Final Project CYT215 IT Forensics
Weight 18%

Total 100 Marks

As a forensic analyst, your assignment is to address the three forensic challenges outlined below. You are required to document your findings for each respective part in a comprehensive report. Ensure that each section is clearly labeled and separated with titles and subtitles. Additionally, include a table of contents in the main report to facilitate easy navigation.

Part 1 – Redline Endpoint Forensics Challenge - 40 Marks
Part 2 – Steganography - 30 Marks
Part 3 - Blockchain Forensics and OSINT – 30 Marks

Note – All three parts should be in one document (either below in this document or a brand-new document).

Follow the following naming convention: CYT215-Final Project - Student Name & ID

Part 1 – Redline Endpoint Forensics Challenge - 40 Marks

As a member of the Security Blue team: Your assignment is to analyze a memory dump using Redline and Volatility tools. Your goal is to trace the steps taken by the attacker on the compromised machine and determine how they managed to bypass the Network Intrusion Detection System "NIDS". Your investigation will involve identifying the specific malware family employed in the attack, along with its characteristics. Additionally, your task is to identify and mitigate any traces or footprints left by the attacker.

Deliverable – Answer the following questions:

1. What is the name of the suspicious process? – 5 marks
2. What is the child process name of the suspicious process? – 5 marks
3. What is the memory protection applied to the suspicious process memory region? – 5 marks
4. What is the name of the process responsible for the VPN connection? – 5 marks
5. What is the attacker's IP address? – 5 Marks
6. Based on the previous artifacts. What is the name of the malware family? – 5 Marks
7. What is the full URL of the PHP file that the attacker visited? – 5 marks
8. What is the full path of the malicious executable? – 5 Marks

Steps

- Go to the challenge https://cyberdefenders.org/blueteam-ctf-challenges/106#nav-questions
- Create an account and Login.
- Download the Challenge. Uncompress the challenge (pass: cyberdefenders.org).
- Answer the 8 challenge questions. Tool Used: Volatility.
- Show complete screenshots of all your work.

- The memory file will also be provided to you on blackboard in a ZIP File.

- Like the labs, you can refer to the below write ups and replicate the steps in your own machine.

- https://medium.com/@ahmad77.omari77/cyberdefenders-readline-af3822a3aa1d

- https://medium.com/@manasmbellani/cyberdefenders-org-redline-cf3f7318d3cb

- Show your genuine signs of your work is done on your machine. This includes:
- Screenshots that show your desktop background with Date/Time.
- Show a pop-up bx that shows “your name + IP”.

Part 2 – Steganography - 30 Marks

You are part of a cybersecurity training program that simulates real-world scenarios. For this project, you will take on two roles: a red teamer and a forensic analyst.

Red Team Exercise. – 10 Marks

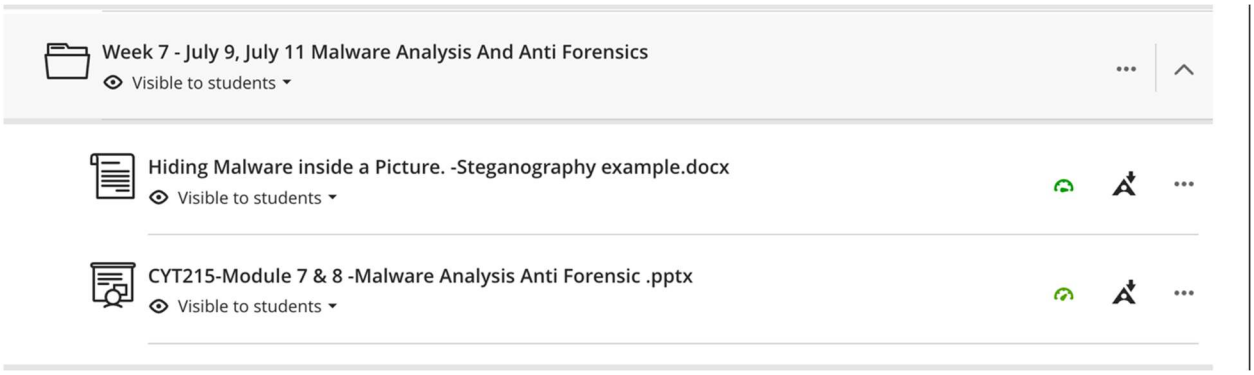
Mission Briefing: As a member of the red team, your mission is to covertly transmit sensitive information to a teammate without it being detected by potential adversaries. To achieve this, you will use steganography to hide a text file containing a secret message within an image of your choice.

Forensic Analyst Exercise – 20 Marks

Mission Briefing: Now, assume the role of a forensic analyst. Your mission is to detect and extract hidden information from the same image in Part 1.

This is like the example shown in class.

Refer to following notes from blackboard as a guide.



Document each step.

Part 3: Blockchain Forensics and OSINT – 30 Marks

You are a Forensic analyst and you have been assigned to track cryptocurrency wallets, analyze transaction histories, and use Open-Source Intelligence (OSINT) techniques to identify a public figure's social media profiles and occupation.

Part 1: Introduction to .sol and. eth Domains

Background:

- .sol domains are used in the Solana blockchain ecosystem.
- . eth domains are used in the Ethereum blockchain ecosystem.

Given:

- .sol domain: gautamgg.sol
- . eth domain: gautamgg.eth

Part 2: Tracking Cryptocurrency Wallets

Identify Wallet Addresses: - 15 Marks

- Use blockchain explorers like Solana Explorer and Etherscan to find the wallet addresses associated with the given domains.
- Solana Explorer: https://explorer.solana.com/
- Etherscan: https://etherscan.io/
- Analyze Transaction History:
- Track the transaction history of the identified wallet addresses.
- Note down significant transactions, including dates, amounts, and recipient addresses.

Part 3: Open-Source Intelligence (OSINT) – 15 Marks

Finding the Identity of the Public Figure: - 5 Marks

- Use the transaction history to identify any patterns or links to known entities.
- Search for any mentions of the wallet addresses or transaction details in public forums, social media, or news articles.

Social Media Profiles: - 5 Marks

- Use social media platforms (Twitter, LinkedIn, Facebook, etc.) to find profiles associated with the public figure.
- Look for usernames, handles, or email addresses linked to the wallet addresses.

Occupation: - 5 Marks

- Investigate the public figure's occupation through their social media profiles, public records, and professional networking sites.

Tools and Resources:

Blockchain Explorers:

- Solana Explorer: https://explorer.solana.com/
- Etherscan: https://etherscan.io/

OSINT Tools:

- Google Search: https://www.google.com/
- Twitter Search: https://twitter.com/search
- LinkedIn: https://www.linkedin.com/
- Facebook: https://www.facebook.com/
- Have I Been Pwned: https://haveibeenpwned.com/

Document your findings into a report.

Reminders

- Submit your report name: CYT215-FinalProject-Student Name & ID
- Submit via the BB relevant link ONLY. NO submission via email please. Be sure to submit the final version file ONLY.
- NOTE – THIS IS AN INDVIDUAL REPORT AND MUST BE IN YOUR OWN WORDS. YOUR REPORT SHOULD BE YOUR OWN.
- Show your genuine signs of your work is done on your machine. This includes:
- Screenshots that show your desktop background with Date/Time (where applicable)
- Show a pop-up bx that shows “your name + IP” (where applicable)

Please follow and abide by the Seneca Academic Integrity policy –

Academic Integrity at Seneca

What is Academic Integrity?

The International Center for Academic Integrity defines academic integrity as a commitment, even in the face of adversity, to six Fundamental Values of Academic Integrity: honesty, trust, fairness, respect, responsibility, and courage. From these values flow principles of behavior that enable academic communities to translate ideals into action.

Why does Academic Integrity Matter?

When each member of the Seneca Community embraces and incorporates these values into our teaching, learning and working environments, then we are able to maintain the college's reputation as a leading educational institution and to graduate high quality students who are poised to succeed in their careers and contribute meaningfully to society.

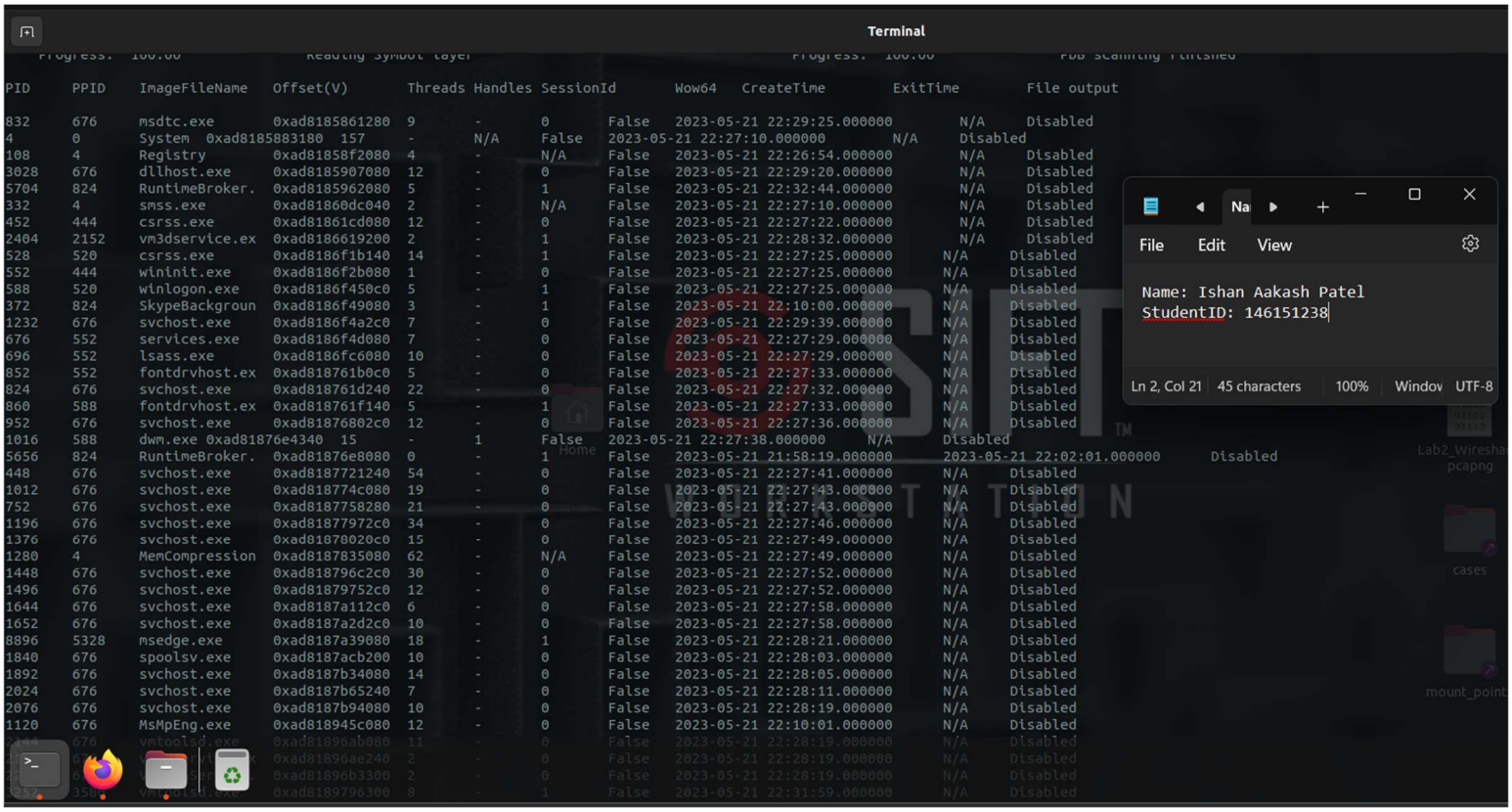
Academic Integrity - Student Resources

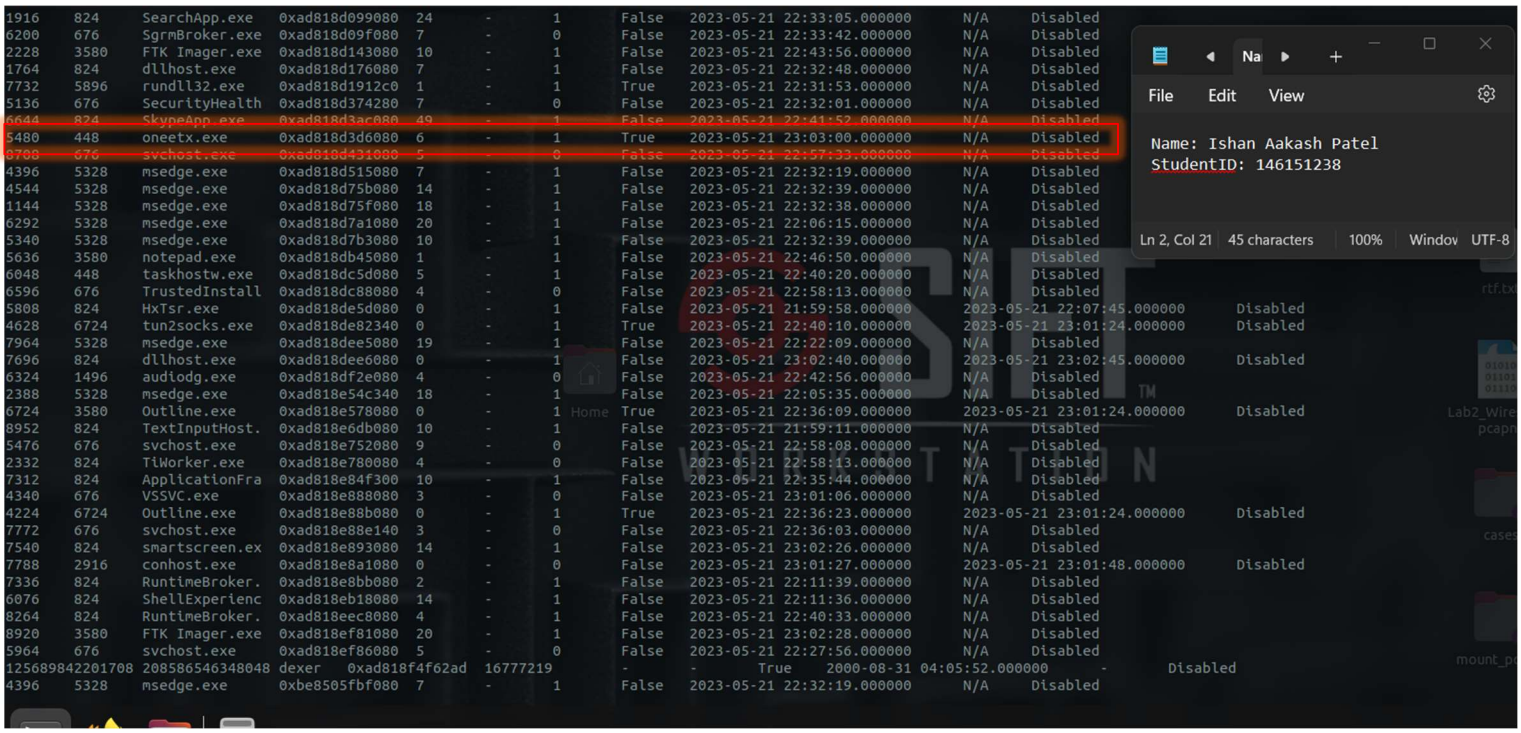
You may start the report below or in a brand-new document.

----------Report Starts Below----------

Part – 1 Redline Endpoint Forensics Challenge

1. **What is the name of the suspicious process? – 5 marks**



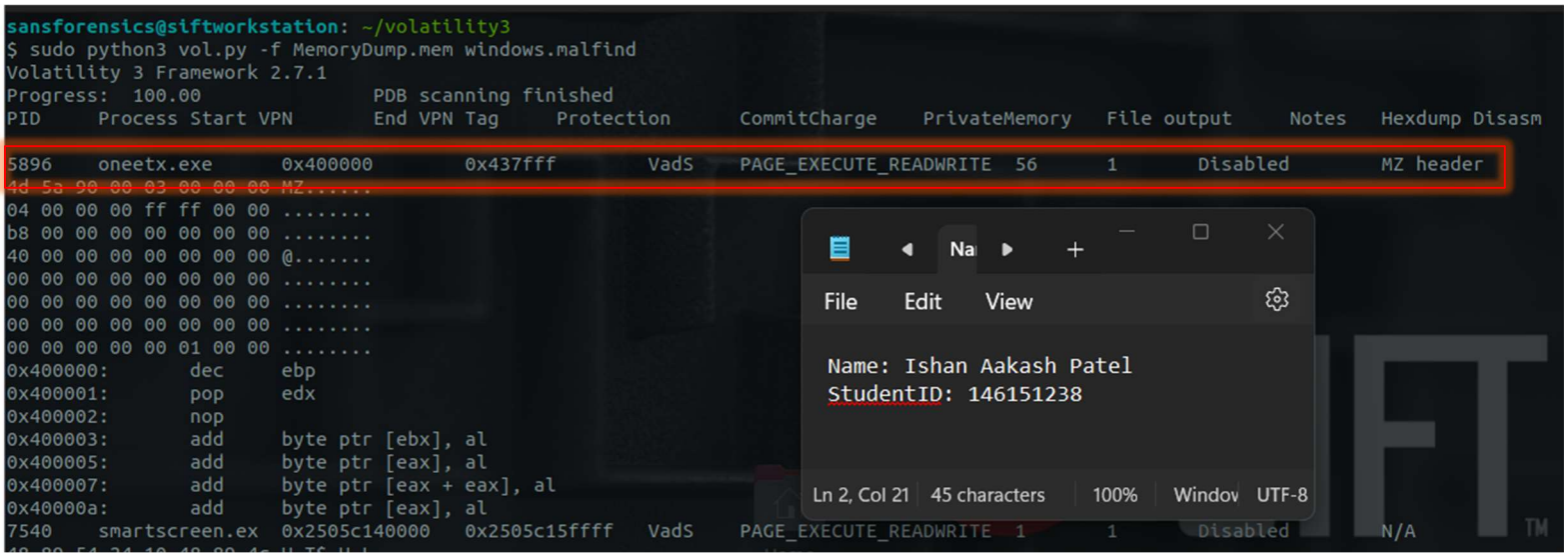


The command used above is :

