Purpose

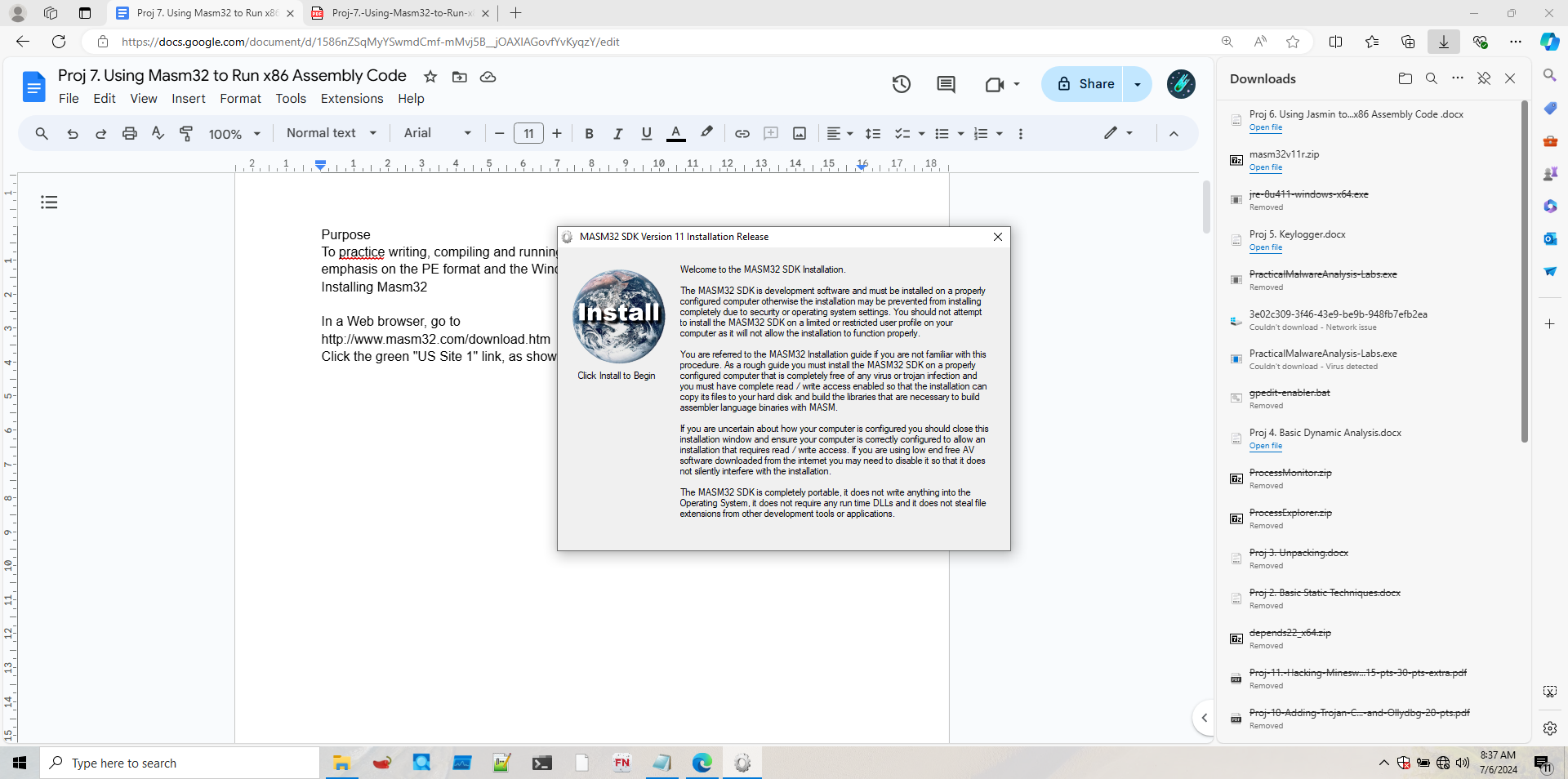
To practice writing, compiling and running basic Windows x86 assembly code, with particular emphasis on the PE format and the Windows API.

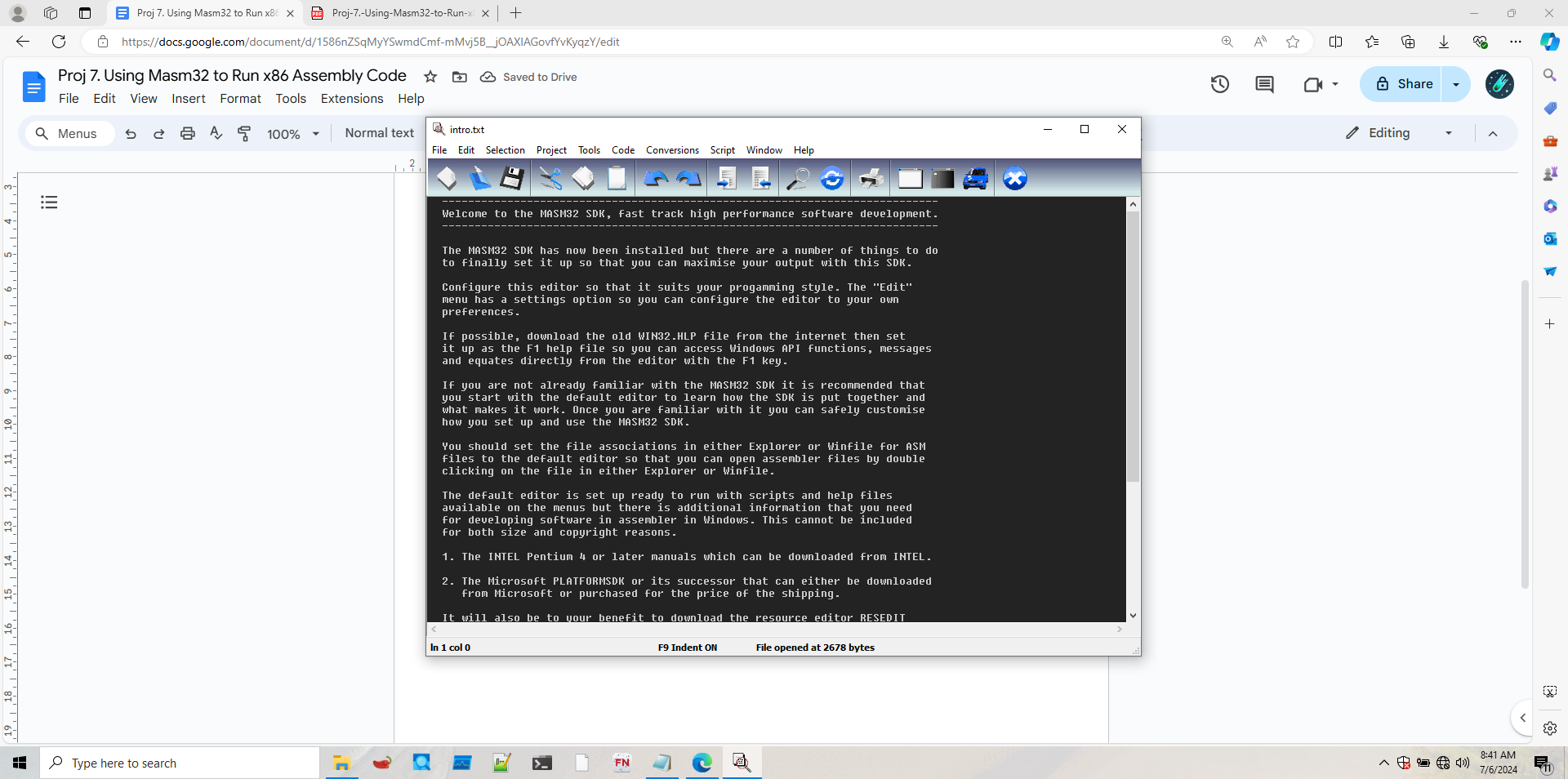
Installing Masm32

In a Web browser, go to

http://www.masm32.com/download.htm

Click the green "US Site 1" link, as shown below.





