



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- On iOS (often hailed as more privacy-friendly), research into privacy violations by apps is scarce and outdated.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

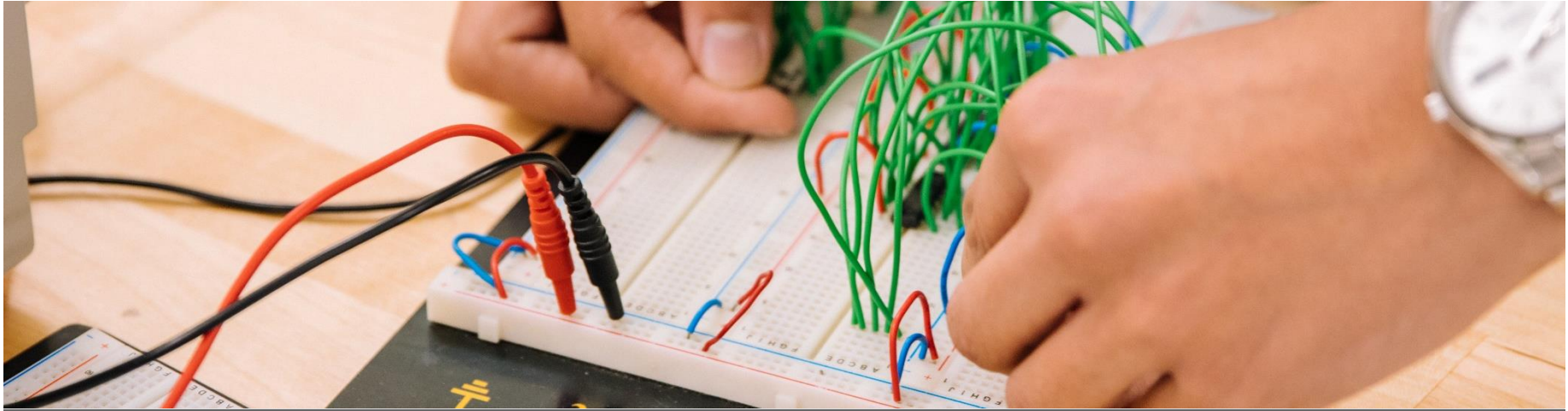


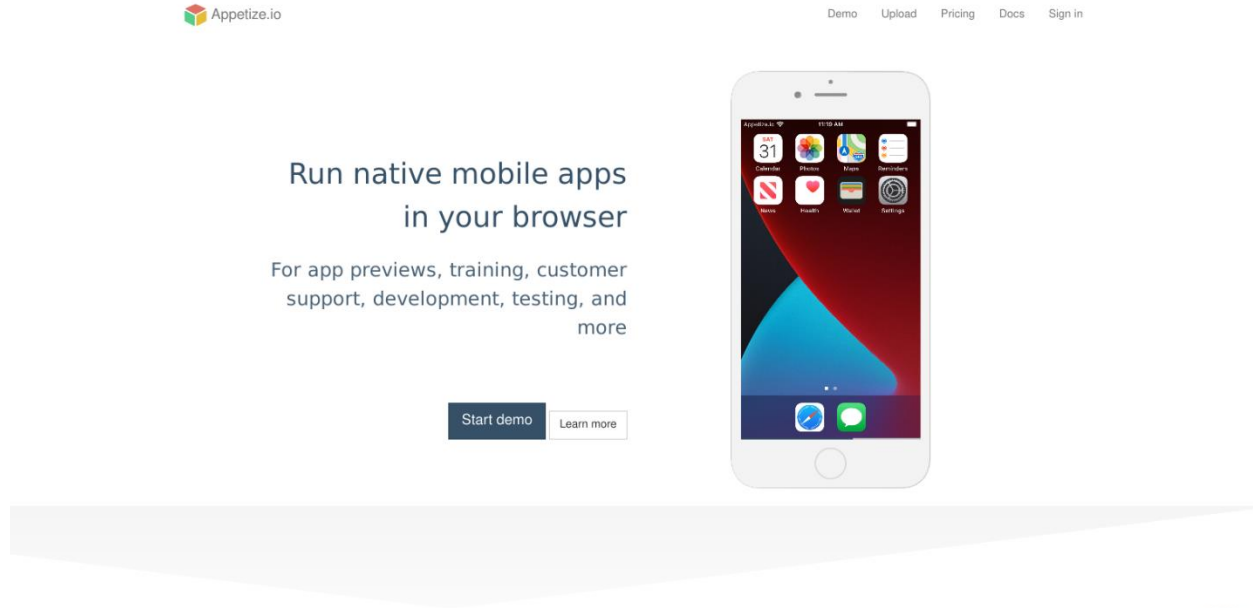
Image: Jeswin Thomas (Unsplash license)

Method

Is emulation an option?



Maybe commercial providers can help?



Appetize.io

Demo Upload Pricing Docs Sign in

Run native mobile apps
in your browser

For app previews, training, customer support, development, testing, and more

Start demo Learn more

The screenshot shows the Appetize.io website interface. At the top left is the logo 'Appetize.io'. To the right are navigation links: 'Demo', 'Upload', 'Pricing', 'Docs', and 'Sign in'. The main content area features the headline 'Run native mobile apps in your browser' and a sub-headline 'For app previews, training, customer support, development, testing, and more'. Below the text are two buttons: 'Start demo' and 'Learn more'. On the right side, there is a large image of a white iPhone displaying an iOS home screen with various app icons like Calendar, Photos, Maps, and Settings. A large, light gray arrow-shaped graphic points downwards from the phone area towards the bottom of the slide.



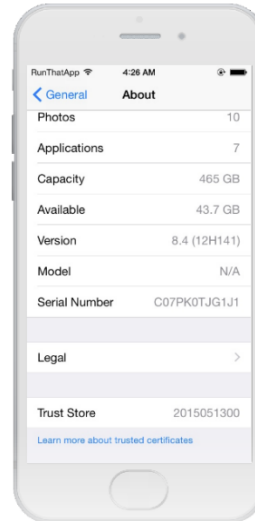
<https://appetize.io/>

Maybe commercial providers can help?

RUN THAT APP

[Start](#) [Team](#) [Pricing](#) [Upload](#) [Press](#) [Features](#) [Contact](#)

Go ahead, click and play



[Go Fullscreen iOS](#)

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

Maybe commercial providers can help?

The screenshot shows the Appetize.io documentation website. The top navigation bar includes 'Home', 'Demo', 'Upload', and 'Pricing', along with a search bar. A left sidebar lists various documentation topics, with 'Uploading apps' highlighted. The main content area is titled 'Uploading apps' and contains the following text:

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](#).

Below this text are two tabs: 'iOS' (selected) and 'Android'. A yellow box highlights the following text:

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 `xcodebuild`.

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

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

Maybe commercial providers can help?

Browse... No file selected.

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

Submit

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

Apple has it hidden away in SOME xCode versions. 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-cgcerwyxpmekwdqrgobouaiccx/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
- 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 on The Register website. The article title is "Judge rules Corellium iOS research app 'fair use' in slap to Apple". The author is Matthew Hughes, and the date is Mon 4 Jan 2021 / 16:03 UTC. The article discusses a court ruling in favor of Corellium, a Florida startup that offers virtualized iOS instances for security researchers. The ruling states that Corellium's product does not infringe upon Apple's intellectual property because it is a specialist research tool aimed at a smaller audience than Apple's products. The article also mentions that Corellium's product is a repackaged version of iOS in a virtual environment, with several changes to iOS and its own code to create a product that serves a transformative purpose.

SIGN IN The Register

{* VIRTUALIZATION *}

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

5

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?

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](#) →

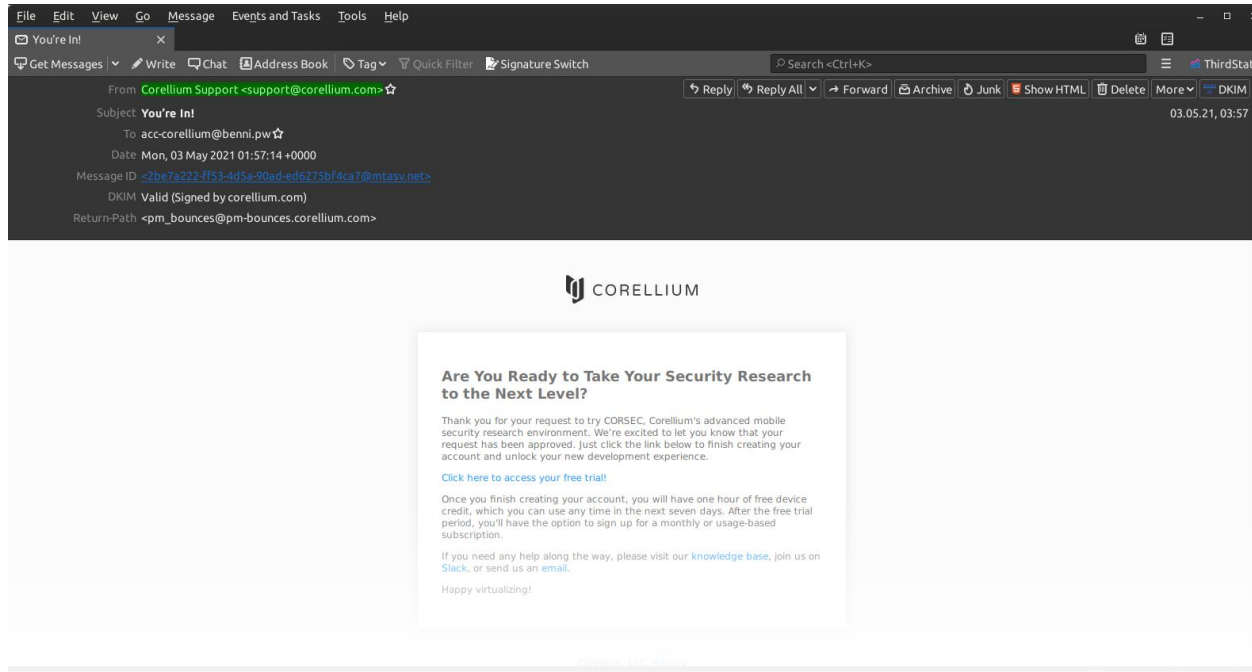


SPEED

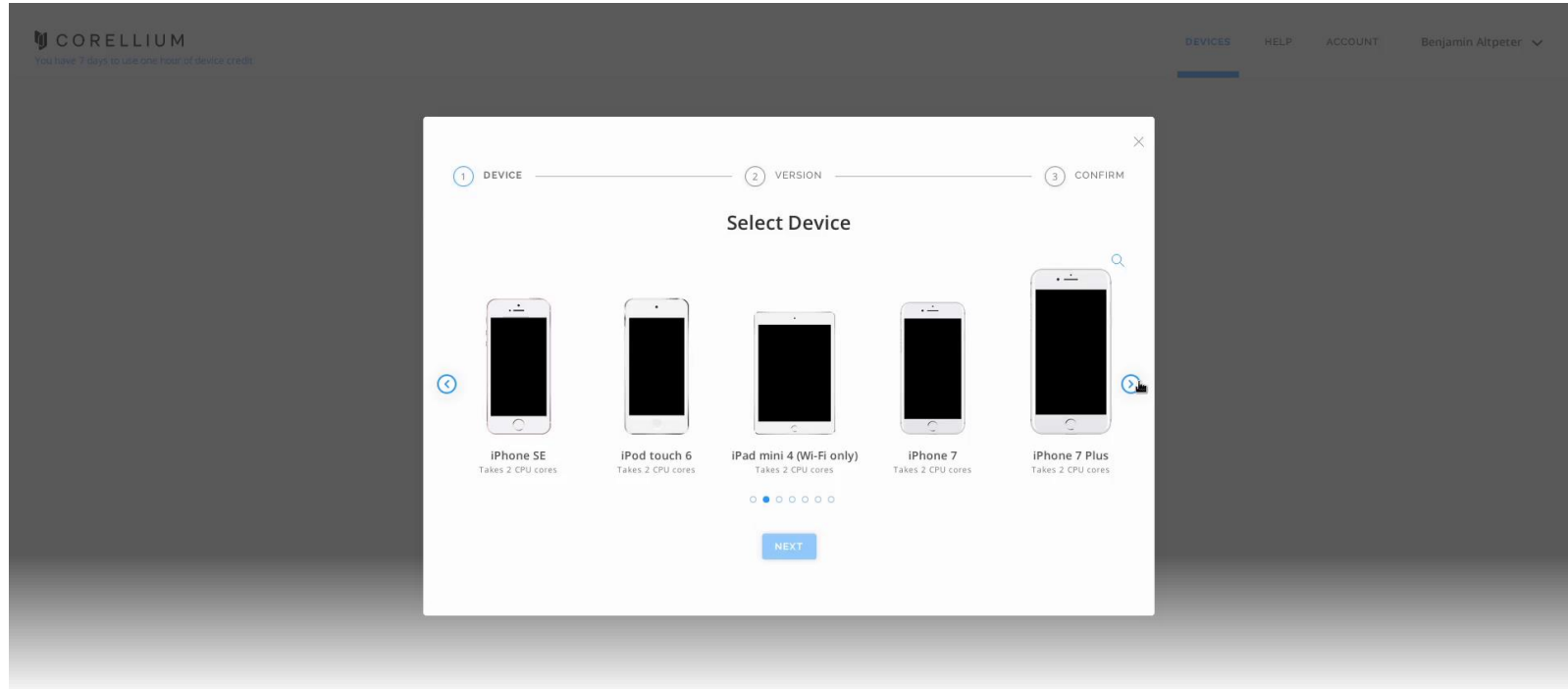
Set up in no time. Spin up devices on demand and integrate seamlessly with your existing workflows.

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

I'm in!

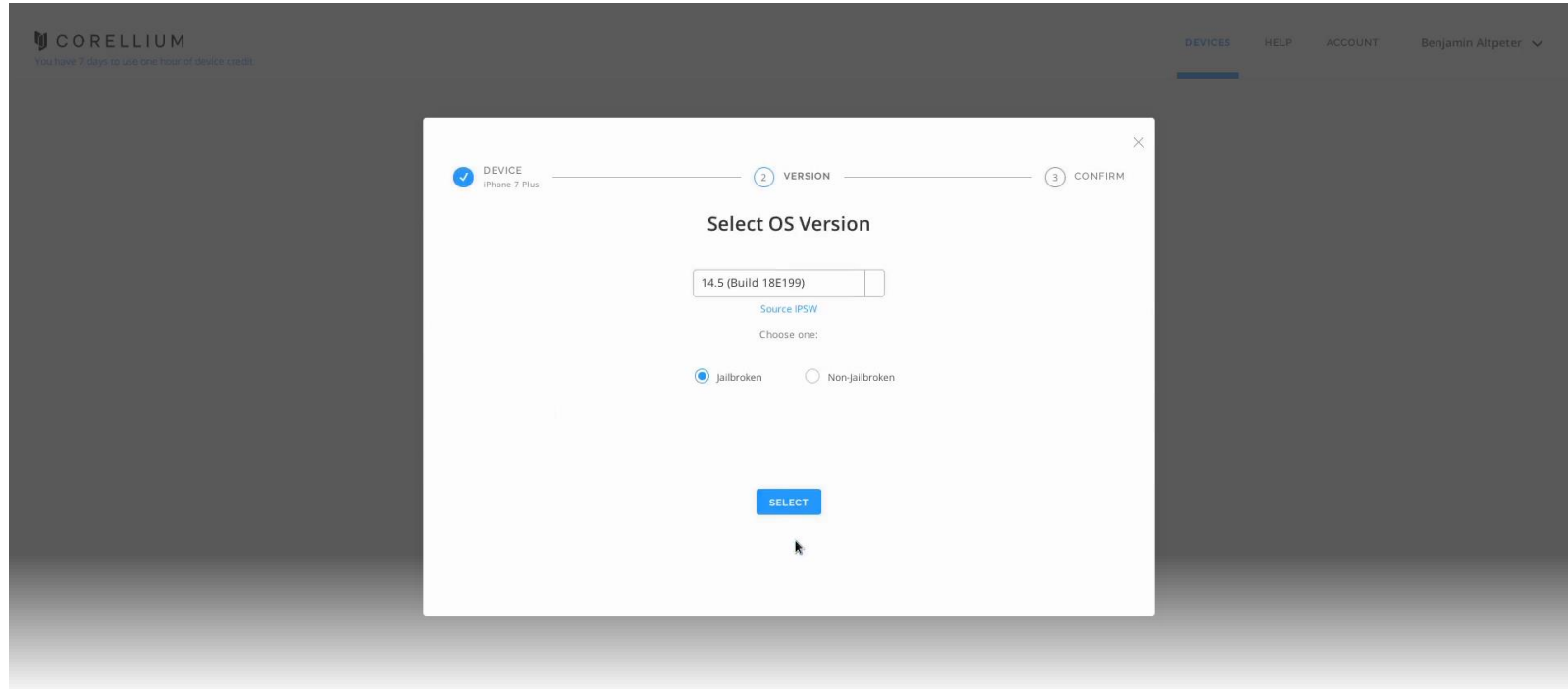


I'm in!



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

I'm in!



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

I'm in!

The screenshot displays the Corellium web interface. At the top left, the Corellium logo is visible with the text "CORELLIUM" and "You have 7 days to use 47 minutes of device credit". The top right shows navigation links for "DEVICES", "HELP", "ACCOUNT", and the user name "Benjamin Altpeter". Below the header, the device information "test (iPhone 7 Plus | 14.5 | 18E199 | ✓ Jailbroken)" is shown. The main interface is divided into two panels. The left panel shows a virtual iPhone 7 Plus with a jailbroken home screen. The right panel is titled "CONNECT" and contains two main sections: "1 Set Up VPN" and "2 Connect To Device". The "Set Up VPN" section includes a button for "OVPN FILE". The "Connect To Device" section provides instructions for connecting via WiFi, USB, and advanced options like SSH and kernel gdb. At the bottom right of the interface, a status bar shows "Wi-Fi IP: 10.11.0.1" and "Services IP: 10.11.1.1".

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


I'm in!

The screenshot displays the Corellium application interface. On the left, a simulated iPhone 7 Plus is shown with a browser displaying the website datenanfragen.de. The page content includes the text "Du hast ein Recht auf Dat" and a button labeled "Nutze es.". On the right, the "Network Monitor" tab is active, showing a table of captured HTTP traffic. The table has columns for INDEX, CODE, METHOD, HOST, START, and SIZE. The selected entry (index 35) shows a 200 status code for a GET request to www.datenanfragen.de with a size of 17.8 KB. Below the table, a snippet of the HTTP response body is visible, containing HTML elements like <a href=

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.dacdn.de	May 3, 2021 2:55 PM	57.7 KB

<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...



Andy Ibanez

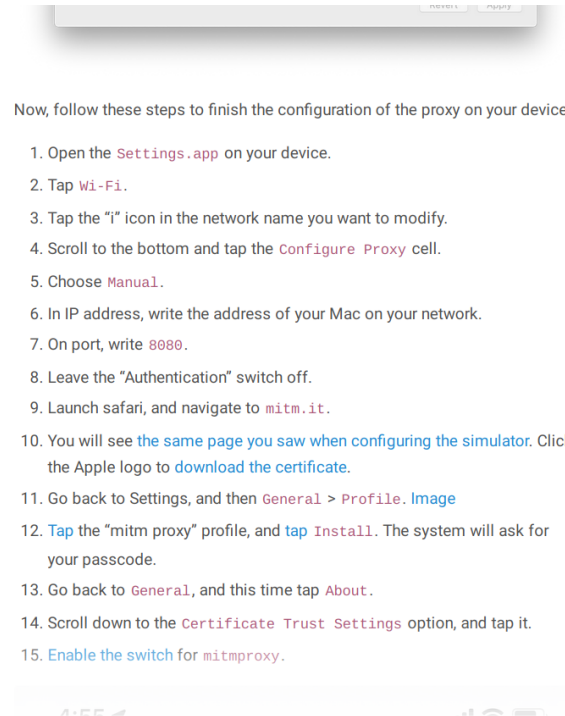


Software Developer from La Paz, Bolivia. Programming for iOS since 2011.

Posts
WWDC 2020
Projects
About Me
Privacy Policy




© 2021 Andrés Ibañez



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 repository page for 'SSL Kill Switch 2'. The repository is owned by 'nabla-c0d3'. The README file is open, showing the following content:

SSL Kill Switch 2

Blackbox tool to disable SSL/TLS certificate validation - including certificate pinning - within iOS and macOS applications. Second iteration of <https://github.com/ISECPartners/ios-ssl-kill-switch>.

Description

Once loaded into an iOS or macOS application, SSL Kill Switch 2 will patch low-level functions responsible for handling SSL/TLS connections in order to override and disable the system's default certificate validation, as well as any kind of custom certificate validation (such as certificate pinning).

It was successfully tested against various applications implementing certificate pinning including the Apple App Store. The first version of SSL Kill Switch was released at Black Hat Vegas 2012.

The most recent version iOS that is known to be supported is 14.2.

iOS Instructions

On iOS, SSL Kill Switch 2 can be installed as a Cydia Substrate tweak on a jailbroken device.

