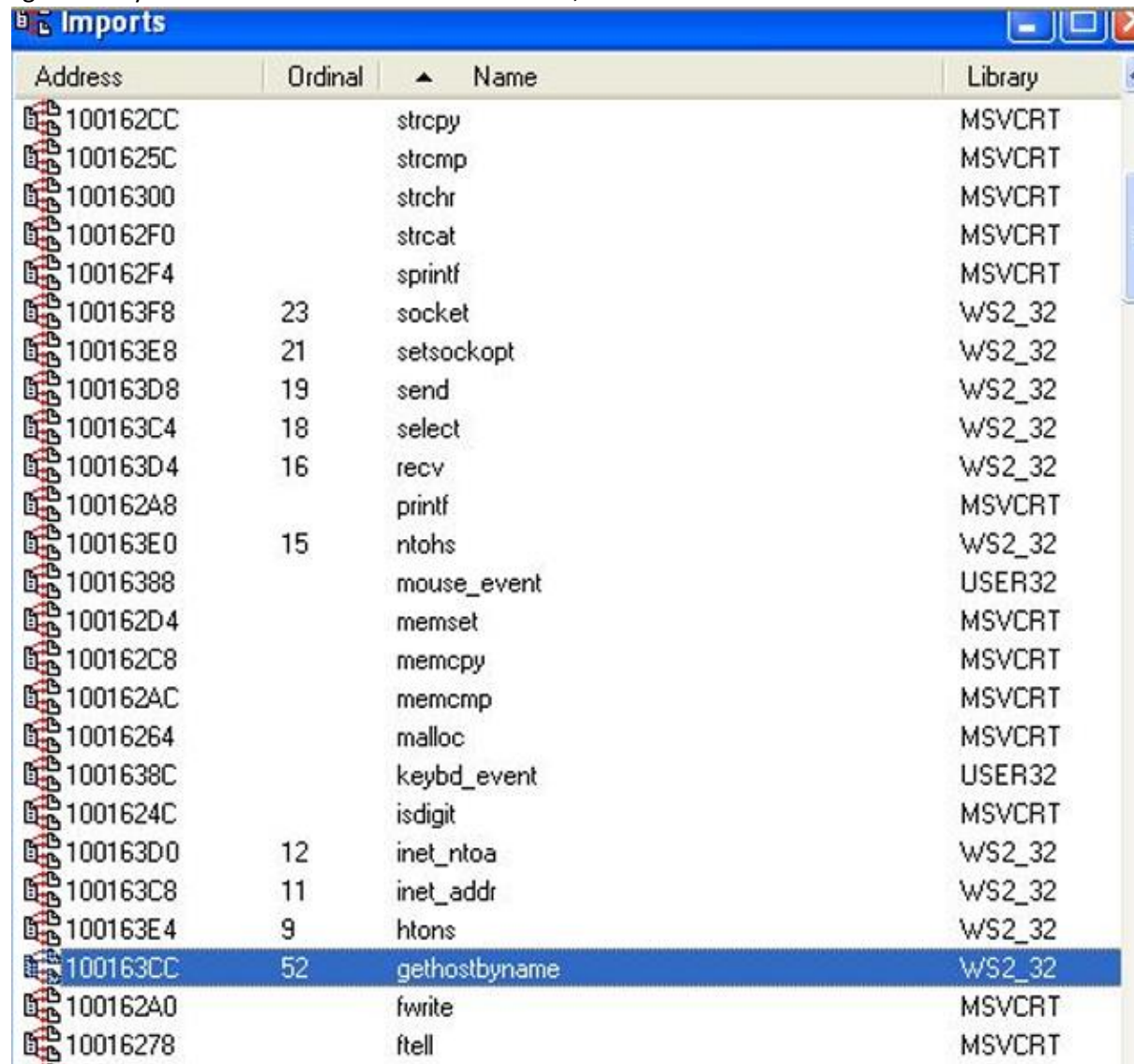


1) Per individuare la posizione della funzione DllMain, procediamo caricando il file eseguibile tramite IDA Pro. Successivamente, selezioniamo la modalità testuale e recuperiamo l'indirizzo della funzione principale, il quale è 1000D02E.

2) Accediamo alla finestra degli "imports" tramite IDA Pro e individuiamo la funzione desiderata. "gethostbyname" è situato all'indirizzo 100163CC, come evidenziato nell'illustrazione.



Address	Ordinal	Name	Library
100162CC		strcpy	MSVCRT
1001625C		strcmp	MSVCRT
10016300		strchr	MSVCRT
100162F0		strcat	MSVCRT
100162F4		sprintf	MSVCRT
100163F8	23	socket	WS2_32
100163E8	21	setsockopt	WS2_32
100163D8	19	send	WS2_32
100163C4	18	select	WS2_32
100163D4	16	recv	WS2_32
100162A8		printf	MSVCRT
100163E0	15	ntohs	WS2_32
10016388		mouse_event	USER32
100162D4		memset	MSVCRT
100162C8		memcpy	MSVCRT
100162AC		memcmp	MSVCRT
10016264		malloc	MSVCRT
1001638C		keybd_event	USER32
1001624C		isdigit	MSVCRT
100163D0	12	inet_ntoa	WS2_32
100163C8	11	inet_addr	WS2_32
100163E4	9	htons	WS2_32
100163CC	52	gethostbyname	WS2_32
100162A0		fwrite	MSVCRT
10016278		ftell	MSVCRT

3) Inizialmente, è necessario navigare all'indirizzo desiderato utilizzando la funzione di ricerca o la barra laterale. A tale indirizzo, troviamo 20 variabili con offset negativo rispetto a EBP.

4) Dall'illustrazione correlata, è evidente che solo un argomento viene passato alla funzione, con un offset positivo rispetto a EBP. IDA ha identificato questo parametro come "arg_0".

```
.text:10001656 ; !!!!!!!!!!!!!!! S U B R O U T I N E !!!!!!!!!!!!!!!
.text:10001656
.text:10001656
.text:10001656 ; DWORD __stdcall sub_10001656(LPVOID)
.text:10001656 sub_10001656      proc near                                ; DATA XREF
.text:10001656
.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
```