Native modules trên Android và sức mạnh của FRIDA

CTF for fun

TABLE OF CONTENTS

01

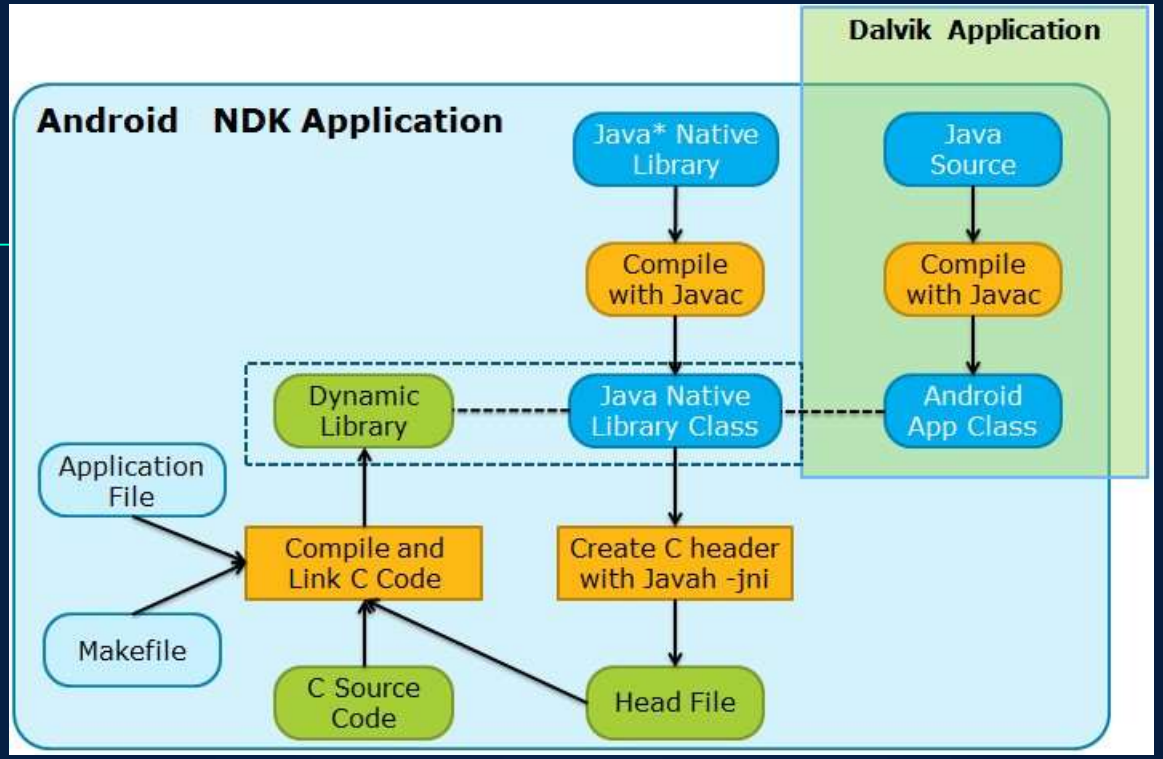
NDK, JNI?

Something you win, something you learn...

NDK

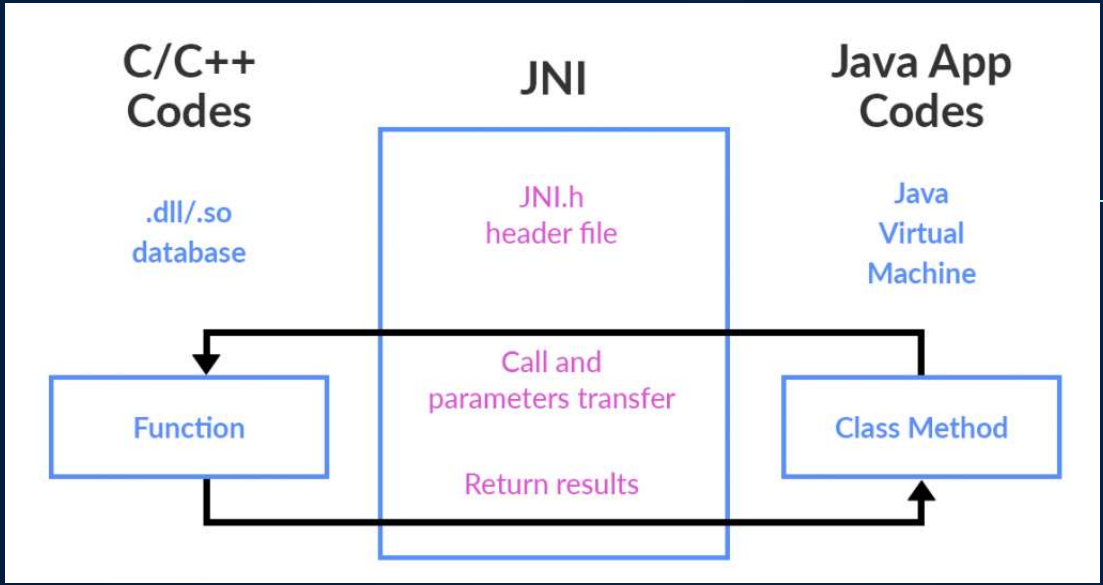
Native Development Kit

Tool để cho lập trình C/C++ trên thiết Android (bao gồm cả SDK) → cải thiện hiệu năng cho chương trình. Source code sẽ được compile ra mã máy (theo kiến trúc của CPU). Hầu hết các application thường sử dụng cả native-code và java-code để hiệu năng đạt cao nhất.
Nhưng làm thế nào để java-code tương tác được với native-code?
→ JNI



