# 一、题目描述

题目链接：[www.ctfhub.com/#/challenge](http://www.ctfhub.com/#/challenge)

题目来源平台：CTFHUB

题目名称：2020-CSICTF-Misc-unseen

题目描述：With his dying breath, Prof. Ter Stegen hands us an image and a recording. He tells us that the image is least significant, but is a numerical key to the recording and the recording hides the answer. It may seem as though it’s all for nothing, but trust me it’s not！

翻译

带着最后一口气，斯特根教授递给我们一张照片和一段录音。他告诉我们，图像是最不重要的，但它是录音的数字键，录音隐藏了答案。看起来好像这一切都是徒劳的，但相信我不是！

题目类型：MISC

题目附件：[[金山文档] 1044\_af6d6babed3b701af4129212243951ef6e068e4b.zip](https://kdocs.cn/l/cdA6DeImVdkr)

FLAG：csictf{7h47\_15\_h0w\_y0u\_c4n\_83c0m3\_1nv151813}

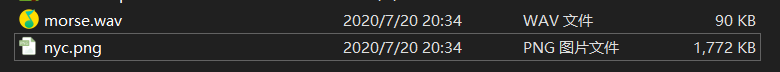
# 二、解题工具

|  |  |  |  |
| --- | --- | --- | --- |
| 工具类型 | 工具名称 | 版本 | 备注 |
| 基础环境 | Python | 3.7 |  |
| Windows |  |  |
| 工具 | Stegsolve |  |  |
| steghide |  |  |
| Win\_hex |  |  |
| 空白解码器 |  | 在github |

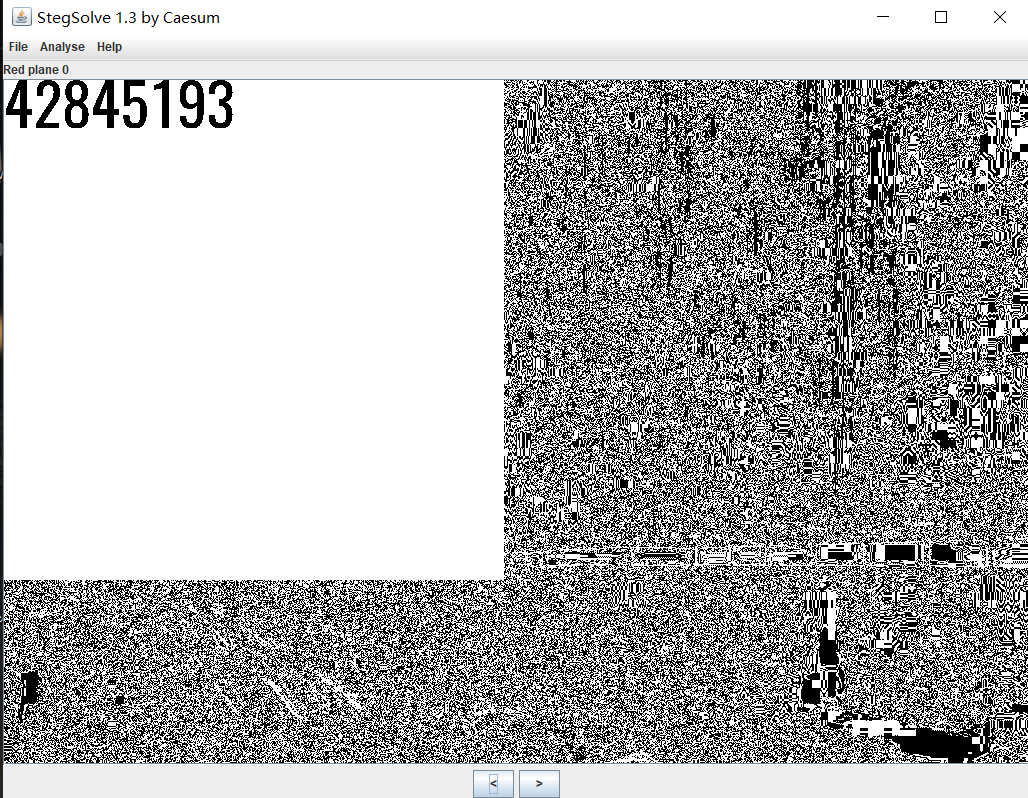
# 三、解题过程

（详细说明CTF赛题的解题过程，分步骤说明）

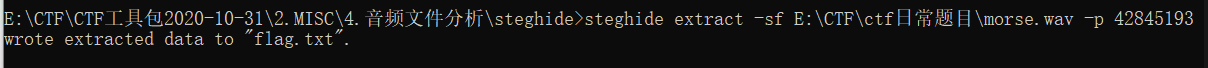
### 步骤1：下载附件发现是一个wav文件和一张图片



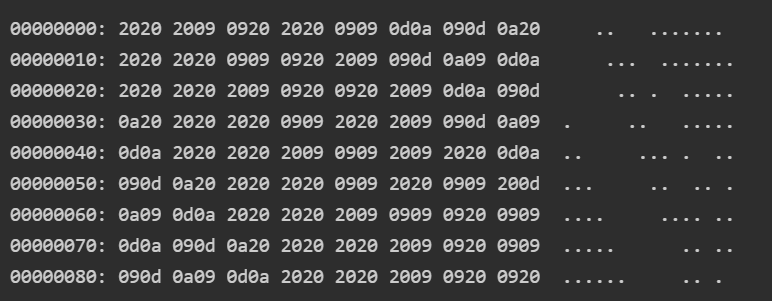
### 步骤2：先看图片用stegsolve打开，翻一下，发现一串数字，由提示可知数字是解开音频的关键

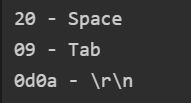


### 步骤3：既然给了数字，就能联想到要使用steghide，只要它是需要密码的，因此用它打开wav文件



得到的flag.txt.文件，放到十六进制的编辑器里

**步骤4**：把他们转换成ASCII码，可以看到，/t是1、“”是0



**步骤5：**可以使用空白解码器，在github上（不知道为什么我的电脑打不开了，所以无法上链接了）解码得到flag

