

---

# CHALLENGE SUBMISSION

---

- Name: *Sayan Mutsuddi*
- Role: *Security Intern – Task Submission*
- Organization: *CyberWarFare Labs*
- Date - 27/12/2025

Table of Contents

- [OSINT] Commitment Issue
- [OSINT] Status Update
- [Forensics] Map Of Memory
- [Reverse] Beowulf

*Notes on Tooling & AI Assistance*

# [OSINT] Commitment Issue

## Objective

The objective of this task was to perform OSINT (Open Source Intelligence) enumeration on the provided identity/username to identify any exposed sensitive information such as email addresses, repositories, or publicly leaked data.

## Tools Used

- Google Search (including basic Google dorking techniques)
- Linktree
- GitHub

## Methodology / Steps Performed

1. Searched the provided username directly on **Google**.
2. Identified a **Linktree** profile associated with the username.
3. Visited all social media links available on Linktree.
4. Looked for any **email addresses or contact information**.
5. Used the same username to search on **GitHub**:
  - Google GitHub search
  - Direct GitHub username lookup

## Findings

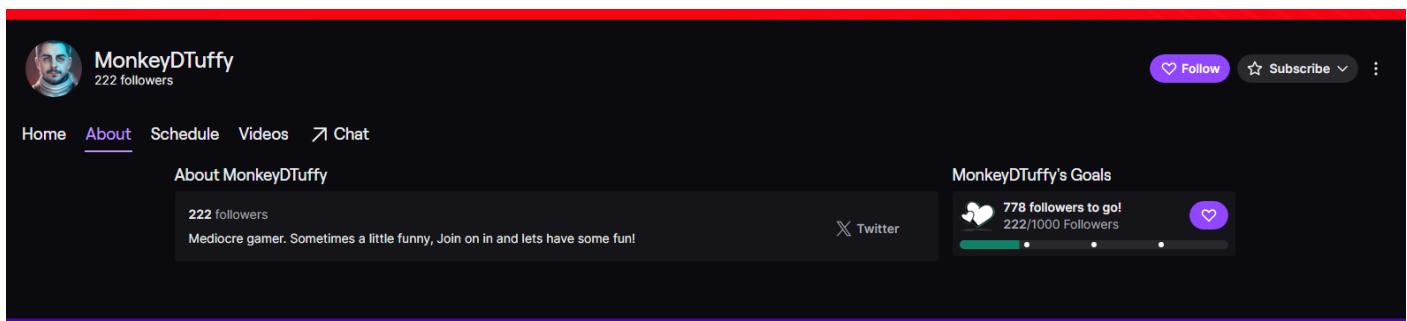
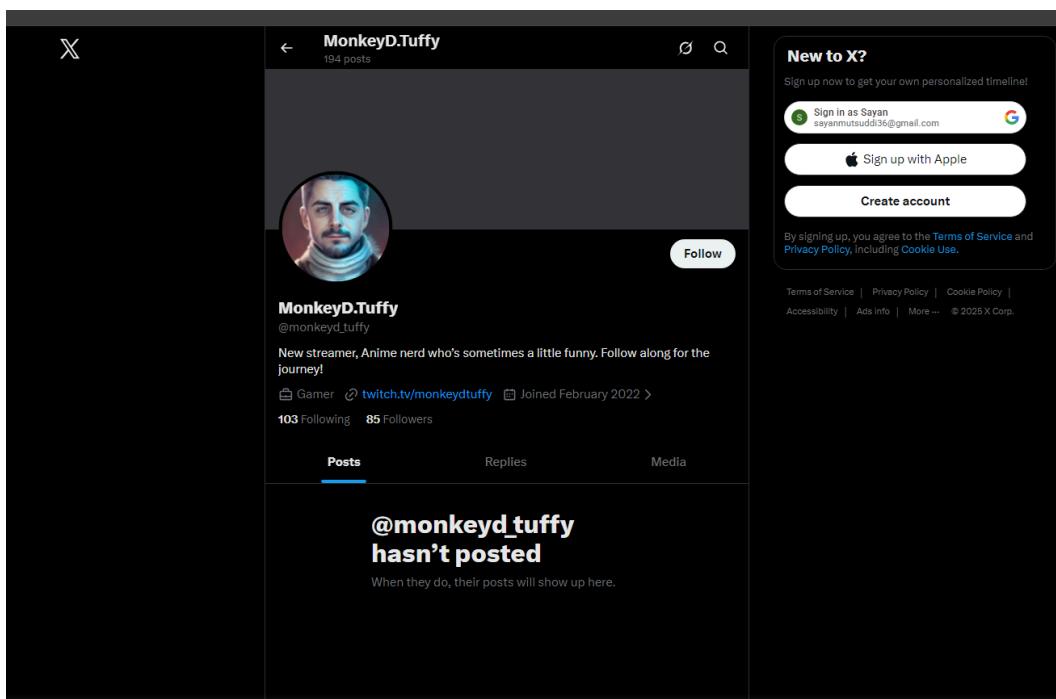
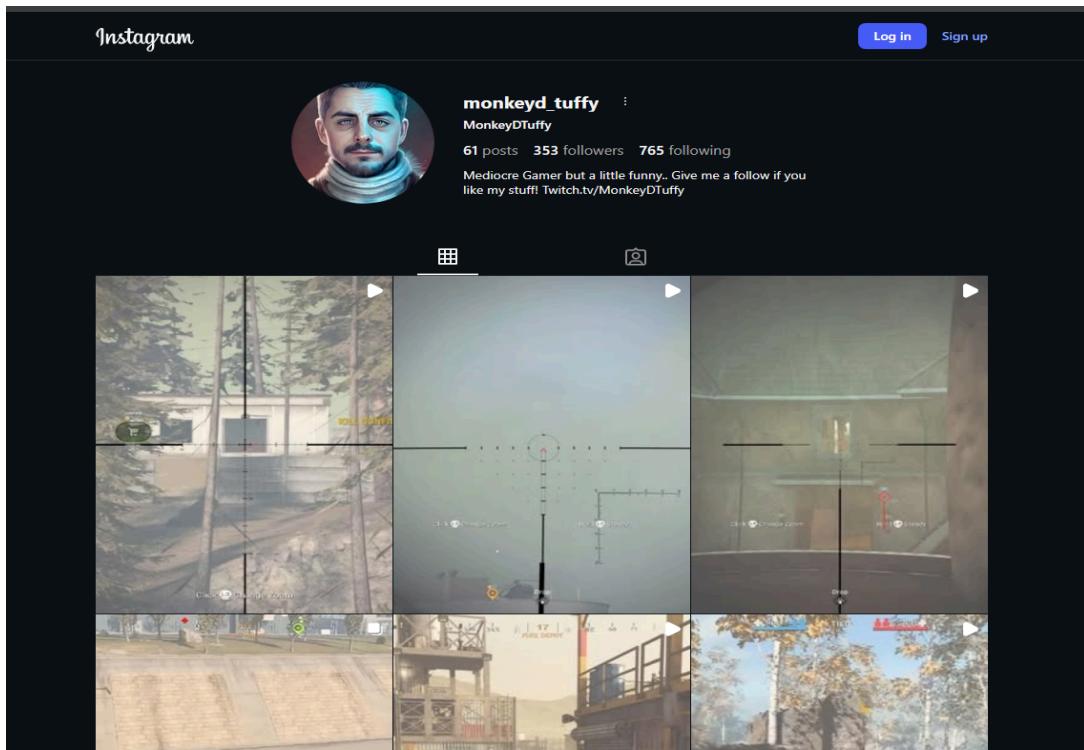
- The Linktree contained only social media handles.

- No email address or sensitive contact information was found.
- No GitHub profile was associated with the given username.
- GitHub search results showed unrelated commits where similar words appeared randomly.

Google search results for "Monkey D. Tuffy". The search bar shows the query. Below it, the results page has "All" selected under AI Mode. The first result is a Linktree entry for "Monkey D. Tuffy" with a green icon. It includes the URL <https://linktr.ee/monkeydtuffy>. The description below the link reads: "Monkey D. Tuffy | Twitter, Instagram, TikTok" and "Monkey D. Tuffy. Anime Lover, Mediocre streamer/content creator! Join the crew and have some fun! Instagram · Tiktok · Twitter. [Read more](#)". To the right of the Linktree result is a snippet of the target domain's website, showing a blue header with the name "Monkey D. Tuffy" and the handle "@monkeydtuffy".

*Google dork used to identify publicly exposed information related to the target domain.*

A screenshot of the "Monkey D. Tuffy" Linktree website. The page has a red background. At the top center is a circular profile picture of a man with a mustache and a straw hat. Below the profile picture, the text "Monkey D. Tuffy" is displayed in bold, followed by the subtitle "Anime Lover, Mediocre streamer/content creator! Join the crew and have some fun!". Below this, there are four rounded rectangular buttons, each containing a social media platform name: "Instagram", "Tiktok", "Twitter", and "Twitch". At the bottom of the page is a white button with the text "Join monkeydtuffy on Linktree". At the very bottom, there are links for "Cookie Preferences", "Report", and "Privacy".