Sudo python3 vol.py -f MemoryDump.mem windows.pslist

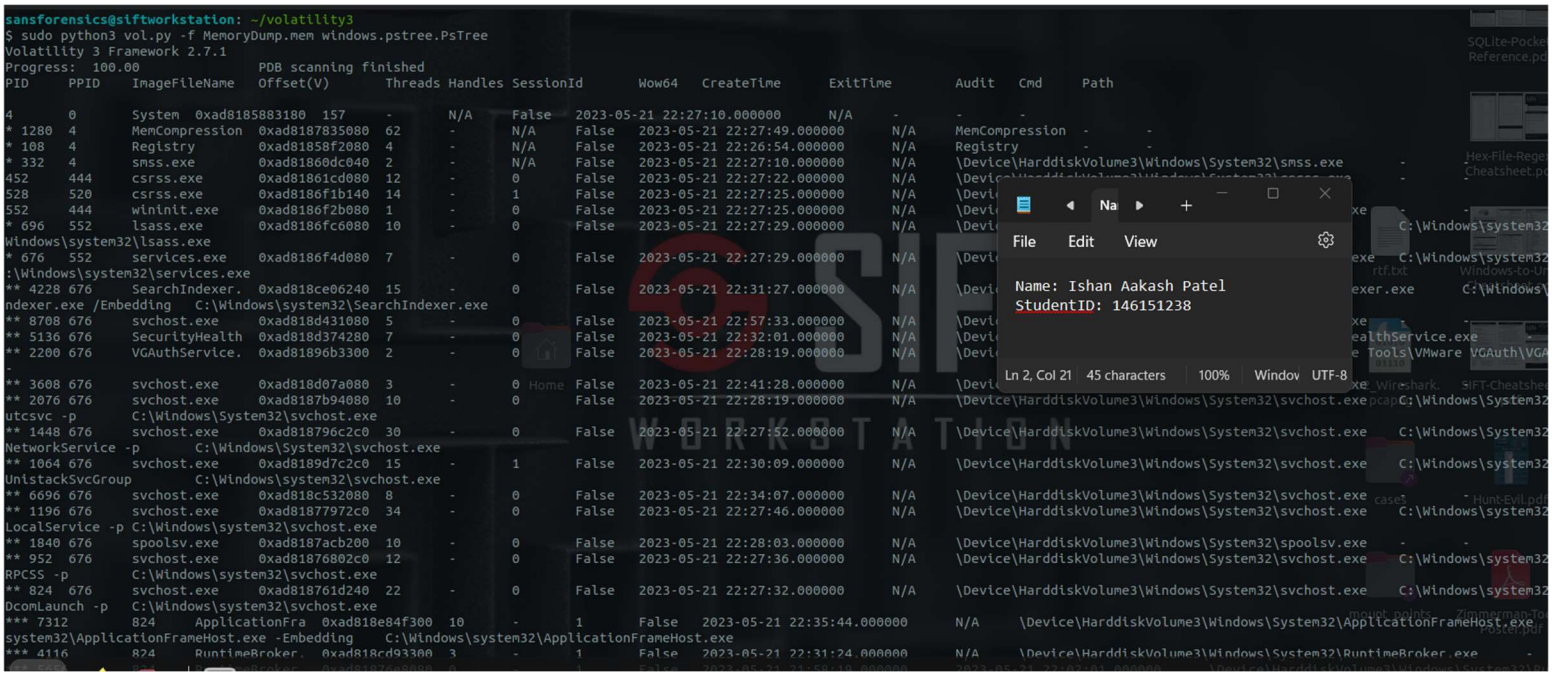
We had a doubt on oneetx.exe, So to check that we will use the malfind function of volatility.

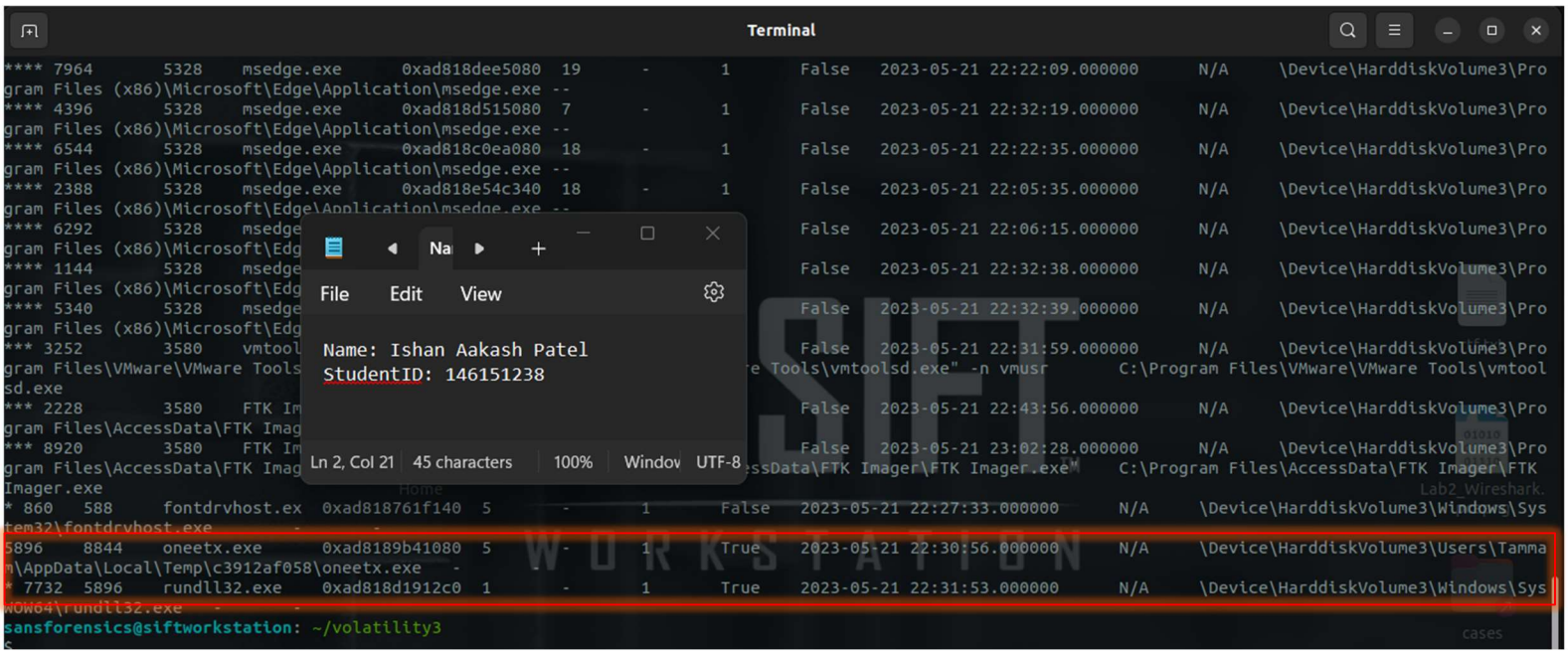
Command : Sudo python3 vol.py -f MemoryDump.mem windows.malfind



Answer : oneetx.exe

2. **What is the child process name of the suspicious process? – 5 marks**

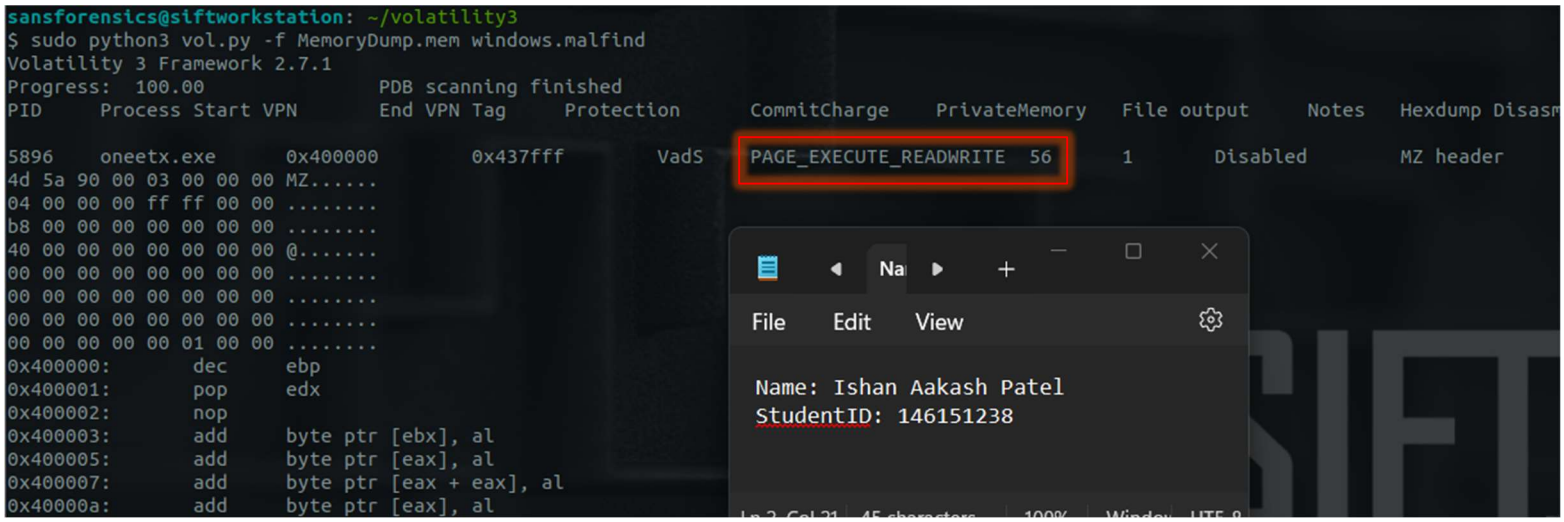




Command : Sudo python3 vol.py -f MemoryDump.mem windows.pstree.PsTree

Answer : rundll32

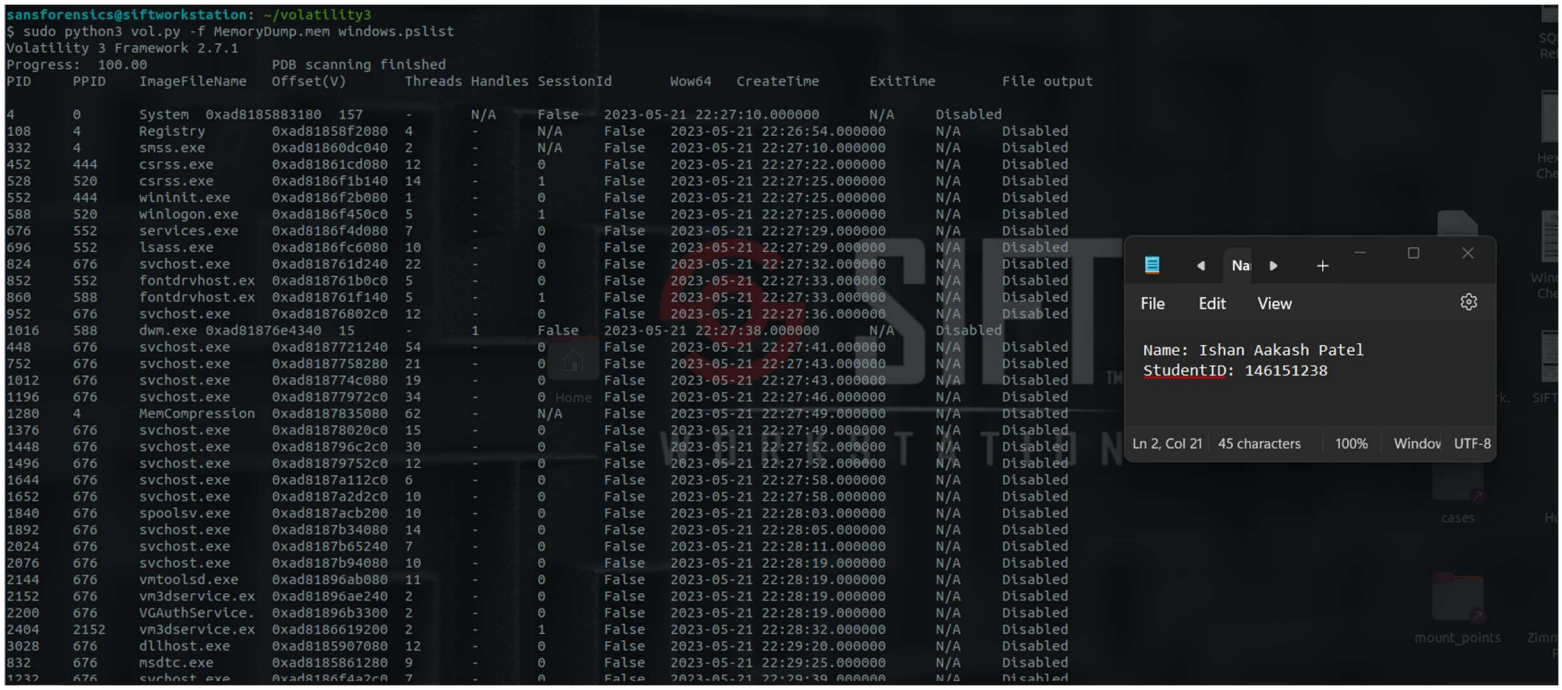
3. **What is the memory protection applied to the suspicious process memory region? – 5 marks**

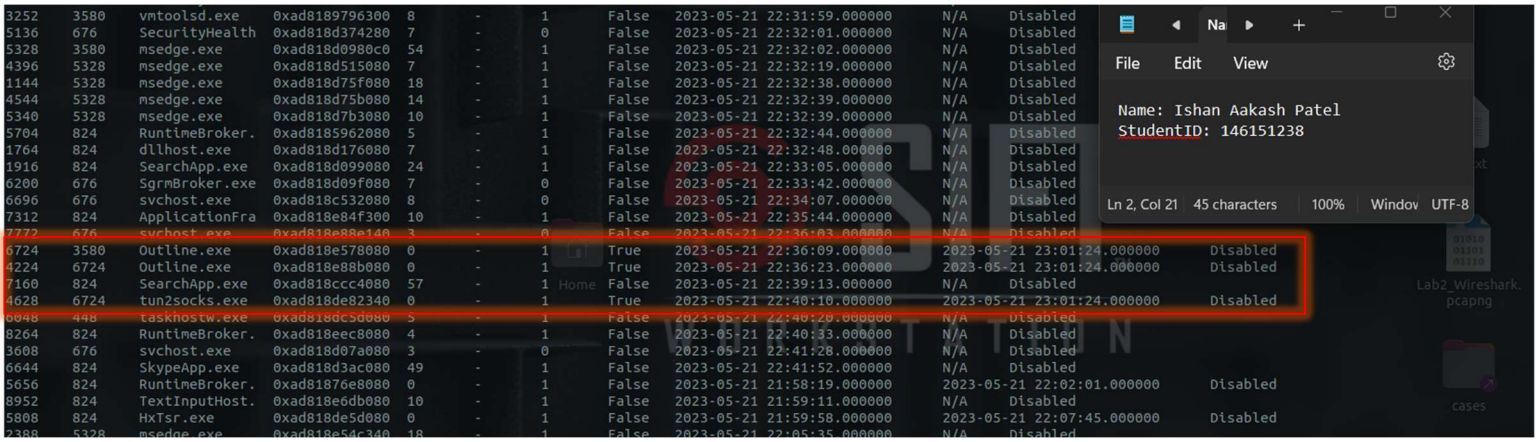


Command : Sudo python3 vol.py -f MemoryDump.mem windows.malfind

Answer : PAGE_EXECUTE_READWRITE

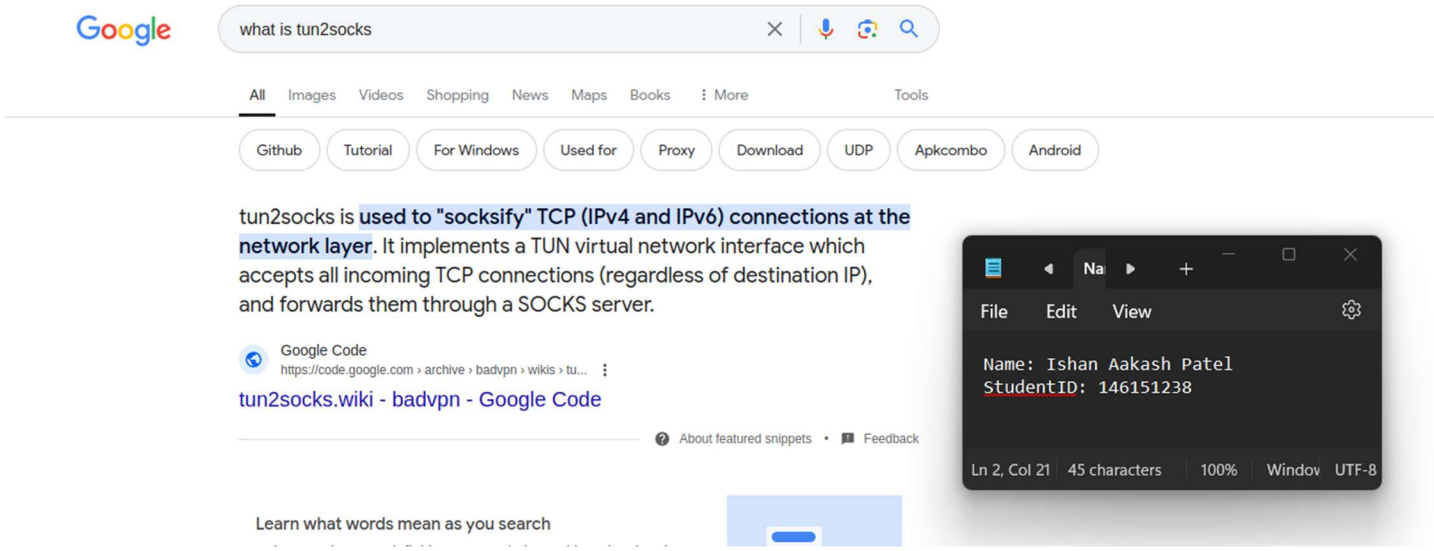
4. **What is the name of the process responsible for the VPN connection? – 5 marks**





