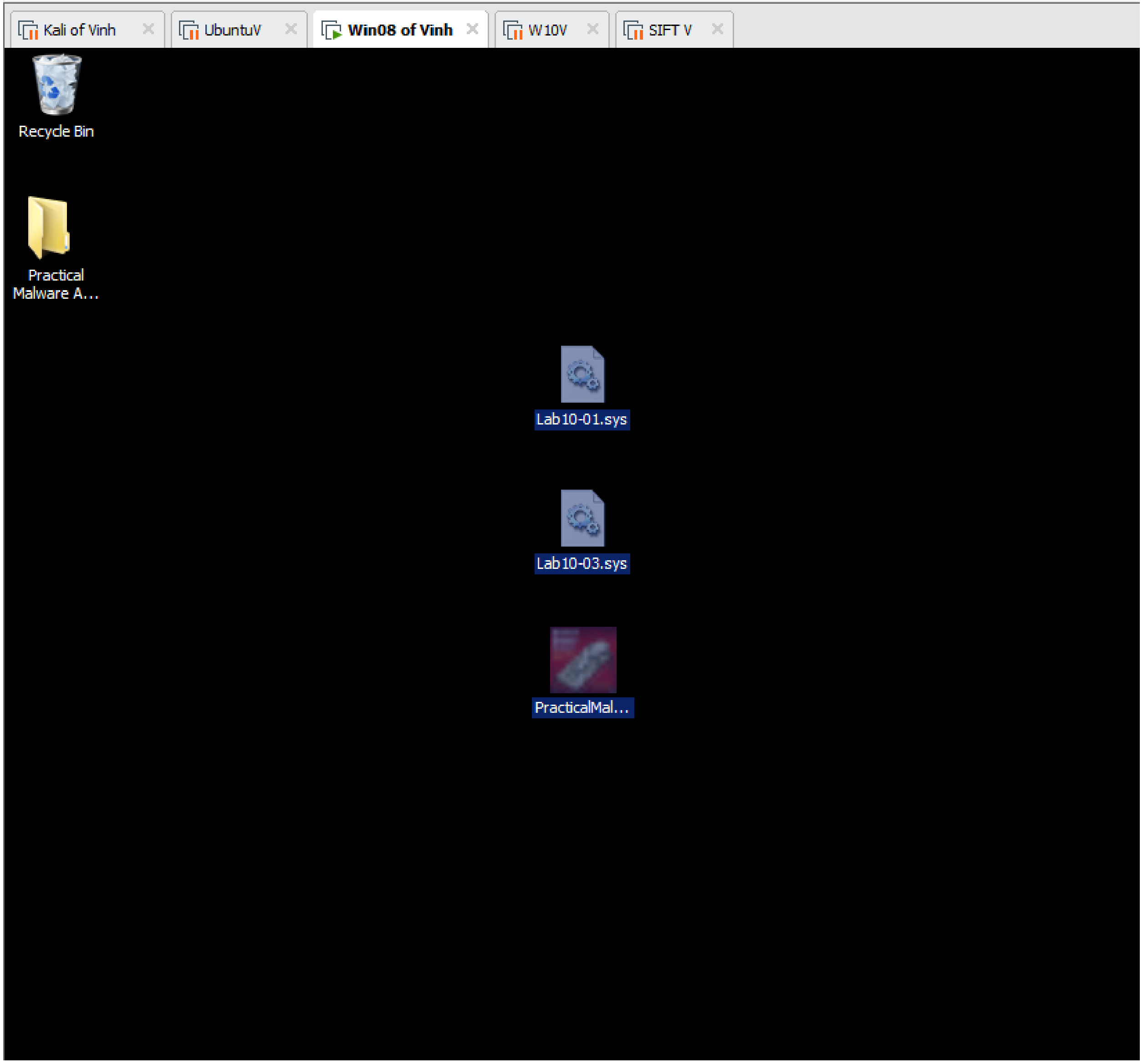
LAB 8: IDA Pro

Course Name: Malware Analysis and Reverse Engineering (IAM302)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 15/2/2023

