



Cell Phone Location Evidence for Legal Professionals

Larry Daniel
DFCP, EnCE, ACE, AME, BCE, CTNS, CTA, CWA

Locating Cell Phones

- Least Precise to Most
 - Call Detail Records
 - (Drive Testing)
 - Google Location Services
 - E-911 Records
 - Phone Based Location
 - Find my iPhone



2 of 68

Call Detail Records "The Evidence"

3 of 68

Call Detail Records (CDRs)



- What are they?
 - Legal proof of a service provided
 - A technical road map of a call
 - A financial transaction record

4 of 68

Call Detail Records (CDRs)



- How to get them
 - Account holder can request with notarized letter
 - Via subpoena
 - Via discovery
 - Always get copies of the original files
 - Contact us for specific subpoena language...It is free.

5 of 68

Call Detail Records (CDRs)



- How are they used?
 - Associate a phone call with a cell tower
 - Show connections between phone numbers
 - Show frequency of connections
 - Show "user" activity

6 of 68

Call Detail Records (CDRs)



- What can they contain?
 - Voice call activity
 - Call forwarding information
 - Text message transaction
 - Data transactions

7 of 68

Call Detail Records (CDRs)



- How are they used?
 - Most common type of evidence in "Cell Phone Location Maps"
 - IMPORTANT
 - You have the location of the cell tower, *NOT* the phone
 - A tenuous relationship to the phone's location
 - *NOT* triangulation @#&^(@!!!

8 of 68

Call Detail Records (Retention)



Carrier	Subscriber	Call History Only	Call History with Towers	SMS Content	"Precision Location"
Verizon	7-10 Years	7 Years	Rolling 12 months	3 to 10 days	8 Days
AT&T/Cricket	7 Years	7 Years	7 Years	N/A	8 Days
Sprint	10 Years	18 Months	18 Months	N/A	180 Days
T-Mobile/ Metro PCS	3 to 5 years	23 Months	23 Months	N/A	23 Months
US Cellular	7 Years	Rolling 12 Months	Rolling 12 months	3 to 5 Days	N/A

9 of 68

Call Detail Records (AT&T)



Time	Orig. Date	Orig. Time	Release Time	Originating Number	Terminating Number	Elapsed Time	Number Dialed	DNIS	DNIS	Description	Cell Location
1	01/08/14	05:03:30	0:05	1601	1731	0:14	1731	012784000	3104104312	MGM_DIR	(14999/20912)++
2	01/08/14	05:04:27	0:07	1731	1731	0:07	1731	012784000	3104104312	MGM_DIR	(14999/20912)++
3	01/08/14	05:05:09	0:04	1731	1731	1:13	1731	012784000	3104104312	MGM_DIR	(14999/20912)++
4	01/08/14	05:05:59	0:07	1731	1731	0:04	2475	012784000	3104104312	MGM_DIR	(14999/20912)++
5	01/08/14	05:06:09	0:07	1731	1731	0:07	1731	012784000	3104104312	MGM_DIR	(14999/20912)++
6	01/08/14	05:06:09	0:07	1731	1731	0:07	1731	012784000	3104104312	MGM_DIR	(14999/20912)++
7	01/08/14	05:06:09	0:07	1731	1731	0:07	1731	012784000	3104104312	MGM_DIR	(14999/20912)++
8	01/08/14	05:06:09	0:07	1731	1731	0:07	1731	012784000	3104104312	MGM_DIR	(14999/20912)++
9	01/08/14	05:06:09	0:07	1731	1731	0:07	1731	012784000	3104104312	MGM_DIR	(14999/20912)++
10	01/08/14	05:06:09	0:07	1731	1731	0:07	1731	012784000	3104104312	MGM_DIR	(14999/20912)++
11	01/08/14	05:06:09	0:07	1731	1731	0:07	1731	012784000	3104104312	MGM_DIR	(14999/20912)++
12	01/08/14	05:06:09	0:07	1731	1731	0:07	1731	012784000	3104104312	MGM_DIR	(14999/20912)++
13	01/08/14	05:06:09	0:07	1731	1731	0:07	1731	012784000	3104104312	MGM_DIR	(14999/20912)++
14	01/08/14	05:06:09	0:06	1239	1731	1:18	1731	012784000	3104104312	MGM_DIR	(14999/20912)++
15	01/08/14	05:10:20	0:13	1731	1731	0:12	1731	012784000	3104104312	MGM_DIR	(14999/20912)++

