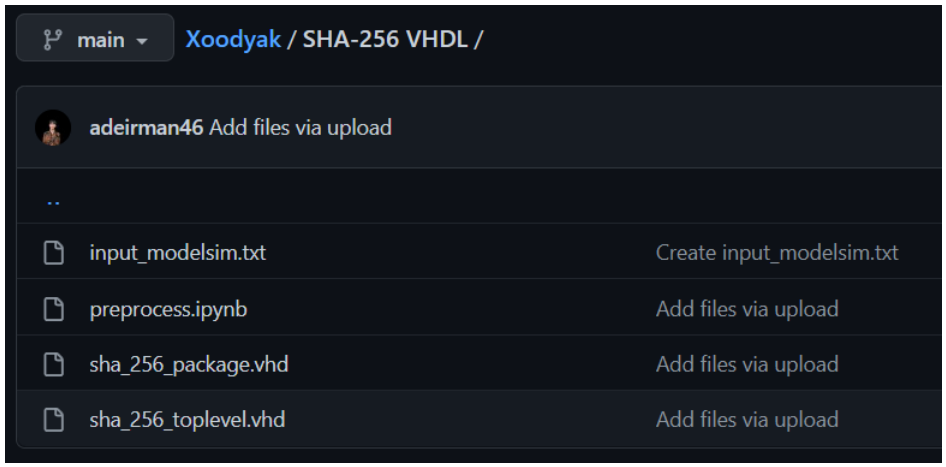
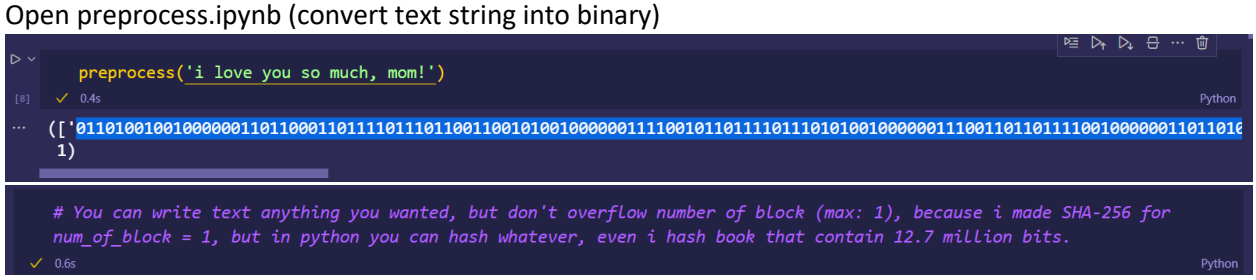
HOW TO USE SHA-256 USING MODELSIM

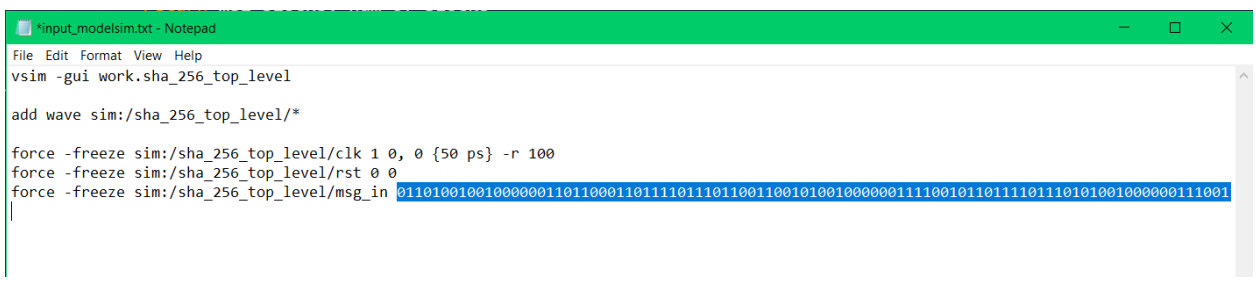
1. Download those 4 files



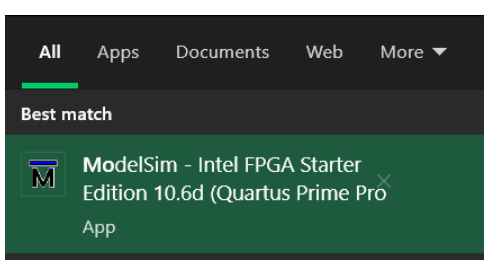
2. Open preprocess.ipynb (convert text string into binary)



