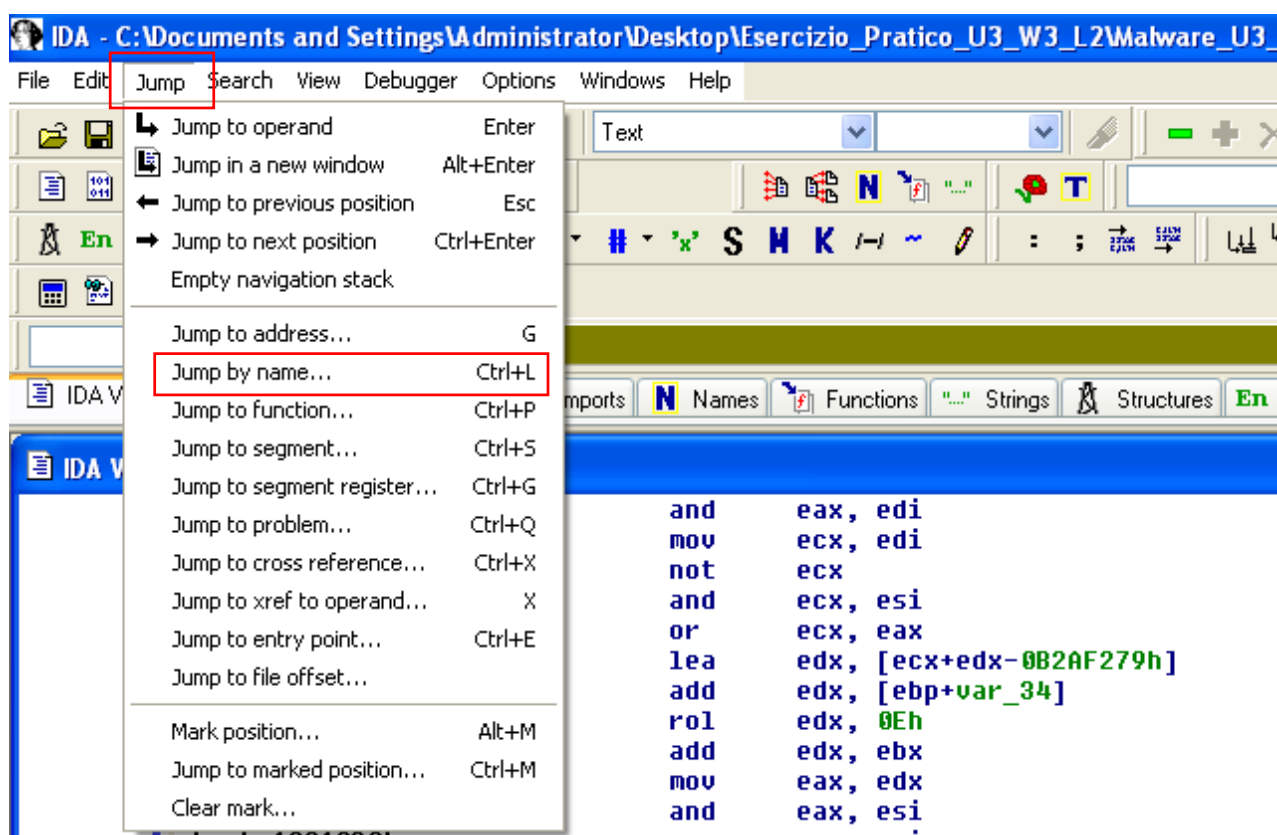


# ANALISI STATICA AVANZATA IDA

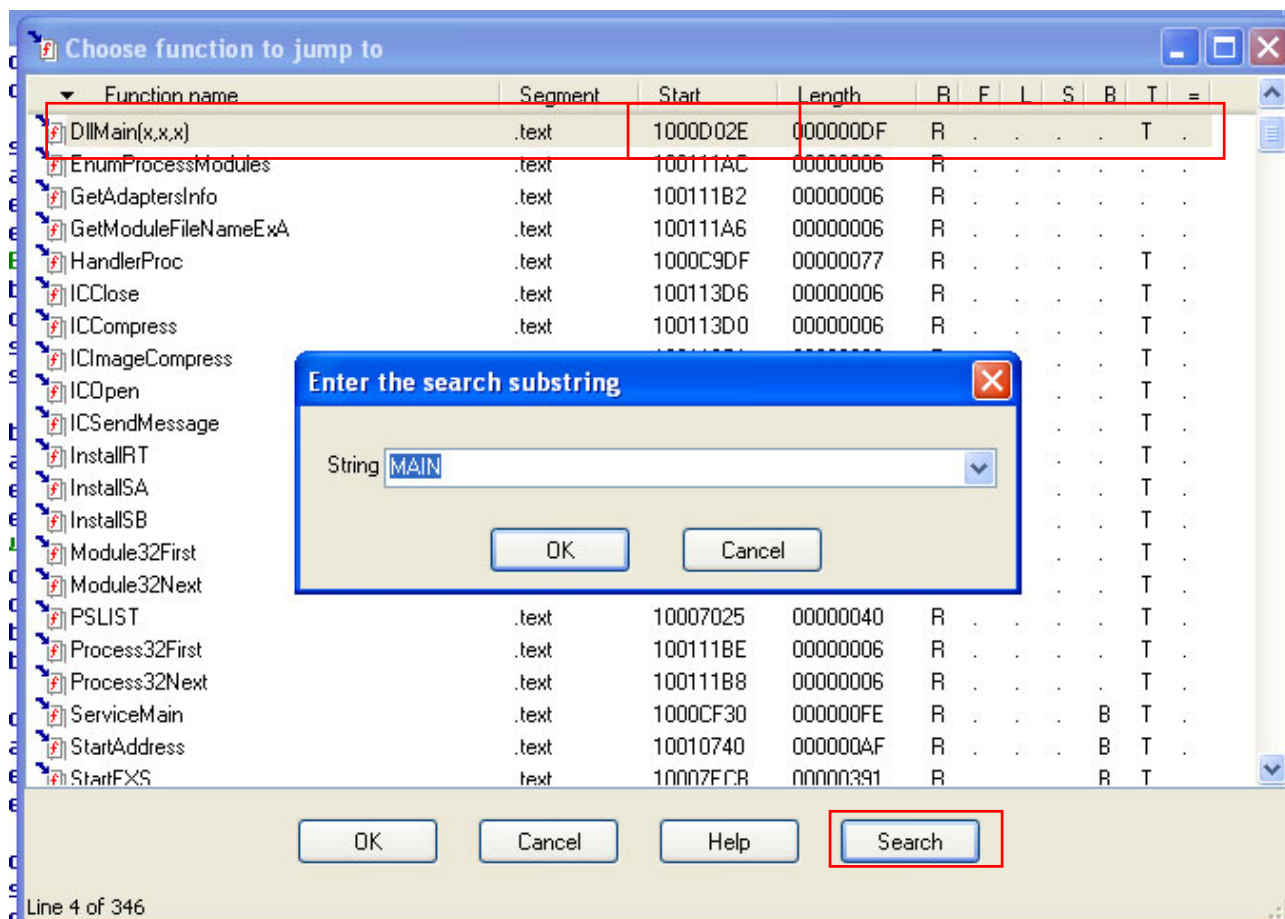
Con riferimento al file **MALWARE\_U3\_W3\_L2**

- Individuare l'indirizzo alla funzione **DLLMain**
- Dalla scheda "imports" individuare la funzione **gethosbyname**. Qual è l'indirizzo dell'import?
- Quante sono le variabili locali della funzione alla locazione di memoria **0x10001656**?
- Quanti sono invece, i parametri della funzione sopra?
- Considerazioni comportameto del Malware

