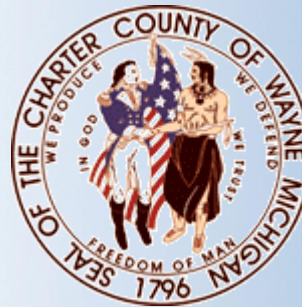




# Cell Phone Science

*Criminal Advocacy Program*

October 10, 2014



**SRR**

STOUT | RISIUS | ROSS

Financial Advisory Services

# Select Professionals



## Brian A. Rosenthal, CISSP, EnCE

Digital Forensic Manager  
Direct +1.646.807.4242  
Mobile +1.917.858.1083  
[brosenthal@srr.com](mailto:brosenthal@srr.com)

---

B.S.  
Rutgers College  
*Computer Science*

---

Certified Information  
Systems Security  
Professional (CISSP)

Encase Certified Engineer  
(EnCE)

Brian A. Rosenthal is a Digital Forensic Manager in the Computer Forensics and E-Discovery practice within the Dispute Advisory & Forensic Services Group. Mr. Rosenthal has a background in Computer Forensics, E-Discovery, and Forensic Analysis of digital media including: computers, servers, cell phones and other mobile media storage devices.

Mr. Rosenthal has extensive experience working with law firms, corporate counsel, litigation support managers, and paralegals to manage their electronic data from collection through production. He combines his knowledge of the legal industry with his experience working on large complex document management projects to improve efficiencies and reduce overall project costs. Mr. Rosenthal's experience with Forensic Investigations and E-Discovery projects spans many industries including manufacturing, automotive, finance, retail, marketing, government, energy, healthcare, and insurance.

Prior to joining SRR, Mr. Rosenthal was a Senior Consultant at various national digital forensics and e-discovery companies including Kroll Ontrack.

Mr. Rosenthal received a B.S. in Computer Science from Rutgers University and is an Encase Certified Engineer (EnCE) and a Certified Information Systems Security Professional (CISSP). Additionally, Mr. Rosenthal is a member of the International High Technology Crime Investigation Association (HTCIA) and International Information Systems Security Certification Consortium (ISC<sup>2</sup>).



## Garry A. Pate, CFCE, CHFI, CCFE, EnCE, CEECS

### Director

Direct +1.248.432.1304

Mobile +1.313.701.0941

gpate@srr.com

### Education

---

M.S.

American Intercontinental  
University

*Information Technology*

B.S.

*University of Maryland  
Criminal Justice*

Garry A. Pate is a Director of the E-Discovery practice within the Dispute Advisory & Forensic Services Group. Mr. Pate has a background in Computer Forensics, E-Discovery, internal investigations, database management, document automation, scanning coding and extensive experience working with business owners, attorneys and federal, state, and local government/law enforcement across the United States. Mr. Pate has strong knowledge of electronic data collection, processing and production as well as program and policy development given his 16 years of experience in the legal industry.

Mr. Pate has extensive experience managing E-Discovery projects from collection through production in complex litigation cases involving issues such as IP theft, business technology, copyrights, patents, trademarks, employment disputes, environmental, divorce, and numerous other disputes.

Prior to joining SRR, Mr. Pate was the Director of E-Discovery at a national forensics and e-discovery vendor where he served as a strategic resource for electronic discovery, document collection, review and production, trial preparation methodologies and other practice support needs. Mr. Pate also was an IT Specialist at the Securities and Exchange Commission (SEC) where he was a founding member of the computer forensic laboratory analysis team. He worked on numerous high profile matters including the SEC v. Enron.

Mr. Pate is a Computer Hacking Forensic Investigator – EC-Council (CHFI), Certified Computer Forensics Examiner - Information Assurance Certification Review Board (IACRB) (CCFE), EnCase Certified Examiner (EnCE) – Guidance Software, Inc., Certified Forensic Computer Examiner (CFCE)/Certified Electronic Evidence Collection Specialist (CEECS) – International Association of Computer Investigative Specialists, Certified Handheld [Cell/PDA] Examiner; Certified Advanced Cell Phone Examiner – Paraben Corporation.

Mr. Pate is a member of the Information Assurance Certification Review Board, EC-Council, Association of Certified Fraud Examiners, International Association of Computer Investigative Specialists, High Technology Crime Investigation Association, Regional Computer Forensics Group, and National Institute of Science and Technology – Computer Forensic Tool Testing Committee.

# Overview of SRR

Stout Risius Ross is a global financial advisory services firm that is known for premier expertise, deep industry knowledge, and unparalleled responsiveness.



## Investment Banking

- Mergers & acquisitions
- Private market financing
- Distressed transaction advisory
- Strategic assessments
- Fairness opinions

## Valuation & Financial Opinions

- Fairness & solvency opinions
- Financial reporting
- Corporate tax related valuations
- ESOP & ERISA advisory
- Succession & shareholder planning
- Real estate valuation
- Machinery & equipment valuation

## Dispute Advisory & Forensic Services

- Family Law Valuation & Advisory Services
- Pre-litigation consulting
- Forensic and Discovery services
- Complex damage analysis
- Economic assessments for settlement and case evaluation
- Expert opinions and consultations

ATLANTA BALTIMORE CHICAGO CLEVELAND DALLAS DENVER DETROIT  
HOUSTON LOS ANGELES NEW YORK TYSONS CORNER WASHINGTON, DC

# Mobile Device Forensics

## Overview

- Introduction
- History Of Mobile Devices
- What is Mobile Device Forensics?
- Mobile Device Analysis
- Application Forensics
- Practices and Trends in the Field
- Questions?

# Mobile Device Forensics



In The Beginning....

## What is a cell phone?

- A mobile (cellular) phone is a phone that can make and receive telephone calls over a radio link while moving around a wide geographic area.
- It does so by connecting to a cellular network provided by a mobile phone operator, allowing access to the public telephone network.
- In addition to telephony, modern mobile phones also support a wide variety of other services such as text messaging, MMS, email, Internet access, short-range wireless communications (infrared, Bluetooth), business applications, gaming, and photography.

# Mobile Device Forensics

In The Beginning....

## List of countries by number of mobile phones in use:

Rank ↕	Country or regions ↕	Number of mobile phones ↕	Population ↕
-	World	6,800,000,000+	7,012,000,000 <sup>[1]</sup>
01	 China	1,227,360,000 <sup>[4]</sup>	1,349,585,838 <sup>[5]</sup>
02	 India	904,510,000	1,220,800,359 <sup>[6]</sup>
03	 United States	327,577,529	317,874,628 <sup>[8]</sup>
04	 Brazil	276,200,000	201,032,714 <sup>[10]</sup>
05	 Russia	256,116,000	142,905,200 <sup>[10]</sup>
06	 Indonesia	236,800,000	237,556,363
07	 Nigeria	167,371,945	177,155,754
08	 Pakistan	140,000,000 <sup>[14]</sup>	180,854,781 <sup>[15]</sup>
09	 Japan	121,246,700	127,628,095
10	 Bangladesh	116,508,000	165,039,000

# Mobile Device Forensics

In The Beginning....

## USA Mobile Phone Carriers

- The USA uses two main radio network standards:
  - GSM (Global System for Mobile)

 T-Mobile



- CDMA (Code Division Multiple Access)

 Sprint



 metroPCS





# Mobile Device Forensics

In The Beginning....

## Cell Phone Forensics Short History

- The first hand-held cell phone - DynaTAC 8000x - was demonstrated in Europe by John F. Mitchell and Dr. Martin Cooper of Motorola in 1973.
- In 1979, Japan launched the first commercial cellular network.



# Mobile Device Forensics

# Mobile Device Forensics

In The Beginning....

## Cell Phone Forensics Short History

- Shortly thereafter in 1981, the Nordic Mobile Telephone (NMT) system was launched in Europe. The United States began developing a mobile telephone network in the early 1980s.



# Mobile Device Forensics

In The Beginning....

## Cell Phone Forensics Short History

- In 1991, the 2G digital cellular network was launched.
- Cell phones were “dumb” phones and their capabilities were limited to
  - Making phone calls
  - Paging
  - Push to talk
  - Voicemail



# Mobile Device Forensics

The Smartphone is Born...

## Cell Phone Forensics Short History

In 2007, this guy introduced this device...

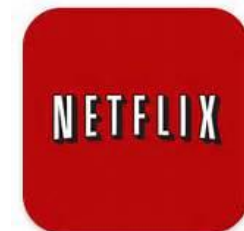


# Mobile Device Forensics

Today

## Cell Phone Forensics Short History

- 4G Smartphones
- RIM's Blackberry is on life support...
- Need a more robust network because...



# Mobile Device Forensics

Today....



# Mobile Device Forensics



Today



**The average smartphone today has more computing power than NASA had in 1969 when the United States sent astronauts to the moon...**





# Mobile Device Forensics

## Mobile Device vs Computer Forensics

### Mobile Device Forensics is **NOT** Computer Forensics Similar Intent = Different Method

- **Computer Forensics**: – Only a few major Operating System Standards: Windows, Mac, Linux. Standard practice is to image the hard drive and examine the data.
- **Mobile Device Forensics**: – Multiple Operating Systems. Various Communication Standards. Each manufacturer has their own: Nokia, Samsung, Motorola, Palm, Blackberry, etc. Communication Standards are evolving. Started this way but is consolidating to four or five. Mobile Forensics is becoming more like computer forensics in some ways.
- **Mobility Aspect**: - Mobile devices are live things roaming around. It's not just about what's on the device, but where has it been and what connections have been made?

What's retained by the network varies from carrier to carrier, but apart from the billing essentials, not much data is saved after 30 days. Some Exceptions.

