Deleted Apps Information

- IOS – All about Bundle
- Each app has a plist file named [BundleID].plist in the preferences folder
- Source path reveals the UUID for that APP
- Bundle ID is still searchable in the file system
- Deleted or Just Offloaded
- “Offloaded” offload apps not frequently used but keep the documents and data.

BundleIDs

- We can search for the App online
  - Ex Google: facebook IOS app in apple store
    - Generally look for https://apps.apple.com
    - After click on on the required app
      - Look for numerical number after ID at the end of the URL
        - https://apps.apple.com/us/app/facebook/id**284882215**
    - Once we got the numerical number, paste this number after '=' in the following url
      - https://apps.apple.com/lookup?id=**284882215**
        - It will download a .txt file containing the information of the app and Ta-Da the BundleID for that app

Info artifacts inside bundleid

- Mobile Installation Logs
- UninstalledApplications.plist
- DAAP.sqlitedb
- AppPurchaseHistory.6.sqlitedb
- ScreenTime
- PowerLog.PLSQL
- KnowledgeC.db
- DataUsage
- CallHistory.storedata ???

Apple Apps Info

- Once IOS device info is extracted
- We can go to the following location
- **\private\var\mobile\library\FrontBoard\applicationState.db**
- **Itz a treasure map**
  - **AppSource Location : /private/var/containers/Bundle/Application/(GUID reference)/xxxx.app**
  - **Application Data Location : /private/var/mobile/Containers/Data/Application/(GUID reference no.)**
- **Offloaded applications lose applicationstate.db**

- Mobileinstallation Log may have it depending on time.
  - **/private/var/installed/Library/Logs/MobileInstallation/*.Log(0 or 1)**
    - Tracks when apps are installed, uninstalled, moved containers and destroyed containers.
    - Gives Timestamp and path to app.
    - Search in GitHub for Alex's iS-Mobile-Installation-Logs-Parser

UninstalledApplication.plist

- \private\var\installd\Libray\MobileInstallation\UninstalledApplications.plist

DAAP.sqlitedb

- DAAP – Digital Audio Access Protocol for sharing media across a local network
- Path - \private\var\mobile\library\caches\com.apple.appstored\DAAP.sqlitedb
  - Lists all apps purchased by particular Apple ID(In any Device)
  - Appears added in IOS 12
  - Lists the user that bought in a group use (family)

AppPurchaseHistory.6.sqlitedb

- Path - \private\var\mobile\Library\caches\com.apple.storeservices\AppPurchaseHistory.6.sqlitedb
- Similar to DAAP
- Also found in the older versions IOS
- Includes original purchase date

Screen Time

- Path - \private\var\mobile\Library\Application Support\com.apple.remotemanagementd\RMAdminStore-Local.sqlite
- Added in IOS-12
- Tracks Daily usage History of Apps
- Only stores the last 7 Days for times, app notifications and on-screen time.
- Synced applications (though App is not used but it is reporting to screen time)

PowerLog.PLSQL

- Stores much amount of Data
- Tracks app usage and deletion times
- Further info can be obtained from https://github.com/mac4n6/APOLLO

- **Note:** Lists offloaded apps as deleted (caeful!)
  Timestamps didn't appear as accurate and different from table to table

KnowledgeC.db

- Based on C
- Useful to track application install/Uninstall dates/times
- Application in focus (even after removal)
- Best location to check for persistence of malicious Apps

DataUsage.sqlite

- Path – private\var\wireless\Library\Databases\DataUsage.sqlite
- Also found in iTunes backups and full file system
- Keeps longer records of deleted apps
- Tracks several usage timestamps

- **Note :** Tracks only cellular data usage (app must be used once on cellular network to make an entry)

Netusage.sqlite

- Path – private/var/networkd/netusage.sqlite
- Almost identical structure as datausage.sqlite
- Better at clearing deleted apps
- Tracks WiFi/Cellular/Wired data sizes
- Multiple potential timestamps

Timelining Activity IOS

App Puchase Times	→ DAAP / AppPurchase.6.sqlite
Potential Install Times	→ Mobile Installation Logs
Usage / Connection Times	→ DataUsage / NetUsage / PowerLog
Times in Focus (Last 7-30 days)	→ KnowledgeC / ScreenTime
Deleted Time	→ Mobile Installation Logs / DeletedApplications.plist / PowerLog