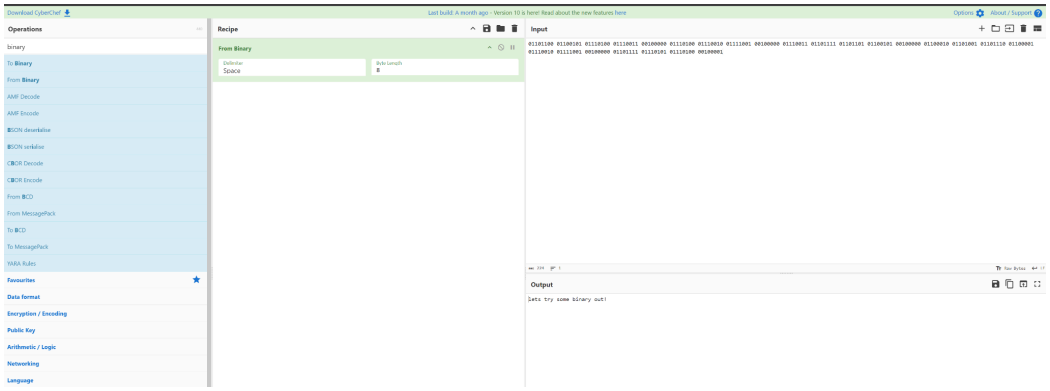
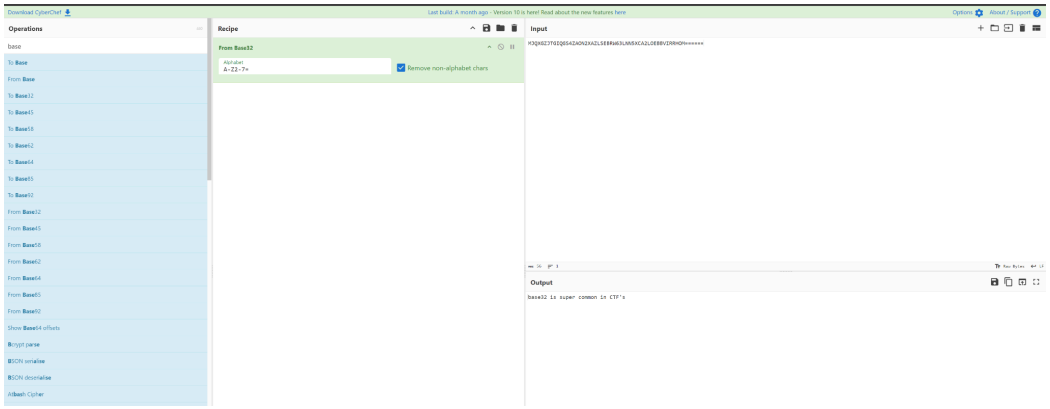
Stick-Cmd c4ptur3-th3-fl4g Project journal

Date: 09-20-2024	**Entry: 001**
Description	We are given encryption to decode, c4n y0u c4p7u23 7h3 f149?
Tool(s) used	No tools needed except basic logic.
Details	• **Who**: TryHackMe Practice Room • **What**: Decryption of the provided encrypted phrases • **Why**: To gain real world experience with encryption and decryption methods
Additional notes	

