JOHN JAY COLLEGE – CENTER FOR CYBERCRIME STUDIES

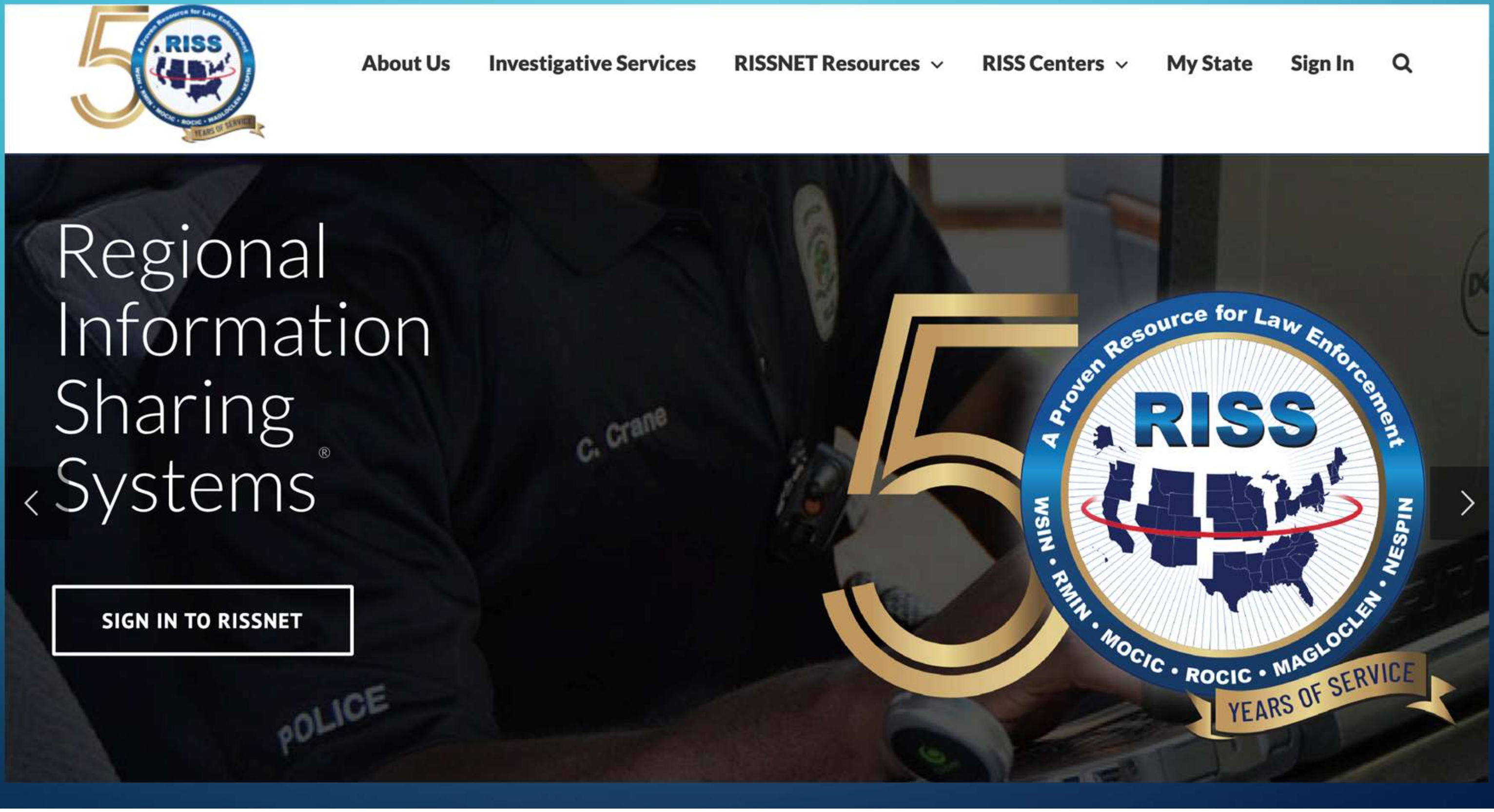
JOHN JAY
COLLEGE
OF
CRIMINAL
JUSTICE

Mission Statement: To lead, coordinate, catalyze, and produce cutting-edge, multidisciplinary research on cybercrime and develop evidence-based solutions to counter cybercrime.

The Center draws on cross-disciplinary expertise to:

1) conduct innovative and collaborative research on cybercrime;
2) inform policies and practices designed to investigate, respond to, mitigate, and prevent cybercrime; and
3) assist national and international public and private sectors in recognizing the changing cybercrime risk landscape, detecting cybersecurity vulnerabilities, and identifying the methods used by cybercriminals to adapt to and evade law enforcement and cybersecurity measures.

RISS.NET



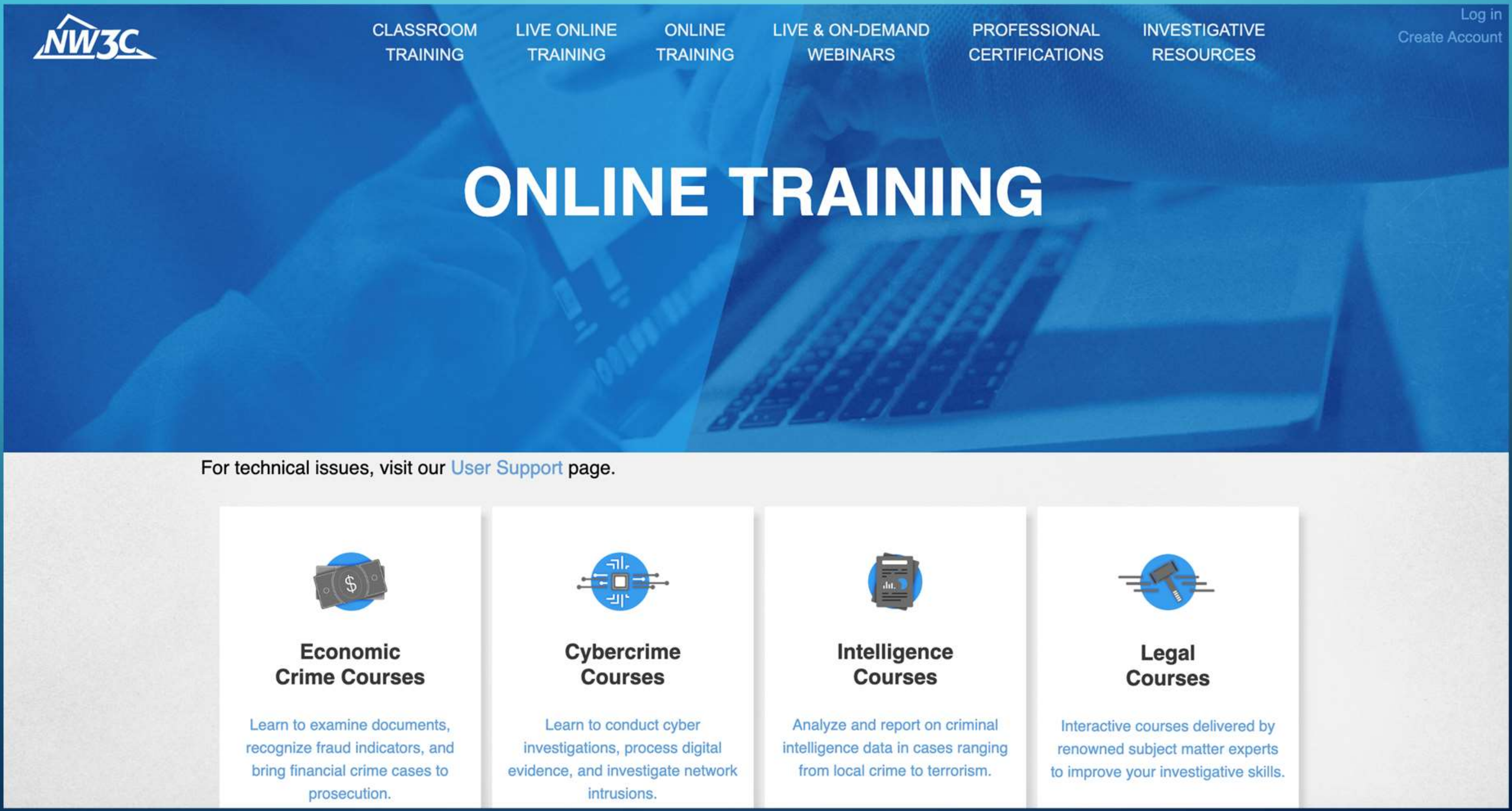
About Us Investigative Services RISSNET Resources ⌄ RISS Centers ⌄ My State Sign In

Regional Information Sharing Systems®

SIGN IN TO RISSNET

RISS
A Proven Resource for Law Enforcement
WSIN • RMIN • MOCIC • ROCIC • MAGLOCLEN • NESPIN
50 YEARS OF SERVICE
C. Crane
POLICE

NATIONAL WHITE COLLAR CRIME CENTER



ONLINE TRAINING

For technical issues, visit our User Support page.

Economic Crime Courses

Learn to examine documents, recognize fraud indicators, and bring financial crime cases to prosecution.

Cybercrime Courses

Learn to conduct cyber investigations, process digital evidence, and investigate network intrusions.

Intelligence Courses

Analyze and report on criminal intelligence data in cases ranging from local crime to terrorism.

Legal Courses

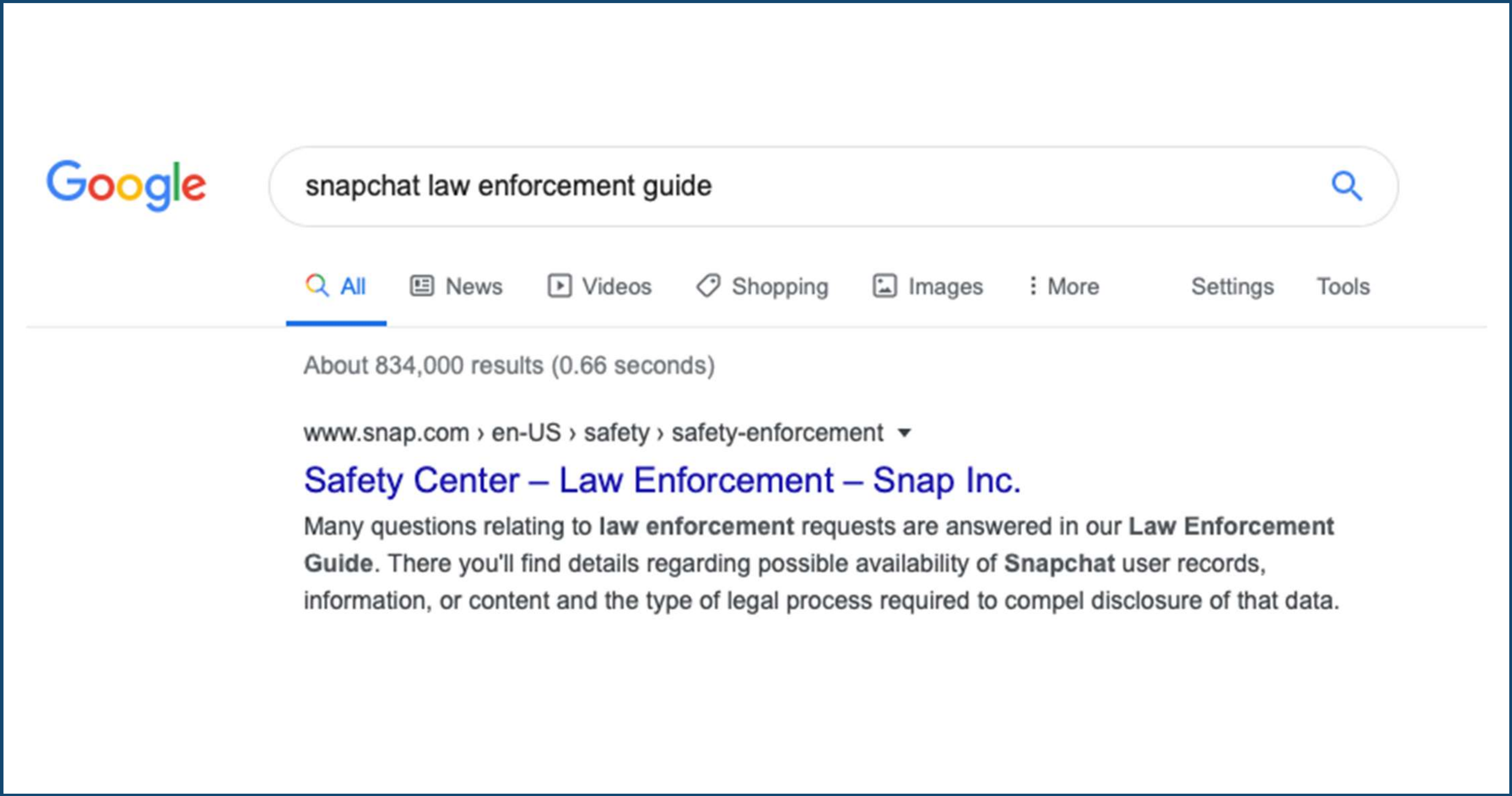
Interactive courses delivered by renowned subject matter experts to improve your investigative skills.

What is NCFTA ?

- Non- profit created in 2002 by Industry and Academia
- Neutral environment for sharing threat information
  - Not government owned
  - Not industry owned
- Co-located Staff
  - HQ based Law Enforcement
  - Industry analysts or investigators
  - NCFTA intelligence analysts

LAW ENFORCEMENT RESOURCE GUIDES

- IDENTIFY THE SERVICE PROVIDER YOU WANT INFORMATION FROM.
- MOST SERVICE PROVIDERS HAVE ONLINE GUIDES FOR LAW ENFORCEMENT AND LEGAL COMPLIANCE.
- VISIT THEIR WEBSITE OR GOOGLE “X LAW ENFORCEMENT GUIDE.”



