Writeup for I see wires everywhere

Name : I see wires everywhere

Description : In 2005, M@ssimo Banzi, with D@vid Mellis, another IDII student, and David Cuartielles, extended wiring by adding support for the cheaper ATmega8 microcontroller. The new project, forked from wiring, was called Arduino.

Difficulty : Medium

Points : 300

Domain : Steganography

Author : Ankush Kaudi, Naman Chordia, Yohaan Dhuri

Given files : lissen_carefully.wav & a_hint_for_you.jpg

We have been provided with two files a_hint_for_you.jpg and lissen_carefully.wav. Trying to extract hidden files from these using steghide,, it asks for passwords. From the description, we can see the first two names are written different. Trying massimobanzi as password for lissen_carefully.wav and davidmellis for a_hint_for_you.jpg, files get extracted as shown below.
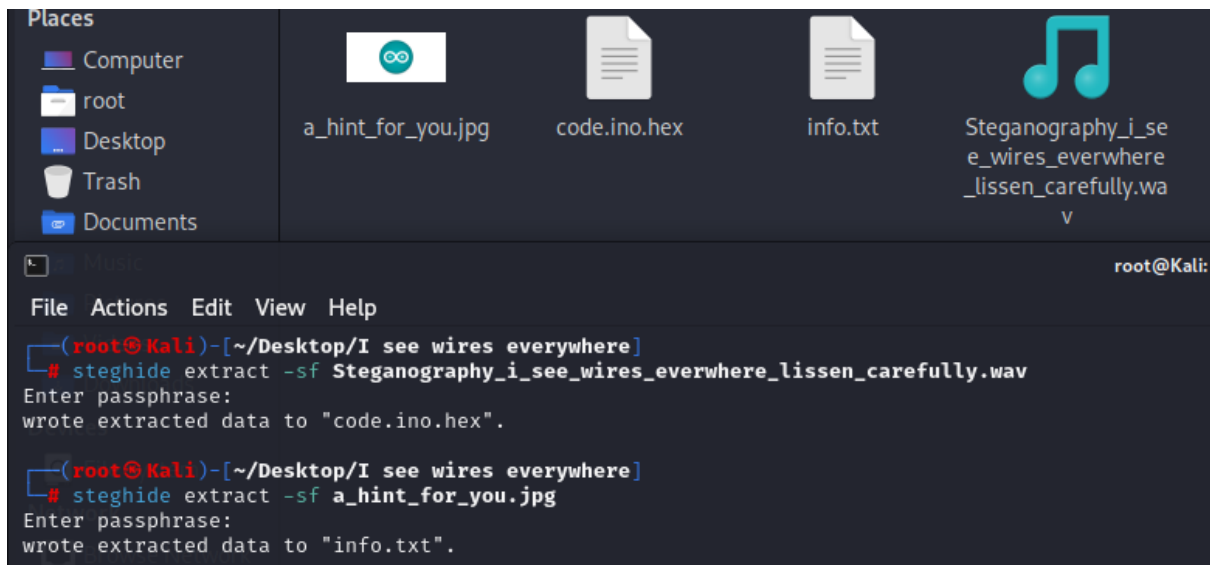

We can see code.ino.hex and info.txt files appeared. info.txt has the following data

```
1 Arduino Uno V2
2 LCD display
3 3 XOR Gates
4 4 Logic Toggle
```

