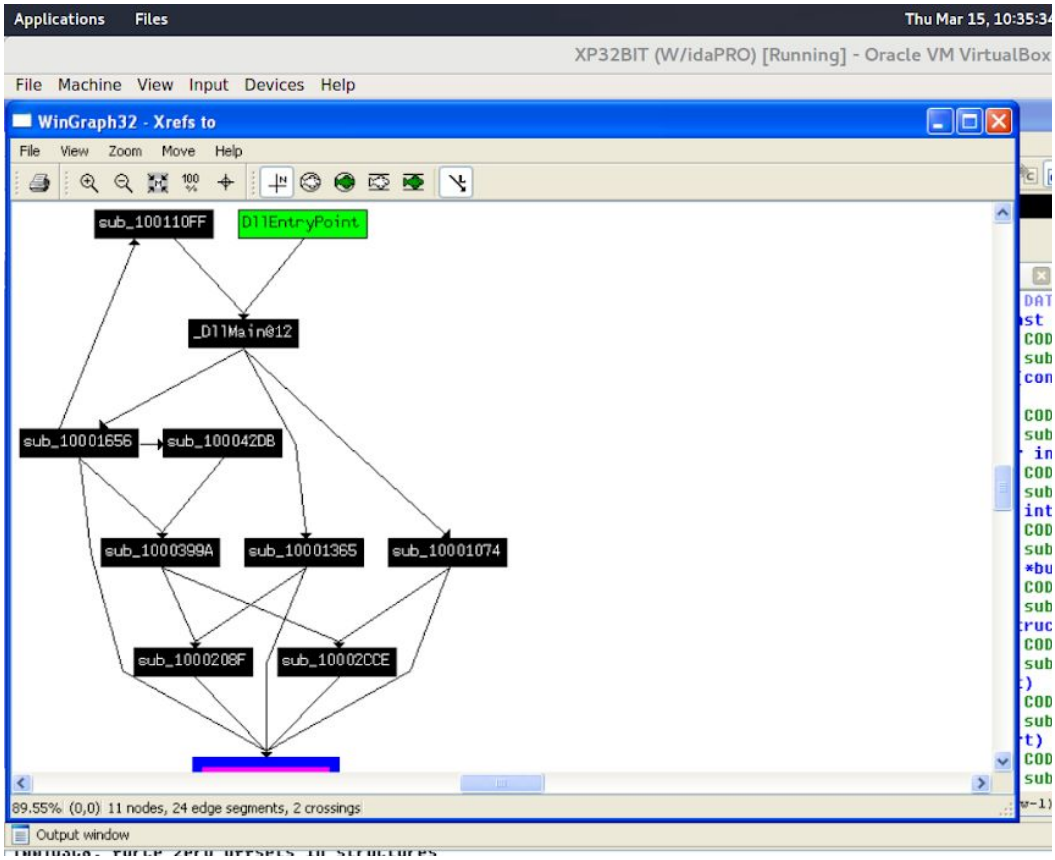
Song Yang (sy540)
Xin Yang (xy213)
Zhuohang Li(zl299)

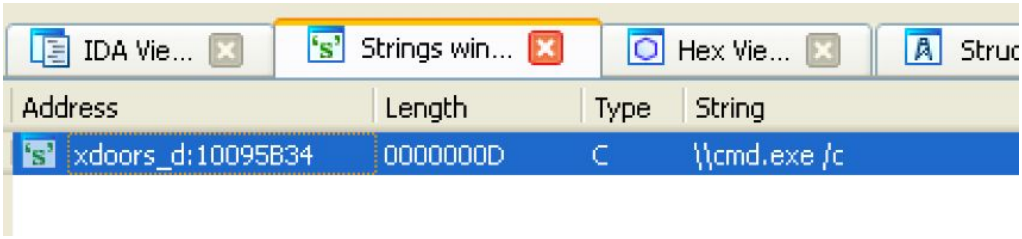
Report of Homework 3

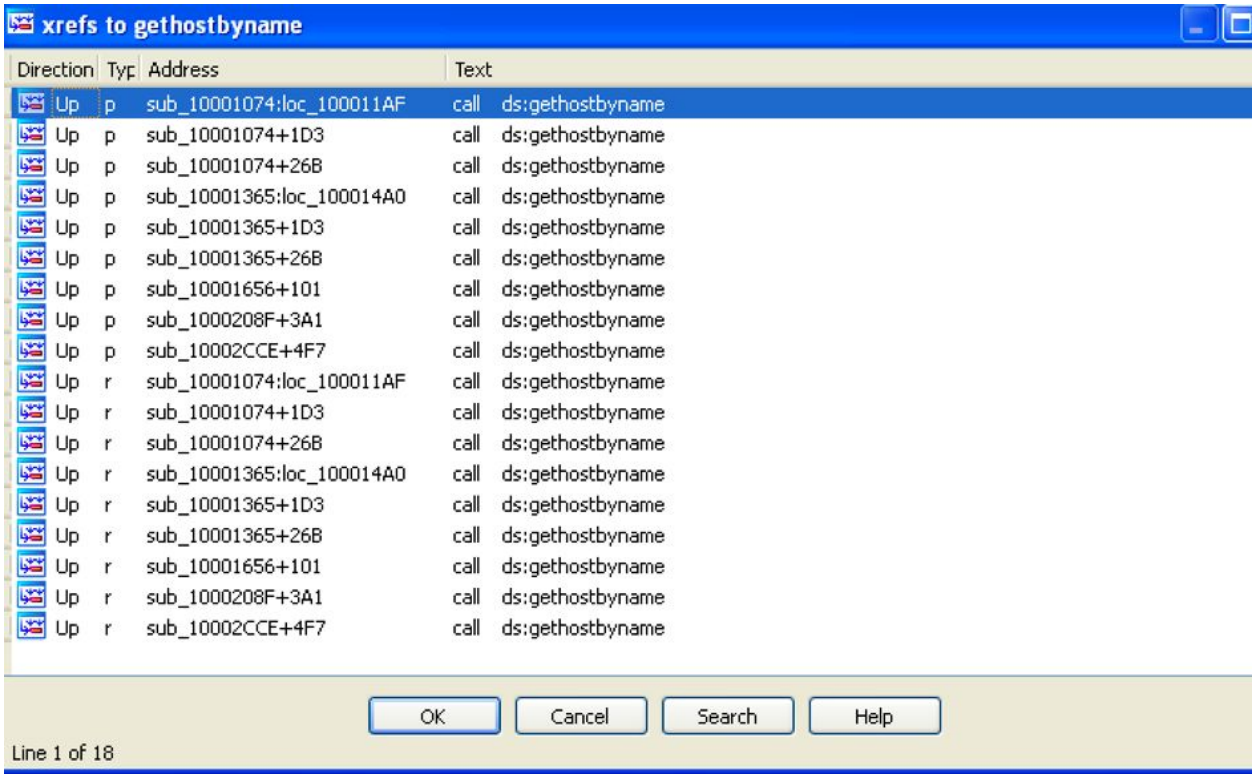
1. The address of DllMain is .text:1000D02E

