

Cell Phone Evidence

Philip J. Mergen - Senior Investigator, Madison Trial Office

Visual vs. Forensic Examination

Visual Examination



Cell Phone Worksheet

Philip J. Mergen

17 S Fairchild - 2nd Floor
Madison, WI 53703
office - 608-267-1762
fax - 608-267-1777
mergenp@od.wi.gov

Client -	<input type="text"/>
Case Number -	<input type="text"/>
Attorney -	<input type="text"/>
Device Owner -	<input type="text"/>
Phone Number -	<input type="text"/>
Manufacturer -	<input type="text"/>
Model -	<input type="text"/>
Service Provider -	<input type="text"/>
PIN / Password -	<input type="text"/>
Pattern Lock -	
Other -	<input type="text"/>

[Link to form](#)

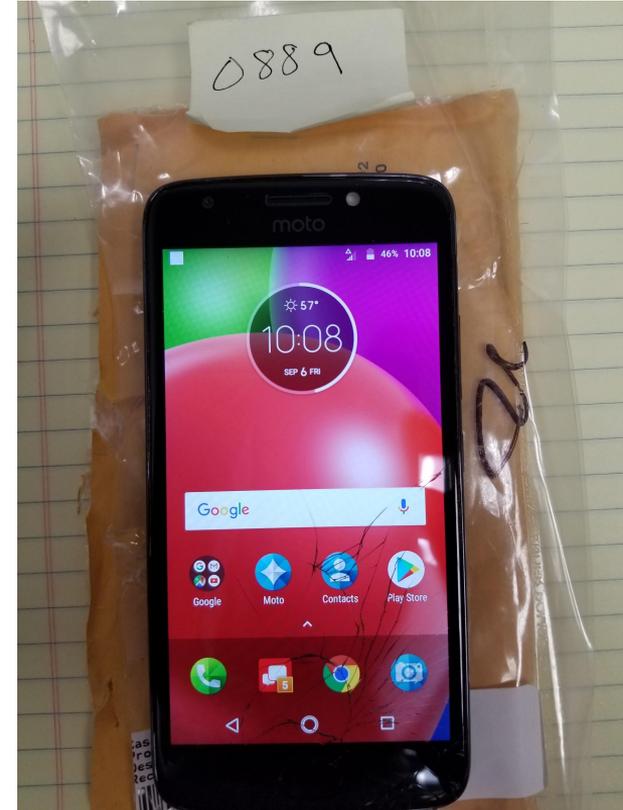
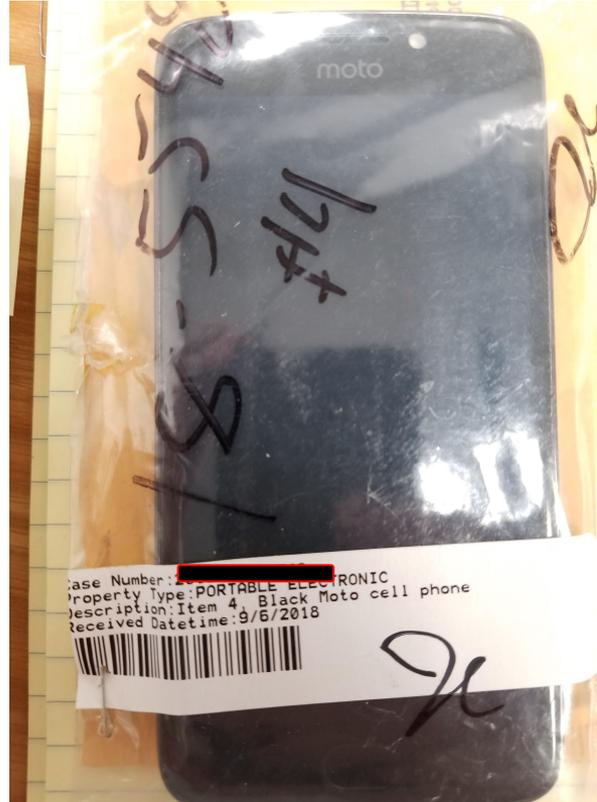
Visual Examination Method #1: Camera

- o Use camera to take photos of the screen
- o Incoming/outgoing calls
- o Incoming/outgoing text messages
- o Photos
- o Emails
- o Social media app messages
- o Contacts
- o Calendar



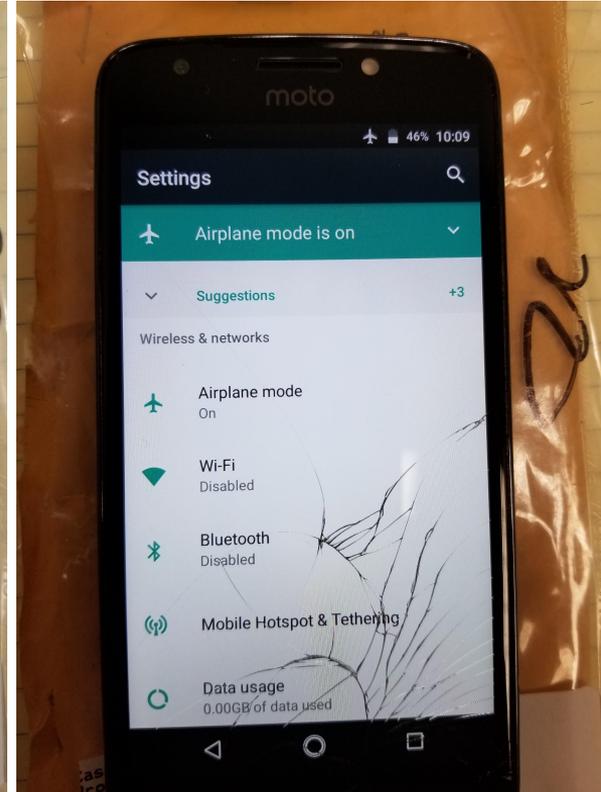
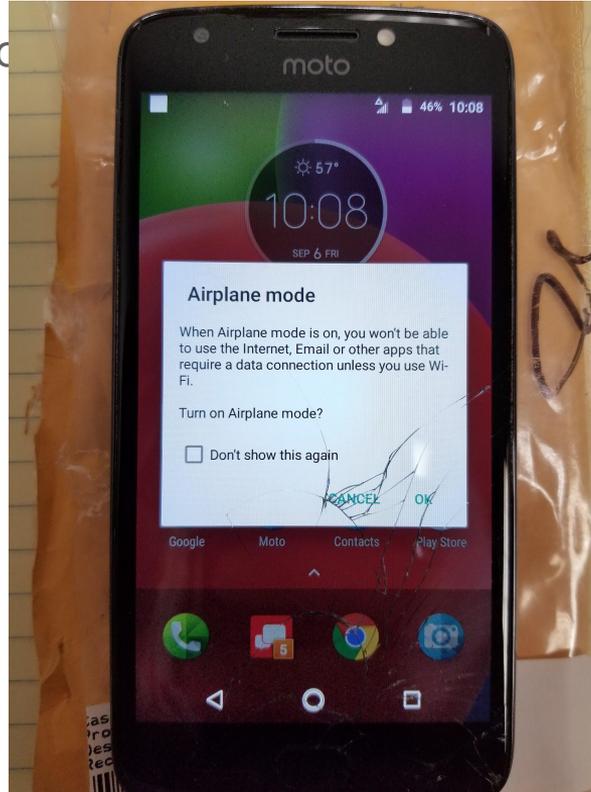
Visual Examination Method #1: Camera

