Ethical Issues and Technology

Presented By:

Barrett Kiernan, Cozen O'Connor

Matt Scott, Practice Leader, Digital Forensics Group

ENVISTA FORENSICS

COZEN O'CONNOR

Overview

- Use of social media in claim investigation and litigation
- Metadata – what is it and how can you use it?
- Cellphone investigations

COZEN O'CONNOR

Social Media

- Let me count the ways

COZEN O'CONNOR

Social Media

- Recoverable from devices

#	Sender Name	Message Sent Date/Tim...	Message	Message ID
1...	[redacted]	08/24/2013 06:19:26 PM	Jeffrey I'm glad to know that you may it back safe. I Love you and see you soon.	eo3I+RjlqF1pge/dAtQ+JQ
1...	[redacted]	08/24/2013 02:18:31 PM	Kool	fOCQjcyTvnXXm6OEhRdBZQ
1...	[redacted]	08/26/2013 12:40:02 PM	Nothing much..what's up?	mid.1377534156569:622abff9ae58c2d596
1...	[redacted]	08/25/2013 11:14:07 PM	Oh...ok	82ywr0JRolHR+nua3MKVgw
2...	[redacted]	08/03/2013 11:35:31 AM	Okay just let me know my man and Have a good time at the Party	mid.1375385887628:ae96b6994b157dfd58
2...	[redacted]	08/02/2013 08:57:42 PM	Or I guess I should say Meet Again. You can call me when you get a chance. 412-758-76...	mid.1375477250384:c1a63757a76da6f699
1...	[redacted]	08/26/2013 04:22:32 AM	That is what I am trying to figure out....I do not know this dude.....so wjhy is he trying to add...	msg.f697d1bf2b07d71d31b5be5d0f54c15d19
2...	[redacted]	08/02/2013 04:58:18 PM	well, I am shocked :-P	mid.1375477098099:40222b592a4ff3b594
1...	[redacted]	08/14/2013 12:45:06 AM	What poppin off tonight?	id.514414661911758
1...	[redacted]	08/25/2013 10:58:11 PM	Who are you?	mid.1377485891710:b12aa9983015216d84
1...	[redacted]	08/25/2013 09:29:25 AM	Yes you did but I had no way of knowing when exactly you would be here. I will just have t...	7udRviMsPvPxC03KEiHvfQ
1...	[redacted]	08/10/2013 10:31:33 PM	You should call Kim to see if she wants to hang out 412-241-8079. Chucky's group Brothe...	YIB4toUF7zpdmK3JhRg6fA
1...	n/a	12/11/2013 03:17:16 PM	Did?	mid.1386363018035:0654acb18567cbe038

COZEN O'CONNOR

Social Media

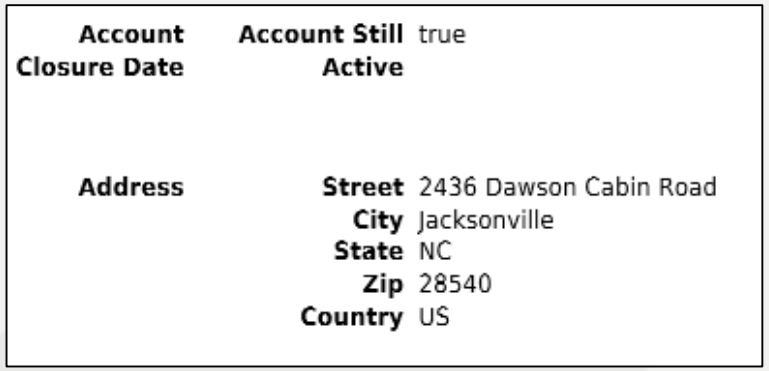
- Facebook records example

Facebook Business Record Page 1

Service Facebook
Target 1430216564
Generated 2017-01-10 17:05:24 UTC
Date Range 2014-05-01 00:00:00 UTC to 2014-10-31 23:59:59 UTC
NCMEC Cybertips

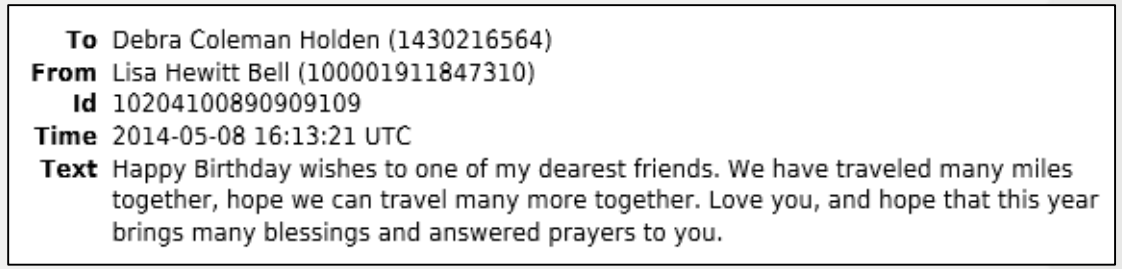
Name
First Debra
Middle Coleman
Last Holden

Registered Email Addresses debra.c.holden@facebook.com, sis3ms@aol.com



Account Closure Date
Account Still Active true

Address
Street 2436 Dawson Cabin Road
City Jacksonville
State NC
Zip 28540
Country US



To Debra Coleman Holden (1430216564)
From Lisa Hewitt Bell (100001911847310)
Id 10204100890909109
Time 2014-05-08 16:13:21 UTC
Text Happy Birthday wishes to one of my dearest friends. We have traveled many miles together, hope we can travel many more together. Love you, and hope that this year brings many blessings and answered prayers to you.

Includes

- Logins
- likes
- Posts
- Comments
- Photos
- Location data
- More…

COZEN O'CONNOR

Social Media

- Obtaining social media information informally
  - Do account holders have a privacy interest in social media content?
  - Ethical limitations on use and “friending” opposing parties.
  - Ethical rules on contacting represented parties via social media.
  - Duty to investigate.

COZEN O'CONNOR

Social Media

- Obtaining social media information in litigation
  - Stored Communications Act, 18 U.S.C. § 2701
  - Narrow discovery requests are important because social media sites are “notoriously resistant to subpoena efforts, and websites urge parties to resolve discovery issues without involving them.”
  - Crispin v. Christian Audiger, Inc., 717 F. Supp. 965 (C.D. Cal. 2010): subpoena for Facebook and MySpace private messages was quashed and case remanded “to determine whether wall postings and comments were public or private.”

COZEN O’CONNOR

Social Media

- Attorneys should make formal discovery requests to parties for social media content.
- Request must be – no broad fishing expedition.
- Privacy interests is not an absolute bar to discovery.
- Case example - Romano v. Steelcase Inc., 907 N.Y.S.2d 650 (S. Ct. Suff. Cty. 2010) (“Discovery of Plaintiff’s Myspace and Facebook accounts was material and relevant to claim that she could no longer participate in certain activities as a result of injuries sustained in an accident”)
- Duty to Preserve Evidence
  - Model Rules
  - Federal Rules of Evidence