2. Import gethostbyname is at .idata:100163CC

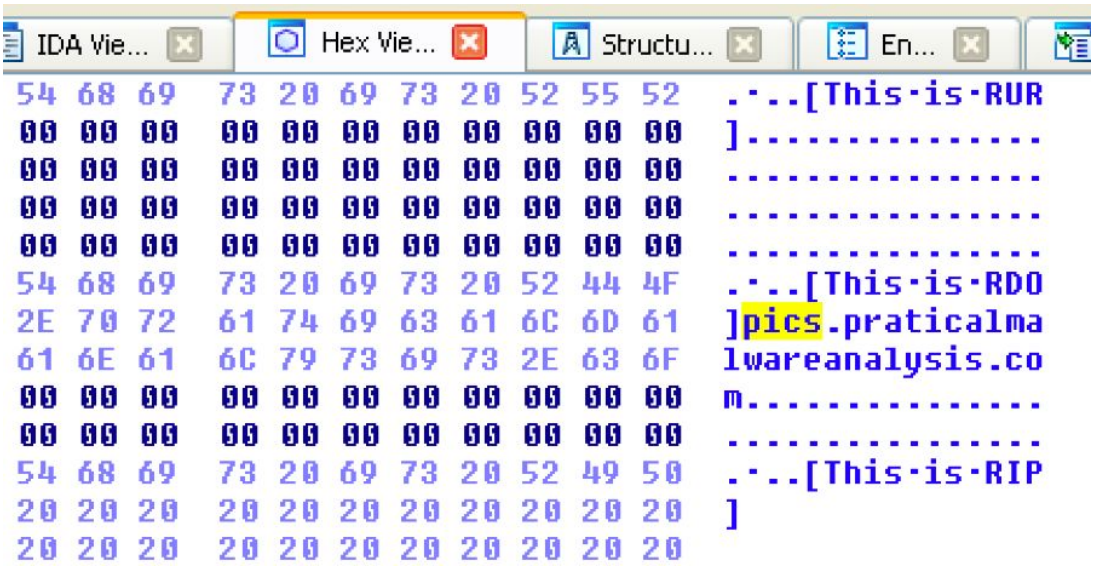
3. 9 times



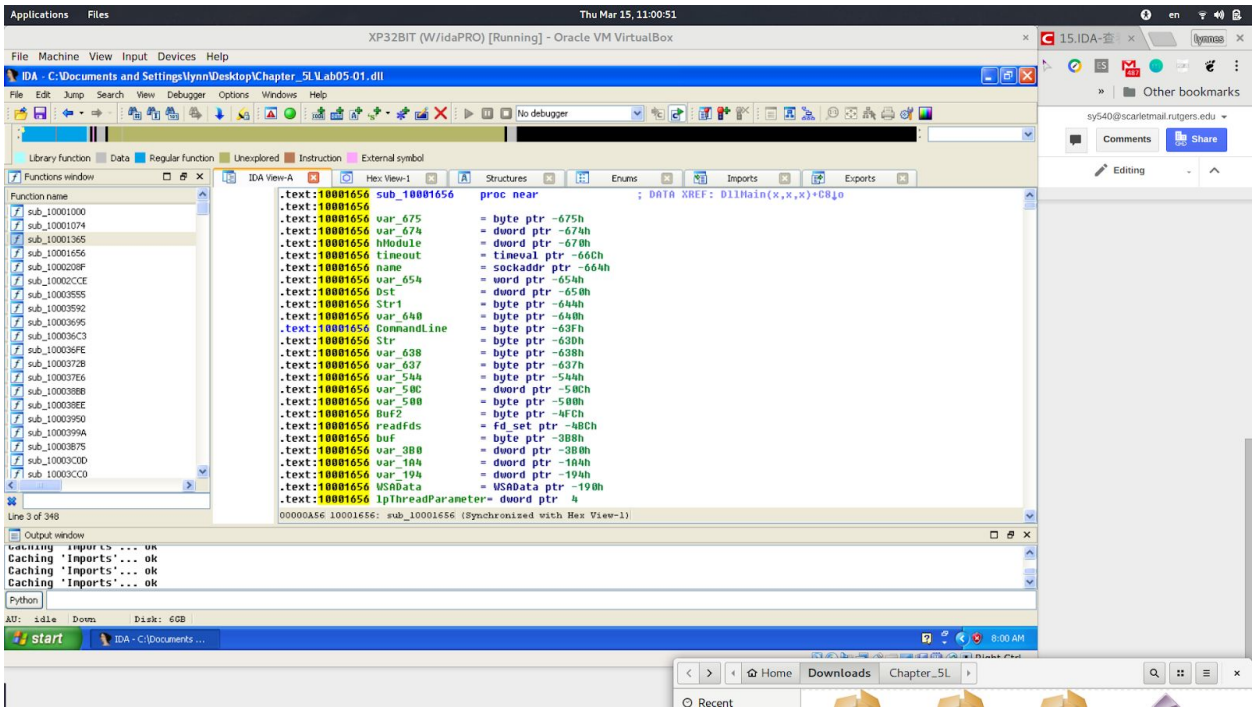




4. The program pushed the off_10019040 to the stack and add 0Dh for calling as a parameter of gethostbyname, and the off_10019040 should be somehow the DNS. 0Dh_10019040 locates to the string, '[This is RDO]pics.praticalmalwareanalysis.com'.



5. Totally there are 24 variables, but the number of variables that begin with var_ is 12.



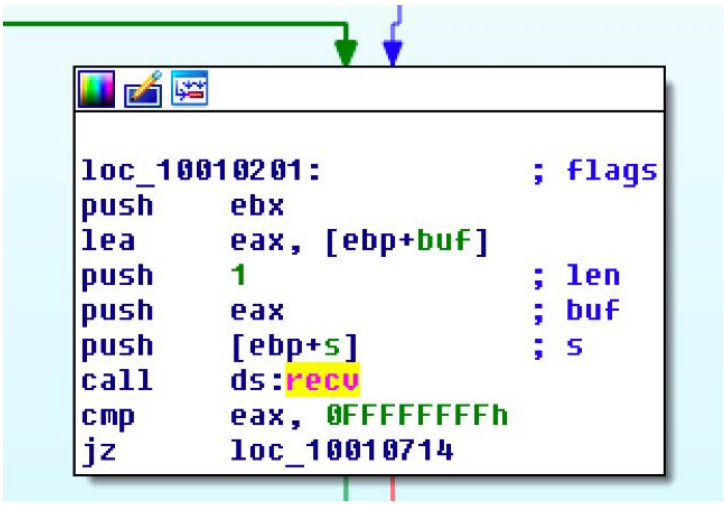
6. It says:
.text:10001656 ; DWORD __stdcall sub_10001656(LPVOID lpThreadParameter)
So that means there is one parameter.

7. C \\cmd.exe /c is located in xdoors_d:10095B34

```
xdoors_d:10095B1D 00 00 00                                align 10h
xdoors_d:10095B20                       ; char aCommand_exeC[]
xdoors_d:10095B20 5C 63 6F 6D 6D 61+aCommand_exeC   db '\command.exe /c ',0 ; DATA XREF: sub_1000FF58:loc_10
xdoors_d:10095B31 00 00 00                          align 4
xdoors_d:10095B34 5C 63 6D 64 2E 65+aCmd_exeC       db '\cmd.exe /c ',0     ; DATA XREF: sub_1000FF58+278↑o
xdoors_d:10095B41 00 00 00                          align 4
xdoors_d:10095B44                       ; char aHiMasterDDDDDD[]
xdoors_d:10095B44 48 69 2C 4D 61 73+aHiMasterDDDDDD db 'Hi,Master [%d/%d/%d %d:%d:%d]',0Dh,0Ah
