



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



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

	Time	From	Number	Duration	Deleted Date	Listen	Hashes
	09/17/2013 12:31:01			00:00:21		238.amr	MD5: 9e9a49373a225adfafab39913046b03d SHA1: 44a48cfefa89e6a90738c561d932648a4eeb0d85
	09/26/2013 07:51:34 EDT			00:00:25		239.amr	MD5: 91f98e01a77e4fce6914330e8abcc2fc SHA1: 95fff9d74c86b88609b87a34785aef86406b8051
	09/20/2013 19:09:41 EDT			00:00:26		237.amr	MD5: 3c47cc0fd7c949df3e6e136999ede72b SHA1: a78cf38247bef7defd904be7bf10164d574d3fec
	09/17/2013 15:36:54 EDT			00:00:27		236.amr	MD5: 10c098081496d1d6dfb1ba78e1743b48 SHA1: e7368e834e3a89c693fc85d6d299785da7c225ff
	09/14/2013 17:59:39 EDT			00:00:10	09/14/2013	235.amr	MD5: 5fb8732deecb9804ca9002cb97560fb0 SHA1: eb5663abf5c42450d9e53c0938caf2a1048e5507
	09/14/2013 15:22:46 EDT			00:00:28	09/14/2013	234.amr	MD5: a3b830702726420d84216ce2349cf2f1 SHA1: ab9721b4f281b1230c9673dd8c32b058db2a3541
	09/07/2013 06:21:27 EDT			00:00:06	09/07/2013	231.amr	MD5: ab433e05b2484d6f2ce7133c143e6033 SHA1: 71f3d3baaa0b5a2eb2058fdef7ae8e153e6e9d1a
	09/02/2013 06:14:06 EDT			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	N [REDACTED]	0 [REDACTED]	Open
	09/07/2013 17:25:52 EDT	last joined	E [REDACTED]	5 [REDACTED]	Open
	09/03/2013 20:28:39 EDT	last joined	F [REDACTED]	0 [REDACTED]	Secure
	08/04/2013 20:02:44 EDT	last joined	K [REDACTED]	0 [REDACTED]	Secure
	07/29/2013 15:38:24 EDT	last joined	C [REDACTED]	2 [REDACTED]	Open
	07/10/2013 15:05:33 EDT	first joined	C [REDACTED]	2 [REDACTED]	Open
	07/05/2013 14:42:32 EDT	last joined	F [REDACTED]	2 [REDACTED]	Open
	06/04/2013 12:50:39 EDT	first joined	N [REDACTED]	0 [REDACTED]	Open
	05/31/2013 21:14:29 EDT	last joined	t [REDACTED]	7 [REDACTED]	Secure

- If Geo-tagging is enabled:

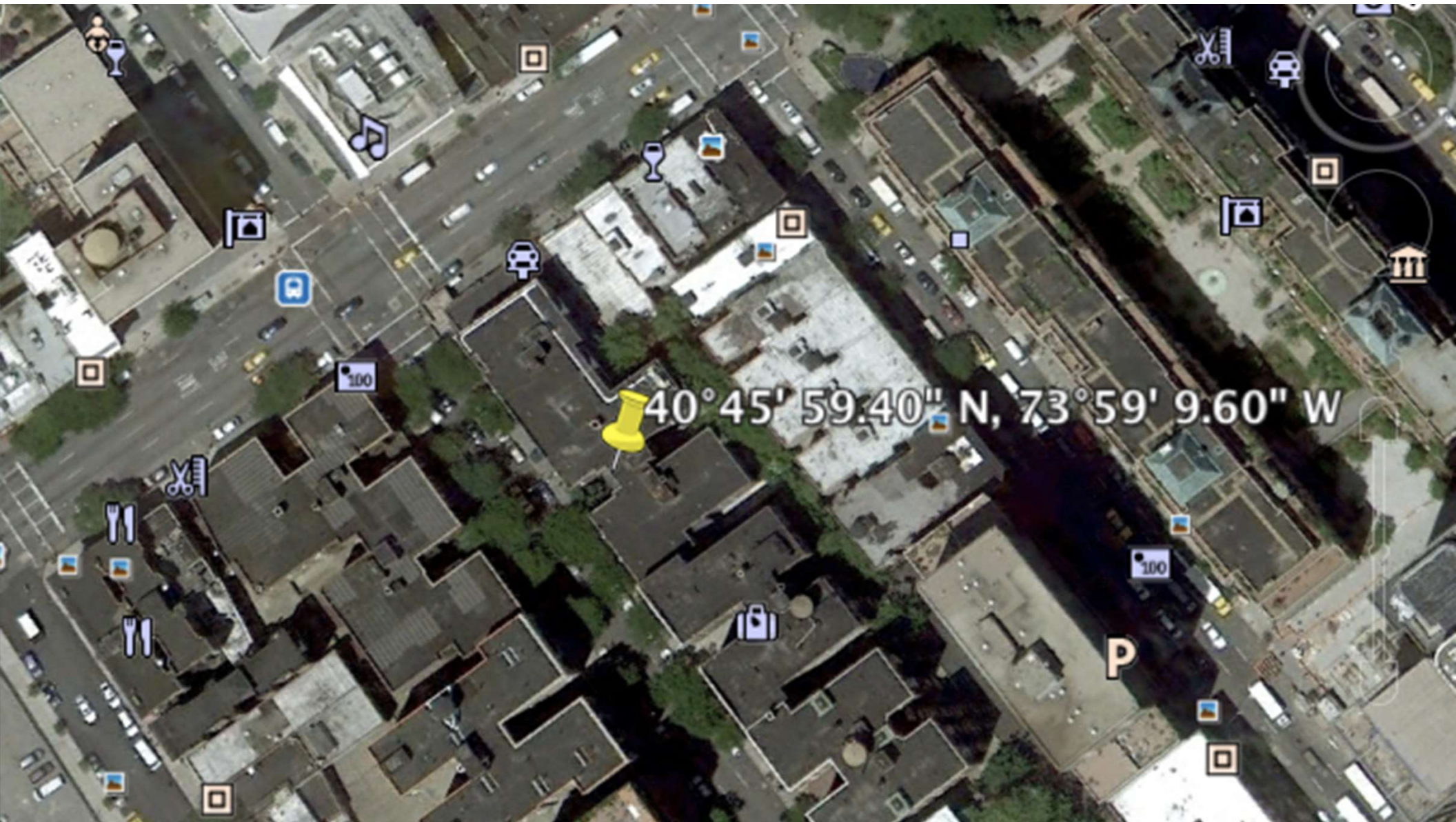
- Can pinpoint where photo was taken.
- Copy and paste numbers in Google or Google Earth.

