Smoking Gun Forensics

Who: Tommy Thompson; certified DATAPILOT Operator & Digital Forensics Investigator
What: DATAPILOT 10 forensic tool
When: TBD by client
Where: TBD by client
Why: Digital evidence must be forensically acquired if it is going to be used in court proceedings.
How: If you think your case needs digital evidence collected off a phone or other digital device, reach out to theSGF team to discuss with Tommy, address resource issues, and schedule the tool deployment.

The DATAPILOT tool is handheld. Everything you need to perform a download comes with the device case. There is no need to have a computer or laptop on scene. It works on Apple and Android devices.

DATAPILOT offers a variety of options to capture data all within this handheld device. The time it takes to capture the data is going to depend on what method you use and the amount of data that is being downloaded.

Tommy evaluated his personal cellphone, iPhone 16, with about 50 gigabytes of data. Here is how long each method took to capture the data and what types were captured.

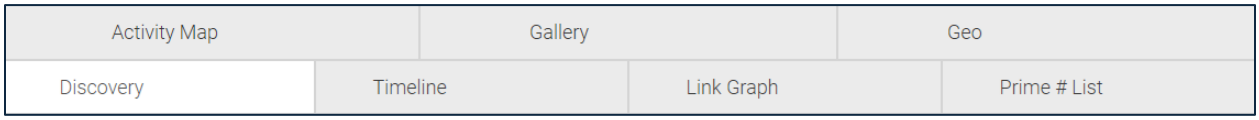
COMPLETE ACQUISITION (GIVE ME EVERYTHING)	1hr13m 55 app icons (apps downloaded to phone) 223 contacts 499 calls made/received 302 Google Calendar events 9890 Texts 3294 total files (photos, videos, downloads, etc.)

Last 30 Days **(Calls, Texts, Full app list, Full contact list)**	7m39s 55 app icons (apps downloaded to phone) 223 contacts 148 calls made/received 1667 Texts No photos or media unless they were sent via text
ADB Backup (The phone stores a backup of itself, and we grab that backup. This method requires additional analysis to parse.)	47m28s 55 app icons (apps downloaded to phone) 3283 total files (photos, videos, downloads, calls, contacts, etc.) This method is a timesaver up front but does require more time for analysis on the backend.

DATAPILOT DESKTOP ANALYSIS

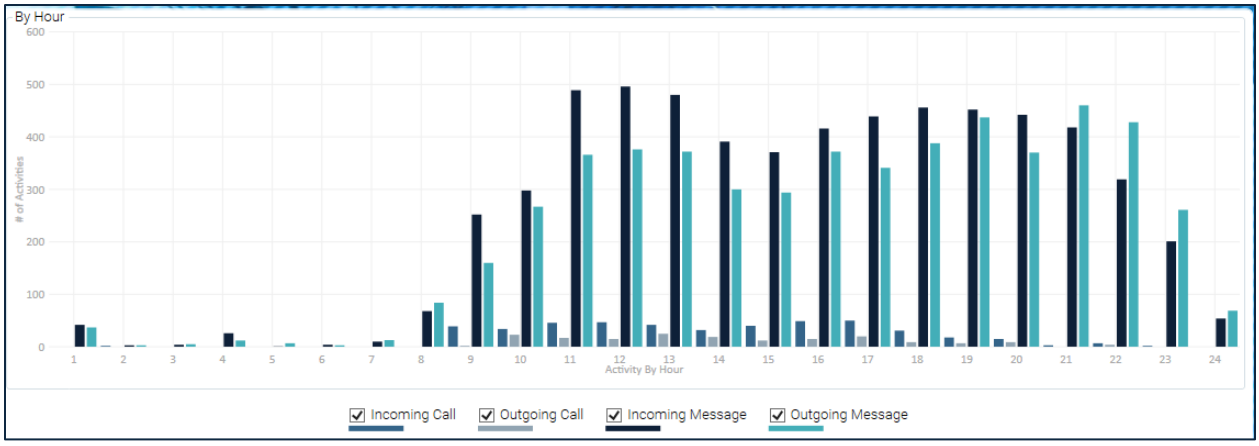
Okay, Tommy did the download…now what?

DATAPILOT offers a desktop analysis tool that can create graphs, charts, link diagrams, show maps data, and generate reports, all in one easy-to-use tool. If the client wants further analysis of the downloaded data, this software provides that. If they just want a download and a standard 500-page PDF report, it can do that too.



Activity Map: When was the device active?

We can sort by hour of the day, day of the week, or by date. This feature is great for building your timeline.



Prime # List: Who is communicating with this device?

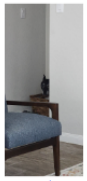
DATAPILOT automatically ranks every stored contact and number not stored, by how many times this device communicated with that number and how many times that number communicated with this device.

