PSG COLLEGE OF TECHNOLOGY

COMPUTER SCIENCE & ENGINEERING ASSOCIATION

THE EYE

visio protectoris

presents

AEROVISION

FINAL REPORT

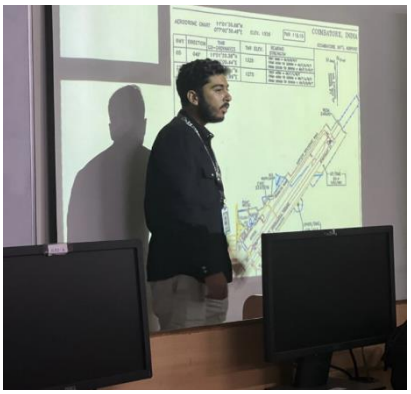
21 AUG 2023 - 1 SEP 2023

Day -1

Aero-Space Cybersecurity Workshop

Introduction:

The Aerovision Cybersecurity workshop focused on the significance of aerospace cybersecurity, using Coimbatore Airport Charts as a case study. The workshop emphasized the critical importance of cybersecurity within the aerospace sector and highlighted the severe consequences that can arise when security is not given due attention.



Session 1: Aerospace Cybersecurity Overview

(Speaker: Aaditya Rengarajan):

The workshop began by emphasizing the sign ificance of cybersecurity in the aerospace sector. It explained that safeguardingsensitive data, systems, and operations is paramount in aviation.

Session 2: Drone Technology and Security

(Speaker: Soorya Subramani):

The second part of the workshop introduced participants to drone technology and provided basic insights into securing drones from potential hacks. Given the diverse audience with varying technical backgrounds, the session aimed to strike a balance between accessibility and relevance to the subject.

Session 3: GitHub and Repositories

(Speaker: S Karun Vikhash):

The workshop then shifted focus to GitHub, introducing the concept of repositories. This section was designed to familiarize participants with essential tools for collaboration and code management,considering that not all attendees had prior knowledge in this area.

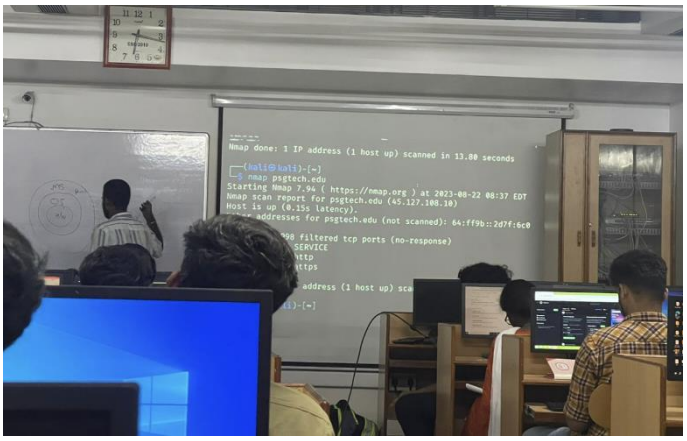
Session 4: Phishing Attacks

(Speaker: Dhanush Gowdhaman):

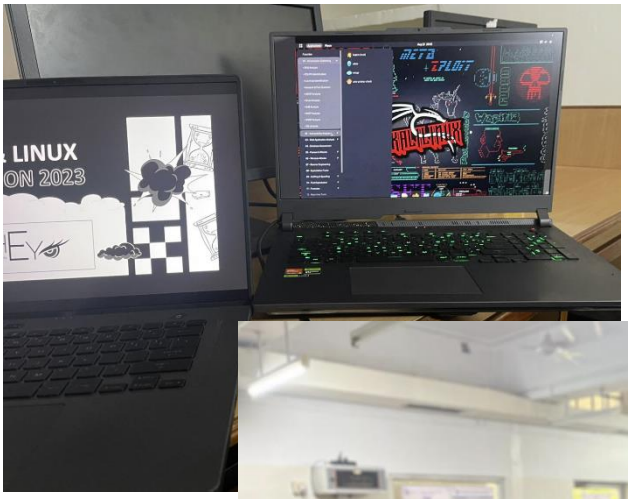
The fourth session revolved around the concept of phishing attacks and their potential consequ ences, including password theft. To illustrate this, the presenters conducted an ethical social experiment as anexample.