7.1 "Hello, World!"

In the MASM32 Editor menu bar, click File, New. Paste in the code below

.486 ; create 32 bit code

.model flat, stdcall ; 32 bit memory model

option casemap :none ; case sensitive

include \masm32\include\windows.inc ; always first

include \masm32\macros\macros.asm ; MASM support macros

; -----------------------------------------------------------------

; include files that have MASM format prototypes for function calls

; -----------------------------------------------------------------

include \masm32\include\masm32.inc

include \masm32\include\gdi32.inc

include \masm32\include\user32.inc

include \masm32\include\kernel32.inc

; ------------------------------------------------

; Library files that have definitions for function

; exports and tested reliable prebuilt code.

; ------------------------------------------------

includelib \masm32\lib\masm32.lib

includelib \masm32\lib\gdi32.lib

includelib \masm32\lib\user32.lib

includelib \masm32\lib\kernel32.lib

.code ; Tell MASM where the code starts

; Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«

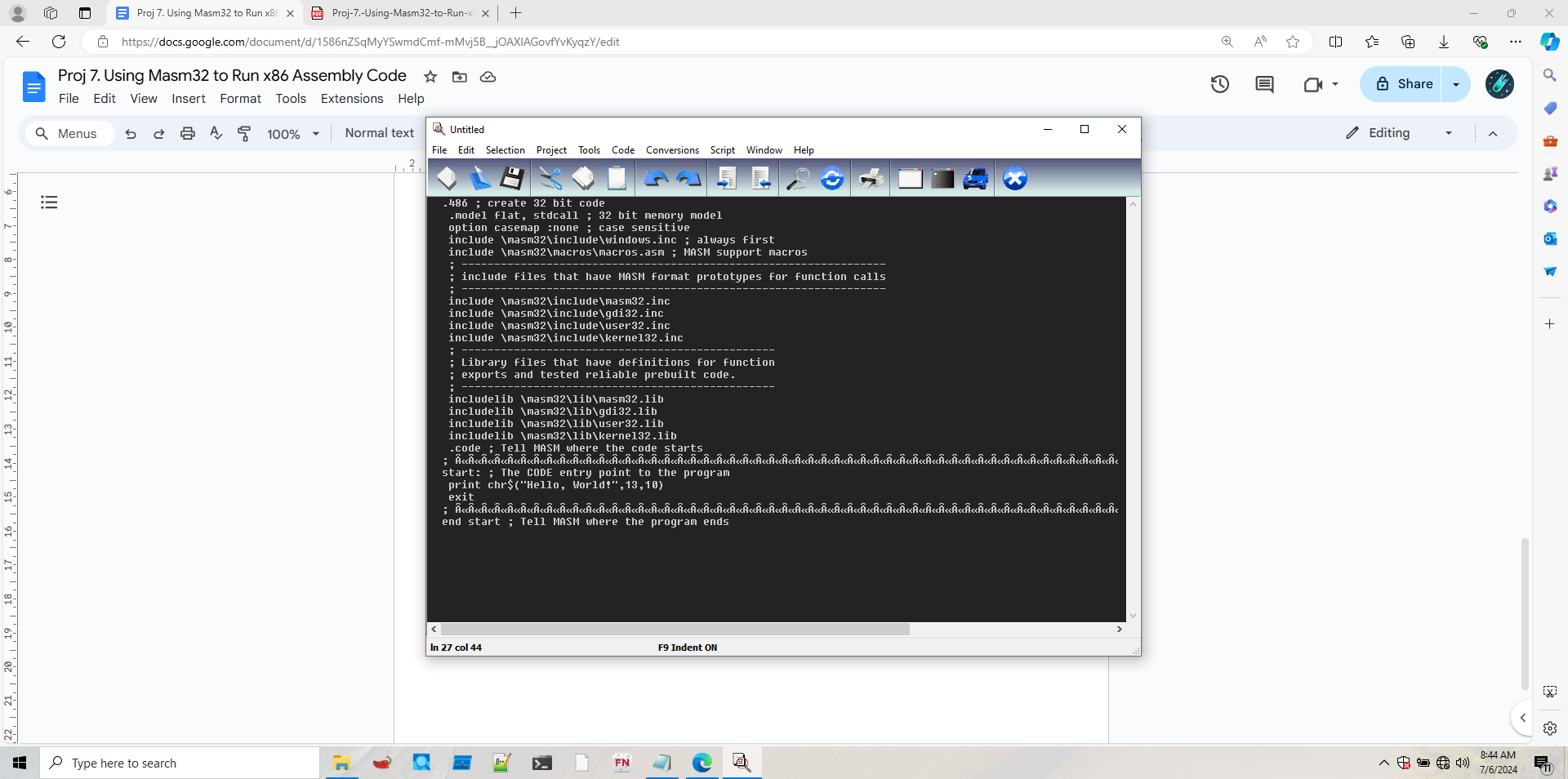
start: ; The CODE entry point to the program

print chr$("Hello, World!",13,10)

