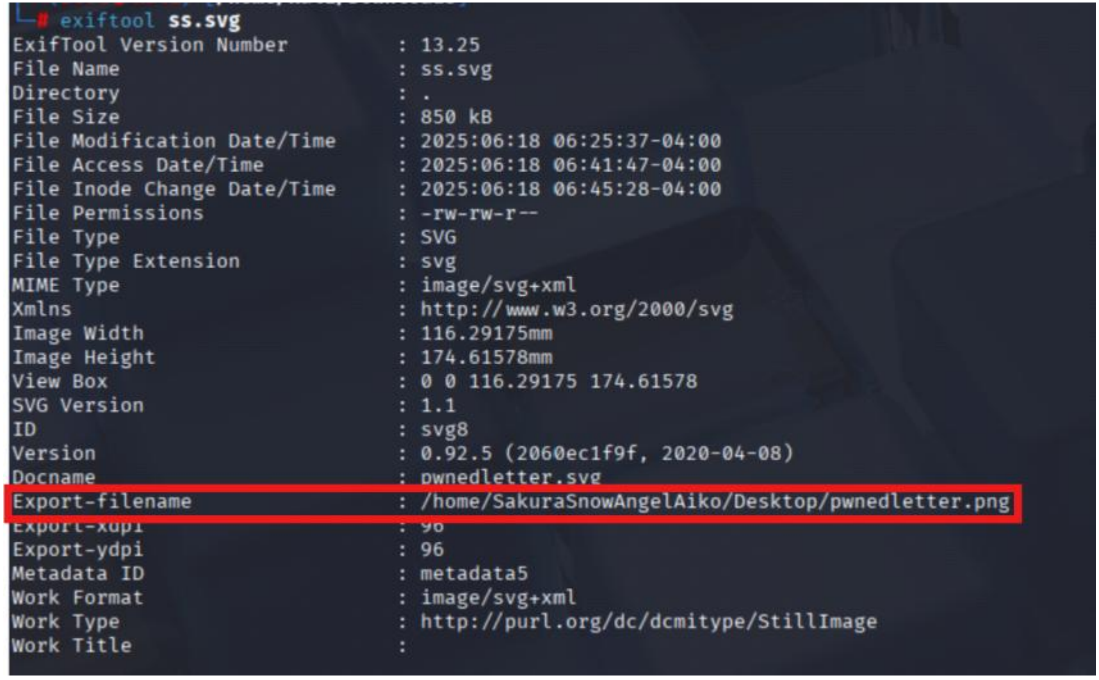
1. Sakura Room

18 June 2025 16:13

Task 2:

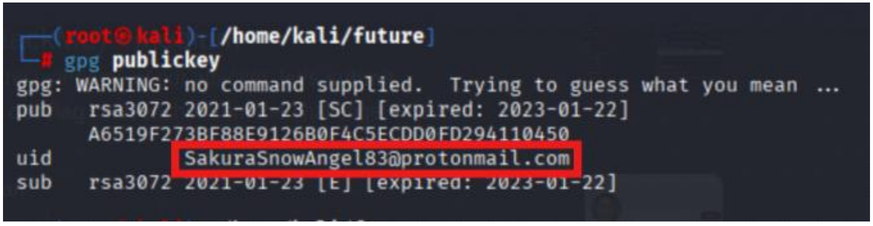
Just take the meta data using exiftool and then you can see the export filename was home/SakuraSnowAngelAiko/Desktop/Pwnedletter.jpg so of course the username is SakuraSnowAngelAiko



```
└─# exiftool ss.svg
ExifTool Version Number         : 13.25
File Name                       : ss.svg
Directory                       : .
File Size                       : 850 kB
File Modification Date/Time     : 2025:06:18 06:25:37-04:00
File Access Date/Time           : 2025:06:18 06:41:47-04:00
File Inode Change Date/Time     : 2025:06:18 06:45:28-04:00
File Permissions                : -rw-rw-r--
File Type                       : SVG
File Type Extension             : svg
MIME Type                       : image/svg+xml
Xmlns                           : http://www.w3.org/2000/svg
Image Width                     : 116.29175mm
Image Height                    : 174.61578mm
View Box                        : 0 0 116.29175 174.61578
SVG Version                     : 1.1
ID                              : svg8
Version                         : 0.92.5 (2060ec1f9f, 2020-04-08)
Docname                         : pwnedletter.svg
Export-filename                 : /home/SakuraSnowAngelAiko/Desktop/pwnedletter.png
Export-xdpi                     : 96
Export-ydpi                     : 96
Metadata ID                     : metadata5
Work Format                     : image/svg+xml
Work Type                       : http://purl.org/dc/dcmitype/StillImage
Work Title                      :
```