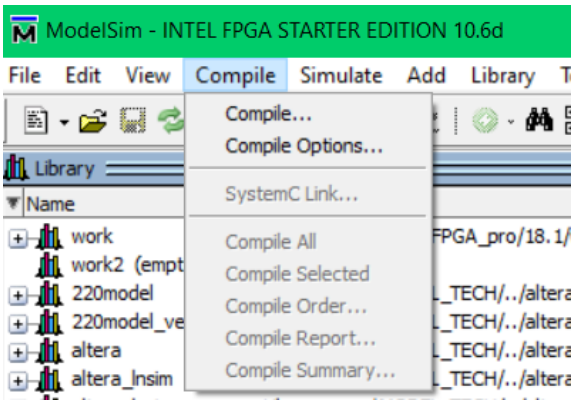
3. Copy and paste that binary into input_modelsim.txt

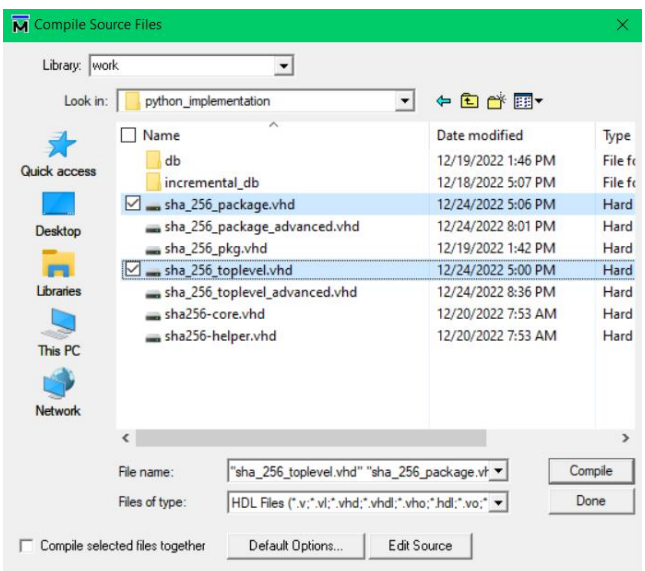


4. Open ModelSim

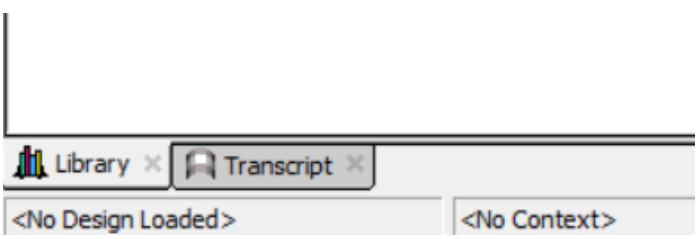


5. Compile **sha_256_toplevel.vhd** and **sha_256_package.vhd**, make sure you know the location of your file.





6. You can see whether your compile is success or not in Transcript



```
# Reading C:/intelFPGA_pro/18.1/modelsim_ase/tcl/vsim/pref.tcl
vcom -reportprogress 300 -work work {C:/Users/adeir/Documents/Tubes Sisdig/python_implementation/sha_256_package.vhd}
# Model Technology ModelSim - Intel FPGA Edition vcom 10.6d Compiler 2018.02 Feb 24 2018
# Start time: 07:08:16 on Dec 27,2022
# vcom -reportprogress 300 -work work C:/Users/adeir/Documents/Tubes Sisdig/python_implementation/sha_256_package.vhd
# -- Loading package STANDARD
# -- Loading package TEXTIO
# -- Loading package std_logic_1164
# -- Loading package NUMERIC_STD
# -- Compiling package sha_256_package
# -- Compiling