NowSecure®

From Internals to Insights

Reversing React, Flutter and Unity apps with Radare2

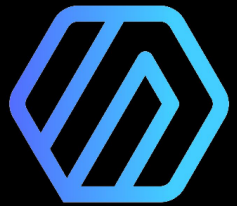
pancake@nowsecure.com
@pancake@infosec.exchange



MAScon Berlin
October 2026

Who am I?

- Sergi Alvarez i Capilla (aka **pancake**)
- Author of **radare2** and other free software
- Mobile **Security Research** Engineer at **NowSecure**


| © Copyright 2026 NowSecure, Inc. All Rights Reserved. Proprietary information. Do not distribute.

NowSecure®

From Internals



MAScon Berlin
October 2026

Blast from Vienna's MasCon

In MasCon Vienna, we went deep down into the low level internal details of **React Native**, **Unity** and **Flutter** frameworks and explored some fun tricks and optimizations that may be interesting for reverse engineering those apps for iOS or Android.

Presented the 3 plugins for radare2.

You can find the slides here:

`https://radare.org/get/r2mascon2026-vienna-mobiletriad.pdf`

| © Copyright 2026 NowSecure, Inc. All Rights Reserved. Proprietary information. Do not distribute.

Today’s Menu

Today, we go for a more practical and fully static perspective:

- Quick introduction, installation of the toolchain and plugins
- Overview of **Unity**, **React** and **Flutter** from the reverser POV
- Extract details from apps, find key places, patch instructions, profit



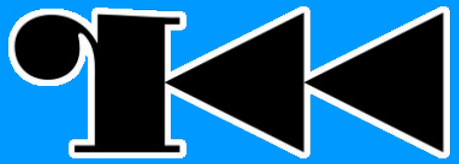
NowSecure®

Setup



MAScon Berlin
October 2026

What's Radare2?



+20yo Free and Open Source Multiplatform Unix Friendly Reversing Framework

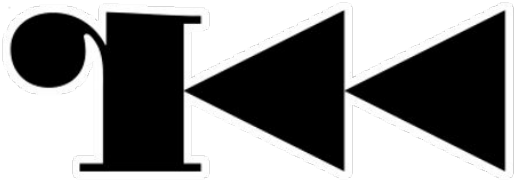
https://radare.org

- Widely known a set of easily scriptable commandline tools
- Built on top of several libraries, extensible with plugins
- CLI repl, Visual/Panels mode
- Also ships a webserver to expose webuis
- Builds for WASM (https://radare.org/jslr2)
- Several frontends:
  - QT UI (iaito), r2 web, r2mcp and r2ai

| © Copyright 2026 NowSecure, Inc. All Rights Reserved. Proprietary information. Do not distribute.

Setting up Radare2

As usual r2 and the plugins:



```
$ curl -sL radare.org/install | sh
```

jk, you have releases binaries in github/flatpak/snap/termux/...

```
$ git clone https://github.com/radareorg/radare2
$ radare2/sys/install.sh
```

Install Iaito if you want a fancy GUI QT gui

- https://github.com/radareorg/iaito

| © Copyright 2026 NowSecure, Inc. All Rights Reserved. Proprietary information. Do not distribute.

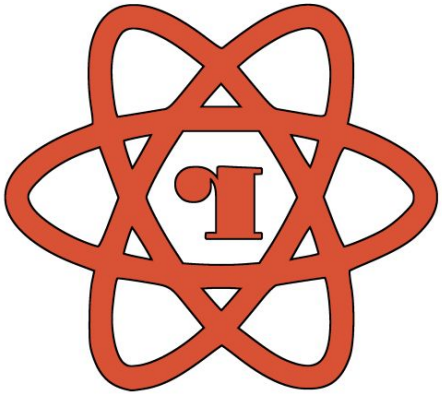
The infamous Mobile development Triad

Solved in just 3 plugins and cli programs for radare2:

```
r2pm -ci r2unity
```



```
r2pm -ci r2hermes
```



```
r2pm -ci r2flutter
```

