

# Native modules trên Android và sức mạnh của FRIDA

---

CTF for fun

## NDK, JNI?

Giới thiệu về các khái niệm và tại sao nó liên quan đến Native-lib

01

## NATIVE LIBRARY

Tìm kiếm và xác định native library file

02

# TABLE OF CONTENTS

03

## Hooking with FRIDA

Một số solution hooking với native-lib

04

## Mở rộng

Làm khó rev và hướng giải quyết (theo suy nghĩ cá nhân)

# 01

## NDK, JNI?

---

Something you win, something you learn...



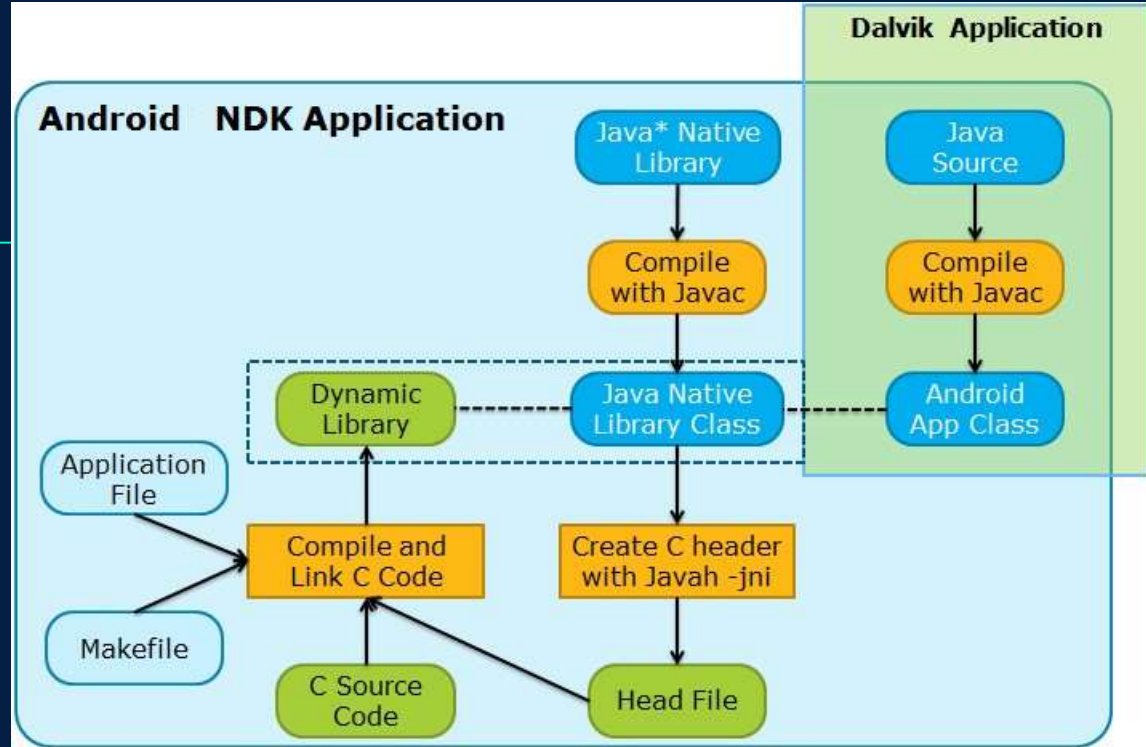
# NDK

## Native Development Kit

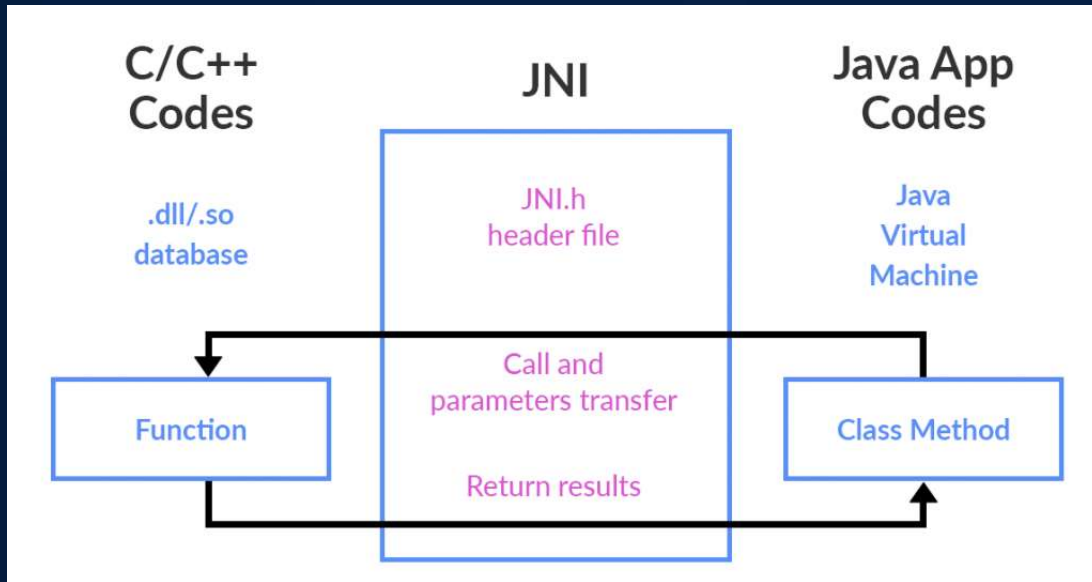