Breadcrumbs

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

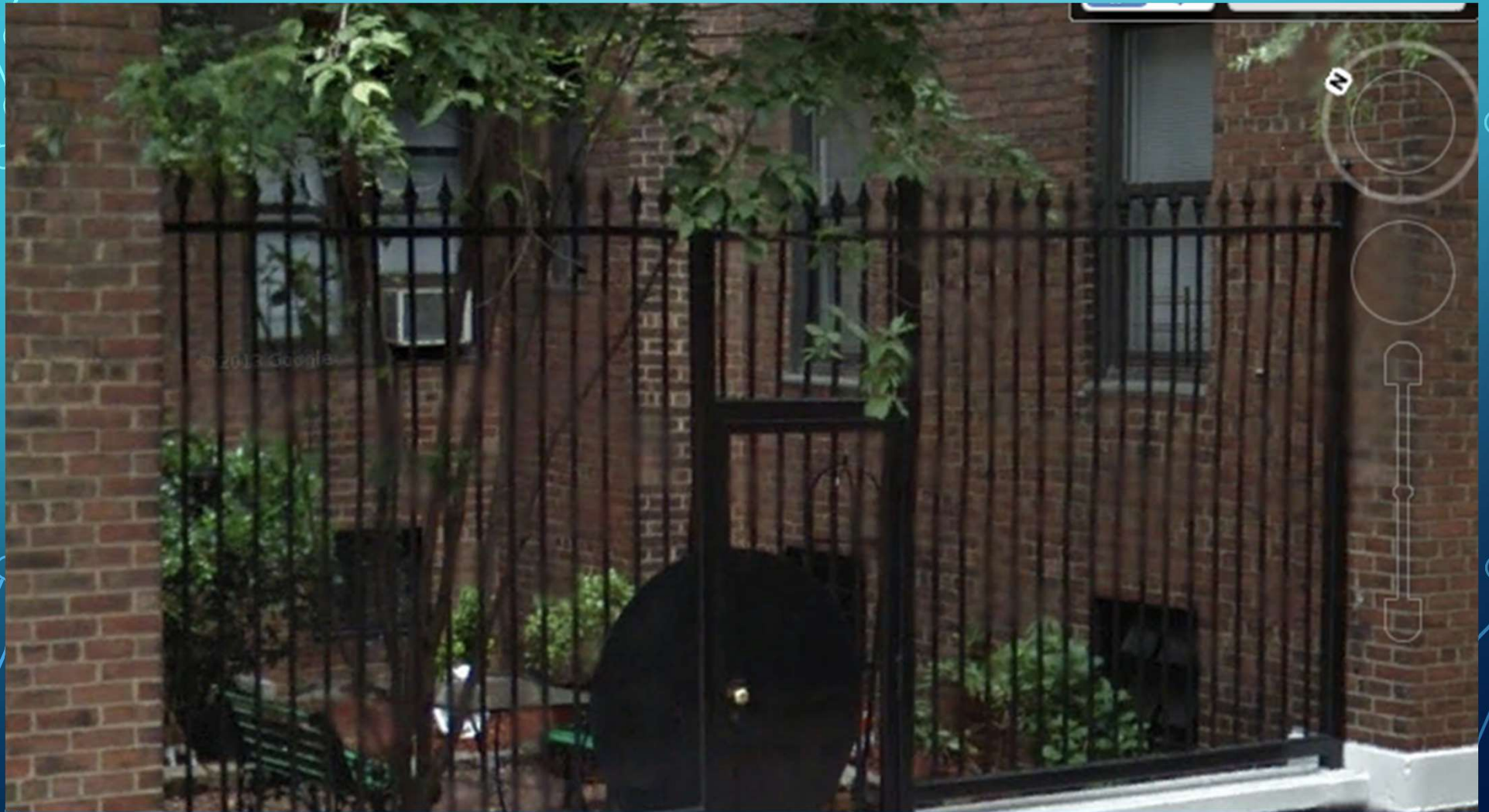
ACTUAL PICTURE





40° 45' 59.40" N, 73° 59' 9.60" W

PICTURE FROM GOOGLE EARTH



report.pdf - Adobe Reader

File Edit View Window Help

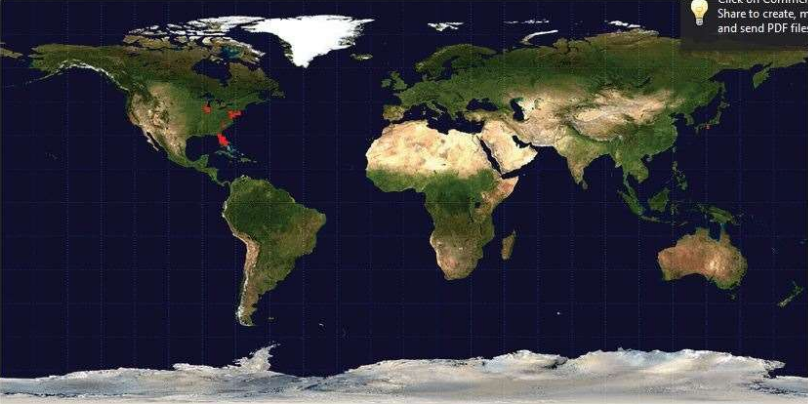
304 / 1496 100%

Comment Share

Bookmarks

- Image Hash
- Details
- Plugins
- Contents
- Application Usage
- Calendar
- Call Log
 - Incoming
 - Missed
 - Outgoing
- Chats
 - Skype
- Contacts
 - (Uncategorized)
 - Skype : cybgasia
- Cookies
- GPS
- Locations
 - Cell towers
 - Wifi networks
- MMS Messages
 - Inbox
 - Sent
- Notes
- SMS Messages
 - Inbox
 - Sent
 - Skype
- User Accounts