COZEN O’CONNOR

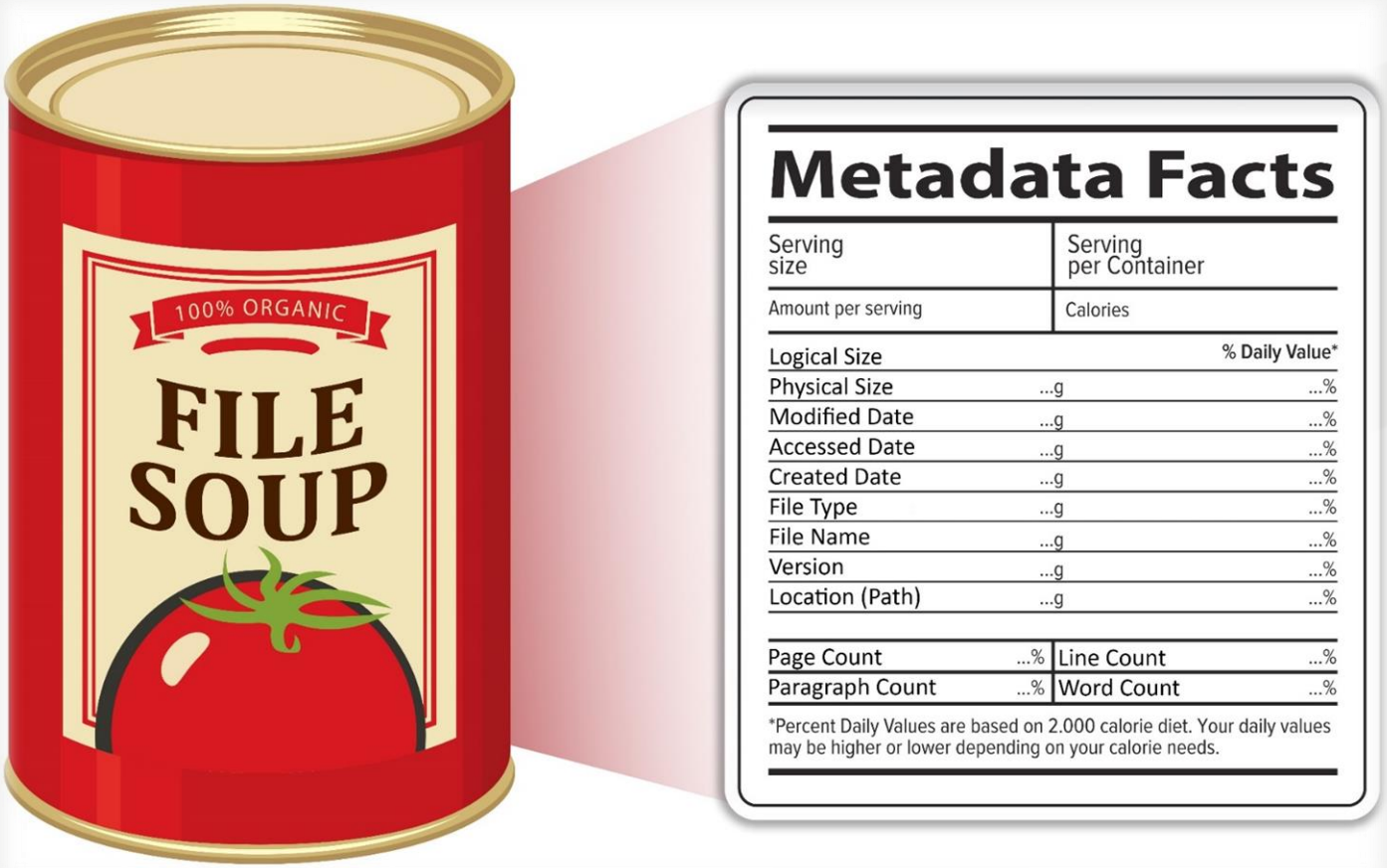
Metadata

- Data About Data
- Metadata can show digital content embedded in files, including:
  - How or by what means the data was created or originated;
  - Creator or author of the content;
  - Location of the data on a computer or network; and
  - Standards used in creation.
- Metadata can be created in photographs, audio recordings, video recordings, and telecommunications.
- There is an increase in GPS metadata duty to GPS enabled cameras, phones, and automobiles, and other equipment.
- Even if metadata has been deleted, it is never truly gone—forensic experts can find the metadata to be investigated.

COZEN O'CONNOR

Metadata

- Data About Data



COZEN O'CONNOR

Metadata

- Using Metadata in Practice About Data
- Attorney for insurer should confront the insured under oath and on the record about matters relating to the claim and insurance.
- In a medical malpractice lawsuit, a Pennsylvania judge required a hospital to turn over metadata so that the plaintiff could reconcile the discrepancies between her medical records and the defendant's testimony.
- In Washington, a man used photographs as proof of ownership of items that were stolen, and were the subject of insurance claims. However, metadata from the photographs revealed that they were taken a month after he submitted his insurance claim.
- An owner of a flatbed truck submitted an insurance claim for four stolen tires and a stolen battery. The policy was purchased four days before the alleged loss. Investigators found a witness who had taken pictures of the truck with a cell phone camera three hours before the insurance policy was purchased, and determined that the tires and battery were missing at that time.

COZEN O'CONNOR

Metadata

- Metadata Tells the Story:

Analyzing Philosophy Paper 1 – Folk Psychology.doc

Document Name: Analyzing Philosophy Paper 1 – Folk Psychology.doc
Path: E:\Johnson\New Folder
Document Format: Word Document

Built-in Document Properties:
Built-in Properties Containing Metadata: 3
Author: UNC
Company: UNC

Document Statistics:
Document Statistics Containing Metadata: 6
Creation Date: 11/16/2014 7:49PM
Last Save Time: 11/18/2014 9:27AM
Last Print Time: 11/18/2014 9:30AM
Last Saved By: UNC
Revision Number: 32
Total Edit Time: 831 Minutes

COZEN O'CONNOR

Metadata

- Metadata Tells The Story

11. A review of the keyword searches of the "CHLC – SanDisk 8GB" USB Drive resulted in identifying a Microsoft Word document residing in four different folders named "Ramaraj Physician Employment Agreement.docx". Each of these documents have the same Md5 hash value and are identical. The Microsoft Word Document "Ramaraj Physician Employment Agreement.docx" metadata indicates the document was created on April 8, 2014 at 11:14 AM, and last saved April 15, 2015 at 8:36 PM. Four

CONCLUSIONS

19. The Microsoft Word versions identified on "CHLC" systems and email, pertaining to the "CHLC-Ramaraj" 2014 contract each had associated metadata consistent with a document generated in April of 2014.

COZEN O'CONNOR

Metadata

- Claim That Voicemail Date Was Altered

> 8. My analysis of HTC One cell phone further revealed that based upon the file naming convention of the two voicemails the voicemail was received on April 30th, 2014 at approximately 6:13 PM. The date and time of the voicemail(s) on the HTC One cell phone was determined through analysis of the time stamp, stored in a Unix millisecond value, included in the file naming convention of the voicemail(s), and through analysis of the timestamps in relation to the user created screenshots of the voicemail. *See* **Exhibit B & C**.

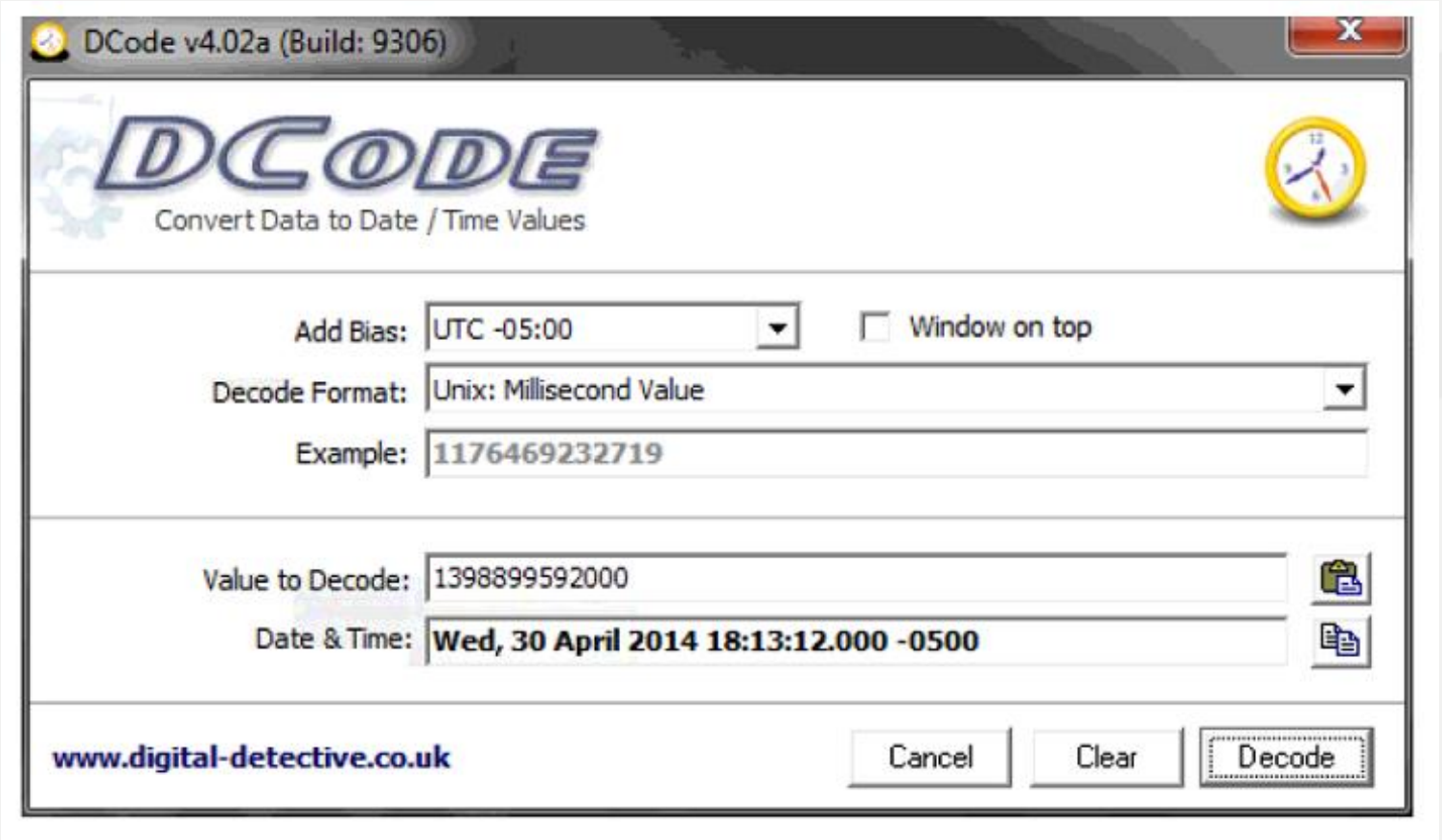
An .amr file is a voice mail file, and on this cellphone the filename was stored as the "callers number" followed by an underscore and then the "date/time". The date in the filename is stored in a Unix type value where the value is represented by the number of milliseconds which have elapsed since January 1st, 1970 (UTC). Time values stored in a Unix numeric type format can be easily converted to show the actual date/time value using many different types of converters.