Tool để cho lập trình C/C++ trên thiết Android (bao gồm cả SDK) → cải thiện hiệu năng cho chương trình. Source code sẽ được compile ra mã máy (theo kiến trúc của CPU). Hầu hết các application thường sử dụng cả native-code và java-code để hiệu năng đạt cao nhất.

Nhưng làm thế nào để java-code tương tác được với native-code?

→ JNI



# 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 dụng JNI, C/C++ functions sẽ được map như một method và data types chuyển đến cho Java và ngược lại (như hình).



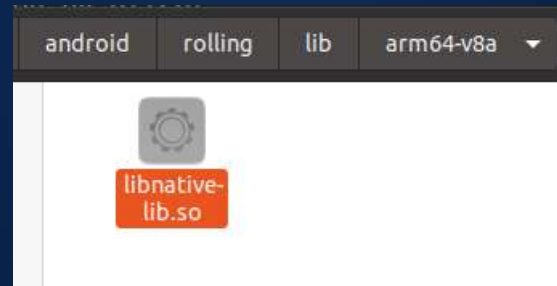
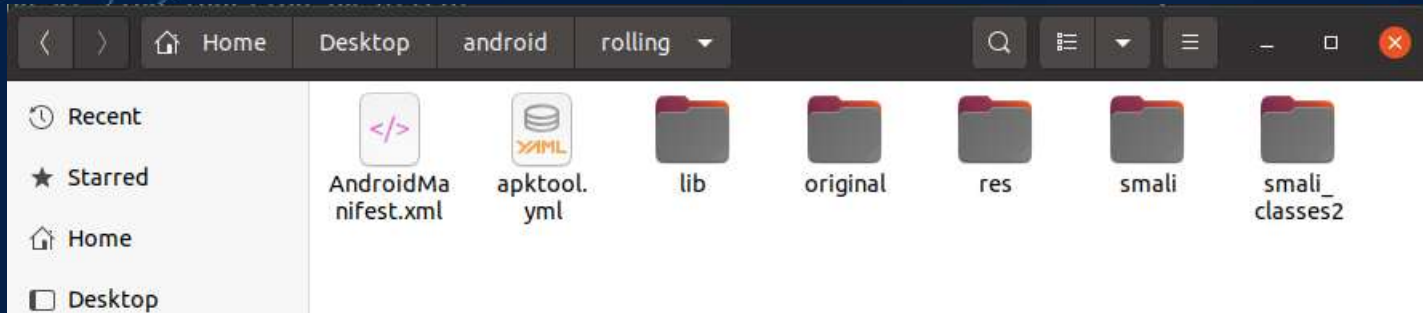
02

