

The ultimate guide to understanding **Mobile App Marketing Analytics**



Mobile app marketing analytics solutions

	In-app	Web	Campaign
Definition	Tracks user's journey through an app, time spent within app and bounce rate	Tracks user's journey through mobile websites and web apps, time spent on website/within web app and bounce rate	Tracks marketing campaign performance, used for KPI monitoring and ad spend optimization. For apps: attributes installs and in-app user actions to the user's original ad click.
Major providers	Flurry	Google Analytics	Trademob, HasOffers, AD-X
What data is collected?	User behavior statistics, user flow and bounces		Marketing KPIs such as volume and cost of clicks, installs, in-app conversion points (e.g. in-app-purchase)
Purpose	Product/user experience improvement		Campaign optimization

In-app/web analytics and campaign analytics solutions offer different data and serve different purposes. While in-app and web analytics provide information on areas

for product improvement, campaign analytics allows app marketers to optimize their marketing spend and ROI.

Tracking technologies for campaign analytics



Campaign tracking for mobile apps is complex for a number of reasons:

- As iOS and Android are entirely unique technological ecosystems, there is no universal solution
- Also, apps and the mobile web are different ecosystems with different technological characteristics, so multiple technologies are needed to cover all types of traffic
- On iOS especially, there is little transparency as data cannot be transferred through the black box that is the App Store. Solutions that act like a bridge between the click and in-app user activity are needed to enable conversion attribution

Tracking technologies for campaign analytics

	Apple						Android
	device id						
	MAC Address + ODIN*	Open UDID + SecurID*	UDID*	IDFA	Finger-printing	Cookies*	Android Referrer
Privacy-compliant	✗	✗	✗	✓	✓	✓	✓
Accepted by Apple / Android	✗	✗	✗	✓	✓	✗	✓
Goes unnoticed by end user	✓	✓	✓	✓	✓	✗	✓
Accurate conversion matching	✓	✓	✓	✓	✓	✓	✓
Tracks in-app traffic	✓	✓	✓	✓	✓	✓	✓
Tracks web, SMS, social media and email traffic	✗	✗	✗	✗	✓	✓	✓
Supports click fraud detection	✗	✗	✗	✗	✓	✗	✓
Independent of publisher data	✗	✗	✗	✗	✓	✓	✓

Traffic supported: ✓ Yes ✓ Yes, with limitation ✗ No | * banned or soon banned by Apple

While on Android, the Android Referrer is the standard solution to track campaign performance, multiple solutions have been developed on iOS in the past years. The most common techniques are device ID and fingerprint tracking.

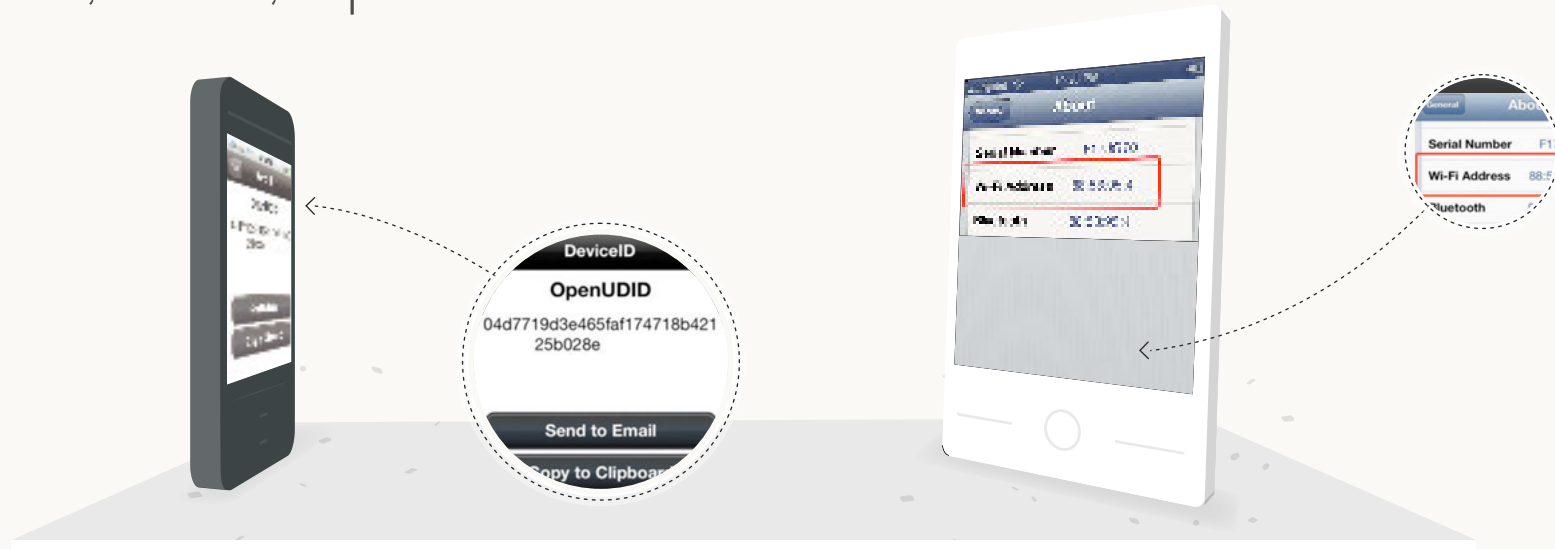
(We will elaborate more on both mechanics on the following pages.) The standard web solution, cookie tracking, is not commonly used by app marketers as it causes a bad user experience in the case of a slow Internet connection. Apple thus nowadays bans apps using cookie tracking.