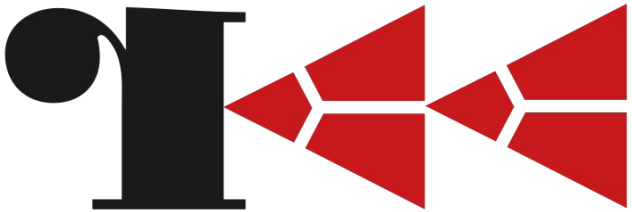


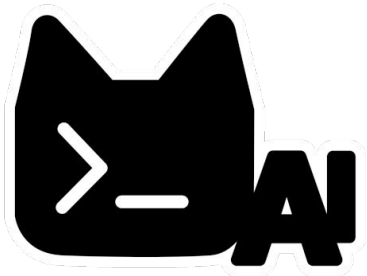
| © Copyright 2026 NowSecure, Inc. All Rights Reserved. Proprietary information. Do not distribute.

The infamous Mobile development Triad

Those plugins provide new commands in r2 so you can learn them, or just tell r2mcp, r2ai or your favourite agent to use them for you.

I won’t go into details about how to use radare2... who needs docs?







| © Copyright 2026 NowSecure, Inc. All Rights Reserved. Proprietary information. Do not distribute.

NowSecure

Basic Theory



MAScon Berlin
October 2026

Unity

Cross Platform Game Engine



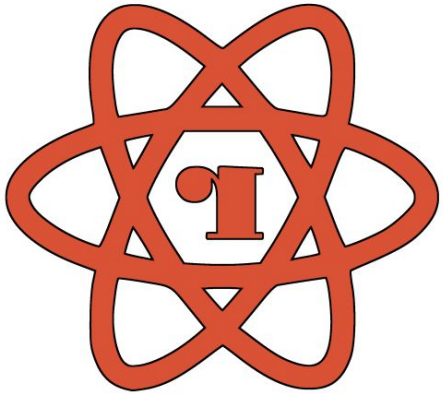
- Written in C# and transpiles to C++
- Compiled as native code into PE / ELF / MACHO
  - libil2cpp.so, GameAssembly
- Ecma335 global-metadata.dat
  - Data/Managed/Metadata
- Supports arm32/64 x86-32/64
- Serialized assets v22
- Supports from 2017 to 2023 (Unity6)

| © Copyright 2026 NowSecure, Inc. All Rights Reserved. Proprietary information. Do not distribute.

React Native

Javascript Bytecode interpreter VM by Meta

- Apps written in TypeScript
- Reuse the NPM ecosystem
- Interacts with native code
- Supports from v51 to v99
- Assembler, Disassembler and Decompiler
- Patch sha1 integrity hash



| © Copyright 2026 NowSecure, Inc. All Rights Reserved. Proprietary information. Do not distribute.

Flutter

The Google response to multiplatform



- Apps from Dart 2.10 to 3.12
- Compiles into an AOT library
- Custom ABI for arm64 and x64
- Loads obfuscated map files

Other alternatives require docker + flutter sdk for each version > 2GB
r2flutter is just 300KB and covers all the versions and archs

| © Copyright 2026 NowSecure, Inc. All Rights Reserved. Proprietary information. Do not distribute.

Flutter

Very Unstable ABI.. version is sha1 of the sdk headers

Dart VM	PatchClass	Library	Namespace	Code	Object Pool	Array	String	OneByteString	NumPredefined
2.10.0	5	13	14	16	20	78	80	81	156
2.13.0	5	11	12	15	18	75	77	78	148
2.14.0	5	12	13	16	20	79	81	82	152
2.15.0	6	13	14	17	21	79	82	83	153
2.19.0	6	13	14	17	21	89	92	93	176
3.0.5	6	13	14	18	22	90	93	94	177
3.4.3	6	13	14	18	22	89	92	93	174
3.10.7	6	13	14	18	23	90	93	94	175



| © Copyright 2026 NowSecure, Inc. All Rights Reserved. Proprietary information. Do not distribute.

