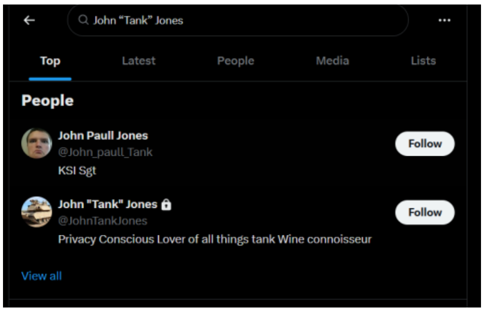
Name: Finding a dork

Type: OSINT, Steganography

Description: We have reason to believe that a malicious actor is currently planning on meeting with a war thunder player they met through social media in an unknown location to share important documents (again). We have no other information about these individuals, only a name: John “Tank” Jones. We need to find out the location so we can put a stop to this!

Solution:

Given we know it’s on social media. Attempt to find the account. You’ll get a hit on twitter by searching the provided name. Given we know they’re a war thunder player, the tank makes it pretty clear which one is the right one.



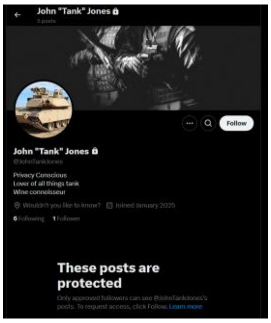
John “Tank” Jones

People

John Paull Jones
@John_paull_Tank
KSI Sgt

John "Tank" Jones
@JohnTankJones
Privacy Conscious Lover of all things tank Wine connoisseur

Going to the profile will tell you almost nothing – because it’s a private account.

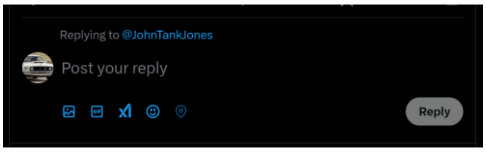


John "Tank" Jones
3 posts

John "Tank" Jones
@JohnTankJones
Privacy Conscious
Lover of all things tank
Wine connoisseur
Wouldn't you like to know? Joined January 2025
6 Following 1 Follower

These posts are protected
Only approved followers can see @JohnTankJones's posts. To request access, click Follow. Learn more

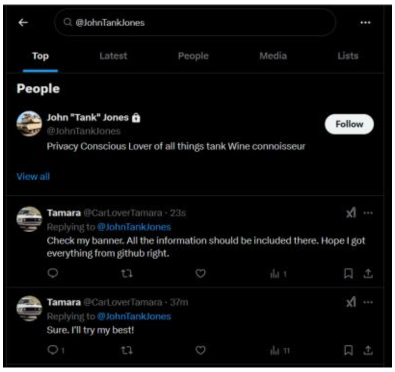
Through twitter, we can search for people John has interacted with as twitter automatically tags people when you reply to them, as seen below:



Replying to @JohnTankJones

Post your reply

Therefore, by simply searching his @, “@JohnTankJones” in the search bar we can see posts sent to him by other people, who don’t have their accounts private:

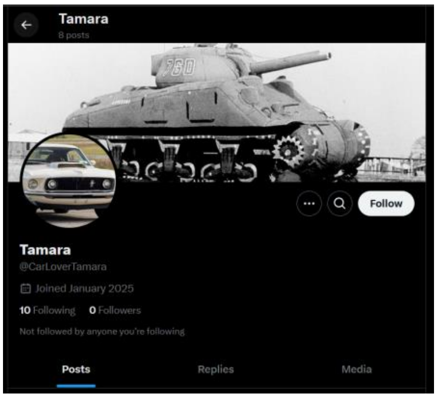


John "Tank" Jones @JohnTankJones
Privacy Conscious Lover of all things tank Wine connoisseur

Tamara @CarLoverTamara · 23s
Replying to @JohnTankJones
Check my banner. All the information should be included there. Hope I got everything from github right.

Tamara @CarLoverTamara · 37m
Replying to @JohnTankJones
Sure. I'll try my best!

This leads us to our second account, Tamara – who appears to have sent two tweets to John.

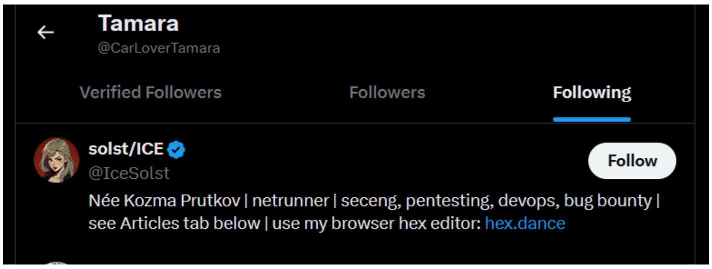


Tamara
@CarLoverTamara
Joined January 2025
10 Following 0 Followers
Not followed by anyone you're following

From these messages we know two things:

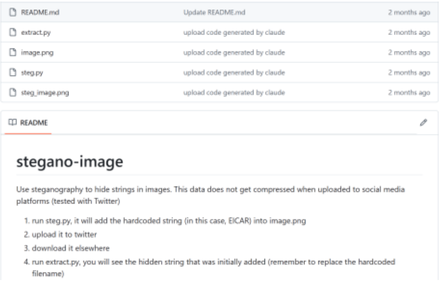
- There's something in her "Banner" – likely the tank on her twitter banner
- She used something from github

Looking at her follower list, the account that most stands out (and is last followed) is this one:



solst/ICE @IceSolst
Née Kozma Prutkov | netrunner | seceng, pentesting, devops, bug bounty | see Articles tab below | use my browser hex editor: hex.dance

Checking this person's github reveals a few projects, notably "stegano-image" – which sounds like it might be relevant.



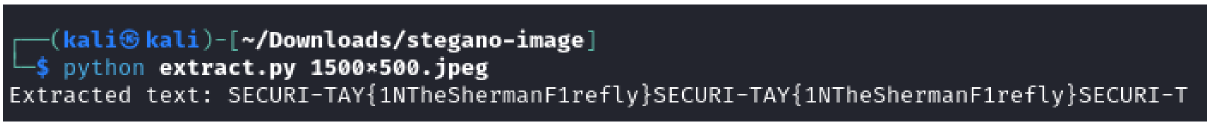
README.md	Update README.md	2 months ago
extract.py	upload code generated by claude	2 months ago
image.png	upload code generated by claude	2 months ago
steg.py	upload code generated by claude	2 months ago
steg_image.png	upload code generated by claude	2 months ago

stegano-image

Use steganography to hide strings in images. This data does not get compressed when uploaded to social media platforms (tested with Twitter)

1. run steg.py, it will add the hardcoded string (in this case, EICAR) into image.png
2. upload it to twitter
3. download it elsewhere
4. run extract.py, you will see the hidden string that was initially added (remember to replace the hardcoded filename)

If we download the tool, then save the profile banner, and then run the extraction.py, it should give us the flag:



```
┌──(kali㉿kali)-[~/Downloads/stegano-image]
└─$ python extract.py 1500×500.jpeg
Extracted text: SECURI-TAY{1NTheShermanF1refly}SECURI-TAY{1NTheShermanF1refly}SECURI-T
```

FLAG:

SECURI-TAY{1NTheShermanF1refly}