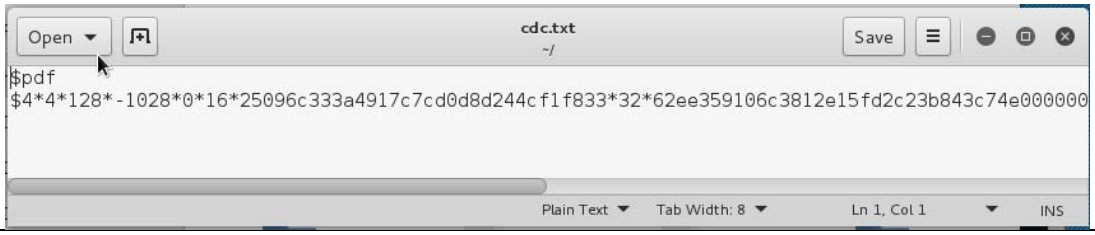
Puzzle 2

This is a multi-tiered puzzle that utilizes the following concepts:

- Password cracking
- Deciphering a Rebus puzzles
- Audio analysis
- Deciphering a Playfair cipher

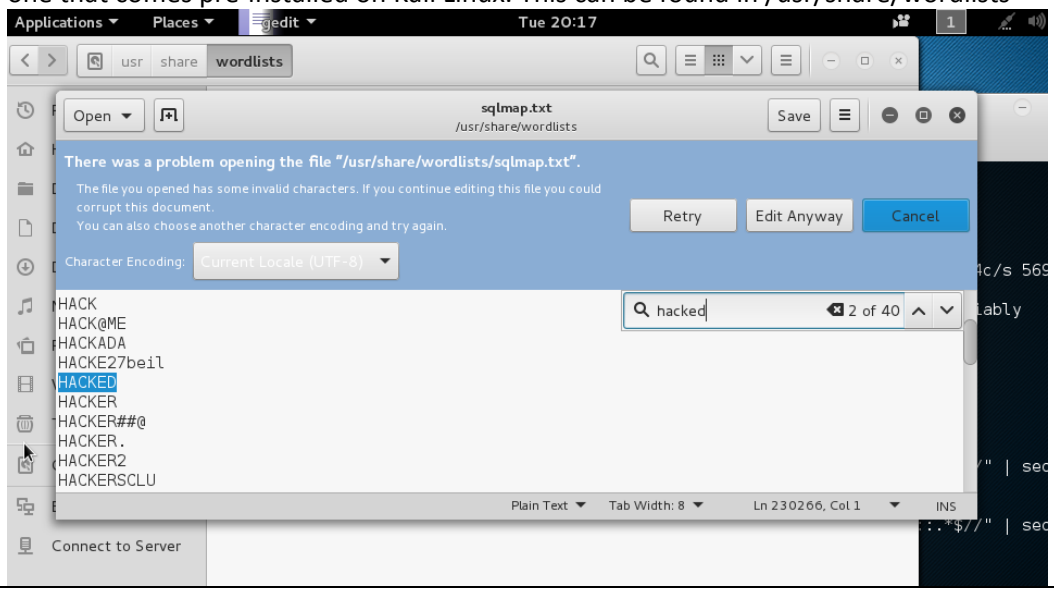
Description:	In order to crack the hash on this pdf, the user will need to download pdf2john.py – which works with John the Ripper on Kali Linux
Code:	wget https://github.com/magnumripper/JohnTherRipper/archive/bleeding-jumbo.zip unzip bleeding-jumbo.zip cp JohnTheRIpper-bleeding-jumbo/run/pdf2john.py .

