3 GREAT WAYS TO LEARN YOUR LOCATION.
3 GREAT WAYS TO LEARN YOUR LOCATION.

NOW WITHOUT PERMISSIONS!
API response:

```json
{
    "gsm": false,
    "wifi": true,
    "success": true,
    "cdma": false,
    "results": [
        {
            "trilat": 37.86978912,
            "trilong": -122.27120972,
            "ssid": "ICSI"
        }
    ]
}
```
One way is to just ask directly!
Step 1: open socket
Step 2: connect to 192.168.0.1:1900
Step 3: ask for its MAC address

get /igd.xml
Step 4: learn router MAC address

...<UDN>uuid:12345678−9abc−def0−1234−18d6c78c8ce3</UDN>...
Another is to find it written down somewhere.
.prologue
.line 183
const-string v0, "android.permission.ACCESS_WIFI_STATE"

invoke-virtual {p0, v0}. Lcom/openx/view/plugplay/sdk/deviceData/managers/DeviceInfoImpl->isPermissionGranted(Ljava/lang/String;)Z
move-result v0
if-eqz v0, :cond_0
.prologue
.line 183
const-string v0, "android.permission.ACCESS_WIFI_STATE"

invoke-virtual {p0, v0}, Lcom/openx/view/plugplay/sdk/deviceData/managers/DeviceInfoImpl;->isPermissionGranted(Ljava/lang/String;)Z
move-result v0
if-eqz v0, :cond_0

.line 185
iget-object v0, p0, Lcom/openx/view/plugplay/sdk/deviceData/managers/DeviceInfoImpl;->mWifiManager:Landroid/net/wifi/WifiManager;
if-eqz v0, :cond_0

iget-object v0, p0, Lcom/openx/view/plugplay/sdk/deviceData/managers/DeviceInfoImpl;->mWifiManager:Landroid/net/wifi/WifiManager;
 invoke-virtual {v0}, Landroid/net/wifi/WifiManager;->getConnectionInfo()Landroid/net/wifi/WifiInfo;
move-result-object v0
if-eqz v0, :cond_0
.prologue
.const-string v0, "android.permission.ACCESS_WIFI_STATE"

invoke-virtual {p0, v0}, Lcom/openx/view/plugplay/sdk/deviceData/managers/DeviceInfoImpl:-isPermissionGranted(Ljava/lang/String;)Z
move-result v0
if-eqz v0, :cond_0

.ine 185
iget-object v0, p0, Lcom/openx/view/plugplay/sdk/deviceData/managers/DeviceInfoImpl:-mWifiManager:android/net/wifi/WifiManager;
if-eqz v0, :cond_0
iget-object v0, p0, Lcom/openx/view/plugplay/sdk/deviceData/managers/DeviceInfoImpl:-mWifiManager:android/net/wifi/WifiManager;
invoke-virtual {v0}, Landroid/net/wifi/WifiManager:-getConnectionInfo()Landroid/net/wifi/WifiInfo;
move-result-object v0
if-eqz v0, :cond_0

.ine 187
iget-object v0, p0, Lcom/openx/view/plugplay/sdk/deviceData/managers/DeviceInfoImpl:-mWifiManager:android/net/wifi/WifiManager;
invoke-virtual {v0}, Landroid/net/wifi/WifiManager:-getConnectionInfo()Landroid/net/wifi/WifiInfo;
move-result-object v0
invoke-virtual {v0}, Landroid/net/wifi/WifiInfo:-getMacAddress()Ljava/lang/String;
move-result-object v0

.ine 188
if-eqz v0, :cond_0

.ine 199
:goto_0
return-object v0
invoke-virtual {p0, v0}. Lcom/openx/view/plugplay/sdk/deviceData/managers/DeviceInfoImpl:-isPermissionGranted(Ljava/lang/String;)Z
move-result v0
if-eqz v0. :cond_0

.invoke-virtual {v0}. Landroid/net/wifi/WifiManager:-getConnectionInfo()Landroid/net/wifi/WifiInfo;
move-result-object v0
if-eqz v0. :cond_0

.invoke-virtual {v0}. Landroid/net/wifi/WifiInfo:-getMacAddress()Ljava/lang/String;
move-result-object v0

if-eqz v0. :cond_0

:goto_0
return-object v0

:cond_0
invoke-direct {p0}. Lcom/openx/view/plugplay/sdk/deviceData/managers/DeviceInfoImpl:-getDeviceMacAddressesFromArp()Ljava/util/ArrayList;
move-result-object v0
new-instance v3, Ljava/util/ArrayList:

invoke-direct {v3}, Ljava/util/ArrayList;-><init>()V

const/4 v2, 0x0

new-instance v1, Ljava/io/BufferedReader;

new-instance v0, Ljava/io/FileReader;

const-string v4, "/proc/net/arp"

invoke-direct {v0, v4}, Ljava/io/FileReader;-><init>(Ljava/lang/String;)V

invoke-direct {v1, v0}, Ljava/io/BufferedReader;-><init>(Ljava/io/Reader;)V

:try_end_0
.catch Ljava/io/FileNotFoundException: {:try_start_0 .. :try_end_0} :catch_7
.catch Ljava/io/IOException: {:try_start_0 .. :try_end_0} :catch_3
.catchall {:try_start_0 .. :try_end_0} :catchall_0

:cond_0
:goto_0
:try_start_1
invoke-virtual {v1}, Ljava/io/BufferedReader;->readLine()Ljava/lang/String:

move-result-object v0
```
$ cat /proc/net/arp
IP address     HW type  Flags  HW address     Mask  Device
192.168.0.1     0x1     0x2     18:d6:c7:8c:8c:e3  *      wlan0
```
Sept 6th submitted bug report 2018
Sept 6th submitted bug report
bug bounty received Oct 2nd 2018
Sept 6th submitted bug report bug bounty received
Oct 2nd
Nov 1st removed OpenX 90% of affected apps
2018 removed OpenX
90% of affected apps
2018
Sept 6th submitted bug report
Oct 2nd received bug bounty
Nov 1st removed OpenX 90% of affected apps
March 8th "bountycon" skitrip to lake tahoe
You can also find the location written down too!
.method public getLatitude()F
    .locals 1

    .line 149
    iget v0, p0, Lcom/shutterfly/android/commons/apc/service/v1/model/PhotoMetadata$Location:->latitude:F

    return v0
.end method

.method public getLongitude()F
    .locals 1

    .line 141
    iget v0, p0, Lcom/shutterfly/android/commons/apc/service/v1/model/PhotoMetadata$Location:->longitude:F

    return v0
.end method
If you want to know more, like how we even found these, come to my talk in the morning: in track 1—Mobile Security
Apps using Side and Covert Channels
Posted by Joel Reardon on June 1, 2019

The 2019 USENIX Security Symposium includes our study on the use of side and covert channels by apps in order to circumvent the permission system. In addition to our paper, we have a series of blog posts to explain our main findings. In this post we provide the name, version, and MD5 hash of the... Continue reading→

Why do you even need the IMEI?
Posted by Joel Reardon on April 26, 2019

The International Mobile Equipment Identity, or IMEI, is a special number that is tied to every unique mobile phone. It is used whenever the phone is registered on a mobile network. It can also be used to blacklist a phone off of the network, which happens, for example, when it is reported as stolen. Blacklisting... Continue reading→

Ad IDs Behaving Badly
Posted by Serge Egelman on February 14, 2019