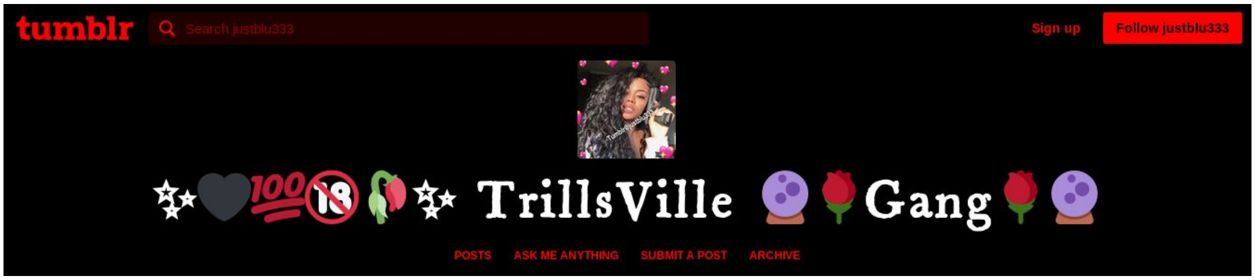
OSINT Investigations On Tumblr

We often forget about Tumblr in OSINT investigations and it is not as commonly used in investigations as some of the bigger social media platforms such as Twitter, Facebook, and Instagram. Still, Tumblr offers a wealth of information for open source intelligence (OSINT) investigations. This is largely due to the age of the Tumblr platform, which was founded in 2007, and the large amount of accounts that have gone inactive over the years without having their information removed from the internet.

These days many targets do well to sanitize or misattribute their personal information, such as employing an alias or by not revealing too much information about their personal lives, on freshly made accounts. Many of these same targets failed to practice such methods on their older accounts, such as a former Tumblr blog, thus leaving vital information of investigative importance out in the open. That being said, not all Tumblr accounts will have the same points of exploitation.

Some of these points may be hidden due on the user's blog layout or missing outright. Additionally OSINT investigators may have a difficult time remembering the totality of points on a Tumblr profile which can be exploited, particularly if Tumblr is not a regular platform in which the investigator frequents. This article is designed to mitigate these challenges by guiding investigators through the Tumblr attack surface for OSINT exploitation.

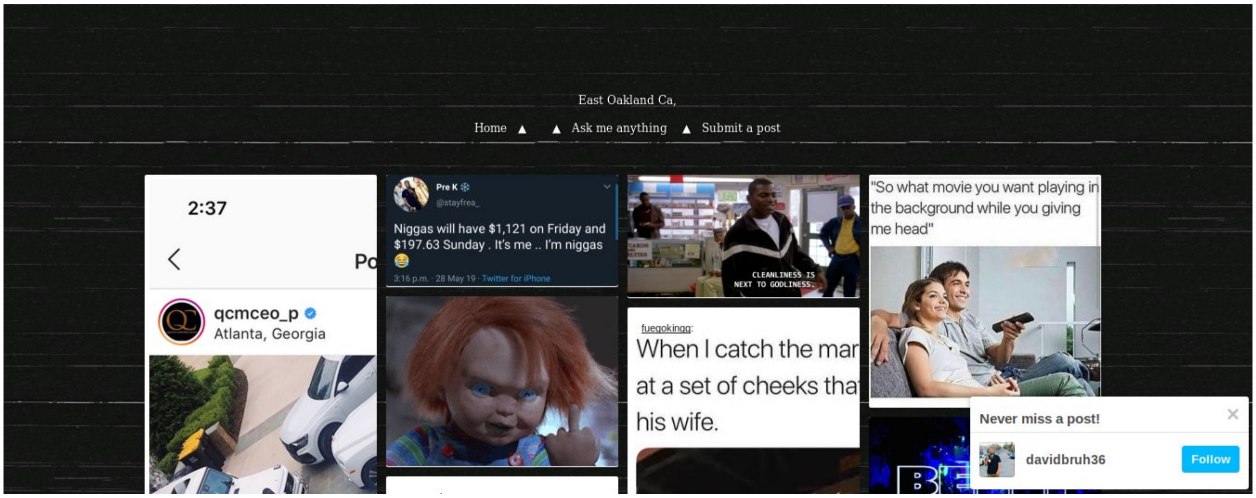
The Username



Tumblr usernames are one of the few points of exploitation that will be available by default for all Tumblr accounts. This username will appear in the url (justblu333.tumblr.com in the example above) as well as on multiple points on the user's blog.

Pay particular attention to any identifiable information present in a username such as possible first names, year of births, or locations. As many people use the same username across a number of sites, looking for the username on other platforms is also a good way to locate additional accounts by the same user. That being said, be wary of common usernames which will provide you with false positive matches. Looking at the Tumblr account above, I was able to locate a number of additional social media accounts, including Instagram and Pinterest, likely owned by the same user as the justblu333 Tumblr account.

