



Android™ App Forensic Evidence Database (AndroidAED)

NIST
National Institute of
Standards and Technology
Center of Excellence

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

**IOWA STATE
UNIVERSITY**



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



UIUC Chinese Scholar Kidnapping



YINGYING ZHANG, 27, VISITING SCHOLAR FROM CHINA

MISSING GIRL

Urbana-Champaign Area

If you spot her or
see this car, CALL
911 or 217-333-1216

non emergency contact: police@illinois.edu

- 5'3
- shoulder length brown hair
- round glasses
- long-sleeved light-colored shirt
- light blue jeans
- white shoes
- dark cap and a dark blue shoulder bag



same model

Yingying was taken by a black Saturn Astra at Goodwin and Clark on Jun. 9 at 2 pm. She has lost all contact since.





Mobile App's Evidence: UIUC Kidnapping

Obtain the suspect's
mobile device

Extract the file
system image

Identify evidence
in the image

abduction 101

abduction 101 question and answers

3,298 members | [Join Group](#)

[About & Rules](#)

[Discussions](#)

[Members](#)

[← return to discussions](#)

Perfect abduction fantasy

by [redacted] 3 months ago

Hey everybody! What would be your perfect abduction fantasy whether you're the abductee or the abducted?

Perfect abduction fantasy

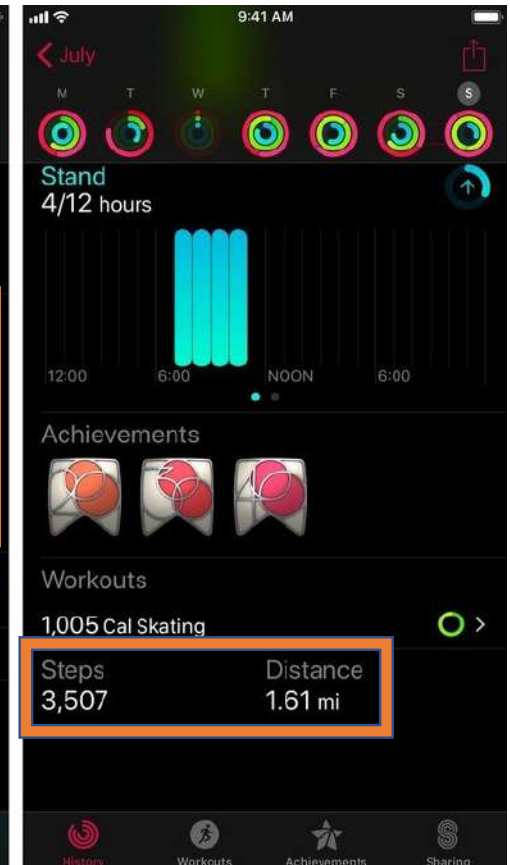


Rape and Murder in Germany





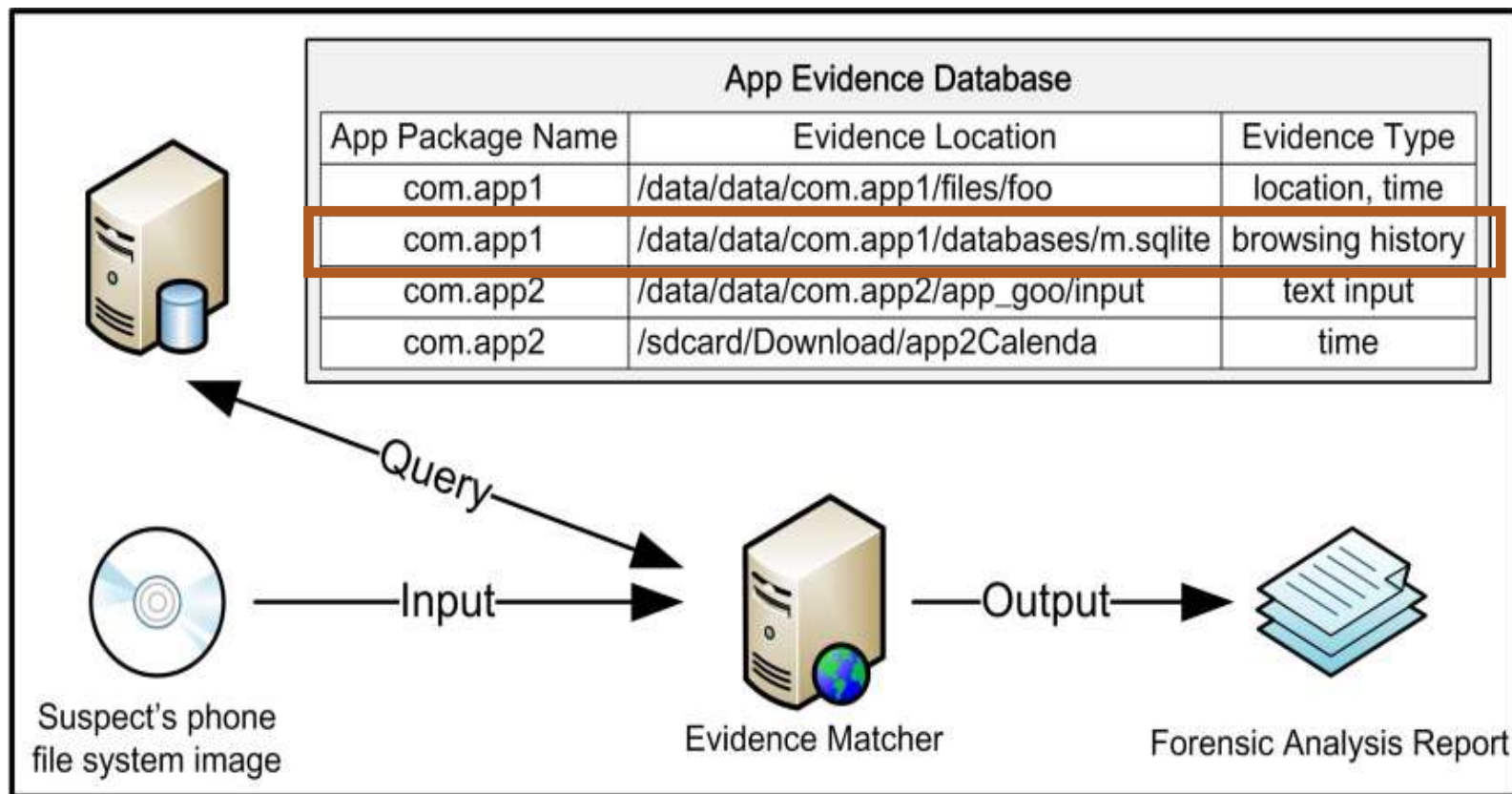
Mobile App's Evidence: Rape and Murder



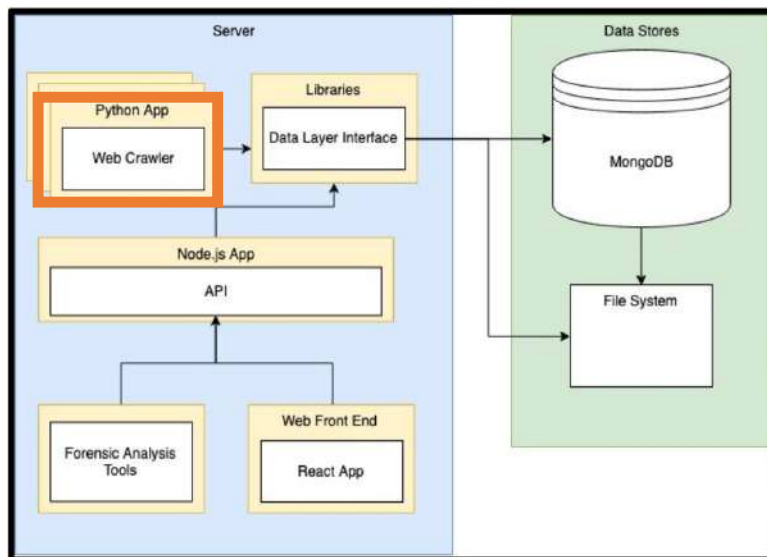
Mobile Forensics Problems

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?

App Evidence Database



Design and Implementation



System Diagram

Forensic Android App Database

Keyword:

applications : 299

versions : 1402

Store : Aptoide
Number of Apps : 11

Store : ApkPure
Number of Apps : 143

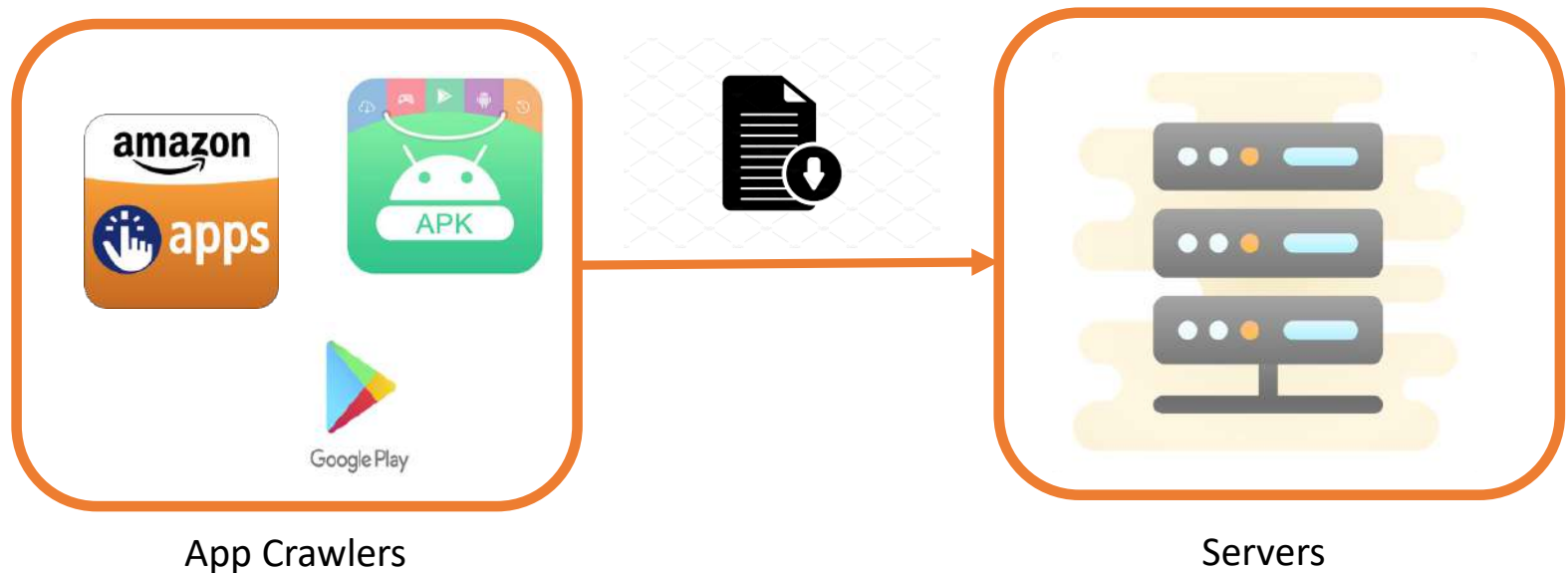
Store : APKMirror
Number of Apps : 80

Store : GooglePlay
Number of Apps : 65

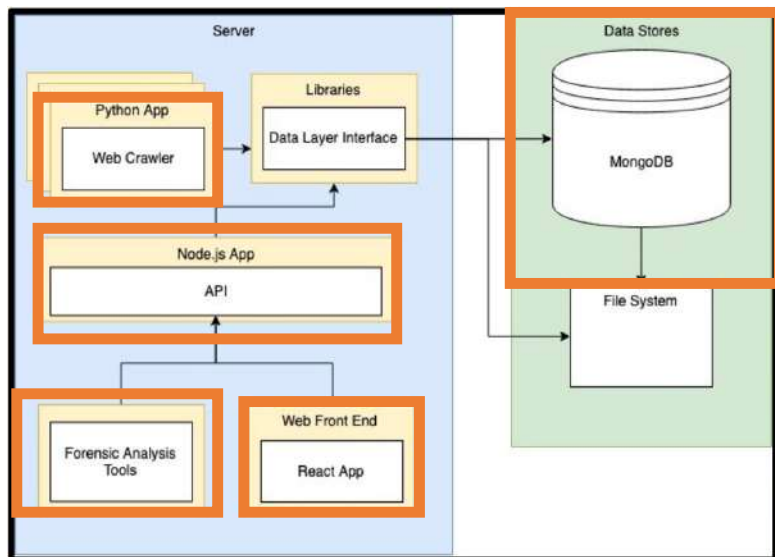
Website UI

App Crawlers Development

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



Design and Implementation



System Diagram

Forensic Android App Database

Keyword:

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



enter keyword to search

Forensic Android App Database

Keyword: Chrome

Submit

Upload

App Name

App Name: google chrome: fast & secure

Developer: Google LLC

Packager: Google LLC

Store: GooglePlay

Category: Communication

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

various sources

App Name: google chrome: fast & secure

Developer: Google LLC

Packager: 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

Packager: Google LLC

Store: ApkMirror

Category: Communication APP

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

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 is a patch for CS24 phone. Consolidating changes.