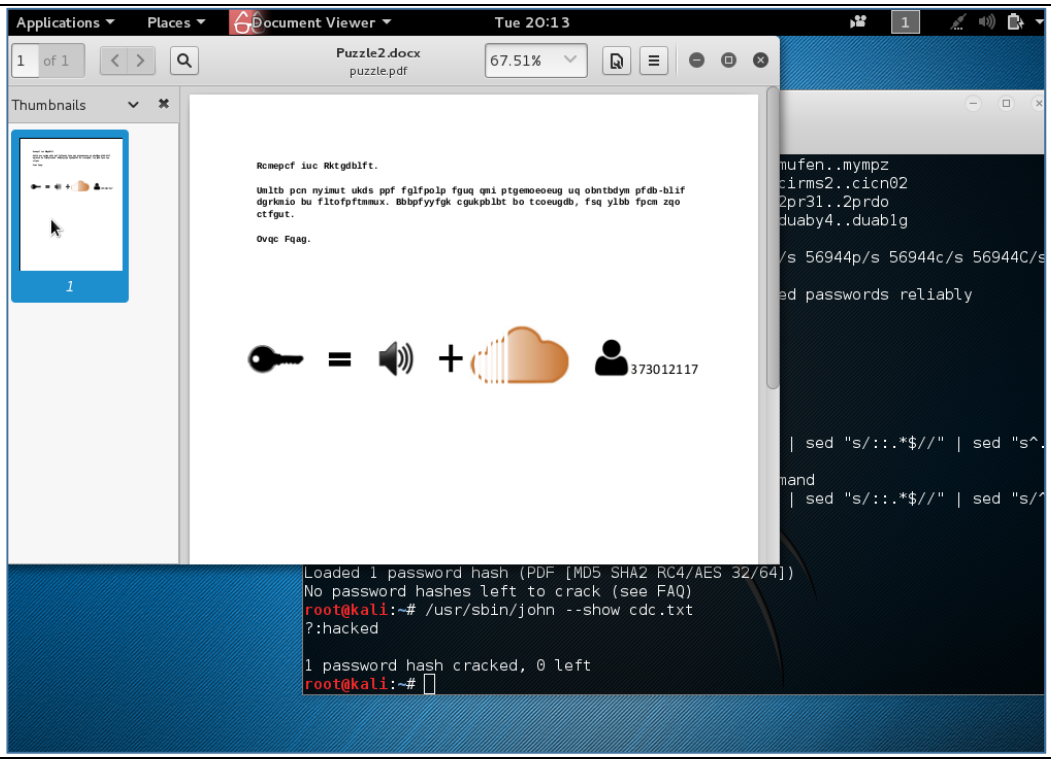
Description:	The user will then have to run pdf2john.py against the puzzle.pdf to extract the hash from the PDF.
Code:	./pdf2john.py (location of puzzle)/Puzzle.pdf | sed "s/::.*$//" | sed "s/^.*://" > cdc.txt 

Description:	The output of the hash is saved in the “cdc.txt” file, or whatever the user has named their output file: 
Code:	

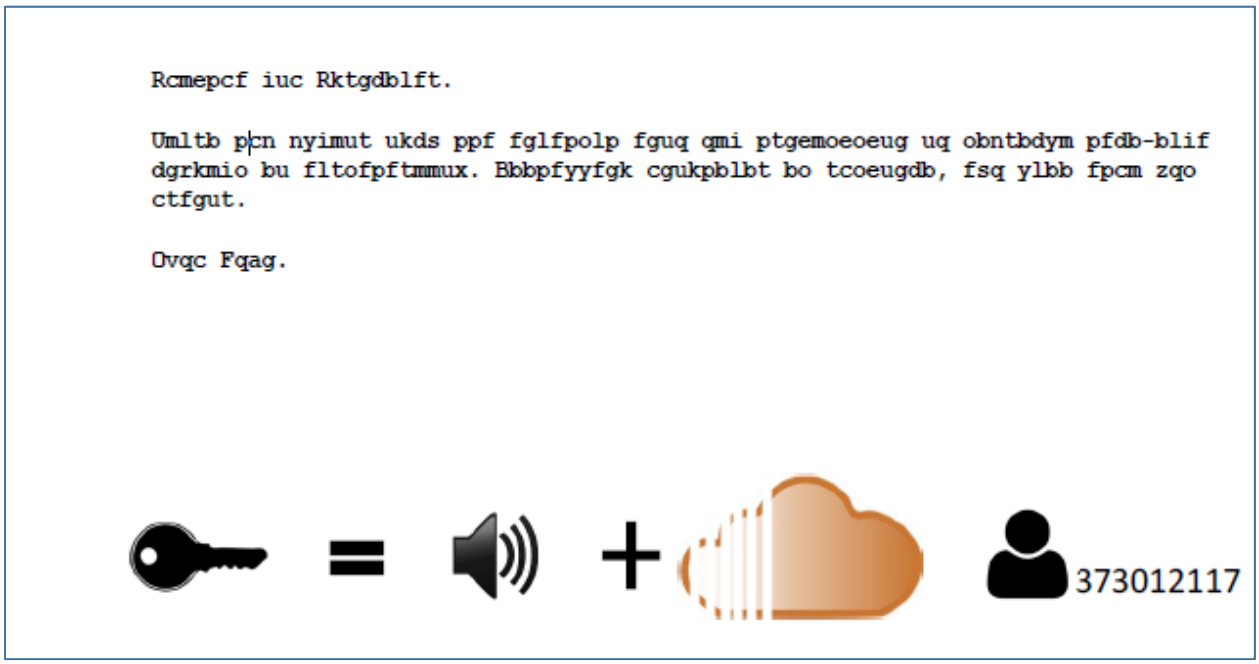
This obtained hash is now ready to be cracked with John The Ripper, Hashcat, or some other type of hash cracking program

