Computer Science 491/691
Malware Analysis
Homework 4
Assigned: March 13, 2019
Due: March 25, 2019

Submitted by: Sai Sasaank Pallerla
ID: HG13015

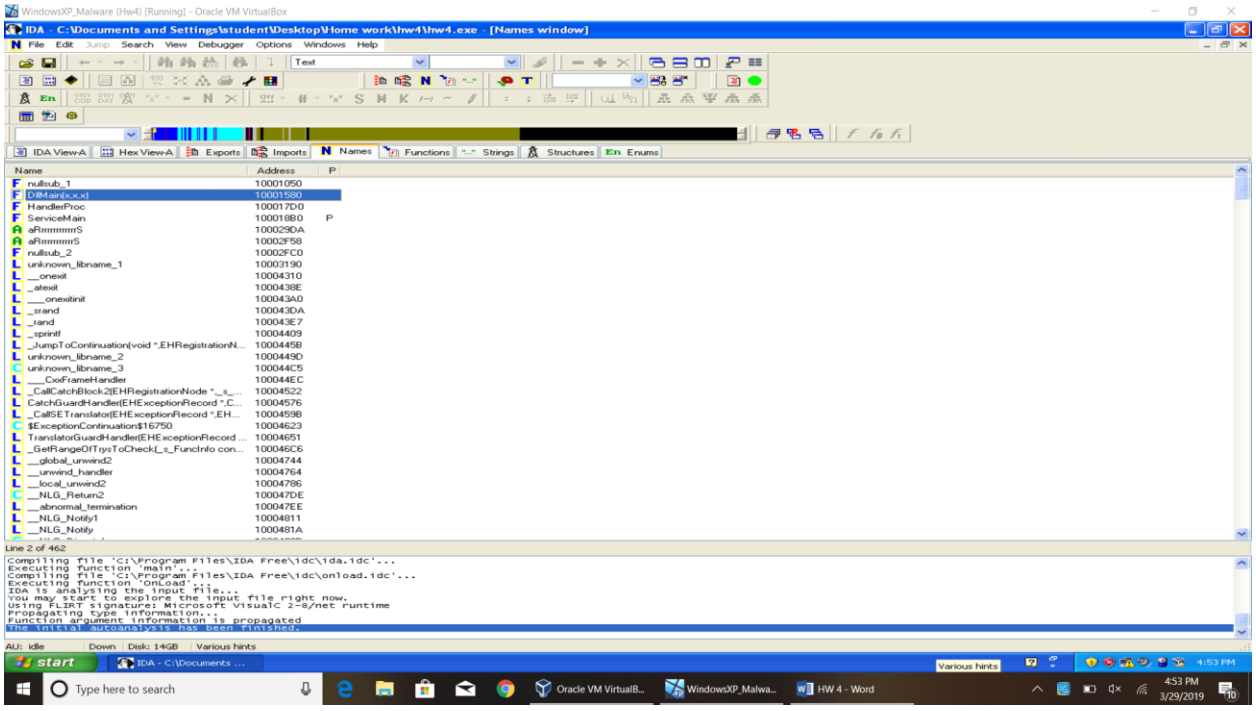
How to turn this in for grading: You can edit your answers right into this file. Email it to the TAs as described in class. Make sure your name appears in the body of the document.

Hint: Chapter 5 of your Practical Malware Analysis textbook is a very useful reference!

Download hw4.7z and extract it. The password is "infected". Answer the following questions using IDA Pro (or the disassembler of your choice).

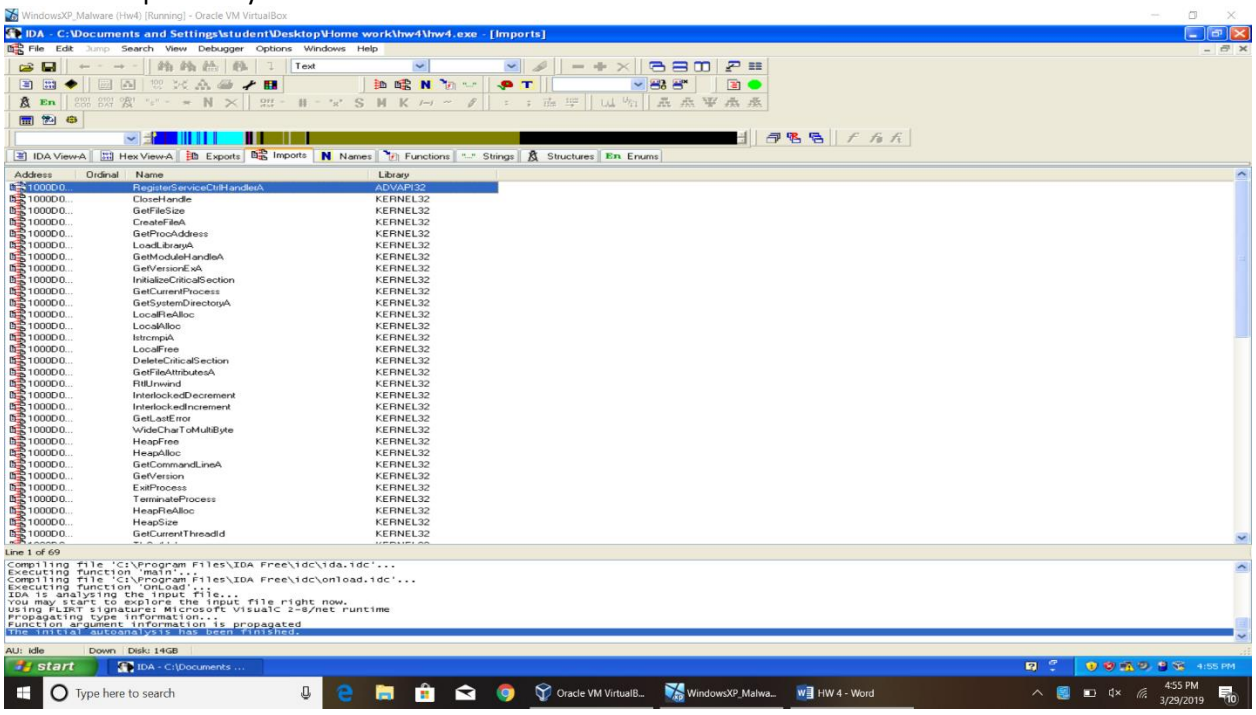
1) What is the address of the DllMain function? (5 pts)

