Think Outside the App
An Investigator's Guide to Mobile App OSINT

Dr. Darren Hayes
Pace University
Biography

• Pace University
• Director of Digital Forensics
• Manage Computer Forensics Lab
• Focus on Mobile Forensics
• App Analysis
• Investigator
• Intelligence
• Legal Consultant
• Expert Witness
Current Initiatives

• Twitter
  • Language Analytics with Rosette API
  • Cree.py

• Telegram
  • 100+ Channels Collected
  • FOCA (Elevenpaths)
  • Developing a Glossary of ISIS Search Terms
ISIS Children’s App
Opioid Sales on Twitter

• 620,000 Tweets Analyzed

• Keywords:
  • Codeine
  • Percocet
  • Fentanyl
  • Vicodin
  • Oxycontin
  • Oxycodone
  • Hydrocodone
Federal Agencies Use Cellphone Location Data for Immigration Enforcement

Commercial database that maps movements of millions of cellphones is deployed by immigration and border authorities.

How the U.S. Government Obtains and Uses Cellphone Location Data

The U.S. government is using app-generated marketing data based on the movements of millions of cellphones around the country for some forms of law enforcement. We explain how such data is being gathered and sold.
Apps of Interest

• Tinder
  • Profile Sharing
  • Human Trafficking

• Starbucks
  • Geodata

• Instagram
  • Arms, Drugs

• Threema
  • Secure Messaging
  • Approved by IS
Known Terrorist Apps

- Alrawi
  - ISIS Developed App
  - Alternative to Telegram
  - GhostSec, CT Offshoot of Anonymous

- Frendica
- VK
- Quitter
- Twister

- BitChirp
- Bitmessage
- Twitter
Apps of Interest

- Wickr
- enLegion
- Cryptocat
- TextSecure
- WhatsApp
- Skype
- Signal
- SnoopSnitch
- Agent Edward Snowden
- TikTok
- FaceApp
LocalScope

Location Browser for your iPhone

LocalScope is a window to your world that lets you explore your surroundings like never before. Discover and find places, people and information around you using geo-tagged data from multiple local search engines, social networks, media sharing services and other apps.
Cellphone Investigations

• Find Out the Owner of a Cellphone #
• Hear Voicemail
• Lookup Name
Cellphone Investigations

- Dirty Phonebook
- Spoofcard or BluffMyCall & Call Dominos
- Maltego
- Dominos
Twitter Analytics

- **Foller.me**
  - Identifies:
  - Owner Name
  - Account Creation Time & Date
  - Tweets
  - Followers
  - Following
  - Topics
  - Replies
  - Tweets with Mentions

- **Most Linked Domains**
- **Attitude**
- **Device(s) Used to Tweet** 😊
Creepy

- [https://dev.twitter.com/oauth/overview/application-owner-access-tokens](https://dev.twitter.com/oauth/overview/application-owner-access-tokens)
FOCA (Fingerprinting Organizations with Collected Archives) is a tool used mainly to find metadata and hidden information in the documents its scans. These documents may be on web pages, and can be downloaded and analyzed with FOCA.

It is capable of analyzing a wide variety of documents, with the most common being Microsoft Office, Open Office, or PDF files, although it also analyzes Adobe InDesign or SVG files, for instance.
Fourth & Fifth Amendments

Biometrics
- Fingerprint
- Face ID
- Fourth Amendment (Warrant)

Password
- Protected by Fifth Amendment
Background

App Markets:
- Google Play: 3.6m apps
- Apple App Store: 2.1m apps
- 8.5% of Apps: Cross-platform

Online Dating:
- 15% of Adults in USA have used Online Dating Websites or Apps
- Dating Website Usage: 10% → 27% in 2 Years
Methodology

