Cellphone Forensics:
Applications in Discovery and Investigations

Fred Behning, EnCE
Director of Digital Forensics

State Bar of Texas
Sponsor Number A15272

Califorensics
a division of Capitol Digital

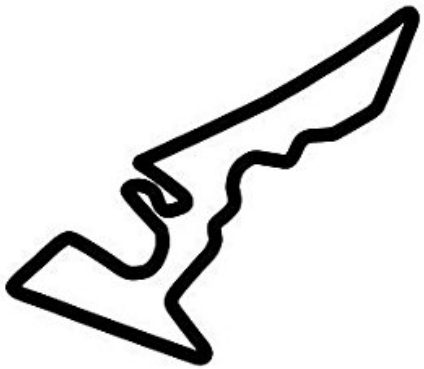
100 Congress Ave, Suite 2000
Austin, TX 78701
fbehning@califorensics.com
(855) 839-9084

FRED BEHNING

- BS Forensic Science – Baylor University
- Over 12 years experience in Digital Forensics
- EnCase Certified Examiner
- Mobile Phone Seizure Certified – BK Forensics
- Licensed Texas Private Investigator

- High Technology Crime Investigation Association Member

- Testified in Texas Civil Court – Harris County



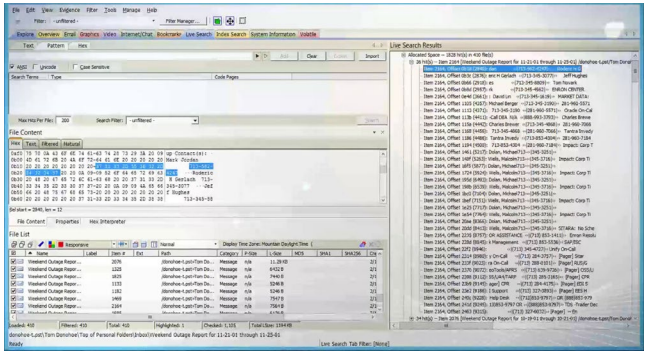
Californics
a division of Capitol Digital

AGENDA

- BACKGROUND
  - What is Digital Forensics
  - Why Do We Need It
- MOBILE FORENSICS
  - Mobile Technology
  - The Internet of Things
  - When Do We Need Mobile Forensics
- TYPICAL CASES
  - Criminal Defense Cases
  - Plaintiff Cases
  - Inappropriate Use of Work Devices
  - Sexual Harassment in the Workplace
  - Theft of Intellectual Property
- THE FORENSIC PROCESS
  - Collection
  - The Importance of Cellphone Preservation
  - Extraction Types
  - Data Types
  - Communications
  - Images
  - Location Data
- PRIVACY ISSUES
  - Reasons for Resistance
  - Location Data
- DIGGING DEEPER
- THE FUTURE
  - Forensic Traces
  - 'Cloudentity'


BACKGROUND

WHAT IS DIGITAL FORENSICS?



WHY DO WE NEED IT?

Evidence Preservation

- Prevent loss of data
- Maintain integrity of evidence

Detailed Analysis

- Find user activity
- Recover deleted files
- Search for relevant evidence

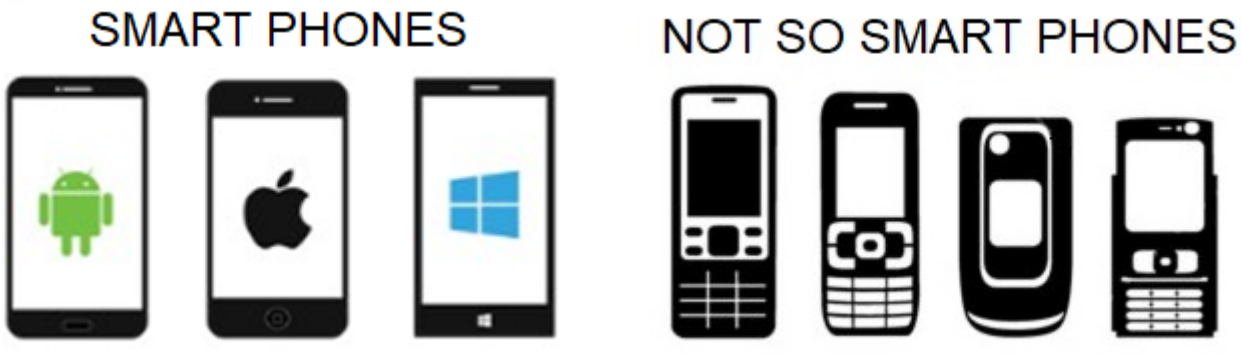
Production of Results

- Produce written report
- Review relevant documents
- Court testimony
- Explaining complex concepts to the court (e.g. Snapchat, etc.)

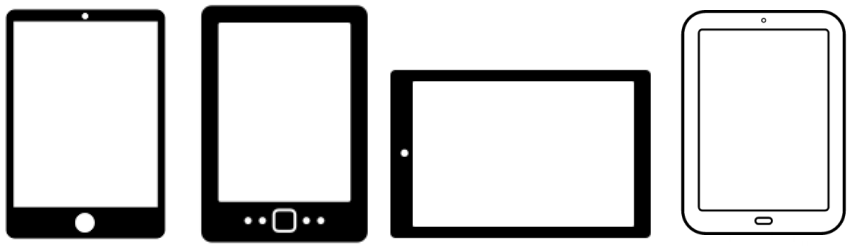

MOBILE FORENSICS

MOBILE FORENSICS: MOBILE TECHNOLOGY

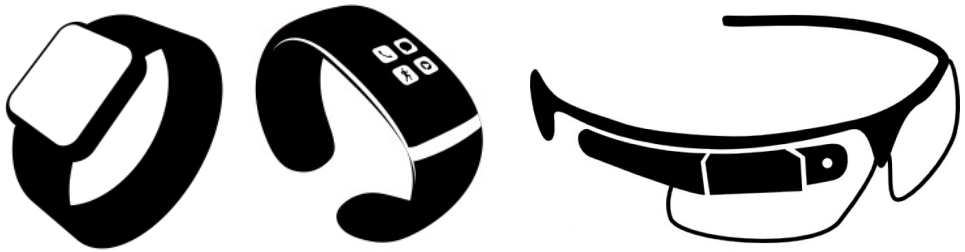
Cellphones:



Tablets:



Wearables:



MOBILE FORENSICS: THE INTERNET OF THINGS

Additional devices thanks in part to the rise of the Echo.

- Thermostats
- Light Bulbs
- Crockpots
- Garage Door Opener
- Door Locks
- Refrigerator
- Camera Systems
- Beds

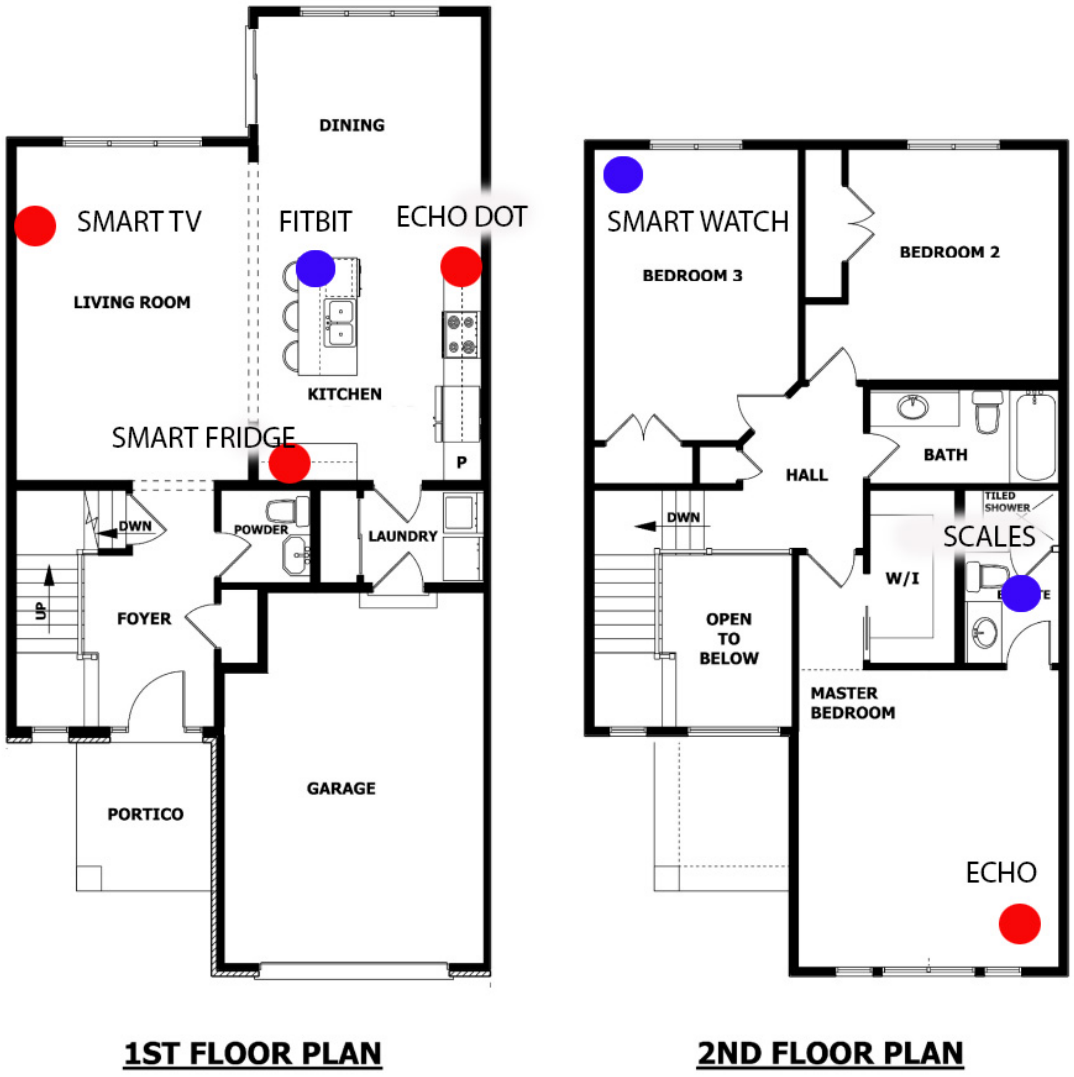
FORENSIC TRACES

Imagine a domestic homicide.

