

Android™ App Forensic Evidence Database

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

Iowa State University
NIST Center of Excellence in Forensic Science – CSAFE

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

**IOWA STATE
UNIVERSITY**



NIST
National Institute of
Standards and Technology
Center of Excellence

Animal Poaching: Washington State 17'



1+ felony charge & 1+ misdemeanor count

Mobile App's Evidence: Animal Poaching

**Text messages
found on suspect's
phone aided
investigation**

Washington Department of Fish & Wildlife investigators seized William Haynes' phone and allegedly found videos, phone messages and communications

**... today we struck a
huge bear ...**

Mom // 2:27 p.m.

Almost home . today we struck a huge bear right after daylight ran it for about 4 hours and the Gps said the dogs...were all sitting on the edge of about a 300 foot cliff. The bear ran right off it into the river dead as hell. From the size of the tracks it was around 350-400 pounds it was a huge bear.

William Haynes // 2:49 p.m.

**... the bear ran right off it into the river
dead as hell...**

mother that hunting dogs
chased a large bear to

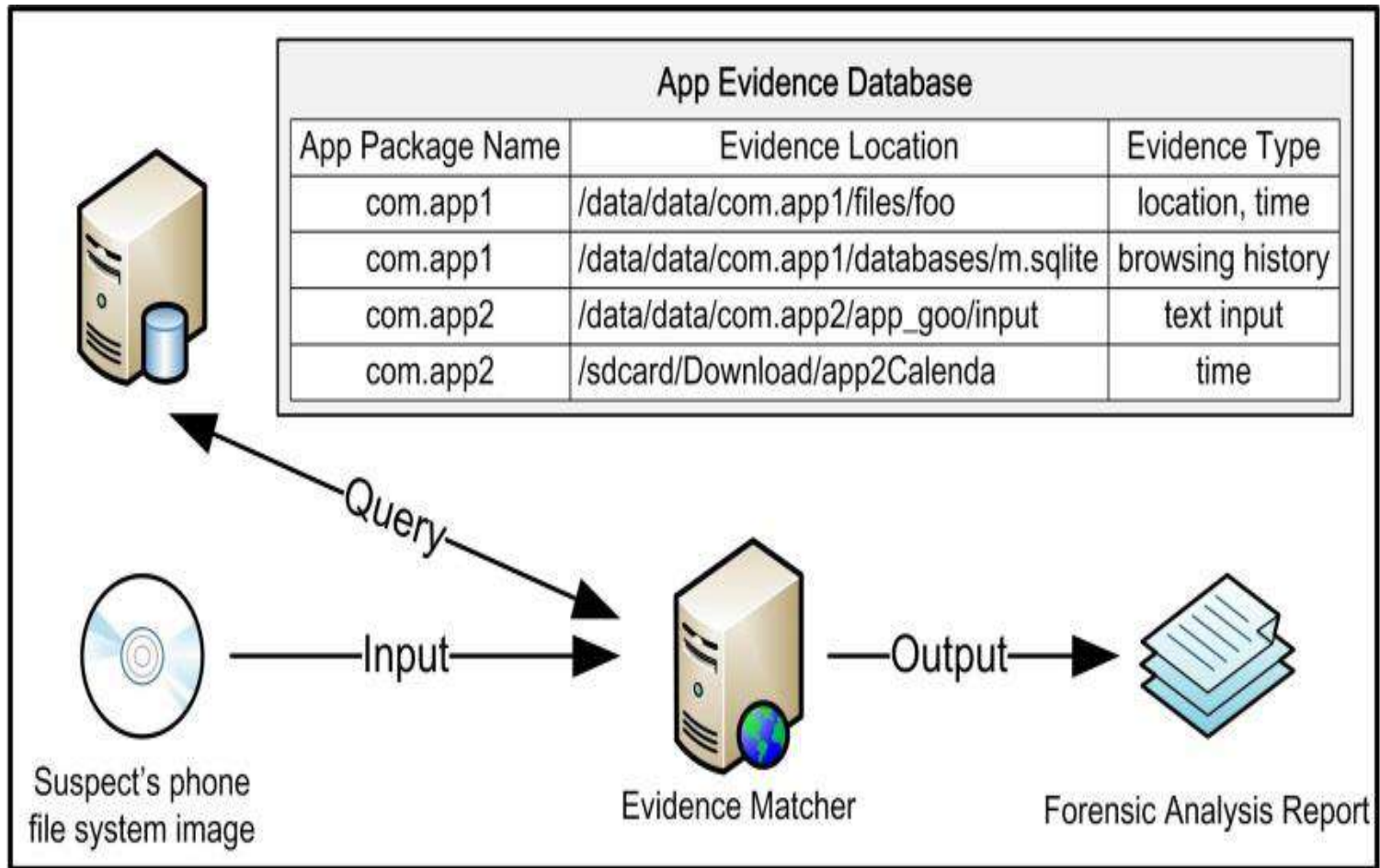
Identify evidence
in the image

Text messages

Mobile Forensics Problems

1. Given an app, what kinds of artifacts 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