DllMain Address: 10001580



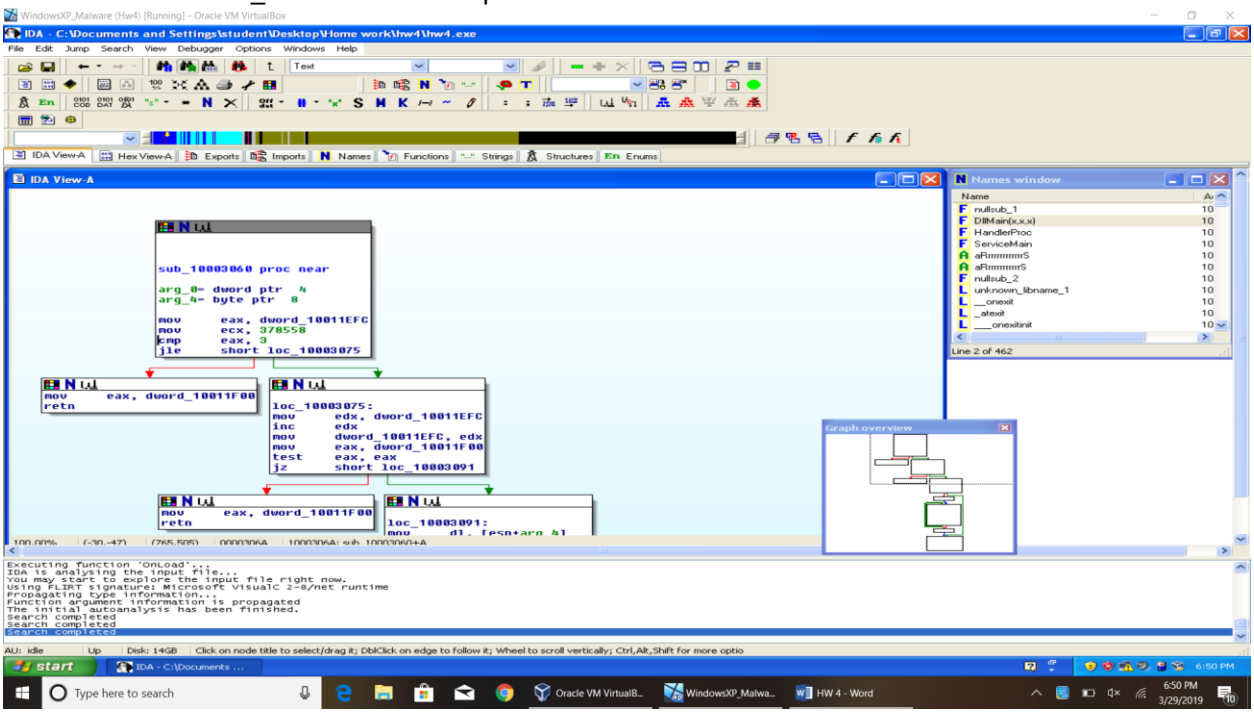
2) From which libraries does the malware import? (5 pts)

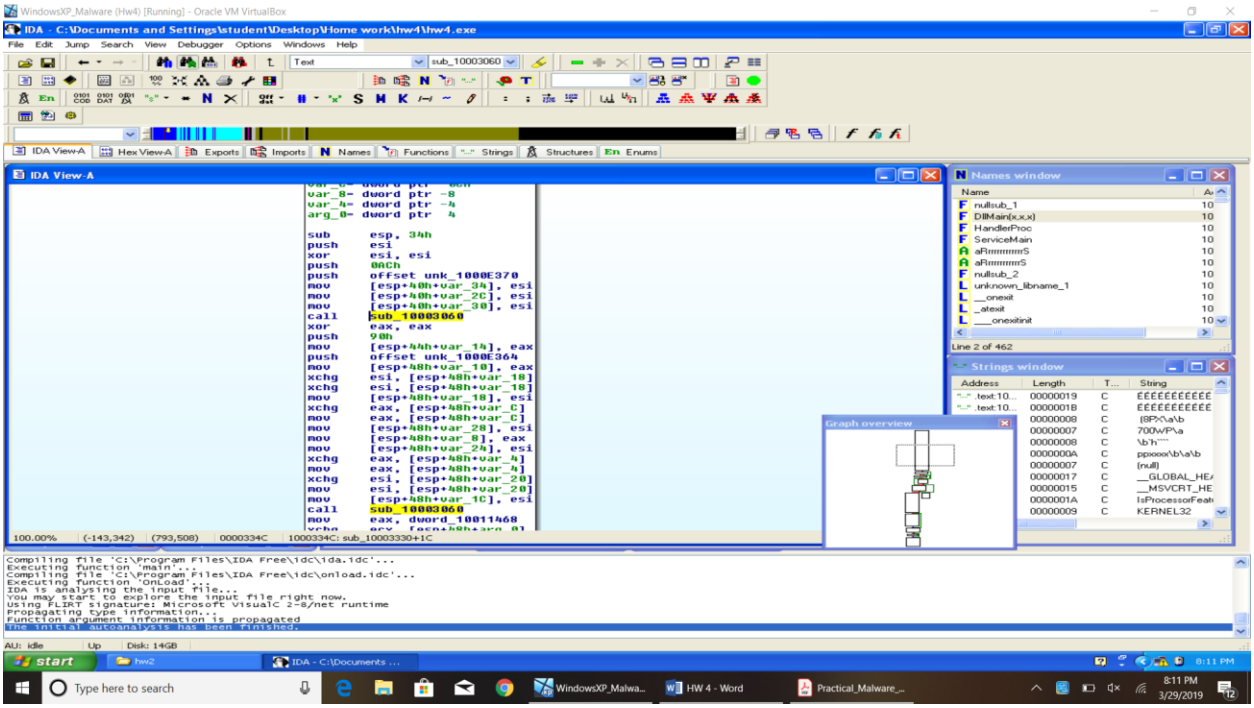
Libraries imported by malware: 1. ADVAPI32 2. KERNEL32 3. USER32



