Fuzzy Hashes

for Reversing & Classification

About me

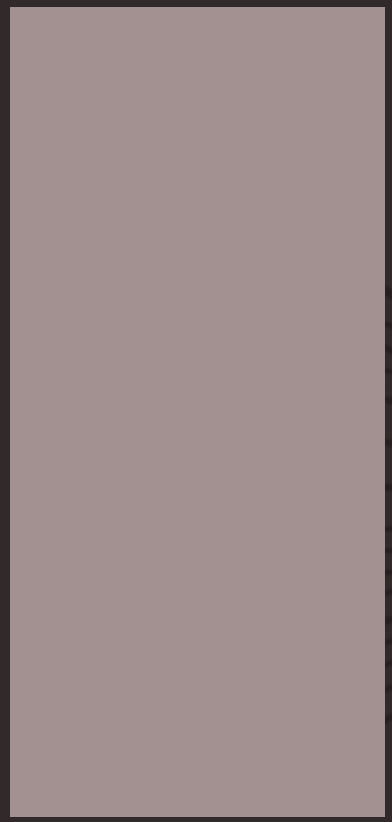
coco@hexgolems.de

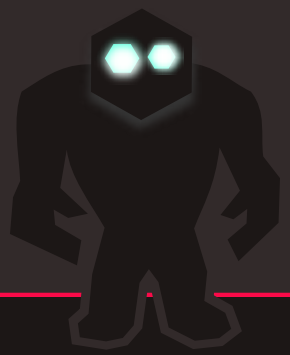
PHD student from Ruhr-Universität Bochum