xdoors_d:10095B44 74 65 72 20 5B 25+                ; DATA XREF: sub_1000FF58+145↑o
xdoors_d:10095B44 64 2F 25 64 2F 25+                db 'WelCome Back...Are You Enjoying Today?',0Dh,0Ah
xdoors_d:10095B44 64 20 25 64 3A 25+                db 0Dh,0Ah
xdoors_d:10095B44 64 3A 25 64 5D 0D+                db 'Machine UpTime  [%-.2d Days %-.2d Hours %-.2d Minutes
xdoors_d:10095B44 0A 57 65 6C 43 6F+                db 'ds]',0Dh,0Ah
xdoors_d:10095B44 6D 65 20 42 61 63+                db 'Machine IdleTime [%-.2d Days %-.2d Hours %-.2d Minute
xdoors_d:10095B44 6B 2E 2E 2E 41 72+                db 'nds]',0Dh,0Ah
xdoors_d:10095B44 65 20 59 6F 75 20+                db 0Dh,0Ah
xdoors_d:10095B44 45 6E 6A 6F 79 69+                db 'Encrypt Magic Number For This Remote Shell Session [
xdoors_d:10095B44 6E 67 20 54 6F 64+                db 0Dh,0Ah,0
xdoors_d:10095C5C                       ; char asc_10095C5C[]
xdoors_d:10095C5C 3E 00                 asc_10095C5C    db '>',0                ; DATA XREF: sub_1000FF58+4B↑o
xdoors_d:10095C5C                                       ; sub_1000FF58+3E1↑o
xdoors_d:10095C5E 00 00 00 00 00 00+                align 400h
xdoors_d:10095C5E 00 00 00 00 00 00+xdoors_d        ends
xdoors_d:10095C5E 00 00 00 00 00 00+
xdoors_d:10095C5E 00 00 00 00 00 00+
xdoors_d:10095C5E 00 00 00 00 00 00+                end DllEntryPoint
```

