Then I started doing the tasks:TASK1 was just to click submit

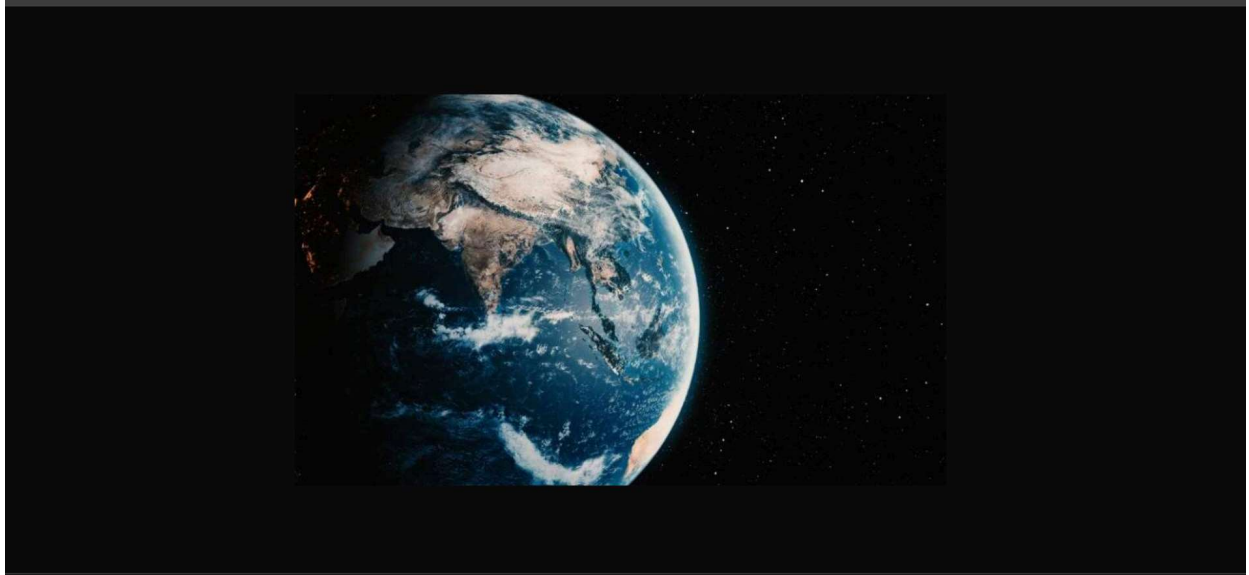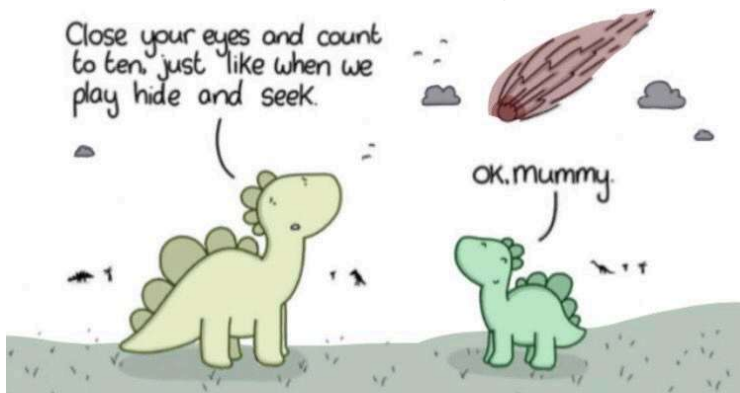Task 2 was to decode the base 64string I used an online converter

The third task was to decode the following file:

Task 4:I used exif tool and decoded the key

I used steghide to decode it and grep

Task 5: I just tried copying the hidden part possible highlighting the hidden flag

Room completed (100%)

Task 4 ✅ Mon, are we going to be okay?

Task 5 ✅ Erm......Magick

Huh, where is the flag? THM{wh173_fl46}

Answer the questions below

Did you find the flag?

THM{wh173_fl46}   ✓ Correct Answer   💡 Hint

Task 6 ✅ QRrrrr

Task 7 ✅ Reverse it or read it?

Task 8 ✅ Another decoding stuff

Task 9 ✅ Left or right

TASK 6:I used QRscan and got the key
Task 7:decoded elf 64 binary using
Task 8:base 58 string decode
Task 9:ceaser cipher decoding using logic and online decoder

Room completed (100%)

Task 8 ✅ Another decoding stuff

Task 9 ✅ Left or right

Left, right, left, right... Rot 13 is too mainstream. Solve this

MAF{atbe_max_vtxltk}

Answer the questions below

What did you get?