GPS

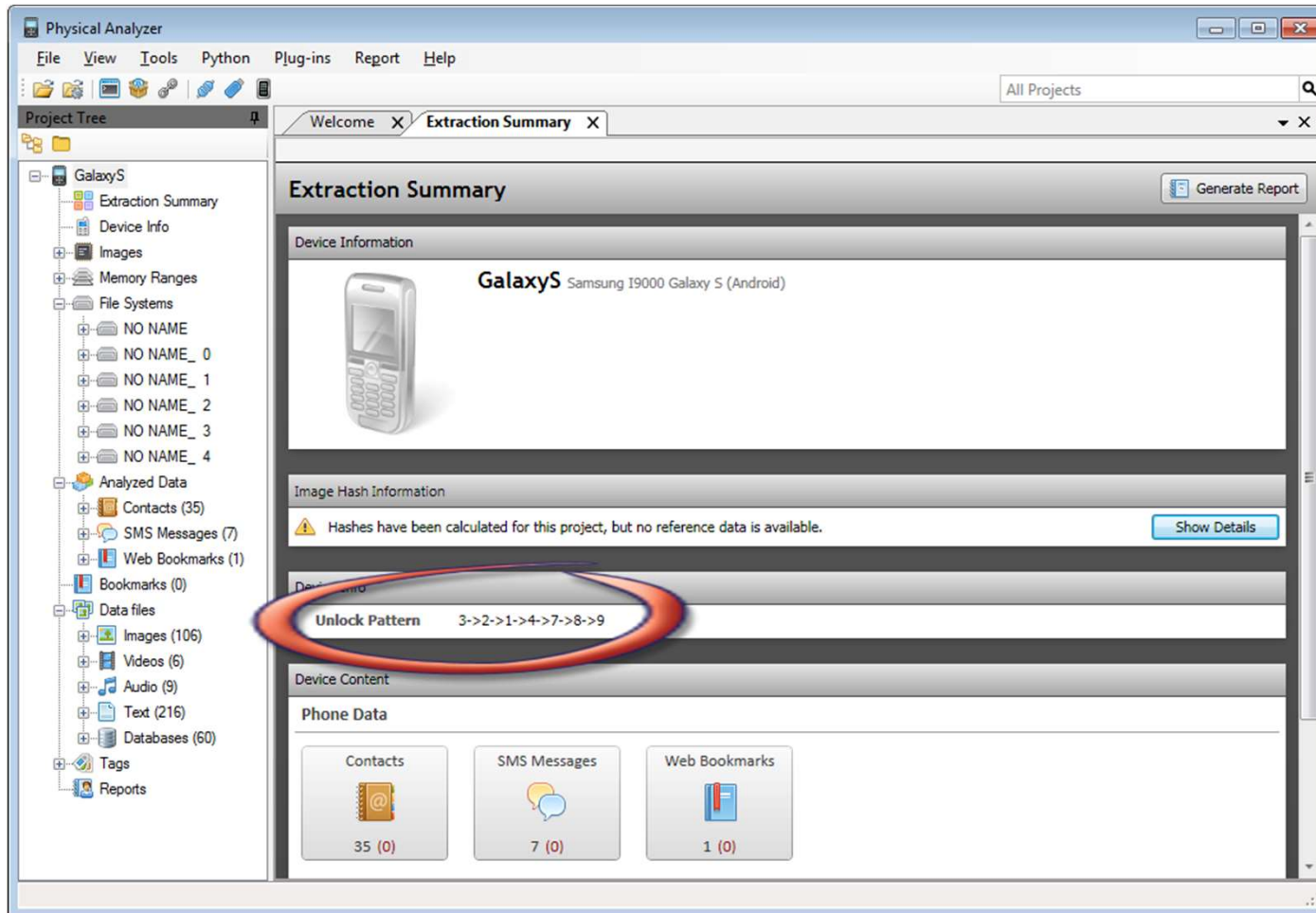


Click on Comment and Share to create, mark-up and send PDF files.

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	



Physical Analyzer

File View Tools Python Plug-ins Report Help

Project Tree

- 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

Extraction Summary X Call Log (101) X

Table View

Del?	Type	Name	Party	Timestamp	Duration	Source
<input checked="" type="checkbox"/>	Outgoing		156	9/11/2010 6:52:04 PM (UTC...	00:01:17	
<input checked="" type="checkbox"/>	Incoming		941	9/11/2010 6:29:44 PM (UTC...	00:15:37	
<input checked="" type="checkbox"/>	Outgoing		941	9/11/2010 6:25:58 PM (UTC...	00:00:40	
<input checked="" type="checkbox"/>	Outgoing		156	9/11/2010 6:25:06 PM (UTC...	00:00:00	
<input checked="" type="checkbox"/>	Outgoing	N...	+13...	9/11/2010 4:33:16 PM (UTC...	00:00:00	
<input checked="" type="checkbox"/>	Outgoing		156	9/11/2010 4:23:49 PM (UTC...	00:06:02	
<input checked="" type="checkbox"/>	Outgoing		156	9/11/2010 4:19:13 PM (UTC...	00:01:28	
<input checked="" type="checkbox"/>	Incoming	N...	352	9/11/2010 4:11:40 PM (UTC...	00:00:59	
<input checked="" type="checkbox"/>	Incoming		727	9/10/2010 8:47:32 PM (UTC...	00:03:37	
<input checked="" type="checkbox"/>	Outgoing		240	9/10/2010 8:25:39 PM (UTC...	00:04:42	
<input checked="" type="checkbox"/>	Outgoing		541	9/10/2010 8:16:43 PM (UTC...	00:08:13	
<input checked="" type="checkbox"/>	Missed		240	9/10/2010 8:24:17 PM (UTC...	00:00:00	
<input checked="" type="checkbox"/>	Outgoing		561	9/10/2010 8:06:59 PM (UTC...	00:02:12	
<input checked="" type="checkbox"/>	Incoming	P...	352	8/28/2010 12:24:02 AM (UTC...	00:02:34	
<input checked="" type="checkbox"/>	Outgoing		17	8/31/2010 12:24:16 AM (UTC...	00:00:00	
<input checked="" type="checkbox"/>	Outgoing		170	8/31/2010 12:24:52 AM (UTC...	00:00:00	
<input checked="" type="checkbox"/>	Incoming		170	8/31/2010 7:39:06 PM (UTC...	00:03:02	
<input checked="" type="checkbox"/>	Outgoing	K...	170	8/31/2010 8:30:11 PM (UTC...	00:16:06	
<input checked="" type="checkbox"/>	Outgoing		156	8/31/2010 8:57:47 PM (UTC...	00:03:32	