WARNING: THIS TWEAK WILL MAKE YOUR DEVICE INSECURE

Installing SSL Kill Switch 2 allows anyone on the same network as the device to easily perform man-in-the-middle attacks against *any* SSL or HTTPS connection. This means that it is trivial to get access to emails, websites viewed in Safari and any other data downloaded by any App running on the device.

Installation

On the right side of the repository page, there are sections for 'Contributors' (8) and 'Languages'. The 'Languages' section shows a bar chart with the following data:

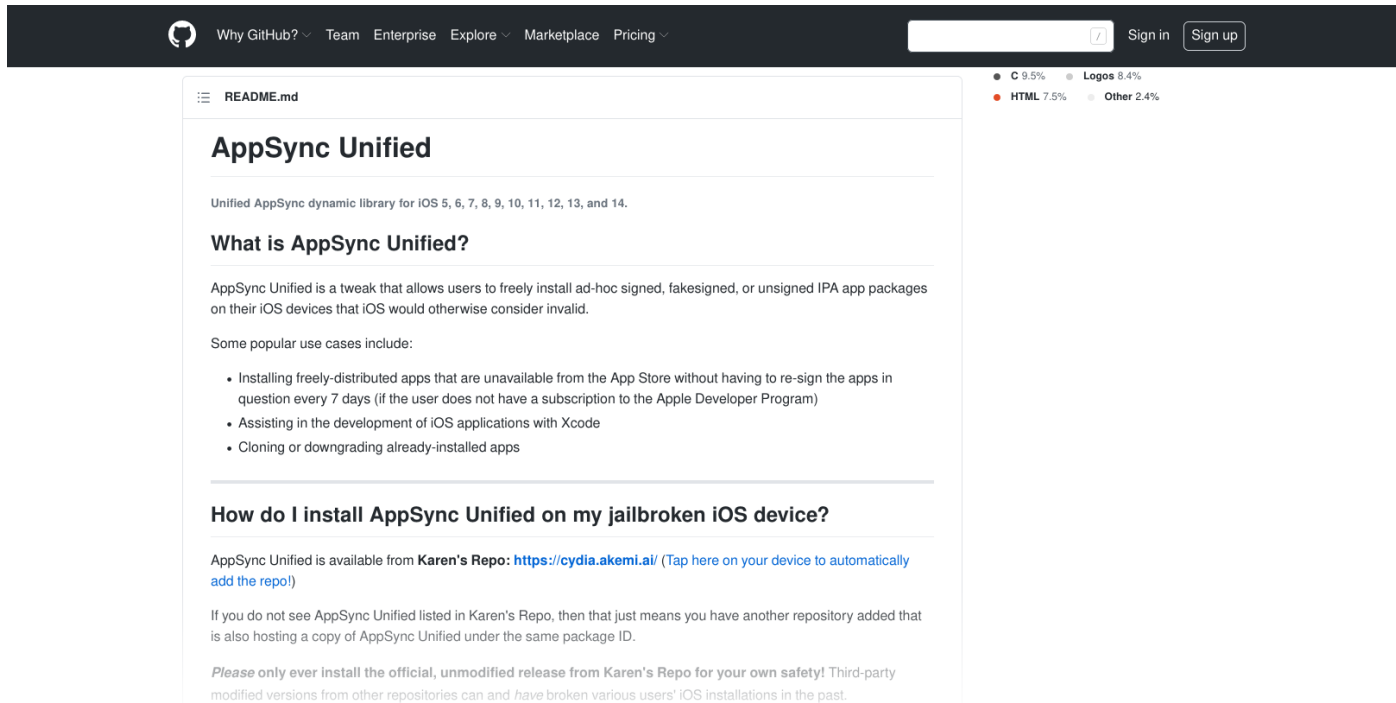
Language	Percentage
Objective-C	58.3%
C	40.4%
Makefile	1.3%

<https://github.com/nabla-c0d3/ssl-kill-switch2>

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&amp;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 page header includes navigation links like 'Why GitHub?', 'Team', 'Enterprise', 'Explore', 'Marketplace', and 'Pricing'. A search bar and 'Sign in'/'Sign up' buttons are also visible. The main content area displays the README for 'AppSync Unified', which is a dynamic library for iOS. The README includes sections for 'What is AppSync Unified?' and 'How do I install AppSync Unified on my jailbroken iOS device?'. A small chart on the right side of the page shows the repository's language distribution: C (9.5%), Logos (8.4%), HTML (7.5%), and Other (2.4%).

Why GitHub? Team Enterprise Explore Marketplace Pricing

Sign in Sign up

README.md

AppSync Unified

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.

● C 9.5% ● Logos 8.4%
● HTML 7.5% ● Other 2.4%

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

Let's start with a wish list



Apple Services Marketing Tools

RSS Feed Generator

Feed Settings

Country or Region: Germany
Media Type: iOS Apps
Feed Type: Top Free
Genre: All

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

Feed URL

<https://rss.itunes.apple.com/api/v1/de/ios-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
culaburkle GmbH



Corona-Warn-App
Robert Koch-Institut



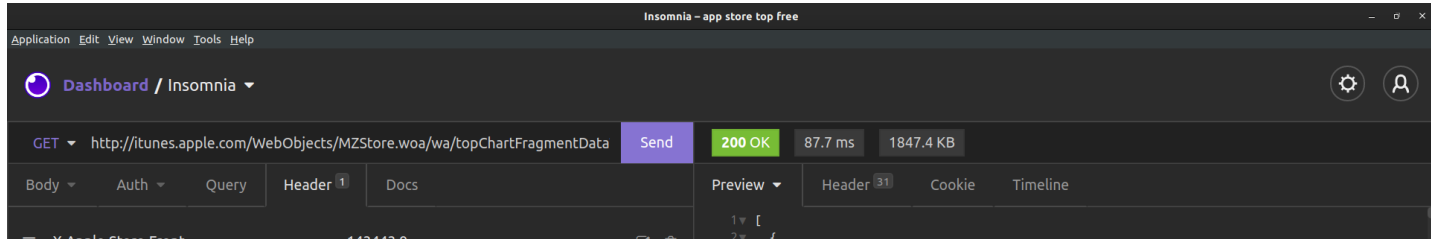
Google Maps - Transit
& Essen
Google LLC



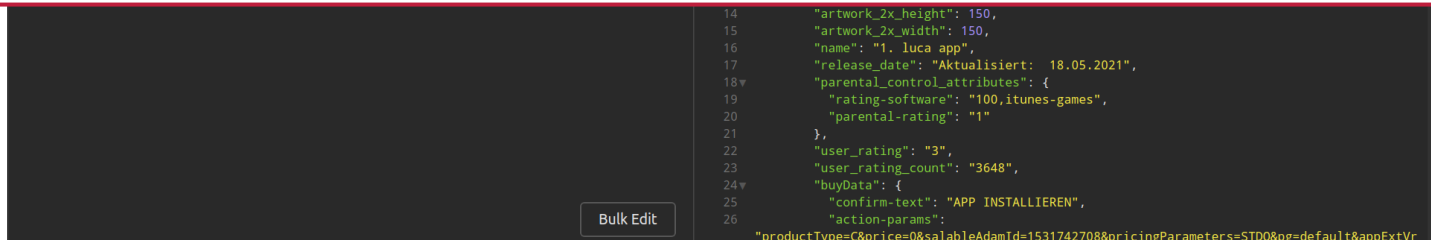
WhatsApp Messenger
WhatsApp Inc.