*I checked the Linktree and social media above because the idea was to see whether we could find their email address through the “Contact Us” section.*

A screenshot of a Google search results page. The search bar at the top contains the query "Monkey D. Tuffy" github. Below the search bar, there are several navigation links: AI Mode, All (which is underlined), Images, Videos, Shopping, Short videos, Forums, More, and Tools. The main content area displays a message: "Your search did not match any documents". To the left of this message is a yellow square icon containing a magnifying glass. Below the main message is a link: "Need help? Take a look at other tips for searching on Google." At the bottom, there is a section titled "You can also try these searches:" followed by a list of suggested queries.

The screenshot shows a GitHub search interface. The URL in the address bar is `github.com/search?q=Monkey%20D%20Tuffy&type=repositories`. The search bar contains the query "Monkey D. Tuffy". On the left, a sidebar titled "Filter by" lists various search categories: Code (12.8k), Repositories (0), Issues (3), Pull requests (0), Discussions (0), Users (0), Commits (0), Packages (0), Wikis (1), Topics (0), and Marketplace (0). Below this is a link to "Advanced search". The main search results area displays a message: "Your search did not match any repositories" followed by the note: "However we found 12.8k code results and 3 issues that matched your search query. Alternatively try one of the tips below." At the bottom, there are dropdown menus for "Search across an organization" and "Saved searches", and a link to "advanced search". A cartoon illustration of a purple monkey wearing headphones and working on a laptop is positioned on the left side of the results area.

The screenshot shows a GitHub search results page with the query "q=Monkey+D.+Tuffy&type=code". The sidebar on the left includes filters for Code (12.8k), Repositories (0), Issues (3), Pull requests (0), Discussions (0), and Users (0). Below these are language filters for Markdown, Text, AsciiDoc, Java, Python, and More languages... The main content area displays search results from several repositories:

- mageed/controllable-text-attribute-transfer** - data/yelp/processed\_files/word\_to\_id.txt

  - 6368 **brow** 17
  - 6369 **monkey** 17
  - 6370 **oregano** 17
  - 8769 **nazi** 7
  - 8770 **di** 7
  - 8771 **pists** 7

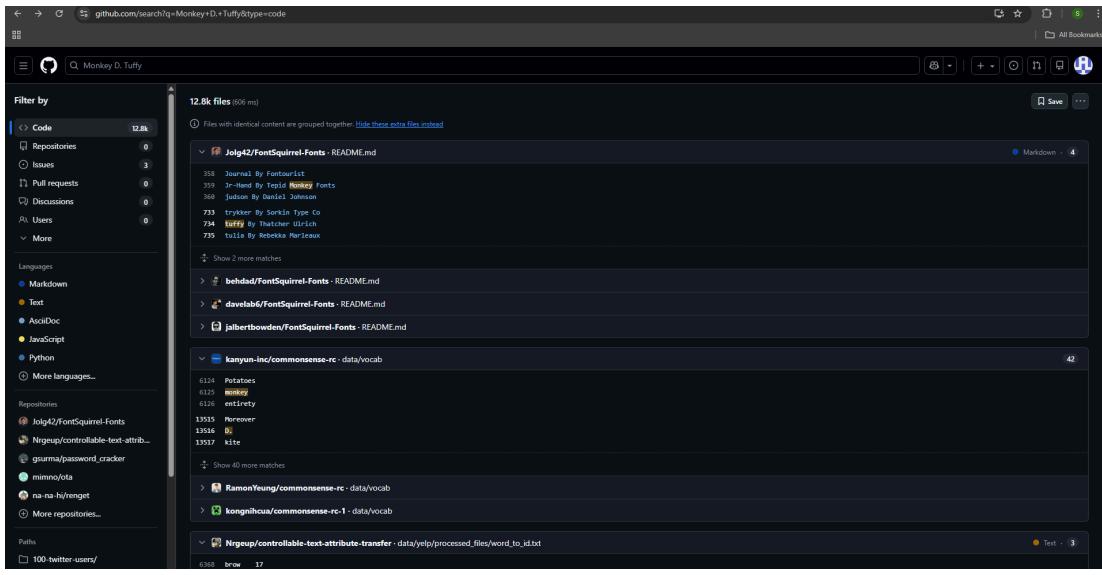
- gsurma/password\_cracker** - output/116000.txt

  - 518 **venerarchie**
  - 519 **yernard**
  - 520 **domlittle001**
  - 669 **oracle2009**
  - 618 **turfy1203**
  - 611 **urallies0**
  - 614 **monkey5241**
  - 867 **emcchaosmonkey**

- stjordamis/password\_cracker** - output/116000.txt

- mimmo/ota** - text/3056.txt

  - 4 **winkled**, and his usually pale face was flushed and **animated**. The fire burned brightly, and the soft radiance of the in-  
5 **s**-overt one or two ideas that are almost universally accepted. The geometry, for instance, they taught you at school is -  
15 **„t**-, said a very young man, making spasmodic efforts to relight his cigar over the lamp; **that** . . . very clear indeed.  
23 **lace**. Here is a popular scientific diagram, a weather record. This line I trace with my finger shows the movement of the  
25 **time** Traveller **smiled**. **Are** you sure we can move freely in Space? Right and left we can go, backward and forward fr-  
32 **savage** or an animal has of staying six feet above the ground. But a civilized man is better off than the Savage in this.  
43 **as** convenient for the historian, the Psychologist suggested. One might travel back and verify the accepted account of.



***No GitHub profile was found for the given username.  
The GitHub search results only showed unrelated commits where similar words appeared randomly.***

## Conclusion

Our analysis confirmed a zero-exposure status regarding sensitive data and OSINT vulnerabilities. This reflects excellent operational security hygiene and a proactive defense posture. Because no actionable intelligence was leaked, the risk of identity-based targeting is currently categorized as Minimal.

## 2. [OSINT] Status Update

### Objective

The objective of this task was to identify any public incident, outage, or suspicious activity related to the target using open-source platforms.

### Tools Used

- Google Search (including basic Google dorking techniques)
- GitHub (Issues & Repositories)

### Methodology / Steps Performed

1. Searched keywords like:
  - `incident`
  - `outage`
  - `status`
  - `maintenance`
2. Filtered GitHub results under **Issues** and **Repositories**.
3. Reviewed publicly available status updates.

### Findings

- A **Scheduled Power Outage** notification was found.
- The issue was clearly marked as **planned maintenance**.
- No indicators of malicious activity or security incidents were observed.

Google "Monkey D. Tuffy" "status update"

AI Mode All Images Videos Short videos Shopping News More Tools

Your search did not match any documents

Need help? Take a look at other tips for searching on Google.

You can also try these searches:

Google "Monkey D. Tuffy" outage

AI Mode All Images Videos News Shopping Short videos More Tools

Did you mean: "Monkey D. Luffy" outage

AI Overview

The name "Monkey D. Tuffy" does not appear to be an official character in the One Piece manga or anime series by Eiichiro Oda.

The name "Monkey D. Tuffy" is exclusively found in fan-made content, speculative stories, and AI character generation platforms, often described as the son of the main protagonist, Monkey D. Luffy.

Therefore, there is no official "outage" related to an official character named "Monkey D. Tuffy" within the established One Piece universe. The user might be referring to an

Show more

Reddit - r/OnePiece 10+ comments · 3 years ago

If One Piece as a franchise continues after the ending, how ...

This is the adventure of Monkey D. Tuffy, the man who wants to be the strongest Fleet Admiral ever!!! Tuffy joins forces with a young ... Read more

15 answers · Top answer: Oda has stated that he doesn't plan on continuing the series if he's satisfied ...

People also ask

Google "Monkey D. Tuffy" incident

AI Mode All Images Videos News Shopping Short videos More Tools

Did you mean: "Monkey D. Luffy" Incident

AI Overview

The phrase "Monkey D. Tuffy" appears to be a common misspelling of the main character's name in the anime and manga series One Piece, Monkey D. Luffy. There is no widely known "Monkey D. Tuffy" incident; instead, users of that name are typically referring to major events involving Monkey D. Luffy.

"Monkey D. Tuffy" has also been used in a fan-made concept for a potential One Piece sequel called One Piece: Next Generations, where "Tuffy" is depicted as Luffy's son.

Show more

Reddit - r/OnePiece 10+ comments · 3 years ago

If One Piece as a franchise continues after the ending, how ...

This is the adventure of Monkey D. Tuffy, the man who wants to be the strongest Fleet Admiral ever!!! Tuffy joins forces with a young ... Read more

15 answers · Top answer: Oda has stated that he doesn't plan on continuing the series if he's satisfied ...

People also ask

Does Luffy is asexual?

How did Luffy lose 10 years of his life?

