The complexity of reversing Flutter applications

Axelle Apvrille, Fortinet

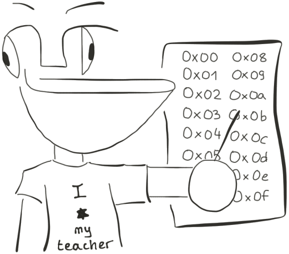
Nullcon, March 2024

Who am I?

Axelle Apvrille

Principal Security Researcher at **Fortinet**, @cryptax
Lead organizer of **Ph0wn CTF**
I analyze **Android malware** and **IoT** malware

Goal of this talk



Understand how to reverse Flutter applications with a special focus on Android malware

sub-goal: solve GreHack CTF 2023 Dart challenge

Dart is an **object**-oriented programming language with a **C-style** syntax

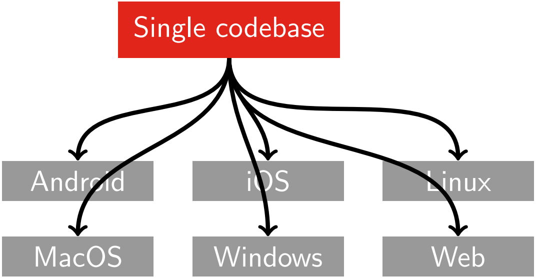
```dart
class Hello {
  void sayHello() {
    print("Hello Nullcon!");
  }
}

void main() {
  var hello = Hello();
  hello.sayHello();
}
```

Dart: 4 output formats

Output format	Size	Time
Self contained	5,919,728	0,006s
AOT snapshot	873,440 **14%**	0,012s **2x**
JIT snapshot	4,924,048 **83%**	0,333s **55x**
Kernel snapshot	1968 **0.03%**	0,411s **68x**

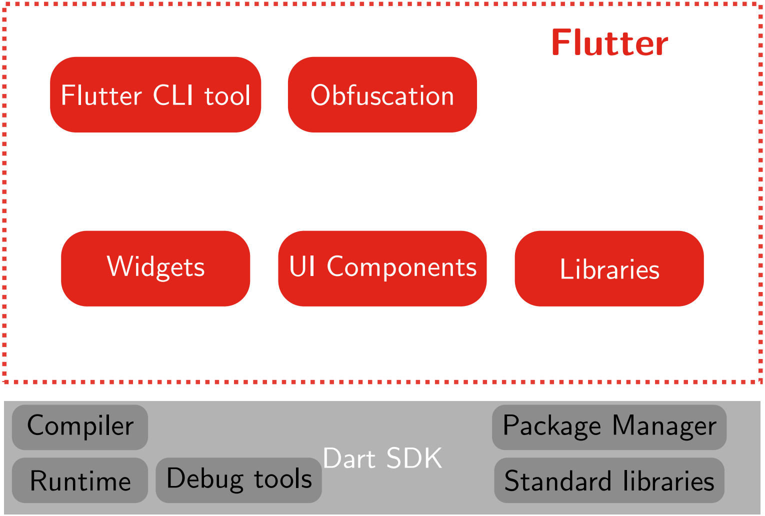
```
dart compile exe|aot-snapshot|jit-snapshot|kernel file.dart
```

Dart can be natively compiled for multiple platforms



Dart	**Java**
Native machine code	Byte code
Android and iOS: apps bundled with a Dart VM runtime	Android and iOS: JVM for mobile exists but primarily for dev and testing.

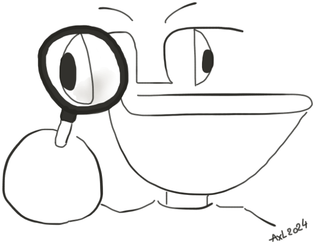
Flutter uses the Dart language and SDK



Flutter output types

Output type	Speed	Comments
Kernel snapshot	Slow	Flutter **Debug** builds. Portable. Easy to reverse
~~JIT snapshot~~		*Not used in Flutter*
AOT snapshot	Fast	Flutter **Release** builds. **Compiled Natively**. Difficult to reverse
~~Self contained~~		*Not used in Flutter*

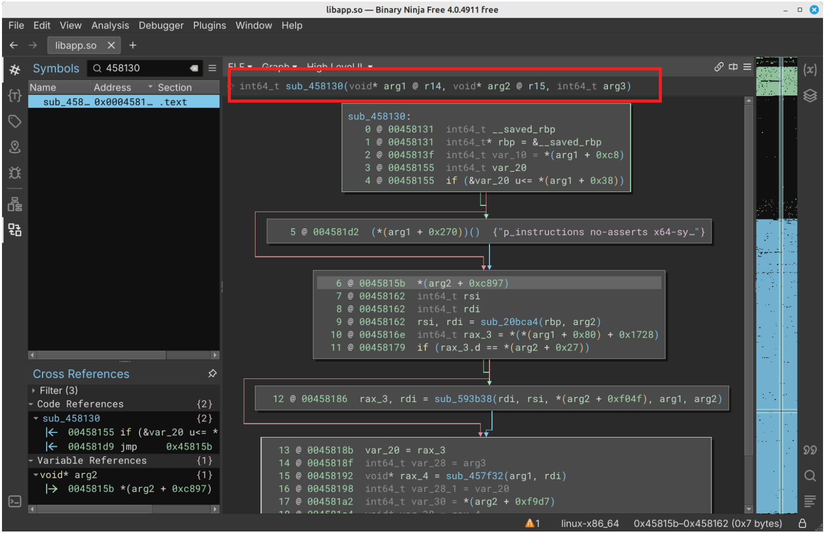
Focus



1. Understand how to reverse **Flutter** applications for Android, especially malware. **Release** applications → **Dart AOT snapshot**.
2. Solve **GreHack CTF 2023 Dart challenge** → It's a **Dart AOT snapshot**

Let's focus on **Dart AOT snapshots**

Disassemblers do not support AOT snapshots



libapp.so — Binary Ninja Free 4.0.4911 free
File Edit View Analysis Debugger Plugins Window Help
libapp.so
Symbols
458130
ELF ▾ Graph ▾ High Level IL ▾
linux-x86_64
0x45815b–0x458162 (0x7 bytes)

