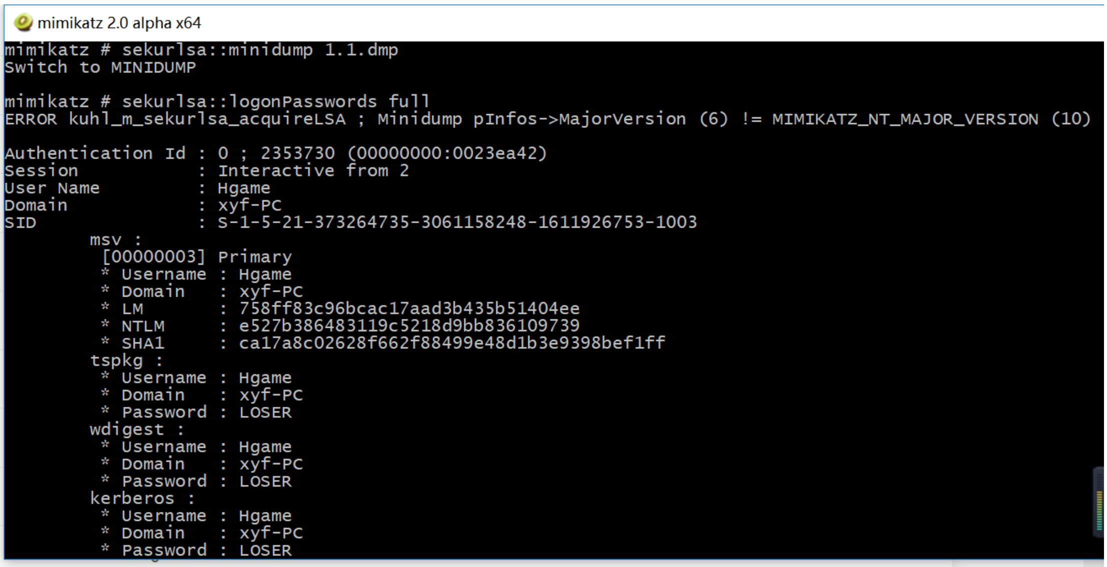
Hgame week4 Write up—FAD18

3.Misc

3.1WARMUP

提示 mimikatz，百度后得知软件打开的是 dmp 文件，用 winhex 打开题目文件，发现开头是 dmp 格式，更改后缀，放到 mimikatz，得到 flag

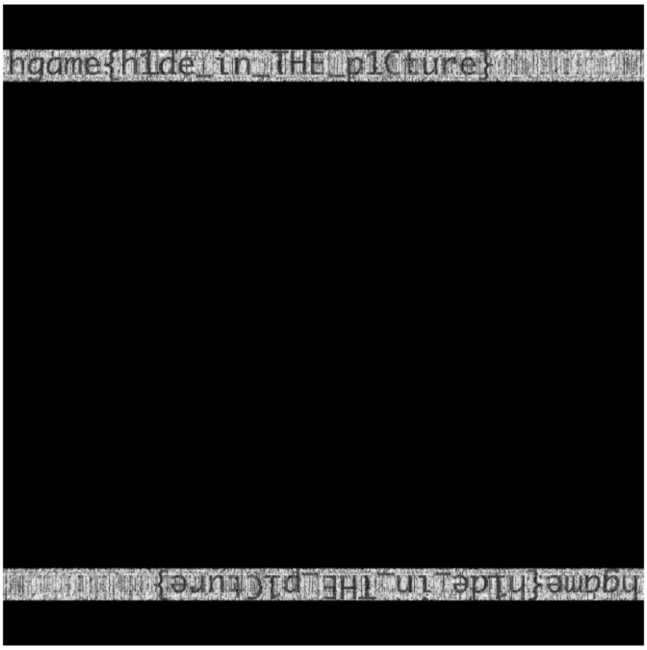

mimikatz 2.0 alpha x64

```
mimikatz # sekurlsa::minidump 1.1.dmp
Switch to MINIDUMP

mimikatz # sekurlsa::logonPasswords full
ERROR kuhl_m_sekurlsa_acquireLSA ; Minidump pInfos->MajorVersion (6) != MIMIKATZ_NT_MAJOR_VERSION (10)

Authentication Id : 0 ; 2353730 (00000000:0023ea42)
Session           : Interactive from 2
User Name         : Hgame
Domain            : xyf-PC
SID               : S-1-5-21-373264735-3061158248-1611926753-1003
        msv :
         [00000003] Primary
         * Username : Hgame
         * Domain   : xyf-PC
         * LM       : 758ff83c96bcac17aad3b435b51404ee
         * NTLM     : e527b386483119c5218d9bb836109739
         * SHA1     : ca17a8c02628f662f88499e48d1b3e9398bef1ff
        tspkg :
         * Username : Hgame
         * Domain   : xyf-PC
         * Password : LOSER
        wdigest :
         * Username : Hgame
         * Domain   : xyf-PC
         * Password : LOSER
        kerberos :
         * Username : Hgame
         * Domain   : xyf-PC
         * Password : LOSER
```

> dd6dffcd56b77597157ac6c1beb514aa4c59d033098f806d88df89245824d3f5

3.3 暗藏玄机

两张看似一模一样的图片，百度后发现应该是盲水印，找了个 python 脚本，得到 flag


hgame{h1de_in_THE_p1Cture}