Introduction and Front Matter

Goh Weihan
ICT3215 Digital Forensics
BEng (Hons) in Information and Communications Technology
(Information Security)
September 2024

/usr/bin/whoami

SINGAPORE INSTITUTE OF TECHNOLOGY

- 🎓 Graduated from NTU in 2008
- 🏫 Teaching cybersecurity at SIT since 2015
- 🖥️ Building a cyber range at SIT
- 🔐 Interested in new ways to teach cybersecurity
- ⛳ Plays CTFs, low-key vulnerability researcher

Goh Weihan // 'icebear'

Associate Professor
Infocomm Technology Cluster
Singapore Institute of Technology

https://www.singaporetech.edu.sg/directory/faculty/weihan-goh
Weihan.Goh {at} Singaporetech.edu.sg | +65 6592 8517 | icebear#2479 (Discord)

🔢 ICT3215 Digital Forensics AY2024/25 Trimester 1 in Numbers

SINGAPORE INSTITUTE OF TECHNOLOGY

130 full-time students

73 MINDEF DIS Cyber Specialists

2 practical session groups across one timeslot

4 Capture-the-flag format assessments

1 team-based project assignment

No exams

Academic Matters

🏫 What's In The Module (In a Nutshell)

SINGAPORE INSTITUTE OF TECHNOLOGY

Instructors

👩‍🏫 Weihan Goh

Support

👩‍🏫 Remy Mohamed

- **Primary resource**
  None in particular...
- **Recommended resource**
  Too many to list...

What (we hope) you will gain after this module

📘 Understand fundamental forensic concepts and be able to use associated technical commands

📘 Able to identify and use appropriate tools and techniques to acquire information of interest from single systems, as well as in a complex, multi-system scenarios

📘 Able to design and develop complex and novel solutions to aid in the digital forensics process

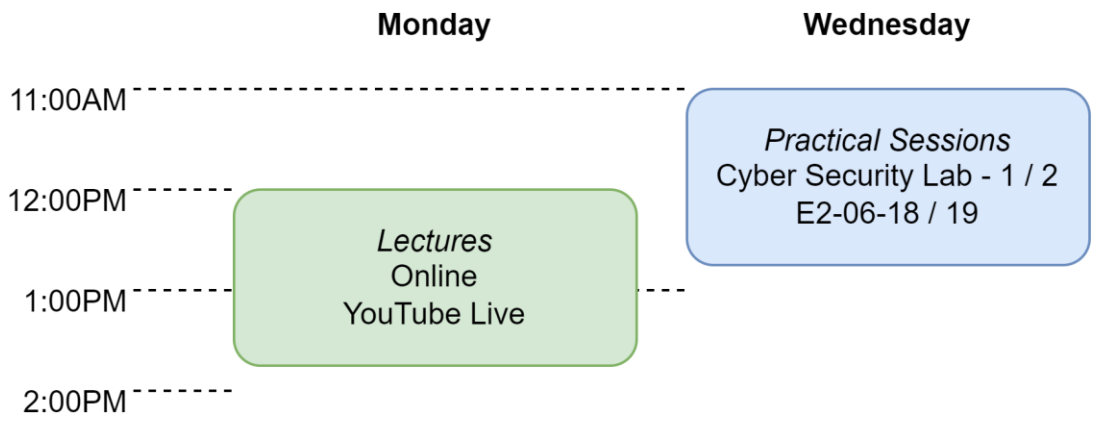
When We Say That There Are Too Many Resources to List...

Topic to be Covered (Tentative, and Not Limited To)

SINGAPORE INSTITUTE OF TECHNOLOGY

- Introduction to digital forensics and anti-forensics
- Data acquisition from file systems and storage devices
- Preservation of data
- Data integrity verification
- Analysis of preserved data
- Issues in anti-forensics
- Tools and techniques for digital forensics

✍️ Weekly Lesson Structure



📣 Lectures

- 📅 Mondays
- 🕐 12:00PM to 2:00PM SGT
- 🖥️ Online @ YouTube Live

🧪 Practical Sessions (for Labs / Project / Assessments)

- 📅 Wednesdays
- 🕐 11:00AM to 1:00PM SGT
- 🖥️ On-Campus @
  - E2-06-18 Cyber Security Lab 1 (P1)
  - E2-06-19 Cyber Security Lab 2 (P2)

All in-class sessions will be held at our SIT Punggol campus

The E2-06-18 / 19 Cyber Security Lab 1 / 2 are BYOD labs, thus there are no computers in the lab

A navigation app can be found at Campus Wayfinder | Singapore Institute of Technology (singaporetech.edu.sg)

📋 Ground Rules

Lessons shall start on time

If there are questions, do ask; however please be considerate to other students

Be present in the correct lab according to your practical session group

Some of the practical session timeslots will be used for in-class assessments

Assessments (Tentative)