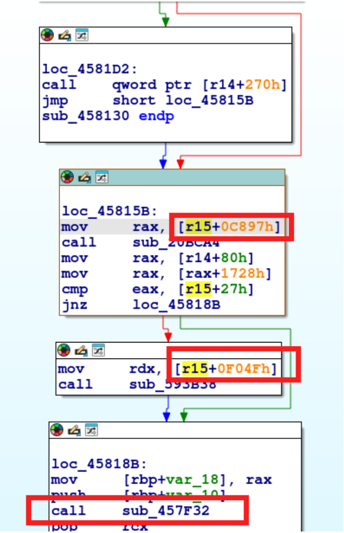
Name	Address	Section
sub_458…	0x0004581…	.text

```
Cross References
▸ Filter (3)
▾ Code References                 {2}
  ▾ sub_458130                    {2}
     |← 00458155 if (&var_20 u<= *
     |← 004581d9 jmp       0x45815b
▾ Variable References             {1}
  ▾void* arg2                     {1}
     |→ 0045815b *(arg2 + 0xc897)
```

```
int64_t sub_458130(void* arg1 @ r14, void* arg2 @ r15, int64_t arg3)

sub_458130:
   0 @ 00458131  int64_t __saved_rbp
   1 @ 00458131  int64_t* rbp = &__saved_rbp
   2 @ 0045813f  int64_t var_10 = *(arg1 + 0xc8)
   3 @ 00458155  int64_t var_20
   4 @ 00458155  if (&var_20 u<= *(arg1 + 0x38))

   5 @ 004581d2  (*(arg1 + 0x270))()  {"p_instructions no-asserts x64-sy…"}

   6 @ 0045815b  *(arg2 + 0xc897)
   7 @ 00458162  int64_t rsi
   8 @ 00458162  int64_t rdi
   9 @ 00458162  rsi, rdi = sub_20bca4(rbp, arg2)
  10 @ 0045816e  int64_t rax_3 = *(*(arg1 + 0x80) + 0x1728)
  11 @ 00458179  if (rax_3.d == *(arg2 + 0x27))

  12 @ 00458186  rax_3, rdi = sub_593b38(rdi, rsi, *(arg2 + 0xf04f), arg1, arg2)

  13 @ 0045818b  var_20 = rax_3
  14 @ 0045818f  int64_t var_28 = arg3
  15 @ 00458192  void* rax_4 = sub_457f32(arg1, rdi)
  16 @ 00458198  int64_t var_28_1 = var_20
  17 @ 004581a2  int64_t var_30 = *(arg2 + 0xf9d7)
```

No function name, wrong arguments for the function

Disassemblers do not support AOT snapshots



```
loc_4581D2:
call     qword ptr [r14+270h]
jmp      short loc_45815B
sub_458130 endp
```

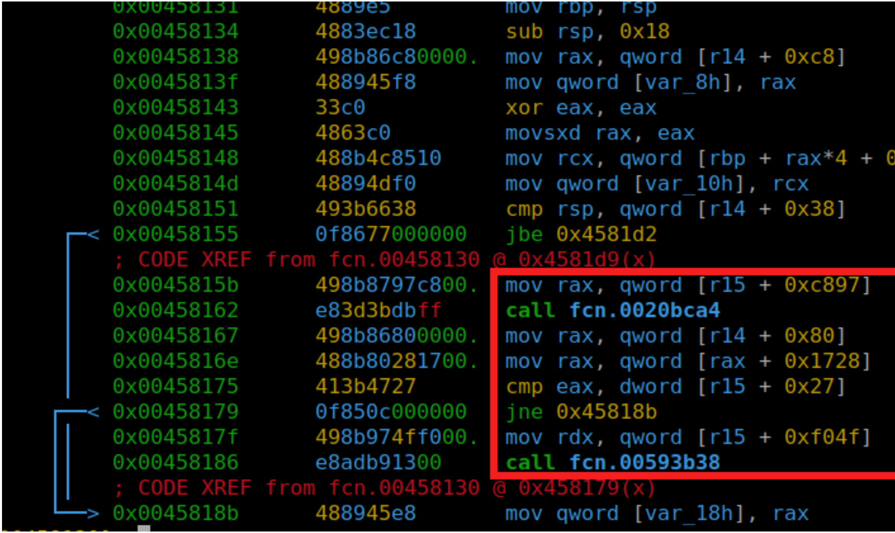
```
loc_45815B:
mov      rax, [r15+0C897h]
call     sub_20BCA4
mov      rax, [r14+80h]
mov      rax, [rax+1728h]
cmp      eax, [r15+27h]
jnz      loc_45818B
```

```
mov      rdx, [r15+0F04Fh]
call     sub_593B38
```

```
loc_45818B:
mov      [rbp+var_18], rax
push     [rbp+var_10]
call     sub_457F32
pop      rcx
```

No strings, no literals, no function names

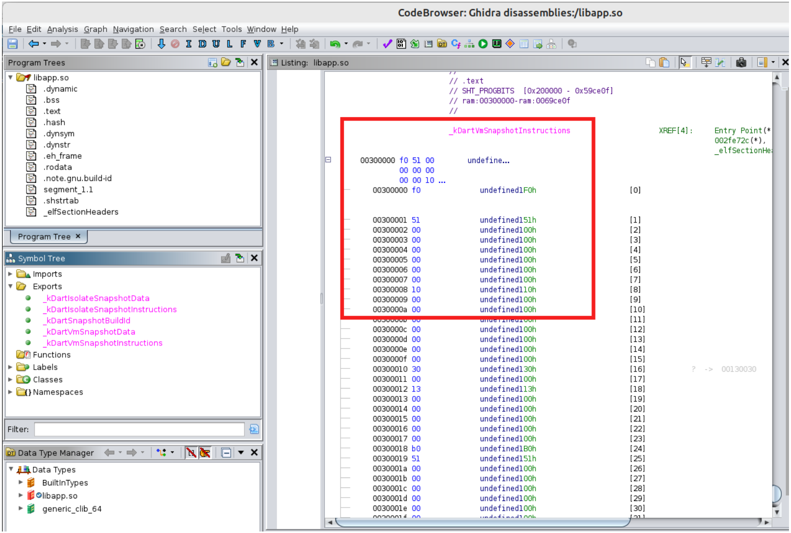
Disassemblers do not support AOT snapshots



```
      0x00458131      4889e5          mov rbp, rsp
      0x00458134      4883ec18        sub rsp, 0x18
      0x00458138      498b86c80000.   mov rax, qword [r14 + 0xc8]
      0x0045813f      488945f8        mov qword [var_8h], rax
      0x00458143      33c0            xor eax, eax
      0x00458145      4863c0          movsxd rax, eax
      0x00458148      488b4c8510      mov rcx, qword [rbp + rax*4 + 0
      0x0045814d      48894df0        mov qword [var_10h], rcx
      0x00458151      493b6638        cmp rsp, qword [r14 + 0x38]
   ┌─< 0x00458155      0f8677000000    jbe 0x4581d2
   │  ; CODE XREF from fcn.00458130 @ 0x4581d9(x)
   │  0x0045815b      498b8797c800.   mov rax, qword [r15 + 0xc897]
   │  0x00458162      e83d3bdbff      call fcn.0020bca4
   │  0x00458167      498b86800000.   mov rax, qword [r14 + 0x80]
   │  0x0045816e      488b80281700.   mov rax, qword [rax + 0x1728]
   │  0x00458175      413b4727        cmp eax, dword [r15 + 0x27]
  ┌──< 0x00458179      0f850c000000    jne 0x45818b
  ││  0x0045817f      498b974ff000.   mov rdx, qword [r15 + 0xf04f]
  ││  0x00458186      e8adb91300      call fcn.00593b38
  │   ; CODE XREF from fcn.00458130 @ 0x458179(x)
  └──> 0x0045818b      488945e8        mov qword [var_18h], rax
```

