

# 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}

```
7 37 _D<WfR%#Zz-^1Aw7
5 59 UnG:HwQY2a:T&GeY
5 2A >$sH>[!xFWNL@1U*
4 5F HKCTF{grep_and_
D 65 you_will_find_me
5 34 } =fg=y+vS~oe.E4
9 09 mhZ4NlIqvgtfVqI
5 7C /D4&.$%C,0Y+sR%|
8 47 1:@IG0&KxYa>`DxG
4 6C #Qn)+A/RWlq&azT1
```

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}

```
0A    <dc:creator>
20    <rdf:Seq>
4F    <rdf:li>HKCTF{O
4A    pen2019_b07209aJ
2F    }</rdf:li>    </
3A    rdf:Seq>    </dc:
3A    creator>    </rdf:
3C    Description>    <
20    rdf:Description
78    rdf:about=''    x
```

## 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}

```
.:4 6D 49 | bkNOECjQcaUOoDmI
:0 00 00 | 4y00
:0 00 00 |
:F 73 41 | HKCTF{sTrIngS_sA
:7 64 63 | VeS_Time_4c987dc
:0 00 00 | wxq}
:5 7A 70 | 2ZAc8qXmgAelouzp
:0 00 00 | OkhfsBkZTRn
:9 49 46 | lp7hXnKdojcZYIIF
:0 00 00 | syc
:0 00 00 |
```

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}

```
9 65 app.AppCompatVie
E 73 wInflater sans
3 41 -serif-light A
F 72 pp HKCTF{pwyor
3 65 owkw3} sans-se
6 46 rif 999+ OFF
4 65 ON Navigate
E 20 up Choose an
6 00 app Searchâ€¦
0 08 Search query
```