CSCI 2303 PRINCIPLES OF IT SECURITY

CASE 06: MURDER

Group 12

INTRODUCTION

You are at a crime scene, which is the home of a suspected serial killer named **Jordan.** the chief police officer tells you that Jordan used his email to get the victim's list from an unknown friend. they also communicate by using hidden tactics known as **steganography** to hide the information.

By examining Jordan's laptop, you find out that there are many suspicious files and steganography installed on the laptop including **S-tools, Quick Stego, SNOW, and Oursecret.** there is one suspicious file named **Ahzore7.zip** saved on the computer Desktop.

Team

Yusuf Mohammad Yunus (2314467)

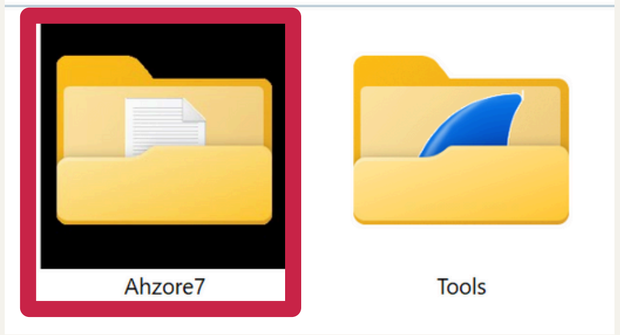
Huthifah (2229009)

Muhammad Fadhil (2222961)

Muhd Hadi Husaini (2316199)

WHITE HAT: FINDING EVIDENCE

Azhore7

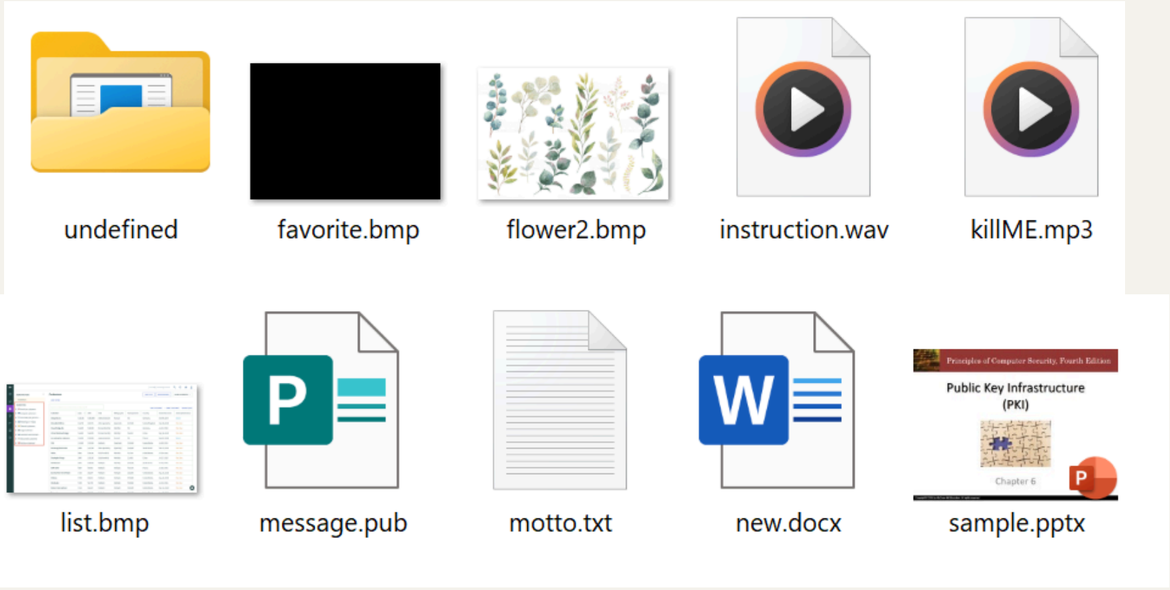


the file name when decode through rot cypher at Rot-N, where N =13 gave us two options:

- Number 4: If number is NOT rotated
- Number 7: If number is rotated

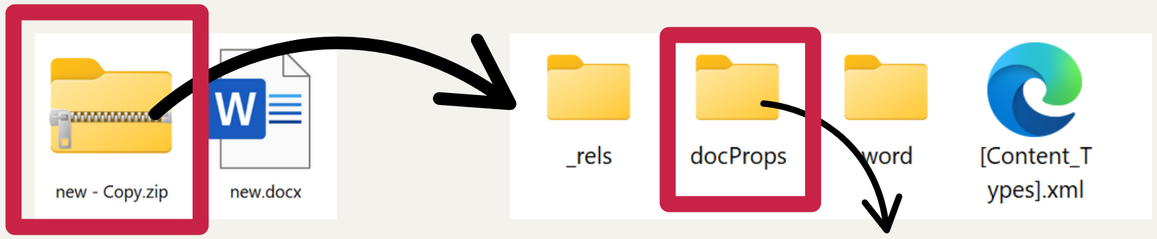
https://www.dcode.fr/rot-cipher

Inside Azhore7



there are total 10 different evidences

new.docs



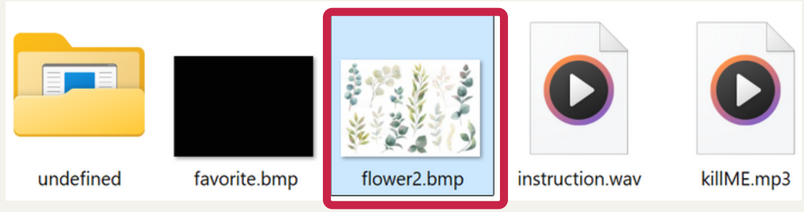
Upon converting new.docs to zip file and opening the core.xml file, we found out rot cypher text :

