

## Esercizio S11-L1

Individuare l'indirizzo della funzione DLLMain (così com'è, in esadecimale) 2. Dalla scheda «imports» individuare la funzione «gethostbyname». Qual è l'indirizzo dell'import? Cosa fa la funzione? 3. Quante sono le variabili locali della funzione alla locazione di memoria 0x10001656? 4. Quanti sono, invece, i parametri della funzione sopra?

1

1000D02E

sub_1000D1D3	.text	1000D1D3	00000098	R	.	.	.	B	T	.
sub_1000D10D	.text	1000D10D	000000C6	R	.	.	.	B	T	.
DLLMain(x,x,x)	.text	1000D02E	000000DF	R	.	.	.	.	T	.
ServiceMain	.text	1000CF30	000000FE	R	.	.	.	B	T	.
sub_1000C006	.text	1000C006	0000032A	R	.	.	.	R	T	.

2 Indirizzo 100163CC

Imports				
Address	Ordinal	Name	Library	
100162...		fseek	MSVCRT	
10016278		ftell	MSVCRT	
100162A0		fwrite	MSVCRT	
100163...	52	gethostbyname	WS2_32	
100163E4	9	htons	WS2_32	
100163C8	11	inet_addr	WS2_32	
100163...	12	inet_ntoa	WS2_32	
1001624C		isdigit	MSVCRT	
1001638C		keybd_event	USER32	

3 e 4

Le variabili sono 20 e 1 parametro.

## IDA View-A



```
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

sub     esp, 678h
```

30.00% (783,133) (23,159) 00000A56 10001656: sub\_10001656