



Security in knowledge

iOS App Analysis

Michael Price

Appthority

RSACONFERENCE
EUROPE 2013

Session ID: MBS-R01

Session Classification: Intermediate

Background

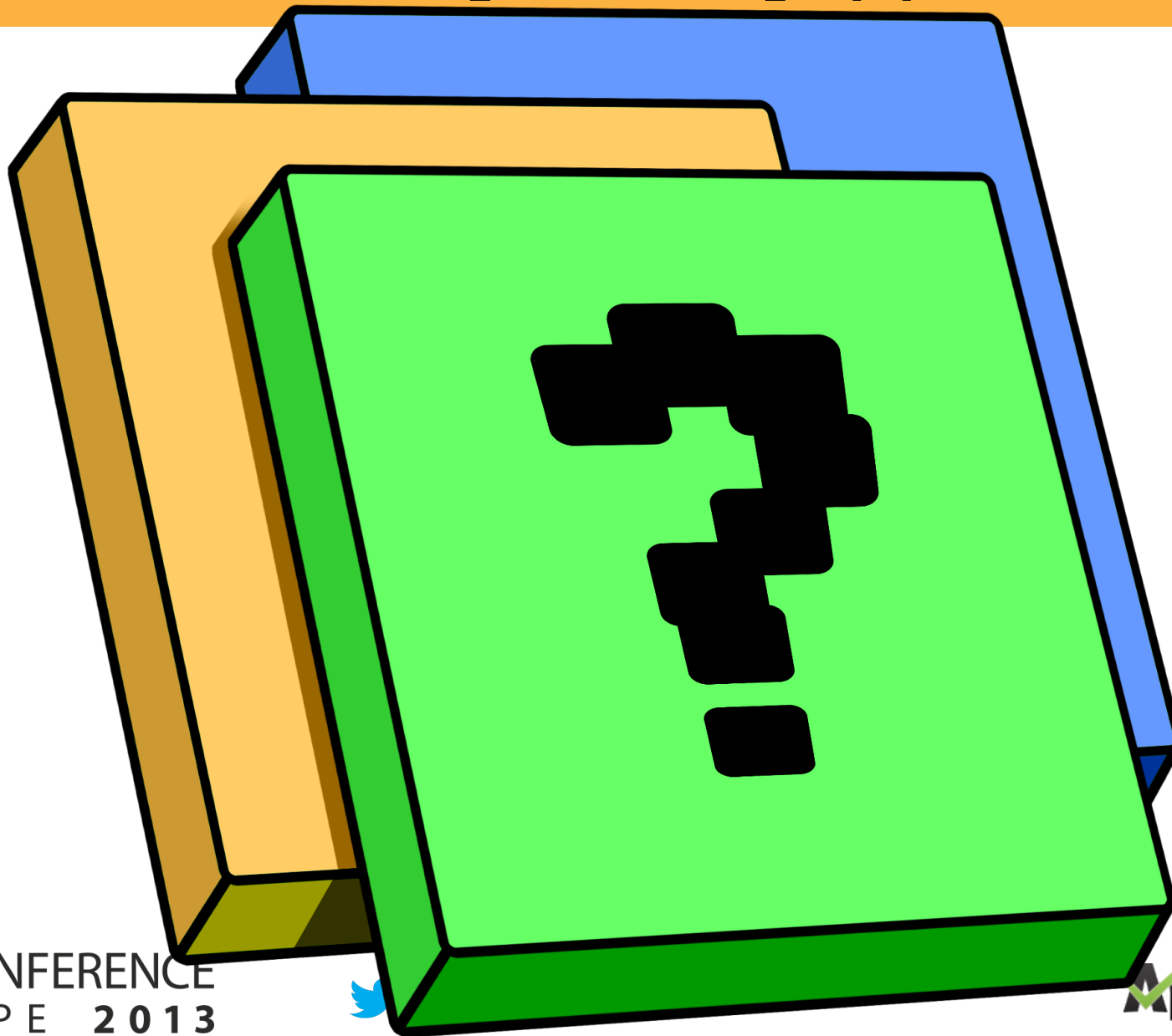


RSACON
EUROP

 #RSAC

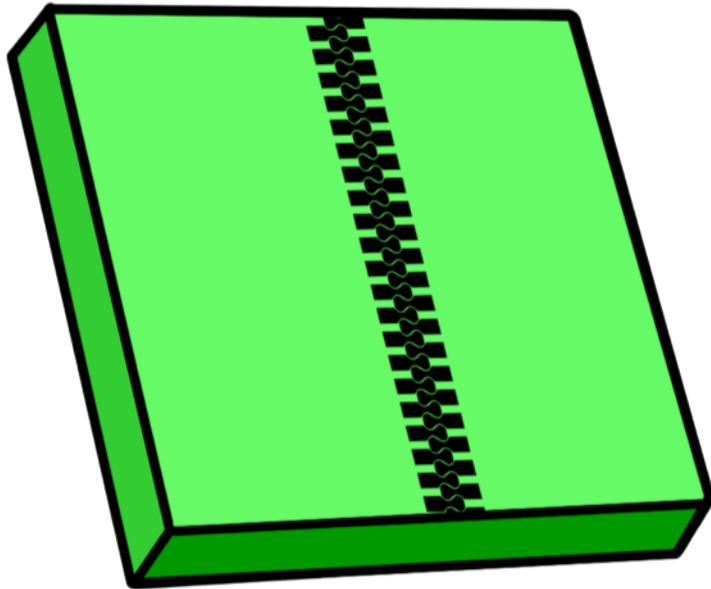
 Appthority®
Trust Your Apps

Whats[in that]App?

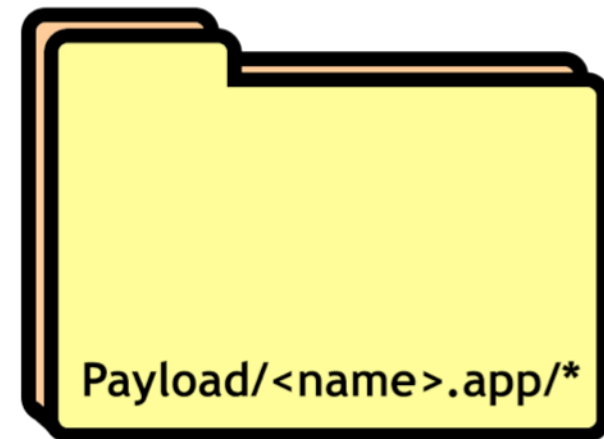


Whats[in that]App?

