



Technische
Universität
Braunschweig

IAS | INSTITUTE FOR
APPLICATION
SECURITY



iOS watching you: Automated analysis of “zero-touch” privacy violations under iOS

Benjamin Altpeter, 2021-08-03

Quick recap and introduction

- Previous research [[Altpeter, Wessels](#)] on Android to answer how common tracking in apps is actually.
- Built framework to automatically install and run apps for 60 seconds and collect their network traffic.
- Thus, looked at tracking that happens without consent (as there was no user input).
- Analysis of 1,296 apps showed that automated data collection in the background is common in Android apps. Apps commonly transmit device details, sensor data, events, or even the geolocation and which data is entered in the app; often to third-parties.
- On iOS (often hailed as more privacy-friendly), research into privacy violations by apps is scarce and outdated.
- I have thus repeated our previous research for iOS using a very similar approach to allow for comparisons.

Quick GDPR recap

- GDPR concerns itself with *processing of personal data* (explicitly broad terms)
- Legal basis (Art. 6(1) GDPR) needed to process personal data
 - in practice, processing in apps is usually based on consent or legitimate interest
 - but supervisory authorities say that consent is necessary for tracking in most cases
 - Recital 32 mandates conditions for consent: “Consent should be given by a clear affirmative act [...]. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. [...]”
- Schrems II ruling by the ECJ (July 2020) makes it almost impossible to legally transfer data to the US
 - thus: tracking with US providers most likely illegal, especially without consent

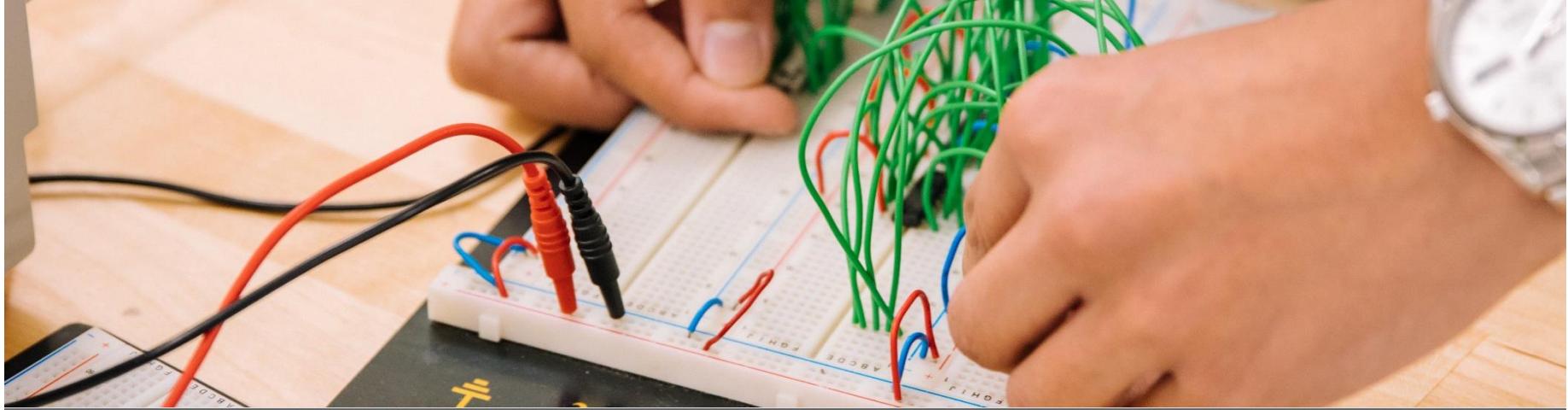


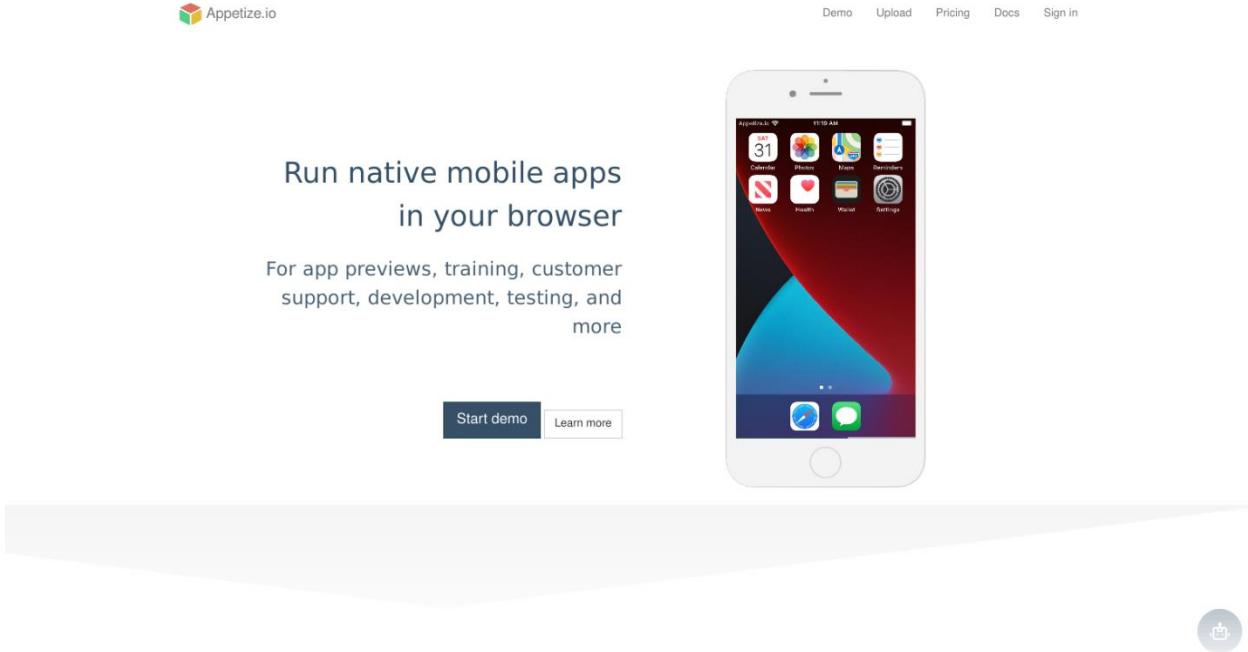
Image: Jeswin Thomas (Unsplash license)

Method

Is emulation an option?



Maybe commercial providers can help?



The screenshot shows the Appetize.io homepage. At the top left is the logo 'Appetize.io' with a small cube icon. Top right navigation links include 'Demo', 'Upload', 'Pricing', 'Docs', and 'Sign in'. The main content area features the text 'Run native mobile apps in your browser' and 'For app previews, training, customer support, development, testing, and more'. Below this are two buttons: 'Start demo' (dark blue) and 'Learn more' (light gray). To the right is a large image of a white iPhone displaying its home screen with various app icons like Calendar, Photos, Maps, and Settings.

<https://appetize.io/>

Maybe commercial providers can help?

RUN THAT APP

Start Team Pricing Upload Press Features Contact

Go ahead, click and play



The screenshot shows an iPhone displaying the 'About' section of the iOS Settings app. The screen includes the following information:

Setting	Value
Photos	10
Applications	7
Capacity	465 GB
Available	43.7 GB
Version	8.4 (12H141)
Model	N/A
Serial Number	C07PK0TJG1J1
Legal	>
Trust Store	2015051300
Learn more about trusted certificates	

Go Fullscreen iOS

<https://www.runthatapp.com/demo/>

Maybe commercial providers can help?

The screenshot shows the Appetize.io Docs website with the following structure:

- Header:** Appetize.io Docs, Home, Demo, Upload, Pricing, Search...
- Left Sidebar (CORE FEATURES):**
 - Getting started
 - Uploading apps** (highlighted)
 - Playback options
 - Embed your app
 - App permissions
 - Cross-document messages
 - Custom launch pages
- Content Area:**

Uploading apps

You may upload apps directly via your web browser at <https://appetize.io/upload>, or you may upload programmatically via our [API](#).

We also have many 3rd party integrations with tools such as [fastlane](#), [Bitrise](#), and [Expo](#).

iOS **Android**

For iOS, upload a `.zip` or `.tar.gz` file containing your compressed `.app` bundle.

Your `.app` bundle must represent a iOS Simulator build of your app. A simulator build can be run in the iOS Simulator via Xcode. This is different than a IPA file, which is compiled for ARM architecture CPUs and can only be run on physical iOS devices.

One way to get the iOS Simulator build is to run your app in an iOS Simulator, and then to find the file that is automatically generated. After running in the iOS Simulator via Xcode, look in:

```
~/Library/Developer/Xcode/DerivedData/<project-name>/Build/Products/Debug-iphonesimulator/
```

You may also generate the iOS Simulator build of your app by building it directly via the command line using xcdebuild.

If you have a `.xcodeproj` file, you may run:

<https://docs.appetize.io/core-features/uploading-apps>

Maybe commercial providers can help?

No file selected.

Fill in Email for your receipt URL. E-mail:

Its Easy. How to find your iOS simulator release build of your .app :

Apple has it hidden away in SOME xCode versons. But first, ensure you are targeting the build to the Simulator, not hardware, we only accept simulator builds at this time.

For speed, verify your scheme is set to "release" instead of the slower running "debug" build mode.

In Xcode there is a command shortcut key, but the menu location is :

"Product -> Scheme -> Edit Scheme... -> Run YourAppName -> Info Tab -> Build configuration"

1> Change your Build Configuration from "debug" to "release" for extra speed, if not already set.

2> Build your app, then test it once in the simulator.

3> Locate your .app and its optional debug symbol file (dSYM), if you want detailed crash information from us. Switch to the finder and go to the root level of where all xCode builds are stored. Use the Finder command "Go To Folder (Shift Command G)". The path to go to first is "~/Library/Developer/Xcode/DerivedData/" without the quotes.

Your projects builds are typically inside "~/Library/Developer/Xcode/DerivedData/". A typical path to a release build looks like this "/Users/me/Library/Developer/Xcode/DerivedData/MyCoolApp-cgcerwyxpmeekwdqrgobouaoiccx/Build/Products/Release-iphonesimulator/MyCoolApp.app"

4> Zip together the .app and the optional dSYM into one zip, by putting them into a single temp directory, or not.

5> Go to the page you are probably already reading now to send the zip file to us: [my.RunThatApp.com/upload.html](http://upload.runthatapp.com/upload.html)

6> Enter your email address you want the link sent to, that can be used on other web sites in an iFrame, or sent in a email, or used as a link.

7> Hit the Submit button. Eventually an email will be sent regarding the status of the upload.

Done

If you get tired of the steps above, a simple script can be added to the final build phase, to automate sending, with permission, on every build. (soon)

<http://upload.runthatapp.com/upload.html>

What about Corellium?

The screenshot shows a news article from The Register. The header includes a 'SIGN IN' button, a logo for 'The Register', a search bar, and a menu icon. Below the header, a red banner displays the text '(* VIRTUALIZATION *)'. The main title of the article is 'Judge rules Corellium iOS research app 'fair use' in slap to Apple'. A subtitle below it reads 'But DMCA claims about circumventing security protections still stand'. The author is listed as 'Matthew Hughes' with a timestamp of 'Mon 4 Jan 2021 // 16:03 UTC'. The article content discusses a court ruling where a judge rejected Apple's claim against Corellium for circumventing iOS security protections, finding it to be legally permissible under fair use exemptions. It also notes that Corellium is a specialist research tool for security researchers.

Judge rules Corellium iOS research app 'fair use' in slap to Apple

But DMCA claims about circumventing security protections still stand

Matthew Hughes Mon 4 Jan 2021 // 16:03 UTC

A judge has ruled against Apple in its [copyright battle with Corellium](#), a Florida startup that offers virtualized iOS instances for security researchers.

In a surprise ruling in the US district court for southern Florida last week [[PDF](#)], Judge Rodney Smith rejected Apple's claim that the core Corellium product infringed upon Apple's intellectual property, finding it to be legally permissible under fair use exemptions.

This was, in part, because Corellium isn't a direct competitor to iOS aimed at the same consumer and business users, but rather a specialist research tool aimed at a vastly smaller audience - a virtual iPhone on a desktop. It doesn't, for example, offer access to the App Store, allow the user to make calls, or take pictures. The variant of iOS virtualized is stripped back and surrounded by a suite of tools that wouldn't be of interest to the average bod – such as the ability to modify the kernel, see and halt processes, and capture live snapshots of an instance.

"The evidence establishes that the Corellium Product is not merely a repackaged version of iOS – this time in a virtual environment as opposed to an iPhone," wrote Smith. "Rather, Corellium makes several changes to iOS and incorporates its own code to create a product that serves a transformative purpose."

https://www.theregister.com/2021/01/04/corellium_ios_ruling/

What about Corellium?



TECHNOLOGY PRODUCTS ↓ ABOUT US BLOG CONTACT LOGIN

Security Research

Physical devices are limited. Your security research shouldn't be. Corellium's revolutionary cloud-based research environment combines high-fidelity virtual devices with powerful integrated tools, giving you unparalleled insight, efficiency, and control to accelerate your mobile security work.

[Start Your Free Trial](#)

[Plans and Pricing →](#)



SPEED

Set up in no time. Spin up devices on demand and integrate seamlessly with your existing workflows.

<https://corellium.com/security-research>

I'm in!

The screenshot shows an email client interface with the following details:

- From:** Corellium Support <support@corellium.com>
- Subject:** You're In!
- To:** acc-corellium@benji.pw
- Date:** Mon, 03 May 2021 01:57:14 +0000
- Message ID:** <2be7a222-f53-4d5a-90ad-ed6275bf4ca7@m1asv.net>
- DKIM:** Valid (Signed by corellium.com)
- Return-Path:** <pm_bounces@pm-bounces.corellium.com>

The message body contains the following text:

Are You Ready to Take Your Security Research to the Next Level?

Thank you for your request to try CORSEC. Corellium's advanced mobile security research environment. We're excited to let you know that your request has been approved. Just click the link below to finish creating your account and unlock your new development experience.

[Click here to access your free trial!](#)

Once you finish creating your account, you will have one hour of free device credit, which you can use any time in the next seven days. After the free trial period, you'll have the option to sign up for a monthly or usage-based subscription.

If you need any help along the way, please visit our [knowledge base](#), join us on [Slack](#), or send us an [email](#).

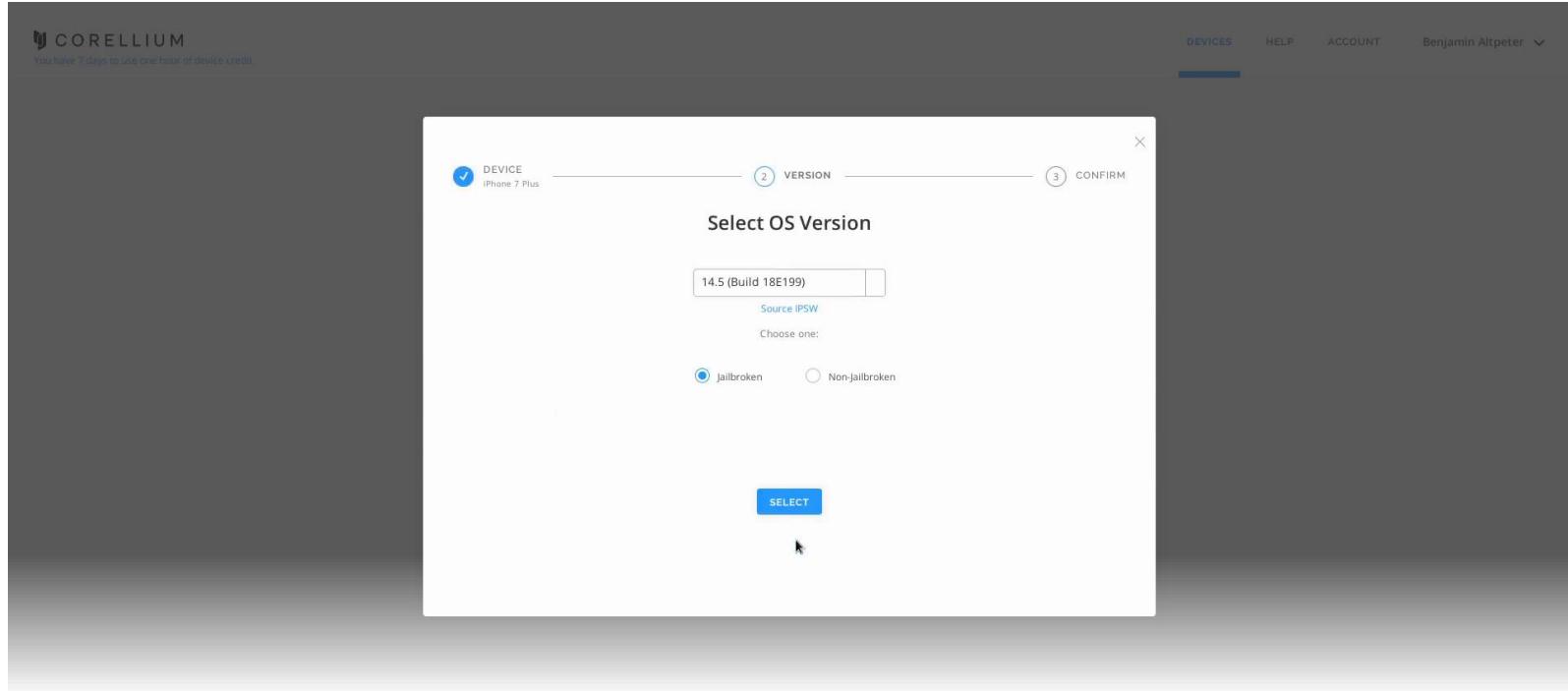
Happy virtualizing!

I'm in!

The screenshot shows the Corellium web application interface. At the top, there is a header with the Corellium logo, a message about device credit, and navigation links for Devices, Help, Account, and a user profile for Benjamin Altpeter. Below the header, a modal window titled "Select Device" is open. The modal has a progress bar at the top with three steps: 1. DEVICE, 2. VERSION, and 3. CONFIRM. Step 1 is highlighted. The main area of the modal displays five device options: iPhone SE, iPod touch 6, iPad mini 4 (Wi-Fi only), iPhone 7, and iPhone 7 Plus. Each device is shown with a small image and a brief description indicating it takes 2 CPU cores. To the right of the devices is a search bar and a "NEXT" button. The background of the page is dark, and the overall interface is clean and modern.

<https://app.corellium.com/>

I'm in!



<https://app.corellium.com/>

I'm in!

The screenshot shows the Corellium web interface with a device named "test" (iPhone 7 Plus | 14.5 | 18E199 | ✓ Jailbroken). The main area displays the iOS home screen. On the left, a sidebar lists physical buttons: Home, Side Button, Vol. Up, Vol. Down, and Keyboard. The top navigation bar includes links for DEVICES, HELP, ACCOUNT, and a user account dropdown for Benjamin Altpeter. Below the device name, there are control icons for volume, brightness, and power.

CONNECT (highlighted) | FILES | APPS | NETWORK | CORETRACE | SETTINGS | CONSOLE | [\(i\)](#)

① Set Up VPN
To use adb, ssh, gdb, or serial console, you must first connect to VPN. Download the VPN configuration file to connect.
[Download OVPN FILE](#)

② Connect To Device
WiFi
In Settings app, click "Wi-Fi" and select the "Corellium" network. Enter any 8-digit password.
USB
Download USBFlux to use your virtual device over USB with programs like Xcode or libimobiledevice.
[Download USBFLUX FOR MAC](#)
Linux source

Advanced Options
To connect to an SSH daemon running on the device over USB/lockdownd:
[SSH ssh root@10.11.1.1](#)
To attach to the iOS kernel ([download here](#)) using a debugger with the gdb-remote protocol:
[kernelgdb llbd --one-line "gdb-remote 10.11.1.1:4000"](#)
To interact with the device's serial console:
[console nc 10.11.1.1 2000](#)

Wi-Fi IP: 10.11.0.1 Services IP: 10.11.1.1

<https://app.corellium.com/>

I'm in!

The Corellium interface displays a summary bar at the top with the device name "test (iPhone 7 Plus | 14.5 | 18E199 | ✓ Jailbroken)". It includes links for Devices, Help, Account, and a user name "Benjamin Altpeter". Below this is a toolbar with icons for Home, Side Button, Vol. Up, Vol. Down, and Keyboard.

The main area shows the device screen with a browser displaying "Datenanfragen.de" and the message "Du hast ein Recht auf Dat".

The navigation bar below the device screen includes CONNECT, FILES, APPS, NETWORK (selected), CORETRACE, SETTINGS, and CONSOLE.

The "Network Monitor" section captures HTTP/S traffic. It has a red "STOP MONITORING" button and a blue "CLEAR LOG" button. The table lists network requests:

INDEX ^	CODE	METHOD	HOST	START	SIZE
34	301	GET	datenanfragen.de	May 3, 2021 2:55 PM	—
35	200	GET	www.datenanfragen.de	May 3, 2021 2:55 PM	17.8 KB
36	200	GET	mesu.apple.com	May 3, 2021 2:55 PM	81.3 KB
37	200	GET	updates-http.cdn-apple.com	May 3, 2021 2:55 PM	118 KB
38	200	GET	www.datenanfragen.de	May 3, 2021 2:55 PM	6.23 KB
39	200	GET	www.datenanfragen.de	May 3, 2021 2:55 PM	1.21 KB
40	200	GET	www.datenanfragen.de	May 3, 2021 2:55 PM	2.63 KB
41	200	GET	static.dacdnn.de	May 3, 2021 2:55 PM	57.7 KB
42	200	GET	...	May 3, 2021 2:55 PM	26.4 KB

Below the table, the "OVERVIEW", "REQUEST", and "RESPONSE" tabs are visible. The "RESPONSE" tab shows the raw HTML content of the captured page, which includes links to "Artikel", "Anfrage generieren", "Unternehmensdatenbank", "Meine gespeicherten Daten", "Datenschutzeinstellungen", "Finden uns bei GitHub", "Unterhalte Dich mit uns über Matrix", and "Folge uns bei Mastodon" and "Folge uns auf Twitter".

<https://app.corellium.com/>

Another dead end

 CORELLIUM

To install an Android .apk file, simply click the **Install** button in the upper right corner of the Apps tab, and select the desired file. Click "OK," and a green progress bar will appear at the bottom of the screen indicating the progress as your app is uploaded and installed on the device. Once installation is complete, the app will appear in the list of Apps, as well as on the virtual device screen.

How to Install an iOS IPA

Important Note: On iOS, loading an app requires that the app be properly signed. You must load an app just as you would load it on a physical device. This is required both for jailbroken and non-jailbroken devices. If you receive an error when uploading an app, please ensure your app is appropriately signed and that you can load it on a physical device.

All iOS applications must be signed before they can be installed on a real or virtual device. Corellium does not enable users to download apps from the App Store.

Ensure that the UDID of the virtual devices corresponds to the UDID of your provisioning profile. You can adjust the UDID of the virtual device in the Settings -> Device IDs tab. Once you update the UDID, click "Save and Reboot" for the change to take effect.

Once your app is properly signed and the UDID is set accordingly, click the "Install" button on the Apps tab and select your signed .ipa file. A green progress bar will appear at the bottom of the screen indicating the progress as your app is uploaded and installed on the device. Once installation is complete, the app will appear in the list of Apps, as well as on the virtual device screen.

[Click here for information on testing third-party iOS apps.](#)

Troubleshooting Tips

If you are having trouble loading an app, please check the following before contacting support:

1. Does your app load on a real device of the same model and OS version?
2. If you are loading an iOS app, is it properly signed? Does it have the proper entitlements?

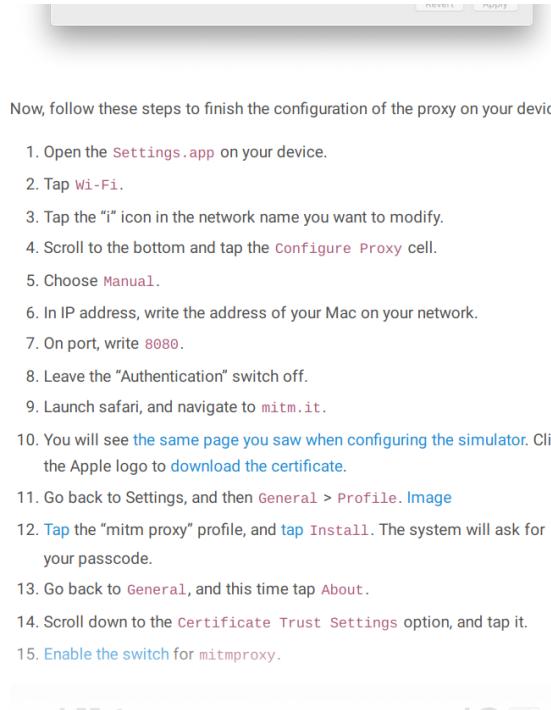
<https://support.corellium.com/hc/en-us/articles/360051662354-Apps>

Let's make the device usable



<https://checkra.in/>

Surprisingly easy...

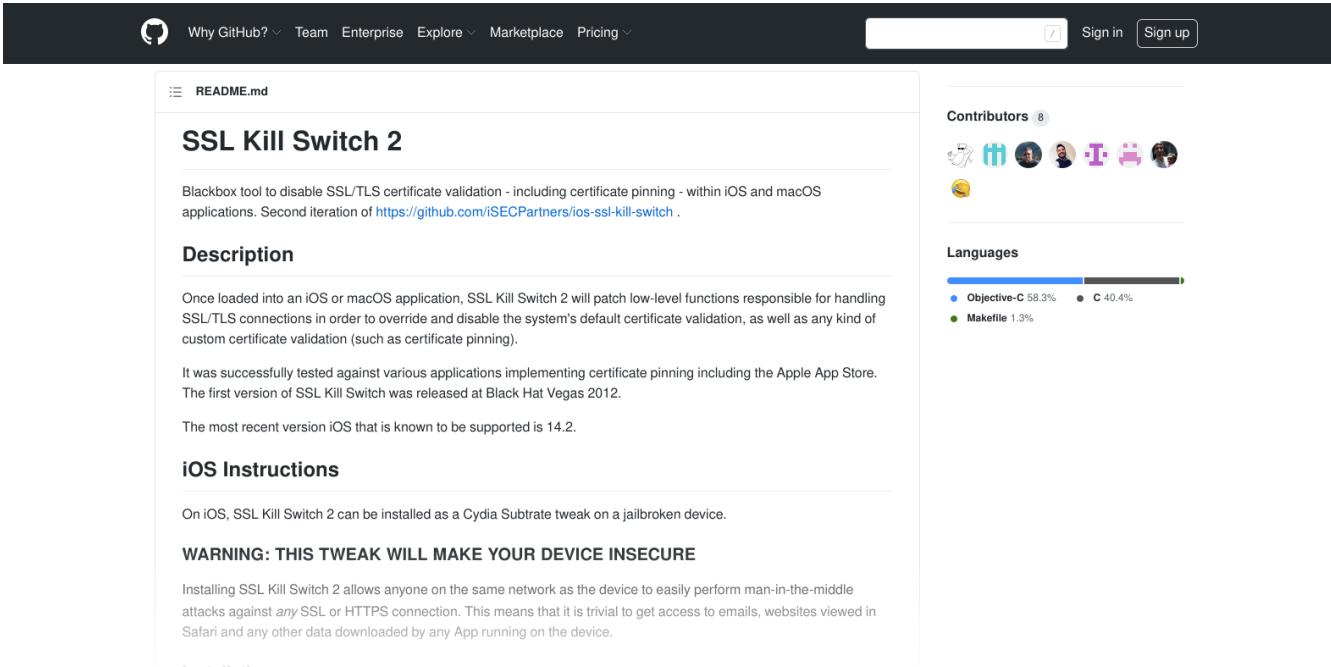


Now, follow these steps to finish the configuration of the proxy on your device:

1. Open the `Settings.app` on your device.
2. Tap `Wi-Fi`.
3. Tap the “i” icon in the network name you want to modify.
4. Scroll to the bottom and tap the `Configure Proxy` cell.
5. Choose `Manual`.
6. In IP address, write the address of your Mac on your network.
7. On port, write `8080`.
8. Leave the “Authentication” switch off.
9. Launch `safari`, and navigate to `mitm.it`.
10. You will see [the same page you saw when configuring the simulator](#). Click the Apple logo to download the certificate.
11. Go back to `Settings`, and then `General > Profile`. [Image](#)
12. Tap the “mitm proxy” profile, and tap `Install`. The system will ask for your passcode.
13. Go back to `General`, and this time tap `About`.
14. Scroll down to the `Certificate Trust Settings` option, and tap it.
15. [Enable the switch for mitmproxy](#).

