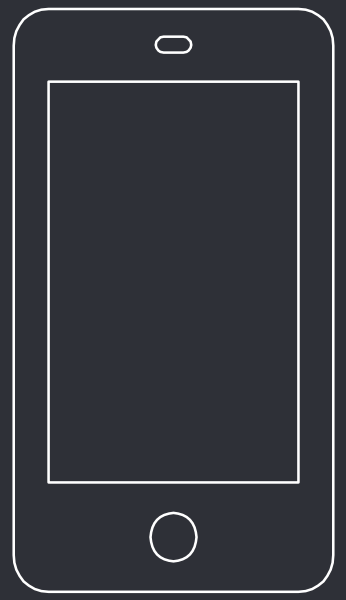
Meticulously Modern Mobile Manipulations



[DEF CON 27, Las Vegas] - Leon Jacobs

$ whoami

- Leon Jacobs / @leonjza
- Security Researcher @ SensePost
- Been Hacking “stuff” for ~ 10 years

I also hated mobile application security a lot more in the past...


LOCAL CALL
10¢
LONG DISTANCE
CROSLEY
LOCAL CALL
10¢
LONG DISTANCE
CROSLEY
LOCAL CALL
10¢
LONG DISTANCE
CROSLEY

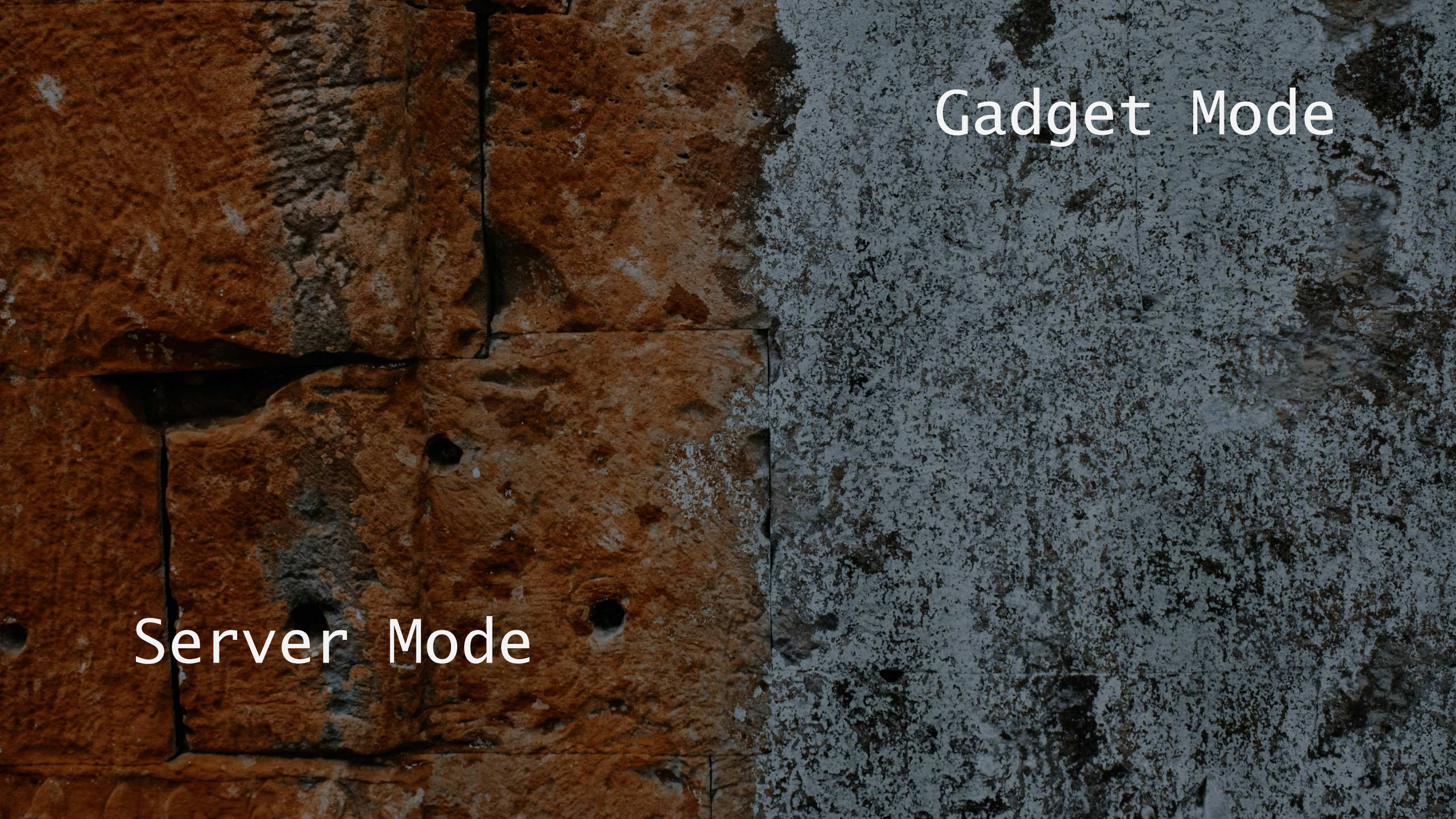
Lets be honest about mobile application hacking

