ISSN: 2167-1508
v10 n4511

Geolocation Tracking and Privacy Issues Associated with the Uber Mobile Application

Dr. Darren R. Hayes
Pace University
dhayes@pace.edu
Sapienza Università di Roma
darren.hayes@uniroma1.it

Christopher Snow
csnow@pace.edu

Saleh Altuwayjiri
sa07549n@pace.edu

Pace University
New York, NY

Abstract

This research examined the Uber mobile application and determined that the company utilizes very precise and potentially invasive geolocation tracking techniques. Our experiments indicate that Uber tracks the location of its users, after the conclusion of a ride, for longer than its official privacy policy would indicate. The most interesting finding is that geolocation tracking is performed by the Uber app even when the user does not take an Uber ride. Additionally, its geolocation tracking of users using competing services may be disconcerting for some consumers. While our findings may be a privacy concern for some consumers, the Uber app also has tremendous potential for digital forensics investigators.

Keywords: Uber, mobile apps, mobile forensics, geolocation, privacy

1. INTRODUCTION

Uber is a service that enables drivers to act as flexible contractors and provide transportation services that compete with traditional taxi services. Consumers, using the Uber mobile app, can search for a car service in their area. The benefit to the consumer is that they are visually provided with the mapped location of Uber cars in their locality and be provided with an upfront quote for a specific journey (or "ride"). Uber operates in 570 cities worldwide. In recent times, Uber has received negative press about it geolocation tracking of users and raised a number of concerns regarding its privacy policies and potentially invasive data collection practices. The research, herein, sought to identify the type of personally identifiable information (PII) collected by the company. More precisely, this research identifies what geolocation data the Uber mobile application (app) collects on the user.

In April 2017, the New York Times published a story that documented a meeting, at Apple headquarters, in 2015, between Travis Kalanick, CEO of Uber, and Tim Cook, CEO of Apple (Issac, 2017). The article alleges that Mr. Cook scolded Mr. Kalanick for identifying and tagging iPhones after the Uber app had been uninstalled or the device had been wiped. Apparently, this type of user identifying coding violated the Apple developer terms of service agreement (Newman, 2017).

A recent article in The New York Times detailed how Unroll.me, which purported to purge your device's mail Inbox of annoying advertising messages, was actually being used to spy on competitors (Isaac & Lohr, 2017). The article documented how Unroll.me would scan a user's Inbox, identify if there were service receipts, from competing companies like Lyft, and then sell that information to Lyft's competitor - Uber.

2. BACKGROUND

Since the introduction of iOS 5, Apple has been limiting app developer access to the iPhone's UDID (Unique Device Identifier)(Schonfeld, 2011). A notice from Apple stated, "Starting May 1, the App Store will no longer accept new apps or app updates that access UDIDs. Please update your apps and servers to associate users with the Vendor or Advertising identifiers introduced in iOS 6" (Panzarino, M.). Apple now prefers that app developers utilize the official Apple advertising platform to track app users. Based on Apple's *Advertising and Privacy* policy, it appears that Apple does collect user data and then subsequently shares it with third-parties (Apple, 2017). Nevertheless, developers can obtain extensive information about an app user through the integration of the *UIDevice* object. The UIDevice object can be used by an app developer to determine the assigned name of the device, device model and iOS version, orientation (*orientation* property) of the device, battery charge (*batteryState* property) and distance of the device to the user (*proximityState* property) (Apple). Moreover, developers can integrate code, during app development, for third-party analytics into their app. These third-party companies include Localytics, mixpanel, UXCam and fabric. Companies like Apptopia provide app developers with extensive, nay invasive, analytics on competitor apps.

The use of the user UDID has not always been used for nefarious purposes, however; the UDID was often used to identify if the user of an app was a legitimate user and could block a user's access if an account was compromised or potentially stolen. Fingerprinting is yet another methodology, used by third-parties, to uniquely identify users, based on application configuration. Fingerprinting is best known for identifying online users based on user settings from their browser, which may include user cookies and browser plug-ins. The Electronic Frontier Foundation (EFF) created a project known as Panopticlick (panopticlick.eff.org) to raise awareness about how your browser is used by advertisers, and others, to identify and track you on the Web. The EFF announced that 84% of online users can be uniquely identified by their browser (Budington, 2015).

According to Uber's *USER PRIVACY STATEMENT*, there are two categories of information collected about users: (a) Information You Provide to Us, which can include name, email, phone number, postal address, profile picture, payment method, and (b) Information We Collect Through Your Use of Our Services, which can include location information, contacts, transactions, usage and preference, device information, call and SMS data and log information (Uber, 2015). Of particular interest is the Device Information (hardware model, operating system and version, software and file names and versions, preferred language, unique device identifier, advertising identifiers, serial number, device motion information, and mobile network information). In terms of Location Information, Uber is not specific about the extent to which the user's location is being tracked but states that they "may also collect the precise location of your device when the app is running in the foreground or background" (Uber, 2015). Uber provides more detailed information about the use of Location Services on its Website under iOS App Permissions (Uber).

What is most interesting, for the purposes of our research, is that during our installation of the Uber app, a dialog box appears and states that "Uber collects your location (i) when the app is open and (ii) from the time of the trip request through five minutes after the trip ends" (see Figure 1). Uber states in their FAQ that the reasoning behind this data collection is to "improve pickups, drop-offs, customer service, and to enhance safety" (Uber). However, users reported seeing the Uber app using location services weeks after the app was used, past the 5 minutes they claim. Uber responded to these reports blaming Apple's iOS Maps extension that Uber uses to serve regional maps to their customers (Perez, 2016).