Profile Photo



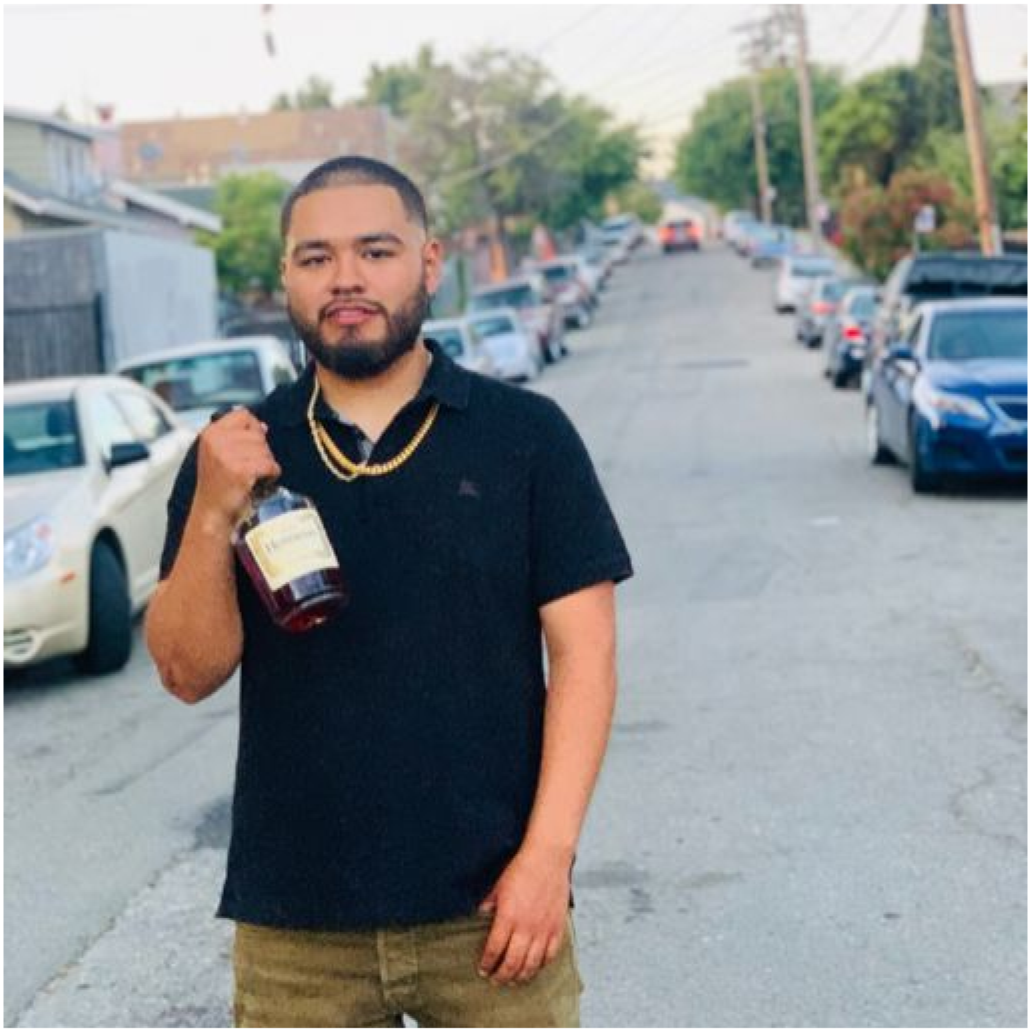
Niggas will have $1,121 on Friday and $197.63 Sunday . It's me .. I'm niggas 😂

When I catch the mar
at a set of cheeks tha
his wife.

"So what movie you want playing in the background while you giving me head"

How long did it take you to locate the account's profile photo above? (Hint: bottom right.) Not all Tumblr accounts will have a user uploaded profile photo, and some that do may have it hidden on their page due to their custom theme such as above.