<input checked="" type="checkbox"/>	Outgoing	J...	156	8/31/2010 9:02:55 PM (UTC...	00:03:10	
<input checked="" type="checkbox"/>	Outgoing		156	8/31/2010 9:08:47 PM (UTC...	00:00:47	
<input checked="" type="checkbox"/>	Incoming		170	12/13/1976 8:27:33 PM (UTC...	07:23:53	
<input checked="" type="checkbox"/>	Missed				00:00:00	
<input checked="" type="checkbox"/>	Incoming	N...	+13...	3/24/2010 3:07:45 PM (UTC...	00:00:13	Skype: cybgasia
<input checked="" type="checkbox"/>	Outgoing	E...	Te...	9/27/2009 3:35:22 PM (UTC...		Skype: cybgasia
<input checked="" type="checkbox"/>	Outgoing	P...	+19...	9/29/2009 10:01:39 AM (UTC...		Skype: cybgasia
<input checked="" type="checkbox"/>	Outgoing	N...	+13...	11/30/2009 2:48:33 AM (UTC...	00:00:20	Skype: cybgasia
<input checked="" type="checkbox"/>	Outgoing	E...	Te...	3/24/2010 3:03:45 PM (UTC...	00:00:03	Skype: cybgasia
<input checked="" type="checkbox"/>	Incoming	sau...		8/6/2010 2:54:09 AM (UTC+0)		Skype: cybgasia
<input checked="" type="checkbox"/>	Outgoing	N...	+13...	3/29/2010 11:52:56 PM (UTC...	00:04:37	Skype: cybgasia
<input checked="" type="checkbox"/>	Outgoing	N...	+13...	3/28/2010 9:45:20 PM (UTC...	00:03:53	Skype: cybgasia
<input checked="" type="checkbox"/>	Outgoing	srs...		1/11/2010 11:43:35 PM (UTC...		Skype: cybgasia
<input checked="" type="checkbox"/>	Outgoing	nan...		6/1/2010 3:43:00 AM (UTC+0)		Skype: cybgasia
<input checked="" type="checkbox"/>	Outgoing	E...	Te...	3/24/2010 3:01:57 PM (UTC...	00:00:23	Skype: cybgasia
<input checked="" type="checkbox"/>	Outgoing	N...	nan...	6/1/2010 3:44:08 AM (UTC+0)	00:00:12	Skype: cybgasia
<input checked="" type="checkbox"/>	Outgoing	N...	+13...	4/8/2010 12:45:03 PM (UTC...	00:03:21	Skype: cybgasia
<input checked="" type="checkbox"/>	Outgoing	E...	Te...	3/24/2010 3:01:00 PM (UTC...	00:00:07	Skype: cybgasia
<input checked="" type="checkbox"/>	Outgoing	N...	+13...	11/24/2009 3:39:18 PM (UTC...		Skype: cybgasia
<input checked="" type="checkbox"/>	Outgoing	N...	+13...	4/6/2010 2:01:23 AM (UTC+0)	00:03:09	Skype: cybgasia