This text files tells about the electronic components and their quantity. Reversing the audio given gives the hint of making connections. We can assume building a circuit using these components might get us the flag. Also, using Arduino in simulation requires a hex file, looking for some simulation softwares like Proteus make it possible. According to the audio, the connections will look as follows.
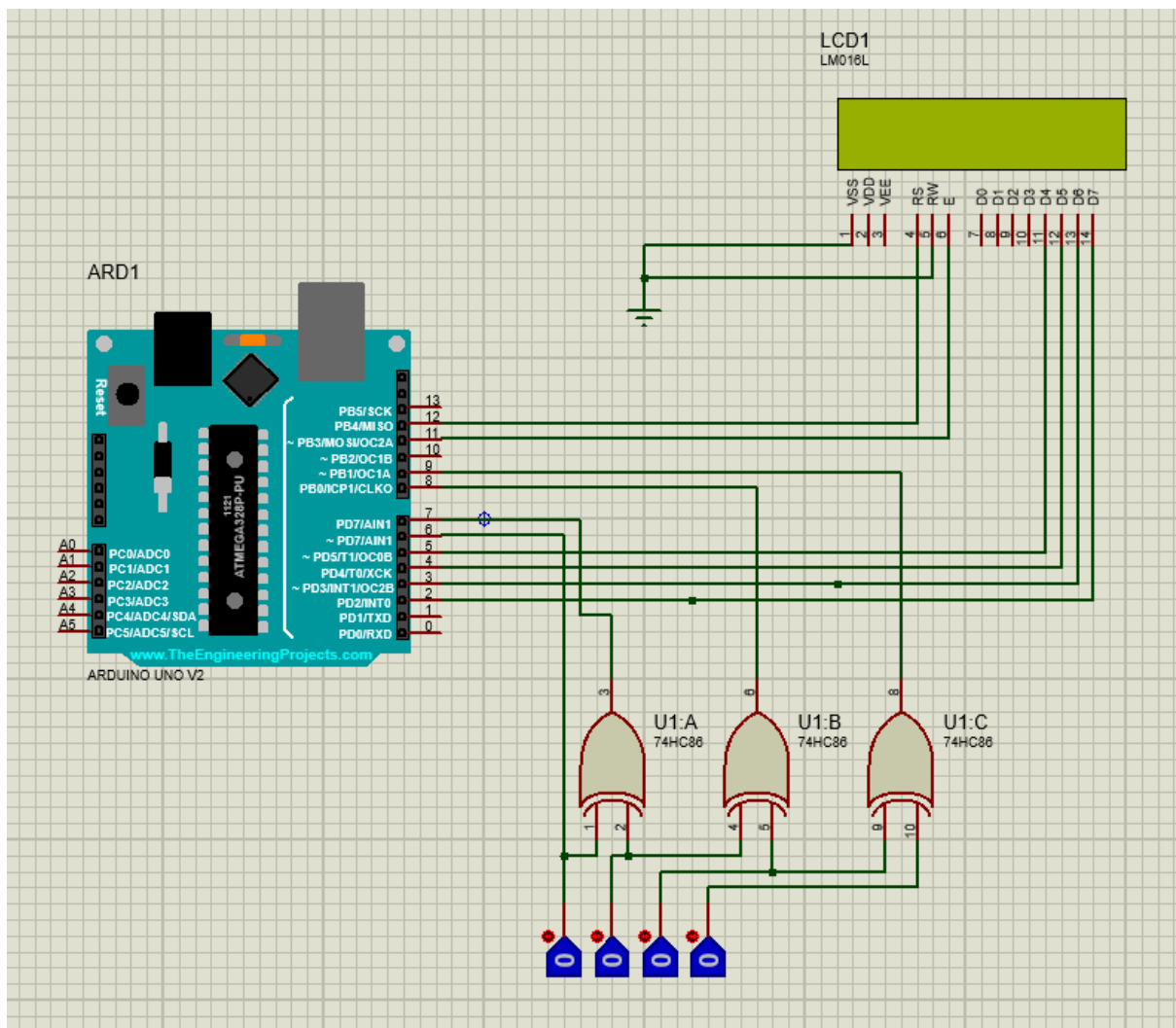

