VIDE - Vault App Identification and Extraction System for iOS Devices

By: **Gokila Dorai** (Augusta University), Sudhir Aggarwal (Florida State University), Neet Patel (Florida State University), and Charisa Powell (Florida State University)

From the proceedings of

The Digital Forensic Research Conference

DFRWS 2020 USA

Virtual -- July 20-24

VIDE - Vault App Identification and Extraction System for iOS Devices

Speaker: Dr. Gokila Dorai

Introduction

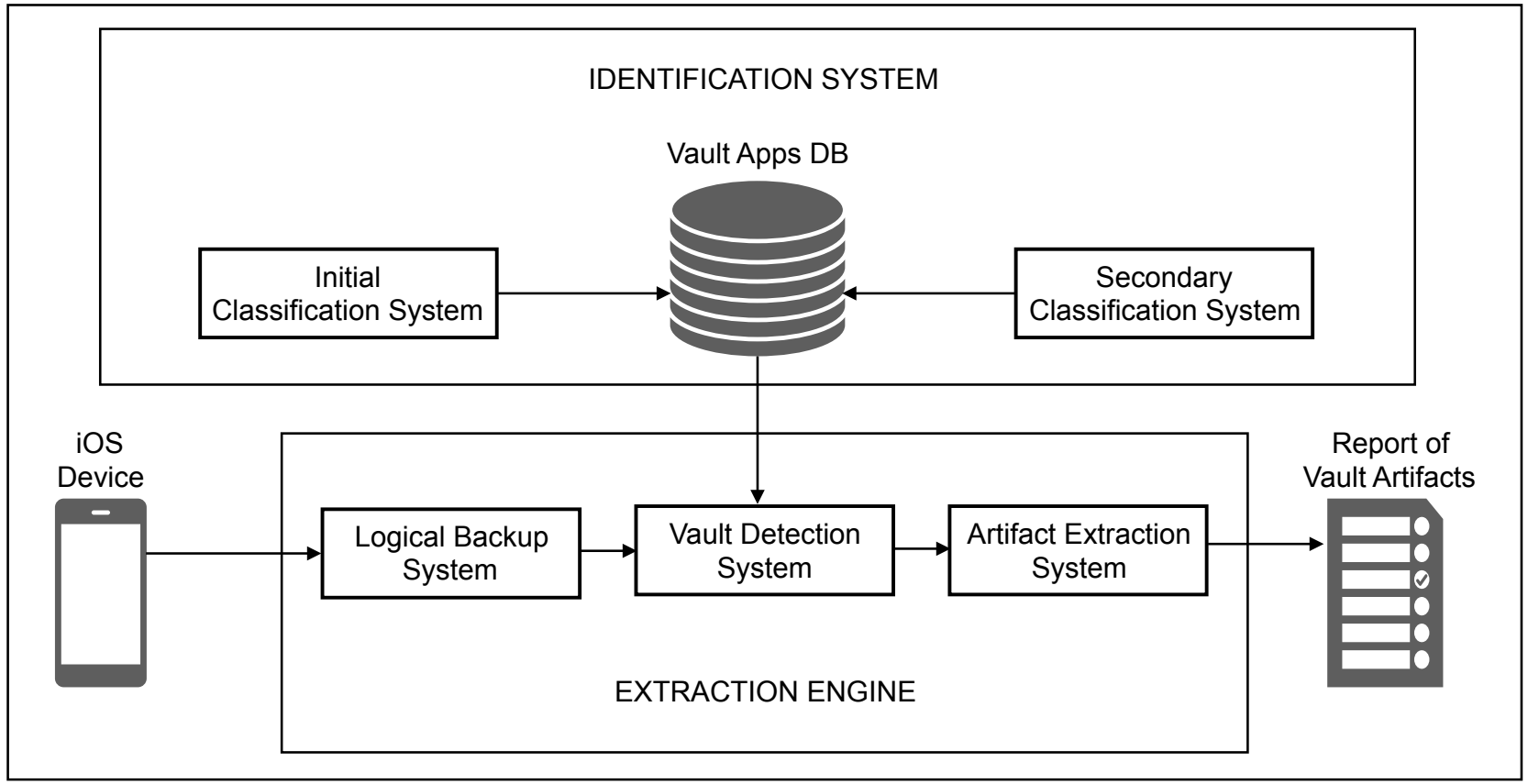
- The term “content hiding app” refers to apps that allow users to hide photos, videos, documents and other files secretly and in a secure way on their smartphones.
- Criminal uses - drug dealing, spying, trafficking, etc.
- Purpose of these apps – Spoofing, Private Browsing, Content-hiding (hides photo, video, notes, messages), Secret audio recording, Password Managing, Decoy, Private Messaging, Censoring