Did the spouse turn on the lights when he entered the house?

How did they behave after discovering the victim?

Did they run the water for a long time?

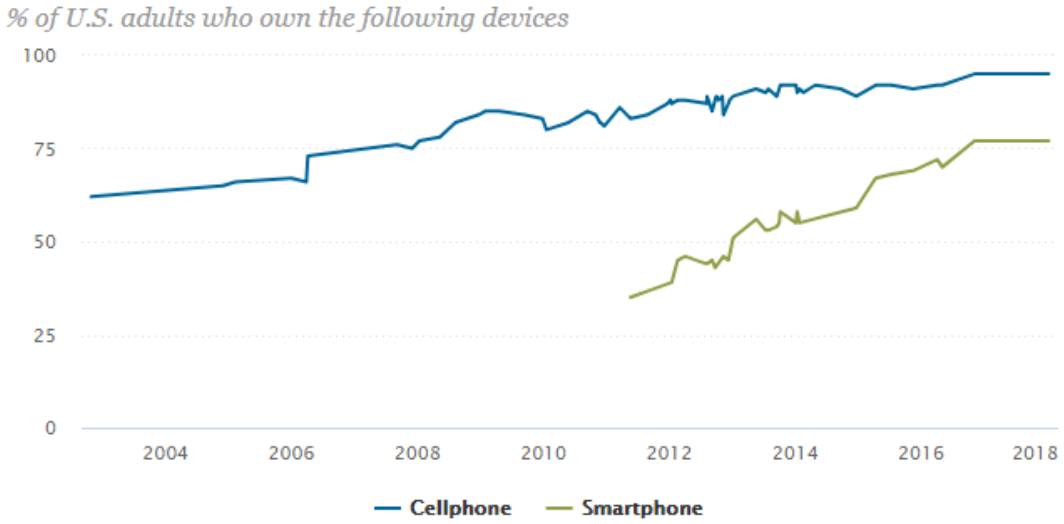


1ST FLOOR PLAN

2ND FLOOR PLAN

WHEN DO WE NEED MOBILE FORENSICS?

What types of cases need mobile forensics?



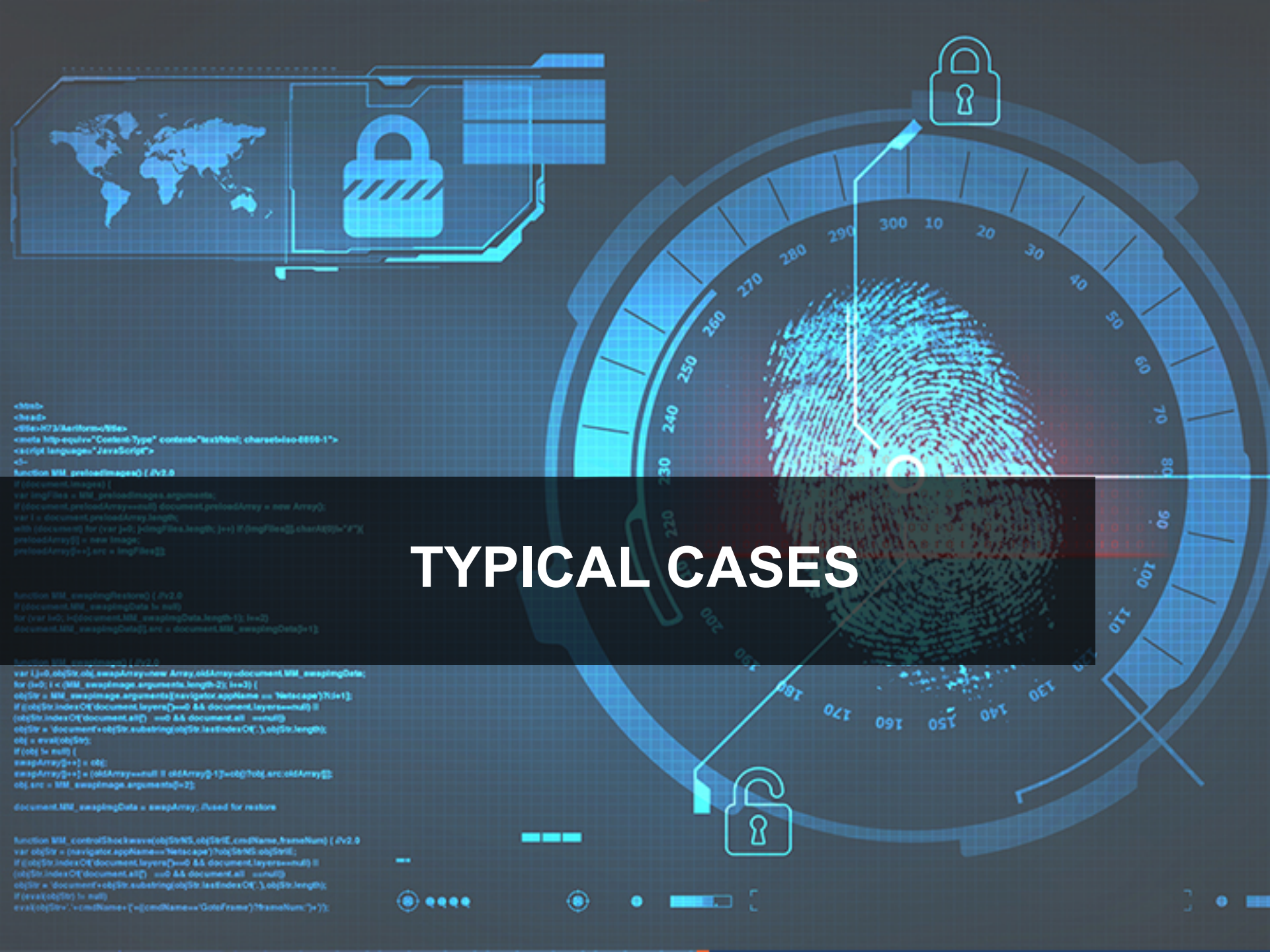
Cellphone ownership > 95%

77% own Smart Phones

Source: http://www.pewinternet.org/fact-sheet/mobile/

Most common types of mobile forensics cases:

- Criminal defense cases
- Intellectual property theft cases
- Family Law/Divorce
- Sexual harassment in the workplace

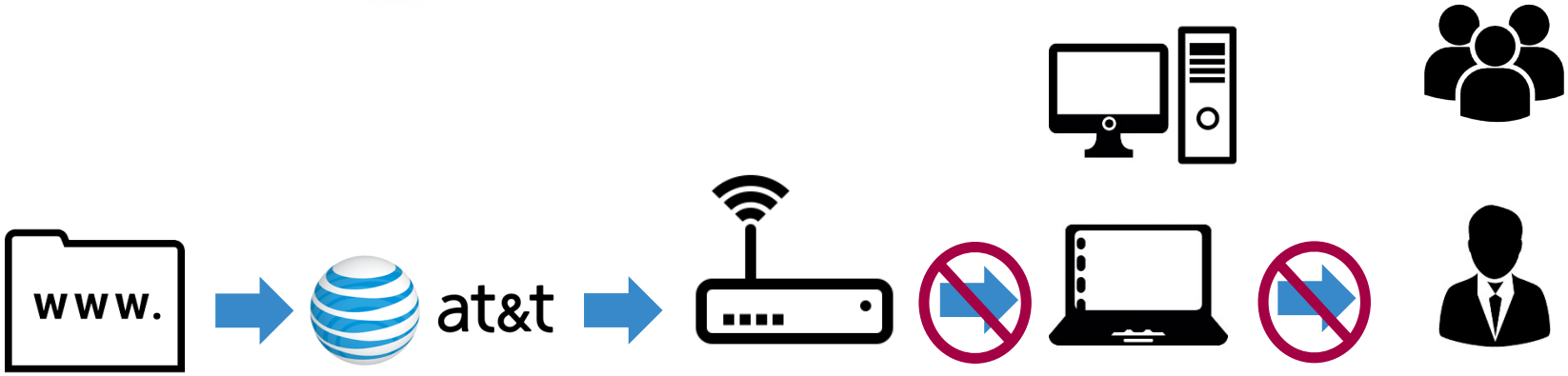

TYPICAL CASES

CRIMINAL DEFENSE – DISCOVERY REVIEW

HOW DID LAW ENFORCEMENT COME TO KNOCK ON YOUR CLIENT'S DOOR ?

Example:

"We subpoenaed AT&T and they confirmed that the IP address used to access this site belonged to your client."



- Router logs may have key data
- Volatile- May be overwritten
- Unlikely to be taken in a search warrant

CIVIL IP THEFT – FINDING SUPPORTING EVIDENCE

KEY EMPLOYEE LEAVES, STARTS COMPETING COMPANY – POSSIBLE IP THEFT

Where to start?

Preserve everything!

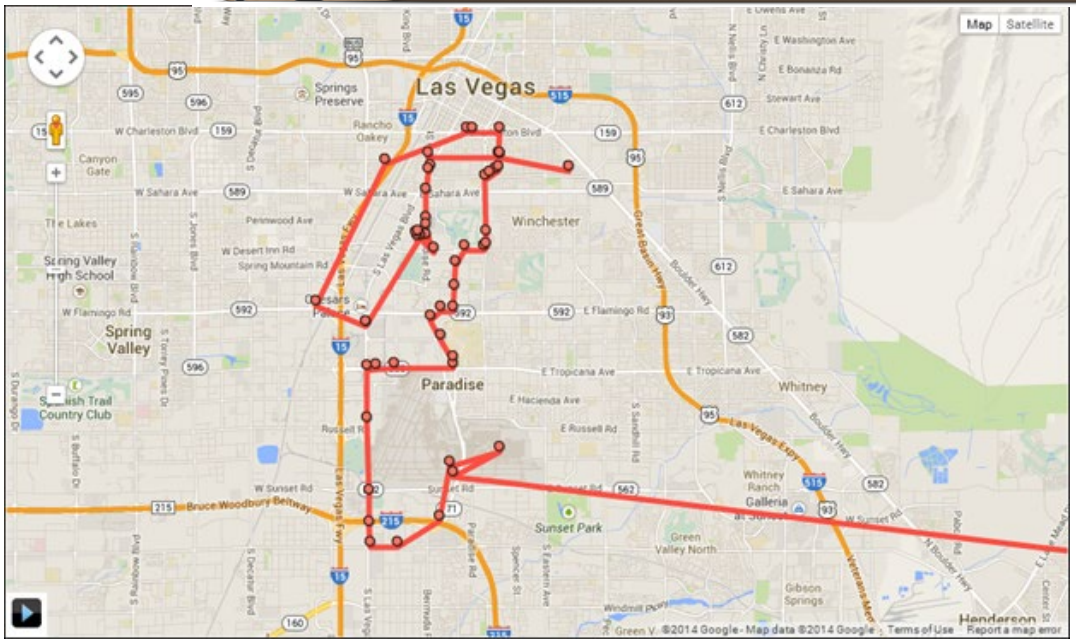
- Laptop, mobile devices, email, cloud storage
- Issue preservation notices
- Request images of relevant devices not owned by the Plaintiff

