S11-L2

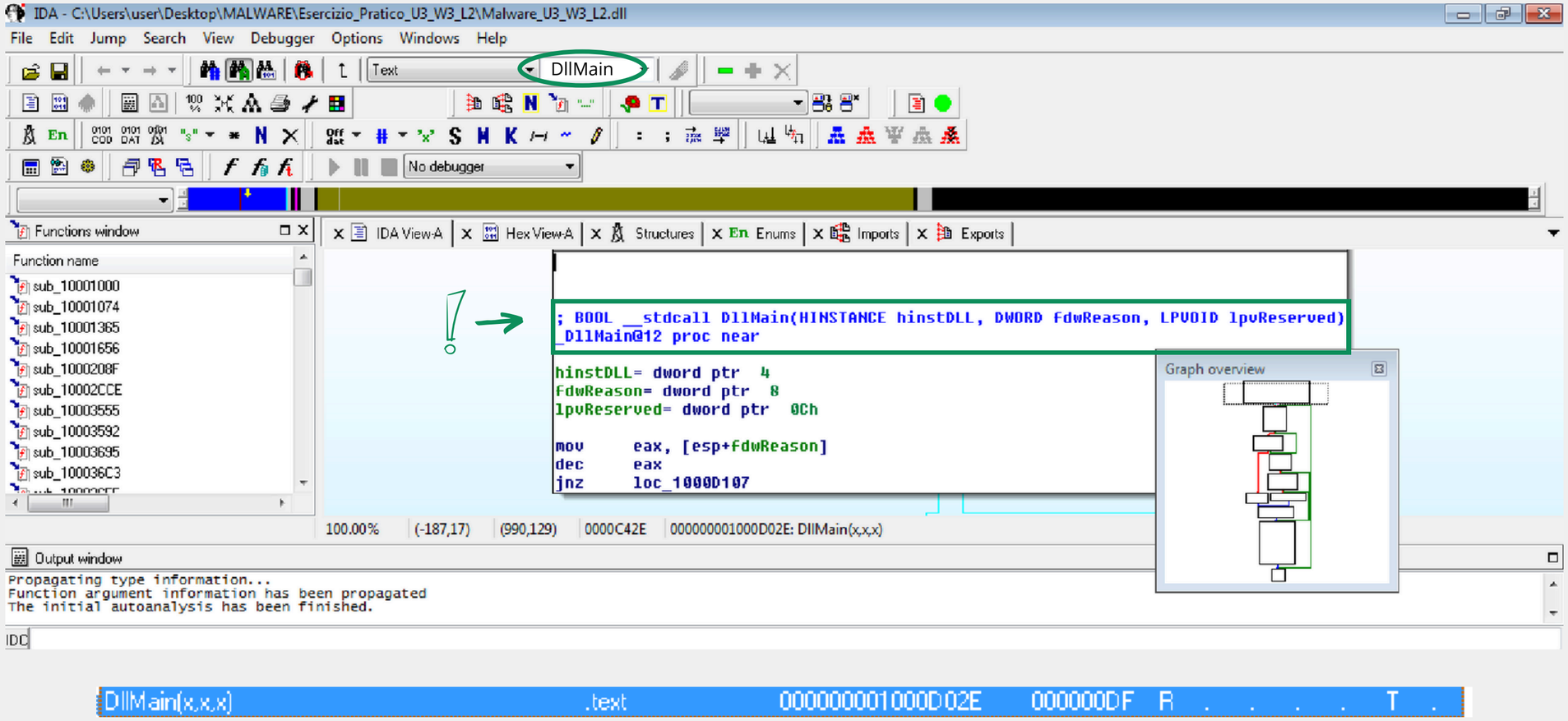
ANALISI STATICA AVANZATA

TRACCIA

TRACCIA: ESERCIZIO ANALISI STATICA LO SCOPO DELL'ESERCIZIO DI OGGI È DI ACQUISIRE ESPERIENZA CON IDA, UN TOOL FONDAMENTALE PER L'ANALISI STATICA . A TAL PROPOSITO, CON RIFERIMENTO AL MALWARE CHIAMATO «MALWARE_U3_W3_L2 » PRESENTE ALL'INTERNO DELLA CARTELLA «ESERCIZIO_PRATICO_U3_W3_L2 » SUL DESKTOP DELLA MACCHINA VIRTUALE DEDICATA ALL'ANALISI DEI MALWARE, RISPONDERE AI SEGUENTI QUESITI, UTILIZZANDO IDA PRO.