Purpose

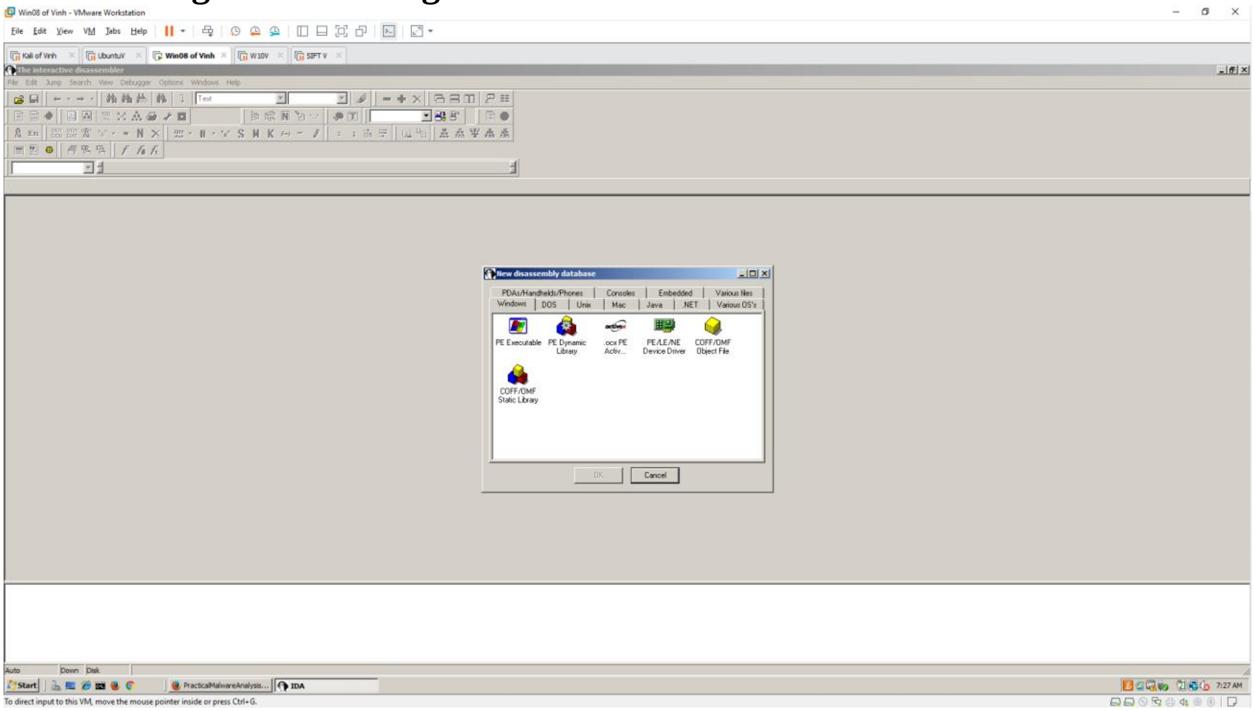
- You will practice using IDA Pro.
- You should already have the lab files



What you need:

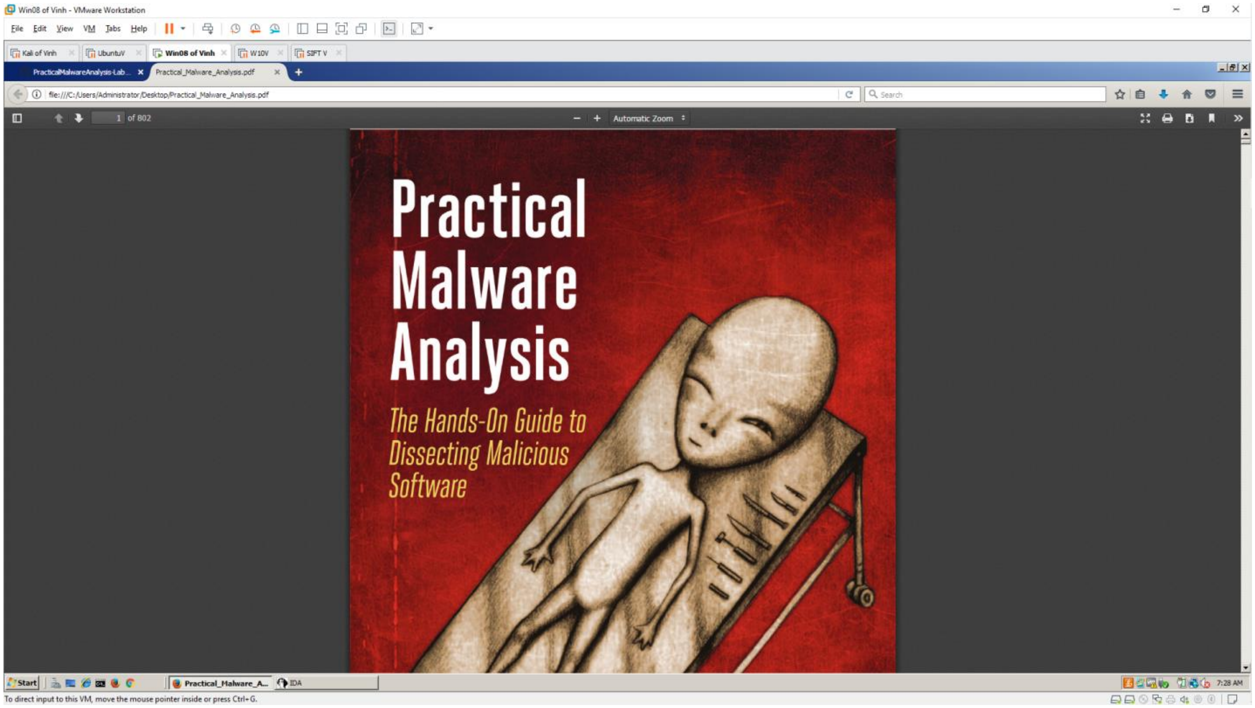
- A Windows machine, real or virtual, such as the Windows 2008 Server VM we've been using
- The textbook: "Practical Malware Analysis"