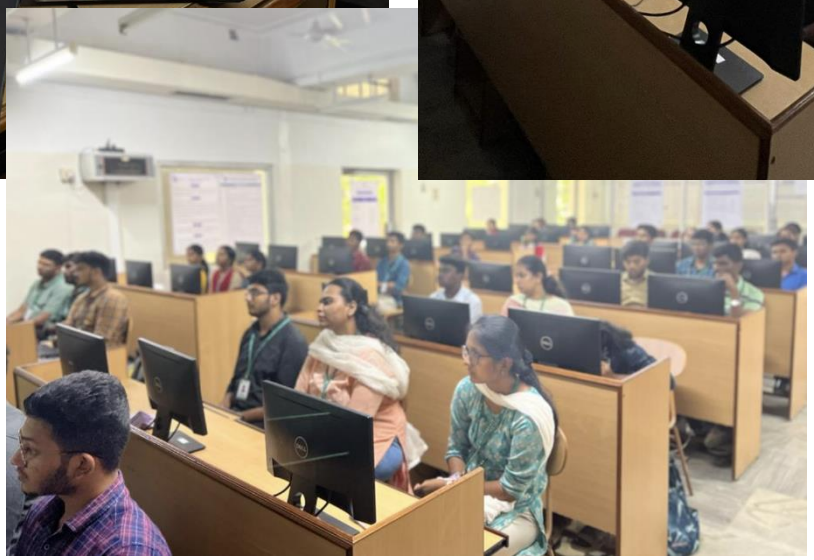
Session 5: Linux Environment and Its Advantages

(Speaker: Dhanush Gowdhaman):



The workshop concluded by highlighting the significance of the Linux environment and explaining why it is often preferred in cybersecurity contexts. Th is segment aimed to provide participants with valuable insights into the practical aspects of cybersecurity.





Day 2 **GitHub Stream**

Introduction :

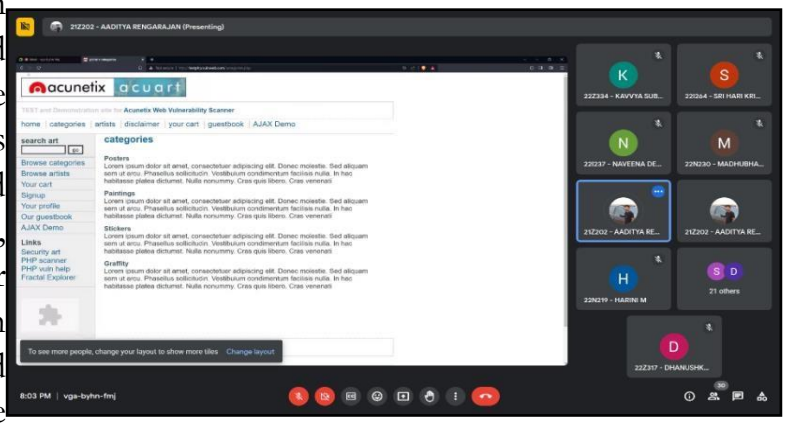
The Workshop about the Aero-Security was conducted in onlinemode via Google Meet and It was Begun by a short overview about the previous session. The introduction about Secure Coding in the AeroSpaceDomain and Capture-The-Flag was given.

Session 1 : Secure Coding (Speaker: Aaditya Rengarajan):

As the First Session of the Workshop, Secure Coding for Aerospace was explained and some key principles and guidelines about the Secure Coding in Aerospace were discussed.

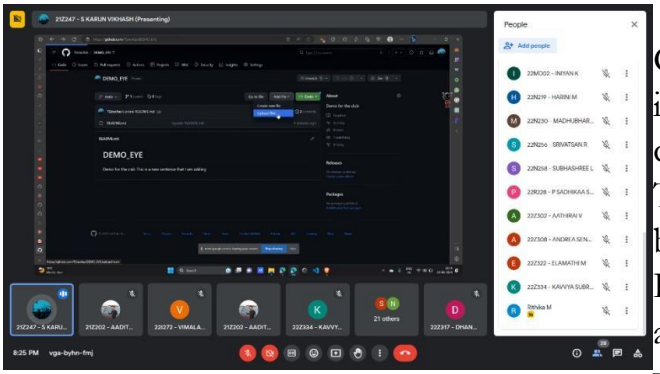
Session 2 : Vulnerabilities in Commercial Aviation and Embedded System

(Speaker: Aaditya Rengarajan):



The Top 10 Vulnerabilities in Commercial Aviation and Embedded System like Malware and Malicious Software , Software and Hardware Vulnerabilities , Physical Security and Insider Threats were discussed with acunnetix website. A Detailed Explanation was given to the students aboutthe SQL. SQL cheetsheet and SQL Injection. And the Login Failure was experienced and the solution was explained to the participants.

Session 3 : GitHub and GitGuardian (Speaker: S Karun Vikhash):



In the Third Session GitHub and GitGuardian were explained and The introduction about the GitHub and creating an Account were discussed. Then the Session was getting deeply in by explaining about the GitHub Repositories with the two types Public and Private. Creation of the Repository was explained with an example. And the Purpose of README.txt file in repositories was explained. The Private Collaborations on the GitHub was given by with hands-on training and a live example.

Session 4 : SDR and ADS-B Technologies (Speaker: S Karun Vikhash):

In the Last Session , The Topics **S**oftware-**D**efined **R**adio and **A**utomatic **D**ependent **S**urveillance–**B**roadcast **(ADS-B)** Technologies were Discussed. The Purpose and Uses of **S**oftware-**D**efined **R**adio (**SDR**) were Discussed. Then the Session moved on by Discussing about Importance of the ADS-B Surveillance Technology in The AeroSpaceCyberSecurity.