IPA = ZIP



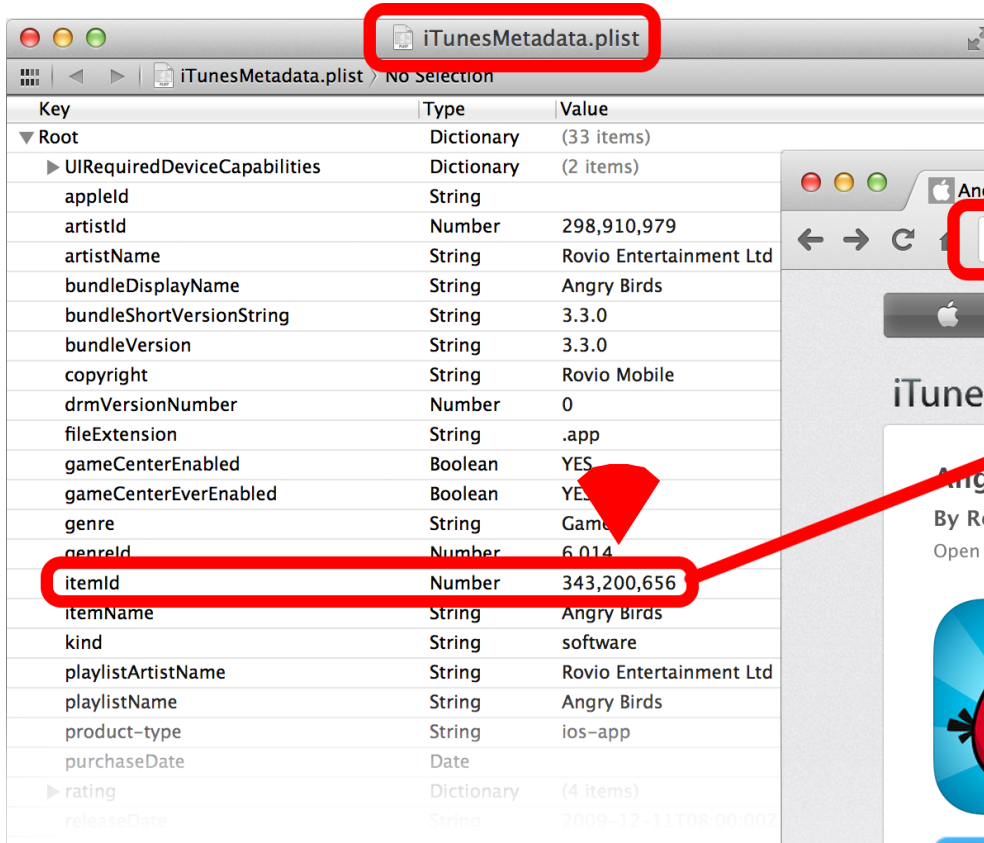
512 x 512



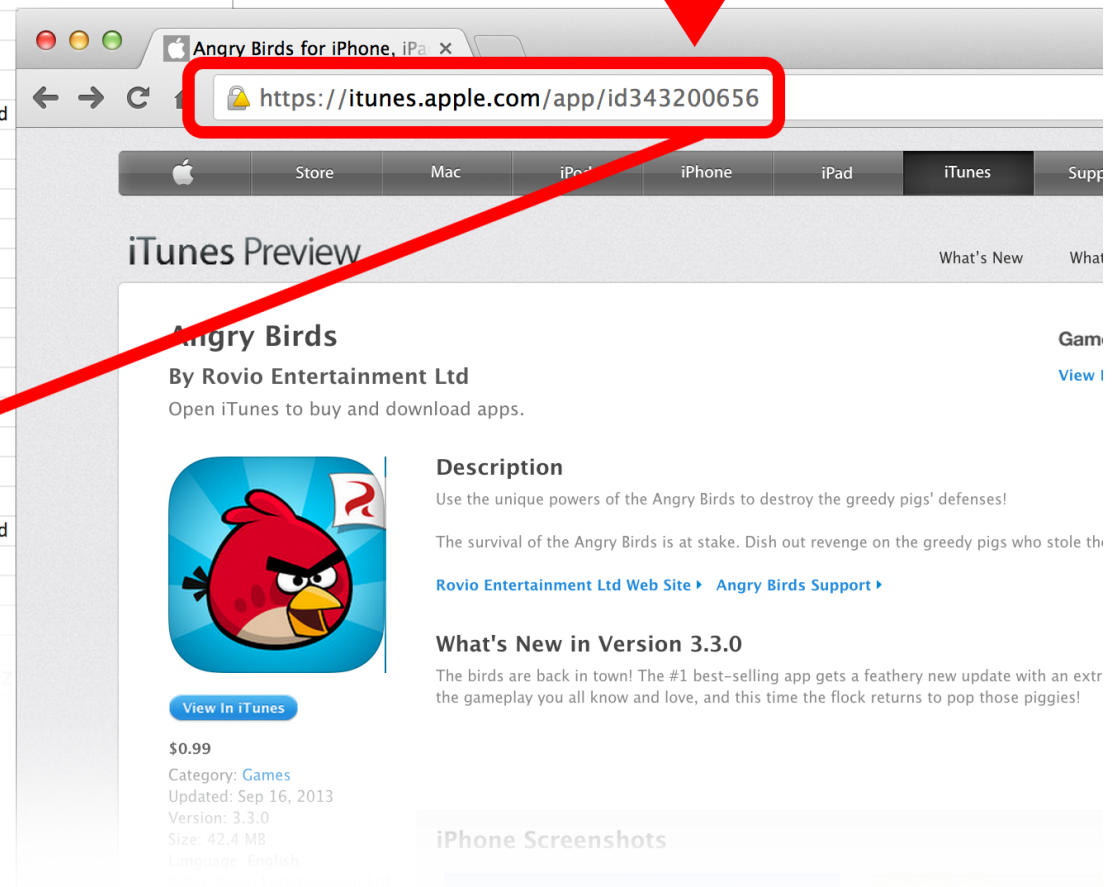
iTunesMetadata.plist

iTunesMetadata

PLIST



Key	Type	Value
Root	Dictionary	(33 items)
UIRequiredDeviceCapabilities	Dictionary	(2 items)
appleId	String	
artistId	Number	298,910,979
artistName	String	Rovio Entertainment Ltd
bundleDisplayName	String	Angry Birds
bundleShortVersionString	String	3.3.0
bundleVersion	String	3.3.0
copyright	String	Rovio Mobile
drmVersionNumber	Number	0
fileExtension	String	.app
gameCenterEnabled	Boolean	YES
gameCenterEverEnabled	Boolean	YES
genre	String	Games
genreId	Number	6.014
itemId	Number	343,200,656
itemName	String	Angry Birds
kind	String	software
playlistArtistName	String	Rovio Entertainment Ltd
playlistName	String	Angry Birds
product-type	String	ios-app
purchaseDate	Date	
rating	Dictionary	(4 items)
releaseDate	String	2009-12-11T08:00:00Z



Angry Birds for iPhone, iPad

<https://itunes.apple.com/app/id343200656>

iTunes Preview

Angry Birds

By Rovio Entertainment Ltd

Open iTunes to buy and download apps.



[View In iTunes](#)

Description

Use the unique powers of the Angry Birds to destroy the greedy pigs' defenses!

The survival of the Angry Birds is at stake. Dish out revenge on the greedy pigs who stole the

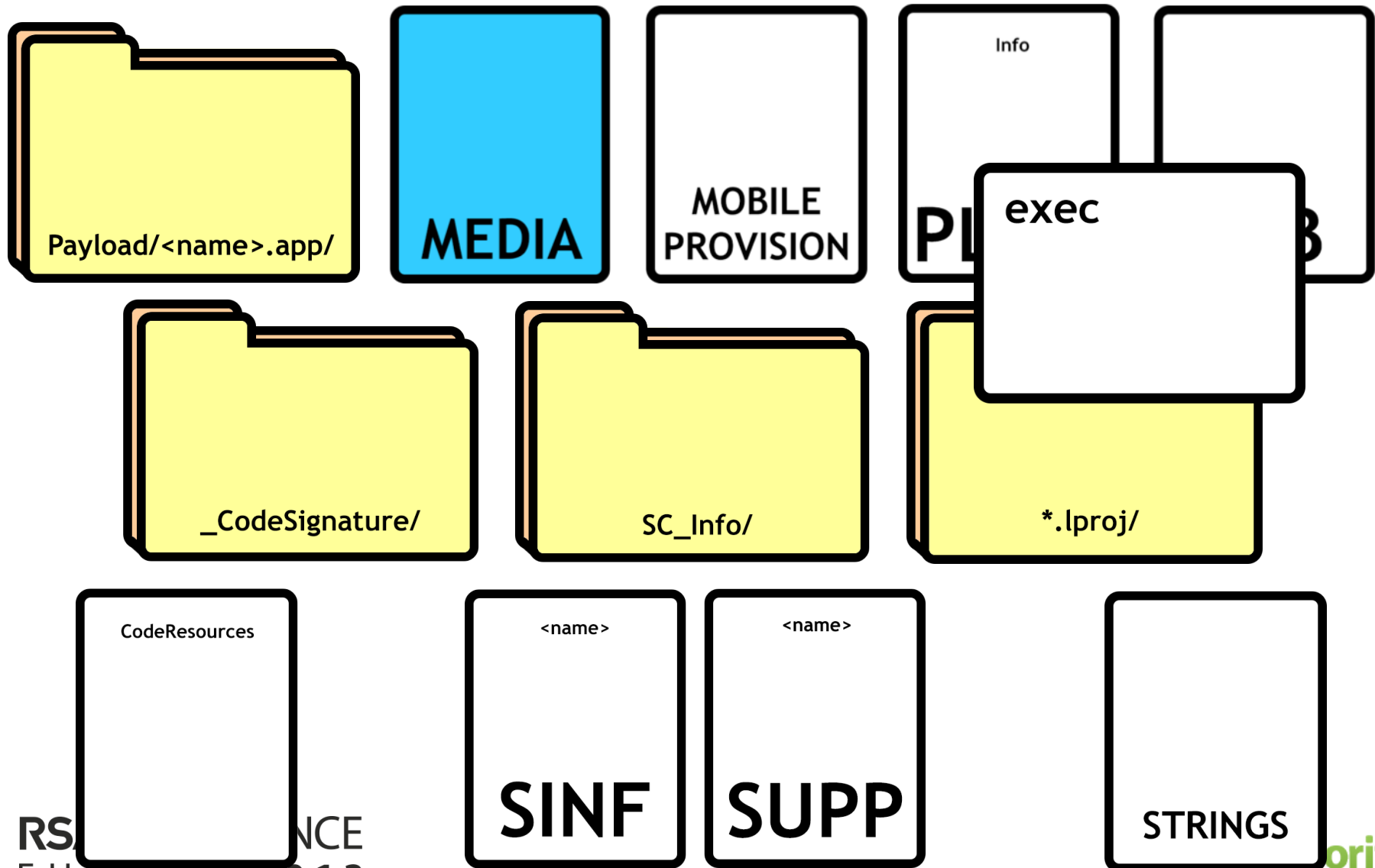
[Rovio Entertainment Ltd Web Site](#) [Angry Birds Support](#)

