

Mobile Forensics

Dr. Darren Hayes





Government





- 1.7 Billion Downloads
- Rovio Entertainment
- Snowden Claims NSA & GCHQ Uses the Game to Spy
 - Personal Data
 - Location Information
 - Political Affiliation
 - Sexual Orientation

Angry Birds





Where's the Evidence?



Where's the Evidence?



Where's the Evidence?

- Secure Digital Card
 - FAT32
 - App Evidence
 - Larger Files
 - Video
 - Photos
 - Write-Blocker

Evidence (SD)

- EF_ADN
 - Abbreviated Dialing Numbers (ADN)
- EF_FPLMN
 - Forbidden Public Land Mobile Network (FPLMN)
- EF_LND
 - Last Numbers Dialed (LND)
- EF_LOCI
 - Area where user last powered down the phone
- EF_SMS
 - Short Message Service (SMS)

SIM File System



Smartphone Tracking

© Dr. Darren R. Hayes | Pace University

- Photos
 - EXIF Data
- Social Media Postings
 - Foursquare
 - Twitter
- Bluetooth
- Hot Spots
 - SSID
- GPS
- Cell Sites
 - Tower
 - Antenna

What's Your Location?

Firefox | Localscope - social data powered GPS a... | www.cynapse.com/localscope | Bing

Cynapse Products Solutions Downloads Store Resources About Us Partners Community

Localscope
Discover your locality

Localscope **Overview** iOS webOS Support API

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.

LocalScope



Google+



You Tube

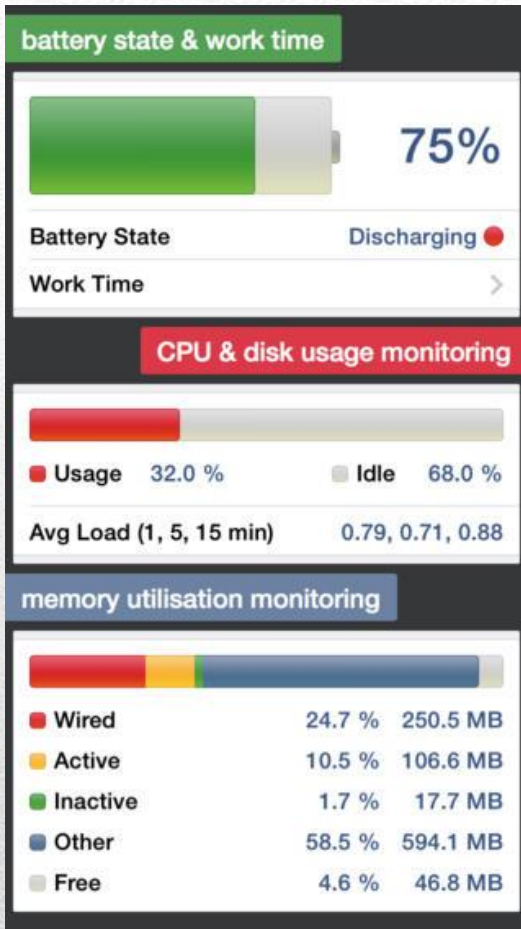


Geotagged Apps

- TaintDroid
- Tracks how Apps Use Sensitive Information on a Smartphone
- <http://appanalysis.org/>



Realtime Privacy Monitoring on Smartphones



System Status



Brightest Flashlight

- Application Permissions:
- Write to External Storage
- Access Information about Wi-Fi Networks
- Access Coarse (e.g., Cell-ID, Wi-Fi) Location
- Open, Close, or Disable the Status bar and its icons
- Read only access to phone state
- Required to be able to access the camera device
- Open network sockets
- Access fine (e.g. GPS) location
- PowerManager WakeLocks to keep processor from sleeping or screen from dimming
- Access information about networks
- Access the flashlight

