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

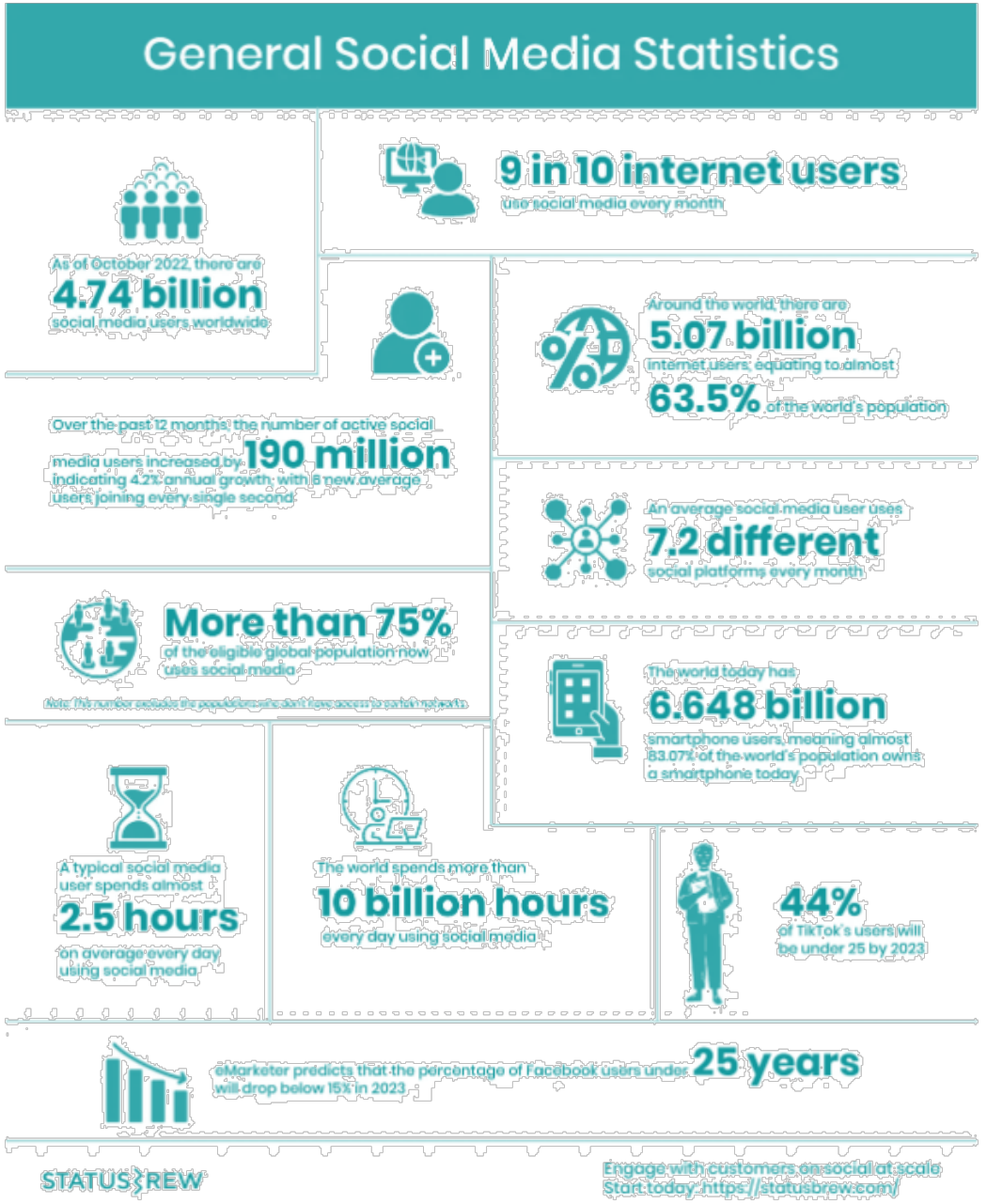
Social Media Today

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