RE, security, theory and bouldering

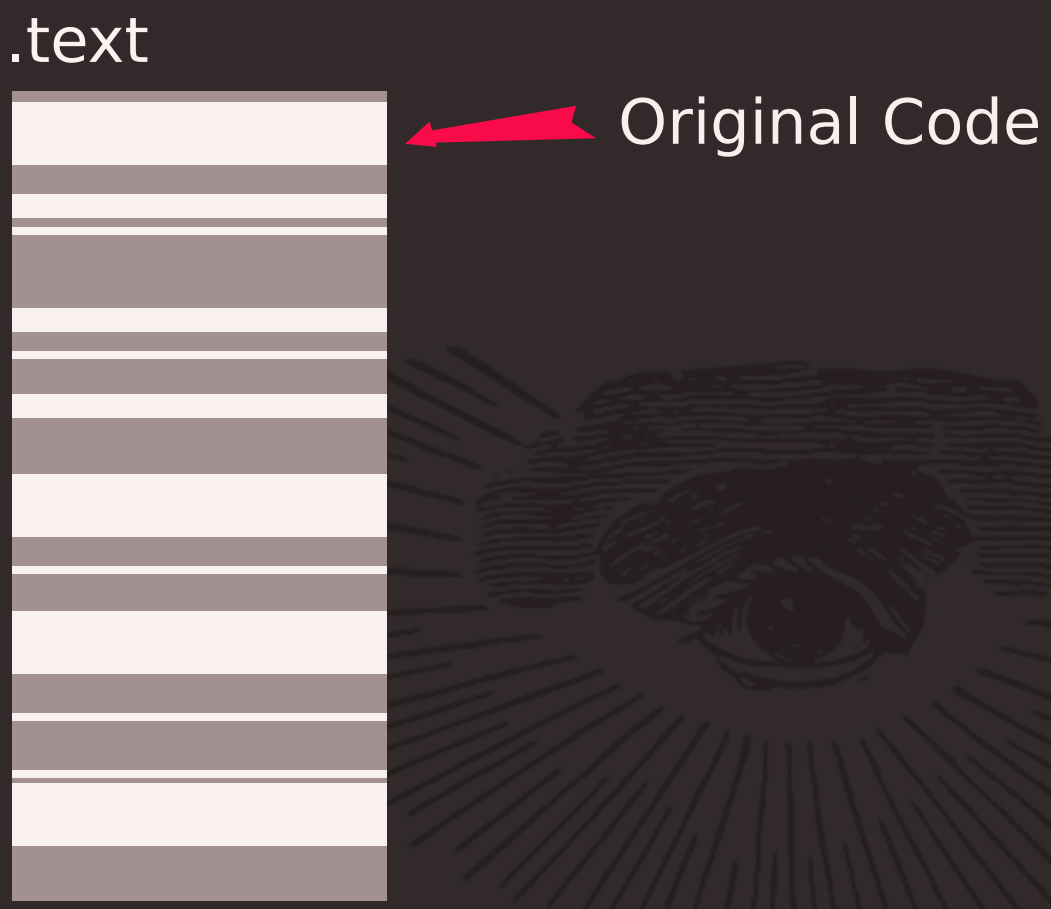
Static Linking

.text

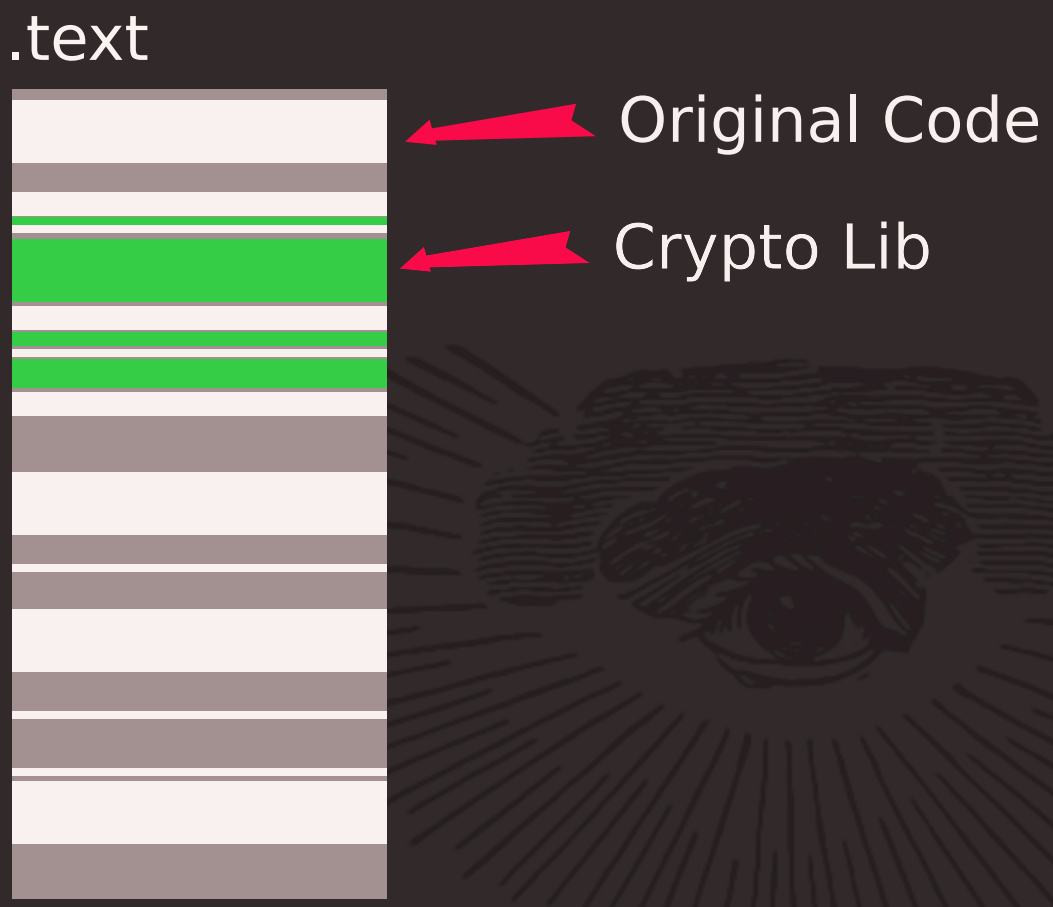




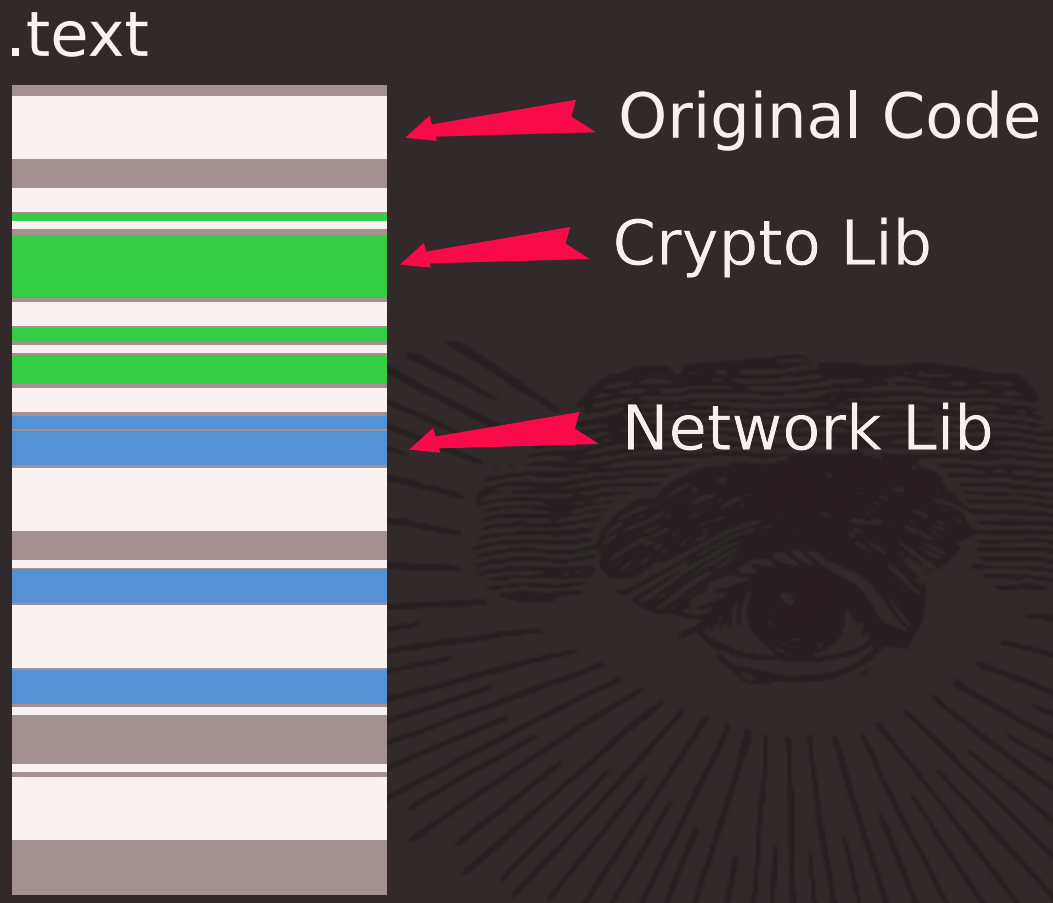
Static Linking



Static Linking

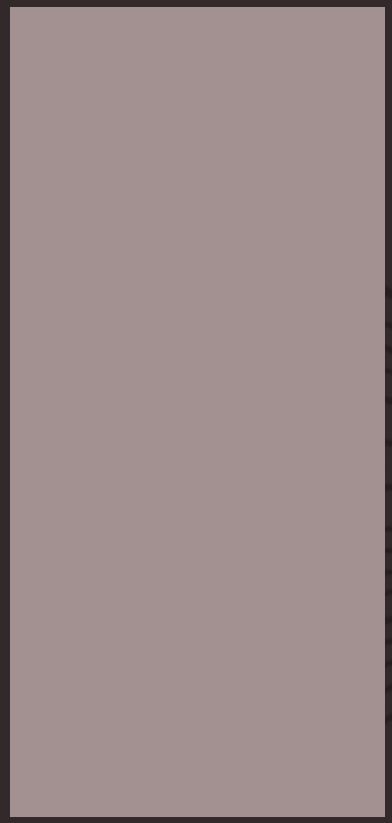


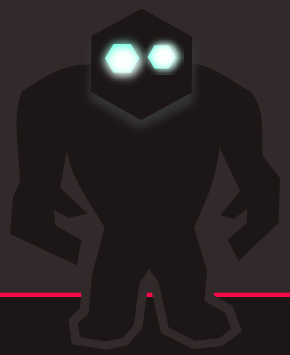
Static Linking



Malware Families

.text

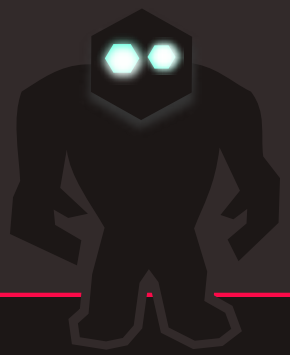




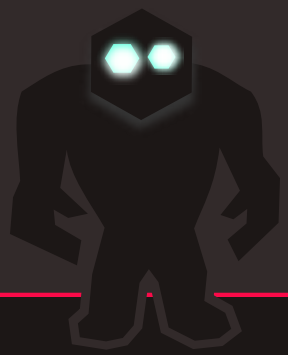
Malware Families

Malware Families

Don't do work twice



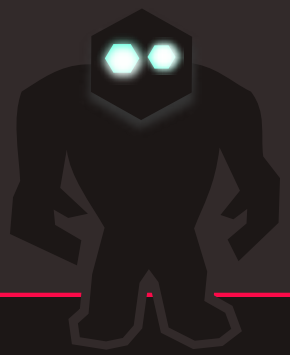
FLIRT



Fast Library Identification Technology

FLIRT

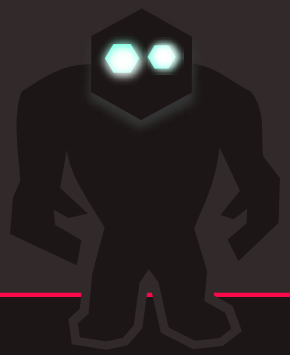
& Recognition



Cornelius Aschermann

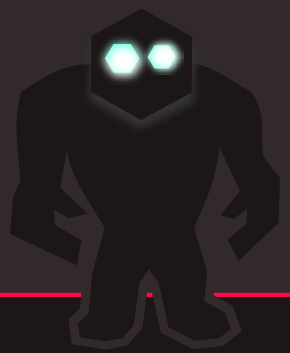
FLIRT

```
        mov     eax, 85304fh
        push    rbp
        sub     rax, 853048h
        cmp     rax, 0eh
        mov     rbp, rsp
        ja exit
        mov     eax, 0
        test    rax, rax
        jz exit
        pop     rbp
        mov     edi, 853048h
        ret
exit:
        pop     rbp
        ret
```



FLIRT

```
  mov     xxx, xxxxxx
  push    xxx
  sub     xxx, xxxxxx
  cmp     xxx, xx
  mov     xxx, xxx
  ja exit
  mov     xxx, x
  test    xxx, xxx
  jz exit
  pop     xxx
  mov     xxx, xxxxx
  ret
exit:
  pop     xxx
  ret
```