https://stackoverflow.com/tags/android-ndk/info

JNI



https://redwerk.com/blog/3-reasons-why-we-love-jni/

Java Native Interface

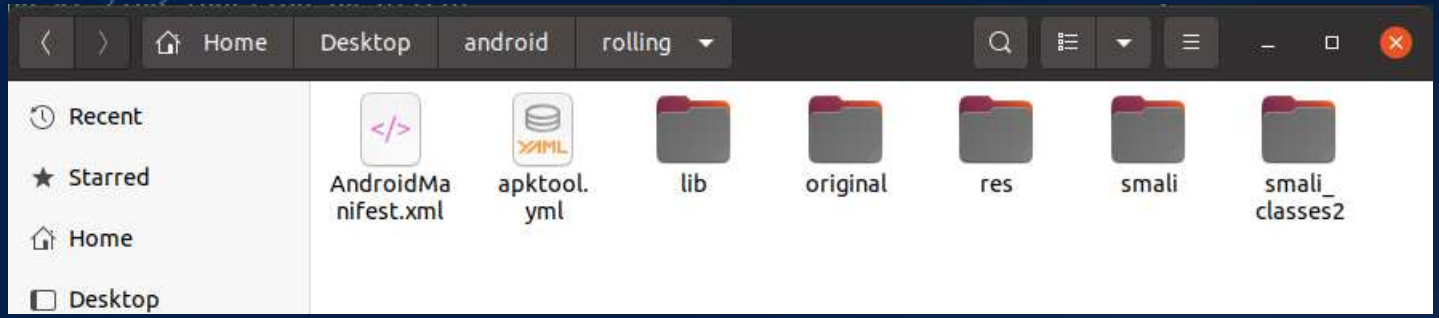
- Là giao diện hỗ trợ tương tác giữa C/C++ và Java
- Khi sử dụngJNI, C/C++ functions sẽ được map như một method và data types chuyển đến cho Java và ngược lại (như hình).

02

Native Library

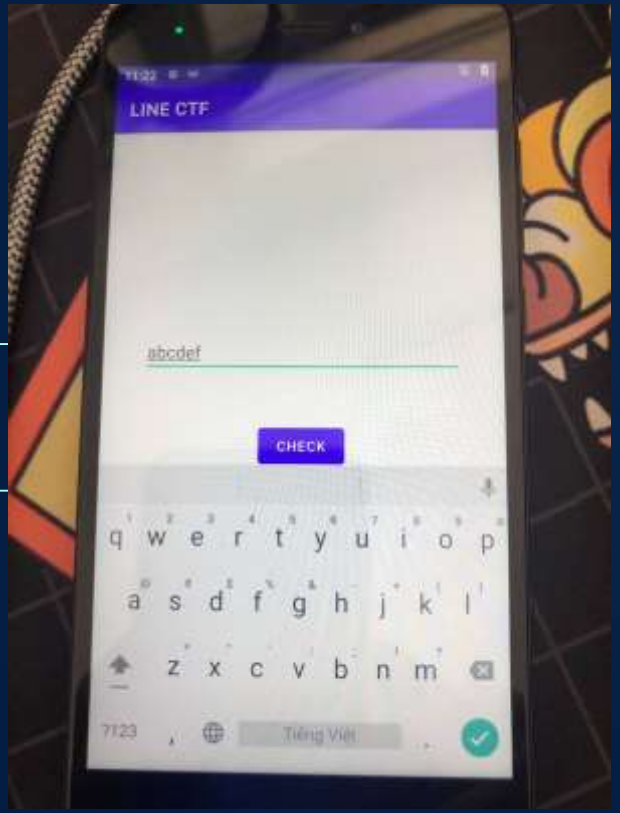
Native library?

- Các hàm native sẽ được đóng trong các library → native library
- Một file native-lib là .so file (so=Shared Object), tương tự như một file lib trong C/C++.