NowSecure®

Hands On



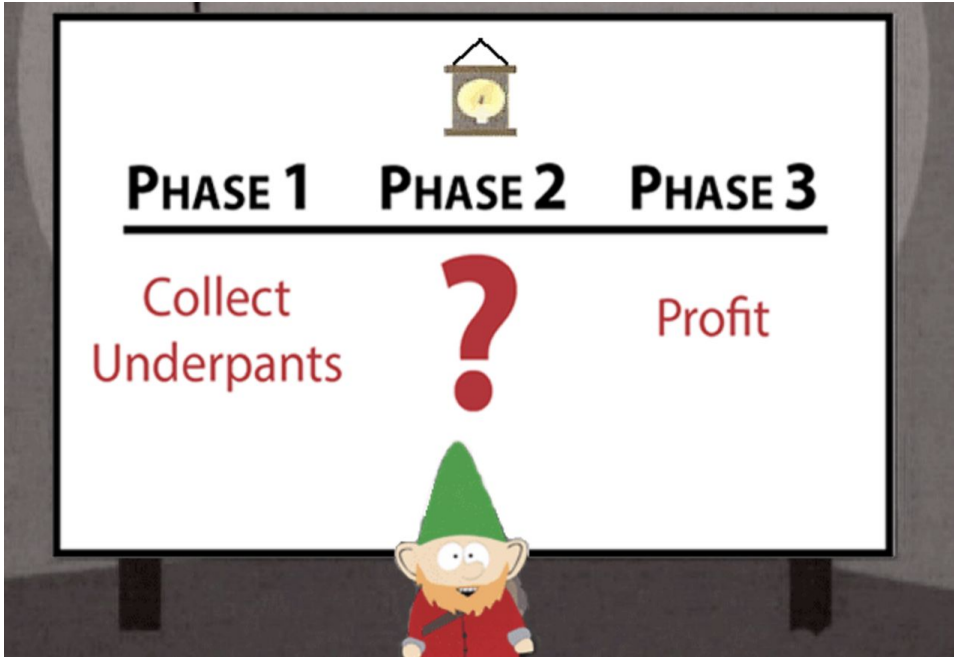
MAScon Berlin
October 2026

Static Analysis

Radare2 ships a native debugger and also plays well with Frida or GDB/LLDB.

Static approach is easier to reproduce, scales better and gives us to get a good understanding of the target.

Collect data, do things and boom!



| © Copyright 2026 NowSecure, Inc. All Rights Reserved. Proprietary information. Do not distribute.

SBOM

Identifying which libraries have been used to build an app is important to understand the capabilities, vulnerable versions.

```
$ (r2flutter | r2unity | r2hermes) -S
```

The optional -j outputs the SBOM in CycloneDX format.

- **R2Flutter** can recover Dart Package names (not versions)
  - We could if we generate signatures
- **R2Unity** recovers everything
- **R2Hermes** infused from strings

| © Copyright 2026 NowSecure, Inc. All Rights Reserved. Proprietary information. Do not distribute.

ResoUrces (iu)

React Native apps use to embed blobs as base64 or data uris as strings.

Unity games package all data into assets.

- UnityFramework <- il2cpp output
- maps from global-metadata

```
1$ r2 Data/sharedassets0.assets
 -- what happens in #radare, stays in #radare
[0x00000000]> iu
Resource 0
  name: Default-Skybox
  id: -
  named: true
  timestamp: -
  origin: SerializedFile.path_2
  vaddr: 0x00000180
  paddr: 0x00000180
  size: 268
  type: Unity.Material
  type_id: 21
  language: -
  language_id: 4294967295
  codepage: 0
[0x00000000]>
```