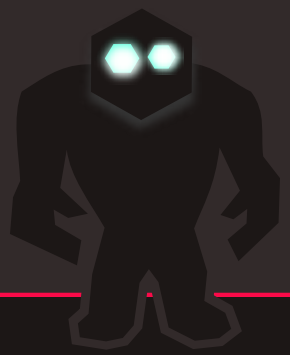


FLIRT

558Bxx0EFF7604xxxx59595xx3558BExx

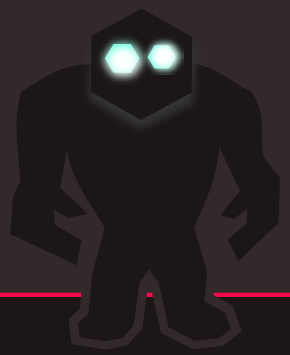
FLIRT

Compiler



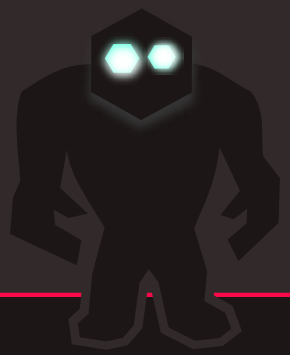
FLIRT

Compiler Version



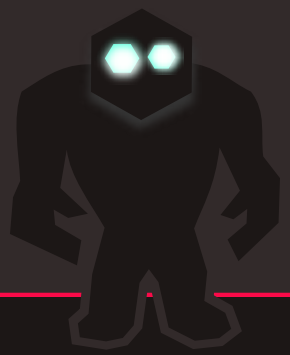
FLIRT

Compiler Flags

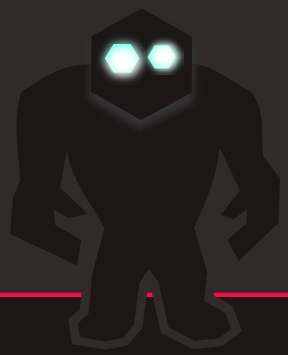


FLIRT

Other factors

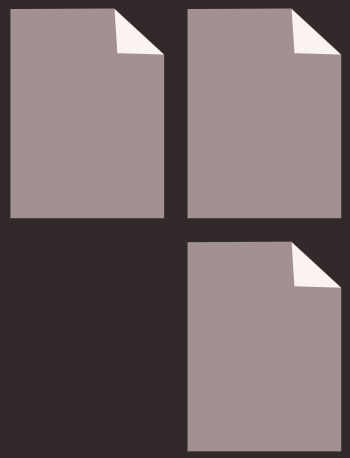


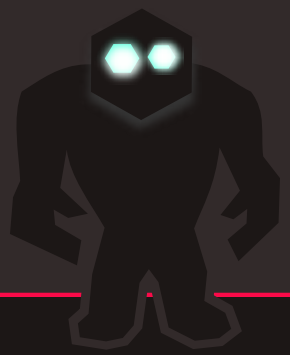
More Resilient Hash



More Resilient Hash

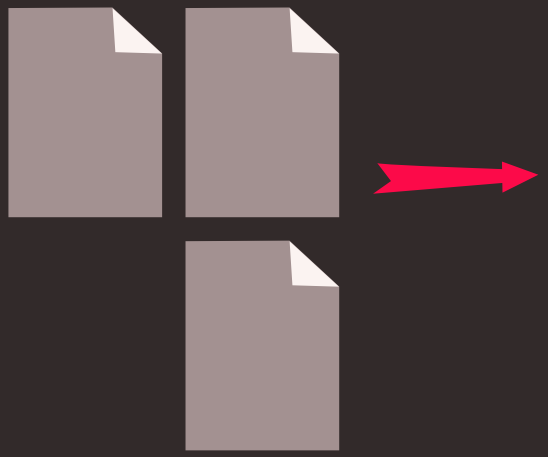
/usr/lib



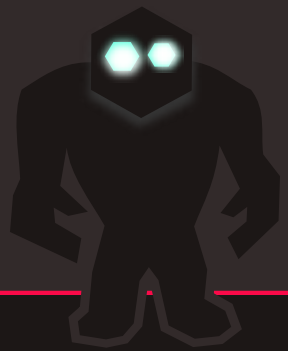


More Resilient Hash

/usr/lib



```
ld:srec_get_symbol_info    =>  acf7f7a019f7ee...
ld:reconcat                =>  bcef02e958d4ed...
ld:deflateResetKeep        =>  8fc60e4edee345...
ld:string_delete           =>  07e307fedae307...
ld:_bfd_elf_strtab_add     =>  07c6c5e99ec514...
ld:exp_binop               =>  4669f2eecdf4f4...
ld:exp_intop               =>  07faf4fadaf4f4...
ld:htab_create_alloc_ex    =>  070ef4b1dac2f4...
ld:elf_link_adjust_relocs  =>  07052229da8905...
ld:string_prepend          =>  bcef02e958d4ed...
ld:_bfd_link_section_stabs =>  07e4efe4da3a45...
```

