CELL PHONE FORENSICS

LARS DANIEL, ENCE, CCO, CTNS, CTA, CWA, CIPTS, CCPA

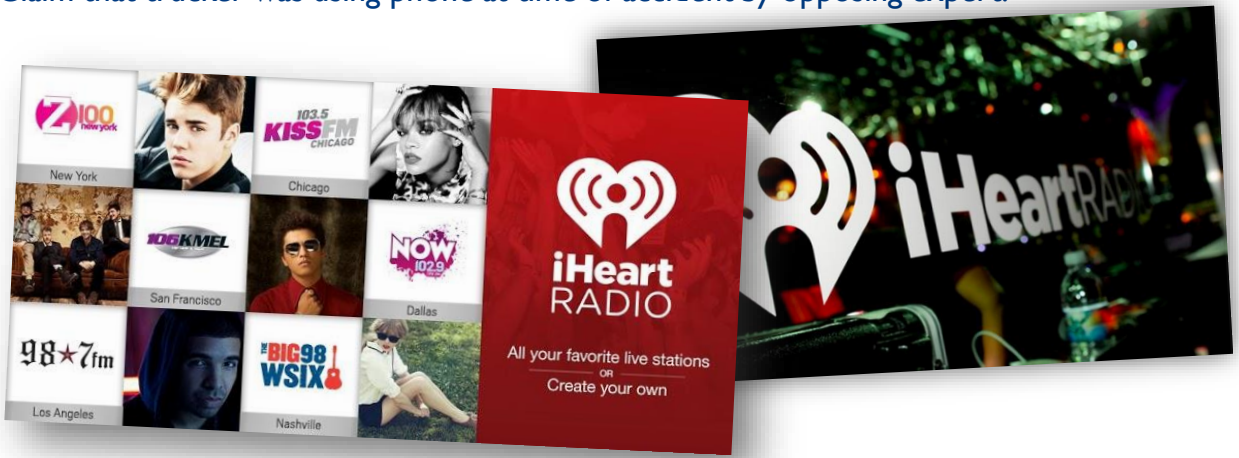
© 2017 Envista Forensics

Case Study – Trucking Accident

- The evidence
  - Call Detail Records
  - Driver Logs
  - Cell phone
- Plaintiff's claim
  - Driver fatigue caused accident
  - Driver distracted at time of accident

Case Study – Trucking Accident

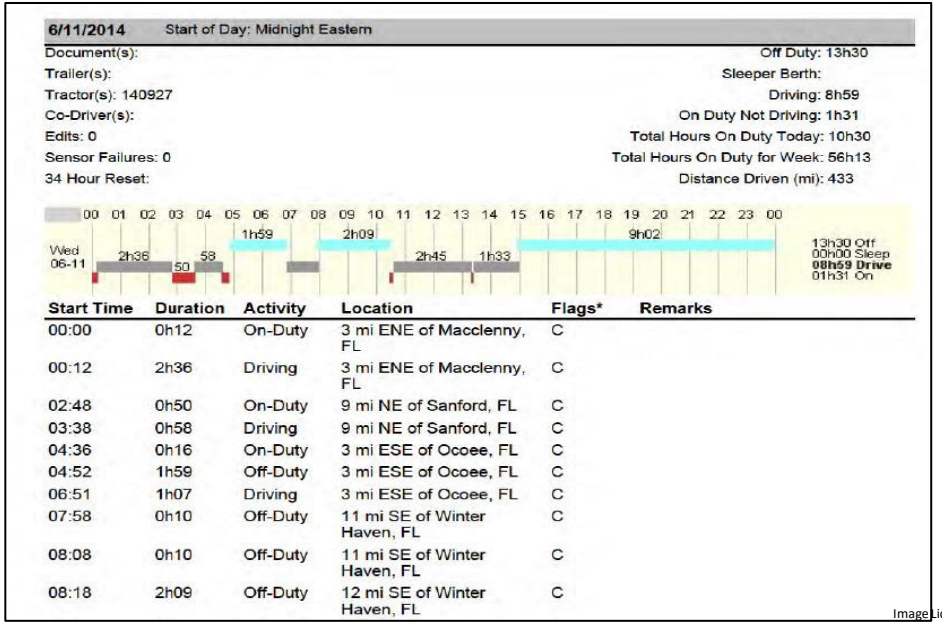
- The evidence
  - Cell Phone (Distraction)
    - Claim that trucker was using phone at time of accident by opposing expert.



Images purchased and used with permission from istockphoto.com

Capabilities: Examples

- Drivers log



6/11/2014 Start of Day: Midnight Eastern

Document(s):
Trailer(s):
Tractor(s): 140927
Co-Driver(s):
Edits: 0
Sensor Failures: 0
34 Hour Reset:

Off Duty: 13h30
Sleeper Berth:
Driving: 8h59
On Duty Not Driving: 1h31
Total Hours On Duty Today: 10h30
Total Hours On Duty for Week: 56h13
Distance Driven (mi): 433

00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 00

Wed 06-11 — 2h36 | 50 | 58 | 1h59 | 2h09 | 2h45 | 1h33 | 9h02

13h30 Off
00h00 Sleep
08h59 Drive
01h31 On

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	

Image Licensed; (c) Lars Daniel

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]				

Image Licensed; (c) Lars Daniel

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		To	Girl Friend (Nichole)
Voice Call (Outgoing)		10:18:20 PM		To	52 mins 35 secs
Voice Call (Incoming)		11:17:11 PM	Girl Friend (Nichole)	To	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

Image Licensed; (c) Lars Daniel

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

Image Licensed; (c) Lars Daniel

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

Image Licensed; (c) Lars Daniel

Cell Phones

- Unique Butterflies Everywhere



© 2017 Envista Forensics

Collection and Acquisition

- Unique Preservation Issues
  - Phone must be isolated from network
    - Faraday Bag

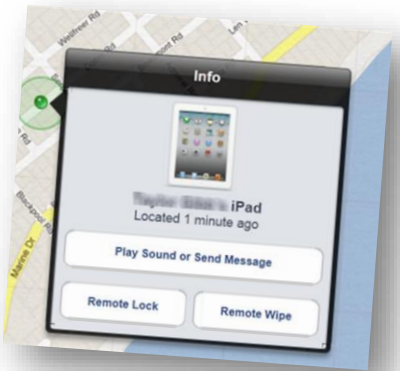


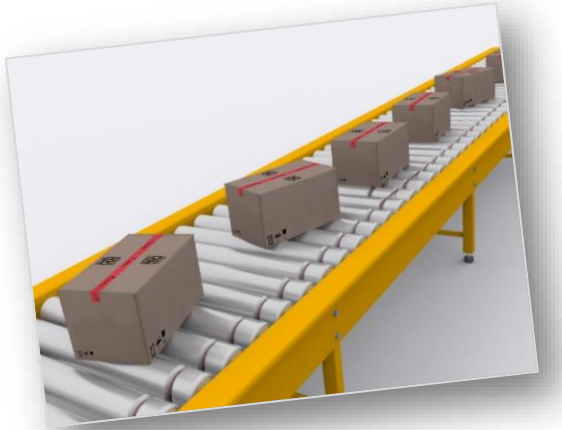


© 2017 Envista Forensics

Collection and Acquisition

- Unique Preservation Issues
  - Simply turning the phone on can destroy data permanently if not isolated from networks





© 2017 Envista Forensics

Collection and Acquisition

- What should happen
  - Phone collected and turned off
    - No concern about passcode lock, or passcode is known.
  - Phone collected, kept active, and left on.
    - If passcode locked



© 2017 Envista Forensics

Collection and Acquisition

- What happens too often…
  - First responder thumbs through phone at scene, "thumb forensics"
    - No documentation
    - No forensic training
    - No clue



© 2017 Envista Forensics

Collection and Acquisition

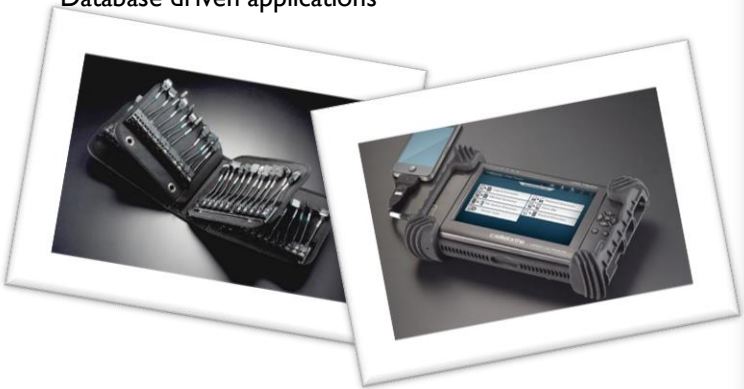
- First responder thumbs through phone at scene
  - not forensically sound
    - Potentially cannot tell if:
      - Something created
      - Something deleted
      - Something manipulated



© 2017 Envista Forensics

Types of Acquisitions

- Logical
  - Only gets still existing data
  - It *can* recover "deleted" data
    - Deleted data in logical space
      - Database driven applications





© 2017 Envista Forensics

Types of Acquisitions

- File System
  - Logical Data
  - "Deleted Files"
  - More raw materials

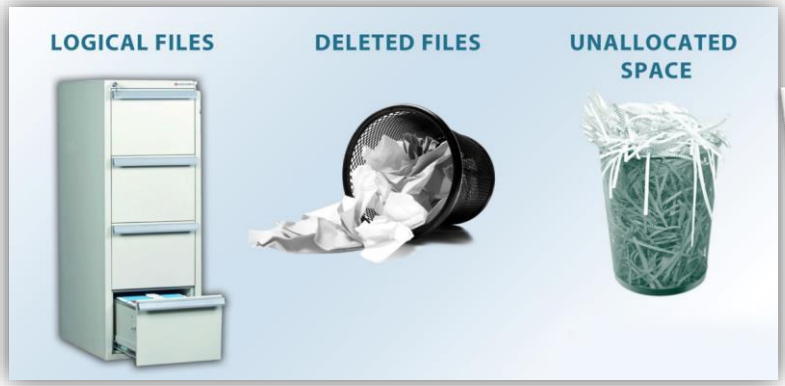


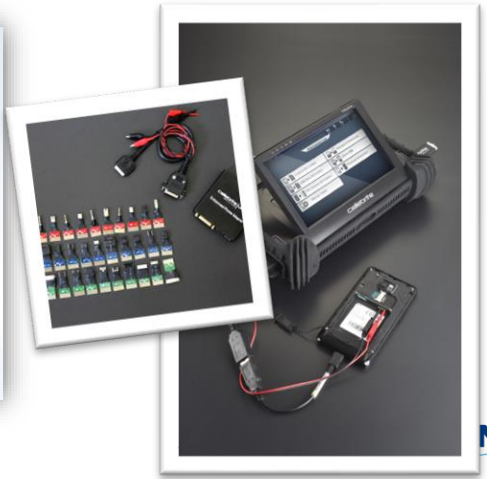


© 2017 Envista Forensics

Types of Acquisitions

- Physical
  - Gets it all





© 2017 Envista Forensics

Types of Acquisition

- Chip Off/JTAG



© 2017 Envista Forensics

Analysis:

- Acquisitions
  - Low level of expertise, comparatively speaking, needed to use tools
- Analysis
  - Requires real skills

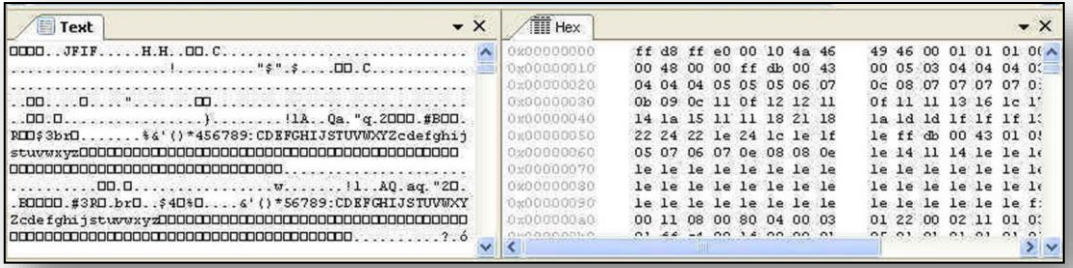




© 2017 Envista Forensics

Analysis:

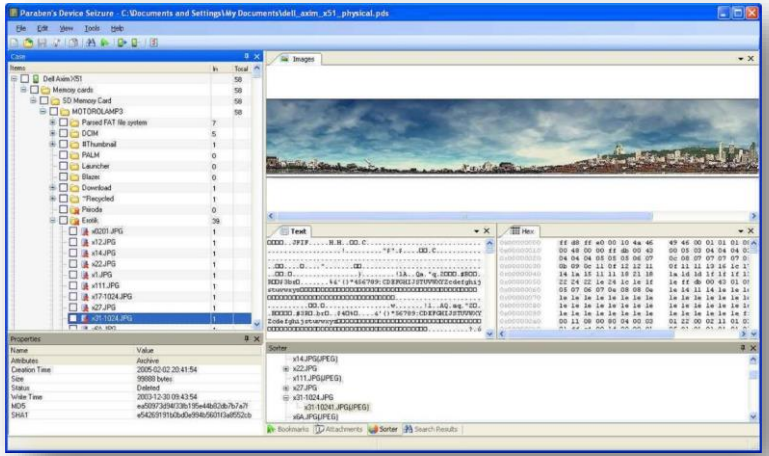
- Analysis
  - Requires real skills



© 2017 Envista Forensics

Analysis:

- Analysis
  - Requires real skills



© 2017 Envista Forensics

Analysis:

- Analysis
  - Requires real skills

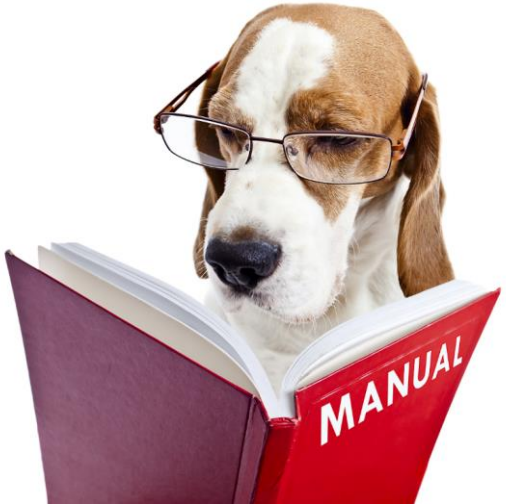




© 2017 Envista Forensics

Manual Examination

- Last Resort
  - If no other option is available
  - Must follow best forensic practices



© 2017 Envista Forensics

Manual Examination

- Last Resort
  - If no other option is available
  - Must follow best forensic practices





© 2017 Envista Forensics

Manual Examination

- How it should be done
  - Camera takes pictures of screen
    - Examiner manipulates touchscreen or keypad, going through the different types of data and photographs each screen.
  - Video camera records entire examination
    - From the time the phone is taken out of evidence and powered on, through the entire examination, until being powered off and returned to evidence storage.
  - Without full documentation (video) you have:
    - ***NO verification***
      - Modified? Deleted? Changed?
        - **INTENTIONAL? UNINTENTIONAL?**



© 2017 Envista Forensics

Capabilities: Examples

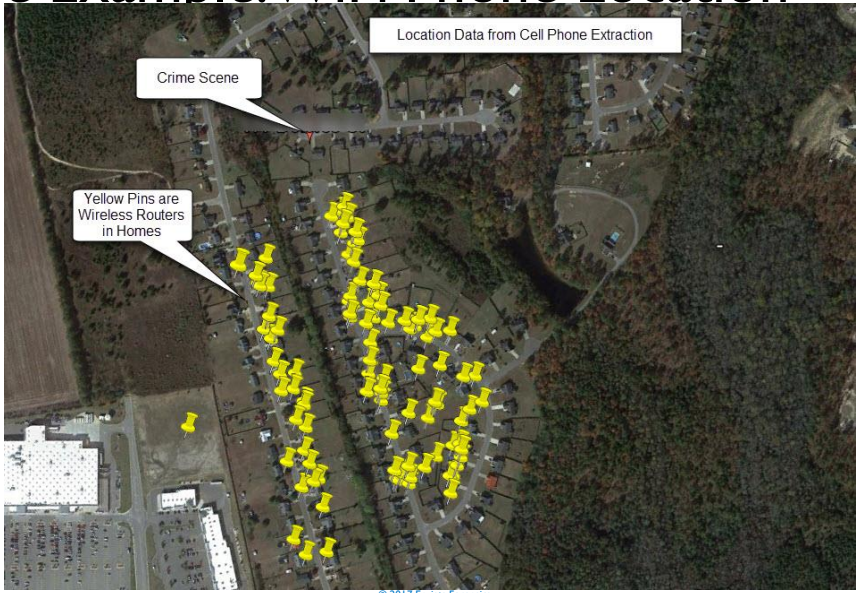
- Location
  - Wireless Networks

	↓ 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)



© 2017 ENVISTA Forensics

Case Example: WiFi Phone Location



© 2017 Envista Forensics

Capabilities: Examples

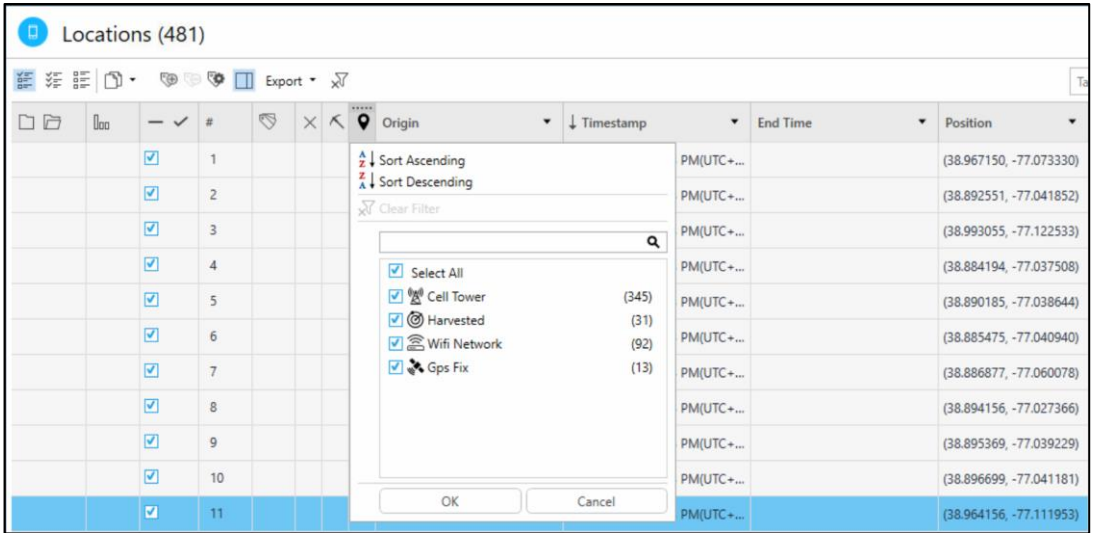
- Location
  - Google Maps

Category	Timestamp	Position	Name
Google Maps	1/11/2014 12:41:30 AM(UTC-5)	(39.658502, -79.585629)	Co Rte 5/21/Old Co 26/12
Google Maps	9/24/2010 10:16:30 PM(UTC-4)	(36.839771, -76.212776)	Federal Bureau-Investigation
Google Maps	1/7/2014 11:51:12 AM(UTC-5)	(39.312693, -79.963859)	Knottsville Cemetery
Google Maps	1/20/2014 4:56:20 PM(UTC-5)	(39.587111, -79.966314)	[redacted] Morgantown, WV 26508
Google Maps	12/31/2013 10:51:03 PM(UTC-5)	(39.657908, -79.585410)	[redacted] Bruceton Mills, WV 26525

© 2017 Envista Forensics

Location Data

- Location data from multiple sources, from the cell phone.



© 2017 ENVISTA Forensics

Location Data

Location Data extracted by Cellebrite

11/1/2015 11:53:49 AM	YouTube	41.58	-81.20
11/1/2015 11:55:15 AM	YouTube	41.58	-81.20
11/1/2015 12:01:01 PM	Maps	41.58	-81.20
11/2/2015 8:35:47 AM	Play Store	41.58	-81.20
11/2/2015 8:37:35 AM	Play Store	41.58	-81.20
11/2/2015 8:38:07 AM	Play Store	41.58	-81.20
11/2/2015 8:38:42 AM	Play Store	41.58	-81.20
11/2/2015 8:39:17 AM	Play Store	41.58	-81.20
11/2/2015 8:44:07 AM	Play Store	41.58	-81.20

© 2017 Envista Forensics

Capabilities: Examples

- User Accounts
  - Generate leads



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

© 2017 Envista Forensics

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

© 2017 Envista Forensics

Case Study: Distracted Driving

- Searching at time of impact



Images purchased and used with permission from istockphoto.com

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%20ma
9/19/2013 4:01:57 PM(UTC-4)	rpda maxim 500z - Google Search	http://www.google.com/search?q=rpda%20ma
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)	corporate office - Google Search	http://www.google.com/search?q=glenmark%2
9/5/2013 12:51:34 PM(UTC-4)	zelton 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 - Google Search	http://www.google.com/search?ei=w_X0UqnW
2/6/2014 1:07:09 PM(UTC-5)	jibber jabber doll - Google Search	http://www.google.com/search?ei=nZuwUvKV
12/17/2013 1:45:30 PM(UTC-5)	jibber jabber - Google Search	http://www.google.com/search?ei=nZuwUvKV
3/11/2014 8:32:53 AM(UTC-4)	chemical formula for poop - Google Search	http://www.google.com/search?ei=nfX0UrqJNq

ENVISTA FORENSICS

Case Study: Distracted Driving

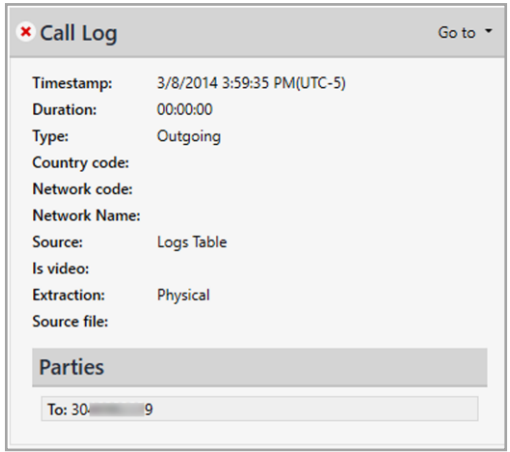
- Detailed timeline analysis at point of impact



Images purchased and used with permission from istockphoto.com

Capabilities: Examples

- Call Logs



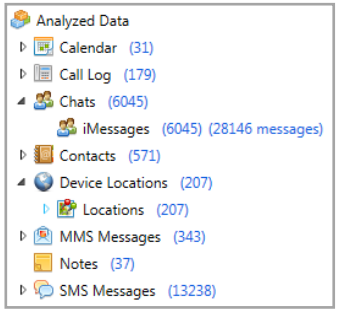
Parties	Timestamp	Duration	Type
To:	3/6/2014 8:58:41 PM(UTC-5)	01:15:58	Outgoing
To: Matt	3/6/2014 8:20:54 PM(UTC-5)	00:00:10	Outgoing
To: Linda	3/6/2014 6:44:21 PM(UTC-5)	00:01:27	Outgoing
From: Matt	3/6/2014 5:42:24 PM(UTC-5)	00:15:49	Incoming
From: Matt	3/6/2014 5:26:58 PM(UTC-5)	00:06:27	Incoming
To: Matt	3/6/2014 5:18:51 PM(UTC-5)	00:02:07	Outgoing
To:	3/6/2014 5:16:49 PM(UTC-5)	00:01:53	Outgoing
Unknown	3/6/2014 3:54:40 PM(UTC-5)	00:01:27	Incoming
From:	3/6/2014 3:45:35 PM(UTC-5)	00:10:47	Incoming
From: Linda	3/6/2014 3:32:22 PM(UTC-5)	00:11:31	Incoming
To:	3/6/2014 9:44:10 AM(UTC-5)	00:06:04	Outgoing
To:	3/6/2014 8:48:52 AM(UTC-5)	00:55:04	Outgoing
To: Matt	3/5/2014 6:06:04 PM(UTC-5)	00:00:00	Outgoing

© 2017 Envista Forensics

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



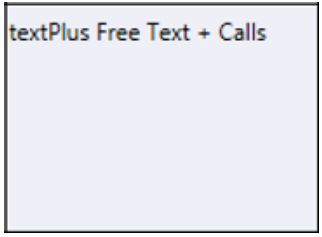
		Timestamp	Parties	Body	Folder	Status
✖		3/24/2016 8:38:18 AM(UTC-4)	From: +17 35 T y	Bye bye sweetie	Inbox	Read
✖		3/24/2016 8:45:41 AM(UTC-4)	To: 75 5 T y	The bus is late	Sent	Sent
		3/24/2016 8:45:54 AM(UTC-4)	To: 7 4 L y	Lizzy	Sent	Sent
✖		3/24/2016 8:46:02 AM(UTC-4)	From: +1 35 T y	Guess so itll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

© 2017 Envista Forensics

Capabilities: Examples

- Installed Applications

	#	Name	Purchase Date	Identifier	Permissions
☑	13	Jewels Pro	8/3/2012 7:47:15 AM(UTC+0)	com.play.Jewels3	
☑	14	Pool Master Pro	7/26/2012 11:19:15 PM(UTC+0)	com.forthblue.pool	Network Phone Calls Storage
☑	15	Jewels Miner!	7/26/2012 10:40:42 PM(UTC+0)	com.ezjoynetwork.jewelsminer	
☑	16	Bubble Pop Plus!	7/8/2012 1:43:45 AM(UTC+0)	com.popcasuals.bubblepop2	Network Accounts Phone Calls Storage
☑	17	YouTube	6/18/2012 10:29:01 PM(UTC+0)	com.google.android.youtube	
☑	18	Google Search	6/18/2012 10:27:45 PM(UTC+0)	com.google.android.googlequicksear...	
☑	19	Worldstarhiphop	6/17/2012 10:45:41 PM(UTC+0)	com.pt.wshhp	Network Storage
☑	20	textPlus Free Text + Calls	6/17/2012 10:39:33 PM(UTC+0)	com.gogii.textplus	Accounts Application Info Audio Bluetooth Messages
☑	21	Music Download Paradise...	6/17/2012 10:38:37 PM(UTC+0)	com.androidfreak.entertainment.musi...	Network Application Info Phone Calls Locations Storage



© 2017 Envista Forensics

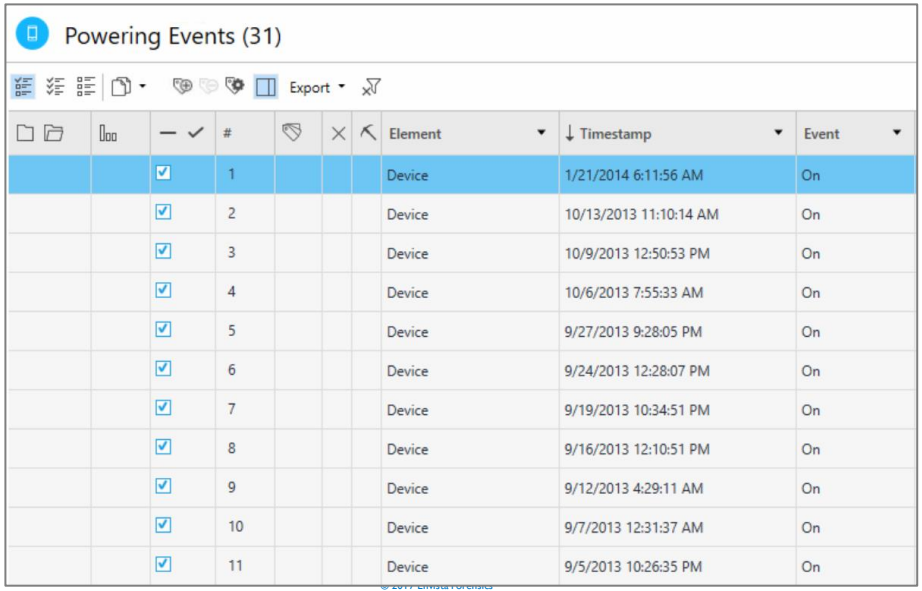
Capabilities: Examples

- Media
  - Pictures, videos, audio, voicemails

#	Image	Name	Path	Size (b)	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

© 2017 Envista Forensics

Powering Events



Powering Events (31)

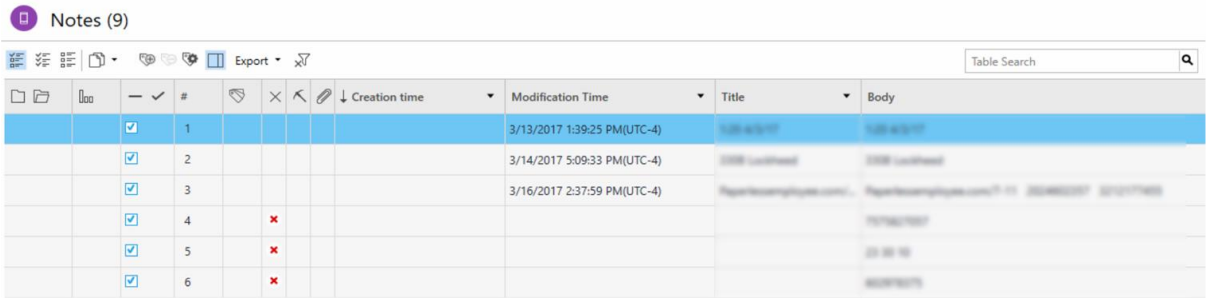
Export

#	Element	Timestamp	Event
1	Device	1/21/2014 6:11:56 AM	On
2	Device	10/13/2013 11:10:14 AM	On
3	Device	10/9/2013 12:50:53 PM	On
4	Device	10/6/2013 7:55:33 AM	On
5	Device	9/27/2013 9:28:05 PM	On
6	Device	9/24/2013 12:28:07 PM	On
7	Device	9/19/2013 10:34:51 PM	On
8	Device	9/16/2013 12:10:51 PM	On
9	Device	9/12/2013 4:29:11 AM	On
10	Device	9/7/2013 12:31:37 AM	On
11	Device	9/5/2013 10:26:35 PM	On

© 2017 ENVISTA Forensics

Notes

- Includes last modification time



© 2017 Envista Forensics

Capabilities: Examples

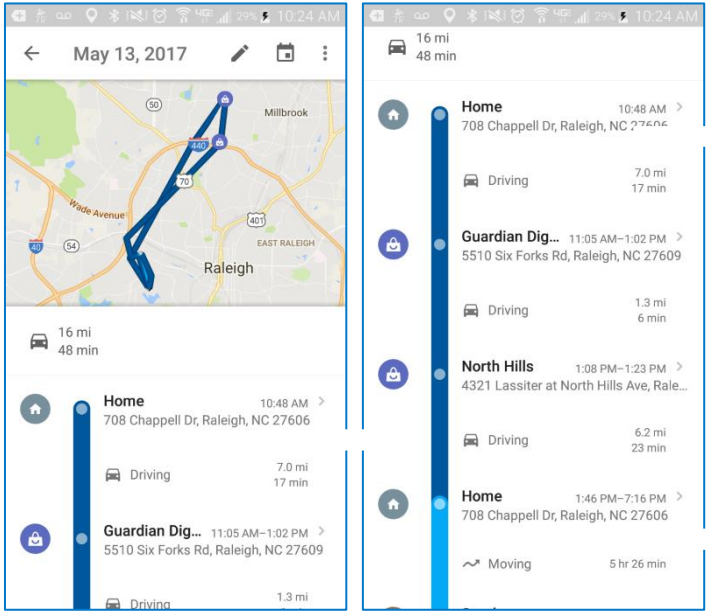
- User Dictionary
  - User created
    - Attribution
      - Names
      - Email accounts
      - addresses
    - Unique spelling
      - Acronyms
      - Slang
      - Nicknames

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

© 2017 Envista Forensics

Capabilities: Examples

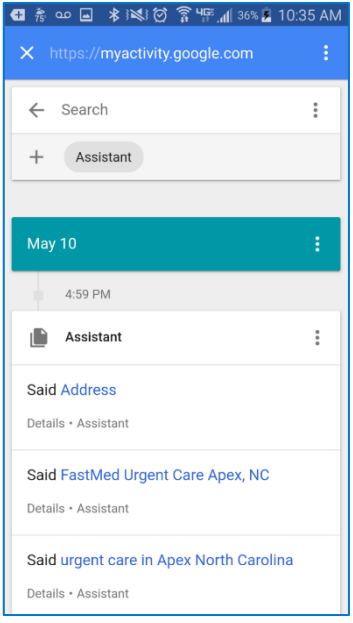
- Google is watching
  - Location activity
  - Full route

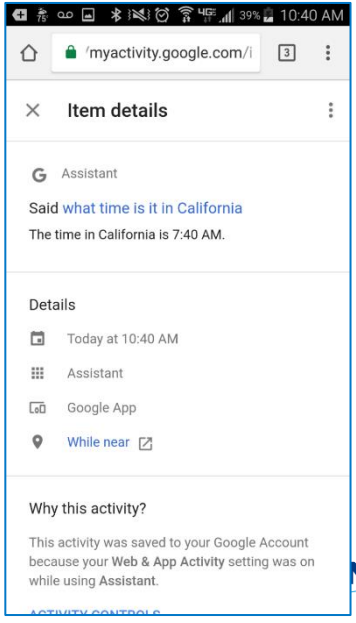


© 2017 Envista Forensics

Capabilities: Examples

- Google is listening
  - Location activity
  - Full route

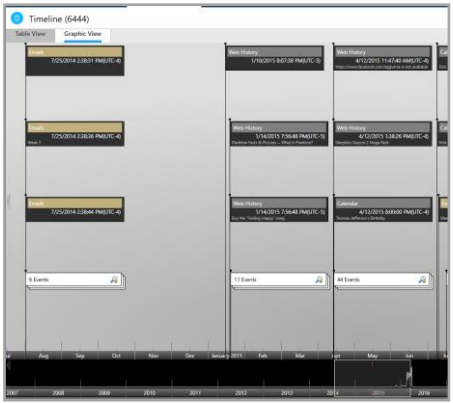




© 2017 Envista Forensics

Capabilities: Examples

- Timelines!
  - All activity
  - Specific activity
  - Advanced analysis



Type	Timestamp	Party	Description
SMS Messages	3/23/2016 6:11:37 PM(UTC-4)	To: 7577	Where you at
SMS Messages	3/23/2016 6:12:21 PM(UTC-4)	From: +	Right side towards the back
SMS Messages	3/23/2016 6:12:38 PM(UTC-4)	To: 7577	In the cafe
SMS Messages	3/23/2016 6:15:10 PM(UTC-4)	To: 7577	Where in the cafertira
SMS Messages	3/23/2016 6:15:16 PM(UTC-4)	To: 7577	Waiting
SMS Messages	3/23/2016 6:15:51 PM(UTC-4)	From: +	Kk be there in a few
Instant Messages	3/23/2016 6:58:08 PM(UTC-4)	From: 1	The Big Five. Hiccup, Rapunzel, M...
Web History	3/23/2016 7:37:56 PM(UTC-4)		Yahoo
Web History	3/23/2016 7:37:58 PM(UTC-4)		Yahoo
Web History	3/23/2016 7:38:05 PM(UTC-4)		Yahoo
Web History	3/23/2016 7:38:22 PM(UTC-4)		Yahoo
Web History	3/23/2016 7:38:24 PM(UTC-4)		Yahoo
Web History	3/23/2016 7:39:31 PM(UTC-4)		Yahoo
Web History	3/23/2016 7:40:48 PM(UTC-4)		Yahoo
Web History	3/23/2016 7:40:52 PM(UTC-4)		Yahoo
Web History	3/23/2016 7:41:32 PM(UTC-4)		Yahoo
SMS Messages	3/23/2016 8:41:16 PM(UTC-4)	To: Dad	Will you talk to mom tonight
SMS Messages	3/23/2016 8:45:27 PM(UTC-4)	To: Dad	So I don't have to get up in the m...

© 2017 Envista Forensics

Examination of Plaintiff's Phone

Time	Category	Item
[redacted] 11:48:44 AM(UTC-6)	DB	Phone (dialer.db)
[redacted] 11:48:44 AM(UTC-6)	Text File	com.android.dialer.xml
[redacted] 11:48:47 AM(UTC-6)	Picture	1841 task thumbnail.DELETED.png
[redacted] 11:48:55 PM(UTC-6)	E-Mail	Received E-Mail from [redacted] (Assistant Services)
[redacted] 11:49:17 AM(UTC-6)	SMS From: [redacted] Mother	Ohhhh, well if it can be gotten for less than$5 a sheet it might be worth it, but i don't think This truck could haul it all at once and 2 trips would probably break even with $12 delivered
[redacted] 11:49:17 AM(UTC-6)	SMS From: [redacted] Mother	Ohhhh, well if it can be gotten for less than$5 a sheet it might be worth it, but i don't think This truck could haul it all at once and 2 trips would probably break even with $12 delivered
[redacted] 11:51:02 AM(UTC-6)	Text File	rti.mqtt.counter.MqttLite.tp.DELETED.xml
[redacted] 11:52:23 PM(UTC-6)	Text File	event data[redacted]
[redacted] 11:55:47 AM(UTC-6)	Text File	BattStatsPrefs.DELETED 1.xml
[redacted] 11:55:48 AM(UTC-6)	Text File	com.google.android.gms.auth.devicesignals.DeviceSignalsStore.DELETED.xml
[redacted] 11:55:48 AM(UTC-6)	Text File	com.google.android.gms.tapandpay.service.TapAndPayServiceStorage.DELETED.xml
[redacted] 11:55:48 AM(UTC-6)	Text File	settings_secure.DELETED.xml
[redacted] 11:56:14 AM(UTC-6)	Picture	1843 task thumbnail.png
[redacted] 11:59:00 AM(UTC-6)	Cookie: E-Mail	mail.google.com
[redacted] 11:59:00 AM(UTC-6)	Cookie: E-Mail	mail.google.com
[redacted] 11:59:00 AM(UTC-6)	Cookie: E-Mail	mail.google.com
[redacted] 11:59:00 AM(UTC-6)	DB	Gmail (Cookies)
[redacted] 11:59:02 PM(UTC-6)	Text File	AnalyticsPlatformPrefsFile.xml
[redacted] 11:59:02 PM(UTC-6)	Text File	AnalyticsPlatformPrefsFile.DELETED.xml
[redacted] 11:59:39 AM(UTC-6)	Text File	Account[redacted].DELETED.xml
[redacted] 11:59:58 AM(UTC-6)	Text File	com.google.android.gms.auth.authzen.cryptauth.DeviceStateSyncManager.xml
[redacted] 12:00:01 AM(UTC-6)	Text File	com.motorola.motodisplay.analytics.MD_BREATHS.DELETED.xml
[redacted] 12:00:01 AM(UTC-6)	Text File	com.motorola.motodisplay.analytics.MD_NOTIF.DELETED.xml
[redacted] 12:00:01 AM(UTC-6)	Text File	com.motorola.motodisplay.analytics.TOUCH.DELETED.xml
[redacted] 12:00:05 AM(UTC-6)	Text File	rti.mqtt.counter.MqttLite.tp.DELETED 1.xml
[redacted] 12:00:05 AM(UTC-6)	Text File	DebugAnalytics.DELETED 1.xml
[redacted] 12:00:20 PM(UTC-6)	Picture	IMG [redacted] 120016201.jpg
[redacted] 12:00:23 PM(UTC-6)	DB	Google Photos (media_store_extras)
[redacted] 12:00:23 PM(UTC-6)	Picture	IMG [redacted] 120021204.jpg
[redacted] 12:00:23 PM(UTC-6)	Text File	com.google.android.apps.photos_preferences.DELETED 4.xml
[redacted] 12:00:24 AM(UTC-6)	Text File	BattStatsPrefs.DELETED 2.xml
[redacted] 12:00:24 PM(UTC-6)	Picture	IMG [redacted] 120022835.jpg
[redacted] 12:00:24 PM(UTC-6)	Text File	com.google.android.apps.photos_preferences.DELETED 3.xml
[redacted] 12:00:25 PM(UTC-6)	DB	Google+ (trash.db)
[redacted] 12:00:25 PM(UTC-6)	Text File	com.google.android.apps.photos_preferences.DELETED 2.xml
[redacted] 12:00:25 PM(UTC-6)	Text File	com.google.android.apps.photos_preferences.DELETED 5.xml
[redacted] 12:00:26 PM(UTC-6)	Text File	com.google.android.apps.photos_preferences.xml
[redacted] 12:00:26 PM(UTC-6)	Text File	com.google.android.apps.photos_preferences.DELETED.xml
[redacted] 12:00:26 PM(UTC-6)	Text File	com.google.android.apps.photos_preferences.DELETED 1.xml
[redacted] 12:00:58 PM(UTC-6)	Text File	MailAppProvider.DELETED 1.xml
[redacted] 12:00:59 AM(UTC-6)	Text File	Pmaps.xml
[redacted] 12:00:59 PM(UTC-6)	Text File	Account[redacted].DELETED 1.xml
[redacted] 12:00:59 PM(UTC-6)	Text File	MailAppProvider.DELETED.xml

Image Licensed; (c) Lars Daniel

CHALLENGING THE EVIDENCE

© 2017 Envista Forensics

Challenging the Evidence

- Challenging Manual Examinations
  - Rarely performed correctly
    - Isolate phone from networks
    - Video verification
    - Complete documentation

© 2017 Envista Forensics

Challenging the Evidence

- Challenging Manual Examinations
  - Affidavit Highlights
    - Taking screenshots or pictures of a cell phone constitutes a forensic manual examination of a cell phone as the actual evidence item (the phone) must be manipulated by a forensic examiner in order to preserve the contents of the phone.
    - The forensic acquisition of a cell phone through the process of a manual examination requires specific skills, training, and experience in order to properly document, acquire, and preserve the evidence on a phone.

© 2017 Envista Forensics

Challenging the Evidence

- Challenging Manual Examinations
  - Affidavit Highlights
    - Isolation from the Cellular Network
      - The forensic acquisition of a cell phone using any kind of forensic examination requires that a cell phone be isolated from the cellular network. If the phone is not isolated from the cellular network, new data is coming onto the phone and potentially destroying evidentiary data in the process of overwriting old data with that newer data.

© 2017 Envista Forensics

Challenging the Evidence

- Challenging Manual Examinations
  - Isolation from the Cellular Network

> Isolating the phone from the radio network is important to keep new traffic, such as SMS messages, from overwriting existing data, if the phone is turned on when found. Besides the risk of overwriting potential evidence, the question may arise whether data received on the phone after seizure is within the scope of the original authority granted. Add-on programs, such as LockMe[12] and OmaiProtect[13], are also available that enable the phone lock to be set remotely upon receipt of a properly formatted message. Moreover, vulnerabilities may exist that can be exploited. For example, a malformed message sent to a Nokia 6210 phone has been shown to disable it completely, much like the a malformed ICMP packet known as the "ping of death" did to older Windows computers [Ley01].

The following quote is from the National Institute for Standards in Technology (NIST) article "Guidelines on Cell Phone Forensics" by Wayne Jansen and Rick Ayers.

© 2017 Envista Forensics

Challenging the Evidence

- Challenging Manual Examinations
  - Isolation from the Cellular Network

Network isolation ensures that the contents of a phone reflect the time at which it was seized, disallowing changes that may occur to it after it has been seized. Actions over the network that can alter content include receiving phone calls, messages, network polling activity, and the use of remote erasure systems; the latter being an enterprise feature designed for corporate smart phones. Such network activities can alter the contents of a mobile device, potentially adding new data, overwriting existing data or unallocated space, or erasing the phone contents remotely.

Some devices can be reconfigured to prevent communication with the network. Devices that do not have such a feature can be isolated from radio waves by placing them in Faraday isolation, such as radio-frequency shielded evidence containers, which block network communications. Signal jamming systems provide another means for preventing mobile devices from communicating with a network but this type of equipment is illegal in some jurisdictions. Network isolation practices must be maintained during forensic analysis, and this is achieved with shielded mobile phone examination rooms or extraction cases. To protect the device against damage or accidental activation, package it in an envelope or bag.

"Digital Evidence and Computer Crime, Third Edition" by Eoghan Casey and Benjamin Turnbull

© 2017 Envista Forensics

Challenging the Evidence

- Challenging Manual Examinations
  - Isolation from the Cellular Network

37.1.1 Protecting cell phone evidence

Like all digital evidence, the data on cell phones must be protected from being changed or destroyed during the examination process that can occur if the cell phone is allowed to connect to a cellular network. To do this, a cell phone must be isolated from all networks to prevent the phone from sending or receiving. This is usually handled by using a Faraday bag to block radio signals to or from the phone. Figure 37.2 shows a phone inside a Faraday bag for isolation during an exam.

A Faraday bag blocks any signals that a cell phone might pick up by blocking electrical fields and radio frequencies. A microwave uses this same technology, utilizing a Faraday cage to contain the radio frequency generated by the magnetron within the cooking chamber. A cell phone can also be isolated from any networks by wrapping the phone in radio frequency shielding cloth and placing the phone into Airplane mode. These are the most common methods of isolating a cell phone from any networks it might connect to. There are others, but whatever methods are used to block the cell phone's signal, they need to comply with best forensic practices and be recognized as a viable solution by the digital forensics community.

"Digital Forensics for Legal Professionals", by Larry Daniel and Lars Daniel.

© 2017 Envista Forensics

Challenging the Evidence

- Challenging Manual Examinations
  - Affidavit Highlights
    - Video Verification
      - When performing a manual examination of a cell phone, video verification must be made to comply with cell phone forensics Best Practices for the forensic acquisition of a cell phone. Otherwise, there can be no way to determine if evidence was deleted, created, or modified intentionally to tamper with the evidence, or unintentionally through ineptitude.
      - Best Practices require that the entirety of a manual examination of a cell phone, from the moment it is turned on until the examination is completed and the phone is powered off, that every moment of the manual forensic examination is recorded for verification purposes.

© 2017 Envista Forensics

Challenging the Evidence

- Challenging Manual Examinations
  - Video Verification

> Invariably, not all relevant data viewable on a phone using the available menus can be captured through a logical acquisition. For example, draft and archived messages are sometimes not recovered by forensic tools. Manually scrutinizing the contents via the phone interface menus while video recording the process not only allows such items to be captured and reported, but also confirms that the contents reported by the tool are consistent with observable data. Manual acquisition must always be done with care, preserving the integrity of the device in case further, more elaborate acquisitions need to be conducted.

This quote is from the NIST article 'Guidelines on Cell Phone Forensics" by Wayne Jansen and Rick Ayers

"Digital Forensics for Legal Professionals", by Larry Daniel and Lars Daniel.

© 2017 Envista Forensics

Challenging the Evidence

- Challenging Manual Examinations
  - Video Verification

Table 20.2 Methods of Extracting Information from Mobile Devices

Method	Description
Manual operation via user interface	Examiner manually accesses the phone through the user interface. To ensure that all details are documented and the chain of custody is preserved, this process is normally photographed or videotaped. Only data accessible through the operating system is retrievable. The most basic process.

This quote is from the book "Digital Evidence and Computer Crime, Third Edition" by Eoghan Casey and Benjamin Turnbull.

"Digital Forensics for Legal Professionals", by Larry Daniel and Lars Daniel.

© 2017 Envista Forensics

Challenging the Evidence

- Challenging Manual Examinations
  - Video Verification

> Pictures only tell part of the story; what could have happened during the time between the individual pictures being taken? Pictures alone do not provide any real verification that the phone evidence has not been modified or tampered with. The only way to make a truly verifiable manual examination of a cell phone is to also record the process using a digital video camera running continuously throughout the process with no breaks, pauses, or edits. The video should begin before the phone is taken out of the secure evidence container and should be powered on in view of the camera. At the end of the examination, the phone should be powered down in view of the camera and placed back into a secure evidence container.

This quote is from the book "Digital Forensics for Legal Professionals", by Larry Daniel and Lars Daniel.

© 2017 Envista Forensics

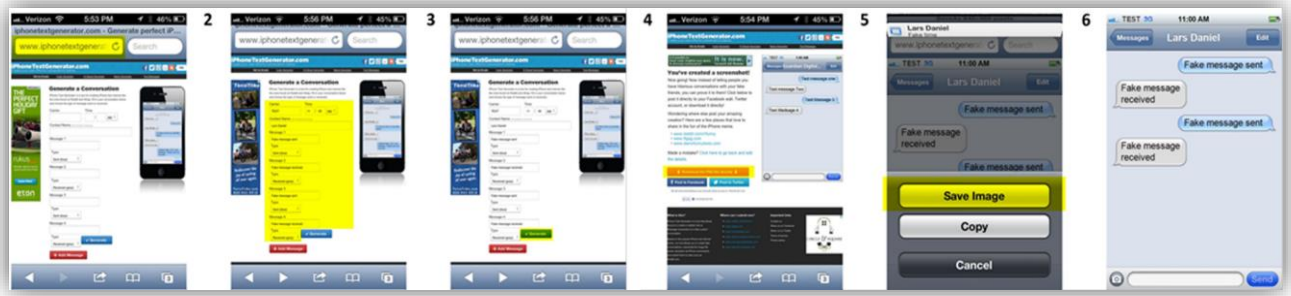
Challenging the Evidence

- Challenging Manual Examinations
  - Fake Messages are real.
    - Pictures or screenshots of text messages are not enough. They can be faked easily, quickly, and require a low level of technical sophistication.

© 2017 Envista Forensics

Challenging the Evidence

- Challenging Manual Examinations
  - Fake Messages
    - Websites



© 2017 Envista Forensics

Challenging the Evidence

- Challenging Manual Examinations
  - Fake Messages
    - Name Change



© 2017 Envista Forensics

Challenging the Evidence

- Challenging Manual Examinations
  - Fake Messages
    - Time Change





© 2017 Envista Forensics

Challenging the Evidence

- Challenging Manual Examinations
  - Fake Messages
    - Voices in my head



© 2017 Envista Forensics

Spoofing – Case Example

- Violation of Restraining Order
  - Client accused by ex girlfriend of threatening her
  - Client arrested and sitting in jail for 6 months

Statement of Investigating Officer In Detail

1. What happened? How was crime committed?

THE VICTIM HAS A 50B ORDER ON THE DEFENDANT THAT STATES HE CANNOT CONTACT HER VIA TEXT OR PHONE. THE DEFENDANT SENT A TEXT TO THE VICTIM STATING THAT HE WAS GOING TO GO TO HER PLACE OF WORK WITH A GUN AND CAUSE DEATH OR BODILY INJURY TO HER.

© 2017 Envista Forensics

Spoofing – Case Example

- Violation of Restraining Order
  - Client accused by ex girlfriend of threatening her
  - Client arrested and sitting in jail for 6 months

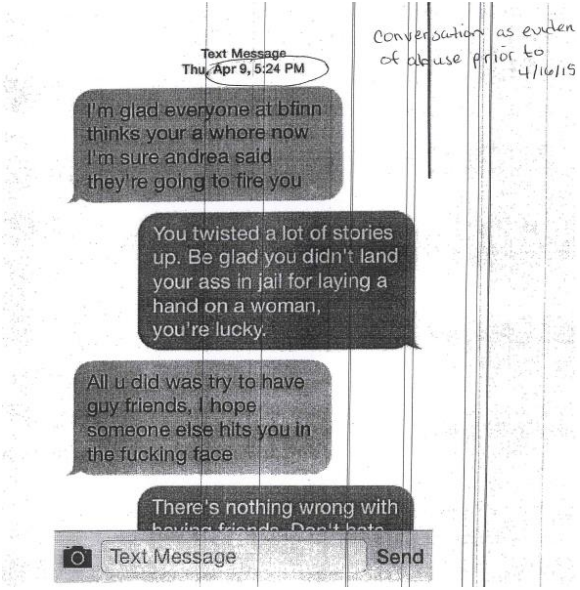
2. What facts point to this (these) defendant(s) guilt?

THE DEFENDANT HAS VIOLATED THE 50B ORDER TWICE IN THE PAST AND STATED ON THE TEXT THAT HE IS AWARE OF THE POLICE AND WILL STILL GO AFTER HER, THREATENING HER LIFE. HE STATED "UR SO DUMB I DON'T CARE ABOUT A RESTRAIN ORDER BITCH", "I DON'T GIVE A FUCK ABOUT THE LAW i'LL DO WHATEVER i WANT YOU CAN'T CALL THE POLICE", "UR FUCKED WHEN I GET OFF WORK 2NITE i 'M COMING TO ALE HOUSE AND U BETTER WATCH OUT CUZ THE LAW DIDN'T TAKE MY GUNS! YOULL NEVER BE SEEN AGAIN WHEN I GET TO YOU"

© 2017 Envista Forensics

Spoofing – Case Example

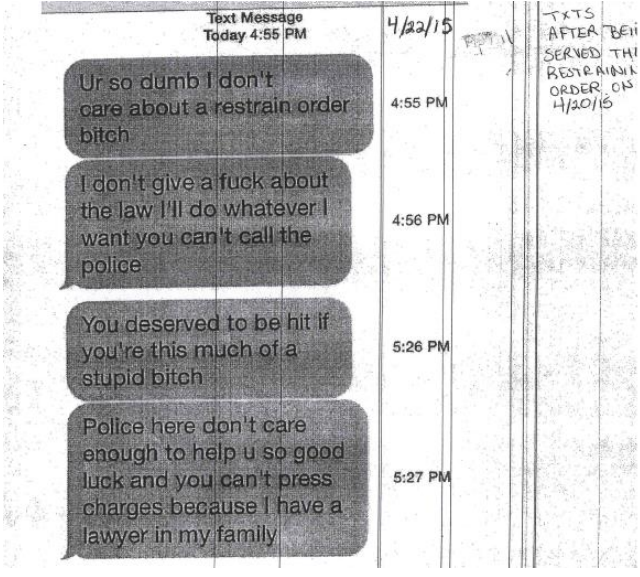
- What is the evidence of the crime?
  - Photos of the text messages on the girl friends phone.



© 2017 Envista Forensics

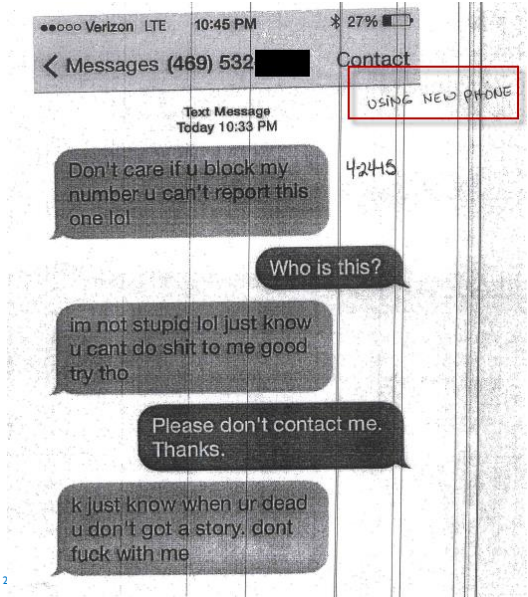
Spoofing – Case Example

- What is the evidence of the crime?
  - Photos of the text messages on the girlfriend's phone.



Spoofing – Case Example

- What is the evidence of the crime?
  - Photos of the text messages on the girlfriend's phone.
  - Girlfriend claims he got a new phone number.



© 2

Spoofing – Case Example

- Did he really get a new number?
- How can we find out?
  - Tracked phone number to GoTextMe service.
  - Sent a subpoena for subscriber information.

Subscriber Information for (469) 532[redacted] / id #80808333

- **User id**: 80808333
- **Username**: jakedasnakek3816
- **Signup Date (UTC)**: April 25, 2015, 2:32 a.m.
- **Last Login (UTC)**: June 2, 2015, 5:01 p.m.
- **Email**: jakedasnakek@tahoo.com *Not verified - as specified by user*
- **Phone number**: *Not verified - as specified by user*
- **TextMe number**: +146953[redacted]
- **IP when number assigned**: 70.193[redacted] - on 2015-04-25 02:32:55.352938
- **Device Id**: 5311B946-C314-41C1-A6A5-DC27C915F22A
- **idfa**: 3532203C-7771-4D0E-96CA-66C987DD8B7E
- **Geolocation**: Longitude: -78.4371 / Latitude 35.6263 (*May be inaccurate*)

Creation date

IP Address when created

Physical phone ID

Notes: All dates in this report are UTC, message length in characters, call duration in seconds

© 2017 Envista Forensics

Spoofing – Case Example

- Did he get a new number?
- How can we find out?
  - IP address for account creator
    - Belongs to Verizon. (His phone is on Sprint.)

IP Information for 70.193.54.95

Quick Stats

IP Location	United States Myrtle Beach Verizon Wireless
ASN	AS22394 CELLCO - Cellco Partnership DBA Verizon Wireless, US (registered Apr 24, 2007)
Resolve Host	95.sub-70-193-54.myvzw.com
Whois Server	whois.arin.net
IP Address	70.193.54.95

© 2017 Envista Forensics

Spoofing – Case Example

- Did he really get a new number?
- How can we find out?
  - Subpoena to Verizon
    - Who had this IP address on that date and time?
      - She did!!



© 2017 Envista Forensics

Spoofing – Case Example

- Did he really get a new number?
- How can we find out?
  - Sent a subpoena for subscriber information.

Phone Device ID matches her phone in Verizon response.

Subscriber Information for (469) 532-[redacted] / id #80808333

- **User id**: 80808333
- **Username**: jakedasnakek3816
- **Signup Date (UTC)**: April 25, 2015, 2:32 a.m.
- **Last Login (UTC)**: June 2, 2015, 5:01 p.m.
- **Email**: jakedasnakek@tahoo.com *Not verified - as specified by user*
- **Phone number**: *Not verified - as specified by user*
- **TextMe number**: +146953[redacted]
- **IP when number assigned**: 70.193[redacted] - on 2015-04-25 02:32:55.352938
- **Device Id**: 5311B946-C314-41C1-A6A5-DC27C915F22A
- **idfa**: 3532203C-7771-4D0E-96CA-66C987DD8B7E
- **Geolocation**: Longitude: -78.4371 / Latitude 35.6263 (*May be inaccurate*)

Creation date

IP Address when created

Physical phone ID

Notes: All dates in this report are UTC, message length in characters, call duration in seconds

© 2017 Envista Forensics

Spoofing

- Fake messages are real!
  - Pictures or screenshots of text messages are not enough.
  - Many services available for creation of new phone numbers, text message, etc.



© 2017 Envista Forensics

Challenging the Evidence

- Challenging the Evidence
  - Boppin'em on the head



© 2017 Envista Forensics

Challenging the Evidence

- Challenging the Evidence
  - Boppin'em on the head
    - Did the defendant have a gun at the time of the thefts?

File Info		Additional file info		Thumbnail	Deleted
Name:	IMG_0964.JPG	**Size (bytes):**	475428		
Path:	/Data/mobile/Media/DCIM/100APPLE/IMG_0964.JPG	**Created:**	11/11/2013 6:18:26 PM(UTC-5)		
		Modified:	11/11/2013 6:18:26 PM(UTC-5)		
SHA256:		**Accessed:**	11/11/2013 6:18:26 PM(UTC-5)		
		Meta Data:			
		Camera Make:	Apple		
		Camera Model:	iPhone 4S		
		Capture Time:	10/30/2013 2:54:29 PM		
		Pixel resolution:	3264x2448		
		Resolution:	72x72 (Unit: Inch)		
		Make:	Apple		
		Model:	iPhone 4S		

© 2017 Envista Forensics

Challenging the Evidence

- Challenging the Evidence
  - Boppin'em on the head
    - Pictures on phone

The phones are identified throughout this report by their serial number. Both cell phones were model iPhone 4. There serial numbers for the phones is as follows:

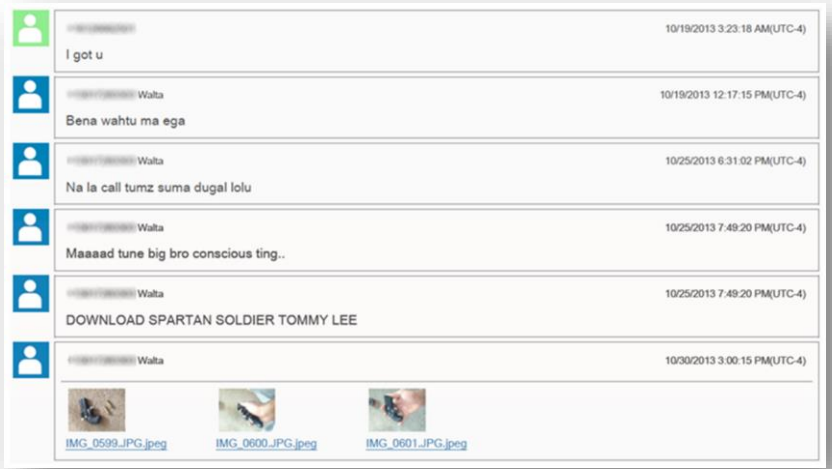
1. iPhone SN 870230YBA4S
2. iPhone SN 87120P9PDZZ



© 2017 Envista Forensics

Challenging the Evidence

- Challenging the Evidence
  - Boppin'em on the head



© 2017 Envista Forensics

Challenging the Evidence

- Challenging the Evidence
  - Boppin'em on the head

These same images also exist in the DCIM folder of the phone. All three of these images located in the DCIM folder were taken with an iPhone 4S according the metadata contained in the images. Both of the defendant's phones were the model iPhone 4.

The most probable explanation is that the following three images were saved to the phone's picture folder from the messages stream between Walta and the defendant. The images were received by the defendant originally from Walta, and the metadata for these pictures does not match the defendant's model of phone.

Further, the "Capture Time" of the images (when the photo was actually taken) is minutes before the message containing the images was sent to the defendant from Walta, and the filesystem metadata for the images shows that they were created on the phone days later on 11/11/2013.

© 2017 Envista Forensics

Challenging the Evidence

- Challenging the Evidence
  - Signed, sealed, delivered.
    - Technology argument
      - Intent to possess contraband?



© 2017 Envista Forensics

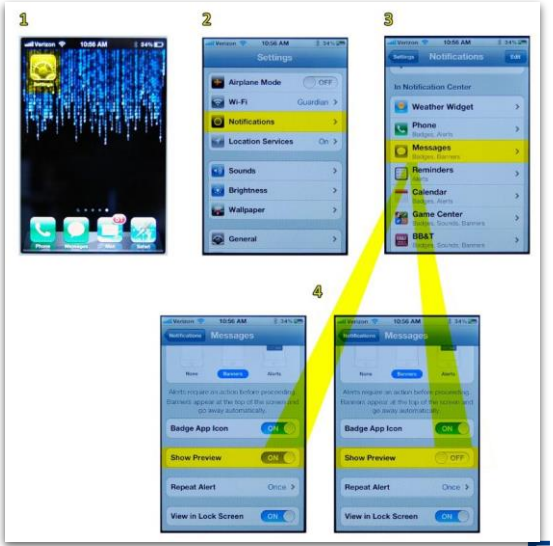
Challenging the Evidence

- Challenging the Evidence
  - Signed, sealed, delivered.
    - When receiving a MMS or SMS message on an iPhone, the recipient of the message cannot determine the contents of the message until it has already been received and viewed. Further, with a SMS or MMS message, the user does not have the ability to prevent the reception of the message.
    - If a person sends a SMS or MMS message to someone else, that message is automatically delivered to the other person ***regardless of their consent*** or intent to receive that message.
    - The delivery and receiving of MMS and SMS messages is an ***automated*** process carried out by cellular service providers and cell phone hardware that does not allow for a user to determine what SMS or MMS messages they receive. The only way to determine what the contents of SMS and MMS message are is to view the message. This description of the sending and receiving of MMS and SMS text messages is not isolated only to iPhones, but is the normal operation of almost all cellular phones.

© 2017 Envista Forensics

Challenging the Evidence

- Challenging the Evidence
  - Signed, sealed, delivered.
    - Preview on, or off.



© 2017 Envista Forensics

Challenging the Evidence

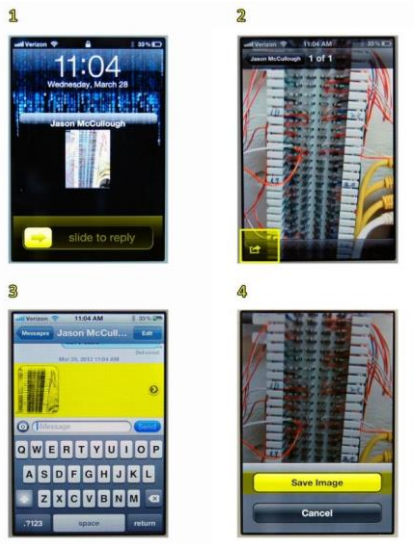
- Challenging the Evidence
  - Signed, sealed, delivered.
    - Preview on, or off.



© 2017 Envista Forensics

Challenging the Evidence

- Challenging the Evidence
  - Signed, sealed, delivered.
    - For a user to intentionally preserve that image, it has to be saved to the *Photos* application on the iPhone by selecting the image, then viewing it in full screen mode, selecting the *Share* icon, and then selecting *Save Image* option in the pop-up dialogue box.



© 2017 Envista Forensics

Challenging the Evidence

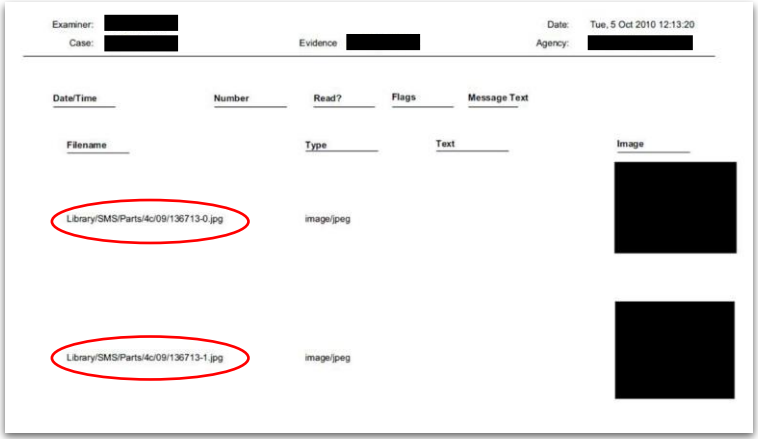
- Challenging the Evidence
  - Signed, sealed, delivered.
    - When an MMS message containing a picture is received on an iPhone, ***it will only exist within the SMS folder of the file system on iPhone***. The picture is ***automatically saved*** there upon receipt of the message without any input or preservation steps taken by the user. An image existing within the SMS folder of an iPhone file system will have file path that is consistent with the following example:

- **Library/SMS/Parts/35/05/55555-5.jpg**

© 2017 Envista Forensics

Challenging the Evidence

- Challenging the Evidence
  - Signed, sealed, delivered.
    - Images only existed in the SMS folder of the iPhone file system.


Examiner: [redacted]
Case: [redacted]
Evidence [redacted]
Date: Tue, 5 Oct 2010 12:13:20
Agency: [redacted]

Date/Time | Number | Read? | Flags | Message Text

Filename | Type | Text | Image

Library/SMS/Parts/4c/09/136713-0.jpg | image/jpeg | [redacted]

Library/SMS/Parts/4c/09/136713-1.jpg | image/jpeg | [redacted]

© 2017 Envista Forensics

Beyond Cell Phones

- Backups
  - Cloud and local
- Data Syncing
  - Device ecosystems
    - Don't "bank" on it being gone.
- Pods, players, and pads





© 2017 Envista Forensics

ENVISTA FORENSICS

CELLULAR LOCATION

CSLI (CELL SITE LOCATION INFORMATION)

© 2017 Envista Forensics

AUTOMATED SOFTWARE

IT DOESN'T WORK.

© 2017 Envista Forensics

Automated Software

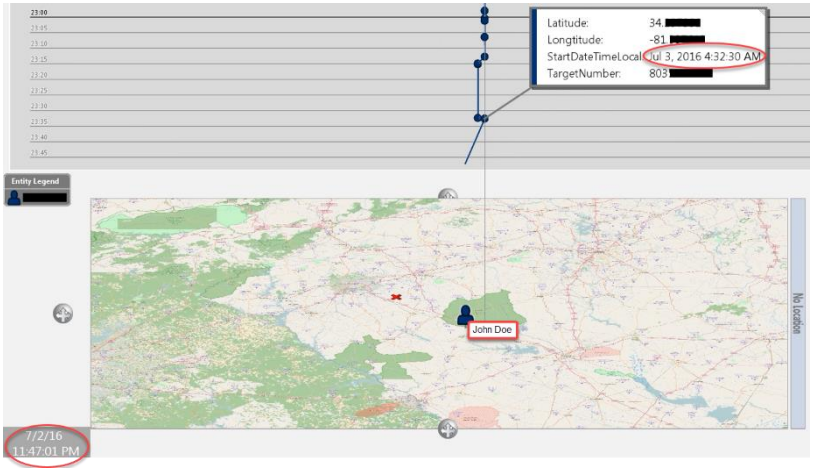
- Coverage area?
- This odd shape is not based on science or any other factual data.



© 2017 Envista Forensics

Automated Software

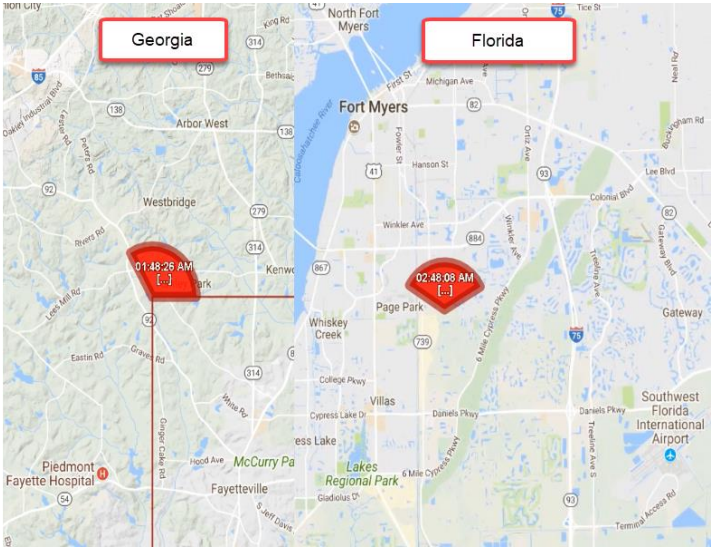
- The State's "Expert" admitted, the software made mistakes. UTC to local offsets set incorrectly
- EDT = UTC-4, not +5
- Again faulty and unreliable/unscientific method of standard coverage



© 2017 Envista Forensics

Automated Software

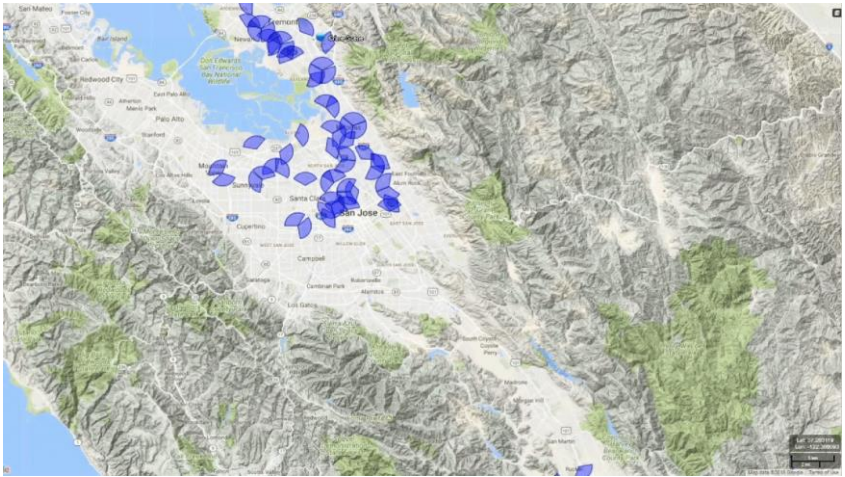
- Again we proved to the Prosecution that the automation and lack of real expert using the software caused inaccuracies. This software plotted a call in Georgia and then in Florida with a one hour time difference.



© 2017 Envista Forensics

Automated Software

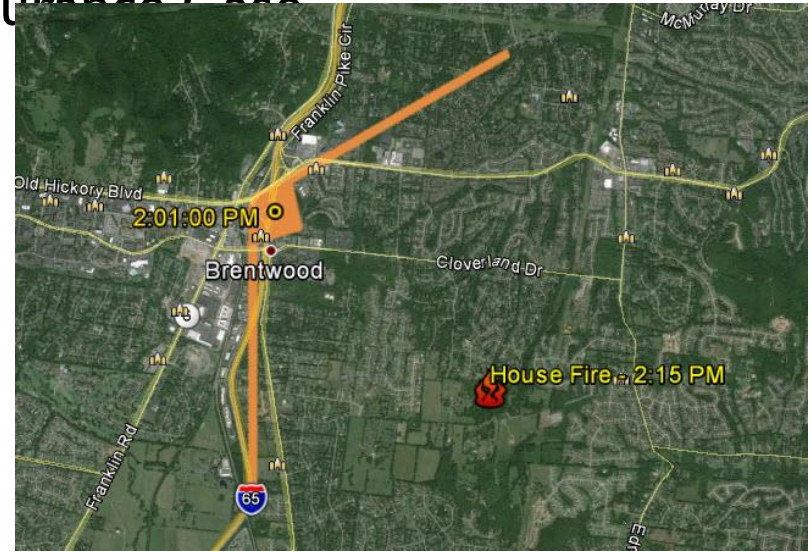
- They also make cool videos



© 2017 Envista Forensics

Call Detail Records: Insurance Case

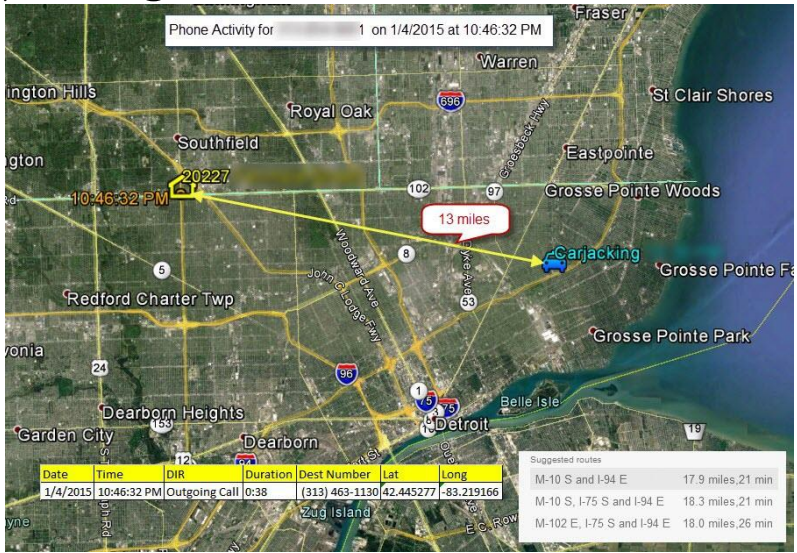
- Hall, we do our tasks
  - Direction of radio waves
  - Bandwidth (spread)



© 2017 Envista Forensics

Call Detail Records: Carjacking

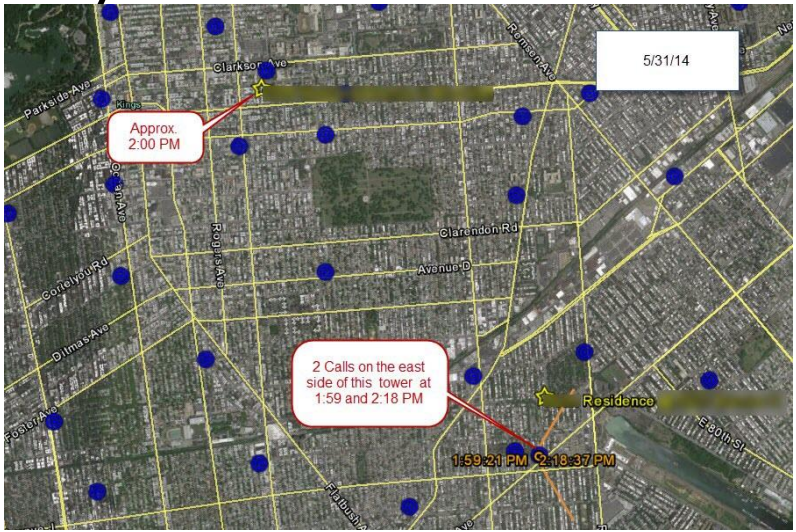
- Accused of carjacking
  - Detriot
  - Phone is 13 miles away, one minute.
  - Case dismissed upon seeing map



© 2017 Envista Forensics

Call Detail Records: Robbery

- Bronx
  - Accused of doing multiple burglaries
  - 2:00PM – location of burglaries
  - Uses tower across town (where his home is) one minute before the burglary.
  - Case dismissed



© 2017 Envista Forensics

Call Detail Records: Murder

- Alibi location
  - Green house
  - Claims to be here from 6-8PM
- Phone location?
  - Uses cell tower of crime location from 6-8
- Resulted in plea bargain

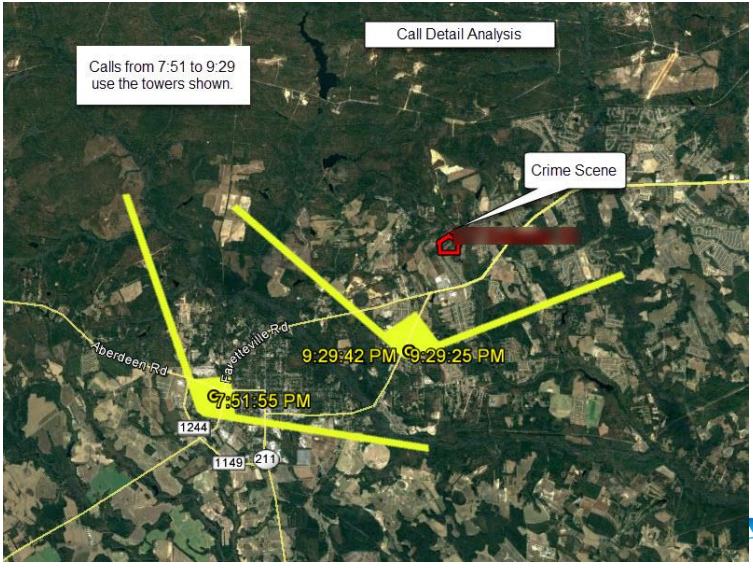


Time	DURATION	M_R_	1ST CELL	Azimuth
6:00:48 PM	438	Inbound	10630	20
6:56:45 PM	21	Outbound	10630	20
6:57:13 PM	5	Outbound	10630	20
7:05:11 PM	16	Outbound	10630	20
7:06:28 PM	17	Outbound	10630	20
7:09:53 PM	112	Inbound	10630	20
7:12:54 PM	45	Outbound	10630	20
7:13:10 PM	24	Inbound	10630	20
7:13:50 PM	27	Inbound	10630	20
7:14:19 PM	608	Inbound	10630	20
7:32:35 PM	60	Inbound	10630	20
7:33:40 PM	11	Outbound	10630	20
7:33:54 PM	10	Outbound	10630	20
7:34:06 PM	10	Outbound	10630	20
7:34:20 PM	90	Outbound	10630	20
7:42:51 PM	182	Inbound	10630	20
7:52:10 PM	182	Inbound	10630	20

© 2017 Envista Forensics

Case Example: CDR and Phone Location

- Location Data
  - Puts defendant's phone near location of the crime scene
    - Cannot say he is at the scene, can only put the phone in the area based upon cellular location analysis.



© 2017 Envista Forensics

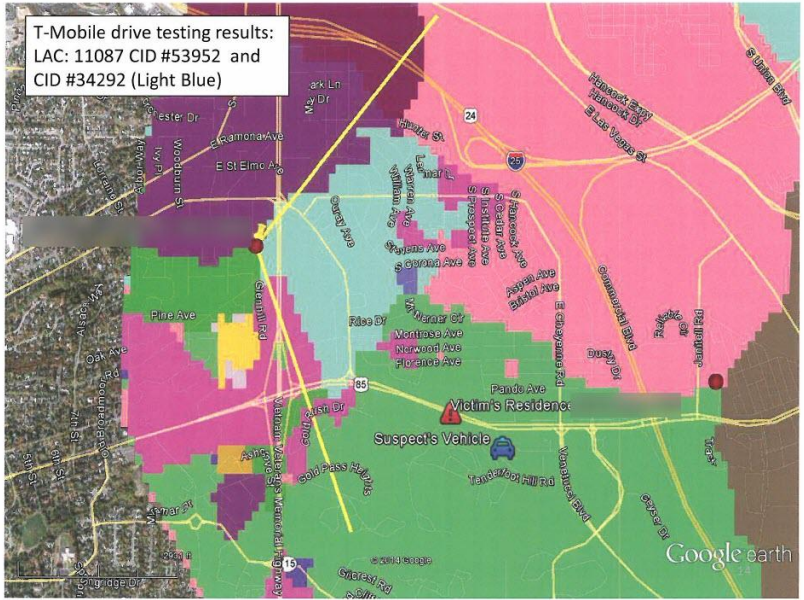
Drive testing

- Radio waves not static
  - Larry Daniel testified
    - Defendant was acquitted
- Only tested certain towers
  - Didn't test all surrounding towers
  - Homicide location in area right now but not tomorrow
    - Ever stood somewhere and watched bars go up and down on phone?



© 2017 Envista Forensics

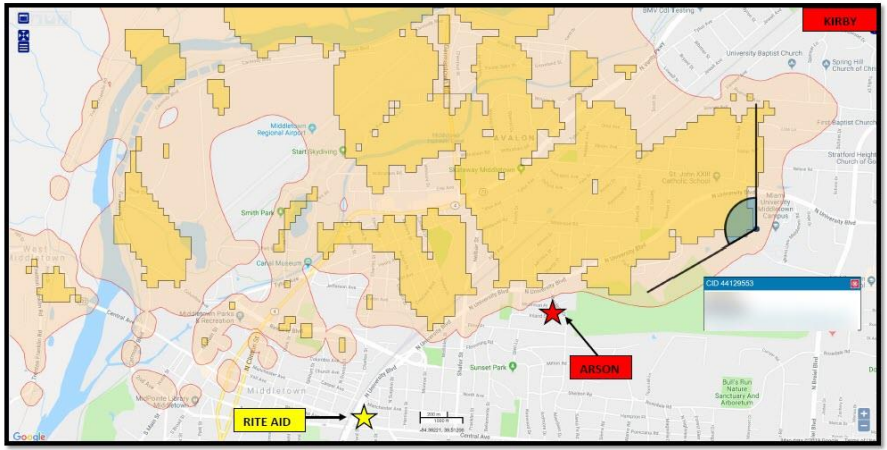
Drive Testing



© 2017 Envista Forensics

Drive Testing

FINAL – 02/04/2019; MODIFIED 04/02/2019

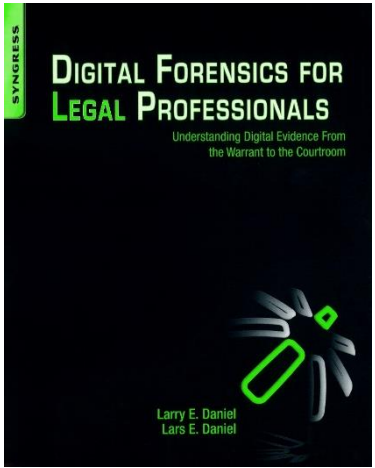


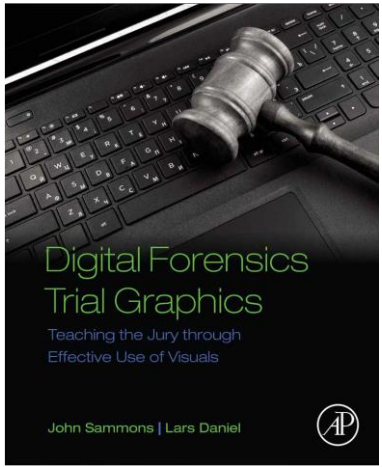
SEPTEMBER 1, 2017 [redacted] utilized the above illustrated cell sites. Drive test footprint for the sector is show above. The dark color shows the DOMINANT signal, which is the strongest best quality signal from the sector. Phones that are within the DOMINANT signal will select this sector for service. The lighter color shows the WEAKER signal, which represents a measurable (but not necessarily a usable) signal.

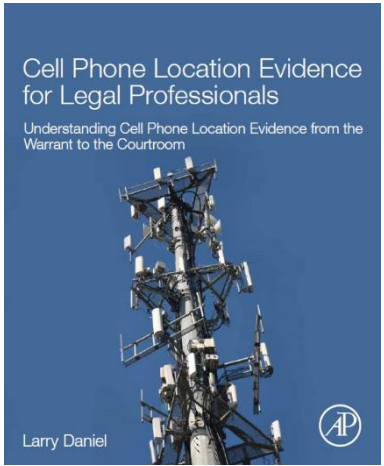
© 2017 Envista Forensics

QUESTIONS?

lars.daniel@envistaforensics.com / 919-621-9335







© 2017 Envista Forensics