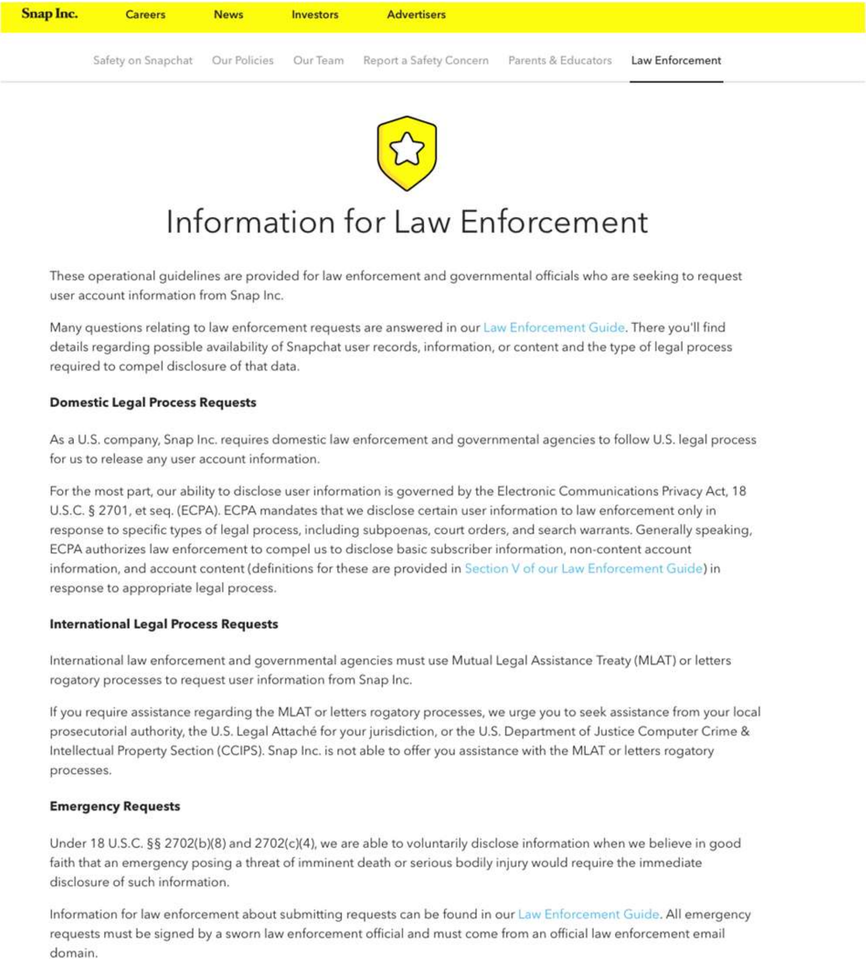
snapchat law enforcement guide

About 834,000 results (0.66 seconds)

www.snap.com › en-US › safety › safety-enforcement

Safety Center – Law Enforcement – Snap Inc.

Many questions relating to **law enforcement** requests are answered in our **Law Enforcement Guide**. There you'll find details regarding possible availability of **Snapchat** user records, information, or content and the type of legal process required to compel disclosure of that data.



Information for Law Enforcement

These operational guidelines are provided for law enforcement and governmental officials who are seeking to request user account information from Snap Inc.

Many questions relating to law enforcement requests are answered in our Law Enforcement Guide. There you'll find details regarding possible availability of Snapchat user records, information, or content and the type of legal process required to compel disclosure of that data.

Domestic Legal Process Requests

As a U.S. company, Snap Inc. requires domestic law enforcement and governmental agencies to follow U.S. legal process for us to release any user account information.

For the most part, our ability to disclose user information is governed by the Electronic Communications Privacy Act, 18 U.S.C. § 2701, et seq. (ECPA). ECPA mandates that we disclose certain user information to law enforcement only in response to specific types of legal process, including subpoenas, court orders, and search warrants. Generally speaking, ECPA authorizes law enforcement to compel us to disclose basic subscriber information, non-content account information, and account content (definitions for these are provided in Section V of our Law Enforcement Guide) in response to appropriate legal process.

International Legal Process Requests

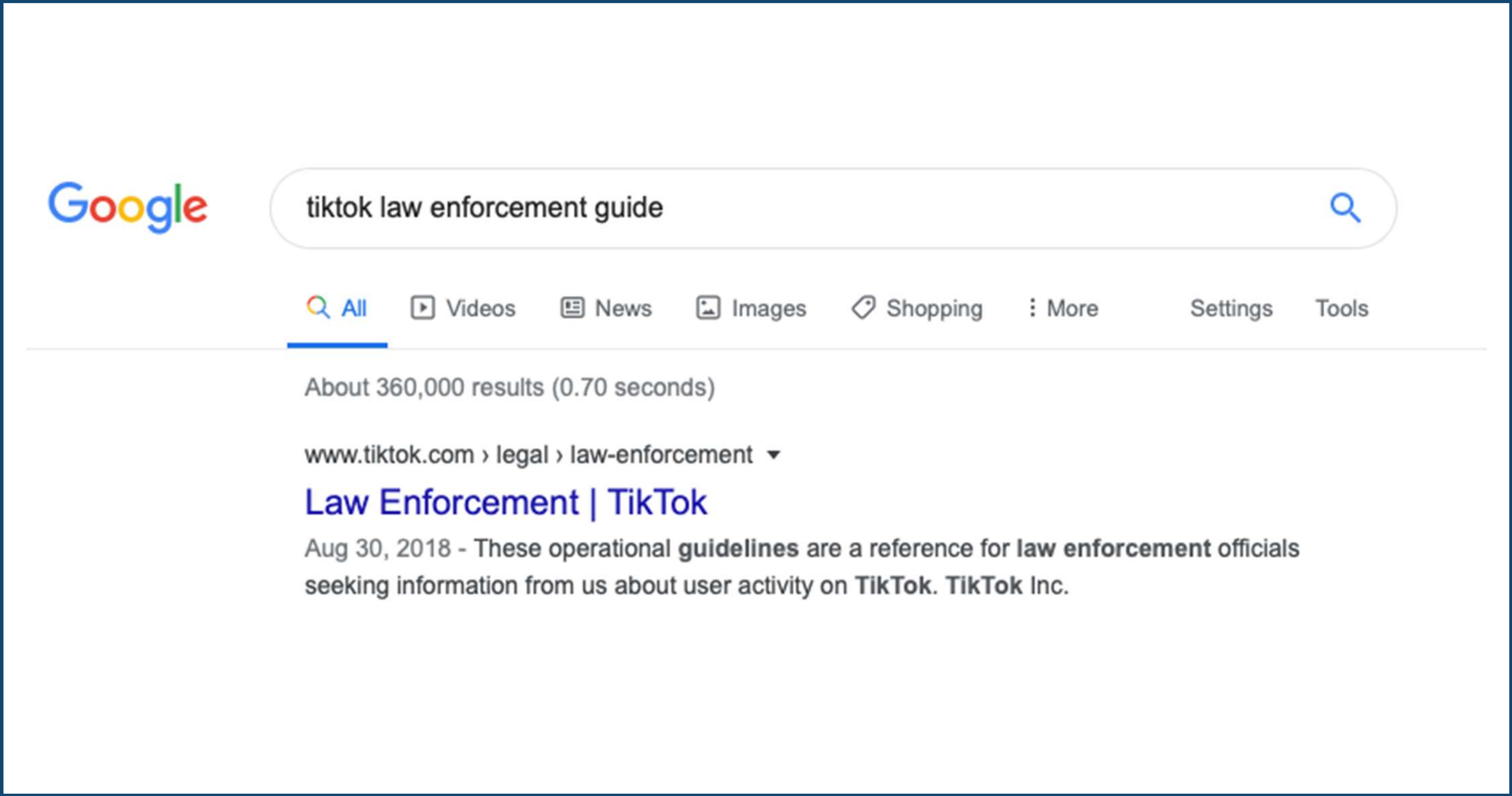
International law enforcement and governmental agencies must use Mutual Legal Assistance Treaty (MLAT) or letters rogatory processes to request user information from Snap Inc.

If you require assistance regarding the MLAT or letters rogatory processes, we urge you to seek assistance from your local prosecutorial authority, the U.S. Legal Attaché for your jurisdiction, or the U.S. Department of Justice Computer Crime & Intellectual Property Section (CCIPS). Snap Inc. is not able to offer you assistance with the MLAT or letters rogatory processes.

Emergency Requests

Under 18 U.S.C. §§ 2702(b)(8) and 2702(c)(4), we are able to voluntarily disclose information when we believe in good faith that an emergency posing a threat of imminent death or serious bodily injury would require the immediate disclosure of such information.

Information for law enforcement about submitting requests can be found in our Law Enforcement Guide. All emergency requests must be signed by a sworn law enforcement official and must come from an official law enforcement email domain.



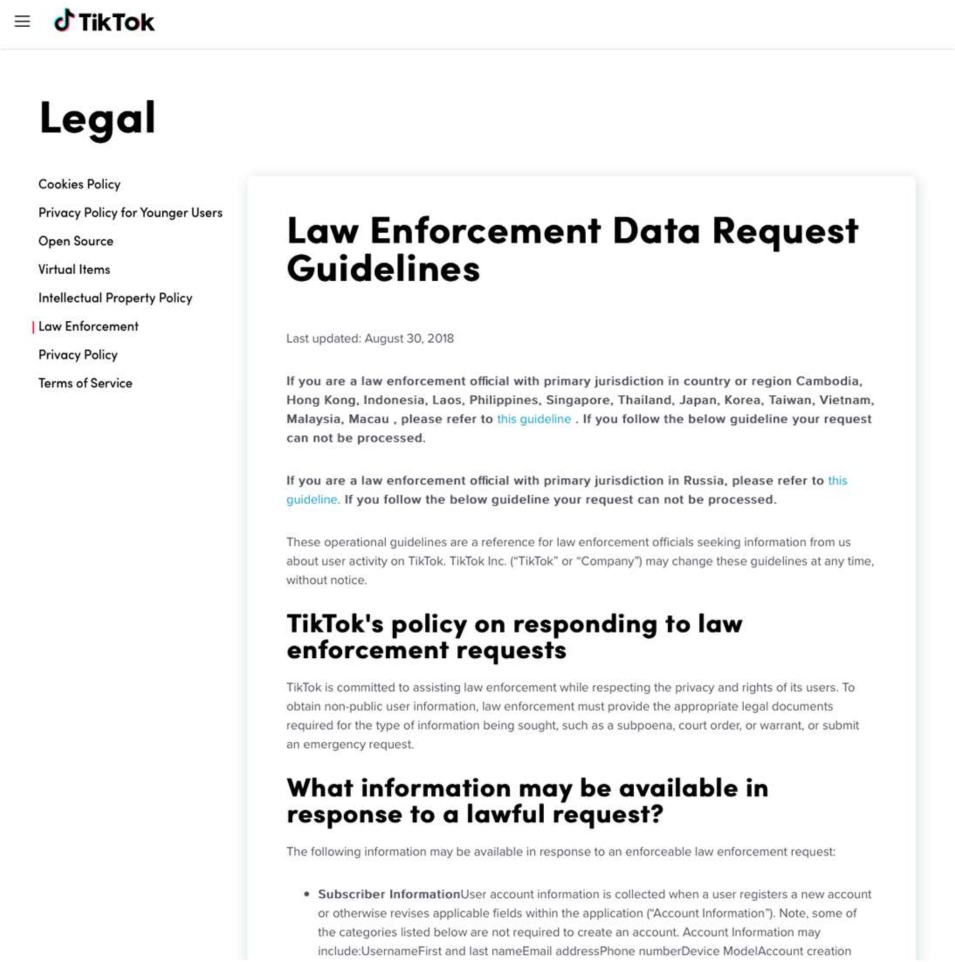
tiktok law enforcement guide

About 360,000 results (0.70 seconds)

www.tiktok.com › legal › law-enforcement

Law Enforcement | TikTok

Aug 30, 2018 - These operational **guidelines** are a reference for **law enforcement** officials seeking information from us about user activity on **TikTok**. **TikTok** Inc.



Legal

- Cookies Policy
- Privacy Policy for Younger Users
- Open Source
- Virtual Items
- Intellectual Property Policy
- Law Enforcement
- Privacy Policy
- Terms of Service

Law Enforcement Data Request Guidelines

Last updated: August 30, 2018

If you are a law enforcement official with primary jurisdiction in country or region Cambodia, Hong Kong, Indonesia, Laos, Philippines, Singapore, Thailand, Japan, Korea, Taiwan, Vietnam, Malaysia, Macau , please refer to this guideline **. If you follow the below guideline your request can not be processed.**

If you are a law enforcement official with primary jurisdiction in Russia, please refer to this guideline. **If you follow the below guideline your request can not be processed.**

These operational guidelines are a reference for law enforcement officials seeking information from us about user activity on TikTok. TikTok Inc. ("TikTok" or "Company") may change these guidelines at any time, without notice.

TikTok's policy on responding to law enforcement requests

TikTok is committed to assisting law enforcement while respecting the privacy and rights of its users. To obtain non-public user information, law enforcement must provide the appropriate legal documents required for the type of information being sought, such as a subpoena, court order, or warrant, or submit an emergency request.

What information may be available in response to a lawful request?

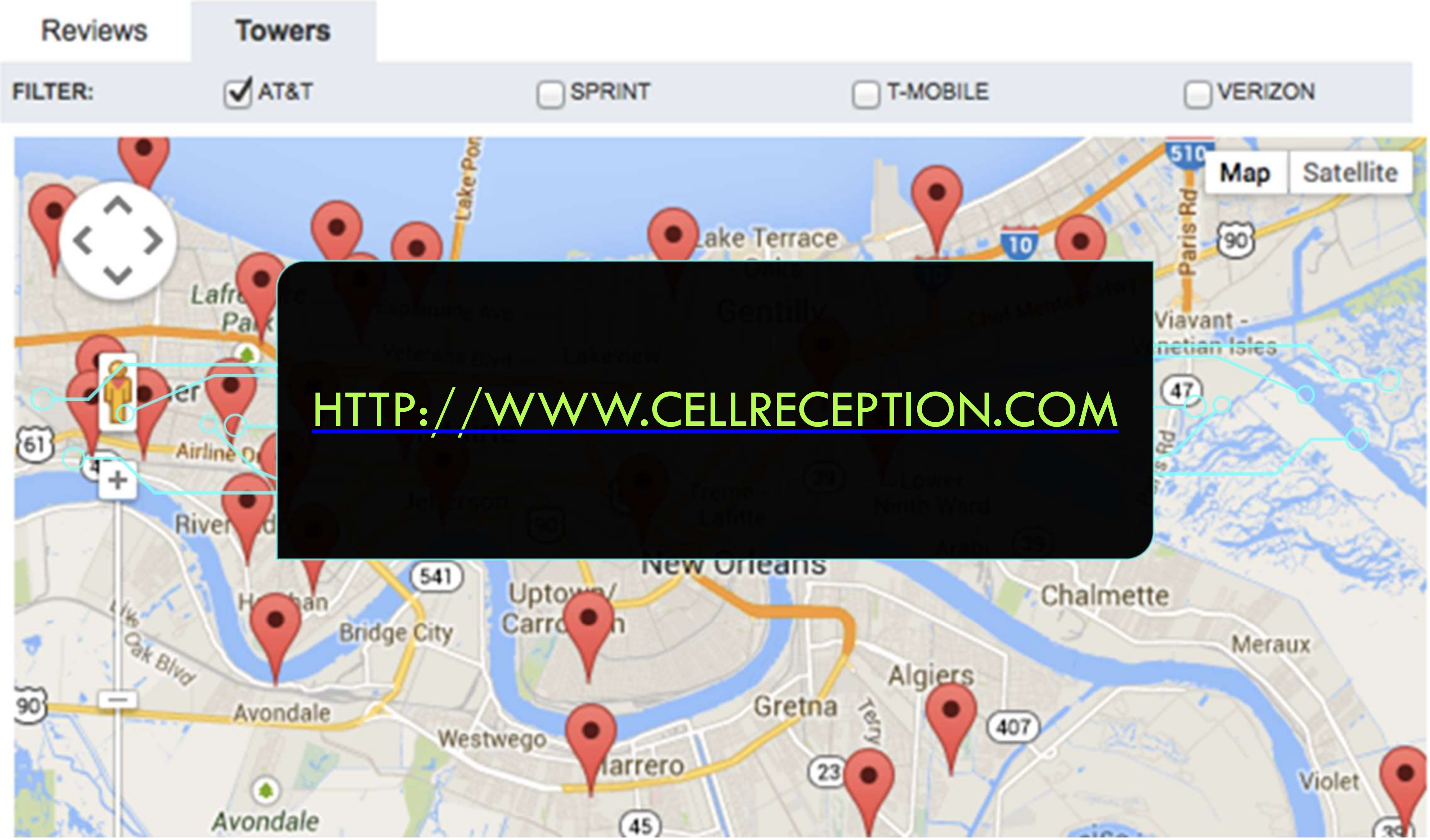
The following information may be available in response to an enforceable law enforcement request:

- **Subscriber Information**User account information is collected when a user registers a new account or otherwise revises applicable fields within the application ("Account Information"). Note, some of the categories listed below are not required to create an account. Account Information may include:UsernameFirst and last nameEmail addressPhone numberDevice ModelAccount creation

CELL TOWERS

- Coverage ~ 10 square miles
- Strong signal, near tower*
- Towers can be leased
- Can be disguised in trees, water towers, houses, etc.
- For CELL tower reference
  - http://www.cellreception.com

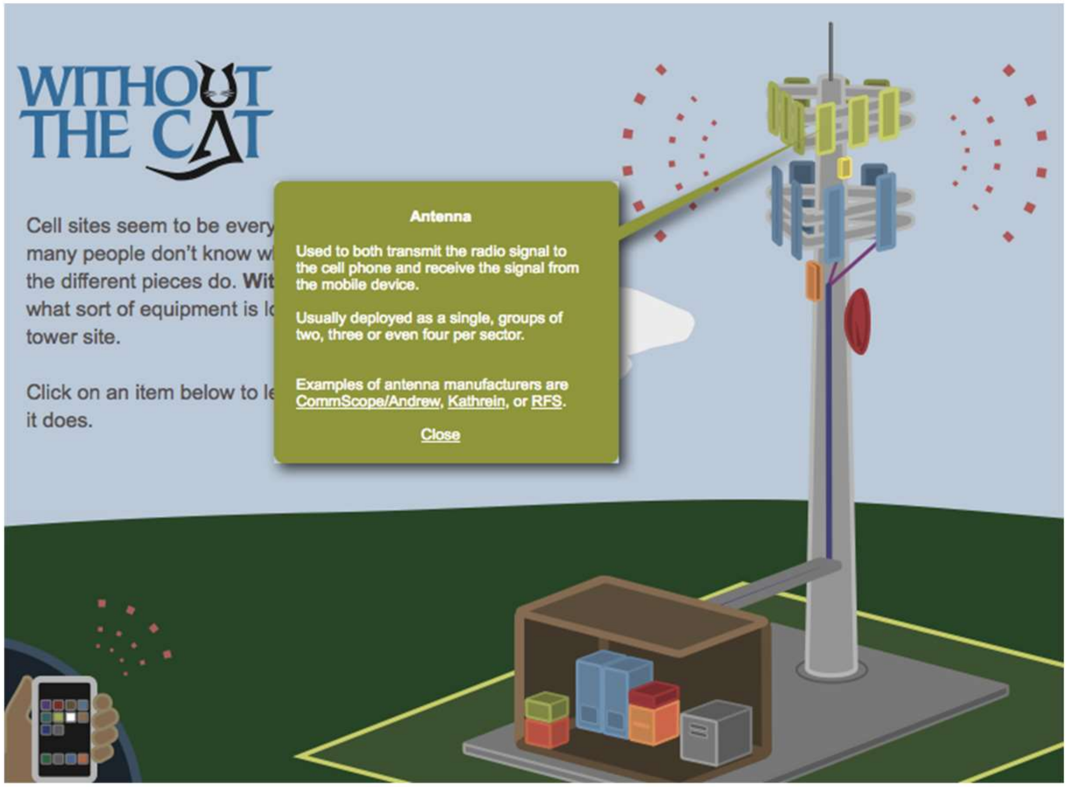
- *** The closest CELL tower does not**
- **have to pick up your signal**



Reviews | Towers

FILTER: ☑ AT&T □ SPRINT □ T-MOBILE □ VERIZON

HTTP://WWW.CELLRECEPTION.COM



Cell sites seem to be every
many people don't know w
the different pieces do. **Wit**
what sort of equipment is l
tower site.

Click on an item below to le
it does.

Antenna

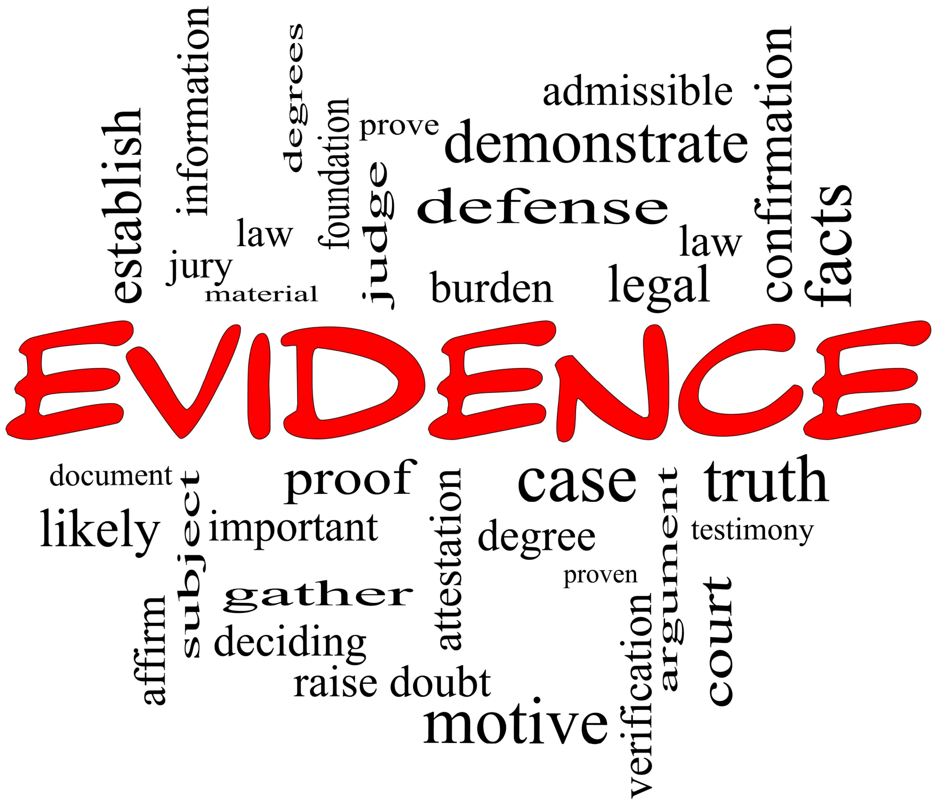
Used to both transmit the radio signal to the cell phone and receive the signal from the mobile device.

Usually deployed as a single, groups of two, three or even four per sector.

Examples of antenna manufacturers are CommScope/Andrew, Kathrein, or RFS.

Close

WITHOUTTHECAT.COM


EVIDENCE
establish
information
degrees
foundation
judge
prove
admissible
demonstrate
defense
confirmation
facts
law
jury
material
burden
law
legal
document
likely
subject
important
proof
gather
deciding
affirm
attestation
raise doubt
case
degree
proven
motive
verification
argument
truth
testimony
court

EVIDENCE ADMISSIBILITY

Evidence Collection

- Follow established legal processes.
- Use accepted and proven techniques and tools.
- Employ certified digital experts.

CHAIN OF CUSTODY

- Chronological Documentation
  - Accounts for location and access of evidence from the time it is collected/seized until the time it is used in a legal or administrative proceeding.

IN GENERAL CHAIN-OF-CUSTODY FOR ELECTRONIC EVIDENCE IS NOT MUCH DIFFERENT THAN OTHER PHYSICAL EVIDENCE – BUT REQUIRES A LOT MORE INFORMATION

CHAIN-OF-CUSTODY

The "sequencing" of the CoC follows this order: identification and collection; analysis; storage; preservation; transportation; presentation in court; return to owner.

The CoC shows: who obtained the evidence; where and when the evidence was obtained; who secured the evidence; who had control or possession of the evidence.

EVIDENCE

- Evidence should be handled according to agency policy while maintaining a chain of custody.
- Network isolation should be maintained.
- Additional forensic analysis may need to be performed:
  - To conduct traditional forensic processes on a mobile phone (DNA, latent prints, etc.).
  - Contact appropriate crime lab personnel for guidance on processing order to avoid the destruction of forensic evidence.

EVIDENCE: FARADAY

- Faraday Bag/Box: Used for digital evidence collection, preservation and examination.
  - Shields digital evidence from cellular, WiFi, Bluetooth and radio frequency (RF) signals.
  - https://edecdf.com/collections/mobile
- Faraday Cage/Tent

FARADAY BAGS/BOXES/CAGES/TENTS

- Evidence
- Preservation
- Examination

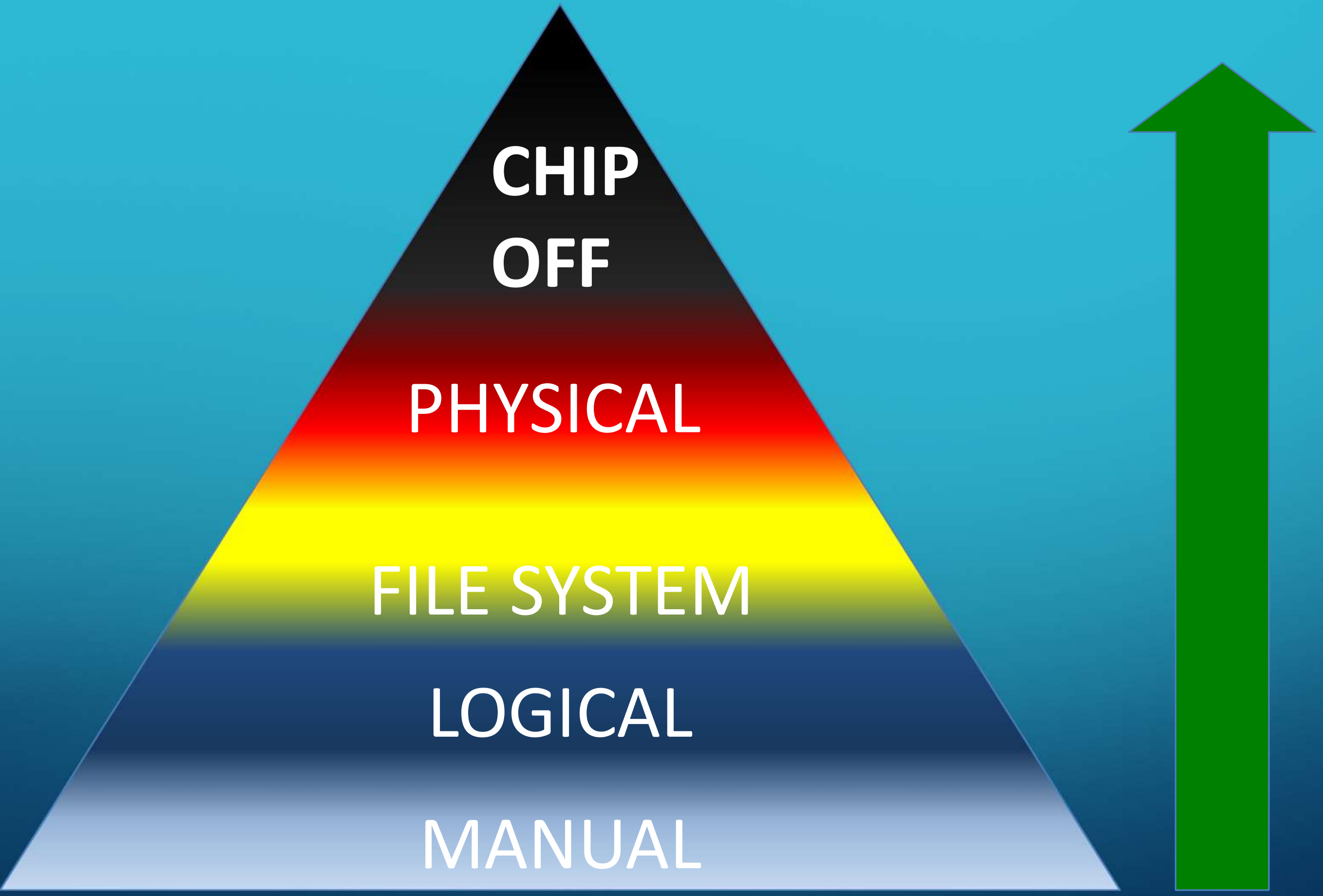
Seizing Evidence

- Review search warrant.
- **“Ask” mobile user for pass codes or PINs.**
- Process Immediately OR Turn off Phone and remove battery?
  - Turning OFF:
    - Preserves call logs and last cell tower location information (LOCI).
    - Prevents overwriting deleted data.
    - Prevents improper mobile phone handling.
    - CON – Removes information from active memory.
    - CON – May make it harder for forensic analysis.

Seizing Evidence

- Locking the phone by password or PIN.
- Many mobile phones can be placed in “Airplane” mode.
    - Not really a great solution – Does not do what people expects
- Collect associated chargers, cables, peripherals, and manuals.

PYRAMID LEVELS OF EXAMINATION

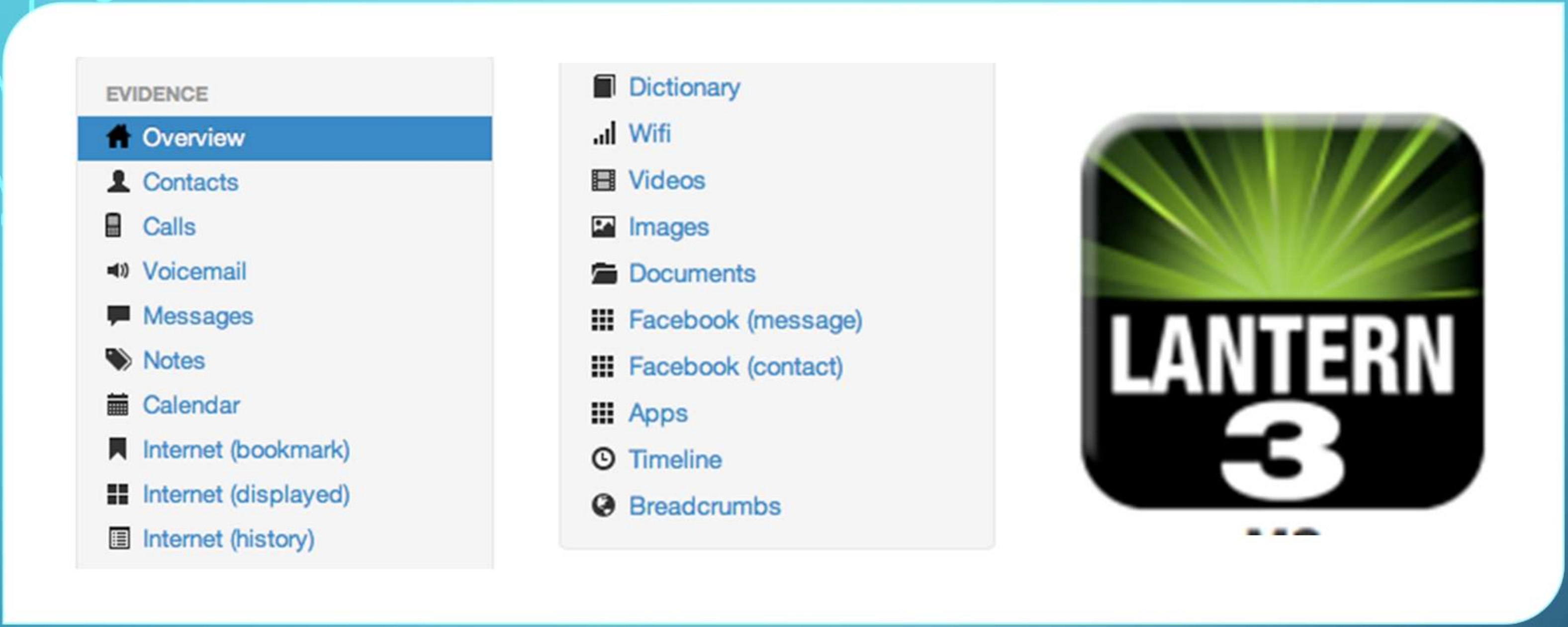


- The higher the level, the more complex
- Tools more $
- Longer analysis times
- More training
- More Invasive

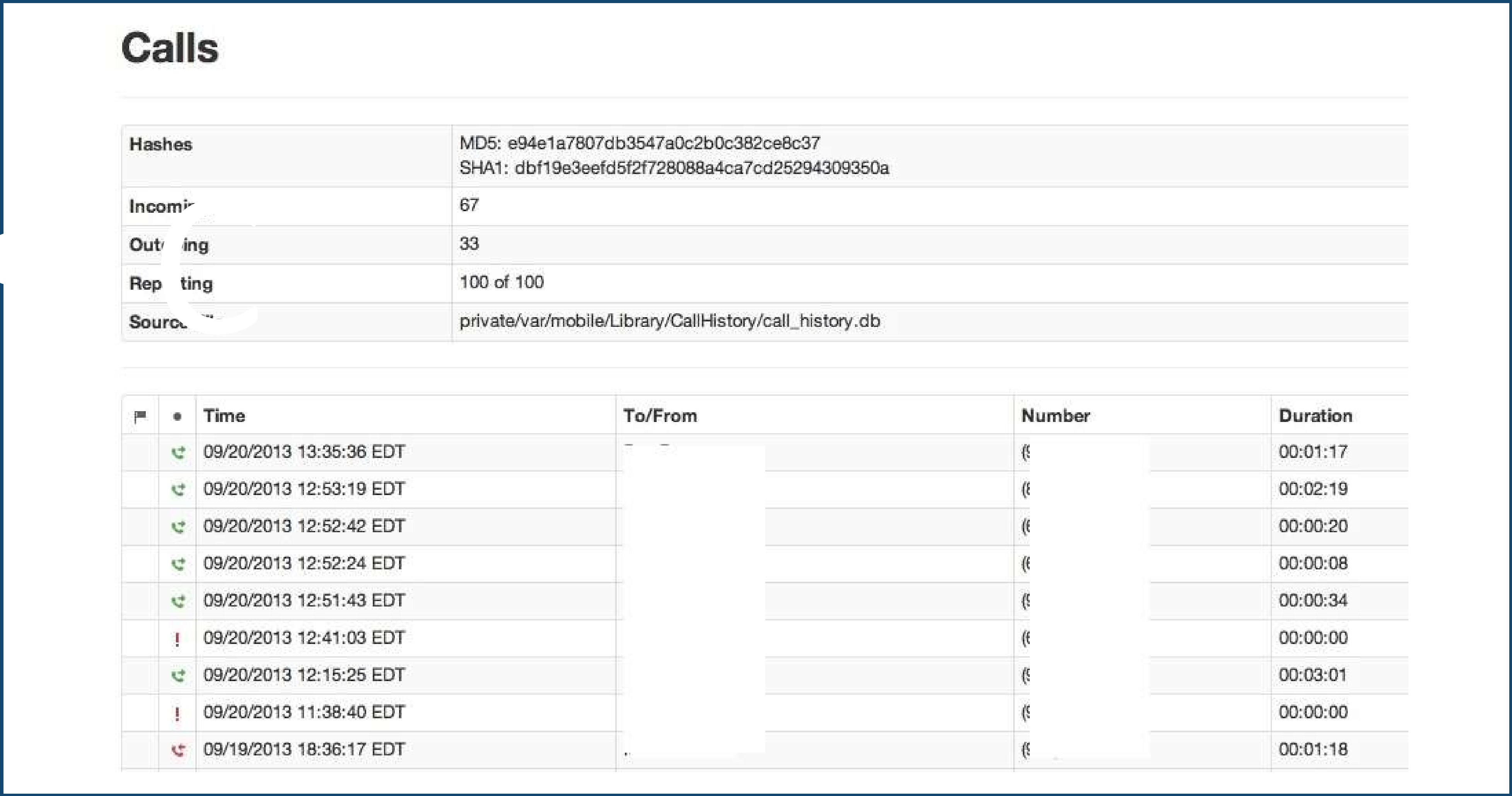
mobileforensics

MOBILE FORENSIC PRODUCTS

- EnCase Mobile Investigator: $???
- AccessData MPE+: $5,000
- Cellebrite UFED Ultimate: $15,000
- Lantern 3: $600
- Oxygen Forensic: $12,000+
- Magnet AXIOM: $1700 + Annual Maintenance
- Cellebrite Advanced Services: $1000 / Phone
- berla.co: Cars & GPS Units


EVIDENCE
Overview
Contacts
Calls
Voicemail
Messages
Notes
Calendar
Internet (bookmark)
Internet (displayed)
Internet (history)
Dictionary
Wifi
Videos
Images
Documents
Facebook (message)
Facebook (contact)
Apps
Timeline
Breadcrumbs
LANTERN
3

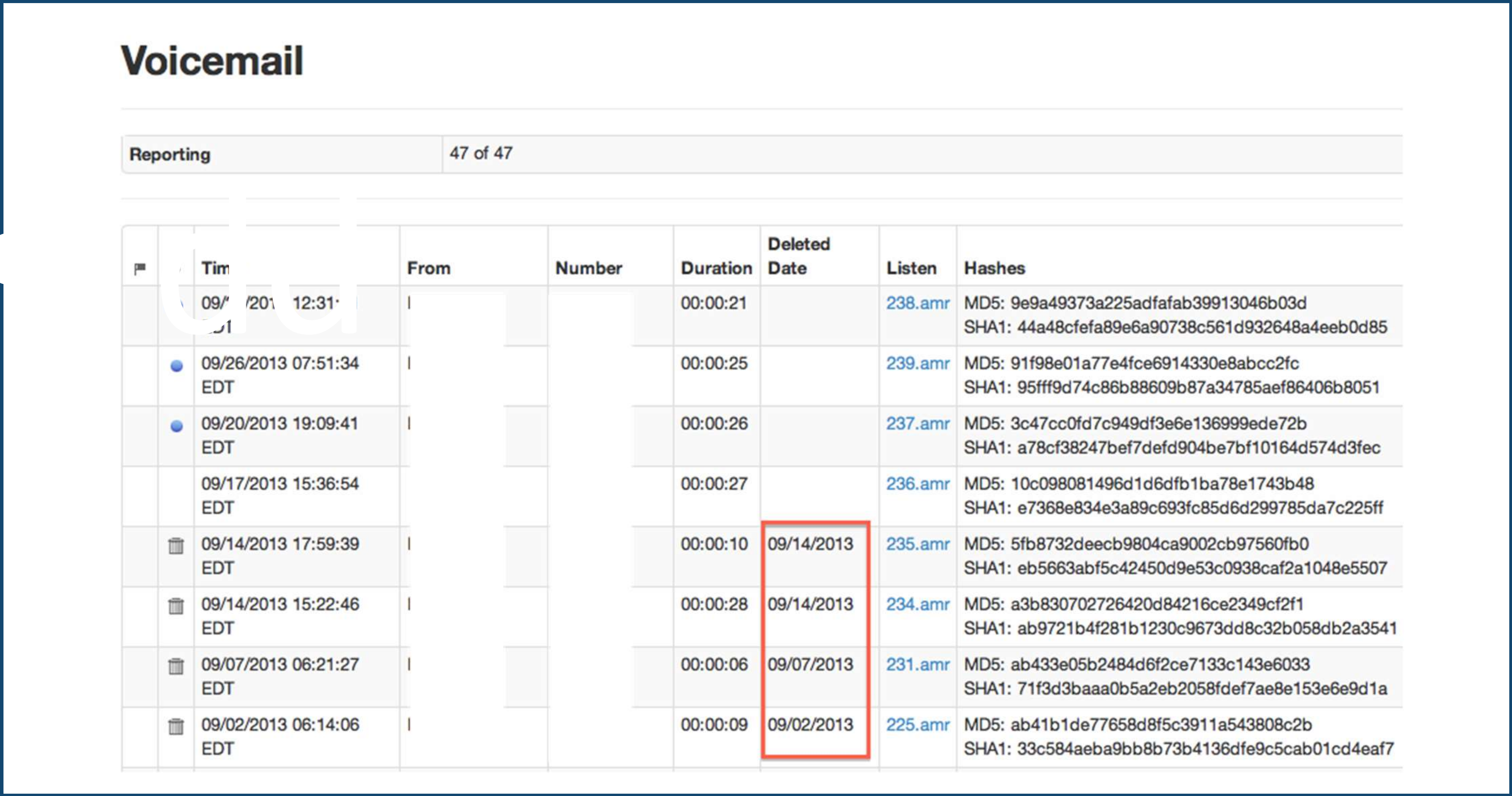
LANTERN3



Calls

Hashes	MD5: e94e1a7807db3547a0c2b0c382ce8c37 SHA1: dbf19e3eefd5f2f728088a4ca7cd25294309350a
Incoming	67
Outgoing	33
Reporting	100 of 100
Source	private/var/mobile/Library/CallHistory/call_history.db

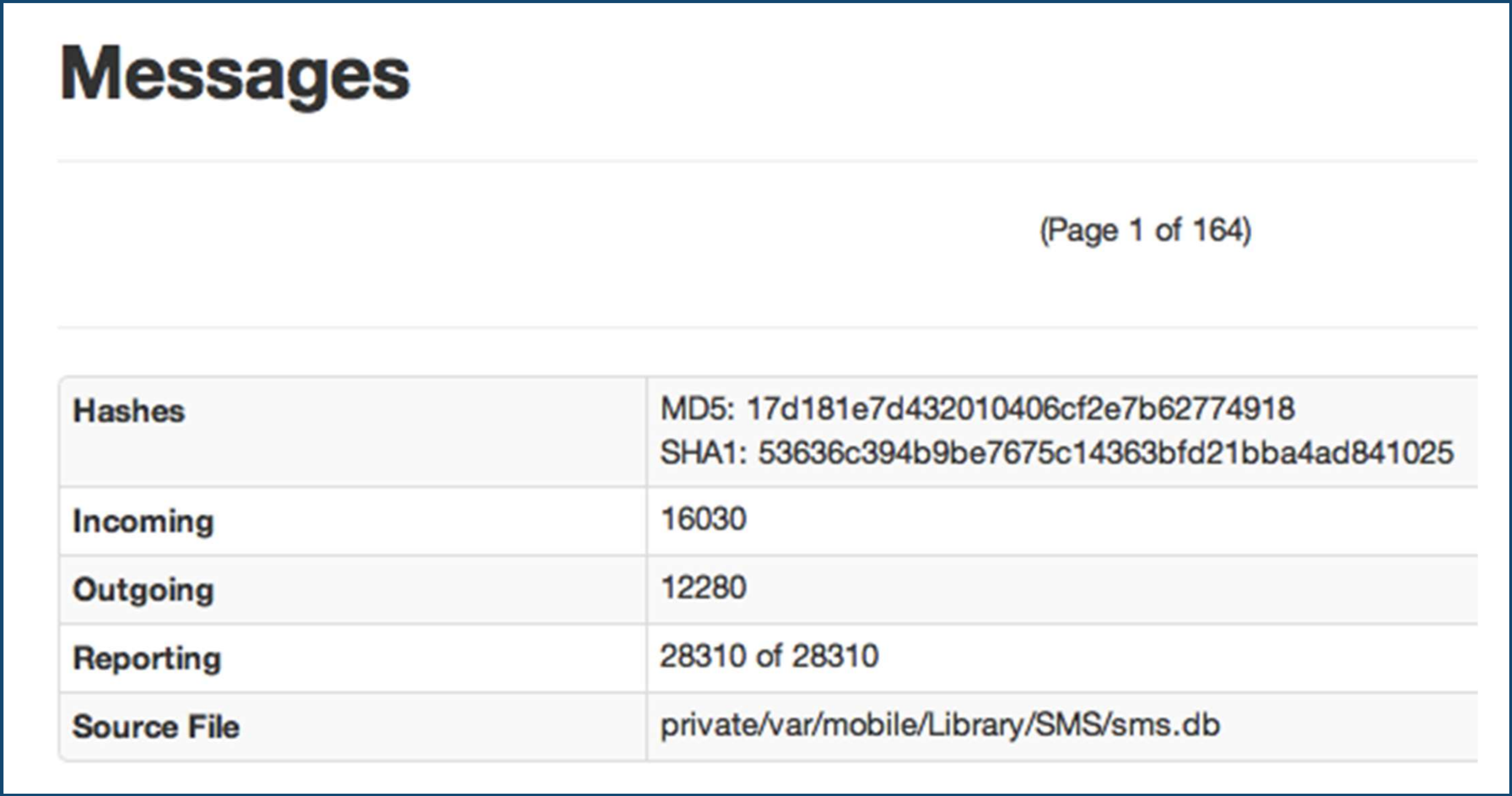
⚑	●	Time	To/From	Number	Duration
	☎	09/20/2013 13:35:36 EDT	[redacted]	([redacted]	00:01:17
	☎	09/20/2013 12:53:19 EDT	[redacted]	([redacted]	00:02:19
	☎	09/20/2013 12:52:42 EDT	[redacted]	([redacted]	00:00:20
	☎	09/20/2013 12:52:24 EDT	[redacted]	([redacted]	00:00:08
	☎	09/20/2013 12:51:43 EDT	[redacted]	([redacted]	00:00:34
	!	09/20/2013 12:41:03 EDT	[redacted]	([redacted]	00:00:00
	☎	09/20/2013 12:15:25 EDT	[redacted]	([redacted]	00:03:01
	!	09/20/2013 11:38:40 EDT	[redacted]	([redacted]	00:00:00
	☎	09/19/2013 18:36:17 EDT	[redacted]	([redacted]	00:01:18



Voicemail

Reporting	47 of 47

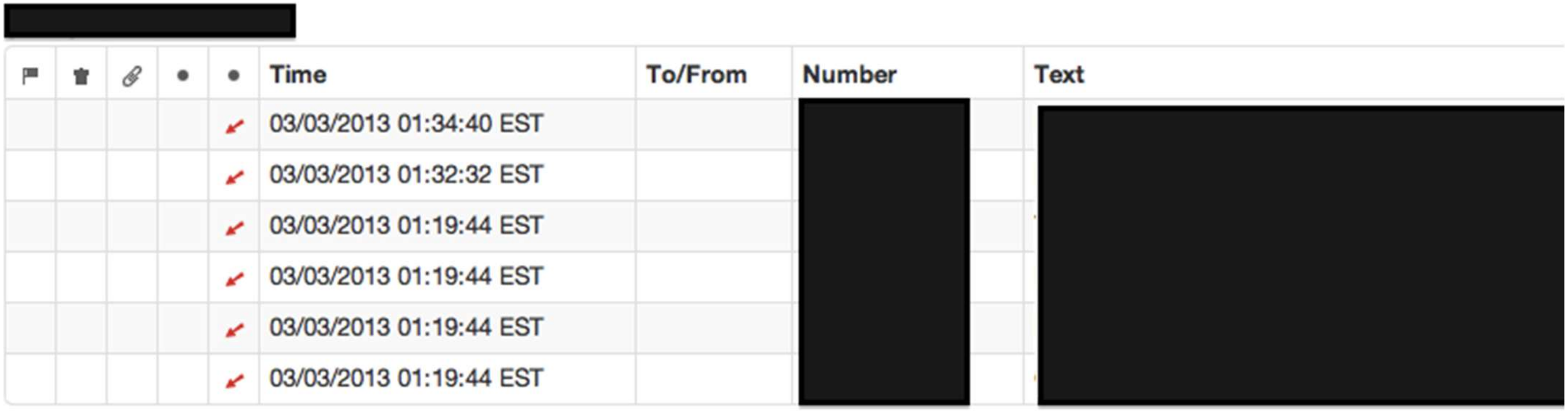
⚑		Tim	From	Number	Duration	Deleted Date	Listen	Hashes
	●	09/[illegible]/201[illegible] 12:31[illegible] EDT	[redacted]	[redacted]	00:00:21		238.amr	MD5: 9e9a49373a225adfafab39913046b03d SHA1: 44a48cfefa89e6a90738c561d932648a4eeb0d85
	●	09/26/2013 07:51:34 EDT	[redacted]	[redacted]	00:00:25		239.amr	MD5: 91f98e01a77e4fce6914330e8abcc2fc SHA1: 95fff9d74c86b88609b87a34785aef86406b8051
	●	09/20/2013 19:09:41 EDT	[redacted]	[redacted]	00:00:26		237.amr	MD5: 3c47cc0fd7c949df3e6e136999ede72b SHA1: a78cf38247bef7defd904be7bf10164d574d3fec
		09/17/2013 15:36:54 EDT	[redacted]	[redacted]	00:00:27		236.amr	MD5: 10c098081496d1d6dfb1ba78e1743b48 SHA1: e7368e834e3a89c693fc85d6d299785da7c225ff
	🗑	09/14/2013 17:59:39 EDT	[redacted]	[redacted]	00:00:10	09/14/2013	235.amr	MD5: 5fb8732deecb9804ca9002cb97560fb0 SHA1: eb5663abf5c42450d9e53c0938caf2a1048e5507
	🗑	09/14/2013 15:22:46 EDT	[redacted]	[redacted]	00:00:28	09/14/2013	234.amr	MD5: a3b830702726420d84216ce2349cf2f1 SHA1: ab9721b4f281b1230c9673dd8c32b058db2a3541
	🗑	09/07/2013 06:21:27 EDT	[redacted]	[redacted]	00:00:06	09/07/2013	231.amr	MD5: ab433e05b2484d6f2ce7133c143e6033 SHA1: 71f3d3baaa0b5a2eb2058fdef7ae8e153e6e9d1a
	🗑	09/02/2013 06:14:06 EDT	[redacted]	[redacted]	00:00:09	09/02/2013	225.amr	MD5: ab41b1de77658d8f5c3911a543808c2b SHA1: 33c584aeba9bb8b73b4136dfe9c5cab01cd4eaf7



Messages

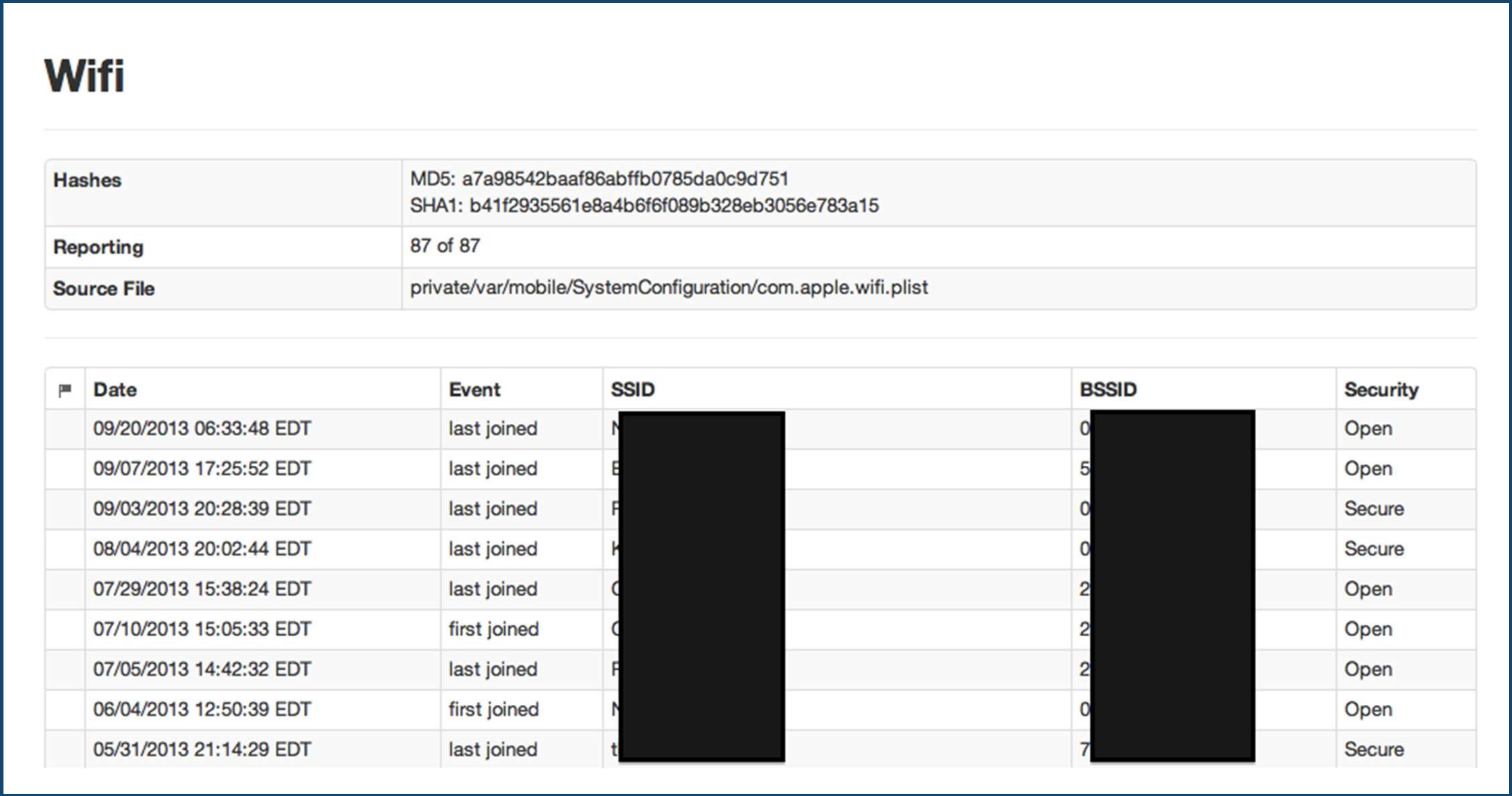
(Page 1 of 164)

Hashes	MD5: 17d181e7d432010406cf2e7b62774918 SHA1: 53636c394b9be7675c14363bfd21bba4ad841025
Incoming	16030
Outgoing	12280
Reporting	28310 of 28310
Source File	private/var/mobile/Library/SMS/sms.db



[redacted]

⚑	🗑	📎	●	●	Time	To/From	Number	Text
				↙	03/03/2013 01:34:40 EST		[redacted]	[redacted]
				↙	03/03/2013 01:32:32 EST		[redacted]	[redacted]
				↙	03/03/2013 01:19:44 EST		[redacted]	[redacted]
				↙	03/03/2013 01:19:44 EST		[redacted]	[redacted]
				↙	03/03/2013 01:19:44 EST		[redacted]	[redacted]
				↙	03/03/2013 01:19:44 EST		[redacted]	[redacted]

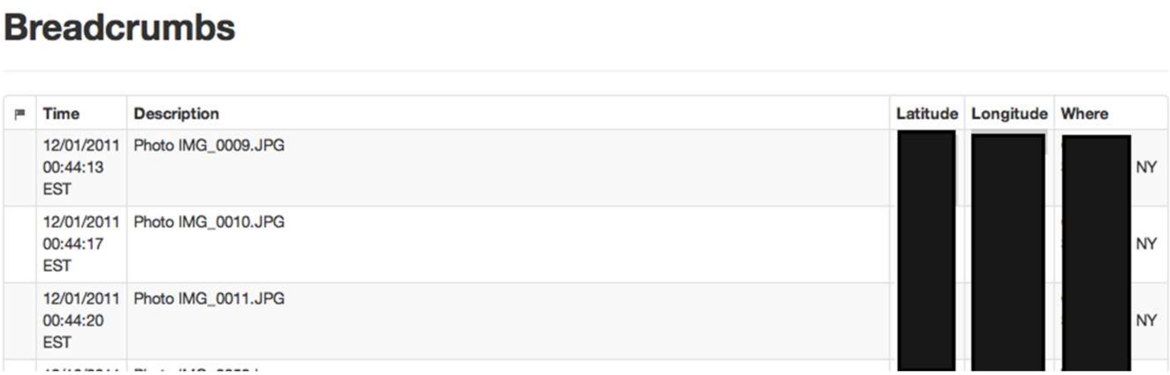


Wifi

Hashes	MD5: a7a98542baaf86abffb0785da0c9d751 SHA1: b41f2935561e8a4b6f6f089b328eb3056e783a15
Reporting	87 of 87
Source File	private/var/mobile/SystemConfiguration/com.apple.wifi.plist

⚑	Date	Event	SSID	BSSID	Security
	09/20/2013 06:33:48 EDT	last joined	[redacted]	[redacted]	Open
	09/07/2013 17:25:52 EDT	last joined	[redacted]	[redacted]	Open
	09/03/2013 20:28:39 EDT	last joined	[redacted]	[redacted]	Secure
	08/04/2013 20:02:44 EDT	last joined	[redacted]	[redacted]	Secure
	07/29/2013 15:38:24 EDT	last joined	[redacted]	[redacted]	Open
	07/10/2013 15:05:33 EDT	first joined	[redacted]	[redacted]	Open
	07/05/2013 14:42:32 EDT	last joined	[redacted]	[redacted]	Open
	06/04/2013 12:50:39 EDT	first joined	[redacted]	[redacted]	Open
	05/31/2013 21:14:29 EDT	last joined	[redacted]	[redacted]	Secure