Device IDs

Device IDs are used to track users by exactly matching user actions within an app to the original ad click. Any app can collect the device ID, which uniquely identifies an iOS device. The publisher app collects and transmits the ID when serving an ad while the advertiser collects the ID upon install and each in-app user action. Composing all actions belonging to one device ID, the entire user journey and the user's original source can be matched with 100% accuracy. However, device IDs can only be obtained when a user clicks on an in-app ad and can therefore only be used to track in-app traffic and not Web, email, social media or SMS traffic. Also, this type of tracking is dependent on publishers and advertisers transmitting the required data.



UDID, MAC, ODIN, Open UDID and SecurID



Before May 1st 2013, the UDID tracking was the most common procedure on iOS, but has been banned due to privacy concerns because it cannot be changed or reset on a device. The IDFA is Apple's answer to the UDID and will become the new industry standard. In the wake of Apple's plan to deprecate the UDID (2011-mid 2012), alternative solutions had been developed: the MAC Address, ODIN, OpenUDID and SecureUDID. The Media Access Control (MAC) address is a permanent and unique number of the Wi-Fi inter-

face on each iOS device. The ODIN is a similar solution based on the Mac ID. The Open UDID and SecurID are workaround solutions accessing the pasteboard on the iPhone to place and read out a device specific ID. However, privacy issues remained because all solutions establish a single identifier per device that cannot be reset by the user and are therefore no different to the UDID. With iOS 7, Apple will also eliminate MAC based and pasteboard tracking. The IDFA will remain as single reliant device ID.

IDFA



The Identifier for Advertisers (IDFA) is Apple's own Advertising Identifier and replacement to the UDID. It is privacy compliant as it is possible for users to reset it at any time and to opt out of targeted ads on their device under settings-privacy-advertising. However, it still only tracks

in-app traffic and not Web, SMS, social media or email traffic, and the universal migration of publishers from UDID to IDFA will take some more time before the IDFA will be established as a universal new standard in the iOS app ecosystem.

Summary of device IDs

Traffic supported:

✓ In-app

✗ Web

✗ SMS

✗ Email

✗ Social media

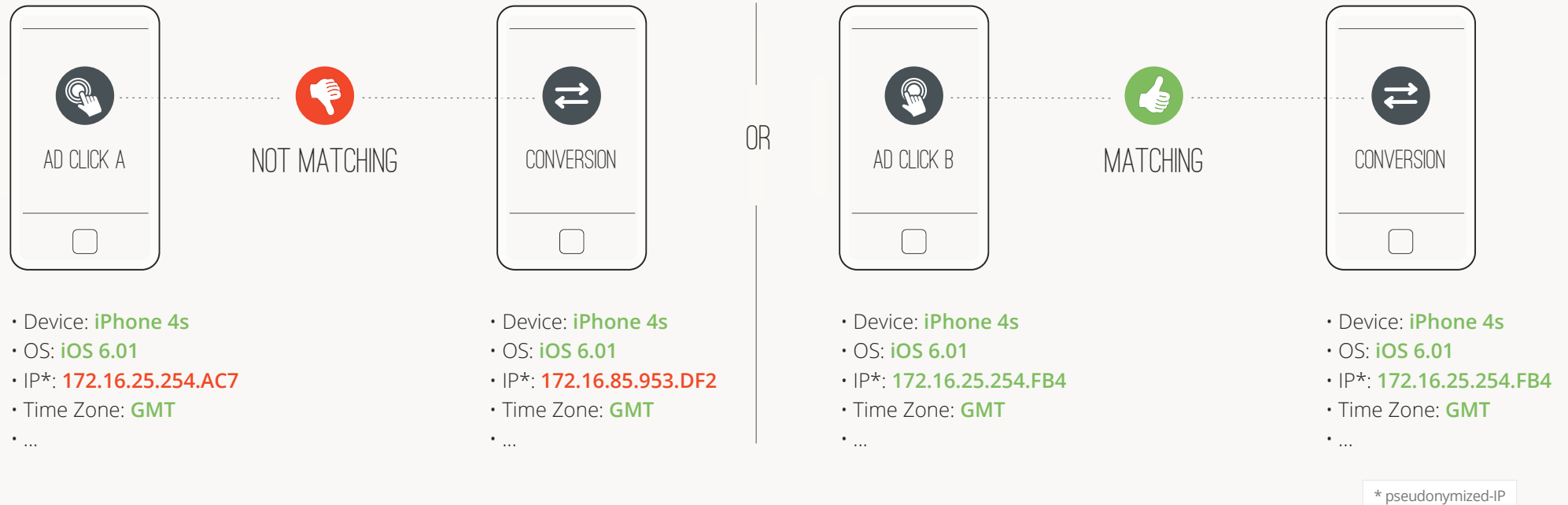
Required technical set-up:

- **Publisher:** needs to collect device ID and to transmit them to ad network (usually via publisher SDK)
- **Advertiser:** needs to collect device ID and to transmit them to tracking partner (usually via advertiser SDK)

Accuracy: 100% accurate matching of ad click and conversions e.g. install, in-app actions.



Fingerprinting



Fingerprinting tracks all types of mobile traffic, and is based on algorithmic analyses of the device characteristics behind each click and conversion. By analyzing the data behind a user action, the fingerprinting technology and algorithm performs matches between user actions based on similarities between a wide set of parameters,

including operating system, pseudonymized IP, device model, carrier, country, language, time and mobile network code. It is independent of publisher data, however it can never be completely accurate due to its probabilistic nature. With our advanced algorithm, Trademob's fingerprint solution reaches around 95% accuracy.

Summary of fingerprinting

Traffic supported:

✓ In-app

✓ Web

✓ SMS

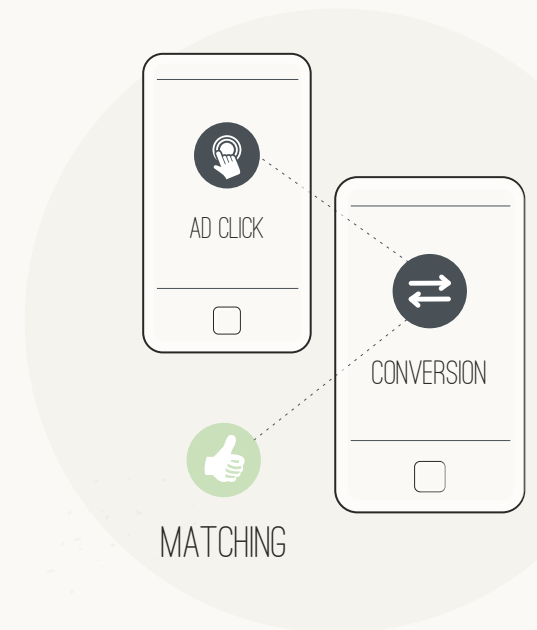
✓ Email

✓ Social media

Required technical set-up:

- **Publisher:** no set-up required, data is collected via javascript when a user clicks on an ad
- **Advertiser:** needs to collect device ID and to transmit them to tracking partner (usually via advertiser SDK)

Accuracy: Not fully accurate as it's a probabilistic approach
(Trademob algorithm reaches up to 95%)

