

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.

The screenshot shows a list of course materials and files:

- Week 7 - July 9, July 11 Malware Analysis And Anti Forensics**
Visible to students
- Hiding Malware inside a Picture. -Steganography example.docx**
Visible to students
- CYT215-Module 7 & 8 -Malware Analysis Anti Forensic .pptx**
Visible to students

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 INDIVIDUAL 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

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	File output
832	676	msdtc.exe	0xad8185861280	9	-	0	False	2023-05-21 22:29:25.000000	N/A	Disabled
4	0	System	0xad8185883180	157	-	N/A	False	2023-05-21 22:27:10.000000	N/A	Disabled
108	4	Registry	0xad81858f2080	4	-	N/A	False	2023-05-21 22:26:54.000000	N/A	Disabled
3028	676	dllhost.exe	0xad8185907080	12	-	0	False	2023-05-21 22:29:20.000000	N/A	Disabled
5704	824	RuntimeBroker.	0xad8185962080	5	-	1	False	2023-05-21 22:32:44.000000	N/A	Disabled
332	4	smss.exe	0xad81860dc040	2	-	N/A	False	2023-05-21 22:27:10.000000	N/A	Disabled
452	444	cssrs.exe	0xad81861cd080	12	-	0	False	2023-05-21 22:27:22.000000	N/A	Disabled
2404	2152	vm3dservice.ex	0xad8186619200	2	-	1	False	2023-05-21 22:28:32.000000	N/A	Disabled
528	520	cssrs.exe	0xad8186fb140	14	-	1	False	2023-05-21 22:27:25.000000	N/A	Disabled
552	444	wininit.exe	0xad8186f2b080	1	-	0	False	2023-05-21 22:27:25.000000	N/A	Disabled
588	520	winlogon.exe	0xad8186f45c0	5	-	1	False	2023-05-21 22:27:25.000000	N/A	Disabled
372	824	SkypeBackground	0xad8186f49080	3	-	1	False	2023-05-21 22:10:00.000000	N/A	Disabled
1232	676	svchost.exe	0xad8186f4a2c0	7	-	0	False	2023-05-21 22:29:39.000000	N/A	Disabled
676	552	services.exe	0xad8186f4d080	7	-	0	False	2023-05-21 22:27:29.000000	N/A	Disabled
696	552	lsass.exe	0xad8186fc6080	10	-	0	False	2023-05-21 22:27:29.000000	N/A	Disabled
852	552	fontdrvhost.ex	0xad818761b0c0	5	-	0	False	2023-05-21 22:27:33.000000	N/A	Disabled
824	676	svchost.exe	0xad818761d240	22	-	0	False	2023-05-21 22:27:32.000000	N/A	Disabled
860	588	fontdrvhost.ex	0xad818761f140	5	-	1	False	2023-05-21 22:27:33.000000	N/A	Disabled
952	676	svchost.exe	0xad81876802c0	12	-	0	False	2023-05-21 22:27:36.000000	N/A	Disabled
1016	588	dwm.exe	0xad81876e4340	15	-	1	False	2023-05-21 22:27:38.000000	N/A	Disabled
5656	824	RuntimeBroker.	0xad81876e8080	0	-	1	False	2023-05-21 21:58:19.000000	2023-05-21 22:02:01.000000	Disabled
448	676	svchost.exe	0xad8187721240	54	-	0	False	2023-05-21 22:27:41.000000	N/A	Disabled
1012	676	svchost.exe	0xad818774c080	19	-	0	False	2023-05-21 22:27:43.000000	N/A	Disabled
752	676	svchost.exe	0xad8187758200	21	-	0	False	2023-05-21 22:27:43.000000	N/A	Disabled
1196	676	svchost.exe	0xad81877972c0	34	-	0	False	2023-05-21 22:27:46.000000	N/A	Disabled
1376	676	svchost.exe	0xad81878020c0	15	-	0	False	2023-05-21 22:27:49.000000	N/A	Disabled
1280	4	MemCompression	0xad8187835080	62	-	N/A	False	2023-05-21 22:27:49.000000	N/A	Disabled
1448	676	svchost.exe	0xad818796c2c0	30	-	0	False	2023-05-21 22:27:52.000000	N/A	Disabled
1496	676	svchost.exe	0xad81879752c0	12	-	0	False	2023-05-21 22:27:52.000000	N/A	Disabled
1644	676	svchost.exe	0xad8187a112c0	6	-	0	False	2023-05-21 22:27:58.000000	N/A	Disabled
1652	676	svchost.exe	0xad8187a2d2c0	10	-	0	False	2023-05-21 22:27:58.000000	N/A	Disabled
8896	5328	msedge.exe	0xad8187a39080	18	-	1	False	2023-05-21 22:28:21.000000	N/A	Disabled
1840	676	spoolsv.exe	0xad8187ac2b00	10	-	0	False	2023-05-21 22:28:03.000000	N/A	Disabled
1892	676	svchost.exe	0xad8187b34080	14	-	0	False	2023-05-21 22:28:05.000000	N/A	Disabled
2024	676	svchost.exe	0xad8187b65240	7	-	0	False	2023-05-21 22:28:11.000000	N/A	Disabled
2076	676	svchost.exe	0xad8187b94080	10	-	0	False	2023-05-21 22:28:19.000000	N/A	Disabled
1120	676	MsMpEng.exe	0xad818945c080	12	-	0	False	2023-05-21 22:10:01.000000	N/A	Disabled
244	676	vmt01lsd.exe	0xad81896ab080	11	-	0	False	2023-05-21 22:28:19.000000	N/A	Disabled
			0xad81896ae240	2	-	0	False	2023-05-21 22:28:19.000000	N/A	Disabled
			0xad81896b3300	2	-	0	False	2023-05-21 22:28:19.000000	N/A	Disabled
			0xad8189796300	8	-	1	False	2023-05-21 22:31:59.000000	N/A	Disabled
1916	824	SearchApp.exe	0xad818d099080	24	-	1	False	2023-05-21 22:33:05.000000	N/A	Disabled
6200	676	SgrmBroker.exe	0xad818d09f080	7	-	0	False	2023-05-21 22:33:42.000000	N/A	Disabled
2228	3580	FTK Imager.exe	0xad818d143080	10	-	1	False	2023-05-21 22:43:56.000000	N/A	Disabled
1764	824	dllhost.exe	0xad818d176080	7	-	1	False	2023-05-21 22:32:48.000000	N/A	Disabled
7732	5896	rundll32.exe	0xad818d1912c0	1	-	1	True	2023-05-21 22:31:53.000000	N/A	Disabled
5136	676	SecurityHealth	0xad818d374280	7	-	0	False	2023-05-21 22:32:01.000000	N/A	Disabled
6644	824	SkypeApp.exe	0xad818d3ac080	49	-	1	False	2023-05-21 22:41:52.000000	N/A	Disabled
5480	448	oneTEX.exe	0xad818d3d6080	6	-	1	True	2023-05-21 23:03:00.000000	N/A	Disabled
6708	676	svchost.exe	0xad818d3f1080	5	-	0	False	2023-05-21 22:37:53.000000	N/A	Disabled
4396	5328	msedge.exe	0xad818d515080	7	-	1	False	2023-05-21 22:32:19.000000	N/A	Disabled
4544	5328	msedge.exe	0xad818d75b080	14	-	1	False	2023-05-21 22:32:39.000000	N/A	Disabled
1144	5328	msedge.exe	0xad818d75f080	18	-	1	False	2023-05-21 22:32:38.000000	N/A	Disabled
6292	5328	msedge.exe	0xad818d7a1080	20	-	1	False	2023-05-21 22:06:15.000000	N/A	Disabled
5340	5328	msedge.exe	0xad818d7b3080	10	-	1	False	2023-05-21 22:32:39.000000	N/A	Disabled
5636	3580	notepad.exe	0xad818d845080	1	-	1	False	2023-05-21 22:46:40.000000	N/A	Disabled
6048	448	taskhostw.exe	0xad818dc5d080	5	-	1	False	2023-05-21 22:40:20.000000	N/A	Disabled
6596	676	TrustedInstall	0xad818dc88080	4	-	0	False	2023-05-21 22:58:13.000000	N/A	Disabled
5808	824	Hxisr.exe	0xad818d5e080	0	-	1	False	2023-05-21 21:59:58.000000	2023-05-21 22:07:45.000000	Disabled
4628	6724	tun2socks.exe	0xad818d82340	0	-	1	True	2023-05-21 22:40:10.000000	2023-05-21 23:01:24.000000	Disabled
7964	5328	msedge.exe	0xad818ddee080	19	-	1	False	2023-05-21 22:22:09.000000	N/A	Disabled
7696	824	dllhost.exe	0xad818de6080	0	-	1	False	2023-05-21 22:02:40.000000	2023-05-21 23:02:45.000000	Disabled
6324	1496	audiogd.exe	0xad818df2e080	4	-	0	False	2023-05-21 22:42:56.000000	N/A	Disabled
2388	5328	msedge.exe	0xad818e54c340	18	-	1	False	2023-05-21 22:35:35.000000	N/A	Disabled
6724	3580	Outline.exe	0xad818e578080	0	-	1	True	2023-05-21 22:36:09.000000	2023-05-21 23:01:24.000000	Disabled
8952	824	TextInputHost.	0xad818e6db080	10	-	1	False	2023-05-21 21:59:11.000000	N/A	Disabled
5476	676	svchost.exe	0xad818e752080	9	-	0	False	2023-05-21 22:58:08.000000	N/A	Disabled
2332	824	TlWorker.exe	0xad818e780080	4	-	0	False	2023-05-21 22:58:13.000000	N/A	Disabled
7312	824	ApplicationFra	0xad818e84f300	10	-	1	False	2023-05-21 22:35:44.000000	N/A	Disabled
4340	676	VSSVC.exe	0xad818e88080	3	-	0	False	2023-05-21 23:01:06.000000	N/A	Disabled
4224	6724	Outline.exe	0xad818e88b080	0	-	1	True	2023-05-21 22:36:23.000000	2023-05-21 23:01:24.000000	Disabled
7772	676	svchost.exe	0xad818e88e140	3	-	0	False	2023-05-21 22:36:03.000000	N/A	Disabled
7540	824	smartscreen.ex	0xad818e893080	14	-	1	False	2023-05-21 23:02:26.000000	N/A	Disabled
7788	2916	conhost.exe	0xad818e8a1080	0	-	0	False	2023-05-21 23:01:27.000000	2023-05-21 23:01:48.000000	Disabled
7336	824	RuntimeBroker.	0xad818e8b080	2	-	1	False	2023-05-21 22:11:39.000000	N/A	Disabled
6076	824	ShellExperienc	0xad818eb18080	14	-	1	False	2023-05-21 22:11:36.000000	N/A	Disabled
8264	824	RuntimeBroker.	0xad818eeb080	4	-	1	False	2023-05-21 22:40:33.000000	N/A	Disabled
8920	3580	FTK Imager.exe	0xad818ef81080	20	-	1	False	2023-05-21 23:02:28.000000	N/A	Disabled
5964	676	svchost.exe	0xad818ef86080	5	-	0	False	2023-05-21 22:27:56.000000	N/A	Disabled
125689842201708	208586546348048	dexer	0xad818f4f62ad	16777219	-	-	True	2000-08-31 04:05:52.000000	-	Disabled
4396	5328	msedge.exe	0xbe8505fb080	7	-	1	False	2023-05-21 22:32:19.000000	N/A	Disabled