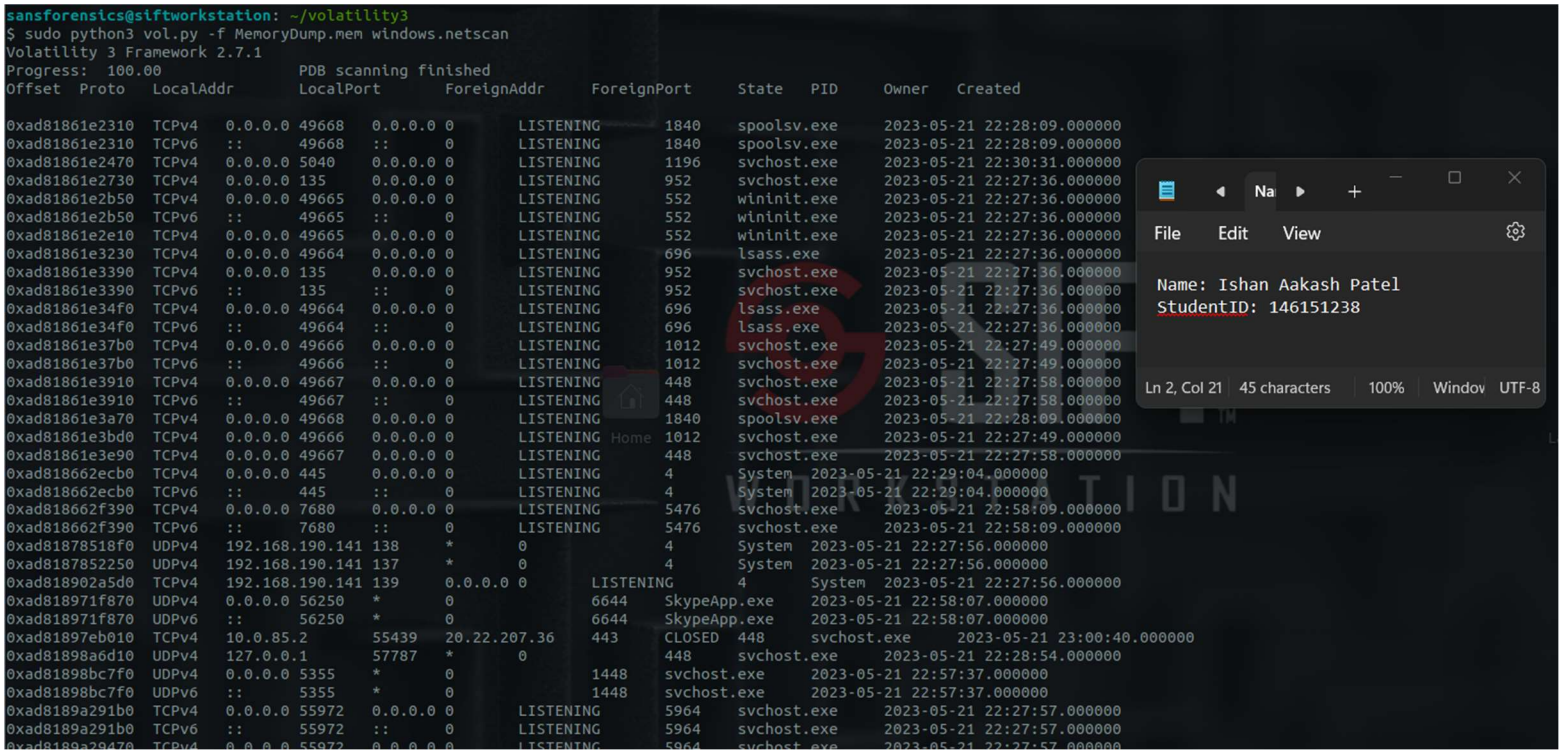
Command : Sudo python3 vol.py -f MemoryDump.mem windows.pslist

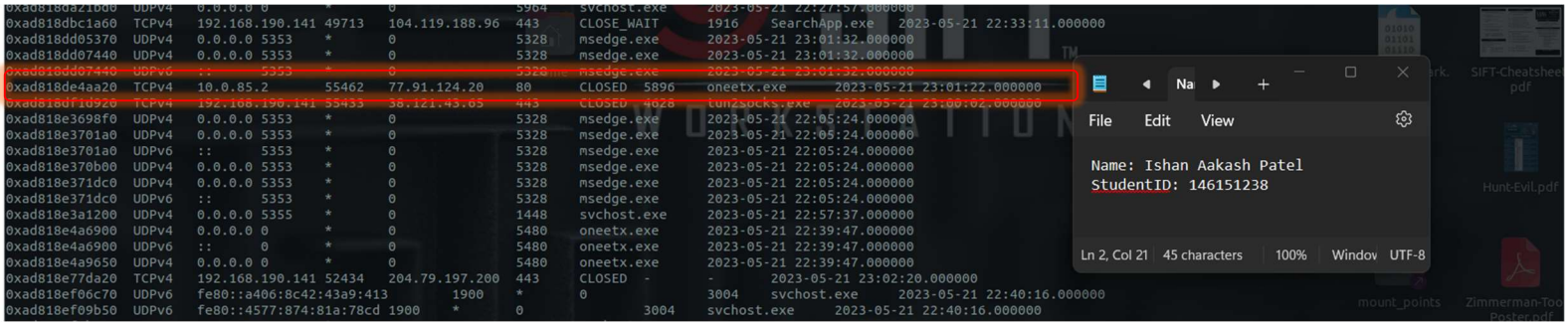
Tun2socks is the child process of outlook.exe



Answer : tun2socks.exe

5. **What is the attacker's IP address? – 5 Marks**

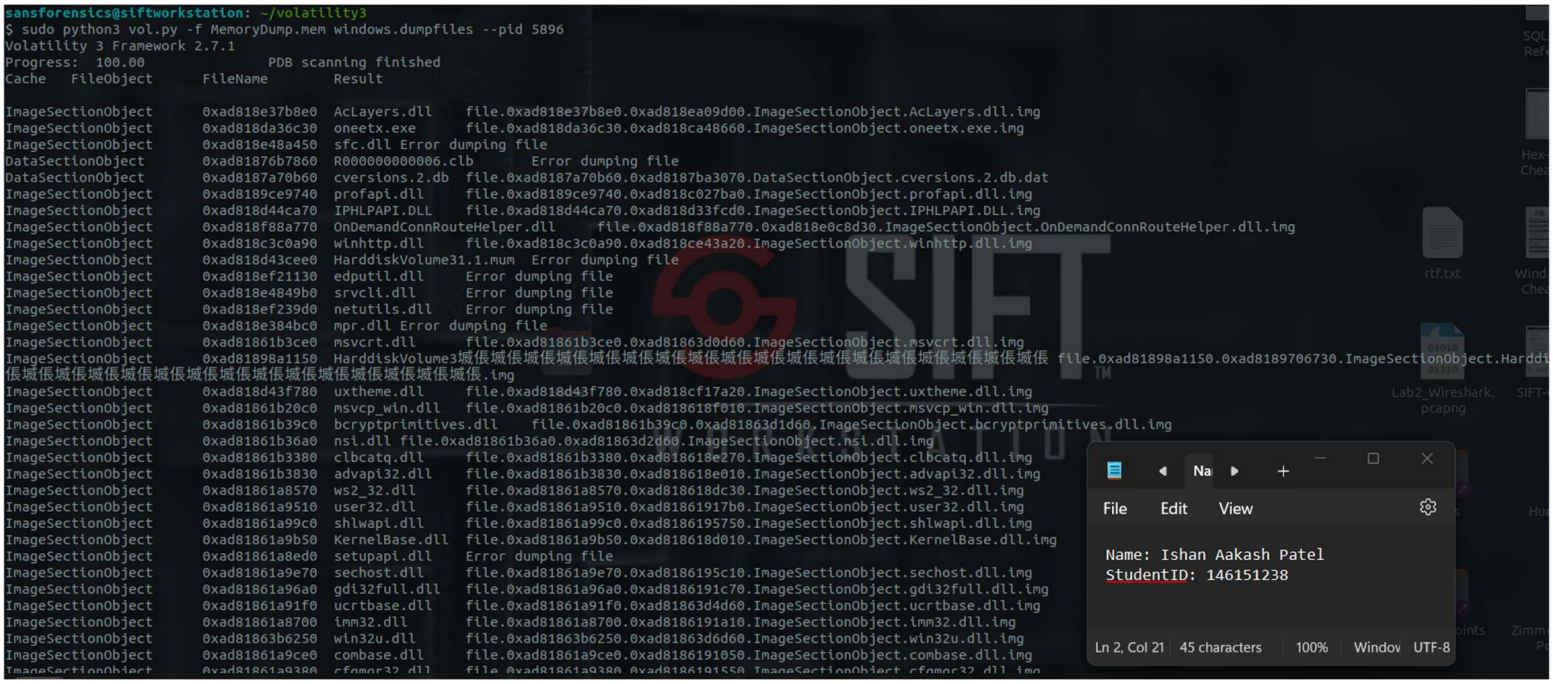




Command : Sudo python3 vol.py -f MemoryDump.mem windows.netscan

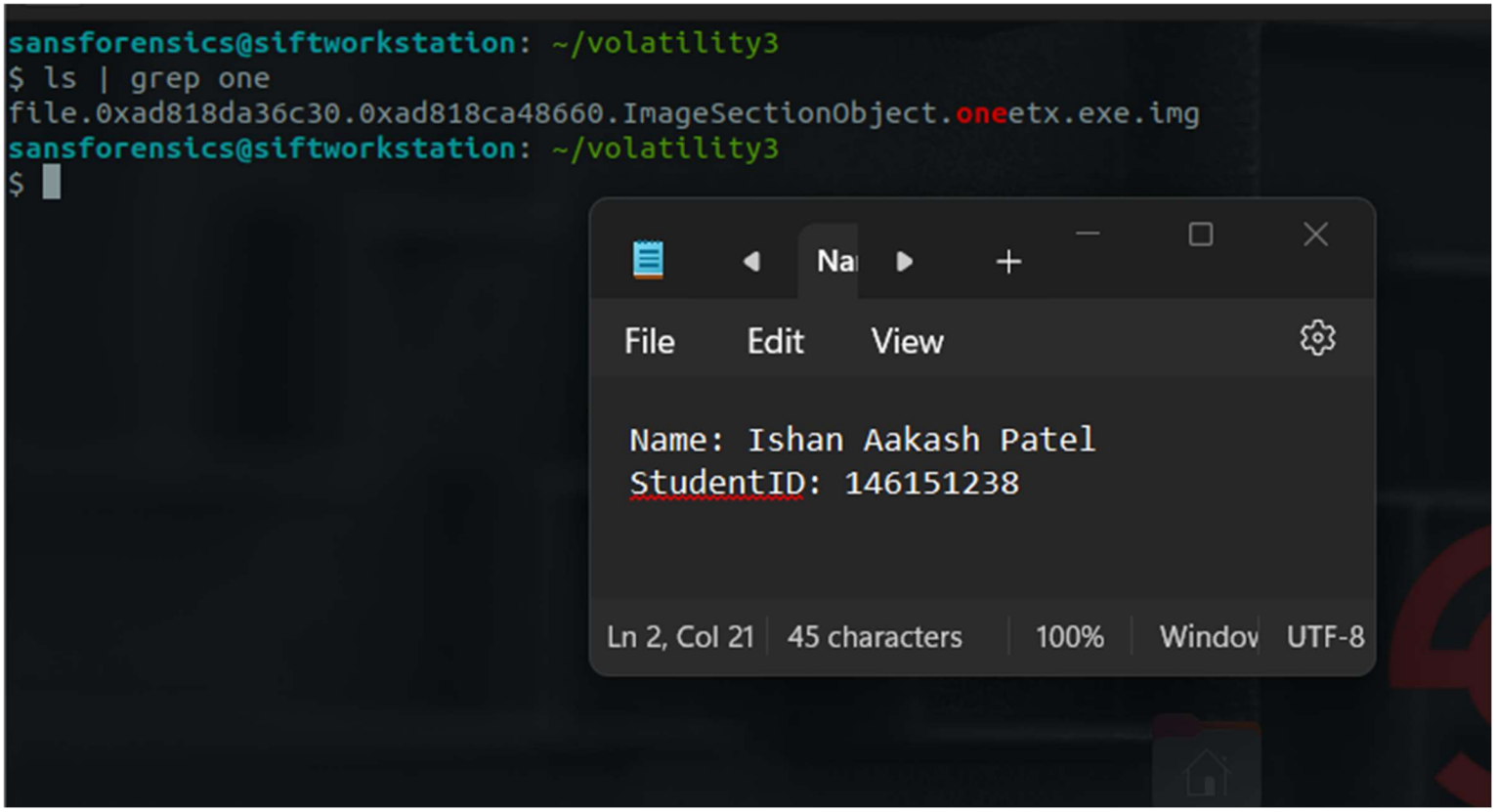
Answer : 77.91.124.20

6. **Based on the previous artifacts. What is the name of the malware family? – 5**

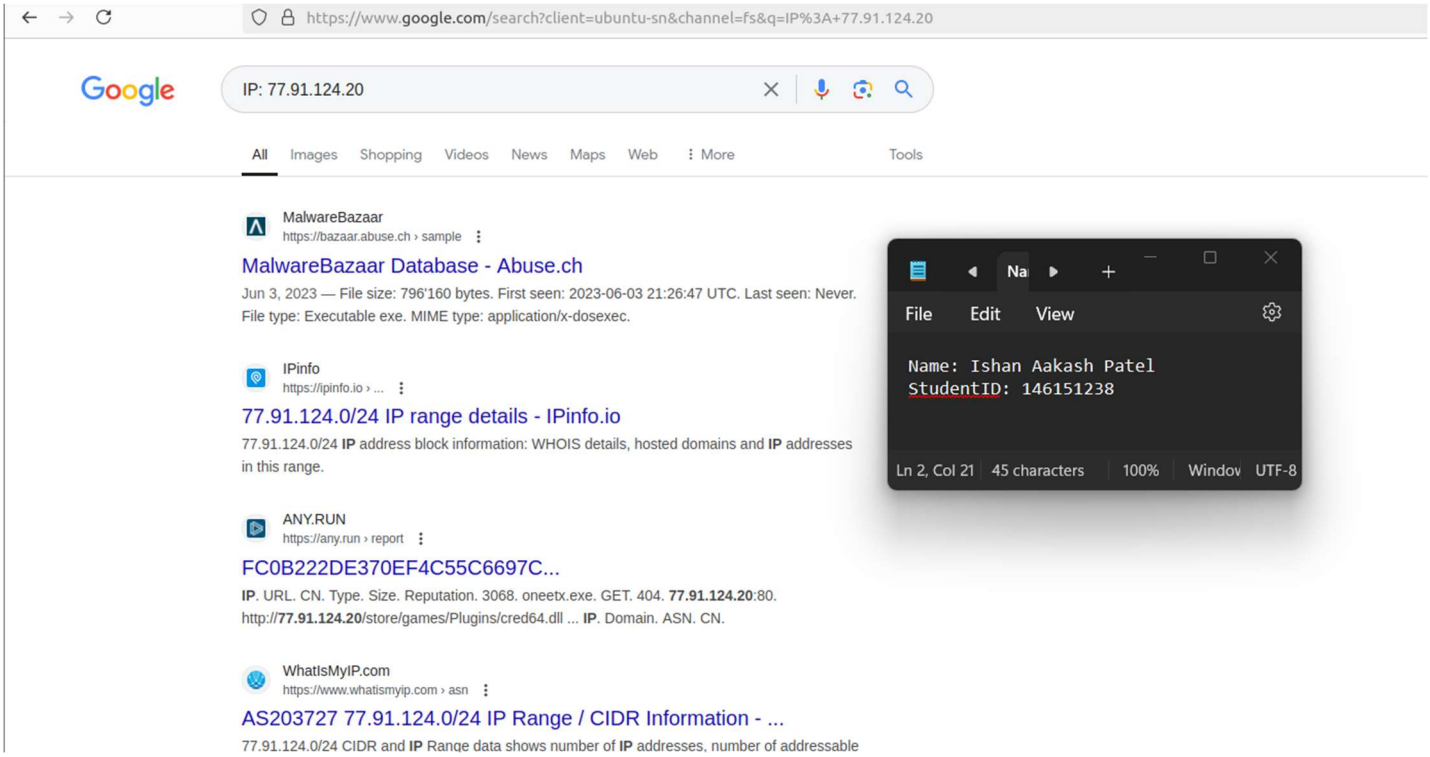


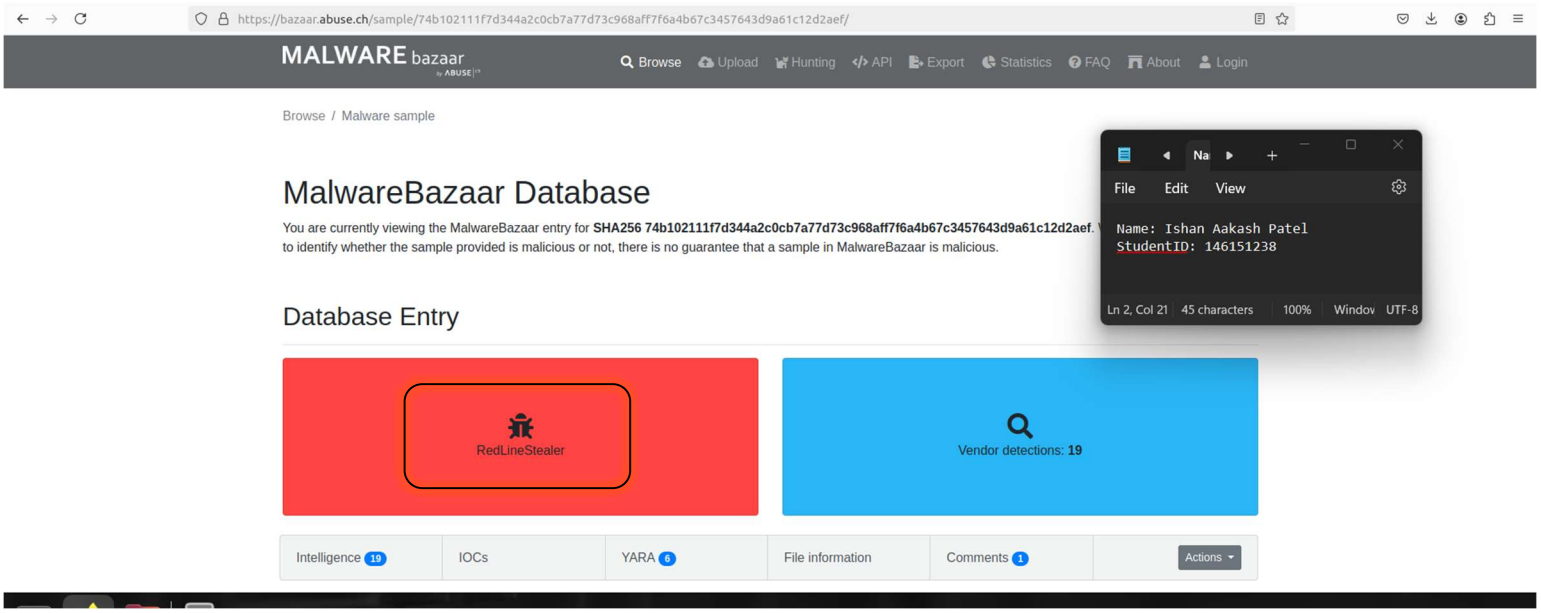
Marks

Command (To dumpfiles) : Sudo python3 vol.py -f MemoryDump.mem windows.dumpfiles –pid 5896