DAY 3 **CTF WorkShop**

Introduction :

Session 1 : Capture The Flag :

The Explanation about the Capture The Flag (CTF) was givenand How the CTF is used in Hacking Stream and its basics were Discussed in the picoCTF web by completed Challenges and examples.Then Tips toScore in the CTF Exercises were discussed with various tasks. Doing CTF in Linux OS and Directories and Commands in the picoCTF were discussed with live examples. A short introduction about the Cryptography was givenby a Simple CTF Task.

Session 2 : Identifying the Vulnerabilities :

The Identification of Vulnerabilities with the help of using theLockheed Martin's Kill chain which is a Intelligence Driven Defense Model was discussed. Then the steps in the Cyber Kill Chain was explained with an example. And It's Roles in the Cyber Security and benefits and uses of Lockheed Kill Chain were explained.

Session 3 : OWASP TOP 10 :

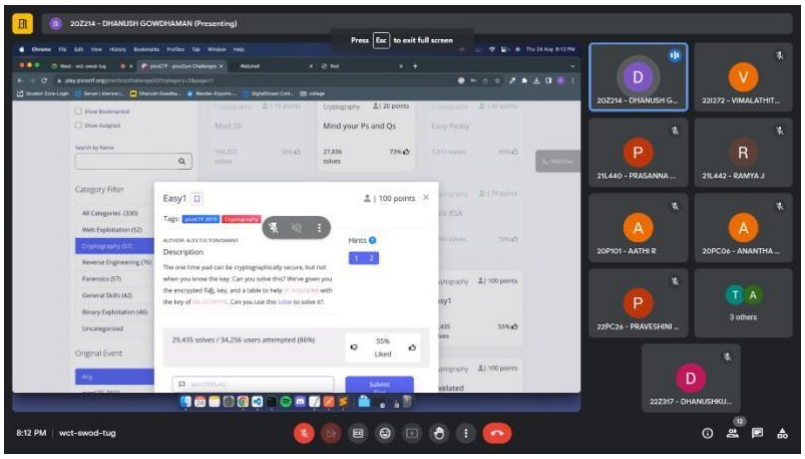
In this Session , The Introduction about the OWASP Community and its Importance in the Web Application Security was given to the participants. Then The Top 10 Vulnerabilities which was given by the **O**pen **W**eb **A**pplication **S**ecurity **P**roject (OWASP) were discussed.

Session 4 : SCADA :

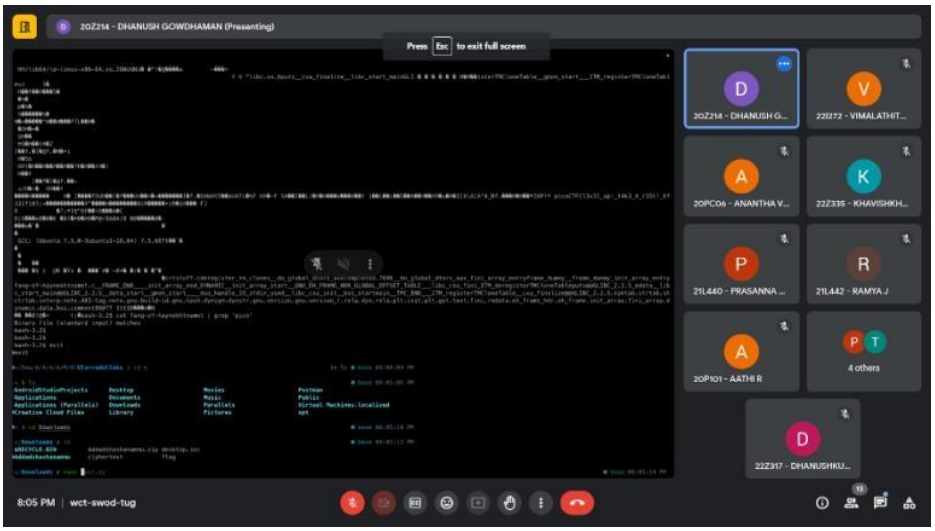
At the End of the Workshop , The Introducing the Basics of The Control System Architecture **SCADA** was done. Then the examples and uses of the **S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition (SCADA) were discussed. Finally , The Various Methods to Test SCADA was explained bylive examples.

FEEDBACK :

I'm Vimalathithan.D from B.Tech IT. The session was amazing andI got to know a lot of things. Thanks a lot !