No strings, no literals, no function names

Disassemblers do not support AOT snapshots


CodeBrowser: Ghidra disassemblies:/libapp.so
File Edit Analysis Graph Navigation Search Select Tools Window Help
Program Trees
Listing: libapp.so
Program Tree ×
Symbol Tree
Filter:
Data Type Manager

- libapp.so
  - .dynamic
  - .bss
  - .text
  - .hash
  - .dynsym
  - .dynstr
  - .eh_frame
  - .rodata
  - .note.gnu.build-id
  - segment_1.1
  - .shstrtab
  - _elfSectionHeaders

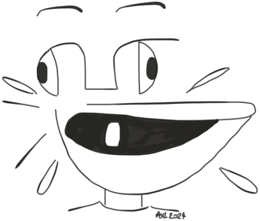
- Imports
- Exports
  - _kDartIsolateSnapshotData
  - _kDartIsolateSnapshotInstructions
  - _kDartSnapshotBuildId
  - _kDartVmSnapshotData
  - _kDartVmSnapshotInstructions
- Functions
- Labels
- Classes
- Namespaces

- Data Types
  - BuiltInTypes
  - libapp.so
  - generic_clib_64

```
                        //
                        // .text
                        // SHT_PROGBITS  [0x200000 - 0x59ce0f]
                        // ram:00300000-ram:0069ce0f
                        //
                        _kDartVmSnapshotInstructions              XREF[4]:     Entry Point(*
                                                                               002fe72c(*),
                                                                               _elfSectionHe
   00300000 f0 51 00        undefine...
            00 00 00
            00 00 10 ...
      00300000 f0             undefined1F0h          [0]


      00300001 51             undefined151h          [1]
      00300002 00             undefined100h          [2]
      00300003 00             undefined100h          [3]
      00300004 00             undefined100h          [4]
      00300005 00             undefined100h          [5]
      00300006 00             undefined100h          [6]
      00300007 00             undefined100h          [7]
      00300008 10             undefined110h          [8]
      00300009 00             undefined100h          [9]
      0030000a 00             undefined100h          [10]
      0030000b 00             undefined100h          [11]
      0030000c 00             undefined100h          [12]
      0030000d 00             undefined100h          [13]
      0030000e 00             undefined100h          [14]
      0030000f 00             undefined100h          [15]
      00300010 30             undefined130h          [16]       ?  ->  00130030
      00300011 00             undefined100h          [17]
      00300012 13             undefined113h          [18]
      00300013 00             undefined100h          [19]
      00300014 00             undefined100h          [20]
      00300015 00             undefined100h          [21]
      00300016 00             undefined100h          [22]
      00300017 00             undefined100h          [23]
      00300018 b0             undefined1B0h          [24]
      00300019 51             undefined151h          [25]
      0030001a 00             undefined100h          [26]
      0030001b 00             undefined100h          [27]
      0030001c 00             undefined100h          [28]
      0030001d 00             undefined100h          [29]
      0030001e 00             undefined100h          [30]
      0030001f 00             undefined100h          [31]
```

Bad entry point, Completely lost

Dart assembly defines its own registers!



	x86_64	**Aarch32**	**Aarch64**
Stack Pointer (SP)	R4	R14	**X15** (custom)
Object Pool (PP)	**R15**	**R5**	**X27**
VM Thread (THR)	**R14**	**R10**	**X26**

Documentation is ... the code

https://github.com/dart-lang/sdk/

```
enum Register {
...
R5  = 5,  // PP
R6 = 6,  // CODE_REG
R7 = 7,  // FP on iOS, DISPATCH_TABLE_REG on non-iOS (AOT only)
R8 = 8,
R9 = 9,
R10  = 10,  // THR
R11 = 11,  // FP on non-iOS, DISPATCH_TABLE_REG on iOS (AOT only)
R12 = 12,  // IP aka TMP
R13 = 13,  // SP
R14 = 14,  // LR
R15 = 15,  // PC
```

https://github.com/dart-lang/sdk/blob/main/runtime/vm/constants_arm.h

Example of Function Prologue for Aarch64

```
; push frame pointer and link register on the stack
STP       X29, X30, [X15, #FFFFFFF0h]!
; update frame pointer
MOV       X29, X15
; allocate 16 bytes on the stack
SUB       X15, X15, #10h
; stack overflow check
LDR       X16, [X26, #38h]
CMP       X15, X16
B.LS      loc_3D75DC
```