> “ Vault apps hide in plain sight, often mimicking other apps, so keep your eyes open for duplicates. ”

Primary Contributions

- The first in-depth exploration of content hiding apps for iOS devices.
- We have explored the iOS App Store and found several of those applications.
- The capability to do rapid identification of content hiding apps from any App Store, including foreign stores such as in Russia, India and China.
- A lightweight vault app identification system with high accuracy and using only textual description of apps.
- We built an automated “Vault Identifier and Data Extraction” (VIDE) system for content-hiding apps installed on iOS devices.

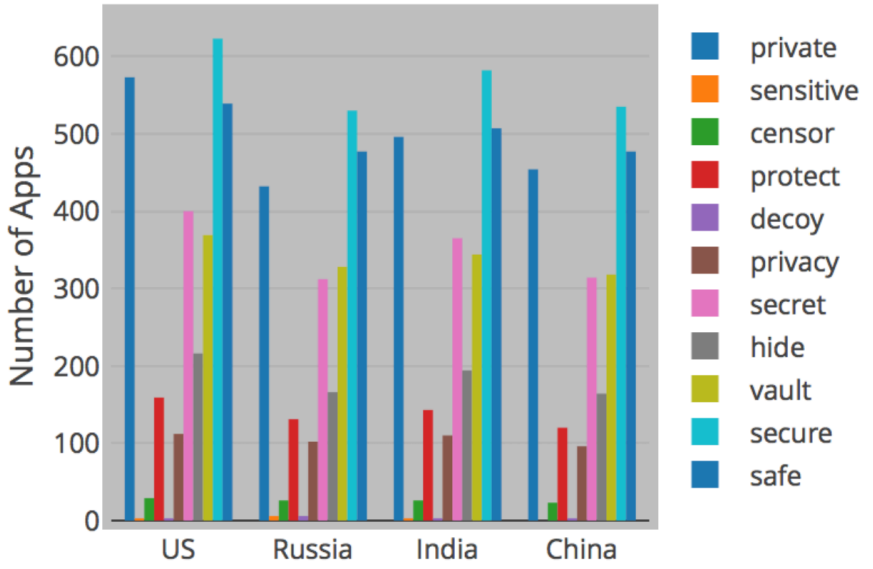
VIDE System Design



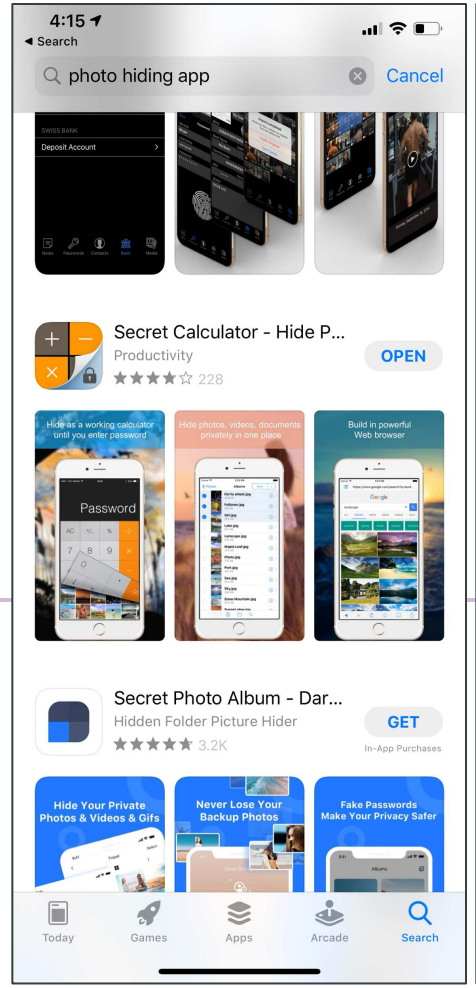
Keywords for Initial Scan

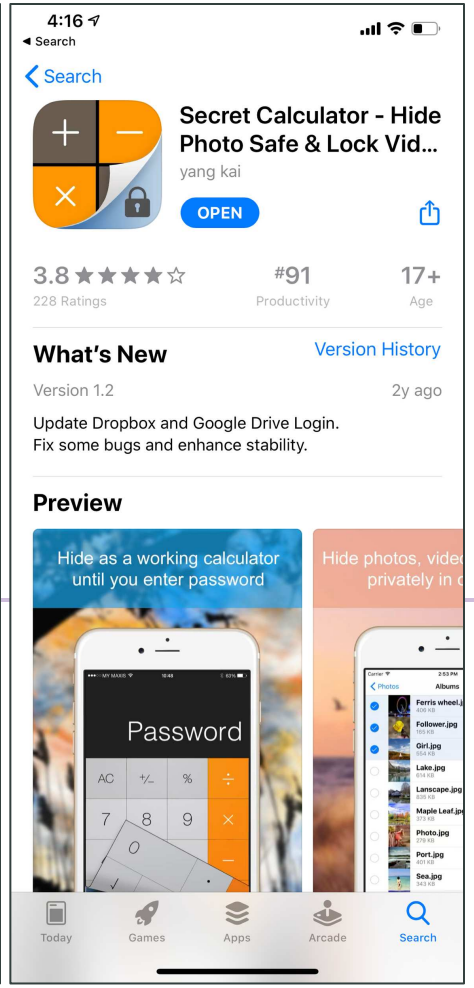
- Initial Scan Set (keywords): [private, sensitive, censor, protect, decoy, privacy, secret, hide, vault, secure, safe]

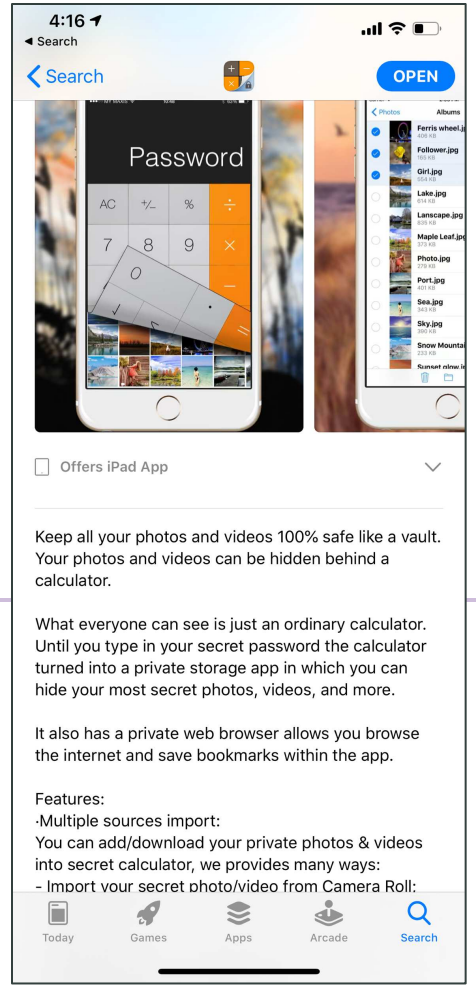
English Keyword (Russian Keyword)
private (ЧастНый)
sensitive (ЧувСТвиТеЛьНый)
censor (цеНЗОР)
protect (ЗащИщаТ)
decoy (МаНОК)
privacy (ОНфИдеНцИаЛьНОСТь)
secret (СеКреТ)
hide (скРЫваТь)
vault (СвОд)
secure (бе3ОПасНый)
safe (бе3ОПаСНО)

