**PicoCTF Challenge Documentation**

**[GAURAV ROKADE]**

**Organisation: [ Vault-Tec Security]**

**Date: [Oct 2024]**

---

**Contents**


1. **Introduction**
2. **Methodology and Detailed Solutions**
3. **Challenge Breakdown**
4. **Conclusion**
5. **References**
6. **Acknowledgment**


---

**Contact Information:**


GAURAV MAHADU ROKADE

Intern, Vault-Tec Security, Ahmedabad, Gujarat.

linkedin.com/in/vault-tec-security-052948306


---

**Introduction**

This documentation provides a detailed report on my experience solving more than **40 challenges** from the **PicoCTF** competition. It aims to encapsulate my learning journey through various cybersecurity domains, including **Forensics**, **General Skills**, **Cryptography**, and more.

---


I would like to express my gratitude to the **PicoCTF** organizers and the cybersecurity community for facilitating a platform that fosters learning and skill development.


---

# 1. Introduction

## ❖ Purpose of Documentation

The purpose of this documentation is to provide a comprehensive and detailed account of my experiences and solutions while participating in the **PicoCTF** cybersecurity challenges. This report aims to:

- Demonstrate Understanding: Illustrate my understanding of various cybersecurity concepts and techniques across multiple domains, such as Forensics, Cryptography, and General Skills.
- Document Solutions: Capture the step-by-step processes used to solve each challenge, including my thought process, the methodologies employed, and any tools utilized.
- Reflect on Learning: Facilitate self-reflection on my learning journey, highlighting key takeaways and areas for future improvement in the field of cybersecurity.
- Serve as a Resource: Provide a valuable reference for myself and others interested in enhancing their cybersecurity skills, offering insights into problem-solving approaches and techniques.
- Encourage Collaboration: Foster a sense of community by sharing knowledge and experiences, encouraging discussions and collaborations within the cybersecurity field.

## ❖ Overview of PicoCTF

**Objectives:** The main objectives of PicoCTF are to:

- Inspire interest in cybersecurity among students and enthusiasts.
- Provide a safe and engaging platform for practical learning.
- Encourage critical thinking and problem-solving skills in a competitive yet collaborative setting.

**PicoCTF** is a cybersecurity competition designed to engage students and individuals in hands-on learning through a series of challenges that simulate real-world security scenarios. Created by the cybersecurity experts at Carnegie Mellon University, PicoCTF aims to provide participants with an interactive platform to develop and enhance their skills in various areas of cybersecurity.

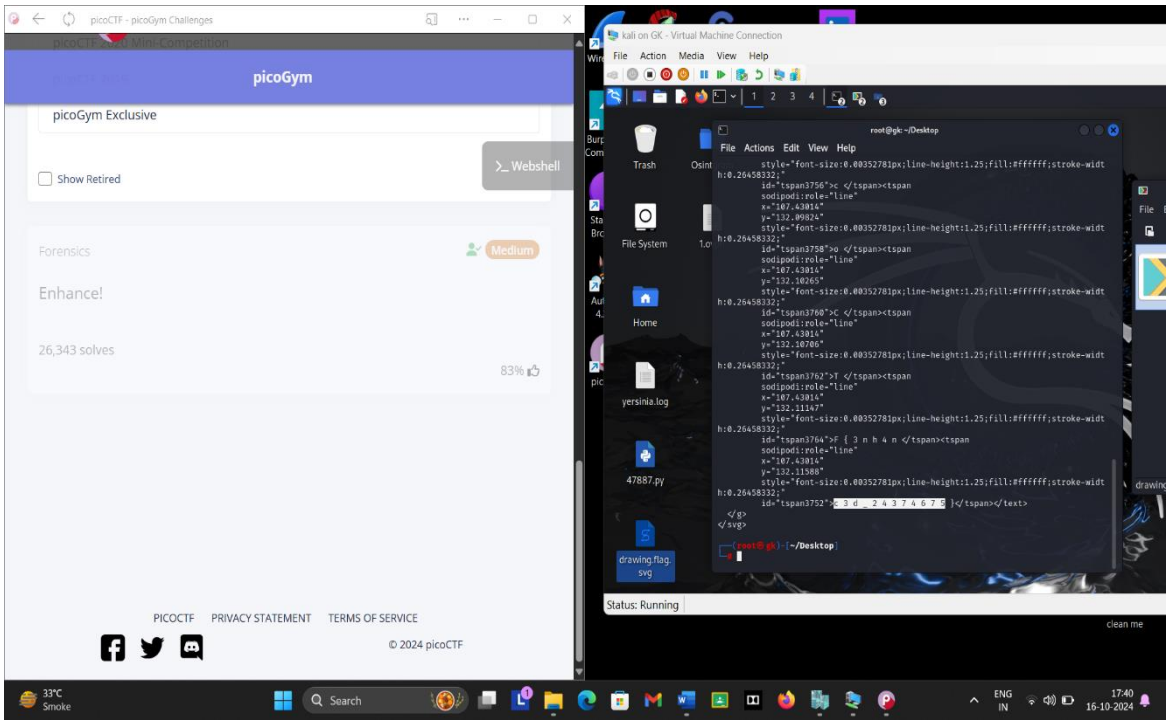
**Key Features:**

- Accessibility: PicoCTF is designed for participants of all skill levels, from beginners to advanced users. It provides educational resources and hints to guide participants through the challenges.
- Diverse Challenges: The competition includes a wide range of challenges categorized into various domains, such as: Forensics, Cryptography, Web Exploitation, Binary Exploitation
- Educational Focus: The competition emphasizes learning and skill development, encouraging participants to research and explore cybersecurity concepts.
- Community Engagement: PicoCTF fosters a supportive community where participants can discuss challenges, share strategies, and collaborate on solutions, making it a collaborative learning environment.
- Real-World Relevance: The challenges reflect real-world cybersecurity problems, equipping participants with the skills necessary to address contemporary security threats.

## 2. Methodology and Detailed Solutions

### Challenge 1: [Enhance!]

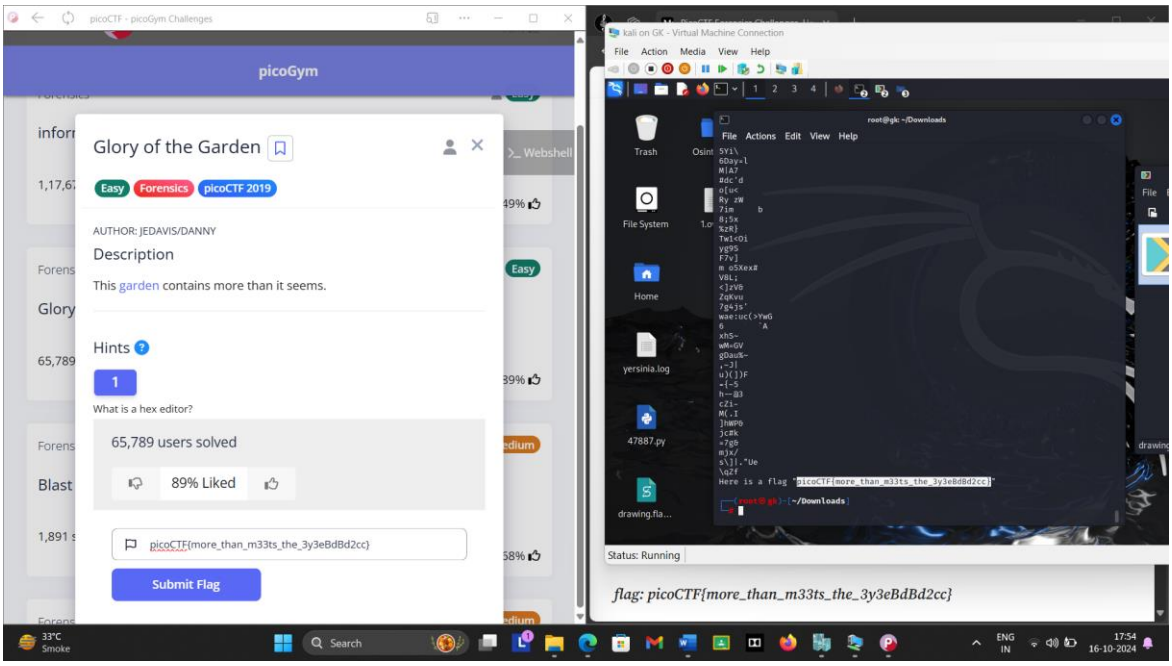
- **Category**: [Forensics]
- **Description**: Download this image file and find the flag.
- **Thought Process**: Open the image see what is form of image, try to read image via terminal see the strings of the image file
- **Solution**:




- **Outcome**: *picoCTF{3nh4n c3d_24374675}*

## Challenge 2: [Glory of the Garden]

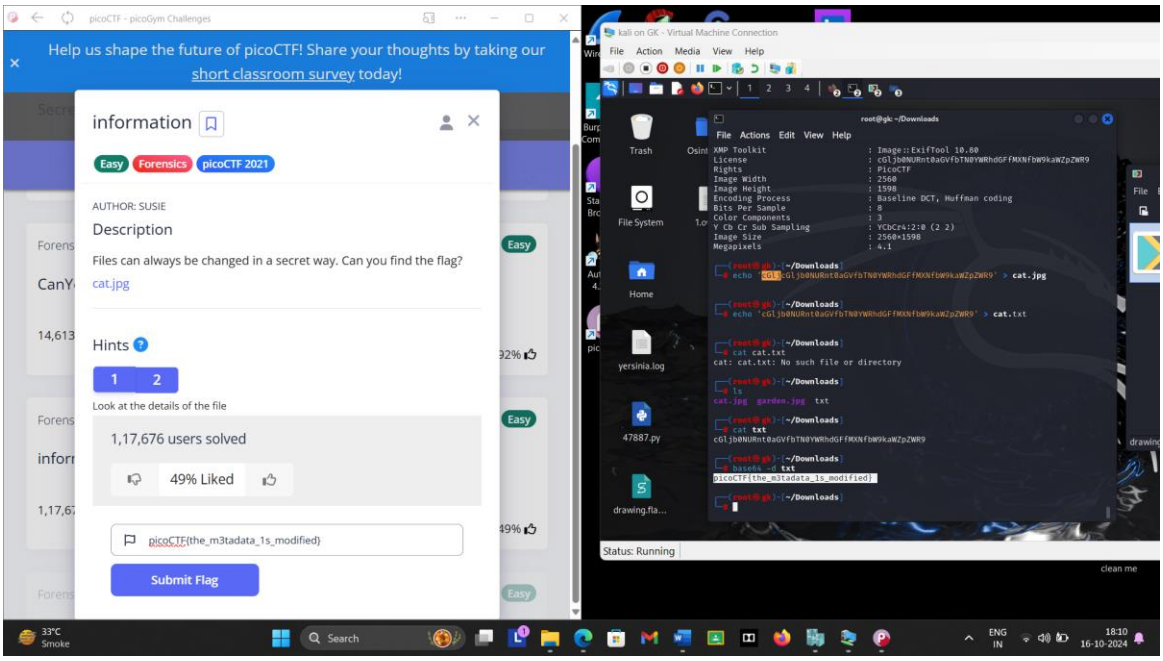
- **Category**: [Forensics]
- **Description**: This garden contains more than it seems. What is a hex editor?
- **Thought Process**: I used the ***strings*** tool for the image , Most commercial and open source forensic tools allow for string searches and will search the allocated, unallocated, and file slack spaces.
- **Solution**:




- **Outcome**: *picoCTF{more_than_m33ts_the_3y3eBdBd2cc}*

## Challenge 3: [Information]

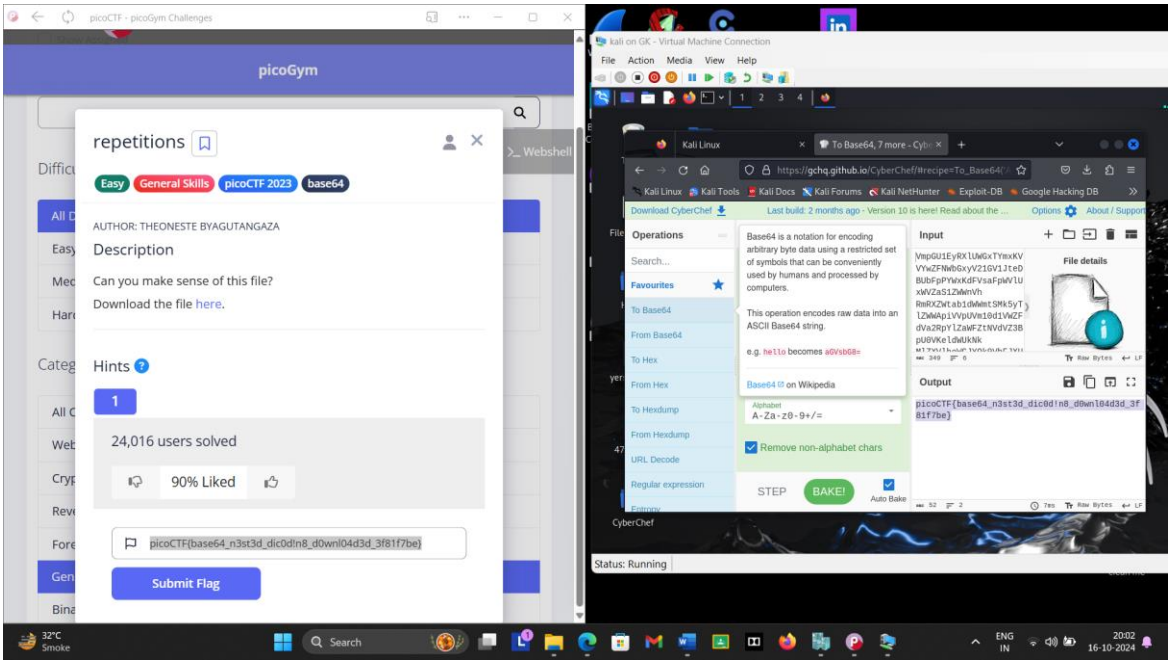
- **Category**: [Forensics]
- **Description**: Files can always be changed in a secret way. Can you find the flag? cat.jpg
- **Thought Process**: First thing I will use ***exiftool***, this is a pre-installed tool on kali that provide you with the metadata of a file/image. Found a **base64** code in the image's metadata, take the base64 code into a text file to decode it and flag is there.
- **Solution**:




- **Outcome**: *picoCTF{the_m3tadata_1s_modified}*

## Challenge 4: [repetitions]

- **Category**: [General skill]
- **Description**: Can you make sense of this file?Download the file here.
- **Thought Process**: Make sure to read the description and tags for every challenge so you'll have a better understanding on what type of challenge you're dealing with. The first **clue** to solving majority of CTF challenge is noticing the **hint** embedded in their **title.** For this challenge, download the file. Upload it to CyberChef, use the Recipe from Base64 (4) times to get the flag.
- **Solution**:



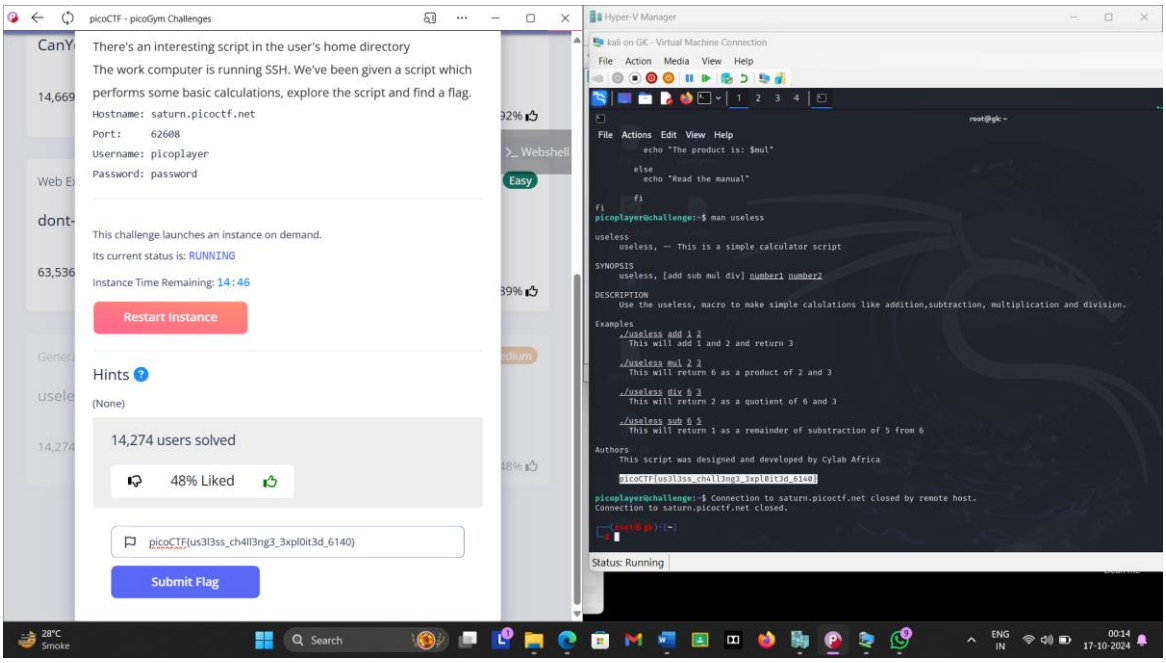

- **Outcome**: *picoCTF{base64_n3st3d_dic0d!n8_d0wnl04d3d_3f81f7be}*

## Challenge 5: [useless]

- **Category**: [General Skills]
- **Description**: There's an interesting script in the user's home directoryThe work computer is running SSH. We've been given a script which performs some basic calculations, explore the script and find a flag.

  - Hostname: saturn.picoctf.net
  - Port: 54944
  - Username: picoplayer
  - Password: password

- **Thought Process**: Launch the challenge instance then **ssh** into the remote machine, There will be an “interesting script”
- **Solution**:



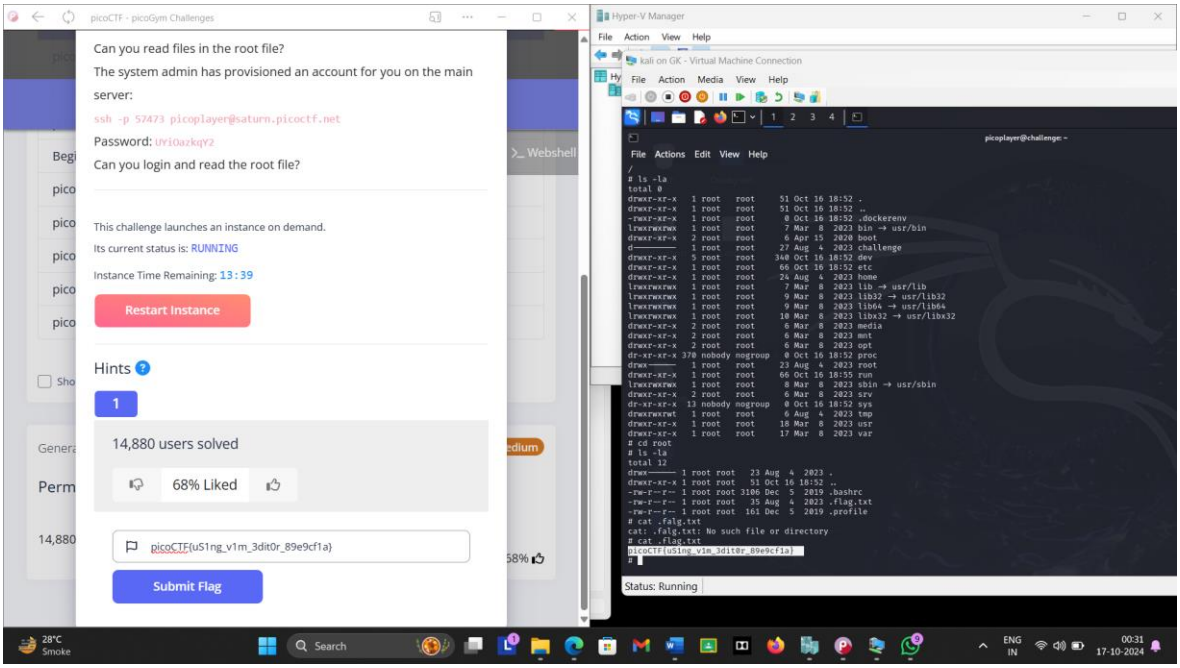

- **Outcome**: *picoCTF{us3l3ss_ch4ll3ng3_3xpl0it3d_6140}*

## Challenge 6: [permissions]

- **Category**: [General Skills]
- **Description**: Description, can you read files in the root file? Can you read files in the root file?

  - The system admin has provisioned an account for you on the main server:
  - ssh -p 57473 picoplayer@saturn.picoctf.netPassword: UYiOazkqY2
  - Can you login and read the root file?