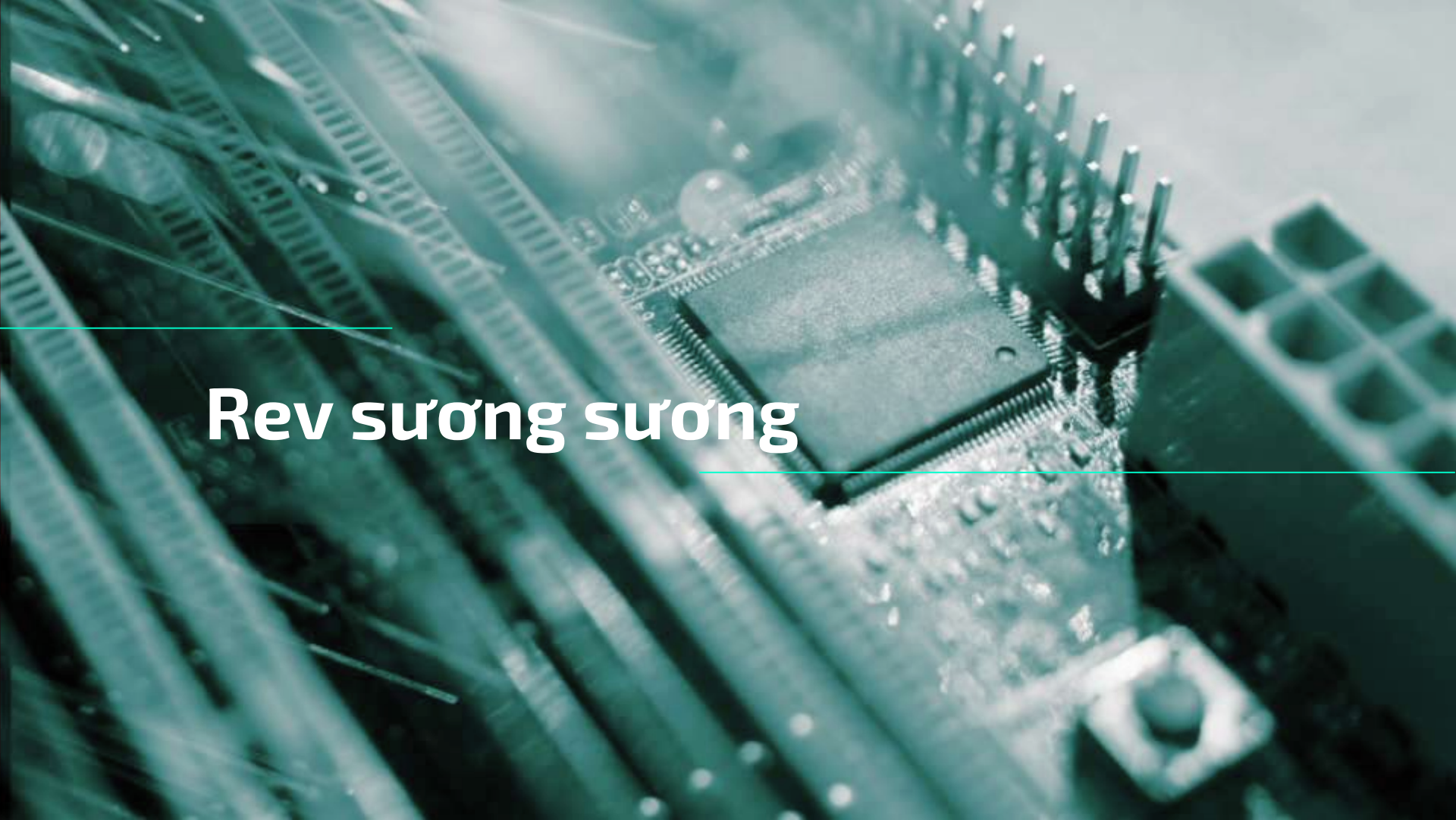



03
Hooking with FRIDA

DEMO

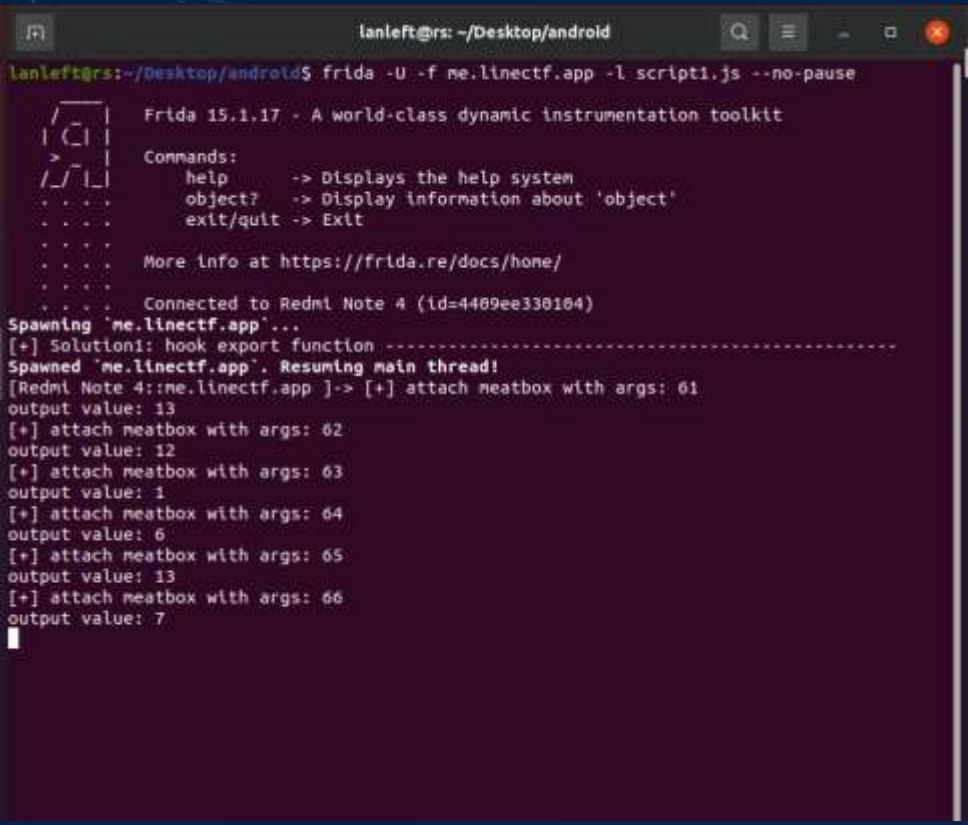


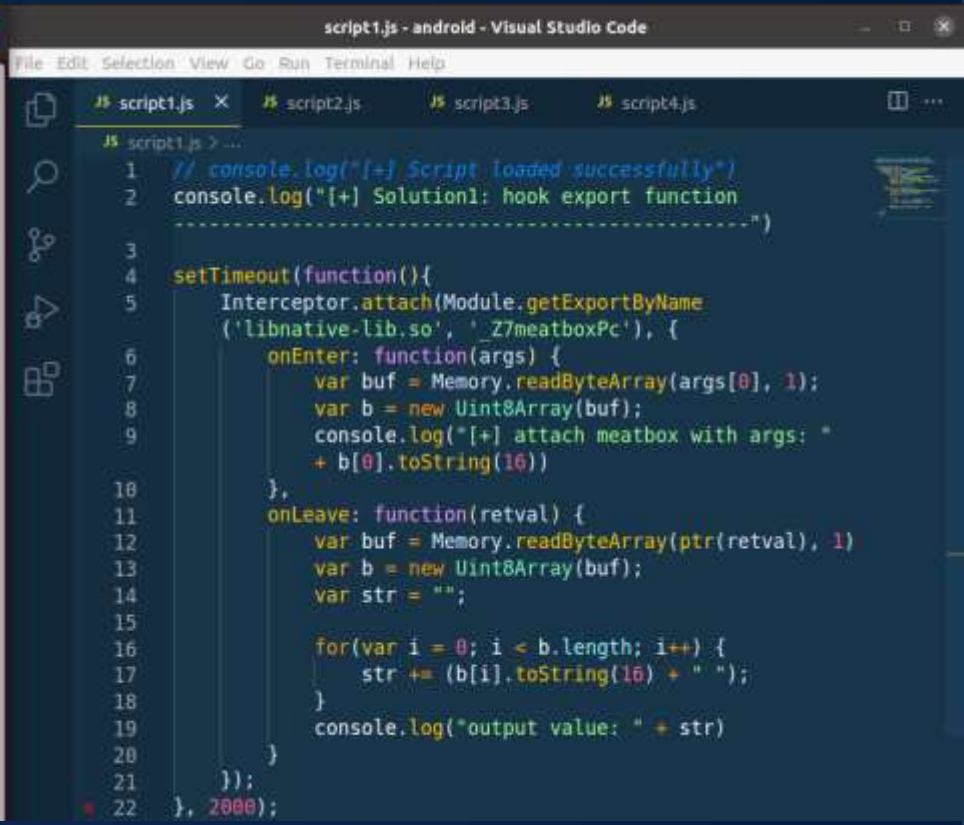
https://score.linectf.me/challenges



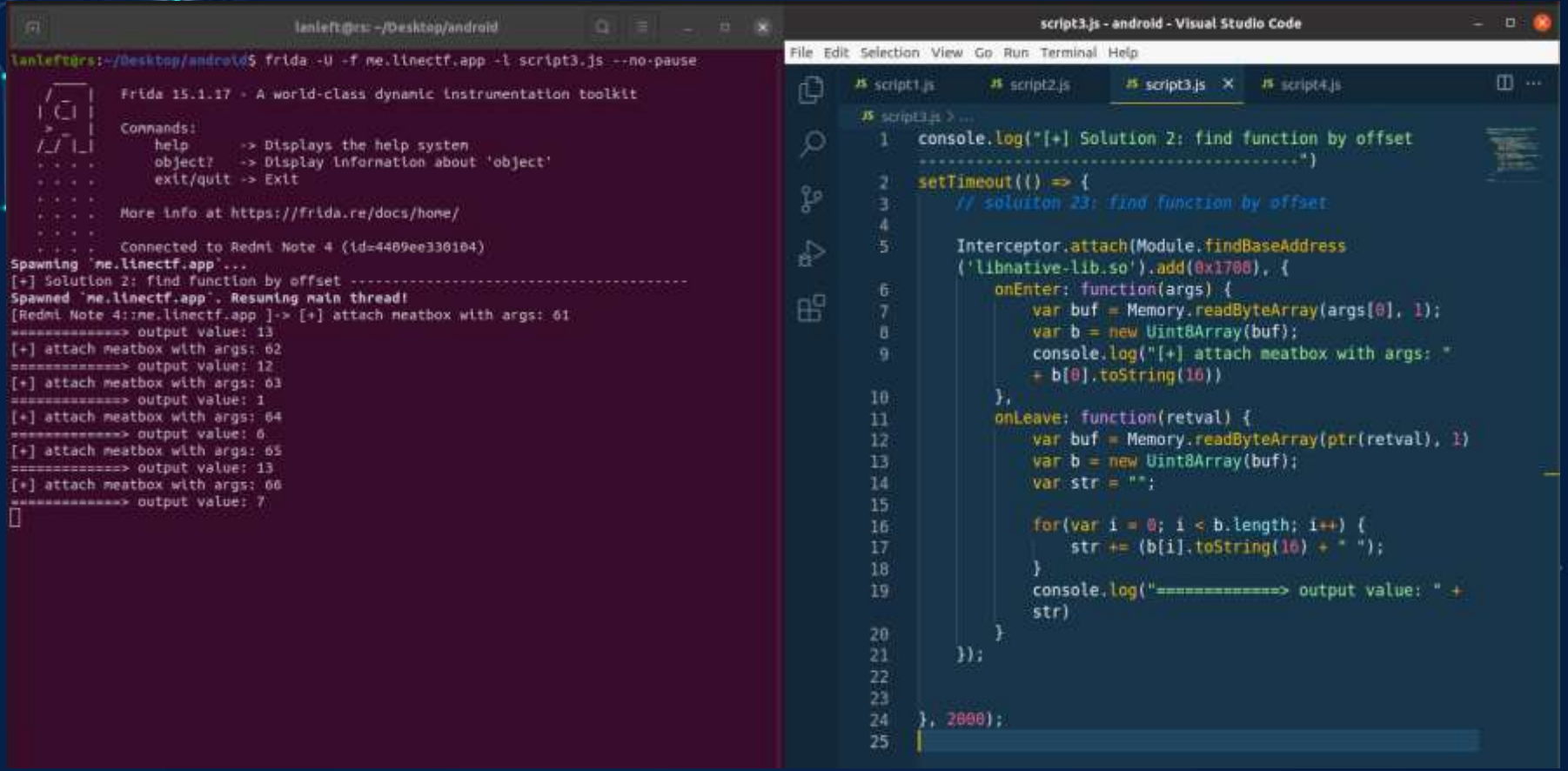
Rev sương sương

Solution 1: exported functions

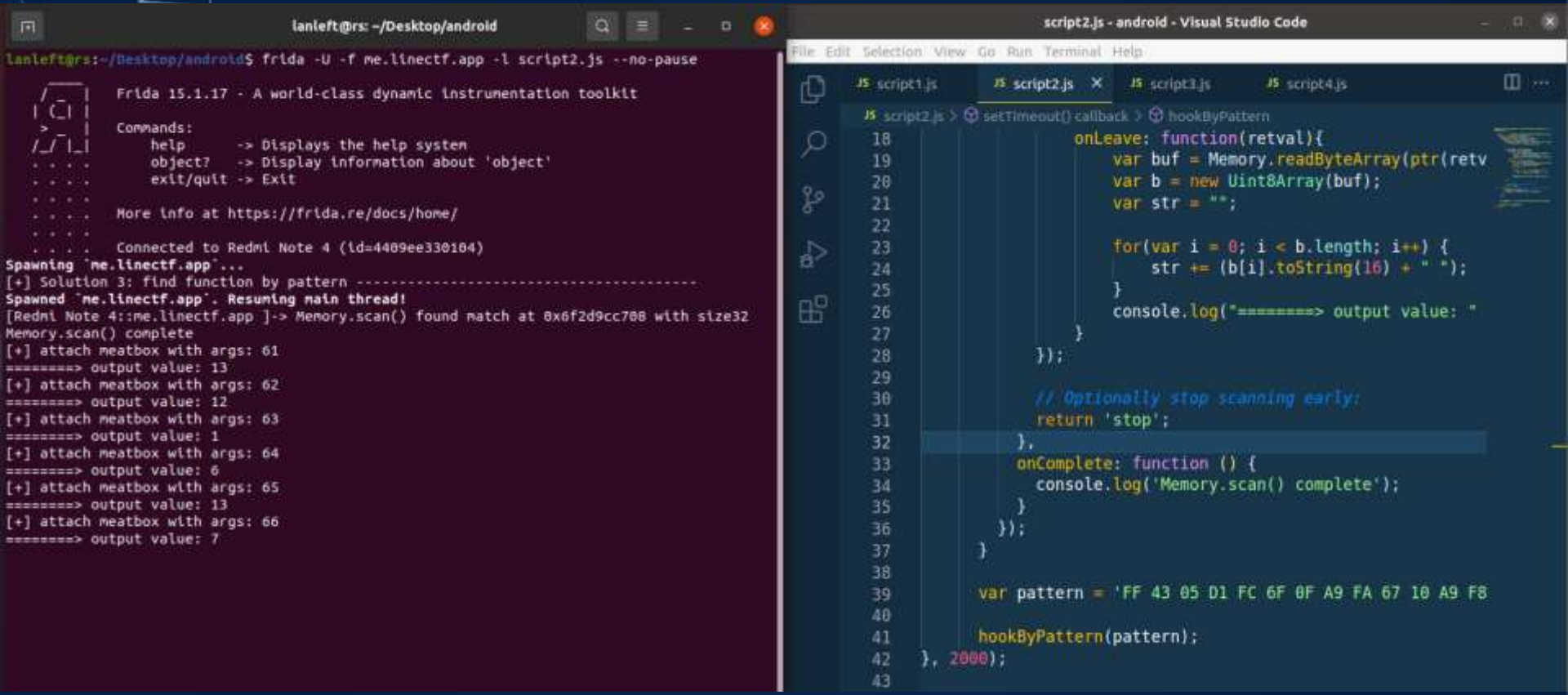




