StringCheese

How to get 15 first bloods in 15 seconds

About the author

Mathis HAMMEL

@MathisHammel

Head of Cybersecurity R&D @ Sogeti
Co-founder, Challenge Designer @ h25

Let’s solve some challs!

But how does it work? 😖

Underlying algorithm

Under the hood : `strings | grep FLAG{`

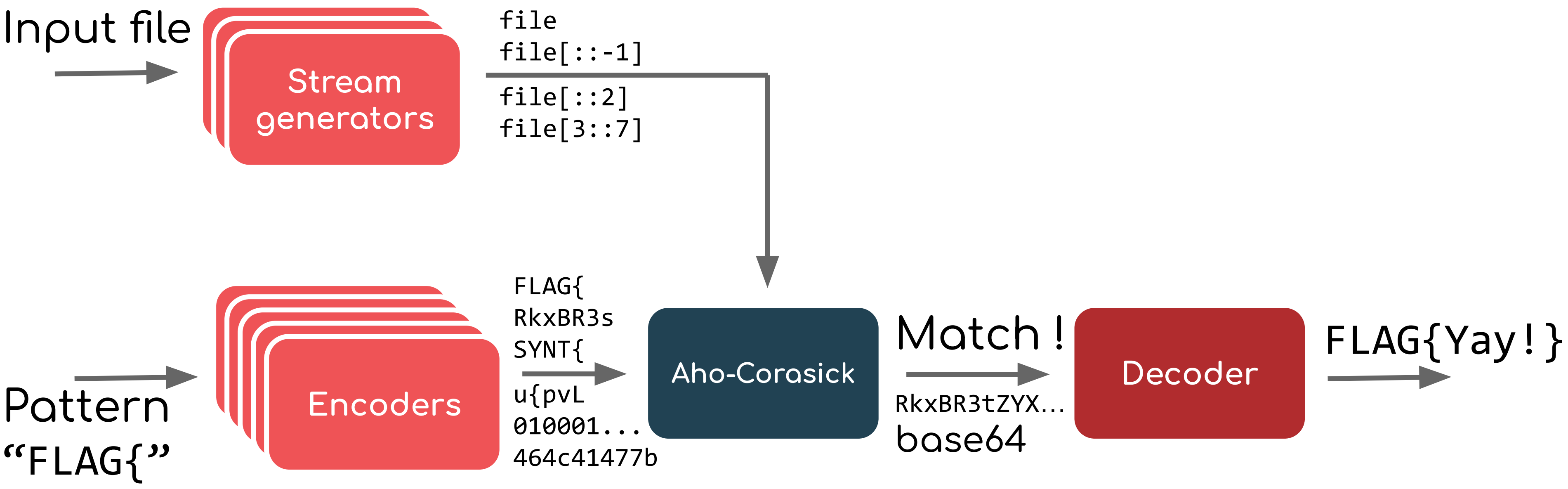
with cocaine and steroids

Pattern matching

Use of the Aho-Corasick Algorithm

- Single stream, multiple patterns
- Formerly used in grep
- Fast implementation in C

Flag processing



Input file

Stream generators

```
file
file[::-1]
file[::2]
file[3::7]
```

Pattern "FLAG{"

Encoders

```
FLAG{
RkxBR3s
SYNT{
u{pvL
010001...
464c41477b
```

Aho-Corasick

Match !

RkxBR3tZYX...