10 of 68

Call Detail Records (Sprint)



CALLING_NBR	CALLED_NBR	DIALED_DIGITS	M.R.#	START_DATE	END_DATE	DURATION(SEC)	NEID	REPO#	1ST CELL	LAST CELL
(777)	(777)	(777)	Outbound	1/22/12 22:05:03	1/22/12 22:10:19	316	96	71	10661	25661

11 of 68

Call Detail Records (Sprint Towers)



Cell	NEID	Report	Address	City	County	State	Zip	Latitude	Longitude	RIS Manufacturer	Sector	Altitude
80	432	2960	Metzerott Road	College Park	Prince George S	MD	20783	39.00546	76.95705	LUCENT	3	210
80	432	2960	Metzerott Road	College Park	Prince George S	MD	20783	39.00546	76.95705	LUCENT	3	210
80	432	2960	Metzerott Road	College Park	Prince George S	MD	20783	39.00546	76.95705	LUCENT	3	210
80	432	33801	Georgia Ave.	Silver Spring	Montgomery	MD	20906	39.0877797	77.0708293	LUCENT	3	135
80	432	33801	Georgia Ave.	Silver Spring	Montgomery	MD	20906	39.0877797	77.0708293	LUCENT	3	135
80	432	33801	Georgia Ave.	Silver Spring	Montgomery	MD	20906	39.0877797	77.0708293	LUCENT	3	135
80	432	11235	Oak Leaf Dr.	Silver Spring	Montgomery	MD	20901	39.0411097	76.9938997	LUCENT	3	135
80	432	11235	Oak Leaf Dr.	Silver Spring	Montgomery	MD	20901	39.0411097	76.9938997	LUCENT	3	135
80	432	11235	Oak Leaf Dr.	Silver Spring	Montgomery	MD	20901	39.0411097	76.9938997	LUCENT	3	135
80	432	49	Randolph Rd.	Silver Spring	Montgomery	MD	20904	39.0761093	77.00333	LUCENT	3	135
80	432	49	Randolph Rd.	Silver Spring	Montgomery	MD	20904	39.0761093	77.00333	LUCENT	3	135
80	432	49	Randolph Rd.	Silver Spring	Montgomery	MD	20904	39.0761093	77.00333	LUCENT	3	135
80	432	15430	Old Columbia Pike	Burtonsville	Montgomery	MD	20866	39.10889	76.9366697	LUCENT	3	135
80	432	15430	Old Columbia Pike	Burtonsville	Montgomery	MD	20866	39.10889	76.9366697	LUCENT	3	135
80	432	15430	Old Columbia Pike	Burtonsville	Montgomery	MD	20866	39.10889	76.9366697	LUCENT	3	135

12 of 68

What About Burner Phones?



13 of 68

Burner Phone F.A.Qs



- What are they?
 - Pre-Paid Phones
 - No verification of identity needed
 - No valid "Subscriber" information
 - How to you get the records?
 - Seller may reveal the phone company

14 of 68

Burner Phone F.A.Qs



- Getting the records
 - Finding the carrier for the phone number
 - www.fonefinder.net
 - Who owns the number
 - No Porting Information
 - All burner phones have a phone company
 - T-Mobile
 - Metro PCS
 - Verizon
 - Etc.

15 of 68

Burner Phone F.A.Qs



- Getting the records
 - Subpoena the carrier
 - Pre-paid phone records may be a shorter retention period than a post-paid phone.
 - 90 to 180 days in many cases

16 of 68

Cell Phones



17 of 68

The Flip Phone

(Invented by Star Trek writers)

- Simplest form –
 - Just a 2 way radio
- Newer form
 - Calls
 - Texts
 - Some small apps



18 of 68

The Smart Phone

Powerful handheld computer

- Still a 2 way radio
- Plus
 - Camera
 - Texts
 - Millions of Apps



19 of 68

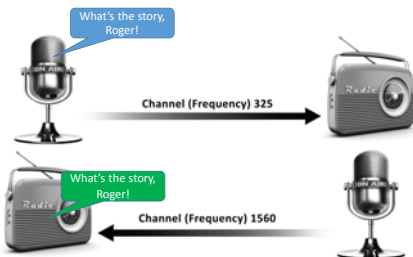
How does a cell phone work?



