Mobile Application Hacking

BSides Vancouver 2019

Wesley Wineberg

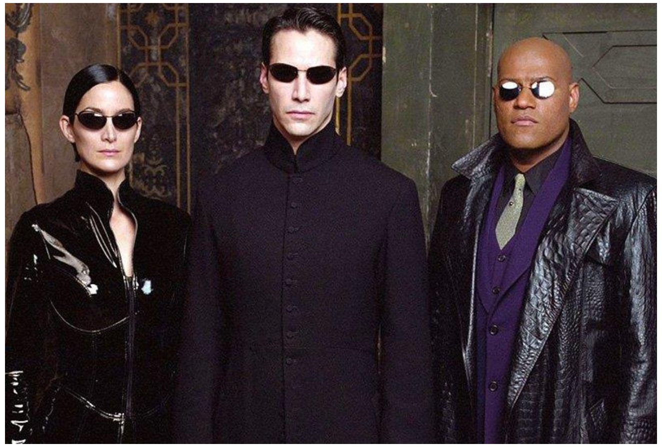
Hack like it's 1999

(The past is always better than it really was)

Refresher on the year 1999….

Hacking is mostly trying to do things as cool as it looks in the movies

This is 4 years old

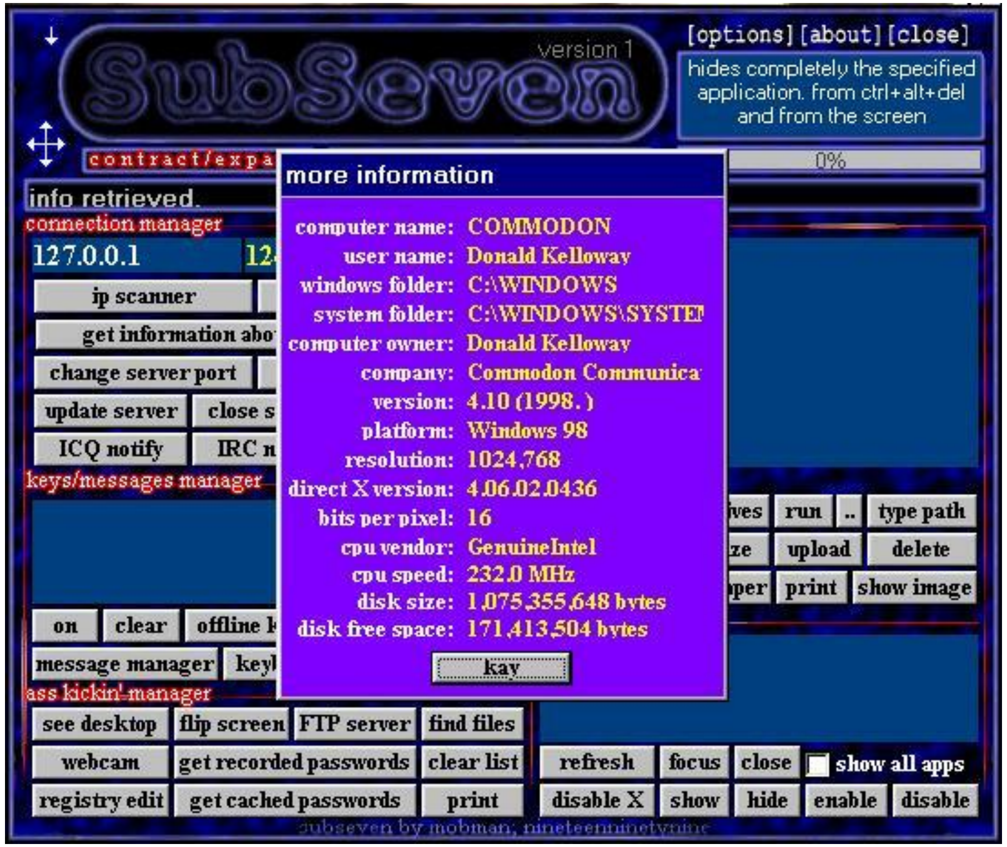


This is every hacker's dream

No explanation required

Hacking Tools From 1999

"Hacking"



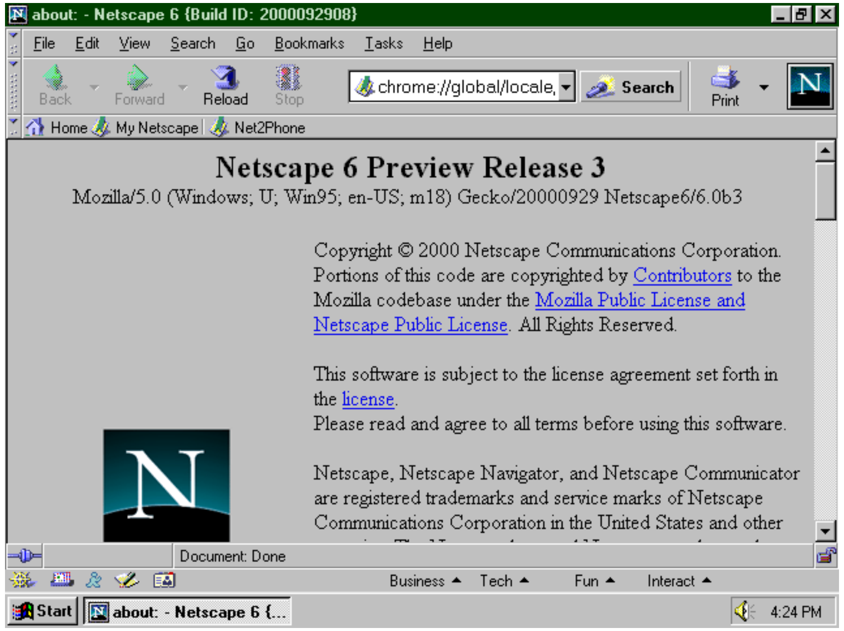
hides completely the specified application. from ctrl+alt+del and from the screen

info retrieved.

127.0.0.1 12

more information

computer name: COMMODON
user name: Donald Kelloway
windows folder: C:\WINDOWS
system folder: C:\WINDOWS\SYSTEI
computer owner: Donald Kelloway
company: Commodon Communica
version: 4.10 (1998.)
platform: Windows 98
resolution: 1024,768
direct X version: 4.06.02.0436
bits per pixel: 16
cpu vendor: GenuineIntel
cpu speed: 232.0 MHz
disk size: 1,075,355,648 bytes
disk free space: 171,413,504 bytes



Netscape 6 Preview Release 3

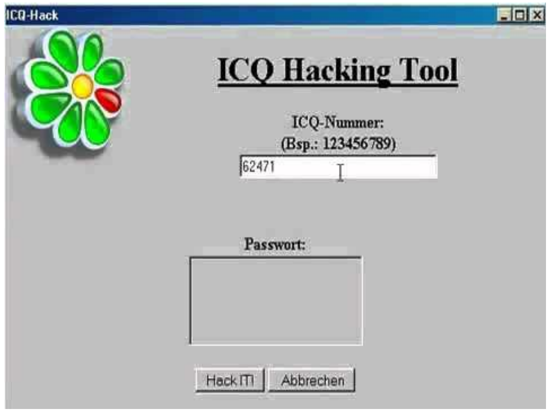
Mozilla/5.0 (Windows; U; Win95; en-US; m18) Gecko/20000929 Netscape6/6.0b3

Copyright © 2000 Netscape Communications Corporation. Portions of this code are copyrighted by Contributors to the Mozilla codebase under the Mozilla Public License and Netscape Public License. All Rights Reserved.

This software is subject to the license agreement set forth in the license.

Please read and agree to all terms before using this software.

Netscape, Netscape Navigator, and Netscape Communicator are registered trademarks and service marks of Netscape Communications Corporation in the United States and other



ICQ Hacking Tool

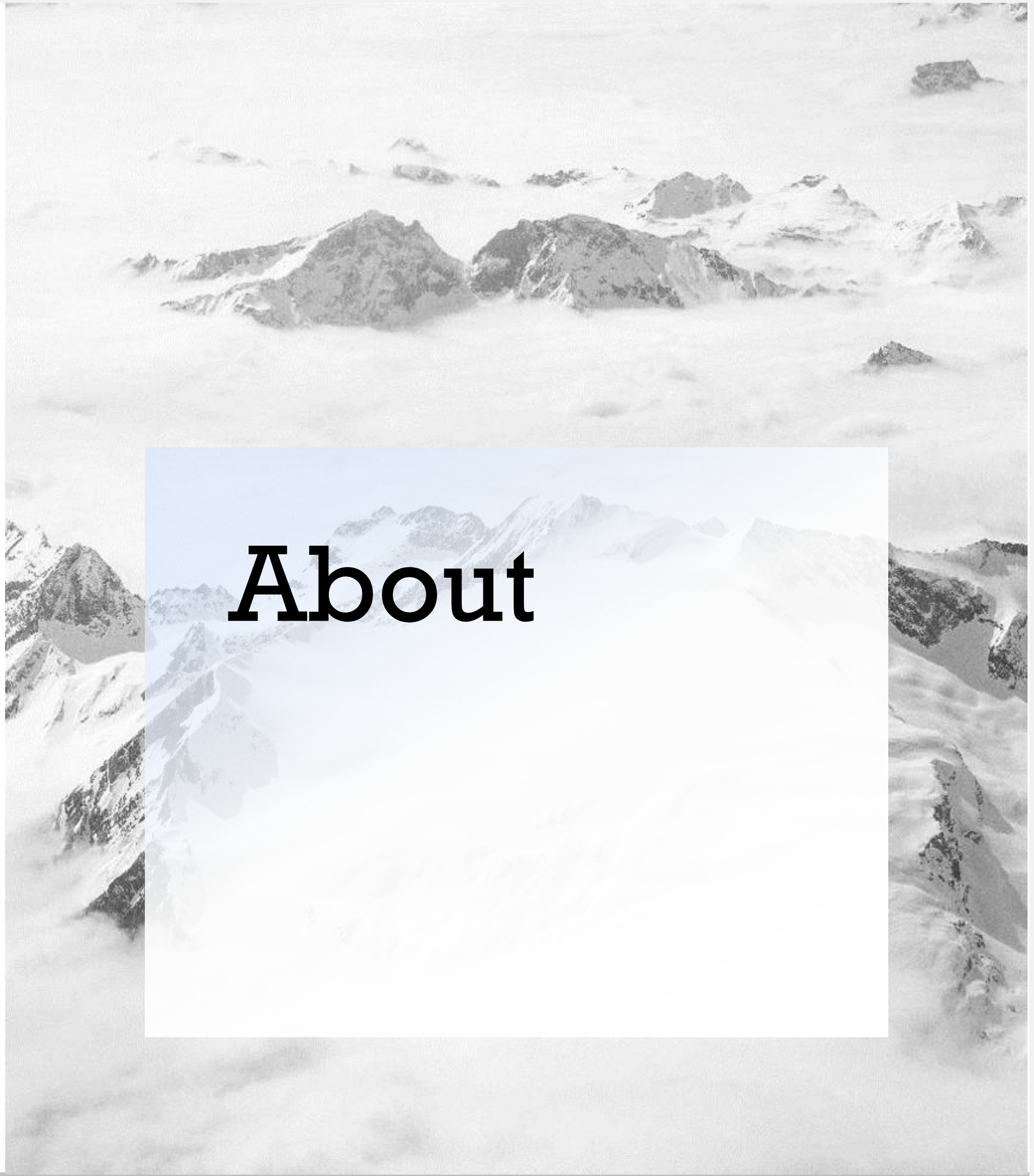
ICQ-Nummer:
(Bsp.: 123456789)
62471

Passwort:

Techniques / Vulnerabilities In 1999

- Client Side Validation
  - Full client applications
  - Web applications!
  - Your operating system
- Security By Obscurity
  - Binary file formats
  - XOR encryption
  - Hardcoded credentials, backdoors, etc
  - SSL? What SSL?
- "Trusting" Users
  - Email viruses
  - Instant message viruses
  - The invention of the euphemism "social engineering"

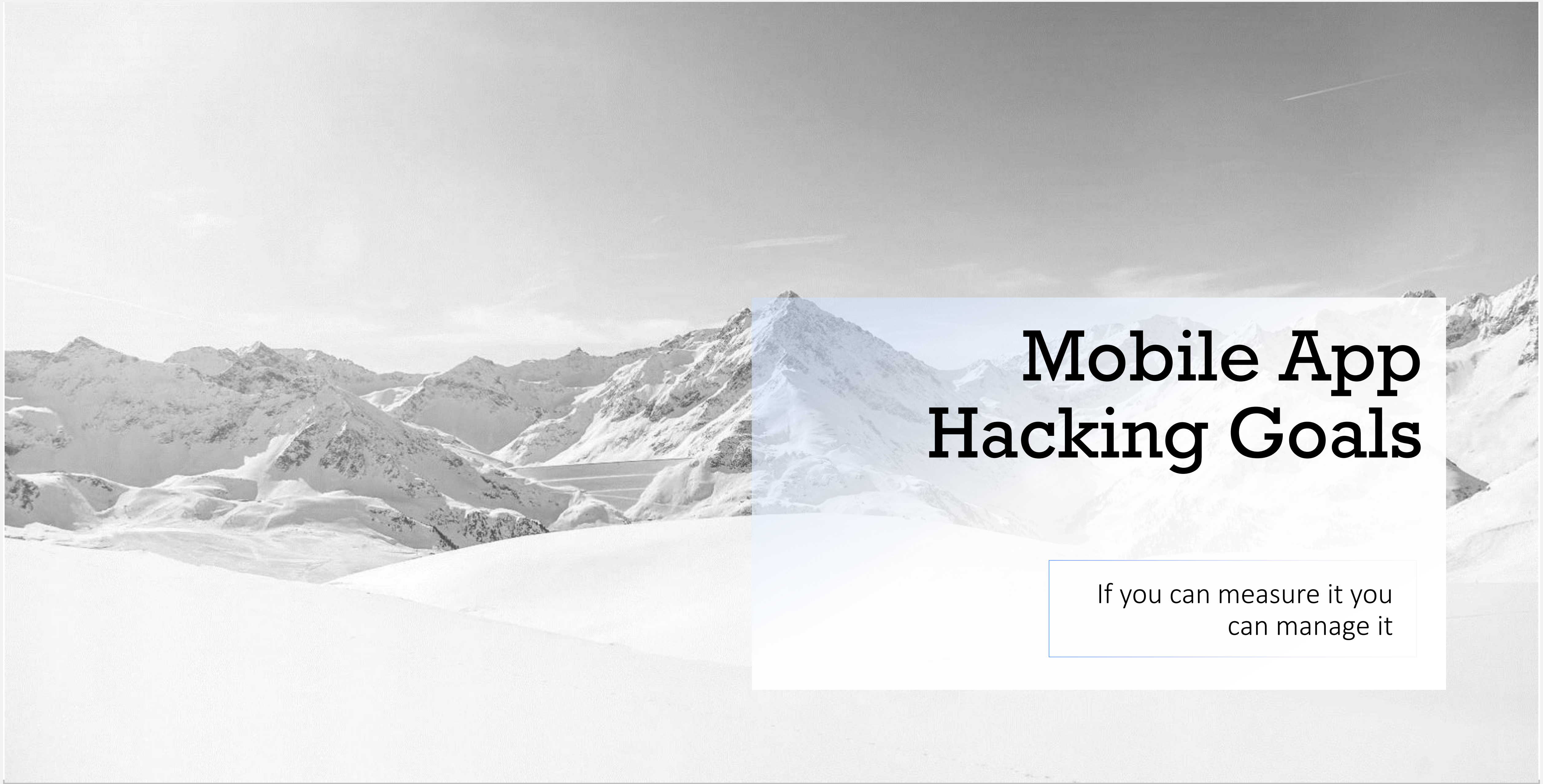
Just like mobile apps today!



About

Wesley Wineberg

- Back in Vancouver!
- Previously Red Team at Microsoft
- Infosec for more than a decade (almost as long as the iPhone is old)
- 4th time speaking at BSides Vancouver



Mobile App Hacking Goals

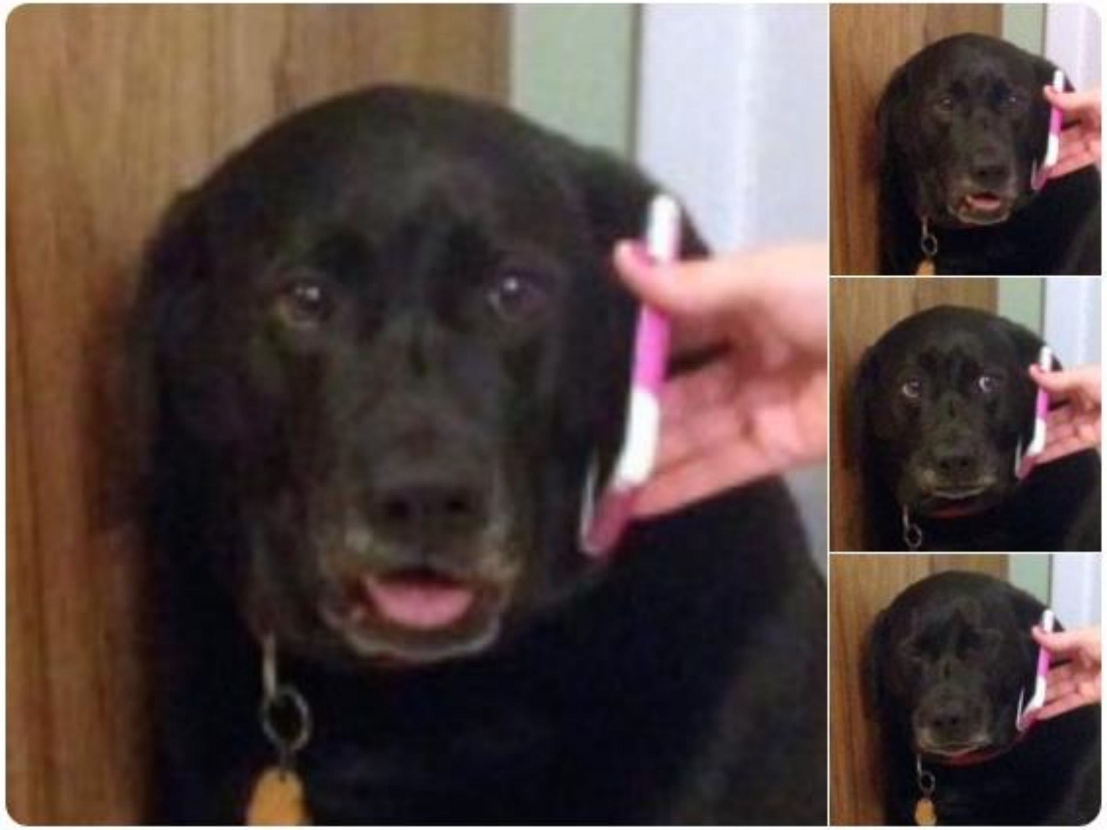
If you can measure it you can manage it

Objectives – Less Hacking, More Analyzing

- Usually *not* to break into a phone
  - Mobile operating systems mostly make this difficult
  - Mobile malware is partially mitigated by the app store model
- Compromise app access or data
  - Data on the phone
  - Data in transit
- Backend / Vendor Accounts
  - Compromising the backend is way more efficient than hacking users one by one
  - App secrets / access tokens
  - Test and staging infrastructure

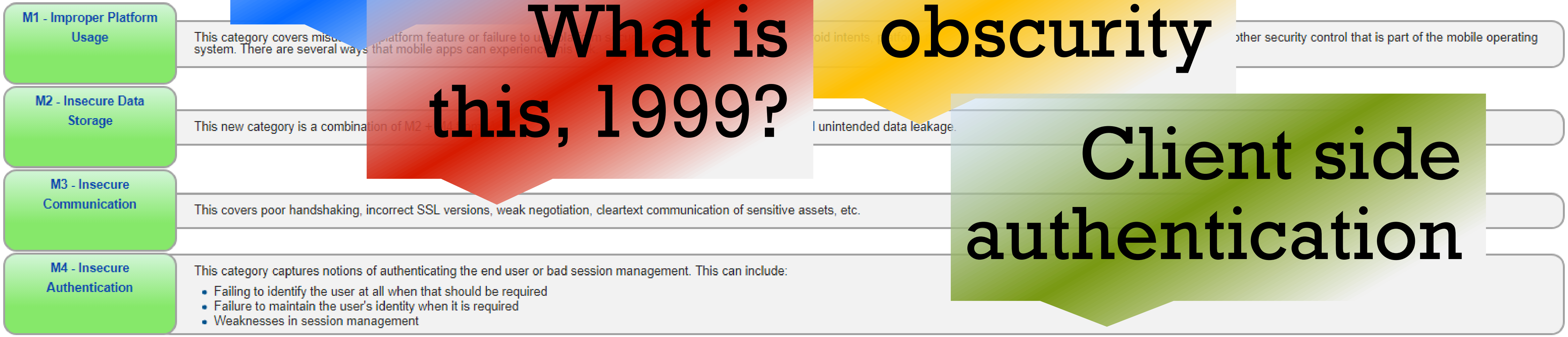
Scope Disclaimer

- There's lots more to go wrong with mobile apps. The content in this talk is just a starting point!



OWASP Top 10

OWASP does mobile too!



M1 - Improper Platform Usage	This category covers misu… platform feature or failure to u… …oid intents, … other security control that is part of the mobile operating system. There are several ways that mobile apps can experienc… this
M2 - Insecure Data Storage	This new category is a combination of M2 + M4 … unintended data leakage.
M3 - Insecure Communication	This covers poor handshaking, incorrect SSL versions, weak negotiation, cleartext communication of sensitive assets, etc.
M4 - Insecure Authentication	This category captures notions of authenticating the end user or bad session management. This can include: • Failing to identify the user at all when that should be required • Failure to maintain the user's identity when it is required • Weaknesses in session management

"Used the OS wrong"

What is this, 1999?

Security by obscurity

Client side authentication

OWASP Top 10

“We’ll check permissions in the app”

e 90’s want r XOR back

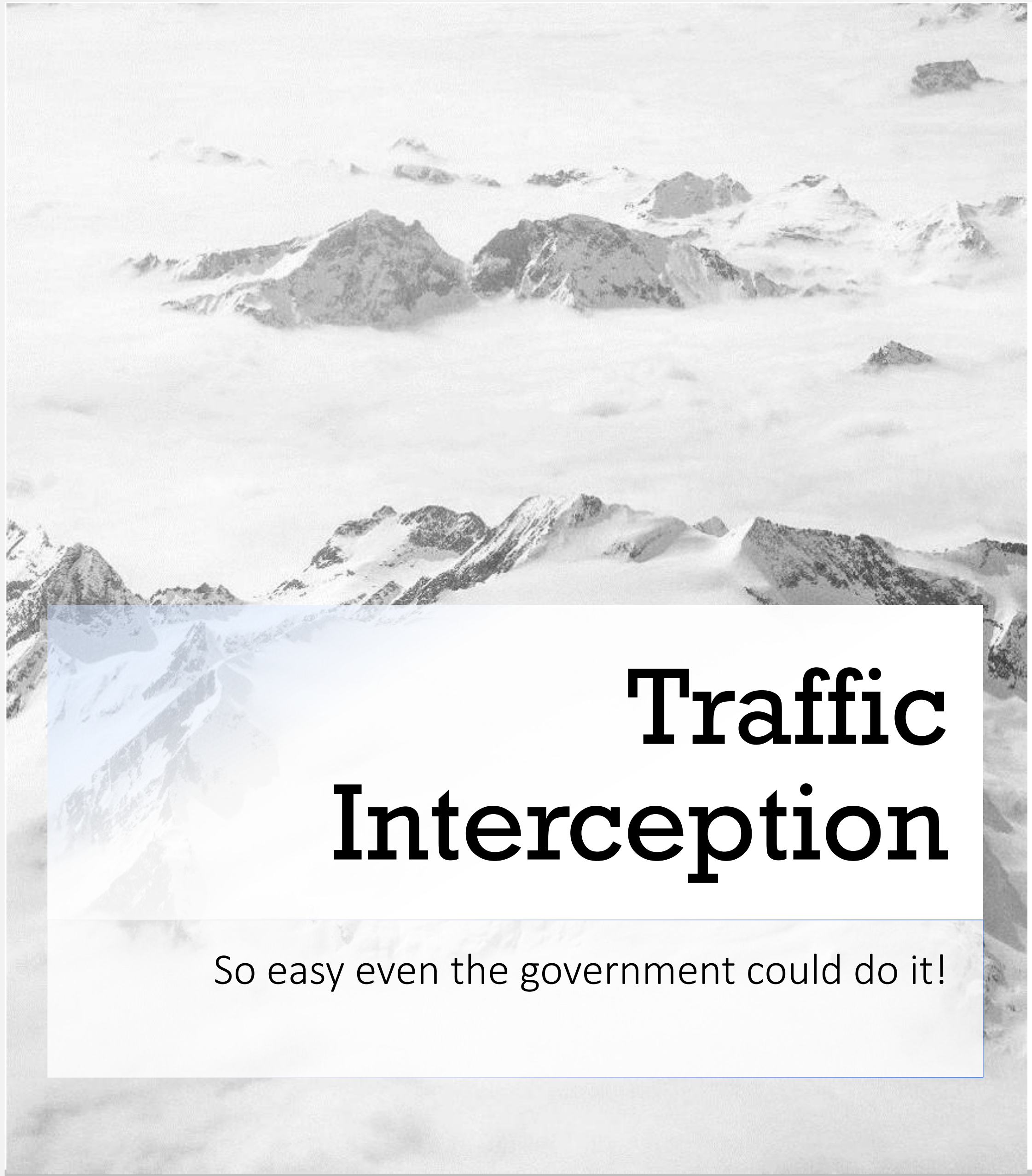
Only a problem for games

get this last

Security by obscurity

“No one will ever know”

M5 - Insufficient Cryptography	The code applies cryptography t… that probably belongs in M2 … way. Note that anything and everything related to TLS or SSL goes in M3. Also, if the app fails to use cryptography at all when it should, … rectly.
M6 - Insecure Authorization	This is a category to capture … authorization (e.g., a… ication, etc.). If the app does not authenticate users at all in a situation where it … is an authentication failure not an authorization failure.
M7 - Client Code Quality	This was the "Security Decisions Via Untrusted Inputs… de-level implementation problems in the mobile client… mistakes. This would capture things like buffer overflows, format string vulnera… e some code that…
M8 - Code Tampering	This category covers binary patching, local resource modification… amic memory modification. Once the application is delivered to the mobile device, the co… cker can either directly modify the code… system APIs that the application uses, or modify the application's data and re… of subverting the intended use of th…
M9 - Reverse Engineering	This category includes analysis o… ther assets. Software … Hopper, otool, and other binary inspection tools give the attacker insight into the inner workings of the application. This may be use… information about back end … rs, cryptographic constants and ciphers, and intellectual property.
M10 - Extraneous Functionality	Often, developers include hidden backdoor functionality or other internal development security controls that are not intended to be released into a production environment. For example, a developer may accidentally include a password as a comment in a hybrid app. Another example includes disabling of 2-factor authentication during testing.



Traffic Interception

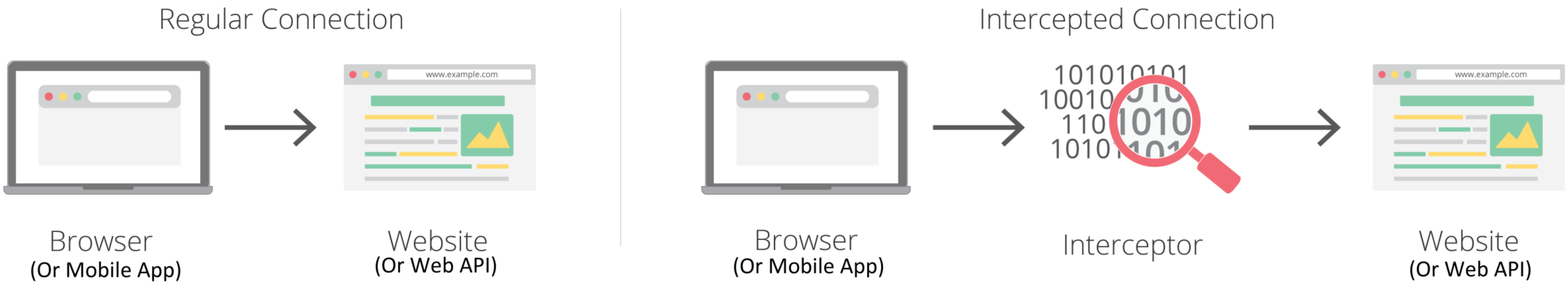
So easy even the government could do it!

