Mobile Forensics

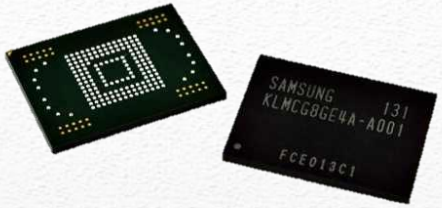
Dr. Darren Hayes

Government

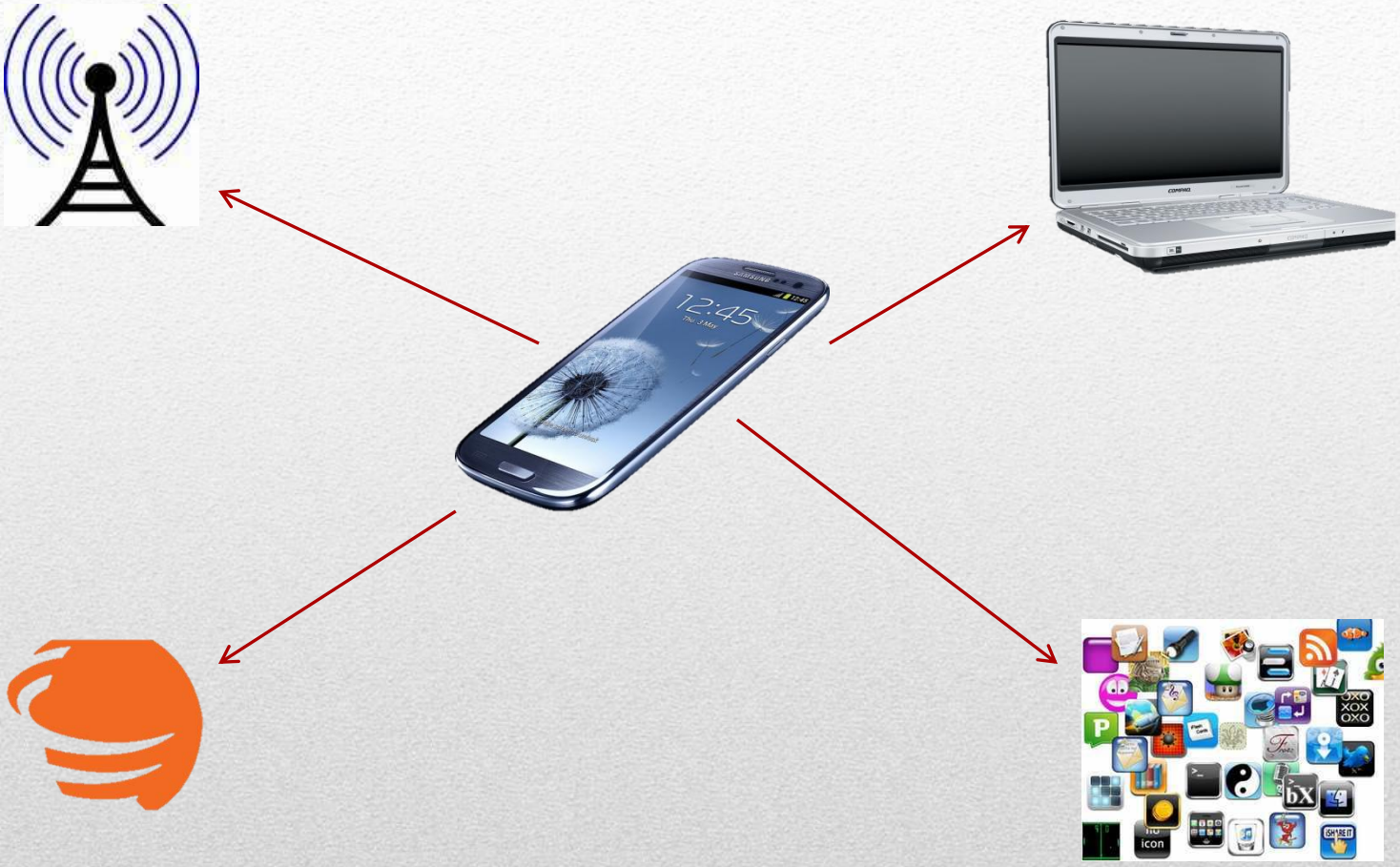
Angry Birds

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

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)

