Hunting: Elmer Ngo

Saturday, December 30, 2023 4:21 PM

Let's talk about the FBI today.
FBI OPEN UP! :)

There is an article on their website asking for assistance on an investigation regarding Elmer Ngo. He is being charged with sexual exploitation of minors and coercion and enticement of minors.

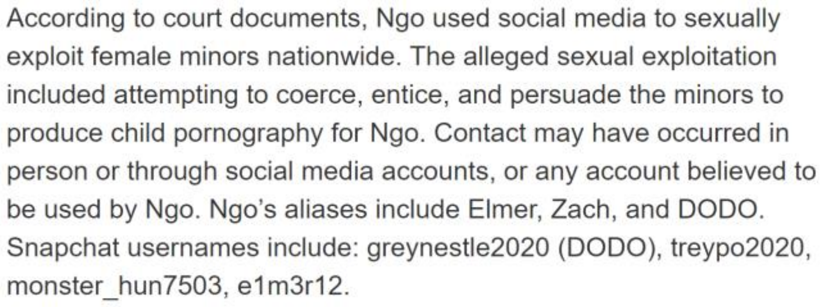
The FBI (FBI_Elmer_Ngo) is specifically asking for victims to step forward and help build a strong case against him. When you have actual people come forward and testify it makes the case stronger instead of just presenting facts. Sure he will still face a sentence with the facts but he will face more punishment when victims testify.

That got me thinking. What if we don't have to wait for victims to come forward. What if we come to them?

Here's why:
It's extremely difficult for victims to come forward and face the monster in person who terrorized their life. This will prove to be much more difficult yes, but all we have to do is find them. Remember these victims had to live through it. We have to make it easier on them.

Here's how:
This can be possible with more information available to us. Such as devices used in these crimes, social media accounts used, learning the language (lingo) the criminal used to coerce the victims. They all have specific patterns which if you want to read more about it you can find out here from here John Douglas (Masterclass) and by using Google_Dorking. Google dorking involves using operators in the Google search engine to locate specific sections of text on websites that are evidence of vulnerabilities, for example specific versions of vulnerable Web applications. We don't always have to use techniques for their intended purposes. This is where thinking outside the box comes into play and trying to be innovative to produce results.

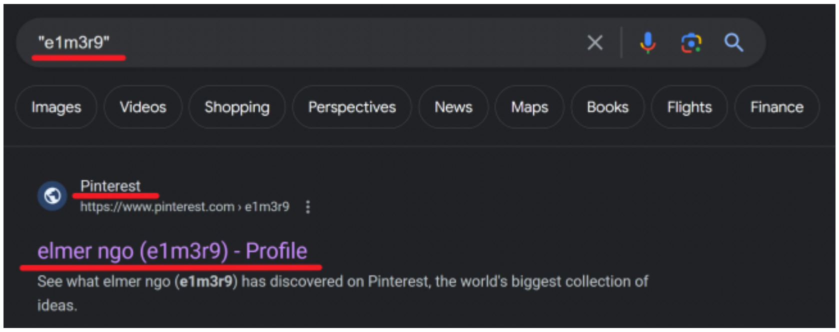
Here's what we know from the FBI:
Aliases that Elmer Ngo used, Contact may have occurred in person or through social media accounts, or any account believed to be used by Ngo. Ngo's aliases include Elmer, Zach, and DODO. Snapchat usernames include: greynestle2020 (DODO), treypo2020, monster_hun7503, e1m3r12.



According to court documents, Ngo used social media to sexually exploit female minors nationwide. The alleged sexual exploitation included attempting to coerce, entice, and persuade the minors to produce child pornography for Ngo. Contact may have occurred in person or through social media accounts, or any account believed to be used by Ngo. Ngo's aliases include Elmer, Zach, and DODO. Snapchat usernames include: greynestle2020 (DODO), treypo2020, monster_hun7503, e1m3r12.