<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
```



Officially supported?

OSXDaily

Home Mac OS iPhone iPad Tips & Tricks News iOS Troubleshooting

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

Dec 15, 2011 - 12 Comments

Subscribe to OSXDaily

Tips & Tricks

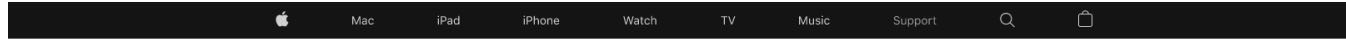
- How to Cancel Pre-Orders on iPhone & iPad
- How to Check Warranty & Apple Care+ Status of Your Mac
- Forgot Apple Watch Passcode? Here's How to Reset It
- How to Change Storage Limit for Photos on Apple Watch
- How to Share iCloud Storage with Family on iPhone & iPad

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?

reddit Search Log In Sign Up

4 iTunes 12.6.5.3 working with iOS 13 Close

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/d6p9tb/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

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

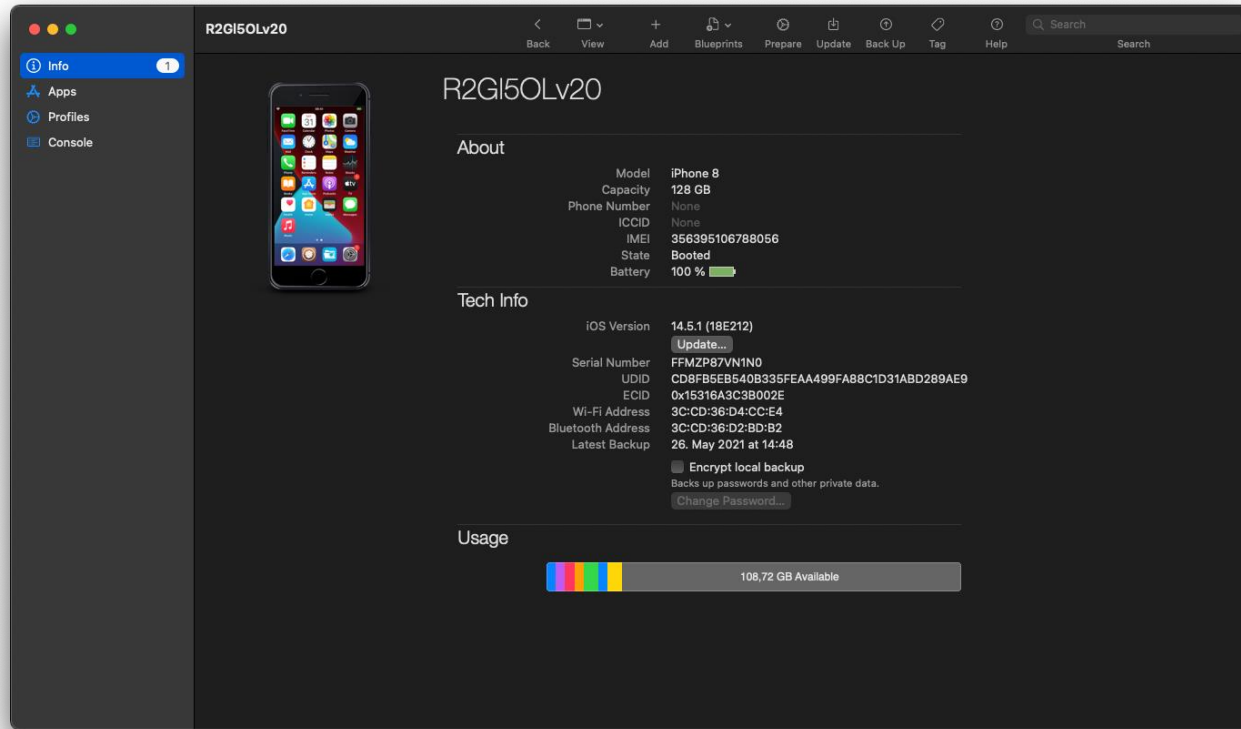
Join

TOP POSTS APRIL 12TH 2020

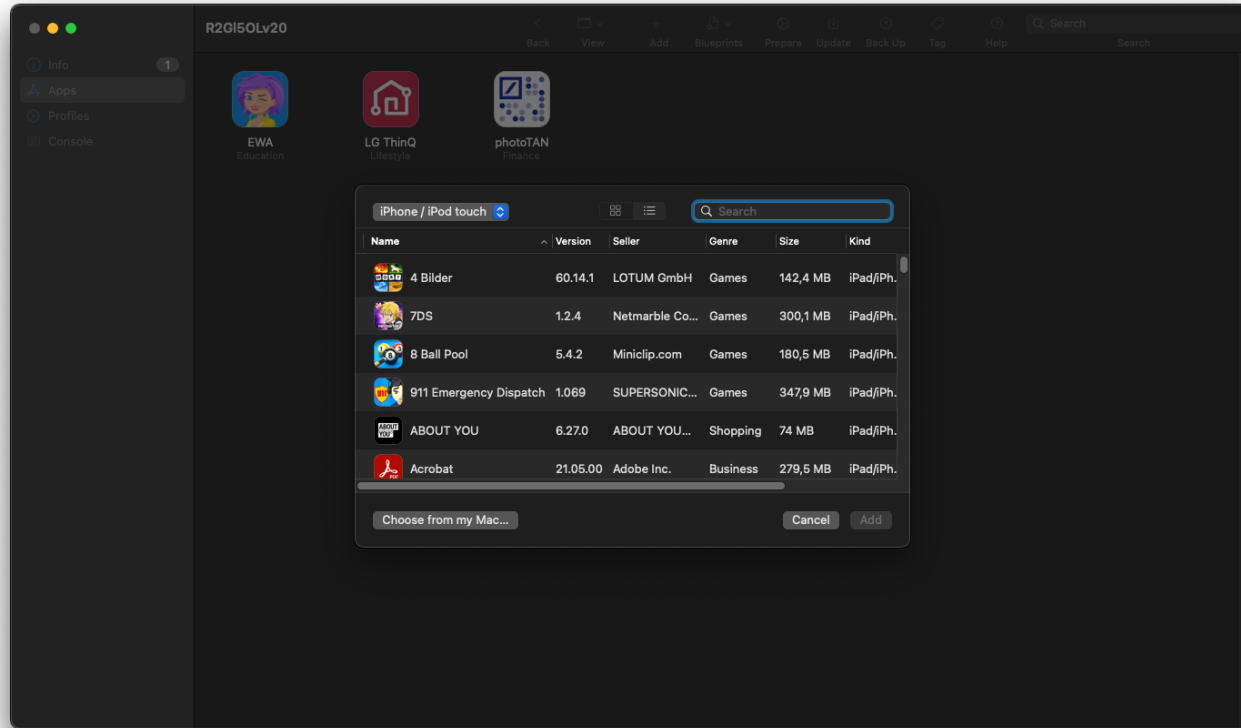
TOP POSTS OF APRIL, 2020

http://web.archive.org/web/20210527200153if_/https://www.reddit.com/r/ITunes/comments/g01qqh/itunes_12653_working_with_ios_13/

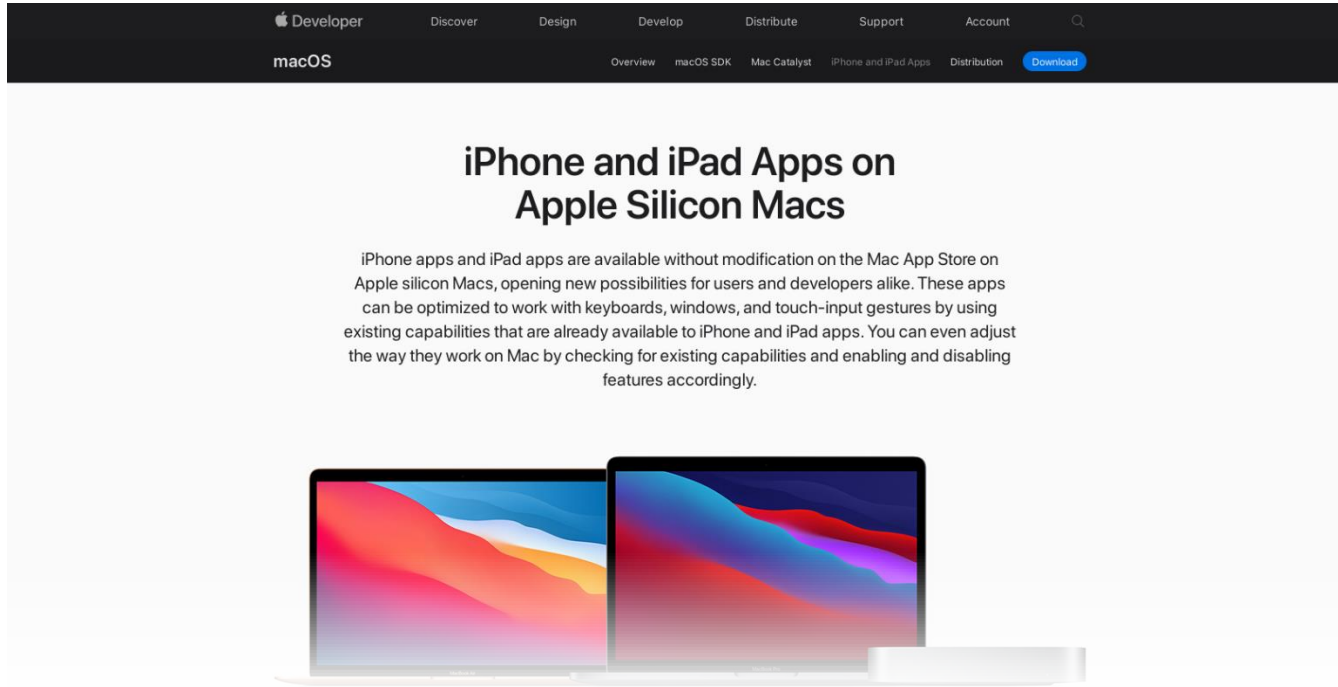
Officially supported 2.0



Officially supported 2.0—not quite, though



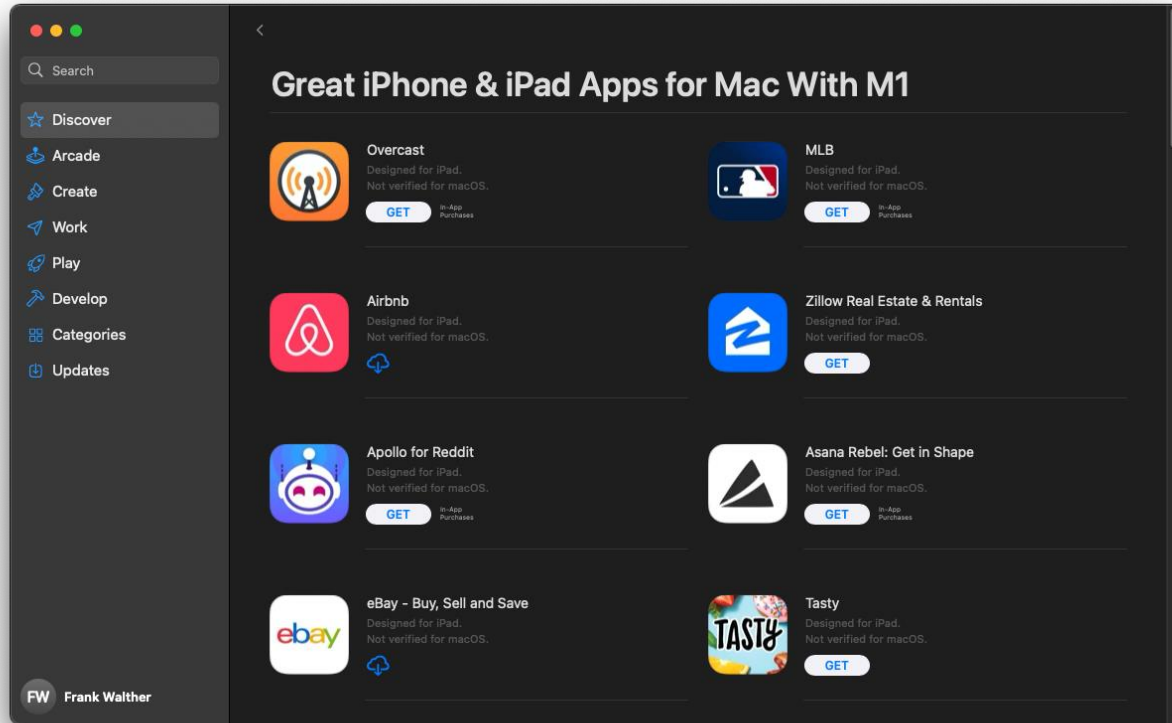
Officially supported 3.0



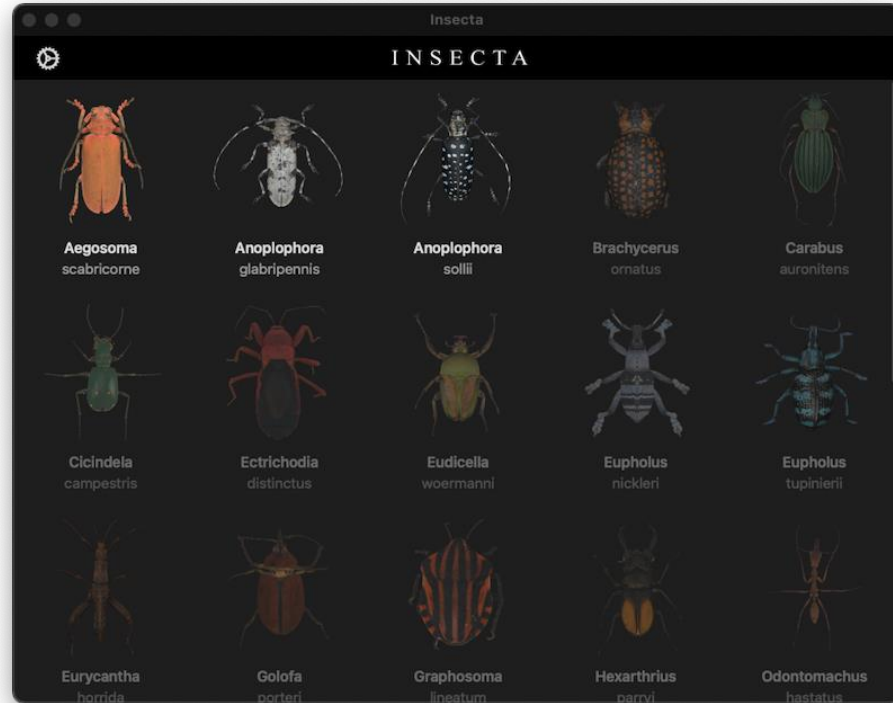
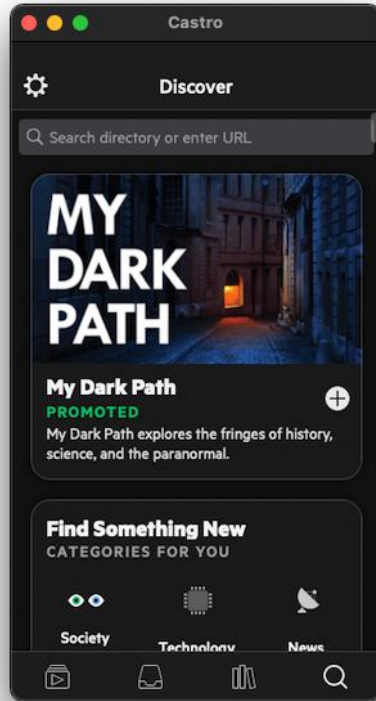
The screenshot shows the top navigation bar of the Apple Developer website with links for Discover, Design, Develop, Distribute, Support, and Account. Below the navigation, the 'macOS' section is active, with a 'Download' button. The main heading reads 'iPhone and iPad Apps on Apple Silicon Macs'. The text below explains that iPhone and iPad apps are available on Apple silicon Macs without modification, and can be optimized for keyboards, windows, and touch-input gestures. At the bottom of the page, there is an image of two laptops displaying colorful abstract wallpapers.

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

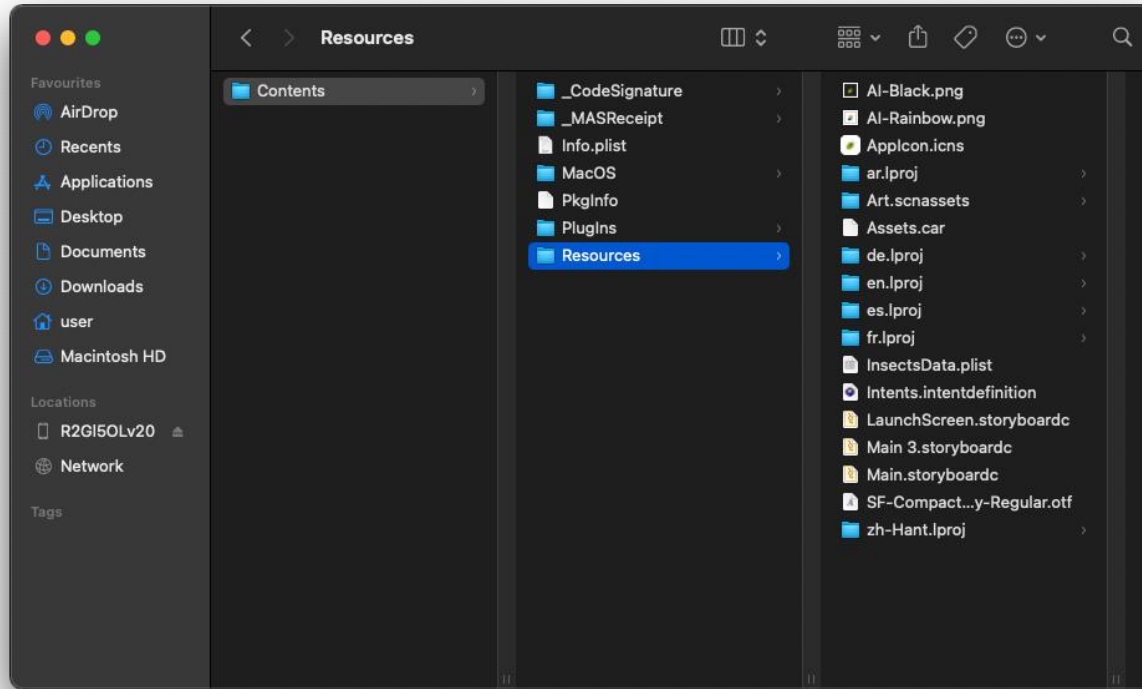
Officially supported 3.0



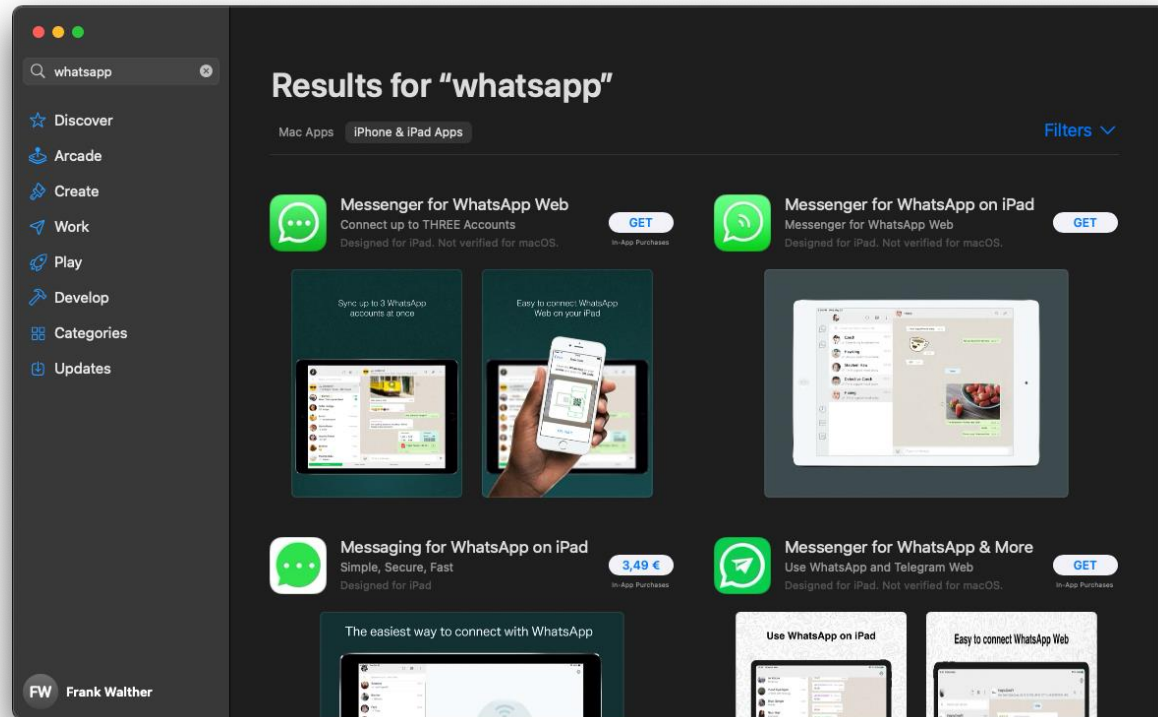
Officially supported 3.0



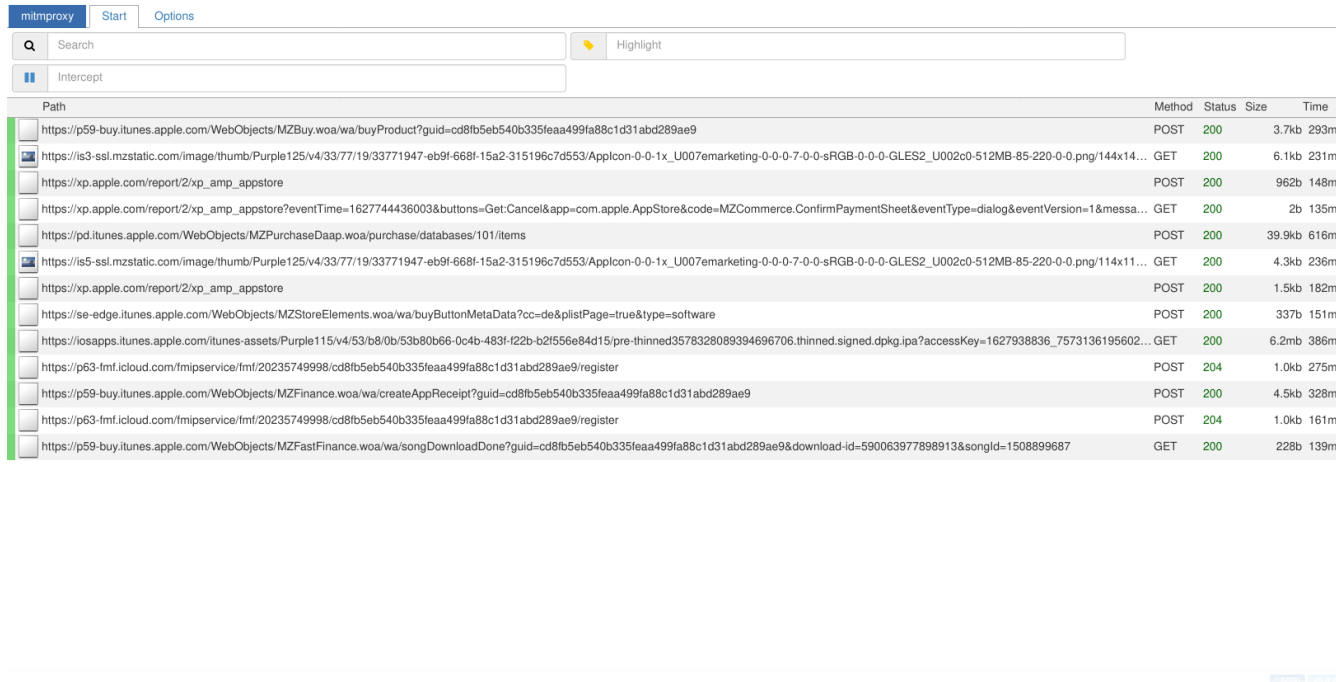
Probably just the .ipa?



Not all of them, though

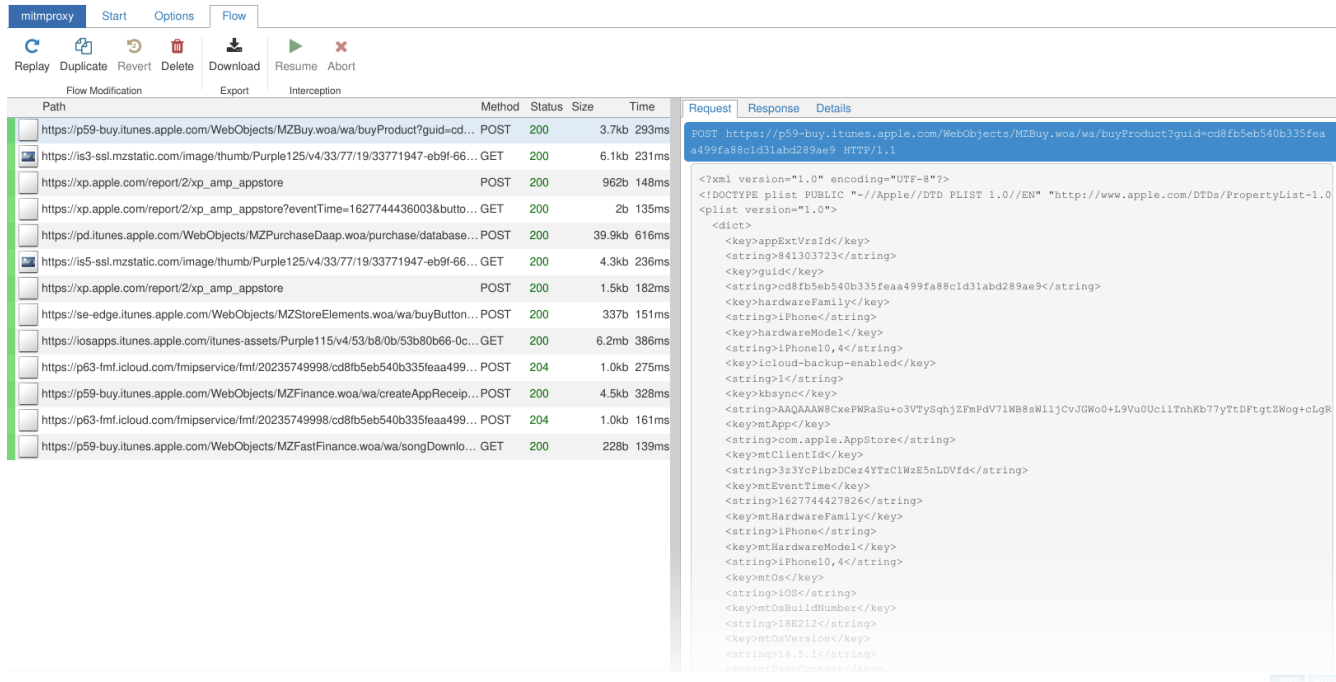


How does the App Store do it?



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-0-0-0-7-0-0-sRGB-0-0-0-GLES2_U002c0-512MB-85-220-0-0.png/144x144... https://xp.apple.com/report/2/xp_amp_appstore	GET	200	6.1kb	231ms
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&messa...	POST	200	962b	148ms
https://pd.itunes.apple.com/WebObjects/MZPurchaseDaap.woa/purchase/databases/101/items	GET	200	2b	135ms
https://is5-ssl.mzstatic.com/image/thumb/Purple125/v4/33/77/19/33771947-eb9f-668f-15a2-315196c7d553/AppIcon-0-0-1x_U007emarketing-0-0-0-7-0-0-sRGB-0-0-0-GLES2_U002c0-512MB-85-220-0-0.png/114x114...	POST	200	39.9kb	616ms
https://is5-ssl.mzstatic.com/image/thumb/Purple125/v4/33/77/19/33771947-eb9f-668f-15a2-315196c7d553/AppIcon-0-0-1x_U007emarketing-0-0-0-7-0-0-sRGB-0-0-0-GLES2_U002c0-512MB-85-220-0-0.png/114x114...	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.thinned.signed.dpkg.ipa?accessKey=1627938836_7573136195602...	GET	200	6.2mb	386ms
https://p63-fmf.icloud.com/fmpservice/fmf/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-fmf.icloud.com/fmpservice/fmf/20235749998/cd8fb5eb540b335feaa499fa88c1d31abd289ae9/register	POST	204	1.0kb	161ms
https://p59-buy.itunes.apple.com/WebObjects/MZFastFinance.woa/wa/songDownloadDone?guid=cd8fb5eb540b335feaa499fa88c1d31abd289ae9&download-id=590063977898913&songId=1508899687	GET	200	228b	139ms

How does the App Store do it?



The screenshot shows the mitmproxy interface with the 'Flow' tab selected. The top toolbar includes icons for Replay, Duplicate, Revert, Delete, Download, Resume, and Abort. Below the toolbar are sections for Flow Modification, Export, and Interception. The main area displays a list of intercepted flows with columns for Path, Method, Status, Size, and Time. The selected flow is a POST request to `https://p59-buy.itunes.apple.com/WebObjects/MZBuy.woa/wa/buyProduct?guid=cd...`. The right pane shows the request details, including the URL and the XML body of the request.

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/2/xp_amp_appstore	POST	200	962b	148ms
https://xp.apple.com/report/2/xp_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/2/xp_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/53b80b66-0c...	GET	200	6.2mb	386ms
https://p63-fmf.icloud.com/fmpservice/fmf/20235749998/cd8fb5eb540b335feaa499...	POST	204	1.0kb	275ms
https://p59-buy.itunes.apple.com/WebObjects/MZFinance.woa/wa/createAppReceip...	POST	200	4.5kb	328ms
https://p63-fmf.icloud.com/fmpservice/fmf/20235749998/cd8fb5eb540b335feaa499...	POST	204	1.0kb	161ms
https://p59-buy.itunes.apple.com/WebObjects/MZFastFinance.woa/wa/songDownlo...	GET	200	228b	139ms

```
POST https://p59-buy.itunes.apple.com/WebObjects/MZBuy.woa/wa/buyProduct?guid=cd8fb5eb540b335feaa499fa88c1d31abd289ae9 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.dtd">
<plist version="1.0">
  <dict>
    <key>appExtVrsId</key>
    <string>841303723</string>
    <key>guid</key>
    <string>cd8fb5eb540b335feaa499fa88c1d31abd289ae9</string>
    <key>hardwareFamily</key>
    <string>iPhone</string>
    <key>hardwareModel</key>
    <string>iPhone10,4</string>
    <key>iCloud-backup-enabled</key>
    <string>1</string>
    <key>kbaync</key>
    <string>AAQAAW8CxePWRaSu+o3VtYsqhj2FmPdV71WB8sM1jCvJGwo0+L9Vu0Uc1lTnhKb77yTtDFgtZWog+cLgR</string>
    <key>mtApp</key>
    <string>com.apple.AppStore</string>
    <key>mtClientId</key>
    <string>3z3YcPlbzDcez4YTtClWzE5nLDVfd</string>
    <key>mtEventTime</key>
    <string>1627744427826</string>
    <key>mtHardwareFamilies</key>
    <string>iPhone</string>
    <key>mtHardwareModel</key>
    <string>iPhone10,4</string>
    <key>mtOs</key>
    <string>iOS</string>
    <key>mtOsBuildNumber</key>
    <string>18E212</string>
    <key>mtOsVersion</key>
    <string>14.5.1</string>
    <key>mtPanoContext</key>
```

How does the App Store do it?

The screenshot shows the mitmproxy interface with the 'Flow' tab selected. The top navigation bar includes 'mitmproxy', 'Start', 'Options', and 'Flow'. Below this are icons for 'Replay', 'Duplicate', 'Revert', 'Delete', 'Download', 'Resume', and 'Abort'. The main area is divided into 'Flow Modification', 'Export', and 'Interception' sections.

Path	Method	Status	Size	Time
https://p59-buy.itunes.apple.com/WebObjects/MZBuy.wa/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/2/xp_amp_appstore	POST	200	962b	148ms
https://xp.apple.com/report/2/xp_amp_appstore?eventTime=1627744436003&butto...	GET	200	2b	135ms
https://pd.itunes.apple.com/WebObjects/MZPurchaseDaap.wa/wa/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/2/xp_amp_appstore	POST	200	1.5kb	182ms
https://se-edge.itunes.apple.com/WebObjects/MZStoreElements.wa/wa/buyButton...	POST	200	337b	151ms
https://iosapps.itunes.apple.com/itunes-assets/Purple115/v4/53/b8/0b/53b80b66-0c...	GET	200	6.2mb	386ms
https://p63-fmf.icloud.com/fmpservice/fmf/20235749998/cd8fb5eb540b335faea499...	POST	204	1.0kb	275ms
https://p59-buy.itunes.apple.com/WebObjects/MZFinance.wa/wa/createAppReceip...	POST	200	4.5kb	328ms
https://p63-fmf.icloud.com/fmpservice/fmf/20235749998/cd8fb5eb540b335faea499...	POST	204	1.0kb	161ms
https://p59-buy.itunes.apple.com/WebObjects/MZFastFinance.wa/wa/songDownlo...	GET	200	228b	139ms

The detailed view of the selected request shows the following information:

- Request:** GET https://iosapps.itunes.apple.com/itunes-assets/Purple115/v4/53/b8/0b/53b80b66-0c4b-483f-f22b-b2f556e84d15/pre-thinned3578328089394696706.thinned.signed.dpkg.ipa?accessKey=1627938836_7573136195602413663_z4T1DTWf4Qs%2F3sPnbaMaYwLJr%2BqoYRUuSVFukkMQHf%2B23ihw8vDip3lGyNRVOREjope2G%2BnOh9S9rLfsyKoUdeBLE1D2hAx%2Bc%2FdiPk9KoOweBPLZ09u3AdmiLklzJHGZ2SawUgfwVL5781CORGEAt6hKeOOC67gWdHauNJCddhMVFJPLlp6im95t1P15NLSNrtHkwbvzIw88%2Bf0vP4Yg139%3D HTTP/1.1
- Response:** Host: iosapps.itunes.apple.com; Apple-Download-Type: buy; Accept: */*; User-Agent: com.apple.appstored/1.0 iOS/14.5.1 model1/iPhone10,4 hwp/t8015 build/18E212 (6; dt:160) AMS/1; Accept-Language: en-us; Accept-Encoding: gzip, deflate, br; Connection: keep-alive.
- Details:** Request content missing.

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+o3VTySqhjZFmPdV71WB8sWlljCvJGwo0+L9Vu0UcilTnhKb77yTtDFtgtZWog+cLgRrFg
    5dyPoHbgK5LsSIRKTJ6fddbnpnk1YXj/3F4CXwLI9xZwecRfiREfpu89yXK7T04q3L6fOLux6uPdNUmo+YaLvYPeZXfU1
    Oh1HgDODF31ZH91duBHw2dV1AI0EztNjGm00ldTT5d8RwgVuWLCohiEksnguxd0tACECxYIpDtPL8PaY9ex4bNbj1y2xG
    jBYUs0kr7wMhMZZQeaeXCNS2qX+ZNNpBq+m4J1drkgQ+1WdtkKkVE4J5iw3j9bpiSwQfpc2KYm2B8Jhd0R/hZYRTDsV+
    Vw0tG4QPcE9/zNq/KgRXp+yEBE6FL6WkKprg72ttDulrB/idwKy1Z6XUcLi1jdrHZV</string>
  </dict>
</plist>
```

kbsync, you say?



