



Posts to Proof: A Comprehensive Guide to Social Media Forensics

Angel Garrow
Digital Forensic Analyst

Erin Swakopf
Digital Forensic Analyst



4/27/2023

Agenda

- 01 Social Media Forensics
- 02 Collection Tools and Capabilities
- 03 Attorney Expectations
- 04 Social Media Collection Limitations
- 05 Additional Resources

LET'S BEGIN!





Social Media Forensics



Social Media Today

More than 75% of eligible global population now uses social media

As of October 2022, there are 4.74 billion social media users worldwide

9 in 10 internet users use social media every month

An average social media user uses 7.2 different social media platforms every month

General Social Media Statistics



As of October 2022, there are
4.74 billion
social media users worldwide



9 in 10 internet users

use social media every month



Around the world, there are
5.07 billion
internet users, equating to almost
63.5% of the world's population

Over the past 12 months, the number of active social media users increased by **190 million**, indicating 4.2% annual growth, with 6 new average users joining every single second



An average social media user uses
7.2 different
social platforms every month



More than 75%
of the eligible global population now
uses social media

Note: This number excludes the population who don't have access to social networks



The world today has
6.648 billion
smartphone users, meaning almost
83.07% of the world's population owns
a smartphone today



A typical social media user spends almost
2.5 hours
on average every day
using social media



