Analisi statica avanzata con IDA

Malware_U3_W3_L2

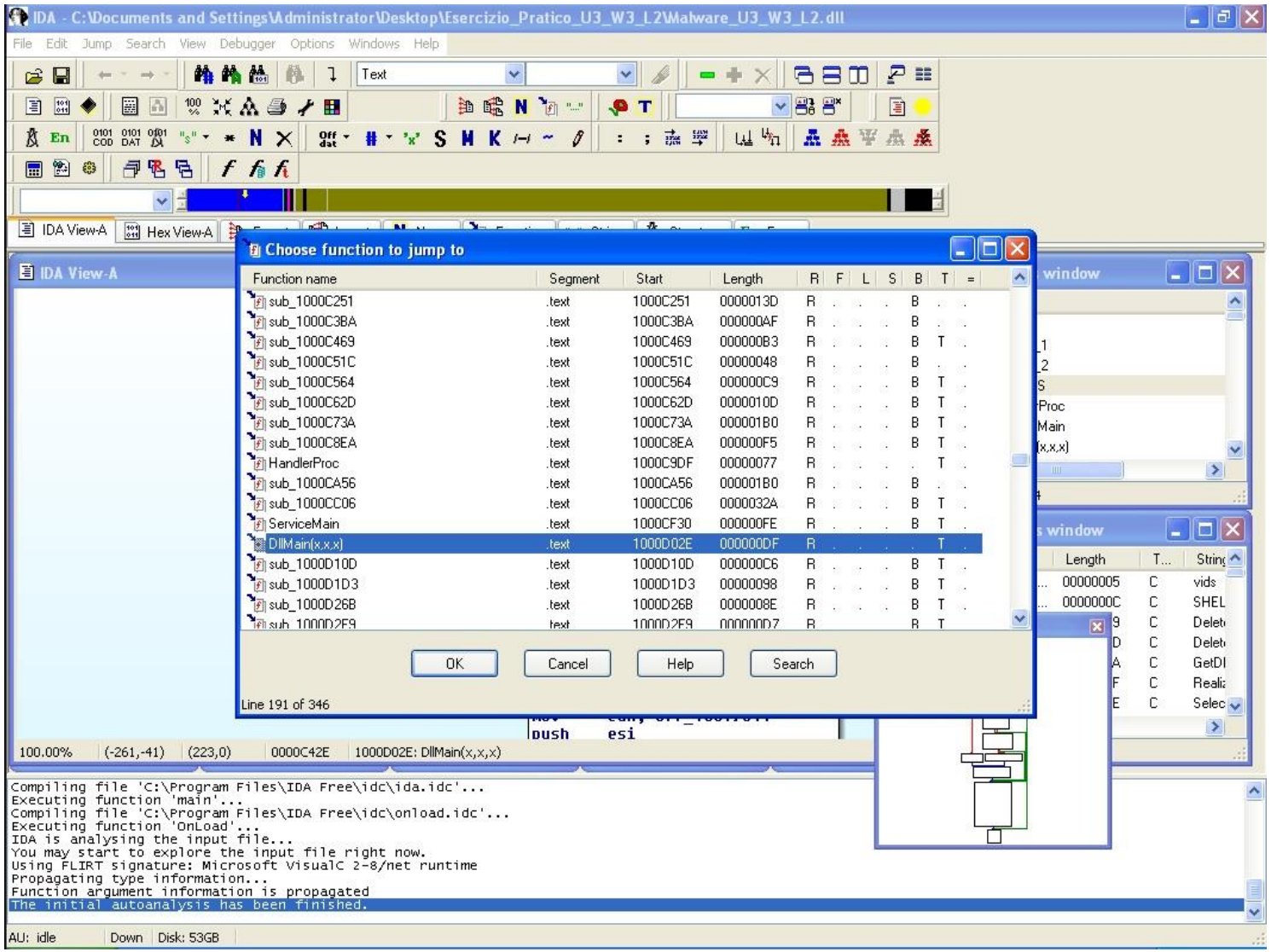
Individuazione indirizzo della funzione DLLMain

Dalla schermata *imports* individuazione della funzione *gethostbyname*
Qual è l'indirizzo dell'import?