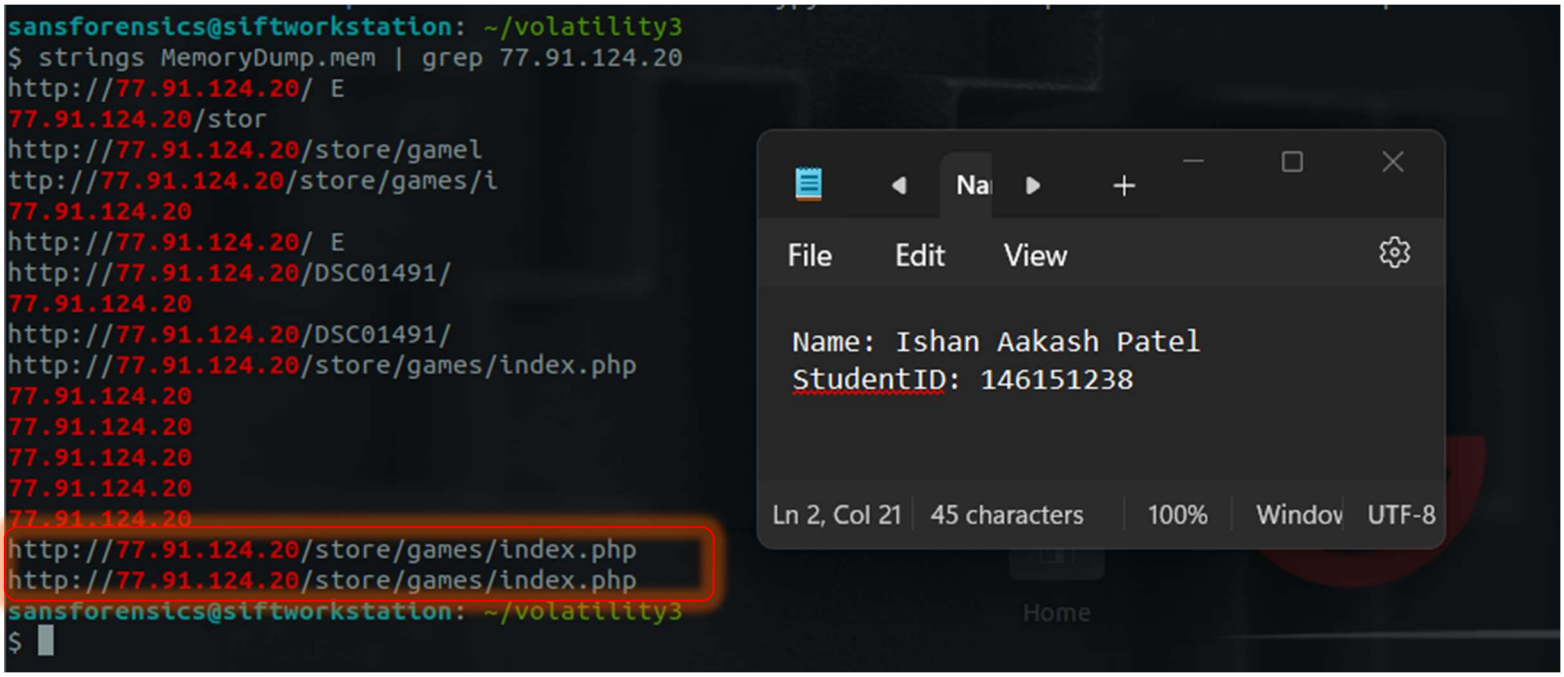
Found the malicious file, now we can check it in VirusTotal
But on virus Total the name wasn't specified and we had to search on google for any links and we found the link of MalwareBazaar.





Answer : RedLine Stealer

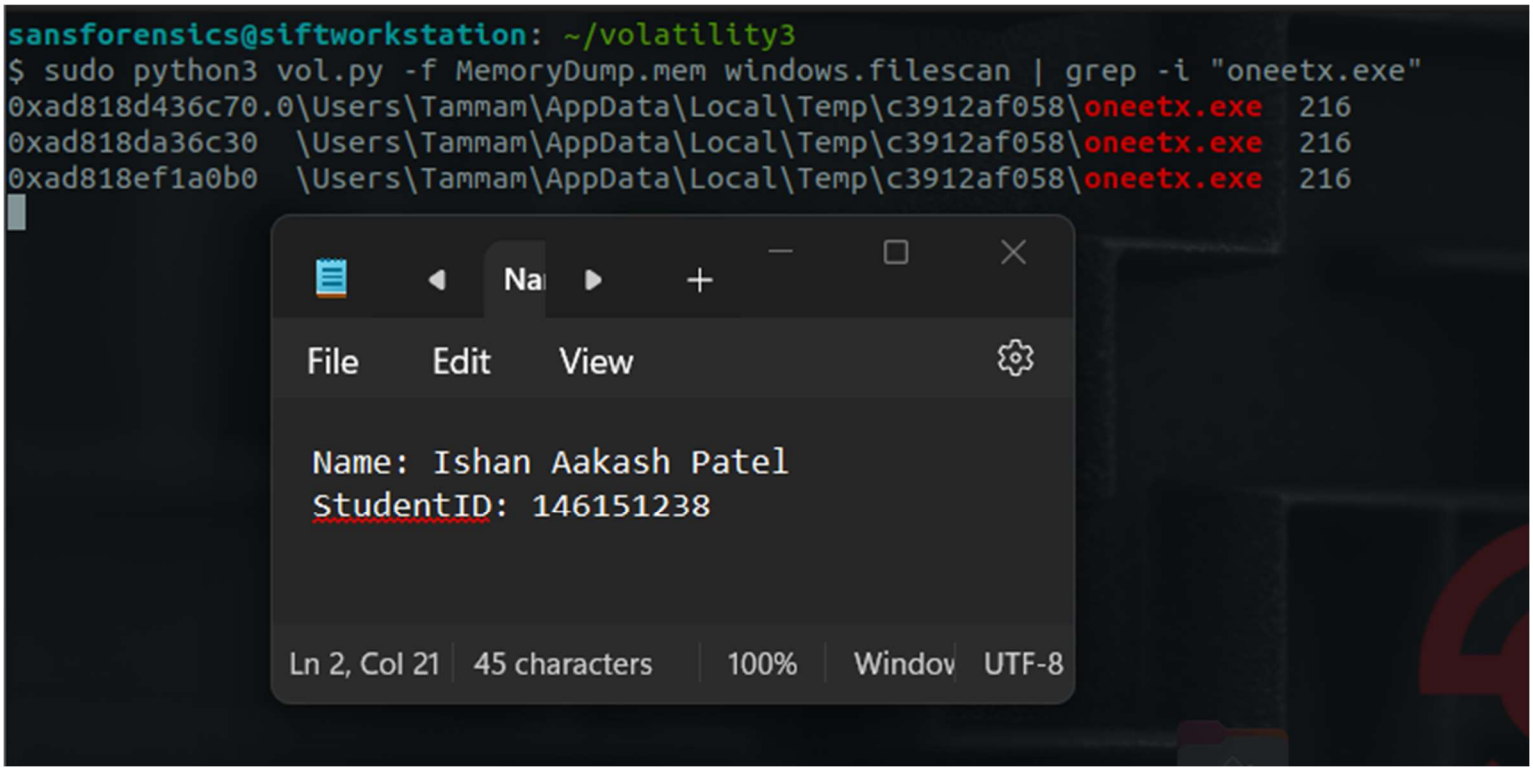
7. **What is the full URL of the PHP file that the attacker visited? – 5 marks**



Command : strings MemoryDump.mem | grep 77.91.124.20

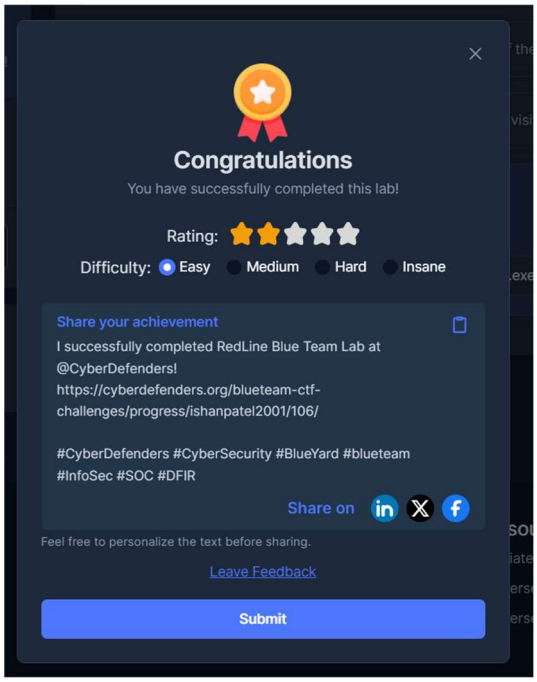
Answer : http://77.91.124.20/store/games/index.php

8. **What is the full path of the malicious executable? – 5 Marks**



Command : Sudo python3 vol.py -f MemoryDump.mem windows.filescan | grep -I "oneetx.exe"

Answer : C:\Users\Tammam\AppData\Local\Temp\c3912af058\oneetx.exe



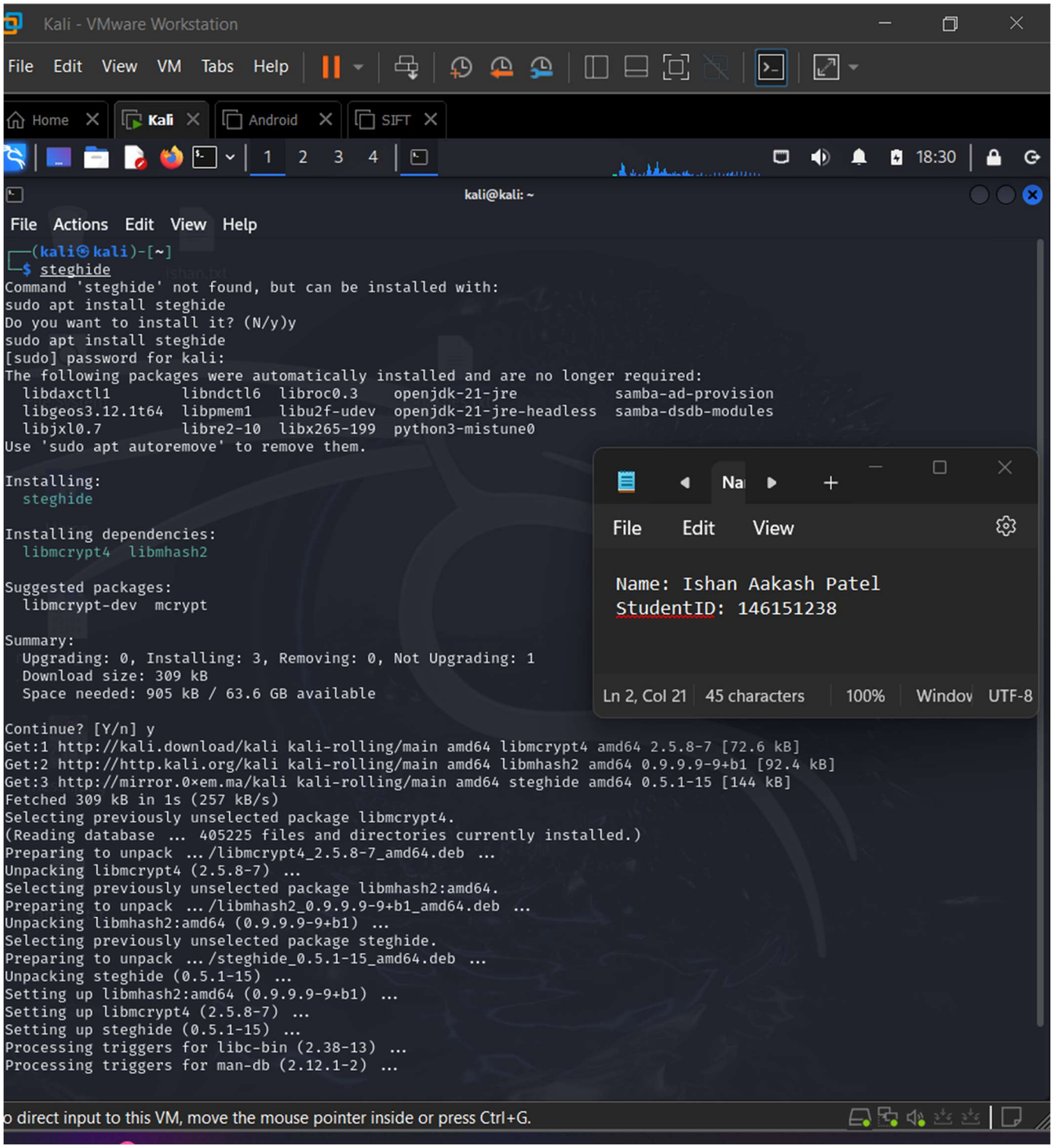
Challenge Completed...

Part – 2 Steganography

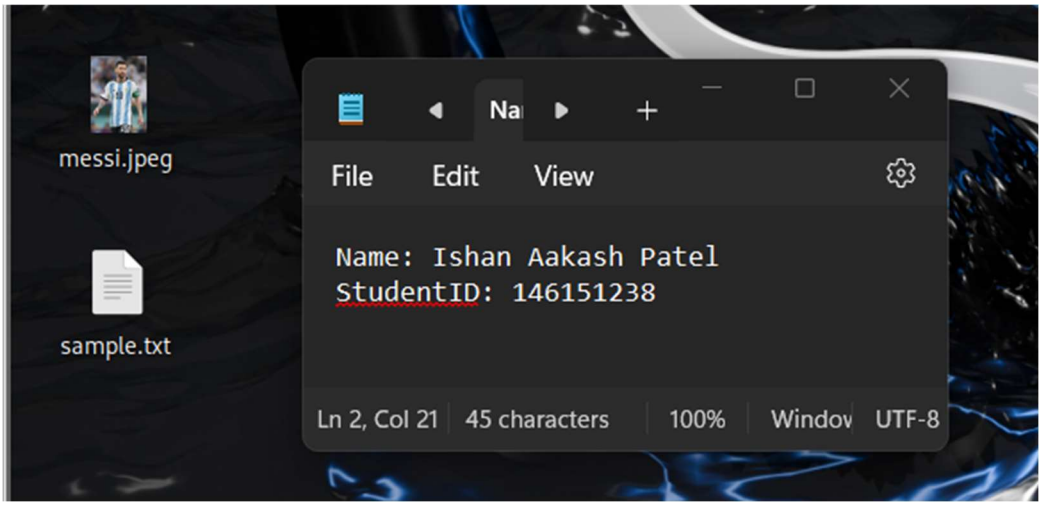
Task – 1

Embedding malware into an image...