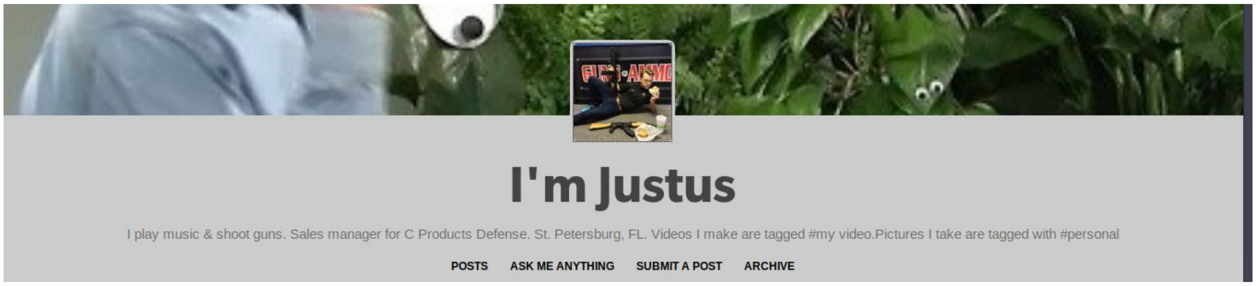
Profile photos may provide an insight to how the user behind the account looks and may also be exploited to locate additional accounts. Profile photos should be inspected to determine any identifiable information such as people, locations, foreign language content, etc. Even unique clothing or unique objects can be beneficial in determining where a photo was taken or who is depicted. As a rule of thumb, always utilize a reverse image search tool (such as images.google.com) on photos when possible. This helps rule out the possibility of a user pulling a profile photo from elsewhere on the web and passing it off as their own. A reverse image search may also provide insight on where else the photo appears online which allows the investigator to locate additional accounts. A high resolution image is much better to work with than the small one provided by default. Looking at the above account, I utilized a homemade javascript bookmarklet to grab the full size profile photo of the account.



Reverse image searches came back negative, so there is not a whole lot to go off of in terms of finding additional accounts with the same profile photo. That being said, the lack of a reverse image hit increases the chances that this is indeed the Tumblr user's original photo. The photo's content only provides us with the information that the user is likely a male close to or of drinking age and that he is in a city with parallel street parking and in a country where cars drive on the right based on the arrangement of parked cars (with the blue one on the right being an outlier).

On its own that is not a lot to go off of, but should an investigator be able to narrow down a location later they could likely match it to a street on Google maps using the row of trees and the unique buildings found on the left side of the photo. Although I could have provided a better example here where more information was found, I wanted to show that not all information points will provide valuable information all the time.

Biography



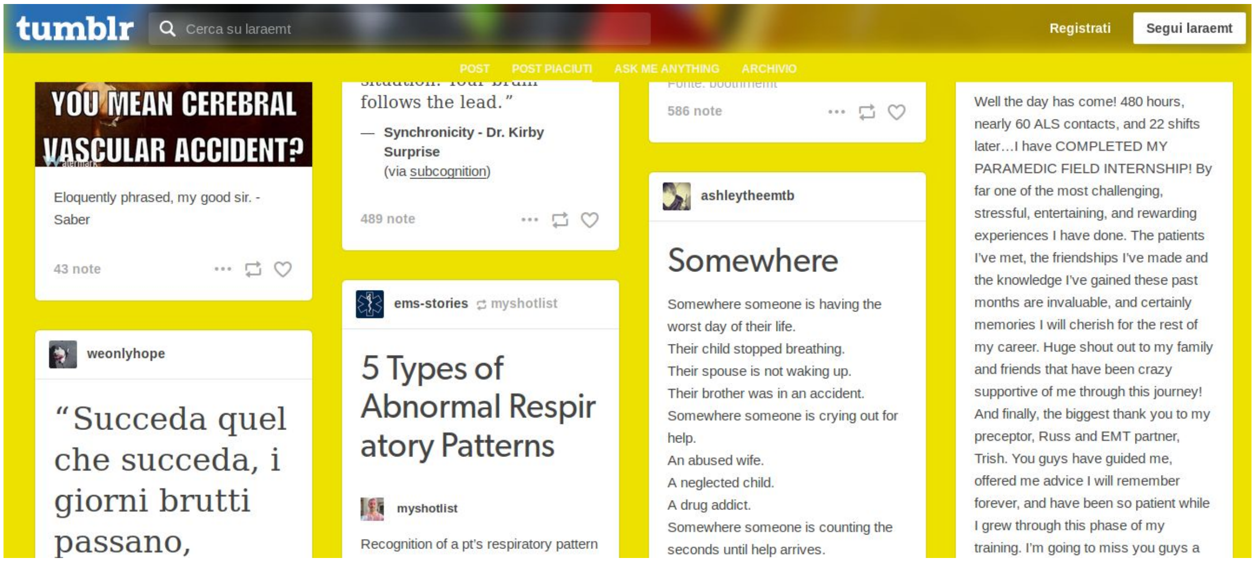
I'm Justus

I play music & shoot guns. Sales manager for C Products Defense. St. Petersburg, FL. Videos I make are tagged #my video.Pictures I take are tagged with #personal

For accounts that have biographies, an investigator can usually find relevant real-world information on the account owner here. Popular bits of information found in this section include hobbies, locations, links to other accounts owned by the user, and partial names. As a user can enter whatever they wish here always be sure to verify information as they could also use this information for misattribution by providing intentionally false information to complicate investigations.

In the example above I can see that this user is active in the firearms community, and it would be a good idea to look in those areas to see if he shares the same username. He also provides a first name and the location to where he works, which would facilitate a further search via social media. Using the information the user above provided in his biography I was able to quickly find his associated Facebook account.