exit

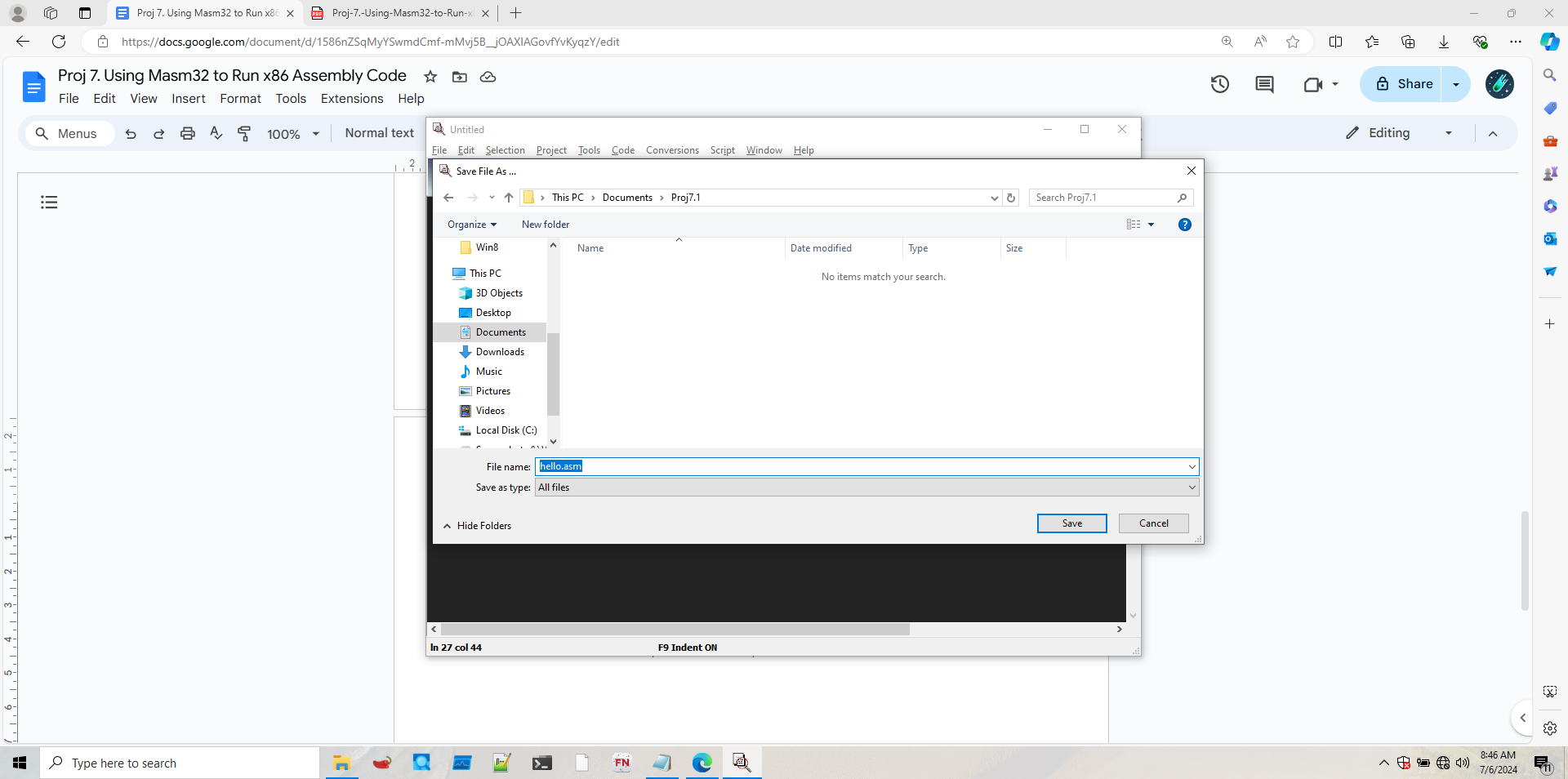
; Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«Â«

end start ; Tell MASM where the program ends



From the menu bar, click File, Save. In the "Save File As..." box, click "Browse Folders". Navigate to your Documents folder, as shown below. Right-click an empty portion of the folder pane and click New, Folder.

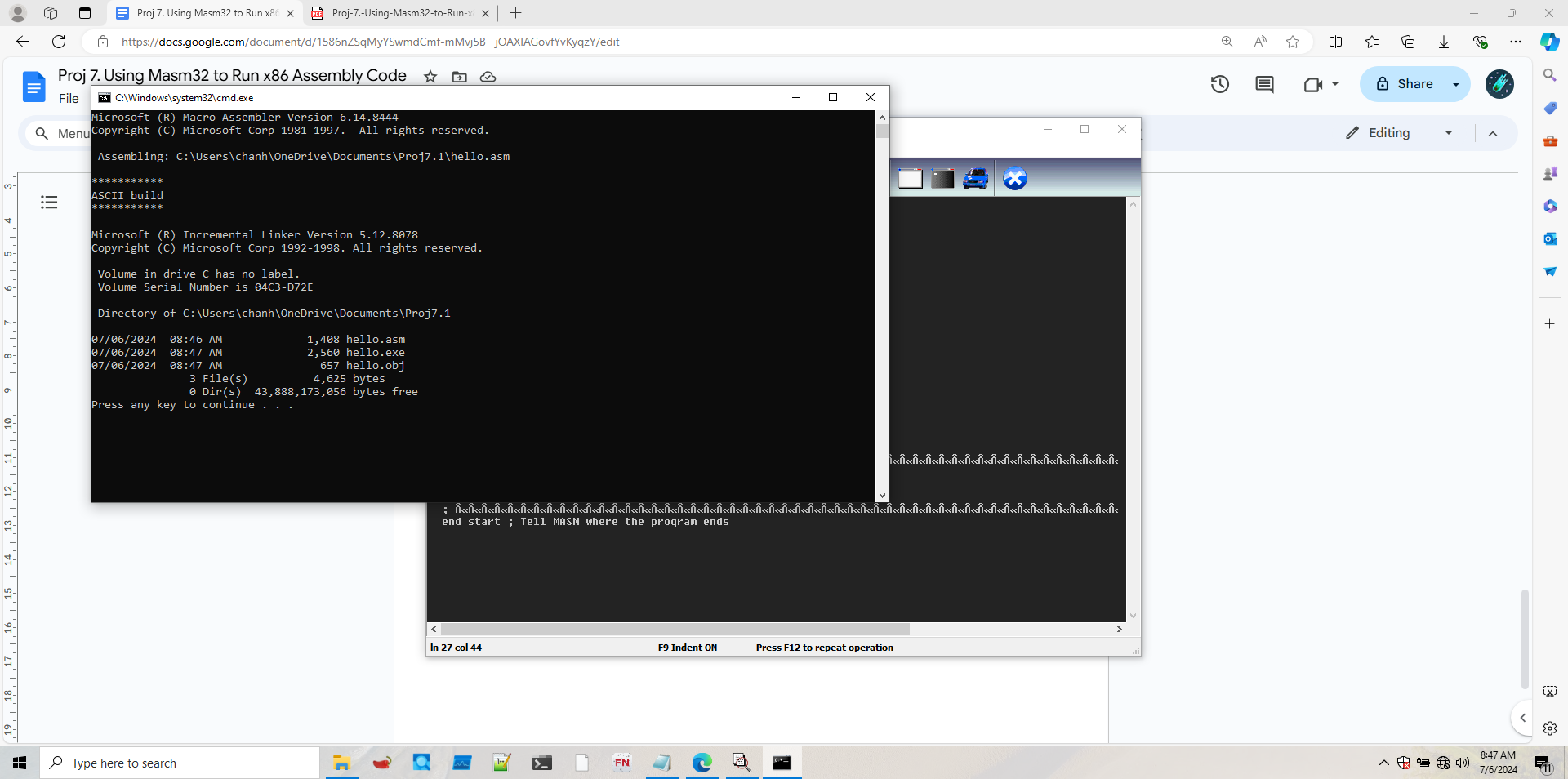
Name the new folder Proj7.1 and press Enter to open the new folder, as shown below



Enter a filename of hello.asm, as shown below, and click Save

From the MASM32 menu bar, click Project, "Console Build All".