<https://www.andyibanez.com/posts/intercepting-network-mitmproxy/#physical-ios-devices>

Surprisingly easy...



The screenshot shows the GitHub README page for the project "SSL Kill Switch 2". The page includes a brief description of the tool, its history, and usage instructions for iOS. It also displays the project's contributors and languages used.

Contributors: 8

Languages:

- Objective-C 58.3%
- C 40.4%
- Makefile 1.3%

Obtaining apps

```
<?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>artistName</key>
    <string>AMZN Mobile LLC</string>
    <key>bundleDisplayName</key>
    <string>Amazon Alexa</string>
    <!-- [...] -->
    <key>storeCohort</key>
    <string>7|date=1622133000000&sf=143443</string>
    <key>appleId</key>
    <string>frank.walther.1978@icloud.com</string>
    <key>aiBuy</key>
    <true/>
</dict>
</plist>
```

Obtaining apps

The screenshot shows a GitHub repository page for "AppSync Unified". The top navigation bar includes links for "Why GitHub?", "Team", "Enterprise", "Explore", "Marketplace", and "Pricing". On the right, there are "Sign in" and "Sign up" buttons. The repository stats show 9.5% in C, 8.4% in Logos, 7.5% in HTML, and 2.4% in Other. The repository description reads: "Unified AppSync dynamic library for iOS 5, 6, 7, 8, 9, 10, 11, 12, 13, and 14." A section titled "What is AppSync Unified?" explains it as a tweak that allows users to freely install ad-hoc signed, fakesigned, or unsigned IPA app packages on their iOS devices that iOS would otherwise consider invalid. It lists popular use cases such as installing freely-distributed apps, assisting in development, and cloning/downgrading apps. Another section, "How do I install AppSync Unified on my jailbroken iOS device?", provides instructions on how to add the repository via Cydia. A note cautions against installing unmodified versions from other repositories due to safety concerns.

Unified AppSync dynamic library for iOS 5, 6, 7, 8, 9, 10, 11, 12, 13, and 14.

What is AppSync Unified?

AppSync Unified is a tweak that allows users to freely install ad-hoc signed, fakesigned, or unsigned IPA app packages on their iOS devices that iOS would otherwise consider invalid.

Some popular use cases include:

- Installing freely-distributed apps that are unavailable from the App Store without having to re-sign the apps in question every 7 days (if the user does not have a subscription to the Apple Developer Program)
- Assisting in the development of iOS applications with Xcode
- Cloning or downgrading already-installed apps

How do I install AppSync Unified on my jailbroken iOS device?

AppSync Unified is available from Karen's Repo: <https://cydia.akemi.ai/> (Tap here on your device to automatically add the repo!)

If you do not see AppSync Unified listed in Karen's Repo, then that just means you have another repository added that is also hosting a copy of AppSync Unified under the same package ID.

Please only ever install the official, unmodified release from Karen's Repo for your own safety! Third-party modified versions from other repositories can and have broken various users' iOS installations in the past.

<https://github.com/akemin-dayo/AppSync>

Let's start with a wish list

The screenshot shows the "RSS Feed Generator" interface from Apple Services Marketing Tools. The search parameters are set to: Country or Region: Germany, Media Type: iOS Apps, Feed Type: TopFree, and Genre: All. The Results limit is set to 100, and the Format is JSON. The "Allow explicit" option is set to Yes. The Feed URL is https://rss.itunes.apple.com/api/v1/de/os-apps/top-free/1/100/explicit.json. The Feed Results Preview displays five app icons: CovPass (Robert Koch-Institut), luca app (culture4life GmbH), Corona-Warn-App (Robert Koch-Institut), Google Maps - Transit & Essen (Google LLC), and WhatsApp Messenger (WhatsApp Inc.).

Apple Services Marketing Tools

RSS Feed Generator

Feed Settings

Country or Region: Germany | Media Type: iOS Apps | Feed Type: TopFree | Genre: All

Results limit: 100 | Format: **JSON** | Allow explicit: Yes No

Feed URL

https://rss.itunes.apple.com/api/v1/de/os-apps/top-free/1/100/explicit.json

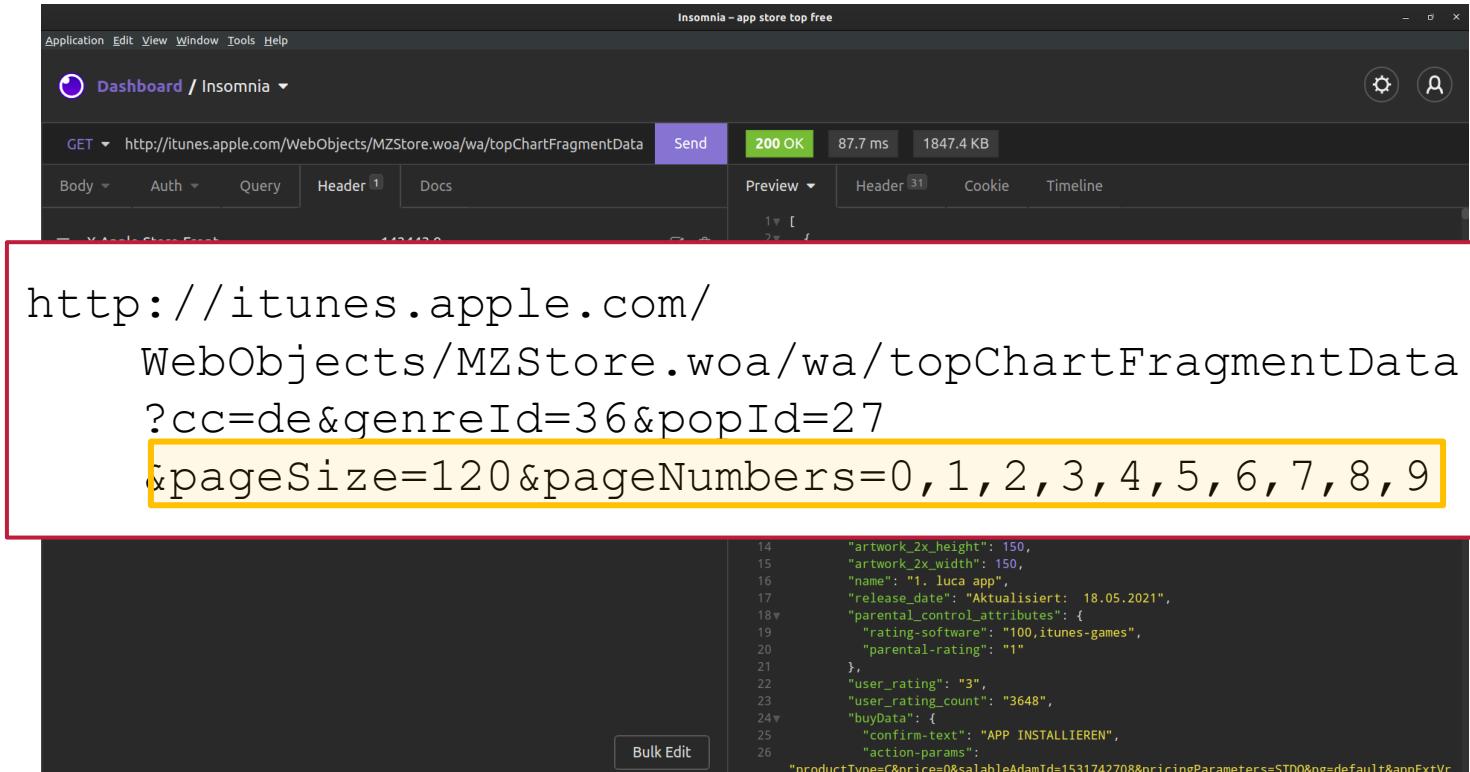
Feed Results Preview

iOS Apps : Top Free 1 - 5 of 100. [View More](#)

 CovPass Robert Koch-Institut	 luca app culture4life GmbH	 Corona-Warn-App Robert Koch-Institut	 Google Maps - Transit & Essen Google LLC	 WhatsApp Messenger WhatsApp Inc.
--	--	---	--	--

<https://rss.itunes.apple.com/en-us>

Backwards compatibility to the rescue



http://itunes.apple.com/
WebObjects/MZStore.woa/wa/topChartFragmentData
?cc=de&genreId=36&popId=27
&pageSize=120&pageNumbers=0,1,2,3,4,5,6,7,8,9

```
14     "artwork_2x_height": 150,  
15     "artwork_2x_width": 150,  
16     "name": "1. luca app",  
17     "release_date": "Aktualisiert: 18.05.2021",  
18     "parental_control_attributes": {  
19         "rating-software": "100_itunes-games",  
20         "parental-rating": "1"  
21     },  
22     "user_rating": "3",  
23     "user_rating_count": "3648",  
24     "buyData": {  
25         "confirm-text": "APP INSTALLIEREN",  
26         "action-params":  
"productType=C&price=0&salableAdamId=1531742708&pricingParameters=STD0&pg=default&appExtVr
```

Officially supported?



Where iOS Apps Are Stored Locally in Mac OS X and Windows

Dec 15, 2011 - 12 Comments



iOS apps are downloaded as bundles with a .ipa file extensions, but they are stored in different places than your [default iOS backups location](#). If you want to access iPhone and iPad apps manually, here's where to find them for both Mac OS X Lion, Snow Leopard, and Windows 7:

The easiest way to access these directories is by hitting **Command+Shift+G** and using Go To Folder, note the path is different depending on the OS:

- Mac OS X 10.7 Lion: ~/Music/iTunes/iTunes Media/Mobile Applications/
- Mac OS X 10.6: ~/Music/iTunes/Mobile Applications/

Subscribe to OSXDaily



Follow @OSXDaily

Tips & Tricks

- How to Cancel Pre-Orders on iPhone & iPad
- How to Check Warranty & Apple Care+ Status of Your Mac
- Forgot Apple Watch Passcode? Here's How to Reset It
- How to Change Storage Limit for Photos on Apple Watch
- How to Share iCloud Storage with Family on iPhone & iPad

News

- Public Beta 4 of iOS 15, iPadOS 15, MacOS Monterey Released for Testing
- MacOS Monterey Beta 4 Available to Download

<https://osxdaily.com/2011/12/15/where-ios-apps-stored-locally-in-mac-os-x-and-windows/>

Officially supported?



Deploy apps in a business environment with iTunes

Learn how to deploy apps with iTunes.

 This article has been archived and is no longer updated by Apple.

Apple offers [Volume Purchase Programmes](#) and Apple Configurator on Mac to help enterprise environments manage and mass-deploy apps on iOS devices. But certain business partners might still need to use iTunes to install apps.

Install apps with iTunes

If you've already installed a newer version of iTunes, you can download this version of iTunes¹ for your [Mac²](#), [PC \(32-bit\)](#) or [PC \(64-bit\)](#) and run the installer. After installation is complete, you can continue to deploy apps with iTunes.

You won't be prompted to download new versions of iTunes after you install this version. Manually [update to the latest version of iTunes](#) when you finish managing your devices to ensure you have the most up-to-date software.

1. Apple provides technical support only for the latest version of iTunes.

2. This version of iTunes is not compatible with macOS Mojave.

Published Date: February 26, 2020

<https://support.apple.com/en-gb/HT208079>

How about not so officially supported?

The screenshot shows a Reddit post titled "iTunes 12.6.5.3 working with iOS 13". The post was posted by a user named "4" one year ago. It contains a link to a archived comment from another user. The post includes several steps for using iTunes with iOS 13, mentioning MSI files and specific service stops. To the right of the post is a sidebar for the r/iTunes subreddit, which has 4.7k members and 25 online users. The sidebar also shows a created date of June 16, 2009, and a "Join" button. Below the sidebar is a meme featuring a dog and a child.

↑ Posted by 1 year ago

4 iTunes 12.6.5.3 working with iOS 13

Since the posting on 'iTunes 12.6.5.3 working with iOS 13' (https://www.reddit.com/r/iTunes/comments/d6g9tb/itunes_12653_ios_13/) is archived and replies/comments are no longer allowed, I'm posting this thread.

I've been using 'iTunes 12.6.5.3' with the latest iOS 13 Drivers for sometime now without problems.

The process is a bit 'manual' so for those interested, here are the steps:

-download the latest (whatever it may be) iTunes.exe installer (either 64bit or 32bit --don't even know if apple still supports only 32 bit installations--) -extract (using 7 Zip, Winrar, or your EXE extractor of choice) from the downloaded "iTunes.exe":

-AppleApplicationSupport.msi

-AppleMobileDeviceSupport.msi

-AppleMobileDeviceSupport64.msi (available for 64 bit installer/systems)

MSI Files are not like EXE files that can run other commands, thus, Prior to the install (since msi files are not 'intelligent' as exe, thus for safety I did this) I stoped the following Services:

-Apple Mobile Device Service

-Bonjour Service

-iPod Service

then -Run (to install):

-AppleApplicationSupport.msi

-AppleMobileDeviceSupport.msi

-AppleMobileDeviceSupport64.msi

More...

Log In Sign Up

Close

r/iTunes

r/iTunes is a 100% community-driven subreddit. We are not officially endorsed by nor affiliated with Apple.

4.7k Members 25 Online

Created Jun 16, 2009

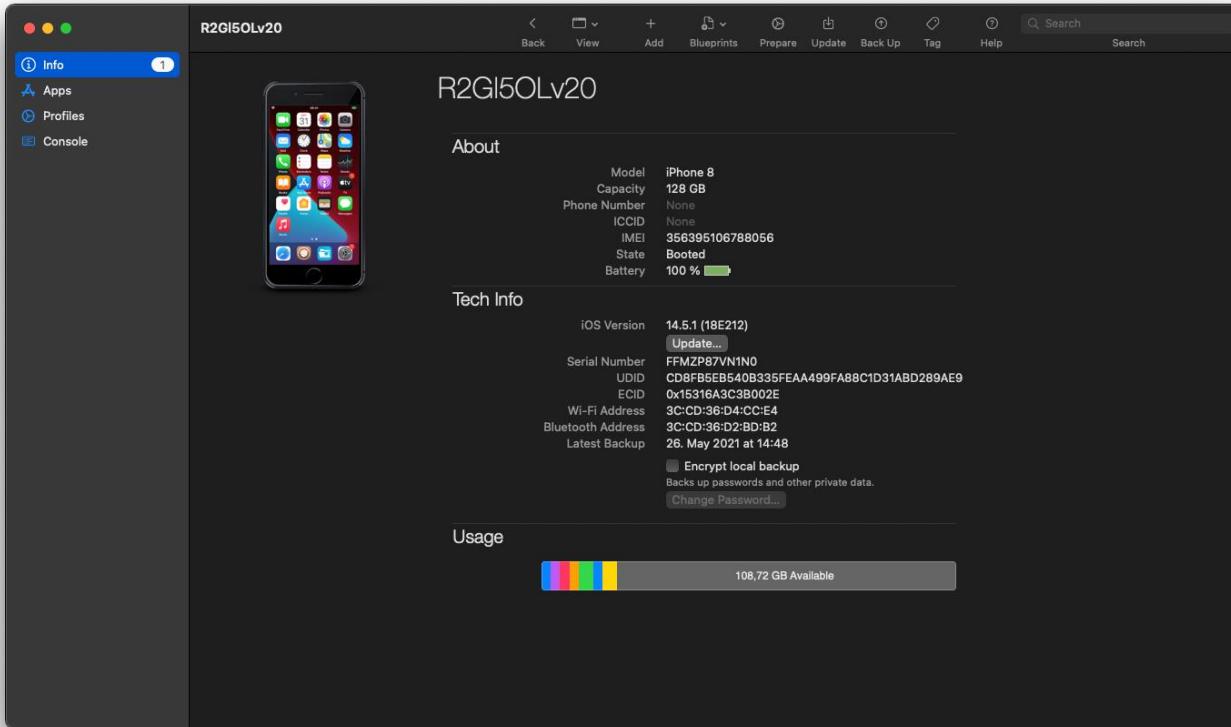
Join

TOP POSTS APRIL 12TH 2020

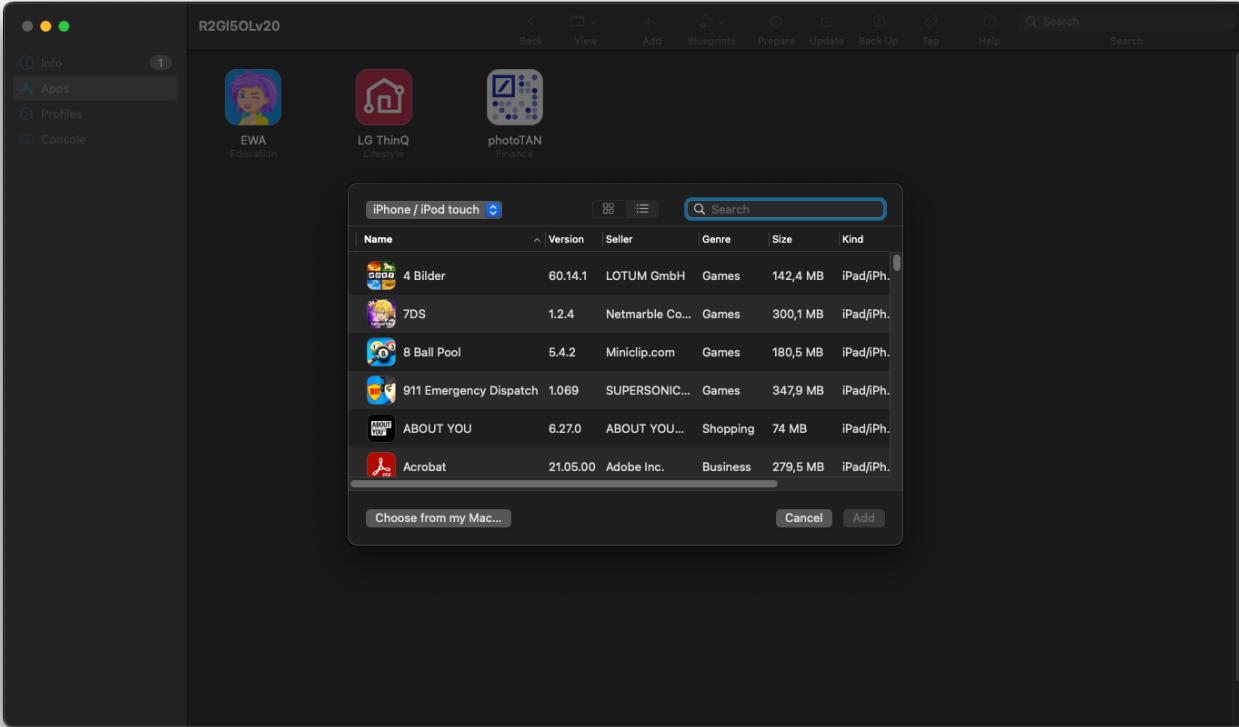
TOP POSTS OF APRIL, 2020

http://web.archive.org/web/20210527200153if_/https://www.reddit.com/r/iTunes/comments/g01qgh/itunes_12653_working_with_ios_13/

Officially supported 2.0



Officially supported 2.0—not quite, though

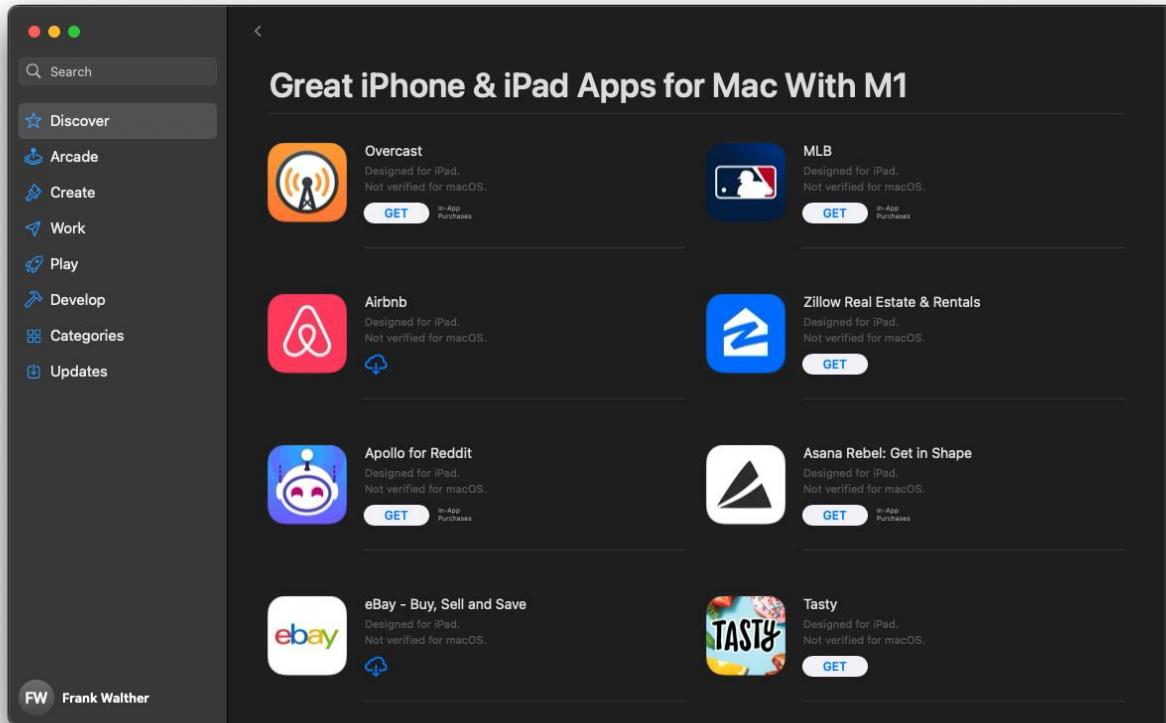


Officially supported 3.0

The screenshot shows the Apple Developer website's navigation bar with links for Discover, Design, Develop, Distribute, Support, Account, and a search icon. Below the navigation is a secondary menu for macOS with links for Overview, macOS SDK, Mac Catalyst, iPhone and iPad Apps, Distribution, and a prominent blue 'Download' button. The main content area features a large title 'iPhone and iPad Apps on Apple Silicon Macs'. Below the title is a paragraph explaining that iPhone and iPad apps are available without modification on the Mac App Store on Apple silicon Macs, mentioning optimization for keyboards, windows, and touch-input gestures. At the bottom of the content area are two images of Apple silicon Macs displaying colorful abstract backgrounds.

<https://developer.apple.com/macos/iphone-and-ipad-apps/>

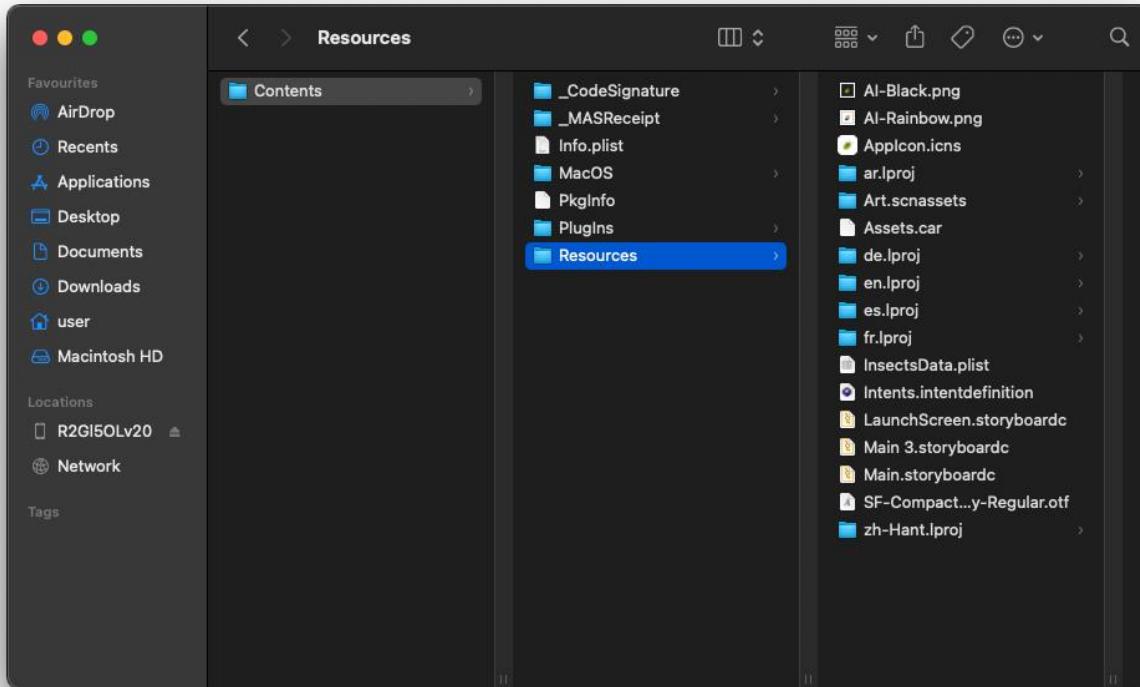
Officially supported 3.0



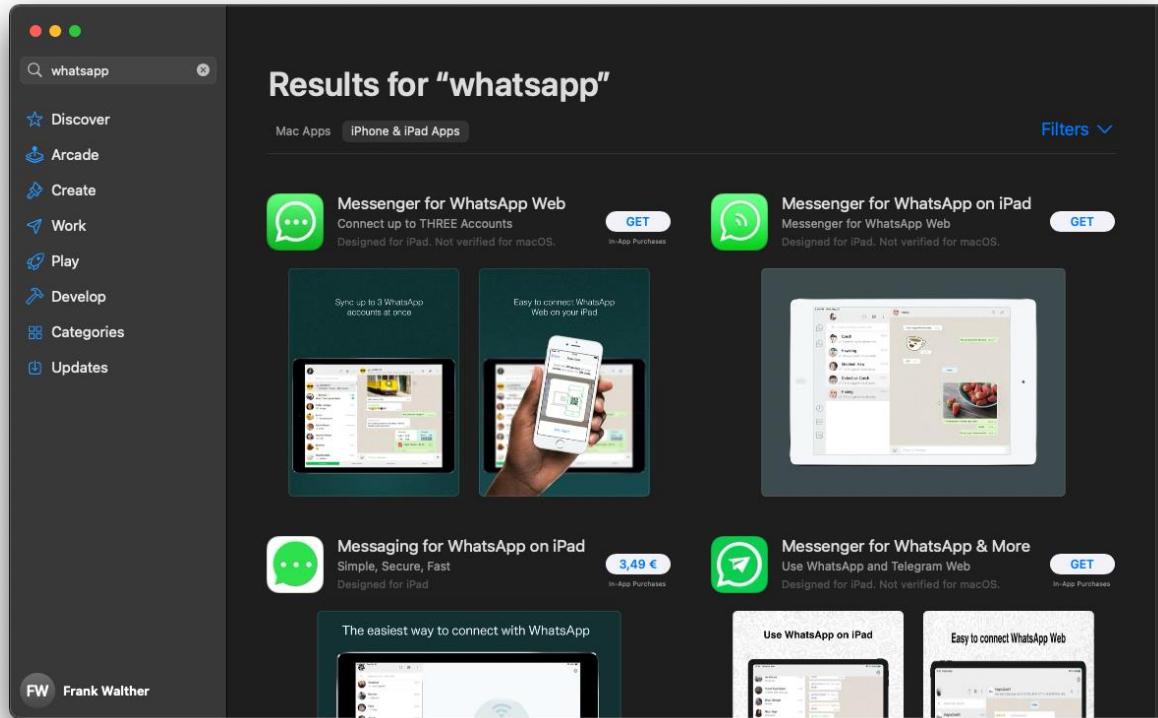
Officially supported 3.0



Probably just the .ipa?



Not all of them, though



How does the App Store do it?

