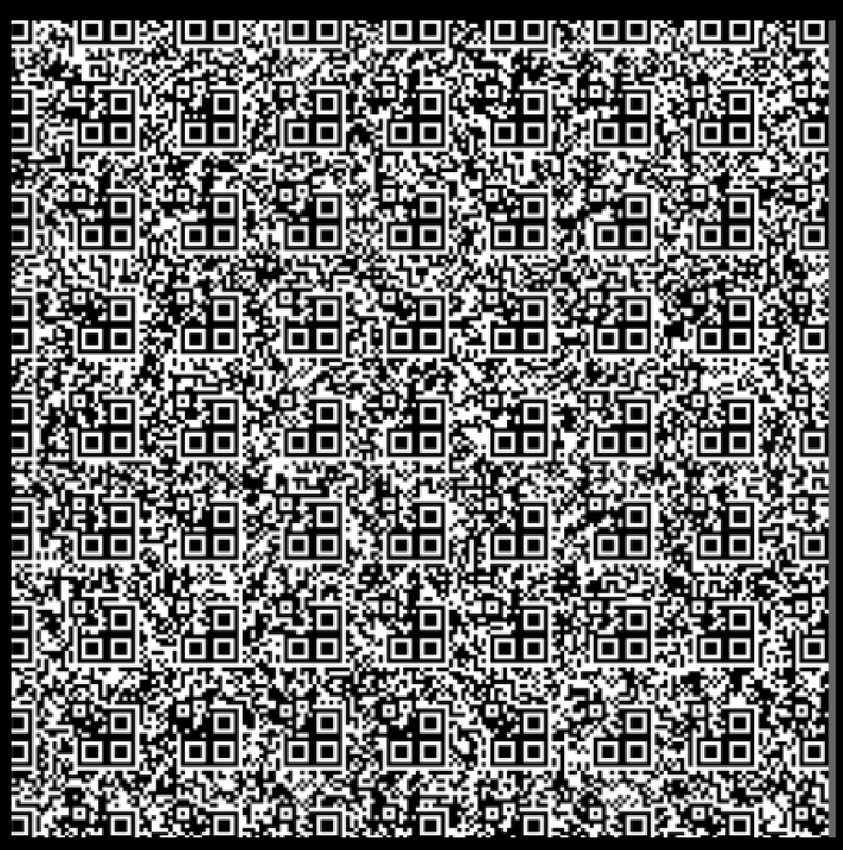
UMASS CTF

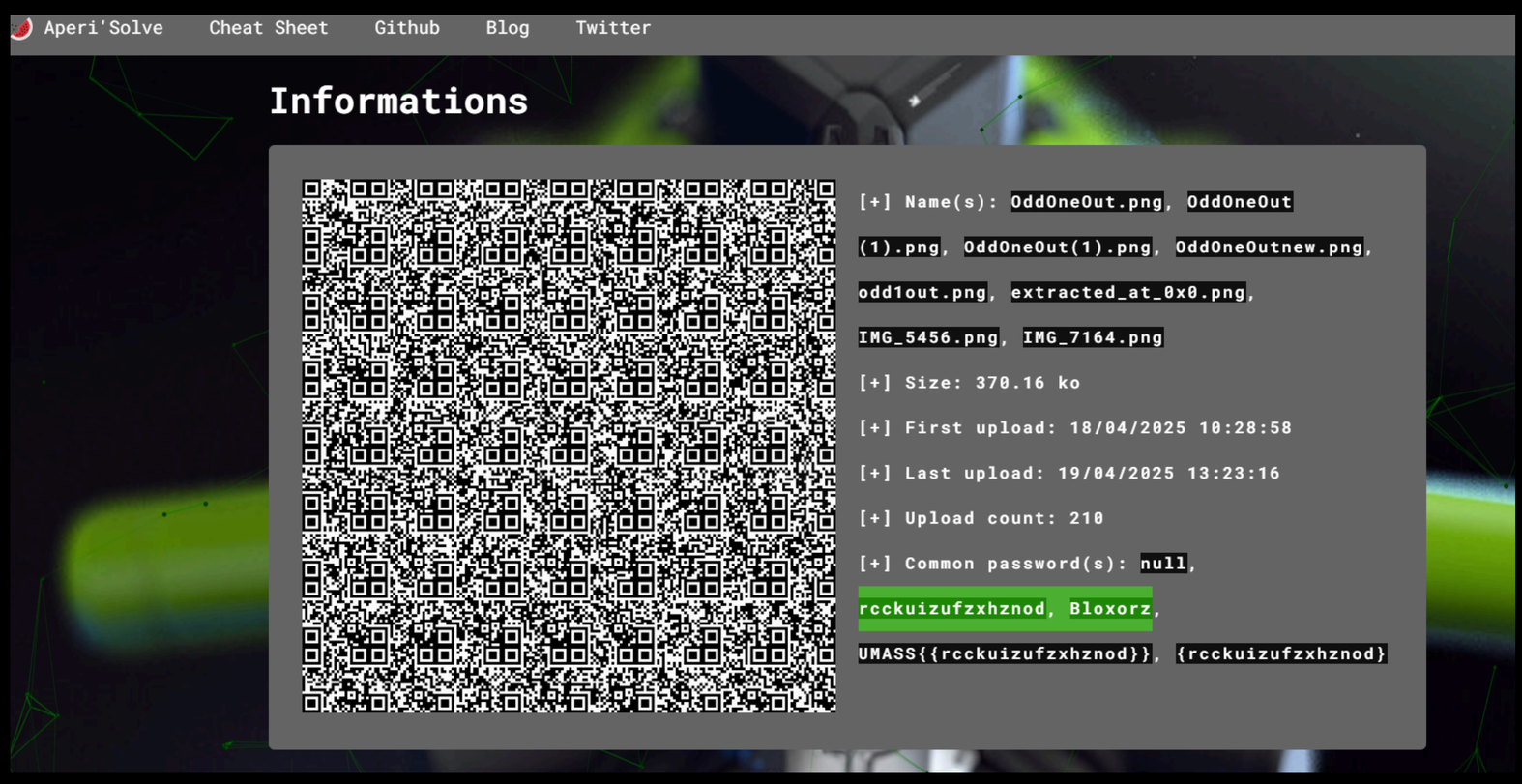
The **UMass Cybersecurity Club** organizes **UMassCTF 2025**, a global cybersecurity competition featuring challenges in web exploitation, cryptography, reverse engineering, and more. They aim to provide an engaging learning experience with expert talks, networking opportunities, and exciting prizes. Here’s How i solved Some of the challanges...