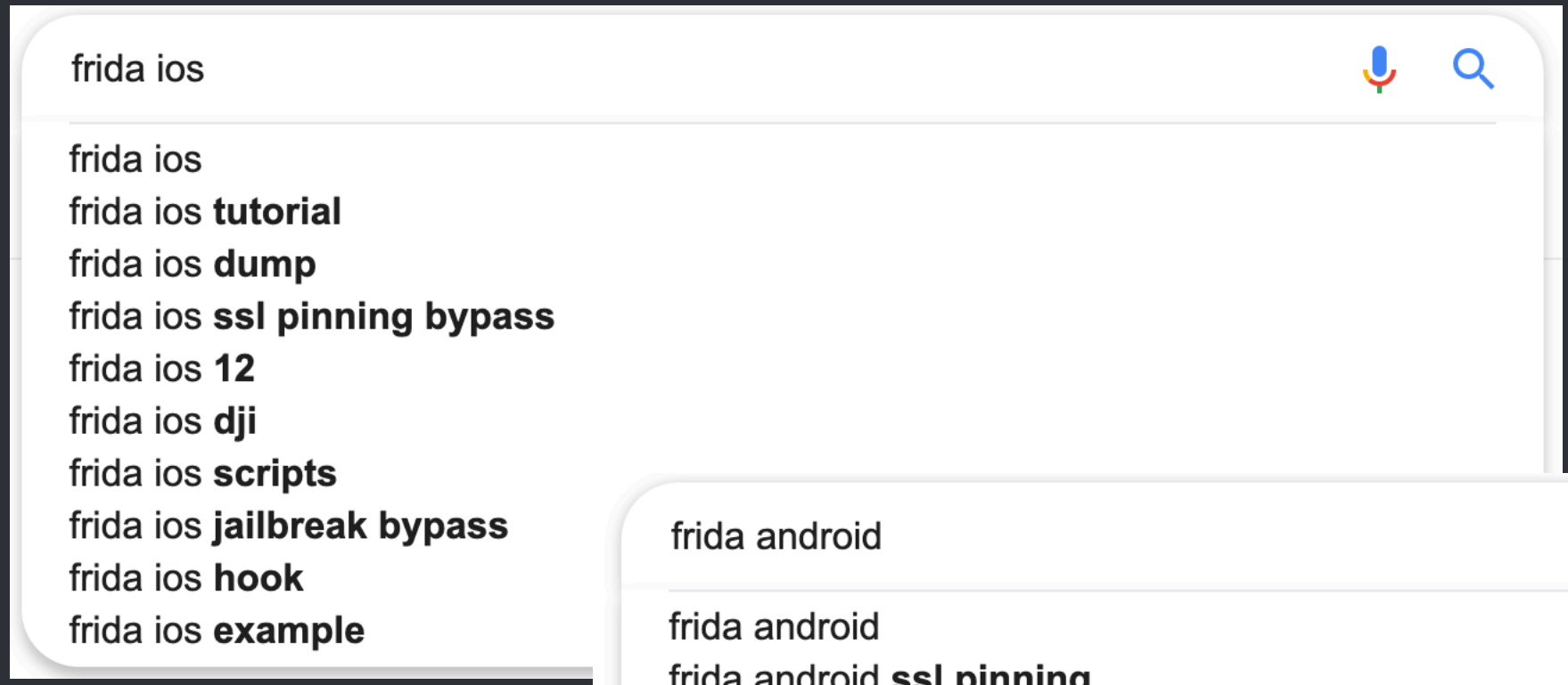
$days since last public jailbreak

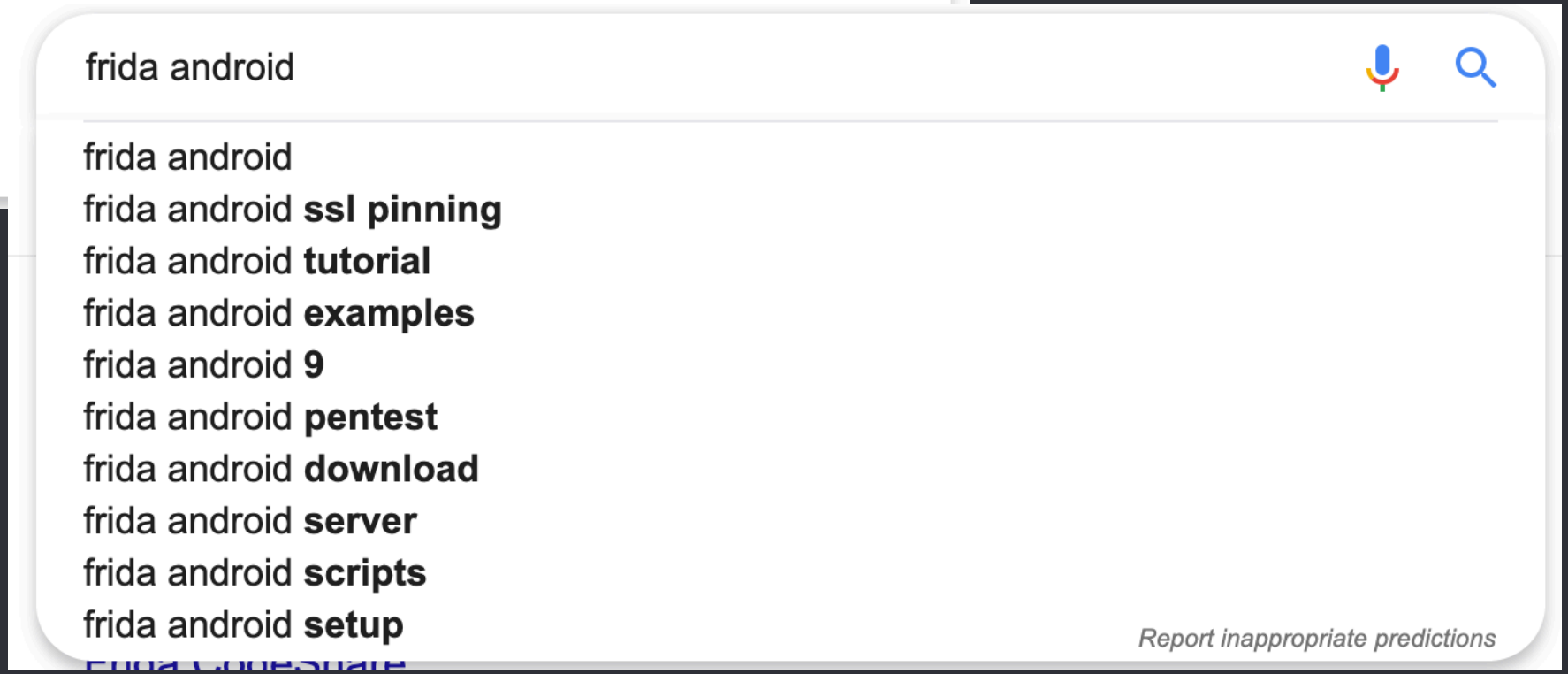

BIG DATA IS
ATCHING YOU

FRIDA


FRIDA

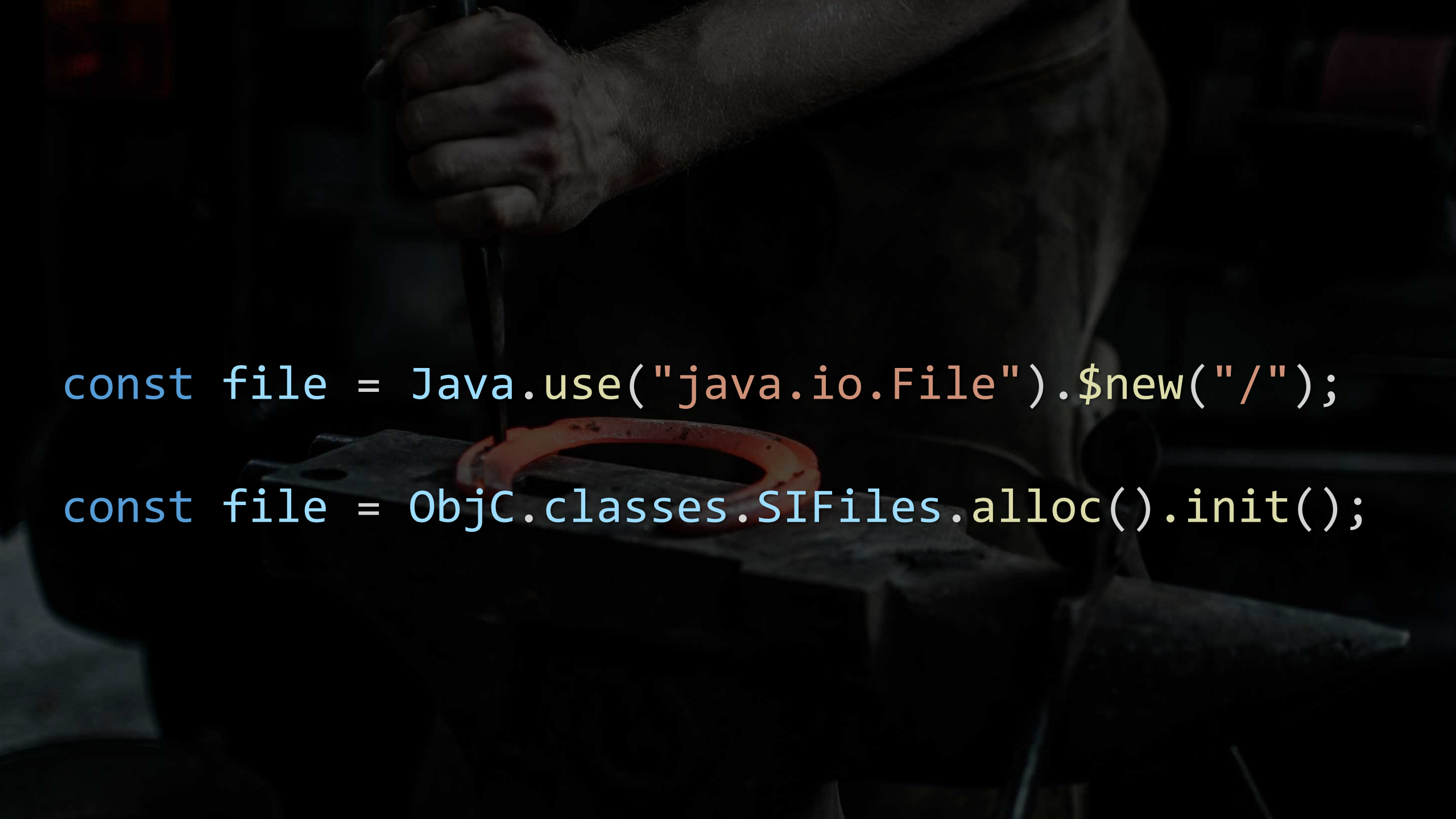

Gadget Mode
Server Mode


frida ios
frida ios
frida ios tutorial
frida ios dump
frida ios ssl pinning bypass
frida ios 12
frida ios dji
frida ios scripts
frida ios jailbreak bypass
frida ios hook
frida ios example

