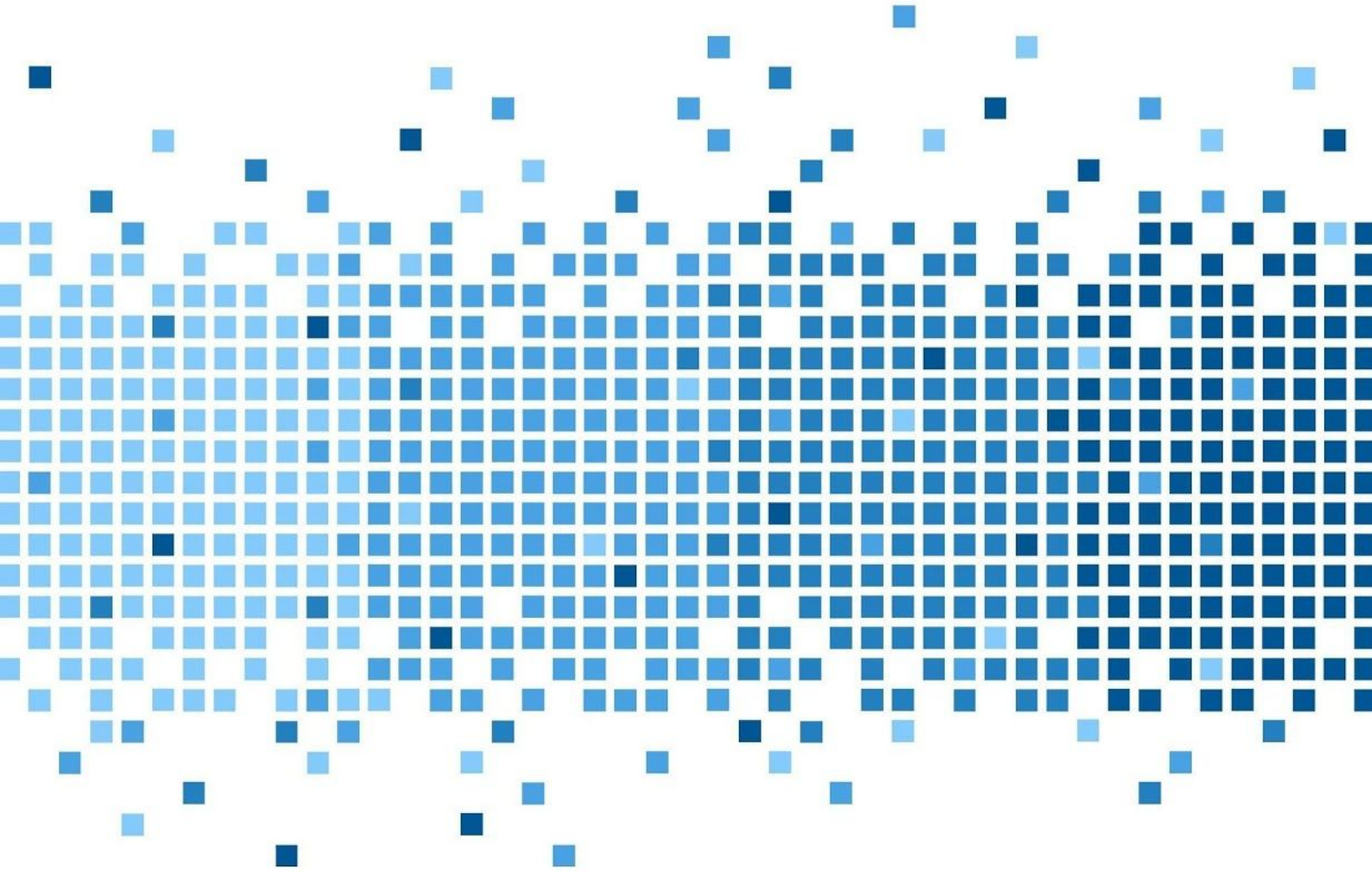
CHAMPLAIN COLLEGE | LCDI Leahy Center for Digital Investigation

Expedia Mobile Forensics



175 Lakeside Ave, Room 300A
Burlington, Vermont 05401
Phone: (802)865-5744
Fax: (802)865-6446
http://www.lcdi.champlain.edu

12/14/2018

Disclaimer:

This document contains information based on research that has been gathered by employee(s) of The Senator Patrick Leahy Center for Digital Investigation (LCDI). The data contained in this project is submitted voluntarily and is unaudited. Every effort has been made by LCDI to assure the accuracy and reliability of the data contained in this report. However, LCDI nor any of our employees make no representation, warranty or guarantee in connection with this report and hereby expressly disclaims any liability or responsibility for loss or damage resulting from use of this data. Information in this report can be downloaded and redistributed by any person or persons. Any redistribution must maintain the LCDI logo and any references from this report must be properly annotated.

Contents

Introduction

What data is stored in the travel app Expedia? Expedia is an app which allow users to search destinations in order to plan, view, and manage created trips to said destinations. The main focus: What device-stored data by Expedia is useful to forensic analysts?

Background

This is the second data analyzation/extraction project by the Mobile App Forensics team. That being said, the methodology for the first project, analysis of the app KAYAK, was similar to the process for this project. However, because the app used in this project (Expedia) is designed differently than KAYAK, certain parts of the methodology do not sync exactly between the two projects.

Purpose and Scope

Our team is looking for all artifacts that give evidence to the users planned trips and possible locations. Two phones and two tablets were used as the Scope of this project. This project is a mid-level analysis. At the least, user-generated data such as Hotel, Flight, Bundle, and Car reservations will be analyzed. Nothing past user-generated data will be part of the scope.

Research Questions

1. What data is stored on the devices by the app Expedia?
2. Why is the data stored on the device important to forensic analysts?

Terminology

Identify tools and practices used that could not be easily explained to a lay audience. Use definitions from the LCDI Wiki first, if an article for the term exists.

ADB (Android Debugging Bridge)- ADB is a command line and client/server tool, allowing the communication between the Android device and Developer. ADB can be used to install and debug apps, while also allowing user access to a Unix shell. This shell can be used to run a variety of useful commands on a device like ‘push/pull’.

Allocated Space- An organized area of space in a device’s storage containing user data and operating system. Only logical data extractions allow a user to obtain data from allocated space.

Bootloader- A small piece of code injected into RAM at start-up, allowing the flashing of firmware. However, for forensic analysts, this is a means of gaining access to user data, and then copying it.

Extraction- The process of obtaining mobile device data, then, storing the data in an approved location to be processed after.

Physical Data Extraction- Accessing device data layers in unallocated and allocated space. Specifically, Cellebrite 4PC accesses three different groups of content within the data layers: *logical, deleted content,* and

content the phone collects that is non-user generated. The user is able to view the collected data because 4PC creates a copy of the device's flash memory.

Rooting- Rooting an Android device is the act of an owner by-passing factory settings to gain 'root' or 'superuser' access - which gives the owner Administrative rights. Rooting an Android phone gives the owner access to the operating system.

SQLiteDatabase- Database file format commonly used for data storage of mobile and application data.

UFED Cellebrite 4PC- Cellebrite's UFED is extraction software designed to extract and analyze mobile device data. This includes cell phones and tablets. With 4PC the user has many options of data extraction, including but not limited to Physical and Logical data extractions. After the user chooses whichever data extraction they care for, they are able to analyze the extracted data with Physical Analyzer.

UFED Cellebrite Physical Analyzer (PA)- Cellebrite's Physical Analyzer is an application capable of analysis, decoding and reporting. PA offers a wide variety of variables to explore once extracted data has been loaded. An example of what PA is capable of reporting: timeline graphs/details, device calls, texts, cookies, databases, files, instant messages, locations, and images. PA carves images and locations as well.

Unallocated Space- Area on a device's memory outside the defined file system available to be written to.

Methodology and Methods

For the Expedia project, we are going to be generating data on the devices and then extracting them. The generated data is on a case by case basis, so it will be included in the results page for each device. Cellebrite tools are used to extract the information. To analyze our data, we are going to look through the databases of the app and look through each item one by one. We will document the purpose of each item and analyze the information each row and column contains if it is important to our research. Ones that are not important will be blank items. For this research in particular, lots of cross analyzation had to take place, thus we document IDs that pop up across the databases.

Equipment Used

The tool UFED Cellebrite Physical Analyzer 7 and UFED Cellebrite 4PC.

Table 1: List of Devices

Device	OS Version	Serial Number	Comments
Huawei H1511 Nexus 6P LCDI-5017	Android 8.1.0	84B7N16302000150	Used for phone data generation/analysis
Huawei H1511 Nexus 6P LCDI-5016	Android 8.1.0	84B7N16302000871	Used for phone data generation/analysis
Nexus 7 LCDI-6028	Android 6.0.1	094e2f8a	Used for tablet data generation/analysis

Nexus 7	Android 6.0.1	092958a2	Used for tablet data generation/analysis

Data Collection

The data will be collected by using Cellebrite 4PC to perform an ADB Root extraction. It will then be analyzed via the Cellebrite UFED Physical Analyzer. Data will be found by analyzing the databases for the app. Each database item and the rows and columns will be analyzed. Data that is documented include important or notable findings.

Analysis

Expedia's users expect an app allows them to find "greatly priced" reservations whether it be airline tickets, hotel reservations, or car rentals. This being said, through the extractions, the team expects to find the searches for said reservations. Searches are expected to be in .db or .sqlite form,however, based on other extraction projects, it is possible to also find data by looking through the Cache.

Results

The results of the physical extraction for both devices (Nexus & Huawei) is quite bare. There was very little user-generated data able to be found. Nearly all data found from the physical extraction of the Nexus tablets and Huawei phones is comprised of auto generated data.

Nexus 7 K009 Expedia Results

userdata (ExtX)/Root/data/com.expedia.bookings/shared_prefs/carnivalSharedPreferencesInstance.xml

Table 2: User data found in: userdata (ExtX)/Root/data/com.expedia.bookings/shared_prefs/carnivalSharedPreferencesInstance.xml

Name	Value
product_view_hotel_destination	New York (and vicinity), New York, United States of America
app_open_launch_relaunch_notification_type	[MKTG, SERV, PROMO]
product_view_hotel_number_of_adults	1
checkout_start_hotel_length_of_stay	1
product_view_hotel_length_of_stay	
checkout_start_hotel_check-in_date	Sat Nov 10 00:00:00 EST 2018
checkout_start_flight_number_of_adults	1
search_hotel_destination	New York (and vicinity), New York, United States of America
search_hotel_check-in_date	Sat Nov 10 00:00:00 EST 2018
search_flight_destination	Florence, Italy (FLR-Peretola)
app_open_launch_relaunch_booked_product	[]
app_open_launch_relaunch_loyalty_tier	BLUE
app_open_launch_relaunch_pos	expedia.com

checkout_start_hotel_hotel_name	Hotel Indigo Lower East Side New York
search_flight_departure_date	Sat Nov 10 00:00:00 EST 2018
search_hotel_number_of_adults	1
search_hotel_length_of_stay	1
checkout_start_flight_destination	Florence, Italy (FLR-Peretola)
checkout_start_flight_airline	[TAP Portugal]
product_view_hotel_hotel_name	Hotel Indigo Lower East Side New York
search_flight_number_of_adults	1
checkout_start_flight_length_of_flight	37:35
checkout_start_hotel_number_of_adults	1
app_open_launch_relaunch_userid	1376573792
app_open_launch_relaunch_user_email	hopekaiya1001@gmail.com
checkout_start_flight_flight_number	[878, 202, 201, 877]
product_view_hotel_check-in_date	Sat Nov 10 00:00:00 EST 2018
app_open_launch_relaunch_location_enabled	true
checkout_start_flight_departure_date	Sat Nov 10 00:00:00 EST 2018
app_open_launch_relaunch_sign-in	true
app_open_launch_relaunch_last_location	null, null
checkout_start_hotel_destination	New York (and vicinity), New York, United States of America

The information in the table above are Flights, Hotel Reservations, and Bundle deals saved by the team.

Conclusion

According to the results the team pulled through physical extraction of each member's devices, there isn't a whole lot of information/data that would be useful to forensic analysts. Reason being, the amount of data able to be retrieved is fairly trivial;most data able to be pulled from Expedia is *not* user-generated but rather, it is automatically filled by the app itself. The small amount of user generated data able to be extracted from the Nexus 7 K009 is the only user-generated data able to be found.

Further Work

The team missed a lot of things due to the fact that only small amounts of user-generated data was found. It would be interesting and more productive if the team was able to find the user-generated data. If anything about this project could be changed, perhaps the method of extraction should be chosen. Possibly, if the team were to choose a different way of extraction (logical, not using Cellebrite and using the actual ADB program), then perhaps more user-generated data could be found.

Appendix

Expedia Data Generation Nexus 7 KOO9

Table 3: HOTEL

Title	Booking dates	Price (in $USD)	Search Timestamp
Hotel Indigo	November 10th - 11th, 2018	429	3:34 PM 10/30/2018

Table 4: FLIGHT

Title	Booking dates	Destination	Layover	Price (in $USD)	Search Timestamp
Hotel Indigo	November 11th, 2018	Florence, Italy	Lisbon, Portugal	966	3:46 PM 10/30/2018

Table 5: BUNDLE

Title	Booking dates	From	Destination/Location	Price (in $USD)	Search Timestamp
Flight: Air Dolomiti; Round trip	November 11th, 2018	JFK	Florence, Italy	605.04	4:05 PM 10/30/2018
Hotel: Hotel Real	November 11th - November 13	N/A	Florence, Italy	(Bundled with Flight)	4:05 PM 10/30/2018

Table 6: CAR RENTAL

Title	Model	Booking dates	Price (per day in $USD)	Search Timestamp
Budget	Volkswagen Golf or Similar	November 10th - 11th, 2018	58	4:10 PM 10/30/2018

The team left "feedback" for Expedia at **4:17 PM 10/30/2018:**

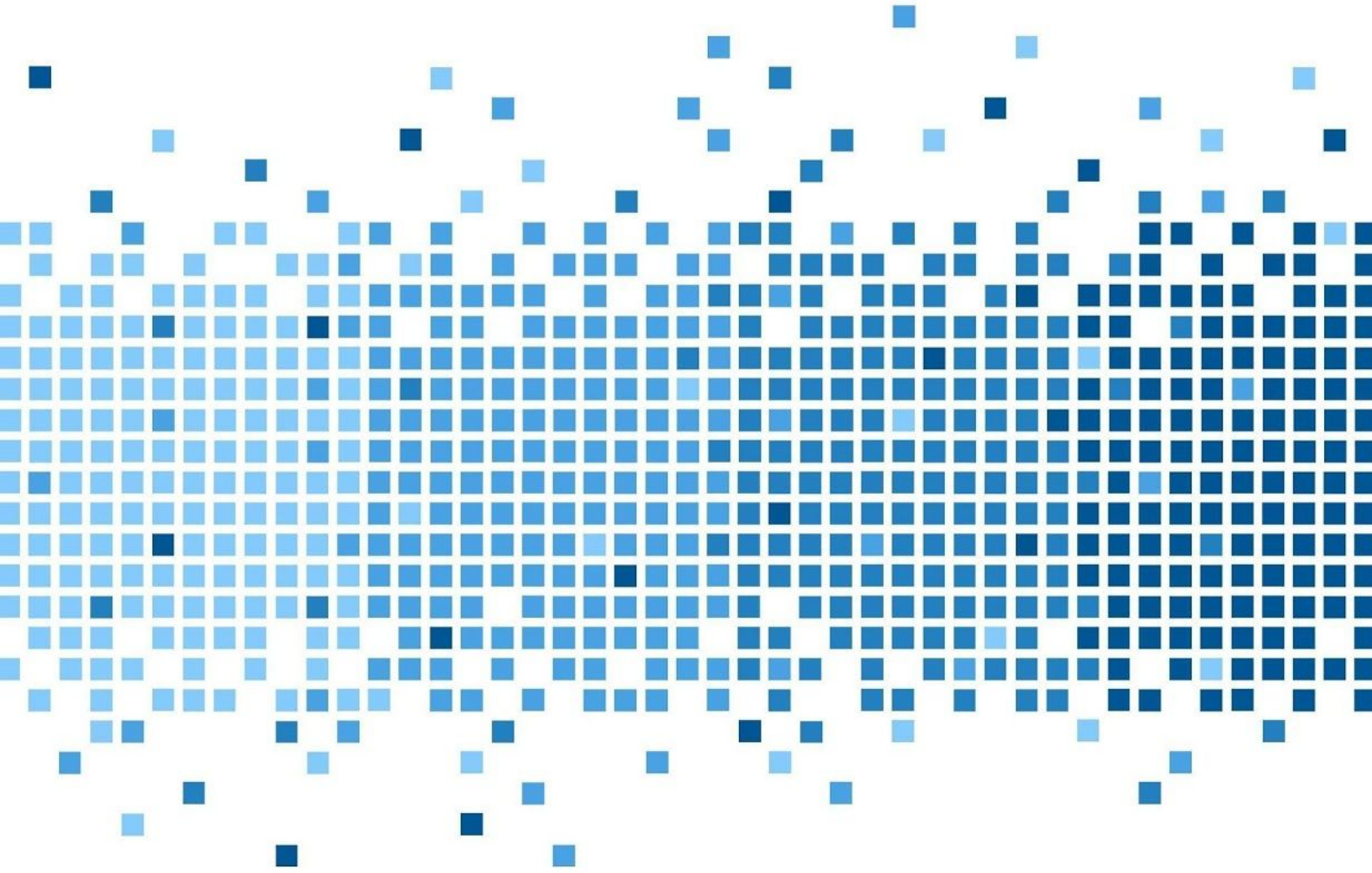
- "Great!"
- Also rated it "++ 10/10"

References

"What Happens When You Press That Button?" *Smarterforensics.com*, smarterforensics.com/wp-content/uploads/2014/06/Explaining-Cellebrite-UFED-Data-Extraction-Processes-final.pdf.

CHAMPLAIN COLLEGE | LCDI Leahy Center for Digital Investigation

Google Trips Mobile Forensics



175 Lakeside Ave, Room 300A
Burlington, Vermont 05401
Phone: (802)865-5744
Fax: (802)865-6446
http://www.lcdi.champlain.edu

12/14/2018

Disclaimer:

This document contains information based on research that has been gathered by employee(s) of The Senator Patrick Leahy Center for Digital Investigation (LCDI). The data contained in this project is submitted voluntarily and is unaudited. Every effort has been made by LCDI to assure the accuracy and reliability of the data contained in this report. However, LCDI and its employees make no representation, warranty or guarantee in connection with this report and hereby expressly disclaim any liability or responsibility for loss or damage resulting from use of this data. Information in this report can be downloaded and redistributed by any person or persons. Any redistribution must maintain the LCDI logo and any references from this report must be properly annotated.

Contents

Introduction

What data is stored in the app Google Trips? Google Trips is an app which allow users to set destinations in order to plan, view, and manage created trips to said destinations. Our main focus is to discover what device-stored data by Google Trips is useful to forensic analysts.