1.ODD ONE OUT:🚀

This **Steganography + Cryptography** challenge presents an image packed with multiple QR codes. Let’s break it down step by step:
First, I uploaded the image to Aperi'Solve website **(https://www.aperisolve.com)**, a powerful tool for analyzing hidden image data. This revealed a hash along with a key



The hash looked suspiciously like it was encrypted using the Vigenère cipher, a classic encryption technique.

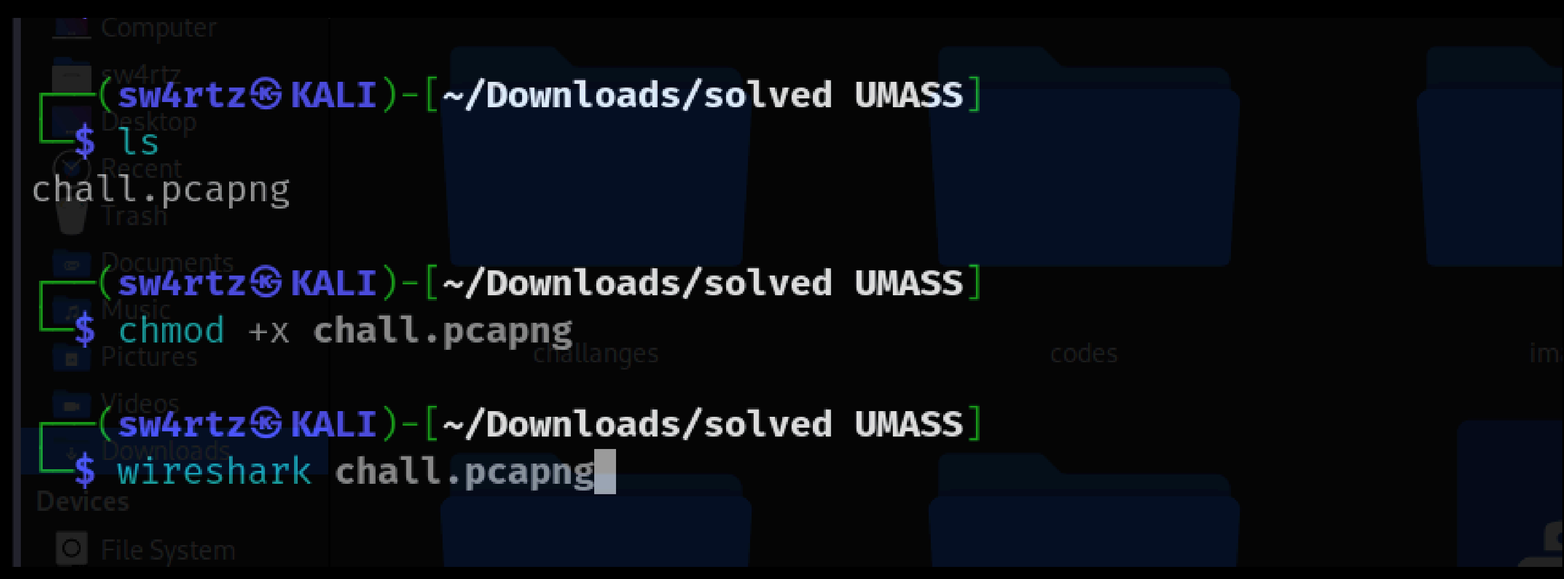


Decrypting the Flag Using DCode's Vigenère Cipher Solver **(https://www.dcode.fr/vigenere-cipher)**, I decrypted the hash using the key provided by Aperi'Solve. Boom! The flag was revealed!