Copyright © 2014
SECOND EDITION

COMPUTER FORENSICS

Cybercriminals, Laws, and Evidence



MARIE-HELEN MARAS
Copyrighted Material

MARIE-HELEN MARAS
ISBN-13: 978-1449692223



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.

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 hold 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

20%

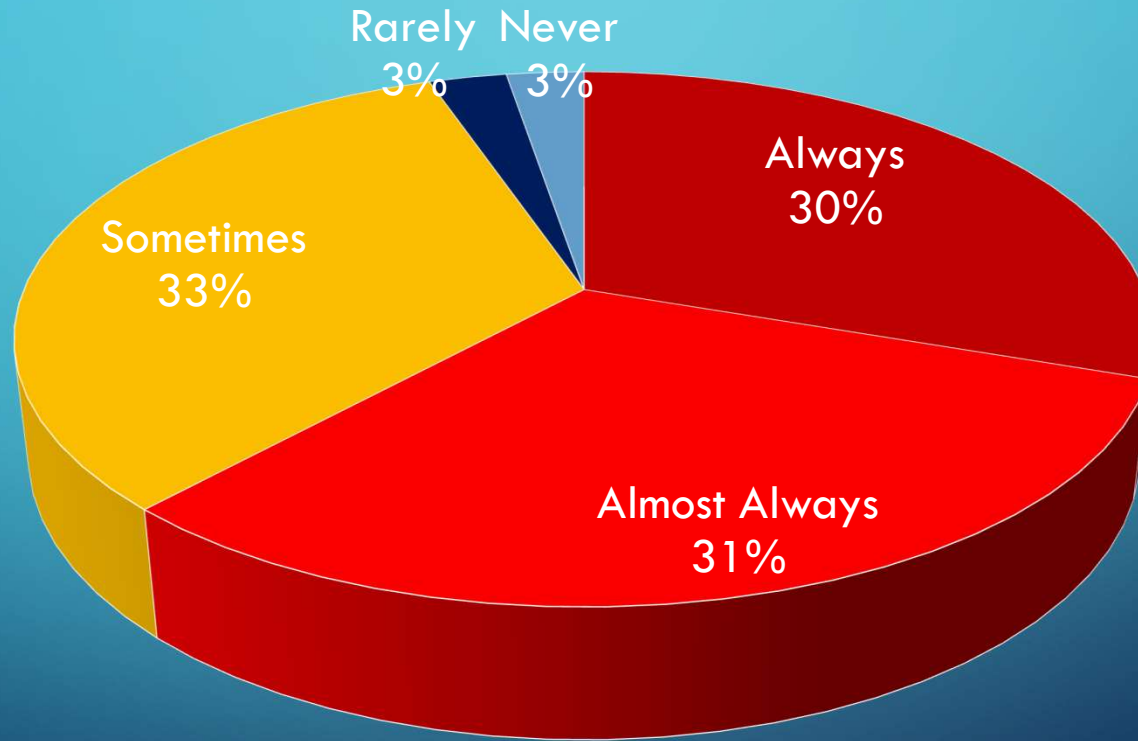


ASSOCIATION OF INSPECTORS GENERAL ANNUAL MEETING SURVEY

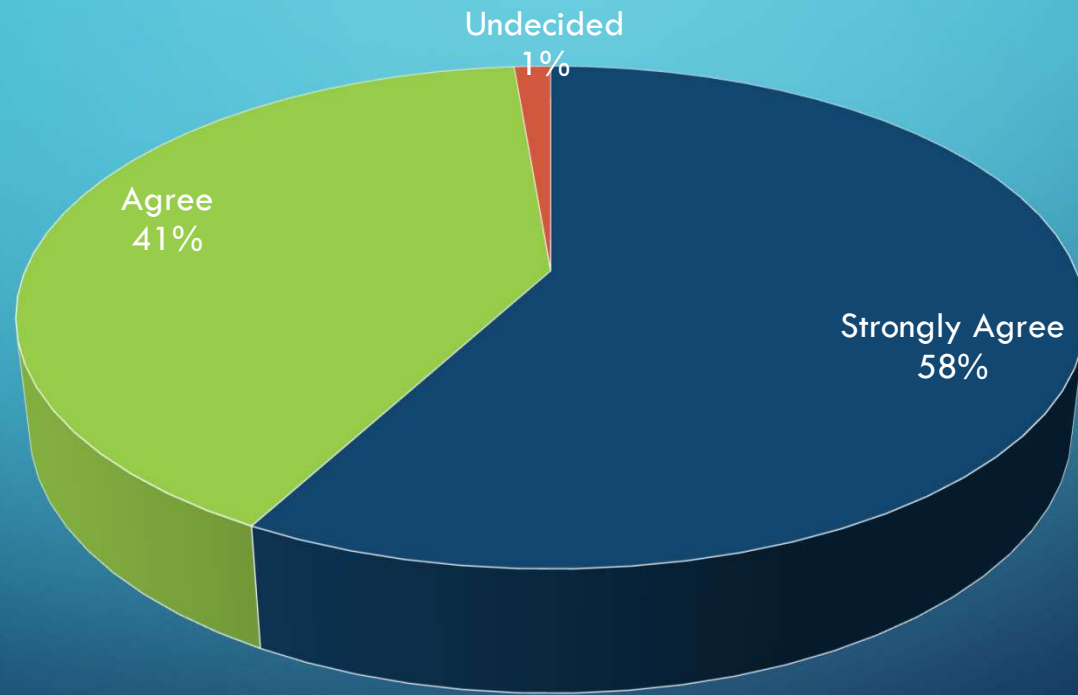
2022

N = 76

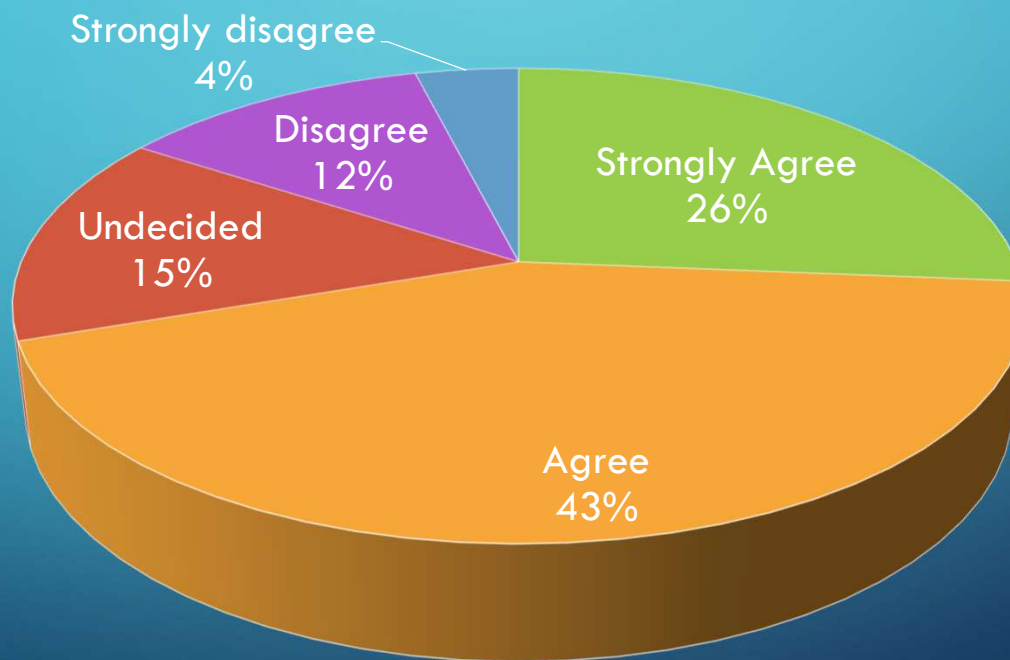
HOW OFTEN DO YOU SEARCH SOCIAL MEDIA FOR EVIDENCE RELATED TO A CRIME OR ADMINISTRATIVE PROCEEDING ON A CASE YOU ARE ASSIGNED TO INVESTIGATE?