Perhaps unsurprisingly, Uber has invested heavily in data science to retain its competitive advantage, as evidenced by its aggressive recruitment of data scientists (Wilde, 2015). We also know that Uber extensively uses a telematics pilot program, called *Autohawk*, to identify the location of its drivers and perform diagnostic testing on the vehicle to ensure passenger safety (Wisniewski, 2016). In fact, Uber provides geolocation information, provided by its data visualization team, on its Website at eng.uber.com/data-viz-intel. Uber integrates both Fabric and Localytics in its mobile app. Fabric provides companies, like Uber, with real-time information about the health of their app. These analytics include application crash analytics.

3. RELATED WORK

The research group at Pace University has previously published research on how geolocation information from mobile apps could be used by governments to track users in an article entitled "Leakage of Geolocation Data by Mobile Ad Networks" (Snow, Hayes, Dwyer, 2016) and another article entitled "Mobile Ad Networks and Security Issues Regarding Geolocation Data" (Snow, Hayes, Dwyer, 2016). More specifically, this research focused on the claims of the whistleblower, Edward Snowden, that mobile apps, like Angry Birds, could be used to profile individuals and track their whereabouts through communications with mobile advertisements.

EURCOM's research paper, entitled "Taming the Android AppStore: Lightweight Characterization of Android Application", examined the network connections established by "legitimate" apps (Vigneri, Chandrashekar, Pefkianakis, & Heen, 2015). Ultimately, their research determined that the 2,146 applications that they examined connected to approximately 250,000 distinct URLs; many of these server connections were to domains known to maintain malware.

A recent paper published by IEEE titled "Location Privacy Breach: Apps Are Watching You in Background" (Liu, D., Gao X., & Wang, H.) examined the correlation between the frequency of locational requests and potential security risks associated with user data leakage. The study concluded that shorter intervals between each geolocation request from a mobile app correlate to a higher privacy risk. Therefore, mobile applications that constantly update with a user's location, such as a car service are at high risk of leaking a user's location because of their high request rate.

It is also known that mobile users are not generally aware when an app is accessing personal data in the background, as noted in the research study "Android permissions remystified: a field study on contextual integrity" published by USENIX Security (Wijesekera P., Baokar A., Hosseini A., Egelman S., Wagner D., and Beznosov K.). The 2015 study analyzed how 36 participants used their mobile applications and concluded that 80% of participants studied noted that at least one permission request, made by a mobile application, as inappropriate. These permission requests were approved when the user accepted the end-user agreement during installation. The participants were unaware about exactly what they were allowing the mobile application to access. Thus, a majority of the participants experienced an invasion of (locational) privacy from the mobile applications they used.

4. EXPERIMENTAL RESEARCH

Our methodology, for this research, involved performing both a static and dynamic analysis of the Uber mobile application for iOS (iPhone) and for Android. The static analysis primarily involved an analysis of the SQLite database associated with the app, utilizing mobile forensic tools on an iPhone. Additionally, our static analysis included reverse engineering the Android application package (APK) file. The purpose of the latter was to review the code to identify the application's manifest. This app manifest would include permissions on the user device, which could include access to contacts, user location (based on GPS, cell sites or local access points), access to device hardware, like the camera or microphone and identifying information about the user. The dynamic analysis focused on how the application behaved during execution. The latter would use a series of DNS analytical tools to identify domain and network connections.

Google Maps

The Uber app for Android utilizes the Google Maps API (application programming interface) (see Figure 2) for locating Uber drivers in the vicinity of the consumer. We also confirmed this through our dynamic analysis of PCAPs from the Uber app (see Figure 3).

APK Analysis

An examination of the Uber APK file will provide a list of permissions requested by the application. A review of the APK manifest will quickly identify location permissions requested of the user. A search for the "Uber APK file" will quickly identify where the application can be downloaded from the Web. Once downloaded there are a number of applications that can be used to review the code and manifest for the APK. One tool for reviewing APK developer code is *dex2jar* (dex compiler), which can be downloaded from SourceForge. Yet another application for viewing the APK is FileViewer Plus. For our research we chose to use an online APK decompiler application, which is available from www.javadecompilers.com/apk. The rationale for selecting this tool to decompile the APK is that no download is required and the APK file can simply be uploaded on the fly. An analysis of the APK manifest reveals the following permissions related to location:

android.permission.ACCESS_COARSE_LOCATION
android.permission.ACCESS_FINE_LOCATION

There is nothing unusual about these location permissions being requested by the Uber app. The location of a user device can be based on GPS, proximity to a cellular tower (cell site) or WiFi. ACCESS_COARSE_LOCATION is a permission that enables the app to access the approximate location of the user device, which is based on NETWORK_PROVIDER (cell sites). ACCESS_FINE_LOCATION enables the app to determine the location of the user device based on NETWORK_PROVIDER and GPS (GPS_PROVIDER).

Using BlackLight (BlackBag Tech) and MPE+ (AccessData) forensics tools, we can determine that the data associated with the Uber app can be found in the following application files:

Library>Application Support>com.ubercab.UberClient\xxxx.ldb

Library>Application Support>com.ubercab.UberClient\Cache.db

Data>data>com.ubercab\files\rider\0000xx.ldb

Analysis Background

The data below was compiled using two analyst programs:

- Debookee by iwaxx
- BlackLight by BlackBag

The initial experiments were run from an iPhone 7 Plus device running iOS 10.2.1. The Uber app was downloaded for the first time on this new iPhone. The user account on the Uber app was new and no ride history existed. Actions that were performed include searching for a nearby Uber car, mapping out a pick-up point and destination address to determine ETA (estimated time of arrival) and price in addition to adding a PayPal payment method.

