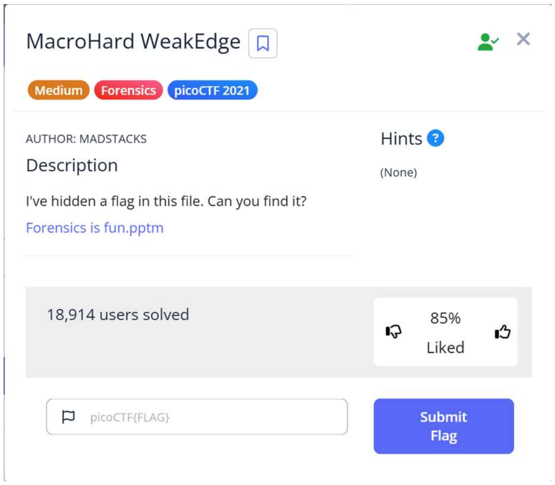
**MacroHard WeakEdge**
By: Achideon (?!)



MacroHard WeakEdge

Medium Forensics picoCTF 2021

AUTHOR: MADSTACKS

Description

I've hidden a flag in this file. Can you find it?

Forensics is fun.pptm

Hints

(None)

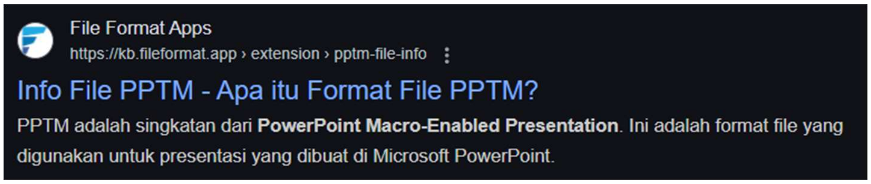
18,914 users solved

85%
Liked

picoCTF{FLAG}

Submit Flag

Take a look at this challenge yeah
The given file is in format of '.pptm', a quick google search shows this

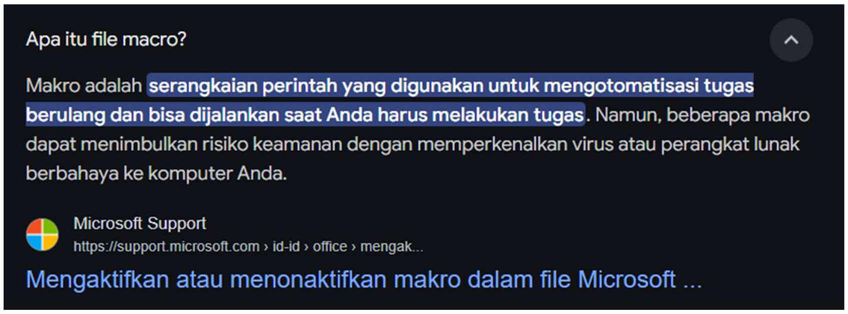


File Format Apps
https://kb.fileformat.app › extension › pptm-file-info

Info File PPTM - Apa itu Format File PPTM?

PPTM adalah singkatan dari **PowerPoint Macro-Enabled Presentation**. Ini adalah format file yang digunakan untuk presentasi yang dibuat di Microsoft PowerPoint.

Well most likely this challenge is linked with macros, but what is macro?



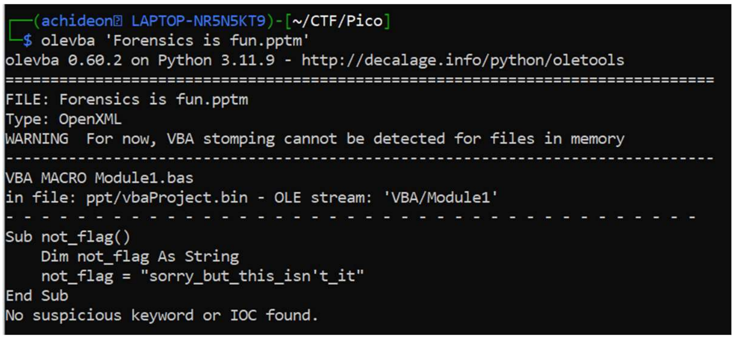
Apa itu file macro?

Makro adalah serangkaian perintah yang digunakan untuk mengotomatisasi tugas berulang dan bisa dijalankan saat Anda harus melakukan tugas. Namun, beberapa makro dapat menimbulkan risiko keamanan dengan memperkenalkan virus atau perangkat lunak berbahaya ke komputer Anda.