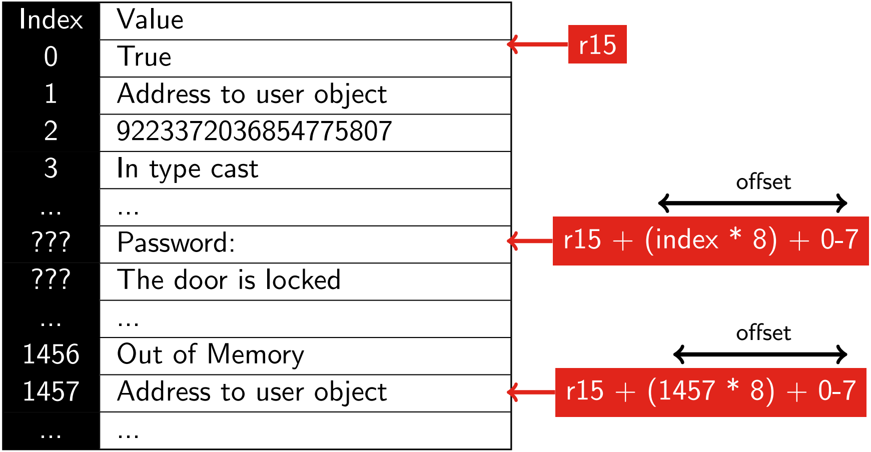
- **X15**: custom stack pointer for AAarch64
- **X26**: holds a pointer to the current thread

Dart Object Pool

Index	Value
0	True
1	Address to user object
2	9223372036854775807
3	In type cast
...	...
???	Password:
???	The door is locked
...	...
1456	Out of Memory
1457	Address to user object
...	...

r15

Dart Object Pool



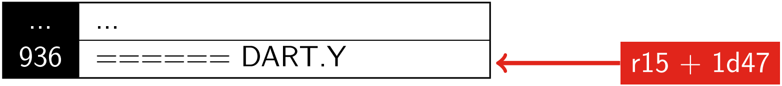
Index	Value
0	True
1	Address to user object
2	9223372036854775807
3	In type cast
...	...
???	Password:
???	The door is locked
...	...
1456	Out of Memory
1457	Address to user object
...	...

$$\textbf{offset} = (\textbf{index} * 8) + (0\text{-}7)$$

$$\text{index} = \text{offset} \; // \; 8$$

Examples of access to the Object Pool

```
; x86-64
mov        r11, qword ptr ds:[r15+1D47h]
```



...	...
936	====== DART.Y

r15 + 1d47

Big indexes are computed - example on Aarch64

```
; loads object pool + 0x0F038
ADD        X17, X27, #Fh, LSL #12
LDR        X17, [X17, #38h]
```

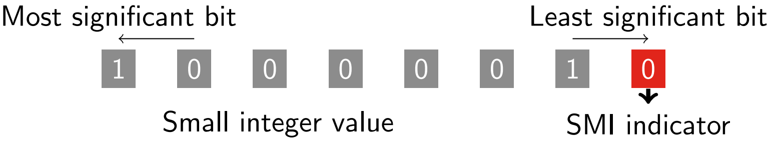
Loads object pool (X27) + 0xF000 (0xF LSL 12) + 0x38 = 0x0F038

Dart's representation of integers: SMI/MINT

```
mov qword [rbp - 0x18], rax
mov r11d, 0x75e ; decimal value = 943
mov qword [rax + 0x17], r11
mov r11d, 0x760 ; 944
mov qword [rax + 0x1f], r11
mov r11d, 0x422 ; 529
```

Dart has 2 different representations of integers:

1. **Small Integers** (SMI). They fit on 31 bits. **Least significant bit set to 0**.
2. **Medium Integers** (Mint). Bigger.



Most significant bit

Least significant bit

1	0	0	0	0	0	1	0

Small integer value

SMI indicator

https://cryptax.medium.com/reversing-flutter-apps-darts-small-integers-b922d7fae7d9

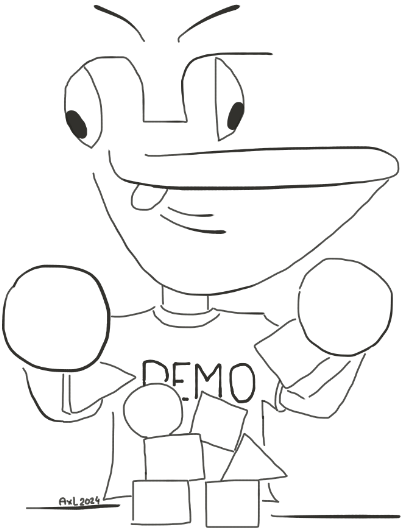
DART.Y CTF challenge

Pico bought a connected fridge at DART.Y. It locks up his favorite caviar from predators, except Pico is hungry and can't remember the password to open his fridge...

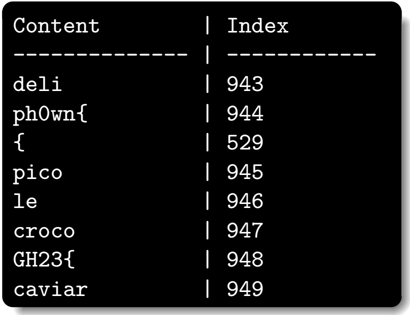
```
====== DART.Y - Your Secure & Smart Fridge ======
Password:
```

- Dart AOT snapshot, not stripped
- Flag format is `GH23{.........}`
- The challenge was renamed in GreHack CTF 2023

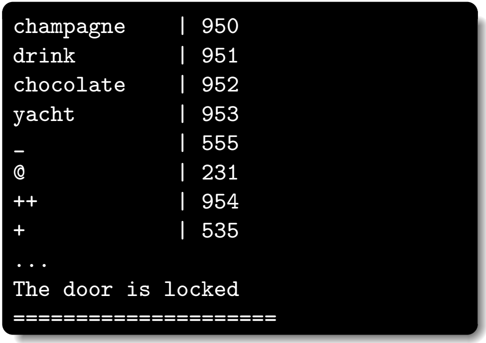
Demo



When you enter the wrong password



```
Content        | Index
-------------- | ------------
deli           | 943
ph0wn{         | 944
{              | 529
pico           | 945
le             | 946
croco          | 947
GH23{          | 948
caviar         | 949
```



```
champagne      | 950
drink          | 951
chocolate      | 952
yacht          | 953
_              | 555
@              | 231
++             | 954
+              | 535
...
The door is locked
=====================
```

It's an Object Pool!

