This is the super sensitive, confidential document that was affected by the ransomware. Congratulations on the bruteforce!

You can paste your bruteforce script in the box below:

|  |
| --- |
| '''  Forage AIG Cybersecurity Program  Bruteforce starter template  '''  from zipfile import ZipFile  # Use a method to attempt to extract the zip file with a given password  def attempt\_extract(zf\_handle, password):  zf\_handle.extractall(pwd=password.encode('ascii'))  def main():  print("[+] Beginning bruteforce ")  extracted = False  with ZipFile('enc.zip') as zf:  with open('rockyou.txt', 'rb') as f:  # Iterate through password entries in rockyou.txt  pwds = (f.read().decode('ascii')).split('\n')  for pwd in pwds:  # Attempt to extract the zip file using each password  try:  attempt\_extract(zf, pwd)  extracted = True  # Handle correct password extract versus incorrect password attempt)  except RuntimeError as e:  pass  if not extracted:  print("[+] Password not found in list")  if \_\_name\_\_ == "\_\_main\_\_":  main() |