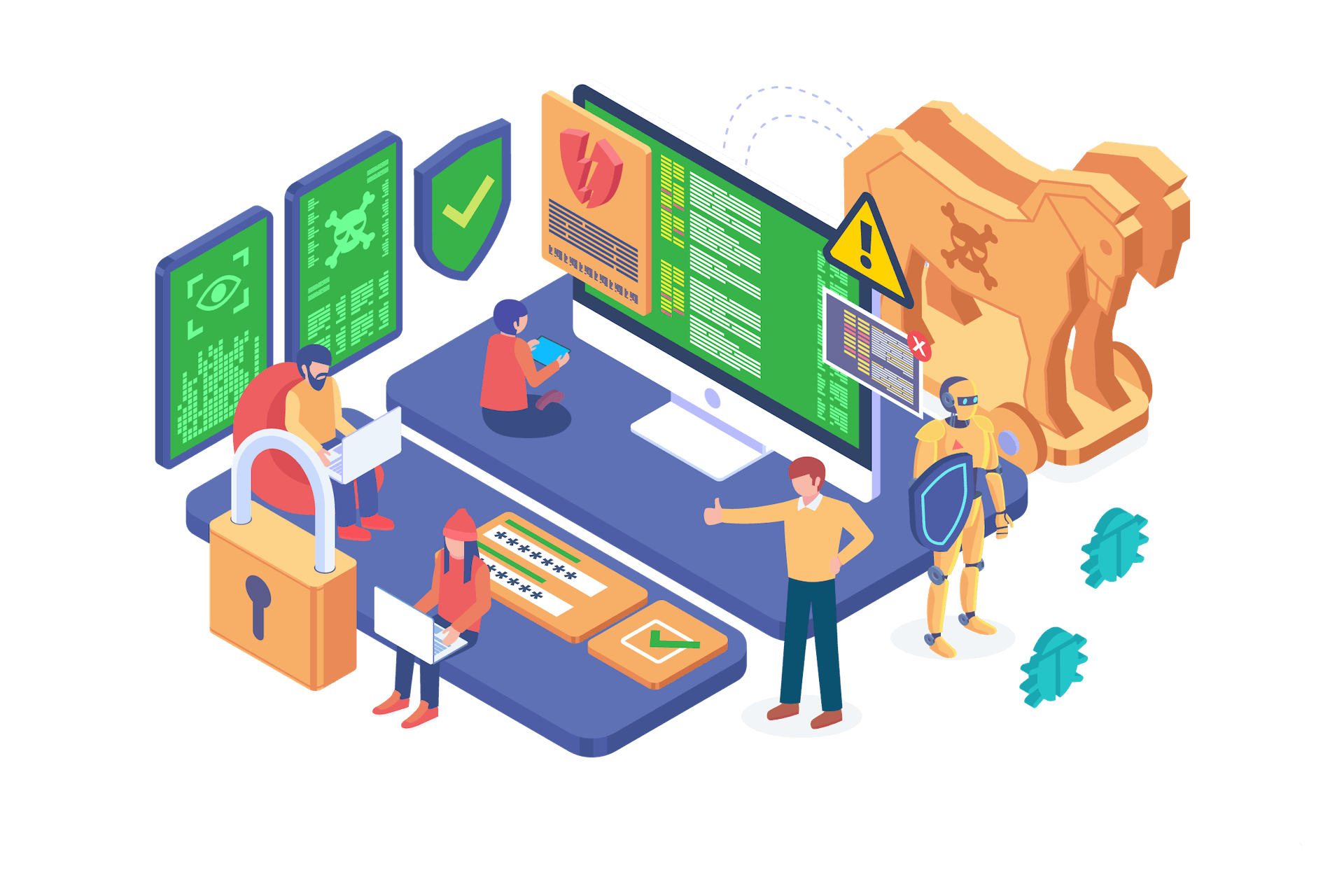
 National Forensic Sciences University

NICFS – DELHI CAMPUS



Malware Analysis And Forensics

Subject Code: CTMSDFIS SII P3

Submitted By

Shubhang Gupta

ER. No.: 022200300003026

M.Sc. Digital Forensics And Information Security

**LAB 2**

**AIM:**

To disassemble an exe file having a “hello world” program written in C

**SOFTWARE REQUIRED:**

Code::Blocks, IDA Freeware

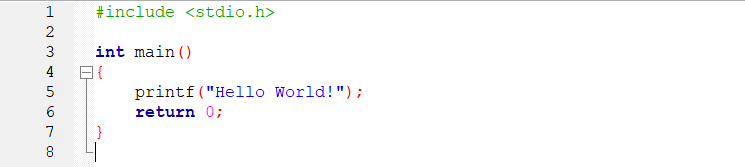
**INTRODUCTION:**

Assembly language is a low-level programming language for a computer or other programmable device.