Session Speaker :
Dhanush Gowdhaman



AEROVISON 2023

Vulnerability Assessment Capture-The-Flag Write-Up

1. **Knock_on_Numbers**

   The python file exposed the flag

```
print("48.8584, 2.2945")
inp=input("Enter your guess:(in camel case) ")
if inp=='TheEiffelTower':
    print("The flag is, Aerovision{tH3_31ff3l_t0w3r}")

```

2. **Just_a_dot**

   The flag was present in the last few lines of the svg file given

```
style="font-size:0.00352781px;line-height:1.25;fill:#ffffff;stroke-width:0.26458332;"
id="tspan3764">F { 3 n h 4 n </tspan><tspan
sodipodi:role="line"
x="107.43014"
y="132.11588"
style="font-size:0.00352781px;line-height:1.25;fill:#ffffff;stroke-width:0.26458332;"
id="tspan3752">c 3 d _ 2 4 3 7 4 6 7 5 }</tspan></text>
```

3. **Julius _message**

   Julius → Caesar Ciper Encoded

CAESAR CIPHER DECODER

CAESAR SHIFTED CIPHERTEXT

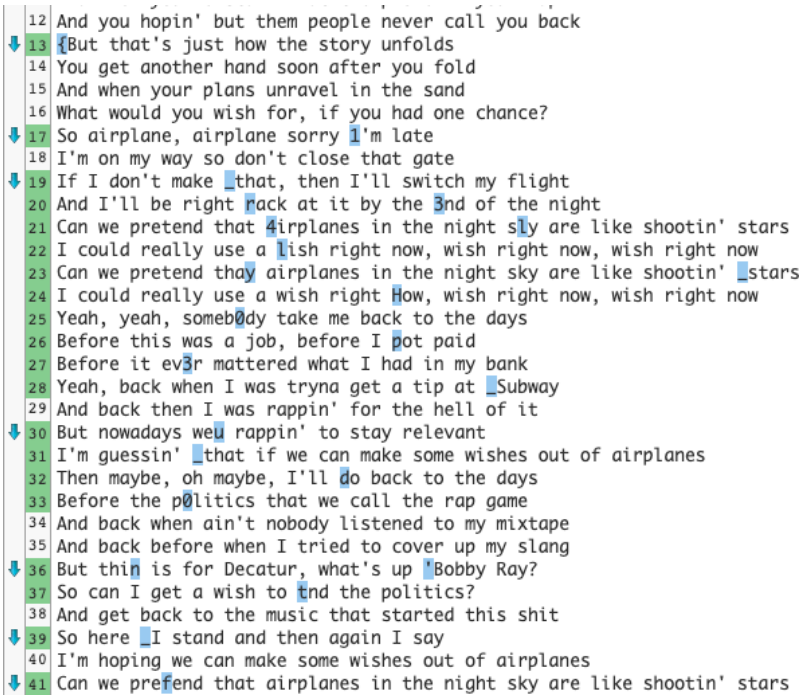
```
iob vdih, eh fbehuvhfxuh
```

↑↓	↑↓
□3 (□23)	fly safe, be cybersecure

4. **General/Aeroplanes**

   Song name: Aeroplanes by B.o.B

   Found the lyrics in google and the compared them using text-compare.com



5. **General/Base64**

   Copied the text from enc.txt and pasted into base 64 decoder Repeated until the

   flag was found

   Vm0wd2QyVkZOVWRpUm1ScFVtMW9WRll3Wkc5WFZsbDNXa1JTV0ZKdGVIbFhhMk0xVmpGYWMySkVUbHBXVmxwU

   Vm0wd2VFNUdiRmRpUm1oVFYwZG9XVll3WkRSWFJteHlXa2M1VjFac2JETlpWVlpQVjBaYWRHVkVRbUZTVmxsM1dWZ

   Vm0weE5GbFdiRmhTV0doWVYwZDRXRmxyWkc5V1ZsbDNZVVZPV0ZadGVEQmFSVll3WVd4YWMxTnNiRlZXYkVwVVZ

   Vm0xNFlWbFhSWGhYV0d4WFlrZG9WVll3YUVOWFZteDBaRVYwYWxac1NsbFVWbEpUVkcxS1NHVkVRbFZpUmtwRVd

   Vm14YVlXRXhXWGxXYkdoVVYwaENXVmx0ZEV0alZsSllUVlJTVG1KSGVEQlViRkpEWVVkS1YxZHNXbGROVjJneldWY3

   VmxaYWExWXlWbGhUV0hCWVltdEtjVlJYTVRSTmJHeDBUbFJDYUdKV1dsWldNV2gzWVcxR2MxSnFVbUZXYlZKUVZU

   VlZaa1YyVlhTWHBYYmtKcVRXMTRNbGx0TlRCaGJWWlZWMWh3YW1Gc1JqUmFWbVJQVTFac1ZWSllhRTVOYWxaMV

   VVZkV2VXSXpXbkJqTW14MlltNTBhbVZVV1hwamFsRjRaVmRPU1ZsVVJYaE5NalZ1VFRNd1BRPT0=

   UVdWeWIzWnBjMmx2Ym50amVUWXpjalF4ZVdOSVlURXhNMjVuTTMwPQ==

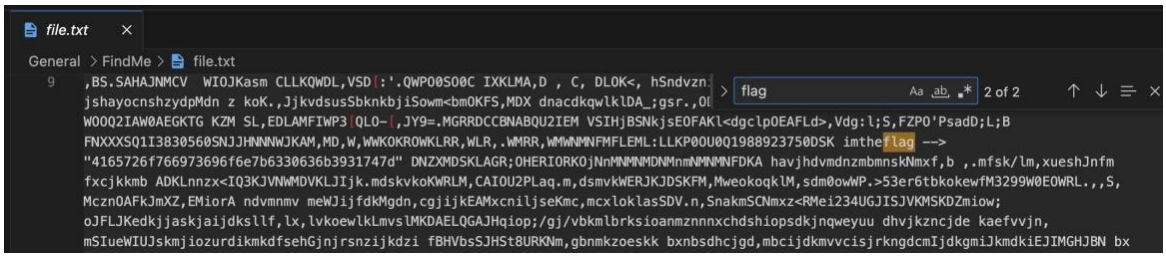
   QWVyb3Zpc2lvbntjeTYzcjQxeWNIYTExM25nM30=