The world spends more than
10 billion hours
every day using social media

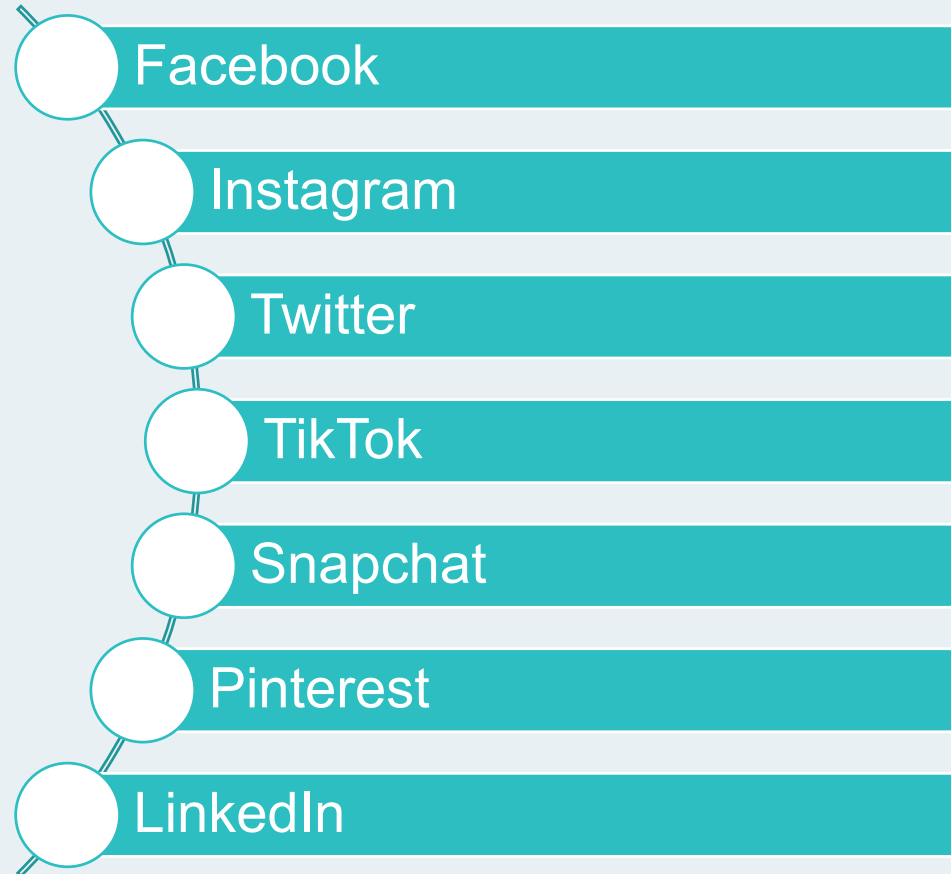


44%
of TikTok's users will
be under 25 by 2023

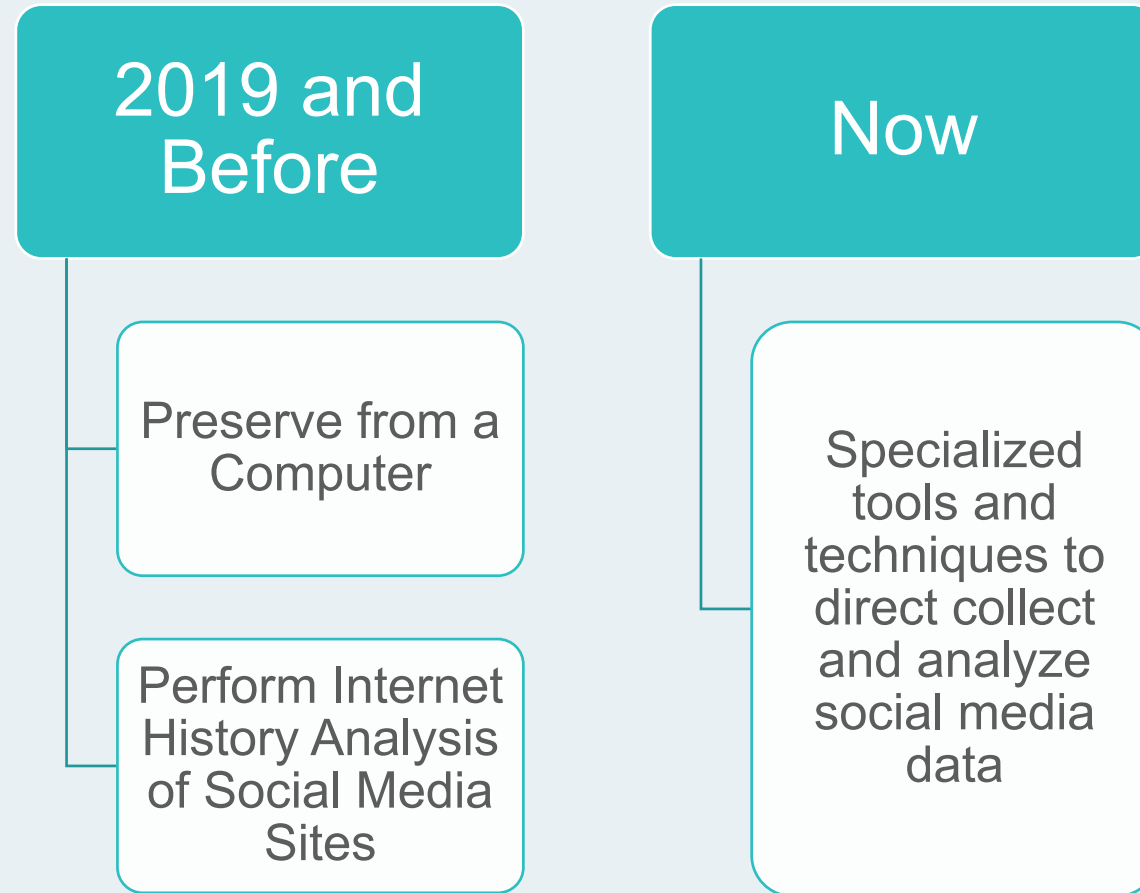


eMarketer predicts that the percentage of Facebook users under **25 years** will drop below 15% in 2023

Types of Social Media



What is Social Media Forensics



Are Social Media Accounts Considered Forensically Collected?

Almost Always

3 Basic but Essential Principles:

- Reliable, Defensible, Reproducible

Technology often grows faster than policies or laws resulting in a lack of official guidelines

Collection Tools and Capabilities

Types of Tools for Social Media Collections

Open Source / Publicly Available Tools

- DYI = Download Your Information (NOT DIY)
- Download Your Account Data

Commercial Tools

- Axiom
- Cellebrite

Deeper Dive Commercial Tools

- X1



DYI – Meta (Facebook) vs. Instagram

What categories of data are available in your Facebook settings?

The Access Your Information tool and Download Your Information tool both provide a summary of your Facebook profile information that you can access at any time and in a single place. We've categorized this information by type.