The screenshot shows a forum post on the '看雪论坛' (Kexue Forum) website. The post title is '[求助]有人研究过itunes kbsync这个算法吗?' (Help: Has anyone researched the iTunes kbsync algorithm?). The post is dated 2012-10-3 17:02 and has 15467 views. The content discusses the algorithm used for app verification on iTunes, providing a long alphanumeric string: AIAALNZmi92d8M2KkNEHZLZvnxT/toPqCOL2B9FdbQksfimEcV+e5sRKjc8JS489ZG w+MwVh8ip5oTWtU1hOW5 A7pm4R1QVRjyp28eLr2iWXswL9EGKcwqH7eku4Ef25kQ2g==. The author mentions they lack experience with reverse engineering and OD, and provides a link to a thread on the forum. Below the post, there are icons for '收藏 +1' (Bookmark +1), '点赞' (Like), '打赏' (Tip), and '分享' (Share). On the right side, there is a user profile for 'cantellow' with 5 posts, 8 replies, and a rank of 10. Below the profile is a list of other articles by the user, including '[求助]某app加密接口', '[未解决]折腾一个月了, 关于网络验证机制', '[求助]有人研究过itunes kbsync这个算法吗?', and '[求助]高手看看ollyDBG这段汇编'. At the bottom right, there is a blue banner for '看雪安卓应用安全能力认证 重磅出炉' (Kexue Android Application Security Certification Officially Released).

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

kbsync, you say?

Хабр | КАК СТАТЬ АВТОРОМ | Питчи джава-работодателя | DS, DE, ETL – кто-нибудь знает, что всё это значит?

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

ZonD80 7 августа 2012 в 15:19

Реверс-инжиниринг in-app покупок Apple. (или «там» все тоже ленивые)

Информационная безопасность

Intro

Привет, хабр! Ты наверное знаешь о недавних событиях, которые распиарили по интернету как «взлом» системы in-app покупок apple. Так вот, это было не совсем так. Это даже не было взломом. И ключевые выводы, которые я сделал:

- Закрывать<->Защищенность
- В Apple тоже очень даже ленивые люди работают

Так вот, я хочу рассказать как и что делалось, добавить немного сорцов, да и вообще, попытаться направить мысли в правильное русло.

Технология

В расцвет облачных и сервисных инфраструктур, очень многое полагается именно на серверную часть. И зря. Как показала практика, как разработчики клиентов, так и разработчики серверов очень лениятся. Только в случае с последними это выливается в большой скандал.

54 | 131 | 25

ЧИТАЮТ СЕЙЧАС

Вертолеты на Марсе жужжат и не отбрасывают тень
26K | 49

Почему я отказался от 18 тысяч долларов по баунти-программе Apple
10K | 11

Космонавты впервые вошли в модуль «Наука»
7.4K | 57

[Личный опыт] Лондон: не всегда мечта для программиста. Как жителя в столице Британии во время коронавируса
2.8K | 2

Пользователи объяснили, почему Google необычно обрабатывает строку «Turn! Turn! Turn!»
9.3K | 3

«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

赞 1

分享

闲得蛋疼, 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, 混个熟练。

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 the Ymsky website interface. At the top, there are navigation links for Weibo, Baidu Space, Technical Support, Programmers' Publicity, and a QR code to join a group. The main header features the '源码世界' (Source Code World) logo and a search bar. Below the header is a navigation menu with categories like Home, Source Code Download, Code Sharing, etc. The main content area displays a post titled 'itunes 模拟登陆' (iTunes Simulation Login) by '源码世界' from 2014-03-10. The code is as follows:

```
#encoding=utf-8
import urllib2
import httplib
import urllib
import cookielib
import urllib2
import socket
import json
import ssl
from xml.dom.minidom import parseString
import time
from sgmlib import SXMLParser
import re

timeout = 40
socket.setdefaulttimeout(timeout)
sleep_download_time= 10
time.sleep(sleep_download_time)

def link_server(host):
    """ link server
```

On the right side, there is a '分类列表' (Category List) table:

Java	linux
Python	SQL
C/C++	C#
JavaScript	PHP
Perl	Android
Ruby/Rails	HTML
XML	CSS
ASP/Basic	Delphi/Pascal
Scala	Groovy
Lua	IOS
Google Go	Flash/ActionScript/Flex
WPF/SliverLight	Shell/批处理
其他	Objective-C
ASP.NET	JSP
网站安全	

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

Some one else must have figured this out, right?

iMazing Features - Reviews Download Enterprise Store Support - Blog English -

Download & Install Apps to iPhone or iPad from Mac & PC

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.

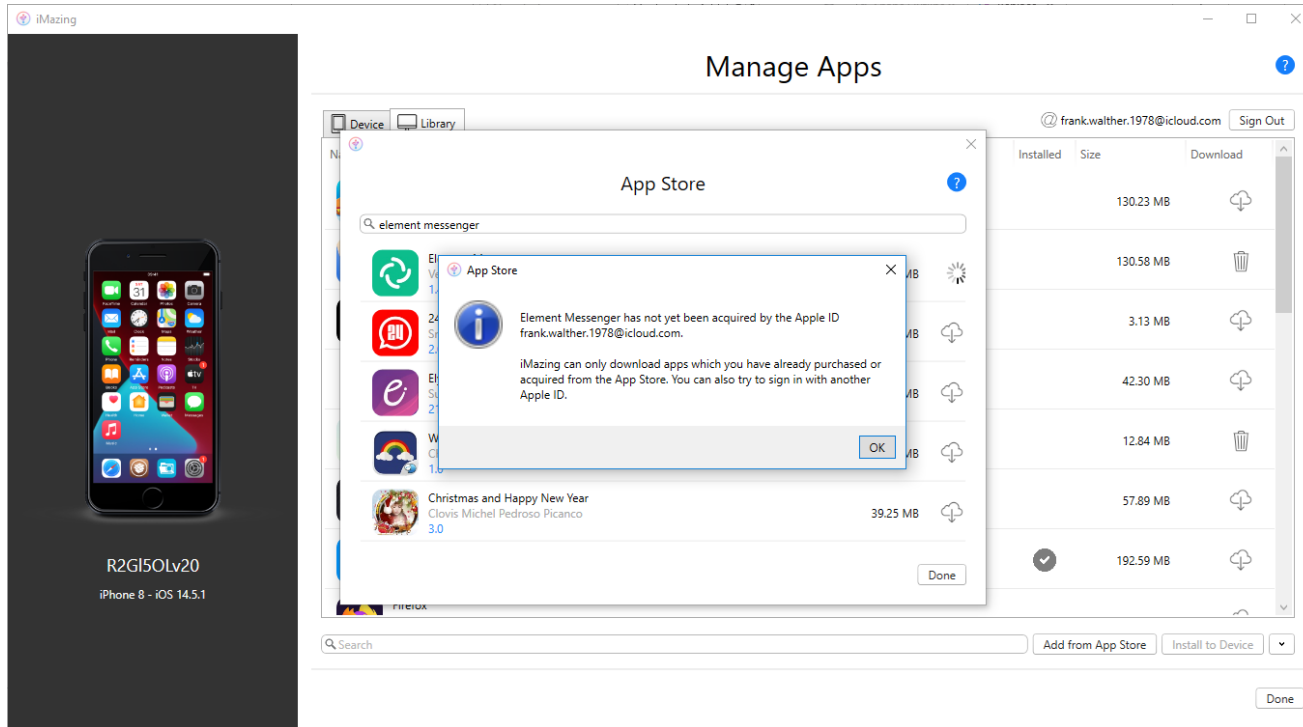
[Free Download](#) [Buy Now](#)

Apple Windows iOS 15

Phone Contacts Calendars Other Data **Apps** Quick Transfer File System Transfer Backup Extractor

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

Not so iMazing, after all

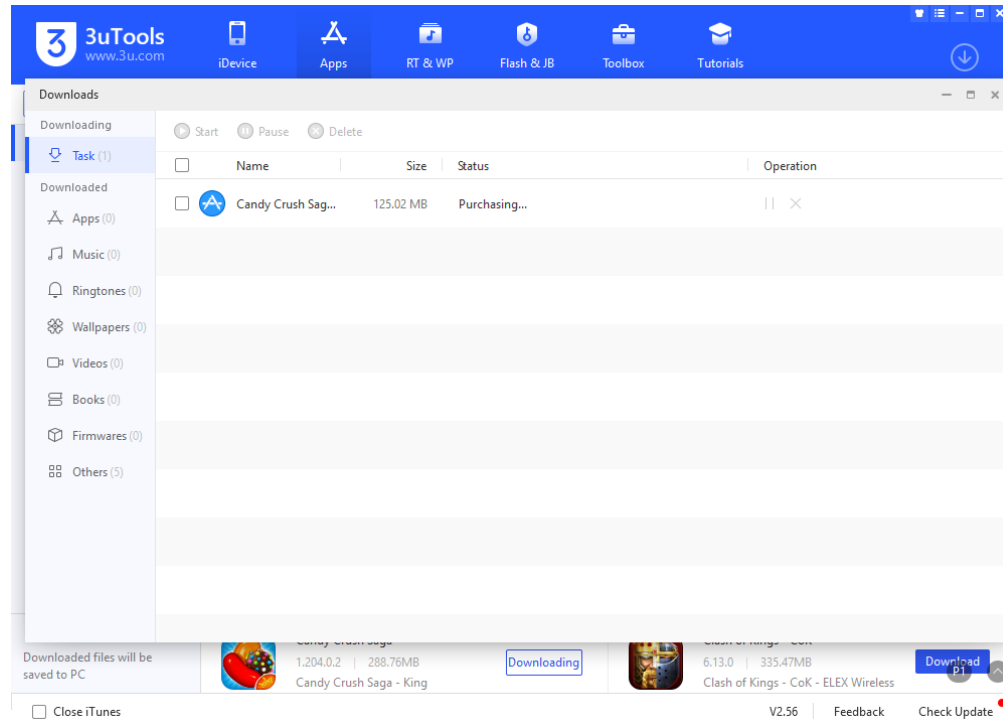


3uTools saves the day

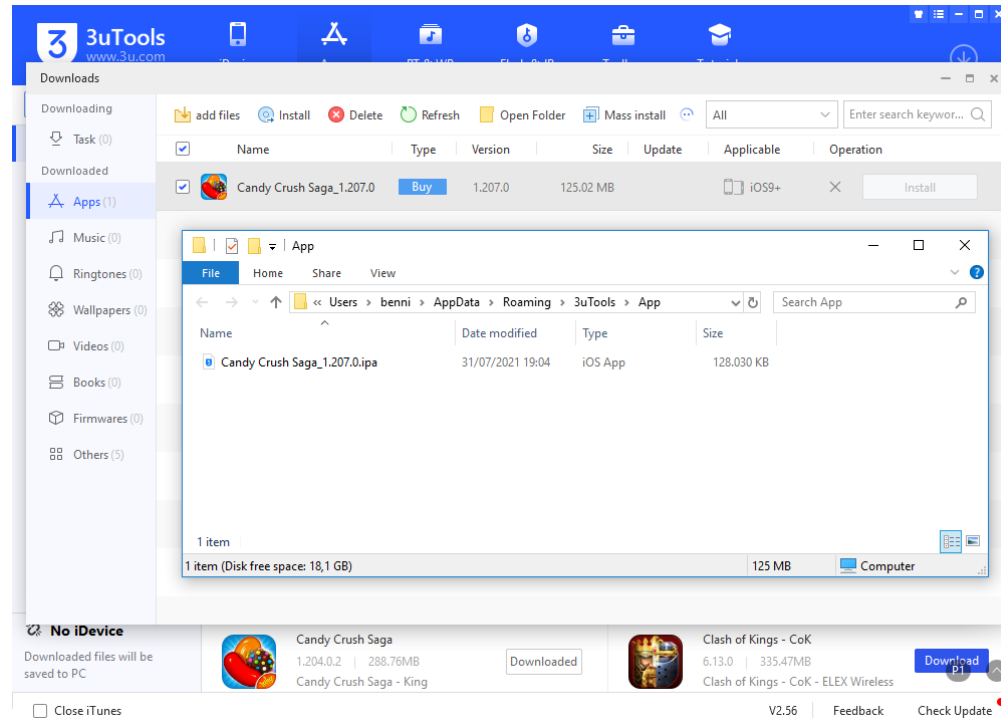
The screenshot shows the 3uTools website interface. At the top, there is a blue navigation bar with the 3uTools logo and website URL (www.3u.com). Below the navigation bar, there are tabs for 'iPhone' and 'iPad', a search bar for 'Search app & games', and an 'Apple ID' field containing 'frank.walther.1978@iclou...'. The main content area is divided into sections: 'Featured' (with sub-sections for 'Apps' and 'Games'), and 'No iDevice'. The 'Featured' section contains a large banner with the text 'Why you must bind Apple ID before purchasing apps?' and several app icons. Below the banner, there are six app listings, each with an icon, name, version, size, developer, and a 'Download' button. The 'No iDevice' section contains one app listing: Candy Crush Saga.

App Name	Version	Size	Developer	Action
Clash Royale	3.3.2	188.15MB	Clash Royale - Supercell	Download
Mobile Strike	8.2.2.638	215.73MB	Mobile Strike - Epic War LLC	Download
Game of War - Fire Age	8.2.2.638	278.37MB	Game of War - Fire Age - Machine Z...	Download
Clash of Clans	13.576.8	237.88MB	Clash of Clans - Supercell	Download
Candy Crush Saga	1.204.0.2	288.76MB	Candy Crush Saga - King	Download
Clash of Kings - CoK	6.13.0	335.47MB	Clash of Kings - CoK - ELEX Wireless	Download

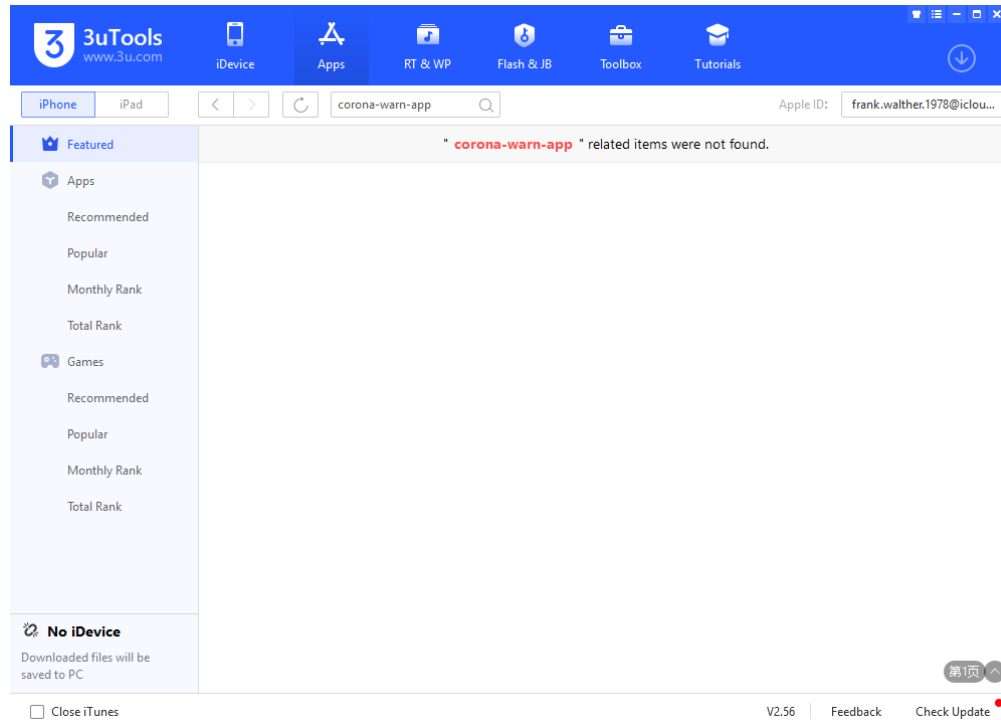
3uTools saves the day



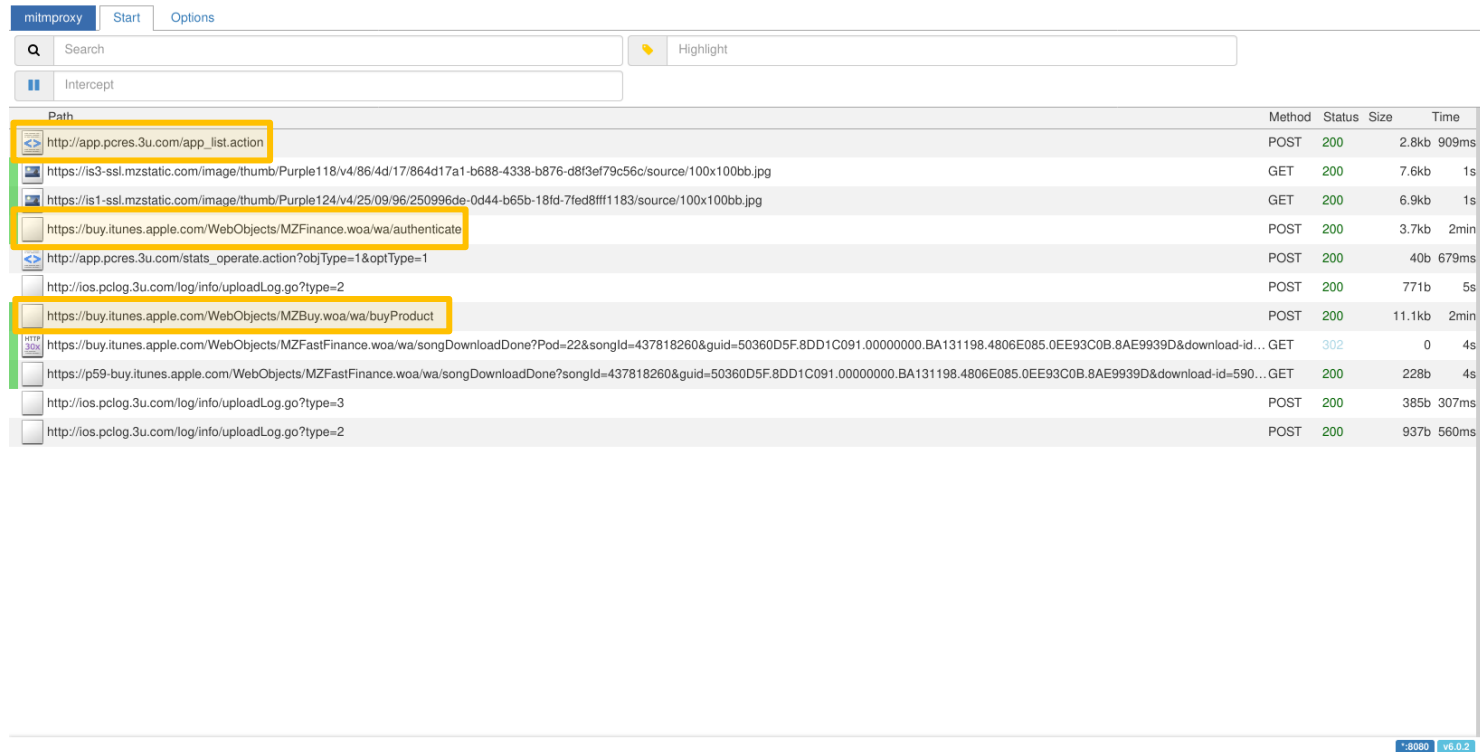
3uTools saves the day



A final road block



Or just a minor hurdle?