Brightest Flashlight

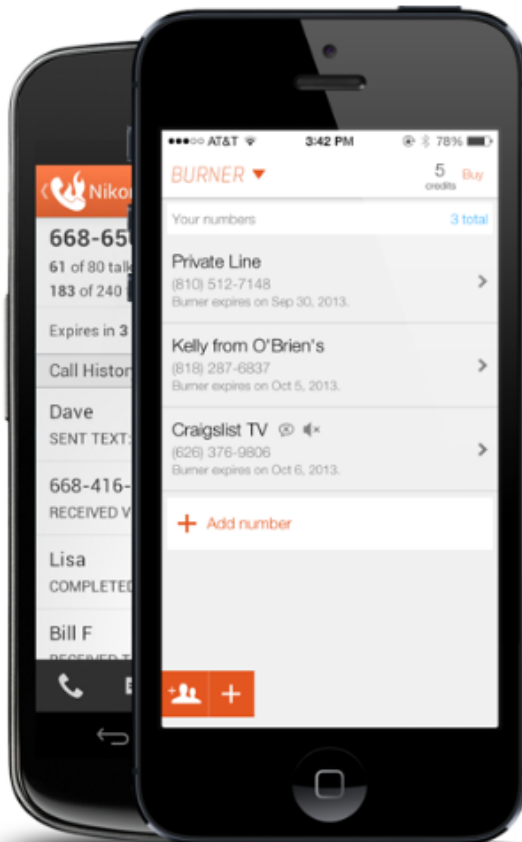
- Problem is with Legitimate Apps
- Access to Contacts
- Passwords Stored in Contact List

Smartphone Privacy

- \$629 Per Unit
- PrivatOS
- www.blackphone.ch



Blackphone



Be private, publicly

Burner is a privacy layer for your iPhone or Android. Get phone numbers you control at the push of a button.



Burner

Android

- Auto Industry
- Dacor's Android-Powered Oven
 - Operates Based on Recipes from Tablet
- Fridges
 - Barcode Scan – Monitors Freshness of Food
 - Diet App
 - Grocery List
- Air Conditioners
 - Remote Operation
- LG Washer & Dryer



Android Appliances



Android Apps

- Date & Time When App is Executed is Stored
- Developer Decides What Data to Share
 - Forensics Software Only as Good As Data Developer Shared

Android Apps

- Developers Have 4 Mechanisms for Storing Data
 - Preference
 - Files
 - SQLite Database (Best Source)
 - Cloud

Android Apps

- Open Source
- Free
- Relational Database
- Small File Size
- One Cross-Platform File
- Accessible through Command-line or Application

SQLite

- SQLite Database Browser
 - <http://sqlitebrowser.sourceforge.net/>
- SQLite Viewer
 - <http://www.oxygen-forensic.com/en/features/sqliteviewer/>
- SQLite Analyzer
 - http://www.kraslabs.com/sqlite_analyzer.php

SQLite Viewers

- Cache.wifi
 - Captures WiFi Connections
 - Do Not Need to Connect to Record
 - Can Be Mapped



App Evidence

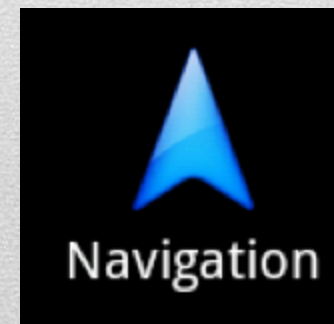
- Emailprovider.db
 - Path:
/data/data/com.android.email/databases/EmailProvider.db
 - Exchange Login & Password in Plaintext
- HostAuth
 - Gmail
 - com.google.android.gm
 - Gmail Login & Password in Plaintext



App Evidence

- Da_destination.db
 - Turn-by-Turn Navigation
 - .WAV Files Stored

App Evidence



- Metal Gear Solid
 - Symbian-based Suit of Malware
 - Malware Disables Anti-Virus
 - Cabir Virus
 - Developed in 2004
 - Computer Worm
 - Spreads through Bluetooth
 - “Caribe” Displayed every time Device is Turned On

Symbian Malware

- 70%+ Mobile Device Malware is on Android
- 450,000 Android Apps
- Average of 15 Malware Programs on Google Play
- 26% of Android Malware are Trojans
- Corporate Adoption Rate of Android = 6x iPhone (Gartner)

Android Malware

- Q3 2013 – 252 New Mobile Threats (F-Secure Labs)
 - Increase in Amount of Malware & Complexity of Malware
- Q2 2013 – Android Malware Increased 40%, from 509,000 to 718,000 (Trend Micro)

