**Open Source Intelligence**

SherlockPwns

Sakura Room  
A TRY HACK ME WRITE UP



# INTRODUCTION

This room is designed to test a wide variety of different OSINT techniques. With a bit of research, most beginner OSINT practitioners should be able to complete these challenges. This room will take you through a sample OSINT investigation in which you will be asked to identify a number of identifiers and other pieces of information in order to help catch a cybercriminal. Each section will include some pretext to help guide you in the right direction, as well as one or more questions that need to be answered in order to continue on with the investigation. Although all of the flags are staged, this room was created using working knowledge from having led and assisted in OSINT investigations both in the public and private sector.

NOTE: All answers can be obtained via passive OSINT techniques, DO NOT attempt any active techniques such as reaching out to account owners, password resets, etc to solve these challenges.

## Task 1

Once you have read all of the introduction section the last section tell syou what you need to answer the question which is.

For this task if you read all the way through the information tells you the following

“Ready to get started? Type in "Let's Go!" in the answer box below to continue.”

### Answer

* Let’s Go

# TIP-OFF

## Task 2

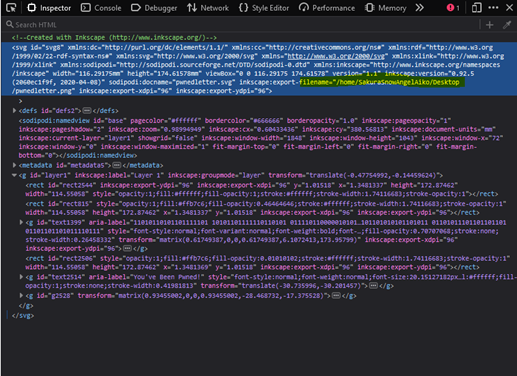
### Background

The OSINT Dojo recently found themselves the victim of a cyber attack. It seems that there is no major damage, and there does not appear to be any other significant indicators of compromise on any of our systems. However during forensic analysis our admins found an image left behind by the cybercriminals. Perhaps it contains some clues that could allow us to determine who the attackers were?

This section gives you a link to a URL which is a SVG which is a scalable vector graphics meaning that sometimes this can contain metadata embedded in the file when the image is generated.

https://raw.githubusercontent.com/OsintDojo/public/3f178408909bc1aae7ea2f51126984a8813b0901/sakurapwnedletter.svg

Clicking the inspect button to view the data we were given the data about the image (shown below.) this gives us the path of whee this users directory is filename=”home/SakuraSnowAngelAiko/desktop



### Answer

* SakuraSnowAngelAiko

# RECONNAISSANCE

## Task 3

### Background

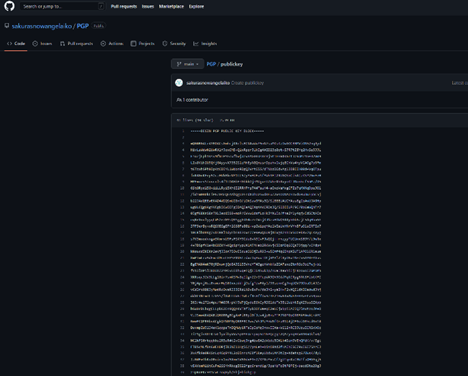
It appears that our attacker made a fatal mistake in their operational security. They seem to have reused their username across other social media platforms as well. This should make it far easier for us to gather additional information on them by locating their other social media accounts.

### Instructions

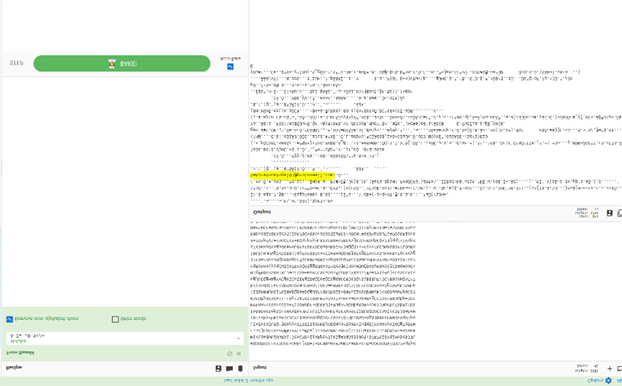
Most digital platforms have some sort of username field. Many people become attached to their usernames, and may therefore use it across a number of platforms, making it easy to find other accounts owned by the same person when the username is unique enough. This can be especially helpful on platforms such as on job hunting sites where a user is more likely to provide real information about themselves, such as their full name or location information.