Perform a Static & Dynamic Analysis of Tinder, Bumble & Grindr

Grindr under Investigation in EU

Static Analysis → Reverse-engineer Code (.apk) & Examine SQLite DB

Dynamic Analysis → DNS Connections

Deep-Linking with Social Media Accounts

Privacy Policy
Methodology

- Static Analysis
  - Reverse-Engineer the APK & iOS app File
  - dex2jar
  - FileViewer Plus
  - Review of Permissions Manifest
  - Forensics on SQLite DB
    - BlackLight
Methodology

- Dynamic Analysis
  - WiFi Traffic
  - DNS Connections & HTTP Requests
- Debookee
- Privacy Policy
- EULA
Tinder

Potential Matches based on Location

Swipe Left - Dislike a Profile

User Can Un-Swipe Left

Swipe Right - Like a Profile

Swipe Up - “Super Like” Notification Sent to User

Ability to Block a User
Tinder Usage

• 50% of Tinder Users Active at 21:00
• Active Users Login 4 Times Daily
• Core Base: 18-24
• Match Group Revenue: $1.3 bn in 2017
  • Tinder Revenue: $800m in 2018
• 95% of Tinder Users Meet their Matches within 1 Week
  • Only 25% for Online Dating
• Average Male Message is 12 Characters & 122 Characters for Women
Tinder Findings

- Connects to a User’s Spotify Profile
- Connects to Instagram
- Deep-linking
Tinder Findings

• Tinder2.sqlite
• Location Data Stored Locally in Plaintext:
  • ZLASTVIIST TIMESTAMP
  • ZLATITUDE FLOAT
  • ZLATITUDE FLOAT
• Deep-Linking to Facebook
• Deep-Linking to Spotify
  • Spotify ID
  • Playlist
• Spotify Playlist used for Match Algorithm
Tinder Findings

• Taplytics
  • Birthday, city, country, county, data provider, gender, language, location radius, device model, iOS version, UID & age
  • Obtained through Facebook
  • Undisclosed in Privacy Policy

• Crashlytics

• Conversations in Plaintext
  • Incoming Messages Only
Tinder Findings

- Links to Images Online: http://images-ssl.gotinder.com
  - Links in Plaintext
  - No SSL/TLS
- Tinder Communications Use TLS
- Debookee Decrypted Wireless Traffic
iPhone Tracking through App Development

- UIDevice Class
  - Assigned Name
  - Device Model
  - Operating System Name & Version
  - Physical Orientation
  - Battery Level
  - Proximity of Device to User
iPhone Tracking through App Development

Most App Developers Use Analytics Tools to Track Users

Each Analytic Tool has its Own Implementation for Tracking Users

All Analytics Tools Generate a Long Unique Key that is Stored on their Server
- User #92271D59-36B5-499E-855B-EB6D06B5BE2B

Probably Not Using MAC or UID
iPhone Tracking through App Development

Advertising Identifier

Does this app use the Advertising Identifier (IDFA)?

The Advertising Identifier (IDFA) is a unique ID for each iOS device and is the only way to offer targeted ads. Users can choose to limit ad targeting on their iOS device.

If your app is using the Advertising Identifier, check your code—including any third-party code—before you submit it to make sure that your app uses the Advertising Identifier only for the purposes listed below and respects the Limit Ad Tracking setting. If you include third-party code in your app, you are responsible for the behavior of such code, so be sure to check with your third-party provider to confirm compliance with the usage limitations of the Advertising Identifier and the Limit Ad Tracking setting.

This app uses the Advertising Identifier to (select all that apply):

- Serve advertisements within the app
- Attribute this app installation to a previously served advertisement
- Attribute an action taken within this app to a previously served advertisement

If you think you have another acceptable use for the Advertising Identifier, contact us.