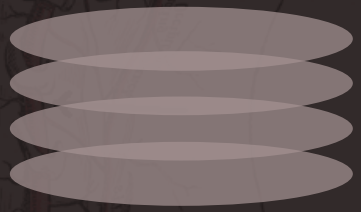


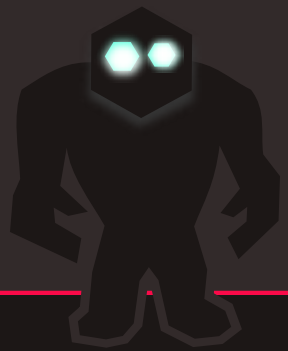
More Resilient Hash

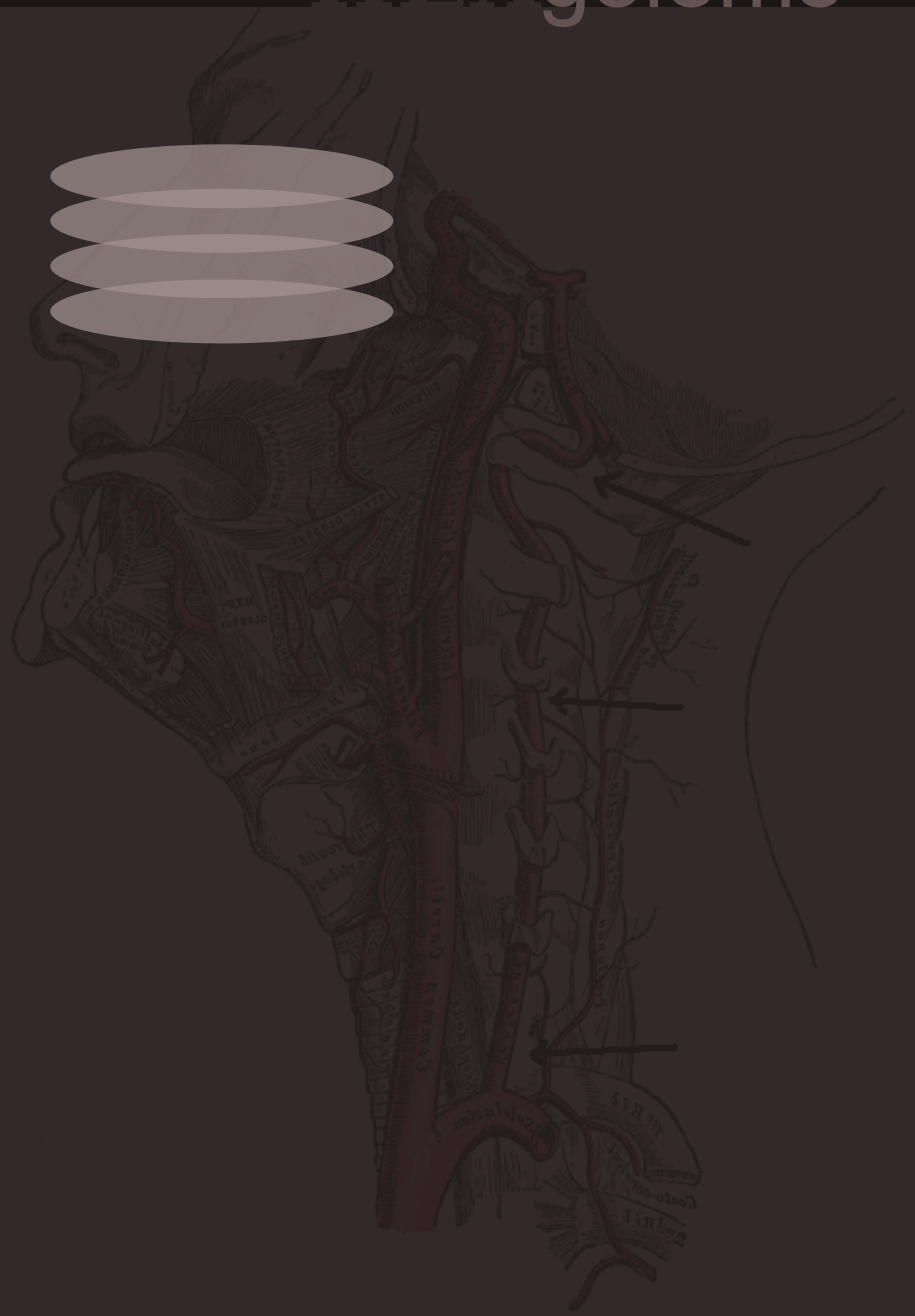
/usr/lib

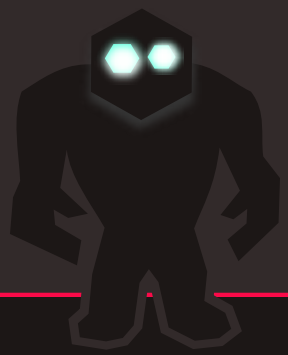
```
ld:srec_get_symbol_info    =>  acf7f7a019f7ee...
ld:reconcat                =>  bcef02e958d4ed...
ld:deflateResetKeep        =>  8fc60e4edee345...
ld:string_delete           =>  07e307fedae307...
ld:_bfd_elf_strtab_add     =>  07c6c5e99ec514...
ld:exp_binop               =>  4669f2eecdf4f4...
ld:exp_intop               =>  07faf4fadaf4f4...
ld:htab_create_alloc_ex    =>  070ef4b1dac2f4...
ld:elf_link_adjust_relocs  =>  07052229da8905...
ld:string_prepend          =>  bcef02e958d4ed...
ld:_bfd_link_section_stabs =>  07e4efe4da3a45...
```