Computer Artifacts	Mobile Device Artifacts
USB Logs	Text Messages
Lnk Files	Location Tags
Registry Entries	Chat Applications
ShellBags	Email
Deleted Files	Cloud Applications
Volume Shadow Copies	Pictures/Screen Shots

Family Law

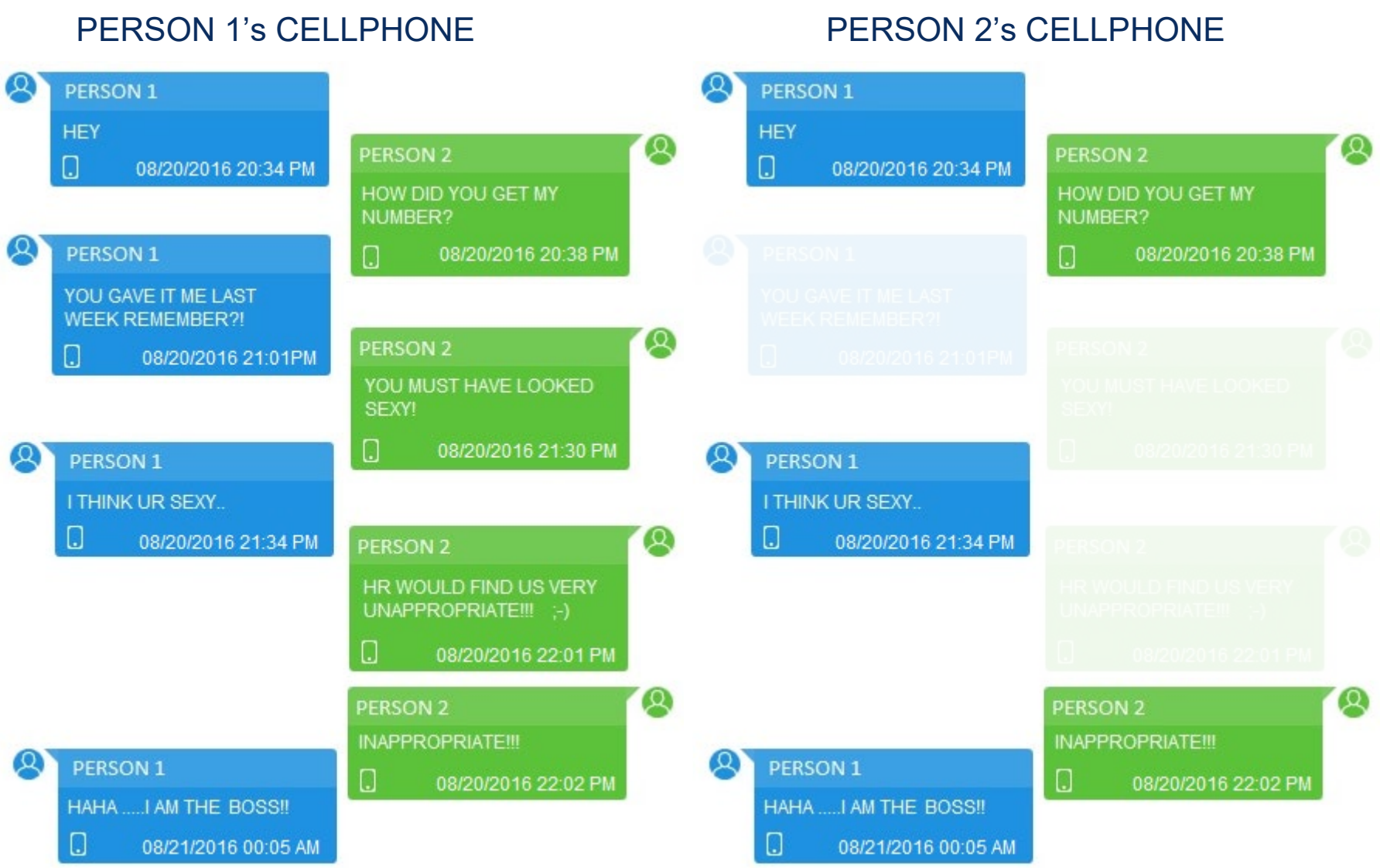
Divorce

- Custody disputes
- Harassment
- Illicit Images
- Spouse tracking
- Mobile banking records
- Facetime logs
- Social media



Californics
a division of Capitol Digital

SEXUAL HARASSMENT IN THE WORKPLACE




THE FORENSIC PROCESS

COLLECTION

What steps should you take upon receiving evidence?

Step 1. If the device is off, leave it off; if the device is on, leave it on.

Step 2. If it's on: place into ‘Airplane Mode’.

Step 3. Make sure to gather all passcode/password information.

Step 4. Hand to a digital forensic specialist.

Next steps will be:

- Photograph the device
- Use of a Faraday device
- Start of a chain of custody
- Documented imaging form

IMPORTANCE OF CELLPHONE DATA PRESERVATION

Mobile technology data is volatile:

Crucial data can be lost by:

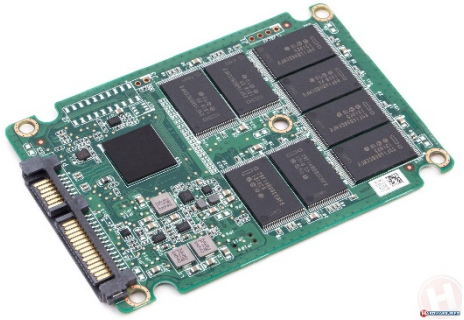
- User selective deletion
- App updates
- Constant OS updates
- 'Factory Reset' simple and effective
- Remote wipe capability

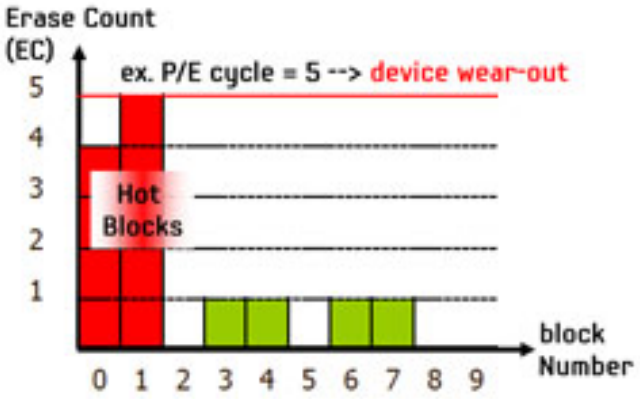
Deleted data may not be recoverable because:

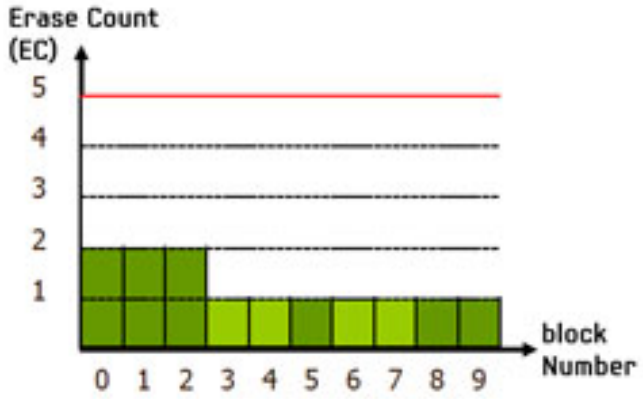
- Security on the device
- Wear-levelling of NAND technology