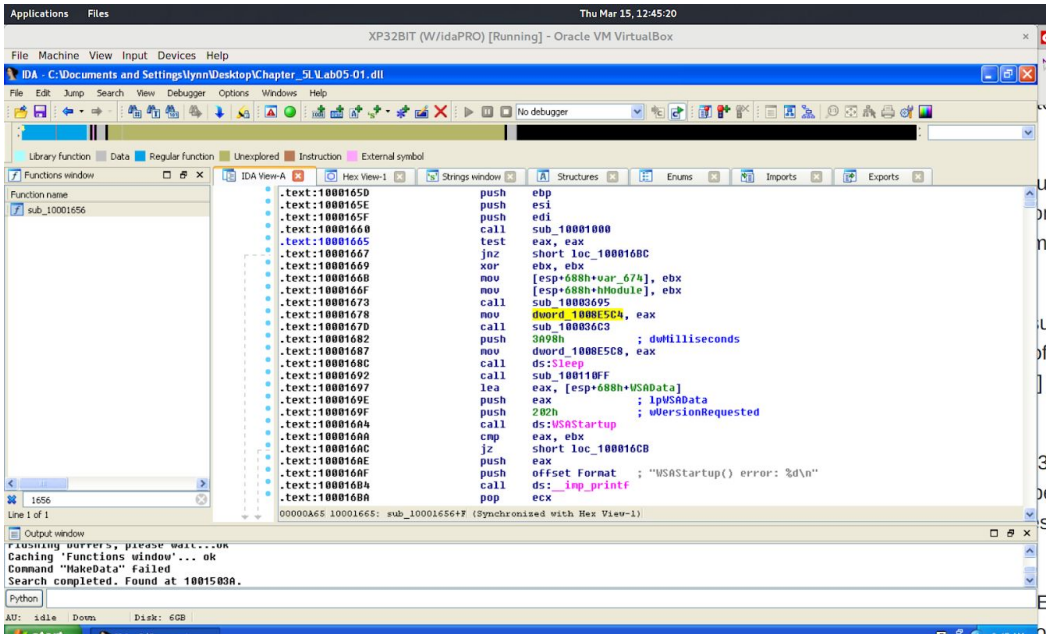
8. It's part of the function calling named GetSystemDirectoryA. In the area of code that references \cmd.exe /c, command.exe or cmd.exe will be executed and display some information such as "Hi, Master" in an interface like a command line. Also it mentioned "Encrypt Magic Number For This Remote Shell Session", which could mean that it's a remote shell launching part. Also follow the control flow we can trace the recv function call, which is related to web socket.

```
xdoors_d:10095B04 65 6E 6D 61 67 69+aEnmagic        db 'enmagic',0          ; DATA XREF: sub_1000FF58+429↑o
xdoors_d:10095B0C 63 64 00          aCd             db 'cd',0               ; DATA XREF: sub_1000FF58+3AA↑o
xdoors_d:10095B0F 00                                align 10h
xdoors_d:10095B10 65 78 69 74 00    aExit           db 'exit',0             ; DATA XREF: sub_1000FF58+38D↑o
xdoors_d:10095B15 00 00 00                          align 4
xdoors_d:10095B18 71 75 69 74 00    aQuit           db 'quit',0             ; DATA XREF: sub_1000FF58+36F↑o
xdoors_d:10095B1D 00 00 00                          align 10h
xdoors_d:10095B20                       ; char aCommand_exeC[]
xdoors_d:10095B20 5C 63 6F 6D 6D 61+aCommand_exeC   db '\command.exe /c ',0 ; DATA XREF: sub_1000FF58:loc_100101D7↑o
xdoors_d:10095B31 00 00 00                          align 4
xdoors_d:10095B34 5C 63 6D 64 2E 65+aCmd_exeC       db '\cmd.exe /c ',0     ; DATA XREF: sub_1000FF58+278↑o
```



9. Check the cross-reference of dword_1008E5C4, shows the capture below. After entering the main function, it calls sub_10001656 first.

```
.text:10001673 E8 1D 20 00 00          call    sub_10003695
.text:10001678 A3 C4 E5 08 10          mov     dword_1008E5C4, eax
```



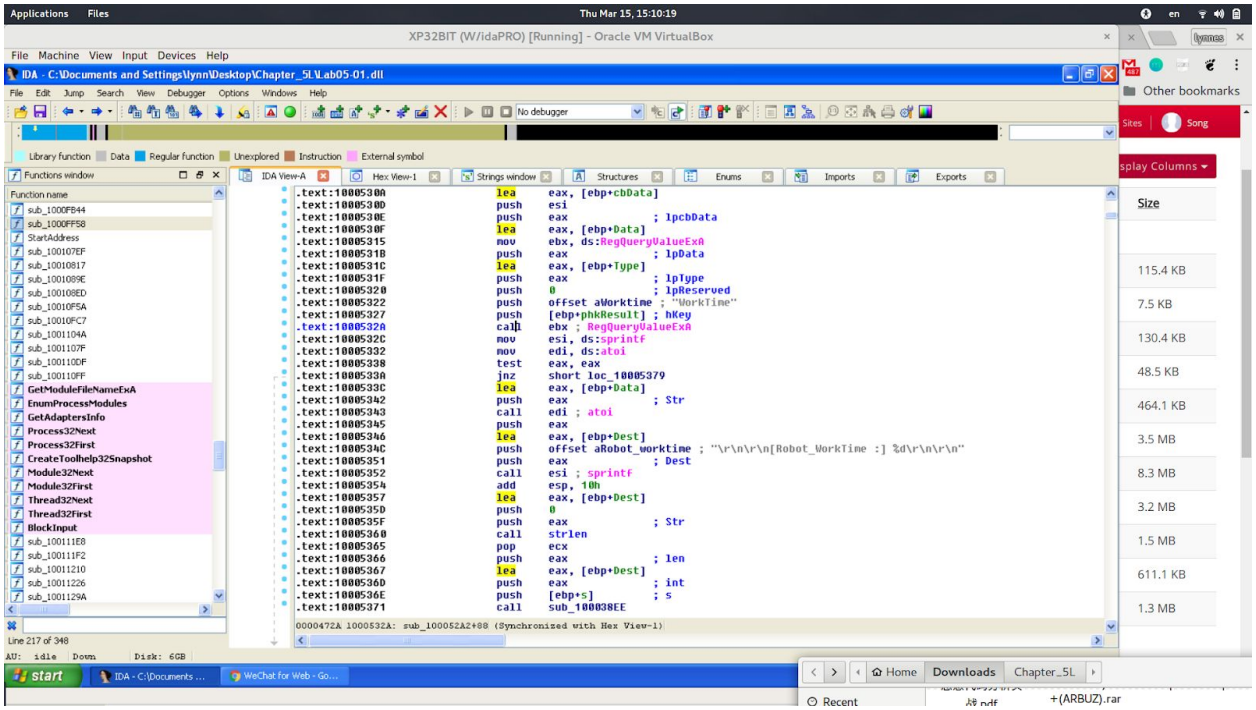
It shows in the capture highlighted in yellow, before calling sub_100036C3. The dword_1008E5C4 itself in the sub_10001656.