**Native Library**

---

# Native library?

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







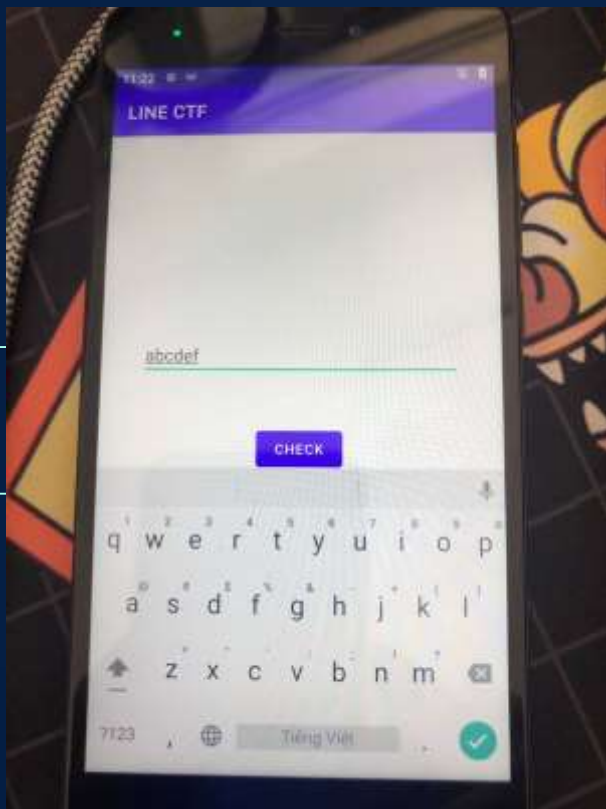
# 03

## Hooking with FRIDA

---



# DEMO



<https://score.linectf.me/challenges>



**Rev sương sương**

# Solution 1: exported functions

```
lanleft@rs: ~/Desktop/android
Frida 15.1.17 - A world-class dynamic instrumentation toolkit

Commands:
  help      -> Displays the help system
  object?   -> Display information about 'object'
  exit/quit -> Exit

More info at https://frida.re/docs/home/

Connected to Redmi Note 4 (id=4409ee330104)
Spawning 'me.linectf.app'...
[+] Solution1: hook export function -----
Spawned 'me.linectf.app'. Resuming main thread!
[Redmi Note 4::me.linectf.app ]-> [+] attach meatbox with args: 61
output value: 13
[+] attach meatbox with args: 62
output value: 12
[+] attach meatbox with args: 63
output value: 1
[+] attach meatbox with args: 64
output value: 6
[+] attach meatbox with args: 65
output value: 13
[+] attach meatbox with args: 66
output value: 7
```

```
script1.js - android - Visual Studio Code
File Edit Selection View Go Run Terminal Help

script1.js x script2.js script3.js script4.js

JS script1.js > ...
1 // console.log("[+] Script loaded successfully")
2 console.log("[+] Solution1: hook export function
   -----")
3
4 setTimeout(function(){
5   Interceptor.attach(Module.getExportByName
   ('libnative-lib.so', '_Z7meatboxPc'), {
6     onEnter: function(args) {
7       var buf = Memory.readByteArray(args[0], 1);
8       var b = new Uint8Array(buf);
9       console.log("[+] attach meatbox with args: "
10        + b[0].toString(16))
11     },
12     onLeave: function(retval) {
13       var buf = Memory.readByteArray(ptr(retval), 1)
14       var b = new Uint8Array(buf);
15       var str = "";
16
17       for(var i = 0; i < b.length; i++) {
18         str += (b[i].toString(16) + " ");
19       }
20       console.log("output value: " + str)
21     }
22   });
23 }, 2000);
```