Useful for discovering:

- Insecure communications
- Client side authentication
- API keys
- Backend API's

Intercepting Proxies

“Offline mobile apps are great” – said no one ever



Regular Connection

Browser
(Or Mobile App)

Website
(Or Web API)

Intercepted Connection

Browser
(Or Mobile App)

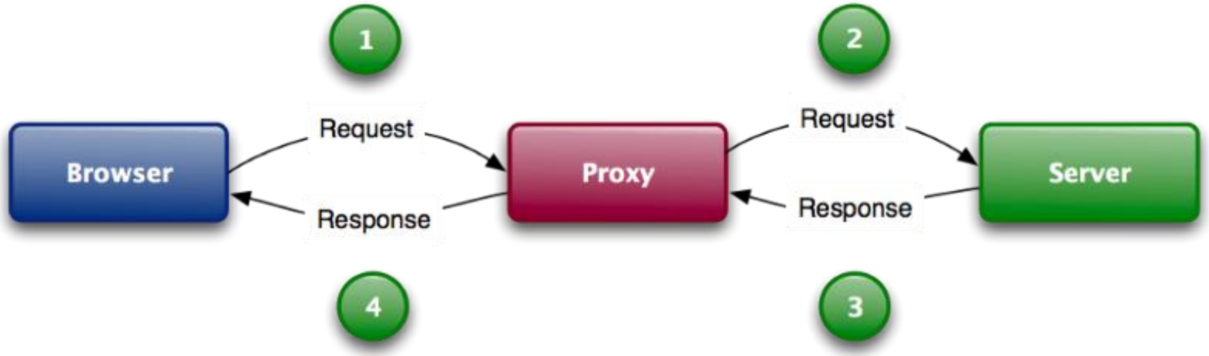
Interceptor

Website
(Or Web API)

- To capture and analyze traffic from mobile apps we need to intercepting their outgoing requests and the incoming server responses
- Proxies do this in practice on many networks already – mobile operating systems are designed with this in mind
- “Intercepting Proxies” are specifically designed for analysis functionality

Popular Intercepting Proxies

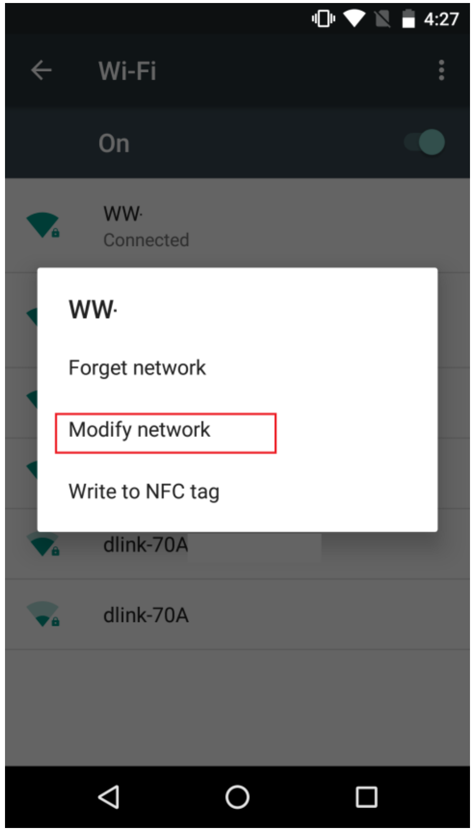
- Burp Suite Professional (or Community Edition)
  - Most popular and overall best
- ZAP – Zed Attack Proxy
  - Long time intercepting proxy tool
- Fiddler
  - Popular for normal web debugging



Proxy Setup

Android

- Settings -> Wifi -> Wifi Name -> Manage network settings



4:27

Wi-Fi

On

WW·
Connected

WW·

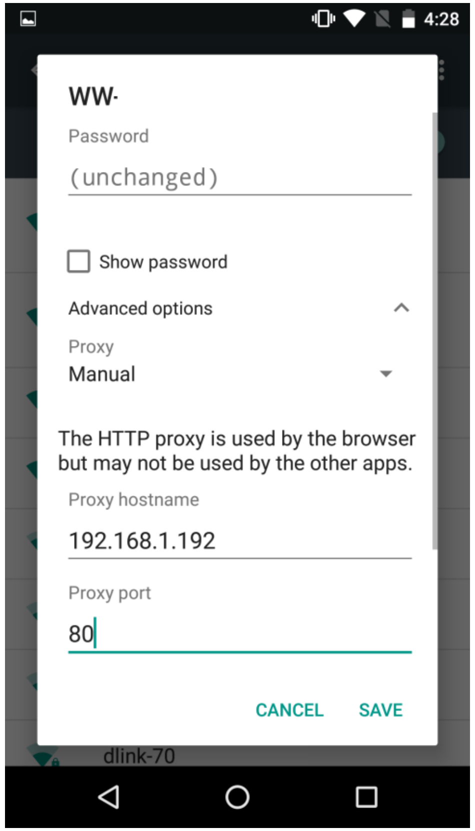
Forget network

Modify network

Write to NFC tag

dlink-70A

dlink-70A



4:28

WW·

Password

(unchanged)

□ Show password

Advanced options

Proxy
Manual

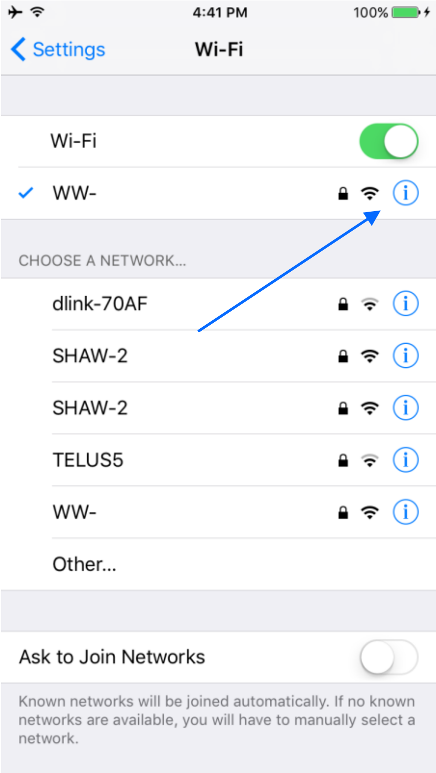
The HTTP proxy is used by the browser but may not be used by the other apps.

Proxy hostname
192.168.1.192

Proxy port
80

iOS

- Settings -> Wifi -> Wifi Name -> HTTP Proxy



4:41 PM 100%

< Settings Wi-Fi

Wi-Fi

✓ WW-

CHOOSE A NETWORK...

dlink-70AF

SHAW-2

SHAW-2

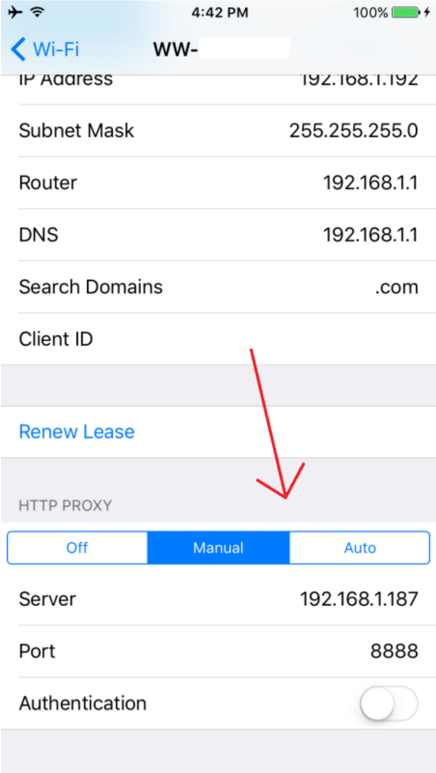
TELUS5

WW-

Other...

Ask to Join Networks

Known networks will be joined automatically. If no known networks are available, you will have to manually select a network.



4:42 PM 100%

< Wi-Fi WW-

IP Address	192.168.1.192
Subnet Mask	255.255.255.0
Router	192.168.1.1
DNS	192.168.1.1
Search Domains	.com
Client ID	

Renew Lease

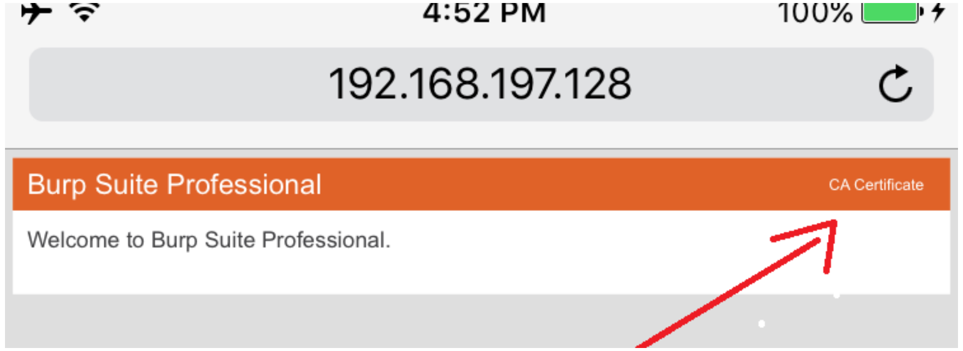
HTTP PROXY

Off [✓ Manual] Auto

Server	192.168.1.187
Port	8888
Authentication	

Certificate Authority Setup

Browse to http://127.0.0.1 (or your proxy IP)



4:52 PM 100%

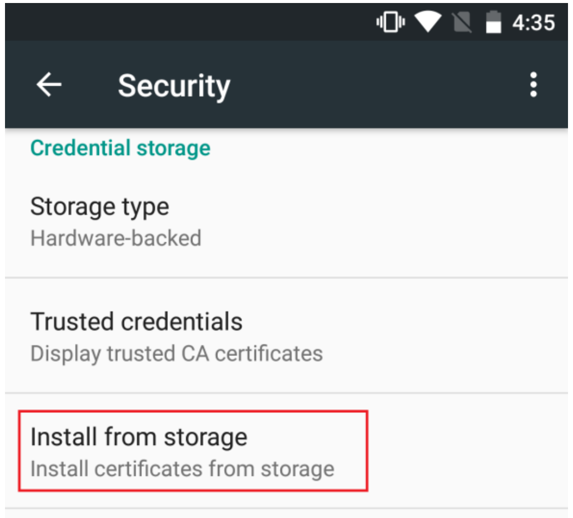
192.168.197.128

Burp Suite Professional — CA Certificate

Welcome to Burp Suite Professional.

Android:

Rename to .cer first



4:35

Security

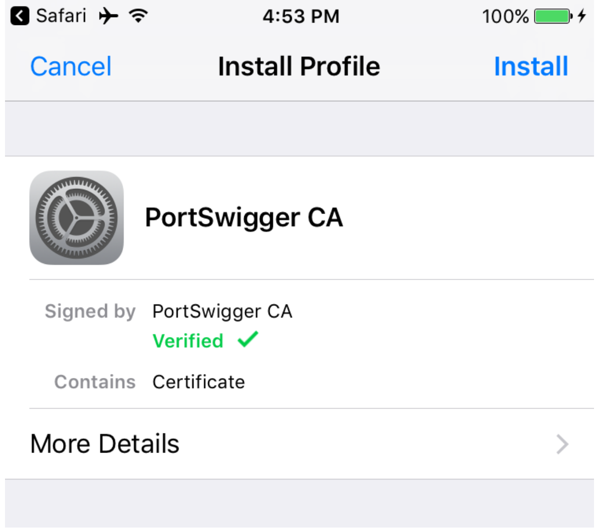
Credential storage

Storage type
Hardware-backed

Trusted credentials
Display trusted CA certificates

Install from storage
Install certificates from storage

iOS:



Safari 4:53 PM 100%

Cancel — Install Profile — Install

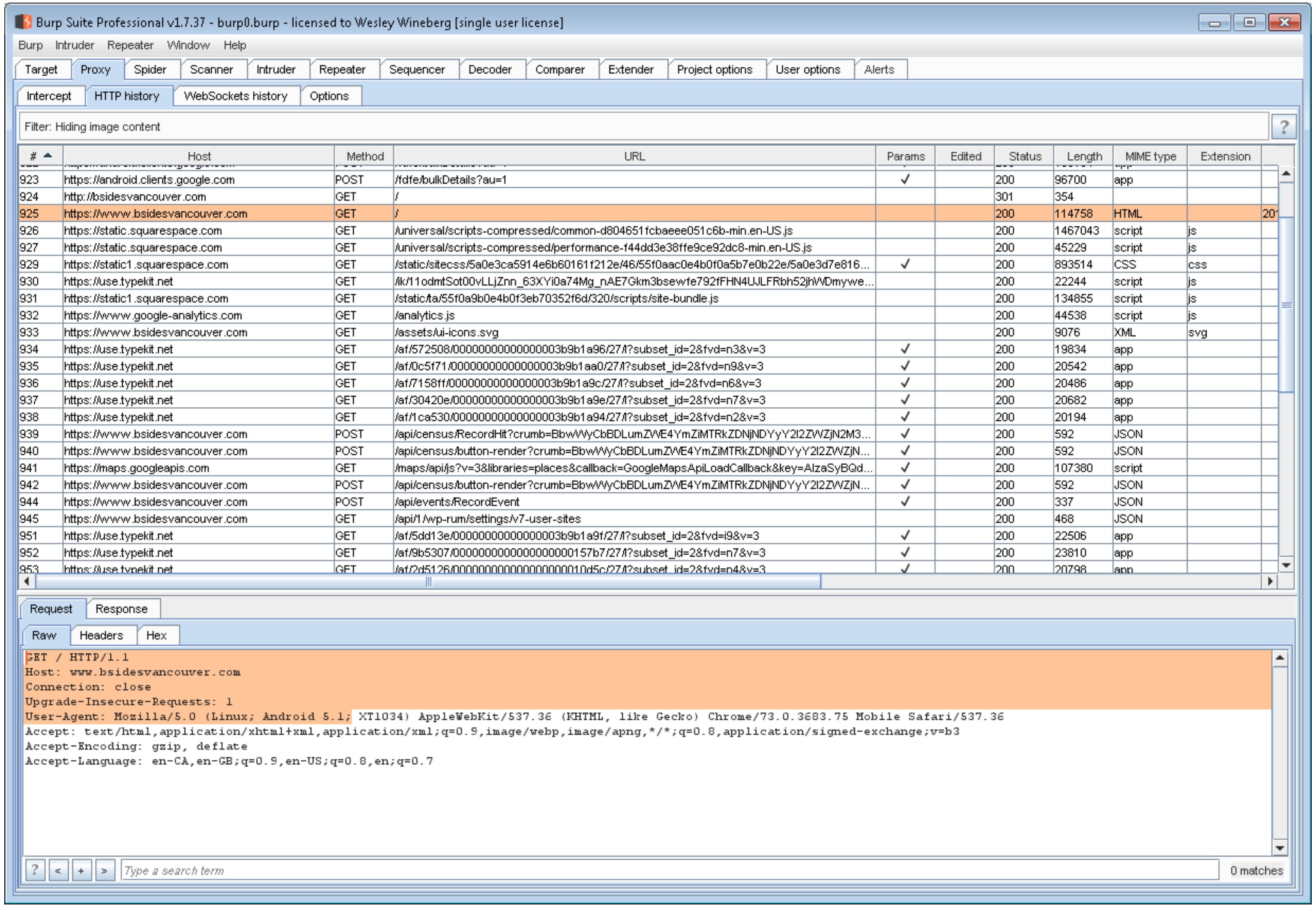
PortSwigger CA

Signed by PortSwigger CA
Verified ✓

Contains Certificate

More Details

Try it out – *Then* start hacking - Demo



Filter: Hiding image content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	
923	https://android.clients.google.com	POST	/fdfe/bulkDetails?au=1	✓		200	96700	app		
924	http://bsidesvancouver.com	GET	/			301	354			
925	https://www.bsidesvancouver.com	GET	/			200	114758	HTML		20
926	https://static.squarespace.com	GET	/universal/scripts-compressed/common-d804651fcbaeee051c6b-min.en-US.js			200	1467043	script	js	
927	https://static.squarespace.com	GET	/universal/scripts-compressed/performance-f44dd3e38ffe9ce92dc8-min.en-US.js			200	45229	script	js	
929	https://static1.squarespace.com	GET	/static/sitecss/5a0e3ca5914e6b60161f212e/46/55f0aac0e4b0f0a5b7e0b22e/5a0e3d7e816...	✓		200	893514	CSS	css	
930	https://use.typekit.net	GET	/ik/11odmtSot00vLLjZnn_63XYi0a74Mg_nAE7Gkm3bsewfe792fFHN4UJLFRbh52jhWDmywe...			200	22244	script	js	
931	https://static1.squarespace.com	GET	/static/ta/55f0a9b0e4b0f3eb70352f6d/320/scripts/site-bundle.js			200	134855	script	js	
932	https://www.google-analytics.com	GET	/analytics.js			200	44538	script	js	
933	https://www.bsidesvancouver.com	GET	/assets/ui-icons.svg			200	9076	XML	svg	
934	https://use.typekit.net	GET	/af/572508/00000000000000003b9b1a96/27/l?subset_id=2&fvd=n3&v=3	✓		200	19834	app		
935	https://use.typekit.net	GET	/af/0c5f71/00000000000000003b9b1aa0/27/l?subset_id=2&fvd=n9&v=3	✓		200	20542	app		
936	https://use.typekit.net	GET	/af/7158ff/00000000000000003b9b1a9c/27/l?subset_id=2&fvd=n6&v=3	✓		200	20486	app		
937	https://use.typekit.net	GET	/af/30420e/00000000000000003b9b1a9e/27/l?subset_id=2&fvd=n7&v=3	✓		200	20682	app		
938	https://use.typekit.net	GET	/af/1ca530/00000000000000003b9b1a94/27/l?subset_id=2&fvd=n2&v=3	✓		200	20194	app		
939	https://www.bsidesvancouver.com	POST	/api/census/RecordHit?crumb=BbwWyCbBDLumZWE4YmZiMTRkZDNjNDYyY2I2ZWZjN2M3...	✓		200	592	JSON		
940	https://www.bsidesvancouver.com	POST	/api/census/button-render?crumb=BbwWyCbBDLumZWE4YmZiMTRkZDNjNDYyY2I2ZWZjN...	✓		200	592	JSON		
941	https://maps.googleapis.com	GET	/maps/api/js?v=3&libraries=places&callback=GoogleMapsApiLoadCallback&key=AIzaSyBQd...	✓		200	107380	script		
942	https://www.bsidesvancouver.com	POST	/api/census/button-render?crumb=BbwWyCbBDLumZWE4YmZiMTRkZDNjNDYyY2I2ZWZjN...	✓		200	592	JSON		
944	https://www.bsidesvancouver.com	POST	/api/events/RecordEvent	✓		200	337	JSON		
945	https://www.bsidesvancouver.com	GET	/api/1/wp-rum/settings/v7-user-sites			200	468	JSON		
951	https://use.typekit.net	GET	/af/5dd13e/00000000000000003b9b1a9f/27/l?subset_id=2&fvd=i9&v=3	✓		200	22506	app		
952	https://use.typekit.net	GET	/af/9b5307/0000000000000000000157b7/27/l?subset_id=2&fvd=n7&v=3	✓		200	23810	app		
953	https://use.typekit.net	GET	/af/2d5126/000000000000000000010d5c/27/l?subset_id=2&fvd=n4&v=3	✓		200	20798	app		

```
GET / HTTP/1.1
Host: www.bsidesvancouver.com
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Linux; Android 5.1; XT1034) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.75 Mobile Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Accept-Encoding: gzip, deflate
Accept-Language: en-CA,en-GB;q=0.9,en-US;q=0.8,en;q=0.7
```

Sample App – Grouse Mountain iOS Demo

Grouse Mountain's mobile apps will be the unlucky demo for network traffic

Apologies for picking on them!

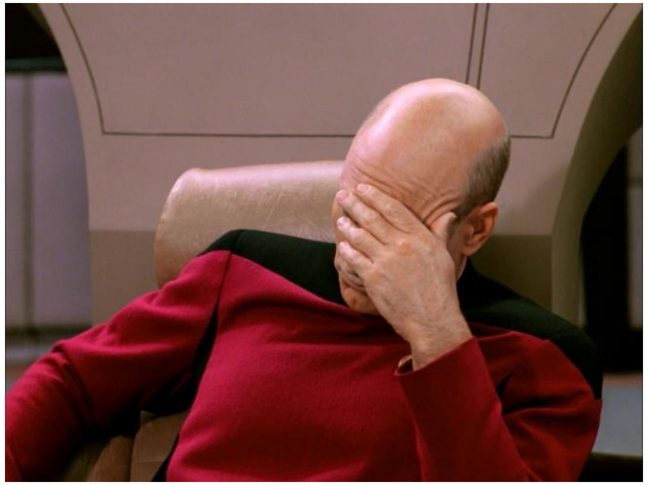
Sample App – Grouse Mountain iOS Demo

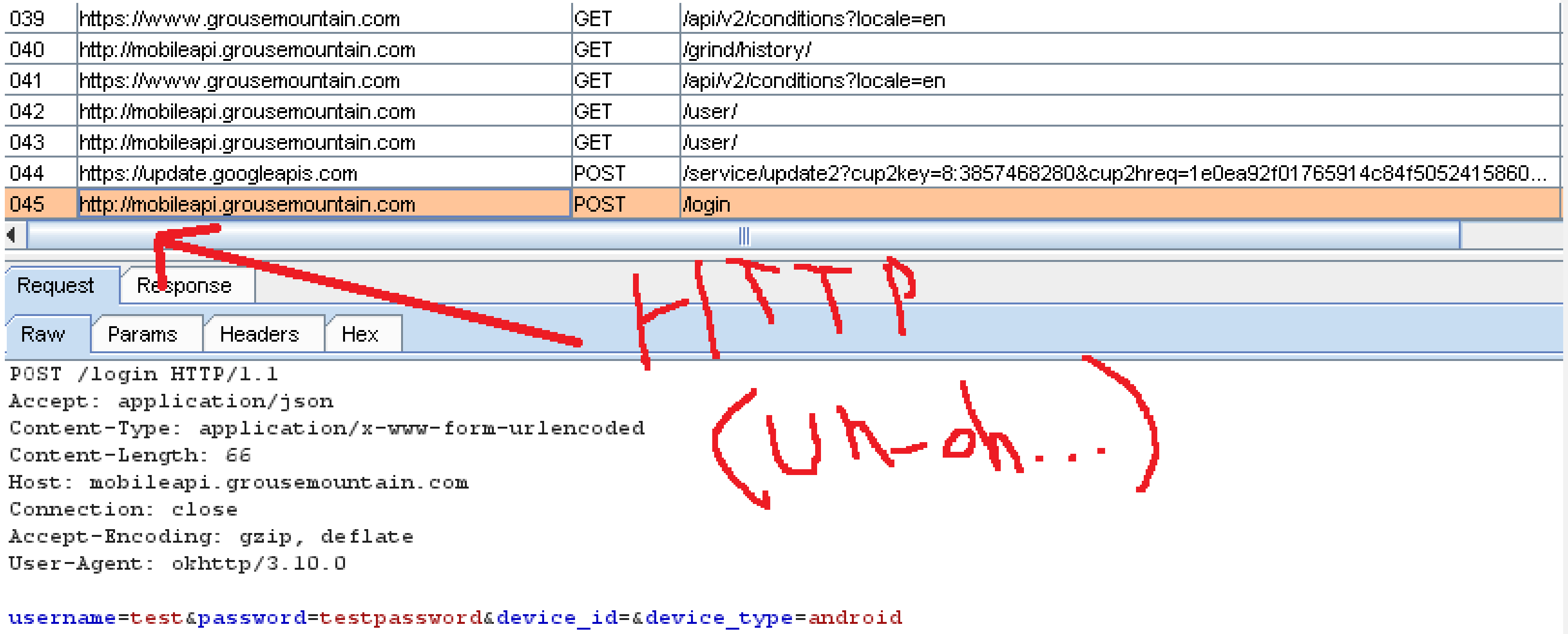
- Backend API's
- Third party services
- Types of data being sent
- No need for advanced "hacks", just look at the traffic!

Demo continues (hopefully)

Sample App – Grouse Mountain Android Demo

- No HTTPS for any authentication requests
  - HTTPS is used for other less sensitive things
- iOS “Grouse Grind” App is the same
- Typically of **many** mobile applications, even in 2019





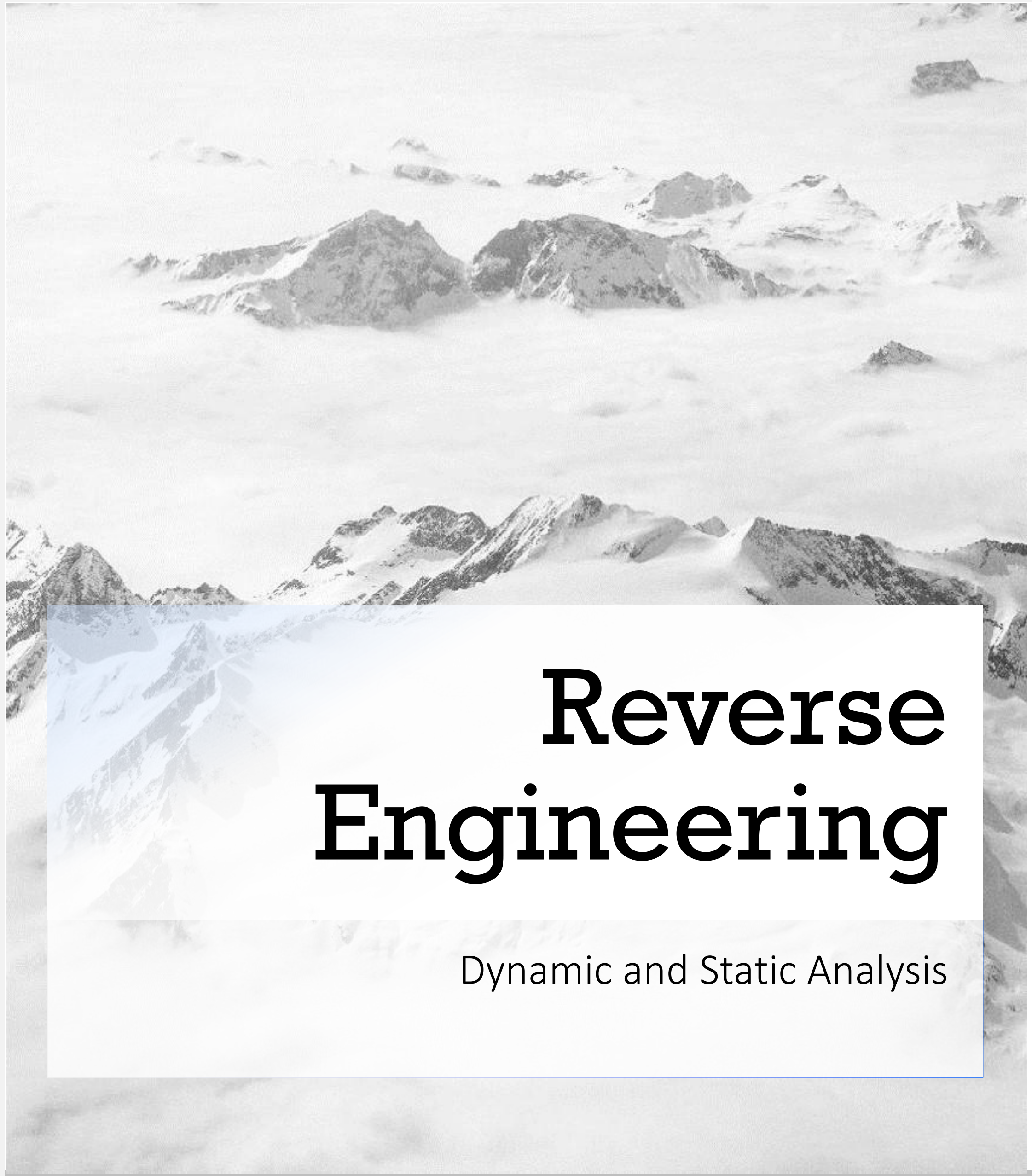
039	https://www.grousemountain.com	GET	/api/v2/conditions?locale=en
040	http://mobileapi.grousemountain.com	GET	/grind/history/
041	https://www.grousemountain.com	GET	/api/v2/conditions?locale=en
042	http://mobileapi.grousemountain.com	GET	/user/
043	http://mobileapi.grousemountain.com	GET	/user/
044	https://update.googleapis.com	POST	/service/update2?cup2key=8:3857468280&cup2hreq=1e0ea92f01765914c84f5052415860...
045	http://mobileapi.grousemountain.com	POST	/login

```
POST /login HTTP/1.1
Accept: application/json
Content-Type: application/x-www-form-urlencoded
Content-Length: 66
Host: mobileapi.grousemountain.com
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.10.0

username=test&password=testpassword&device_id=&device_type=android
```

Bypass Certificate Pinning: iOS Kill Switch

- iOS Kill Switch 2
  - Originally from iSecPartners
  - https://github.com/nabla-c0d3/ssl-kill-switch2

- Bypasses almost all certificate pinning on iOS



Reverse Engineering

Dynamic and Static Analysis

Useful for discovering:

- Hardcoded secrets
- Client side authentication
- API keys
- Test and debug functionalities
- Dev / test / staging environment details
- Backdoor mechanisms
- Missing security options

Mobile Application Reverse Engineering

Android

- Runs a Linux like OS
- Mostly ARM, now x86 too
- Java mostly
- Applications *decompile* nicely
  - Java is an compiled to an intermediate form, not to raw machine code
  - Compiled Java bytecode contains (by default at least) a large amount of metadata
  - End result is easy reverse engineering

iOS

- Runs a BSD like OS
- ARM processors (older was 32bit, newer is 64)
- Objective C mostly
- Applications do not easily *decompile*
  - Application binaries contain raw machine code
  - Disassembly to assembly language
  - Possible decompilation back to C
  - Limited metadata
  - End result is reverse engineering is not super easy

Android Apps

How to actually get a copy of an app

- All normal Android apps are distributed through the Google Play Store
  - There's also FireOS with the Amazon app store
  - Or developer / non-public apps
- No direct way to download to PC
  - Various ways to interface with the play store API's, but these are always changing or being blocked
- Download to device -> Copy to PC
  - The best option!
  - Can use an emulator if really necessary

No Jailbreak Required!