THM{hail_the_caesar}   ✓ Correct Answer   💡 Hint
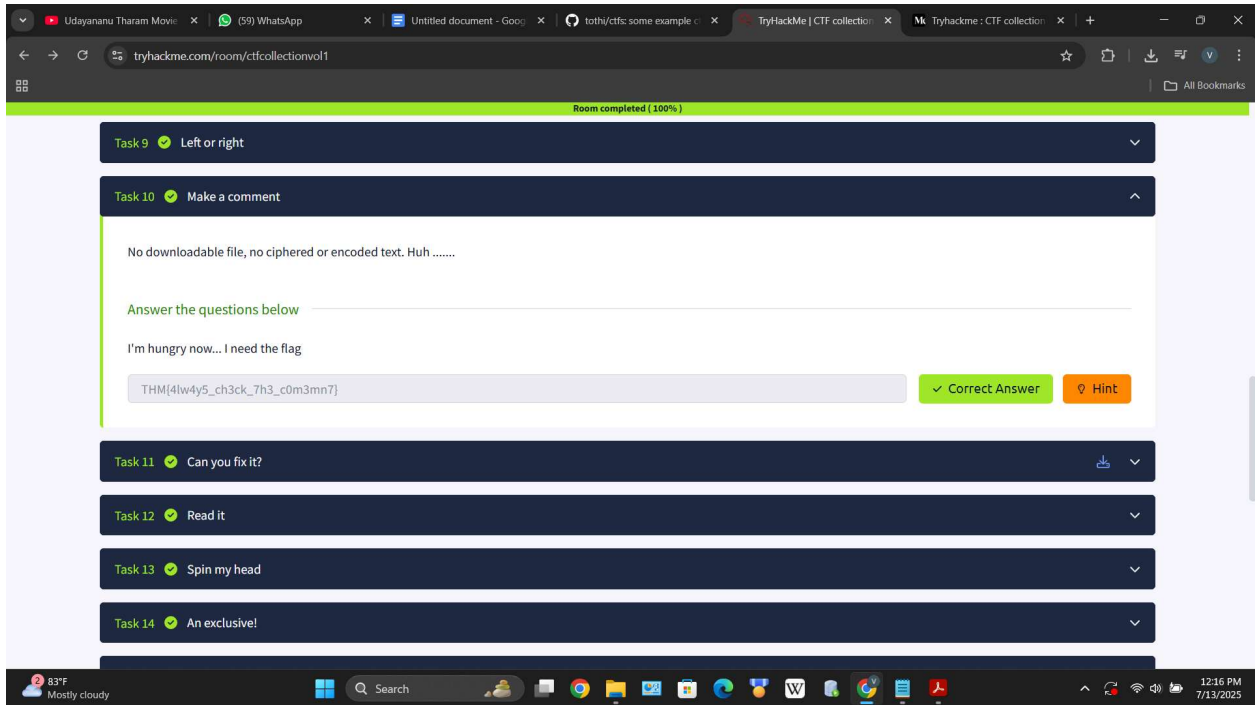
Task 10 ✅ Make a comment

Task 11 ✅ Can you fix it?

Task 12 ✅ Read it

Task 13 ✅ Spin my head
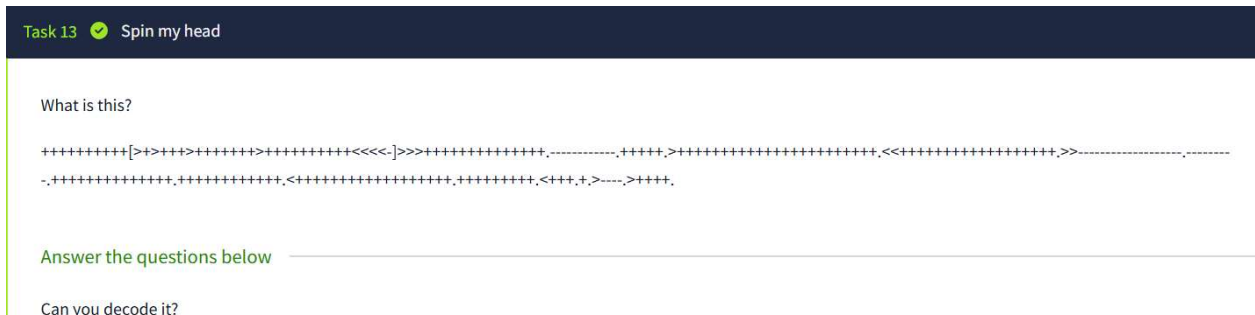
Task 10:INSPECTED

AND FOUND IN <P></P>

TASK 11:I decoded by analyzing with help of head

TASK 12:searched tryhackme room reddit flag

TASK13:decode the brainfuck ,note it is wrongly written as binaryfuck they are slightly different.

TASK 14:perform xor and set output to 256 ascii

Exclusive strings for everyone!

S1: 44585d6b2368737c65252166234f20626d
S2: 1010101010101010101010101010101010

Answer the questions below

Did you crack it? Feed me now!

THM{3xclu51v3_0r}

Task 15:decoded the file binwalk by converting it into zip file and unzipped it to get the key
TASK16:I decoded using stegsolve

| Full Red | Full Green | Full Blue | Inverse (RGB) | LSB Half |

| Extract Files/Data | Embed Files/Data | Embed B/W Image in Bit Plane |

| Show Strings | Show RGBA Values | Show PNG Info |

| Exit | Preload Bit Planes |

<< < Blue 1 > >>

THM{7h3r3_15_h0p3_1n_7h3_d4rkn355}

Task 17:a sounding qr redirecting to soundcloud ,key was of format THM{flag}
Task 18:GO TO INTERNETARCHIVES ,FILTER THE URL ,SET DATE AS REQUIRED YOU CAN FIND IT EASILY

Sometimes we need a 'machine' to dig the past

Targetted website: https://www.embeddedhacker.com/
Targetted time: 2 January 2020

Answer the questions below

Did you found my past?

TASK 19:USED VIGENERE CIPHER ,SET KEY AS THM AND DECODED
MYKAHODTQ{RVG_YVGGK_FAL_WXF}
Flag format: TRYHACKME{FLAG IN ALL CAP}

TASK 20:converted decimal
581695969015253365094191591547859387620042736036246486373595515576333 6
93 to hex and then ascii
TASK 21:uploaded the .pcapng file to wireshark and set filter https request ==get filter
and opened the stream to find the decoded flag