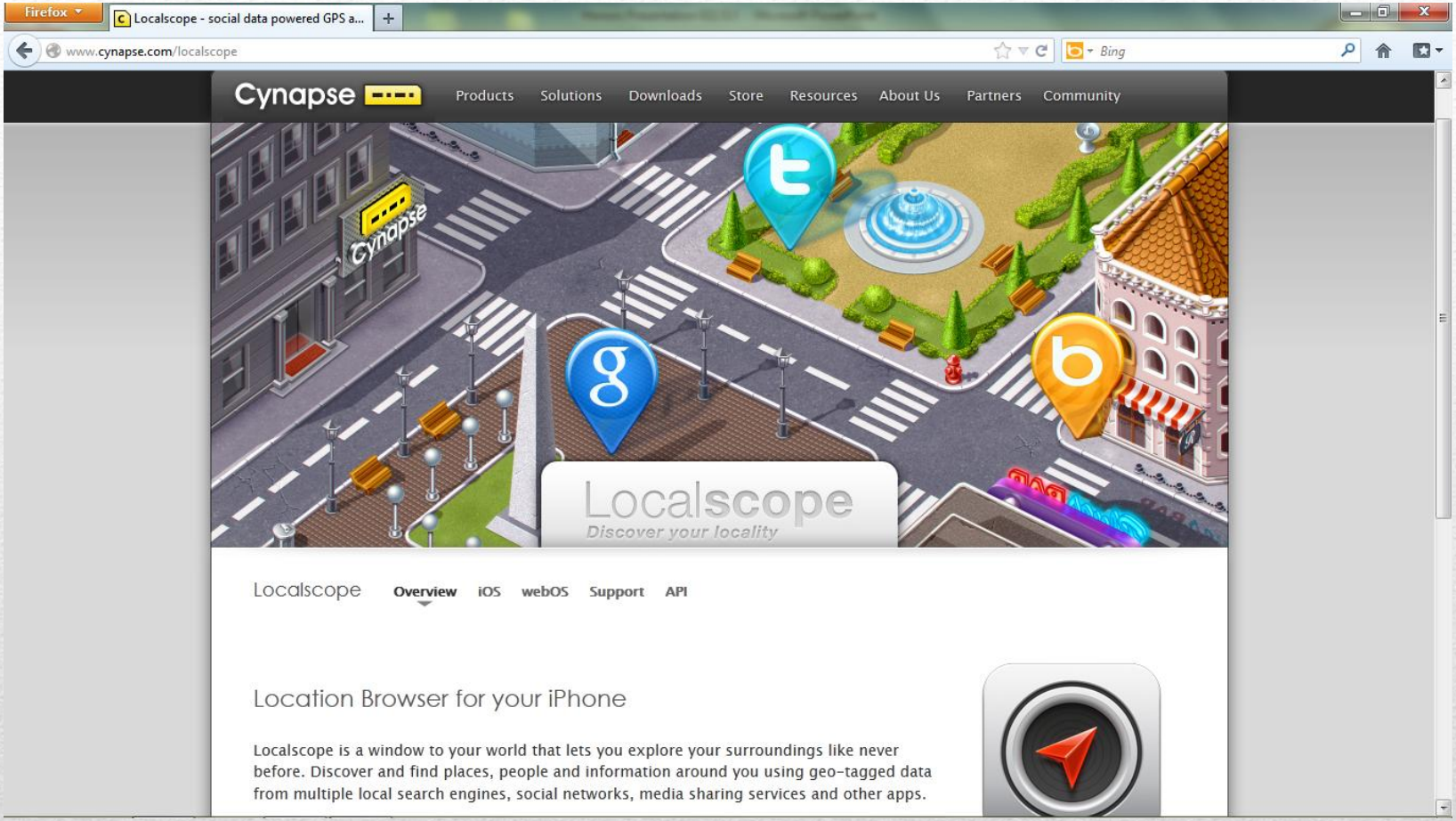
- EF_ADN
  - Abbreviated Dialing Numbers (ADN)
- EF_FPLMN
  - Forbidden Public Land Mobile Network (FPLMN)
- EF_LND
  - Last Numbers Dialed (LND)
- EF_LOCI
  - Area where user last powered down the phone
- EF_SMS
  - Short Message Service (SMS)

SIM File System

Smartphone Tracking

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

What's Your Location?