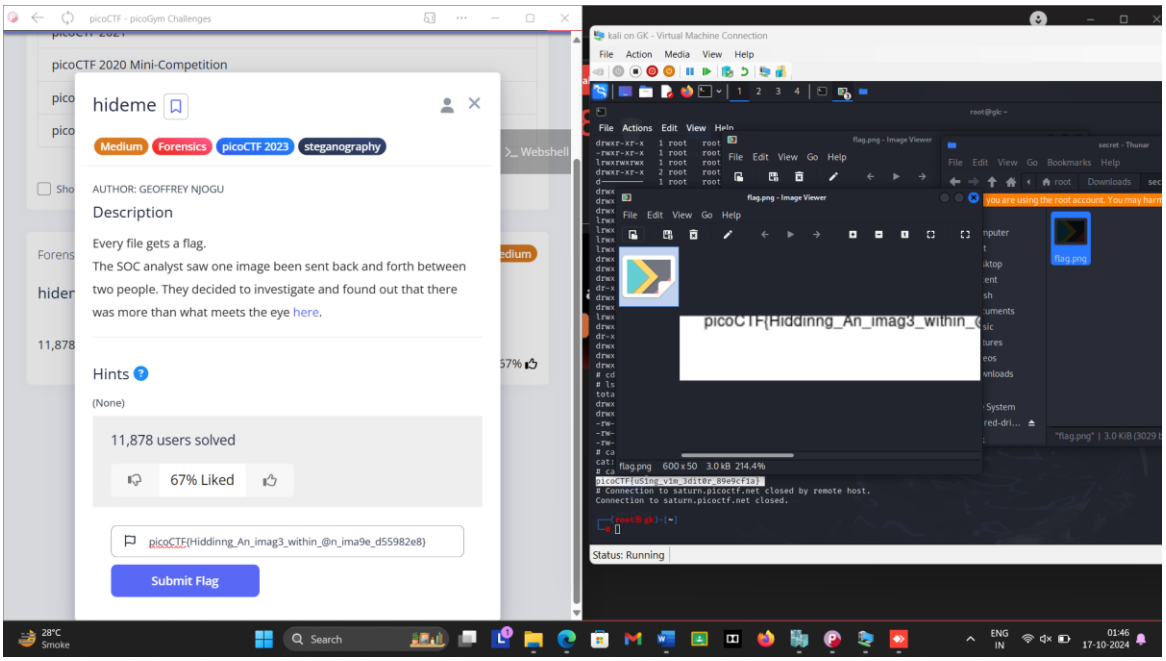
- **Thought Process**: firstly, I have to check the root user is configured with any different name or not, then try to access that user.
- **Solution**:




- **Outcome**: *picoCTF{uS1ng_v1m_3dit0r_89e9cf1a}*

## Challenge 7: [ hideme]

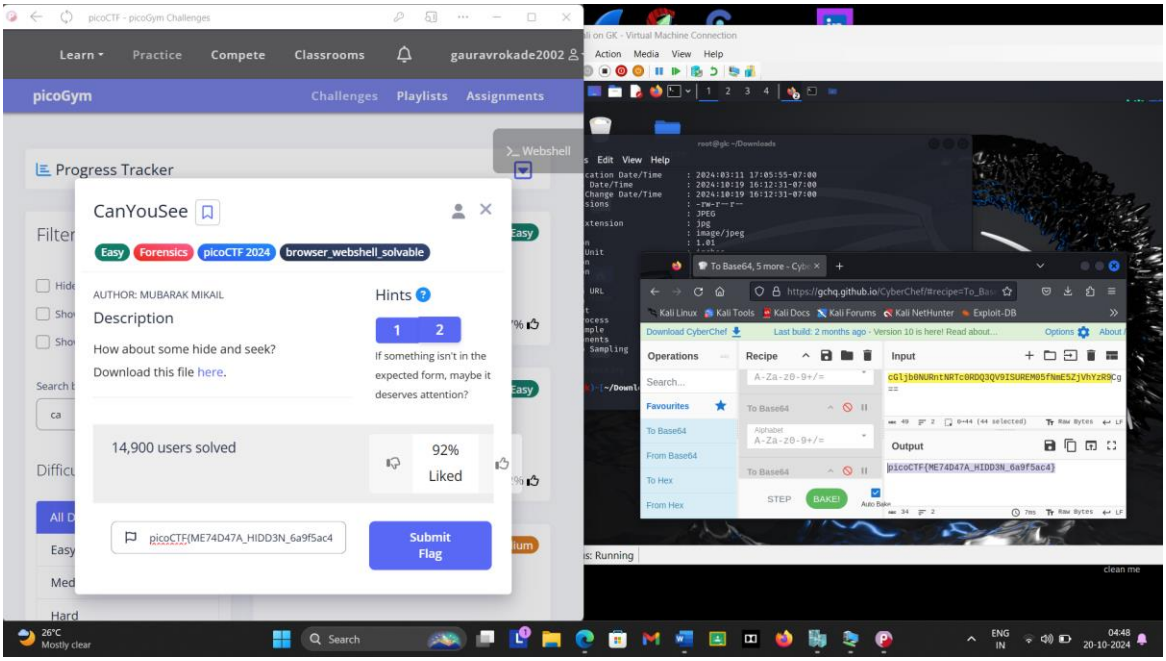
- **Category**: [Forensics]
- **Description**: Every file gets a flag.The SOC analyst saw one image been sent back and forth between two people. They decided to investigate and found out that there was more than what meets the eye here.
- **Thought Process**: with user of cyberchef exatrt files from
- **Solution**:




- **Outcome**: *picoCTF{Hidding_An_Imag3_within_@n_ima9e_d55982e8}*

## Challenge 8: [CanYouSee]

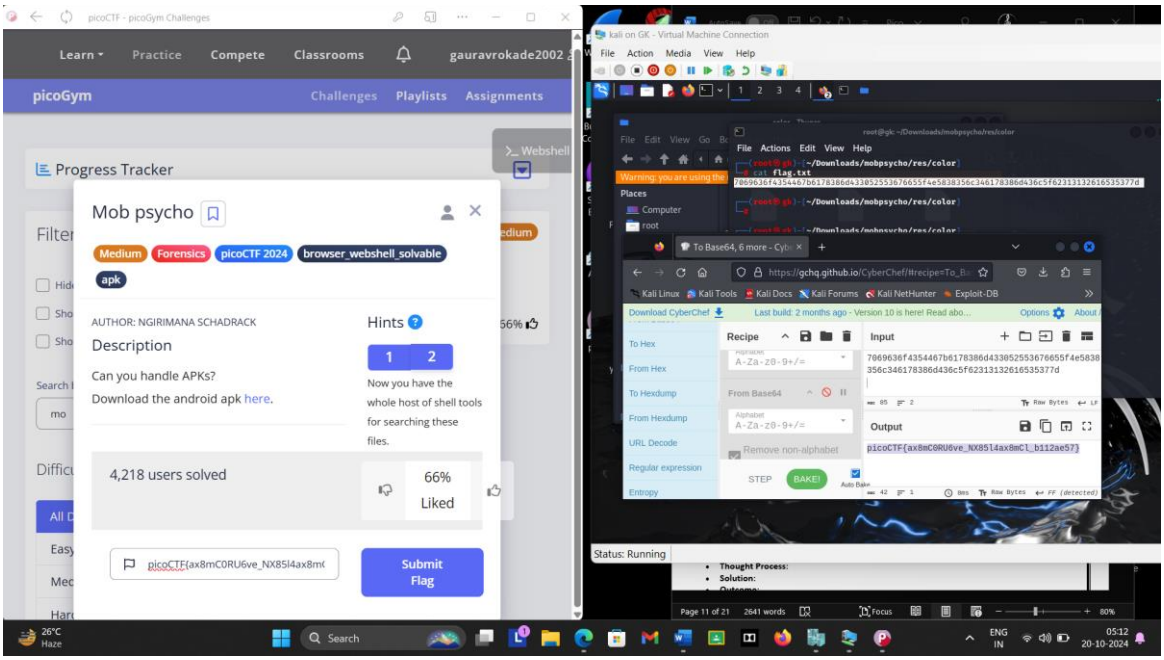
- **Category**: [Forensics]
- **Description**: How about some hide and seek?Download this file here,
- **Thought Process**: How can you view the information about the picture? If something isn't in the expected form, maybe it deserves attention?
- **Solution**:




- **Outcome**: *picoCTF{ME74D47A_HIDD3N_6a9f5ac4}*

## Challenge 9: [Mob psycho]

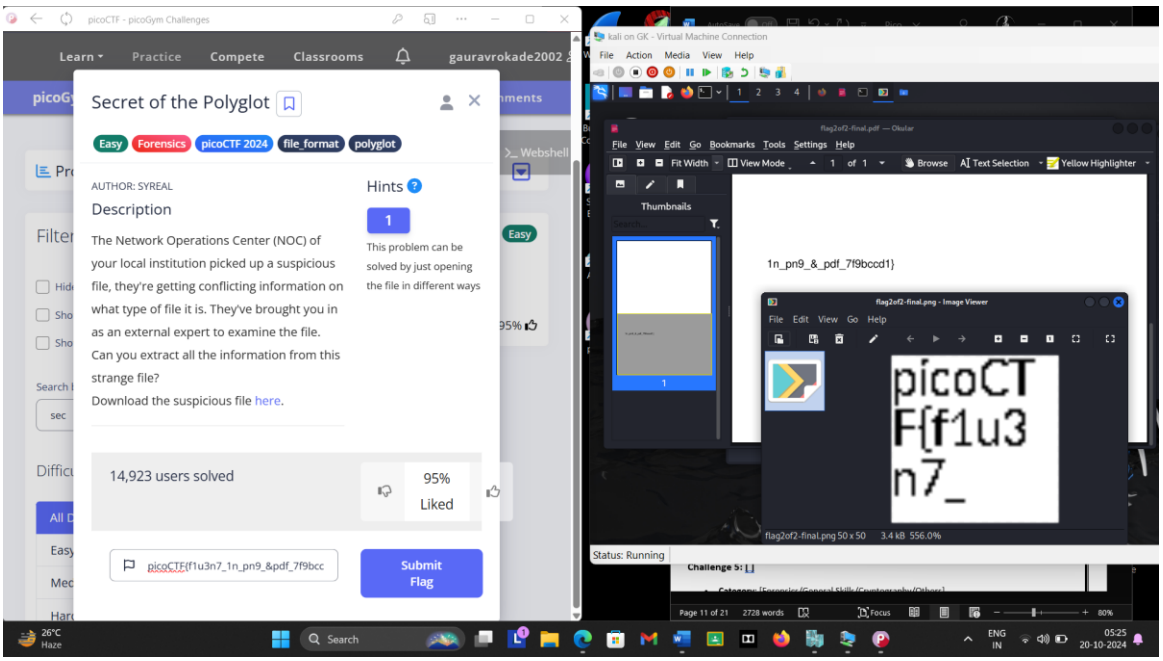
- **Category**: [Forensics]
- **Description**: Can you handle APKs?Download the android apk here.
- **Thought Process**: Now you have the whole host of shell tools for searching these files.
- **Solution**:




- **Outcome**: *picoCTF{ax8mC0RU6ve_NX85l4ax8mCl_b112ae57}*

## Challenge 10: [Secret of the Polyglot]

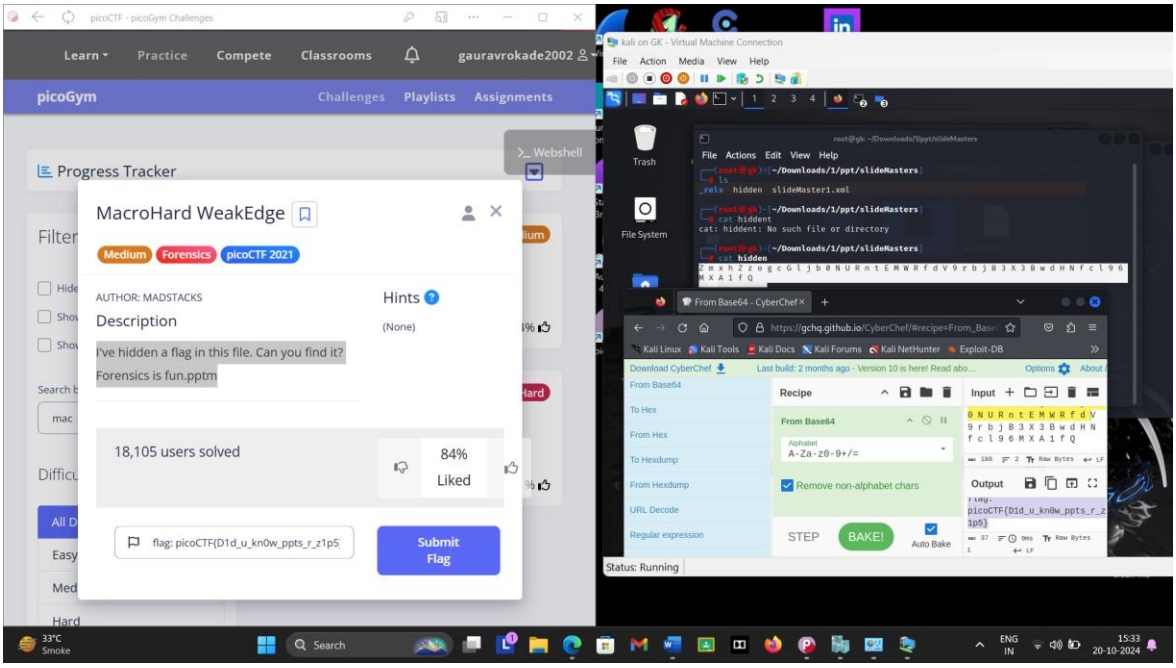
- **Category**: [Forensics/General Skills/Cryptography/Others]
- **Description**: The Network Operations Center (NOC) of your local institution picked up a suspicious file, they're getting conflicting information on what type of file it is. They've brought you in as an external expert to examine the file. Can you extract all the information from this strange file?Download the suspicious file here.
- **Thought Process**: This problem can be solved by just opening the file in different ways
- **Solution**:




- **Outcome**: *picoCTF{f1u3n7_1n_pn9_&_pdf_7f9bccd1}*

## Challenge 11: [MacroHard WeakEdge]

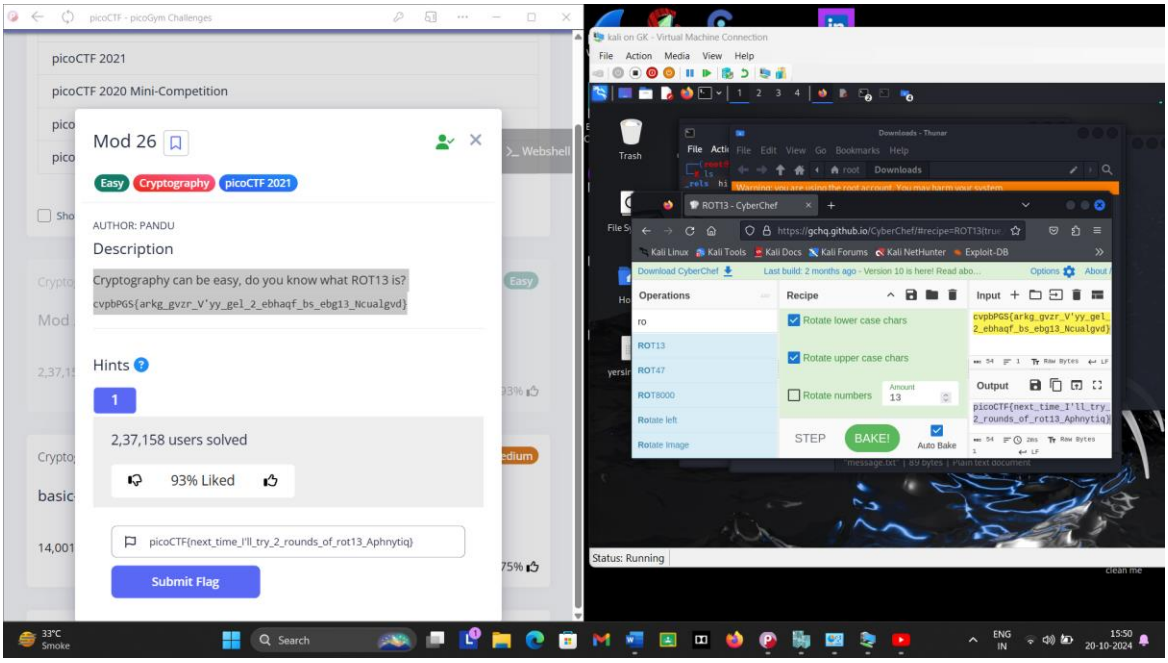
- **Category**: [Forensics]
- **Description**: I've hidden a flag in this file. Can you find it? Forensics is fun.pptm
- **Thought Process**: First I used ***strings*** tool to see the content of the file.
- I saw a very strange path that contains **hidden** file in it.
- **Solution**:




- **Outcome**: *picoCTF{D1d_u_kn0w_ppts_r_z1p5}*

## Challenge 12: [Mod 26]

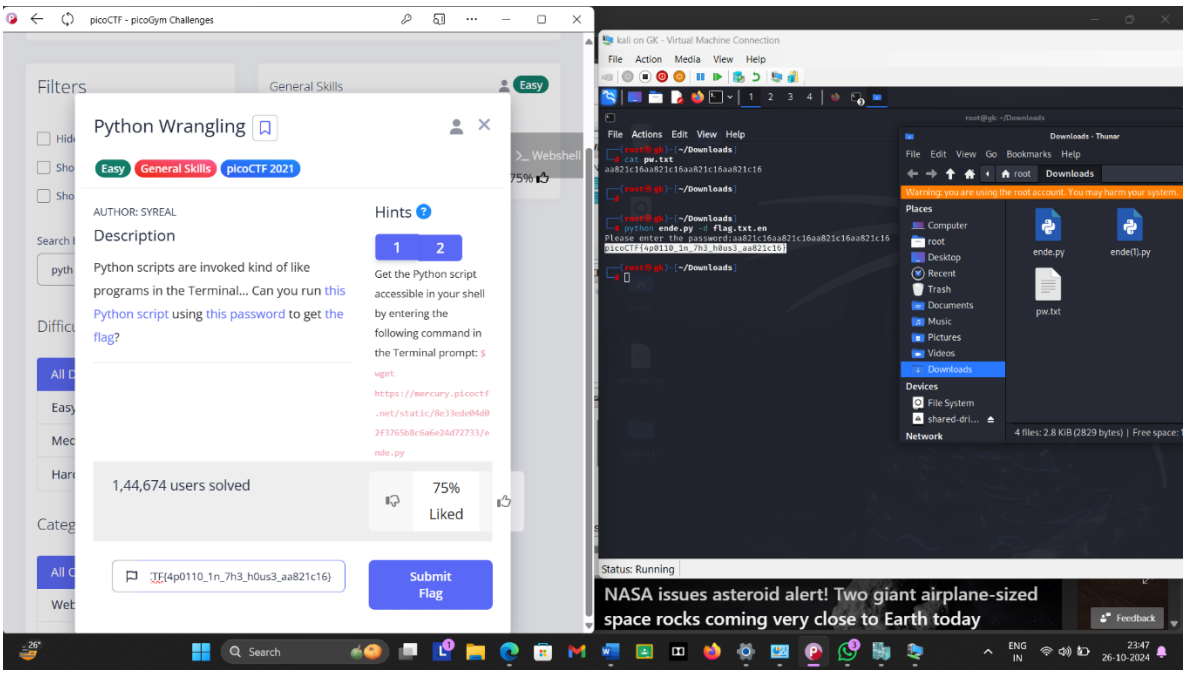
- **Category**: [Cryptography]
- **Description**: Cryptography can be easy, do you know what ROT13 is? cvpbPGS{arkg_gvzr_V'yy_gel_2_ebhaqf_bs_ebg13_Ncualgvd}
- **Thought Process**: just decode it using rot32 convertor
- **Solution**:




- **Outcome**: *picoCTF{next_time_I'll_try_2_rounds_of_rot13_Aphnytiq}*

## Challenge 13: [Python Wrangling]

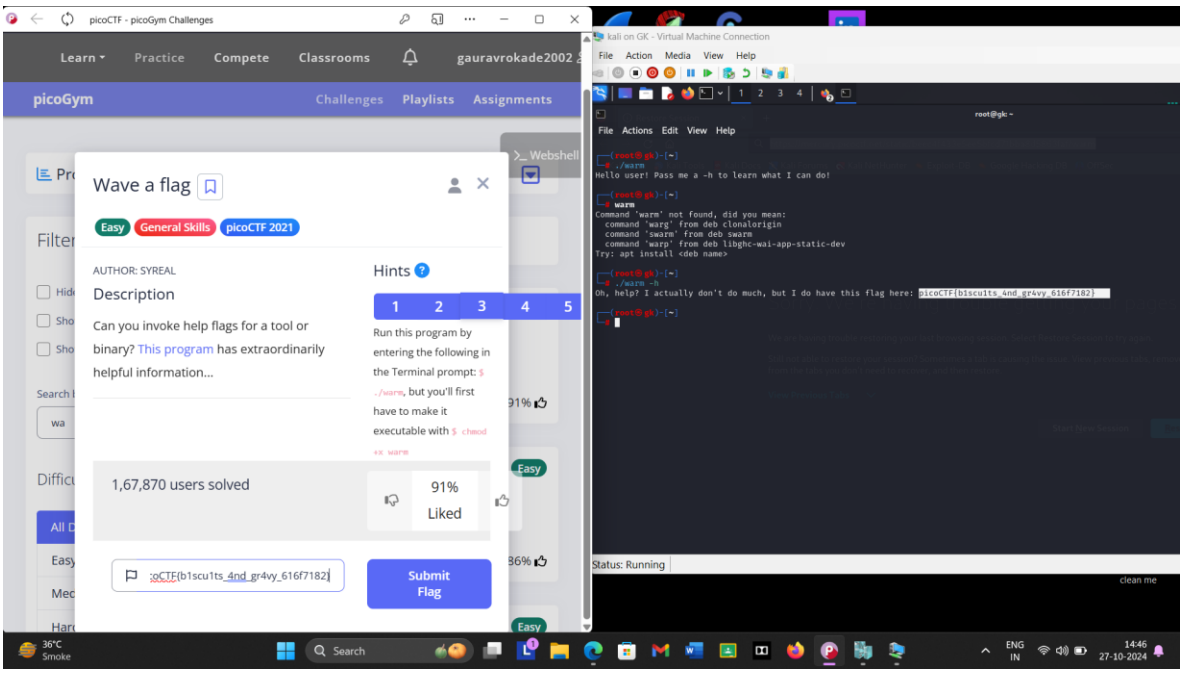
- **Category**: [General Skills]
- **Description**: Python scripts are invoked kind of like programs in the Terminal... Can you run this Python script using this password to get the flag?
- **Thought Process**: Get the Python script accessible in your shell by entering the following command in the Terminal prompt: $ wget https://mercury.picoctf.net/static/8e33ede04d02f3765b8c6a6e24d72733/ende.py
- **Solution**:




- **Outcome**: *picoCTF{4p0110_1n_7h3_h0us3_aa821c16}*

## Challenge 14: [Wave a flag]

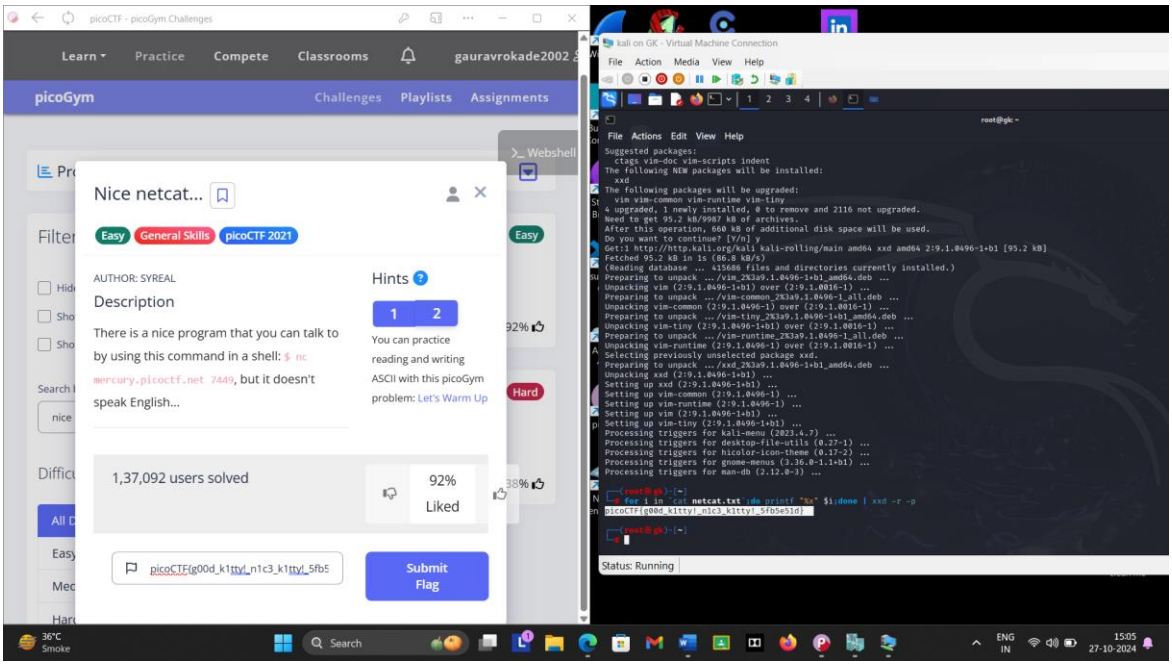
- **Category**: [General Skills]
- **Description**: Can you invoke help flags for a tool or binary? This program has extraordinarily helpful information...
- **Thought Process**: Run this program by entering the following in the Terminal prompt: $ ./warm, but you'll first have to make it executable with $ chmod +x warm and -h and --help are the most common arguments to give to programs to get more information from them!
- **Solution**:




- **Outcome**: *picoCTF{b1scu1ts_4nd_gr4vy_616f7182}*

## Challenge 15: [Nice netcat...]

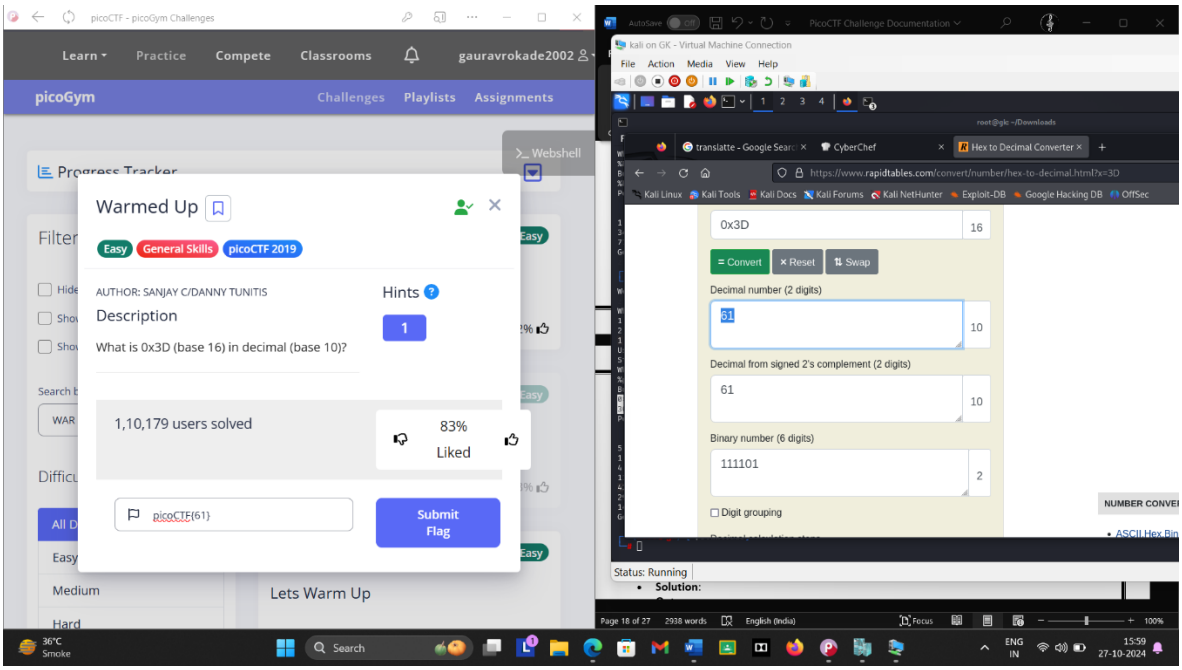
- **Category**: [General Skills]
- **Description**: There is a nice program that you can talk to by using this command in a shell: $ nc mercury.picoctf.net 7449, but it doesn't speak English...
- **Thought Process**: simple just try to decode it bt hexadecimal the we can try hex or base64 or ascii convert
- **Solution**:




- **Outcome**: *picoCTF{g00d_k1tty!_n1c3_k1tty!_5fb5e51d}*

## Challenge 16: [Warmed up]

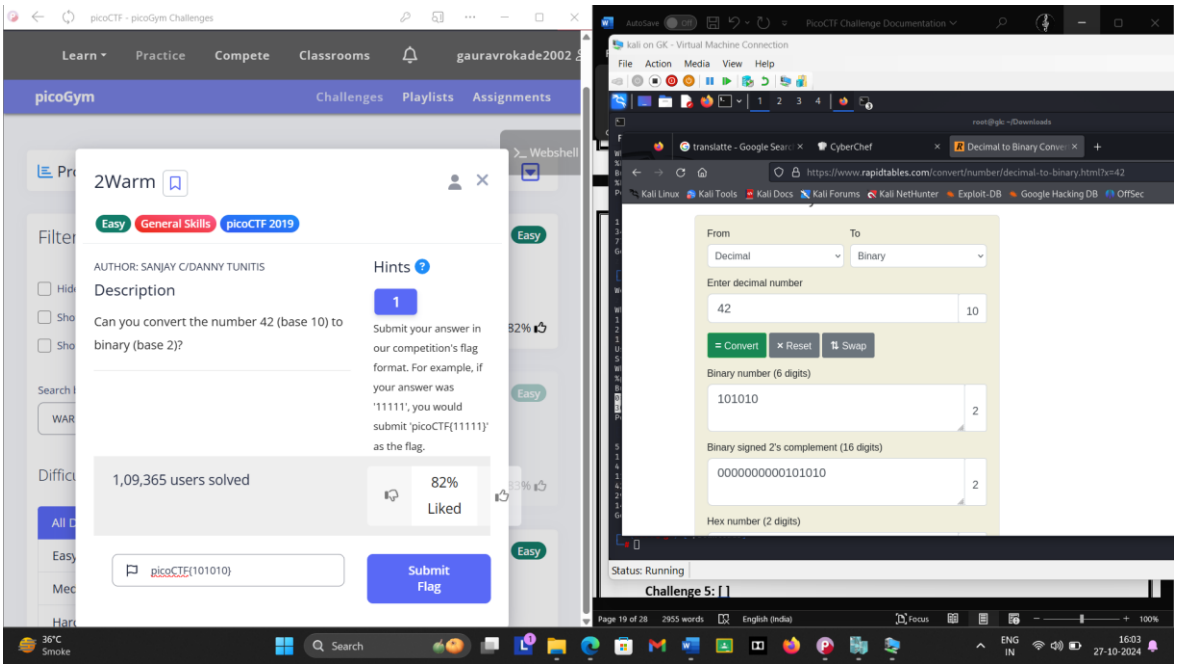
- **Category**: [General Skills]
- **Description**: What is 0x3D (base 16) in decimal (base 10)?
- **Thought Process**: I can use online convertor for this
- **Solution**:




- **Outcome**: *picoCTF{61}*

## Challenge 17: [2 warm]

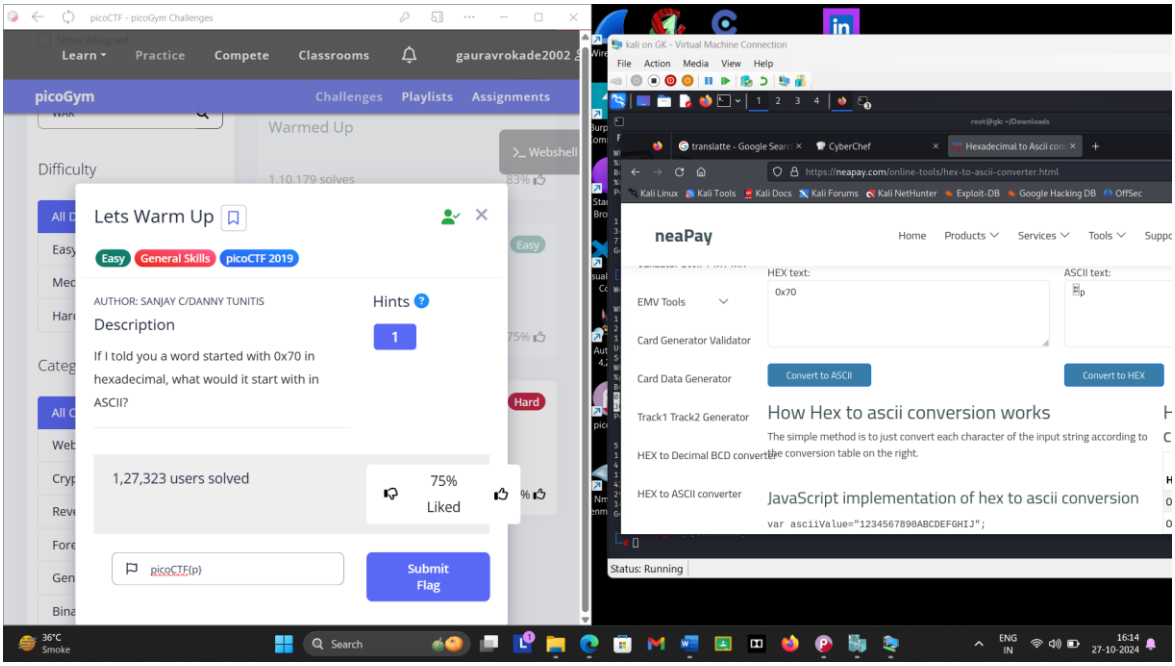
- **Category**: [Forensics/General Skills/Cryptography/Others]
- **Description**: Can you convert the number 42 (base 10) to binary (base 2)?
- **Thought Process**: I can you online convertor
- **Solution**:




- **Outcome**: *picoCTF{101010}*

## Challenge 18: [Lets Warm Up]

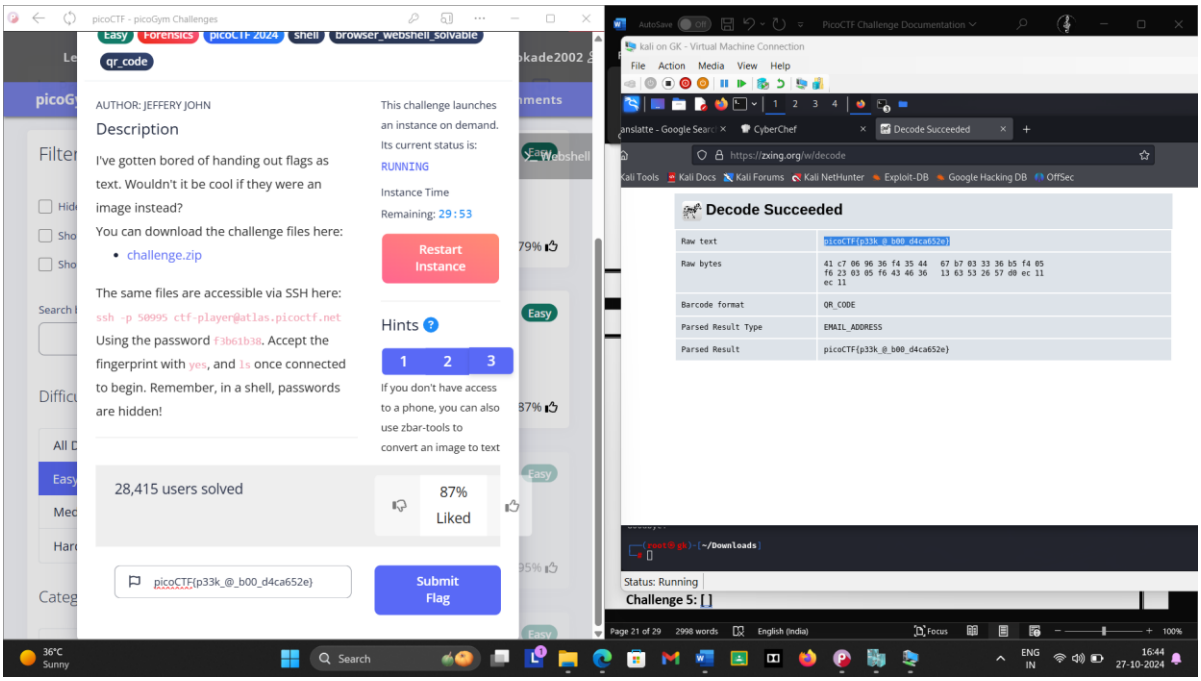
- **Category**: [General Skills]
- **Description**: If I told you a word started with 0x70 in hexadecimal, what would it start with in ASCII?
- **Thought Process**: use online tool for this
- **Solution**:




- **Outcome**: *picoCTF{p}*

## Challenge 19: [Scan Surprise]

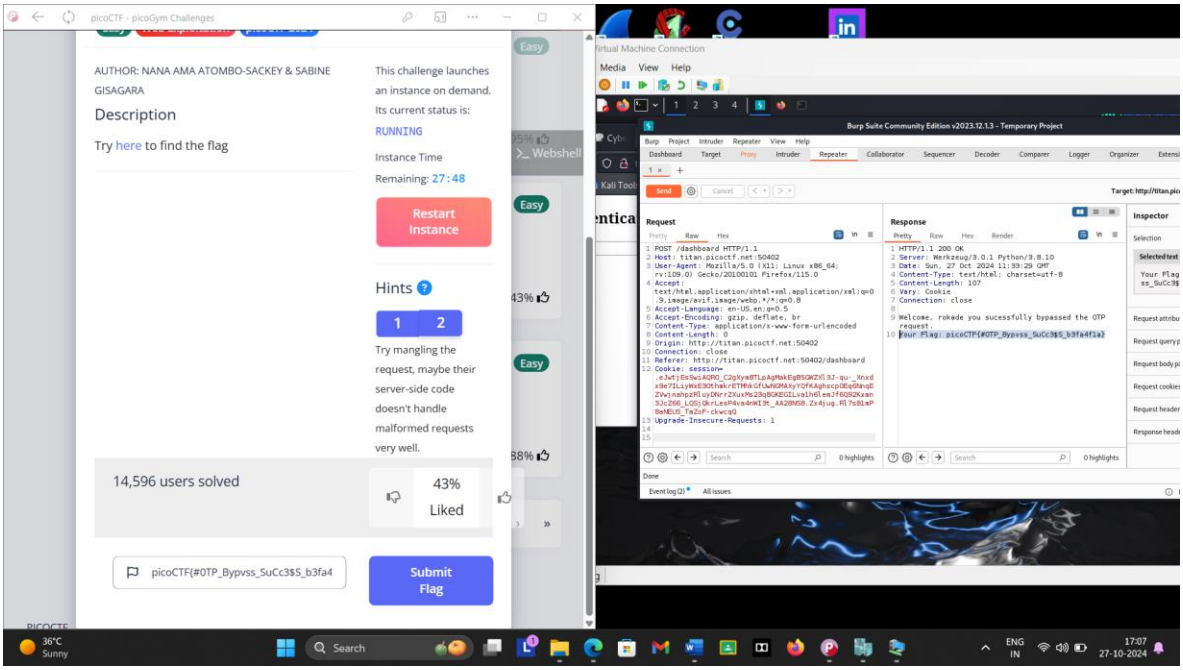
- **Category**: [Forensics]
- **Description**: I've gotten bored of handing out flags as text. Wouldn't it be cool if they were an image instead?You can download the challenge files here:
- challenge.zip
- **Thought Process**: QR cod  reader can help me out
- **Solution**:




- **Outcome**: *picoCTF{p33k_@_b00_d4ca652e}*

## Challenge 20: [ IntroToBurp]

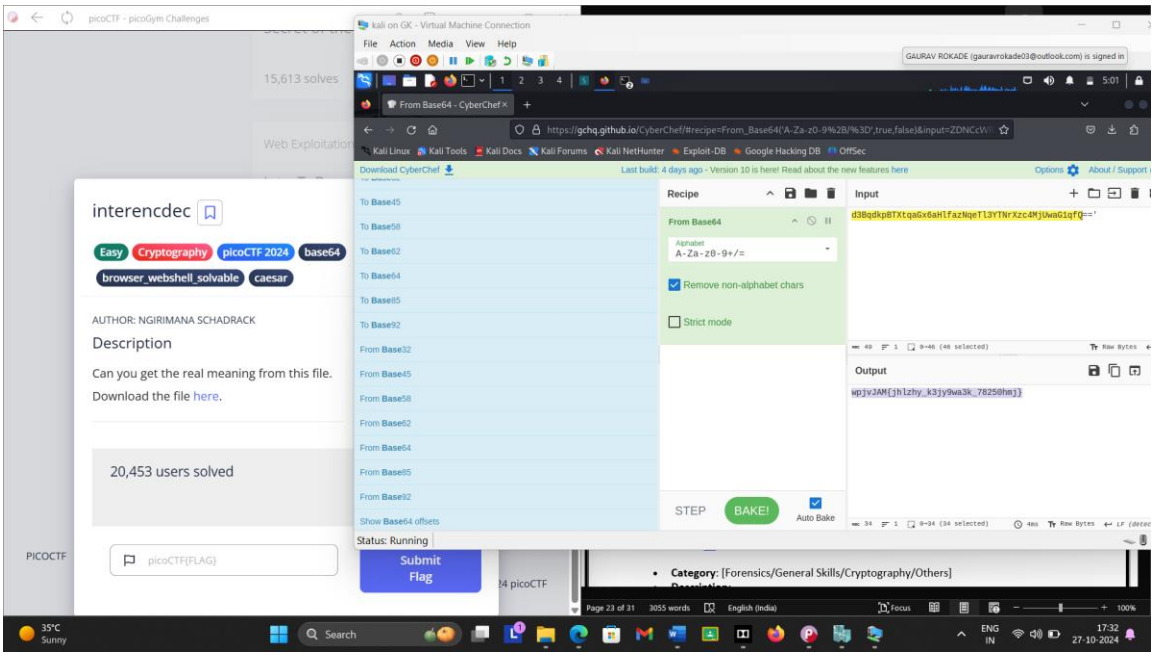
- **Category**: [Others (web exploitation)]
- **Description**: capture the flag from burp suit
- **Thought Process**: try to find out any flag with capture the request in burp by change the input
- **Solution**:



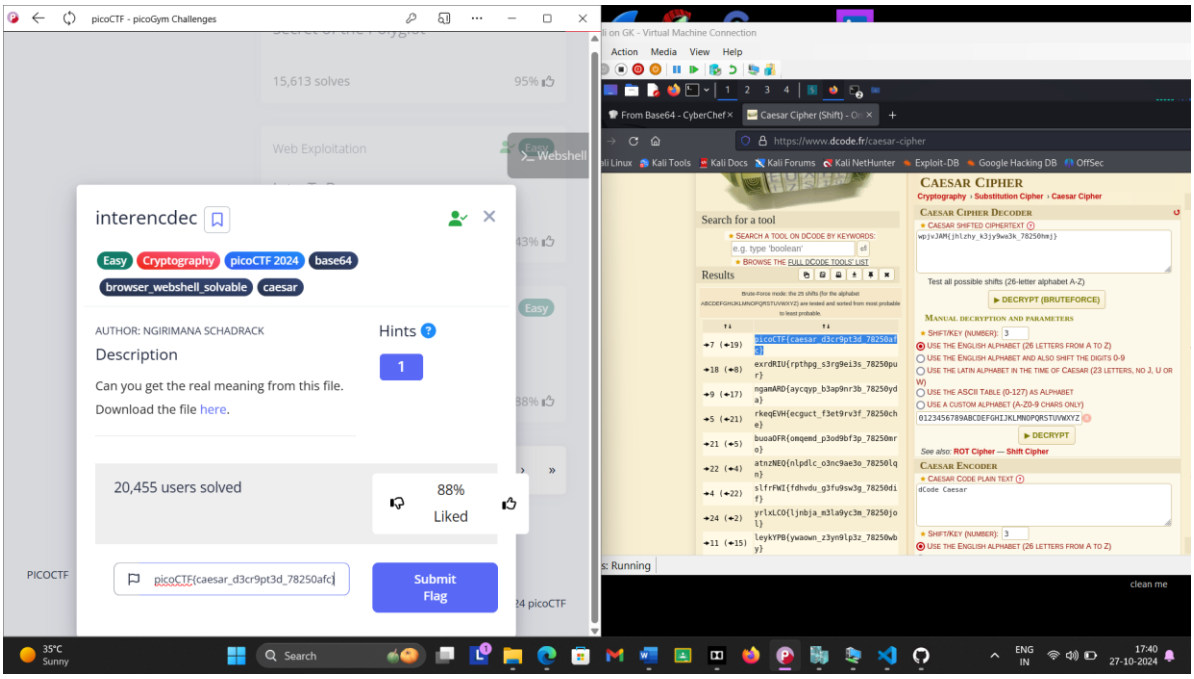

- **Outcome**: *picoCTF{#0TP_Bypvss_SuCc3$S_b3fa4f1a}*

## Challenge 21: [ ]

- **Category**: [Cryptography]
- **Description**:
- **Thought Process**:
- **Solution**:



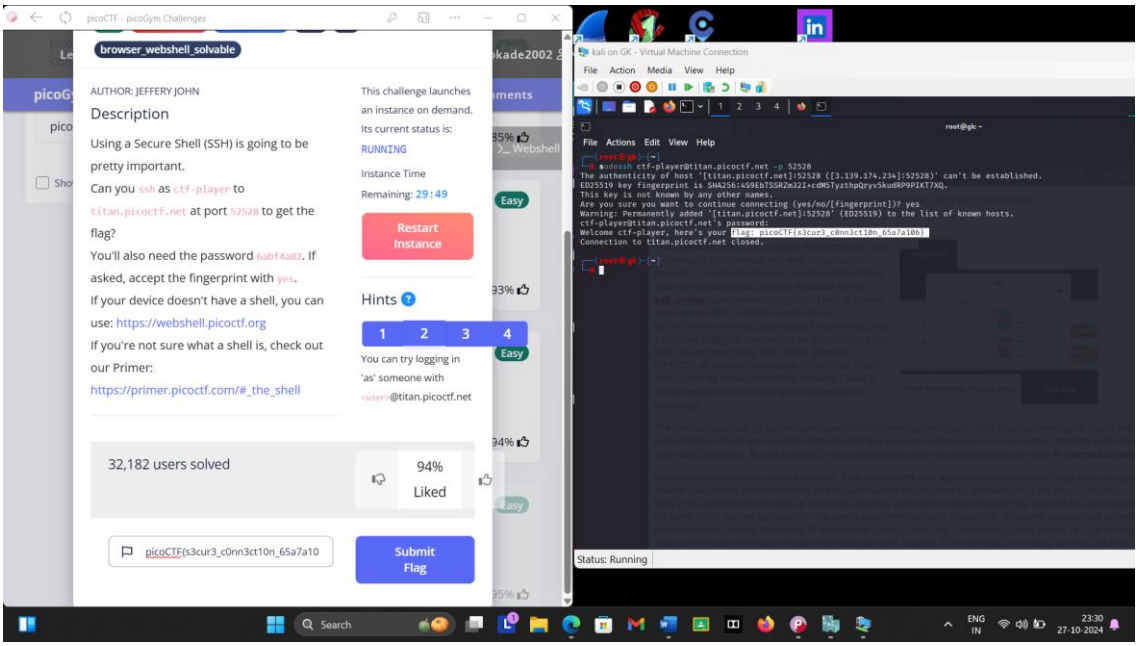

Caesar chipper tool




- **Outcome**: *picoCTF{caesar_d3cr9pt3d_78250afc}*

## Challenge 22: [ ]

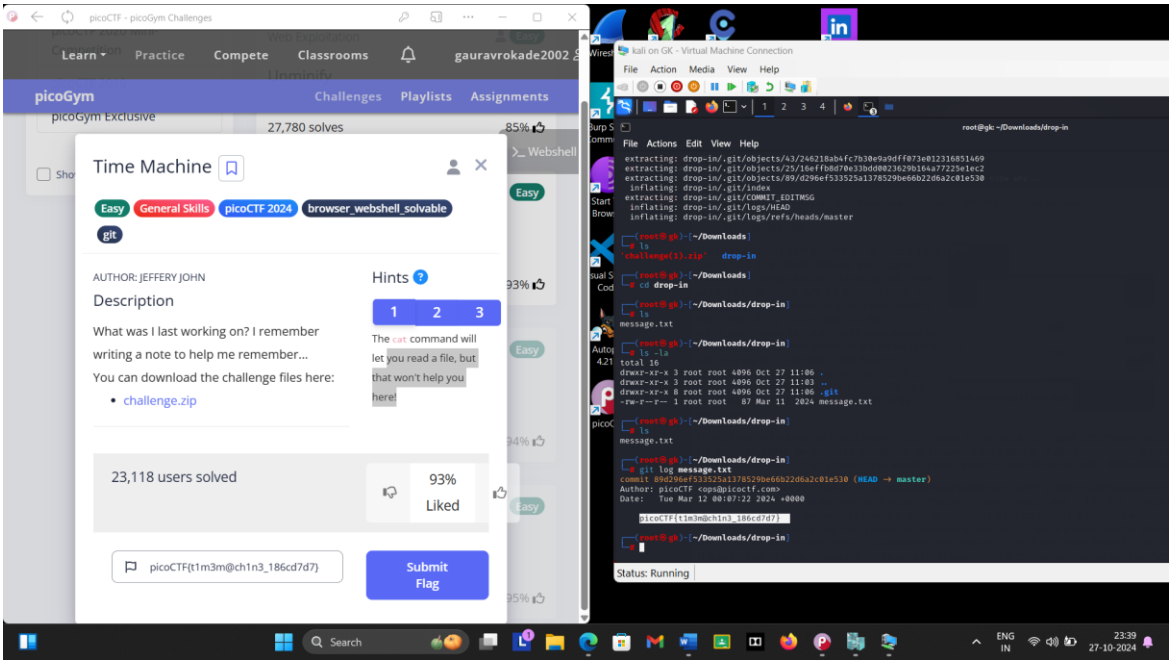
- **Category**: [General Skills]
- **Description**: Using a Secure Shell (SSH) is going to be pretty important.Can you ssh as ctf-player to titan.picoctf.net at port 52528 to get the flag?You'll also need the password 6abf4a82. If asked, accept the fingerprint with yes.
- **Thought Process**: You can try logging in 'as' someone with <user>@titan.picoctf.net
- **Solution**:




- **Outcome**: *picoCTF{s3cur3_c0nn3ct10n_65a7a106}*

## Challenge 23: [Time machine]

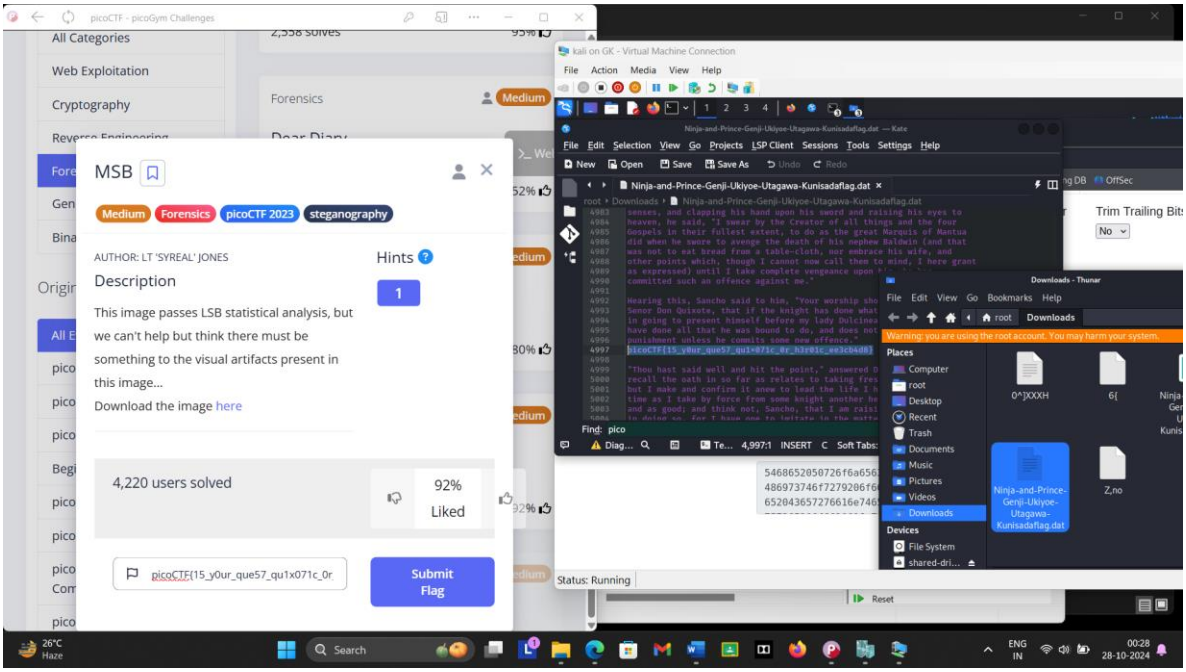
- **Category**: [General Skills]
- **Description**: What was I last working on? I remember writing a note to help me remember...You can download the challenge files here: challenge.zip
- **Thought Process**: git log file
- **Solution**:




- **Outcome**: *picoCTF{t1m3m@ch1n3_186cd7d7}*

## Challenge 24: [MSB]

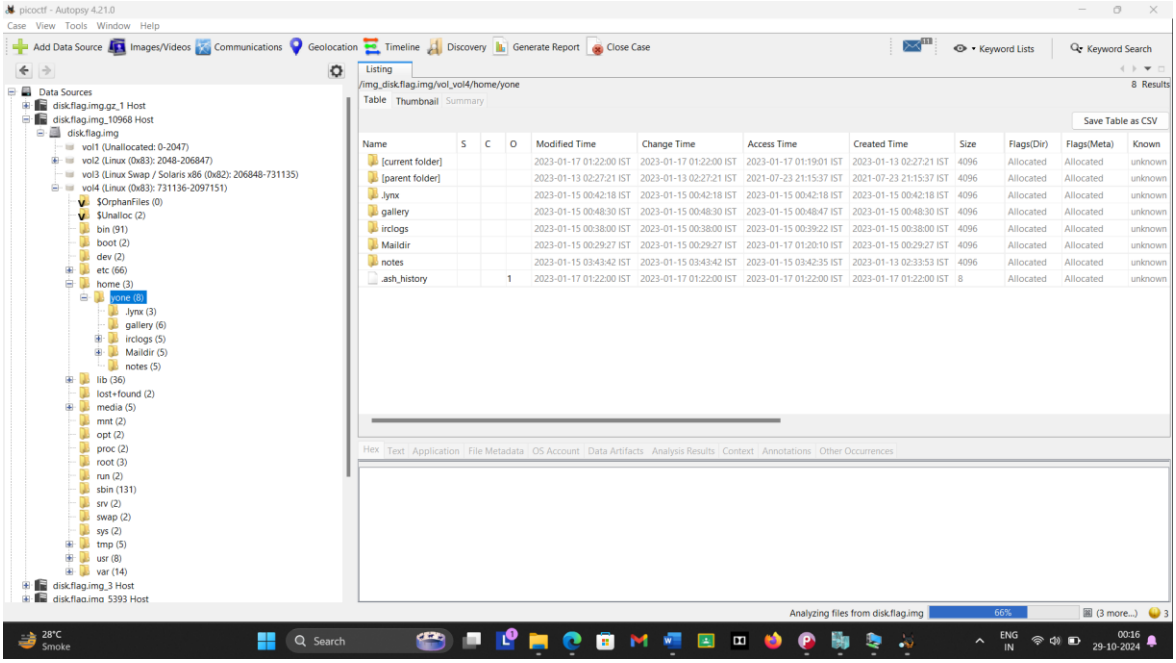
- **Category**: [Forensics]
- **Description**: This image passes LSB statistical analysis, but we can't help but think there must be something to the visual artifacts present in this image...Download the image here
- **Thought Process**:  What's causing the 'corruption' of the image? Search through out file
- **Solution**:

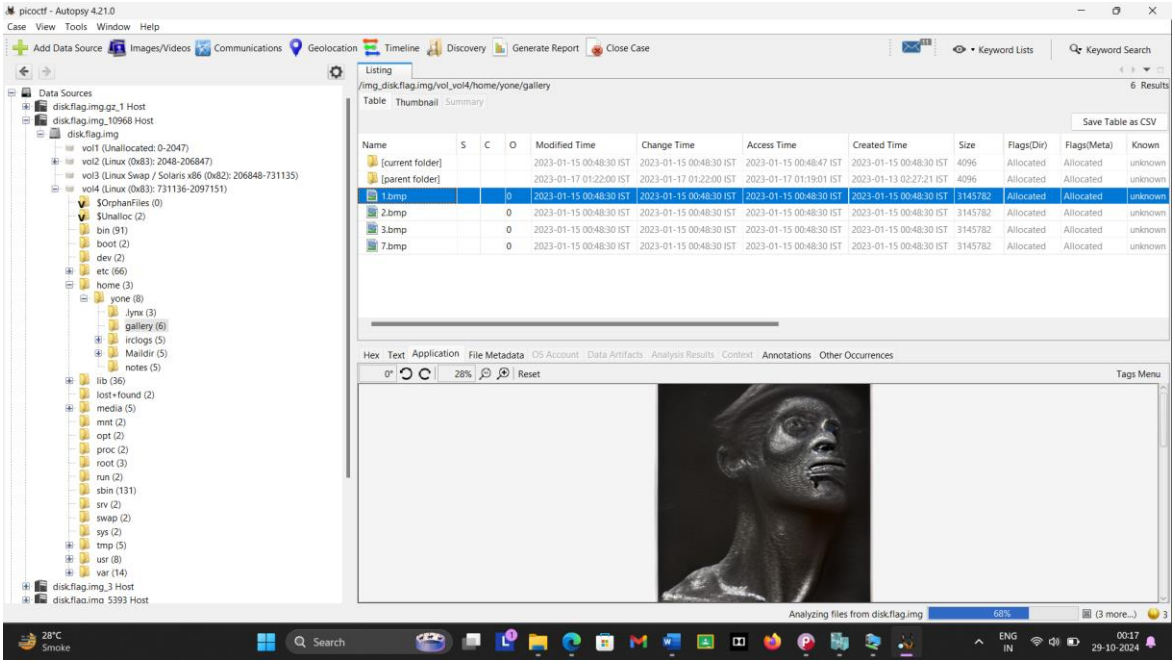


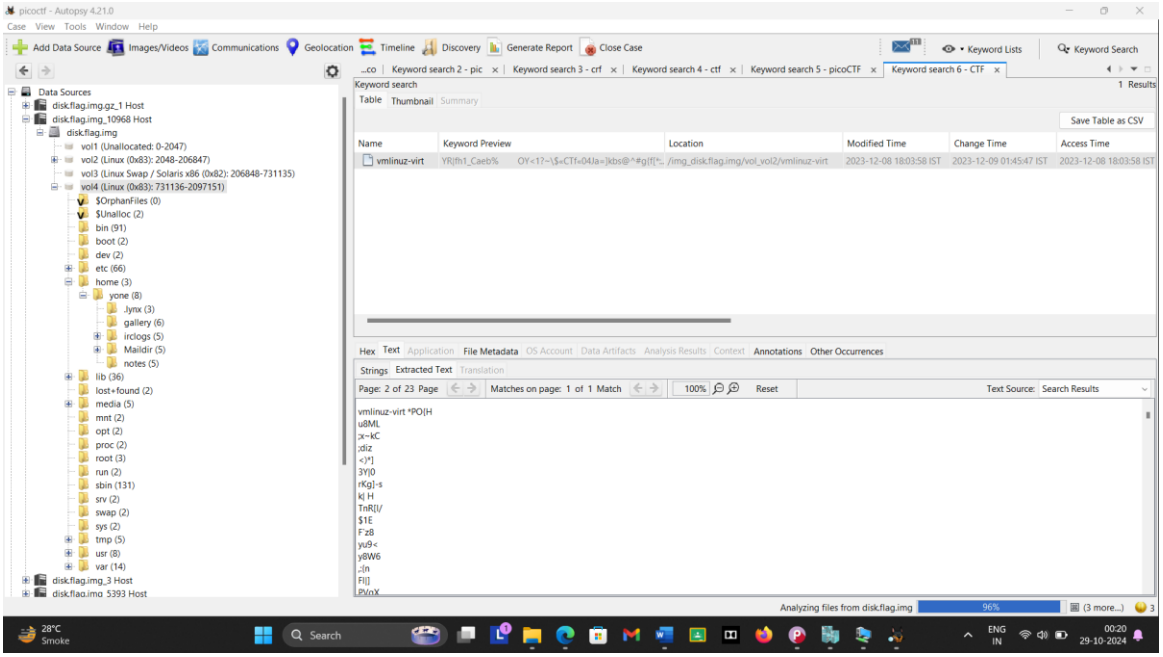

- **Outcome**: *picoCTF{15_y0ur_que57_qu1x071c_0r_h3r01c_ee3cb4d8}*

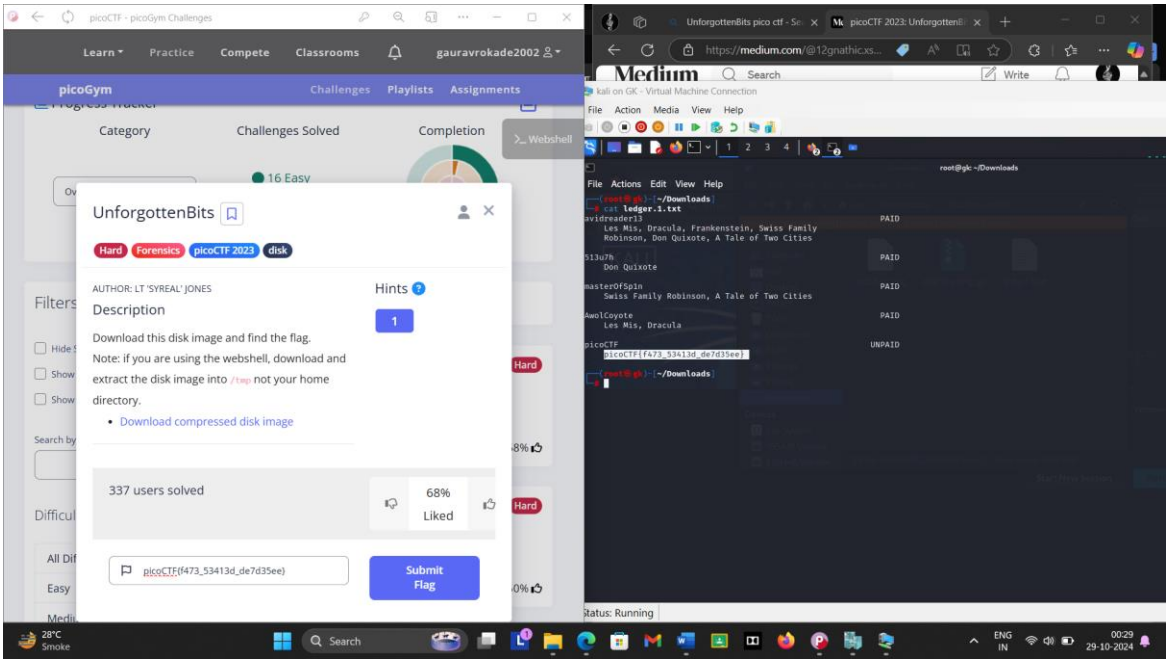
## Challenge 25: [ ]

- **Category**: [Forensics/General Skills/Cryptography/Others]
- **Description**: find the flag from given disk
- **Thought Process**: let just elaborate the disk using autopsy tool
- **Solution**:



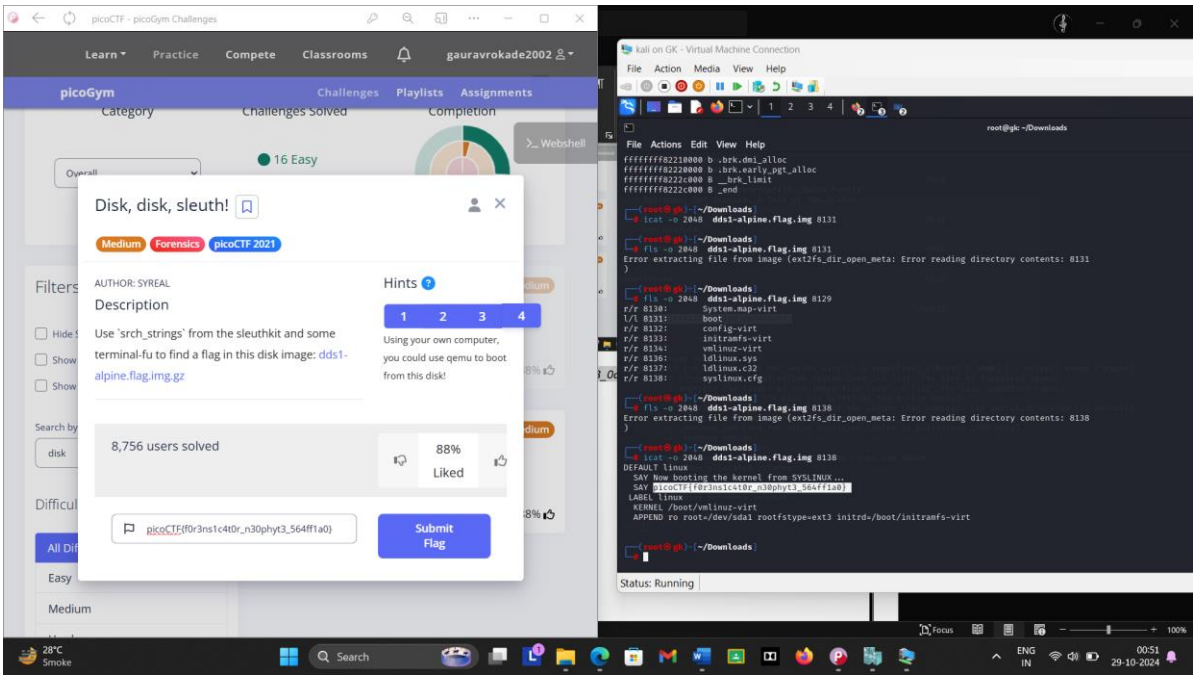



- **Outcome**: *picoCTF{f473_53413d_de7d35ee}*

## Challenge 26: [Disk, disk, sleuth!]

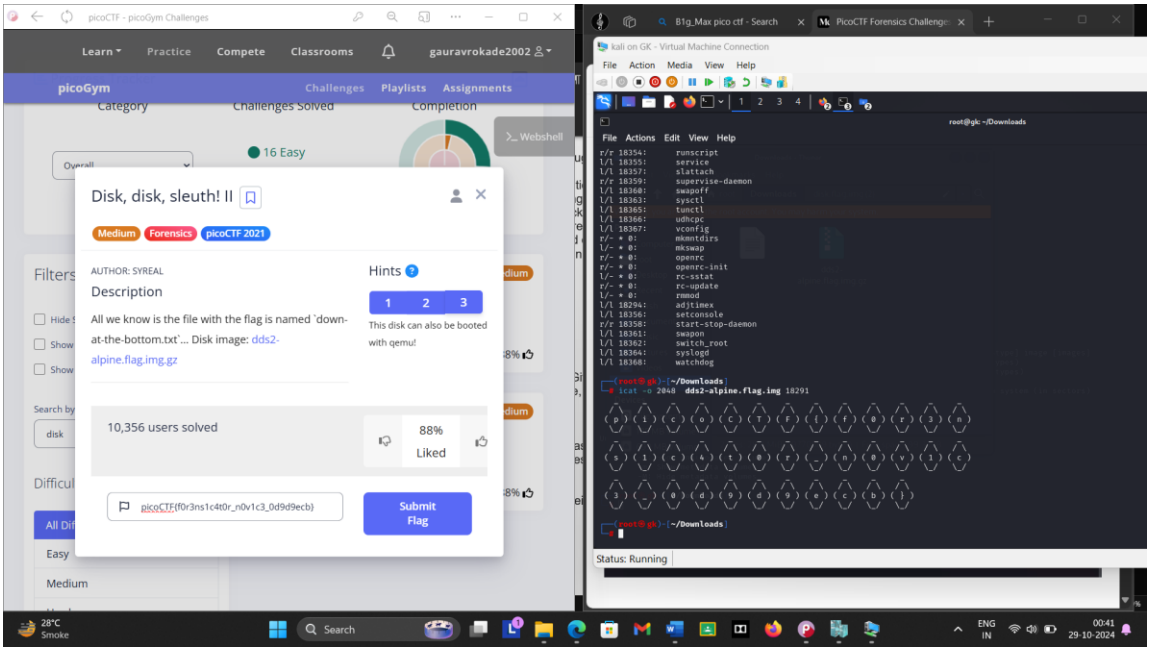
- **Category**: [Forensics]
- **Description**: Use `srch_strings` from the sleuthkit and some terminal-fu to find a flag in this disk image: [dds1-alpine.flag.img.gz]
- **Thought Process**: Using your own computer, you could use qemu to boot from this disk! Now try to search for the boot files
- **Solution**:




- **Outcome**: *picoCTF{f0r3ns1c4t0r_n30phyt3_564ff1a0*

## Challenge 27: [ Disk, disk, sleuth! II]

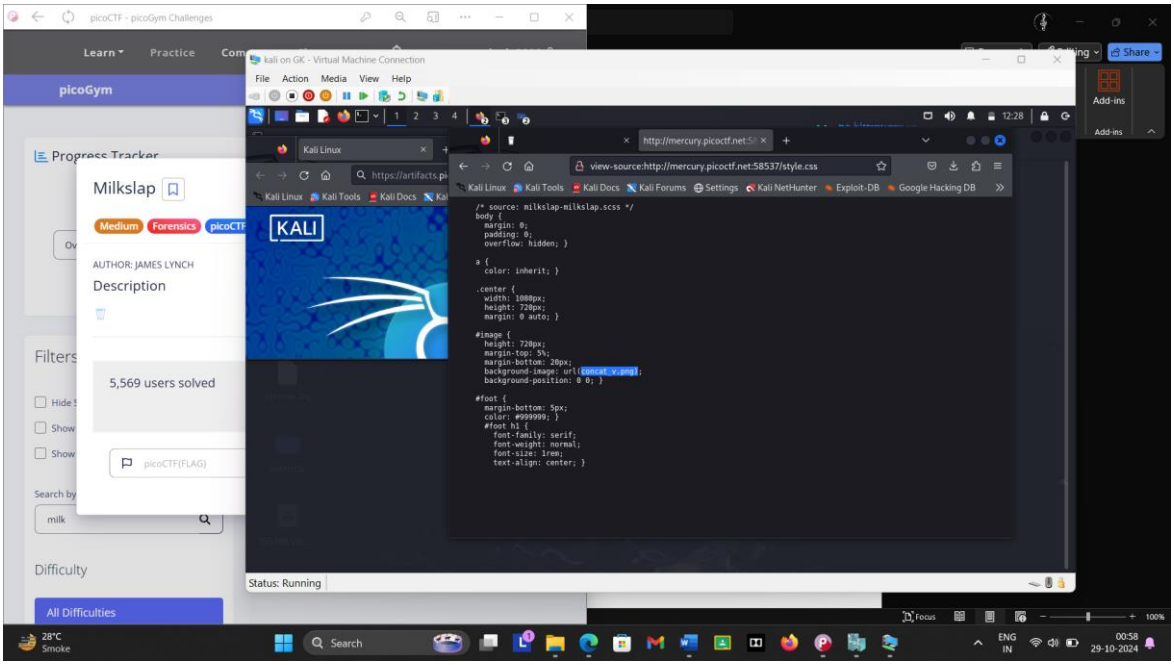
- **Category**: [Forensics]
- **Description**: All we know is the file with the flag is named `down-at-the-bottom.txt`... Disk image: [dds2-alpine.flag.img.gz]
- **Thought Process**: This disk can also be booted with qemu! Check out from the root file
- **Solution**:

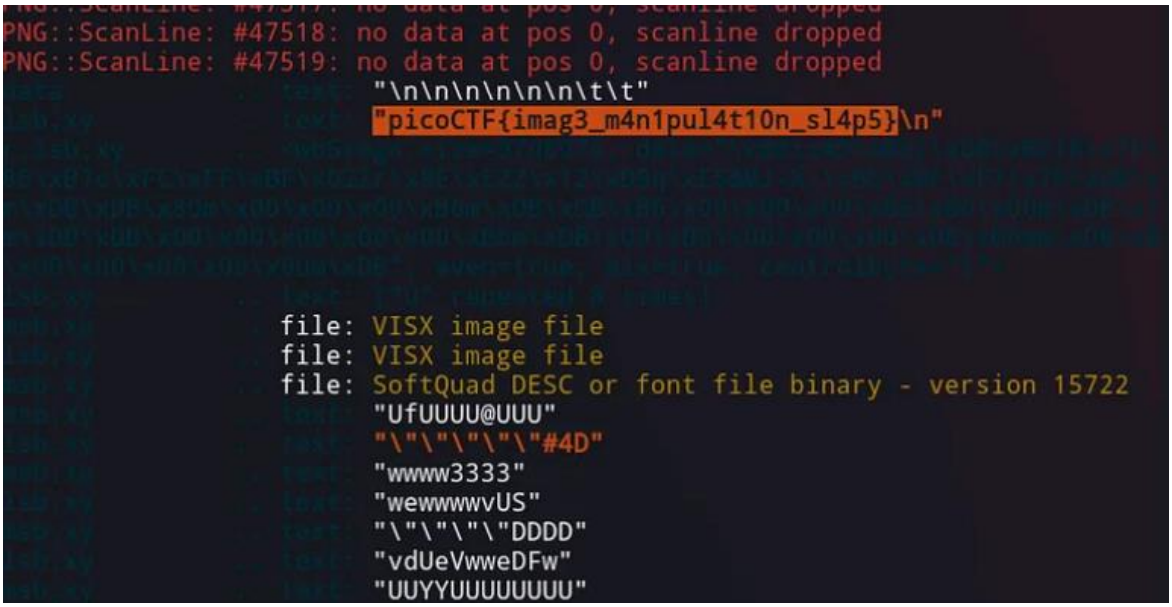


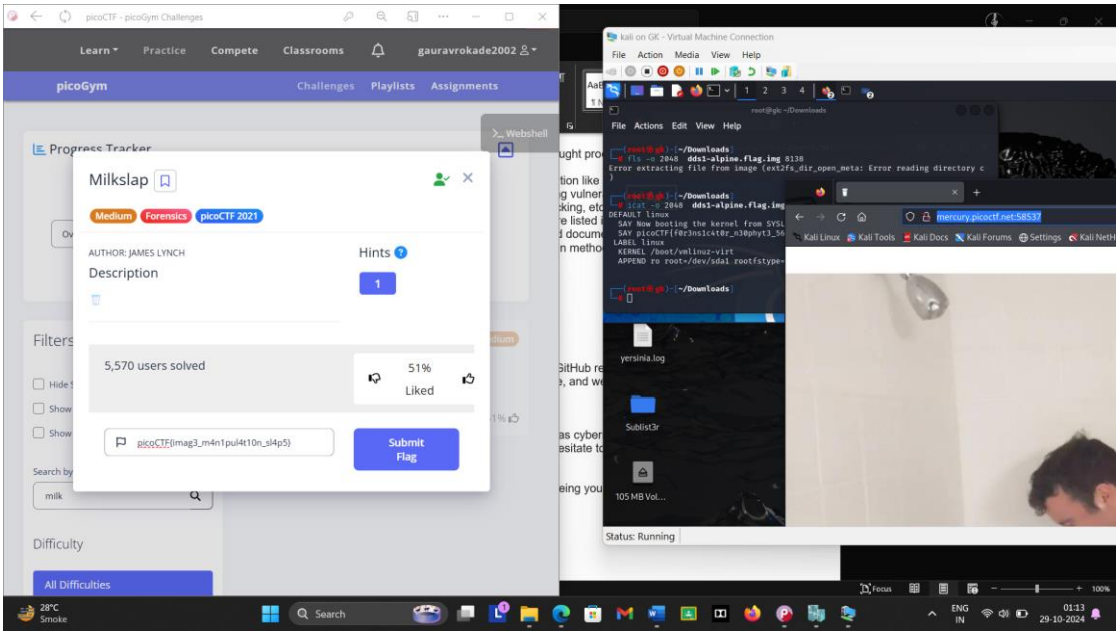

- **Outcome**: *picoCTF{f0r3ns1c4t0r_n0v1c3_0d9d9ecb}*

## Challenge 28: [Milkslap]

- **Category**: [Forensics]
- **Description**: site is provided
- **Thought Process**: inside css langange png file is there cat the file using or try using tools like zstag
- **Solution**:



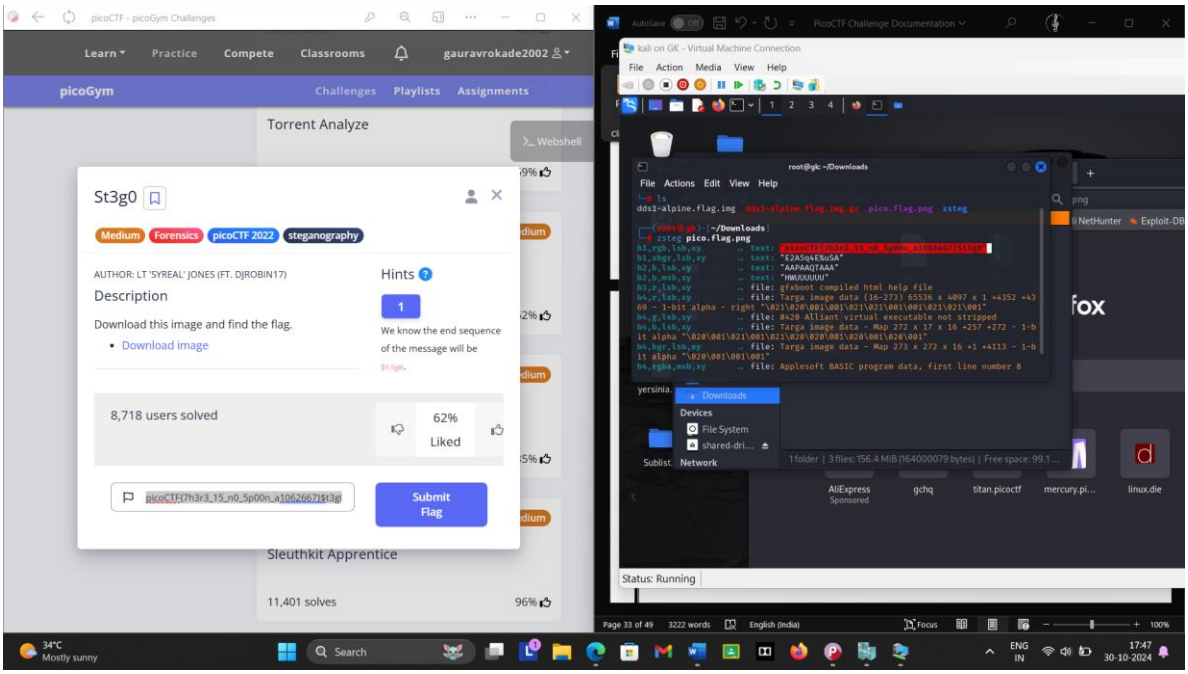






- **Outcome**: *picoCTF{imag3_m4n1pul4t10n_sl4p5}*

## Challenge 29: [ St3g0]

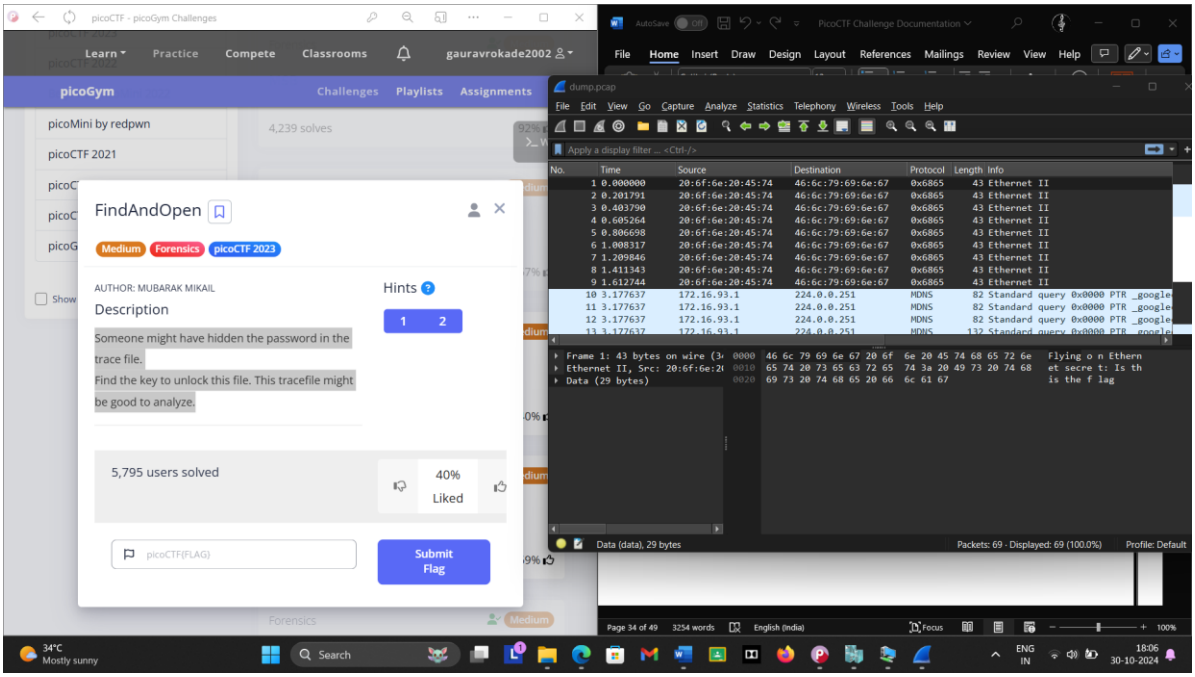
- **Category**: [Forensics]
- **Description**: Download this image and find the flag.
- **Thought Process**: I can use image reader tool like zsteg
- **Solution**:

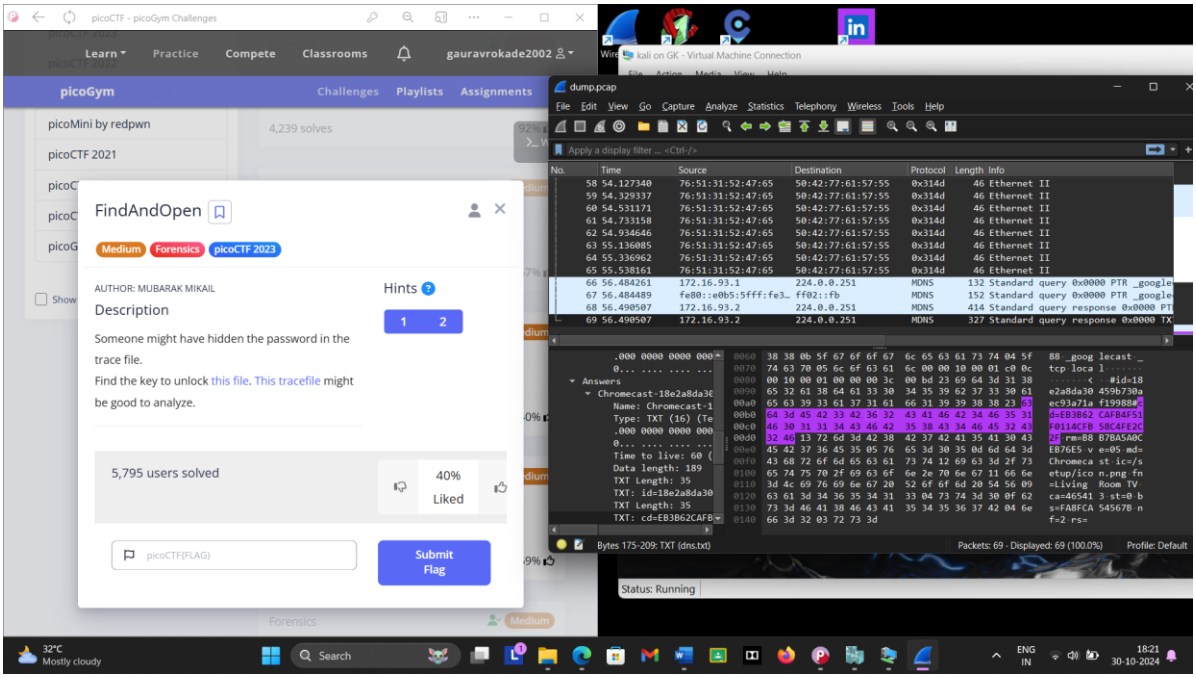


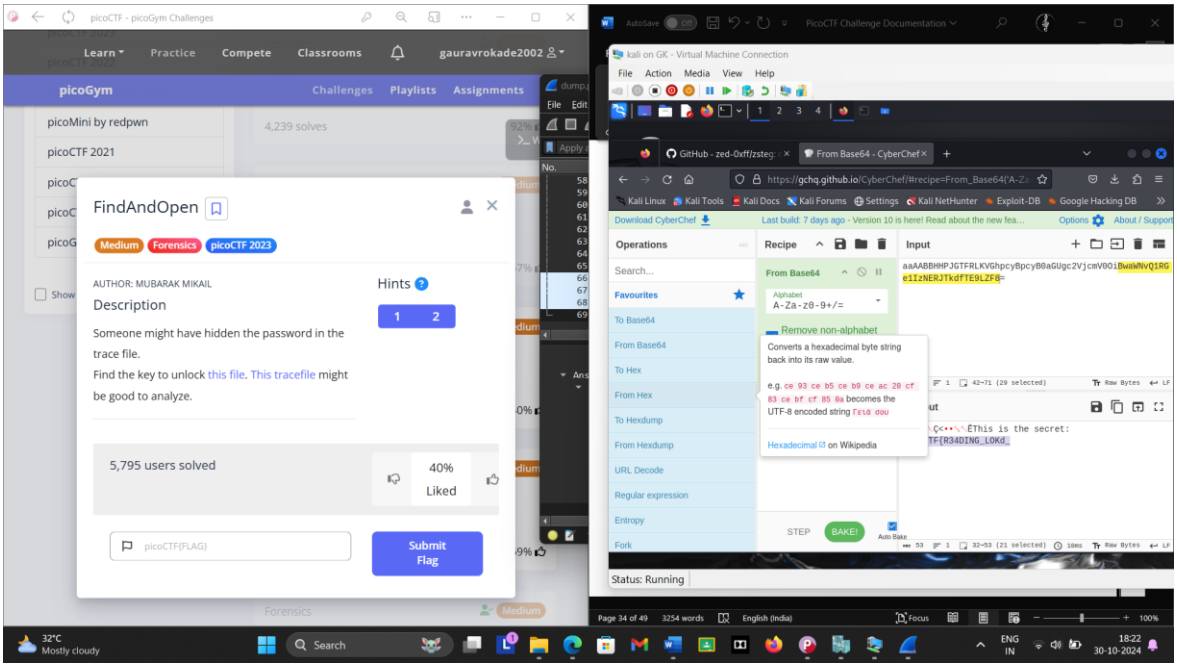

- **Outcome**: *picoCTF{7h3r3_15_n0_5p00n_a1062667}*

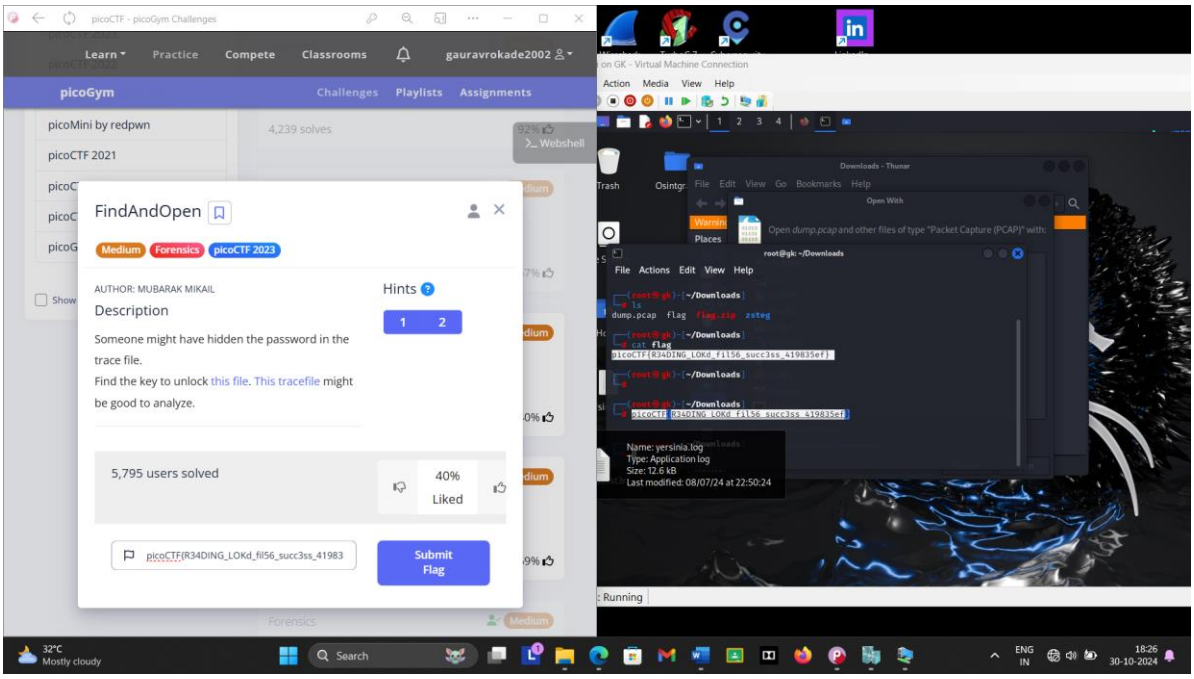
## Challenge 30: [FindAndOpen]