Android Apps

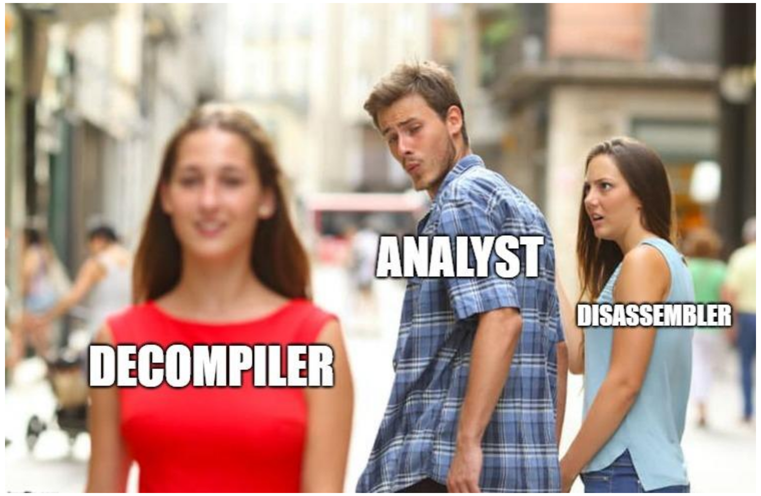
How to actually get a copy of an app

1. Enable USB Debugging
   a. https://developer.android.com/studio/debug/dev-options
2. **adb shell pm list packages** – this lists installed apps with their full names
3. **adb shell pm path your-package-name** – this prints the path to the "apk" file
4. **adb pull full/directory/of/the.apk** – this downloads the "apk" to your PC

Android SDK Required – It includes the **adb** application

From Dalvik To Java

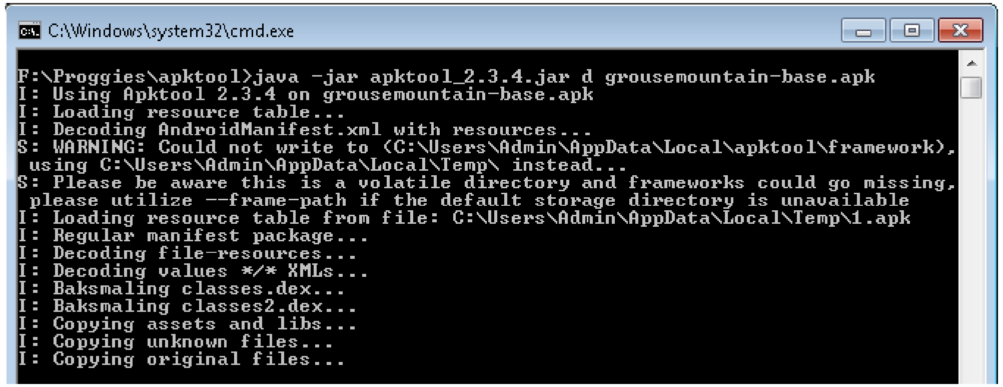
- Android Uses “Dalvik” (technically “ART” these days) not a normal “JVM”
  - All this means is the bytecode is different
  - Dalvik bytecode is stored in “dex” files instead of “class” files
- Disassembled “Dalvik” bytecode is known as “Smali” or “Baksmali”
  - You can also just call it disassembled Dalvik if you like
- Dalvik bytecode is *almost* the same as Java bytecode – translation tools exist



From Dalvik To Java

- Dex2Jar
  - **d2j-dex2jar.bat <yourapp.apk>**
  - Will output a “jar” file

- apktool
  - **java –jar apktool_2.3.4.jar d <yourappname.apk>**
  - Will output “smali” files along with “resource” files

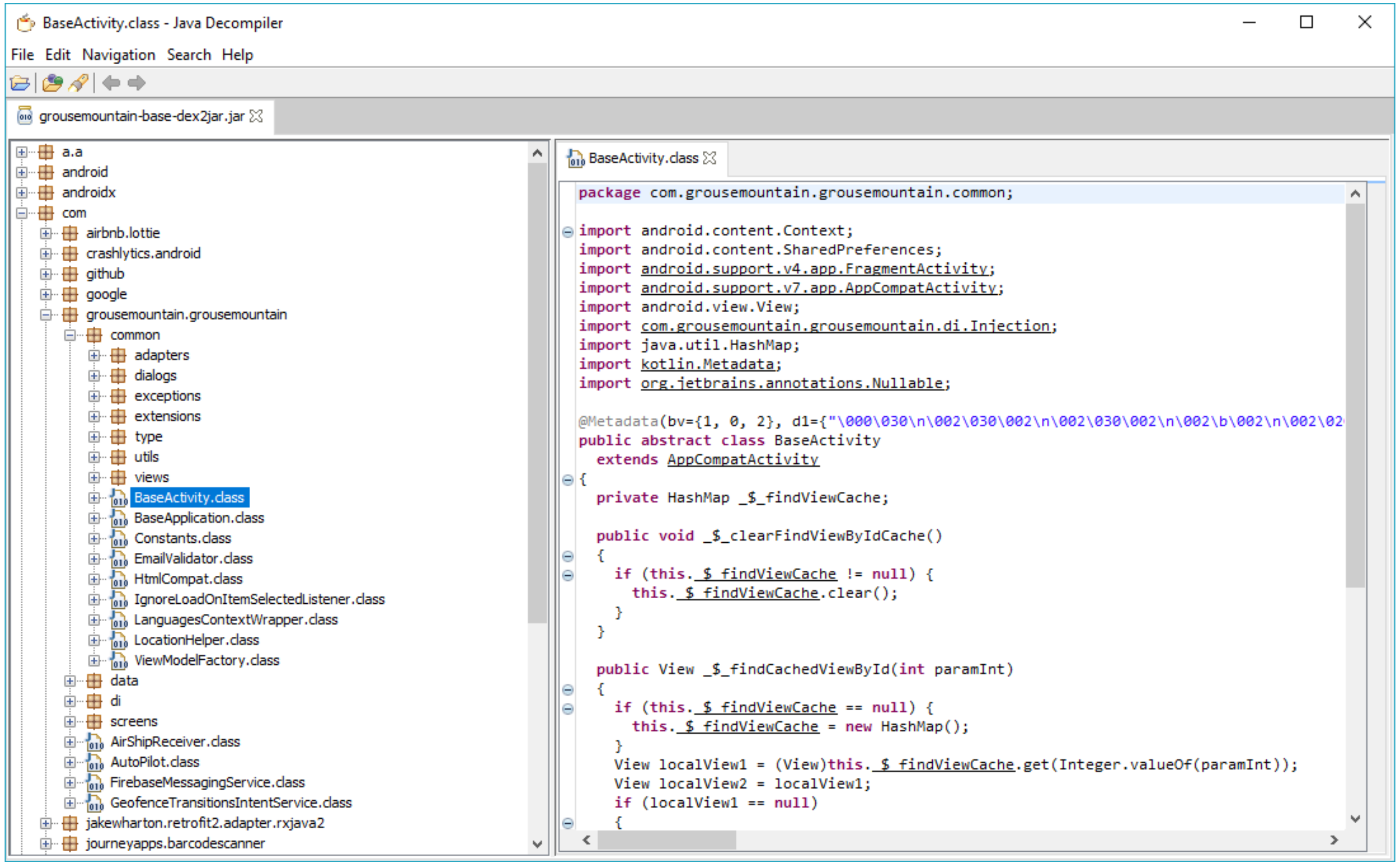


```
F:\Proggies\apktool>java -jar apktool_2.3.4.jar d grousemountain-base.apk
I: Using Apktool 2.3.4 on grousemountain-base.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
S: WARNING: Could not write to (C:\Users\Admin\AppData\Local\apktool\framework),
 using C:\Users\Admin\AppData\Local\Temp\ instead...
S: Please be aware this is a volatile directory and frameworks could go missing,
 please utilize --frame-path if the default storage directory is unavailable
I: Loading resource table from file: C:\Users\Admin\AppData\Local\Temp\1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Baksmaling classes2.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
```

Decompiling Java – Almost As Good As Source

- JD Core / JD Gui
  - http://java-decompiler.github.io/

- Application obfuscation is fairly common on Android
- Most common obfuscation results in variable and function names like a, aa, aa1, aa2, etc

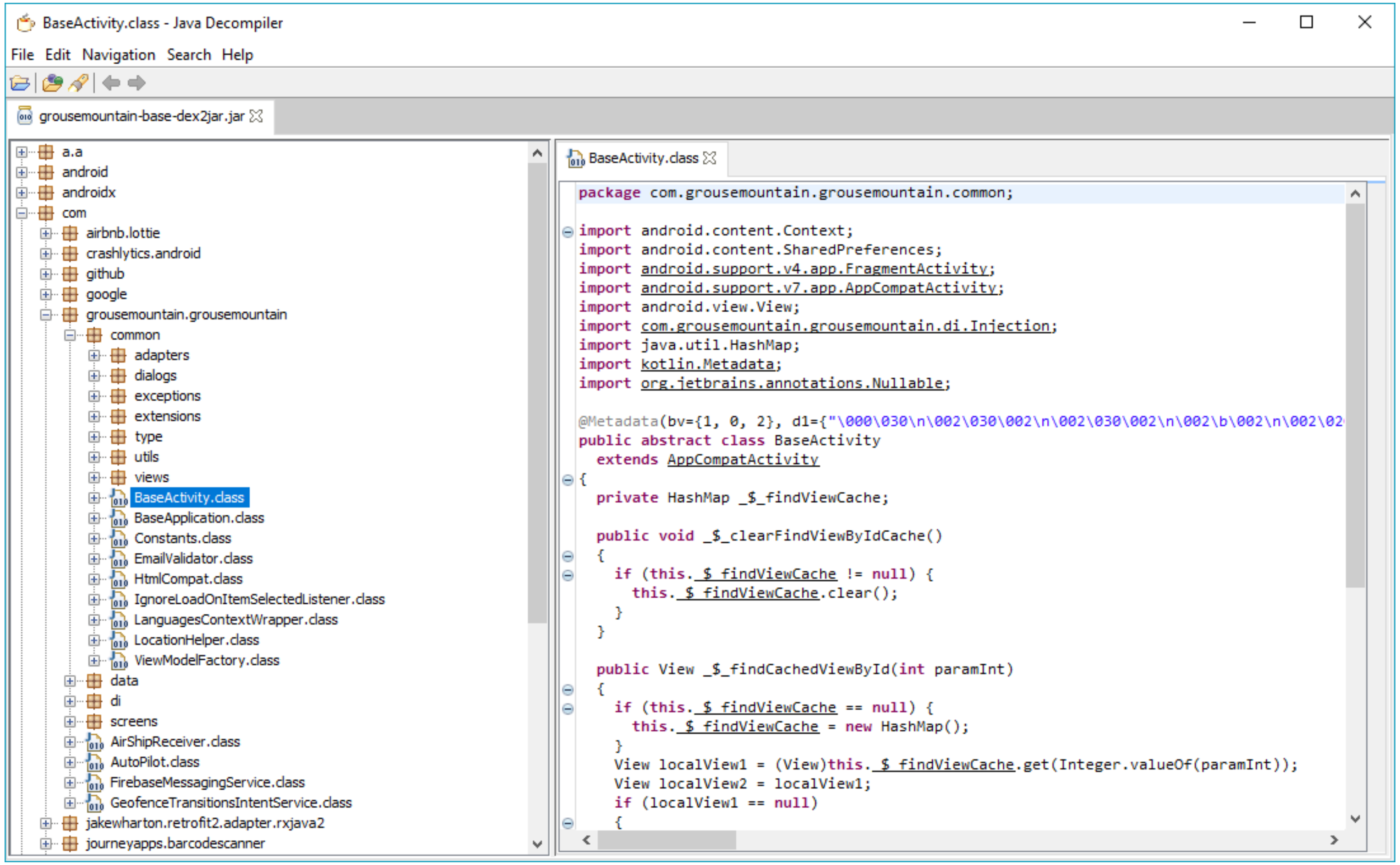


BaseActivity.class - Java Decompiler
File Edit Navigation Search Help
grousemountain-base-dex2jar.jar
BaseActivity.class

```
a.a
android
androidx
com
  airbnb.lottie
  crashlytics.android
  github
  google
  grousemountain.grousemountain
    common
      adapters
      dialogs
      exceptions
      extensions
      type
      utils
      views
      BaseActivity.class
      BaseApplication.class
      Constants.class
      EmailValidator.class
      HtmlCompat.class
      IgnoreLoadOnItemSelectedListener.class
      LanguagesContextWrapper.class
      LocationHelper.class
      ViewModelFactory.class
    data
    di
    screens
    AirShipReceiver.class
    AutoPilot.class
    FirebaseMessagingService.class
    GeofenceTransitionsIntentService.class
  jakewharton.retrofit2.adapter.rxjava2
  journeyapps.barcodescanner
```

```java
package com.grousemountain.grousemountain.common;

import android.content.Context;
import android.content.SharedPreferences;
import android.support.v4.app.FragmentActivity;
import android.support.v7.app.AppCompatActivity;
import android.view.View;
import com.grousemountain.grousemountain.di.Injection;
import java.util.HashMap;
import kotlin.Metadata;
import org.jetbrains.annotations.Nullable;

@Metadata(bv={1, 0, 2}, d1={"\000\030\n\002\030\002\n\002\030\002\n\002\b\002\n\002\02
public abstract class BaseActivity
  extends AppCompatActivity
{
  private HashMap _$_findViewCache;

  public void _$_clearFindViewByIdCache()
  {
    if (this._$_findViewCache != null) {
      this._$_findViewCache.clear();
    }
  }

  public View _$_findCachedViewById(int paramInt)
  {
    if (this._$_findViewCache == null) {
      this._$_findViewCache = new HashMap();
    }
    View localView1 = (View)this._$_findViewCache.get(Integer.valueOf(paramInt));
    View localView2 = localView1;
    if (localView1 == null)
    {
```

Decompiling Java – Demo


BaseActivity.class - Java Decompiler
File Edit Navigation Search Help
grousemountain-base-dex2jar.jar
a.a
android
androidx
com
airbnb.lottie
crashlytics.android
github
google
grousemountain.grousemountain
common
adapters
dialogs
exceptions
extensions
type
utils
views
BaseActivity.class
BaseApplication.class
Constants.class
EmailValidator.class
HtmlCompat.class
IgnoreLoadOnItemSelectedListener.class
LanguagesContextWrapper.class
LocationHelper.class
ViewModelFactory.class
data
di
screens
AirShipReceiver.class
AutoPilot.class
FirebaseMessagingService.class
GeofenceTransitionsIntentService.class
jakewharton.retrofit2.adapter.rxjava2
journeyapps.barcodescanner
BaseActivity.class

```java
package com.grousemountain.grousemountain.common;

import android.content.Context;
import android.content.SharedPreferences;
import android.support.v4.app.FragmentActivity;
import android.support.v7.app.AppCompatActivity;
import android.view.View;
import com.grousemountain.grousemountain.di.Injection;
import java.util.HashMap;
import kotlin.Metadata;
import org.jetbrains.annotations.Nullable;

@Metadata(bv={1, 0, 2}, d1={"\000\030\n\002\030\002\n\002\030\002\n\002\b\002\n\002\02
public abstract class BaseActivity
  extends AppCompatActivity
{
  private HashMap _$_findViewCache;

  public void _$_clearFindViewByIdCache()
  {
    if (this._$_findViewCache != null) {
      this._$_findViewCache.clear();
    }
  }

  public View _$_findCachedViewById(int paramInt)
  {
    if (this._$_findViewCache == null) {
      this._$_findViewCache = new HashMap();
    }
    View localView1 = (View)this._$_findViewCache.get(Integer.valueOf(paramInt));
    View localView2 = localView1;
    if (localView1 == null)
    {
```

Android Resource Files

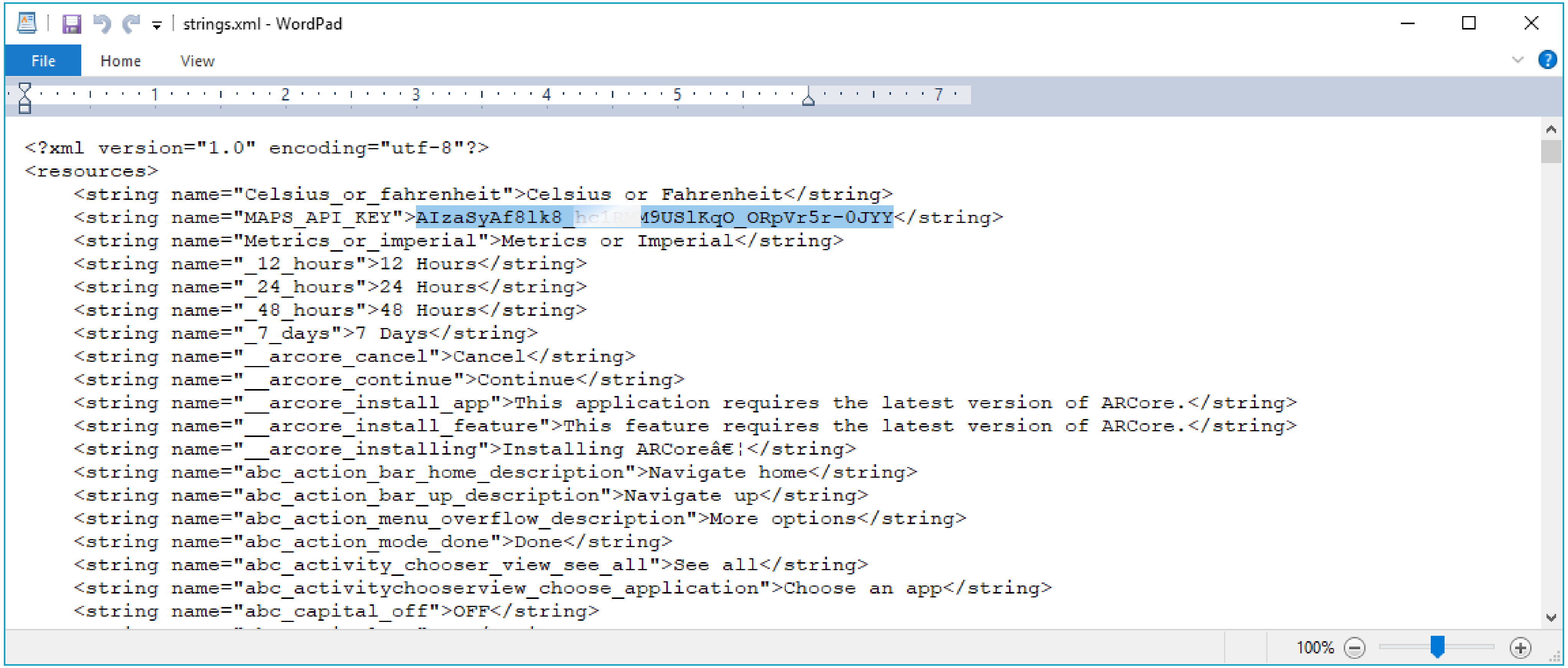
APK’s contain more than executables:

- resources.arsc
- AndroidManifest.xml
- /res/ folder
- /lib/
- App specific files (often including configuration files)

Use apktool to extract resources.arsc and AndroidManifest.xml

Android Resource Files

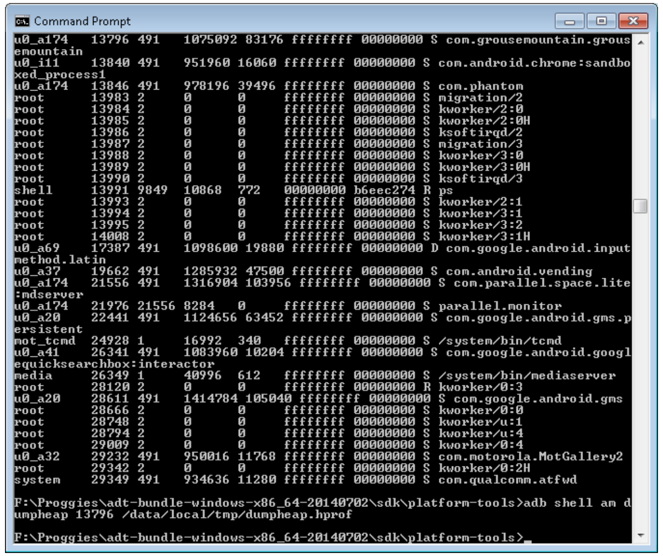
Resources.arsc will extract to /res/values/<types>



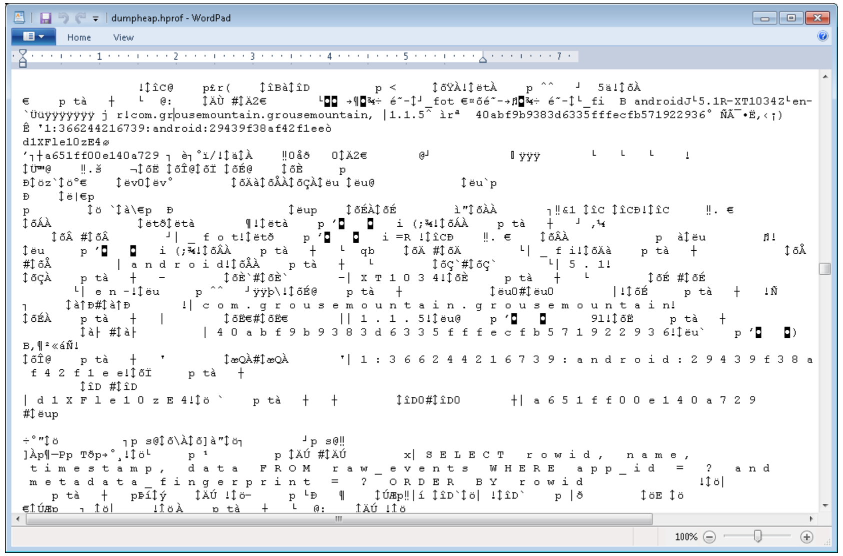
```
<?xml version="1.0" encoding="utf-8"?>
<resources>
    <string name="Celsius_or_fahrenheit">Celsius or Fahrenheit</string>
    <string name="MAPS_API_KEY">AIzaSyAf8lk8_[redacted]M9USlKqO_ORpVr5r-0JYY</string>
    <string name="Metrics_or_imperial">Metrics or Imperial</string>
    <string name="_12_hours">12 Hours</string>
    <string name="_24_hours">24 Hours</string>
    <string name="_48_hours">48 Hours</string>
    <string name="_7_days">7 Days</string>
    <string name="__arcore_cancel">Cancel</string>
    <string name="__arcore_continue">Continue</string>
    <string name="__arcore_install_app">This application requires the latest version of ARCore.</string>
    <string name="__arcore_install_feature">This feature requires the latest version of ARCore.</string>
    <string name="__arcore_installing">Installing ARCoreâ€¦</string>
    <string name="abc_action_bar_home_description">Navigate home</string>
    <string name="abc_action_bar_up_description">Navigate up</string>
    <string name="abc_action_menu_overflow_description">More options</string>
    <string name="abc_action_mode_done">Done</string>
    <string name="abc_activity_chooser_view_see_all">See all</string>
    <string name="abc_activitychooserview_choose_application">Choose an app</string>
    <string name="abc_capital_off">OFF</string>
```