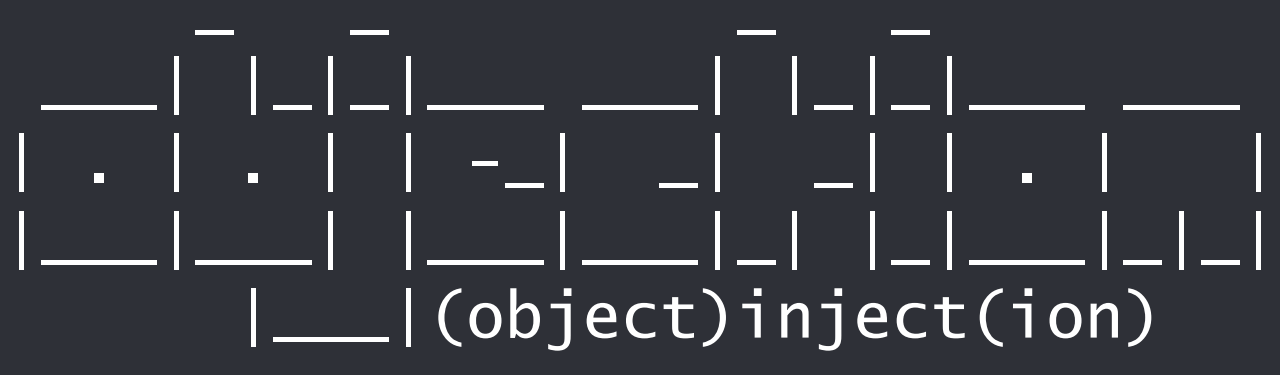

frida android
frida android
frida android ssl pinning
frida android tutorial
frida android examples
frida android 9
frida android pentest
frida android download
frida android server
frida android scripts
frida android setup
Report inappropriate predictions


pinning.checkPin.implementation =
function () {
//
}

That's useful
We can do more


const file = Java.use("java.io.File").$new("/");
const file = ObjC.classes.SIFiles.alloc().init();

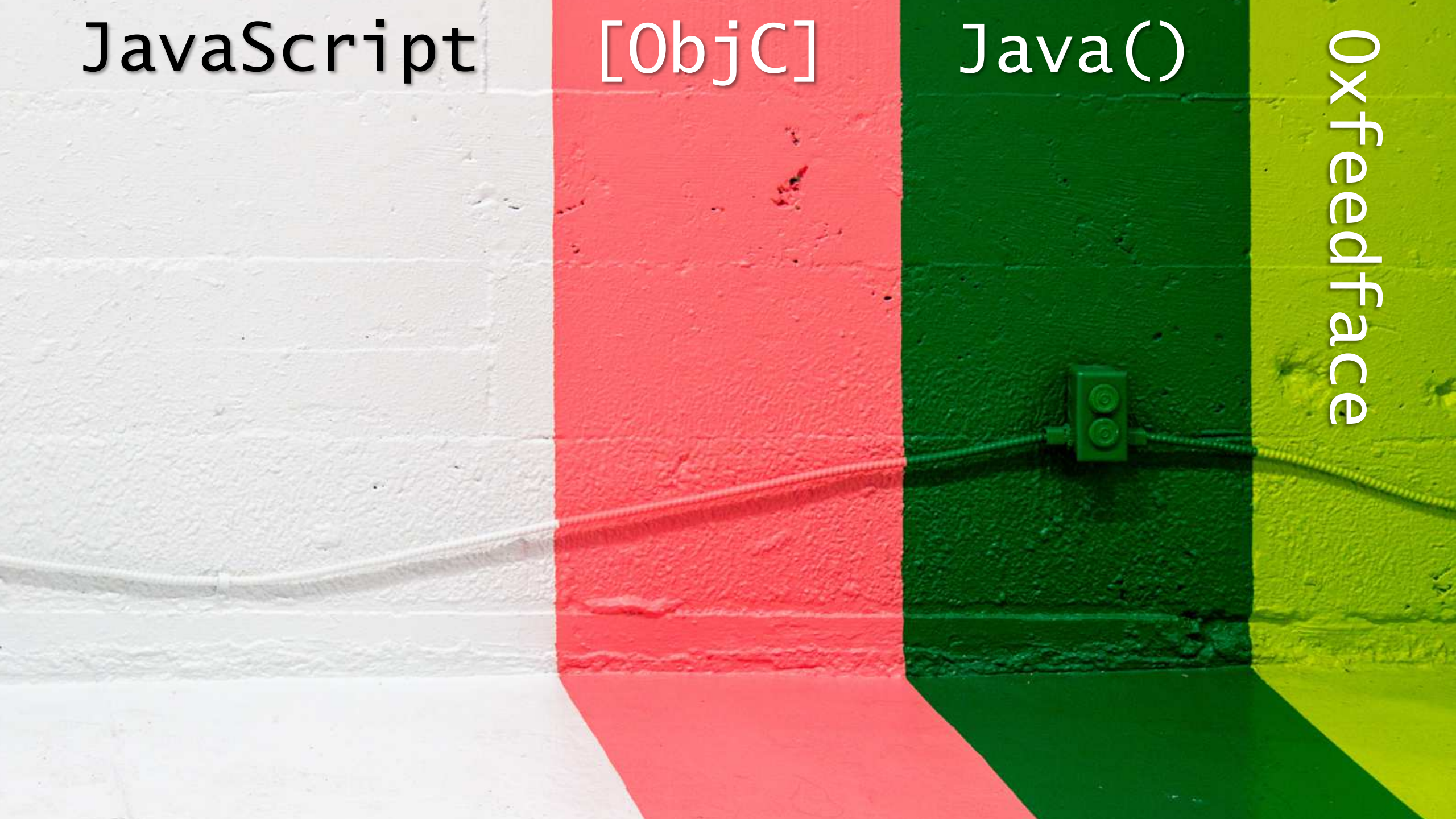
```
za.sensepost.ipewpew on (iPhone: 12.3.1) [usb] # ls
NSFileType    Read    Write    Owner          Size      Creation                    Name
-----------  ------  -------  -----------  --------  --------------------------  ----------------
Regular       True    True     mobile (501)  277.0 B   2019-07-14 14:19:18 +0000  credentials.plist
Regular       True    True     mobile (501)  12.0 KiB  2019-07-14 14:09:06 +0000  pewpew.sqlite

Readable: True  Writable: True
za.sensepost.ipewpew on (iPhone: 12.3.1) [usb] # file download credentials.plist
Downloading /var/mobile/Containers/Data/Application/58BA0C7C-E170-4B43-8F38-E8BE8A8AAF53/Documents/cr
ials.plist to credentials.plist
```