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

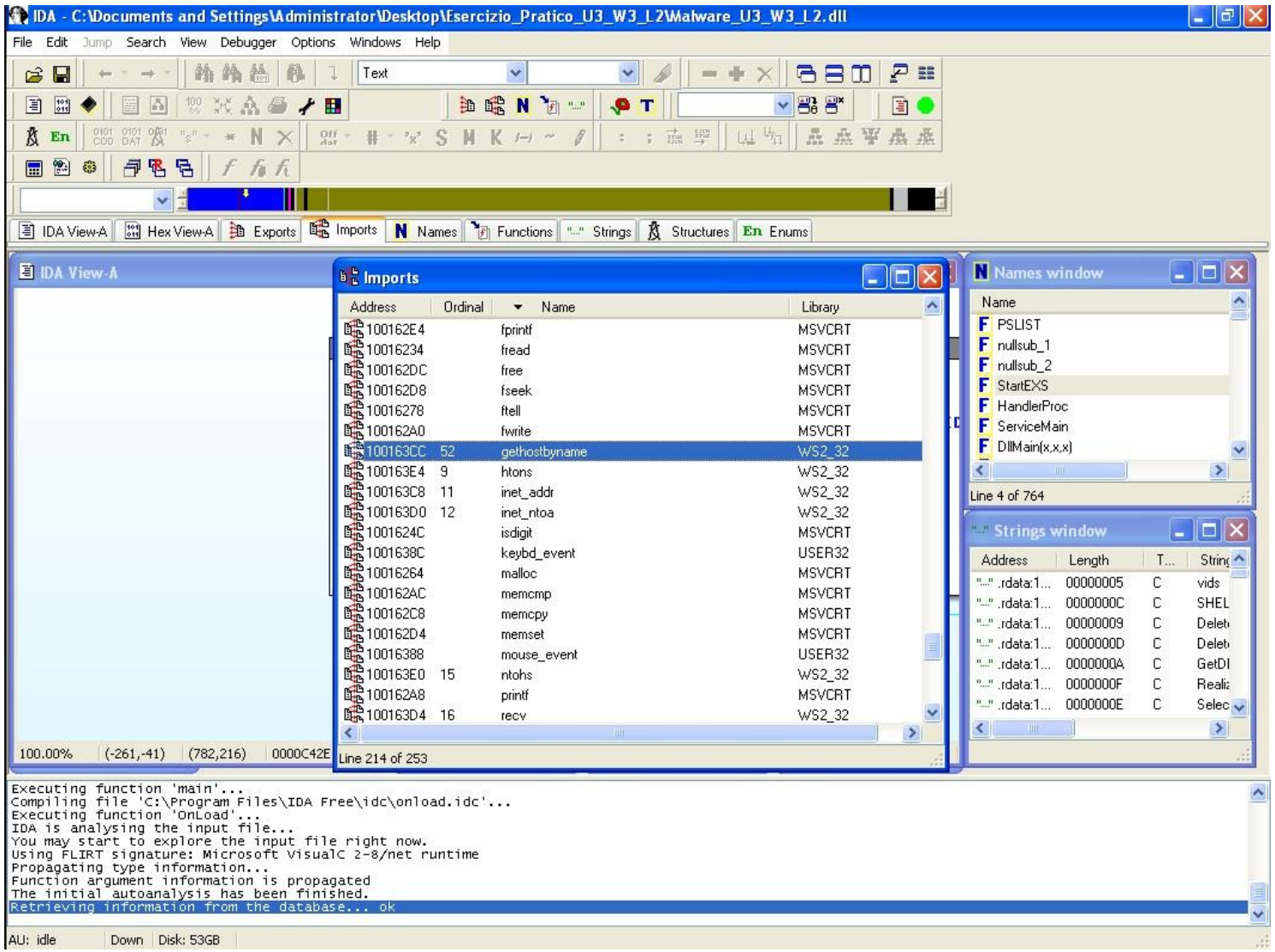
Quanti sono i parametri della funzione sopra?

Orlando Tangari



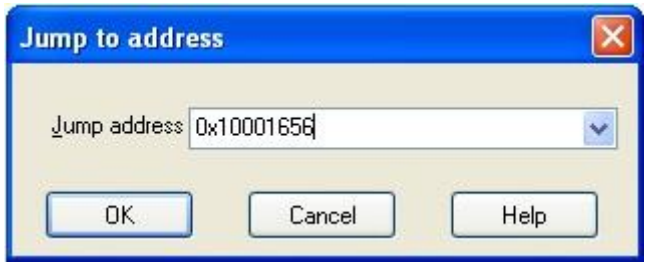
Individuazione indirizzo della funzione *DLLMain*

Dal tool IDA Pro, nel menu a tendina Jump, si seleziona Jump to function e si cerca la funzione DLLMain per individuare il suo indirizzo, cioè: 100D02E.



Individuazione indirizzo della funzione *gethostbyname*

Nella scheda imports, si individua la funzione gethostbyname per individuare il suo indirizzo, cioè: 100163CC.




```
; 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 -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
```

Parametri e variabili locali della funzione alla locazione di memoria 0x10001656

Nel menu a tendina Jump, si seleziona Jump tu address e si individuano le variabili della funzione alla locazione di memoria 0x10001656, cioè: 20.

L'unico parametro individuato si trova all'ultima riga: *arg_0= dword ptr 4* .