Disassembling the AOT snapshot

Fortunately, it's *not* stripped

```
[0x00058000]> afl~main
0x000afb90     6     201 main
0x000b297c     3      33 sym.main_1
```

We don't have the entire Object Pool but we can guess some

```
mov r11, qword [r15 + 0x1d47] <-- guess: ====== DART.Y ...
mov qword [rsp], r11
call sym.printToConsole
call sym.stdout
mov qword [var_8h], rax
mov r11, qword [r15 + 0x1d4f] <-- guess: Password:
mov qword [rsp], r11
call sym._StdSink.write
call sym.stdin                <-- wait for user input
```

Create Flag

```
mov qword [rsp], rax
call sym.Stdin.readLineSync
mov qword [var_bp_8h], rax
call sym.createFlag         <-- Ooooooooooh! createFlag
```

In createFlag

```
[0x000afb90]> s sym.createFlag
[0x000afc5c]> pif
...
mov r11, qword [r15 + 0x1d6f] <-- Guess: Content | Index
mov qword [rsp], r11
call sym.printToConsole
mov r11, qword [r15 + 0x1d77] <-- Guess: ----- | -----
mov qword [rsp], r11
call sym.printToConsole
```

Many objects are loaded from the Object Pool

```
call sym.stub__iso_stub_AllocateArrayStub
mov qword [var_8h], rax
mov r11, qword [r15 + 0x1d7f]
mov qword [rax + 0x17], r11
mov r11, qword [r15 + 0x1d87]
mov qword [rax + 0x1f], r11
mov r11, qword [r15 + 0x108f]
mov qword [rax + 0x27], r11
mov r11, qword [r15 + 0x1d8f]
mov qword [rax + 0x2f], r11
mov r11, qword [r15 + 0x1d97]
mov qword [rax + 0x37], r11
mov r11, qword [r15 + 0x1d9f]
mov qword [rax + 0x3f], r11
mov r11, qword [r15 + 0x1da7]
mov qword [rax + 0x47], r11
mov r11, qword [r15 + 0x1daf]
mov qword [rax + 0x4f], r11
mov r11, qword [r15 + 0x1db7]
mov qword [rax + 0x57], r11
...
```

Index	Value
0x1d7f // 8	deli
0x1d87 // 8	ph0wn{
0x108f // 8	{

$$0x1d7f//8 = 943$$
$$0x1d87//8 = 944$$

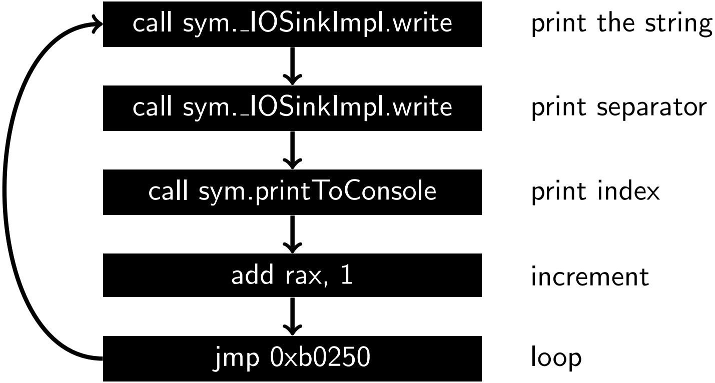
```
Content     | Index
----------- | ----------
deli        | 943
ph0wn{      | 944
```

Those are the indexes of the supplied Object Pool

```
mov r10d, 0x70
call sym.stub__iso_stub_AllocateArrayStub
mov qword [rbp - 0x18], rax
mov r11d, 0x75e
mov qword [rax + 0x17], r11
mov r11d, 0x760
mov qword [rax + 0x1f], r11
mov r11d, 0x422
```

Index	SMI	Value
0x1d7f // 8 = 943_{10}	$943_{10} << 1 =$ 0x75e	deli
0x1d87 // 8 = 944_{10}	$944_{10} << 1 =$ 0x760	ph0wn{
0x108f // 8 = 529_{10}	$529_{10} << 1 =$ 0x422	{

Loop to print the Object Pool



call sym._IOSinkImpl.write

print the string

call sym._IOSinkImpl.write

print separator

call sym.printToConsole

print index

add rax, 1

increment

jmp 0xb0250

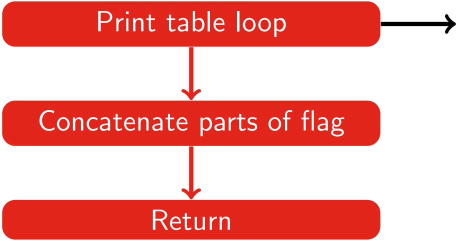
loop

Final part of createFlag

```
mov r11, qword [r15 + 0x115f ]
mov qword [rsp], r11
call fcn.0007880c
mov qword [var_sp_8h], rax
mov r11, qword [r15 + 0x1e5f ]
mov qword [rsp], r11
call fcn.0007880c
mov qword [var_sp_8h], rax
mov r11, qword [r15 + 0x1e77 ]
...
mov rsp, rbp
pop rbp
ret
```

- Access to many objects of the Object Pool
- `fcn.0007880c` is string concatenation
- The result is returned by `createFlag`, so it's the flag!

createFlag summary



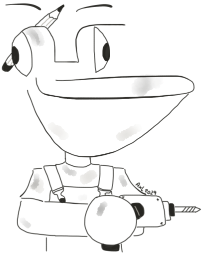
```
Content        | Index
-------------- | ------------
deli           | 943
ph0wn{         | 944
{              | 529
pico           | 945
le             | 946
croco          | 947
GH23{          | 948
caviar         | 949
```

Recover the flag

0x1da7	GH23{
0x115f	_
0x1e5f	s
0x1e77	lurp
0x115f	_
0x1e9f	it
0x115f	_
0x1e5f	s
0x115f	_
0x1d7f	deli
0x1ea7	cious

GH23{_slurp_it_s_delicious_with_some_lobster!}

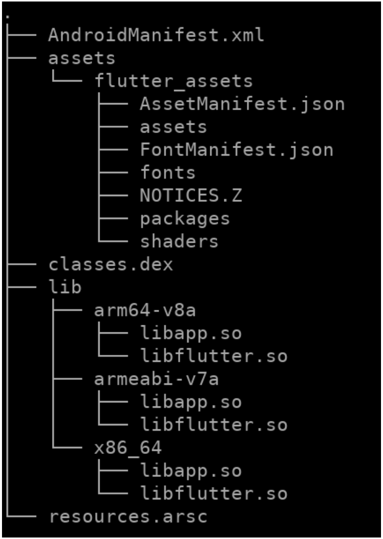
Next Goal



1. Understand how to reverse **Flutter** applications for Android, especially malware. **Release** applications → **Dart AOT snapshot**.
2. ~~Solve **GreHack CTF 2023 Dart challenge** → It's a **Dart AOT snapshot**~~. DONE

