc.so!fopen+0x54
[dtf onLeave][Tue Sep 28 2021 13:17:49 GMT+0200] open@0x7406330664 - args: "/data/local/bin/su". Retval: 0xffffffff backtr
637ea64 libc.so!fopen+0x54
[dtf onLeave][Tue Sep 28 2021 13:17:49 GMT+0200] open@0x7406330664 - args: "/data/local/xbin/su". Retval: 0xffffffff backt
0637ea64 libc.so!fopen+0x54
[dtf onLeave][Tue Sep 28 2021 13:17:49 GMT+0200] open@0x7406330664 - args: "/sbin/su". Retval: 0xffffffff backtrace: 0x740
bc.so!fopen+0x54
[dtf onLeave][Tue Sep 28 2021 13:17:49 GMT+0200] open@0x7406330664 - args: "/su/bin/su". Retval: 0xffffffff backtrace: 0x7
libc.so!fopen+0x54
[dtf onLeave][Tue Sep 28 2021 13:17:49 GMT+0200] open@0x7406330664 - args: "/system/bin/su". Retval: 0x43 backtrace: 0x740
bc.so!fopen+0x54
[dtf onLeave][Tue Sep 28 2021 13:17:49 GMT+0200] open@0x7406330664 - args: "/system/bin/.ext/su". Retval: 0xffffffff backt
0637ea64 libc.so!fopen+0x54
[dtf onLeave][Tue Sep 28 2021 13:17:49 GMT+0200] open@0x7406330664 - args: "/system/bin/failsafe/su". Retval: 0xffffffff b
0x740637ea64 libc.so!fopen+0x54
[dtf onLeave][Tue Sep 28 2021 13:17:49 GMT+0200] open@0x7406330664 - args: "/system/sd/xbin/su". Retval: 0xffffffff backtr
637ea64 libc.so!fopen+0x54
[dtf onLeave][Tue Sep 28 2021 13:17:49 GMT+0200] open@0x7406330664 - args: "/system/usr/we-need-root/su". Retval: 0xffffff
x54,0x740637ea64 libc.so!fopen+0x54
[dtf onLeave][Tue Sep 28 2021 13:17:49 GMT+0200] open@0x7406330664 - args: "/system/xbin/su". Retval: 0xffffffff backtrace
ea64 libc.so!fopen+0x54
[dtf onLeave][Tue Sep 28 2021 13:17:49 GMT+0200] open@0x7406330664 - args: "/cache/su". Retval: 0xffffffff backtrace: 0x74
ibc.so!fopen+0x54
[dtf onLeave][Tue Sep 28 2021 13:17:49 GMT+0200] open@0x7406330664 - args: "/data/su". Retval: 0xffffffff backtrace: 0x740
bc.so!fopen+0x54
[dtf onLeave][Tue Sep 28 2021 13:17:49 GMT+0200] open@0x7406330664 - args: "/dev/su". Retval: 0xffffffff backtrace: 0x7406
c.so!fopen+0x54
[dtf onLeave][Tue Sep 28 2021 13:17:49 GMT+0200] open@0x7406330664 - args: "/product/bin/su". Retval: 0xffffffff backtrace
ea64 libc.so!fopen+0x54
```

R2f Plugins



R2frida Plugins

- Written in JavaScript.
- Register the plugin via pluginRegister() API.

- Load a plugin from the specified file

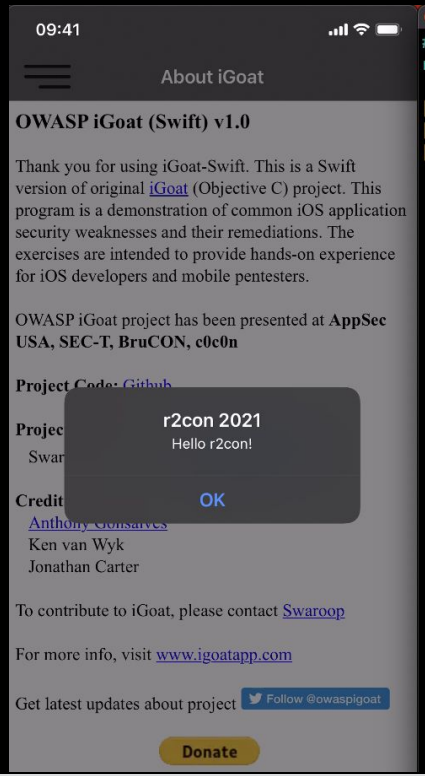
```
[0x00000000]>:. <filename>
```

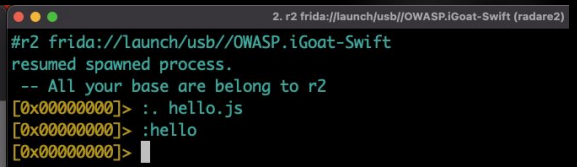
- List loaded plugins:

```
[0x00000000]>:.
```

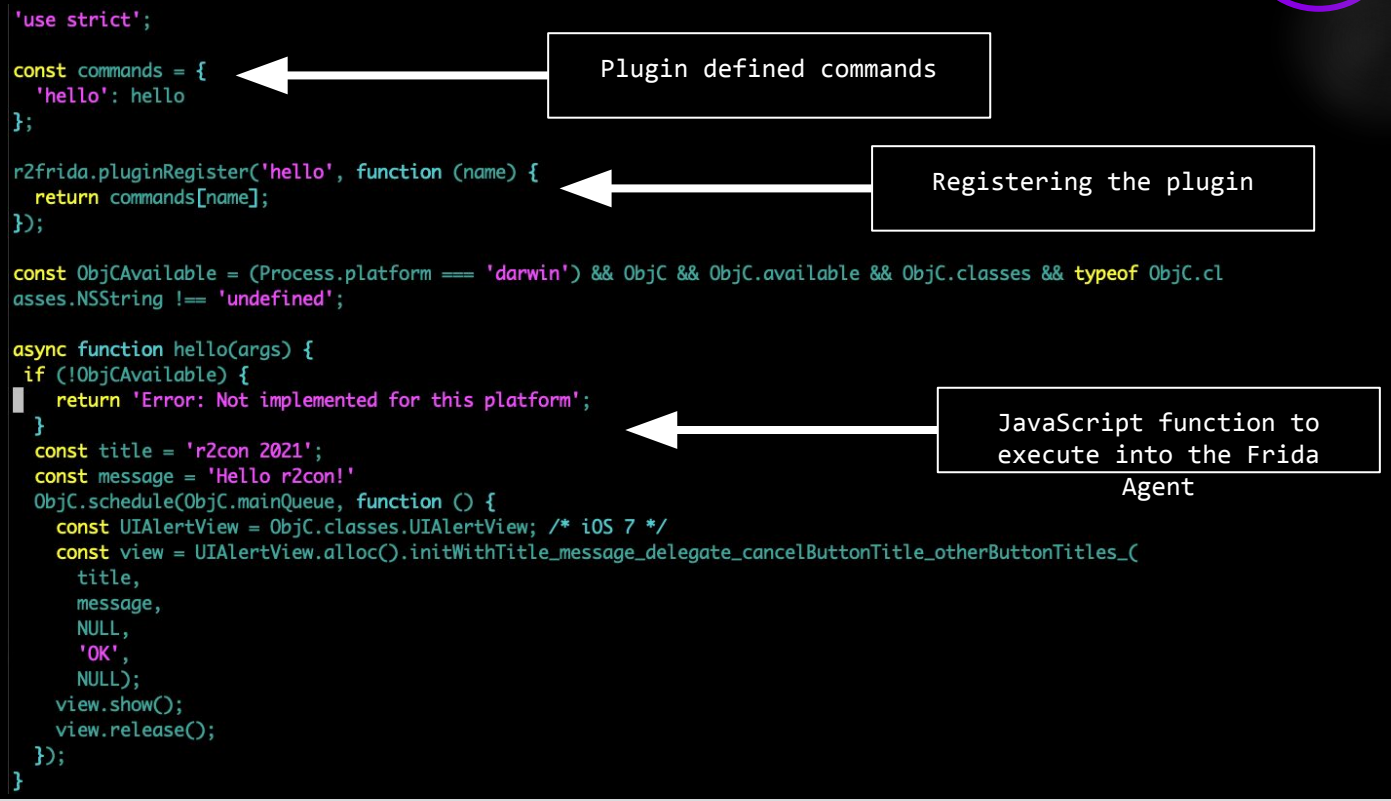
- Unload plugin with the specified name.

