**Tin Balloon**

***Forensics***

**Challenge:**

We've discovered that DEADFACE was somehow able to extract a fair amount of data from Techno Global Research Industries. We are still working out the details, but we believe they crafted custom malware to gain access to one of TGRI's systems. We intercepted a Word document that we believe mentions the name of the malware, in addition to an audio file that was part of the same conversation. We're not sure what the link is between the two files, but I'm sure you can figure it out!

Submit the flag as: flag{executable\_name}. Example: flag{malware.exe}.

Attached - Sequence 01.zip

**Approach:**

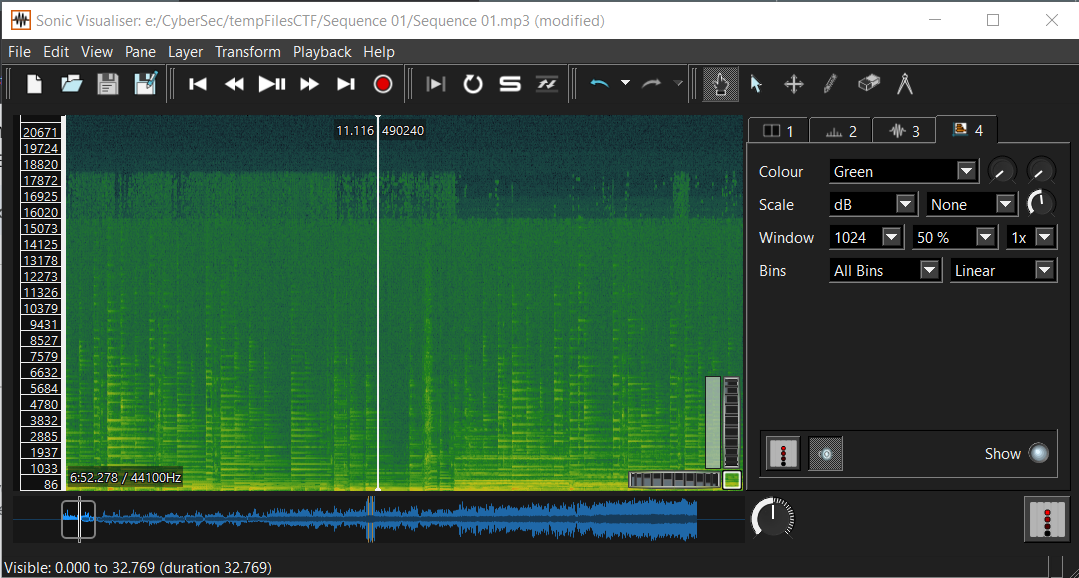
Now this is a good one, not that tough but yeah

The zip file contains 2 files, an audio file and a word document.

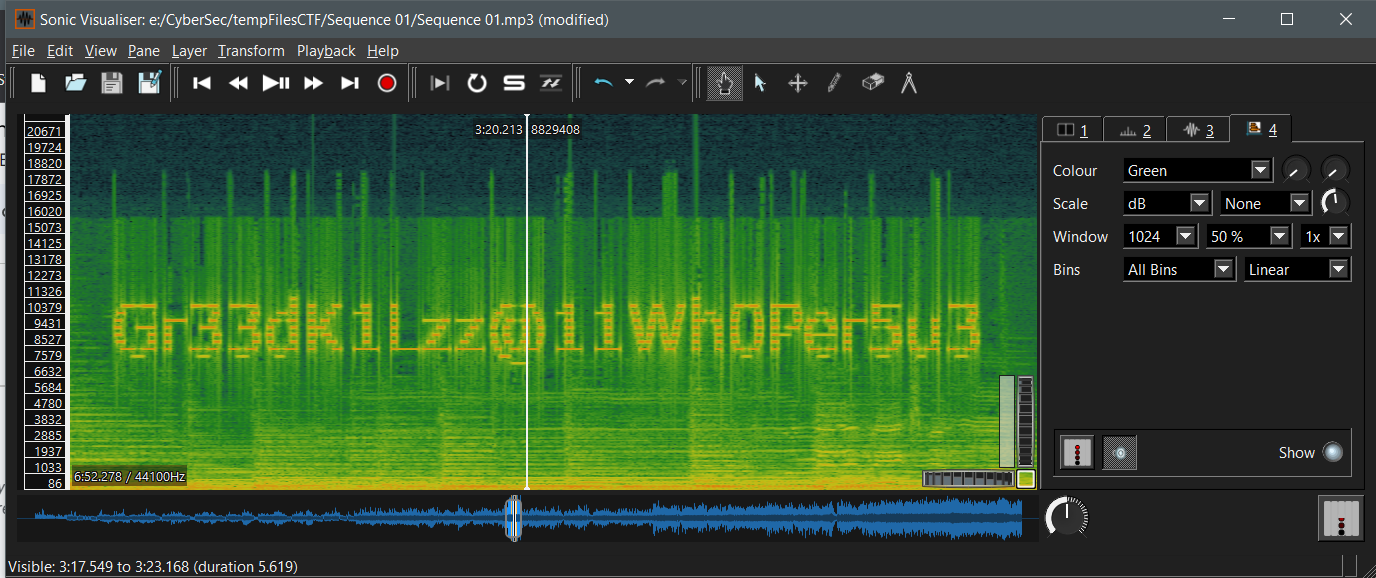
When we try to open the audio document, it asks for a password which we don’t have??

The audio when played is a nice 6 minute long song (enjoy the song for a while)

Challenges including audio files sometimes have some data hidden inside its spectrogram (Spectrogram steganography) so we open up our tool (Sonic Visualizer) and open its spectrogram view:



We scroll through a bit and see this compressed text, zoom in a bit, and we see it clear:



Text: Gr33dK1Lzz@11Wh0Per5u3

We use this text as password for our word document and finally get the name of the malware mentioned in it. Hence our flag

**Flag: flag{Wh1t3\_N01Z3.exe}**

Congrats!!

Happy Hacking!