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

```
sansforensics@siftworkstation: ~/volatility3
$ sudo python3 vol.py -f MemoryDump.mem windows.malfind
Volatility 3 Framework 2.7.1
Progress: 100.00          PDB scanning finished
PID      Process Start VPN      End VPN Tag      Protection      CommitCharge      PrivateMemory      File output      Notes      Hexdump Disasm
5896      oneetx.exe      0x400000      0x437fff      VadS      PAGE_EXECUTE_READWRITE  56      1      Disabled      MZ header
4d 5a 00 00 03 00 00 00 MZ.....
04 00 00 00 ff ff 00 00 ..... .
b8 00 00 00 00 00 00 00 ..... .
40 00 00 00 00 00 00 00 @..... .
00 00 00 00 00 00 00 00 ..... .
00 00 00 00 00 00 00 00 ..... .
00 00 00 00 00 00 00 00 ..... .
00 00 00 00 00 01 00 00 ..... .
0x400000: dec    ebp
0x400001: pop    edx
0x400002: nop
0x400003: add    byte ptr [ebx], al
0x400005: add    byte ptr [eax], al
0x400007: add    byte ptr [eax + eax], al
0x40000a: add    byte ptr [eax], al
7540      smartscreen.ex 0x2505c140000 0x2505c15ffff VadS      PAGE_EXECUTE_READWRITE  1      1      Disabled
10 00 51 34 10 48 00 45 U TS U L

```

A screenshot of a terminal window showing volatility3 output. The terminal shows memory dump data for processes like oneetx.exe and smartscreen.ex. A floating text editor window is overlaid on the terminal, containing the following text:

Name: Ishan Aakash Patel
StudentID: 146151238

Below the text editor, the terminal status bar shows: Ln 2, Col 21 | 45 characters | 100% | Window | UTF-8

Answer : oneetx.exe

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

```
sansforensics@siftworkstation: ~/volatility3
$ sudo python3 vol.py -f MemoryDump.mem windows.pstree.PsTree
Volatility 3 Framework 2.7.1
Progress: 100.00          PDB scanning finished
PID    PPID   ImageFileName      Offset(V)      Threads Handles SessionId      Wow64   CreateTime      ExitTime      Audit   Cmd      Path
4      0       System            0xad8185883180 157      -      N/A    False  2023-05-21 22:27:10.000000  N/A      -      -      MemCompression
* 1280  4       MemCompression 0xad8187835080 62      -      N/A    False  2023-05-21 22:27:49.000000  N/A      -      -      Registry
* 108   4       Registry        0xad81858f2080 4      -      N/A    False  2023-05-21 22:26:54.000000  N/A      -      -      \Device\HarddiskVolume3\Windows\System32\smss.exe
* 332   4       smss.exe       0xad81860dc040 2      -      N/A    False  2023-05-21 22:27:10.000000  N/A      -      -      \Device\HarddiskVolume3\Windows\System32\smss.exe
452   444   csrss.exe       0xad81861cd080 12      -      0      False  2023-05-21 22:27:22.000000  N/A      -      -      \Device\HarddiskVolume3\Windows\System32\csrss.exe
528   520   csrss.exe       0xad8186fb1b40 14      -      1      False  2023-05-21 22:27:25.000000  N/A      -      -      \Device\HarddiskVolume3\Windows\System32\csrss.exe
552   444   wininit.exe     0xad8186fc0b080 1      -      0      False  2023-05-21 22:27:25.000000  N/A      -      -      \Device\HarddiskVolume3\Windows\System32\wininit.exe
* 696   552   lsass.exe       0xad8186fc6080 10      -      0      False  2023-05-21 22:27:29.000000  N/A      -      -      \Device\HarddiskVolume3\Windows\System32\lsass.exe
Windows\System32\lsass.exe
* 676   552   services.exe    0xad8186ffd080 7      -      0      False  2023-05-21 22:27:29.000000  N/A      -      -      \Device\HarddiskVolume3\Windows\System32\services.exe
:Windows\System32\services.exe
** 4228  676   SearchIndexer 0xad818ce06240 15      -      0      False  2023-05-21 22:31:27.000000  N/A      -      -      \Device\HarddiskVolume3\Windows\System32\SearchIndexer.exe
indexer.exe /Embedding C:\Windows\system32\SearchIndexer.exe
** 8708  676   svchost.exe    0xad818d431080 5      -      0      False  2023-05-21 22:57:33.000000  N/A      -      -      \Device\HarddiskVolume3\Windows\System32\svchost.exe
** 5136  676   SecurityHealth 0xad818d374280 7      -      0      False  2023-05-21 22:32:01.000000  N/A      -      -      \Device\HarddiskVolume3\Windows\System32\SecurityHealth.exe
** 2200  676   VGAuthService. 0xad81896b3300 2      -      0      False  2023-05-21 22:28:19.000000  N/A      -      -      \Device\HarddiskVolume3\Windows\System32\VGAuthService.exe
-
** 3608  676   svchost.exe    0xad818d07a080 3      -      0      Home  False  2023-05-21 22:41:28.000000  N/A      -      -      \Device\HarddiskVolume3\Windows\System32\svchost.exe
** 2076  676   svchost.exe    0xad8187b94080 10      -      0      False  2023-05-21 22:28:19.000000  N/A      -      -      \Device\HarddiskVolume3\Windows\System32\svchost.exe
utcsvc -p C:\Windows\System32\svchost.exe
** 1448  676   svchost.exe    0xad818796c200 30      -      0      False  2023-05-21 22:27:52.000000  N/A      -      -      \Device\HarddiskVolume3\Windows\System32\svchost.exe
NetworkService -p C:\Windows\System32\svchost.exe
** 1064  676   svchost.exe    0xad8189d7c200 15      -      1      False  2023-05-21 22:30:09.000000  N/A      -      -      \Device\HarddiskVolume3\Windows\System32\svchost.exe
UnistackSvcsGroup C:\Windows\System32\svchost.exe
** 6696  676   svchost.exe    0xad818c532080 8      -      0      False  2023-05-21 22:34:07.000000  N/A      -      -      \Device\HarddiskVolume3\Windows\System32\svchost.exe
** 1196  676   svchost.exe    0xad81877972c0 34      -      0      False  2023-05-21 22:27:46.000000  N/A      -      -      \Device\HarddiskVolume3\Windows\System32\svchost.exe
LocalService -p C:\Windows\System32\svchost.exe
** 1840  676   spoolsv.exe    0xad8187acb200 10      -      0      False  2023-05-21 22:28:03.000000  N/A      -      -      \Device\HarddiskVolume3\Windows\System32\spoolsv.exe
** 952   676   svchost.exe    0xad81876802c0 12      -      0      False  2023-05-21 22:27:36.000000  N/A      -      -      \Device\HarddiskVolume3\Windows\System32\svchost.exe
** 824   676   svchost.exe    0xad818761d240 22      -      0      False  2023-05-21 22:27:32.000000  N/A      -      -      \Device\HarddiskVolume3\Windows\System32\svchost.exe
DcomLaunch -p C:\Windows\System32\svchost.exe
*** 7312  824   ApplicationFra 0xad818e84f300 10      -      1      False  2023-05-21 22:35:44.000000  N/A      -      -      \Device\HarddiskVolume3\Windows\System32\ApplicationFrameHost.exe
system32\ApplicationFrameHost.exe -Embedding C:\Windows\System32\ApplicationFrameHost.exe
*** 4116  824   RuntimeBroker. 0xad818rc93300 3      -      1      False  2023-05-21 22:31:24.000000  N/A      -      -      \Device\HarddiskVolume3\Windows\System32\RuntimeBroker.exe
*** 4116  824   RuntimeBroker. 0xad818rc93300 3      -      1      False  2023-05-21 22:31:24.000000  N/A      -      -      \Device\HarddiskVolume3\Windows\System32\RuntimeBroker.exe
```

```
sansforensics@siftworkstation: ~/volatility3
$ sudo python3 vol.py -f MemoryDump.mem windows.pstree.PsTree
Volatility 3 Framework 2.7.1
Progress: 100.00          PDB scanning finished
PID    PPID   ImageFileName      Offset(V)      Threads Handles SessionId      Wow64   CreateTime      ExitTime      Audit   Cmd      Path
**** 7964  5328   msedge.exe    0xad818dee5080 19      -      1      False  2023-05-21 22:22:09.000000  N/A      -      -      \Device\HarddiskVolume3\Pro
gram Files (x86)\Microsoft\Edge\Application\msedge.exe --
**** 4396  5328   msedge.exe    0xad818d515080 7      -      1      False  2023-05-21 22:32:19.000000  N/A      -      -      \Device\HarddiskVolume3\Pro
gram Files (x86)\Microsoft\Edge\Application\msedge.exe --
**** 6544  5328   msedge.exe    0xad818c0ea080 18      -      1      False  2023-05-21 22:22:35.000000  N/A      -      -      \Device\HarddiskVolume3\Pro
gram Files (x86)\Microsoft\Edge\Application\msedge.exe --
**** 2388  5328   msedge.exe    0xad818e54c340 18      -      1      False  2023-05-21 22:05:35.000000  N/A      -      -      \Device\HarddiskVolume3\Pro
gram Files (x86)\Microsoft\Edge\Application\msedge.exe --
**** 6292  5328   msedge      -      -      -      False  2023-05-21 22:06:15.000000  N/A      -      -      \Device\HarddiskVolume3\Pro
gram Files (x86)\Microsoft\Edge\Edg
**** 1144  5328   msedge      -      -      -      False  2023-05-21 22:32:38.000000  N/A      -      -      \Device\HarddiskVolume3\Pro
gram Files (x86)\Microsoft\Edge\Edg
**** 5340  5328   msedge      -      -      -      False  2023-05-21 22:32:39.000000  N/A      -      -      \Device\HarddiskVolume3\Pro
gram Files (x86)\Microsoft\Edge\Edg
*** 3252  3580   vmtool      -      -      -      False  2023-05-21 22:31:59.000000  N/A      -      -      \Device\HarddiskVolume3\Pro
gram Files\VMware\VMware Tools
sd.exe
*** 2228  3580   FTK Im
gram Files\AccessData\FTK Imag
*** 8920  3580   FTK Im
gram Files\AccessData\FTK Imag
Ln 2, Col 21 | 45 characters | 100% | Window  UTF-8
File   Edit   View
Name: Ishan Aakash Patel
StudentID: 146151238
False  2023-05-21 22:43:56.000000  N/A      -      -      \Device\HarddiskVolume3\Pro
File   Edit   View
Name: Ishan Aakash Patel
StudentID: 146151238
False  2023-05-21 23:02:28.000000  N/A      -      -      \Device\HarddiskVolume3\Pro
File   Edit   View
Name: Ishan Aakash Patel
StudentID: 146151238
False  2023-05-21 22:27:33.000000  N/A      -      -      \Device\HarddiskVolume3\Windows\Sys
tem32\fondrvhost.exe
5896  8844   oneetx.exe     0xad8189b41080 5      -      1      True   2023-05-21 22:30:56.000000  N/A      -      -      \Device\HarddiskVolume3\Users\Tamma
\Temp\Local\Temp\c3912af058\oneetx.exe
* 7732  5896   rundll32.exe  0xad818d1912c0 1      -      1      True   2023-05-21 22:31:53.000000  N/A      -      -      \Device\HarddiskVolume3\Windows\Sys
tem32\fondrvhost.exe
WOW64\undll32.exe
sansforensics@siftworkstation: ~/volatility3
```