Team Project Assignment	Project work, reasonably complex tasks, etc. Duration spans across the entire trimester
Capture-the-Flag Assessments	Focused on skill(s) Conducted during practical session timeslots More information will be provided in due time

Fully CA-based module, no final exams

100% from assignments and practical assessments

Assessment Breakdown (Tentative)

Team Project Assignment: Students are tasked to develop a tool to aid in (or hinder) the digital forensics process **[~35%]**

CTF Assessment 1: Capture-the-flag on fundamental forensic concepts and technical commands **[~20%]**

CTF Assessment 2: Given an evidence computer and disk, analyze these items to identify information of interest, in a capture-the-flag setting **[~15%]**

CTF Assessment 3: Given a smart mobile device memory dump, analyze the dump and identify information of interest, in a capture-the-flag setting **[~15%]**

CTF Assessment 4: Given a complex, multi-system scenario, analyze the systems and identify information of interest, in a capture-the-flag setting **[~15%]**

📊 Assessment Schedule (Tentative)

Team Project Assignment

- **Week 1:** Students to form teams
- **Week 4:** Submission of 2-page project proposal
- **Week 13:** Submission of final deliverables

CTF Assessment 1: Wednesday, October 2, 2024 ***[Week 5]***

CTF Assessment 2: Wednesday, October 23, 2024 ***[Week 8]***

CTF Assessment 3: Wednesday, November 6, 2024 ***[Week 10]***

CTF Assessment 4: Wednesday, November 20, 2024 ***[Week 12]***

Labs will gradually be uploaded from Week 1 onwards 

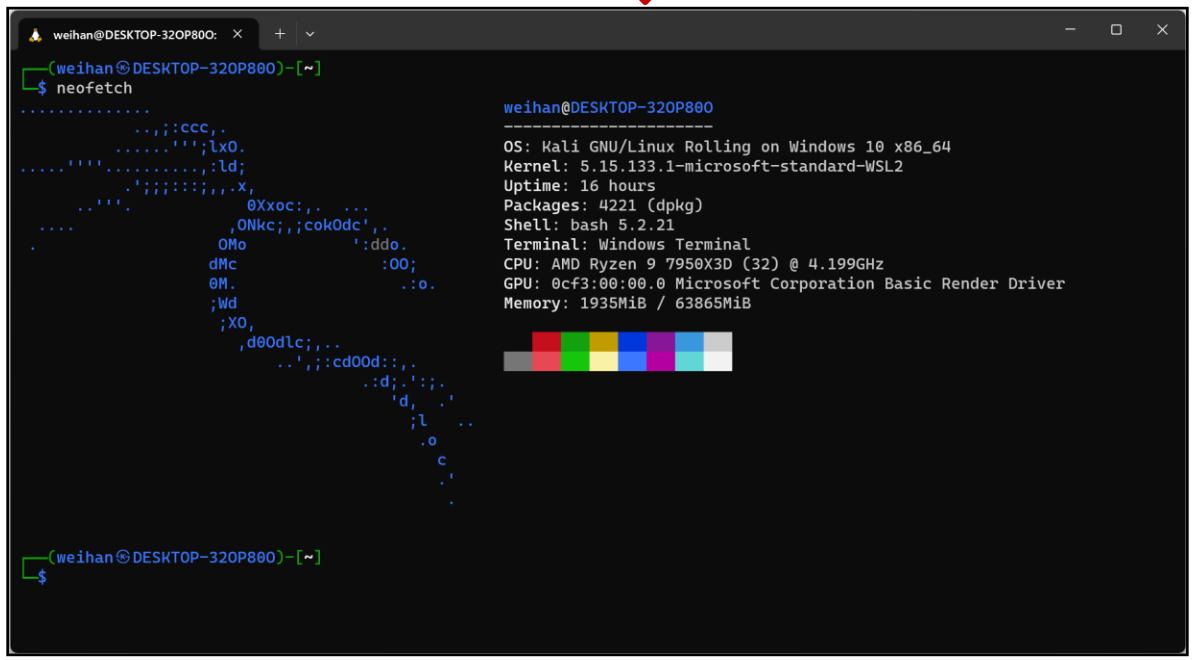
Tools and Software

Software for the Module

- **Operating systems**
  - **Kali Linux:** https://www.kali.org/get-kali/
    - Either live boot, or a virtual machine with USB passthrough
    - WSL2 can be used when hardware access is not required

- **Protip:** VMware Workstation Pro and VMware Fusion Pro are free for personal use
  - VMware Workstation Pro: Now Available Free for Personal Use - VMware Workstation Zealot

WSL2 is not enough...