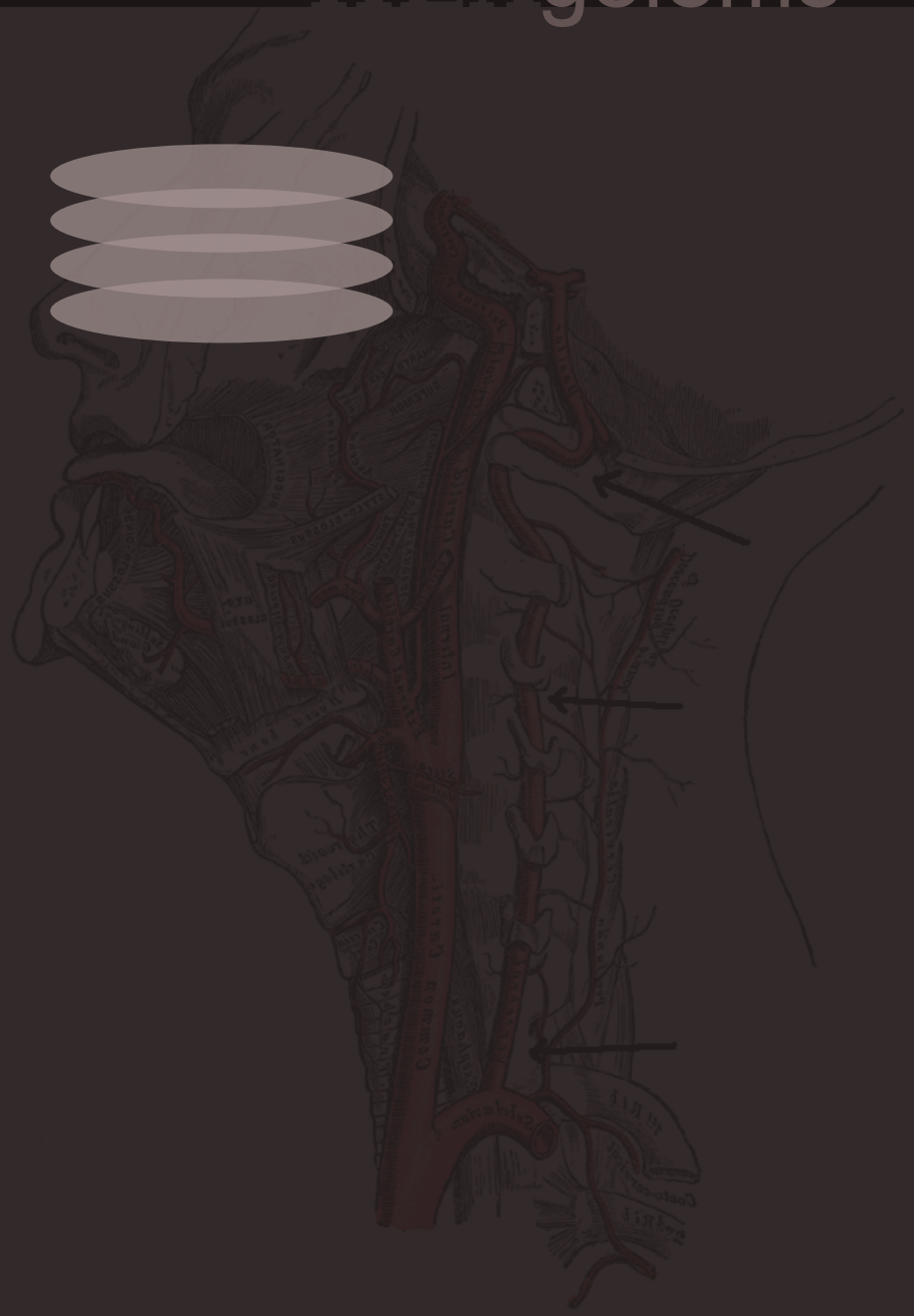
Online DB



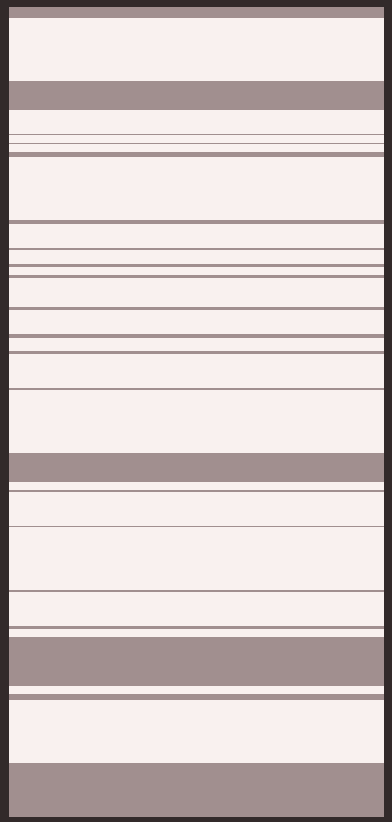


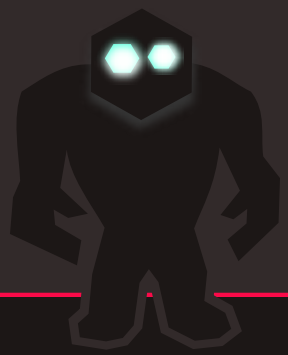


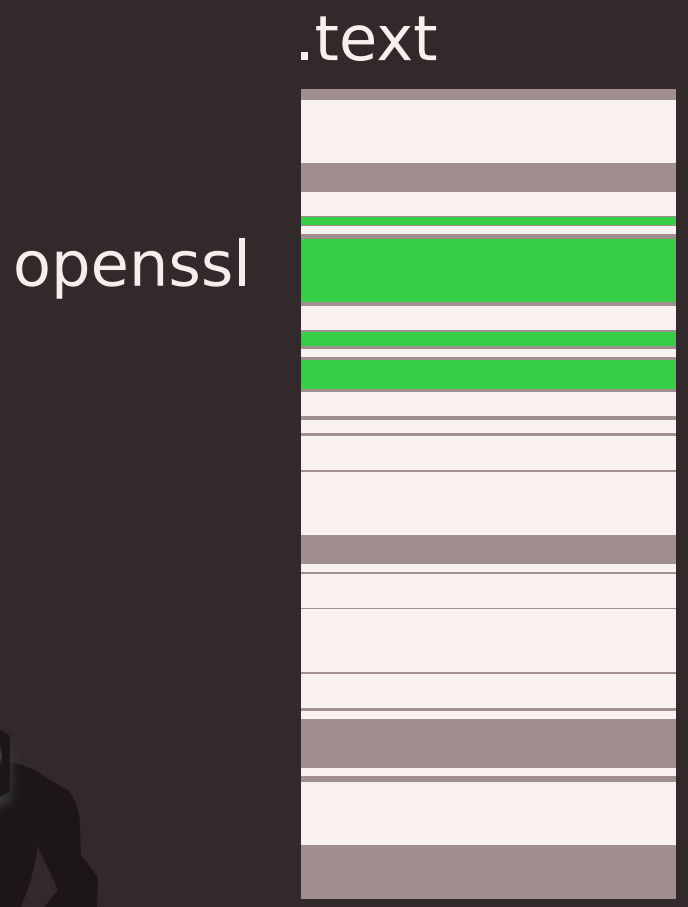


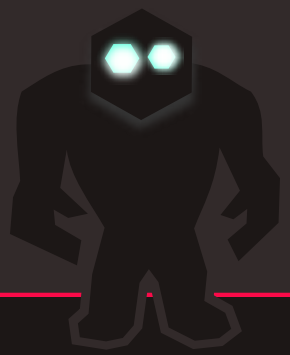


.text

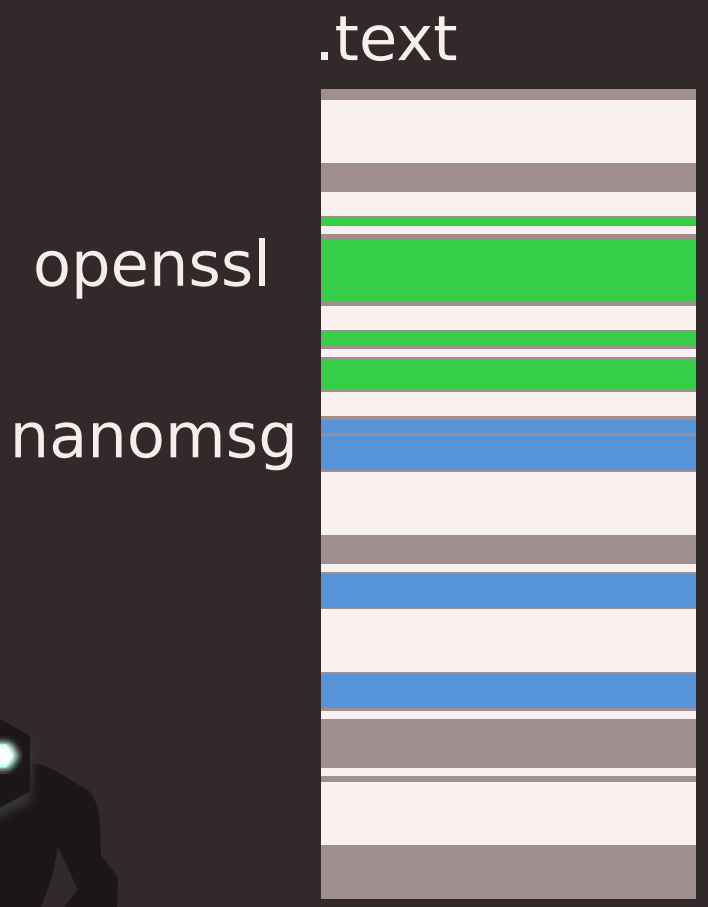





.text
openssl

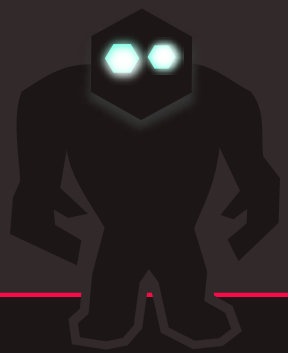



.text
openssl
nanomsg



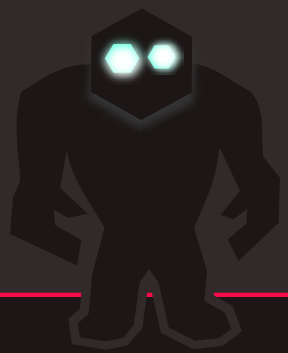
"shares 75% with ZBot.z"

Disclaimer



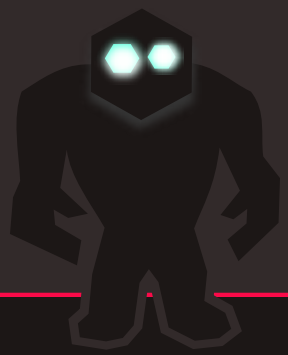
Disclaimer

Broken



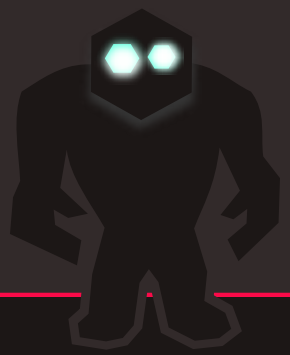
Disclaimer

Broken Inactive



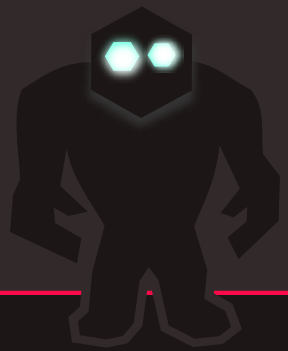
Disclaimer

Broken Inactive Research Code



Hash WHAT is DONE

(not what the code looks like)



```
mov     eax, 85304fh
push    rbp
sub     rax, 853048h
cmp     [rax], 0eh
mov     rbp, rsp
ja      exit
```

```
mov     [eax], 0
test    rax, rax
jz      exit
```

```
pop     rbp
mov     edi, 853048h
ret
```

```
exit:
pop     rbp
ret
```

```
mov     eax, 85304fh
push    rbp
sub     rax, 853048h
cmp     [rax], 0eh
mov     rbp, rsp
ja      exit
```

```
mov     [eax], 0
test    rax, rax
jz      exit
```

```
pop     rbp
mov     edi, 853048h
ret
```

```
exit:
pop     rbp
ret
```

W(0xA8..,0x4F..)

```
mov     eax, 85304fh
push    rbp
sub     rax, 853048h
cmp     [rax], 0eh
mov     rbp, rsp
ja      exit
```

```
mov     [eax], 0
test    rax, rax
jz      exit
```

```
pop     rbp
mov     edi, 853048h
ret
```

```
exit:
pop     rbp
ret
```

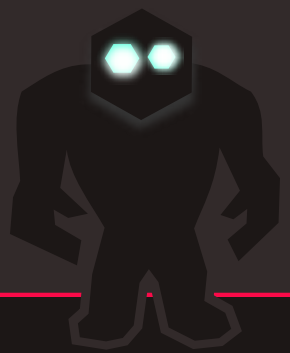
W(0xA8..,0x4F..)
R(0x37..,0x8E..)

```
mov     eax, 85304fh
push    rbp
sub     rax, 853048h
cmp     [rax], 0eh
mov     rbp, rsp
ja      exit
```

```
mov     [eax], 0
test    rax, rax
jz      exit
```

```
pop     rbp
mov     edi, 853048h
ret
```

```
exit:
pop     rbp
ret
```



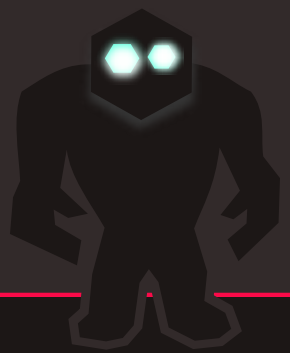
W(0xA8..,0x4F..)
R(0x37..,0x8E..)

```
mov     eax, 85304fh
push    rbp
sub     rax, 853048h
cmp     [rax], 0eh
mov     rbp, rsp
ja      exit
```

```
mov     [eax], 0
test    rax, rax
jz      exit
```

```
pop     rbp
mov     edi, 853048h
ret
```

```
exit:
pop     rbp
ret
```



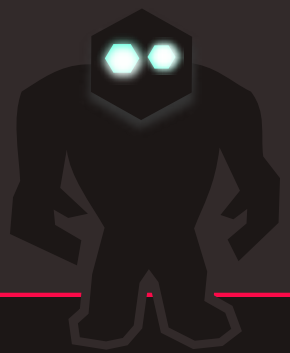
W(0xA8..,0x4F..)
R(0x37..,0x8E..)

```
mov     eax, 85304fh
push    rbp
sub     rax, 853048h
cmp     [rax], 0eh
mov     rbp, rsp
ja      exit
```

```
mov     [eax], 0
test    rax, rax
jz      exit
```

```
pop     rbp
mov     edi, 853048h
ret
```

```
exit:
pop     rbp
ret
```