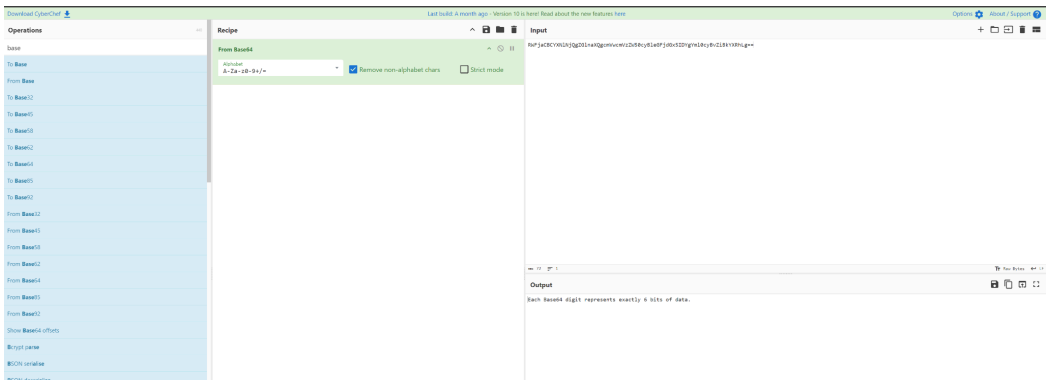
Date: 09-20-2024	**Entry: 002**
Description	Decrypt the binary - 01101100 01100101 01110100 01110011 00100000 01110100 01110010 01111001 00100000 01110011 01101111 01101101 01100101 00100000 01100010 01101001 01101110 01100001 01110010 01111001 00100000 01101111 01110101 01110100 00100001

Tool(s) used	Used an online app called CyberChef: https://gchq.github.io/CyberChef/
Details	 In the CyberChef tool you have to make sure to search 'From Binary' as the output setting to get the answer.
Additional notes	

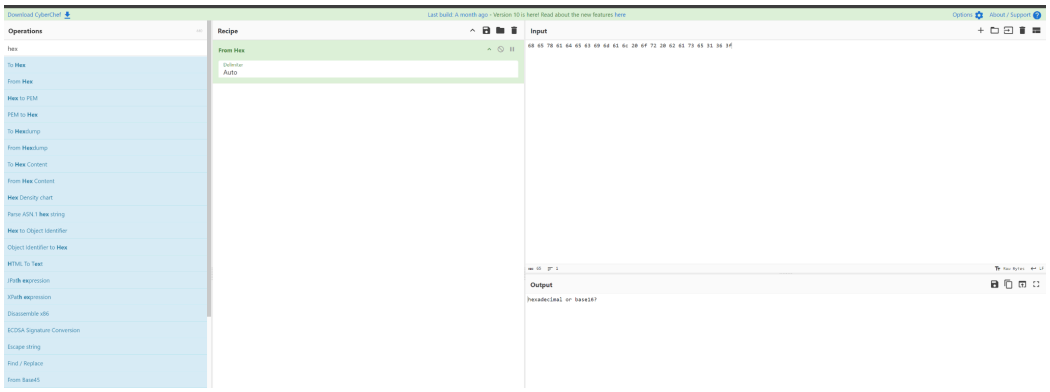
Date: 09-20-2024	**Entry: 003**
Description	Decode the Encryption - MJQXGZJTGIQGS4ZAON2XAZLSEBRW63LNN5XCA2LOEBBVIRRHOM======
Tool(s) used	Google Search, CyberChef

Details	 In order to get the answer I first needed the type of encryption, which Google helped with. I then set the output of CyberChef to'From Base32' as this will provide the answer.

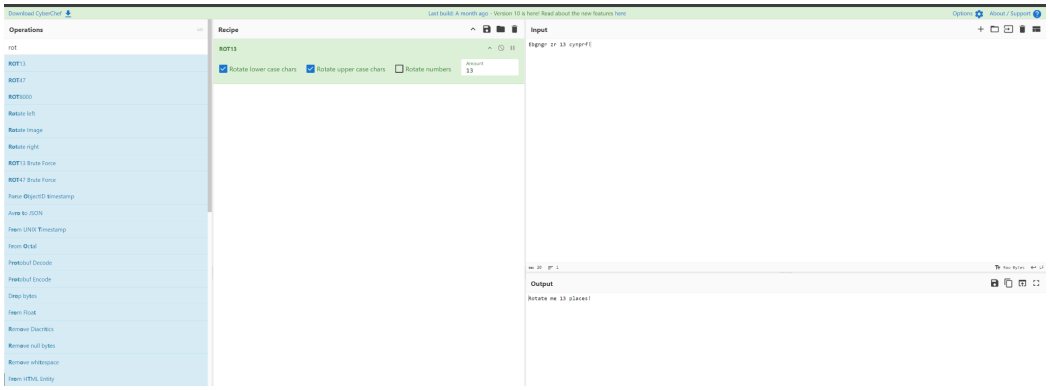
Date: 09-20-2024	**Entry: 004**
Description	Decode the phrase - RWFjaCBCYXNlNjQgZGlnaXQgcmVwcmVzZW50cyBleGFjdGx5IDYgYml0cyBvZiBkYXRhLg==
Tool(s) used	Google Search, CyberChef

