



CSCI 2303 PRINCIPLES
OF IT SECURITY

CASE 06: MURDER

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

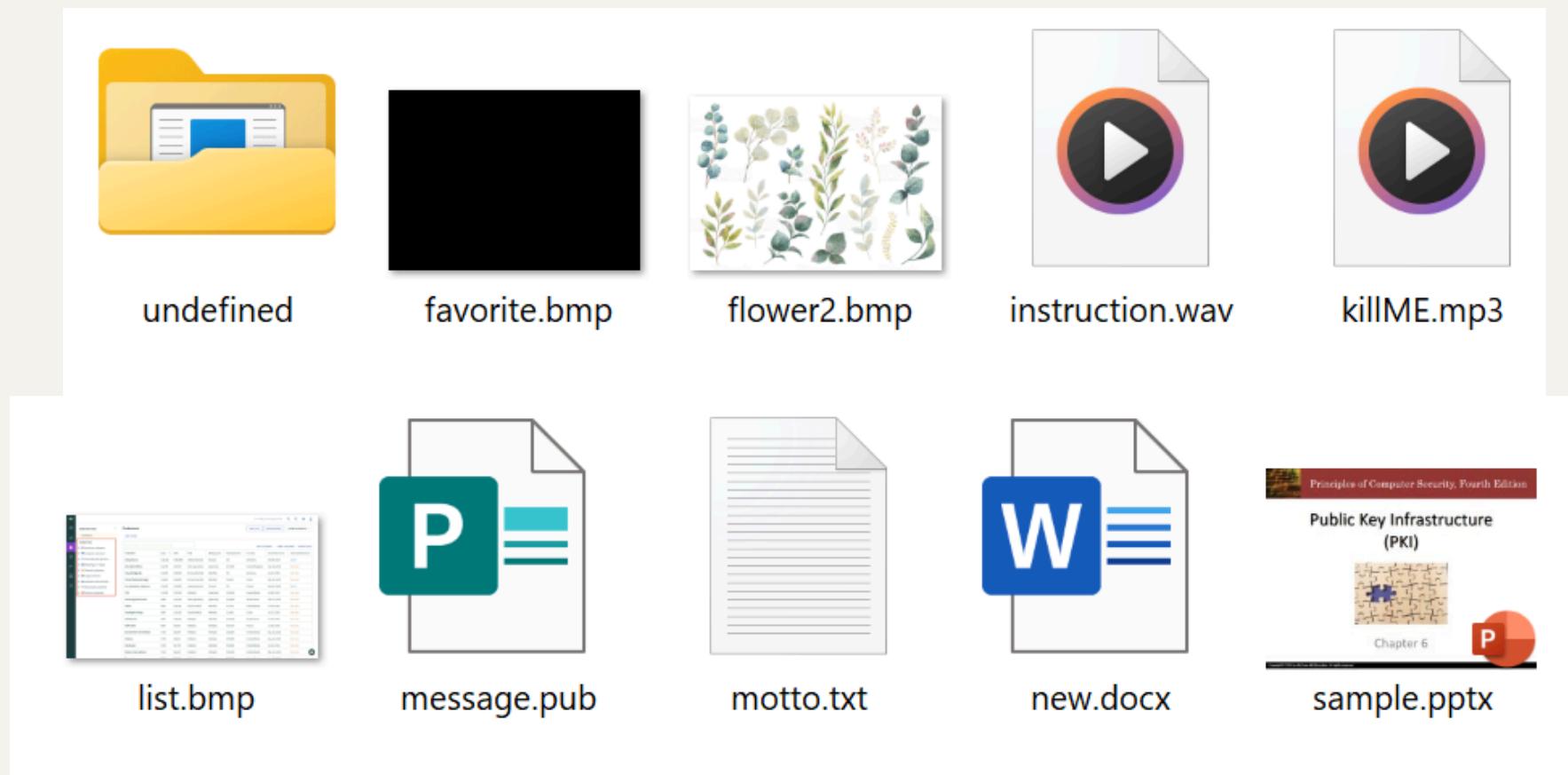
the file name when decode through rot cypher at Rot-N, where N =13 gave us two options:

- **Number 4:** If number is Not rotated
- **Number 7:** If number is rotated

	↑↓	↑↓
[A-Z] [0-9]+25	Baipsf2	
[A-Z0-9]+3	7we1ob4	
[A-Z]+25	Baipsf7	
[A-Z] [0-9]+13	Nmumber4	
[A-Z]+13	Nmumber7	

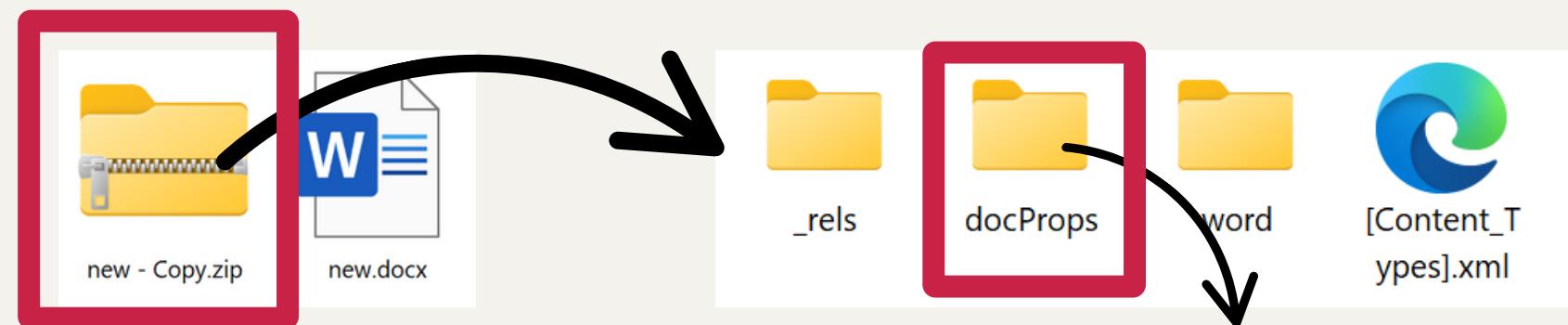
<https://www.dcode.fr/rot-cipher>

Inside Azhore7



there are total 10
different evidences

new.docs



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```

<cp:coreProperties xmlns:cp="http://schemas.openxmlformats.org/package/2006/metadata/core-properties"
    xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:dcterms="http://purl.org/dc/terms/"
    xmlns:dcmitype="http://purl.org/dc/dcmitype/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <dc:title/>
    <dc:subject/>
    <dc:creator>lab</dc:creator>
    <cp:keywords/>
    <dc:description>eee.pwebwsqtt.kwu</dc:description>
    <cp:lastModifiedBy>lab</cp:lastModifiedBy>
    <cp:revision>3</cp:revision>
    <dcterms:created xsi:type="dcterms:W3CDTF">2020-06-30T18:03:00Z</dcterms:created>
    <dcterms:modified xsi:type="dcterms:W3CDTF">2020-06-30T18:04:00Z</dcterms:modified>
</cp:coreProperties>

