

MASVS-STORAGE-1:

Appropriate users/group have access to the app files:

```
drwxrwx--x  2 u0_a68 u0_a68          4096 2024-04-29 03:04 app_textures
drwxrwx--x  5 u0_a68 u0_a68          4096 2024-04-29 03:04 app_webview
drwxrws--x  7 u0_a68 u0_a68_cache    4096 2024-04-29 03:04 cache
drwxrws--x  2 u0_a68 u0_a68_cache    4096 2024-04-29 03:03 code_cache
drwxrwx--x  2 u0_a68 u0_a68          4096 2024-04-29 03:07 databases
drwxrwx--x  2 u0_a68 u0_a68          4096 2024-04-29 03:04 files
drwxrwx--x  2 u0_a68 u0_a68          4096 2024-04-29 03:04 no_backup
drwxrwx--x  2 u0_a68 u0_a68          4096 2024-04-29 03:07 shared_prefs
```

In Shared preferences found access tokens and auth codes for the app's mobile wallet.

```
at mobilewallet_united_android_public.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <string name="AUTH_CODE">Default_Auth_Code</string>
  <string name="ACCESS_TOKEN">wvv26PLLZ5Q1ZAbJUe0i9j7j7srFH449L2PV7KRbXu0dgf5r6bjB6Pg5J+iNpkAuCLC8FmP64jr/bxynaQRUX
HdToddjfvvebb8wggYGrJNmPtNat4ok6NzIg7kaRqCmIB5qJ5/k3kY/pQHn2Cw==</string>
  <string name="EXPIRES_IN">2024-04-27T14:03:44</string>
  <string name="TOKEN_TYPE"></string>
  <string name="REFRESH_TOKEN"></string>
</map>
emu64xa:/data/data/com.united.mobile.android/shared_prefs # cat mo
mobilewallet_united_android_public.xml          mobilewallet_united_android_semi_private.xml
at mobilewallet_united_android_semi_private.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <string name="AUTH_CODE">Default_Auth_Code</string>
  <string name="ACCESS_TOKEN">wvv26PLLZ5Q1ZAbJUe0i9j7j7srFH449L2PV7KRbXu0dgf5r6bjB6Pg5J+iNpkAuCLC8FmP64jr/bxynaQRUX
HdToddjfvvebb8wggYGrJNmPtNat4ok6NzIg7kaR1Qa4TMbQ7MkYkt2qpAOI3jw==</string>
  <string name="EXPIRES_IN">2024-04-27T14:03:44</string>
  <string name="TOKEN_TYPE"></string>
  <string name="REFRESH_TOKEN"></string>
</map>
emu64xa:/data/data/com.united.mobile.android/shared_prefs #
PS C:\Users\migue>
```

Found encrypted keys for the flight status features.

```
at pcu_flight_status_model.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <string name="__androidx_security_crypto_encrypted_prefs_key_keyset__">12a90160e66484dc1151101b20d18fa92815b2e2e3137
3c6e533060e7d00f956469602022c527b2f6a1e1c33c3a6794a0e3e9ee927926aa5fde5c2aefd2e5a0de87a248be5d97c92e0c6a4475d961f698a752
e0088bdc7b1642f30c9676773651df9437cd56d82dfcf470577c9270a81ae1ed0df7cf683bb922460b5e064864f7a047ae6409d4ce467dca59bb703d
a38dd27fc5a8b86243744163eaae4c1f3b13a0fc6b22231c5bee7d9585e1a4408d9ee939806123c0a30747970652e676f6f676c65617069732e636f6
d2f676f6f676c652e63727970746f2e74696e6b2e4165735369764b6579100118d9ee9398062001</string>
  <string name="__androidx_security_crypto_encrypted_prefs_value_keyset__">128601a3dcd0690237e1923608de2a922196950fd4b
6b304b733ceaea579859c2da81cb1e84a42efd479d5bf650355efb3d9e7e4d207f41501d9f123c0c11fb65df914d41a9dab0b540fd5c01749eb80849
a467ba5758eaa0e2217d421b2993454db01f7b28904c34a38672602ad3f22c7364836096dddaf6a72a231e6bf1107e680cb75bb64729c011a4208c4e
be821123b0a30747970652e676f6f676c65617069732e636f6d2f676f6f676c652e63727970746f2e74696e6b2e41657347636d4b6579100118c4ebe
8212001</string>
</map>
emu64xa:/data/data/com.united.mobile.android/shared_prefs #
```