```
[0x00000000]>:.-hello
```





r2f Hello World



iOS Symbol Resolver

```
'use strict';

r2frida.pluginRegister('resolver', function (commandName) {
    if (commandName === 'find') {
        return function (args) {
            var query = args.join(' ');
            return new ApiResolver('objc').enumerateMatchesSync(query)
            .map(function (match) {
                return match.address + '\t' + match.name;
            }).join('\n');
        }
    }
});
```

```
#r2 frida://launch/usb//OWASP.iGoat-Swift
resumed spawned process.
 -- Well this is embarrasing ...
[0x00000000]> :. resolver.js
[0x00000000]> :find *[*SQLInjectionExerciseVC* *]
0x1046ef1c4     -[iGoat_Swift.SQLInjectionExerciseVC setSearchField:]
0x1046ef1a4     -[iGoat_Swift.SQLInjectionExerciseVC searchField]
0x1046ef8b4     -[iGoat_Swift.SQLInjectionExerciseVC search]
0x1046ef9ec     -[iGoat_Swift.SQLInjectionExerciseVC initWithCoder:]
0x1046ef8e0     -[iGoat_Swift.SQLInjectionExerciseVC initWithNibName:bundle:]
0x1046efadc     -[iGoat_Swift.SQLInjectionExerciseVC .cxx_destruct]
[0x00000000]>
```

Mach0 Parser in Memory

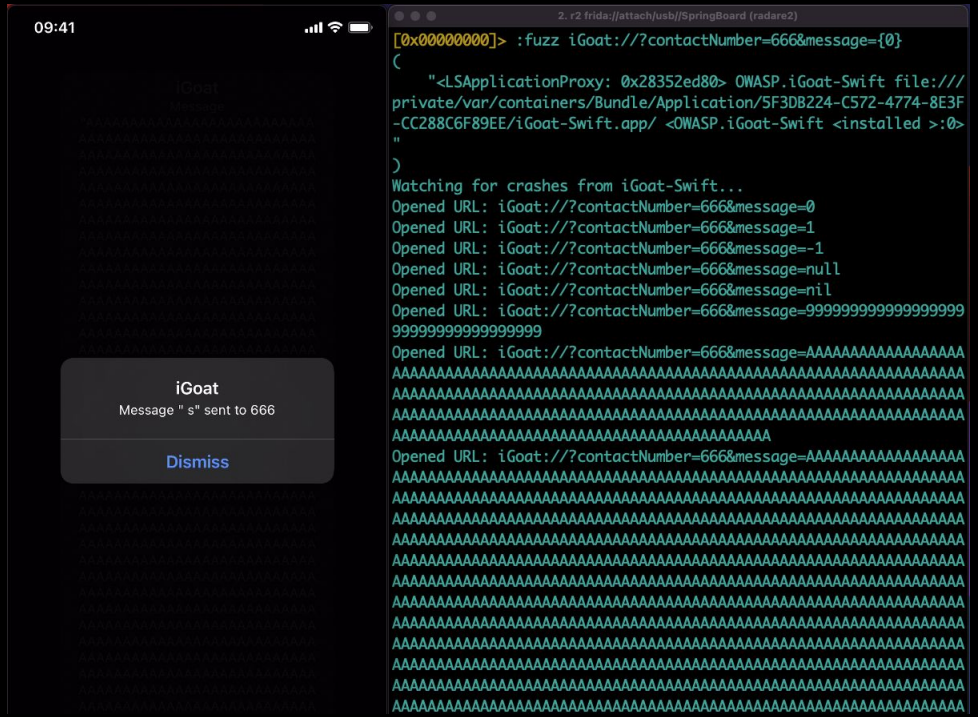
```
#r2 frida://launch/usb//OWASP.iGoat-Swift
resumed spawned process.
 -- THE CAKE IS A PIE
[0x00000000]> :. analyze_macho.js
[0x00000000]> :analyze*
[*] Parsing Macho header at addr: 0x10046c000
[*] Segment __TEXT found at 0x100000000
[*] Segment __DATA found at 0x100238000
[*] Segment __LINKEDIT found at 0x1002bc000
[*] Section __text found at 0x100473d78
[*] Section __stubs found at 0x100642d78
[*] Section __stub_helper found at 0x100644ab8
[*] Section __const found at 0x1006467e0
[*] Section __gcc_except_tab__TEXT found at 0x10064c44c
[*] Section __cstring found at 0x1006516e0
[*] Section __objc_methname found at 0x100677dc3
[*] Section __objc_classname__TEXT found at 0x10069471d
[*] Section __objc_methtype found at 0x100696120
[*] Section __swift5_typeref__TEXT found at 0x10069b2b8
[*] Section __swift5_builtin__TEXT found at 0x10069bbe0
[*] Section __swift5_reflstr__TEXT found at 0x10069bc50
[*] Section __swift5_fieldmd__TEXT found at 0x10069c7f4
[*] Section __swift5_assocty__TEXT found at 0x10069d360
[*] Section __swift5_proto found at 0x10069d390
[*] Section __swift5_types found at 0x10069d3c4
[*] Section __swift5_capture__TEXT found at 0x10069d4b4
[*] Section __swift5_protos found at 0x10069d840
[*] Section __ustring found at 0x10069d848
[*] Section __unwind_info found at 0x10069d8b0
[*] Section __eh_frame found at 0x1006a3a30
[*] Detected LC_ENCRYPTION_INFO_64 at 0x10046cf68
```