3) How many parameters does the function sub_10003060 take? (5 pts)

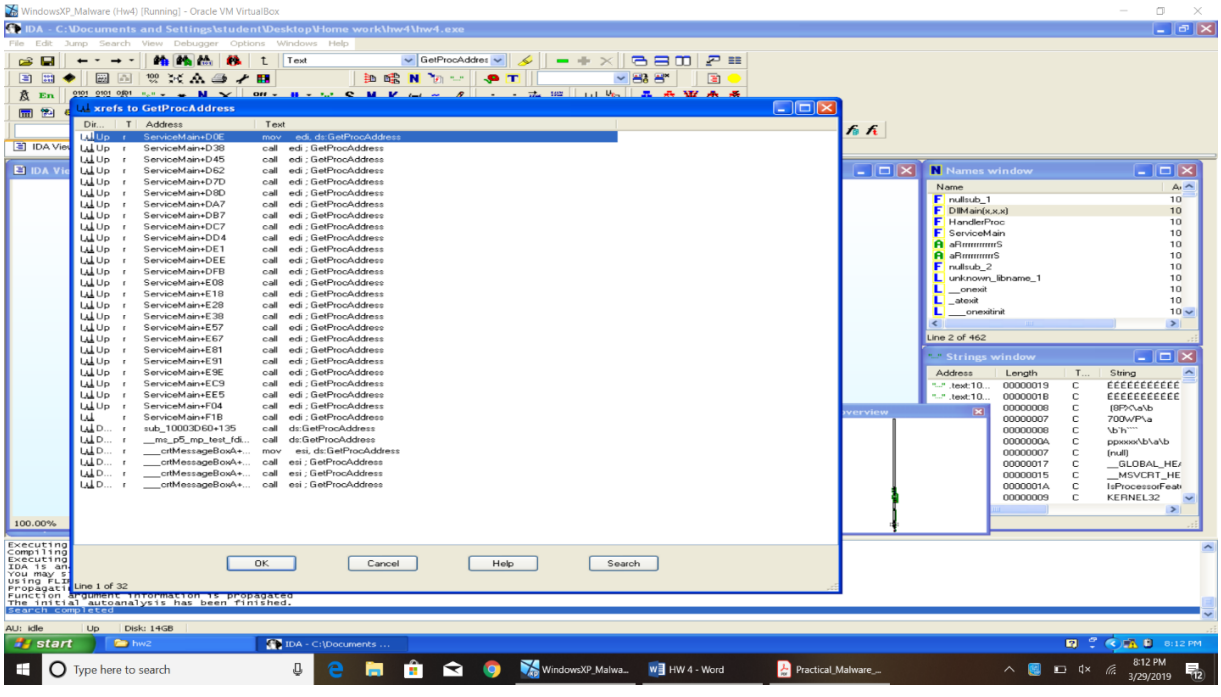
The function sub_10003060 takes 2 parameters