IMPORTANCE OF CELLPHONE DATA PRESERVATION

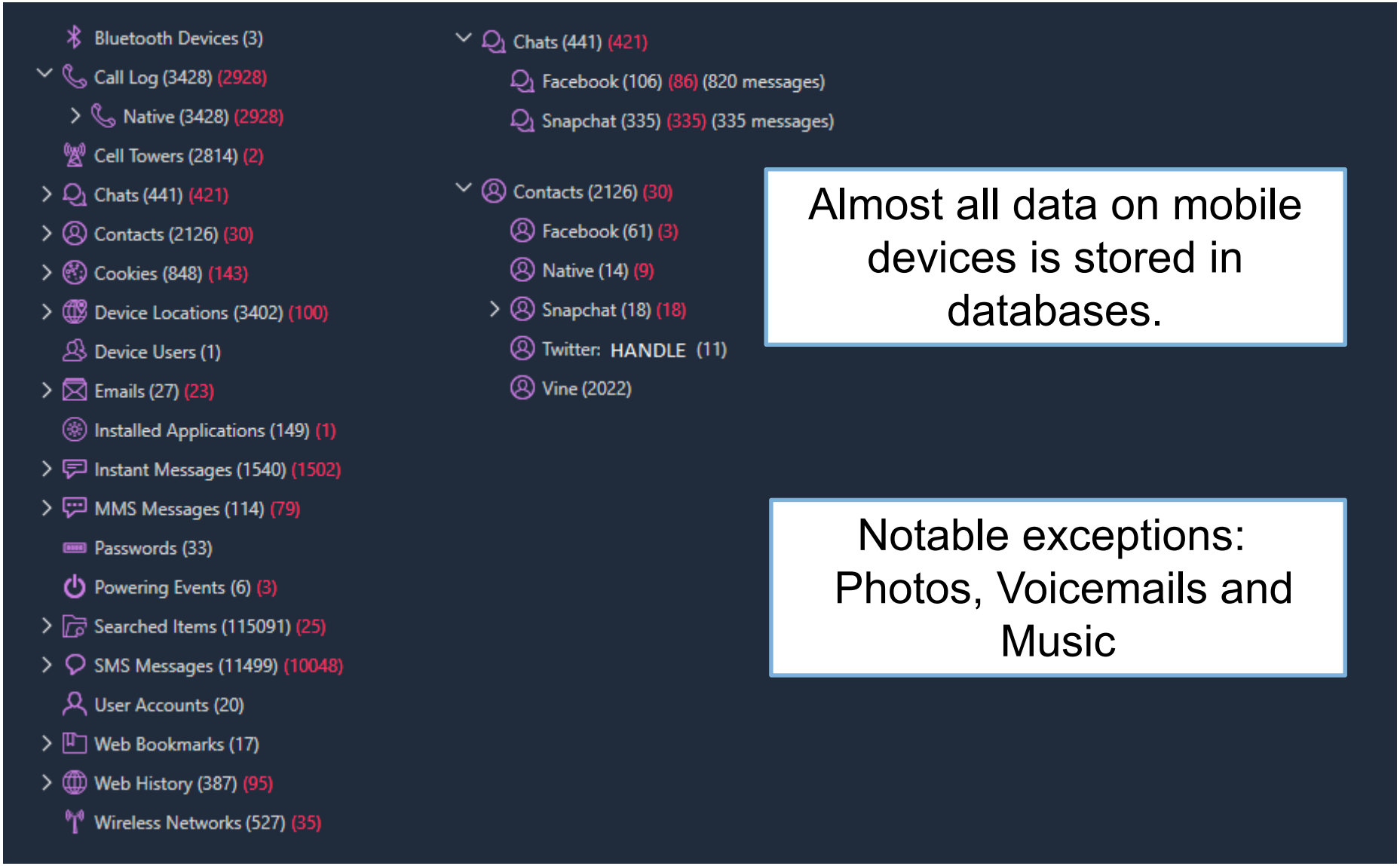
NAND Technology







HOW MOBILE DEVICES STORE INFORMATION



Almost all data on mobile devices is stored in databases.

Notable exceptions: Photos, Voicemails and Music

EXTRACTION TYPES

1. Logical Extraction
   - Just the active files of the device – within the operating system
   - Deleted space, deleted files and fragments will NOT be captured
   - Essentially everything visible to the user on the cellphone

2. File System Extraction
   - System files on the device – within the operating system
   - May include some deleted material

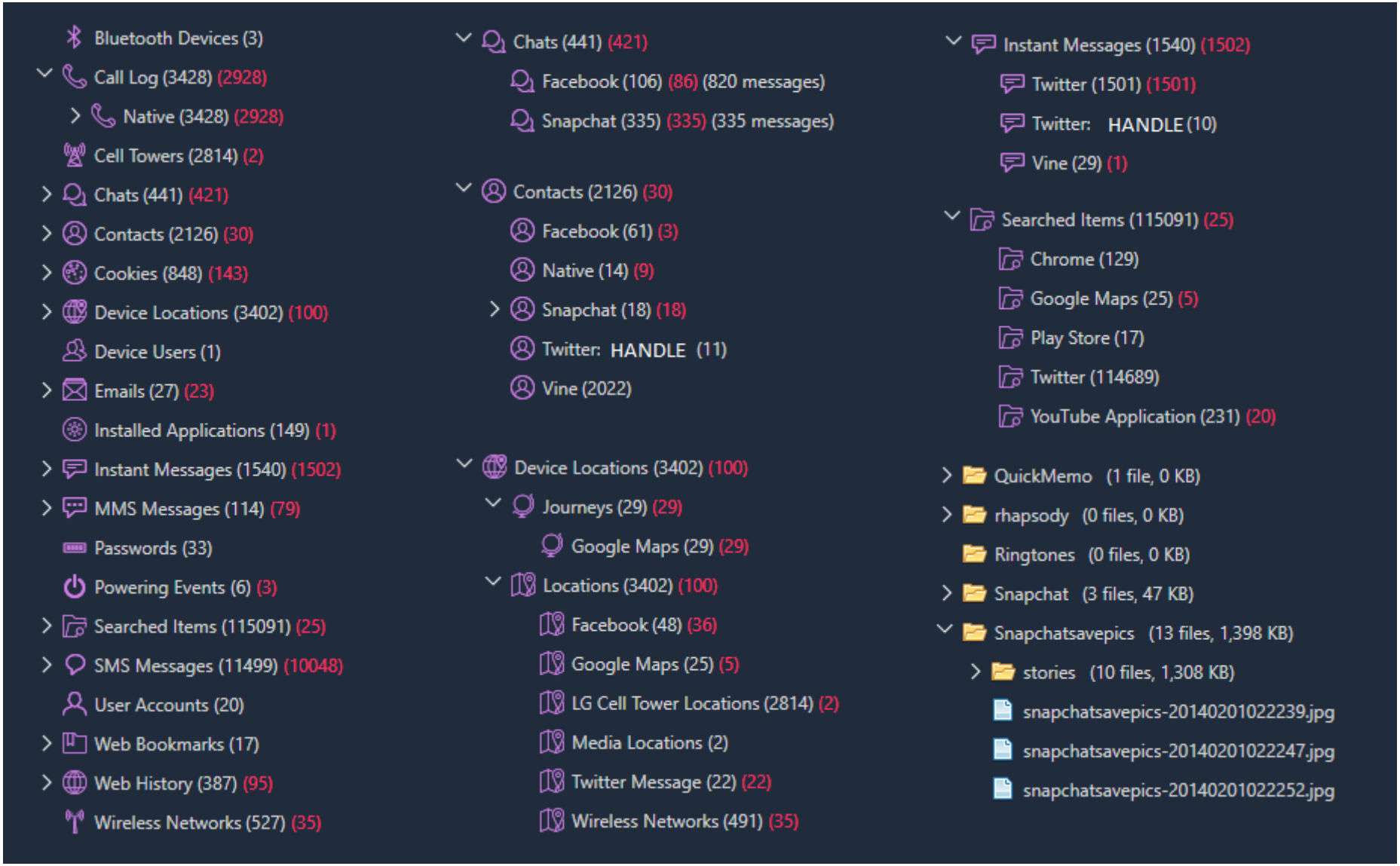
3. Advanced Logical Extraction
   - iPhone specific extraction
   - Asking OS for files – very helpful OS
   - Databases provided produce a substantial amount of deleted data

EXTRACTION TYPES

4. Physical Extraction

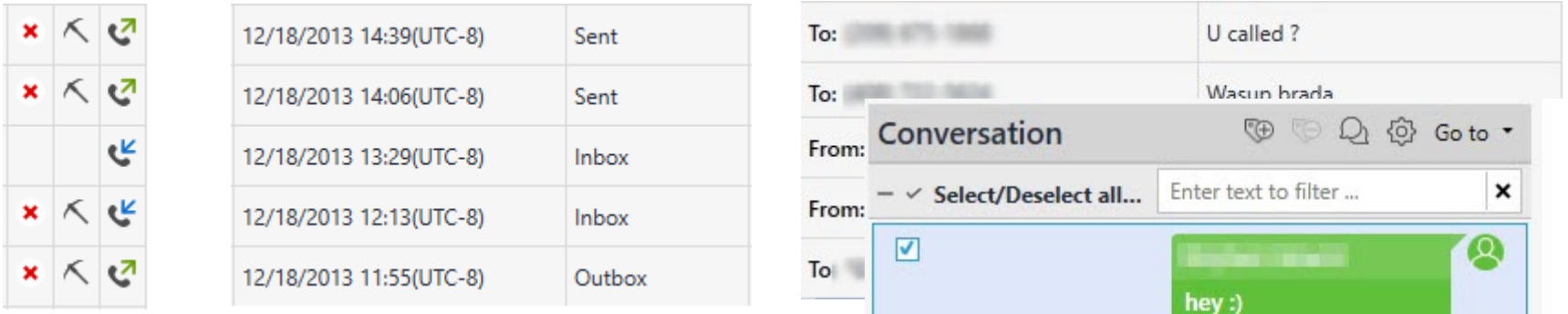
- All data on the chip
- A large amount of deleted data
- Allows for ‘carving’ of data
- More likely on an Android
- iPhone 4 or earlier
- Bypass any passcode

DATA TYPES



COMMUNICATIONS

SMS / MMS



12/18/2013 14:39(UTC-8)	Sent
12/18/2013 14:06(UTC-8)	Sent
12/18/2013 13:29(UTC-8)	Inbox
12/18/2013 12:13(UTC-8)	Inbox
12/18/2013 11:55(UTC-8)	Outbox

To:	U called ?
To:	Wasup brada
From:	
From:	
To:	

Conversation

Go to

Select/Deselect all...

Enter text to filter ...

hey :)

9/5/2013 09:43(UTC-7)

Sources (1)

Hi

9/5/2013 09:54(UTC-7)

Sources (1)

how u doing ?

9/6/2013 11:24(UTC-7)

Sources (1)

CHATS

						Participants	Start Time
			1	3	2	(owner)	9/5/2013 09:

THE UNIQUE LANGUAGE OF TEXTING

CASE STUDY – How to form useful keywords for text/chat data

Worked Case: "Major partner left his longtime employer to start up a new competing company"

