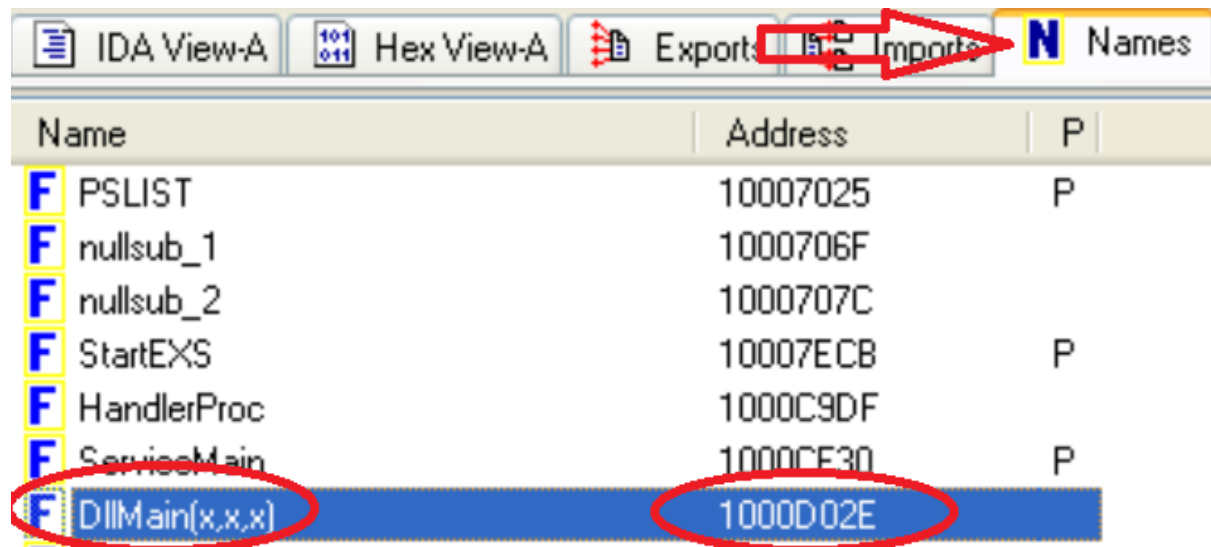


## IDA

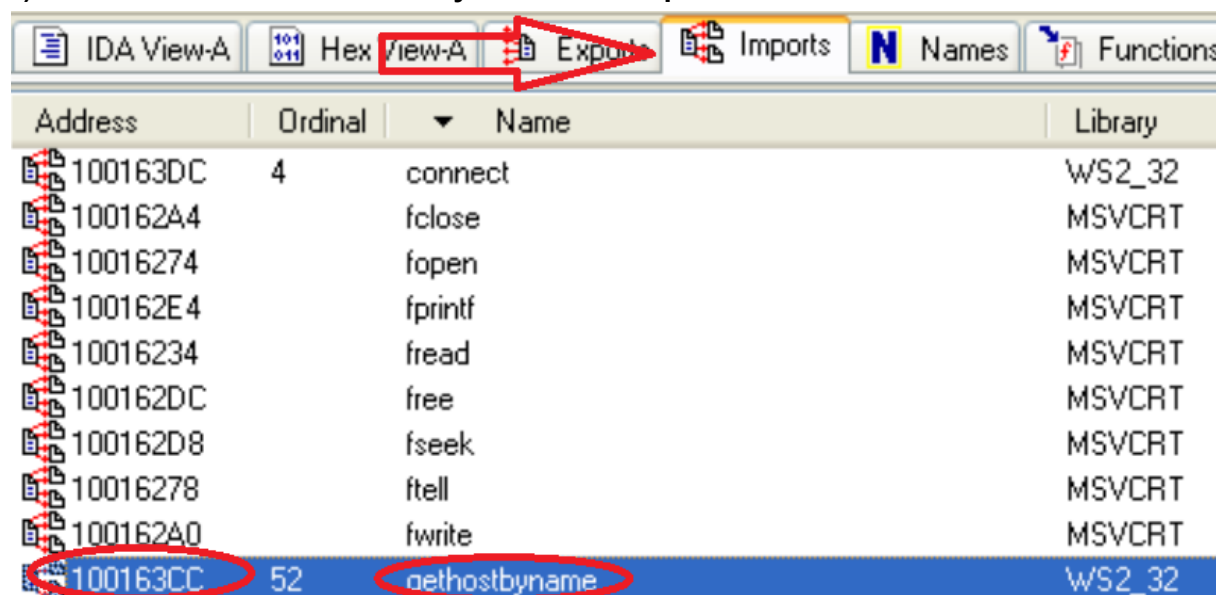
Dopo aver aperto il file del malware da analizzare andiamo a risolvere i task.