The screenshot shows the mitmproxy interface with a list of intercepted HTTP requests. The interface includes a search bar, a 'Highlight' button, and an 'Intercept' toggle. The main area displays a table of requests with columns for Path, Method, Status, Size, and Time. Several requests are highlighted with yellow boxes:

Path	Method	Status	Size	Time
http://app.pcores.3u.com/app_list.action	POST	200	2.8kb	909ms
https://is3-ssl.mzstatic.com/image/thumb/Purple118/v4/86/4d/17/864d17a1-b688-4338-b876-d8f3ef79c56c/source/100x100bb.jpg	GET	200	7.6kb	1s
https://is1-ssl.mzstatic.com/image/thumb/Purple124/v4/25/09/96/250996de-0d44-b65b-18fd-7fed8fff1183/source/100x100bb.jpg	GET	200	6.9kb	1s
https://buy.itunes.apple.com/WebObjects/MZFinance.woa/wa/authenticate	POST	200	3.7kb	2min
http://app.pcores.3u.com/stats_operate.action?objType=1&optType=1	POST	200	40b	679ms
http://ios.pclg.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/songDownloadDone?Pod=22&songId=437818260&guid=50360D5F8DD1C091.00000000.BA131198.4806E085.0EE93C0B.8AE9939D&download-id...	GET	302	0	4s
https://p59-buy.itunes.apple.com/WebObjects/MZFastFinance.woa/wa/songDownloadDone?songId=437818260&guid=50360D5F8DD1C091.00000000.BA131198.4806E085.0EE93C0B.8AE9939D&download-id=590...	GET	200	228b	4s
http://ios.pclg.3u.com/log/info/uploadLog.go?type=3	POST	200	385b	307ms
http://ios.pclg.3u.com/log/info/uploadLog.go?type=2	POST	200	937b	560ms

At the bottom right of the interface, there is a status bar showing ':0080 v6.0.2'.

Doesn't that request look familiar?

The screenshot shows the mitmproxy interface. The top bar includes 'mitmproxy', 'Start', 'Options', and 'Flow'. Below this are icons for 'Replay', 'Duplicate', 'Revert', 'Delete', 'Download', 'Resume', and 'Abort'. The main area is divided into 'Flow Modification' and 'Export' sections. A table lists several requests, with the last one highlighted in blue. The detailed view of this request shows the following headers and body:

Path	Method	Status	Size	Time
http://app.pcores.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.pcores.3u.com/stats_operate.action?objType=1&optType=1	POST	200	40b	679ms
http://ios.pclg.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/songDownlo...	GET	200	228b	4s
http://ios.pclg.3u.com/log/info/uploadLog.go?type=3	POST	200	385b	307ms
http://ios.pclg.3u.com/log/info/uploadLog.go?type=2	POST	200	937b	560ms

Request Details:

```
POST https://buy.itunes.apple.com/WebObjects/MZBuy.woa/wa/buyProduct HTTP/1.1
Host: buy.itunes.apple.com
User-Agent: iTunes/11.4 (Windows; Microsoft Windows 7 x86 Ultimate Edition S
ervice Pack 1 (Build 7601)) AppleWebKit/536.30.1
Accept: */*
Cookie: ns-mzf-inst=104-14-443-52-240-9019-597195-59-st44; countryVerifi
ed=1; hsacent=1; mzf_in=597195; session-store-id=933443C4AC59F08
CD0BC4688F05D8816; NSC_nagjobodf-bopo-gppm*0=ffffff0944761c455
25d5f4f58455e445a4a42378b; mz_mt0-20235749998=An1mEe09CRmJKIVUsp
wic8WHPG5kTDHJyLd+EvyH10j3HFqo/zsY23n5lb8oKEuhF5aFVXKezcnHAdahD
cGvP21sJgUg8xtcz+dHoryivpmVQM2+m2mV6ZSPrO7NZ4FKJT9Ircrbv6bLSA60S
/2Kxmp8ipP5cncGwF70xGBFI1AAG1ZjG1zz+JiiDzvfTjYU9I8Ie; X-DsId=2
0235749998; itspod=59; mz_at0-20235749998=AwQAAAECAAGvQAAAAABgr1
Gk4w2EaacJH7Y63804kjh+KngIhV0=; mz_at_ssl-20235749998=AwUAAECAA
GvQAAAAABgr1GkaLZyfxp1H7y1NlyZnwbVnzJvtA=; pldfitcid=ec8960372f
244c3db043866ab575bb91059; vrep=COG0LFLFLEgQIBRAAEgQICBAEgQICAA
EgQIEBAEgQIAhAAEgQIBxAAEgQIDxAAEgQIARAMEgQICRAEgQIERAAEgQIAxAA
EgQIDRAEgQIBhAAEgQIBBAEgQICxAAEgQIDhAAEgQIDBAA; wosid-lite=7WV
4fPoxJWF4bbfun8BF0
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: AwIAAAECAAGvQAAAAABgr1Gkf7sNCsrOrfwplAtNZOYjaK1ZHyI=
X-DsId: 20235749998
Connection: Close
Content-Length: 1323

<?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. At the top, there are tabs for 'mitmproxy', 'Start', 'Options', and 'Flow'. Below these are icons for 'Replay', 'Duplicate', 'Revert', 'Delete', 'Download', 'Resume', and 'Abort'. The main area is divided into two panes. The left pane is a table of network flows, and the right pane shows the details of a selected request and response.

Path	Method	Status	Size	Time
http://app.pcores.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.pcores.3u.com/stats_operate.action?objType=1&optType=1	POST	200	40b	679ms
http://ios.pclg.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/songDownlo...	GET	200	228b	4s
http://ios.pclg.3u.com/log/info/uploadLog.go?type=3	POST	200	385b	307ms
http://ios.pclg.3u.com/log/info/uploadLog.go?type=2	POST	200	937b	560ms

The right pane shows the details of a selected request and response. The request is a GET request to a URL. The response is a JSON object with the following structure:

```
HTTP/1.1 200 OK
{
  "co": 20,
  "list": [
    {
      "appname": "Clash For Dawn-3D PVP MMORPG",
      "downloaded": "2",
      "icon": "https://is3-ssl.mzstatic.com/image/thumb/Purple118/v4/86/4d/17/864d17a1-b688-4482",
      "id": 4482,
      "isfull": 0,
      "itemid": "994842141",
      "longversion": "2.0.3",
      "md5": "",
      "minversion": "7.0",
      "path": "",
      "pkagetype": 1,
      "shortversion": "2.0.3",
      "sizebyte": "118799360",
      "slogan": "Clash For Dawn-3D PVP MMORPG - LEDO",
      "slogancolor": "#f0f0f0",
      "sort": 2,
      "sourceid": "com.wanmei.mini.dod.ios.ledo",
      "version": "2.0.3",
      "versionid": "0"
    },
    {
      "appname": "C-Date",
      "downloaded": "2",
      "icon": "https://is3-ssl.mzstatic.com/image/thumb/Purple115/v4/5b/b0/dd/5bb0dd36-303",
      "id": 1775,
      "isfull": 0,
      "itemid": "1078584965",
      "longversion": "4",
      "md5": "",
      "versionid": "0"
    }
  ]
}
```

The only logical solution

```
def response(self, flow: http.HTTPFlow):
    if(flow.request.pretty_url == "http://app.pcrs.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 website interface. At the top, there is a navigation bar with icons for iDevice, Apps, RT & WP, Flash & JB, Toolbox, and Tutorials. Below the navigation bar, there is a search bar and a field for Apple ID. The main content area is divided into a left sidebar and a main grid. The sidebar has categories like Featured, Apps, Games, and No iDevice. The main grid displays a list of recommended apps with their names, versions, sizes, and download buttons. The apps listed are:

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

At the bottom of the interface, there are options to "Close iTunes", "V2.56", "Feedback", and "Check Update".

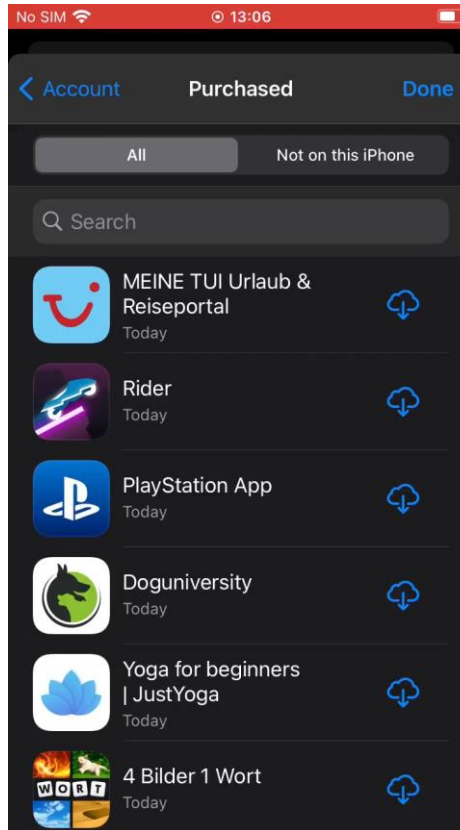
Click, click, click...

The screenshot displays a Windows desktop environment. On the left, a 'Downloads' window is open, showing a list of files being downloaded. The files include 'TikTok_19.5.1.ipa', 'Klarna_21.19.146.ipa', 'Telegram_7.7.ipa', 'YouTube_16.20.5.1...', 'Google_161.1.ipa', 'Teams_3.7.0.ipa', 'Kleinanzeigen_12...', 'Zoom_5.6.4.ipa', 'QRBot_1.9.8.ipa', and 'PictureThis_3.3.1...'. The status of each file is shown, such as '2.31 MB/s' and '67%' for TikTok.

In the bottom-left corner, a terminal window is open, displaying a series of 'clientdisconnect' messages, indicating a high frequency of disconnections from a specific IP address (127.0.0.1).

The main window is the 3uTools application, which is used for managing and downloading apps to an iPhone. The interface shows a list of recommended apps, including Microsoft Word, TIER E-Scooter & E-Roller, Reddit, Royal Match, Water Sort Puzzle, Burger King®, Subway Surfers, mobile.de - Automarkt, Airbnb, wetter.com, and Project Makeover. Each app entry includes its name, version, size, and a 'Download' button. The 'Download' button for '91. Reddit' is highlighted with a mouse cursor.

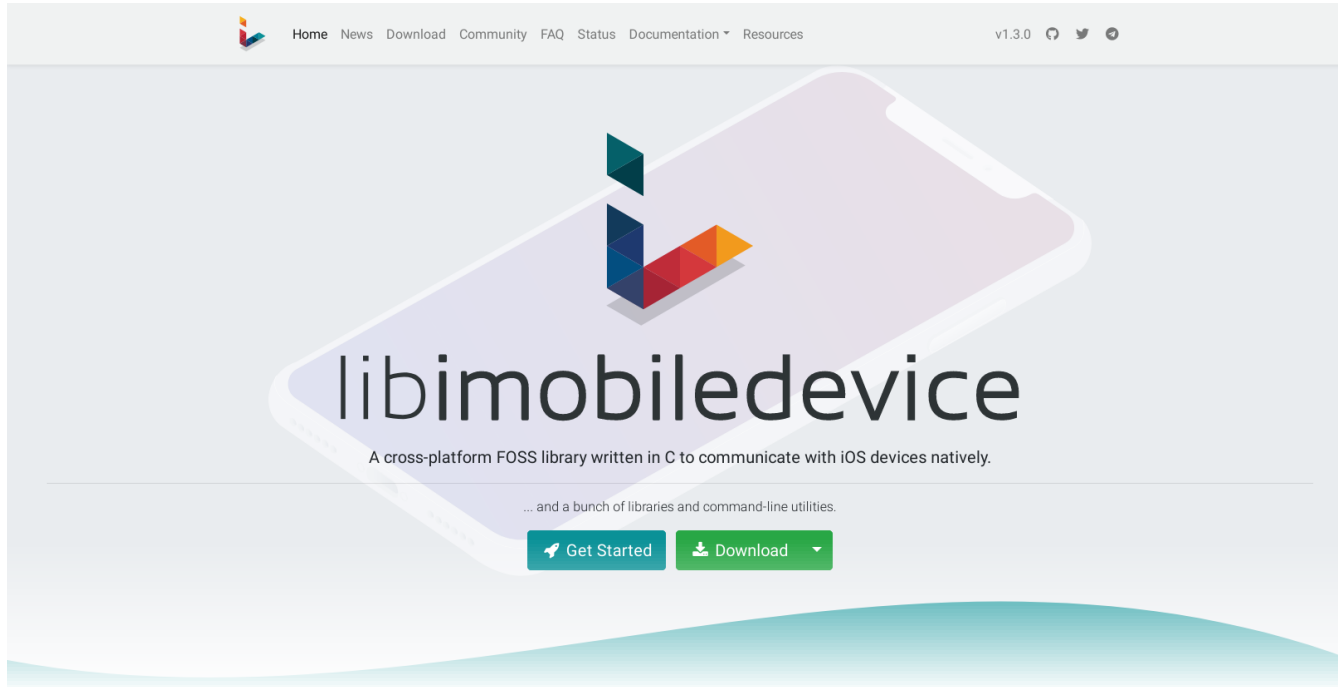
The reward



Automation

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

Automation

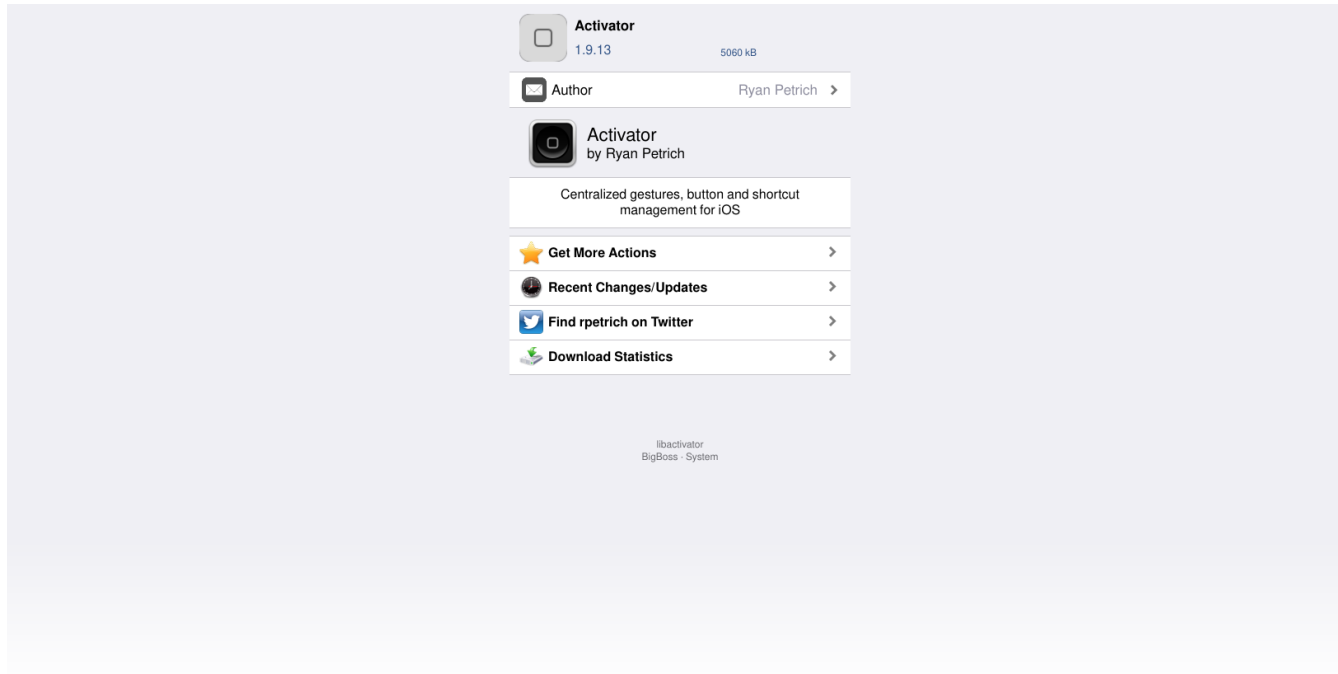


<https://libimobiledevice.org/>

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



<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

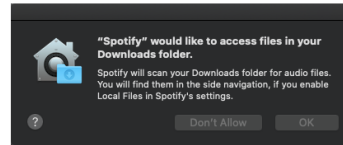
CVE-2020-9934: Bypassing TCC

...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. macOS 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, `tccd`, 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.

```
natt@natt1-MacBook-Pro:~$ ps ax | grep tccd | grep -v grep
163 ?? Ss   0:51.51 /System/Library/PrivateFrameworks/TCC.framework/Resources/tccd_system
561 ?? S     0:26.76 /System/Library/PrivateFrameworks/TCC.framework/Resources/tccd
```

listing currently running TCC daemons

Automatically granting permissions

```
Terminal
R2G150Lv20:~ root# tccutil
-sh: tccutil: command not found
R2G150Lv20:~ root# ps | grep tccd
 2253 ttys000    0:00.01 grep tccd
R2G150Lv20:~ 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
R2G150Lv20:~ root#
```

Automatically granting permissions

The screenshot shows a SQLite database table named 'access' with the following columns: 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, and last_modified. The 'auth_value' column is highlighted in yellow, and a red arrow points from the callout box to a row where auth_value is 0.

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	Filter	0	2	4	1	NULL	NULL	0 UNUSED	NULL	0	1620829599
KTCCServiceLiverpool	com.apple.Health	Filter	0	2	4	1	NULL	NULL	0 UNUSED	NULL	0	1620991202
kTCCServiceUbiquity	com.apple.mobilesafari	Filter	0	2	4	1	NULL	NULL	0 UNUSED	NULL	0	1620991211
kTCCServiceUbiquity	com.apple.iBooks	Filter	0	2	4	1	NULL	NULL	0 UNUSED	NULL	0	1620991213
kTCCServiceUbiquity	com.apple.Passbook	Filter	0	2	4	1	NULL	NULL	0 UNUSED	NULL	0	1620991213
kTCCServiceUbiquity	com.apple.MailCompositionService	Filter	0	2	4	1	NULL	NULL	0 UNUSED	NULL	0	1620991213
kTCCServiceUbiquity	com.apple.mobilemail	Filter	0	2	4	1	NULL	NULL	0 UNUSED	NULL	0	1620991213
kTCCServiceUbiquity	com.apple.DocumentsApp	Filter	0	2	4	1	NULL	NULL	0 UNUSED	NULL	0	1620991214
kTCCServiceUbiquity	com.apple.shortcuts	Filter	0	2	4	1	NULL	NULL	0 UNUSED	NULL	0	1620991214
kTCCServiceLiverpool	com.apple.shortcuts	Filter	0	2	4	1	NULL	NULL	0 UNUSED	NULL	0	1620991272
kTCCServiceLiverpool	com.apple.stocks	Filter	0	2	5	1	NULL	NULL	0 UNUSED	NULL	0	1621001132
kTCCServiceWebKitIntelli...	org.mozilla.ios.Firefox	Filter	0	2	5	1	NULL	NULL	0 UNUSED	NULL	0	1621081431
kTCCServiceWebKitIntelli...	com.apple.mobilesafari	Filter	0	2	5	1	NULL	NULL	0 UNUSED	NULL	0	1621081877
kTCCServiceLiverpool	com.apple.upload-request...	Filter	0	2	4	1	NULL	NULL	0 UNUSED	NULL	0	1623176245
kTCCServiceLiverpool	com.apple.accessibility.Accessibility...	Filter	0	2	5	1	NULL	NULL	0 UNUSED	NULL	0	1623439707
kTCCServiceLiverpool	com.apple.security.cuttlefish	Filter	0	2	4	1	NULL	NULL	0 UNUSED	NULL	0	1623440322

auth_value == 0:
permission not granted

auth_value == 2:
permission granted

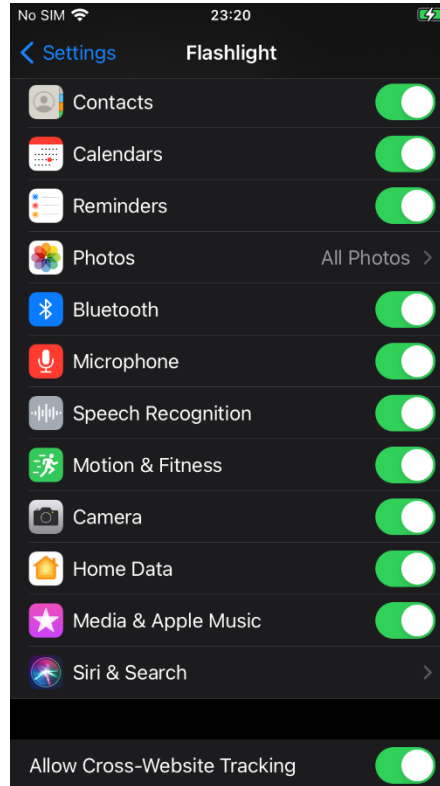
The available permissions

	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”
X	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”
X	kTCCServiceCamera	Camera	“Access the Camera”
X	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 CLLocationAuthorizationStatus status = [CLLocationManager _authorizationStatusForBundleIdentifier:bundleId bundle:nil];
152 if (permissionList.count == 0 && (status == kCLLocationAuthorizationStatusNotDetermined || status == kCLLocationAuthorizationStatusRestricted)) {
153     FR_Log(@"No permissions requested! Do not show reset permission");
154     return originalShortcutItems;
155 }
156 FR_Log(@"Requested: %@, locationStatus: %@, permissionList: %@",
157        SBSApplicationShortcutItem *shortcutItem = [[objc_getClass("SBSApplicationShortcutItem") alloc] init];
158 shortcutItem.type = tweakIdentifier;
159 shortcutItem.localizedTitle = @"Reset permission";
160 shortcutItem.bundleIdentifierToLaunch = bundleId;
161
162 NSMutableArray *newShortcutItems = [originalShortcutItems mutableCopy] : [NSMutableArray arrayWithCapacity:1];
163 [newShortcutItems addObject:shortcutItem];
164 FR_Log(@"New shortcutItems: %@", newShortcutItems);
165 return newShortcutItems;
166 }
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 [C API](#).