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

```
sansforensics@siftworkstation: ~/volatility
$ sudo python3 vol.py -f MemoryDump.mem windows.malfind
Volatility 3 Framework 2.7.1
Progress: 100.00          PDB scanning finished
PID      Process Start VPN      End VPN Tag      Protection      CommitCharge      PrivateMemory      File output      Notes      Hexdump Disasm
5896      oneetx.exe      0x4000000      0x437fff      VadS      PAGE_EXECUTE_READWRITE 56      1      Disabled      MZ header
4d 5a 90 00 03 00 00 00 00 MZ.....
04 00 00 00 ff ff 00 00 .....
b8 00 00 00 00 00 00 00 .....
40 00 00 00 00 00 00 00 @.....
00 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 .....
00 00 00 00 00 01 00 00 .....
0x400000: dec    ebp
0x400001: pop    edx
0x400002: nop
0x400003: add    byte ptr [ebx], al
0x400005: add    byte ptr [eax], al
0x400007: add    byte ptr [eax + eax], al
0x4000a: add    byte ptr [eax], al
```

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

```
sansforensics@siftworkstation: ~/volatility
$ sudo python3 vol.py -f MemoryDump.mem windows.pslist
Volatility 3 Framework 2.7.1
Progress: 100.00          PDB scanning finished
PID      PPID      ImageFileName      Offset(V)      Threads Handles SessionId      Wow64      CreateTime      ExitTime      File output
4      0      System      0xad8185883180      157      -      N/A      False      2023-05-21 22:27:10.000000      N/A      Disabled
108     4      Registry      0xad81858f2080      4      -      N/A      False      2023-05-21 22:26:54.000000      N/A      Disabled
332     4      smss.exe      0xad81860dc040      2      -      N/A      False      2023-05-21 22:27:10.000000      N/A      Disabled
452     444      csrss.exe      0xad81861cd080      12      -      0      False      2023-05-21 22:27:22.000000      N/A      Disabled
528     520      csrss.exe      0xad8186f1b140      14      -      1      False      2023-05-21 22:27:25.000000      N/A      Disabled
552     444      wininit.exe      0xad8186f2b080      1      -      0      False      2023-05-21 22:27:25.000000      N/A      Disabled
588     520      winlogon.exe      0xad8186f450c0      5      -      1      False      2023-05-21 22:27:25.000000      N/A      Disabled
676     552      services.exe      0xad8186f4d080      7      -      0      False      2023-05-21 22:27:29.000000      N/A      Disabled
696     552      lsass.exe      0xad8186fc6080      10      -      0      False      2023-05-21 22:27:29.000000      N/A      Disabled
824     676      svchost.exe      0xad818761d240      22      -      0      False      2023-05-21 22:27:32.000000      N/A      Disabled
852     552      fontdrvhost.ex      0xad818761b0c0      5      -      0      False      2023-05-21 22:27:33.000000      N/A      Disabled
860     588      fontdrvhost.ex      0xad818761f140      5      -      1      False      2023-05-21 22:27:33.000000      N/A      Disabled
952     676      svchost.exe      0xad81876802c0      12      -      0      False      2023-05-21 22:27:36.000000      N/A      Disabled
1016     588      dwm.exe      0xad81876e4340      15      -      1      False      2023-05-21 22:27:38.000000      N/A      Disabled
448     676      svchost.exe      0xad8187721240      54      -      0      False      2023-05-21 22:27:41.000000      N/A      Disabled
752     676      svchost.exe      0xad8187758280      21      -      0      False      2023-05-21 22:27:43.000000      N/A      Disabled
1012     676      svchost.exe      0xad818774c080      19      -      0      False      2023-05-21 22:27:43.000000      N/A      Disabled
1196     676      svchost.exe      0xad81877972c0      34      -      0      False      2023-05-21 22:27:46.000000      N/A      Disabled
1280     4      MemCompression      0xad8187835080      62      -      N/A      False      2023-05-21 22:27:49.000000      N/A      Disabled
1376     676      svchost.exe      0xad8187802c0      15      -      0      False      2023-05-21 22:27:49.000000      N/A      Disabled
1448     676      svchost.exe      0xad818796c230      30      -      0      False      2023-05-21 22:27:52.000000      N/A      Disabled
1496     676      svchost.exe      0xad81879752c0      12      -      0      False      2023-05-21 22:27:52.000000      N/A      Disabled
1644     676      svchost.exe      0xad8187a112c0      6      -      0      False      2023-05-21 22:27:58.000000      N/A      Disabled
1652     676      svchost.exe      0xad8187a2dzc0      10      -      0      False      2023-05-21 22:27:58.000000      N/A      Disabled
1840     676      spoolsv.exe      0xad8187acb200      10      -      0      False      2023-05-21 22:28:03.000000      N/A      Disabled
1892     676      svchost.exe      0xad8187b34080      14      -      0      False      2023-05-21 22:28:05.000000      N/A      Disabled
2024     676      svchost.exe      0xad8187b65240      7      -      0      False      2023-05-21 22:28:11.000000      N/A      Disabled
2076     676      svchost.exe      0xad8187b94080      10      -      0      False      2023-05-21 22:28:19.000000      N/A      Disabled
2144     676      vmtoolsd.exe      0xad81896ab080      11      -      0      False      2023-05-21 22:28:19.000000      N/A      Disabled
2152     676      vm3dservice.ex      0xad81896ae240      2      -      0      False      2023-05-21 22:28:19.000000      N/A      Disabled
2200     676      VAuthService.      0xad81896b3300      2      -      0      False      2023-05-21 22:28:19.000000      N/A      Disabled
2404     2152      vm3dservice.ex      0xad8186619200      2      -      1      False      2023-05-21 22:28:32.000000      N/A      Disabled
3028     676      dllhost.exe      0xad8185907080      12      -      0      False      2023-05-21 22:29:20.000000      N/A      Disabled
832      676      msdtc.exe      0xad8185861280      9      -      0      False      2023-05-21 22:29:25.000000      N/A      Disabled
1222     676      eurhost.exe      0xad818586127a      7      -      0      False      2023-05-21 22:29:39.000000      N/A      Disabled
```

3525	3580	vmtoolsd.exe	0xad8189796300	8	-	1	False	2023-05-21 22:31:59.000000	N/A	Disabled		
5136	676	SecurityHealth	0xad81d374280	7	-	0	False	2023-05-21 22:32:01.000000	N/A	Disabled		
5328	3580	msedge.exe	0xad81bd098c0	54	-	1	False	2023-05-21 22:32:02.000000	N/A	Disabled		
4396	5328	msedge.exe	0xad81bd515080	7	-	1	False	2023-05-21 22:32:19.000000	N/A	Disabled		
1144	5328	msedge.exe	0xad81bd7f5080	18	-	1	False	2023-05-21 22:32:38.000000	N/A	Disabled		
4544	5328	msedge.exe	0xad81bd75b080	14	-	1	False	2023-05-21 22:32:39.000000	N/A	Disabled		
5340	5328	msedge.exe	0xad81bd7b3080	10	-	1	False	2023-05-21 22:32:39.000000	N/A	Disabled		
5704	824	RuntimeBroker.	0xad8185962080	5	-	1	False	2023-05-21 22:32:44.000000	N/A	Disabled		
1764	824	dllhost.exe	0xad81bd176080	7	-	1	False	2023-05-21 22:32:48.000000	N/A	Disabled		
1916	824	SearchApp.exe	0xad81bd099080	24	-	1	False	2023-05-21 22:33:05.000000	N/A	Disabled		
6200	676	SgrmBroker.exe	0xad81bd09f080	7	-	0	False	2023-05-21 22:33:42.000000	N/A	Disabled		
6696	676	svchost.exe	0xad81bc532080	8	-	0	False	2023-05-21 22:34:07.000000	N/A	Disabled		
7312	824	ApplicationFra	0xad818e84f300	10	-	1	False	2023-05-21 22:35:44.000000	N/A	Disabled		
7772	676	svchost.exe	0xad81e8e1e140	3	-	0	False	2023-05-21 22:36:03.000000	N/A	Disabled		
6724	3580	Outline.exe	0xad81e578080	0	-	1	True	2023-05-21 22:36:09.000000	2023-05-21 23:01:24.000000	Disabled		
4224	6724	Outline.exe	0xad81e88b080	0	-	1	True	2023-05-21 22:36:23.000000	2023-05-21 23:01:24.000000	Disabled		
7160	824	SearchApp.exe	0xad81bcc4080	57	-	1	Home	False	2023-05-21 22:39:13.000000	N/A	Disabled	
4628	6724	tun2socks.exe	0xad81de823240	0	-	1	True	2023-05-21 22:40:10.000000	2023-05-21 23:01:24.000000	Disabled		
6048	448	taskhostw.exe	0xad81bd50800	5	-	1	False	2023-05-21 22:40:20.000000	N/A	Disabled		
8264	824	RuntimeBroker.	0xad81beec080	4	-	1	False	2023-05-21 22:40:33.000000	N/A	Disabled		
3608	676	svchost.exe	0xad81bd70a080	3	-	0	False	2023-05-21 22:41:28.000000	N/A	Disabled		
6644	824	SkypeApp.exe	0xad81bd3ac080	49	-	1	False	2023-05-21 22:41:52.000000	N/A	Disabled		
5565	824	RuntimeBroker.	0xad8176e0800	0	-	1	False	2023-05-21 21:58:19.000000	2023-05-21 22:02:01.000000	Disabled		
8952	824	TextInputHost.	0xad81beed0b00	10	-	1	False	2023-05-21 21:59:11.000000	N/A	Disabled		
5808	824	HxTsr.exe	0xad81bd5d080	0	-	1	False	2023-05-21 21:59:58.000000	2023-05-21 22:07:45.000000	Disabled		
2388	5328	msedge.exe	0xad81e54c340	18	-	1	False	2023-05-21 22:05:35.000000	N/A	Disabled		

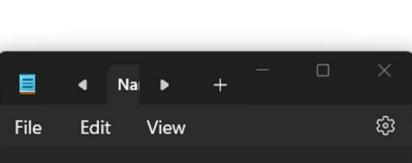
Command : Sudo python3 vol.py -f MemoryDump.mem windows.pslist
Tun2socks is the child process of outlook.exe

tun2socks is [used to "socksify" TCP \(IPv4 and IPv6\) connections at the network layer](#). It implements a TUN virtual network interface which accepts all incoming TCP connections (regardless of destination IP), and forwards them through a SOCKS server.