Man-in-the-Middle Analysis

The highlighted lines in Figure 4 are HTTPS requests made by the Uber app. These lines were captured using Debookee, a LAN scanning program by iwaxx; the tool can capture traffic on a targeted device. Each request uses the SSL, under the HTTPS protocol, as seen in the "method" column. The HTTPS protocol ensures that data being pushed from the user, like location, to the Uber servers is encrypted and therefore illegible to bad actors listening to the connection. One can infer that *cn-geo1.uber.com* is a domain used specifically for transferring information about a user's location and nearby Uber vehicles.

Location Analysis with BlackLight

Using BlackLight, we were able to find an interesting file called "eyeball", as seen in Figure 5.

```
"etaString":"5
minutes","etaStringShort":"5mins","averag
eEta":292,"minEta":5},"39":{"
vehiclepaths":{"8d8269c664cbd9342acbdd
14b5cf5ccca82fd2d4":[{"latitude":40.7098
1,
"course":133,"longitude":-
74.00881,"epoch":1497472606280},{"latit
ude":40.70974, "course":133,"longitude":-
74.00870999999999,"epoch":1497472610
512},
{"latitude":40.70969,"course":133,"longitu
de":-74.00864,"epoch":1497472614714},
{"latitude":40.70959000000001,"course":1
33,"longitude":-74.00851,…
```

The above string is a sampling of many similar strings that were found in a file labeled "eyeball" under the following folder pathway in the UberClient application folder:

Library>Application Support>PersistentStorage>BootstrapStore>RealtimeApp.StreamModelKey

It can be inferred that "eyeball" refers to the radius circle of a user's location to capture nearby Uber vehicles. This "etaString" operation is repeated throughout the "eyeball" storage file for multiple vehicles in the area. The string explains an Estimated Time of Arrival (ETA) of 5 minutes and provides an array of latitude and longitude numbers connected to a "vehicle path" followed by a string of numbers and letters that can be concluded as a serial number for the specific vehicle. When the various longitude and latitude coordinates in the array are mapped out, the points display a route that this specific nearby Uber vehicle was following. Figure 6 shows the latitude and longitude coordinates mapped out on Google Maps. It can be inferred that each of these coordinates was a ping from the nearby Uber vehicle to the app in order to update the driver's position on the user's screen.

The most important string from this same "eyeball" storage file came at the very end. The following string shows a "reverseGeocode" operation that was able to identify the exact address of where the user was located.

```
"reverseGeocode":{"latitude":40.71023066
52868,"components":[{"long_name":"163
William Street","short_name":"163 William
Street","types":["premise"]},
{"long_name":"Lower
Manhattan","short_name":"Lower
Manhattan","types"
:["neighborhood","political"]},{"long_nam
e":"Manhattan","short_name":
"Manhattan","types":["political","sublocalit
y","sublocality_level_1"]},{"long_name":
"New York","short_name":"New
York","types":["locality","political"]},
{"long_name":"New York
County","short_name":"New York
County","types"
:["administrative_area_level_2","political"
(…) "longAddress":"163 William Street,
New York, NY 10038,
USA","nickname":"163 William
Street","uuid":"3938134a-1b86-4f87-8ad0-
f29c66ea674d","longitude":-
74.00613835924165,"shortAddress":"163
William Street"}}
```

This "reverseGeocode" protocol was able to accurately identify the user's current location as "163 William Street" without this exact address being explicitly provided. The application then used this geocode to find Uber vehicles in the area. We can deduce that a user's location is saved as well as the vehicles in the area regardless if an Uber is requested for a pick-up. Even if the "reverseGeocode" was not provided, the previous "vehiclepaths" could be mapped out to determine the general location of where the Uber customer stood by seeing where nearby Uber vehicles were pinging.

Privacy Analysis with BlackLight

```
[{"useCase":"personal","hasBalance":false
,"status":"active","accountName":"Apple
Pay Display","tokenDisplayName":"Apple
Pay Display","tokenType":
"apple_pay_display","uuid":"f8b461f2-
a12e-4e3f-afdb-682c79497726"},
{"useCase":"personal","cardNumber":"pay
p","cardExpiration":"20**-**-
12T14:48:11.257+00:00","cardType":"Pay
Pal","hasBalance":false,"status":"active","
accountName":"*********@me.com","car
dExpirationEpoch":1812811691257,"token
DisplayName":"*********@me.com","uuid
":"3a48e583-71dc-4a51-82f0-
01ddd8b7106b","tokenType":"paypal"}]
```

**portions redacted for privacy*

The above string was found in a file labeled "profiles" under the following folder pathway in the UberClient application folder:

Library>Application Support>PersistentStorage>Store>PaymentBase.PaymentStreamModelKey

The string displays two payment methods that were saved on the Uber app. The first being Apple Pay, this method was not set up on the target device. The second being PayPal, which was the connected method of payment when requesting rides. The redacted portions represent areas where the user's PayPal login username was saved in plain text. Other fields for "cardExpiration as well as "cardNumber" are also seen.

As part of our static analysis, we analyzed searches for trips and actual trips using the Uber app on an iPhone. Using BlackLight, we determined that all the locations of pick-ups and drops offs were found in a file called database.db located here:

Root>Mobile>Applications>UberClient>database.db

In the first experiment, the Uber user searched for an address in Brooklyn (3xx Gold St, Brooklyn, New York 11201). The user decided to take a NYC Yellow Cab instead of using Uber, yet the app tracked the user's trip with a competitor service, as noted in Figure 7. Interestingly, using Blacklight, we can determine that the Yellow Cab journey was recorded in a very similar way as an Uber journey, as shown in Figure 8.