Limited use of proper pronouns

Misspellings are more common

Frequent use of abbreviations

Limit keyword searching

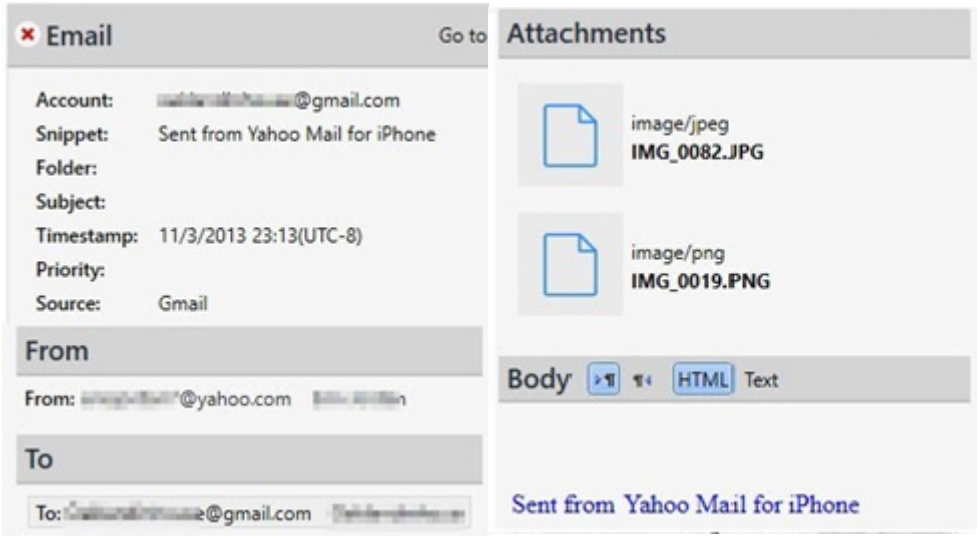
Increase emphasis on context

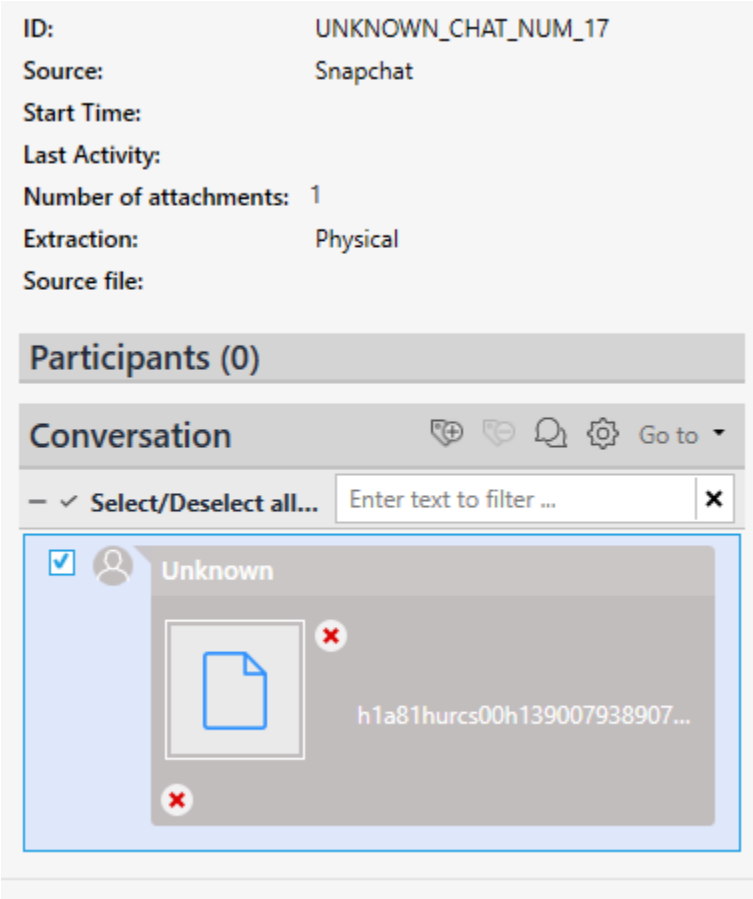
Lengthen date range/broaden review

Results: Many of the communications spoke generically and conversations had to be pieced together from multiple custodians due to deletions. Review took longer.

COMMUNICATIONS

Email and Snapchat – limited content

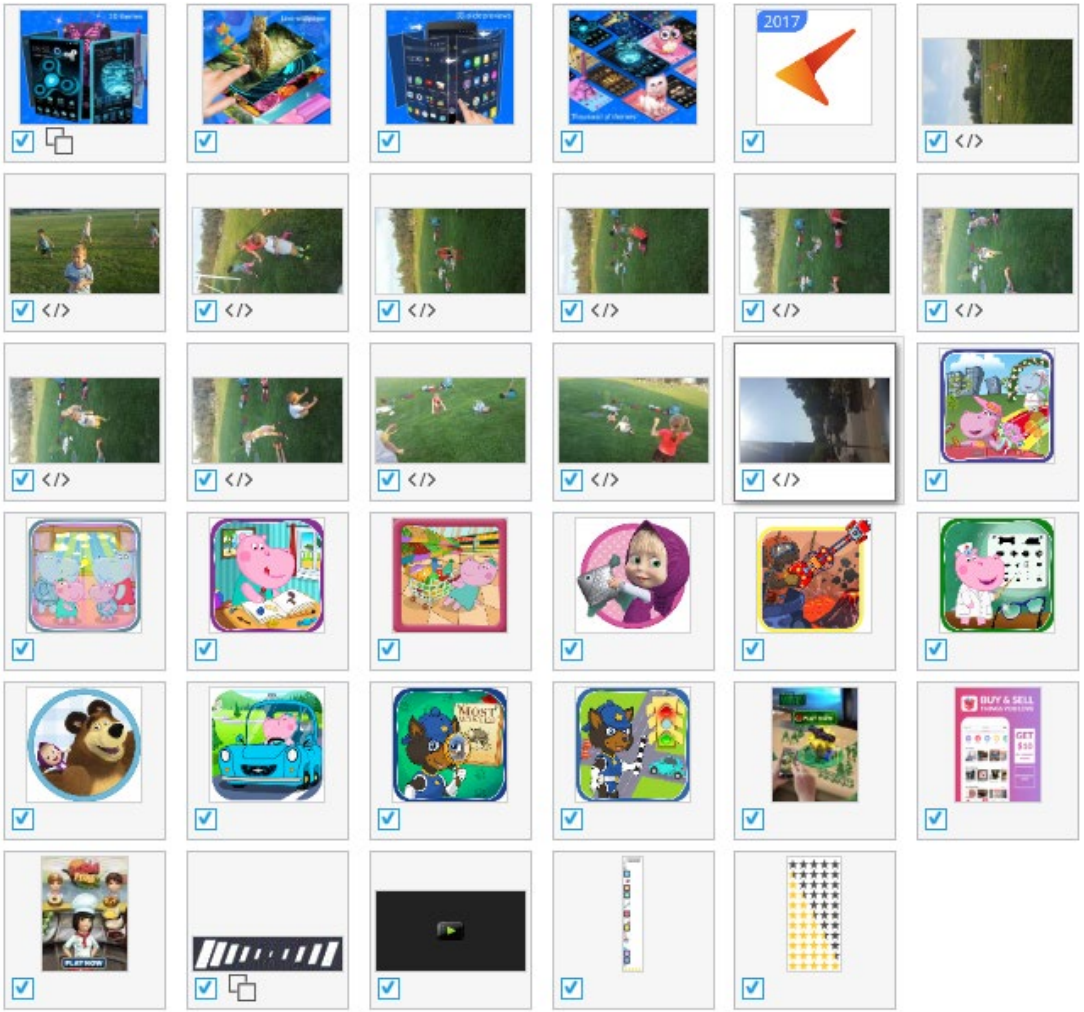


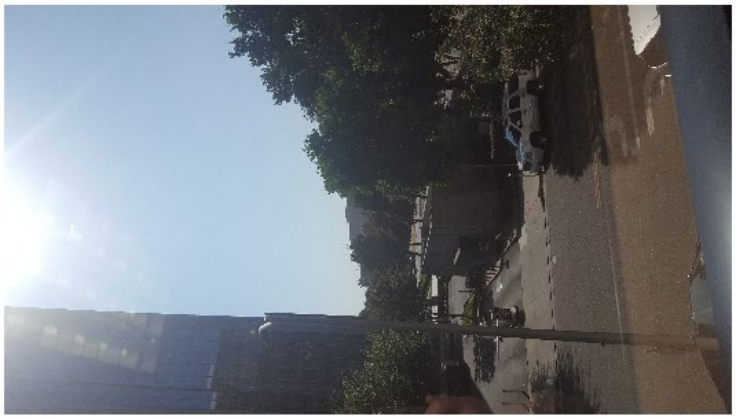


Better way to get email data:

1. Request username and password;
2. Collection by forensic specialist;
3. Triangle agreement to protect privilege and non-relevant data.

IMAGES





Name:	20170908_104113.jpg
Type:	Images
Size (bytes):	3936751
Path:	Media/Phone/DCIM/Camera/20170908_104113.jpg
Created:	9/8/2017 10:41
Accessed:	
Modified:	
Deleted:	
Extraction:	Logical
MD5:	e05b5257b845496cb7ca5bd3da098618
Source file:	20170908_104113.jpg

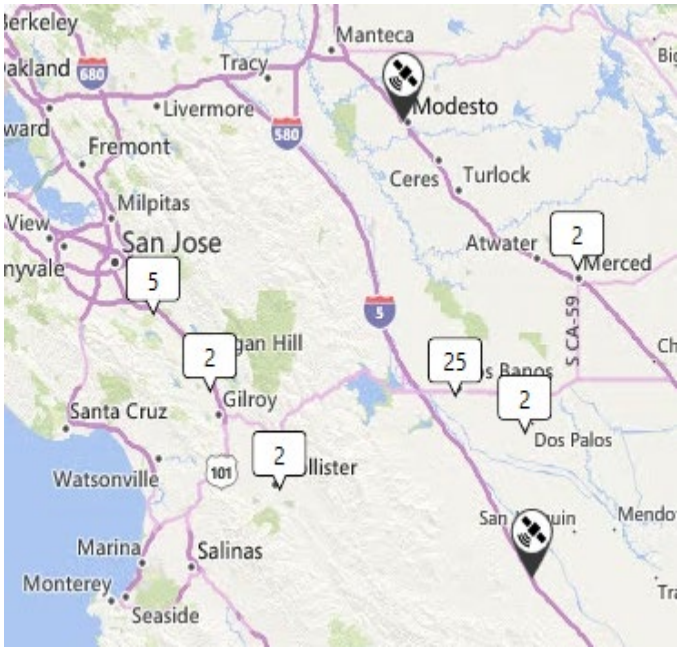
Metadata

Camera Make:	samsung
Camera Model:	SM-G920T
Capture Time:	9/8/2017 10:41
Pixel resolution:	5312x2988
Resolution:	72x72 (Unit: Inch)
Orientation:	Rotate 90 CW

Map

Position:	
Address:	

LOCATION DATA - METADATA



Name:	PART_1387687825658_IMG_4870.jpeg
Type:	Images
Size (bytes):	155973
Path:	userdata (ExtX)/Root/data/com.android.providers.telephony/app_parts/PART_1387687825658_IMG_4870.jpeg
Created:	12/21/2013 20:50(UTC-8)
Accessed:	12/21/2013 20:50(UTC-8)
Modified:	12/21/2013 20:50(UTC-8)

Metadata

Camera Make:	Apple
Camera Model:	iPhone 5c
Capture Time:	12/21/2013 20:36
Pixel resolution:	1536x2048
Resolution:	72x72 (Unit: Inch)
Lat/Lon:	36.840294 / -121.391450

Map

Position:	(36.840294, -121.391450)
Address:	
Map Address:	

LOCATION DATA –TOWER DATA FROM PROVIDER

GSM - Global System for Mobile Communications – New Cell Networks

MOBILITY USAGE
(with cell location)

AT&T has queried for records using Mountain Time Zone. AT&T's records are stored and provided in UTC.