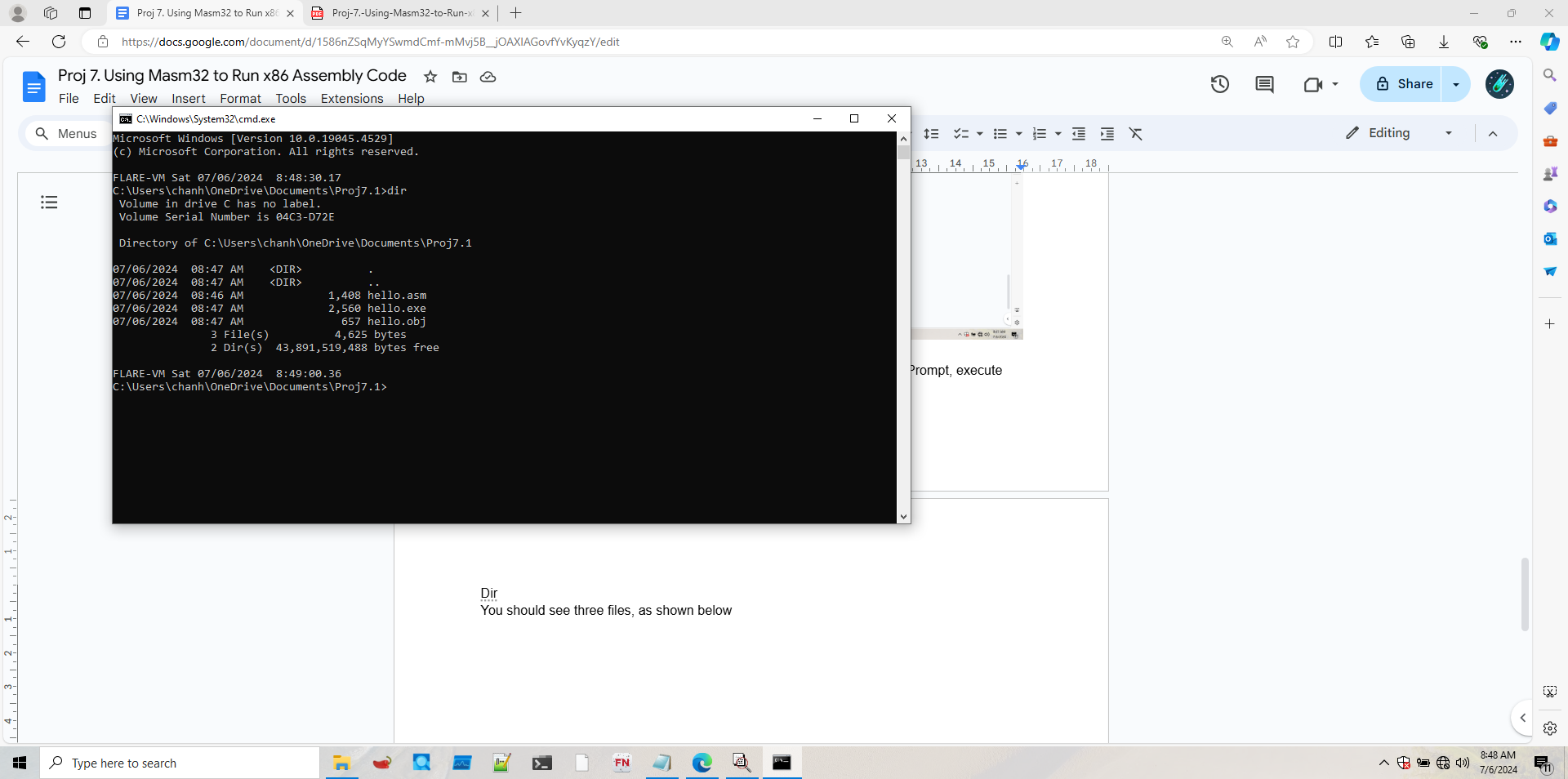
A Command Prompt window opens, saying "Press any key to continue...", as shown below



From the MASM32 menu bar, click File, "Cmd Prompt". In the Command Prompt, execute this command:

Dir

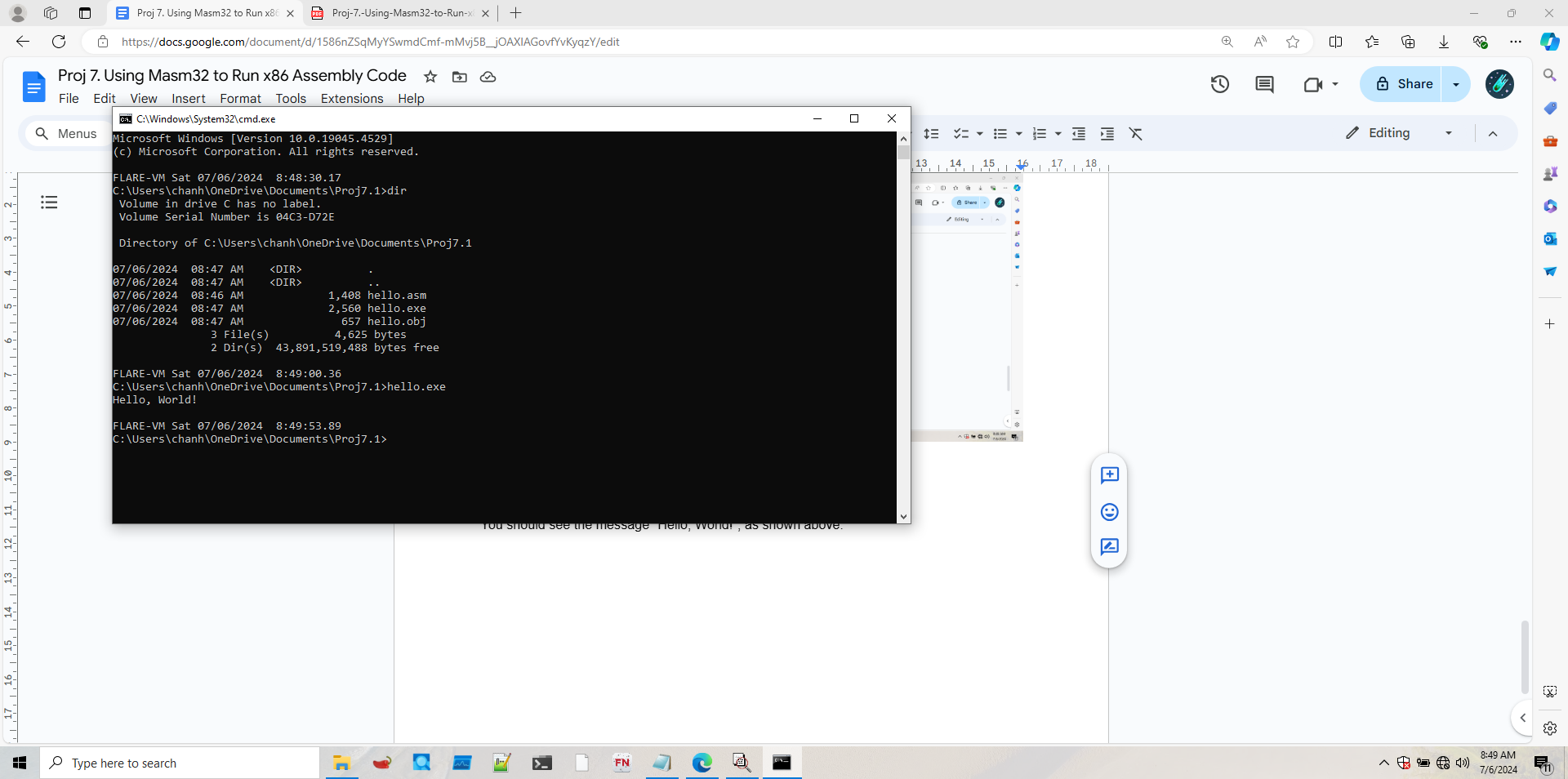
You should see three files, as shown below