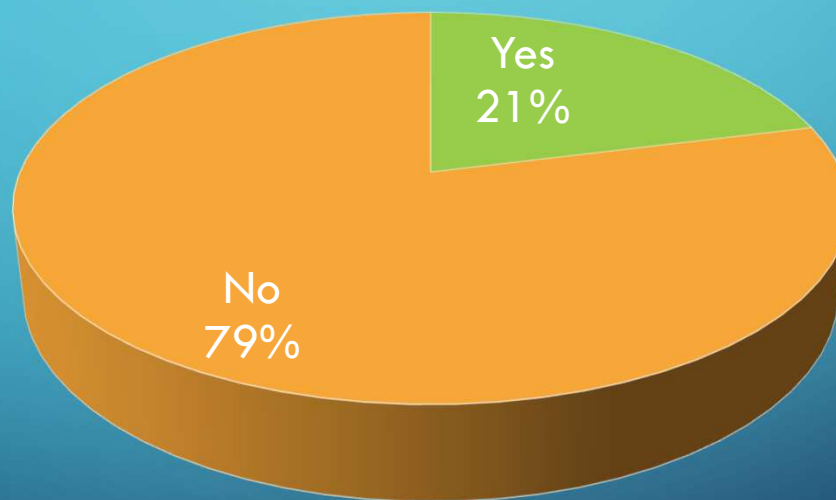
SOCIAL MEDIA IS A VALUABLE TOOL IN INVESTIGATING CRIMES



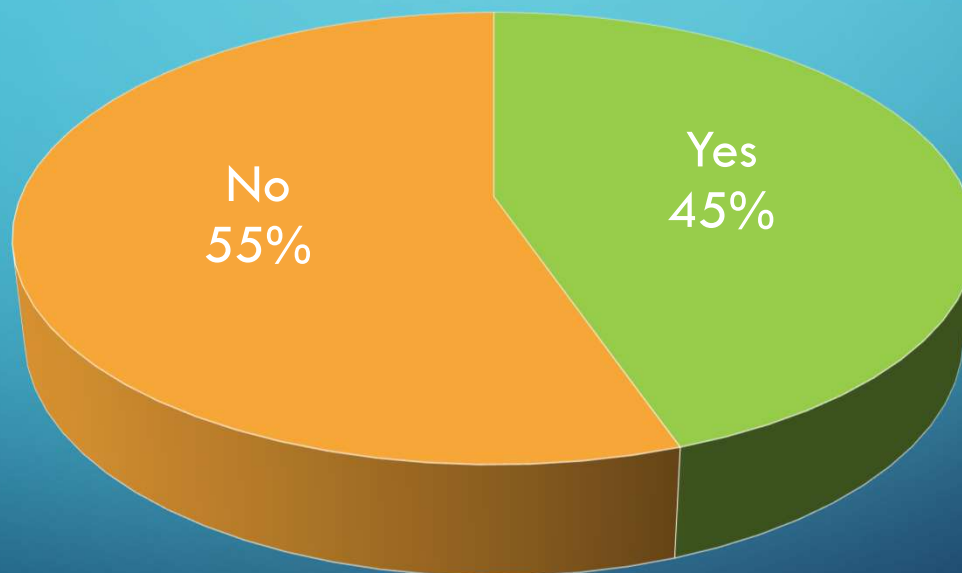
THOSE IN COMMAND AT MY AGENCY ENCOURAGE THE USE OF SOCIAL MEDIA FOR INVESTIGATION



MY DEPARTMENT/AGENCY PROVIDES FORMAL TRAINING
IN USING SOCIAL MEDIA TO GATHER EVIDENCE FOR
INVESTIGATIONS.