The Linux terminal is your friend 

Software for the Module

- **Digital forensics platform**
  - **Autopsy:** https://www.autopsy.com/
    - Open-source digital forensics platform and graphical interface to The Sleuth Kit
    - Can be extended using add-ons
      - https://github.com/sleuthkit/autopsy_addon_modules

- **Other digital forensic tools**
  - Some other tools that we might use include
    - Kroll Artifact Parser And Extractor (KAPE)
    - Eric Zimmerman's tools
    - NirSoft
    - iLEAPP, ALEAPP, RLEAPP, …
    - Belkasoft RAM Capturer, Magnet DumpIt, …
    - Volatility 3
    - …

Module Logistics

Next Steps

Get Kali Linux up and running

Kali Linux: https://www.kali.org/downloads/

- Get it to run "live" from a USB drive
- If not possible, at least get it running in WSL or a virtual machine for now
  - You will eventually still need to get it running "live", as certain labs and assessments will require that
- Configure your Kali to your liking
  - You may consider installing the *kali-linux-everything* metapackage if you are running Kali in WSL or in a virtual machine

Next Steps

Form teams of five (5) individuals for your project assignment

You and your peers, **regardless of your practical session groups**, may come together to form your own teams

- Your team can consist of at most five (5) individuals
- Submit your team information at https://forms.office.com/r/5EYfV2fhsS
- **Deadline for submission:** End of Wednesday, September 11, 2024
  - If you are unable to be part of a team by the end of the deadline, you, and others like you, may be grouped together into teams

Err Excuse Me, What's a Capture-the-Flag?

⛳ What's a Capture-the-Flag?

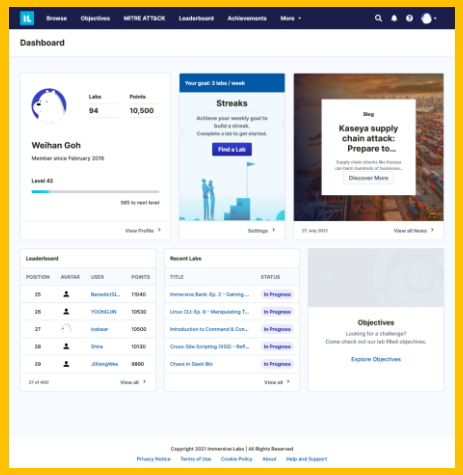
- **Challenge:** *You found the following two-dimensional barcode discarded in the trash and made a scan of it. It purportedly contains a secret code. What is the code?*
- **Maximum Attempts:** 10
- **Challenge Difficulty:** Very Easy

⚒️ Not all Capture-the-Flags are Equal!