No.	Flag	Name	Phone # / Email address	Total	Call Total	Received Call	Dialed Call	Message Total	Inbox	Outbox
1			627	2712	1	0	1	2711	1273	1438
2			569	1109	72	43	29	1037	322	715
3			560	1058	52	25	27	1006	544	462
4			161	963	2	0	2	961	455	506
5			802	528	4	1	3	524	326	198
6			735	425	0	0	0	425	289	136
7			946	360	0	0	0	360	132	228
8			820	329	0	0	0	329	166	163
9			499	301	0	0	0	301	185	116
10			173	240	0	0	0	240	126	114

Messages Viewer: They said what?

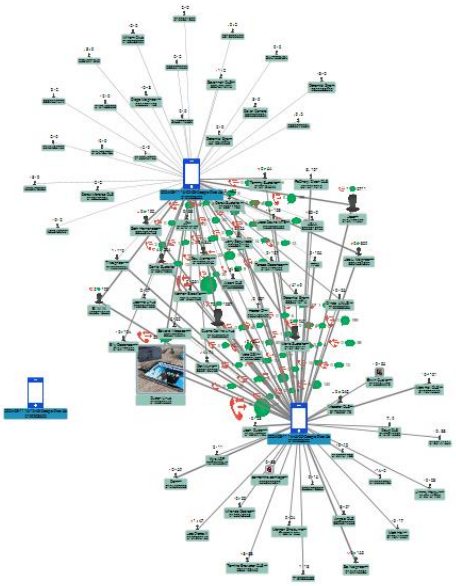
All data tells a story, and text messages can be a key indicator of a person's intent. They can also serve as standalone evidence of threats, harassment, bullying, and so forth. We need to capture this data in a forensically sound manner, as it may prove critical to our case. We cannot accept screenshots of critical pieces to our case, because screenshots cannot be authenticated. There are plenty of third-party apps that can spoof messages, emails, and even social media posts, so we need to ensure we are authenticating the message at its source.

The DATAPILOT analysis suite allows us to see where a message came from on the phone (inbox/outbox), who sent it or who it was sent to, what was said and if there was any media attached, and if that message was read by the device we're looking at.

Type	Number/Address	Name	Messages	Service	Status	Report
Outbox	+12	**	Okay		Sent	2024-08-11 16-02-58-Google Pixel 6a
Inbox	+12 +12	**	can i ride my bike to david's house to go swimming with me noah david and kevin		Read	2024-08-11 16-02-58-Google Pixel 6a
Outbox	+1		Creeper		Sent	2024-08-11 16-02-58-Google Pixel 6a
Inbox	512 210		 Resized_20240811_143004_1723404620158.jpeg		Read	2024-08-11 16-02-58-Google Pixel 6a

Link Analysis: Visualize the network around your subject.

DATAPILOT has an excellent feature that takes every text, call, shared photo, and puts it all in a link diagram that allows you to see who's who in the zoo and more importantly, generate follow on leads for your investigation.

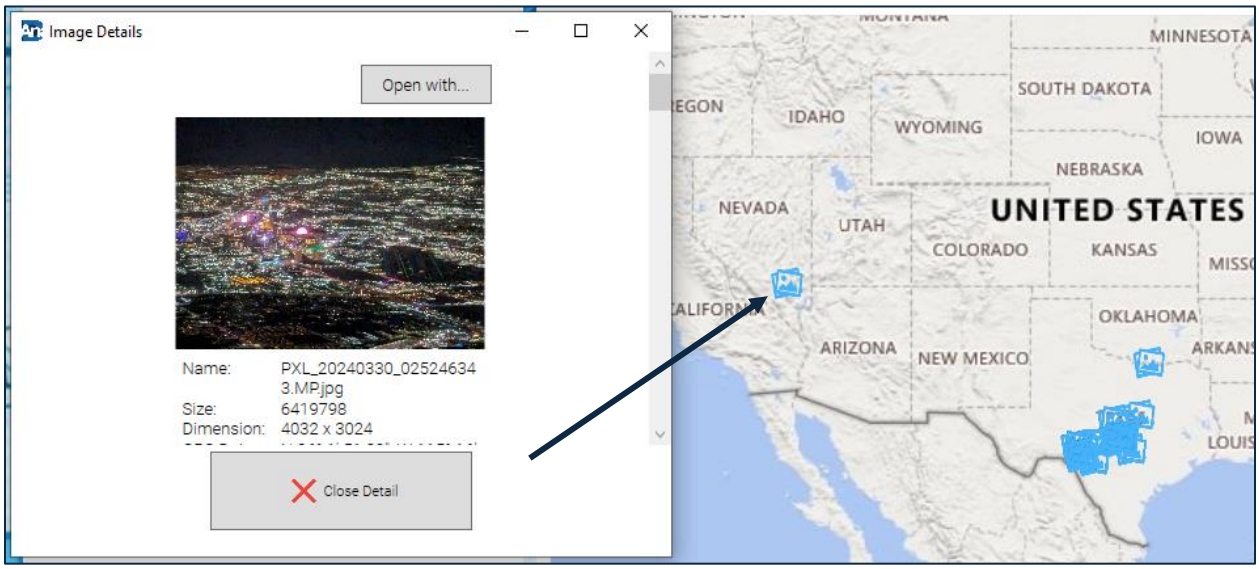


Gallery: What pictures and videos are on this device?