Background

This is the second data analyzation/extraction project by the Mobile App Forensics team. That being said, the methodology for the first project, analyzation on the app KAYAK, was similar to the process for this project. However, because the app used in this project (Google Trips) is designed differently than KAYAK, certain parts of the methodology do not sync exactly between the two projects.

The same tools and extraction process were used for the this project, as compared to the KAYAK project.

Purpose and Scope

Our team is looking for all artifacts that give evidence to the users planned trips and possible locations. Two phones and two tablets were used as the Scope of this project. This project is a mid-level analysis. At the least, user-generated data such as: Trips, Favorites, Starred Places, Want to go, Reviews (only by the Mobile App Forensics team) Day Plans, Usernames, and Passwords will sought out for. Nothing past user-generated data will be part of the search scope.

Research Questions

1. What data is stored on the devices by the app Google Trips?
2. Why is the data stored on the device important to forensic analysts?

Terminology

ADB (Android Debugging Bridge)- ADB is a command line and client/server tool, allowing the communication between the Android device and Developer. ADB can be used to install and debug apps, while also allowing user access to a Unix shell. This shell can be used to run a variety of useful commands on a device like ‘push/pull’.

Allocated Space- An organized area of space in a device’s storage containing user data and operating system. Only logical data extractions allow a user to obtain data from allocated space.

Bootloader- A small piece of code injected into RAM at start-up, allowing the flashing of firmware. However, for forensic analysts, this is a means of gaining access to user data, and then copying it.

Extraction- The process of obtaining mobile device data, then, storing the data in an approved location to be processed after.

Physical Data Extraction- Accessing device data layers in unallocated and allocated space. Specifically, Cellebrite 4PC accesses three different groups of content within the data layers: *logical, deleted content,* and

content the phone collects that is non-user generated. The user is able to view the collected data because 4PC creates a copy of the device's flash memory.

Rooting- Rooting an Android device is the act of an owner by-passing factory settings to gain 'root' or 'superuser' access which gives the owner administrative rights. Rooting an Android phone gives the owner access to the operating system.

SQLiteDatabase- Database file format commonly used for data storage of mobile and application data.

UFED Cellebrite 4PC- Cellebrite's UFED is extraction software designed to extract and analyze mobile device data. This includes cell phones and tablets. With 4PC the user has many options of data extraction, including but not limited to physical and logical data extractions. After the user chooses whichever data extraction they care for, they are able to analyze the extracted data with Physical Analyzer.

UFED Cellebrite Physical Analyzer (PA)- Cellebrite's Physical Analyzer is an application capable of analysis, decoding and reporting. PA offers a wide variety of variables to explore once extracted data has been loaded. Examples of what PA is capable of reporting include: timeline graphs/details, device calls, texts, cookies, databases, files, instant messages, locations, and images. PA carves images and locations as well.

Unallocated Space- Area on a device's memory outside the defined file system available to be written to.

MID- Locations are all listed as a set of IDs**.**
They can vary between a couple of styles:
/m/(6-7 Characters)
/cid/(36 Characters)
/g/(6-9 Characters)
From now on, all IDs that follow these formats will be referred to as **MIDs**.

F:0x47a84e373f035901:0x42120465b5e3b70- The ID assigned to Berlin, Germany by Google Trips.

Methodology and Methods

For this research project, we are going to generate data on the devices and then extract them. The generated data is on a case by case basis, so it will be included in the results page for each device. Cellebrite tools are used to extract the information. To analyze our data, we are going to look through the databases of the apps and look through each item one by one. We will document the purpose of each item and analyze the information each row and column contains if it is important to our research. Ones that are not important will be blank items. For this research in particular, lots of cross analyzation had to take place, thus we document IDs that pop up across the databases.

Equipment Used

The tool UFED Cellebrite Physical Analyzer 7 and UFED Cellebrite 4PC.

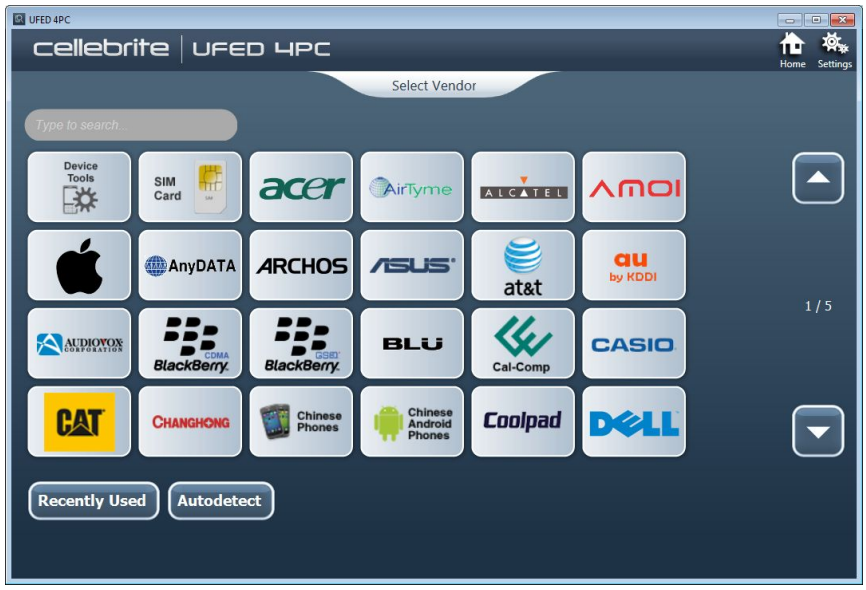


Table 1: List of Devices

Device	OS Version	Serial Number	Comments
Huawei H1511 Nexus 6P LCDI-5017	Android 8.1.0	84B7N16302000150	Used for phone data generation/analysis
Huawei H1511 Nexus 6P LCDI-5016	Android 8.1.0	84B7N16302000871	Used for phone data generation/analysis
Nexus 7 LCDI-6028	Android 6.0.1	094e2f8a	Used for tablet data generation/analysis
Nexus 7	Android 6.0.1	092958a2	Used for tablet data generation/analysis

Data Collection

The data will be collected by conducting an ADB Root via Cellebrite 4PC. Then it will be analyzed via the Cellebrite UFED Physical Analyzer. Data will be found by analyzing the databases for the app. Each database item, row, and column will be analyzed. Data that is documented will include important or notable findings.

Analysis

The app Google Trips expects users to use it for recording travel information. Users store differing amounts of PII and payment information depending on their preferences. Travel information in this context refers to things such as airline tickets, hotel reservations, and bus tickets, all of which are being stored by the apps in the internal storage of the user's devices. The information stored by Google trips is useful for forensic analysts because it can be used in different scenarios of investigation. For example, if an analyst were to be tasked to find the travel plans of "Person X", the analyst would simply obtain their phone, image it, and analyze the Google Trips data.

Results

Nexus K009 Tablet (Serial Number 094e2f8a)

Google Trips Results

All under 'Guide_106090829529772234695 6.db'

The table ConstellationLists contained the titles that were saved by the team under "Things to do". This includes the following titles: Starred Places, Favorites, and Want to go. This table also contained the LastModificationTimestamps. See table 1.

Table 2: ConstellationLists

ServerId	ClientID	SyncToken	ListDescriptorProto	Synced	LastModificationTimestamp
starred_places_list		CLLijbbsLBJrCAISSAoAEAEaEgkA_GVbeHkFACEA_GVbeHkFACIUCRbGc2t4eQUAEAIZWPOeTqbgVsgyGAoWCAIRJkt0a3h5BQAYACEAAAAAAAAAABgBIhgKFggCESZLdGt4eQUAGAAhAAAAAAAAAC4BgI=	starred_places_listStarred places(@	0	1540498357428 Thursday, October 25, 2018 4:12:37.428 PM GMT-04:00 DST
CReqNsQxfos0ALBX_qFybbcEsb4Wtg	list:106908295297722346956:1000	GicKHkNSZXFOc1F4Zm9zMEFMQlhfcUZ5YmJjRXNiNFd0ZxDzkIa27CwaJwoed2dpZlRYWEF2MHR4QUh2d2JSOUVJOFIyZy1BV3RRENaNirbsLCAA	#list:106908295297722346956:1001? Favorites(@	1	Thursday, October 25, 2018 5:11:00.435 PM GMT-04:00 DST
wgifTXXAv0txAHvwbR9EI8R2g-AWtQ	list:106908295297722346956:1001	GicKHkNSZXFOc1F4Zm9zMEFMQlhfcUZ5YmJjRXNiNFd0ZxDzkIa27CwaJwoed2dpZlRYWEF2MHR4QUh2d2JSOUVJOFIyZy1BV3RRENaNirbsLCAA	#list:106908295297722234:1001? Want to go(@	1	Thursday, October 25, 2018 5:11:04.888 PM GMT-04:00 DST

The table ConstellationPOIs contains the actual variables listed under the lists "Things to do".

Table 3: ConstellationPOIs

ListId	ListEntryProto	Synced	LastModificationTimestamp
starred_places_list	/m/01ck3b L(6?* /m/01ck3bCheckpoint Charlie	1	1540932928434
starred_places_list	/m/064lq (vl??*/m/064lqPotsdamer Platz	1	1540932988512

The table "CuratedMoods" found in the Google Trips database file "Guide_1060908295297722346956.db" contains the three locations the team saved under our ConstellationLists [see table below].

Table 4: CuratedMoods

DestinationID	CuratedMoodProto	LastUpdatedTimestamp
F:0x47a84e373f035901:0x42120465b5e3b70	? Q Berlin Wall Berlin Wall:5https://www.gstatic.com/trips/res/v1/mood_history.png /m/01ck3b /m/0kbh59w /m/03t4ff/m/064lq /g/11b6dz2rss /g/1tg5b3vz ? Q Small museums Small museums"1https://www.gstatic.com/trips/res/v1mood_art.png/cid/9504443459442203694 /g/1223qcn6/cid/9967395468153302924 /g/12vqp4xxt /g/11_ygnlrc /m/0119by9y /m/0g5sbyx /m/0ddc280 ? U Jewish Berlin Jewish Berlin"5https://www.gstatic.com/trips/res/v1/mood_history.png /m/053jwh /m/02s49b /g/1tdw2hn7/cid/15464703148802214141 /m/03ddr2/cid/7107847227975070600 /m/02z485r/cid/7819966749613956	1540930849910 [Tuesday, October 30, 2018 4:20:49.910 PM GMT-04:00 DST]

	/m/065x24p /m/047mkmn ? Y Literary BerlinLiterary Berlin”5https://www.gstatic.com/trips/res/v1/mood_history.png/cid/13135120527728336905/cid/7717063477044946780/cid/12763323479323138895/cid/27630780897222 5804/cid/14495639625621081180/cid/12750650827794620281/cid/182543218424263 26569/cid/279941198522453192 ? a M...	

The table “Destinations” contains the trips created by the team, along with the ID appointed to said trips.

Note: only the last two entries in the table apply. The other entries above the last two are old entries due to the fact data was generated on the tablet before this project and it wasn’t wiped before starting the new one.

Table 5: Destinations

TripID	Destination ID	DestinationStatus	LastUpdatedTimestamp
EPHEMERAL:F:0x4cc91a541c64b70d:0x654e3138211fefef	F:0x4cc91a541c64b70d:0x654e3138211fefef	2	1540498901028 [Thursday, October 25, 2018 4:21:41.028 PM GMT-04:00 DST]
Trip:5bcdf639-0000-252d-a9e7-2405886e5098	F:0x4cc91a541c64b70d:0x654e3138211fefef	1	1540501963315 [Thursday, October 25, 2018 5:12:43.315 PM GMT-04:00 DST]
EPHEMERAL:F:0x47a84e373f035901:0x42120465b5e3b70	F:0x47a84e373f035901:0x42120465b5e3b70	2	1540930733209 [Tuesday, October 30, 2018 4:18:53.209 PM GMT-04:00 DST]
Trip:5bd72ef0-0000-2e24-bf49-f40304384cf0	F:0x47a84e373f035901:0x42120465b5e3b70	2	1540930853175 [Tuesday, October 30, 2018 4:20:53.175 PM GMT-04:00 DST]

The table “Itineraries” contains data that was browsed by the team under “Things to do”; however, this data was not specifically saved by us but rather, it was saved automatically by Google Trips.

Table 6: Itineraries

_id	Destination ID	Creation Type	ItineraryPhoto	LastUpdatedTimestamp
13	F:0x47a84e373f01x42120465b5e3b70	1	Kid-friendly attractionsdCriss-crossing Berlin with young children, including a famous zoo & interactive technology exhibits. /m/03ylf7?T” ?L .?# /m/02r3p9?8? “ ??M?=?” /m/0drxn?*?” f?J?M/?*https://goo.gl/maps/iRbxSO	1540930853175 [Tuesday, October 30, 2018 4:20:53.175 PM GMT-04:00 DST]

The table “Trips” contains data entered under “Reservations”. Essentially, this contains the destination locations the team entered into Google Trips under the trip “Trip to Berlin”. The table “Trips” contains airline, bus, and train data.

Table 7: Trips

_id	TripName	Start Date	EndDate	Photo Data	TripStatus	LastUpdateTimestamp	TripProto	UserCreated	IsEphemeral
13	F:0x47a84e373f01x42120465b5e3b70	1	1542672000000 [Tuesday, November 19, 1974 6:40:15.755 AM GMT-05:00]	1542758400000 [Tuesday, November 20, 2018 7:00:00 PM GMT-05:00	System.Byte[]	0	**Does not fit this cell. See next Table.**	1	0

TripProto - TripProto was moved to its own table due to the fact that there was a lot of data that did not fit in the table above.

TripProto
)Trip5bd72ef0-0000-2e24-bf49-f40304384cf0? ? ? 123z   DLDeltadB $?????,America/New_York?????????:????, Europe/Berlin<’ JFK New York City” BERBerlinZ; 9FlightLegReservation:5bd72f4f-0000-2aba-9d12-2405886ca488?232j? S Ostabhnhof (Berlin)q   ?xL i.?GN?G+?K{??p*/cid/8123277159338381232&Koppenstraße 3, 10243 Berlin, Germanyr Europe/Berlinr?????, Europe/Berlin<?v Hamburg Central Station[????? ?? D?G$’z??\I*/cid/5286241596730335268 2Hamburg, Germanyr Europe/Berlin??????, Europe/Berlin<?   Hope Kaiya?E CTransportationRouteReservation:5bd72c8c=0000-2723-814c-f40304384070?2?321j? Berlin Central Station}

?ND? {????Q?G????x<z*/cid/880804700103671722622Hauptbahnhof,Europaplatz 1, 10557 Berlin, Germanyr Europe/Berlinr????,
Eu...

Huawei H1511 Nexus 6P LCDI-5017

Google Trips Results

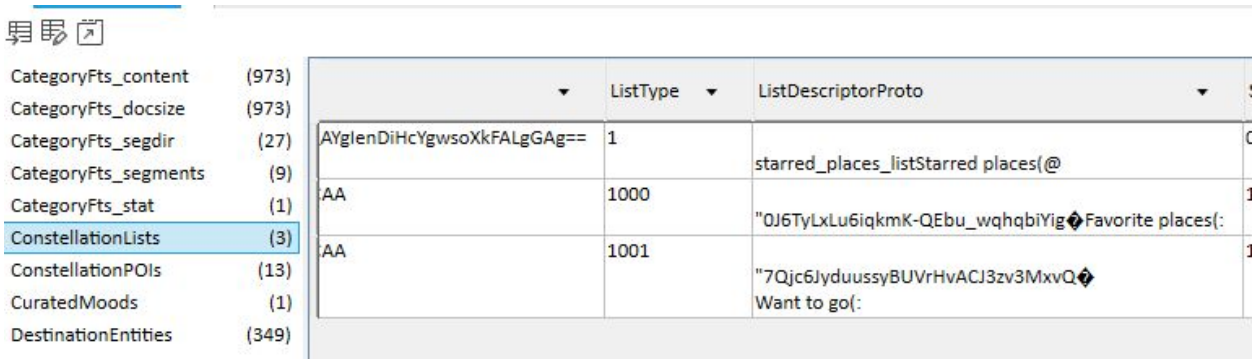
The ID for the user created trip is: 5bda769e-0000-274d-98b9-f403043e9068

Catagory Content and Docsize contain all the MIDs and the categories they fall under for all locations in Berlin.

Category segments may contain information about the categories, but is mostly gibberish.

ConstellationLists contains information about ‘Starred’, ‘Favorited’, and ‘Want To Go’. It doesn’t contain information about what is actually in those containers, just descriptions of what they are.