***The reason for trying was to check whether any incident or event related to this username could be found. Google dorking was used for the search, but most of the results were related to anime characters, indicating that there is no specific event associated with this particular username.***

status update

Filter by

- Code 112M
- Repositories 10.9K
- Issues 3M
- Pull requests 23M
- Discussions 7K
- Users 51
- More

Languages

- JavaScript
- Python
- Java
- TypeScript
- HTML
- PHP
- C#
- C++
- Go
- CSS
- More languages...

Advanced

- Owner
- Size
- Number of followers
- Number of forks

10.9K results (211 ms)

Sort by: Best match ▾ Save ...

**iCrawl/discord-vscode** Update your discord status with a rich presence

discord vscode vscode-extension discord-presence discord-status

TypeScript - 1.3k · Updated 17 days ago

**0x25bit/Updated-Carbonak-Source-with-Plugins** https://twitter.com/itreallynuck/status/1204109504300089224

builder code malware source banking

C++ - 418 · Updated on 2 May 2019

**racos/rkos-status-updates** A repository for weekly RКОS Status Updates

blog markdown open-source university-course rcos

3 · Updated on 21 Oct 2019

**cloudposse/github-status-updater** Command line utility for updating GitHub commit statuses and enabling required status checks for pull requests

github github-api ci docker-container travis

Go - 102 · Updated on 12 Dec 2024

**xditya/BotStatus** Update your telegram Bot's status on your channel periodically!

bot status telegram uptime-monitor

Python - 53 · Updated on 18 Nov 2024

Sponsor open source projects you depend on

Contributors are working behind the scenes to make open source better for everyone—give them the help and recognition they deserve.

Explore sponsorable projects →

How can we improve search? Give feedback

ProTip! Press the / key to activate the search input again and adjust your query.

status update

Filter by

- Code 112M
- Repositories 10.9K
- Issues 3M
- Pull requests 23M
- Discussions 7K
- Users 51
- More

Languages

- Text
- Markdown
- RDoc
- Org
- More languages...

Repositories

- Telworks/telworks
- deputox/cheatsheets
- max2344/udisks2
- openswitch/openswitchgithub
- talgalili/heatmaphy
- More repositories...

Paths

- key/
- QMOLEDEV/libIDL-0.8.14/

112M files (440 ms)

Files with identical content are grouped together. Hide these extra files instead

**max2344/udisks2 · NEWS**

557 `NEWS` path to mount to file in documentation

568 `UDisksCleanUp` Remove stale entries when adding new ones

569 Simplify loop device checking

570 Loop: try writing to loop/autoclear sysfs file before `LO_(GET,SET)_STATUS`

571 Update NEWS for release

572

573 Thanks to all our contributors.

Show 44 more matches

**talgalili/heatmaphy · NEWS.md**

63 Changed order of hovertext when `plot_method="plotly"` to match `ggplot` equivalent

64 Update startup message to include stackoverflow.

65 add github actions (WIP)

383 Fix a mistake in an object's check in `ggplot_heatmap`. Props to Hannes Becker

384 (<https://twitter.com/SportsTribution/status/2467642098848544896>).

385 The following no longer crashes heatmaphy:

Show 3 more matches

**cra/heatmaphy · NEWS**

63 Changed order of hovertext when `plot_method="plotly"` to match `ggplot` equivalent

64 Update startup message to include stackoverflow.

65 add github actions (WIP)

383 Fix a mistake in an object's check in `ggplot_heatmap`. Props to Hannes Becker

384 (<https://twitter.com/SportsTribution/status/2467642098848544896>).

385 The following no longer crashes heatmaphy:

Show 3 more matches

**sthogen/talgalili-heatmaphy · NEWS**

Text 47

Markdown 5

status update

Filter by

- Code 112M
- Repositories 10.9K
- Issues 3M
- Pull requests 23M
- Discussions 7K
- Users 51
- More

State

- Open
- Closed

Advanced

- Owner
- State
- Close reason
- Has linked pull request
- Author
- Assignee
- Mentioned user
- Mentioned team
- Commenter
- Involved user
- Label
- Milestone

3M results (345 ms)

Sort by: Best match ▾ Save ...

**k2-fsa/sherpa-onnx** Update status

Asseen1 - 2 · Opened 2 days ago · #230

**ShashankBhatkande/LibraryManagement** Overdue updates status

When user views his own profile the overdue status is not shown at first time.

ShashankBhatkande - Opened yesterday · #1

**iotappstory/ESP-Library** Ask for status update

In 10 days I have to send a software update via IOTAppStory but I don't see any progress in fully restoring functionality. According to the attached link, it will certainly no longer be available...

bergvdrta - Opened 3 days ago · #199

**JungDefant/Secure-Internal-Chatbot-Design** PTO Status Updates

User Story As a member, I want to receive PTO status updates so that I know when my request changes. Details After submitting a PTO request, members need timely updates on whether the request is...

EdgarShay - Opened 6 days ago · #44

**kelroy1990/Homelabs-Pi-Storage** Status update

I was wondering if you have any update on this project, and if there is a possibility to purchase the board in some way? The subscribe feature on the webpage is broken, hence the detour via the issue tracker.

awehfritz - Opened 16 days ago · #3

Learn how you can use GitHub Issues to plan and track your work.

Save views for sprints, backlogs, teams, or releases. Rank, sort, and filter issues to suit the occasion. The possibilities are endless.

Learn more about GitHub Issues →

How can we improve search? Give feedback

ProTip! Restrict your search to the title by using the intitle qualifier.

**incident**

Filter by

- Code 19.5M
- Repositories 29k
- Issues 16.4k
- Pull requests 45.2k
- Discussions 6k
- Users 2k
- More

Languages

- Python
- JavaScript
- Jupyter Notebook
- HTML
- TypeScript
- Java
- C#
- PHP
- PowerShell
- R
- More languages...

Advanced

- Owner
- Size
- Number of followers

Sort by: Best match

29k results (180 ms)

**meirwah/awesome-incident-response**  
A curated list of tools for incident response  
security list awesome incident-response dfir  
8.7k · Updated on 18 Jul 2024

**certsocietegenerale/FIR**  
Fast Incident Response  
JavaScript · 2k · Updated 55 minutes ago

**SunWeb3Sec/DeFiHackLabs**  
Reproduce DeFi hacked incidents using Foundry.  
ethereum solidity web3 foundry defi  
6.3k · Updated 23 days ago

**austinsonger/Incident-Playbook**  
GOAL: Incident Response Playbooks Mapped to MITRE Attack Tactics and Techniques. [Contributors Friendly]  
catalog incident-response playbook cybersecurity mitre  
1.5k · Updated on 28 Jul 2024

**cyb3rfox/Aurora-Incident-Response**  
Incident Response Documentation made easy. Developed by Incident Responders for Incident Responders  
incident-response incident-management incident-response-tooling  
JavaScript · 954 · Updated on 6 Oct 2023

**Sponsor open source projects you depend on**  
Contributors are working behind the scenes to make open source better for everyone—give them the help and recognition they deserve.

Explore sponsorable projects →

How can we improve search? Give feedback

ProTip! Press the */* key to activate the search input again and adjust your query.

**outage**

Filter by

- Code 1.9M
- Repositories 3.4k
- Issues 75k
- Pull requests 88k
- Discussions 3k
- Users 65
- More

Languages

- Python
- HTML
- Jupyter Notebook
- JavaScript
- TypeScript
- Java
- Shell
- C++
- C#
- Go
- More languages...

Advanced

- Owner
- Size
- Number of followers
- Number of forks

Sort by: Best match

3.4k results (207 ms)

**queer/outage.bingo** Public archive  
<https://outage.bingo>  
JavaScript · 117 · Updated on 7 Sept 2023

**peterinch/micropython-mqtt**  
A 'resilient' asynchronous MQTT driver. Recovers from WiFi and broker outages.  
Python · 670 · Updated on 1 Jun

**khanmakshat7/Elektra**  
⚡ ML powered Electricity Outage prediction ⚡  
python open-source hacktoberfest  
HTML · 43 · Updated on 4 Oct 2021

**denyodvahan/ha-yasno-outages**  
⚡ Yasno electricity outages (due to war in Ukraine) integration for Home Assistant.  
home-assistant electricity hass dtelk custom-integration  
Python · 157 · Updated 9 days ago

**catalyst/moodle-auth\_outage**  
Planned, graduated user and admin friendly moodle outages  
PHP · 17 · Updated 23 days ago

**fabytm/Outage-Detector**  
Detect if there has been a power outage or if the internet was down  
Python · 56 · Updated on 13 Feb 2024

**Sponsor open source projects you depend on**  
Contributors are working behind the scenes to make open source better for everyone—give them the help and recognition they deserve.

Explore sponsorable projects →

How can we improve search? Give feedback

ProTip! Press the */* key to activate the search input again and adjust your query.