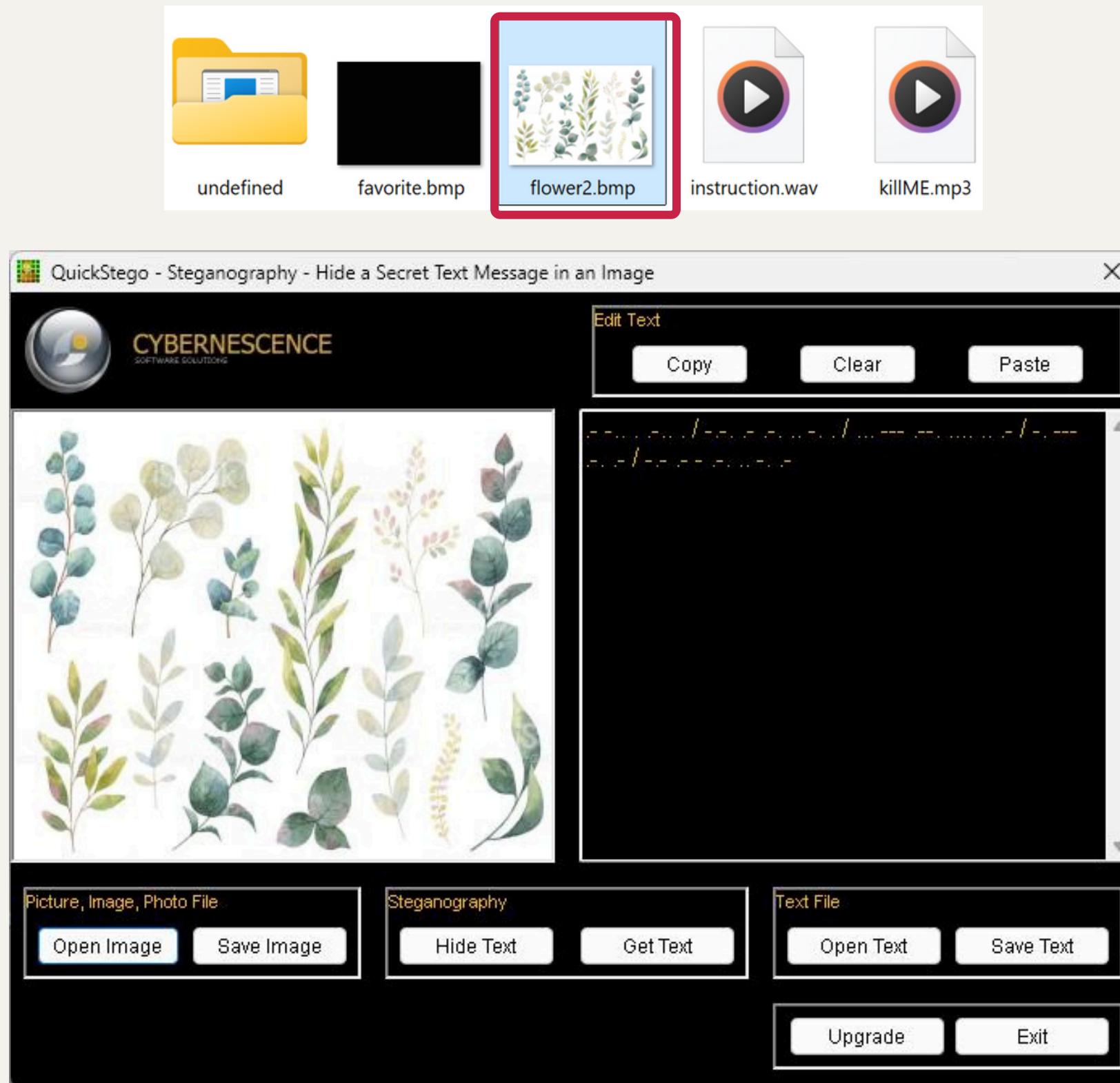
```

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



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

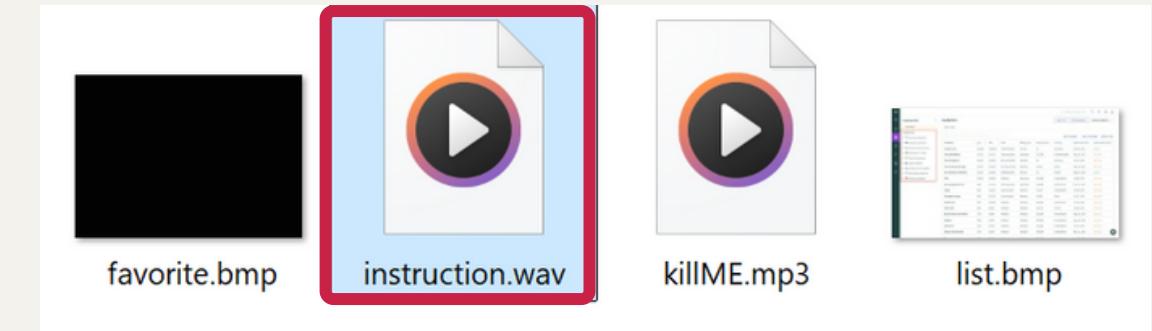
Upon decoding this file via mp3
stego and online"

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

we got:

USE MDC JORDAN

(we used this in the next artifact)

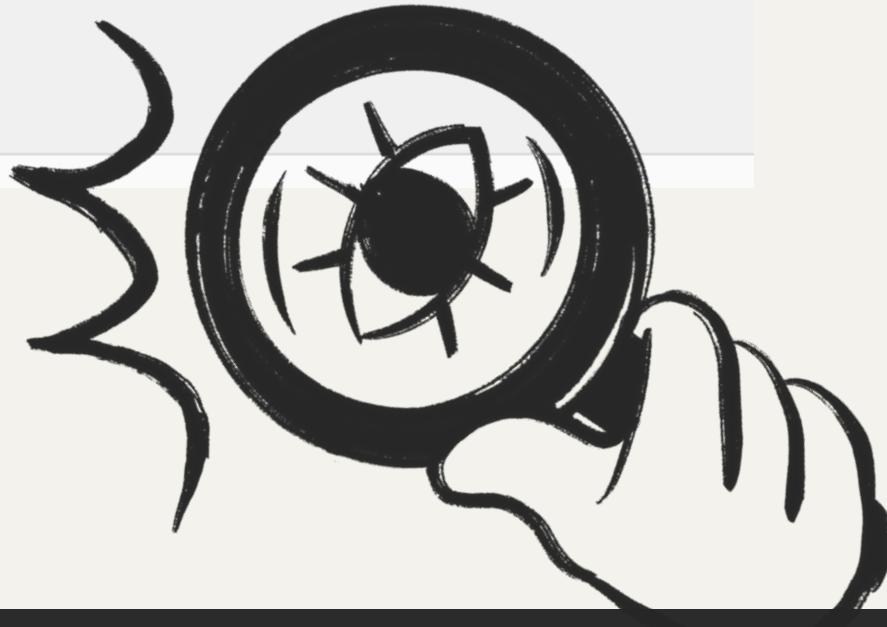


Filename: "instruction.wav"

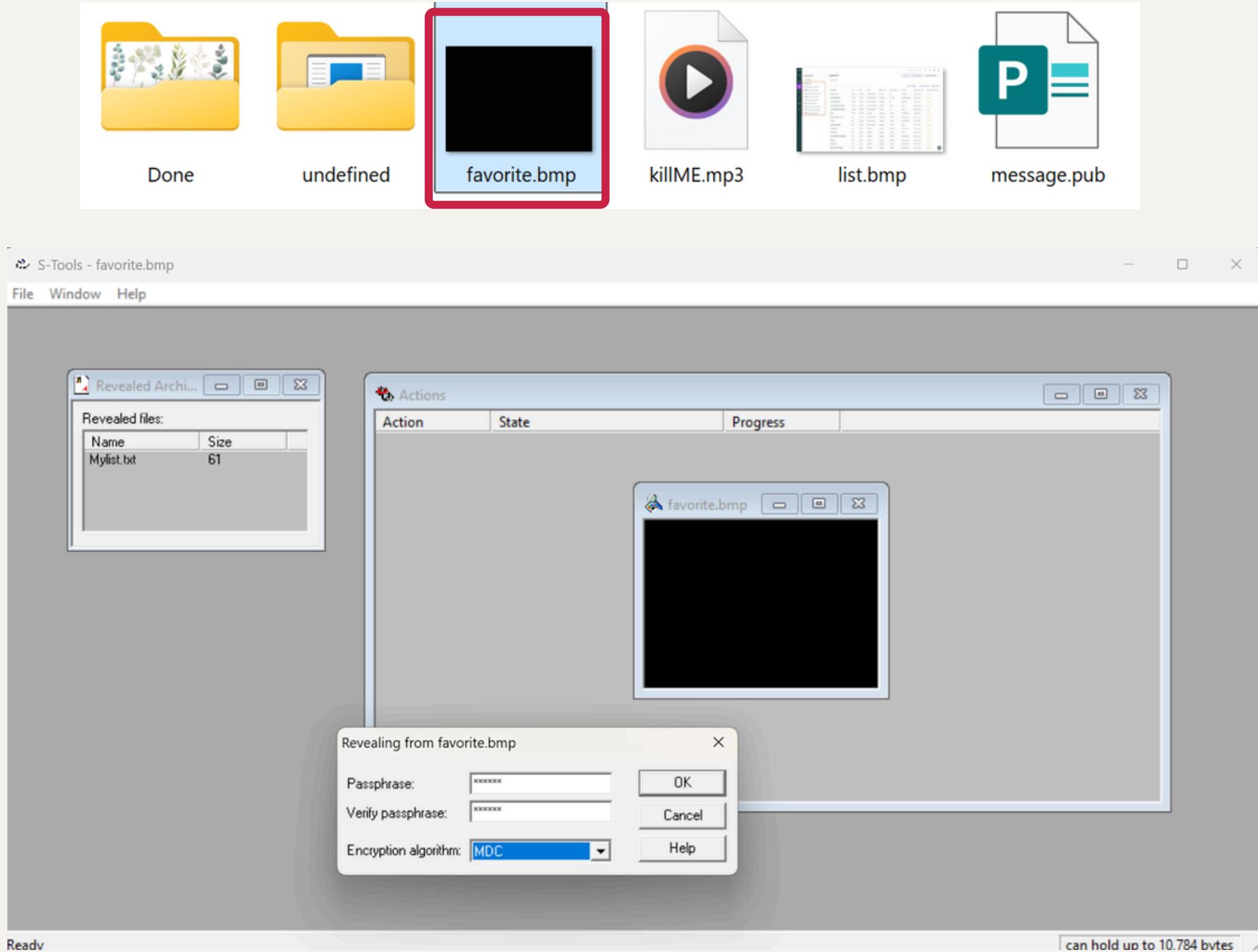
Listen Stop

Upload Play Stop

USE MDC JORDAN

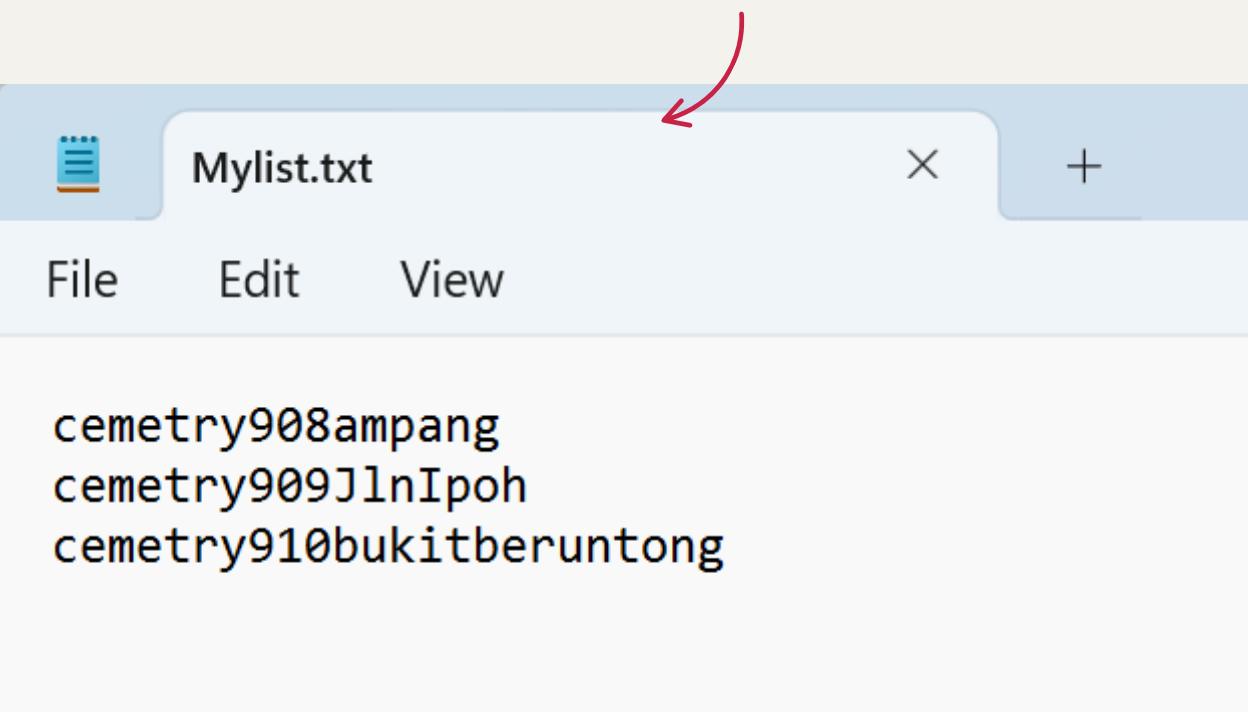


mp3-stego + morsecode.world



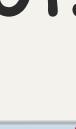
favorite.bmp

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

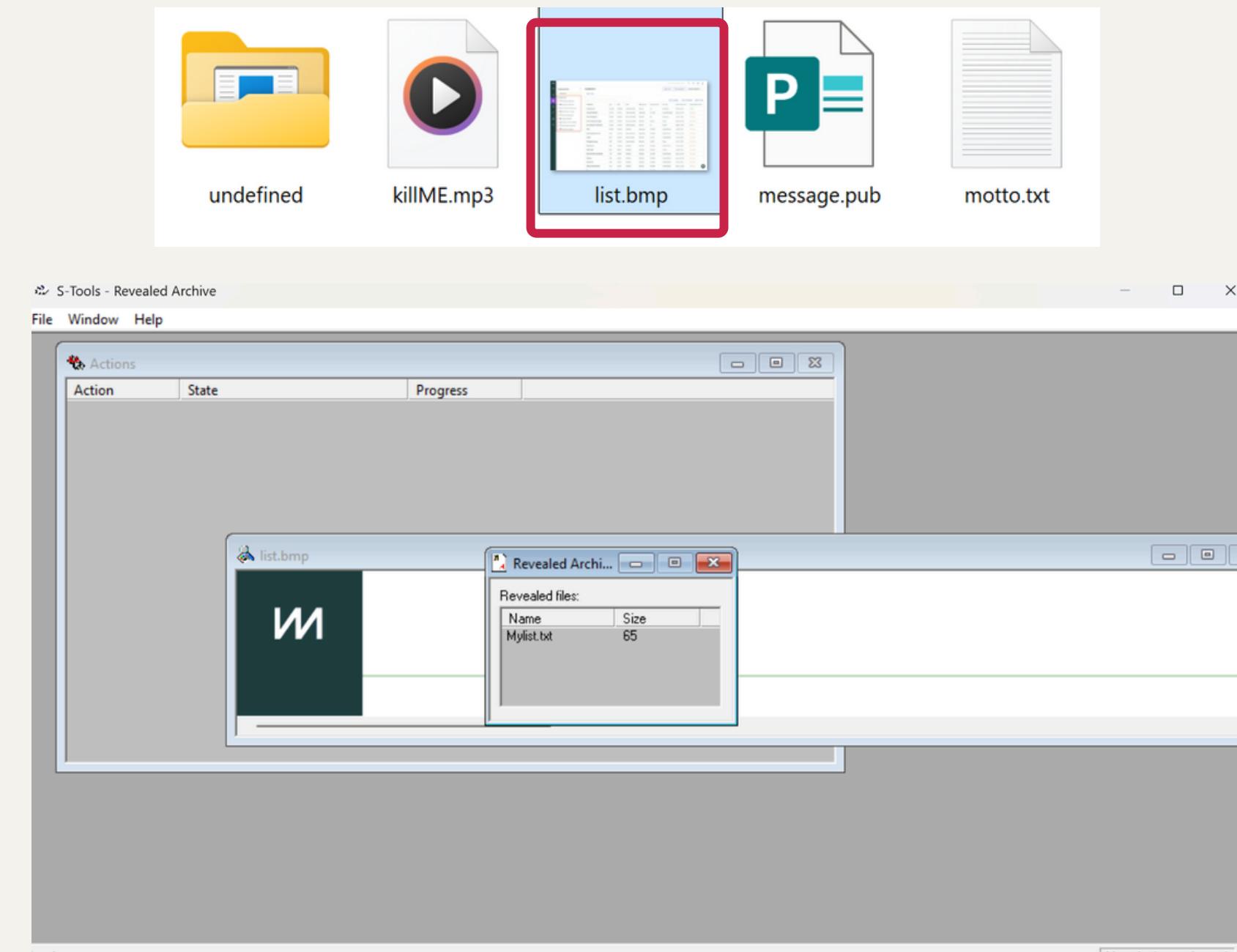


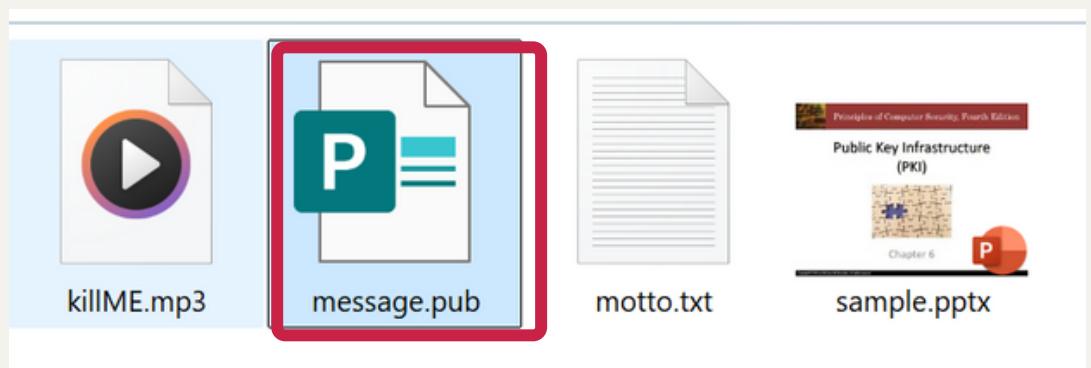
List.bmp

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
mikael15
```