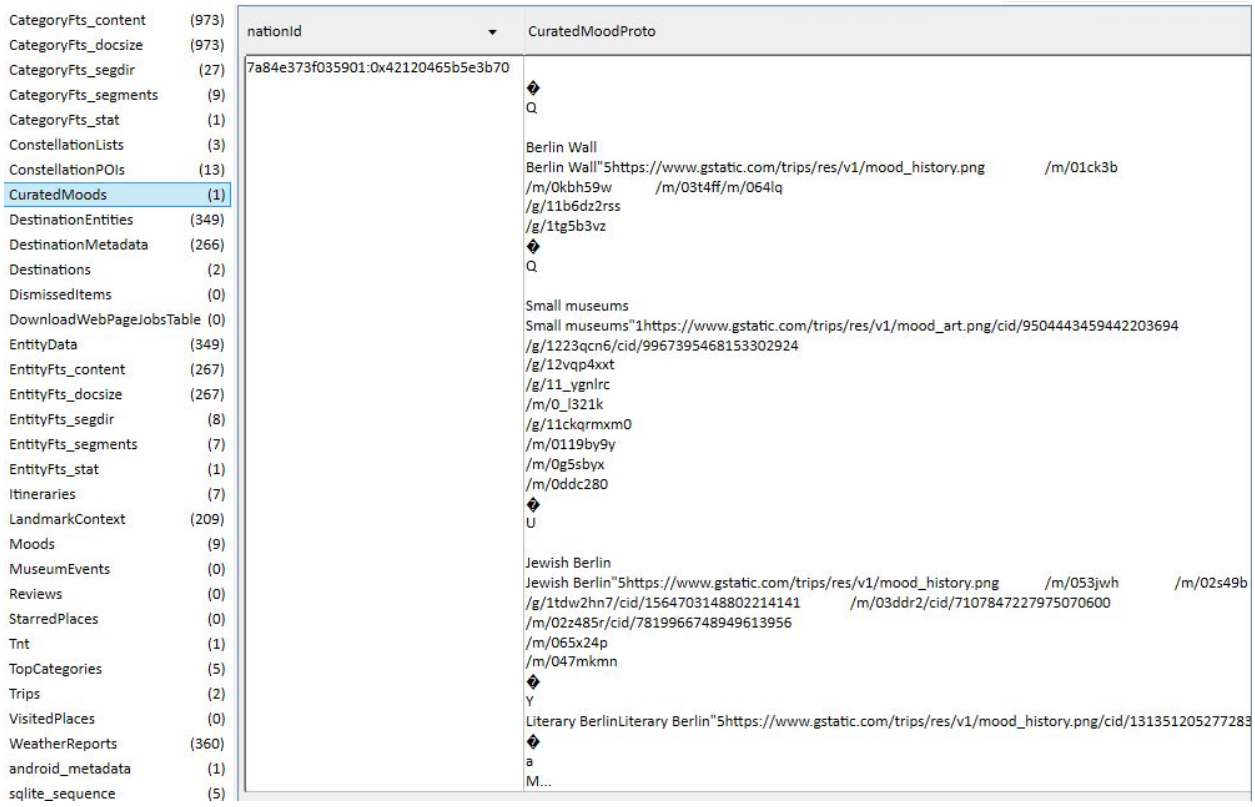
Figure 1: ConstellationLists Screenshot



The selected Starred, Favorited and Want To Go places are in ConstellationPOIs

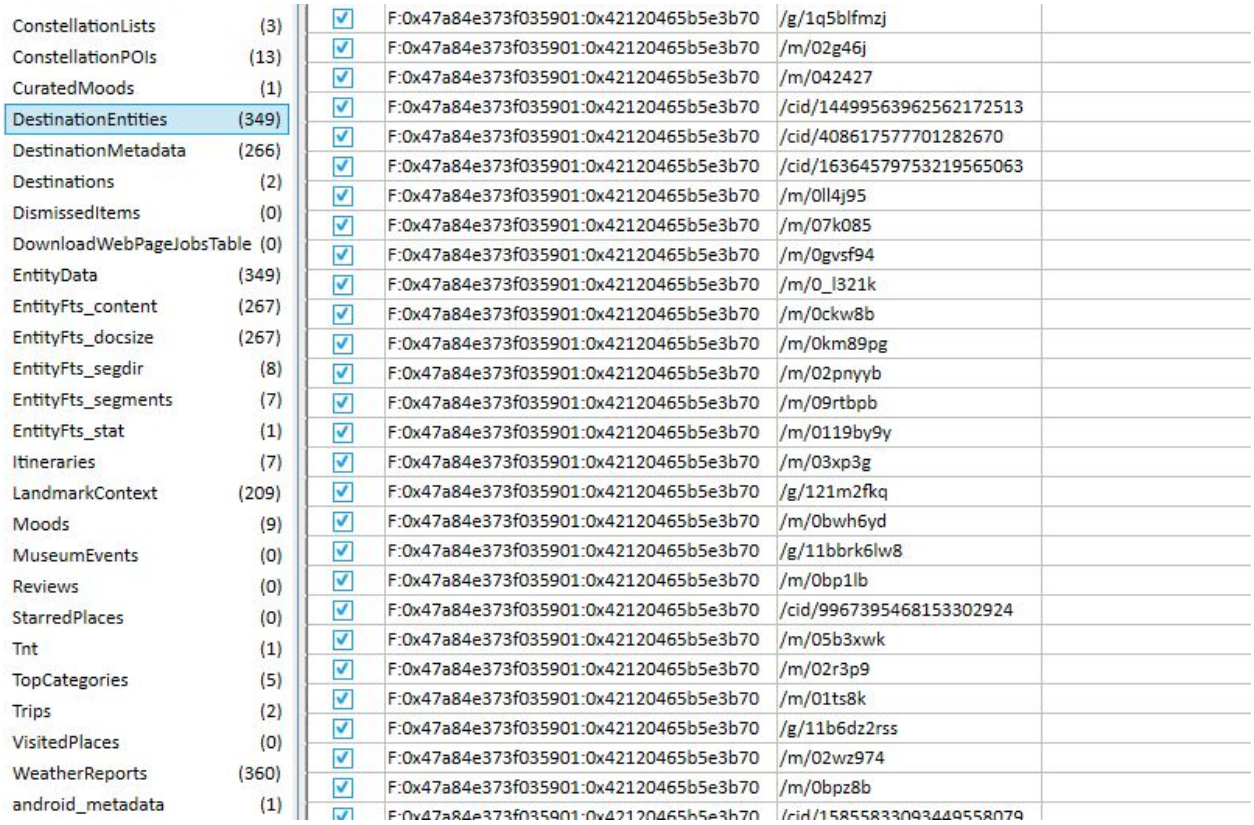
CuratedMoods is most likely the day plans made. The Jewish Berlin referenced in this table is likely in reference to the Memorial to the Murdered Jews of Europe that I did not include in any sections besides day plans.

Figure 2: CuratedMoods Screenshot



DestinationEntities may be all the possible destinations of the trip. There are two columns, the DestinationID, and the MID, which contains of the various IDs described at the top.

Figure 3: DestinationEntities Screenshot



ConstellationLists	(3)
ConstellationPOIs	(13)
CuratedMoods	(1)
DestinationEntities	(349)
DestinationMetadata	(266)
Destinations	(2)
DismissedItems	(0)
DownloadWebPageJobsTable	(0)
EntityData	(349)
EntityFts_content	(267)
EntityFts_docsize	(267)
EntityFts_segdir	(8)
EntityFts_segments	(7)
EntityFts_stat	(1)
Itineraries	(7)
LandmarkContext	(209)
Moods	(9)
MuseumEvents	(0)
Reviews	(0)
StarredPlaces	(0)
Tnt	(1)
TopCategories	(5)
Trips	(2)
VisitedPlaces	(0)
WeatherReports	(360)
android_metadata	(1)

F:0x47a84e373f035901:0x42120465b5e3b70	/g/1q5blfmzj
F:0x47a84e373f035901:0x42120465b5e3b70	/m/02g46j
F:0x47a84e373f035901:0x42120465b5e3b70	/m/042427
F:0x47a84e373f035901:0x42120465b5e3b70	/cid/14499563962562172513
F:0x47a84e373f035901:0x42120465b5e3b70	/cid/408617577701282670
F:0x47a84e373f035901:0x42120465b5e3b70	/cid/16364579753219565063
F:0x47a84e373f035901:0x42120465b5e3b70	/m/0ll4j95
F:0x47a84e373f035901:0x42120465b5e3b70	/m/07k085
F:0x47a84e373f035901:0x42120465b5e3b70	/m/0gvsf94
F:0x47a84e373f035901:0x42120465b5e3b70	/m/0_l321k
F:0x47a84e373f035901:0x42120465b5e3b70	/m/0ckw8b
F:0x47a84e373f035901:0x42120465b5e3b70	/m/0km89pg
F:0x47a84e373f035901:0x42120465b5e3b70	/m/02pnyyb
F:0x47a84e373f035901:0x42120465b5e3b70	/m/09rtbpb
F:0x47a84e373f035901:0x42120465b5e3b70	/m/0119by9y
F:0x47a84e373f035901:0x42120465b5e3b70	/m/03xp3g
F:0x47a84e373f035901:0x42120465b5e3b70	/g/121m2fkq
F:0x47a84e373f035901:0x42120465b5e3b70	/m/0bwh6yd
F:0x47a84e373f035901:0x42120465b5e3b70	/g/11bbrk6lw8
F:0x47a84e373f035901:0x42120465b5e3b70	/m/0bp1lb
F:0x47a84e373f035901:0x42120465b5e3b70	/cid/9967395468153302924
F:0x47a84e373f035901:0x42120465b5e3b70	/m/05b3xwk
F:0x47a84e373f035901:0x42120465b5e3b70	/m/02r3p9
F:0x47a84e373f035901:0x42120465b5e3b70	/m/01ts8k
F:0x47a84e373f035901:0x42120465b5e3b70	/g/11b6dz2rss
F:0x47a84e373f035901:0x42120465b5e3b70	/m/02wz974
F:0x47a84e373f035901:0x42120465b5e3b70	/m/0bpz8b
F:0x47a84e373f035901:0x42120465b5e3b70	/cid/15855833093449558079

DestinationMetadata contains the same values as DestinationEntities, but also a Position number. Currently unknown what this number does.

Under Destinations, there are two rows, each with a TripId, DestinationId, DestinationStatus, and LastUpdateTimestamp. The info is as follows:

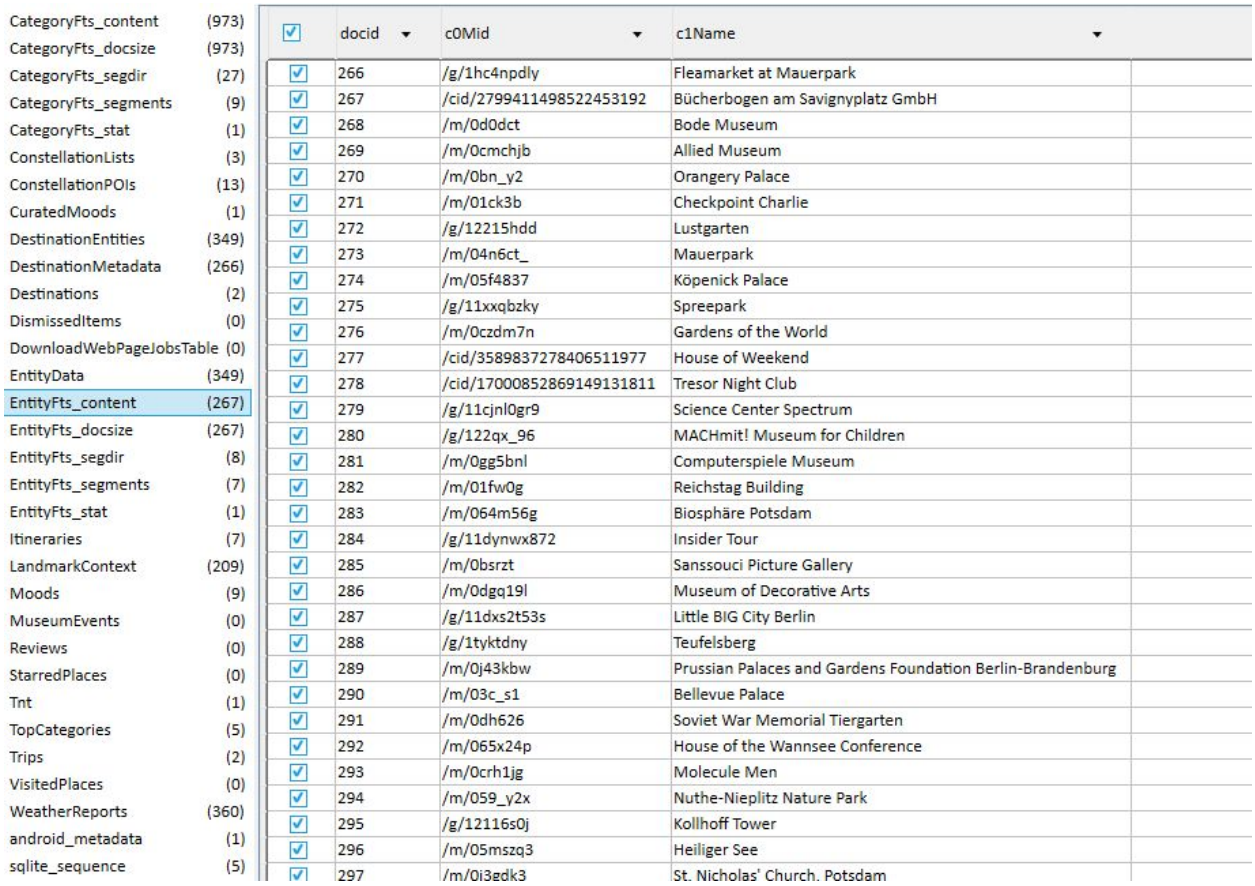
First Row:
TripId: EPHEMERAL:F:0x47a84e373f035901:0x42120465b5e3b70
DestinationId: F:0x47a84e373f035901:0x42120465b5e3b70
DestinationStatus: 2
LastUpdateTimestamp: 1541106790229 (Thu, 01 November 2018 21:13:10.229 UTC)

Second Row:
TripId: Trip:5bda769e-0000-274d-98b9-f403043e9068
DestinationId: F:0x47a84e373f035901:0x42120465b5e3b70
DestinationStatus: 2
LastUpdateTimestamp: 1541106893885 (Thu, 01 November 2018 21:14:53.885 UTC)

EntityData is the description of each MID and reveals insight as to what ID correlates to what location. It includes the Mid, EntityProto, RatingHistogram, IsAttraction, DetailedLevel, LastUpdateTimestamp.

The last item is further expanded under EntityFts_content. This provides 3 columns, docid, c0Mid, and c1Name. This is an extremely useful item in that it provides the exact name of each location along with their correlating MID.

Figure 3: EntityFts_content Screenshot

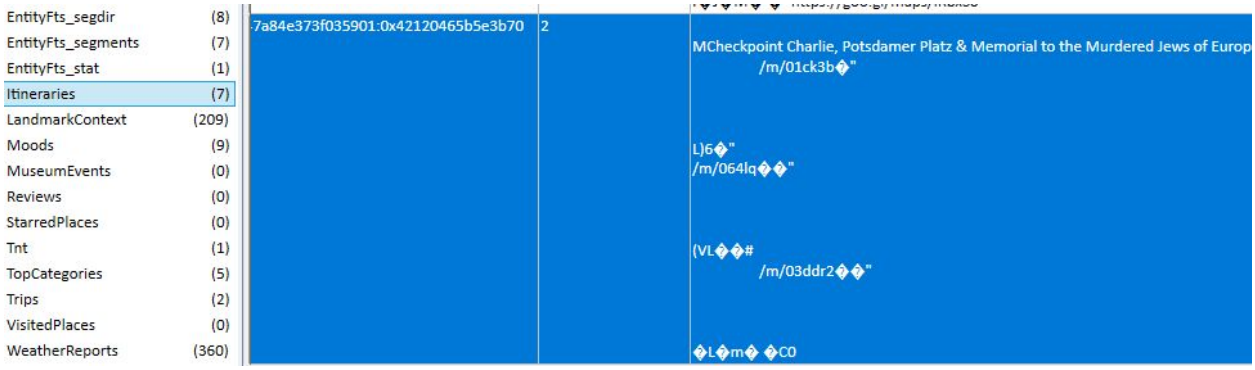


CategoryFts_content	(973)
CategoryFts_docsize	(973)
CategoryFts_segdir	(27)
CategoryFts_segments	(9)
CategoryFts_stat	(1)
ConstellationLists	(3)
ConstellationPOIs	(13)
CuratedMoods	(1)
DestinationEntities	(349)
DestinationMetadata	(266)
Destinations	(2)
DismissedItems	(0)
DownloadWebPageJobsTable	(0)
EntityData	(349)
EntityFts_content	(267)
EntityFts_docsize	(267)
EntityFts_segdir	(8)
EntityFts_segments	(7)
EntityFts_stat	(1)
Itineraries	(7)
LandmarkContext	(209)
Moods	(9)
MuseumEvents	(0)
Reviews	(0)
StarredPlaces	(0)
Tnt	(1)
TopCategories	(5)
Trips	(2)
VisitedPlaces	(0)
WeatherReports	(360)
android_metadata	(1)
sqlite_sequence	(5)

docid	c0Mid	c1Name
266	/g/1hc4npdly	Fleamarket at Mauerpark
267	/cid/2799411498522453192	Bücherbogen am Savignyplatz GmbH
268	/m/0d0dct	Bode Museum
269	/m/0cmchjb	Allied Museum
270	/m/0bn_y2	Orangery Palace
271	/m/01ck3b	Checkpoint Charlie
272	/g/12215hdd	Lustgarten
273	/m/04n6ct_	Mauerpark
274	/m/05f4837	Köpenick Palace
275	/g/11xxqbzky	Spreepark
276	/m/0czdm7n	Gardens of the World
277	/cid/3589837278406511977	House of Weekend
278	/cid/17000852869149131811	Tresor Night Club
279	/g/11cjnl0gr9	Science Center Spectrum
280	/g/122qx_96	MACHmit! Museum for Children
281	/m/0gg5bnl	Computerspiele Museum
282	/m/01fw0g	Reichstag Building
283	/m/064m56g	Biosphäre Potsdam
284	/g/11dynwx872	Insider Tour
285	/m/0bsrzt	Sanssouci Picture Gallery
286	/m/0dgq19l	Museum of Decorative Arts
287	/g/11dxs2t53s	Little BIG City Berlin
288	/g/1tyktdny	Teufelsberg
289	/m/0j43kbw	Prussian Palaces and Gardens Foundation Berlin-Brandenburg
290	/m/03c_s1	Bellevue Palace
291	/m/0dh626	Soviet War Memorial Tiergarten
292	/m/065x24p	House of the Wannsee Conference
293	/m/0crh1jg	Molecule Men
294	/m/059_y2x	Nuthe-Nieplitz Nature Park
295	/g/12116s0j	Kollhoff Tower
296	/m/05mszq3	Heiliger See
297	/m/0i3gdk3	St. Nicholas' Church, Potsdam

The Itineraries item is the list of day plans are presented by Google and ones that are made by the user. It contains the 3 destinations I chose for my day plan through Berlin. It contains information of the locations, MIDs, and sometimes a Google Maps link. However, this Google Maps link does not appear to work when typed in to a browser.

Figure 4: Itineraries Screenshot



LandmarkContext contains a list of MIDs and a column called LanmarkVisitDataProto. This could be a description of each landmark, but the text in UFED Cellebrite DB viewer cannot translate the text.

Moods contains a list of tabs that is inside the "Things to do" section of the trip. A screenshot of this section with the tabs is below. The item in the database contains the basics of the algorithm that will generate items and locations for you to visit and other parameters.

Figure 5: Showcase of the tiles the user can select on the phone. "Things to do" is the blue tile.

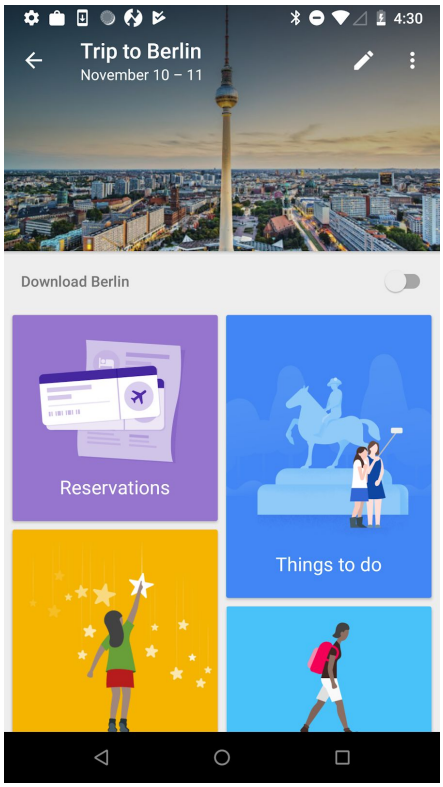


Figure 6: Screenshot showcasing the different selectable tabs in “Things to do".

