

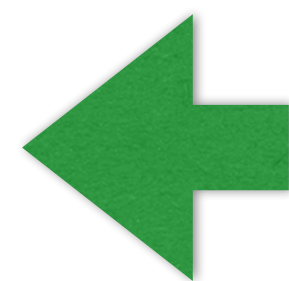
Exploring the Android APK via Pokemon GO



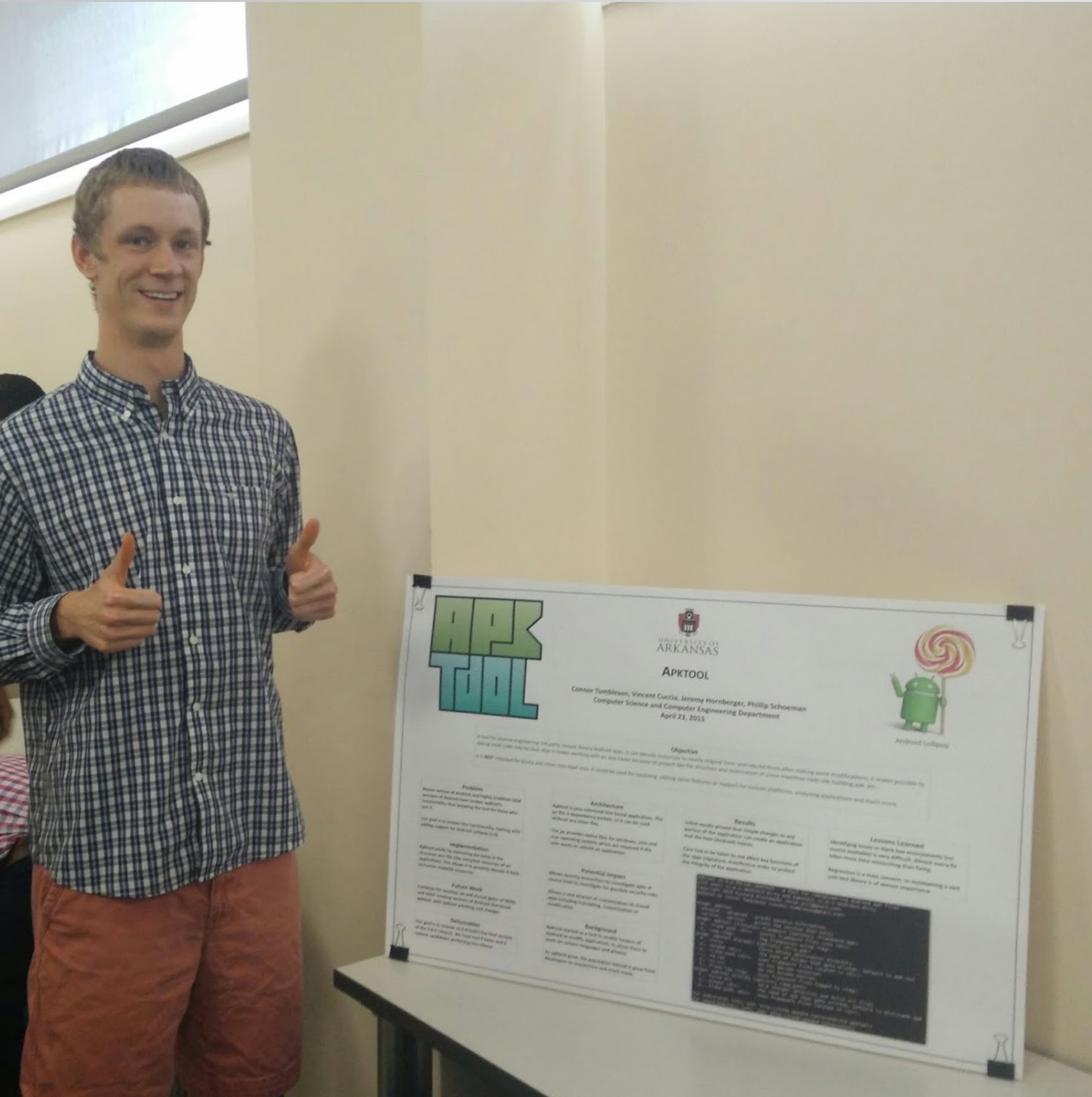
The story of a Cat and a Mouse

- Structure of APK
- Extraction Techniques
- Solutions

Us →



Niantic (Pokemon Go)



Connor Tumbleson

Software Engineer

Apktool Maintainer



@iBotPeaches



connortumbleson.com



Pokemon Go

Why Pokemon?

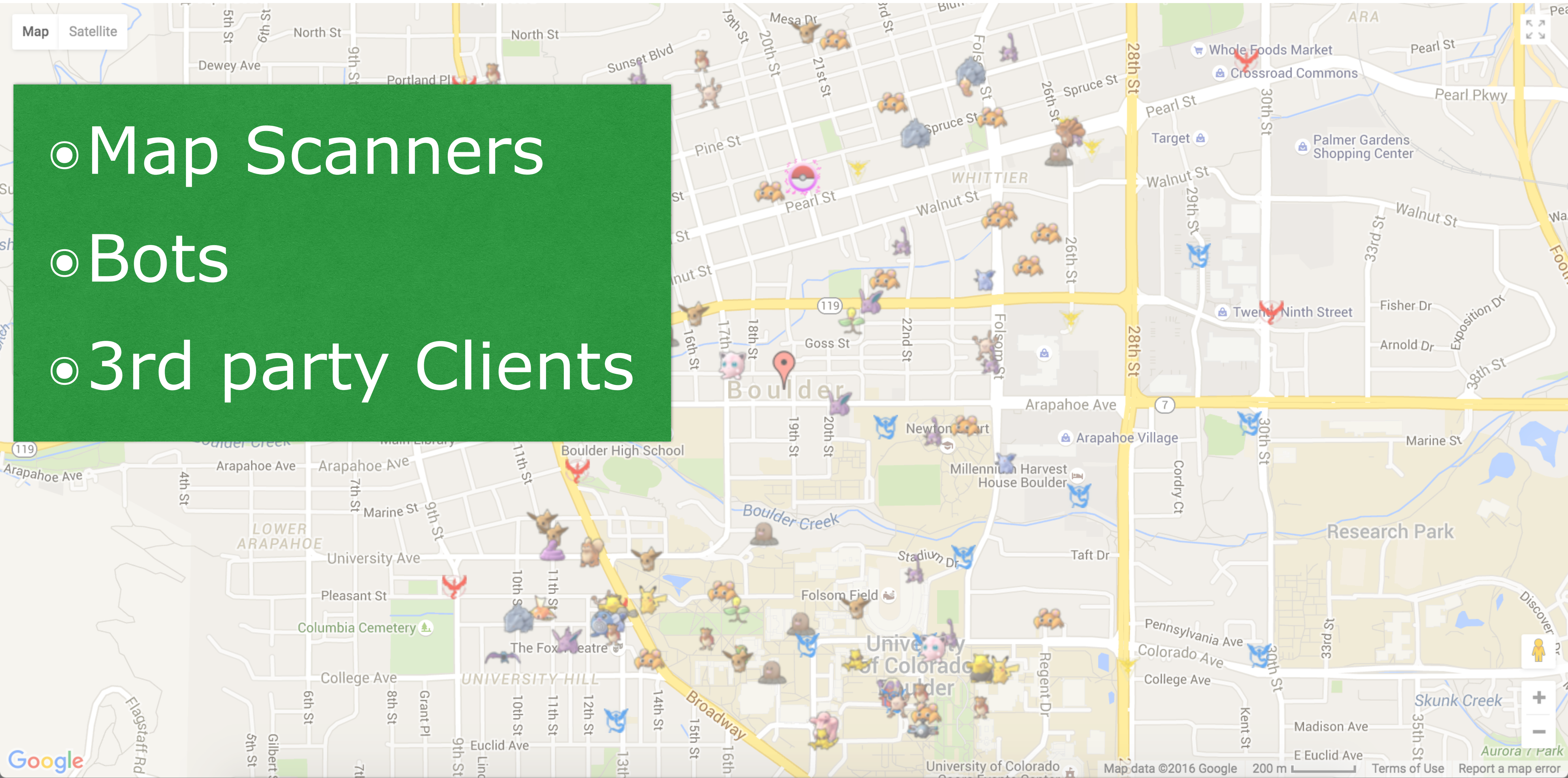
- Popularity
- Rough Launch
- Augmented Reality