Recent Statistics

- Angry Birds Rio Unlocker
 - Most-Widely Downloaded Malware
- 600,000 Clickjack Attacks Occur Every Day (AVG)
- \$20 Million of Revenue Every Day (AVG)

Mobile Game App Malware

- CATE
 - Call Blocking
 - SMS Blocking
 - MMS Blocking
- Snapchat
- Voxel
- TigerText
- HeyWire
 - Free Texting
- Pinger
 - Free Talk & Text
 - Turns an iPod into a Cellphone

Mobile Apps

- Girls Around Me
 - Creepy App



- FlexiSPY
 - Spying on Other People
 - Stealth Mode



Mobile Apps

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



Cellphone Investigations

DIRTYPHONEBOOK

Uncensored People Reviews

KEYWORD SEARCH

- Search over **101 million** phone numbers.
- Find your friends, lovers, & colleagues.
- See what people really think of you for FREE.
- **MAKE ANONYMOUS FREE CALLS!**
- Share comments, aliases, locations, & ratings.



Search any 10-digit phone number:

 - -

Like 1.8k

Tweet

f t

Latest **Random**

- This is about BJ. Although him and abbey do share the same last name. Leave her alone, yes she's ...
615-491-8164
-
- Robert Ashley is a great guy.
303-564-3978
-
- Lisa Estes Burris (615-785-3736) is a moron. Do not trust her for nothing. She is a con artist. ...
615-785-3736
-
- Vilma Vega is a hoe!!! Don't trust her. She has had a man for years but lies and says she doesn't...
650-995-7583
-
- EXTRACT: "I helped MS Lilly for a month.....and get labeled a "Would Be Pimp.".....I tried to c...
931-249-4768
-
- EXTRACT: "I helped MS Lilly for a month.....and get labeled a "Would Be Pimp.".....I tried to c...
931-249-4768
-
- Another fat ass hooker is Abbey jones. Where can I find a hooker who is not fat, dont do drugs, N...
615-491-8164

Sign Up for FREE

- to follow your friends
- to comment and rate content
- to view all photos
- to block your number
- to block specific comments

Login

Username:

Password:

Remember me

[Forgot your password?](#)



iPhone Forensics

- iPhoneTrackerWin
 - Displays Information about iPhone User's Movements on Maps
 - URL: <http://www.huseyint.com/iPhoneTrackerWin/>
- iOS Tracker
 - <http://tom.zickel.org/iostracker/>

iPhone Tracking

- Developed by Apple for iOS 7
- Open Source Code
- Bluetooth Low Energy (BLE)
 - Bluetooth 4.0
- Indoor Tracking
- Used by Retailers
- Target Knew About a Teenage Girl Being Pregnant Before Parents Knew

iBeacons

- Home Automation
 - Lighting
 - TV Channels Follow You in the Home
- Used to Find Your Car

iBeacons

- Texas Instruments
- BLE (Bluetooth 4.0)
- Sensors:
 - Humidity
 - Pressure
 - Accelerometer
 - Gyroscope
 - Magnetometer

SensorTag

- Bleu Station
 - Bleu.io
- Apps:
 - Bleu Setup
 - Locate IB
 - Geohopper

BLE



iPhone 5c



iPhone 5S

- Control Center
 - Swipe Upwards
- AirDrop
 - Share Data via Bluetooth

iOS 7

- Advanced Encryption Standard 256 (AES)
 - Encryption is at Block Level
- Unique Device Identifier (UDID)
 - 40-Digit Alpha-Numeric Identifier
 - Uniquely Identifies Each Apple iOS Device
- Unique Identifier (UID) & Device Group Identifier (GID)
 - AES 256-bit keys – Hard Coded in Application Processor
 - Chipoff is Impossible
- Data Cryptographically Linked Specific Device

iOS 7 Security

- 4-Digit PIN
- 8-Digit Passcode Option Available
- Increasing Time Delay with Brute Force Attack
- Data Protection
 - Files Encrypted in Flash Memory to Allow for Incoming Calls
 - 256 Bit Key for Each File

iOS 7 Security

- Wearable Technology
- Eye Tracking
- Motion Capture
- Facial Recognition
- Emotion Recognition

Future of Computer Forensics



Wearable Technology

Dr. Darren R. Hayes
(212) 346-1005
dhayes@pace.edu

Questions