Android App Memory Dump

- If an app is heavily obfuscated, just do a memory dump!
  - adb shell ps
  - adb shell am dumpheap <procid> /data/local/tmp/dumpheap.hprof
  - adb pull /data/local/tmp/dumpheap.hprof
- If an app isn't "debuggable", rewrite manifest or use app virtualization



```
u0_a174   13796 491   1075092 83176 ffffffff 00000000 S com.grousemountain.grous
emountain
u0_i11    13840 491   951960 16060 ffffffff 00000000 S com.android.chrome:sandbo
xed_process1
u0_a174   13846 491   978196 39496 ffffffff 00000000 S com.phantom
root      13983 2     0      0     ffffffff 00000000 S migration/2
root      13984 2     0      0     ffffffff 00000000 S kworker/2:0
root      13985 2     0      0     ffffffff 00000000 S kworker/2:0H
root      13986 2     0      0     ffffffff 00000000 S ksoftirqd/2
root      13987 2     0      0     ffffffff 00000000 S migration/3
root      13988 2     0      0     ffffffff 00000000 S kworker/3:0
root      13989 2     0      0     ffffffff 00000000 S kworker/3:0H
root      13990 2     0      0     ffffffff 00000000 S ksoftirqd/3
shell     13991 9849  10868  772   00000000 b6eec274 R ps
root      13993 2     0      0     ffffffff 00000000 S kworker/2:1
root      13994 2     0      0     ffffffff 00000000 S kworker/3:1
root      13995 2     0      0     ffffffff 00000000 S kworker/3:2
root      14008 2     0      0     ffffffff 00000000 S kworker/3:1H
u0_a69    17387 491   1098600 19880 ffffffff 00000000 D com.google.android.input
method.latin
u0_a37    19662 491   1285932 47500 ffffffff 00000000 S com.android.vending
u0_a174   21556 491   1316904 103956 ffffffff 00000000 S com.parallel.space.lite
:mdserver
u0_a174   21976 21556 8284   0     ffffffff 00000000 S parallel.monitor
u0_a20    22441 491   1124656 63452 ffffffff 00000000 S com.google.android.gms.p
ersistent
mot_tcmd  24928 1     16992  340   ffffffff 00000000 S /system/bin/tcmd
u0_a41    26341 491   1083960 10204 ffffffff 00000000 S com.google.android.googl
equicksearchbox:interactor
media     26349 1     40996  612   ffffffff 00000000 S /system/bin/mediaserver
root      28120 2     0      0     ffffffff 00000000 R kworker/0:3
u0_a20    28611 491   1414784 105040 ffffffff 00000000 S com.google.android.gms
root      28666 2     0      0     ffffffff 00000000 S kworker/0:0
root      28748 2     0      0     ffffffff 00000000 S kworker/u:1
root      28794 2     0      0     ffffffff 00000000 S kworker/u:4
root      29009 2     0      0     ffffffff 00000000 S kworker/0:4
u0_a32    29232 491   950016 11768 ffffffff 00000000 S com.motorola.MotGallery2
root      29342 2     0      0     ffffffff 00000000 S kworker/0:2H
system    29349 491   934636 11280 ffffffff 00000000 S com.qualcomm.atfwd

F:\Proggies\adt-bundle-windows-x86_64-20140702\sdk\platform-tools>adb shell am d
umpheap 13796 /data/local/tmp/dumpheap.hprof

F:\Proggies\adt-bundle-windows-x86_64-20140702\sdk\platform-tools>_
```



```
              !↨îC@    p£r(    ↨îBà↨îD          p <     ↨õŸÀ!↨ëtÀ    p ^^    ┘  5ä!↨õÅ
€    p tà    ┼    └   @:      ↨ÄÙ #↨Ä2€        └ →¶ ¾÷ é˜-↨┘_fot €¤õé˜-→ ¾÷ é˜-↨└_fi   B androidJ└5.1R-XT1034Z└en-
`Üüÿÿÿÿÿÿÿ j r!com.grousemountain.grousemountain, |1.1.5^ ìrª  40abf9b9383d6335fffecfb571922936° ÑÃ¯•Ë,‹¡)
Ê '1:366244216739:android:29439f38af42f1eeò
d1XFle10zE4ø
'┐┼a651ff00e140a729 ┐ è┐°ï/!↨ä↨À    ‼0åð    0↨Ä2€        @┘              ÿÿÿ       └    └    └     !
↨Ü™@    ‼.š     ¬↨õË ↨õÎ@↨õÏ ↨õÉ@    ↨õÈ     p
Ð↨öz`↨ö°€      ↨ëv0↨ëv°        ↨õÄà↨õÅÀ↨õÇÀ↨ëu ↨ëu@              ↨ëu`p
Ð     ↨ë|€p
p          ↨ö `↨à\€p  Ð                   ↨ëup     ↨õÉÀ↨õÉ          ì"↨õÀÀ         ┐‼&1 ↨îC ↨îCÐ!↨îC      ‼. €
↨õÁÀ              ↨ëtð↨ëtà          ¶!↨ëtà     p '     i (;¾!↨õÁÀ     p tà    ┼    ┘ ,¼
    ↨õÂ #↨õÂ          ┘| _ f o t!↨ëtð     p '     i =R !↨îCÐ     ‼. €     ↨õÂÀ              p  à↨ëu          ♫!
↨ëu       p '     i (;¾!↨õÂÀ      p tà    ┼    └   qb      ↨õÄ #↨õÄ          └| _ f i!↨õÄà     p tà    ┼          ↨õÅ
#↨õÅ            | a n d r o i d!↨õÅÀ     p tà    ┼    └            ↨õÇ`#↨õÇ`         └| 5 . 1!
↨õÇÀ      p tà    ┼    –           ↨õÈ`#↨õÈ`         –| X T 1 0 3 4!↨õÈ       p tà    ┼    └          ↨õÉ #↨õÉ
        └| e n -!↨ëu       p ^^    ┘ÿÿþ\!↨õÉ@     p tà    ┼                ↨ëu0#↨ëu0          |!↨õÉ      p tà    ┼    !Ñ
┐        ↨à↑Ð#↨à↑Ð          !| c o m . g r o u s e m o u n t a i n . g r o u s e m o u n t a i n!
↨õÉÀ      p tà    ┼    |            ↨õË€#↨õË€         || 1 . 1 . 5!↨ëu@      p '          9l!↨õË      p tà    ┼
        ↨à├ #↨à├          | 4 0 a b f 9 b 9 3 8 3 d 6 3 3 5 f f f e c f b 5 7 1 9 2 2 9 3 6!↨ëu`     p '     )
B,¶²«áÑ!
↨õÎ@      p tà    ┼    '           ↨æQÀ#↨æQÀ          '| 1 : 3 6 6 2 4 4 2 1 6 7 3 9 : a n d r o i d : 2 9 4 3 9 f 3 8 a
 f 4 2 f 1 e e!↨õÏ       p tà    ┼
        ↨îD #↨îD
| d 1 X F l e 1 0 z E 4!↨ö `     p tà    ┼    ┼           ↨îD0#↨îD0          ┼| a 6 5 1 f f 0 0 e 1 4 0 a 7 2 9
#↨ëup

÷°"↨ö          ┐p s@↨õ\À↨õ]à"↨ö┐          ┘p s@‼
]Àp¶—Ðp Tðp→°¸!↨ö└     p ¹          p ↨ÄÚ #↨ÄÚ          x| S E L E C T   r o w i d ,   n a m e ,
 t i m e s t a m p ,   d a t a   F R O M   r a w _ e v e n t s   W H E R E   a p p _ i d   =   ?   a n d
 m e t a d a t a _ f i n g e r p r i n t   =   ?   O R D E R   B Y   r o w i d               !↨ö|
    p tà    ┼    pÐí↨ý    ↨ÄÚ !↨ö–     p └Ð   ¶    ↨ÚÆp‼|í ↨îD`↨ö| !↨îD`    p |ð          ↨öE ↨ö
€↨ÚÆp   ┐ ↨ö|      !↨öÀ    p tà    ┼    └  @:     ↨ÄÚ !↨ö
```

iOS Apps

How to actually get a copy of an app

- All normal iOS apps are distributed through the Apple App Store
  - Or developer / non-public apps
- PC downloads are encrypted
  - Apple’s FairPlay DRM protects executables
- Download to PC -> Copy to device -> Unprotect -> Copy to PC
  - Tools change across iOS versions
  - Once setup process is fairly painless
  - Works best on iOS 10

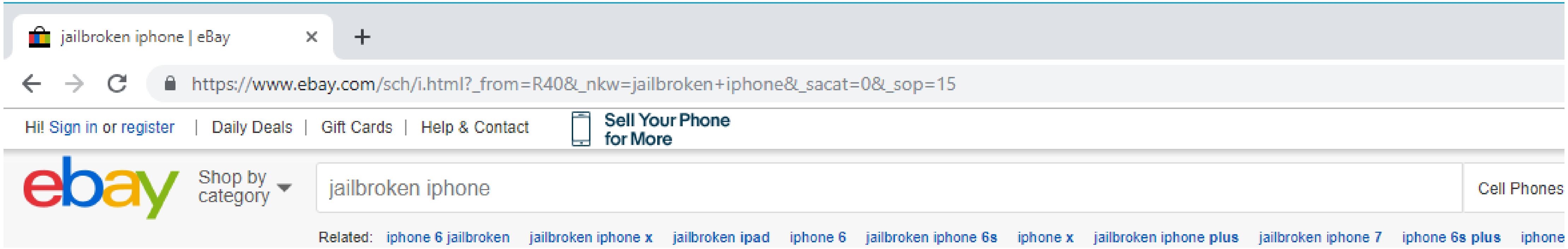
Jailbreak Required™

By The Way…

If you are unfamiliar with Jailbreaking on iOS:

1. Get your credit card

2. Type in “Jailbroken iPhone” on ebay.com



jailbroken iphone | eBay

https://www.ebay.com/sch/i.html?_from=R40&_nkw=jailbroken+iphone&_sacat=0&_sop=15

Hi! Sign in or register | Daily Deals | Gift Cards | Help & Contact

Sell Your Phone for More

Shop by category

jailbroken iphone

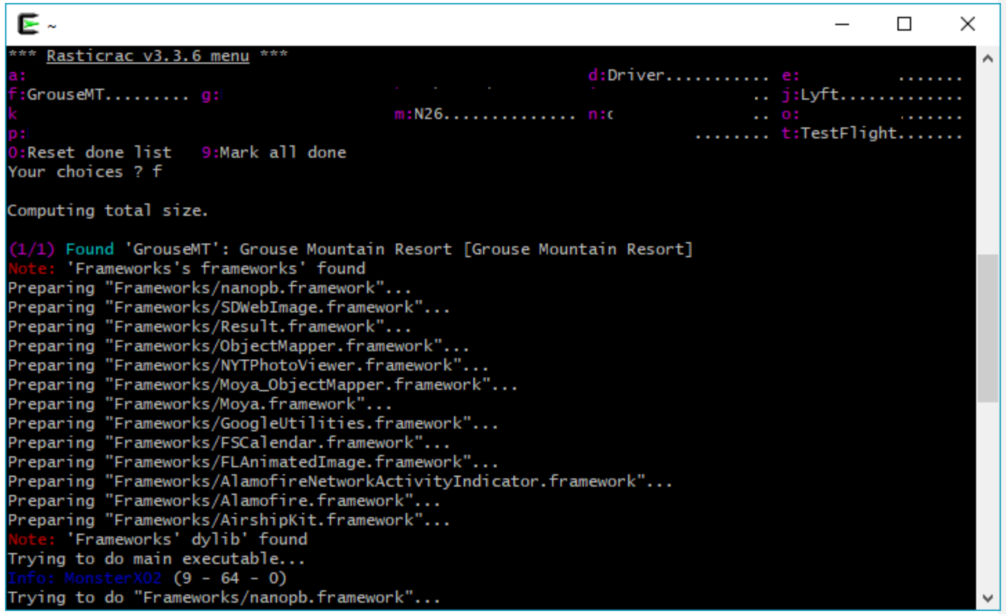
Cell Phones

Related: iphone 6 jailbroken jailbroken iphone x jailbroken ipad iphone 6 jailbroken iphone 6s iphone x jailbroken iphone plus jailbroken iphone 7 iphone 6s plus iphone

iOS Apps

How to actually get a copy of an app

1. Download via iTunes on your PC
2. Sync to your iPhone
3. SSH into your iPhone
4. **rc -m** - this launches the menu for rasticrac
5. **Clutch –d <id>** - for older phones
6. **bfinject**, etc for iOS 11
7. SFTP to your phone and copy the outputted “ipa” package to your PC



```
*** Rasticrac v3.3.6 menu ***
a:                                                        d:Driver.......... e:           .......
f:GrouseMT......... g:                                                    .. j:Lyft............
k                                        m:N26............. n:c            .. o:           .......
p:                                                                ........ t:TestFlight.......
0:Reset done list   9:Mark all done
Your choices ? f

Computing total size.

(1/1) Found 'GrouseMT': Grouse Mountain Resort [Grouse Mountain Resort]
Note: 'Frameworks's frameworks' found
Preparing "Frameworks/nanopb.framework"...
Preparing "Frameworks/SDWebImage.framework"...
Preparing "Frameworks/Result.framework"...
Preparing "Frameworks/ObjectMapper.framework"...
Preparing "Frameworks/NYTPhotoViewer.framework"...
Preparing "Frameworks/Moya_ObjectMapper.framework"...
Preparing "Frameworks/Moya.framework"...
Preparing "Frameworks/GoogleUtilities.framework"...
Preparing "Frameworks/FSCalendar.framework"...
Preparing "Frameworks/FLAnimatedImage.framework"...
Preparing "Frameworks/AlamofireNetworkActivityIndicator.framework"...
Preparing "Frameworks/Alamofire.framework"...
Preparing "Frameworks/AirshipKit.framework"...
Note: 'Frameworks' dylib' found
Trying to do main executable...
Info: MonsterX02 (9 - 64 - 0)
Trying to do "Frameworks/nanopb.framework"...
```

Rasticrac is available in iPhoneCake and AppAddict repositories. Or as standalone.

Clutch is available from AppAddict repository or as standalone

Disassembling iOS Applications

- Hopper
- IDA Pro
- Others… Binary Ninja, Ghidra, etc

Disassembling iOS Applications

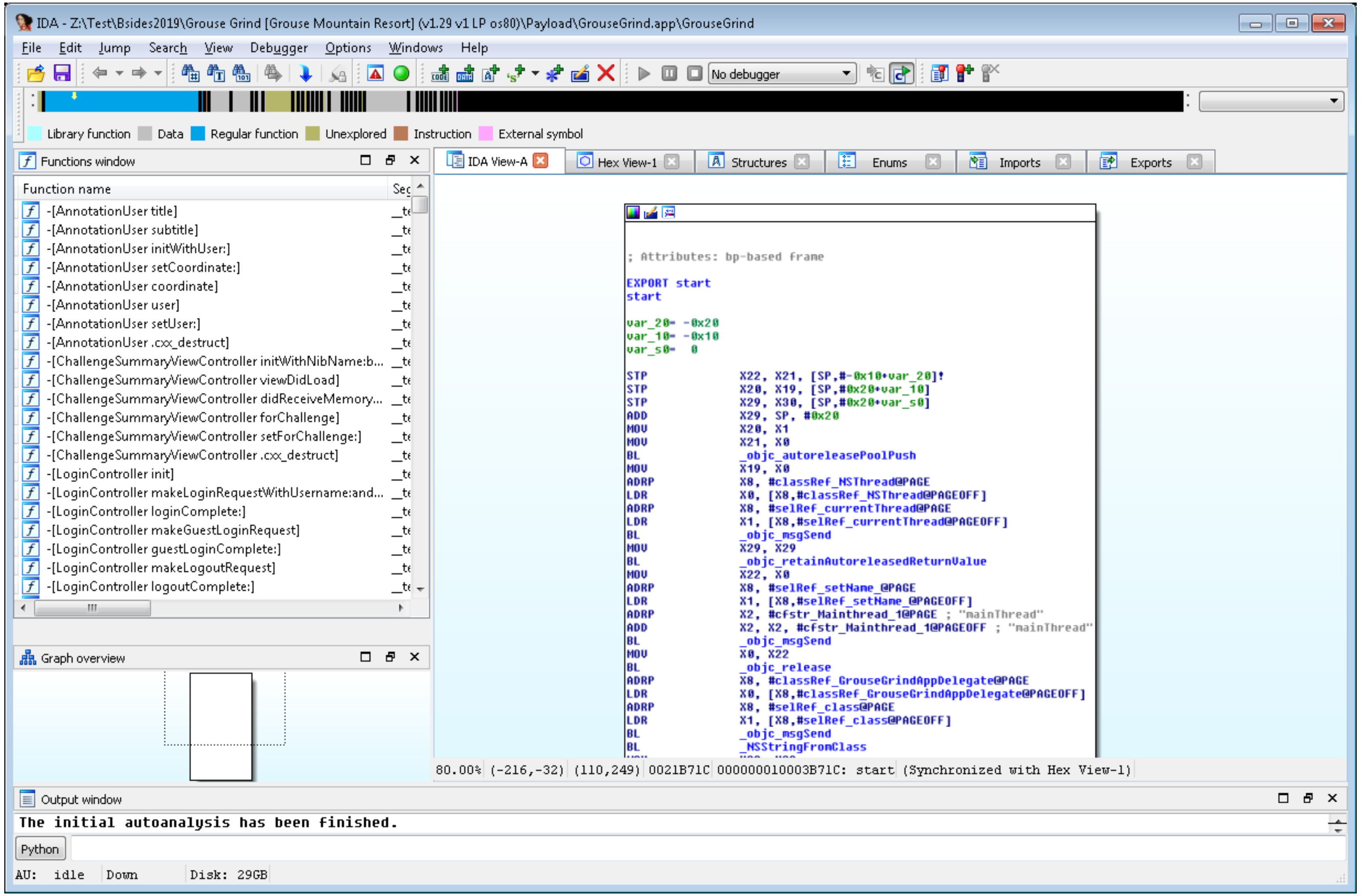
Possible to recover:

- Program structure
- Function names
- Some variable names

Does not recover:

- High level instructions

Applications are rarely obfuscated



IDA - Z:\Test\Bsides2019\Grouse Grind [Grouse Mountain Resort] (v1.29 v1 LP os80)\Payload\GrouseGrind.app\GrouseGrind

```
Function name                                              Seg
-[AnnotationUser title]                                    _te
-[AnnotationUser subtitle]                                 _te
-[AnnotationUser initWithUser:]                            _te
-[AnnotationUser setCoordinate:]                           _te
-[AnnotationUser coordinate]                               _te
-[AnnotationUser user]                                     _te
-[AnnotationUser setUser:]                                 _te
-[AnnotationUser .cxx_destruct]                            _te
-[ChallengeSummaryViewController initWithNibName:b...      _te
-[ChallengeSummaryViewController viewDidLoad]              _te
-[ChallengeSummaryViewController didReceiveMemory...       _te
-[ChallengeSummaryViewController forChallenge]             _te
-[ChallengeSummaryViewController setForChallenge:]         _te
-[ChallengeSummaryViewController .cxx_destruct]            _te
-[LoginController init]                                    _te
-[LoginController makeLoginRequestWithUsername:and...      _te
-[LoginController loginComplete:]                          _te
-[LoginController makeGuestLoginRequest]                   _te
-[LoginController guestLoginComplete:]                     _te
-[LoginController makeLogoutRequest]                       _te
-[LoginController logoutComplete:]                         _te
```

```
; Attributes: bp-based frame

EXPORT start
start

var_20= -0x20
var_10= -0x10
var_s0=  0

STP             X22, X21, [SP,#-0x10+var_20]!
STP             X20, X19, [SP,#0x20+var_10]
STP             X29, X30, [SP,#0x20+var_s0]
ADD             X29, SP, #0x20
MOV             X20, X1
MOV             X21, X0
BL              _objc_autoreleasePoolPush
MOV             X19, X0
ADRP            X8, #classRef_NSThread@PAGE
LDR             X0, [X8,#classRef_NSThread@PAGEOFF]
ADRP            X8, #selRef_currentThread@PAGE
LDR             X1, [X8,#selRef_currentThread@PAGEOFF]
BL              _objc_msgSend
MOV             X29, X29
BL              _objc_retainAutoreleasedReturnValue
MOV             X22, X0
ADRP            X8, #selRef_setName_@PAGE
LDR             X1, [X8,#selRef_setName_@PAGEOFF]
ADRP            X2, #cfstr_Mainthread_1@PAGE ; "mainThread"
ADD             X2, X2, #cfstr_Mainthread_1@PAGEOFF ; "mainThread"
BL              _objc_msgSend
MOV             X0, X22
BL              _objc_release
ADRP            X8, #classRef_GrouseGrindAppDelegate@PAGE
LDR             X0, [X8,#classRef_GrouseGrindAppDelegate@PAGEOFF]
ADRP            X8, #selRef_class@PAGE
LDR             X1, [X8,#selRef_class@PAGEOFF]
BL              _objc_msgSend
BL              _NSStringFromClass
```

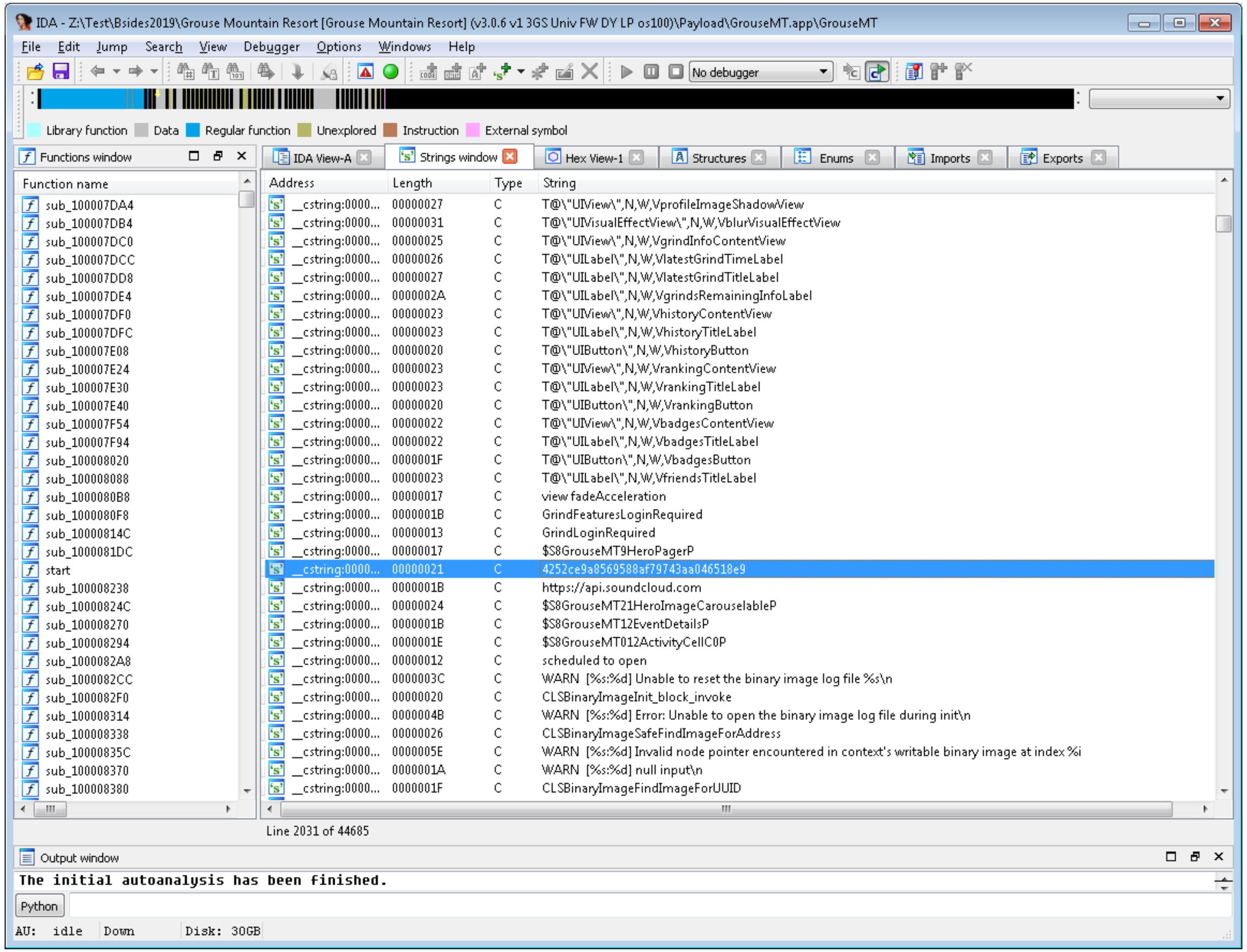
```
80.00% (-216,-32) (110,249) 0021B71C 000000010003B71C: start (Synchronized with Hex View-1)
```

```
The initial autoanalysis has been finished.
```

```
AU:  idle   Down    Disk: 29GB
```

B|Sides Vancouver

Disassembling iOS Applications



Function name
sub_100007DA4
sub_100007DB4
sub_100007DC0
sub_100007DCC
sub_100007DD8
sub_100007DE4
sub_100007DF0
sub_100007DFC
sub_100007E08
sub_100007E24
sub_100007E30
sub_100007E40
sub_100007F54
sub_100007F94
sub_100008020
sub_100008088
sub_1000080B8
sub_1000080F8
sub_10000814C
sub_1000081DC
start
sub_100008238
sub_10000824C
sub_100008270
sub_100008294
sub_1000082A8
sub_1000082CC
sub_1000082F0
sub_100008314
sub_100008338
sub_10000835C
sub_100008370
sub_100008380

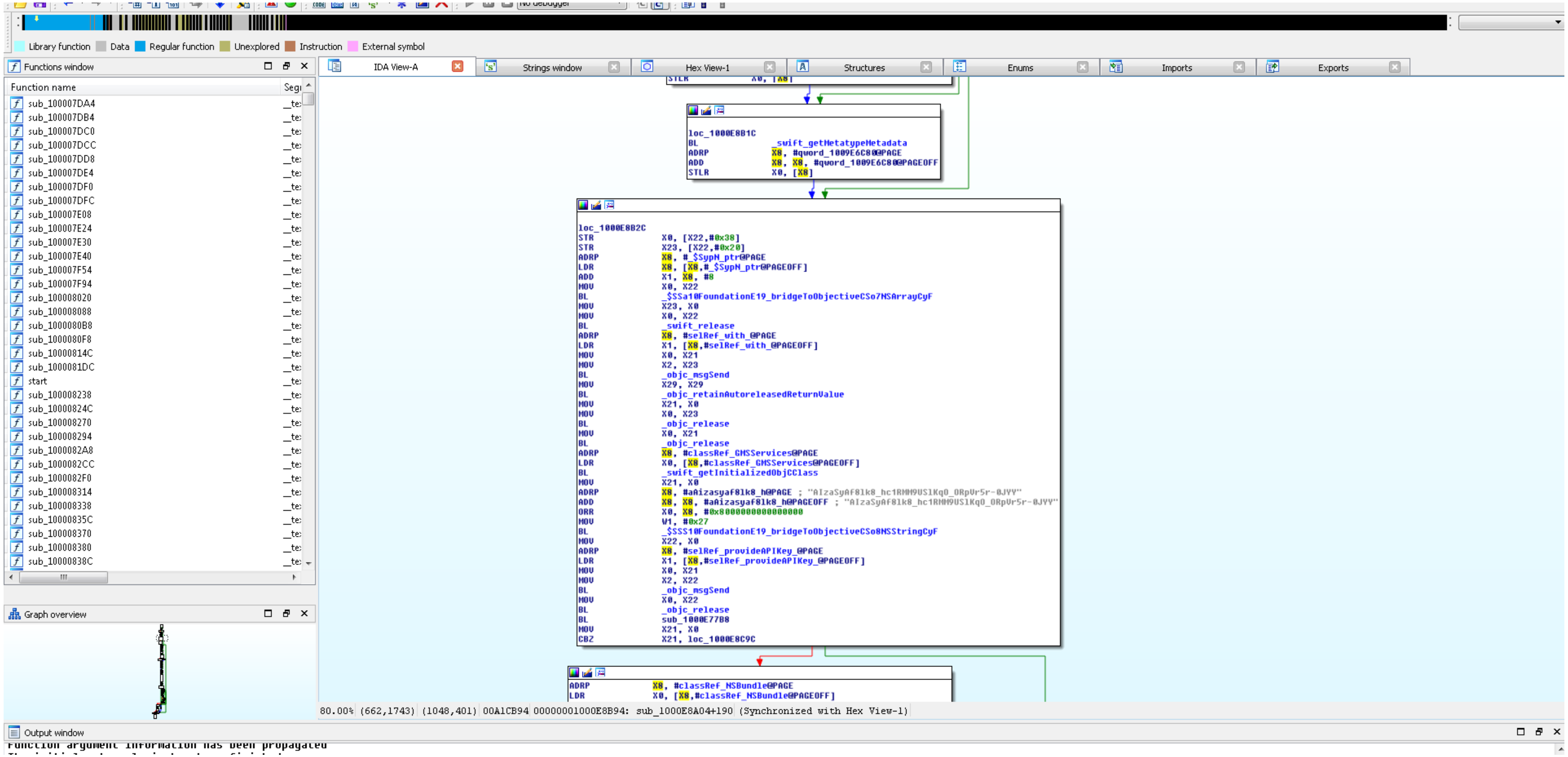
Address	Length	Type	String
__cstring:0000...	00000027	C	T@\"UIView\",N,W,VprofileImageShadowView
__cstring:0000...	00000031	C	T@\"UIVisualEffectView\",N,W,VblurVisualEffectView
__cstring:0000...	00000025	C	T@\"UIView\",N,W,VgrindInfoContentView
__cstring:0000...	00000026	C	T@\"UILabel\",N,W,VlatestGrindTimeLabel
__cstring:0000...	00000027	C	T@\"UILabel\",N,W,VlatestGrindTitleLabel
__cstring:0000...	0000002A	C	T@\"UILabel\",N,W,VgrindsRemainingInfoLabel
__cstring:0000...	00000023	C	T@\"UIView\",N,W,VhistoryContentView
__cstring:0000...	00000023	C	T@\"UILabel\",N,W,VhistoryTitleLabel
__cstring:0000...	00000020	C	T@\"UIButton\",N,W,VhistoryButton
__cstring:0000...	00000023	C	T@\"UIView\",N,W,VrankingContentView
__cstring:0000...	00000023	C	T@\"UILabel\",N,W,VrankingTitleLabel
__cstring:0000...	00000020	C	T@\"UIButton\",N,W,VrankingButton
__cstring:0000...	00000022	C	T@\"UIView\",N,W,VbadgesContentView
__cstring:0000...	00000022	C	T@\"UILabel\",N,W,VbadgesTitleLabel
__cstring:0000...	0000001F	C	T@\"UIButton\",N,W,VbadgesButton
__cstring:0000...	00000023	C	T@\"UILabel\",N,W,VfriendsTitleLabel
__cstring:0000...	00000017	C	view fadeAcceleration
__cstring:0000...	0000001B	C	GrindFeaturesLoginRequired
__cstring:0000...	00000013	C	GrindLoginRequired
__cstring:0000...	00000017	C	$S8GrouseMT9HeroPagerP
__cstring:0000...	00000021	C	4252ce9a8569588af79743aa046518e9
__cstring:0000...	0000001B	C	https://api.soundcloud.com
__cstring:0000...	00000024	C	$S8GrouseMT21HeroImageCarouselableP
__cstring:0000...	0000001B	C	$S8GrouseMT12EventDetailsP
__cstring:0000...	0000001E	C	$S8GrouseMT012ActivityCellC0P
__cstring:0000...	00000012	C	scheduled to open
__cstring:0000...	0000003C	C	WARN [%s:%d] Unable to reset the binary image log file %s\n
__cstring:0000...	00000020	C	CLSBinaryImageInit_block_invoke
__cstring:0000...	0000004B	C	WARN [%s:%d] Error: Unable to open the binary image log file during init\n
__cstring:0000...	00000026	C	CLSBinaryImageSafeFindImageForAddress
__cstring:0000...	0000005E	C	WARN [%s:%d] Invalid node pointer encountered in context's writable binary image at index %i
__cstring:0000...	0000001A	C	WARN [%s:%d] null input\n
__cstring:0000...	0000001F	C	CLSBinaryImageFindImageForUUID