### 1) Trovare l'indirizzo di DLLMain.



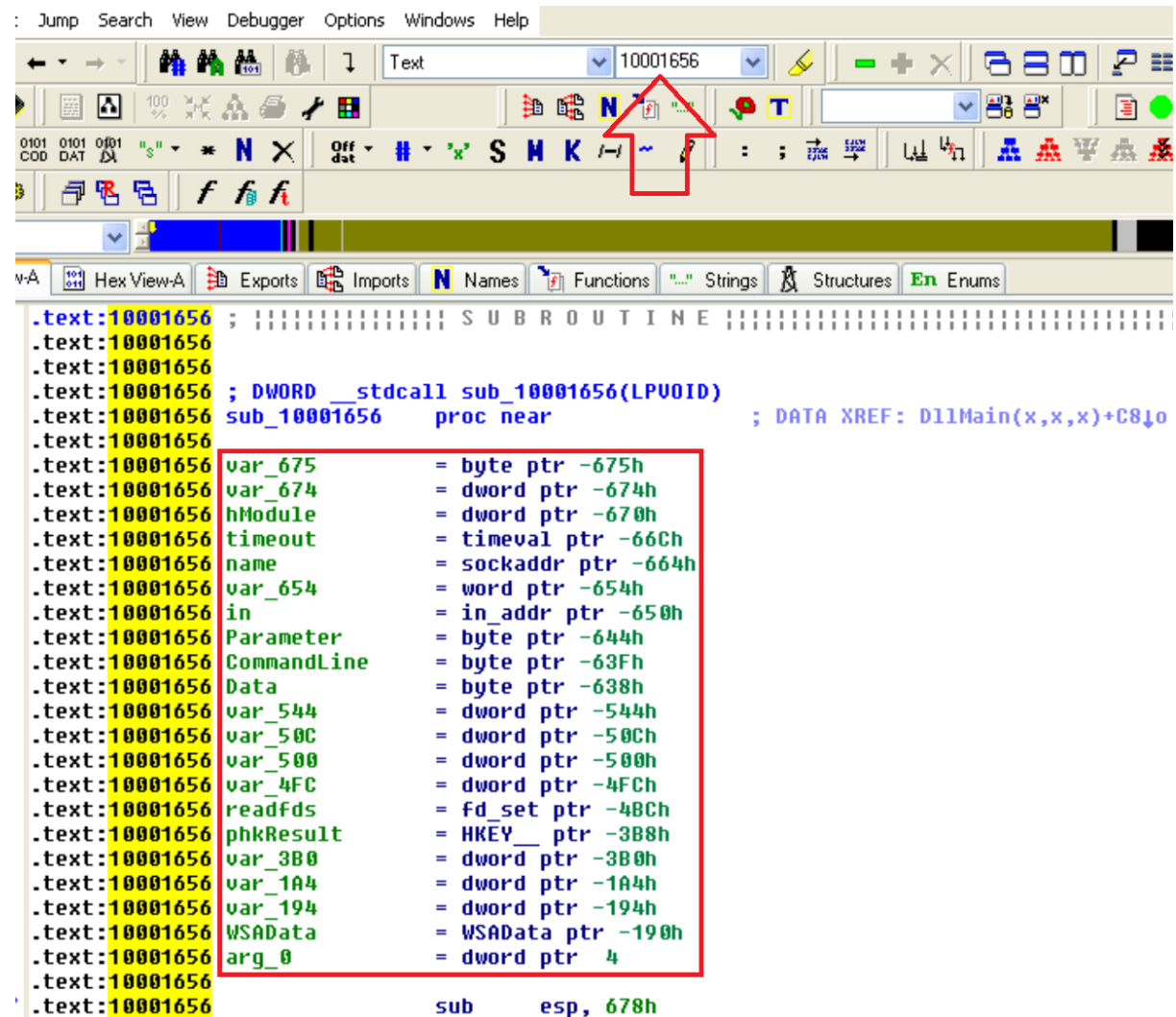
Per trovare l'indirizzo di una qualsiasi funzione, parametro o variabile, spostiamoci all'interno della tab NAMES

### 2) Trovare l'indirizzo di Gethostbyname nella imports tab



Nella tab imports possiamo trovare tutte le librerie di funzioni che il nostro programma malevolo utilizza per eseguirsi. E' sufficiente trovare il nome della funzione per avere subito il suo indirizzo e la libreria dalla quale proviene.

### 3&4) Trovare i parametri e le variabili della funzione all'indirizzo 0x10001656



The screenshot shows the IDA Pro interface with the 'Text' view selected. The address field in the top toolbar is set to 10001656. The main window displays the disassembly of the function at this address. A red box highlights the list of local variables and parameters, which are automatically named by IDA. The list includes:

- var\_675 = byte ptr -675h
- var\_674 = dword ptr -674h
- hModule = dword ptr -670h
- timeout = timeval ptr -66Ch
- name = sockaddr ptr -664h
- var\_654 = word ptr -654h
- in = in\_addr ptr -650h
- Parameter = byte ptr -644h
- CommandLine = byte ptr -63Fh
- Data = byte ptr -638h
- var\_544 = dword ptr -544h
- var\_50C = dword ptr -50Ch
- var\_500 = dword ptr -500h
- var\_4FC = dword ptr -4FCh
- readfds = fd\_set ptr -4BCh
- phkResult = HKEY\_\_ ptr -3B8h
- var\_3B0 = dword ptr -3B0h
- var\_1A4 = dword ptr -1A4h
- var\_194 = dword ptr -194h
- WSAData = WSAData ptr -190h
- arg\_0 = dword ptr 4

The function signature is: `sub_10001656 proc near ; DWORD __stdcall sub_10001656(LPVOID)`. The function body starts with `sub esp, 678h`.

Come possiamo vedere dalla vista stile testo all'indirizzo seguente (10001656) che possiamo raggiungere semplicemente digitandolo sopra, ci evidenzia tutte le variabili e i parametri della funzione DWORD. IDA nomina le variabili in maniera automatica con lo stile var\_XXX.