Pokémon GO OSINT Techniques: Part I

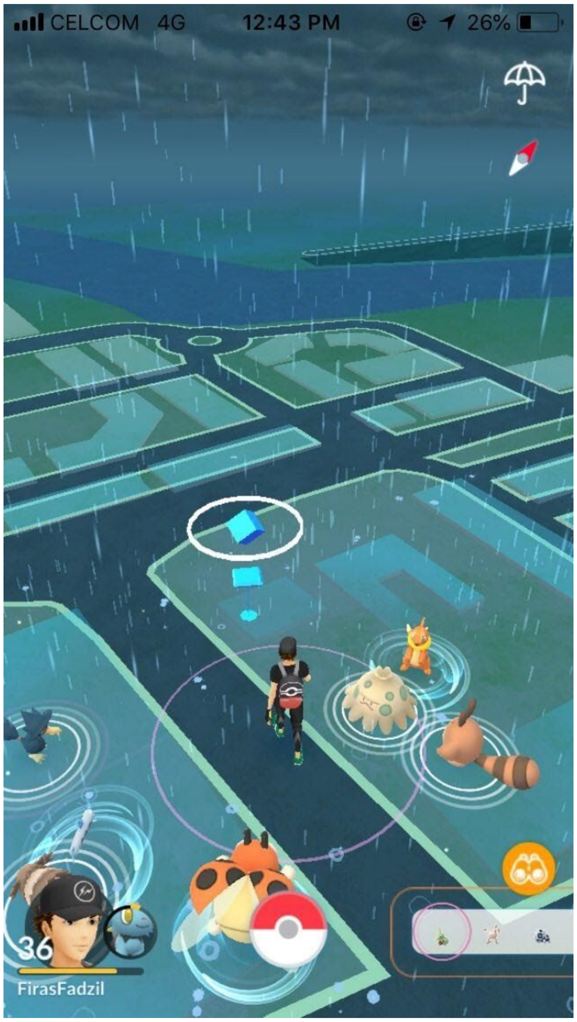
Released in July 2016, Pokémon GO quickly became one of the most popular games of all time with millions of users spread all over the world. As the game relies heavily upon user location for playing there is a wealth of location-based information that the game utilizes to display specific points of interest on the over world map.

Investigators may exploit such publicly obtainable information from a user’s screenshots on social media or by adding them as a friend in the game in order to gather additional intelligence. This OSINT guide will be split up into two sections. This first section will focus solely on exploiting the different types of screenshots that Pokémon GO players commonly post to social media. The second portion of the guide will focus on ways to exploit information from accounts that users have befriended in-game.

Part I: Exploiting Screenshots

The most likely way of obtaining information on a Pokémon GO user would come from their in-game screenshots uploaded to another social media platform. Users are not shy about uploading their screenshots to show off their rare Pokémon, recently visited Gyms, or the map of a new area they visited while on vacation. Although users can take a screenshot of any in-game action I will only be covering common screenshots which may provide information useable in an investigation.

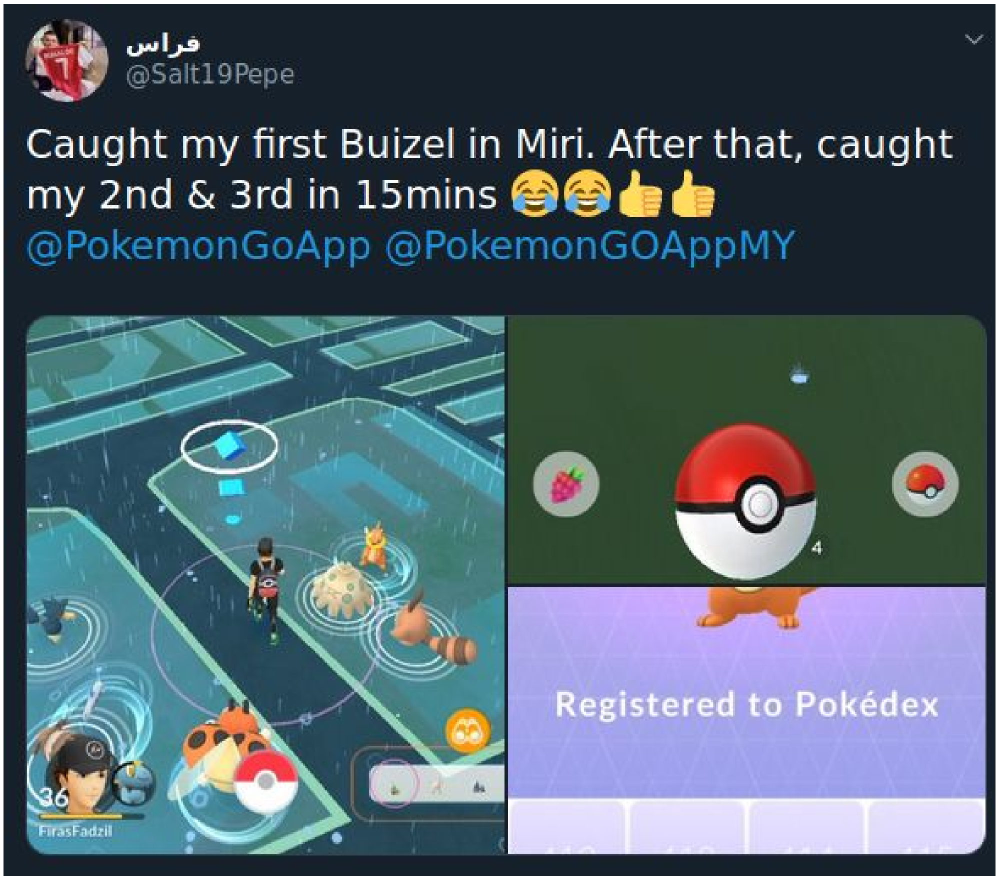
Overworld Map



Much of the game mechanics revolve around the overworld map in which the player's avatar walks on a map rendered to replicate the real-world locations that the user is in. The overworld map may also display the player's username in the lower-left corner, however we are going to cover that later on in the second section of this guide. Instead, we are going to analyze the map itself to narrow down a user's location at the time of the screenshot.

As Pokémon GO utilizes OpenStreetMaps (OSM), this should be your main mapping reference as the routes, buildings, and other mapped information should be near identical between the two. When trying to compare the game's overworld map to real life it is imperative that you have additional information to help narrow down your area. Using just the overworld map itself without anything else will make it near impossible to locate the specific area. Instead, I highly recommend looking at neighboring posts by the user to see if they mention a city or post photos of nearby Pokéstops or Pokémon gyms.

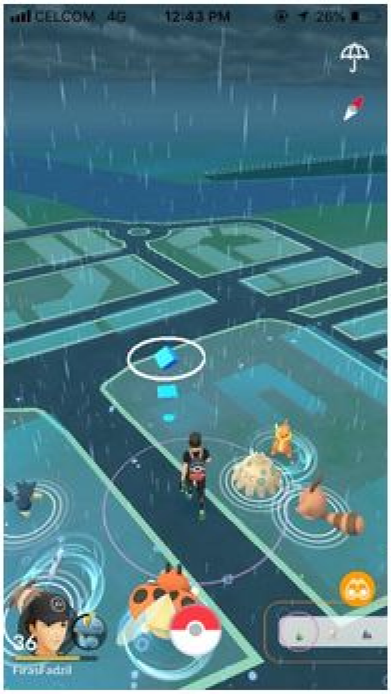
In our above example, we can see that the user posted a screenshot of their game while on the overworld map. The tweet in which they included the above screenshot mentioned being “in Miri”.

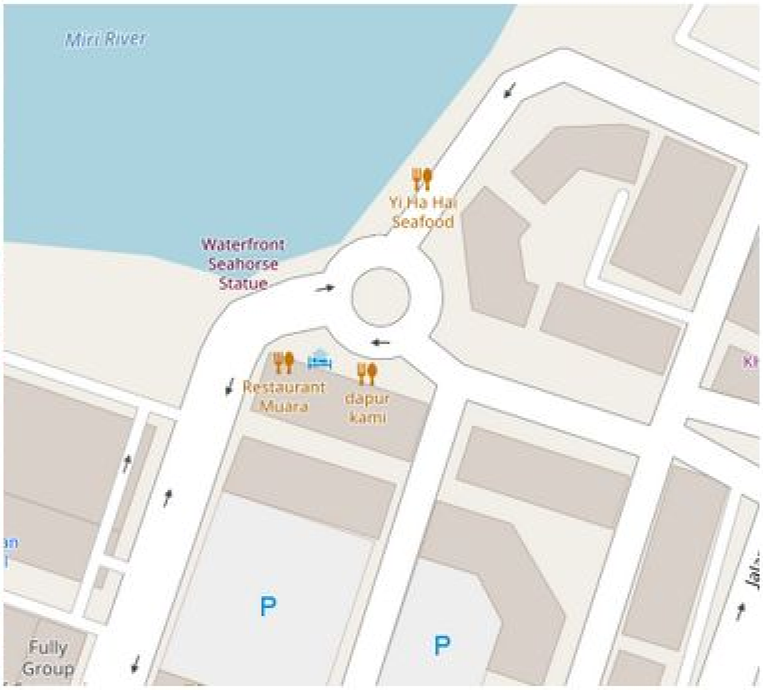


فراس
@Salt19Pepe

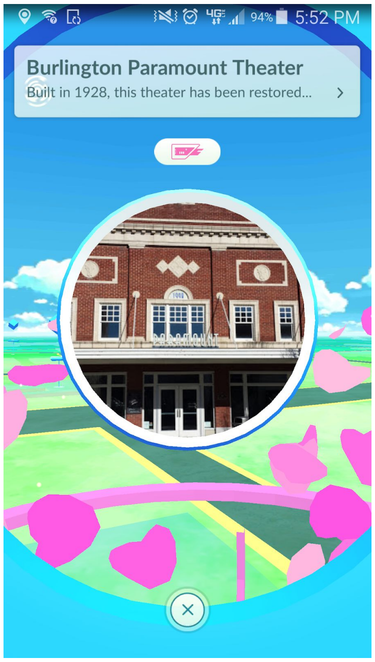
Caught my first Buizel in Miri. After that, caught my 2nd & 3rd in 15mins 😂😂👍👍 @PokemonGoApp @PokemonGOAppMY

After a bit of Google Dorking I was able to determine that "Miri" was likely Miri, Malaysia. I then navigated to Miri, Malaysia in OSM and began looking for jumping-off points within the user's screenshot. Following the river in Miri I scanned for a roundabout nearby and was able to quickly locate the area on OSM here. Below are the two maps side by side for comparison. Note that the uniquely shaped buildings appear identical in both maps, this is the major reason for suggesting OSM over any other mapping service when cross-referencing Pokémon GO maps.





Pokéstops



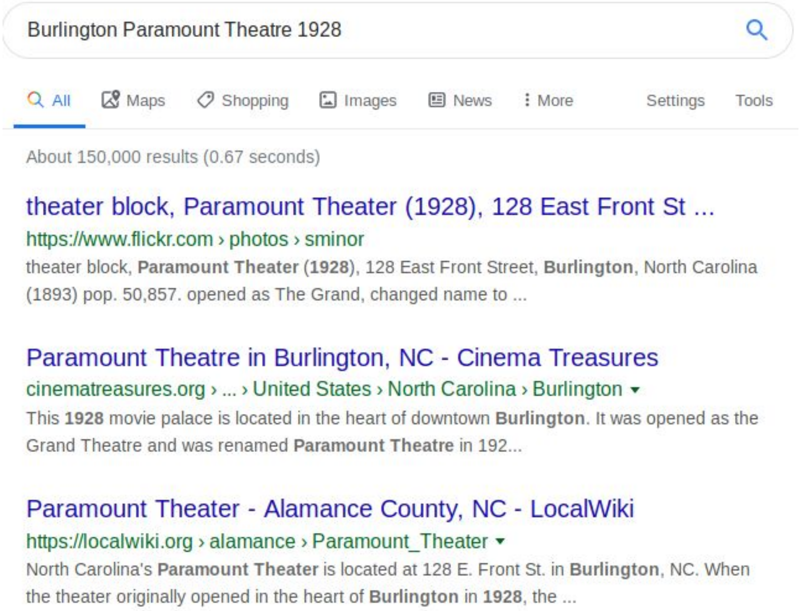
Burlington Paramount Theater

Built in 1928, this theater has been restored...

Pokéstops are the floating blue cube or Pokéball-like icons (sometimes with white rings around them to indicate the user has never visited them before) that are scattered across the overworld map. These stops can be “spun” by players in order to obtain items or gifts to send to other players. Pokéstops correspond to real-world points of interest such as signs, monuments, etc, with new ones added or updated by users on a regular basis. On the otherworld map Pokéstops may help narrow down a user’s location if there is a unique spread of them that can be cross-referenced to one of the online Pokéstop maps such as Pokélytics or Pokémap. If a user selects an individual Pokéstop, a new screen will open that stops a photo of the Pokéstop location as well as the name and a short description, both provided by other players.