Let's focus on Flutter applications for Android

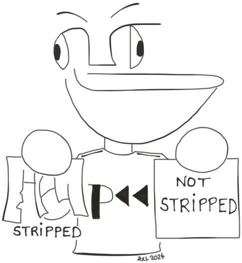
Flutter application on Android: locating the payload



```
.
├── AndroidManifest.xml
├── assets
│   └── flutter_assets
│       ├── AssetManifest.json
│       ├── assets
│       ├── FontManifest.json
│       ├── fonts
│       ├── NOTICES.Z
│       ├── packages
│       └── shaders
├── classes.dex
├── lib
│   ├── arm64-v8a
│   │   ├── libapp.so
│   │   └── libflutter.so
│   ├── armeabi-v7a
│   │   ├── libapp.so
│   │   └── libflutter.so
│   └── x86_64
│       ├── libapp.so
│       └── libflutter.so
└── resources.arsc
```

- `classes.dex`: contains Java code, and Dalvik to Flutter glue
- `./lib/xxx/libflutter.so`: Flutter implementation
- `./lib/xxx/libapp.so`: payload!

Reversing Flutter applications: what's different?



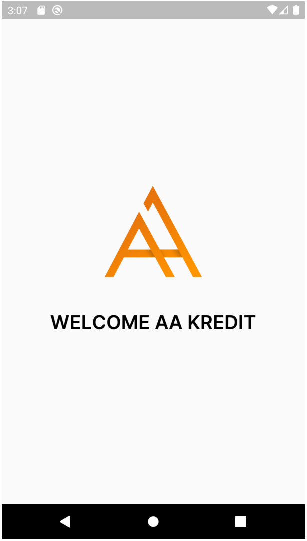
Releases are stripped

```
dart compile aot-snapshot -S ./debuginfo file.dart
```

```
[0x00170000]> afl
0x003f7b80     9    212 fcn.003f7b80 <-- no function names
0x003db6c0    28    464 fcn.003db6c0
0x0036f024    14    232 fcn.0036f024
0x00332678    14    232 fcn.00332678
```

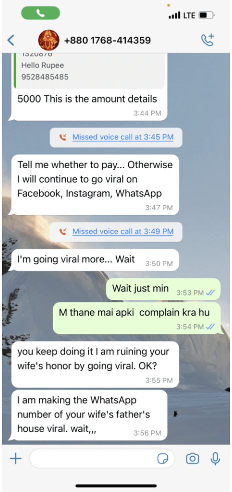
Example: Android/SpyLoan (2023)

- Attract victims for easy loans
- Complete a loan application, enter personal information.
- Malware blackmails victims to repay more quickly.



Example: Android/SpyLoan (2023)

- Attract victims for easy loans
- Complete a loan application, enter personal information.
- Malware blackmails victims to repay more quickly.



+880 1768-414359

1320676
Hello Rupee
9528485485

5000 This is the amount details 3:44 PM

Missed voice call at 3:45 PM

Tell me whether to pay... Otherwise I will continue to go viral on Facebook, Instagram, WhatsApp 3:47 PM

Missed voice call at 3:49 PM

I'm going viral more... Wait 3:50 PM

Wait just min 3:53 PM

M thane mai apki complain kra hu 3:54 PM

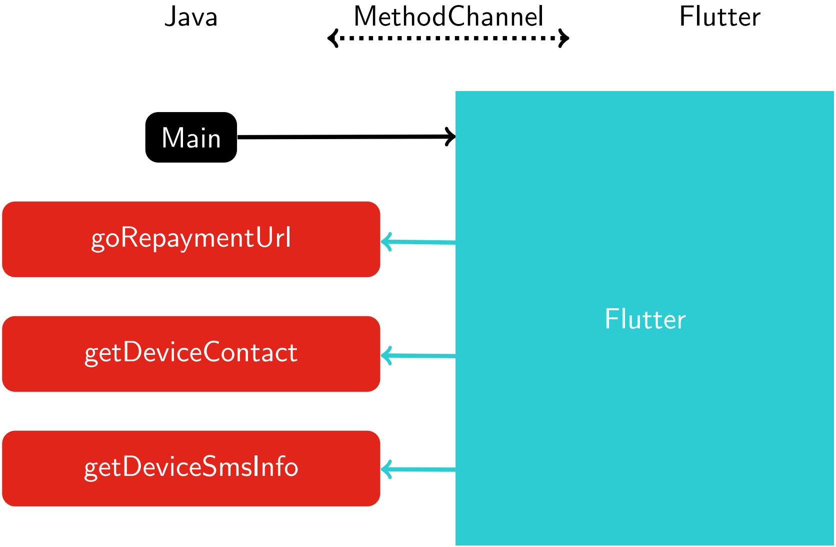
you keep doing it I am ruining your wife's honor by going viral. OK? 3:55 PM

I am making the WhatsApp number of your wife's father's house viral. wait,,, 3:56 PM

Source:

https://www.dailyradar.in/aa-kredit-loan-app-review/

Android/SpyLoan: implementation



Java

MethodChannel

Flutter

Main

goRepaymentUrl

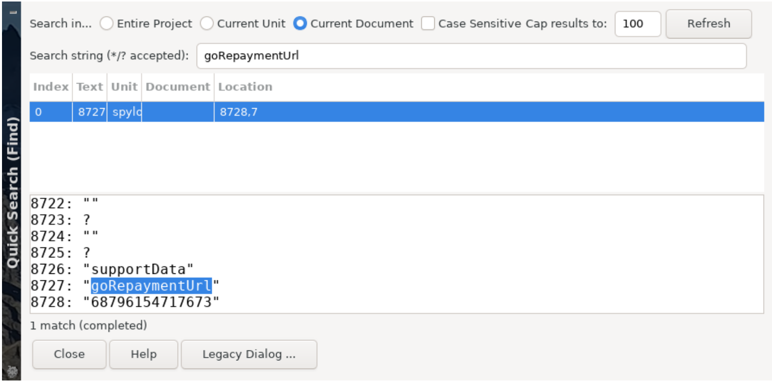
getDeviceContact

getDeviceSmsInfo

Flutter

Where is goRepaymentUrl called?