Workflow of Updating AED



Crawl Apps from
markets

Update apps, metadata,
forensic analysis result

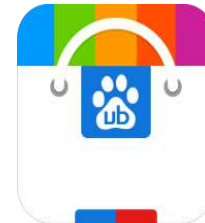


Apply program analysis
and generate result

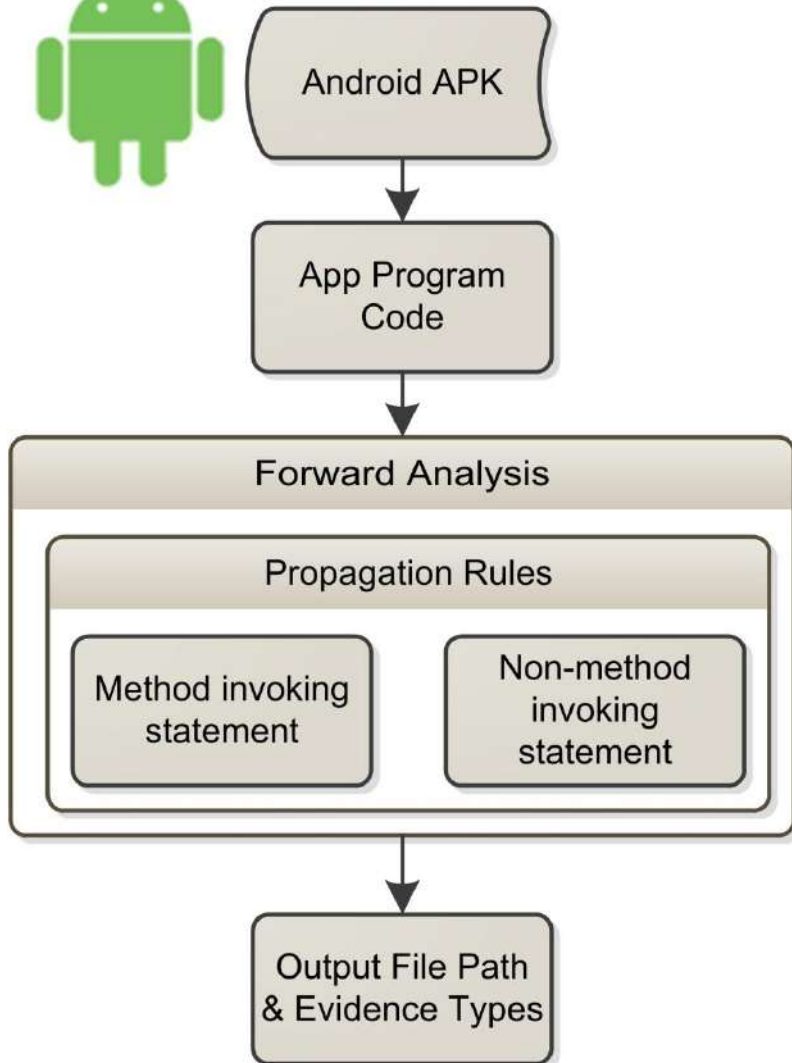


App Crawlers Development

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

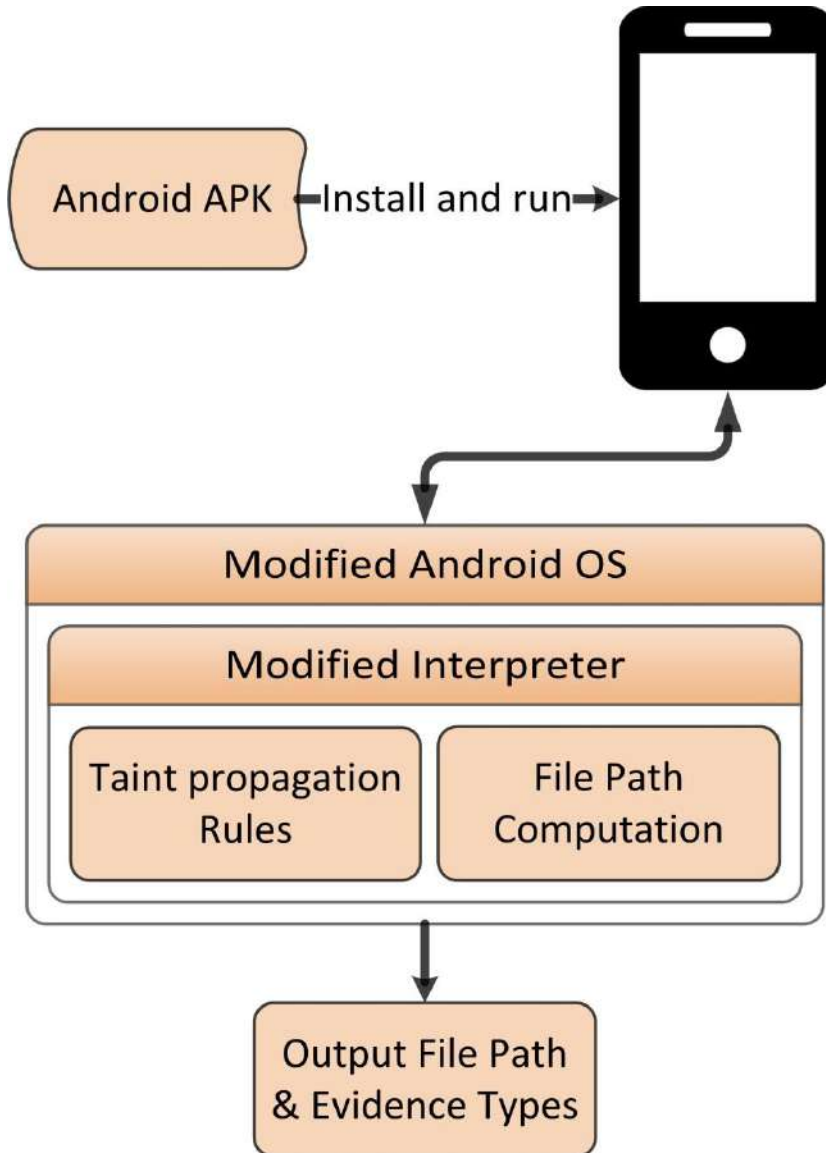


Static Program Analysis: EviHunter



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

Dynamic Program Analysis



Preprocessing:

Install customized Android OS on device

For each app:

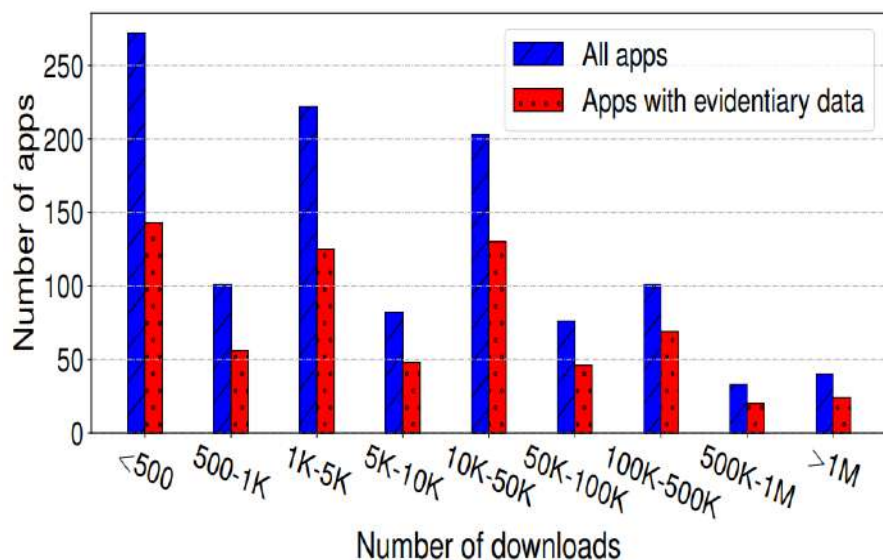
1. Install and run it on device carried modified OS
2. Output when reaching a sink method (file system)