MD5 : 6b5a193ab88

SHA1 : b3081e2d95e

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

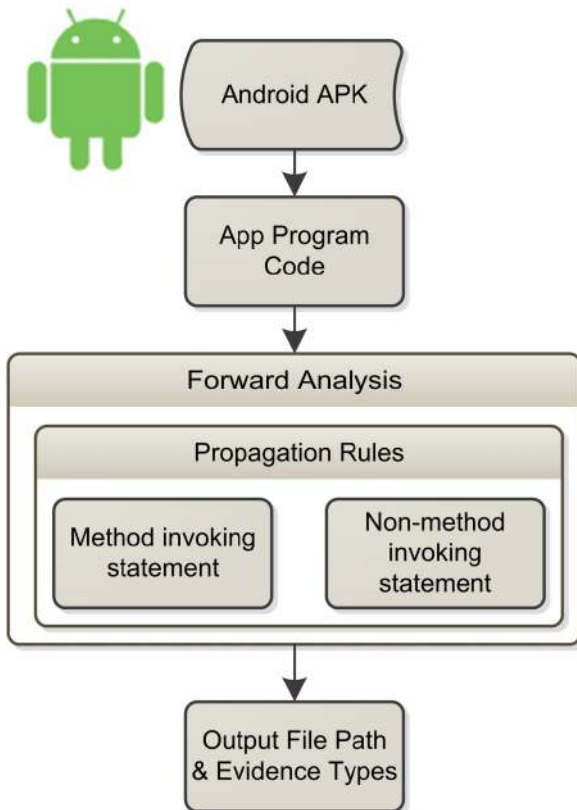
file path : /data/data/com.harris.rf.beonptt.android.ui/shared_prefs/com.harris.rf.beonptt.android.ui_preferences

file evidence types :

metadata

evidentiary data

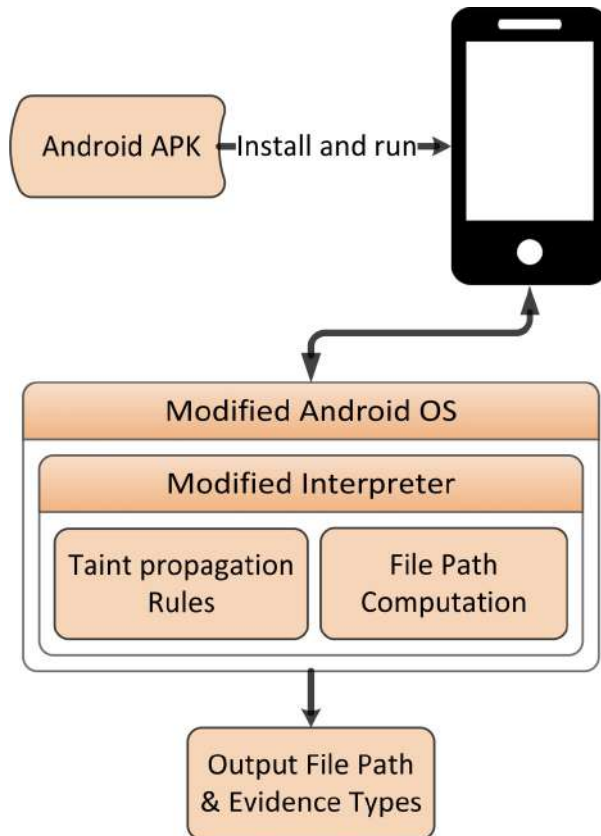
EviHunter - Static Program Analysis



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

EviHunter - Dynamic Program Analysis



Preprocessing:

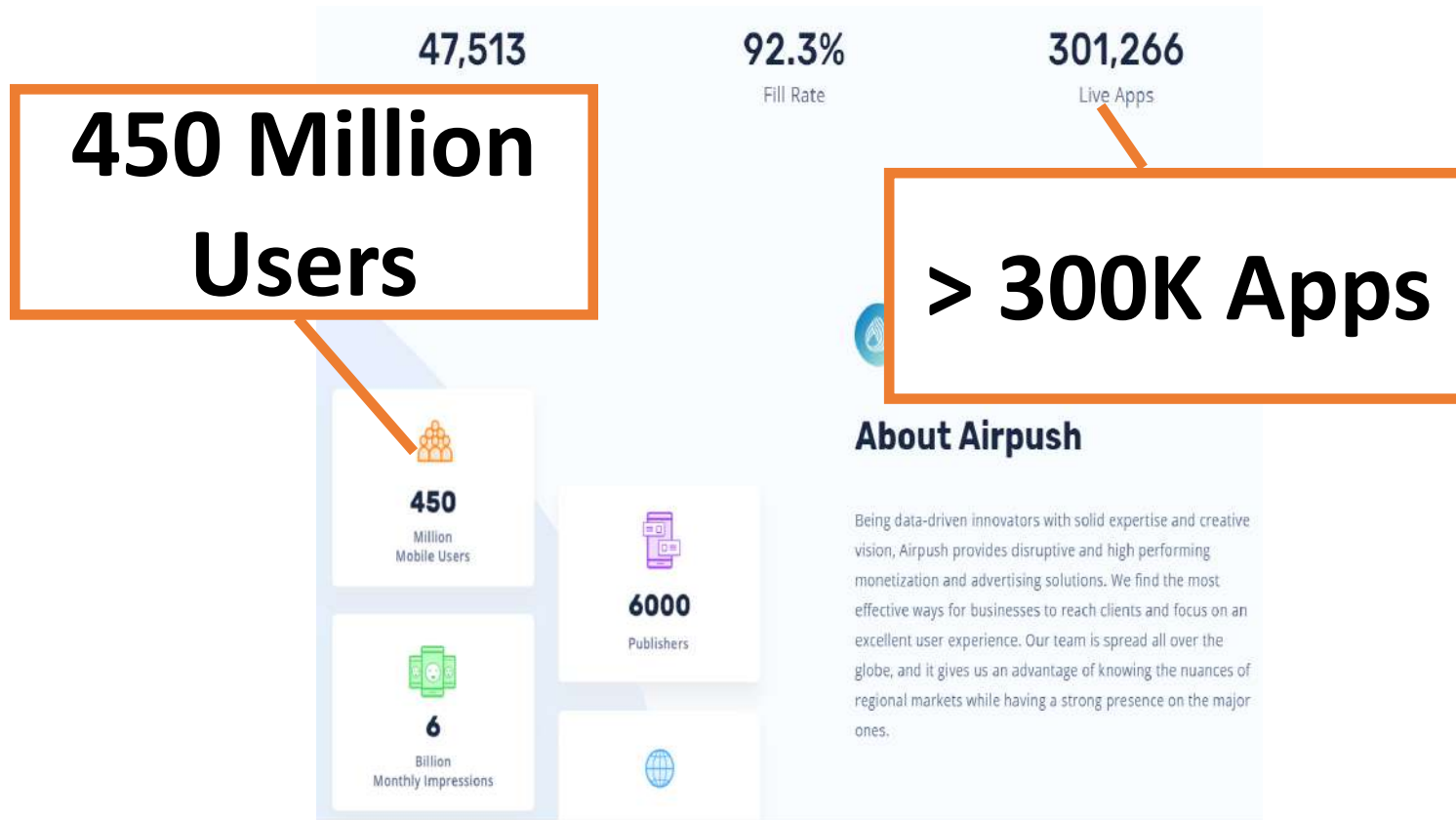
Install customized Android OS on device

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*

Case Study - Airpush Ads



About Airpush

Being data-driven innovators with solid expertise and creative vision, Airpush provides disruptive and high performing monetization and advertising solutions. We find the most effective ways for businesses to reach clients and focus on an excellent user experience. Our team is spread all over the globe, and it gives us an advantage of knowing the nuances of regional markets while having a strong presence on the major ones.

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

Case Study - Airpush Ads

Hourly Tracking

Table: 

	_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

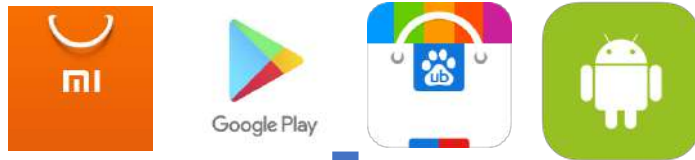
133 apps:

Path: [/data/data/<package name>/databases/ldata.db](#)

Evidence Type: [Location](#) and [Time](#)

Workflow of Building & Updating AED

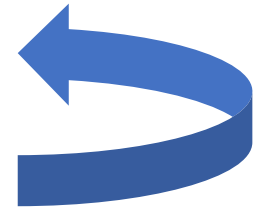
Step1. Crawl Apps
from markets



Step2. Apply EviHunter
to generate result



Step3. Upload apps,
metadata, forensic
analysis result



Summary and Future Directions

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