package body sha_256_package
# -- Loading package sha_256_package
# End time: 07:08:16 on Dec 27,2022, Elapsed time: 0:00:00
# Errors: 0, Warnings: 0
vcom -reportprogress 300 -work work {C:/Users/adeir/Documents/Tubes Sisdig/python_implementation/sha_256_toplevel.vhd}
# Model Technology ModelSim - Intel FPGA Edition vcom 10.6d Compiler 2018.02 Feb 24 2018
# Start time: 07:08:16 on Dec 27,2022
# vcom -reportprogress 300 -work work C:/Users/adeir/Documents/Tubes Sisdig/python_implementation/sha_256_toplevel.vhd
# -- Loading package STANDARD
# -- Loading package TEXTIO
# -- Loading package std_logic_1164
# -- Loading package NUMERIC_STD
# -- Loading package sha_256_package
# -- Compiling entity sha_256_top_level
# -- Compiling architecture sha_256_arch of sha_256_top_level
# End time: 07:08:16 on Dec 27,2022, Elapsed time: 0:00:00
# Errors: 0, Warnings: 0
```

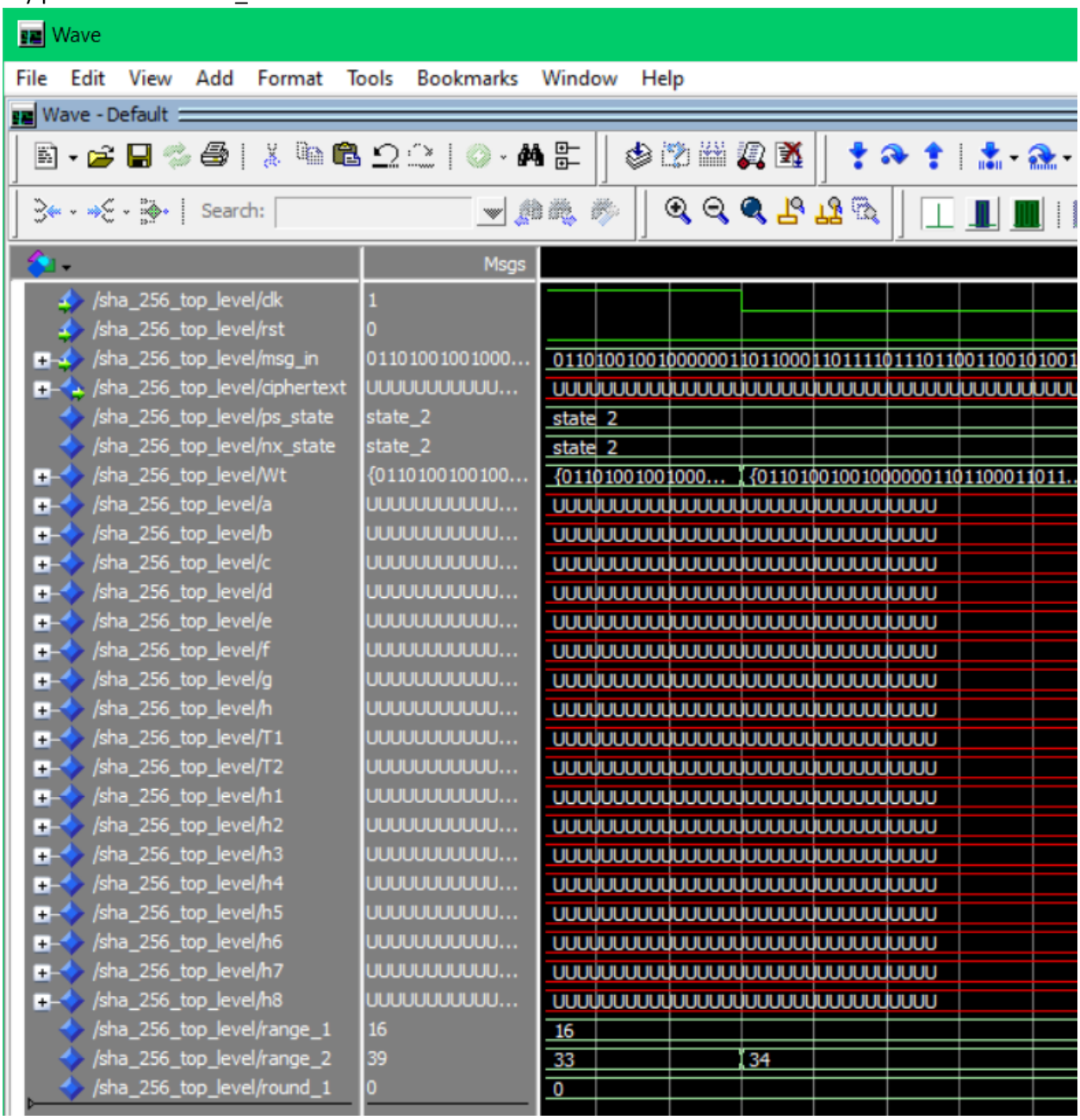
As you can see, both of them are successfully compiled, 0 Errors and 0 Warnings.