Giving the obtained hex file as input to the Arduino, the circuit starts working and LCD begins to display as follows.
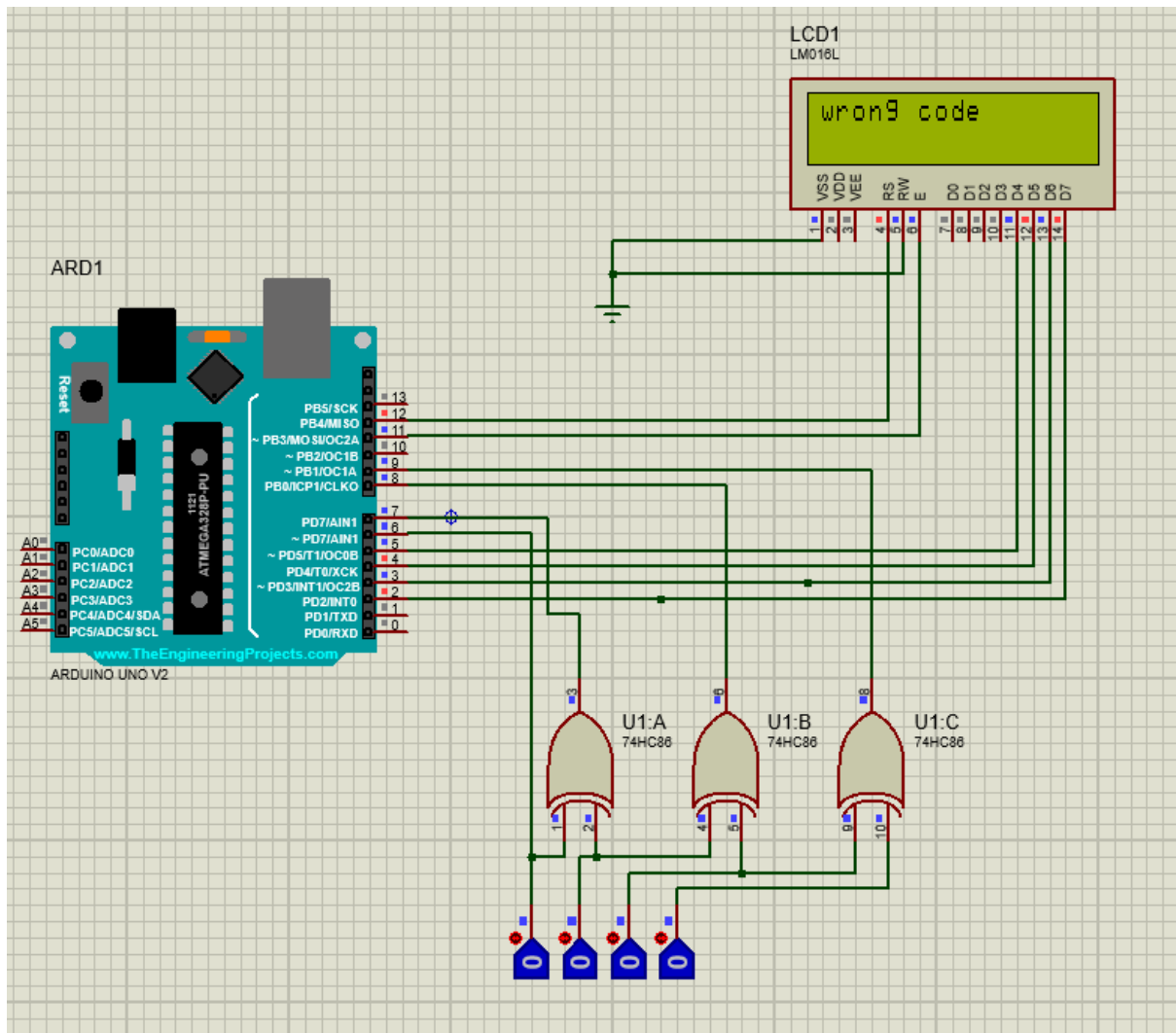
But the flag is not displaying, maybe a correct input to logic toggle may give us the flag. Looking at some other steganographic methods, we can try exiftool on the image.

```
XMP Toolkit       : Image::ExifTool 12.48
Certificate       : Grey code is 1110 enter binary
Image Width       : 1919
Image Height      : 972
Encoding Process  : Baseline DCT, Huffman coding
Bits Per Sample   : 8
```

We can see in the certificate tag, a message is written as "Grey code is 1110 enter binary", entering binary value can give us the flag For grey code 1110, the binary will be 1011. Trying out this in the circuit gives the flag on the LCD screen.
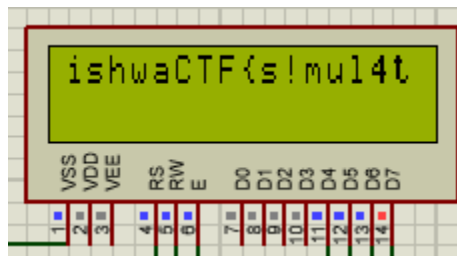
Flag : VishwaCTF{s!mul4t3_b3f0r3_!mpl3m3nt4t!0n}