Roman Vish

CSA

End of Semester CTF

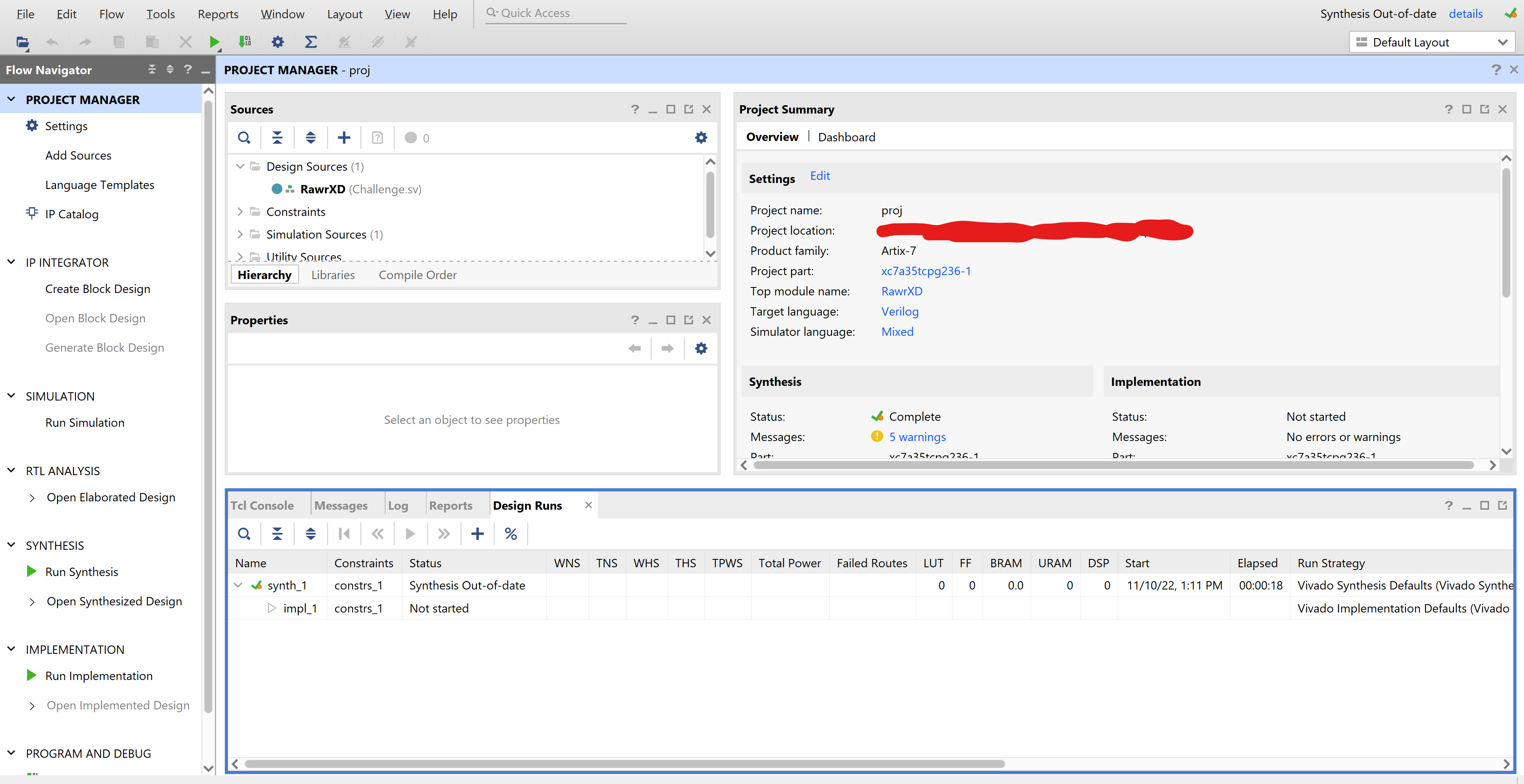
11/10/22

Flying Pterodactyls Going Away

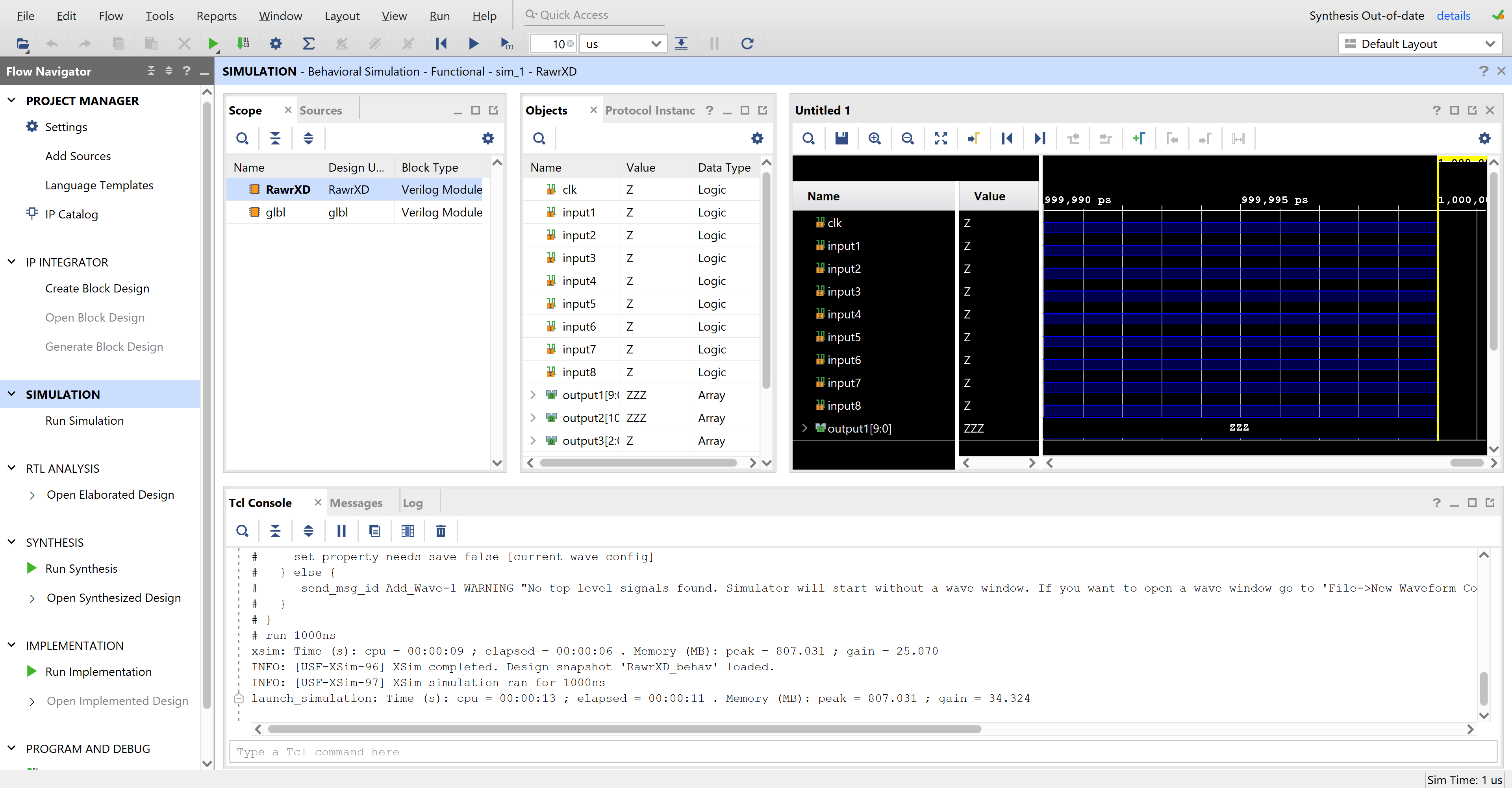
There are a variety of ways to go about solving this challenge. For convenience, I will only go through the two easiest.

Solution #1:

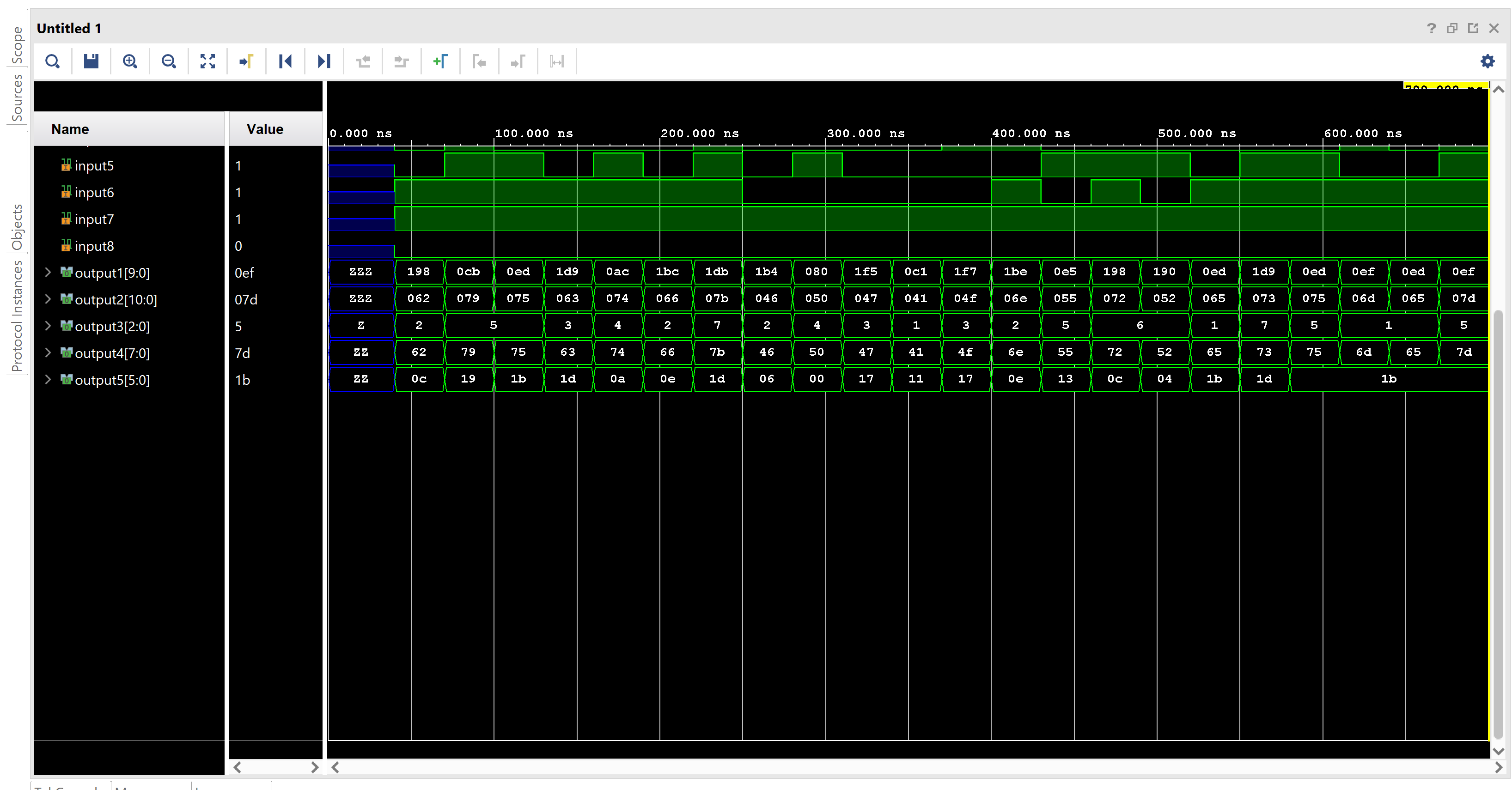
Upon unzipping the file the user must investigate the directory and first notice that there is a Vivado Project File (proj.xpr), if the user has Vivado, they can simply open the project file and be greeted with a pre-configured project that has everything they need. That looks like this:



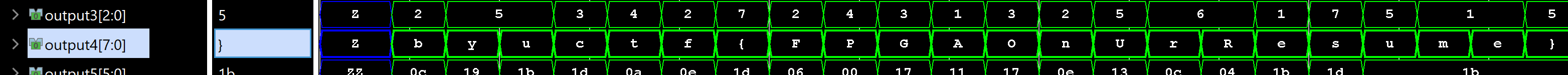
If the user does not have Vivado, it is an open-source FPGA programmer that has a free lab version available on Xilinx.com and they can download it. The easiest track from here is to poke around the interface and click “Run Simulation”, upon which this screen will show:



After the user clicks “Tools” on the toolbar, a dropdown will have an option to “Run Tcl Script” and the user can then select the already implemented, and in same directory TryThis.tcl. After running that script, and investigating the waveform, they see something that looks like this:



Upon noticing that output4 only has printable ASCII values, the user can right click on the output4 variable and go down to “Radix” and hit ASCII to reveal the flag:



Byuctf{FPGAOnUrResume}

Solution #2:

The other way to do this is significantly hard and more time consuming. Choosing to not download Vivado, the user can learn SystemVerilog and notice that only two of the outputs have the required 8 bits for an ASCII character and manually go through the .tcl file and replace the bit values with 1s or 0s as shown in the script. It will be extremely time consuming and not at all fun, but technically it still is possible.