What's New in Version 3.3.0

The birds are back in town! The #1 best-selling app gets a feathery new update with an extra the gameplay you all know and love, and this time the flock returns to pop those piggies!

iPhone Screenshots

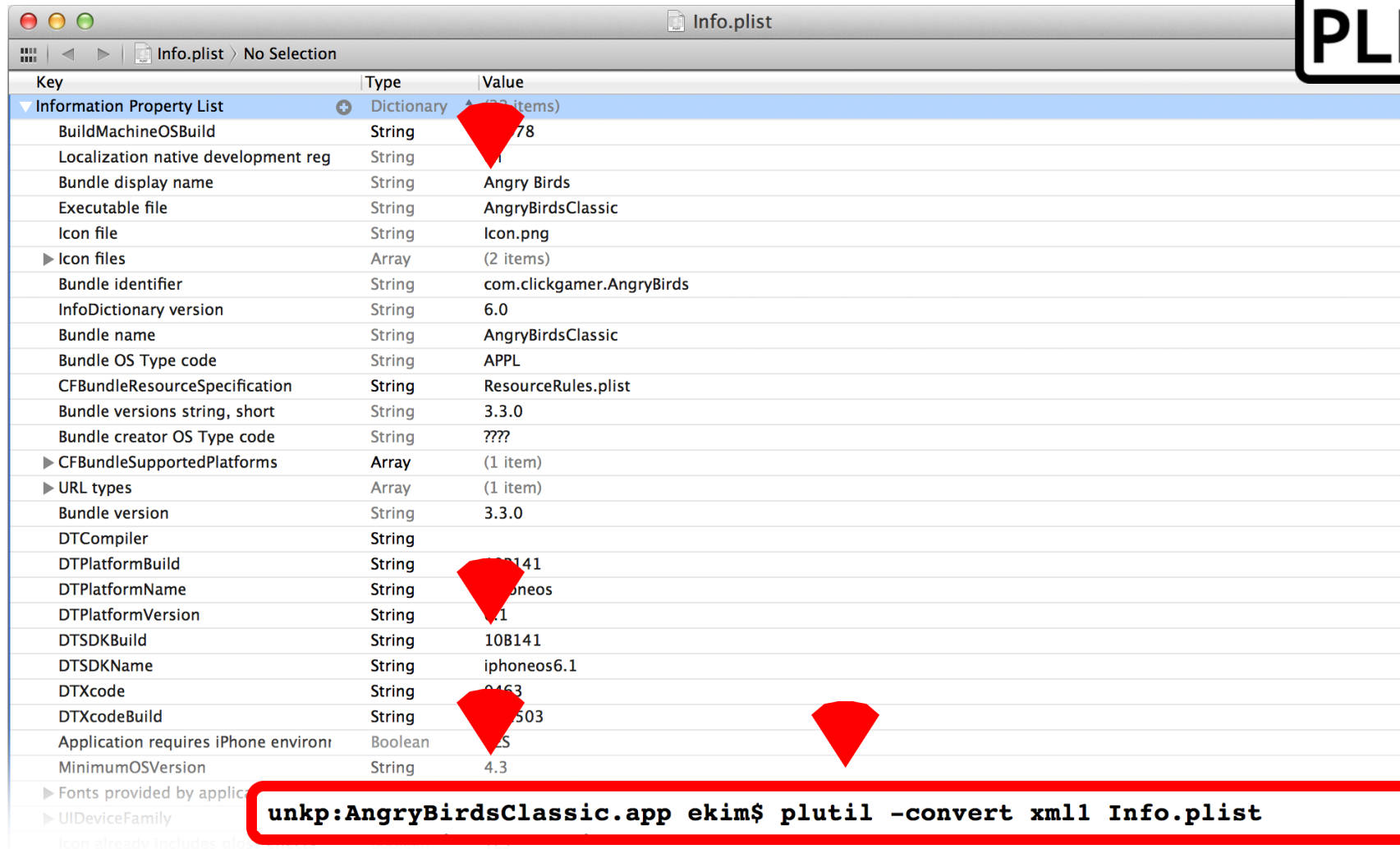
Whats[in that]App?



Info.plist

Info

PLIST



Key	Type	Value
Information Property List	Dictionary (2 items)	
BuildMachineOSBuild	String	78
Localization native development reg	String	1
Bundle display name	String	Angry Birds
Executable file	String	AngryBirdsClassic
Icon file	String	Icon.png
Icon files	Array	(2 items)
Bundle identifier	String	com.clickgamer.AngryBirds
InfoDictionary version	String	6.0
Bundle name	String	AngryBirdsClassic
Bundle OS Type code	String	APPL
CFBundleResourceSpecification	String	ResourceRules.plist
Bundle versions string, short	String	3.3.0
Bundle creator OS Type code	String	???
CFBundleSupportedPlatforms	Array	(1 item)
URL types	Array	(1 item)
Bundle version	String	3.3.0
DTCompiler	String	
DTPlatformBuild	String	10B141
DTPlatformName	String	iPhoneOS
DTPlatformVersion	String	1
DTSDKBuild	String	10B141
DTSDKName	String	iPhoneOS6.1
DTXcode	String	1
DTXcodeBuild	String	503
Application requires iPhone environ	Boolean	YES
MinimumOSVersion	String	4.3
Fonts provided by application	Array	(0 items)
UIDeviceFamily	String	iPhone

```
unpk:AngryBirdsClassic.app ekim$ plutil -convert xml1 Info.plist
```

NIB

~UNDOCUMENTED

NIB

000	4e 49 42 41 72 63 68 69	76 65 01 00 00 00 09 00	NIBArchive.....
0010	00 00 23 00 00 00 32 00	00 00 2e 00 00 00 9b 00	...#...2.....
00000020	00 00 72 00 00 00 77 03	00 00 0a 00 00 00 98 06	...r...w.....
00000030	00 00 89 80 85 80 85 81	84 86 84 80 8a 81 80 8b	
00000040	81 80 8c 81 84 8d 84 82	91 83 80 94 81 81 95 85	
00000050	86 9a 84 80 9e 81 80 9f	81 80 a0 81 80 a1 81 81	
00000060	a2 85 80 a7 81 83 a8 87	81 af 81 82 b0 83 81 b3	
00000070	85 85 b8 81 81 b9 83 82	bc 83 86 bf 84 86 c3 86	
00000080	87 c9 83 80 cc 81 80 cd	81 85 ce 81 80 cf 81 88	
00000090	d0 90 88 e0 90 86 f0 81	80 f1 81 8e 4e 53 49 6e	NSIn
000000a0	6c 69 6e 65 64 56 61 6c	75 65 88 55 49 53 6f 75	linedValue.UISou
000000b0	72 63 65 8f 55 49 4e 75	6d 62 65 72 4f 66 4c 69	rce.UINumberOfLi
000000c0	6e 65 73 a3 55 49 4e 69	62 41 63 63 65 73 73 69	nes.UINibAccessi

```
796      <key>CF$UID</key>
797      <integer>45</integer>
798    </dict>
799  </dict>
800  <string>infoButtonTouched</string>
801  <dict>
802    <key>$classes</key>
803    <array>
804      <string>UIRuntimeEventConnection</string>
805      <string>UIRuntimeConnection</string>
806      <string>NSObject</string>
807    </array>
808    <key>$classname</key>
```