- o Document each step of the examination



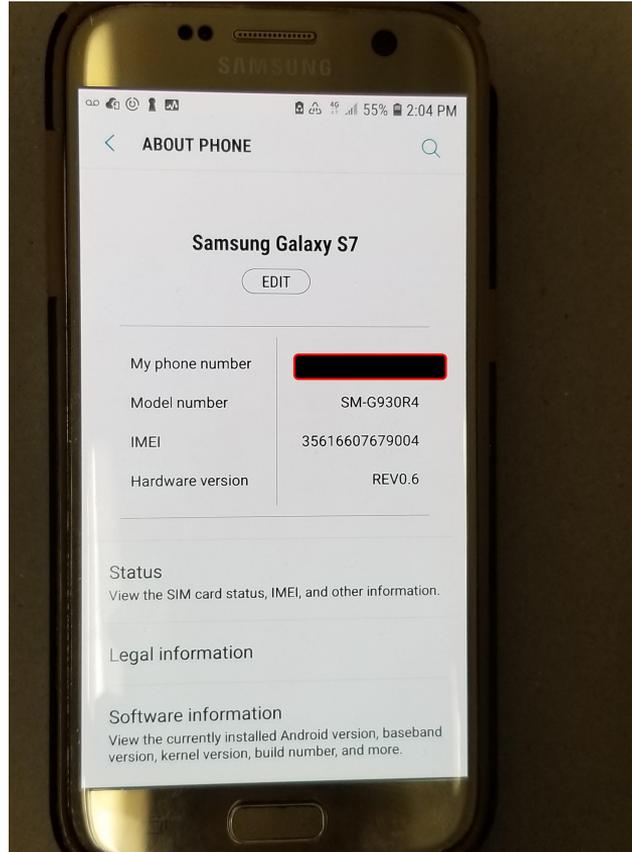
Visual Examination Method #1: Camera

- Turn on “Airplane Mode” to prevent changes to the phone



Visual Examination Method #1: Camera

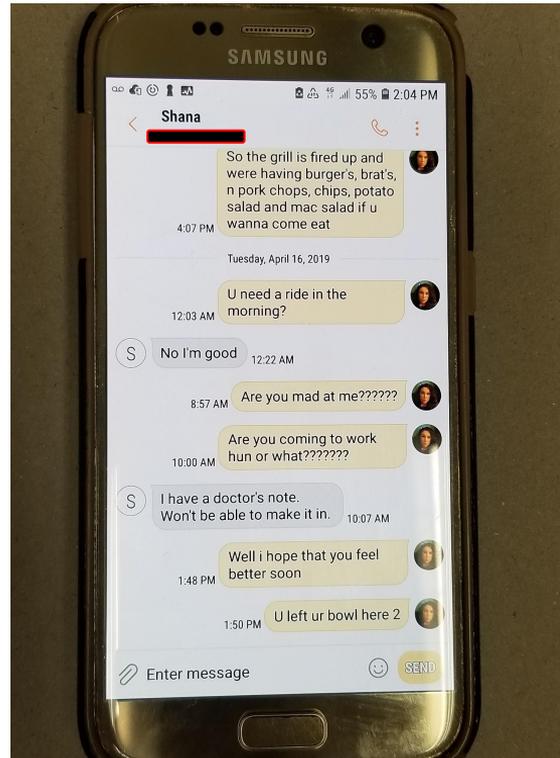
- o Preserve “About Phone” details contained within the settings menu



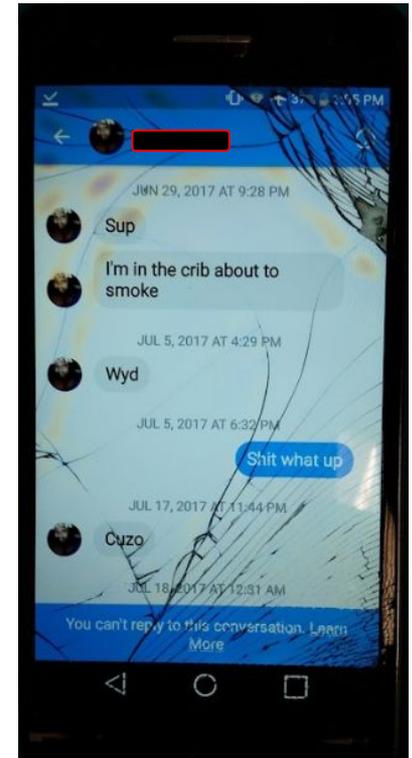
Visual Examination Method #1: Camera

- o Photograph each screen
- o Each message needs to have date + time displayed

SMS



Messenger

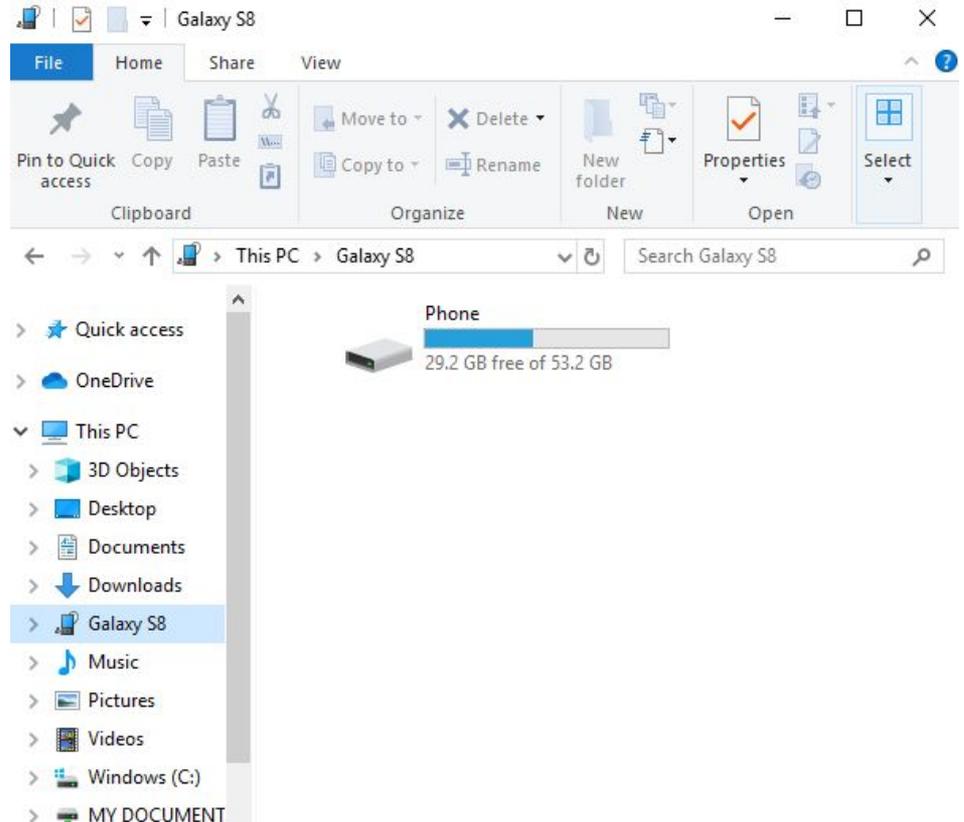


Visual Examination Method #2: Video Camera

- o Best practice.
- o Use video camera to record entire examination.
- o Provides verification that nothing was modified, deleted or changed during your visual examination.

Visual Examination Method #3: Connect to PC

- o Connect phone to PC
- o Limited to Photos, Videos and other Downloaded media



**Forensic Examination:
Oxygen Forensic Suite**



Device Data Report

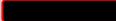
Common information	
Alias	Samsung Galaxy Grand Prime (SAMSUNG-SM-G530AZ)
Retail name	Samsung Samsung Galaxy Grand Prime (SAMSUNG-SM-G530AZ)
Manufacturer	Samsung
Internal name	SAMSUNG-SM-G530AZ
Platform	Android OS
S/N	cd28ec7b
Software revision	5.1.1
Rooted	No
IMSI	N/A

Oxygen Forensic Suite: Text Messages

Messages (3752)

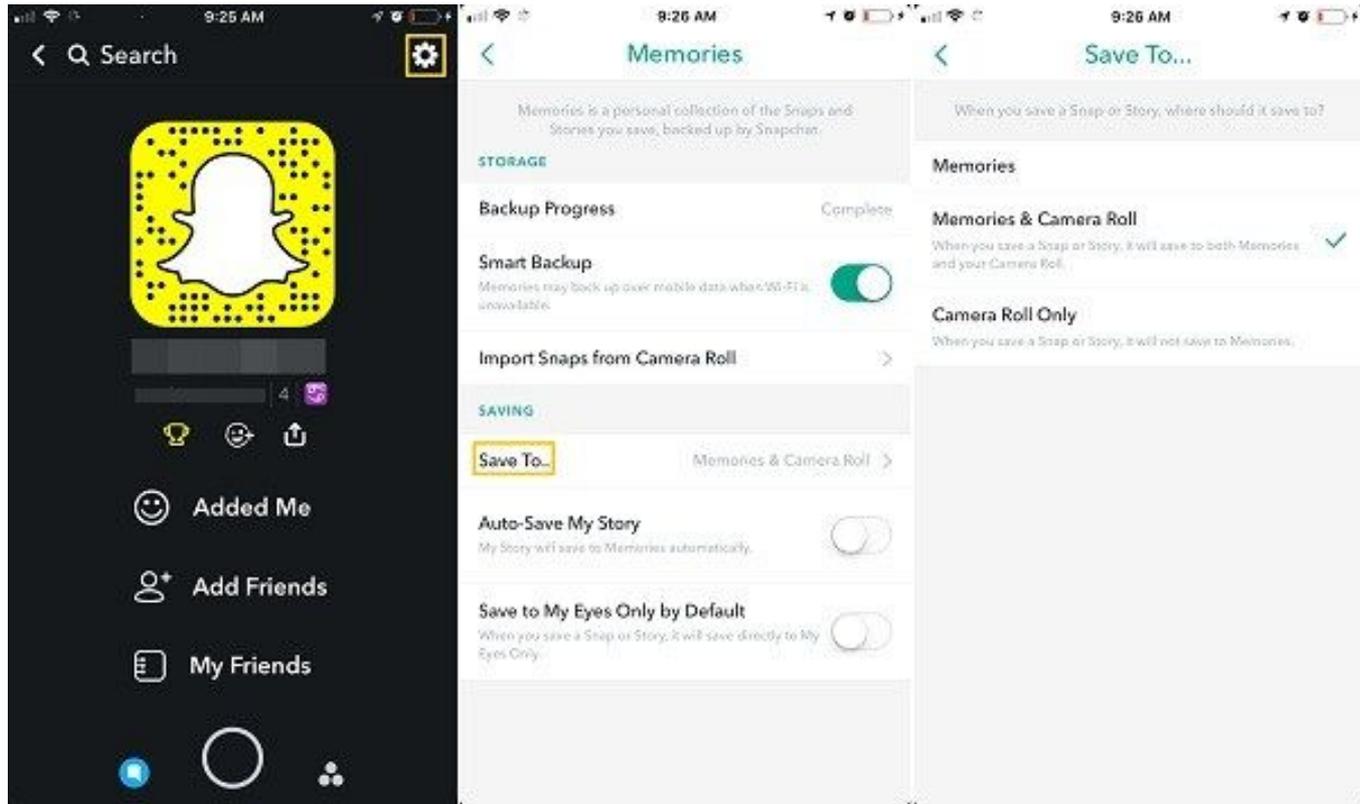
1	  SMS - Inbox SMS	
Description: I see ur trying to set me up again... U		
From: Cyndi <[REDACTED]>	Time stamp (Device time -06:00): 1/20/2019 2:50:41 AM	
To: Randall [REDACTED]		
Remote party: Cyndi <[REDACTED]>		
Direction: Incoming	Read status: Read	Deleted: No
I see ur trying to set me up again... U know ur really a monster.... PS my neck is really starting to swell and is painful		
2	  SMS - Inbox SMS	
Description: I see you're trying to set me up again..		
From: [REDACTED]	Time stamp (Device time -06:00): 1/20/2019 2:50:40 AM	
To: Randall [REDACTED]		
Remote party: [REDACTED]		
Direction: Incoming	Read status: Read	Deleted: No
I see you're trying to set me up again... U know ur really a monster		

Oxygen Forensic Suite: Incoming/Outgoing Calls

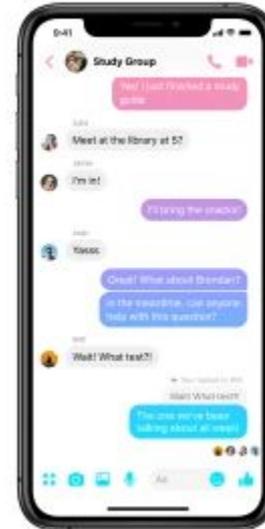
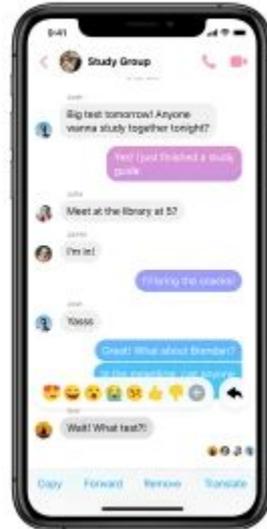
100	 Outgoing	 Voice	+16084770804 	1/18/2019 6:50:00 PM		No
		Country code: US				
101	 Outgoing	 Voice	+16084770804 	1/18/2019 6:49:27 PM	00:00:03	No
		Country code: US				
102	 Outgoing	 Voice	6088363888 6088363888	1/18/2019 6:41:43 PM	00:02:14	No
		Country code: US				
103	 Outgoing	 Voice	6088363888 6088363888	1/18/2019 6:36:54 PM	00:04:26	No
		Country code: US				
104	 Outgoing	 Voice	6084255061 6084255061	1/18/2019 10:01:51 AM		No
		Country code: US				

Social Media Apps

Social Media Apps: Snapchat



Social Media Apps: Facebook Messenger



Download Your Information

You can download a copy of your Facebook information at any time. You can download a complete copy, or you can select only the types of information and date ranges you want. You can choose to receive your information in an HTML format that is easy to view, or a JSON format, which could allow another service to more easily import it.

Downloading your information is a password-protected process that only you will have access to. Once your copy has been created, it will be available for download for a few days.

If you'd like to view your information without downloading it, you can [Access Your Information](#) at any time.

Request Copy

Available Copies

Date Range:

All of my data ▾

Format:

HTML ▾

Media Quality:

Medium ▾

Create File

Your Information ⓘ

Deselect All



Posts

Posts you've shared on Facebook, posts that are hidden from your timeline, and polls you have created



Photos and Videos

Photos and videos you've uploaded and shared



Comments

Comments you've posted on your own posts, on other people's posts or in groups you belong to



Likes and Reactions

Posts, comments and Pages you've liked or reacted to



Friends

The people you are connected to on Facebook



Stories

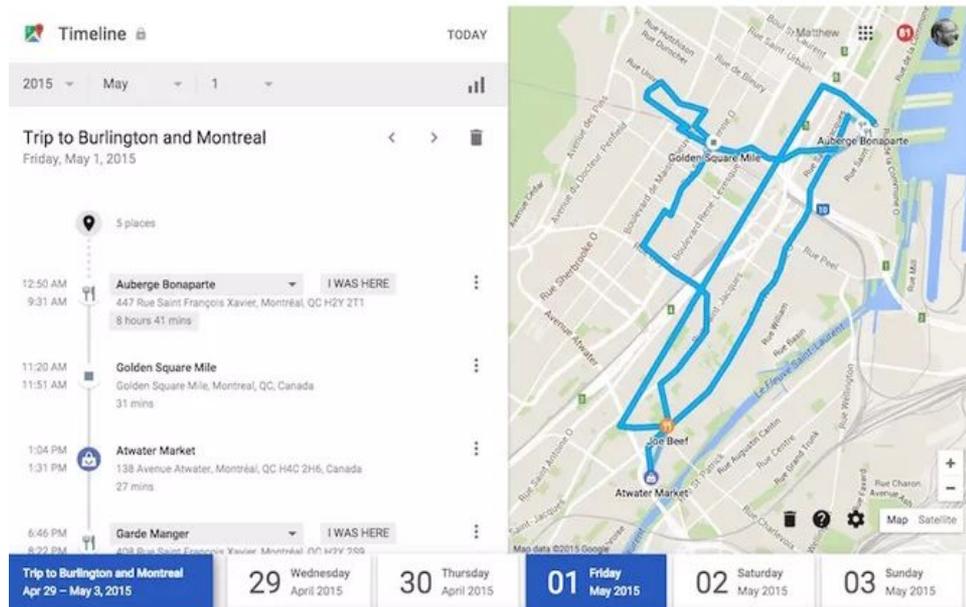
Photos and videos you've shared to your story



Google Location History

Google Location History: Establish Alibi

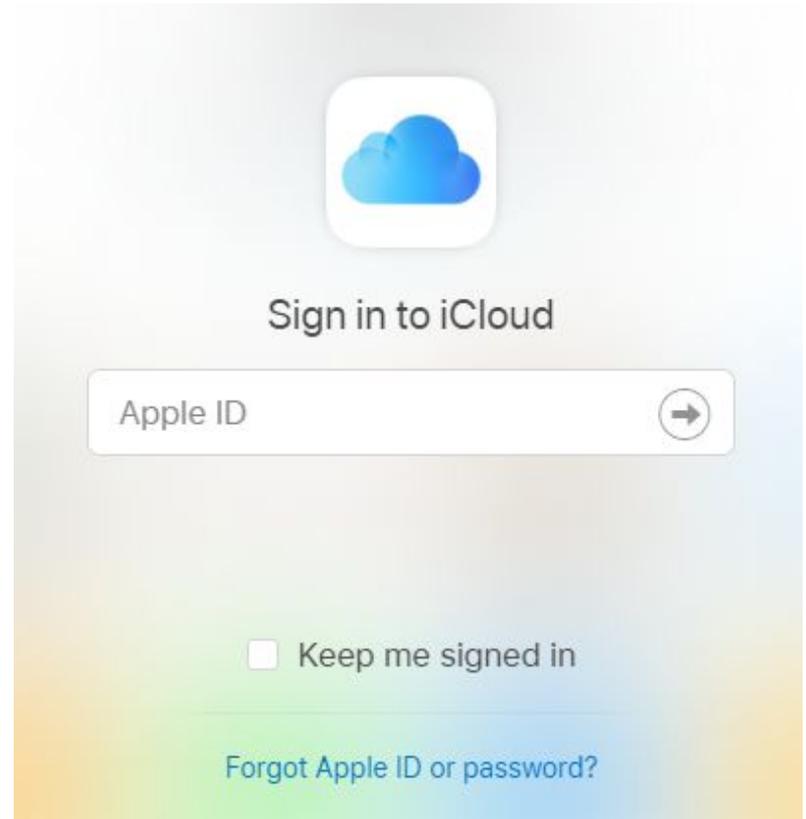
- How to view your location history in Google Maps:
 - Launch Google Maps
 - Tap the more button (three horizontal lines) on the top left corner
 - Tap your timeline
 - Tap the calendar icon to view a particular day
 - Swipe left or right to switch months
 - Tap a date to view your location history



Data Backed Up to Cloud

Cloud Data: Apple iCloud

- o Accessible from PC
- o Requires Apple ID + password
- o iMessages, SMS + MMS, Call History, Contacts, Calendars, Mail, Notes, Photos + Videos, Purchase History, Apple Watch Backup, App Data



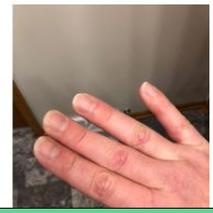
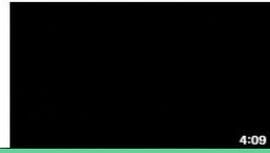
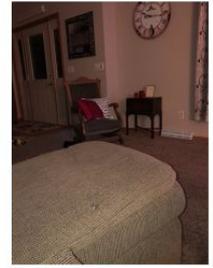
- Library
- Photos
 - Favorites
 - Hidden
 - Recently Deleted
- Albums
- Media Types
 - My Albums

October 2018

476 Items

Madison - East Side, WI Oct 12, 2018 - Crest Line Dr

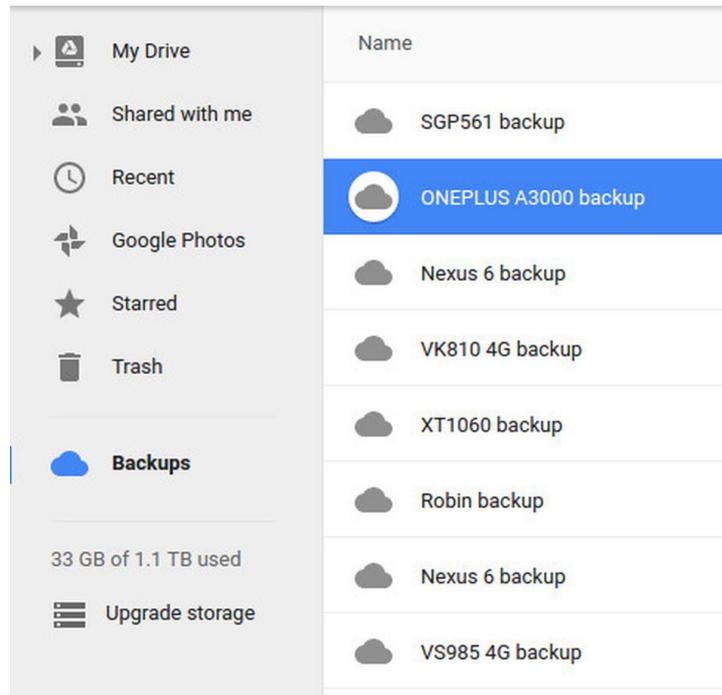
Deselect



Cloud Data: Google Drive Sync

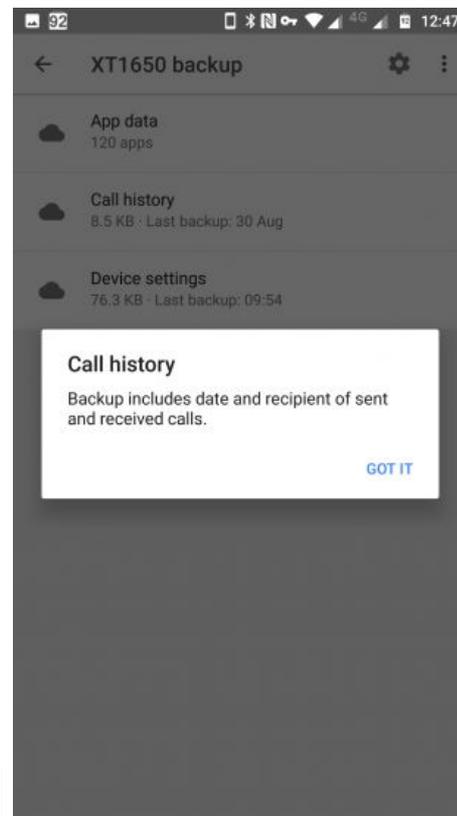
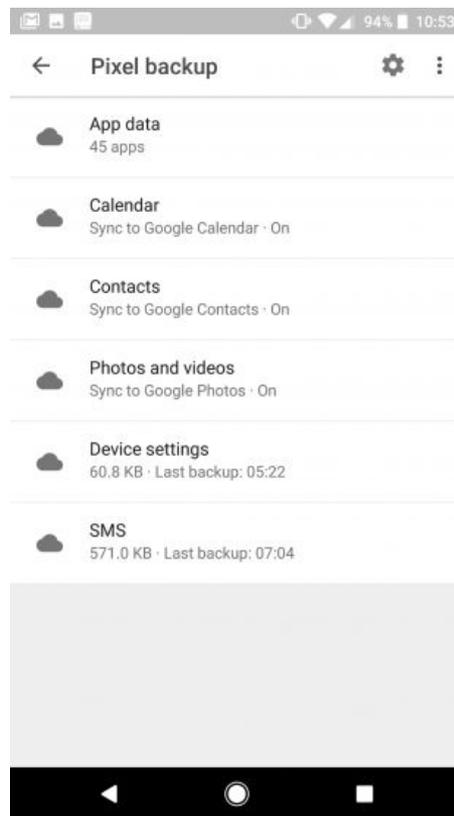
- App data, Call history, Device settings, Contacts, Calendar, Photos + Videos (Android 6.0 and up)
- SMS not backed up

1. Open the [Google Drive](#) app.
2. Tap Menu  > **Backups**.
3. Tap on the backup you want to manage.



Cloud Data: Android Backup

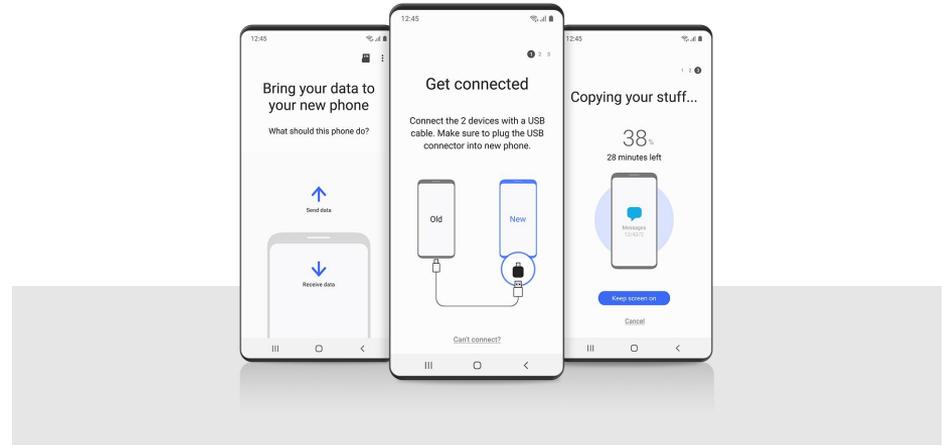
- Only on Android 6.0 and newer
- **NOT** Accessible from Google Drive on PC. Requires additional software to view data
- App data, Calendar, Contacts, Photos + Videos, Device settings, SMS (Pixel phones or Android 8.0 only), Call history (most devices)



Other Data Extraction Options

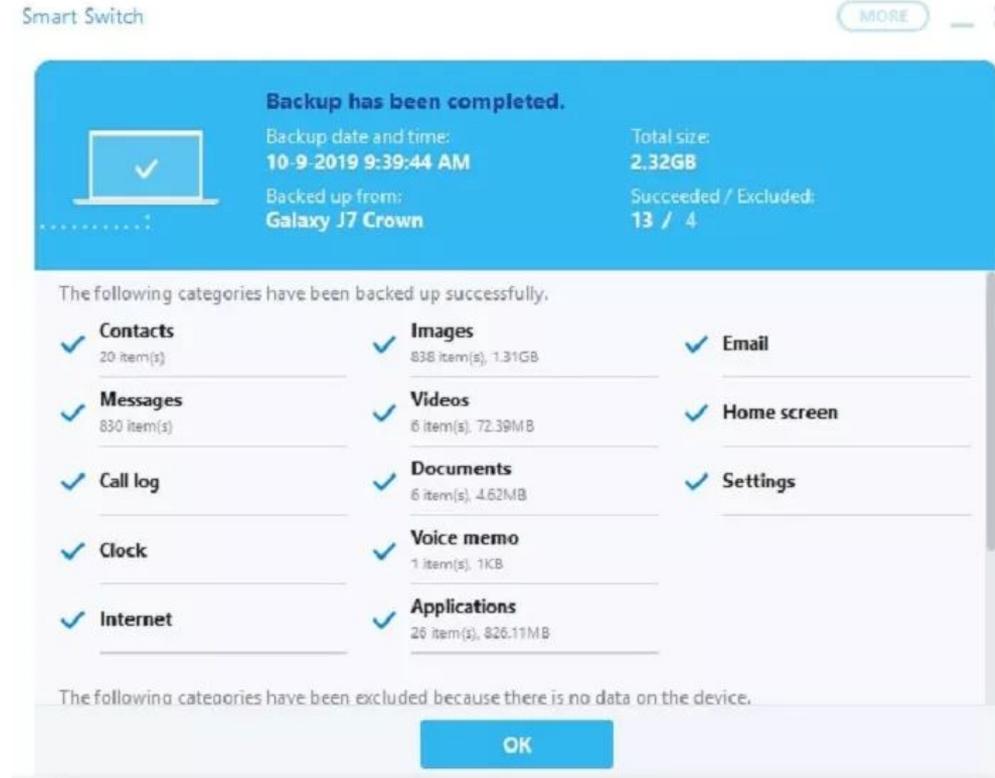
Other Options: Samsung Smart Switch to Phone

- Transfer data directly to cell phone
- Text Messages, Photos + Videos, Contacts and Call logs
- Requires a second Samsung phone



Other Options: Samsung Smart Switch to PC

- Backup data to PC
- Text Messages, Photos + Videos, Contacts and Call logs
- USB to PC



Other Options: ViaForensics

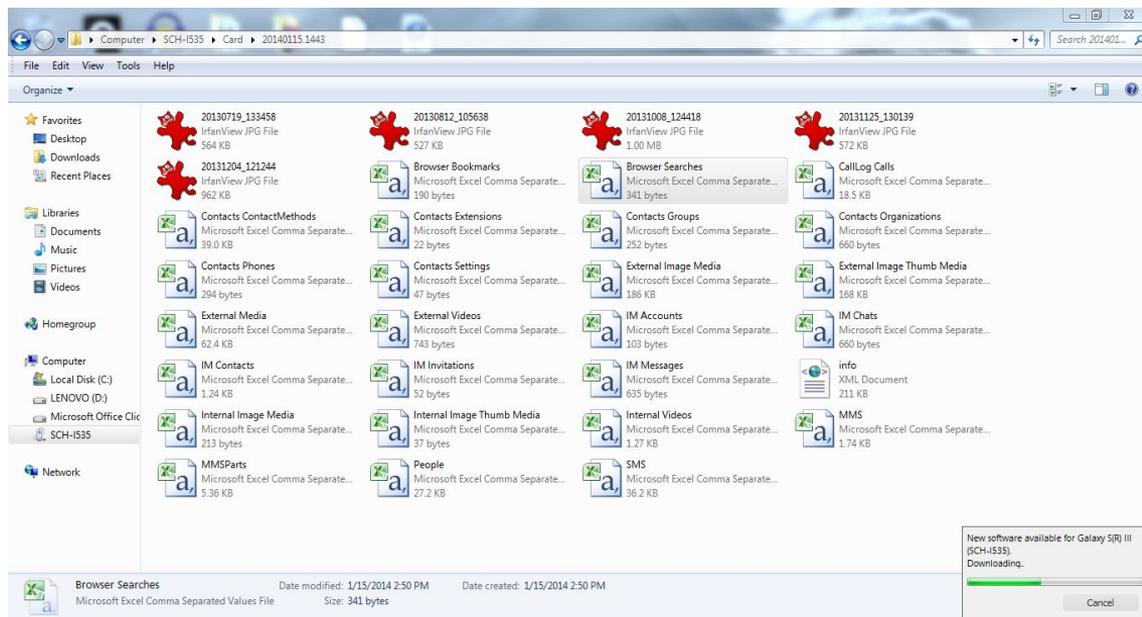
- Download + Install .apk file to target phone*

- Text Messages, Photos + Videos, Contacts and Call logs

- Download Link:

<https://drive.google.com/file/d/0BxWmHuvad7O7RUFWQVBTv1o2aXc/view?usp=sharing>

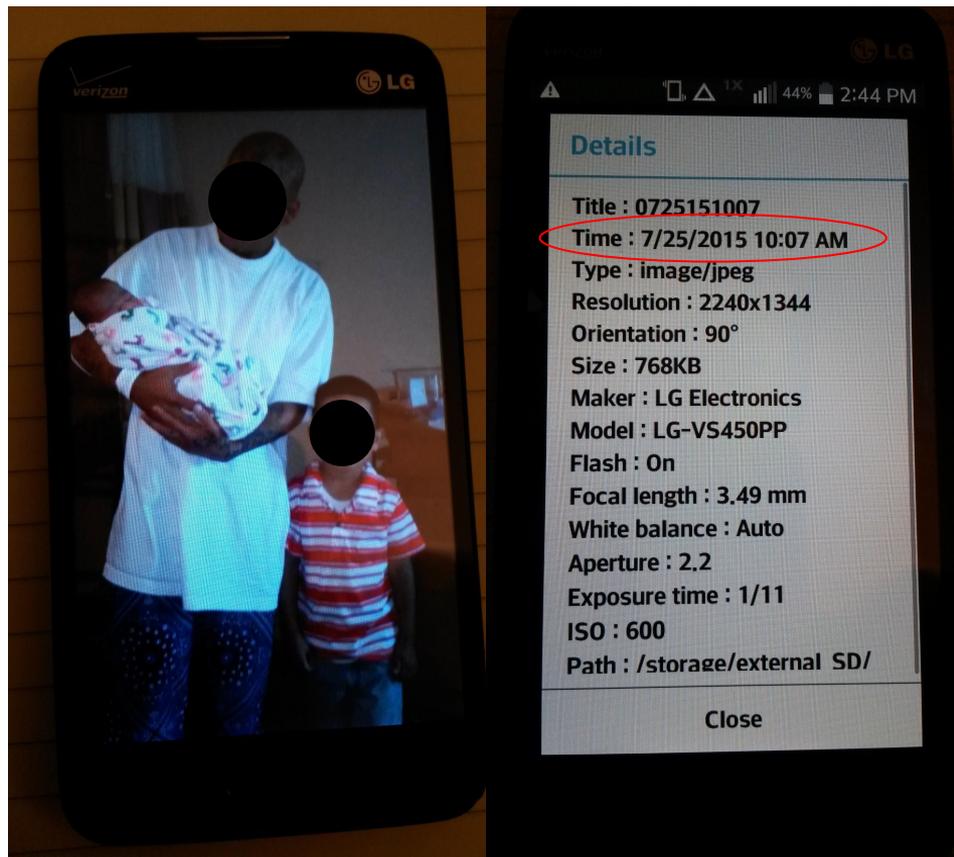
- *Does make changes to phone



Cell Phone Photos

Cell Phone Photos: Metadata

- Use data embedded in photos to establish date, time and location.
- Establish Alibi:
 - Complaining witness alleged that incident occurred on 7/25/2015 at approximately 10:00 a.m.
 - Data from client's cell phone photo shows that he was at the hospital at 10:07 a.m. on 7/25/2015 for the birth of his son.



Cell Phone Photos: Metadata

Jeffrey's Image Metadata Viewer

URL:

or...

File: No file chosen

I'm not a robot

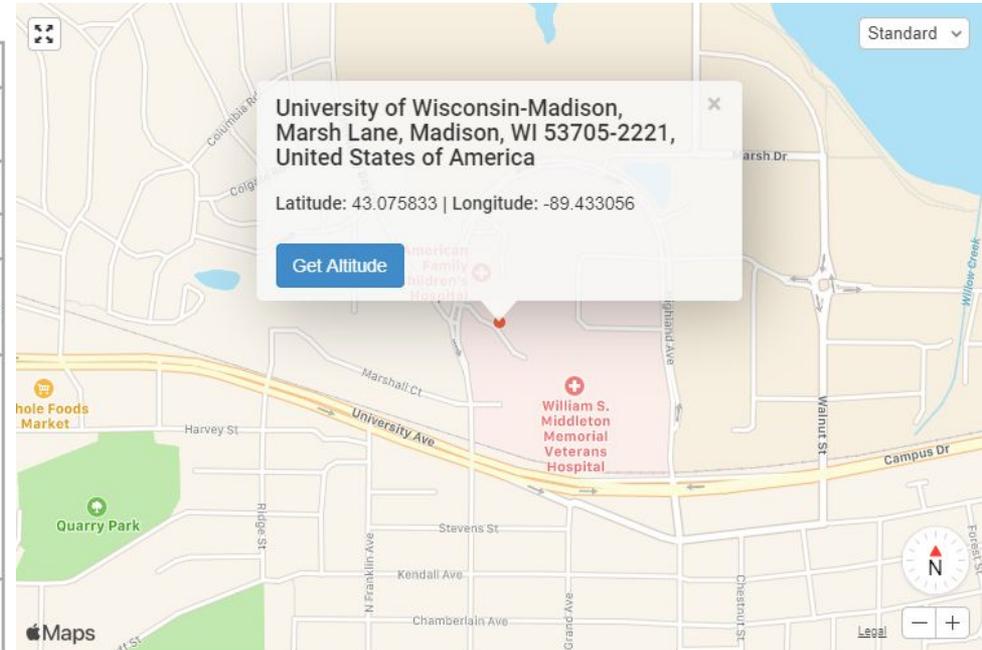

reCAPTCHA
Privacy - Terms

<http://exif.regex.info/exif.cgi>

Basic Image Information

Target file: 20170813_045435.jpg

Camera:	samsung SM-J327P
Lens:	2.4 mm (Max aperture f/2.2) (shot wide open)
Exposure:	Auto exposure, Program AE, $\frac{1}{30}$ sec, f/2.2, ISO 125
Flash:	none
Date:	August 13, 2017 4:54:35AM (timezone not specified) (2 years, 1 month, 26 days, 6 hours, 44 minutes, 45 seconds ago, assuming image timezone of 6 hours behind GMT)
Location:	Latitude/longitude: 43° 4' 33" North, 89° 25' 59" West (43.075833, -89.433056)
	Map via embedded coordinates at: Google , Yahoo , WikiMapia , OpenStreetMap , Bing (also see the Google Maps pane below)
	Timezone guess from earthtools.org: 6 hours behind GMT
File:	1,616 × 1,212 JPEG (2.0 megapixels) 498,768 bytes (487 kilobytes)



(<https://www.gps-coordinates.net/>)



Target file: IMG_1044.JPEG

Camera:	Apple iPhone 8 Plus
Lens:	iPhone 8 Plus back dual camera 3.99mm f/1.8 Shot at 4 mm
Exposure:	Auto exposure, Program AE, 1/17 sec, f/1.8, ISO 40
Flash:	Auto, Did not fire
Date:	October 12, 2018 10:27:32PM (timezone not specified) (11 months, 27 days, 10 hours, 17 minutes, 3 seconds ago, assuming image timezone of 6 hours behind GMT)
Location:	Latitude/longitude: 43° 7' 58.3" North, 89° 18' 44.7" West (43.132861, -89.312417) Map via embedded coordinates at: Google , Yahoo , WikiMapia , OpenStreetMap , Bing (also see the Google Maps pane below)
	Altitude: 283 meters (928 feet) Camera Pointing: Northwest Timezone guess from earthtools.org: 6 hours behind GMT
File:	1,536 × 2,048 JPEG (3.1 megapixels) 481,183 bytes (470 kilobytes)



43°07'58.3"N 89°18'44.7"W

43.132861, -89.312417



Directions



Save



Nearby



Send to your
phone



Share



2606 Crest Line Dr, Madison, WI 53704



4MMQ+42 Madison, Wisconsin



Add a missing place

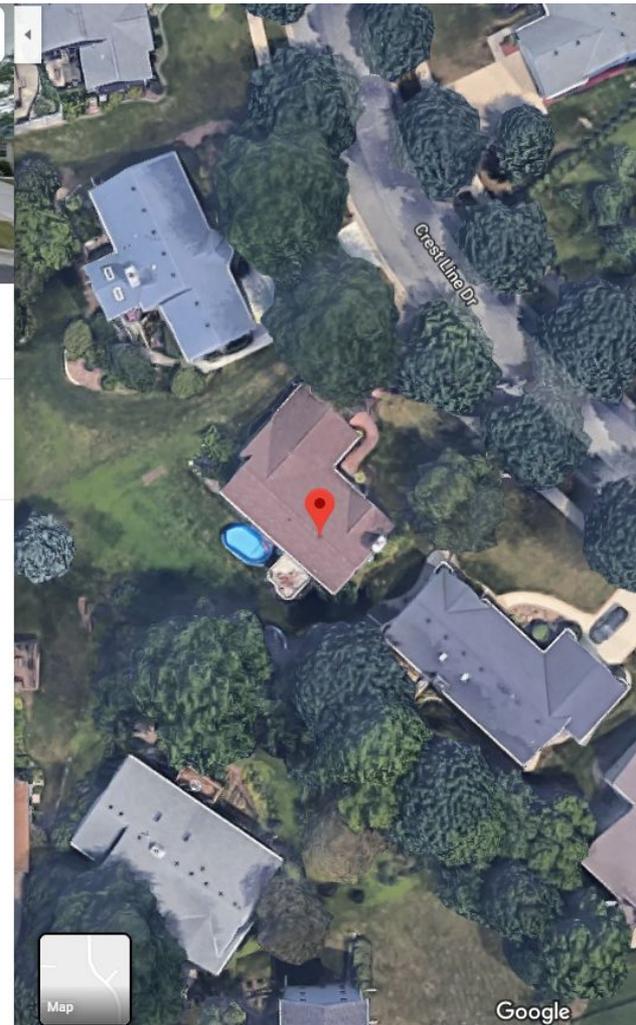


Add your business



Add a label

Photos



Reading Cell Phone Extraction Reports

Reading Cell Phone Extraction Reports

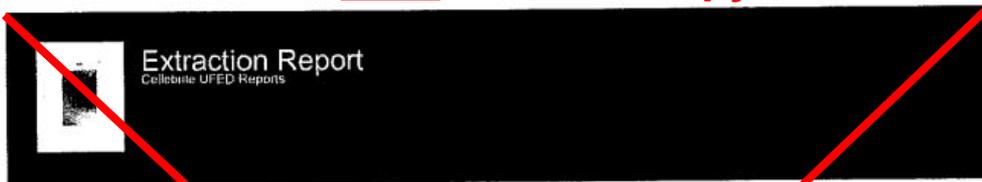
- Always request full Cellebrite extraction report
- Always request all Cellebrite extracted files + .ufdr (UFED) file
- Download UFED Reader to load + analyze data extraction (.ufdr file)
- [Download link](#)

Name	Date modified	Type	Size
AccountPackage	10/17/2018 10:04 ...	File folder	
chats	10/17/2018 10:04 ...	File folder	
files	10/17/2018 10:25 ...	File folder	
 fp18-0003357_McInnis	3/20/2018 2:31 PM	Adobe Acrobat D...	25,431 KB
 fp18-0003357_McInnis.ufdr	3/20/2018 2:30 PM	UFDR File	1,028,335 KB
 UFEDReader	1/23/2018 6:19 PM	Application	221,305 KB

LG > LG CDMA_US375 K8

Name	Date modified
AccountPackage	2/16/2018 10:59 AM
chats	2/16/2018 10:39 AM
contacts	2/16/2018 10:39 AM
email	2/16/2018 10:40 AM
files	2/16/2018 10:38 AM
gps	2/16/2018 10:53 AM
resources	2/16/2018 10:53 AM
thumbnails	2/16/2018 10:39 AM
 FP18-0001752	2/16/2018 10:58 AM
 UFEDReader	1/23/2018 6:19 PM

NOT scanned copy



- o Full digital Cellebrite extraction report (PDF w/links)

644	Name: IMG_0532.JPG Path: Joshua's iPhone/var/mobile/Media/DCIM/100APPLE/IMG_0532.JPG MD5: 6a540dccb8bd1b0ab0872ddd456689c2	Size (bytes): 101122 Created: 3/10/2018 9:43:08 AM(UTC-6) Modified: 3/10/2018 9:43:08 AM(UTC-6) Deleted: 3/12/2018 2:08:38 PM(UTC-5) <u>Meta Data:</u> Camera Make: Apple Camera Model: iPhone 8 Capture Time: 3/10/2018 9:43:08 AM Pixel resolution: 1024x576 Resolution: 72x72 (Unit: Inch) Orientation: Rotate 90 CW
645	Name: IMG_0533.JPG Path: Joshua's iPhone/var/mobile/Media/DCIM/100APPLE/IMG_0533.JPG MD5: 47a4552ece96e5caa3e1c1eee2bb056d	Size (bytes): 104825 Created: 3/10/2018 9:43:16 AM(UTC-6) Modified: 3/10/2018 9:43:16 AM(UTC-6) Deleted: 3/12/2018 2:08:38 PM(UTC-5) <u>Meta Data:</u> Camera Make: Apple Camera Model: iPhone 8 Capture Time: 3/10/2018 9:43:16 AM Pixel resolution: 1024x576 Resolution: 72x72 (Unit: Inch) Orientation: Rotate 90 CW

Timeline (458)

#	Type	Direction	Attachment	Location	Timestamp	Party	Description	Deleted
1	Chats				6/15/2017 6:32:16 PM(UTC-5)	[REDACTED]	Facebook messenger	
2	Instant Messages	Outgoing			6/15/2017 8:32:45 PM(UTC-5)	From: 100013464152668 [REDACTED]	For you homie If I don't get this back I'm obviously not a close friend. Now, I have a game for you, it's been played since 1977. Once you read this, you have to send it to 15 people, Your next 5 days will be like this: Day 1 - you will wake up to the biggest shock of your life. Day 2 - you will cross paths with an old friend you have missed. Day 3 - you will find yourself with a lot of money. Day 4 - your day will be perfect. Day 5 - the love of your life will kiss you. Don't break this. Send it to 14 friends in 10 minutes. It's not that hard. Whoever sent this to you must care about you. Don't know how to send it? Lol. Just hold your finger on it and it should go forward.	
3	Chats				7/15/2017 3:19:00 PM(UTC-5)	[REDACTED]	Facebook messenger	
4	Chats				8/28/2017 5:41:28 PM(UTC-5)	[REDACTED]	Facebook messenger	
5	Chats				8/28/2017 10:28:40 PM(UTC-5)	[REDACTED]	Facebook messenger	

Date: September 8, 2015

To: City of Madison Police Department - Records Division

From: Philip Mergen, SPD Investigator

Subject: [REDACTED] - MPD Incident #15-[REDACTED]

I would like to please request a digital copy of the UFED Physical Analyzer report referenced in Inv. B. Shaul's supplemental police report.

Reading Cell Phone Extraction Reports

- Emails
- Facebook Messenger
- GPS data

LG > LG CDMA_US375 K8 > email > [REDACTED]@gmail.com

Name	Date modified
Drafts	2/16/2018 10:39 AM
Inbox	2/16/2018 10:39 AM
Inbox,	2/16/2018 10:39 AM
Inbox, Starred	2/16/2018 10:39 AM
Native	2/16/2018 10:39 AM
Starred, Drafts	2/16/2018 10:39 AM
Starred, Inbox	2/16/2018 10:39 AM
Trash	

LOCATION (H:) > LG > LG CDMA_US375 K8 > gps

Name	Date modified
house	2/16/2018 10:53 AM
jquery-min	2/16/2018 10:53 AM
location_pin	2/16/2018 10:53 AM
locations	2/16/2018 10:53 AM
locations.kml	2/16/2018 10:53 AM
map	2/16/2018 10:53 AM
minus	2/16/2018 10:53 AM
plus	2/16/2018 10:53 AM

LG > LG CDMA_US375 K8 > chats > Facebook messenger

Name	Date modified
attachments1	2/16/2018 10:39 AM
attachments6	2/16/2018 10:39 AM
attachments15	2/16/2018 10:39 AM
attachments18	2/16/2018 10:39 AM
attachments31	2/16/2018 10:39 AM
attachments36	2/16/2018 10:39 AM
attachments37	2/16/2018 10:39 AM

Cell Tower Plotting

Cell Tower Plotting

- o Mapping historical data from a user's cell phone records
- o Cell phone records are acquired from user's cell phone company via subpoena
- o Use interactive Google Map designed by Will Mattered to map cell phone towers, crime scene location and alibi location: <http://www.celltowerplotter.com/>

Cell Tower Plotting: Requesting Records

In addition to the standard language used in cell phone records subpoenas (subscriber information, incoming/outgoing call + text detail, etc...), request the following:

1. All available call detail record (CDR) data in Lat/Long coordinates with physical address.
2. All available cell identification (CID) data, including switch, repoll, system ID, azimuth of each sector.
3. All available round-trip delay (RTD) data.
4. Tower coverage map (Propagation map).
5. All current U.S. market cell carrier tower sites and identifiers in Microsoft Excel format with Lat/Long, physical address and azimuth information.



Wisconsin State Public Defender

107 3rd St.

Baraboo, WI 53913

Office Number: 608-355-3180 / Fax Number: 608-355-3190

www.wisspd.org

Serving Sauk, Columbia, Juneau and Marquette Counties

Kelli S. Thompson

State Public Defender

Catherine Dori

Trial Division Director

Catherine Ankenbrandt

Attorney Manager

STAFF ATTORNEYS

Mark J. Gumz
Randall M. Holtz
M. Peter Middleton, II
Liz Mitchel
Debra V. O'Rourke
Amanda K. Riek
Thomas L. Steinman

CLIENT SERVICES SPECIALIST

Colleen Hunt

INVESTIGATOR

Shannon Holmes

6/12/2017

RE: Cell Phone Number - Requester's Case -

Our requested period of time is between and .

Requested Information:

- Subscriber information
- Incoming and outgoing calls
- Incoming and outgoing text messages
- Data regarding identity of each person/agency that made inquiry into subscriber's account
- All available data regarding the "Ported" history of subscriber cell number
- All Cellular Carrier Tower data including:
 - All available call detail record (CDR) data in Lat/Long coordinates with physical address
 - All available Cell Identification (CID) data including Switch, Repoll, System ID, azimuth of each sector
 - All available Round-Trip Delay (RTD) data
 - Tower Coverage Map (Propagation Map)
- All current U.S. market cell carrier tower sites and identifiers, in Microsoft Excel format, with all Lat/Long and physical address and azimuth information

Please forward information to our office via email: or mail the information to:

Thank you for your anticipated cooperation into this matter.

Cell Tower Plotting: Reading Records

When reading the information received from the cell phone provider, you must know what each column of the spreadsheet refers to. The information you need is:

1. Tower Location (Latitude, Longitude)
2. Sector Used
3. Tower Name

Cell Tower Plotting: Reading Records

[Sprint](#)

[T-Mobile](#)

[T-Mobile Metro PCS](#)

[TracFone](#)

[US Cellular](#)

[US Cellular-NORTEL Towers](#)

[Verizon Phone Calls](#)

[Verizon Text Messages](#)

[Verizon Cell Sites](#)

[Verizon VOLTE](#)

Downloadable Tower Maps for Google Maps:

[Sprint \(.kml\)](#)

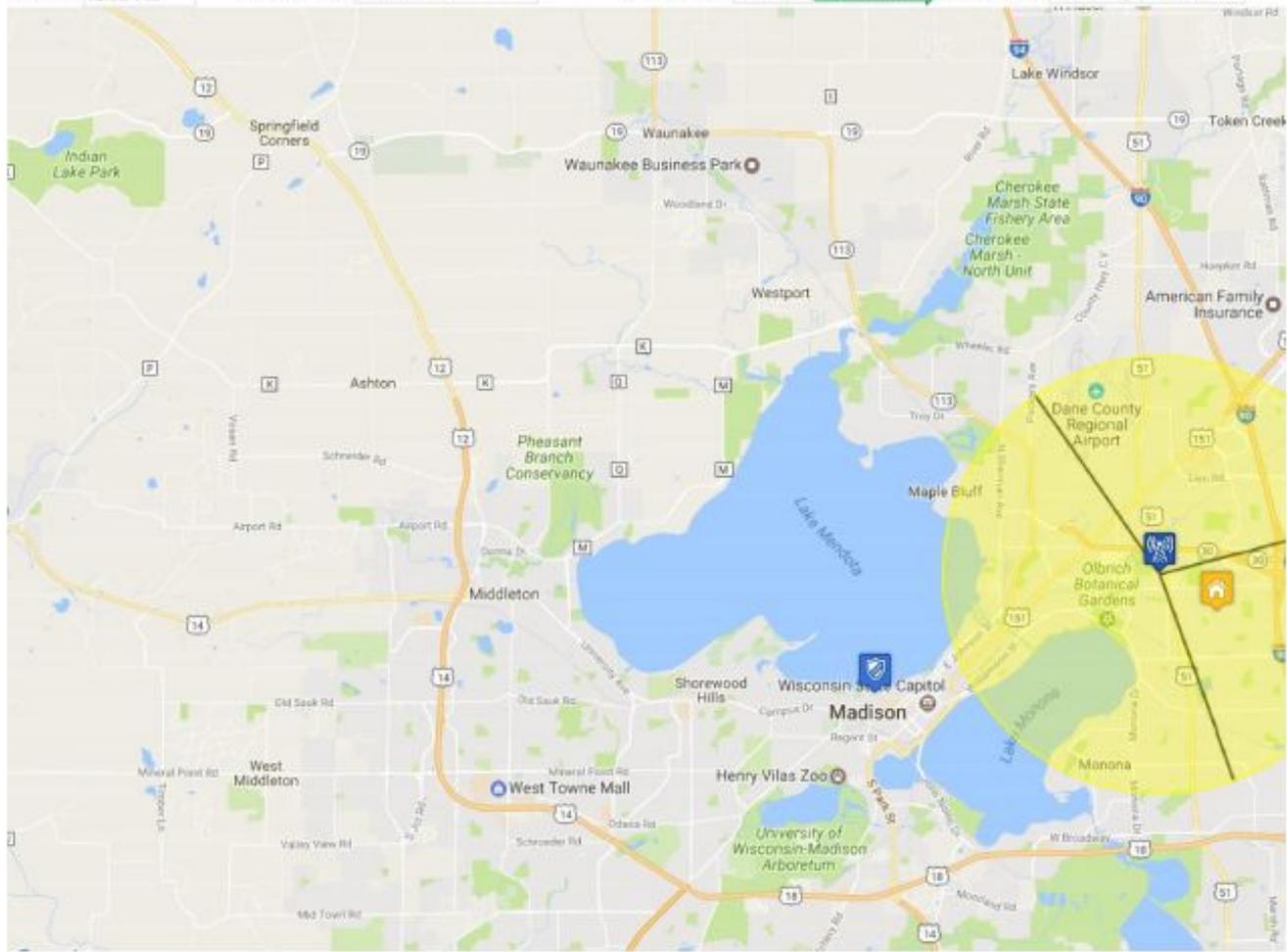
[Sprint \(.kmz\)](#)

[US Cellular \(.kml\)](#) [US Cellular \(.kmz\)](#)

Tower Name: Tower XYZ Sector Angles: 75 160 325 Sector Used: 2 Tower Location: 43.101129, -89.318488
Call Time: 12:56 PM Called Number: 608-261-7981 Alibi Location: 43.093203, -89.300003 Crime Location: 43.076297, -89.399277

How do we use it?