SINGAPORE INSTITUTE OF TECHNOLOGY

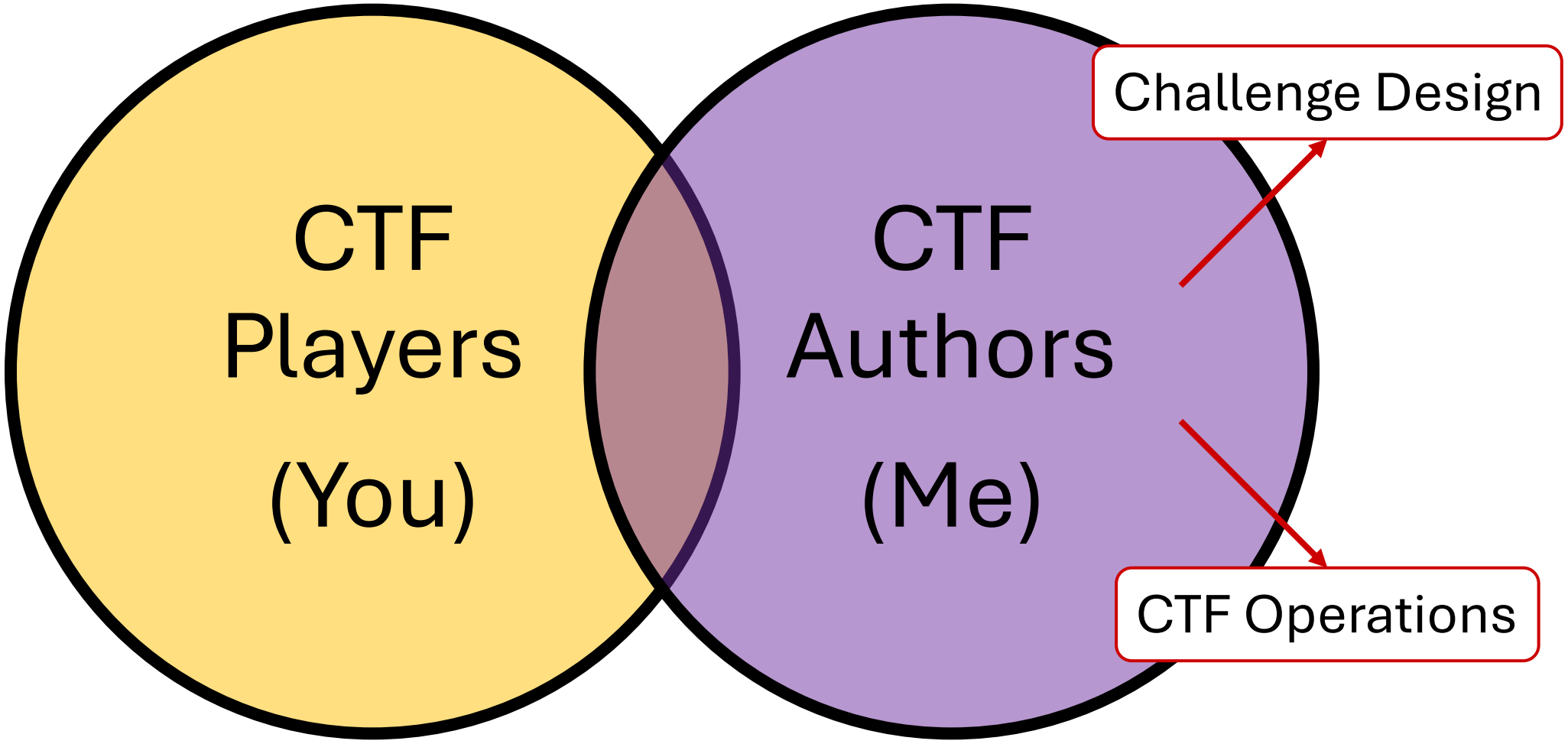
Competitions

Assessments



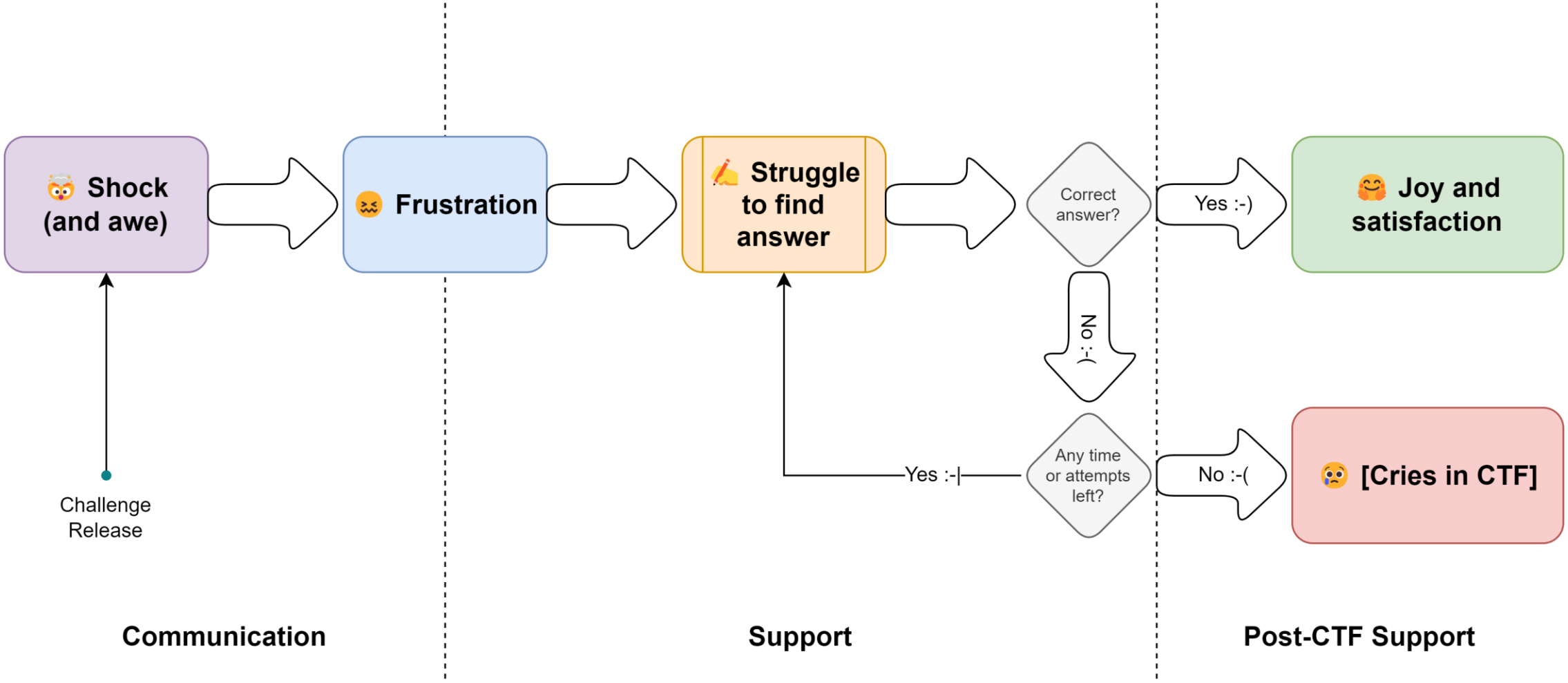
Learning

Fun 🙂

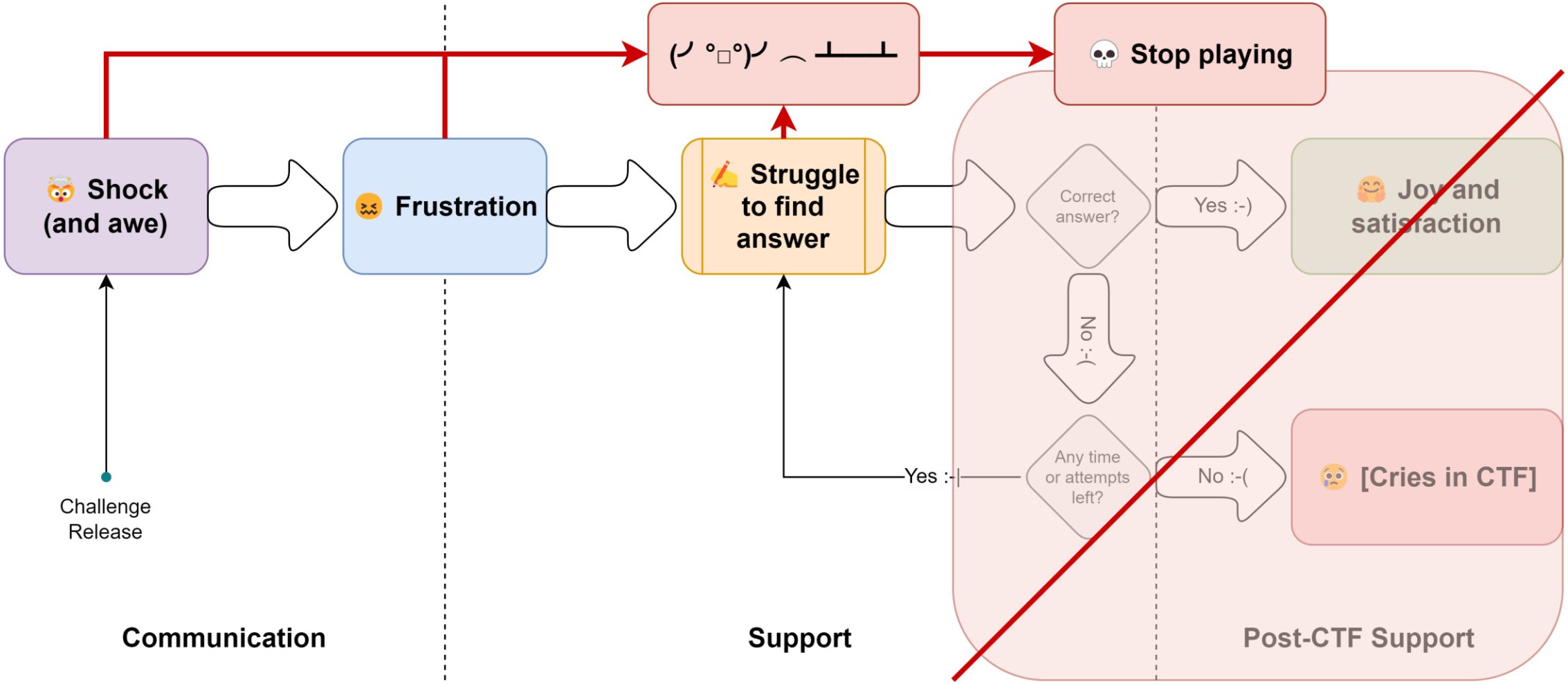

CTF
Players
(You)
CTF
Authors
(Me)
Challenge Design