Our above example shows what a Pokéstop looks like when a user clicks on it. This screenshot gives us a cropped photo of the building, as well as the name of the building (Burlington Paramount Theatre”, and the description includes the year the building was constructed (1928).

Doing a general search of “Burlington Paramount Theatre 1928” gives multiple results for a theatre in North Carolina.



Burlington Paramount Theatre 1928

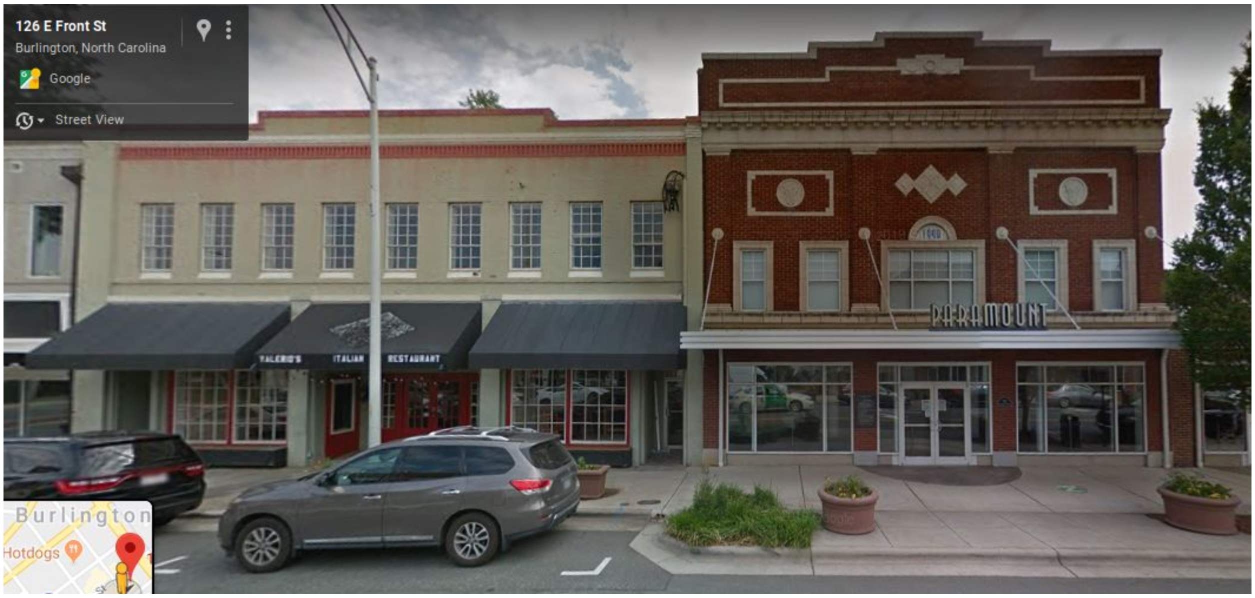
About 150,000 results (0.67 seconds)

theater block, Paramount Theater (1928), 128 East Front St ...
https://www.flickr.com › photos › sminor
theater block, **Paramount Theater** (**1928**), 128 East Front Street, **Burlington**, North Carolina (1893) pop. 50,857. opened as The Grand, changed name to ...

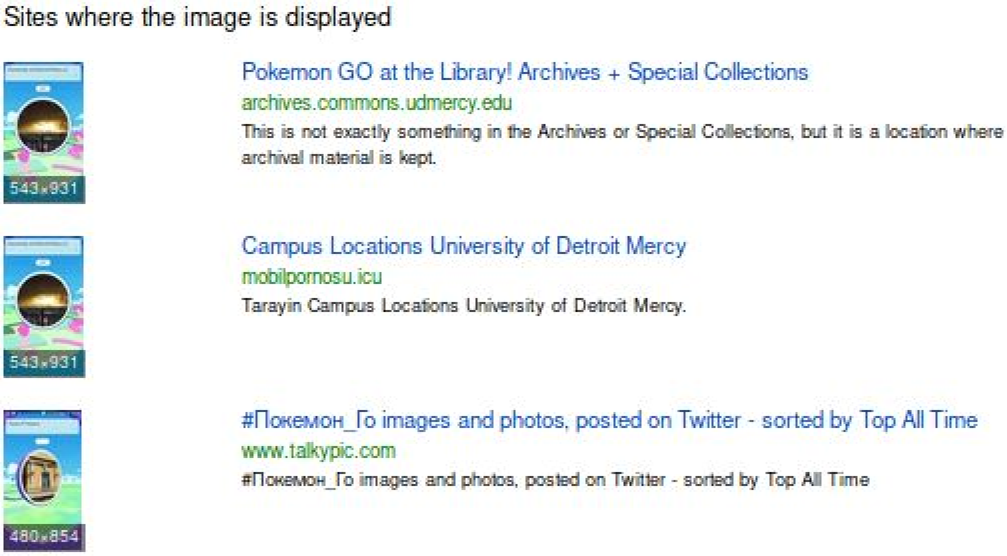
Paramount Theatre in Burlington, NC - Cinema Treasures
cinematreasures.org › ... › United States › North Carolina › Burlington
This **1928** movie palace is located in the heart of downtown **Burlington**. It was opened as the Grand Theatre and was renamed **Paramount Theatre** in 192...

Paramount Theater - Alamance County, NC - LocalWiki
https://localwiki.org › alamance › Paramount_Theater
North Carolina's **Paramount Theater** is located at 128 E. Front St. in **Burlington**, NC. When the theater originally opened in the heart of **Burlington** in **1928**, the ...

Pulling the address from the first result (128 East Front Street, Burlington, North Carolina) and throwing it into street view from Google Maps (at 36.0934714,-79.4364187) shows us the same building front as the photo.



As the location title and description are user-generated it is not always enough to find the point of interest in the real world. In such instances another route we can try is to do a reverse image search on our above Pokéstop example. Doing a normal search for it on Google and Yandex returned only results of other Pokéstop images.


Sites where the image is displayed

543×931

Pokemon GO at the Library! Archives + Special Collections
archives.commons.udmercy.edu
This is not exactly something in the Archives or Special Collections, but it is a location where archival material is kept.

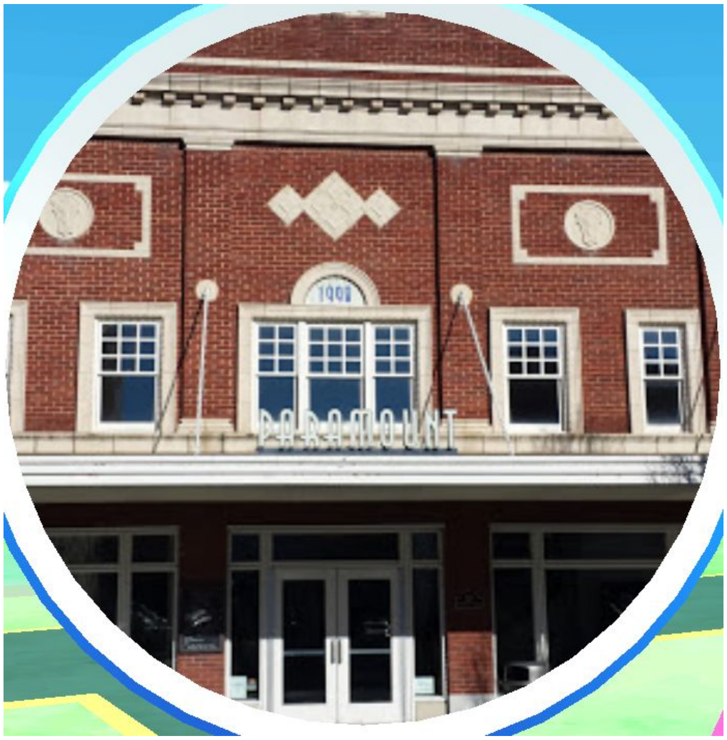
543×931

Campus Locations University of Detroit Mercy
mobilpornosu.icu
Tarayin Campus Locations University of Detroit Mercy.

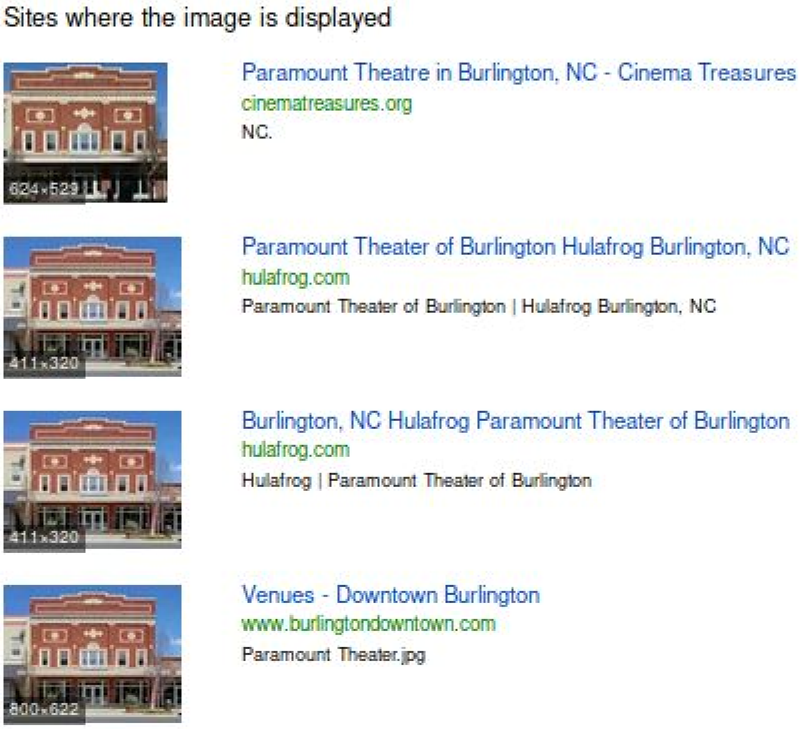
480×854

#Покемон_Го images and photos, posted on Twitter - sorted by Top All Time
www.talkypic.com
#Покемон_Го images and photos, posted on Twitter - sorted by Top All Time

Rather than running a reverse image search on the full photo we will crop it down to just the image containing the building we want to locate.



Running our cropped image through Yandex provides us with much better results this time around and confirms that it is indeed the same as the one we found in North Carolina previously.



Sites where the image is displayed

624×529

Paramount Theatre in Burlington, NC - Cinema Treasures
cinematreasures.org
NC.

411×320

Paramount Theater of Burlington Hulafrog Burlington, NC
hulafrog.com
Paramount Theater of Burlington | Hulafrog Burlington, NC

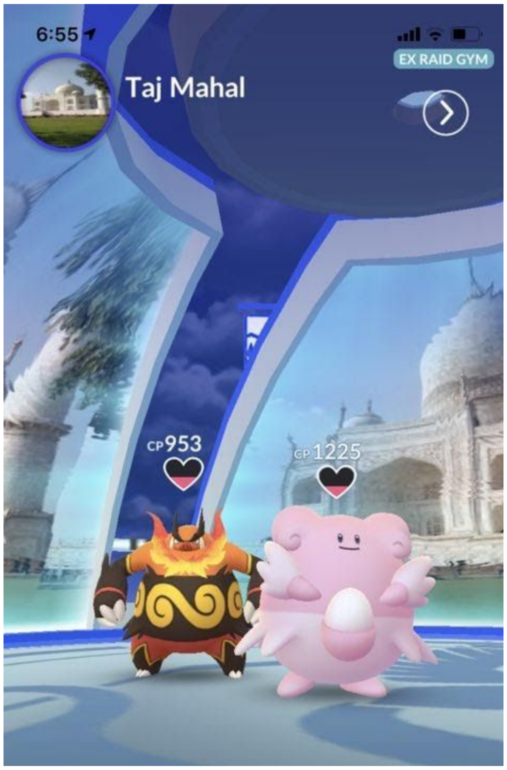
411×320

Burlington, NC Hulafrog Paramount Theater of Burlington
hulafrog.com
Hulafrog | Paramount Theater of Burlington

800×622

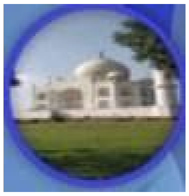
Venues - Downtown Burlington
www.burlingtondowntown.com
Paramount Theater.jpg

Pokémon Gyms

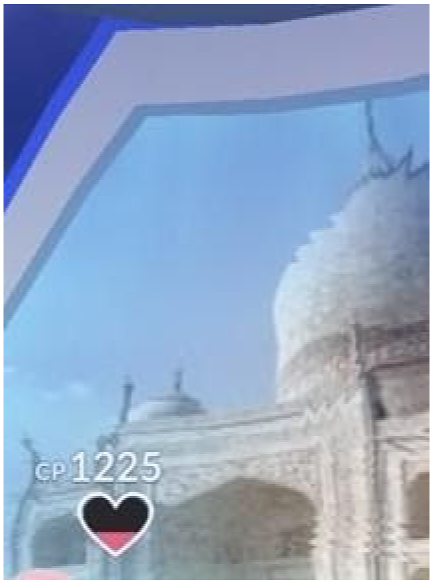


Like Pokéstops, Pokémon Gyms also appear on the overworld map, however they display as larger icons and may be blue, red, yellow, or gray to denote the color of the team (or lack thereof) that currently controls it. Users may battle other players in the gym or leave their own Pokémon in the gym to defend it. When selected, the gyms will display the Pokémon in the gym as well as the gym name and an image of the gym point of interest both in the mini photosphere in the top left as well as on the background of the gym. Some gyms may also show that they are sponsored or ex-raid eligible on the upper right side.