Description:	The user can run John the Ripper to crack the hash using the following commands:
Code:	root@kali:~# /usr/sbin/john cdc.txt root@kali:~# /usr/sbin/john cdc3.txt Using default input encoding: UTF-8 Loaded 1 password hash (PDF [MD5 SHA2 RC4/AES 32/64]) Will run 2 OpenMP threads Press 'q' or Ctrl-C to abort, almost any other key for status 0g 0:00:00:12 3/3 0g/s 42696p/s 42696c/s 42696C/s mufen..mympz 0g 0:00:02:25 3/3 0g/s 51998p/s 51998c/s 51998C/s cirms2..cicn02 0g 0:00:05:01 3/3 0g/s 56037p/s 56037c/s 56037C/s 2pr31..2prdo 0g 0:00:07:00 3/3 0g/s 56986p/s 56986c/s 56986C/s duaby4..duab1g hacked (?) 1g 0:00:07:36 DONE 3/3 (2016-03-22 20:01) 0.002188g/s 56944p/s 56944c/s 56944C/s habm9d..hack03 Use the "--show" option to display all of the cracked passwords reliably Session completed **Note: it's going to take around 10 minutes to crack this password**

Description:	Using the "show' command, we can identify the password, which is, "hacked":
Code:	root@kali:~# ./pdf2john.py /root/Desktop/puzzle.pdf | sed "s/::.*$//" \| sed "s^.*://" > cdc.txt sed: -e expression #1, char 7: unterminated `s' command root@kali:~# ./pdf2john.py /root/Desktop/puzzle.pdf \| sed "s/::.*$//" | sed "s/^.*://" > cdc.txt root@kali:~# /usr/sbin/john cdc.txt Using default input encoding: UTF-8 Loaded 1 password hash (PDF [MD5 SHA2 RC4/AES 32/64]) No password hashes left to crack (see FAQ) root@kali:~# /usr/sbin/john --show cdc.txt ?:hacked 1 password hash cracked, 0 left This is a pretty common password that can be found in different password lists, including one that comes pre-installed on Kali Linux. This can be found in /usr/share/wordlists 

Description:	The user can now use the password obtained by John the Ripper to open the PDF:
Code:	

Now that the document is open, the user will see that there is some ciphertext and a rebus puzzle that needs decoding



To decode the rebus puzzle:
Here, the user is able to deduce that the Key symbol means the key to unlock the cipher.

the  image stands for “sound” and the  image stands for cloud. This means that the clue to the key is on SoundCloud.com.

the  symbol means user, and the “373012117” is the username of the user(me) who uploaded the sound file.

In order to obtain the passphrase to break this cipher, they have to go to SoundCloud.com for it is there that the user will find the passphrase to the cipher.

The user must search for user 373012177.