DeviceID can be found


```
generic_x86_64:/data/data/com.united.mobile.android/shared_prefs # cat device.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <string name="deviceId">da70879d-e271-45af-bb00-4e723abd2024</string>
</map>
generic_x86_64:/data/data/com.united.mobile.android/shared_prefs #
```

The only other thing of significance found were encrypted key value pairs:

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <string name="__androidx_security_crypto_encrypted_prefs_key_keyset__">12a90199df98b26389d16d857dba36b7b5e2d571ed5aa4f18ae067a14d82d8b69338b2fb9235a30d7c51cef5942b74696b8999339be4df6d4f4fab9a
  <string name="ARodBVty+if5mEvG185XnksBKQ0FMJ0JFC0ume50zFeqH+VYlRavSnos">AS8bbbxZ79Wd0SL0mZvH40ES6pPengRnxqo1BoFR5C1oZY15C2mQtnp1RXJcFbCuyA==</string>
  <string name="__androidx_security_crypto_encrypted_prefs_value_keyset__">1288018245e585d7c0c0b2c2072b2944b4e2c50990e5524bf9ec6e6e94fe4f9fe4201aad1fb9a3512bb537a6b1414e323fa5e970de9e73abacd16fe
</map>
```

SQLite databases:

 **SQLITE DATABASE**



FILES
data/data/com.united.mobile.android/app_webview/Cookies
data/data/com.united.mobile.android/app_webview/Web Data
data/data/com.united.mobile.android/databases/com.google.android.datatransport.events
data/data/com.united.mobile.android/databases/com.usebutton.events
data/data/com.united.mobile.android/databases/events
data/data/com.united.mobile.android/databases/united.db
data/data/com.united.mobile.android/no_backup/androidx.work.workdb

Showing 1 to 7 of 7 entries

I have found in the events database the android os version:

analyticsEvent			
serverType	accountID	jsonString	retryCount
PRODUCTION	A1D4XY4NEBABI9	{ "_eventType": "appAndUserProperties", "_eventId": "dda9c123-c3cb-4fb2-8ff8-50fb361e8e54", "_eventVersion": "1", "installId": "fa2c7311-0205-4d57-a7f3-0a862488c5fd", "timestamp": "2024-04-29T10:04:36.510Z", "shortAccountID": "A1D4XY4NEBABI9", "productName": "LocusMaps Android", "SDK": "productVersion": "3.2.51", "deviceTimezone": "America\\Los_Angeles", "deviceOSName": "Android", "deviceOSVersion": "28", "uiLocale": "en_US", "browserName": null, "browserVersion": null, "kioskName": null, "kioskLocation": null, "hostAppld": "com.united.mobile.android.UnitedApplication", "hostAppVersion": "4.1.102", "hostAppProperties": {} }	0

This app does not use Realm databases.

MASVS-STORAGE-2:

- Testing Backups for Sensitive Data:

The app does not allow for backups or automatic backups. There is also a directory that has several files telling what not to backup. I also tested with the [android-backup-extractor](#) and found no package for united airlines app.

android:name="com.united.mobile.android.UnitedApplication" android:allowBackup="false"