We get three calls near dword_1008E5C4, they are sub_10001000, sub_10003965 (before dword) and sub_100036C3 (after dword). Sub_10001000 gets current process id and sub_10003965 runs a function named GetVersionExA to get system version information. This malware would set dword_1008E5C4 to 1 if this is a 64 bit system, which runs rundll64.exe instead of rundll32.exe.

```
1040                lea     eax, [ebp+Str1]
1046                push    offset Str2     ; "rundll32.exe"
104B                push    eax             ; Str1
104C                call    esi ; _stricmp
104E                add     esp, 14h
1051                test    eax, eax
1053                jz      short loc_1000106D
1055                lea     eax, [ebp+Str1]
105B                push    offset aRundll64_exe ; "rundll64.exe"
1060                push    eax             ; Str1
1061                call    esi ; _stricmp
1063                pop     ecx
1064                test    eax, eax
1066                pop     ecx
1067                jz      short loc_1000106D
1069                xor     eax, eax
106B                jmp     short loc_10001070
```

10. In loc_10010444, we get the string “robotwork”, if memcmp is successfully matched, sub_100052A2 will be called. Sub_100052A2 open a path of register key of 'SOFTWARE\Microsoft\Windows\CurrentVersion', and query “WorkTime” as a key saved in

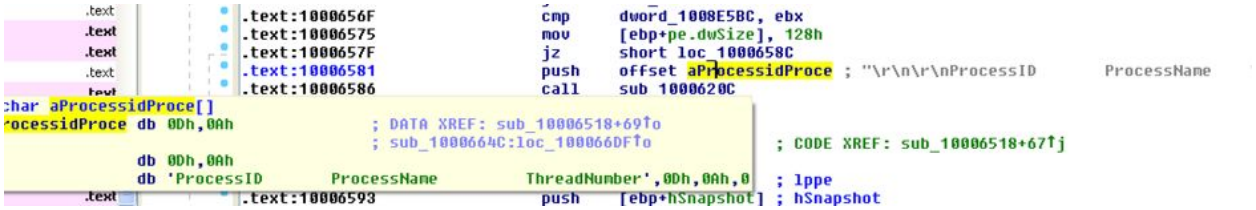
variable ebp. The atoi function change string to integer value. Put ebp to the path named "\r\n\r\n[Robot_WorkTime :] %d\r\n\r\n" and coutinue to sub_100038EE.



11. PSLIST calls sub_100036C3 (function description in question 9) and sub_10006518 which can get process ids and current process snapshot and return a list of them, then write them into xinstall.dll.

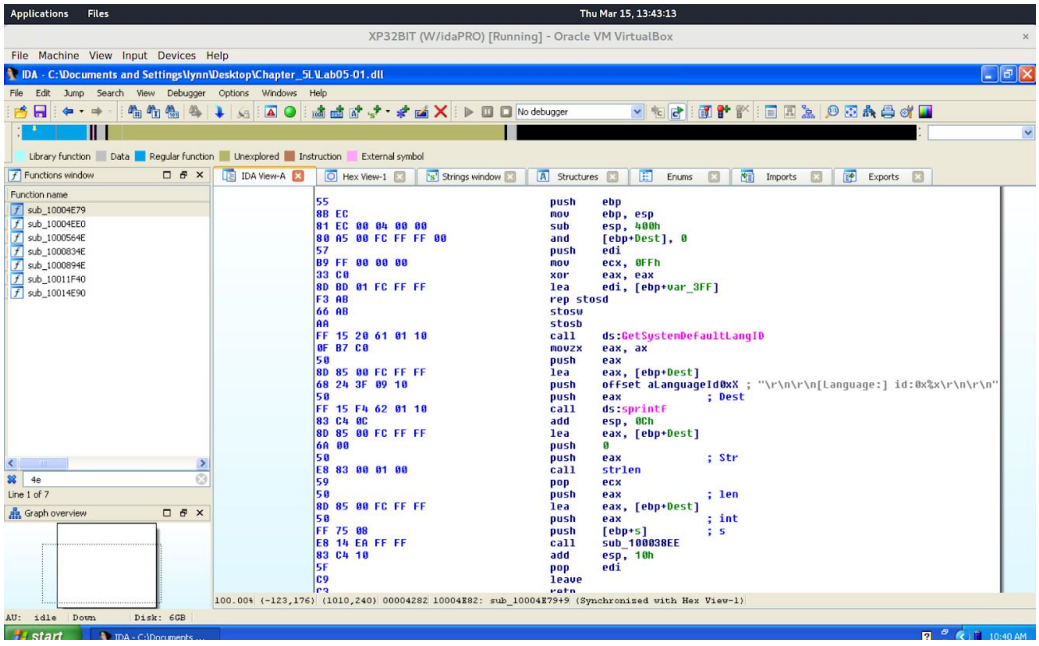
.