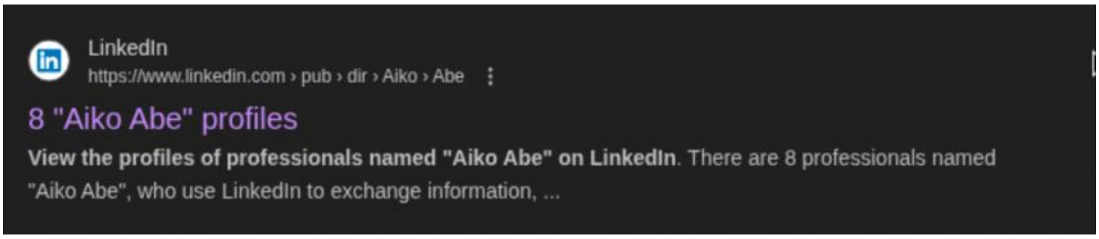
Task 3:

Question 1: you see a pgp repo in the github profile with the same username and inside theres a public key you can check the details to find the email. The public key pgp file can be extracted from using gpg tool on kali.



```
┌──(root㉿kali)-[/home/kali/future]
└─# gpg publickey
gpg: WARNING: no command supplied.  Trying to guess what you mean ...
pub   rsa3072 2021-01-23 [SC] [expired: 2023-01-22]
      A6519F273BF88E9126B0F4C5ECDD0FD294110450
uid           SakuraSnowAngel83@protonmail.com
sub   rsa3072 2021-01-23 [E] [expired: 2023-01-22]
```

Question2: We can find a linkedin account with the same name giving out the full name.



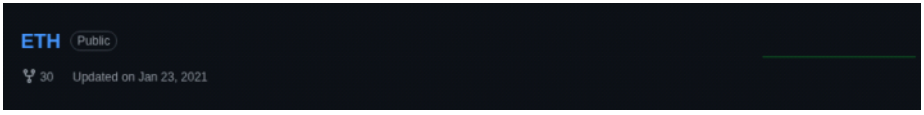
LinkedIn
https://www.linkedin.com › pub › dir › Aiko › Abe

8 "Aiko Abe" profiles

View the profiles of professionals named "Aiko Abe" on LinkedIn. There are 8 professionals named "Aiko Abe", who use LinkedIn to exchange information, ...

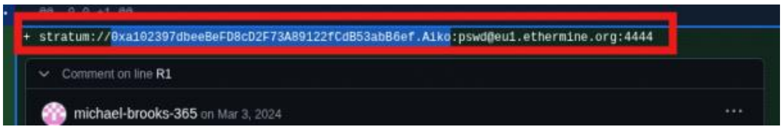
Task 4:

Question 1: We find a repo with the name ETH which is short form for ethereum hinting at the fact that the crypto might be ethereum



ETH Public
30 Updated on Jan 23, 2021

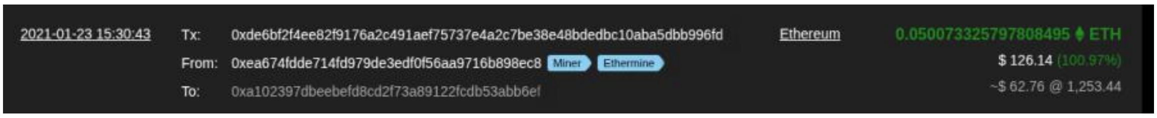
Question 2: As hinted in the details if you do check the previous versions of the file we get the address and password



```
+ stratum://0xa102397dbeeBeFD8cD2F73A89122fCdB53abB6ef.Aiko:pswd@eu1.ethermine.org:4444
```