Line 2031 of 44685

```
The initial autoanalysis has been finished.
```

```
AU:  idle   Down      Disk: 30GB
```

Disassembling iOS Applications



```
Function name                  Segm
sub_100007DA4                  _te
sub_100007DB4                  _te
sub_100007DC0                  _te
sub_100007DCC                  _te
sub_100007DD8                  _te
sub_100007DE4                  _te
sub_100007DF0                  _te
sub_100007DFC                  _te
sub_100007E08                  _te
sub_100007E24                  _te
sub_100007E30                  _te
sub_100007E40                  _te
sub_100007F54                  _te
sub_100007F94                  _te
sub_100008020                  _te
sub_100008088                  _te
sub_1000080B8                  _te
sub_1000080F8                  _te
sub_10000814C                  _te
sub_1000081DC                  _te
start                          _te
sub_100008238                  _te
sub_10000824C                  _te
sub_100008270                  _te
sub_100008294                  _te
sub_1000082A8                  _te
sub_1000082CC                  _te
sub_1000082F0                  _te
sub_100008314                  _te
sub_100008338                  _te
sub_10000835C                  _te
sub_100008370                  _te
sub_100008380                  _te
sub_10000838C                  _te
```

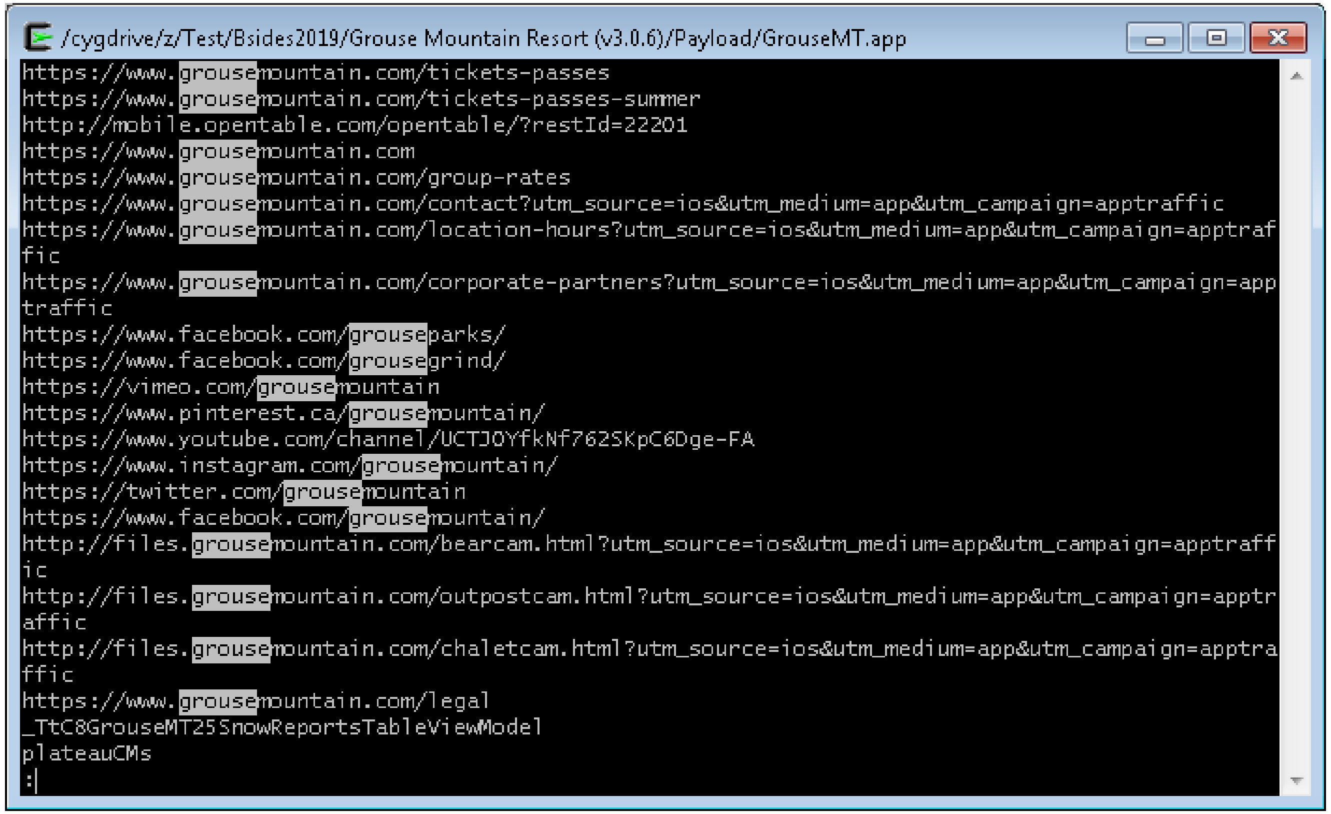
```
STLR            X0, [X8]

loc_1000E8B1C
BL              _swift_getMetatypeMetadata
ADRP            X8, #qword_1009E6C80@PAGE
ADD             X8, X8, #qword_1009E6C80@PAGEOFF
STLR            X0, [X8]

loc_1000E8B2C
STR             X0, [X22,#0x38]
STR             X23, [X22,#0x20]
ADRP            X8, #_$SypN_ptr@PAGE
LDR             X8, [X8,#_$SypN_ptr@PAGEOFF]
ADD             X1, X8, #8
MOV             X0, X22
BL              _$SSa10FoundationE19_bridgeToObjectiveCSo7NSArrayCyF
MOV             X23, X0
MOV             X0, X22
BL              _swift_release
ADRP            X8, #selRef_with_@PAGE
LDR             X1, [X8,#selRef_with_@PAGEOFF]
MOV             X0, X21
MOV             X2, X23
BL              _objc_msgSend
MOV             X29, X29
BL              _objc_retainAutoreleasedReturnValue
MOV             X21, X0
MOV             X0, X23
BL              _objc_release
MOV             X0, X21
BL              _objc_release
ADRP            X8, #classRef_GMSServices@PAGE
LDR             X0, [X8,#classRef_GMSServices@PAGEOFF]
BL              _swift_getInitializedObjCClass
MOV             X21, X0
ADRP            X8, #aAizasyaf8lk8_h@PAGE ; "AIzaSyAf8lk8_hc1RMM9USlKqO_ORpVr5r-0JYY"
ADD             X8, X8, #aAizasyaf8lk8_h@PAGEOFF ; "AIzaSyAf8lk8_hc1RMM9USlKqO_ORpVr5r-0JYY"
ORR             X0, X8, #0x8000000000000000
MOV             W1, #0x27
BL              _$SSS10FoundationE19_bridgeToObjectiveCSo8NSStringCyF
MOV             X22, X0
ADRP            X8, #selRef_provideAPIKey_@PAGE
LDR             X1, [X8,#selRef_provideAPIKey_@PAGEOFF]
MOV             X0, X21
MOV             X2, X22
BL              _objc_msgSend
MOV             X0, X22
BL              _objc_release
BL              sub_1000E77B8
MOV             X21, X0
CBZ             X21, loc_1000E8C9C

ADRP            X8, #classRef_NSBundle@PAGE
LDR             X0, [X8,#classRef_NSBundle@PAGEOFF]
```

```
80.00% (662,1743) (1048,401) 00A1CB94 00000001000E8B94: sub_1000E8A04+190 (Synchronized with Hex View-1)
```

```
Function argument information has been propagated
```

Analyzing iOS Applications

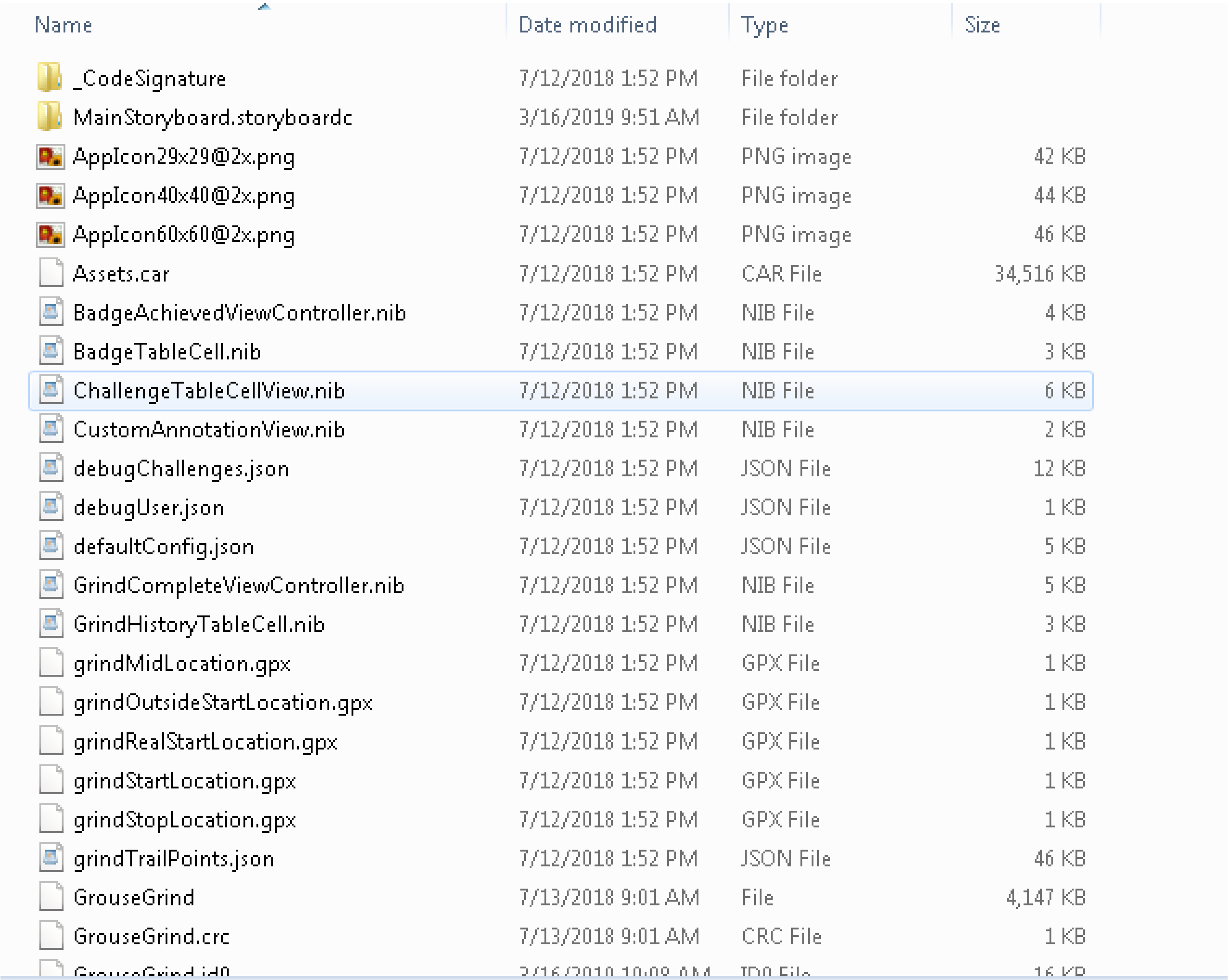
- Analyzing disassembly is (somewhat) hard
- Just use **strings** and **grep** instead!



/cygdrive/z/Test/Bsides2019/Grouse Mountain Resort (v3.0.6)/Payload/GrouseMT.app

```
https://www.grousemountain.com/tickets-passes
https://www.grousemountain.com/tickets-passes-summer
http://mobile.opentable.com/opentable/?restId=22201
https://www.grousemountain.com
https://www.grousemountain.com/group-rates
https://www.grousemountain.com/contact?utm_source=ios&utm_medium=app&utm_campaign=apptraffic
https://www.grousemountain.com/location-hours?utm_source=ios&utm_medium=app&utm_campaign=apptraf
fic
https://www.grousemountain.com/corporate-partners?utm_source=ios&utm_medium=app&utm_campaign=app
traffic
https://www.facebook.com/grouseparks/
https://www.facebook.com/grousegrind/
https://vimeo.com/grousemountain
https://www.pinterest.ca/grousemountain/
https://www.youtube.com/channel/UCTJOYfkNf762SKpC6Dge-FA
https://www.instagram.com/grousemountain/
https://twitter.com/grousemountain
https://www.facebook.com/grousemountain/
http://files.grousemountain.com/bearcam.html?utm_source=ios&utm_medium=app&utm_campaign=apptraff
ic
http://files.grousemountain.com/outpostcam.html?utm_source=ios&utm_medium=app&utm_campaign=apptr
affic
http://files.grousemountain.com/chaletcam.html?utm_source=ios&utm_medium=app&utm_campaign=apptra
ffic
https://www.grousemountain.com/legal
_TtC8GrouseMT25SnowReportsTableViewModel
plateauCMs
:
```

iOS Resource Files



Name	Date modified	Type	Size
_CodeSignature	7/12/2018 1:52 PM	File folder	
MainStoryboard.storyboardc	3/16/2019 9:51 AM	File folder	
AppIcon29x29@2x.png	7/12/2018 1:52 PM	PNG image	42 KB
AppIcon40x40@2x.png	7/12/2018 1:52 PM	PNG image	44 KB
AppIcon60x60@2x.png	7/12/2018 1:52 PM	PNG image	46 KB
Assets.car	7/12/2018 1:52 PM	CAR File	34,516 KB
BadgeAchievedViewController.nib	7/12/2018 1:52 PM	NIB File	4 KB
BadgeTableCell.nib	7/12/2018 1:52 PM	NIB File	3 KB
ChallengeTableCellView.nib	7/12/2018 1:52 PM	NIB File	6 KB
CustomAnnotationView.nib	7/12/2018 1:52 PM	NIB File	2 KB
debugChallenges.json	7/12/2018 1:52 PM	JSON File	12 KB
debugUser.json	7/12/2018 1:52 PM	JSON File	1 KB
defaultConfig.json	7/12/2018 1:52 PM	JSON File	5 KB
GrindCompleteViewController.nib	7/12/2018 1:52 PM	NIB File	5 KB
GrindHistoryTableCell.nib	7/12/2018 1:52 PM	NIB File	3 KB
grindMidLocation.gpx	7/12/2018 1:52 PM	GPX File	1 KB
grindOutsideStartLocation.gpx	7/12/2018 1:52 PM	GPX File	1 KB
grindRealStartLocation.gpx	7/12/2018 1:52 PM	GPX File	1 KB
grindStartLocation.gpx	7/12/2018 1:52 PM	GPX File	1 KB
grindStopLocation.gpx	7/12/2018 1:52 PM	GPX File	1 KB
grindTrailPoints.json	7/12/2018 1:52 PM	JSON File	46 KB
GrouseGrind	7/13/2018 9:01 AM	File	4,147 KB
GrouseGrind.crc	7/13/2018 9:01 AM	CRC File	1 KB
GrouseGrind.id0	3/16/2019 10:08 AM	ID0 File	16 KB

iOS Resource Files

IPA’s contain more than executables:

- plist files
- Info.plist
- Storyboard folders – not useful
- /frameworks/ (this is actually just more executables)
- App specific files (often including configuration files)

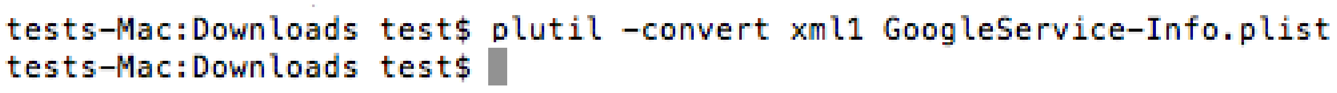
Use **plutil** to extract plist files

iOS Resource Files

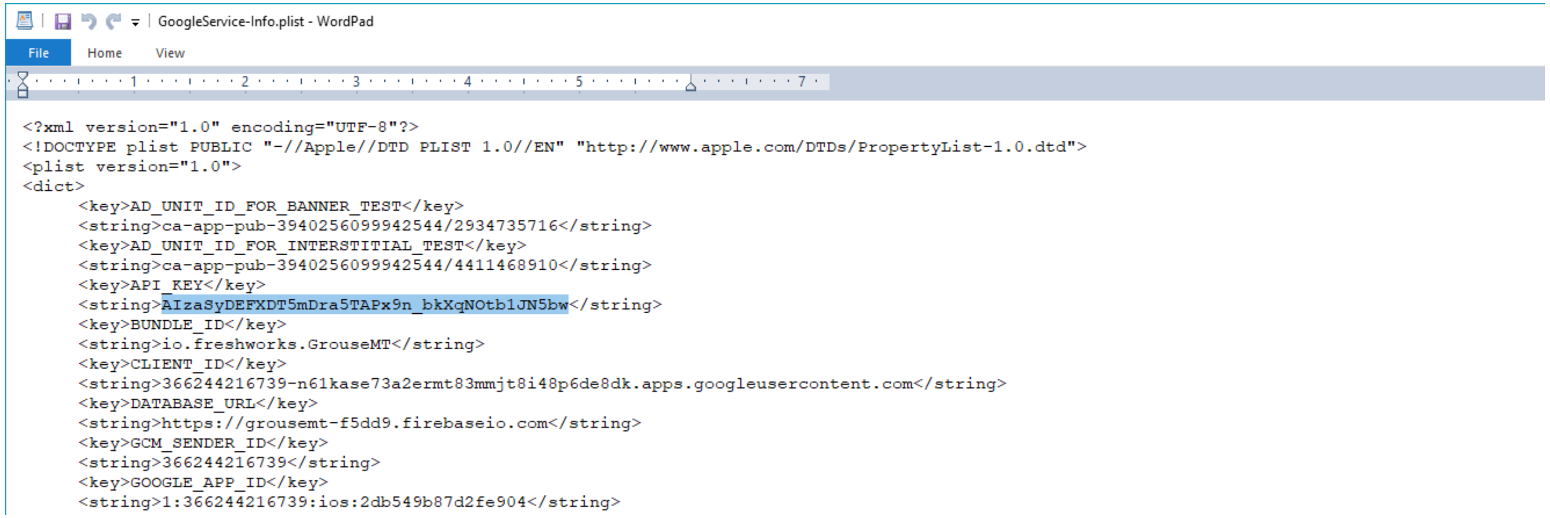
To convert a plist to XML:

- plutil –convert xml1 filename.plist

For example:



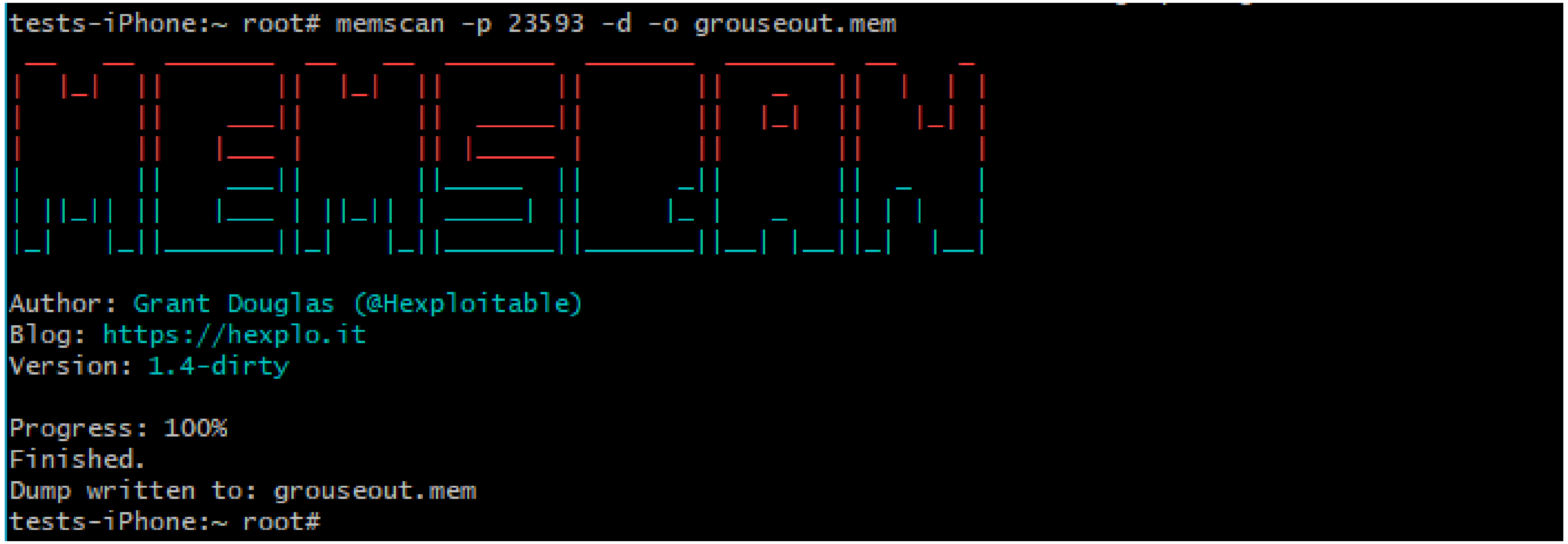
```
tests-Mac:Downloads test$ plutil -convert xml1 GoogleService-Info.plist
tests-Mac:Downloads test$
```



```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
	<key>AD_UNIT_ID_FOR_BANNER_TEST</key>
	<string>ca-app-pub-3940256099942544/2934735716</string>
	<key>AD_UNIT_ID_FOR_INTERSTITIAL_TEST</key>
	<string>ca-app-pub-3940256099942544/4411468910</string>
	<key>API_KEY</key>
	<string>AIzaSyDEFXDT5mDra5TAPx9n_bkXqNOtb1JN5bw</string>
	<key>BUNDLE_ID</key>
	<string>io.freshworks.GrouseMT</string>
	<key>CLIENT_ID</key>
	<string>366244216739-n61kase73a2ermt83mmjt8i48p6de8dk.apps.googleusercontent.com</string>
	<key>DATABASE_URL</key>
	<string>https://grousemt-f5dd9.firebaseio.com</string>
	<key>GCM_SENDER_ID</key>
	<string>366244216739</string>
	<key>GOOGLE_APP_ID</key>
	<string>1:366244216739:ios:2db549b87d2fe904</string>
```

iOS App Memory Dump

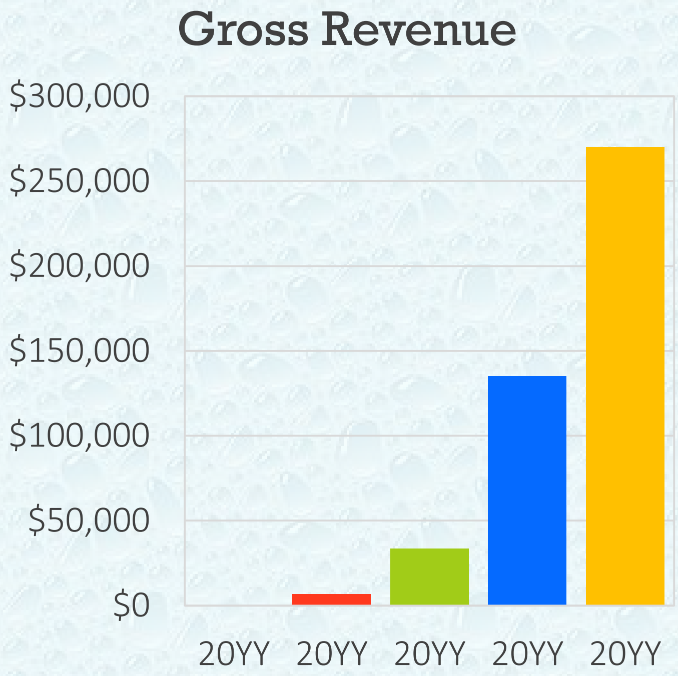
- If an app is heavily obfuscated, just do a memory dump!
  - memscan -p 8650 -d -o rbos.mem
  - or
  - python fridump.py –U appnamehere

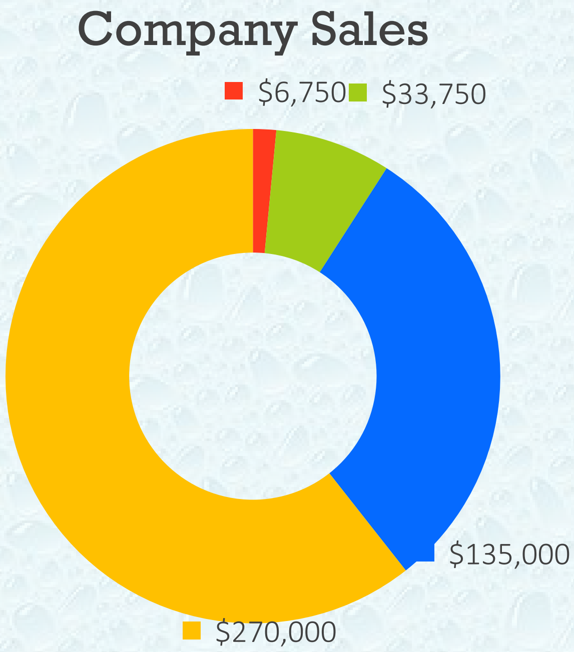


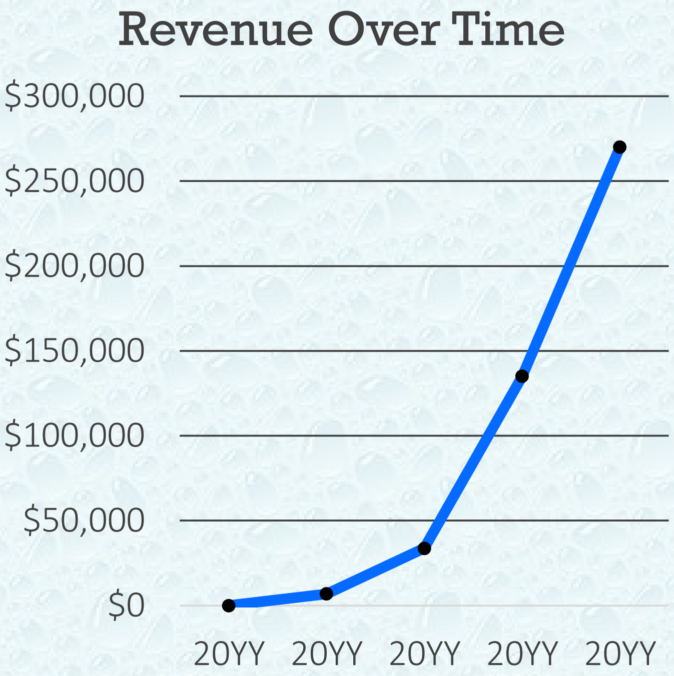
```
tests-iPhone:~ root# memscan -p 23593 -d -o grouseout.mem

Author: Grant Douglas (@Hexploitable)
Blog: https://hexplo.it
Version: 1.4-dirty

Progress: 100%
Finished.
Dump written to: grouseout.mem
tests-iPhone:~ root#
```

Real World Examples

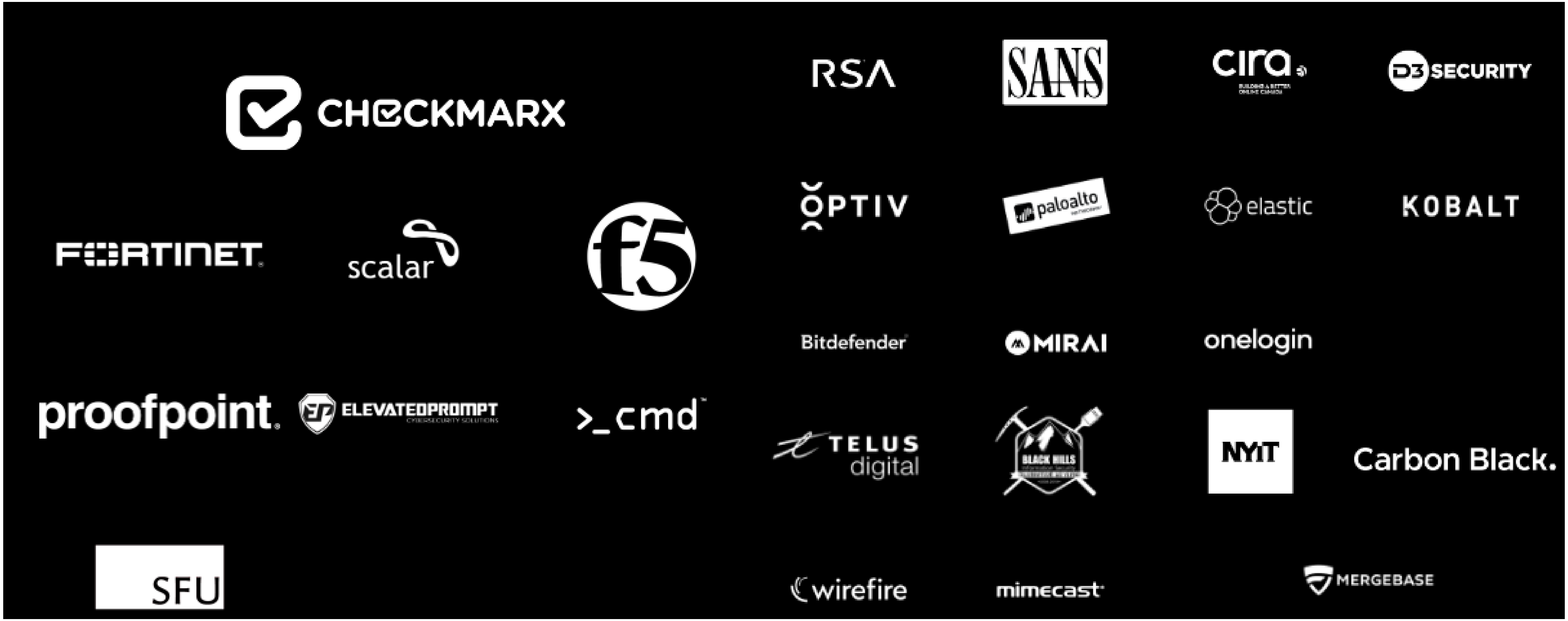
What does this look like for real world apps?