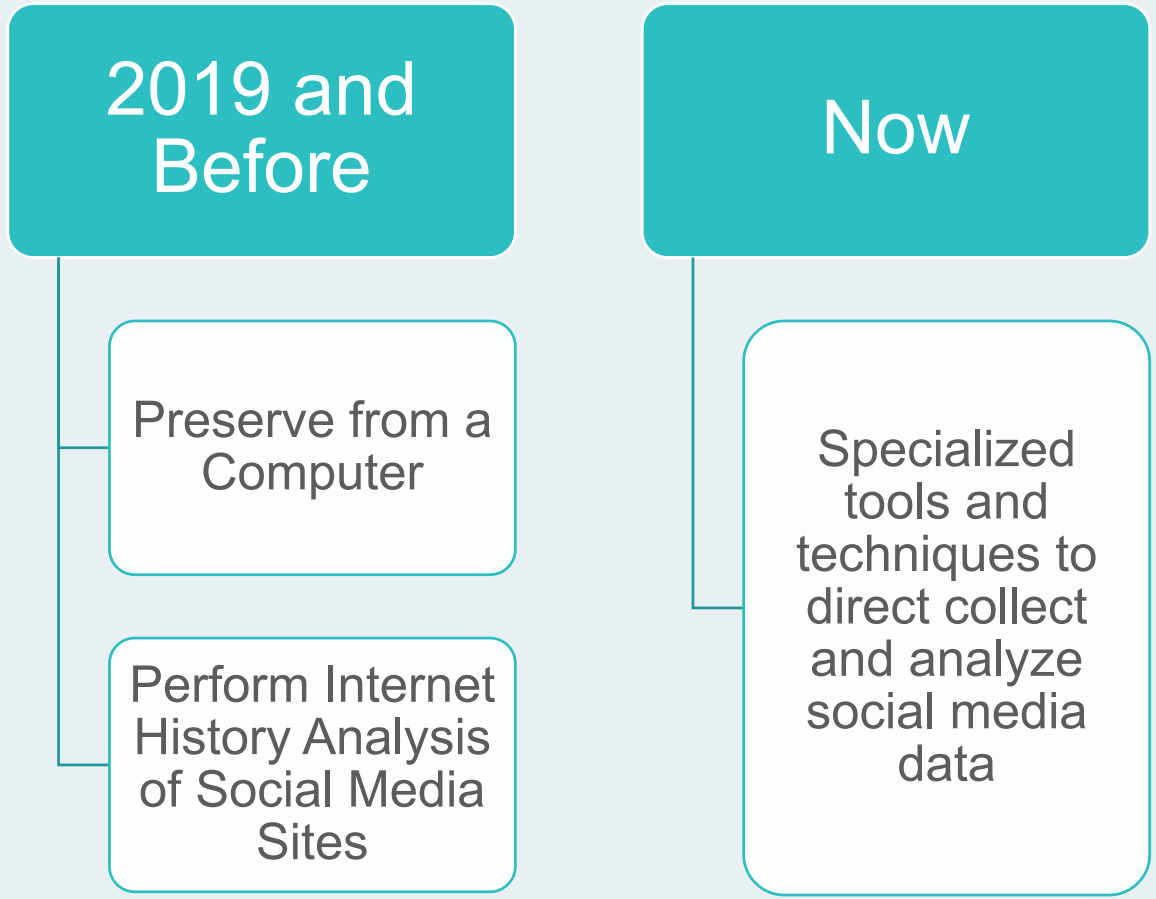
An average social media user uses 7.2 different social media platforms every month