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 legitimate 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 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 interesting message:

The screenshot shows the spammimic.com homepage with the word 'spam' in orange and 'mimic' in blue. Below it, the word 'Decoded' is displayed. To the left is a sidebar with links: Encode, Decode, Explanation, Credits, FAQ & Feedback, and Terms. The main content area contains the decoded message: 'Your spam message Dear Internet user , You made the right ... decodes to: meet me tomorrow at 9pm'. There is also a link to 'Encode' and a note 'Look wrong?, try the old version'. At the bottom, a copyright notice reads 'Copyright © 2000-2025 spammimic.com, All rights reserved'.

"meet me tomorrow at 9pm"

DontFeelGuilty.docx

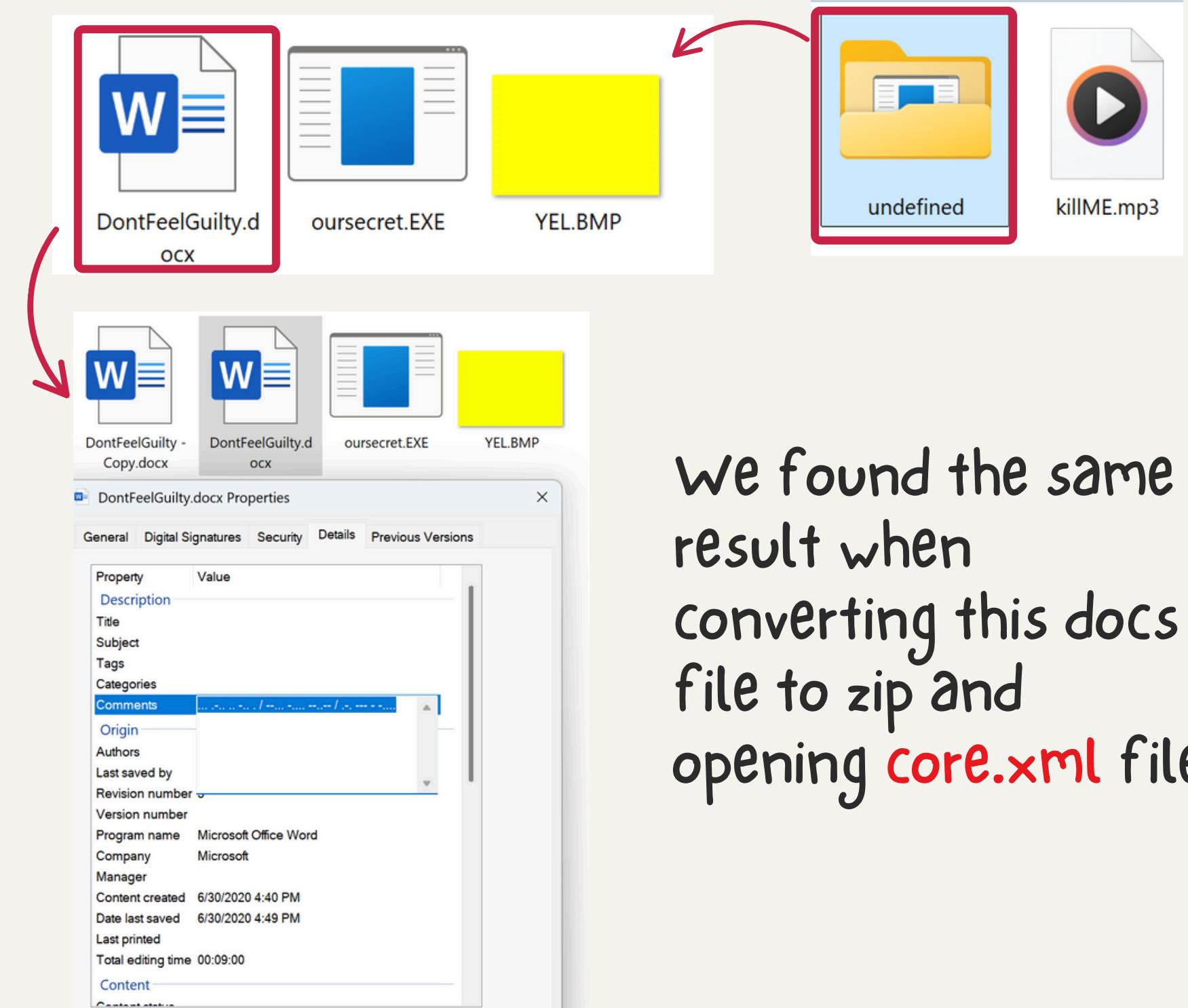
Going to the comments of this docs, we found a morse code which translates to:

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

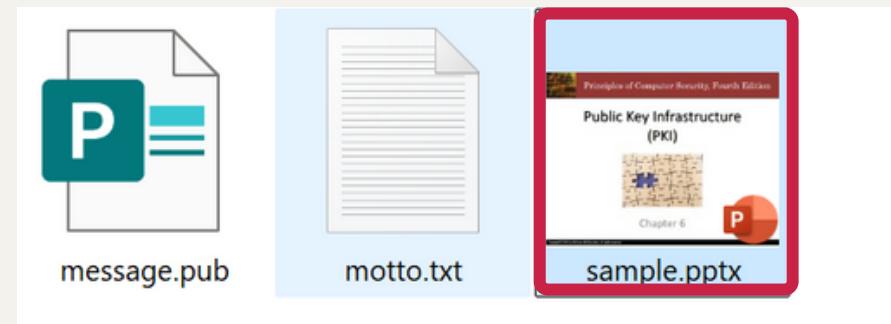
```
Input:
... .-... -... / --... -.... --- - / ..- - - - -....|
```

Output:

```
SLIDE 76, ROT6
```



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



Copyright © 2016 by McGraw-Hill Education. All rights reserved.

76 Figure 6.14 illustrates this a peer-to-peer trust model. The two different CAs will certify the public key for each other, which creates a bidirectional trust. O ngbk g tkc royz. Skkz gz ygsk vrgik zusuxuc gz 3vs This is referred to as *cross-certification*, since the CAs are not receiving their certificates and public keys from a superior CA, but instead are creating them for each other.

77

78

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

Search for a tool

★ SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type 'boolean'

★ BROWSE THE FULL DCODE TOOLS' LIST

Results

↑↓	↑↓
[A-Z]+6	I have a new list. Meet at same place tomorrow at 3pm
[A-Z][0-9]+6	I have a new list. Meet at same place tomorrow at 7pm

ROT CIPHER DECODER

★ ROTED TEXT
O ngbk g tkc royz. Skkz gz ygsk vrgik zusuxuc gz 3vs

AUTOMATIC DECRYPTION (BRUTE-FORCE)

★ (EXPECTED) PLAINTEXT LANGUAGE English

► DECRYPT

CUSTOM DECRYPTION

★ ROTATION TO USE ROT-N, N= 13

sample.pptx

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

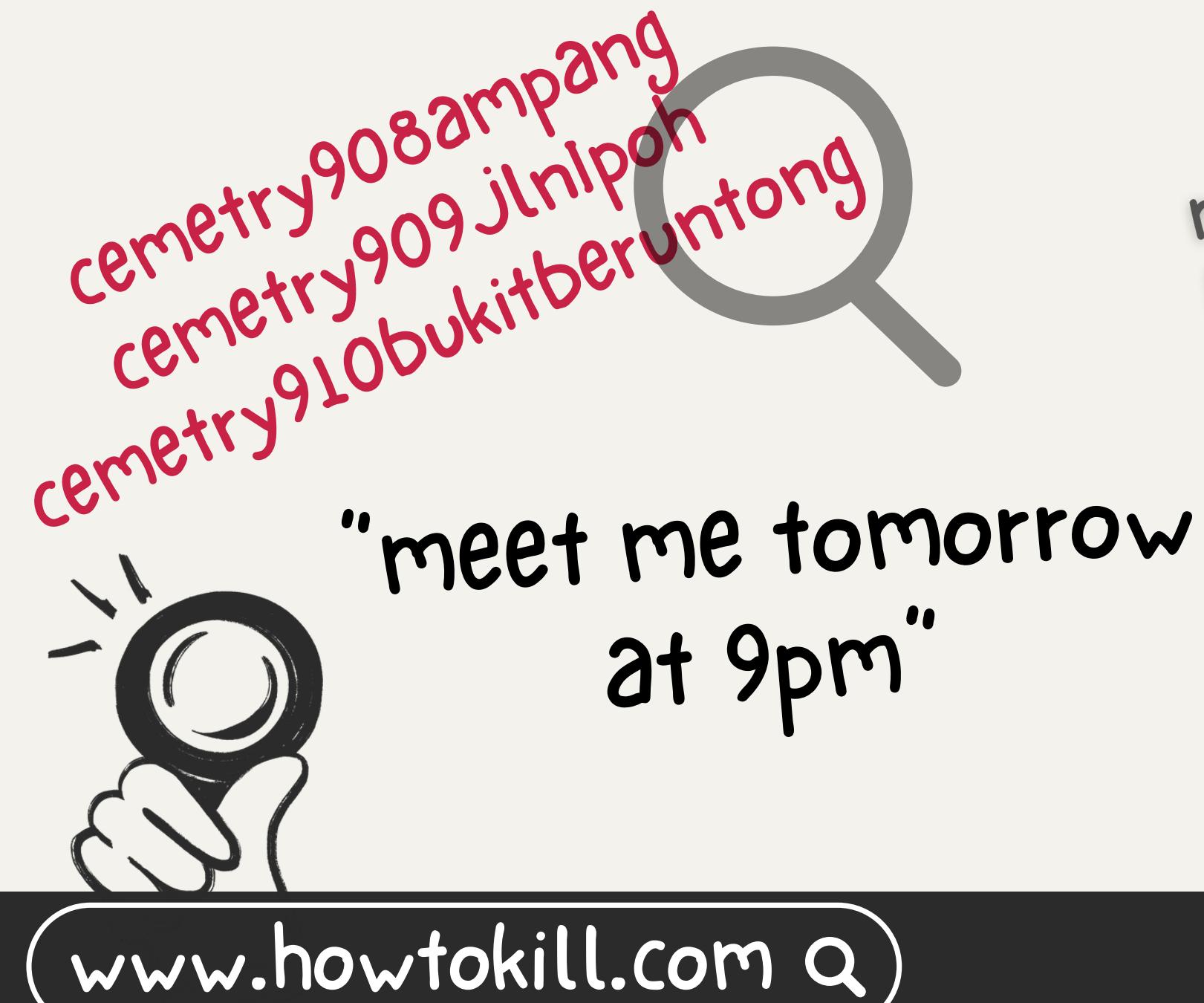
I have a new list.
Meet at same place tomorrow at 3pm

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



www.howtokill.com Q

Meet at same place tomorrow at 3pm
I have a new list.
Number
4???