Path	Method	Status	Size	Time
https://p59-buy.itunes.apple.com/WebObjects/MZBuy.woa/wa/buyProduct?guid=cd8fb5eb540b335feaa499fa88c1d31abd289ae9	POST	200	3.7kb	293ms
https://is3-ssl.mzstatic.com/image/thumb/Purple125/v4/33/77/19/33771947-eb9f-668f-15a2-315196c7d553/AppIcon-0-0-1x_U007emarketing-0-0-7-0-0-sRGB-0-0-0-GLES2_U002c0-512MB-85-220-0-0.png/144x14...	GET	200	6.1kb	231ms
https://xp.apple.com/report/2/xp_amp_appstore	POST	200	962b	148ms
https://xp.apple.com/report/2/xp_amp_appstore?eventTime=1627744436003&buttons=Get:Cancel&app=com.apple.AppStore&code=MZCommerce.ConfirmPaymentSheet&eventType=dialog&eventVersion=1&messag...	GET	200	2b	135ms
https://pd.itunes.apple.com/WebObjects/MZPurchaseDaap.woa/purchase/databases/101/items	POST	200	39.9kb	616ms
https://is3-ssl.mzstatic.com/image/thumb/Purple125/v4/33/77/19/33771947-eb9f-668f-15a2-315196c7d553/AppIcon-0-0-1x_U007emarketing-0-0-7-0-0-sRGB-0-0-0-GLES2_U002c0-512MB-85-220-0-0.png/114x11...	GET	200	4.3kb	236ms
https://xp.apple.com/report/2/xp_amp_appstore	POST	200	1.5kb	182ms
https://se-edge.itunes.apple.com/WebObjects/MZStoreElements.woa/wa/buyButtonMetaData?cc=de&plistPage=true&type=software	POST	200	337b	151ms
https://iosapps.itunes.apple.com/itunes-assets/Purple115/v4/53/b8/0b/53b80b66-0c4b-483f-f22b-b2f556e84d15/pre-thinned3578328089394696706.thinmed.signed.pkg.ipa?accessKey=1627938836_7573136195602...	GET	200	6.2mb	386ms
https://p63-fml.icloud.com/mipservice/fml/20235749998/cd8fb5eb540b335feaa499fa88c1d31abd289ae9/register	POST	204	1.0kb	275ms
https://p59-buy.itunes.apple.com/WebObjects/MZFinance.woa/wa/createAppReceipt?guid=cd8fb5eb540b335feaa499fa88c1d31abd289ae9	POST	200	4.5kb	328ms
https://p63-fml.icloud.com/mipservice/fml/20235749998/cd8fb5eb540b335feaa499fa88c1d31abd289ae9/register	POST	204	1.0kb	161ms
https://p59-buy.itunes.apple.com/WebObjects/MZFastFinance.woa/wa/songDownloadDone?guid=cd8fb5eb540b335feaa499fa88c1d31abd289ae9&downloadId=590063977898913&songId=1508899687	GET	200	228b	139ms

How does the App Store do it?

The screenshot shows the mitmproxy interface. The top navigation bar includes 'mitmproxy', 'Start', 'Options', and 'Flow' (which is selected). Below the bar are various controls: 'Replay', 'Duplicate', 'Revert', 'Delete', 'Download', 'Resume', 'Abort', 'Flow Modification', 'Export', and 'Interception'. The main pane displays a list of network flows. A specific POST request to <https://p59-buy.itunes.apple.com/WebObjects/MZBuy.woa/wa/buyProduct?guid=cd8fb5eb540b335fea499fa8c1d31abd289ae9> is highlighted. The request details show the XML payload sent to the server:

```
POST https://p59-buy.itunes.apple.com/WebObjects/MZBuy.woa/wa/buyProduct?guid=cd8fb5eb540b335fea499fa8c1d31abd289ae9 HTTP/1.1

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.plist" version="1.0">
<dict>
    <key><appExtVrsId></key>
    <string>841303723</string>
    <key><guid></key>
    <string>cd8fb5eb540b335fea499fa8c1d31abd289ae9</string>
    <key><hardwareFamily></key>
    <string>iPhone</string>
    <key><hardwareModel></key>
    <string>iPhone10,4</string>
    <key><cloud-backup-enabled></key>
    <string>1</string>
    <key><bsync></key>
    <string>AAQAAA8CxePWRaSu+o3VTySqhjZFmPdV71WB8sW1lJcvJGWo+L9Vu0Uci1TnhKb77yTtDfTgtZWoq+cLgR</string>
    <key><tApp></key>
    <string>com.apple.AppStore</string>
    <key><tClientId></key>
    <string>3231C91bd2Ce44TzClWzE5nLDVfd</string>
    <key><tEventTime></key>
    <string>162774427826</string>
    <key><tHardwareFamily></key>
    <string>iPhone</string>
    <key><tHardwareModel></key>
    <string>iPhone10,4</string>
    <key><tOs></key>
    <string>iOS</string>
    <key><tOsBuildNumber></key>
    <string>18E212</string>
    <key><tOsVersion></key>
    <string>iOS14.5.1</string>
    <key><mtNameContent></key>
```

How does the App Store do it?

The screenshot shows the mitmproxy tool interface. The top navigation bar includes 'mitmproxy', 'Start', 'Options', and 'Flow' (which is selected). Below the bar are buttons for 'Replay', 'Duplicate', 'Revert', 'Delete', 'Download', 'Resume', 'Abort', 'Flow Modification', 'Export', and 'Interception'. The main area displays a table of network flows. The columns are 'Path', 'Method', 'Status', 'Size', and 'Time'. The table lists several requests, mostly from 'https://p59-buy.itunes.apple.com' and 'https://iosapps.itunes.apple.com'. One specific request is highlighted in blue, showing its details. The 'Request' tab is active, displaying the full URL and query parameters. The 'Response' tab shows the status code 200 and the response content 'Request content missing.' The 'Details' tab is also visible.

Path	Method	Status	Size	Time
https://p59-buy.itunes.apple.com/WebObjects/MZBuy.woa/wa/buyProduct?guid=cd...	POST	200	3.7kb	293ms
https://is3-ssl.mzstatic.com/image/thumb/Purple125/v4/33/77/19/33771947-eb9f-66... GET	200	6.1kb	231ms	
https://xp.apple.com/report/2xp_amp_appstore	POST	200	962b	148ms
https://xp.apple.com/report/2xp_amp_appstore?eventTime=1627744436003&butto...	GET	200	2b	135ms
https://pd.itunes.apple.com/WebObjects/MZPurchaseDaap.woa/purchase/database...	POST	200	39.9kb	616ms
https://is5-ssl.mzstatic.com/image/thumb/Purple125/v4/33/77/19/33771947-eb9f-66... GET	200	4.3kb	236ms	
https://xp.apple.com/report/2xp_amp_appstore	POST	200	1.5kb	182ms
https://se-edge.itunes.apple.com/WebObjects/MZStoreElements.woa/wa/buyButton...	POST	200	337b	151ms
https://iosapps.itunes.apple.com/itunes-assets/Purple115/v4/53/b8/0b/53b80b66-0c4b-483f-f22b...	GET	200	6.2mb	386ms
https://p63-fml.icloud.com/mipservice/fml/20235749998/cdfbf5eb540b335fea499...	POST	204	1.0kb	275ms
https://p59-buy.itunes.apple.com/WebObjects/MZFinance.woa/wa/createAppReceipt...	POST	200	4.5kb	328ms
https://p63-fml.icloud.com/mipservice/fml/20235749998/cdfbf5eb540b335fea499...	POST	204	1.0kb	161ms
https://p59-buy.itunes.apple.com/WebObjects/MZFastFinance.woa/wa/songDownlo...	GET	200	228b	139ms

What do we actually need for the request?

```
<plist version="1.0">
<dict>
    <!-- [Not all parameters listed, some reordered.] -->
    <key>appExtVrsId</key>
    <string>841303723</string>
    <key>salableAdamId</key>
    <string>1508899687</string>
    <key>hardwareFamily</key>
    <string>iPhone</string>
    <key>hardwareModel</key>
    <string>iPhone10,4</string>
    <key>osVersion</key>
    <string>14.5.1</string>
    <key>kbsync</key>
    <string>AAQAAAW8CxePWRaSu+o3VTySqhjZFmPdV71WB8sW11jCvJGw0+L9Vu0Uc1TnhKb77yTtDftgtZWog+cLgRrFg
        5dyPoHbgK5LsSIRKTJ6fddbnPnk1YXj/3F4CXwLI9xZwecRfiREFpu89yXK7T04q3L6fOLux6uPdNUmo+YaLvYPeZXFU1
        Oh1HgDODF31ZH91duBHw2dV1AI0EztNJGm001dTt5d8RwgVuWLcohiEksnguxd0tACECxYIpDtPL8PaY9ex4bNbj1y2xG
        jBYUs0kR7wMHmCZZQeaeXCNs2qX+ZNNpBq+m4J1drkgQ+1WDtkKkVE4J5iw3j9bpiswQfpC2KYm2B8Jhd0R/hZYRTDsV+
        Vw0tG4QPcE9/zNq/KgRXp+yEBe6FL6WkKprg72ttDulrb/idwKy1Z6XucLi1jdrHZV</string>
</dict>
</plist>
```

kbsync, you say?

The screenshot shows a forum post on the website bbs.pediy.com. The post is titled "[求助]有人研究过itunes kbsync这个算法吗?" (Help needed: Has anyone studied the iTunes kbsync algorithm?). It was posted on October 3, 2012, at 17:02, with 15467 views. The post contains a string of characters: AAIAALNzml92d8M2KkNEHztZvnxT/toPqC0l2B9FbdbQksfimEcV+e5sRKjc8JS489ZG w+MwVh8ip5oTwU1hOW5A7pm4R1QRjyp28eLr2iWxswL9EGKcwqH7eku4Ef25kQ2g==. The poster asks for help with reverse engineering the algorithm used by iTunes to generate this string. They mention they have no experience with OD (Object Detacher) and ask for help with the DLL code. A link to another thread on the same site is provided: [The post ends with a call for help regarding the SDC 2021 conference.](http://bbs.pediy.com/showthread.php?p=1104955#post1104955)

帖子下方有四个操作按钮：收藏 (1), 点赞, 打赏, 分享。

右侧栏显示了发帖用户的个人信息：

- 用户名: cantellow
- 等级: 银质*
- 经验值: 5
- 回帖数: 8
- 排名: 10
- 关注按钮: + 关注
- 私信按钮: 私信

右侧栏还展示了其他文章的列表：

- [求助]某app加密接口 # 3902
- [未解决]折腾一个月了, 关于网络验证机制 # 12015
- [求助]有人研究过itunes kbsync这个算法吗? # 15468
- [求助]高手看看ollyDBG这段汇编 # 1540

下方有一个关于看雪安卓应用安全能力认证的广告横幅。

<https://bbs.pediy.com/thread-156752.htm>

kbsync, you say?

The screenshot shows a blog post on the Habr platform. The post is titled "Реверс-инжиниринг in-app покупок Apple. (или «там» все тоже ленивые)" (Reverse engineering of Apple's in-app purchases. (or "there" all are also lazy)). It was written by ZonD80 on August 7, 2012, at 15:19. The post discusses how reverse engineers cracked Apple's in-app purchase system, despite Apple's reputation for strict security. It includes a list of findings and a conclusion. The sidebar on the right lists other popular posts, such as one about helicopters on Mars and another about a developer's experience in London during the pandemic.

Хабр | КАК СТАТЬ АВТОРОМ | Питчи джава-работодателей

DS, DE, ETL – кто-нибудь знает, что всё это значит?

Все потоки | Разработка | Администрирование | Дизайн | Менеджмент | Маркетинг | Научноп

Считают сейчас

Вертолеты на Марсе жужжат и не отбрасывают тень

Почему я отказался от 18 тысяч долларов по баунти-программе Apple

Космонавты впервые вошли в модуль «Наука»

[Личный опыт] Лондон: не всегда мечта для программиста. Как живется в столице Британии во время коронавируса

Пользователи объяснили, почему Google необычно обрабатывает строку «Turn! Turn! Turn!»

«МойОфис»: анализируем данные

<https://habr.com/ru/post/149207/>

kbsync, you say?

知乎

写文章

苹果 gsa 服务器login 算法

看雪学院
看雪学院，为IT专业人士、技术专家提供了一个民间交流与合作空间。

1人赞同了该文章

分享

闹得蛋疼，对iTunes 登陆过程进行了初步的分析。解密得到了spd字段内容。将分析过程写出来，混个熟脸。

在分析这个东西之前，需要做一些准备工作。比如收集论坛前辈们的工作经验，github上某些开源代码。

通过对iTunes windows 和iOS10.x 系统进行抓包。发现数据包基本是大同小异，iOS 调试非常不方便，特别构造win7 x86环境对 iTunes 12.6.20 进行了逆向分析。

加上 标准版OD + 海风StrongOD，开始了这次逆向分析。

在分析之前，大概介绍下apple的这套东西，和平日玩windows逆向的区别。iTunes 或者mac iTunes 或者 iOS 的绝大部分代码是完全一样的。

对登陆过程进行抓包



▲ 赞同 1 ▾ 添加评论 分享 喜欢 收藏 申请转载 ...

<https://www.zhihu.com/column/p/29278195>

So close and yet so far...

The screenshot shows a web page from the YMSKY.NET website. At the top, there's a navigation bar with links like '首页', '源码下载', '代码分享', etc. Below the navigation is a search bar and a sidebar with a '分类列表' (Category List) containing various programming languages and technologies. The main content area displays a Python script titled 'itunes 模拟登陆'. The script uses modules such as `urllib2`, `httpplib`, `socket`, `json`, `ssl`, `xml.dom.minidom`, and `sgmlib` to perform a login operation. The code includes comments explaining the purpose of each part, such as setting up a socket timeout and defining a link server function.

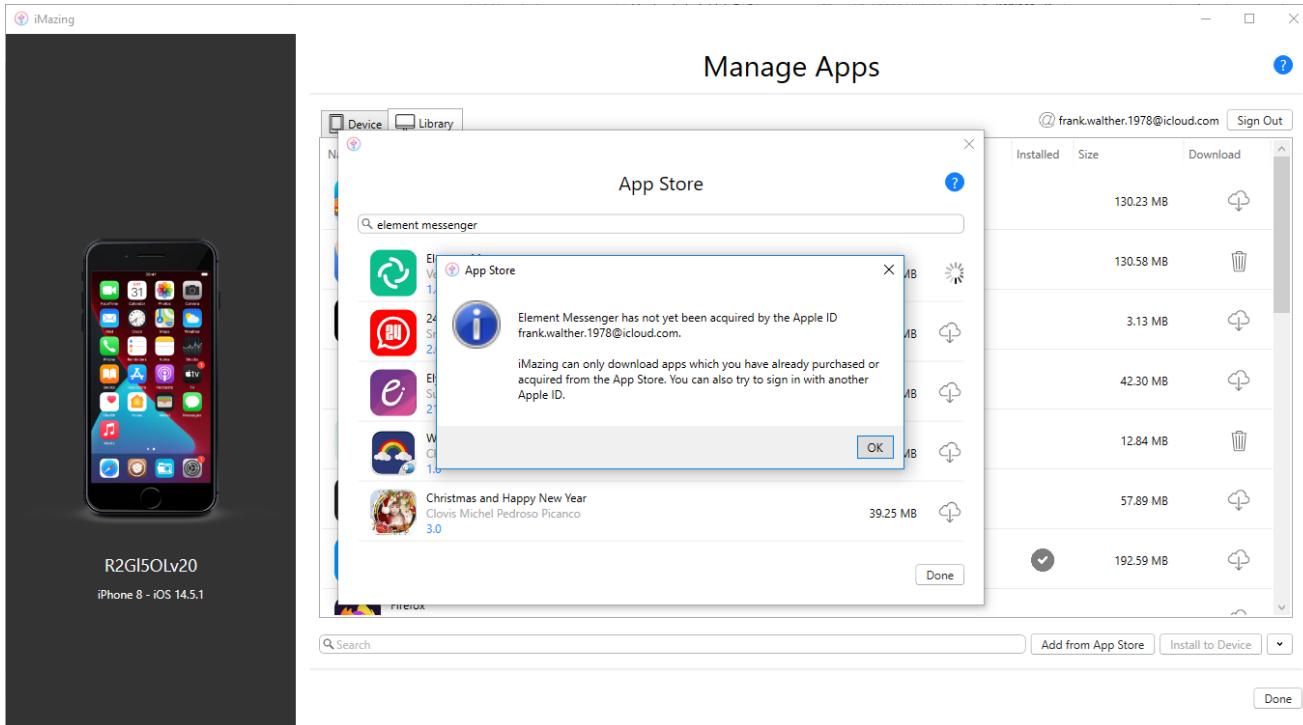
<http://www.ymsky.net/views/64756.shtml>

Some one else must have figured this out, right?

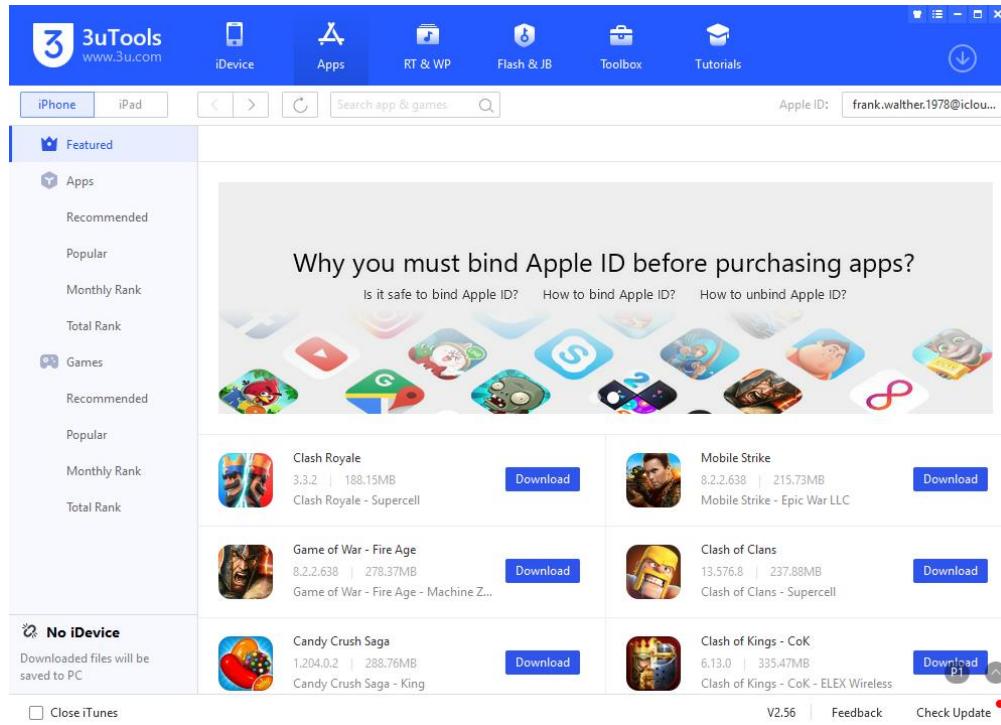
The screenshot shows the iMazing website homepage. At the top, there's a navigation bar with links for "Features", "Reviews", "Download", "Enterprise", "Store", "Support", "Blog", and language selection ("English"). The main heading is "Download & Install Apps to iPhone or iPad from Mac & PC". Below it, a sub-copy reads: "Manage your iOS apps your way. Enjoy a powerful tool to download your apps (.ipa) to your computer, and install them to your iOS devices. Save and restore your game progress or app documents and settings." There are two buttons: "Free Download" and "Buy Now". Below the text, there's a section for supported platforms: "iOS 15" and "Windows". On the right side of the main image, a Mac screen displays a file browser window titled "Choose Data to Restore" with various app icons like "Garena", "Call of Duty", "Grand Theft Auto V", and "Grand Theft Auto V: San Andreas". A smartphone and a tablet are shown next to the Mac. At the bottom, there's a navigation bar with icons for Phone, Contacts, Calendars, Other Data, Apps (which is underlined), Quick Transfer, File System, Transfer, and Backup Extractor.

<https://imazing.com/ios-app-management>

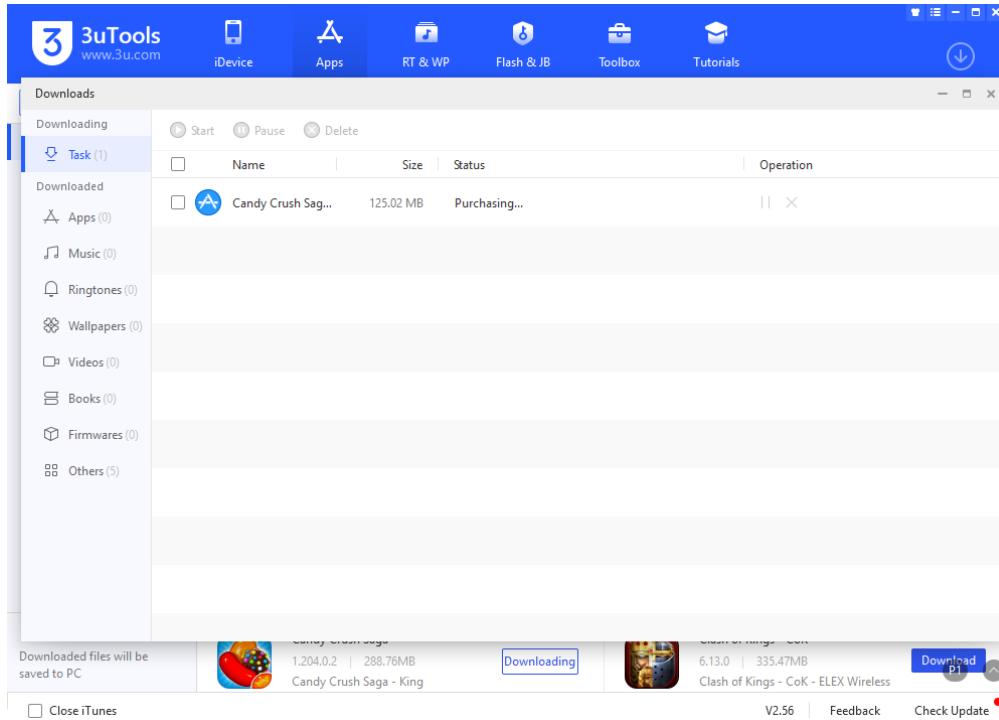
Not so iMazing, after all



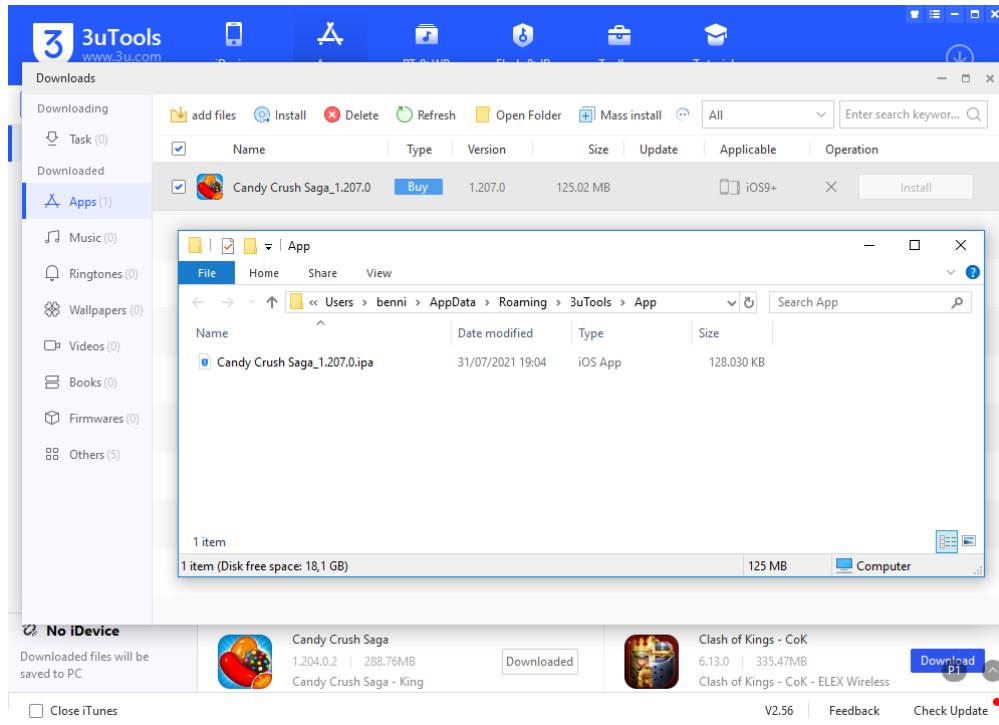
3uTools saves the day



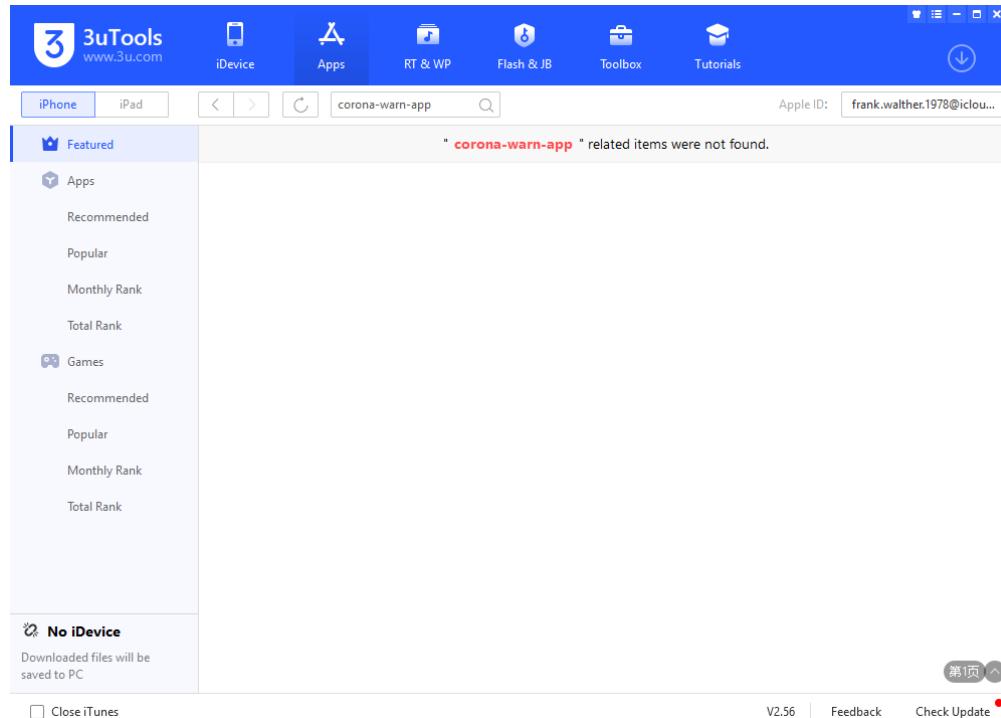
3uTools saves the day



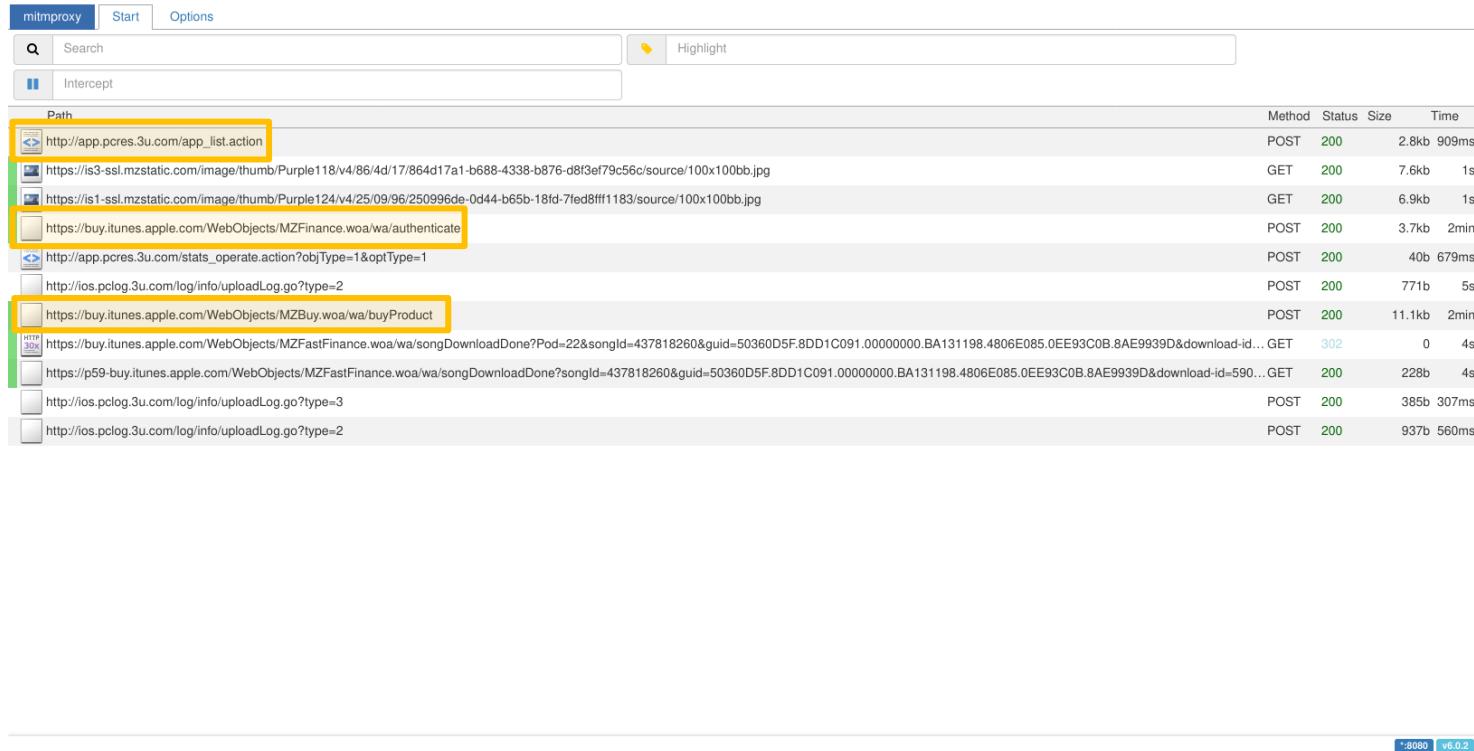
3uTools saves the day



A final road block



Or just a minor hurdle?



