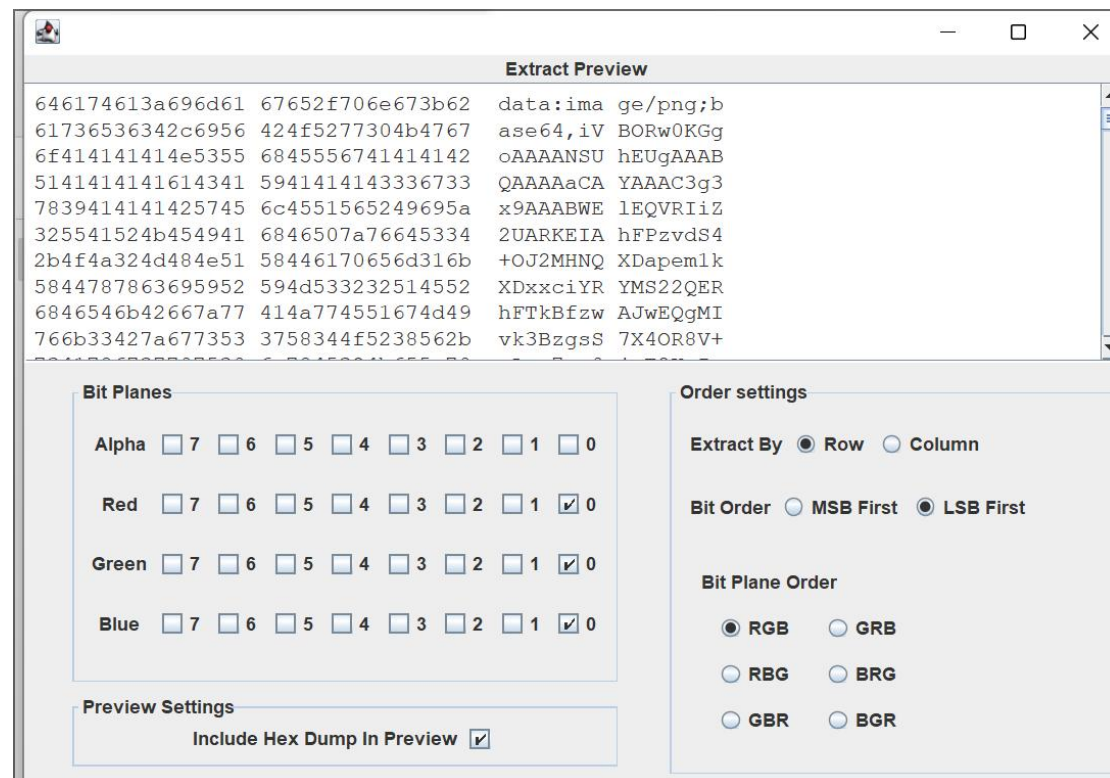


打开压缩文件，发现有一张图片，一个 wav 音频和一个 wavkey 组成，我们先查看图片有没有什么有用的信息

使用 stegsolve 打开，查看 rgb 通道 0 得到以下信息



发现是 base64 编码，而且是很明显的 base64 转图片格式，在在线网站中进行解密



解密出来的图片很容易联想到 piet 编程，使用工具进行解密尝试

工具下载地址：<https://www.berntnase.de/npviet/npviet-1.3a-win32.zip>

发现并不能成功解密，回头继续看其他文件

Wav 解密没什么头绪，先看 txt 文本，发现第二行显示的行数与实际不符，猜测使用了 0 宽隐写



```
文件 编辑 查看
[注意看，这个穿蓝衣服的男人叫小帅，他总是能使你的屏幕变灰夺去你的颜色
flag格式：nuaactf{}]
```

行 2, 列 65 | 100% | Windows (CRLF) | UTF-8

解密如下：

Unicode Steganography with Zero-Width Characters

This is plain text steganography with zero-width characters of Unicode.
Zero-width characters is inserted within the words.

JavaScript library is below.

