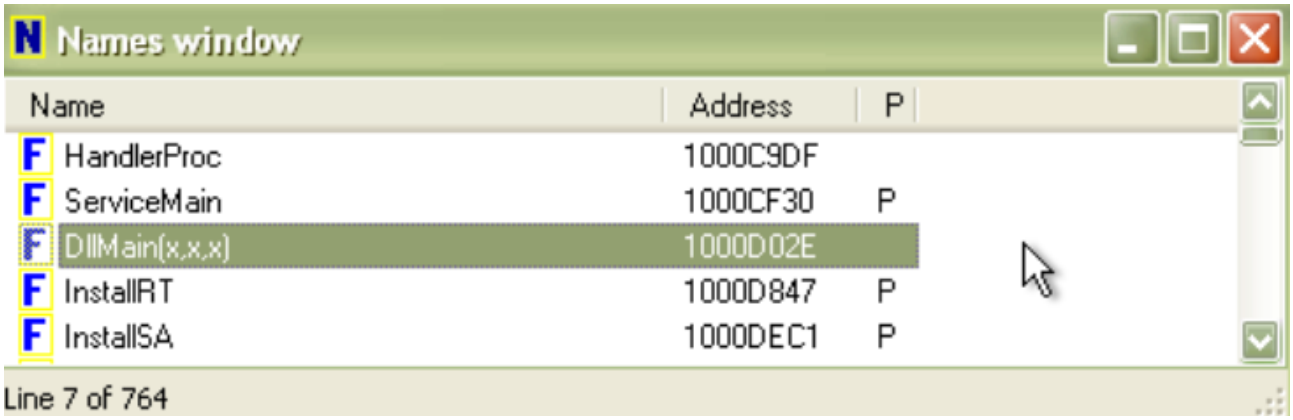
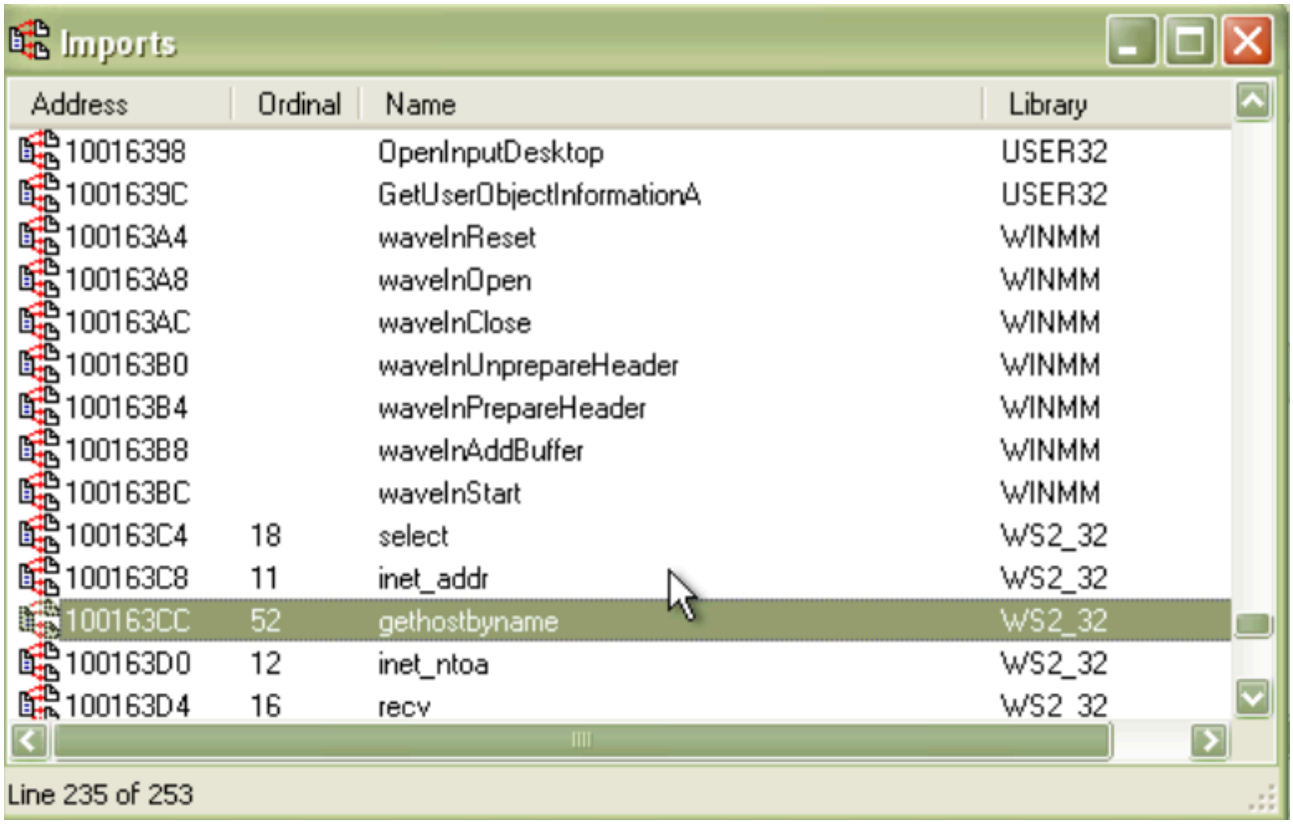
Analisi statica con IDA pro versione 5.0

L'esercizio di oggi ci richiede di fare un'analisi statica con il tool IDA.

Il primo punto che ci chiede l'esercizio è quello di individuare l'indirizzo della funzione DLLMain e come si può vedere dalla foto sotto l'indirizzo è 1000D02E



Il secondo punto dell'esercizio ci richiede di individuare la funzione gethostbyname che si trova nella scheda import e individuare l'indirizzo dell'import e in questo caso l'indirizzo è 100163CC come si può vedere dalla foto sotto



Parametro della funzione

```
.text:10001656 arg_0                   = dword ptr  4
```

Le variabili locali sono : var_674 - hmodule - wsadata

```
.text:10001656 var_675                 = byte ptr -675h
.text:10001656 var_674                 = dword ptr -674h
.text:10001656 hModule                 = dword ptr -670h
.text:10001656 timeout                 = timeval ptr -66Ch
.text:10001656 name                    = sockaddr ptr -664h
.text:10001656 var_654                 = word ptr -654h
.text:10001656 in                      = in_addr ptr -650h
.text:10001656 Parameter               = byte ptr -644h
.text:10001656 CommandLine             = byte ptr -63Fh
.text:10001656 Data                    = byte ptr -638h
.text:10001656 var_544                 = dword ptr -544h
.text:10001656 var_50C                 = dword ptr -50Ch
.text:10001656 var_500                 = dword ptr -500h
.text:10001656 var_4FC                 = dword ptr -4FCh
.text:10001656 readfds                 = fd_set ptr -4BCh
.text:10001656 phkResult               = HKEY__ ptr -3B8h
.text:10001656 var_3B0                 = dword ptr -3B0h
.text:10001656 var_1A4                 = dword ptr -1A4h
.text:10001656 var_194                 = dword ptr -194h
.text:10001656 WSAData                 = WSAData ptr -190h
.text:10001656 arg_0                   = dword ptr  4
```