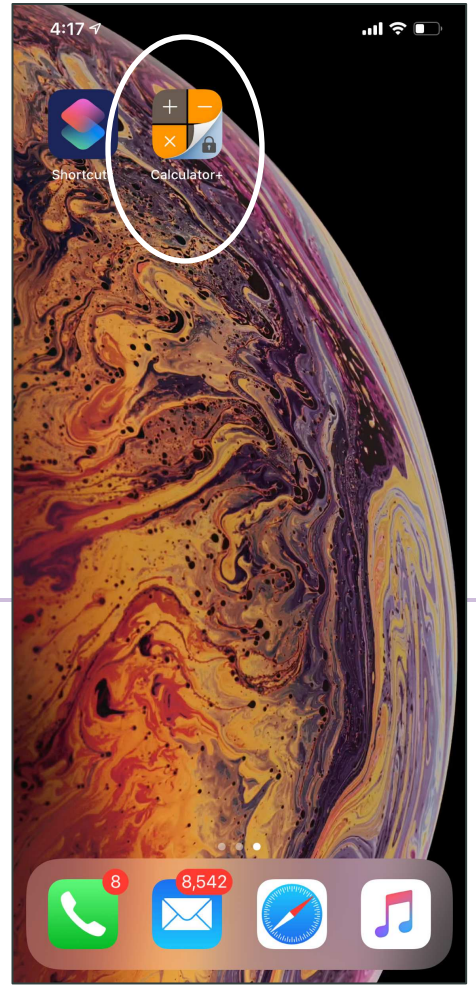


Example App – Secret Calculator

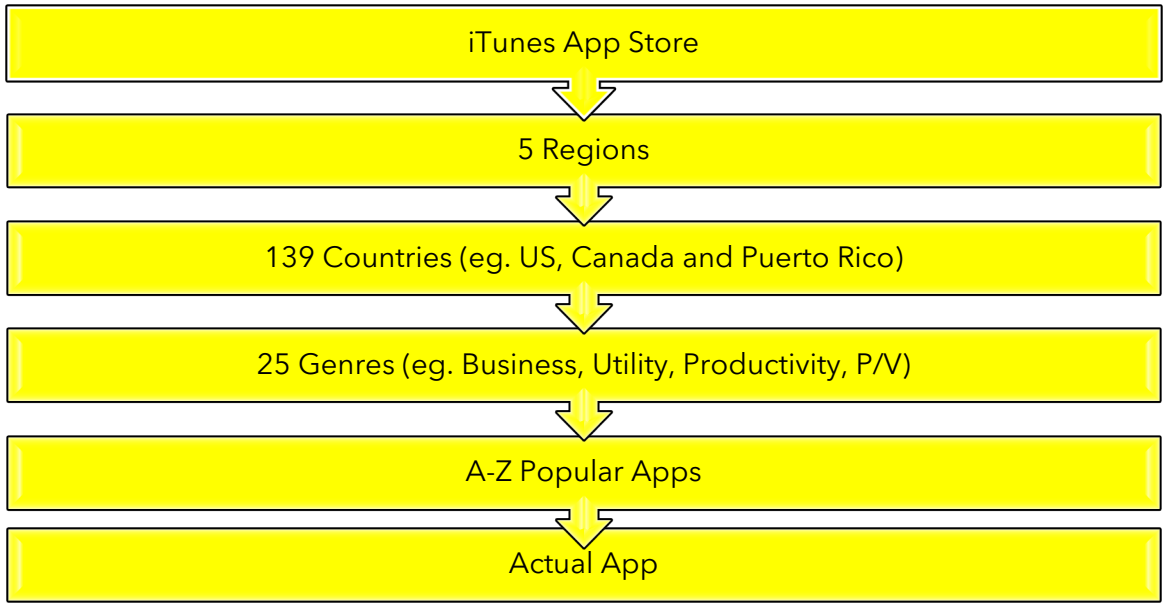


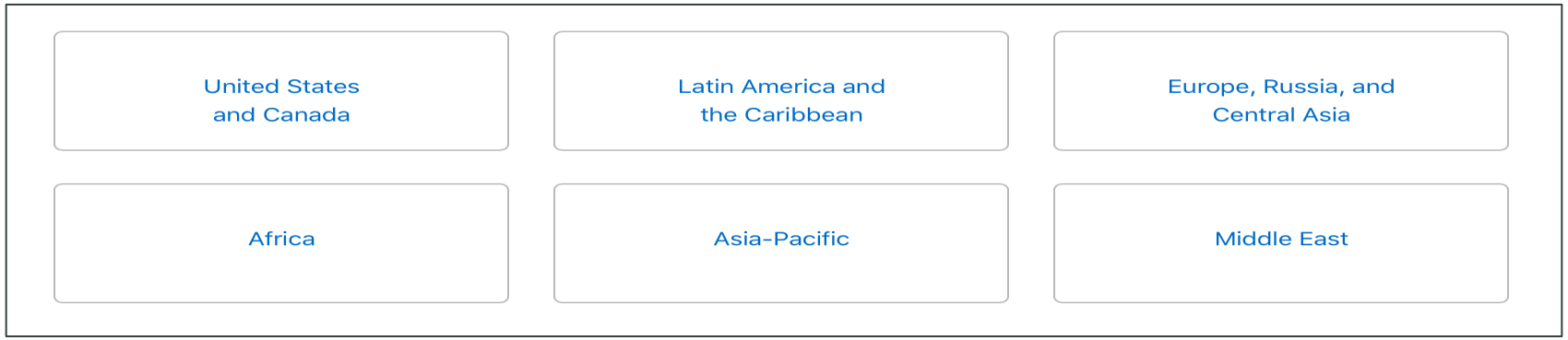






App Store Organization





Initial Identification: Potential Vault Apps

- Web scraping of US App Store to explore popular apps
- https://itunes.apple.com/us/genre/
  - https://itunes.apple.com/us/genre/ios-photo-video/id6008?mt=8&letter=A
    - https://itunes.apple.com/us/app/secret-apps-photo-lock/id492342639?mt=8
- The initial categorization system is designed to quickly obtain a list of potential vault apps (PVAs)
- app title/subtitle, app URL, etc for each app along with the app ID

```
<title>Secret Apps Photo Lock on the App Store</title>
    <link rel="canonical" href="https://itunes.apple.com/us/app/secret-apps-photo-lock/id492342639?mt=8">
    <meta name="description" content="Read reviews, compare customer ratings,
see screenshots, and learn more about Secret Apps Photo Lock.
Download Secret Apps Photo Lock and enjoy it on your iPhone, iPad, and iPod touch."
id="ember124133210" class="ember-view">
<h2 class="product-header__subtitle app-header__subtitle">
App vault to hide &amp;amp; keep video</h2>
```

Data Collection

	id	name	description	url
	Filter	Filter	Filter	Filter
1	284334840	SplashID Safe Password M...	SplashID is the world's most trusted password ...	https://itunes.apple.com/us/app/s
2	295471964	Private Ear Recorder	Set it and forget it! Private Ear is the only secu...	https://itunes.apple.com/us/app/p
3	296475186	Cache Vault	Designed exclusively for the Apple iPhone™ an...	https://itunes.apple.com/us/app/c
4	303027817	Secret!	Secret! is a program for storing passwords, PIN...	https://itunes.apple.com/us/app/s
5	303740913	Picture Safe - Hidden phot...	Picture Safe provides a much needed way to s...	https://itunes.apple.com/us/app/p

- Vault Apps Database – periodically updated
- "Initial Scan" followed by "Sequential Scan" using Lookup URL and parsed data
- https://itunes.apple.com/us/app/secret-apps-photo-lock/id492342639?mt=8
- https://itunes.apple.com/lookup?id=492342639