Gross Revenue

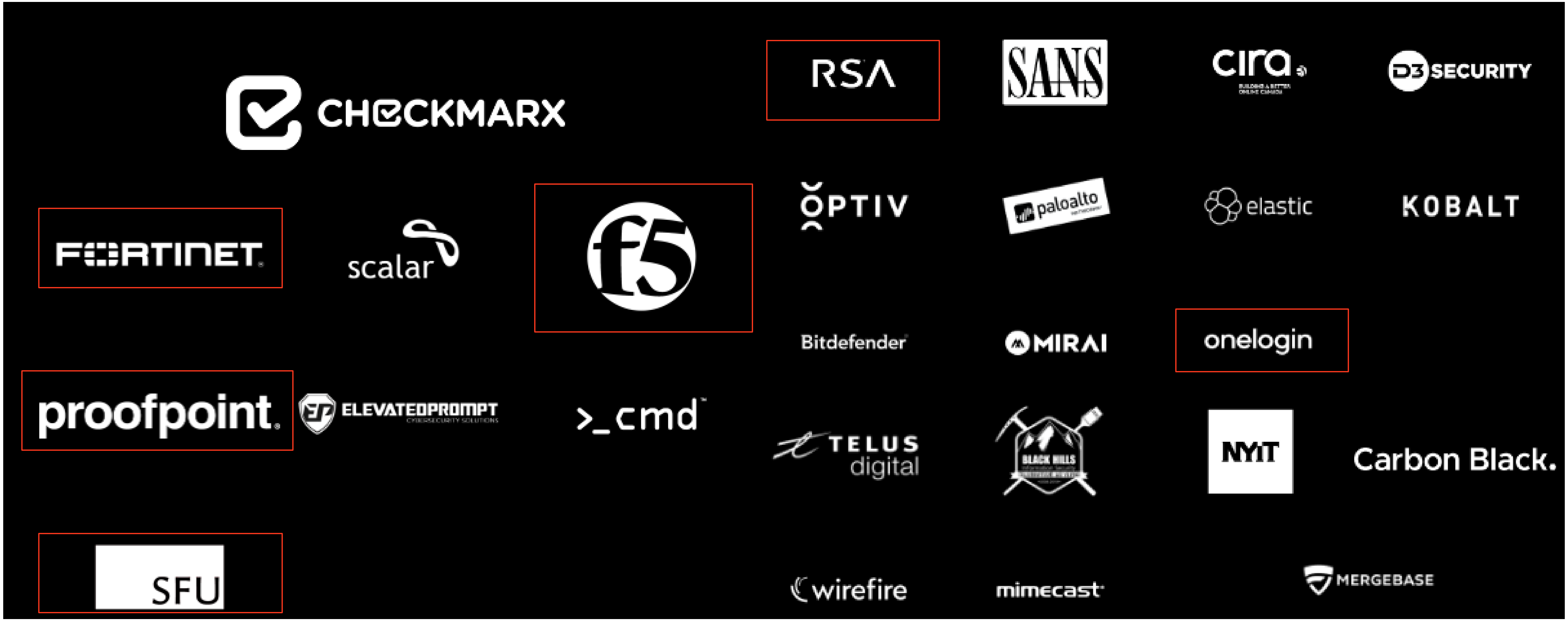

Company Sales


Revenue Over Time

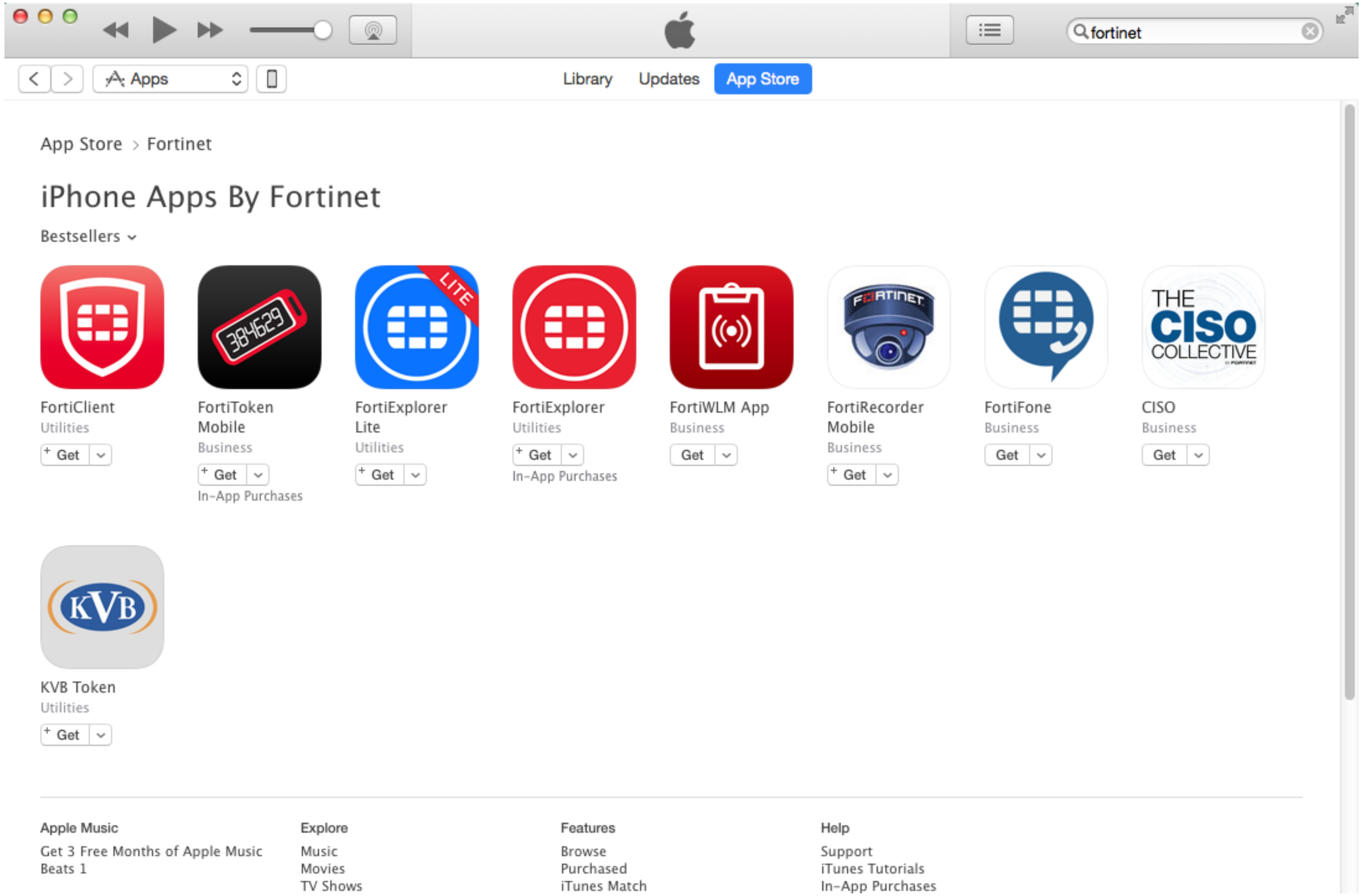
Real World Examples – BSides Sponsors!



Real World Examples – BSides Sponsors!



Fortinet – Too Many Apps



App Store > Fortinet

iPhone Apps By Fortinet

Bestsellers

App	Category	
FortiClient	Utilities	Get
FortiToken Mobile	Business	Get In-App Purchases
FortiExplorer Lite	Utilities	Get
FortiExplorer	Utilities	Get In-App Purchases
FortiWLM App	Business	Get
FortiRecorder Mobile	Business	Get
FortiFone	Business	Get
CISO	Business	Get
KVB Token	Utilities	Get

Apple Music
Get 3 Free Months of Apple Music
Beats 1

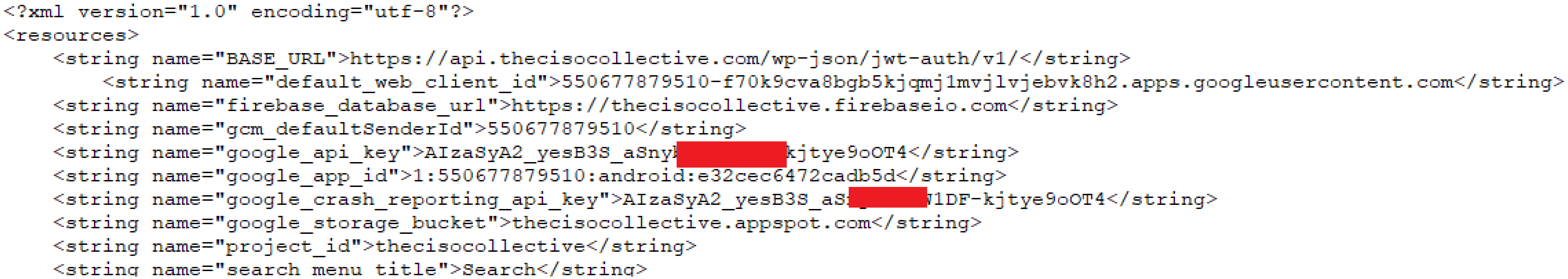
Explore
Music
Movies
TV Shows

Features
Browse
Purchased
iTunes Match

Help
Support
iTunes Tutorials
In-App Purchases

Fortinet – The CISO Collection

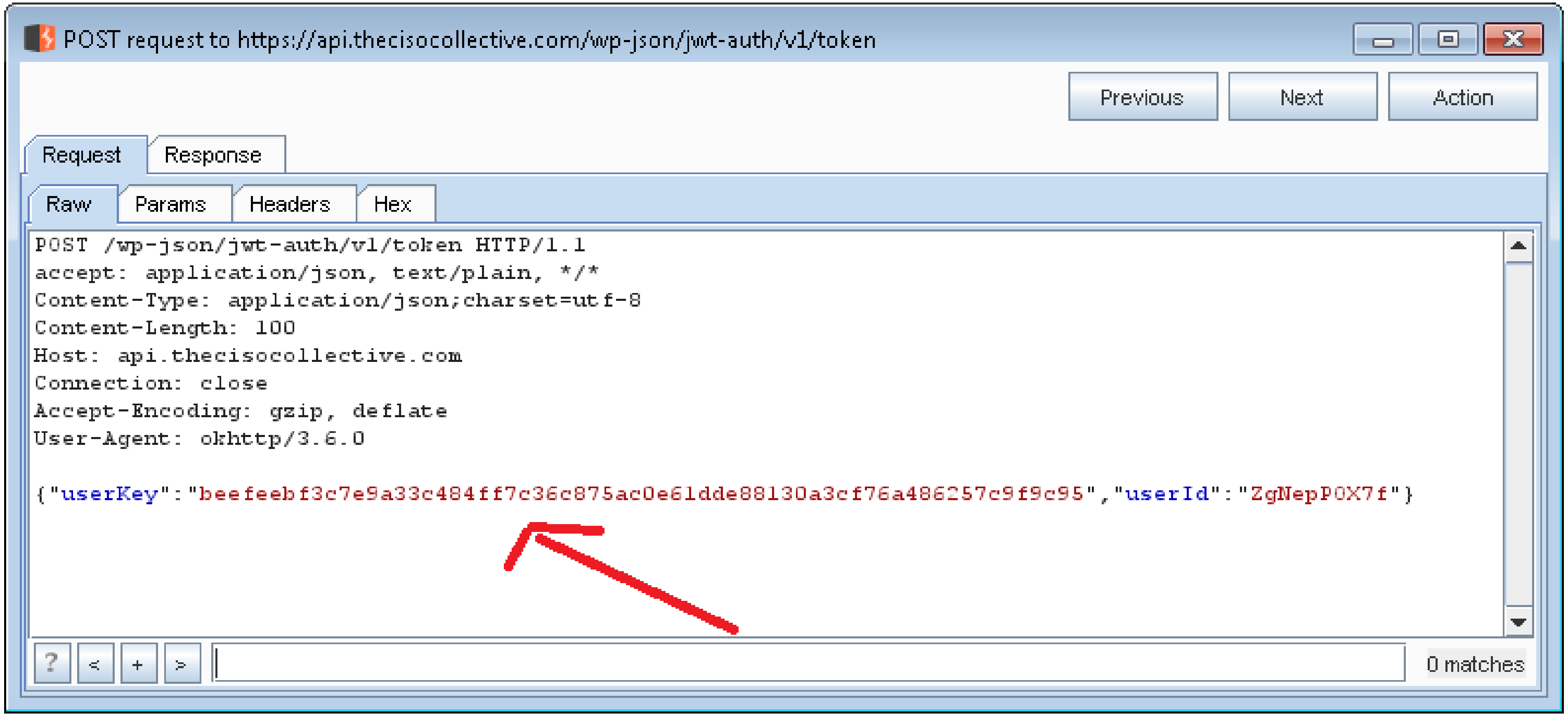
- Resources files:
  - Google API keys – work for some services



```
<?xml version="1.0" encoding="utf-8"?>
<resources>
    <string name="BASE_URL">https://api.thecisocollective.com/wp-json/jwt-auth/v1/</string>
        <string name="default_web_client_id">550677879510-f70k9cva8bgb5kjqmj1mvjlvjebvk8h2.apps.googleusercontent.com</string>
    <string name="firebase_database_url">https://thecisocollective.firebaseio.com</string>
    <string name="gcm_defaultSenderId">550677879510</string>
    <string name="google_api_key">AIzaSyA2_yesB3S_aSny[redacted]kjtye9oOT4</string>
    <string name="google_app_id">1:550677879510:android:e32cec6472cadb5d</string>
    <string name="google_crash_reporting_api_key">AIzaSyA2_yesB3S_aS[redacted]1DF-kjtye9oOT4</string>
    <string name="google_storage_bucket">thecisocollective.appspot.com</string>
    <string name="project_id">thecisocollective</string>
    <string name="search_menu_title">Search</string>
```

Fortinet – The CISO Collection

- Auth Method – Where does the key come from?

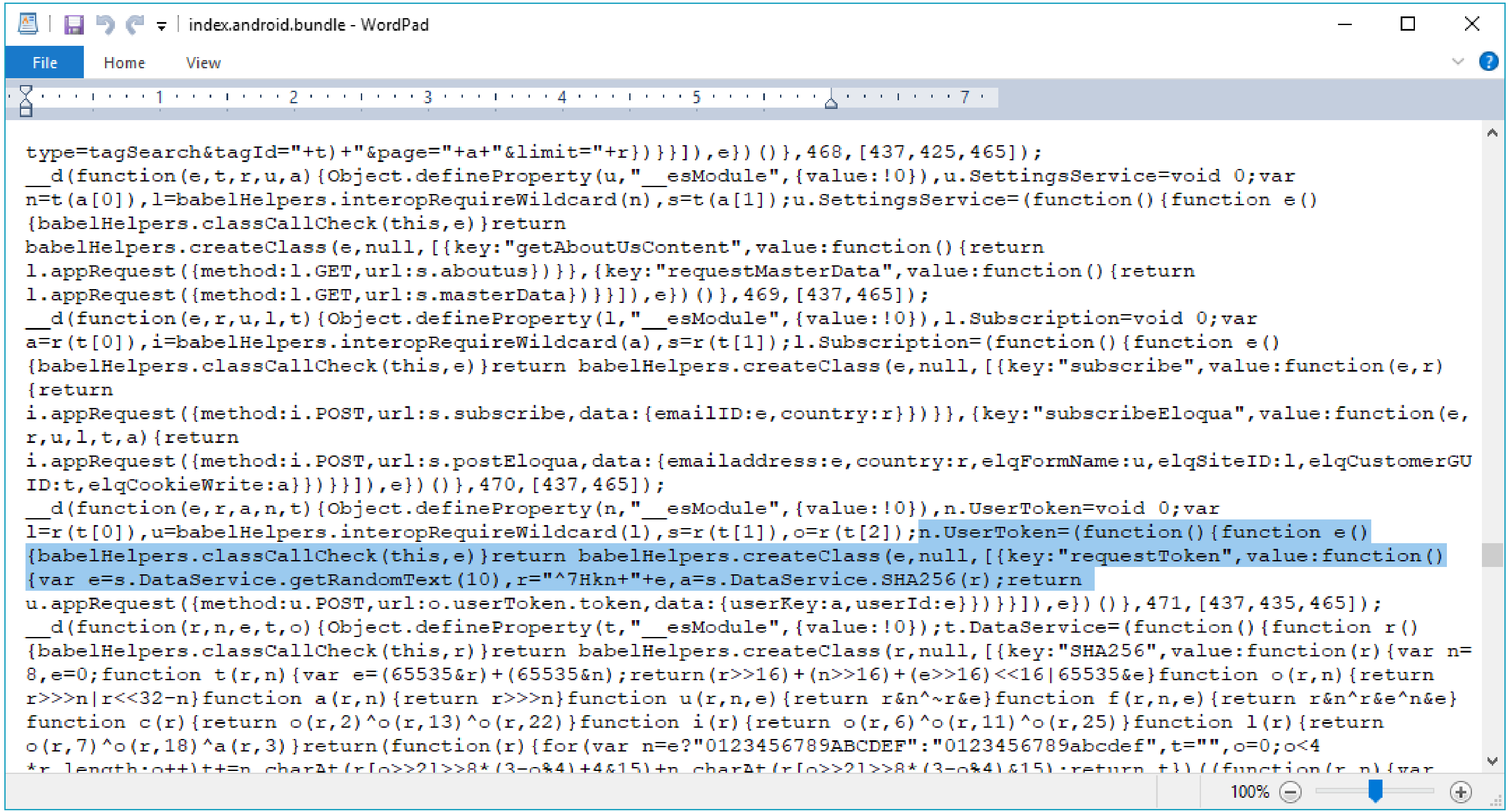

POST request to https://api.thecisocollective.com/wp-json/jwt-auth/v1/token
Previous
Next
Action
Request
Response
Raw
Params
Headers
Hex
?
<
+
>
0 matches

```
POST /wp-json/jwt-auth/v1/token HTTP/1.1
accept: application/json, text/plain, */*
Content-Type: application/json;charset=utf-8
Content-Length: 100
Host: api.thecisocollective.com
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.6.0

{"userKey":"beefeebf3c7e9a33c484ff7c36c875ac0e61dde88130a3cf76a486257c9f9c95","userId":"ZgNepP0X7f"}
```

B|Sides Vancouver

Fortinet – The CISO Collection

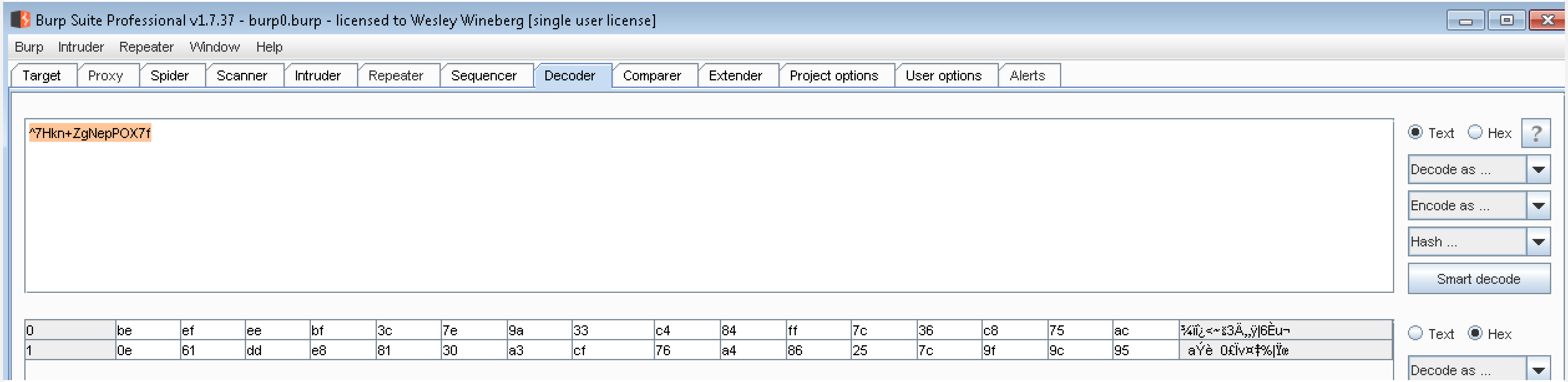
- Auth Method – Resource Files Javascript:



```
type=tagSearch&tagId="+t)+"&page="+a+"&limit="+r})}}]),e})()},468,[437,425,465]);
__d(function(e,t,r,u,a){Object.defineProperty(u,"__esModule",{value:!0}),u.SettingsService=void 0;var
n=t(a[0]),l=babelHelpers.interopRequireWildcard(n),s=t(a[1]);u.SettingsService=(function(){function e()
{babelHelpers.classCallCheck(this,e)}return
babelHelpers.createClass(e,null,[{key:"getAboutUsContent",value:function(){return
l.appRequest({method:l.GET,url:s.aboutus})}},{key:"requestMasterData",value:function(){return
l.appRequest({method:l.GET,url:s.masterData})}}]),e})()},469,[437,465]);
__d(function(e,r,u,l,t){Object.defineProperty(l,"__esModule",{value:!0}),l.Subscription=void 0;var
a=r(t[0]),i=babelHelpers.interopRequireWildcard(a),s=r(t[1]);l.Subscription=(function(){function e()
{babelHelpers.classCallCheck(this,e)}return babelHelpers.createClass(e,null,[{key:"subscribe",value:function(e,r)
{return
i.appRequest({method:i.POST,url:s.subscribe,data:{emailID:e,country:r}})}},{key:"subscribeEloqua",value:function(e,
r,u,l,t,a){return
i.appRequest({method:i.POST,url:s.postEloqua,data:{emailaddress:e,country:r,elqFormName:u,elqSiteID:l,elqCustomerGU
ID:t,elqCookieWrite:a}})}}]),e})()},470,[437,465]);
__d(function(e,r,a,n,t){Object.defineProperty(n,"__esModule",{value:!0}),n.UserToken=void 0;var
l=r(t[0]),u=babelHelpers.interopRequireWildcard(l),s=r(t[1]),o=r(t[2]);n.UserToken=(function(){function e()
{babelHelpers.classCallCheck(this,e)}return babelHelpers.createClass(e,null,[{key:"requestToken",value:function()
{var e=s.DataService.getRandomText(10),r="^7Hkn+"+e,a=s.DataService.SHA256(r);return
u.appRequest({method:u.POST,url:o.userToken.token,data:{userKey:a,userId:e}})}}]),e})()},471,[437,435,465]);
__d(function(r,n,e,t,o){Object.defineProperty(t,"__esModule",{value:!0});t.DataService=(function(){function r()
{babelHelpers.classCallCheck(this,r)}return babelHelpers.createClass(r,null,[{key:"SHA256",value:function(r){var n=
8,e=0;function t(r,n){var e=(65535&r)+(65535&n);return(r>>16)+(n>>16)+(e>>16)<<16|65535&e}function o(r,n){return
r>>>n|r<<32-n}function a(r,n){return r>>>n}function u(r,n,e){return r&n^~r&e}function f(r,n,e){return r&n^r&e^n&e}
function c(r){return o(r,2)^o(r,13)^o(r,22)}function i(r){return o(r,6)^o(r,11)^o(r,25)}function l(r){return
o(r,7)^o(r,18)^a(r,3)}return(function(r){for(var n=e?"0123456789ABCDEF":"0123456789abcdef",t="",o=0;o<4
*r.length;o++)t+=n.charAt(r[o>>2]>>8*(3-o%4)+4&15)+n.charAt(r[o>>2]>>8*(3-o%4)&15);return t}}((function(r,n){var
```

Fortinet – The CISO Collection

- Auth Method – SHA256(Magic + Rand)