Solution 2: offset



Solution 3: pattern



Solution 4: by string reference

Ideas:
- Radare2
  - Frida + python ← lib, life python

// Open(“libabc.so”, “rb”)…
// life.parse(“lib_name”)
//

04
Mở rộng

File native-lib bị obfuscate strings, strip function?

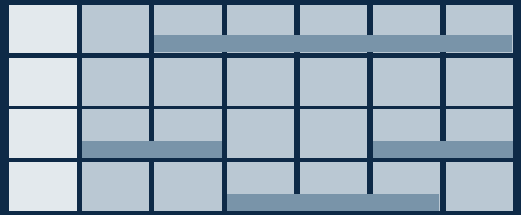
```
// open the shared object
void *dlh = dlopen("libnative-lib.so", RTLD_LAZY);
// void *dlh=NULL;
if (dlh == NULL) {

  printf("[-] open library fail\n");
  exit(1);
}
// resolve the function symbol
h_meatbox meatbox = dlsym(dlh, "_Z7meatboxPc");
```

File native-lib sử dụng custom bytecode?

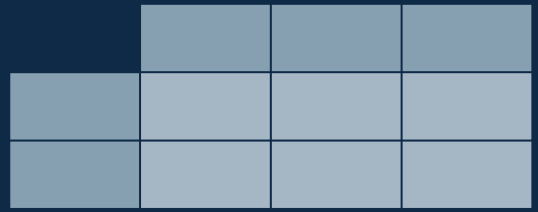
