We built our tool to assist with inefficiencies and potential intelligence gaps. Social media analysis consumed a significant percentage of analysts' time conducting manual reviews of popular sites looking for suspicious posts, or posts that contain specific keywords or were authored by known actors. These manual reviews are not only inefficient, but the limited capacity of a manual review left many posts unreviewed. To address this, we built an application that automatically searches Facebook, Instagram, and Twitter for suspicious activity and saves evidentiary copies of suspicious posts, saving analysts' time and allowing the Client to more holistically leverage social media to further the mission of protecting Alaska.

To that end, we built a Windows Desktop Application that periodically searches the most popular social media sites (Facebook, Instagram, and Twitter) looking for keywords and parses flagged posts for the most relevant information. Additionally, the application supports flagging accounts so that every new post made will be saved regardless of whether it contains keywords. Our client is able to configure the keyword lists to tailor the product to specific investigations or institutional priorities, and can use the flagged users functionality to keep an eye on known actors that are of particular interest. To address the common tactic of suspicious posts being taken down quickly, the web scraping functionality downloads copies of the content onto the local drive. Recognizing this feature may impose substantial memory problems, the product supports the use of custom output directories to include external harddrives. Our web scraping scripts, written in Python, use a webdriver to emulate user actions. Necessary information is collected by the GUI and passed off the scraping scripts, and real time updates are printed to the GUI. Full results are written into a tabular html format that is easy to use and share.