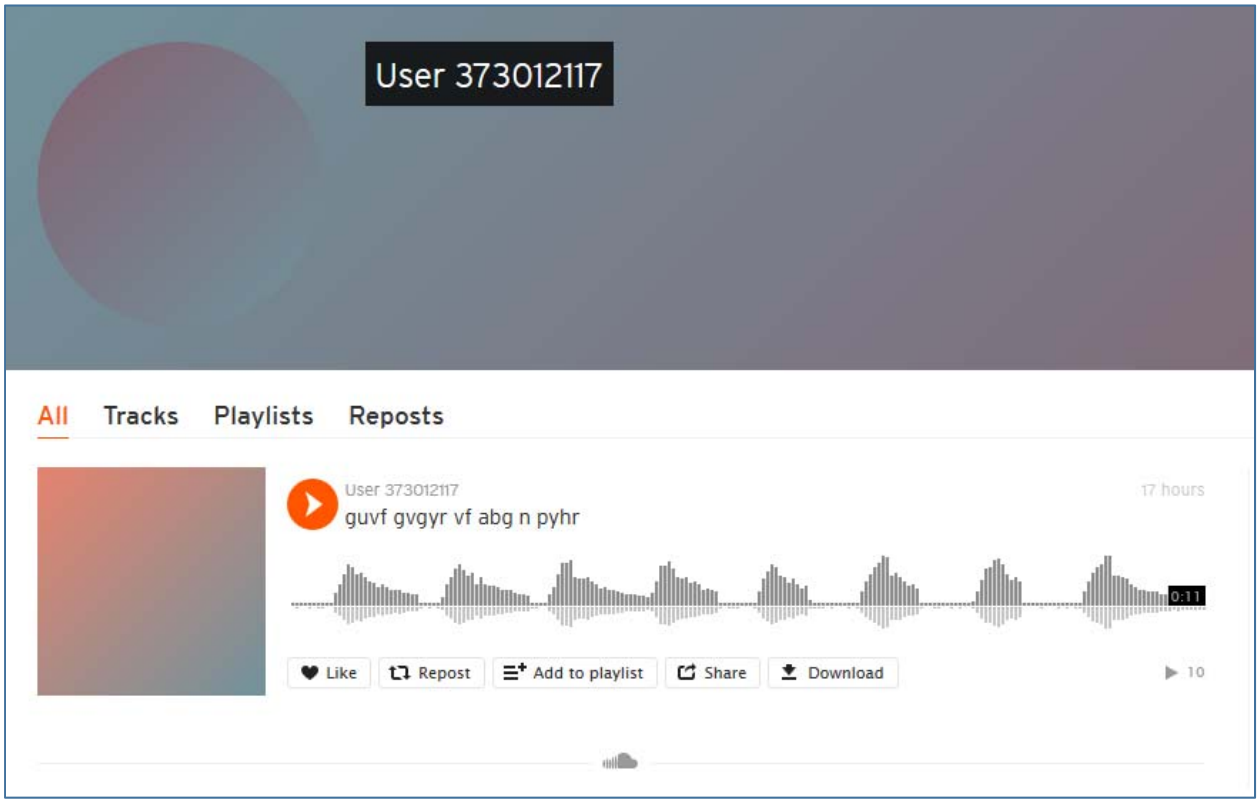
Upon doing so, the user is presented with a .wav file

The user will run into a few issues.

Firstly, it is an audio recording that is obfuscated.

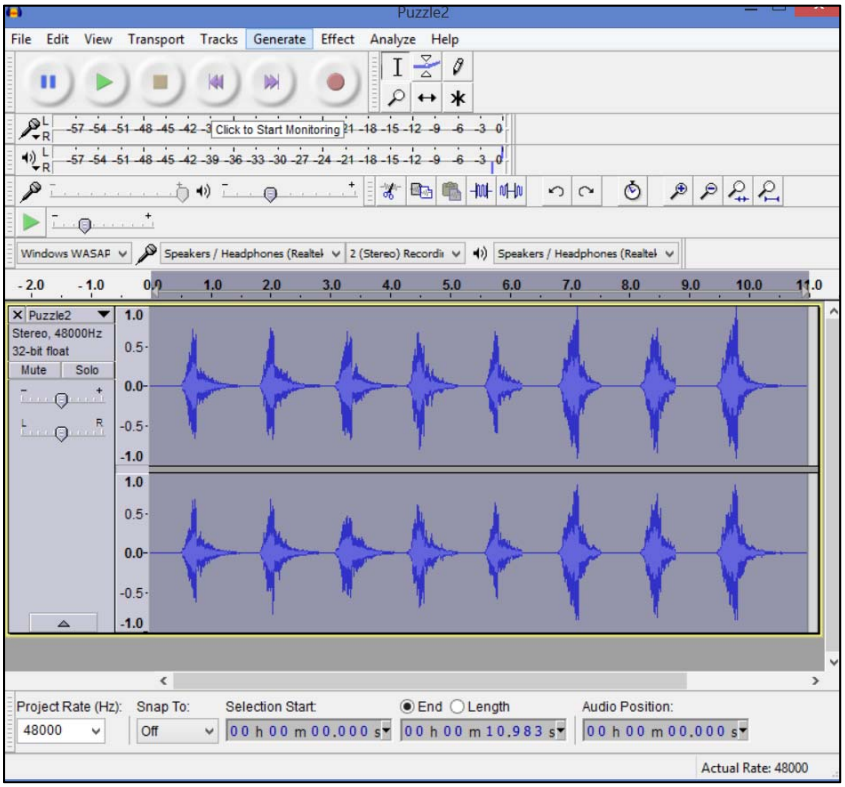
They also see that the title of the recording is some type of ciphertext. This is just a red herring – the title is a ROT13 cipher. When decrypted, it says “this title is not a clue”