In the second experiment, the user used the Uber app to find the cost of a journey. The Uber app was then closed. The user then used the Lyft app (competitor service) to see if the journey was cheaper than Uber. Given the cost saving, the user selected the ride with the Lyft app. The user took a Lyft ride from the Cheesecake Factory (100 Cambridge Side Place, Cambridge, MA 02141) to Harvard University. Using Blacklight, we discovered that this Lyft ride was recorded in the Uber app, as shown in Figures 9 and 10. Furthermore, we found that the Uber app was tracking the user for approximately 11 minutes after the Lyft ride had ended, thereby negating Uber's claim that a user will only be tracked for up to 5 minutes after the conclusion of a ride, although the ride was with a competing service. We proved this by reviewing the route, recorded by the app's Google API, after the ride had ended and determined that it took the user 11 minutes to complete the mapped route.

5. FUTURE EXPERIMENTS

Our research discovered that the Uber app uses Crashlytics. This third-party analytics service, which was acquired by Google, provides the app developer with crash analytics. Theoretically, while this service is providing real-time crash analytics, it could also be collecting the location of the user device. During our dynamic app analysis with Debookee, we discovered that there were continuous HTTPS requests going back and forth between the device and the Crashlytics server(s), even though the app was not experiencing any crash problems. Additionally, a more extensive examination of comparable "ride" apps would be appropriate to identify whether there are simply privacy concerns with Uber and not with its competitors. There are suggestions that iOS 11 will limit geolocation tracking by third-party app providers. It will be interesting to see how this will impact the Uber app and its tracking abilities.

6. CONCLUSIONS

In an age where many people, especially in the United States, are concerned about government agencies, like the NSA, collecting vast quantities of PII and geolocation information, consumers should also understand the data collection practices of companies, including Uber. Even though Uber placed blame for their app accessing locational services after 5 minutes on Apple's iOS Maps, it is clear from our findings that their application could store locational data after 5 minutes. With the application able to access location from the iOS Map issue they have cited, the Uber app may still then be able to tap into a user's location past the 5 minutes indicated in their privacy agreement. The Uber mobile application is saving this location data from vehicles in a user's area locally to the user's device. In addition, user's exact address locations are being determined and locally saved through longitude and latitude coordinates. It is clear that Uber is not just saving trip locations from completed rides, they are collecting geolocation data when the app is not being used for a ride and, more interestingly, is being used to monitor rides with competing services. From a forensics perspective, this research demonstrates the tremendous potential for criminal investigators to use the Uber app to track a suspect and/or victim. The value of this information cannot be overstated given the detailed unencrypted user information available, in plaintext, using forensic imaging tools, like BlackLight.

7. REFERENCES

Apple (2017, January 16). About Advertising and Privacy. Retrieved June 10, 2017, from https://support.apple.com/en-us/HT205223

Apple. UIDevice: A representation of the current device. Retrieved June 10, 2017, from https://developer.apple.com/documentation/uikit/uidevice

Budington, Bill (2015, December 17). Panopticlick 2.0 Launches, Featuring New Tracker Protection and Fingerprinting Tests. Retrieved June 11, 2017, from https://www.eff.org/deeplinks/2015/12/panopticlick-20-launches-featuring-new-tracker-protection-and-fingerprinting-tests

Liu, D., Gao X., & Wang, H. (2017, July 17). Location Privacy Breach: Apps Are Watching You in Background, IEEE 37th International Conference on Distributed Computing Systems (ICDCS), 2017.

Google. (2015, April 17). Inside AdWords: ads take a step towards "HTTPS everywhere". Retrieved June 10, 2017, from http://adwords.blogspot.com/2015/04/ads-take-step-towards-https-everywhere.html

Hof, R. (2014, August 27). Study: mobile ads actually do work - especially in apps. Retrieved June 10, 2017 from http://www.forbes.com/sites/roberthof/2014

/08/27/study-mobile-ads-actually-do-work-especially-in-apps/

Isaac, Mike (2017, April 23). Uber’s C.E.O. Plays With Fire. Retrieved June 10, 2017 from https://www.nytimes.com/2017/04/23/technology/travis-kalanick-pushes-uber-and-himself-to-the-precipice.html?_r=1

Isaac, Mike, & Lohr, S. (2017, April 24). Unroll.me Service Faces Backlash Over a Widespread Practice: Selling User Data. Retrieved June 10, 2017 from https://www.nytimes.com/2017/04/24/technology/personal-data-firm-slice-unroll-me-backlash-uber.html

Lee, M. (2015, January 26). Secret 'BADASS' intelligence program spied on smartphones. *First Look Media*. Retrieved June 10, 2017, from https://firstlook.org/theintercept/2015/01/26/secret-badass-spy-program/

Newman, Lily Hay (2017, April 24). Uber Didn’t Track Users Who Deleted the App, But it Still Broke the Rules. Retrieved June 10, 2017 from https://www.wired.com/2017/04/uber-didnt-track-users-deleted-app-still-broke-rules/

Panzarino, Matthew (2013, March 21). Apple to reject any apps that use UDIDs, don’t support Retina, iPhone 5 displays as of May 1st. Retrieved June 10, 2017 from https://thenextweb.com/apple/2013/03/21/after-a-year-of-warnings-apple-will-no-longer-accept-any-apps-that-use-udids-as-of-may-1st/

Perez, Sarah (2016, Dec 22). Uber Explains Why It Looks like Its App Is Still Tracking Your Location, Long after Drop-Off, Tech Crunch. Retrieved August 1, 2018 from https://techcrunch.com/2016/12/22/uber-explains-why-it-looks-like-its-app-is-still-tracking-your-location-long-after-drop-off/

Schonfeld, Erick (August 19, 2011). Apple Sneaks A Big Change Into iOS 5: Phasing Out Developer Access To The UDID. Retrieved June 10, 2017, from https://techcrunch.com/2011/08/19/apple-ios-5-phasing-out-udid/

Snow, C., Hayes, & D., Dwyer, C. (2016). Leakage of Geolocation Data by Mobile Ad Networks, Journal of Information Systems Applied Research, 2016.