A quick search on a reputable search engine can help find matching usernames on other platforms, and there are also a large number of specialty tools that exist for that very same purpose. Keep in mind that sometimes a platform will not show up in either the search engine results or in the specialized username searches due to false negatives. In some cases you need to manually check the site yourself to be 100% positive if the account exists or not. In order to answer the following questions, use the attacker's username found in Task 2 to expand the OSINT investigation onto other platforms in order to gather additional identifying information on the attacker. Be wary of any false positives!

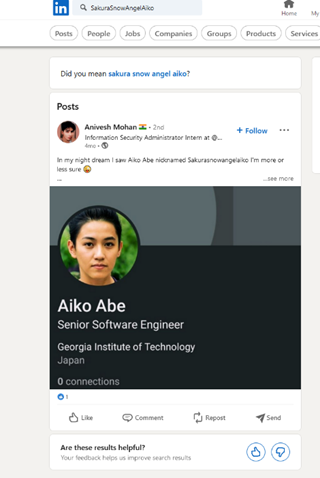
Using the above information from the previous task a google dork search provided a github account https://github.com/sakurasnowangelaiko and what stood out was one of the repositories called PGP ( pretty good privacy). A quick glance into the PGP shows us that this is a key and it's in a base64 format so we can try to decode this using cyberchef



Using cyber chef we were able to gain the users email answering the next question



After finding this email i used google again to find any social media accounts which i found a linkedin profile giving us the users name



### Answers

* SakuraSnowAngel83@protonmail.com
* Aiko Abe

# 

# UNVEIL

## Task 4

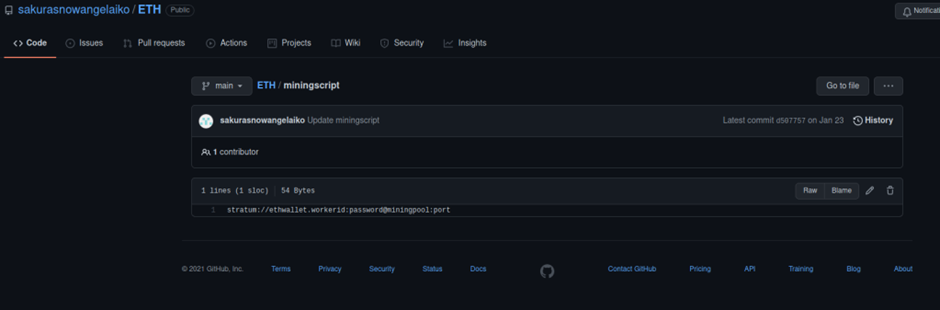
### Background

It seems the cybercriminal is aware that we are onto them. As we were investigating into their Github account we observed indicators that the account owner had already begun editing and deleting information in order to throw us off their trail. It is likely that they were removing this information because it contained some sort of data that would add to our investigation. Perhaps there is a way to retrieve the original information that they provided?