Types of Social Media

- Facebook
- Instagram
- Twitter
- TikTok
- Snapchat
- Pinterest
- LinkedIn

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

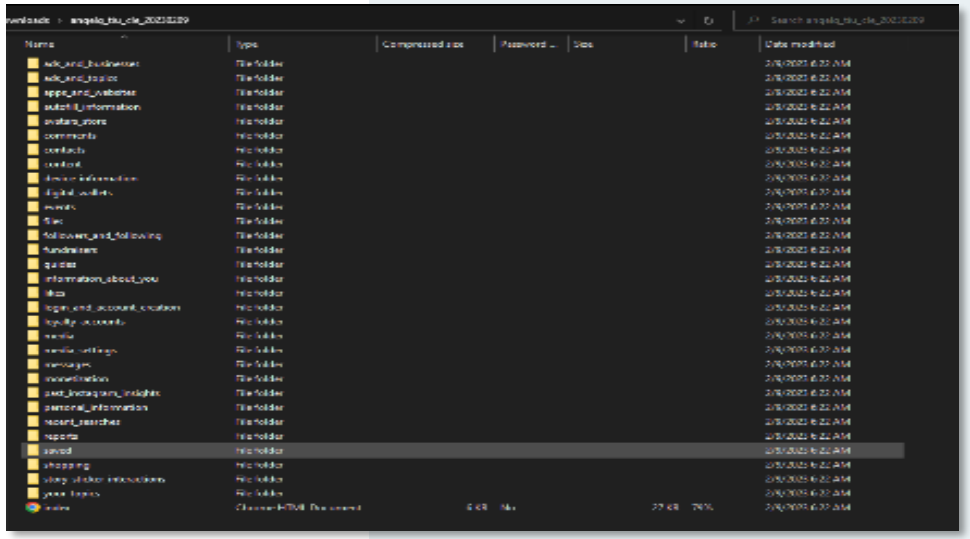
Deeper Dive Commercial Tools

- 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.



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 Kha	https://w	Angel Gar	2022-03-03 20:09:53	U	Hi Angel, Thanks for accepting my request	INBOX
8	2-ZTcwYmRiNzItYTQ0C		Manik Kha	https://w	Angel Gar	2022-03-03 19:56:52	U	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-MjU3MTgxNmYtYTYz		Nick Epple	https://w	Angel Gar	2022-03-01 21:19:22	U	Hello Angel, thanks for connecting! Please let me know if I can be a resource in any way.	INBOX
0	2-NzE4MDllYzQtNjdlZS		Amber Sch	https://w	Angel Gar	2022-03-01 18:31:33	U	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
1	2-YzkzYTVlNWMtZGI0Y		Alexandra	https://w	Angel Gar	2022-03-01 18:31:08	U	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
2	2-NWRmODNkMGEtYjI		Dr Todd H	https://w	Angel Gar	2022-03-01 18:30:55	U	Love to connect to a fellow digital forensic specialist I am a licensed investigator and work in the video/photographic/audio area with	INBOX
3	2-YjAxNmQ(	Lets get c	Shah Rukh	https://w	Angel Gar	2021-11-1	Lets get c	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

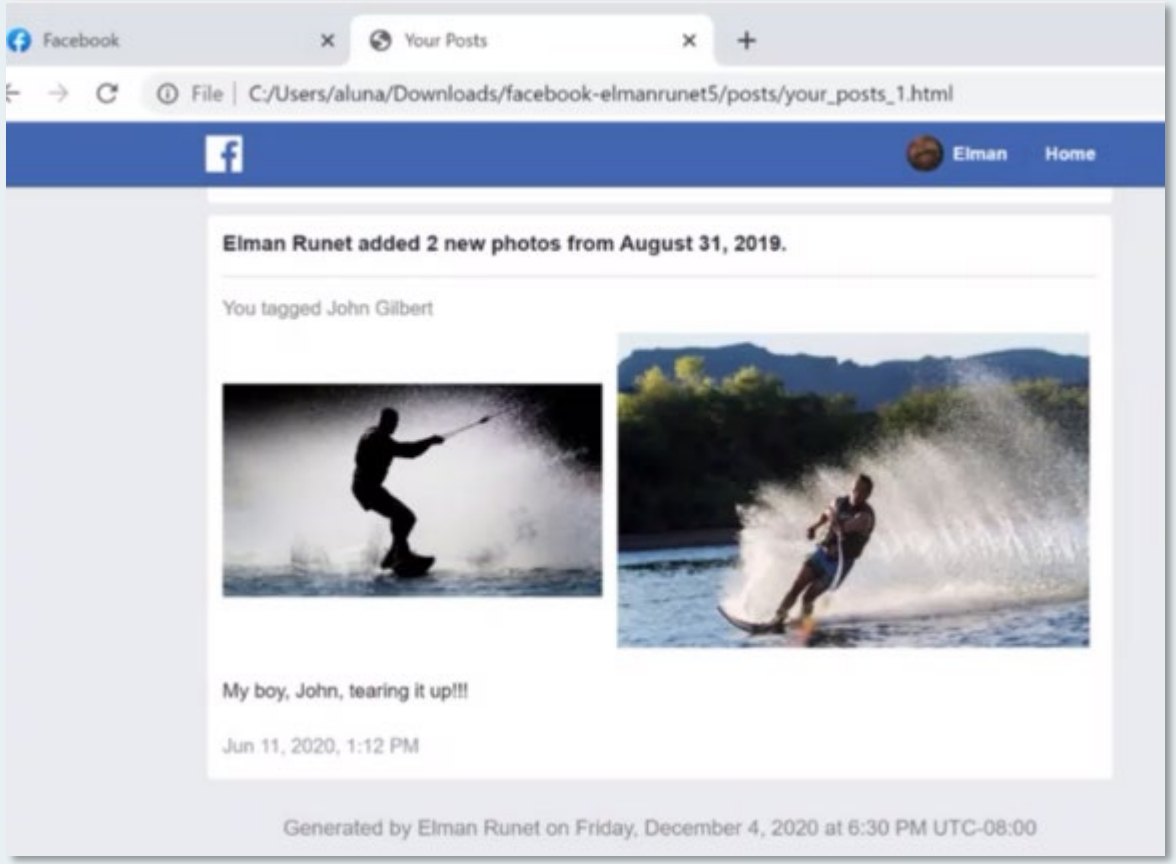
Great for Twitter, Tumbler, Facebook, and YouTube