Real-world Apps Evidence (1)

App	Evidence Location	Evidence Type
Twitter	/data/data/com.twitter.android/cache/.fcaches/fileStreamCacheDownloader/journal.tmp	Text Input
Instagram	/data/data/com.instagram.android/shared_prefs/rti.mqtt.mqtt_radio_active_time.xml	Location
FB Messenger	/data/data/com.facebook.orca/files/mobileconfig/sessionless.data/0.mctable	Text Input
WhatsApp	/sdcard/Android/data/com.whatsapp/cache/SSLSessionCache/157.240.2.53.443	Location
WhatsApp	/data/user/0/com.whatsapp/shared_prefs/registration.RegisterPhone.xml	Text Input

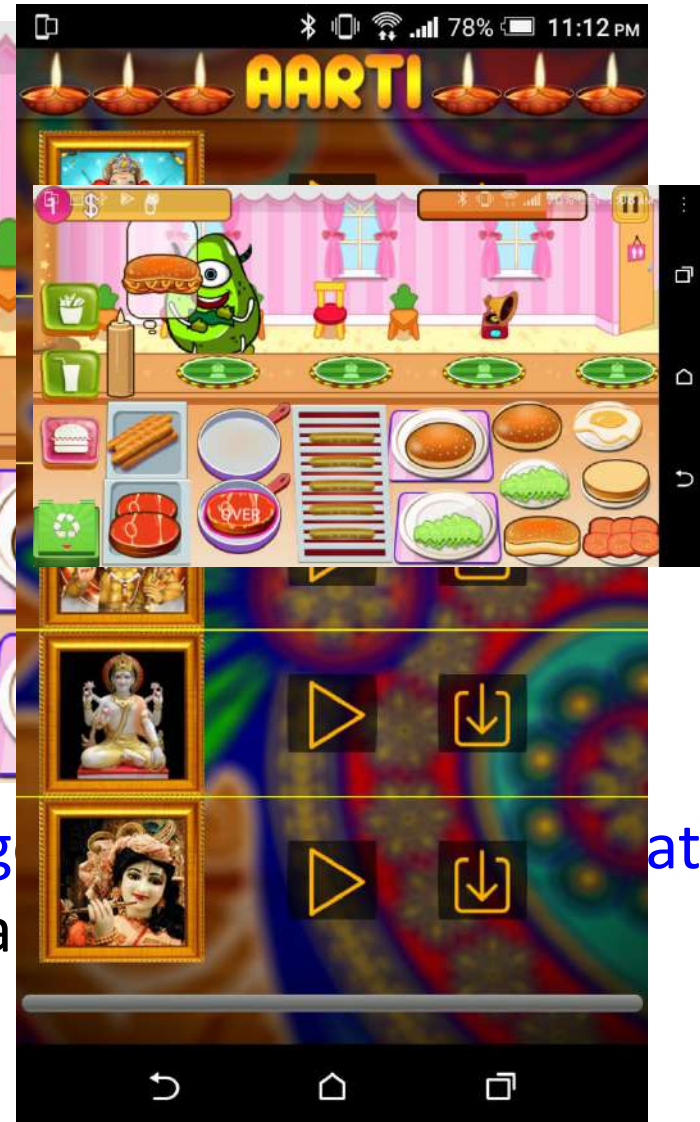
Real-world Apps Evidence (2)

- 8,690 Google Play Store apps
- **SharedPreferences** is the most likely evidentiary file type.
- **Time** is the most type evidence in file system.
- Manual verification: 90% precision and 89% recall.