base64

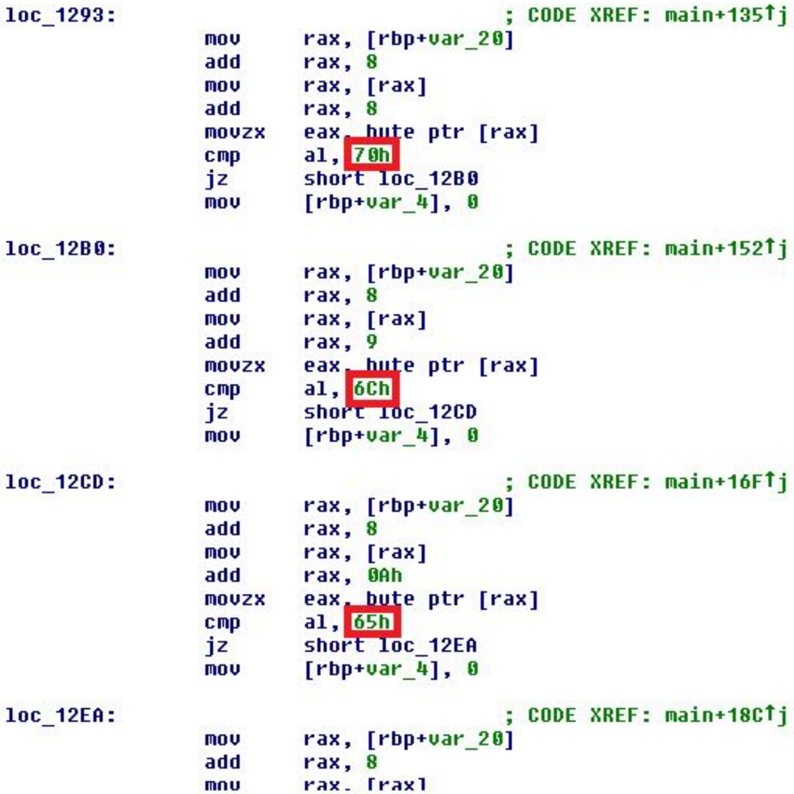
Decoder

FLAG{Yay!}

Pattern matching

Detect any (implemented) encoding with regular spacing inside the file

Pattern matching

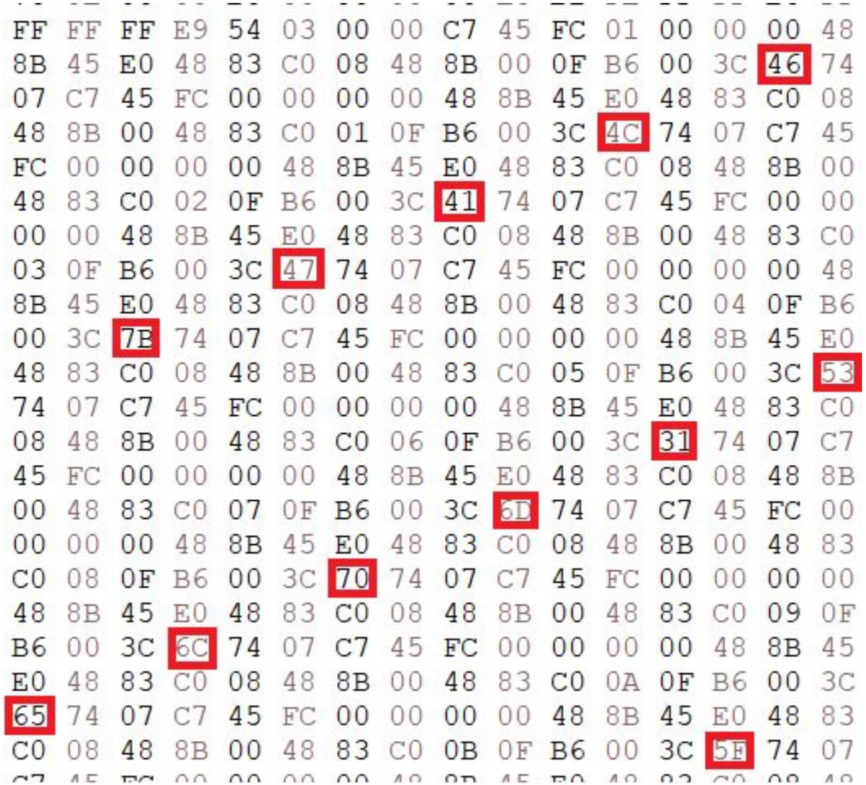


```
loc_1293:                               ; CODE XREF: main+135↑j
                mov     rax, [rbp+var_20]
                add     rax, 8
                mov     rax, [rax]
                add     rax, 8
                movzx   eax, byte ptr [rax]
                cmp     al, 70h
                jz      short loc_12B0
                mov     [rbp+var_4], 0

loc_12B0:                               ; CODE XREF: main+152↑j
                mov     rax, [rbp+var_20]
                add     rax, 8
                mov     rax, [rax]
                add     rax, 9
                movzx   eax, byte ptr [rax]
                cmp     al, 6Ch
                jz      short loc_12CD
                mov     [rbp+var_4], 0

loc_12CD:                               ; CODE XREF: main+16F↑j
                mov     rax, [rbp+var_20]
                add     rax, 8
                mov     rax, [rax]
                add     rax, 0Ah
                movzx   eax, byte ptr [rax]
                cmp     al, 65h
                jz      short loc_12EA
                mov     [rbp+var_4], 0

loc_12EA:                               ; CODE XREF: main+18C↑j
                mov     rax, [rbp+var_20]
                add     rax, 8
                mov     rax, [rax]
```



```
FF FF FF E9 54 03 00 00 C7 45 FC 01 00 00 00 48
8B 45 E0 48 83 C0 08 48 8B 00 0F B6 00 3C 46 74
07 C7 45 FC 00 00 00 00 48 8B 45 E0 48 83 C0 08
48 8B 00 48 83 C0 01 0F B6 00 3C 4C 74 07 C7 45
FC 00 00 00 00 48 8B 45 E0 48 83 C0 08 48 8B 00
48 83 C0 02 0F B6 00 3C 41 74 07 C7 45 FC 00 00
00 00 48 8B 45 E0 48 83 C0 08 48 8B 00 48 83 C0
03 0F B6 00 3C 47 74 07 C7 45 FC 00 00 00 00 48
8B 45 E0 48 83 C0 08 48 8B 00 48 83 C0 04 0F B6
00 3C 7B 74 07 C7 45 FC 00 00 00 00 48 8B 45 E0
48 83 C0 08 48 8B 00 48 83 C0 05 0F B6 00 3C 53
74 07 C7 45 FC 00 00 00 00 48 8B 45 E0 48 83 C0
08 48 8B 00 48 83 C0 06 0F B6 00 3C 31 74 07 C7
45 FC 00 00 00 00 48 8B 45 E0 48 83 C0 08 48 8B
00 48 83 C0 07 0F B6 00 3C 6D 74 07 C7 45 FC 00
00 00 00 48 8B 45 E0 48 83 C0 08 48 8B 00 48 83
C0 08 0F B6 00 3C 70 74 07 C7 45 FC 00 00 00 00
48 8B 45 E0 48 83 C0 08 48 8B 00 48 83 C0 09 0F
B6 00 3C 6C 74 07 C7 45 FC 00 00 00 00 48 8B 45
E0 48 83 C0 08 48 8B 00 48 83 C0 0A 0F B6 00 3C
65 74 07 C7 45 FC 00 00 00 00 48 8B 45 E0 48 83
C0 08 48 8B 00 48 83 C0 0B 0F B6 00 3C 5F 74 07
```

How do I use it?

```
pip install stringcheese
```

```
stringcheese FLAG{ --file chall.txt
```

or

```
cat chall.txt | stringcheese FLAG{
```

How do I help?

MathisHammel/stringcheese

Contributions are welcome!

Thanks !

Any questions ?

Mathis HAMMEL

@MathisHammel

discord.h25.io

twitch.h25.io