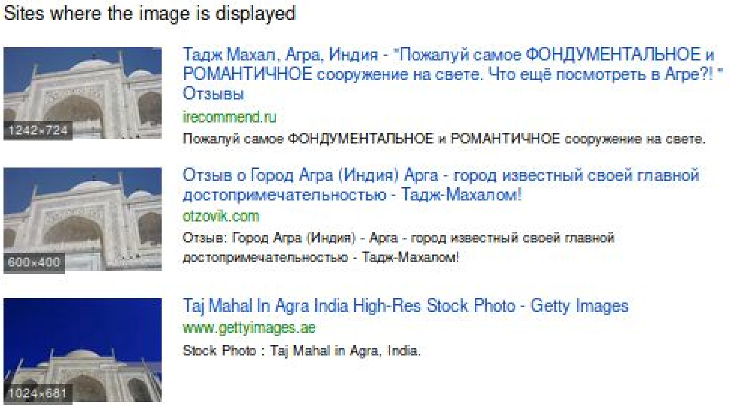
For the most part, investigating a Pokémon gym location will be identical in technique as a Pokéstop with the name of the point of interest and the photos of the gym being used to narrow down a location. For our above example I am going to assume everyone can find the Taj Mahal by Google Dorking so I will not bore you with the steps to find it via the name alone. Instead, let's take a look at doing a reverse image search. We already know from Pokéstops that uploading the full image likely will not work. Skipping that we can move to the cropped small image of the gym as our first try.



Google came back negative and Yandex provided results of a similar building in Indonesia, but not what we are looking for. This is likely due to the size and overall quality of the image. Next, we will crop out the larger image from the background of the gym.



This is not ideal for a reverse image search, with such a small image and the Pokémon health bar overlapping our photograph, but still worth a try especially for more notable landmarks. Google once again let us down, though it at least identified the image as being a tourist landmark, while Yandex came through with matching results.



Sites where the image is displayed

1242×724

Тадж Махал, Агра, Индия - "Пожалуй самое ФОНДУМЕНТАЛЬНОЕ и РОМАНТИЧНОЕ сооружение на свете. Что ещё посмотреть в Агре?! " Отзывы

irecommend.ru

Пожалуй самое ФОНДУМЕНТАЛЬНОЕ и РОМАНТИЧНОЕ сооружение на свете.

600×400

Отзыв о Город Агра (Индия) Арга - город известный своей главной достопримечательностью - Тадж-Махалом!

otzovik.com

Отзыв: Город Агра (Индия) - Арга - город известный своей главной достопримечательностью - Тадж-Махалом!

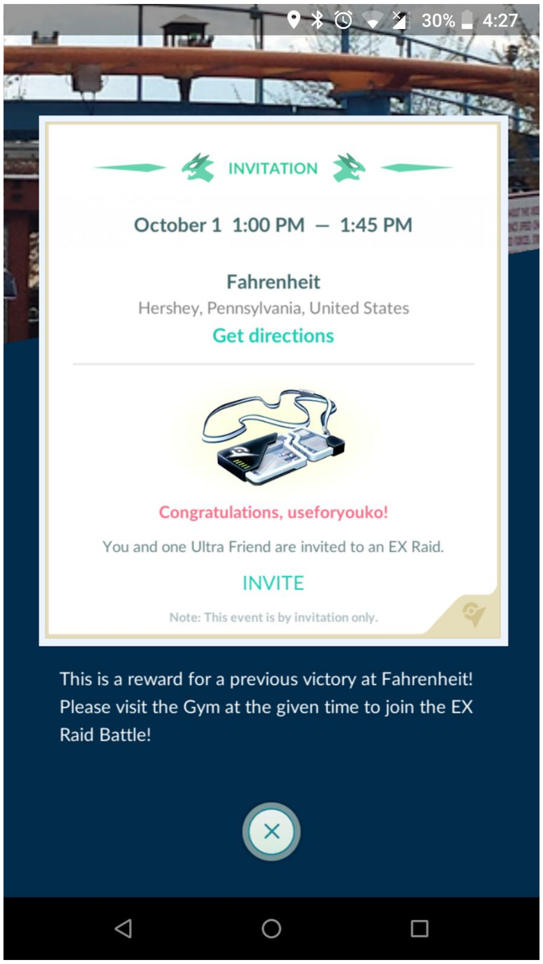
1024×681

Taj Mahal In Agra India High-Res Stock Photo - Getty Images

www.gettyimages.ae

Stock Photo : Taj Mahal in Agra, India.

EX-Raid Passes



INVITATION

October 1 1:00 PM — 1:45 PM

Fahrenheit

Hershey, Pennsylvania, United States

Get directions

Congratulations, useforyouko!

You and one Ultra Friend are invited to an EX Raid.

INVITE

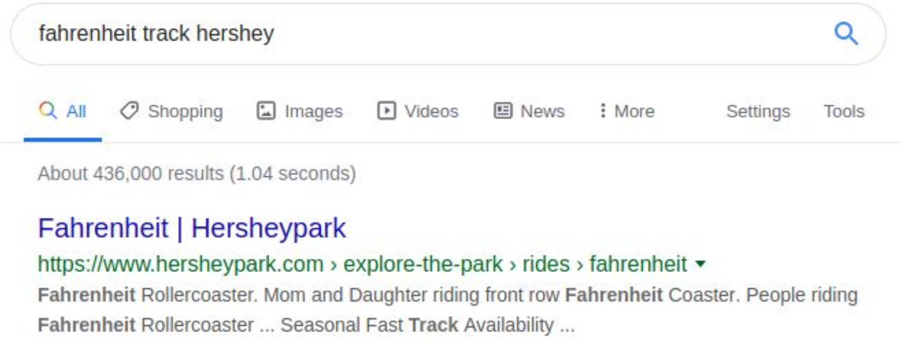
Note: This event is by invitation only.

This is a reward for a previous victory at Fahrenheit! Please visit the Gym at the given time to join the EX Raid Battle!

Players that win a battle against a computer Pokémon at eligible Gyms may also be rewarded with an EX-Raid Pass. These passes allow a player to return to that same gym at a predetermined time and fight a rarer and more powerful Pokémon together with other players. Screenshots of a user's EX-Raid Pass provides a lot of valuable information such as partial photo of the gym the EX-Raid will be at, the date and time of the EX-Raid, the name of the EX-Raid gym, the city and country of the gym (not always), and finally the username of the player which received the EX-Raid Pass. The best part about users that screenshot their Ex-Raid passes is that you now know the time and place that they will likely return to the area for the EX-Raid. This makes it easier to narrow down the potential pool of subjects if you are able to surveil the same location during the Ex-Raid window.

Reverse image search results for the above example came back negative, even with the photo cropped down. This comes as no surprise as there is almost no useable information to match in the sliver of the remaining image. Using the location information along with the gym name and what we can make out of the photo, which appears to be a track of some sort, appears to be a better avenue.

Google Dorking with "fahrenheit track hershey" returned results that suggest a rollercoaster named Fahrenheit in Hershey Park.

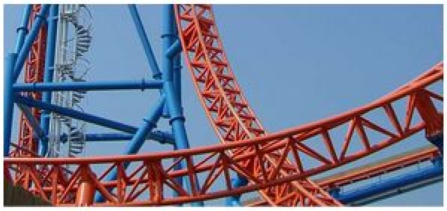


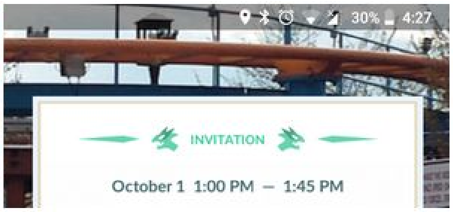
fahrenheit track hershey

About 436,000 results (1.04 seconds)

Fahrenheit | Hersheypark
https://www.hersheypark.com › explore-the-park › rides › fahrenheit
Fahrenheit Rollercoaster. Mom and Daughter riding front row **Fahrenheit** Coaster. People riding **Fahrenheit** Rollercoaster ... Seasonal Fast **Track** Availability ...

Looking at photos of the rollercoaster, the color-scheme and connection between the red and blue track pieces confirms this as a match to the location seen in the photo behind the EX-Raid invite.

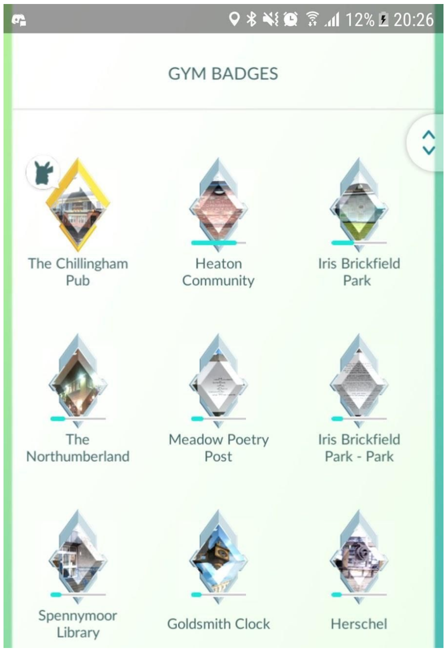




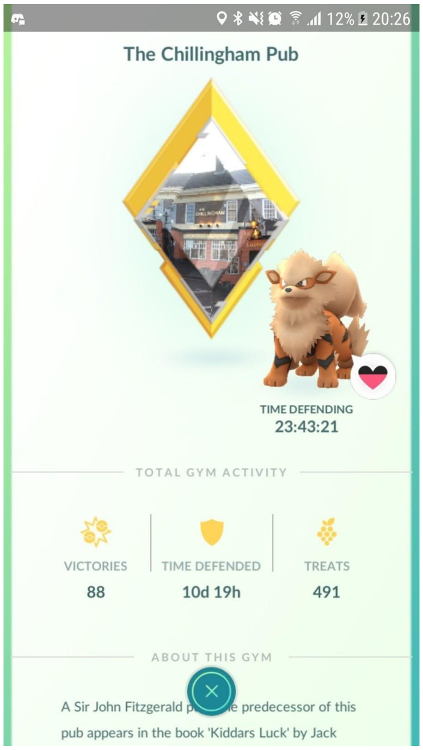
INVITATION

October 1 1:00 PM — 1:45 PM

Gym Badges



The more a player interacts with a gym the more points they get for it. These points correspond to different badge levels (bronze, silver, gold). There are two different types of screenshots corresponding to Gym badges. The overall screenshot (such as in the above example) showcases gym badges in order of most recently visited by the user. This view will display the most recently visited gyms, their badge level and points bar, as well as the gym names. They may also contain an icon indicating the user currently has a Pokémon defending the gym, or if they have an upcoming EX-Raid in one of the gyms. Clicking on any one of these specific gym badges will display a more detailed version of that badges such as the one below. This view will show a larger photo of the gym, the gym name, the user’s total activity at that specific gym, as well as the individual Pokémon defending it if applicable.



The Chillingham Pub

TIME DEFENDING
23:43:21

TOTAL GYM ACTIVITY

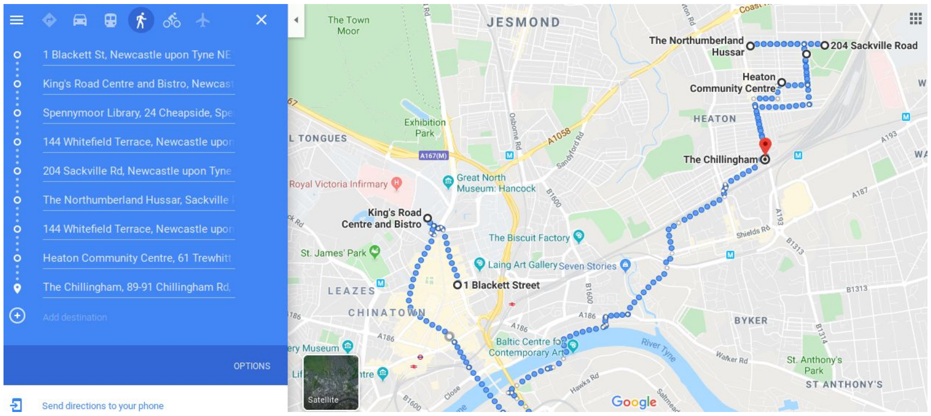
VICTORIES 88 | TIME DEFENDED 10d 19h | TREATS 491

ABOUT THIS GYM

A Sir John Fitzgerald p... e predecessor of this pub appears in the book 'Kiddars Luck' by Jack

Knowing the recently visited and most interacted with gyms of a player is valuable information for reading pattern of life. Unless the user is spoofing their location, gym badges could show the route recently or commonly taken by the player in their everyday routines. In our above example, we can see that the most interacted with gym (based on it being the only gold level one) is a pub. The user might work at this pub, visit it often, live near it, or pass it regularly on their way to work and/or school. The first step to mapping this out would be to locate the pub on OSM and cross-reference it on Pokélytics or another Pokéstop map of your choice if needed to confirm the photo images match on the gym badges as on the Pokélytics map (be aware that not all are there). Also keep in mind that this will not be an exact science as these gym names can be added, deleted, or changed over time. Using these two resources I set out to individually locate and map out as many of the 9 most recently visited gyms visited as I could find.

