


Analisi Statica con IDA Pro

Individuare l'indirizzo della funzione DLLMain:

```
.text:1000D02E
.text:1000D02E ; ===== S U B R O U T I N E =====
.text:1000D02E
.text:1000D02E |
.text:1000D02E ; BOOL __stdcall DLLMain(HINSTANCE hinstDLL, DWORD fdwReason, LPVOID lpvReserved)
.text:1000D02E _DllMain@12 proc near ; CODE XREF: DllEntryPoint+48↓p
.text:1000D02E ; DATA XREF: sub_100110FF+2D↓o
.text:1000D02E
.text:1000D02E hinstDLL = dword ptr 4
.text:1000D02E fdwReason = dword ptr 8
.text:1000D02E lpvReserved = dword ptr 0Ch
.text:1000D02E
.text:1000D02E mov eax, [esp+fdwReason]
1000D02E
```

Dalla scheda «imports» individuare la funzione «gethostbyname». Qual è l'indirizzo dell'import? Cosa fa la funzione?

 100163CC 52 gethostbyname WS2_32
100163CC

La funzione “gethostbyname” è una funzione utilizzata in molti linguaggi di programmazione per ottenere informazioni su un host specifico tramite il suo nome di dominio. In pratica, questa funzione prende in input il nome di dominio di un host e restituisce una struttura di dati contenente informazioni sull'host, come il suo indirizzo IP.

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

```
.text:10001656
.text:10001656 ; ===== S U B R O U T I N E =====
.text:10001656
.text:10001656 ; DWORD __stdcall sub_10001656(LPVOID)
.text:10001656 sub_10001656 proc near ; DATA XREF: DllMain(x,x,x)+C8↓o
.text:10001656
.text:10001656 var_675 = byte ptr -675h
.text:10001656 var_674 = dword ptr -674h
.text:10001656 hLibModule = dword ptr -670h
.text:10001656 timeout = timeval ptr -66Ch
.text:10001656 name = sockaddr ptr -664h
.text:10001656 var_654 = word ptr -654h
.text:10001656 Dst = dword ptr -650h
.text:10001656 Parameter = byte ptr -644h
.text:10001656 var_640 = byte ptr -640h
.text:10001656 CommandLine = byte ptr -63Fh
.text:10001656 Source = byte ptr -63Dh
.text:10001656 Data = byte ptr -638h
.text:10001656 var_637 = byte ptr -637h
.text:10001656 var_544 = dword ptr -544h
```

```

.text:10001656 var_50C      = dword ptr -50Ch
.text:10001656 var_500      = dword ptr -500h
.text:10001656 Buf2        = byte ptr -4FCh
.text:10001656 readfds     = fd_set ptr -48Ch
.text:10001656 phkResult   = byte ptr -388h
.text:10001656 var_380     = dword ptr -380h
.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
.text:10001656
.text:10001656             sub     esp, 678h

```

20 variabili con offset negativo rispetto ad EBP

Quanti sono, invece, i parametri della funzione sopra?

```

.text:10001656 arg_0      = dword ptr 4

```

Si può osservare un unico parametro trasmesso alla funzione, con offset positivo rispetto ad EBP, ovvero “arg_0”.