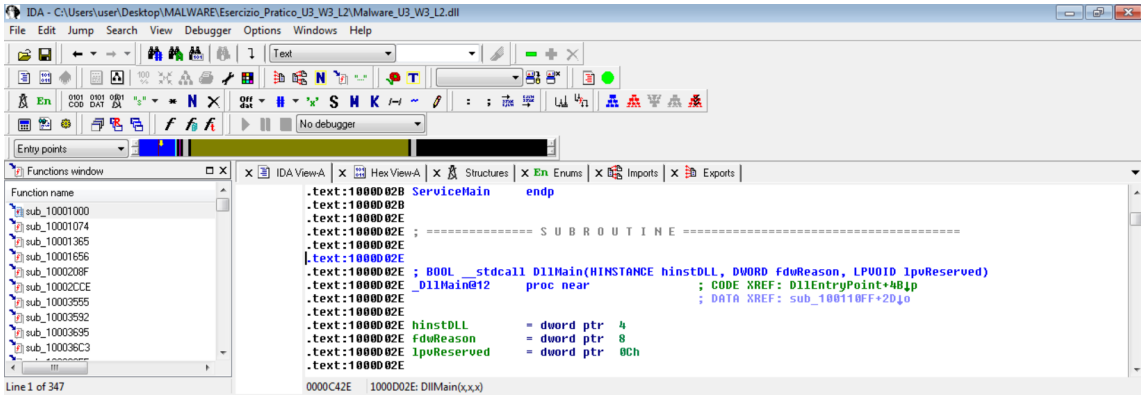
# Advanced static analysis with IDA

## Objective

The objective of this analysis is to identify specific addresses and details related to functions and memory locations within an executable file using IDA Pro.

## Tasks and Solutions

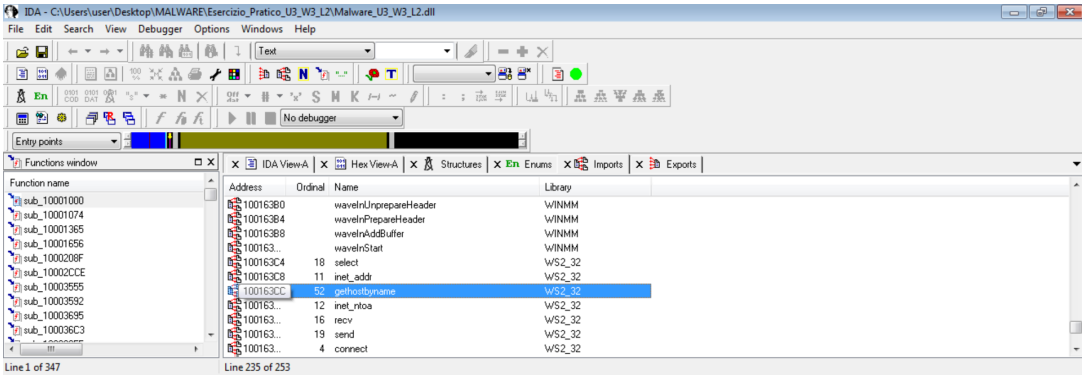
1. **Identify the Address of the `DLLMain` Function**
   - **Procedure:**
     - Load the executable file in IDA Pro.
     - Switch to textual mode.
     - Retrieve the address of the `main` function.




   - **Result:**
     - The address of the `DLLMain` function is identified as `1000D02E`.

2. **Identify the Import Address of the `gethostbyname` Function**
   - **Procedure:**
     - Open the "imports" window in IDA Pro.

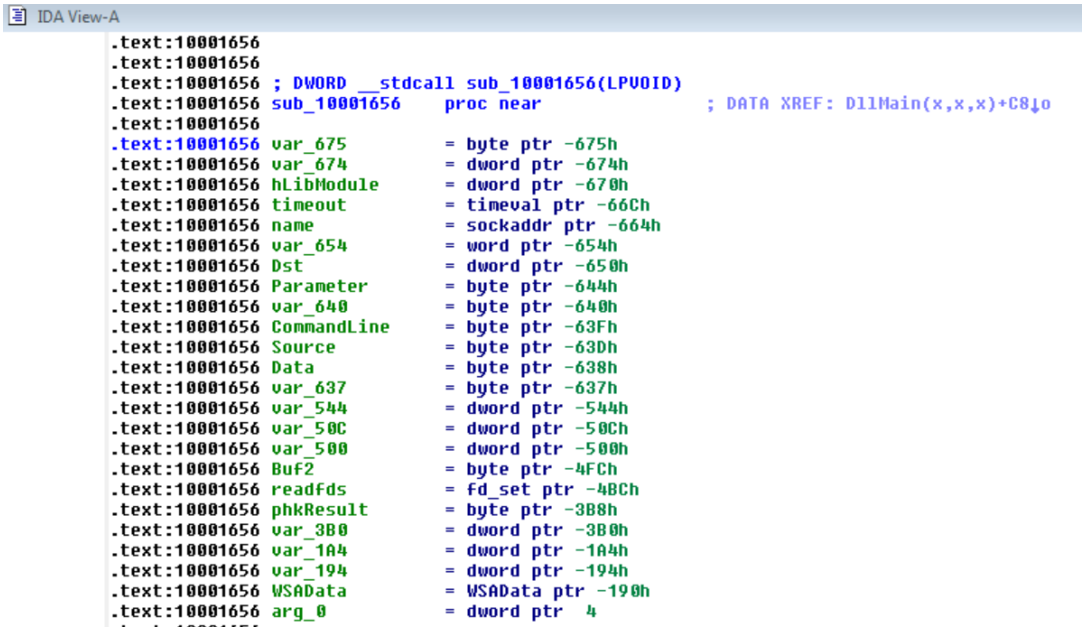
- Locate the function `gethostbyname` within the imports list.




- **Result:**
  - The import address for `gethostbyname` is `100163CC`.

3. **Identify Local Variables at Memory Location 10001656**

- **Procedure:**
  - Analyze the function at memory location `10001656` to determine the number of local variables.




- **Result:**
  - The number of local variables is 20 because 20 variables have a negative offset value compared to

EBP.

4. **Identify Parameters of the Function at Memory Location 10001656**
   - **Procedure:**
     - Analyze the function at memory location `10001656` to determine the number of parameters.

```
IDA View-A
.text:10001656
.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 -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
.text:10001656 arg_0           = dword ptr  4
```

   - **Result:**
     - The number of parameters is just one, its name is `arg_0.`

       It is the only one with a positive offset value compared to EBP.

---

## Conclusion

This analysis demonstrated the use of IDA Pro for identifying function addresses and import addresses within an executable file. The address of the `DLLMain` function and the import address for `gethostbyname` were successfully identified. Further analysis is required to determine the number of local variables and parameters for the function at memory location `10001656`.

---