DATAPILOT pulls whatever amount of camera photos, downloaded pictures, videos, memes, screenshots, etc., that you tell it to. Each item will have EXIF data that may have date timestamps, GPS information, and other useful bits of information for your investigation.

Geo: What GPS data did you recover?

DATAPILOT's software can recover exchangeable image file format (EXIF) data from pictures, videos, and other media that contain that data set. DATAPILOT automatically generates a map view of that data, showing where photos and/or videos were taken. DATAPILOT is not going to recover GPS data from background apps or Google Map locations that pull GPS data. This feature is strictly for reading EXIF metadata and unlocking those files.



FAQs

- **Can DATAPILOT crack a phone's password?**
  - *No. This tool requires a password to operate and cannot be used against phones that do not turn on or are damaged beyond normal use. This tool is surgical in nature and is not simply a "plug and play" system. Contact Tommy if you think there may be something worth capturing on a phone or computer to see if the DATAPILOT will be effective.*
- **Can DATAPILOT get as much data as law enforcement gets with their tools?**
  - *No. Law enforcement uses a different tool that pulls an entirely distinct set of data stored deep within the phone's memory and includes deleted data. DATAPILOT struggles to recover deleted data but it can.*
- **Can DATAPILOT only get data from phones?**
  - *No. DATAPILOT has a unique feature called Linked Screen Capture that allows us to forensically capture critical data from HDMI devices. If the device uses an HDMI cable, the DATAPILOT can plug that cable into a special port and capture the data.*
- **Can you plug the DATAPILOT into a USB slot on a computer and download all the computer stuff, like cookies and email?**
  - *No. DATAPILOT is designed for a specific technical data set mostly available on phones. Using DATAPILOT on non-phone devices is possible but will require an advanced knowledge of technology and the data.*
- **How long does a download take?**
  - *It depends. That is like asking how long does it take to grow a tree? If you know what digital evidence you are looking for, the time it takes to capture it is minutes. If you do not know what you want and say, "give me everything" that takes hours. It is always best to consult with Tommy prior to deploying the DATAPILOT to ensure both efficiency and ability.*
- **Why can't the client just text me that witness photo or video?**
  - *If it is important to your case, you need to protect it by using forensic techniques. Both Federal and State rules of evidence recognize how digital evidence should be collected, and how it should not. DATAPILOT protects that evidence from being discredited as unauthentic.*
- **My client was sent an encrypted file, and they cannot open it. Can DATAPILOT open it?**
  - *No. DATAPILOT does not have the ability to decrypt files. This can be done after capturing the data, but the tool itself cannot.*

- **My client has video from that night, but they do not want to turn their phone over and lose access to it.**
    - *DATAPILOT can go after only whatever data the client or witness wants to provide. They can have their phone back in less than an hour.*
- ***What about Snapchat, Signal, WhatsApp, and those messenger apps?***
    - The unique ability to capture what is still on the device is what makes DATAPILOT so great for immediate triage and acquisition. DATAPILOT can capture a historical message stream from encrypted apps like Snapchat and WhatsApp if those messages are still viewable on the target phone. In most cases, a consented search of the device will result in an encryption passkey being initiated by the file system, which allows that message to be viewed. This is not always the case with after-the-fact seized phones where the software has to try and break into an encrypted file.
    - File-based encryption, end-to-end encryption, and locally stored keys which are no longer stored in the cloud, are all barriers that law enforcement must overcome to access the data residing in a phone. Advanced software is extremely powerful but is also financially out of reach for most small agencies and private businesses. Especially considering that expensive software vendor cannot guarantee you access to software versions that the device operating system has recently updated to.
- **What do you mean by "forensic capture," and why should I care?**
    - *As it pertains to Digital Media Evidence (DME), the courts are beginning to realize that the authentication of digital evidence may require more than testimony alone. The truth lies within the metadata. Digital data travels an irrefutable path because computers and machines cannot mislead the sender or receiver of the data stream. The only way to capture this metadata, its source and destination, is to use forensic tools like DATAPILOT.*
        - *DATAPILOT preserves the acquisition of the data by applying hash values along the way that will prove or disprove a piece of evidence was tampered with before trial.*