Likes



YOU MEAN CEREBRAL VASCULAR ACCIDENT?

Eloquently phrased, my good sir. - Saber

43 note

weonlyhope

“Succeda quel che succeda, i giorni brutti passano,

follows the lead.”

— Synchronicity - Dr. Kirby Surprise
(via subcognition)

489 note

ems-stories myshotlist

5 Types of Abnormal Respiratory Patterns

myshotlist

Recognition of a pt's respiratory pattern

586 note

ashleytheemtb

Somewhere

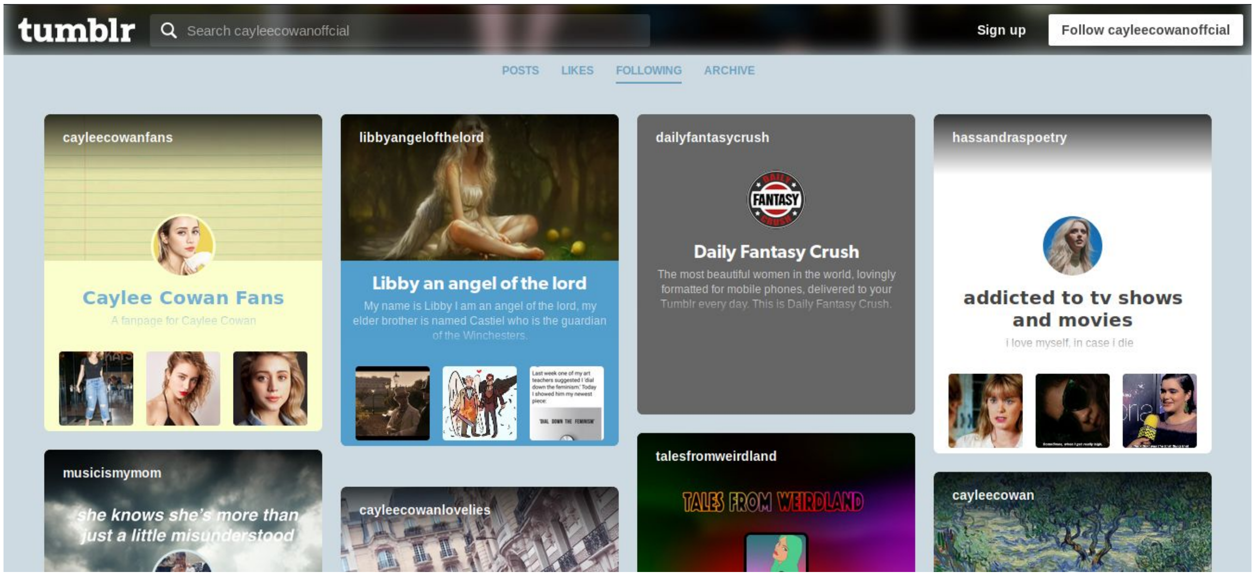
Somewhere someone is having the worst day of their life.
Their child stopped breathing.
Their spouse is not waking up.
Their brother was in an accident.
Somewhere someone is crying out for help.
An abused wife.
A neglected child.
A drug addict.
Somewhere someone is counting the seconds until help arrives.

Well the day has come! 480 hours, nearly 60 ALS contacts, and 22 shifts later…I have COMPLETED MY PARAMEDIC FIELD INTERNSHIP! By far one of the most challenging, stressful, entertaining, and rewarding experiences I have done. The patients I've met, the friendships I've made and the knowledge I've gained these past months are invaluable, and certainly memories I will cherish for the rest of my career. Huge shout out to my family and friends that have been crazy supportive of me through this journey! And finally, the biggest thank you to my preceptor, Russ and EMT partner, Trish. You guys have guided me, offered me advice I will remember forever, and have been so patient while I grew through this phase of my training. I'm going to miss you guys a

Investigating a user's likes can be finicky. Sometimes users hide this section of their profile with a custom layout and sometimes it is not enabled at all. The quickest way to determine if they have the likes section enabled is to add “/likes” to the end of their Tumblr account (ie user.tumblr.com/likes). If you receive an error then likes are either disabled by the user or they have not liked any posts yet. If they have likes enabled you will see the posts that the account has liked.

This will help establish some basic information such as what users on Tumblr they interact with most and what type of content they are associated with. It also isn't uncommon for a user to like posts that include photos they are in. The likes from the above user are heavily focused on posts about the medical and EMT fields. Additional information for the account shows that the user is indeed training to enter this field of work. They also like many posts that are written in both English and Italian, suggesting that they have at least some understanding, if not fluency, in both of the languages.

Followers and Following



cayleecowanfans

Caylee Cowan Fans

A fanpage for Caylee Cowan

libbyangelofthelord

Libby an angel of the lord

My name is Libby I am an angel of the lord, my elder brother is named Castiel who is the guardian of the Winchesters.