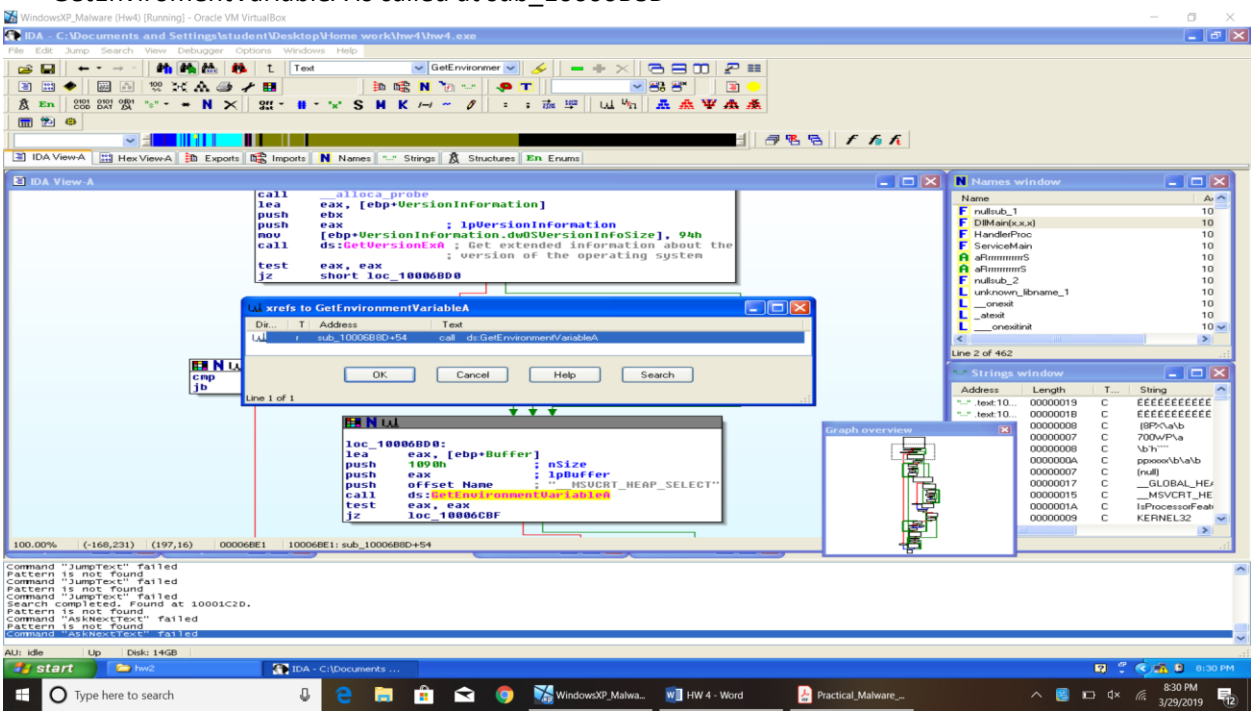
4) How many times is GetProcAddress called? What does the malware's use of GetProcAddress indicate? (10 pts)

The function GetProcAddress is 30 called times. GetProcAddress is used to call a function without using its actual name, this way the malware can indirectly call a function (without the analyst noticing). Retrieves the address of an exported function or variable from the specified dynamic-link library. Malware uses GetProcAddress with a combination of LoadLibraryA to access any function from any Dll whenever it wants to, even though its not mapped. Here the malware loads the library into a register and then this register is being called in GetProcAddress.



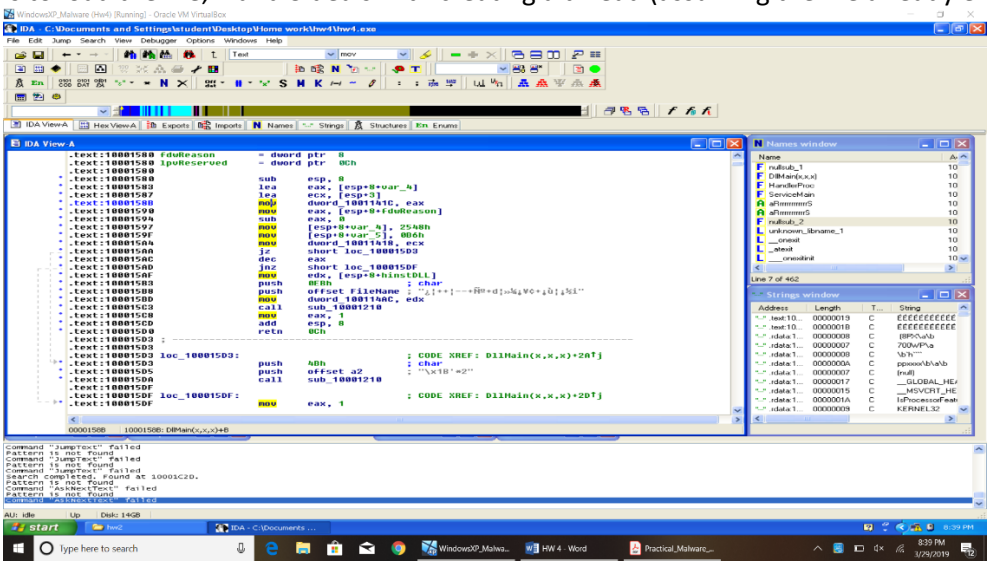
5) In which function is GetEnvironmentVariableA called? (5 pts)