PLIST

An app's executable

exec

ARM

32-bit -or- 64-bit

"OS X ABI Mach-O File Format"

/usr/include/mach-o/loader.h



Framework

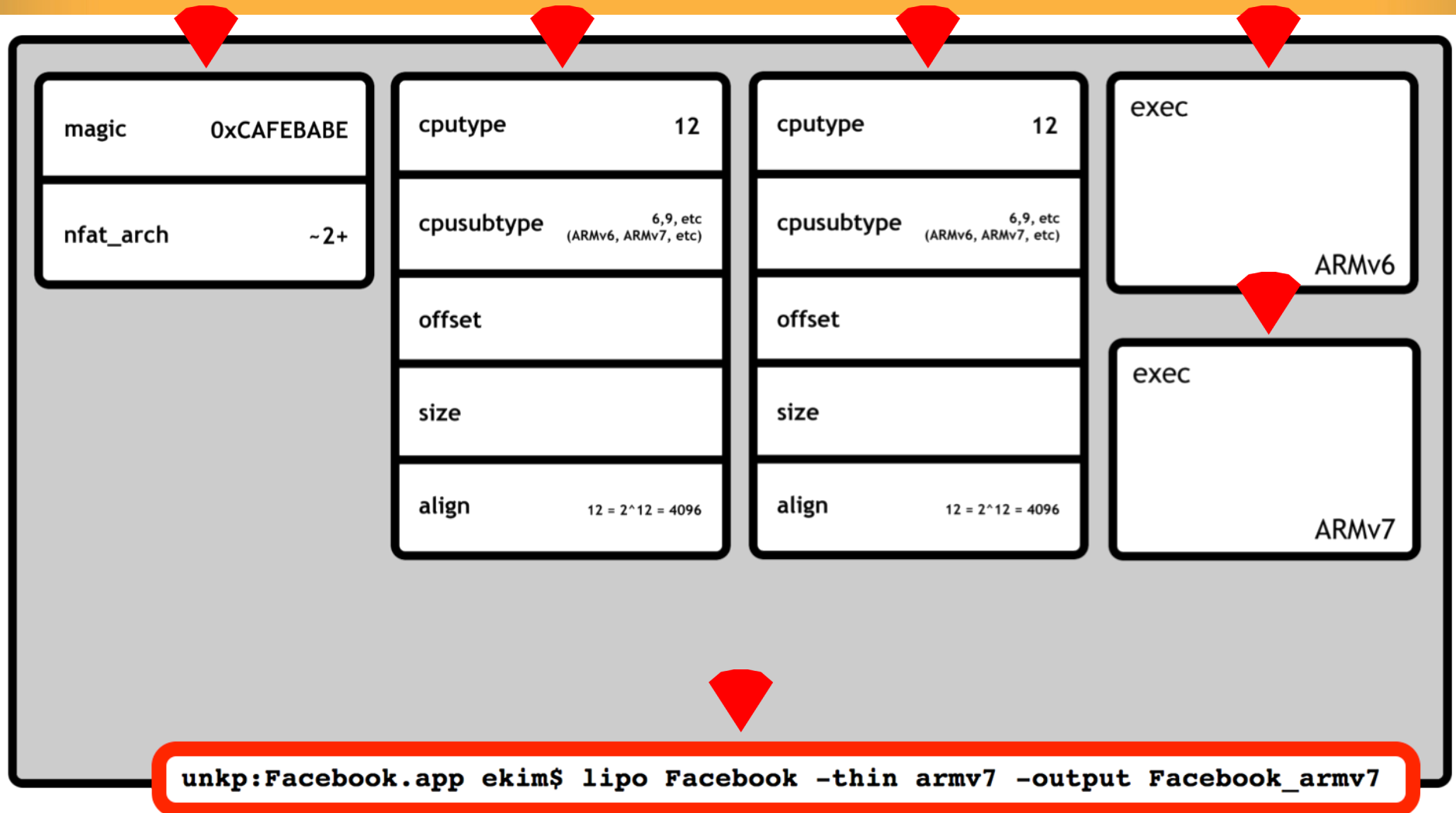


Dlib

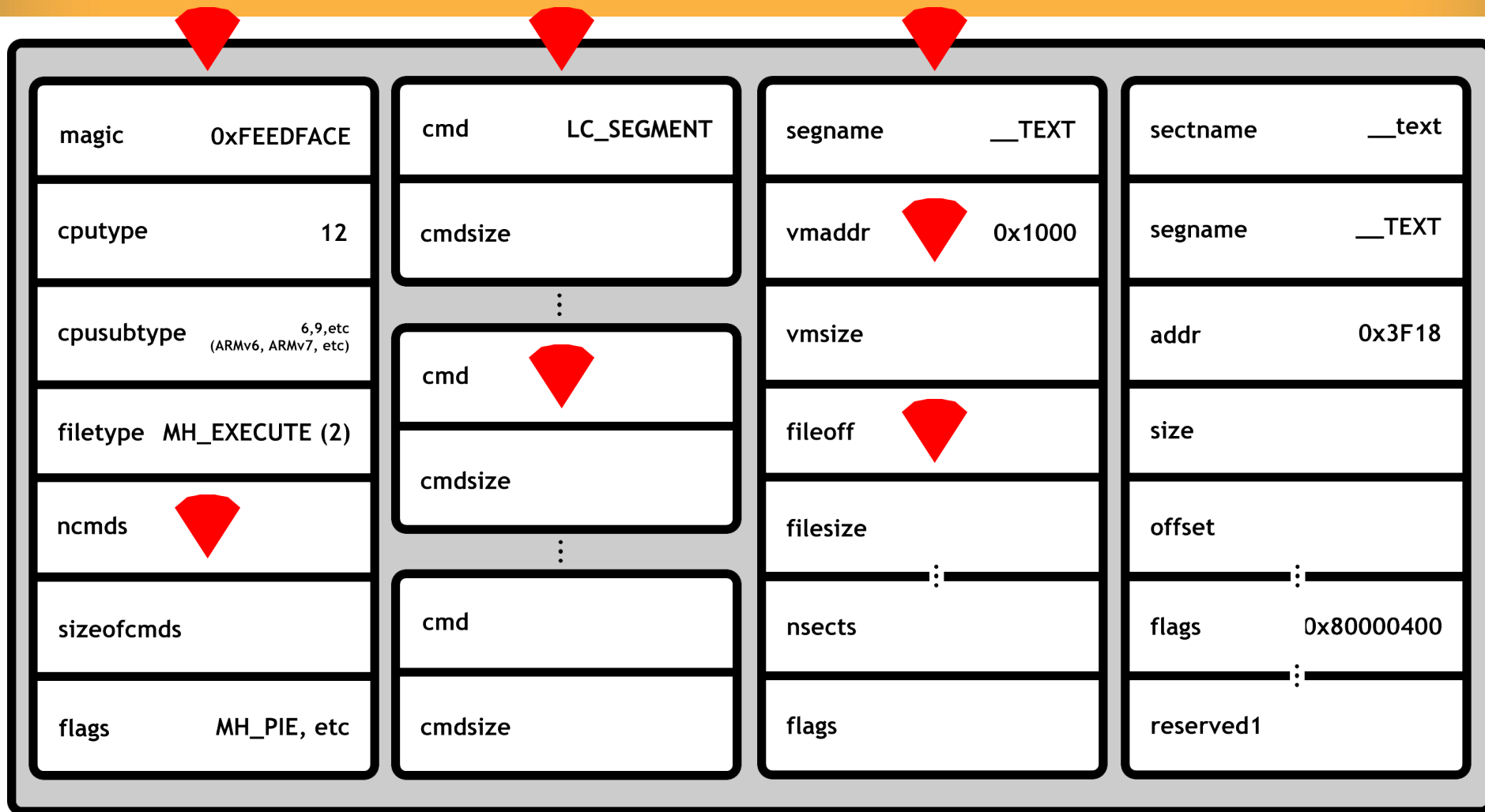


Static
library

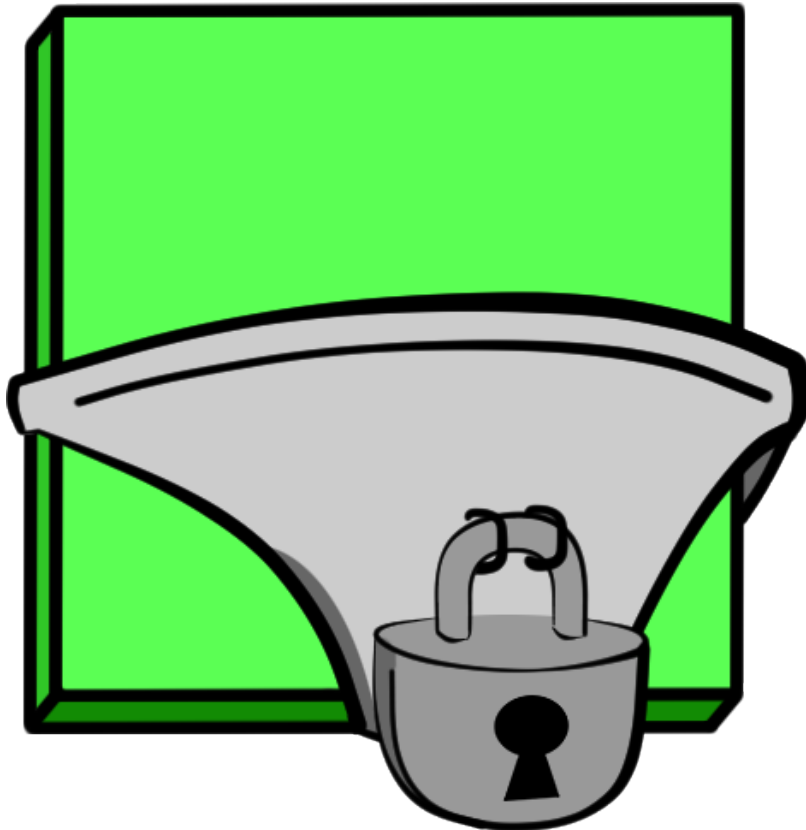
Fat vs. thin



Mach-O header



DRM



Load command 9

```
cmd LC_ENCRYPTION_INFO
cmdsize 20
cryptoff 8192
cryptsize 2482176
cryptid 0
```

ekims-iPhone:~ root# ./r30c5.sh

*** Rasticrac v3.0 c5 ***

Note: running iOS61 on '11' cpu

WARNING: iOS6 compatibility sucks !

Note: using dirty workaround now

Note: iPhone5 support is experimental

Note: please always check if IPA is

GDB: Apple version gdb-1821

List/Help: r30c5.sh

Menu: r30c5.sh [-v] -m [CN [CFN]
:

How to analyze

STATIC

strings

otool

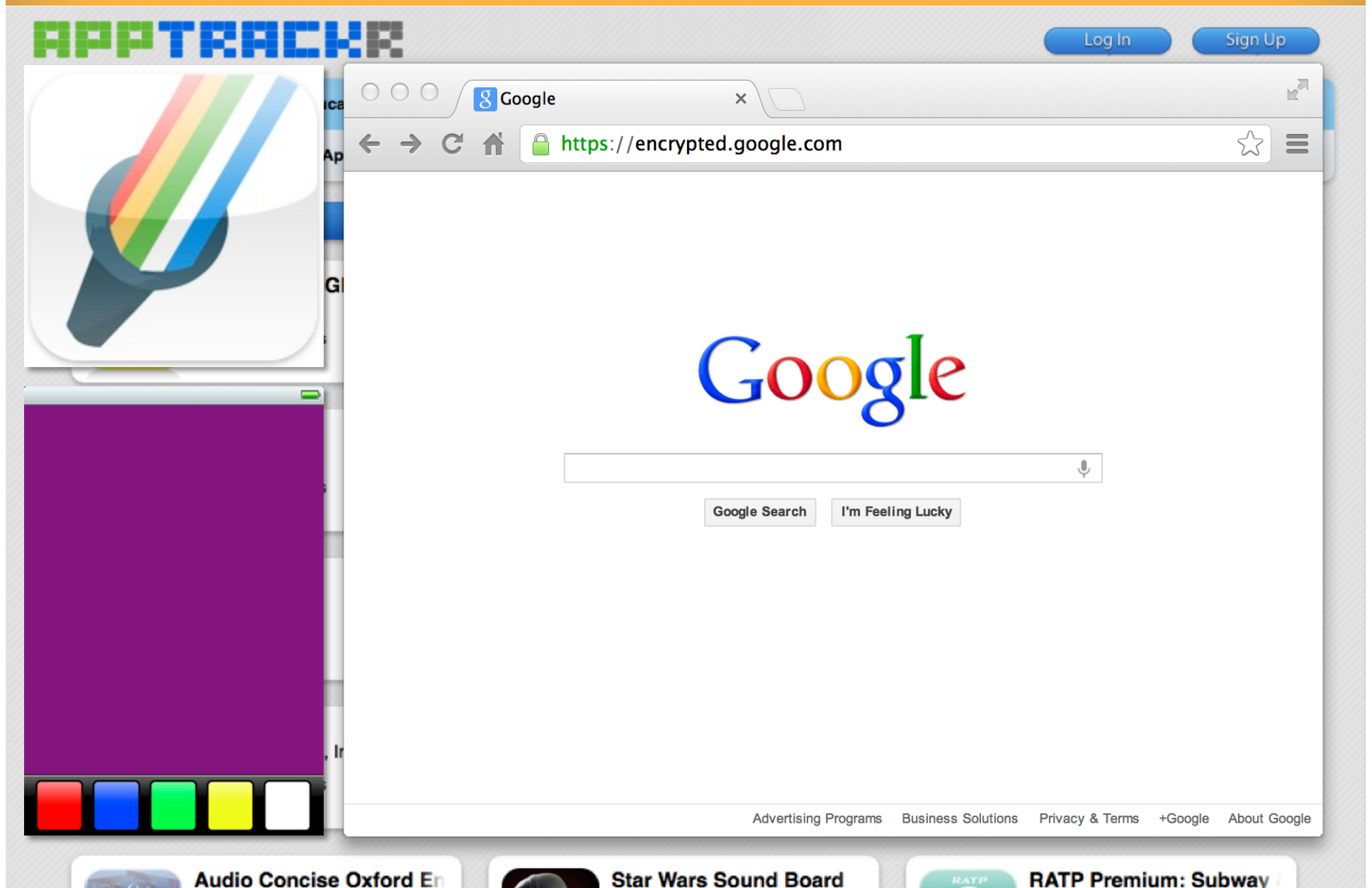
IDA Pro

DYNAMIC

GDB

MobileSubstrate

Example #1



Example #1

```
unkp:tmp ekim$ ls
HandyLight-1.0.1-Cusipzz.ipa
unkp:tmp ekim$ unzip HandyLight-1.0.1-Cusipzz.ipa
Archive:  HandyLight-1.0.1-Cusipzz.ipa
  creating: Payload/
  creating: Payload/HandyLight.app/
 inflating: Payload/HandyLight.app/HandyLight
 inflating: Payload/HandyLight.app/Info.plist
 inflating: iTunesArtwork
 inflating: iTunesMetadata.plist
 inflating: Payload/HandyLight.app/HandyLightView
Controller.nib
 inflating: Payload/HandyLight.app/MainWindow.nib
 extracting: Payload/HandyLight.app/PkgInfo
```

Example #1

```
unkp:tmp ekim$ file Payload/HandyLight.app/HandyLight
Payload/HandyLight.app/HandyLight: Mach-O executable arm
```

```
unkp:tmp ekim$ strings Payload/HandyLight.app/HandyLight | more
release
starting
%@:%d
local
window
@"UIWindow"
statusViewController
@"HandyLightViewController"
setWindow:
```

