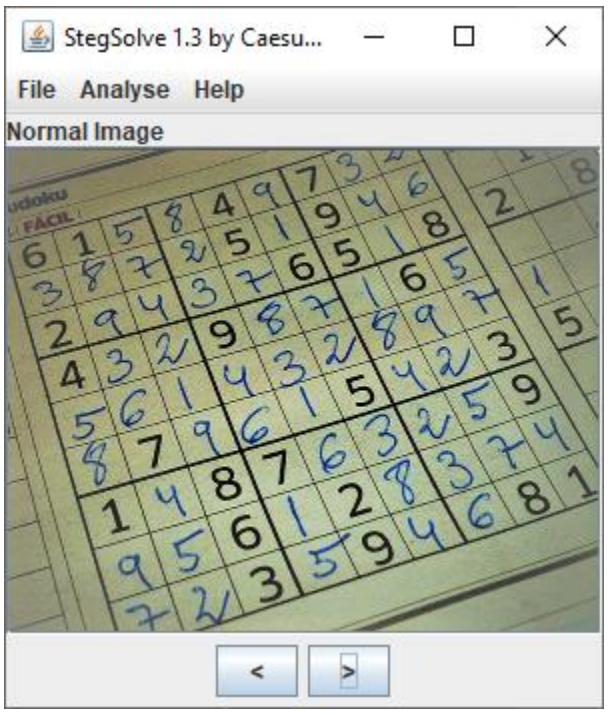
Dragomir Ioan – trupples

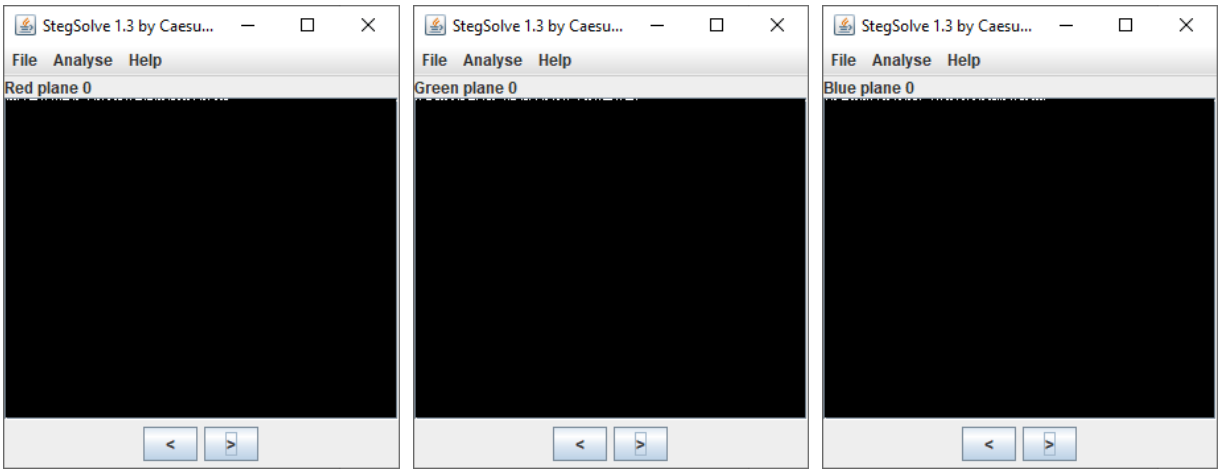
NSU Crypto 2020 first round, problem 5 "Mysterious event"

This is a classic LSB steganography problem. PNG's lossless compression allows us to encode information by subtly changing the image colors (in this case, using the least significant bit to bear our data), and we know that change will persist, unlike in a lossy compression format like JPEG.