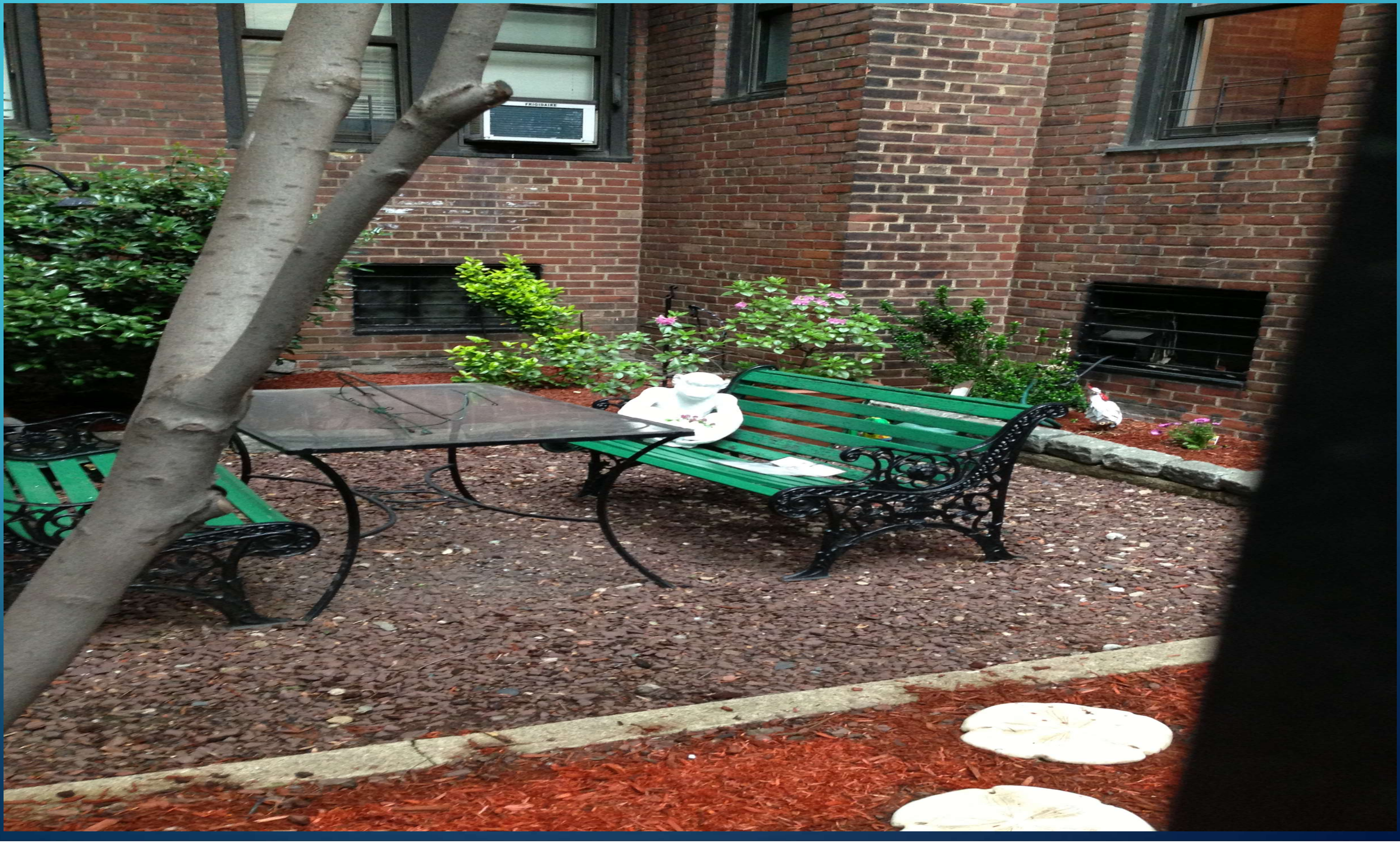
- If Geo-tagging is enabled:
  - Can pinpoint where photo was taken.
  - Copy and paste numbers in Google or Google Earth.

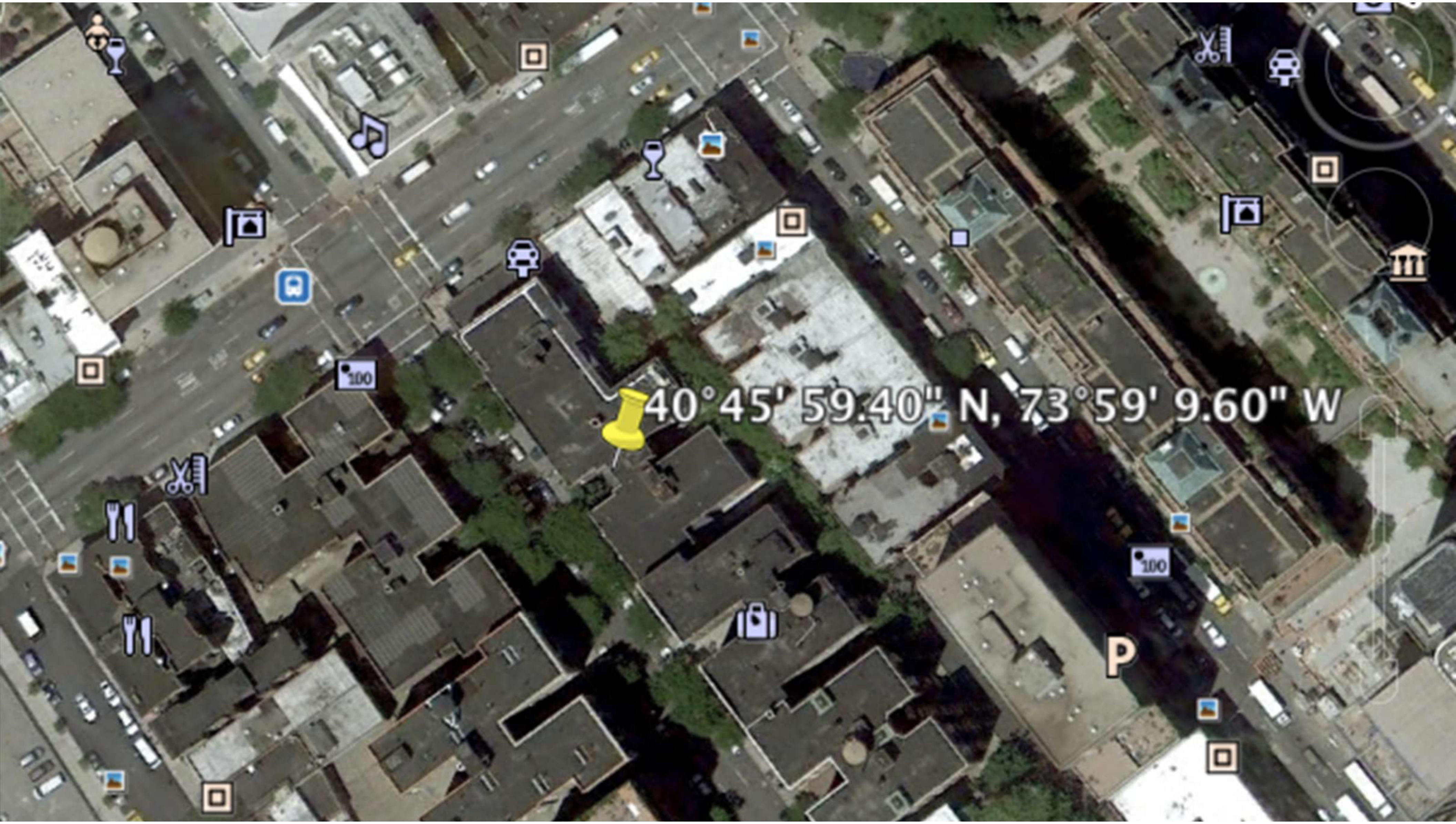


Breadcrumbs

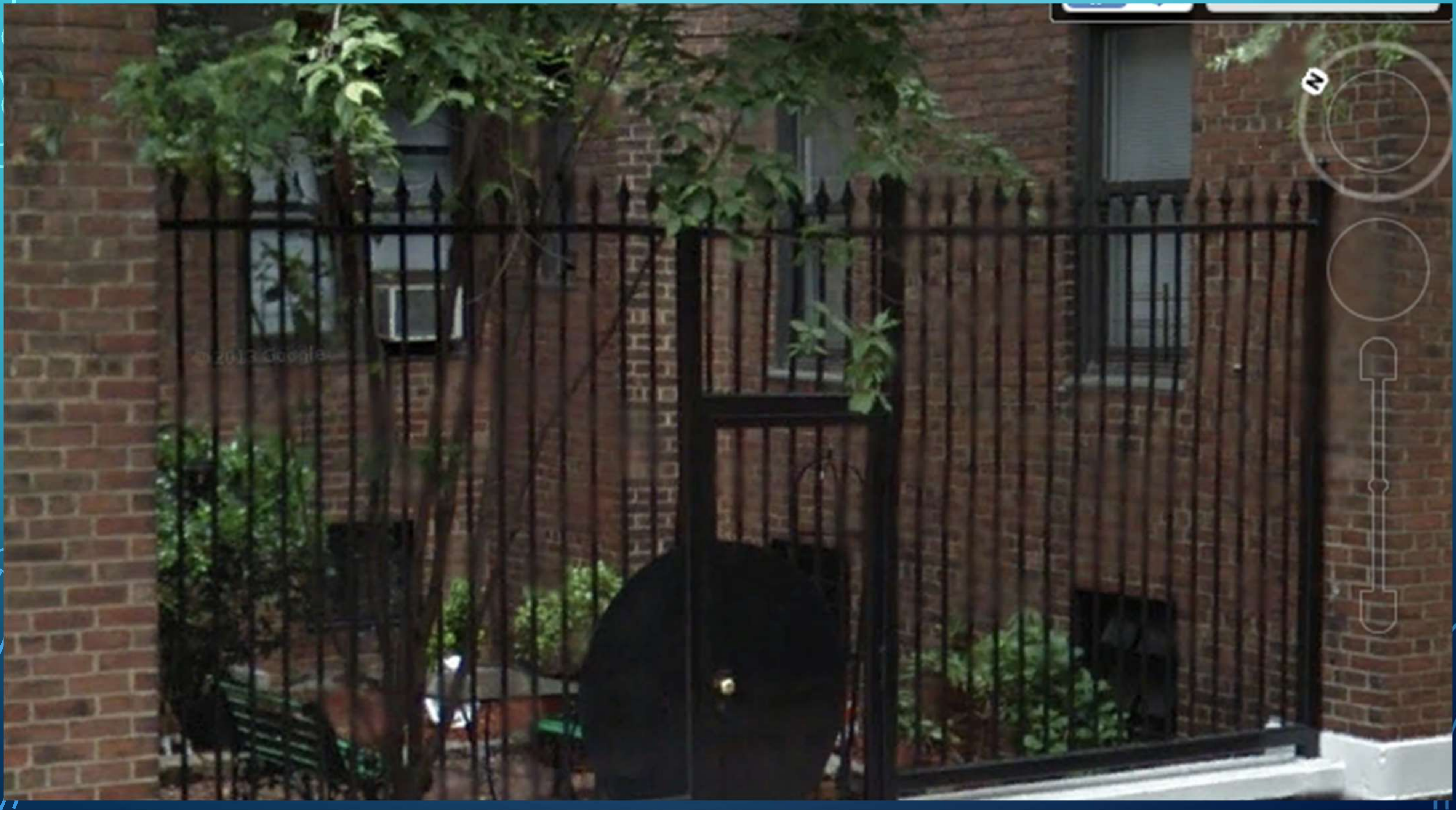
⚑	Time	Description	Latitude	Longitude	Where
	12/01/2011 00:44:13 EST	Photo IMG_0009.JPG	[redacted]	[redacted]	[redacted] NY
	12/01/2011 00:44:17 EST	Photo IMG_0010.JPG	[redacted]	[redacted]	[redacted] NY
	12/01/2011 00:44:20 EST	Photo IMG_0011.JPG	[redacted]	[redacted]	[redacted] NY