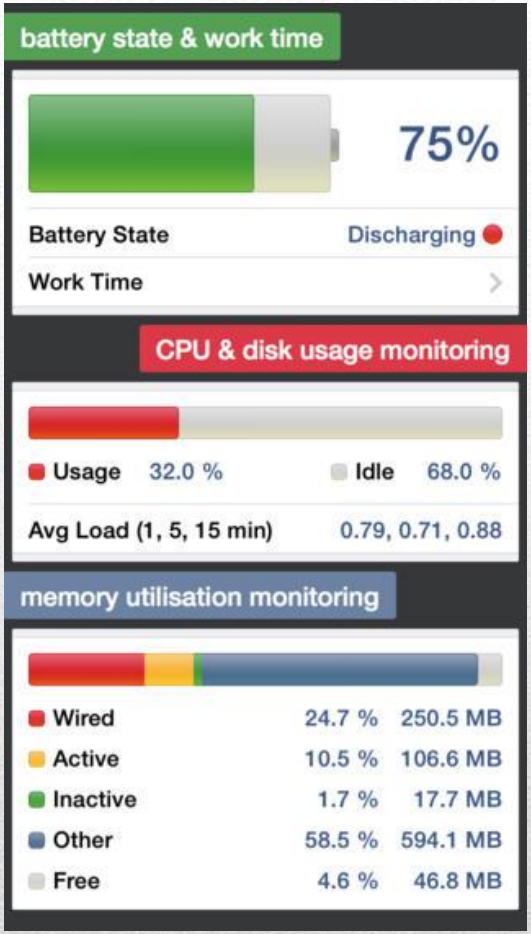


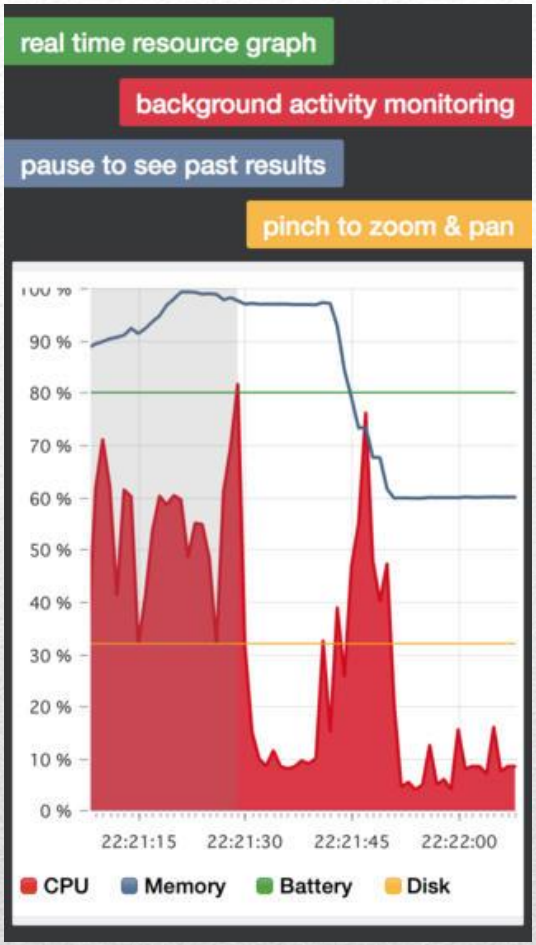
LocalScope

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

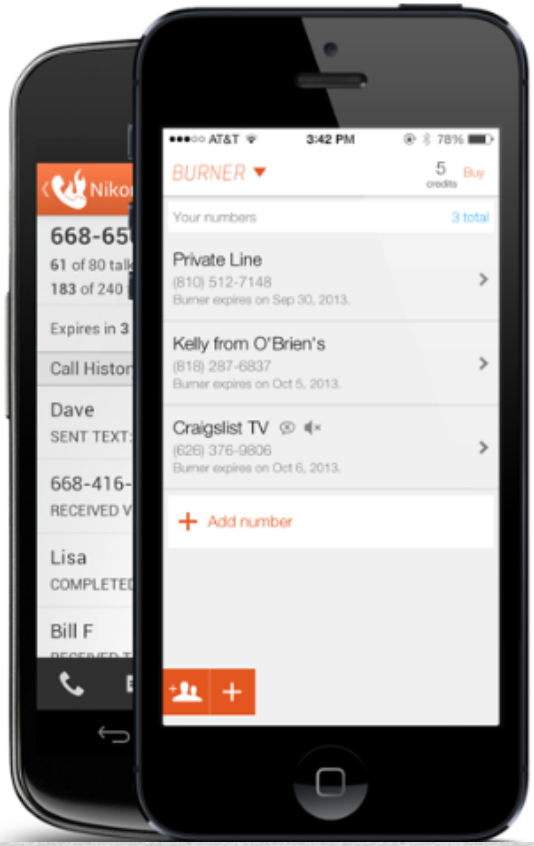
Smartphone Privacy

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

Blackphone

BURNER

Support Blog About us



Be private, publicly

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

Download on the App Store

GET IT ON Google play

Burner

Android

Android Appliances

- 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 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 Viewers