```
emu64xa:/data/data/com.united.mobile.android/no_backup # ls
androidx.work.workdb      androidx.work.workdb-wal      com.google.android.gms.appid-no-backup
androidx.work.workdb-shm  com.google.InstanceId.properties
emu64xa:/data/data/com.united.mobile.android/no_backup #
```

Found no evidence of backupAgent either in the android manifest.

Found no evidence of file being sent to cloud backup either. Firebase Scanner turned up nothing.

- Determining Whether the Keyboard Cache Is Disabled for Text Input Fields:
 - Search suggestions appear in app for airports but also for local locations. This app likely uses other third-party app or tool such as google maps to integrate this feature.



Select departure

Search

flor



Include airports within 100 miles



Search results



Key West, FL, US (EYW)



Rome, IT (FCO)



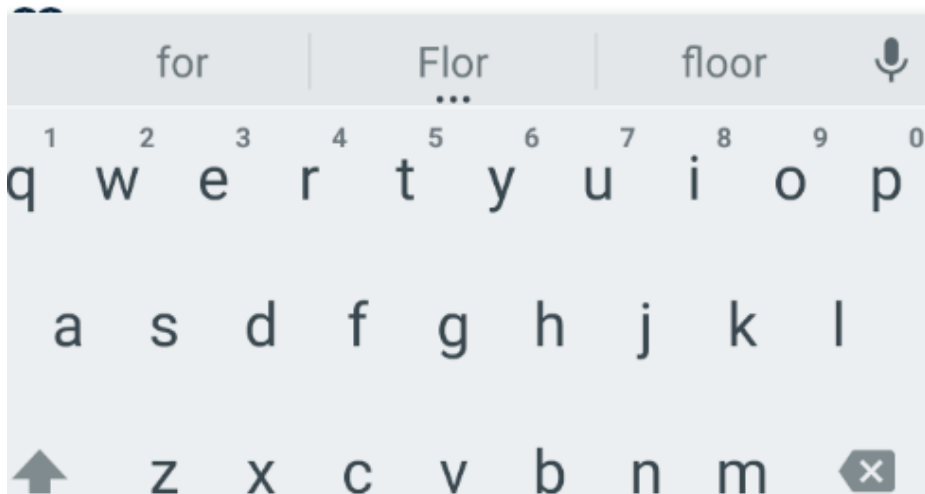
Fort Lauderdale, FL, US (FLL)