The screenshot shows the mitmproxy traffic capture interface. At the top, there are tabs for 'mitmproxy' (which is selected), 'Start', and 'Options'. Below the tabs is a search bar with a magnifying glass icon and a 'Highlight' button with a yellow exclamation mark icon. Underneath is an 'Intercept' button with a blue and white icon.

The main area displays a list of network requests. Each request is represented by a row with the following columns from left to right:

- Icon representing the request type (e.g., file download, POST, GET).
- Request URL.
- Method (e.g., POST, GET).
- Status (e.g., 200, 302).
- Size (e.g., 2.8kb, 7.6kb).
- Time (e.g., 909ms, 1s, 2min).

Three specific requests are highlighted with yellow boxes:

- `http://app.pcres.3u.com/app_list.action` (POST, 200, 2.8kb, 909ms)
- `https://i3-ssl.mzstatic.com/image/thumb/Purple118/v4/86/4d/17/864d17a1-b688-4338-b876-d8f3ef79c56c/source/100x100bb.jpg` (GET, 200, 7.6kb, 1s)
- `https://i1-ssl.mzstatic.com/image/thumb/Purple124/v4/25/09/96/250996de-0d44-b65b-18fd-7fed8fff1183/source/100x100bb.jpg` (GET, 200, 6.9kb, 1s)

Other requests listed include:

- `https://buy.itunes.apple.com/WebObjects/MZFinance.woa/wa/authenticate` (POST, 200, 3.7kb, 2min)
- `http://app.pcres.3u.com/stats_operate.action?objType=1&optType=1` (POST, 200, 40b, 679ms)
- `http://ios.pclog.3u.com/log/info/uploadLog.go?type=2` (POST, 200, 771b, 5s)
- `https://buy.itunes.apple.com/WebObjects/MZBuy.woa/wa/buyProduct` (POST, 200, 11.1kb, 2min)
- `HTTP [302] https://buy.itunes.apple.com/WebObjects/MZFastFinance.woa/wa/songDownloadDone?Pod=22&songId=437818260&guid=50360D5F.8DD1C091.00000000.BA131198.4806E085.0EE93C0B.8AE9939D&download-id=590...` (GET, 302, 0, 4s)
- `https://p59-buy.itunes.apple.com/WebObjects/MZFastFinance.woa/wa/songDownloadDone?songId=437818260&guid=50360D5F.8DD1C091.00000000.BA131198.4806E085.0EE93C0B.8AE9939D&download-id=590...` (GET, 200, 228b, 4s)
- `http://ios.pclog.3u.com/log/info/uploadLog.go?type=3` (POST, 200, 385b, 307ms)
- `http://ios.pclog.3u.com/log/info/uploadLog.go?type=2` (POST, 200, 937b, 560ms)

In the bottom right corner of the mitmproxy window, it says '1:8080 v6.0.2'.

Doesn't that request look familiar?

The screenshot shows the mitmproxy browser interface. The top navigation bar includes 'mitmproxy', 'Start', 'Options', and 'Flow' tabs. Below the navigation is a toolbar with icons for 'Replay', 'Duplicate', 'Revert', 'Delete', 'Download', 'Resume', and 'Abort'. A dropdown menu for 'Flow Modification' and an 'Export' button are also present. The main window displays a list of network requests:

Path	Method	Status	Size	Time
http://app.pcrecs.3u.com/app_list.action	POST	200	2.8kb	909ms
https://is3-ssl.mzstatic.com/image/thumb/Purple118/v4/86/4d/17/864d17a1-b688-4... GET	200	7.6kb	1s	
https://is1-ssl.mzstatic.com/image/thumb/Purple124/v4/25/09/96/250996de-0d44-b... GET	200	6.9kb	1s	
https://buy.itunes.apple.com/WebObjects/MZFinance.woa/wa/authenticate	POST	200	3.7kb	2min
http://app.pcrecs.3u.com/stats_operate.action?objType=1&optType=1	POST	200	40b	679ms
http://ios.pclog.3u.com/log/info/uploadLog.go?type=2	POST	200	771b	5s
https://buy.itunes.apple.com/WebObjects/MZBuy.woa/wa/buyProduct	POST	200	11.1kb	2min
https://buy.itunes.apple.com/WebObjects/MZFastFinance.woa/wa/songDownloadD... GET	302	0	4s	
https://p59-buy.itunes.apple.com/WebObjects/MZFastFinance.woa/wa/songDownload... GET	200	228b	4s	
http://ios.pclog.3u.com/log/info/uploadLog.go?type=3	POST	200	385b	307ms
http://ios.pclog.3u.com/log/info/uploadLog.go?type=2	POST	200	937b	560ms

A specific request to `https://buy.itunes.apple.com/WebObjects/MZBuy.woa/wa/buyProduct` is selected and expanded. The 'Request' tab shows the full HTTPS request message, which includes a large payload (the body of the POST request) containing a Property List (plist) file. The 'Response' tab shows the server's response, and the 'Details' tab provides a detailed breakdown of the request headers.

Request Headers (selected):

- Host: buy.itunes.apple.com
- User-Agent: iTunes/11.4 (Windows; Microsoft Windows 7 x86 Ultimate Edition Service Pack 1 (Build 7601); AppleWebKit/536.30.1)
- Accept: */*
- Cookie: ns-mzf-inst=104-14-443-52-240-9019-597195-59-st44; countryVerified=1; hsacctn=1; mz_in=597195; session-store-id=933443CAc59F08CDB0C468FB05D8816; NSC_nagjobodf=bopo-qqpn*0xffffffffF0944761c45525d5f458455e445a4a2378b; mz_mt=0-20235749998=AnImEo9CrnJk1VUpwlc8NHpG5kTDRJyLd-EvyHl0j3Hfqo/zsYZ3n5lb8xEuhFx5afVXKezcnnHdahcGVpZ1sJgUg8xtcz+dHoryivpmVM2+mn2mV6ZSPt0ZNZ4PKJT91Qrcrbv6b15A60S/2Kxnm81pP5cnCGWf70xGBF11AA1G1ZG1zz+J1idzvf7MJY39181=; X-Dsid=20235749998; itspod=59; mg_at=0-20235749998=AwUAAAECAGvQAAAAABgr1Gk4wZeeacJH7Y63804kH+Kng1Hv0=; mz_at_sel=20235749998=AwUAAAECAAGrpQAAAABgr1GkaLzyfjxp1H7Y1M1jZnwvVmzJvtA=; pldflcid=ec8960372f244c3db043866ab575bb91059; vrep=C0601LFLEGQIBRAAEgQICRAAEgQICRAAEgQIAxAAEgQIDRAAEgQIBhAAEgQIBbAAEgQICQIAEgQICRAAEgQICRAAEgQIDhAAEgQIDhAAEgQIDBAA; wosid-lite=7NW4fpoxJJWT4bbfun8BF0
- X-Apple-Store-Front: 143443-1,17
- Content-Type: application/x-apple-plist
- Cache-Control: no-cache
- Referer: http://itunes.apple.com/cn/app//id1225032527?mt=8
- Accept-Language: zh-cn, zh;q=0.5
- X-Apple-Tz: 28800
- X-Token: AwUAAAECAGvQAAAAABgr1Gkf7sNCsrOrfwplAtNZOYjaK1ZHyl=
- X-Dsid: 20235749998
- Connection: Close
- Content-Length: 1323

Request Body (selected):

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.plist version="1.0">
<dict>
```

We've identified our hurdle

The screenshot shows the mitmproxy interface. On the left, a list of network requests and responses is displayed. On the right, a detailed view of a selected request (HTTP/1.1 200 OK) is shown, with its JSON content expanded. The JSON response includes fields such as 'co' (20), 'list' (an array of game entries), and various metadata like 'appname', 'icon', 'id', 'isfull', 'itemid', 'longversion', 'md5', 'minversion', 'path', 'pkagetype', 'shortversion', 'sizebyte', 'slogan', 'slogancolor', 'sort', 'sourcedid', 'version', and 'versionid'. The mitmproxy UI includes tabs for Request, Response, and Details, and status indicators at the bottom right.

Path	Method	Status	Size	Time
http://app.pcres.3u.com/app_list.action	POST	200	2.8kb	909ms
https://is3-ssl.mzstatic.com/image/thumb/Purple118/v4/86/4d/17/864d17a1-b688-4... GET	200	7.6kb	1s	
https://is1-ssl.mzstatic.com/image/thumb/Purple124/v4/25/09/96/250996de-0d44-b... GET	200	6.9kb	1s	
https://buy.itunes.apple.com/WebObjects/MZFinance.woa/wa/authenticate	POST	200	3.7kb	2min
http://app.pcres.3u.com/stats_operate.action?objType=1&optType=1	POST	200	40b	679ms
http://ios.pclog.3u.com/log/info/uploadLog.go?type=2	POST	200	771b	5s
https://buy.itunes.apple.com/WebObjects/MZBuy.woa/wa/buyProduct	POST	200	11.1kb	2min
https://buy.itunes.apple.com/WebObjects/MZFastFinance.woa/wa/songDownloadD... GET	302	0	4s	
https://p59-buy.itunes.apple.com/WebObjects/MZFastFinance.woa/wa/songDownload... GET	200	228b	4s	
http://ios.pclog.3u.com/log/info/uploadLog.go?type=3	POST	200	385b	307ms
http://ios.pclog.3u.com/log/info/uploadLog.go?type=2	POST	200	937b	560ms

The only logical solution

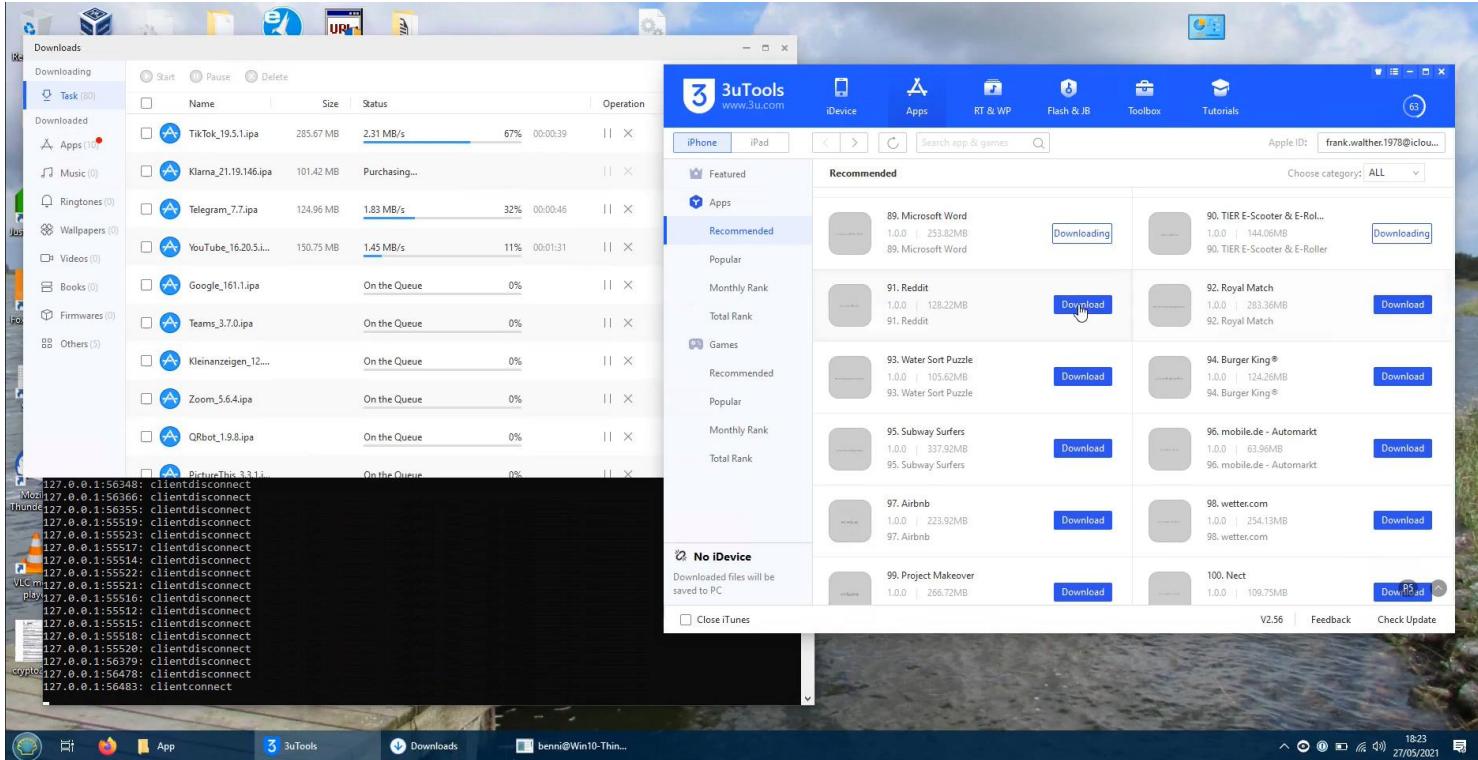
```
def response(self, flow: http.HTTPFlow):
    if(flow.request.pretty_url == "http://app.pcres.3u.com/app_list.action"):
        i = int(flow.request.urlencoded_form.get("page")) - 1
        apps = self.apps[0+i*20:20+i*20]
        res_apps = [
            "versionid": "0",
            "icon": f"https://via.placeholder.com/100?text={a['buyData']['bundle-id']}",
            "itemid": a['id'],
            "id": idx + i * 20,
            "slogancolor": "#f0f0f0",
            "appname": a['name'],
            "sourceid": a['buyData']['bundle-id'],
            "minversion": a['buyData']['minimum-os-version'],
            "sizebyte": a['buyData']['file-size'],
            "longversion": a['buyData']['minimum-os-version'],
            # [...]
        } for idx, a in enumerate(apps)]
        res = { "success": True, "type": 104, "list": res_apps, "co": 20 }
        flow.response.content = json.dumps(res).encode("utf-8")
```

An improved 3uTools

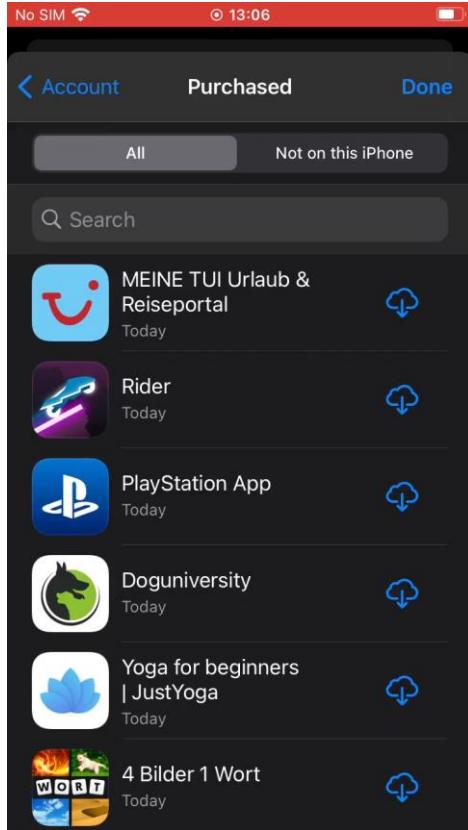
The screenshot shows the 3uTools software interface. The top navigation bar includes links for iDevice, Apps, RT & WP, Flash & JB, Toolbox, and Tutorials. A search bar at the top right allows users to search for apps and games. The main content area displays a list of recommended applications, categorized by type (Featured, Apps, Games) and popularity (Popular, Monthly Rank, Total Rank). Each entry includes the app icon, name, version, file size, and a 'Download' button. The 'Featured' section is currently selected. The 'No iDevice' section at the bottom indicates that downloaded files will be saved to the PC.

Recommended	
 1. luca app 1.0.0 27.68MB 1. luca app	 2. Google Arts & Culture 1.0.0 111.11MB 2. Google Arts & Culture
 3. Poparazzi 1.0.0 68.32MB 3. Poparazzi	 4. Darf ich das? 1.0.0 26.78MB 4. Darf ich das?
 5. CapCut 1.0.0 118.52MB 5. CapCut	 6. Like A Dino! 1.0.0 51.85MB 6. Like A Dino!
 7. Signal – Sicherer Messenger 1.0.0 164.76MB 7. Signal – Sicherer Messenger	 8. Google Maps - Transit & Essen 1.0.0 222.63MB 8. Google Maps - Transit & Essen
 9. PayPal 1.0.0 280.98MB 9. PayPal	 10. Instagram 1.0.0 167.3MB 10. Instagram
 11. TikTok 1.0.0 399.52MB 11. TikTok	 12. Klarna Shop now. Pay later. 1.0.0 172.34MB 12. Klarna Shop now. Pay later.

Click, click, click...



The reward



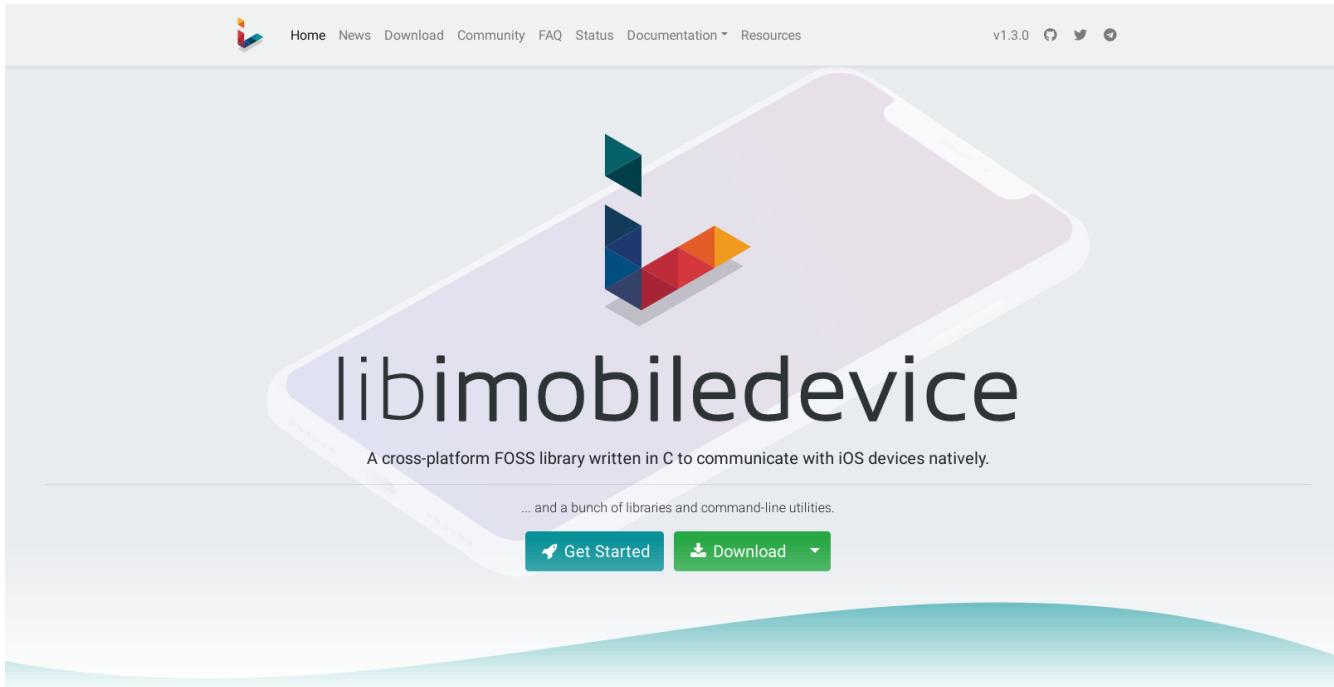
The (way) better reward



Automation

- On macOS, Configurator can be scripted:
 - `cfgutil install-app "<file.ipa>"`
 - `cfgutil remove-app "<bundle_id>"`

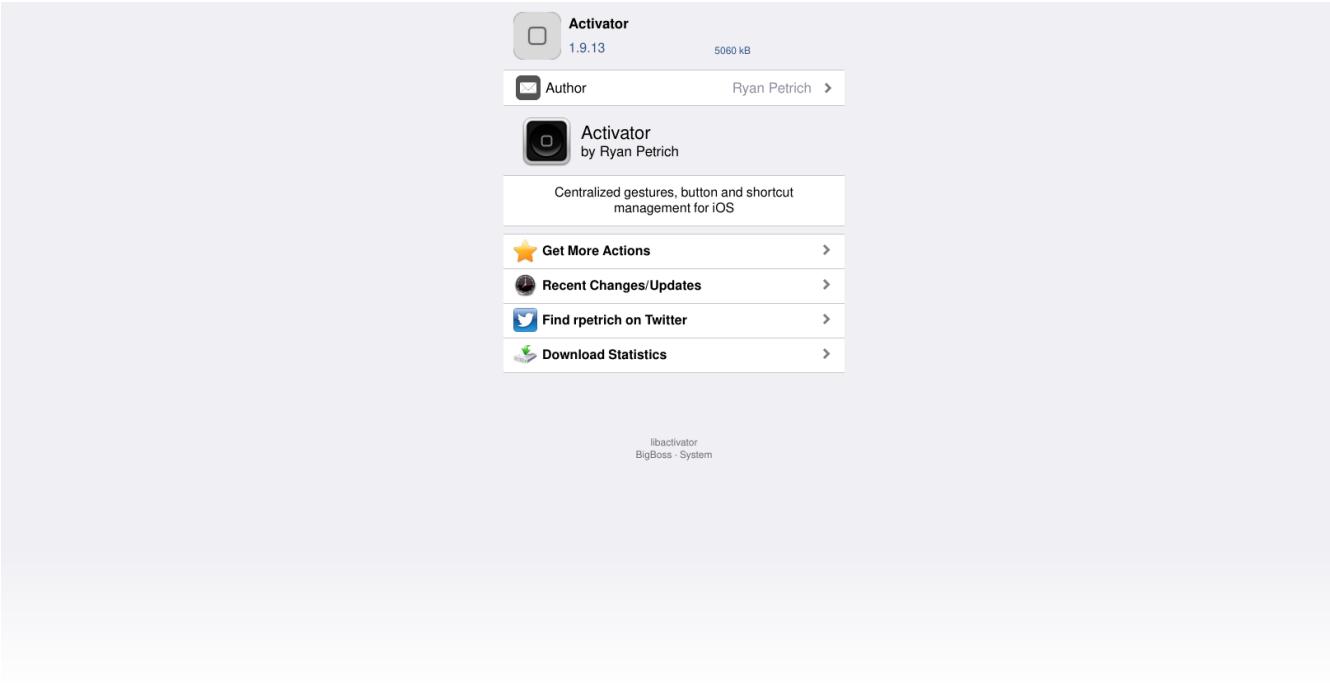
Automation



Automation

- On macOS, Configurator can be scripted:
 - `cfgutil install-app "<file.ipa>"`
 - `cfgutil remove-app "<bundle_id>"`
- On Linux, we use libimobiledevice:
 - `ideviceinstaller --install "<file.ipa>"`
 - `ideviceinstaller --uninstall "<bundle_id>"`

Automation



libactivator
BigBoss · System

<https://cydia.saurik.com/package/libactivator/>

Automation

- On macOS, Configurator can be scripted:
 - `cfgutil install-app "<file.ipa>"`
 - `cfgutil remove-app "<bundle_id>"`
- On Linux, we use libimobiledevice:
 - `ideviceinstaller --install "<file.ipa>"`
 - `ideviceinstaller --uninstall "<bundle_id>"`
- For the rest, we SSH into the device and use Activator:
 - `activator send libactivator.system.homebutton`
 - `activator send "<bundle_id>"`
 - `activator` listeners

Automatically granting permissions



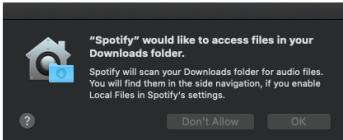
products malware blog store about

CVE-2020-9934: Bypassing TCC ...for unauthorized access to sensitive user data!

by Matt Shockley / July 28, 2020

Background

The Transparency, Consent, and Control (TCC) Framework is an Apple subsystem which denies installed applications access to sensitive user data without explicit permission from the user (generally in the form of a pop-up message):



TCC prompt when opening Spotify for the first time

While TCC also runs on iOS, this bug is restricted to the OS X variant. To learn more about how TCC works, especially with Catalina, I recommend reading [this article](#)

If an application attempts to access files in a directory protected by TCC without user authorization, the file operation will fail. TCC stores these user-level entitlements in a SQLite3 database on disk at \$HOME/Library/Application Support/com.apple.TCC/TCC.db. Apple uses a dedicated daemon, tcdd, for each logged-in user (and one system level daemon) to handle TCC requests. These daemons sit idle until they receive an access request from the OS for an application attempting to access protected data.

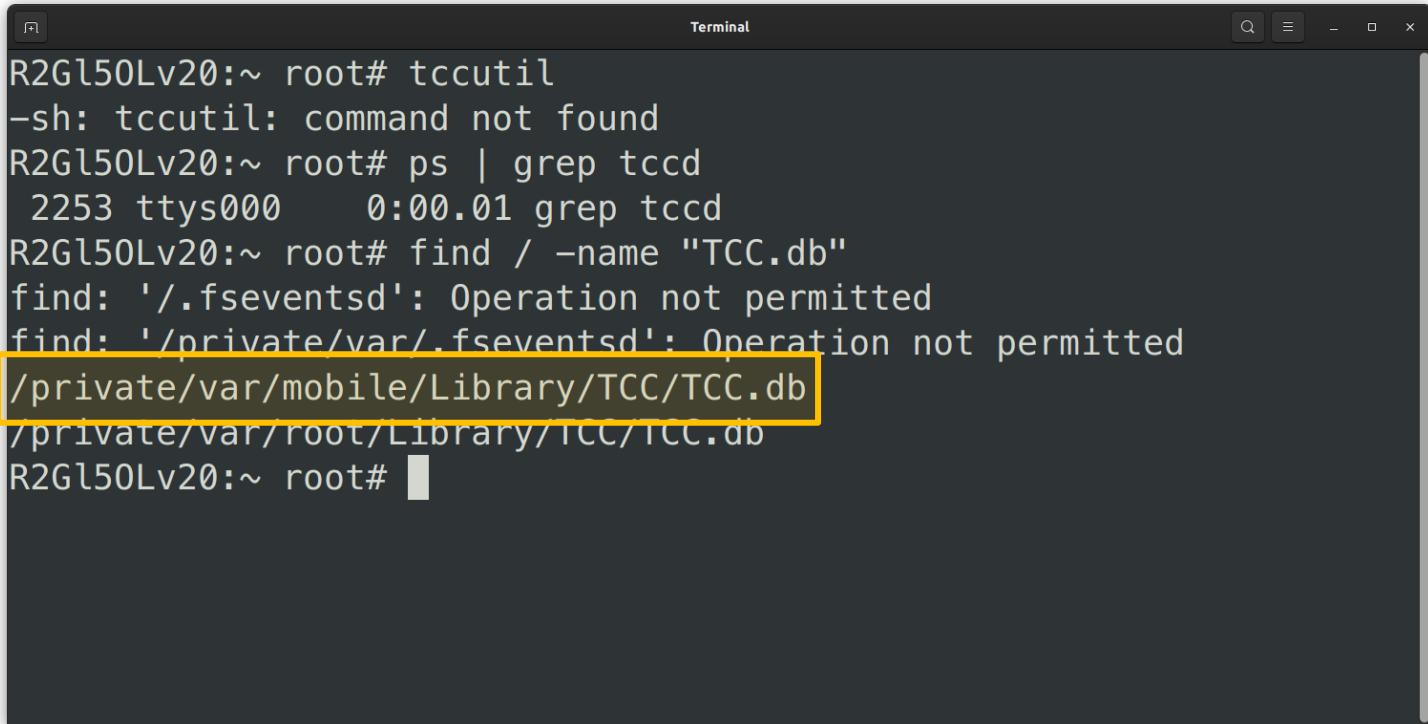
```
matt@Matt-MacBook-Pro: ~ $ ps ax | grep tcdd | grep -v grep
183 ?? Ss 0:51.51 /System/Library/PrivateFrameworks/TCC.framework/Resources/tcdd system
501 ?? S 0:25.76 /System/Library/PrivateFrameworks/TCC.framework/Resources/tcdd
```

listing currently running TCC daemons

Support Us!

https://objective-see.com/blog/blog_0x4C.html

Automatically granting permissions