DOES YOUR AGENCY/DEPARTMENT HAVE A POLICY FOR OBTAINING/SEARCHING EVIDENCE POSTED ON SOCIAL MEDIA FOR USE IN INVESTIGATIONS?





DEFINING “SOCIAL MEDIA”

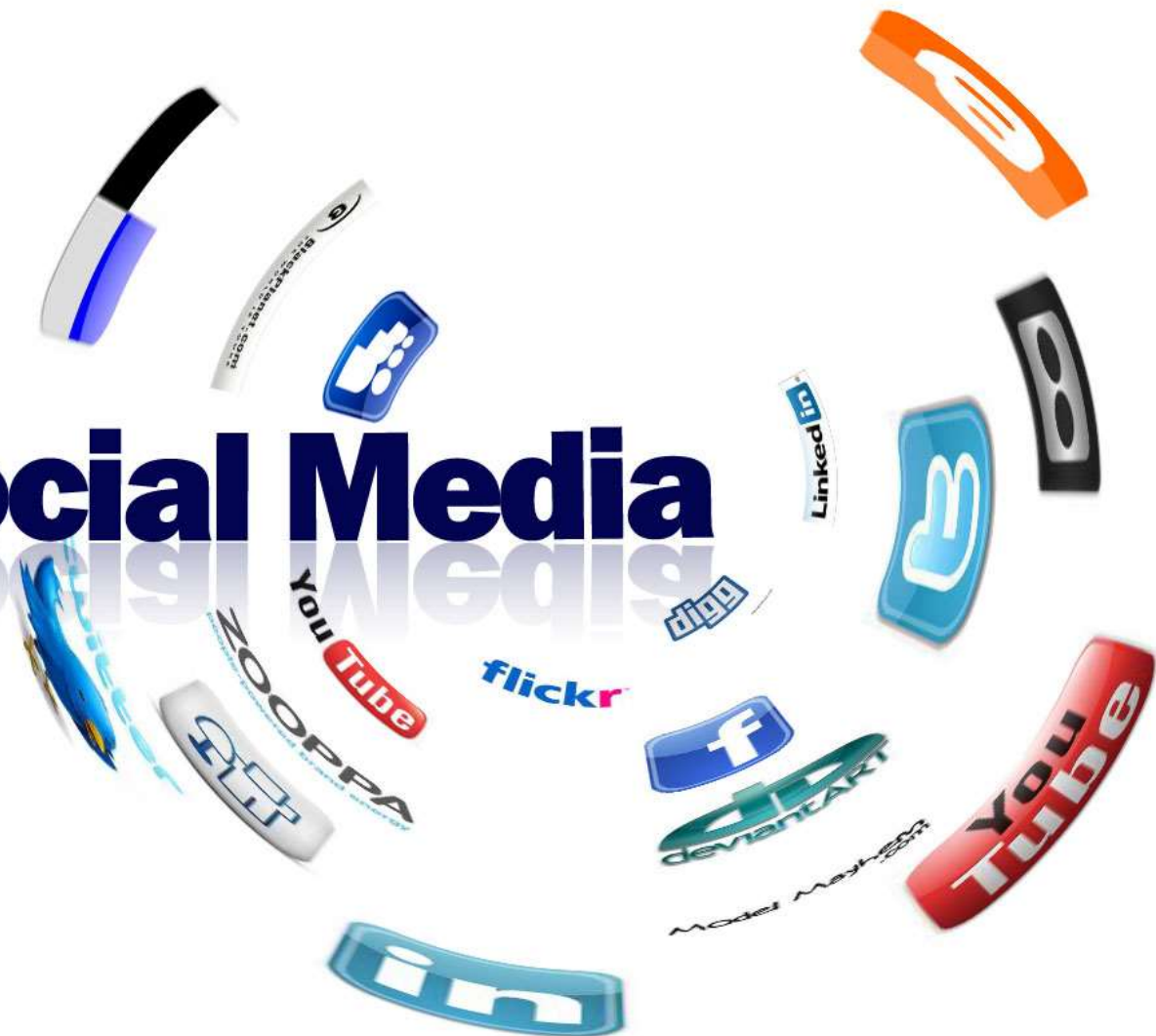
“We define social [media] as web-based services that allow individuals to

- (1) construct a public or semi-public profile within a bounded system,
- (2) articulate a list of other users with whom they share a connection, and
- (3) view and transverse their list of connections and those made by others within the system.

The nature and nomenclature of these connections may vary from site to site.”

-Boyd, D.M., and Ellison, N.B. (2007), *Social Network Sites: Definition, History, and Scholarship*. *Journal of Computer-Mediated Communication*, 13: 210-230, available at <http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2007.00393.x/full>.

Social Media



INVESTIGATIVE METHODS



SCREEN CAPTURE



ARCHIVING SOLUTIONS



FORENSIC SOFTWARE



BUSINESS RECORDS