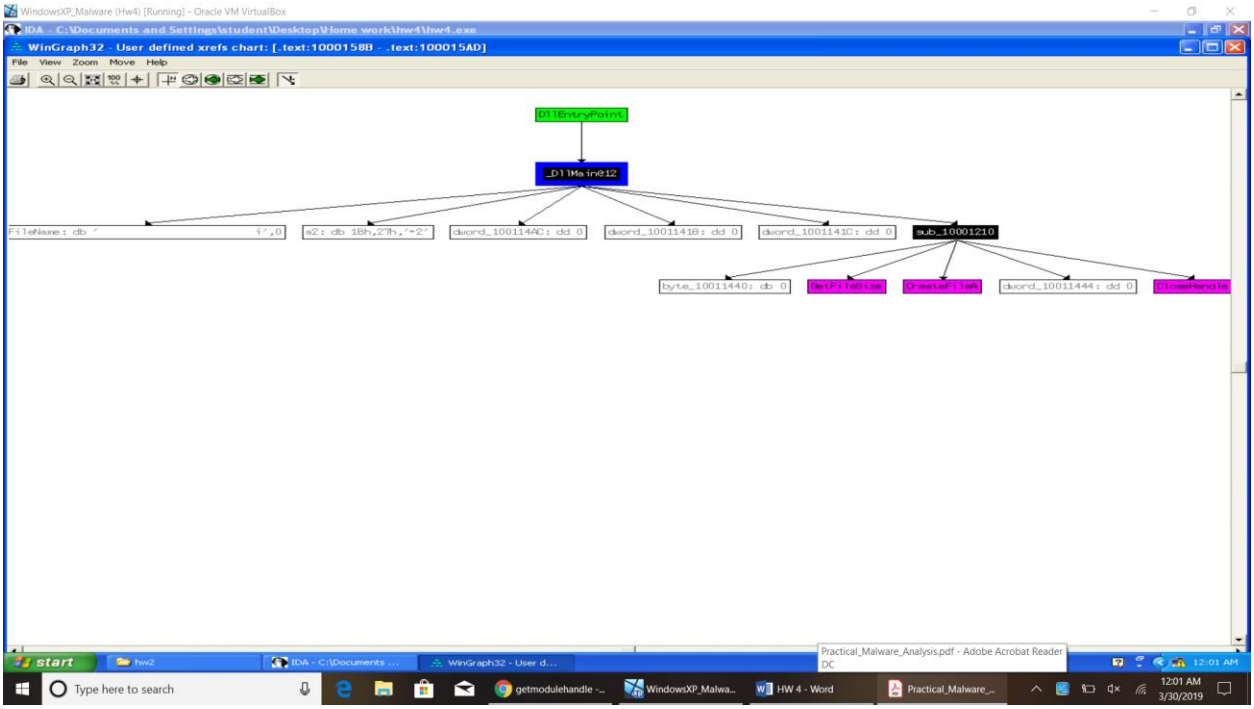
GetEnviromentVariableA is called at sub_10006B8D



6) Describe in detail what occurs from 0x1000158B to 0x100015AD. Why is the malware doing this? (Hint: What is setting the zero flag?) (15 pts)

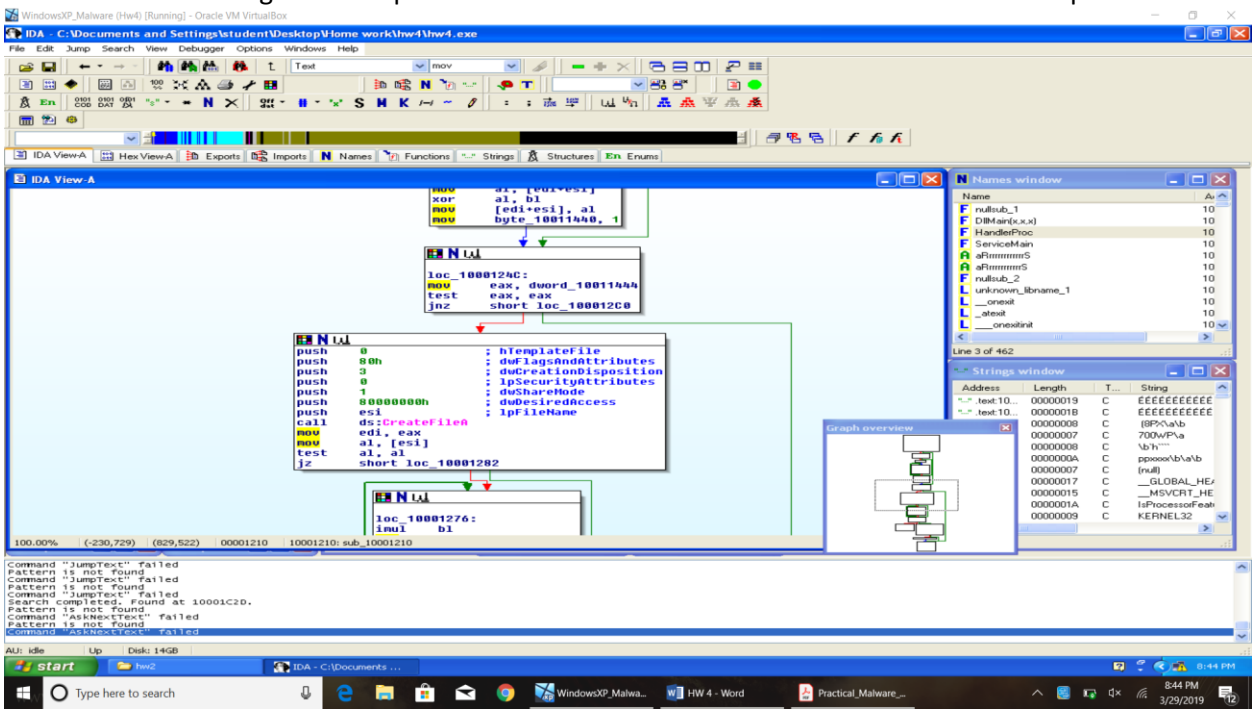
This is a snippet of the code from DllMain function. Here DllMain takes three parameters as input lpvReserved, fdwReason, hinstDll. But here in the snippet we deal with fdwReason, which is more like the reason for entry into DllMain. This takes LoadLibrary as an input parameter. This parameter take/ considers path of the module or the file. So here it is checking if a file (possibly a malware file) already exists or not. It does so by copying the value to eax register, if the file exists there will be a path and the (result of sub eax,0 will be 0) and the zero flag will be set. fwdReason takes four flags. 0 is to create file, 1 is to load the file, 2 and 3 deals with creating a thread (assuming the file already exisits).





