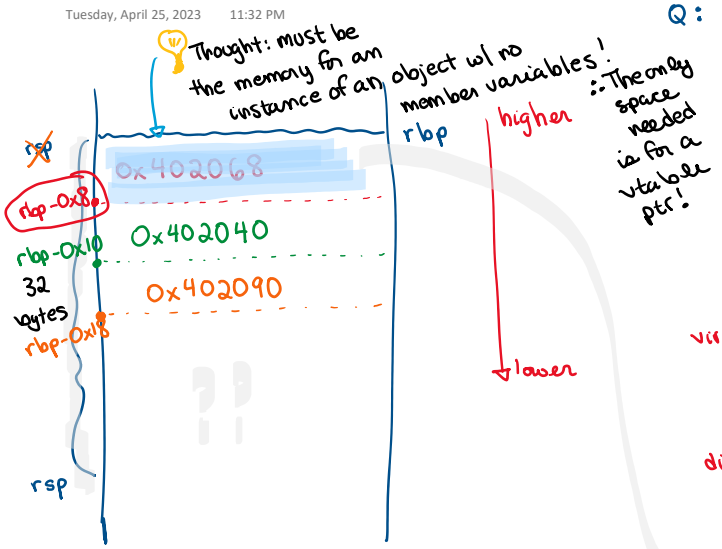
VTables For Squirrels

Tuesday, April 25, 2023 11:32 PM



Q: what does 0x402068 point to?

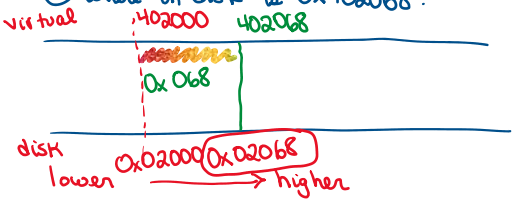
① Find out the section!

ⓐ use the readelf output!

Fact: section .rodata starts @ 402000 ✓

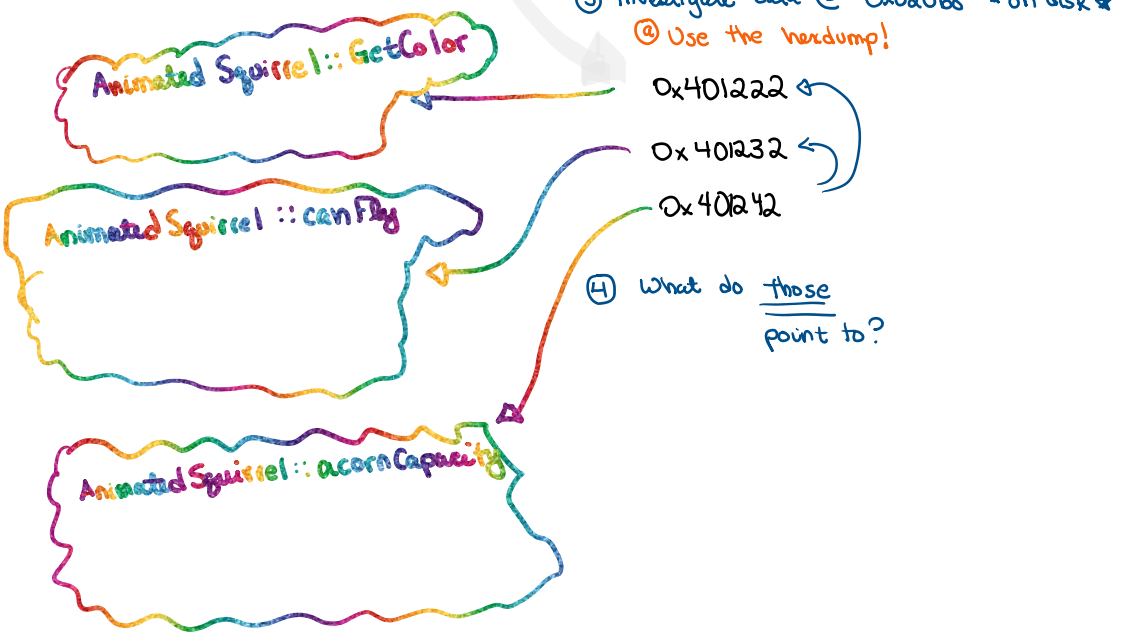
ends @ 0x402122 (+122)

② where on disk is 0x402068?



③ Investigate data @ 0x02068 * on disk *

ⓐ Use the hexdump!



④ What do those point to?

```
401179:   48 8d 45 f8          lea    rax,[rbp-0x8]
40117d:   48 89 c7             mov    rdi,rax
401180:   e8 9d 00 00 00       call   401222 <_ZNK16AnimatedSquirrel8getColorEv>
```

rax = address rbp-0x8 ie a ptr to something we think is a instance of an object!

mov rax to rdi

When we make a function call, rdi is arg. 0! (on Unix-like platforms)