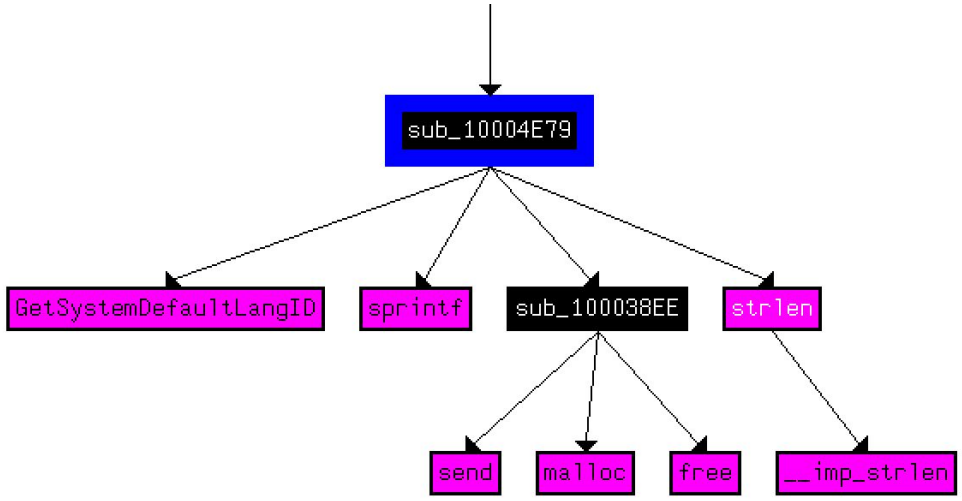
```
push    ebp
mov     ebp, esp
sub     esp, 94h
lea     eax, [ebp+VersionInformation]
mov     [ebp+VersionInformation.dwOSVersionInfoSize], 94h
push    eax             ; lpVersionInformation
call    ds:GetVersionExA
cmp     [ebp+VersionInformation.dwPlatformId], 2
jnz     short loc_100036FA
cmp     [ebp+VersionInformation.dwMajorVersion], 5
jb      short loc_100036FA
push    1
pop     eax
leave
retn
```



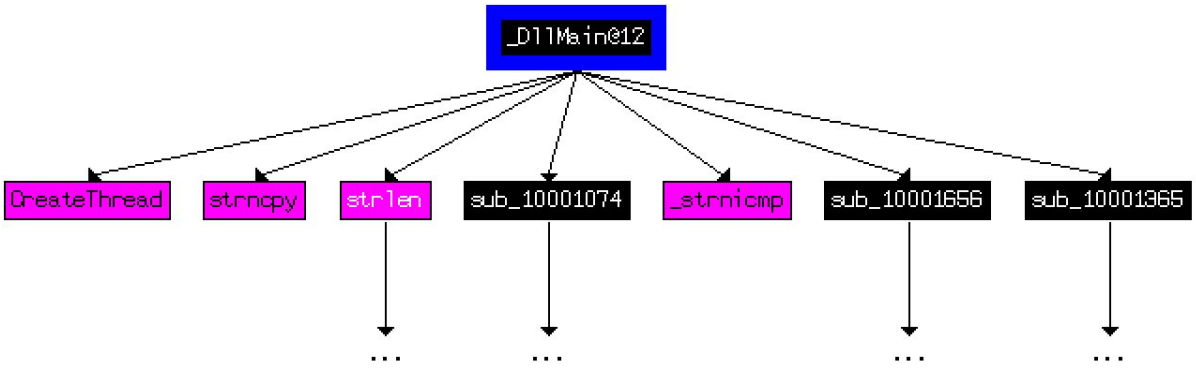
```
.text:10006228                  push    eax             ; DstBuf
.text:10006229                  call    ds:_vsnprintf
.text:1000622F                  push    offset aA       ; "a"
.text:10006234                  push    offset aXinstall_dll ; "xinstall.dll"
.text:10006239                  call    ds:fopen
.text:1000623F                  mov     esi, eax
.text:10006241                  add     esp, 18h
.text:10006244                  test    esi, esi
.text:10006246                  jz      short loc_10006265
.text:10006248                  lea     eax, [ebp+DstBuf]
.text:1000624E                  push    eax
.text:1000624F                  push    offset aS_0     ; "%s\n"
.text:10006254                  push    esi             ; File
.text:10006255                  call    ds:fprintf
```