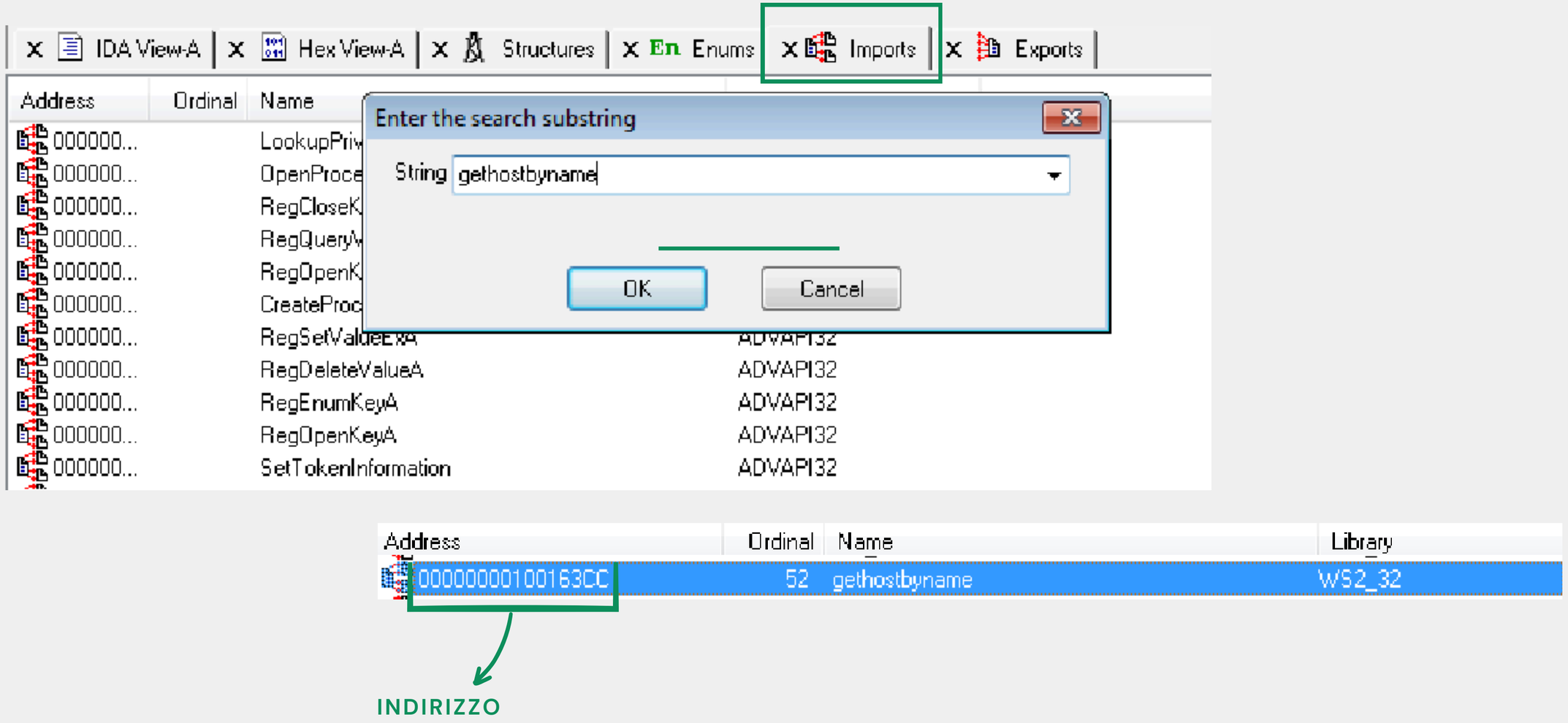
1. INDIVIDUARE L'INDIRIZZO DELLA FUNZIONE DLLMAIN (COSÌ COM'È, IN ESADECIMALE)
2. DALLA SCHEDA «IMPORTS» INDIVIDUARE LA FUNZIONE «GETHOSTBYNAME ». QUAL È L'INDIRIZZO DELL'IMPORT? COSA FA LA FUNZIONE?
3. QUANTE SONO LE VARIABILI LOCALI DELLA FUNZIONE ALLA LOCAZIONE DI MEMORIA 0X10001656?
4. QUANTI SONO, INVECE, I PARAMETRI DELLA FUNZIONE SOPRA?
5. INSERIRE ALTRE CONSIDERAZIONI MACRO LIVELLO SUL MALWARE (COMPORTAMENTO)

01 FUNZIONE DLLMAIN



DllMain(x,x,x) .text 000000001000D02E 000000DF R . . . . T .