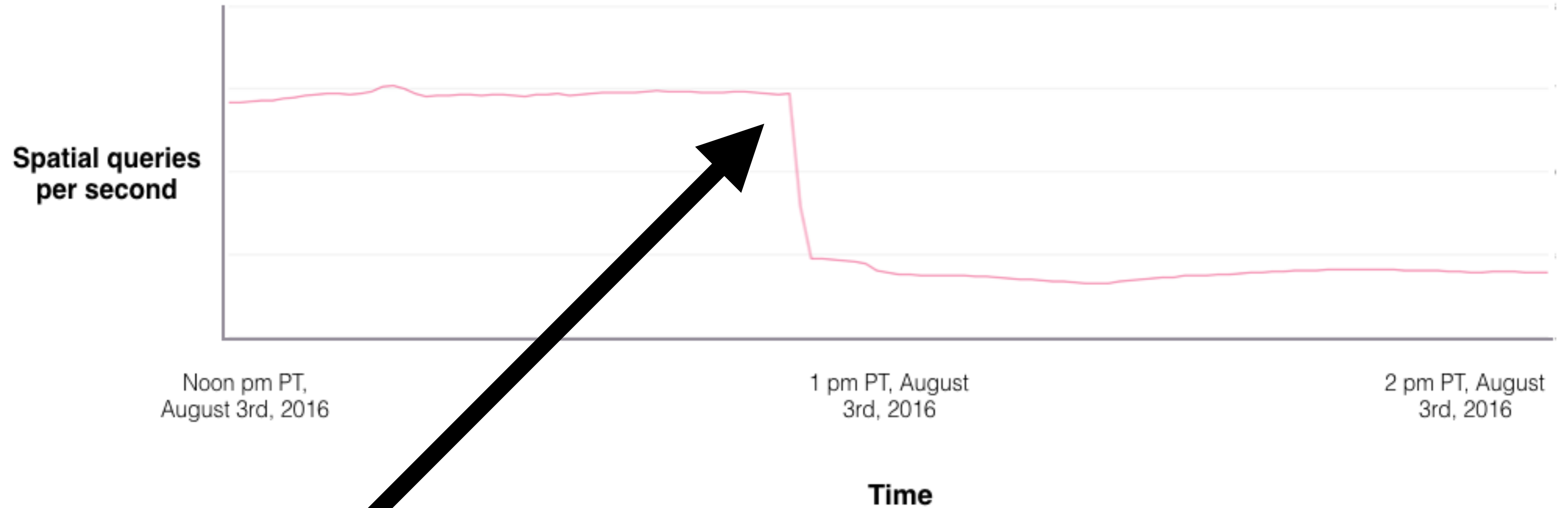
Pokemon Go - Unofficial Project Boom

github.com/AHAAAAAAA/PokemonGo-Map

- Map Scanners
- Bots
- 3rd party Clients



Player Count or API Abuse?



Unofficial API Requests blocked.

Where did it begin?

Where did it begin?



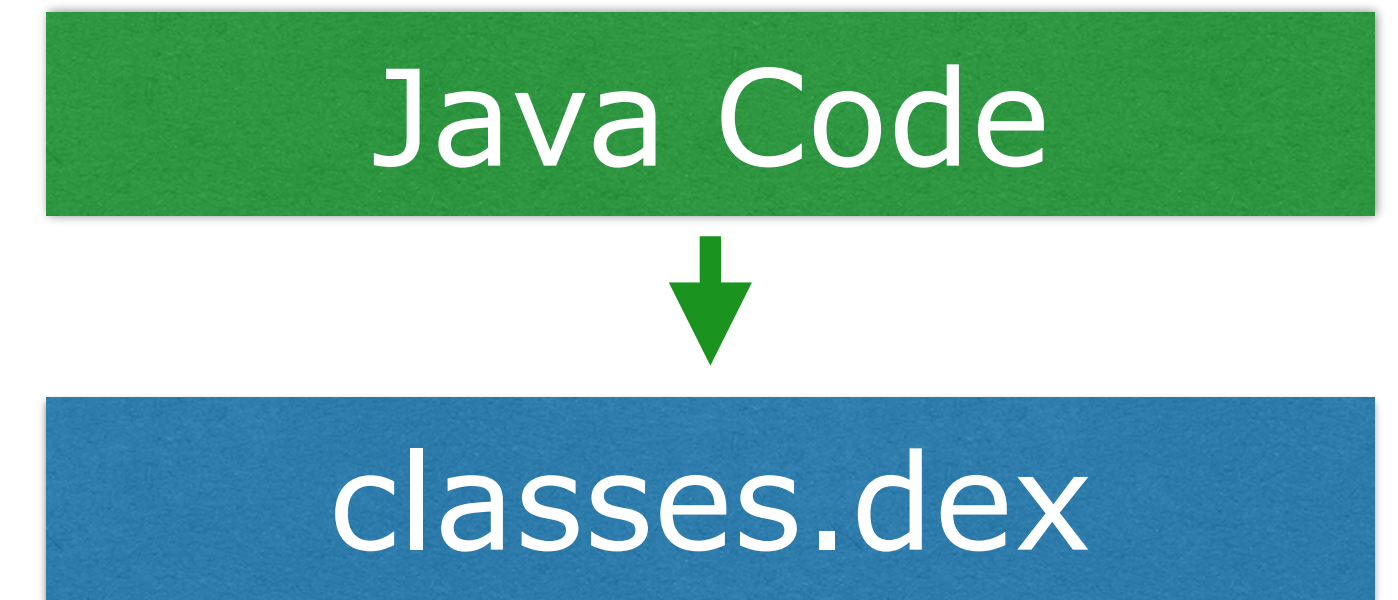
Let's learn about APKs

So let's take a look at Pokemon Go

```
total 6884
-rw-rw-r-- 1 ibotpeaches ibotpeaches 18132 Sep 23 20:14 AndroidManifest.xml
drwxrwxr-x 3 ibotpeaches ibotpeaches 4096 Oct 8 12:51 assets
-rw-rw-r-- 1 ibotpeaches ibotpeaches 6730584 Sep 23 20:08 classes.dex
drwxrwxr-x 3 ibotpeaches ibotpeaches 4096 Oct 8 12:51 lib
drwxrwxr-x 2 ibotpeaches ibotpeaches 4096 Oct 8 12:51 META-INF
drwxrwxr-x 15 ibotpeaches ibotpeaches 4096 Oct 8 12:51 res
-rw-rw-r-- 1 ibotpeaches ibotpeaches 276912 Sep 23 20:07 resources.arsc
→ decoded █
```

So what is in an APK?

