Identifying Overlooked Sources of Social Media

Digital Forensics – Case Study & Analysis

Innovative Discovery, LLC

Context

The Client needed to collect data spanning from 2012 to present day from specific Custodians' machines and personal, business, and social media accounts. Innovative Discovery, LLC ("ID") was initially provided one personal computer and login credentials to three email accounts and one email marketing software account.

Challenges

A distinct challenge that arises with personal and business data collection, especially when social media is involved, is that the initial request from the Client will not include all the different platforms that are available for collection – consequently, some sources of data can be unintentionally left out or overlooked.

An incomplete initial data collection request also affects the extraction method(s) used, which are further discussed in the next section. If account information and login credentials are not provided, it is possible that only a partial collection may be completed.

Collection

ID uses three common collection methods:

(1) **Collect as User** – Account information and login credentials are provided by Client/Custodian. ID has full access to Custodian's account and data.
(2) **Concerned Party Collection** – Some account information is known, however 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 (For example: viewing the Custodian's Facebook profile through a user that is "friends" with the Custodian)
(3) **Anonymous User Collection** – No account information or login credentials are provided. ID can only collect data that is available to the public.

In this specific collection, ID was asked to collect all materials unless otherwise indicated by the Client. Consequently, ID's Forensic Experts analyzed the personal computer, marketing software and email accounts provided and concluded that there were at least ten more sources that could be collected from. The Client was immediately informed of these additional platforms and accounts and requested ID move forward with their collection as well – however login credentials could only be provided for two of the ten sources.

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 on that platform. When a connection between two Custodians could not be found, ID employed the Anonymous User Collection method. This method is typically only utilized when the first two methods are not available or appropriate, due to the fact that the amount of data collected can be significantly less than what is available.

In conclusion, ID extracted data from 15 different sources and provided over five times more data than the Client initially anticipated – significantly reducing the Client's exposure to any information previously thought to be unobtainable.