Evidence Type	SQLite DB	SharedPreferences	Ordinary File
Location	145	195	151
Time	343	1129	435
Visited URL	20	25	19
Text Input	166	411	186

Case Study: Airpush Ads (1)



- 133 reported cases
 - Path: /data/data/<package>
 - Evidence Type: Location and
- Manual verification

ata.db

Case Study: Airpush Ads (2)

Hourly Tracking

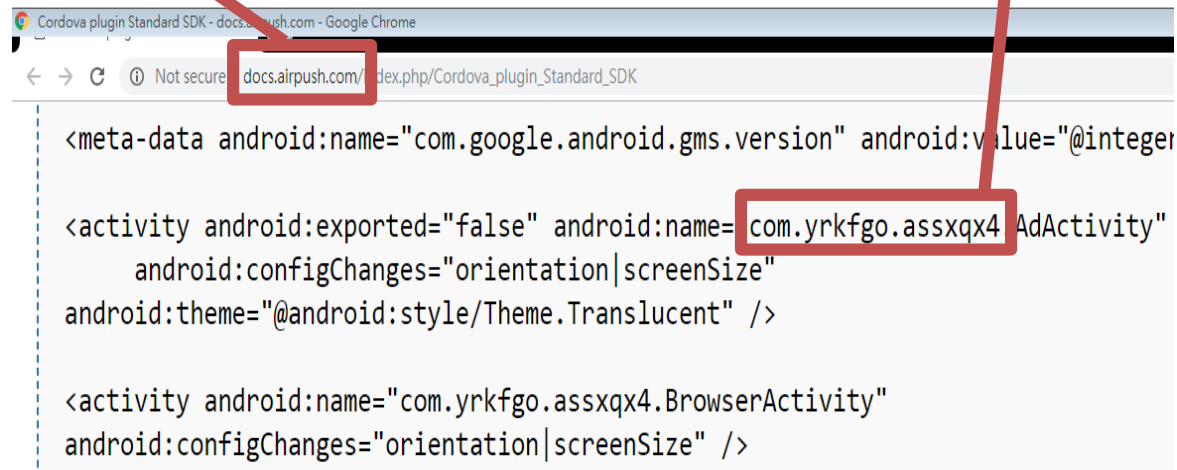
Table: 

	_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

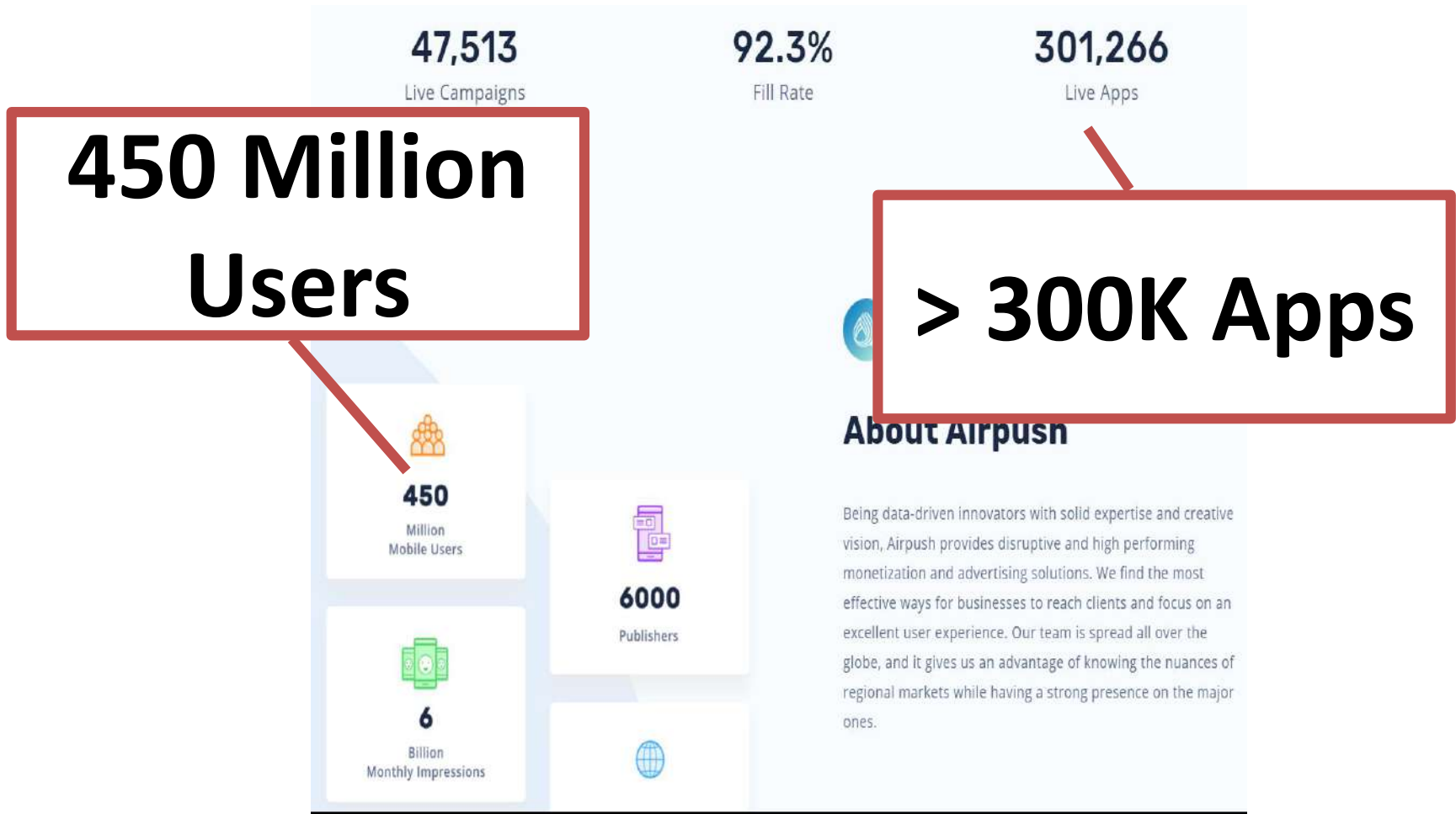
Case Study: Airpush Ads (3)

