**PACKET ANALYZING USING WIRESHARK**

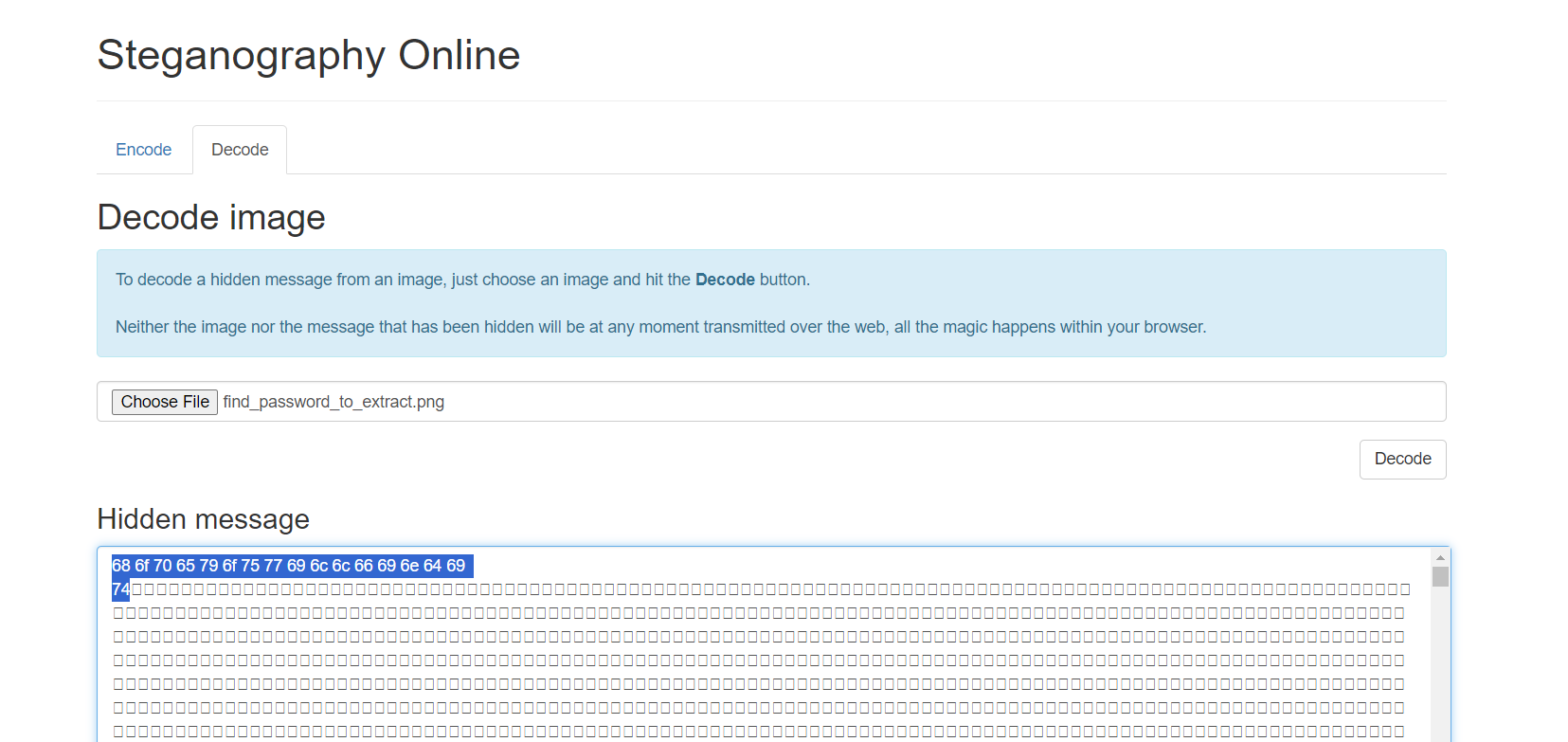
This task basically focused on extracting the user and the password entered by the malicious user.