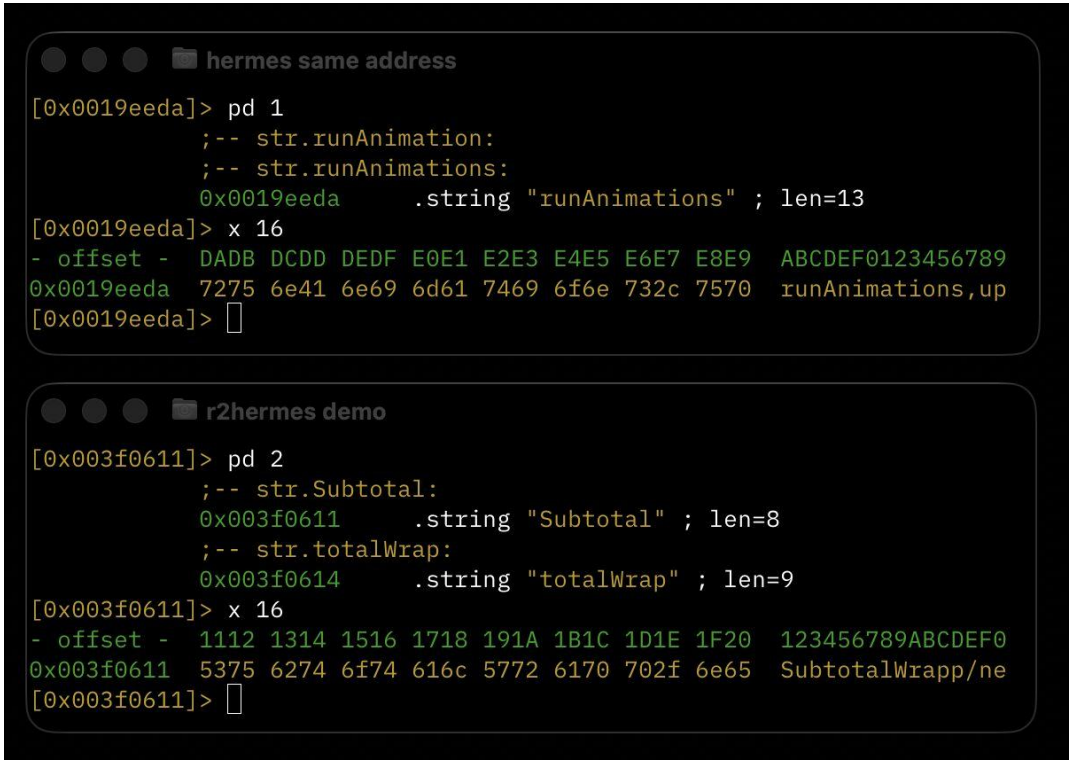

| © Copyright 2026 NowSecure, Inc. All Rights Reserved. Proprietary information. Do not distribute.

Strings and Xrefs

In Hermes, we have utf16 interlaced strings.

- R2 is the only disassembler capable to represent this

R2Flutter-AA find strings, the refs to the constant pool, and then the refs from cp to code.



| © Copyright 2026 NowSecure, Inc. All Rights Reserved. Proprietary information. Do not distribute.

Strings and Xrefs

```
0$ r2 libapp.so
 -- To debug a program, you can call r2 with 'dbg://<path-to-program>' or '-d <path..>'
[0x00170000]> r2flutter-AAA
INFO: Flutter analysis: 10178 functions, 47498 calls, 0 fields, 71 classes, 0 types, 4593 strings, 23073 PP refs,
[0x00170000]> s str.password123
[0x0003a857]> pd 1
            ;-- str.password123:
            ;-- dart.str.password123.0x3a857:
            ; STRN XREF from str.ApA @ +0x1361(r)
            ; STRN XREF from method._PasswordPageState_417334925._checkPassword_417334925 @ 0x2be0ec(r)
            0x0003a857     .string "password123" ; len=12
[0x0003a857]> s method._PasswordPageState_417334925._checkPassword_417334925
[0x002be0ac]> pd 20
            ;-- dart.method._PasswordPageState_417334925._checkPassword_417334925.0x2be0ac:
            ; CALL XREF from fcn.002be074 @ 0x2be094(x)
            ; CALL XREF from method._PasswordPageState_417334925._anon_closure @ 0x2be90c(x)
┌ 444: void *method._PasswordPageState_417334925._checkPassword_417334925 (_PasswordPageState_417334925 *this);
│ `- args(x1, sp[0x10..0x18]) vars(3:sp[0x8..0x18])
; method._PasswordPageState_417334925._checkPassword_417334925 | dart:
; method._PasswordPageState_417334925._checkPassword_417334925
│           0x002be0ac      fd79bfa9       stp x29, x30, [x15, -0x10]!
│           0x002be0b0      fd030faa       mov x29, x15
│           0x002be0b4      efa100d1       sub x15, x15, 0x28
```


| © Copyright 2026 NowSecure, Inc. All Rights Reserved. Proprietary information. Do not distribute.