demo

http-file-browser.mov


CRAFTSMAN
NICKEL PLATED
CAYUGA


JavaScript
[ObjC]
Java()
0xfeedface


Application Heaps


Crypto Handlers
Sockets
Config Classes
Class Loaders
State Classes

- Methods get / set properties
- Property values have this data

- Calling methods can alter state

```
Java.choose(className, callbacks);

ObjC.choose(specifier, callbacks);
```

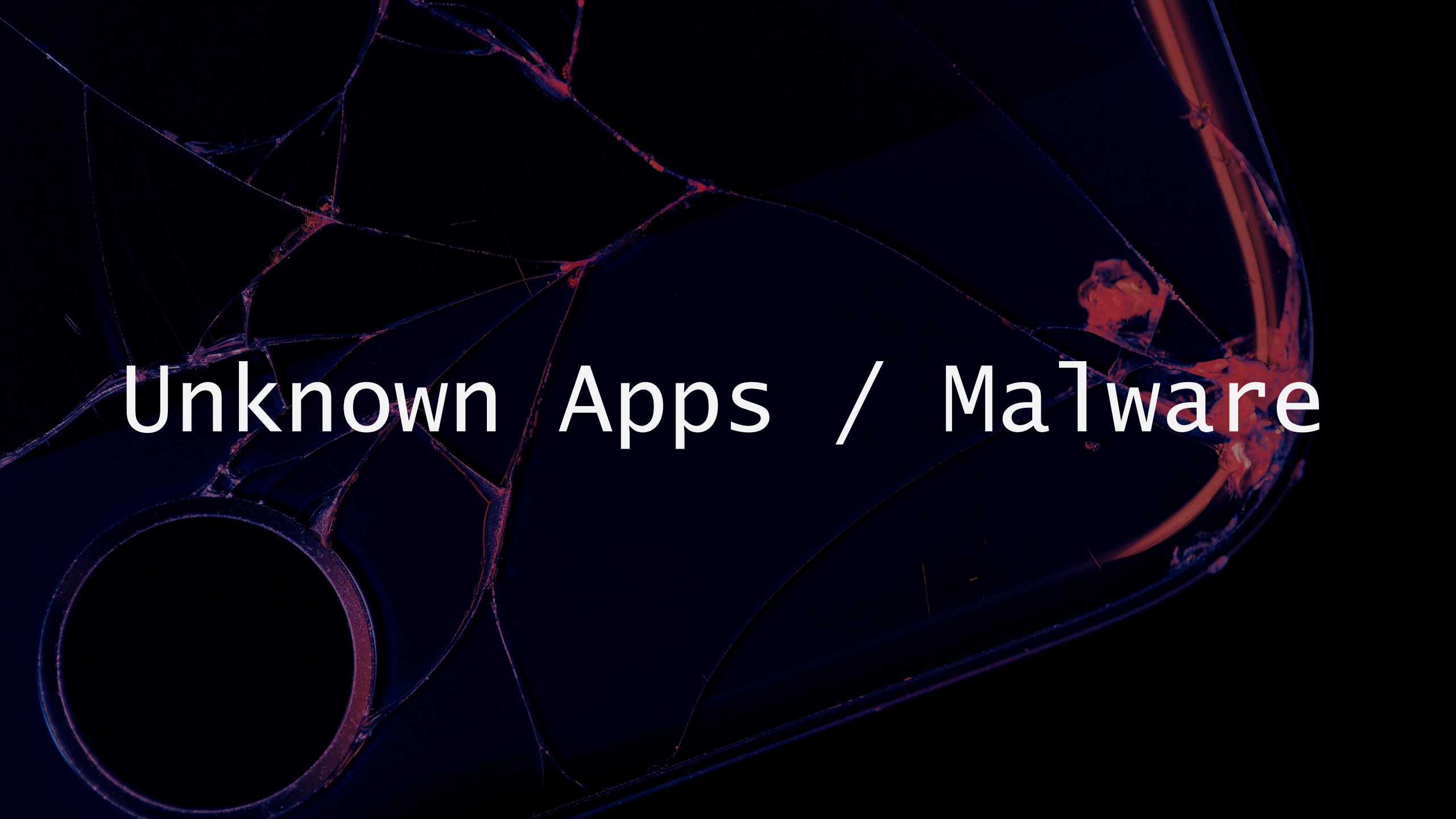
demo

heap-ios-tiktok.mov

dalvik.system.DexClassLoader

```
com.google.android.youtube on (samsung: 7.1.2) [usb] # android heap search instances dalvik.system.DexClassLoader
Using exsiting matches for dalvik.system.DexClassLoader. Use --fresh flag for new instances.
Handle    Class                          toString()
--------  -----------------------------  ------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
0x20073a  dalvik.system.DexClassLoader  dalvik.system.DexClassLoader[DexPathList[[zip file "/data/user/0/com.google.android.youtube/app_dg_cache/3BDC4DF7D61BCB67C4FE6D7A05610D6918A86A00/the.apk"],nativeLibraryDirectories=[/system/lib, /vendor/lib]]]
0x100736  dalvik.system.DexClassLoader  dalvik.system.DexClassLoader[DexPathList[[zip file "/data/user/0/com.google.android.youtube/cache/1548865591327.jar"],nativeLibraryDirectories=[/system/lib, /vendor/lib]]]
com.google.android.youtube on (samsung: 7.1.2) [usb] #
```

```
com.google.android.youtube on (samsung: 7.1.2) [usb] # cd ..
/data/user/0/com.google.android.youtube/app_dg_cache/3BDC4DF7D61BCB67C4FE6D7A05610D6918A86A00
com.google.android.youtube on (samsung: 7.1.2) [usb] # ls
Type       Last Modified              Read    Write    Hidden    Size       Name
---------  -------------------------  ------  -------  --------  ---------  -------
Directory  2019-07-18 18:08:51 GMT    True    True     False     4.0 KiB    opt
File       2019-07-18 18:09:58 GMT    True    True     False     0.0 B      t
File       2019-07-14 18:34:56 GMT    True    True     False     164.4 KiB  the.apk

Readable: True  Writable: True
com.google.android.youtube on (samsung: 7.1.2) [usb] # file download the.apk
Downloading /data/user/0/com.google.android.youtube/app_dg_cache/3BDC4DF7D61BCB67C4FE6D7A05610
 the.apk
Streaming file from device...
Writing bytes to destination...
Successfully downloaded /data/user/0/com.google.android.youtube/app_dg_cache/3BDC4DF7D61BCB67C
0/the.apk to the.apk
```


Unknown Apps / Malware


SAGA
MASTODON
Sonic Youth
JOHN CALE
ENVY
USED LP - R

demo

reflection.mov

Existing Tools

```
Module.load("/path/to/library.dylib");
```

```
const loader = pathClassLoader.$new(
  "/tool.jar", null, getClassLoader());

loader.loadClass("com.tool.Name");
```