```
R2Gl50Lv20:~ root# tccutil
-sh: tccutil: command not found
R2Gl50Lv20:~ root# ps | grep tccd
 2253 ttys000    0:00.01 grep tccd
R2Gl50Lv20:~ root# find / -name "TCC.db"
find: './fsevents': Operation not permitted
find: '/private/var/.fsevents': Operation not permitted
/private/var/mobile/Library/TCC/TCC.db
/private/var/root/Library/TCC/TCC.db
R2Gl50Lv20:~ root#
```

Automatically granting permissions

DB Browser for SQLite - /home/benni/tmp/ios-tcc/TCC.db

File Edit View Tools Help

New Database Open Database Write Changes Revert Changes Open Project Save Project Attach Database Close Database

Database Structure Browse Data Edit Pragmas Execute SQL

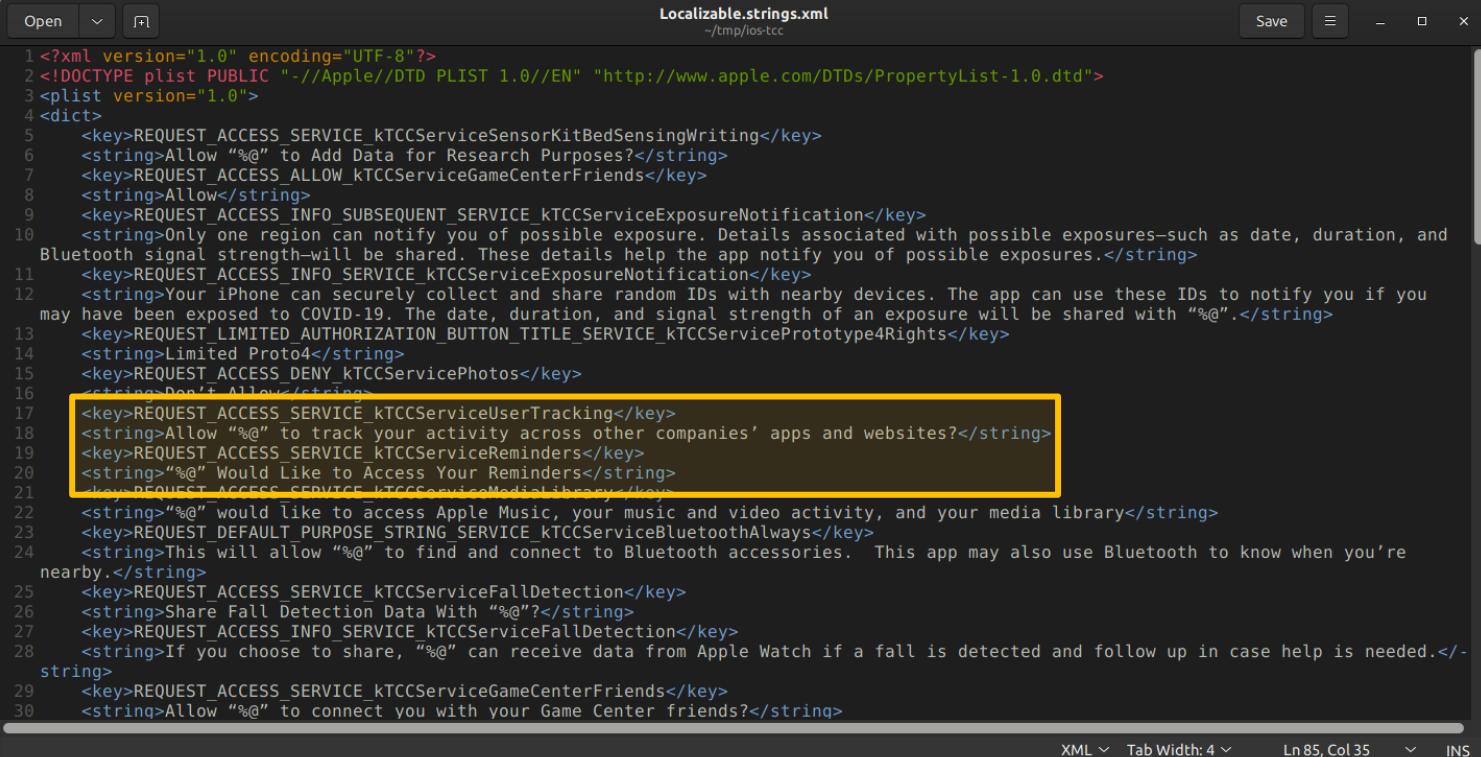
Table: access

service	client	client_type	auth_value	auth_reason	auth_version	csreq	policy_id	indirect_object_identifier_type	indirect_object_identifier	indirect_object_code_identity	flags	last_modified
KTCCServiceMotion	com.apple.Health		0	2	4	1	NULL	NULL	0	UNUSED	NULL	0 1620829599
KTCCServiceLiverpool	com.apple.Health		0	2	4	1	NULL	NULL	0	UNUSED	NULL	0 1620991202
KTCCServiceUbiquity	com.apple.mobilesafari		0	2	4	1	NULL	NULL	0	UNUSED	NULL	0 1620991211
KTCCServiceUbiquity	com.apple.iBooks		0	2	4	1	NULL	NULL	0	UNUSED	NULL	0 1620991213
KTCCServiceUbiquity	com.apple.Passbook		0	2	4	1	NULL	NULL	0	UNUSED	NULL	0 1620991213
KTCCServiceUbiquity	com.apple.MailCompositionService		0	2	4	1	NULL	NULL	0	UNUSED	NULL	0 1620991213
KTCCServiceUbiquity	com.apple.mobilemail		0	2	4	1	NULL	NULL	0	UNUSED	NULL	0 1620991213
KTCCServiceUbiquity	com.apple.DocumentsApp		0	2	4	1	NULL	NULL	0	UNUSED	NULL	0 1620991214
KTCCServiceUbiquity	com.apple.shortcuts		0	2	4	1	NULL	NULL	0	UNUSED	NULL	0 1620991214
KTCCServiceLiverpool	com.apple.shortcuts		0	2	4	1	NULL	NULL	0	UNUSED	NULL	0 1620991272
KTCCServiceLiverpool	com.apple.stocks		0	2	5	1	NULL	NULL	0	USED	NULL	0 1621001132
KTCCServiceWebKitIntelli...	org.mozilla.ios.Firefox		0	2	5	1	NULL	NULL	0	USED	NULL	0 1621081431
KTCCServiceWebKitIntelli...	com.apple.mobilesafari		0	2	5	1	NULL	NULL	0	USED	NULL	0 1621081877
KTCCServiceLiverpool	com.apple.upload-request...		0	2	4	1	NULL	NULL	0	USED	NULL	0 1623176245
KTCCServiceLiverpool	com.apple.accessibility.Accessibility...		0	2	5	1	NULL	NULL	0	USED	NULL	0 1623439707
KTCCServiceLiverpool	com.apple.security.cuttlefish		0	2	4	1	NULL	NULL	0	USED	NULL	0 1623440322

auth_value == 0:
permission not granted

auth_value == 2:
permission granted

Automatically granting permissions



The screenshot shows a code editor window with the file "Localizable.strings.xml" open. The file contains XML code defining localization strings for various permission requests. A yellow box highlights a specific block of text related to user tracking and reminders:

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
3 <plist version="1.0">
4 <dict>
5   <key>REQUEST_ACCESS_SERVICE_kTCCServiceSensorKitBedSensingWriting</key>
6   <string>Allow "%@" to Add Data for Research Purposes?</string>
7   <key>REQUEST_ACCESS_ALLOW_kTCCServiceGameCenterFriends</key>
8   <string>Allow</string>
9   <key>REQUEST_ACCESS_INFO_SUBSEQUENT_SERVICE_kTCCServiceExposureNotification</key>
10  <string>Only one region can notify you of possible exposure. Details associated with possible exposures—such as date, duration, and Bluetooth signal strength—will be shared. These details help the app notify you of possible exposures.</string>
11  <key>REQUEST_ACCESS_INFO_SERVICE_kTCCServiceExposureNotification</key>
12  <string>Your iPhone can securely collect and share random IDs with nearby devices. The app can use these IDs to notify you if you may have been exposed to COVID-19. The date, duration, and signal strength of an exposure will be shared with "%@".</string>
13  <key>REQUEST_LIMITED_AUTHORIZATION_BUTTON_TITLE_SERVICE_KTCCServicePrototype4Rights</key>
14  <string>Limited Proto4</string>
15  <key>REQUEST_ACCESS_DENY_kTCCServicePhotos</key>
16  <string>Don't Allow</string>
17  <key>REQUEST_ACCESS_SERVICE_kTCCServiceUserTracking</key>
18  <string>Allow "%@" to track your activity across other companies' apps and websites?</string>
19  <key>REQUEST_ACCESS_SERVICE_kTCCServiceReminders</key>
20  <string>"%" Would Like to Access Your Reminders?</string>
21  <key>REQUEST_ACCESS_SERVICE_kTCCServiceMediaLibrary</key>
22  <string>"%" would Like to access Apple Music, your music and video activity, and your media library</string>
23  <key>REQUEST_DEFAULT_PURPOSE_STRING_SERVICE_kTCCServiceBluetoothAlways</key>
24  <string>This will allow "%" to find and connect to Bluetooth accessories. This app may also use Bluetooth to know when you're nearby.</string>
25  <key>REQUEST_ACCESS_SERVICE_kTCCServiceFallDetection</key>
26  <string>Share Fall Detection Data With "%@"?</string>
27  <key>REQUEST_ACCESS_INFO_SERVICE_kTCCServiceFallDetection</key>
28  <string>If you choose to share, "%" can receive data from Apple Watch if a fall is detected and follow up in case help is needed.<!--
29  <key>REQUEST_ACCESS_SERVICE_kTCCServiceGameCenterFriends</key>
30  <string>Allow "%@" to connect you with your Game Center friends?</string>
```

XML ▾ Tab Width: 4 ▾ Ln 85, Col 35 ▾ INS

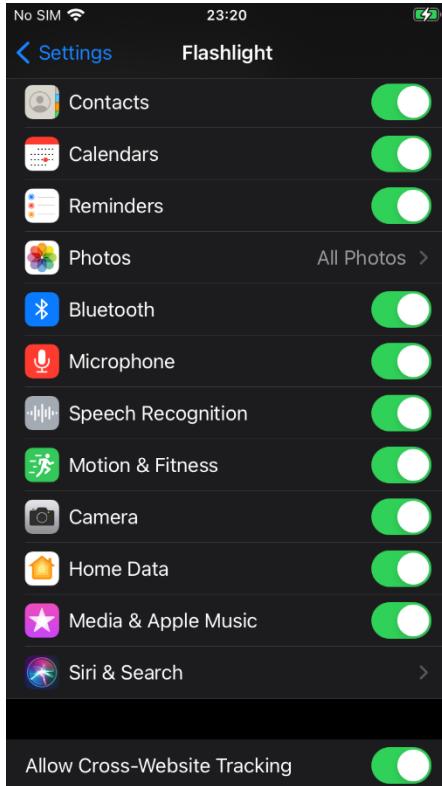
The available permissions

	service	Label in Settings	Description
✓	kTCCServiceCalendar	Calendars	“Access Your Calendar”
✓	kTCCServiceAddressBook	Contacts	“Access Your Contacts”
✓	kTCCServiceReminders	Reminders	“Access Your Reminders”
✓	kTCCServicePhotos	Photos (All Photos)	“Access your photos”
✗	kTCCServicePhotosAdd	Photos (Add Photos Only)	“Add to your Photos”
✓	kTCCServiceMediaLibrary	Media & Apple Music	“Access Apple Music, your music and video activity, and your media library”
✓	kTCCServiceBluetoothAlways	Bluetooth	“Find and connect to Bluetooth accessories. This app may also use Bluetooth to know when you’re nearby.”
□	kTCCServiceSpeechRecognition	Speech Recognition	“Access Speech Recognition”, “Speech data from this app will be sent to Apple to process your requests. This will also help Apple improve its speech recognition technology.”
✓	kTCCServiceMotion	Motion & Fitness	“Access Your Motion & Fitness Activity”
✗	kTCCServiceCamera	Camera	“Access the Camera”
✗	kTCCServiceMicrophone	Microphone	“Access the Microphone”
✓	kTCCServiceWillow	Home Data	“Access Your Home Data”

The available permissions (cont'd)

	service	Label in Settings	Description
X	kTCCServiceUserTracking	Allow Tracking	"Track your activity across other companies' apps and websites"
<input type="checkbox"/>	kTCCServiceWebKitIntelligentTrackingPrevention	Allow Cross-Website Tracking	0 means do allow, 2 means don't allow
✓	kTCCServiceLiverpool	<i>no visible effect</i>	maybe related to location access
✓	kTCCServiceUbiquity	<i>no visible effect</i>	maybe related to iCloud
<input type="checkbox"/>	kTCCServiceSensorKitBedSensingWriting	<i>no visible effect</i>	"Add Data for Research Purposes", "Record bed sensing Sensor & Usage data"
<input type="checkbox"/>	kTCCServiceGameCenterFriends	<i>no visible effect</i>	"Connect you with your Game Center friends"
<input type="checkbox"/>	kTCCServicePrototype3Rights	<i>no visible effect</i>	"Authorization to Test Service Proto3Right"
<input type="checkbox"/>	kTCCServicePrototype4Rights	<i>no visible effect</i>	"Authorization to Test Service Proto4Right"
<input type="checkbox"/>	kTCCServiceFallDetection	<i>no visible effect</i>	"Receive data from Apple Watch if a fall is detected and follow up in case help is needed"
<input type="checkbox"/>	kTCCServiceSiri	<i>no visible effect</i>	"Some of your %@ data will be sent to Apple to process your requests."
<input type="checkbox"/>	kTCCServiceBluetoothPeripheral	<i>no visible effect</i>	"Make data available to nearby Bluetooth devices even when you're not using the app"
<input type="checkbox"/>	kTCCServiceCalls	<i>no visible effect</i>	"Receive VoIP Calls in the Background"
✓	kTCCServiceExposureNotification	Exposure Notifications	"Your iPhone can securely collect and share random IDs with nearby devices. The app can use these IDs to notify you if you may have been exposed to COVID-19. The date, duration, and signal strength of an exposure will be shared."

ALL THE PERMISSIONS!



We're missing the location permission

```
#!/bin/bash
# Adapted after: https://stackoverflow.com/a/53875499 and
#                  https://stackoverflow.com/a/29548123
NEEDLE="com.bryceco.GoMap"

find / -name '*.*db' -print0 | while IFS= read -r -d '' file; do
    for X in $(sqlite3 $file .tables); do
        sqlite3 $file "SELECT * FROM $X;" | grep >/dev/null $NEEDLE
        && echo "Found in file '$file', table '$X'";
    done
done
```

It's not quite as simple

Found in file '/private/var/mobile/Library/Caches/com.apple.appstored/storeUser.db', table '**launch_events**'
Found in file '/private/var/mobile/Library/Caches/com.apple.appstored/storeUser.db', table '**purchase_history_apps**'
Found in file '/private/var/mobile/Library/Caches/com.apple.appstored/storeUser.db', table '**current_apps_crossfire**'
Found in file '/private/var/mobile/Library/TCC/TCC.db', table '**access**'
Found in file '/private/var/mobile/Library/DuetExpertCenter/_ATXDataStore.db', table '**anchorModelTrainingData**'
Found in file '/private/var/mobile/Library/DuetExpertCenter/_ATXDataStore.db', table '**appInfo**'
Found in file '/private/var/mobile/Library/FrontBoard/applicationState.db', table '**application_identifier_tab**'
Found in file '/private/var/mobile/Library/FrontBoard/applicationState.db', table '**kvs_debug**'
Found in file '/private/var/mobile/Library/CoreDuet/Knowledge/knowledgeC.db', table '**ZOBJECT**'
Found in file '/private/var/Keychains/Analytics/trust_analytics.db', table '**hard_failures**'

Do we have to dust off our Objective C skills?

```
139         else {
140             FR_Log(@"Failed to retrieve TCC information for %@", bundleId);
141         }
142         CFRelease(bundle);
143     }
144     else {
145         FR_Log(@"Cannot create bundle for %@", bundle);
146     }
147 }
148 else {
149     FR_Log(@"Use list from caches.");
150 }
151 CLAuthorizationStatus status = [CLLocationManager _authorizationStatusForBundleIdentifier:bundleId bundle:nil];
152 if (permissionList.count == 0 && (status == kCLAuthorizationStatusNotDetermined || status == kCLAuthorizationStatusRestricted)) {
153     FR_Log(@"No permissions requested! Do not show reset permission");
154     return originalShortcutItems;
155 }
156 FR_Log(@"Requested: %@, locationStatus: %@", permissionList, status);
157
158 SBSApplicationShortcutItem *shortcutItem = [[objc_getClass("SBSApplicationShortcutItem") alloc] init];
159 shortcutItem.type = tweakIdentifier;
160 shortcutItem.localizedTitle = @"Reset permission";
161 shortcutItem.bundleIdentifierToLaunch = bundleId;
162
163 NSMutableArray *newShortcutItems = originalShortcutItems ? [originalShortcutItems mutableCopy] : [NSMutableArray arrayWithCapacity:1];
164 [newShortcutItems addObject:shortcutItem];
165 FR_Log(@"New shortcutItems: %@", newShortcutItems);
166 return newShortcutItems;
167 }
168 }
```

<https://github.com/lucalz-Idx/ForceReset/blob/de004718c1ebde9a80dc686040853089ceea20a0/Tweak.x#L151-L155>

Enter Frida

FRIDA

[OVERVIEW](#) [DOCS](#) [NEWS](#) [CODE](#) [CONTACT](#)

Dynamic instrumentation toolkit for developers, reverse-engineers, and security researchers.

Scriptable

Inject your own scripts into black box processes. Hook any function, spy on crypto APIs or trace private application code, no source code needed. Edit, hit save, and instantly see the results. All without compilation steps or program restarts.

Portable

Works on Windows, macOS, [GNU/Linux](#), iOS, Android, and QNX. Install the Node.js bindings from [npm](#), grab a Python package from [PyPI](#), or use Frida through its [Swift bindings](#), [.NET bindings](#), [Qt/Qml bindings](#), or [CAPI](#).

Free

Frida is and will always be [free software](#) (free as in freedom). We want to empower the next generation of developer tools, and help other free software developers achieve interoperability through reverse engineering.

Battle-tested

We are proud that [NowSecure](#) is using Frida to do fast, deep analysis of mobile apps [at scale](#). Frida has a comprehensive test-suite and has gone through years of rigorous testing across a broad range of use-cases.

<https://frida.re/>

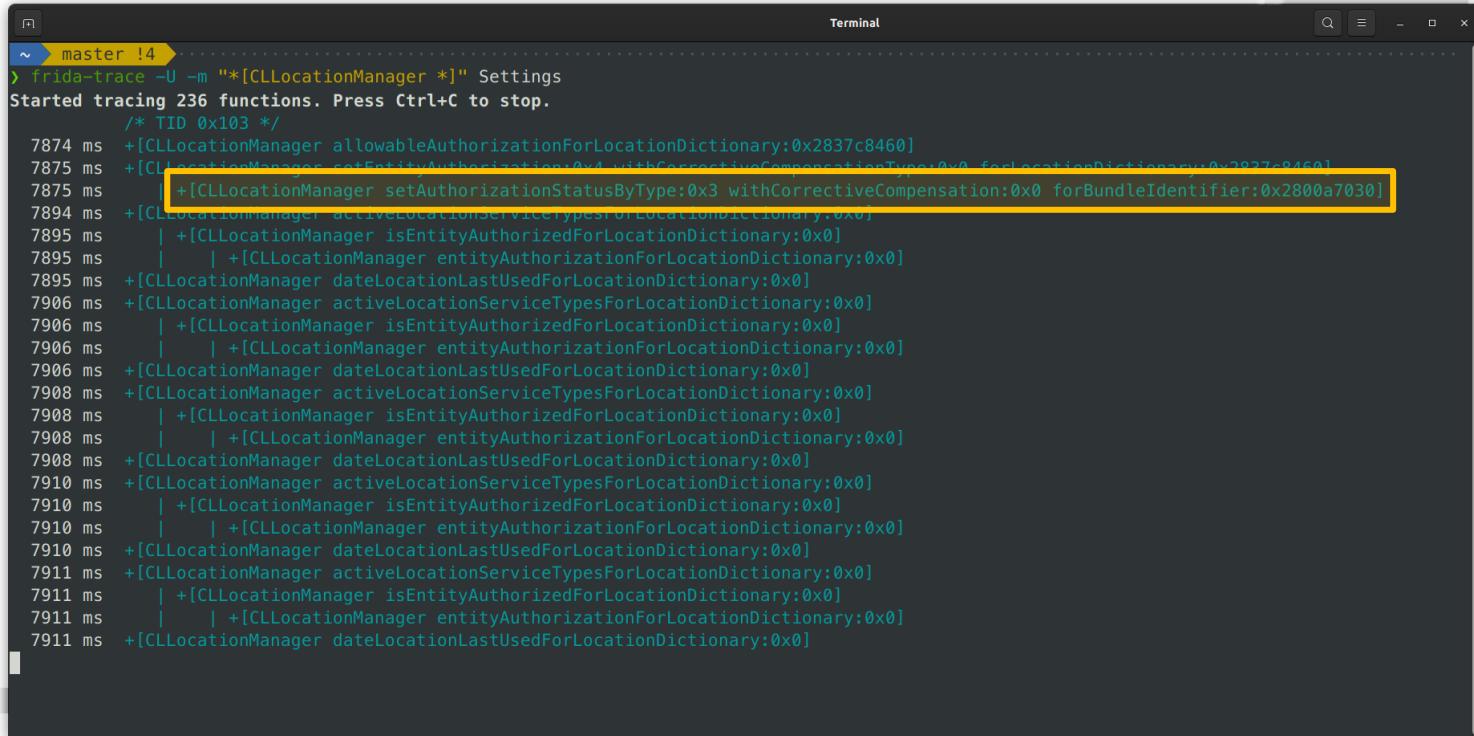
Frida is great

The screenshot shows a terminal window with the following content:

```
> frida -U Flashlight
  /__|  Frida 14.2.18 - A world-class dynamic instrumentation toolkit
 |__|  Commands:
 >_  help      -> Displays the help system
 ._. object?   -> Display information about 'object'
 ._. exit/quit -> Exit
 ._. More info at https://frida.re/docs/home/

[iOS Device::Flashlight]-> function bundleURL(id) {
    var all_apps = ObjC.classes.LSApplicationWorkspace.defaultWorkspace().allInstalledApplications();
    for (var i = 0; i < all_apps.count(); i++) {
        var app = all_apps.objectAtIndex_(i);
        if (app.bundleIdentifier().toString() == id) return app.bundleURL();
    }
}
[iOS Device::Flashlight]-> var CFBundleCreate_addr = Module.findExportByName(null, "CFBundleCreate");
var CFBundleCreate = new NativeFunction(CFBundleCreate_addr, "pointer", [ "pointer", "pointer" ]);
[iOS Device::Flashlight]-> var KCFAllocatorDefault = Module.findExportByName(null, "KCFAllocatorDefault");
[iOS Device::Flashlight]-> var b = bundleURL("com.7thq.Flashlight");
[iOS Device::Flashlight]-> var bundle = CFBundleCreate(KCFAllocatorDefault, b);
[iOS Device::Flashlight]-> bundle
"0x121f07bf0"
[iOS Device::Flashlight]-> (new ObjC.Object(bundle)).toString()
"CFBundle 0x121f07bf0 </private/var/containers/Bundle/Application/917CDF6B-D1CE-4BF4-AD16-C8D69E3D5B0C/iPhone4Flashlight.app (executable, loaded)"
[iOS Device::Flashlight]-> var TCCAccessCopyInformationForBundle_addr = Module.findExportByName("/System/Library/Frameworks/TCC.framework/TCC", "TCCAccessCopyInformationForBundle");
[iOS Device::Flashlight]-> var TCCAccessCopyInformationForBundle = new NativeFunction(TCCAccessCopyInformationForBundle_addr, "pointer", [ "pointer" ]);
[iOS Device::Flashlight]-> TCCAccessCopyInformationForBundle(bundle)
"0x0"
[iOS Device::Flashlight]->
[iOS Device::Flashlight]->
[iOS Device::Flashlight]-> ObjC.classes.CLLocationManager.setAuthorizationStatusByType_forBundleIdentifier_
setAuthorizationPromptMapDisplayEnabled_
setAuthorizationStatusByType_forBundleIdentifier_
setAuthorizationStatusByType_forBundle_
setAuthorizationStatusByType_withCorrectiveCompensation_forBundleIdentifier_
setAuthorizationStatusByType_withCorrectiveCompensation_forBundle_
setAuthorizationStatusByBundleIdentifier_
setAuthorizationStatus_forBundle_
```

Frida is (really!) great



```
master !4
> frida-trace -U -m "*[CLLocationManager *]" Settings
Started tracing 236 functions. Press Ctrl+C to stop.
    /* TID 0x103 */
7874 ms +[CLLocationManager allowableAuthorizationForLocationDictionary:0x2837c8460]
7875 ms +[CLLocationManager setEntityAuthorization:0x1 withCorrectiveCompensationType:0x0 forLocationDictionary:0x2837c8460]
7875 ms | +[CLLocationManager setAuthorizationStatusByType:0x3 withCorrectiveCompensation:0x0 forBundleIdentifier:0x2800a7030]
7894 ms +[CLLocationManager activeLocationServiceTypesForLocationDictionary:0x0]
7895 ms | +[CLLocationManager isEntityAuthorizedForLocationDictionary:0x0]
7895 ms | | +[CLLocationManager entityAuthorizationForLocationDictionary:0x0]
7895 ms +[CLLocationManager dateLocationLastUsedForLocationDictionary:0x0]
7906 ms +[CLLocationManager activeLocationServiceTypesForLocationDictionary:0x0]
7906 ms | +[CLLocationManager isEntityAuthorizedForLocationDictionary:0x0]
7906 ms | | +[CLLocationManager entityAuthorizationForLocationDictionary:0x0]
7906 ms +[CLLocationManager dateLocationLastUsedForLocationDictionary:0x0]
7908 ms +[CLLocationManager activeLocationServiceTypesForLocationDictionary:0x0]
7908 ms | +[CLLocationManager isEntityAuthorizedForLocationDictionary:0x0]
7908 ms | | +[CLLocationManager entityAuthorizationForLocationDictionary:0x0]
7908 ms +[CLLocationManager dateLocationLastUsedForLocationDictionary:0x0]
7910 ms +[CLLocationManager activeLocationServiceTypesForLocationDictionary:0x0]
7910 ms | +[CLLocationManager isEntityAuthorizedForLocationDictionary:0x0]
7910 ms | | +[CLLocationManager entityAuthorizationForLocationDictionary:0x0]
7910 ms +[CLLocationManager dateLocationLastUsedForLocationDictionary:0x0]
7911 ms +[CLLocationManager activeLocationServiceTypesForLocationDictionary:0x0]
7911 ms | +[CLLocationManager isEntityAuthorizedForLocationDictionary:0x0]
7911 ms | | +[CLLocationManager entityAuthorizationForLocationDictionary:0x0]
7911 ms +[CLLocationManager dateLocationLastUsedForLocationDictionary:0x0]
```

Programmatically setting the location permission

- To set the location permission using Frida (in the context of the Settings app):

```
ObjC.classes.CLLocationManager
    .setAuthorizationStatusByType_forBundleIdentifier_
        (<value>, "<bundle_id>"
    ) ;
```

- Empirically determined values:

- 0: Ask every time, 2: Never, 3: Always, 4: While using the app

- To check:

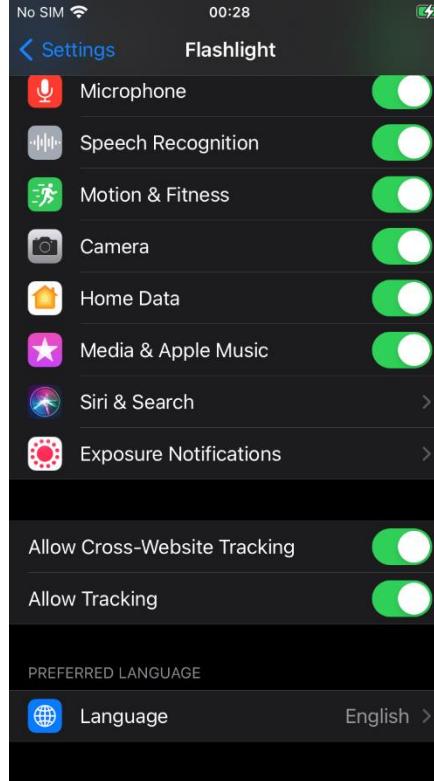
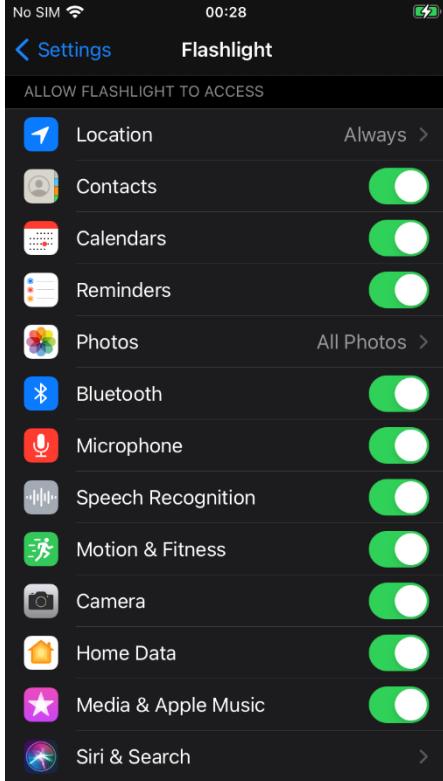
```
// For the running app.
```

```
ObjC.classes.CLLocationManager.authorizationStatus() ;
```

```
// For an arbitrary app.
```

```
ObjC.classes.CLLocationManager
    .authorizationStatusForBundleIdentifier_("<bundle_id>") ;
```

(Truly) ALL THE PERMISSIONS!