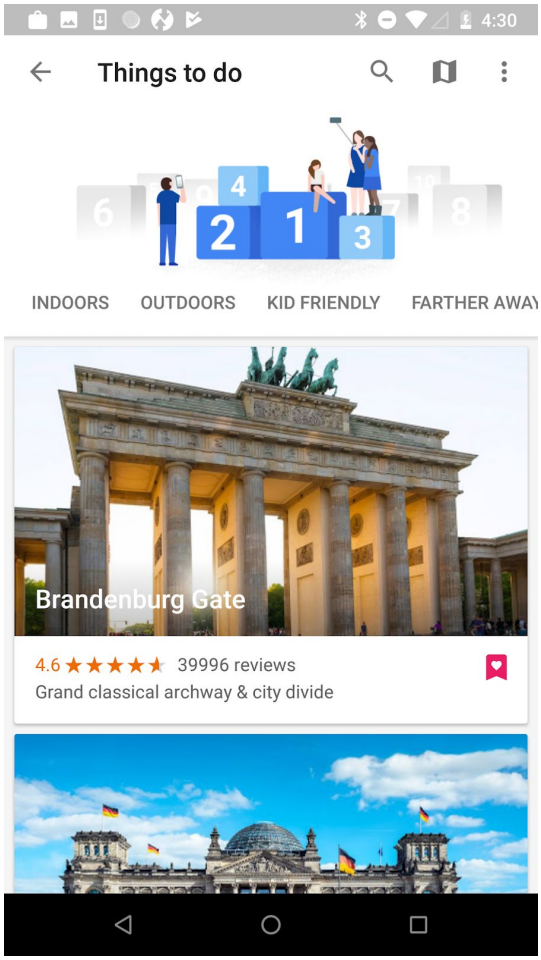
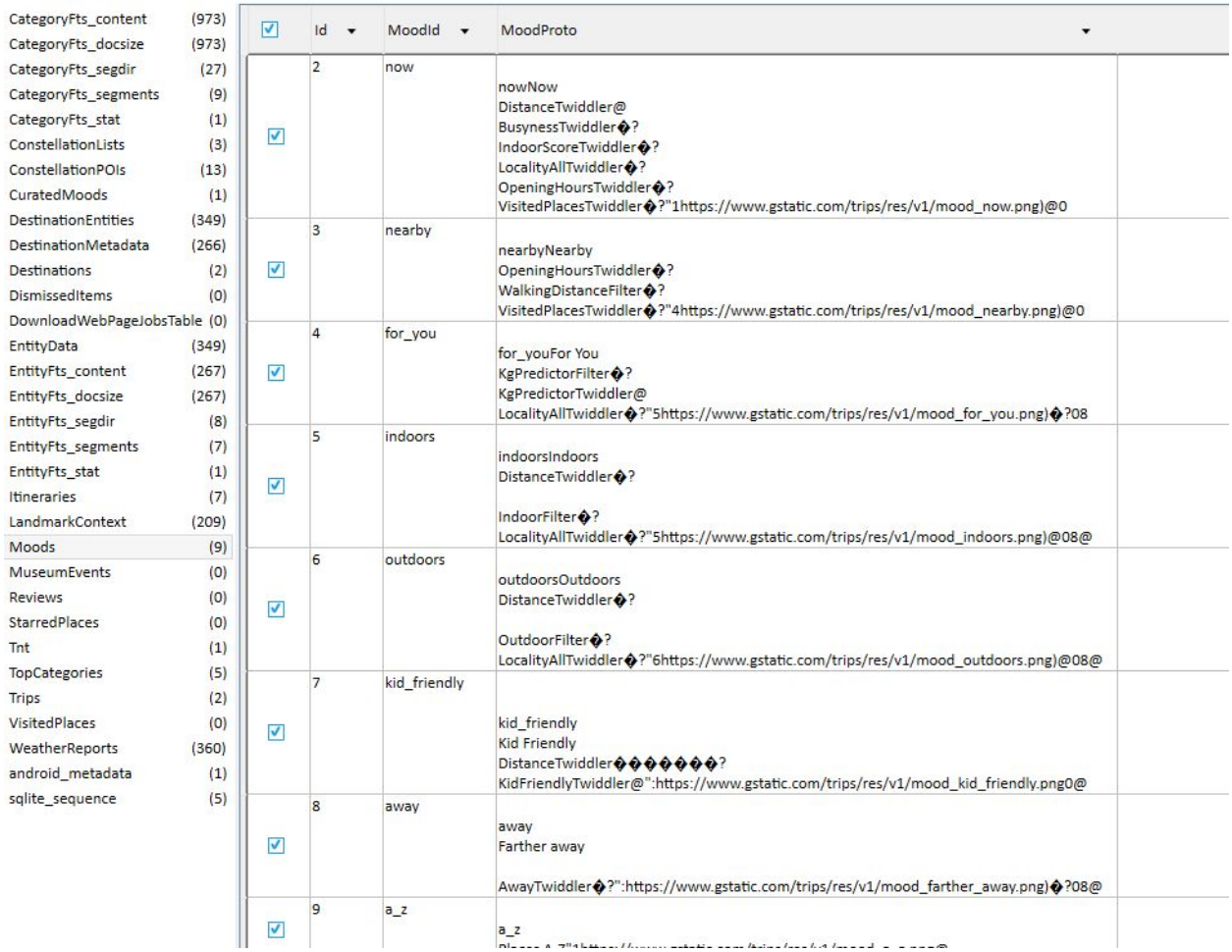


Figure 7: Moods Screenshot



CategoryFts_content	(973)
CategoryFts_docsize	(973)
CategoryFts_segdir	(27)
CategoryFts_segments	(9)
CategoryFts_stat	(1)
ConstellationLists	(3)
ConstellationPOIs	(13)
CuratedMoods	(1)
DestinationEntities	(349)
DestinationMetadata	(266)
Destinations	(2)
DismissedItems	(0)
DownloadWebPageJobsTable	(0)
EntityData	(349)
EntityFts_content	(267)
EntityFts_docsize	(267)
EntityFts_segdir	(8)
EntityFts_segments	(7)
EntityFts_stat	(1)
Itineraries	(7)
LandmarkContext	(209)
Moods	(9)
MuseumEvents	(0)
Reviews	(0)
StarredPlaces	(0)
Tnt	(1)
TopCategories	(5)
Trips	(2)
VisitedPlaces	(0)
WeatherReports	(360)
android_metadata	(1)
sqlite_sequence	(5)

Id	MoodId	MoodProto
2	now	nowNow DistanceTwiddler@ BusynessTwiddler IndoorScoreTwiddler LocalityAllTwiddler OpeningHoursTwiddler VisitedPlacesTwiddler"1https://www.gstatic.com/trips/res/v1/mood_now.png)@0
3	nearby	nearbyNearby OpeningHoursTwiddler WalkingDistanceFilter VisitedPlacesTwiddler"4https://www.gstatic.com/trips/res/v1/mood_nearby.png)@0
4	for_you	for_youFor You KgPredictorFilter KgPredictorTwiddler@ LocalityAllTwiddler"5https://www.gstatic.com/trips/res/v1/mood_for_you.png)?08
5	indoors	indoorsIndoors DistanceTwiddler IndoorFilter LocalityAllTwiddler"5https://www.gstatic.com/trips/res/v1/mood_indoors.png)@08@
6	outdoors	outdoorsOutdoors DistanceTwiddler OutdoorFilter LocalityAllTwiddler"6https://www.gstatic.com/trips/res/v1/mood_outdoors.png)@08@
7	kid_friendly	kid_friendly Kid Friendly DistanceTwiddler KidFriendlyTwiddler@":https://www.gstatic.com/trips/res/v1/mood_kid_friendly.png0@
8	away	away Farther away AwayTwiddler":https://www.gstatic.com/trips/res/v1/mood_farther_away.png)?08@
9	a_z	a_z

The Tnt item contains a description of the food in Berlin. This is under an MID. A screenshot of the location of the description in the app and the item in the DB viewer is below.

Figure 8: Screenshot showcasing an overview of the Food & Drink description for Berlin. This correlates with Tnt.

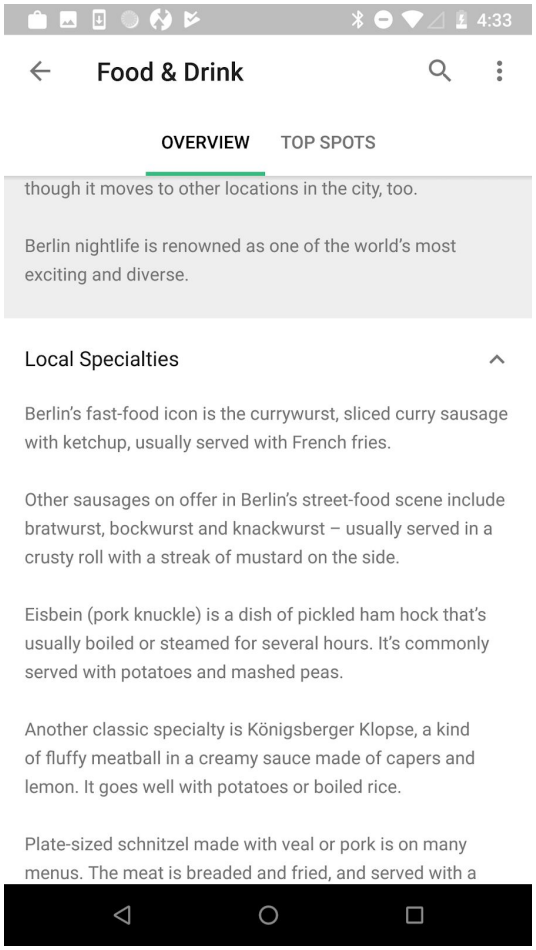
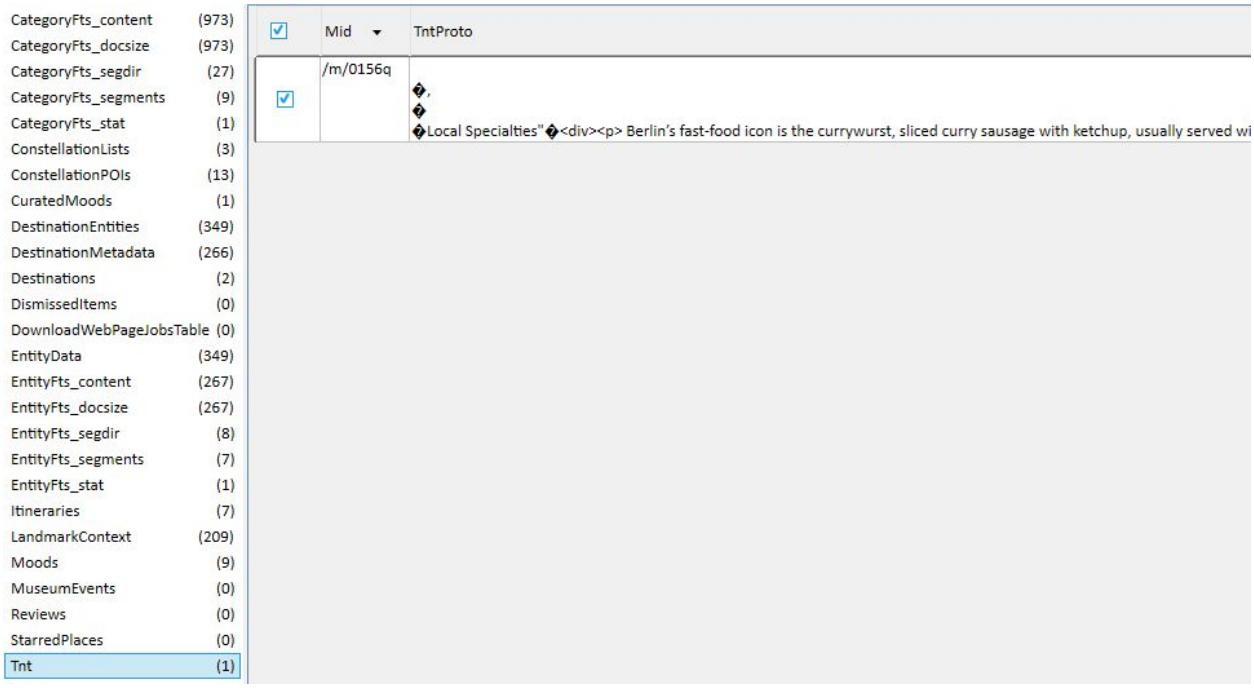
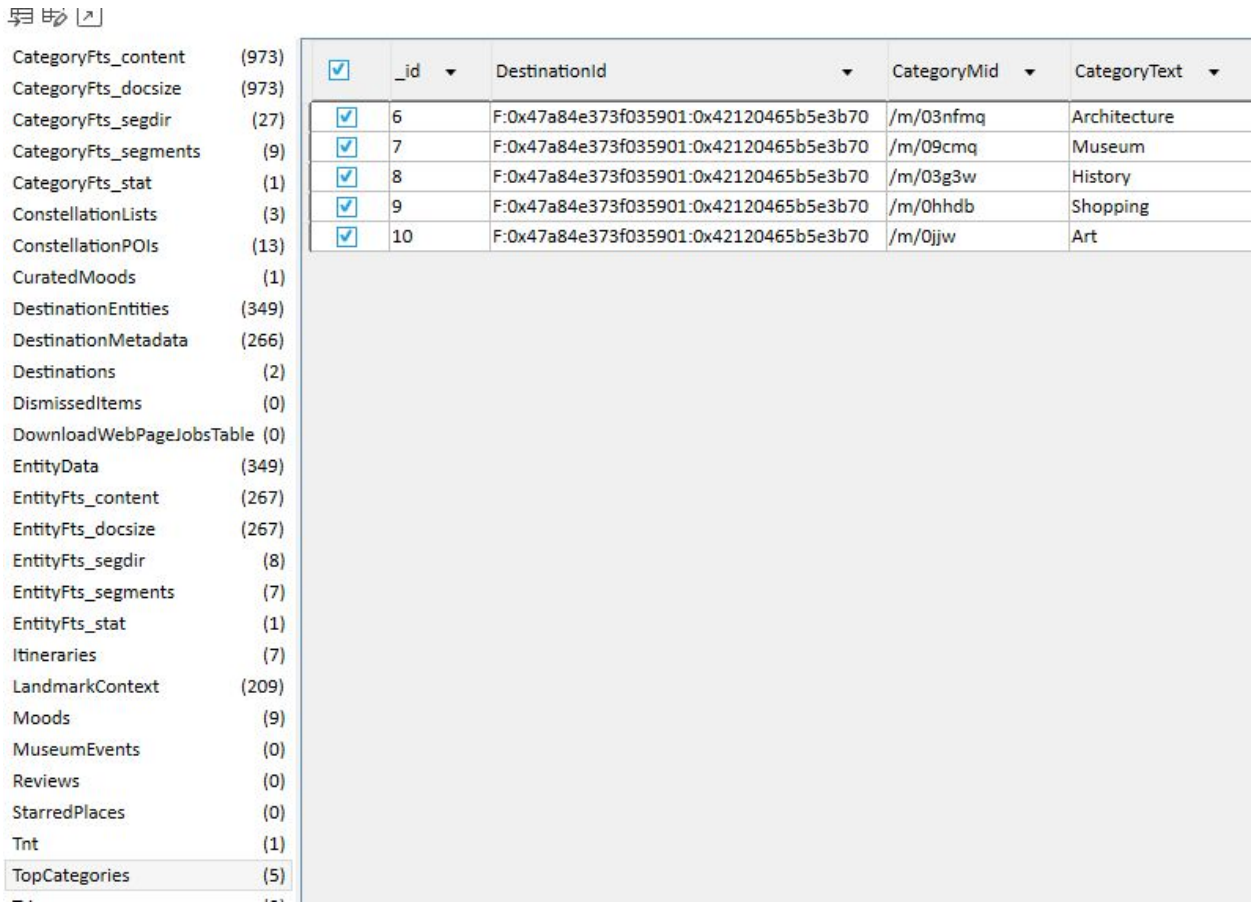


Figure 9: Tnt Screenshot



The TopCategories item contains a list of categories (Architecture, Museum, Shopping) for locations and the top 5 most recommended or viewed by the user. For this list, Architecture, Museum, History, Shopping, and Art are the top 5. This could be based on the saved places by the fact that all of them can be fit into at least 1 of these categories.

Figure 10: TopCategories Screenshot



The Trips item contains lots of detail regarding the trips the user has planned. This goes into more detail than Destinations. This is the only item that contains references to the reservations made. You can see the reservations made in the second row information below. There are two rows, only one of them being trips created by the user.

First Row:
_id: EPHEMERAL:F:0x47a84e373f035901:0x42120465b5e3b70
TripName: Berlin
StartDate: N/A
EndDate: N/A
TripStatus: 0
LastUpdateTimestamp: 1541106784682 (Thu, 01 November 2018 21:13:04.682 UTC)
TripProto:

Figure 11: Trip Proto First Row Screenshot

UserCreated: 0
IsEphemeral: 1

Second Row:
_id: Trip:5bda769e-0000-274d-98b9-f403043e9068
TripName: Trip to Berlin
StartDate: 1541808000000 (Sat, 10 November 2018 00:00:00.000 UTC)
EndDate: 1541894400000 (Sun, 11 November 2018 00:00:00.000 UTC)
TripStatus: 0
LastUpdateTimestamp: 1541107543756 (Thu, 01 November 2018 21:25:43.756 UTC)
TripProto:

Figure 12: TripProto Second Row Screenshot

UserCreated: 1
IsEphemeral: 0

The second row information from TripProto contains all of the reservations created, although with limited data. The confirmation number is even there, although hard to find. It is in between the Reservation ID number and the destination name.

WeatherReports possibly contains information about weather reports. There are a variety of weather reports listed, all including a DestinationId, ValidFrom timestamp, ValidUntil timestamp, and WeatherPleasantess. It should be apparent that weather is rated by pleasantness, which scales from 1 - 4. It could go to a limit of 4 because the weather in Berlin may not be pleasant at all, and I am unable to see if the limit goes higher. Taking the latest timestamp in the list, we can see a variety of data on how far the weather reports go into the future and how long each report lasts.
Timestamp: ValidFrom 1542398400000 and ValidUntil 1542402000000 with a pleasantness of 4.

The timestamps translate to:
ValidFrom: Fri, 16 November 2018 20:00:00.000 UTC
ValidUntil: Fri, 16 November 2018 21:00:00.000 UTC

As we can see, the weather reports last for 1 hour.

The first weather report row as sorted by timestamp starts at:
Thu, 01 November 2018 21:14:53.814 UTC
Based on the Data Generation timeline, this is when the trip was created. Therefore, the weather reports 15 days ahead.

Huawei H1511 Nexus 6P LCDI-5016

Google Trips Results

All under 'Guide_10891479499766246813 6.db'

DestinationID	CuratedMoodProto	LastUpdatedTimeStamp
F:0x132a56a680d2d6ad:0x93d57917efc72a03	? H GardensGardens"4https://www.gstatic.com/trips/res/v1/mood_unique.png /m/025pcj /m/02609zg /m/0ch3gv7 /m/0406v6p /m/05f5gy8 /g/122s95sm/cid/3940084649289042783 /g/11bvtbnn3_/cid/3790944124135236403 /m/0wxp_bx ? X Kid-friendly Kid-friendly":https://www.gstatic.com/trips/res/v1/mood_kid_friendly.png/cid/4342550643295199486	1541103426366

	/g/1v9nk774 /m/03m9bp9/cid/4402879251543680521/cid/16074805750548982422/cid/19762594344666642920/cid/11204713257590437495 /g/122s95sm /m/0wxp_bx ? X Local favoritesLocal favorites”4https://www.gstatic.com/trips/res/v1/mood_unique.png /m/02r020c /g/1238gdz1 /m/02r3pwf /m/03mdjr5 /g/12222442 /m/03hjch /m/06hthb /m/033dz2/cid/13931513850502124499 /m/047twj9 /m/05zq7rr /m/03m3w0t ? U Science museumsScience museums”1https://www.gstatic.com/trips/res/v1/mood_art.png /m/0bnsyp /m/0ccj86 /g/1238s76r /g/121bwbkl /g/1thn7mv9 /g/12z84m_9n /m/057bqn /m/0jkzhfx ? K Modern art Modern art”1https://www.gstatic....	