Last week one of my art teachers suggested I 'dial down the feminism.' Today I showed him my newest piece:

'DIAL DOWN THE FEMINISM'

dailyfantasycrush

Daily Fantasy Crush

The most beautiful women in the world, lovingly formatted for mobile phones, delivered to your Tumblr every day. This is Daily Fantasy Crush.

hassandraspoetry

addicted to tv shows and movies

i love myself, in case i die

musicismymom

she knows she's more than just a little misunderstood

cayleecowanlovelies

talesfromweirdland

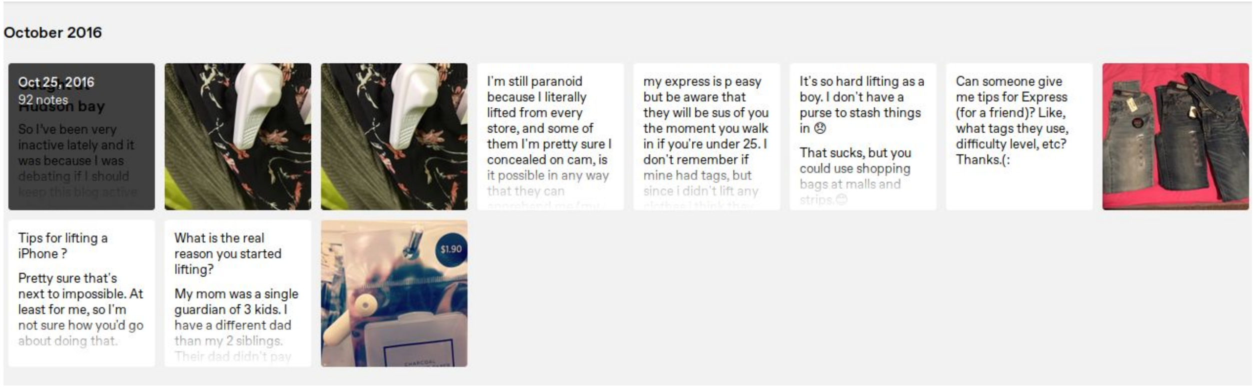
cayleecowan

Investigating a user's followers and following is similar to investigating their likes. Following and followers can be hidden by the user, however simply hiding the links to these pages is not enough to hide the pages from prying eyes. If the user has their following and/or followers enabled you can append "/following" or "/followers" to the end of their Tumblr account (ie user.tumblr.com/followers or user.tumblr.com/following). If an error is displayed then the user has likely disabled this feature.

The user is much less likely to have Followers enabled, and when they do users tend to have a number of different ways of displaying the information (such as here or here). A user's following is far more consistent and tends to show a stronger and more relevant association than followers because it is the target that is choosing the follow these blogs.

Ideally, if you have a list of the blog's followers and following you can parse out the mutuals to see if there are any additional accounts that may be associated with the subject in real life or virtually, and therefore may contain additional information on the original target. Even if your original target practices good OPSEC chances are not all of their mutuals will do so. This may provide additional breadcrumbs that make it easier to confirm some previous assumptions or perhaps uncover additional photos of the subject. In the above example, the user follows a great deal of blogs that are also associated with the same actress as fan pages. There are additional photographs that appear in some of the blogs the account follows that is not in the original target's.

Posts: User Archives



October 2016

Oct 25, 2016
92 notes
Hudson bay
So I've been very inactive lately and it was because I was debating if I should keep this blog active

I'm still paranoid because I literally lifted from every store, and some of them I'm pretty sure I concealed on cam, is it possible in any way that they can apprehend me (my

my express is p easy but be aware that they will be sus of you the moment you walk in if you're under 25. I don't remember if mine had tags, but since i didn't lift any clothes I think they

It's so hard lifting as a boy. I don't have a purse to stash things in ☹

That sucks, but you could use shopping bags at malls and strips.😊

Can someone give me tips for Express (for a friend)? Like, what tags they use, difficulty level, etc? Thanks.(:

Tips for lifting a iPhone ?

Pretty sure that's next to impossible. At least for me, so I'm not sure how you'd go about doing that.