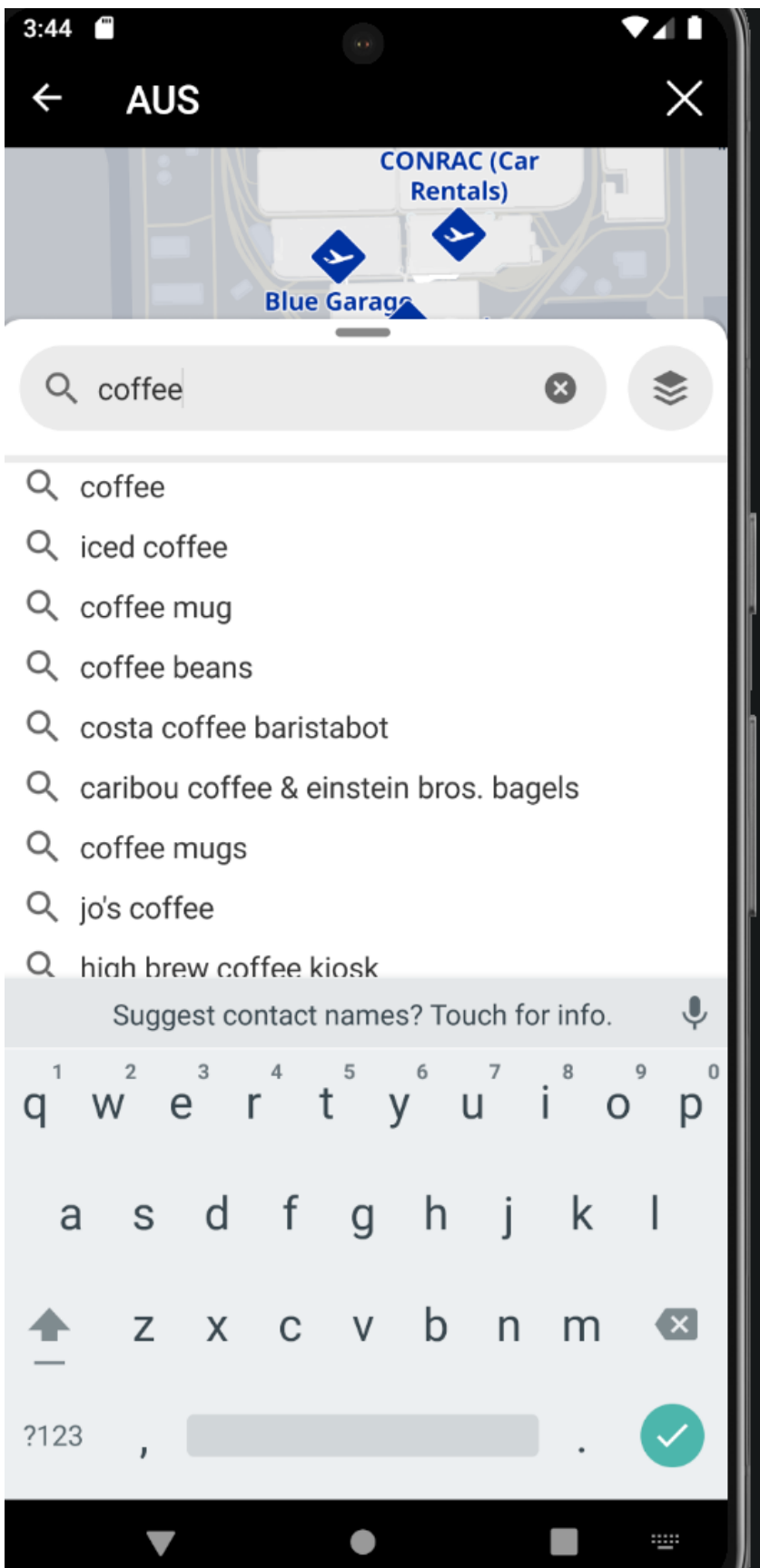


Jacksonville, FL, US (JAX)



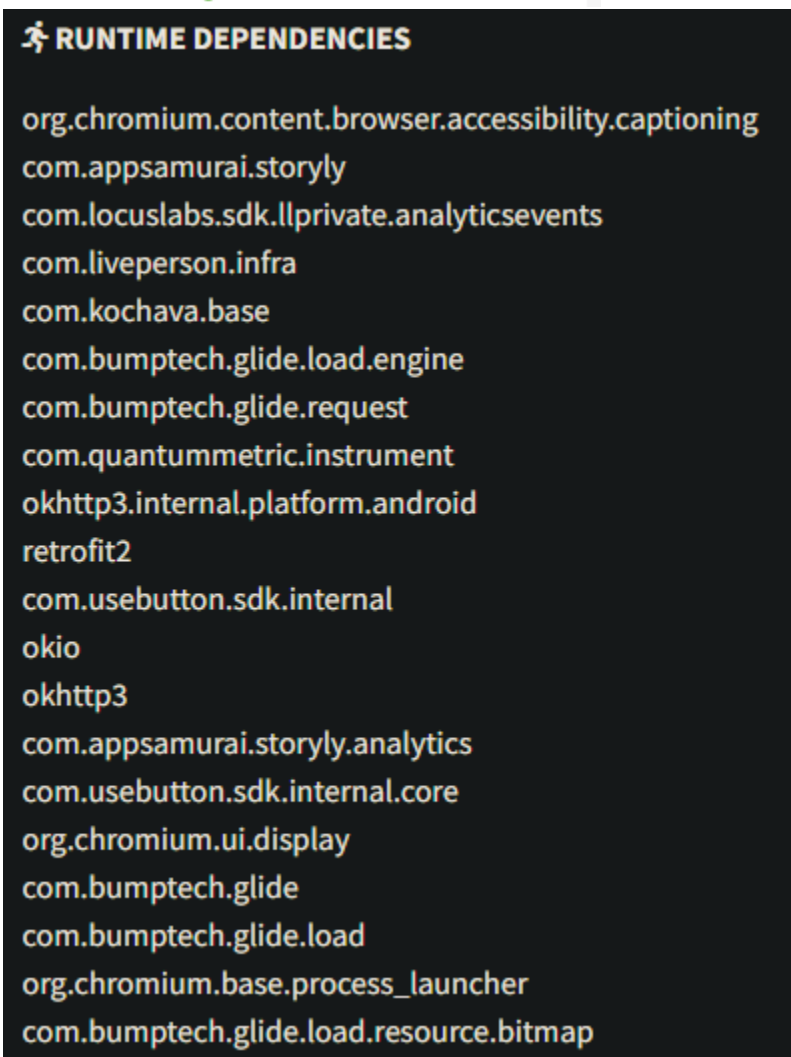
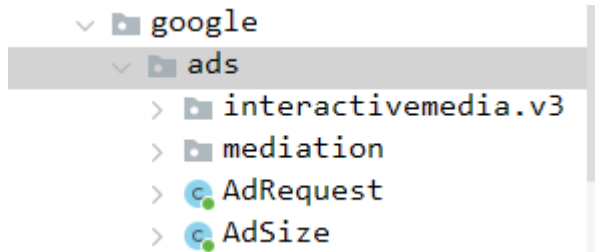
Orlando, FL, US (MCO)





- Determining whether sensitive data is sent to third parties by embedded services:

The following apps were found to be running at the same time and potentially transferring user data



TRACKERS		
TRACKER NAME	CATEGORIES	URL
Qualtrics		https://reports.exodus-privacy.eu.org/trackers/306

<https://smartphone.united.com/customerprofile/api/updatepassword>
<https://www.united.com/ual/en/us/fly/travel/inflight/wifi.html>
<https://mobileapi.united.com/receiptservice/api/sendreceipt>
<https://wifi.inflightinternet.com/app/ifc/sponsor/verification>

Further Communication testing will have to be done as SSL pinning is required to see the traffic coming from these 3rd parties and to detect potentially leaked secrets.