## Solution 2: offset

```
lanleft@cs: ~/Desktop/android
lanleft@cs:~/Desktop/android$ frida -U -f me.linectf.app -l script3.js --no-pause

Frida 15.1.17 - A world-class dynamic instrumentation toolkit

Commands:
  help           -> Displays the help system
  object?        -> Display information about 'object'
  exit/quit      -> Exit

More info at https://frida.re/docs/home/

Connected to Redmi Note 4 (id=4409ee330104)
Spawning 'me.linectf.app'...
[+] Solution 2: find function by offset -----
Spawned 'me.linectf.app'. Resuming main thread!
[Redmi Note 4::me.linectf.app ]-> [+] attach meatbox with args: 61
=====> output value: 13
[+] attach meatbox with args: 62
=====> output value: 12
[+] attach meatbox with args: 63
=====> output value: 1
[+] attach meatbox with args: 64
=====> output value: 6
[+] attach meatbox with args: 65
=====> output value: 13
[+] attach meatbox with args: 66
=====> output value: 7
[]
```

```
script3.js - android - Visual Studio Code
File Edit Selection View Go Run Terminal Help

# script1.js # script2.js # script3.js X # script4.js

# script3.js > ...
1 console.log("[+] Solution 2: find function by offset
  .....")
2 setTimeout(() => {
3     // solution 23: find function by offset
4
5     Interceptor.attach(Module.findBaseAddress
  ('libnative-lib.so').add(0x1700), {
6         onEnter: function(args) {
7             var buf = Memory.readByteArray(args[0], 1);
8             var b = new Uint8Array(buf);
9             console.log("[+] attach meatbox with args: "
10                + b[0].toString(16))
11         },
12         onLeave: function(retval) {
13             var buf = Memory.readByteArray(ptr(retval), 1)
14             var b = new Uint8Array(buf);
15             var str = "";
16
17             for(var i = 0; i < b.length; i++) {
18                 str += (b[i].toString(16) + " ");
19             }
20             console.log("=====> output value: " +
21                str)
22         }
23     });
24 }, 2000);
25
```

## Solution 3: pattern

```
lanleft@rs: ~/Desktop/android
lanleft@rs:~/Desktop/android$ frida -U -f me.linectf.app -l script2.js --no-pause

Frida 15.1.17 - A world-class dynamic instrumentation toolkit

Commands:
  help           -> Displays the help system
  object?       -> Display information about 'object'
  exit/quit     -> Exit

More info at https://frida.re/docs/home/

Connected to Redmi Note 4 (id=4409ee330104)

Spawning 'me.linectf.app'...
[+] Solution 3: find function by pattern -----
Spawning 'me.linectf.app'. Resuming main thread!
[Redmi Note 4:me.linectf.app] -> Memory.scan() found match at 0x6f2d9cc708 with size32
Memory.scan() complete
[+] attach meatbox with args: 61
=====> output value: 13
[+] attach meatbox with args: 62
=====> output value: 12
[+] attach meatbox with args: 63
=====> output value: 1
[+] attach meatbox with args: 64
=====> output value: 6
[+] attach meatbox with args: 65
=====> output value: 13
[+] attach meatbox with args: 66
=====> output value: 7
```

```
script2.js - android - Visual Studio Code
File Edit Selection View Go Run Terminal Help

JS script1.js JS script2.js JS script3.js JS script4.js

JS script2.js > setTimeout() callback > hookByPattern

18         onLeave: function(retval){
19             var buf = Memory.readByteArray(ptr(retval));
20             var b = new Uint8Array(buf);
21             var str = "";
22
23             for(var i = 0; i < b.length; i++) {
24                 str += (b[i].toString(16) + " ");
25             }
26             console.log("=====> output value: "
27
28         });
29
30         // Optionally stop scanning early:
31         return 'stop';
32     },
33     onComplete: function () {
34         console.log('Memory.scan() complete');
35     }
36 });
37
38
39 var pattern = 'FF 43 05 D1 FC 6F 0F A9 FA 67 10 A9 F8
40
41 hookByPattern(pattern);
42 }, 2000);
43
```

## 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 bi 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?**

???