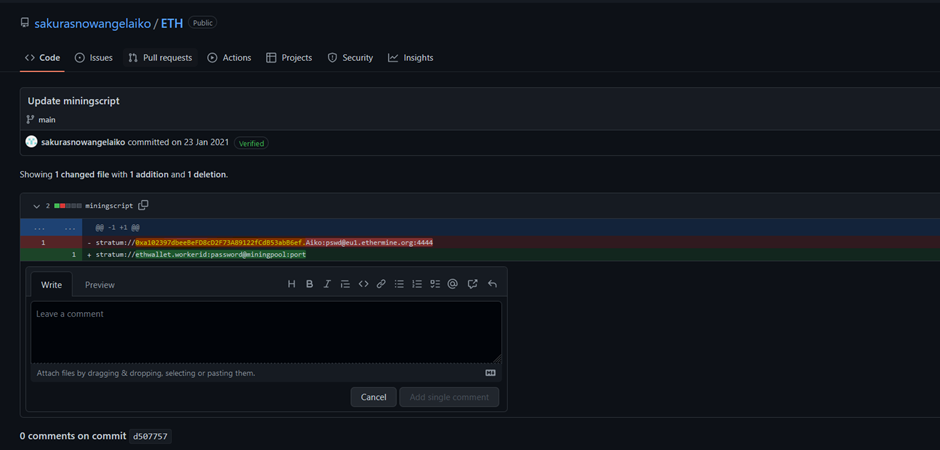
### Instructions

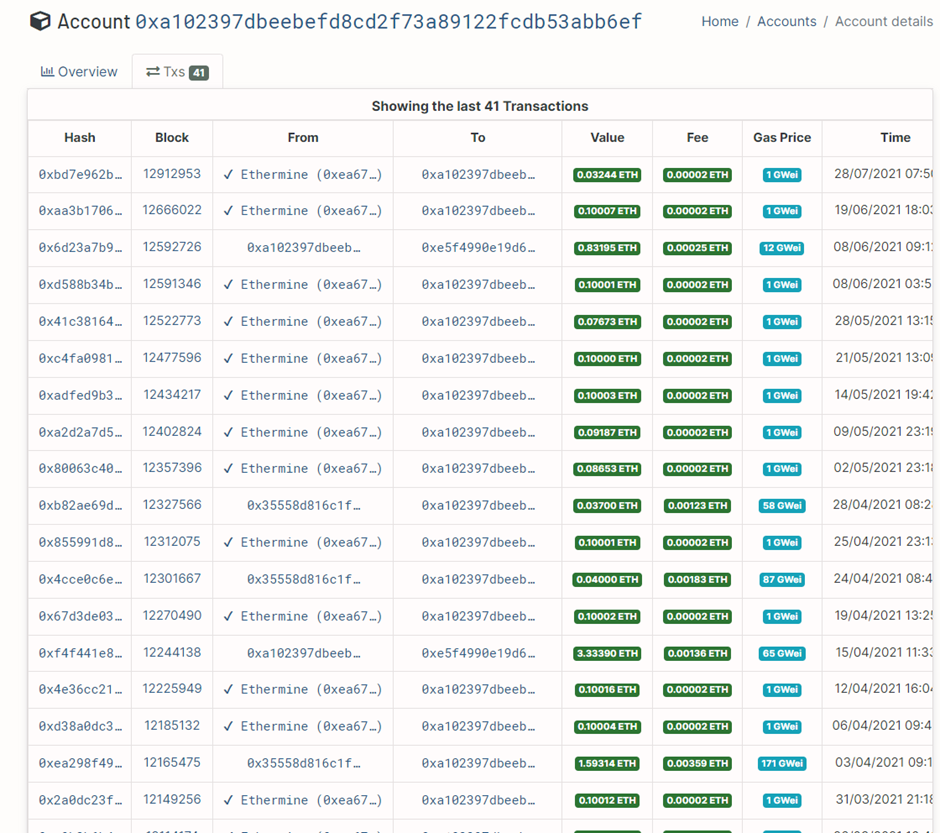
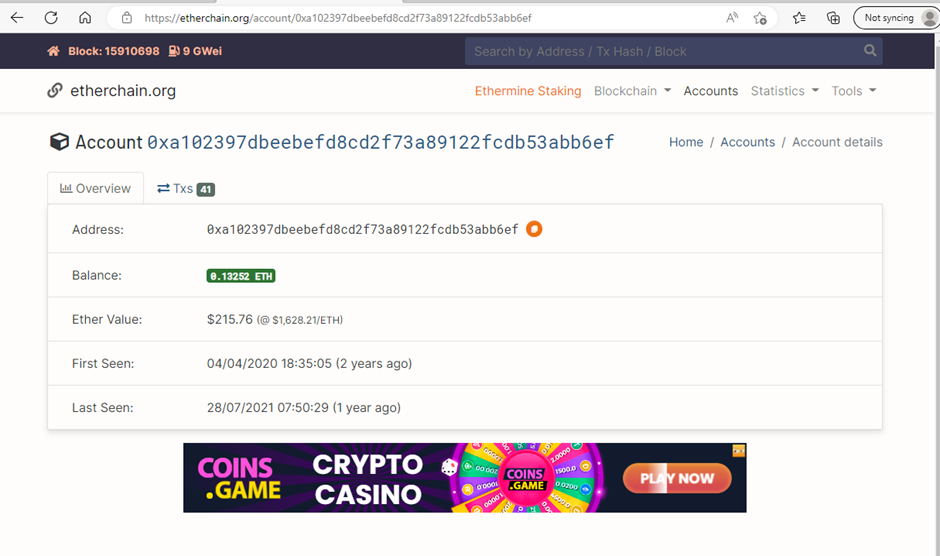
On some platforms, the edited or removed content may be unrecoverable unless the page was cached or archived on another platform. However, other platforms may possess built-in functionality to view the history of edits, deletions, or insertions. When available this audit history allows investigators to locate information that was once included, possibly by mistake or oversight, and then removed by the user. Such content is often quite valuable in the course of an investigation. In order to answer the below questions, you will need to perform a deeper dive into the attacker's Github account for any additional information that may have been altered or removed. You will then utilize this information to trace some of the attacker's cryptocurrency transactions.