● Text ○ Hex

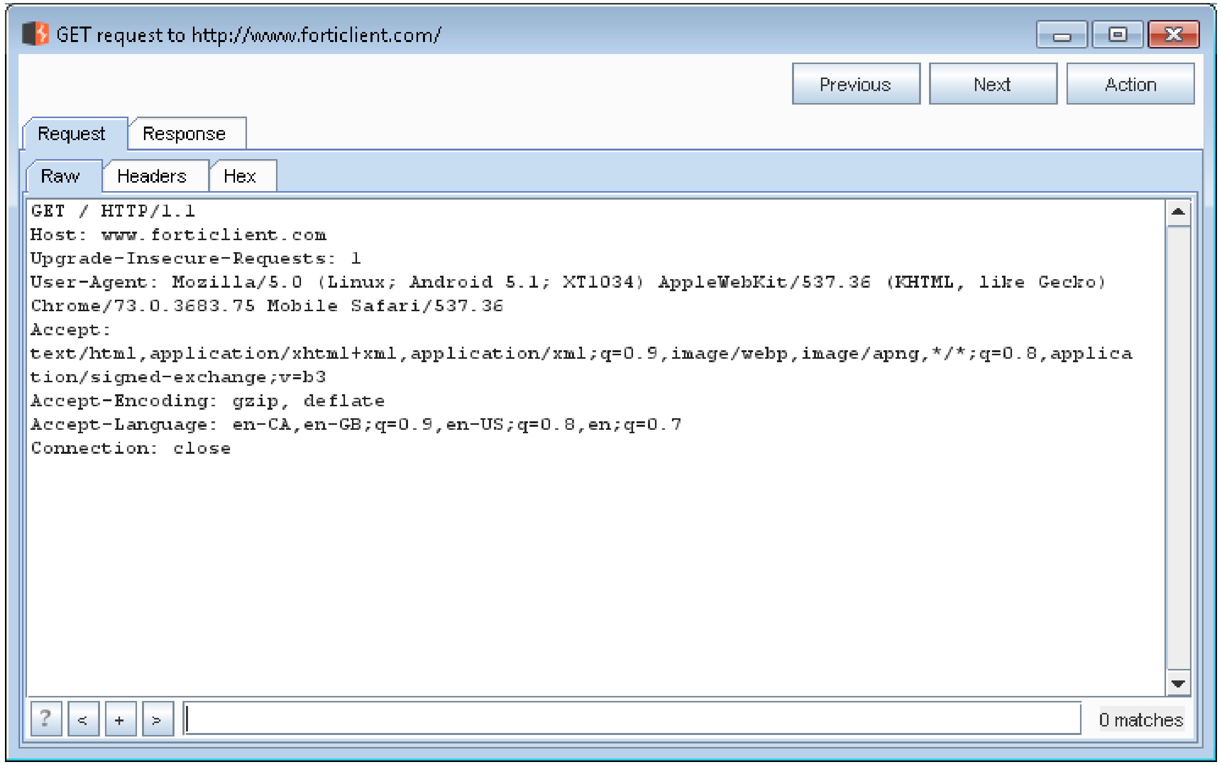
```
^7Hkn+ZgNepPOX7f
```

○ Text ● Hex

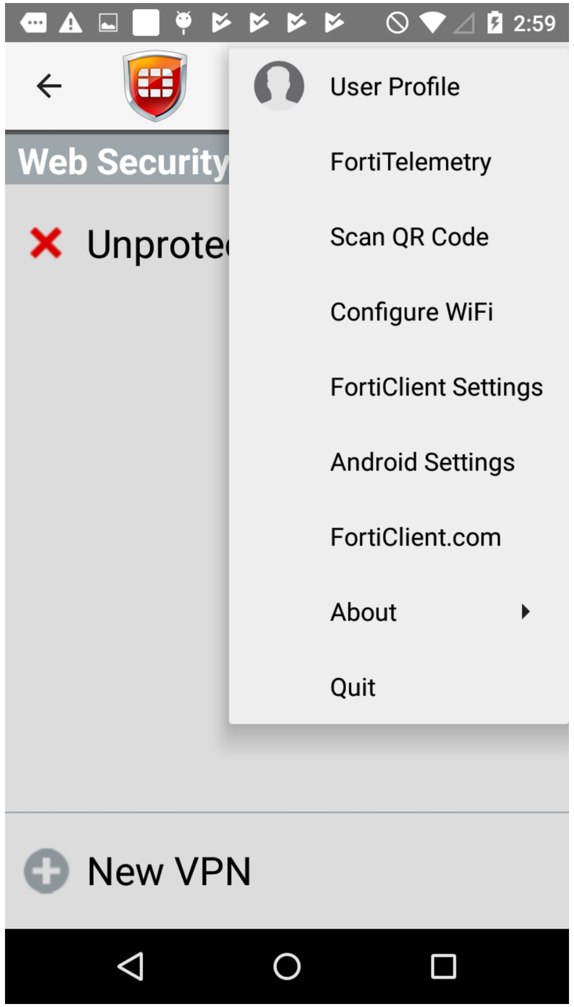
```
0  be  ef  ee  bf  3c  7e  9a  33  c4  84  ff  7c  36  c8  75  ac  ¾ïî¿<~š3Ä„ÿ|6Èu¬
1  0e  61  dd  e8  81  30  a3  cf  76  a4  86  25  7c  9f  9c  95   aÝè 0£Ïv¤‡%|Ÿœ
```

Fortinet – FortiClient VPN

- Missing HTTPS on URL’s
  - Not for auth, but for the main menu link

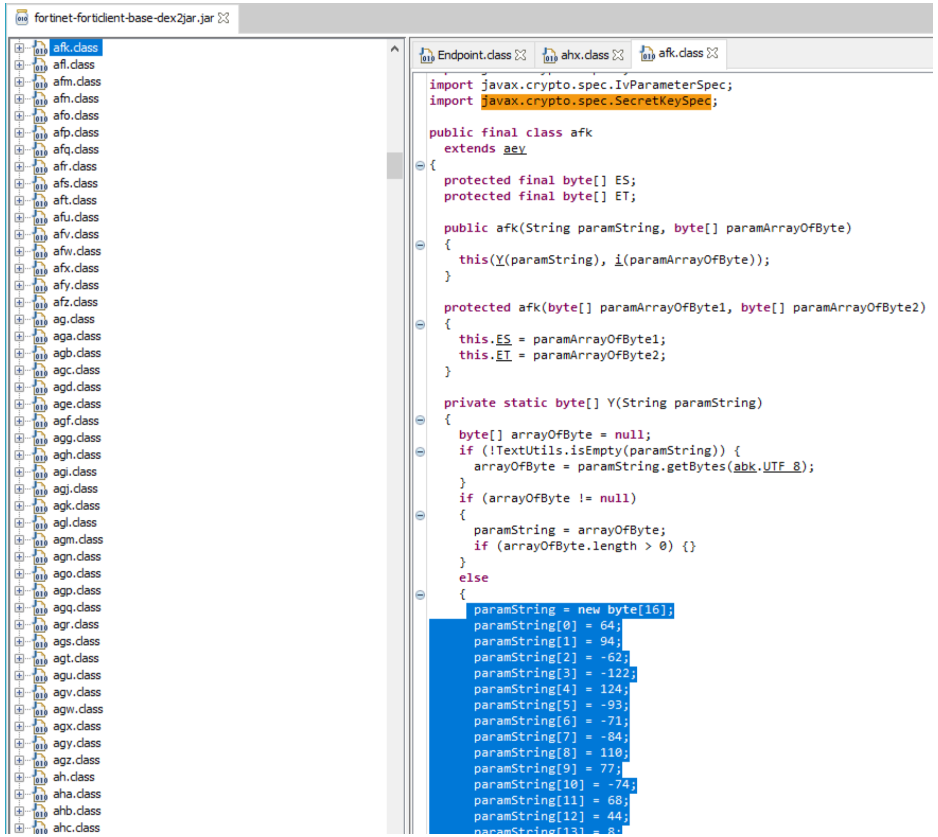


```
GET / HTTP/1.1
Host: www.forticlient.com
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Linux; Android 5.1; XT1034) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/73.0.3683.75 Mobile Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,applica
tion/signed-exchange;v=b3
Accept-Encoding: gzip, deflate
Accept-Language: en-CA,en-GB;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close
```

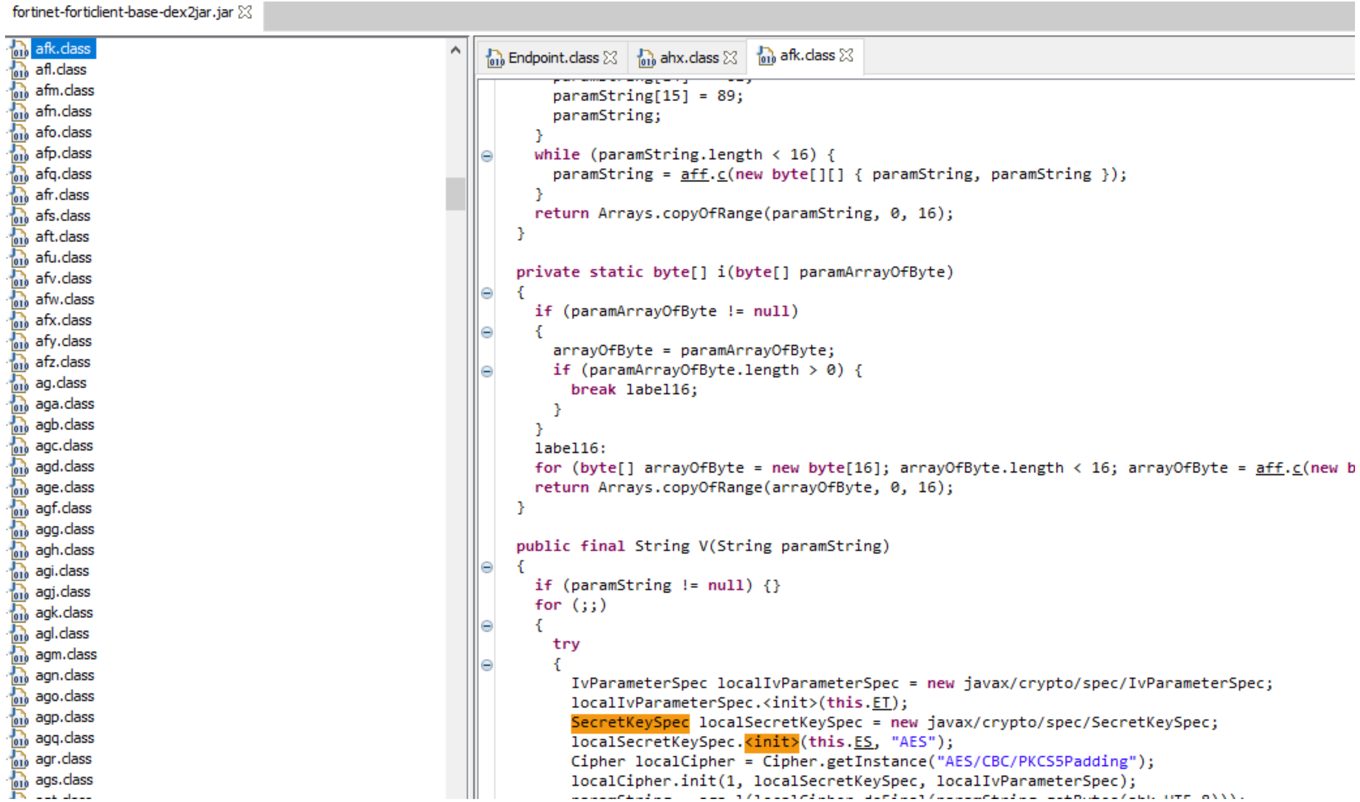


Fortinet – FortiClient

- Hardcoded Encryption Key
  - The purpose of this key was not determined or tested



```java
import javax.crypto.spec.IvParameterSpec;
import javax.crypto.spec.SecretKeySpec;

public final class afk
  extends aey
{
  protected final byte[] ES;
  protected final byte[] ET;

  public afk(String paramString, byte[] paramArrayOfByte)
  {
    this(Y(paramString), i(paramArrayOfByte));
  }

  protected afk(byte[] paramArrayOfByte1, byte[] paramArrayOfByte2)
  {
    this.ES = paramArrayOfByte1;
    this.ET = paramArrayOfByte2;
  }

  private static byte[] Y(String paramString)
  {
    byte[] arrayOfByte = null;
    if (!TextUtils.isEmpty(paramString)) {
      arrayOfByte = paramString.getBytes(abk.UTF_8);
    }
    if (arrayOfByte != null)
    {
      paramString = arrayOfByte;
      if (arrayOfByte.length > 0) {}
    }
    else
    {
      paramString = new byte[16];
      paramString[0] = 64;
      paramString[1] = 94;
      paramString[2] = -62;
      paramString[3] = -122;
      paramString[4] = 124;
      paramString[5] = -93;
      paramString[6] = -71;
      paramString[7] = -84;
      paramString[8] = 110;
      paramString[9] = 77;
      paramString[10] = -74;
      paramString[11] = 68;
      paramString[12] = 44;
      paramString[13] = 8;
```



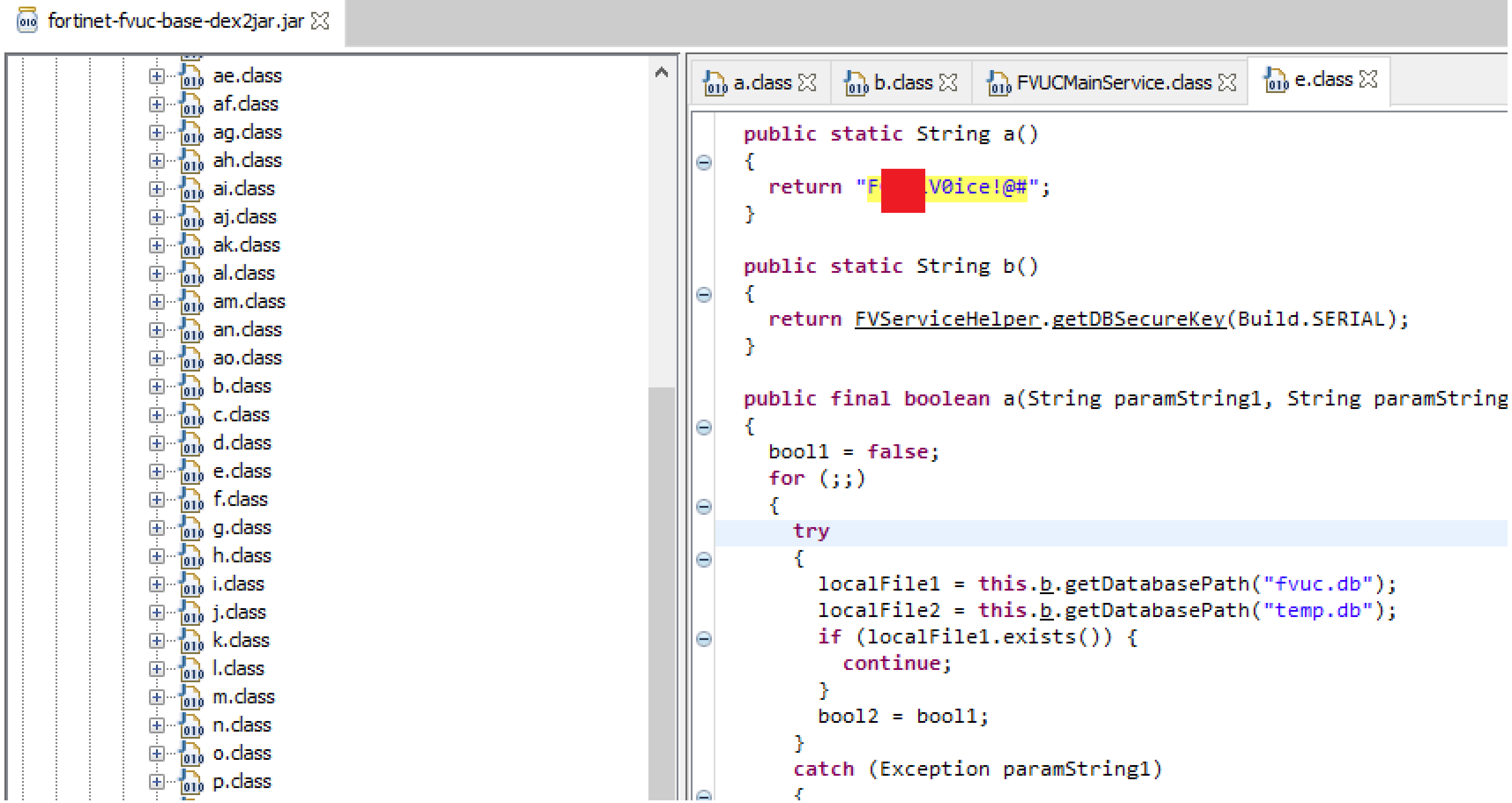
```java
      paramString[15] = 89;
      paramString;
    }
    while (paramString.length < 16) {
      paramString = aff.c(new byte[][] { paramString, paramString });
    }
    return Arrays.copyOfRange(paramString, 0, 16);
  }

  private static byte[] i(byte[] paramArrayOfByte)
  {
    if (paramArrayOfByte != null)
    {
      arrayOfByte = paramArrayOfByte;
      if (paramArrayOfByte.length > 0) {
        break label16;
      }
    }
    label16:
    for (byte[] arrayOfByte = new byte[16]; arrayOfByte.length < 16; arrayOfByte = aff.c(new b
    return Arrays.copyOfRange(arrayOfByte, 0, 16);
  }

  public final String V(String paramString)
  {
    if (paramString != null) {}
    for (;;)
    {
      try
      {
        IvParameterSpec localIvParameterSpec = new javax/crypto/spec/IvParameterSpec;
        localIvParameterSpec.<init>(this.ET);
        SecretKeySpec localSecretKeySpec = new javax/crypto/spec/SecretKeySpec;
        localSecretKeySpec.<init>(this.ES, "AES");
        Cipher localCipher = Cipher.getInstance("AES/CBC/PKCS5Padding");
        localCipher.init(1, localSecretKeySpec, localIvParameterSpec);
```

B|Sides Vancouver

Fortinet – FortiClient

Fortinet – FortiFone

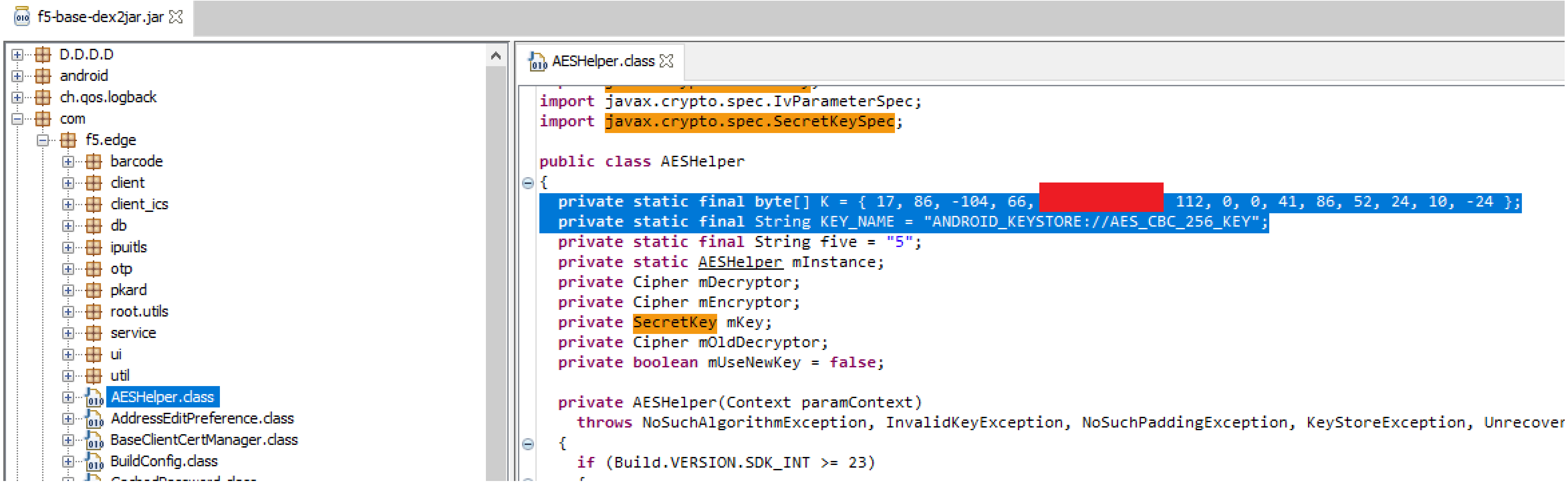
- Hardcoded Database Encryption Secret



```
public static String a()
{
  return "F[redacted]V0ice!@#";
}

public static String b()
{
  return FVServiceHelper.getDBSecureKey(Build.SERIAL);
}

public final boolean a(String paramString1, String paramString
{
  bool1 = false;
  for (;;)
  {
    try
    {
      localFile1 = this.b.getDatabasePath("fvuc.db");
      localFile2 = this.b.getDatabasePath("temp.db");
      if (localFile1.exists()) {
        continue;
      }
      bool2 = bool1;
    }
    catch (Exception paramString1)
    {
```

F5 Networks – F5 Access

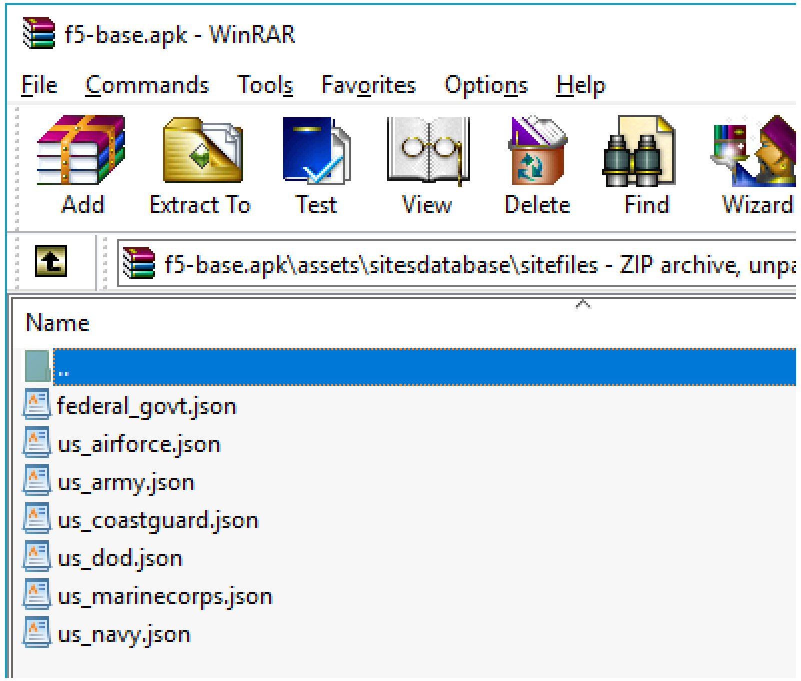
- Hardcoded Encryption Key
  - The purpose of this key was not determined or tested



```
import javax.crypto.spec.IvParameterSpec;
import javax.crypto.spec.SecretKeySpec;

public class AESHelper
{
  private static final byte[] K = { 17, 86, -104, 66, [redacted] 112, 0, 0, 41, 86, 52, 24, 10, -24 };
  private static final String KEY_NAME = "ANDROID_KEYSTORE://AES_CBC_256_KEY";
  private static final String five = "5";
  private static AESHelper mInstance;
  private Cipher mDecryptor;
  private Cipher mEncryptor;
  private SecretKey mKey;
  private Cipher mOldDecryptor;
  private boolean mUseNewKey = false;

  private AESHelper(Context paramContext)
    throws NoSuchAlgorithmException, InvalidKeyException, NoSuchPaddingException, KeyStoreException, Unrecover
  {
    if (Build.VERSION.SDK_INT >= 23)
```

F5 Networks – F5 Access

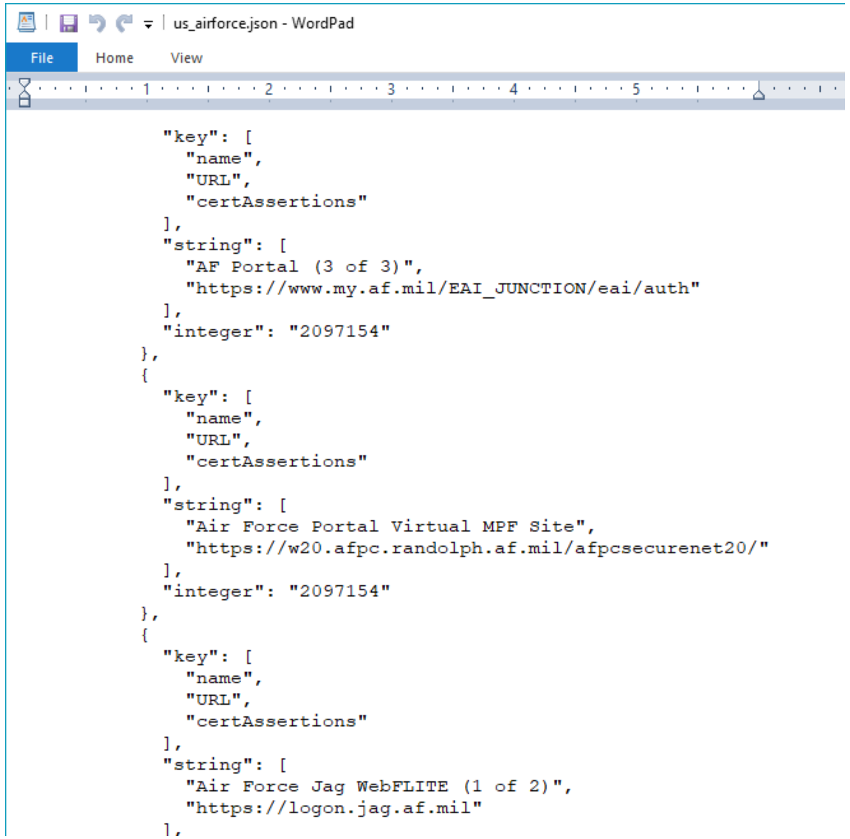
- Resource Files – “Site Database”
  - I can only assume this is supposed to be public 😐



f5-base.apk\assets\sitesdatabase\sitefiles - ZIP archive, unpa

Name

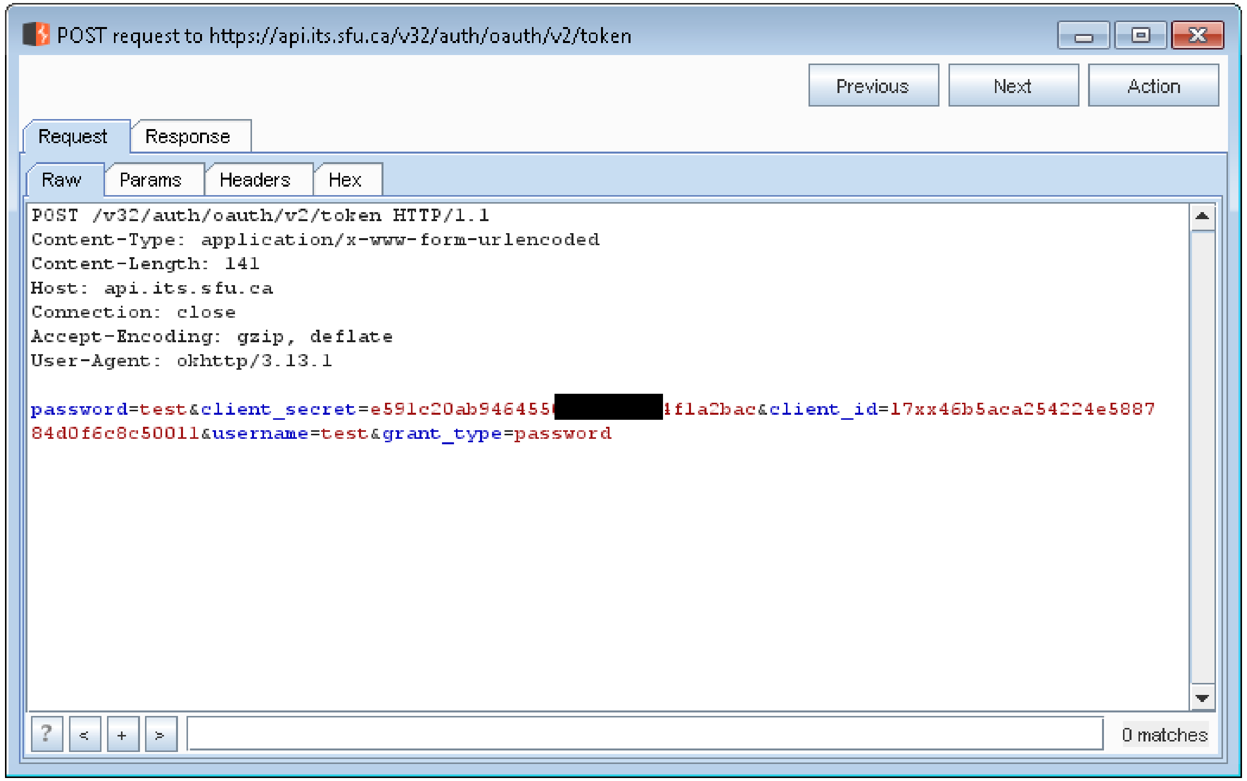
..
federal_govt.json
us_airforce.json
us_army.json
us_coastguard.json
us_dod.json
us_marinecorps.json
us_navy.json



```
      "key": [
        "name",
        "URL",
        "certAssertions"
      ],
      "string": [
        "AF Portal (3 of 3)",
        "https://www.my.af.mil/EAI_JUNCTION/eai/auth"
      ],
      "integer": "2097154"
    },
    {
      "key": [
        "name",
        "URL",
        "certAssertions"
      ],
      "string": [
        "Air Force Portal Virtual MPF Site",
        "https://w20.afpc.randolph.af.mil/afpcsecurenet20/"
      ],
      "integer": "2097154"
    },
    {
      "key": [
        "name",
        "URL",
        "certAssertions"
      ],
      "string": [
        "Air Force Jag WebFLITE (1 of 2)",
        "https://logon.jag.af.mil"
      ],
```