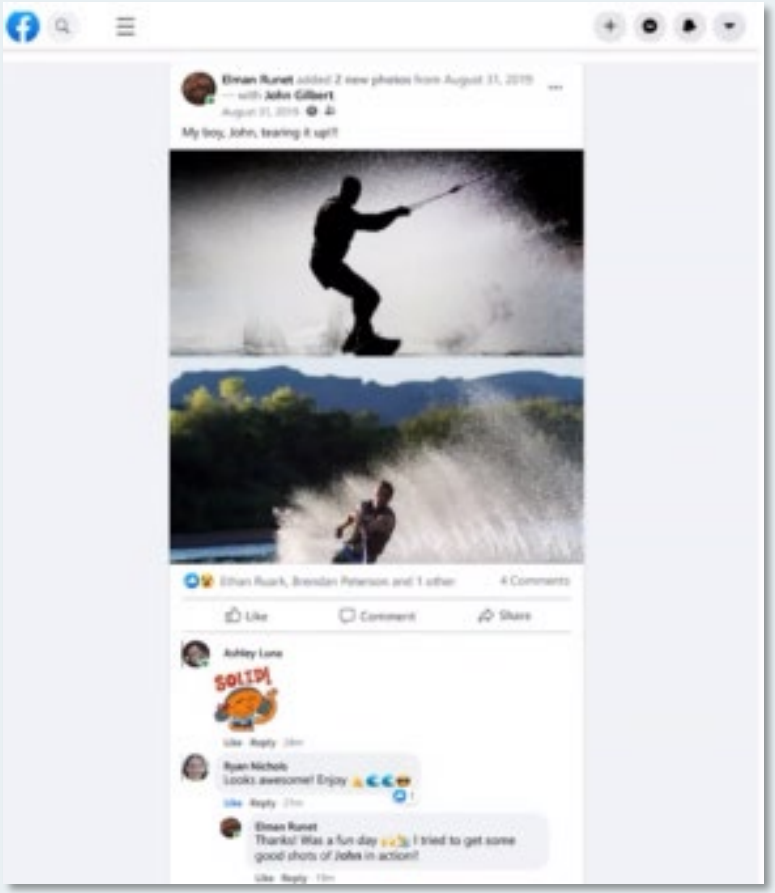
- Adding Instagram Auto Scanner

Also helpful for:

- Web Page Capture
- Web Crawls

DYI vs. X1





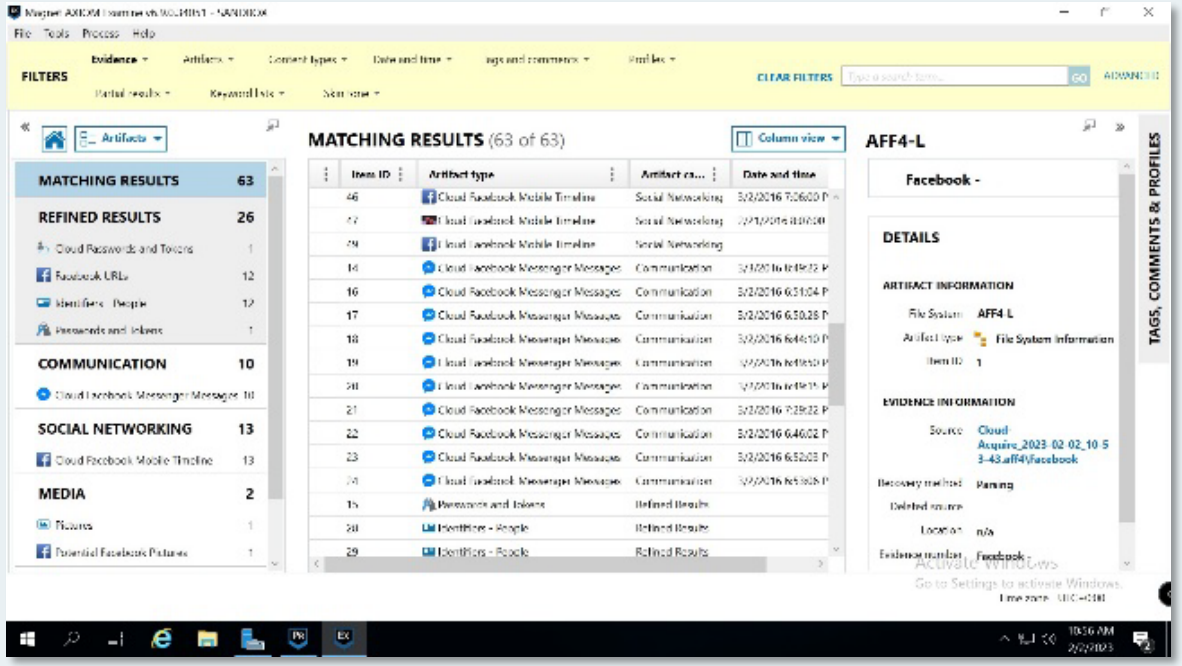
Images provided by X1 w/ permission to use during this presentation