Name	Type	Compressed size	Password	Size	Date	Date modified
ad_accounts	The folder				2/18/2021 6:22 AM	
ad_accounts	The folder				2/18/2021 6:22 AM	
apps_and_websites	The folder				2/18/2021 6:22 AM	
auth_info	The folder				2/18/2021 6:22 AM	
avatars_posts	The folder				2/18/2021 6:22 AM	
comments	The folder				2/18/2021 6:22 AM	
contacts	The folder				2/18/2021 6:22 AM	
contact	The folder				2/18/2021 6:22 AM	
device_information	The folder				2/18/2021 6:22 AM	
digital_wallets	The folder				2/18/2021 6:22 AM	
events	The folder				2/18/2021 6:22 AM	
files	The folder				2/18/2021 6:22 AM	
followers_and_following	The folder				2/18/2021 6:22 AM	
fundraisers	The folder				2/18/2021 6:22 AM	
games	The folder				2/18/2021 6:22 AM	
information_about_you	The folder				2/18/2021 6:22 AM	
likes	The folder				2/18/2021 6:22 AM	
login_and_account_creation	The folder				2/18/2021 6:22 AM	
login_accounts	The folder				2/18/2021 6:22 AM	
media	The folder				2/18/2021 6:22 AM	
media_settings	The folder				2/18/2021 6:22 AM	
messages	The folder				2/18/2021 6:22 AM	
notifications	The folder				2/18/2021 6:22 AM	
past_instagram_insights	The folder				2/18/2021 6:22 AM	
personal_information	The folder				2/18/2021 6:22 AM	
recent_posts	The folder				2/18/2021 6:22 AM	
reports	The folder				2/18/2021 6:22 AM	
saved	The folder				2/18/2021 6:22 AM	
shopping	The folder				2/18/2021 6:22 AM	
using_facebook_applications	The folder				2/18/2021 6:22 AM	
your_posts	The folder				2/18/2021 6:22 AM	

Your Activity Across Facebook	Information and activity from different areas of Facebook, such as posts you've created, photos you're tagged in, groups you belong to and more.
Personal Information	Information that you've provided when you set up your Facebook accounts and profiles.
Connections	Who and how you've connected with people on Facebook including things like your friends and followers.
Logged Information	Information that Facebook logs about your activity, including things like your location history and search history.
Security and Login Information:	Technical information and logged activity related to your account.
Apps and Websites off of Facebook	Apps you own and activity we receive from apps and websites off of Facebook.
Preferences	Actions you've taken to customize your experience on Facebook.
Ad information	Your interactions with ads and advertisers on Facebook.



Download Your Account Data – LinkedIn

	A	B	C	D	E	F	G	H	I
7	2-ZGIwY2NhZDEtYzNiN	Manik Kh	https://w	Angel Gar	2022-03-03 20:09:53			Hi Angel, Thanks for accepting my request	INBOX
8	2-ZTcwYmRiNzItYTQ0C	Manik Kh	https://w	Angel Gar	2022-03-03 19:56:52			Hi Angel, I have a Fully Remote job opening as Digital Forensic Analyst with AT&T Client and they are offering \$82/Hr. on W2. My name	INBOX
9	2-MjU3MTgxNmYtYTZ	Nick Eppl	https://w	Angel Gar	2022-03-01 21:19:22			Hello Angel, thanks for connecting! Please let me know if I can be a resource in any way.	INBOX
10	2-NzE4MDIiYzQtNjdZS	Amber Sch	https://w	Angel Gar	2022-03-01 18:31:33			Angel, I would like to connect with you to share DFIR tips and tricks. I maintain a blog at forensic-impact.com and feel it is always good	INBOX
11	2-YzkzYTViNWMTZGI0Y	Alexandra	https://w	Angel Gar	2022-03-01 18:31:08			Hello Angel, I see you deal with digital forensics. I am quite familiar with this topic. I am lead OSINT consultant at Social Links.Â Let's	INBOX
12	2-NWRmODNkMGEtYjI	Dr Todd H	https://w	Angel Gar	2022-03-01 18:30:55			Love to connect to a fellow digital forensic specialist I am a licensed investigator and work in the video/photographic/audio area with	INBOX
13	2-YiAxNmQ	Lets get cc	Shah Bukh	https://w	Angel Gar	2021-11-1		Lets get cc Dear Angel, Hope this email finds you well!! While scouting out for the remote position of Digital Forensic IR Investigator with one of	INBOX