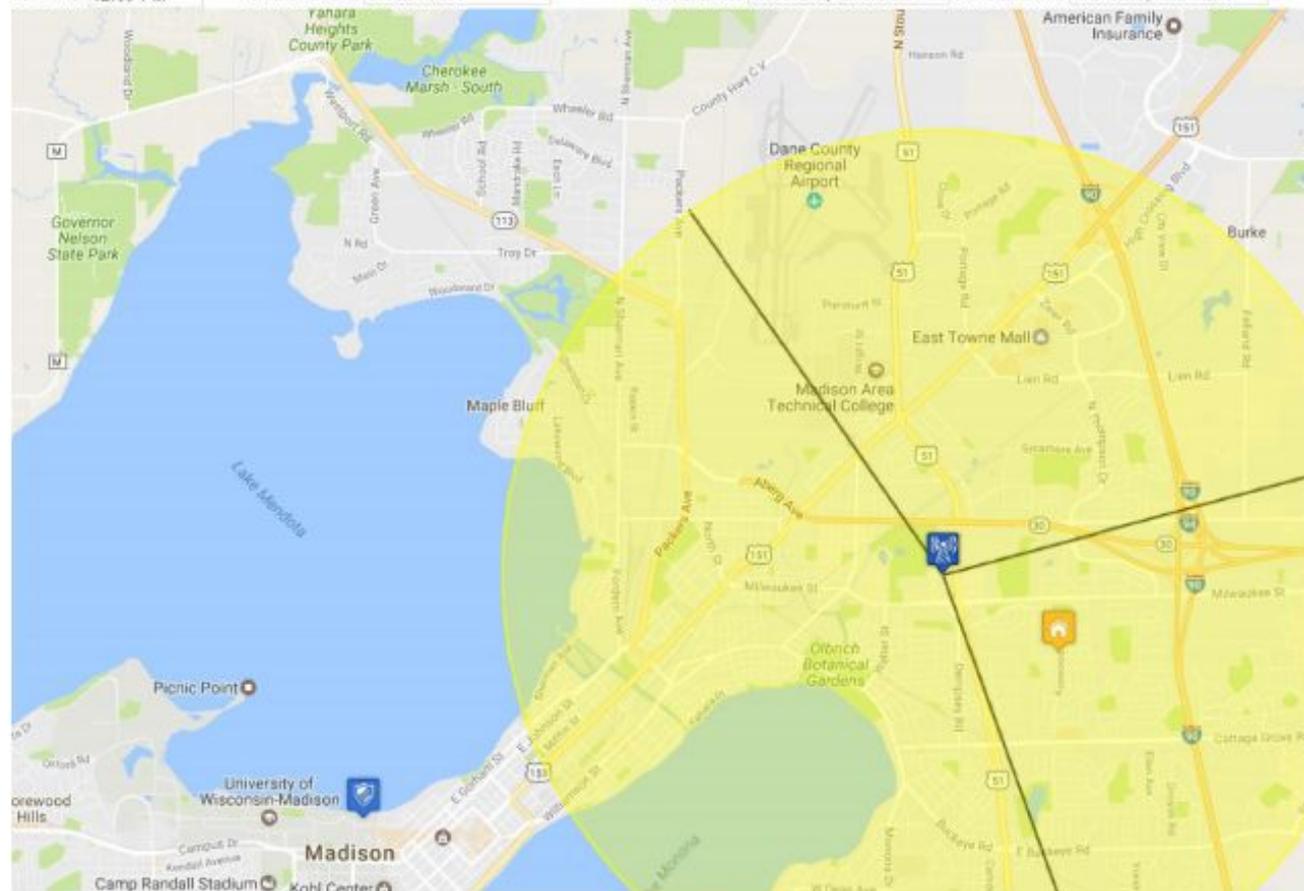
- Input the tower name
- Input sectors
- Input sector used
- Input tower location
- Input call time and called number
- Input alibi location
- Input crime scene location



How do we use it?

- You can now pan and zoom the map
- Show that phone was being used on far east side of Madison and the crime scene was near the Madison Memorial Union

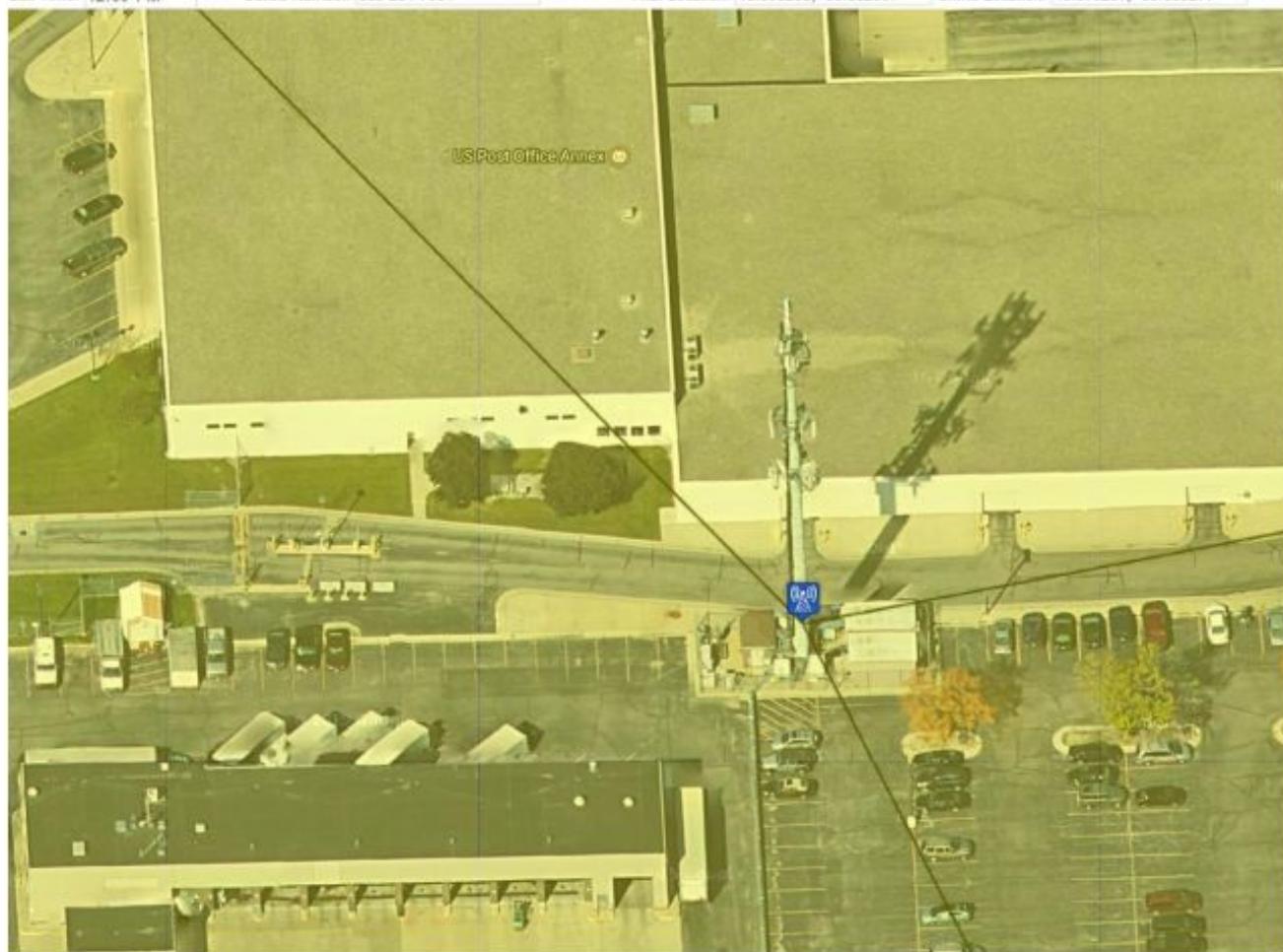
Tower Name: Tower XYZ Sector Angles: 75 160 325 Sector Used: 2 Tower Location: 43.101129, -89.318488
Call Time: 12:56 PM Called Number: 608-261-7981 Alibi Location: 43.093203, -89.302397 Crime Location: 43.076297, -89.399277



Tower Name: Tower XYZ Sector Angles: 75 160 325 Sector Used: 2 Tower Location: 43.101129, -89.318488
Call Time: 12:56 PM Called Number: 608-261-7981 Alibi Location: 43.093203, -89.302397 Crime Location: 43.076297, -89.399277

How do we use it?

- The best part, you can zoom in on the tower to show the accuracy of your plotted cell tower and visually see it



Questions?

Philip J. Mergen

State Public Defender Investigator

17 S. Fairchild St., Second Floor

Madison, WI 53703

(608) 267-1762 office

(608) 301-7669 cell

mergenp@opd.wi.gov / <https://www.linkedin.com/in/philipmergen/>