In the Command Prompt, execute this command:

hello.exe

You should see the message "Hello, World!", as shown above

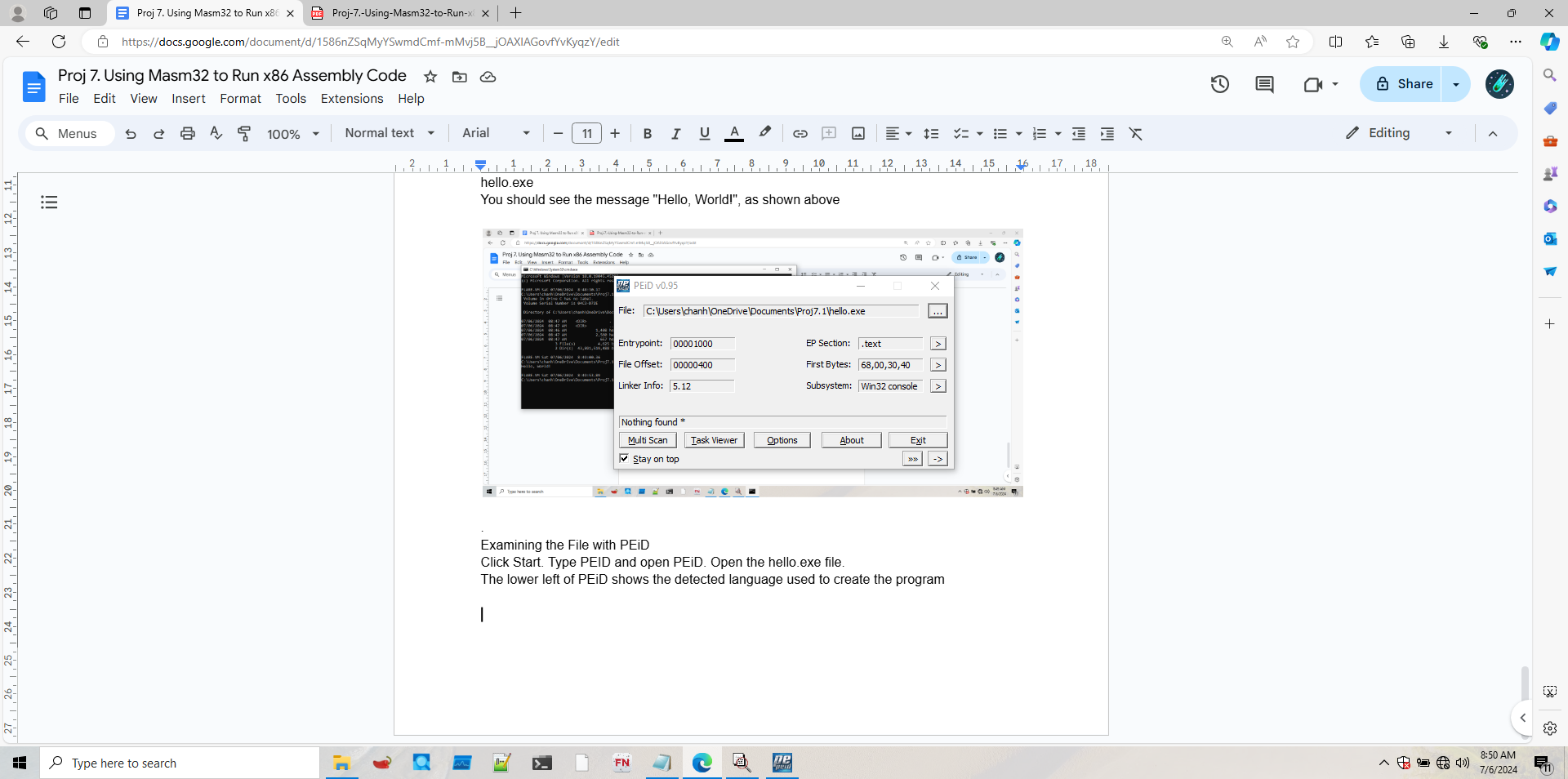


.

Examining the File with PEiD

Click Start. Type PEID and open PEiD. Open the hello.exe file.