7) What is the third parameter passed to the call to CreateFile in sub_10001210? What does this parameter indicate? (10 pts)

The parameter that is being passed in CreateFile (at the function sub_10001210) is dwShareMode. To get this parameter we just need to count the third push in reverse direction (i.e. bottom to top), so we get push 1 as the third parameter.

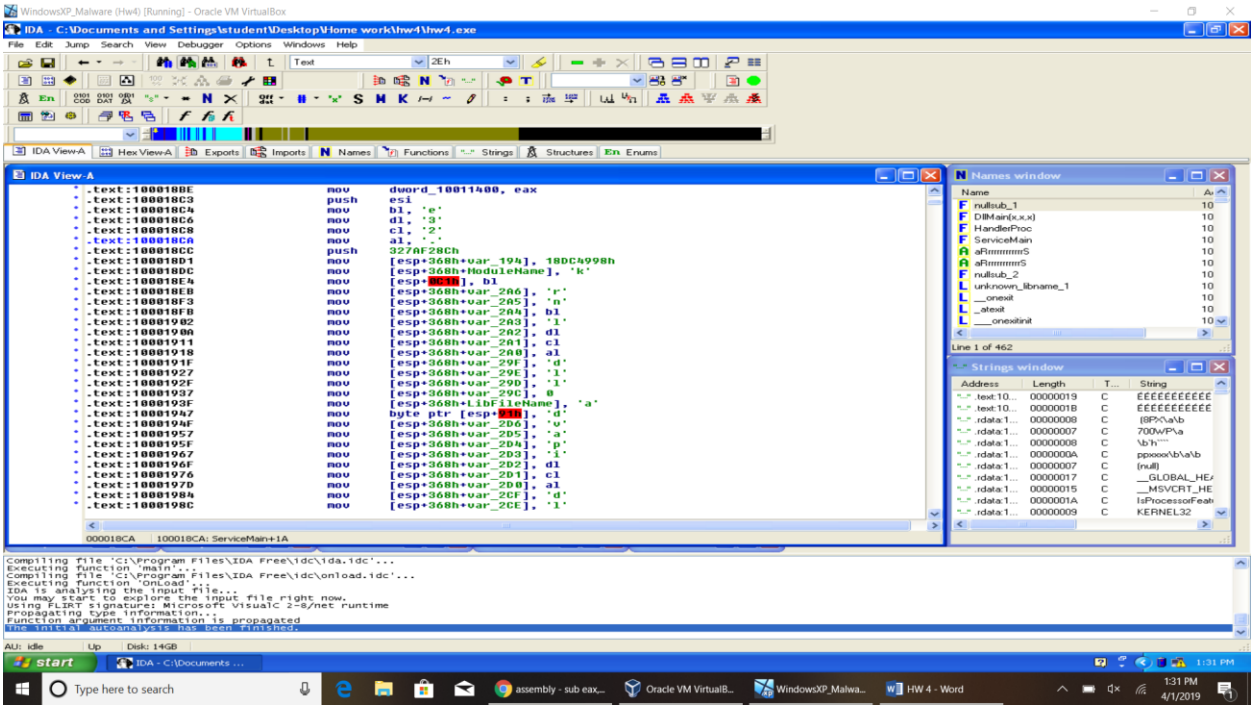


dwShareMode: This parameter is used to restrict/control access to the file (i.e. read, write, modify and delete operations. There are a total of 4 possible flags and with a combination of these flags and CreateFile function, this parameter behaves in different ways. Here the flag is set to 1 so it's used to request read access.

Value	Meaning
0 0x00000000	Prevents other processes from opening a file or device if they request delete, read, or write access.
FILE_SHARE_DELETE 0x00000004	Enables subsequent open operations on a file or device to request delete access. Otherwise, other processes cannot open the file or device if they request delete access. If this flag is not specified, but the file or device has been opened for delete access, the function fails. **Note** Delete access allows both delete and rename operations.
FILE_SHARE_READ 0x00000001	Enables subsequent open operations on a file or device to request read access. Otherwise, other processes cannot open the file or device if they request read access. If this flag is not specified, but the file or device has been opened for read access, the function fails.
FILE_SHARE_WRITE 0x00000002	Enables subsequent open operations on a file or device to request write access. Otherwise, other processes cannot open the file or device if they request write access. If this flag is not specified, but the file or device has been opened for write access or has a file mapping with write access, the function fails.

8) Describe in detail what occurs from 0x100018DC to 0x10001937. (15 pts)

