



Capture The Flag (CTF)  
Wargames.my 2021

**05/Dec/2021 - 06/Dec/2021**

**Here we present to you**

**WRITE-UP**

**BY Dilettante**

# FORENSIC

The screenshot shows the MG MY challenge interface. On the left, there's a sidebar with categories like 'forensic' (50 points), 'C2 Hostname' (436 points), 'DGA Algorithms' (499 points), and 'cryptography' (easyrsa 176 points). The main content area displays the 'Forensic' challenge with a score of 50. It includes a message from the Security Team about a triggered alert, mentioning the collection of artifacts related to a malicious email. It also notes that the team hasn't understood the threat or security implications yet. Attached is a password-protected zip file. Below the message is a note about running the malware in a VM. At the bottom, there's a 'Flag' input field and a 'Submit' button.

In this challenge we used “foremost” to extract the artifact.zip file, then we got the .eml file. We used cyberchef to get the hash value of the file.

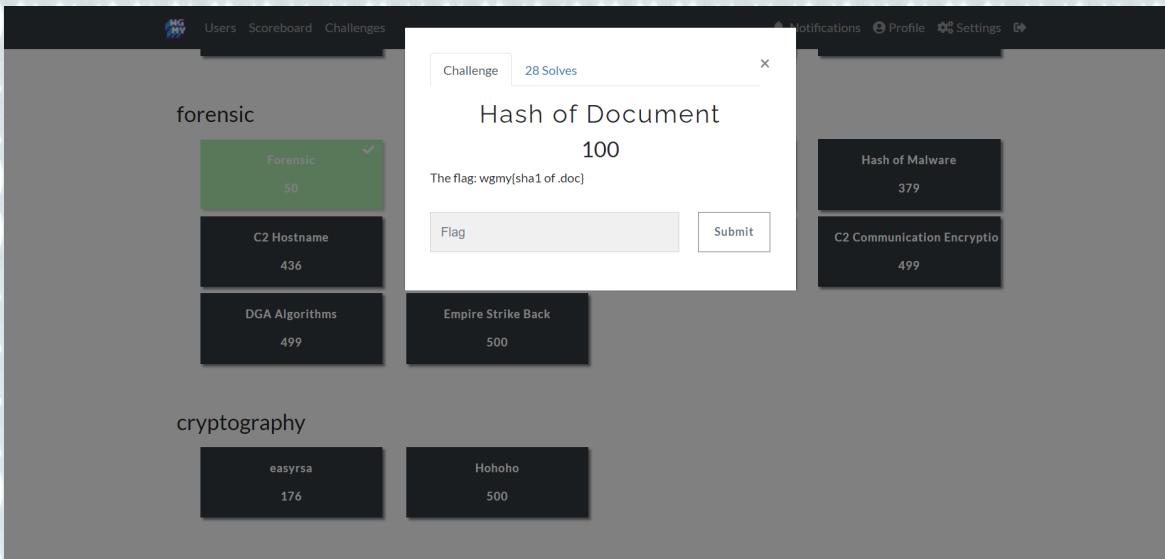
The screenshot shows the CyberChef interface. In the 'Operations' panel on the left, 'sha' is selected. Under 'Recipe', 'SHA2' is chosen with 'Size' set to '256' and 'Rounds' set to '64'. In the 'Input' panel, a file icon is shown with the following details: Name: [Job Application] Security E..., Size: 143,608 bytes, Type: message/rfc822, Loaded: 100%. In the 'Output' panel, the resulting hash is displayed as f4053a1aca84638b565c5f941a21b9484772520d7536e31ca41de0deaee14e2c.

Flag:

wgmy{f4053a1aca84638b565c5f941a21b9484772520d7536e31ca41de0deaee

14e2c}

# HASH OF DOCUMENT

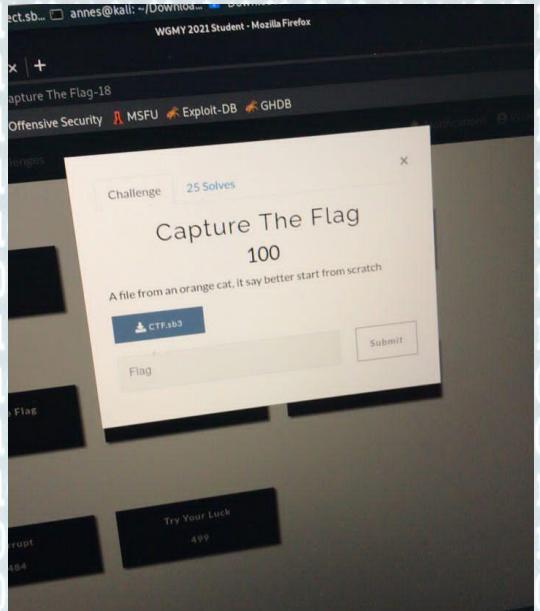


We opened and saved the doc file.

