Accessing Locked Social Media Accounts

A DIGITAL FORENSICS CASE STUDY

THE SITUATION

The client needed to collect data spanning from 2012 to present day from specific custodians' machines and personal, business, and social media accounts. ID's forensic experts concluded that there were at least ten custodians that could be collected from – however social media login credentials could only be provided for two of the ten.

THE SOLUTION

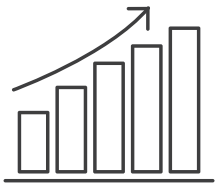
For the remaining platforms, ID took advantage of the multiple custodians in the request and the likelihood of their connection to one another on various and multiple social media sites. As long as ID possessed the login credentials for one custodian on a specific platform, ID would be able to complete a Concerned Party Collection for any other custodians connected to the first user. When a connection between two custodians could not be found, ID employed the Anonymous User Collection method.

Concerned Party Collection – Login credentials are not provided/known. ID does not have full access to custodian's account but can collect data by viewing custodian's account through a related user (i.e. a "friend").

Anonymous User Collection – No account information or login credentials are provided. ID can only collect data that is available to the public.

15
different sources of extracted data

5x
more data produced than expected



THE RESULT

In conclusion, ID extracted data from 15 different custodians and provided over five times more data than the client initially anticipated, properly preparing them with the information they may need for litigation.