Javascript file


```
{
 "resultCount":1,
 "results": [
{
"screenshotUrls":["https://is3-ssl.mzstatic.com/image/thumb/Purple118/v4/db/6d/21/db6d217e-fbed-b9d8-b0d2-daaf58070d99/pr_source.jpg/696x696bb.jpg",
"https://is4-ssl.mzstatic.com/image/thumb/Purple128/v4/ef/ca/29/efca29db-934a-8bc6-ae11-a6b762917288/pr_source.jpg/696x696bb.jpg", "https://is5-
ssl.mzstatic.com/image/thumb/Purple128/v4/85/b3/5f/85b35f36-adcc-f3af-5b6c-40d97a4a1654/pr_source.jpg/696x696bb.jpg", "https://is4-
ssl.mzstatic.com/image/thumb/Purple128/v4/6c/d7/d6/6cd7d660-a7dc-fe96-e784-9ae6c2cfbb1e/pr_source.jpg/696x696bb.jpg", "https://is1-
ssl.mzstatic.com/image/thumb/Purple118/v4/f9/11/e3/f911e38f-b6de-0ad8-b924-6e0902dd347d/pr_source.jpg/696x696bb.jpg"],
"ipadScreenshotUrls":["https://is4-ssl.mzstatic.com/image/thumb/Purple128/v4/65/4a/50/654a5045-45d1-cd7c-01f6-c24aa7b90983/pr_source.jpg/1024x768bb.jpg",
"https://is2-ssl.mzstatic.com/image/thumb/Purple128/v4/c7/44/bd/c744bd8b-21d4-5b2e-6dc5-42c290c81704/pr_source.jpg/1024x768bb.jpg", "https://is4-
ssl.mzstatic.com/image/thumb/Purple128/v4/03/a0/74/03a07453-5032-be68-ab2e-2adc11a7f8ff/pr_source.jpg/1024x768bb.jpg", "https://is4-
ssl.mzstatic.com/image/thumb/Purple128/v4/1f/b1/ed/1fb1ed74-20f5-3afb-96ca-a8bed0b9fd0d/pr_source.jpg/1024x768bb.jpg", "https://is1-
ssl.mzstatic.com/image/thumb/Purple62/v4/84/10/0d/84100dd9-23c8-e8e6-75c5-89d4ebcd2acd/pr_source.jpg/1024x768bb.jpg"], "appletvScreenshotUrls":[],
"artworkUrl60":"https://is4-ssl.mzstatic.com/image/thumb/Purple118/v4/3d/49/6c/3d496c36-b5d2-d28a-8628-e23a7d02609a/source/60x60bb.jpg",
"artworkUrl512":"https://is4-ssl.mzstatic.com/image/thumb/Purple118/v4/3d/49/6c/3d496c36-b5d2-d28a-8628-e23a7d02609a/source/512x512bb.jpg",
"artworkUrl100":"https://is4-ssl.mzstatic.com/image/thumb/Purple118/v4/3d/49/6c/3d496c36-b5d2-d28a-8628-e23a7d02609a/source/100x100bb.jpg",
"artistViewUrl":"https://itunes.apple.com/us/developer/easy-tiger-apps-llc/id570748343?mt=8&uo=4", "advisories":[],
```


App Bundle-ID

Table: PVA Results

Item	USA	Russia	India	China
Apps in significant categories	477002	448389	451432	460551
Number of potential vault apps	2364	1968	2169	1986
Run Time initial categorization	48m2s	38m1s	39m43s	39m37s

Table: Apps Deployed in Mutual App Stores

Region	Count
Apps found in US region as well as Russian region	1831
Apps found in US region as well as Indian region	2015
Apps found in US region as well as Chinese region	1836
Apps found in US, Russia, India and China	1735

Binary Classification

- Ground Truth established using manual labeling process.
- Gaussian Naive Bayes (GNB)
- Support Vector Machine (SVM)
- Decision Tree Classifier (DT)
- Extended features to 20
- New features helped in minimizing FP values
- [‘private’, ‘sensitive’, ‘censor’, ‘protect’, ‘decoy’, ‘privacy’, ‘secret’, ‘hide’, ‘vault’, ‘secure’, ‘safe’, ‘photos’, ‘videos’, ‘notes’, ‘passwords’, ‘contacts’, ‘password-protected’, ‘password protected’, ‘browser’, ‘private browser’]

Training/Testing

- Labeled Dataset: 2963 apps
- Vault apps: 1118 apps
- Non-vault apps: 1845 apps
- To appropriately balance vault versus non-vault apps for our identification goals we used all the vault applications and 690 of the non-vault applications for a total of 1808 apps for training and testing.
- The dataset was partitioned into 60% (Training Set) and 40% (Test Set) with random seeds.
- 4-fold cross validation was for each classifier type.