Snow, C., Hayes, & D., Dwyer, C. (2015). Mobile Ad Networks and Security Issues Regarding Geolocation Data, EDSIG Conference 2015.

Uber. iOS App Permissions. Retrieved June 11, 2017 from https://www.uber.com/legal/other/ios-permissions/

Uber (2015, July 15). User Privacy Statement. Retrieved June 11, 2017 from https://www.uber.com/legal/privacy/users/en/

Uber.). How does Uber use location (Android)? Retrieved July 31, 2017 from https://help.uber.com/h/ba9dd342-158d-421f-a9ea-0e6c7aaad726

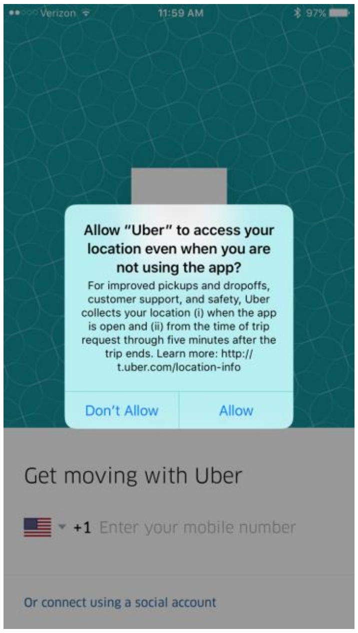
Vigneri, L., Chandrashekar, J., Pefkianakis, I., & Heen, O. (2015). Taming the Android AppStore: lightweight characterization of Android applications. *arXiv preprint arXiv:1504.06093*.

Wijesekera P., Baokar A., Hosseini A., Egelman S., Wagner D., and Beznosov K. (2015). Android permissions remystified: A field study on contextual integrity, Proceedings of the 24th USENIX Conference on Security Symposium

Wilde, Ben (2015). Data Science Disruptors: How Uber Uses Applied Analytics For Competitive Advantage. Retrieved June 11, 2017 from https://georgianpartners.com/data-science-disruptors-uber-uses-applied-analytics-competitive-advantage/

Wisniewski, Mary (2016). Uber says monitoring drivers improves safety, but drivers have mixed views. Retrieved June 11, 2017 from http://www.chicagotribune.com/news/local/breaking/ct-uber-telematics-getting-around-20161218-column.html

Appendices and Annexures



Allow "Uber" to access your location even when you are not using the app?

For improved pickups and dropoffs, customer support, and safety, Uber collects your location (i) when the app is open and (ii) from the time of trip request through five minutes after the trip ends. Learn more: http://t.uber.com/location-info

Verizon
11:59 AM
97%
Don't Allow
Allow
Get moving with Uber
+1 Enter your mobile number
Or connect using a social account

Figure 1. Uber dialog box during installation

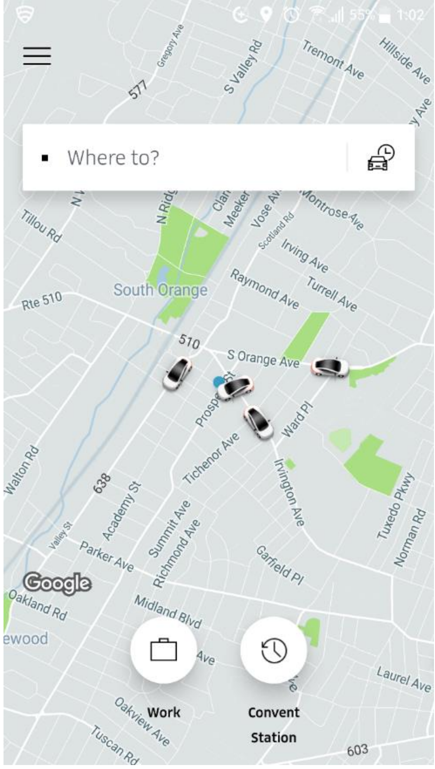
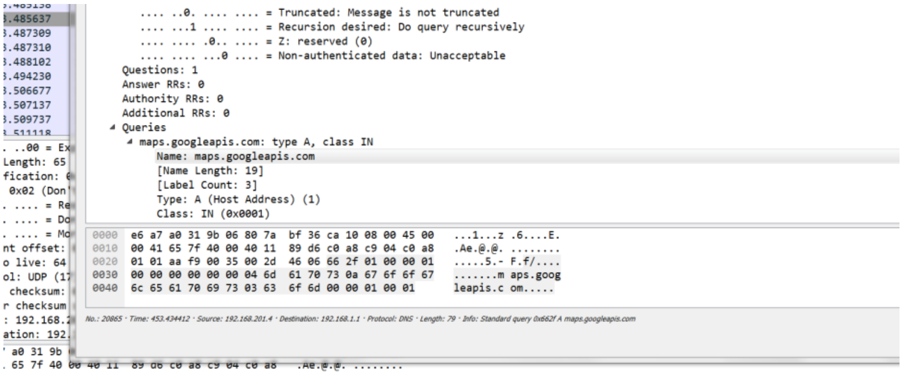
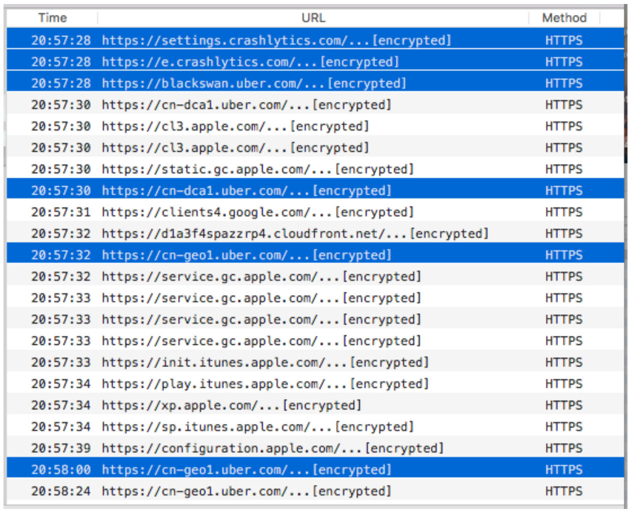