Example #1

```
%s: line %d: %s
parse port number.
parse_addr error.
parse mask length.
dest port missing or invalid, ignore this line.
dest port range is invalid.
proxy address parse error.
%s:%s-%s/%s-%s:%s %u(%u/%u) %u.%06u
write: %m
read: %m
select: %m
ioctl: %m
accept: %m
child: cur %d; exeedeing max(%d)
%s[%s] connected
```

Example #1



```
unkp:HandyLight.app ekim$ otool -tv -Q HandyLight |  
more  
HandyLight:  
(__TEXT,__text) section  
start:  
000028c8          e59d0000          ldr      r0, [sp]  
000028cc          e28d1004          add      r1, sp, #4  
                @ 0x4  
000028d0          e2804001          add      r4, r0, #1  
                @ 0x1  
000028d4          e0812104          add      r2, r1, r4  
, lsl #2  
000028d8          e3cdd007          bic      sp, sp, #7  
                @ 0x7  
000028dc          e1a03002          mov      r3, r2
```

Example #1

```
08      (adr r6, 0x3c9c)
00003bca      0000      lsls      r0, r0, #0
00003bcc      a630      add       r6, pc, #1
92      (adr r6, 0x3c90)
00003bce      0000      lsls      r0, r0, #0
00003bd0      a3d0      add       r3, pc, #8
32      (adr r3, 0x3f14)
00003bd2      0000      lsls      r0, r0, #0
-[HTTPServer start]:
00003bd4      b5f0      push      {r4, r5, r
6, r7, lr}
00003bd6      465e      mov       r6, fp
00003bd8      4655      mov       r5, sl
00003bda      4644      mov       r4, r8
```

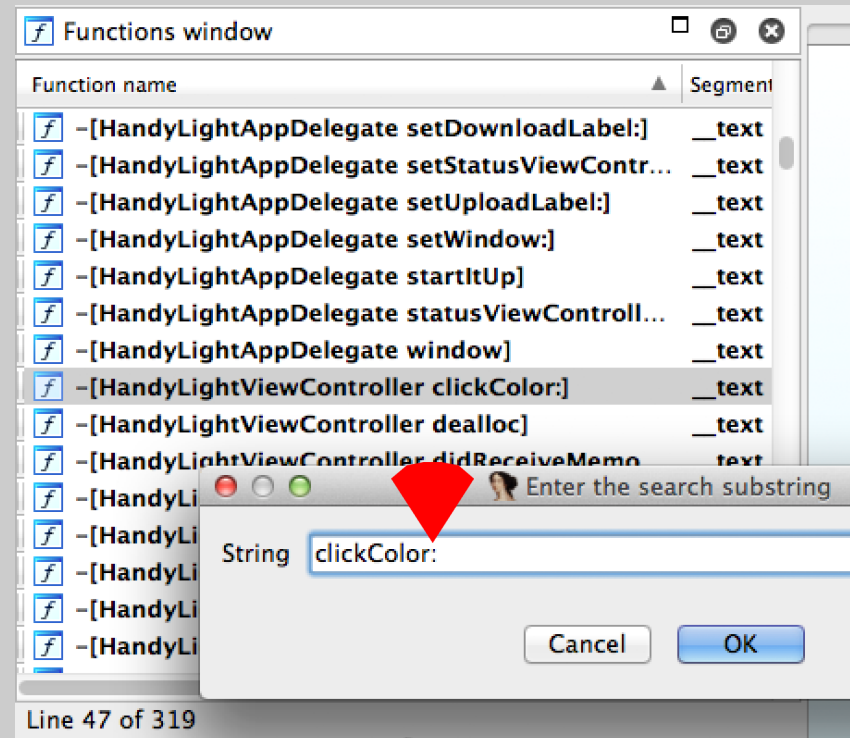
:

Example #1

```
unkp:HandyLight.app ekim$ ls  
HandyLight  
HandyLightViewController.nib  
Info.plist  
MainWindow.nib  
unkp:HandyLight.app ekim$
```

PkgInfo
colors.png
icon.png
icon@2x.png

```
unkp:HandyLight.app ekim$ strings - \\  
> HandyLightViewController.nib | grep \\  
> ":"  
clickColor:  
unkp:HandyLight.app ekim$
```



Example #1

```
if ( !v3->sequence )
{
    v3->sequence = (struct NSString *)CFSTR("");
    v3->sequence = (struct NSString *)objc_msgSend(v3->sequence, "stringByAppendingString:", CFSTR(""));
    objc_msgSend(v3->sequence, "retain");
    if ( (unsigned int)objc_msgSend(v3->sequence, "isEqualToString:", CFSTR("1")) )
    {
        v16 = objc_msgSend(v3, "view");
        v17 = objc_msgSend(&OBJC_CLASS__UIColor, "purpleColor", v17);
        objc_msgSend(v3->mydel, "startItUp");
    }
}
```

```
objc_msgSend(v7, "setText:", v4);
v8 = objc_msgSend(&OBJC_CLASS__NSString, "stringByAppendingString:", v8);
v9 = objc_msgSend(v2->statusViewController, "po", v8);
objc_msgSend(v9, "setText:", v8);
v10 = objc_msgSend(&OBJC_CLASS__NSString, "stringByAppendingString:", v10);
v12 = (int)local;
v13 = (int)-1;
v15 = (int)-1;
objc_msgSend(v10, "UTF8String");
local_main(4, &v12);
v11 = objc_msgSend(&OBJC_CLASS__HTTPServer, "sharedHTTPServer");
objc_msgSend(v11, "start");
*(DWORD*)(4 * ((unsigned int)v30 >> 5) + dword_B004) |= 1 << (v30 & 0x1F);
```



```
if ( !serv_sock_ind )
{
    v17 = serv_init(":");
    if ( v17 < 0 )
    {
        v18 = "cannot open server socket\n";
        LABEL_57:
        msg_out(2, v18);
        goto LABEL_44;
    }
}
if ( !*(DWORD*)dword_B03C && queue_init(v17) )
{
    v18 = "cannot init signal queue\n";
}
```

```
if ( bind(v30, *(const struct sockaddr **)(i + 24), *(DWORD*)(i + 16)) < 0 )
{
    goto LABEL_45;
}
if ( listen(v30, 64) < 0 )
{
    goto LABEL_45;
}
v23 = dword_B000;
v24 = dword_B014;
v25 = 4 * *(DWORD*)dword_B000 + *(DWORD*)dword_B014;
*(DWORD*)v25 = strdup(v31);
v26 = 4 * *(DWORD*)v23;
if ( !*(DWORD*)(v26 + *(DWORD*)v24) )
{
    goto LABEL_45;
}
*(DWORD*)(v26 + *(DWORD*)dword_B010) = v30;
*(DWORD*)(4 * ((unsigned int)v30 >> 5) + dword_B004) |= 1 << (v30 & 0x1F);
```

Example #2

[App Store](#) > [Lifestyle](#) > [Hatch Labs, Inc.](#)



Update

★★★★☆ (756)
Rated 12+

LINKS

[Privacy Policy](#)
[Developer Website](#)

Copyright © 2013 Tinder.