SFU – SFU Snap

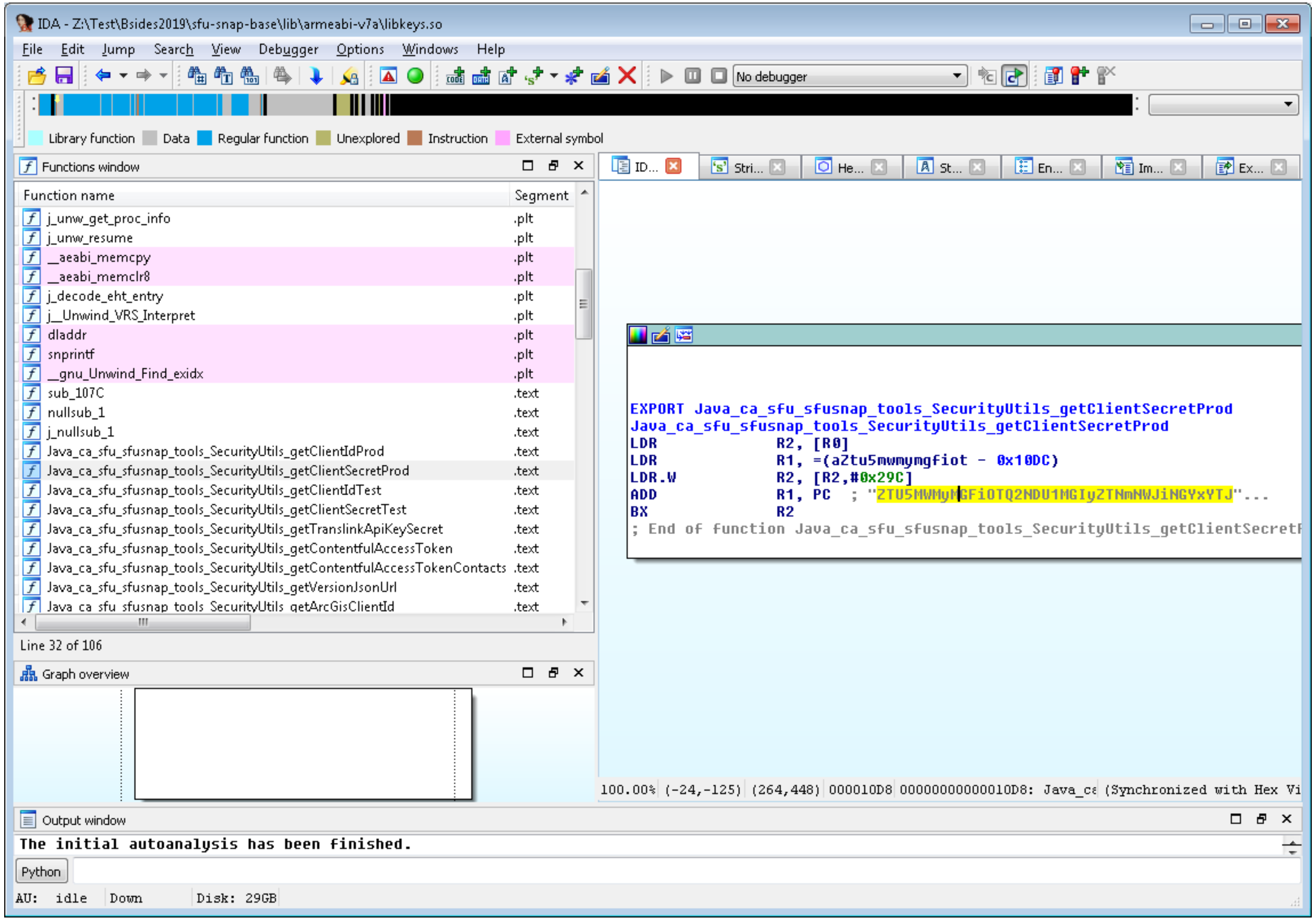
- Hidden API Keys?
  - Network traffic showed various API keys (internal, Google Maps, etc)



```
POST /v32/auth/oauth/v2/token HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Content-Length: 141
Host: api.its.sfu.ca
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.13.1

password=test&client_secret=e591c20ab946455[redacted]fla2bac&client_id=17xx46b5aca254224e5887
84d0f6c8c50011&username=test&grant_type=password
```

SFU – SFU Snap

- Keys moved into compiled “library” file



IDA - Z:\Test\Bsides2019\sfu-snap-base\lib\armeabi-v7a\libkeys.so

Function name	Segment
j_unw_get_proc_info	.plt
j_unw_resume	.plt
__aeabi_memcpy	.plt
__aeabi_memclr8	.plt
j_decode_eht_entry	.plt
j__Unwind_VRS_Interpret	.plt
dladdr	.plt
snprintf	.plt
__gnu_Unwind_Find_exidx	.plt
sub_107C	.text
nullsub_1	.text
j_nullsub_1	.text
Java_ca_sfu_sfusnap_tools_SecurityUtils_getClientIdProd	.text
Java_ca_sfu_sfusnap_tools_SecurityUtils_getClientSecretProd	.text
Java_ca_sfu_sfusnap_tools_SecurityUtils_getClientIdTest	.text
Java_ca_sfu_sfusnap_tools_SecurityUtils_getClientSecretTest	.text
Java_ca_sfu_sfusnap_tools_SecurityUtils_getTranslinkApiKeySecret	.text
Java_ca_sfu_sfusnap_tools_SecurityUtils_getContentfulAccessToken	.text
Java_ca_sfu_sfusnap_tools_SecurityUtils_getContentfulAccessTokenContacts	.text
Java_ca_sfu_sfusnap_tools_SecurityUtils_getVersionJsonUrl	.text
Java_ca_sfu_sfusnap_tools_SecurityUtils_getArcGisClientId	.text

Line 32 of 106

```
EXPORT Java_ca_sfu_sfusnap_tools_SecurityUtils_getClientSecretProd
Java_ca_sfu_sfusnap_tools_SecurityUtils_getClientSecretProd
LDR             R2, [R0]
LDR             R1, =(aZtu5mwmymgfiot - 0x10DC)
LDR.W           R2, [R2,#0x29C]
ADD             R1, PC  ; "ZTU5MWMyMGFiOTQ2NDU1MGIyZTNmNWJiNGYxYTJ"...
BX              R2
; End of function Java_ca_sfu_sfusnap_tools_SecurityUtils_getClientSecretP
```

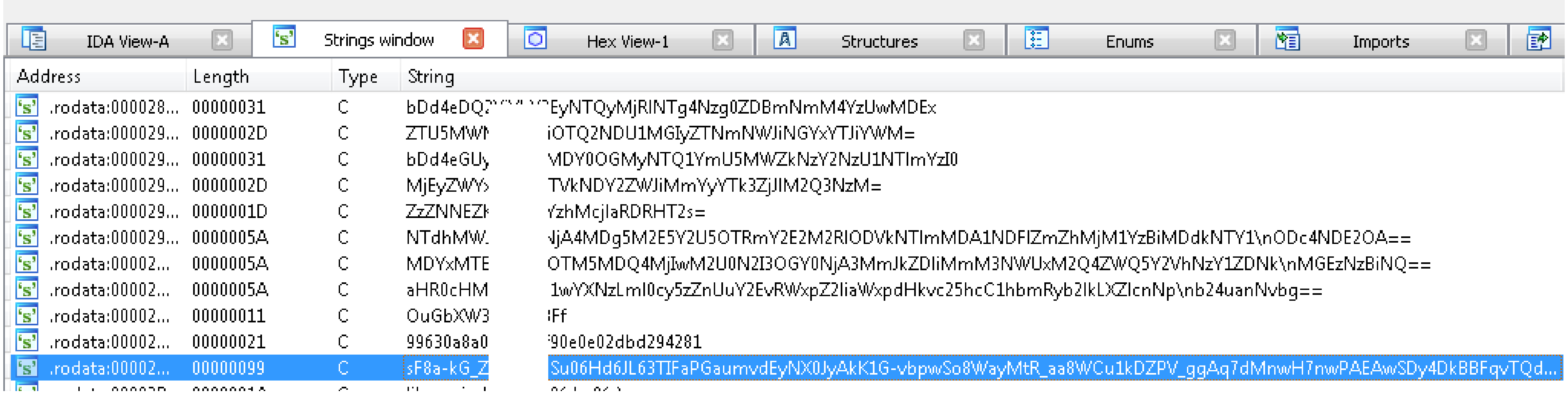
```
100.00% (-24,-125) (264,448) 000010D8 00000000000010D8: Java_ca (Synchronized with Hex Vi
```

```
The initial autoanalysis has been finished.
```

```
AU:  idle  Down      Disk: 29GB
```

SFU – SFU Snap

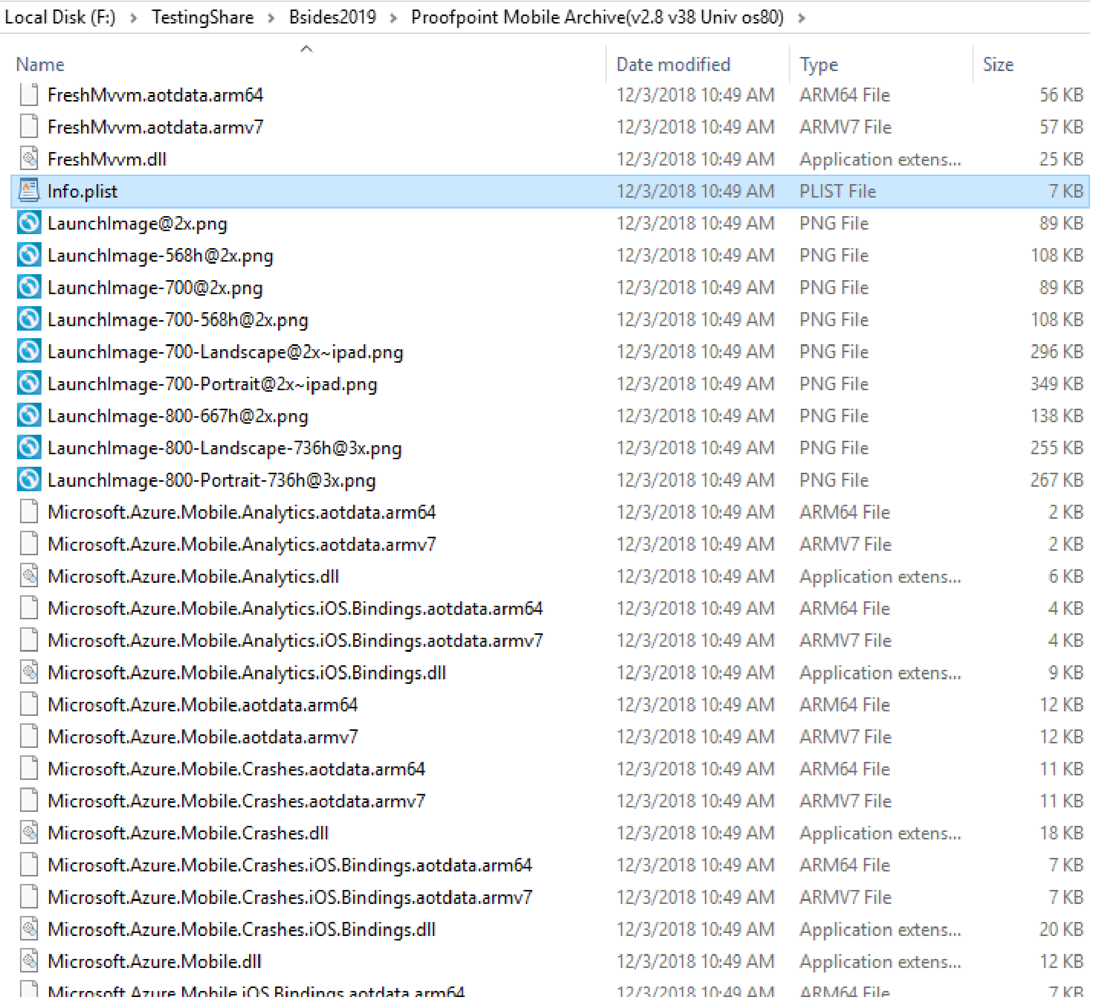
- Keys are Base64 encoded



Address	Length	Type	String
.rodata:000028...	00000031	C	bDd4eDQ2 EyNTQyMjRINTg4Nzg0ZDBmNmM4YzUwMDEx
.rodata:000029...	0000002D	C	ZTU5MWN iOTQ2NDU1MGIyZTNmNWJiNGYxYTJiYWM=
.rodata:000029...	00000031	C	bDd4eGUy MDY0OGMyNTQ1YmU5MWZkNzY2NzU1NTImYzI0
.rodata:000029...	0000002D	C	MjEyZWY TVkNDY2ZWJiMmYyYTk3ZjJIM2Q3NzM=
.rodata:000029...	0000001D	C	ZzZNNEZk YzhMcjlaRDRHT2s=
.rodata:000029...	0000005A	C	NTdhMW NjA4MDg5M2E5Y2U5OTRmY2E2M2RIODVkNTImMDA1NDFIZmZhMjM1YzBiMDdkNTY1\nODc4NDE2OA==
.rodata:00002...	0000005A	C	MDYxMTE OTM5MDQ4MjIwM2U0N2I3OGY0NjA3MmJkZDliMmM3NWUxM2Q4ZWQ5Y2VhNzY1ZDNk\nMGEzNzBiNQ==
.rodata:00002...	0000005A	C	aHR0cHM 1wYXNzLmI0cy5zZnUuY2EvRWxpZ2liaWxpdHkvc25hcC1hbmRyb2lkLXZlcnNp\nb24uanNvbg==
.rodata:00002...	00000011	C	OuGbXW3 Ff
.rodata:00002...	00000021	C	99630a8a0 90e0e02dbd294281
.rodata:00002...	00000099	C	sF8a-kG_Z Su06Hd6JL63TIFaPGaumvdEyNX0JyAkK1G-vbpwSo8WayMtR_aa8WCu1kDZPV_ggAq7dMnwH7nwPAEAwSDy4DkBBFqvTQd...

Proofpoint – Proofpoint Archive

- Not a vuln in any way but…
- Windows DLL’s on iOS and Android, who could’ve seen that coming?!



Local Disk (F:) › TestingShare › Bsides2019 › Proofpoint Mobile Archive(v2.8 v38 Univ os80) ›

Name	Date modified	Type	Size
FreshMvvm.aotdata.arm64	12/3/2018 10:49 AM	ARM64 File	56 KB
FreshMvvm.aotdata.armv7	12/3/2018 10:49 AM	ARMV7 File	57 KB
FreshMvvm.dll	12/3/2018 10:49 AM	Application extens...	25 KB
Info.plist	12/3/2018 10:49 AM	PLIST File	7 KB
LaunchImage@2x.png	12/3/2018 10:49 AM	PNG File	89 KB
LaunchImage-568h@2x.png	12/3/2018 10:49 AM	PNG File	108 KB
LaunchImage-700@2x.png	12/3/2018 10:49 AM	PNG File	89 KB
LaunchImage-700-568h@2x.png	12/3/2018 10:49 AM	PNG File	108 KB
LaunchImage-700-Landscape@2x~ipad.png	12/3/2018 10:49 AM	PNG File	296 KB
LaunchImage-700-Portrait@2x~ipad.png	12/3/2018 10:49 AM	PNG File	349 KB
LaunchImage-800-667h@2x.png	12/3/2018 10:49 AM	PNG File	138 KB
LaunchImage-800-Landscape-736h@3x.png	12/3/2018 10:49 AM	PNG File	255 KB
LaunchImage-800-Portrait-736h@3x.png	12/3/2018 10:49 AM	PNG File	267 KB
Microsoft.Azure.Mobile.Analytics.aotdata.arm64	12/3/2018 10:49 AM	ARM64 File	2 KB
Microsoft.Azure.Mobile.Analytics.aotdata.armv7	12/3/2018 10:49 AM	ARMV7 File	2 KB
Microsoft.Azure.Mobile.Analytics.dll	12/3/2018 10:49 AM	Application extens...	6 KB
Microsoft.Azure.Mobile.Analytics.iOS.Bindings.aotdata.arm64	12/3/2018 10:49 AM	ARM64 File	4 KB
Microsoft.Azure.Mobile.Analytics.iOS.Bindings.aotdata.armv7	12/3/2018 10:49 AM	ARMV7 File	4 KB
Microsoft.Azure.Mobile.Analytics.iOS.Bindings.dll	12/3/2018 10:49 AM	Application extens...	9 KB
Microsoft.Azure.Mobile.aotdata.arm64	12/3/2018 10:49 AM	ARM64 File	12 KB
Microsoft.Azure.Mobile.aotdata.armv7	12/3/2018 10:49 AM	ARMV7 File	12 KB
Microsoft.Azure.Mobile.Crashes.aotdata.arm64	12/3/2018 10:49 AM	ARM64 File	11 KB
Microsoft.Azure.Mobile.Crashes.aotdata.armv7	12/3/2018 10:49 AM	ARMV7 File	11 KB
Microsoft.Azure.Mobile.Crashes.dll	12/3/2018 10:49 AM	Application extens...	18 KB
Microsoft.Azure.Mobile.Crashes.iOS.Bindings.aotdata.arm64	12/3/2018 10:49 AM	ARM64 File	7 KB
Microsoft.Azure.Mobile.Crashes.iOS.Bindings.aotdata.armv7	12/3/2018 10:49 AM	ARMV7 File	7 KB
Microsoft.Azure.Mobile.Crashes.iOS.Bindings.dll	12/3/2018 10:49 AM	Application extens...	20 KB
Microsoft.Azure.Mobile.dll	12/3/2018 10:49 AM	Application extens...	12 KB
Microsoft.Azure.Mobile.iOS.Bindings.aotdata.arm64	12/3/2018 10:49 AM	ARM64 File	7 KB

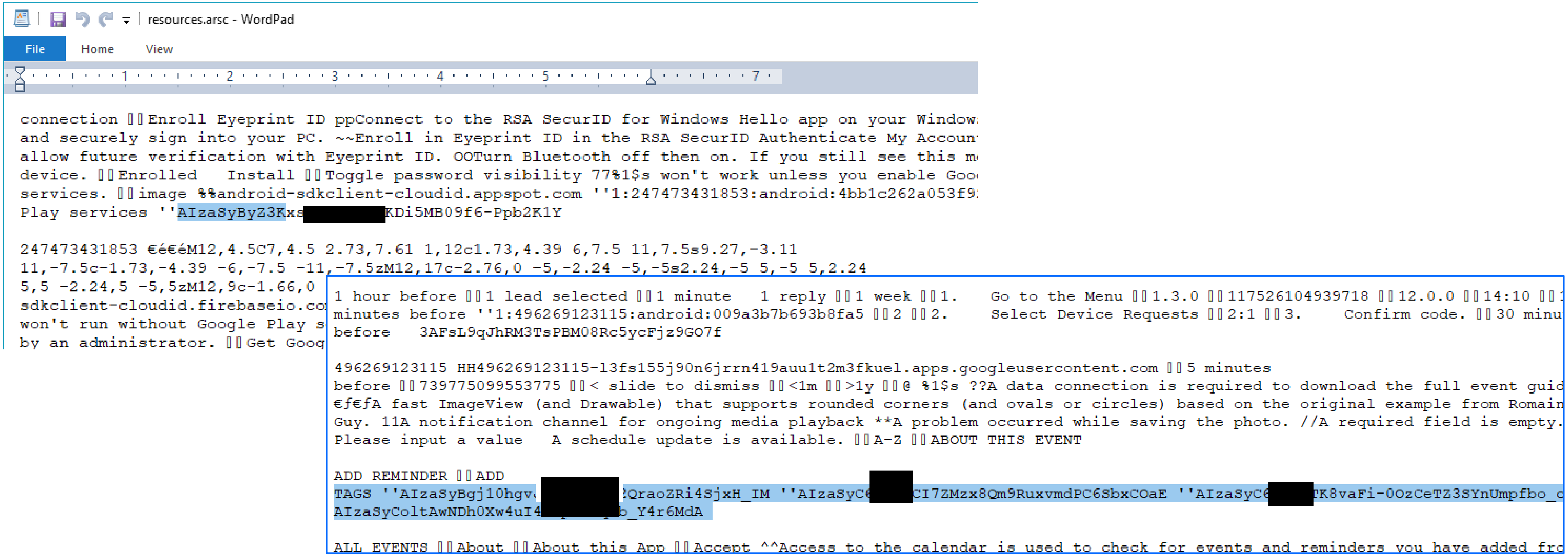
OneLogin – OneLogin Mobile

- REDACTED, sorry

[redacted]

RSA

- Various unrestricted Google API keys

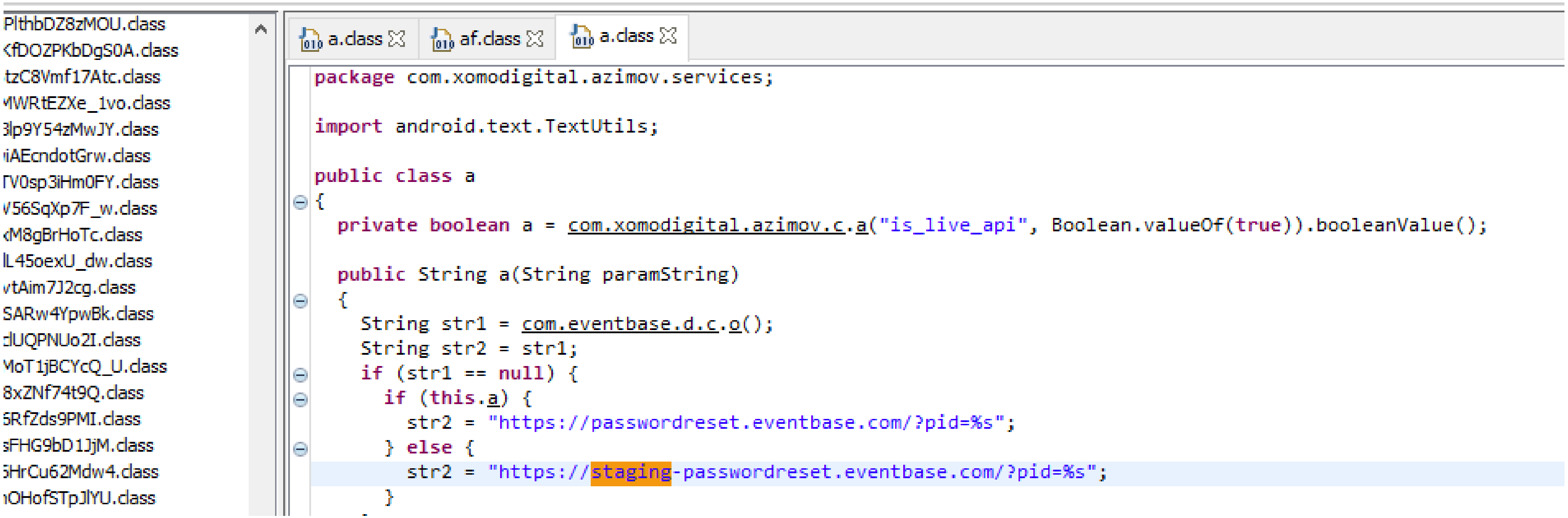


```
connection ▯▯Enroll Eyeprint ID ppConnect to the RSA SecurID for Windows Hello app on your Window
and securely sign into your PC. ~~Enroll in Eyeprint ID in the RSA SecurID Authenticate My Accoun
allow future verification with Eyeprint ID. OOTurn Bluetooth off then on. If you still see this m
device. ▯▯Enrolled   Install ▯▯Toggle password visibility 77%1$s won't work unless you enable Goo
services. ▯▯image %%android-sdkclient-cloudid.appspot.com ''1:247473431853:android:4bb1c262a053f9
Play services ''AIzaSyByZ3Kxs[redacted]KDi5MB09f6-Ppb2K1Y

247473431853 €é€éM12,4.5C7,4.5 2.73,7.61 1,12c1.73,4.39 6,7.5 11,7.5s9.27,-3.11
11,-7.5c-1.73,-4.39 -6,-7.5 -11,-7.5zM12,17c-2.76,0 -5,-2.24 -5,-5s2.24,-5 5,-5 5,2.24
5,5 -2.24,5 -5,5zM12,9c-1.66,0
sdkclient-cloudid.firebaseio.co
won't run without Google Play s
by an administrator. ▯▯Get Goog
```

```
1 hour before ▯▯1 lead selected ▯▯1 minute   1 reply ▯▯1 week ▯▯1.   Go to the Menu ▯▯1.3.0 ▯▯117526104939718 ▯▯12.0.0 ▯▯14:10 ▯▯
minutes before ''1:496269123115:android:009a3b7b693b8fa5 ▯▯2 ▯▯2.   Select Device Requests ▯▯2:1 ▯▯3.   Confirm code. ▯▯30 minu
before   3AFsL9qJhRM3TsPBM08Rc5ycFjz9GO7f

496269123115 HH496269123115-13fs155j90n6jrrn419auu1t2m3fkuel.apps.googleusercontent.com ▯▯5 minutes
before ▯▯739775099553775 ▯▯< slide to dismiss ▯▯<1m ▯▯>1y ▯▯@ %1$s ??A data connection is required to download the full event guid
€f€fA fast ImageView (and Drawable) that supports rounded corners (and ovals or circles) based on the original example from Romain
Guy. 11A notification channel for ongoing media playback **A problem occurred while saving the photo. //A required field is empty.
Please input a value   A schedule update is available. ▯▯A-Z ▯▯ABOUT THIS EVENT

ADD REMINDER ▯▯ADD
TAGS ''AIzaSyBgj10hgv[redacted]QraoZRi4SjxH_IM ''AIzaSyC6[redacted]CI7ZMzx8Qm9RuxvmdPC6SbxCOaE ''AIzaSyC6[redacted]TK8vaFi-0OzCeTZ3SYnUmpfbo_
AIzaSyColtAwNDh0Xw4uI4[redacted]b_Y4r6MdA

ALL EVENTS ▯▯About ▯▯About this App ▯▯Accept ^^Access to the calendar is used to check for events and reminders you have added fro
```

RSA – RSA Conference App

- Reference to test environment (not a vuln necessarily)



```
PlthbDZ8zMOU.class
KfDOZPKbDgS0A.class
tzC8Vmf17Atc.class
MWRtEZXe_1vo.class
3lp9Y54zMwJY.class
iAEcndotGrw.class
TV0sp3iHm0FY.class
V56SqXp7F_w.class
kM8gBrHoTc.class
lL45oexU_dw.class
vtAim7J2cg.class
SARw4YpwBk.class
dUQPNUo2I.class
MoT1jBCYcQ_U.class
8xZNf74t9Q.class
5RfZds9PMI.class
sFHG9bD1JjM.class
5HrCu62Mdw4.class
nOHofSTpJlYU.class
```

```java
package com.xomodigital.azimov.services;

import android.text.TextUtils;

public class a
{
  private boolean a = com.xomodigital.azimov.c.a("is_live_api", Boolean.valueOf(true)).booleanValue();

  public String a(String paramString)
  {
    String str1 = com.eventbase.d.c.o();
    String str2 = str1;
    if (str1 == null) {
      if (this.a) {
        str2 = "https://passwordreset.eventbase.com/?pid=%s";
      } else {
        str2 = "https://staging-passwordreset.eventbase.com/?pid=%s";
      }
```

So Many Apps, So Little Time

- Mobile apps don’t need to be mystery
- Open the app store, take a look at some more!

Thank You

Wesley Wineberg

wesley@exfiltrated.com
www.exfiltrated.com/research.php

Image Credits

http://voxvalley.com/images/lawful-interception.png

https://blog.cloudflare.com/content/images/2017/08/Artboard-9.png

https://cdn-images-1.medium.com/max/800/0*kLiTfW5SWQSoySkP.

https://res.cloudinary.com/peerlyst/image/upload/c_limit,dpr_auto,f_auto,fl_lossy,h_252,q_auto,w_421/v1/post-attachments/1542793833824_pzaqqh

https://avatars2.githubusercontent.com/u/6716868?s=400&v=4

https://lc-gold-cdn.xitu.io/9fd48dc18360b9e212ab.jpg

https://www.google.com/url?sa=i&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwj8t7-mz4fhAhVLsFQKHZoRAtMQjRx6BAgBEAU&url=http%3A%2F%2Fwww.commodon.com%2Fthreat%2Fthreat-sub7.htm&psig=AOvVaw07LJeqE5EyG3_mPNm8SOfi&ust=1552858579112648

http://diysolarpanelsv.com/images/live-clipart-for-android-47.jpg

https://denisbloch.com/wp-content/uploads/2018/01/kristin-simmons-holy-profits-american-excess.jpg