The user can download the audio clip for further analysis:

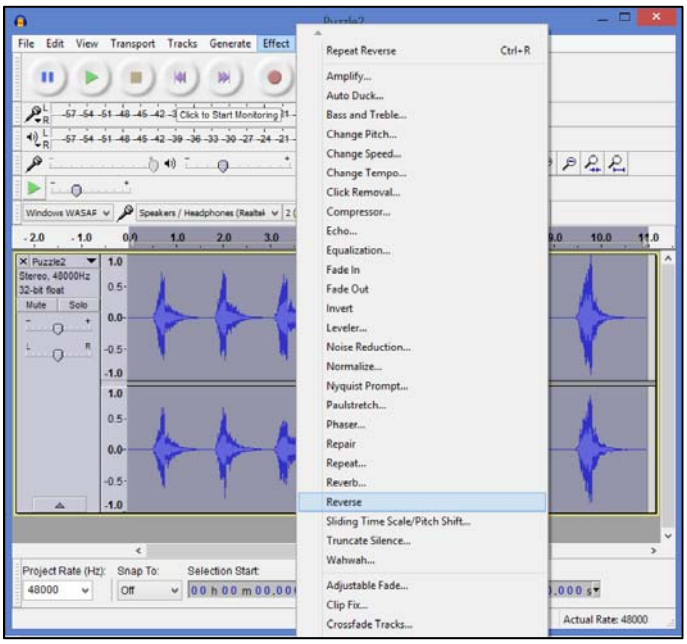


The user can download any type of audio software to investigate the wav file. I chose an open source program called Audacity from sourceforge.net

