

1. Open the mkv file and see the video carefully, it has Part 1 of the password embedded in the frame at 0:00:07. It gives us n3uer6ona



2. Running Strings command on the mkv gives the part 2 of the password: G1v3y0uvP

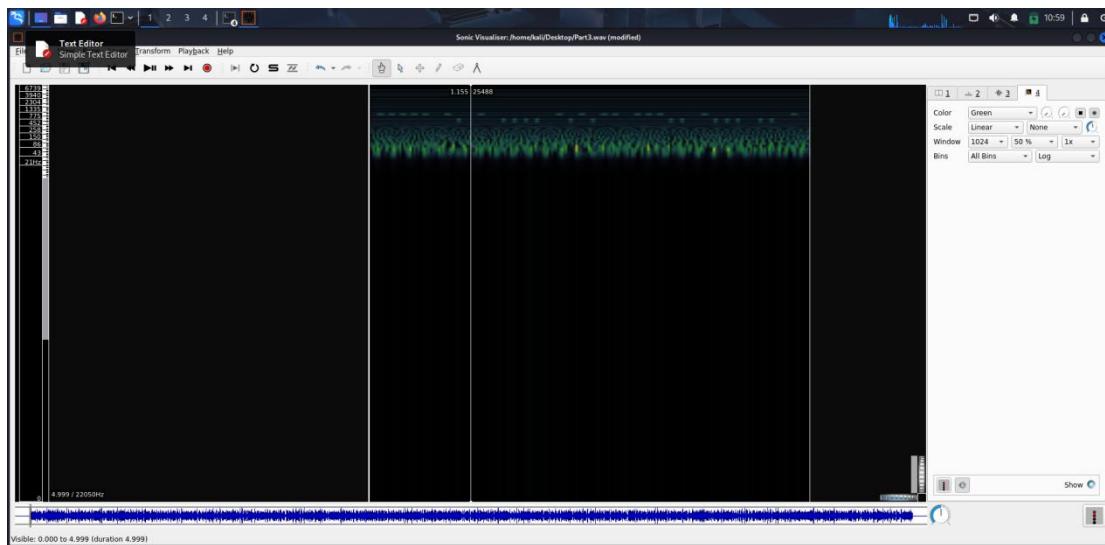
```
root@kali:~/Desktop$ strings Media.mkv | grep pass
Part2 of the password: G1v3y0uvP

root@kali:~/Desktop$ bimwlmk Media.mkv

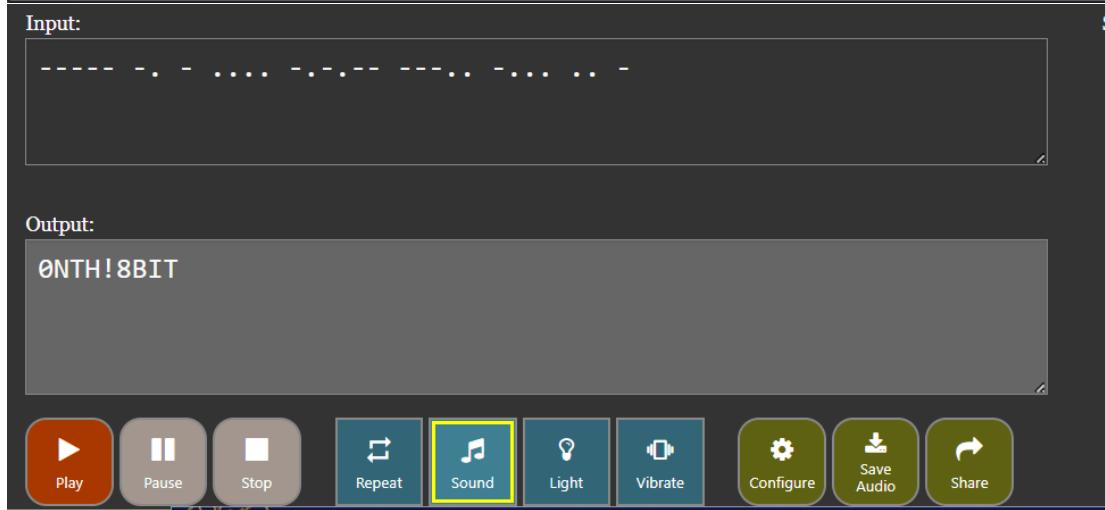
          DECIMAL      HEXADECIMAL      DESCRIPTION
0           0x0          EBNL file, Matroska data
1675245    0x398ED        JBOOT ST46 header, image id: 6, timestamp 0x0022D488, image size: 86182282 bytes, image JBOOT che
cksum: 0x590A, header JBOOT checksum: 0xC21
2270748    0x2C9E8        MySQL ISAM compressed data file Version 6
5373477    0x401F525       MySQL ISAM index file Version 11
7159268    0x601600        MySQL ISAM index file Version 3
8103154    0x401F522       MySQL ISAM compressed data file Version 6, image id: 5, timestamp 0x773C8908, image size: 3272408643 bytes, image JBOOT c
hecksum: 0x0D03, header JBOOT checksum: 0xC813
14125638   0x017AE        JBOOT STAR header, image id: 14, timestamp 0x43C3AA51, image size: 2820556720 bytes, image JBOOT
checksum: 0xB1B0A4, header JBOOT checksum: 0xC813
16558908   0x10216A        Broadcast header, number of sections: 1085286476,
16915238   0x1021826       RIFF audio data (WAV), PCM, 2 channels, 22958 sample rate

root@kali:~/Desktop$
```

3. It also shows the presence of a wav file, So extract the file using dd if=Media.mkv of=Part3.wav bs=1 skip=16915238.



4.



5.

6. Analysing the wav file in morse decoder gives us the part3 of the password: OntH!8biT
7. On extract the audio part of the mkv using ffmpeg -i .\Media.mkv -vn -acodec copy extracted.wav and running a general script of the LSB Decoding, We get the 4th part of the password: C4nnv3?
8. This completes the password and we get the flag.txt on unzipping flag.zip using n3uer6onaG1v3y0uvP0ntH!8biTC4nnv3?
- 9.The flag is DJSISACA{Damn_you_are_good_with_media}