???

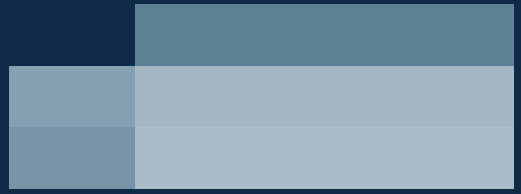
THANKS

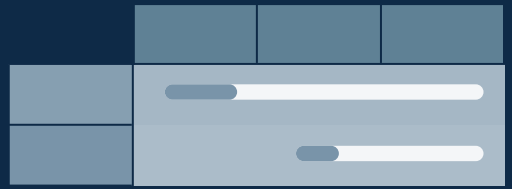
Does anyone have any questions?

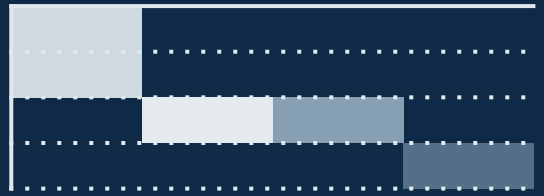


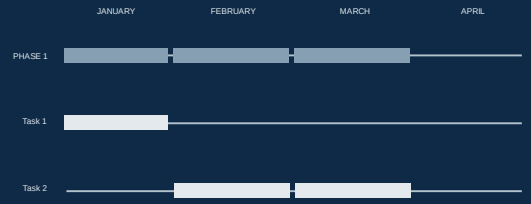

JANUARY
FEBRUARY
MARCH
APRIL
MAY
JUNE
PHASE 1
Task 1
Task 2
PHASE 2
Task 1
Task 2