After mapping them out it became apparent that although the user has interacted with the Spennymoor Library enough to reach silver level, it was an outlier compared to their other commonly and recently visited gyms which were all around the same area. Additionally, based on the location of one of the gyms, which was on a University campus, this may be the user's route to an from school. Below is an ordered walking route mapped on Google (with Spennymoor Library cut off at the bottom).



1 Blackett St, Newcastle upon Tyne NE

King's Road Centre and Bistro, Newcast

Spennymoor Library, 24 Cheapside, Spe

144 Whitefield Terrace, Newcastle upor

204 Sackville Rd, Newcastle upon Tyne

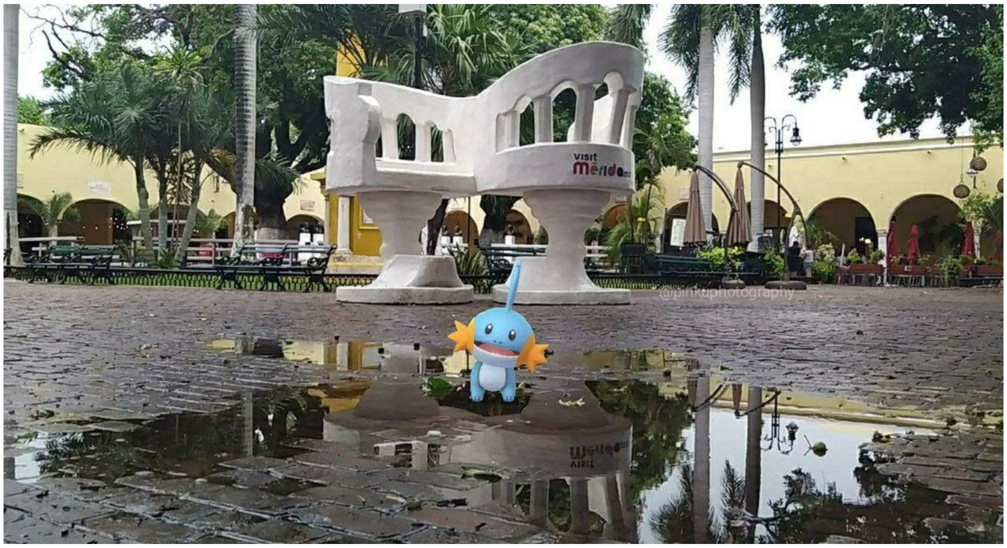
The Northumberland Hussar, Sackville

144 Whitefield Terrace, Newcastle upor

Heaton Community Centre, 61 Trewhitt

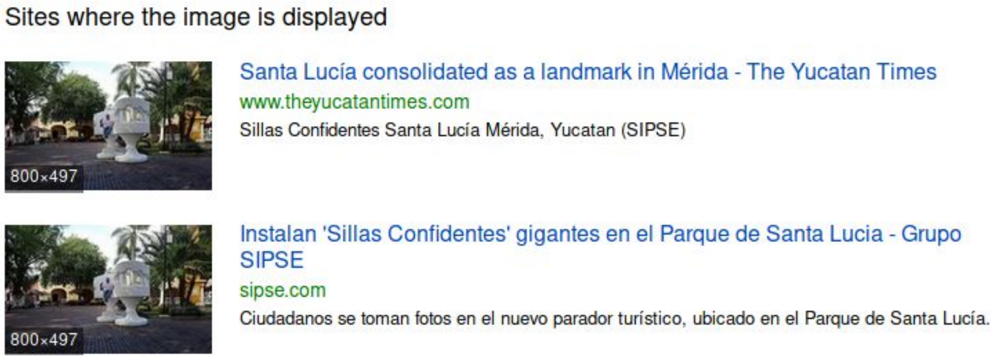
The Chillingham, 89-91 Chillingham Rd,

Pokémon Snapshots



These are not technically screenshots but are instead photographs enhanced with augmented reality that allows players to take a photo of their real-world surroundings with any of their caught Pokémon. As with any other photo, standard OSINT practices apply such as looking for contextual clues within the image and running it through a reverse image search. It is worth pointing out here that in most cases the Pokémon overlay will not hinder the use of a Yandex reverse image search, though Google can be hit on miss depending on how much of the image is covered by the Pokémon.

Our above example depicts two chairs with the text “Visit Merida” on one of them. Top search engine results for “Visit Merida” all point back to a Merida in Yucatan, Mexico. At first glance this area appears to be a match based on the architecture in the background of our snapshot. A reverse image search using Google found no matching photos while Yandex pulled matching images confirming our initial results.



Sites where the image is displayed

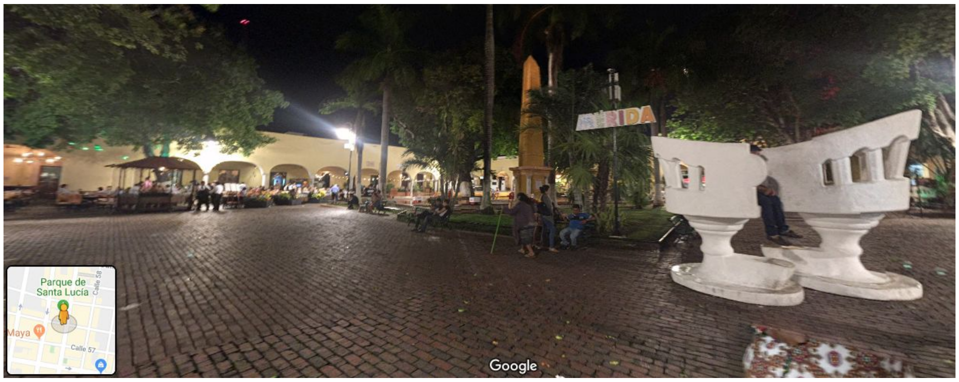
800×497

Santa Lucía consolidated as a landmark in Mérida - The Yucatan Times
www.theyucatantimes.com
Sillas Confidentes Santa Lucía Mérida, Yucatan (SIPSE)

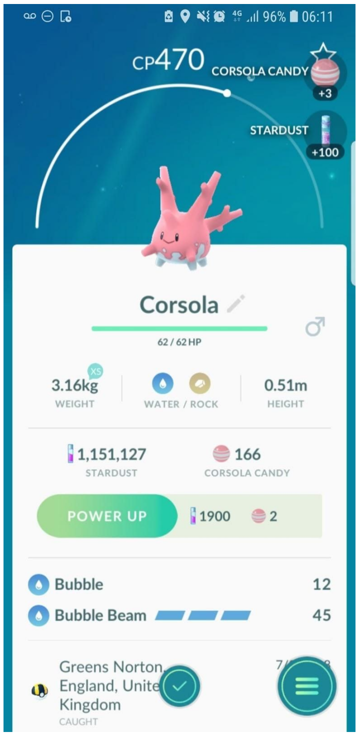
800×497

Instalan 'Sillas Confidentes' gigantes en el Parque de Santa Lucia - Grupo SIPSE
sipse.com
Ciudadanos se toman fotos en el nuevo parador turístico, ubicado en el Parque de Santa Lucía.

Additional searching in Merida for a Santa Lucia Park gives us the final location (20.9710505,-89.6225523) of where the snapshot was taken.



Caught Pokémon



96% 06:11

CP470

CORSOLA CANDY +3

STARDUST +100

Corsola

62 / 62 HP

3.16kg WEIGHT

WATER / ROCK

0.51m HEIGHT

1,151,127 STARDUST

166 CORSOLA CANDY

POWER UP 1900 2

Bubble 12

Bubble Beam 45

Greens Norton, England, Unite Kingdom

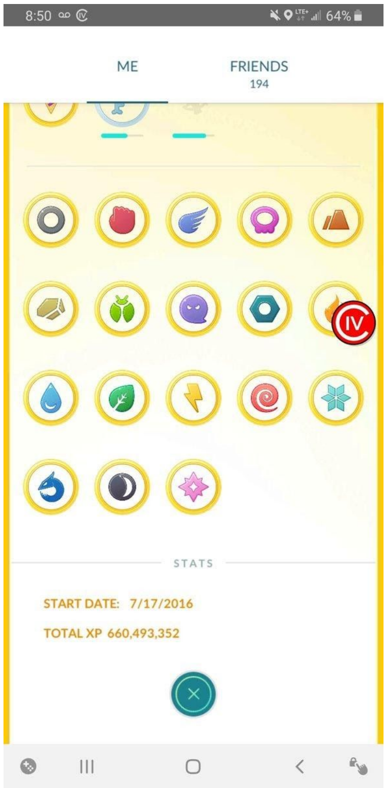
CAUGHT

7/

It is not uncommon for users to screenshot and share recently caught Pokémon, especially when they find one that is newly released, regional, or otherwise rare. Information that may be found on Pokémon screenshots includes the Pokémon name (by default) or nickname (if the user changed the default name), the general area in which it was captured, and the date on which it was captured. Different types of Pokémon spawn in different real-world environments. Additionally, some Pokémon are only found at certain times of the year during events, or in very specific parts of the world (aka “regionals”). As this can affect the usual spawning locations it is always a good idea to cross-reference any dates to check for any events that might have occurred at those times. Such screenshots may allow investigators to place a user in a certain area on a certain date. Some might also contain additional information, such as showing that the monster was received by trade from another user rather than captured on their own.

Our above example shows a screenshot of a Corsola caught in the United Kingdom sometime during July 2018. We can reference a list of regionals here and here to see that Corsola tends to have a limited area to regions close to the equator. Had the user not posted the bottom portion of the photo showing the caught location and caught date we might make a possible guess on the location in which they caught the Pokémon based on their usual spawn location. However, looking at the caught location we can see that it was in fact encountered in the United Kingdom, far away from the usual spawn points. Referencing this list of events and doing some Google Dorking I looked for events that occurred in July 2018 (what could be seen in the screenshot) and discovered that Corsola was available in the United Kingdom for a limited time per this article. Combining everything together we can now say the user which posted the screenshot above was in Greens Norton, England, UK on either July 3 or July 4, 2018.

Stats



START DATE: 7/17/2016

TOTAL XP 660,493,352

Users that screenshot their profile may also include their stats section which shows when their account was created as well as their total amount of XP (experience points). This section provides some pattern of life information and helps an investigator determine how long the account has been open as well as how active the user is.

In our above example we can see that the user created their account on the 17th of July. This tells us the user has an older account, as the game first came out in July 6, 2016. This join date might also assist in narrowing down the user’s country or region if it corresponds with the “day one” release date for a particular area. The user may have been a few days late to the party if they were in the United States, however it is also possible that they are a day-one player from Canada, which had their initial release on July 17, 2016. For a reference of release dates by country, see here. (For those wondering, the player is indeed a day one player out of Canada as confirmed by his Twitter)

Next, looking at the overall amount of XP tells us that this user is a very hardcore player as it takes 20 million XP to reach the current max level of an account (level 40). This user has played enough to theoretically level up several accounts to that level already. You can find a chart mapping XP to trainer level here.