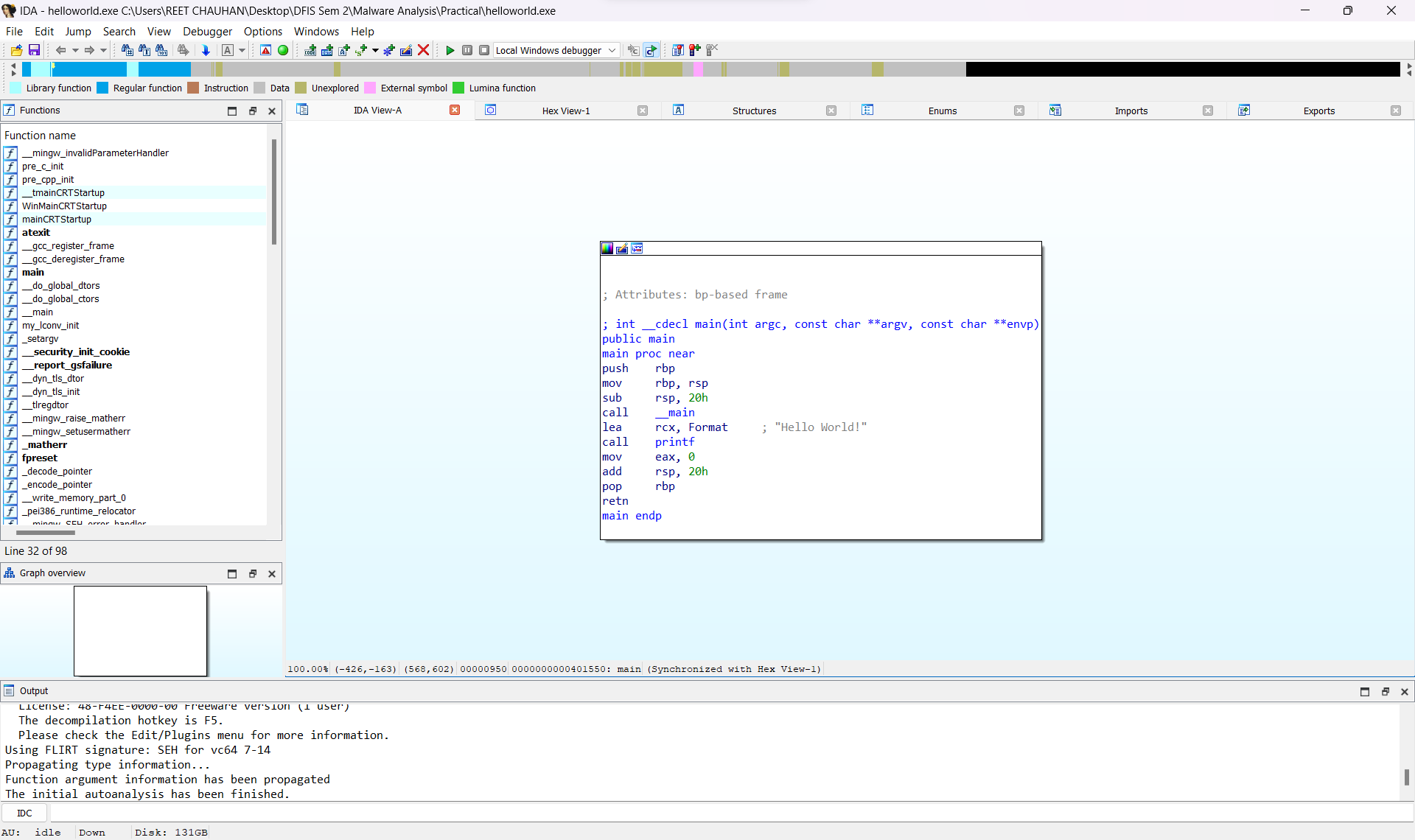
The Interactive Disassembler (IDA) is a disassembler for computer software which generates assembly language source code from machine-executable code. It supports a variety of executable formats for different processors and operating systems.

IDA is used widely in software reverse engineering, including for malware analysis and software vulnerability research.

**Program**

****

**Disassembled code**

****