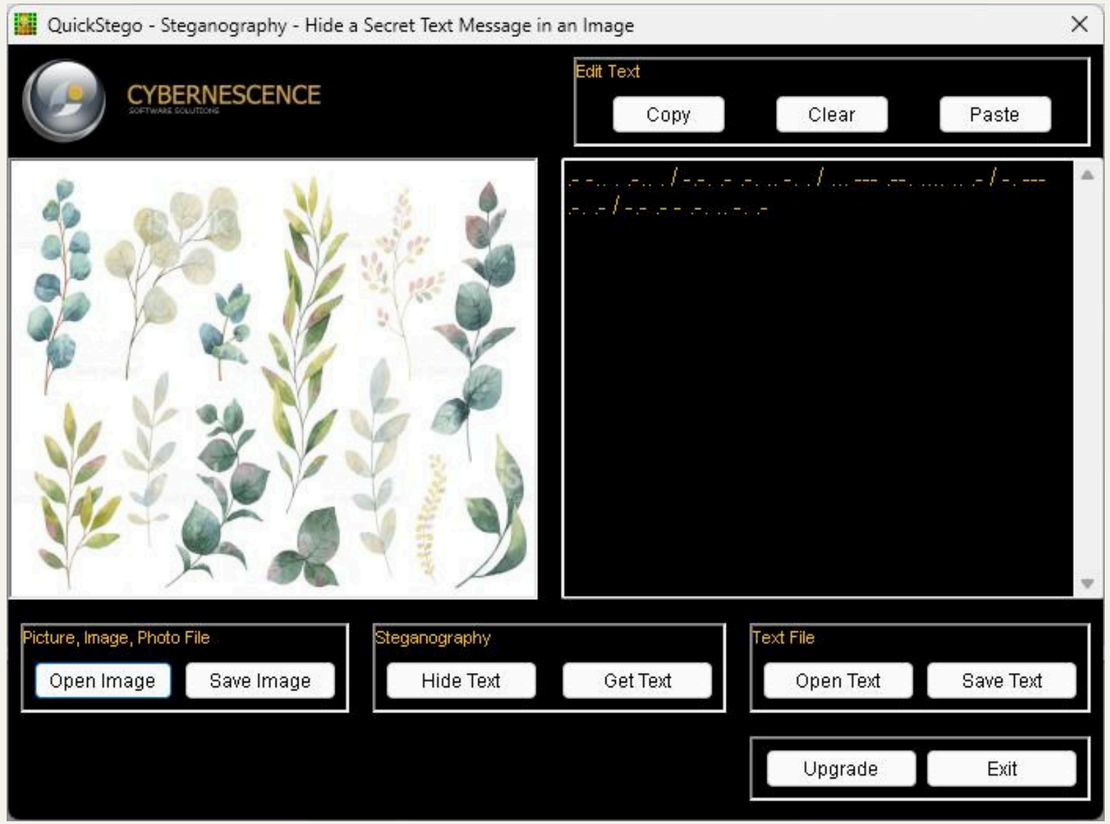
eee.pwebwsqtt.kwu

On rot-cypher:
[A-Z]+8=

www.howtokill.com

https://www.dcode.fr/rot-cipher





flower.bmp

upon decoding them through quickstego and S-tools we got the morsecode:

.- -... . .-.. . / -.-. .- .-. .. -. . / ... --- .--. ....- / -. --- .-. .- / -.- .- - .-. .. -. .-

Which upon decoding gives

using :morsecode.world/international/translator.html

DELE CARINE SOPHIA NORA KATRINA

Instruction.wav

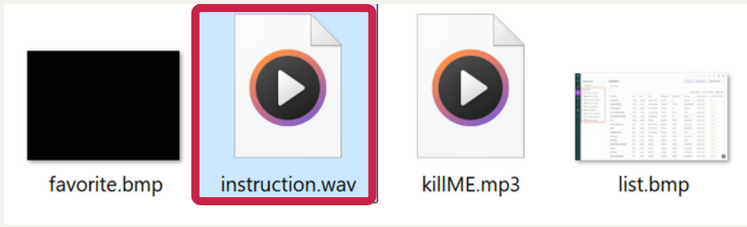
Upon decoding this file via mp3 stego and online"

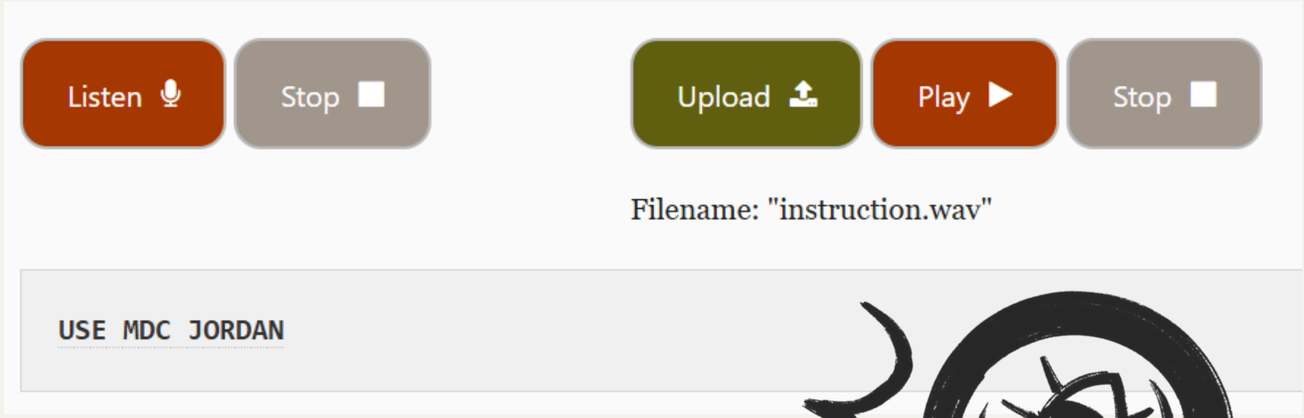
morsecode.world/international/decoder/audio-decoder-adaptive.html

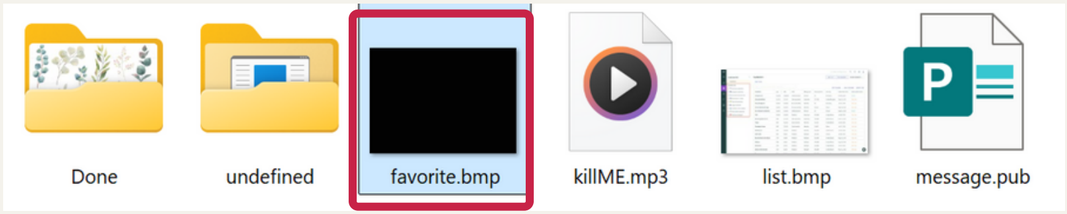
we got:

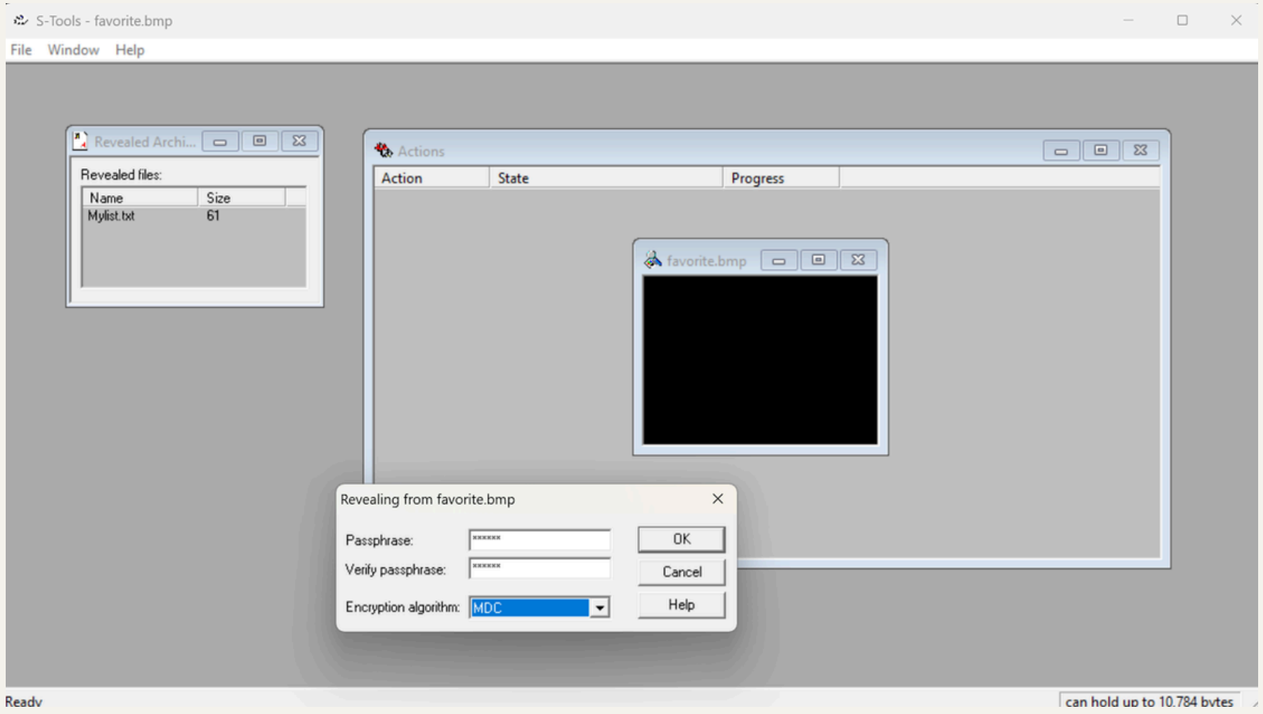
USE MDC JORDAN

(we used this in the next artifact)





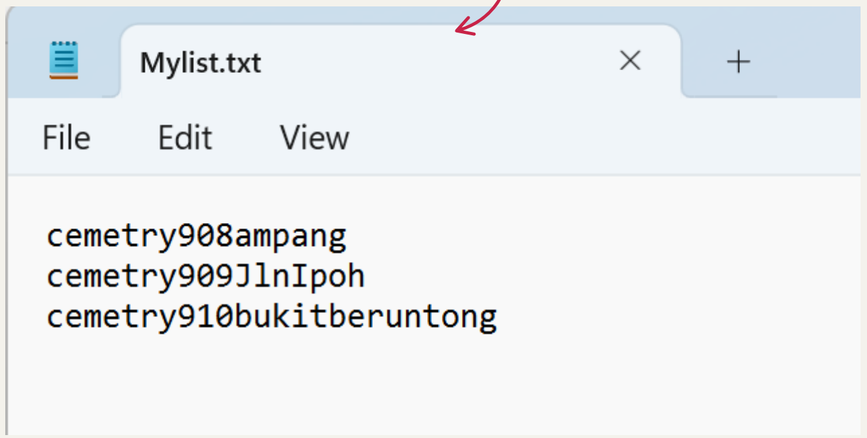




favorite.bmp

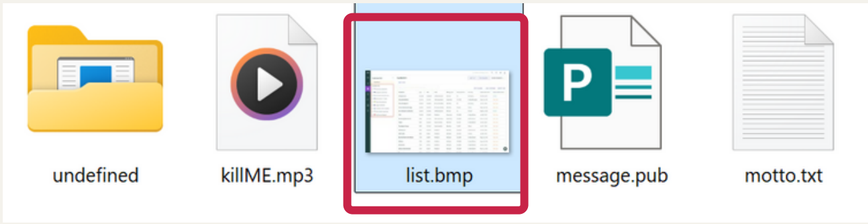
when using MDC option on S-tools while decoding favorite, we used jordan (small letters) as the passphrase we got:

Mylist.tex t



List.bmp

when using MDC option on S-tools while decoding favorite, we used jordan (small letters) as the passphrase we got:

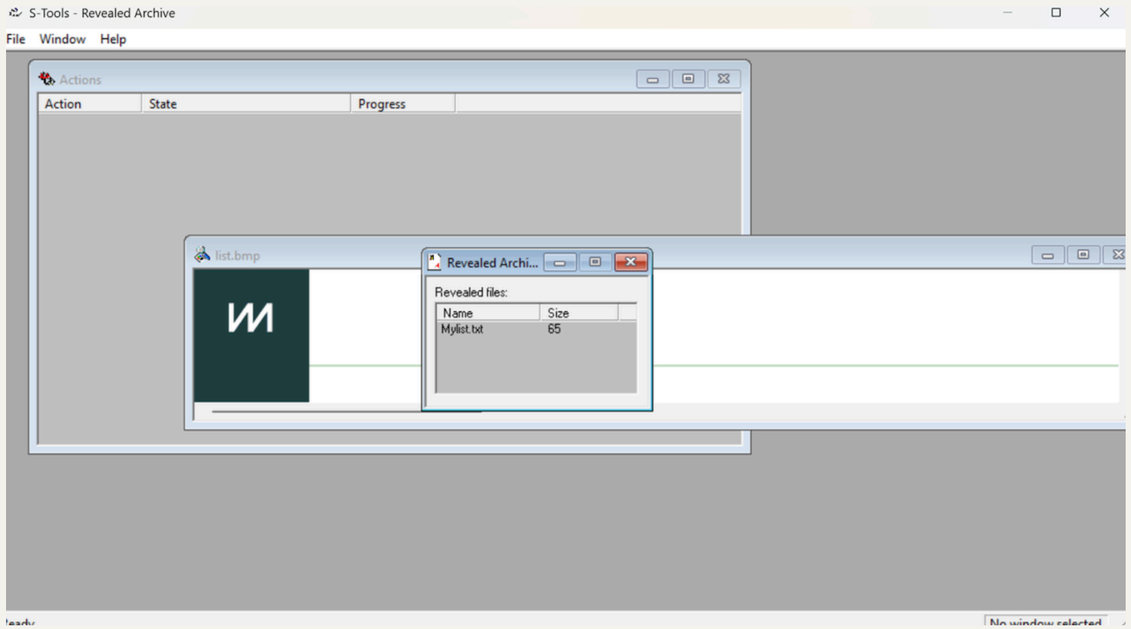


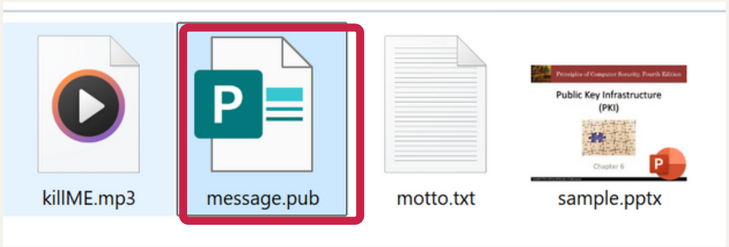
Mylist.txt | Mylist2.txt

File Edit View

```
maryam17
hannah15
ashley14
sophea10

danny10
ben19
mikael5
```