FLAG: UMASS{QRONGRATULATIONS}

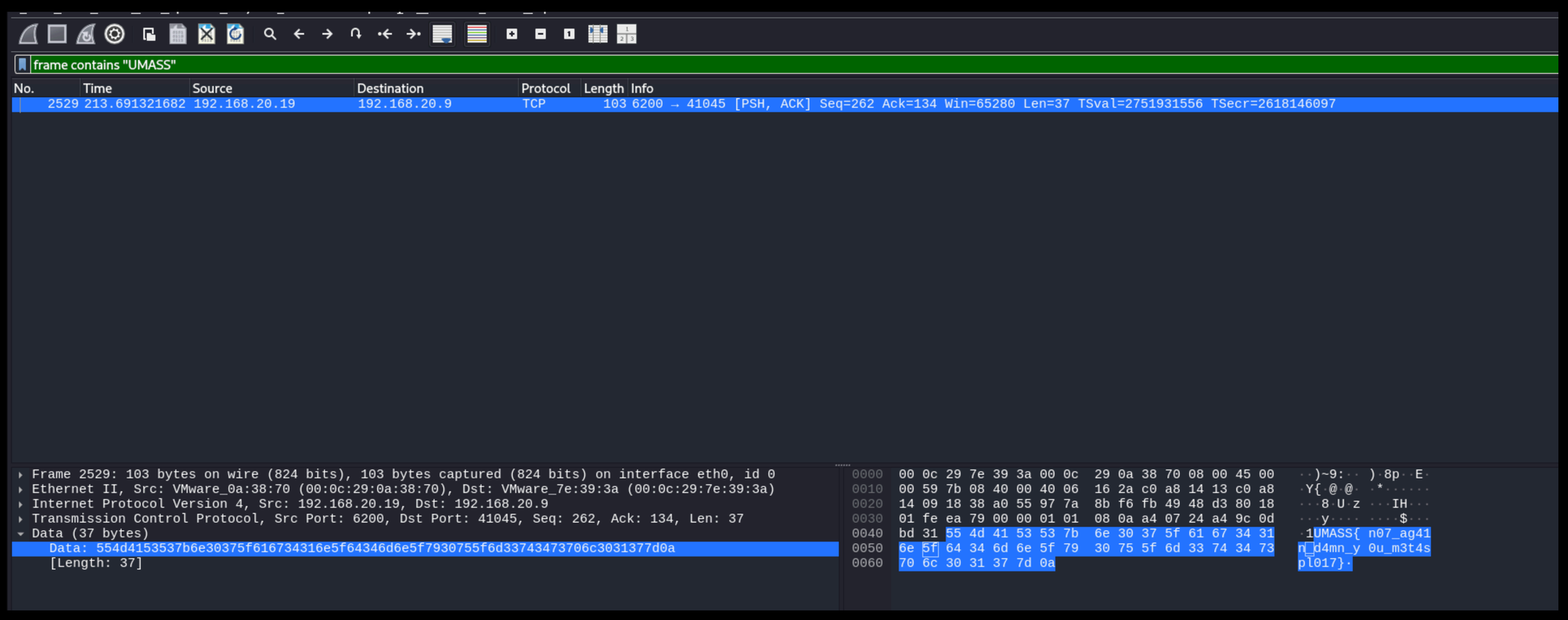
2.CHALL2:🚀

Making the File Usable I started by modifying the file's permissions with **chmod +x chall.pcapng**, allowing it to be executed or properly read. With that, it was ready for deeper analysis!



Next Step With the file accessible, I loaded it into **Wireshark**, a powerful network analysis tool, and applied the filter **frame contains "UMASS"**, which pinpointed a relevant packet—

Boom! The flag was revealed!



FLAG: UMASSCTF{07_AG41N_1N_4NOTH3R_7CP_M3SS4G3}

"Two halls uncovered, yet the path of learning stretches infinitely ahead—
every solved challenge fuels the fire to conquer more."