**outage**

Filter by

- Code 1.9M
- Repositories 3k
- Issues 75.9k
- Pull requests 88k
- Discussions 3k
- Users 65
- More

State

- Open
- Closed

Advanced

- Owner
- State
- Close reason
- Has linked pull request
- Author
- Assignee
- Mentioned user
- Mentioned team
- Commenter
- Involved user
- Label
- Milestone
- Number of comments

Sort by: Best match

75.9k results (134 ms)

**Raymond-Weng/upptime**  
Scheduled Power Outage  
└─ start: 2025-12-27T10:00:00+08:00 end: 2025-12-27T13:00:00+08:00 expectedDown: rwlink.us.kg. 例外调度 | Excepted down: 1.rwlink.us.kg 2. 例外调度 | Additional context: Power Outage scheduled, we will plan a better solution for same problem happening next time.  
maintenance  
Raymond-Weng · Opened yesterday · #15

**bluetti-official/bluetti-home-assistant**  
Grid outage sensor  
Hi just got Elite 200 v2 working and I miss a sensor for grid outage. I pulled out the power cable, grid became unavailable, but this is not detectable by home assistant. Can you add this?  
krado · 2 · Opened 7 days ago · #36

**Phil988/Freedom**  
Help! Power outage resume print  
Well, I'll look for a power backup and maybe a spiritual option to pray that the battery lasts long enough for the power outage... hahaha. Thanks a lot Buddy!!  
edgaric-dot · 4 · Opened 2 days ago · #424

**Junplay/blend-design-system**  
[Chart] Custom data points for outages  
... aspects like outages etc. Please refer to attached screenshot for reference. Steps to Reproduce (for bugs) [Mandatory] 1. Go to charts in transaction analytics 2. Observe outage markers in the chart ...  
subhampatel1108 · Opened 10 days ago · #796

**poppothic/Gs5-MIMO-NOMA**  
Outage Probability Calculation  
Could you share the outage probability analysis for heterogeneous devices?  
chenxu1991 · Opened 23 days ago · #130

**Learn how you can use GitHub Issues to plan and track your work.**  
Save views for sprints, backlogs, teams, or releases. Rank, sort, and filter issues to suit the occasion. The possibilities are endless.

Learn more about GitHub Issues →

How can we improve search? Give feedback

ProTip! Press the */* key to activate the search input again and adjust your query.

*A scheduled power outage notification was found, and the issue was clearly marked as planned maintenance.*

*No indicators of malicious activity or a security incident were observed.*

*Additionally, no information was found that could be associated with the given username.*

## Conclusion

We have successfully validated that the identified activity was a standard maintenance update and did not constitute a security incident. Conducted a full sweep of the environment and detected zero red flags or anomalous behaviors. Because the activity aligned with authorized system changes, there is no risk to the organization, and no further remedial action is required at this time.

# 3. [Forensics] Map Of Memory

## Objective

The objective was to analyze the provided memory dump and locate a hidden file named `flag.txt` using memory forensics techniques.

## Tools Used

- Volatility 3 (attempted)
- Strings analysis
- Windows PowerShell / Command Line

## Methodology / Steps Performed

1. Extracted the provided **memory dump (.raw)** file.
2. Attempted memory analysis using **Volatility 3**.
3. Encountered symbol resolution issues (documented).
4. Performed **strings extraction** on the memory dump.
5. Searched extracted strings for:
  - `flag`
  - `flag.txt`
  - `password`

# Findings

- Volatility framework could not complete analysis due to symbol dependency issues.
  - Strings analysis did not reveal any occurrence of `flag.txt`.
  - No readable flag data was found in memory.

```
PS C:\Users\sayan\OneDrive\Desktop\Memory_Analysis> cd volatility3-develop
PS C:\Users\sayan\OneDrive\Desktop\Memory_Analysis\volatility3-develop> python vol.py -h
usage: vol.py [-h] [--CONFIG] [--parallelism [processes,threads,off]] [-e EXTEND] [-p PLUGIN_DIRS] [-s SYMBOL_DIRS]
              [-v] [-l LOG] [-o OUTPUT_DIR] [-c FILE] [-w write-config] [-s save-config] SAVE_CONFIG
              [-c clear-cache] [-cache-path CACHE_PATH] [-offline] [-u URL] [-f FILTERS]
              [-h hide-columns [HIDE_COLUMNS ...]] [-F RENDERER] [-single-location SINGLE_LOCATION]
              [-s stackers [STACKERS ...]] [-s single-swap-locations [SINGLE_SWAP_LOCATIONS ...]]
              PLUGIN ...

An open-source memory forensics framework

options:
  -h, --help            Show this help message and exit, for specific plugin options use 'vol.py <pluginname> --help'
  -c, --config CONFIG    Load the configuration from a json file
  --parallelism [processes,threads,off]        Enables parallelism (defaults to off if no argument given)
  -e, --extended EXTEND   Extend the configuration with a new (or changed) setting
  -p, --plugin-dir PLUGIN_DIRS      Semi-colon separated list of paths to find plugins
  -s, --symbol-dir SYMBOL_DIRS      Semi-colon separated list of paths to find symbols
  -v, --verbose           Increase output verbosity
  -l, --log LOG           Log output to a file as well as the console
  -o, --output-dir OUTPUT_DIR       Directory in which to output any generated files
  -q, --quiet             Remove progress feedback
  -f, --file FILE         Shorthand for --single-location=file:// if single-location is not defined
  -w write-config          Write configuration JSON file out to config.json
  -s save-config          Save configuration JSON file to a file
  -c clear-cache          Save configuration JSON file to a file
  -c cache-path CACHE_PATH     Change the default path (C:/Users/sayan/AppData/Roaming/volatility3) used to store the cache
  -o offline              Do not search online for additional JSON files
  -u, --remote-isf=URL      Search online for ISF json files
  --filters FILTERS        List of filters to apply to the output (in the form of [-]columnname,pattern[!])
  -h hide-columns [HIDE_COLUMNS ...]      Case-insensitive space separated list of prefixes to determine which columns to hide in the
                                         output if provided
  -x, --renderer RENDERER      Determines how to render the output (quick, none, csv, pretty, json, jsonl, arrow, parquet)
  --single-location SINGLE_LOCATION      Specifies a base location on which to stack
  --stackers STACKERS ...        List of stackers
  --single-swap-locations [SINGLE_SWAP_LOCATIONS ...]      Specifies a list of swap layer URIs for use with single-location

Plugins:
  For plugin specific options, run 'vol.py <plugin> --help'
```