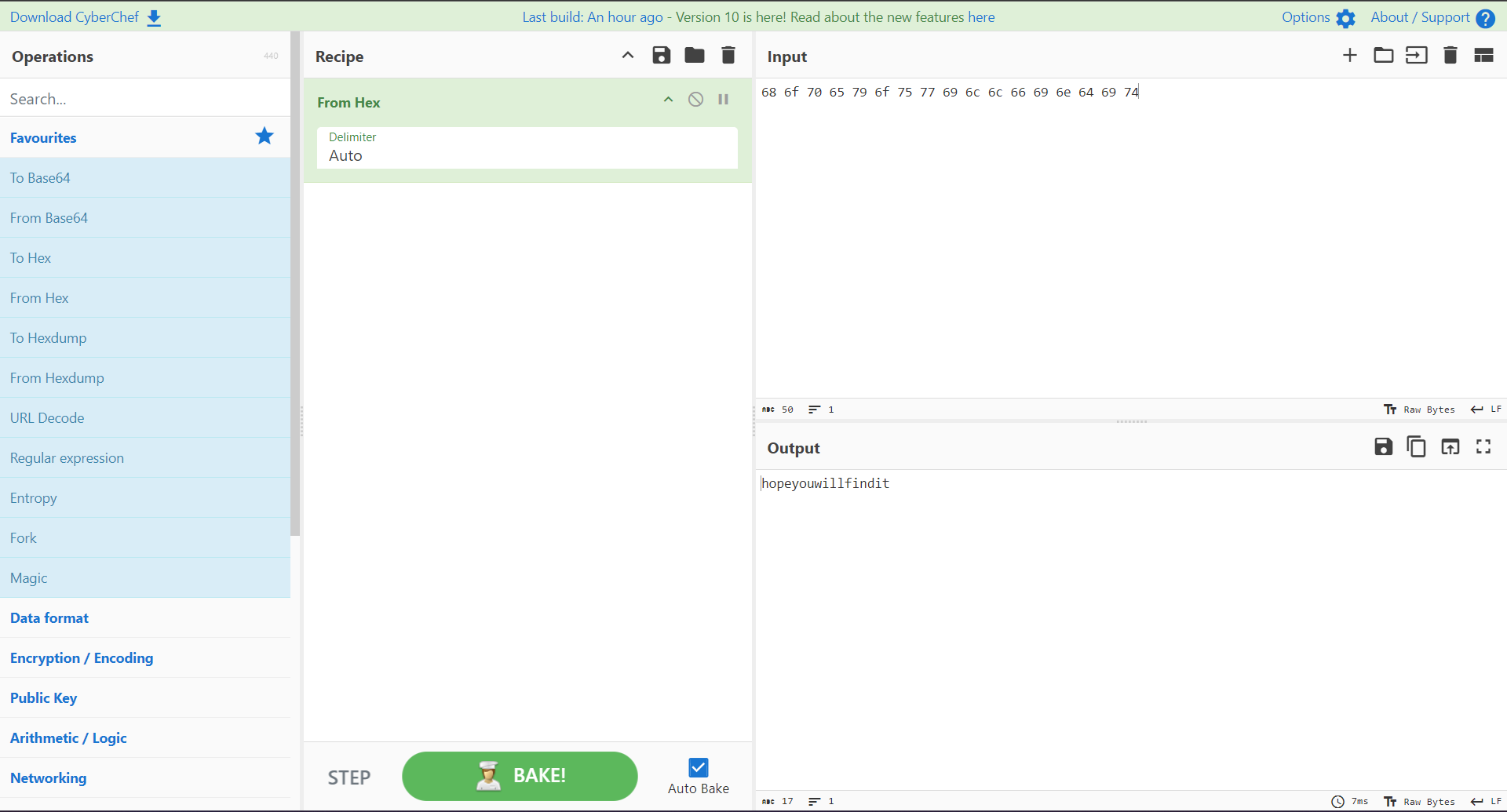
A .pcap file was provided to capture traffic of the malicious activity, the password for the zipped file was hidden in an image using steganography.

Steganography is a way of hiding information inside other files, like images or audio, so that the hidden message is not obvious. Instead of making the message unreadable, like encryption does, steganography hides the fact that there's a secret message at all. For example, you might hide a secret note in a picture file in such a way that nobody can see the note just by looking at the picture. This is the method that is used in this task as well. This technique is used to keep messages private and unnoticed.

The image is added in an online steganography tool to get the hex code then the hex code is decrypted to a text using CyberChef to finally get the password for the zipped file.

CyberChef allows users to perform various data manipulation tasks, particularly in the fields of cybersecurity and digital forensics. Particularly in this task, it was used to perform steganographic operations, such as hiding or extracting data from images.

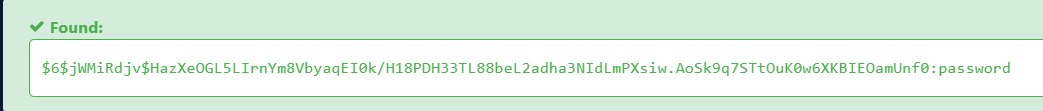




So the password for the zipped file is **“hopeyouwillfindit”**



The user is **“marcelle”** and for the password the hash code needs to be encrypted



Hence the password is **“password”**.

USER: marcelle

PASSWORD: password