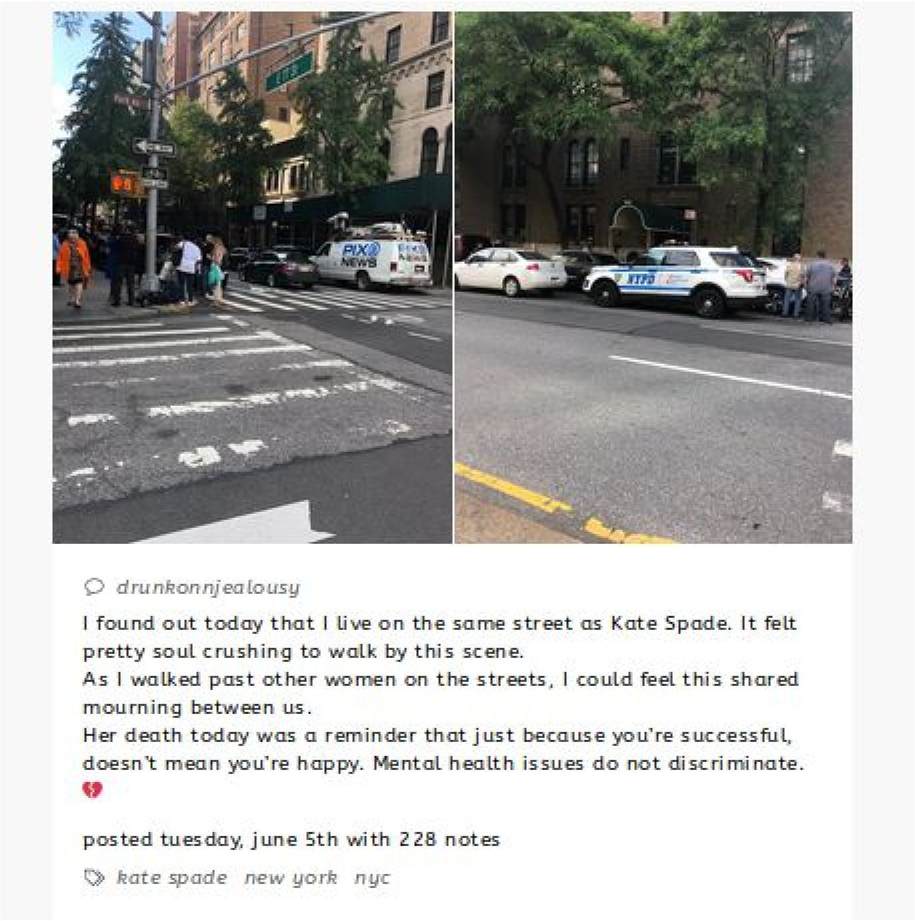
What is the real reason you started lifting?

My mom was a single guardian of 3 kids. I have a different dad than my 2 siblings. Their dad didn't pay

The archive is usually the first place I start to investigate a target. Many themes will have a link to the user's archive, however if that is hidden you simply need to add "/archive" to the end of their Tumblr account (ie user.tumblr.com/archive). The archive will show you all of a user's posts, whether it contains media, is a reblog, or is text only. For particularly large blogs there is a search function on the top left of the page that facilitates a more targeted search either by a timeframe or commonly used tags. Be sure to scan for common themes before drilling down into individual posts.

A user's archive is a great way to quickly get a read on the user and pull out quick information. As a habit I always do a screenshot of the user's entire archive just in case something happens to be removed or go down while I'm digging deeper into the user. In the archive above it only took a few seconds of scrolling to see numerous posts of the user shoplifting. I was able to see how often she shoplifted and the recurring types of items she seemed to target the most.