Interoperability with Native APIs

GlobalMetadata ships all the dotnet metadata, we can find out imports and exports (managed vs native methods)

$ r2unity-P
$ r2unity-R

```
[0x00004000]> r2unity-P
# P/Invoke methods (managed -> native), wire version 39
# IMAGE METHOD  DLL     ENTRY   FLAGS   CONFIDENCE
mscorlib.dll    Sys.CloseDir    <unresolved>    <default>       internal static extern
mscorlib.dll    Sys.ConvertErrorPalToPlatform   <unresolved>    <default>   internal stati
mscorlib.dll    Sys.ConvertErrorPlatformToPal   <unresolved>    <default>   internal stati
mscorlib.dll    Sys.GetNonCryptographicallySecureRandomBytes    <unresolved><default>
mscorlib.dll    Sys.GetReadDirRBufferSize       <unresolved>    <default>   internal stati
mscorlib.dll    Sys.LChflagsCanSetHiddenFlag    <unresolved>    <default>   private statio
mscorlib.dll    Sys.LStat       <unresolved>    <default>       internal static extern
mscorlib.dll    Sys.OpenDir     <unresolved>    <default>       internal static extern
mscorlib.dll    Sys.ReadDirR    <unresolved>    <default>       internal static extern
mscorlib.dll    Sys.ReadLink    <unresolved>    <default>       private static extern
mscorlib.dll    Sys.Stat        <unresolved>    <default>       internal static extern
mscorlib.dll    Sys.Stat        <unresolved>    <default>       internal static extern
# summary: pinvokes=21
[0x00004000]>
```

```
[0x00004000]> r2unity-R
# Reverse-P/Invoke methods (native -> managed), wire version 39
# IMAGE METHOD  ATTRIBUTE       FLAGS   CONFIDENCE
mscorlib.dll    System.Globalization.CultureInfo.OnCultureInfoChangedInAppX
mscorlib.dll    System.Threading.OSSpecificSynchronizationContext.InvocationEntry
# summary: reverse_pinvokes=2
[0x00004000]>
```


| © Copyright 2026 NowSecure, Inc. All Rights Reserved. Proprietary information. Do not distribute.

Decompilation

Hermes bytecode is a javascript VM, with some custom optimizations, the pd:h command exposes the decompiler inside r2.

For Unity and Dart we can use decai or r2ai.

- Take the output from pdc/pdg/.. and fed an LLM

Spoiler: I am working on a native decompiler that can render Swift, CSharp, Dart, TypeScript, ObjC, C++, C, Python, ... and works well with all the semantics and runtimes specific to each target.

| © Copyright 2026 NowSecure, Inc. All Rights Reserved. Proprietary information. Do not distribute.

Boolean Patches

Changing a function that returns bool in Dart is not just return 0 or 1.

Dart have 2 heap objects, the PP (pool pointer) x27 (r15 on x64)

- Fast lookup of common constants indexed by x22 register
- x22 is also known as the null register

Dart value	Address	AArch64 instruction	Bytes	Register-level encoding
null	closure 0x003971c8	mov x0, x22	e0 03 16 aa	x22 itself = Dart null
true	closure 0x0039b594	add x0, x22, #0x20	c0 82 00 91	x22 + 0x20
false	closure 0x003a02f4	add x0, x22, #0x30	c0 c2 00 91	x22 + 0x30
42	sym.returnNumber 0x00245a40	mov x0, #0x54	80 0a 80 d2	SMI: 42 << 1 = 0x54
"Hello from Dart"	sym.returnString 0x00245a0c	ldr x0, [x27, #0x68]	60 37 40 f9	pooled object via PP (x27)

| © Copyright 2026 NowSecure, Inc. All Rights Reserved. Proprietary information. Do not distribute.

Reversing with Curl

radare2 can start a background webserver, so you can just run commands in background while having your iaito/r2 shell loaded and fully interactive.

$ r2 -e http.port=9090 -c'=h &' /path/to bin

$ curl -d 'pd 20' http://localhost:9090/cmd

> Tell pmai to find the password

| © Copyright 2026 NowSecure, Inc. All Rights Reserved. Proprietary information. Do not distribute.

NowSecure®

Q&A



MAScon Berlin
October 2026

Thank you!



MAScon Berlin
October 2026