20 of 68

Communications

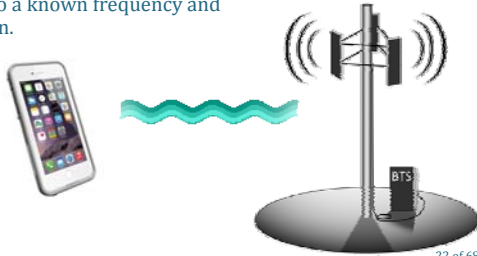
- Walkie-Talkie



21 of 68

Registration

- On Power up
 - Phone tunes to a known frequency and begins to listen.



22 of 68

The Hook Up: Choosing a Tower

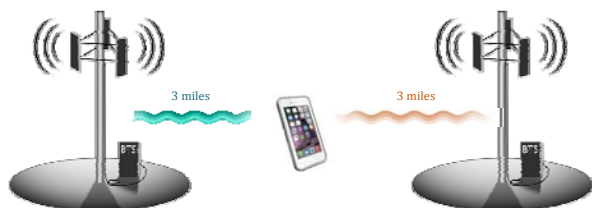
- How does the phone choose a tower?



23 of 68

The Hook Up: Choosing a Tower

- when equidistant, no way to know.



24 of 68

The Hook Up: Choosing a Tower

- Occlusions



25 of 68

The Hook Up: Choosing a Tower

- Channels must be available
 - Let it Snow!



26 of 68

Choosing a Tower: Moving Around

- Hand offs
 - No record of intermediate hand offs
 - May get starting and ending cell towers



27 of 68



How the Cellular System Works

28 of 68



The Cellular System: Cell Site



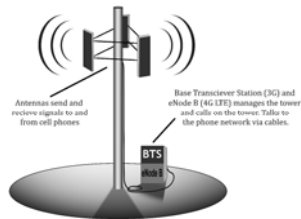
• A Cell Site

• Antennas

- Send and receive signals to and from cell phones

• Base Station Transceiver

- Manages the tower and calls on the tower
- Talks to the phone via network cables

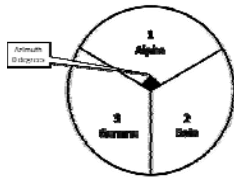


30 of 68

Cell Tower Sectors



- Sector Layout and Azimuth
 - Cell towers can have from 0 to 6 sectors
 - Most common is three sectors
 - Azimuth is the direction the antenna points

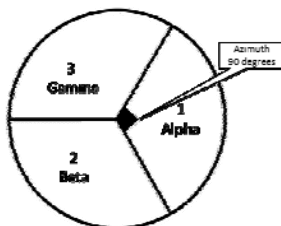
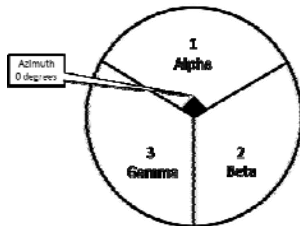


31 of 68

Cell Tower Sectors



- Sector Layout and Azimuth



32 of 68

Cell Tower Sectors



33 of 68



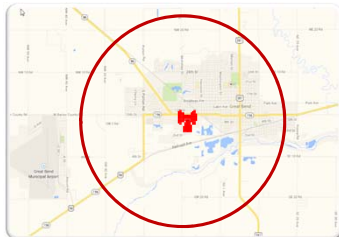
Cell Tower Coverage

34 of 68

Cell Coverage

- Area size is determined by customer needs

- More people, more towers
- More cows, less towers

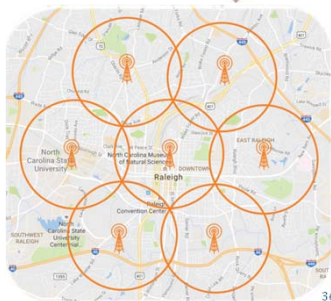


35 of 68

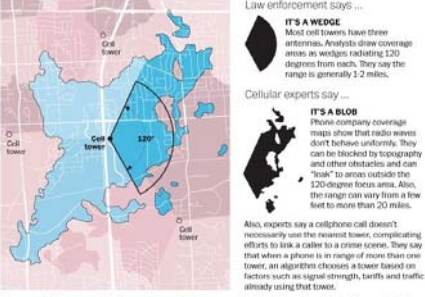
Subscriber Density

- As subscribers increase:

- Coverage size per tower gets smaller
 - Each cell site may have 200 channels (100 calls)
- Need more towers with smaller radius versus one large tower.