It's a great start for us. How can we improve this list? We can use Fuzzing. We're going to change around some of the numbers and letters that can resemble the same meaning the criminal tried to use. Example: E with diacritics: Ĕ ĕ Ḝ ḝ Ê ê Ê ê Ê̄ ê̄ Ê̌ ê̌ Ề ề Ế ế Ể ể Ễ ễ Ệ ệ Ẻ ẻ Ḙ ḙ Ě ě Ɇ ɇ.
We can use this method to create countless variations that the criminal may use.

Here's what I did:
For starters I replaced the 12 at the end of e1m3r12 with time of date in years. I started off with 23 for 2023.
Example: e1m3r23, e1m3r22, e1m3r21, e1m3r20 all the way down to 1. You may not get search results with each variation.
e1m3r9 gave us a hit from google.com.

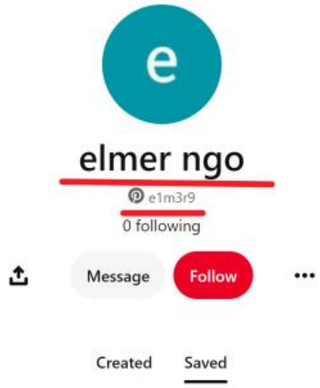


"e1m3r9"

Pinterest
https://www.pinterest.com › e1m3r9

elmer ngo (e1m3r9) - Profile

See what elmer ngo (**e1m3r9**) has discovered on Pinterest, the world's biggest collection of ideas.



elmer ngo

e1m3r9

0 following

Heres how this can help:
This will provide more evidence for the FBI. We are now strengthening the pattern that the criminal uses with social media sites which is what we learned from John Douglas (Masterclass). We will have more information such as Geotagging which we can find the locations where that account may have been logged in at and the possible device used. This device may not have been confiscated during the investigation and this new device can produce evidence that may involve messages with the victims we did not know about. This can also lead to extra IP addresses the criminal may have used depending on the log in locations, if there was Wi-Fi used such as Starbucks Wi-Fi. Which can then lead us with dates accessed and investigate security footage from the locations and get images of the criminal. By the way the logs from searches using public Wi-Fi could stay there for quite a while depending on the security settings used by Starbucks.

Recap:
Digital Footprint Analysis: Leveraging both algorithmic and manual investigation techniques to scrutinize the digital traces left by suspects across various online platforms.

Advanced Google Dorking Techniques: Utilizing specialized search queries to unearth concealed online information, pivotal for unearthing evidence and identifying potential victims who may not come forward voluntarily.

Username Pattern Recognition: Employing analytical methods to link multiple online identities of a suspect, thereby offering a comprehensive view of their digital persona and activities.

Geotagging and IP Address Correlation: Integrating geotagging data with public Wi-Fi logs, this method aims to trace the physical movements of suspects, enhancing the precision in locating and apprehending them.

Proactive Victim Identification: Developing a sensitive approach to pinpoint and assist potential victims, thereby strengthening the case against perpetrators and offering crucial support to those affected.

There you have it. Hopefully this lesson can help you find more information for what you need it for. Remember you don't have to use this technique for investigations, be creative and see what else you can use it for.

Gustavo Flores

FBI_Elmer_Ngo
FBI. “Seeking Victim Information in the Elmer Ngo Investigation.” How We Can Help You, FEDERAL BUREAU OF INVESTIGATION, 14 Dec. 2023, www.fbi.gov/how-we-can-help-you/victim-services/seeking-victim-information/seeking-victim-information-in-the-elmer-ngo-investigation.

Google_Dorking
Wikimedia Foundation. (2023, November). *Google hacking*. Wikipedia. https://en.wikipedia.org/wiki/Google_hacking

John Douglas (Masterclass)
MasterClass. *John Douglas: About the Former FBI Criminal Profiler*, https://www.masterclass.com/articles/john-douglas.

Fuzzing
https://owasp.org/www-community/Fuzzing

Geotagging
https://en.wikipedia.org/wiki/Geotagging