X1 – Rolling Screen Capture

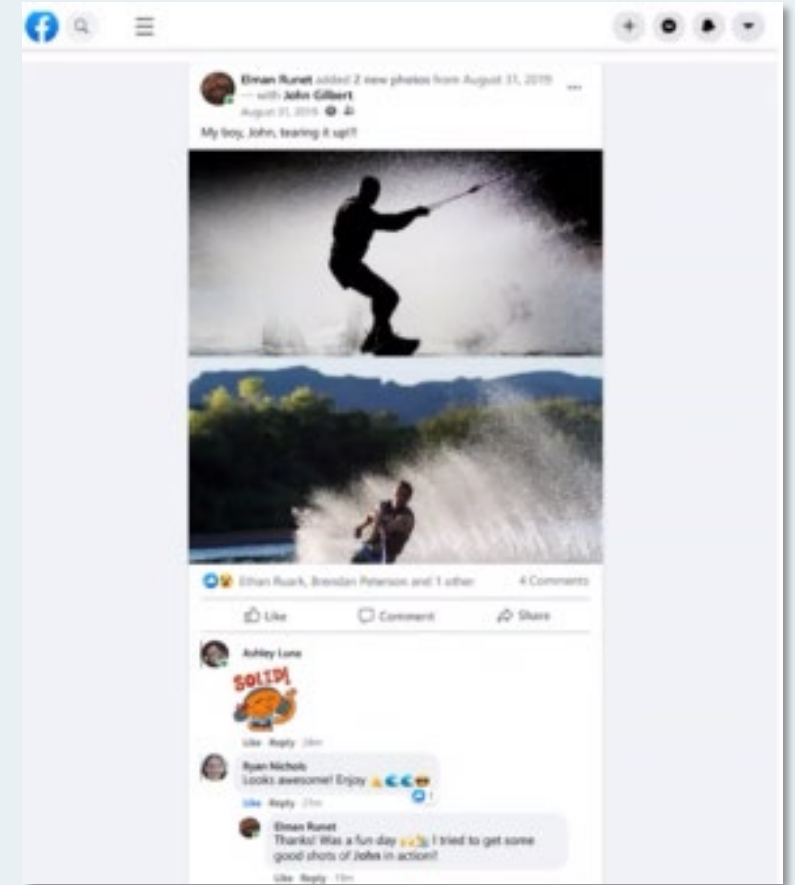
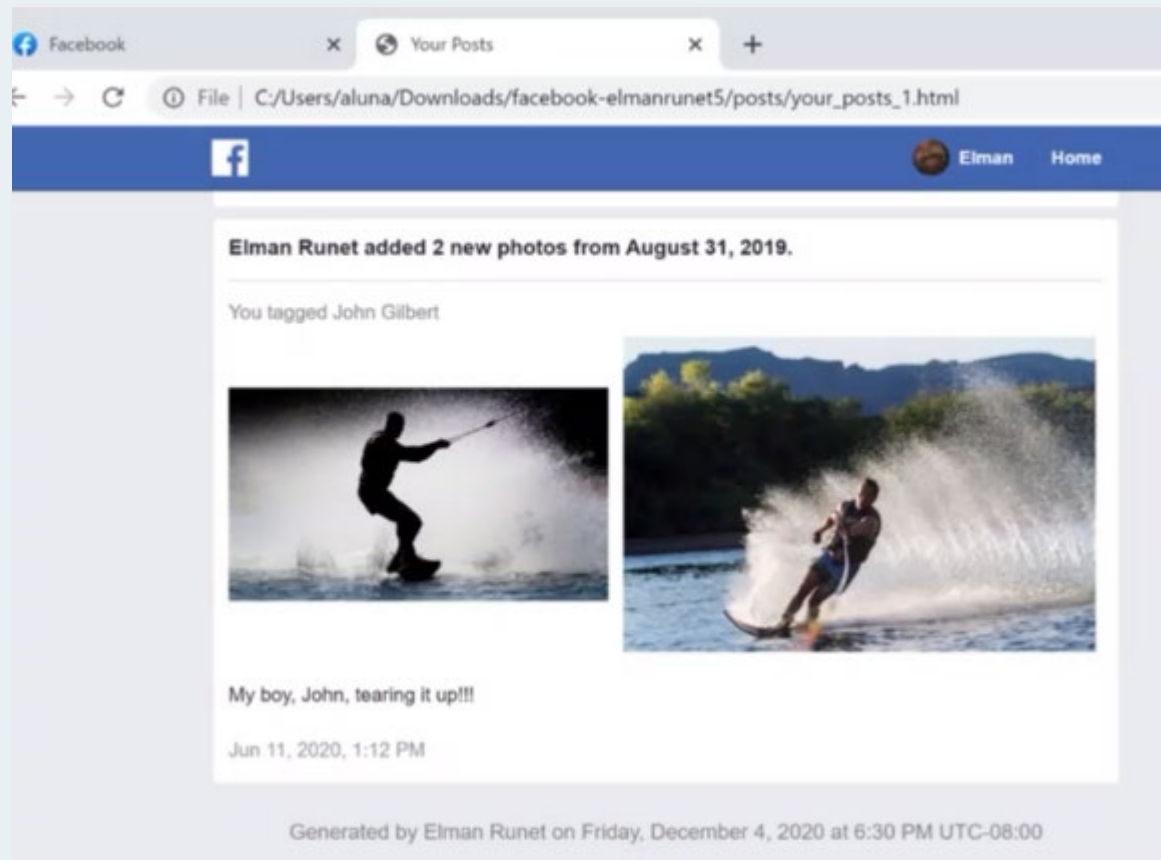
Great for Twitter, Tumblr, Facebook, and YouTube

- Adding Instagram Auto Scanner

Also helpful for:

- Web Page Capture
- Web Crawls

DYI vs. X1



Axiom Rocks

Can Collect

- Facebook
- Instagram
- Twitter
- WhatsApp
- Slack
- Microsoft Teams



Types of Data Axiom Can Collect

Magnet AXIOM Learning v10.0.14051 - NANOBOOK

File Tools Process Help

Evidence Artifacts Content types Date and time Tags and comments Profiles

Filters Partial results Keyword lists Scan time

Artifacts

MATCHING RESULTS (63 of 63)

Item ID	Artifact type	Artifact c...	Date and time
46	Cloud Facebook Mobile Timeline	Social Networking	5/2/2016 7:06:00 P
47	Cloud Facebook Mobile Timeline	Social Networking	2/21/2016 11:00:00
48	Cloud Facebook Mobile Timeline	Social Networking	
14	Cloud Facebook Messenger Messages	Communication	5/2/2016 10:19:03 P
16	Cloud Facebook Messenger Messages	Communication	5/2/2016 6:51:04 P
17	Cloud Facebook Messenger Messages	Communication	5/2/2016 6:50:18 P
18	Cloud Facebook Messenger Messages	Communication	5/2/2016 6:46:10 P
19	Cloud Facebook Messenger Messages	Communication	5/2/2016 6:45:01 P
20	Cloud Facebook Messenger Messages	Communication	5/2/2016 6:44:14 P
21	Cloud Facebook Messenger Messages	Communication	5/2/2016 7:29:02 P
22	Cloud Facebook Messenger Messages	Communication	5/2/2016 6:46:02 P
23	Cloud Facebook Messenger Messages	Communication	5/2/2016 6:50:03 P
24	Cloud Facebook Messenger Messages	Communication	5/2/2016 6:50:03 P
15	Passwords and Tokens	Identified Results	
28	Identifiers - People	Identified Results	
29	Identifiers - People	Refined Results	

Facebook -

DETAILS

ARTIFACT INFORMATION

File System: AFF4-L

Artifact type: File System Information

Item ID: 1

EVIDENCE INFORMATION

Source: Cloud-Acquire_2023-02-02_10-53-43 AFF4/Facebook

Recovery method: Parsing

Deleted source: n/a

Location: n/a

Evidence marker: Facebook

Go to Settings to activate Windows. Time zone: UTC+080

Magnet AXIOM Learning v10.0.14051 - SM-test

File Tools Process Help

Evidence Artifacts Content types Date and time Tags and comments Profiles

Filters Partial results Keyword lists Scan time

Artifacts

MATCHING RESULTS (2,255 of 2,255)

Item ID	Artifact type	Artifact c...	Date and time
1	File System Information	Operating System	
2	Cloud Accounts Information	Operating System	
3	Cloud Instagram Direct Messages	Social Networking	10/31/2022 11:12:45 PM
4	Cloud Instagram Direct Messages	Social Networking	12/4/2022 11:26:04 PM
5	Cloud Instagram Direct Messages	Social Networking	1/12/2023 12:34:00 AM
6	Cloud Instagram Direct Messages	Social Networking	1/12/2023 12:33:14 AM
7	Cloud Instagram Direct Messages	Social Networking	12/22/2022 7:11:11 PM
8	Cloud Instagram Direct Messages	Social Networking	12/16/2022 4:54:30 PM
9	Cloud Instagram Direct Messages	Social Networking	11/28/2022 7:51:43 PM
10	Cloud Instagram Direct Messages	Social Networking	1/11/2023 9:41:19 PM
11	Cloud Instagram Direct Messages	Social Networking	9/29/2022 4:07:58 AM
12	Cloud Instagram Direct Messages	Social Networking	12/2/2022 12:52:48 AM
13	Cloud Instagram Direct Messages	Social Networking	10/5/2022 1:11:13 AM
14	Cloud Instagram Direct Messages	Social Networking	1/15/2023 7:26:03 AM
15	Cloud Instagram Direct Messages	Social Networking	12/16/2022 4:42:19 PM
16	Cloud Instagram Direct Messages	Social Networking	10/31/2022 11:12:45 PM

Instagram User Account -

DETAILS

ARTIFACT INFORMATION

File System: AFF4-L

Artifact type: File System Information

Item ID: 1

EVIDENCE INFORMATION

Source: Cloud-Acquire_2023-02-02_09-57-36 AFF4/Instagram User Account

Recovery method: Parsing

Deleted source: n/a

Location: n/a

Evidence marker: Instagram

Go to Settings to activate Windows. Time zone: UTC+090

Types of Data Axiom Can Collect

Magnet AXIUM Examine v6.10.0.34490 - Sandbox

File Tools Process Help

FILTERS Evidence ▾ Artifacts ▾ Content types ▾ Date and time ▾ Tags and comments ▾ Profiles ▾

Partial results ▾ Keyword lists ▾ Scan time ▾

CLEAR FILTERS GO ADVANCED

Artifacts ▾

REFINED RESULTS 197

- Cloud Passwords and Tokens 1
- Identifiers - People 180
- Passwords and Tokens 1
- Social Media URLs 15

SOCIAL NETWORKING 81

- Cloud Twitter Direct Messages 18
- Cloud Twitter Posts 11
- Cloud Twitter Users 52

MEDIA 3

- Pictures 1

OPERATING SYSTEM 2

- Cloud Accounts Information 1
- File System Information 1

MATCHING RESULTS (18 of 18) Column view ▾

M...	Send...	R...	T...	Send/Received...	S...	Send...
130813...	Ask_S...	Angel...	Thank...	9/21/2020 7:52:41 PM	1164256...	Angel Car
130847...	Ask_S...	Angel...	Thank...	9/22/2020 6:36:25 PM	1164256...	Angel Car
130811...	Ask_S...	Angel...	Thank...	9/21/2020 6:54:07 PM	1164256...	Angel Car
130765...	Ask_S...	Angel...	Apolog...	9/20/2020 12:01:44 PM	1164256...	Angel Car
130765...	Ask_S...	Angel...	We h...	9/20/2020 11:06:05 AM	1164256...	Angel Car
130765...	Ask_S...	Angel...	React...	9/20/2020 11:07:55 AM	1164256...	Angel Car
131475...	Ask_Spectrum	Angel...	Thank...	10/10/2020 2:31:11 AM	19638927	Ask Spect
130847...	Ask_Spectrum	Angel...	I'm ch...	9/22/2020 6:39:58 PM	19638927	Ask Spect
130848...	Ask_Spectrum	Angel...	Looks l...	9/22/2020 6:59:26 PM	19638927	Ask Spect
130813...	Ask_Spectrum	Angel...	That is...	9/21/2020 7:53:08 PM	19638927	Ask Spect
130811...	Ask_Spectrum	Angel...	Thank...	9/21/2020 6:56:22 PM	19638927	Ask Spect
130765...	Ask_Spectrum	Angel...	Hello, I...	9/20/2020 12:00:17 PM	19638927	Ask Spect
126758...	Angel...	Angel...	https://	6/27/2020 3:10:01 AM	2761469...	
126711...	Angel...	Angel...	https://	5/31/2020 3:37:45 PM	2761469...	
126711...	Angel...	Angel...	https://	5/31/2020 3:37:17 PM	2761469...	
121744...	Angel...	Angel...	Interact...	3/10/2020 6:23:44 PM	2761469...	

1308132381253988357

Twitter User Account -

PREVIEW

Ask Spectrum @Ask_Spectrum

9/21/2020 7:53:08 PM

That is great to hear. Please let us know if you have any other issues or questions. Thank you. :D

Activate Windows

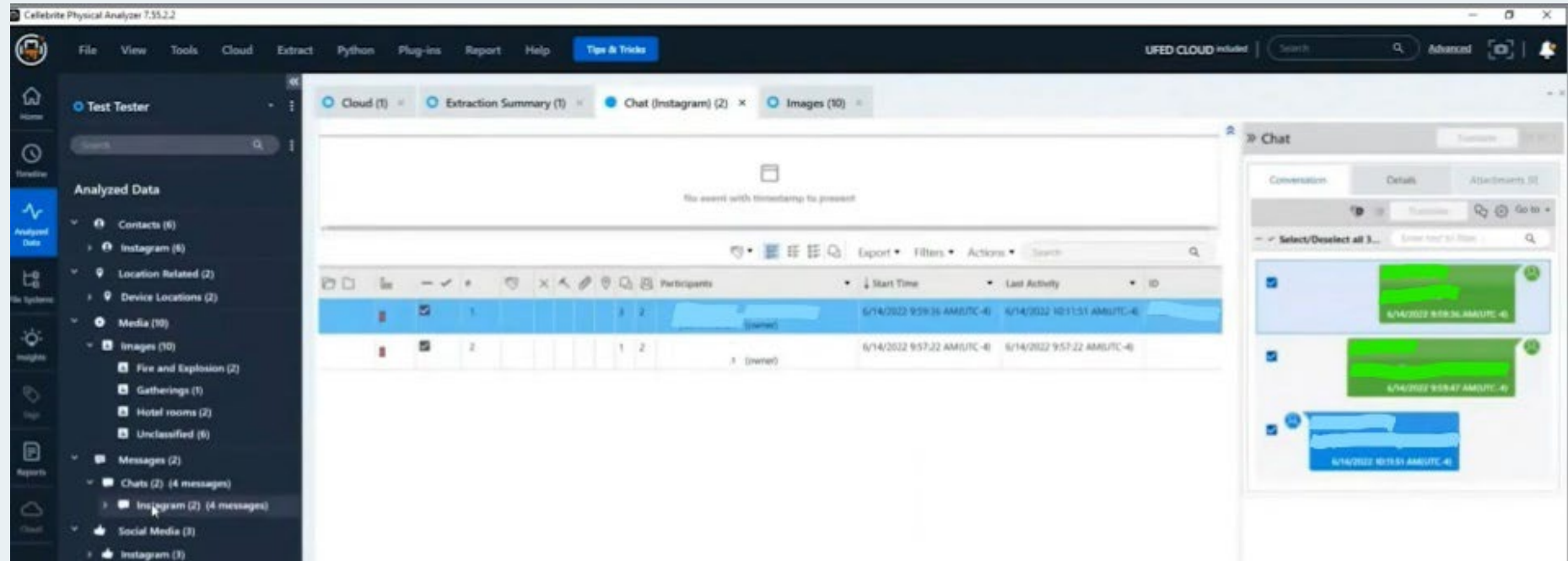
TAGS, COMMENTS & PROFILES



Cellebrite

Can Collect

- Facebook
- Instagram
- Twitter
- LinkedIn
- Snapchat
- TikTok
- WhatsApp



Collecting Directly from Devices





Export Options and How to Prepare Data for Review

Axiom

- Load file
- HTML chat threads for chat-based communication

Cellebrite and X1

- Concordance load file



Attorney Expectations



What Else Can I Do?