Results of Classification

Classification Report of Gaussian NB Classifier (Support=724)

	Precision	Recall	F1-Score
0 (non-vault)	0.73	0.93	0.82
1 (vault)	0.95	0.79	0.86
Average	0.87	0.84	0.85

Classification Report of SVM Classifier (Support=724)

	Precision	Recall	F1-Score
0 (non-vault)	0.91	0.83	0.86
1 (vault)	0.90	0.95	0.92
Average	0.90	0.90	0.90

Classification Report of Decision Tree Classifier (Support=724)

	Precision	Recall	F1-Score
0 (non-vault)	0.82	0.89	0.85
1 (vault)	0.93	0.88	0.90
Average	0.89	0.88	0.88

Results of Classification

Cross Validation Scores of Classifiers and their Accuracy (4-fold)

Category	Run 1	Run 2	Run 3	Run 4
GNB Cross Validation Score	0.854304	0.783664	0.840707	0.764966
GNB Accuracy	0.81 (+/- 0.07)			
SVM Cross Validation Score	0.891832	0.891832	0.89601	0.889135
SVM Accuracy	0.89 (+/- 0.00)			
DT Cross Validation Score	0.87858	0.883002	0.878318	0.853658
DT Accuracy	0.87 (+/- 0.02)			

Estimated Number of Vault Apps from International App Stores using Trained Classifiers.

Classifier	US	Russia	India	China
Gaussian Naive Bayes	1091	768	874	767
Support Vector Machine	1680	1272	1413	1263
Decision Tree	1412	1037	1171	1038

Extraction/Forensic Analysis of Vault Apps

App Name	Bundle-ID	Passwords	Notes	Multimedia	Contacts	Encryption	Recovered Artifacts
My Wallet Lite [3]	sk.mediaware.mywalletlite	✓				✗	Passwords
My Browser White [6]	com.savysoda.privatebrowserwhite					✗	Browsing history
My Secret Notes [2]	com.gummybearstudios.mysecretnotes		✓			✗	Saved notes
Private Journal [5]	com.penzu.ios.Penzu		✓	✓		✗	Notes
Secret Photos - KYMS[7]	it.ideasolution.mediasafe		✓	✓		✓	Audio, Encrypted images
My Secret Folder [1]	com.red.msf		✓	✓	✓	✗	Photos, Audio, Notes
Passwords + [4]	com.dataviz.PasswordsPlus	✓	✓		✓	✓	None

- App structure analysis was required for the completion of VIDE automation tool.
- Jailbroken/Off-the-shelf iOS devices were used for analysis which was performed on Linux OS.

VIDE Report

VAULT IDENTIFICATION, DETECTION AND EXTRACTION REPORT

Details about the Device:

Device Name: XXXXXX iPhone
Phone Number:+1 (XXX) XXX-XXXX
IMEI Number: 35XXXXXXXXX1202
Product Version: 12.3.1
Logical Acquisition Status: Finished
Logical Acquisition Date Time: 2019-05-10 17:04:46.278286

Total numbers of Apps Found on the Device: 70

Numbers of Vault Apps Found on the Device: 5

List of Vault Apps Detected:

1. lockmyfolder
2. com.appostrophe.privatecalc
3. my.com.pragmatic.My-Apps-Lite
4. org.whispersystems.signal
5. com.GalaxyStudio.PasswordSafeFree

Files and Artifacts Extracted:

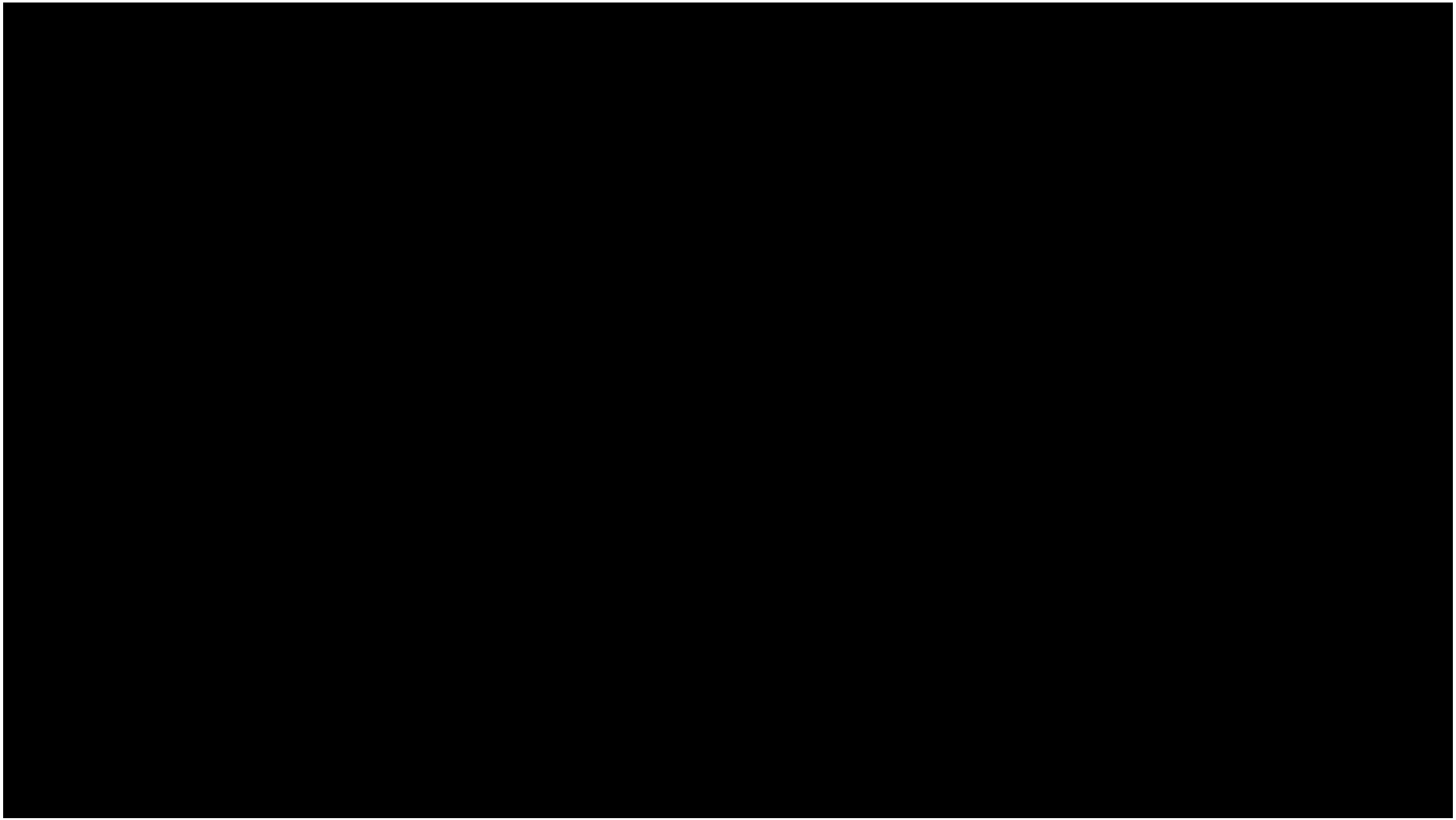
1. **App Bundle ID: lockmyfolder**

PLIST FILES:
Library/Preferences/lockmyfolder.plist
Library/Application Support/com.crashlytics/CLSUserDefaults.plist

IMAGE FILES:
Documents/PHOTOS/A6A5B438-3028-4B49-9E8F-B467356F5DB1/IMG1.jpg
Documents/PHOTOS/8632C492-5014-434B-9F83-4DB9661CB2C5/IMG3.jpg
Documents/PHOTOS/8632C492-5014-434B-9F83-4DB9661CB2C5/IMG2.jpg
Documents/PHOTOS/8632C492-5014-434B-9F83-4DB9661CB2C5/IMG1.jpg

DATABASE FILES:
Documents/LockMyFolder.sqlite

Any media files found? Yes



Thank you!