Posts: Text



drunkonnjealousy

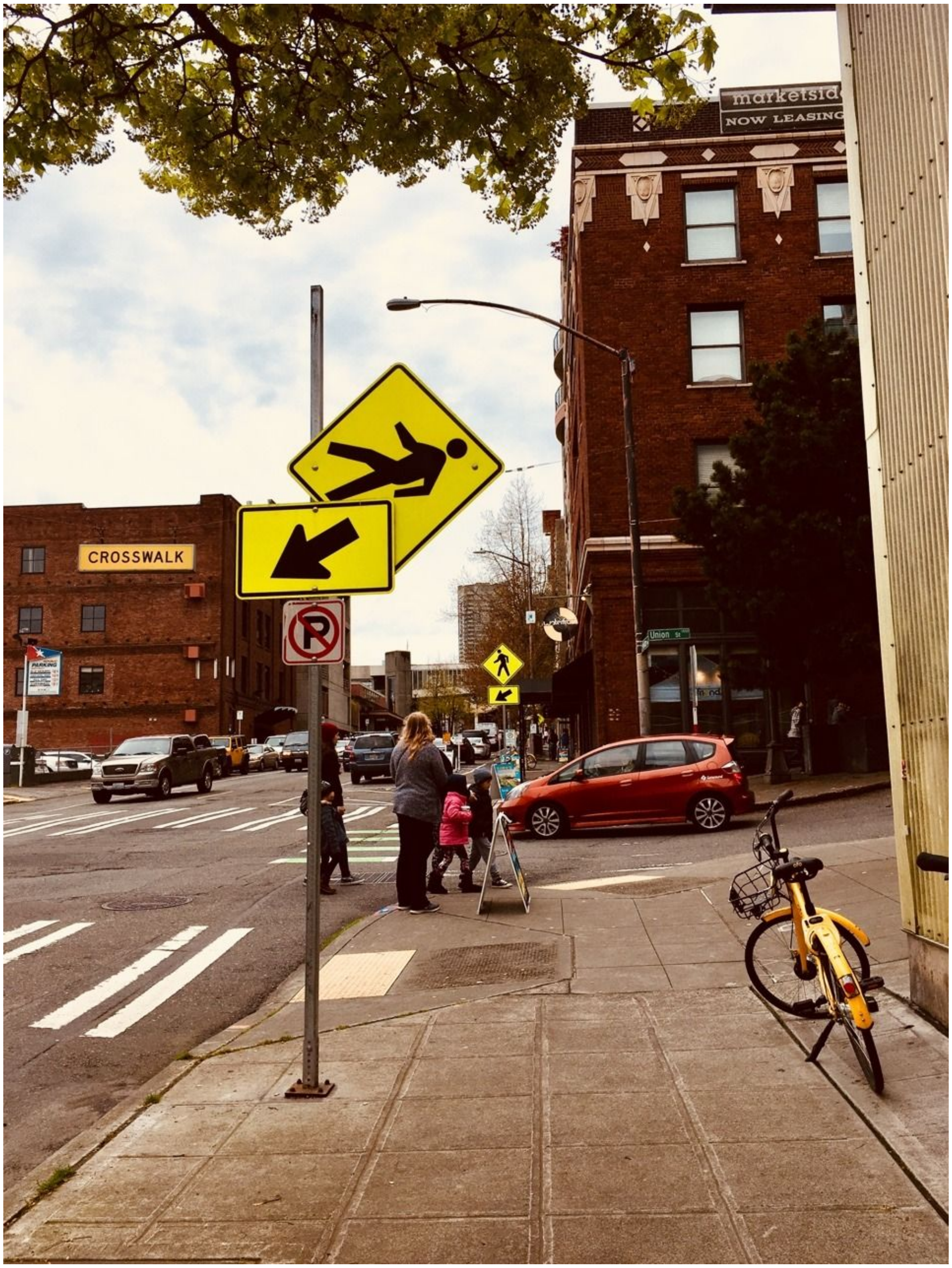
I found out today that I live on the same street as Kate Spade. It felt pretty soul crushing to walk by this scene.
As I walked past other women on the streets, I could feel this shared mourning between us.
Her death today was a reminder that just because you're successful, doesn't mean you're happy. Mental health issues do not discriminate.
💔

posted tuesday, june 5th with 228 notes

kate spade new york nyc

Every post made in the user's blog can contain different types of content, including text, photos, tags, as well as user interactions such as likes, reblogs, and comments. Each of these bits of data can provide additional information for identifying or locating the owner of the blog. Also be on the lookout for posts made by the target which include responses to anonymously asked questions. For text posts be sure to check for any real names, locations, recurring phrases or geographically-specific slang, etc. In the post above the user gives way more information about where they live then they probably intended. By identifying the city, street, and by posting this photo possibly even the block, the user provided information that would be very beneficial to helping identify or locate the account owner.

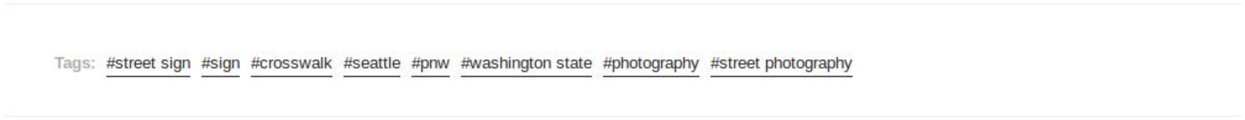
Posts: Photos and Videos



Photos and videos that are posted, whether with text or on their own, are investigated much in the same way as the user’s profile photo was above. You will want to run the image through reverse image searches and look for anything unique within the photos that may help steer the investigation. I like to think of videos as multiple photos compiled together and treat them as such. You will want to watch videos multiple times and pause and stop to note or screenshot pertinent parts. Also be sure to look out for image and video posts that have been reblogged by the user, meaning that they are not the source or original owner of the post.

Using the above photo (The full size image can be found in this post) there are a number of points within the photo worth noting. The biggest things to take notice of in analyzing this photo is the sign showing the cross street stating Union St, as well as the building with the Marketside Now Leasing sign on it. Another notable point is that the people outside are wearing winter gear, which may help in indicating the time of year or location of the photo. Some of the smaller things to point out are that the cars are being driven on the right side of the road, and that there is an Ofo dockless bike in the foreground. To locate where this photo was taken, I simply searched for a Marketside on Union Street in Google Maps and quickly found the same location here.