Figure 2. Screenshot of Google Maps in the Uber app



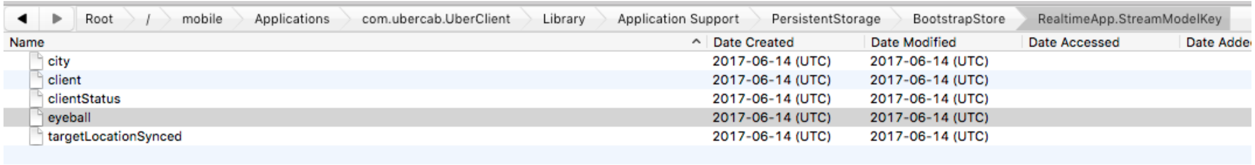
```
        .... ..0. .... .... = Truncated: Message is not truncated
        .... ...1 .... .... = Recursion desired: Do query recursively
        .... .... .0.. .... = Z: reserved (0)
        .... .... ...0 .... = Non-authenticated data: Unacceptable
      Questions: 1
      Answer RRs: 0
      Authority RRs: 0
      Additional RRs: 0
    ◢ Queries
      ◢ maps.googleapis.com: type A, class IN
          Name: maps.googleapis.com
          [Name Length: 19]
          [Label Count: 3]
          Type: A (Host Address) (1)
          Class: IN (0x0001)

0000  e6 a7 a0 31 9b 06 80 7a  bf 36 ca 10 08 00 45 00   ...1...z .6....E.
0010  00 41 65 7f 40 00 40 11  89 d6 c0 a8 c9 04 c0 a8   .Ae.@.@. ........
0020  01 01 aa f9 00 35 00 2d  46 06 66 2f 01 00 00 01   .....5.- F.f/....
0030  00 00 00 00 00 00 04 6d  61 70 73 0a 67 6f 6f 67   .......m aps.goog
0040  6c 65 61 70 69 73 03 63  6f 6d 00 00 01 00 01      leapis.c om.....

No.: 20865 · Time: 453.434412 · Source: 192.168.201.4 · Destination: 192.168.1.1 · Protocol: DNS · Length: 79 · Info: Standard query 0x662f A maps.googleapis.com
```

Figure 3. Google Maps API identified in a PCAP captured by Wireshark



Time	URL	Method
20:57:28	https://settings.crashlytics.com/...[encrypted]	HTTPS
20:57:28	https://e.crashlytics.com/...[encrypted]	HTTPS
20:57:28	https://blackswan.uber.com/...[encrypted]	HTTPS
20:57:30	https://cn-dca1.uber.com/...[encrypted]	HTTPS
20:57:30	https://cl3.apple.com/...[encrypted]	HTTPS
20:57:30	https://cl3.apple.com/...[encrypted]	HTTPS
20:57:30	https://static.gc.apple.com/...[encrypted]	HTTPS
20:57:30	https://cn-dca1.uber.com/...[encrypted]	HTTPS
20:57:31	https://clients4.google.com/...[encrypted]	HTTPS
20:57:32	https://d1a3f4spazzrp4.cloudfront.net/...[encrypted]	HTTPS
20:57:32	https://cn-geo1.uber.com/...[encrypted]	HTTPS
20:57:32	https://service.gc.apple.com/...[encrypted]	HTTPS
20:57:33	https://service.gc.apple.com/...[encrypted]	HTTPS
20:57:33	https://service.gc.apple.com/...[encrypted]	HTTPS
20:57:33	https://service.gc.apple.com/...[encrypted]	HTTPS
20:57:33	https://init.itunes.apple.com/...[encrypted]	HTTPS
20:57:34	https://play.itunes.apple.com/...[encrypted]	HTTPS
20:57:34	https://xp.apple.com/...[encrypted]	HTTPS
20:57:34	https://sp.itunes.apple.com/...[encrypted]	HTTPS
20:57:39	https://configuration.apple.com/...[encrypted]	HTTPS
20:58:00	https://cn-geo1.uber.com/...[encrypted]	HTTPS
20:58:24	https://cn-geo1.uber.com/...[encrypted]	HTTPS

Figure 4. HTTPS requests initiated by Uber



◀ ▶ Root / mobile Applications com.ubercab.UberClient Library Application Support PersistentStorage BootstrapStore RealtimeApp.StreamModelKey

Name	Date Created	Date Modified	Date Accessed	Date Adde
city	2017-06-14 (UTC)	2017-06-14 (UTC)		
client	2017-06-14 (UTC)	2017-06-14 (UTC)		
clientStatus	2017-06-14 (UTC)	2017-06-14 (UTC)		
eyeball	2017-06-14 (UTC)	2017-06-14 (UTC)		
targetLocationSynced	2017-06-14 (UTC)	2017-06-14 (UTC)		

Figure 5. File in Uber application called "eyeball"