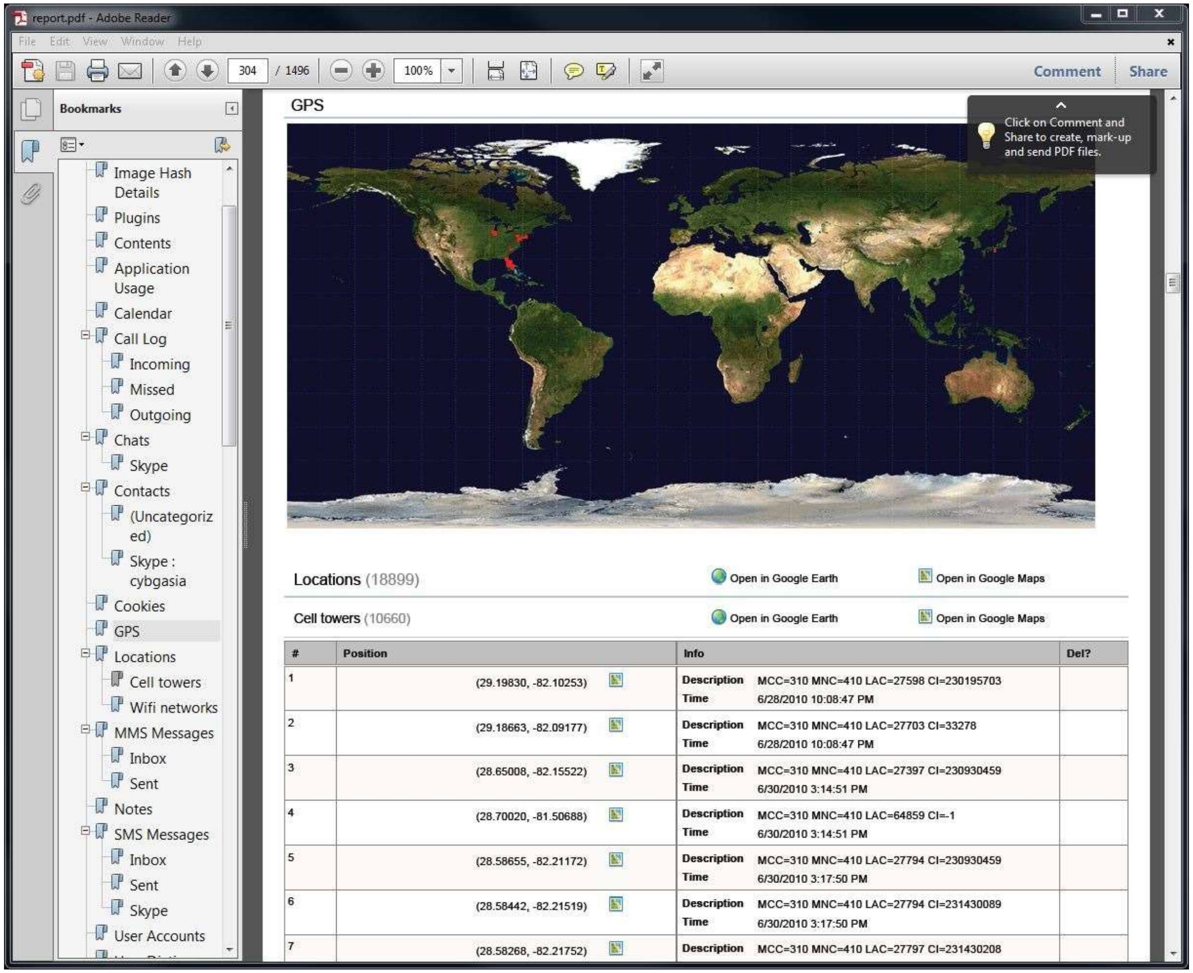
ACTUAL PICTURE




40°45' 59.40" N, 73°59' 9.60" W
100
100
P

PICTURE FROM GOOGLE EARTH





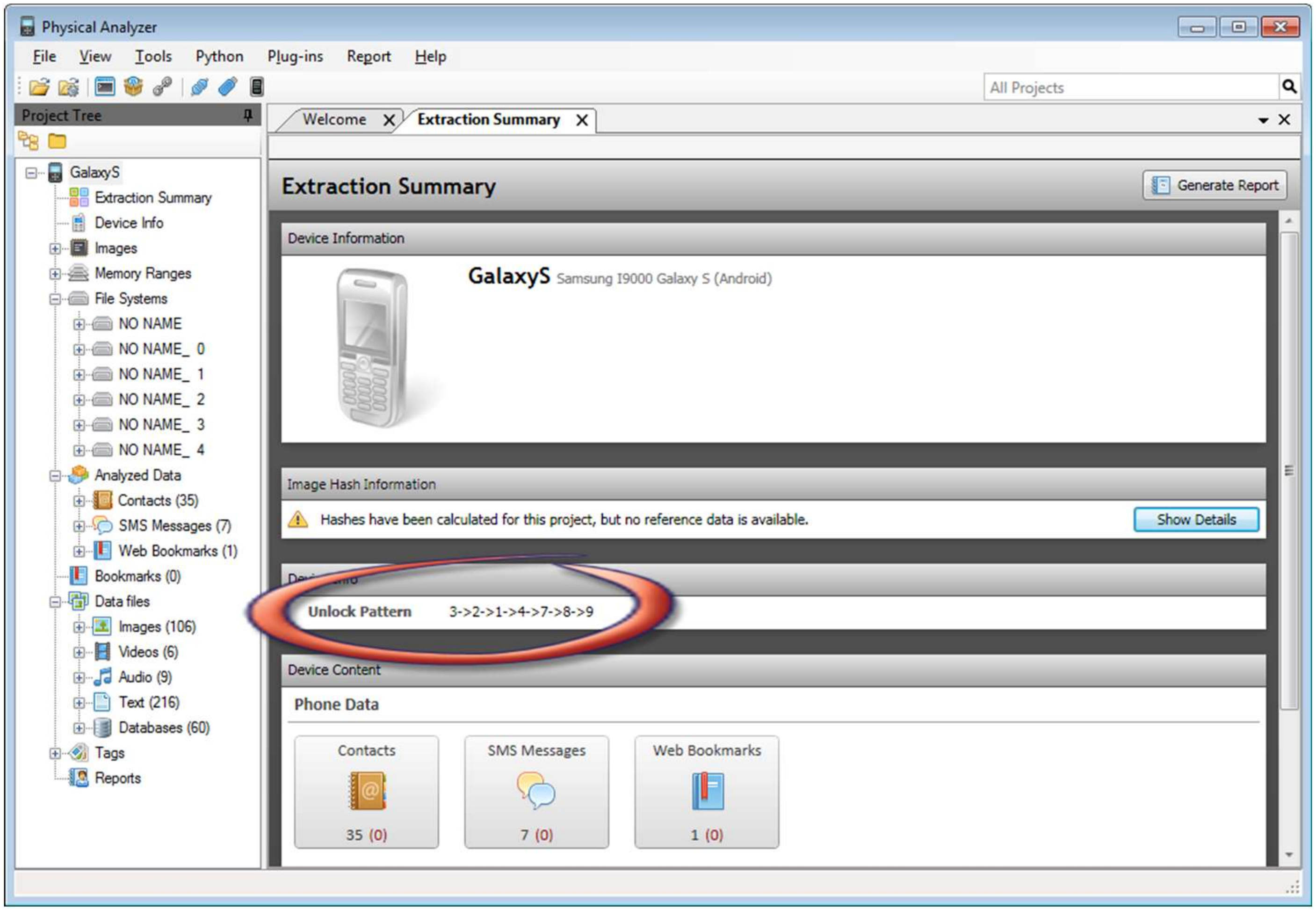
Click on Comment and Share to create, mark-up and send PDF files.

GPS

Locations (18899) Open in Google Earth Open in Google Maps

Cell towers (10660) Open in Google Earth Open in Google Maps

#	Position	Info	Del?
1	(29.19830, -82.10253)	**Description** MCC=310 MNC=410 LAC=27598 CI=230195703 **Time** 6/28/2010 10:08:47 PM	
2	(29.18663, -82.09177)	**Description** MCC=310 MNC=410 LAC=27703 CI=33278 **Time** 6/28/2010 10:08:47 PM	
3	(28.65008, -82.15522)	**Description** MCC=310 MNC=410 LAC=27397 CI=230930459 **Time** 6/30/2010 3:14:51 PM	
4	(28.70020, -81.50688)	**Description** MCC=310 MNC=410 LAC=64859 CI=-1 **Time** 6/30/2010 3:14:51 PM	
5	(28.58655, -82.21172)	**Description** MCC=310 MNC=410 LAC=27794 CI=230930459 **Time** 6/30/2010 3:17:50 PM	
6	(28.58442, -82.21519)	**Description** MCC=310 MNC=410 LAC=27794 CI=231430089 **Time** 6/30/2010 3:17:50 PM	
7	(28.58268, -82.21752)	**Description** MCC=310 MNC=410 LAC=27797 CI=231430208	



Extraction Summary

Device Information

GalaxyS Samsung I9000 Galaxy S (Android)

Image Hash Information

⚠ Hashes have been calculated for this project, but no reference data is available.

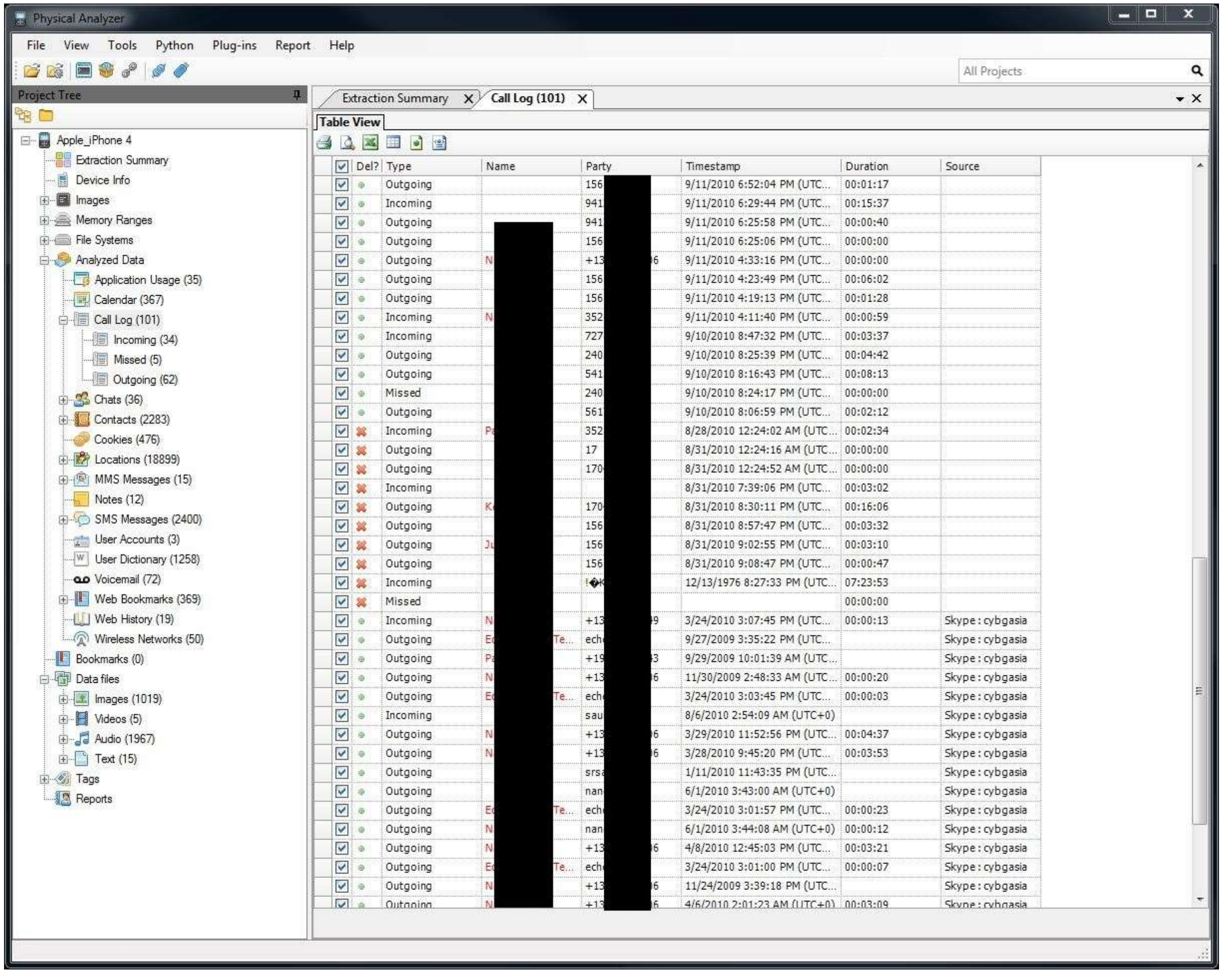
Device Info

Unlock Pattern 3->2->1->4->7->8->9

Device Content

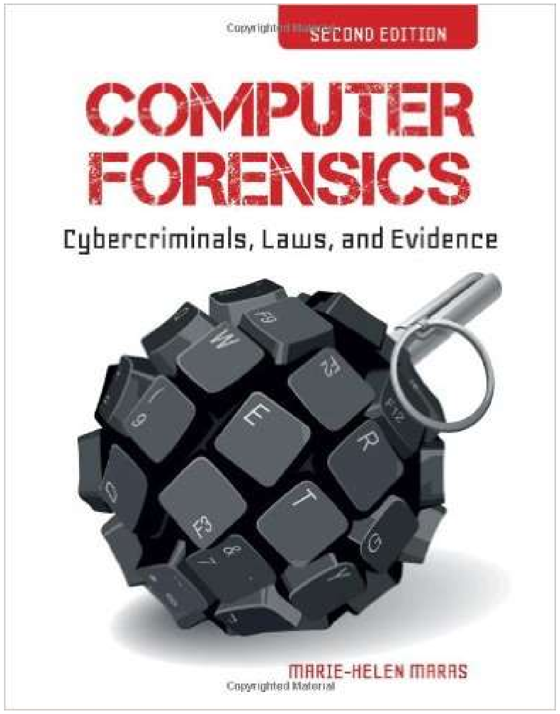
Phone Data

Contacts	SMS Messages	Web Bookmarks
35 (0)	7 (0)	1 (0)



- Apple_iPhone 4
  - Extraction Summary
  - Device Info
  - Images
  - Memory Ranges
  - File Systems
  - Analyzed Data
    - Application Usage (35)
    - Calendar (367)
    - Call Log (101)
      - Incoming (34)
      - Missed (5)
      - Outgoing (62)
    - Chats (36)
    - Contacts (2283)
    - Cookies (476)
    - Locations (18899)
    - MMS Messages (15)
    - Notes (12)
    - SMS Messages (2400)
    - User Accounts (3)
    - User Dictionary (1258)
    - Voicemail (72)
    - Web Bookmarks (369)
    - Web History (19)
    - Wireless Networks (50)
  - Bookmarks (0)
  - Data files
    - Images (1019)
    - Videos (5)
    - Audio (1967)
    - Text (15)
  - Tags
  - Reports