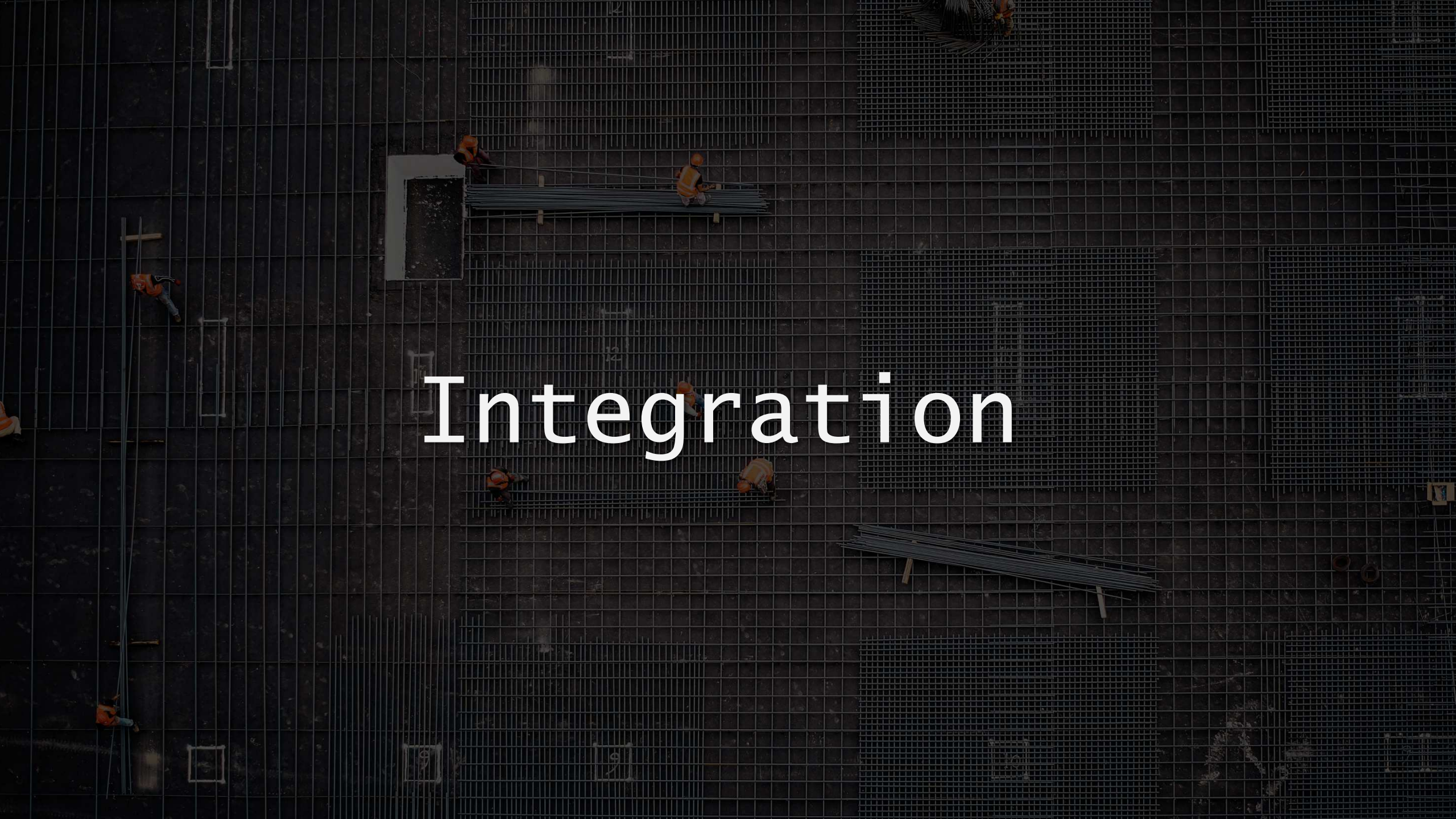
- @Flipboard - FLEX
  https://github.com/Flipboard/FLEX