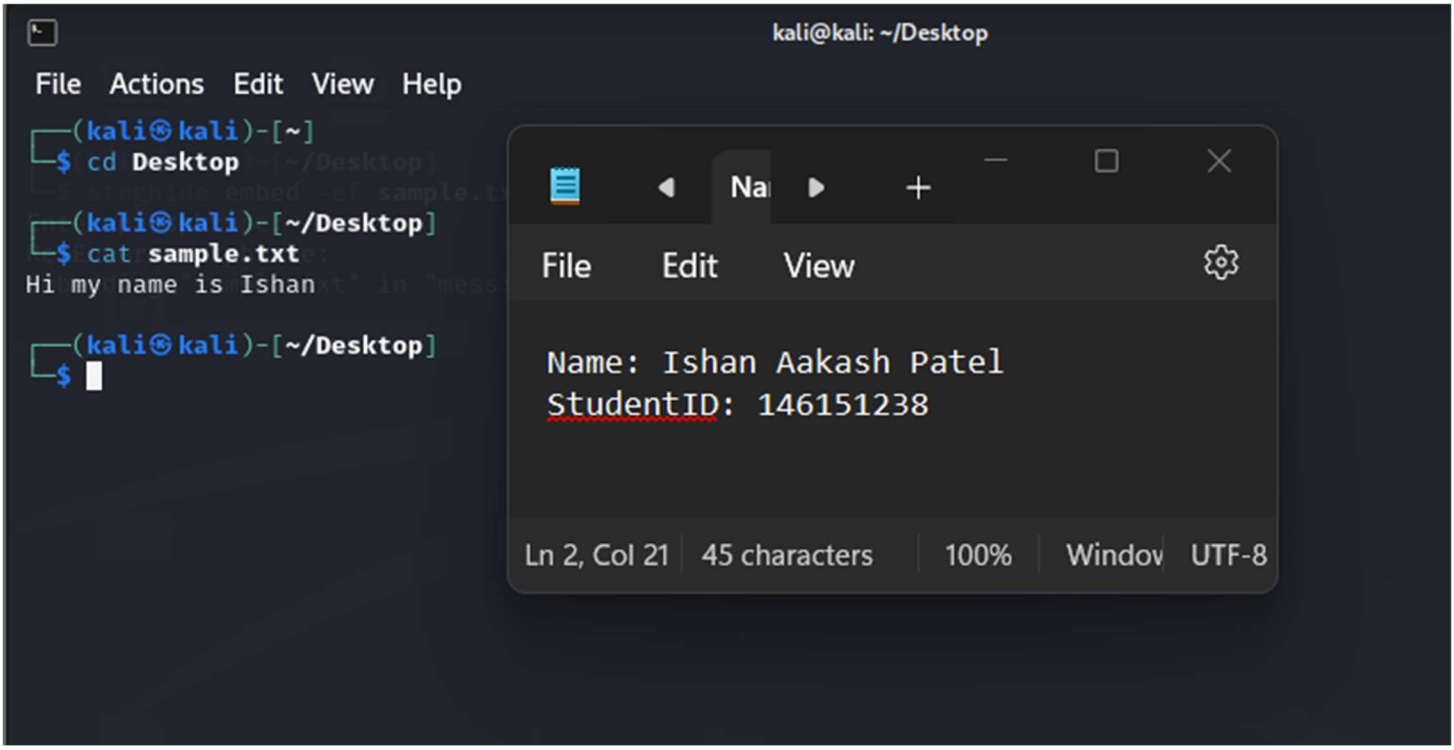
Step 1 - Install Steghide

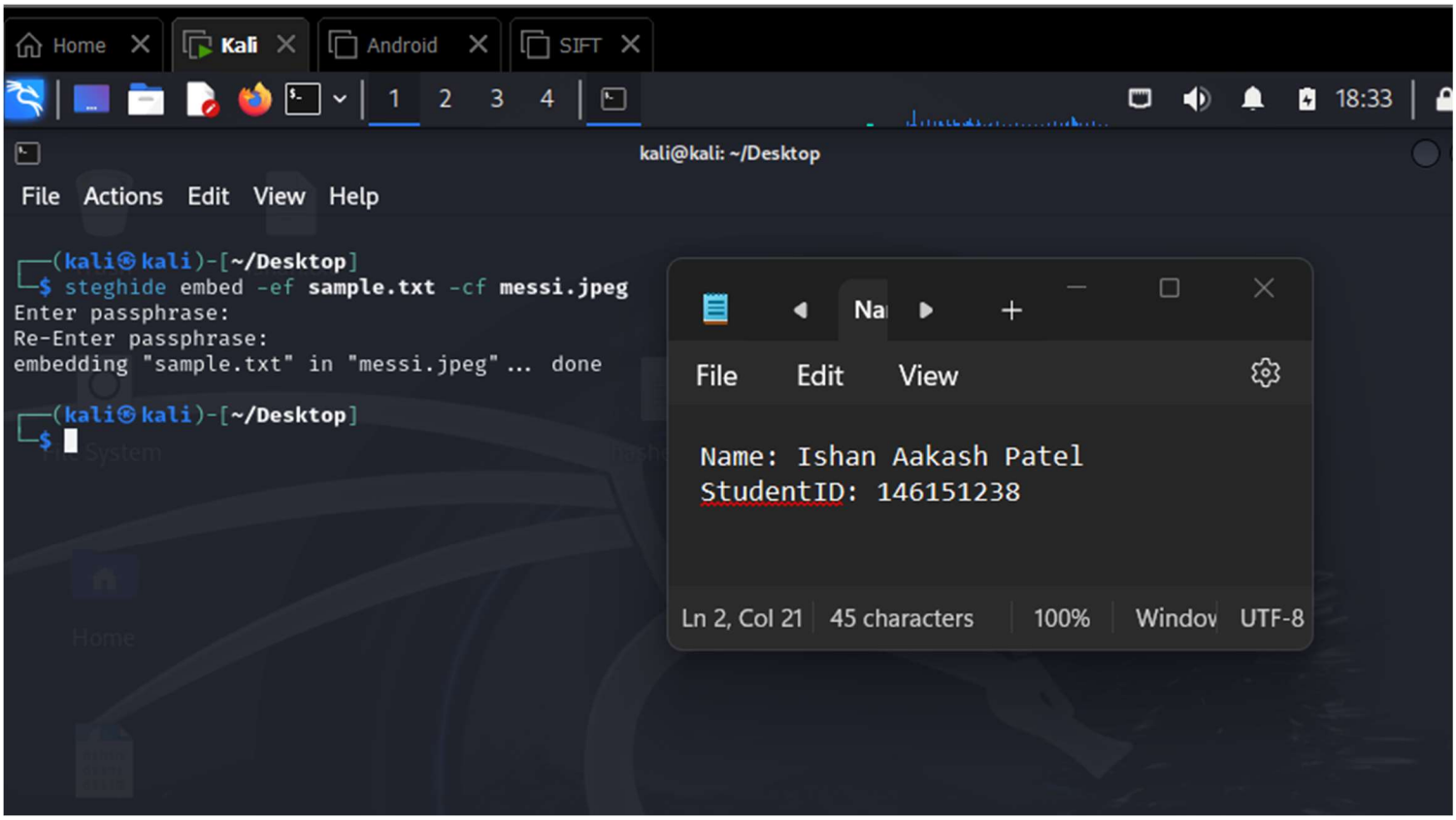


Sample try...



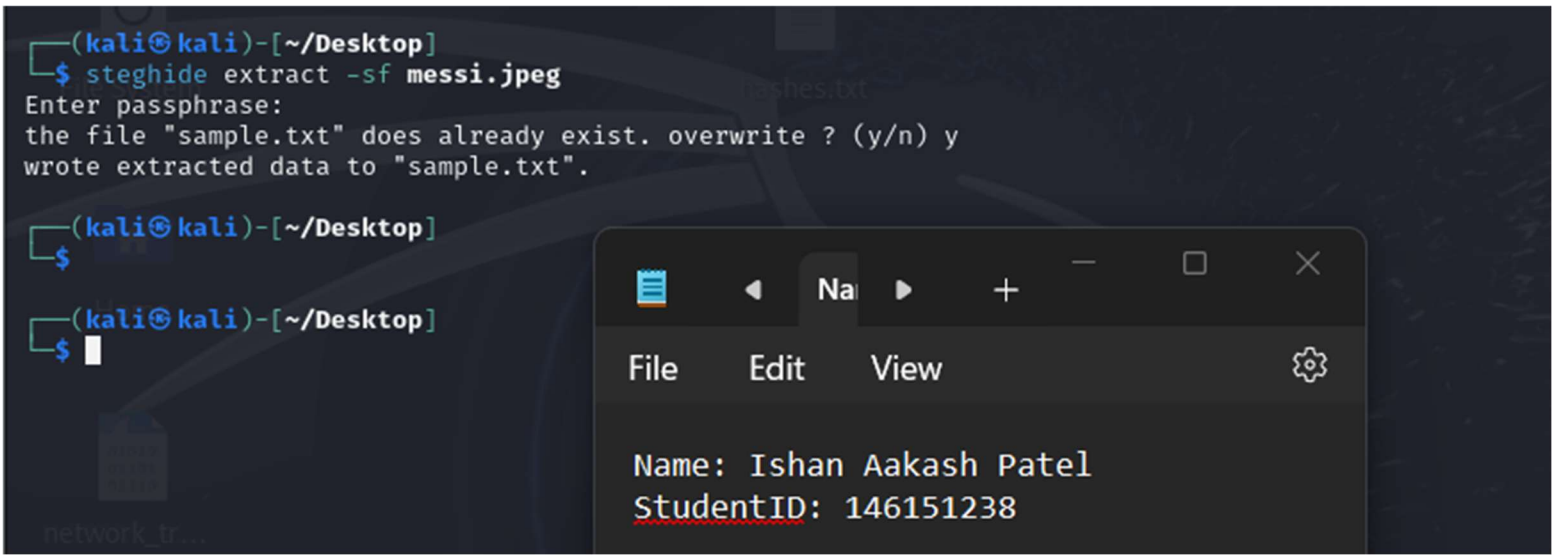
Sample.txt





Command : steghide embed -ef sample.txt -cf messi.jpeg

Now we will extract it....

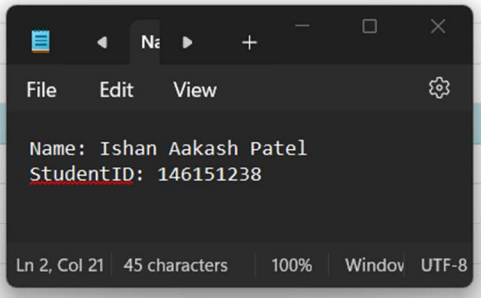


Command : steghide extract -df messi.jpeg

Now we will try using a real malware...

Intelligence 12 | IOCs | YARA | File information | Comments | Actions

SHA256 hash:	8d00031eb1f2c8f1c716ac21960328454b7dc000045903f01a737fe9086a2511
SHA3-384 hash:	b8e34eef62cc236241ece203b92b27cc02eb46e5f8b39b064f676da5ea5c081a6d66bbe20b6d34bd0a5602a55fd6625f
SHA1 hash:	8a196958a5e8b96b019b941525439faac77923c0
MD5 hash:	8fa2b75f9216e639117fd227300e4aa7
humanhash:	vegan-one-hamper-oven
File name:	271141082232885603.bat
Download:	download sample
Signature	StrelaStealer Alert
File size:	2'150 bytes
First seen:	2024-07-15 06:36:56 UTC
Last seen:	*Never*
File type:	bat
MIME type:	text/plain
ssdeep	24:YqpOB8EwPpD+e8VMw7kNwO/78zWNej867A4r3qRESL4rie6t4X4YYDex0xYBJIYV:9p3CcFsJWC72DGN6XzLLPXzLLAB
TLSH	T1FD4108EE12344F3A2D672ACA2149F9552052AE313FA4D4DEF918D076C0FA4FD268C973
Reporter	cocaman



Got the malware from malware bazar...

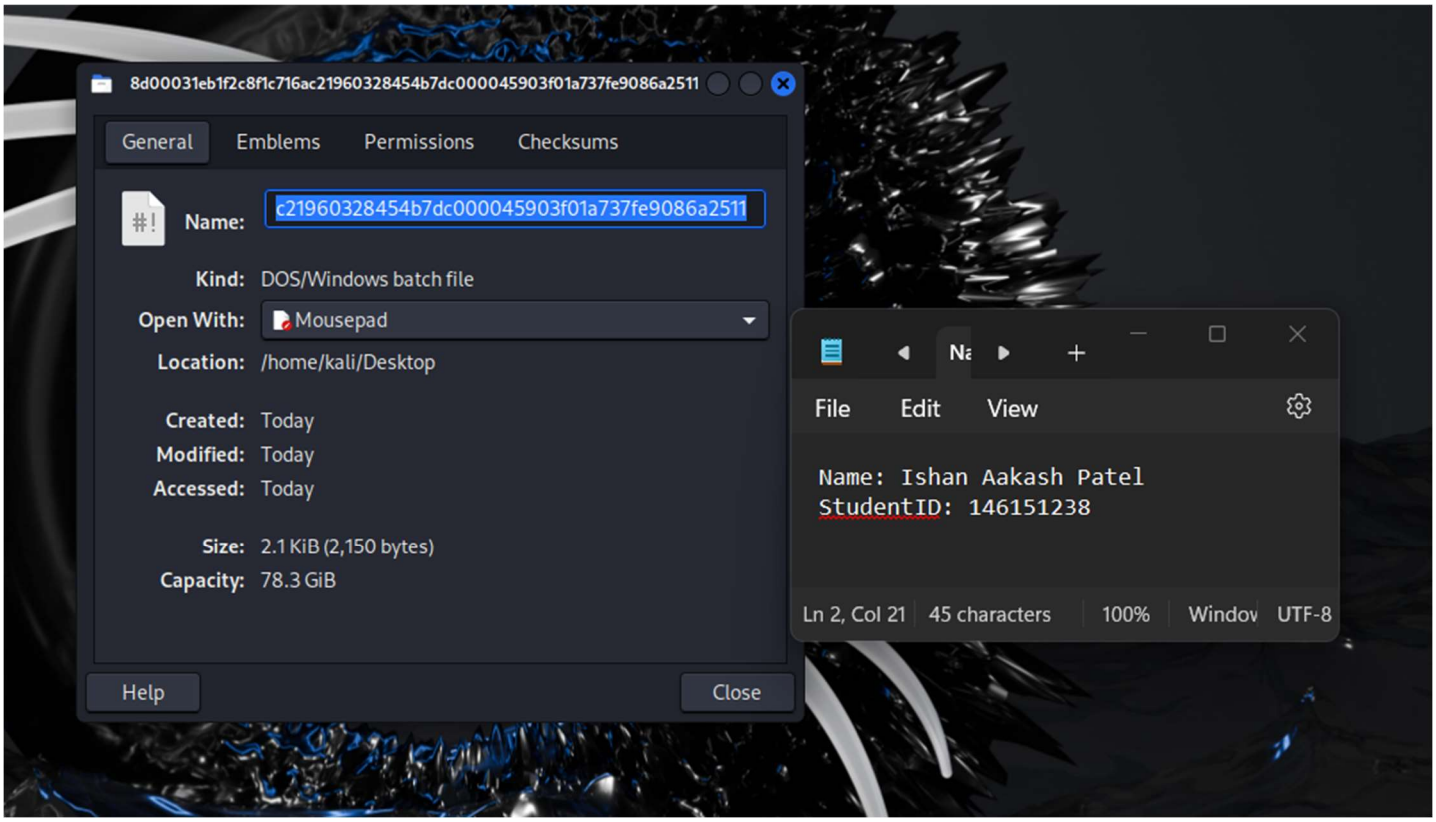
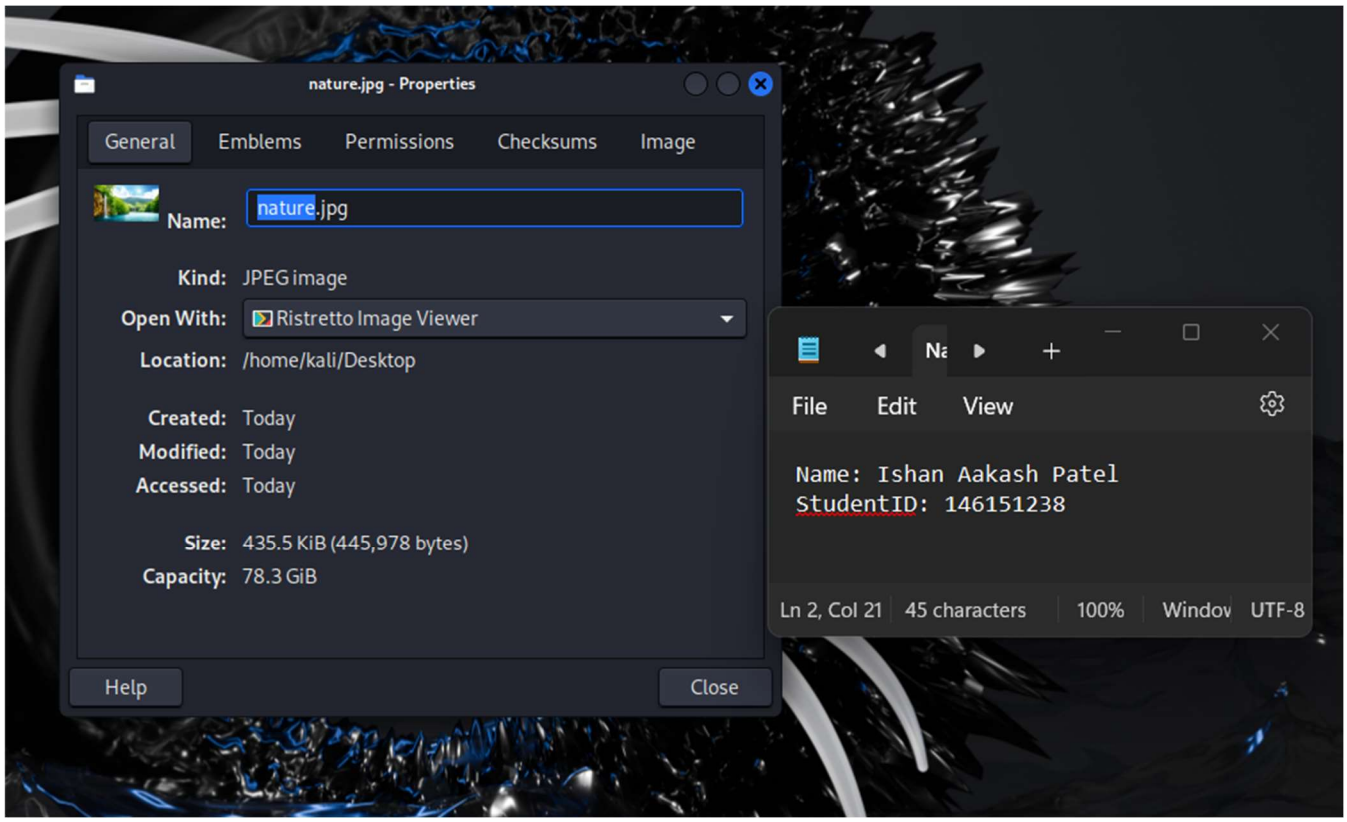
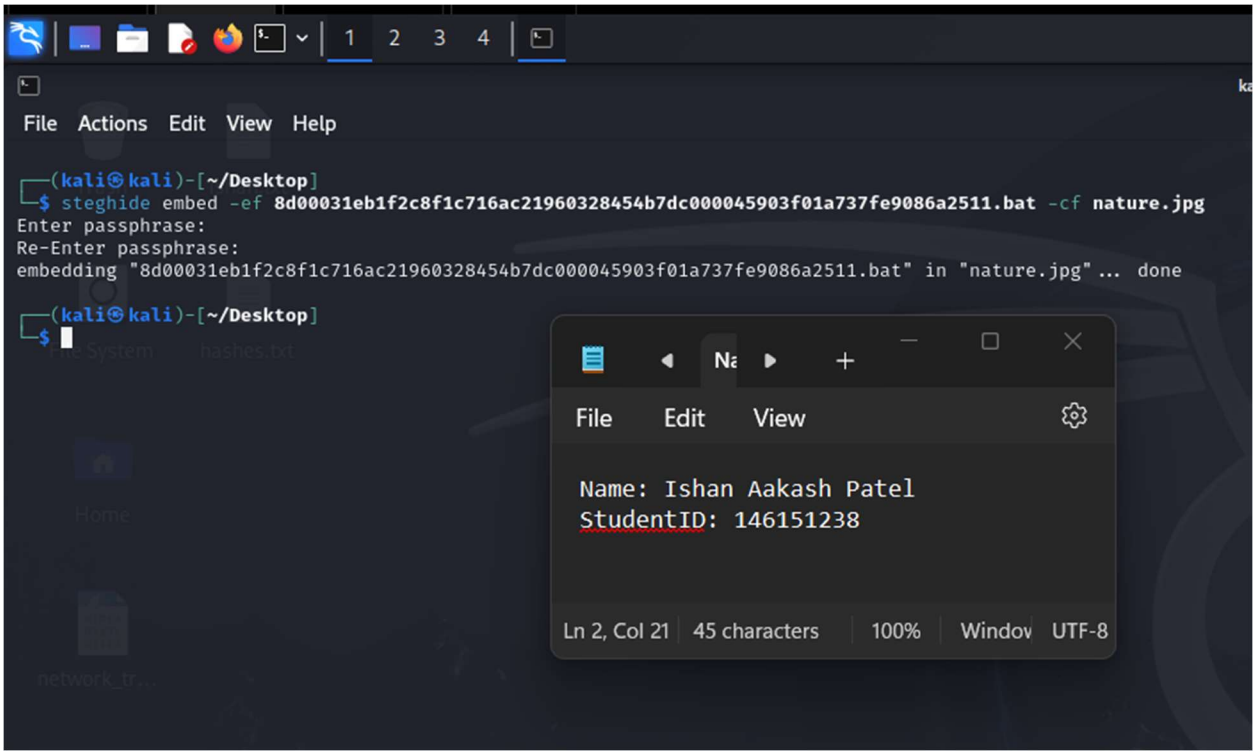


