Android™ App Forensic Evidence Database (AndroidAED)

Chen Shi, Chris Chao-Chun Cheng, Brody Concannon, Neil Zhenqiang Gong, and Yong Guan

National Institute of Standards and Technology

Center of Excellence

IOWA STATE UNIVERSITY

csafe
Center for Statistics and Applications in Forensic Evidence

Acknowledgement: Barbara Guttman, Michael Ogata, and James Lyle (NIST)

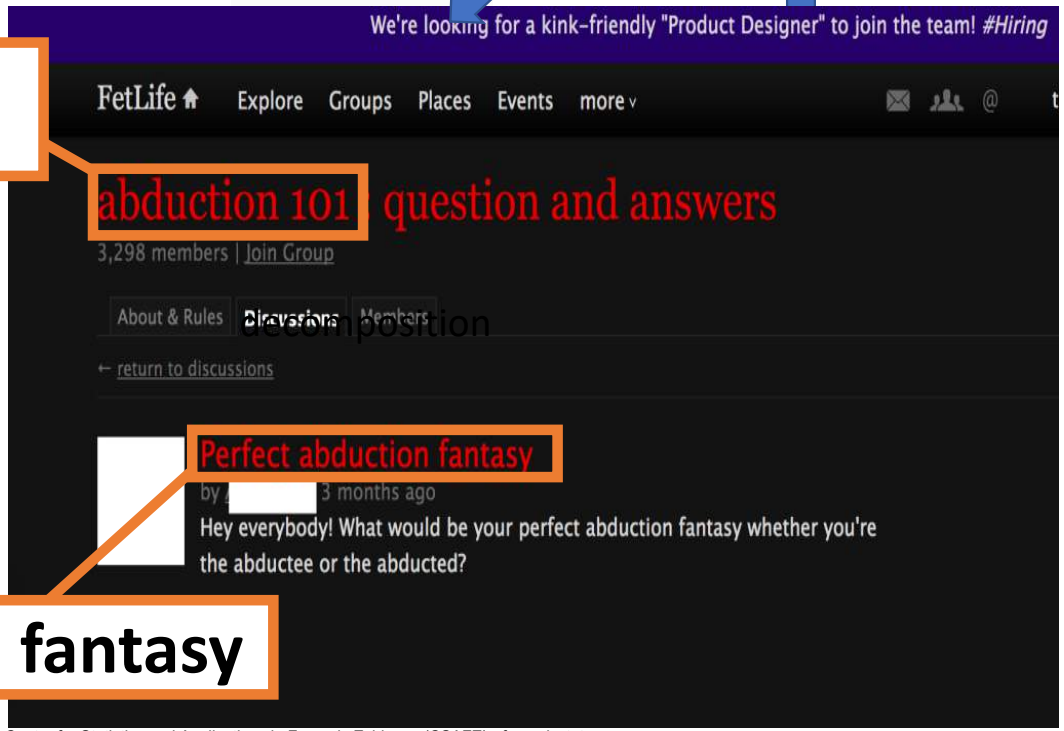
UIUC Chinese Scholar Kidnapping

Research funded by the Center for Statistics and Applications in Forensic Evidence (CSAFE) - forensicstats.org

Mobile App's Evidence: UIUC Kidnapping

Obtain the suspect's mobile device → Extract the file system image → Identify evidence in the image

