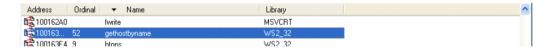
## **FUNZIONE DLLMAIN**

Apriamo il file con Ida e tramite la barra di ricerca cerchiamo la funzione DLLMAIN

```
; BOOL __stdcall DllMain(HINSTANCE hinstDLL,DWORD fdwReason,LPU0ID lpvReserved)
_DllMain@12 proc near
hinstDLL= dword ptr 4
fdwReason= dword ptr 8
lpvReserved= dword ptr 0Ch
```

## **FUNZIONE GETHOSTBYNAME**

La funzione gethostbyname recupera informazioni host corrispondenti a un nome host da un database host



## VARIABILI LOCALI DELLA FUNZIONE ALLA LOCAZIONE DI MEMORIA 0X10001656

```
.text:10001656
.text:10001656 ; DWORD
                           stdcall sub 10001656(LPV0ID)
.text:10001656 sub_10001656
                                                             ; DATA XREF: DllMain(x,x,x)+C810
                                  proc near
.text:10001656
= byte ptr -675h
                                  = dword ptr -674h
= dword ptr -670h
.text:10001656 var_674
.text:10001656 hModule
.text:10001656 timeout
                                  = timeval ptr -66Ch
                                  = sockaddr ptr -664h
= word ptr -654h
.text:10001656 name
.text:10001656 var_654
.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
.text:10001656 var_500
                                    dword ptr -544h
                                  = dword ptr -50Ch
.text:10001656 var_500
.text:10001656 var_4FC
                                    dword ptr -500h
                                    dword ptr -4FCh
.text:10001656 readfds
                                    fd_set ptr -4BCh
                                  = HKEY ptr -388h
= dword ptr -50Ch
.text:10001656 phkResult
.text:10001656 var_50C
.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 -380h
.text:10001656 var_1A4
                                  = dword ptr -1A4h
.text:10001656 var 194
                                  = dword ptr -194h
.text:10001656 WSAData
                                  = WSAData ptr -190h
```