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

```
Terminal
> 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.apple.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/PrivateFrameworks/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_
setAuthorizationStatus_forBundleIdentifier_
setAuthorizationStatus_forBundle_
```

Frida is (really!) great

```
Terminal
~ 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:0x4 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:

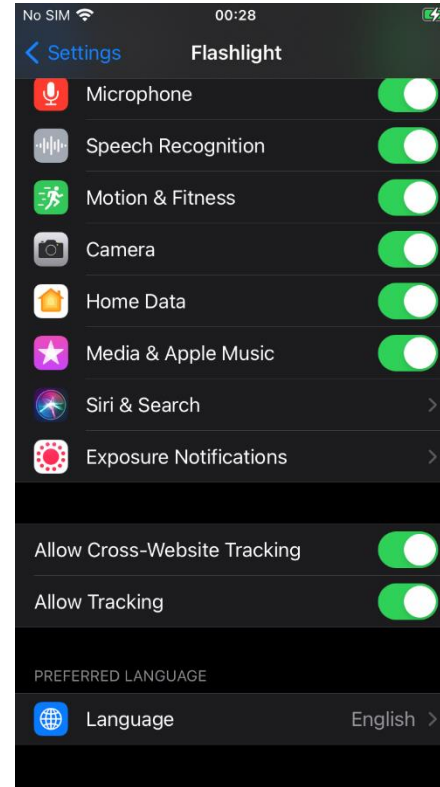
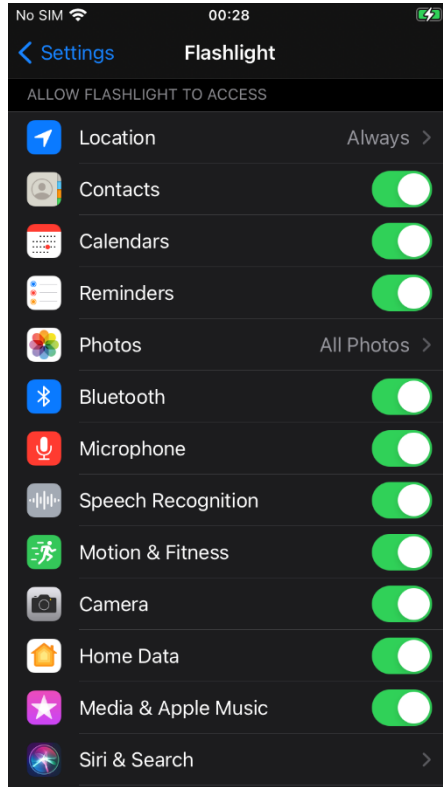
```
// For the running app.
```

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

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

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

(Truly) ALL THE PERMISSIONS!

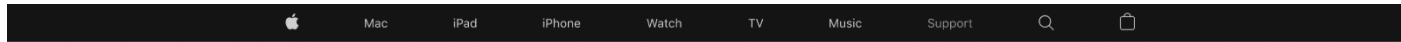


Programmatically seeding the clipboard

- 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.

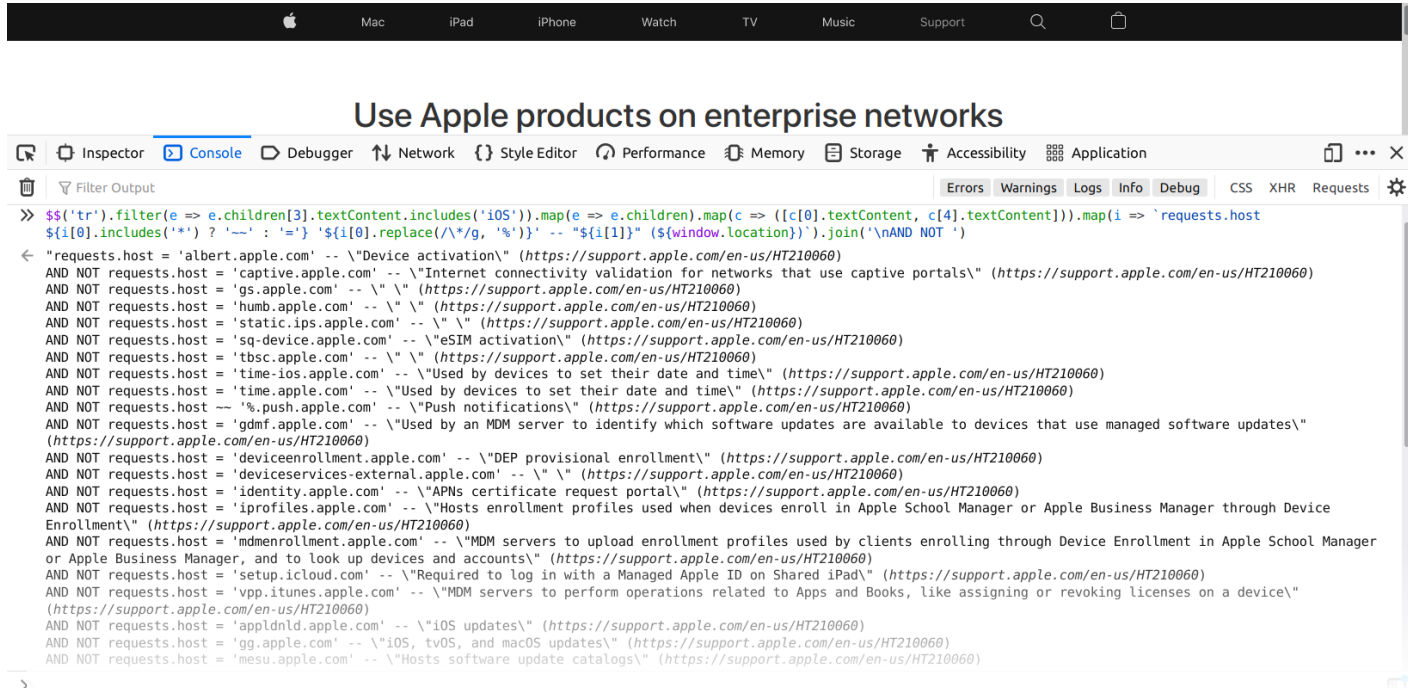
Device setup

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, 80	TCP	iOS, tvOS, and macOS		Yes

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

Background noise filter



The screenshot shows a web browser window with the title "Use Apple products on enterprise networks". The address bar contains the URL <https://support.apple.com/en-us/HT210060>. The browser's developer console is open, displaying a complex JavaScript filter function. The function is designed to filter out requests from various Apple-related domains and services. The console output shows the function being executed and the resulting list of filtered requests.

```
Filter Output
Errors Warnings Logs Info Debug CSS XHR Requests
>> $$('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' -- \"eSIM 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 = 'appldnld.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?



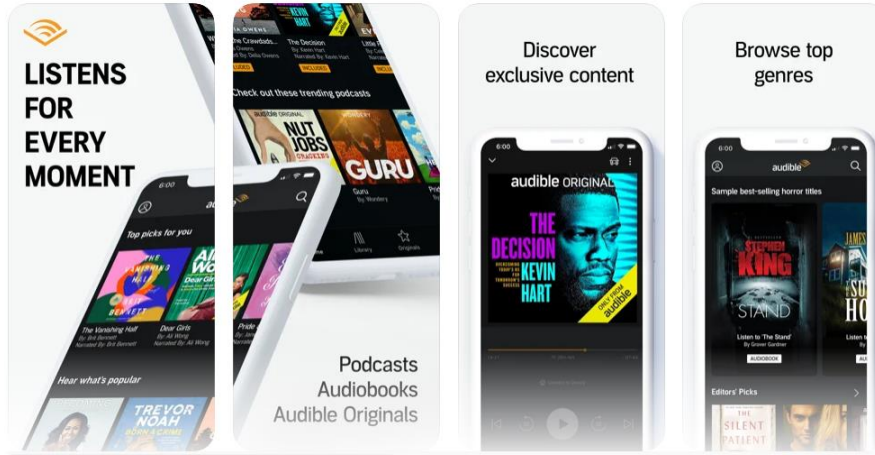
Audible audiobooks & podcasts 4+

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>



```
"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

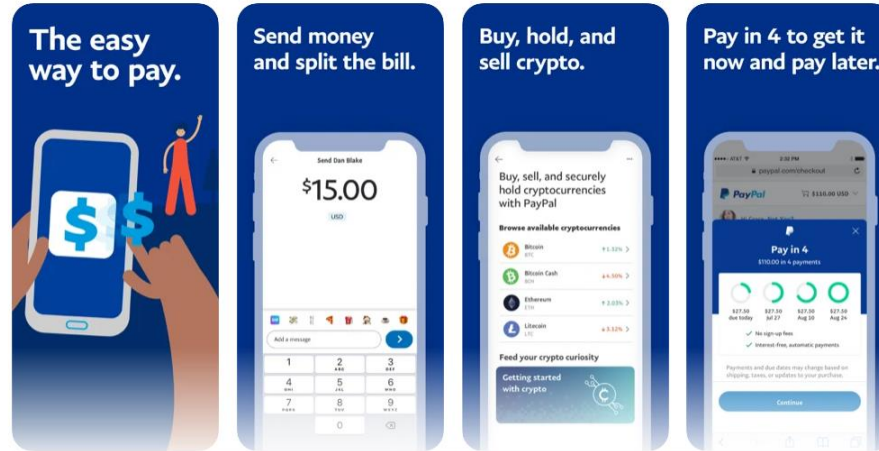


PayPal: Mobile Cash 4+

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>




```
"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,
```

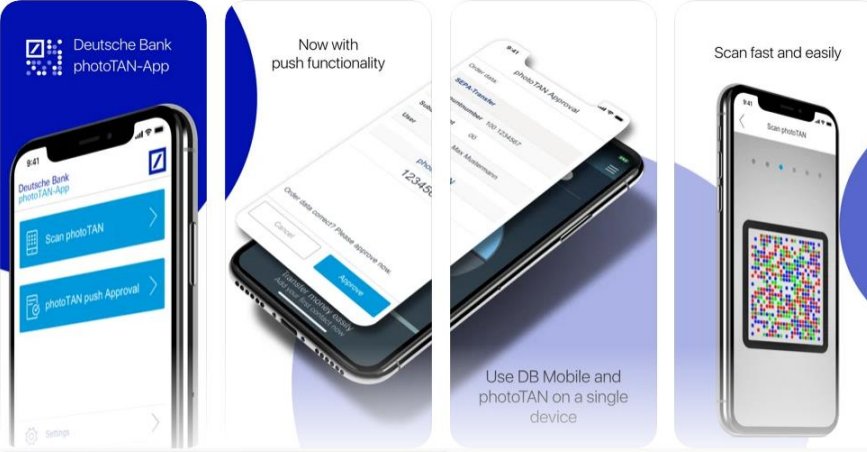
```
"location_auth_status": "authorizedWhenInUse",
"total_storage_space": 127968497664,
"tz_name": "Europe/Berlin",
"conn_type": "wifi",
"ssid": "WLAN3.ALTPETER.ME",
"bssid": "34:81:c4:dc:36:1",
"ip_addresses": [
  "10.0.0.83",
  "fd31:4159::cf9:d932:11c3:bede",
  "fd31:4159::5998:c752:9f96:5e30",
  "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 4+
Deutsche Bank AG
★★★★★ 4.8 • 480 Ratings
Free

iPhone Screenshots



Deutsche Bank photoTAN-App

Now with push functionality

Scan fast and easily

Use DB Mobile and photoTAN on a single device

<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": "d8c72cfc1da53dc497b2ce83171e108d",
    "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.

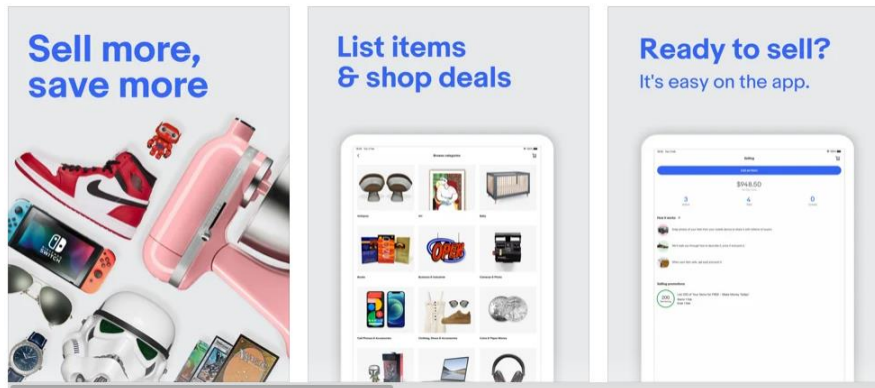
Designed for iPad

#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 trending tabletop cards and top tech.