Part I Conclusion

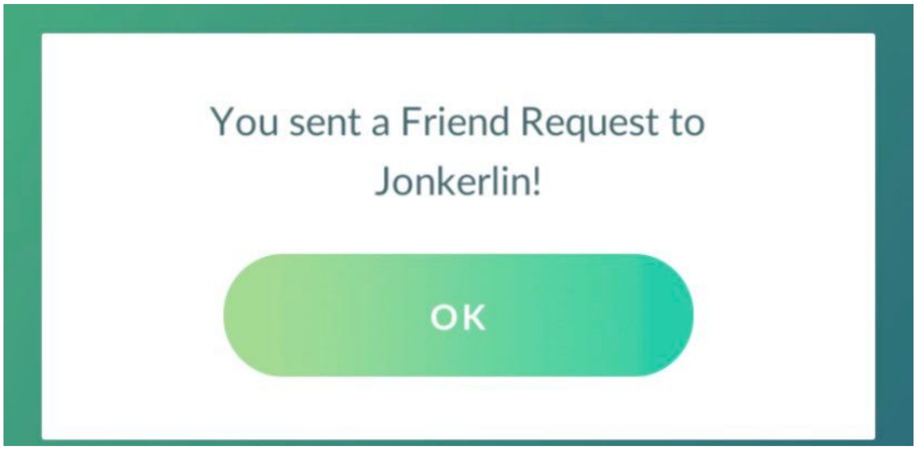
Now that you’ve learned how to extract a great deal of information from any number of Pokémon GO screenshots, I hope that you can put these skills to use during your next OSINT investigation. Keep in mind that for the most part these methods of investigation are not limited to Pokémon GO and can be applied to nearly any investigation in which an image or screenshot is available. Be sure to keep an eye out for the next portion of this guide which will focus on how to exploit information from Pokémon GO accounts that you have befriended in-game. As always, should you have any questions please feel free to reach out to me on Twitter.

Pokémon GO OSINT Techniques: Part II

Pokémon Go is a very social game and regular interaction with other users is the fastest and most effective way of increasing your trainer level and catching ‘em all. User interaction can provide a host of benefits, including addition experience points (XP), the ability to find rare Pokémon outside your local area, receive invites to EX-Raids and intelligence that can only be gathered in game from 'friends'.

While Part I focused solely on screenshots, Part II will concentrate more on intelligence that can be gathered in-game from users that an investigator has befriended. There will be references to techniques and tools used in Part I, as well as some additional discussion of screenshots where applicable. If you haven’t already read through Part 1 I highly recommend that you do, check it out here.

Adding Friends

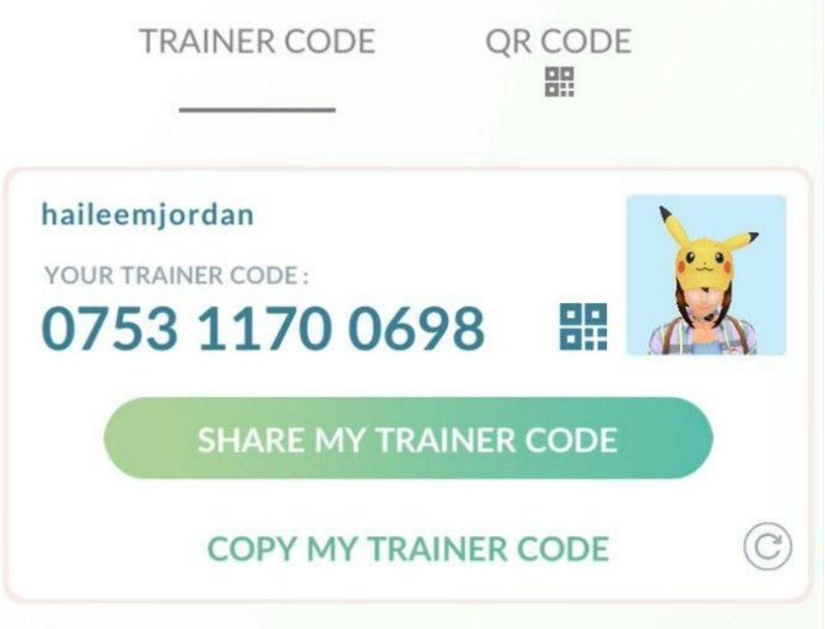


You sent a Friend Request to Jonkerlin!

In order to interact with and view live information on a Pokémon Go trainer you must first send them a friend request in-game. This can be done by either scanning a QR code provided by the user or by manually entering their 12-digit friend code into the app. After the friend request is sent, the username of the trainer you sent the request to will appear on the screen. Be sure to screenshot this as it will allow you to begin exploiting the username without having to wait on the user to accept your request.

Once done, the user will have to accept it on the other side to complete the process. Although both friend and QR codes work in the same manner, the way in which they can be exploited differ. As an investigator may have access to only one or the other, it is important to see how to circle from one of the forms to the next to ensure that all avenues are explored.

Friend Codes



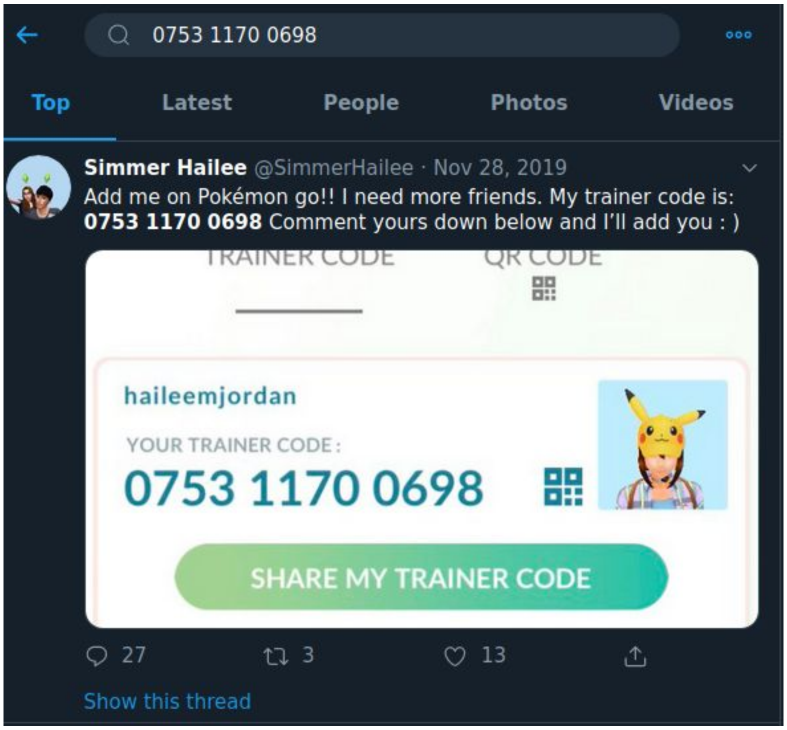
haileemjordan

YOUR TRAINER CODE:
0753 1170 0698

Adding a user via their friend code appears to be the most common way, as users seem to share their numerical code (either in plain text or via a screenshot) more often than their QR code. This might be due to a number of factors, including whether people are less trusting of scanning what could be a rogue QR code disguised as a friend code, or simply the fact that when retrieving your friend code in the user profile the default option is the friend code rather than the QR code. In addition to using the friend code to befriend a user, an investigator can search across the internet and social media for accounts that might have shared their friend code for others to add.

There are too many numerical trainer code databases to cover here, and the great majority of them require you to have some sort of additional info to be of much use. For example, here and here are two sites that allow you to view trainer codes, and obtain the username, but both require you to know the country or general area that the target lives in. When searching on social media and across search engines, try to note what formats are being used. Overall, I've had far greater luck searching for codes using the #### #### #### format over the ############ one, though this might not be the case for all databases.

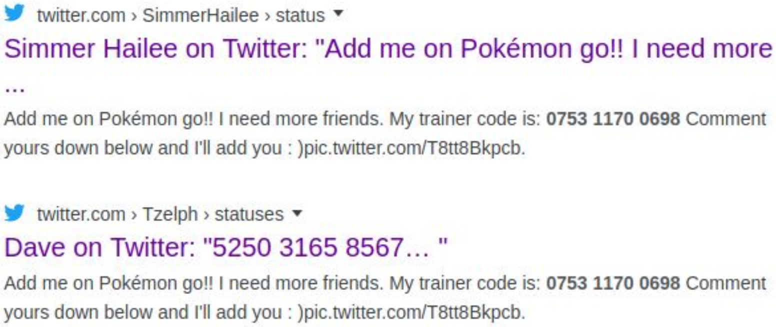
I created a quick bookmarklet tool to run the above example across Google (had little luck during testing with the other search engines), Twitter, and a subreddit for sharing Pokémon Go friend codes. These sites seemed the most consistent for finding matches. Results for Reddit were negative, however Twitter returned a post in which a Twitter user shared the trainer code in the text as well as the screenshot.



0753 1170 0698

Simmer Hailee @SimmerHailee · Nov 28, 2019
Add me on Pokémon go!! I need more friends. My trainer code is: **0753 1170 0698** Comment yours down below and I'll add you :)

Google results for the same code returned results, and although it shows two results they are just different views of the same result (including the replies section of the tweet).

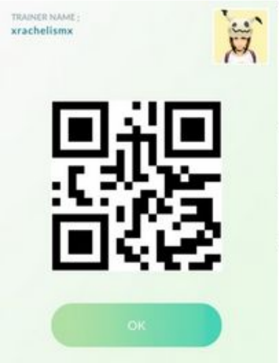


twitter.com › SimmerHailee › status ▾
Simmer Hailee on Twitter: "Add me on Pokémon go!! I need more ...
Add me on Pokémon go!! I need more friends. My trainer code is: **0753 1170 0698** Comment yours down below and I'll add you :)pic.twitter.com/T8tt8Bkpcb.

twitter.com › Tzelph › statuses ▾
Dave on Twitter: "5250 3165 8567… "
Add me on Pokémon go!! I need more friends. My trainer code is: **0753 1170 0698** Comment yours down below and I'll add you :)pic.twitter.com/T8tt8Bkpcb.

Although we did not manage to obtain a Reddit account from the trainer code, Twitter does have a great deal of additional points that could be exploited to find information on the target.

QR Codes

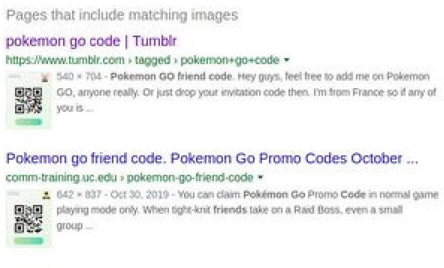


TRAINER NAME :
xrachelismx

QR codes appear to be less common that their numerical counterparts, though they may exist in a few different flavors. Most QR codes found in the wild will appear via an in-game screenshot from the user. Some third-party websites may also generate QR codes for players to scan and quickly add a number of friends all at one time without having to search for codes. The first instance may also provide the player's username in the screenshot, making it easier to run additional searches on the user should they not accept the friend request. QR codes from third party sites may or may not include any additional information other than the QR code, making it more difficult to know who you are adding.

QR codes are also more difficult to exploit, as although the QR code can be run through a reverse image search, the chances of it returning any matches are slim to none. This is especially true for the third-party codes that have nothing else in the image, though you should always run a reverse image search to cover all your bases. Scanning the QR code does not provide any additional information, instead the 12 digit friend code is just converted into a QR code for quick adding of friends. However, if you only have the QR code to begin with it might not be a bad idea to scan it and obtain the numeric version to search on friend code websites, search engines, or social media. There are a great number of QR readers online or via the appstore for your smartphone of choice. For Pokémon Go I am a fan of WebQR as it doesn't require me to crop the screenshot of a user's QR code, allowing me to upload either of the two types of commonly seen QR codes.

In an effort to gather more information on the above two examples, I ran them both through Google and Yandex reverse image search tools. Although both platforms thought they had matched the images, none of them had the same trainer as the ones uploaded.



Pages that include matching images

pokemon go code | Tumblr

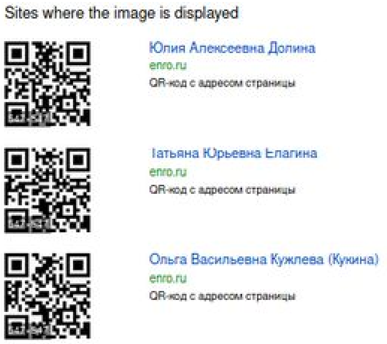
https://www.tumblr.com › tagged › pokemon+go+code ▾

540 × 704 - **Pokemon GO friend code**. Hey guys, feel free to add me on Pokemon GO, anyone really. Or just drop your invitation code then. I'm from France so if any of you is ...

Pokemon go friend code. Pokemon Go Promo Codes October ...

comm-training.uc.edu › pokemon-go-friend-code ▾

642 × 837 - Oct 30, 2019 - You can claim **Pokémon Go** Promo **Code** in normal game playing mode only. When tight-knit **friends** take on a Raid Boss, even a small group ...