## Individuare l'indirizzo alla funzione **DLLMain**



Una volta caricato il file andiamo sulla barra degli strumenti. Apriamo lo strumento **Jump** e poi **Jump by name (Ctrl+L)**. Si aprirà una nuova finestra con una lista delle funzioni presenti all'interno del nostro file. In basso a destra clicchiamo **search** e digitiamo il nome della funzione che ci interessa. In questo caso **DLLMAIN**



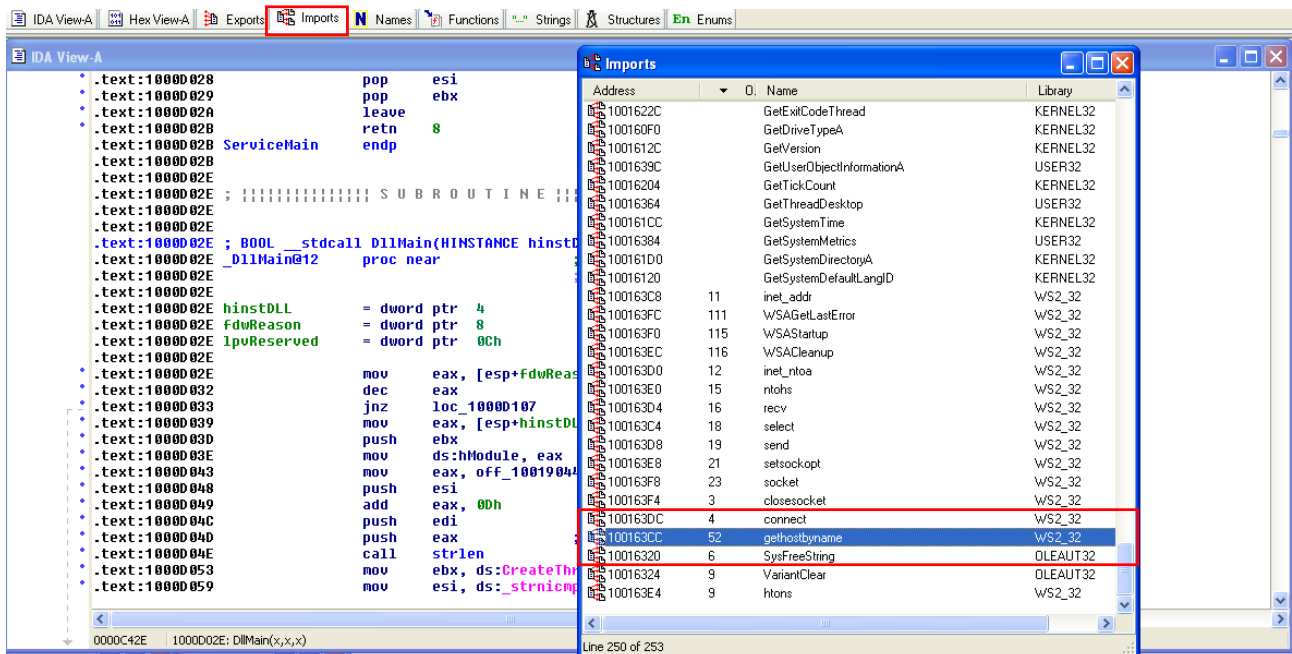
Una volta cercata e trovata la nostra funzione possiamo anche risalire all'indirizzo.

Cliccando due volte sulla funzione DLLMAIN si aprirà un'ulteriore pagina con all'interno evidenziata la nostra funzione e il suo indirizzo

```
.text:1000D02E
.text:1000D02E ; BOOL __stdcall DllMain(HINSTANCE hinstDLL,DWORD fdwReason,LPVOID lpvReserved)
.text:1000D02E _DllMain@12 proc near ; CODE XREF: DllEntryPoint+4B1p
.text:1000D02E ; DATA XREF: sub_100110FF+2D10
.text:1000D02E
```

Dalla scheda “imports” individuare la funzione gethostname. Qual è l’indirizzo dell’import?

