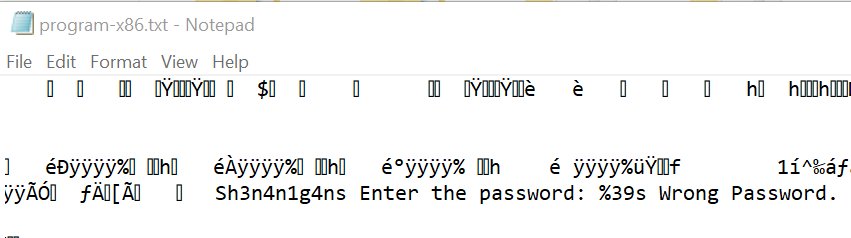
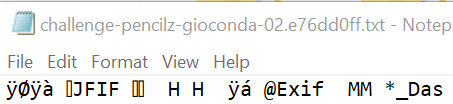
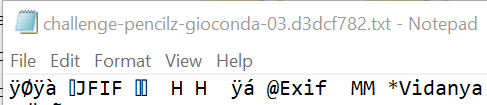
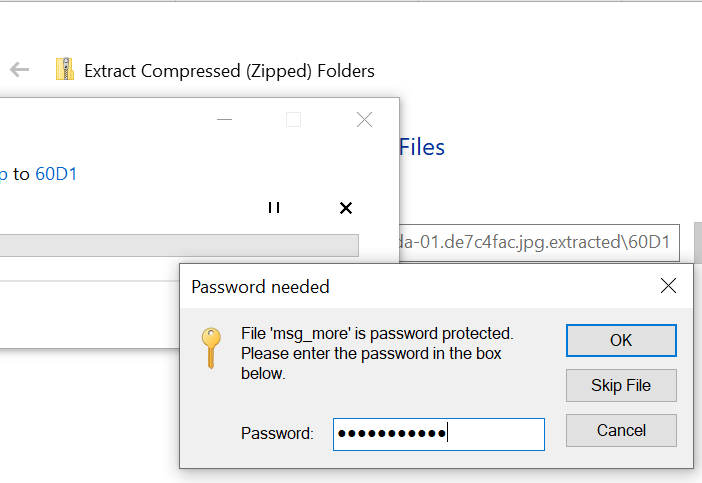
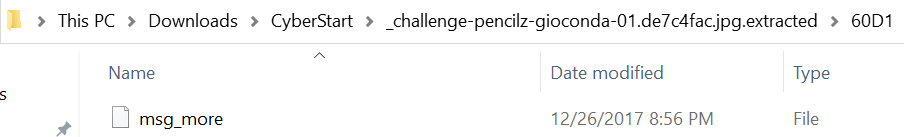
Tayga Bears ( ←Name of Challenge)

1. Binwalk extract Bear 6

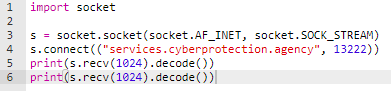
Cold File ( ←Name of Challenge)

1. Change program to .txt
2. Password is next to “Enter the password: ” (Sh3n4n1g4ns)
3. Change program back to original type (remove the .txt)
4. Chmod +x the program
5. Open the program and put in the password
6. 

Perilous Pencils ( ←Name of Challenge)

1. Binwalk extract Pencil 1
2. Change the other pencils to .txt
3. The password to the zip file is the words in the first line of the files combined (Vidanya\_Das)
4. Execute the program in the unzipped folder
5. 
6. 
7. 
8. 

Silver Service

1. <https://trinket.io/embed/python3>
2. 
3. Cipher mode = CBC, key size = 256,

Brazilian Blather ( ←Name of Challenge)

1. Download and import the pcapng file into Wireshark
2. Filter for POP protocol
3. Right click any packet and Follow > TCP Stream
4. Scroll down the bottom with the gzip file encoded in Base64
5. Decode and export the Base64 to a gzip file
6. Unzip the file and run the executable inside
7. Above the gzip block is the question in HTML code
   1. What year did AMD release the K6 Processor?