Code construct: A code construct is a building block or a functional property of a program and are a group of instructions which perform a specific task within a program. This unit explains how to identify ten different code constructs within assembly, and you go from there.

Global variables vs Local Variables:

Global variables are loaded as arguments and local variables are loaded as stack variables (referred to by ebp).

As defined in chapter 4- arithmetic operations have definite instructions in assembly and chapter 4 defines how they are executed.

If Statements: If Statements use jump instructions to execute decisions. Take IDA pro’s help for nested if statements.

Loops can be recognized by jump statements- also IDA pro can help here.

Function calls:

Cdecl-

Caller is responsible for cleaning up the stack and parameters are loaded from right to left.

Stdcall-

The function being called is responsible for cleaning up the stack and it is the naming convention for windows API.

Fastcall-

First two arguments are stored in EDX and ECX and additional arguments are added from right to left and the calling function is responsible for cleaning up the stack.

Push vs move:

Both the above instructions can be used to move stuff onto the stack, Visual studio uses push and GCC uses move.