Tinder

Hatch Labs, Inc. >

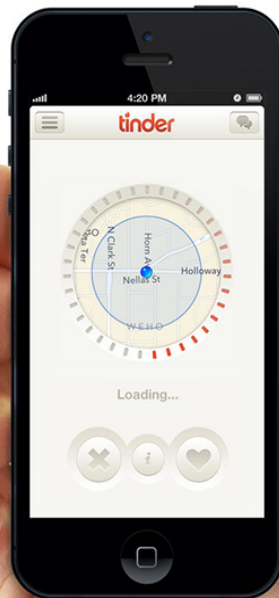
Details

Ratings and Reviews

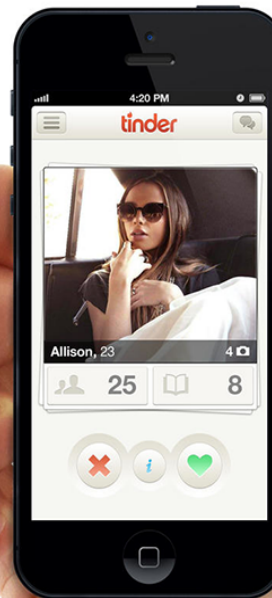
Related

iPhone Screenshots

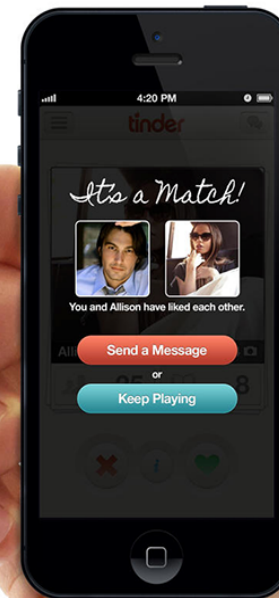
Tinder **finds interesting people** around you



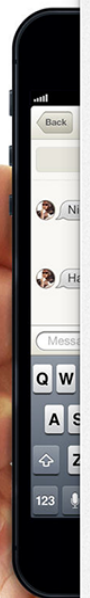
Anonymousl**y like or pass** on each suggestion



If two people happen to **like each other...**



Chat w
ins



Description

Tinder finds out who likes you nearby and connects you with them if you're also interested. It's the new way to meet people around you.

Example #2

```
0x3a112e30 in mach_msg_trap ()
(gdb) break SSLWrite
Breakpoint 1 at 0x33c65788
(gdb) c
Continuing.
[Switching to process 30222 thread 0x3c03]
Breakpoint 1, 0x33c65788 in SSLWrite ()
(gdb) x/s $r1
0x23b40050: "POST /updates HTTP/1.1\r\nHost:
api.gotinder.com\r\nAuthorization: Token token=\"
\r\nAccept: *
/*\r\nContent-Type: application/json; charset=utf-
8\r\nAccept-Language: en;q=1, "...
(gdb)
```

Example #2

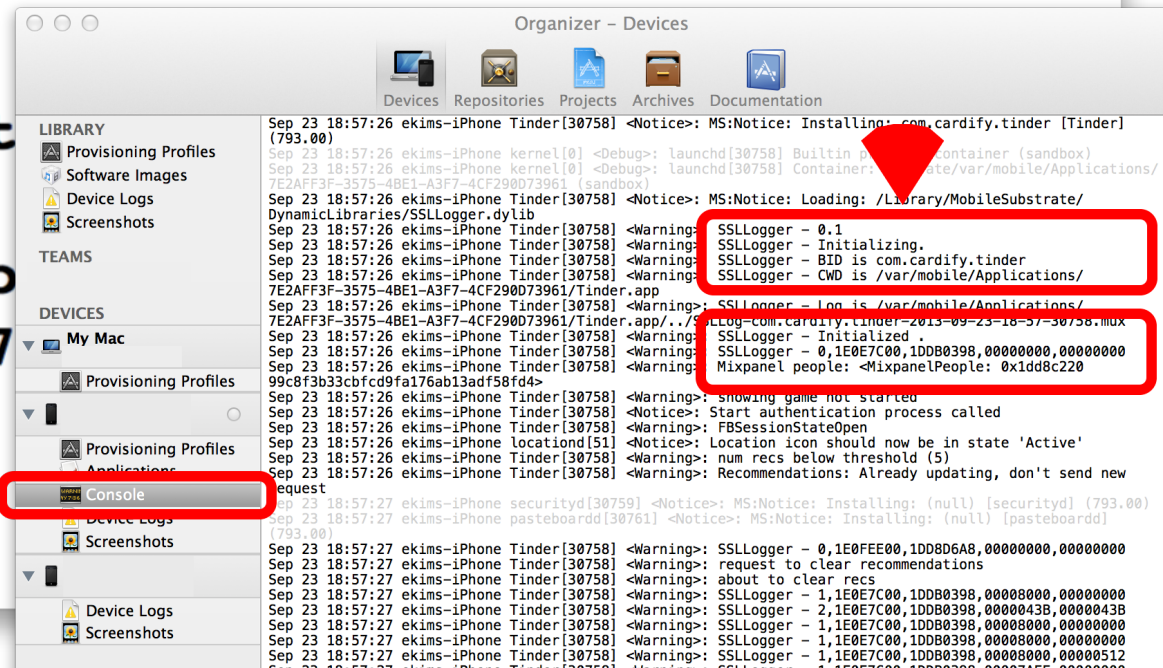


```
ekims-iPhone:~/code/SSLLogger root# ls -l
Makefile
SSLLogger.dylib*
SSLLogger.mm
SSLLogger.o
SSLLogger.plist
ekims-iPhone:~/code/SSLLogger root#
```

Example #2

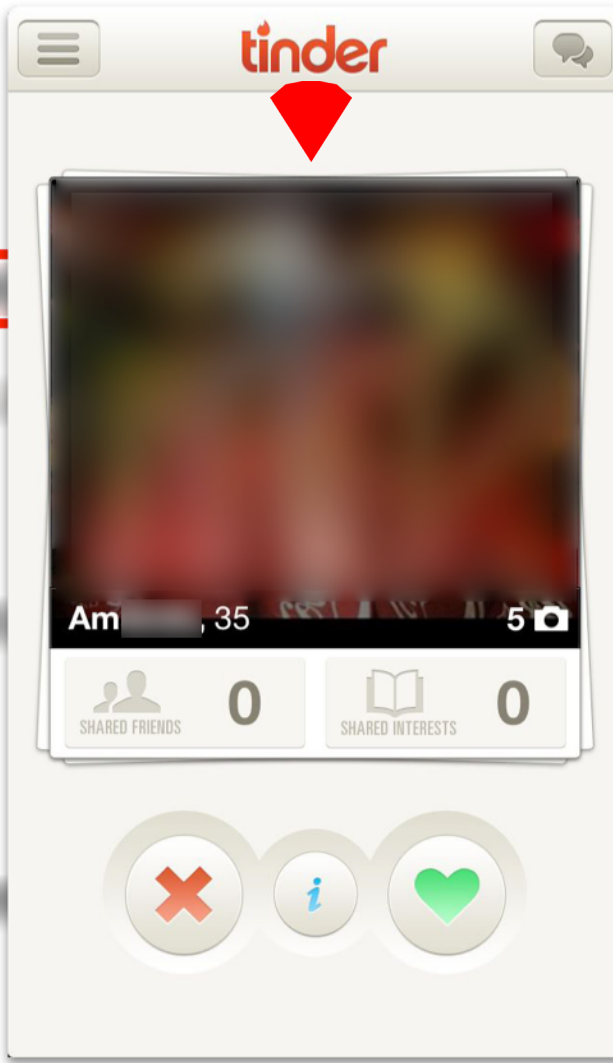
```
ekims-iPhone: /var/mobile/Applications/7E2AFF3F-357
5-4BE1-A3F7-4CF290D73961 root# ls
Documents/
Library/
SSLLog-com.cardify.tinder-2013-09-23-15-44-30222.m
ux
```

```
Tinder.app/
iTunesArtwork
iTunesMetadata.plist
tmp/
ekims-iPhone: /var/mo
5-4BE1-A3F7-4CF290D7
```