CTF Operations

A CTF is not a competition between the challenge authors and the players

😭 Four Stages of CTF Grief



😭 Four Stages of CTF Grief



😟 Frustration is Normal(?)

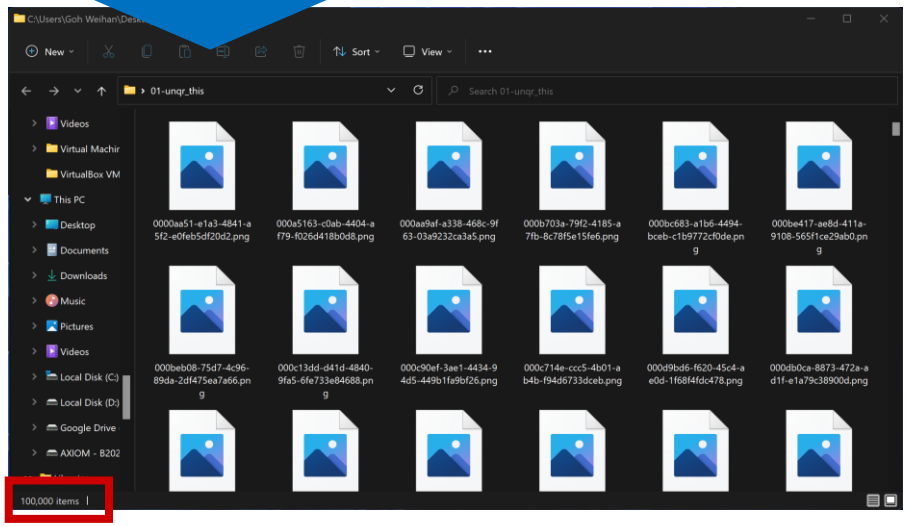
People do not play CTFs to feel frustrated...