Microsoft Support
https://support.microsoft.com › id-id › office › mengak...

Mengaktifkan atau menonaktifkan makro dalam file Microsoft ...

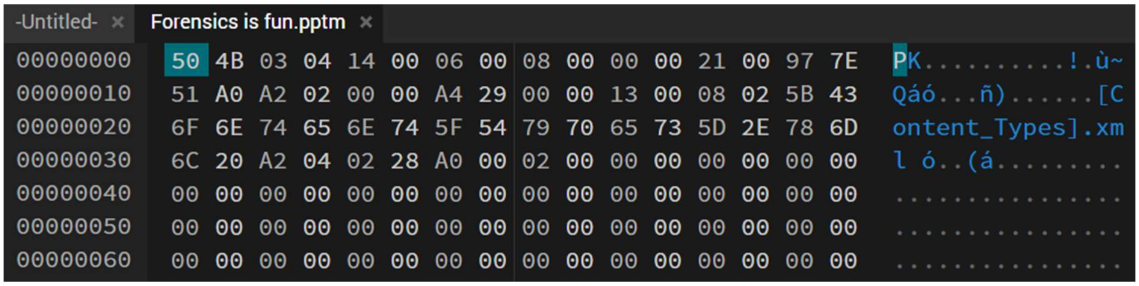
TL;DR Macro is a line of code that is run when you open a file (which, usually an Office file)
So I tried to check the macro inside this .pptm file using 'olevba' (shoutout to Billy for introducing me to this), however it leads to a dead end



```
┌──(achideon㉿ LAPTOP-NR5N5KT9)-[~/CTF/Pico]
└─$ olevba 'Forensics is fun.pptm'
olevba 0.60.2 on Python 3.11.9 - http://decalage.info/python/oletools
===============================================================================
FILE: Forensics is fun.pptm
Type: OpenXML
WARNING  For now, VBA stomping cannot be detected for files in memory
-------------------------------------------------------------------------------
VBA MACRO Module1.bas
in file: ppt/vbaProject.bin - OLE stream: 'VBA/Module1'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Sub not_flag()
    Dim not_flag As String
    not_flag = "sorry_but_this_isn't_it"
End Sub
No suspicious keyword or IOC found.
```