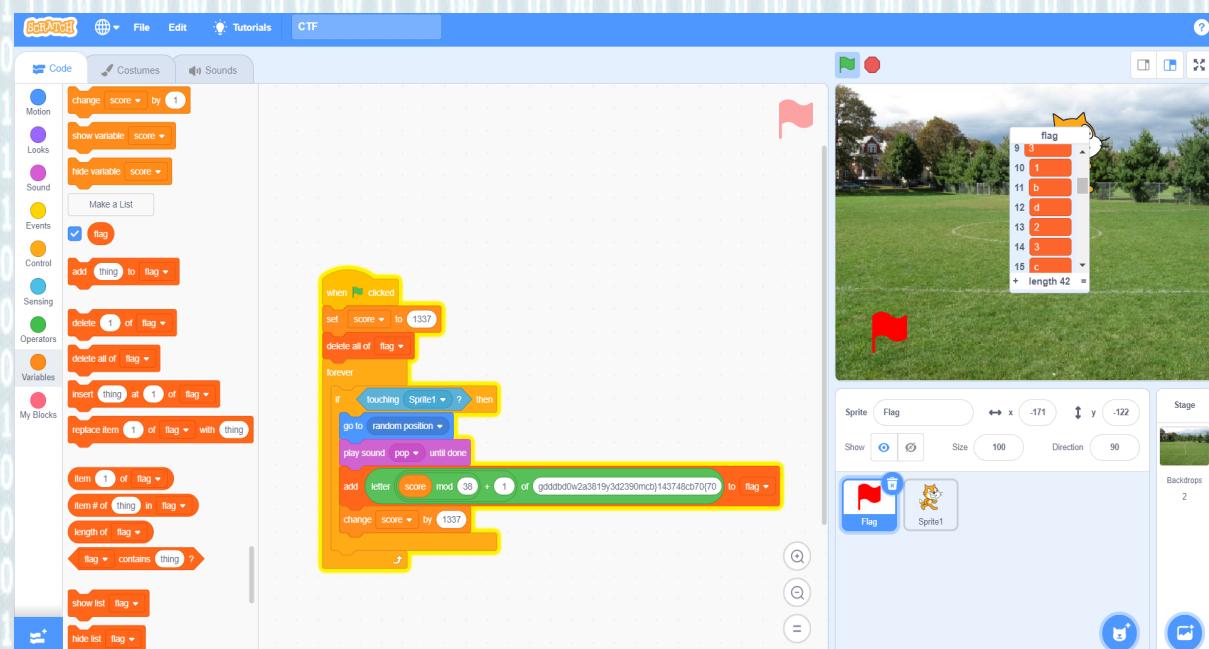
Then, we used cyberchef to hash the doc file using SHA-1 hash.

Flag: **wgm{706301fc19042ffcab697775c30fe7dd9db4c5a6}**

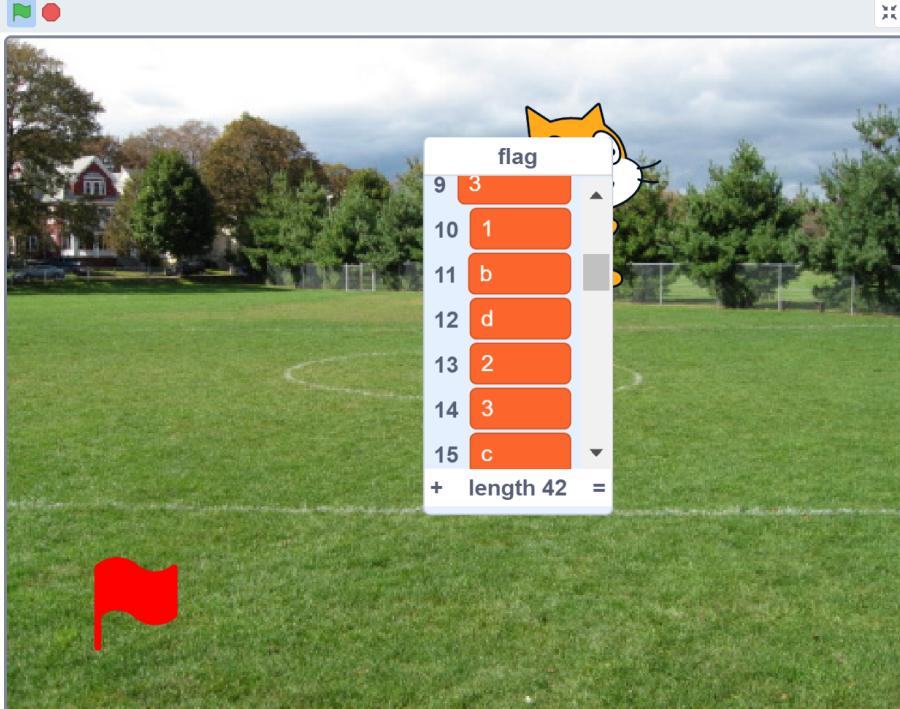
# CAPTURE THE FLAG



The file above is a Scratch file.



When we opened the file in Scratch, it displayed like this. In the Code tab, we clicked on the Variable and checked at 'flag'. Then we could see a table named flag pops up.



When we moved the cat around to get the flag, the scores were entered in the flag table. There , we got the answer.

Flag: **wgmy{78b13db324cd79174adb089030d023c}**