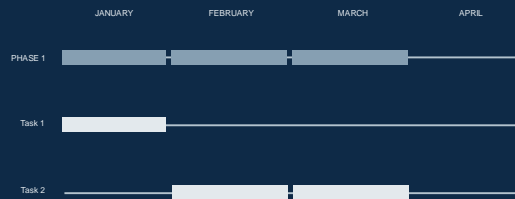
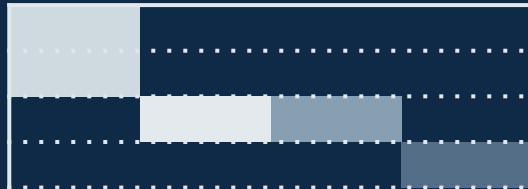
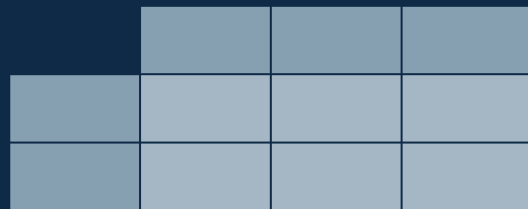
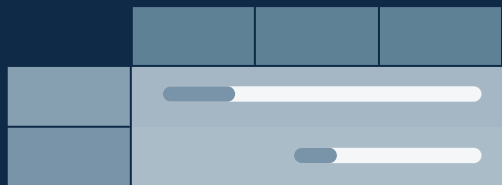
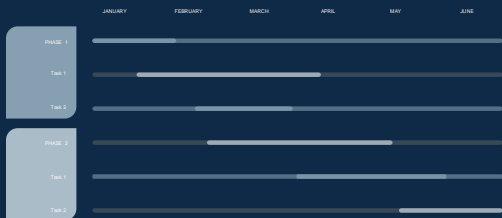
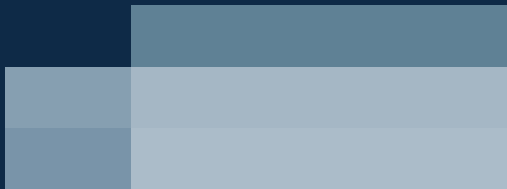
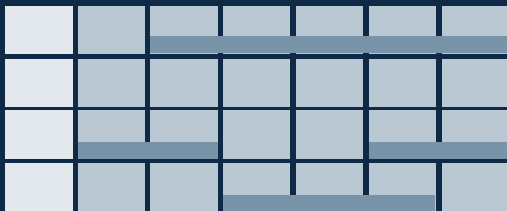