12. As we have GetSystemDefaultLangID and sprintf, we can just call it GetSystemLang().



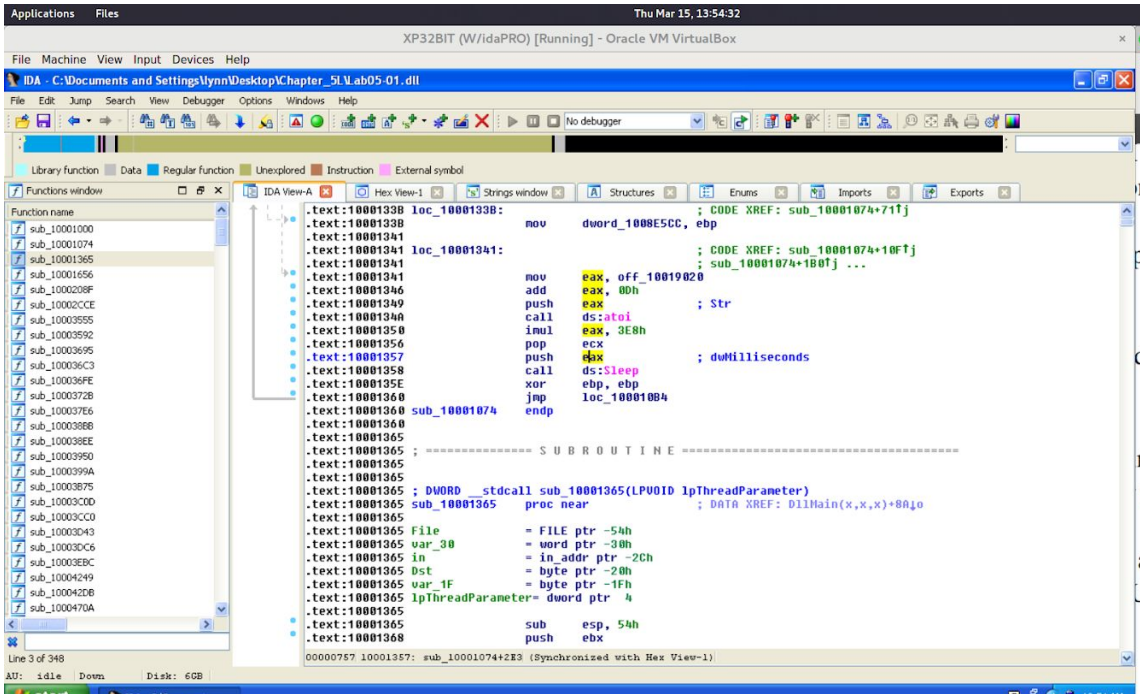


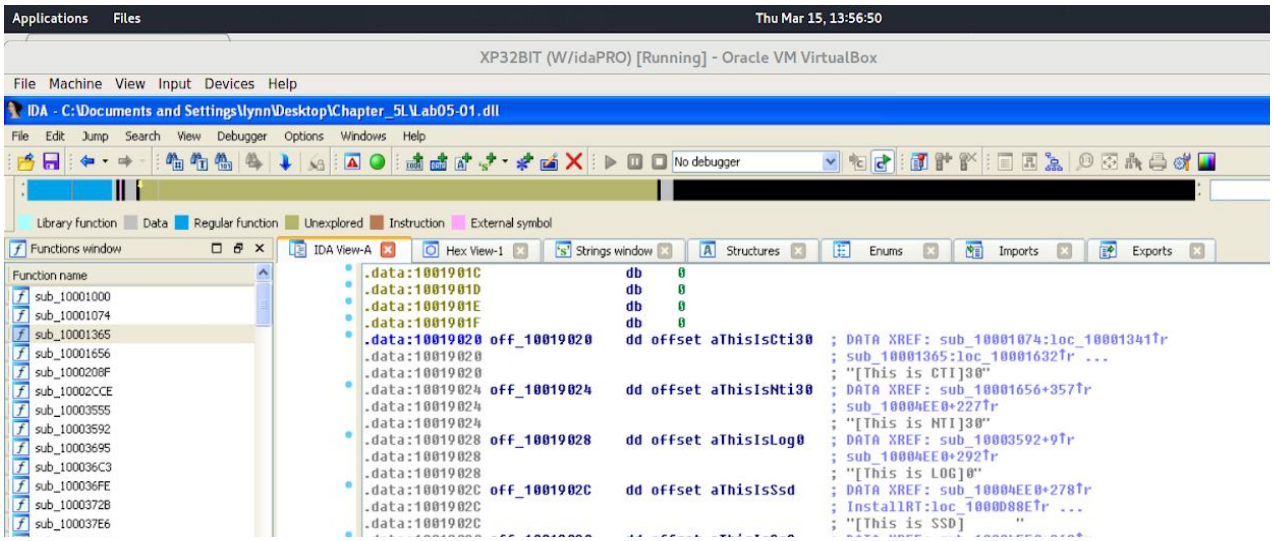
13. Strlen, _strnicmp, strncpy, CreateThread are called directly in DllMain.



Many API functions are called at depth of 2, including WinExec, gethostbyname, memcpy, Sleep, CreateThread etc.

14. Showed in capture, the variable eax is the one who decide how long the system will sleep, so trace back the number off_10019020. It was number 30 multiplied by 1000 that is 30000 ms which is 30 sec.





15. The parameters are 2, 1, 6 (af, type, protocal).

```
.text:100016FB loc_100016FB:                           ; CODE XREF: sub_10001656+374↓j
.text:100016FB                                         ; sub_10001656+A09↓j
.text:100016FB                 push    6               ; protocol
.text:100016FD                 push    1               ; type
.text:100016FF                 push    2               ; af
.text:10001701                 call    ds:socket
.text:10001707                 mov     edi, eax
.text:10001709                 cmp     edi, 0FF
.text:1000170C                 jnz     short loc_10001714
.text:1000170E                 call    ds:WSAGetLastError
.text:10001714                 push    eax
```

```
SOCKET __stdcall socket(int af, int type, int protocol)
                extrn socket:dword      ; CODE XREF: sub_10001656+AB↑p
                                        ; sub_1000208F+3F4↑p ...
```