1. ``goRepaymentUrl'' is provided to MethodChannel
2. Search ``goRepaymentUrl'' in the Object Pool
3. Index is **8727=0x110b8**



Quick Search (Find)
Search in... ○ Entire Project ○ Current Unit ● Current Document □ Case Sensitive Cap results to: 100 Refresh

Search string (*/? accepted): goRepaymentUrl

Index	Text	Unit	Document	Location
0	8727	spylo		8728,7

```
8722: ""
8723: ?
8724: ""
8725: ?
8726: "supportData"
8727: "goRepaymentUrl"
8728: "68796154717673"
```

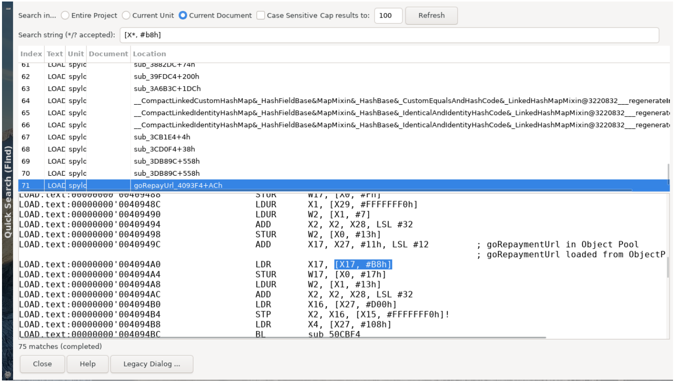
1 match (completed)

Close
Help
Legacy Dialog ...

Where is goRepaymentUrl called?

1. ``goRepaymentUrl'' is provided to `MethodChannel`
2. Search ``goRepaymentUrl'' in the Object Pool
3. Index is **8727=0x110b8**
4. Search assembly loading the index:

```
ADD REGISTER, X27, #11h, LSL #12
LDR REGISTER, [REGISTER, #B8h]
```



Search in... ○ Entire Project ○ Current Unit ● Current Document □ Case Sensitive Cap results to: 100 Refresh

Search string (*/? accepted): [X*, #b8h]

Index	Text	Unit	Document	Location
61	LOAD	spylc		sub_3882DC+74h
62	LOAD	spylc		sub_39FDC4+200h
63	LOAD	spylc		sub_3A6B3C+1DCh
64	LOAD	spylc		__CompactLinkedCustomHashMap&_HashFieldBase&MapMixin&_HashBase&_CustomEqualsAndHashCode&_LinkedHashMapMixin@3220832___regenerateI
65	LOAD	spylc		__CompactLinkedIdentityHashMap&_HashFieldBase&MapMixin&_HashBase&_IdenticalAndIdentityHashCode&_LinkedHashMapMixin@3220832___regenerat
66	LOAD	spylc		__CompactLinkedIdentityHashMap&_HashFieldBase&MapMixin&_HashBase&_IdenticalAndIdentityHashCode&_LinkedHashMapMixin@3220832___regenerat
67	LOAD	spylc		sub_3CB1E4+4h
68	LOAD	spylc		sub_3CD0F4+38h
69	LOAD	spylc		sub_3DB89C+558h
70	LOAD	spylc		sub_3DB89C+558h
71	LOAD	spylc		goRepayUrl_4093F4+ACh

```
LOAD.text:00000000'00409488          STUR     W17, [X0, #Fh]
LOAD.text:00000000'0040948C          LDUR     X1, [X29, #FFFFFFF0h]
LOAD.text:00000000'00409490          LDUR     W2, [X1, #7]
LOAD.text:00000000'00409494          ADD      X2, X2, X28, LSL #32
LOAD.text:00000000'00409498          STUR     W2, [X0, #13h]
LOAD.text:00000000'0040949C          ADD      X17, X27, #11h, LSL #12        ; goRepaymentUrl in Object Pool
                                                                              ; goRepaymentUrl loaded from ObjectP
LOAD.text:00000000'004094A0          LDR      X17, [X17, #B8h]
LOAD.text:00000000'004094A4          STUR     W17, [X0, #17h]
LOAD.text:00000000'004094A8          LDUR     W2, [X1, #13h]
LOAD.text:00000000'004094AC          ADD      X2, X2, X28, LSL #32
LOAD.text:00000000'004094B0          LDR      X16, [X27, #D00h]
LOAD.text:00000000'004094B4          STP      X2, X16, [X15, #FFFFFFF0h]!
LOAD.text:00000000'004094B8          LDR      X4, [X27, #108h]
LOAD.text:00000000'004094BC          BL       sub_50CBF4
```

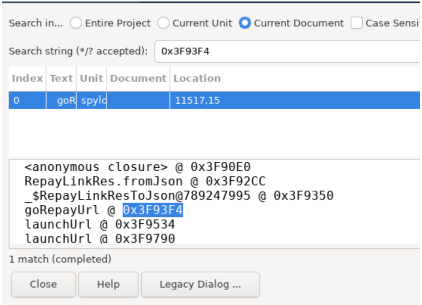
75 matches (completed)

What is the name of this Flutter function?

```
sub_4093F4      proc
...
STUR      X0, [X29, #FFFFFFE8h]
ADD       X17, X27, #Bh, LSL #12
LDR       X17, [X17, #C88h]
STUR      W17, [X0, #Fh]
LDUR      X1, [X29, #FFFFFFF0h]
LDUR      W2, [X1, #7]
ADD       X2, X2, X28, LSL #32
STUR      W2, [X0, #13h]
ADD       X17, X27, #11h, LSL #12 ; goRepaymentUrl loaded from ObjectPool
LDR       X17, [X17, #B8h]
```

- JEB relocation base for zero based relocatable objects: **0x10000** (Options / General / Back-end properties: root, parsers, native, disas)
- The function is at 0x4093F4-0x10000=0x3F93F4
- Search Code Information for **0x3F93F4**

Function name found



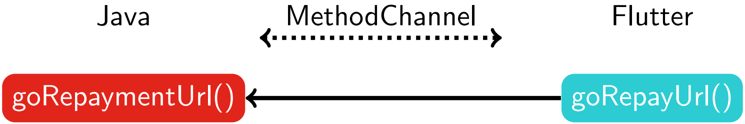
Search in... ○ Entire Project ○ Current Unit ● Current Document □ Case Sensi

Search string (*/? accepted): 0x3F93F4

Index	Text	Unit	Document	Location
0	goR	spylc		11517,15

```
<anonymous closure> @ 0x3F90E0
RepayLinkRes.fromJson @ 0x3F92CC
_$RepayLinkResToJson@789247995 @ 0x3F9350
goRepayUrl @ 0x3F93F4
launchUrl @ 0x3F9534
launchUrl @ 0x3F9790
```

1 match (completed)



Java

MethodChannel

Flutter

goRepaymentUrl()

goRepayUrl()

Flutter apps for Android AArch64: status

With JEB

- Read the Object Pool: **Yes** (strings only)
- Find function names: **Yes** via Code Information.
- Find string cross references: **Yes** via Search.