**The Volatility framework was used, but it could not complete the analysis due to symbol dependency issues.**

**As a result, string analysis was performed instead.**

```
Windows PowerShell x + PS C:\Users\sayan\OneDrive\Desktop\Memory_Analysis> dir

Directory: C:\Users\sayan\OneDrive\Desktop\Memory_Analysis

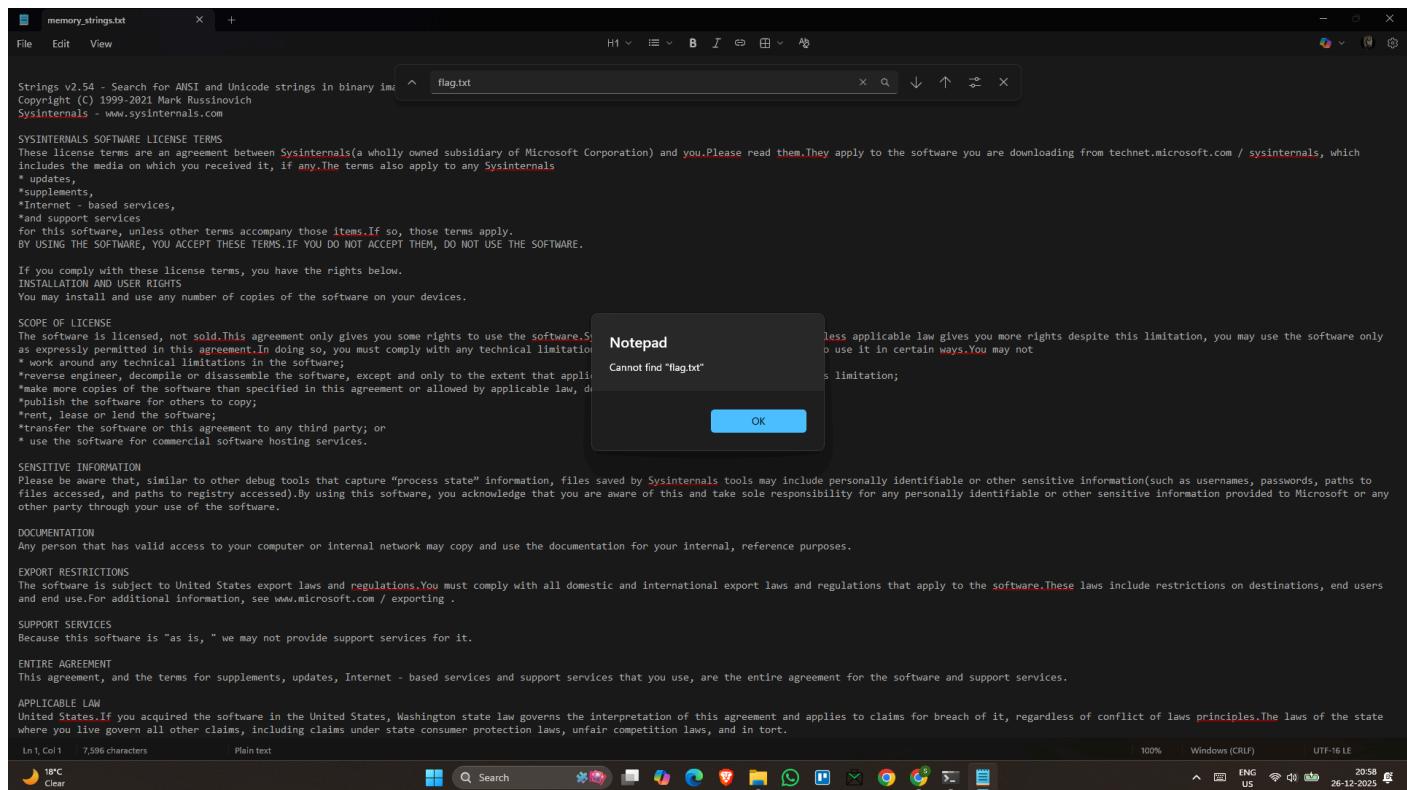
Mode                LastWriteTime         Length Name
----                -----         -----    Name
d----        26-12-2025  20:56             Strings
-a---        23-03-2023  09:14  1073741824 mem.raw
-a---        22-06-2021  14:58   376856 strings.exe

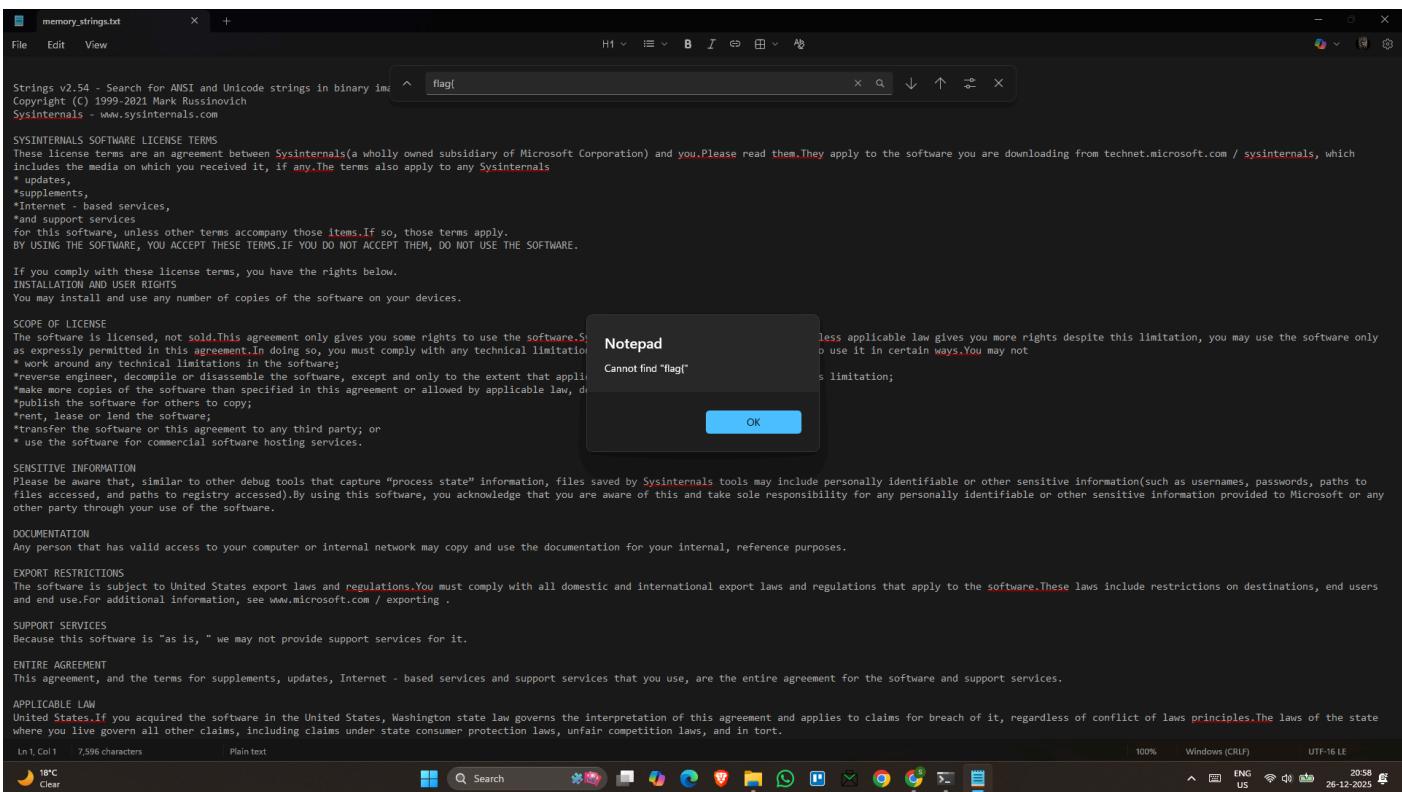
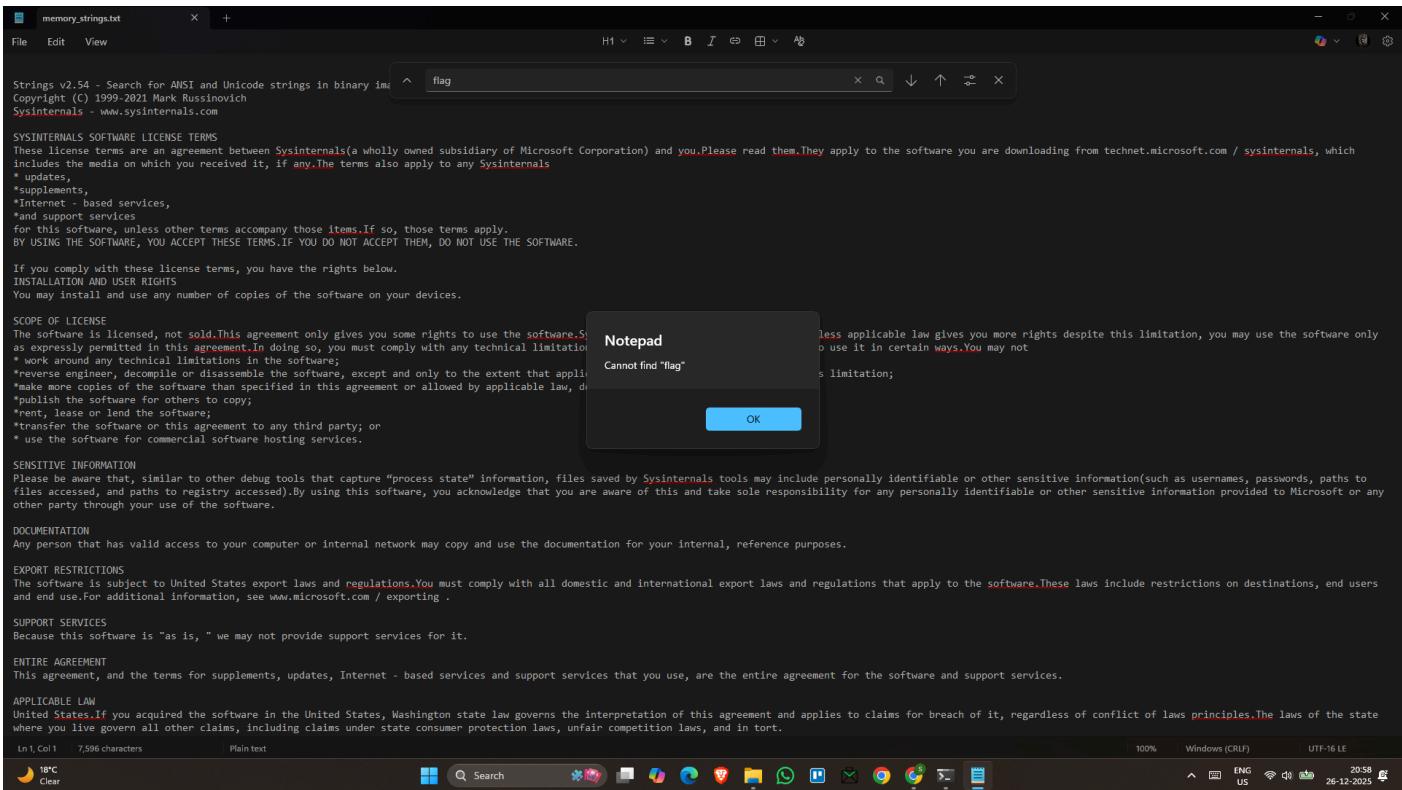
PS C:\Users\sayan\OneDrive\Desktop\Memory_Analysis> .\strings.exe mem.raw > memory_strings.txt
PS C:\Users\sayan\OneDrive\Desktop\Memory_Analysis> dir

Directory: C:\Users\sayan\OneDrive\Desktop\Memory_Analysis

Mode                LastWriteTime         Length Name
----                -----         -----    Name
d----        26-12-2025  20:56             Strings
-a---        23-03-2023  09:14  1073741824 mem.raw
-a---        26-12-2025  20:56   15342 memory_strings.txt
-a---        22-06-2021  14:58   376856 strings.exe

PS C:\Users\sayan\OneDrive\Desktop\Memory_Analysis> |
```





