Detecting Dirt

Computer/Internet Monitoring Data Analysis Techniques

Brian J. Kelly, Cyber Analyst - IPPC Technologies

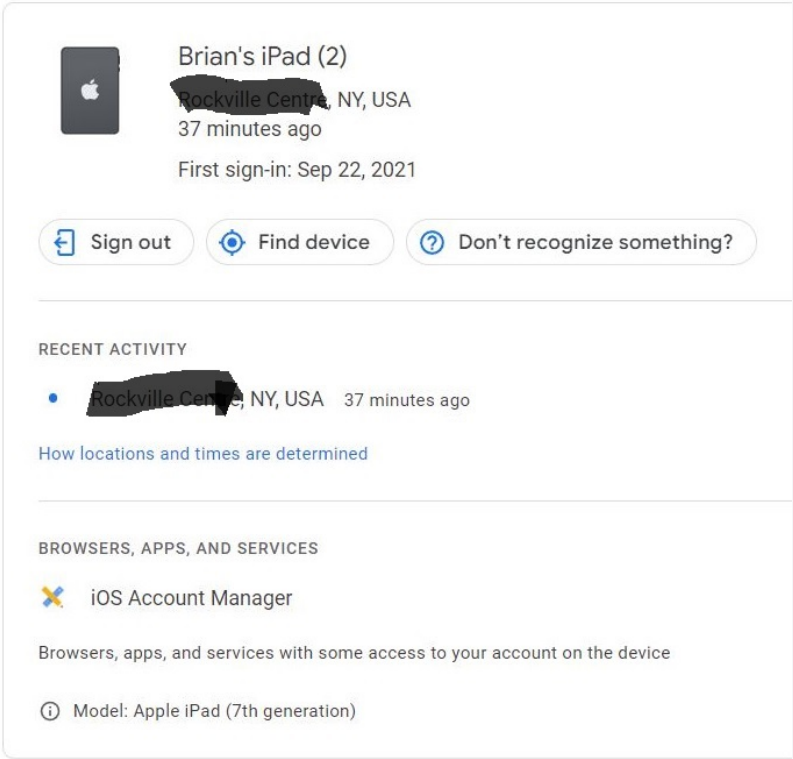
As a huge fan of HBO's critically acclaimed series The Wire, one of the phrases that stuck with me from the show was "doing dirt". Typically, this was used to explain individuals engaged in criminal activity, usually selling narcotics. As an officer, I incorporated the term into my vernacular as an umbrella term for violation or criminal activity while under supervision.

There are many nuances to the computer & Internet monitoring of persons under supervision but setting the parameters of what is and what isn't allowed is paramount. What devices can he/she use? Which devices are being monitored? What other devices are in the residence being used by family members? Asking these questions and collecting that information throughout supervision is extremely important in controlling risk. Once the parameters are

set and the person has an approved device being monitored, the hard work begins. Detecting “dirt” by analyzing computer & Internet monitoring data can be very straightforward (i.e. pornography) at times, and at other times, obscure. Many times as an officer, I was able to detect persons under supervision maintaining an unapproved and unmonitored Internet-capable device so they could “do dirt”. There are many strategies that officers can use to detect unapproved devices, from traditional supervision techniques (i.e. home contacts) to more technical solutions which include the analysis of data collected by computer & Internet monitoring technologies.

One strategy that reaped many benefits in this regard during my time as an officer was using data collected by Internet Service Providers (“ISPs”). It is safe to say that there are many people that maintain a Gmail email address, thereby having a “Google account”. Many persons under supervision maintained approved Google accounts, as reported to their officer. Google, as a regular course of business, maintains a significant amount of information on the user and the account. If you have a Google account, you can see for yourself what data is collected and maintained by logging into your account and clicking “Manage your Google account”. Once in this area, click “Security” and scroll down to “Your devices”. By expanding this view, you can see every device you used to access your Google account. You can also see when it was last used to access the account (see the screenshot below). Many persons under supervision are creatures of habit, so even though they would go to the lengths of obtaining an unreported/unauthorized device and using that device to “do dirt”, they would still use the Google account reported/known to their officer. We often used the information contained in the “Your devices” to further investigate the activity and eventually conduct a search to locate the device. Please be

aware that accessing a person under supervision's Google account would typically require consent or order from the Court. Check your agency's policies and other legal guidance before engaging in such activity. Other ISPs, such as Yahoo, collect and maintain similar information.



Officers can obtain leads from computer & Internet monitoring data that can be used as reasonable suspicion to gain access to a user account, searches, etc. For example, analysis may reveal the person under supervision received an email indicating a sign-in to their Google account from another device. As we pilot our Spotlight service, we have discovered these indicators and provided the case officer an alert regarding this activity. IPPC is also developing techniques to isolate two-factor authentication indicators to detect use of possible unreported/unauthorized devices. For more information on IPPC's services such as Spotlight, please contact me at bkelly@ippctech.net or by calling 888 WEB-IPPC (932-4772) extension 535.

2022 IPPC Certification Training

September 20-21, 2022

Microsoft Training Facility in Malvern, PA

IPPC is pleased to announce that we are brining back our in-person, hands-on training for supervision professionals. This two-day course covers all aspects of IPPC's monitoring software. But, also includes discussions on techniques to manually review smartphones, current cybercrime trends, and smart-devices of concern.

For more information on this course, as well as, the required registration form, please review the linked document. Please note that seats are limited and will be allotted on a first-come, first-serve basis.

IPPC Certification Training Packet

If you have any questions, please feel free to contact Phillip Danford at pdanford@ippctech.net.

Share

Tweet

Share

Forward

IPPC TECHNOLOGIES
PO BOX 60144
KING OF PRUSSIA, PA 19406
TEL: 888-WEB-IPPC (932-4772)
INFO@IPPCTECH.NET
WWW.IPPCTECH.NET