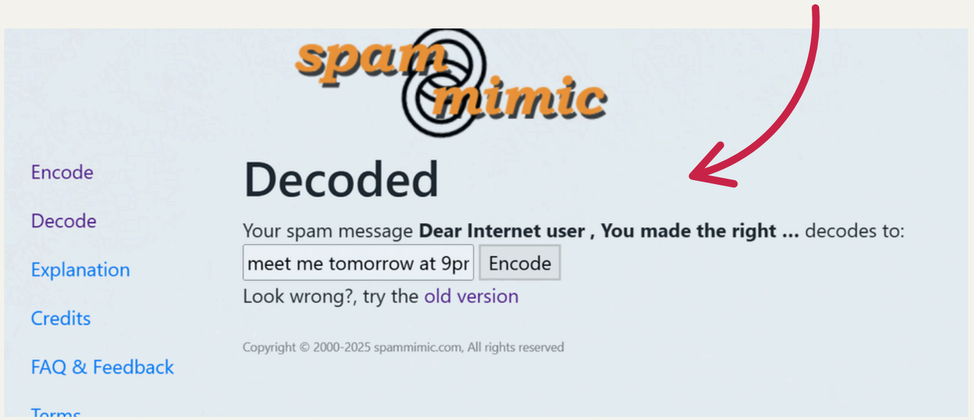




Dear Internet user , You made the right decision when you signed up for our database ! This is a one time mailing there is no need to request removal if you won't want any more ! This mail is being sent in compliance with Senate bill 1623 , Title 2 , Section 308 . This is NOT unsolicited bulk mail ! Why work for somebody else when you can become rich inside 30 weeks ! Have you ever noticed more people than ever are surfing the web and people love convenience . Well, now is your chance to capitalize on this . We will help you increase customer response by 160% and increase customer response by 200% . You are guaranteed to succeed because we take all the risk . But don't believe us ! Ms Anderson who resides in Alabama tried us and says "Now I'm rich, Rich, RICH" . We are licensed to operate in all states ! DO NOT DELAY - order today . Sign up a friend and you'll get a discount of 30% ! God Bless ! Dear Colleague , Thank-you for your interest in our publication . This is a one time mailing there is no need to request removal if you won't want any more . This mail is being sent in compliance with Senate bill 1622 , Title 2 , Section 308 . This is a ligitimate business proposal . Why work for somebody else when you can become rich within 59 DAYS ! Have you ever noticed more people than ever are surfing the web & nearly every commercial on television has a .com on in it ! Well, now is your chance to capitalize on this ! WE will help YOU increase customer response by 180% plus deliver goods right to the customer's doorstep ! You can begin at absolutely no cost to you ! But don't believe us . Mrs Simpson of Utah tried us and says "I've been poor and I've been rich - rich is better" . We assure you that we operate within all applicable laws ! If not for you then for your LOVED ONES - act now ! Sign up a friend and your friend will be rich too ! Warmest regards . Dear Sir or Madam , This letter was specially selected to be sent to you ! This is a one time mailing there is no need to request removal if you won't want any more ! This mail is being sent in compliance with Senate bill 2716 ; Title 3 ; Section 302 ! THIS IS NOT MULTI-LEVEL MARKETING ! Why work for somebody else when you can become rich within 23 days ! Have you ever noticed people love convenience and nobody is getting any younger ! Well, now is your chance to capitalize on this ! WE will help YOU sell more & use credit cards on your website . The best thing about our system is that it is absolutely risk free for you ! But don't believe us ! Ms Anderson of Nevada tried us and says "I was skeptical but it worked for me" . We assure you that we operate within all applicable laws ! We IMPLORE you - act now . Sign up a friend and your friend will be rich too ! Cheers .

Message.pub

upon uploading the spam text on spammimic.com and using "jordan" as the password, we ended up with a interseting message:



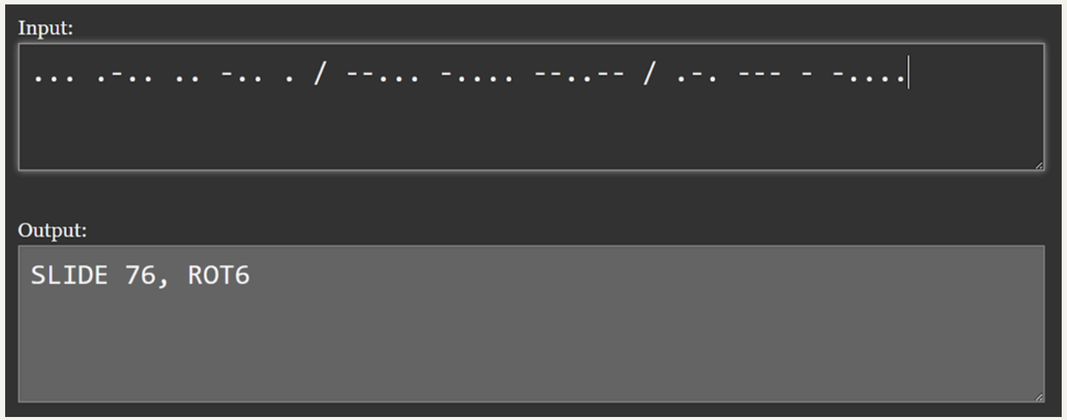
"meet me tomorrow at 9pm"

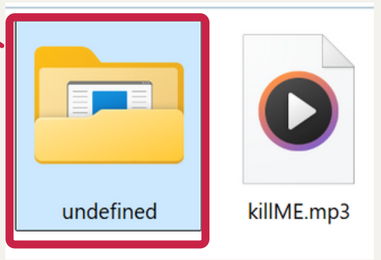
www.spammimic.com/decode.cgi

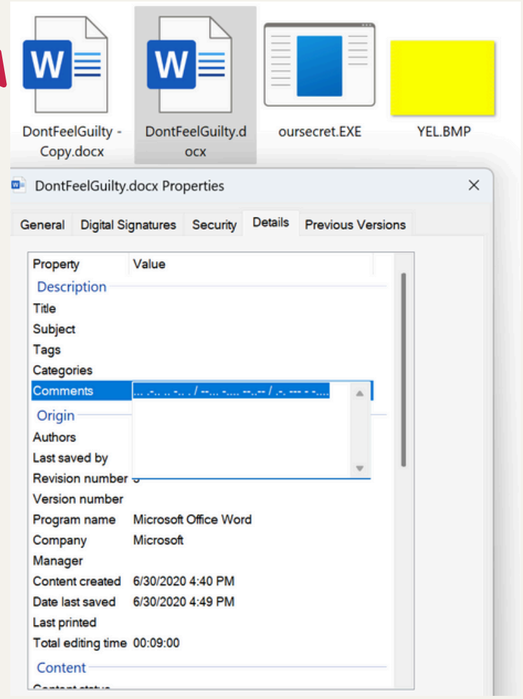
DontFeelGuilty.docx

Going to the comments of this docs, we found a morse code which translates to:

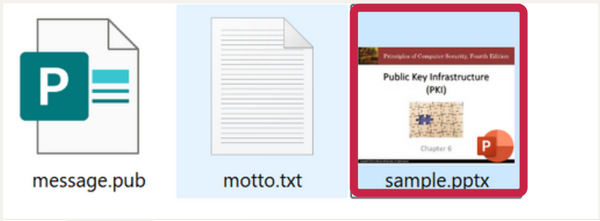
... .-.. .. -.. . / --... -.... --..-- / .-. --- - -....