 [Google Code](https://code.google.com/archive/badvpn/wikis/tu...)
https://code.google.com/archive/badvpn/wikis/tu... : :

[tun2socks.wiki - badvpn - Google Code](#)

Learn what words mean as you search



Name: Ishan Aakash Patel
StudentID: 146151238

Ln 2, Col 21 | 45 characters | 100% | Window | UTF-8

Answer : tun2socks.exe

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

```
sansforensics@siftworkstation: ~/volatility3
$ sudo python3 vol.py -f MemoryDump.mem windows.netscan
Volatility 3 Framework 2.7.1
Progress: 100.00          PDB scanning finished
Offset Proto LocalAddr      LocalPort    ForeignAddr   ForeignPort  State   PID  Owner   Created
0xad81861e2310 TCPv4  0.0.0.0 49668  0.0.0.0 0    LISTENING  1840  spoolsv.exe 2023-05-21 22:28:09.000000
0xad81861e2310 TCPv6  ::    49668  ::    0    LISTENING  1840  spoolsv.exe 2023-05-21 22:28:09.000000
0xad81861e2470 TCPv4  0.0.0.0 5040  0.0.0.0 0    LISTENING  1196  svchost.exe 2023-05-21 22:30:31.000000
0xad81861e2730 TCPv4  0.0.0.0 135   0.0.0.0 0    LISTENING  952   svchost.exe 2023-05-21 22:27:36.000000
0xad81861e2b50 TCPv4  0.0.0.0 49665 0.0.0.0 0    LISTENING  552   wininit.exe 2023-05-21 22:27:36.000000
0xad81861e2b50 TCPv6  ::    49665  ::    0    LISTENING  552   wininit.exe 2023-05-21 22:27:36.000000
0xad81861e2e10 TCPv4  0.0.0.0 49665 0.0.0.0 0    LISTENING  552   wininit.exe 2023-05-21 22:27:36.000000
0xad81861e3230 TCPv4  0.0.0.0 49664 0.0.0.0 0    LISTENING  696   lsass.exe 2023-05-21 22:27:36.000000
0xad81861e3390 TCPv4  0.0.0.0 135   0.0.0.0 0    LISTENING  952   svchost.exe 2023-05-21 22:27:36.000000
0xad81861e3390 TCPv6  ::    135   ::    0    LISTENING  952   svchost.exe 2023-05-21 22:27:36.000000
0xad81861e34f0 TCPv4  0.0.0.0 49664 0.0.0.0 0    LISTENING  696   lsass.exe 2023-05-21 22:27:36.000000
0xad81861e34f0 TCPv6  ::    49664  ::    0    LISTENING  696   lsass.exe 2023-05-21 22:27:36.000000
0xad81861e34f0 TCPv4  0.0.0.0 49664 0.0.0.0 0    LISTENING  696   lsass.exe 2023-05-21 22:27:36.000000
0xad81861e37b0 TCPv4  0.0.0.0 49666 0.0.0.0 0    LISTENING  1012  svchost.exe 2023-05-21 22:27:49.000000
0xad81861e37b0 TCPv6  ::    49666  ::    0    LISTENING  1012  svchost.exe 2023-05-21 22:27:49.000000
0xad81861e3910 TCPv4  0.0.0.0 49667 0.0.0.0 0    LISTENING  448   svchost.exe 2023-05-21 22:27:58.000000
0xad81861e3910 TCPv6  ::    49667  ::    0    LISTENING  448   svchost.exe 2023-05-21 22:27:58.000000
0xad81861e3a70 TCPv4  0.0.0.0 49668 0.0.0.0 0    LISTENING  1840  spoolsv.exe 2023-05-21 22:28:09.000000
0xad81861e3b00 TCPv4  0.0.0.0 49666 0.0.0.0 0    LISTENING  1012  svchost.exe 2023-05-21 22:27:49.000000
0xad81861e3e90 TCPv4  0.0.0.0 49667 0.0.0.0 0    LISTENING  448   svchost.exe 2023-05-21 22:27:58.000000
0xad818662ecb0 TCPv4  0.0.0.0 445   0.0.0.0 0    LISTENING  4     System 2023-05-21 22:29:04.000000
0xad818662ecb0 TCPv6  ::    445   ::    0    LISTENING  4     System 2023-05-21 22:29:04.000000
0xad818662f390 TCPv4  0.0.0.0 7680  0.0.0.0 0    LISTENING  5476  svchost.exe 2023-05-21 22:58:09.000000
0xad818662f390 TCPv6  ::    7680  ::    0    LISTENING  5476  svchost.exe 2023-05-21 22:58:09.000000
0xad81878518f0 UDPv4  192.168.190.141 138   *    0    LISTENING  4     System 2023-05-21 22:27:56.000000
0xad8187852250 UDPv4  192.168.190.141 137   *    0    LISTENING  4     System 2023-05-21 22:27:56.000000
0xad818902a5d0 TCPv4  192.168.190.141 139   0.0.0.0 0    LISTENING  4     System 2023-05-21 22:27:56.000000
0xad818971f870 UDPv4  0.0.0.0 56250  *    0    LISTENING  6644  SkypeApp.exe 2023-05-21 22:58:07.000000
0xad818971f870 UDPv6  ::    56250  *    0    LISTENING  6644  SkypeApp.exe 2023-05-21 22:58:07.000000
0xad81897eb010 TCPv4  10.0.85.2   55439  20.22.207.36  443   CLOSED 448   svchost.exe 2023-05-21 23:00:40.000000
0xad81898a6d10 UDPv4  127.0.0.1   57787  *    0    LISTENING  448   svchost.exe 2023-05-21 22:28:54.000000
0xad81898bc7f0 UDPv4  0.0.0.0 5355  *    0    LISTENING  1448  svchost.exe 2023-05-21 22:57:37.000000
0xad81898bc7f0 UDPv6  ::    5355  *    0    LISTENING  1448  svchost.exe 2023-05-21 22:57:37.000000
0xad8189a291b0 TCPv4  0.0.0.0 55972 0.0.0.0 0    LISTENING  5964  svchost.exe 2023-05-21 22:27:57.000000
0xad8189a291b0 TCPv6  ::    55972  ::    0    LISTENING  5964  svchost.exe 2023-05-21 22:27:57.000000
0xad8189a29470 TCPv4  0.0.0.0 55972 0.0.0.0 0    LISTENING  5964  svchost.exe 2023-05-21 22:27:57.000000

0xad8180a21000 UDPv4  0.0.0.0 0    *    0    5964  svchost.exe 2023-05-21 22:27:57.000000
0xad8180bc1a600 UDPv4  192.168.190.141 49713  104.119.188.96 443   CLOSE_WAIT 1916  SearchApp.exe 2023-05-21 22:33:11.000000
0xad818d05370 UDPv4  0.0.0.0 5353  *    0    5328  msedge.exe 2023-05-21 23:01:32.000000
0xad818d07440 UDPv4  0.0.0.0 5353  *    0    5328  msedge.exe 2023-05-21 23:01:32.000000
0xad818d0d67440 UDPv6  ::    5353  *    0    5328  msedge.exe 2023-05-21 23:01:32.000000
0xad818de4a20 TCPv4  10.0.85.2   55462  77.91.124.20  80    CLOSED 5896  oneetx.exe 2023-05-21 23:01:22.000000
0xad818d0f10220 TCPv4  192.168.190.141 53435  35.121.43.05  443   CLOSED 4028  lumsacks.exe 2023-05-21 23:00:02.000000
0xad818e3698f0 UDPv4  0.0.0.0 5353  *    0    5328  msedge.exe 2023-05-21 22:05:24.000000
0xad818e3701a0 UDPv4  0.0.0.0 5353  *    0    5328  msedge.exe 2023-05-21 22:05:24.000000
0xad818e3701a0 UDPv6  ::    5353  *    0    5328  msedge.exe 2023-05-21 22:05:24.000000
0xad818e370b00 UDPv4  0.0.0.0 5353  *    0    5328  msedge.exe 2023-05-21 22:05:24.000000
0xad818e371dc0 UDPv4  0.0.0.0 5353  *    0    5328  msedge.exe 2023-05-21 22:05:24.000000
0xad818e371dc0 UDPv6  ::    5353  *    0    5328  msedge.exe 2023-05-21 22:05:24.000000
0xad818e3a1200 UDPv4  0.0.0.0 5355  *    0    1448  svchost.exe 2023-05-21 22:57:37.000000
0xad818e4a6900 UDPv4  0.0.0.0 0    *    0    5480  oneetx.exe 2023-05-21 22:39:47.000000
0xad818e4a6900 UDPv6  ::    0    *    0    5480  oneetx.exe 2023-05-21 22:39:47.000000
0xad818e4a9650 UDPv4  0.0.0.0 0    *    0    5480  oneetx.exe 2023-05-21 22:39:47.000000
0xad818e77da20 TCPv4  192.168.190.141 52434  204.79.197.200 443   CLOSED -  - 2023-05-21 23:02:20.000000
0xad818ef06c70 UDPv4  fe80::4a06:8c42:43a9:413 1900   *    0    3004  svchost.exe 2023-05-21 22:40:16.000000
0xad818ef09b50 UDPv6  fe80::4577:874:81a:78cd 1900   *    0    3004  svchost.exe 2023-05-21 22:40:16.000000
```

File Edit View

Name: Ishan Aakash Patel
StudentID: 146151238

Ln 2, Col 21 | 45 characters | 100% | Window | UTF-8

File Edit View

Name: Ishan Aakash Patel
StudentID: 146151238

Ln 2, Col 21 | 45 characters | 100% | Window | UTF-8

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

```
sansforensics@siftworkstation: ~/volatility3
$ sudo python3 vol.py -f MemoryDump.mem windows.dumpfiles --pid 5896
Volatility 3 Framework 2.7.1
Progress: 100.00          PDB scanning finished
Cache   FileObject      FileName        Result
ImageSectionObject 0xad818e37b8e0  AcLayers.dll    file.0xad818e37b8e0.0xad818ea09d00.ImageSectionObject.AcLayers.dll.img
ImageSectionObject 0xad818da36c30  oneetx.exe     file.0xad818da36c30.0xad818ca48660.ImageSectionObject.oneetx.exe.img
ImageSectionObject 0xad818e48a450  sfc.dll       Error dumping file
DataSectionObject 0xad81876b7860  R0000000000006.clb  Error dumping file
DataSectionObject 0xad8187a70b60  cversions.2.db   file.0xad8187a70b60.0xad8187ba3070.DataSectionObject.cversions.2.db.dat
ImageSectionObject 0xad8189ce9740  profapi.dll   file.0xad8189ce9740.0xad818c027ba0.ImageSectionObject.profapi.dll.img
ImageSectionObject 0xad818d44ca70  IPHLAPI.DLL   file.0xad818d44ca70.0xad818d33fc0.ImageSectionObject.IPHLAPI.DLL.img
ImageSectionObject 0xad818f88a770  OnDemandConnRouteHelper.dll file.0xad818f88a770.0xad818e0c8d30.ImageSectionObject.OnDemandConnRouteHelper.dll.img
ImageSectionObject 0xad818c3c0a90  winhttp.dll   file.0xad818c3c0a90.0xad818ce43a20.ImageSectionObject.winhttp.dll.img
ImageSectionObject 0xad818d43ce00  HarddiskVolume31.i.mnu Error dumping file
ImageSectionObject 0xad818e21130  edputil.dll   Error dumping file
ImageSectionObject 0xad818e4849b0  srvccli.dll   Error dumping file
ImageSectionObject 0xad818ef239d0  netutil.dll    Error dumping file
ImageSectionObject 0xad818e384bc0  mpr.dll      Error dumping file
ImageSectionObject 0xad81861b3ce0  msrvct.dll   file.0xad81861b3ce0.0xad81863d0d60.ImageSectionObject.msrvct.dll.img
ImageSectionObject 0xad81898a1150  HarddiskVolume31.mnu file.0xad81898a1150.0xad8189706730.ImageSectionObject.HarddiskVolume31.mnu
ImageSectionObject 0xad818d43f780  uxtheme.dll   file.0xad818d43f780.0xad818cf17a20.ImageSectionObject.uxtheme.dll.img
ImageSectionObject 0xad81861b20c0  msvcp_win.dll file.0xad81861b20c0.0xad818618f010.ImageSectionObject.msvcp_win.dll.img
ImageSectionObject 0xad81861b39c0  bcryptprimitives.dll file.0xad81861b39c0.0xad81863d1d60.ImageSectionObject.bcryptprimitives.dll.img
ImageSectionObject 0xad81861b30a0  nst.dll      file.0xad81861b30a0.0xad81863d2b60.ImageSectionObject.nst.dll.img
ImageSectionObject 0xad81861b3380  clbcatq.dll file.0xad81861b3380.0xad818618e270.ImageSectionObject.clbcatq.dll.img
ImageSectionObject 0xad81861b3830  advapi32.dll file.0xad81861b3830.0xad818618e010.ImageSectionObject.advapi32.dll.img
ImageSectionObject 0xad81861a8570  ws2_32.dll   file.0xad81861a8570.0xad818618dc30.ImageSectionObject.ws2_32.dll.img
ImageSectionObject 0xad81861a9510  user32.dll   file.0xad81861a9510.0xad81861917b0.ImageSectionObject.user32.dll.img
ImageSectionObject 0xad81861a99c0  shlwapi.dll file.0xad81861a99c0.0xad8186195750.ImageSectionObject.shlwapi.dll.img
ImageSectionObject 0xad81861a99b0  KernelBase.dll file.0xad81861a99b0.0xad818618d010.ImageSectionObject.KernelBase.dll.img
ImageSectionObject 0xad81861a8ed0  setupapi.dll Error dumping file
ImageSectionObject 0xad81861a9e70  sechost.dll file.0xad81861a9e70.0xad8186195c10.ImageSectionObject.sechost.dll.img
ImageSectionObject 0xad81861a96a0  gdi32full.dll file.0xad81861a96a0.0xad8186191c70.ImageSectionObject.gdi32full.dll.img
ImageSectionObject 0xad81861a91f0  ucrtbase.dll file.0xad81861a91f0.0xad81863dd60.ImageSectionObject.ucrtbase.dll.img
ImageSectionObject 0xad81861a8700  imm32.dll   file.0xad81861a8700.0xad8186191a10.ImageSectionObject.imm32.dll.img
ImageSectionObject 0xad81863b6250  win32u.dll  file.0xad81863b6250.0xad81863dd60.ImageSectionObject.win32u.dll.img
ImageSectionObject 0xad81861a9ec0  combase.dll file.0xad81861a9ec0.0xad8186191050.ImageSectionObject.combase.dll.img
0xad81861a9380  cfmonr32.dll file.0xad81861a9380.0xad8186191550.ImageSectionObject.cfmonr32.dll.img
```

Marks

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

```
sansforensics@siftworkstation: ~/volatility3
$ ls | grep one
file.0xad818da36c30.0xad818ca48660.ImageSectionObject.oneetx.exe.img
sansforensics@siftworkstation: ~/volatility3
$
```

Name: Ishan Aakash Patel
StudentID: 146151238

Ln 2, Col 21 | 45 characters | 100% | Window | UTF-8

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.

Google search results for IP: 77.91.124.20:

- MalwareBazaar Database - Abuse.ch**
Jun 3, 2023 — File size: 796'160 bytes. First seen: 2023-06-03 21:26:47 UTC. Last seen: Never.
File type: Executable exe. MIME type: application/x-dosexec.
- IPinfo**
https://ipinfo.io > ...
77.91.124.0/24 IP range details - IPinfo.io
77.91.124.0/24 IP address block information: WHOIS details, hosted domains and IP addresses in this range.
- ANY.RUN**
https://any.run > report
FC0B222DE370EF4C55C6697C...
IP. URL. CN. Type. Size. Reputation. 3068. oneetx.exe. GET. 404. **77.91.124.20:80**.
http://77.91.124.20/store/games/Plugins/cred64.dll ... IP. Domain. ASN. CN.
- WhatIsMyIP.com**
https://www.whatismyip.com > asn
AS203727 77.91.124.0/24 IP Range / CIDR Information - ...
77.91.124.0/24 CIDR and IP Range data shows number of IP addresses, number of addressable

MALWARE bazaar

MalwareBazaar Database

You are currently viewing the MalwareBazaar entry for **SHA256 74b102111f7d344a2c0cb7a77d73c968aff7f6a4b67c3457643d9a61c12d2aef**. To identify whether the sample provided is malicious or not, there is no guarantee that a sample in MalwareBazaar is malicious.

Database Entry

RedLineStealer

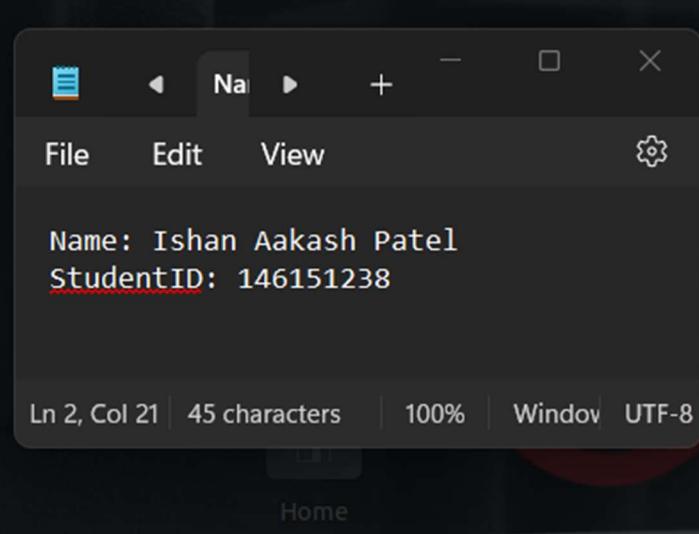
Vendor detections: 19

Intelligence 19 | IOCs | YARA 3 | File information | Comments 1 | Actions ▾

Answer : RedLine Stealer

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

```
sansforensics@siftworkstation: ~/volatility3
$ strings MemoryDump.mem | grep 77.91.124.20
http://77.91.124.20/ E
77.91.124.20/stor
http://77.91.124.20/store/gamel
http://77.91.124.20/store/games/i
77.91.124.20
http://77.91.124.20/ E
http://77.91.124.20/DSC01491/
77.91.124.20
http://77.91.124.20/DSC01491/
http://77.91.124.20/store/games/index.php
77.91.124.20
77.91.124.20
77.91.124.20
77.91.124.20
77.91.124.20
http://77.91.124.20/store/games/index.php
http://77.91.124.20/store/games/index.php
sansforensics@siftworkstation: ~/volatility3
$
```

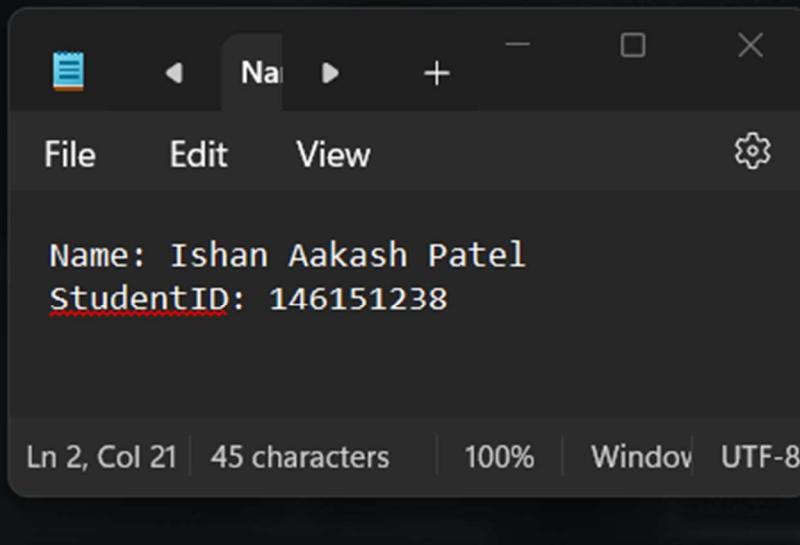


Command : strings MemoryDump.mem | grep 77.91.124.20

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

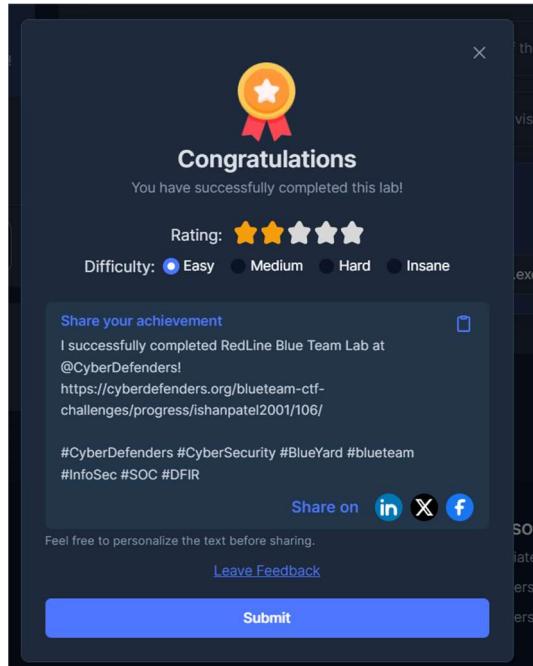
8. What is the full path of the malicious executable? – 5 Marks

```
sansforensics@siftworkstation: ~/volatility3
$ sudo python3 vol.py -f MemoryDump.mem windows.filescan | grep -i "oneetx.exe"
0xad818d436c70.0\Users\Tammam\AppData\Local\Temp\c3912af058\oneetx.exe 216
0xad818da36c30 \Users\Tammam\AppData\Local\Temp\c3912af058\oneetx.exe 216
0xad818ef1a0b0 \Users\Tammam\AppData\Local\Temp\c3912af058\oneetx.exe 216
```



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...