Under ConstellationPOIs, I found the places that I had starred while using Google Trips. I starred the Montreal Botanical Garden, Olympic Stadium, and Café Résonance. The last column is the Last Modification Time Stamp.

ListId	ListEntryProto	Synced	ForDeletion	LastModificationTimestamp
starred_places_list	/m/02v_n7 ``'`,'* /m/02v_n7Montreal Botanical Garden	1	0	1540936461145
starred_places_list	/m/02p3hm 5`'``(* /m/02p3hmOlympic Stadium	1	0	1540936461146
starred_places_list	/cid/11237377514764009247' z`!``!*/cid/11237377514764009247Café Résonance	1	0	1540936461147
starred_places_list	/m/0446t_ T`e``* /m/0446t_Palazzo Vecchio	1	0	1541104260773

ListID	ListEntryProto	LastUpdatedTimeStamp
starred_places_list	/m/02v_n7 ??'?,'?* /m/02v_n7Montreal Botanical Garden	1540936461145
starred_places_list	/m/02p3hm 5?'??(?* /m/02p3hmOlympic Stadium	1540936461146
starred_places_list	/cid/11237377514764009247' z?!??!?*/cid/11237377514764009247Café Résonance	1540936461147

Found this and the name of the town hall Palazzo Vecchio which corresponds to what I put in Day plans and in Favorites, Want to go, and Starred Places in Hex View.

```
.....
.....-._.Trip:5bd72fe8-0000-2
aba-9d12-2405886ca488.4.o.EPHEMERAL:F:0x132a56a680d2d6a
d:0x93d57917efc72a03.....|.l.....(.f...5.....
ra.....riginally.....palazzo.....
.....eontology.....sso.....ecci.....
```

EntityData is the description of each MID and reveals insight as to what ID correlates to what location. It includes the Mid, EntityProto, RatingHistogram, IsAttraction, DetailLevel, LastUpdateTimestamp.

Mid	EntityProto	LastUpdatedTime Stamp
/m/01g82f	/m/01g82f"Cathedral of Santa Maria del Fiore? ?Florence Cathedral, formally the Cattedrale di Santa Maria del Fiore, is the cathedral of Florence, Italy. It was begun in 1296 in the Gothic style to a design of Arnolfo di Cambio and was structurally completed by 1436, with the dome designed by Filippo Brunelleschi. The exterior of the basilica is faced with polychrome marble panels in various shades of green and pink, bordered by white, and has an elaborate 19th-century Gothic Revival façade by Emilio De Fabris. The cathedral complex, in Piazza del Duomo, includes the Baptistery and Giotto's Campanile. These three buildings are part of the UNESCO World Heritage Site covering the historic centre of Florence and are a major tourist attraction of Tuscany. The basilica is one of Italy's largest churches, and until the development of new structural materials in the modern era, the dome was the largest in the world. It remains the largest brick dome ever constructed. The cathedral is ...	1541104206286
/m/068wp	/m/068wp Ponte Vecchio? ?The Ponte Vecchio is a medieval stone closed-spandrel segmental arch bridge over the Arno River, in Florence, Italy, noted for still having shops built along it, as was once common. Butchers initially occupied the shops; the present tenants are jewelers, art dealers and souvenir sellers. The Ponte Vecchio's two neighbouring bridges are the Ponte Santa Trinita and the Ponte alle Grazie."(Medieval stone bridge with jewelry shops)"?	

I found the place Cathedral of Santa Maria del Fiore which was in Things to do category under Entity Data. This was selected in Google Trips at 4:22 pm on November 1st, 2018. Cathedral of Santa Maria del Fiore was

selected in Google Trips at 4:28 pm under the category Days Plan on November 1st, 2018. In addition, I found Ponte Vecchio and Palazzo Vecchio which are places I put under Day Plans in Google Trips.

/m/0446t_	/m/0446t_Palazzo Vecchio The Palazzo Vecchio is the town hall of Florence, Italy. It overlooks the Piazza d Originally called the Palazzo della Signoria, after the Signoria of Florence, the ruli palace during its long history. The building acquired its current name when the M T e O x T* W T + ! W T + * /m/0446t_ Europe/Rome2 [http://t0.gstatic.com/images?q=tbn:ANd9GcT4rqGCAqJGNdbzIW2vNQbYUWyX
/m/068wp	/m/068wp Ponte Vecchio The Ponte Vecchio is a medieval stone closed-spandrel segmental arch bridge dealers and souvenir sellers. The Ponte Vecchio's two neighbouring bridges are t t W T X g V* 0 1@! 0 1@*/m/068wp2&Ponte Vecchio, 50125 Firenze FI, ItalyjITr Europe/Rome2 [http://t3.gstatic.com/images?q=tbn:ANd9GcTFMoawQWCdOxxHNhgeFa7zUhH DFgUZl5MvyibsdrR2IbmWTXbGPO2f9CeceXiyYrhz8YPBmT2GuTOMo9gli_o7Uvir d0jvEkoZunUI-D4i64KvpaN3swI6c9r...

/m/068wp

/m/068wp
Ponte Vecchio
The Ponte Vecchio is a medieval stone closed-spandrel segmental arch bridge over the Arno River, in Florence, Italy, noted for still having shops built along it, as was once common. Butchers initially occupied the shops; the present tenants are jewelers, art dealers and souvenir sellers. The Ponte Vecchio's two neighbouring bridges are the Ponte Santa Trinita and the Ponte alle Grazie."(Medieval stone bridge with jewelry shops"

t

W T

X g V* 0
1@! 0
1@*/m/068wp2&Ponte Vecchio, 50125 Firenze FI, ItalyjiTr
Europe/Rome2
[http://t3.gstatic.com/images?q=tbn:ANd9GcTFMoawQWCdOxxHNhgeFa7zUhHdv9DN4bsxLxAhLtjGRLZaQBxX https://lh3.googleusercontent.com/proxy/gwsOf7j6yk8od--DFgUZl5MvyibsdrR2IbmWTXbGPO2f9CeceXiyYrhz8YPBmT2GuTOMo9gli_o7UvirUrcixmBRQ2sEROok24dLKcHZImqB0rj-0MKjTdiL9vdgeqqiltX_F9dvmOUSFig8 l@@@2https://lh5.googleusercontent.com/-cZaPuKC3aWE/WjLLNH2LgoI/AAAAAAABFo8/d0jvEkoZunUI-D4i64KvpaN3swI6c9r...

1541104136086

/m/01g82f

/m/01g82f"Cathedral of Santa Maria del Fiore

Florence Cathedral, formally the Cattedrale di Santa Maria del Fiore, is the cathedral of Florence, Italy. It was begun in 1296 in the Gothic style to a design of Arnolfo di Cambio and was structurally completed by 1436, with the dome designed by Filippo Brunelleschi. The exterior of the basilica is faced with polychrome marble panels in various shades of green and pink, bordered by white, and has an elaborate 19th-century Gothic Revival façade by Emilio De Fabris.

The cathedral complex, in Piazza del Duomo, includes the Baptistery and Giotto's Campanile. These three buildings are part of the UNESCO World Heritage Site covering the historic centre of Florence and are a major tourist attraction of Tuscany. The basilica is one of Italy's largest churches, and until the development of new structural materials in the modern era, the dome was the largest in the world. It remains the largest brick dome ever constructed.

The cathedral is ...

1541104206286

The last item is further expanded under EntityFts_content. This provides 3 columns, docid, c0Mid, and c1Name. This is an extremely useful item in that it provides the exact name of each location along with their correlating MID.

The Academy of Florence Art Gallery was one of my places to go in Florence, Italy under Day Plans 4:28 pm 72 hours in Florence Day 1.

	docid	c0Mid	c1Name
☑	750	/m/0w196y8	Academy Of Florence Art Gallery

The Itineraries item is the list of day plans that are presented by Google, and ones that are made by the user. It contains the 3 destinations I chose for my day plan in Florence, Italy. It contains information on the locations, MIDs, and sometimes a Google Maps link. However, this Google Maps link does not appear to work when typed into a browser.

Itineraries	(6)
LandmarkContext	(142)
Moods	(9)
MuseumEvents	(0)

DestinationId	CreationType	ItineraryProto	LastUpdateTimestamp
F:0x132a56a680d2d6ad:0x93d57917efc72a03	1	72 hours in Florence: Day 1`A full day encompassing the masterpieces of the Uffizi, the iconic duomo & Michelangelo's David. /m/068wp /m/0cfjp /m/07qj_l /m/0446t_ /m/03352s /m/099xrq /m/01g82f /m/0w196y8 https://goo.gl/maps/tjvvE0	1541104040179

DestinationId	CreationType	ItineraryProto	LastUpdateTimestamp
F:0x132a56a680d2d6ad:0x93d57917efc72a03	1	72 hours in Florence: Day 2RA day exploring top sights on both sides of the Arno, including a famed city view. /m/0345mr /m/05lh8w /m/0dg3r0 /m/025pcj /m/044bh6 /m/03hqjz /m/0415qbd	1541104040179

DestinationId	CreationType	ItineraryProto	LastUpdateTimestamp
F:0x132a56a680d2d6ad:0x93d57917efc72a03	1	72 hours in Florence: Day 3aA day of art-filled churches & museums & an afternoon trip to the panoramic hill town of Fiesole. /m/01fsd9\ufffd" \ufffdz#\ufffd\ufffd& /g/1hc561k3g\ufffd\ufffd" \ufffd\ufffduF\ufffd" /m/01fsgd\ufffdU" R\ufffd\ufffd`\ufffd$ /m/07s4mg6\ufffd\ufffd" \ufffdd\ufffd# /m/03hr8n\ufffd \ufffd" s\ufffd\ufffd4\ufffd# /m/05_5tc1\ufffd" \ufffd\ufffd\ufffd!\ufffd$ /m/0272rmj\ufffd\ufffd" \ufffd\ufffd% /g/121qgf8h\ufffd\ufffd"	1541104040179

When I clicked on Passwords, under User Accounts I found my fake gmail address pop up seven times and the fake name I made pop up two times.

Name	Username
	mattcauliflower456@gmail.com
	mattcauliflower456@gmail.com
	mattcauliflower456@gmail.com
	mattcauliflower456@gmail.com
	mattcauliflower456@gmail.com
matt cauliflower	
matt cauliflower	mattcauliflower456@gmail.com
mattcauliflower456@gmail.com	1540928735212

Conclusion

Google Trips keeps lots of data on its device. In fact, it can be argued that it keeps all trip data on the database. There were some things missing from the database, mainly descriptions and information about Berlin that is contained in the 'Need to know' section. This section contains emergency info, etiquette, and more. Despite this, it contains almost all aspects of the trip that was created. This includes reservations, saved places, and day plans. A forensic investigator could easily track down when and where a person could be if they got ahold of this data.

Further Work

It would be interesting to study Google's ID system. There seems to be an order to things, and being able to tell the difference between CID, M, and G MIDs would be beneficial.

Appendix

Google Trips Data Generation Nexus 7 K009

Table 6: FLIGHT

Title	Flight #	From	Destination	Departure Time/Date	Arrival Time/Date	Confirmation #	Creation Timestamp
Delta	100	JFK, US	Berlin, Brandenberg	November 20, 2018 at 10:00 AM	November 20, 2018 at 1:00 PM	123	4:16 PM 10/30/2018

Table 7: HOTEL

Title	Flight #	From	Destination	Departure Time/Date	Arrival Time/Date	Confirmation #	Creation Timestamp
Hotel deRome	100	JFK, US	Berlin, Brandenberg	November 20, 2018 at 10:00 AM	November 20, 2018 at 1:00 PM	123	4:28 PM 10/30/2018

Table 8: TRAIN

Title	From	Destination	Departure Time/Date	Arrival Time/Date	Passenger	Confirmation #	CreationTimestamp
Amtrak	S Ostbahnhof (Berlin)	Hamburg Central Station	November 20, 2018 at 04:00 PM	November 21, 2018 at 06:00 PM	Hope Kaiya	321	4:34 PM 10/30/2018

Table 9: BUS

Title	From	Destination	Departure Time/Date	Arrival Time/Date	Confirmation #	Creation Timestamp
FlixBus	Berlin Central Station	U Stadtmitte	November 20, 2018 at 05:00 PM	November 21, 2018 at 07:00 PM	321	4:40 PM 10/30/2018

Table 10: CAR RENTAL

Title	Phone Number:	Pick-Up Location	Pick Up Time/Date	Confirmation #	Car Type	Creation Timestamp
Sixt Autovermietung	+49 180 6 666666	Berlin, Germany	November 20, 04:00 PM	321	Compact	4:47 PM 10/30/2018

Table 11: RESTAURANT

Title	Phone Number:	Address	Date	Departure Time/Date	Confirmation #	Number of Guests	Creation Timestamp
Subway	+49 30 25321 975	Alte Potsdamer Straße, Berlin, Germany	November 21, 2018	November 20, 2018 at 02:00 PM	321	1	4:52 PM 10/30/2018

Table 12: FAVORITES

Title	Address	Creation Timestamp
Brandenburg Gate	Pariser Platz, 10117, Berlin, Germany	4:54 PM 10/30/2018
Reichstag	Platz der Republik 1, 11011, Berlin, Germany	4:54 PM 10/30/2018

Table 13: WANT TO GO

Title	Address	Creation Timestamp
Museum Island	Museum Island, Berlin, Germany	4:55 PM 10/30/2018
Alexanderplatz	10178 Berlin, Germany	4:55 PM 10/30/2018

Table 14: STARRED PLACES

Title	Address	Creation Timestamp
Checkpoint Charlie	Fredrichstraße 42-45, 10117	4:55 PM 10/30/2018

Potsdamer Platz	Potsdamer Platz, 10798 Berlin, Germany	4:55 PM 10/30/2018

Table 15: DAY PLANS: "KID FRIENDLY ATTRACTIONS"

Title	Address	Creation Timestamp
Zoo Berlin	Hardenbergplatz 8, 10787 Berlin, Germany	5:04 PM 10/30/2018
Aquadom & SEA LIFE Berlin	Spandauer Str, 3, 10178 Berlin, Germany	5:04 PM 10/30/2018
German Museum of Technology	Trebbiner Str. 9, 10963 Berlin, Germany	5:04 PM 10/30/2018

The team left "feedback" for Google Trips at **4:17 PM 10/30/2018:**

- "Very Cool!"

Google Trips Data Generation Huawei Nexus 6p LCDI-5017

All events take place on 11/1/2018
App Downloaded at 5:09
App First opened at 5:12
Trip created at 5:14

Table 16: FLIGHT

Title	Flight #	From	Destination	Departure Time/Date	Arrival Time/Date	Confirmation #	Creation Timestamp
Delta	100	JFK, US	Berlin, Brandenberg	November 10, 2018 at 6:00 AM	November 10, 2018 at 12:00 PM	123	5:16 PM

Table 17: HOTEL

Title	Address	Check In	Check Out	Confirmation Number	Phone Number	Creation Timestamp
Hotel de Rome	Behrenstraße, Berlin, Germany	Saturday November 10, 2018	Sunday, November 11, 2018	321	+49 30 4606090	5:17 PM

Table 18: TRAIN

Title	From	Destination	Departure Time/Date	Arrival Time/Date	Passenger	Confirmation #	Creation Timestamp
Amtrak	S Ostbahnhof (Berlin)	Hamburg Central Station	November 10, 2018 at 4:00 PM	November 10, 2018 at 06:00 PM	Leviticus Cornwall	321	5:19 PM

Table 19: BUS

Title	From	Destination	Departure Time/Date	Arrival Time/Date	Passenger	Confirmation #	Creation Timestamp
N/A	Berlin Central Station	U Stadtmitte	November 10, 2018 at 05:00 PM	November 10, 2018 at 07:00 PM	Leviticus Cornwall	321	5:21 PM

Table 20: CAR RENTAL

Title	Phone Number:	Pick-Up/Drop-Off Location	Pick Up Time/Date	Dropoff Time/Date	Confirmation #	Car Type	Creation Timestamp
Sixt Autovermietung	+49 180 6 666666	Berlin, Germany	November 10, 04:00 PM	November 11, 2018 at 04:00 PM	321	Compact	5:23 PM

Table 21: RESTAURANT

Title	Phone Number	Address	Date/Time	Confirmation #	Number of Guests	Creation Timestamp
Subway	+49 30 25321975	Alte Potsdamer Straße, Berlin, Germany	November 10, 2018, 02:00 PM	321	1	5:25 PM

Table 22: FAVORITES

Title	Address	Creation Timestamp
Brandenburg Gate	Pariser Platz, 10117, Berlin, Germany	5:26 PM
Reichstag	Platz der Republik 1, 11011, Berlin, Germany	5:26 PM

Table 23: WANT TO GO

Title	Address	Creation Timestamp
Museum Island	Museum Island, Berlin, Germany	5:26 PM
Alexanderplatz	10178 Berlin, Germany	5:26 PM

Table 24: STARRED PLACES

Title	Address	Creation Timestamp
Checkpoint Charlie	Fredrichstraße 42-45, 10117	5:26 PM
Potsdamer Platz	Potsdamer Platz, 10798 Berlin, Germany	5:26 PM