Image info

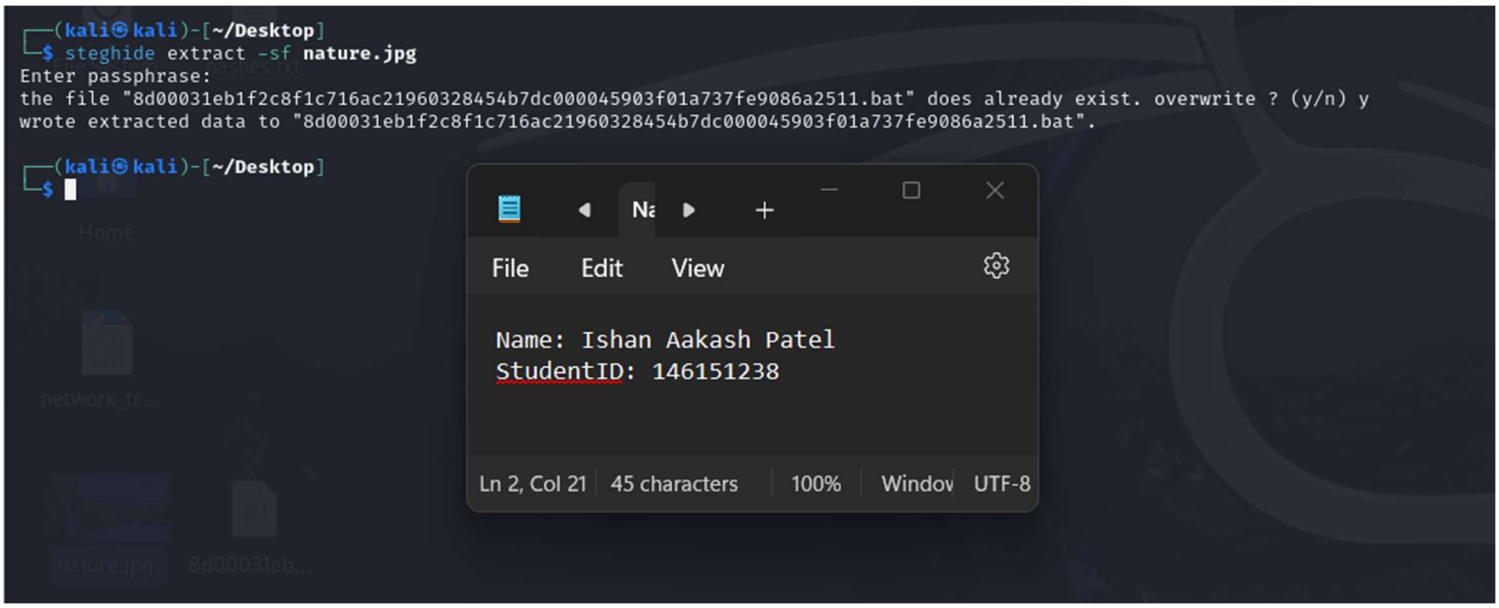




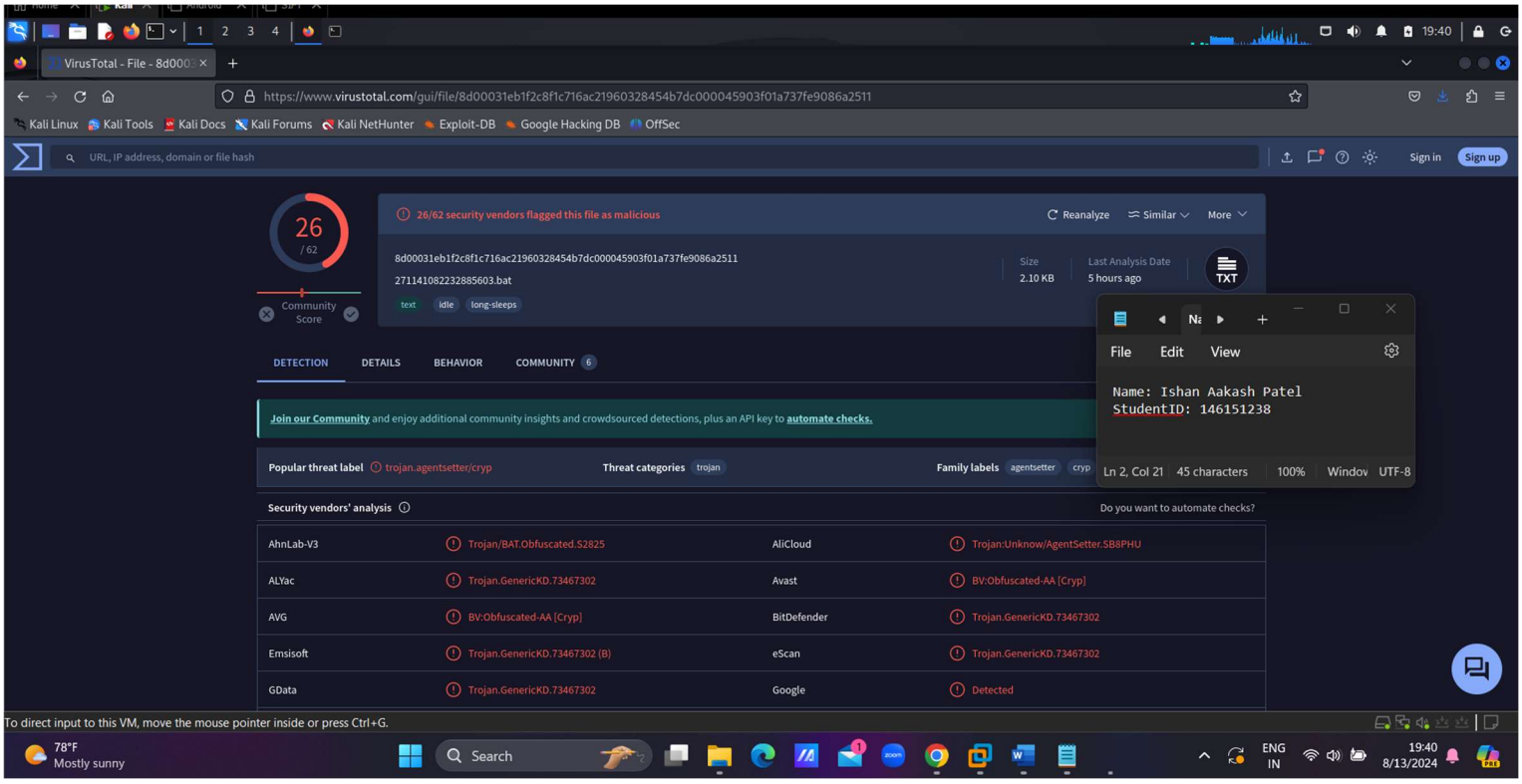
Malware embedded...

Task 2 – Detecting the malware....

Now we will extract it...



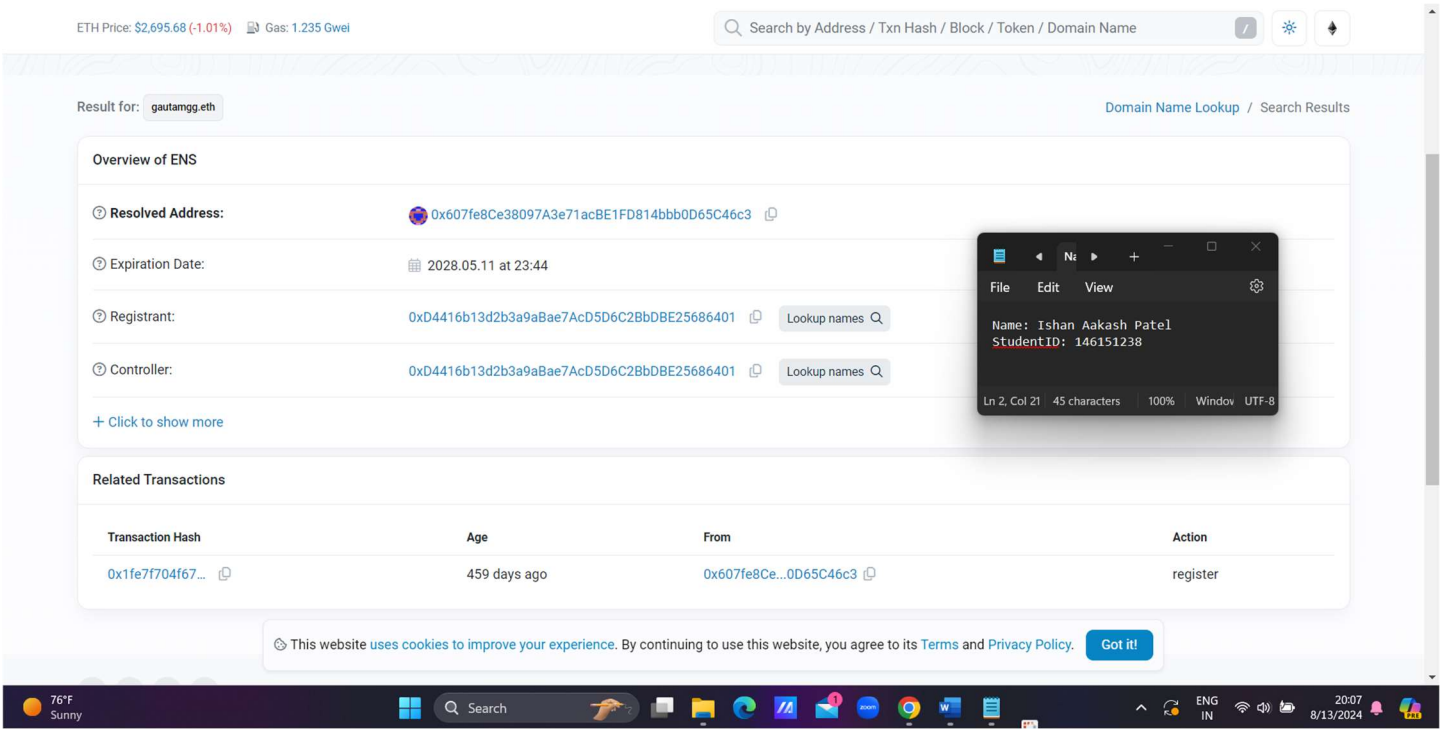
Check the file in VirusTotal



Part – 3 Blockchain Forensics and OSINT

Part 1: Introduction to .sol and .eth Domains
Background:
• .sol Domains:
The .sol domain is part of the Solana blockchain ecosystem, a highly performant blockchain known for its speed and low transaction costs. These domains are used to represent addresses, making it easier for users to interact with decentralized applications (dApps), wallets, and other services on the Solana network without needing to remember long and complex alphanumeric addresses.
• .eth Domains:
The .eth domain is part of the Ethereum blockchain ecosystem, widely recognized as the most popular platform for decentralized applications and smart contracts. Similar to .sol domains, .eth domains simplify interactions by allowing users to replace their Ethereum wallet addresses with human-readable names. The .eth domains are managed by the Ethereum Name Service (ENS), which provides decentralized naming for wallets, websites, and more within the Ethereum ecosystem.

gautamgg.eth
Overview of ENS (Ethereum Name Service)
The Ethereum Name Service (ENS) is a decentralized domain name service on the Ethereum blockchain. It allows users to register .eth domains that can be used to represent Ethereum addresses, making it easier to send and receive cryptocurrency or interact with decentralized applications (dApps). ENS names can also be used for other



data, such as IPFS hashes or metadata, linking your Ethereum identity with other blockchain-based services.

Resolved Address

- **Address:** 0x607fe8Ce38097A3e71acBE1FD814bbb0D65C46c3
- This is the Ethereum address that the ENS domain gautamgg.eth resolves to. Anyone can use this domain to send Ethereum or interact with the address in a human-readable format.

Expiration Date

- **Date:** 2028.05.11 at 23:44
- The ENS domain gautamgg.eth is registered until May 11, 2028, ensuring that the address remains mapped to the domain until then.

Registrant

- **Registrant:** 0xD4416b13d2b3a9aBae7AcD5D6C2BbDBE25686401
- The registrant is the Ethereum address that owns the gautamgg.eth domain. This address has full control over the domain, including renewing it or transferring ownership.

Controller

- **Controller:** 0xD4416b13d2b3a9aBae7AcD5D6C2BbDBE25686401
- The controller is the address that manages the ENS domain's records, such as the resolved address or other metadata. In this case, the controller and registrant are the same, meaning the owner is also managing the domain.

Related Transactions

The table below provides a summary of transactions related to the gautamgg.eth domain and its associated Ethereum address.

Transaction Hash			From	Action
0x1fe7f704f676df90b30226d3d44cc7affbdfaa96860b8745140f977fe80edd0a			0x607fe8Ce...0D65C46c3	Register

Overview of gautamgg.sol

Address

- **Address:** BzTD2xNUedEfCkkKYaX8C6gz4LZskN1RpGdunS7NDUSU
- This is the Solana address associated with the gautamgg.sol domain.

Balance

- **Balance (SOL):** ◎10.364942642
- The Solana address currently holds approximately 10.36 SOL, which is the native cryptocurrency of the Solana blockchain.

Assigned Program Id

- **Program ID:** System Program
- The Solana address is linked to the System Program, which is the standard account for basic operations on the Solana blockchain.

Transaction History

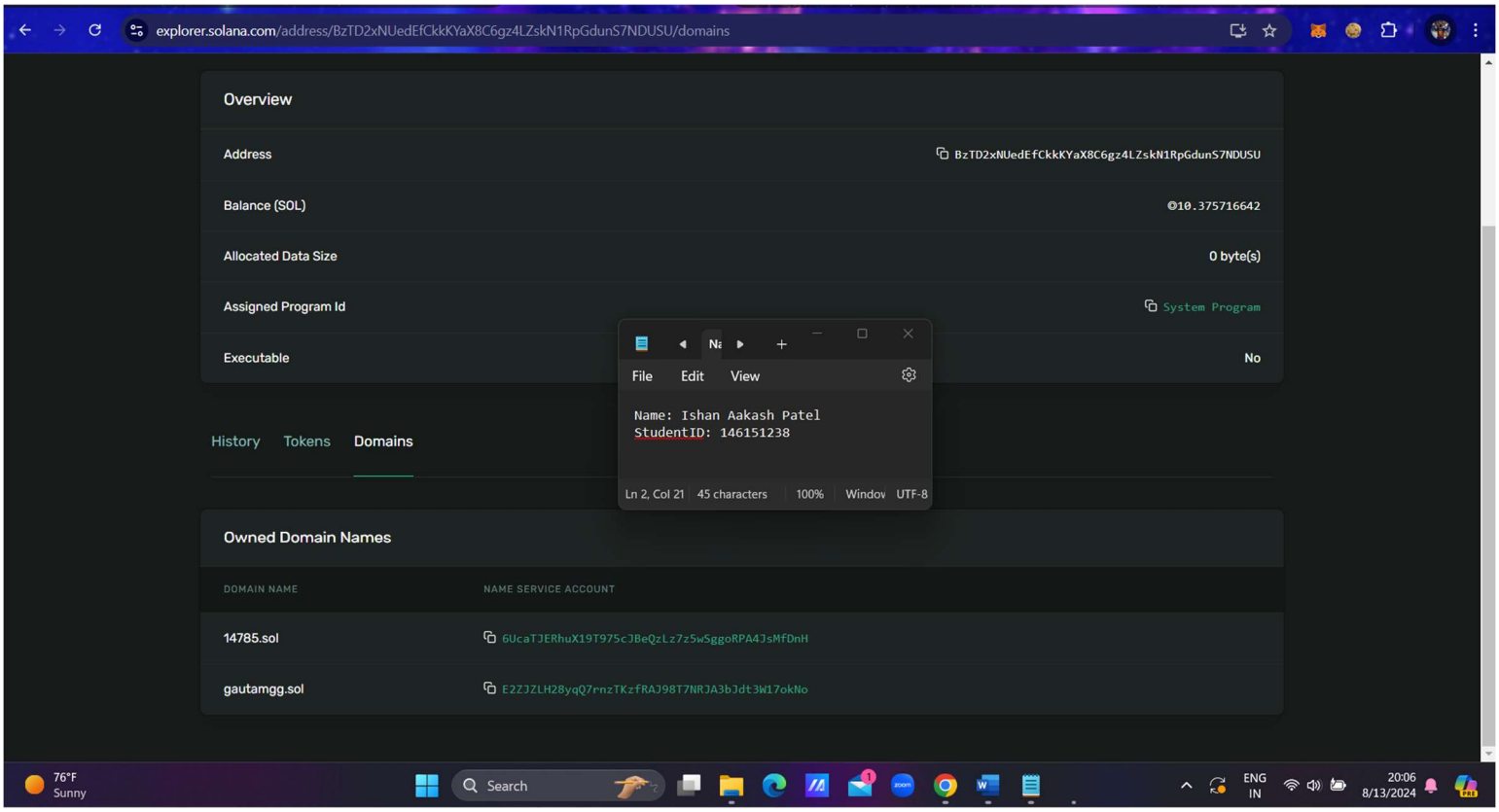
The table below lists the recent transactions associated with the gautamgg.sol domain and its Solana address.