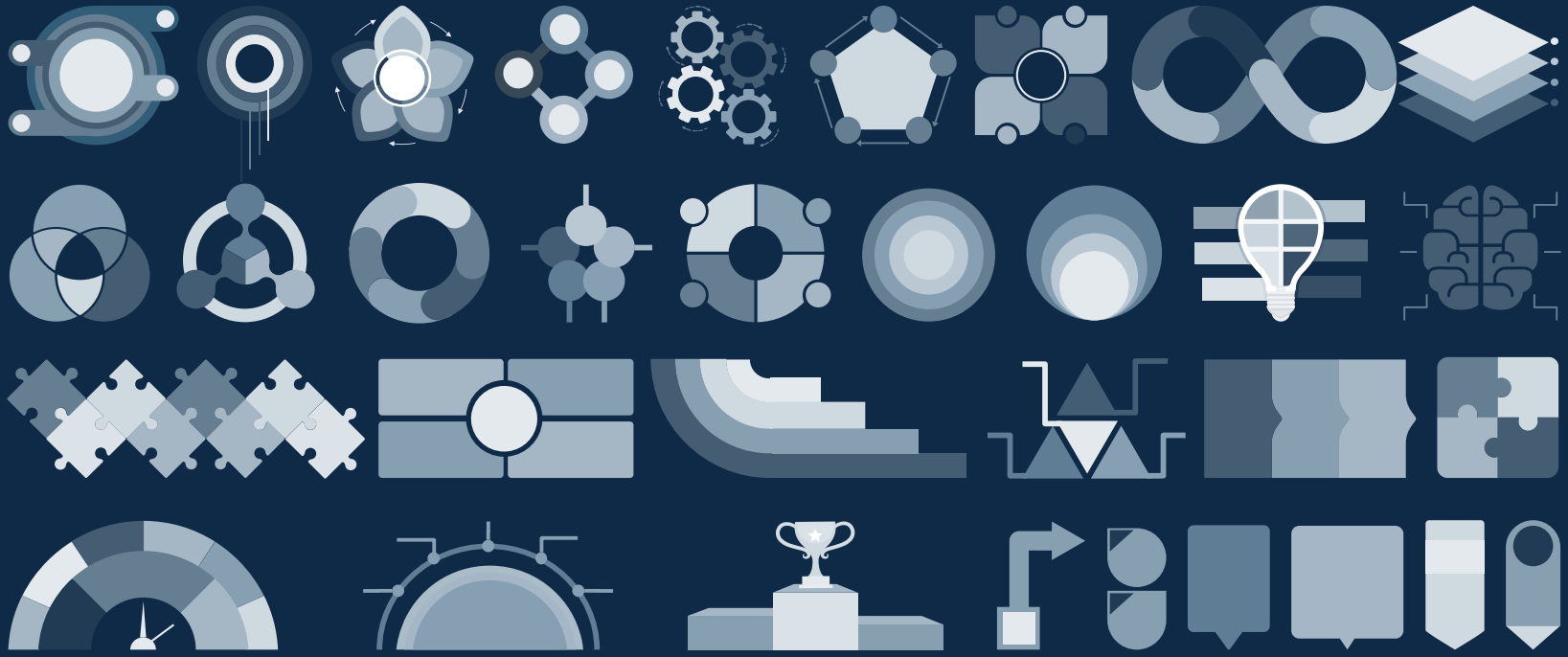


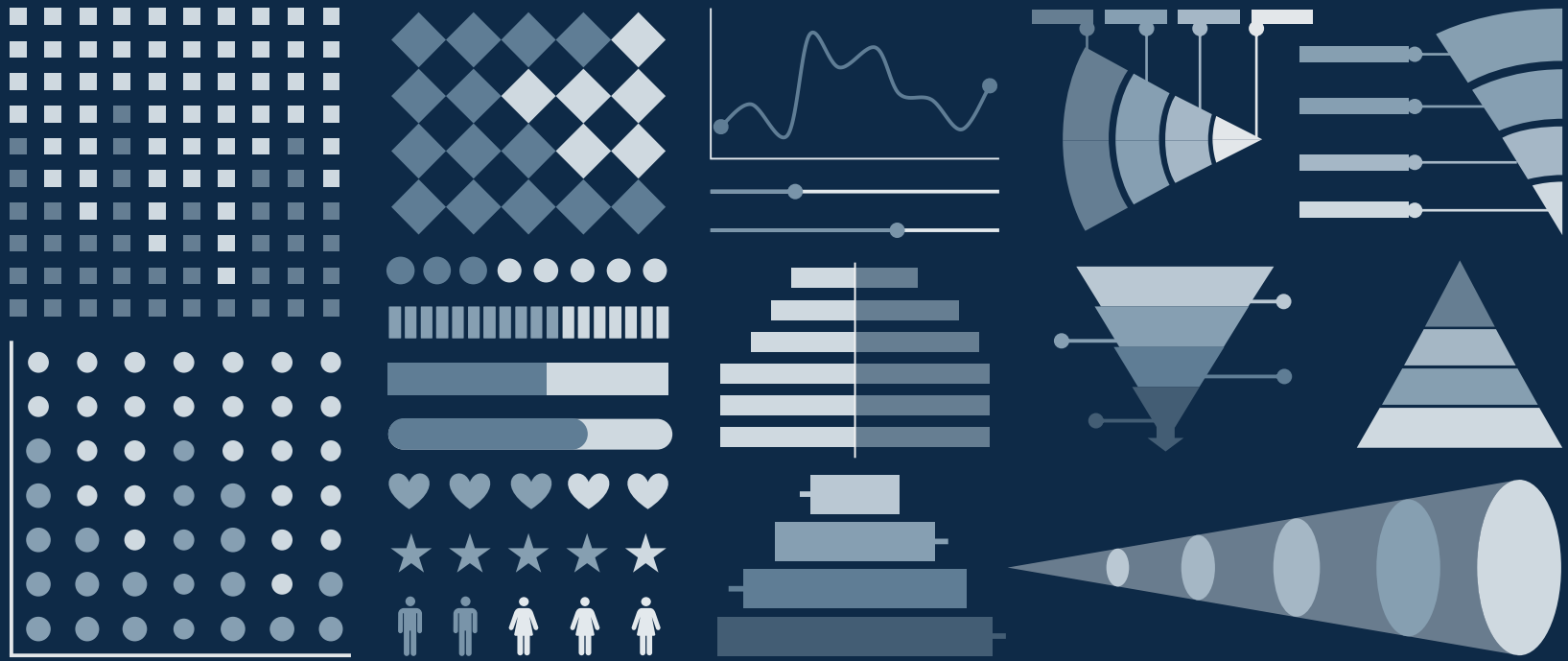







JANUARY
FEBRUARY
MARCH
APRIL
PHASE 1
Task 1
Task 2





...and our sets of editable icons

You can resize these icons without losing quality.
You can change the stroke and fill color; just select the icon and click on the paint bucket/pen.
In Google Slides, you can also use Flaticon's extension, allowing you to customize and add even more icons.

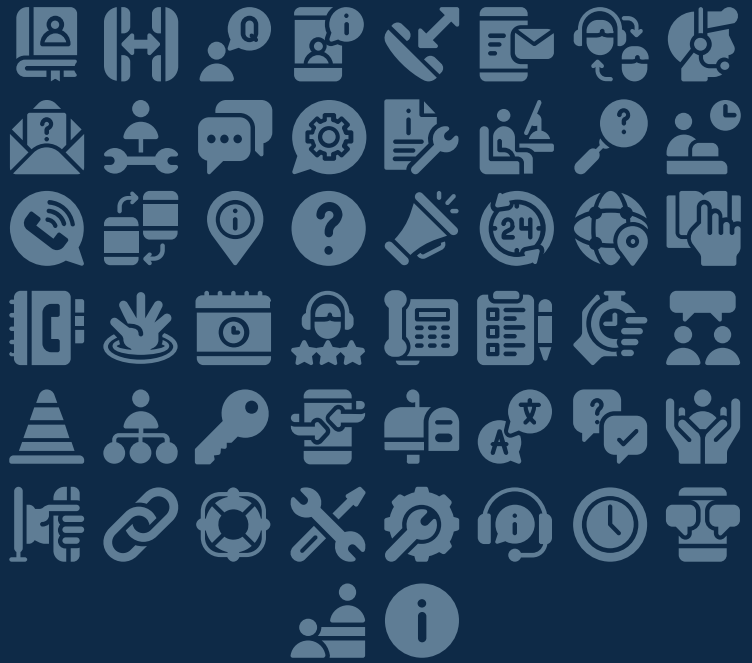
Educational Icons

Medical Icons

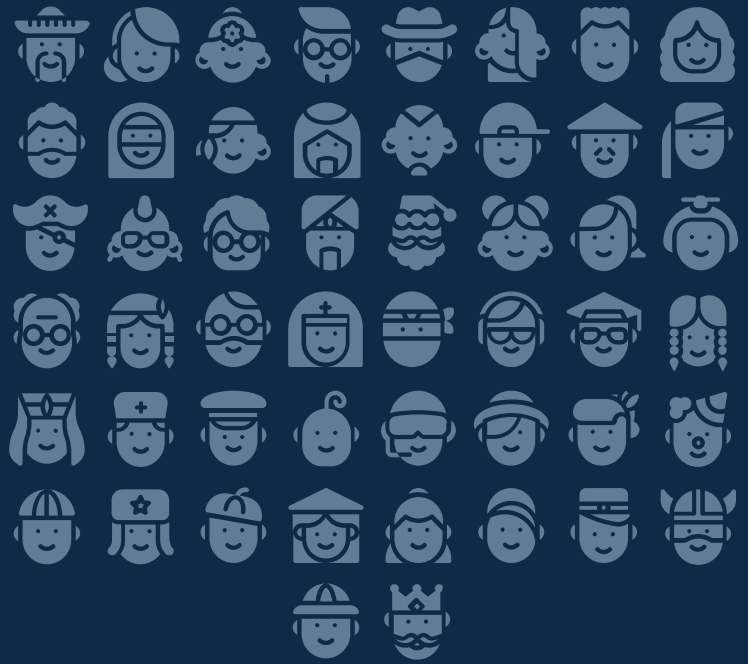
Business Icons

Teamwork Icons

Help & Support Icons



Avatar Icons



Creative Process Icons

Performing Arts Icons

Nature Icons

SEO & Marketing Icons


slidesgo