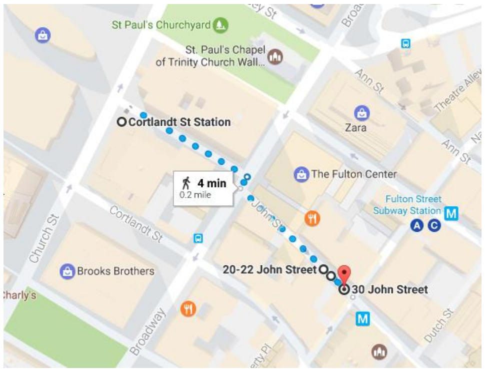


Figure 6. Vehicle path displayed in the Uber application

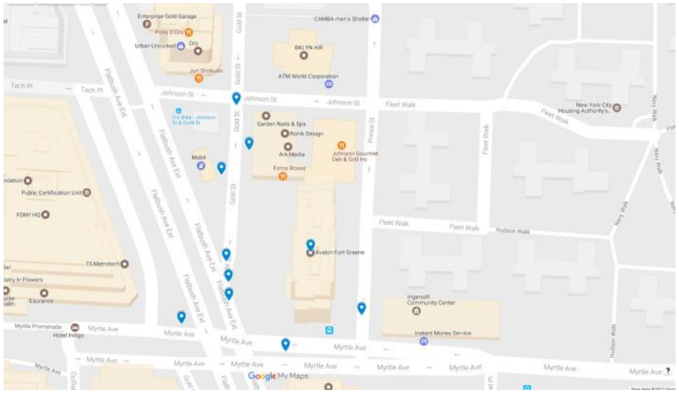
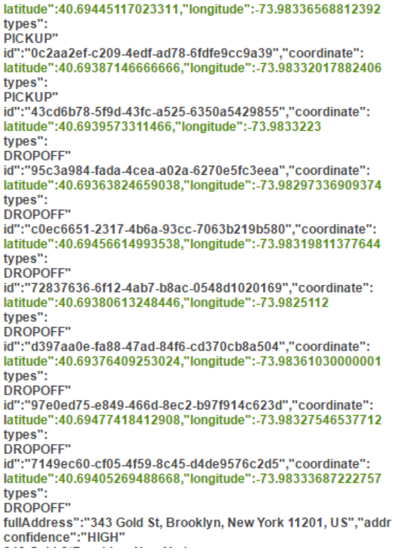
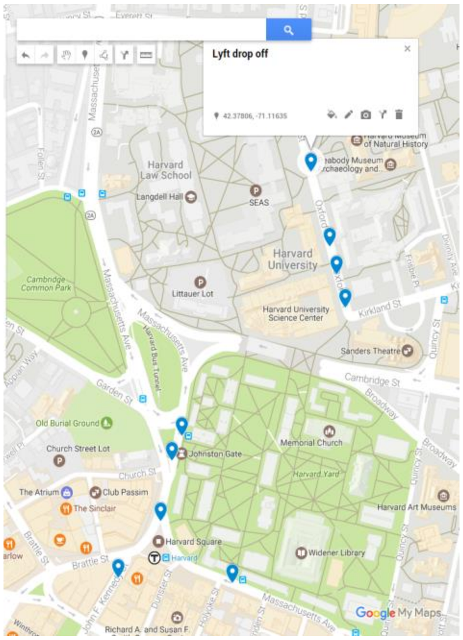


Figure 7. Map in Uber application tracking user in a Yellow Cab



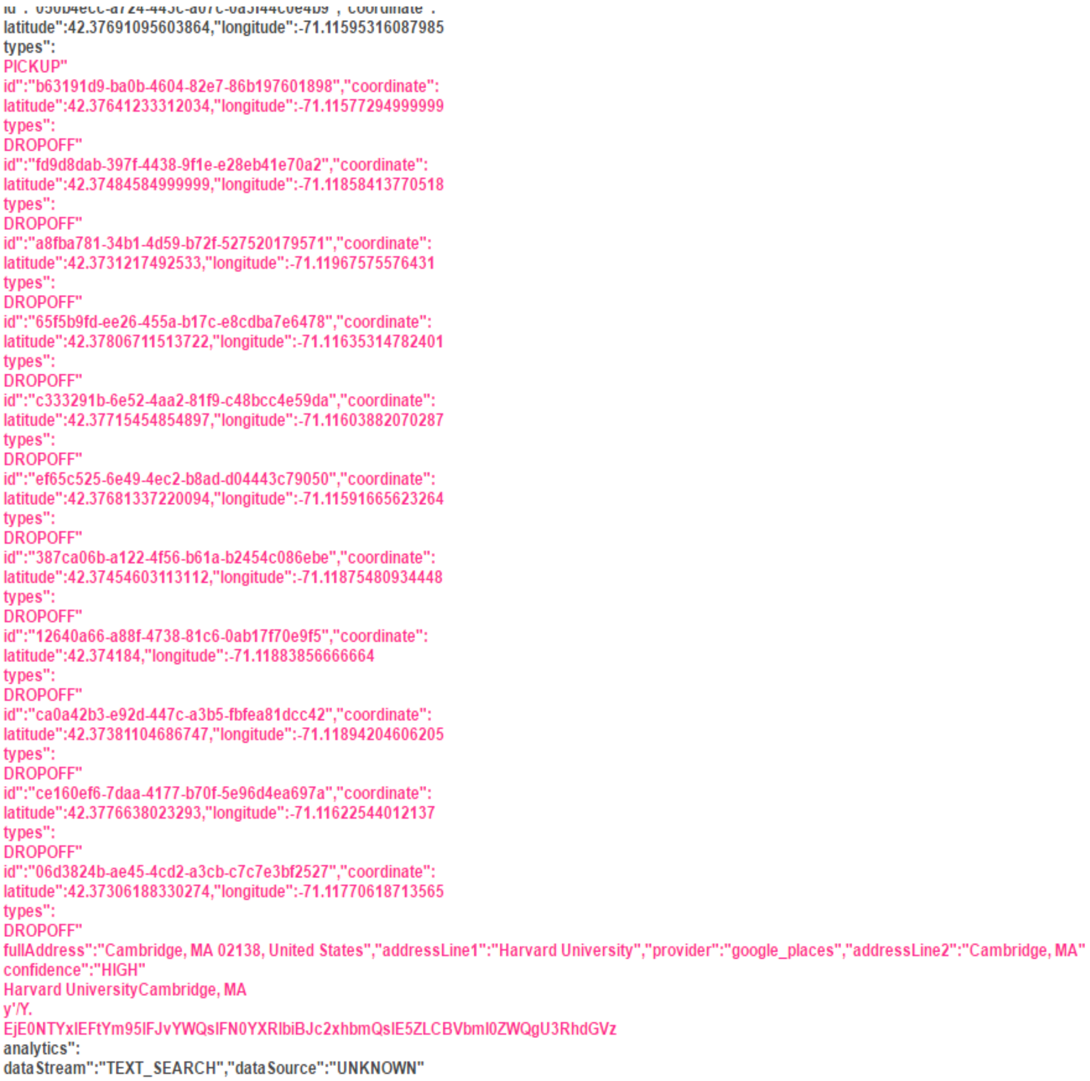
```
latitude":40.69445117023311,"longitude":-73.98336568812392
types":
PICKUP"
id":"0c2aa2ef-c209-4edf-ad78-6fdfe9cc9a39","coordinate":
latitude":40.69387146666666,"longitude":-73.98332017882406
types":
PICKUP"
id":"43cd6b78-5f9d-43fc-a525-6350a5429855","coordinate":
latitude":40.6939573311466,"longitude":-73.9833223
types":
DROPOFF"
id":"95c3a984-fada-4cea-a02a-6270e5fc3eea","coordinate":
latitude":40.69363824659038,"longitude":-73.98297336909374
types":
DROPOFF"
id":"c0ec6651-2317-4b6a-93cc-7063b219b580","coordinate":
latitude":40.69456614993538,"longitude":-73.98319811377644
types":
DROPOFF"
id":"72837636-6f12-4ab7-b8ac-0548d1020169","coordinate":
latitude":40.69380613248446,"longitude":-73.9825112
types":
DROPOFF"
id":"d397aa0e-fa88-47ad-84f6-cd370cb8a504","coordinate":
latitude":40.69376409253024,"longitude":-73.98361030000001
types":
DROPOFF"
id":"97e0ed75-e849-466d-8ec2-b97f914c623d","coordinate":
latitude":40.69477418412908,"longitude":-73.98327546537712
types":
DROPOFF"
id":"7149ec60-cf05-4f59-8c45-d4de9576c2d5","coordinate":
latitude":40.69405269488668,"longitude":-73.98333687222757
types":
DROPOFF"
fullAddress":"343 Gold St, Brooklyn, New York 11201, US","addr
confidence":"HIGH"
```