Limit Ad Tracking setting in iOS

I, Jessica, confirm that this app, and any third party that interfaces with this app, uses the Advertising Identifier checks and honors a user’s Limit Ad Tracking setting in iOS and, when it is enabled by a user, this app does not use Advertising Identifier, and any information obtained through the use of the Advertising Identifier, in any way other than for “Limited Advertising Purposes” as defined in the iOS Developer Program License Agreement.
Customer Analytics

- iOS 5+ → Not by UDID but through Advertising Identifiers
- Fabric
- mixpanel
- UXCam
- Localytics
- Crashlytics
iPhone Tracking through App Development

- Tracks App Usage
- User Location
  - GPS, Towers, WiFi
  - Works with App Closed
- 10,000 Geofences (Locations) for Push Notifications
- Geofence Analytics
  - Foot Traffic
  - Dwell Time
Localytics Customers

Media & Entertainment
- COMCAST
- FOX
- The Weather Channel
- The New York Times
- CBS
- Grindr

Commerce & Travel
- priceline
- TJX
- macy's
- Wendy's
- zipcar

Finance & Technology
- AVIS
- SAFEWAY
- Microsoft
- E*TRADE
- Nuance
- Fidelity Investments
- verizon
- Amazon
iPhone Tracking through App Development

- Tracks User’s Search History
- Website Clicks
- Profile Creation
- Location (City/Country)
- Operating System
- User ID
- Email
iPhone Tracking through App Development

- Performs Screen Recording
- Captures Touch Points & User Gestures
- Record Google Map Fragments
Website Security & Recon

SSL LABS - TEST SITE CERTIFICATES & SSL IMPLEMENTATION

MX TOOLBOX → SITE MISCONFIGURATIONS

DNSDUMPSTER → DNS RECON

ROBTEX → DNS MAPPING
Tinder Vulnerabilities

- Are You on Tinder? Someone May Be Watching You Swipe
- Eavesdropping → Same WiFi Network
- Insecure HTTP Connections
- [https://info.checkmarx.com/hubfs/Tinder_Research.pdf](https://info.checkmarx.com/hubfs/Tinder_Research.pdf)

### Discovered Vulnerabilities:

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>CVSS Score</th>
<th>CVE ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Insecure HTTP connections</td>
<td>4.3</td>
<td>CVE-2018-6017</td>
</tr>
<tr>
<td>2) Predictable HTTPS response size</td>
<td>4.3</td>
<td>CVE-2018-6018</td>
</tr>
</tbody>
</table>
Grindr

- Unsecured Communications
- Smaato
  - Location
  - Gender
  - Device Type
- Octopus-X
  - IP Address
Why Uber?

• Unroll.me → Service to PurgeSpam from Inbox
  • Application Searched for Lyft Receipts & Sent Information to Uber
• March 2017 – Greyball Program Used to Target City Officials
• April 2017 – Meeting between Tim Cook & Travis Kalanick
• May 2017 – DoJ Investigates Uber’s Use of Software to Evade Transportation Regulators
• August 2017 – DoJ Investigates Uber for Foreign Bribery
• September 2017 – Uber Faces FBI Probe Over Program Targeting Rival Lyft
Uber Privacy Policy

• Uber Collects Your Location:
• (i) when the app is open &
• (ii) from the time of the trip request through five minutes after the trip ends
Experiments

① Trip with Yellow Cab
② Trip with Lyft
Results

• **Experiment 1:**
  • Uber Recorded the Yellow Cab Ride

• **Experiment 2:**
  • Uber Recorded the Lyft Ride
  • Uber Tracked the User 11 Minutes after the Ride Concluded
Summary

Benefits of Dating Apps for Intelligence:
- Popular
- Multiplatform
- Real-time Intel
- Deep-linking to Social Media
- Location Data

Concerns
- Privacy Issues
- GDPR
Funding Acknowledgement

We would like to acknowledge the support from the Department of Defense under Grant No. H98230-19-1-0293 and from the National Science Foundation under Grant No. 1503760. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation, the Department of Defense, or the U.S. government.
Questions

dhayes@pace.edu

#CyberOSINT & #Codedetective