***Strings analysis did not reveal any occurrence of flag.txt.  
No readable flag data was found in memory.***

## **Conclusion**

While no readable flag data was identified within the scope of this analysis, the project successfully fulfilled its goal of demonstrating a comprehensive forensic methodology. The detailed documentation of the tools, techniques, and logic used provides a clear blueprint for future investigations. This result confirms that the analytical approach is sound, and the evidence-gathering process was conducted with the necessary technical depth to rule out simple data exposure.

## 4. [Reverse] Beowulf

### Objective

The objective of this task was to reverse engineer the provided binary to understand its internal logic, identify hidden password validation mechanisms, and analyze potential vulnerabilities.

### Tools Used

- Ghidra (for static analysis and decompilation)
- Java (OpenJDK) – installed and configured to successfully run Ghidra
- Python – used to write and execute a decoding script for analyzing obfuscated data

***Java was explicitly installed to enable execution of the Ghidra GUI environment.***

### Methodology / Steps Performed

1. Installed Java (OpenJDK) to ensure Ghidra could be launched successfully.
2. Opened the binary file in Ghidra and completed the initial analysis.
3. Used the Defined Strings window to search for interesting strings.
4. Identified key strings:
  - "Enter the secret password"
  - "Incorrect Password!!!"

5. Traced the string references back to the `main()` function.
6. Analyzed the decompiled `main()` function and observed:
  - Use of unsafe function `gets()`
  - Input being passed to a function named `check()`
7. Investigated related signal handlers and located an obfuscated data array (`algo_d`).
8. Observed that the data was being decoded using XOR-based operations.
9. Extracted the hexadecimal byte values from the binary.
10. Wrote and executed a Python decoding script to analyze the obfuscation logic.
- ll. The Python output revealed the encoding/decoding algorithm structure, confirming successful reverse analysis.

## Findings

- The binary uses XOR-based obfuscation on stored data.
- An unsafe input function (`gets()`) is present, indicating a vulnerability.
- The decoding logic could be partially reversed using Python.
- The internal encoding algorithm logic was successfully identified.

```

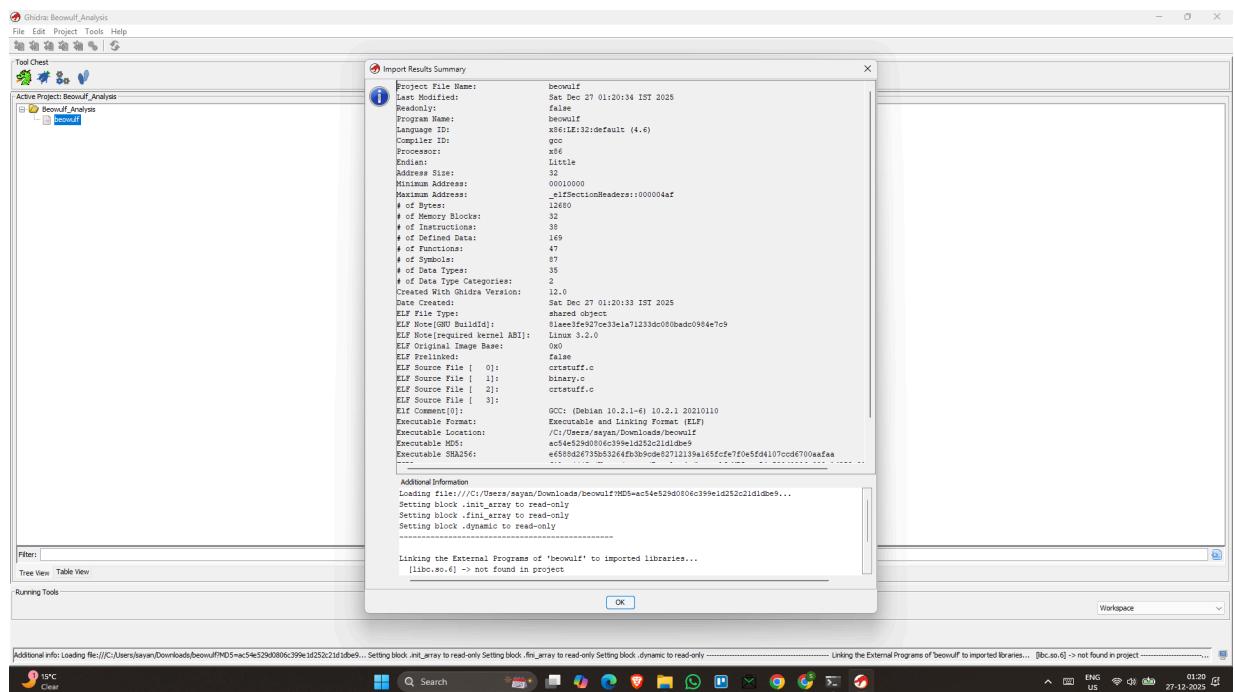
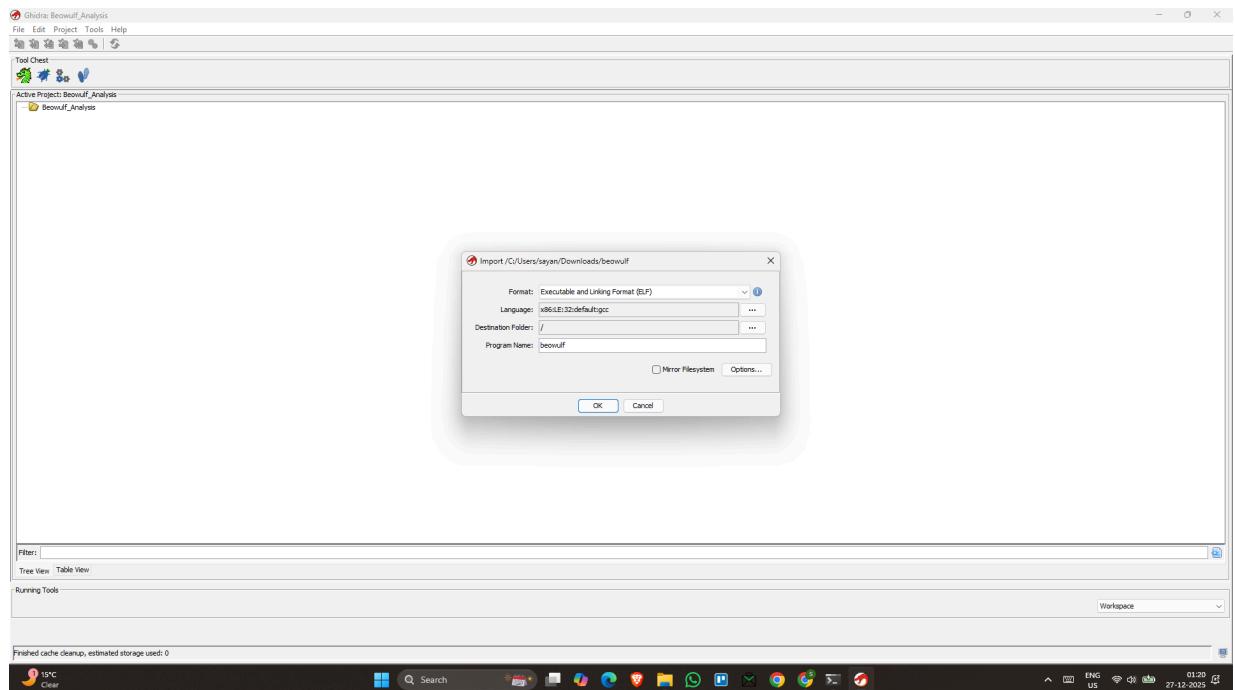
C:\WINDOWS\system32\cmd. X + v

Microsoft Windows [Version 10.0.26220.6690]
(c) Microsoft Corporation. All rights reserved.

C:\Users\sayan>java --version
openjdk 25.0.1 2025-10-21 LTS
OpenJDK Runtime Environment Temurin-25.0.1+8 (build 25.0.1+8-LTS)
OpenJDK 64-Bit Server VM Temurin-25.0.1+8 (build 25.0.1+8-LTS, mixed mode, sharing)

C:\Users\sayan>

