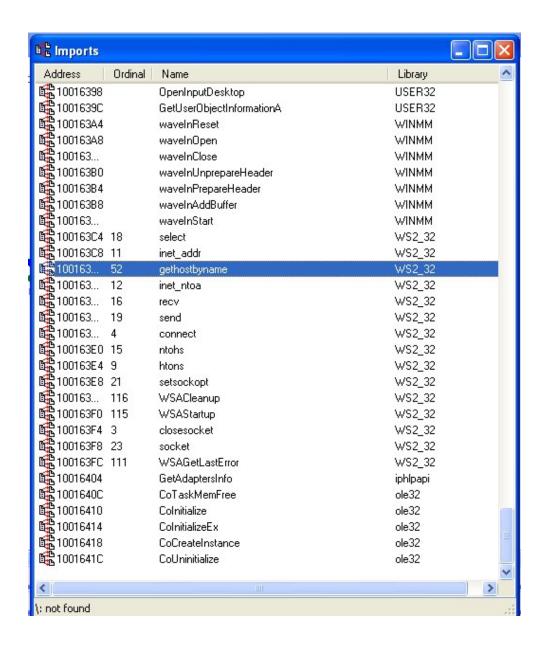
## Traccia:

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
- 2. Dalla scheda «imports» individuare la funzione «gethostbyname». Qual è l'indirizzo dell'import?
- 3. Quante sono le variabili locali della funzione alla locazione di memoria 0×10001656?
- 4. Quanti sono, invece, i parametri della funzione sopra?

```
.text:1000D02B
 .text:1000D02E
 .text:1000D02E
 .text:1000D02E
 .text:1000D02E ; BOOL __stdcall DllMain(HINSTANCE hinstDLL,DWORD fdwReason,LPUOID lpvReserved)
                                                  ; CODE XREF: DllEntryPoint+4Blp
; DATA XREF: sub_100110FF+2Dlo
 .text:1000D02E _D11Main@12
                            proc near
 .text:1000D02E
 .text:1000D02E
 .text:1000D02E hinstDLL
                             = dword ptr 4
 .text:1000D02E fdwReason
                             = dword ptr
                                         8
 .text:1000D02E lpvReserved
                             = dword ptr
                                         BCh
 .text:1000D02E
                                    eax, [esp+fdwReason]
 .text:1000D02E
                             mov
 .text:1000D032
                             dec
                                    eax
.text:1000D033
                                    loc 1000D107
                             jnz
```

L'indirizzo della funzione main è: 1000D02E



L'indirizzo di "gethostbyname" è: 100163CC

```
国 IDA View-A
            .text:10001656
            .text:10001656
            .text:10001656
.text:10001656 ; DWORD
                                           _stdcall sub_10001656(LPVOID)
            .text:10001656 sub_10001656
                                                                                   ; DATA XREF: DllMain(x,x,x)+C8to
                                                   proc near
            .text:10001656
            .text:10001656 var_675
                                                   = byte ptr -675h
                                                  = dword ptr -674h

= dword ptr -679h

= timeval ptr -66Ch

= sockaddr ptr -664h

= word ptr -654h
            .text:10001656 var_674
            .text:10001656 hModule
            .text:10001656 timeout
            .text:10001656 name
            .text:10001656 var_654
            .text:10001656 in
                                                   = in_addr ptr -650h
                                                  = byte ptr -644h
= byte ptr -63Fh
= byte ptr -638h
= dword ptr -544h
           .text:10001656 Parameter
.text:10001656 CommandLine
            .text:10001656 Data
           .text:10001656 var_544
.text:10001656 var_50C
                                                   = dword ptr -50Ch
            .text:10001656 var_500
.text:10001656 var_4FC
.text:10001656 readfds
                                                   = dword ptr -500h
                                                   = dword ptr -4FCh
                                                   = fd_set ptr -4BCh
= HKEY__ ptr -3B8h
= dword ptr -3B0h
            .text:10001656 phkResult
            .text:10001656 var_380
           .text:10001656 var_1A4
.text:10001656 var_194
.text:10001656 WSAData
                                                   = dword ptr -1A4h
= dword ptr -194h
= WSAData ptr -190h
            .text:10001656 arg_0
                                                   = dword ptr
            .text:10001656
            .text:10001656
                                                              esp, 678h
          .text:1000165C
                                                    push
                                                              ebx
            .text:1000165D
                                                    push
                                                              ebp
            .text:1000165E
                                                    push
                                                              esi
           .text:1000165F
                                                              edi
                                                    push
```

A questo indirizzo (10001656) ci sono 20 variabili

C'è un solo argomento passato alla funzione, ha offset positivo rispetto a EBP, chiamato da IDA "arg\_0"