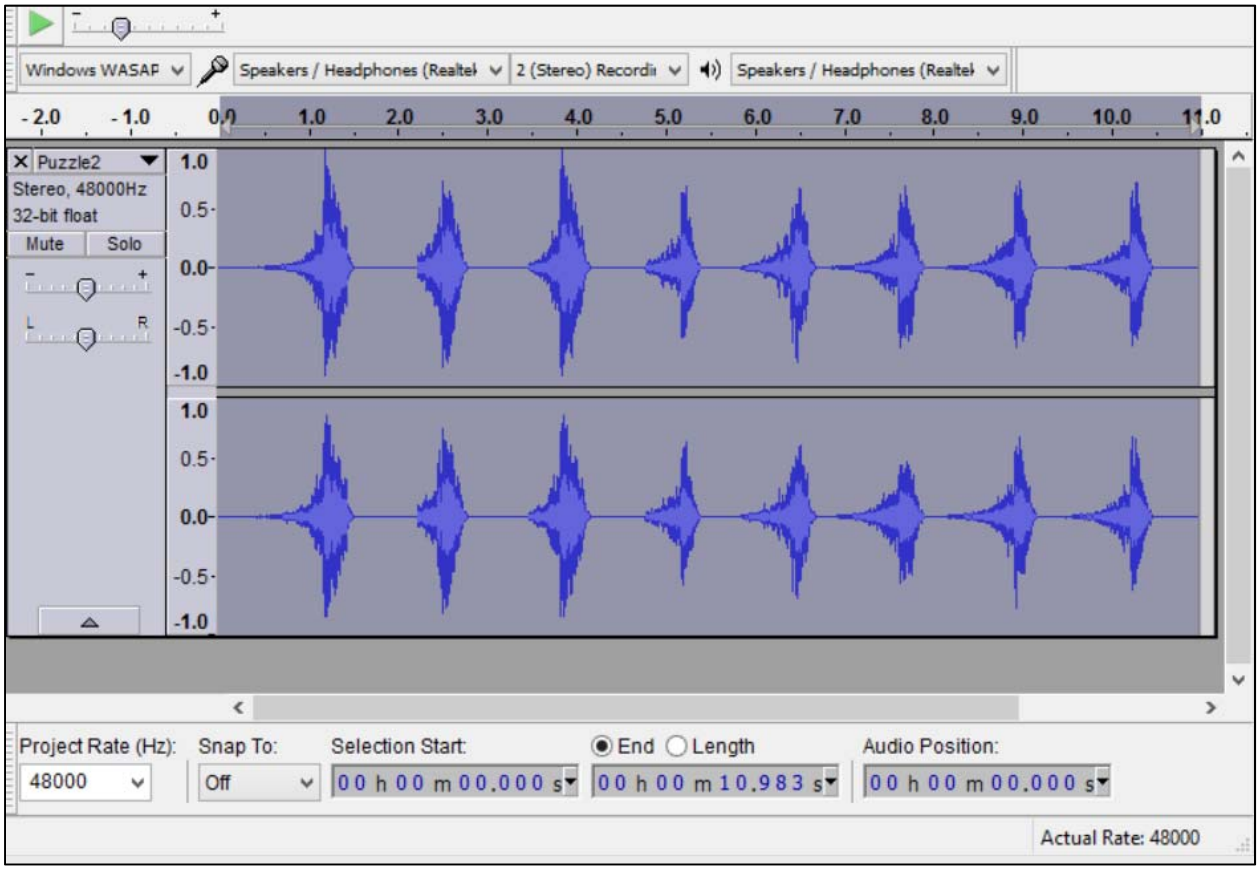
Upon opening the .wav file, the user can listen again for further inspection



The user will notice that the .wav file seems nonsensical. All the user has to do is reverse the track, or xor the bits.

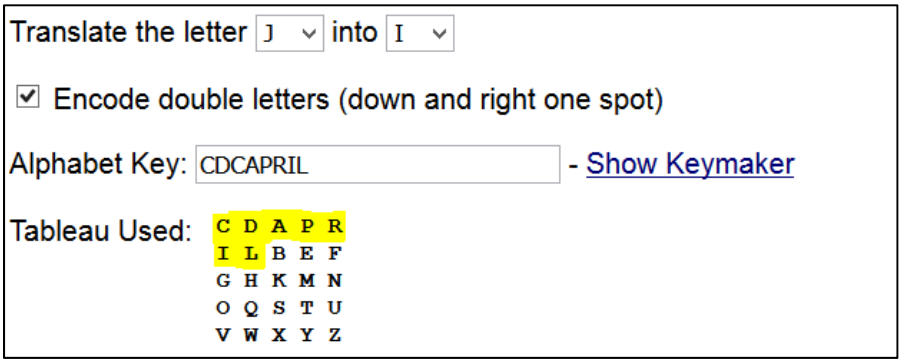


The user can then playback the audio, and the clip will play CDCAPRIL, which is the passphrase for the PDF file that the user cracked earlier in the challenge.



The final challenge will be deciding what type of cipher is applied to the PDF.

I used the Playfair cipher, which is a digraph substitution cipher. It employs a table where one letter of the alphabet is omitted, and the letters are arranged in a 5x5 grid. Typically, the J is removed from the alphabet and an I takes its place in the text that is to be encoded. Below is an unkeyed grid. However, Playfair ciphers do not utilize the letter if it is repeated in the alphabet key. So in the CDCAPRIL passphrase, the second C is omitted, making it CDAPRIL



The user can go to any cipher cracking website, such as rumkin.com and apply the passphrase and the encoded text to obtain the clue: