The Foundation of an Aggressive OSINT Operation:

A Former Facebook Investigator's Perspective

BY **CHRISTOPHER SALGADO,** CO-FOUNDER OF ALL POINTS INVESTIGATIONS, LLC

Facebook? Instagram? Twitter? LinkedIn? WhatsApp? TikTok? YouTube? Snapchat? Tumblr? Pinterest? Which platform offers the most valuable information for your OSINT investigation? Is there such a thing as an effective regimen when uncovering the truth about someone?

As both the physical world and the Etherworld continue to age, so too does our online investigative checklist. How do you remain vigilant to solidify the best ROI on your online exhaustion? Many times, the greatest challenge with OSINT is not a lack of information on a given subject but the navigation of the enormity of information on a subject. This plethora of information can come in the form of positive "hits" or false positives. Sure, there are caveats to these. Some results can appear to be false positives when they are, in fact, positive. They only appear to be false due to a lack of information at the time. An example is when the subject of surveillance is observed but dismissed as the subject only to later realize that this person was the subject after you ascertain additional information. These "delayed positive hits" can certainly be experienced in the cyber world as well.

Effective OSINT investigators consistently employ a robust regimen of investigative steps. These investigators remain relevant by routinely updating their regimen, per the new standards within the industry. The cyber world is ever-changing. This includes social media platforms, online interfaces and other various digital resources. It is critical that you not only identify an effective OSINT SOP for your investigations, but you must also dedicate yourself to ensure your agenda remains relevant. An overused example of this is the dismantling of Facebook's Graph Search. Now that Facebook's Graph Search has gone the way of the Dodo bird, what can stop the bleeding? When this tool was removed from the arsenal of many, some experienced unbridled despair and surrendered to the loss, believing that there was no hope in ascertaining similar results. Keep in mind that while some social media platforms have updated their capabilities and allowances, directly or indirectly, there are other options.

In order to be successful in OSINT investigations, you do not have to be any form of a hacker. You do not need to possess a degree in IT or any other technical degree. I can very effectively crack open a hard drive and unveil its secrets, including files or network maps that have been "deleted" with wiping programs;

however, I am not an "IT guy." IT folks have a more official and fundamental knowledge of computers than I do. I simply excel at prying into a computer and extracting the secrets within! (There is quite a difference between cyber and IT knowledge.) One of the skills that you do need in order to be a solid cyber investigator is diligence. Some cyber know-how – beyond Googling someone – is beneficial as well.

These days, more people are Google-savvy, more people are internet-savvy and more people are security-savvy online. This translates to more people being careful with their online information. They privatize their social media accounts, deactivate them or even delete them. Some may even remove their online information on websites outside of social media platforms. This makes your job more difficult. Although you can't request for your subject to abandon his safer online habits, you can upskill yourself to become more versatile to answer these problems. Keep in mind that these obstacles can surface with subjects who aren't tech-savvy or aware of these counter-surveillance measures. Your subject can simply benefit from a security enhancement on the platform that they exist on. So how do you remain effective with your mission?

Subscription databases can springboard your quest, but, in my opinion, they are not necessary. I am a staunch advocate of being independent of any one resource. This methodology offers double the benefit by negating any reliance on a paid resource and challenging yourself to achieve cyber greatness! First, you must identify your objectives: What is your main goal? Who/What is your subject? How will you conduct your research? Maybe you start with Googling a name, an address or a telephone number. There are innumerous resources to obtain good results in such inquiries. I am not a fan of listing resources because great resources today can turn sour the next. This is due to the ever-changing digital world.

As mentioned, a strong cyber investigator can go very far without any formal IT skills. Certainly, you've got a leg up if you come preloaded with some level of technical aptitude. Let me give you a few examples of some highly impactful efforts that can be obtained with no formal IT training. A strong cyber investigator can overcome websites that block their content to non-members. (EX: A landing page that forces you to sign in before you view a profile, thus, restricting non-members from viewing some or all content.). A solid OSINT investigator can download seemingly "protected" or "restricted" videos or photos for evidentiary purposes. (EX: A website that prevents videos or photos from being downloaded.) A reliable high-tech investigator can locate the original, unedited source of a modified photo. (EX: A cropped photo that had the incriminating context removed from it.) Additional examples of impactful results include identifying emails and passwords from data dump sites, uncovering dox evidence (online broadcasting of a person's PII), confirming inter-country moves via cargo shipping manifests, monitoring flights in real-time or locating historic flight records – even on private flights, identifying cryptocurrency wallets, etc. The list truly goes on and on.

Teasingly prying open the treasure chest of opportunities through a bit more intricate cyber skills, a diligent online investigator can extract and analyze video and photo metadata for analysis. (EX: A video/photo that does not indicate where or when it was taken but is a key piece of evidence.) Extreme results can include the identification of hidden text and hidden links on websites, decoding malicious anagrams within websites and even identifying viruses inside photo and video files. You can also locate servers used by subjects, which can help you confirm affiliations to companies or educational institutions. This can hold weight in corporate espionage cases, proof of employment or proof of education. IP addresses used by your subject can be located and their location can be identified. Be mindful of VPNs or IP spoofing, however.

While I understand that these latter more extreme examples aren't likely to be run-of-the-mill needs for everyone's investigations, I highlight them to introduce greater treasures offered by serious cyber investigations. Keep in mind that this is far from an exhaustive list of benefits that can be yielded through the power of an effective OSINT operation. And no, this operation does not have to entail a team of techies. It can truly be a single person operation.

Hopefully, I've gotten your attention with these opportunities to really reign in some impressive results for your clients. The next hard-hitting question is "How?" How do you upgrade the impact of your current OSINT methodology so that you experience similar results? – All the while, not requiring a one-to-three-year educational commitment with tuition that can cripple you for the foreseeable future? While I've had the great opportunity to provide such training to investigators, companies, law firms, law enforcement agencies and members of the European Commission across the globe, these training programs are tailored to each person's current skillset. A fundamental

understanding of their starting point prevents either a too elementary or too collegiate-level course that doesn't meet anyone's expectations. Having laid out this caveat, I will issue some general tips.

Reading code (HTML or JSON) is tremendously helpful! HTML or JSON is the code that makes up the website. This is beyond a simple interface that allows you to easily put together a website in 10 minutes, which is very popular these days. Even those easy-to-build sites have code behind the "drag and drop" method. Think of code as the recipe and ingredients that make up the website. If you can begin to understand code, you can significantly upskill yourself quickly. No, this won't give you the keys to the city, but it will allow you to rope in more effective results from your OSINT investigative efforts.

Another method is to dial back URLs to identify the origin of a webpage, photo, video or profile. Have you ever come across a great piece of evidence online, but you couldn't prove where it came from? Sometimes you can simply modify the URL and find your "smoking gun."

While these skills can certainly significantly boost your OSINT capabilities, the two main skills to sharpen your results that I would preach to you are diligence and versatility. Be diligent in your search; be versatile. OSINT is changing, cyber is changing, social media is changing. It behooves you to reinvent today's investigative plan from yesterday's. Stay relevant. Today's best cyber investigator can easily personify a 404 Error tomorrow by a lack of intentional effort to stay on top of changes in social media, search engine capabilities, privacy laws and OSINT investigations.

So, where do you go for these awesome results? All of the above can be available on the surface, deep and dark web. A word of caution, even in modern times, many people's perception of the surface web, deep web and dark web tend to be semi-incorrect or entirely incorrect. To clarify, all three can be viewed as layers of information in the Etherworld. The top layer is the surface web, the middle layer is the deep web and the bottom layer is the dark web.