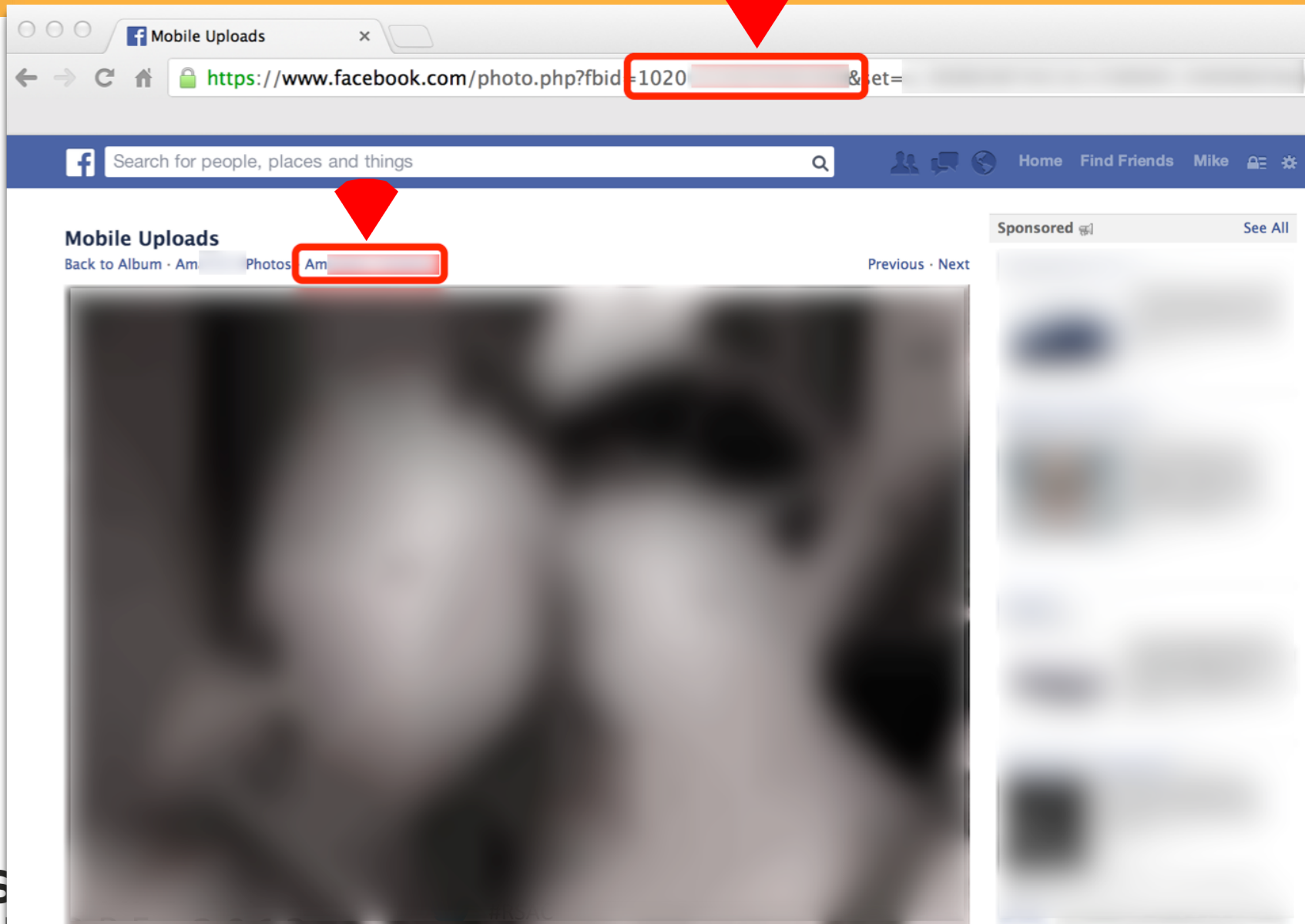


Example #2

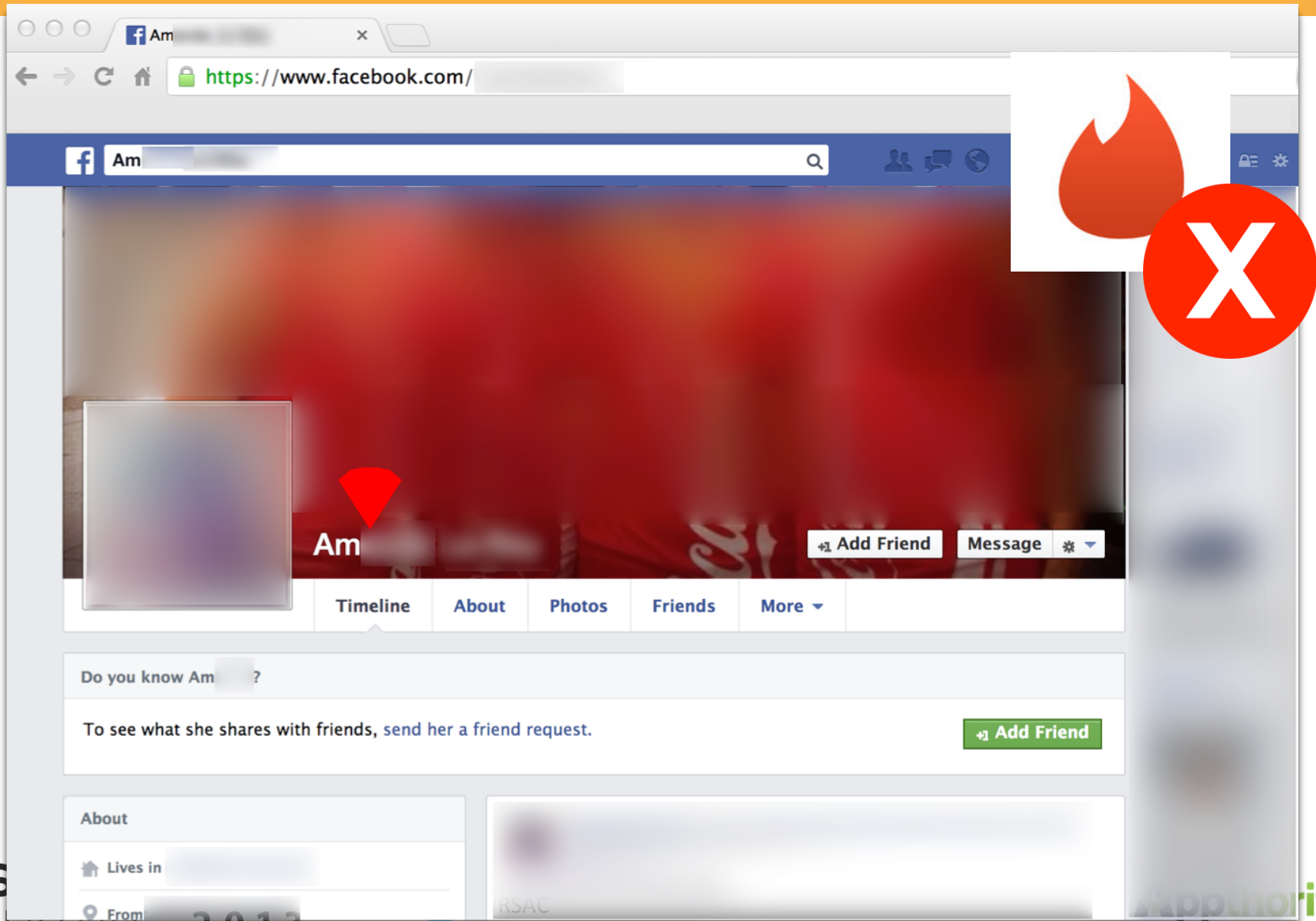
```
22 {
23   "status": 200,
24   "results": {
25     "bio": " ",
26     "name": "Am ",
27     "birth_date": "1978-",
28     "gender": 1,
29     "ping_time": " ",
30     "photos": [
31       {
32         "xdistance_percent": 1,
33         "id": " ",
34         "xoffset_percent": 0,
35         "yoffset_percent": 0.2188477,
36         "ydistance_percent": 0.5625,
37         "main": true,
38         "fileName": " ",
39         "fbId": "1020 ",
```



Example #2



Example #2



Example #2

Google Maps interface showing a map of a city area. A red box contains the following pseudocode:

```
while true
  # spoof our location
  ping(lat, lon)

  # get dist from user
  dist = dist(id)

  if dist < 0.25
    break # found
  end

  # update lat, lon
  lat, lon =
  update_loc(lon, lat, dist)
end
```

A red arrow points from the red box to a location marker on the map. The map shows streets, landmarks, and a search bar at the top with the coordinates -33.41166702432400,-70.55045447124121. The search bar also includes a microphone icon and a search button. The map interface includes a scale bar (500 ft, 200 m) and a copyright notice: Map data ©2013 Google, Mapcity.

Conclusion



Security in knowledge



RSACCONFERENCE
EUROPE 2013

Questions?

mprice@appthority.com



Security in knowledge



RSAC CONFERENCE
EUROPE 2013