   Aerovision{cy63r41ycHa113ng3}

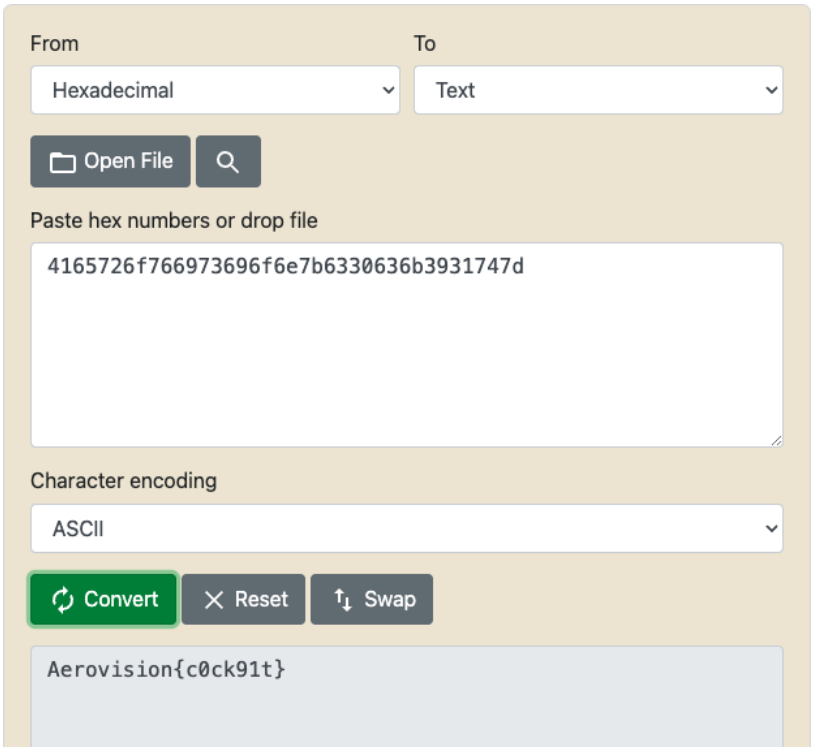
6. **General/FindMe**

Unzipped the given file

After extracting, got this image of a cockpit and file.txt

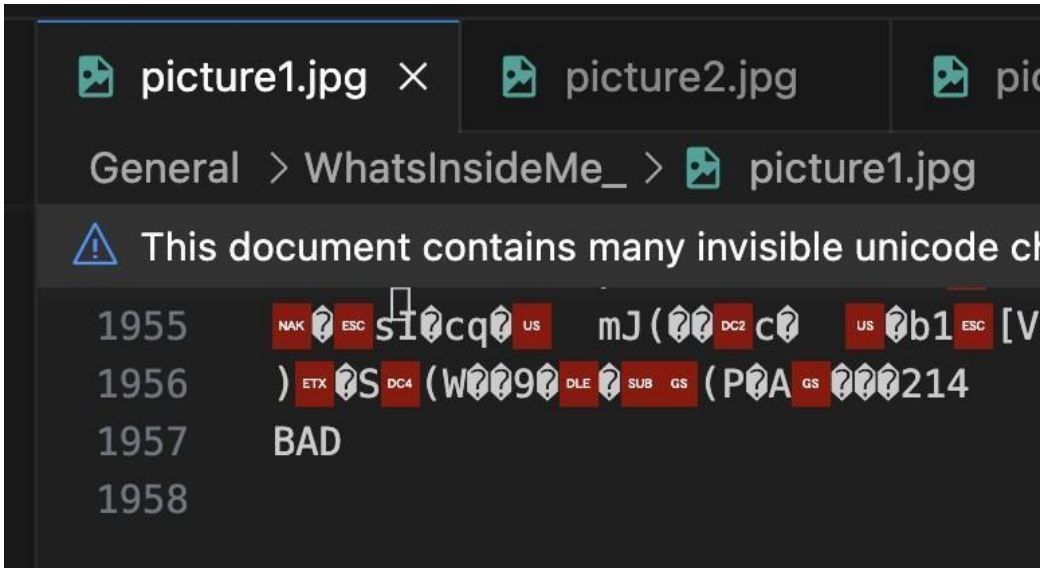


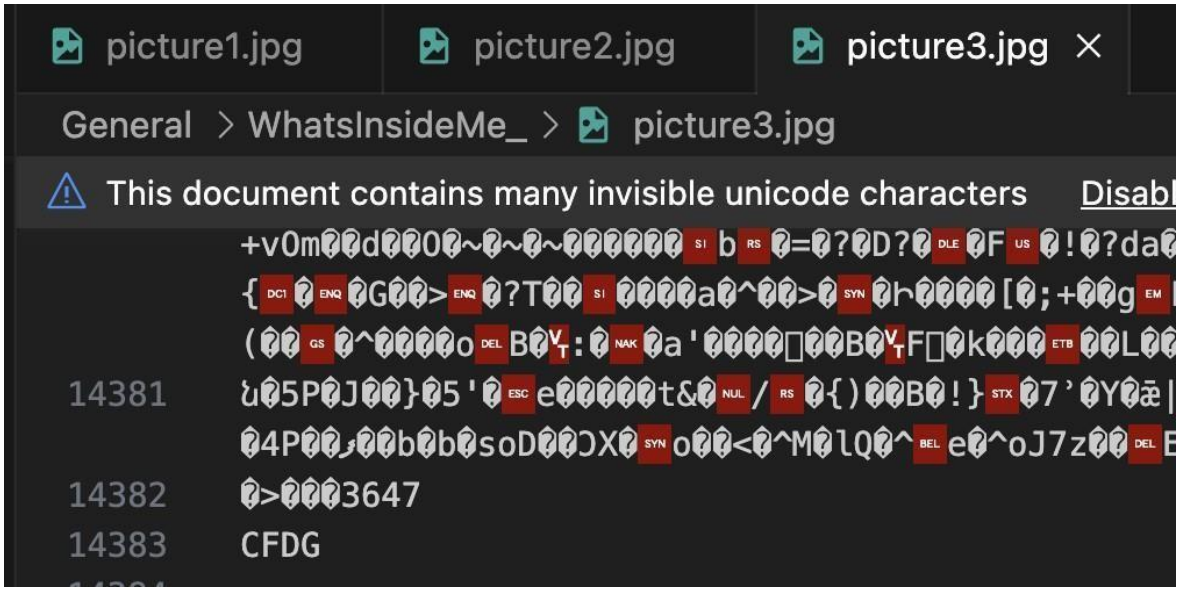
Used a hex to ascii convertor for the given text



7. **General/WhatsInsideMe_** Opened

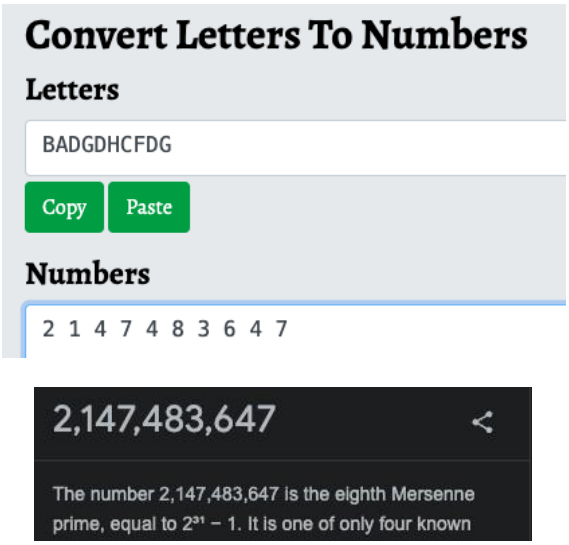
   the 3 images in text format





BADGDHCFDG

Converted this text to numbers (A - 1, B -2, etc.)



Flag: eighth **MERSENNE PRIME**

8. **Retrieve_my_forebearer**

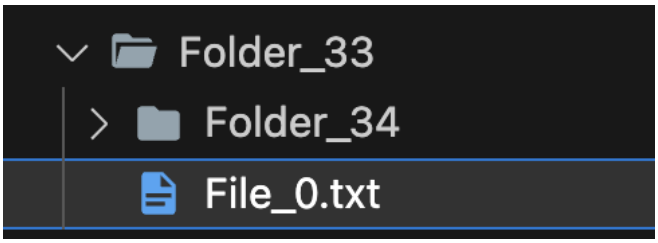
Decompiling the sample.class file resulted in revealing the flag.

```
// Source code is decompiled from a .class file using FernFlower decompiler.
class sample {
   sample() {
   }

   public static void main(String[] var0) {
      System.out.println("Aerovision {Fly Risk free}");
   }
}
```

9. **scavenger_hunt**

Found the flag in folder 33



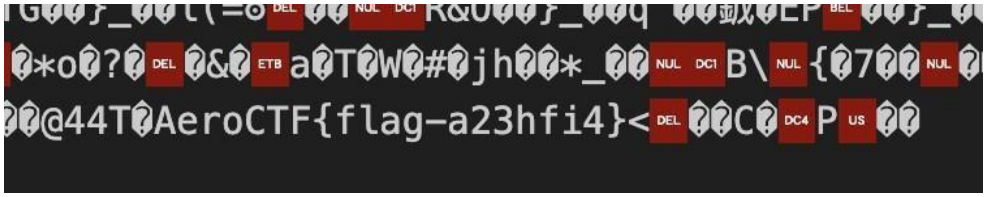

```
1    Aerovision(4ll-th4t-w0rk-f0r-th1s)
```