Programmatically seeding the clipboard

- Knowing that, seeding the keyboard is easy:

```
ObjC.classes.UIPasteboard.generalPasteboard()  
    .setString_("<string>");
```

Background noise filter



Use Apple products on enterprise networks

Learn which hosts and ports are required to use your Apple products on enterprise networks.

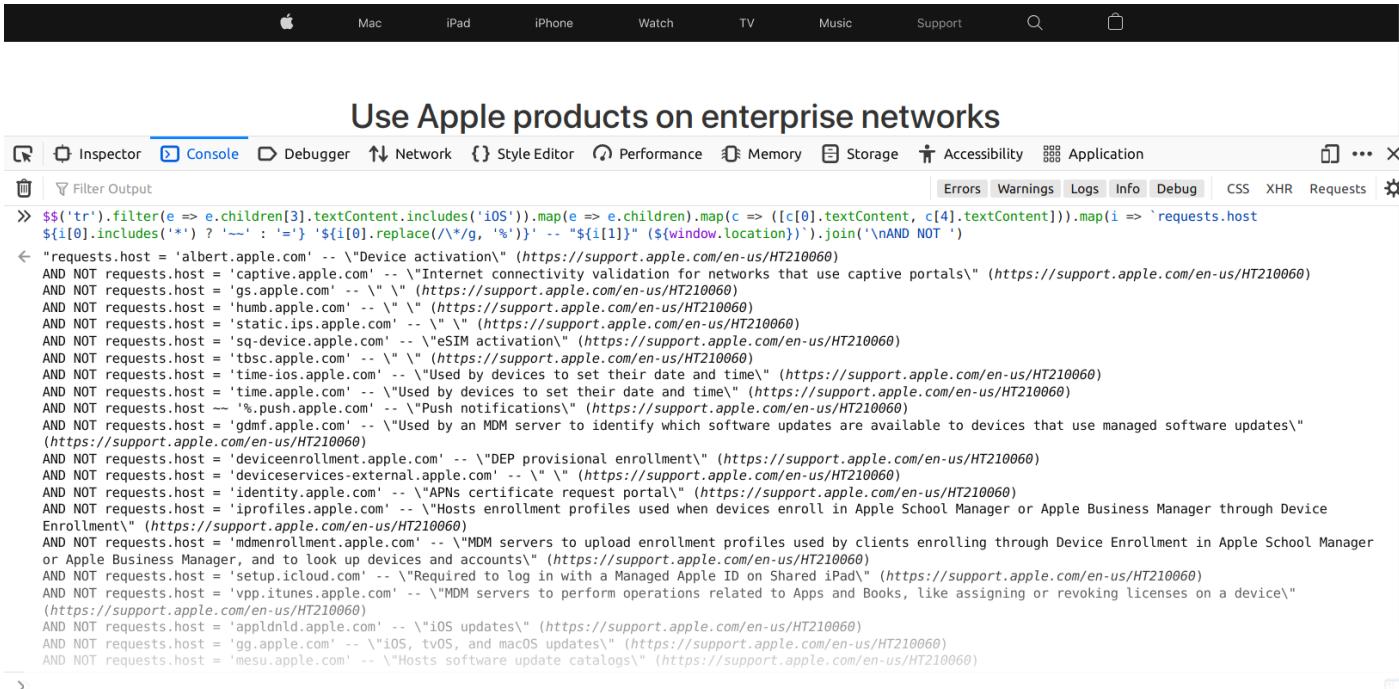
Device setup

Access to the following hosts might be required when setting up your device, or when installing, updating or restoring the operating system.

Hosts	Ports	Protocol	OS	Description	Supports proxies
albert.apple.com	443	TCP	iOS, tvOS, and macOS	Device activation	Yes
captive.apple.com	443, 80	TCP	iOS, tvOS, and macOS	Internet connectivity validation for networks that use captive portals	Yes
gs.apple.com	443	TCP	iOS, tvOS, and macOS		Yes
humb.apple.com	443	TCP	iOS, tvOS, and macOS		Yes
static.ips.apple.com	443, 444, 445	TCP	iOS, tvOS, and macOS		Yes

<https://support.apple.com/en-us/HT210060>

Background noise filter



```
» $('tr').filter(e => e.children[3].textContent.includes('iOS')).map(e => e.children).map(c => ([c[0].textContent, c[4].textContent])).map(i => `requests.host
${i[0]}.includes('*') ? '~' : '} ${i[0].replace(/\$/g, '%')} -- "${i[1]}" (${window.location})`).join('\nAND NOT ')
← "requests.host = 'albert.apple.com' -- \Device activation\" (https://support.apple.com/en-us/HT210060)
AND NOT requests.host = 'captive.apple.com' -- \"Internet connectivity validation for networks that use captive portals\" (https://support.apple.com/en-us/HT210060)
AND NOT requests.host = 'gs.apple.com' -- \" \" (https://support.apple.com/en-us/HT210060)
AND NOT requests.host = 'humb.apple.com' -- \" \" (https://support.apple.com/en-us/HT210060)
AND NOT requests.host = 'static.ips.apple.com' -- \" \" (https://support.apple.com/en-us/HT210060)
AND NOT requests.host = 'sq-device.apple.com' -- \"\neSIM activation\" (https://support.apple.com/en-us/HT210060)
AND NOT requests.host = 'tbsc.apple.com' -- \" \" (https://support.apple.com/en-us/HT210060)
AND NOT requests.host = 'time-ios.apple.com' -- \"Used by devices to set their date and time\" (https://support.apple.com/en-us/HT210060)
AND NOT requests.host = 'time.apple.com' -- \"Used by devices to set their date and time.\" (https://support.apple.com/en-us/HT210060)
AND NOT requests.host = '%.push.apple.com' -- \"Push notifications\" (https://support.apple.com/en-us/HT210060)
AND NOT requests.host = 'gdmf.apple.com' -- \"Used by an MDM server to identify which software updates are available to devices that use managed software updates\" (https://support.apple.com/en-us/HT210060)
AND NOT requests.host = 'deviceenrollment.apple.com' -- \"DEP provisional enrollment\" (https://support.apple.com/en-us/HT210060)
AND NOT requests.host = 'deviceservices-external.apple.com' -- \" \" (https://support.apple.com/en-us/HT210060)
AND NOT requests.host = 'identity.apple.com' -- \"APNs certificate request portal\" (https://support.apple.com/en-us/HT210060)
AND NOT requests.host = 'iprofiles.apple.com' -- \"Hosts enrollment profiles used when devices enroll in Apple School Manager or Apple Business Manager through Device Enrollment\" (https://support.apple.com/en-us/HT210060)
AND NOT requests.host = 'mdmenrollment.apple.com' -- \"MDM servers to upload enrollment profiles used by clients enrolling through Device Enrollment in Apple School Manager or Apple Business Manager, and to look up devices and accounts\" (https://support.apple.com/en-us/HT210060)
AND NOT requests.host = 'setup.icloud.com' -- \"Required to log in with a Managed Apple ID on Shared iPad\" (https://support.apple.com/en-us/HT210060)
AND NOT requests.host = 'vpp.itunes.apple.com' -- \"MDM servers to perform operations related to Apps and Books, like assigning or revoking licenses on a device\" (https://support.apple.com/en-us/HT210060)
AND NOT requests.host = 'appldld.apple.com' -- \"iOS updates\" (https://support.apple.com/en-us/HT210060)
AND NOT requests.host = 'gg.apple.com' -- \"iOS, tvOS, and macOS updates\" (https://support.apple.com/en-us/HT210060)
AND NOT requests.host = 'mesu.apple.com' -- \"Hosts software update catalogs\" (https://support.apple.com/en-us/HT210060)
```

<https://support.apple.com/en-us/HT210060>

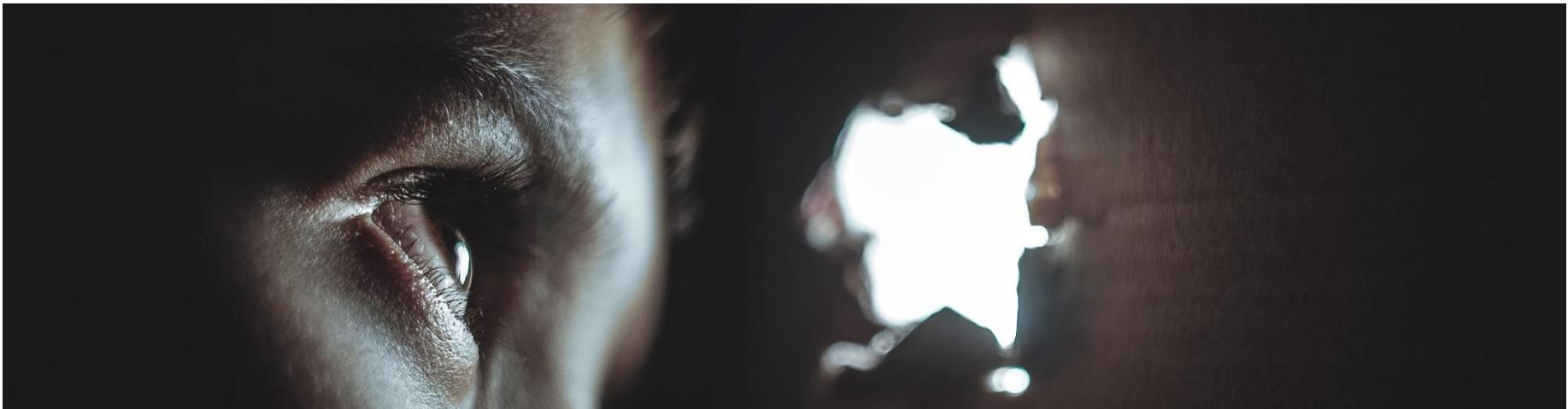


Image: Dmitry Ratushny (Unsplash license)

A first look

Is iOS really more privacy-friendly than Android?

App Store



Audible audiobooks & podcasts 4+

Listen to audio books, stories

Audible, Inc.

#2 in Books

★★★★★ 4.9 • 3.7M Ratings

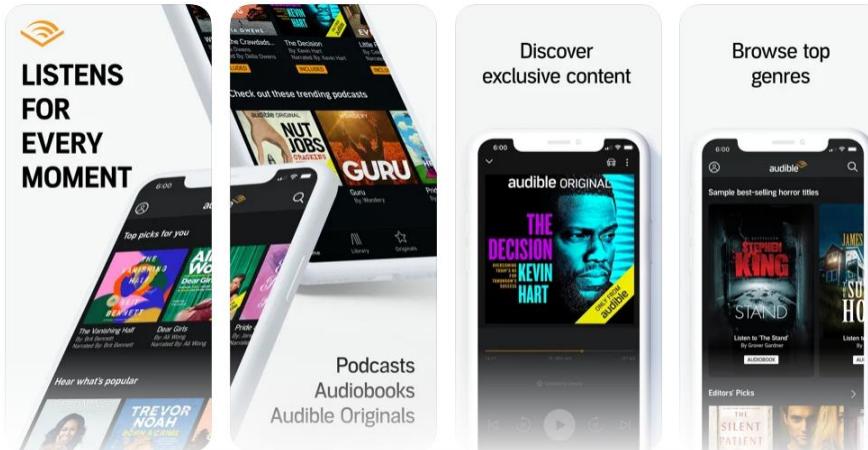
Free · Offers In-App Purchases

Screenshots

[iPhone](#)

[iPad](#)

[Apple Watch](#)



<https://apps.apple.com/us/app/audible-audiobooks-podcasts/id379693831>

Audible

POST <https://control.kochava.com/track/json>



```
"action": "install",
"sdk_protocol": "16",
"data": {
    "os_version": "iOS 14.5.1",
    "device": "iPhone10,4",
    "disp_h": 1334,
    "disp_w": 750,
    "device model": "iPhone",
    "identity_link": {
        "marketingcloudvisitorid": "49728088823015189425548504973918371147"
    },
    "app_short_string": "3.48",
    "app name": "Audible",
    "locale": "en_DE",
    "device_orientation": "portrait",
    "is_genuine": false,
    "uptime": 0.2443,
    "app_limit_tracking": true,
    "usertime": 1624132516,
    "device_limit_tracking": true,
    "volume": 0.125,
    "network_conn_type": "wifi",
},
"bms": 1621257545080,
"notifications_enabled": true,
"idfv": "02185687-FB54-4F8E-82C5-5E6DE159943D",
"system_ua": "Mozilla/5.0 (iPhone; CPU iPhone OS 14_5_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148".
"screen_brightness": 0.0226,
"ad_services_token_time": 1624132516,
"battery_level": 100,
"package": "com.audible.iphone",
"language": "en-DE",
"app_tracking_transparency": { "att": false },
"battery_status": "full",
"app_version": "665",
"timezone": "Europe/Berlin"
},
"nt_id": "F6CB7FBC-51E89335-4608-4D00-8BCD-4EC76055F160",
"kochava_device_id": "KI1624132516T5FA1F93998744B36880D477DB976FB15",
"send_date": "2021-06-19T19:55:17.731Z",
"sdk_version": "iOSTracker 4.5.0"
```

App Store



PayPal: Mobile Cash 4+

Money App & Mobile Wallet

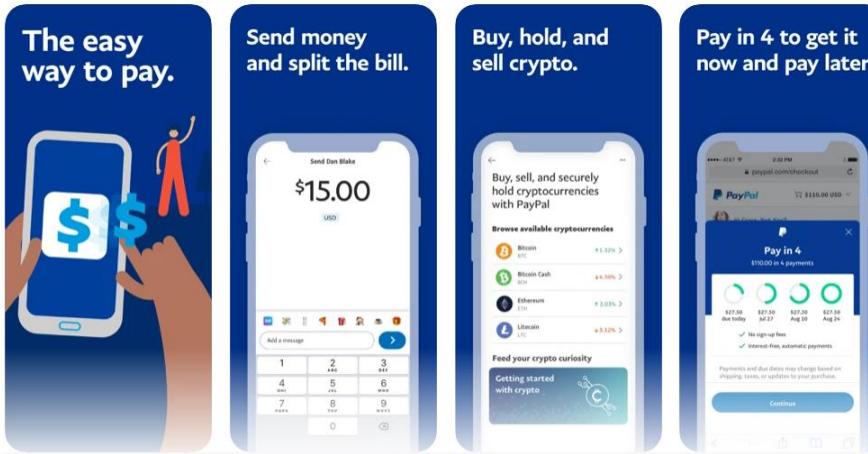
PayPal, Inc.

#3 in Finance

★★★★★ 4.8 • 5.6M Ratings

Free

iPhone Screenshots



<https://apps.apple.com/us/app/paypal-mobile-cash/id283646709>

PayPal

POST <https://api-m.paypal.com/v1/mfsauth/proxy-auth/token>

```
"app_id": "com.yourcompany.PPClient",
"app_guid": "8384FB18-571B-44F0-9809-40F040EB0961",
"source_app_version": "7.40.5",
"cloud_identifier":
  "a2a058f2-9367-4920-8190-bc504b4c90d9",
"local_identifier":
  "8b8cc6fa-aa04-4109-a27d-ae957c8db00d",
"linker_id": "71842c5e-88c0-45c7-a482-0a9cb9d71d58",
"risk_comp_session_id":
  "26afa6d4-1b33-483f-ba2e-169d431f75a2",
"dc_id": "b07f13e37dde7971d431b95a263a55f0",
"timestamp": 1624222636861,
"device_uptime": 807997862,
"locale_lang": "en",
"device_name": "R2G150Lv20",
"os_type": "iOS",
"os_version": "14.5.1",
"device_model": "iPhone10,4",
"is_rooted": true,
"is_emulator": false,
"TouchIDEnrolled": "false",
"PasscodeSet": "true",
"email_configured": true,
"sms_enabled": true,
```

```
"location_auth_status": "authorizedWhenInUse",
"total_storage_space": 127968497664,
"tz_name": "Europe/Berlin",
"conn_type": "wifi",
"ssid": "WLAN3.ALTPETER.ME",
"bssid": "34:81:c4:dc:36:1",
"ip_addresses": [
  "10.0.0.83",
  "fd31:4159::cf9:d932:11c3:bede",
  "fd31:4159::5998:c752:9f96:5e30",
  "fd31:4159::30a2:88d6:66c9:125f",
  "2003:dd:af1c:ab00:cc6:9a3a:7bf5:90d7",
  "2003:dd:af1c:ab00:69d6:4c4d:cabc:5168",
  "2003:dd:af1c:ab00:c81:68e1:2199:631",
  "fd31:4159::c9a3:68ec:ea3f:f085",
  "fe80::f631:960f:130f:5dc1",
  "fe80::87bf:b362:c6d3:616f"
],
"proxy_setting":
  "host=10.0.0.68,port=8080,type=kCFProxyTypeHTTPS",
"location": {
  "lng": 10.564191494436333,
  "lat": 52.23529052734375, "acc": 65
}
```



App Store



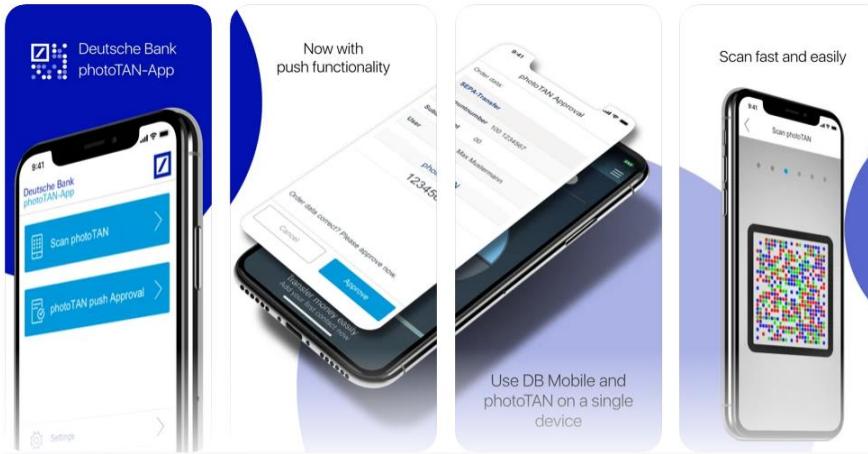
Deutsche Bank photoTAN

Deutsche Bank AG

★★★★★ 4.8 • 480 Ratings

Free

iPhone Screenshots



<https://apps.apple.com/us/app/deutsche-bank-phototan/id937259592>

DB photoTAN

```
POST https://col.eum-appdynamics.com/
eumcollector/mobileMetrics?version=2

{
    "cpuCount": 6,
    "av": "3.1.3",
    "mv": "3.1.3.5.0",
    "dmo": "iPhone10,4",
    "sessionCounter": -1,
    "images": [
        {
            "imageUUID": "b2b882c11d213146ae3009417cdd3bb5",
            "baseAddress": 4367171584,
            "imageSize": 4472832,
            "codeType": {
                "type": 16777228,
                "subType": 0
            },
            "imagePath":
                "/private/var/containers/Bundle/Application/5D1
                 D54AD-3A7E-4261-9665-3B34DECF590F/DB_PhotoTAN_
                 PROD.app/DB_PhotoTAN_PROD"
        },
        {
            "imageUUID": "bf3b96c2bd3b390ebfcf33656588c86e",
            "baseAddress": 4372971520,
            "imageSize": 16384,
            "codeType": {
                "type": 16777228,
                "subType": 0
            },
            "imagePath":
                "/usr/lib/substrate/SubstrateBootstrap.dylib"
        },
        {
            "imageUUID": "d8c72cf1da53dc497b2ce83171e108d",
            "baseAddress": 7156641792,
            "imageSize": 958464,
            "codeType": {
                "type": 16777228,
                "subType": 0
            },
            "imagePath":
                "/System/Library/Frameworks/CoreTelephony.frame
                 work/CoreTelephony"
        },
        // [...]
    ]
}
```

App Store



eBay - Buy, Sell, and Save 12+

Sneakers, Watches, Tech & More

eBay Inc.

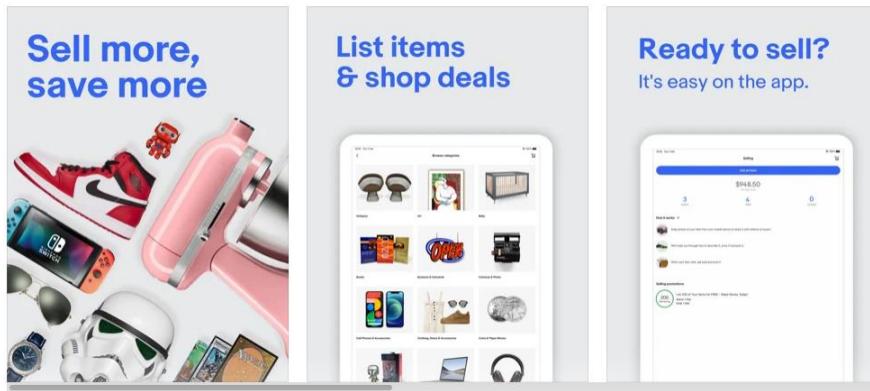
Designed for iPad

#9 in Shopping

4.8 • 2.7M Ratings

Free

Screenshots iPad iPhone iMessage



Buy, sell, and discover deals on the things you love most—from rare sneakers and luxury watches, to
treasures, trading cards, and top tech.

<https://apps.apple.com/us/app/ebay-buy-sell-and-save/id282614216>

POST <https://mobiletelemetry.ebay.com/aplsio/v1/error>

```
"appInfo": {  
    "appBuildConfiguration": "release",  
    "appBuildIdentifier": "2412",  
    "appVersion": "6.17.0",  
    "appVersionHash":  
        "9IA9pz28zzmAnmHWcQ2sZ4NyjbaS4ReTNZxmKena51kpCIu  
        9fSNBQfaBKWx3QNL72HZtRQCIFufs1hn0VRBBAw==",  
    "vendorAppId": "com.ebay.iphone"  
},  
"deviceInfo": {  
    "clientType": "mobile",  
    "emulator": false,  
    "localeIdentifier": "en_DE",  
    "lowPowerModeEnabled": false,  
    "manufacturer": "Apple",  
    "model": "iPhone10,4",  
    "osName": "iOS",  
    "osVersion": "14.5.1",  
    "physicalMemory": 2070495232,  
    "processorArchitecture": "arm",  
    "processorCount": 6,  
    "processorWordSize": 64,  
    "systemUptime": 763195.016,  
    "thermalState": "nominal",  
    "timeZone": "Europe/Berlin",  
    "userLanguage": "en"  
},  
"ebayConfiguration": {  
    "configVersion": "W/\"77\"",  
    "countryCode": "de",  
    "environment": "production",  
    "globalId": "EBAY-DE",  
    "mrollp": 75.58  
},  
"networkInfo": [{  
    "constrained": false,  
    "expensive": false,  
    "network": "wifi",  
    "networkScore": 0.6,  
    "networkSubtype": "unknown",  
    "supportsIPv4": true,  
    "supportsIPv6": true  
}],  
"sessionGuid": "288af0e417aedc9e31a7cf4001d35186",  
"userInfo": {  
    "deviceGuid": "288aed6817a35f1f474999b001568ca8"  
}
```

App Store



Hill Climb Racing 9+

Race and drive uphill to win!

Fingersoft

Designed for iPad

#21 in Racing

★★★★★ 4.6 • 45.6K Ratings

Free - Offers In-App Purchases

Screenshots

iPad

iPhone

Apple TV



PLAY THE ORIGINAL!



AIR TIME
+50

PLAY IN DOZENS OF LEVELS!



UNLOCK OVER 30 VEHICLES!

One of the most addictive and entertaining physics based driving game ever made! And it's free!

The Original - Play now!

Meet Newton Bill, the young aspiring uphill racer. He is about to embark on a journey that takes him [more](#)

What's New

- Power ups

Power up your life with the all-new double bonus, invader, and mega fuel!

Version History

Version 1.50.0

<https://apps.apple.com/us/app/hill-climb-racing/id564540143>

Hill Climb Racing

POST <https://live.chartboost.com/api/config>

```
"device_name": "R2G150Lv20",
"dark_mode": true,
"timezone": "GMT+02:00",
"disk_space": 115240787968,
"use_metric": true,
"currency": "EUR",
"os": "14 5 1",
"audio_output_type": ["Speaker"],
"n": 150,
"w": 1334,
"country": "DE",
"carrier": {
    "mobile_network_code": null,
    "iso_country_code": null,
    "mobile_country_code": null,
    "carrier_name": null
},
"screen_fps": 60,
"last_bootup": 1621257545,
"session_ID": "87e8c86f7fa2ee329a72d15a618676d70b25a811",
"calendar": "gregorian",
"scr_up_time": 765422,
"audio_input_name": [],
"input_language": ["en-GB", "de-DE", "emoji"],
"incr_contrast": false,
"total_disk": 127968497664,
"audio_volume": 0.125,
"rooted_device": true,
"screen_bright": 0.35547930002212524,
"is_portrait": false,
"charging": false,
"device_type": "iPhone10,4",
"audio_input_type": [],
"model": "iPhone",
"language": "en-DE",
"mobile_network": 0,
"audio_output_name": ["Speaker"],
"limit_ad_tracking": true,
"retina": true,
"identity": "eyJpZmEiOiIwMDAwMDAwMC0wMDAwLTAwMDAtMDAwMC0wMDAwMDAwMDAiLCJpZnYiOiIyNDgzMzRERS1EMjc5LTQ5OTQtQUQ0QS04RDQzMUQwNkUxMjkiLCJjYl9pZCI6I1F6QXhNVE5EU1VJdE1VRTJSQzAwTlRkQkxVRTFSall0TwtFM01FRXpPVFZETUVKRSJ9"
```

App Store



Pacer Pedometer & Step Tracker 4.4

Walking, Weight Loss & Health

Pacer Health, Inc

#56 in Health & Fitness

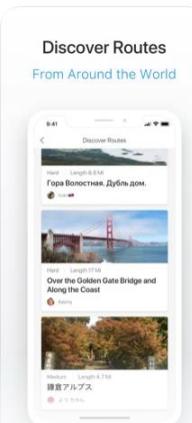
★★★★★ 4.9 • 146.6K Ratings

Free - Offers In-App Purchases

Screenshots

[iPhone](#)

[Apple Watch](#)



<https://apps.apple.com/us/app/pacer-pedometer-step-tracker/id600446812>

Pacer

POST <https://api.pacer.cc/pacer/ios/api/v19/accounts/0/location>

```
client_time=2021-06-20T17:34:30.162+02:00&client_timezone_offset=120&system_location={  
    "sub_locality_level_1": "Südstadt-Rautheim",  
    "iso_country_code": "DE",  
    "administrative_area": "Lower Saxony",  
    "extras": null,  
    "formatted_address": "Schreinerweg 738126 BraunschweigGermany",  
    "sub_thoroughfare": "7",  
    "thoroughfare": "Schreinerweg",  
    "display_name": "Südstadt-Rautheim, Braunschweig",  
    "timezone_name": "Europe\Berlin",  
    "sub_administrative_area": "Brunswick",  
    "postal_code": "38126",  
    "coordinate": {  
        "longitude": 10.564214352048731,  
        "latitude": 52.235299152630958  
    },  
    "country": "Germany",  
    "name": "Schreinerweg 7",  
    "locality": "Braunschweig"  
}
```



NewsBreak: Local Everything 12+

News Updates, Alerts, & More

Particle Media Inc.