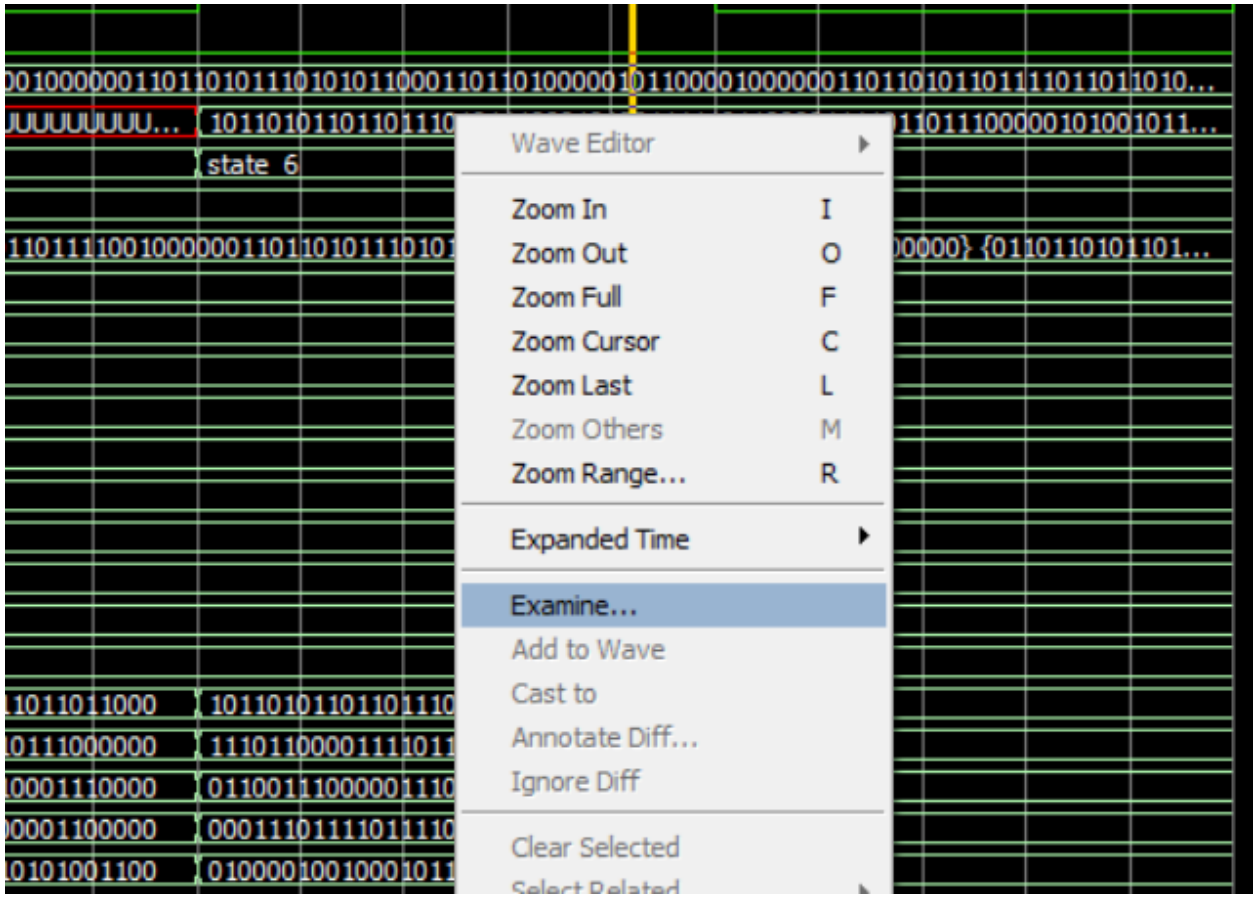
7. Copy Paste input_modelsim.txt into Transcript

```
ModelSim> vsim -gui work.sha_256_top_level

add wave sim:/sha_256_top_level/*

force -freeze sim:/sha_256_top_level/clk 1 0, 0 {50 ps} -r 100
force -freeze sim:/sha_256_top_level/rst 0 0
force -freeze sim:/sha_256_top_level/msg_in 01101001001000000110110001101111011101100110010100100000011110010110111101110101 00
01111011011010010000110000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000011000000
```