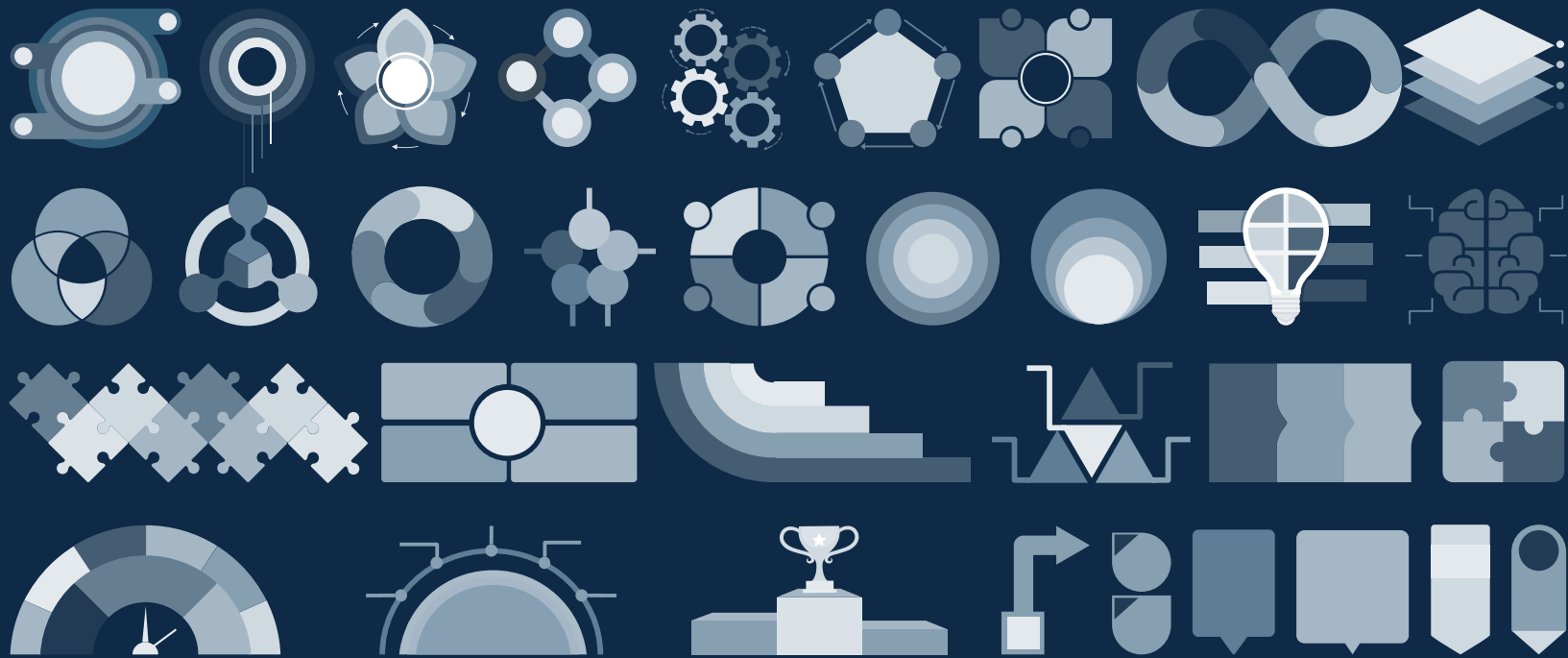
# THANKS

Does anyone have any questions?