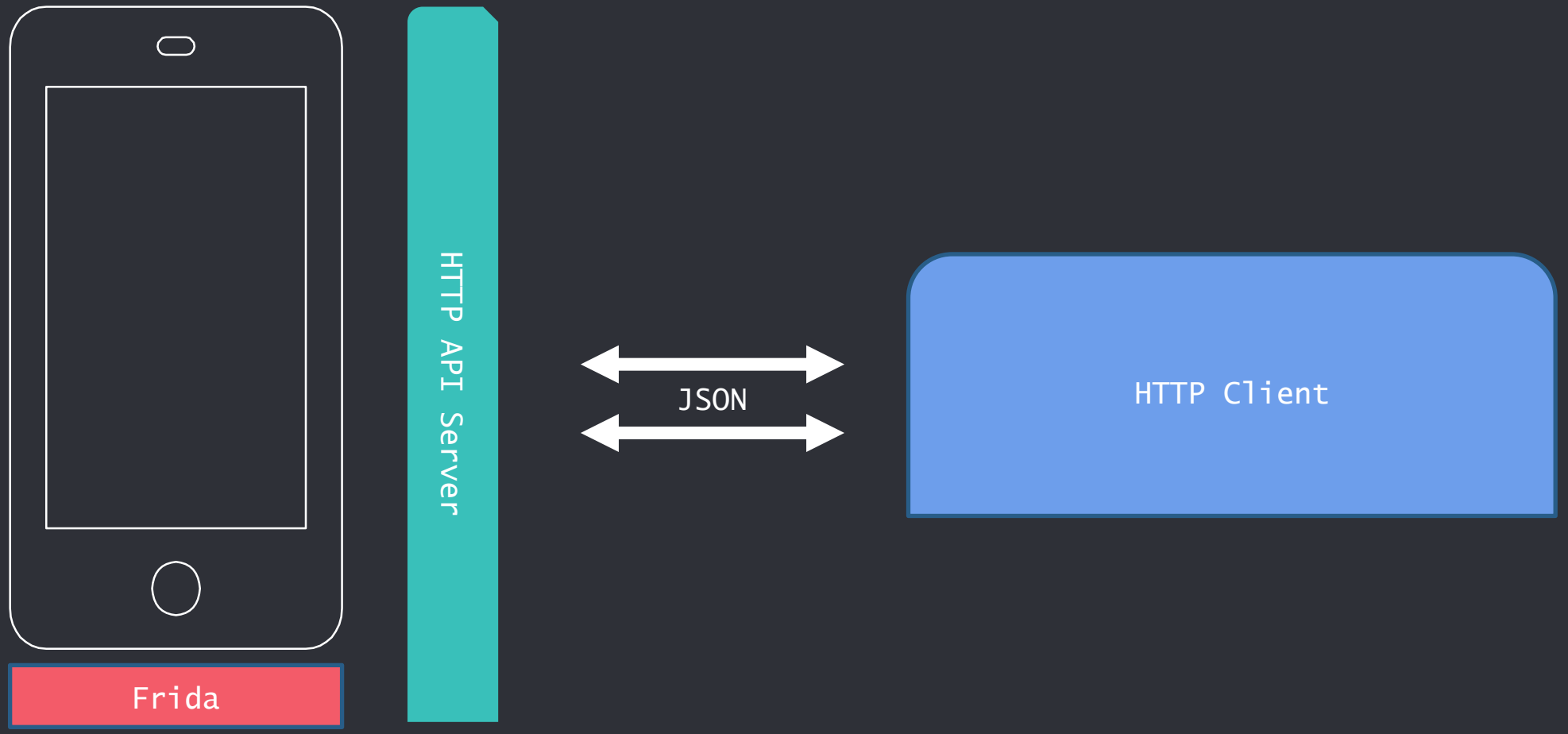
- @Facebook - Stetho
  https://github.com/facebook/stetho