```
f macho_header = 0x10046c000;
f segment.__TEXT = 0x10046c000;
f segment.__DATA = 0x1006a4000;
f segment.__LINKEDIT = 0x100728000;
f section.__text = 0x100473d78;
f section.__stubs = 0x100642d78;
f section.__stub_helper = 0x100644ab8;
f section.__const = 0x1006467e0;
f section.__gcc_except_tab__TEXT = 0x10064c44c;
f section.__cstring = 0x1006516e0;
f section.__objc_methname = 0x100677dc3;
f section.__objc_classname__TEXT = 0x10069471d;
f section.__objc_methtype = 0x100696120;
f section.__swift5_typeref__TEXT = 0x10069b2b8;
f section.__swift5_builtin__TEXT = 0x10069bbe0;
f section.__swift5_reflstr__TEXT = 0x10069bc50;
f section.__swift5_fieldmd__TEXT = 0x10069c7f4;
f section.__swift5_assocty__TEXT = 0x10069d360;
f section.__swift5_proto = 0x10069d390;
f section.__swift5_types = 0x10069d3c4;
f section.__swift5_capture__TEXT = 0x10069d4b4;
f section.__swift5_protos = 0x10069d840;
f section.__ustring = 0x10069d848;
f section.__unwind_info = 0x10069d8b0;
f section.__eh_frame = 0x1006a3a30;
```

```
const commands = {
  'decrypt': decrypt,
  'analyze*': analyzeR2,
  'analyzej': analyze
};

r2frida.pluginRegister('r2flutch', function (name) {
  return commands[name];
});

async function analyzeR2(args) {
  const flags = await analyze(args);
  return flags.map(flag => {
    return `f ${flag.name} = ${flag.addr};`;
  }).join('\n');
}
```

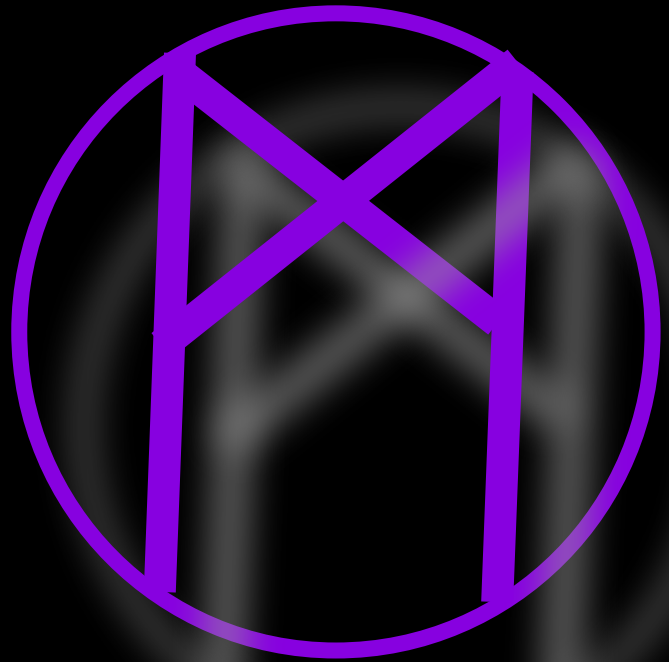
https://github.com/as0ler/r2frida-scripts/blob/main/iOS/plugins/analyze_macho.js

iOS URL Schema Fuzzer

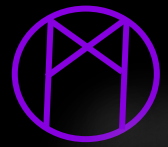


https://github.com/as0ler/r2frida-scripts/blob/main/iOS/plugins/schema_fuzz.js

r2flutch



r2Flutch: Yet another iOS App Decrypter



- Python
- It uses R2pipe + r2frida plugin
- 64 bit Support Only
- It does not requires SSH credentials to download the App Bundle.
- Requirements:
  - Jailbroken device
  - Radare2
  - Frida (installed on the iOS device)

Beta Version: Please open issues to improve it!

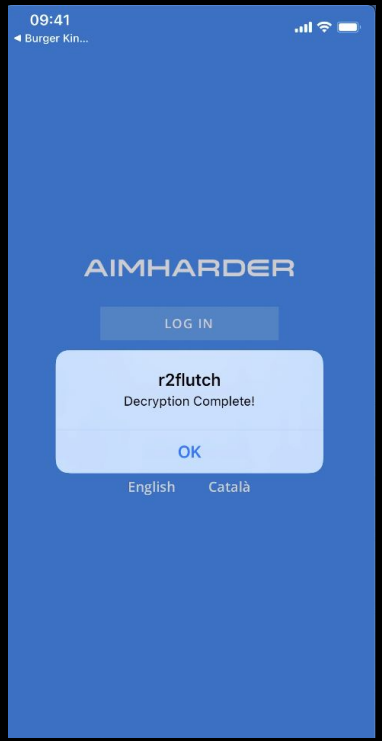
```
~ ▷ r2flutch -h
usage: r2flutch [-h] [-d] [-o OUTPUT] [-i] [-l] [target]