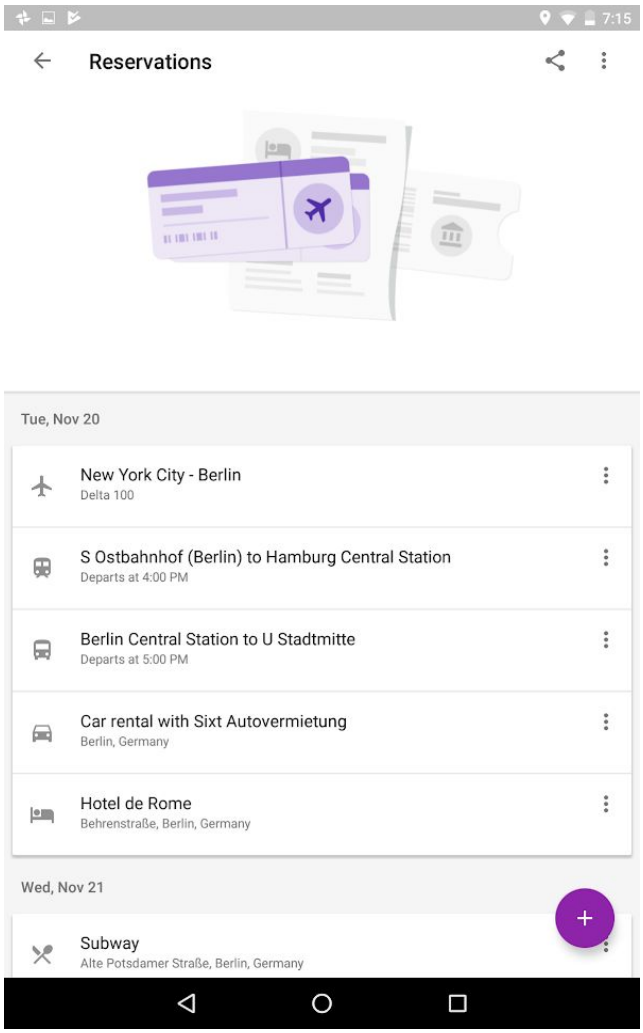
Table 25: DAY PLANS

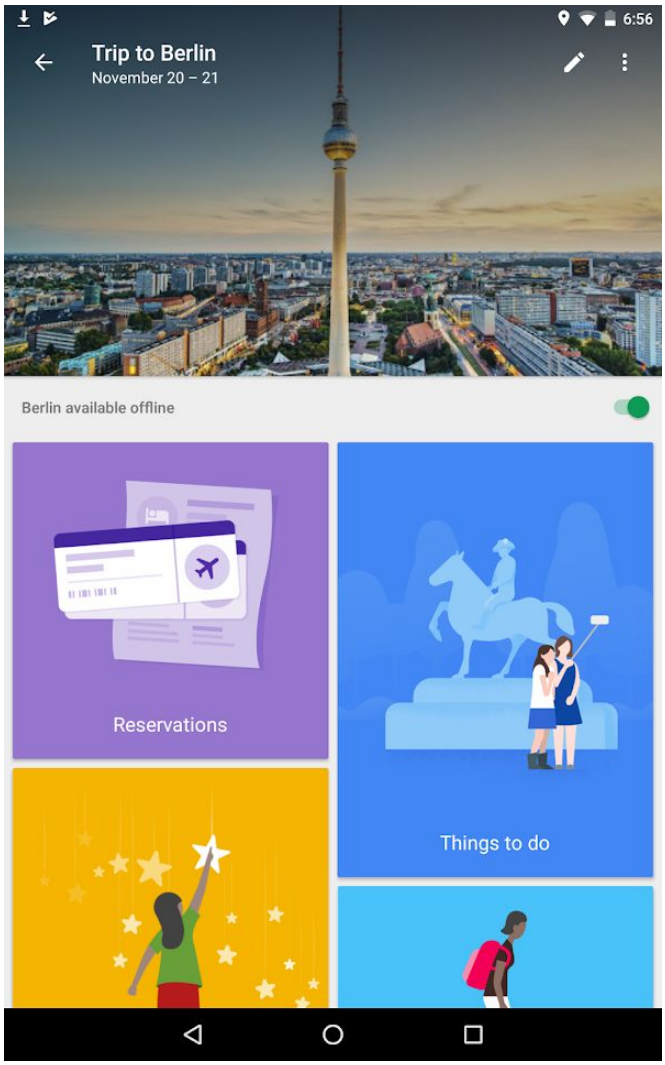
Title	Address	Creation Timestamp
Checkpoint Charlie	Fredrichstraße 42-45, 10117	5:27 PM
Potsdamer Platz	Potsdamer Platz, 10798 Berlin, Germany	5:27 PM
Memorial to the Murdered Jews of Europe	Cora-Berliner-Straße 1, 10117	5:27 PM

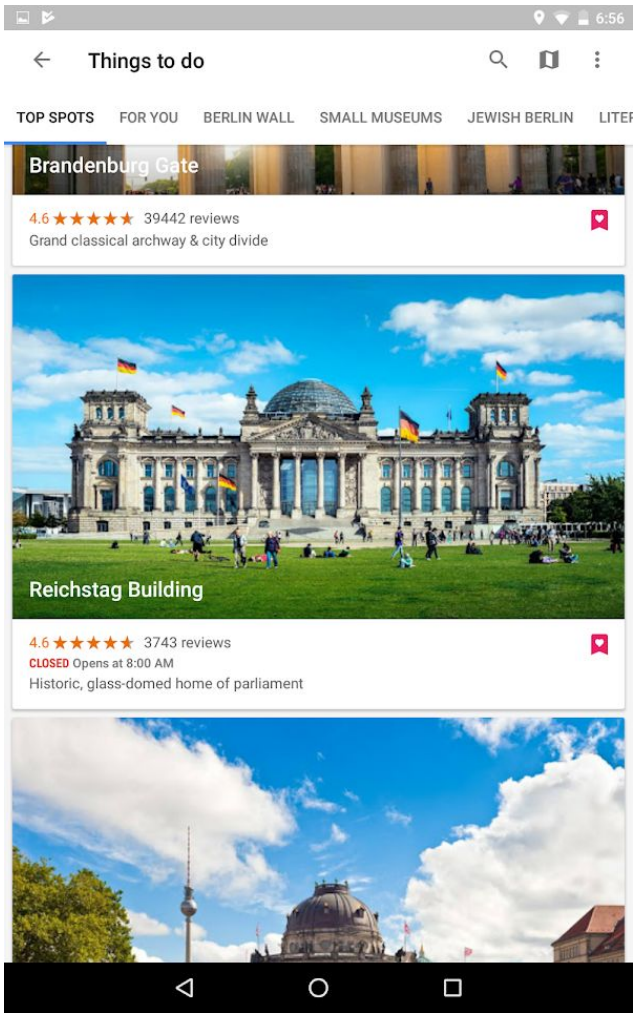
The team left “feedback” for Google Trips at **5:32 PM**

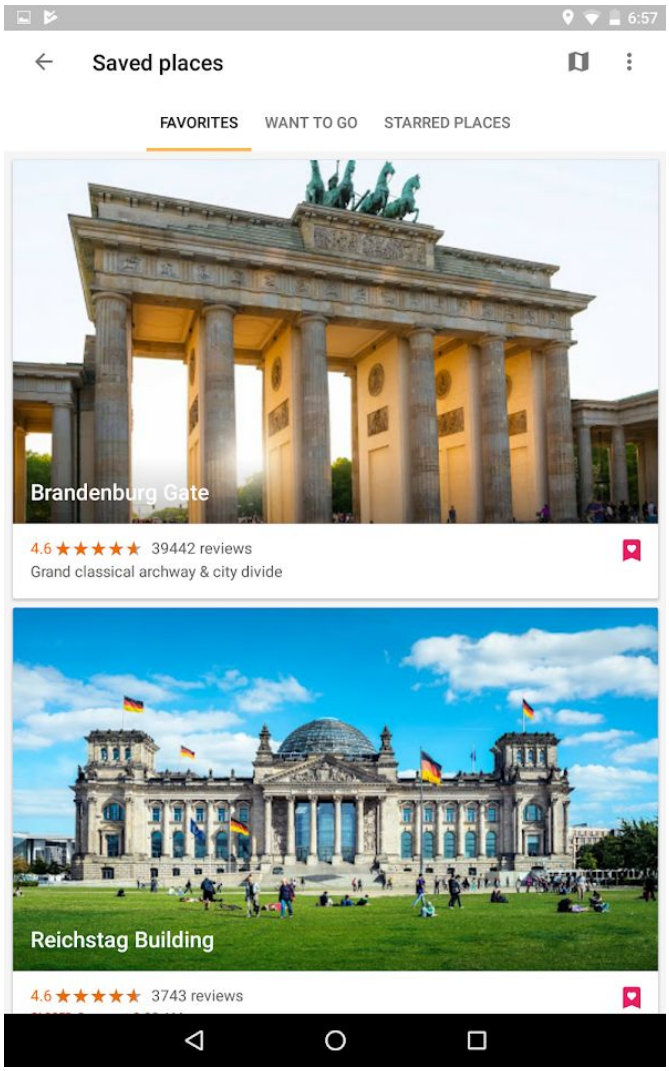
- “Very Cool!”

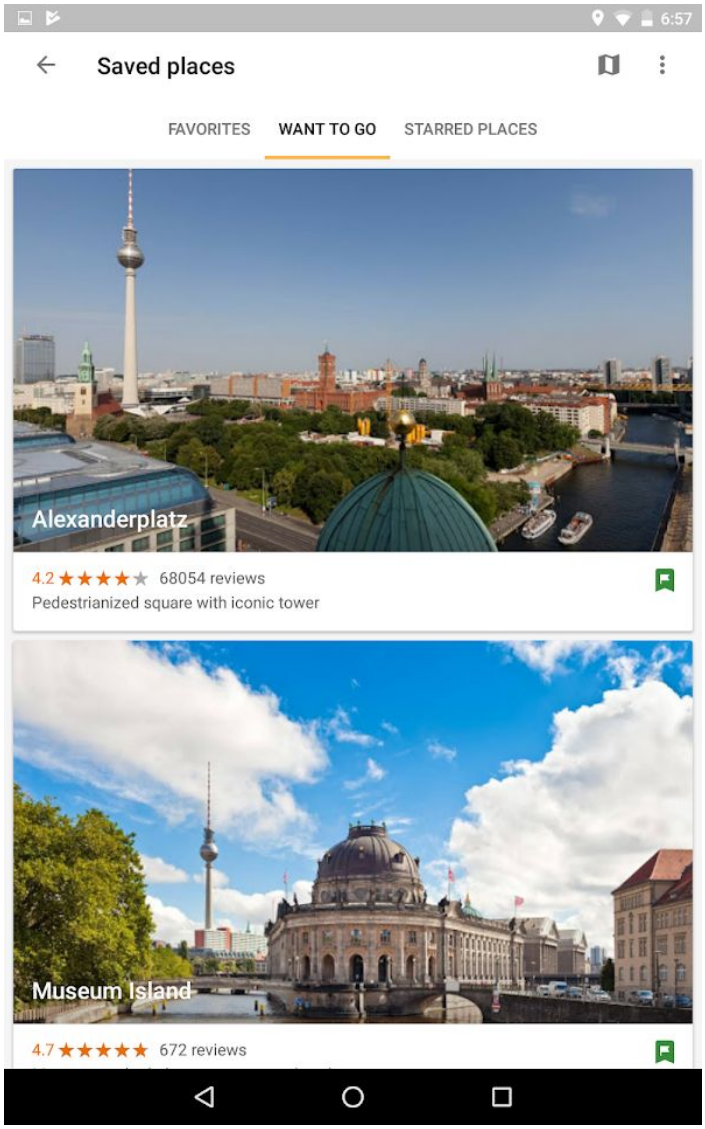
Google Trips Screenshots Nexus 7 K009

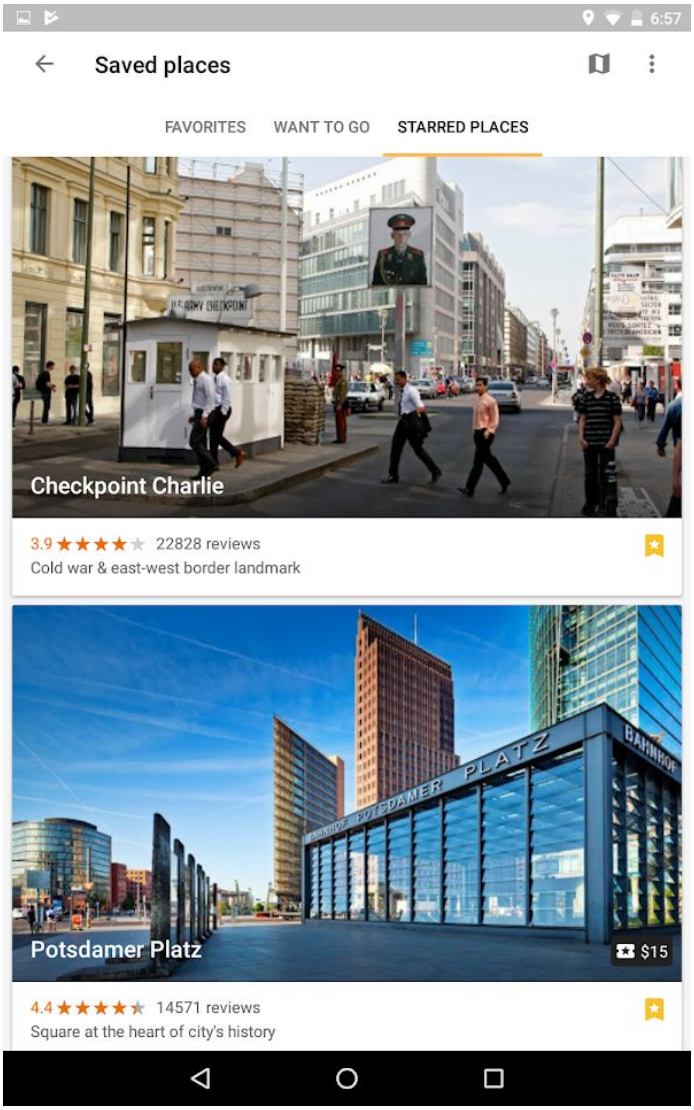



6:56
Trip to Berlin
November 20 – 21
Berlin available offline
Reservations
Things to do


6:56
Things to do
TOP SPOTS
FOR YOU
BERLIN WALL
SMALL MUSEUMS
JEWISH BERLIN
Brandenburg Gate
4.6 39442 reviews
Grand classical archway & city divide
Reichstag Building
4.6 3743 reviews
CLOSED Opens at 8:00 AM
Historic, glass-domed home of parliament


6:57
Saved places
FAVORITES
WANT TO GO
STARRED PLACES
Brandenburg Gate
4.6 ★★★★★ 39442 reviews
Grand classical archway & city divide
Reichstag Building
4.6 ★★★★★ 3743 reviews


6:57
Saved places
FAVORITES
WANT TO GO
STARRED PLACES
Alexanderplatz
4.2 68054 reviews
Pedestrianized square with iconic tower
Museum Island
4.7 672 reviews


6:57
Saved places
FAVORITES
WANT TO GO
STARRED PLACES
Checkpoint Charlie
3.9 22828 reviews
Cold war & east-west border landmark
Potsdamer Platz
$15
4.4 14571 reviews
Square at the heart of city's history

Google Trips Data Generation Huawei Nexus 6P LCDI-5016

Google Trips Results
DATES: 10/30/18 - 11/1/18
Time and Date Entered in App: 10/30/18 5:42 pm

Table 26: Flight

Title	Flight #	From	Destination	Departure Time/Date	Arrival Time/Date	Confirmation #	Creation Timestamp
American Airlines	5226	JFK	Florence (FLR)	Tuesday Nov. 20 4:00 pm	Wednesday Nov. 21 6:00 pm	4356	October 30, 2018 5:42 pm

Time and Date Entered in App: 10/30/18 5:43 pm

Table 27: HOTEL

Title	Address	Check In	Check Out	Confirmation Number	Phone Number	Creation Timestamp
Hotel Club Florence	Via Santa Caterina da Siena, Florence, Metropolitan City of Florence, Italy	Nov. 20	Nov. 27	6426	+39 055 217707	October 30, 2018 5:43 pm

Time and Date Entered in App: 10/30/18 5:46 pm

Table 28: Car Rental

Title	Phone Number:	Pick-Up/Drop-Off Location	Pick Up Time/Date	Dropoff Time/Date	Confirmation #	Car Type	Creation Timestamp
Rental car center, Florence Airport, Peretola, Italy	No phone number	Via Palagio degli Spini, Florence, Metropolitan City of Florence, Italy	Tuesday Nov. 20 4:00 pm	Tuesday Nov. 27 4:00 pm	9305	Infiniti Q30 Midsize	October 30, 2018 5:46 pm

Table 29: Restaurant

Title	Phone Number	Address	Number of Guests	Creation Timestamp
Enoteca Pinchiorri	+39 055 242757	Via Ghibellina, 87, 50122 Firenze Fl, Italy	1	October 30, 2018 5:55 pm

Table 30: FAVORITES

Title	Address	Creation Timestamp
Enoteca Pinchiorri	Via Ghibellina, 87, 50122 Firenze Fl, Italy	October 30, 2018 5:55 pm
Cathedral of Santa Maria del Fiore	Piazza del Duomo, 50122 Firenze FL, Italy	November 1, 2018 4:22 pm
Palazzo Vecchio	Piazza della Signoria, 50122 Firenze Fl, Italy	November 1, 2018 4:22 pm

Table 31: WANT TO GO

Title	Address	Creation Timestamp
Palazzo Vecchio	Piazza della Signoria, 50122 Firenze Fl, Italy	November 1, 2018 4:22 pm
Uffizi Gallery	Piazzale degli Uffizi, 6, 50122 Firenze Fl, Italy	November 1, 2018 4:22 pm

Table 32: STARRED PLACES

Title	Address	Creation Timestamp
Palazzo Vecchio	Piazza della Signoria, 50122 Firenze Fl, Italy	November 1, 2018 4:22 pm

Table 33: DAY PLANS 72 Hours in Florence Day 1

Title	Address	Creation Timestamp
Ponte Vecchio		November 1, 2018 4:28 pm
Uffizi Gallery		November 1, 2018 4:28 pm
Piazza della Signoria		November 1, 2018 4:28 pm
Palazzo Vecchio		November 1, 2018 4:28 pm
The Baptistery of St. John		November 1, 2018 4:28 pm
Giotto’s Bell Tower		November 1, 2018 4:28 pm

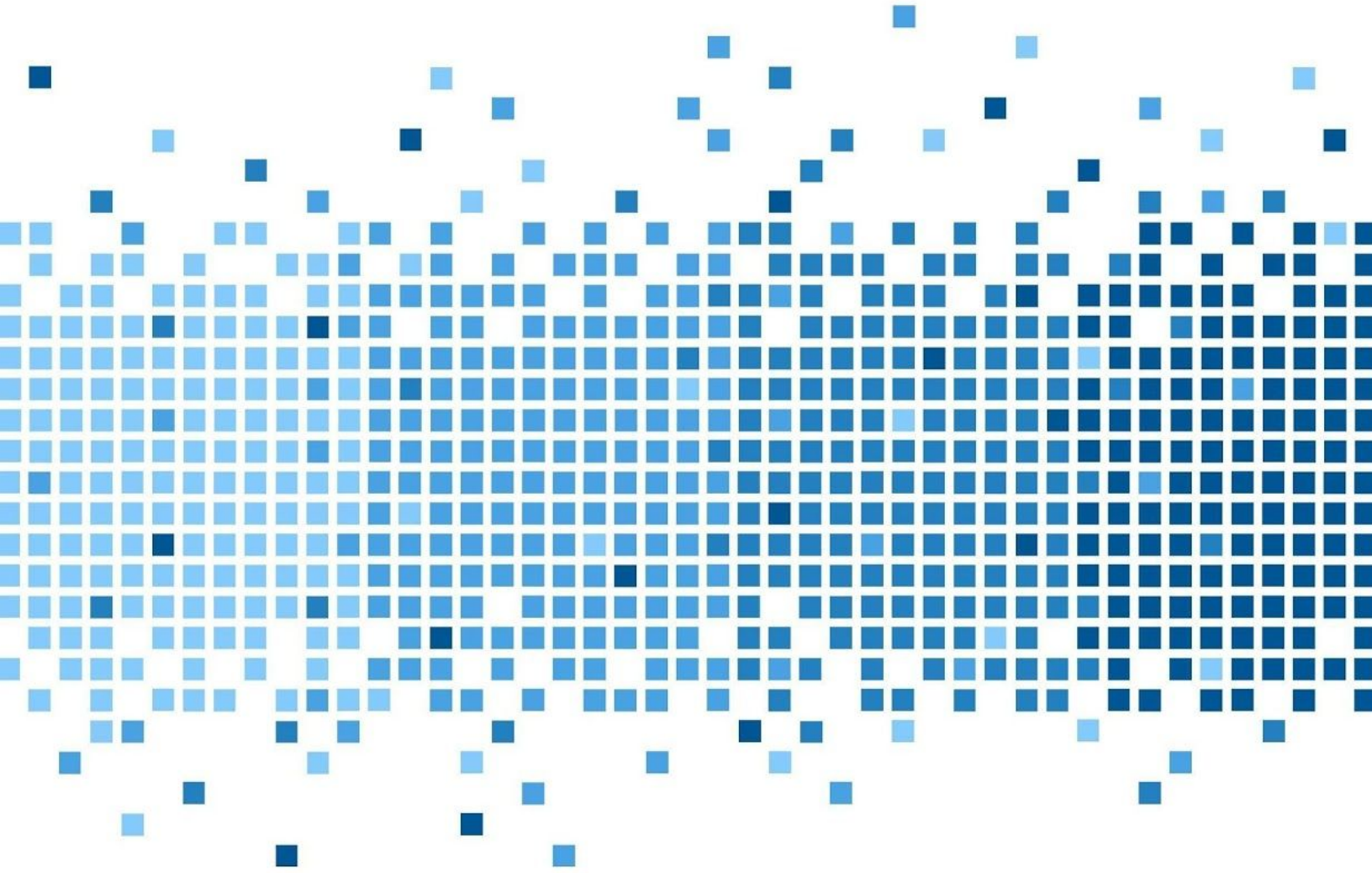
Cathedral of Santa Maria del Fiore		November 1, 2018 4:28 pm
Academy of Florence Art Gallery		November 1, 2018 4:28 pm

Feedback for Academy of Florence Art Gallery : Awesome trip! 4:31 pm

- "Awesome trip!"