# Mobile Device Forensics

## Mobile Device vs Computer Forensics

### Another Difference: Phones Are Always Updating Proper Handling and Isolation Are Essential

- **Cell Phone Forensics is not technically “forensics”. We are just starting to image the drive. Mostly we are engaging it to tell us what’s in there and then recording and analyzing.**
- **Proper training in handling and processing phones is essential in reducing the risk of loss or contamination.**
- **While the acquisition of data is relatively easy, it often requires putting an Agent on the device to assist with data extraction.**
- **A phone is always updating with the network, and remote destruction is possible. Proper isolation of the device from the network and immediate analysis is best when possible.**

# Mobile Device Forensics

## Mobile Device Data

### What Can Be Acquired from the Device

- Phonebook
- Call History and Details (To/From)
- Call Durations
- Text Messages with identifiers (sent-to, and originating) Sent, received, deleted messages
- Multimedia Text Messages with identifiers
- Photos and Video (also stored on external flash)
- Sound Files (also stored on external flash)
- Network Information, GPS location
- Phone Info (CDMA Serial Number)
- Emails, memos, calendars, documents, etc.
- GPS Info, Social Networking data, web browsing history



# Mobile Device Forensics

## Mobile Device Data

### What Can Be Acquired from the Device



- **IMSI: International Mobile Subscriber Identity**
- **IMEI: International Mobile Equipment Identity- Unique Identifier[\*#06#]**
- **ICCID: Integrated Circuit Card Identification (SIM Serial No.)**
- **MSISDN: Mobile Station Integrated Services Digital Network (phone number)**
- **Network Information**
- **LND: Last Number Dialed (sometimes, not always, depends on the phone)**
- **ADN: Abbreviated Dialed Numbers (Phonebook)**
- **SMS: Text Messages, Sent, Received, Deleted, Originating Number, Service Center (also depends on Phone)**
- **SMS Service Center Info: GPRS Service Center Info**
- **Location Information: The GSM channel (BCCH) and Location Area Code (LAC) when phone was used last.**
- \* **When SIM Locked – Cannot Be Cracked without Network Operator Assistance.**



*A PIN Locked SIM is Not Accessible Without PIN – Requires PUK From Carrier*

# Mobile Device Forensics

## Network Call Data Records

---

### Cell Record History

What Is It?

Review of cell provider's historic records.



# Mobile Device Forensics

Why was cell technology developed?

**Limited Space!**

- Just like on the highway, there is a limited amount of space in which wireless frequencies can travel. This works fine when there are limited amount of devices talking to each other (walkie talkies) but presents an issue when there hundreds or thousands of devices.
- There simply isn't enough bandwidth for all of this chatter!



# Mobile Device Forensics

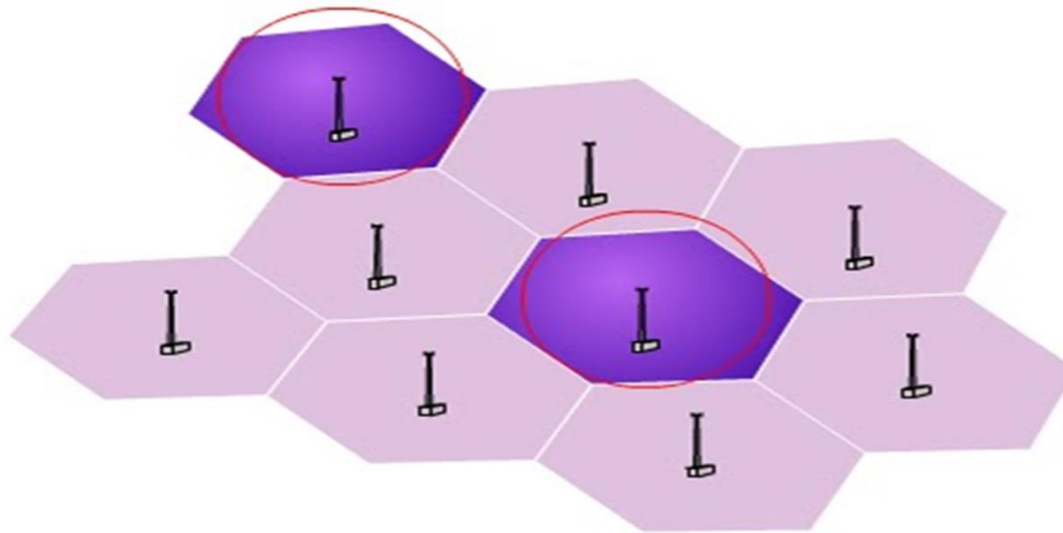


## Cell Grids

- Divide an area into small “cells” of coverage. This allows frequency re-use, so that many phones can be used in the same small area. Cell phones operate within cells, and they can switch cells as they move around.
- Each cell ranges in size depending on the density. Typically sized at about 10 square miles (26 square kilometers). Cells are normally thought of as hexagons on a big hexagonal grid.
- Because cell phones and base stations use low-power transmitters, the same frequencies can be reused in nonadjacent cells. The two purple cells can reuse the same frequencies.

# Mobile Device Forensics

Solution: Cell Grid



Cells are normally thought of as hexagons on a big hexagonal grid.



# Mobile Device Forensics



## MTSO – Carrier’s Central Office

### Mobile Telephone Switching Office

---

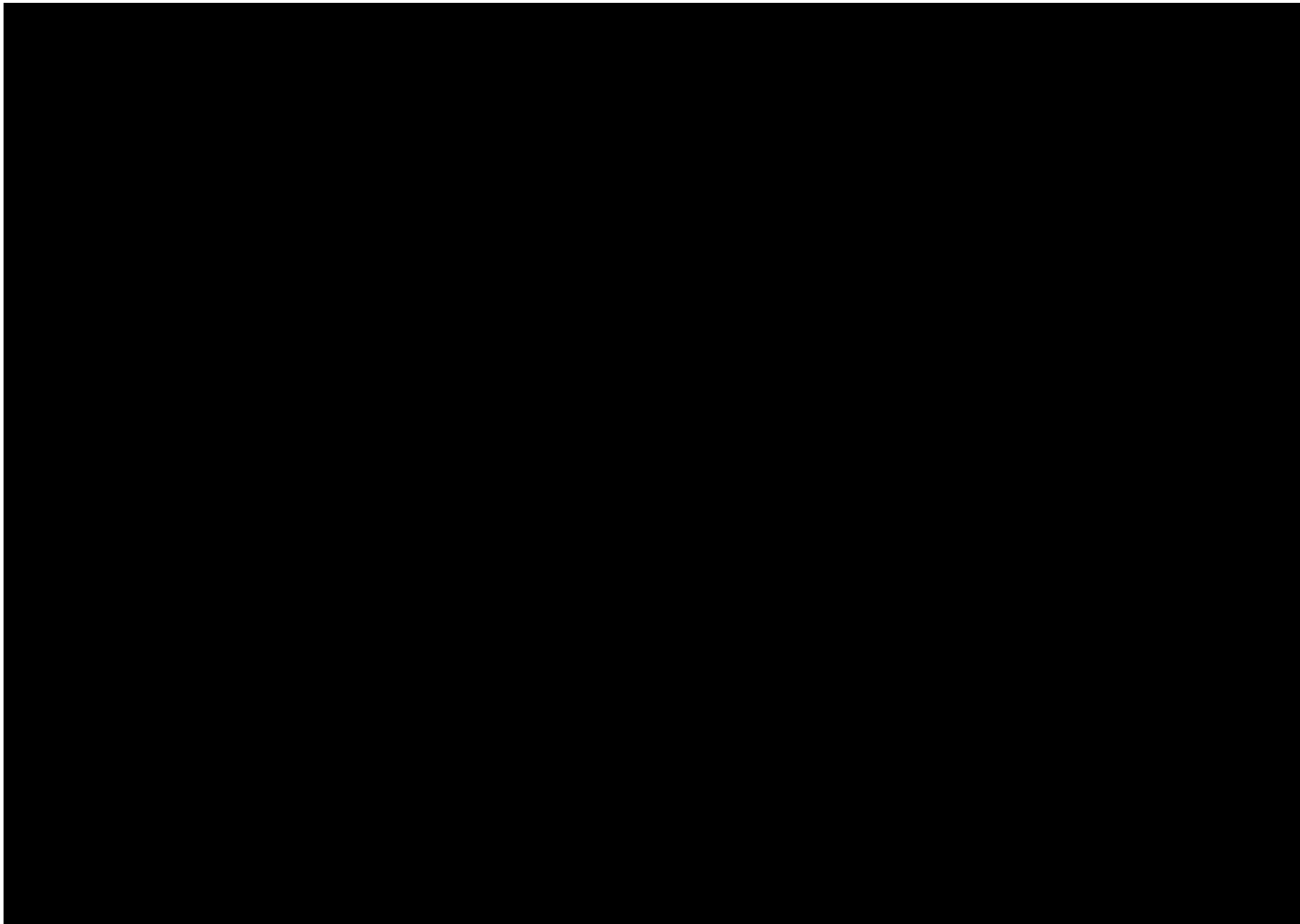
- In cities/regions, mobile carrier operates hundreds or thousands of cell towers, which route calls and data to the carrier’s backbone network.
- Each carrier in each city/region also runs one central office called the Mobile Telephone Switching Office (MTSO). This office handles all of the phone connections to the normal land-based phone system and controls all of the base stations in the region.
- This office handles all of the phone connections to the normal land-based phone system and controls all of the base stations in the region.