When the value of 1398899592000 is converted using the tool "DCode", by Digital Detective, the resulting value converts to April 30th, 2014 6:13:12 PM (UTC -5) and can also be seen below:

COZEN O'CONNOR

Authenticating Voicemail

- Claim That Voicemail Date was Altered by Employee



COZEN O'CONNOR

Metadata

- Duty of Sender
- ABA Opinion: Sender does not have any duty to its clients when transmitting metadata; recipient may review or "mine" the metadata; recipient must notify the sender if metadata is found, "if the lawyer knows or reasonably should know that transmission was inadvertent."
- New York Opinion: sender has a duty to act with reasonable care when transmitting metadata; recipient of metadata may not review or "mine" metadata; recipient must promptly notify the sender if metadata is found.
- Pennsylvania Opinion: sender has a duty to act with reasonable care when transmitting metadata to keep client confidences; no definitive stance as to whether a recipient can mine metadata when it is received, but it is looked at on a case by case basis. A receiving lawyer:
  - "must determine whether he or she may use the data received as a matter of substantive law;"
  - "must consider the potential effect on the client's matter should and the lawyer do so; and,"
  - "should advise and consult with the client about the appropriate course of action under the circumstances."
  - Recipient of inadvertent disclosed metadata must promptly notify the sender if it is found.

COZEN O'CONNOR

Metadata

- Ethics and Legal Opinions
- Maryland Opinion: sender has a duty of reasonable care when sending information with metadata; recipient may mine for metadata; no requirement for the recipient of inadvertently disclosed metadata information to inform the sending attorney.
- Texas Opinion: sender has a duty of reasonable care to protect confidential client information in metadata; receiving lawyers may search and mine for metadata; no requirement for the recipient to notify anyone concerning metadata obtained from a document received.
- Duty of Recipient
- Confidentiality
  - ABA Formal Opinion 477
  - FRE 502

COZEN O'CONNOR

Cellphone Investigation

Some Basic Questions

- Where does the text message reside?
- Are messages ever actually deleted?
- What information can be extracted from a cellphone?
- What can cell tower analysis tell us?

COZEN O'CONNOR

Types of Acquisitions

Logical

- Only gets still existing data
- It can recover “deleted” data
  - Deleted data in logical space
    - Database driven applications