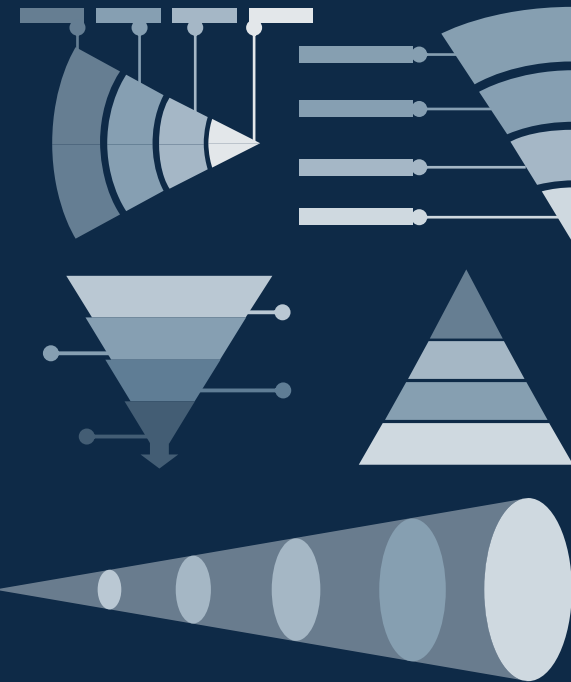
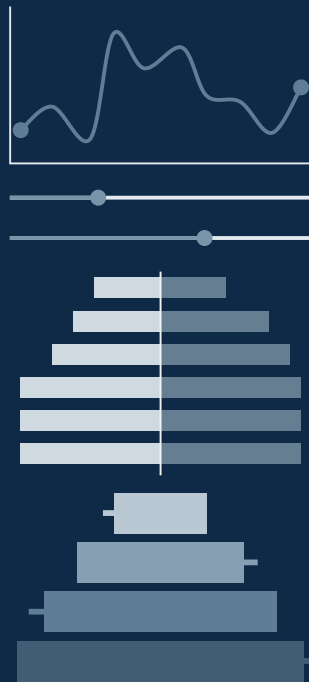
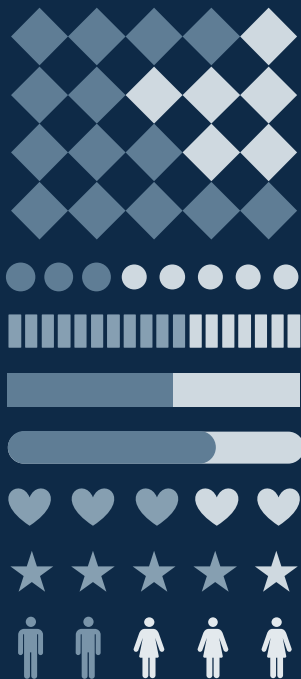
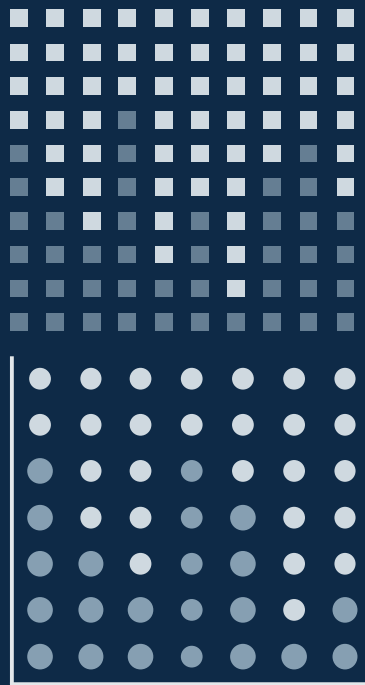
CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, and infographics & images by **Freepik**.

**Please keep this slide for attribution.**









## ...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



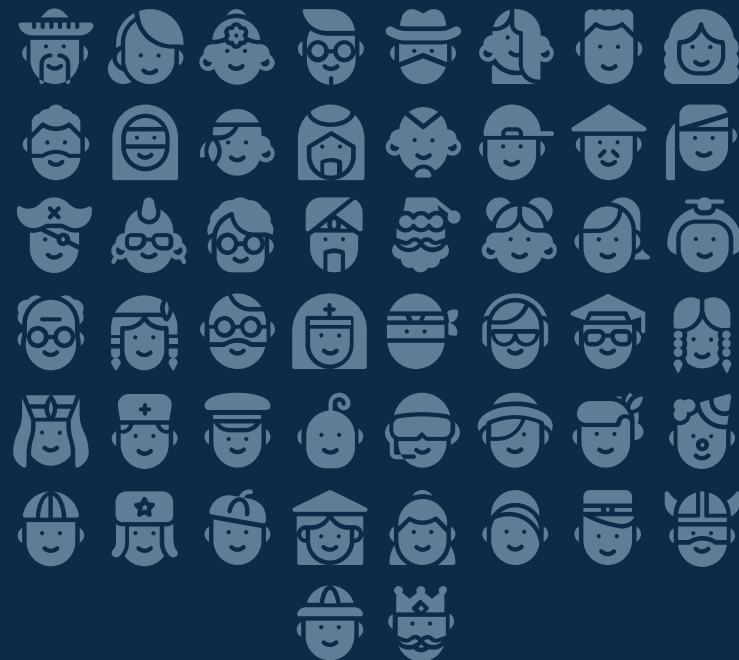
## Teamwork Icons



## Help & Support Icons



## Avatar Icons



# Creative Process Icons



# Performing Arts Icons





# Nature Icons



# SEO & Marketing Icons