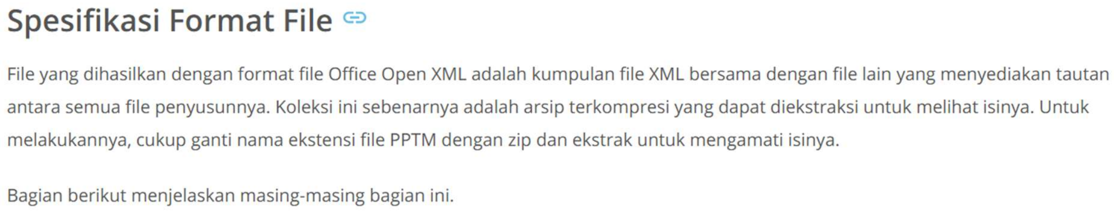
life_is_not_daijobu.jpeg

Well since it’s a forensics challenge my first instinct was to check the hex, and turns out the hex has something in it



```
00000000  50 4B 03 04 14 00 06 00 08 00 00 00 21 00 97 7E  PK..........!.ù~
00000010  51 A0 A2 02 00 00 A4 29 00 00 13 00 08 02 5B 43  Qáó...ñ)......[C
00000020  6F 6E 74 65 6E 74 5F 54 79 70 65 73 5D 2E 78 6D  ontent_Types].xm
00000030  6C 20 A2 04 02 28 A0 00 02 00 00 00 00 00 00 00  l ó..(á.........
00000040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

Does it feel familiar? It’s because 0x504b0304 is in fact a zip file header, that means this .pptm file can be opened as a zip file
(apparently the .pptm format can be converted into .zip format)

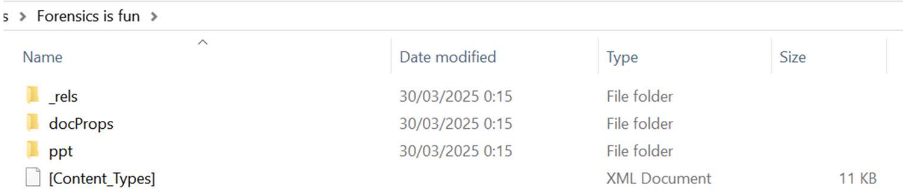


## Spesifikasi Format File

File yang dihasilkan dengan format file Office Open XML adalah kumpulan file XML bersama dengan file lain yang menyediakan tautan antara semua file penyusunnya. Koleksi ini sebenarnya adalah arsip terkompresi yang dapat diekstraksi untuk melihat isinya. Untuk melakukannya, cukup ganti nama ekstensi file PPTM dengan zip dan ekstrak untuk mengamati isinya.

Bagian berikut menjelaskan masing-masing bagian ini.

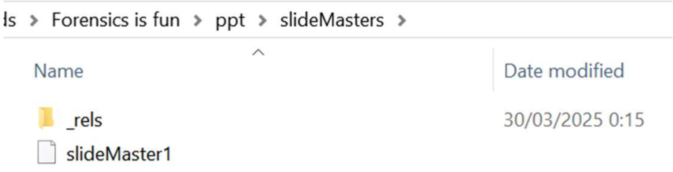
Extracted the zip, and now we have a folder full of the contents inside the .pptm file



| Name | Date modified | Type | Size |
|---|---|---|---|
| _rels | 30/03/2025 0:15 | File folder | |
| docProps | 30/03/2025 0:15 | File folder | |
| ppt | 30/03/2025 0:15 | File folder | |
| [Content_Types] | | XML Document | 11 KB |

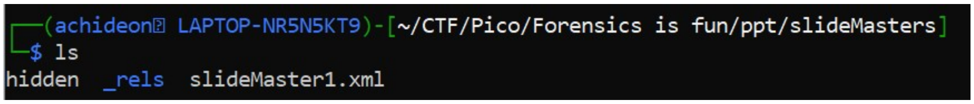
(yippeee)

I admit, this is where I went wrong, I spent hours looking at the xml files which in fact is just the builder file for .pptm, turns out you have to open the folder inside Linux to view the hidden file



| Name | Date modified |
|---|---|
| _rels | 30/03/2025 0:15 |
| slideMaster1 | |

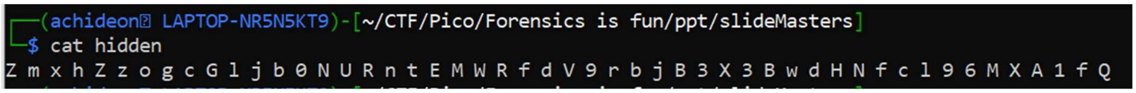
(in Windows)



```
┌──(achideon㉿ LAPTOP-NR5N5KT9)-[~/CTF/Pico/Forensics is fun/ppt/slideMasters]
└─$ ls
hidden  _rels  slideMaster1.xml
```

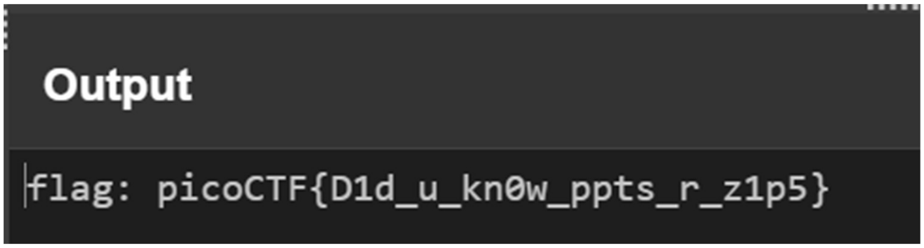
(in Linux)

Well looking inside the ‘hidden’ file I found a base64 code



```
┌──(achideon㉿ LAPTOP-NR5N5KT9)-[~/CTF/Pico/Forensics is fun/ppt/slideMasters]
└─$ cat hidden
Z m x h Z z o g c G l j b 0 N U R n t E M W R f d V 9 r b j B 3 X 3 B w d H N f c l 9 6 M X A 1 f Q
```

After decyphering the code we will get the flag needed



Output

```
flag: picoCTF{D1d_u_kn0w_ppts_r_z1p5}
```

Problem solved
flag: picoCTF{D1d_u_kn0w_ppts_r_z1p5}

(picture unrelated)
(ak mw dapet SSS di USM master T_T)