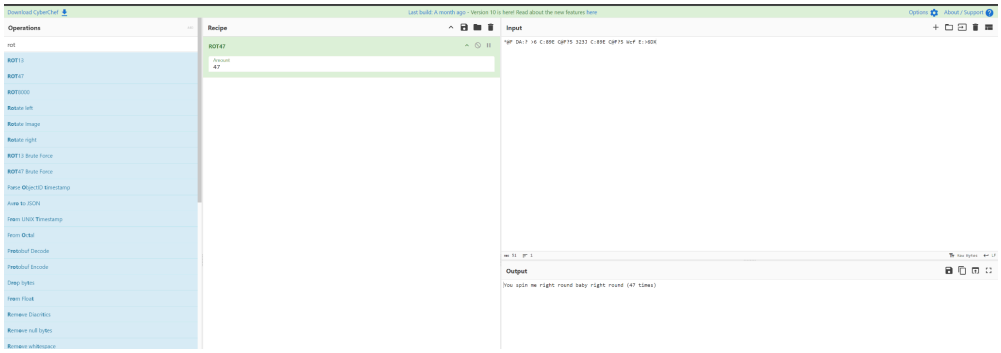
Details	 From google we learn that this encryption is Base64. So in CyberChef I set the Recipe to ‘From Base64’ to get out answer.
Additional notes	

Date: 09-20-2024	**Entry: 005**
Description	Decode - 68 65 78 61 64 65 63 69 6d 61 6c 20 6f 72 20 62 61 73 65 31 36 3f
Tool(s) used	Google, CyberChef

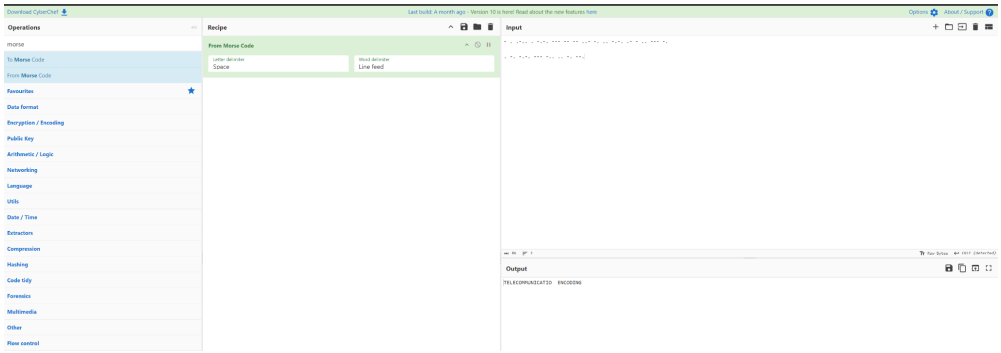
Details	 After a google search we learn that this encryption is hexadecimal. From here we can now get the answer in CyberChef.
Additional notes	

Date: 09-20-2024	**Entry: 006**
Description	Decrypt - Ebgngr zr 13 cynprf!
Tool(s) used	Google Search, CyberChef