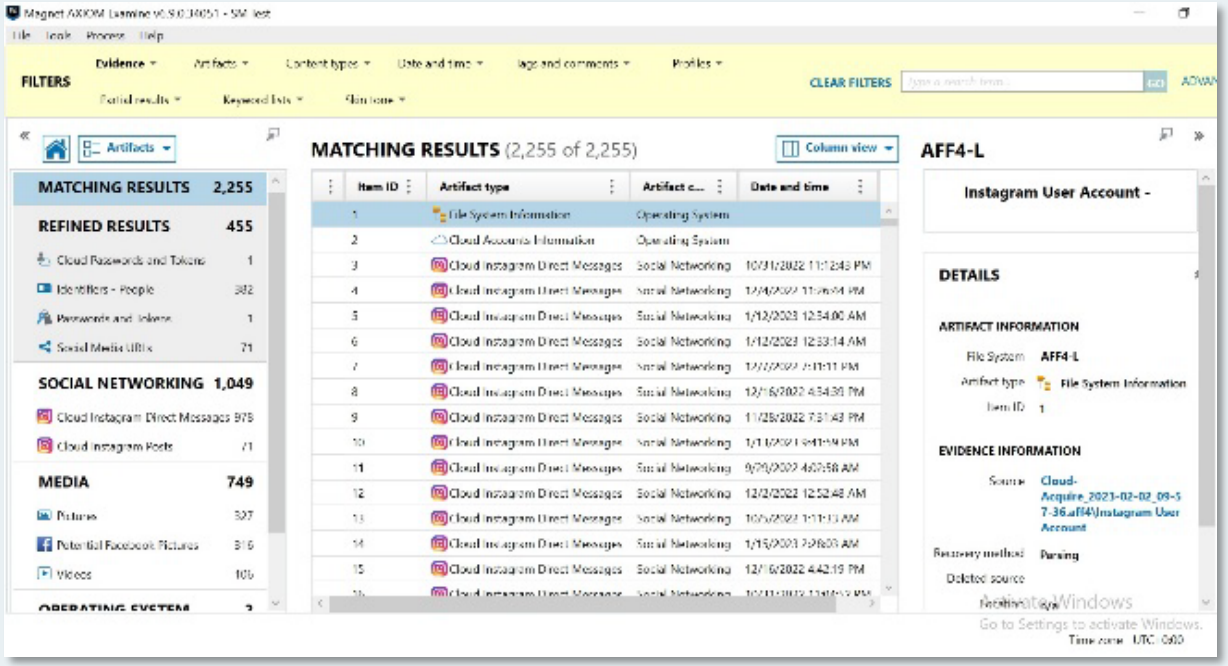
Axiom Rocks

Can Collect

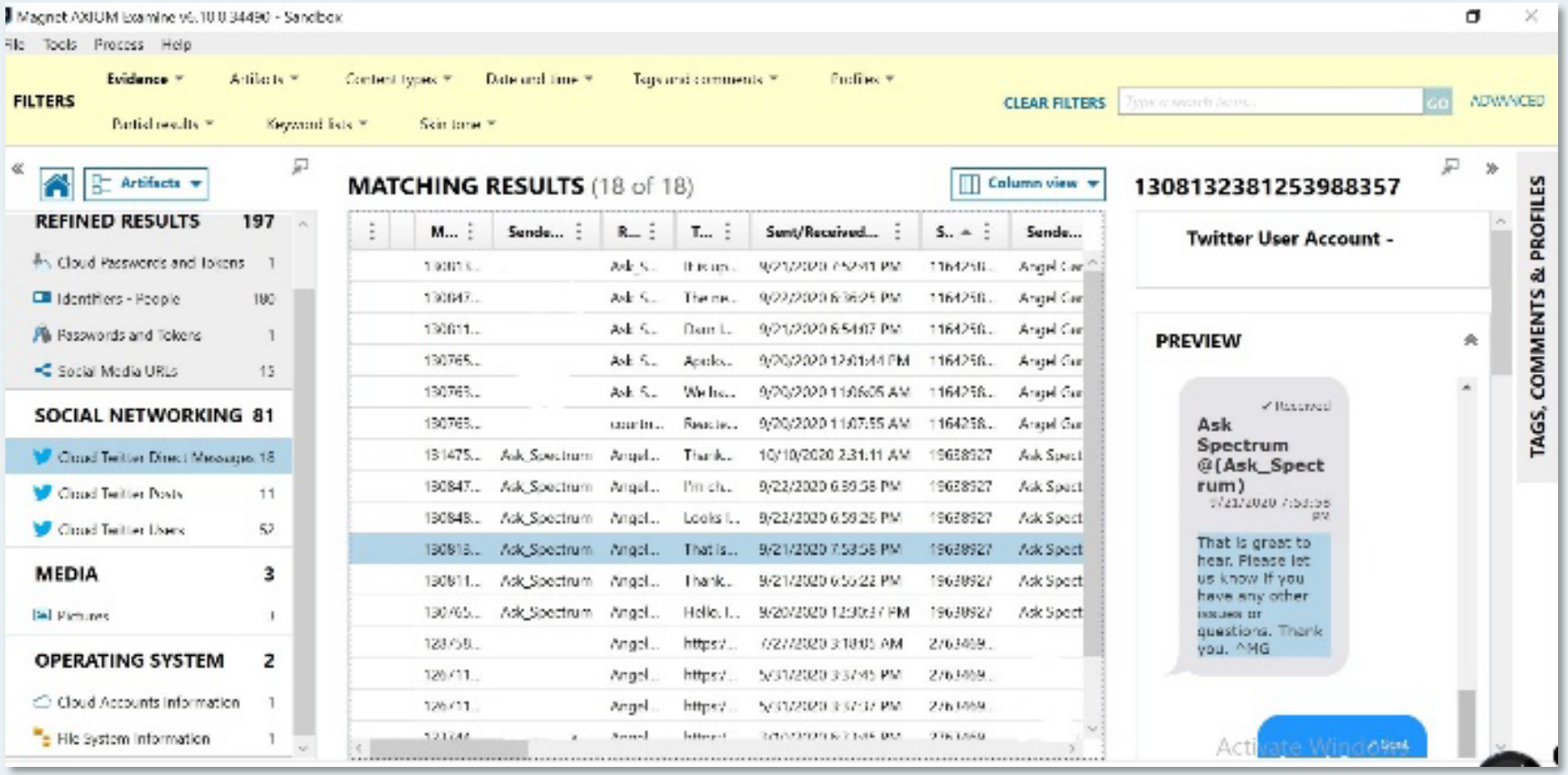
- Facebook
- Instagram
- Twitter
- WhatsApp
- Slack
- Microsoft Teams