The surface web – AKA clearnet – is the top layer, and it's the traditional arena of the web when you think of the internet. These are the websites that you likely visit daily or near-daily: Google, Yahoo, Bing, eBay, Amazon, YouTube, Wikipedia, Zillow, Yelp, news sites, restaurant sites, retailer sites, weather sites, car dealership sites and more. These websites are able to be indexed and queried via search engines.

The deep web is the middle layer within our visual; it is neither surface web nor dark web. It is the largest among all layers of the web. The starkest difference between the deep web and the surface web is that the deep web is not available via typical search engines. The deep web is the information that is possessed behind a log-in portal. Examples of the deep web are your email account, your bank account, your school account and social media (with many caveats). All of these sites require you to log in to view information. It is not quite publicly available. There is no external link to the deep web. Links are what search engines use to crawl and index sites. Think of the deep web as a disconnect from the surface web, leaving no physical path for search engines to travel through and get to it.

Finally, we are left with the infamous dark web – AKA darknet. The dark web is a very hot topic and a common buzz word these days. As such, the dark web may not appear to be as taboo as it was ten years ago. In fact, it may seem inviting to curious minds. Allow me to recalibrate your thoughts on the dark web by telling you to avoid it unless you absolutely have to engage it. The dark web is not for the simply curious. It remains as intense a place as it was ten years ago. It's a virtual haven for unfathomable illicit activity, and it possesses images that you cannot unsee by pressing an undo button.

The dark web can be a virtual sanctuary for gun sales, drug sales, hitmen for hire – including crowdfunded assassinations, child pornography, various types of sexual assault, human trafficking, terrorists, hackers, cybercrimes, counterfeit, other financial crimes and much more. If you can somehow dismiss all of this to answer your curiosity, know that some of the websites on the dark web are illegal. The URLs of dark web sites are unintelligible. Therefore, you may not know what you click on until you find yourself on a site that you wish you could Control+Alt+Delete from. If that doesn't dissuade you, know that the dark web hosts innumerable trolls who find joy in tracking down users who "don't belong" on their sites. These folks are serious hackers and criminals who can dismantle any less-than-robust obfuscation operation and unmask your true identity. Then the real-world problems can start.

From a practical perspective, the dark web is incredibly difficult to search. While some dark web search engines do exist, they regularly produce irrelevant results or outdated links, given the great instability and encryption of dark web sites. Although many people believe that the dark web must be navigated via exclusively dark web browsers, it can actually be viewed via the surface web. Given my thoughts on the dark web, I will refrain from relaying how this can be done. I will tell you that if any of your surface web results end in .ONION, do not view the link without the proper professional obfuscation set-up. This is a dark web link.

Although the dark web lives up to its reputation, there are legitimate sites and uses for it. Its encryption anonymizes persons, which can be helpful for whistleblowers, victims of ongoing crimes, or those seeking refuge. Various professionals are also known to utilize the dark web for such engagement.

In summation, the multi-faceted World Wide Web has proven to be a bittersweet resource to OSINT investigators. This is because the internet can offer a seemingly unending buffet of results to even your well-tuned queries. Depending on your objective, this can be rewarding or overwhelming. Effective OSINT investigators are much more impactful than Googlers and abide by a modern, robust SOP that adapts to the frequent changes in the OSINT world. Those changes come in the form of social media updates, other platform restrictions and new Terms Of Use on other websites. Nonetheless, as those changes continue to surface, remember that when a door closes, a window opens. There's almost always another way to obtain your sought information through creative investigative efforts. And in the event no window opens, move to another home and start your search over again! **PI**

Christopher Salgado is a former managing investigator with Facebook and is currently Co-Founder of All Points Investigations, LLC, a global cyber and physical investigations firm serving Fortune 100 companies. He has been a trusted security and investigations leader for 18 years in corporate risk, brand protection, supply chain, surveillance and SIU investigations. He has presented on cyber and physical investigations to members of Europol, Interpol and the European Union. Any questions or comments? Contact him at csalgado@allpointsinv.com. Thank you for reading!