# Mobile Device Forensics

## Phone Codes



- All cell phones have special **codes** associated with them. These codes are used to identify the phone, the phone's owner and the service provider.
- **GSM:**
  - Serial Number – IMEI/MSISDN
  - SIM Cards - ICCID
  - IMSI – Subscriber Record
- **CDMA:**
  - Serial Number - ESN/MEID (CDMA)
  - Phone Numbers – MIN/MDN
- **System Identification Code (SID):** A unique number that is assigned to each carrier by the FCC



# Mobile Device Forensics

## Congestion within Cell Grids



- 
- Each tower is designed to accommodate a set number of calls per second, per a certain geographic area.
  - In a crisis (9-11, Boston Marathon), when everyone naturally reaches for their phone, that limit is quickly surpassed and the radios on the tower get sluggish.
  - If the closest tower is overloaded, the MTSO can route you to a farther tower.

# Mobile Device Forensics

## Where's your Cell Phone?



- Locational Data (Cell Phone Self Tracking)
  - GPS
  - Triangulation\*
  - Wi-Fi signals\*
    - \*even with the GPS off, a phone can locate itself.
- Service Provider
  - Cell Tower Records

# Mobile Device Forensics

## Location: GPS/Triangulation

- Triangulation – Three cell phone towers are used to approximate the location of the phone.
- GPS – Satellites are used to pinpoint the location of the phone.

Note – FCC E911 regulations require wireless carriers to be able to track 911 callers. FCC proposing rules that would require greater accuracy.

# Mobile Device Forensics

## Location: Cell Tower Records

- Service providers keep logs of what cell phones were connected to what towers at what time.
- Towers are constantly pinging cell phones to provide service, so a caller's whereabouts and path of travel are generally traceable.
- Relies only on tower data — that is, the records of which cell tower the defendant's phone was connecting through and from which angle.
- Police and prosecutors can use this information in order to connect a suspect to a crime location.

# Mobile Device Forensics

## Network Call Data Records

### Call Data Record (CDR)

- **Data is Not Kept Long! Only History.**
- **Tower Information As To Where Calls Originated or Received.**
- **Data Acquired From Call Data Records**
  - **Number Called and Received**
  - **Switch Center / Server Identification (2G/3G Network Interface)**
  - **Call Type for Billing Purposes (Day/Night + Weekend)**
  - **Length of Call**
  - **Start and Stop Time**
  - **Location Area Code (LAC)**
  - **Cell Identity – Start CI and Finish CI**
  - **Tower Location Name and GPS Coordinates**
  - **Voicemail Call Number**
  - **SMS Service Center Number... and more**



# Mobile Device Forensics

## Network Call Data Records

### Sample Call Data Record

Voice Usage For: (203) 855-5387  
Account Number: 3040503059

Item	Date	Time	Number Called	Calls To	Mins	Feature Used	Usage Type	Charge	Roam Type	Switch Code	Sid	Serving Area	LAC	Start / End CI
1	03/14/08	4:32P	(203) 246-0430	NORWALK	5	M2MTMB	DT	\$0.00	H	BOTNM0	T-Mobile / Connecticut	Fairfield CT	32199	62681 / 62681
2	03/14/08	4:42P	(203) 556-7836	INCOMING	2	M2MCNG	DT	\$0.00	H	BOTNM0	T-Mobile / Connecticut	Fairfield CT	32199	63562 / 63221
3	03/14/08	5:02P	(203) 424-1234	STAMFORD	12	M2MCNG	DT	\$0.00	H	BOTNM0	T-Mobile / Connecticut	Fairfield CT	32199	60102 / 60118
4	03/14/08	5:10P	(203) 556-7836	STAMFORD	5	M2MCNG	DT	\$0.00	H	BOTNM0	T-Mobile / Connecticut	Fairfield CT	32199	50002 / 50002
5	02/05/08	6:39P	(203) 424-1230	STAMFORD	2	M2MCNG	DT	\$0.00	H	BOTNM0	T-Mobile / Connecticut	Fairfield CT	32199	60103 / 50002



## Retention Periods of Major Cellular Service Providers

Data gathered by the Computer Crime and Intellectual Property Section, U.S. Department of Justice

	Verizon	T-Mobile	AT&T/Cingular	Sprint	Nextel	Virgin Mobile <sup>1</sup>
<b>Subscriber Information</b>	Post-paid: 3-5 years*	5 years	Depends on length of service	Unlimited	Unlimited	Unlimited
<b>Call detail records</b>	1 rolling year	Pre-paid: 2 years Post-paid: 5 years	Pre-paid: varies Post-paid: 5-7 years	18-24 months	18-24 months	2 years
<b>Cell towers used by phone</b>	1 rolling year	Officially 4-6 months, really a year or more.	From July 2008	18-24 months	18-24 months	Not retained - obtain through Sprint
<b>Text message detail</b>	1 rolling year	Pre-paid: 2 years Post-paid: 5 years	Post paid: 5-7 years	18 months (depends on device)	18 months (depends on device)	60-90 days
<b>Text message content</b>	3-5 days	Not retained	Not retained	Not retained	Not retained	90 days (search warrant required with "text of text" request) Not retained
<b>Pictures</b>	Only if uploaded to website (customer can add or delete pictures any time)	Can be stored online and are retained until deleted or service is canceled	Not retained	Contact provider	Contact provider	Not retained
<b>IP session information</b>	1 rolling year	Not retained	Only retained on non-public IPs for 72 hours. If public IP, not retained.	60 days	60 days	Not retained
<b>IP destination information</b>	90 days	Not retained	Only retained on non-public IPs for 72 hours. If public IP, not retained.	60 days	60 days	Not retained
<b>Bill copies (post-paid only)</b>	3-5 years, but only last 12 months readily available	Not retained	5-7 years	7 years	7 years	n/a <sup>‡</sup>
<b>Payment history (post-paid only)</b>	3-5 years, check copies for 6 months*	5 years	Depends on length of service	Unlimited	Unlimited	n/a <sup>‡</sup>
<b>Store Surveillance Videos</b>	Typically 30 days	2 weeks	Depends. Most stores carry for 1-2 months	Depends	Depends	n/a
<b>Service Applications</b>	Post-paid: 3-5 years*	Not retained	Not retained	Depends	Depends	Not retained

\* May vary by former company

\*\* For records older than mid-Nov. 2007, Sprint can only provide bill reprints with outgoing info

‡ No bill copies, but list of credit card transactions does not expire

<sup>1</sup> Virgin Mobile is now owned by Sprint. Since companies have separate compliance offices, for now they are listed separately.

# Mobile Device Forensics



## Flaws: Cell Tower Records



- 
- When someone places a call, it does not automatically go to the closest tower. It's routed to the tower that the switching center determines is the best.
  - This depends on many factors: weather, time of day, types of equipment and technology, and call traffic.
  - Two individuals, subscribed to the same cellular provider, standing next to each other can still get different towers.

# Mobile Device Forensics



Location: Cell Tower Sensors



---

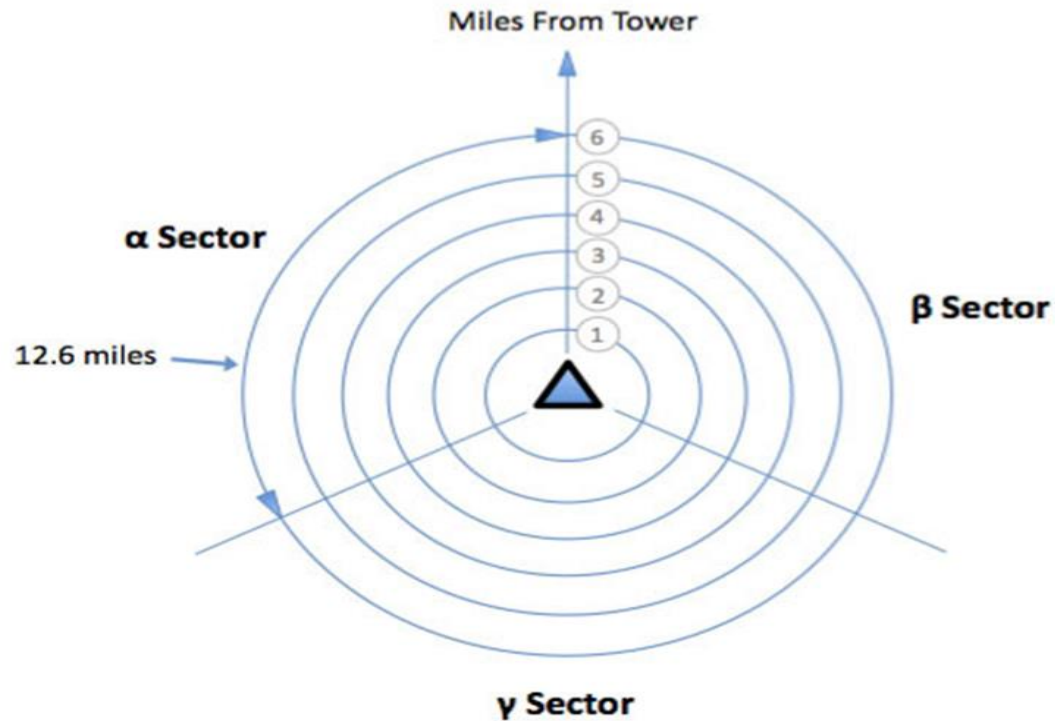
Cell towers typically have 3 sensors, each tracking 120° pie.



# Mobile Device Forensics

## Location: Cell Tower Sensors

Cell towers typically have 3 sensors, each tracking 120° pie.



# Mobile Device Forensics

## Location: Take Away

- The use of historical records is different than triangulation or GPS technology.
- Phone companies do not save GPS or triangulation data for an individual phone.
- Using phone company records. The only thing that you can say with confidence is that the phone connected to a cell site somewhere within a radius of many miles.
- Large margin of error!