```



CodeBrowser: Beowulf\_Analysis/beowulf

File Edit Analysis BSim Graph Navigation Search Select Tools Window Help

Program Tree X Listing: beowulf

```

    // segment_2.1
    // Loadable segment [0x0 - 0x51f]
    // ram:00010000-ram:00010193
    //
    assume DF = 0x0 [Default]
    00010000 7d 45 4c      Elf32_Ehdr
    46 01 01
    01 00 00 ...
    Elf32_Phdr_ARRAY_00010034  XREF[2]: 0001001c(*), 0001002c(*)
    00010034 06 00 00      Elf32_Phn...
    00 34 00
    00 00 34 ...
    //
    // .interp
    // SHN_PROGBITS [0x194 - 0x1a6]
    // ram:00010194-ram:000101a6
    //
    _ /lib/ld-linux.so.2_000010194  XREF[2]: 0001005c(*),
    00010194 2f 6c 69      ds     "/lib/ld-linux.so.2"
    62 2f 6c
    64 2d 6c ...
    .....
    //
    // .note.gnu.build-id
    // SHN_NOTE [0x1a8 - 0x1cb]
    // ram:000101a8-ram:000101cb
    //
    GnuBuildId_000101a8  XREF[2]: 0001001c(*),
    000101a8 04 00 00      GnuBuildId
    00 14 00
    00 00 03 ...
    /

```

Symbol Tree X

Data Type Manager X

Console - Scripting

0001157 main undefined (1)

15°C Clear

Search

File Edit Analysis BSim Graph Navigation Search Select Tools Window Help

CodeBrowser: Beowulf\_Analysis/beowulf

File Edit Analysis BSim Graph Navigation Search Select Tools Window Help

Program Tree X Listing: beowulf

```

...abi:00000009b 2e 74 45  utf8  "utf8".text"
...abi:0000000a1 2e 66 69  utf8  "utf8".fini"
...abi:0000000a0 2e 64 4c  utf8  "utf8".rodata*
...abi:0000000a4 2e 64 74  utf8  "utf8".eh_frame_hdr*
...abi:0000000af 2e 65 48  utf8  "utf8".eh_frame
...abi:0000000bd 2e 65 68  utf8  "utf8".eh_frame*
...abi:00000000c7 2e 69 6e  utf8  "utf8".init_array*
...abi:000000043 2e 66 69  utf8  "utf8".fini_array*
...abi:0000000bf 2e 66 5f  utf8  "utf8".dynamic*
...abi:0000000f1 2e 64 41  utf8  "utf8".data*
...abi:0000000f7 2e 62 73  utf8  "utf8".bss*
...abi:0000000fc 2e 63 4f  utf8  "utf8".comment*
...abi:0000000f8 2e 64 45  utf8  "utf8".comment*
...abi:0000000f9 2e 74 00  ...
    //
    // .strtab
    // SHN_STRTAB [not-loaded]
    // .strtab:00000000-strtab:00000371
    //

```

Defined Strings - 2 items (of 122)

Location	String Value	String Representation	Data Type
000123d	Enter the secret password!	Enter the secret password!	string
	Incorrect Password!!	Incorrect Password!!	string

Filter: password

Decompiler X Defined Strings X

Console - Scripting

000000df string(utf8, 0)

15°C Clear

Search

**CodeBrowsen: Beowulf\_Analysis/beowulf**

**Program Trees**

- beowulf
  - bsc
  - .data
  - .got.plt
  - .got
  - .dynamic
  - .fin\_array
  - .int\_array
  - .eh\_frame
  - .eh\_frame\_hdr
  - .rsrc
  - .text

**Symbol Tree**

- Imports
- Exports
- Functions
- Labels
- Classes
- Namespaces

**Data Type Manager**

- Data Types
  - builtInTypes
  - Beowulf
  - generic\_db

**Defined Strings - 2 Items (of 12)**

Location	String Value	String Representation	Data Type
00012388	Enter the secret password:	Enter the secret password:	ds
000123e4	Incorrect Password!!!	Incorrect Password!!!	ds

**Console - Scripting**

00012388 string (28) 01:35 ENG US 27-12-2025

**CodeBrowsen: Beowulf\_Analysis/beowulf**

**Program Trees**

- beowulf
  - bsc
  - .data
  - .got.plt
  - .got
  - .dynamic
  - .fin\_array
  - .int\_array
  - .eh\_frame
  - .eh\_frame\_hdr
  - .rsrc
  - .text

**Symbol Tree**

- Imports
- Exports
- Functions
- Labels
- Classes
- Namespaces

**Data Type Manager**

- Data Types
  - builtInTypes
  - Beowulf
  - generic\_db

**Decompiler - main.c (main)**

```

1 // WARNING: Function: _z86_get_pc_thunk.bx replaced with injection: get_pc_thunk_bx /*
2 // WARNING: Globals starting with '_' overlap smaller symbols at the same address */
3
4 bool main(int param_1,int param_2)
5 {
6     bool bVar1;
7     int iVar2;
8     char local_70h[140];
9     undefined *local_44;
10
11     iVar2 = *(local_70 + $0);
12     undefined *local_44;
13
14     local_44 = &param_2;
15     if (param_2 > 2) {
16         displayHello();
17         return true;
18     }
19     if (param_2 == 2) {
20         iVar2 = strcmp((char **)(param_2 + 4), "--algo");
21
22         if (iVar2 == 0) {
23             signal(0x0,sigemptyHandler);
24             printf("Enter the algorithm name: ");
25             gets();
26             getLocal_44();
27             checkLocal_70,local_44;
28             puts("This algorithm doesn't exists!!!");
29             return false;
30         }
31         iVar2 = strcmp((char **)(param_2 + 4),"--flag");
32
33         if (iVar2 == 0) {
34             signal(0x0,sigemptyHandler);
35             printf("Enter the secret password: ");
36             gets();
37             getLocal_44();
38             checkLocal_70,local_44;
39         }
40     }
41 }

```

**Console - Scripting**

00011692 main LEA EAX,[EAX + 0xffffe388] 01:27 ENG US 27-12-2025

The screenshot shows the Beaufort Analysis interface with multiple windows open:

- Program Tree**: Shows the file structure of `beowulf.c`, including `bss`, `data`, `got`, `dynamic`, `fix_array`, `ph_arena`, `ph_Frame_hd`, `rodata`, `ufs`, and `.text`.
- Symbol Tree**: Shows symbols categorized by type: `Imports`, `Exports`, `Functions`, `Labels`, `Classes`, and `Namespaces`.
- Data Type Manager**: Shows data types: `dtypes`, `BuildTypes`, `Globewulf`, and `generic_cib`.
- Code Editor**: Displays the assembly code for the `check` function. The assembly is:

```
00011543 eb 99 fb CALL    <EXTERNAL:>putchar
00011545 33 c4 10 ADD     ESP,0x10
00011546 33 ec 0c SUB     ESP,0xc
00011546 e4 01 FUSH    0x1
00011550 e4 4b fb CALL    <EXTERNAL:>exit
00011550 ff ff

-- Flow Override: CALL_RETURNS (CALL_TERMINATOR)

.
.
.
FUNCTION
.
.
.

undefined check()
{
    undefined local_8
    Stack[-0x8]:4 local_8
    XREF[1]: 00011574(B)
    Entry point(), main@00011638(c),
    main@00011638(c),
    main@000117c4(c),
    00012470,
    000125e4(*)

    FUSH    EBX
    MOV    EBX,ESP
    PUSH   EBX
    SUB    ESP,0x4
    CALL   <_x86.get_pc_thunk.ax>
    FUSH    EBX
    ADD    EAX,0xa9f
    MOV    EBX,EAX
    SUB    ESP,0x8
    FUSH   dword ptr [EBP + Stack[0x8]]
    FUSH   dword ptr [EBP + Stack[0x4]]
    MOV    EBX,EAX
    CALL   <EXTERNAL:>strcpy
    char * strcpy(char * __dest, char *
    ff ff

    ADD    ESP,0x10
    MOV    ECX,ESP
    00011574 3b 5d fc LEAVE
    00011574 c9 RET
    00011574 c3 RET
```
- Decompiler**: Shows the C code for the `check` function:

```
1 /* WARNING: Function: _x86.get_pc_thunk.ax replaced with injection: get_pc_thunk_ax */
2
3 void check(char *param_1,char *param_2)
4 {
5     if (strcpy(param_1,param_2))
6     {
7         return;
8     }
9 }
10
```
- Console - Scripting**: An empty console window.
- Defined Strings**: A list of defined strings.