Be Prepared

- List of social media accounts
- Credentials for each account
- Temporarily turn off 2FA/MFA
- Provide client contact information to the analyst
- Set expectations – No cold calls!

Ask Follow-Up Questions

Forensic analysts are available to answer your questions about the data

You can ask for metadata

Social Media Collection Limitations

Social Media Limitations

Social Media Platforms are constantly changing

Tools are limited to current versions of social platforms

Social Media Limitations

Content Ownership – Site Owner vs. User

Do we have permission to collect the posts?

- What about other's posts or comments?

Information you can't download

Your download only contains information that you shared or that is related to your account. Information that others share, like when a friend posts and tags you, will not be included in your download. Your download will include a record of when you were tagged.

You can view information people shared about you anytime.

- Polls >
- Activity you're tagged in >
- Posts hidden from your timeline >
- Videos you've watched >
- Saved items and collections >

Social Media Limitations

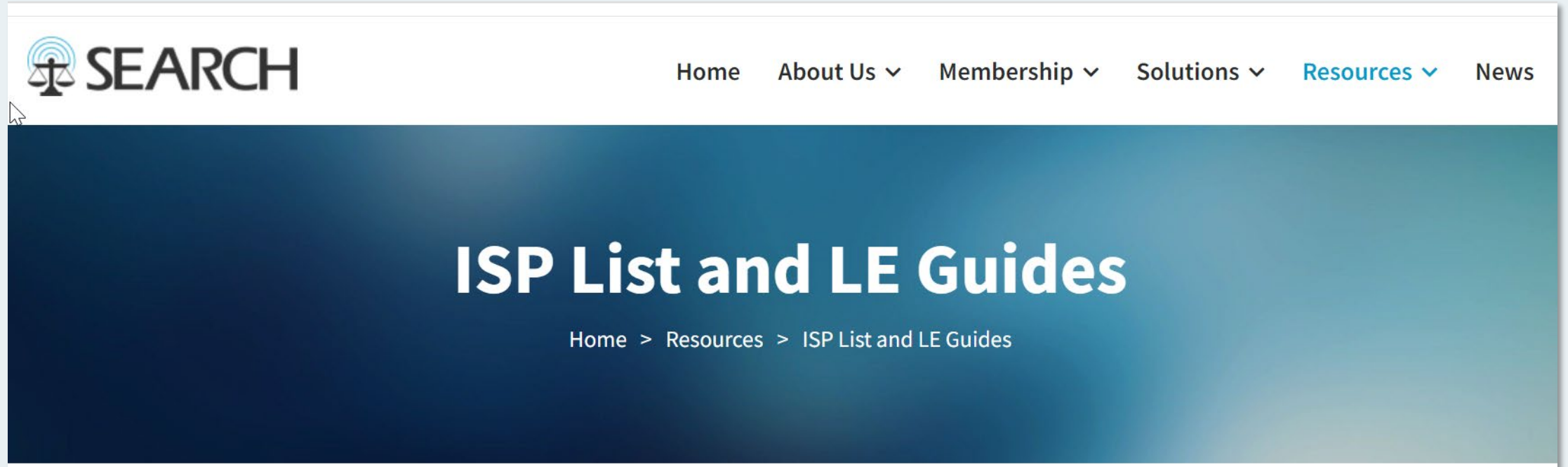
Deleted Data

Temporary hold after deletion

Additional Resources



Legal Requests Contact Information Resource



<https://www.search.org/resources/isp-list/>



Q&A

Angel Garrow

a_garrow@tcdi.com

Erin Swakopf

e_swakopf@tcdi.com



**4508 Weybridge Lane
Greensboro, North Carolina**



**1501 Euclid Avenue, Suite 424
Cleveland, Ohio**



**3 Manhattanville Road, 1st Floor, Suite 106
Purchase, New York**