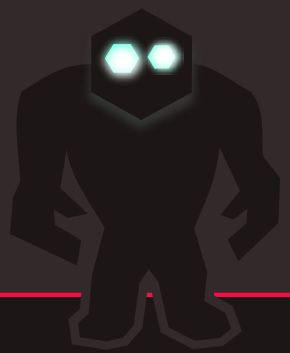
W(0xA8..,0x4F..)
R(0x37..,0x8E..)

```
mov     eax, 85304fh
push    rbp
sub     rax, 853048h
cmp     [rax], 0eh
mov     rbp, rsp
ja      exit
```

```
mov     [eax], 0
test    rax, rax
jz      exit
```

```
pop     rbp
mov     edi, 853048h
ret
```

```
exit:
pop     rbp
ret
```



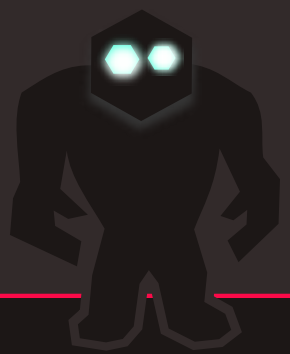
W(0xA8..,0x4F..)
R(0x37..,0x8E..)

```
mov     eax, 85304fh
push    rbp
sub     rax, 853048h
cmp     [rax], 0eh
mov     rbp, rsp
ja      exit
```

```
mov     [eax], 0
test    rax, rax
jz      exit
```

```
pop     rbp
mov     edi, 853048h
ret
```

```
exit:
pop     rbp
ret
```



```
mov     eax, 85304fh
push    rbp
sub     rax, 853048h
cmp     [rax], 0eh
mov     rbp, rsp
ja      exit
```

W(0xA8..,0x4F..)
R(0x37..,0x8E..)
R(0x5A..,0x34..)

```
mov     [eax], 0
test    rax, rax
jz      exit
```

```
pop     rbp
mov     edi, 853048h
ret
```

```
exit:
pop     rbp
ret
```

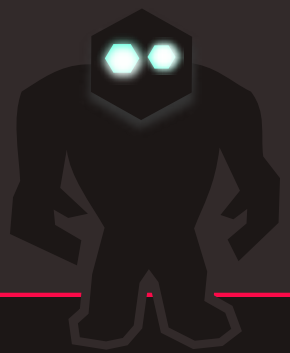
```
mov     eax, 85304fh
push    rbp
sub     rax, 853048h
cmp     [rax], 0eh
mov     rbp, rsp
ja      exit
```

W(0xA8..,0x4F..)
R(0x37..,0x8E..)
R(0x5A..,0x34..)
RET(0x8E..)

```
mov     [eax], 0
test    rax, rax
jz      exit
```

```
pop     rbp
mov     edi, 853048h
ret
```

```
exit:
pop     rbp
ret
```



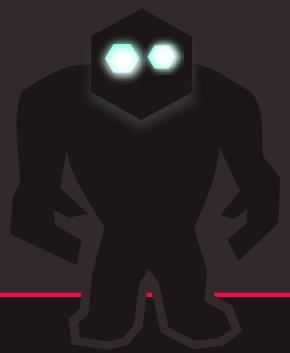
```
mov     eax, 85304fh
push    rbp
sub     rax, 853048h
cmp     [rax], 0eh
mov     rbp, rsp
ja      exit
```

W(0xA8..,0x4F..)
R(0x37..,0x8E..)
R(0x5A..,0x34..)
RET(0x8E..)

```
mov     [eax], 0
test    rax, rax
jz      exit
```

```
pop     rbp
mov     edi, 853048h
ret
```

```
exit:
pop     rbp
ret
```



```
mov     eax, 85304fh
push    rbp
sub     rax, 853048h
cmp     [rax], 0eh
mov     rbp, rsp
ja      exit
```

```
mov     [eax], 0
test    rax, rax
jz      exit
```

```
pop     rbp
mov     edi, 853048h
ret
```

```
exit:
pop     rbp
ret
```

W(0xA8..,0x4F..)
R(0x37..,0x8E..)
R(0x5A..,0x34..)
RET(0x8E..)

```
mov     eax, 85304fh
push    rbp
sub     rax, 853048h
cmp     [rax], 0eh
mov     rbp, rsp
ja      exit
```

W(0xA8..,0x4F..)
R(0x37..,0x8E..)
R(0x5A..,0x34..)
RET(0x8E..)
W(0x8E..,0x0)

```
mov     [eax], 0
test    rax, rax
jz      exit
```

```
pop     rbp
mov     edi, 853048h
ret
```

```
exit:
pop     rbp
ret
```

```
mov     eax, 85304fh
push    rbp
sub     rax, 853048h
cmp     [rax], 0eh
mov     rbp, rsp
ja      exit
```

W(0xA8..,0x4F..)
R(0x37..,0x8E..)
R(0x5A..,0x34..)
RET(0x8E..)
W(0x8E..,0x0)

```
mov     [eax], 0
test    rax, rax
jz      exit
```

```
pop     rbp
mov     edi, 853048h
ret
```

```
exit:
pop     rbp
ret
```

```
mov     eax, 85304fh
push    rbp
sub     rax, 853048h
cmp     [rax], 0eh
mov     rbp, rsp
ja      exit
```

W(0xA8..,0x4F..)
R(0x37..,0x8E..)
R(0x5A..,0x34..)
RET(0x8E..)
W(0x8E..,0x0)

```
mov     [eax], 0
test    rax, rax
jz      exit
```

```
pop     rbp
mov     edi, 853048h
ret
```

```
exit:
pop     rbp
ret
```

```
mov     eax, 85304fh
push    rbp
sub     rax, 853048h
cmp     [rax], 0eh
mov     rbp, rsp
ja      exit
```

W(0xA8..,0x4F..)
R(0x37..,0x8E..)
R(0x5A..,0x34..)
RET(0x8E..)
W(0x8E..,0x0)

```
mov     [eax], 0
test    rax, rax
jz      exit
```

```
pop     rbp
mov     edi, 853048h
ret
```

```
exit:
pop     rbp
ret
```

```
mov     eax, 85304fh
push    rbp
sub     rax, 853048h
cmp     [rax], 0eh
mov     rbp, rsp
ja      exit
```

W(0xA8..,0x4F..)
R(0x37..,0x8E..)
R(0x5A..,0x34..)
RET(0x8E..)
W(0x8E..,0x0)

```
mov     [eax], 0
test    rax, rax
jz      exit
```

```
pop     rbp
mov     edi, 853048h
ret
```

```
exit:
pop     rbp
ret
```

```
mov     eax, 85304fh
push    rbp
sub     rax, 853048h
cmp     [rax], 0eh
mov     rbp, rsp
ja      exit
```

W(0xA8..,0x4F..)
R(0x37..,0x8E..)
R(0x5A..,0x34..)
RET(0x8E..)
W(0x8E..,0x0)
R(0x5A..,0x34..)

```
mov     [eax], 0
test    rax, rax
jz      exit
```

```
pop     rbp
mov     edi, 853048h
ret
```

```
exit:
pop     rbp
ret
```

```
mov     eax, 85304fh
push    rbp
sub     rax, 853048h
cmp     [rax], 0eh
mov     rbp, rsp
ja      exit
```

W(0xA8..,0x4F..)
R(0x37..,0x8E..)
R(0x5A..,0x34..)
RET(0x8E..)
W(0x8E..,0x0)
R(0x5A..,0x34..)

```
mov     [eax], 0
test    rax, rax
jz      exit
```

```
pop     rbp
mov     edi, 853048h
ret
```

```
exit:
pop     rbp
ret
```

```
mov     eax, 85304fh
push    rbp
sub     rax, 853048h
cmp     [rax], 0eh
mov     rbp, rsp
ja      exit
```

```
mov     [eax], 0
test    rax, rax
jz      exit
```

```
pop     rbp
mov     edi, 853048h
ret
```

```
exit:
pop     rbp
ret
```