Transaction Signature	Block	Age	Timestamp	Result
2NyDZhWUvMMzAztP4Gqy4ed8M3iaMC4JspyMAxAVe3iAsGpXQhfUCWUEJD4y...	284,132,318	11 hours ago	Aug 17, 2024, 10:09:02 UTC	Success
25QAWYdnNk9iZopnovY5xm6HjahTDrJe1XaVy4GtzbmaYqxAThdLB5Ff2mcN...	284,132,212	11 hours ago	Aug 17, 2024, 10:08:16 UTC	Success
2ipqDYRCV5APGromyDHYJw7HfX3SqrfEpf1kQqa11qNBFhE24NocMYLmsHNu...	281,371,224	14 days ago	Aug 3, 2024, 19:03:53 UTC	Success
59jFRnGs5snxvbwR6KMDrXdnUCWfqQxAZve7T4w1ZJA4j2ZM2LNMZgAw1ewg...	280,928,040	16 days ago	Aug 1, 2024, 12:26:01 UTC	Success

This provides a detailed look at how both the ENS and Solana domains are functioning, with their associated addresses and transaction histories.

Part 2: Tracking Cryptocurrency Wallets
Identify Wallet Addresses:

1. **Using Blockchain Explorers**
   To track the cryptocurrency wallets associated with the given domains, gautamgg.eth and gautamgg.sol, blockchain explorers like Etherscan and Solana Explorer were utilized.
   - **Solana Explorer**: The Solana address associated with gautamgg.sol was found to be BzTD2xNUedEfCkkKYaX8C6gz4LZskN1RpGdunS7NDUSU.
   - **Etherscan**: The Ethereum address linked to gautamgg.eth was identified as 0x607fe8Ce38097A3e71acBE1FD814bbb0D65C46c3.

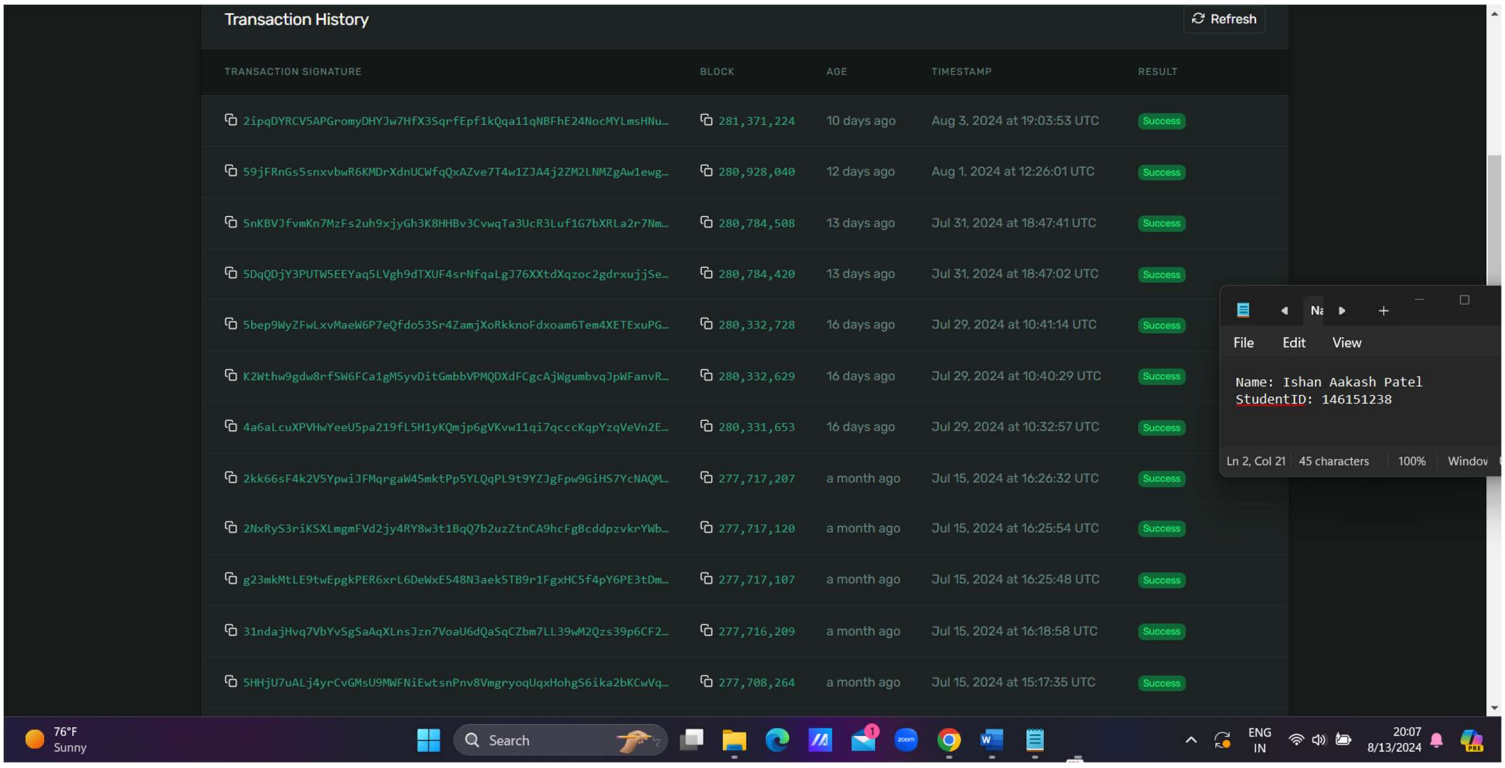


2. **Analyze Transaction History**
   The transaction history for both wallet addresses was examined using the respective blockchain explorers. Below are the significant transactions noted, including details on dates, amounts, and recipient addresses.

Solana Wallet: BzTD2xNUedEfCkkKYaX8C6gz4LZskN1RpGdunS7NDUSU

Transaction Signature	Block	Date	Amount (SOL)	Recipient Address
2NyDZhWUvMMzAztP4Gqy4ed8M3iaMC4JspyMAxAVe3iAsGpXQhfUCWUEJD4y...	284,132,318	Aug 17, 2024, 10:09:02 UTC	N/A	N/A
25QAWYdnNk9iZopnovY5xm6HjahTDrJe1XaVy4GtzbmaYqxAThdLB5Ff2mcN...	284,132,212	Aug 17, 2024, 10:08:16 UTC	N/A	N/A
2ipqDYRCV5APGromyDHYJw7HfX3SqrfEpf1kQqa11qNBFhE24NocMYLmsHNu...	281,371,224	Aug 3, 2024, 19:03:53 UTC	N/A	N/A
59jFRnGs5snxvbwR6KMDrXdnUCWfqQxAZve7T4w1ZJA4j2ZM2LNMZgAw1ewg...	280,928,040	Aug 1, 2024, 12:26:01 UTC	N/A	N/A

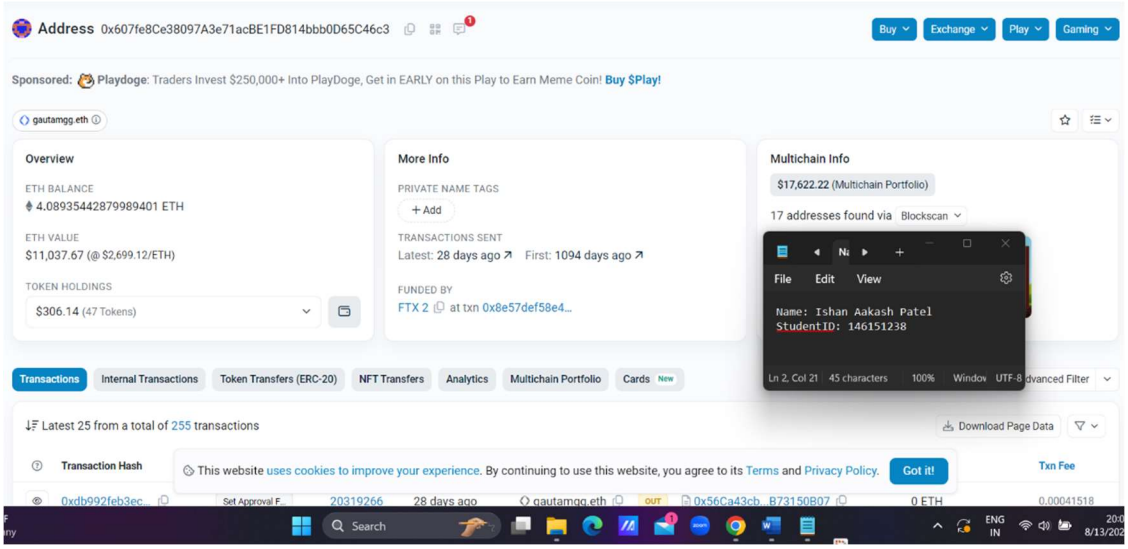
- **Analysis**: The recent transactions include several successful transfers, but specific amounts and recipient details were not provided in the extracted data.

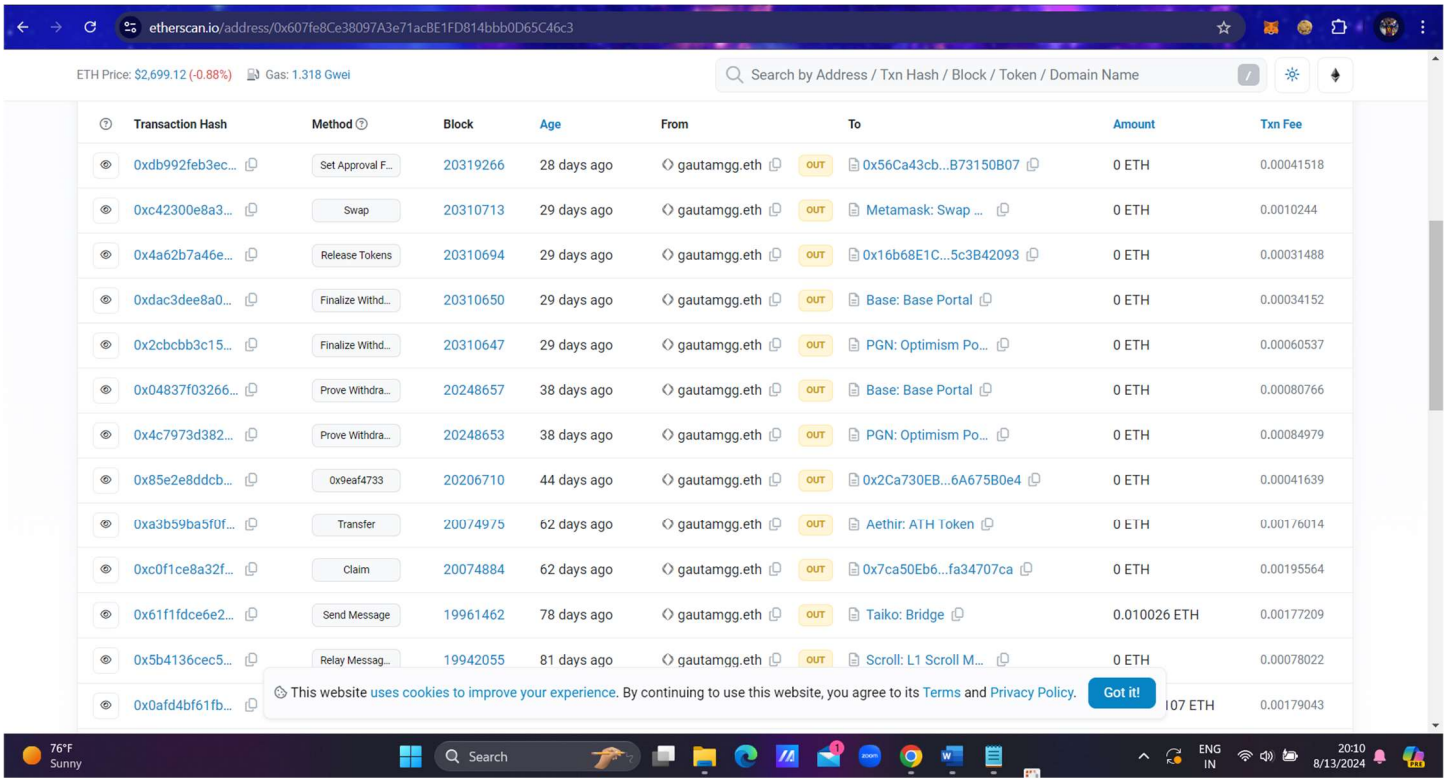


Ethereum Wallet: 0x607fe8Ce38097A3e71acBE1FD814bbb0D65C46c3

Transaction Hash	Date	Recipient Address
0x1fe7f704f676df90b30226d3d44cc7affbdfaa96860b8745140f977fe80edd0a	463 days ago	0x607fe8Ce...0D65C46c3

- **Analysis**: The registration of the gautamgg.eth domain was performed 463 days ago. Specific transaction amounts and further details were not listed, but the registration event is a notable transaction.



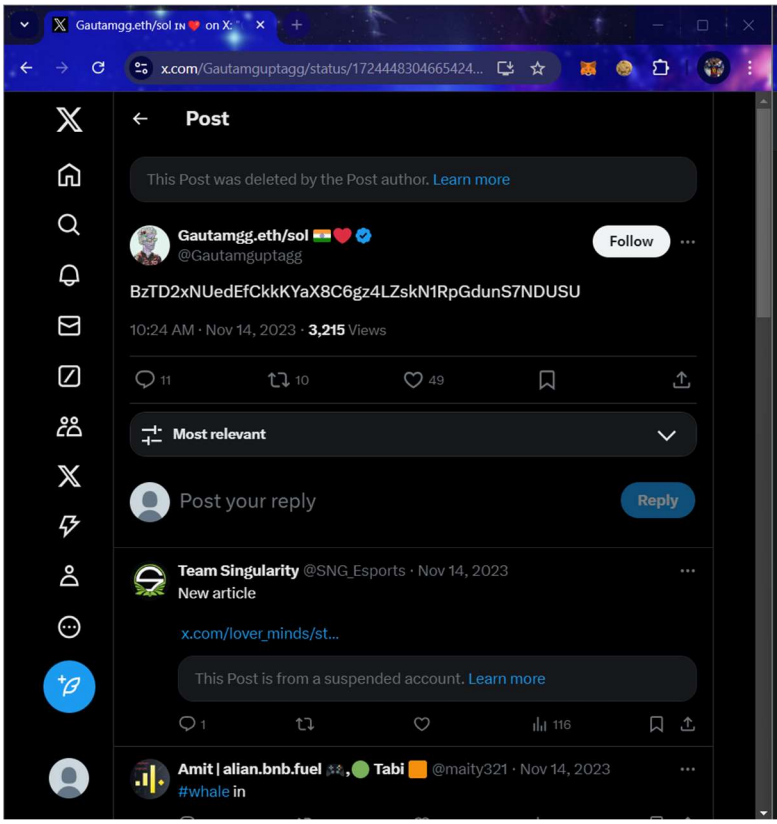


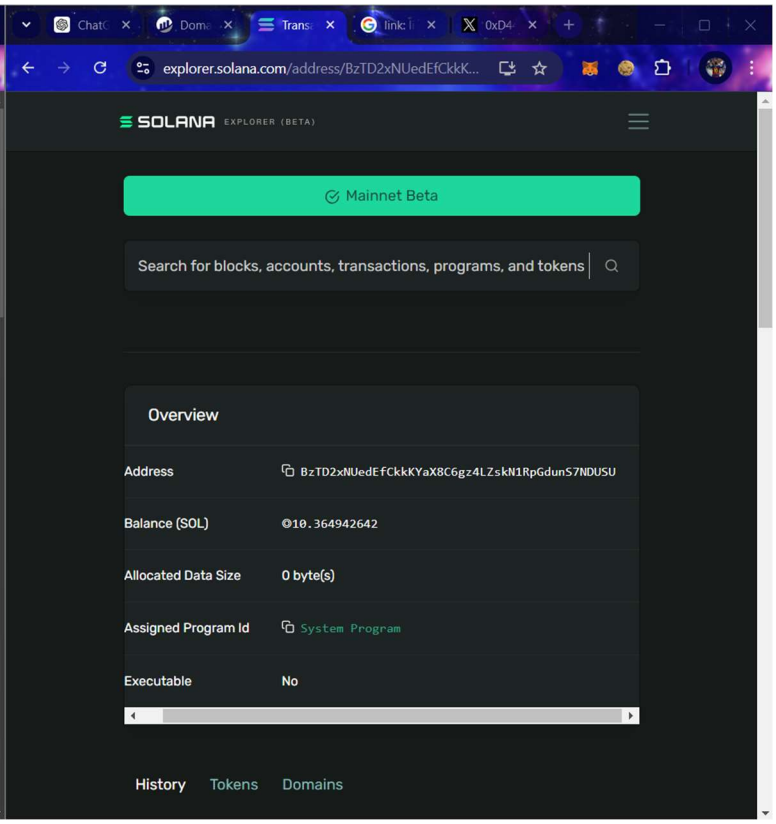
Summary:

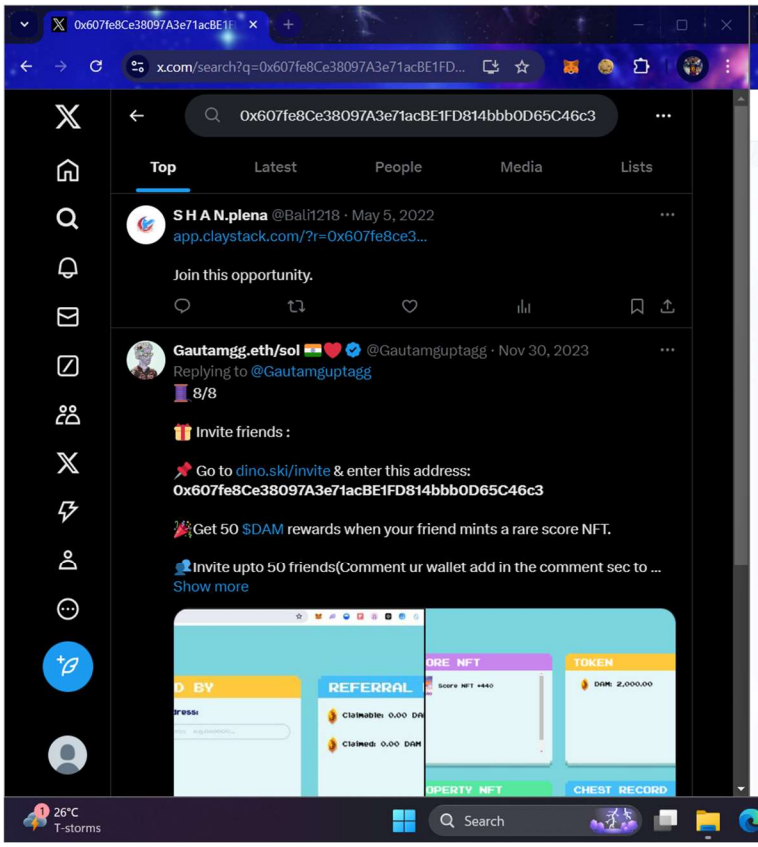
- The Solana address BzTD2xNUedEfCkkKYaX8C6gz4LZskN1RpGdunS7NDUSU associated with gautamgg.sol has a transaction history with multiple successful transactions but lacks specific amounts in the available data.
- The Ethereum address 0x607fe8Ce38097A3e71acBE1FD814bbb0D65C46c3 associated with gautamgg.eth has a significant registration transaction that took place 463 days ago, with further detailed transaction history not provided in the extract.