Are we lost *without* JEB?

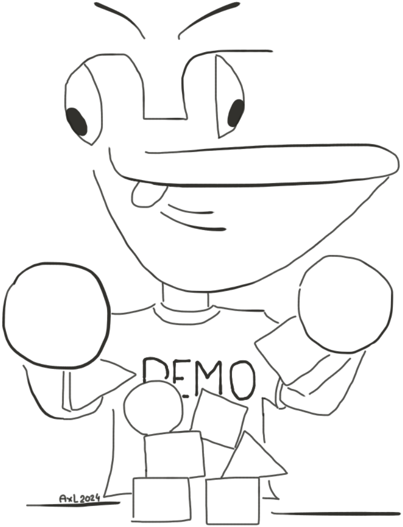
There is still hope

- Blutter: https://github.com/worawit/blutter
- Only works for **recent Android Flutter AAarch64**
- Requires **GCC 13**
- `python3 blutter.py ./malware/spyloan/arm64-v8a outputdir`

Output

- `pp.txt`: all Dart objects in the Object Pool
- `asm/`: assembly code

Demo



Finding goRepaymentUrl with Blutter

grep -C 3 goRepaymentUrl pp.txt

```
[pp+0x110a8] String: ""
[pp+0x110b0] List(7) [0, 0x2, 0x2, 0x1, "mode", 0x1, Null]
[pp+0x110b8] String: "supportData"
[pp+0x110c0] String: "goRepaymentUrl"
[pp+0x110c8] String: "68796154717673"
[pp+0x110d0] Null
[pp+0x110d8] String: " in type cast"
```

- Blutter finds offset **0x110c0**
- In reality, assembly loads **0x110b8** (0x110c0-8)

Finding function name with Blutter

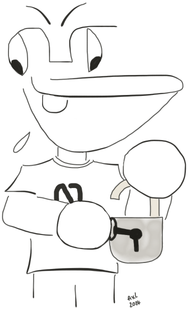
Search for function at **0x3F93F4**

```
$ grep -ri 3F93F4 ./asm/
./asm/flutter_project/plugin/Plugin.dart:    // ** addr: 0x3f93f4
   ...
```

./asm/flutter_project/plugin/Plugin.dart

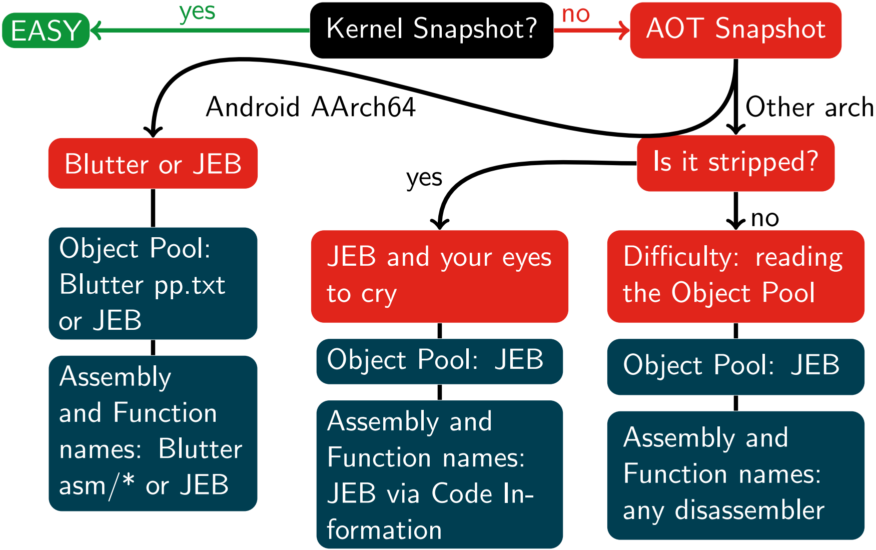
```
static _ goRepayUrl(/* No info */) async {
  // ** addr: 0x3f93f4, size: 0x140
  // 0x3f93f4: EnterFrame
  //     0x3f93f4: stp              fp, lr, [SP, #-0x10]!
  //     0x3f93f8: mov              fp, SP
  // 0x3f93fc: AllocStack(0x18)
  //     0x3f93fc: sub              SP, SP, #0x18
  // 0x3f9400: SetupParameters(dynamic _ /* r1, fp-0x10 */)
```

Goals unlocked



1. ~~Understand how to reverse **Flutter** applications for Android, especially malware. **Release** applications → **Dart AOT snapshot**~~. DONE
2. ~~Solve **GreHack CTF 2023 Dart challenge** → It's a **Dart AOT snapshot**~~. DONE

Reversing Dart / Flutter



Kernel Snapshot?

yes

EASY

no

AOT Snapshot

Android AArch64

Other arch

Blutter or JEB

Object Pool: Blutter pp.txt or JEB

Assembly and Function names: Blutter asm/* or JEB

Is it stripped?

yes

JEB and your eyes to cry

Object Pool: JEB

Assembly and Function names: JEB via Code Information

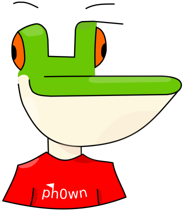
no

Difficulty: reading the Object Pool

Object Pool: JEB

Assembly and Function names: any disassembler

Thanks for your attention!



- https://github.com/cryptax/talks
- @cryptax (X, Mastodon.social)
- https://ph0wn.org CTF - November 29-30, 2024