- ◉ Java Code
 - ◉ compiled to `.class` (javac)
 - ◉ then to `.dex` (dx)
 - ◉ dex file per 65,000 methods



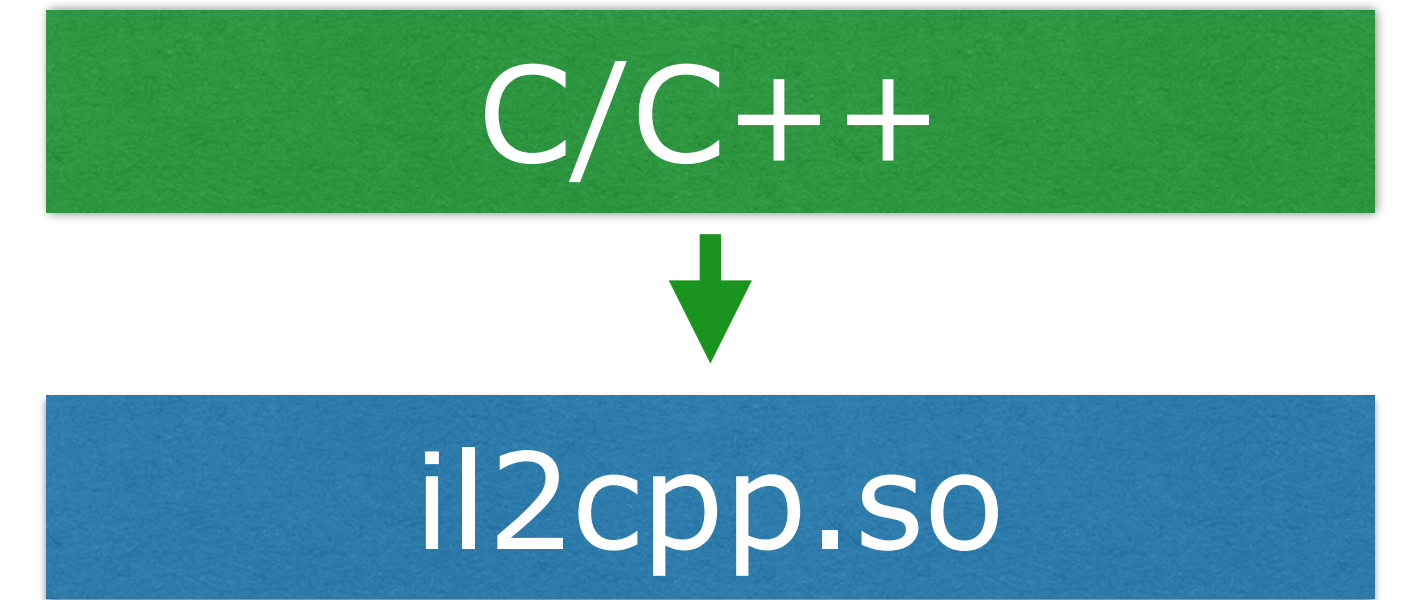
So what is in an APK?

- Resources
 - Strings
 - Layouts
 - Images



So what is in an APK?

- Libraries
 - Game Engines
 - Android NDK
 - Native langs - C / C++



Goals

- ◉ Understand Format
- ◉ Extract
 - ◉ APIs
 - ◉ Assets
- ◉ Rebuild



Meet Apktool

Meet Apktool

(not a plug)

Pokemon Go - Decode

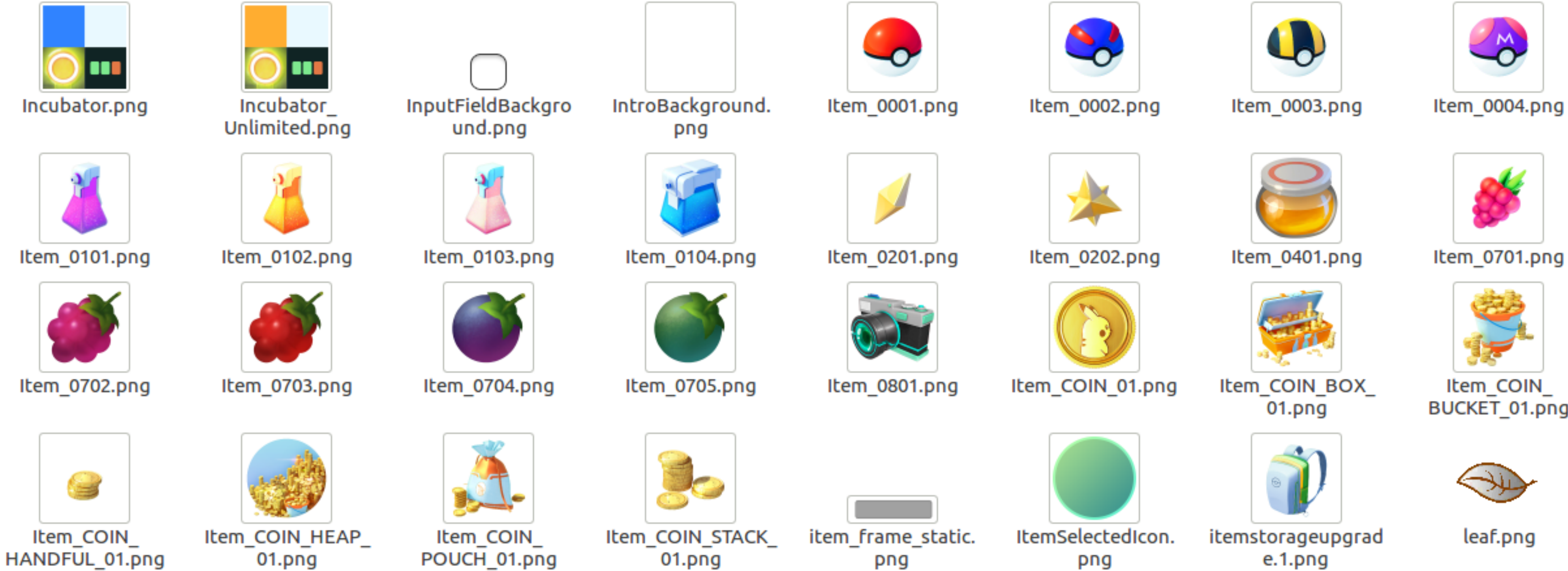
```
→ PokemonGo apktool d pokemon_go.apk -o decoded_apktool
I: Using Apktool 2.2.1-4c93cb-SNAPSHOT on pokemon_go.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/ibotpeaches/.local/share/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
→ PokemonGo █
```