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

```
"appInfo": {
  "appBuildConfiguration": "release",
  "appBuildIdentifier": "2412",
  "appVersion": "6.17.0",
  "appVersionHash":
    "9IA9pz28zzmAnmHWcQ2sZ4NyjbaS4ReTNZxmKena51kpCIu
    9fSNBQfaBKWx3QNL72HZtRQCIFufslhn0VRBBaw==",
  "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 4.6

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](#)



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 ups are now 100% with the 10 new double jump booster and wings!

[Version History](#)

Version 1.50.0

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

App Store



Pacer Pedometer & Step Tracker 4+

Walking, Weight Loss & Health

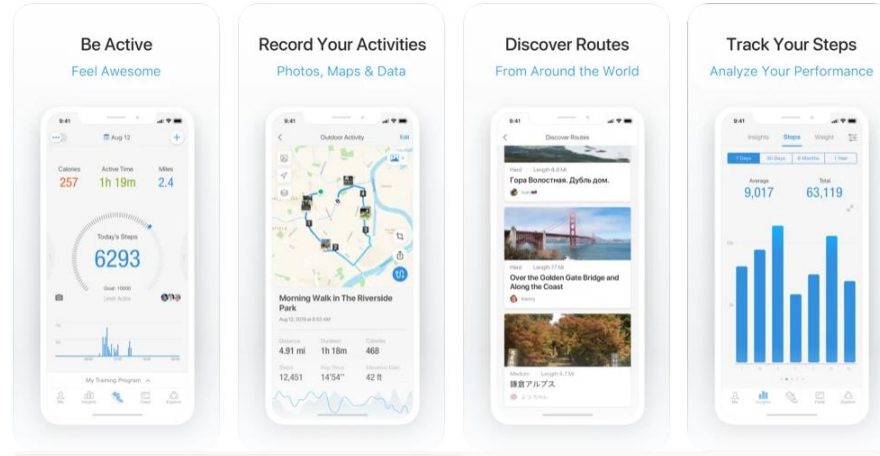
Pacer Health, Inc

#56 in Health & Fitness

★★★★★ 4.9 • 146.6K Ratings

Free • Offers In-App Purchases

Screenshots iPhone Apple Watch

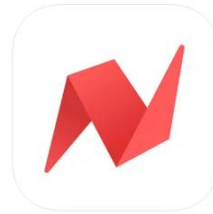


<https://apps.apple.com/us/app/pacer-pedometer-step-tracker/id600446812>

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.

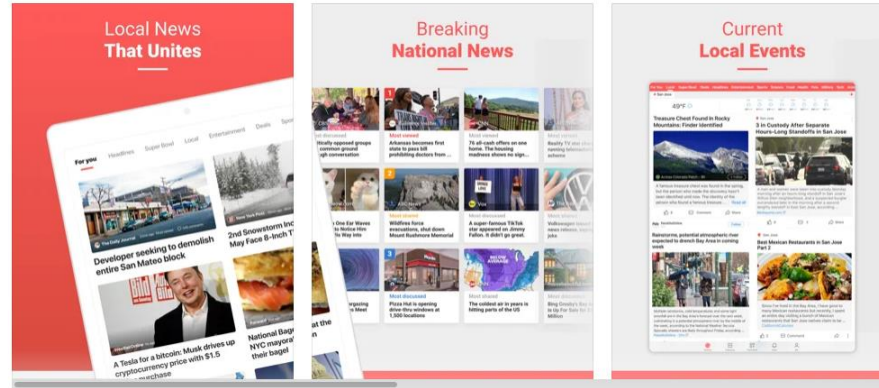
Designed for iPad

#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](#) delivers the most important & interesting news 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!
3rd place in Trivia, 1st in Word by category - 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":
"SCREEN_HEIGHT": "667",
"SCREEN_WIDTH": "375",
"ORIENTATION": "3",
"ROOTED": "2",
"LOCALE": "de_DE",
"IDFA_FLAG": "0",
"UNITY": "0",
"DATA_PROCESSING_OPTIONS_STATE": "null",
"DEBUGGER_ATTACHED": "0",
"COCOS2D": "0",
"MEDIATION_SERVICE":
  "GOOGLE_afma-sdk-i-v7.69.0: 6.2.1.0",
"BUNDLE": "de.lotum.4pics1word",
"DATA_PROCESSING_OPTIONS_COUNTRY": "null",
"DENSITY": "2",
"AD_EXPERIENCE_TYPE":
  "ad_experience_config_rewarded",
"OS": "iOS",
"FUNNEL_CORE_EVENTS":
  "4101,4146,4127,4106,4123,4104,4410,4412,4411",
"VOLUME": "0.125",
"MODEL": "iPhone10,4",
"MAKE": "Apple",
  "{ "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 MacOS 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",
"NUM_ADS_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



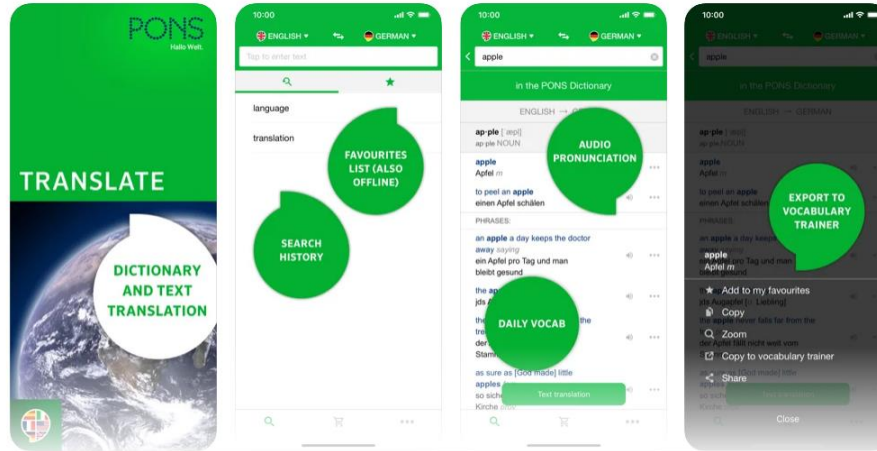
PONS Translate ⁴⁺

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

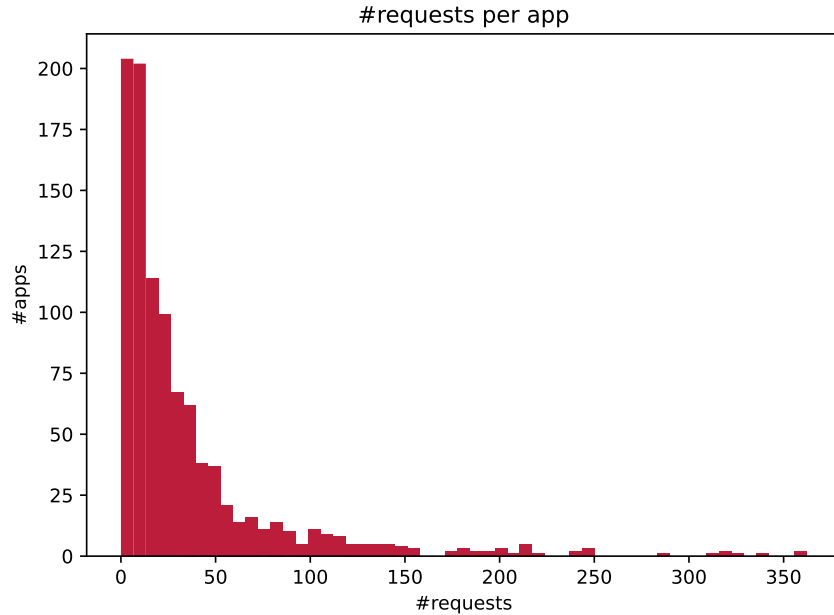
- 1,001 apps from the “Top 1200 Free Apps” for Germany as of May 27, 2021
- Analysis done on an iPhone 8 running iOS 14.5.1

- 74 apps without any requests, including:
 - [Signal - Private Messenger](#)
 - [TeleGuard](#)

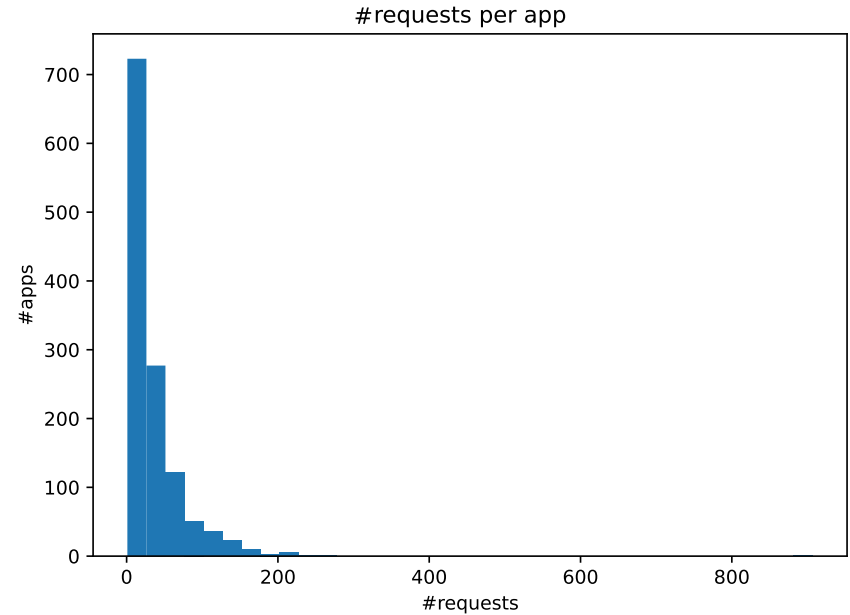
 - [Commerzbank photoTAN](#)
 - [AusweisApp2](#)

 - [Facebook](#)
 - [ZOOM Cloud Meetings](#)

Requests per app

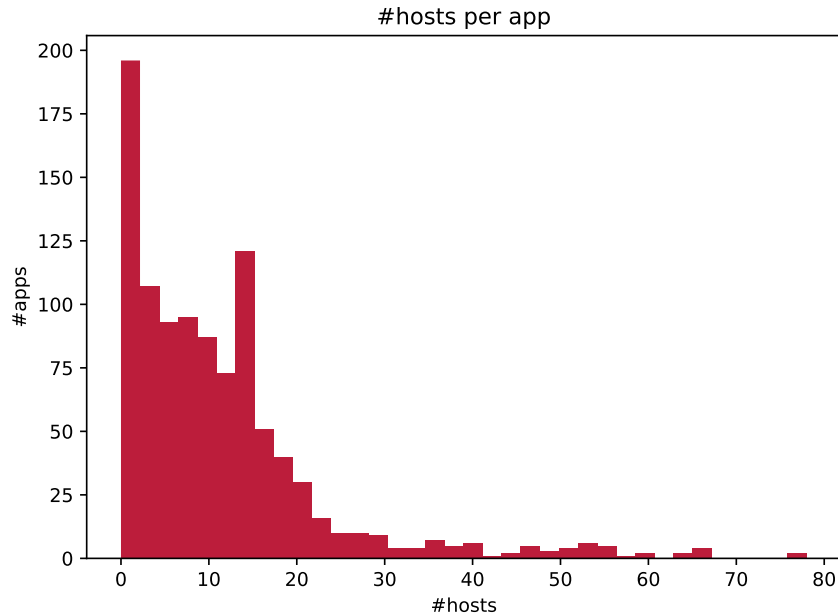


Number of network requests per app on iOS.

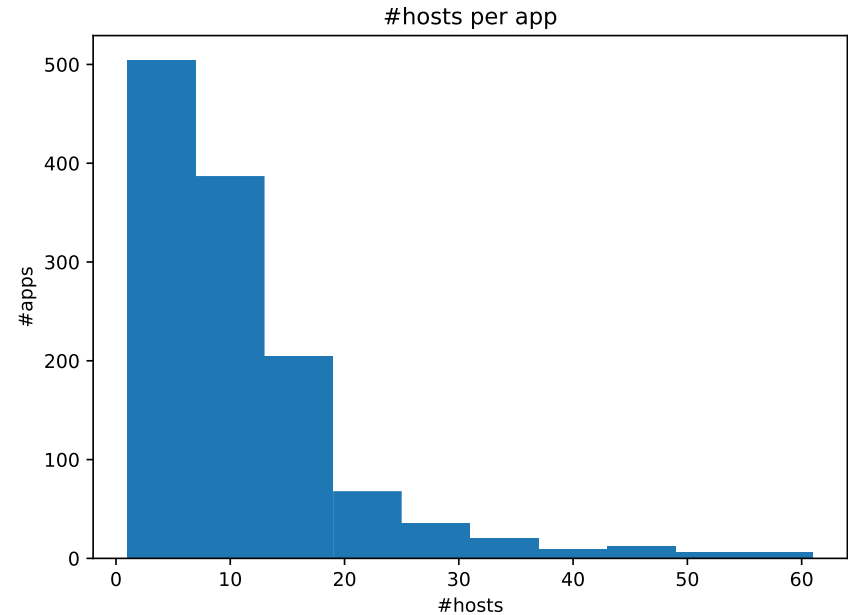


Number of network requests per app on Android [[Altpeter, Wessels](#)].

Hosts per app



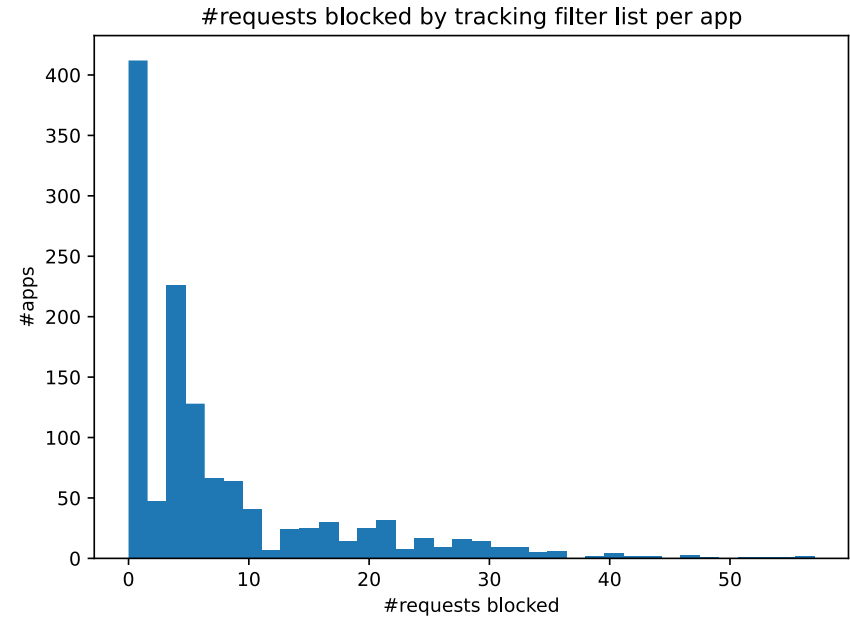
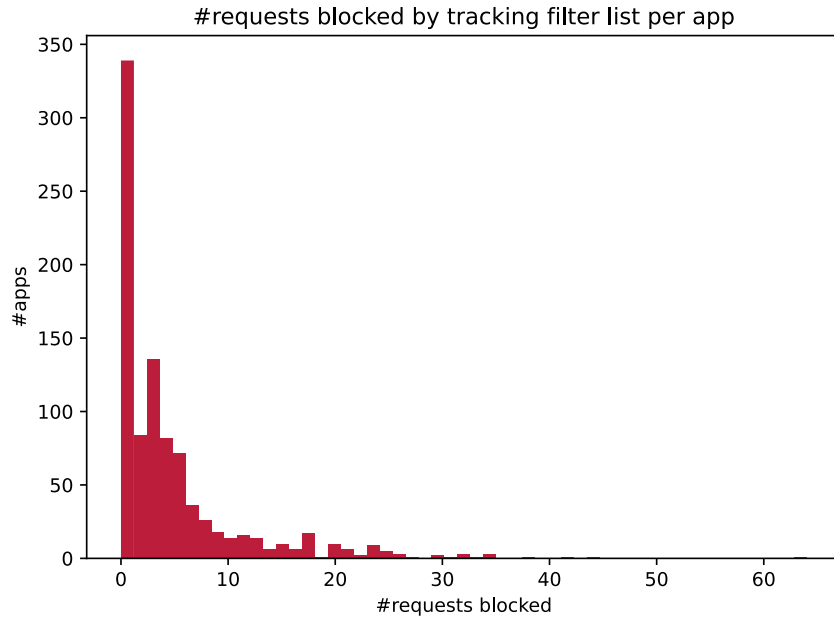
Number of unique hosts requested per app on iOS.



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

Requests blocked by tracking filter lists

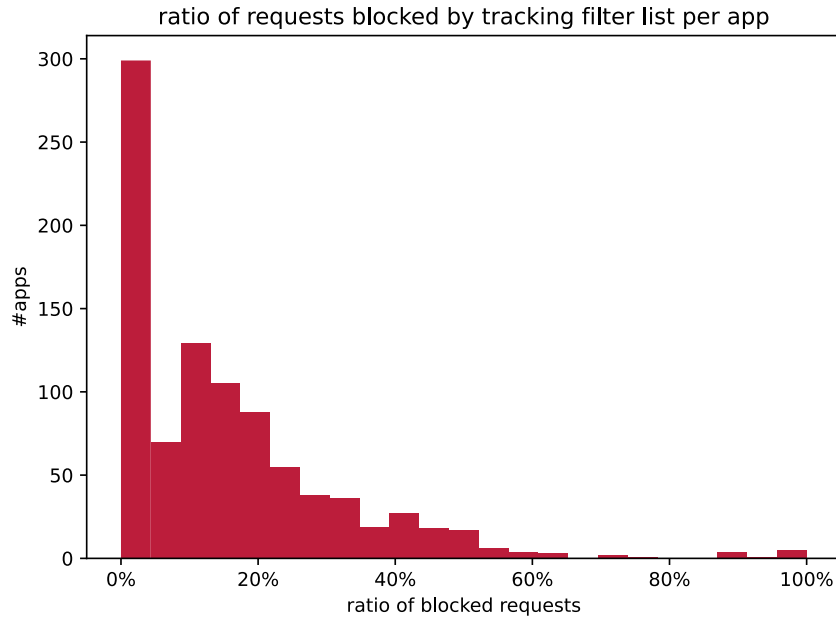
- Total requests: 34,925, requests after filtering: 30,439 (87.16%)



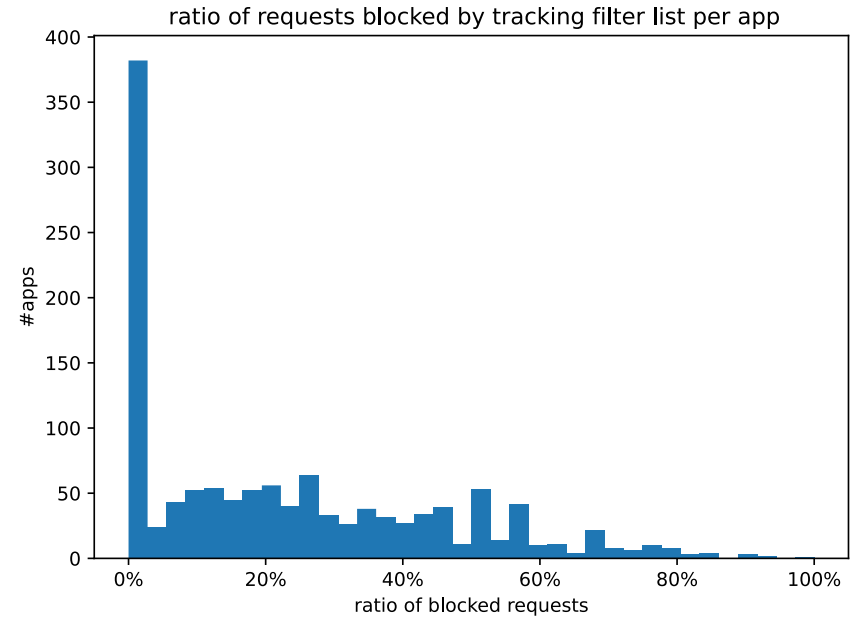
Number of requests blocked per app on iOS when using these tracking filter lists:
[EasyPrivacy](#), [eulaurarien](#), [Perflyst](#).

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

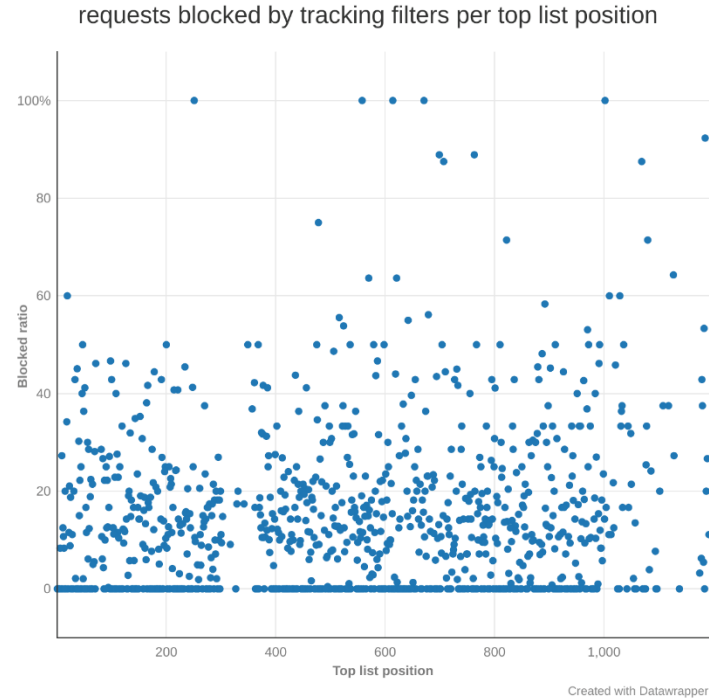


Ratio of requests blocked per app on iOS when using these tracking filter lists:
[EasyPrivacy](#), [eulaurarien](#), [Perflyst](#).



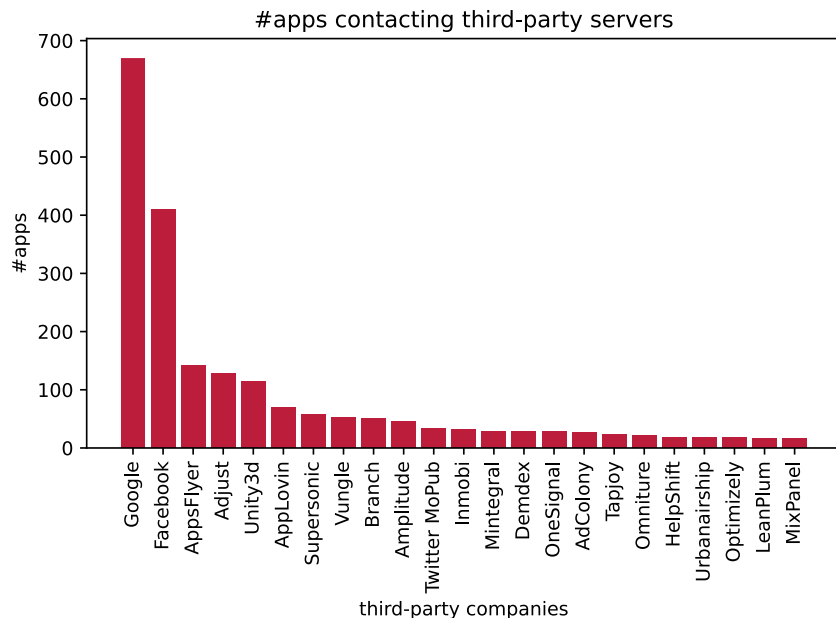
Ratio of requests blocked per app on Android when using these tracking filter lists:
[EasyPrivacy](#), [eulaurarien](#), [Perflyst](#) [Altpeter, Wessels].

Requests blocked by tracking filter lists

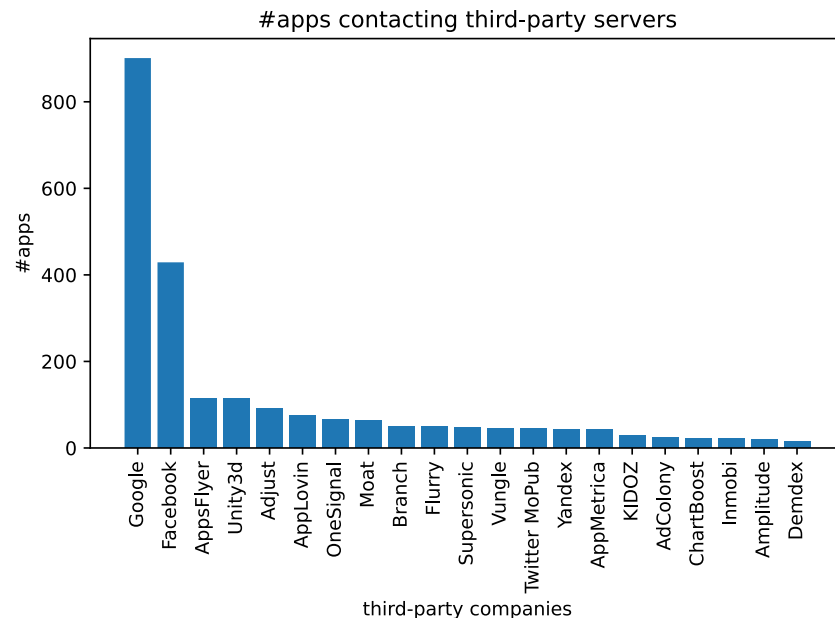


Ratio of requests blocked by tracking filter lists per top list position of the apps,
interactive version: https://www.datawrapper.de/_/8vtM/

Requests to third-party tracking servers

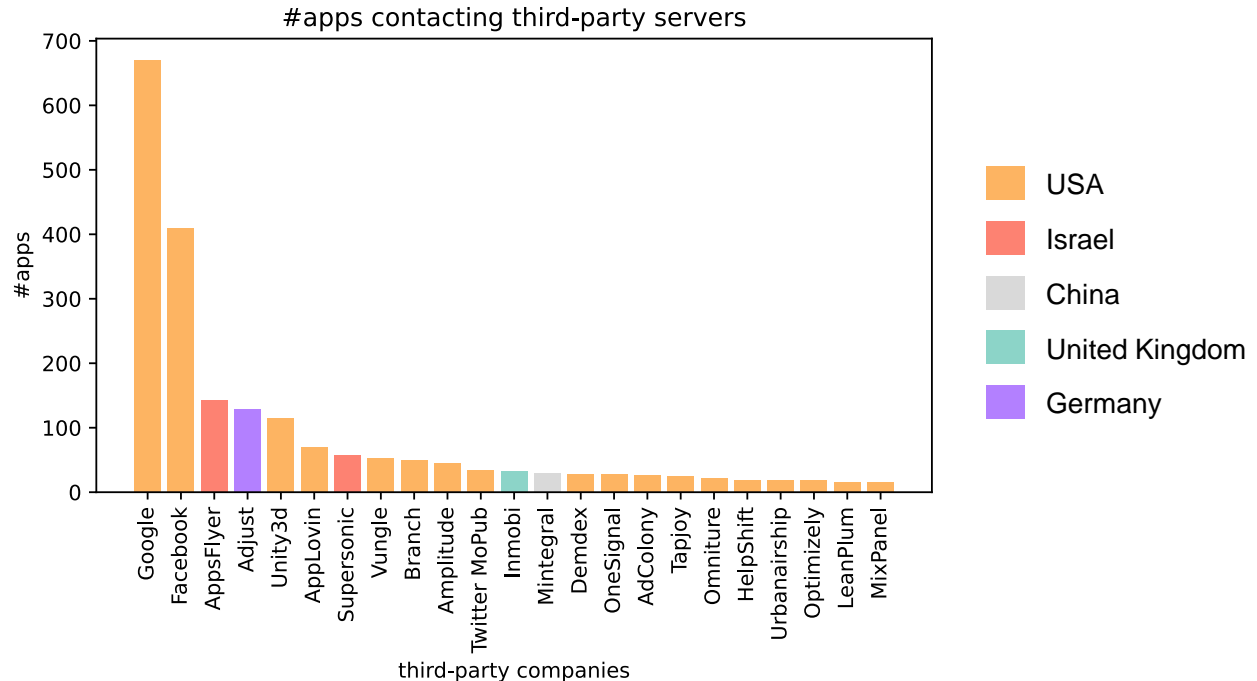


Number of apps contacting the most common third-party tracking servers on iOS, based on [Exodus tracker database](#).



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?

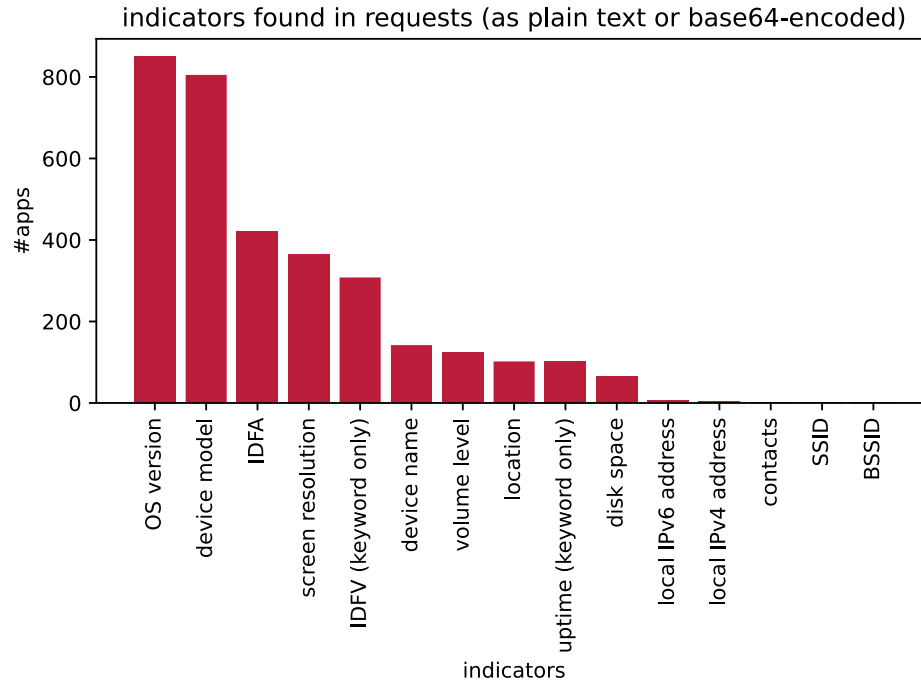


Number of apps contacting the most common third-party tracking servers on iOS and the respective countries, based on [Exodus tracker database](#) and [Datenanfragen.de company database](#).

Honey data

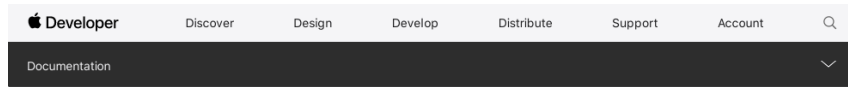
- **Owner:** Frank Walther, frank.walther.1978@icloud.com
- **Contact:** JGKfozntbF TBFFZbBYea, 0155 57543434, RYnlSPbEYh@bn.al, <https://q8phlLSJgq.de>, N2AsWEMI5D 565, 859663 p0GdKDTbYV
- **Messages:** 9FBqD2CNIJ to +4917691377604
- **Photos**, videos, and screenshots
- **Clipboard:** LDDsvPqQdT
- **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



Instance Property

advertisingIdentifier

The UUID that is specific to a device.

Declaration

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

Discussion

The `advertisingIdentifier` is an alphanumeric string that's **unique to each device** and which you only use for advertising. Use this string for frequency capping, attribution, conversion events, estimating the number of unique users, advertising fraud detection, and debugging. On devices running iOS 14.5 and later and iPadOS 14.5 and later, your app must request tracking authorization before it can get the advertising identifier. For more information on getting the advertising identifier, see [AdSupport](#).

The advertising identifier returns either a unique UUID, or all zeros. It returns a unique UUID in the following cases:

Availability

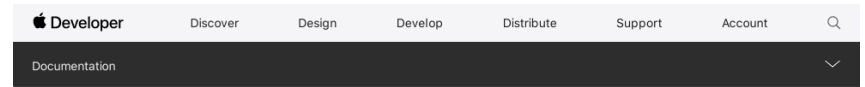
iOS 6.0+
macOS 10.14+
Mac Catalyst 13.0+
tvOS 9.0+

Framework

AdSupport

On This Page

[Declaration](#) 
[Discussion](#) 
[See Also](#) 



Instance Property

identifierForVendor

An alphanumeric string that uniquely identifies a device to the app's vendor.

Declaration