10. **this_is_a_plane**

Repeatedly unzipped the image until we found an error

```
jeyam@Jim this_is_a_plane % unzip s_2.jpg
Archive:  s_2.jpg
warning [s_2.jpg]:  123605 extra bytes at beginning or within zipfile
  (attempting to process anyway)
  inflating: s_3.jpg
jeyam@Jim this_is_a_plane % unzip s_3.jpg
Archive:  s_3.jpg
  End-of-central-directory signature not found.  Either this file is not
  a zipfile, or it constitutes one disk of a multi-part archive.  In the
  latter case the central directory and zipfile comment will be found on
  the last disk(s) of this archive.
unzip:  cannot find zipfile directory in one of s_3.jpg or
        s_3.jpg.zip, and cannot find s_3.jpg.ZIP, period.
```

Opened the image in text format and scrolled down to the end



11. **scaryyy**

Browsed to this site https://futureboy.us/stegano/decinput.html and typed the password as "password", and on processing the image, got the flag


```
Aerovision{T1isd_oe5nt_mxke_5en5e}
```

12. **Web/GuardianFlight**

This was found in the question. Skimming thorugh the site provided http://intellx.in:7100, found the flag.

13. **Web/WebHunt**

Found the key using python, and using decrytption tools online, the flag was found.

14. **Web/Inspect**

Moving to the site, as per the question, the Inspect window was opened using F11 and the flag was found.

15. **Its_about_flow**

The given Cyber.class file was decompiled, and v1510_pr0t3<t0r15 - this was found. On the clue, the whole flag is alphabetic, it was changed to visio_protectoris.

16. **Numerical Maze Solver**

Solving the maze got the first flag required. Now analyzing the maze further based on the coordinates, the second flag was found as well.

17. **Cryptography/DecryptMe**

For the first clue "txkh" - Caesar cipher was applied, it gave "aero" as the key required. Which was later used in Vignere Cipher for the second clue "eexze-ipsd tictithise" - which later provided the answer : eagle-eyed protection

18. **Cryptography/MorseCode**

On an online Morse Code decoder, the .wav file was uploaded the key was generated.

19. **Cryptography/TryMe**

    On a ROT47 decryption site : https://www.browserling.com/tools/rot47 , the secret key "p6C@G:D:@?L`>0Ewb0c=28N" was decrypted for the following flag.

20. **Cryptography2/youCompleteMe**

    For the given key, try it on Caeser Cipher decrypter and got the key.

21. **init**

    This was obvious. The flag was provided in the file “flag”.

22. **12_more_times**

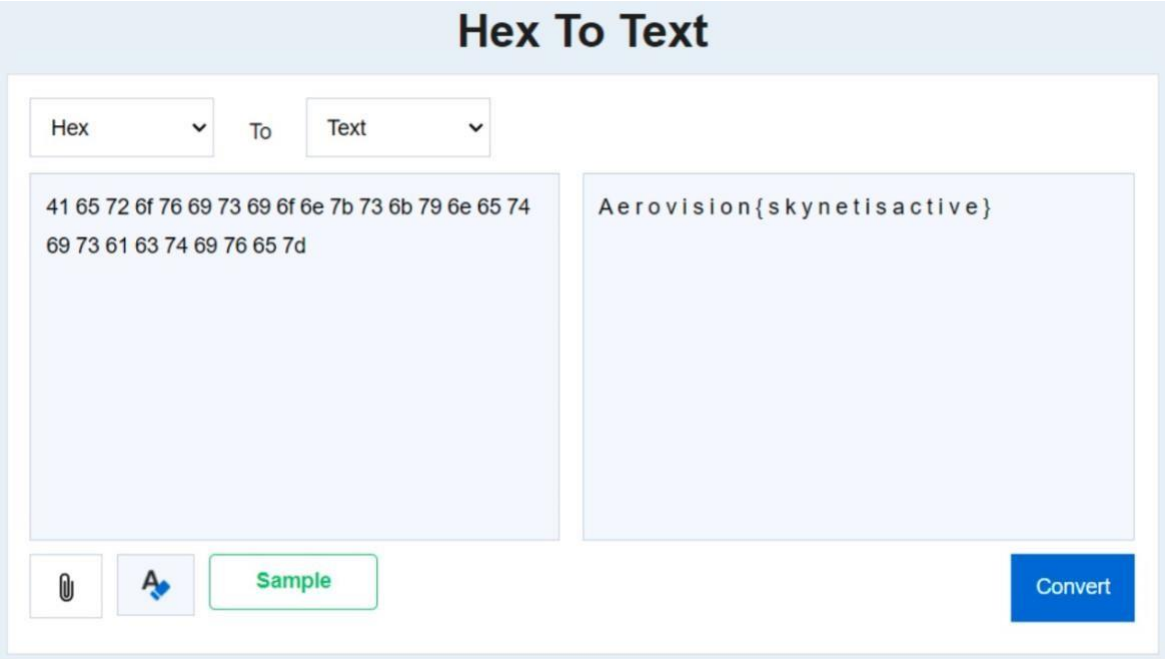
    The numbers were operated under mod37 and the following result occurred: 19 7 27 18 36 22 30 18 36 7 30 17 3. Applying 0 - 25 for alphabets, 26 - 35 for numbers, Got the final flag.