Going back to the github repository from the earlier task i had found a few repositories with some naming conventions related to crypto so started with the ETH respiratory and found the following:



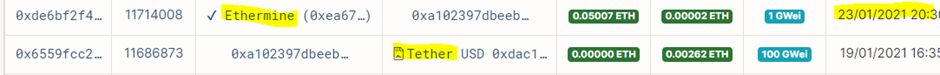
Looking at the hasty section i saw the wallet number within



Googling alot I reached upon <https://etherchain.org/> which we can see the users transactions 

### 

Scrolling down we can see the answers for the next two questions.

****

### 

### Answers

* Ethereum
* 0xa102397dbeeBeFD8cD2F73A89122fCdB53abB6ef
* Ethermine
* Thether

# TAUNT

## Task 5

### Background

Just as we thought, the cybercriminal is fully aware that we are gathering information about them after their attack. They were even so brazen as to message the OSINT Dojo on Twitter and taunt us for our efforts. The Twitter account which they used appears to use a different username than what we were previously tracking, maybe there is some additional information we can locate to get an idea of where they are heading to next?

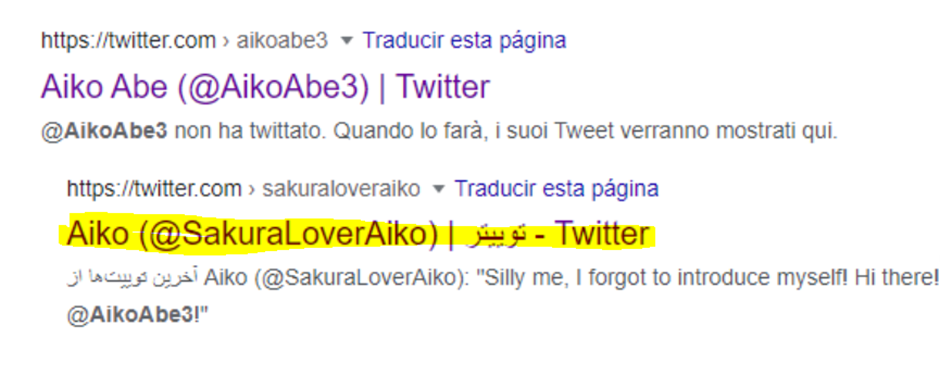
### 

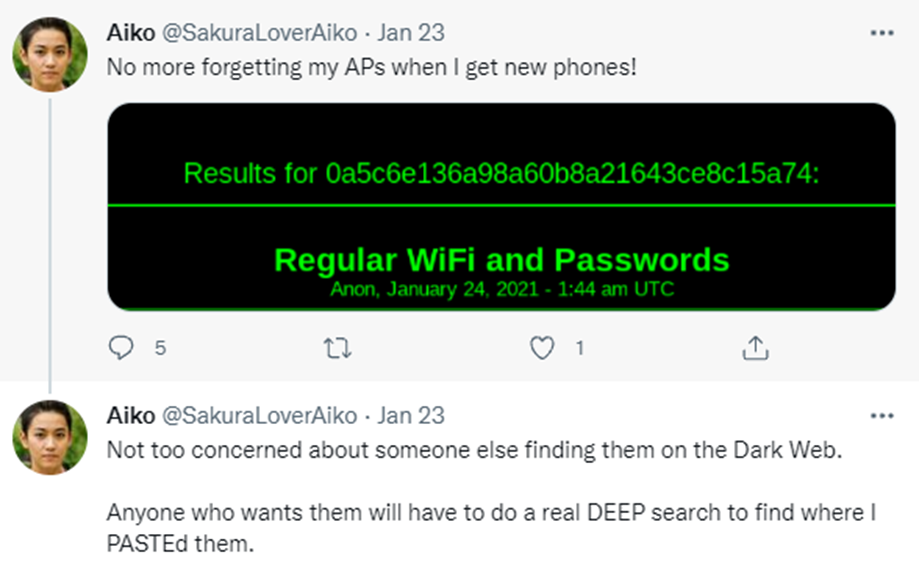
### 

### Instructions

Although many users share their username across different platforms, it isn't uncommon for users to also have alternative accounts that they keep entirely separate, such as for investigations, trolling, or just as a way to separate their personal and public lives.