- Traceback from the class: **com.yrkfgo.assxqx4**

docs.airpush.com



Case Study: Airpush Ads (4)



Conclusion

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

Android App Evidence Database (1)

← → ↻ ⓘ Not secure | sdmay19-38.ece.iastate.edu

Keyword:

App Name

Store	App Name	Developer	Package	Version
ApkPure	google chrome: fast & secure	Google LLC	com.android.chrome	72.0.3626.105
ApkPure	chrome beta	Google LLC	com.chrome.beta	73.0.3683.37
ApkPure	es chromecast plugin	ES Global	com.estrongs.chromecast	1.0
ApkPure	web video cast browser to tv (chrom	InstantBits Inc	com.instantbits.cast.webvideo	4.4.6
GooglePlay	chrome nails	Smartongroup	smartgr.chrome.nails	1.3.3
GooglePlay	chrome river snap	Chrome River Technologies, Inc.	com.chromeriver.crsnap	1.3.4
GooglePlay	living psychometrics	MICRI Consult	com.MicriConsult.Psychometrics	17.0.0
GooglePlay	google chrome: fast & secure	Google LLC	com.android.chrome	Varies with device
GooglePlay	chrome dev	Google LLC	com.chrome.dev	
GooglePlay	iss on live: hd view earth live chrome	PoliLabs	com.polilabs.issonlive	4.5.3

Previous

Page 1 of 1

10 rows ▼

Various sources

Multiple versions

Android App Evidence Database (2)

Search keyword of app

Keyword: PTT Submit

Store	App Name	Developer	Package	Version	Category
GooglePlay	beon ptt	Harris Corporation PSPC	com.harris.rf.beonptt.android.ui		Communication
GooglePlay	zello ptt walkie talkie	Zello Inc	com.loudtalks	Varies with device	Communication

Click to check its evidentiary data

The screenshot shows a web browser window with the address bar displaying "sdmay19-38.ece.iastate.edu". Below the address bar, there is a search bar labeled "Keyword:" containing the text "PTT". To the right of the search bar is a button labeled "Submit".

Below the search bar, there is a table with five columns:

- App Name**
- App Package Name**
- Version**
- File System File Path**
- File System Evidence Types**

The table contains three rows of data, all for the package name "com.harris.rf.beonptt.android.ui". The version for each row is "Varies with device". The file system file paths and evidence types are as follows:

App Name	App Package Name	Version	File System File Path	File System Evidence Types
	com.harris.rf.beonptt.android.ui	Varies with device	/data/data/com.harris.rf.beonptt.android.ui/	Location,DeviceID
	com.harris.rf.beonptt.android.ui	Varies with device	<%unknown>logCatRestart.log	
	com.harris.rf.beonptt.android.ui	Varies with device	/data/data/com.harris.rf.beonptt.android.ui/	

A blue rectangular box highlights the first three rows of the table.