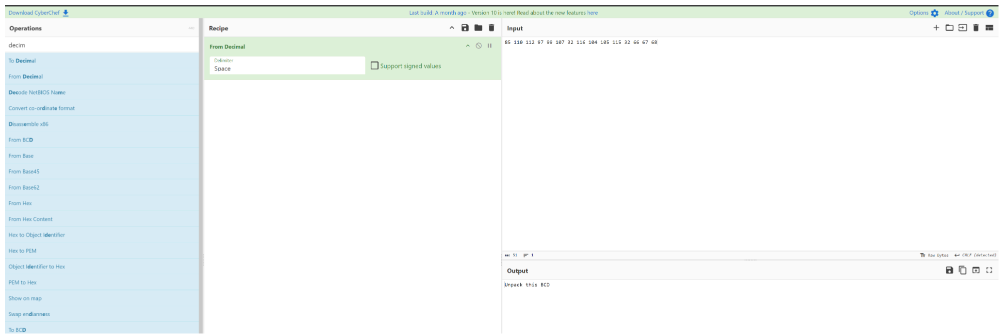
Details	 A simple google search indicates this encryption is ROT13. So we enter that into CyberChef and we can get our answer.
Additional notes	

Date: 09-20-2024	**Entry: 007**
Description	Decrypt - *@F DA:? >6 C:89E C@F?5 323J C:89E C@F?5 Wcf E:>6DX
Tool(s) used	Google Search, CyberChef
Details	 Again, a simple Google Search and then put the encryption type of ROT47 into CyberChef.

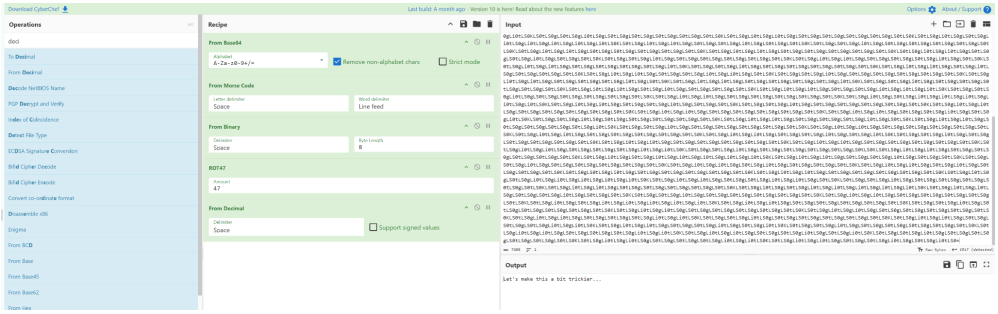
Additional notes	

Date: 09-20-2024	**Entry: 008**
Description	Decrypt - - . .-.. . -.-. --- -- -- ..- -. .. -.-. .- - .. --- -. . -. -.-. --- -.. .. -. --.
Tool(s) used	Google Search, CyberChef
Details	 Same situation as the last entries, only this time we are dealing with Morse Code.
Additional notes	