These alternative accounts might contain information not seen in their other accounts, and should also be investigated thoroughly. In order to answer the following questions, you will need to view the screenshot of the message sent by the attacker to the OSINT Dojo on Twitter and use it to locate additional information on the attacker's Twitter account. You will then need to follow the leads from the Twitter account to the Dark Web and other platforms in order to discover additional information.

Using the image which is given to us in the room a quick google search brings back the attackers new twitter account. 

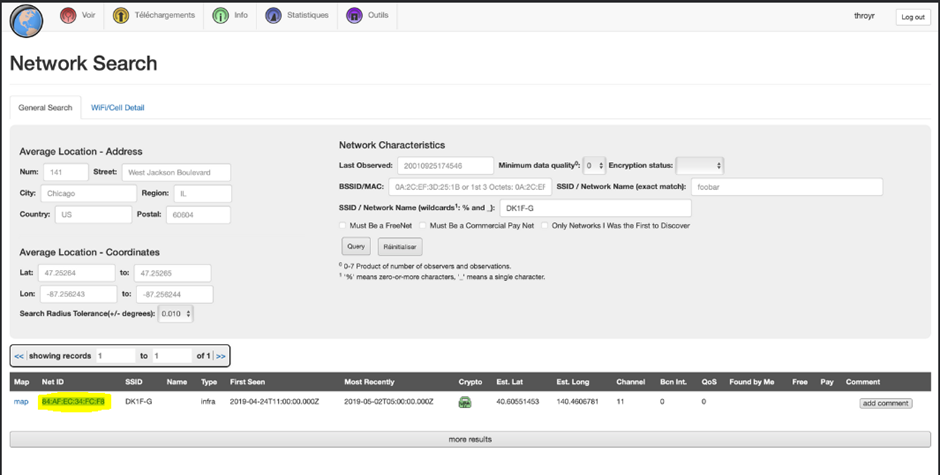
Going through this new twitter account we can have found this tweet 

Here I had to use the screen shot within the hint section as even though I found the darkweb source the website was down and wasn't able to proceed.



Using the url i matched the MD5 hash from the twitter post to get the next question.

We also had the ssd information and a using website <https://wigle.net> it gave us the users location bssid. For the attackers Home Wifi



### 

### Answers

* SakuraLoverAiko
* http://deepv2w7p33xa4pwxzwi2ps4j62gfxpyp44ezjbmpttxz3owlsp4ljid.onion/show.php?md5=b2b37b3c106eb3f86e2340a3050968e2
* 84:af:ec:34:fc:f8

# 

# 

# HOMEBOUND

## Task 6

### Background

Based on their tweets, it appears our cybercriminal is indeed heading home as they claimed. Their Twitter account seems to have plenty of photos which should allow us to piece together their route back home. If we follow the trail of breadcrumbs they left behind, we should be able to track their movements from one location to the next back all the way to their final destination. Once we can identify their final stops, we can identify which law enforcement organization we should forward our findings to.