Extraction - Format

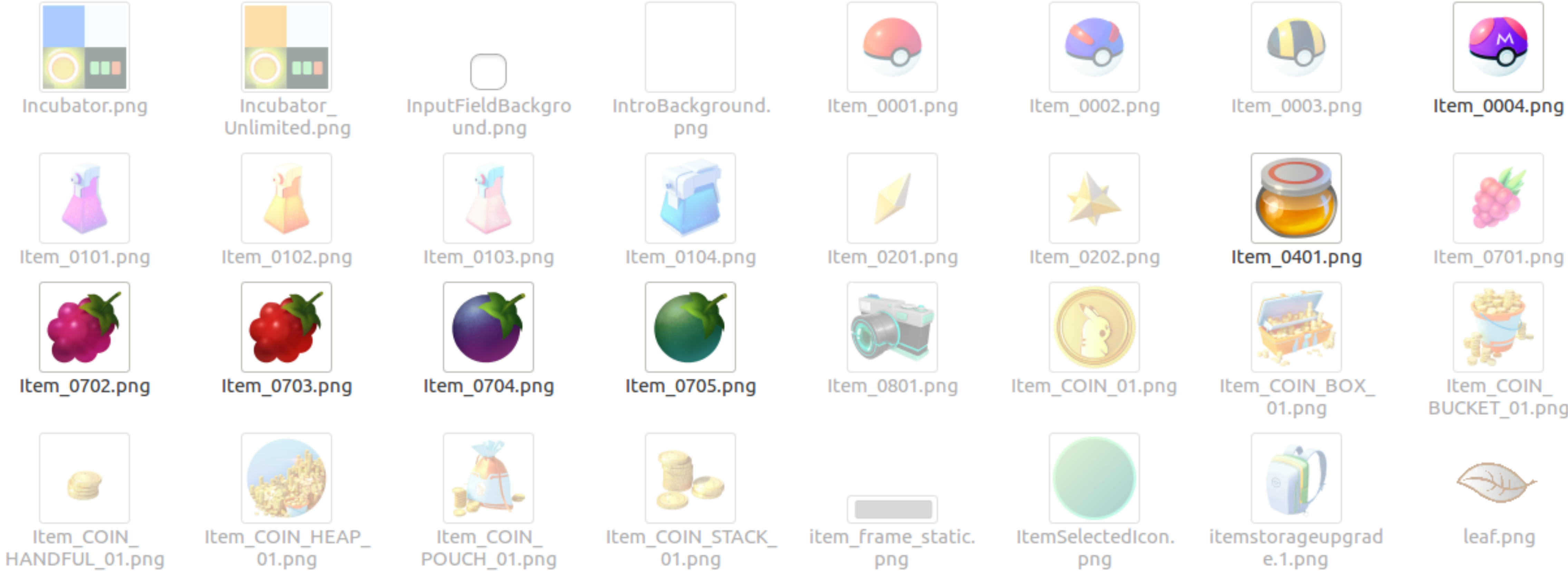
- Unity Game Engine
 - Multi Platform
 - Widely Used



Extraction - Assets



Extraction - Assets



Extraction - Assets



ic_health.png
4.3 kB



ic_inspect.png
7.0 kB



ic_journal.png
3.2 kB



ic_mcd.png
5.1 kB



ic_name.png
2.3 kB



ic_number.png
3.6 kB

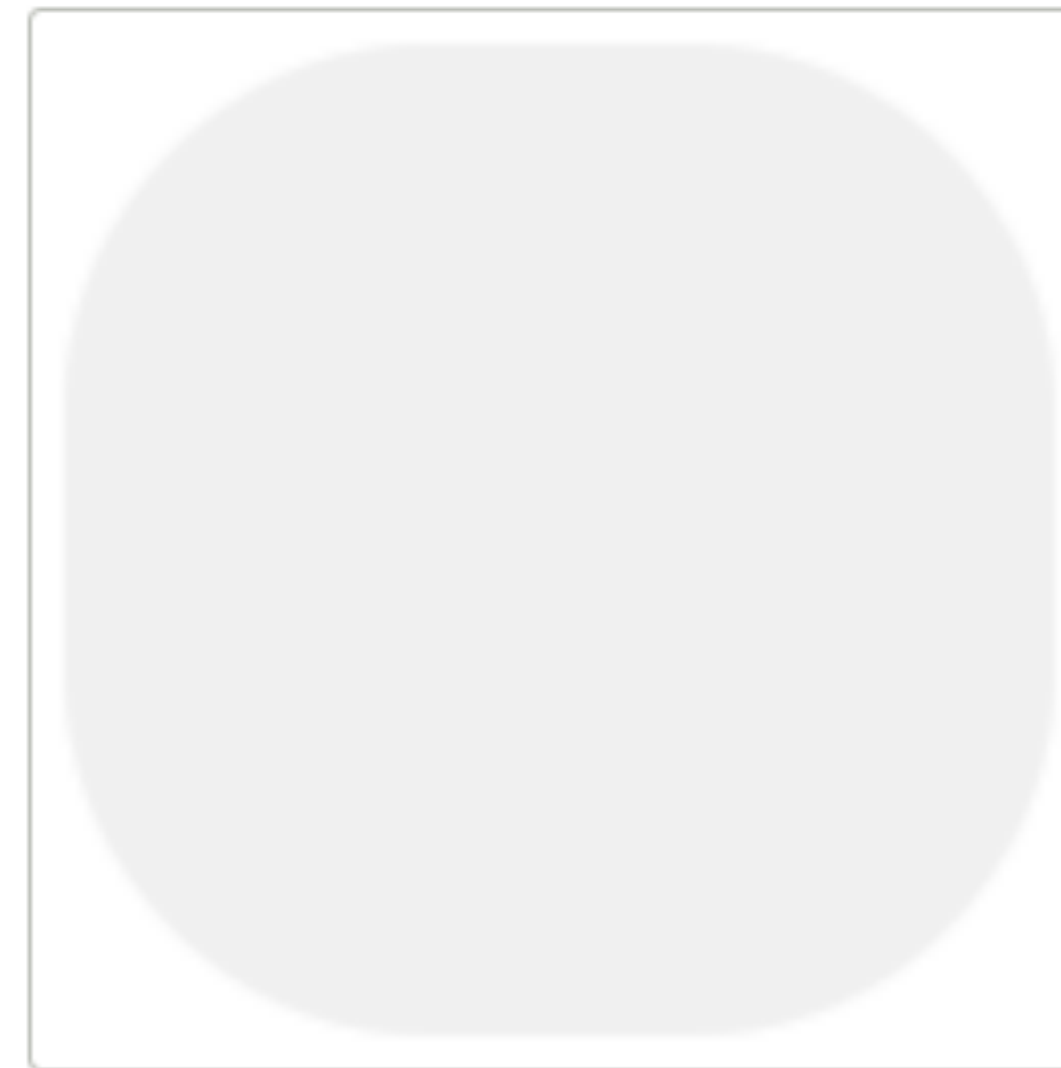
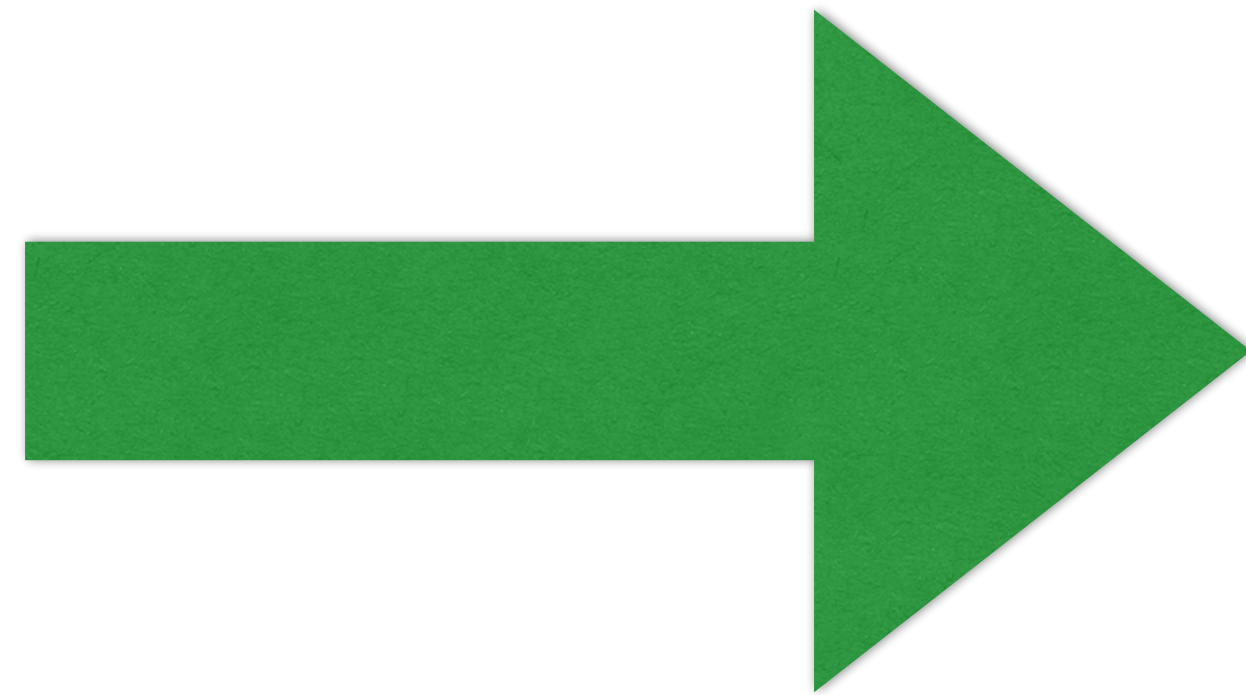
Solution - Assets