Mountain Time Zone.

Conn.Date	Conn. Time UTC	Originating #	Terminating #	IMEI	IMSI	Desc	MAKE	MODEL	Cell Location

SMST APPLE IPHONE6 [42962/41512:-116.64361:48.36667:235:88.0]
SMST APPLE IPHONE6 [42962/41512:-116.64361:48.36667:235:88.0]
SMST APPLE IPHONE6 [42962/41512:-116.64361:48.36667:235:88.0]

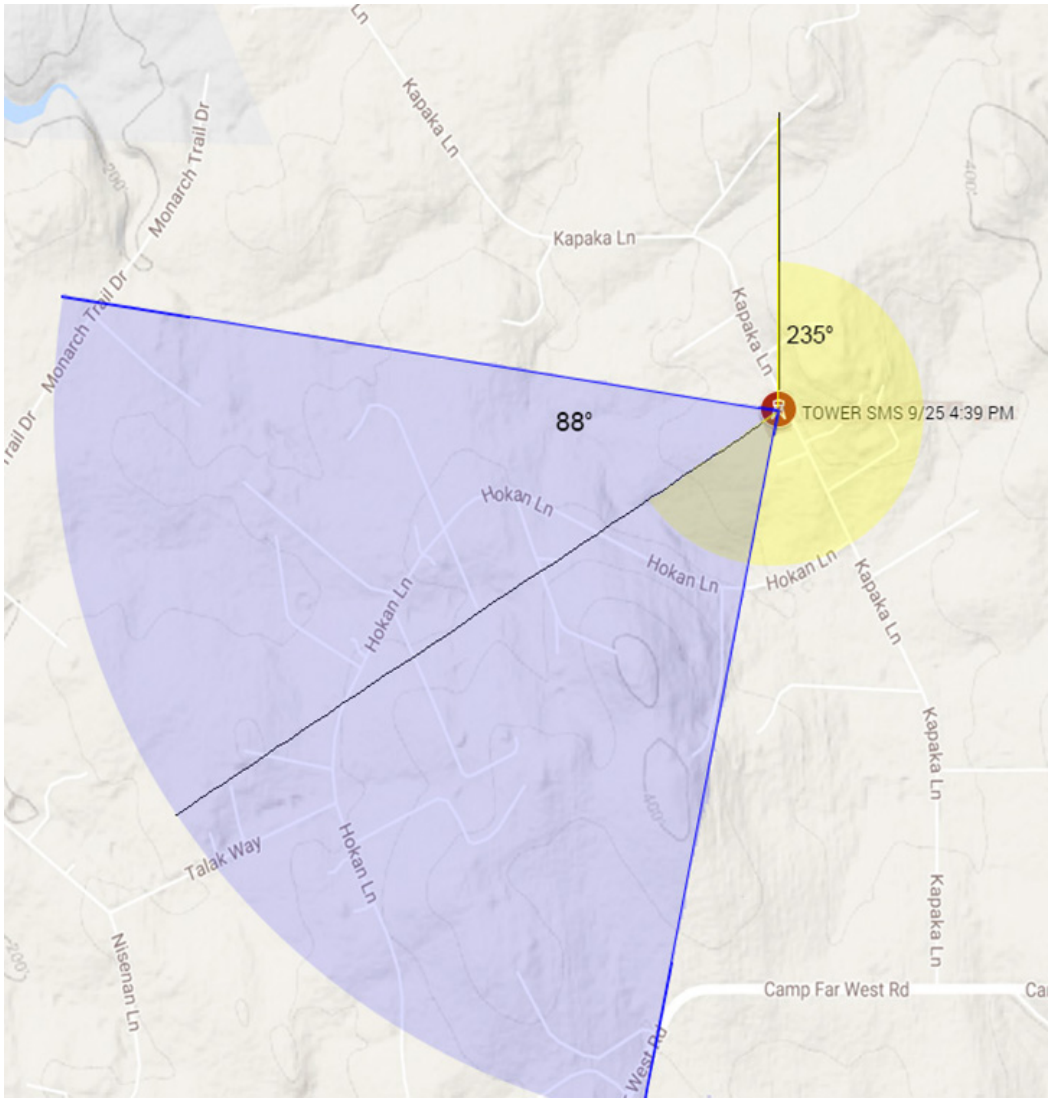
[LAC/CID:Longitude:Latitude:Azimuth:BeamWidth]

LOCATION DATA – TOWER DATA MAPPING

LAC/CID
Longitude, Latitude
- Location of the Tower

Azimuth
- Sector angle from due North

Beam Width
- Angle of coverage of sector.



LOCATION DATA – GPS DATA

Historical Precision Location Information

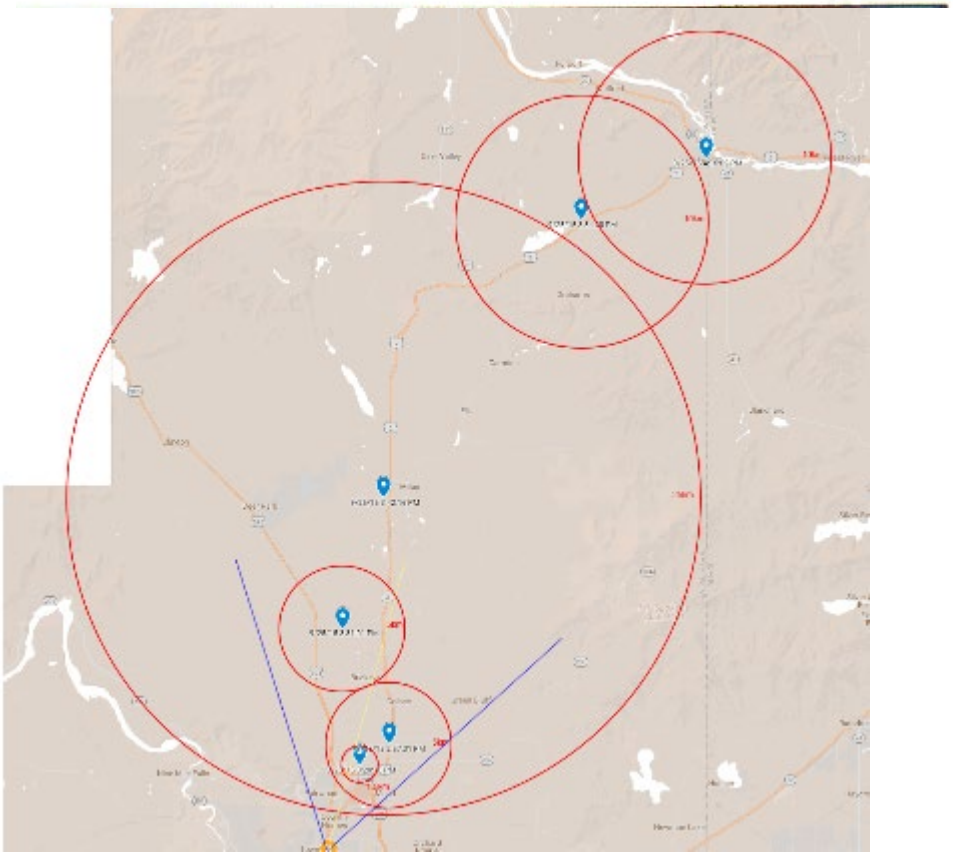
The results provided are AT&T's best estimate of the location of the target number. Please exercise caution in using these records for investigative purposes as location data is sourced from various databases which may cause location results to be less than exact.