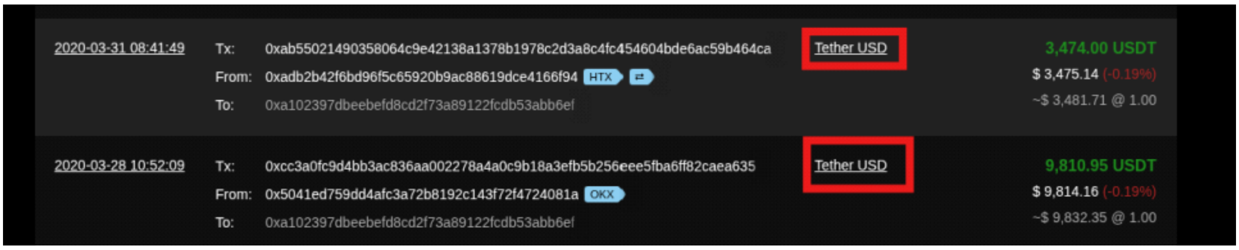
Comment on line R1
michael-brooks-365 on Mar 3, 2024

Question 3: You can use a website like ethplorer to check the transactions on the address and we can see the mining pool



```
2021-01-23 15:30:43   Tx:    0xde6bf2f4ee82f9176a2c491aef75737e4a2c7be38e48bdedbc10aba5dbb996fd   Ethereum   0.050073325797808495 ETH
                      From:  0xea674fdde714fd979de3edf0f56aa9716b898ec8 Miner Ethermine                  $ 126.14 (100.97%)
                      To:    0xa102397dbeebefd8cd2f73a89122fcdb53abb6ef                                  ~$ 62.76 @ 1,253.44
```

Question 4: We can see that some exchanges have been done with tether too so that's the answer to that.



```
2020-03-31 08:41:49   Tx:    0xab55021490358064c9e42138a1378b1978c2d3a8c4fc454604bde6ac59b464ca   Tether USD   3,474.00 USDT
                      From:  0xadb2b42f6bd96f5c65920b9ac88619dce4166f94 HTX ⇄                           $ 3,475.14 (-0.19%)
                      To:    0xa102397dbeebefd8cd2f73a89122fcdb53abb6ef                                 ~$ 3,481.71 @ 1.00

2020-03-28 10:52:09   Tx:    0xcc3a0fc9d4bb3ac836aa002278a4a0c9b18a3efb5b256eee5fba6ff82caea635   Tether USD   9,810.95 USDT
                      From:  0x5041ed759dd4afc3a72b8192c143f72f4724081a OKX                             $ 9,814.16 (-0.19%)
                      To:    0xa102397dbeebefd8cd2f73a89122fcdb53abb6ef                                 ~$ 9,832.35 @ 1.00
```

Task 5:

Question 1:

Question 2: We can search the internet for JAL lounges that's posted on the attacker's twitter and since they posted a picture of their home in japan we can check out the ones in japan leading to HND

Task 6:

Question 1:

Question 2: HND. You can find it by reverse searching the airport lounge and testing out the airports with the same there would be two and the answer would come out as HND

Question 3: Cross Referencing The image with the map of Japan you can find out the name of the lake which turns out to be Lake Inawashiro