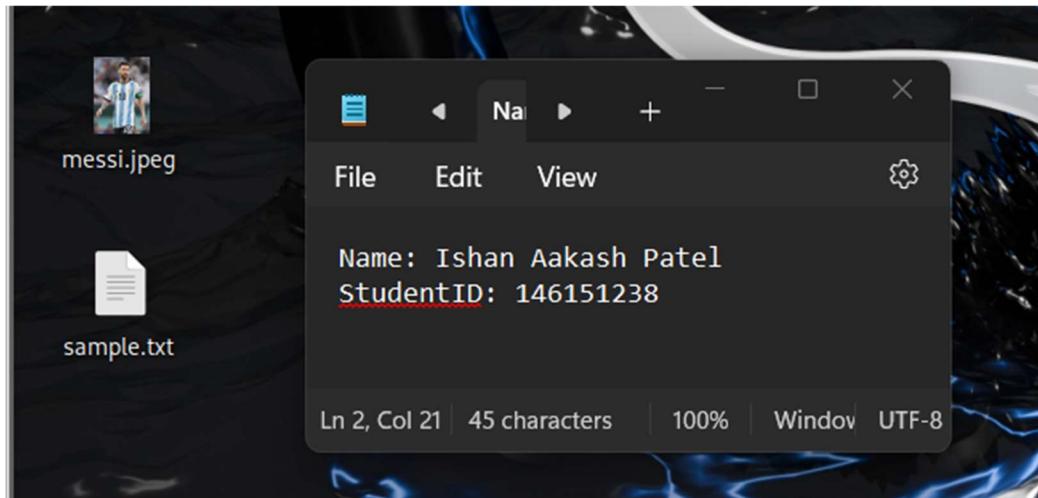
Part – 2 Steganography

Task – 1

Embedding malware into an image...

Step 1 - Install Steghide

Sample try...



Sample.txt

A screenshot of a terminal window titled 'kali@kali: ~/Desktop'. The terminal shows the following session:

```
File Actions Edit View Help
└─(kali㉿kali)-[~]
$ cd Desktop
└─(kali㉿kali)-[~/Desktop]
$ cat sample.txt
Hi my name is Ishan
$
```

Below the terminal, a file viewer window is open, showing the same text content as the terminal:

```
Name: Ishan Aakash Patel  
StudentID: 146151238
```

The status bar at the bottom of the file viewer window shows 'Ln 2, Col 21 | 45 characters | 100% | Window | UTF-8'.

A screenshot of a Kali Linux desktop environment. At the top, there is a dock with icons for Home, Kali, Android, and SIFT. Below the dock is a taskbar with several open windows: Home, Kali, Android, SIFT, and a terminal window. The terminal window shows the command `steghide embed -ef sample.txt -cf messi.jpeg` being run, followed by prompts for a passphrase and confirmation of embedding success. A file viewer window is also visible, displaying the contents of the `messi.jpeg` file, which contains the text "Name: Ishan Aakash Patel" and "StudentID: 146151238". The status bar at the bottom of the terminal window indicates "Ln 2, Col 21 | 45 characters | 100% | Window | UTF-8".

```
(kali㉿kali)-[~/Desktop]
$ steghide embed -ef sample.txt -cf messi.jpeg
Enter passphrase:
Re-Enter passphrase:
embedding "sample.txt" in "messi.jpeg" ... done
(kali㉿kali)-[~/Desktop]
$
```

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

Now we will extract it....

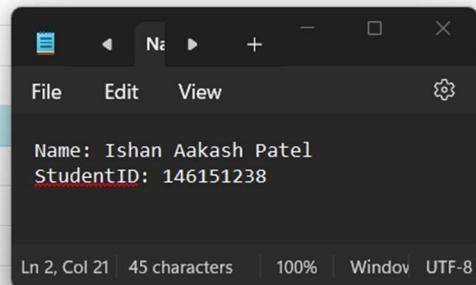
A screenshot of a Kali Linux desktop environment. At the top, there is a dock with icons for Home, Kali, Android, and SIFT. Below the dock is a taskbar with several open windows: Home, Kali, Android, SIFT, and a terminal window. The terminal window shows the command `steghide extract -sf messi.jpeg` being run, followed by a prompt for a passphrase and a confirmation message about overwriting an existing file. A file viewer window is also visible, displaying the contents of the `messi.jpeg` file, which contains the text "Name: Ishan Aakash Patel" and "StudentID: 146151238". The status bar at the bottom of the terminal window indicates "Ln 2, Col 21 | 45 characters | 100% | Window | UTF-8".

```
(kali㉿kali)-[~/Desktop]
$ steghide extract -sf messi.jpeg
Enter passphrase:
the file "sample.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "sample.txt".
(kali㉿kali)-[~/Desktop]
$
```

Command : `steghide extract -df messi.jpeg`

Now we will try using a real malware...

Intelligence	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...

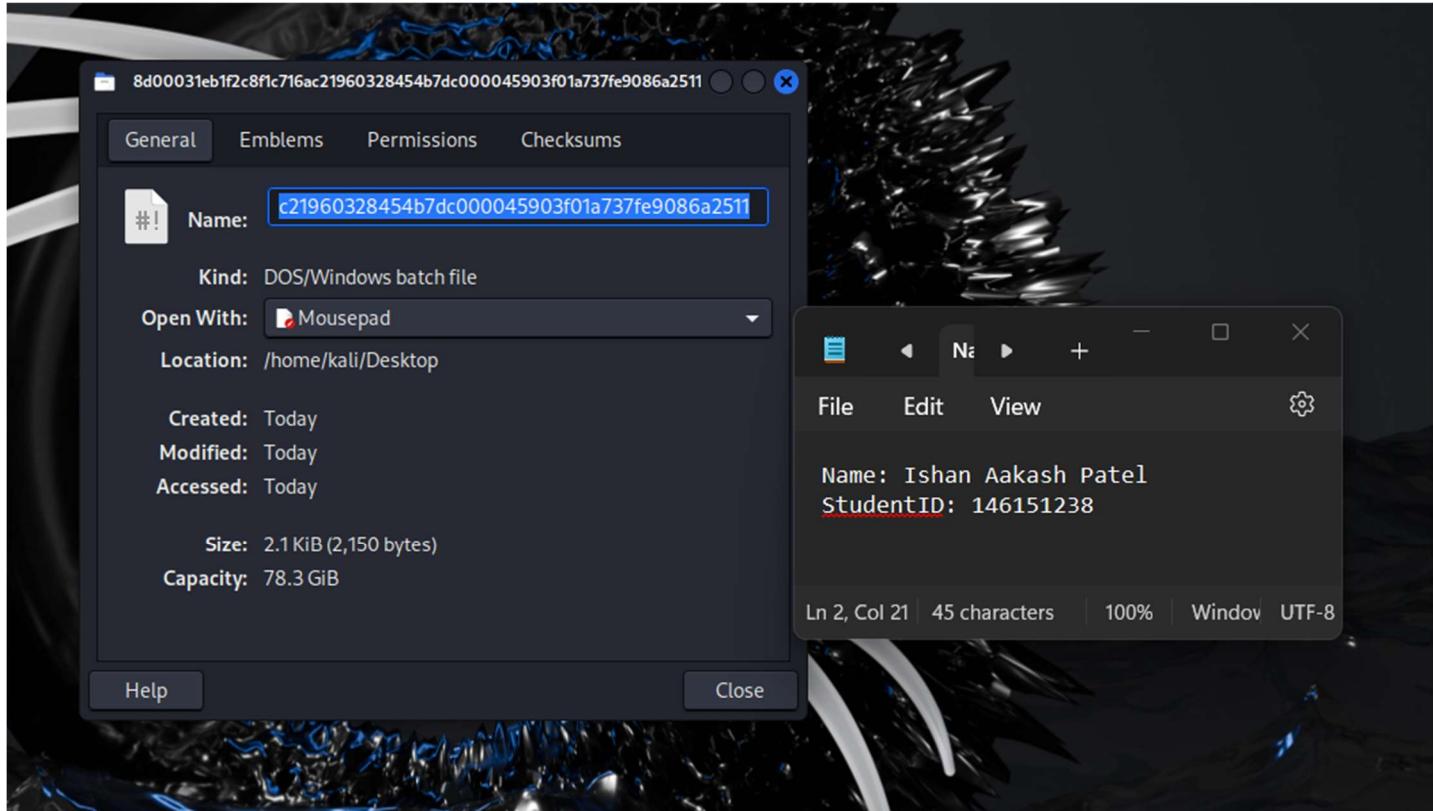
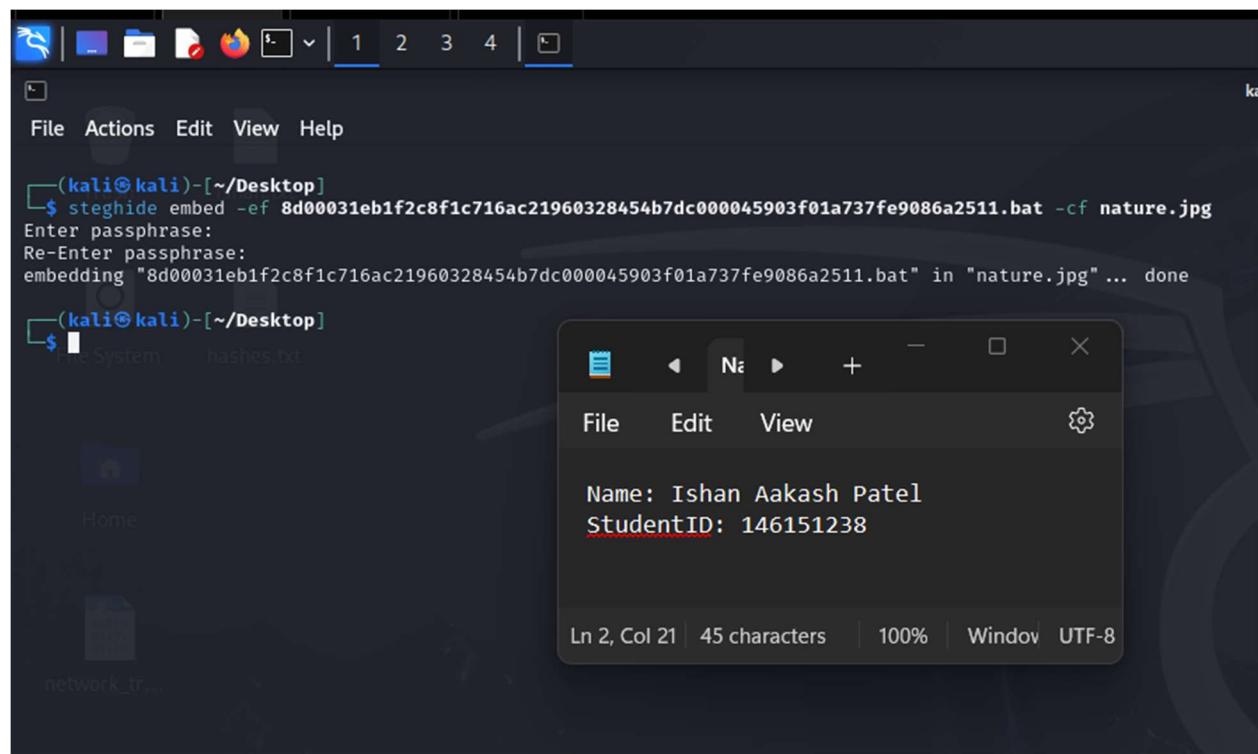
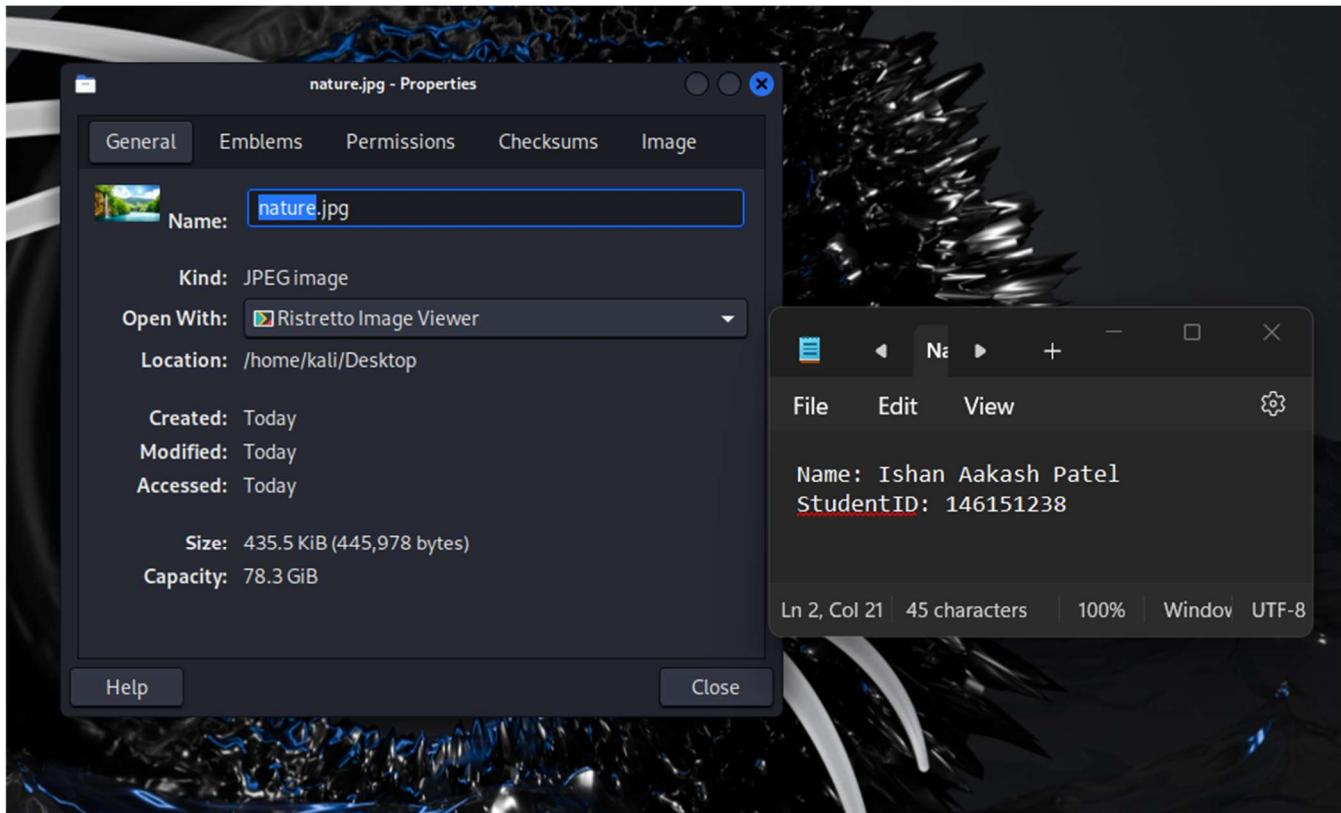