- 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

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

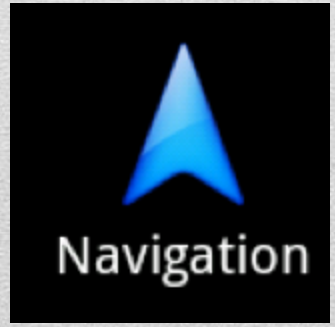
App Evidence

- 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



Symbian Malware

- 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

- 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
- Voxer
- TigerText
- HeyWire
  - Free Texting
- Pinger
  - Free Talk & Text
  - Turns an iPod into a Cellphone

Mobile Apps

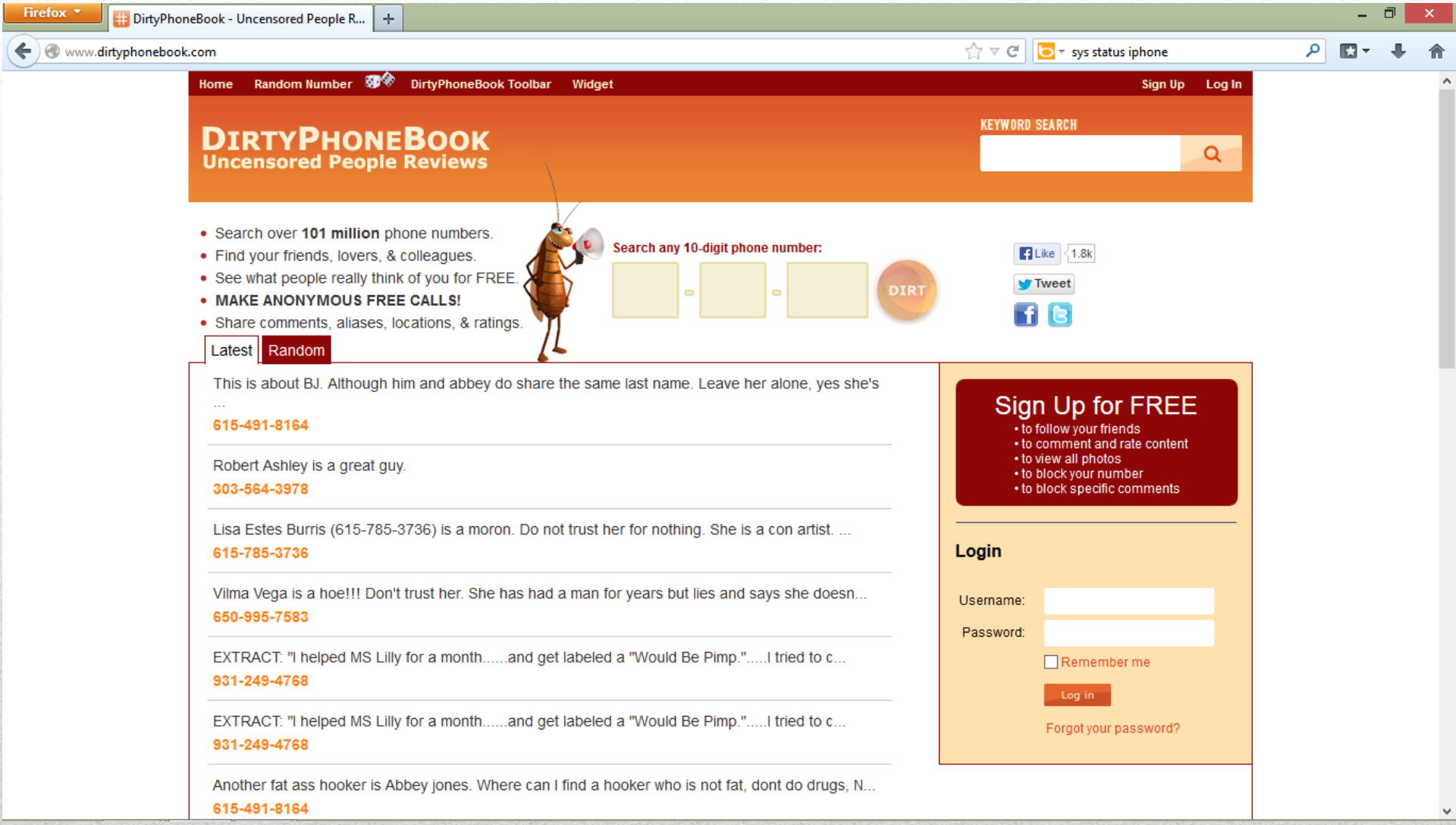
- Girls Around Me
  - Creepy App

- FlexiSPY
  - Spying on Other People
  - Stealth Mode

Mobile Apps

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

Cellphone Investigations



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

SensorTag

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

- 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