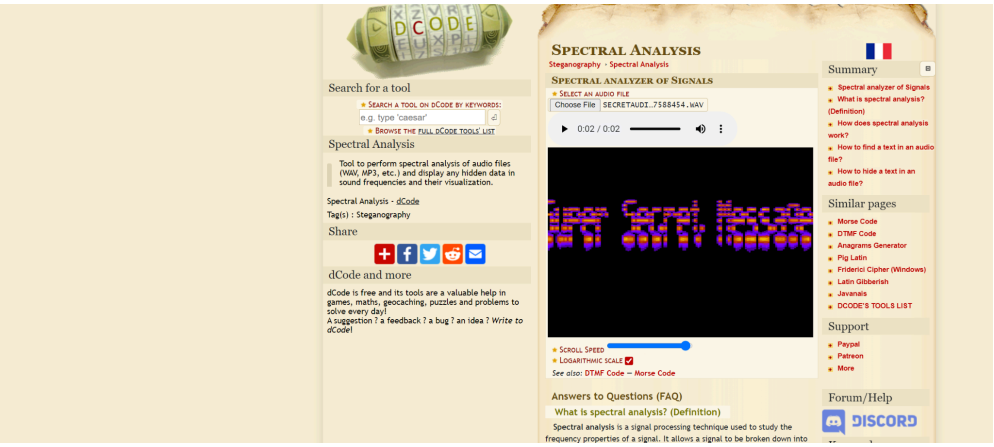
Date:	**Entry: 009**

09-20-2024	
Description	Decrypt - 85 110 112 97 99 107 32 116 104 105 115 32 66 67 68
Tool(s) used	Google Search, CyberChef
Details	 Same as the other entries only now we are dealing with Decimal.
Additional notes	

Date: 09-20-2024	**Entry: 010**
Description	Decrypt - LS0tLS0gLi0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLi0tLS0gLi0tLS0gLS0tLS0KLS0tLS0gLi0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLi0tLS0gLS0tLS0gLi0tLS0KLS0tLS0gLS0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0KLS0tLS0gLi0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0KLS0tLS0gLi0tLS0gLS0tLS0gLi0tLS0gLi0tLS0gLi0tLS0gLi0tLS0KLS0tLS0gLi0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0KLS0tLS0gLS0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0KLS0tLS0gLi0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0KLS0tLS0gLi0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLi0tLS0gLS0tLS0gLi0tLS0KLS0tLS0gLS0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0KLS0tLS0gLi0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLi0tLS0gLS0tLS0KLS0tLS0gLi0tLS0gLi0tLS0gLS0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0KLS0tLS0gLS0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0KLS0tLS0gLi0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0KLS0tLS0gLi0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLi0tLS0gLS0tLS0KLS0tLS0gLS0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0KLS0tLS0gLi0tLS0gLS0tLS0gLi0tLS0gLi0tLS0gLi0tLS0gLi0tLS0gLi0tLS0KLS0tLS0gLi0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLi0tLS0gLi0tLS0gLS0tLS0KLS0tLS0gLS0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0KLS0tLS0gLi0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLi0tLS0KLS0tLS0gLS0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0KLS0tLS0gLi0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0KLS0tLS0gLi0tLS0gLS0tLS0gLi0tLS0gLi0tLS0gLi0tLS0gLi0tLS0gLi0tLS0KLS0tLS0gLi0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLi0tLS0gLi0tLS0KLS0tLS0gLS0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0KLS0tLS0gLi0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0KLS0tLS0gLi0tLS0gLS0tLS0gLi0tLS0gLi0tLS0gLi0tLS0gLi0tLS0gLi0tLS0KLS0tLS0gLi0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLi0tLS0gLS0tLS0gLS0tLS0KLS0tLS0gLS0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0KLS0tLS0gLi0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLi0tLS0KLS0tLS0gLS0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0KLS0tLS0gLi0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0KLS0tLS0gLi0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLi0tLS0gLS0tLS0gLS0tLS0KLS0tLS0gLS0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0KLS0tLS0gLi0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0KLS0tLS0gLi0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLi0tLS0gLS0tLS0gLS0tLS0KLS0tLS0gLS0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0KLS0tLS0gLi0tLS0gLi0tLS0gLS0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0KLS0tLS0gLS0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0KLS0tLS0gLi0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0KLS0tLS0gLi0tLS0gLS0tLS0gLi0tLS0gLi0tLS0gLi0tLS0gLi0tLS0gLi0tLS0KLS0tLS0gLi0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLi0tLS0gLS0tLS0KLS0tLS0gLS0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0KLS0tLS0gLi0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLi0tLS0gLi0tLS0KLS0tLS0gLS0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0KLS0tLS0gLi0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLi0tLS0gLi0tLS0KLS0tLS0gLi0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLi0tLS0gLS0tLS0gLi0tLS0KLS0tLS0gLS0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0KLS0tLS0gLi0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLi0tLS0gLi0tLS0KLS0tLS0gLi0tLS0gLi0tLS0gLS0tLS0gLS0tLS0gLS0tLS0gLi0tLS0gLS0tLS0gLi0tLS0=