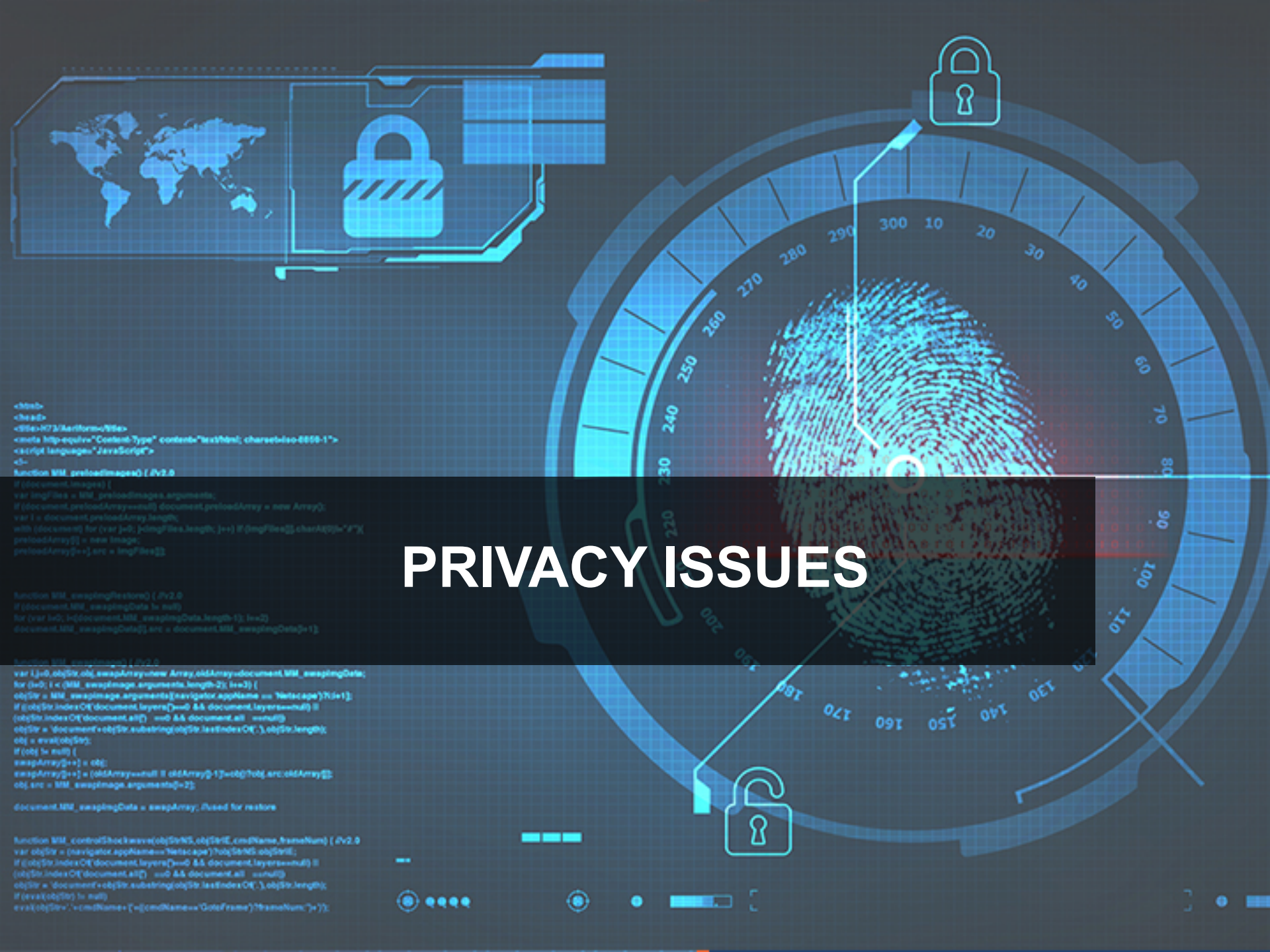
at&t

Connection Date	Connection Time (GMT)	Longitude	Latitude
2015-09-25	23:16:02	-117.042993	48.179664
2015-09-25	22:54:28	-117.164403	48.139839
2015-09-25	22:42:16	-117.356562	47.958957
2015-09-25	22:32:30	-117.356562	47.958939
2015-09-25	22:31:01	-117.396531	47.873763
2015-09-25	22:29:12	-117.356562	47.958939
2015-09-25	22:28:53	-117.39654	47.873736
2015-09-25	22:25:45	-117.351027	47.798235
2015-09-25	22:24:40	-117.351027	47.798235

Location Accuracy

Location accuracy likely better than 10000 meters
Location accuracy likely better than 10000 meters
Location accuracy likely better than 25000 meters
Location accuracy likely better than 5000 meters
Location accuracy likely better than 5000 meters
Location accuracy likely better than 5000 meters
Location accuracy likely better than 10000 meters
Location accuracy likely better than 5000 meters
Location accuracy likely better than 5000 meters




PRIVACY ISSUES

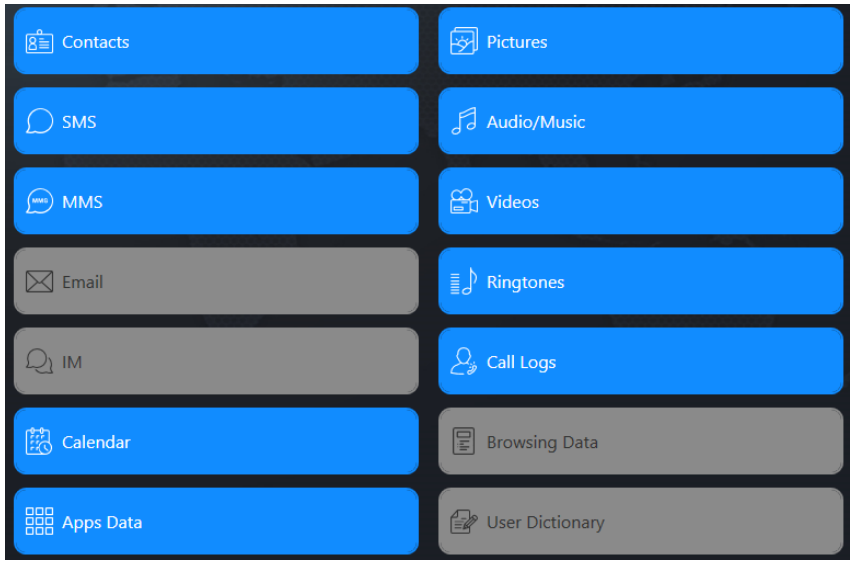
PRIVACY ISSUES – REASONS FOR RESISTANCE

Cellphone resistance to extraction

- Adult images
- Private conversations
- Mistrust of giving more information than needed

Solutions:

- **Selective extraction**
  - Only on Android
  - No deleted data
  - Limited system or app data
- **Triangle agreement**



PRIVACY ISSUES – LOCATION DATA

U.S. Court of Appeals for the Eleventh Circuit's decision in *United States v. Davis*.

- Prosecutors' discovery RE: location of cell towers that routed a defendant's calls
- *NOT* a violation of the defendant's Fourth Amendment right against unreasonable search and seizure.

A cell phone user does not have a reasonable expectation of privacy over a cell service carrier's records that do not reveal content of any communications, the opinion held, even if the records place a defendant's cell phone near a crime scene.

CASE SUMMARIES

CRIMINAL CASE SUMMARIES

Gareic Jerard Hankston v. State Of Texas, Texas Court of Appeals (2017).

Cell Phone records held by a service provider are considered business records and are not protected under the Fourth Amendment. Their disclosure is governed by statutory provisions and procedures.

People v. Nottoli, California Court of Appeals (2011)

Upheld the warrantless search of defendant's smart phone in the passenger compartment of his car when he was arrested for DUI.

Riley v. California, US Supreme Court (2014)

"[A]nswer to the question of what police must do before searching a cell phone seized incident to an arrest is...simple-get a warrant."

State v. Kolanowski, Washington Court of Appeals, (2017)

A case involving the failure to authenticate social media evidence, a criminal defendant unsuccessfully sought to admit a screenshot of Facebook evidence as critical impeachment against the prosecutions' main witness.

US v. Andrew Edward Flyer, US Court of Appeals, Ninth Circuit (2011)

Charges relating to transportation, shipping and possession of Child Pornography. Three of the four counts overturned on appeal through forensic investigation. Most images found in unallocated space and therefore 'knowledgeable possession' questionable. Also corruption of evidence by FBI investigator damaged their case.

PRESERVATION – FRCP Rule 37(e)

Failure to Preserve Evidence - Federal Rule of Civil Procedure 37(e).

The loss or destruction of relevant cell phone texts, intentional or not, can lead to sanctions under Federal Rule of Civil Procedure 37(e).

Rule 37(e) authorizes courts to issue sanctions where four conditions are met:

1. the ESI at issue should have been preserved in the anticipation or conduct of litigation;
2. the ESI is lost;
3. the loss is due to a party's failure to take reasonable steps to preserve it;
4. the ESI cannot be restored or replaced through additional discovery.

CIVIL CASE SUMMARIES

EEOC v. The Original Honey Baked Ham Company of Georgia Inc. *(Feb. 27, 2013)*

EEOC filing suit on behalf of employees alleging sexual harassment and retaliation. Defendant requested cellphone and social media access, court ordered them discoverable and requested production to a "Special Master". EEOC failed to produce and the court issued sanctions against EEOC.

Garcia v. City of Laredo, US Court of Appeals, Fifth Circuit (2012)

Garcia, a former police dispatcher for the City of Laredo, claims Defendants accessed the contents of her cellphone without permission in violation of the Stored Communications Act (SCA). District court granted summary judgement for Defendants – SCA Statute did not apply, upheld on appeal.

Christou v. Beatport, LLC *(D. Colo. Jan. 23, 2013)*

Christou a club owner hired Bradley Roulier who opened a music website called Beatport. Roulier offered part ownership to Christou that was never given. Also opened a rival club and used the threat of being dropped from Beatport site if acts performed at Christou's clubs. Litigation hold sent to defendant 2010. May 2011 discovery request ignored. August 2011 Roulier reportedly lost his iPhone. Plaintiff was able to introduce litigation hold letter and defendants failure to preserve text messages. Can argue for inference.

Nuvasive, Inc. v. Madsen Med. Inc. *(S.D. Cal. Jan. 26, 2016)*

Nuvasive was accused of conspiring with Madsen employees to remove Madsen from the partnership contract at which point Nuvasive would hire on the Madsen team as their own employees. Spoliation sanctions were sought after Nuvasive only moved to preserve the evidence two years after the incident when messages had been lost.

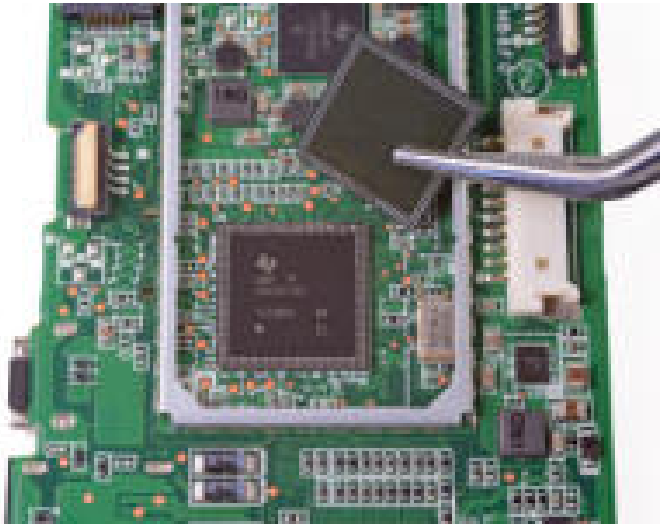

DIGGING DEEPER

DIGGING DEEPER

JTAG & Chip Off – When All Else Fails

JTAG –

- Soldering onto chip to bypass security
- Limited risk of damage



Chip-Off –

- Removing chip to bypass security
- Moderate risk of damage

DIGGING DEEPER

Carving iPhc

Hex View

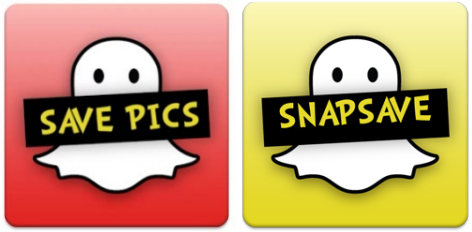
001A91B2	35 46 35		z..wZ.....>.U3.
001A91C8	00 01 00		..)U..........
001A91DE	08 09 08		.....
001A91F4	08 08 08		.....B95532BE-
001A920A	30 41 46		38-A954-586C959
001A9220	46 30 34		d a lick .... t
001A9236	6F 6F 5C		reamtyped.....@
001A924C	84 84 84		utableAttribute
001A9262	64 53 74		....NSAttribute
001A9278	64 53 74		....NSObject...
001A928E	84 84 84		>.U1.....n...)
001A92A4	55 08 04		.....
001A92BA	39 09 08		.....
001A92D0	08 08 00		490C-FF7C-44D0-
001A92E6	39 42 44		02F561C55FOk Ju
001A92FC	6C 69 65		thanks...stream
001A9312	74 79 70		...@....NSMutab