CHAMPLAIN COLLEGE | LCDI Leahy Center for Digital Investigation

Kayak Mobile Forensics



175 Lakeside Ave, Room 300A
Burlington, Vermont 05401
Phone: (802)865-5744
Fax: (802)865-6446
http://www.lcdi.champlain.edu

12/14/2018

Disclaimer:

This document contains information based on research that has been gathered by employee(s) of The Senator Patrick Leahy Center for Digital Investigation (LCDI). The data contained in this project is submitted voluntarily and is unaudited. Every effort has been made by LCDI to assure the accuracy and reliability of the data contained in this report. However, LCDI and its employees make no representation, warranty or guarantee in connection with this report and hereby expressly disclaim any liability or responsibility for loss or damage resulting from use of this data. Information in this report can be downloaded and redistributed by any person or persons. Any redistribution must maintain the LCDI logo and any references from this report must be properly annotated.

Contents

Introduction

What data can be found in the Kayak mobile app? This report examines a travel application which is used to view, manage, and plan trips from one destination to another. The main question being asked here is: What data is stored on the phone that would be useful for a forensic analyst in the field? Being able to see where a person is planning to go could be invaluable as both evidence and seeing how they're planning their next move.

Background

This is the first part of a project to analyze mobile travel apps on Android. The goal of this project is to attempt to analyze these applications in order to provide forensic analysts with good documentation on what to look for when extracting these applications.

Purpose and Scope

The purpose of this data extraction is to address what user-generated data Kayak stores on the device it is installed on. One phone and two tablets were used as the Scope of this project. This is a mid-level analysis and, at the least, we will look for user-generated data such as: Trips, Watchlists, Usernames, and Passwords. We will not look for anything past user-generated data.

Research Questions

1. What data is stored on the phone by the app Kayak?
2. Why is the data stored on the device important to forensic analysts?

Terminology

ADB (Android Debugging Bridge)- ADB is a command line and client/server tool which allows for communication between the Android device and Developer. ADB can be used to install and debug apps, while also allowing user access to a Unix shell. This shell can be used to run a variety of useful commands on a device like 'push/pull'.

Allocated Space- An organized area of space in a device's storage containing user data and operating system. Only logical data extractions allow a user to obtain data from allocated space.

Bootloader- A small piece of code injected into RAM at start-up, allowing the flashing of firmware. However, for forensic analysts, this is a means of gaining access to user data, and then copying it.

Extraction- The process of obtaining mobile device data, then storing the data in an approved location to be processed after.

Physical Data Extraction- Accessing device data layers in unallocated and allocated space. Specifically, Cellebrite 4PC accesses three different groups of content within the data layers: logical, deleted content, and content the phone collects that is non-user generated. The user is able to view the collected data because 4PC creates a copy of the device's flash memory.

Rooting- Rooting an Android device is the act of an owner by-passing factory settings to gain 'root' or 'superuser' access which gives the owner administrative rights. Rooting an Android phone gives the owner access to the operating system.

SQLiteDatabase- Database file format commonly used for data storage of mobile and application data.

UFED Cellebrite 4PC- Cellebrite's UFED is extraction software designed to extract and analyze mobile device data. This includes cell phones and tablets. With 4PC the user has many options of data extraction, including but not limited to physical and logical data extractions. After the user chooses whichever data extraction they care for, they are able to analyze the extracted data with Physical Analyzer.

UFED Cellebrite Physical Analyzer (PA)- Cellebrite's Physical Analyzer is an application capable of analysis, decoding and reporting. PA offers a wide variety of variables to explore once extracted data has been loaded. The following are examples of what PA is capable of reporting: timeline graphs/details, device calls, texts, cookies, databases, files, instant messages, locations, and images. PA carves images and locations as well.

Unallocated Space- Area on a device's memory outside the defined file system available to be written to.

Methodology and Methods

There will be three mobile devices analyzed in this report: one Huawei Nexus 6P device and two Nexus 7 devices. The Nexus 6P device will run Android 8.1, while the Nexus 7 devices will run Android 6.0.1. The purpose of this is to make sure that the data is the same across all devices and version numbers. Datagen was done with the following method:

1. Wipe the device
2. Add Gmail account to the phone
3. Do not turn on “Help location by scanning wi-fi” or “Send diagnostic data to google”. Keep rest on.
4. Download Kayak
5. Login to Kayak with Gmail account
6. Create a new trip: Burlington to Montreal. Be sure to connect inbox to trips@kayak.com.
7. Make sure the date is the sixth to the seventh of October.
8. Add 1 flight from Burlington International to Montreal International. Watchlist the flight, and press the purchase ticket button. It redirects to another page. Exit this page right after.
9. Add one hotel to the watchlist, and press book rooms button. Exit this page right after.
10. Add one car rental to watchlist, and press book. Exit this page right after.

After this is done, extract the Root ADB, make sure the device is on airplane mode, and extract the data.
To conduct our research, we will be using the tool UFED Cellebrite 4PC Physical Analyzer 7 and UFED Cellebrite 4PC. You must install the application Kayak from the Google Play Store onto your mobile device. Using the method mentioned above, enter the information carefully and make sure to avoid adding more information than necessary so that the data extracted is accurate.

Our plan for collecting the data was to first have each person wipe their devices, install the Kayak app on their mobile devices, and login to Kayak with their fake Gmail account. Next, each individual creates a new trip from Burlington to Montreal for the dates October 6 to October 7. Once you add this flight, watchlist it, and press the purchase button. It will redirect you to a different page which you need to exit. You can then repeat the same process for adding one hotel and one car rental to the watchlist.

Extract the data using UFED Cellebrite 4PC. Connect your mobile device to your computer using a USB cable. Once it’s connected, click on UFED 4PC on your desktop.

Equipment Used

We used the tools UFED Cellebrite Physical Analyzer 7 and UFED Cellebrite 4PC which are pictured below.

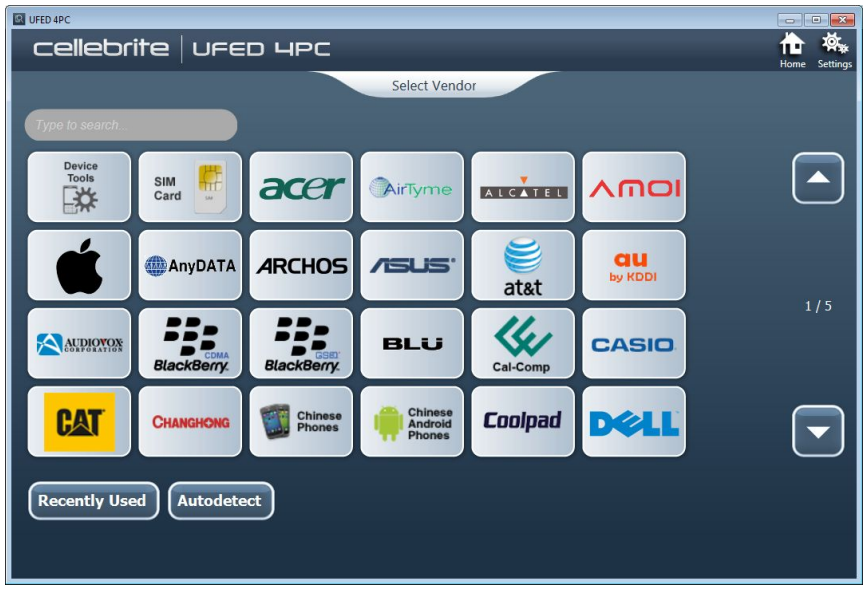


Table 1: List of Devices

Device	OS Version	Serial Number	Comments
Huawei H1511 Nexus 6P LCDI-5017	Android 8.1.0	84B7N16302000150	Used for phone data generation/analysis
Nexus 7 LCDI-6028	Android 6.0.1	094e2f8a	Used for tablet data generation/analysis
Nexus 7	Android 6.0.1	092958a2	Used for tablet data generation/analysis

Data Collection

Data will be collected using UFED Cellebrite 4PC. The data collection for the tablets and phones were slightly different, being that they were different types of mobile devices.

Firstly, both types of devices needed to be rooted in order to collect data. Rooting the devices was different depending on whether it was a tablet or phone. This was due to the fact they ran different versions of Android.

After the devices were properly rooted, giving owners Administrative privileges, UFED Cellebrite 4PC was utilized in performing Physical Extractions for both types of devices.

> **Huawei Nexus 6p:** UFED 4PC gives different options upon start-up to the user for data extractions. For Huawei Nexus 6p, 'Mobile' was selected. 4PC gives the user an option to search for their type of device with a search bar, located at the top right of the screen. Search Huawei Nexus 6p 1151. Select the phone. Do NOT select 1152. In the future, you can use recently used at the bottom. Select Physical Extraction. Select ADB rooted. Unplug and replug the phone, if you have to. It should start. Press continue on any messages that pop up.This process will take an hour AT LEAST. Expect up to an hour and a half.

Nexus 7 Tablet: For the Nexus 7s, the tablets are running Android 6.0.1. Open UFED 4PC. Select Mobile. Cellebrite will ask to automatically detect your device. The team found it easier to use the "Browse Manually" option. Select the device you are using - in this case, select the *Asus ---> K009 Nexus 7.* There is a list of possible extractions: logical and physical extraction, file system extraction, or capture images/screenshots. In this case, the option "physical extraction" was chosen. Cellebrite will give the option of *ADB* physical extraction mode. Select this. Select your Target Path. In this case, the user's personal folder was chosen. The next screen will ask the user to connect their device via USB and turn on USB debugging. Once the device is connected with USB debugging, select "Continue" at the bottom right of the screen. The extraction will begin. The time differs for every device, as well as the amount of data there is stored on the device. Once the extraction process is finished, UFED 4PC will give three options: go to target folder, open UFED Physical Analyzer, or start another extraction.

Analysis

The Kayak app is expected to store a large amount of data. This may include personal account information such as usernames, passwords, and email addresses. Also, it is expected that the application will store data about past, present, and planned trips such as flight, hotel and rental car data. This stored data is important because it allows forensic analysts to possibly track a device or find potential suspects.

Results

To get the results, we had to make a fake Gmail account using fake names. Once that was completed, we installed the Kayak application on our mobile devices. We added a one-way flight from Burlington to Montreal, added it to the watchlist, pressed the purchase button, and exited out of the page. We repeated the same process for adding one hotel and one car rental to the watchlists. After using UFED Cellebrite 4PC and UFED Cellebrite Physical Analyzer, we analyzed the data.

Huawei H1511 Nexus 6P LCDI-5017

Kayak_room.db

All the database categories:
TsaWaitTime
Android_metadata
Boarding_pass
Boarding_pass_segment
Boarding_pass_trip_data
Booking_receipts
flightTrackerResponses
Room_master_table
Sqlite_sequence
Trips_days_tables
Trips_details_tables
Trips_events_details_table
Trips_events_fragments_tables
Trips_notes_table
Trips_shares_table
Trips_summaries_table

As we were not able to book actual tickets, rooms, or cars for this data gen, only a few of these are filled in.

Room_master_table

Sqlite_sequence: Contains the basic sequence information for the trips_events_details_table, trips_events_fragments_tables, and trips_shares_table tables.

	name	seq
☑	trips_events_details_table	6
☑	trips_events_fragments_table	3
☑	trips_shares_table	3

trips_days_table: Contains when the trip will start, in Unix Timestamp

1538784000000 = Sat, 06 Oct 2018 00:00:00 GMT (UTC/GMT), or 8:00:00 PM,Fri,5 Oct 2018 GMT-0400 (Eastern Daylight Time)

The trip is supposed to start on the 6th, so this is accurate. However, the trip's end date is missing.

Trips_details_table

Table 2: trips_details_table Flight Information

Entry Name	Entry
encodedTripID	D76c6t
tripName	Montreal Trip
destination	Montreal
destinationID	l:6966
destinationLat	45.5
destinationLon	-73.583
shareUrl	/trips/!D76c6t8jW2iFutrq
upcoming	1
startTimestamp	1538827200000
endTimestamp	1538913600000
modificationTimestamp	1538514010000
focusTripEventId	68251397
focusLegnum	0
Permissions	{"editor":true,"friend":true,"owner":true}
userNotificationPreferences	{"notificationsEnabled":true}

Trips_events_details_table

Table 3: trips_events_details_table ID 4, Base Flight Information

Entry Name	Entry
Id	4
tripDetailsId	D76c6t
airlines	"AC":"Air Canada","UA":"United Airlines"
cabinClassCode	"E","legs"
canAutoCheckin	false
checkinStartTime	1538758920000
notificationStartTime	1538758920000
booked	false
bookingTimestamp	0
isSplitBooking	false
merchantName	United
merchantSite	united.com
totalCost	$534.05

Table 4: trips_events_details_table ID 4, Burlington to Newark Flight Information

Entry Name	Entry
arrivalAirportCode	EWR
arrivalPlace	"city":"Newark","ctid":"8252","latitude":40.68333333,"longitude":-74.16666667
arrivalTimestamp	1538836020000
departureAirportCode	BTV
departurePlace	"city":"Burlington","ctid":"14027","latitude":44.46666667,"longitude":-73.15,"
departureTimestamp	1538830920000
marketingCarrierName	United Airlines
marketingCarrierNumber	3971
durationMinutes(Flight)	85
durationMinutes(Layover)	213
layover	true
locationName	Newark (EWR)

Table 5: trips_events_details_table ID 4, Newark to Montreal Flight Information

Entry Name	Entry
arrivalAirportCode	YUL
arrivalPlace	"city":"Montreal","ctid":"6966","latitude":45.469723,"longitude":-73.74472,"mappable":true,"name":"Pierre Elliott Trudeau International"
arrivalTimestamp	1538853840000
departureAirportCode	EWR
departurePlace	"city":"Newark","ctid":"8252","latitude":40.68333333,"longitude":-74.16666667
departureTimestamp	1538848800000
marketingCarrierName	Air Canada
marketingCarrierNumber	7743
durationMinutes	84
locationName	Montreal (YUL)

Table 6: trips_events_details_table ID 5, Sofitel Montreal Golden Mile

Entry Name	Entry
Id	5
tripDetailsId	D76c6t
hotel	Sofitel Montréal Golden Mile
localizedAddress	1155 Sherbrooke Ouest, Montreal, QC H3A 2N3
numberOfGuests	1
numberOfRooms	1
latitude	45.501415
longitude	-73.57732
localizedRegion	Quebec
websiteAction	http://priceline.com
totalCost	$343.85
originalBaseUnitPrice	$275.44
originalTotalPrice	343.85000
originalUnitPrice	343.85
updatedTotalPrice	343.85000
updatedUnitPrice	343.85

Table7: trips_events_details_table ID 6, Chevrolet Sonic Sedan

Entry Name	Entry
Id	6
tripDetailsId	D76c6t
agencyName	Avis
carDetails	Chevrolet Sonic Sedan
carType	Economy

dropoffPlace	"city":"Montreal", "ctid":"6966", "country":"Canada", "latitude":45.500416, "longitude":-73.571365", "mappable":true,"rawAddress":"1225 Metcalfe Street, Montreal, Quebec H3B 2V5, Canada","timeZoneId":"America/Toronto"
dropoffTimestamp	1538913600000
pickupPlace	"city":"Montreal","ctid":"6966","country":"Canada","latitude":45.500416,"longitude":-73.571365,"mappable":true,"rawAddress":"1225 Metcalfe Street, Montreal, Quebec H3B 2V5, Canada","timeZoneId":"America/Toronto"
pickupTimestamp	1538827200000
merchantName	Travelocity
merchantSite	Travelocity
totalCost	$76.40

These tables show the following:

Flight: I have a flight with United Airlines and Air Canada. The first leg of the flight is from Burlington to Newark, which takes 1 ½ hours.. There is a layover of 4 hours. The second leg is from Newark to Montreal, which takes 1 ½ hours. Total cost is $534.05.

Hotel: There is a check-in time of 10/6/2018 at 11:00:00 AM and a check-out time of 10/7/2018 at 8:00:00 AM. There is 1 room and 1 guest. The hotel name is Sofitel Montréal Golden Mile and is located at 1155 Sherbrooke Ouest, Montreal, QC. Its phone number is +1 514 285 9000. Website: http://www.sofitel.com/lien_externe.svlt?goto\u003dfiche_hotel\u0026sourceid\u003dfh\u0026code_hotel\u003d3646 Rating: 5 Stars (On Kayak). Purchased on priceline.com

Car: Agency Name: Avis. Car: Chevrolet Sonic Sedan. Type: Economy.

Drop-off location: 1225 Metcalfe Street, Montreal, Quebec. Drop-off time: 10/7/2018, 8:00:00 AM.

Pickup location: 1225 Metcalfe Street, Montreal, Quebec. Pickup Time: 10/6/2018, 8:00:00 AM.