16. 2: AF_INET, 1: SOCK_STREAM, 6: IPPROTO_TCP

AF_INET 2	SOCK_STREAM 1		IPPROTO_TCP 6

17. In sub_10006196 .text:1000D87A, we found Strings: "Found Virtual Machine,Install Cancel."

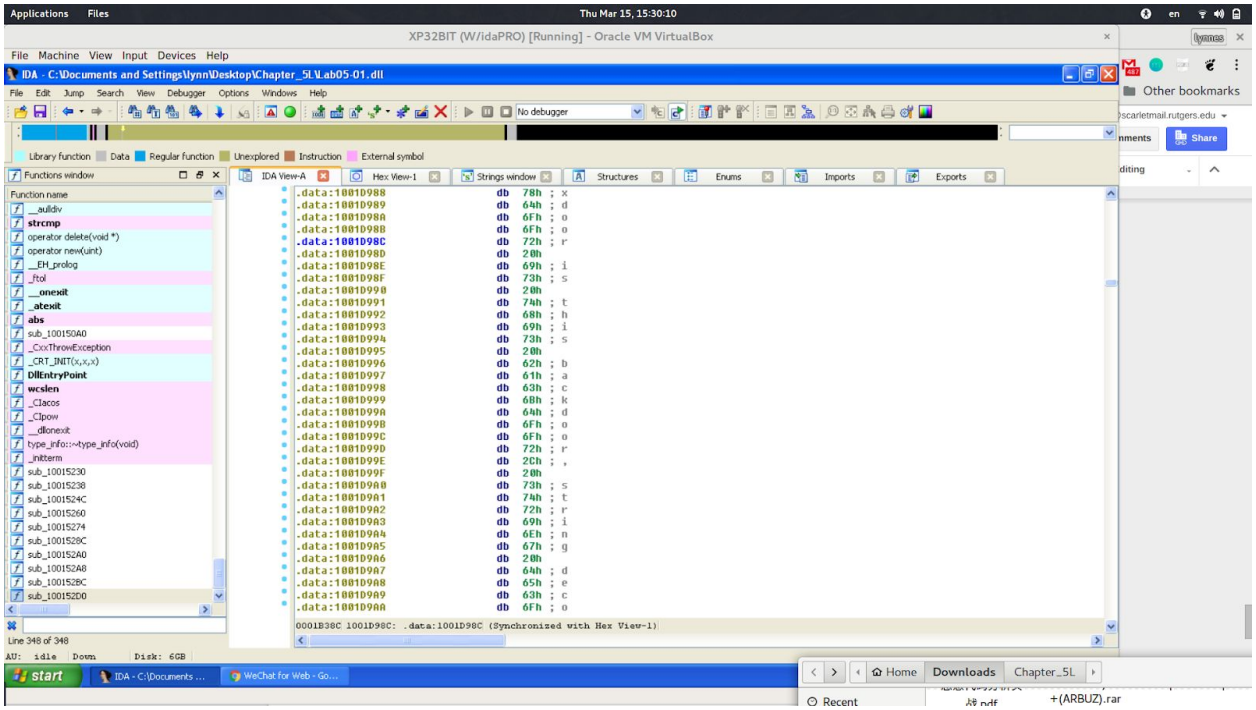
```
.text:100061C4                 push    edx
.text:100061C5                 push    ecx
.text:100061C6                 push    ebx
.text:100061C7                 mov     eax, 564D5868h
.text:100061CC                 mov     ebx, 0
.text:100061D1                 mov     ecx, 0Ah
.text:100061D6                 mov     edx, 5658h
.text:100061DB                 in      eax, dx
.text:100061DC                 cmp     ebx, 564D5868h
.text:100061E2                 setz    [ebp+var_1C]
.text:100061E6                 pop     ebx
.text:100061E7                 pop     ecx
.text:100061E8                 pop     edx
.text:100061E9                 jmp     short loc_100061F6
```

```
0D870 loc_1000D870:                    ; CODE XREF: InstallRT+1E↑j
0D870                 push    offset unk_1008E5F0 ; Format
0D875                 call    sub_10003592
0D87A                 mov     [esp+8+Format], offset aFoundVirtualMa ; "Found Virtual Machine,Install Cancel."
0D881                 call    sub_10003592
```

18. Seems like a sequence of encrypted characters, or can be arguments for some certain commands.

```
.data:1001D987                 db    0
.data:1001D988                 db  2Dh ; -
.data:1001D989                 db  31h ; 1
.data:1001D98A                 db  3Ah ; :
.data:1001D98B                 db  3Ah ; :
.data:1001D98C                 db  27h ; '
.data:1001D98D                 db  75h ; u
.data:1001D98E                 db  3Ch ; <
.data:1001D98F                 db  26h ; &
.data:1001D990                 db  75h ; u
.data:1001D991                 db  21h ; !
.data:1001D992                 db  3Dh ; =
.data:1001D993                 db  3Ch ; <
.data:1001D994                 db  26h ; &
.data:1001D995                 db  75h ; u
.data:1001D996                 db  37h ; 7
.data:1001D997                 db  34h ; 4
.data:1001D998                 db  36h ; 6
.data:1001D999                 db  3Eh ; >
.data:1001D99A                 db  31h ; 1
.data:1001D99B                 db  3Ah ; :
```

19. Result shows below. Character become readable, they are: xdoor is this backdoor, string decoded for Practical Malware Analysis Lab :)1234



20. Press A at 1001D988 or right click and select the strings option, which is set to be ASCII by default.

21. The script includes codes below.

```
# python code begin
sea = ScreenEA()

for i in range(0x00,0x50):
        b = Byte(sea+i)
        decoded_byte = b ^ 0x55
        PatchByte(sea+i,decoded_byte)
#python code end
```

The program does XOR operator with 0x55 for every byte from sea+0x00 to sea+0x50. And call PatchByte which should be a function that can change the original data.