Image info



Malware embedded...

Task 2 – Detecting the malware....

Now we will extract it...

```
(kali㉿kali)-[~/Desktop]
$ steghide extract -sf nature.jpg
Enter passphrase:
the file "8d00031eb1f2c8f1c716ac21960328454b7dc000045903f01a737fe9086a2511.bat" does already exist. overwrite ? (y/n) y
wrote extracted data to "8d00031eb1f2c8f1c716ac21960328454b7dc000045903f01a737fe9086a2511.bat".
```

```
(kali㉿kali)-[~/Desktop]
$
```

Check the file in VirusTotal

VirusTotal - File - 8d00031eb1f2c8f1c716ac21960328454b7dc000045903f01a737fe9086a2511

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Σ URL, IP address, domain or file hash

Community Score 26 / 62

26/62 security vendors flagged this file as malicious

8d00031eb1f2c8f1c716ac21960328454b7dc000045903f01a737fe9086a2511

27114108223285603.bat

text idle long-sleeps

DETECTION DETAILS BEHAVIOR COMMUNITY 6

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.agentsetter/cryp Threat categories trojan Family labels agentsetter cryp

File Edit View

Name: Ishan Aakash Patel
StudentID: 146151238

Size 2.10 KB Last Analysis Date 5 hours ago

TXT

Ln 2, Col 21 | 45 characters | 100% | Window | UTF-8

Security vendors' analysis

Vendor	Analysis	Family	Notes
AhnLab-V3	Trojan/BAT.Obfuscated.S2825	AliCloud	Trojan:Unknown/AgentSetter.SBPHU
ALYac	Trojan.GenericKD.73467302	Avast	BV:Obfuscated-AA [Cryp]
AVG	BV:Obfuscated-AA [Cryp]	BitDefender	Trojan.GenericKD.73467302
Emsisoft	Trojan.GenericKD.73467302 (B)	eScan	Trojan.GenericKD.73467302
GData	Trojan.GenericKD.73467302	Google	Detected

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

78°F Mostly sunny

Search

8/13/2024 19:40 ENG IN

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

ETH Price: \$2,695.68 (-1.01%) Gas: 1.235 Gwei

Search by Address / Txn Hash / Block / Token / Domain Name



Result for: gautamgg.eth

Domain Name Lookup / Search Results

Overview of ENS

② Resolved Address:	0x607fe8Ce38097A3e71acBE1FD814bbb0D65C46c3	
② Expiration Date:	2028.05.11 at 23:44	
② Registrant:	0xD4416b13d2b3a9aBae7AcD5D6C2BbDBE25686401	
② Controller:	0xD4416b13d2b3a9aBae7AcD5D6C2BbDBE25686401	
+ Click to show more		

```
Name: Ishan Aakash Patel  
StudentID: 146151238  
Ln 2, Col 21 | 45 characters | 100% | Window | UTF-8
```

Related Transactions

Transaction Hash	Age	From	Action
0x1fe7f704f67...	459 days ago	0x607fe8Ce...0D65C46c3	register

This website uses cookies to improve your experience. By continuing to use this website, you agree to its [Terms](#) and [Privacy Policy](#).

[Got it!](#)

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
0x1fe7f704f676df90b30226d3d44cc7affbdcaa96860b8745140f977fe80edd0a		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
2ipqDYRCV5APGromyDHYJw7HfX3SqrEpf1kQqa11qNBFhE24NocMYLmsHNu...	281,371,224	14 days ago	Aug 3, 2024, 19:03:53 UTC	Success
59jFRnGs5snxbwR6KMDrXdnUCWfqQxAZve7T4w1ZJA4j2ZM2LNMZgAw1ewg...	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.

The screenshot shows the Solana Explorer interface for the wallet address BzTD2xNUedEfCkkKYaX8C6gz4LZskN1RpGdunS7NDUSU. The main page displays the following information:

- Address:** BzTD2xNUedEfCkkKYaX8C6gz4LZskN1RpGdunS7NDUSU
- Balance (SOL):** 0.375716642 SOL
- Allocated Data Size:** 0 byte(s)
- Assigned Program Id:** System Program
- Executable:** No

Below this, the "Domains" tab is selected, showing two owned domain names:

DOMAIN NAME	NAME SERVICE ACCOUNT
14785.sol	6UcaTJERhuX19t975cJBeQzLz7z5wSggoRPA4JsMfdnH
gautamgg.sol	E2ZJZLH28yqQ7rnzTKzfRAJ98T7NRJA3bJdt3W17okNo

A modal window is open over the interface, displaying personal information:

Name: Ishan Aakash Patel
StudentID: 146151238

The bottom of the screen shows the Windows taskbar with various pinned icons and system status indicators.

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
2ipqDYRCV5APGromyDHYJw7HfX3SqrEpf1kQqa11qNBFlE24NocMYLmsHNu...	281,371,224	Aug 3, 2024, 19:03:53 UTC	N/A	N/A
59jFRnGs5snxbwR6KMDrXdnUCWfqQxAZve7T4w1ZJA4j2ZM2LNMZgAw1ewg...	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.

Transaction History					
TRANSACTION SIGNATURE	BLOCK	AGE	TIMESTAMP	RESULT	
2ipqDYRCV5APGromyDHYJw7HfX3SqrffEpf1kQqa11qNBfH24NocMYLmsHNu...	281,371,224	10 days ago	Aug 3, 2024 at 19:03:53 UTC	Success	
59jFrnG5snxvbwR6KMDrXdnUCWfqQxAZve7T4w1ZJA4j2ZM2LNMZgAw1ewg...	280,928,040	12 days ago	Aug 1, 2024 at 12:26:01 UTC	Success	
SnKBVJfvmKn7MzFs2uh9xjygh3K8HHBv3CvwqTa3UcR3Luf167bXRLa2r7Nm...	280,784,508	13 days ago	Jul 31, 2024 at 18:47:41 UTC	Success	
5DqDjY3PUTW5EEYaq5LVgh9dTXUF4srNfqalqJ76XXtdXqzoc2gdrxujj5e...	280,784,420	13 days ago	Jul 31, 2024 at 18:47:02 UTC	Success	
5bep9WlyZFwlLvxMaeW6P7eQfd053r4ZamjXoRkknoFdxoam6Tem4XETExuPG...	280,332,728	16 days ago	Jul 29, 2024 at 10:41:14 UTC	Success	
K2Whlw9gdw8rf5w6FCa1gH5yvDitGmbbVPMQDXdFcgeAjWgumbvqJpwFanvR...	280,332,629	16 days ago	Jul 29, 2024 at 10:40:29 UTC	Success	
4a6aLcuXPVHwYeeU5pa219fL5H1yKQmjPggVkw1lqi7qcccKqpYzqVeVn2E...	280,331,653	16 days ago	Jul 29, 2024 at 10:32:57 UTC	Success	
2kk66sF4k2V5YpwijFMqrgaW45mktPp5YLQqPL9t9YZjgFpw9GiHS7YcNAQM...	277,717,207	a month ago	Jul 15, 2024 at 16:26:32 UTC	Success	
2NxRyS3riKSXLmgmFvd2jy4RY8w3t1Bq07b2uzZtnCA9hcFgBcddpzvkrYwb...	277,717,120	a month ago	Jul 15, 2024 at 16:25:54 UTC	Success	
g23mkMtLE9twEpgkPER6xrL6DeWxE548N3aek5TB9r1FgxHC5f4pY6PE3tDm...	277,717,107	a month ago	Jul 15, 2024 at 16:25:48 UTC	Success	
31ndaJHvq7VbYvSgSaAqXLnsJzn7voaU6dQaSqCzbm7LL39wM2Qzs39p6CF2...	277,716,209	a month ago	Jul 15, 2024 at 16:18:58 UTC	Success	
5HhjU7uALj4yrCrVmGsU9MwFNiEwtsnPnv8VmrgyoqUqxHoHgS6ika2bKCwVq...	277,708,264	a month ago	Jul 15, 2024 at 15:17:35 UTC	Success	

Ethereum Wallet: 0x607fe8Ce38097A3e71acBE1FD814bbb0D65C46c3

Transaction Hash	Date	Recipient Address
0x1fe7f704f676df90b30226d3d44cc7affbdcaa96860b87 45140f977fe80edd0a	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.

