Forensics : Forensics 0x0001

Value : **100 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 : **flag1.zip**

Solutions :

As we can see the attachment file is a zip with flag.txt on it. Runing 7zip on it for extract his content show an “Headers” error, and the archive seem to ask a password.

```
root@kali:/home/kali/Desktop# 7z x flag1.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, 260 bytes (1 KiB)

Extracting archive: flag1.zip

ERRORS:
Headers Error

--
Path = flag1.zip
Type = zip
ERRORS:
Headers Error
Physical Size = 260


Enter password (will not be echoed):
```

To fix it I used zip with the parameter “-FF” to force fix the zip file.

```
root@kali:/home/kali/Desktop# zip -FF flag1.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  (72 bytes)
Central Directory found...
EOCDR found ( 1    238)...
```

Then I used zip2john to convert the zip to a hash to crack with john.

```
root@kali:/home/kali/Desktop# zip2john new.zip > crackme
ver 2.0 efh 9901 new.zip/flag.txt PKZIP Encr: cmplen=72, decmplen=42, crc=9EC50084
```

Finally we crack it with john.

```
root@kali:/home/kali/Desktop# john --wordlist=/usr/share/wordlists/rockyou.txt crackme
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 128/128 AVX 4x])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
general          (new.zip/flag.txt)
1g 0:00:00:00 DONE (2020-04-07 11:16) 7.142g/s 29257p/s 29257c/s 29257C/s 123456..oooooo
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Extract the zip file with the cracked password and read your flag inside the extracted flag.txt file.

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

```
root@kali:/home/kali/Desktop# cat flag.txt
riftCTF{th1s-1S-_JUST--TH3-B3g3nn1ng-BRUH}
```

Flag : riftCTF{th1s-1S_JUST--TH3-B3g3nn1ng-BRUH}