Write-Up for CTF OPEN 2019 Semi-Final

Name: Wong Ka Chung (ElderHorse)
Team: GRAD501

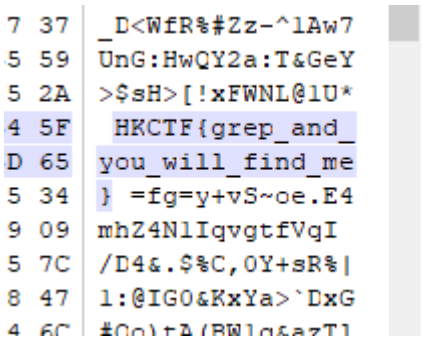
Simple Forensics

Given:
Can you find the flag in this file?

Simply put it into winhex

Use hotkey Ctrl + F and search "HKCTF"

Flag: HKCTF{grep_and_you_will_find_me}



Broken string

Given:
My secret string was broken because of fire. Can you help to decode?

Convert "VEZ7dGg0dF93NHNfYV" from base64 to ascii and get "TF{th4t_w4s_a"

A logical relationship can be made that appending the first broken part is "HKCTF{th4t_w4s_a"

Similarly, inputing "TDNfcXUzc3RpMG" and we can observed that the result is "L3_qu3sti0"

I made a guess that the missing part is "n}", inputing "0n}" results in "MG59"

This matchs the last part of the broken string "MG"

So the string is now "HKCTF{th4t_w4s_a(unknown)L3_qu3sti0n}"

I thought the word might be simple, converting i to 1

Flag: "HKCTF{th4t_w4s_a_s1mpL3_qu3sti0n}"

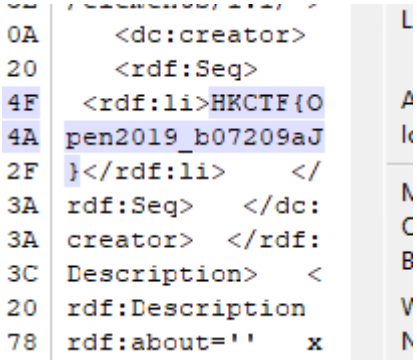
Good Image

Given:
Can you help us find the flag in this image?

Simply put it into winhex

Use hotkey Ctrl + F and search "HKCTF"

Flag: HKCTF{Open2019_b07209aJ}



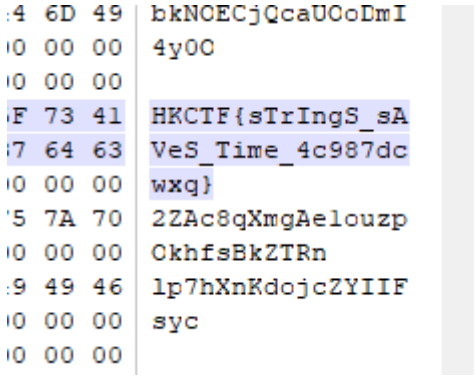
Simple Forensics 2

Given:
Can you find the flag in this file?

Simply put it into winhex

Use hotkey Ctrl + F and search "HKCTF"

Flag: HKCTF{sTrIngS_sAVeS_Time_4c987dcwxq}



Spider man

Given:
Where the spider can't access, where the answer is.

Please access it on http://13.251.58.69:8003

The word spider reminds me the web crawler

A place that a spider can't access should be the robots.txt

Enter http://13.251.58.69:8003/robots.txt

A txt file can be downloaded

Putting it into winhex, we can observe that it has a png header

Convert the extension into png

After observing the png, it seems to be related to npiet

Using the npiet online: https://www.bertnase.de/npiet/npiet-execute.php to execute the image

Flag: HKCTF{Npi3t_Ez_23j2n#S}

```
libpng warning: Extra compressed data.
libpng warning: Extra compression data.
HKCTF{Npi3t_Ez_23j2n#S}HKCTF{Npi3t_Ez_23j2n#S}HKC
```

Simple APK

Given:
A zip file named "app_release.apk.zip"

Unzip it and found a file named "app_release.apk"

Simply put it into winhex

Use hotkey Ctrl + F and search "HKCTF"

Flag: HKCTF{pwyorowkw3}