Forensics: Forensics 0x0002

Value : **300 Pts**

Description :

1. identify the file format.
2. read about the file format.
3. see which properties this particular file has.
4. and fix the file to get the flag.
5. brute-forcing won't help but you can do whatever you want.
6. flag format ritsCTF{<---flag-here--->}.
Good Luck.!

Attachment : **flag002.zip**

Solutions :

As we can see the attachment file is a zip with **flag.txt** file on it. Running **7zip** on it for extract it content show an "**Headers**" error, and the archive is password protected.

```
root@kali:/home/kali/Desktop# 7z x flag002.zip

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits
65U CPU @ 1.80GHz (806EB),ASM,AES-NI)

Scanning the drive for archives:
1 file, 165 bytes (1 KiB)

Extracting archive: flag002.zip

ERRORS:
Headers Error

--
Path = flag002.zip
Type = zip
ERRORS:
Headers Error
Physical Size = 165



Archives with Errors: 1

Open Errors: 1
```

I fixed it using **zip** and the parameter "**-FF**" for force fix the zip file.

```
root@kali:/home/kali/Desktop# zip -FF flag002.zip --out fixed.zip
Fix archive (-FF) - salvage what can
 Found end record (EOCDR) - says expect single disk archive
Scanning for entries...
 copying: flag.txt  (51 bytes)
Central Directory found...
EOCDR found ( 1    143)...
```

Trying to unzip the **fixed.zip** file give me a empty directory named **flag.txt**, so I tried to extract the content of **fixed.zip** with **binwalk** and it worked.

```
root@kali:/home/kali/Desktop# binwalk -e fixed.zip

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Zip archive data, at least v2.0 to extract, compressed
pressed size: 51, name: flag.txt
143           0x8F            End of Zip archive, footer length: 22

root@kali:/home/kali/Desktop# cd _fixed.zip.extracted/
root@kali:/home/kali/Desktop/_fixed.zip.extracted# ls
0.zip  flag.txt
root@kali:/home/kali/Desktop/_fixed.zip.extracted# cat flag.txt
riftCTF{Y0u-M4st33r3-THE_ZIP_FILE-\x50\x4B\x01\x02}root@kali:/home/kali/Desktop/_fixe
```

Flag : riftCTF{Y0u-M4st33r3-THE_ZIP_FILE-\x50\x4B\x01\x02}