- Placeholders
- Download assets on runtime



ic_mcd.png
5.1 kB
Aug 31



sponsor.png
2.3 kB
Aug 31

Extraction - MITM



Host	Path	Start	Duration	Size	Status
stats.unity3d.com	/HWStatsUpdate.cgi	09:48:16	164 ms	633 bytes	Complete
pgorelease.nianticlabs.com	/plfe/rpc	09:48:29	313 ms	1.40 KB	Complete
pgorelease.nianticlabs.com	/plfe/22/rpc	09:48:29	254 ms	1.59 KB	Complete
pgorelease.nianticlabs.com	/plfe/22/rpc	09:48:30	75 ms	1.88 KB	Complete
pgorelease.nianticlabs.com	/plfe/22/rpc	09:48:30	75 ms	1.20 KB	Complete
android.clients.google.com		09:48:30	1933344...	2.38 KB	Sending request bo...
single.upsight-api.com		09:48:31	464 ms	5.80 KB	Complete
pgorelease.nianticlabs.com	/plfe/22/rpc	09:48:32	83 ms	11.76 KB	Complete
pgorelease.nianticlabs.com	/plfe/22/rpc	09:48:32	194 ms	46.81 KB	Complete
bootstrap.upsight-api.com	/config/v1/a9cc12f87adc420baf964f187672ecb4/	09:48:32	104 ms	2.52 KB	Complete
www.google.com		09:48:33	1933342...	5.87 KB	Sending request bo...
pgorelease.nianticlabs.com	/plfe/22/rpc	09:48:33	114 ms	1.44 KB	Complete
pgorelease.nianticlabs.com	/plfe/22/rpc	09:48:34	84 ms	2.42 KB	Complete
pgorelease.nianticlabs.com	/plfe/22/rpc	09:48:34	84 ms	11.83 KB	Complete

- Man in the Middle
 - Peek into SSL traffic

Extraction - MITM



● Not exactly readable

Overview Request Response Summary Chart Notes

```
1 0000000à00«k" 0000(¬0"0Ø0"0~"00"000"002"000£0
2 0uò0pÐ¼45T20K1{Œ¥;k¼4Â1ãŒ00¿>²²0&T∞»Ñ}EÆ²Á7³¿Q¶0Ú»"ÜÙÉÓ#Àê0Œ0@p!00ò0é;ì@0Å00i0p0í00çç7p|Mx0½'L0000Z²ül-4 Ê
0 tŒ000-?+"
3 õqh"µ0ë]'05f0<0æTàÊÀ°^ik²0çòg,ø00)Œ00ý00~00àiz"yúÓ"0¶";0ò00±Jç¬Œzr0<?W"!iüg 0h0VT[0»Y¬02©äl,0³/4ÂST¼4Ý|Rax0ì¥»RÝ±lSD
XÍ0D(KµÚâ00áßW0Œ4±YöGU·ý0<C·;0öÝ0p0z§'§§qD0ñÁ4D0ç0z0'²e0®,s«i°ÀM¶x)sc01Æ1"â¥-0m0ÜÉqâbõçÂm"ê
4 S0Ð000á%eovú00¿JŒ-0-000:cÄvV0xM00ñß00u60D0'Áûç0Éð00§0$µL0±0°00Ð'ÍÓYâ00Œ0Rs0000Ú¬-ì'0°0@ŒwiÑ0T;050OìÂ00000`ld
@AàéxTÀl@á06@Z[
5 @Rç0·ð¥Ä#503ä0o0-K %bB|QËPýZý#Z³GQï0Æñ0aï~(0©ã09;^µ'Â=xy-±Úã«0!00iô«ë*0000A$ú$ë¥ÛUéâ'0¼0`ã0
```

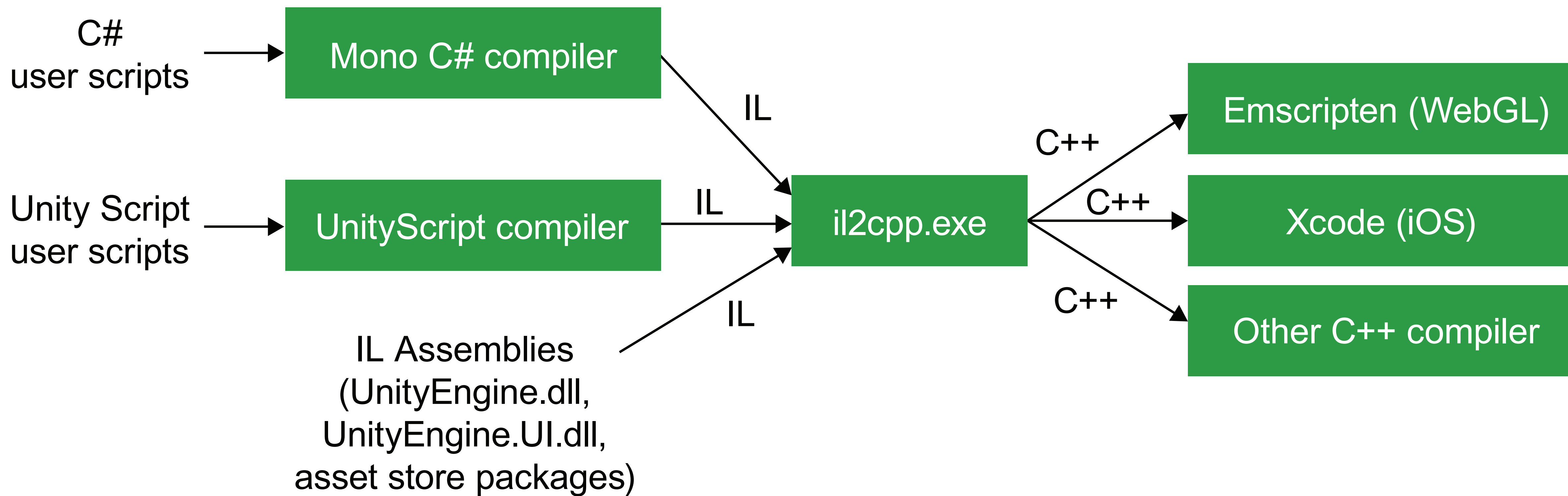
Google - Protocol Buffers

Protocol buffers are Google's language-neutral, platform-neutral, extensible mechanism for serializing structured data – think XML, but smaller, faster, and simpler.

```
message Person {  
  required string name = 1;  
  required int32 id = 2;  
  optional string email = 3;  
}
```