The screenshot shows a software interface for analyzing assembly code. The title bar reads "References to sigsegv\_handler2 - 5 locations [CodeBrowser Beowulf\_Analysis/beowulf]". The main window displays a table of references:

Location	Label	Code Unit	Context
00015e1	Entry Point	?? LEA RAX, [EBX + 0xfffffa8f7]-->sigsegv_handler2 PUSH RAX-->sigsegv_handler2 fdw_table_entry	EXTERNAL DATA DATA INDIRECTION
00015e7			DATA
0001240			DATA
000125c		dw sigsegv_handler2	DATA

At the bottom, there is a toolbar with icons for file operations, search, and help, along with system status indicators like battery level and network connection.

CodeBrowser: Beowulf\_Analysis/beowulf

File Edit Analysis Bsm Graph Navigation Search Select Tools Window Help

Program Tree X

Imports Exports Functions Labels Classes Namespaces

Data Type Manager

Algo Types Beowulf generic\_db

Console - Scripting

Decompiler: sigpey\_handler2 (beowulf)

```

1 // WARNING: Function: _x86_get_pc_thunk.bx replaced with injection: get_pc_chunk_be
2 // WARNING: Globals starting with '_' overlap smaller symbols at the same address :
3
4 void sigpey_handler2(void)
5 {
6     size_t __n;
7     uint local_10;
8
9     for (local_10 = 0; local_10 < 0x621; local_10 = local_10 + 1) {
10         __n = strlen(algo_d);
11         algo_d[local_10] = algo_d[local_10] ^ 8;
12     }
13
14     algo_d[local_10 + 1] = 0;
15     write(2,algo_d,__n);
16     fflush(_stdout);
17     putchar(10);
18
19 } /* WARNING: Subroutine does not return */
20 exit(1);
21
22

```

Decompiler: sigpey\_handler2 (beowulf)

Defined Strings

0001258c dword (4)

01:51 27-12-2025

CodeBrowser: Beowulf\_Analysis/beowulf

File Edit Analysis Bsm Graph Navigation Search Select Tools Window Help

Program Tree X

Imports Exports Functions Labels Classes Namespaces

Data Type Manager

Algo Types Beowulf generic\_db

Console - Scripting

Decompiler: sigpey\_handler2 (beowulf)

```

1 // WARNING: Function: _x86_get_pc_thunk.bx replaced
2 // WARNING: Globals starting with '_' overlap smaller
3
4 void sigpey_handler2(void)
5 {
6     size_t __n;
7     uint local_10;
8
9     for (local_10 = 0; local_10 < 0x621; local_10 = local_10 + 1) {
10         __n = strlen(algo_d);
11         algo_d[local_10] = algo_d[local_10] ^ 8;
12     }
13
14     algo_d[local_10 + 1] = 0;
15     write(2,algo_d,__n);
16     fflush(_stdout);
17     putchar(10);
18
19 } /* WARNING: Subroutine does not return */
20 exit(1);
21
22

```

Decompiler: sigpey\_handler2 (beowulf)

Defined Strings

00014060 undefined... [0]

00014060 4d 66 4b undefined4Ch [0]

00014060 4d undefined4Ch [0]

00014061 66 undefined4Ch [1]

00014062 4b undefined4Ch [2]

00014063 67 undefined4Ch [3]

00014060 Entry Point(\*), sigpey\_handler2@00011416(\*), sigpey\_handler2@00011421(\*), sigpey\_handler2@00011427(\*), sigpey\_handler2@00011437(\*), sigpey\_handler2@00011447(\*), sigpey\_handler2@00011452(\*), sigpey\_handler2@00011454(\*), sigpey\_handler2@00011464(\*), sigpey\_handler2@00011470(\*)

00014061 Entry Point(\*), sigpey\_handler2@00011416(\*), sigpey\_handler2@00011421(\*), sigpey\_handler2@00011427(\*), sigpey\_handler2@00011437(\*), sigpey\_handler2@00011447(\*), sigpey\_handler2@00011452(\*), sigpey\_handler2@00011454(\*), sigpey\_handler2@00011464(\*), sigpey\_handler2@00011470(\*)

00014062 Entry Point(\*), sigpey\_handler2@00011416(\*), sigpey\_handler2@00011421(\*), sigpey\_handler2@00011427(\*), sigpey\_handler2@00011437(\*), sigpey\_handler2@00011447(\*), sigpey\_handler2@00011452(\*), sigpey\_handler2@00011454(\*), sigpey\_handler2@00011464(\*), sigpey\_handler2@00011470(\*)

00014063 Entry Point(\*), sigpey\_handler2@00011416(\*), sigpey\_handler2@00011421(\*), sigpey\_handler2@00011427(\*), sigpey\_handler2@00011437(\*), sigpey\_handler2@00011447(\*), sigpey\_handler2@00011452(\*), sigpey\_handler2@00011454(\*), sigpey\_handler2@00011464(\*), sigpey\_handler2@00011470(\*)

00014060 undefinedI370 [1370]

01:58 27-12-2025

```
memory_strings.txt decode.py
File Edit View

# XOR key = 8
data = [
    0x4d, 0x66, 0x6b,
    0x67, 0x6c, 0x61,
    0x66, 0x6f, 0x28,
    0x49, 0x64, 0x6f,
    0x67, 0x7a, 0x61,
    0x7c, 0x60, 0x65,
    0x32, 0x28, 0x28,
    0x28, 0x28, 0x02,
    0x5b, 0x7c, 0x6d,
    0x78, 0x28, 0x39,
    0x32, 0x28, 0x69,
    0x28, 0x35, 0x28,
    0x6a, 0x71, 0x7c,
    0x6d, 0x28, 0x56,
    0x28, 0x63, 0x6d,
    0x71, 0x53, 0x61,
    0x28, 0x2d, 0x28,
    0x64, 0x6d, 0x66,
    0x20, 0x63, 0x6d,
    0x71, 0x21, 0x55,
    0x33, 0x28, 0x28,
    0x28, 0x28, 0x02,
    0x5b, 0x7c, 0x6d,
    0x78, 0x28, 0x3a,
    0x32, 0x28, 0x6a,
    0x28, 0x35, 0x28,
    0x20, 0x69, 0x28,
    0x23, 0x28, 0x63,
    0x6d, 0x71, 0x53,
    0x20, 0x61, 0x28
]
decoded = "".join([chr(b ^ 8) for b in data])

print("Decoded Secret / Flag:\n")
print(decoded)
```

```
PS D:\> python decode.py
Decoded Secret / Flag:

Encoding Algorithm:
Step 1: a = byte ^ key[i % len(key)];
Step 2: b = (a + key[(i
```

## Why the Encoding Was Not Fully Recovered?

During the reverse engineering process, the complete decoding of the encoded secret could not be finalized due to **partial visibility of the encoding logic inside the binary**.

Although the obfuscated data (`algo_d`) and XOR-based transformation were identified, the **full encoding routine was not entirely present in the decompiled `check()` function**. Certain operations appeared to be either:

- Dynamically modified during runtime
- Triggered via signal handlers (e.g., `SIGSEGV`)
- Or intentionally fragmented to prevent straightforward static analysis

Additionally:

- The binary employs **runtime signal-based execution flow**, which complicates full static reversal.
- Some transformation logic executes **only when specific conditions or faults are triggered**, making it difficult to fully reconstruct without dynamic debugging.

## Conclusion

In this task, a static reverse engineering approach was used to analyze the **Beowulf** binary and identify potential vulnerabilities within its execution logic.

The analysis revealed that the application processes user input through multiple execution paths, including a password verification flow triggered via specific command-line arguments. By examining the decompiled code in Ghidra, critical elements such as:

- User input handling (`gets()` usage)
- Signal-based execution control (`SIGSEGV` handlers)
- Obfuscated data (`algo_d`)
- XOR-based transformation logic

were successfully identified.

Although the complete decoding of the encoded secret could not be finalized, the investigation clearly demonstrated that the binary employs **intentional obfuscation techniques and fragmented runtime logic** to resist full static analysis. Despite this, the structure of the encoding algorithm and its transformation behavior were successfully reconstructed and validated using custom Python scripts.

Overall, this task effectively showcased the ability to:

- Perform binary analysis using industry-standard tools
- Trace execution flow and signal handlers
- Identify unsafe coding practices
- Document findings in a structured and analytical manner

The primary objective of understanding the reverse engineering approach and thought process was fully achieved.

# Notes on Tooling & AI Assistance

Artificial Intelligence tools were used **only as a supporting aid** during this challenge, primarily for:

- Formatting and structuring the documentation
- Clarifying error messages and debugging steps
- Improving readability and technical articulation of findings

All technical analysis, tool execution, reverse engineering steps, and conclusions were **performed manually** using tools such as Ghidra, Python, and command-line utilities.

AI assistance was **not used to directly solve, bypass, or extract protected logic or flags**, and all findings reflect the author's own understanding and execution of the tasks.

This approach aligns with ethical research practices and modern industry workflows, where AI is commonly used as a productivity and documentation aid.