Types of Data Axiom Can Collect





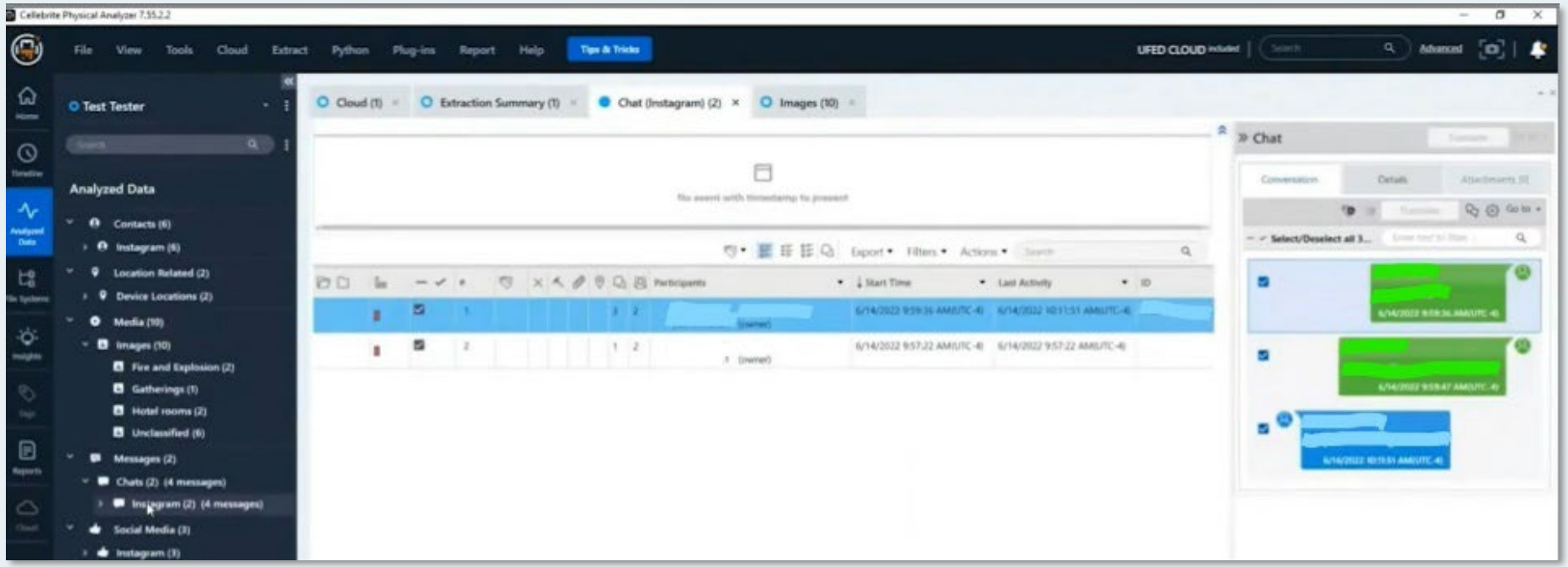
Types of Data Axiom Can Collect



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

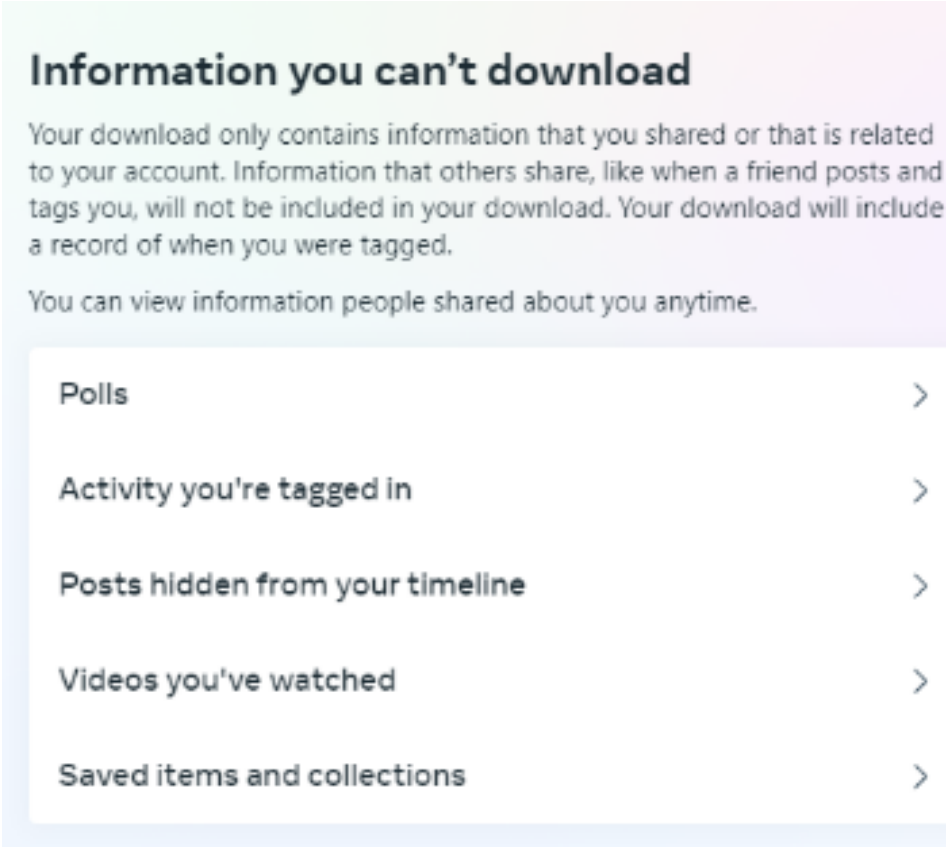
- Social Media Platforms are constantly changing
- Tools are limited to current versions of social platforms