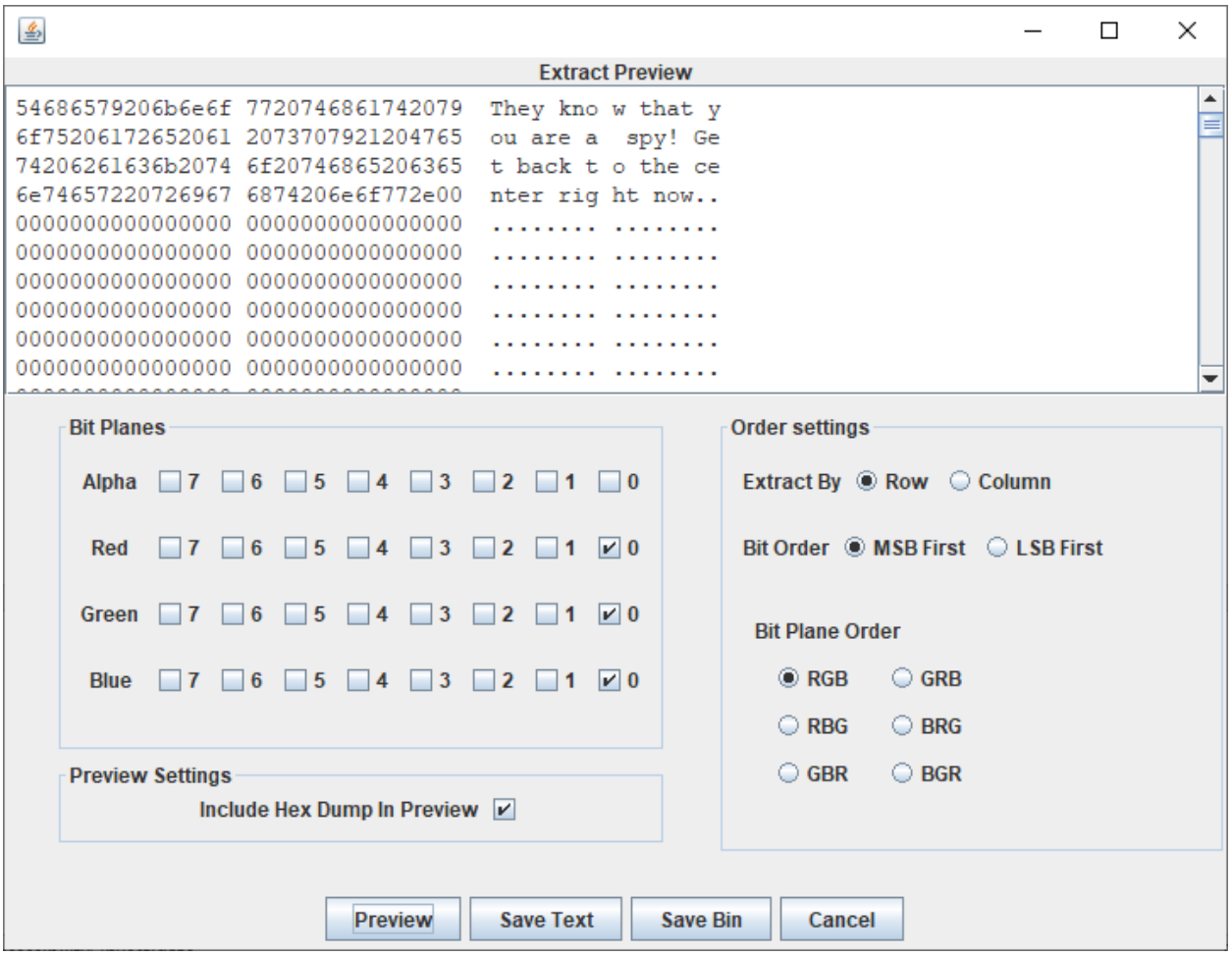
The first tool I try on lossless stegano problems is the infamous stegsolve.jar.



I immediately go to bit plane 0 of each color channel and notice the telltale signs of LSB stegano: it is almost full with zeros (whereas an actual image would have a random distribution of 0 and 1), except for the very beginning, the first row:



Stegsolve has an integrated tool for LSB extraction in Analyse>Data extract, which helps us successfully extract the message:



They know that you are a spy! Get back to the center right now.

We now know that Mr. Bob “disappeared” by going to the spy center, whatever that is.