36 of 68



Law enforcement says ...

IT'S A WEDGE
Most cell towers have three antennas. Analysts draw coverage areas as wedges radiating 120 degrees from each. They say the range is generally 3-2 miles.

Cellular experts say ...

IT'S A BLOB
Phone company coverage maps show that radio waves don't behave uniformly. They can be blocked by topography and other obstacles and can "leak" to areas outside the 120-degree focus area. Also, the range can vary from a few feet to more than 20 miles.

Also, experts say a cellphone call doesn't necessarily use the nearest tower, complicating efforts to link a caller to a crime scene. They say that when a phone is in range of more than one tower, an algorithm chooses a tower based on factors such as signal strength, tariffs and traffic already using that tower.

Sources: FBI Cellular Analysis and Survey Team, Larry Daniel of Guardian Digital Forensics | The Washington Post June 27, 2014

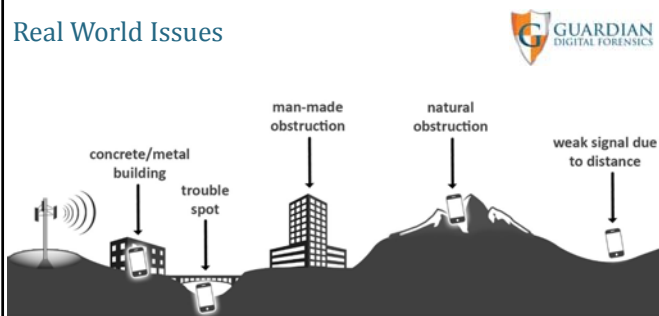
How Far?

- How far can a cell phone be from a tower and still make or receive a call?
 - Assuming a perfectly flat earth, extremely tall cell tower, maximum legal power output, and no other cell towers in the area...
 - GSM (AT&T or T-Mobile) = 22 miles
 - CDMA (Sprint, Verizon, etc.) = 35 Miles
 - Limiting factors
 - Terrain, ground clutter, proximity of other towers, signal strength, cell phone being used, tower height, radio frequency...and the list goes on...

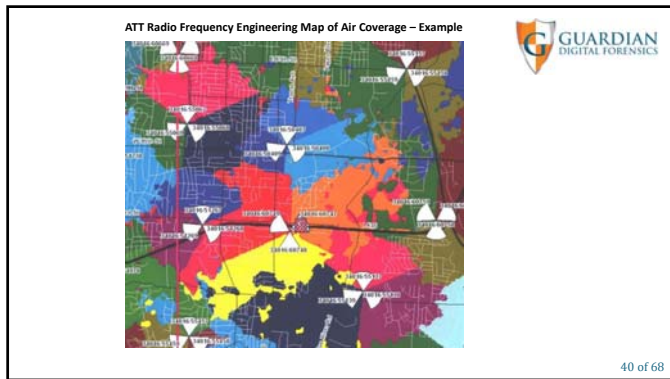


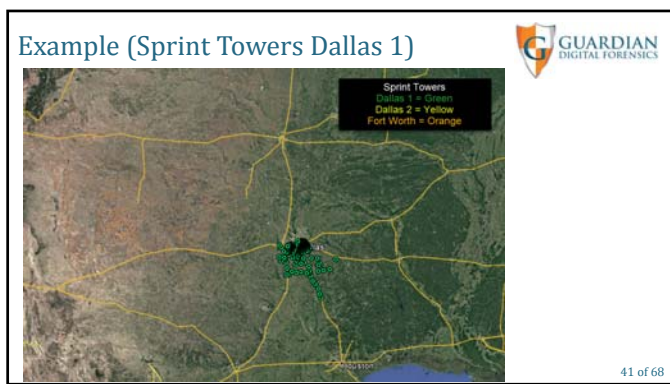
38 of 68

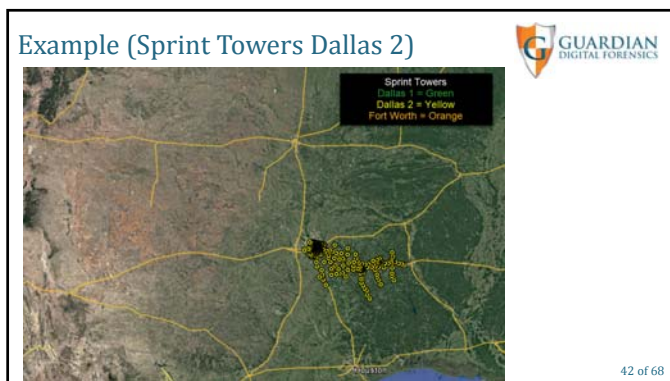
Real World Issues



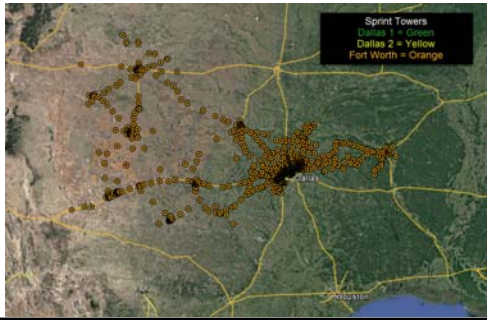
39 of 68





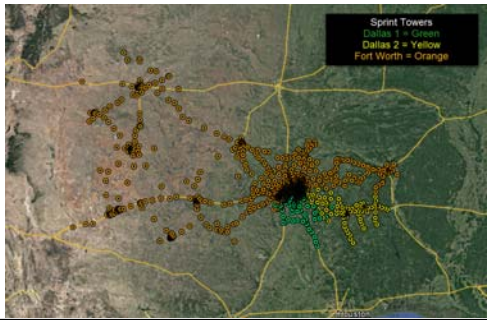


Example (Sprint Towers Ft Worth)



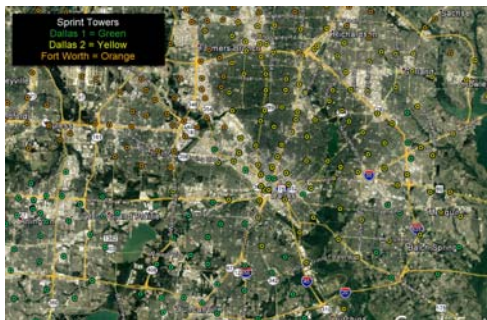
43 of 68

Example (Sprint Towers All)



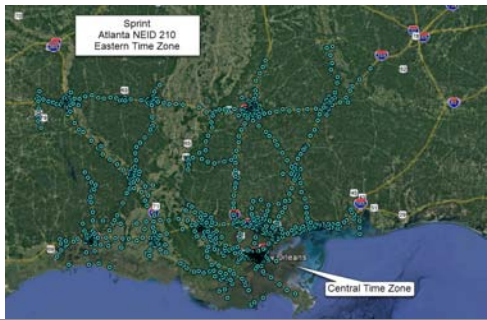
44 of 68

Example (Sprint Towers All)



45 of 68

Example (Sprint Towers Atlanta)



46 of 68

Examples



www.guardiandf.com / 919-868-6291

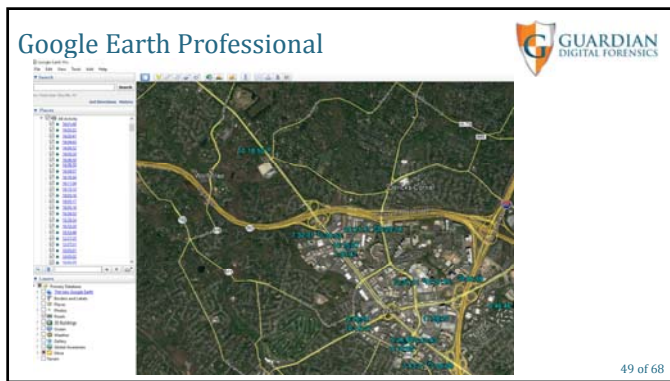
47 of 68

Viewing KML / KMZ files

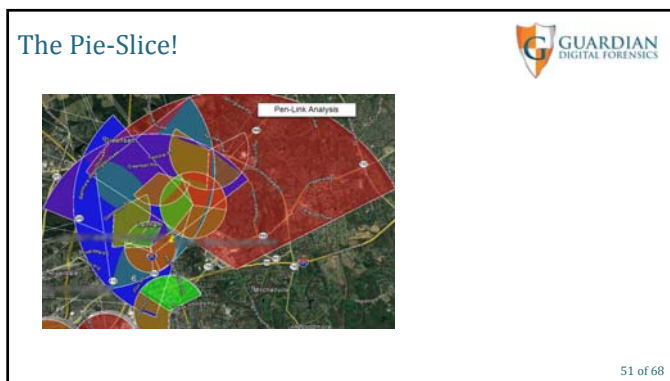
- What are they?
 - Work product output from some police and private experts
- Google Earth File format
 - Can be opened using Google Earth Professional
 - Now a free program



48 of 68







The Pie-Slice! (1)



Figure 4: Map of the Alexandria area of a cellular sector in an urban environment.

52 of 68

The Pie-Slice! (2)

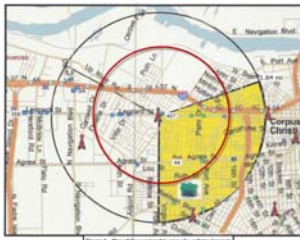


Figure 4: Map of the Alexandria area of a cellular sector in an urban environment.

53 of 68

This is "expert" training?



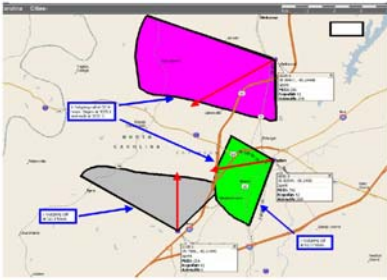
Overlapping antennas.

Example used to show expert training in cellular analysis



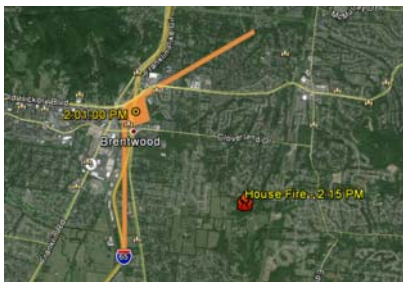
54 of 68

Expert Analysis or Fantasy?



55 of 68

Call Detail Records: Insurance Case



56 of 68

Call Detail Records: Carjacking



57 of 68

Call Detail Records: Robbery



58 of 68

Call Detail Records: Murder



59 of 68

Case Example: CDR and Phone Location



60 of 68

Case Example: CDR and Phone Location



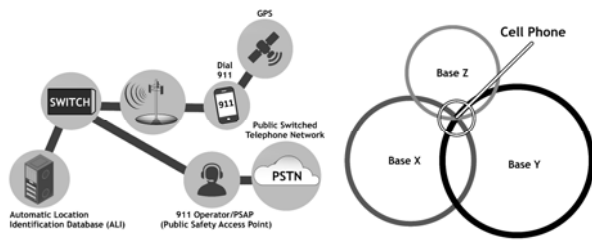
61 of 68

Drive testing



62 of 68

E-911 Location



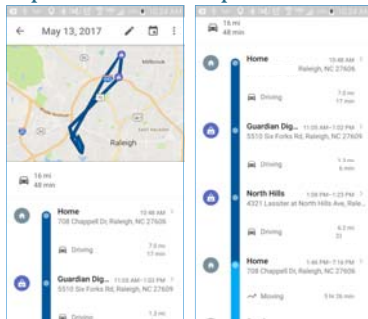
63 of 68

Google Location Services



64 of 68

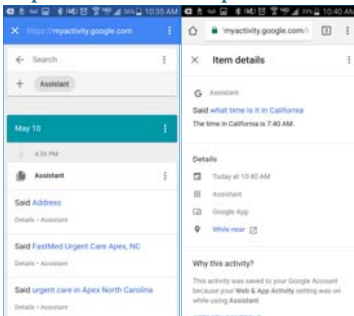
Capabilities: Examples



- Google is watching
 - Location activity
 - Full route

65 of 68

Capabilities: Examples



- Google is listening
 - Location activity
 - Full route

66 of 68

Find my iPhone – Device Based

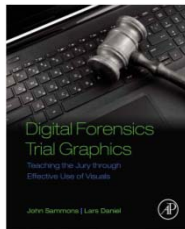
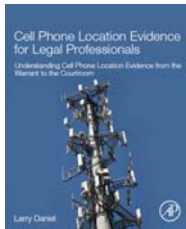
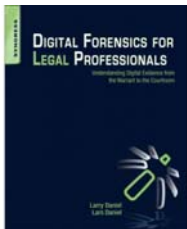


67 of 68

- www.guardiandf.com
- 919-868-6291
- larry@guardiandf.com



Highly qualified experts in computer, cell phone, cellular location, GPS, and cyber risk forensics.



68 of 68