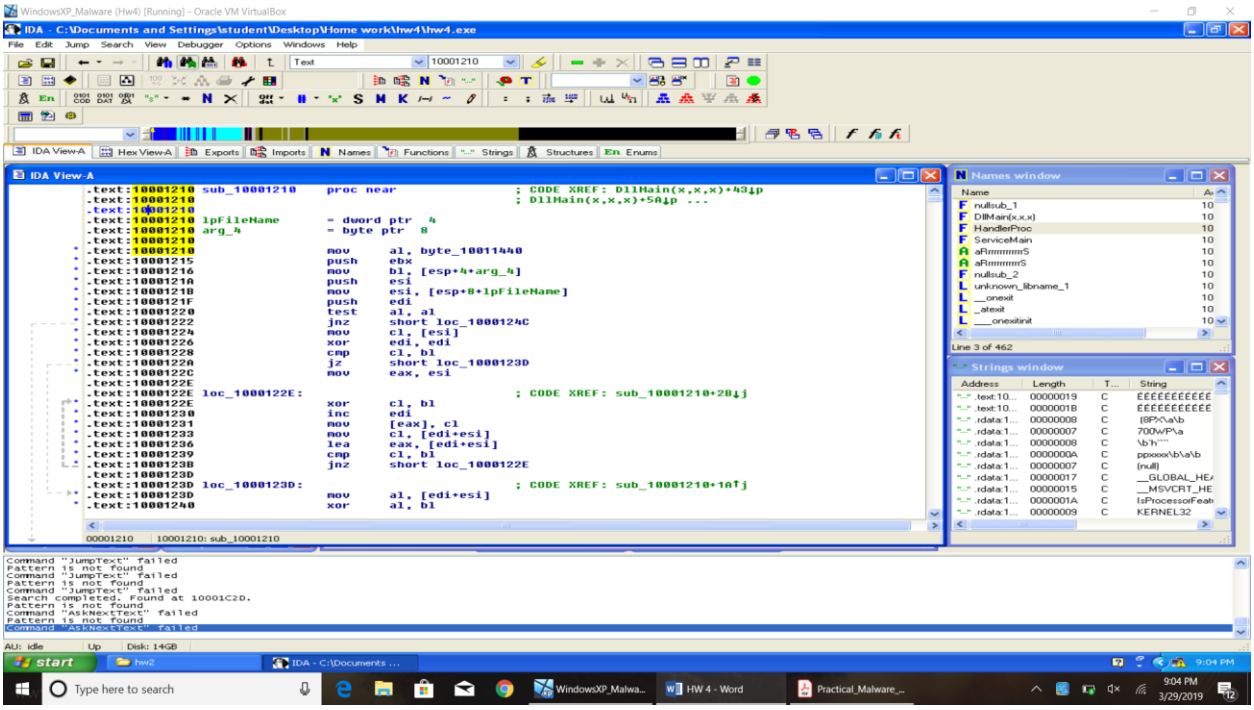
The snippet of assembly code from 100018DC to 10001937 stores the name of the ModuleName which is Kernel32.dll, the individual characters in the stack are stored in Hex values (probably to obfuscate and hide it's)



9) Answer the following questions about sub_10001210: (30 pts)

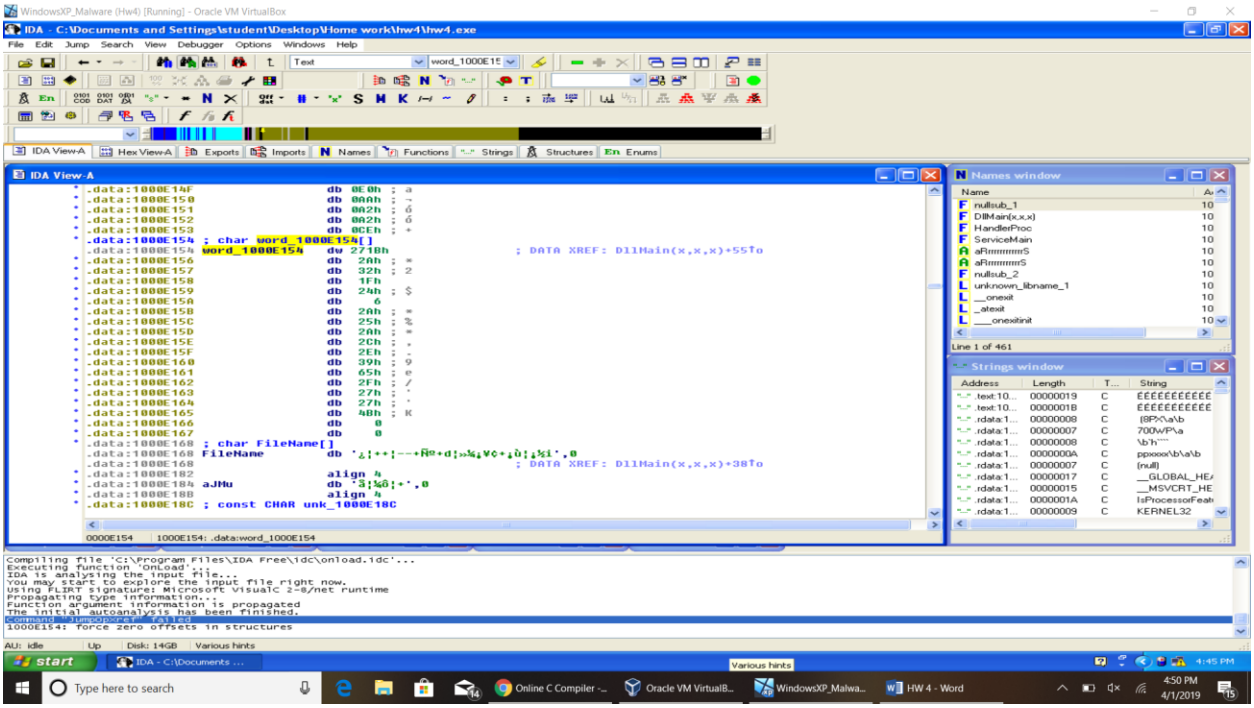
a. **Write a function in C that is equivalent to the instructions from 0x10001210 to 0x1000123B. Assume that the function returns when execution reaches 0x1000123D.**