02 FUNZIONE «GETHOSTBYNAME »



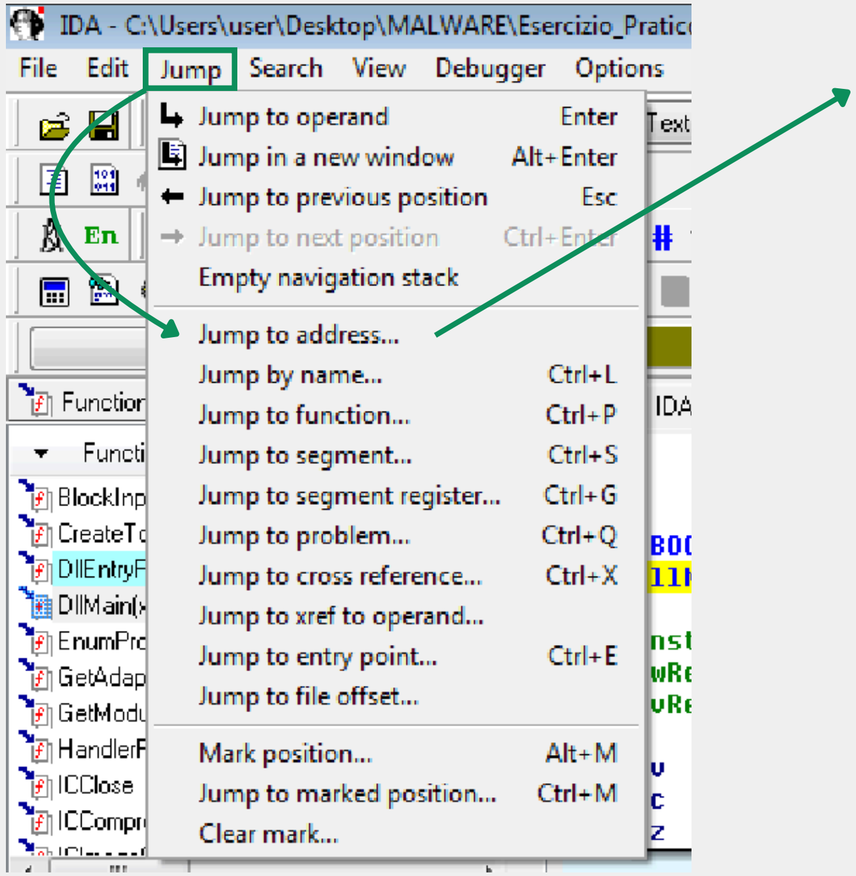
02 FUNZIONE «GETHOSTBYNAME »

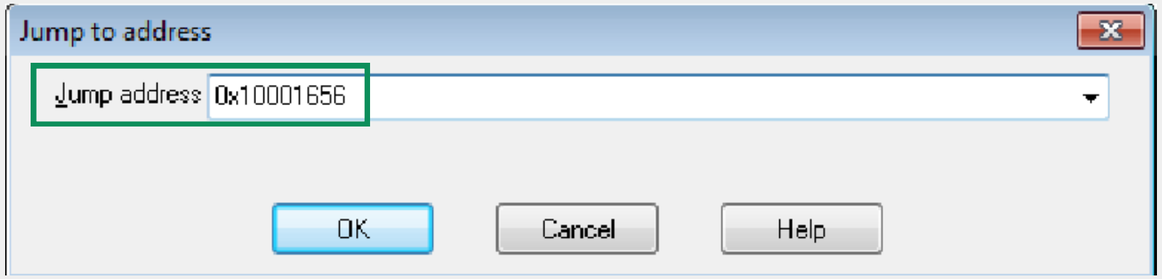
```
.idata:100163CC ; struct hostent *__stdcall gethostbyname(const char *name)
.idata:100163CC                 extrn gethostbyname:dword
.idata:100163CC                                         ; CODE XREF: sub_10001074:loc_100011AF↑p
.idata:100163CC                                         ; sub_10001074+1D3↑p ...
```

La funzione fa parte della libreria delle API di Windows per il networking. La funzione prende come input un nome di host (come un URL o un nome di dominio) e restituisce un puntatore a una struttura hostent, che contiene informazioni sull'host, come l'indirizzo IP associato.

Quindi, la funzione cerca nel DNS l'indirizzo IP associato a un nome di dominio specificato e ritorna queste informazioni strutturate.

03 VARIABILI LOCALI ALLA LOCAZIONE DI MEMORIA 0X10001656






```
.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 -4BCh
.text:10001656 phkResult         = byte ptr -3B8h
.text:10001656 var_3B0           = dword ptr -3B0h
.text:10001656 var_1A4           = dword ptr -1A4h
.text:10001656 var_194           = dword ptr -194h
.text:10001656 WSAData           = WSAData ptr -190h
```

04 PARAMETRI DELLA FUNZIONE SOPRA

```
.text:10001656 arg 0                   = dword ptr  4
```

I parametri (o argomenti) sono valori che vengono passati a una funzione quando questa viene chiamata, permettendo alla funzione di lavorare con dati specifici forniti dal chiamante.

05 ALTRE CONSIDERAZIONI SUL MALWARE

```
call    ds:GetCurrentProcessId
```

La funzione GetCurrentProcessId è una funzione dell'API di Windows che restituisce l'ID (identificatore) del processo corrente. Questo ID è un valore univoco assegnato dal sistema operativo a ciascun processo in esecuzione e può essere utilizzato per identificare e gestire il processo corrente.

```
call    ds:WinExec
```

La funzione WinExec è una funzione della API di Windows utilizzata per eseguire un programma. È stata introdotta nelle prime versioni di Windows e si trova principalmente nelle versioni più vecchie del sistema operativo, come Windows 95, 98 e ME.

```
call    esi ; _stricmp
```

La funzione stricmp è una funzione di confronto di stringhe che, in alcune implementazioni di librerie di C e C++, confronta due stringhe in modo case-insensitive, ossia ignorando le differenze tra maiuscole e minuscole