23. **Forensics/corx1upted**

    A Hex editor was used to find the corrupted flag, and thus.

24. **Forensics/FinTheChat**

    Following the multiple flags, and finding all the hex values, these values were converted to text using https://www.duplichecker.com/hex-to-text.php and here’s the flag.



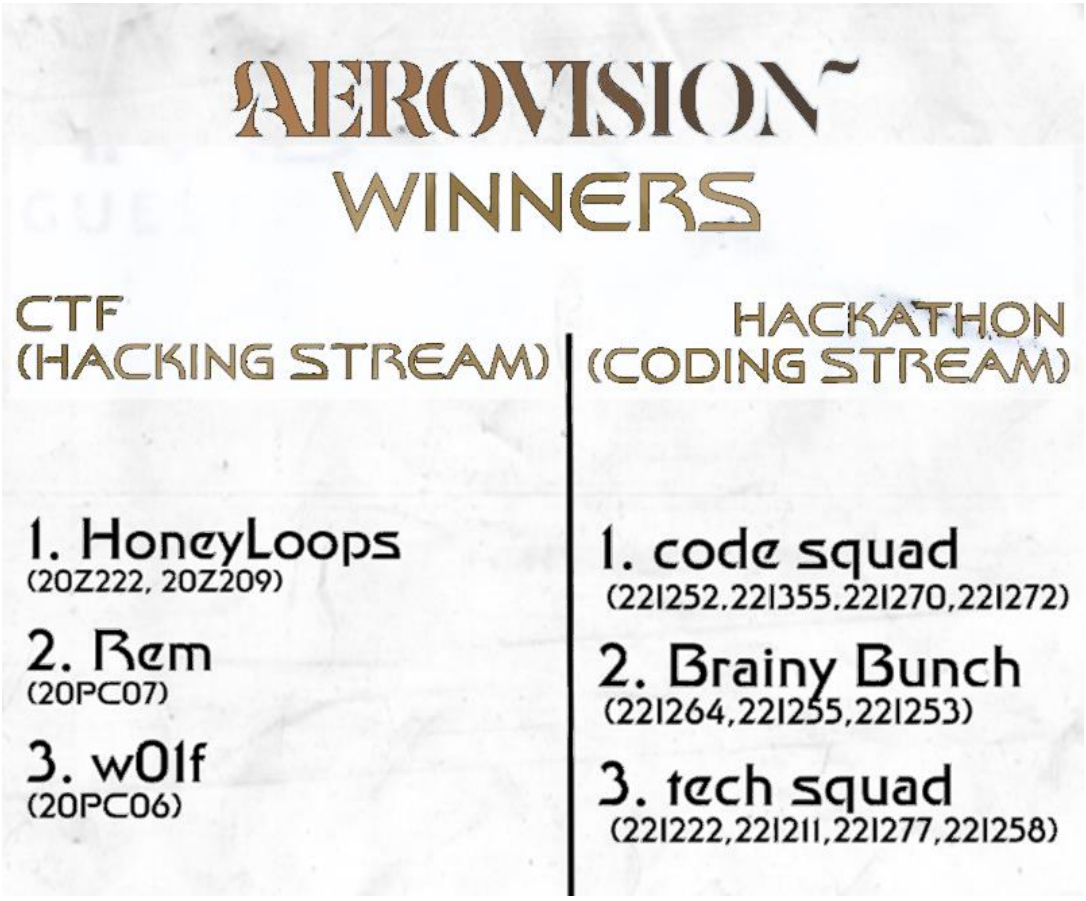
25. **Forensics/itsHot**

    To get the metadata for a file, we used the exiftool linux command. Following that, the word AeroVision was found and thus the flag was concluded.

Coding Stream Hackathon Assessment Sheet

Place	Team	Innovation & Creativity	Technical Implementation	Presentation & Demonstration	Usability & Practicality	Code Redundancy & Documentation	Total Points
🥇	Code_Squad	16	25	20	15	8	84
🥈	Brainy Bunch	15	24	17	12	7	75
🥉	Tech_Squad	15	20	16	13	6	70
4th	The Sharks	26	9	15	10	2	62
5th	Soul Celestia	24	0	19	12	0	55

Final Results



Attendance Lists

# of Registrants	**150**
Day 1 Attendees (Offline)	**48**
Day 2 Attendees (Online)	**35**
# of Hackathon Participants	**53**

Participation Analysis

Participants Analysis Chart