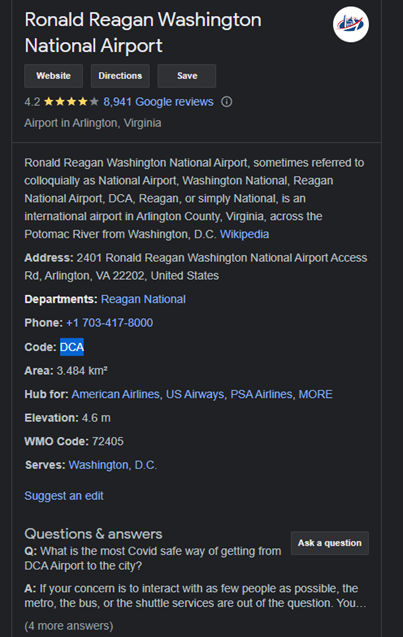
### Instructions

In OSINT, there is oftentimes no "smoking gun" that points to a clear and definitive answer. Instead, an OSINT analyst must learn to synthesize multiple pieces of intelligence in order to make a conclusion of what is likely, unlikely, or possible. By leveraging all available data, an analyst can make more informed decisions and perhaps even minimize the size of data gaps. In order to answer the following questions, use the information collected from the attacker's Twitter account, as well as information obtained from previous parts of the investigation to track the attacker back to the place they call home.

Heading back to twitter and doing a deeper dive we can see the following post which the atatcker is mentioning that they are checking out some cheery blossoms before heading back



From this we can easily pick out the Washington Monument in Washington, DC, United States. Using the location of the water and train tracks we can pinpoint his on google maps . which gives us the airpot location a quick google search gives use the 3 letter code for this airport



The next question asks us where there the attackers layover was so again back to twitter and we can see this tweet

### 

### 

### 

### 

### 

### 

### 

### 

### 

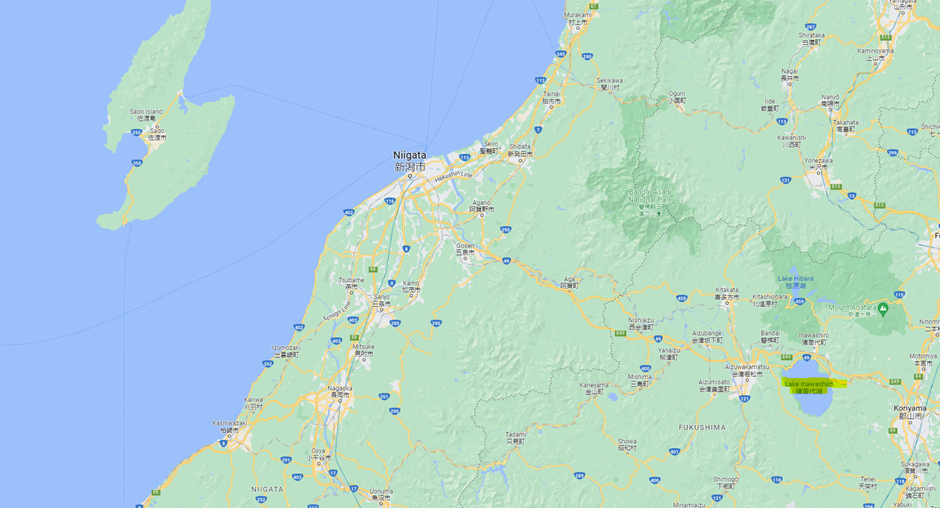
### 

Using an image reverse tool we easily find that this is part of the Haneda Airport



Giving us the answer for our next question 

Heading back to twitter we are give a picture of a map bringing up google maps and scanning the world we can see it leads up to Japan near NIIGATA on the right hand side it shows us this which gives us our next questions answer (highlighted)



The final question we need to bring all the information together

Going back and using wiggle to go back and check out all the ssid , we can conclude that they all belong in the same city but we have also answered this earlier as we had to search for the home ssid in an earlier question to the answer Hirosaki

### Answers

* DCA
* HND
* Lake Inawashiro
* Hirosaki