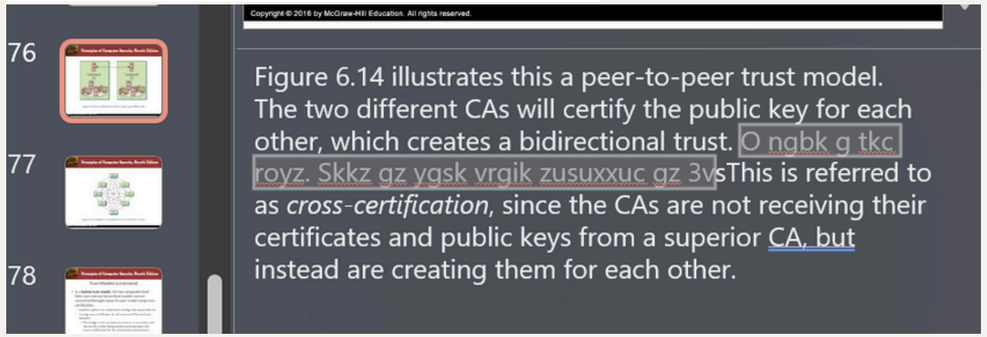




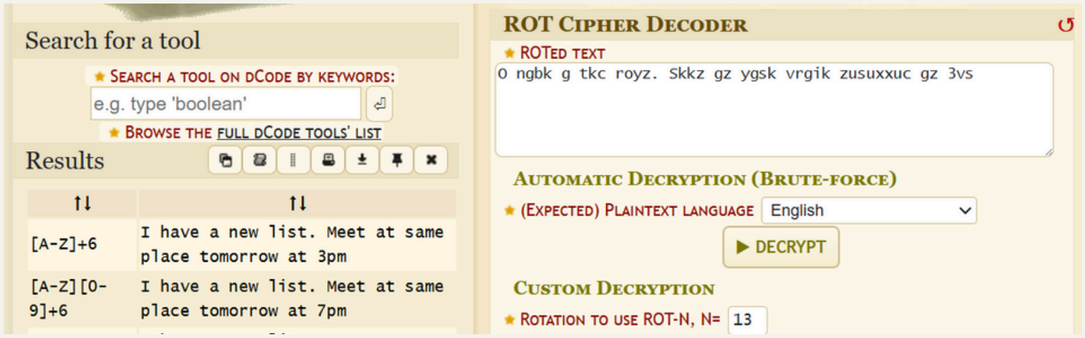


We found the same result when converting this docs file to zip and opening core.xml file





O ngbk g tkc royz. Skkz gz ygsk vrgik zusuxxuc gz 3vs



sample.pptx

When we went to 76th slide of sample.pptx, we found an encrypted text which upon decoding gives us:

I have a new list.
Meet at same place tomorrow at 3pm

OR

I have a new list.
Meet at same place tomorrow at 7pm

WHAT DOES IT MEAN THEN?

NE CARINE
HIA SOPHIA
RA NORA
INA KATRINA

cemetry908ampang
cemetry909jlnlpoh
cemetry910bukitberuntong

"meet me tomorrow at 9pm"

I have a new list.
Meet at same place tomorrow at 3pm

Number 4???

maryam17
hannah15
ashley14
sophea10

danny10
ben19
mikael5

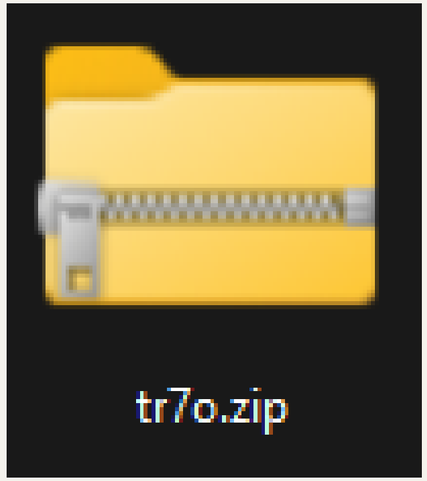
www.howtokill.com

BLACK HAT: HIDING EVIDENCE

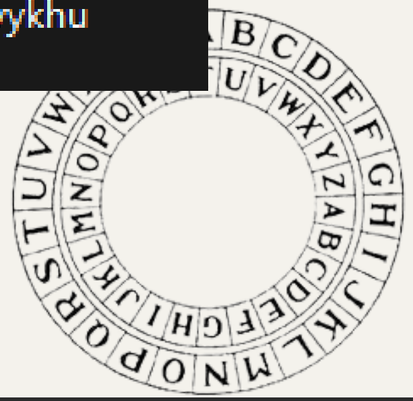
ZIP FILE

- Need password to extract the zip file using Winrar/7zip
- But can be open/viewed using default Window Explorer

- this is the view when opened using Window Explorer
- the file name tr7o.zip is a clue to the password of the file (rearrange to get rot7)



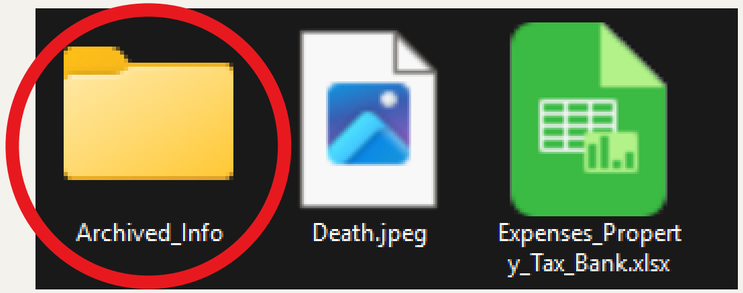
PASSWORD



Using https://www.dcode.fr/rot-cipher , setting the rotation to be ROT7 (based on the clue from the zip file) and then decode file name "qvykhu", we would get "jordan" which is the password to extract the file

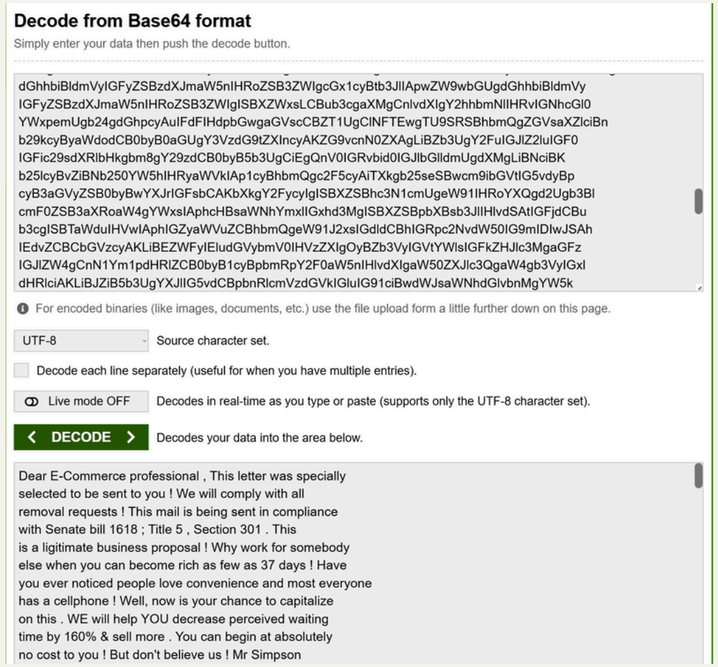
Archived_info

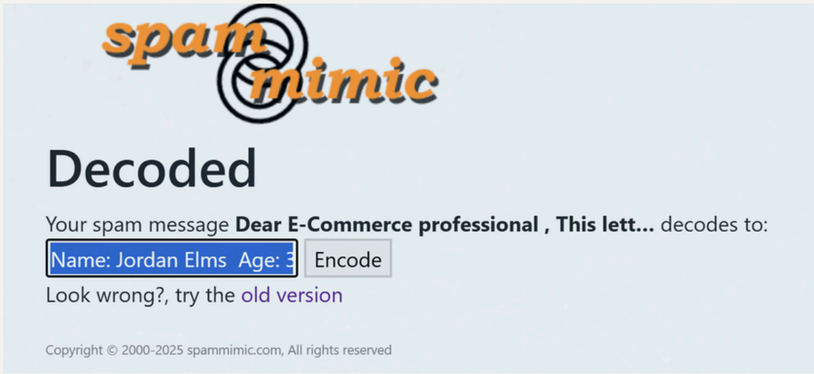
this is slightly difficult as the spam mimic requires a password for the text to be decoded. And if any is unfamiliar with base 64, then they will have a difficult time trying to decode the text.



Name: Jordan Elms Age: 34 Occupation: Groundskeeper at Ravenshade Estate

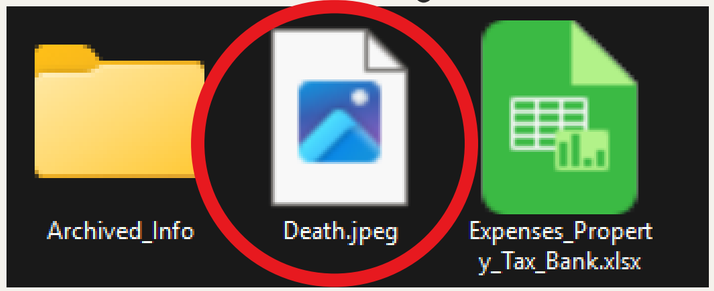
obtain base64 code





go to spam mimic
with password (JORDAN)

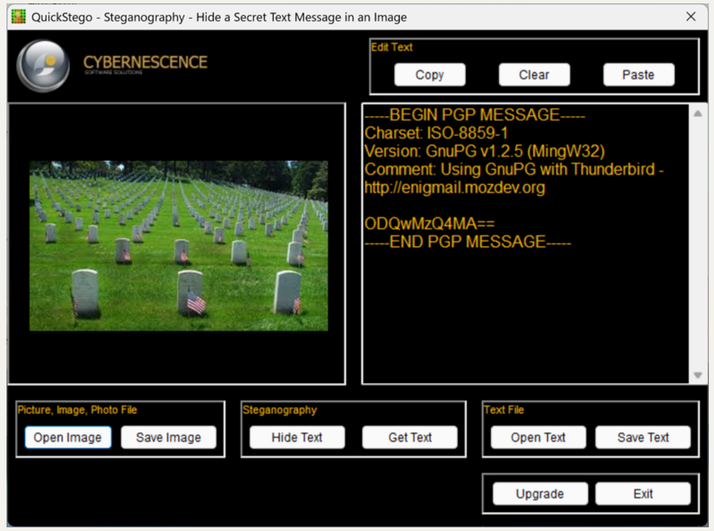
Death.jpeg



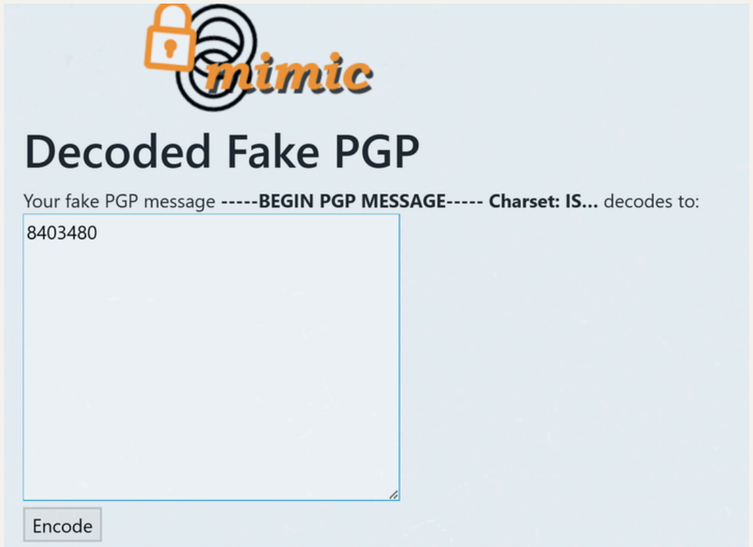
50460 IS THE POSTAL CODE FOR THE CEMETERY

BASE 36

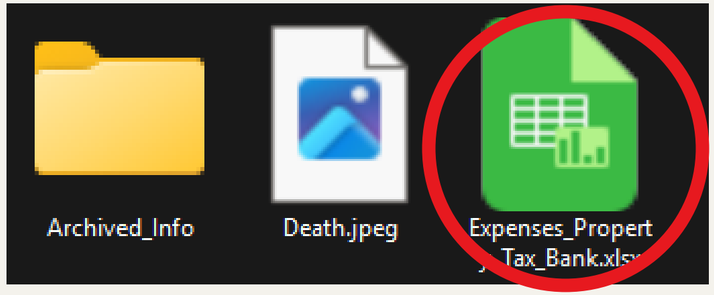
Image Steganography



FAKE PGP

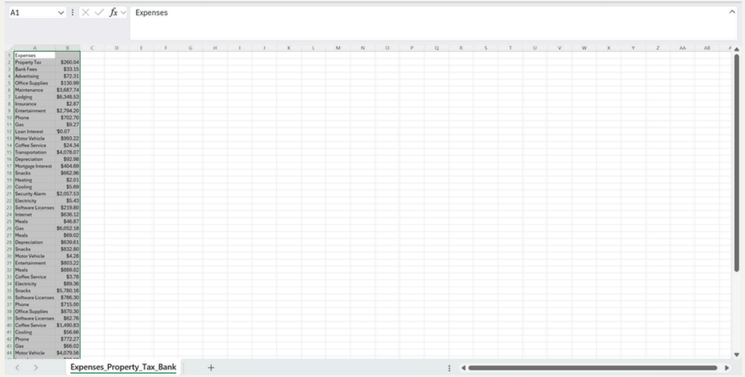


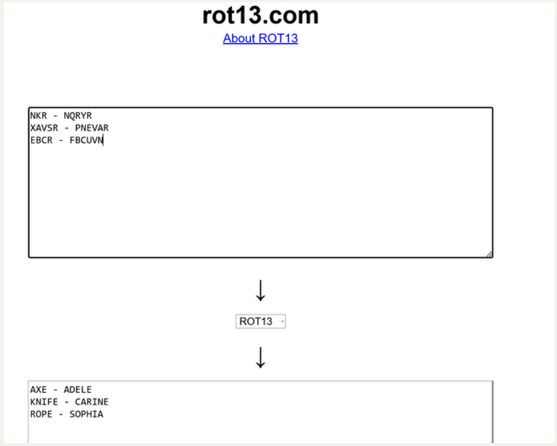
Expenses_Propert_tax_blank.xlsx



AXE - ADELE
KNIFE - CARINE
ROPE - SOPHIA

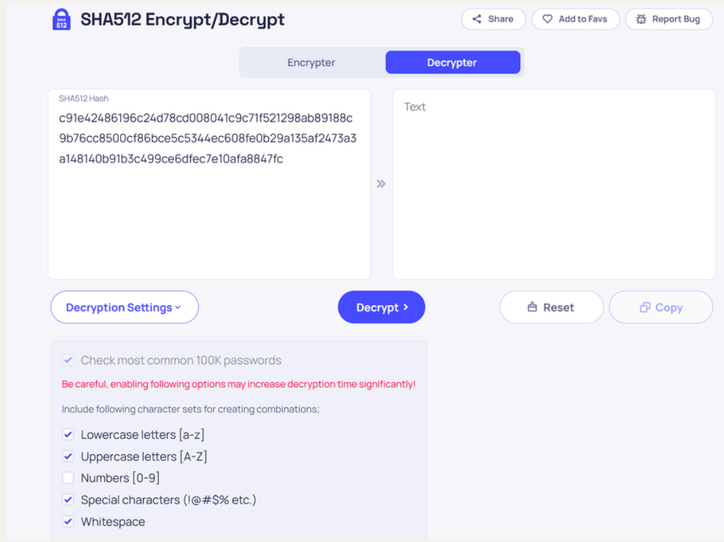
SPREADSHEET MIMIC





NKR - NQRYR
XAVSR - PNEVAR
EBCR - FBCUVN

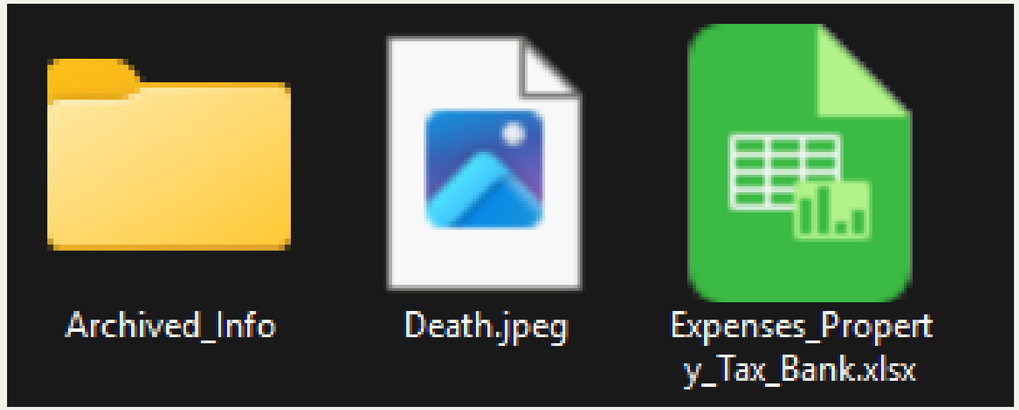
ROT13



SPAM MIMIC
CONVERT TO
CSV.

SHA512

Inside qvykhu



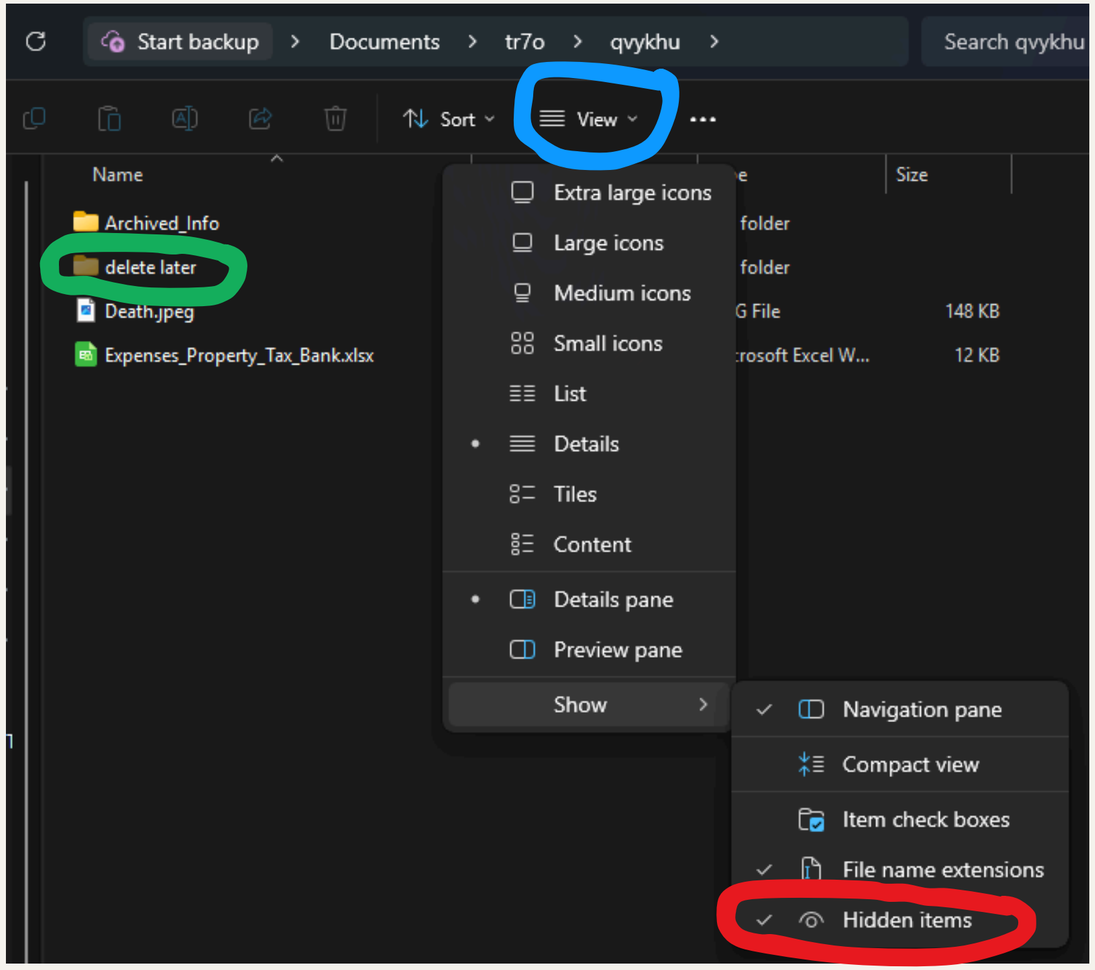
we can see that the files that are inside qvykhu; a folder, a jpeg and one excel spreadsheet.

But this is just a distraction. there are more files located inside qvykhu, and that is the surprise!!

HIDDEN FOLDER

If you clicked View (in blue circle), and then Show, and lastly checked the "Hidden Items" (in red circle), you can find a hidden folder name "delete later" (in green circle).

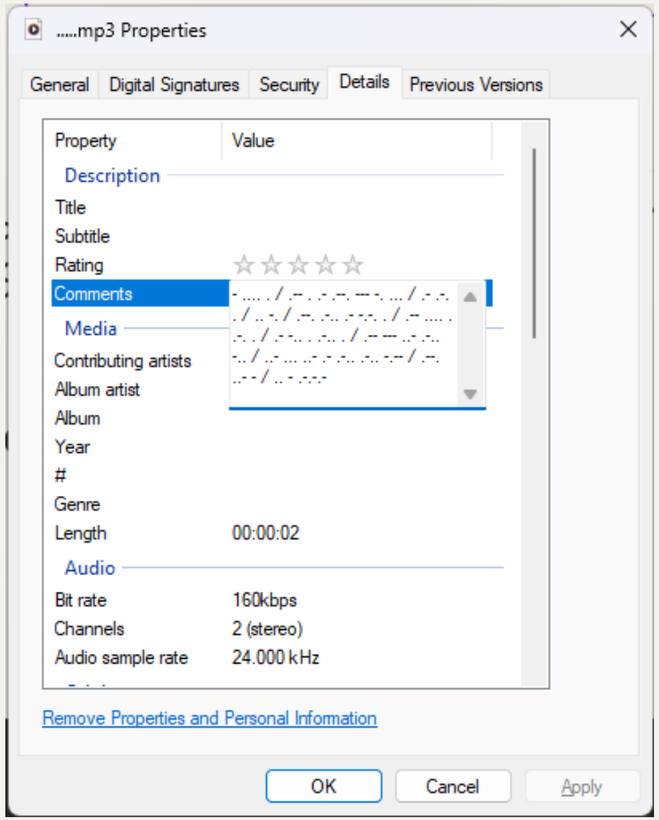
this one of the common ways people use to hide files, especially by software developers.



there are 3 files in the folder; which is an mp3 audio, a pdf containing a red noise static image, and a bmp

the pdf is just a decoy, there's no hidden file/message neither in the file itself nor the image inside it.

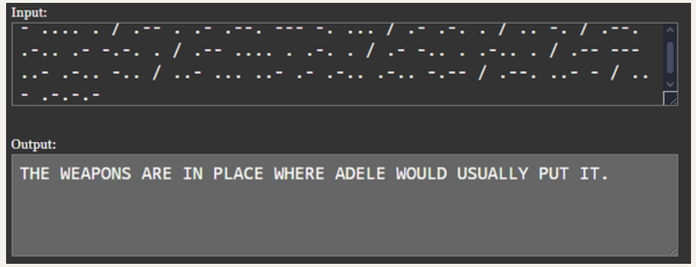
INSIDE "DELETE LATER"



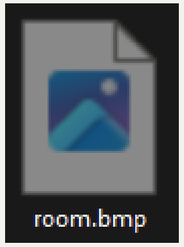
there is a morse code hidden in the comments of ".....mp3"

- .... . / .-- . .- .--. --- -. ... / .- .-. . / .. -. / .--. .-.. .- -.-. . / .-- .... . .-. . / .- -.. . .-.. . / .-- --- ..- .-.. -.. / ..- ... ..- .- .-.. .-.. -.-- / .--. ..- - / .. - .-.-.-

which can be translated using https://morsecode.world/international/translator.html into "THE WEAPONS ARE IN PLACE WHERE ADELE WOULD USUALLY PUT IT."

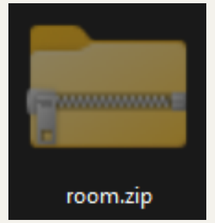


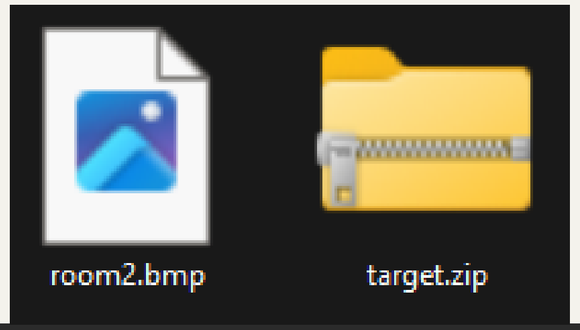
ROOM.BMP

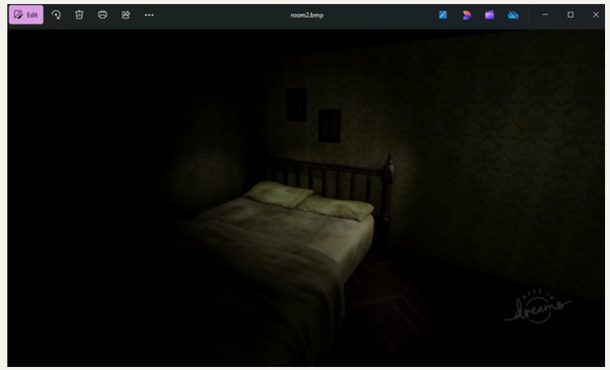


- If we open the "room.bmp", we would get nothing displayed

- But if we rename the file to "room.zip", we can open the zip and see that there are 2 more files
- a "room2.bmp"
- a "target.zip" that contains an image of their next target

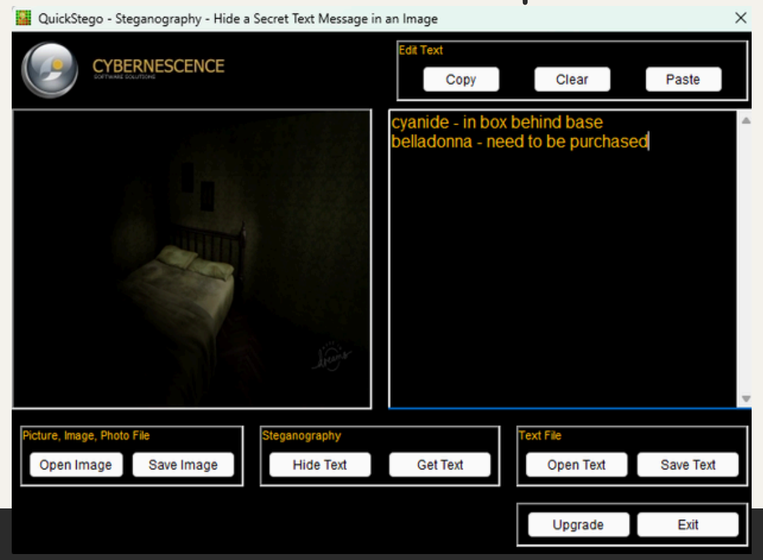






LASTLY, ROOM2.BMP

"room2.bmp" can be loaded into Quick Stego,
and we can find a message of:
"cyanide - in box behind base
belladonna - need to be purchased"



THANK YOU FOR LISTENING!