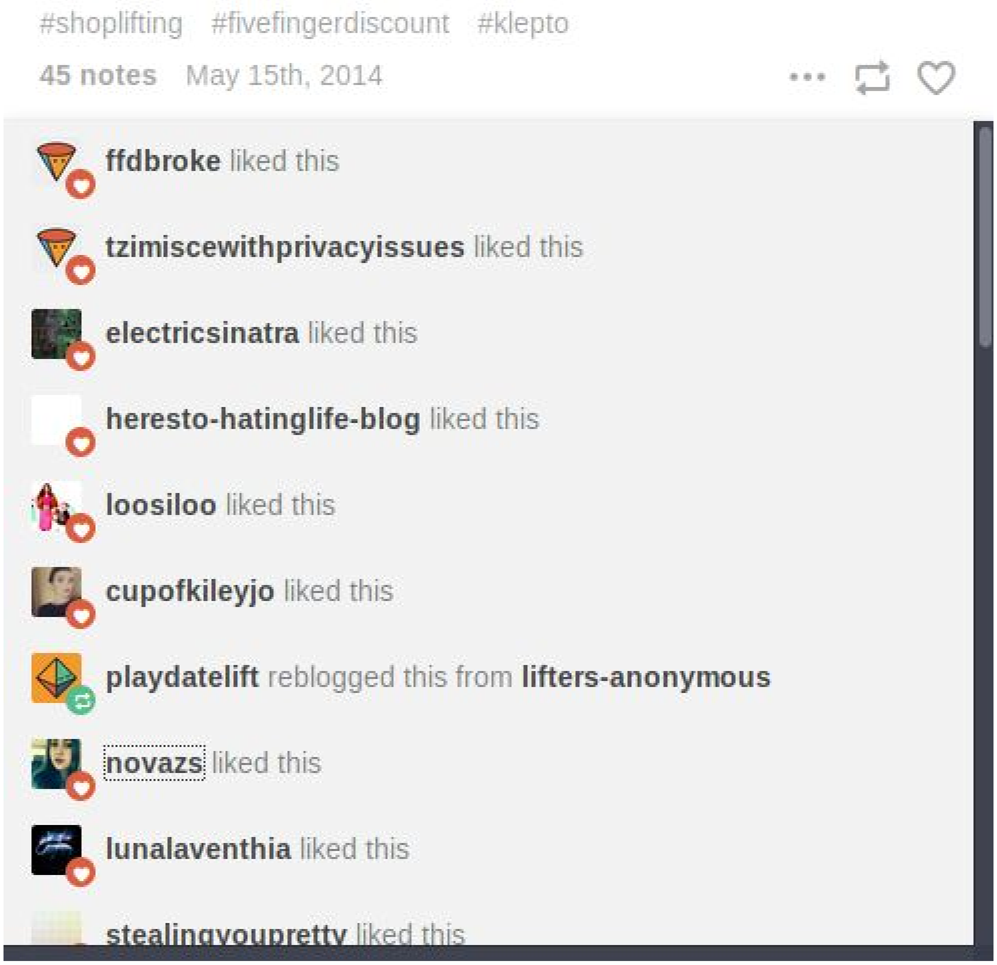
Posts: Tags



Tags: #street sign #sign #crosswalk #seattle #pnw #washington state #photography #street photography

Tags on Tumblr work very similarly to those on Twitter, Instagram, and other social media sites. Searches can be made using tags to find other posts with those same tags. This can be especially helpful when a target is using seemingly “unique” tags or uses the same type of tags to signify some linked persons, events, or locations. The above tags correspond to the earlier photo we analyzed. We now have confirmation based on the tags that the photo was indeed taken in an American city with a colder climate. Had I not initially been able to locate the right area previously, these tags would have enabled me to narrow my search down to the Seattle area.

Posts: User Interactions



#shoplifting #fivefingerdiscount #klepto

45 notes May 15th, 2014

ffdbroke liked this

tzimiscewithprivacyissues liked this

electricsinatra liked this

heresto-hatinglife-blog liked this

loosiloo liked this

cupofkileyjo liked this

playdatelift reblogged this from lifters-anonymous

novazs liked this

lunalaventhia liked this

stealingyoupretty liked this

Other users may interact with a target's posts in a number of ways such as liking, commenting on, or rebloging the post to their page. By looking at the totality of the post (photos, text, tags, etc) and the users interacting with the specific post it may assist in locating additional accounts to investigate that may be tied to the original target. Friends and followers often reblog and like one another's posts, and users that control multiple accounts may also interact with posts between them as a way to artificially build up their account's likes, reblogs, and followers. A great deal of the accounts that liked the above post, which was tagged with various shoplifting tags, are also shoplifting-related Tumblr accounts which post photos of their "hauls".

Conclusion

Hopefully this guide helps prepare you for your next Tumblr-based investigation. In order to assist with investigating Tumblr accounts I have created some handy OSINT tools and graphics to supplement this guide and help get new users started. You can find the Tumblr OSINT Attack

Vector Map to walk you through your first few investigations as well as all of the Tumblr-specific Javascript bookmarklet tools at my Github page here.