The lower left of PEiD shows the detected language used to create the program

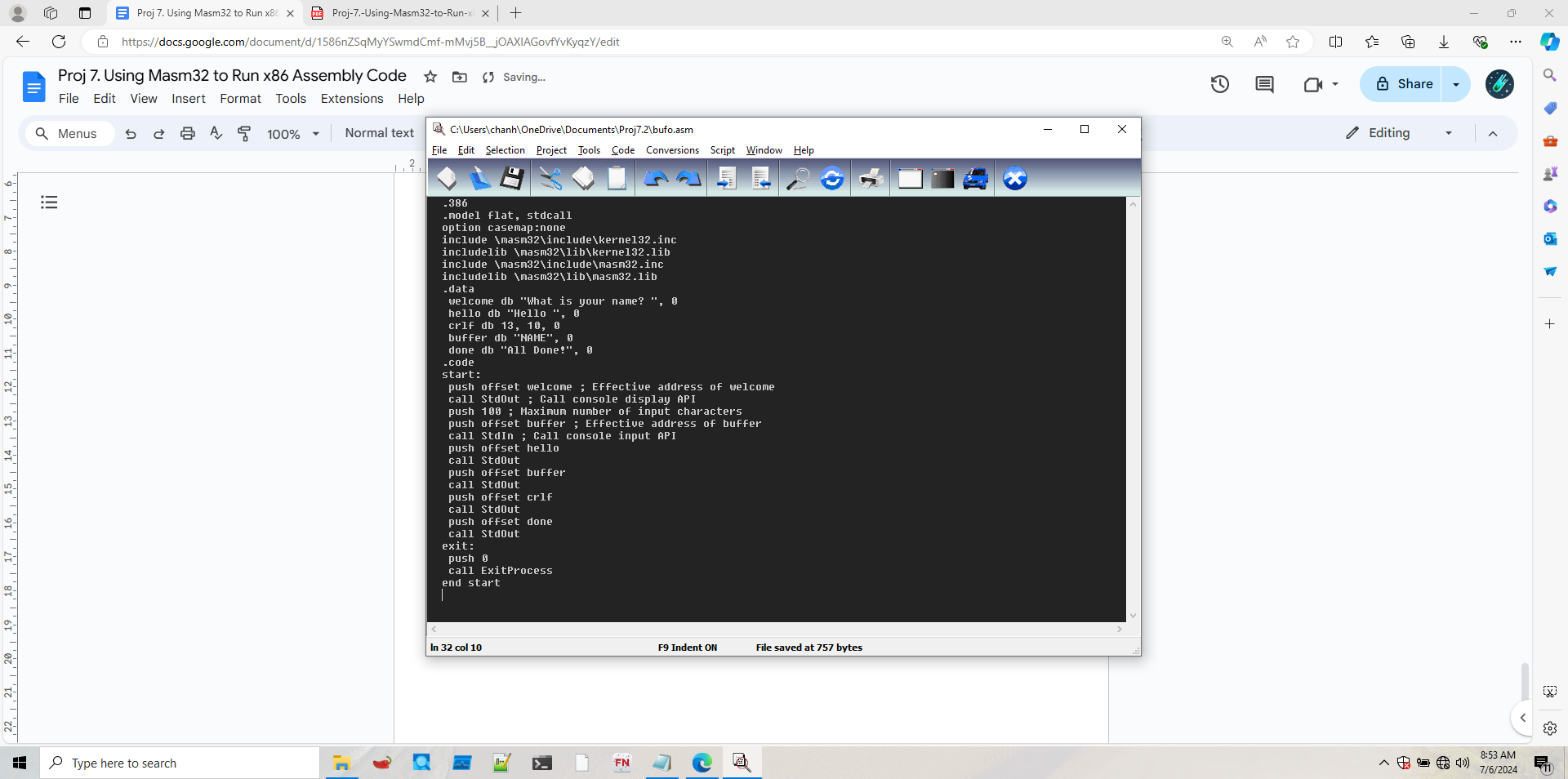


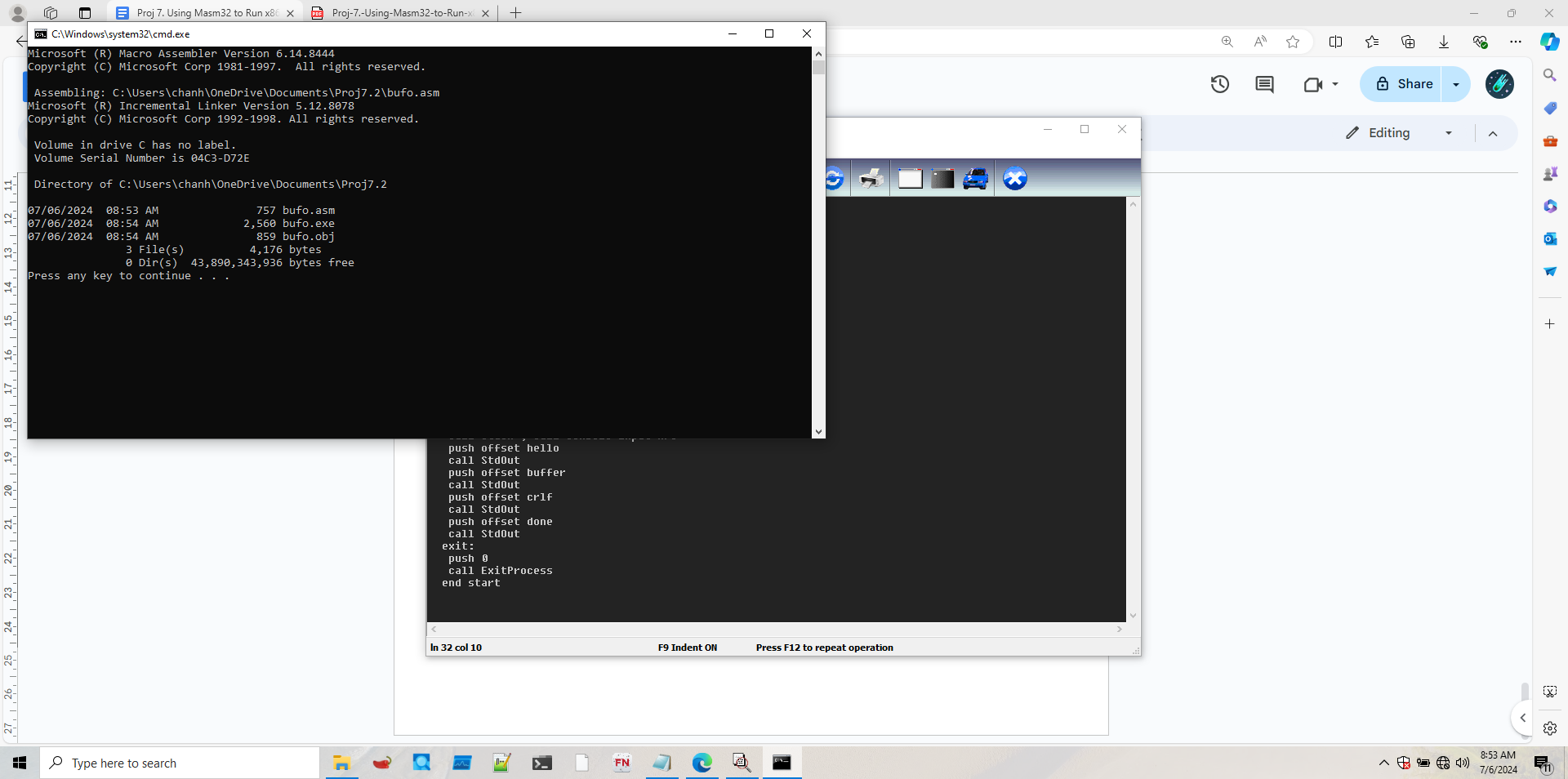
7.2 Buffer Overflow

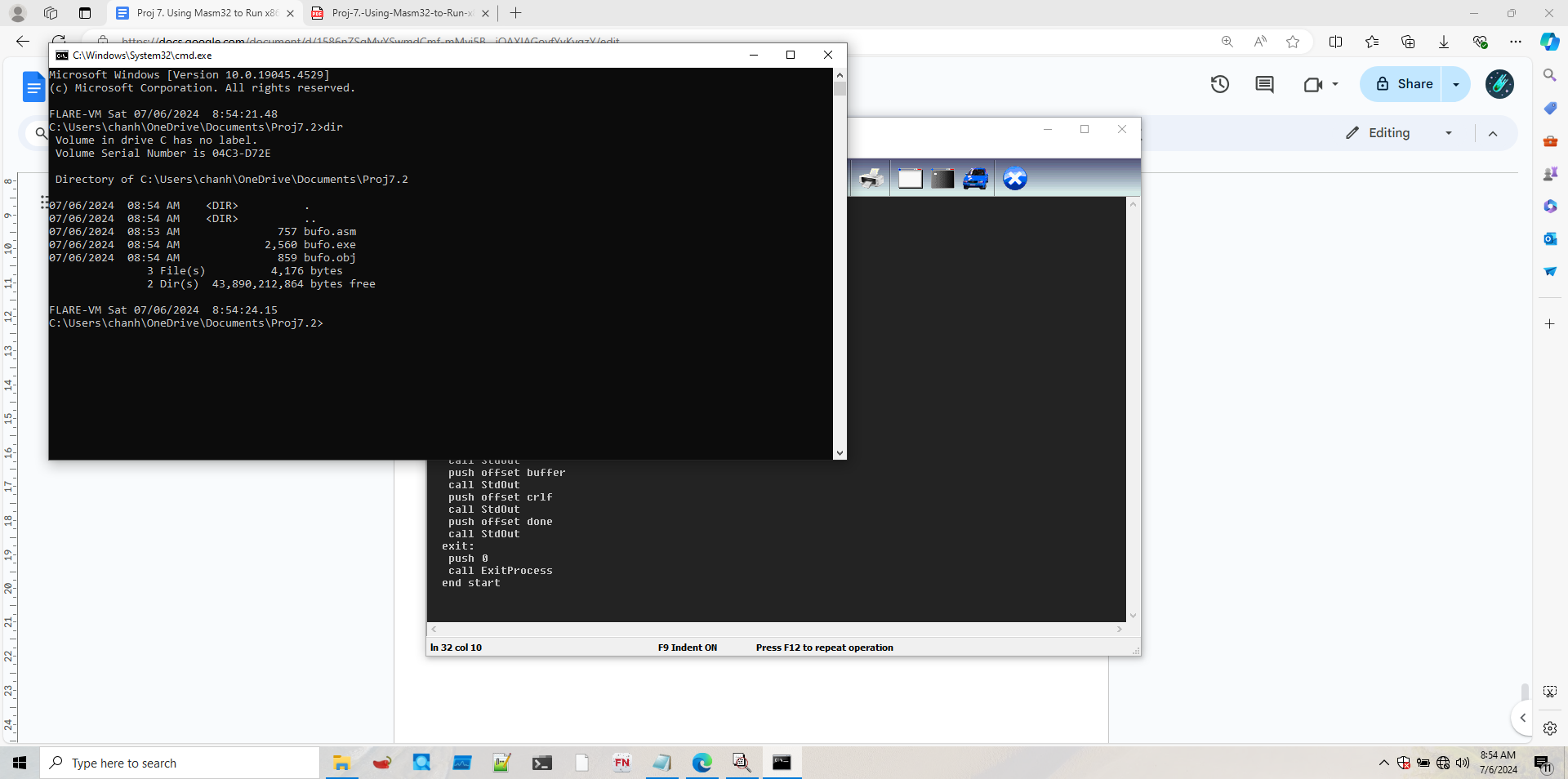
In the MASM32 Editor menu bar, click File, New.