abduction 101



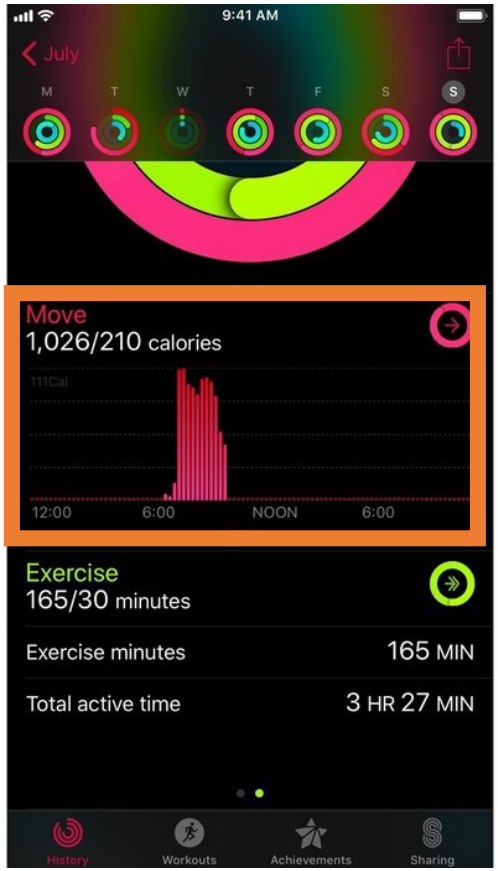
Perfect abduction fantasy

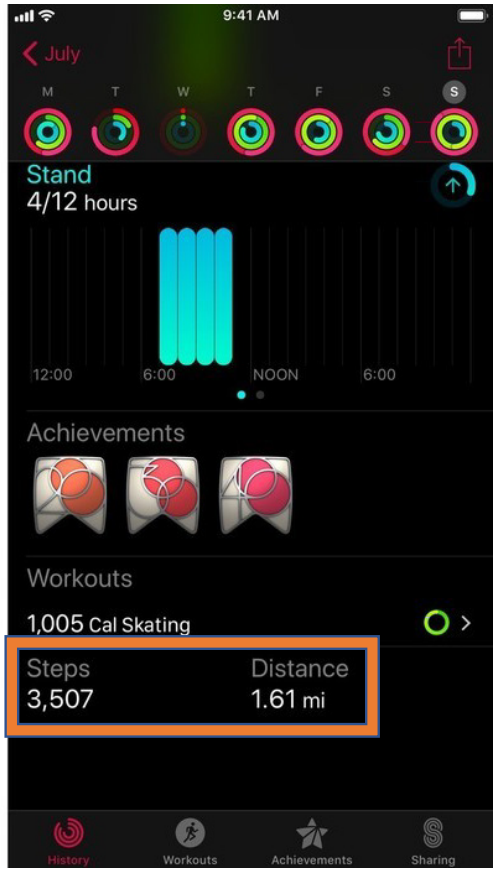
Research funded by the Center for Statistics and Applications in Forensic Evidence (CSAFE) - forensicstats.org

Rape and Murder in Germany

Research funded by the Center for Statistics and Applications in Forensic Evidence (CSAFE) - forensicstats.org

Mobile App's Evidence: Rape and Murder





Research funded by the Center for Statistics and Applications in Forensic Evidence (CSAFE) - forensicstats.org

Mobile Forensics Problems

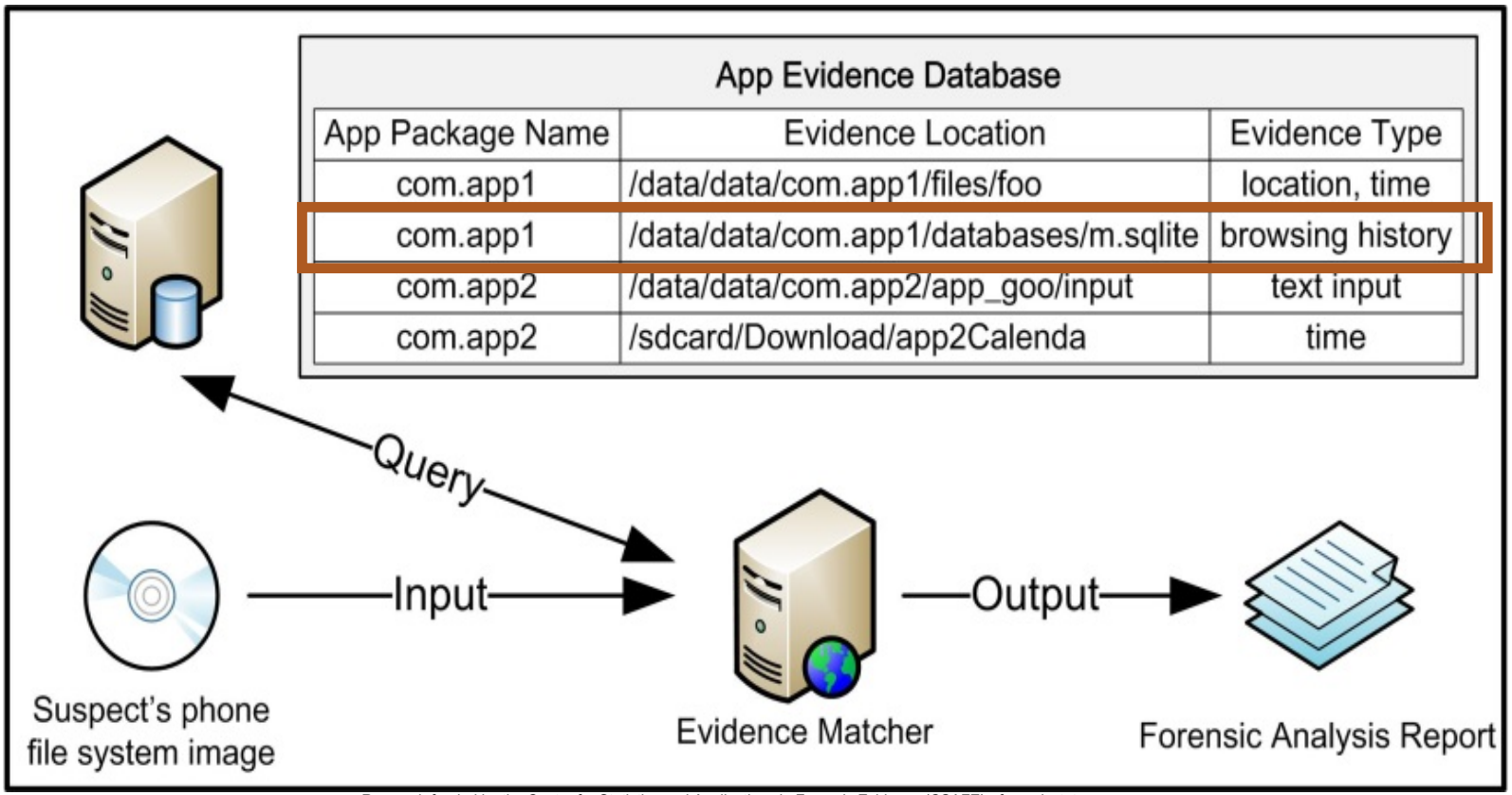
1. Given an app, what kinds of information will be collected and where will it be stored?

2. After the app is updated, what are the changes of the evidentiary data?

3. What kinds of evidence stored in the suspect's device? Where they are?

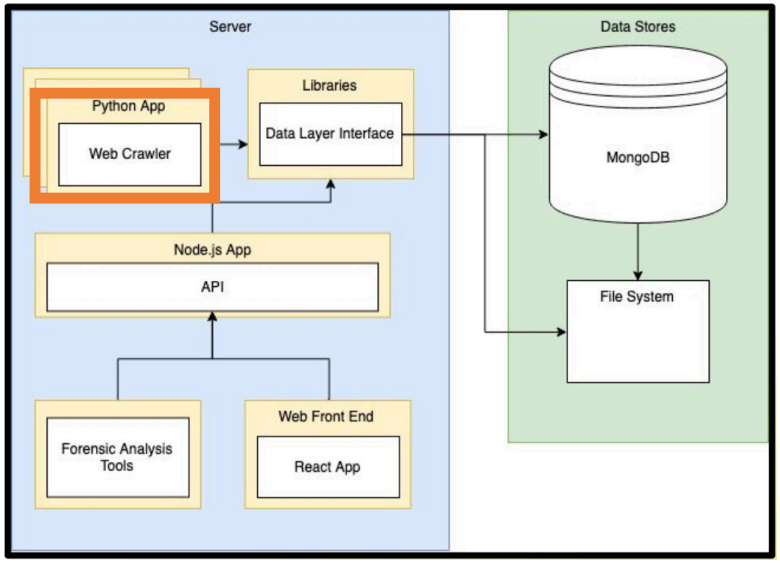
Research funded by the Center for Statistics and Applications in Forensic Evidence (CSAFE) - forensicstats.org

App Evidence Database



Research funded by the Center for Statistics and Applications in Forensic Evidence (CSAFE) - forensicstats.org

Design and Implementation



System Diagram

Forensic Android App Database

Keyword: Submit Upload

applications : 299

versions : 1402

Store : Aptoide
Number of Apps : 11

Store : ApkPure
Number of Apps : 143

Store : APKMirror
Number of Apps : 80

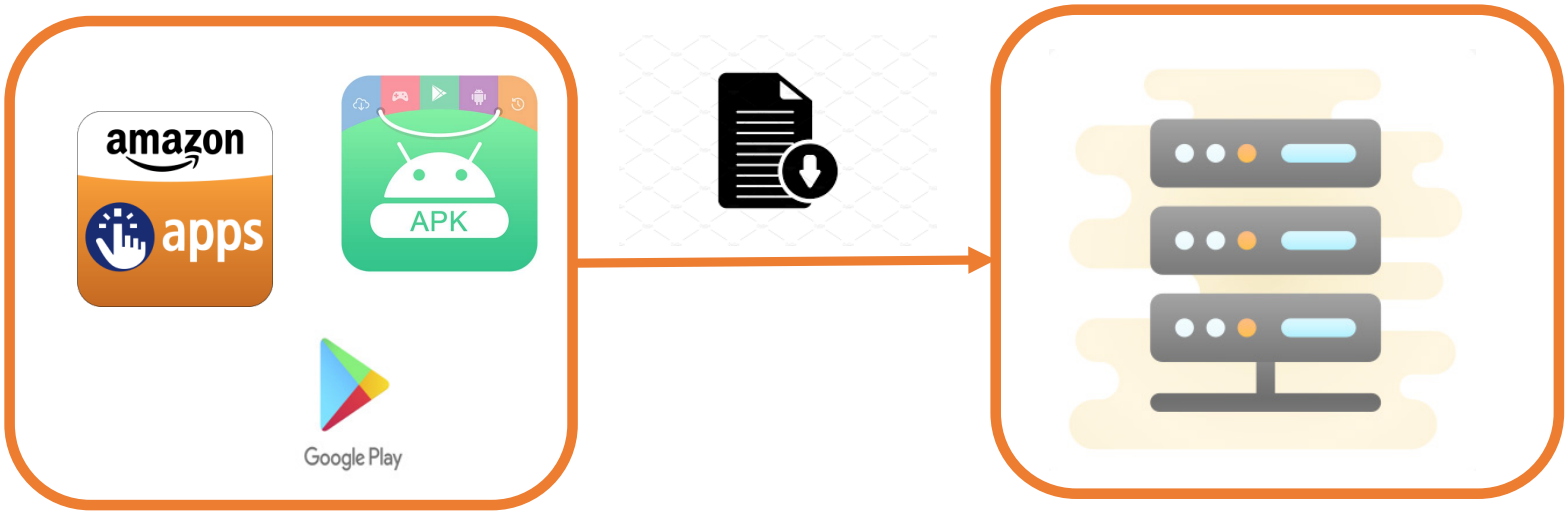
Store : GooglePlay
Number of Apps : 65

Website UI

Research funded by the Center for Statistics and Applications in Forensic Evidence (CSAFE) - forensicstats.org

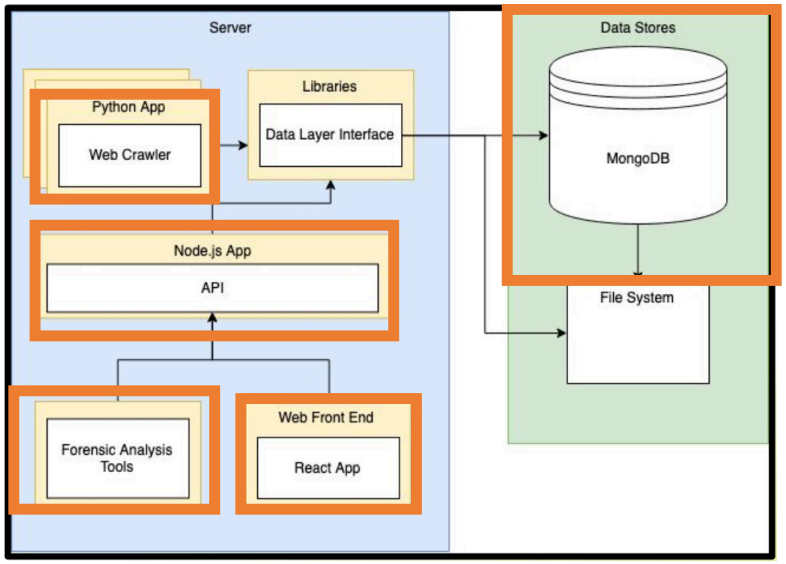
App Crawlers Development

- 54 App Markets: Google Play Store, ApkPure, ApkMirror
- Versions, MD5 hash, Permission list, Release date …



Research funded by the Center for Statistics and Applications in Forensic Evidence (CSAFE) - forensicstats.org

Design and Implementation



System Diagram

Forensic Android App Database

Keyword: Submit Upload

applications : 299

versions : 1402

Store : Aptoide
Number of Apps : 11

Store : ApkPure
Number of Apps : 143

Store : APKMirror
Number of Apps : 80

Store : GooglePlay
Number of Apps : 65

Website UI

Research funded by the Center for Statistics and Applications in Forensic Evidence (CSAFE) - forensicstats.org

enter keyword to search

Forensic Android App Database

Keyword: Chrome Submit Upload

App Name

App Name: google chrome: fast & secure

Developer: Google LLC

Package: Google LLC

Store: GooglePlay

Category: Communication

URL: https://play.google.com/store/apps/details?id=com.android.chrome

App Name: google chrome: fast & secure

Developer: Google LLC

Package: Google LLC

Store: ApkPure

Category: Communication APP

URL: https://apkpure.com/google-chrome-fast-secure/com.android.chrome

App Name: google chrome: fast & secure

Developer: Google LLC

Package: Google LLC

Store: ApkMirror

Category: Communication APP

URL: http://apkpure.com/google-chrome-fast-secure/com.android.chrome

various sources

Research funded by the Center for Statistics and Applications in Forensic Evidence (CSAFE) - forensicstats.org

Forensic Android App Database

Select...

store_id : GooglePlay

app_name : BeOn PTT

version : 6.4.6.24 (R6E05)

apk_type : APK

file_size : 8.2 MB

requirements : 4.1 and up

publish_date : 2019-03-13T00:00:00.000Z

patch_notes : This la
CS24 phone. Consoli
changes.

MD5 : 6b5a193ab88

SHA1 : b3081e2d95

SHA256 :
9c5e022bc22ee2a7ee02fa6a50f54a67a6539044640212d2a68afe54567a4a0d

permissions : undefined android.permission.READ_LOGS
android.permission.FOREGROUND_SERVICE android.permission.VIBRATE
android.permission.RECORD_AUDIO
android.permission.RECEIVE_BOOT_COMPLETED
android.permission.WRITE_EXTERNAL_STORAGE
android.permission.BROADCAST_STICKY
android.permission.ACCESS_FINE_LOCATION com.harris.rf.USE_LMR_CONTROLS
android.permission.ACCESS_COARSE_LOCATION android.permission.INTERNET
android.permission.ACCESS_NETWORK_STATE
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS
android.permission.WAKE_LOCK android.permission.ACCESS_WIFI_STATE
android.permission.MODIFY_AUDIO_SETTINGS android.permission.CAMERA
android.permission.BLUETOOTH android.permission.READ_PHONE_STATE
com.google.android.providers.gsf.permission.READ_GSERVICES

app_package_name : com.harris.rf.beonptt.android.ui

version : undefined

file path : /data/data/com.harris.rf.beonptt.android.ui/beonptt.log

file evidence types : Location,DeviceID

app_package_name : com.harris.rf.beonptt.android.ui

version : undefined

file path : /data/data/com.harris.rf.beonptt.android.ui/beonptt.log

file evidence types : Location,DeviceID

version : undefined

file path :
/data/data/com.harris.rf.beonptt.android.ui/shared_prefs/com.harris.rf.beonptt.android.ui_preferences

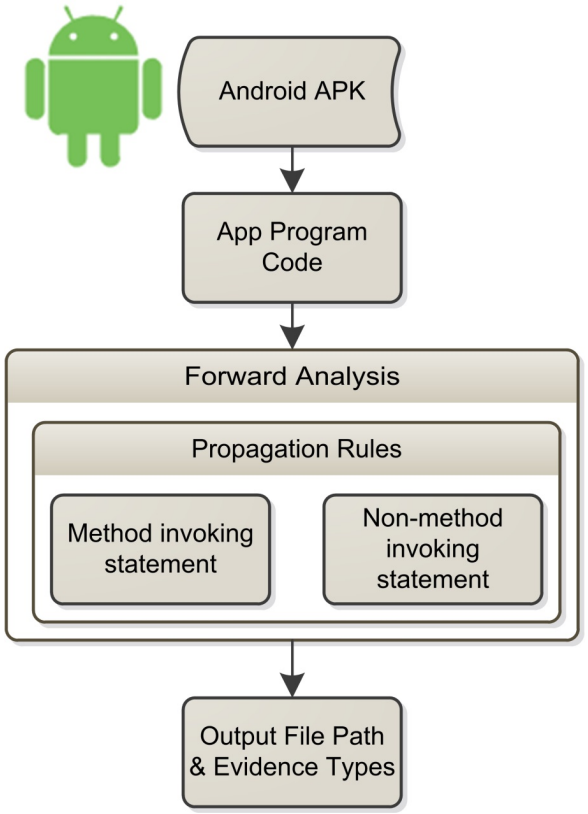
file evidence types :

metadata

evidentiary data

Research funded by the Center for Statistics and Applications in Forensic Evidence (CSAFE) - forensicstats.org

EviHunter - Static Program Analysis

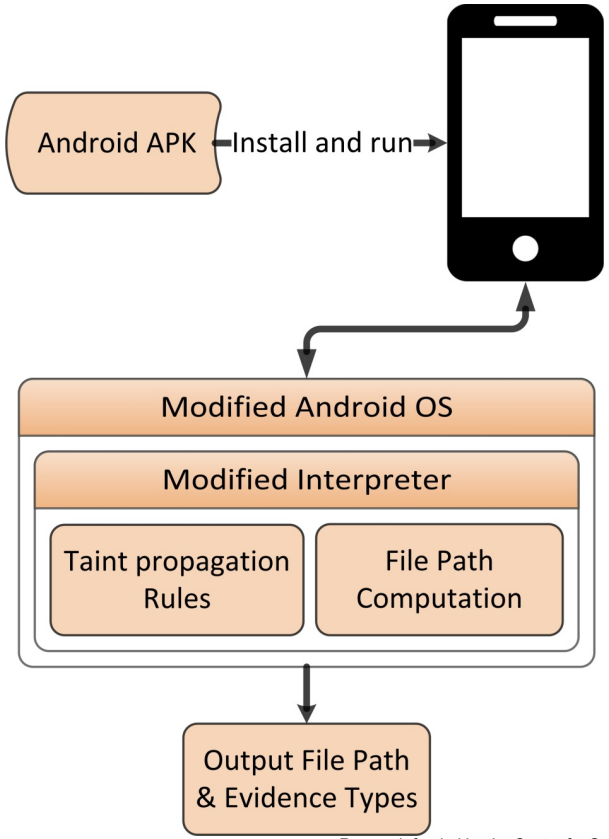


1. Obtain Android Package file
2. Extract app's code
3. Perform forward analysis and apply propagation rules
4. Output when reaching a sink method

Chris Chao-Chun Cheng, Chen Shi, Neil Zhenqiang Gong, and Yong Guan, "EviHunter: Identifying Digital Evidence in the Permanent Storage of Android Devices via Static Analysis," in *ACM CCS* 2018

Research funded by the Center for Statistics and Applications in Forensic Evidence (CSAFE) - forensicstats.org

EviHunter - Dynamic Program Analysis



Preprocessing:

Install customized Android OS on device

For **each app**:

1. Install and run it on device carried modified OS
2. Output when reaching a sink method

Zhen Xu, Chen Shi, Chris Cheng, Neil Gong and Yong Guan, "A Dynamic Taint Analysis Tool for Android App Forensics," in *SADFE 2018*

Research funded by the Center for Statistics and Applications in Forensic Evidence (CSAFE) - forensicstats.org

Case Study - Airpush Ads

Source:https://airpush.com/about/

Research funded by the Center for Statistics and Applications in Forensic Evidence (CSAFE) - forensicstats.org

Case Study - Airpush Ads

Hourly Tracking

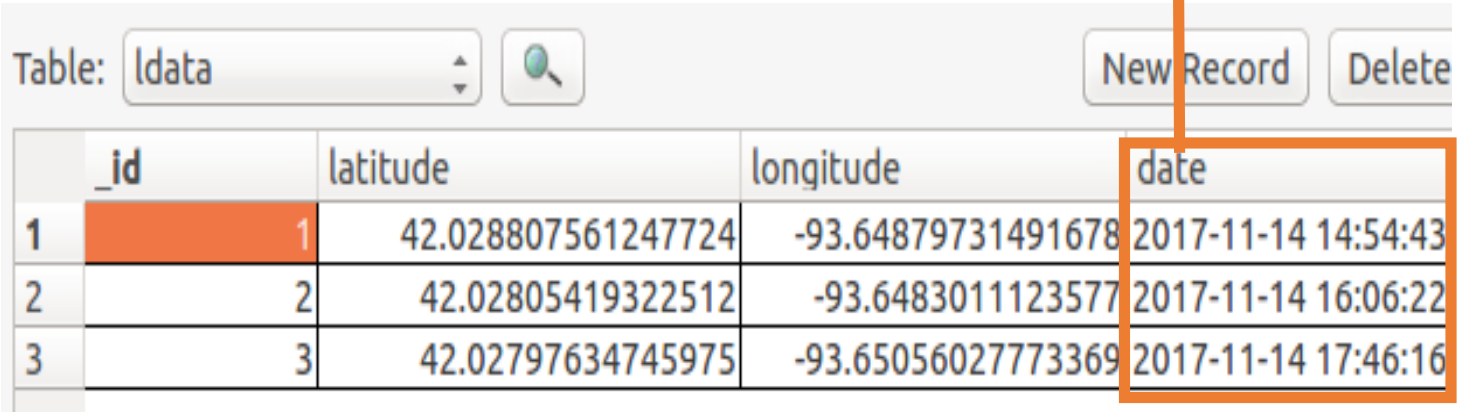


Table: ldata

New Record | Delete

	_id	latitude	longitude	date
1	1	42.028807561247724	-93.64879731491678	2017-11-14 14:54:43
2	2	42.02805419322512	-93.6483011123577	2017-11-14 16:06:22
3	3	42.02797634745975	-93.65056027773369	2017-11-14 17:46:16

133 apps:

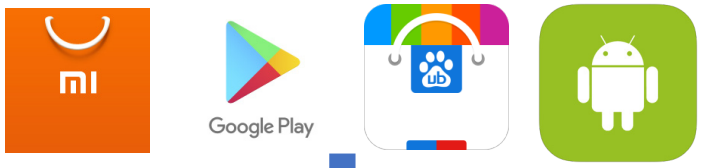
Path: /data/data/<package name>/databases/ldata.db

Evidence Type: Location and Time

Research funded by the Center for Statistics and Applications in Forensic Evidence (CSAFE) - forensicstats.org

Workflow of Building & Updating AED

Step1. Crawl Apps from markets



Step2. Apply EviHunter to generate result

Step3. Upload apps, metadata, forensic analysis result

Research funded by the Center for Statistics and Applications in Forensic Evidence (CSAFE) - forensicstats.org

Summary and Future Directions

- Save time and move fast in real-world cases.
- Up-to-date forensic analysis result of real-world apps.

Research funded by the Center for Statistics and Applications in Forensic Evidence (CSAFE) - forensicstats.org