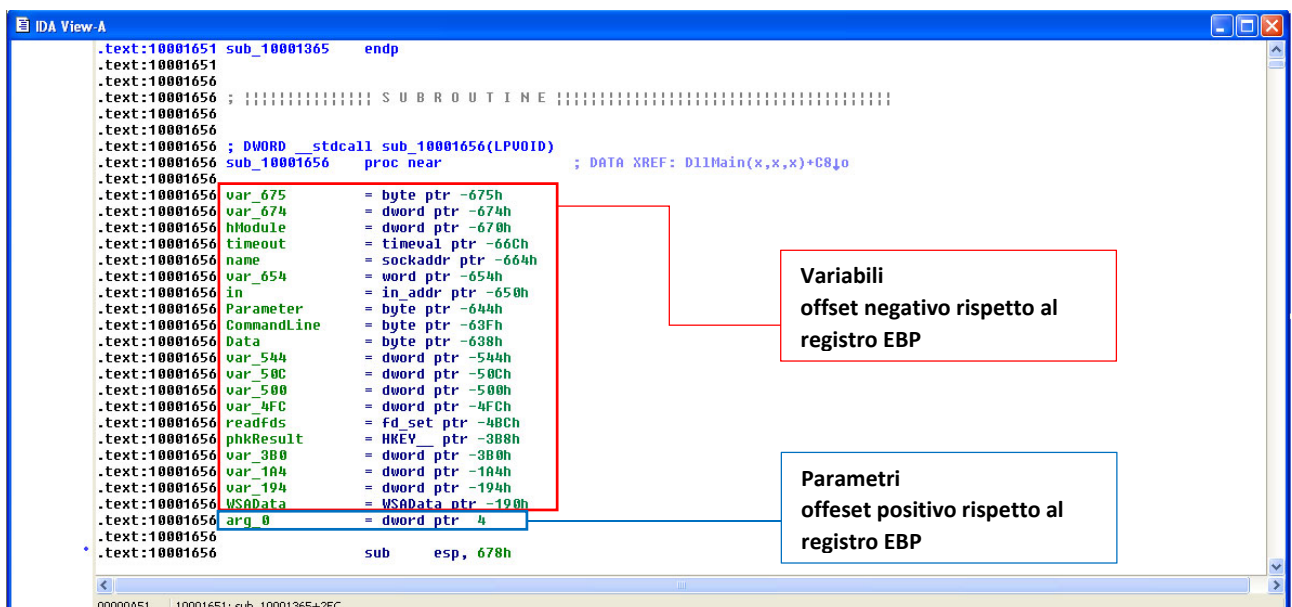
Apriamo la scheda imports che abbiamo sopra la nostra pagina principale.



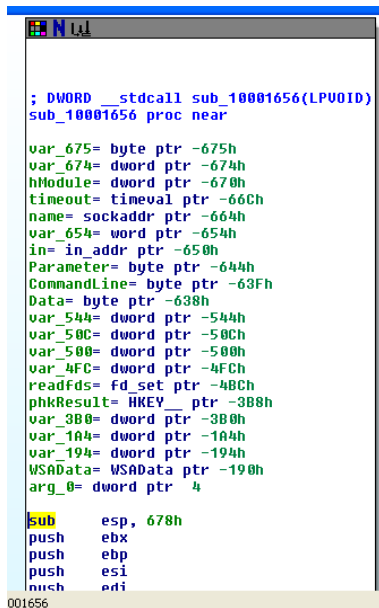
Qui ci comparirà un elenco delle **funzioni importate** dal file. Cerchiamo quella che ci interessa e con doppio click possiamo espandere il suo contenuto

Quante sono le variabili locali della funzione alla locazione di memoria 0x10001656?

Quanti sono invece, i parametri della funzione sopra?



Variabili locali indirizzo 10001656



```
; DWORD __stdcall sub_10001656(LPVOID)
sub_10001656 proc near

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 -48Ch
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

sub     esp, 678h
push    ebx
push    ebp
push    esi
push    edi
```

Qui possiamo notare nella versione “grafica” l’elenco delle variabili e dei parametri che saranno usati all’interno della **sub\_10001656**