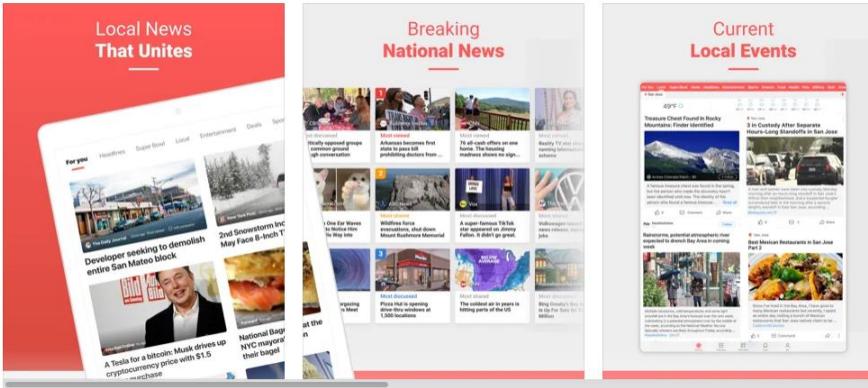
Designed for iPad

#4 in News

4.7 • 647.7K Ratings

Free

Screenshots iPad iPhone Apple Watch



Stay up-to-date on news that you're interested in! The Summer Olympics start July 23, are you ready?
NewsBreak will keep you updated & highlight what's right to your inbox!

<https://apps.apple.com/us/app/newsbreak-local-everything/id1132762804>

NewsBreak

GET <https://api.newsbreakapp.de/Website/user/binding-location>

```
accuracy=53.29285929263329
appid=newsbreak
countries=DE
cv=17.0.0.71
deviceID=0EC765F5-5CCE-44D2-8CF5-B3458F258E11
device_id_ios=0EC765F5-5CCE-44D2-8CF5-B3458F258E11
distribution=com.apple.Appstore
geo_data={
    "locality": "Braunschweig", "country": "Deutschland", "subLocality": "Südstadt-Rautheim",
    "subThoroughfare": "7", "administrativeArea": "Niedersachsen", "ISOcountryCode": "DE",
    "postalCode": "38126", "thoroughfare": "Schreinerweg"
}
languages=de
latitude=52.23529241882057
longitude=10.56423577475987
net=wifi
pf_token_id=000J4bYK
platform=0
profile_id=000J4bYK
version=020066
```

App Store



4 Pics 1 Word 12+

The Classic

LOTUM GmbH

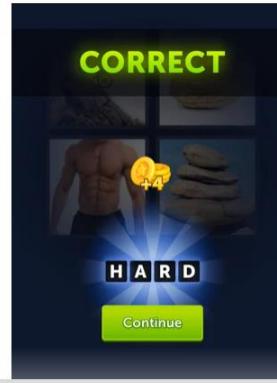
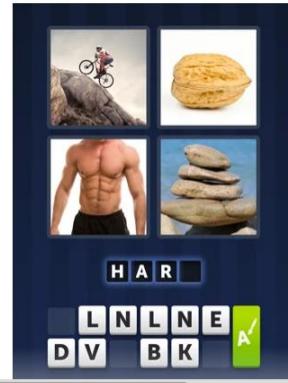
Designed for iPad

#56 in Trivia

★★★★★ 4.7 • 81.9K Ratings

Free - Offers In-App Purchases

Screenshots iPad iPhone



THE #1 HIT WITH OVER 250,000,000 PLAYERS WORLDWIDE!
4 pictures. That have 1 word in common - What is it?

<https://apps.apple.com/us/app/4-pics-1-word/id595558452>

4 Pics 1 Word

POST https://graph.facebook.com/network_ads_common/

```
"ANON_ID": "XZ79F5056E-A25F-4016-BC4B-B36C2AC15F22", "ANALOG":  
  "{\"free_space\":111712808960,\"charging\":1,  
   \"accelerometer_x\":0.025421142578125,  
   \"available_memory\":16793600,  
   \"rotation_z\":-0.0018479675054550171,  
   \"rotation_y\":0.0037262949626892805,  
   \"rotation_x\":-0.0040666470304131508,  
   \"accelerometer_z\":-1.0014801025390625, \"battery\":100,  
   \"accelerometer_y\":0.0040130615234375,  
   \"total_memory\":2070495232}",  
  "COPPA": "0",  
  "USER_AGENT":  
    "Mozilla/5.0 (iPhone; CPU iPhone OS 14_5_1 like Mac OS X)  
     AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148  
      [FBAN/AudienceNetworkForiOS;FBDV/iPhone10,4;FBMD/D201AP;  
       FBSN/iOS;FBSV/14.5.1;FBLC/de_DE;FBVS/6.2.1;FBAB/de.lotum  
        .4pics1word;FBAV/60.14.1;FBBV/60170]",  
  "PLACEMENT_ID": "417220471689883_2814853778593195",  
  "LINKED_WITH_IOS_14_OR_ABOVE": "1",  
  "EVENTS_SEND_ATTEMPTS": "0",  
  "NUMADS_REQUESTED": "1",  
  "SESSION_ID": "422D74C5-61BC-45EB-AB7E-F94EFF53D5D3",  
  "IDFA": "00000000-0000-0000-0000-000000000000",  
  "APPVERS": "60.14.1",  
  "OSVERS": "14.5.1"
```

App Store



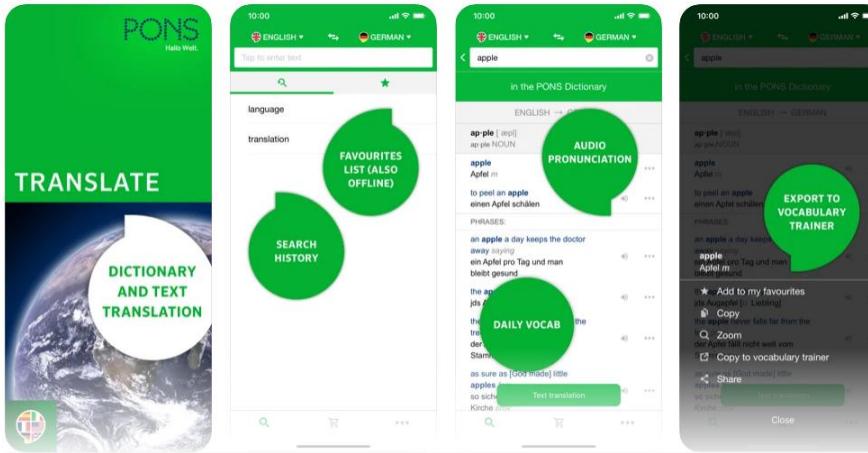
PONS Translate 4+

Dictionary and Text Translator
PONS GmbH

★★★★★ 4.7 • 416 Ratings

Free • Offers In-App Purchases

Screenshots iPhone iPad



<https://apps.apple.com/us/app/pons-translate/id577741918>

PONS

GET <https://api.pons.com>

/dict/search/autocomplete-json?q=LDDsvPqQdT&l=deen&lang=en-US

App Store



Poparazzi 12+

Take photos of your friends

TTYL Inc.

#86 in Photo & Video

★★★★★ 4.6 • 38K Ratings

Free

Screenshots iPhone iPad



<https://apps.apple.com/us/app/poparazzi/id1513680970>

Poparazzi

POST <https://poparazzi.com/api/contacts>

```
"data": [
  {
    "attributes": {
      "is_profile_photo": true,
      "last_name": "TBFFZbBYea",
      "phone_numbers": ["+4915557543434"],
      "full_name": "JGKfozntbF TBFFZbBYea",
      "clean_name": "JGKfozntbF TBFFZbBYea",
      "is_emoji": false,
      "first_name": "JGKfozntbF"
    },
    "type": "contacts",
    "id": "3A575DFF-C7FC-4F13-B40D-89D52F208C15:ABPerson"
  }
]
```



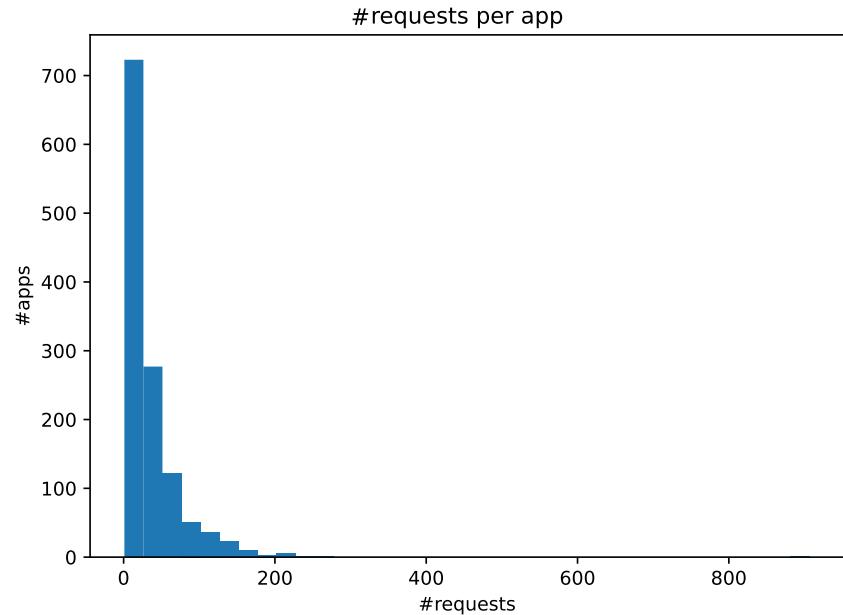
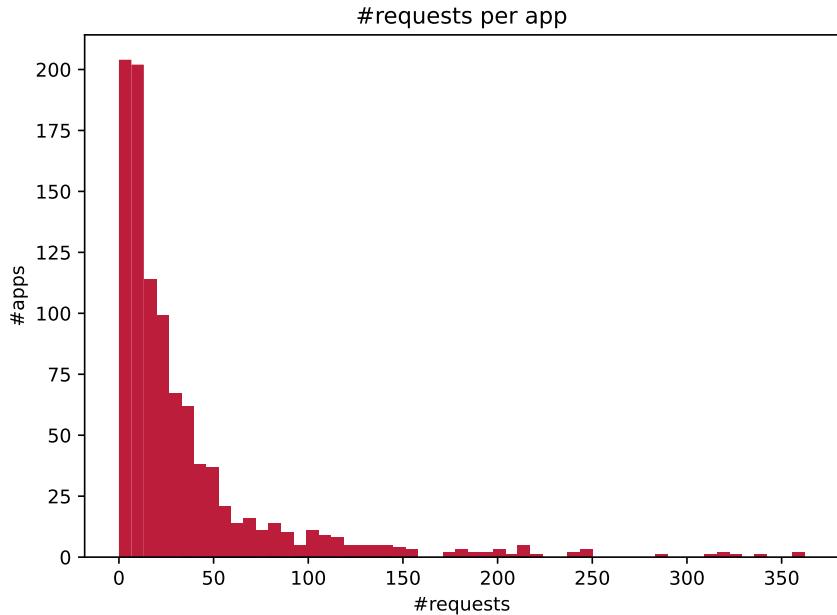
Image: National Cancer Institute (Unsplash license)

Results

Statistics

- 1,001 apps from the “Top 1200 Free Apps” for Germany as of May 27, 2021
- Analysis done on an iPhone 8 running iOS 14.5.1
- 74 apps without any requests, including:
 - Signal - Private Messenger
 - TeleGuard
 - Commerzbank photoTAN
 - AusweisApp2
 - Facebook
 - ZOOM Cloud Meetings

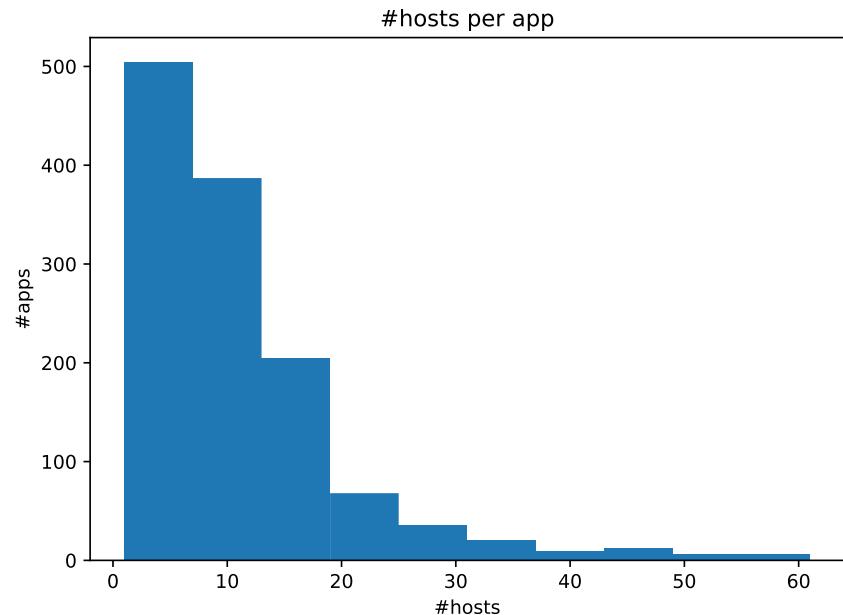
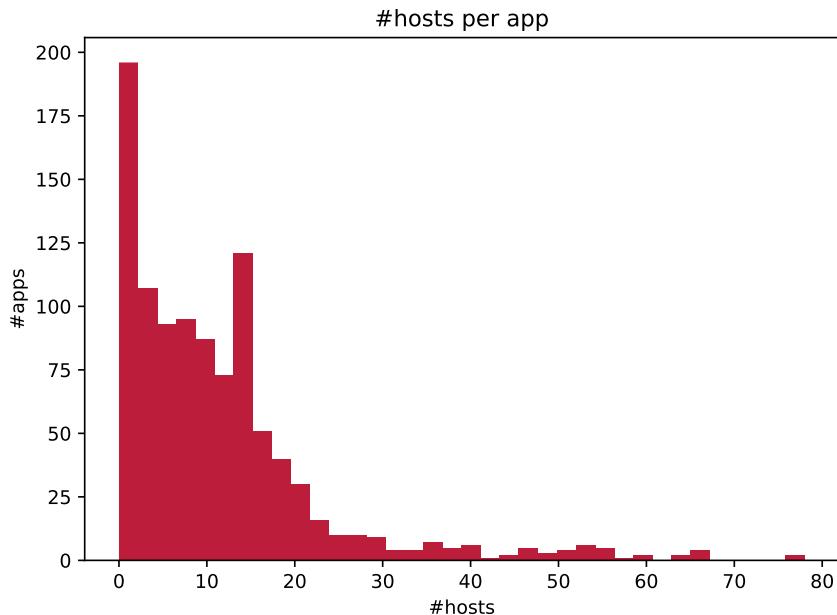
Requests per app



Number of network requests per app on iOS.

Number of network requests per app on Android [[Altpeter, Wessels](#)].

Hosts per app

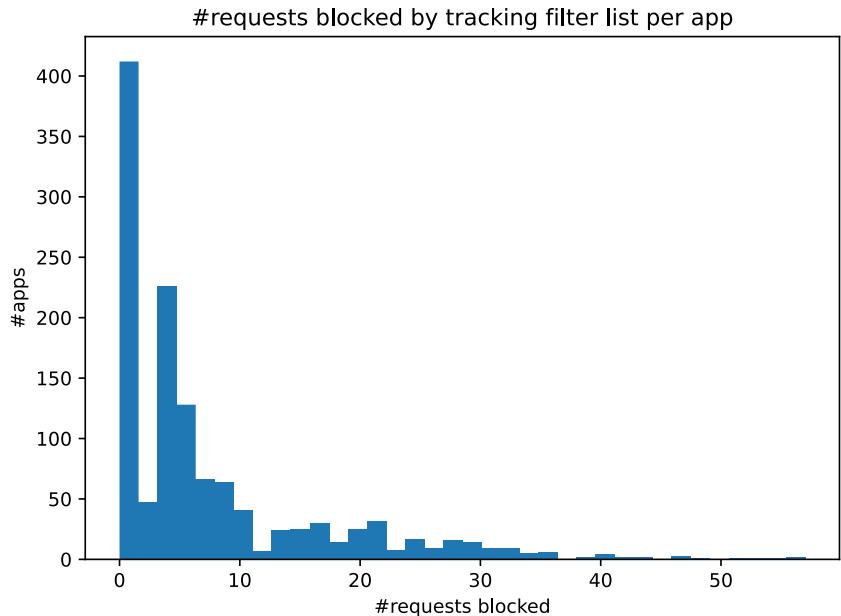
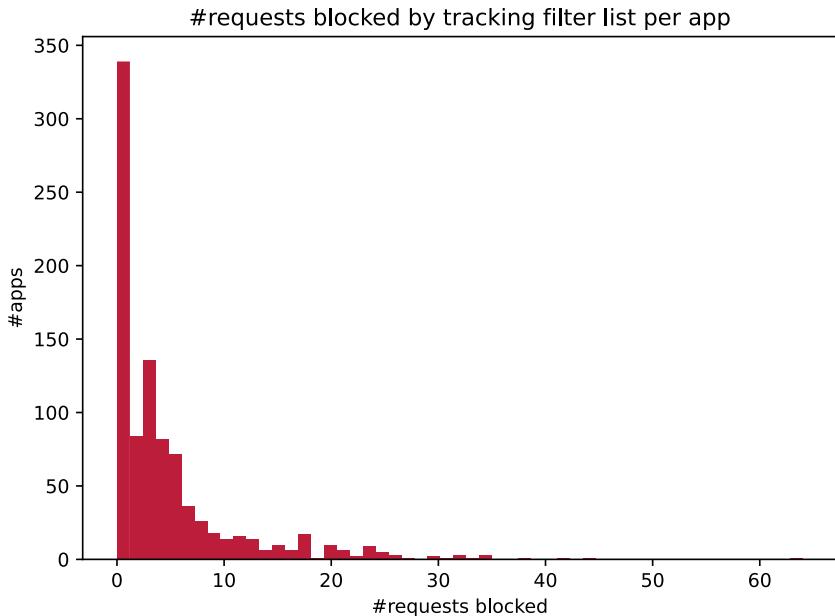


Number of unique hosts requested per app on iOS.

Number of unique hosts requested per app on Android [[Altpeter, Wessels](#)].

Requests blocked by tracking filter lists

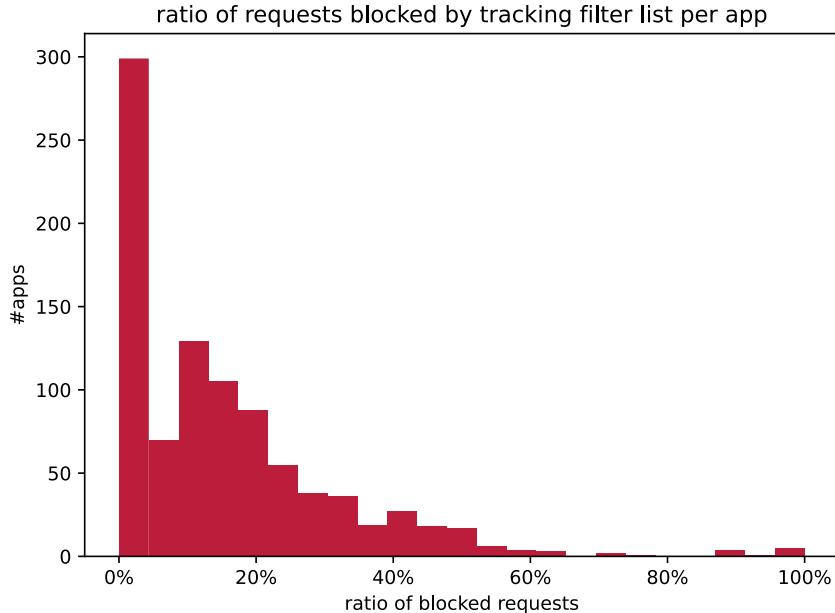
- Total requests: 34,925, requests after filtering: 30,439 (87.16%)



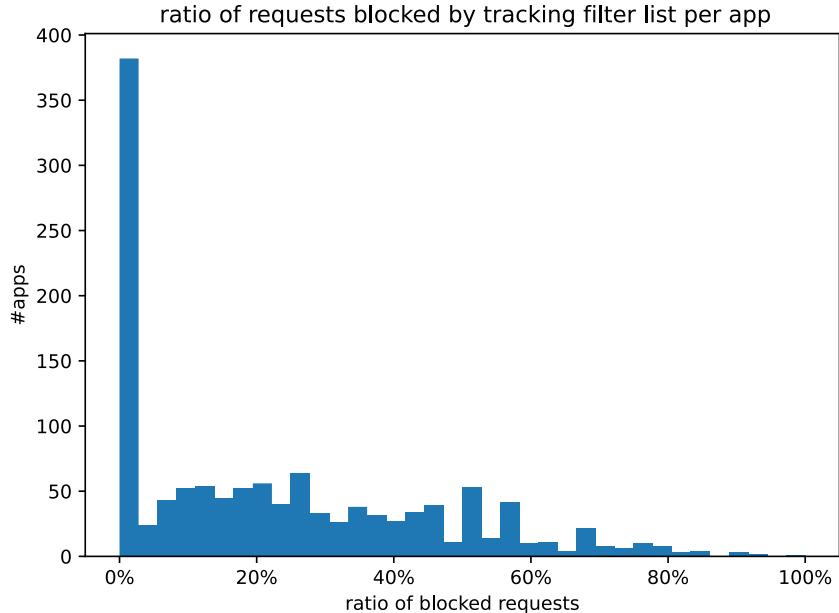
Number of requests blocked per app on iOS when using these tracking filter lists:
[EasyPrivacy](#), [eulaurarien](#), [Perflyst](#).

Number of requests blocked per app on Android when using these tracking filter lists:
[EasyPrivacy](#), [eulaurarien](#), [Perflyst](#) [[Altpeter](#), [Wessels](#)].

Requests blocked by tracking filter lists

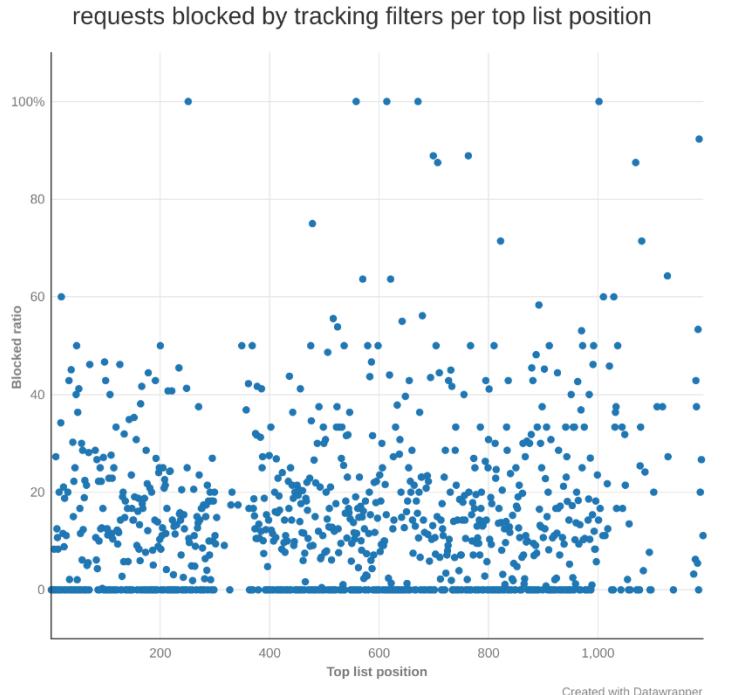


Ratio of requests blocked per app on iOS when using these tracking filter lists:
[EasyPrivacy](#), [eulaurarien](#), [Perflyst](#).



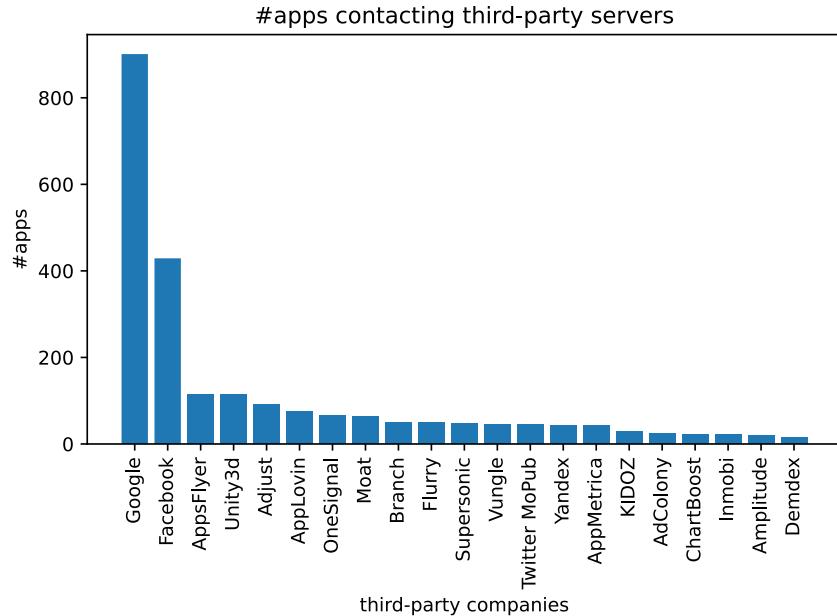
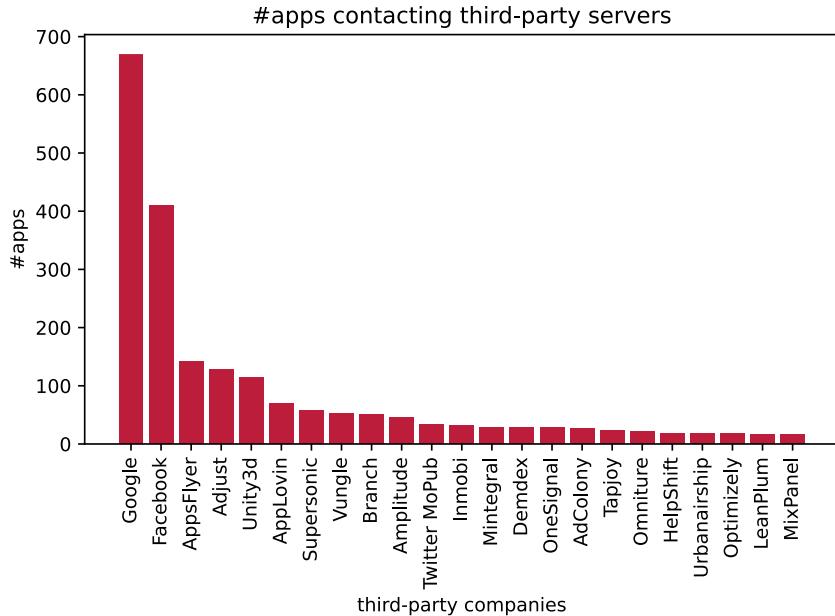
Ratio of requests blocked per app on Android when using these tracking filter lists:
[EasyPrivacy](#), [eulaurarien](#), [Perflyst](#) [[Altpeter](#), [Wessels](#)].