demo

ios-flex-plugin.mov

android-stetho.mov


Integration


HTTP API Server
JSON
HTTP Client
Frida

```
$ curl -s \
       -H "Content-Type: application/json" \
       -X GET http://127.0.0.1:8888/rpc/invoke/iosBinaryInfo | jq --indent 5
{
     "PewPew": {
          "arc": false,
          "canary": true,
          "encrypted": false,
          "pie": true,
          "rootSafe": false,
          "stackExec": false,
          "type": "execute"
     }
}
$
```

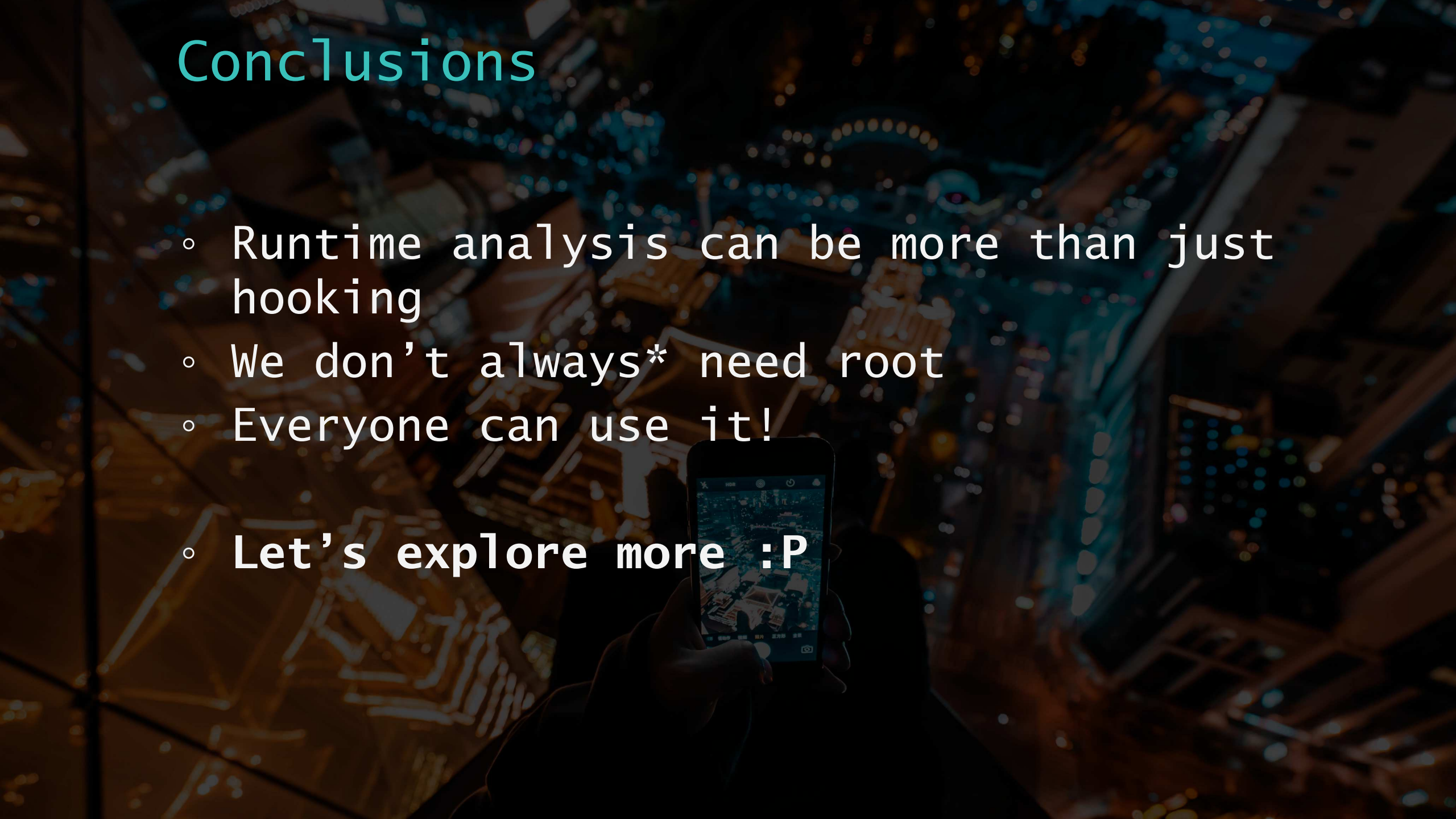
demo

jenkins-binary-protections.mov

Conclusions

- Runtime analysis can be more than just hooking
- We don’t always* need root
- Everyone can use it!

- **Let’s explore more :P**



Thanks!

@leonjza
@sensepost
https://git.io/objection