☑	Del?	Type	Name	Party	Timestamp	Duration	Source
☑	●	Outgoing		[redacted]	9/11/2010 6:52:04 PM (UTC...	00:01:17	
☑	●	Incoming		[redacted]	9/11/2010 6:29:44 PM (UTC...	00:15:37	
☑	●	Outgoing	[redacted]	[redacted]	9/11/2010 6:25:58 PM (UTC...	00:00:40	
☑	●	Outgoing	[redacted]	[redacted]	9/11/2010 6:25:06 PM (UTC...	00:00:00	
☑	●	Outgoing	[redacted]	[redacted]	9/11/2010 4:33:16 PM (UTC...	00:00:00	
☑	●	Outgoing	[redacted]	[redacted]	9/11/2010 4:23:49 PM (UTC...	00:06:02	
☑	●	Outgoing	[redacted]	[redacted]	9/11/2010 4:19:13 PM (UTC...	00:01:28	
☑	●	Incoming	[redacted]	[redacted]	9/11/2010 4:11:40 PM (UTC...	00:00:59	
☑	●	Incoming	[redacted]	[redacted]	9/10/2010 8:47:32 PM (UTC...	00:03:37	
☑	●	Outgoing	[redacted]	[redacted]	9/10/2010 8:25:39 PM (UTC...	00:04:42	
☑	●	Outgoing	[redacted]	[redacted]	9/10/2010 8:16:43 PM (UTC...	00:08:13	
☑	●	Missed	[redacted]	[redacted]	9/10/2010 8:24:17 PM (UTC...	00:00:00	
☑	●	Outgoing	[redacted]	[redacted]	9/10/2010 8:06:59 PM (UTC...	00:02:12	
☑	✖	Incoming	[redacted]	[redacted]	8/28/2010 12:24:02 AM (UTC...	00:02:34	
☑	✖	Outgoing	[redacted]	[redacted]	8/31/2010 12:24:16 AM (UTC...	00:00:00	
☑	✖	Outgoing	[redacted]	[redacted]	8/31/2010 12:24:52 AM (UTC...	00:00:00	
☑	✖	Incoming	[redacted]	[redacted]	8/31/2010 7:39:06 PM (UTC...	00:03:02	
☑	✖	Outgoing	[redacted]	[redacted]	8/31/2010 8:30:11 PM (UTC...	00:16:06	
☑	✖	Outgoing	[redacted]	[redacted]	8/31/2010 8:57:47 PM (UTC...	00:03:32	
☑	✖	Outgoing	[redacted]	[redacted]	8/31/2010 9:02:55 PM (UTC...	00:03:10	
☑	✖	Outgoing	[redacted]	[redacted]	8/31/2010 9:08:47 PM (UTC...	00:00:47	
☑	✖	Incoming	[redacted]	[redacted]	12/13/1976 8:27:33 PM (UTC...	07:23:53	
☑	✖	Missed	[redacted]	[redacted]		00:00:00	
☑	●	Incoming	[redacted]	[redacted]	3/24/2010 3:07:45 PM (UTC...	00:00:13	Skype : cybgasia
☑	●	Outgoing	[redacted]	[redacted]	9/27/2009 3:35:22 PM (UTC...		Skype : cybgasia
☑	●	Outgoing	[redacted]	[redacted]	9/29/2009 10:01:39 AM (UTC...		Skype : cybgasia
☑	●	Outgoing	[redacted]	[redacted]	11/30/2009 2:48:33 AM (UTC...	00:00:20	Skype : cybgasia
☑	●	Outgoing	[redacted]	[redacted]	3/24/2010 3:03:45 PM (UTC...	00:00:03	Skype : cybgasia
☑	●	Incoming	[redacted]	[redacted]	8/6/2010 2:54:09 AM (UTC+0)		Skype : cybgasia
☑	●	Outgoing	[redacted]	[redacted]	3/29/2010 11:52:56 PM (UTC...	00:04:37	Skype : cybgasia
☑	●	Outgoing	[redacted]	[redacted]	3/28/2010 9:45:20 PM (UTC...	00:03:53	Skype : cybgasia
☑	●	Outgoing	[redacted]	[redacted]	1/11/2010 11:43:35 PM (UTC...		Skype : cybgasia
☑	●	Outgoing	[redacted]	[redacted]	6/1/2010 3:43:00 AM (UTC+0)		Skype : cybgasia
☑	●	Outgoing	[redacted]	[redacted]	3/24/2010 3:01:57 PM (UTC...	00:00:23	Skype : cybgasia
☑	●	Outgoing	[redacted]	[redacted]	6/1/2010 3:44:08 AM (UTC+0)	00:00:12	Skype : cybgasia
☑	●	Outgoing	[redacted]	[redacted]	4/8/2010 12:45:03 PM (UTC...	00:03:21	Skype : cybgasia
☑	●	Outgoing	[redacted]	[redacted]	3/24/2010 3:01:00 PM (UTC...	00:00:07	Skype : cybgasia
☑	●	Outgoing	[redacted]	[redacted]	11/24/2009 3:39:18 PM (UTC...		Skype : cybgasia
☑	●	Outgoing	[redacted]	[redacted]	4/6/2010 2:01:23 AM (UTC+0)	00:03:09	Skype : cybgasia



MARIE-HELEN MARAS
ISBN-13: 978-1449692223

CERTIFIED INSPECTOR GENERAL INVESTIGATOR

DIGITAL EVIDENCE

JOHN JAY COLLEGE OF CRIMINAL JUSTICE

ASSOCIATION OF INSPECTORS GENERAL
Founded October 26, 1996, Carpenters' Hall, Philadelphia, PA

ADAM SCOTT WANDT, J.D., M.P.A.
ASSISTANT PROFESSOR OF PUBLIC POLICY
JOHN JAY COLLEGE OF CRIMINAL JUSTICE

awandt@jjay.cuny.edu **http://wandt.us**

CERTIFIED INSPECTOR GENERAL INVESTIGATOR

SOCIAL MEDIA & CLOUD FORENSICS

JOHN JAY COLLEGE OF CRIMINAL JUSTICE

ASSOCIATION OF INSPECTORS GENERAL
Founded October 26, 1996, Carpenters' Hall, Philadelphia, PA

ADAM SCOTT WANDT, J.D., M.P.A.
ASSISTANT PROFESSOR OF PUBLIC POLICY
JOHN JAY COLLEGE OF CRIMINAL JUSTICE

awandt@jjay.cuny.edu **http://wandt.us**

The materials discussed in this presentation are for informational and training purposes only and not for the purpose of providing legal advice.

You should contact your agency attorney to obtain advice with respect to any particular issue or problem.

ADAM SCOTT WANDT

ASSISTANT PROFESSOR OF PUBLIC POLICY
JOHN JAY COLLEGE OF CRIMINAL JUSTICE

ATTORNEY AND COUNSELOR AT LAW
(NEW YORK STATE)

CO-CHAIR NYC BAR ASSOCIATION:
TECHNOLOGY, CYBER & PRIVACY LAW COMMITTEE

FORMER SWORN LAW ENFORCEMENT OFFICER

INSTRUCTOR:
ASSOCIATION OF INSPECTORS' GENERAL

MASTER SCUBA DIVER
UNDERWATER PHOTOGRAPHER

https://wandt.us

wandt.us/aig

CURRICULUM
EDUCATE
CERTIFICATE
EXPERIENCE
INTELLIGENT THEORY LESSON LEARNING BOOKS TRAINING
SUCCESS KNOWLEDGE
PRACTICE
LEARN
TEACH
UNIVERSITY
SUCCESS
TRAINING
STUDY
BOOKS
COMMUNITY
COLLEGE
CULTURE
LEARNING
BACHELOR COURSES
PROGRAM
EXPERIENCE
COMMUNITY
BOOKS
CULTURE
TRAINING

LEARNING OBJECTIVES

- Understand how social media plays key rolls in today’s investigations.
- Understand what types of evidence may be preserved on social media
- Understand the difference between OSINT and legal process investigations.
- Understand the value and basic concepts involved in geofencing.
- Get basic exposure to cloud forensics and understand why it is so difficult to conduct advanced cloud-based investigations.

gang
query
phone
analyst
without
answ
breakthr
much
versus
suspects
consider
forum
replace
good
queries
dots
analysts
Social
calls
exchange
reporting
latter
different
investigative
post
mirror
answer
media's
entered
members
resources
radios
threats
true
colleagues
data
social
summary
relevance
subscribe
valid
indefinitely
patterns
technique
Thinking
distinction
processes
faster
everything
analyzing
still
introducing
Program
police
protocols
regulations
need
questions
group
products
applications
ask
reports
powerful
professionals
email
case
cops
law
useful
clues
stored
relevant
searchable
discussion
investigation
sit
knowledge
example
analysis
investigator
needs
use
inaccessible
Twitter
cars
rearview
dozens
frequently
hoping
communication
tools
collect
cases
creation
using
information
handling
ways
might
communicating
essential
sure
now
question
make
discussions
connect
valuable
enforcement
conform
forgotten
Studies
Intelligence
regional
high
change
marks
tried
future
intelligence
via
available
needing
chime-in
progress
get
Analysts
However
written
facilitate
spray
trends
talking
related
often
work
patrol
repository
like
technology
sites
media
threat
logo
similar
benefit

SOCIAL MEDIA: USE IN LAW ENFORCEMENT

- (LexisNexis® Risk Solutions, 2016)

- Four (4) out of five (5) respondents actively use social media as a tool in investigations.
- Most common uses include:
  - Identifying people and locations.
  - Discovering criminal activity and locations.
  - Gathering evidence and statements.
- Facebook and YouTube are the most widely used platforms for investigations. (Instagram & Snapchat)

SURVEY OF LAW ENFORCEMENT PROFESSIONALS

25% use social media daily for investigations.

73% believe social media helps solve crimes faster.

According to respondents, search warrants utilizing social media to establish probable cause holds up in court when challenged 87% of the time.

Over half (52%) of agencies still don’t have a formal process for using social media for investigations.

Less than 20% of respondents learned how to use social media for investigations through formal training at agency or training.

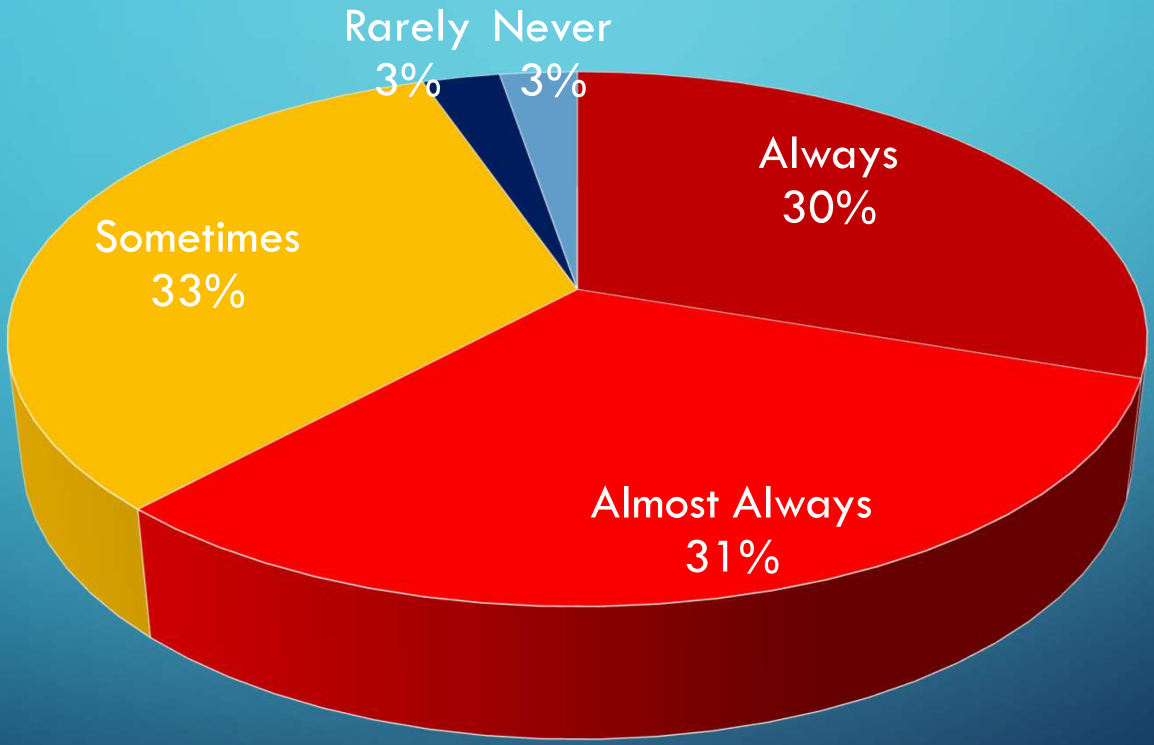
WELCOME TO THE

ASSOCIATION OF INSPECTORS GENERAL ANNUAL MEETING SURVEY

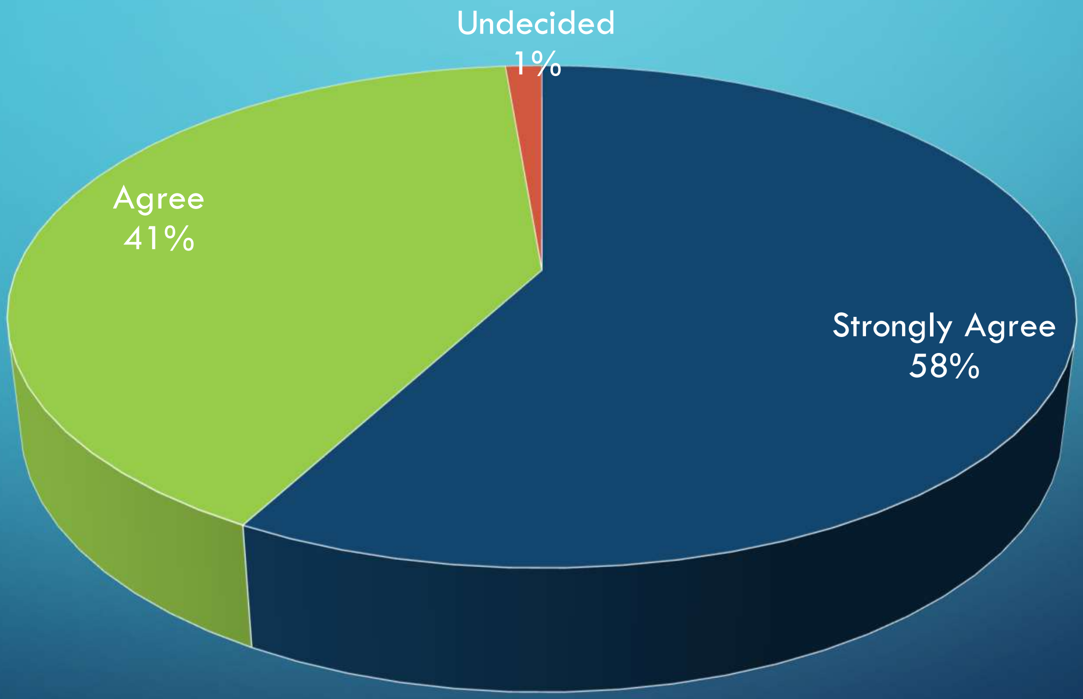
2022

N = 76

HOW OFTEN DO YOU SEARCH SOCIAL MEDIA FOR EVIDENCE RELATED TO A CRIME OR ADMINISTRATIVE PROCEEDING ON A CASE YOU ARE ASSIGNED TO INVESTIGATE?



SOCIAL MEDIA IS A VALUABLE TOOL IN INVESTIGATING CRIMES


Undecided
Agree
Strongly Agree