...but a CTF that do not invoke frustration is boring

- Some random sage

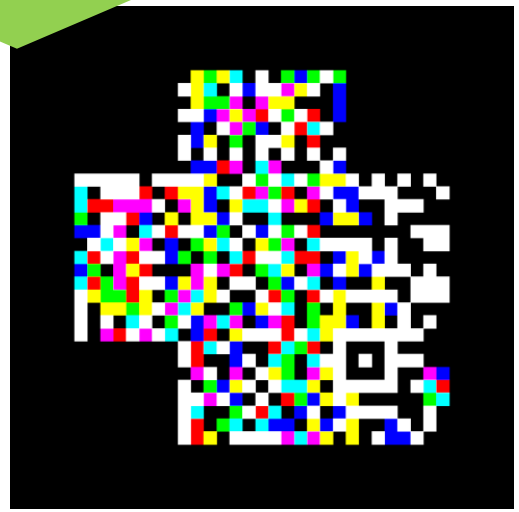
- There will be satisfaction at the end of frustration

Challenge: *Find the flag in these QR code files*



Provoking Thoughts and Inspiration

Challenge: *What is the code?*



When tackling a challenge

- Break down challenges into steps
- Be inspired on what to try next, repeat step-by-step until the flag is revealed
- Consider the 'search space' required to find the challenge solution

Inspiration vs Work Required

Challenges that need ⬇️+➡️ are	little work	some work	a lot of work	too much work
little inspiration	Very easy	Relaxing, disappointing	Uninteresting	Boring
some inspiration	Easy, satisfying	Fun	Exhausting	Frustrating
a lot of inspiration	Surprising, insightful	Challenging	Very hard	Very frustrating
too much inspiration	Guessy	Frustrating	Very frustrating	Unreasonable

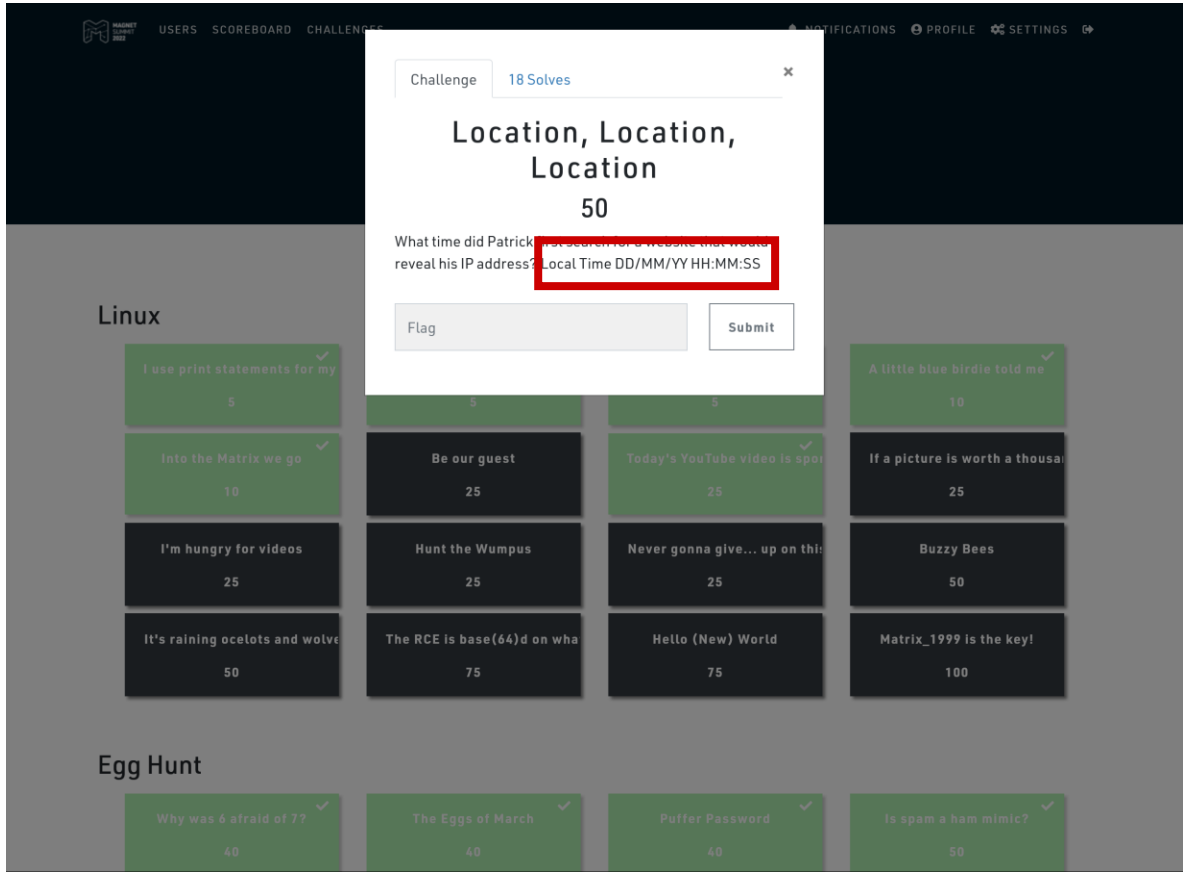
Adapted from CTF Design Guidelines: Design guidelines for CTF authors and organizers (https://bit.ly/ctf-design)