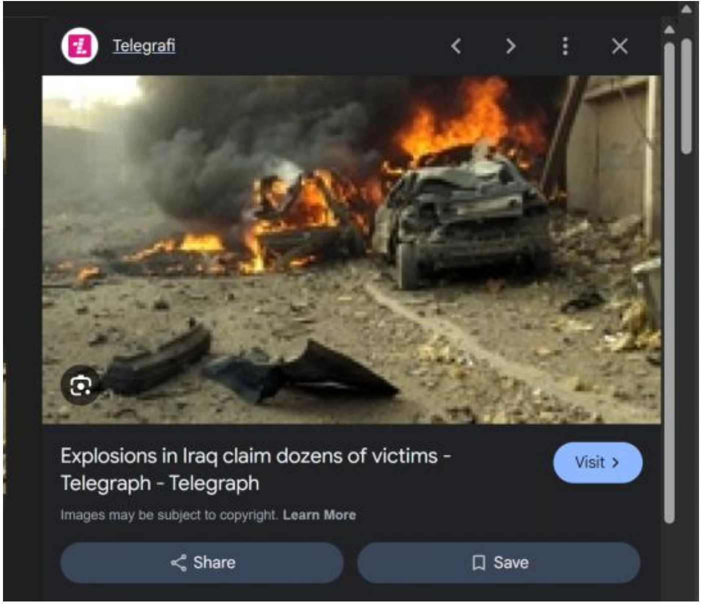
Question 4:

2. Other OSINT challenges

20 June 2025 15:06

a. OSINT Exercise 6

- The image is actually the explosions occurred in Iraq

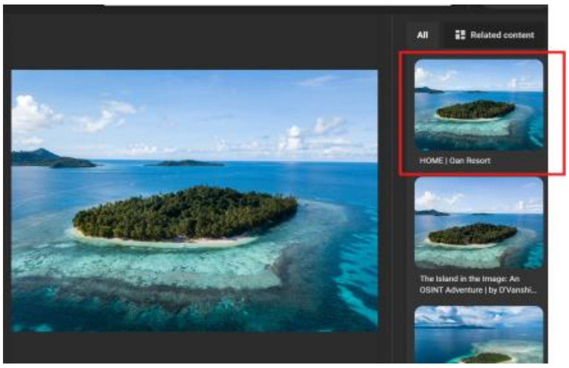


Explosions in Iraq claim dozens of victims - Telegraph - Telegraph

Images may be subject to copyright. Learn More

b. OSINT Exercise 4

- Reverse Searching the image we immediately find out that it's the Oan Resort.

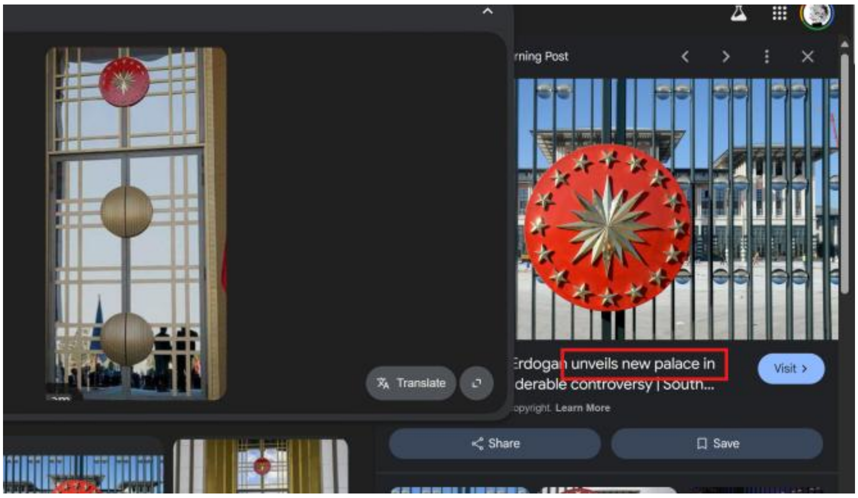


All
Related content
HOME | Oan Resort
The Island in the Image: An OSINT Adventure | by D'Vanshi...

- The coordinates (7.361383772947607, 151.7550374657341) can be found from Google Maps.
- The direction would be almost east (south east) which can be found by opening it up in google earth and changing tilt to around 80 and heading to around 120.

c. OSINT Exercise 3

We can find out the place by reverse searching the image then taking a cutout and reverse searching it again to find similar images linked with the place which leads to an article about the New Palace of President Turkey leading to the actual location.



rning Post
Translate
Erdogan unveils new palace in
derable controversy | South...
opyright. Learn More
Visit >
Share
Save