maryam17
hannah15
ashley14
sophea10

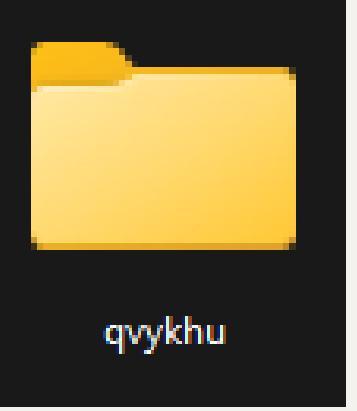
danny10
ben19
mikael5

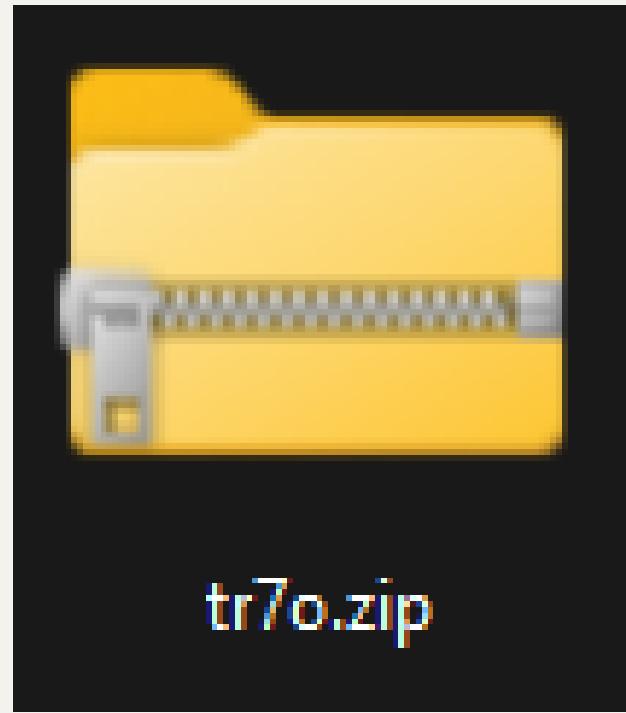




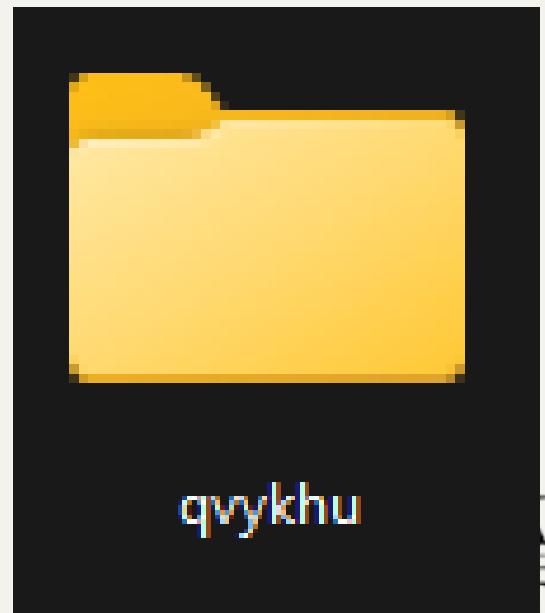
**BLACK HAT:
HIDING
EVIDENCE**

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)
- 



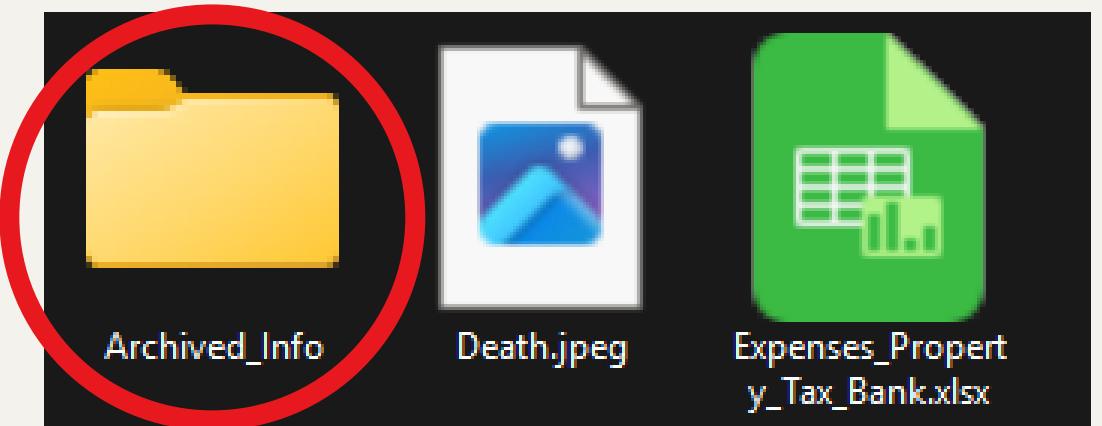
PASSWORD



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

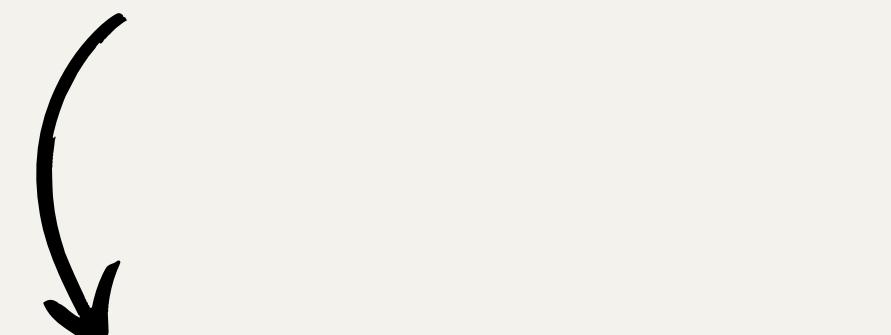


Archived_info



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



Decode from Base64 format
Simply enter your data then push the decode button.

```
dGhhbiBldmVylGFyZSBzdXJmaW5nIHRoZSB3ZWlgcGx1cyBt3JlApwZW9wbGUgdGhhbiBldmVylGFyZSBzdXJmaW5nIHRoZSB3ZWlgISBXZWxsLCBub3cgaXMgCnvdXlgY2hhbmNIIHRvIGNhGIOYWxpeMUb24gdGhpcoyAuFdFIHdpbGwgaGVscCBZT1UgCINFTEwgTU9SRSBhbmgQzGVsaXZlcBnb29kcyByaWdodCB0byB0aGUgY3VzdG9tZXIncyAKZG9vcnN0ZXAgLiBzb3UgY2FuIGJZ2luGF0IGFic29sdXRlbHkgbm8gY29zdCB0byB5b3UgCiEgQnV0IGRvbidoGJlbGldmUgdXMgLiBNciBKb25icyBvZIBNb250YW5hIHyawVklAp1cyBhbmQgc2F5cyAiTXkgb25seSBwcm9ibGvtG5vdyBpcyB3aGVyZSB0byBwYXJrlGFsbCAKbXkgY2FycylgISBXZSBhc3N1cmUgeW91IHRoYXQgd2Ugb3BIcmF0ZSB3aXRoaw4gYWxsAphcHBsaWNhYmxlGxhd3MgISBXZSBpbXsb3JlIhvdsAtIGFjdCBub3cgISBTaWduIHvwApHIGZyaVuZCBhbmgQeW91J2xsGdldCBhlGRpc2NvdW50lG9mlDlwSAhIEdvZCBCbGVzcyAKLjBEZWfyleudGVybmv0lHVzZlglOyBzb3VylGVtYWIslGFZhJlc3MgaGFzIGJIZW4gCnN1Ym1pdHRIZCB0byB1cyBpbmRpY2F0aW5nIhvdxlgaW50ZXJlc3QgaW4gb3VylGxldHRiciAKLjBZiB5b3UgYXJlG5vdCBpbnRlcmVzdGVklGluiG91ciBwdWJsaWNhdGlvbnMgYW5k
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.
 Decode each line separately (useful for when you have multiple entries).
 Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

DECODE Decodes your data into the area below.

Dear E-Commerce professional , This letter was specially selected to be sent to you ! We will comply with all removal requests ! This mail is being sent in compliance with Senate bill 1618 ; Title 5 , Section 301 . This is a legitimate business proposal ! Why work for somebody else when you can become rich as few as 37 days ! Have you ever noticed people love convenience and most everyone has a cellphone ! Well, now is your chance to capitalize on this . WE will help YOU decrease perceived waiting time by 160% & sell more . You can begin at absolutely no cost to you ! But don't believe us ! Mr Simpson