# Mobile Device Forensics

## Location: Live Tracking

- Service provider asks the central switch the following question – “Where is the hardware associated with this phone number and billing record?”
  - Ping – Send a signal to your phone, phone reports back its location from it’s GPS.

# Mobile Device Forensics

## Surveillance

- Rogue tower (Stingray) – Device that impersonates a cell tower. Tricks phone into thinking you are the service provider.
- Only Military/FBI originally, but recently State and Local law enforcement now have this.
- A Private Citizen can theoretically buy it online but officially not legal.





## Legality

- When investigating a crime that occurred in the past, police tend to have two options:
  - seize the phone or
  - obtain the cell records.
- **Riley v. California**, a June 2014 Supreme Court decision made it mandatory for police to obtain warrants before searching the cell phones of people they arrest.
- Federal appellate courts are divided on the issue of whether a search warrant is needed to attain location records from cell providers.
- The disparity in requirements between the two could encourage police to rely increasingly on call-detail records.

# Mobile Device Forensics

## Case of Interest - Lisa Marie Roberts

- Girlfriend had been found strangled and dumped in a park.
- Accused of murdering girlfriend had been found strangled and dumped in a park.
- Prosecution had cell records purportedly showed she used her phone near where the body was found.
- Roberts claimed the call was made 8 miles away while driving.
- Roberts attorney urged her to take a plea, without having seen the evidence.
- Roberts was given a 15 year sentence for manslaughter.

# Mobile Device Forensics

## New Evidence - Exonerated!

- DNA evidence placed another suspect, a man, at the crime scene.
- Cell records showed that moments before the call in question, Roberts had received another call that came through a different cell tower.
- U.S. District Judge Malcolm F. Marsh threw out Roberts' guilty plea.
- Stating that “the presentation of expert testimony at trial, concerning the variables impacting the reliability of cell tower evidence to pinpoint a caller's location, likely would have changed the outcome of the trial.”
- After 12 years in jail, Roberts was released.

# Mobile Device Forensics

## Tools and Techniques of the Trade

### Preservation

- **RF Protection** – Required To Protect Device From The Network.

#### Faraday Box and Bag



**Airplane Mode and Keep the Device Charged.**

# Mobile Device Forensics

## Tools and Techniques of the Trade

### Data Capture Options

- **Screen Captures:** The simplest way. Use a camera to take pictures of what's on the screen. Reporting tools available. Sometimes this is the only way.
- **Logical Analysis:** – Extracting the data on the device that you see and can access on the device. No deleted information with this method. Call logs, phone books, SMS messages, pictures, email, browsing etc. The “active” information on the device can be extracted using a “Logical” extraction tool. This is the standard method today. Plenty of tools and easy to use.
- **Physical Analysis:** – The practice of extracting data from the physical memory of the device, and removable memory. Like PC forensics, you are getting the raw binary / hex data. Requires decoding and understanding of language and techniques used by device manufacturers. Physical analysis is the way to deleted information, but it is difficult and sparsely supported. Only a few tools. Mostly Nokia supported. Early days of the new standard.
- **Chip Level Analysis:** - Analysis of the chips in the phone by removing them from the device and probing for data, or rebuilding another phone. Extremely technical. Broken SIMs analyzed this way.

# Mobile Device Forensics

## Tools and Techniques of the Trade

### The Unfortunate Reality of the Forensic Collection Kit...

- **There Is No One Size Fits All Solution**
- **A Number of Mobile Device Forensic Tools on the Market**
- **Each have their strengths and weaknesses. Plenty of overlap of support, but success with devices varies.**
- **This is due to the challenges in supporting the continuous introductions of new phones and changing technologies. It's a tough job for the examiner to keep up – And equally difficult for the companies making the tools.**
- **Examiners Never Know What They Are Going To Get! Often need more than one tool for the multiple different devices out there.**
- **This is changing somewhat with a consolidation of mobile Operating Systems (Android, Apple, BlackBerry, Windows), but some tools will dig deeper in some areas than others.**

# Mobile Device Forensics

## Tools and Techniques of the Trade

### Today's Mobile Device Forensic Solutions



# Mobile Device Forensics

## Tools and Techniques of the Trade

### Screen Capture

Sometimes Taking A Picture is The Only Way To Get Data Off of a Phone



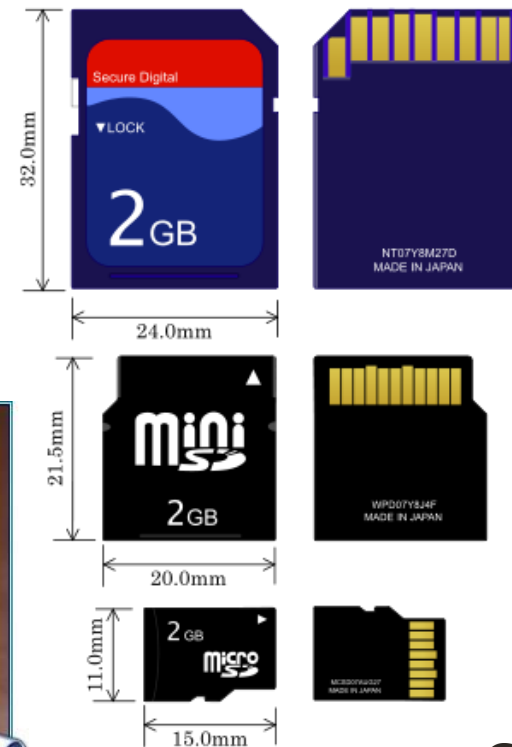


# Mobile Device Forensics

## Tools and Techniques of the Trade

### Storage Card Analysis

Today's smartphones are essentially handheld computers. Most cell phones come with a certain amount of internal storage with the option to expand that storage via an SD card. For example, my cell phone has 16GB of internal storage and I have a 16GB SD card. This allows storage of numerous documents, pictures, songs, videos, etc.



# Mobile Device Forensics

## Tools and Techniques of the Trade

### Logical Acquisition

“Logical” acquisition pulls the “Active” data off the device...

The screenshot displays a 'Project Tree' window with a hierarchical view of data extracted from an iPhone4CDMA device. The tree is organized into several main categories:

- Extraction Summary**
- Device Info**
- Images**
- Memory Ranges**
- File Systems**
  - Data (Apple : HFS [+])
  - System (Apple : HFS [+])
- Analyzed Data**
  - Bluetooth Devices (1)
  - Calendar (615)
  - Call Log (193)
  - Chats (91)
  - Contacts (1666)
  - Emails (394)
  - Installed Applications (77)
  - IP Connections (3)
  - Locations (816)
  - MMS Messages (1072)
    - Inbox (528)
    - Sent (544)
  - Passwords (51)
  - SMS Messages (1288)
  - User Accounts (5)
  - Voicemail (283)
  - Web Bookmarks (2)
  - Web History (13)
  - Wireless Networks (1)
- Data files**
  - Images (32486)
  - Videos (89)
  - Audio (816)
  - Text (577)
  - Databases (615)
  - Configurations (6381)
- Carving**
  - Images
- Tags**
  - Time line (9658)
  - Watch Lists (0)
  - Bookmarks (0)
  - Entity Bookmarks (0)
  - Reports

# Mobile Device Forensics

## Tools and Techniques of the Trade

### Physical Acquisition

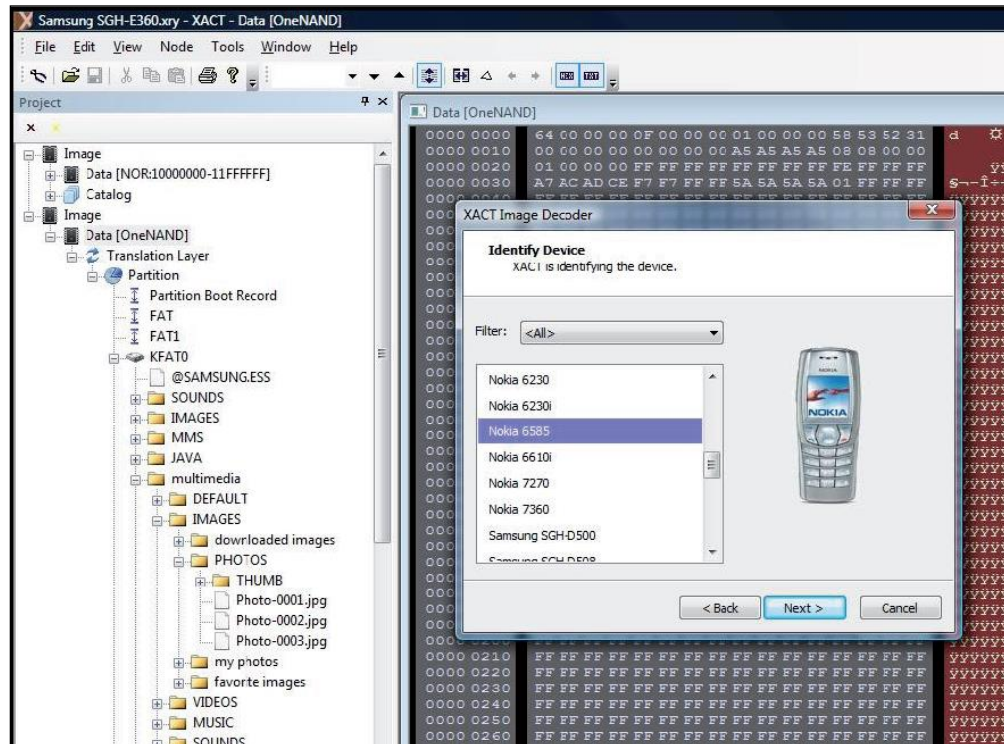
“Physical” acquisition accesses the internal memory and the Raw Data

Today's Top  
Tools:

XRY Physical


and

UFED  
Physical



# Mobile Device Forensics

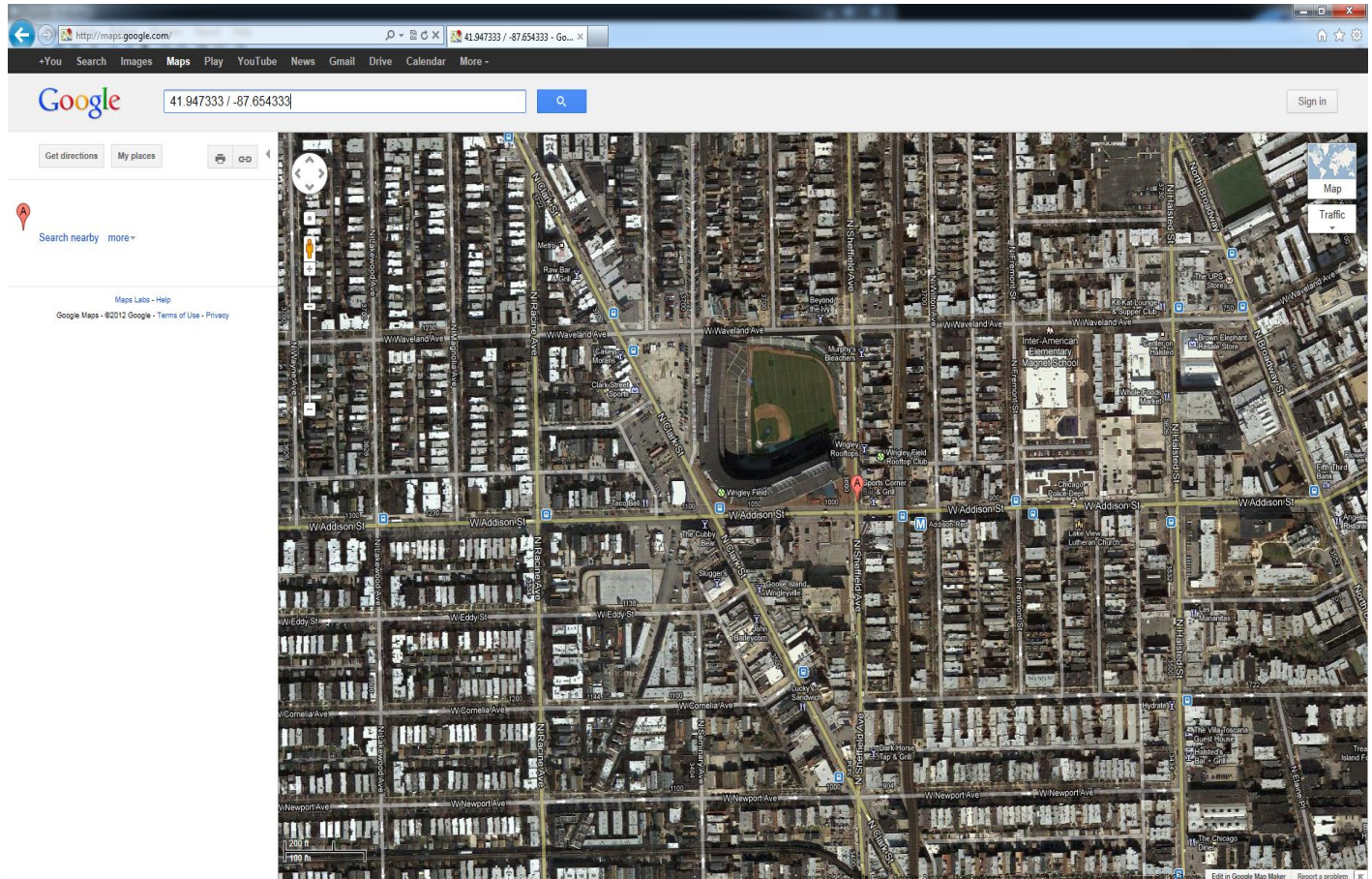
## Tools and Techniques of the Trade



Welcome X Extraction Summary X Locations (816) X IMG_1808.JPG X	
Hex View   Image view   <b>File Info</b>	
Find: <input type="text"/>	
EXIF	
GPSLatitudeRef	N
GPSLatitude	41.56.84.0
GPSLongitudeRef	W
GPSLongitude	87.39.26.0
GPSAltitudeRef	0
GPSAltitude	197
GPSTimeStamp	17.21.9.34
GPSImgDirectionRef	T
GPSImgDirection	319.206008583691
Make	Apple
Model	iPhone4,1
Orientation	0
XResolution	72
YResolution	72
ResolutionUnit	0
Software	5.1.1
DateTime	2012:07:28 12:21:09
YCbCrPositioning	0
ExposureTime	0.000733137829912023
FNumber	2.8
ExposureProgram	0
ISO SpeedRatings	0
ExifVersion	0.0.0.0
DateTimeOriginal	2012:07:28 12:21:09
DateTimeDigitized	2012:07:28 12:21:09
ComponentsConfiguration	0,1,197,1
ShutterSpeedValue	10.4132434089516
ApertureValue	2.97085357390701
BrightnessValue	9.38772663877266
MeteringMode	0
Flash	0
FocalLength	3.85
SubjectArea	1295,967,699,696
FlashpixVersion	3910588146.951570612.2604473868.2158275633
ColorSpace	0
PixelXDimension	2592
PixelYDimension	1936
SensingMethod	0
ExposureMode	0
WhiteBalance	0
DigitalZoomRatio	3.18300996329313
SceneCaptureType	0
Sharpness	0
File Metadata	
Camera Make	Apple
Camera Model	iPhone4,1
Capture Time	7/28/2012 12:21:09 PM
Lat/Lon	41.947333 / -87.654333
Pixel resolution	2592x1936
Resolution	72x72 (Unit: Inch)

# Mobile Device Forensics

## Tools and Techniques of the Trade



# Mobile Device Forensics

## Mobile Virtual Network Operators

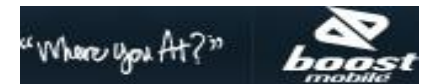
### Throw Away Phones

## Mobile Virtual Network Operators

**What are They?** “Virtual” operators selling mobile services. Operating on larger networks.

**Why are They?** Marketing to specific demographics. Reduce contract restrictions.

**Who are They?**



# Mobile Device Forensics

## Tools and Techniques of the Trade



### Throw Away Phones

#### A Challenge for Forensic Efforts

- Plans and Devices often Paid for in cash. No contract, no identity tied to the device or service contract
- Often a disposable solution for criminals
- Some proprietary devices not widely supported by forensic solutions (this is changing)

#### This Does Not Mean There is Not Valuable Data on Device

- SIM Card Data (TracFone, Boost, T-Mobile)
- Last Numbers Dialed on Device/SIM
- Call Logs, Call Durations
- Pictures
- Text Messages (message identifiers)

# Mobile Device Forensics

## Tools and Techniques of the Trade



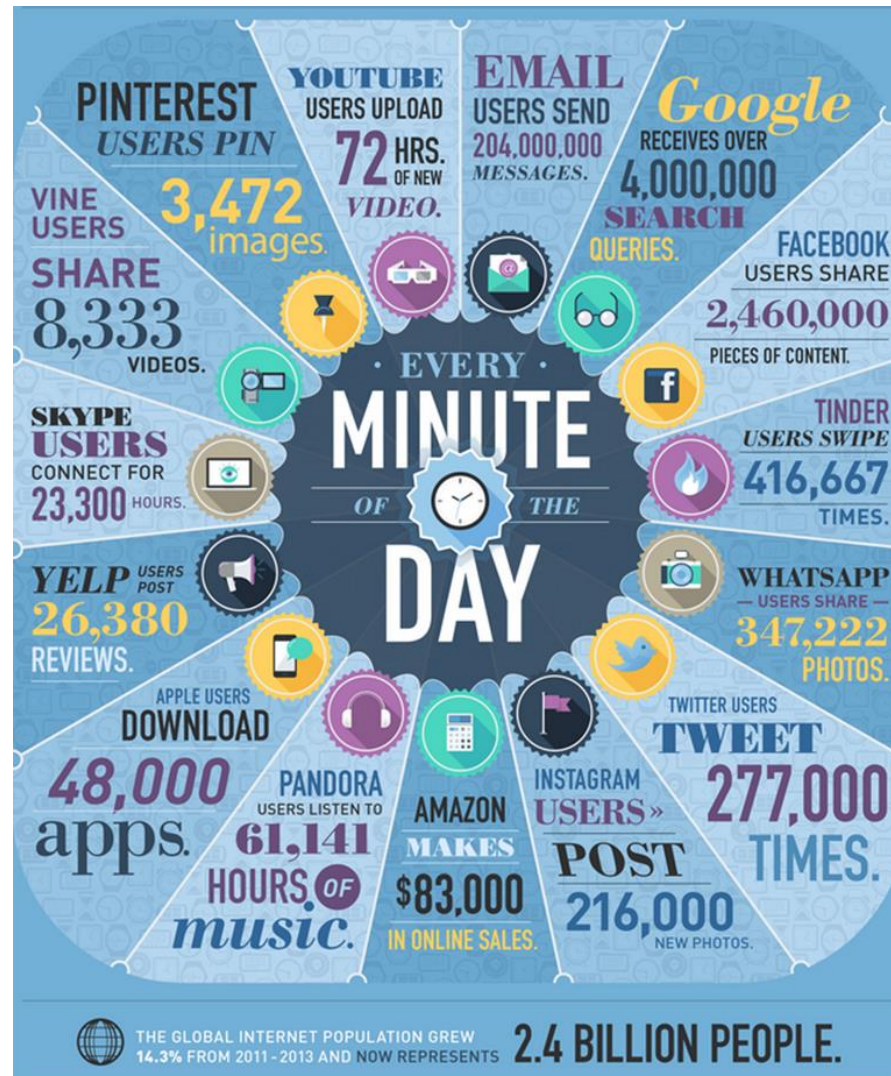
### Questions to ask for a cell phone collection

- What type of phone? Be very specific (i.e. Apple iPhone 5S)
- Is it password protected? If so, attempt to get the password
- Is the phone encrypted?
- How long can the user go without the phone?
- Can the acquisition be done in a lab environment as opposed to on site?
- What information are you looking for?
- Please preserve the phone – photograph, airplane mode, shut off.



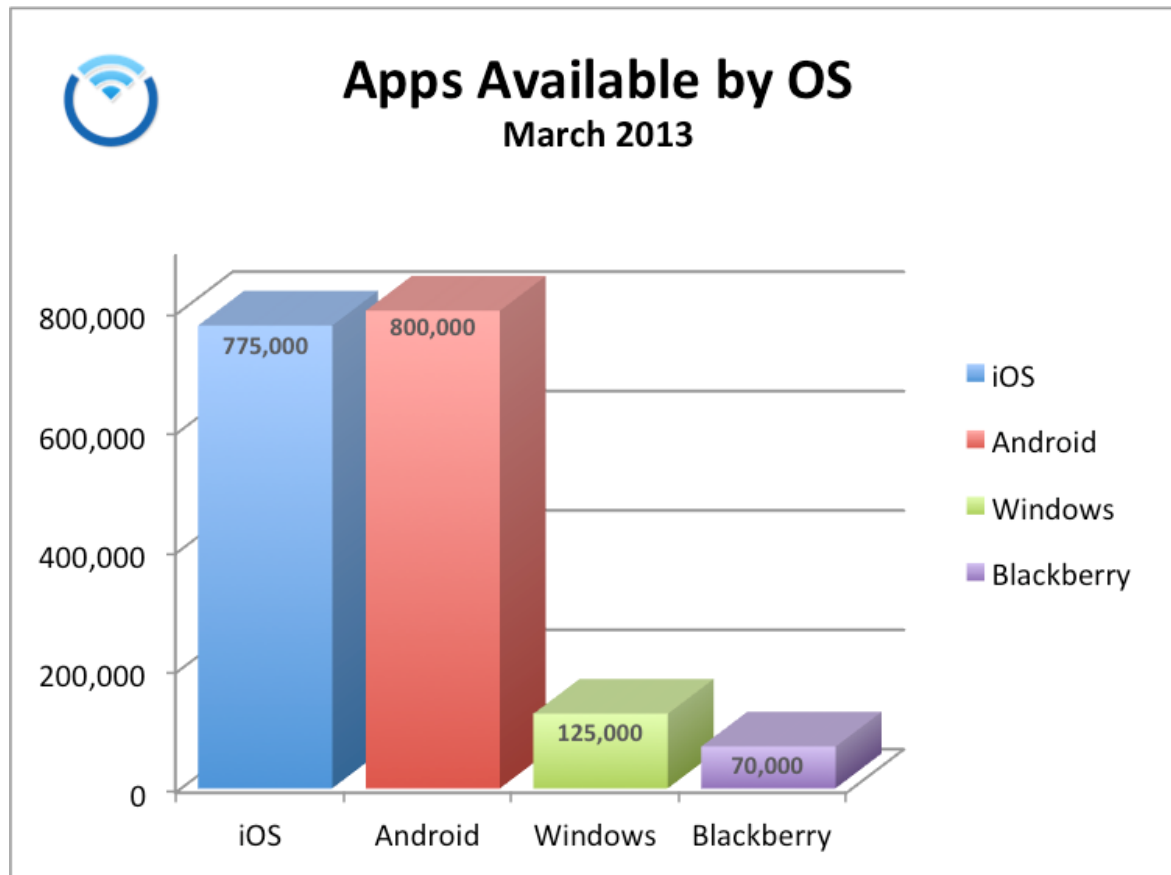
# Every Minute of the Day...

Sixty seconds seems like an insignificant amount of time, but when you look at it in terms of how much data is created, there's a whole lot going on...



# Mobile Device Forensics

## App Store Trends



# Mobile Device Forensics

## Communication in 2014



### Would you call for help?

- Two girls lost in a storm water drain in Adelaide, Australia, updated their Facebook status instead of calling emergency services on Sunday night. They were fortunate a young friend was online at the time and was able to call for help for them.
- In Atlanta, Georgia, a councilman was concerned that his cellphone battery would be “flat” by the time a 911 call connected. Instead, he Tweeted: "Need a paramedic on corner of John Wesley Dobbs and Jackson St. Woman on the ground unconscious. Pls ReTweet".
- A Tulsa woman hid in a basement and used Facebook to call for help when men broke into her home early Monday. "Somebody please help me. Here's my address. Call 911. Call the police. There's people in my house!"

# Mobile Device Forensics

## Application Forensics

The screenshot displays the X1 Social Discovery - v4 application interface. The search bar at the top contains the term "dessert". The left sidebar lists various social media sources: Everything, Twitter, Instagram, Facebook, Web Capture, Gmail, and LinkedIn. The main content area shows a list of search results. The top result is a tweet from Dave Winfields (@DaveWinfields) dated 3/24/2014 at 8:13 AM, mentioning "Dessert Bowls" and "prepping". The second result is a tweet from TATHiessen (@TATHiessen) dated 3/18/2014 at 7:03 PM, mentioning "#DinneratTiffani's Sun, Mar 23rd at 8pm ET/5pm PT on @CookingChannel w/ @NathanFillion @WillieGarson #lindsayprice". The right sidebar shows a list of replies to the selected tweet, including congratulations from Favstar.fm and replies from Kenny Johnson and Zac Young. The bottom status bar indicates "4,389 items indexed", "2 of 2" items displayed, and "Active Case collection is on Indexing Twitter-Howard Williams".

# Mobile Device Forensics

## Application Forensics

The screenshot displays the X1 Social Discovery v4 application interface. The main window is titled "X1 Social Discovery Map" and features a "Location-Based Search" overlay. The search overlay includes a map of the Los Angeles area with a red rectangle indicating the search area. A tweet from user "stonedxf" is highlighted, with the text "O wait is my last RT even still relevant?". The tweet is dated 3/25/2014 4:25:35 PM. The interface also shows a sidebar with navigation options like "Everything", "Twitter", "Public Information", and "Searches". The status bar at the bottom indicates "5,297 items indexed" and "4 (2 items selected / 2 in grid) of 4,682".

# Mobile Device Forensics

## Russian soldier Alexander Sotkin

- Posted two photos of himself to Instagram from within Ukraine -- one on June 30 and another on July 5.
- The Russian army denies that its troops have crossed the Ukraine border.
- Russia claimed the photos were forgeries and the locations of the selfies were falsified.
- Photo Map uses GPS to determine its users' locations, a tool that is generally accurate with 50 feet or so.



# Mobile Device Forensics

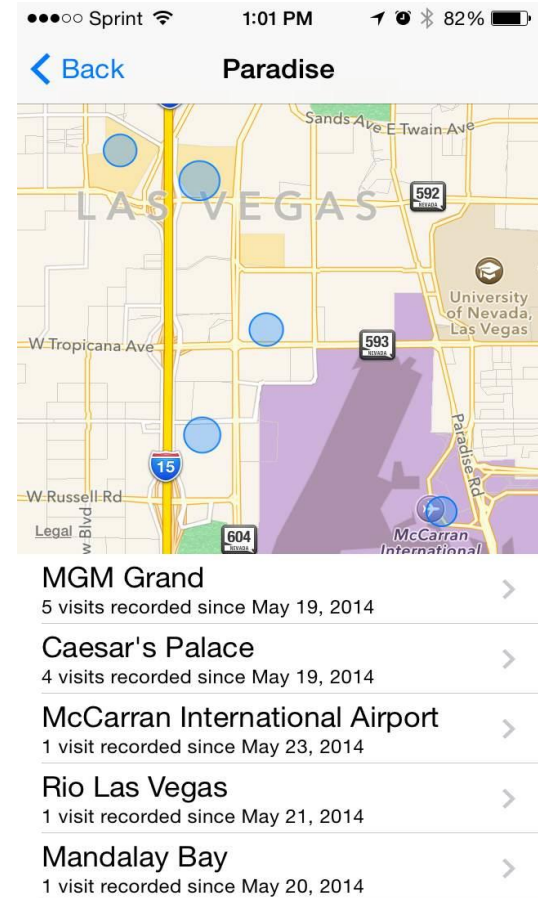
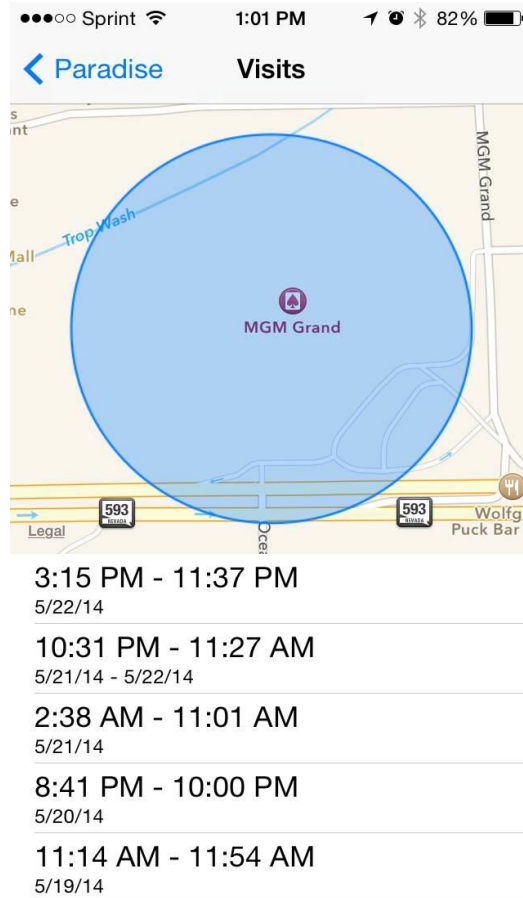
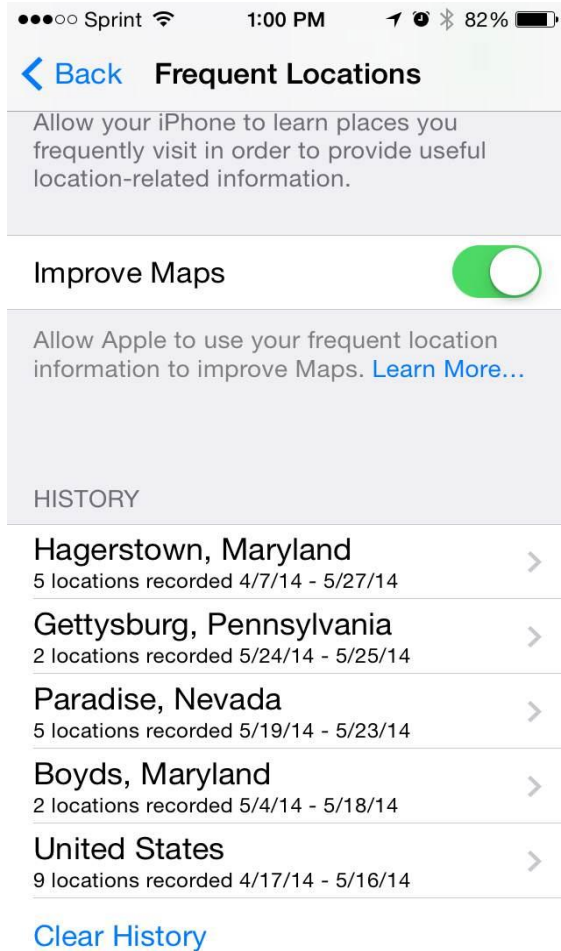


## Terms and Conditions

**(b) Location Data.** Apple and its partners, licensees and third party developers may provide certain services through your iOS Device that rely upon location information. To provide and improve these services, where available, Apple and its partners, licensees and third party developers may transmit, collect, maintain, process and use your location data, including the real-time geographic location of your iOS Device, road travel speed information, location search queries, and location of where you purchase and launch applications. The location data and queries collected by Apple are collected in a form that does not personally identify you and may be used by Apple and its partners, licensees and third party developers to provide and improve location-based products and services. **By using any location-based services on your iOS Device, you agree and consent to Apple's and its partners', licensees' and third party developers' transmission, collection, maintenance, processing and use of your location data and queries to provide and improve such products and services.**




# iPhone Artifacts



Settings | Privacy | Location Services | System Services | Frequent Locations




# Mobile Device Forensics



## Steps in any exam



Attorney or forensic examiner:

- 
- Try to get include the charging cable when taking custody of a phone
  - Ask for the pass code or swipe code!
  - Put into airplane mode, turn off Bluetooth, turn off WiFi
  - If unsure how to put into airplane mode, Google the make/model, download the user manual or user guide
  - Check the manufacturer's site, the wireless provider site, [phonearena.com](http://phonearena.com) or [pdab.net](http://pdab.net) for information

# Mobile Device Forensics

## Steps in any exam

Let's look at the HTC One



# Mobile Device Forensics

## Steps in any exam

Airplane mode, per the user guide, obtained by chatting with a verizonwireless.com tech

Do any of the following to turn Airplane mode on or off:

- Press and hold POWER, and then tap Airplane mode.
- With two fingers, swipe down from the status bar to open the Quick Settings panel. Tap the Airplane mode tile to turn airplane mode on or off.

When enabled, the Airplane mode icon ✈ is displayed in the status bar.

# Mobile Device Forensics

## Steps in any exam

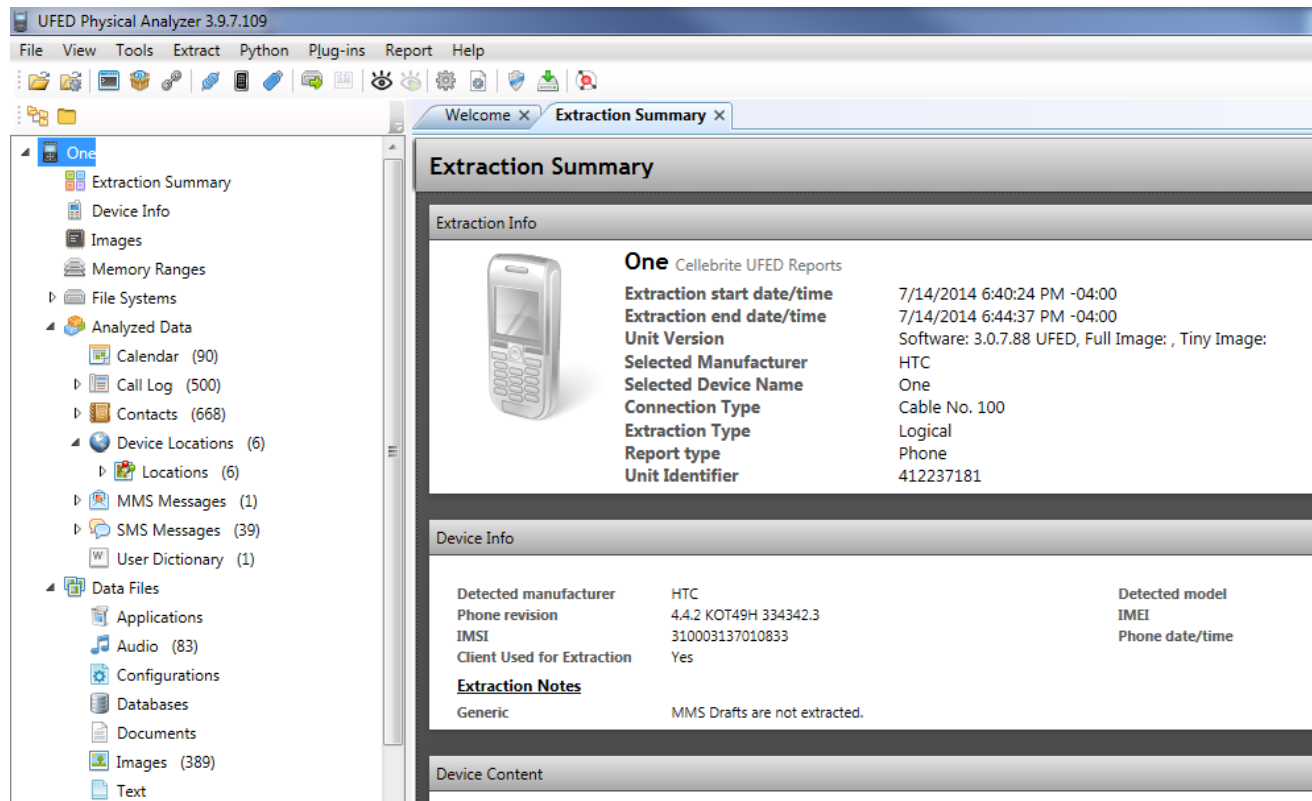
Per the Cellebrite list of supported devices  
[currently 6,513 models]

	A	B	C	D	F	G	H	I	Q	S	U
1	Vendor	Model	Phonebook Read	Call Logs Read	SMS Read	MMS Read	iMessages Read	Email Read	Memory Card Read	Platform	Connectivity Tip
911	HTC	6875 Touch Pro2 (CDMA)	Y	Y	Y				Y	WinMo	Cable A With Black Tip 80
912	HTC	6875 Tilt2 (GSM)	Y	Y	Y				Y	WinMo	Cable A With Black Tip 80
913	HTC	6875 Touch Pro2 (GSM)	Y	Y	Y				Y	WinMo	Cable A With Black Tip 80
914	HTC	HTC6500LVW One	Y	Y	Y	Y				Android	Cable A With Black Tip 100
915	HTC	HTC6515LVW	Y	Y	Y	Y			Y	Android	Cable A With Black Tip 100
916	HTC	XV6975 Imagio (CDMA)	Y	Y	Y				Y	WinMo	Cable A With Black Tip 80
917	HTC	MWP6885 7 Pro (USB)								WinPhone	Cable A With Black Tip 100
918	HTC	MWP6885 7 Pro (BT)	Y							WinPhone	
919	HTC	XV6975 Imagio (GSM)	Y	Y	Y				Y	WinMo	Cable A With Black Tip 80
920	HTC	PN07200 One	Y	Y	Y	Y				Android	Cable A With Black Tip 100
921	HTC	PC93100 Arrive (USB)								WinPhone	Cable A With Black Tip 100
922	HTC	T7575 Arrive (USB)								WinPhone	Cable A With Black Tip 100
923	HTC	PC93100 Arrive (BT)	Y							WinPhone	
924	HTC	T7575 Arrive (BT)	Y							WinPhone	
925	HTC	A8180	Y	Y	Y	Y			Y	Android	Cable A With Black Tip 100
926	HTC	T8788 Surround (USB)								WinPhone	Cable A With Black Tip 100
927	HTC	T8788 Surround (BT)	Y							WinPhone	

# Mobile Device Forensics

## Examination Results


### The extraction summary



The screenshot displays the UFED Physical Analyzer 3.9.7.109 interface. The left sidebar shows a tree view of analyzed data, including Calendar (90), Call Log (500), Contacts (668), Device Locations (6), MMS Messages (1), SMS Messages (39), User Dictionary (1), and Data Files (Applications, Audio (83), Configurations, Databases, Documents, Images (389), Text). The main window shows the 'Extraction Summary' report for a device named 'One'.

**Extraction Summary**

**Extraction Info**

	<b>One</b> Cellebrite UFED Reports
<b>Extraction start date/time</b>	7/14/2014 6:40:24 PM -04:00
<b>Extraction end date/time</b>	7/14/2014 6:44:37 PM -04:00
<b>Unit Version</b>	Software: 3.0.7.88 UFED, Full Image: , Tiny Image:
<b>Selected Manufacturer</b>	HTC
<b>Selected Device Name</b>	One
<b>Connection Type</b>	Cable No. 100
<b>Extraction Type</b>	Logical
<b>Report type</b>	Phone
<b>Unit Identifier</b>	412237181

**Device Info**

<b>Detected manufacturer</b>	HTC	<b>Detected model</b>
<b>Phone revision</b>	4.4.2 KOT49H 334342.3	<b>IMEI</b>
<b>IMSI</b>	310003137010833	<b>Phone date/time</b>
<b>Client Used for Extraction</b>	Yes	

**Extraction Notes**

Generic	MMS Drafts are not extracted.
---------	-------------------------------

**Device Content**

# Mobile Device Forensics

## Examination Results

### Calendar entries

JFED Physical Analyzer 3.9.7.109

View Tools Extract Python Plug-ins Report Help

Welcome x Extraction Summary x Calendar (90) x

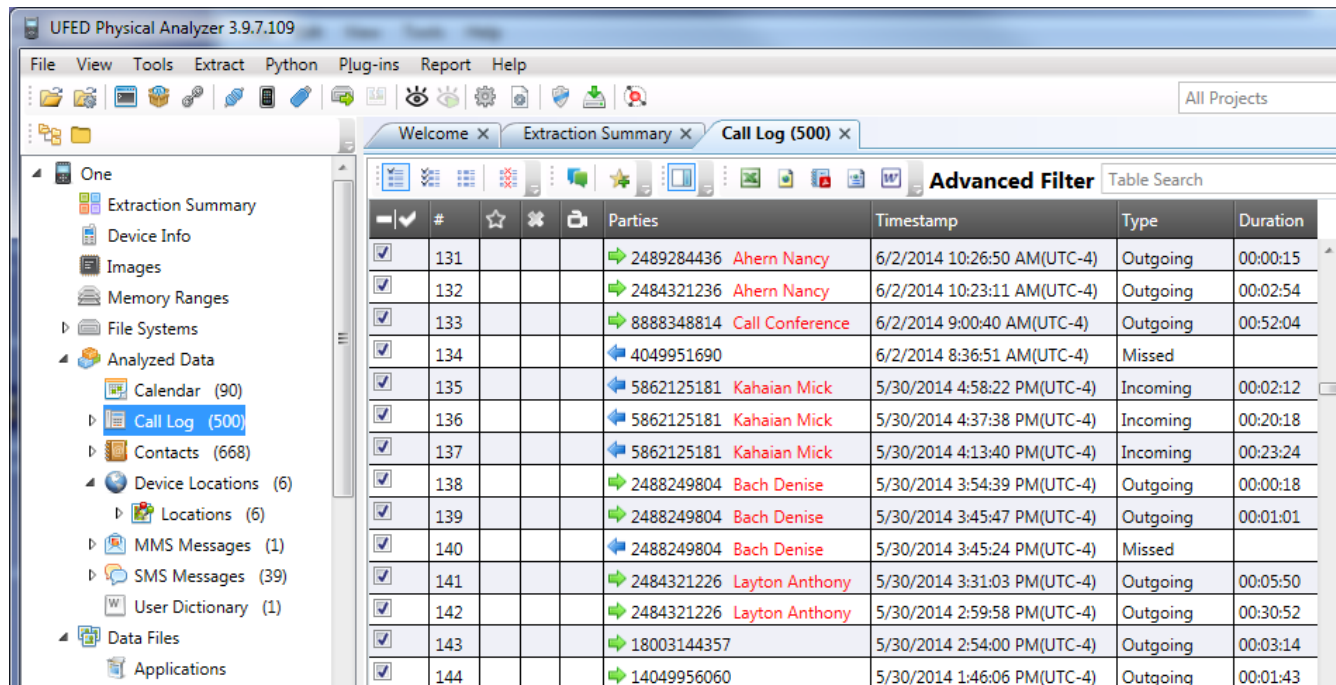
Advanced Filter

#	Location	Subject	Attendees
0	Southfield, MI	Garry In Southfi...	
1		NAZ - PTO	
2	Southfield, MI	Garry In Southfi...	
3	IL Client Conf C (14 - 18)...	DAFS Quarterly...	
4	Host City: Houston	Quarterly Firm-...	
5	Southfield, MI	Garry In Southfi...	
6	Chicago, IL	Relativity Fest	
7		NAZ - PTO	
8	Brush Creek Ranch - Wy...	2014 Retreat Sa...	
9		AJL - PTO	
10		NAZ - PTO	
11	Southfield, MI	Garry In Southfi...	
12		NAZ-PTO	
13	Nashville, TN	ILTA 2014	

# Mobile Device Forensics

## Examination Results

### Call logs



The screenshot displays the UFED Physical Analyzer 3.9.7.109 interface. The 'Call Log (500)' window is active, showing a table of call records. The table has columns for '#', 'Parties', 'Timestamp', 'Type', and 'Duration'. The 'Parties' column includes phone numbers and names. The 'Type' column indicates whether the call was outgoing, incoming, or missed. The 'Duration' column shows the length of each call.

#	Parties	Timestamp	Type	Duration
131	2489284436 Ahern Nancy	6/2/2014 10:26:50 AM(UTC-4)	Outgoing	00:00:15
132	2484321236 Ahern Nancy	6/2/2014 10:23:11 AM(UTC-4)	Outgoing	00:02:54
133	8888348814 Call Conference	6/2/2014 9:00:40 AM(UTC-4)	Outgoing	00:52:04
134	4049951690	6/2/2014 8:36:51 AM(UTC-4)	Missed	
135	5862125181 Kahaian Mick	5/30/2014 4:58:22 PM(UTC-4)	Incoming	00:02:12
136	5862125181 Kahaian Mick	5/30/2014 4:37:38 PM(UTC-4)	Incoming	00:20:18
137	5862125181 Kahaian Mick	5/30/2014 4:13:40 PM(UTC-4)	Incoming	00:23:24
138	2488249804 Bach Denise	5/30/2014 3:54:39 PM(UTC-4)	Outgoing	00:00:18
139	2488249804 Bach Denise	5/30/2014 3:45:47 PM(UTC-4)	Outgoing	00:01:01
140	2488249804 Bach Denise	5/30/2014 3:45:24 PM(UTC-4)	Missed	
141	2484321226 Layton Anthony	5/30/2014 3:31:03 PM(UTC-4)	Outgoing	00:05:50
142	2484321226 Layton Anthony	5/30/2014 2:59:58 PM(UTC-4)	Outgoing	00:30:52
143	18003144357	5/30/2014 2:54:00 PM(UTC-4)	Outgoing	00:03:14
144	14049956060	5/30/2014 1:46:06 PM(UTC-4)	Outgoing	00:01:43

# Mobile Device Forensics

## Examination Results

Analytics which combines a count of how many phone calls and email messages were exchanged between the user and others

#	Is a contact	Name	Phones	Emails	Other Entri	Total	Phone Even	Email Even
1	True	Kahaian Mick	Phone (Mobile) '(586) 212-5181' Phone (Work) '2484321205'			84	84	0
2	True	Ross Stout Risius	Phone (Mobile) '2482088800'			57	57	0
3	True	Layton Anthony	Phone (Mobile) '(248) 996-2053' Phone (Work) '2484321226'			38	38	0
4	True	Astras Paul	Phone (Mobile) '(248) 798-2731' Phone (Work) '2484321202'			37	37	0
5	True	Call Conference	Phone (Work) '8888348814'			31	31	0
6	True	Bach Denise	Phone (Mobile) '(248) 824-9804' Phone (Work) '2484321278'			28	28	0



# Mobile Device Forensics

---



Questions?



# Your Partner in E-Discovery

Bridging the Gap Between Discovery and Technology



## ■ ■ Solutions



Grounded in its core values of positive team attitude, accountability, commitment, entrepreneurial and relationship focused, SRR emphasizes a results-oriented approach which provides creative solutions for your most complex situations.

SRR – Your partner in E-Discovery

**2014** **BEST OF**  
**THE NATIONAL**  
**LAW JOURNAL**

Finalist | Stout Risius Ross | End-to-End E-Discovery Provider



## Disclaimer

This document is intended for the internal use of the recipient only (attendees of the Cell Phone Science Seminar held October 10, 2014, as part of the Criminal Advocacy Program) and may not be distributed or released to any third party without the prior written consent of Stout Risius Ross, Inc. This document presents information designed to educate the recipient on the basics of mobile device tracking and forensics, and is not intended to be formal legal advice.