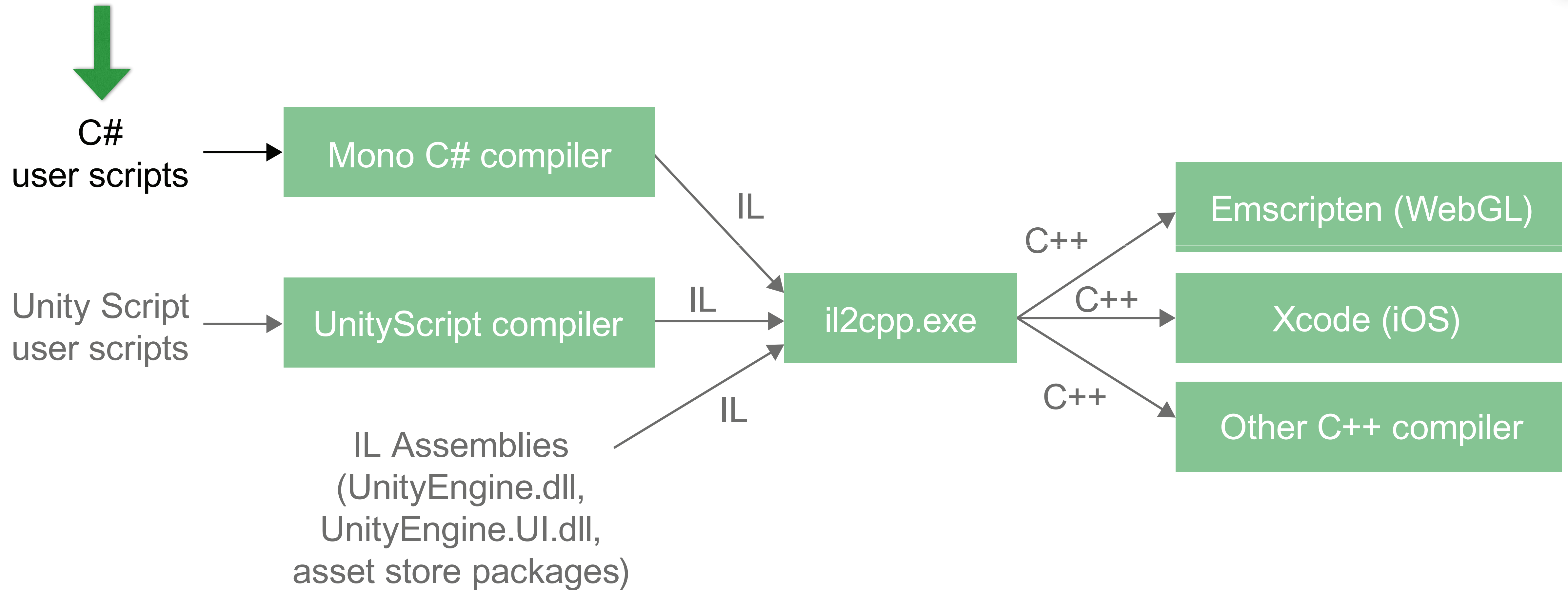



Extraction - il2cpp





Extraction - il2cpp



Extraction - protobuf



```
// Namespace: Niantic.Holoholo.Battle
public sealed class BattleStatus
{
    // Fields
    public int value__;
    public static BattleStatus Unset = 0;
    public static BattleStatus Active = 1;
    public static BattleStatus Victory = 2;
    public static BattleStatus Defeat = 3;
    public static BattleStatus TimedOut = 4;
    public static BattleStatus Quit = 5;
    public static BattleStatus Error = 6;
    // Methods
}
```

Extraction - MITM



```
22 message DownloadItemTemplatesResponse {
23     bool success = 1; ←
24     repeated .POGOProtos.Networking.Responses.DownloadItemTemplatesResponse.ItemTemplate item_templates = 2;
25     uint64 timestamp_ms = 3;
26
27 message ItemTemplate {
28     string template_id = 1;
29     .POGOProtos.Settings.Master.PokemonSettings pokemon_settings = 2;
30     .POGOProtos.Settings.Master.ItemSettings item_settings = 3;
```

```
3673 }
3674 item_templates {
3675     template_id: "V0040_MOVE_BLIZZARD"
3676     move_settings {
3677         movement_id: BLIZZARD
3678         animation_id: 5
3679         pokemon_type: POKEMON_TYPE_ICE
3680         power: 100
3681         accuracy_chance: 1
3682         critical_chance: 0.05
3683         stamina_loss_scalar: 0.11
3684         trainer_level_min: 1
3685         trainer_level_max: 100
3686         vfx_name: "blizzard"
3687         duration_ms: 3900
3688         damage_window_start_ms: 3600
3689         damage_window_end_ms: 3600
3690         energy_delta: -100
3691     }
3692 }
3693 item_templates {
3694     template_id: "V0040_POKEMON_WIGGLYTUFF"
3695     pokemon_settings {
3696         pokemon_id: WIGGLYTUFF
3697         model_scale: 0.89
3698         type: POKEMON_TYPE_NORMAL
3699         type_2: POKEMON_TYPE_FAIRY
```

- Understand Request
- Edit Requests
- Bonus: Precise values

Solution - Sniffing

- SSL Pinning
- Not in launch
- Added in 0.31



Unable to authenticate. Please
try again.

OK





Extraction - Diff Report

New

- location
 - FusedLocationProvider\$4.smali
 - FusedLocationProvider.smali
- network
 - NiaNet.smali
 - NianticTrustManager.smali**



● NianticTrustManager.smali

● hmmm

Old

- location
 - FusedLocationProvider\$4.smali
 - FusedLocationProvider.smali
- network
 - NiaNet.smali
 - NianticTrustManager.smali

Extraction - smali

```
# virtual methods
.method public checkClientTrusted([Ljava/security/cert/X509Certificate;Ljava/lang/String;)V
    .locals 2
    .param p1, "chain"      # [Ljava/security/cert/X509Certificate;
    .param p2, "authType"   # Ljava/lang/String;
    .annotation system Ldalvik/annotation/Throws;
        value = {
            Ljava/security/cert/CertificateException;
        }
    .end annotation

    .prologue
    .line 30
    iget-object v1, p0, Lcom/nianticlabs/ni/network/NianticTrustManager; ->callbackLock:Ljava/lang/Object;
```

Extraction - smali patched

```
# virtual methods
```

```
.method public checkClientTrusted([Ljava/security/cert/X509Certificate;Ljava/lang/String;)V
```

```
return-void
```

```
.locals 2
```

```
.param p1, "chain" # [Ljava/security/cert/X509Certificate;
```

```
.param p2, "authType" # Ljava/lang/String;
```

```
.annotation system Ldalvik/annotation/Throws;
```

```
value = {
```

```
    Ljava/security/cert/CertificateException;
```

```
}
```

```
.end annotation
```

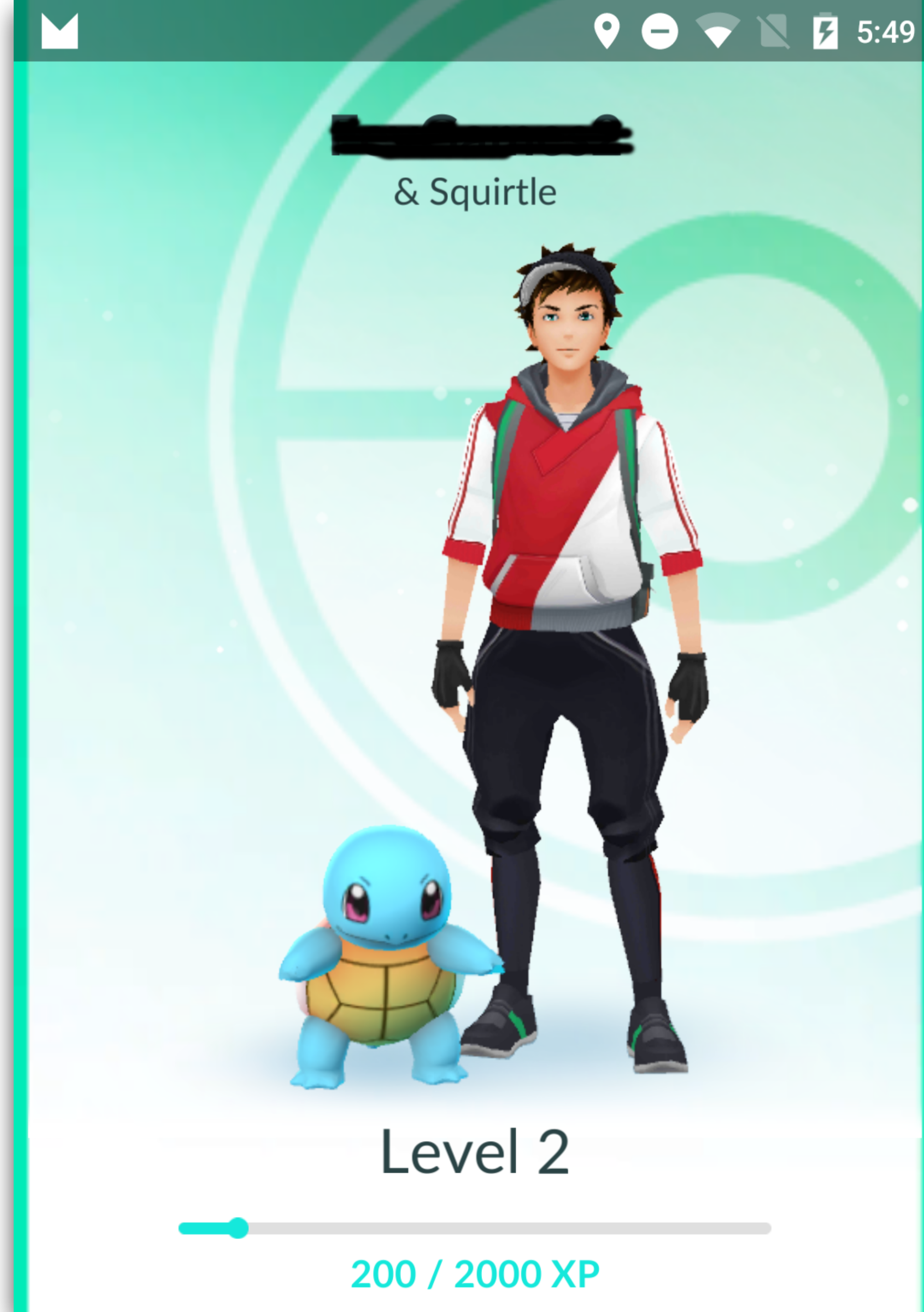
```
.prologue
```

```
.line 30
```

```
iget-object v1, p0, Lcom/nianticlabs/nia/network/NianticTrustManager;->callbackLock:Ljava/lang/Object;
```


Extraction - Rebuild Complete

- We are back
- Caveat: Google Auth



Solution - Java Obfuscation



 o	163.8 kB
 a\$if.smali	1.5 kB
 a\$'.smali	1.1 kB
 a.smali	11.1 kB
 aa.smali	27.9 kB
 aaa.smali	1.7 kB
 aab\$1.smali	733 B
 aab\$if.smali	1.8 kB
 aab.smali	9.6 kB
 aac.smali	2.7 kB
 aad\$if.smali	6.6 kB
 aad\$'.smali	505 B
 aad.smali	476 B
 aae\$1.smali	552 B

Solution - Java Obfuscation



network	4.1 kB
NiaNet.smali	24.2 kB
NianticTrustManager.smali	5.4 kB

network	4.1 kB
NiaNet.smali	23.9 kB
NianticTrustManager.smali	

Old

VS

New

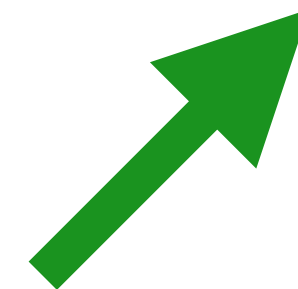
anm\$1.smali	31.9 kB
anm.smali	48.2 kB
ano\$d.smali	
ano\$>.smali	514.1 kB
ao.smali	32.0 kB
aod.smali	20.9 kB
aos\$1.smali	6.4 kB
aou\$J.smali	
aou\$Γ.smali	108.9 kB
aow\$J.smali	

anm\$1.smali	31.9 kB
anm.smali	48.2 kB
ano\$d.smali	510.9 kB
ano\$>.smali	
ao.smali	32.0 kB
aod.smali	20.9 kB
aos\$1.smali	6.4 kB
aou\$J.smali	111.3 kB
aou\$Γ.smali	
aow\$J.smali	120.7 kB

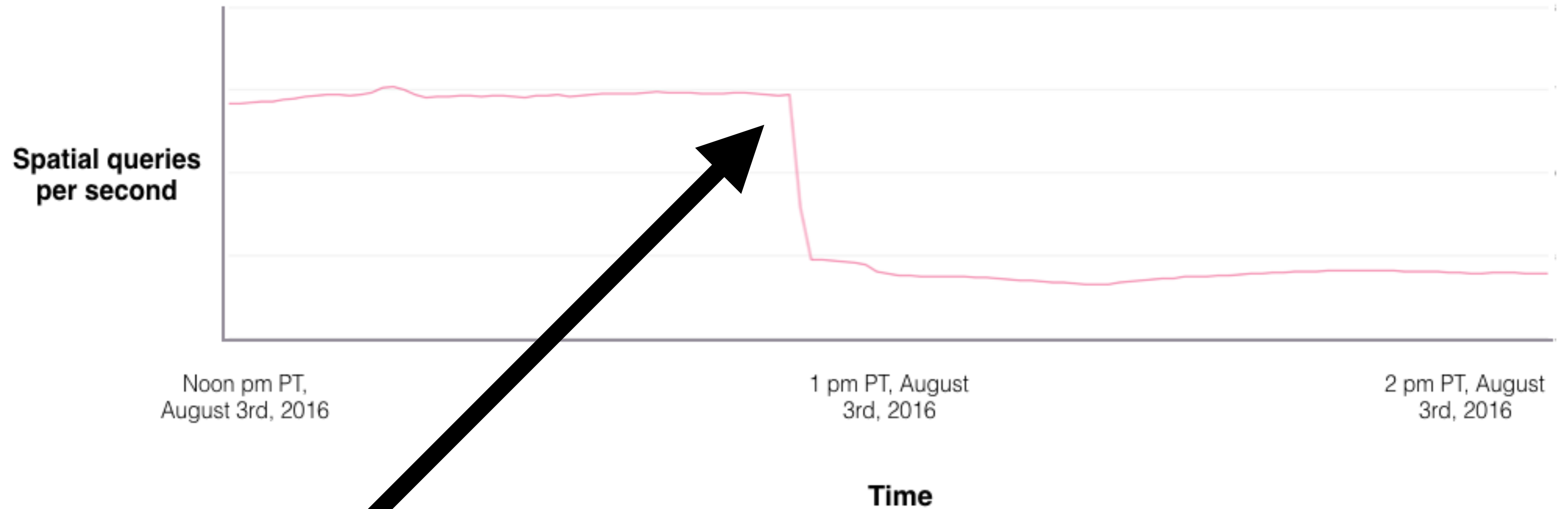
Solution - "Unknown6"



```
8  message RequestEnvelope {
9      int32 status_code = 1;
10
11     uint64 request_id = 3;
12     repeated .POGOProtos.Networking.Requests.Request requests = 4;
13
14     .POGOProtos.Networking.Envelopes.Unknown6 unknown6 = 6;
```



Unofficial API Blackout



Unknown6 Enforced

ClientBlob - "Unknown6"



- GPS
- Sensor
- Device
- Activity

```
"device.manufacturer": "LGE",  
"bundle.schema_hash": "97d170e1550eee4afc0af065b78cda302a97674c",  
"sdk.version": "4.0.6",  
"device.jailbroken": false,  
"device.hardware": "Nexus 5",  
"screen.scale": 1.0,  
"device.connection": "WIFI",  
"screen.dpi": 480,  
"screen.width": 1080,  
"screen.height": 1776,  
"sdk.build": "+release.677f23a",  
"device.os": "android",  
"sdk.plugin": "4.0.7",  
"ids.android_id": "4bd2288959e3a5b6",  
"app.bundleid": "com.nianticlabs.pokemongo",
```

“Unknown6” broken



```
uint64 timestamp_since_start = 2; // in ms
repeated LocationFix location_fix = 4;
AndroidGpsInfo gps_info = 5;
SensorInfo sensor_info = 7;
DeviceInfo device_info = 8;
ActivityStatus activity_status = 9;
uint32 location_hash1 = 10; // Location1 hashed signed based on the auth_token or auth_info - xxHash32
uint32 location_hash2 = 20; // Location2 hashed (unsigned) - xxHash32
bytes session_hash = 22; // 16 bytes, unique per session
uint64 timestamp = 23; // epoch timestamp in ms
repeated uint64 request_hash = 24; // hashes of each request message in a hashArray signed based on the
int64 unknown25 = 25; // for 0.33 its static -8537042734809897855 or 0x898654dd2753a481, generated via :
```

Solution - Native Obfuscation



- Obfuscation
- Anti-Debugger
- Integrity Validation
- Complexity



Hello SafetyNet

Solution - SafetyNet



- SafetyNet enforces the CTS
 - Compatibility Test Suite
- Blocks rooted devices
- Integrity Checks

This device, OS, or software is not compatible with Pokémon GO.

[Learn more](#)



Solution - SafetyNet evolves

- suhide / magisk
 - bypasses SafetyNet
- frequent updates

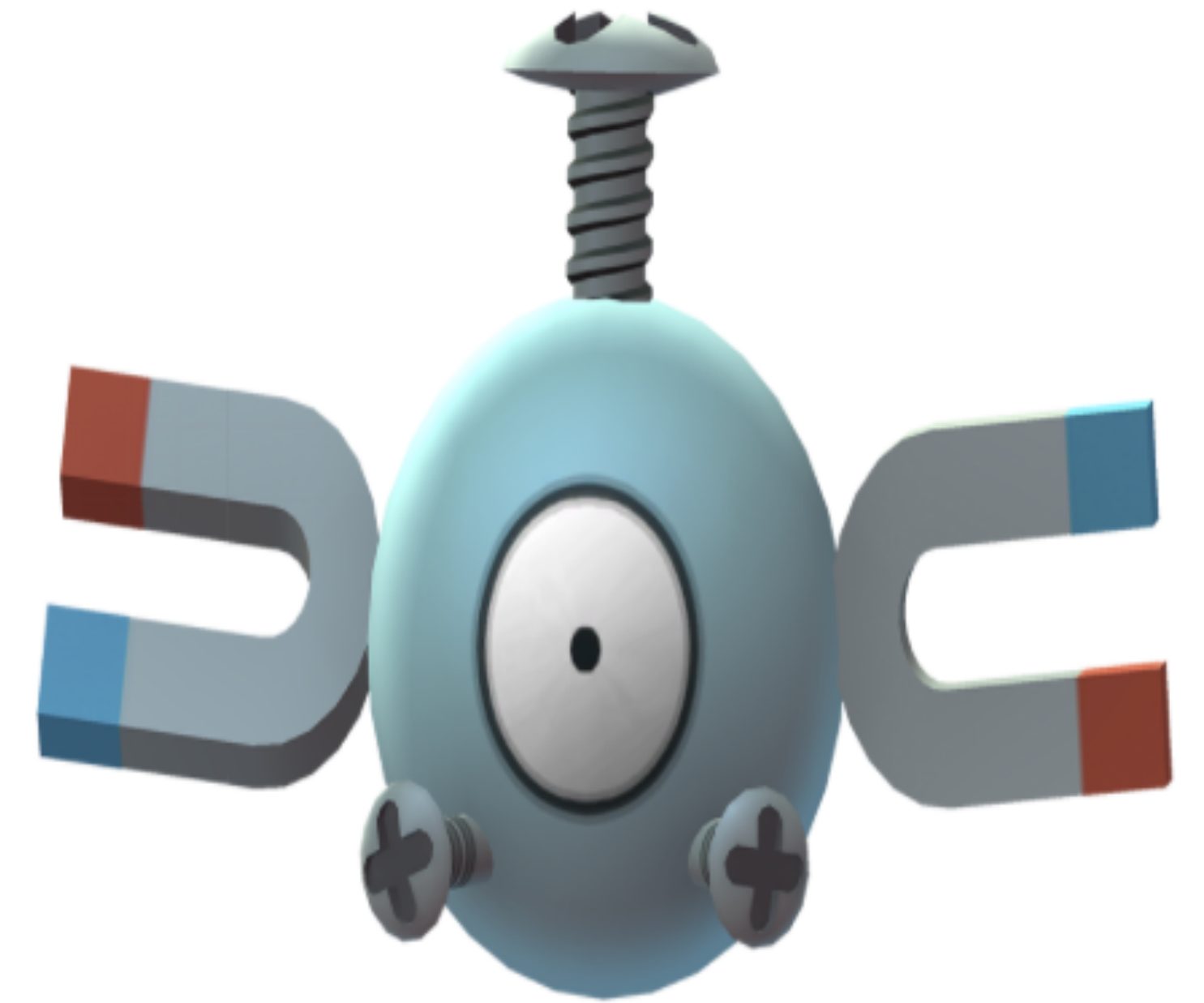


Magisk Manager

Solution - Captcha



- Not all users are equal
- Catch the outliers
- Google's reCAPTCHA

 I'm not a robot
 reCAPTCHA
[Privacy - Terms](#)

Solution - Legal :/



Re: *Mila432/Pokemon_Go_API - Unauthorized Hack of Pokémon GO*

We write on behalf of The Pokémon Company International, Inc. (“**Pokémon**”). Pokémon and its licensees and partners recently learned that you have developed and/or are distributing or offering for download and cloning a script (“**Mila 432/Pokemon_Go_API**”) that appears to be used to hack the Pokémon GO app by interrupting a user’s API calls and substituting other data in place of what would ordinarily be sent to Pokémon GO servers. The script is currently available to clone or download on GitHub at https://github.com/Mila432/Pokemon_Go_API.

Solution - Production is not Development



- Debug code can be abused
- Application contains clues
- Explain features



Solutions - Recap



- Runtime Assets
- Obfuscation
- API Security
- Captcha, SafetyNet, Legal

Q / A



source**toad**

DEVELOPMENT STUDIO



@iBotPeaches



connortumbleson.com

Story Time

Upsight Analytics