- (CRYPTO) Init
  - Description
    - Like two lovers, use the answer to this puzzle to replace "start" in the URL, in ALL CAPS! Example: 20250210.gm.neu-ctf.club/[WORD]
    - https://mywordle.strivemath.com/?word=hcmhc
  - Solution:
    - Solve wordle and go to /LOVER: 20250210.gm.neu-ctf.club/LOVER

- (FORENSICS)
  - Description
    - Snoopy got all dressed up for the occasion! Is there some data hidden in the red bits of this image?

      Hint: Use https://georgeom.net/StegOnline, upload the image, and select extract files/data
  - Solution
    - Do what the hint says, then select all the "R" values in the RGB table on the webpage and hit "go"
    - There is ASCII readable text of /HEART which is the next path

- (CRYPTO) A1Z2MyHeart
  - Description
    - Wow, I fell asleep in Foundies and when I woke up, there was this note on my desk! Maybe it's from a secret admirer???

      13 5 5 20   13 5   1 20   / 6 12 1 7 7 9 6
  - Solution
    - A1Z26 Cipher Decode -> It says meet met at /flaggif

- (CRYPTO)
  - Description:
    - Can you read flag semaphore?
  - Solution:
    - Break up GIF into individual frames (can do this online) and google flag semaphore code to decrypt. First frame indicates numericals. Following frames are binary (either 0, 1, or space)
    - Should decode to binary: 00101111 01110000 01101111 01100101 01101101
    - Decode binary to ascii: /poem

- (CRYPTO) Cupid Vigenere
  - Description

-
- Solution
  - Poem hints to the main place where we announce events- instagram (the GM image needed for this challenge was also sent in the newsletter and in the discord announcement)
  - If you zoom in a lot and look closely at the image, it has "%2HHTFW-UNTX" written in the hearts at the bottom
  - In the caption, there are hashtags #UnlockWithCupid, #KeyOfCupid, #VigenereCodebreaker which hint of a key being "cupid". Ciphertext looks like a substitution cipher, and with a key, it hints to vigenere cipher
  - Vigenere decode with key "cupid" which leads to "%2FNEXT-STEP" which is url encoded
- Next Step
  - /NEXT-STEP

- (OSINT) 5 words Challenge part 1
  - Description

  -
- Solution

- The hashtag stuff was supposed to work, but Instagram cooked us, so we posted a comment on the announcement for the GM by a new account with one post. Look at the post. It shows a location in Shillman (3rd floor by the elevator). They should go to that location. There will be a puzzle on paper they need to grab and solve at their desks, and instructions for that

- (MISC) 5 words Challenge part 2
  - Solution
    - The solution to the puzzle is that the center letter is t and the words are: tobacco, brothel, limited, dormant, jackpot
    - Send an email to neuctfclub@gmail.com with exactly the following as the subject: "t, jackpot, tobacco, brothel, limited, dormant". An automated response has been set up to tell you the next step
  - Next Step
    - /LetsStayInTouch

- (CRYPTO) Let's stay in touch
  - Description
    - Let's stay in touch. Here's my number – well, not quite, but I am sure you can figure it out! I only give people chances if they are smart enough to crack RSA ;). Note, that `e` is really small, I wonder if that's a vulnerability …
      Note: the next link will be /{NUMBERS_HERE}, without the curly braces, i.e. /3283932010

      n = 168264254973663386157121630273521616937
      e = 3
      ciphertext = 2124594493609762363677489728
  - Solution:
    - The exponent `e` is too small, and as a result, when you calculate the ciphertext, it doesn't get `mod`ed because it's not bigger than `n`. So you can just take the cube root of the ciphertext and it gives you the number!
  - Next Step
    - /1285559012

- (PHYSICAL/FORENSICS) Sharks and Wires
  - Description
    - People typically get roses & chocolates from their partners but I got wires and sharks. Maybe there's a hidden message somewhere in here?
  - Solution:
    - Right click on TCP packet > Follow > TCP stream. There are a couple of messages, some in base64 and some in hex! The last one message is in

base64 and tells you that the password to the zip is `psistillloveyou`. You can do File > Export Objects > HTTP and export all the objects sent. Two are images of bad pick-up lines, the last one is a .7z file. Extract it with 7z x super-secret-valentines.7z and the password is psistillloveyou. The cupids-message.png inside tells you to go up to the board and hit a bullseye. Once you hit the targets with the nerf gun, we give you the next location, which is /decode-lockbox

- Dependencies
  - sharks-and-wires.pcapng

- (RE) Final Challenge
  - Description:
    - This app is asking ME for the flag… how am I supposed to know that?!
    - Hint: a .jar file contains packaged Java code. Are there tools to attempt to get the source code from Java applications? Maybe a decompiler?
  - Solution:
    - Open the application in the Java decompiler JADX-GUI. Notice the checkFlag() function is "native", meaning that it is calling through the Java Native Interface. This allows developers to use C code in their Java apps.
    - Find resource liblove.so. This file can be extracted by unzipping the .jar.
    - Open in Ghidra, reverse engineer the checkFlag() function there. It's a relatively simple function checking the individual characters of the flag.
  - Flag:
    - CTF{GR0M!}