Social Media Limitations

Content Ownership – Site Owner vs. User

Do we have permission to collect the posts?

- What about other's posts or comments?

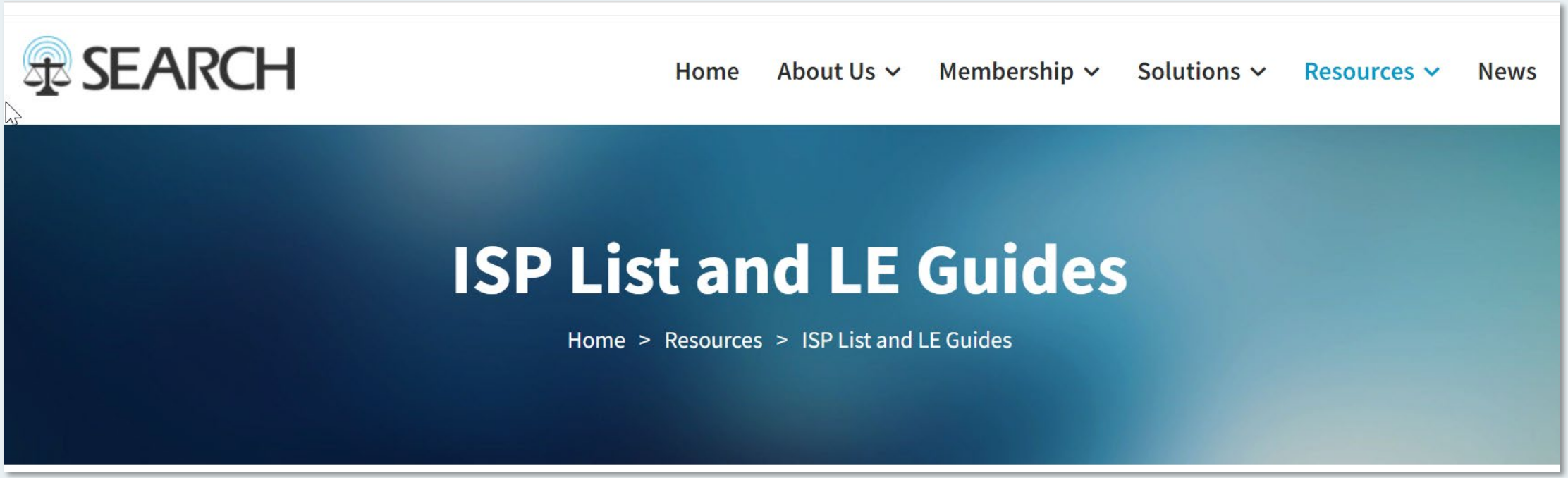


Social Media Limitations

- 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