Requests blocked by tracking filter lists



Ratio of requests blocked by tracking filter lists per top list position of the apps,
interactive version: https://www.datawrapper.de/_8tvtM/

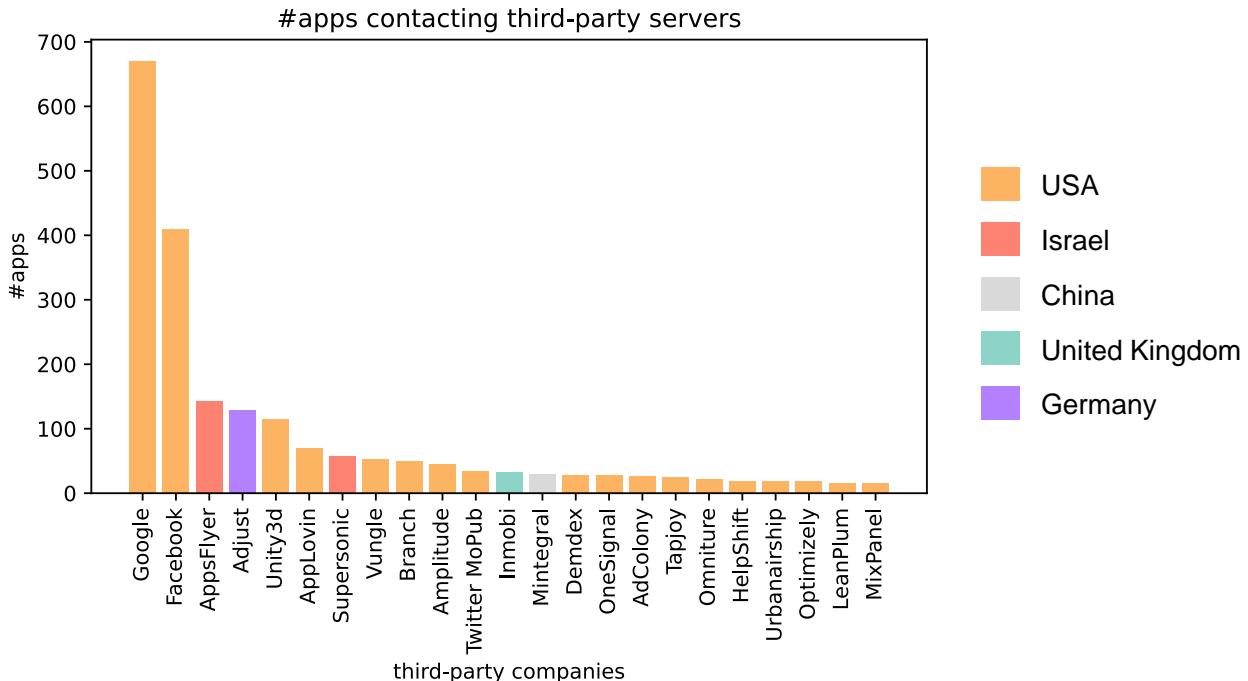
Requests to third-party tracking servers



Number of apps contacting the most common third-party tracking servers on iOS,
based on [Exodus tracker database](#).

Number of apps contacting the most common third-party tracking servers on Android,
based on [Exodus tracker database \[Altpeter, Wessels\]](#).

Where are the trackers based?

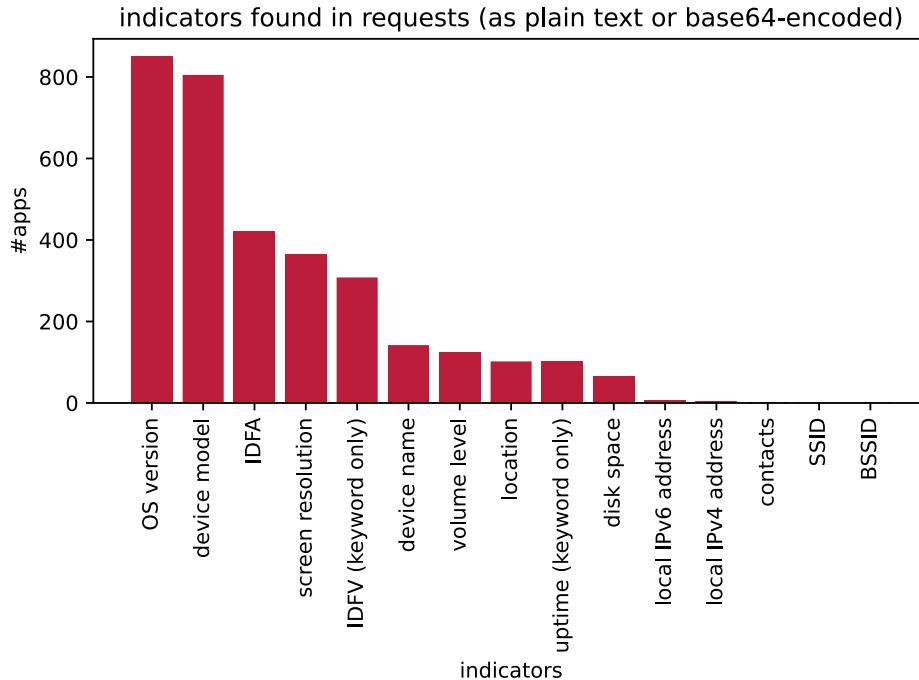


Number of apps contacting the most common third-party tracking servers on iOS and the respective countries, based on [Exodus tracker database](#) and [Datenanfragen.de company database](#).

Honey data

- **Owner:** Frank Walther, frank.walther.1978@icloud.com
- **Contact:** JGKfozntbF TBFFZbBYea, 0155 57543434, RYnISPbEYh@bn.al, <https://q8phILSJgq.de>, N2AsWEMI5D 565, 859663 p0GdKDTbYV
- **Messages:** 9FBqD2CNIJ to +4917691377604
- **Photos,** videos, and screenshots
- **Clipboard:** LDDsvPqQdT
- **Calendar:** fWAs4GFbpN, at urscf2178L, 2021-08-14T08:56 – 2021-08-17T21:24, repeats every month, alarm
- **Reminder:** b5jHg3Eh1k, HQBOdx4kx2 (scheduled for 2021-08-02T13:38)
- **Note:** S0Ei7sFP9b
- **Health details:** Name DkwIXobsJN t5TfTlezmn, DOB 1973-05-15, female, height 146cm, weight 108.5kg
- **Home data:** Rooms bEZf1h06j1 (with wallpaper photo), DX7BgPtH99 (basement); second home g1bVNue3On (with wallpaper photo)
- **Location:** Schreinerweg 6, 38126 Braunschweig; 52.235288, 10.564235
- **WiFi network:** WLAN3.ALTPETER.ME
- **Device name:** R2GI5OLv20
- **Device model:** iPhone10,4
- **OS version:** 14.5.1
- **Model no.:** MX162ZD/A
- **SN:** FFMZP87VN1N0
- **IMEI:** 356395106788056
- **BSSID:** 34:81:c4:dc:36:1
- **WiFi addr:** 3C:CD:36:D4:CC:E4
- **Bluetooth addr:** 3C:CD:36:D2:BD:B2
- **Local IP:** 10.0.0.68
- **Volume level:** 0.125
- **Screen resolution:** 1334x750
- **Disk space:** 127968497664
- **Modem firmware:** 4.03.05
- **SEID:** 044B24632...

Indicators



Number of apps with at least one request that includes the respective indicator. Indicators included in plain text or base64-encoded are considered.

IDFA and IDFV

The screenshot shows the Apple Developer documentation interface. At the top, there's a navigation bar with links for Discover, Design, Develop, Distribute, Support, Account, and a search icon. Below the navigation bar is a dark header bar with the word "Documentation". The main content area starts with a section titled "Instance Property" and "advertisingIdentifier". A brief description follows: "The UUID that is specific to a device." To the right, under "Availability", it lists iOS 6.0+, macOS 10.14+, Mac Catalyst 13.0+, and tvOS 9.0+. Under "Framework", it says AdSupport. Below this, there's a "Declaration" section with a code snippet:

```
var advertisingIdentifier: UUID { get }
```

. The "Discussion" section contains a detailed paragraph about the advertising identifier, mentioning its uniqueness per device and its use for advertising. It also notes that on iOS 14.5 and later, tracking authorization is required. A link to "AdSupport" is provided. At the bottom, it states that the identifier returns either a unique UUID or all zeros, and lists cases where it might return a unique UUID.

This screenshot shows the Apple Developer documentation for the "identifierForVendor" property. The layout is identical to the first screenshot. The "Instance Property" section starts with "identifierForVendor". A brief description: "An alphanumeric string that uniquely identifies a device to the app's vendor." To the right, under "Availability", it lists iOS 6.0+, Mac Catalyst 13.0+, and tvOS 9.0+. Under "Framework", it says UIKit. Below this is a "Declaration" section with the code:

```
var identifierForVendor: UUID? { get }
```

. The "Discussion" section contains a paragraph explaining that the value is the same for apps from the same vendor on the same device, but different for apps from different vendors or devices. It also notes that the vendor ID is determined by the App Store if the app was installed from there. A link to "UIKit" is provided.

IDFA and IDFV

Documentation User Guide **Developer Guide** API Technology Partners Help

Search

Home

+ Platform Wide Features & Behaviors

- Platform Integration Guides

- SDK 101
- + Android
- iOS**
 - + Initial SDK Setup
 - + Push Notifications
 - + In-App Messaging
 - + Content Cards
 - + News Feed
 - + Analytics
 - + Advanced Use Cases
- iOS 14 Upgrade Guide**
 - Storage
 - Sample Apps
 - Changelog
- + Web
- + Cordova
- + FireOS
- + Flutter
- + React Native
- + tvOS
- + Xcode

IDFA and App Tracking Transparency

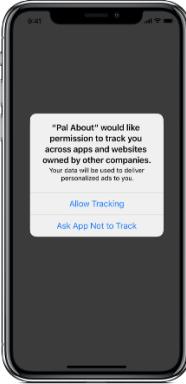
Overview

IDFA (Identifier for Advertisers) is an identifier provided by Apple for use with advertising and attribution partners for cross-device tracking and is tied to an individual's Apple ID.

Starting in iOS 14.5, a new permission prompt [launched by the new [AppTrackingTransparency](#) framework] must be shown to collect explicit user consent for IDFA. This permission prompt to "track you across apps and websites owned by other companies" will be requested similarly to how you'd prompt users to request their location.

If a user does not accept the prompt, or if you do not upgrade to Xcode 12's [AppTrackingTransparency](#) framework, then a blank IDFA value (`(00000000-0000-0000-0000-000000000000)`) will be returned, and your app will not be allowed to prompt the user again.

Important:
These IDFA updates will take effect once end-users upgrade their device to iOS 14.5. Please ensure your app uses the new [AppTransparencyFramework](#) with Xcode 12 if you plan to collect IDFA.

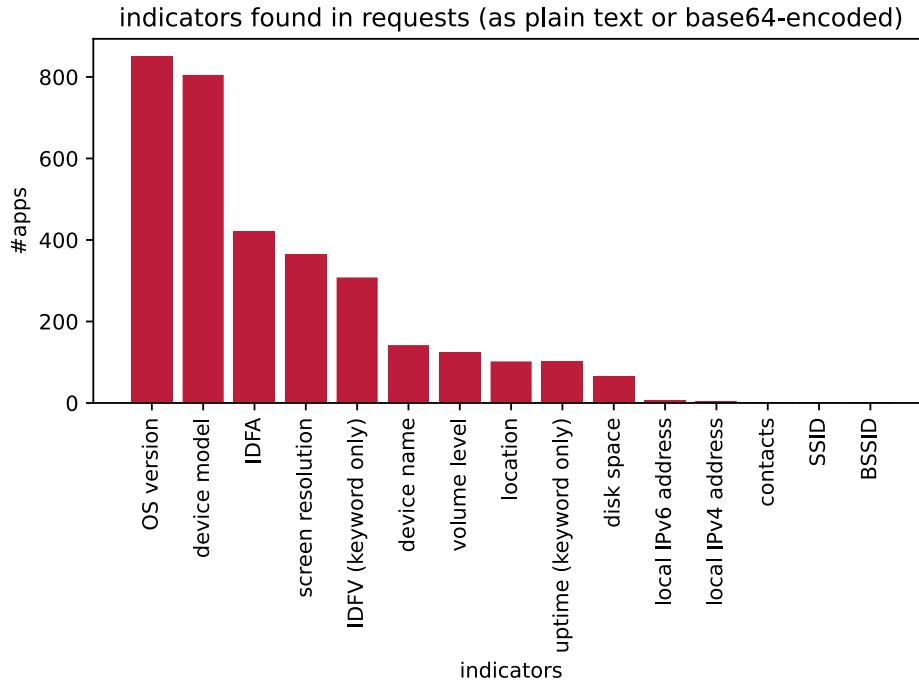


Edit this page on GitHub

On this page...

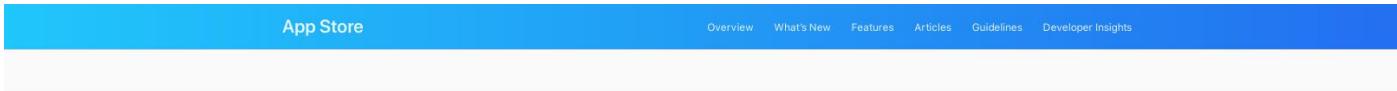
- Upgrade Summary
- iOS 14 Behavior Changes
- Approximate Location Permission
- IDFA and App Tracking Transparency**
- Push Authorization
- iOS 14 New Features
- App Privacy and Data Collection Overview

Indicators



Number of apps with at least one request that includes the respective indicator. Indicators included in plain text or base64-encoded are considered.

Privacy labels

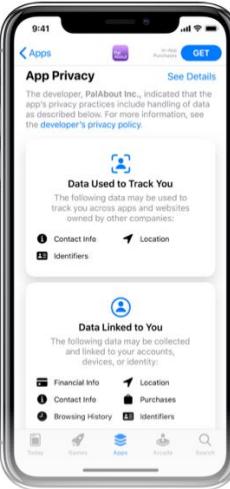


Describing How Your App Uses Data

The App Store better helps users understand an app's privacy practices before they download the app. On each app's product page, users can learn about some of the data types an app may collect, and whether the information is used to track them or is linked to their identity or device.

In order to submit new apps and app updates, you must provide information about your privacy practices in App Store Connect. If you use third-party code — such as advertising or analytics SDKs — you'll also need to describe what data the third-party code collects, how the data may be used, and whether the data is used to track users.

[Learn more >](#)



<https://developer.apple.com/app-store/user-privacy-and-data-use/>

Privacy labels

App Store Preview

App Privacy

The developer, Facebook, Inc., indicated that the app's privacy practices may include handling of data as described below. This information has not been verified by Apple. For more information, see the [developer's privacy policy](#).

Data

The following data may be used to track you across apps and websites owned by other companies:

- Contact Info
- Other Data

To help you better understand the developer's responses, see [Privacy Definitions and Examples](#).

Privacy practices may vary, for example, based on the features you use or your age. [Learn More](#)

Data Used to Track You

The following data may be used to track you across apps and websites owned by other companies:

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

Filter URLs

S...	Met	Domain	File	Initiator	T...	Transfe...	S...
204	O...	amp...	284882215?platform=web&f	xhr	p...	552 B	0 B
200	G...	amp...	284882215?platform=web&f	vendor...	js...	cached	9...

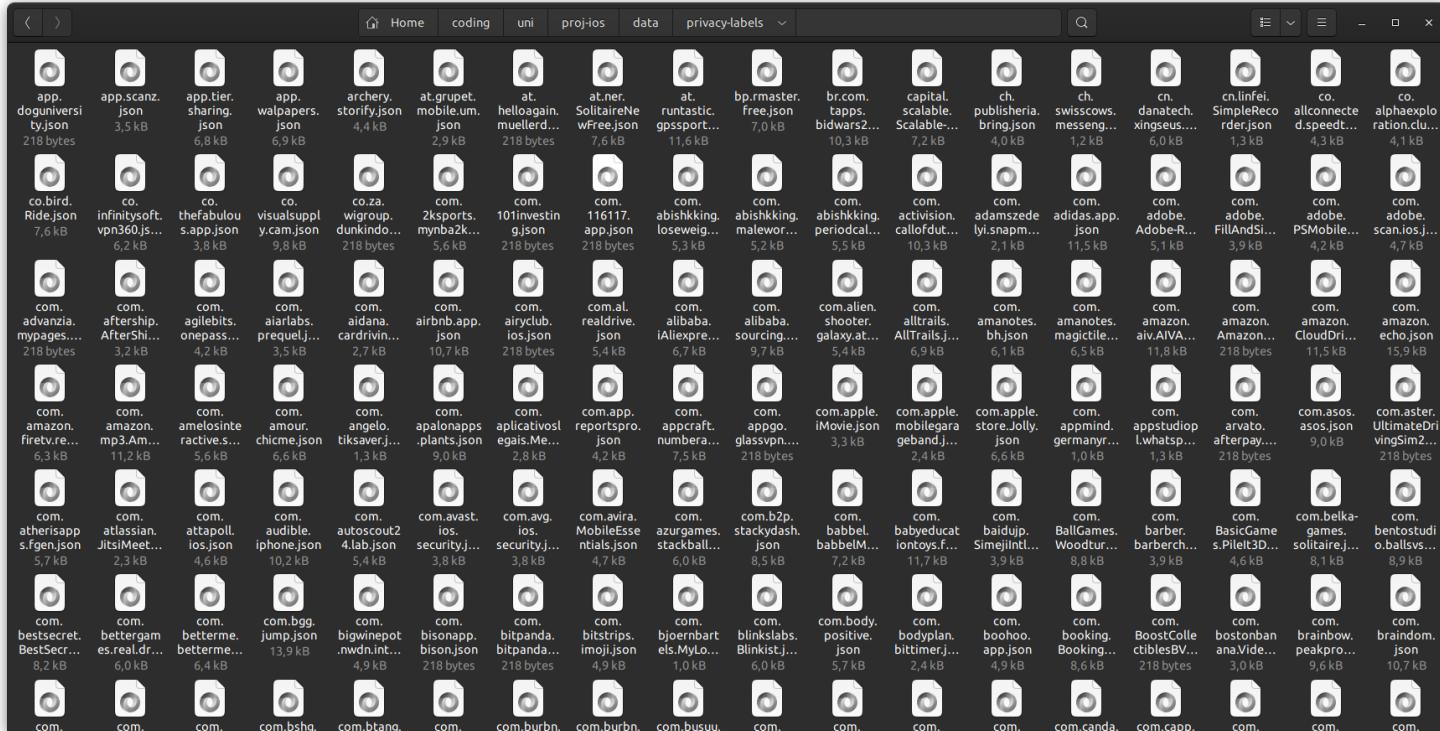
Headers Cookies Request Response Cache Timings Stack Trace Security

Filter Headers Block Resend

Status 200 OK ⓘ

https://apps.apple.com/us/app/facebook/id284882215

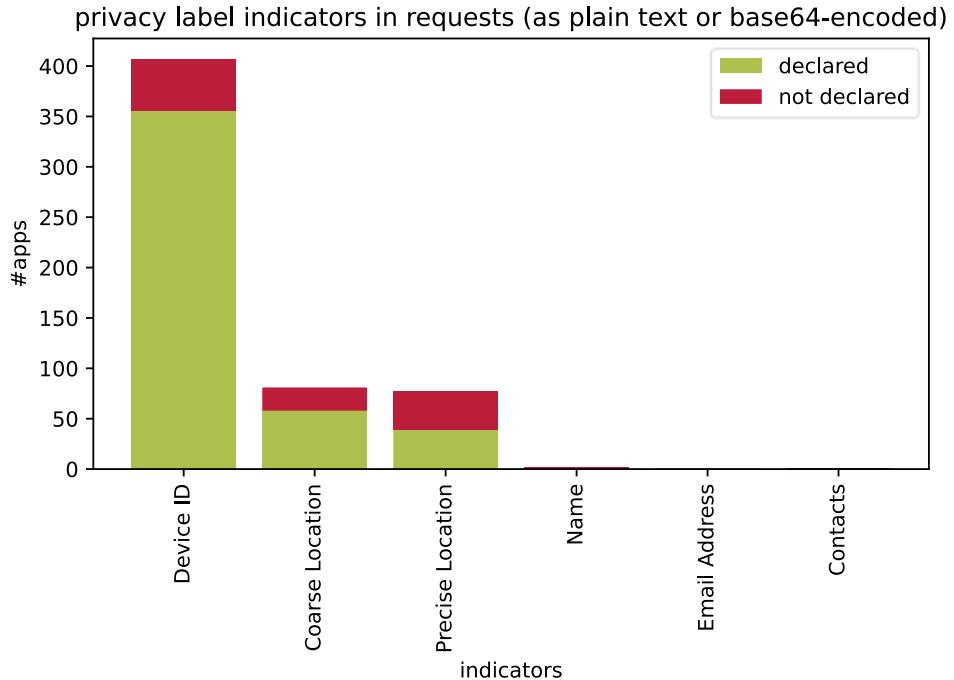
Privacy labels



Privacy labels

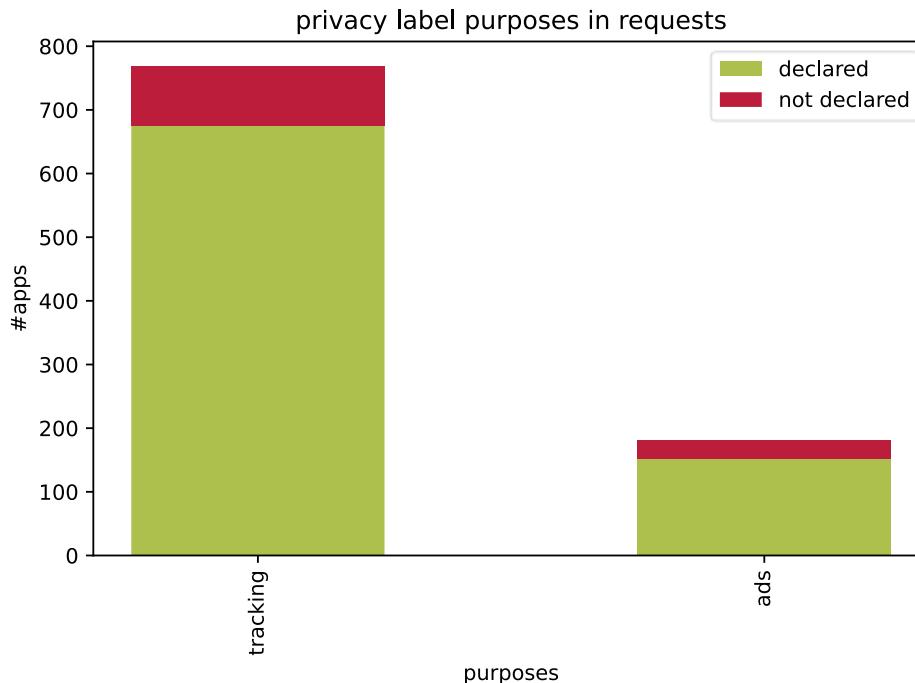
- 841 of 1001 apps have valid privacy labels. Of those, 32 claim not to collect any data, namely:
 - [TeleGuard](#)
 - [Voice Recorder - Audio Editor⁺](#)
 - [Tik Saver : Tik Tok Downloader](#)
 - [whatspoof fake chat](#) 
 - [Stop Motion Studio](#)
 - [WATCHED - Multimedia & Movie](#)  
 - [free2pass](#)
 - [Darf ich das?](#)
 - [Moodle](#) 
 - [VPN TrackBlock: data safety](#)  
 - [PlattinO - Die Plattlern-App](#)
 - [Purepurple Outfit Planner](#)   
 - [Renpho](#) 
 - [Samsung Galaxy Watch \(Gear S\)](#) 
 - [Cisco Webex Meetings](#)
 - [Windscribe VPN](#)
 - [SpiderDoll](#) 
 - [Meine AOK](#)
 - [Sicher Reisen](#) 
 - [Wahl-O-Mat](#)
 - [ePassGo](#)
 - [DSBmobile](#)
 - [DKB-TAN2go](#) 
 - [ElsterSmart](#)
 - [EPICOM](#)
 - [Onlinebefunde](#)
 - [SafeVac](#)
 - [STIKO-App](#) 
 - [atWork Timesheet](#)
 - [Re-open EU](#)
 - [Blutspende](#)
 - [Hayat Eve Sığar](#) 

Indicators



Number of apps with at least one request that includes the respective indicator as specified by the privacy labels and whether it was declared. Indicators included in plain text or base64-encoded are considered.

Purposes



Number of apps with at least one request for the purpose of tracking or ads as specified by the privacy labels and whether it was declared. Based on [Exodus tracker database](#) and most popular ad hosts in data set.

Conclusion

- Very similar results for Android and iOS
- Similar amount of tracking, covering the same data and through the same third-party companies
- Currently major difference w.r.t. ad ID

Conclusion

The screenshot shows a web browser window with the Google Play Console Help interface. At the top, there are navigation links for "Play Console Help" and a search bar with the placeholder "Describe your issue". On the right side, there are icons for help and sign-in.

Advertising ID

⚠ Starting in late 2021, when a user opts out of interest-based advertising or ads personalization, the advertising identifier will not be available. You will receive a string of zeros in place of the identifier.

The advertising ID is a unique, user-resettable ID for advertising, provided by Google Play services. It gives users better controls and provides developers with a simple, standard system to continue to monetize their apps. It enables users to reset their identifier or opt out of personalized ads (formerly known as interest-based ads) within Google Play apps.

Google Play services update in 2021

As part of Google Play services update in late 2021, the advertising ID will be removed when a user opts out of personalization using advertising ID in Android Settings. Any attempts to access the identifier will receive a string of zeros instead of the identifier. To help developers and ad/analytics service providers with regulatory compliance efforts and respect user choice, they will be able to receive notifications for opt-out preferences. If you want to test the aforementioned notification system, fill out this [form](#).

This Google Play services phased rollout will affect apps starting late 2021 and will expand to affect apps running on all devices that support Google Play in early 2022. For essential non ads use-cases such as analytics and fraud prevention, use [App Set ID](#).

Additionally, apps updating their target API level to 31 (Android 12) will need to declare a Google Play services normal permission in the manifest file as follows:

```
<uses-permission android:name="com.google.android.gms.permission.AD_ID"/>
```

Some SDKs, such as the Google Mobile Ads SDK (play-services-ads) may already declare this permission in the SDK's library manifest. If your app uses these SDKs as dependencies, the AD_ID permission from the SDK's library manifest will be merged with your app's main manifest by default, even if you don't explicitly declare the permission in your app's main manifest. Learn more about merging manifest files on the [Android Developers site](#).

Some Google Play policies, such as the [Families Policy](#), require that apps not use the Ad ID. If your app uses SDKs, like the Google Mobile Ads SDK, that declares the AD_ID permission in their library manifests, you must prevent the permission from getting merged into your app by including the following element in your manifest:

<https://support.google.com/googleplay/android-developer/answer/6048248?hl=en>

- Manage policy violations
- How to support your app's users
- Advertising ID
- Declare permissions for your app
- Provide app privacy and security information for Google Play's safety section
- Requirements for distributing apps in specific countries/regions
- Requirements for apps that communicate government information
- Viewing and purchasing your own apps
- Find and troubleshoot your license key
- Use of SMS or Call Log permission groups
- Requesting access to location in the background
- Requirements for coronavirus disease 2019 (COVID-19) apps
- Understand upcoming changes to news and news-related apps
- Use of All files access (MANAGE_EXTERNAL_STORAGE) permission

Conclusion

- Very similar results for Android and iOS
- Similar amount of tracking, covering the same data and through the same third-party companies
- Currently major differences w.r.t. ad ID, but similar changes planned for Android
- Apple does at least innovate somewhat, e.g. through privacy labels (pretty accurate)

Conclusion



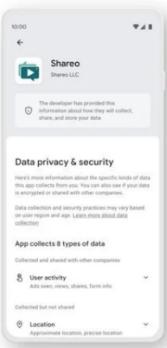
iMore



Google reveals Android version of Apple's privacy nutrition labels

"Developers can share what data their app collects and why, so users can download with confidence."

STEPHEN WARWICK 29 Jul 2021



Source: Google

Developers can share what data their app collects and why, so users can download with confidence

Keep in Touch

Sign up now to get the latest news, deals & more from iMore!

Your Email Address

I would like to receive news and offers from other Future brands.

Yes No

I would like to receive mail from Future partners.

Yes No

SIGN ME UP

No spam, we promise. You can unsubscribe at any time and we'll never share your details without your permission.

<https://www.imore.com/google-reveals-android-version-apples-privacy-nutrition-labels>

Future work

- Improve IPA acquisition “framework”
- Investigate defenses against tracking in general and metadata extraction in particular
- Dive deeper into privacy labels
- More sophisticated data analysis