W(0xA8..,0x4F..)
R(0x37..,0x8E..)
R(0x5A..,0x34..)
RET(0x8E..)
W(0x8E..,0x0)
R(0x5A..,0x34..)
RET(0x8E..)

```
mov     eax, 85304fh
push    rbp
sub     rax, 853048h
cmp     [rax], 0eh
mov     rbp, rsp
ja      exit
```

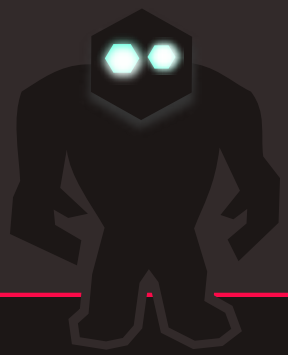
```
mov     [eax], 0
test    rax, rax
jz      exit
```

```
pop     rbp
mov     edi, 853048h
ret
```

```
exit:
pop     rbp
ret
```

W(0xA8..,0x4F..)
R(0x37..,0x8E..)
R(0x5A..,0x34..)
RET(0x8E..)
W(0x8E..,0x0)
R(0x5A..,0x34..)
RET(0x8E..)

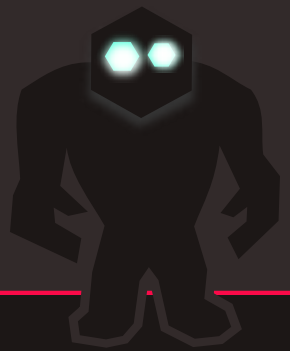
W(0xA8..,0x4F..)
R(0x37..,0x8E..)
R(0x5A..,0x34..)
RET(0x8E..)
W(0x8E..,0x0)
R(0x5A..,0x34..)
RET(0x8E..)



W(0xA8..,0x4F..)
R(0x37..,0x8E..)
R(0x5A..,0x34..)
RET(0x8E..)
W(0x8E..,0x0)
R(0x5A..,0x34..)
RET(0x8E..)

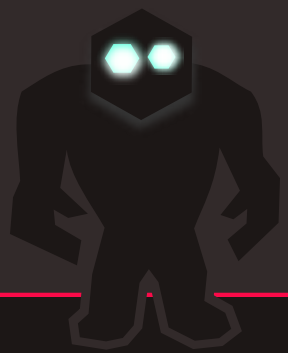
???

9809bf09cecebf3f9...



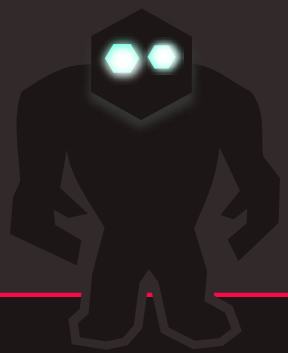
h(0)

W(0xA8..,0x4F..)	5e53
R(0x37..,0x8E..)	20c9
R(0x5A..,0x34..)	b84f
RET(0x8E..)	d464
W(0x8E..,0x0)	428c
R(0x5A..,0x34..)	93f2
RET(0x8E..)	02eb



h(0)

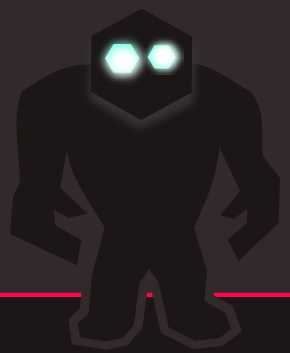
W(0xA8..,0x4F..)	5e53
R(0x37..,0x8E..)	20c9
R(0x5A..,0x34..)	b84f
RET(0x8E..)	d464
W(0x8E..,0x0)	428c
R(0x5A..,0x34..)	93f2
RET(0x8E..)	02eb



W(0xA8..,0x4F..)
R(0x37..,0x8E..)
R(0x5A..,0x34..)
RET(0x8E..)
W(0x8E..,0x0)
R(0x5A..,0x34..)
RET(0x8E..)

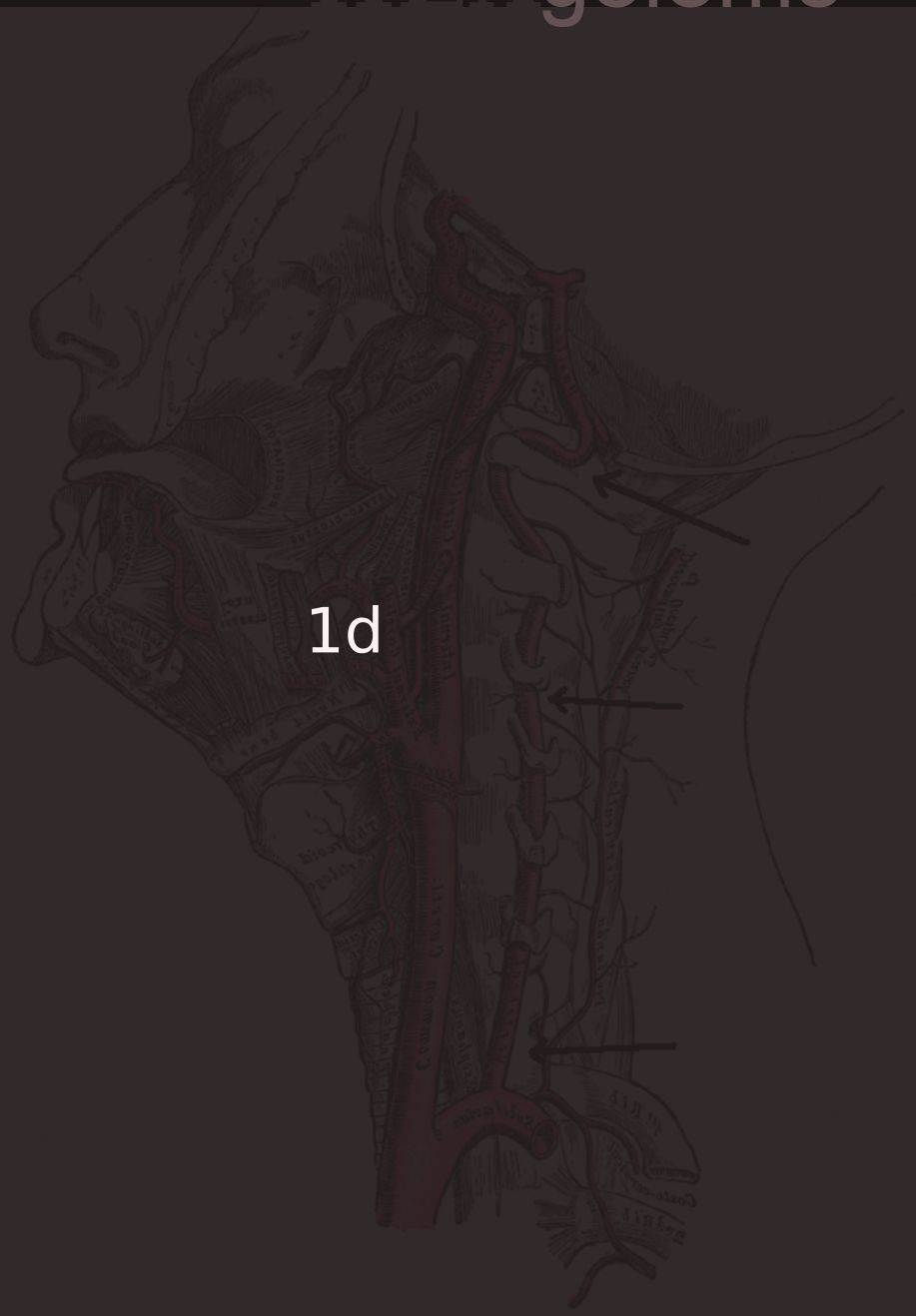
1d

h(final)