r2flutch (by Murphy)

positional arguments:
  target                Bundle identifier of the target app

optional arguments:
  -h, --help            show this help message and exit
  -d, --debug           Show debug messages
  -o OUTPUT, --output OUTPUT
                        Path where output files will be stored.
  -i, --ipa             Generate an IPA file
  -l, --list            List the installed apps
~ ▷
```

r2Flutch: Yet another iOS App Decrypter

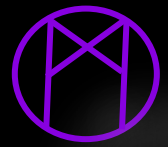
- Installation
  - pip install r2flutch
  - r2pm -ci r2flutch

- **r2flutch -l**
  - List all the installed apps.
- **r2flutch <app bundle>**
  - Downloads the decrypted binary
- **r2flutch -i <app bundle>**
  - Downloads the whole app bundle as an IPA

- Source code:
  - https://github.com/as0ler/r2flutch



r2Flutch: Yet another iOS App Decrypter



- **DEMO**

```
~ ▷ r2flutch -i com.aimharder.mainapp
[+] Open Application Process com.aimharder.mainapp
resumed spawned process.
[+] Mount Application Bundle
Mounted io on /r2f at 0x0
[+] Set block size to 0x80000

[+] Loading all modules
[+] Dumping Module AimHarder at 0x104c57000 (0x1000 Bytes)
Dumped 4096 bytes from 0x104c57000 into /var/folders/bm/ghnl8v_119d5dfh3vk58mwbc0000gn/T/r2flutch-4csaafwj/dump/AimHarder
File 'AimHarder' created. (size: 5008688 bytes)
[+] Writing decrypted data to file /var/folders/bm/ghnl8v_119d5dfh3vk58mwbc0000gn/T/r2flutch-4csaafwj/bin/AimHarder at 0x7000
[+] Patching cryptid at offset 0xca8
[+] Module /var/folders/bm/ghnl8v_119d5dfh3vk58mwbc0000gn/T/r2flutch-4csaafwj/bin/AimHarder successfully decrypted
[+] Copy application bundle to: /var/folders/bm/ghnl8v_119d5dfh3vk58mwbc0000gn/T/r2flutch-4csaafwj/Payload/AimHarder.app
[+] Copy App Bundle to disk
100%| 937/937 [00:45<00:00, 20.37it/s]
[+] Creating IPA file at ./AimHarder.ipa
[+] IPA file saved at ./AimHarder.ipa
[*] SUCCESS - r2flutch Decryption Complete!
~ ▷
```

Credits

This is where we give credit to the ones who help to this workshop

- **@enovella and @hexploitable for their contributions and trainings about r2frida.**
- **@pancake** for the Radare2 project and all his contributors.
- **@oleavr** for the Frida project and all his contributors.
- **@mrmacete** for r2frida support and all his contributors.
- All project-related contributors.

References

- r2flutch Source code: https://github.com/as0ler/r2flutch
- r2frida plugins and examples: https://github.com/as0ler/r2frida-scripts
- r2Clutch Patching iOS binaries (r2con 2016): http://slides.com/as0ler/r2clutch
- Official r2frida source: https://github.com/nowsecure/r2frida
- Official r2frida Gitbook (WIP): https://github.com/nowsecure/r2frida-book
- Unofficial r2frida-wiki: https://github.com/enovella/r2frida-wiki
- r2con 2017: r2frida: https://github.com/radareorg/r2con2017/blob/master/talks/r2frida/r2frida-r2con-2017.pdf

Videos

- r2con 2016: the ultimate static analysis on dynamic steroids - https://www.youtube.com/watch?v=ivCucqeVeZI
- r2con 2017: r2frida - https://www.youtube.com/watch?v=URyd4bcV-Ik
- Pass the Salt 2018: R2frida Better Together - https://passthesalt.ubicast.tv/videos/r2frida-better-together
- R2con 2020 r2frida Workshop: https://www.youtube.com/watch?v=sgNDYgLyAP4&t=8661s

Thank you!