Purchased from: Travelocity

Cookies.db

Travelocity kept a history of the actual URL of when the person booked a car using Kayak.

The first column is creation_utc, the second column is the host key, the third column is the name, and the last column is the value.

The person used a couple of different sites when booking a hotel, car, and flight using Kayak.

☑	13182987500506391	.travelocity.com	rlt_marketing_code_cooki e	MDP.TRAVELOCITY-US.META.KAYAK.CORESEARCH-MOBILE.CAR
☑	13182987500971586	.travelocity.com	_ga	GA1.2.786085069.1538513901
☑	13182987500975905	.travelocity.com	_gid	GA1.2.1519121637.1538513901
☑	13182987501147509	.travelocity.com	_gcl_au	1.1.9482649.1538513901
☑	13182987501446606	www.travelocity.com	_tq_id.TV-097263-1.7986	9653794725e4f136.1538513901.0.1538513901..
☑	13182987502101240	.travelocity.com	yieldify_original_referrer	https%3A//www.kayak.com/book/car%3Fcode%3DEhAm

☑	13182987371629712	.united.com	Session	AuthToken=2c9VP8uK6VUJlJR4Lmonwk3wy1UGEBgO4VqUYjUqar6kU%3DStAFfnuZ5z
☑	13182987371630713	.united.com	Locale	POS=US&Lang=en&UMID=6cbdcdbc-4afe-43de-a308-d1fa4777a48e&POSCODE=
☑	13182987371632001	.united.com	TLTSID	BE023A7E41AC5784DDCE86ABDAC96726
☑	13182987371632306	.united.com	TLTUID	BE023A7E41AC5784DDCE86ABDAC96726
☑	13182987371632685	www.united.com	moovweb_exp	true

☑	13182987234519470	.priceline.com	t-senduserscore	traffic-active
☑	13182987231880524	.www.priceline.com	intent_media_prefs	
☑	13182987234924543	.priceline.com	bopi_cid	3eee31ab-291a-429a-9417-a8623104b079
☑	13182987234935584	.priceline.com	bopi_cid_m	false
☑	13182987235337193	.priceline.com	bopi_lc_id	cdd94616-081b-48ae-830f-16faf5a636b6
☑	13182987235468596	.priceline.com	__gads	ID=249c030dea7b32c4:T=1538513635:S=ALNI_MYisJT0sg6NXdi43qNMYU4Yx25Kmw
☑	13182987236382593	.priceline.com	_dc_gtm_UA-2975581-1	1
☑	13182987228757801	.priceline.com	_ga	GA1.2.415243636.1538513629
☑	13182987228765342	.priceline.com	_gid	GA1.2.866516509.1538513629

☑	13182987221886346	www.kayak.com	p1.med.token	22-evYkbRxyQrdW2OPmXCXCVUlZEH87REq0V0EabA0a0-xHasQlk
☑	13182986955219141	www.kayak.com	p1.med.sid	65-H-4PbLACZj7dztuYdecgqCk-Ka6jB6EAhcbfdM7SpcsUTE_ptN8NY7nkjHvc6nQHts-
☑	13182987221892554	www.kayak.com	Apache	uKueuA-AAABZjaDnpU-5d-dweLGg
☑	13182987221894622	www.kayak.com	kayak	z2B9O9oozrQPFwpW$Y_i
☑	13182987224752238	.kayak.com	_ga	GA1.2.957372724.1538513625
☑	13182987224763313	.kayak.com	_gid	GA1.2.1340860745.1538513625
☑	13182987494687852	.kayak.com	_gat	1

Database view | Hex View | File Info

cookies (109)
meta (3)

☑	key	value
☑	mmap_status	-1
☑	version	10
☑	last_compatible_version	10

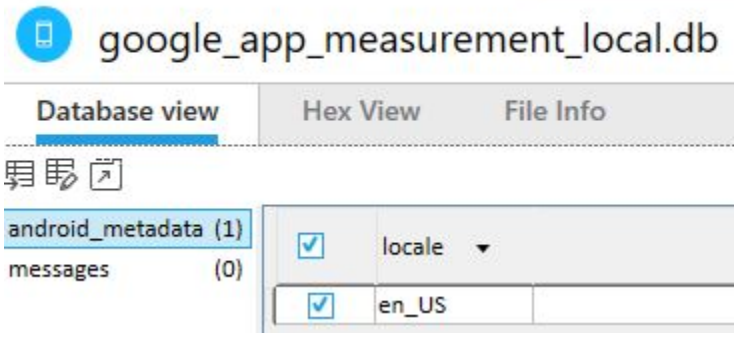
google_analytics_v4.db

Kayak kept some metadata about which operating system the user was using.

app_uid	cid	tid	params	adid	hits_count
0	6219c032-86f2-4b94-9aeb-958ed6393c1f	UA-42209185-11	av=64.0&an=KAYAK&aid=com.kayak.android&aiid=com.android.vending	0	180
0	6219c032-86f2-4b94-9aeb-958ed6393c1f	UA-42209185-8	av=64.0&an=KAYAK&aid=com.kayak.android&aiid=com.android.vending	0	180

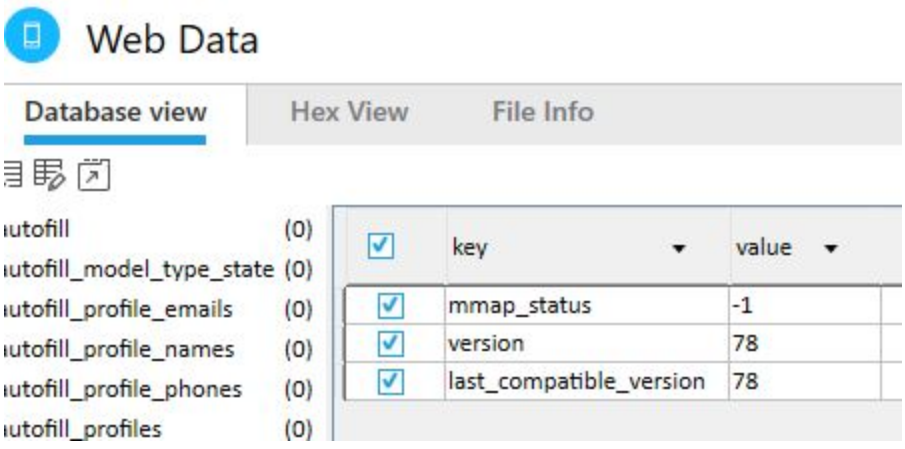
google_app_measurement_local.db

You can see through the Android metadata what formatting version of Android the person used (ex: US) when using Kayak.



Web data.db

You can see what version and the last compatible version of Kayak the person was using.



Nexus K009 Tablet (Serial Number 094e2f8a)

Device and App Details

Data generated before extraction:

- Created a trip from 10/11/2018 to 10/12/2018
- BTV to YUL (Burlington, Vermont airport to Montreal, Canada airport)
- Looked up a flight, car rental, and hotel, pressed "book" for each, and added to them to a Watchlist. (None of the above were actually booked.)
- Connected the fake gmail to Kayak's inbox.

Table 8: Watchlisted Information Generated by User

	Airline Ticket	Rental Car	Hotel
Price in $USD	664	169 per day	473 per night
Type/Brand/Model	American Airlines/United Airlines	Mercedes Benz C-class or similar	Fairmont The Queen Elizabeth

Data Found After Extraction

After performing a Physical Extraction from the Nexus 7 via Cellebrite 4PC, the following tables containing database files were browsed in Cellebrite Physical Analyzer (see appendix for images):

Table 9: Trip details taken from *kayak_db*

Entry Name	Entry Value
tripName	Montreal Trip
userDisplay	Hope Kaiya
startTimestamp	1538915400000
endTimestamp	1538915400000
destinationLat	45.603596
destinationLon	-73.603386

Table 10: Airline details taken from *events_detailsJson*

Entry Name	Entry Value
cabinclasscode	"E"
alertID	"715082261"

cancled	false
createDate	1538514900000
createdByCurrentUser	true
createdType	“SAVED”
private	false
modifiedbyCurrentUser	true
currency	“USD”
originalBaseUnitPrice	-1
originalTotalPrice	-1
originalUnitPrice	-1
resultID	"134662af36bc0c1b2a1d40cf611de2d2hf"
savedEvent	true
searchTimestamp	1538500500000
tripEventId	68251856
type	“FLIGHT”
updatedBaseUnitPrice	-1
updatedTotalPrice	-1
updatedUnitPrice	-1

Table 11: Hotel reservation details taken from *events_detailsJson*

Entry Name	Entry Value
numberOfGuests	2
numberOfRooms	1
booked	false
canceled	false
checkinTimestamp	1538838000000
checkoutTimestamp	1538913600000

createDate	1538514941000
createdByCurrentUser	true
createdType	“SAVED”
currency	“USD”
originalBaseUnitPrice	399.61
originalTotalPrice	473.46
originalUnitPrice	473.46
savedEvent	true
searchTimestamp	1538500500000
tripEventId	68251878
type	“HOTEL”
updatedBaseUnitPrice	399.61
updatedTotalPrice	473.46
updatedUnitPrice	473.46

Table 12: Car Rental details taken from *events_detailsJson*

Entry Name	Entry Value
AgencyName	ACE
carDetails	"Mercedes-Benz C-Class"
carType	“Luxury”
dropoffTimestamp	1538515016000
pickupTimestamp	1538827200000
cancled	false
createdByCurrentUser	true
createdType	“SAVED”
currency	“USD”

modifiedTimestamp	1538515016000
originalBaseUnitPrice	140.35
originalTotalPrice	169.86
originalUnitPrice	169.86
savedEvent	true
searchTimestamp	1538500560000
tripEventId	68251919
type	“CAR_RENTAL”
updatedBaseUnitPrice	140.35
updatedTotalPrice	169.86
updatedUnitPrice	169.86

Cookies

There were a couple base.apk files and a lot of Cookies found in addition to the database files previously presented. However, the base.apk files were for the most part blank or contained no useful information. As for the Cookies, there was a lot of useful data like webpages Kayak takes the user to book their service, be it a plane ticket or a car rental.

Table 13: Car Rental details taken from Cookies

host_key	Entry value
.orbitz.com	%7B%22dps%22%3A%5B%22MDP.ORBITZ-US.META.KAYAK.CORESEARCH-MOBILE.CAR.CAR...LUXURY.Ace.YMQC002.YMQC002.2.0%22%2C1539293449593%5D%2C%22entryPage%22%3A%5B%22page.Car-Search%22%2C1539293449606%5D%2C%22cid%22%3A%5B%22MDP.ORBITZ-US.META.KAYAK.CORESEARCH-MOBILE.CAR%22%2C1539293449608%5D%2C%22cidVisit%22%3A%5B%22MDP.ORBITZ-US.META.KAYAK.CORESEARCH-MOBILE.CAR%22%2C1539293449615%5D%2C%22rlt%22%3A%5B%22MDP.ORBITZ-US.META.KAYAK.CORESEARCH-MOBILE.CAR%22%2C1539293449608%5D%7D

NOTE: There was also data from the domain united.com which is believed to belong to United Airlines. Kayak directed the user to United Airlines to book the airline tickets; however, the value was random characters and did not hint towards the tickets that were Watchlisted.

Conclusion

The data that was found on the devices is mostly comprised of user-generated data relating to trips created. These things include: searches, displayName (user's full name), trips on Watchlist, and other elements of the Watchlist. No passwords or usernames were found; however, trips created and the creator's full name and email address were discovered. Watchlisted information stored on the device in *.db* format was found and analyzed with *Cellebrite*. Aside from user-generated data, general information was also found, such as the tablet's language.

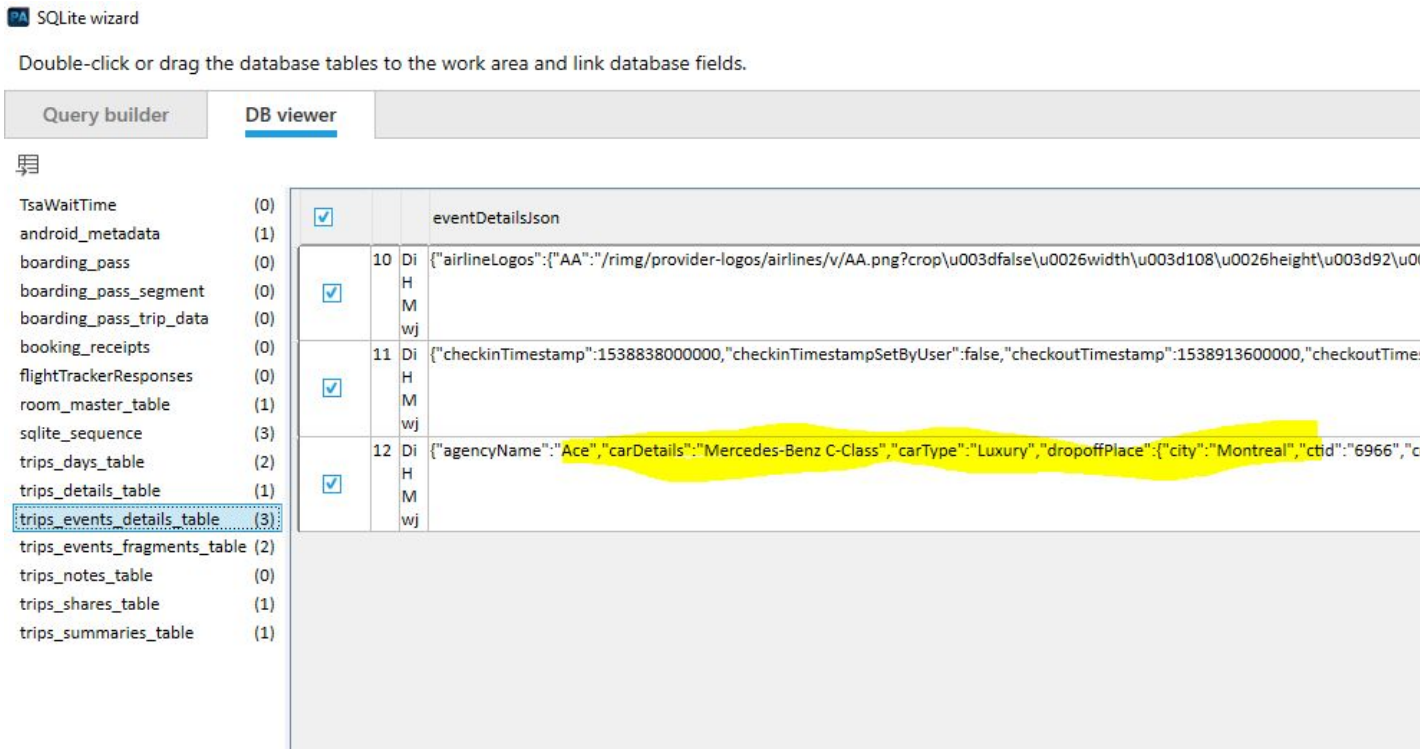
All of the data recovered from the devices using *Cellebrite 4PC* is considered useful to a digital forensic analyst. Although it could be more detailed in some areas (like location of searches, etc.) the average analyst is able to piece together a story, or, *timeline* with said information. For example, the start timestamp and end timestamp of trips are recorded and stored by Kayak. The analyzer now knows the timeframe of a possible trip taken or planned by a criminal whose phone was recovered and imaged by said analyst. Following that information, the app also stores airline ticket information that is crucial: departure timestamps, locations, and destination longitude and latitude. If the analyst needs to somehow prove a criminal left on a certain date, they at least now have the ability to prove a trip was planned thanks to the data they recovered from Kayak.

Further Work

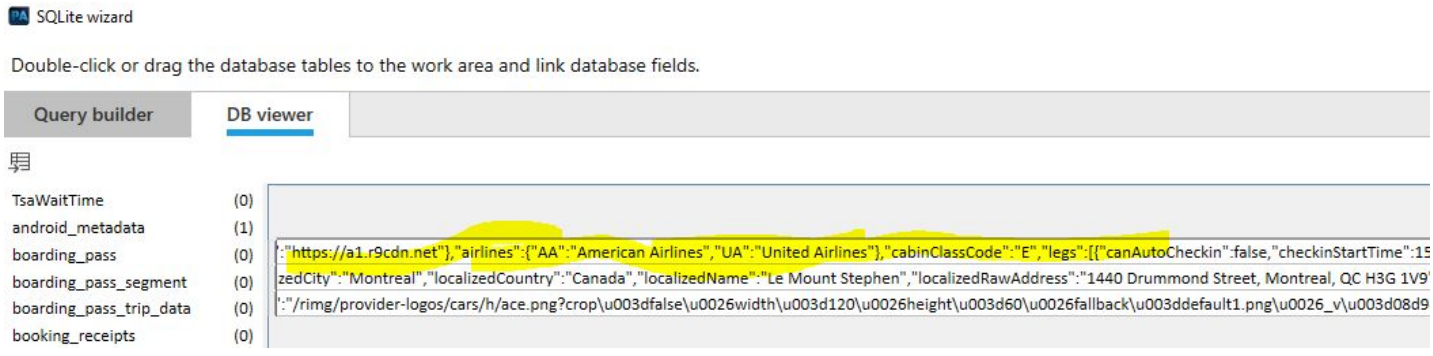
Regarding the Nexus K009, things such as username and password were not discovered. Perhaps more trials could reveal these elements. Most data that was found is considered to be useful for a typical forensic analyst. A different form of extraction may be able to done in order to uncover missing data. A recommendation for another type of extraction could be to use ADB to directly pull files from the Android devices. By doing so, the forensic analyst has the ability to directly acquire Kayak's device-stored data right from the command line or powershell.

Appendix

Data extracted showing Watchlist evidence (airline info)



Data extracted showing Watchlist evidence (car rental)



Data extracted showing Watchlist evidence (airplane tickets)

currentUser	displayName	encodedUid
1	Hope Kaiya	orE7WjD9ES8
1	Hope Kaiya	orE7WjD9ES8

Current user displayed in Cellebrite Physical analyzer

destinationName	tripName	startTimestamp	endTimestamp
Montreal	Montreal Trip	1539270000000	1539518400000
Montreal	Montreal Trip	1538827200000	1538915400000

Timestamps found in kayak_room.db

www.kayak.com	NSC_q4-lbqj	ffffffff094f9a2645525d5f4f58455e445a4a42299c
.orbitz.com	cesc	%7B%22dps%22%3A%5B%22MDP.ORBITZ-US.META.KAYAK.CORESEARCH-MOBILE.CAR.CAR...LUXURY.Ace.YMQC002.YMQC002.2.0%2 %22MDP.ORBITZ-US.META.KAYAK.CORESEARCH-MOBILE.CAR%22%2C1539293449608%5D%7D
.orbitz.com	HMS	3a074963-3d5d-48c2-bb1a-5eacae293056

Cookies from Kayak: orbitz.com

References

"What Happens When You Press That Button?" *Smarterforensics.com*, smarterforensics.com/wp-content/uploads/2014/06/Explaining-Cellebrite-UFED-Data-Extraction-Processes-final.pdf.