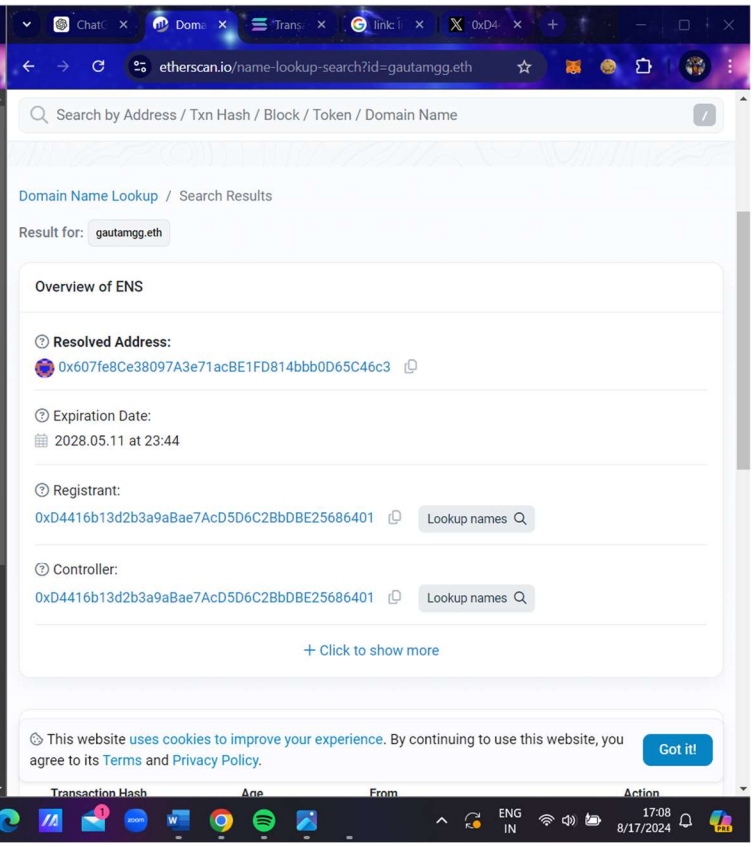
These wallet addresses have active transaction histories, making them critical in tracking financial activity within the Solana and Ethereum ecosystems.

Part 3: Open-Source Intelligence (OSINT)

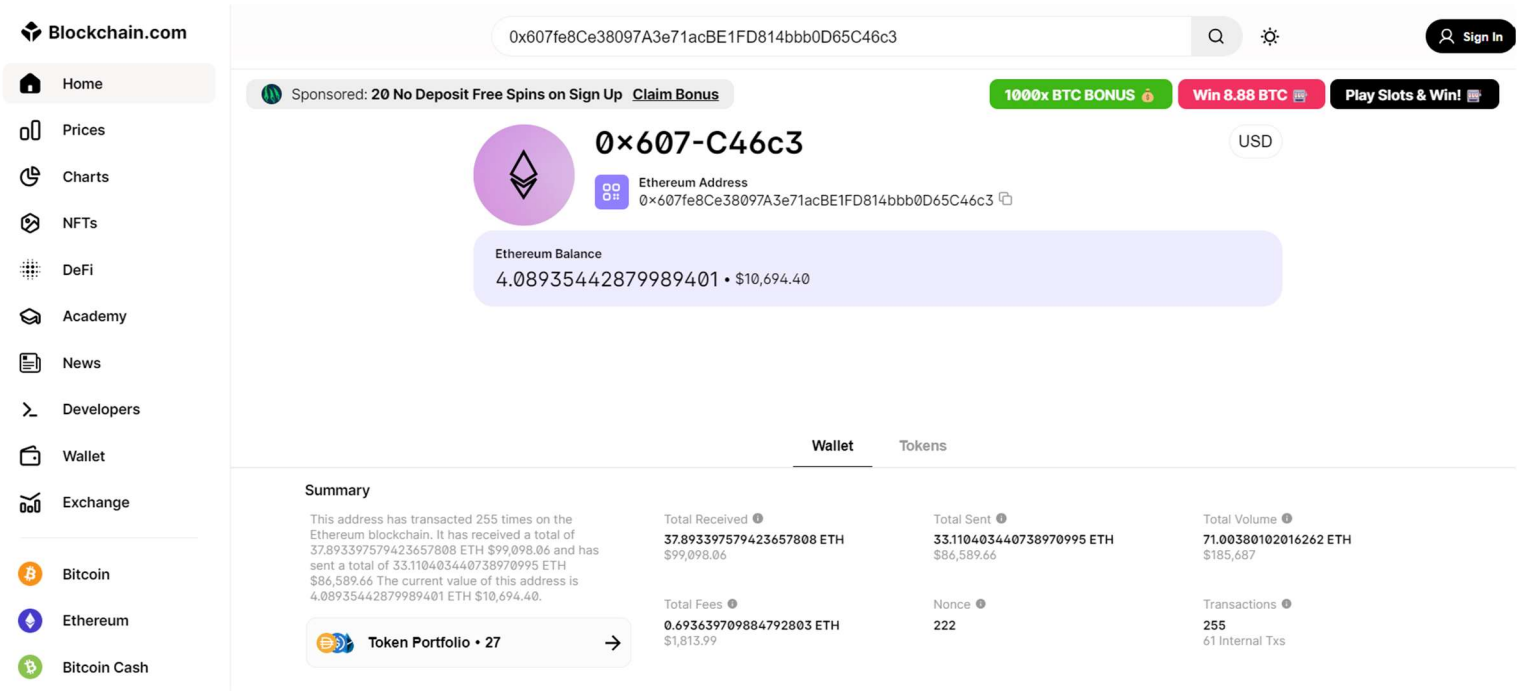








This might be wrong but this is the only thing with the linked address to the .sol and .eth wallets addresses on Twitter.



1. Finding the Identity of the Public Figure

Transaction History Patterns:

- The Solana wallet address (BzTD2xNUedEfCkkKYaX8C6gz4LZskN1RpGdunS7NDUSU) has been publicly shared by the user on a Twitter-like platform
- The Ethereum address (0x607fe8Ce38097A3e71acBE1FD814bbb0D65C46c3) is linked to the ENS domain gautamgg.eth, which is associated with the same social media profile.
- By analyzing the transaction history on Solana Explorer and Etherscan, you can identify interactions with other well-known entities or wallets. For instance, if the addresses frequently interact with known exchanges or dApps, it can indicate the nature of their activity (e.g., trading, staking).

- **Public Mentions:**
  - The Ethereum address has been used in public posts for referral programs and promotions, which are associated with the user "Gautamgg.eth/sol" on social media.
  - These wallet addresses are publicly mentioned, which strongly suggests they belong to the user behind the social media accounts. The public sharing of these addresses can be a key factor in linking the wallet to the individual.

2. Social Media Profiles

- **Twitter Profile:**
  - The Twitter profile linked to the ENS domain gautamgg.eth and the Solana address shows a user with the handle @Gautamguptagg.

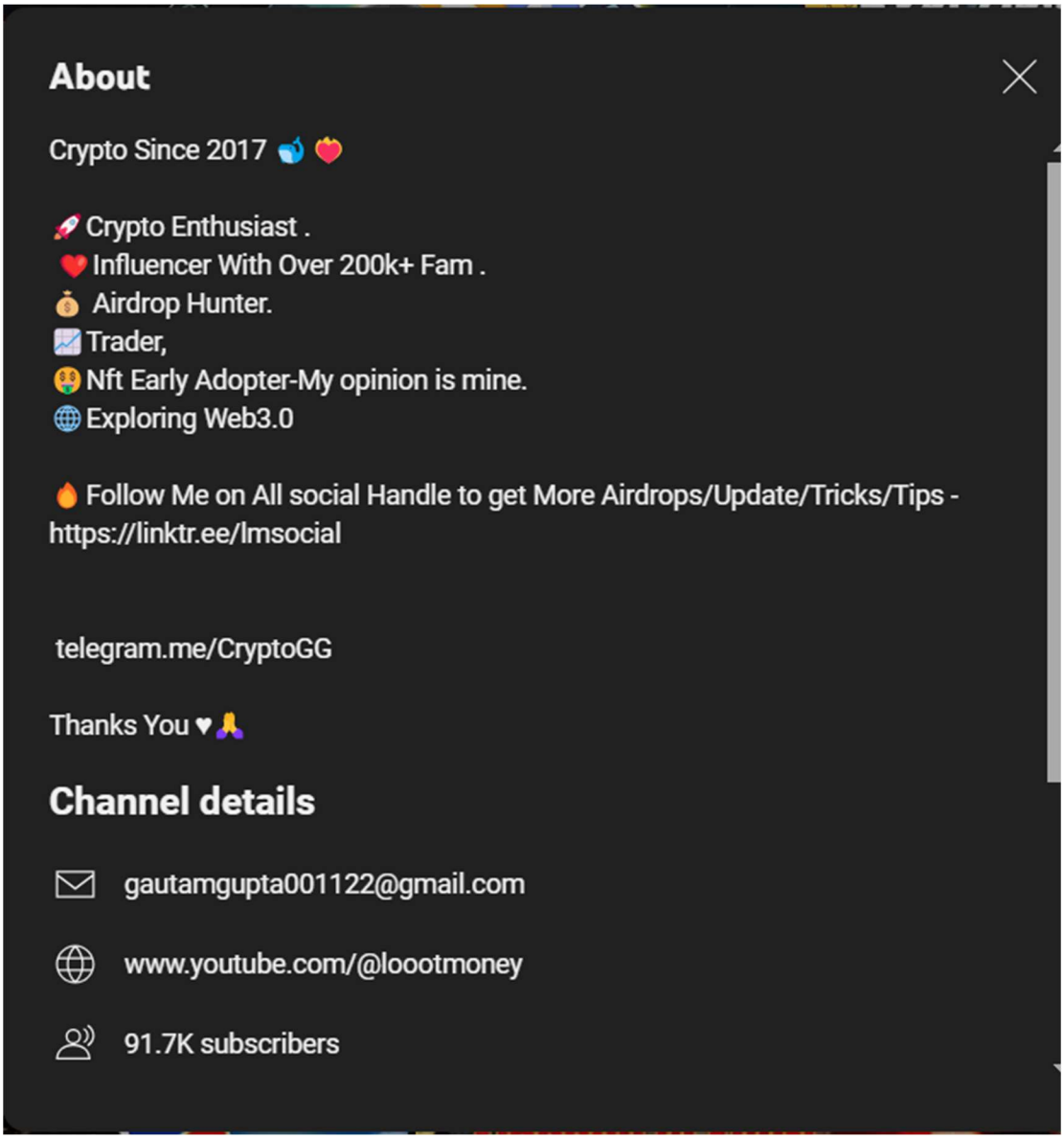
    - The profile description indicates that the person is an analyst, researcher, and crypto enthusiast involved in NFTs, airdrops, early projects, and more.
    - The user also provides a link to their other social profiles or resources via linktr.ee/lmsocial, which could lead to additional information.
- **Social Media Activity:**
    - The user is highly active in the crypto community, as seen from the posts, interactions, and the follower count.

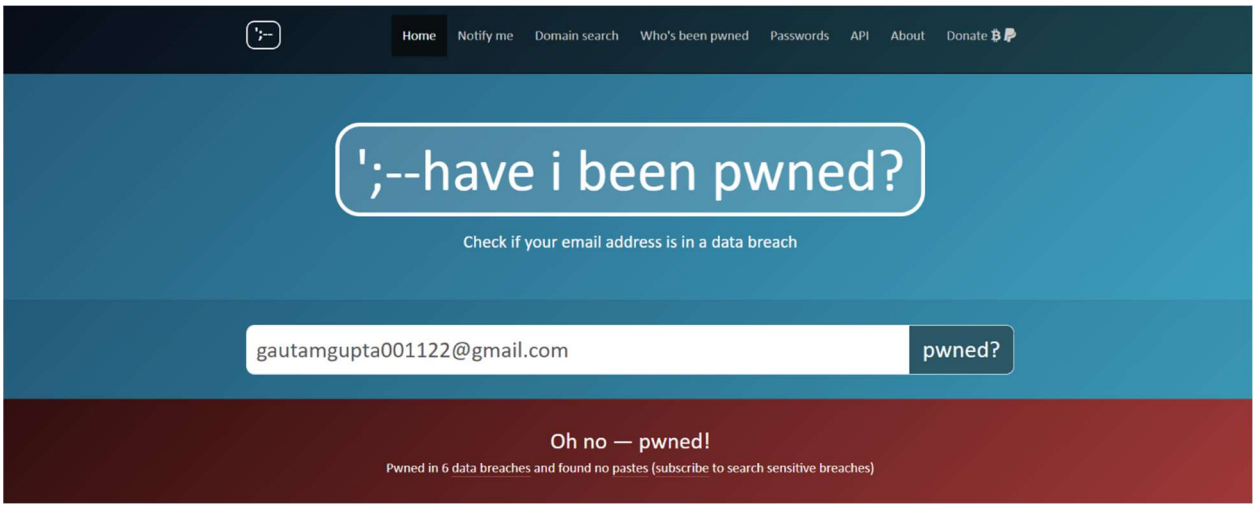
3. Occupation

- **Analyzing Social Media Profiles:**
    - From the Twitter profile, it's evident that the person is engaged in the cryptocurrency industry, specifically in the areas of research, analysis, and advising on crypto projects.
    - The bio mentions that the person has been involved in crypto since 2017, further indicating their deep involvement in the space.
    - The user claims to be an advisor and builder in the crypto community, which suggests they might be associated with specific projects, companies, or startups in the blockchain industry.

Summary

- **Identity:** The public figure behind these wallet addresses appears to be a crypto analyst and researcher active on social media under the handle @Gautamguptagg, with a focus on NFTs, airdrops, and early-stage crypto projects.
- **Occupation:** The person is likely working as an analyst, researcher, advisor, and builder within the cryptocurrency industry.


About
Crypto Since 2017
Crypto Enthusiast .
Influencer With Over 200k+ Fam .
Airdrop Hunter.
Trader,
Nft Early Adopter-My opinion is mine.
Exploring Web3.0
Follow Me on All social Handle to get More Airdrops/Update/Tricks/Tips - https://linktr.ee/lmsocial
telegram.me/CryptoGG
Thanks You
Channel details
gautamgupta001122@gmail.com
www.youtube.com/@loootmoney
91.7K subscribers


Home
Notify me
Domain search
Who's been pwned
Passwords
API
About
Donate
';--have i been pwned?
Check if your email address is in a data breach
gautamgupta001122@gmail.com
pwned?
Oh no — pwned!
Pwned in 6 data breaches and found no pastes (subscribe to search sensitive breaches)

This is all I could I find – I might be wrong…

Learning Experience

During my time working on a project in IT forensics, I learned a lot about analyzing digital evidence. At first, it was a bit overwhelming because there were so many tools and techniques to understand. However, as I started using tools like Volatility and oletools, I became more comfortable with the process. These tools helped me extract valuable information from digital files and memory, which was crucial for the investigation.

One of the most challenging parts was understanding how to properly interpret the data I found. Not everything I extracted was immediately useful, so I had to learn how to filter out what was important. This experience taught me the importance of being patient and methodical, as rushing through the process could lead to missing critical evidence. Over time, I developed a systematic approach to analyzing data, which made the task less daunting and more manageable.

Overall, this experience was incredibly rewarding. I gained a deeper understanding of IT forensics and how to use specific tools to uncover hidden information. The challenges I faced along the way helped me grow as a problem solver and critical thinker. Now, I feel more confident in my ability to handle complex forensic investigations and am eager to apply these skills in future projects.

THANK YOU PROF….