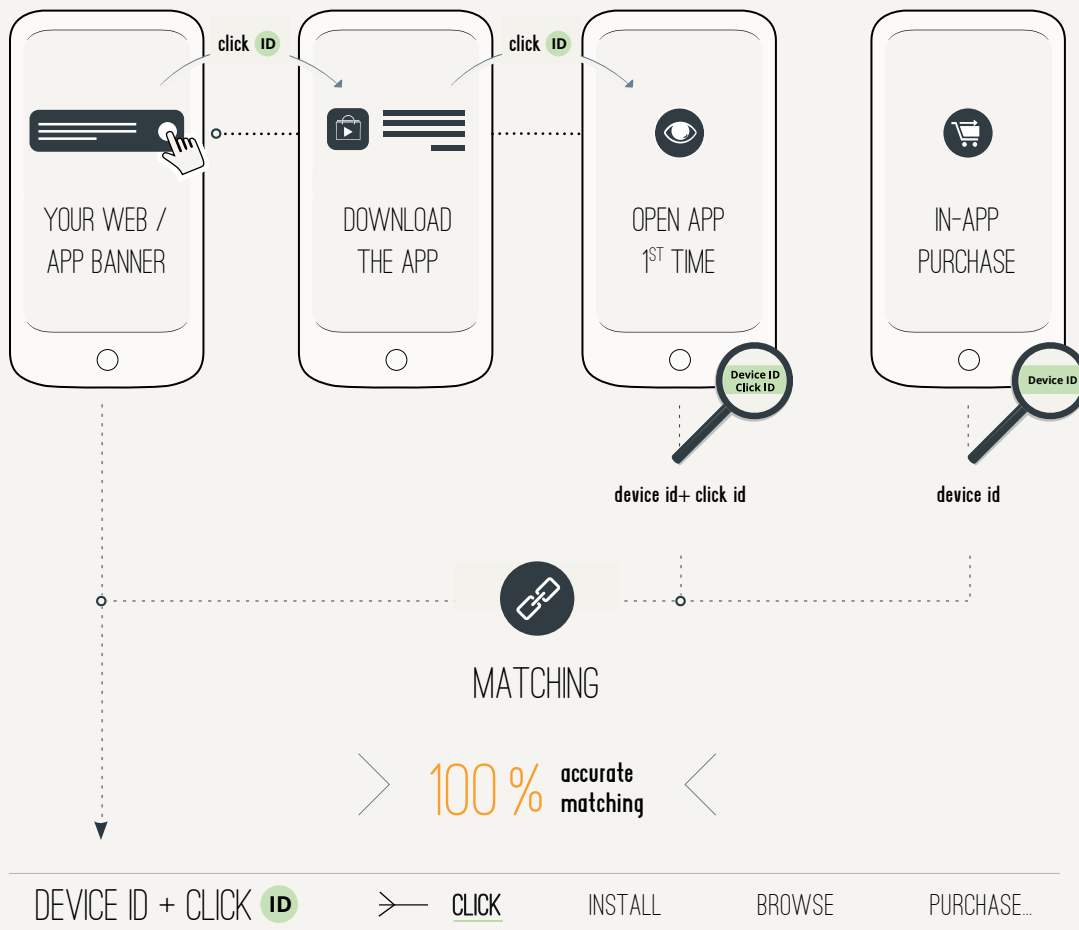


Android Referrer

```
1 <!-- Used for install referrer tracking -->
2 <receiver android:name="com.google.android.apps.analytics.Analyti
3 <intent-filter>
4 <action android:name="com.android.vending.INSTALL_REFERRER" /:
5 </intent-filter>
6 </receiver>
```

Compared to tracking on iOS, tracking campaign performance on Android, at least in the Google Play store, is relatively simple. Using the Google Analytics Android Referrer, installs and campaign performance can be tracked with 100% accuracy and across all types of traffic.

The Android Referrer is a parameter which can be appended to a click URL and filled with a unique value per click ("click ID"). When the app is installed and opened for the first time, the Google Play Store sends the referrer ("click ID") to the app telling the app where the install originates from. An SDK inside the app (like Trade-mob's) can then collect the referrer and match it to the device and all of its subsequent actions inside the app.



Summary of Android Referrer

Traffic supported:

✓ In-app

✓ Web

✓ SMS

✓ Email

✓ Social media




Required technical set-up:

- **Publisher:** no set-up required
- **Advertiser:** needs to create unique ID on the click, collect it upon install using the Android Referrer parameter and transmit to tracking partner (usually via advertiser SDK)

Accuracy: 100% accurate matching



Trademob's solution for iOS & Android

			 TRADEMOB	
	IDFA	Finger-printing	Android Referrer	Trademob's multi tracking technology mix for iOS*
Privacy-compliant	✓	✓	✓	✓
Accepted by Apple	✓	✓	✓	✓
Goes unnoticed by end user	✓	✓	✓	✓
Accurate conversion matching	✓	✓	✓	✓
Tracks in-app traffic	✓	✓	✓	✓
Tracks web, SMS, social media and email traffic	✗	✓	✓	✓
Supports click fraud detection	✗	✓	✓	✓
Independent of publisher data	✗	✓	✓	✓

Traffic supported: ✓ Yes ✓ Yes, with limitation ✗ No

*Trademob is always careful to weigh every opportunity available on the advertising landscape while considering the privacy interests of our end users. This means that — in line with market conventions and adoption — we will be phasing out any UDID-, MAC- and pasteboard-based tracking solutions with the release of iOS 7.

Android

To track campaign performance on Android, we use the Android Referrer.

iOS

As campaign performance analytics is more challenging on iOS, and no single tracking solution offers all of the desired features (100% accuracy, reach and support for all traffic types), we combine multiple solutions to make up a super solution for iOS campaign tracking. Our multi-tracking technology mix is currently the best and most accurate tracking solution available for tracking on iOS. It fits all of the necessary criteria for an accurate and all-encompassing solution.

Contact Germany

Friedrichstraße 126
10117 Berlin

Questions?

DE	+49 30 202 1575-15		info@trademob.com
US	+1 914 703 8262		ny@trademob.com