GU-ID	42393535333242452D304146342D344233382D413935342D353836433935394630343931	
Text:	416E642061206C69636B20F09F918520746F6F	*AND A LICK TOO *
HandleID	5C040B	92
Message Data	73747265616D747970656481E80384014084848419 4E534D757461626C6541747472696275746564537 4 72696E67008484124E5341747472696275746564536 53 7472696E67008484084E534F626A6563740085928 48484833F8E5E3E0055310800010000836E01091D2955	
Error	08	0 = No
Date	04	-
Date_read	04	-
Date_delivered	08	0 = None present
Is_delivered	09	1 = YES
Is_finished	09	1 = YES
Is_emote	08	0 = No
Is_from_me	08	0 = No
Is_empty	08	0 = No
Is_delayed	08	0 = No
Is_auto_reply	08	0 = No
Is_prepared	08	0 = No
Is_read	09	1 = YES
Is_system_message	08	0 = No
Is_sent	08	0 = No
Has_dd_results	08	0 = No
Is_service_message	08	0 = No
Is_forward	08	0 = No
Was_downgraded	08	0 = No
Is_archive	08	0 = No
Cache_has_attachments	08	0 = No
Cache_roomnames	39	-
Was_data_detected	09	1 = YES
Was_duplicated	08	0 = No
Is_audio_message	08	0 = No
Is_played	08	0 = No
Date_played	08	0 = No
Item_type	08	0 = No
Other_handle	08	0 = No
Group_title	00	NULL

DIGGING DEEPER

Application Review

- Snapchat Save Pics app
- Automatically saves images from ‘Friends’ list

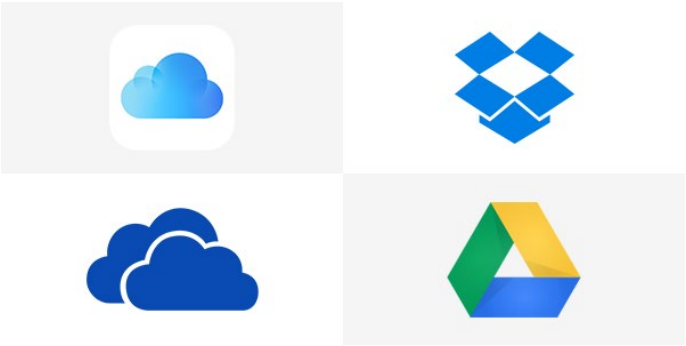


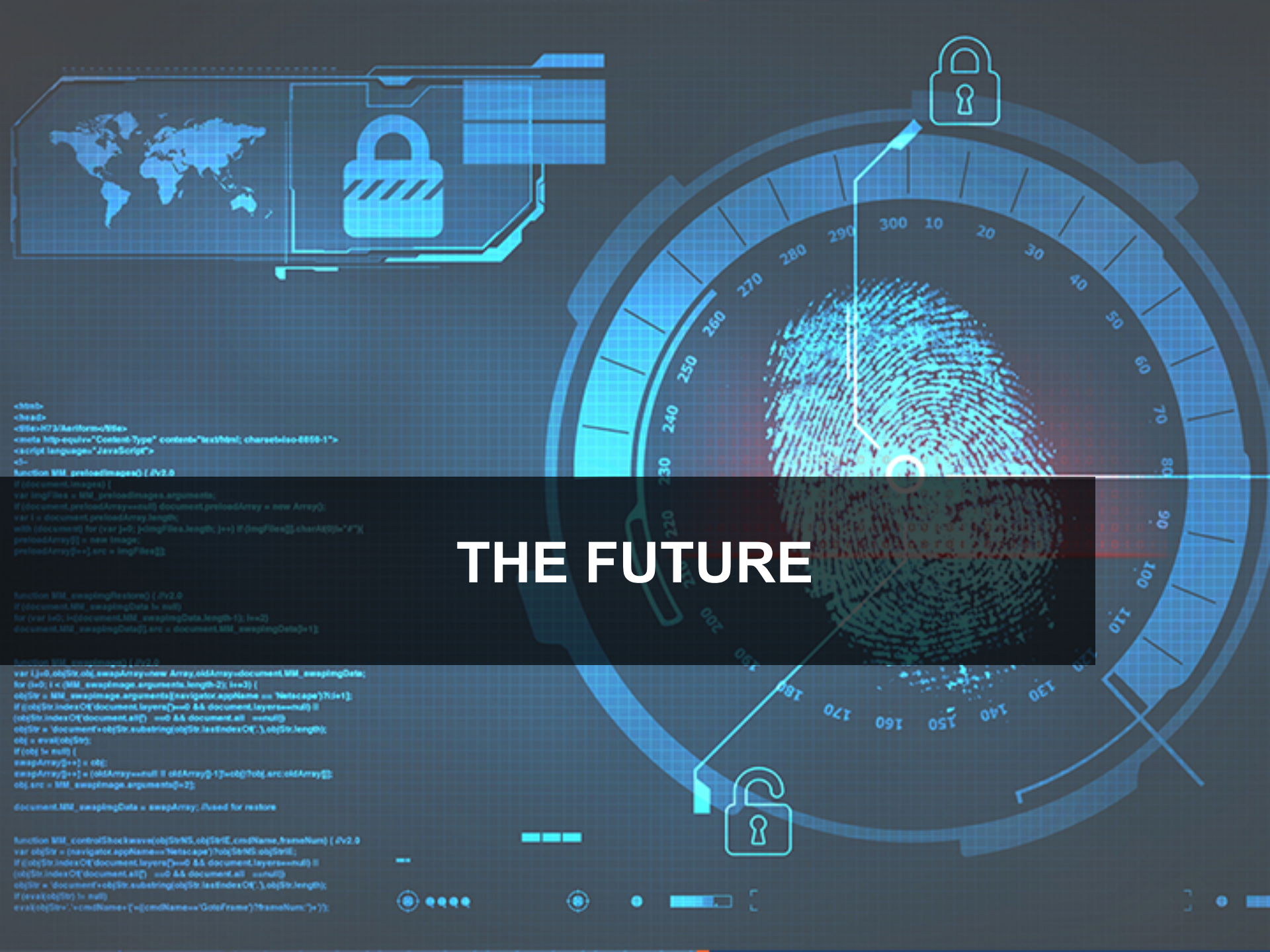
Malware Scan

- Very important in family law cases
- Very common in CP cases that the defendant claims virus

Cloud Sharing Analysis

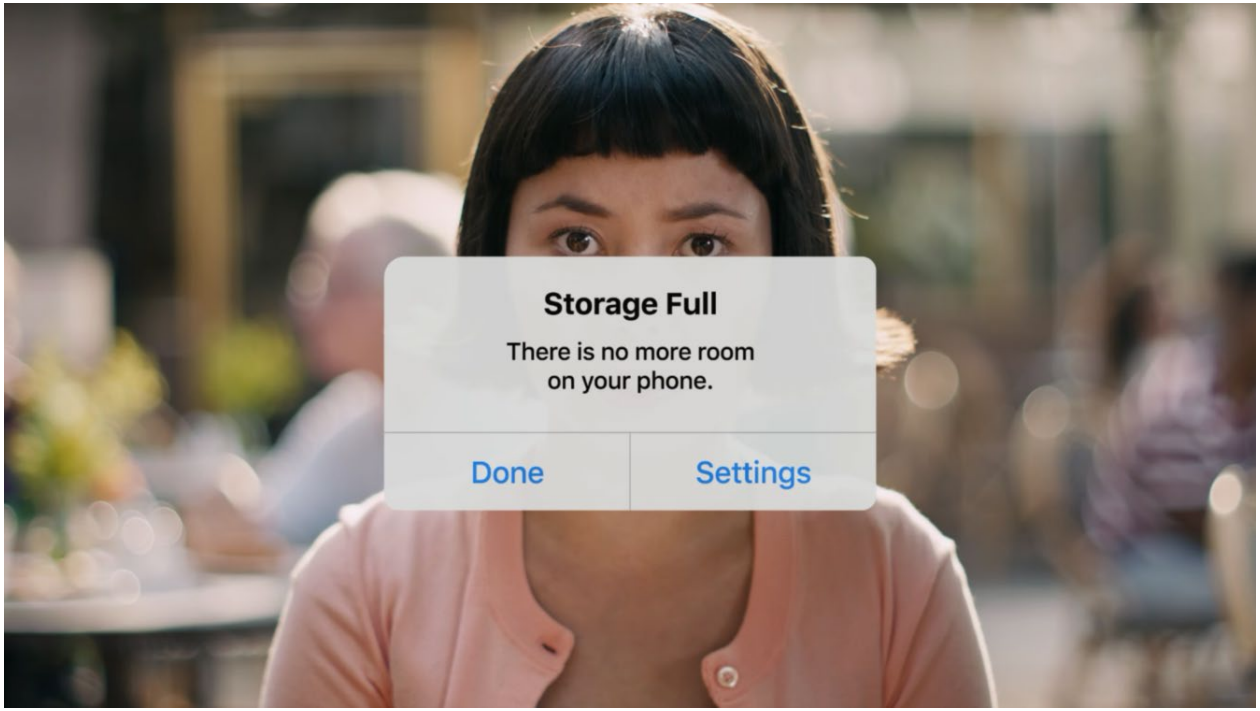
- Pull down iPhone or iPad backups
- Check iCloud Drive and iCloud Photos
- DropBox, etc. key for theft of IP




THE FUTURE

“CLOUDENTITY”

Device Independent Cloud-Based Identity



Possibility that devices won't store personal data and instead will be connected to an online system that turns that device into a phone, TV, etc.

ABOUT CALIFORENSICS

Helping attorneys win cases by finding, interpreting, and explaining digital evidence.

Business Litigation	Employment Law	Criminal Law
Schools & Higher Ed	Family Law	Medical Malpractice

- Plaintiff, defense, or neutral
- Any data source or data type
- Collection, analysis, expert testimony; e-discovery and hosted review
- 17 years in business
- 1,500 clients served nationwide
- Locations in Northern California, Southern California and Central Texas

Californics

a division of Capitol Digital