

HGAME 2021 WEEK WRITE UP

ARK

MISC

结合题中提到的“自律”功能，合理怀疑两个名为 `getBattleReplay` 的文件。打开后发现有一个 `battleReplay` 字段，包括数字、大小写字母，以 `==` 结尾，长度约14k字节。猜测是 `base64` 编码，且包括所有记录操作。解码后得到如下内容（开头部分）

PK□□□???□?·bKRÇÛa□t((?□¾□?
 ???default_entrygM«Ó@□@ÿjKÜF□¹w2□îT\□□"âB□
 6j4Mµl□□øðæÖ/t ÆE_¿lkm;7ç0¼oÍë~ÿ±□ßΩæé

.....

结合 PK 字段及 default_entry，猜测为 zip 文件。将解码后的二进制代码用 winHex 保存 .zip 文件。成功打开并解压，得到 default_entry。用记事本打开，内容如下（开头部分）

```
{
  "campaignOnlyVersion": 1,
  "timestamp": "1612849000",
  "journal": {
    "metadata": {
      "standardPlayTime": 272.999725,
      "gameResult": 1,
      "saveTime": "2021-02-09T13:36:36.552186Z",
      "remainingCost": 99,
      "remainingLifePoint": 3,
      "killedEnemiesCnt": 57,
      "missedEnemiesCnt": 0,
      "levelId": "Activities/act16d5/level_act16d5_10",
      "stageId": "act16d5_10",
      "validKilledEnemiesCnt": 57
    },
    "squad": [
      {
        "charInstId": 8,
        "skinId": "char_2015_dusk#1",
        "tmplId": null,
        "skillId": "skchr_dusk_1",
        "skillIndex": 0,
        "skillLv": 1,
        "level": 1,
        "phase": 0,
        "potentialRank": 0,
        "favorBattlePhase": 38,
        "isAssistChar": true
      }
    ],
    "logs": [
      {
        "timestamp": 0,
        "signature": {
          "uniqueId": 2147483815,
          "charId": "char_2015_dusk",
          "op": 0,
          "direction": 1,
          "pos": {
            "row": 12,
            "col": 12
          }
        },
        "timestamp": 0,
        "signature": {
          "uniqueId": 2147483815,
          "charId": "char_2015_dusk",
          "op": 0,
          "direction": 1,
          "pos": {
            "row": 12,
            "col": 13
          }
        },
        "timestamp": 0,
        "signature": {
          "uniqueId": 2147483815,
          "charId": "char_2015_dusk",
          "op": 0,
          "direction": 1,
          "pos": {
            "row": 12,
            "col": 14
          }
        },
        "timestamp": 0,
        "signature": {
          "uniqueId": 2147483815,
          "charId": "char_2015_dusk",
          "op": 0,
          "direction": 1,
          "pos": {
            "row": 12,
            "col": 15
          }
        }
      ]
    }
  }
}
```

.....

后文内容高度相似，仅有 row 和 col 字段后的数字不同。结合题中 出题人用可部署单位画了个东西 背景是白色的，猜测是一个黑白图像，两个字段对应的像素点为黑色、背景为白色。写一个c语言程序提取并绘制

```
#include<stdio.h>

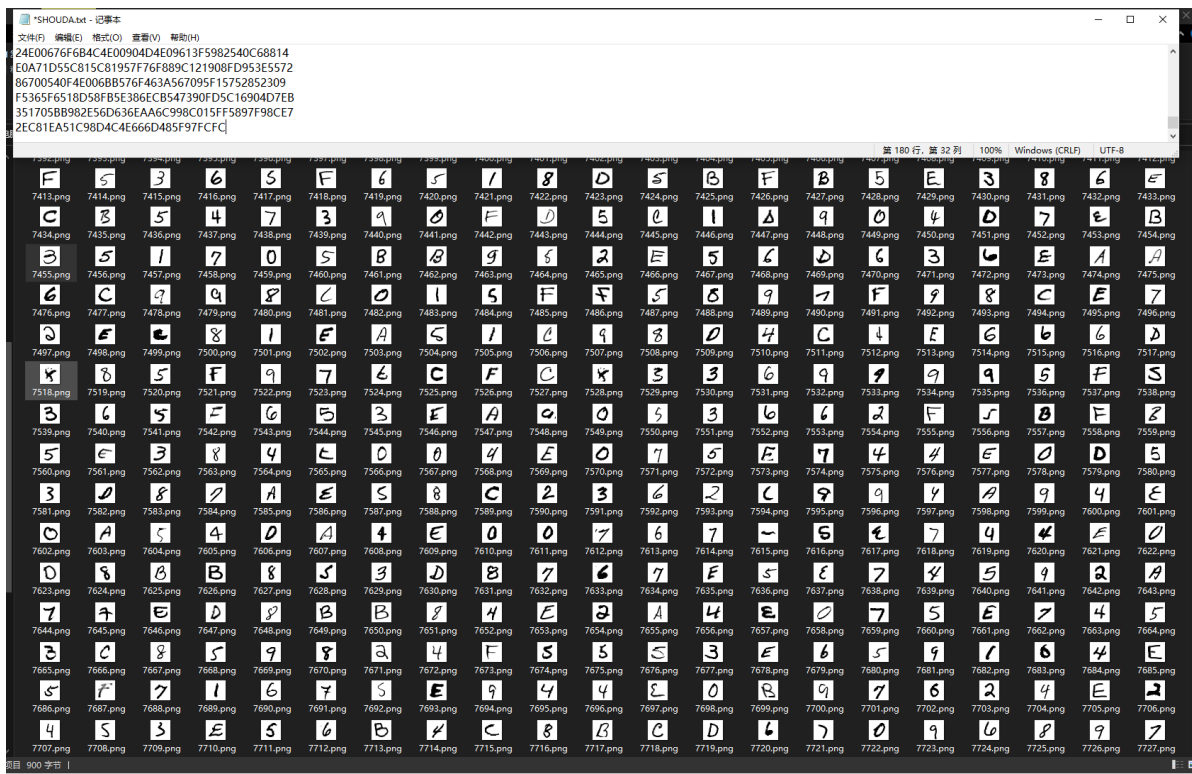
int main(void)
{
    int pixel[100][100] = { 0 };
    int a, b;
    while (freopen("default_entry_mid.txt", "r", stdin) == NULL)
        ; //输入重定向，命令行输入长度上限不够
    for (int i = 0; i < 10000; i++)
    {
        scanf("{ \"timestamp\":0, \"signature\":\n\
{ \"uniqueId\":2147483815, \"charId\": \"char_2015_dusk\" }, \"op\":0, \"direction\":1\n\
, \"pos\": { \"row\":%d, \"col\":%d } }", &a, &b);
        pixel[a][b] = 1; //default_entry开头的内容删除后作为输入
        (偷个懒)
    }
    printf("\n\n\n");

    for (int row = 0; row < 100; row++) { //绘制100*100图像
        for (int col = 0; col < 100; col++)
            if (pixel[row][col])
                printf(" "); //cmd背景为黑色，打印空格即可
            else
                printf("龘"); //复杂一点的字，白色面积更大一些
        printf("\n");
    }
    return 0;
}
```

保存、运行。得到一个二维码，扫码后得到Flag。

accuracy

解压下载的压缩包，分析后得出：用 dataset.csv 的数据训练模型，将 chars.rar 中图片形式的手写数字转换为文本。一番操作后，放弃了 TensorFlow 和 百度AI开放平台，改为自行训练人工智能。AI速率约8bps；功耗三顿饭/十六小时。下为工作截图



全部打完后核对字节数，并上传，成功拿到Flag。