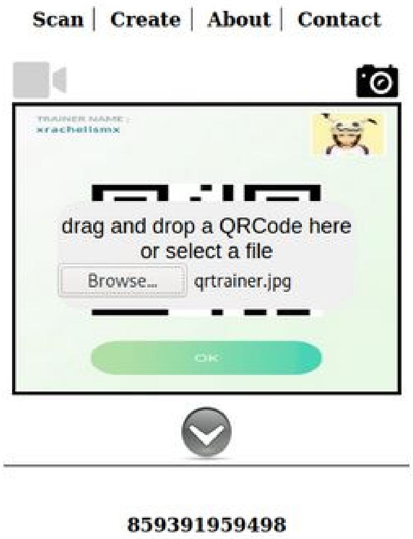
Sites where the image is displayed

Юлия Алексеевна Долина
enro.ru
QR-код с адресом страницы

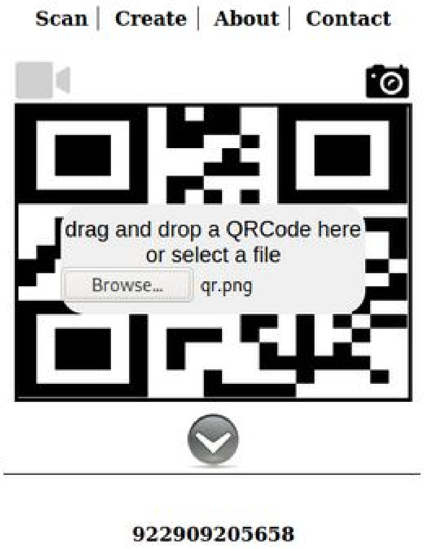
Татьяна Юрьевна Елагина
enro.ru
QR-код с адресом страницы

Ольга Васильевна Кужлева (Кукина)
enro.ru
QR-код с адресом страницы

With nothing actionable from the reverse image searches, I uploaded both of the QR codes into an online QR reader to obtain the friend codes below:

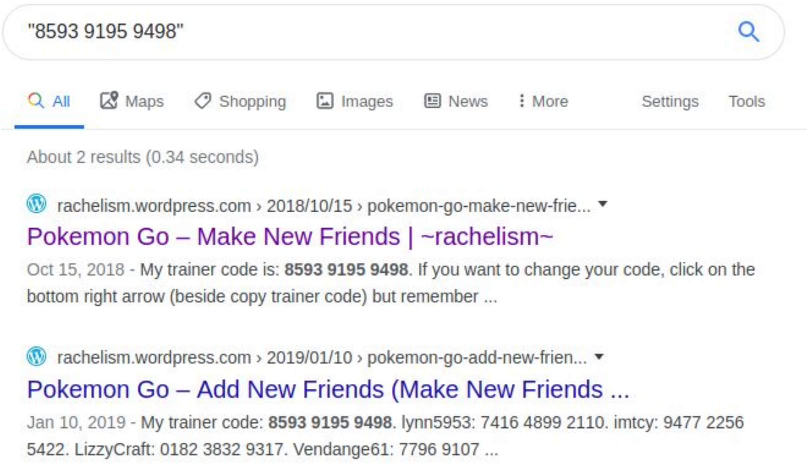


859391959498



922909205658

Once we have extracted the numerical friend code we can exploit it in the same manner as above by searching for the codes on websites and social media by running both codes in the #### #### #### format . The first example hit on a website that appears to be owned by the player tied to the account via the QR code. This site offers a good deal of additional information such as a username and a large amount of additional screenshots over time from their Pokémon Go account.



"8593 9195 9498"

About 2 results (0.34 seconds)

rachelism.wordpress.com › 2018/10/15 › pokemon-go-make-new-frie...

Pokemon Go – Make New Friends | ~rachelism~

Oct 15, 2018 - My trainer code is: **8593 9195 9498**. If you want to change your code, click on the bottom right arrow (beside copy trainer code) but remember ...

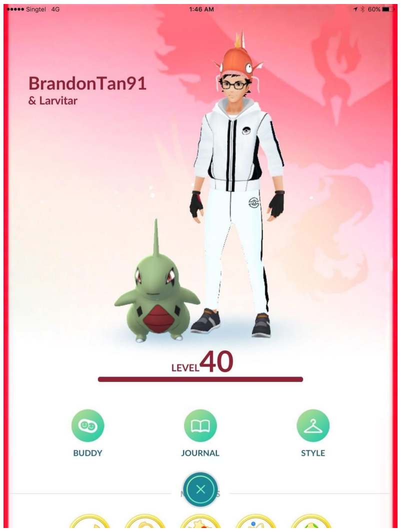
rachelism.wordpress.com › 2019/01/10 › pokemon-go-add-new-frien...

Pokemon Go – Add New Friends (Make New Friends ...

Jan 10, 2019 - My trainer code: **8593 9195 9498**. lynn5953: 7416 4899 2110. imtcy: 9477 2256 5422. LizzyCraft: 0182 3832 9317. Vendange61: 7796 9107 ...

Our second friend code hit on only the same website we started with, and did not offer any more additional information.

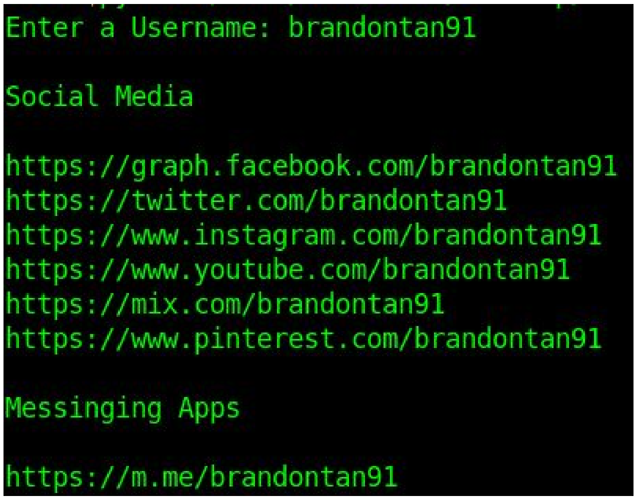
Username



The username is going to be one of the most commonly utilized points of exploitation for Pokémon GO users. A player's username might be one that they share across a number of platforms and may be exploited to find additional sites that may or may not contain additional information such as their name, general location, etc. The account's username may appear on screenshots, however if a screenshot is old it is possible that the user has since changed their username. Therefore I highly recommend pulling the username from recent interactions or from the friends list when possible. Once you've added an account, you can view the friend's username at any time in your friendslist as well as on any gifts that they send to your account.

Usernames can be searched across search engines such as Google, Yandex, Bing, or using specialized tools such as SULTAN, Namechk, etc. I also highly recommend searching usernames on Pokémon Go specific websites such as here or here. Using a combination of these tools should catch the most frequent websites. I also want to point out that a Pokémon Go player's username in-game is in a sans-serif font which makes it difficult to distinguish an uppercase "i" from a lowercase "L". When in doubt, try both combinations. Also be sure to look at any clues that might appear in the username in terms of names, important dates, or locations.

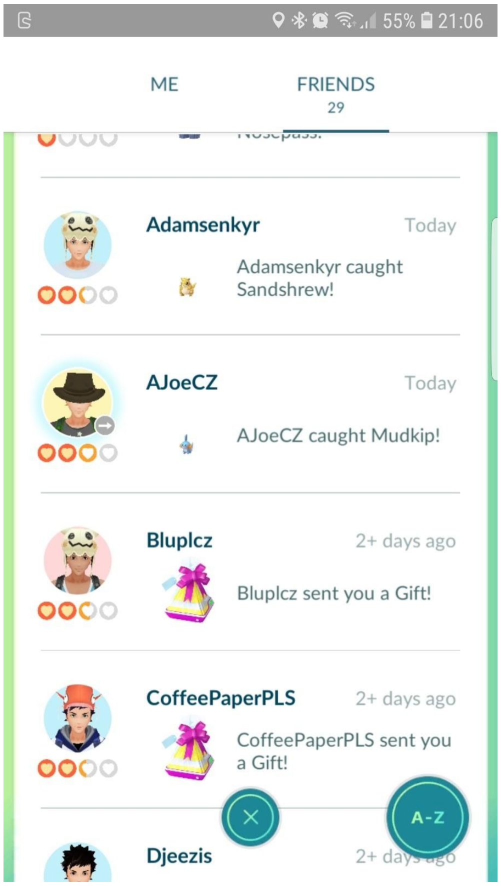
The above photo is a great example of how powerful a common username can be for finding additional accounts. The user (BrandonTan91) has the same username reserved on a number of websites. Running the username through SULTAN returns a number of social media sites, including high-value ones such as Twitter, Youtube, and Instagram, among others.



```
Enter a Username: brandontan91

Social Media

https://graph.facebook.com/brandontan91
https://twitter.com/brandontan91
https://www.instagram.com/brandontan91
https://www.youtube.com/brandontan91
https://mix.com/brandontan91
https://www.pinterest.com/brandontan91

Messinging Apps

https://m.me/brandontan91
```

Finally, looking at the username we can also make a confident guess that the user's real name is likely Brandon Tan, and they possibly were born in 1991.

Recent Activity



Adamsenkyr Today

Adamsenkyr caught Sandshrew!

AJoeCZ Today

AJoeCZ caught Mudkip!

Bluplcz 2+ days ago

Bluplcz sent you a Gift!

CoffeePaperPLS 2+ days ago

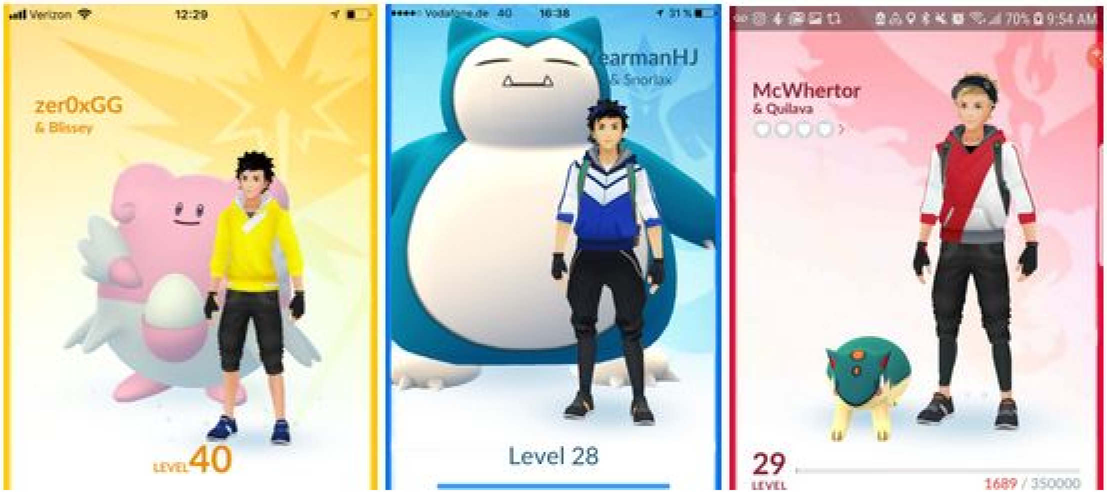
CoffeePaperPLS sent you a Gift!

Djeezis 2+ days ago

Once a player has been befriended in-game, they will appear under the friends tab of your profile. From here the user can quickly see how recently a friend was active, if they have been sent a gift from the user, or click on an individual to see their trainer profile which contains additional exploitable information. The recent activity section can be helpful for seeing how long ago a friend has captured a Pokémon (unless they disabled this feature) or approximately when they sent your account a gift. Unfortunately the times displayed for these occurrences only show the options of “Today”, “Yesterday” and “2+ days ago” making it difficult to know the exact date if they have not been viewed for awhile. Be sure to note any regional Pokémon that might give you an insight on where the user current is located (unless the user is spoofing their location). The date the user sent you a gift might also assist in mapping out their weekly routine.

The above users on the friends list show two users which sent the account a gift 2+ days ago, as well as two other users that caught Pokémon the same day as the screenshot. Although we can state that the two users with the caught Pokémon played today, the gifts do not provide us with much information. However, if the user were to open the gift, these accounts would display the last Pokémon they caught (if enabled), which might provide additional information. Noting the friendship levels of these accounts, it is likely that they are rather active, as they have managed to build up their friendship level a considerable amount by interacting with the owner of the account.