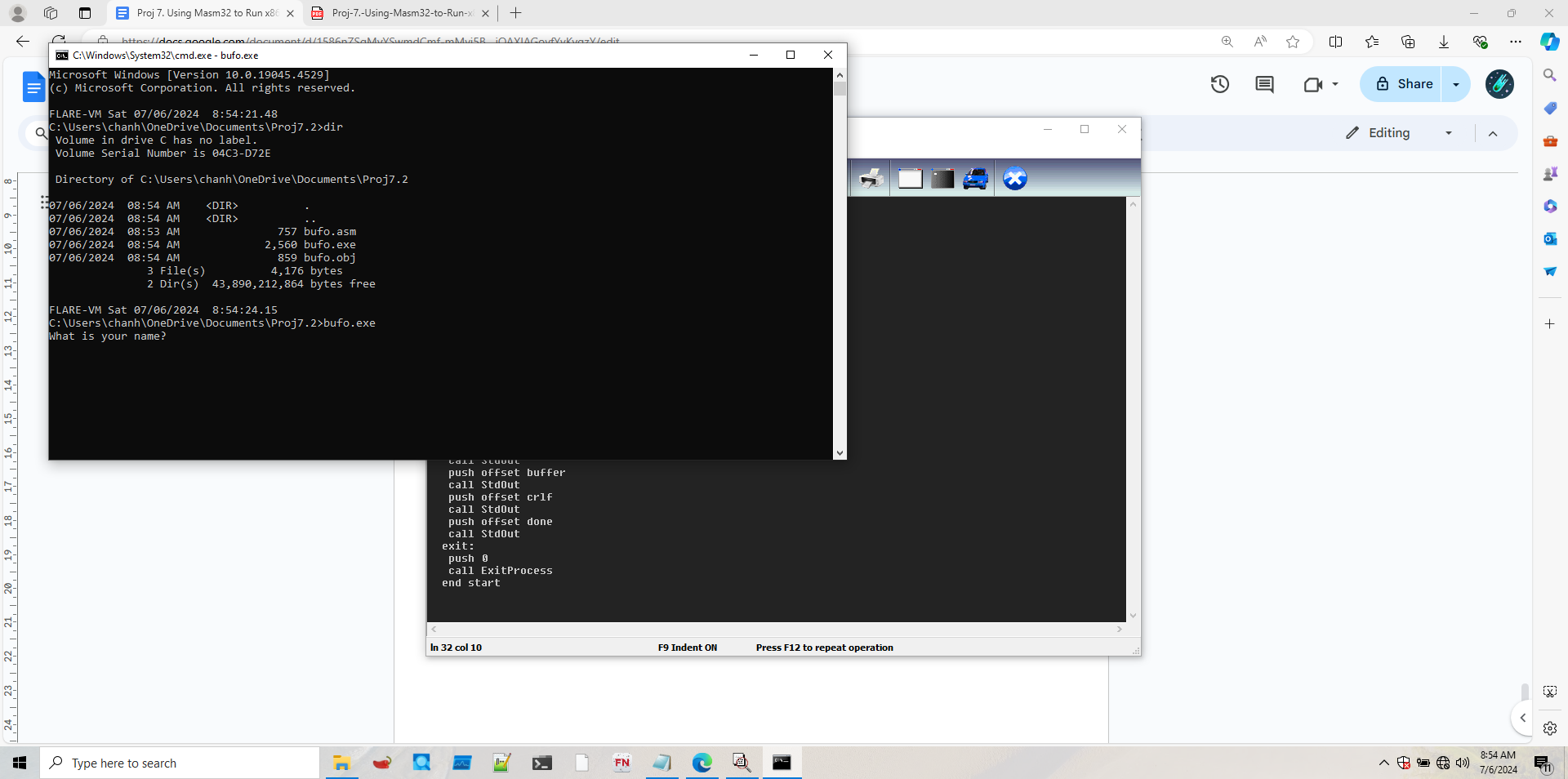
Paste in the code below

Do exactly like hello word

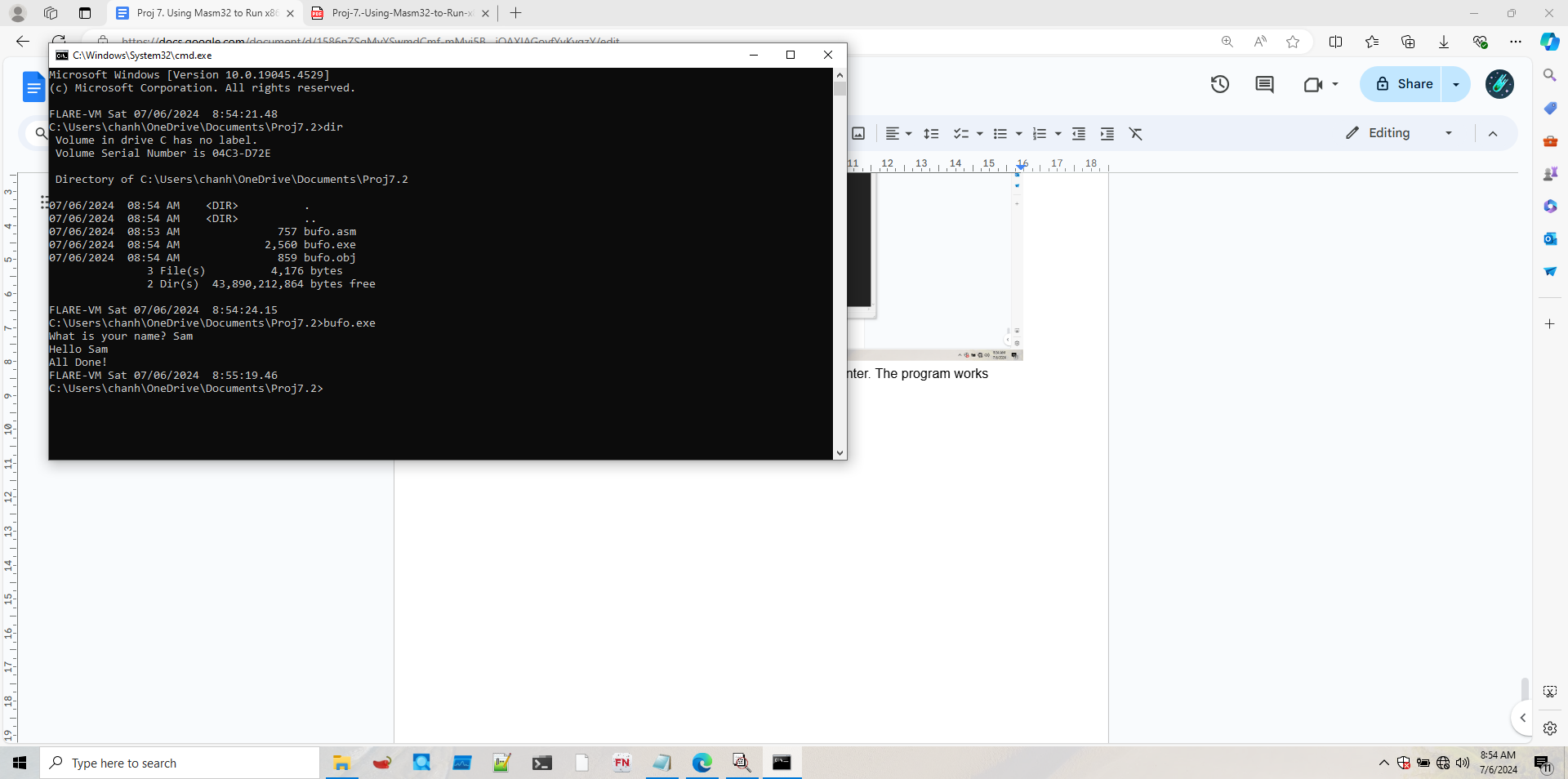


\

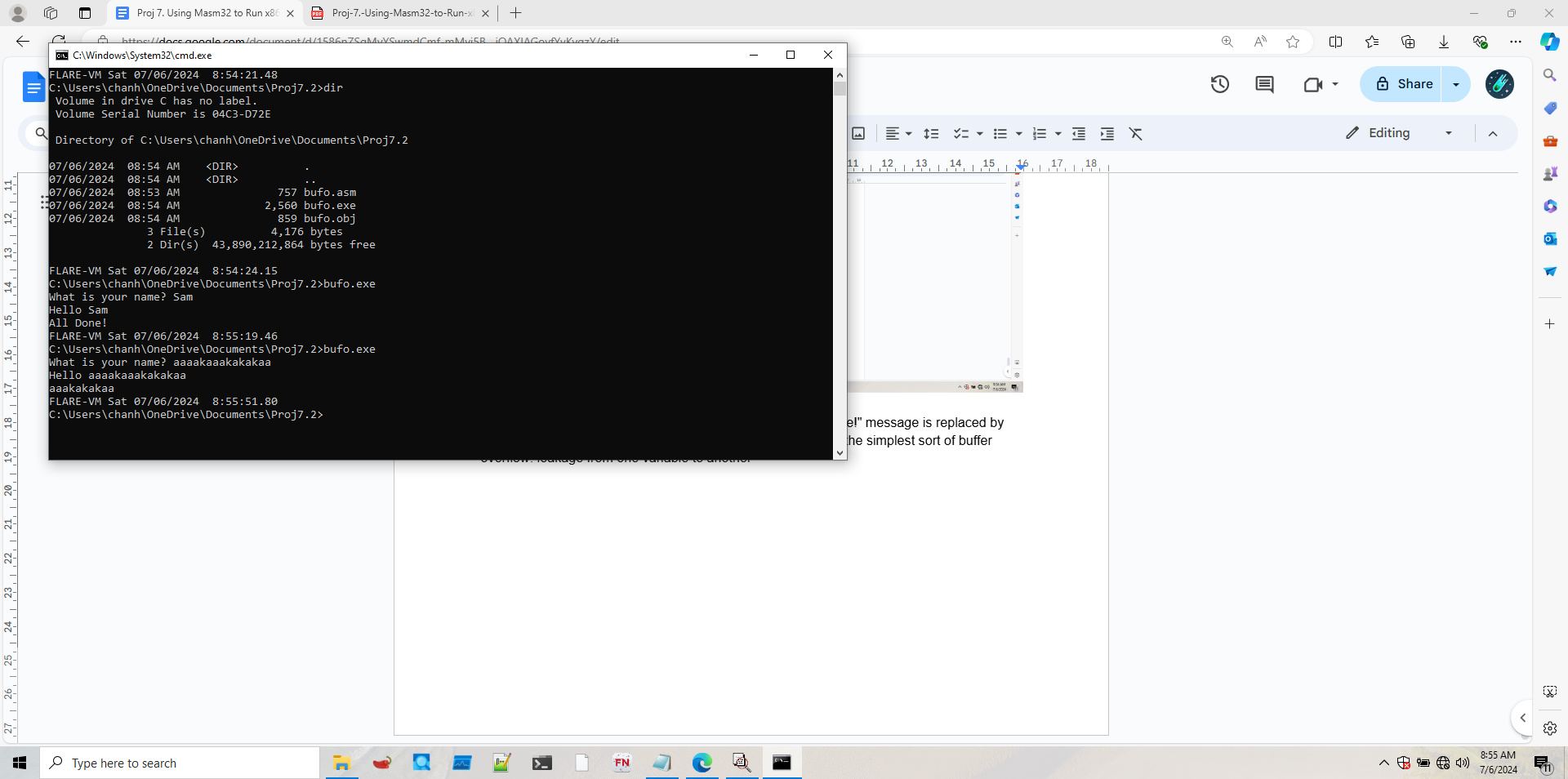




A message asks "What is your name?" Type SAM and press Enter. The program works correctly for such a short name, as shown below



Try longer names, such as WALLY and DILBERT. The "All Done!" message is replaced by characters from the end of the name, as shown above. This is the simplest sort of buffer overflow: leakage from one variable to another



Examining the File with PEview

Click Start. Type PEVIEW and open PEview. Open the bufo.exe file.

In the left pane of PEiD, expand the "SECTION .rdata" container and click "IMPORT Address Table", as shown below.

The right pane shows the functions imported from kernel32.dll