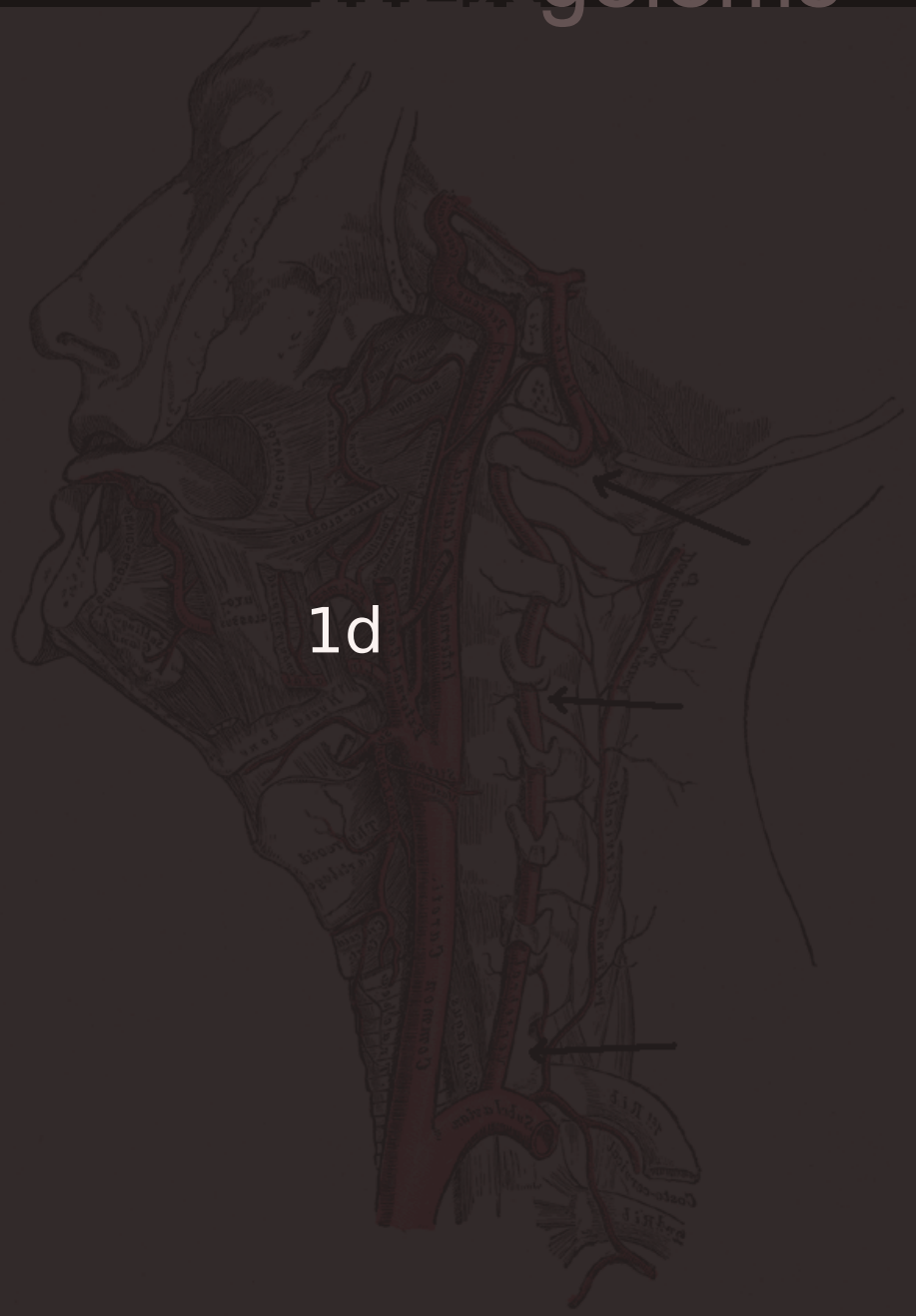
h(1)

W(0xA8..,0x4F..)	46a7
R(0x37..,0x8E..)	f3a6
R(0x5A..,0x34..)	59d7
RET(0x8E..)	18f3
W(0x8E..,0x0)	08be
R(0x5A..,0x34..)	ae20
RET(0x8E..)	fed1



h(1)

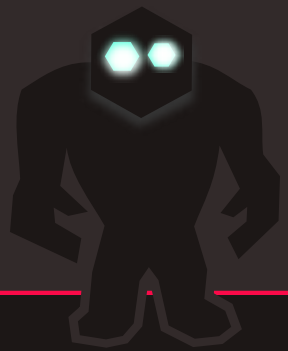
W(0xA8..,0x4F..)	46a7
R(0x37..,0x8E..)	f3a6
R(0x5A..,0x34..)	59d7
RET(0x8E..)	18f3
W(0x8E..,0x0)	08be
R(0x5A..,0x34..)	ae20
RET(0x8E..)	fed1



W(0xA8..,0x4F..)
R(0x37..,0x8E..)
R(0x5A..,0x34..)
RET(0x8E..)
W(0x8E..,0x0)
R(0x5A..,0x34..)
RET(0x8E..)

1d 66

h(final)



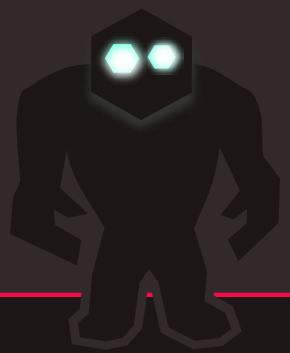
h(2)

W(0xA8..,0x4F..)	967a
R(0x37..,0x8E..)	f5c7
R(0x5A..,0x34..)	e10d
RET(0x8E..)	5688
W(0x8E..,0x0)	fe2e
R(0x5A..,0x34..)	5bb2
RET(0x8E..)	8c4f

h(2)

W(0xA8..,0x4F..)	967a
R(0x37..,0x8E..)	f5c7
R(0x5A..,0x34..)	e10d
RET(0x8E..)	5688
W(0x8E..,0x0)	fe2e
R(0x5A..,0x34..)	5bb2
RET(0x8E..)	8c4f

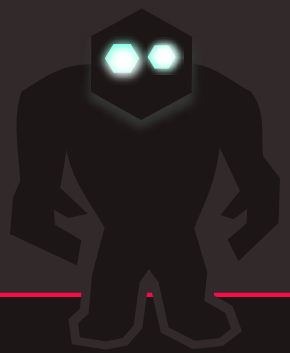
1d 66



W(0xA8..,0x4F..)
R(0x37..,0x8E..)
R(0x5A..,0x34..)
RET(0x8E..)
W(0x8E..,0x0)
R(0x5A..,0x34..)
RET(0x8E..)

1d 66 c4

h(final)

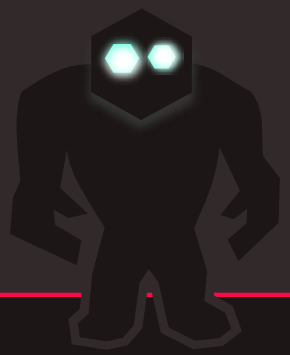


Min Hashing

W(0xA8..,0x4F..)
R(0x37..,0x8E..)
R(0x5A..,0x34..)
RET(0x8E..)
W(0x8E..,0x0)
R(0x5A..,0x34..)
RET(0x8E..)

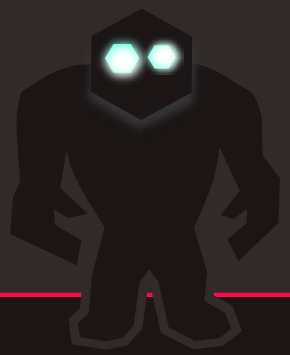
1d 66 c4 ...

gdb with O0, O1, O2



gdb with O0, O1, O2

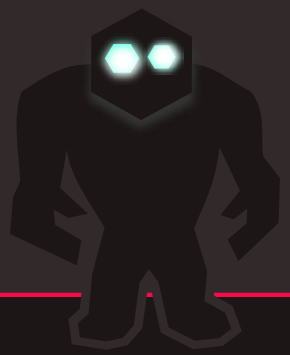
85% True Positives



gdb with O0, O1, O2

85% True Positives

False Positives?



Questions?

Flirt

Blanket Execution

Min Hashing

Indika