Figure 8. "PICKUP" and "DROPOFF", with a Yellow Cab, recorded by the Uber app


Lyft drop off

42.37806, -71.11635

Figure 9. "PICKUP" and "DROPOFF", with the Lyft app, recorded by the Uber app



```
id":"050b4ecc-a724-445c-a07c-0a5f44c0e4b9","coordinate":
latitude":42.37691095603864,"longitude":-71.11595316087985
types":
PICKUP"
id":"b63191d9-ba0b-4604-82e7-86b197601898","coordinate":
latitude":42.37641233312034,"longitude":-71.11577294999999
types":
DROPOFF"
id":"fd9d8dab-397f-4438-9f1e-e28eb41e70a2","coordinate":
latitude":42.37484584999999,"longitude":-71.11858413770518
types":
DROPOFF"
id":"a8fba781-34b1-4d59-b72f-527520179571","coordinate":
latitude":42.373121749253,"longitude":-71.11967575576431
types":
DROPOFF"
id":"65f5b9fd-ee26-455a-b17c-e8cdba7e6478","coordinate":
latitude":42.37806711513722,"longitude":-71.11635314782401
types":
DROPOFF"
id":"c333291b-6e52-4aa2-81f9-c48bcc4e59da","coordinate":
latitude":42.37715454854897,"longitude":-71.11603882070287
types":
DROPOFF"
id":"ef65c525-6e49-4ec2-b8ad-d04443c79050","coordinate":
latitude":42.37681337220094,"longitude":-71.11591665623264
types":
DROPOFF"
id":"387ca06b-a122-4f56-b61a-b2454c086ebe","coordinate":
latitude":42.37454603113112,"longitude":-71.11875480934448
types":
DROPOFF"
id":"12640a66-a88f-4738-81c6-0ab17f70e9f5","coordinate":
latitude":42.374184,"longitude":-71.11883856666664
types":
DROPOFF"
id":"ca0a42b3-e92d-447c-a3b5-fbfea81dcc42","coordinate":
latitude":42.37381104686747,"longitude":-71.11894204606205
types":
DROPOFF"
id":"ce160ef6-7daa-4177-b70f-5e96d4ea697a","coordinate":
latitude":42.3776638023293,"longitude":-71.11622544012137
types":
DROPOFF"
id":"06d3824b-ae45-4cd2-a3cb-c7c7e3bf2527","coordinate":
latitude":42.37306188330274,"longitude":-71.11770618713565
types":
DROPOFF"
fullAddress":"Cambridge, MA 02138, United States","addressLine1":"Harvard University","provider":"google_places","addressLine2":"Cambridge, MA"
confidence":"HIGH"
Harvard UniversityCambridge, MA
y'/Y.
EjE0NTYxIEFtYm95IFJvYWQsIFN0YXRlbiBJc2xhbmQsIE5ZLCBVbml0ZWQgU3RhdGVz
analytics":
dataStream":"TEXT_SEARCH","dataSource":"UNKNOWN"
```

Figure 10. "PICKUP" and "DROPOFF", with the Lyft app, recorded by the Uber app