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  def attempt\_extract(zf\_handle, password):  try:  zf\_handle.extractall(pwd=password.encode())  return True  except Exception as e:  return False  def main():  print("[+] Beginning bruteforce")  with ZipFile('enc.zip') as zf:  with open('./rockyou.txt', 'r', errors='ignore') as f:  # Iterate through password entries in rockyou.txt  for line in f:  password = line.strip()  # Attempt to extract the zip file using each password  if attempt\_extract(zf, password):  print(f"[+] Password found: {password}")  break  else:  print(f"[-] Incorrect password: {password}")  print("[+] Password not found in list")  if \_\_name\_\_ == "\_\_main\_\_":  main() |