📜 Clarity of Communication

If required, the format for a challenge's answer will be communicated to you, but if in doubt, ask!

Some common pitfalls

- Units of measurements, e.g., **MiB** vs **MB**
- Time zone, e.g., **UTC**, **Eastern Time**, etc.
- Date format, e.g., **DD/MM/YYYY** vs **MM/DD/YYYY**
- Date interpretation, e.g., is **06/07/2024** representing **June 7, 2024**, or **July 6, 2024**?



Avoiding Complex Answer Formats

The more complex the answer format, the more frustrating it is, so we try to avoid creating such challenges

What we tend to do instead

- Splitting the challenge into smaller challenges
- Using question pre-requisites as gatekeepers

Challenge: *How many unique acquisition tools were recognized by Marsha's PC, how many times did the acquisition tools connect, and when was the last time an acquisition tool was connected? Format: [unique #] [total #] MM-DD-YYYY HH:MM e.g. 1 3 01-22-2019 19:46*

🗺️ Avoiding Ridiculous Search Space Scope

Challenge: *The key to decrypt the message is a word at the Singapore Institute of Technology website*

Search spaces will be kept reasonable within the context of the challenge and scenario

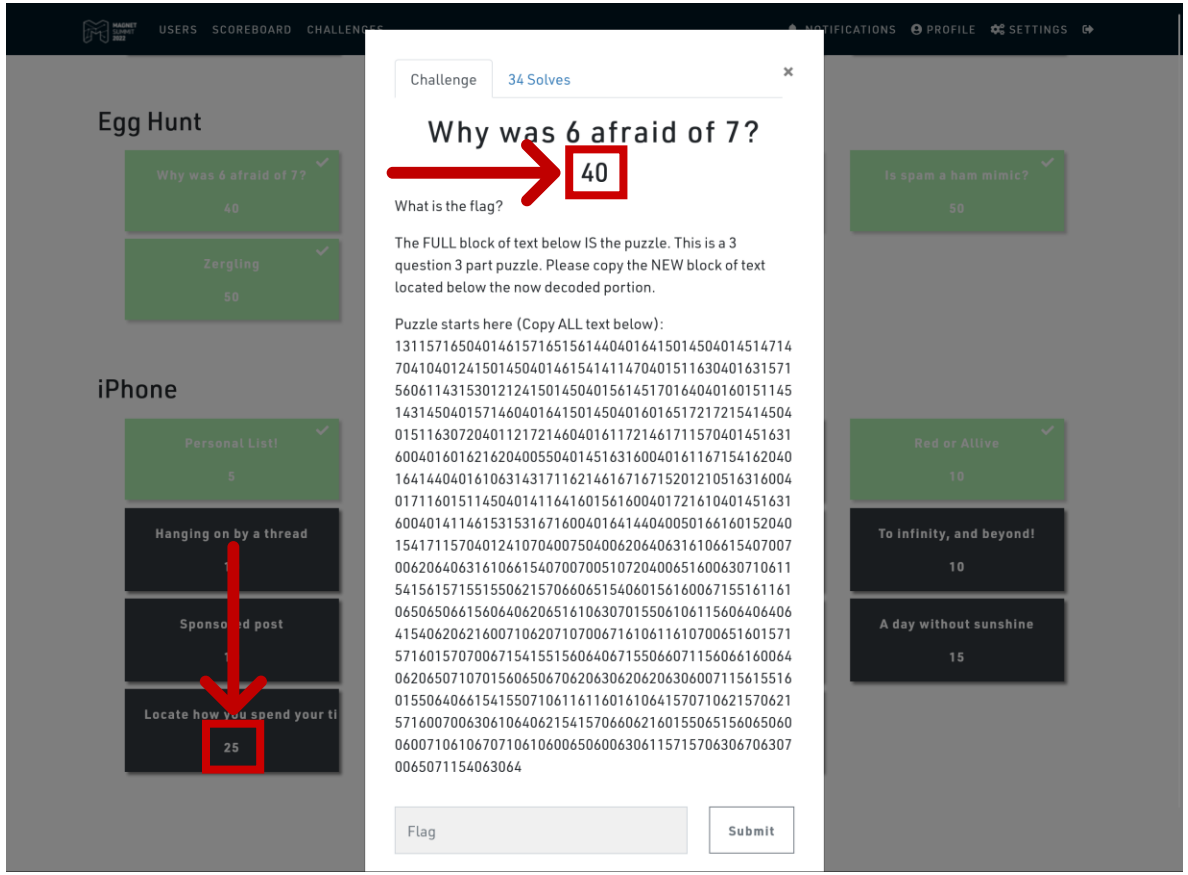
`61b0799ceb1251370a0808187191c6d6c7112d`
`fab4eae5ac4ab5a5b562083bb5`

