

# Because the file is **data** , I used strings to search for some hints, like :  
strings -n 7 e.bin | grep { ctf, CTF, flag, password, ... }

# I found out that the right command is :  
strings e.bin | grep password

# Because at some point I found this plain text :

```
password-reveal
https://app.drivepassword.com?state=%7B%22ids%22:%5B%22{ids}%22%
22%7D
https://myaccount.google.com/signinoptions/password?utm_source=G
../../chrome/browser/safe_browsing/chrome_password_protection_se
one.?time|sms.?(code|token|password|pwd|pass)
../../components/password_manager/core/browser/password_requirem
profile.content_settings.exceptions.password_protection
profile.content_settings.exceptions.password_protection
profile.content_settings.exceptions.password_protection
profile.content_settings.exceptions.password_protection
passwordflagw
passwordflagwi
' contains a username and password, which is disallowed for cros
1.3246144582529556e+16,"lastShortcutLaunchTime":0.0,"pointsAdded
": "13246162003569829", "model":0, "setting":{"lastEngagementTime":
```

# We are looking for a plain text and sha256 it, because this is our requirement. I also ran :  
strings e.bin | grep passwordflag

# And I found the flag correct string : **passwordflagwin**

THE FLAG :

ctf{9586b1bba71db9c301f354be9a84ddde3e1b35f6a933928f0aaf4f7e65d194cf}  
~Z4que