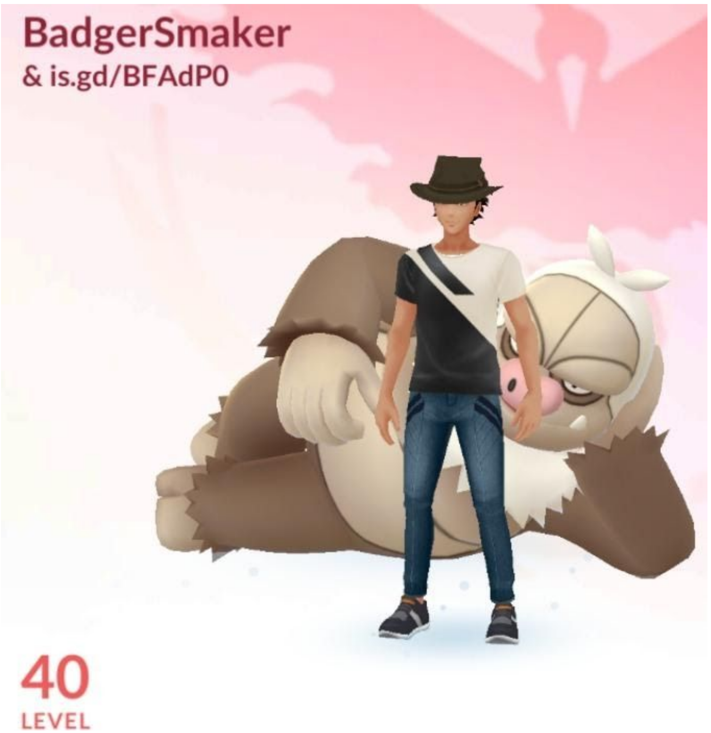
Team



Players are able to choose one of three different in-game teams to support. Team affiliation will affect what gyms players can battle or place their own Pokémon in to defend against other teams. A user's team affiliation can be seen in their trainer profile and include: Team Instinct (Yellow), Team Mystic (Blue) and Team Valor (Red). As team affiliation heavily affects gameplay, users may join Discord, Facebook, or other social media groups dedicated to their specific teams to coordinate with one another. Knowing a player's team affiliation may assist in narrowing down a pool of users on a Discord group or in person. Although many users do not represent their team in such an extreme way, there are indeed users that may have apparel or other accessories with their team logo on it that they like to wear during playtime or special events. Investigators might also see a player's team affiliation in various screenshots from a target. Although it is possible for a player to change their team affiliation, it does cost in-game currency to do so. For this reason it is suggested to pull the team affiliation information from a player's profile after they have been befriended to ensure it is the most up-to-date.

The above examples show an example of what players from all three teams look like, from left to right: Team Instinct, Team Mystic, and Team Valor.

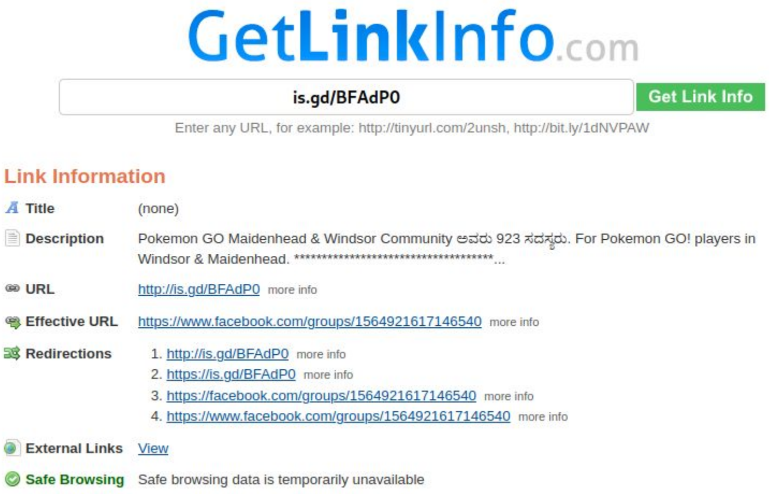
Buddy Name



BadgerSmaker
& is.gd/BFAdP0

Players may choose a Pokémon they previously captured to be their buddy, which provides them with additional features with that specific Pokémon. This includes various buddy mini-games as well as the ability to see the buddy on the overworld map with the user as well as on their profile. Like all Pokémon the user may assign their buddy a nickname. However buddy Pokémon are a unique case as being present on the user's profile means that their nicknames are visible to other players that have befriended the account. Although the buddy name is likely to contain little to no actionable data, or may just be the Pokémon's actual name, there has been discussion on Reddit and other online communities on ways to utilize the buddy nickname for communication (as Pokémon Go currently lacks any in-game communication methods). For those interested, such discussions can be found here, here, and here.

Our above example shows what appears to be a shortened URL used for the buddy nickname. Taking this URL we can utilize one of many URL expanders to check the actual link to where the URL redirects to before entering it into our browser. Utilizing GetlinkInfo we are able to see that it appears to redirect to a Pokémon Go Facebook group page.



GetLinkInfo.com

is.gd/BFAdP0

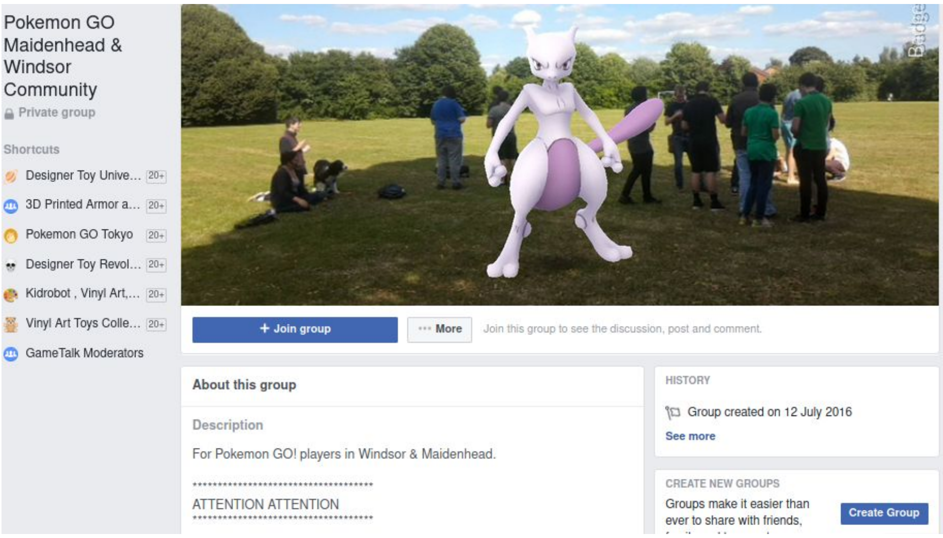
Get Link Info

Enter any URL, for example: http://tinyurl.com/2unsh, http://bit.ly/1dNVPAW

Link Information

Title	(none)
Description	Pokemon GO Maidenhead & Windsor Community ಅವರು 923 ಸದಸ್ಯರು. For Pokemon GO! players in Windsor & Maidenhead. ************************************...
URL	http://is.gd/BFAdP0 more info
Effective URL	https://www.facebook.com/groups/1564921617146540 more info
Redirections	1. http://is.gd/BFAdP0 more info 2. https://is.gd/BFAdP0 more info 3. https://facebook.com/groups/1564921617146540 more info 4. https://www.facebook.com/groups/1564921617146540 more info
External Links	View
Safe Browsing	Safe browsing data is temporarily unavailable

Now that we are aware that the URL lands on a legitimate website, we can navigate to the URL in the results above to view the Facebook page directly and bypass all of the redirects.



Pokemon GO Maidenhead & Windsor Community

Private group

Shortcuts

- Designer Toy Unive... 20+
- 3D Printed Armor a... 20+
- Pokemon GO Tokyo 20+
- Designer Toy Revol... 20+
- Kidrobot , Vinyl Art,... 20+
- Vinyl Art Toys Colle... 20+
- GameTalk Moderators

+ Join group

··· More

Join this group to see the discussion, post and comment.

About this group

Description

For Pokemon GO! players in Windsor & Maidenhead.

****

ATTENTION ATTENTION

****

HISTORY

Group created on 12 July 2016

See more

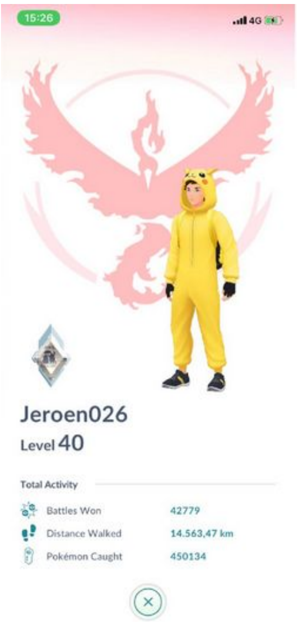
CREATE NEW GROUPS

Groups make it easier than ever to share with friends,

Create Group

From here we can see the Facebook Group is targeted to players in a local area of England. Knowing this information we can make an educated guess that the user with the buddy above is likely in this area of the country quite often and/or likely lives there or nearby. It also allows an investigator to narrow down their list of potential targets by also looking through the users that are within this Facebook group.

Total Activity



Jeroen026
Level 40

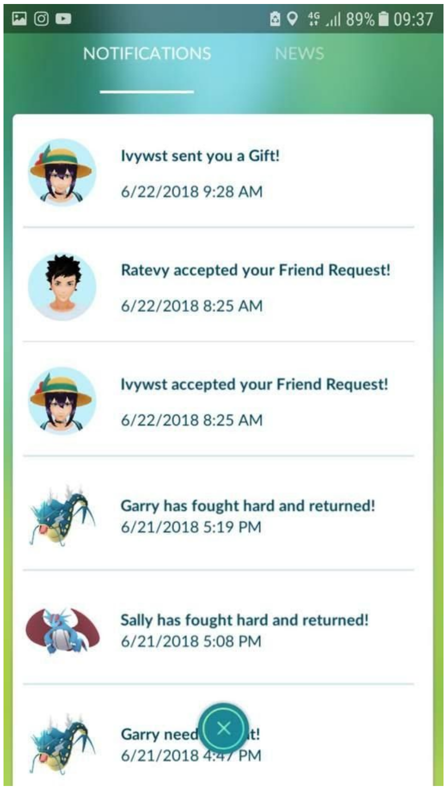
Total Activity

Battles Won	42779
Distance Walked	14.563,47 km
Pokémon Caught	450134

A user’s profile will also display their total in-game activity. Although this does not offer a great deal of actionable information it does assist in building pattern of life on the user regarding how often they play the game. Among the trainer level and username, this section will display the total battles won by the user, their total distance walked since starting the game, as well as the total number of Pokémon they have captured.

Our above example shows a user that has invested a great deal of time and walking into the game. We can see that they are likely more than a casual player based on their trainer level as well as their overall number of Pokémon caught and total distance walked. Finally, it seems that the user has participated in a large number of trainer battles. Coordinating a trainer battle might be a potential avenue for interacting with the user or requesting a meet-up.

Gifts



Ivywst sent you a Gift!
6/22/2018 9:28 AM

Ratevy accepted your Friend Request!
6/22/2018 8:25 AM

Ivywst accepted your Friend Request!
6/22/2018 8:25 AM

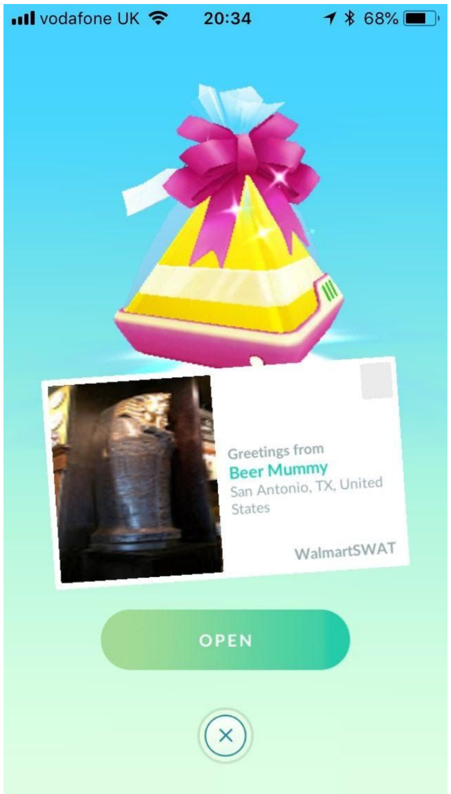
Garry has fought hard and returned!
6/21/2018 5:19 PM

Sally has fought hard and returned!
6/21/2018 5:08 PM

Garry need t!
6/21/2018 4:47 PM

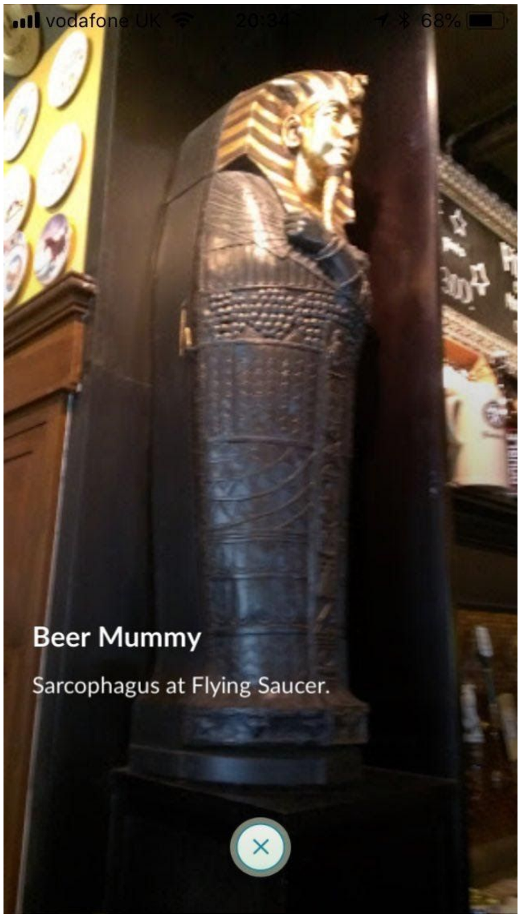
Players can send gifts to their in-game friends that will provide them with additional items and XP. This will appear as a gift box to the right of the friend’s username under the friends list. Clicking on that user will open the user’s profile and the gift screen will open as well. Similar to Pokéstops and gyms, these gifts contain point-of-interest information that corresponds to the location in which the user originally obtained the gift. Much like we did with the gym badges in Part I, we can use the timing of each gift received to map out a possible walking route from the sender by using the timestamps of when the gift(s) were sent via the in-game notifications screen such as in the above photo. Be advised that the timestamps are when the gifts were sent, not when they were obtained by the sender. Users may hold on to gifts and send them in any order they wish.