- **Category**: [Forensics]
- **Description**: Someone might have hidden the password in the trace file.Find the key to unlock [this file](). [This tracefile]() might be good to analyze.
- **Thought Process**: to unzip this file we have to extract password using tracefile
- **Solution**:



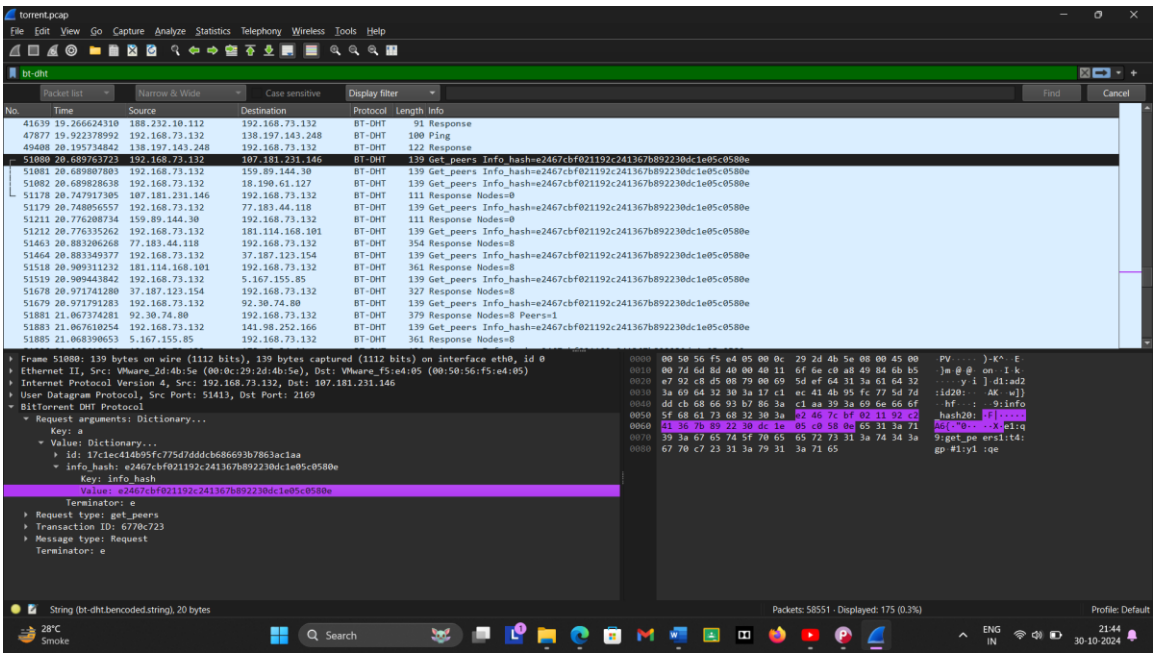


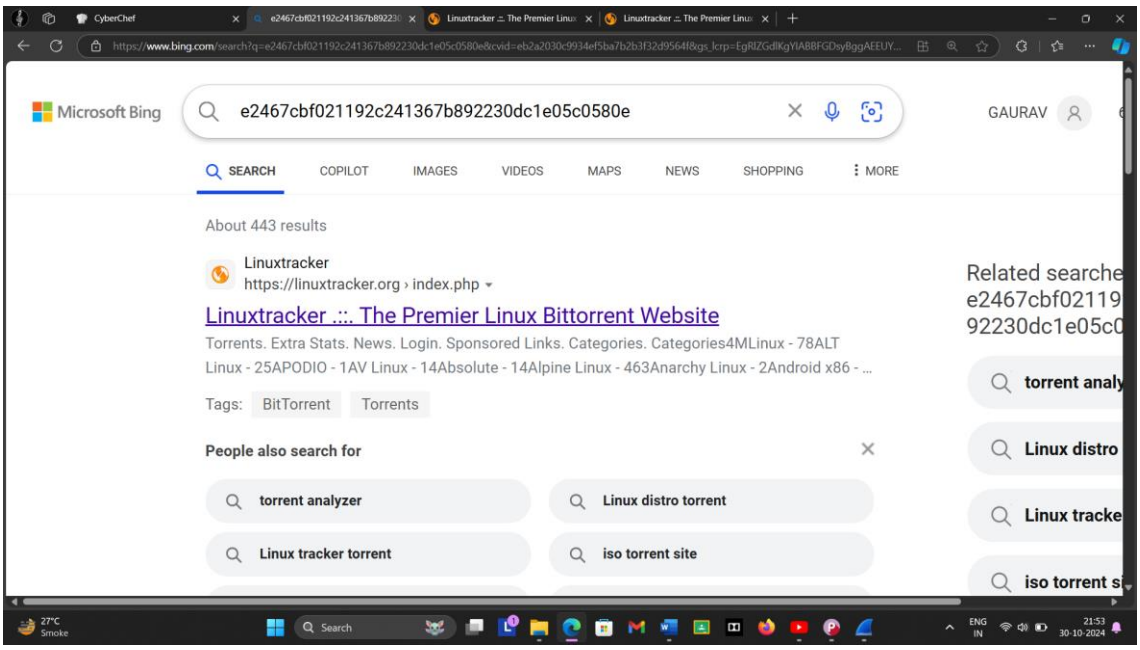



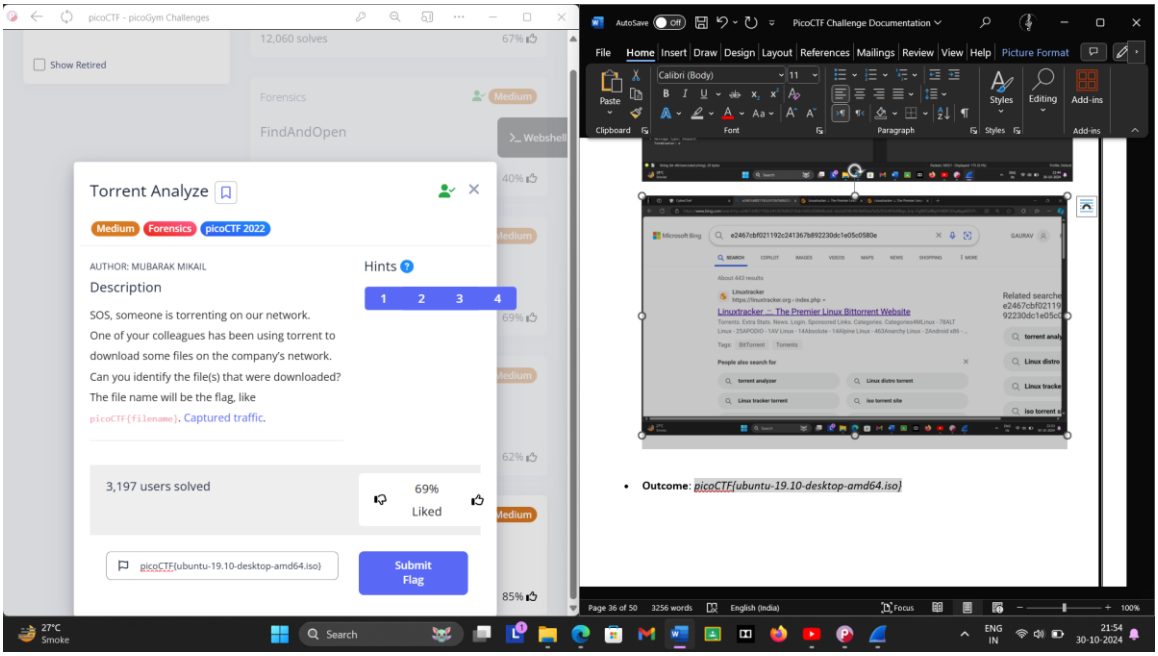

- **Outcome**: *picoCTF{R34DING_LOKd_fil56_succ3ss_419835ef}*

## Challenge 31: [ Toreent Analyze]

- **Category**: [Forensics]
- **Description**: SOS, someone is torrenting on our network.One of your colleagues has been using torrent to download some files on the company's network. Can you identify the file(s) that were downloaded? The file name will be the flag, like picoCTF{filename}. [Captured traffic](#).
- **Thought Process**: Capture on the wire shark and then ttry  to search which hash it is
- **Solution**:



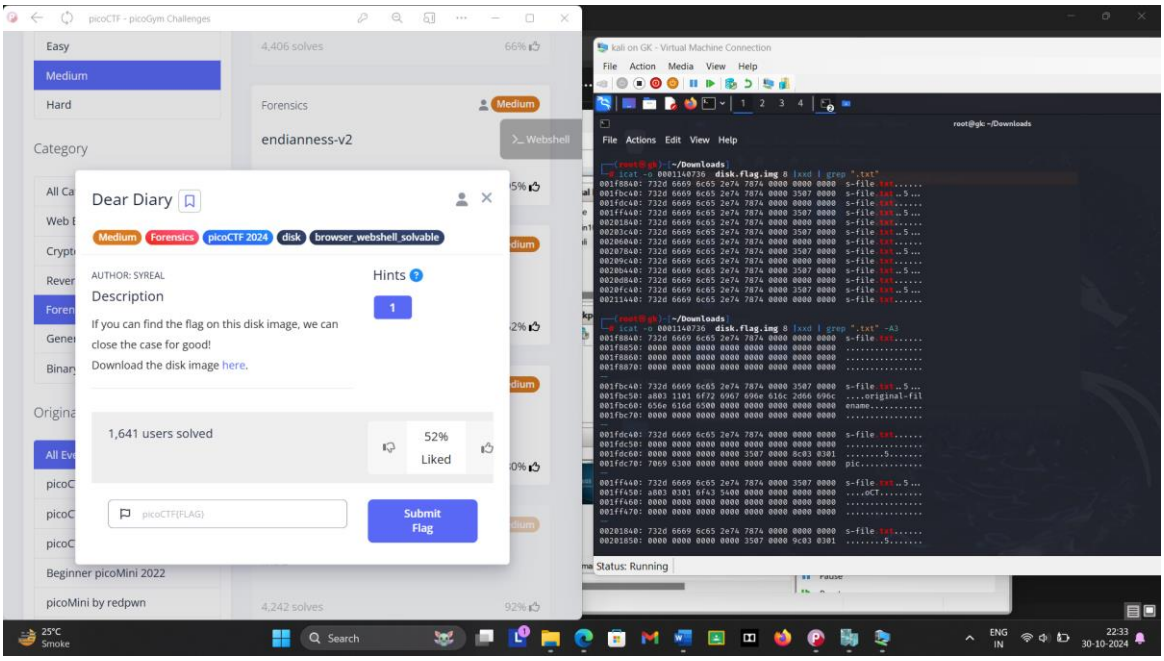



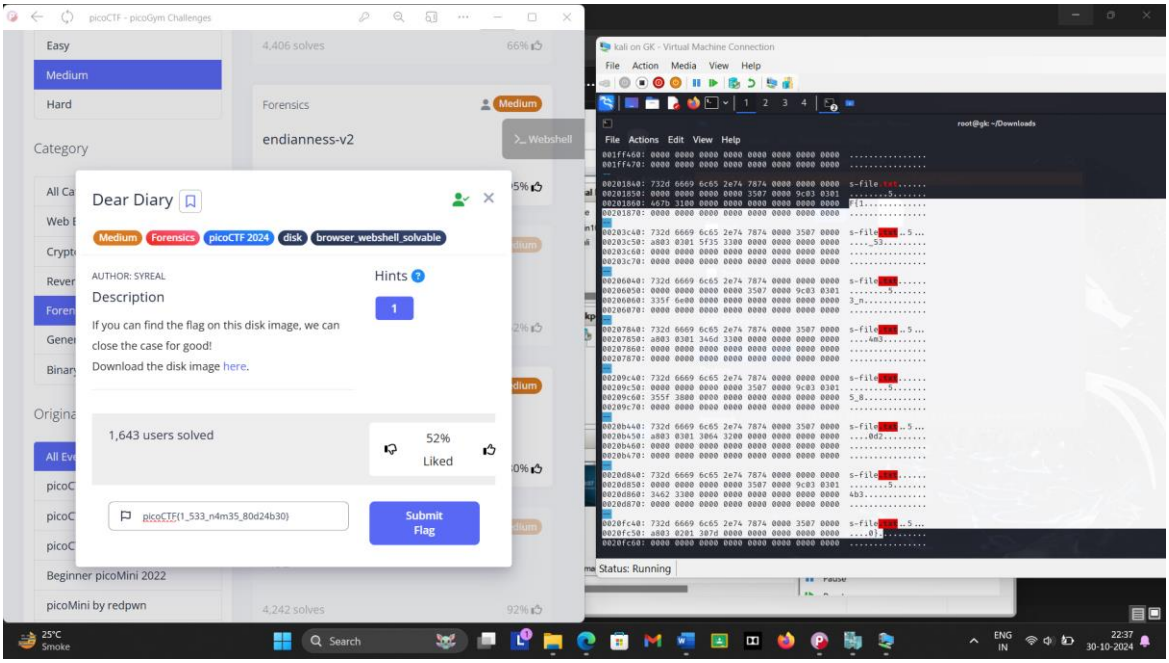



- **Outcome**: *picoCTF{ubuntu-19.10-desktop-amd64.iso}*

## Challenge 32: [ Dear Diary]

- **Category**: [Forensics]
- **Description**: If you can find the flag on this disk image, we can close the case for good!Download the disk image here.
- **Thought Process**: you can use autopsy or simply cat the image using *icat* and sue different compounds
- **Solution**:

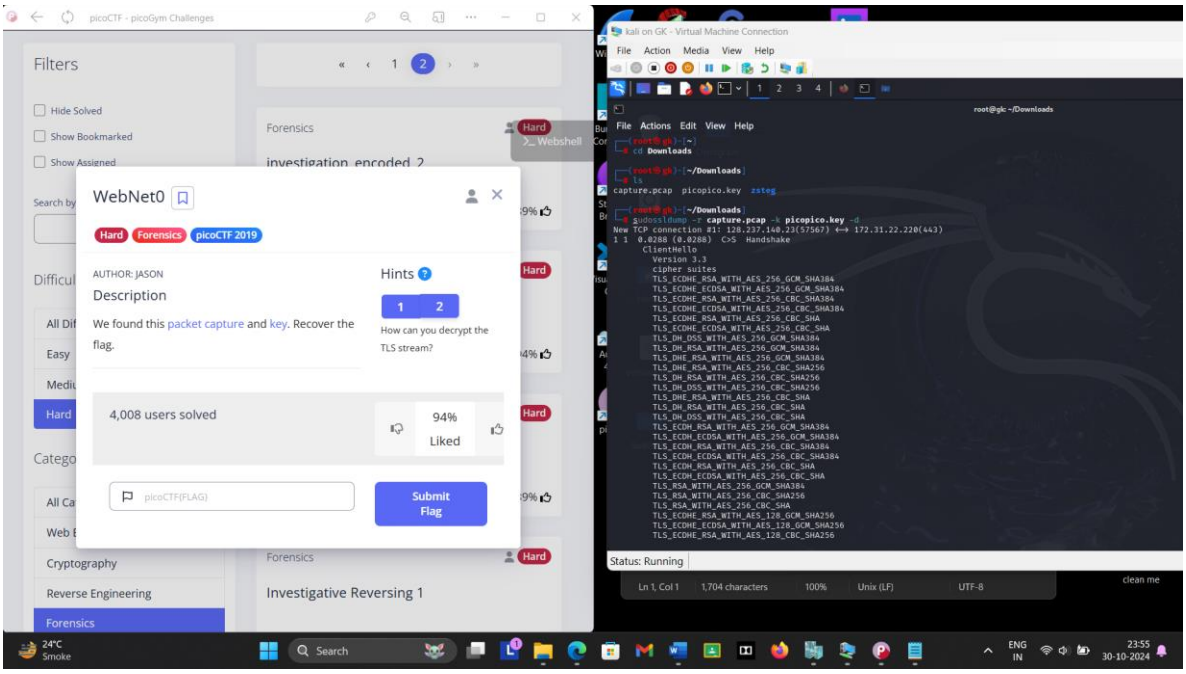


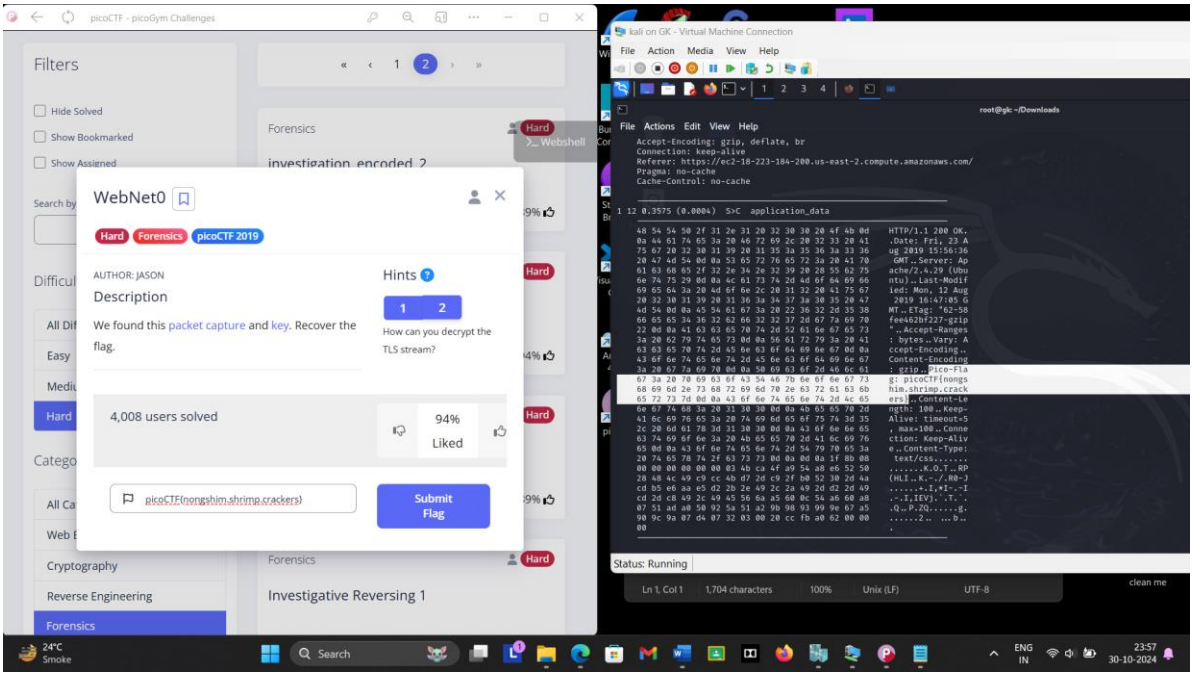




- **Outcome**: *picoCTF{1_533_n4m35_80d24b30}*

## Challenge 33: [WebNet0]

- **Category**: [Forensics]
- **Description**: We found this packet capture and key. Recover the flag.
- **Thought Process**: use wire shark or ssldump to read this files.
- **Solution**:

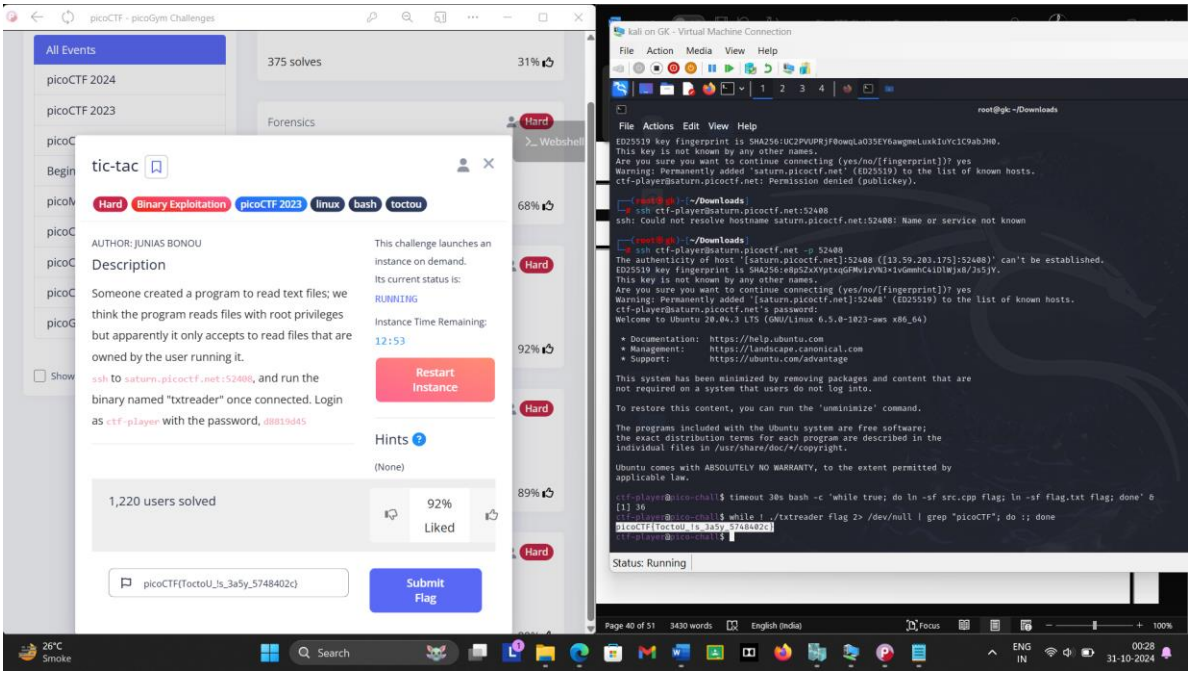



- **Outcome**: *picoCTF{nongshim.shrimp.crackers}*

## Challenge 35: [tic-tac]

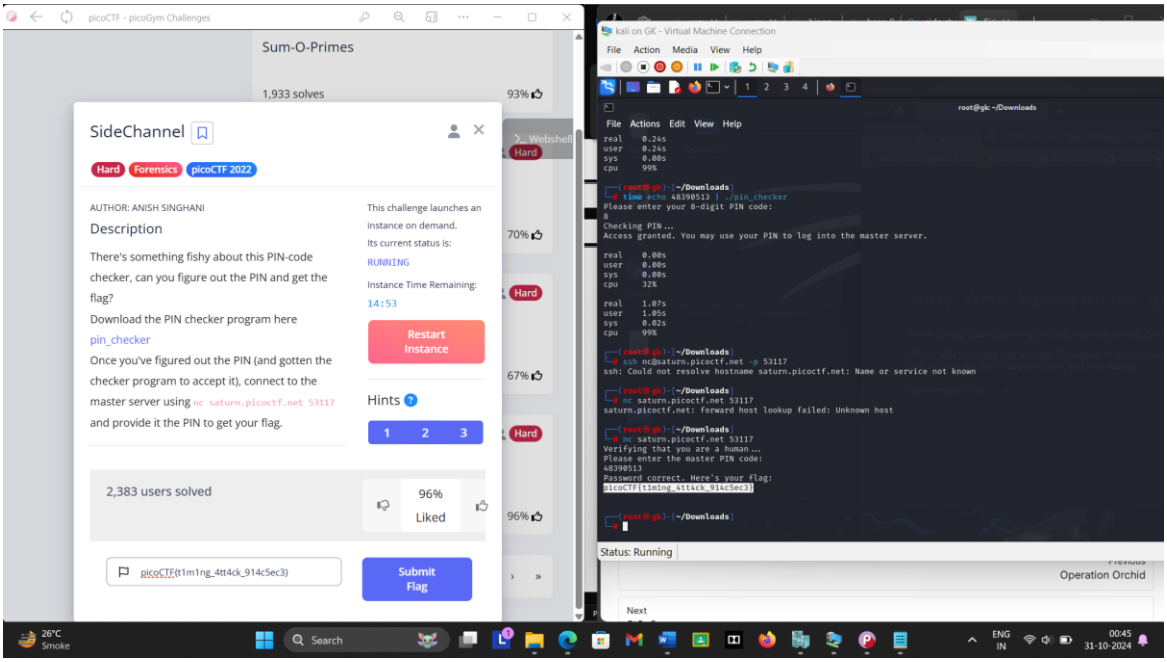
- **Category**: [Binary Exploitation]
- **Description**: Someone created a program to read text files; we think the program reads files with root privileges but apparently it only accepts to read files that are owned by the user running it.ssh to saturn.picoctf.net:52408, and run the binary named "txtreader" once connected. Login as ctf-player with the password, d8819d45
- **Thought Process**: try to exploit using difernt commonds like  grep it true their value change the sorting
- **Solution**:




- **Outcome**: *picoCTF{ToctoU_!s_3a5y_5748402c}*

## Challenge 36: [SideChannel]

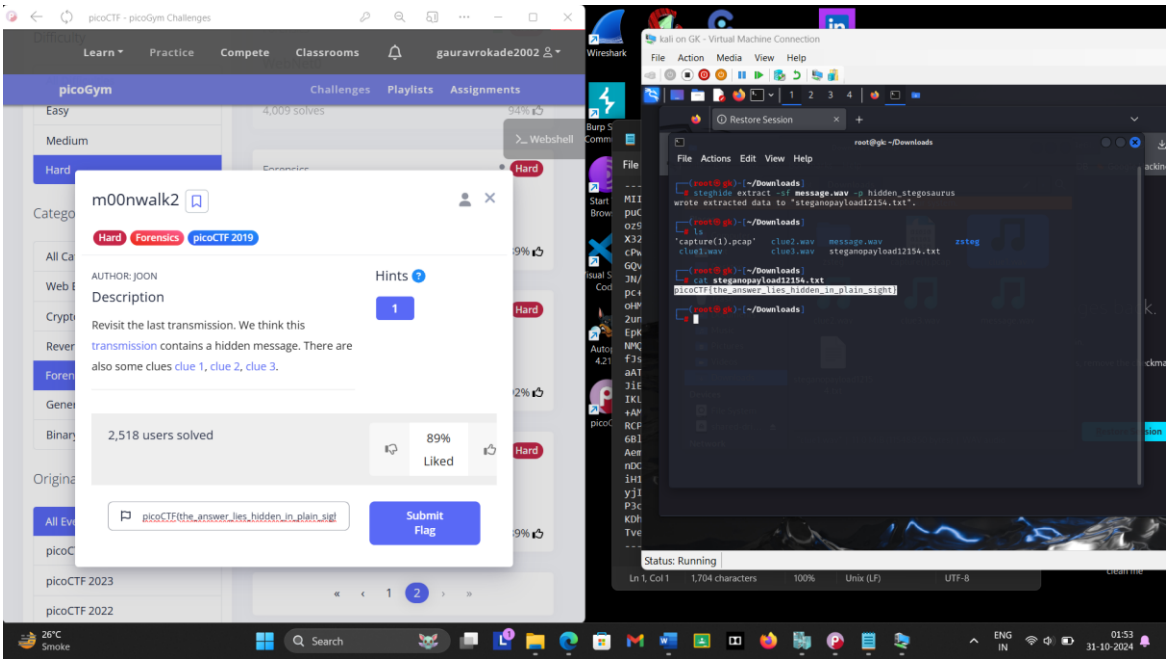
- **Category**: [Forensics]
- **Description**: There's something fishy about this PIN-code checker, can you figure out the PIN and get the flag?Download the PIN checker program here pin_checkerOnce you've figured out the PIN (and gotten the checker program to accept it), connect to the master server using nc saturn.picoctf.net 53117 and provide it the PIN to get your flag.
- **Thought Process**: Attempting to reverse-engineer or exploit the binary won't help you, you can figure out the PIN just by interacting with it and measuring certain properties about it
- **Solution**:




- **Outcome**: *picoCTF{t1m1ng_4tt4ck_914c5ec3}*

## Challenge 37: [m00nwalk2]

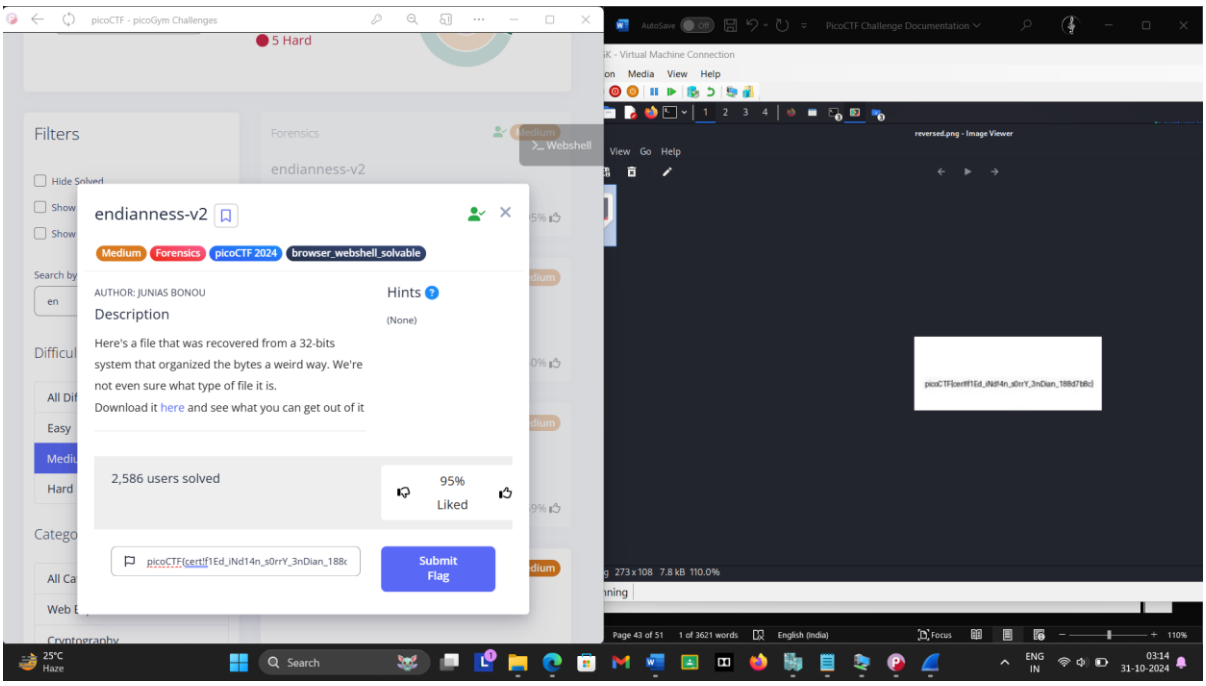
- **Category**: [Forensics]
- **Description**: there are clues and transmission contains a message
- **Thought Process**: we can you tool like stghide inside the kali to read the wav files
- **Solution**:




- **Outcome**: *picoCTF{the_answer_lies_hidden_in_plain_sight}*

## Challenge 38: [endianness-v2]

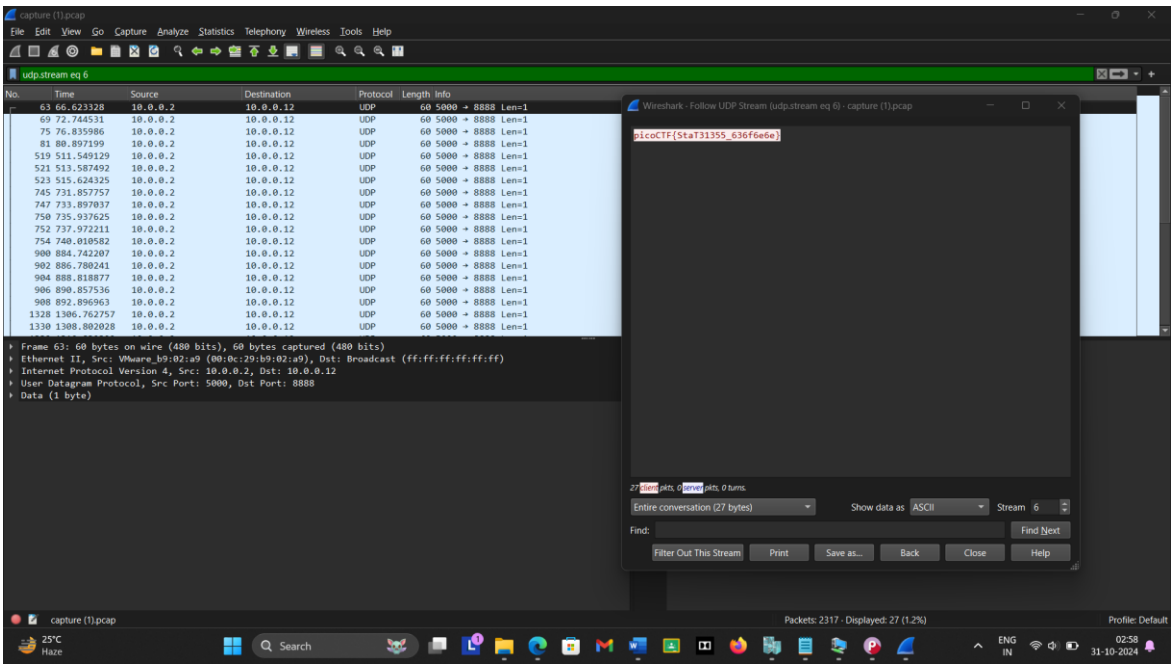
- **Category**: [Forensics]
- **Description**: Here's a file that was recovered from a 32-bits system that organized the bytes a weird way. We're not even sure what type of file it is.Download it here and see what you can get out of it
- **Thought Process**: We first download the challenge file and run the file command on it. It does not specify what type of file it should be so I open the file in hex mode
- **Solution**:

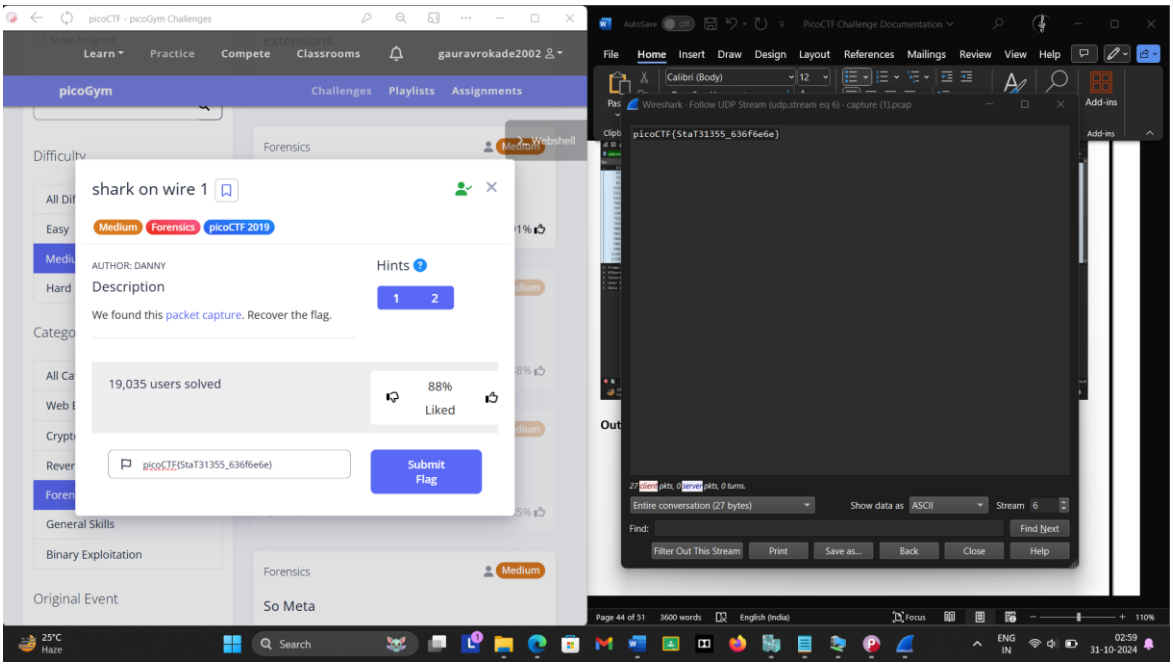



- 
- **Outcome**: *picoCTF{cert!f1Ed_iNd14n_s0rrY_3nDian_188d7b8c}*

## Challenge 39: [ Shark on wire 1 ]

- **Category**: [Forensics/General Skills/Cryptography/Others]
- **Description**: We found this packet capture. Recover the flag.
- **Thought Process**: send udp stream and check one by one by changing their value
- **Solution**:

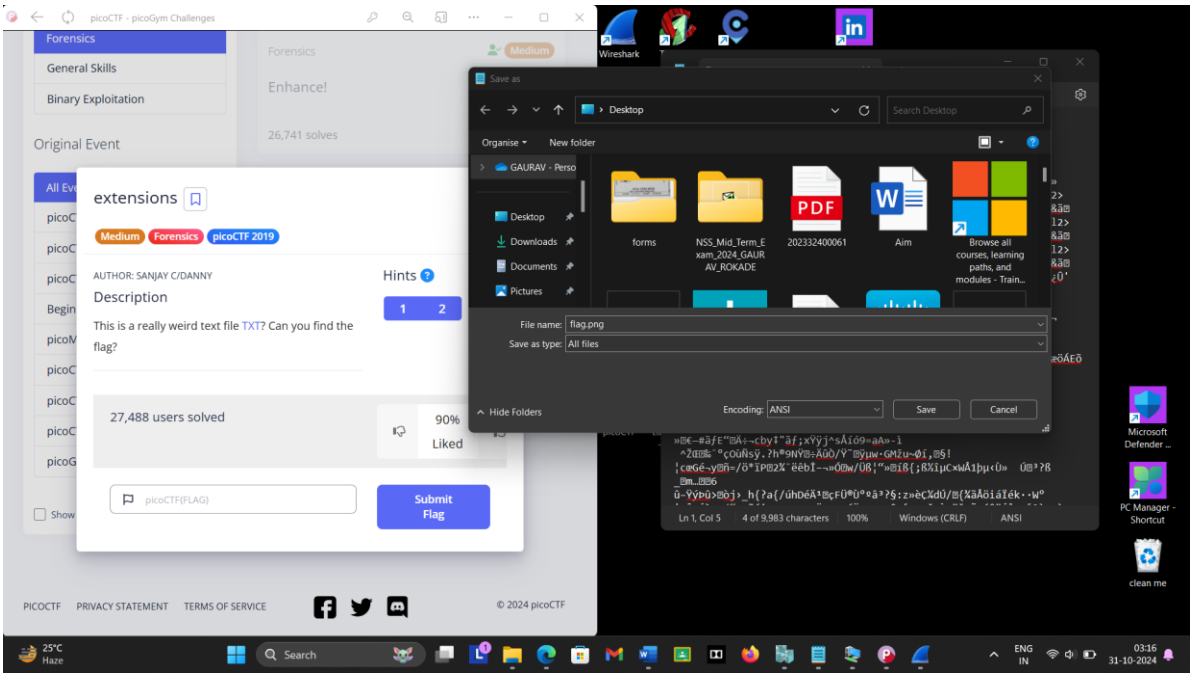


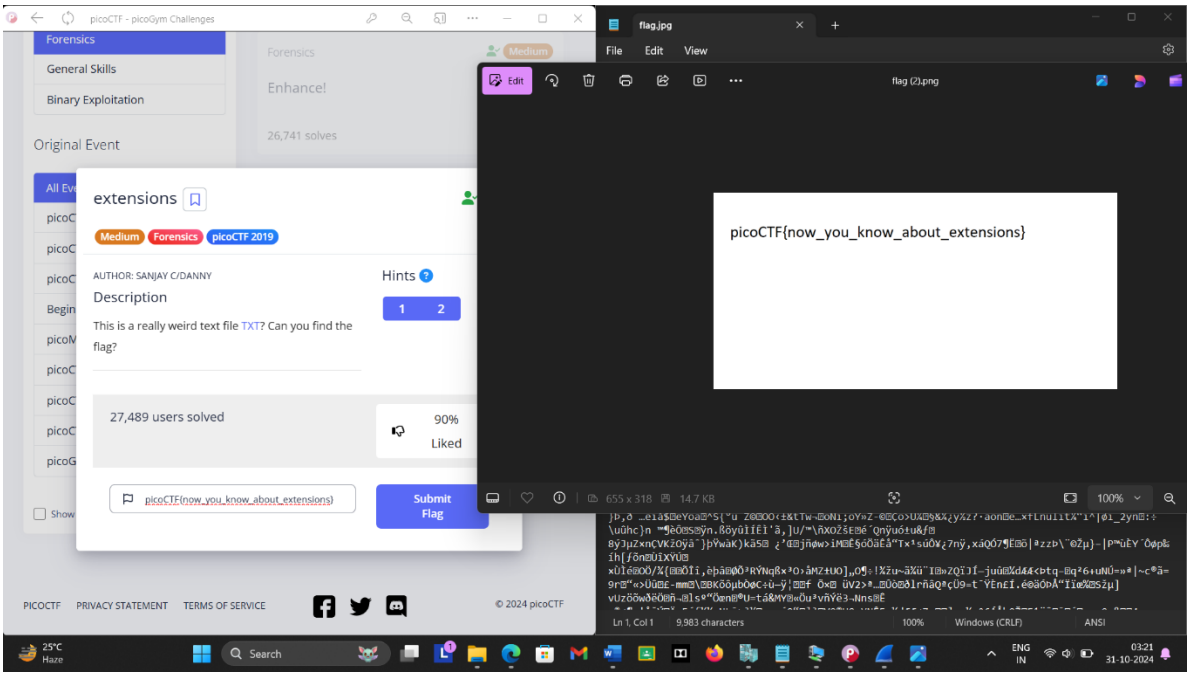

- 

- 
- **Outcome**: *picoCTF{StaT31355_636f6e6e}*

## Challenge 40: [Extensions]

- **Category**: [Forensics/General Skills/Cryptography/Others]
- **Description**:
- **Thought Process**:
- **Solution**:

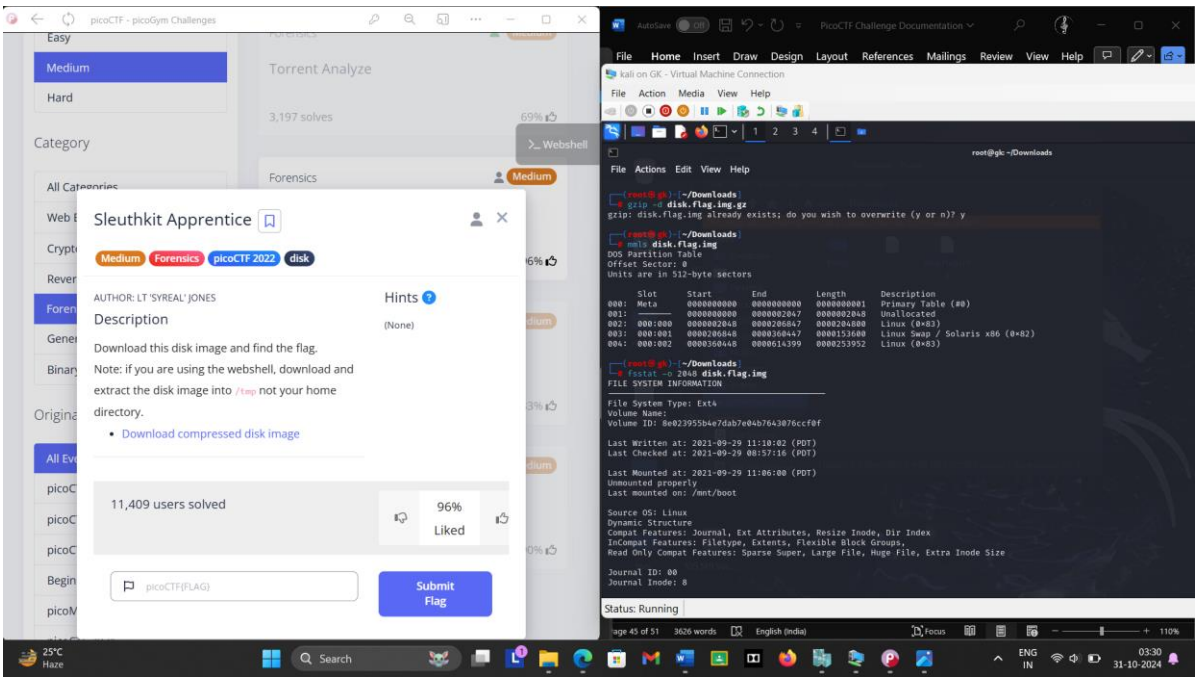


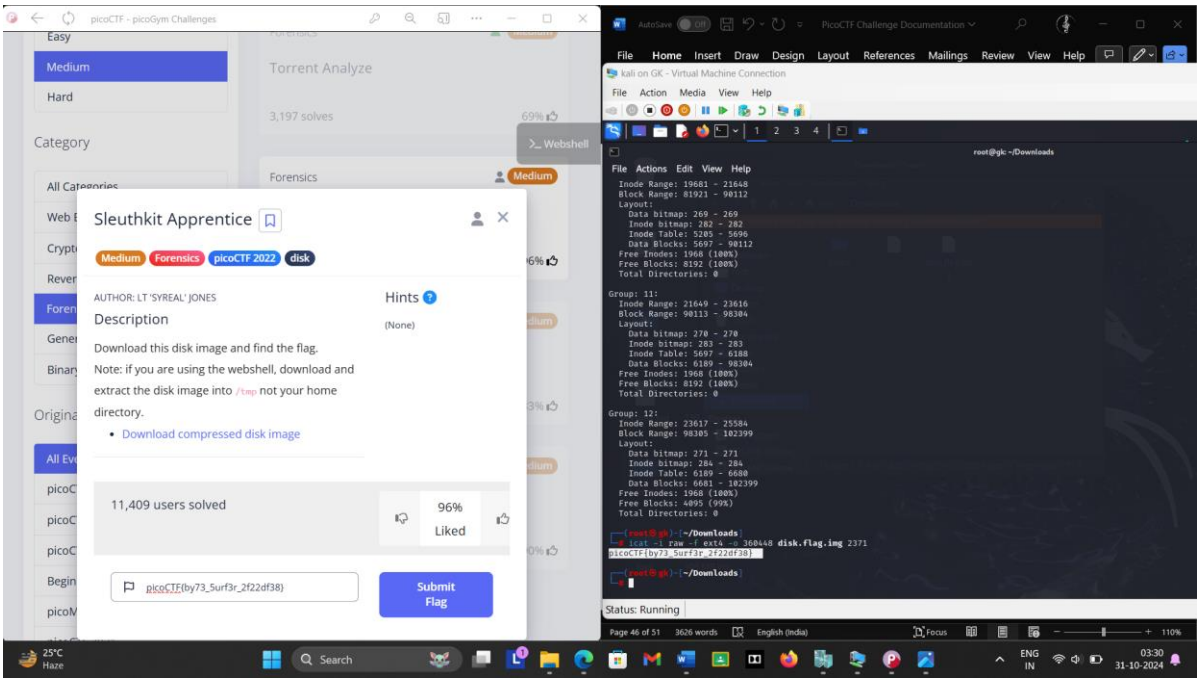




- **Outcome**: *picoCTF{now_you_know_about_extensions}*

## Challenge 41: [Sleuthkit Apprentice]

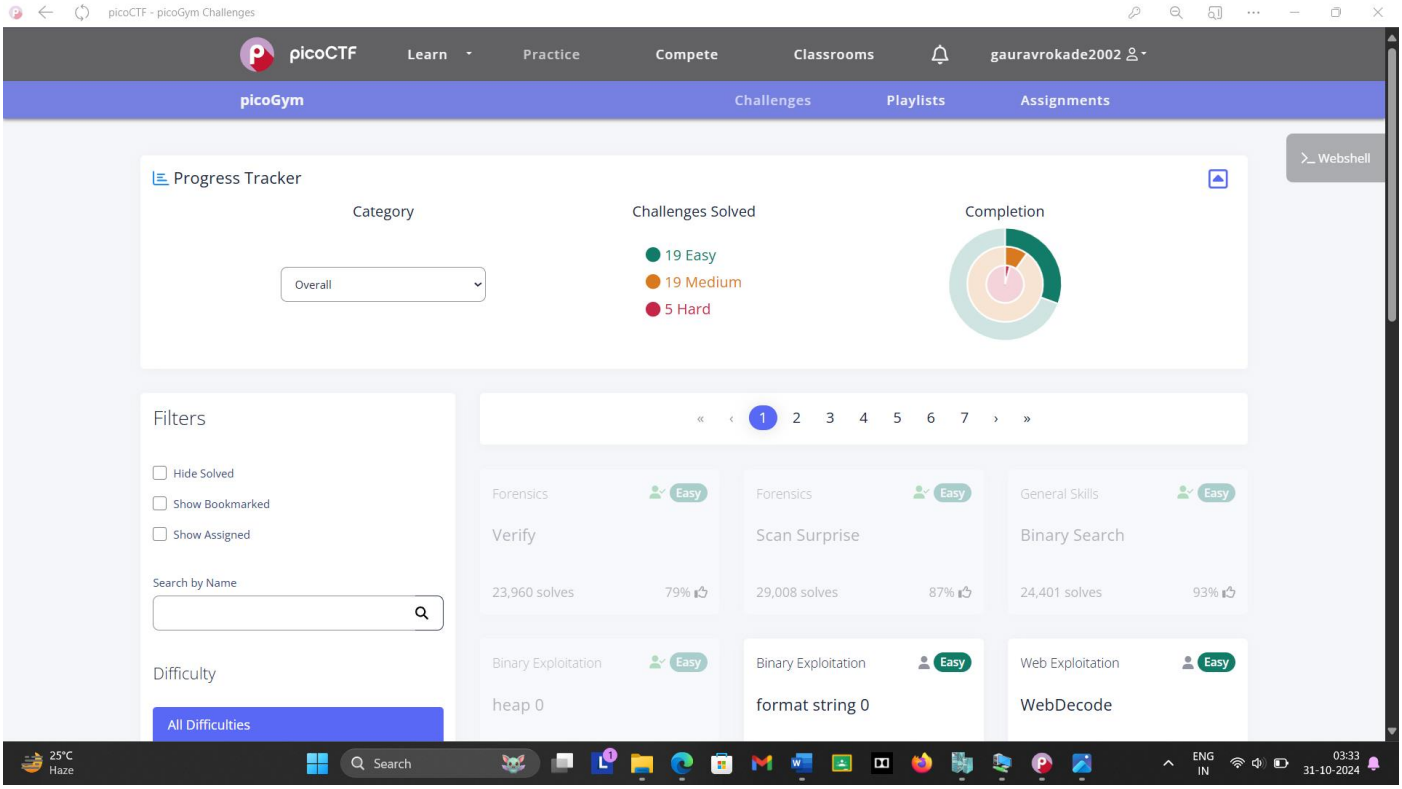
- **Category**: [Forensics]
- **Description**: Download this disk image and find the flag.Note: if you are using the webshell, download and extract the disk image into /tmp not your home directory.
- [Download compressed disk image]
- **Thought Process**: try t read out the disk using ftk or common line like icat with using different functions
- **Solution**:



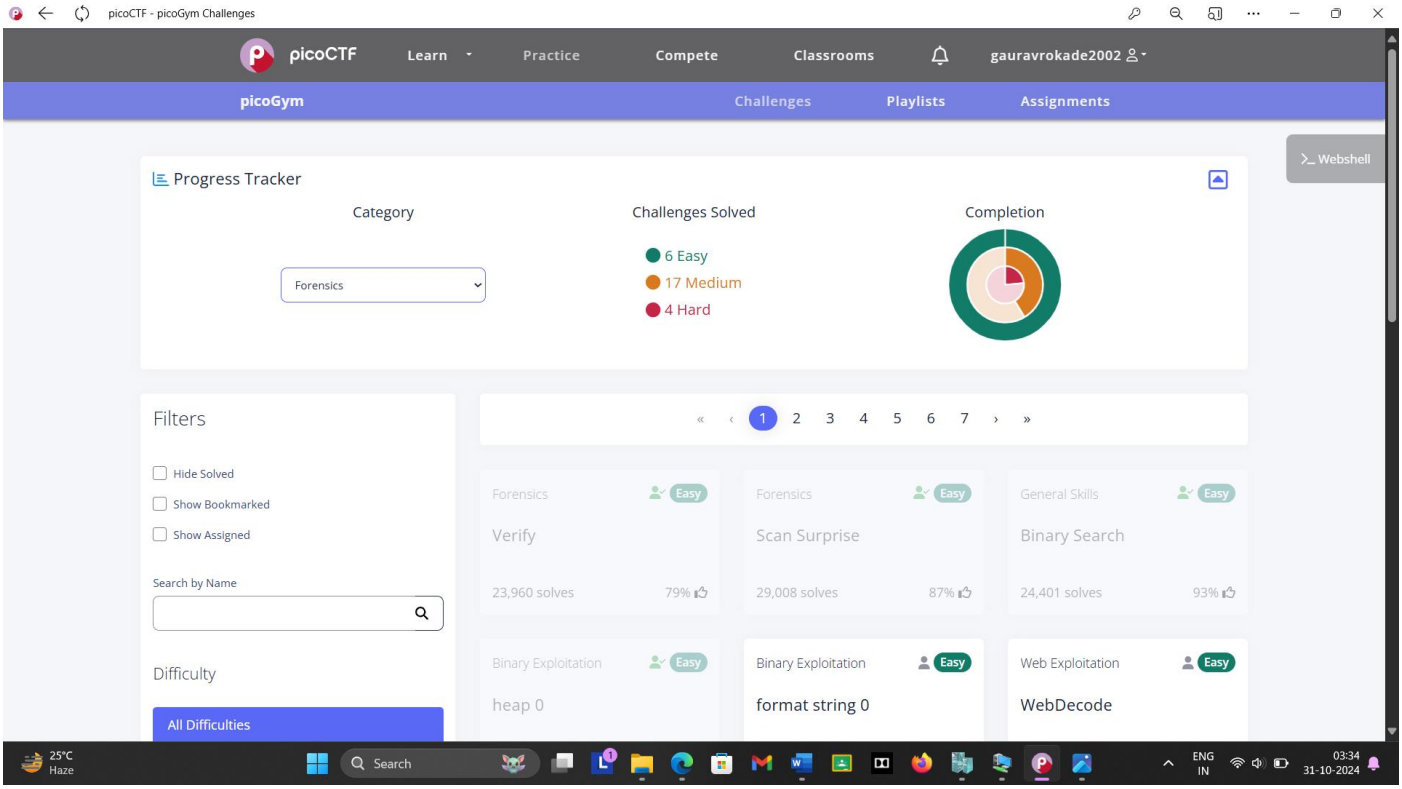




- **Outcome**: *picoCTF{by73_5urf3r_2f22df38}*

## Overall progress track :




## Category which mostly solved:



## 3. Challenge Breakdown

- **Forensics**
  - **Purpose**: The focus is on testing the ability to analyze and recover digital evidence from various sources.
  - **Components**:
    - Data recovery from disk images and storage devices.
    - Analysis of file metadata and contents to gather important information.
    - Examination of network traffic to identify anomalies and potential malicious activities.
    - Memory analysis to extract relevant information from running processes.
  - **Approach**:
    - Utilization of forensic tools like Autopsy and FTK Imager for data recovery and analysis.
    - Examination of file signatures and metadata to gain insights about files.
    - Use of Wireshark to analyze network packets, looking for suspicious patterns.
    - Analysis of memory dumps with tools like Volatility to identify running processes and extract relevant information.
- **General Skills**
  - **Purpose**: The aim is to assess foundational skills and knowledge essential for cybersecurity.
  - **Components**:
    - Practice of basic programming and scripting skills to automate tasks and solve problems.
    - Improvement of proficiency in using command line interfaces and navigating file systems.
    - Enhancement of understanding of web technologies and their manipulation.
    - Application of critical thinking and problem-solving abilities to various scenarios.
  - **Approach**:
    - Practice of common command-line commands and scripting languages like Python and Bash.
    - Familiarization with basic web development concepts (HTML, CSS, JavaScript) to navigate and manipulate web pages effectively.
    - Engagement in logical reasoning exercises to enhance problem-solving skills.
    - Utilization of online resources and forums to clarify concepts and gather different perspectives on challenges.
- **Cryptography**
  - **Purpose**: The focus is on evaluating understanding of encryption and decryption techniques.

- **Components**:
  - Application of classical and modern cryptographic methods to encode and decode messages.
  - Learning techniques for analyzing and breaking cryptographic systems.
  - Exploration of the applications of hashing functions and their vulnerabilities.
  - Investigation of steganography for hiding and revealing information within files.
- **Approach**:
  - Review of common cryptographic algorithms (e.g., AES, RSA, DES) to understand their workings.
  - Utilization of tools like CyberChef and Hashcat for decoding and analyzing encrypted messages.
  - Practice of solving ciphers by hand to grasp the underlying principles and patterns.
  - Experimentation with steganography tools to hide and extract data from images or audio files.

❖ **Others**

- **Purpose**: This category covers a broad range of cybersecurity skills that do not fit into the other categories.
- **Components**:
  - Work on web exploitation techniques targeting vulnerabilities in web applications.
  - Tackle binary exploitation challenges involving reverse engineering and memory manipulation.
  - Focus on networking challenges related to securing and analyzing network communications.
  - Explore miscellaneous topics related to security best practices and methodologies.
- **Approach**:
  - Learning about common web vulnerabilities (e.g., SQL injection, XSS) and exploiting them using tools like Burp Suite and OWASP ZAP.
  - Study of binary exploitation techniques, including buffer overflows and return-oriented programming (ROP).
  - Familiarization with network protocols and tools for analyzing network security (e.g., nmap, netcat).
  - Keeping up-to-date with cybersecurity trends and best practices through blogs, forums, and community discussions.

## 4. Conclusion

Participating in the PicoCTF challenges has been a valuable and enriching experience. Throughout the competition, I have gained practical skills and insights that have deepened my understanding of various cybersecurity concepts. This documentation captures my journey and the lessons learned while tackling a diverse range of challenges.

❖ **Key Takeaways**

- Hands-On Experience: Engaging with real-world cybersecurity problems has provided me with practical experience that theoretical knowledge alone could not offer. I have learned to approach challenges systematically and think critically about potential solutions.
- Interdisciplinary Skills: The challenges encompassed a variety of topics, highlighting the interdisciplinary nature of cybersecurity. I developed skills in areas such as cryptography, digital forensics, web security, and more, underscoring the importance of a well-rounded knowledge base.
- Problem-Solving Techniques: I gained valuable problem-solving techniques, including debugging, reverse engineering, and analyzing network traffic. These skills are essential for identifying vulnerabilities and mitigating security risks.
- Community and Collaboration: Engaging with the PicoCTF community has shown me the value of collaboration in cybersecurity. Sharing insights and strategies with peers enhances learning and fosters a sense of camaraderie.
- Adaptability and Resilience: Tackling challenges that require persistence and adaptability has improved my resilience. I learned to approach complex problems with a growth mindset, viewing failures as opportunities for learning.

❖ **Future Learning Directions**

- Advanced Cybersecurity Concepts: I plan to explore more advanced topics in cybersecurity, such as penetration testing, threat hunting, and incident response, to build on the foundation established by the PicoCTF challenges.
- Certifications and Courses: Pursuing relevant certifications (e.g., CompTIA Security+, Certified Ethical Hacker) and online courses will further enhance my skills and knowledge in specific areas of cybersecurity.
- Participation in More Competitions: I aim to participate in additional Capture the Flag (CTF) competitions and cybersecurity challenges to continue honing my skills and staying updated with emerging trends in the field.
- Contributing to the Community: I hope to contribute to the cybersecurity community by sharing my knowledge through blogs, tutorials, or mentoring newcomers, fostering a culture of learning and collaboration.
- Hands-On Projects: Engaging in hands-on projects, such as creating my own CTF challenges or participating in open-source cybersecurity initiatives, will provide practical experience and help solidify my understanding of various concepts.
- In summary, the PicoCTF experience has been instrumental in shaping my journey into the world of cybersecurity. I look forward to furthering my education, expanding my skill set, and contributing to the ever-evolving field of cybersecurity.

## 5. References

During my participation in the PicoCTF challenges, I utilized a variety of sources and resources to enhance my understanding and assist in solving the problems. Below are the key references:

- PicoCTF Official Website
  - The primary platform for accessing challenges, hints, and educational materials. The website offers detailed explanations for each challenge, which helped clarify concepts.
  - PicoCTF
- Books and eBooks
  - "The Web Application Hacker's Handbook" by Dafydd Stuttard and Marcus Pinto: This book provided insights into web security vulnerabilities and exploitation techniques.
  - "Practical Cryptography" by Niels Ferguson and Bruce Schneier: A valuable resource for understanding cryptographic principles and techniques.
- Community Forums and Discussion Boards
  - Stack Overflow: A helpful resource for troubleshooting coding issues and seeking advice on specific challenges.
  - Reddit: Subreddits like r/cybersecurity and r/CTFs provided community support, tips, and discussions about various challenges.
- Documentation and Technical Resources
  - OWASP (Open Web Application Security Project): Provided guidelines and best practices for web application security, which were useful for related challenges.
  - Cybersecurity Blogs: Blogs like Krebs on Security and The Hacker News kept me updated on current cybersecurity trends and provided insights into various topics.
- Tools and Software
  - Wireshark: A network protocol analyzer that helped in understanding and analyzing network traffic during certain challenges.
  - Burp Suite: An integrated platform for performing security testing of web applications, particularly useful for web exploitation challenges.
  - Ghidra: A software reverse engineering tool that aided in analyzing binary exploitation challenges.
  - Linux OS
- YouTube Channels and Video Tutorials
  - Channels like LiveOverflow and The Cyber Mentor provided video explanations and walkthroughs for similar challenges, offering visual insights into problem-solving techniques.
- GitHub Repositories
  - Numerous GitHub repositories containing walkthroughs for CTF challenges provided inspiration and guidance on approaches to solving problems.

## 6. Acknowledgment

I would like to extend my sincere gratitude to Vault-Tec Security for entrusting me with the challenge of solving more than 40 PicoCTF tasks. This journey has been both educational and engaging, providing valuable experience in cybersecurity concepts, problem-solving techniques, and documentation practices.

This project has allowed me to explore various aspects of cybersecurity and sharpen my analytical skills, enhancing my ability to approach complex challenges systematically. I am grateful for the opportunity to develop these competencies and for the guidance and support provided throughout the process.

Thank you, Vault-Tec Security, for offering me this platform to learn, grow, and demonstrate my skills. I look forward to applying these experiences in future endeavors.