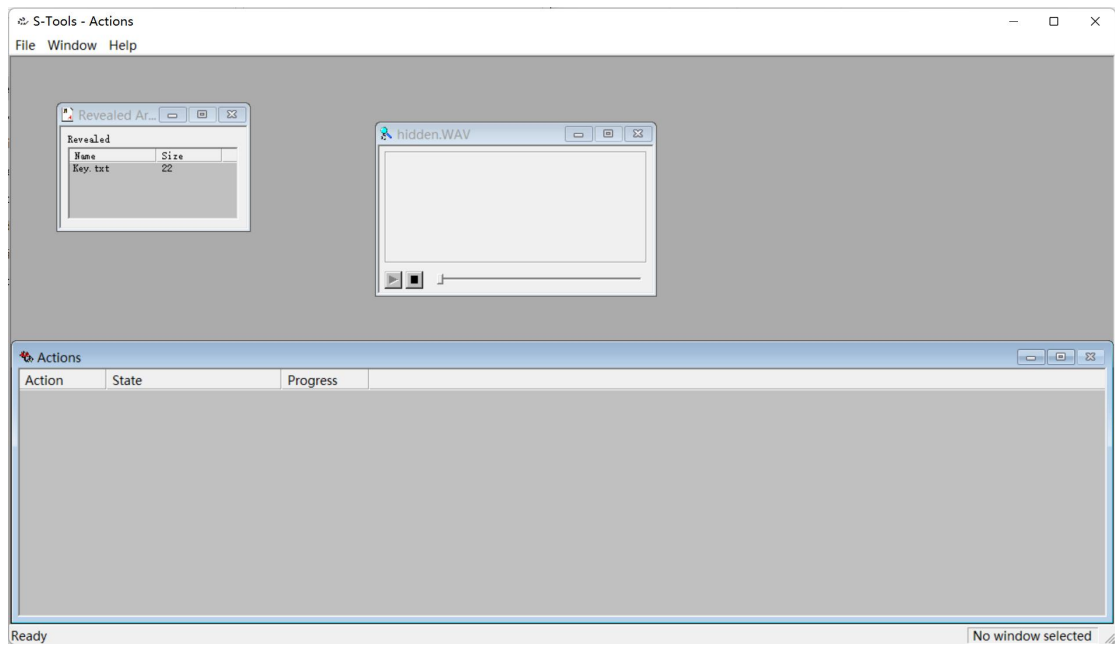
http://330k.github.io/misc_tools/unicode_steganography.js

Text in Text Steganography Sample

| | | |
|--|---|---|
| Original Text: <input type="button" value="Clear"/> (length: 51) <div>注意看，这个穿蓝衣服的男人叫小帅，他总是能使你的屏幕变灰夺去你的颜色 flag格式：nuaactf{}</div> | <input type="button" value="Encode »"/> | Steganography Text: <input type="button" value="Clear"/> (length: 99) <div>注意看，这个穿蓝衣服的男人叫小帅，他总是能使你的屏幕变灰夺去你的颜色 flag格式：nuaactf{}</div> |
| Hidden Text: <input type="button" value="Clear"/> (length: 6) <div>s_tool</div> | | <input type="button" value="« Decode"/> |
| <input type="button" value="Download Stego Text as File"/> | | |

查询 s_tool 发现是一个音频隐写工具，下载之后进行解密，发现缺少密码

查看 zip 备注，发现需要我们关注名字，所以我们将名字复制下来作为密码进行尝试



成功解密得到 key: lnWZZpdyuhclfnkdioehww

结合下载的 piet 工具和 key 成功解出 flag

```
PS C:\ctf\npiet-1.3a-win32> .\npiet.exe -q .\1.png
cygwin warning:
  MS-DOS style path detected: .\1.png
  Preferred POSIX equivalent is: ./1.png
  CYGWIN environment variable option "nodosfilewarning" turns off this warning.
  Consult the user's guide for more details about POSIX paths:
    http://cygwin.com/cygwin-ug-net/using.html#using-pathnames
lnWZZpdyuhclfnkdioehww
nuaactf{piet_is_funny}
```