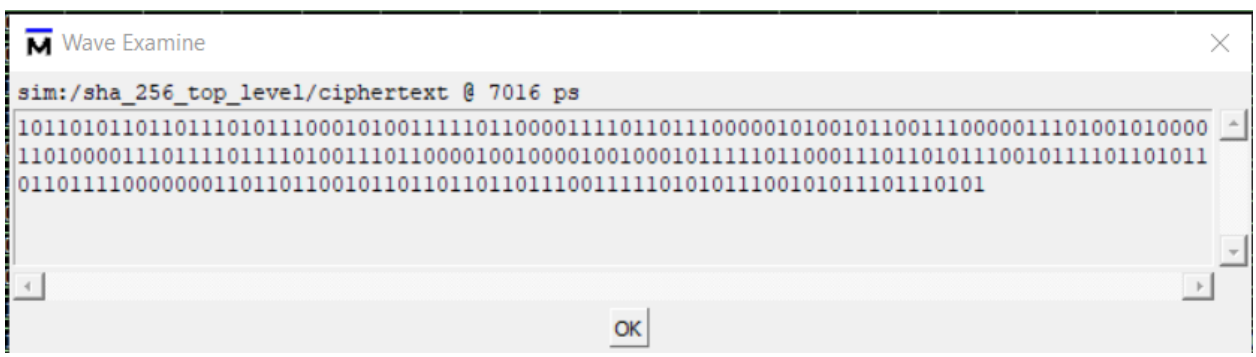
Then click enter!

8. Try press F9 until state_6





Ciphertext is the message digest (Output), to view it, right-click then Examine



TRIVIA

1. Guys, don't worry. Maybe you know SHA-256 has 64 rounds but why it is show 0-64 not 0-63? It is because when i < 64 it will i = i + 1, thus when i = 63, it still add 1.

/sha_256_top_level/range_1	16
/sha_256_top_level/range_2	64
/sha_256_top_level/round_1	64

It also happen in range_1 (0-15). Okay? Don't be frightened.

2. If you wan't to know your Wt (round constant), you can inspect it by "Right-click -> Examine"

3. If you have any questions regarding the SHA-256 algorithm I've made, please email me @adeirman2705.