COZEN O'CONNOR

Beyond Text Messages

Analysis

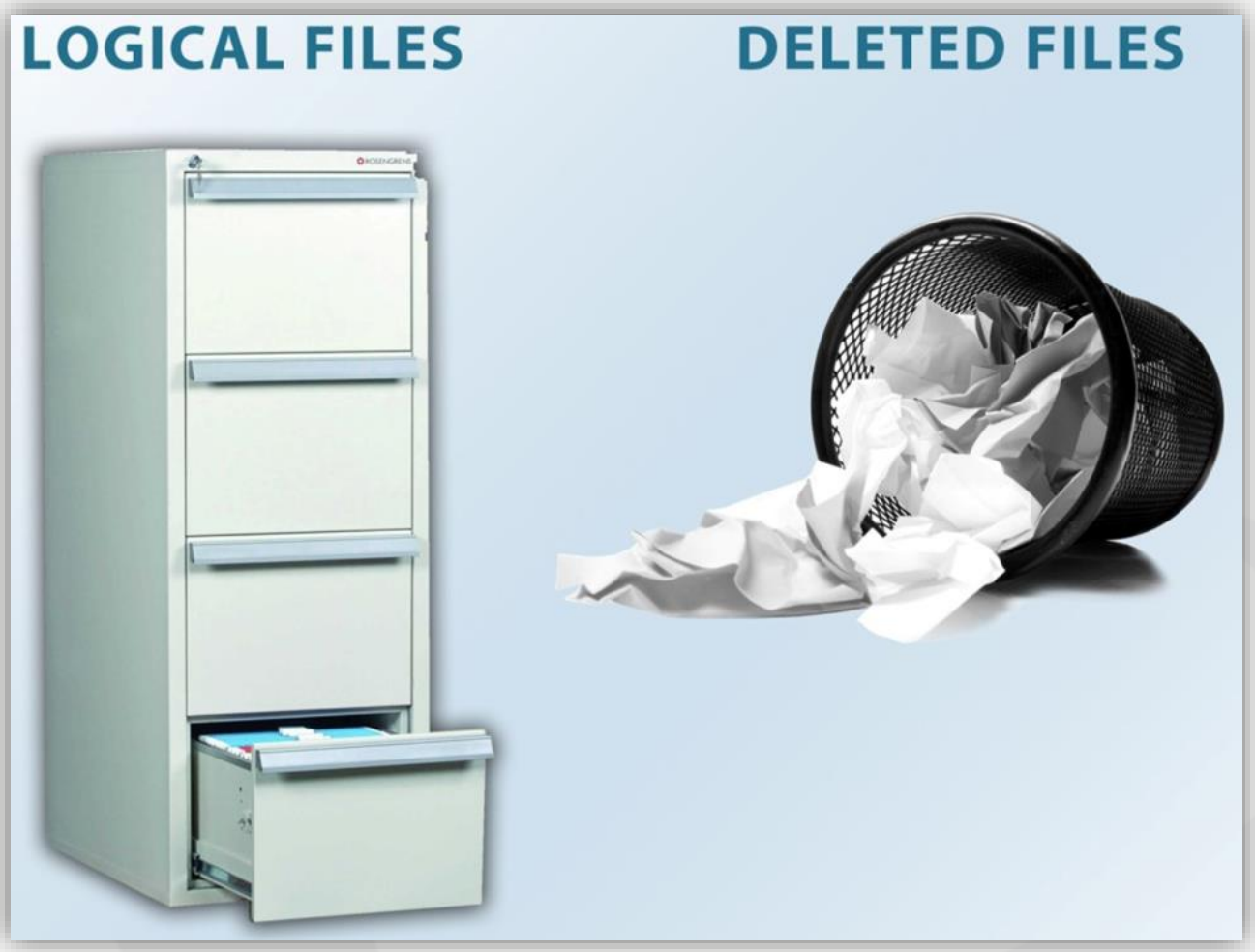
- Messages reside everywhere

COZEN O'CONNOR

Types of Acquisitions

File System

- Logical data
- “Deleted files”
- More raw materials

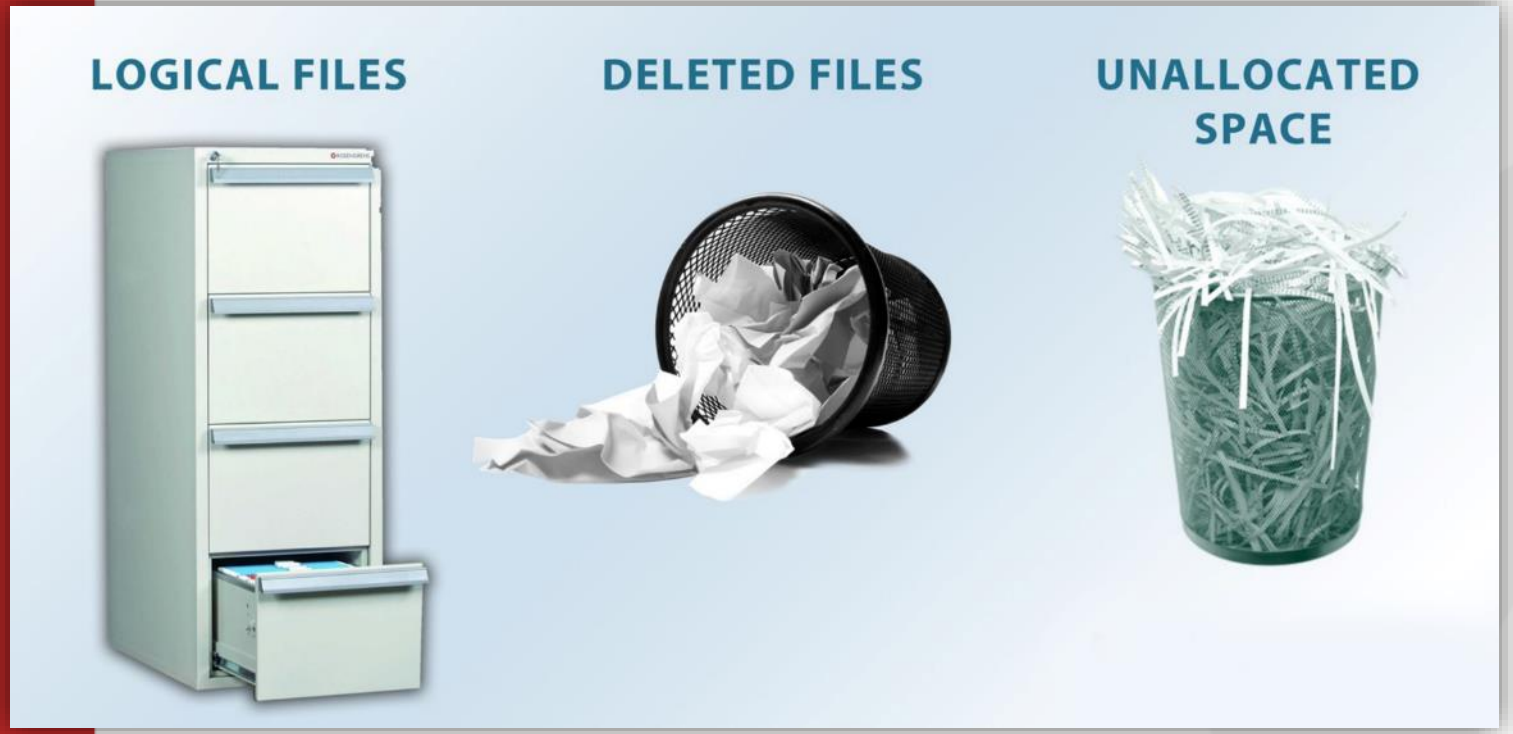


COZEN O'CONNOR

Types of Acquisitions

Physical

- Gets it all



Types of Acquisition

- Chip Off/Jtag

COZEN O'CONNOR

Capabilities: Examples

Location

- Wireless networks

	Timestamp	Description	Category	Name
	4/1/2016 9:30:32 AM(UTC-4)	GooglePlay	Wireless Networks	Bill Wi the Science Fi (e4:f4:c6:0b:5f:51)
	3/31/2016 12:26:16 PM(UTC-4)	GooglePlay	Wireless Networks	Bill Wi the Science Fi (e4:f4:c6:0b:5f:51)
	3/31/2016 12:06:15 PM(UTC-4)	GooglePlay	Wireless Networks	Bill Wi the Science Fi (e4:f4:c6:0b:5f:51)
	3/31/2016 12:00:30 PM(UTC-4)	GooglePlay	Wireless Networks	Bill Wi the Science Fi (e4:f4:c6:0b:5f:51)
	3/30/2016 10:38:17 AM(UTC-4)	GooglePlay	Wireless Networks	Bill Wi the Science Fi (e4:f4:c6:0b:5f:51)
	3/30/2016 8:13:03 AM(UTC-4)	YouTube	Wireless Networks	Bill Wi the Science Fi (e4:f4:c6:0b:5f:51)
	3/30/2016 8:08:37 AM(UTC-4)	YouTube	Wireless Networks	Bill Wi the Science Fi (e4:f4:c6:0b:5f:51)
	3/30/2016 8:04:30 AM(UTC-4)	YouTube	Wireless Networks	Bill Wi the Science Fi (e4:f4:c6:0b:5f:51)
	3/30/2016 8:00:35 AM(UTC-4)	YouTube	Wireless Networks	Bill Wi the Science Fi (e4:f4:c6:0b:5f:51)
	3/30/2016 7:56:44 AM(UTC-4)	YouTube	Wireless Networks	Bill Wi the Science Fi (e4:f4:c6:0b:5f:51)
	3/30/2016 7:53:09 AM(UTC-4)	YouTube	Wireless Networks	Bill Wi the Science Fi (e4:f4:c6:0b:5f:51)
	3/30/2016 7:49:32 AM(UTC-4)	YouTube	Wireless Networks	Bill Wi the Science Fi (e4:f4:c6:0b:5f:51)
	3/30/2016 7:45:45 AM(UTC-4)	YouTube	Wireless Networks	Bill Wi the Science Fi (e4:f4:c6:0b:5f:51)
	3/30/2016 7:21:48 AM(UTC-4)	GooglePlay	Wireless Networks	FiOS-TA0VP (48:5d:36:55:34:38)
	3/30/2016 7:20:43 AM(UTC-4)	GooglePlay	Wireless Networks	FiOS-TA0VP (48:5d:36:55:34:38)
	3/30/2016 7:18:22 AM(UTC-4)	GooglePlay	Wireless Networks	FiOS-TA0VP (48:5d:36:55:34:38)
	3/29/2016 11:39:26 PM(UTC-4)	YouTube	Wireless Networks	FiOS-TA0VP (48:5d:36:55:34:38)

Wireless Network

Go to

BSSID: e4:f4:c6:0b:5f:51
SSId: Bill Wi the Science Fi
Security Mode:
Last Connected:
Last Auto Connected:
Timestamp: 4/1/2016 9:30:32 AM(UTC-4)
End Time:
Package: GooglePlay
Extraction: File System
Source file:

Map

Position:
Map Address:

COZEN O'CONNOR

Capabilities: Examples

- Searches

Timestamp	Value	Source
3/5/2016 11:59:50 PM(UTC-5)	fake text prank	Play Store
3/5/2016 11:30:52 PM(UTC-5)	pranks on your phone	Play Store
3/5/2016 8:45:09 PM(UTC-5)	voice changer	Play Store
3/3/2016 6:26:29 PM(UTC-5)	google	Play Store
2/27/2016 9:44:41 PM(UTC-5)	the idiot test	Play Store
2/27/2016 9:44:25 PM(UTC-5)	the red button	Play Store
2/27/2016 9:40:57 PM(UTC-5)	guess my mi d	Play Store
2/27/2016 9:29:28 PM(UTC-5)	games to play on a roa...	Play Store
2/26/2016 9:44:45 AM(UTC-5)	google	Play Store
2/24/2016 9:34:33 PM(UTC-5)	tsum tsum	Play Store
2/24/2016 7:36:36 PM(UTC-5)	papas games	Play Store

Timestamp	Value	Source
11/5/2013 12:10:22 PM(UTC-5)	prisoner of love bob and tom	YouTube Application
12/18/2013 7:45:13 AM(UTC-5)	god's gonna cut you down	YouTube Application
12/3/2013 12:43:48 PM(UTC-5)	will ferrell pearl the landlord original video	YouTube Application
12/3/2013 2:25:49 PM(UTC-5)	will ferrell the landlord	YouTube Application
12/12/2013 7:32:48 AM(UTC-5)	movie 43 kate winslet hugh jackman scene	YouTube Application
12/18/2013 11:43:53 AM(UTC-5)	christmas jammies	YouTube Application

Timestamp	Value	Source
3/5/2014 1:38:04 PM(UTC-5)	amazon	Chrome
3/5/2014 11:50:23 AM(UTC-5)	hotwire	Chrome
3/5/2014 7:50:54 AM(UTC-5)	r b rebuildables [redacted] wv	Chrome
3/5/2014 7:37:07 AM(UTC-5)	rental cars [redacted] wv	Chrome
3/5/2014 7:31:52 AM(UTC-5)	united bank [redacted]	Chrome
3/5/2014 7:25:32 AM(UTC-5)	rental cars [redacted] wv	Chrome

COZEN O'CONNOR

Capabilities: Examples

Internet History

Last Visited	Title	URL
9/6/2013 12:22:18 PM(UTC-4)	sheetz - Google Search	http://www.google.com/search?q=sheetz
12/19/2013 7:47:41 AM(UTC-5)	saw puppet - Google Search	http://www.google.com/search?q=saw+puppet
12/19/2013 10:43:16 AM(UTC...	saw puppet - Google Search	http://www.google.com/search?q=saw+puppet
12/18/2013 12:48:21 PM(UTC...	saw puppet - Google Search	http://www.google.com/search?q=saw+puppet
10/2/2013 11:37:35 AM(UTC-4)	rpda maxim 500 repair - Google Search	http://www.google.com/search?q=rpda+maxim
9/19/2013 4:05:31 PM(UTC-4)	rpda maxim 500z repair - Google Search	http://www.google.com/search?q=rpda%20max
9/19/2013 4:01:57 PM(UTC-4)	rpda maxim 500z - Google Search	http://www.google.com/search?q=rpda%20max
12/19/2013 10:43:52 AM(UTC...	olive garden - Google Search	http://www.google.com/search?q=olive+garde
12/23/2006 1:29:34 AM(UTC-5)	[redacted] corporate office [redacted] - Google Search	http://www.google.com/search?q=glenmark%2
9/5/2013 12:51:34 PM(UTC-4)	[redacted]zelton [redacted] address - Google Search	http://www.google.com/search?q=fci%20Hazel
10/3/2013 8:50:31 AM(UTC-4)	Ames 3000ss - Google Search	http://www.google.com/search?q=Ames%2030
3/5/2014 8:52:07 AM(UTC-5)	bridgeport [redacted] - Google Search	http://www.google.com/search?ei=w_X0UqnWH
2/6/2014 1:07:09 PM(UTC-5)	jibber jabber doll - Google Search	http://www.google.com/search?ei=nZuwUvKVH
12/17/2013 1:45:30 PM(UTC-5)	jibber jabber - Google Search	http://www.google.com/search?ei=nZuwUvKVH
3/11/2014 8:32:53 AM(UTC-4)	chemical formula for poop - Google Search	http://www.google.com/search?ei=nfX0UrqJNq

COZEN O'CONNOR

Capabilities: Examples

User Accounts

User Account Go to

Name:
Username: [redacted]@yahoo.com
Password: pa[redacted]a1
Creation time: 9/26/2015 11:11:19 AM (UTC-4)
Service Type: https://m.facebook.com/
Server Address:
Extraction: File System
Source file:

Phone numbers and Emails

Organizations

Address

Notes

Creation time	Username	Password	Service Type
1/19/2016 6:45:52 PM(UTC-5)	[redacted]@yahoo.com	Ta[redacted]6996	https://secure.sho.com/
2/7/2016 4:03:41 PM(UTC-5)	[redacted]vbschools.com	ta[redacted]6996	https://member.virginpulse.com/
9/5/2015 4:36:30 PM(UTC-4)	[redacted]edia@hotmail.com	ta[redacted]6996	https://login.live.com/
12/9/2015 5:45:24 PM(UTC-5)	[redacted]	Sq[redacted]dles101	https://studentvue.vbcps.com/
12/9/2015 5:41:47 PM(UTC-5)	[redacted]	Sq[redacted]dles101	https://schools.vbcps.com/
9/26/2015 11:11:19 AM(UTC-4)	[redacted]@yahoo.com	pa[redacted]emma1	https://m.facebook.com/
	[redacted]@gmail.com	oa[redacted]2rt_1/qVyua...	com.google
10/27/2015 9:29:18 PM(UTC-4)	[redacted]edia@hotmail.com	me[redacted]s	https://www.netflix.com/
	[redacted]edia@hotmail.com	me[redacted]s	android://Jzj5T2E45Hb33D-Ik-EHZVCrb...
2/21/2015 8:04:28 AM(UTC-5)	[redacted]	me[redacted]s	https://mikandi.com/
9/30/2015 5:45:01 PM(UTC-4)	[redacted]@gmail.com	jar[redacted]use1	https://accounts.google.com/
3/30/2016 10:14:15 PM(UTC-4)	[redacted]mparis@gmail.com	Ba[redacted]00	https://accounts.google.com/
10/31/2015 2:06:31 AM(UTC-4)	[redacted]@vbschools.com	Ap[redacted]08	https://login.microsoftonline.com/
3/3/2015 4:14:21 PM(UTC-5)	[redacted]vbschools.com	Ap[redacted]04	https://login.microsoftonline.com/
3/3/2015 5:15:26 PM(UTC-5)		al[redacted]n101	https://order.dominos.com/
2/5/2016 10:58:02 AM(UTC-5)	[redacted]edia@hotmail.com	al[redacted]n	https://sellercentral.amazon.com/
7/17/2015 5:44:32 PM(UTC-4)	[redacted]edia@hotmail.com	al[redacted]n	https://www.amazon.com/

COZEN O'CONNOR

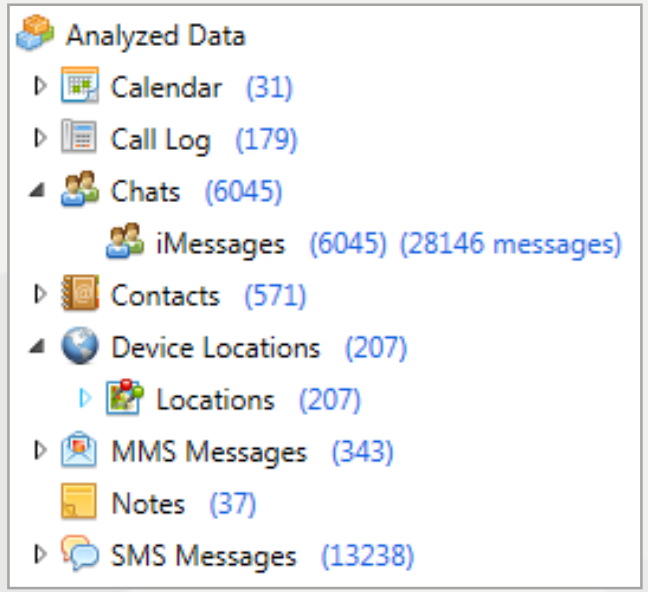
Capabilities: Examples

Messaging

- SMS, MMS, APP Based

Timestamp	Parties	Body	Folder
3/24/2016 8:46:50 AM(UTC-4)	**From:** +17 37 Dad	All good :)	Inbox
3/24/2016 1:34:09 PM(UTC-4)	**To:** 75 5 T y	In health where talking about the uranry systme	Sent
3/24/2016 1:34:45 PM(UTC-4)	**From:** +17 35 T y	Pee pee	Inbox
3/24/2016 1:37:02 PM(UTC-4)	**To:** 75 35 T y	Yup	Sent
3/24/2016 1:37:14 PM(UTC-4)	**To:** 75 35 T y	Where talking about it ughfhg	Sent
3/24/2016 1:44:21 PM(UTC-4)	**From:** +17 35 T y	Aw you don't want to know what I was doing LOL	Inbox

Timestamp	Parties	Body	Folder	Status
3/24/2016 8:38:18 AM(UTC-4)	**From:** +17 35 T y	Bye bye sweetie	Inbox	Read
3/24/2016 8:45:41 AM(UTC-4)	**To:** 75 5 T y	The bus is late	Sent	Sent
3/24/2016 8:45:54 AM(UTC-4)	**To:** 7 4 L y	Lizzy	Sent	Sent
3/24/2016 8:46:02 AM(UTC-4)	**From:** +1 35 T y	Guess so itll be here soon no worries	Inbox	Unread



COZEN O'CONNOR

Capabilities: Examples

Media

- Pictures, videos, audio, voicemail

#	Image	Name	Path	Size (by	Metadata	Created
1271		PART_1352341057650	/data/com.android.providers.telephony/...	447056	**Camera Make** LG Electronics +1 **Camera Model** VM670 **Capture Time** 11/5/2012 7:33:39 PM **Lat/Lon** (35.316667, -78.616667)	11/7/2012 10:17:36 PM
1262		PART_1344817466147	/data/com.android.providers.telephony/...	448362	**Camera Make** SAMSUNG **Camera Model** SPH-M820 **Pixel resolution** 1200x1600 **Resolution** 72x72 (Unit: Inch)	8/12/2012 8:24:26 PM
1282		PART_1353539431966	/data/com.android.providers.telephony/...	455803	**Camera Make** LG Electronics +1 **Camera Model** VM670 **Capture Time** 11/21/2012 3:18:49 PM **Lat/Lon** (35.300000, -78.600000)	11/21/2012 7:10:30 PM
1284		PART_1353541315070	/data/com.android.providers.telephony/...	460505	**Camera Make** LG Electronics +1 **Camera Model** VM670 **Capture Time** 11/21/2012 3:14:55 PM **Lat/Lon** (35.300000, -78.600000)	11/21/2012 7:41:54 PM
1273		PART_1352420119928	/data/com.android.providers.telephony/...	475552	**Camera Make** LG Electronics +1 **Camera Model** VM670 **Capture Time** 11/6/2012 9:30:32 AM **Lat/Lon** (35.300000, -78.600000)	11/8/2012 8:15:18 PM
1274		PART_1352581754733	/data/com.android.providers.telephony/...	484244	**Camera Make** LG Electronics +1 **Camera Model** VM670 **Capture Time** 11/10/2012 3:13:51 PM **Lat/Lon** (35.316667, -78.616667)	11/10/2012 5:09:14 PM

COZEN O'CONNOR

Capabilities: Example

User Dictionary

- User created
  - Attribution
    - Names
    - Email Accounts
    - Addresses
  - Unique spelling
    - Acronyms
    - Slang
    - Nicknames

Word	Locale
whake	
whake	en
wednsay	en_US
untill	
untill	en
undertale	en_US
toriel	en_US
Jasmyn	en_US
infinty	en_US

COZEN O'CONNOR

Cellular Location and Tracking

Cell Towers

Call Detail Records (CDRS)

What are they?

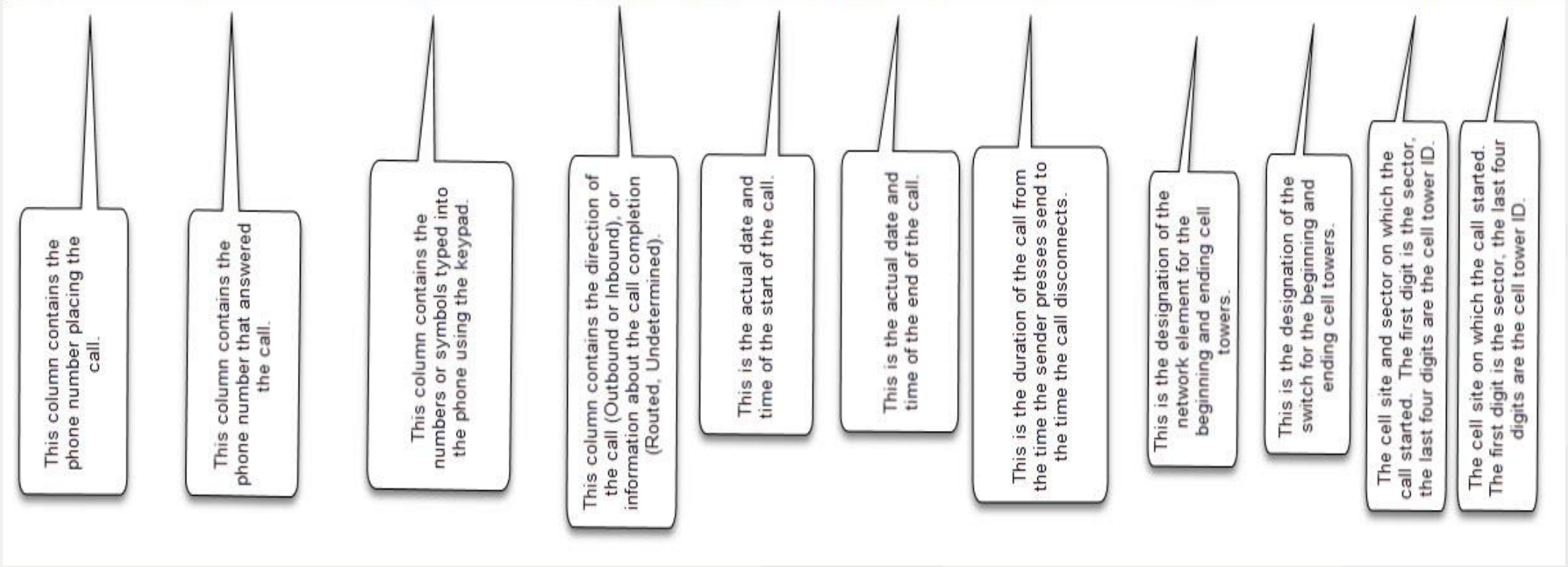
- Legal proof of a service provided
- A technical road map of a call
- A financial transaction record

COZEN O'CONNOR

Call Detail Records (Sprint)

CDR Example

CALLING_NBR	CALLED_NBR	DIALED_DIGITS	M_R_#	START_DATE	END_DATE	DURATION (SEC)	NEID	REPOLL_#	1ST CELL	LAST CELL
(773)	(773)	(773)	Outbound	1/22/12 22:05:03	1/22/12 22:10:19	316	96	71	10561	20561

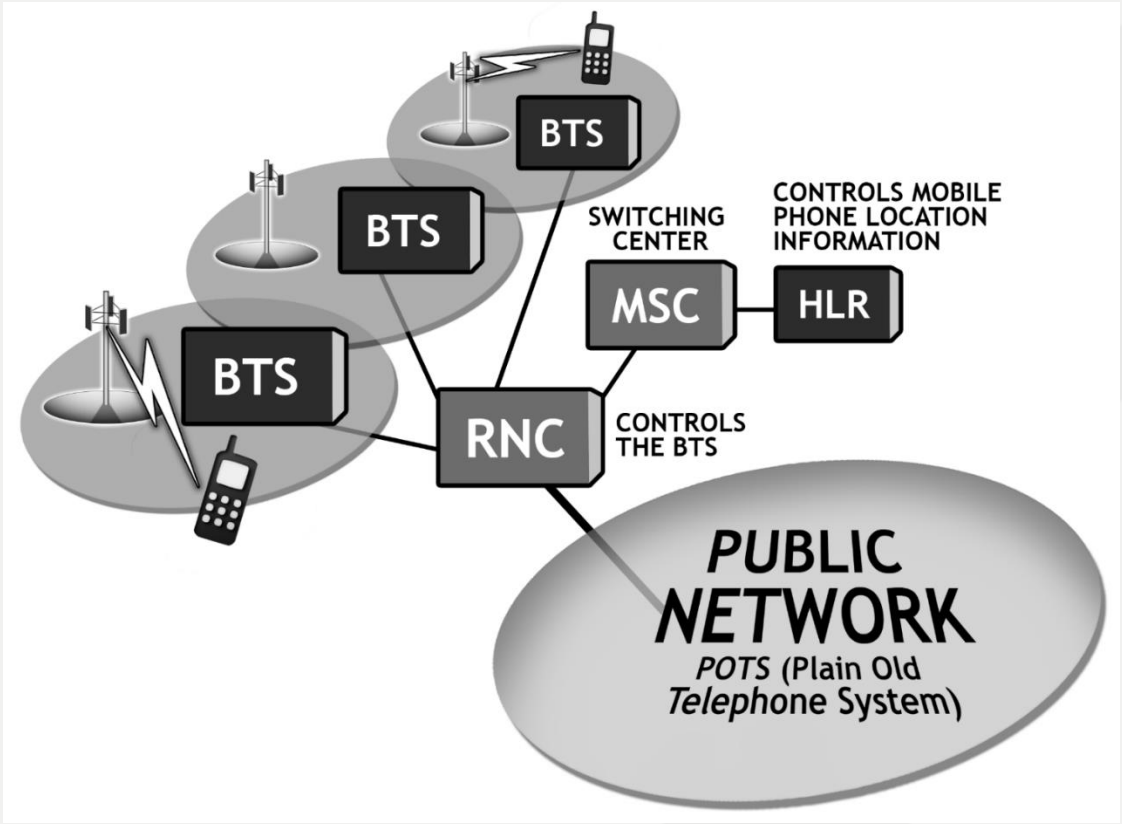


COZEN O'CONNOR

Cellular System in a Nutshell

Cell Phones Talk to Towers

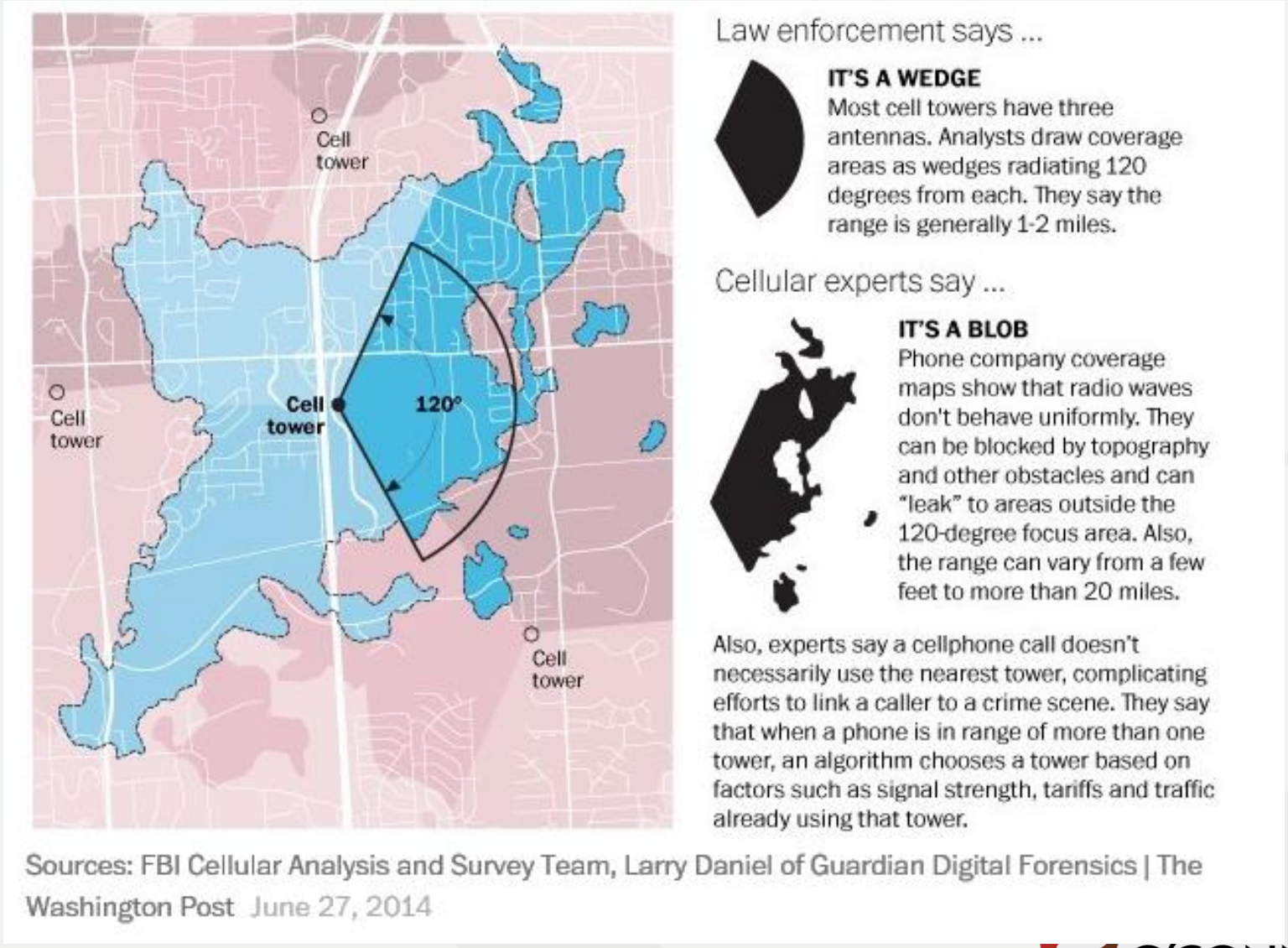
- Everything else talks to pots



COZEN O'CONNOR

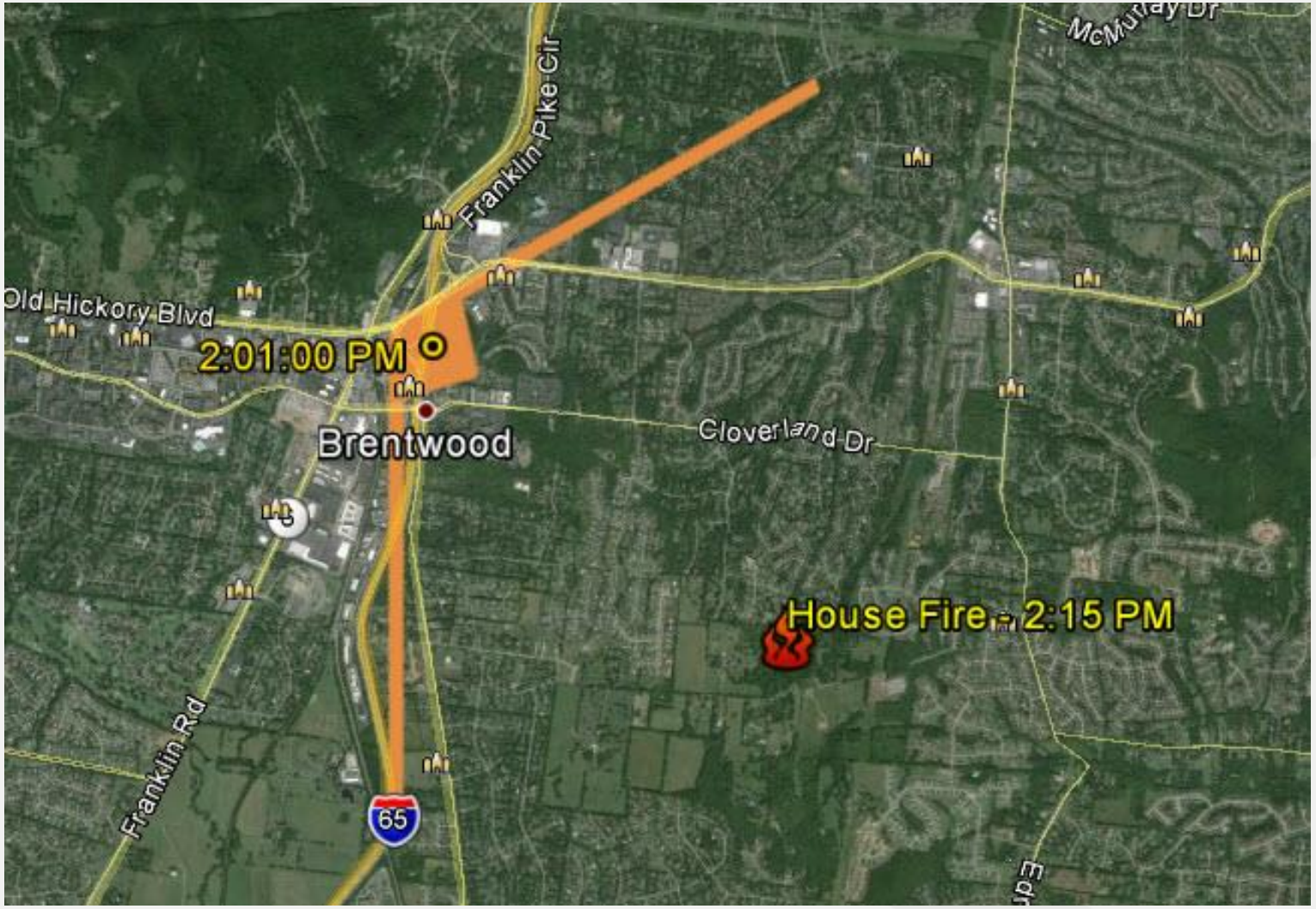
Radio Frequency Map

General Area



Case Example

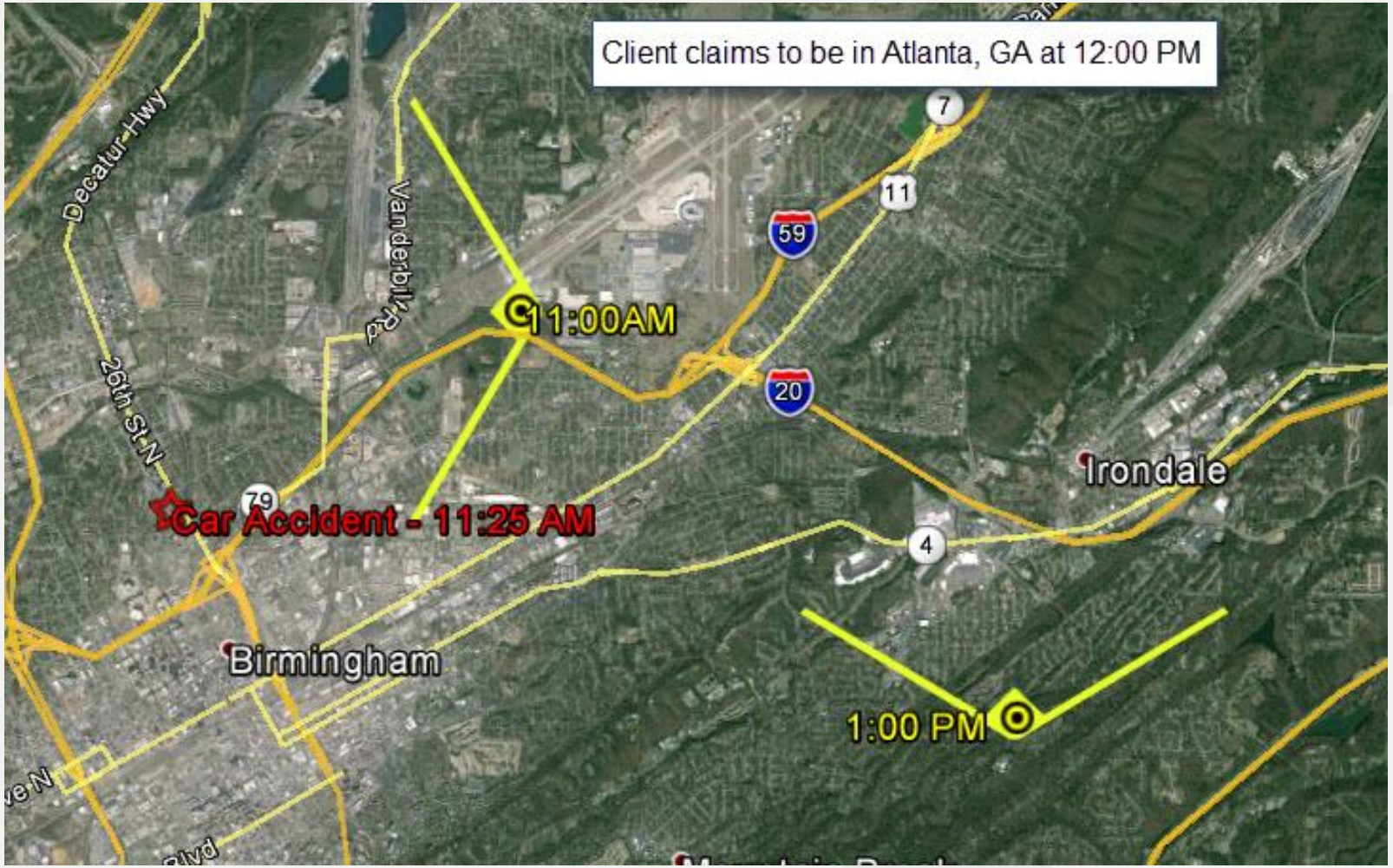
House Fire



COZEN O'CONNOR

Case Example

Car Accident



Cellular Analysis

Vehicle at the accident?

Conclusion:

The location of the subject cell phone at 2:59 PM is approximately 22 air miles away from the location of the accident. There is at least one cell site closer to the accident scene than the tower that carried the phone call at 2:59 OM. Cell phones will not jump over a close tower to connect to a cell tower far way.

Given the density of cell towers in Queens, NY, there is no possibility that the cell phone could have been near the accident location at 3:00 PM

COZEN O'CONNOR

Cellphone Investigations

Case Examples Using Cellebrite Technology

- Recovery of deleted text messages in homicide cases
- Use has been upheld in court decisions
- Even phones that have been soaking in water or shattered can be recovered

COZEN O'CONNOR

Case Study – Trucking Accident

The Evidence

- Cell phone (distraction)
- Claim that trucker was using phone at time of accident by opposing expert.

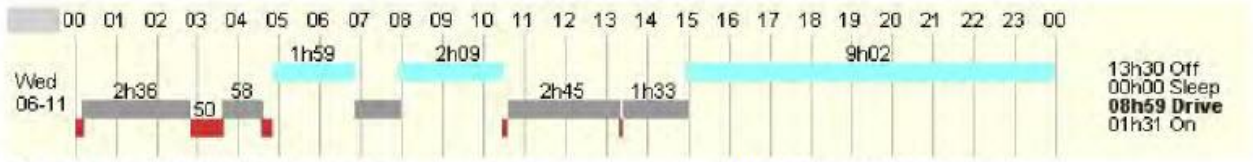
COZEN O'CONNOR

Capabilities: Examples

Drivers Log

6/11/2014 Start of Day: Midnight Eastern

Document(s):	Off Duty: 13h30
Trailer(s):	Sleeper Berth:
Tractor(s): 140927	Driving: 8h59
Co-Driver(s):	On Duty Not Driving: 1h31
Edits: 0	Total Hours On Duty Today: 10h30
Sensor Failures: 0	Total Hours On Duty for Week: 56h13
34 Hour Reset:	Distance Driven (mi): 433



Start Time	Duration	Activity	Location	Flags*	Remarks
00:00	0h12	On-Duty	3 mi ENE of Macclenny, FL	C	
00:12	2h36	Driving	3 mi ENE of Macclenny, FL	C	
02:48	0h50	On-Duty	9 mi NE of Sanford, FL	C	
03:38	0h58	Driving	9 mi NE of Sanford, FL	C	
04:36	0h16	On-Duty	3 mi ESE of Ocoee, FL	C	
04:52	1h59	Off-Duty	3 mi ESE of Ocoee, FL	C	
06:51	1h07	Driving	3 mi ESE of Ocoee, FL	C	
07:58	0h10	Off-Duty	11 mi SE of Winter Haven, FL	C	
08:08	0h10	Off-Duty	11 mi SE of Winter Haven, FL	C	
08:18	2h09	Off-Duty	12 mi SE of Winter Haven, FL	C	

COZEN O'CONNOR

Capabilities: Examples

Phone Records

Phone Records Details For [redacted] (Cont. 14)

Date	Time	From	To	Duration	Call Location / Activity | Detail |		Phone Near
1:00 PM							
6/9/2014	1:00 PM Voice Call (-)	Girl Friend	902		[redacted]	(ENE) (N)	88
6/9/2014	1:00 PM Voice Call (Incoming)	Girl Friend	[redacted]	6 mins 3 secs	[redacted]	(N) (N)	Home 128
6/9/2014	1:08 PM Voice Call (-)	Girl Friend	390		[redacted]	(N) (WSW)	94
6/9/2014	1:08 PM Voice Call (Incoming)	Girl Friend	[redacted]	9 mins 11 secs	[redacted]	(N) (N)	Home 129
6/9/2014	1:20 PM Voice Call (Outgoing)	[redacted]	[redacted]	1 mins 22 secs	[redacted]	(N) (N)	Home 128
6/9/2014	1:26 PM Voice Call (Outgoing)	[redacted]	Electric Company	14 mins 2 secs	[redacted]	(N) (N)	Home 129
6/9/2014	1:49 PM Text Message (Incoming)	[redacted]	[redacted]				
6/9/2014	1:50 PM Text Message (Outgoing)	[redacted]	[redacted]				
6/9/2014	1:51 PM Voice Call (-)	[redacted]	346		[redacted]	(N) (N)	152
6/9/2014	1:51 PM Voice Call (Incoming)	[redacted]	[redacted]	9 mins 24 secs	[redacted]	(N) (NNW)	110
6/9/2014	1:58 PM Text Message (Incoming)	Girl Friend	[redacted]				

COZEN O'CONNOR

Capabilities: Examples

Drivers Log Vs. Phone Records

Driver's Log v. Phone Records

Main Menu

Log Entries for "Driving" Shown with Associated Phone Records
Sun, Jun 8, 2014 to Sun, Jun 22, 2014 (15 Days)
76 Driver Log Entries | 335 Phone Records

Driver's Log
Phone Record

Date	Activity	Start Time	Duration	Phone	
Sun, Jun 8, 2014	Driving	12:13 AM-12:21 AM	0 hrs 8 mins		0 Records | 0 Text | Voice - 0 mins
Sun, Jun 8, 2014	Driving	1:04 AM-1:14 AM	0 hrs 10 mins		0 Records | 0 Text | Voice - 0 mins
Sun, Jun 8, 2014	Driving	1:14 AM-1:58 AM	0 hrs 44 mins		0 Records | 0 Text | Voice - 0 mins
Sun, Jun 8, 2014	Driving	4:10 AM-4:25 AM	0 hrs 15 mins		0 Records | 0 Text | Voice - 0 mins
Sun, Jun 8, 2014	Driving	4:25 AM-5:04 AM	0 hrs 39 mins		0 Records | 0 Text | Voice - 0 mins
Sun, Jun 8, 2014	Driving	5:43 AM-6:37 AM	0 hrs 54 mins		0 Records | 0 Text | Voice - 0 mins
Sun, Jun 8, 2014	Driving	10:18 PM-11:18 PM	1 hr 0 mins		5 Records | 3 Text | Voice 0 hrs 54 min (90%)
Text Message (Incoming)		10:44:08 PM	Girl Friend (Nichole)	To	
Text Message (Incoming)		10:44:45 PM	Girl Friend (Nichole)	To	
Text Message (Outgoing)		10:49:49 PM	[redacted]	To	Girl Friend (Nichole)
Voice Call (Outgoing)		10:18:20 PM	[redacted]	To	[redacted] 52 mins 35 secs
Voice Call (Incoming)		11:17:11 PM	Girl Friend (Nichole)	To	[redacted] 21 mins 31 secs
Sun, Jun 8, 2014	Driving	11:49 PM-12:00 AM	0 hrs 11 mins		0 Records | 0 Text | Voice - 0 mins

COZEN O'CONNOR

Capabilities: Examples

- Sleep Analysis

Phone Sleep Analysis For [redacted]

Main Menu | Charts

Sun, Jun 8, 2014 to Sun, Jun 22, 2014 (15 Days)

15 Days **Average Gap For Period 3.07 Hours**

Date	Largest Gap	Largest Time Gaps	
		Gap Time (this day)	Time Period Inactive
Sunday, June 8, 2014	2 hrs 23 min	2 hrs 23 min	1:22:19 PM - 3:53:27 PM
		1 hr 30 min	5:34:17 AM - 7:05:53 AM
		1 hr 16 min	8:56:22 AM - 10:13:11 AM
Monday, June 9, 2014	2 hrs 24 min	2 hrs 24 min	6:58:07 PM - 9:22:07 PM
		1 hr 59 min	9:13:29 AM - 11:13:35 AM
		1 hr 35 min	9:22:07 PM - 10:57:49 PM
Tuesday, June 10, 2014	5 hrs 9 min	5 hrs 9 min	1:11:58 AM - 6:26:58 AM
		1 hr 34 min	11:33:08 PM - 1:07:38 AM
		1 hr 28 min	5:11:20 PM - 6:39:31 PM
Wednesday, June 11, 2014	1 hr 54 min	1 hr 54 min	4:50:10 AM - 6:46:17 AM
		1 hr 54 min	7:03:04 AM - 8:57:31 AM
		1 hr 46 min	11:30:24 AM - 1:16:40 PM
Thursday, June 12, 2014	2 hrs 59 min	2 hrs 59 min	10:13:39 PM - 1:13:31 AM
		1 hr 58 min	9:55:20 AM - 11:53:58 AM
		1 hr 14 min	3:48:55 PM - 5:03:46 PM

COZEN O'CONNOR

Capabilities: Examples

Gap Analysis

- Opposing expert counted incoming data as user activity

Off Duty Time - 6-8-2014 from 6:37 AM to 9:48 PM							
Start Date	Start Time	End Time	Duration	Direction	Start Date/Time	End Date/Time	GAP
6/8/2014	7:05:53 AM	7:05:53 AM		Text: Outgoing	6/8/14 7:05 AM	6/8/14 7:05 AM	1:30:23
6/8/2014	8:13:41 AM	8:14:23 AM	0 Mins 42 Secs	Voice: Incoming	6/8/14 8:13 AM	6/8/14 8:14 AM	1:07:48
6/8/2014	8:43:34 AM	8:44:04 AM	0 Mins 30 Secs	Voice: Incoming	6/8/14 8:43 AM	6/8/14 8:44 AM	0:29:11
6/8/2014	8:53:33 AM	8:55:28 AM	1 Mins 55 Secs	Voice: Outgoing	6/8/14 8:53 AM	6/8/14 8:55 AM	0:09:29
6/8/2014	8:56:10 AM	8:56:18 AM	0 Mins 8 Secs	Voice: Outgoing	6/8/14 8:56 AM	6/8/14 8:56 AM	0:00:42
6/8/2014	8:56:22 AM	8:56:31 AM	0 Mins 9 Secs	Voice: Outgoing	6/8/14 8:56 AM	6/8/14 8:56 AM	0:00:04
6/8/2014	10:13:11 AM	10:13:11 AM		Text: Outgoing	6/8/14 10:13 AM	6/8/14 10:13 AM	1:16:40
6/8/2014	10:35:14 AM	10:35:14 AM		Text: Outgoing	6/8/14 10:35 AM	6/8/14 10:35 AM	0:22:03
6/8/2014	10:36:39 AM	10:36:39 AM		Text: Outgoing	6/8/14 10:36 AM	6/8/14 10:36 AM	0:01:25
6/8/2014	10:37:24 AM	10:37:24 AM		Text: Outgoing	6/8/14 10:37 AM	6/8/14 10:37 AM	0:00:45
6/8/2014	10:38:32 AM	10:47:45 AM	9 Mins 13 Secs	Voice: Incoming	6/8/14 10:38 AM	6/8/14 10:47 AM	0:01:08
6/8/2014	12:12:07 PM	12:28:53 PM	16 Mins 46 Secs	Voice: Incoming	6/8/14 12:12 PM	6/8/14 12:28 PM	1:24:22

COZEN O'CONNOR

Contact Information

Barrett Kiernan

Cozen O'Connor

bkiernan@cozen.com

Matt Scott

Envista Forensics

matt.scott@envistaforensics.com

ENVISTA FORENSICS

COZEN O'CONNOR