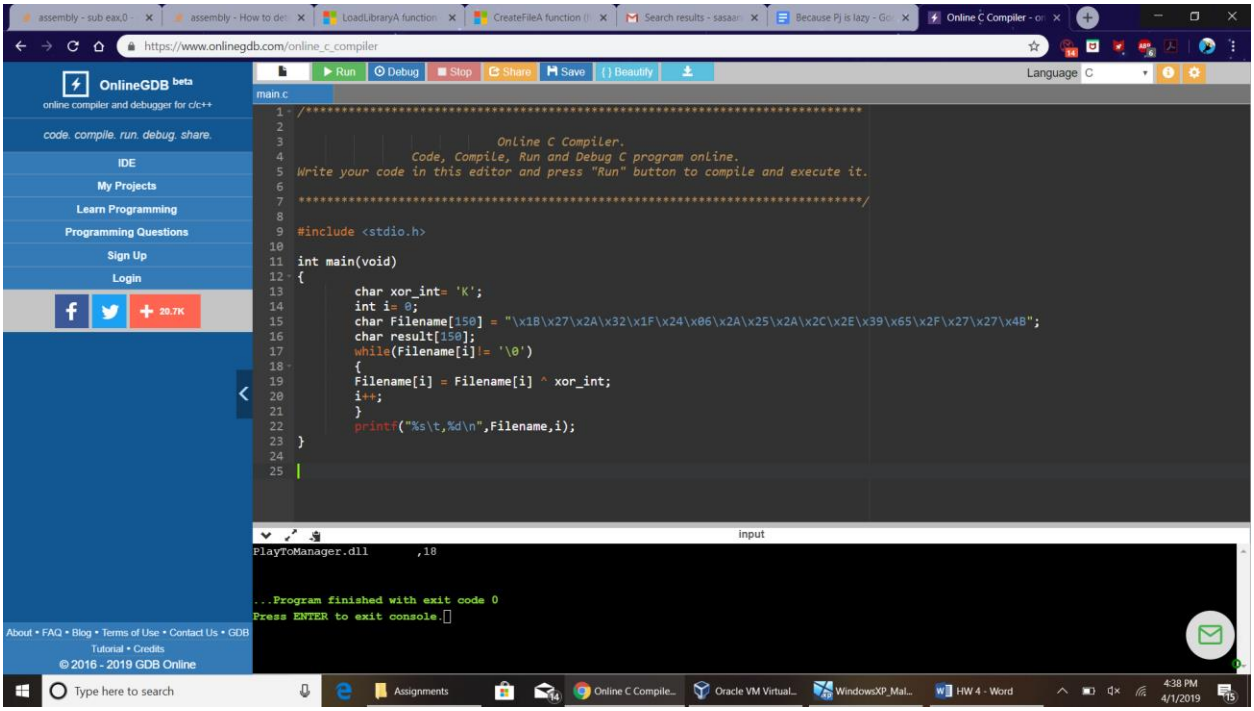
```
int sub_10001210(char* lpFileName, int arg_0){
int var_1 = 0;
char r;
while( lpFileName!= 0 )
        {
        r = lpFileName[var_1];
        r = r ^ arg_0;
        var_1++;
        *lpFileName = r;
        }
return *lpFileName;
}
```



b. **DllMain calls sub_10001210 at 0x100015C3. What is contained in the string pointed to by lpFileName when execution reaches 0x1000123D?**

The Value of the string pointed by lpFileName when the execution reaches 1000123D is PlayToManager.dll


WindowsXP_Malware (Hw4) [Running] - Oracle VM VirtualBox
IDA - C:\Documents and Settings\student\Desktop\Home work\hw4\hw4.exe
File Edit Jump Search View Debugger Options Windows Help
IDA View-A
Hex View-A
Exports
Imports
Names
Functions
Strings
Structures
Enums
Names window
Strings window
.data:1000E154 ; char word_1000E154[]
word_1000E154 dw 2718h ; DATA XREF: DllMain(x,x,x)+55↑o
.data:1000E168 ; char FileName[]
FileName db '¿|++¦--+Ñº+d¦»¼¡¥¢+¡ù¦¿¾i',0
.data:1000E184 aJMu db '?3¦¾8¦+',0
.data:1000E18C ; const CHAR unk_1000E18C
Compiling file 'C:\Program Files\IDA Free\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: Microsoft Visualc 2-8/net runtime
Propagating type information...
Function argument information is propagated
The initial autoanalysis has been finished.
1000E154: force zero offsets in structures
AU: idle
Up
Disk: 14GB
Various hints
start
Type here to search
4:50 PM
4/1/2019


https://www.onlinegdb.com/online_c_compiler
OnlineGDB beta
online compiler and debugger for c/c++
code. compile. run. debug. share.
IDE
My Projects
Learn Programming
Programming Questions
Sign Up
Login
Run
Debug
Stop
Share
Save
{ } Beautify
Language C
main.c
/***
Online C Compiler.
Code, Compile, Run and Debug C program online.
Write your code in this editor and press "Run" button to compile and execute it.
***/
#include <stdio.h>
int main(void)
{
char xor_int= 'K';
int i= 0;
char Filename[150] = "\x18\x27\x2A\x32\x1F\x24\x06\x2A\x25\x2A\x2C\x2E\x39\x65\x2F\x27\x27\x4B";
char result[150];
while(Filename[i]!= '\0')
{
Filename[i] = Filename[i] ^ xor_int;
i++;
}
printf("%s\t,%d\n",Filename,i);
}
input
PlayToManager.dll ,18
...Program finished with exit code 0
Press ENTER to exit console.
About • FAQ • Blog • Terms of Use • Contact Us • GDB Tutorial • Credits
© 2016 - 2019 GDB Online
Type here to search
4:38 PM
4/1/2019