Tool(s) used	Google Search, CyberChef
Details	This one is a doozy. First we have to assume the encryption is in Base64 due to upper and lower case letters. Next we get Morse code in CyberChef. From here CyberChef outputs a Binary code which outputs a ROT47 code. Next and finally the ROT47 code outputs to decimal. We get our answer from here. 
Additional notes	

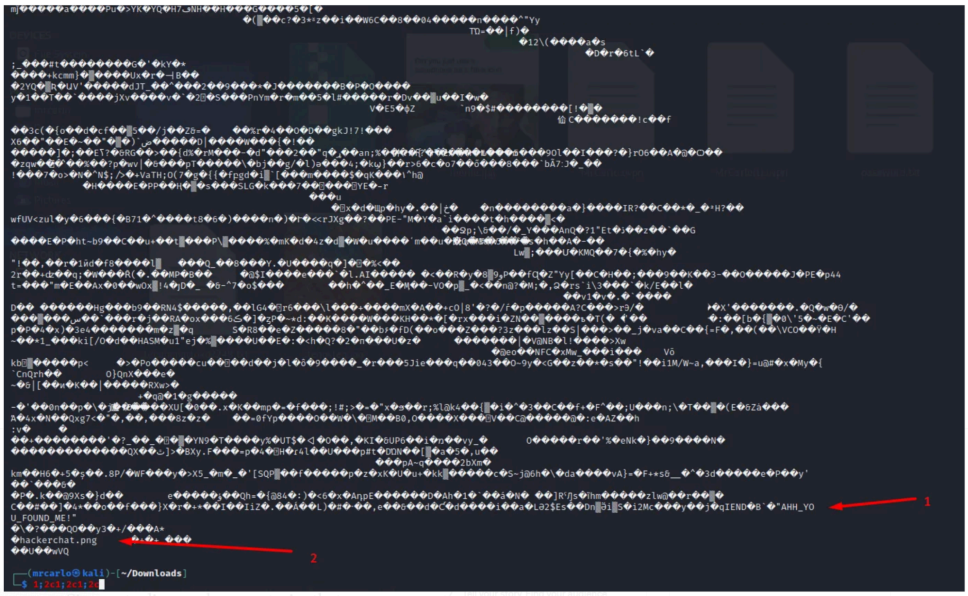
Date: 09-20-2024	**Entry: 011**
Description	This next task we have to decode a Spectrogram. This is an audio file that we have to download.
Tool(s) used	Google Search, dcode.fr
Details	I am using google search to see the best way to decode a Spectrogram. I found the website dcode.fr/spectral-analysis. Once here I chose to upload

	the file that was given to us in the task. I increased the Scroll speed and played back the file. The visual waves presented - 
Additional notes	

Date: 09-20-2024	**Entry: 012**
Description	Decrypt the Steganography pic to get the Flag.
Tool(s) used	Kali Linux and Steghide
Details	First we had to download the picture in the task. We then opened up our terminal in Kali Linux and with the command steghide extract -sf /home/kali/Downloads/stegosteg.jpg we were able to get the text ‘steganopayload2248.txt’. Opening this txt file in our terminal gave us the

	flag. 
Additional notes	

Date: 09-20-2024	**Entry: 013**
Description	Decrypt meme.jpg and find the two flags ‘INSIDE’ the file.
Tool(s) used	Kali Linux, Terminal
Details	After downloading the image file, this was an easy one. All I had to do was enter the command in the terminal: cat meme.jpg. From here we were able

	to see both flags. 
Additional notes	At first I treated this task as another Steganography image. I overthought it and should of just took things one step at a time.

Reflections/Notes: This room was great at teaching the ins and outs of encryption. I am sure this will be useful for later rooms.