spam mimic

Decoded

Your spam message Dear E-Commerce professional , This lett... decodes to:

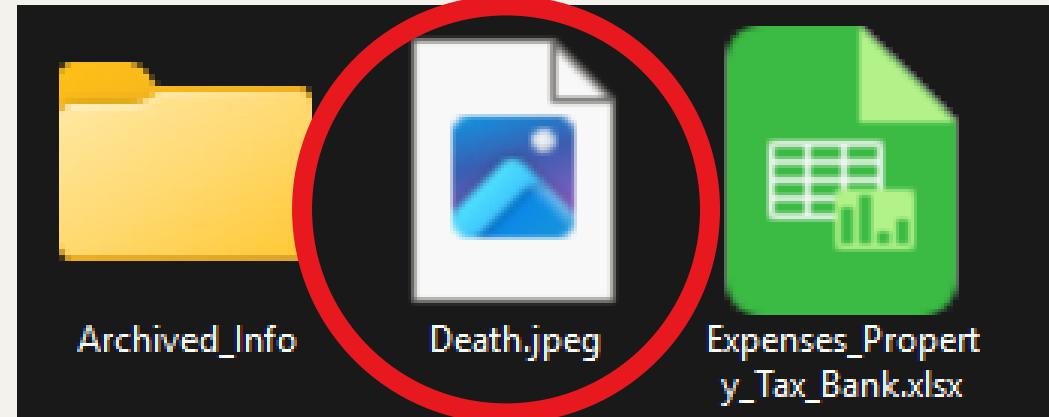
Name: Jordan Elms Age: 34 Encode

Look wrong?, try the [old version](#)

Copyright © 2000-2025 spammimic.com, All rights reserved

go to spam mimic with password (JORDAN)

Death.jpeg



50460
IS THE
POSTAL CODE
FOR THE
CEMETERY

IMAGE
STEGANOGRAPHY

QuickStego - Steganography - Hide a Secret Text Message in an Image

CYBERNESCENCE SOFTWARE SOLUTIONS

Edit Text

Copy Clear Paste

-----BEGIN PGP MESSAGE-----
Charset: ISO-8859-1
Version: GnuPG v1.2.5 (MingW32)
Comment: Using GnuPG with Thunderbird - http://enigmail.mozilla.org
ODQwMzQ4MA==
-----END PGP MESSAGE-----

Picture, Image, Photo File
Open Image Save Image

Steganography
Hide Text Get Text

Text File
Open Text Save Text

Upgrade Exit

FAKE PGP

mimic

Decoded Fake PGP

Your fake PGP message -----BEGIN PGP MESSAGE----- Charset: IS... decodes to:

8403480

Encode

BASE 36 CIPHER

Mathematics • Base 36 Cipher

BASE 36 CONVERTER (FROM NUMBERS TO LETTERS/DIGITS)

SEARCH A TOOL ON dCODE BY KEYWORDS:
e.g. type 'sudoku'

BROWSE THE FULL dCODE TOOLS' LIST

Results

50460 8403480

Base 36 Cipher - dCode

Tag(s) : Mathematics, Cryptography

Share

+ f t g m

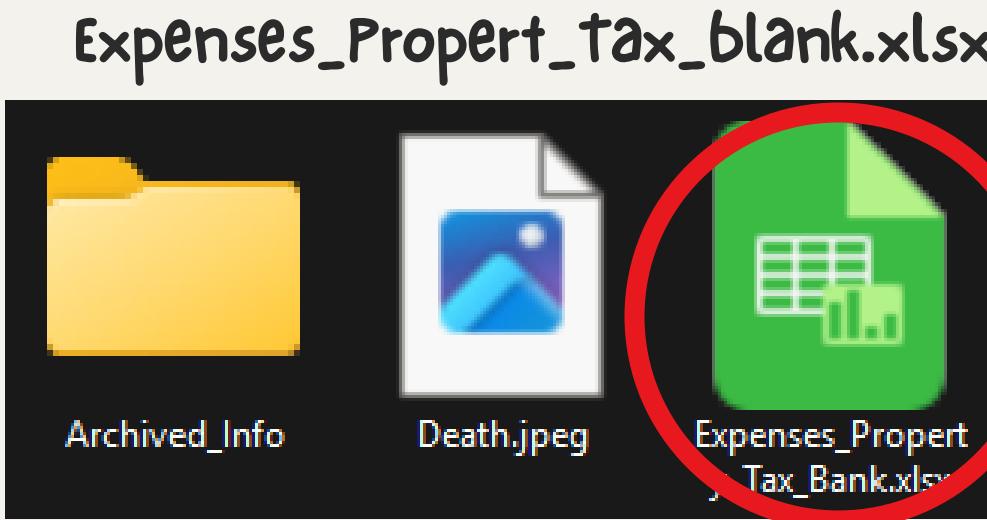
See also: Base 37 Cipher – Base 26 Cipher – Base N Convert

BASE 36 TRANSLATOR (FROM LETTERS/DIGITS TO NUMBERS)



BASE 36





AXE - ADELE
KNIFE - CARINE
ROPE - SOPHIA

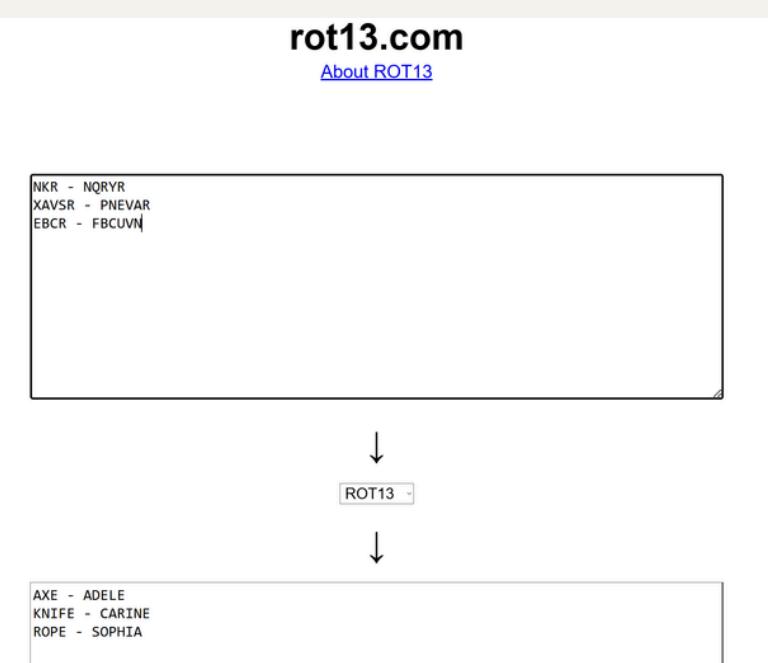
SPREADSHEET MIMIC

	A1	B1	C1	D1	E1	F1	G1	H1	I1	J1	K1	L1	M1	N1	O1	P1	Q1	R1	S1	T1	U1	V1	W1	X1	Y1	Z1	AA1	AB1	AC1
1	Expenses	\$260.04																											
2	Property Tax	\$260.04																											
3	Bank Fee	\$32.15																											
4	Advertising	\$72.31																											
5	Office Supplies	\$130.99																											
6	Meals	\$130.99																											
7	Lodging	\$6,548.53																											
8	Insurance	\$7.27																											
9	Entertainment	\$2,794.26																											
10	Phone	\$702.79																											
11	Gas	\$92.00																											
12	Loan Interest	\$0.07																											
13	Motor Vehicle	\$903.22																											
14	Cooling	\$424.52																											
15	Transportation	\$4,078.07																											
16	Depreciation	\$92.88																											
17	Medical Interest	\$454.44																											
18	Snacks	\$602.06																											
19	Heating	\$1.73																											
20	Cooling	\$1.68																											
21	Security Alarms	\$2,057.53																											
22	Business Licenses	\$3.84																											
23	Software Licenses	\$219.86																											
24	Internet	\$636.12																											
25	Meals	\$4,452.13																											
26	Gas	\$6,052.18																											
27	Meals	\$69.02																											
28	Transportation	\$523.13																											
29	Depreciation	\$532.60																											
30	Snacks	\$532.60																											
31	Motor Vehicle	\$4.28																											
32	Entertainment	\$503.22																											
33	Meals	\$889.02																											
34	Transportation	\$5,137.53																											
35	Meals	\$89.36																											
36	Electricity	\$5,780.16																											
37	Snacks	\$5,780.16																											
38	Utilities	\$100.00																											
39	Phone	\$735.00																											
40	Office Supplies	\$870.36																											
41	Book Licenses	\$1,490.83																											
42	Coffee Service	\$566.68																											
43	Cooling	\$566.68																											
44	Phone	\$772.50																											
45	Gas	\$66.62																											
46	Motor Vehicle	\$4,079.59																											

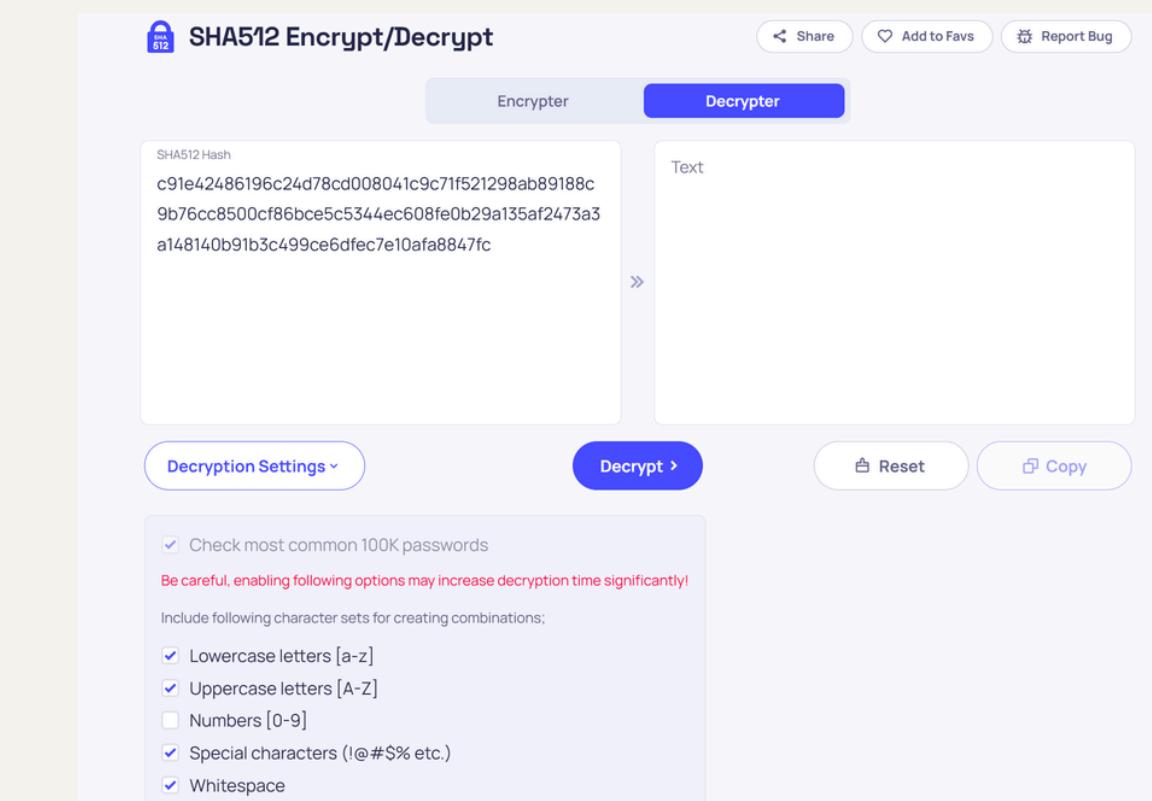
SPAM MIMIC
CONVERT TO
CSV.



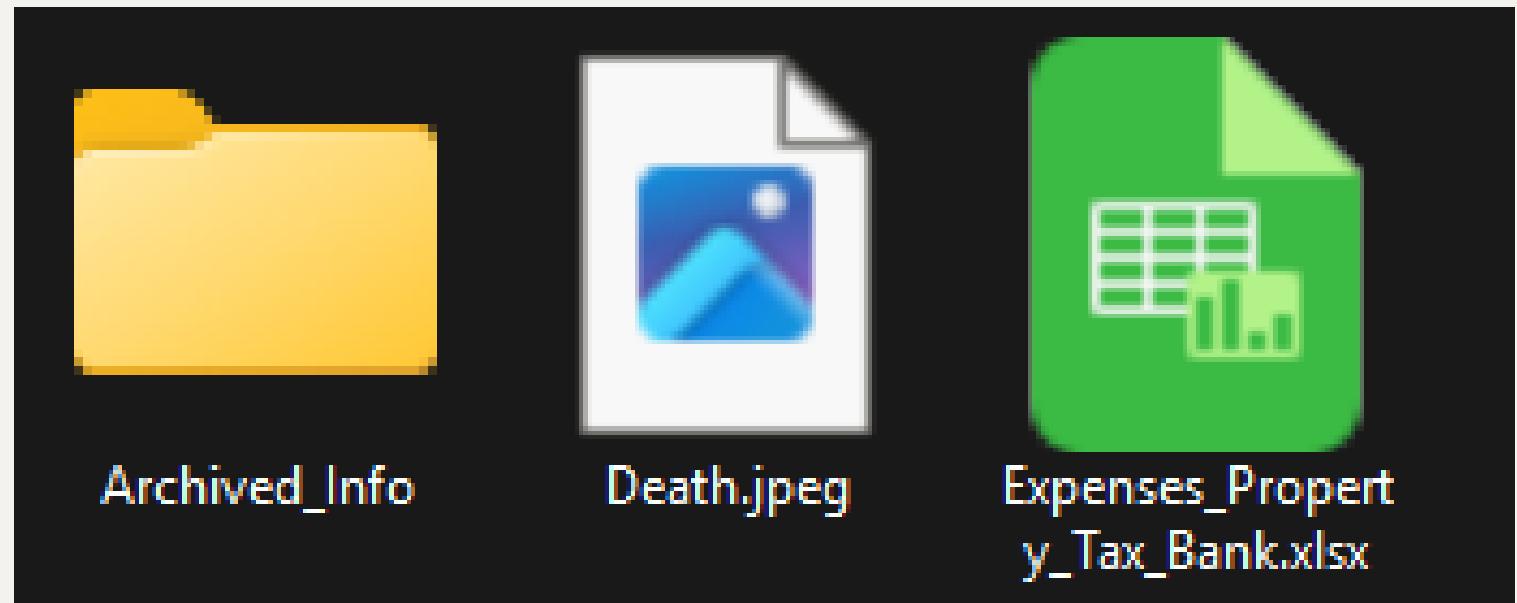
SHAS12



ROT13

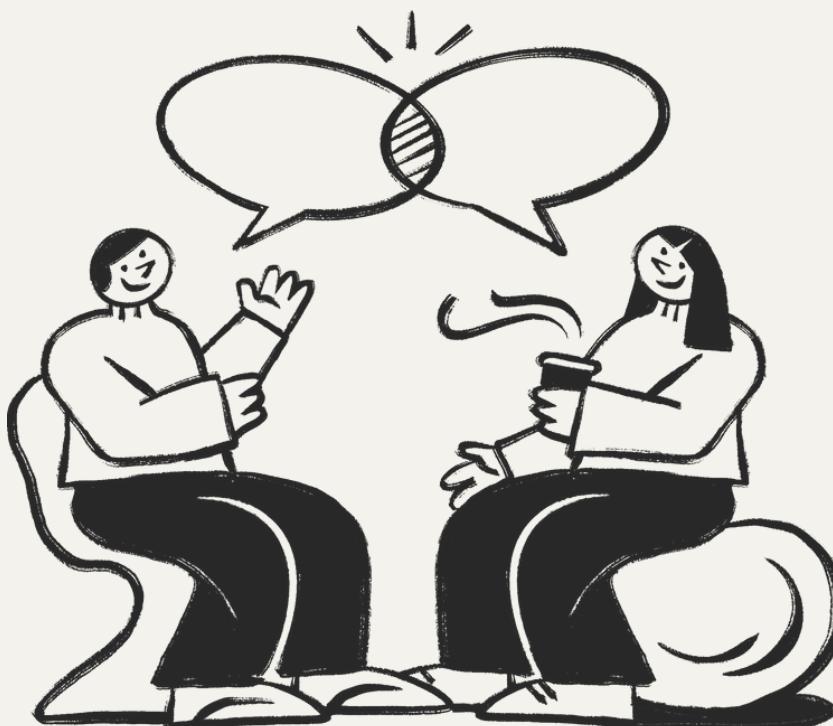


INSIDE QVYKHU



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!!

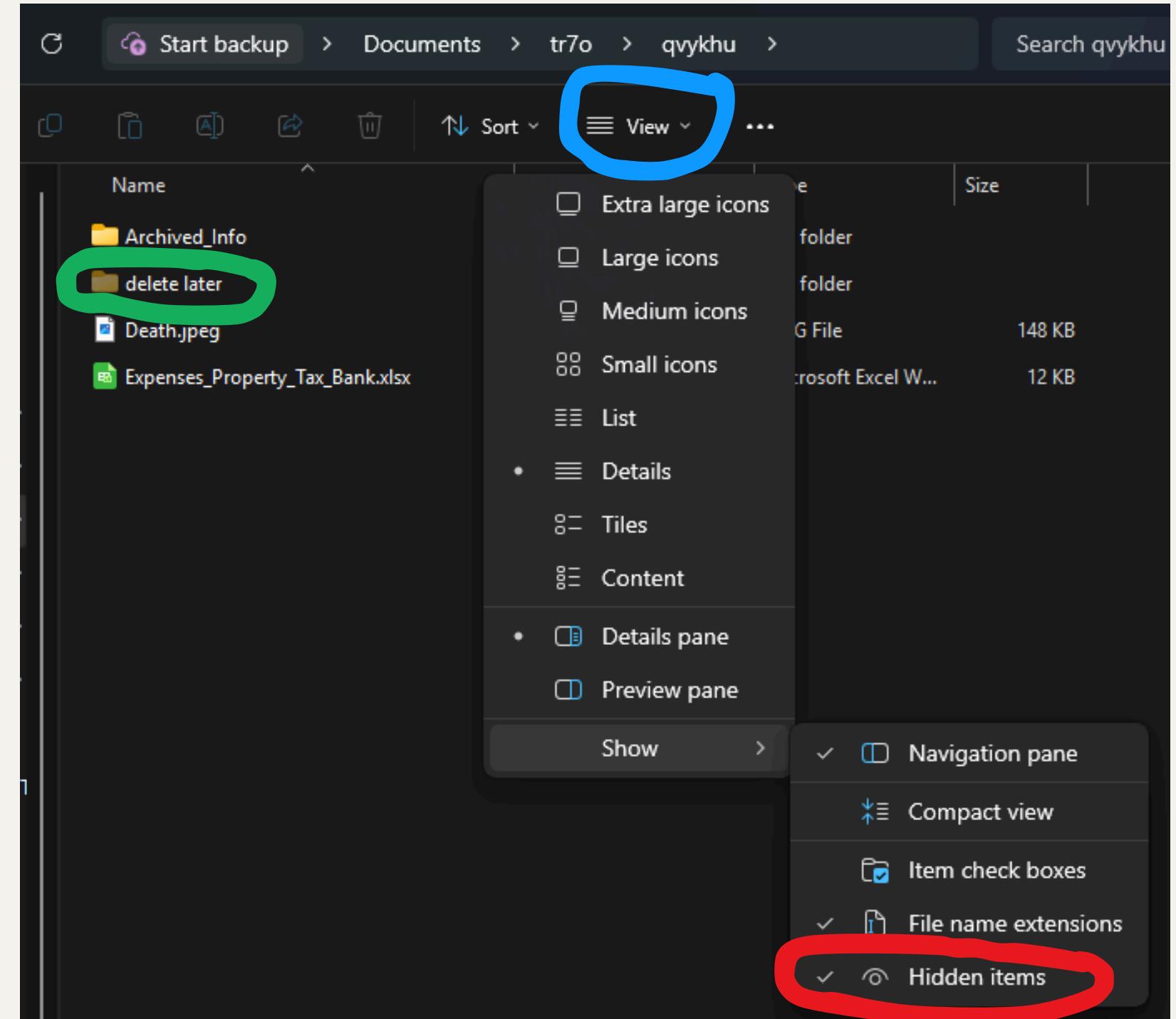




HIDDEN FOLDER

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.



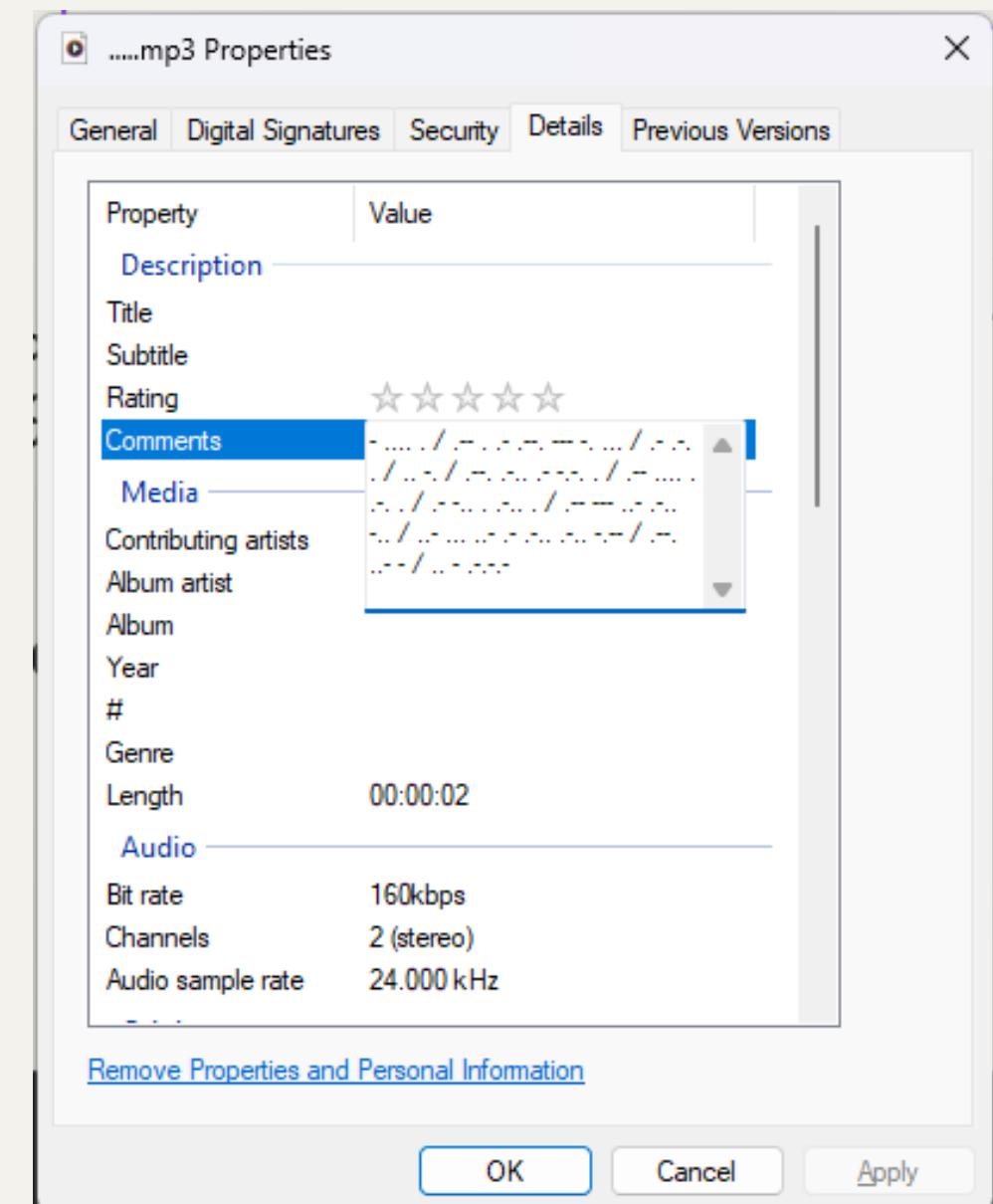
INSIDE "DELETE LATER"

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."



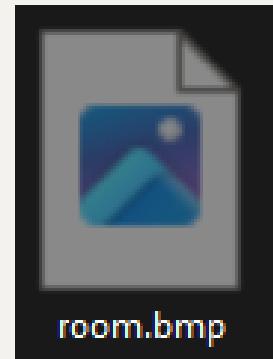
Input:

```
.... / .-- .-. -.- - - . ... / .. - .-. / ..  
. .- . . / .-- - - .. - .. - .. / .. - .. - .. - ..  
. - .. - .. - .. / .-- . - - / .. - .. - .. - ..
```

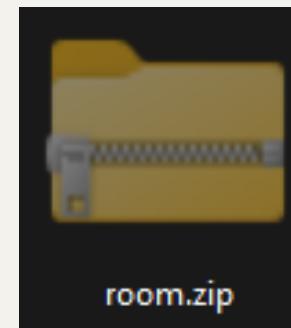
Output:

THE WEAPONS ARE IN PLACE WHERE ADELE WOULD USUALLY PUT IT.

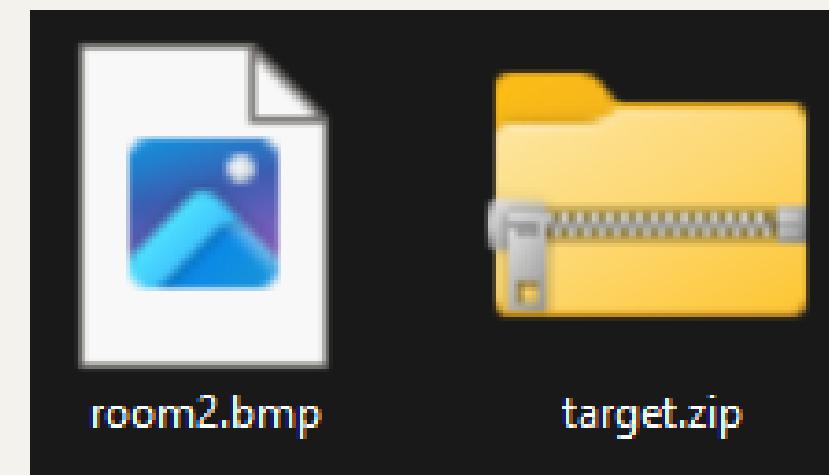
ROOM.BMP

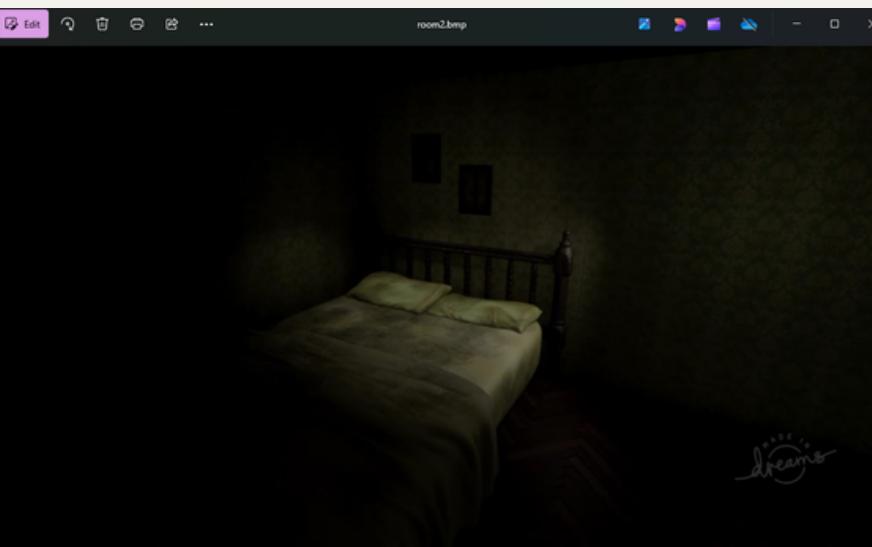


- If we open the "room.bmp", we would get nothing displayed

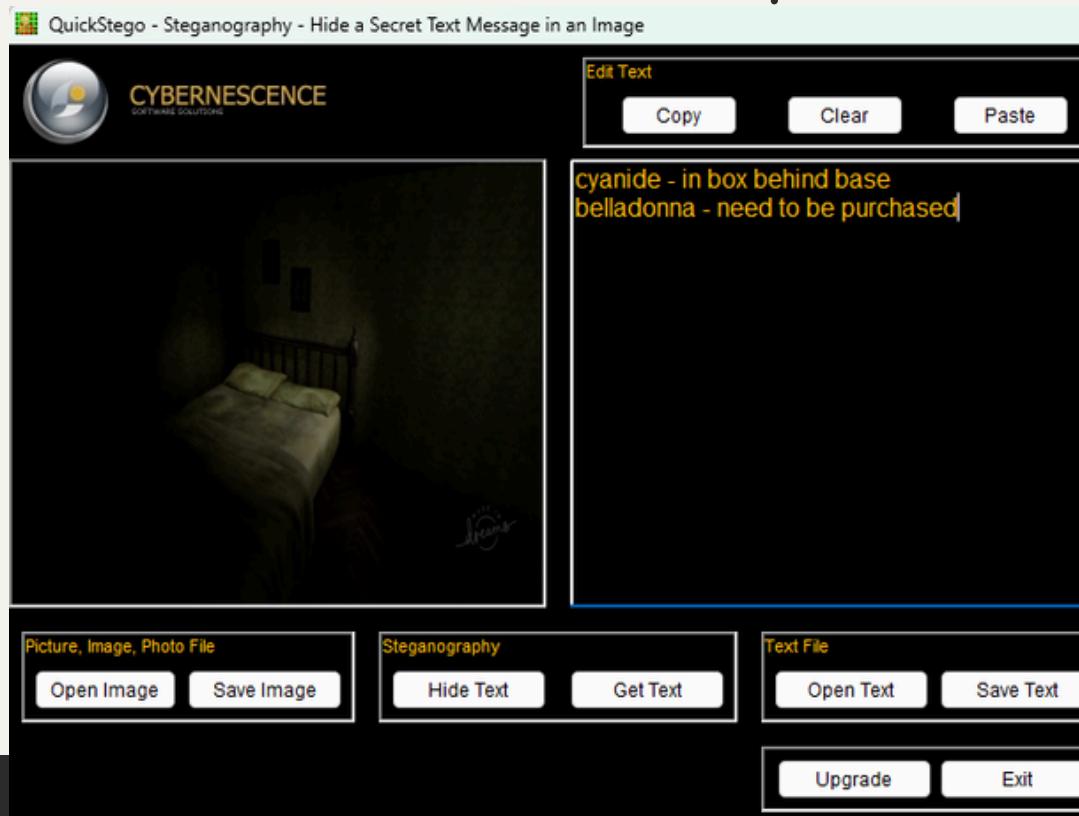


- But if we rename the file to "room.zip", we can open the zip and see that there are 2 more files
- a "room2.bmp"
- a "target.zip" that contains an image of their next target





"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"



**LASTLY,
ROOM2.BMP**





THANK YOU FOR
LISTENING!