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

Discussion

The value of this property is the same for apps that come from the same vendor running on the same device. A different value is returned for apps on the same device that come from different vendors, and for apps on different devices regardless of vendor.

Normally, the vendor is determined by data provided by the App Store. If the app was not installed from the app store (such as enterprise apps and apps still in development), then a vendor identifier is calculated based on the app's bundle ID. The bundle ID is assumed to be in reverse-DNS format.

Availability

iOS 6.0+
Mac Catalyst 13.0+
tvOS 9.0+

Framework

UIKit

On This Page

[Declaration](#) 
[Discussion](#) 
[See Also](#) 

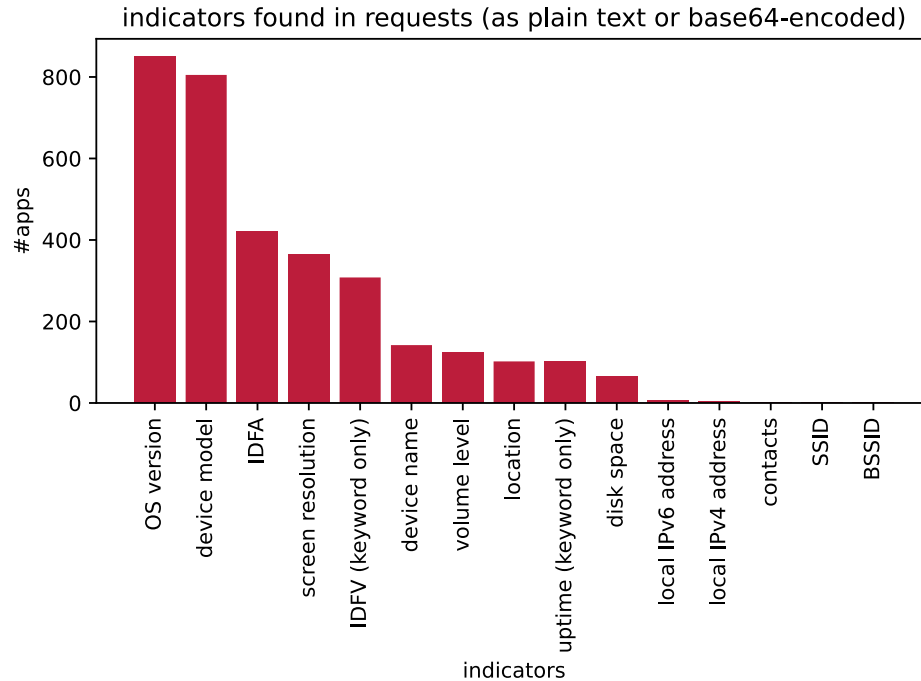
<https://developer.apple.com/documentation/adsupport/asidentifiermanager/1614151-advertisingidentifier>,
<https://developer.apple.com/documentation/uikit/uidevice/1620059-identifierforvendor>

IDFA and IDFV

The screenshot shows the Braze Developer Guide page for "IDFA and App Tracking Transparency". The page has a dark blue header with navigation links: Documentation, User Guide, Developer Guide (selected), API, Technology Partners, and Help. A search icon is on the right. A left sidebar contains a navigation menu with categories like "Platform Wide Features & Behaviors", "Platform Integration Guides", "Android", "iOS", and "iOS 14 Upgrade Guide". The main content area has the title "IDFA and App Tracking Transparency" and an "Overview" section. The overview text explains that IDFA is an identifier provided by Apple for use with advertising and attribution partners for cross-device tracking. A yellow box highlights the sentence: "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." Below this, it states that 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 (highlighted with a yellow box: "(00000000-0000-0000-0000-000000000000)") will be returned, and your app will not be allowed to prompt the user again. To the right of the text is an image of a smartphone displaying a permission prompt: "“Pel About” would like permission to track you across apps and websites owned by other companies. Your data will be used to deliver personalized ads to you." with "Allow Tracking" and "Ask App Not to Track" buttons. Below the main text is an "Important:" callout box with a megaphone icon, stating: "These IDFA updates will take effect once end-users upgrade their device to iOS 14.5. Please ensure your app uses the new `AppTrackingTransparencyFramework` with Xcode 12 if you plan to collect IDFA." At the bottom of the main content area, there is a link: "Changes to Braze IDFA collection". On the right side of the page, there are links to "Edit this page on GitHub" and a "On this page..." section listing various topics like "Upgrade Summary", "iOS 14 Behavior Changes", "Approximate Location Permission", "IDFA and App Tracking Transparency", "Push Authorization", "iOS 14 New Features", and "App Privacy and Data Collection Overview".

https://www.braze.com/docs/developer_guide/platform_integration_guides/ios/ios_14/

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

App Store

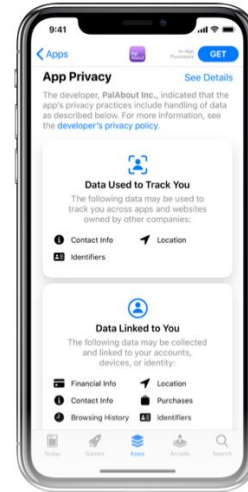
[Overview](#) [What's New](#) [Features](#) [Articles](#) [Guidelines](#) [Developer Insights](#)

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.

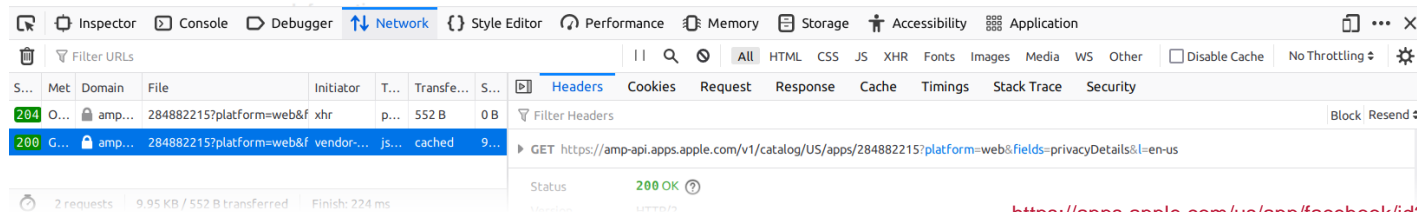
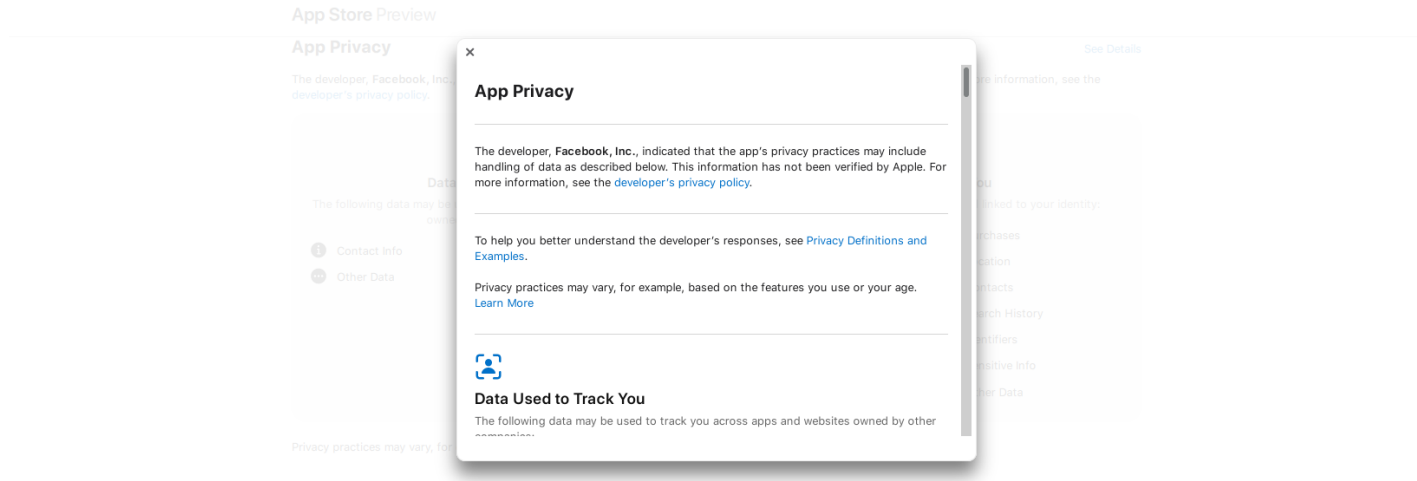
In order to submit new apps and app updates, you must provide information about your privacy practices in App Store Connect. If you use third-party code — such as advertising or analytics SDKs — you'll also need to describe what data the third-party code collects, how the data may be used, and whether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

[Learn more >](#)



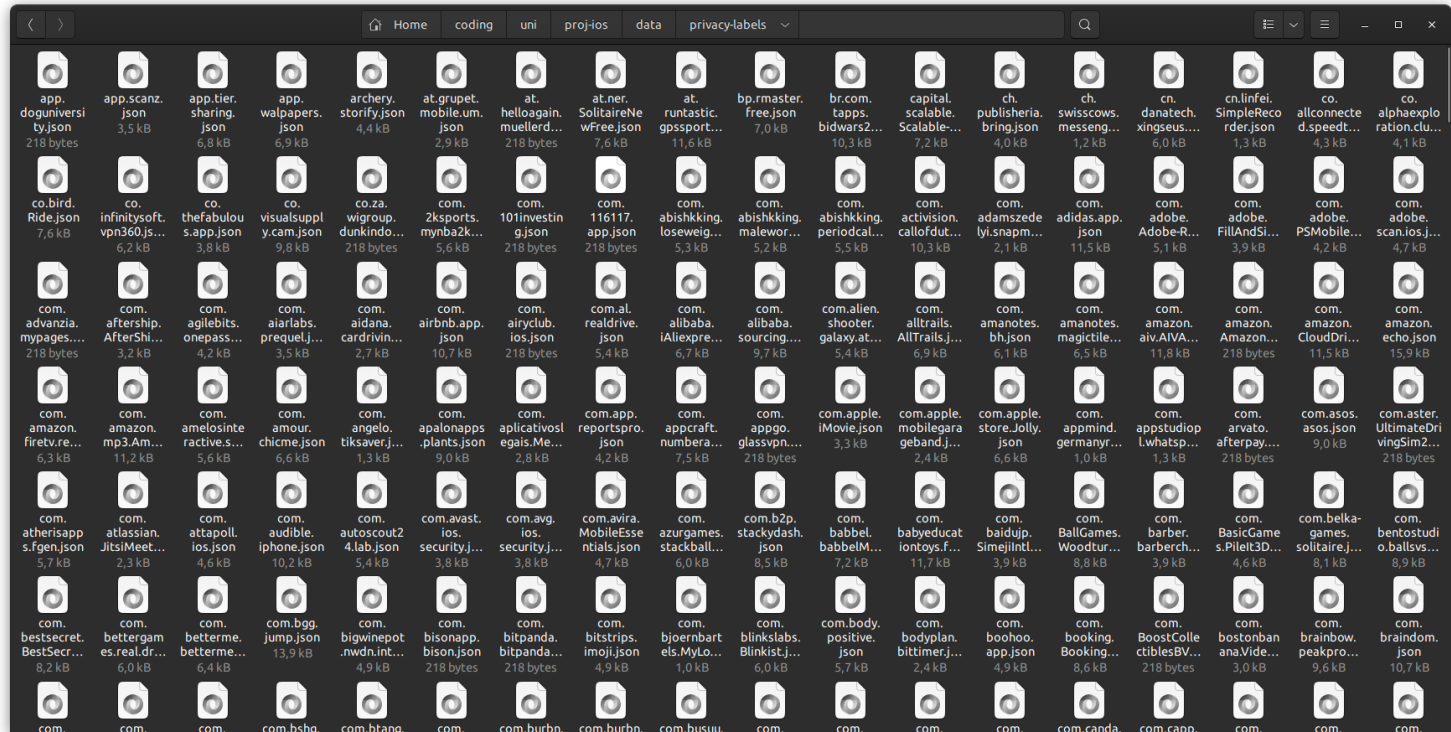
<https://developer.apple.com/app-store/user-privacy-and-data-use/>

Privacy labels



















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

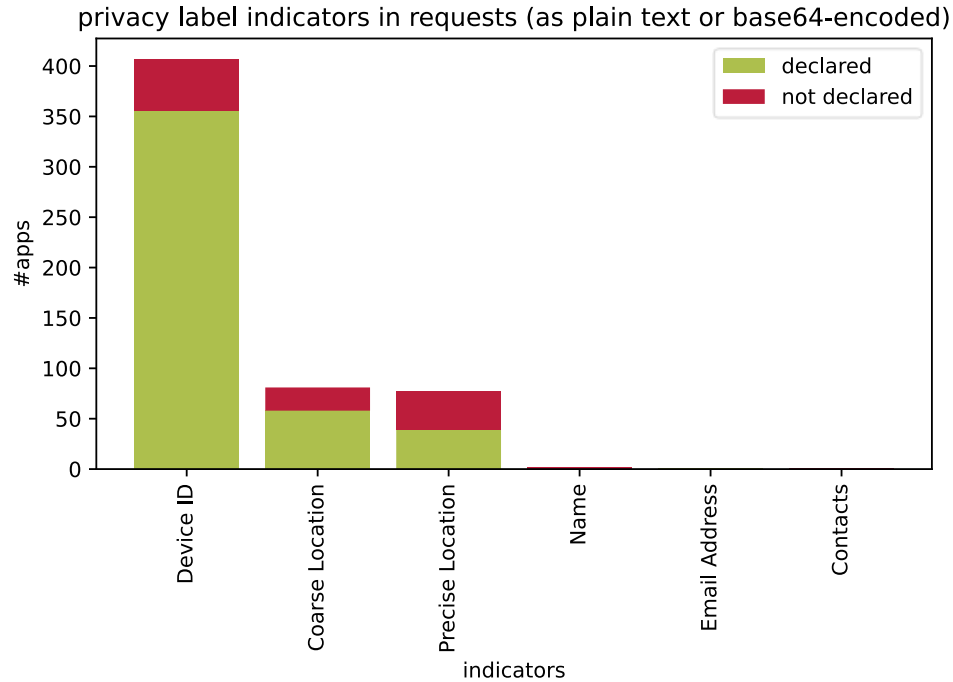
Privacy labels



Privacy labels

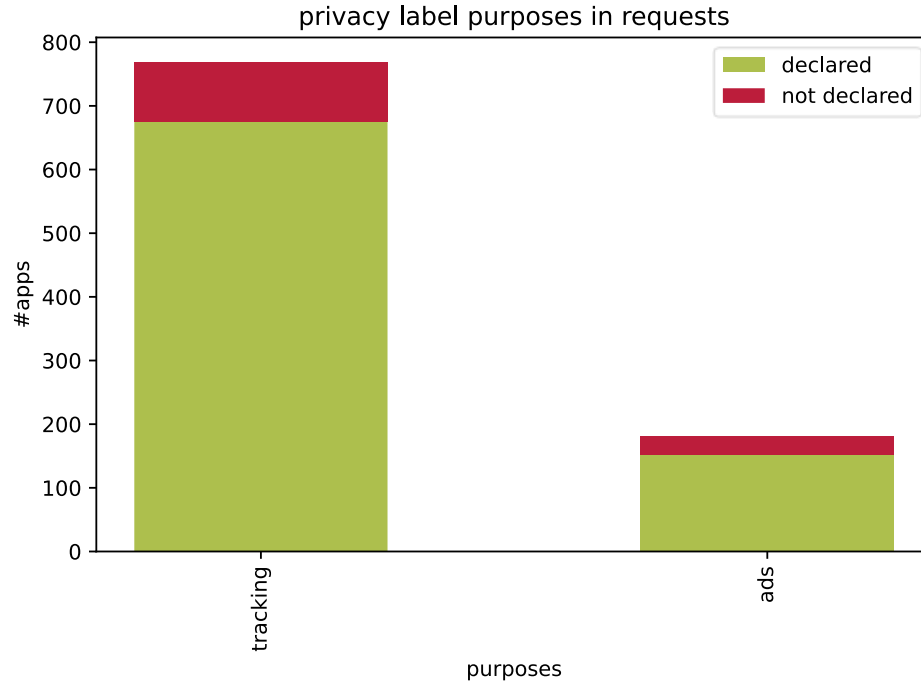
- 841 of 1001 apps have valid privacy labels. Of those, 32 claim not to collect any data, namely:
 - [TeleGuard](#)
 - [Voice Recorder - Audio Editor+](#)
 - [Tik Saver : Tik Tok Downloader](#)
 - [whatsapp fake chat](#)  Google Ads
 - [Stop Motion Studio](#)
 - [WATCHED - Multimedia & Movie](#)  Google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

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 the Google Play Console Help page for Advertising ID. The page has a header with a hamburger menu, 'Play Console Help', a search bar with the text 'Describe your issue', a grid icon, and a 'Sign in' button. The main content area is titled 'Advertising ID' and contains a warning icon and text: '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.' Below this is a paragraph explaining the advertising ID and its purpose. The next section is 'Google Play services update in 2021', which explains that the advertising ID will be removed when a user opts out of personalization. It also mentions that apps starting in late 2021 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"/>`. The text continues to explain that some SDKs, such as the Google Mobile Ads SDK, may already declare this permission, and that developers should learn more about merging manifest files on the Android Developers site. Finally, it notes that some Google Play policies, such as the Families Policy, require that apps not use the Ad ID. On the right side of the page, there is a list of related help topics, including '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', and 'Use of All files access (MANAGE_EXTERNAL_STORAGE) permission'. At the bottom of the page, there is a URL: <https://support.google.com/googleplay/android-developer/answer/6048248?hl=en>.

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



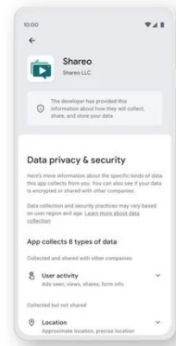
iMore



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