When clicking on a gift via the sender’s profile, a screen similar to the following will open:



Greetings from
Beer Mummy
San Antonio, TX, United States
WalmartSWAT

This screen will give you a great deal of information on where the user obtained the gift. The gift’s title will give some indication of what point-of-interest the gift was received from. As these titles are user-submitted, their accuracy may vary from one gift to the next. Directly below the title is the location of the gift. This will be useful for pegging a starting point on Pokélytics or OpenStreetMaps. Finally, there is a thumbnail photo of the point-of-interest submitted by users. This thumbnail can be reverse image searched, however depending on the point-of-interest and the quality of the photo thumbnail it may provide little to no results. Although the above screen provides a great deal of information, an investigator can obtain additional info by clicking on the postcard image. This will open a second screen which will look similar to the one below:

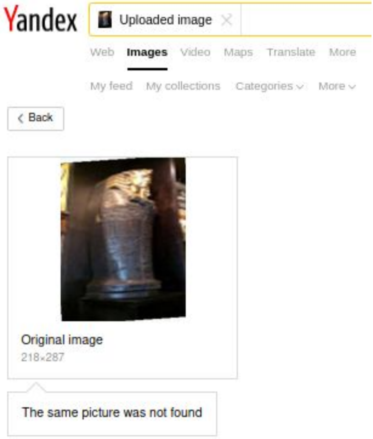


Beer Mummy

Sarcophagus at Flying Saucer.

This new image includes the same title as the initial view, however it provides a much higher resolution photo of the point-of-interest than the original thumbnail. Additionally, there is a short description added below the title which may assist in further narrowing down our location.

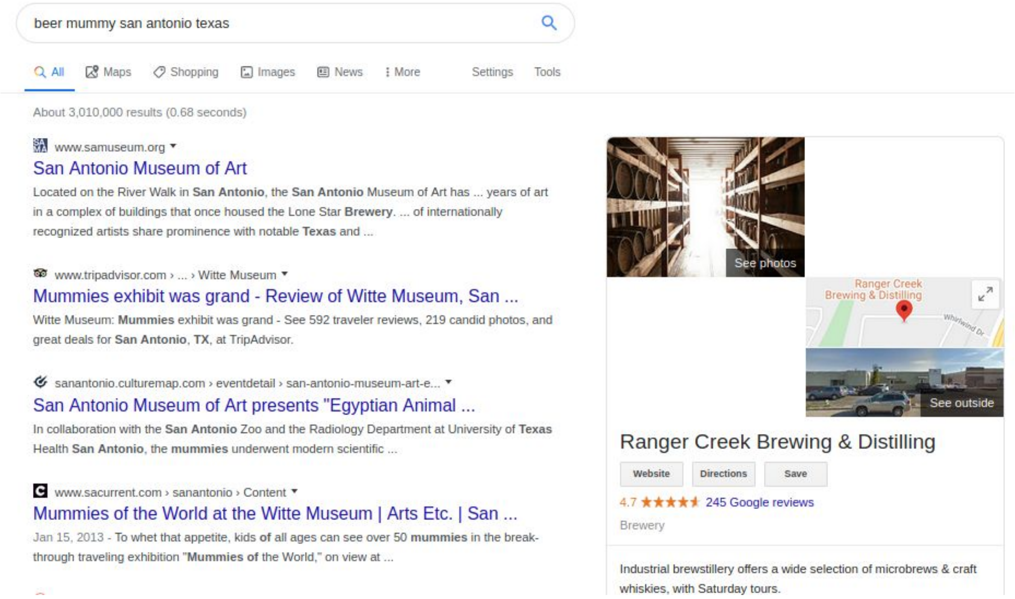
Looking at the initial gift screen above, we can crop the photo to only include the thumbnail of the point-of-interest and run it through a reverse image search. Both Yandex and Google failed to find the same image.



Original image
218×287

The same picture was not found

Next, I attempted to find the location by looking for “Beer Mummy” and “San Antonio Texas”. Unfortunately, there appear to be many results that did not appear to match up to our original photo.



About 3,010,000 results (0.68 seconds)

www.samuseum.org

San Antonio Museum of Art

Located on the River Walk in **San Antonio**, the **San Antonio** Museum of Art has ... years of art in a complex of buildings that once housed the Lone Star **Brewery**. ... of internationally recognized artists share prominence with notable **Texas** and ...

www.tripadvisor.com › ... › Witte Museum

Mummies exhibit was grand - Review of Witte Museum, San ...

Witte Museum: **Mummies** exhibit was grand - See 592 traveler reviews, 219 candid photos, and great deals for **San Antonio**, **TX**, at TripAdvisor.

sanantonio.culturemap.com › eventdetail › san-antonio-museum-art-e...

San Antonio Museum of Art presents "Egyptian Animal ...

In collaboration with the **San Antonio** Zoo and the Radiology Department at University of **Texas** Health **San Antonio**, the **mummies** underwent modern scientific ...

www.sacurrent.com › sanantonio › Content

Mummies of the World at the Witte Museum | Arts Etc. | San ...

Jan 15, 2013 - To whet that appetite, kids **of** all ages can see over 50 **mummies** in the break-through traveling exhibition "**Mummies of** the World," on view at ...

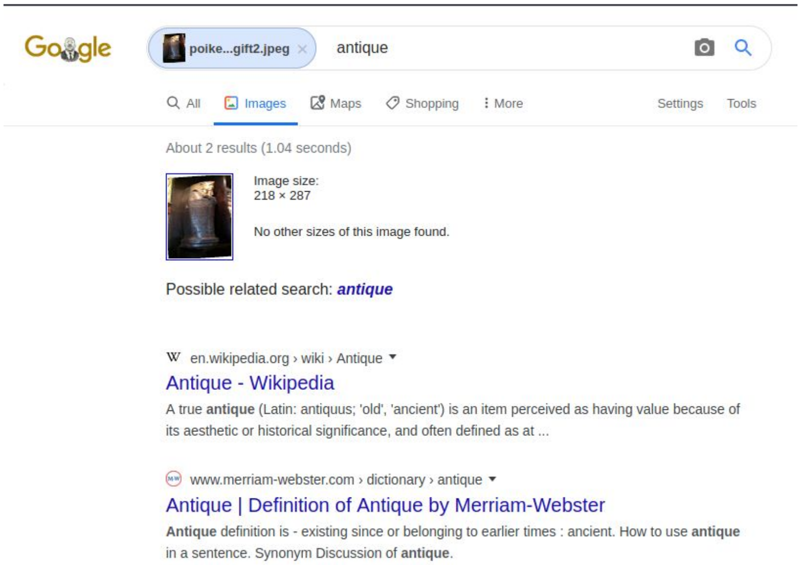
Ranger Creek Brewing & Distilling

4.7 ★★★★★ 245 Google reviews

Brewery

Industrial brewstillery offers a wide selection of microbrews & craft whiskies, with Saturday tours.

Without much to go on for the initial view, let’s add in some of the information from the second view. First off, I ran the larger image through Yandex and Google once again. Unfortunately, same as with the thumbnail, none of the reverse image search tools were able to locate a match. However, Google has attempted to identify what is in the photo as an “antique”.



antique

About 2 results (1.04 seconds)

Image size:
218 × 287

No other sizes of this image found.

Possible related search: ***antique***

en.wikipedia.org › wiki › Antique

Antique - Wikipedia

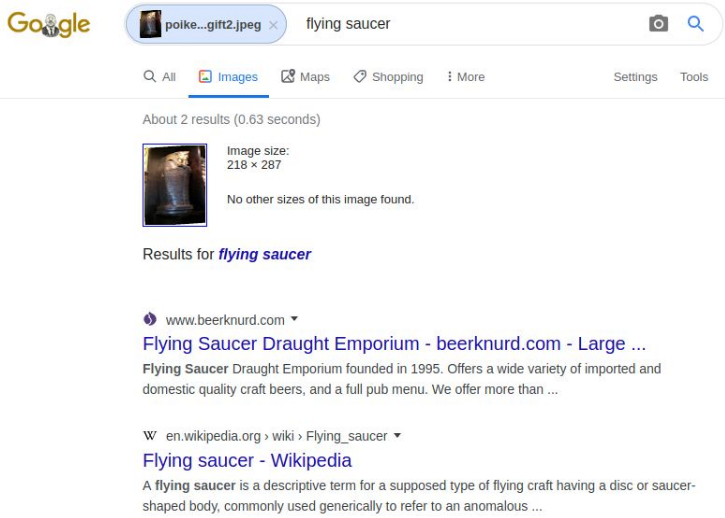
A true **antique** (Latin: antiquus; 'old', 'ancient') is an item perceived as having value because of its aesthetic or historical significance, and often defined as at ...

www.merriam-webster.com › dictionary › antique

Antique | Definition of Antique by Merriam-Webster

Antique definition is - existing since or belonging to earlier times : ancient. How to use **antique** in a sentence. Synonym Discussion of **antique**.

While this identification is not wrong, it doesn’t help much in narrowing down our results to find the location where this gift came from. Perhaps we can modify this keyword to include our additional information from the second screen to include “Flying Saucer”, where the photo was purportedly taken. Doing so gave us new results, the first of which mentions a “Flying Saucer Draught Emporium”.



About 2 results (0.63 seconds)

Image size:
218 × 287

No other sizes of this image found.

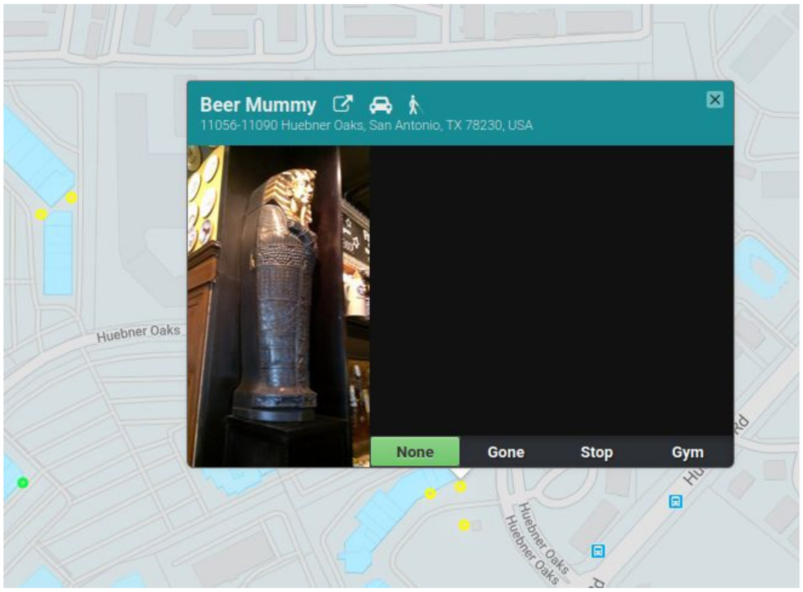
Results for *flying saucer*

www.beerknurd.com ▾
Flying Saucer Draught Emporium - beerknurd.com - Large ...
Flying Saucer Draught Emporium founded in 1995. Offers a wide variety of imported and domestic quality craft beers, and a full pub menu. We offer more than ...

en.wikipedia.org › wiki › Flying_saucer ▾
Flying saucer - Wikipedia
A **flying saucer** is a descriptive term for a supposed type of flying craft having a disc or saucer-shaped body, commonly used generically to refer to an anomalous ...

We can cross-reference this possible location by an additional Google image search and can confirm that it is indeed the location we are looking for.

This trick does not work for everything but is always worth a shot. Had this not worked, the next step would be to attempt to locate the establishment via Google Dorking. Now that we believe we have the right location we can confirm it via Pokélytics, which shows the same point-of-interest title and photo as the one we started with.



Beer Mummy
11056-11090 Huebner Oaks, San Antonio, TX 78230, USA

Using this location information, we can plot it on a map with a note of when the user sent it if we wished to map out a possible route.

Conclusion

Between Parts I and II of this guide you should be well on your way to extracting as much information from a Pokémon Go target as possible. Be sure to check out my Github, which includes a mapping of Pokémon Go OSINT points of exploitation as well as some bookmarks and javascript tools to help aid you in your next investigation. Should you have any OSINT-related questions, whether related to this article or any of my others, please feel free to reach out to me on Twitter.