Unreasonable search spaces can easily kill motivation and lead to frustration

💯 Balancing Points Appropriately

Points will be balanced accordingly, and possibly commensurate to the difficulty level

Imbalanced points distribution can lead to good players giving up



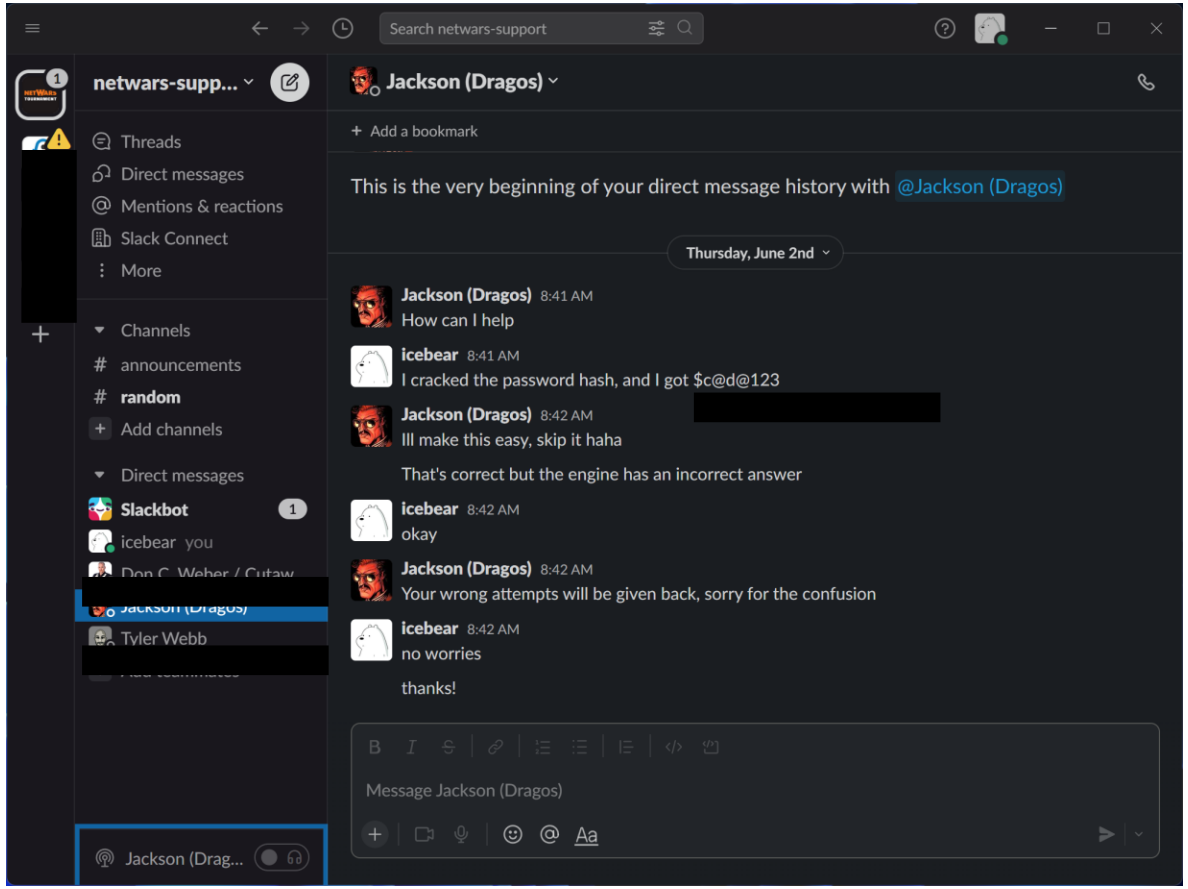
Instructors Will Be on Standby to Monitor the Situation

SINGAPORE INSTITUTE OF TECHNOLOGY

We are here to test your competency, not to torture you

It is bad enough to be stuck, it is worse if you get no support

A broken challenge may be indistinguishable from a difficult challenge



👋 Questions?
Thank You!

- 📨 Weihan.Goh {at} Singaporetech.edu.sg
- 📌 https://www.singaporetech.edu.sg/directory/faculty/weihan-goh
- 📌 https://sg.linkedin.com/in/weihan-goh