Address 0x607fe8Ce38097A3e71acBE1FD814bbb0D65C46c3

Sponsored: Playdoge: Traders Invest \$250,000+ Into PlayDoge, Get in EARLY on this Play to Earn Meme Coin! [Buy \\$Play!](#)

gautamgg.eth

Overview

ETH BALANCE: 4.08935442879989401 ETH

ETH VALUE: \$11,037.67 (@ \$2,699.12/ETH)

TOKEN HOLDINGS: \$306.14 (47 Tokens)

More Info

PRIVATE NAME TAGS: + Add

TRANSACTIONS SENT: Latest: 28 days ago First: 1094 days ago

FUNDED BY: FTX 2 @ tx 0x8e57def58e4...

Multichain Info

\$17,622.22 (Multichain Portfolio)

17 addresses found via Blockscan

Name: Ishan Akash Patel
StudentID: 146151238

etherescan.io/address/0x607fe8Ce38097A3e71acBE1FD814bbb0D65C46c3

ETH Price: \$2,699.12 (-0.88%) Gas: 1.318 Gwei

Search by Address / Txn Hash / Block / Token / Domain Name

Transaction Hash	Method	Block	Age	From	To	Amount	Txn Fee
0xdb992feb3ec...	Set Approval F...	20319266	28 days ago	◇ gautamgg.eth	OUT ↗ 0x56Ca43cb...B73150B07	0 ETH	0.00041518
0xc42300e8a3...	Swap	20310713	29 days ago	◇ gautamgg.eth	OUT ↗ Metamask: Swap ...	0 ETH	0.0010244
0x4a62b7a46...	Release Tokens	20310694	29 days ago	◇ gautamgg.eth	OUT ↗ 0x16b68E1C...5c3B42093	0 ETH	0.00031488
0xdac3dee8a0...	Finalize Withd...	20310650	29 days ago	◇ gautamgg.eth	OUT ↗ Base: Base Portal	0 ETH	0.00034152
0x2cbcbb3c15...	Finalize Withd...	20310647	29 days ago	◇ gautamgg.eth	OUT ↗ PGN: Optimism Po...	0 ETH	0.00060537
0x04837f03266...	Prove Withdra...	20248657	38 days ago	◇ gautamgg.eth	OUT ↗ Base: Base Portal	0 ETH	0.00080766
0x4c7973d382...	Prove Withdra...	20248653	38 days ago	◇ gautamgg.eth	OUT ↗ PGN: Optimism Po...	0 ETH	0.00084979
0x85e2e8ddcb...	0x9ea4733	20206710	44 days ago	◇ gautamgg.eth	OUT ↗ 0x2Ca730EB...6A675B0e4	0 ETH	0.00041639
0xa3b59ba5f0f...	Transfer	200749/5	62 days ago	◇ gautamgg.eth	OUT ↗ Aethir: ATH Token	0 ETH	0.00176014
0xc0f1ce8a32f...	Claim	20074884	62 days ago	◇ gautamgg.eth	OUT ↗ 0x7ca50Eb6...fa34707ca	0 ETH	0.00195564
0x61fd1fdce6e2...	Send Message	19961462	78 days ago	◇ gautamgg.eth	OUT ↗ Taiko: Bridge	0.010026 ETH	0.00177209
0x5b4136cec5...	Relay Messag...	19942055	81 days ago	◇ gautamgg.eth	OUT ↗ Scroll: L1 Scroll M...	0 ETH	0.00078022
0x0afd4bf61fb...				◇ This website uses cookies to improve your experience. By continuing to use this website, you agree to its Terms and Privacy Policy.	Got it!	107 ETH	0.00179043

76°F Sunny

Search

20:10 8/13/2024 ENG IN WiFi Battery

Summary:

- The Solana address BzTD2xNUedEfCkkKYaX8C6gz4LZskN1RpGduS7NDUSU 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)

The collage consists of four screenshots arranged in a 2x2 grid:

- Top Left:** A screenshot of a social media interface showing a deleted post by @Gautamguptagg. The post content is: "BzTD2xNUedEfCkkKYaX8C6gz4LZskN1RpGdunS7NDUSU". It has 11 comments, 10 retweets, and 49 likes. Below it is a reply from Team Singularity (@SNG_Esports) with a link to x.com/lover_minds/st... and a suspended account notice.
- Top Right:** A screenshot of the Solana Explorer (Beta) showing the overview for the address BzTD2xNUedEfCkkKYaX8C6gz4LZskN1RpGdunS7NDUSU. Key details include a balance of 0.10 SOL, 0 byte(s) allocated, and System Program assigned.
- Bottom Left:** A screenshot of a social media interface showing a post by @Gautamguptagg (@Gautamguptagg) replying to @Gautamguptagg. The post content includes a link to app.claystack.com/?r=0x607fe8ce38097A3e71acBE1FD814bbb0D65C46c3 and a referral link. It also mentions invites and NFT rewards.
- Bottom Right:** A screenshot of Etherscan's Domain Name Lookup search results for gautamgg.eth. It shows the resolved address as 0x607fe8Ce38097A3e71acBE1FD814bbb0D65C46c3, the expiration date as 2028.05.11 at 23:44, and the registrant as 0xD4416b13d2b3a9aBae7AcD5D6C2BbDBE25686401.

[←](#) **Gautamgg.eth/sol** 🇮🇳❤️✅
8,158 posts

EXPLORING WEB3.0 \$
CRYPTO SINCE 2017

+ Running with crypto trend

- NFTs
- Airdrops
- Early Projects
- Tips & Tricks
- Crypto News

[Follow](#)

Gautamgg.eth/sol 🇮🇳❤️✅
@Gautamguptagg

🌐 Crypto Since '17 | 🕵️ Analyst & Researcher | ❤️ 250k+ Fam | 💎 Follow Me For Hidden Gem, 🎉 Airdrops | 🚀 Builder | 📚 Advisor | 📡 α - telegram.me/CryptoGG ✅

📝 Education 📈 GG 🌐 linktr.ee/lmsocial 📅 Joined August 2020

1,016 Following 64.8K Followers

Posts Replies Highlights Articles Media

 **Gautamgg.eth/sol** 🇮🇳❤️✅ @Gautamguptagg · Jan 29
Replying to [@dymension](#)
But Wen For Early Adopters (Testnet users) 🎉

...

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

- [Home](#)
- [Prices](#)
- [Charts](#)
- [NFTs](#)
- [DeFi](#)
- [Academy](#)
- [News](#)
- [Developers](#)
- [Wallet](#)
- [Exchange](#)
- [Bitcoin](#)
- [Ethereum](#)
- [Bitcoin Cash](#)

0x607-C46c3

Ethereum Address
0x607fe8Ce38097A3e71acBE1FD814bbb0D65C46c3

Ethereum Balance
4.08935442879989401 • \$10,694.40

USD

Wallet
Tokens

Summary	
Total Received	37.893397579423657808 ETH \$99,098.06
Total Sent	33.110403440738970995 ETH \$86,589.66
Total Fees	0.693639709884792803 ETH \$1,813.99
Nonce	222
Token Portfolio • 27	
Total Volume 71.00380102016262 ETH \$185,687	
Transactions 255 61 Internal Txs	

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.

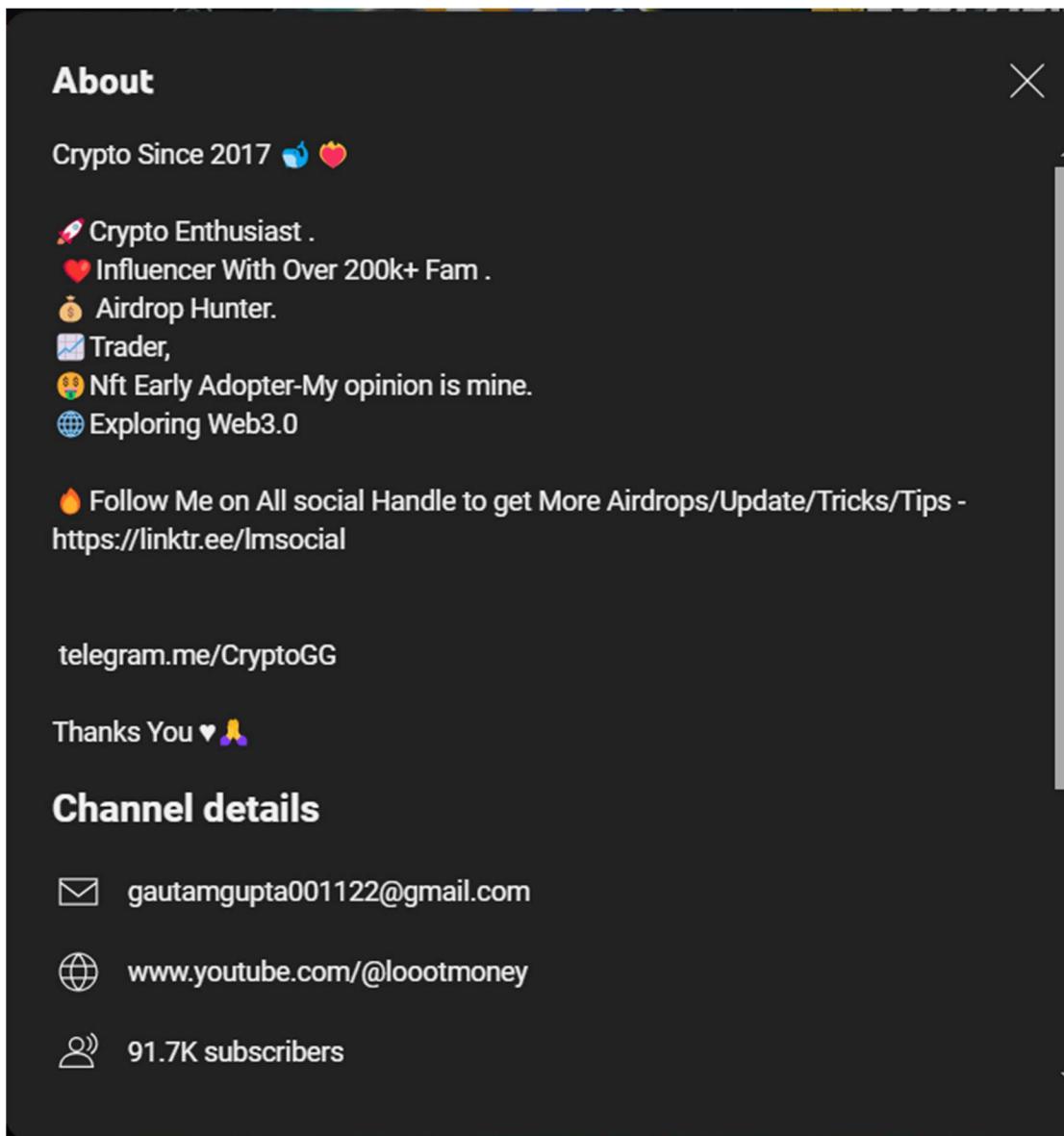
- The profile description indicates that the person is an analyst, researcher, and crypto enthusiast involved in NFTs, airdrops, early projects, and more.
- The user also provides a link to their other social profiles or resources via linktr.ee/lmsocial, which could lead to additional information.
- **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.



;-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 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....