Downloading and Installing IDA Pro



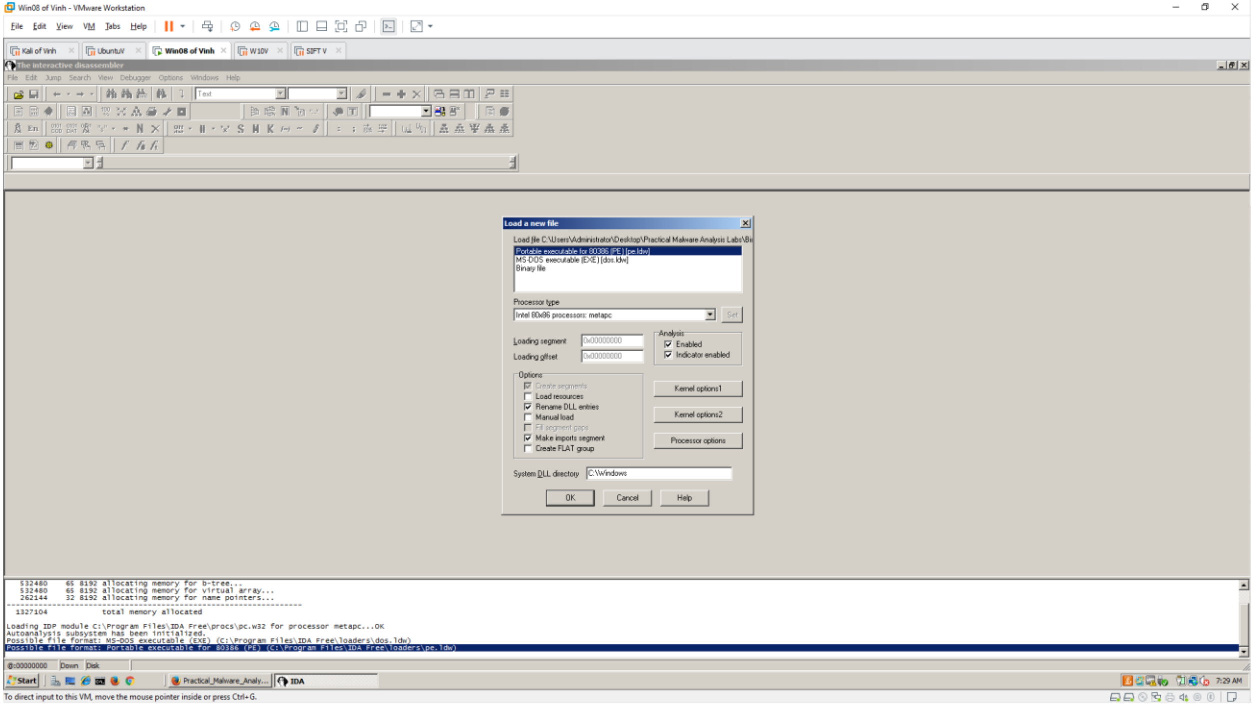
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Follow the Textbook


Win08 of Vinh - VMware Workstation
File Edit View VM Tabs Help
Kali of Vinh
UbuntuV
Win08 of Vinh
W10V
SIFT V
PracticalMalwareAnalysis-Lab...
Practical_Malware_Analysis.pdf
file:///C:/Users/Administrator/Desktop/Practical_Malware_Analysis.pdf
Search
1 of 802
Automatic Zoom
Practical
Malware
Analysis
The Hands-On Guide to
Dissecting Malicious
Software
Start
Practical_Malware_A...
IDA
7:28 AM

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Opening Lab05-01.dll in IDA Pro



Win08 of Vinh - VMware Workstation
File Edit View VM Tabs Help
Kali of Vinh
UbuntuV
Win08 of Vinh
W10V
SIFT V
The interactive disassembler
File Edit Jump Search View Debugger Options Windows Help

Load a new file

Load file C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\Bi

Portable executable for 80386 (PE) [pe.ldw]
MS-DOS executable (EXE) [dos.ldw]
Binary file

Processor type: Intel 80x86 processors: metapc

Loading segment: 0x00000000
Loading offset: 0x00000000

Analysis
☑ Enabled
☑ Indicator enabled

Options
☑ Create segments
□ Load resources
☑ Rename DLL entries
□ Manual load
□ Fill segment gaps
☑ Make imports segment
□ Create FLAT group

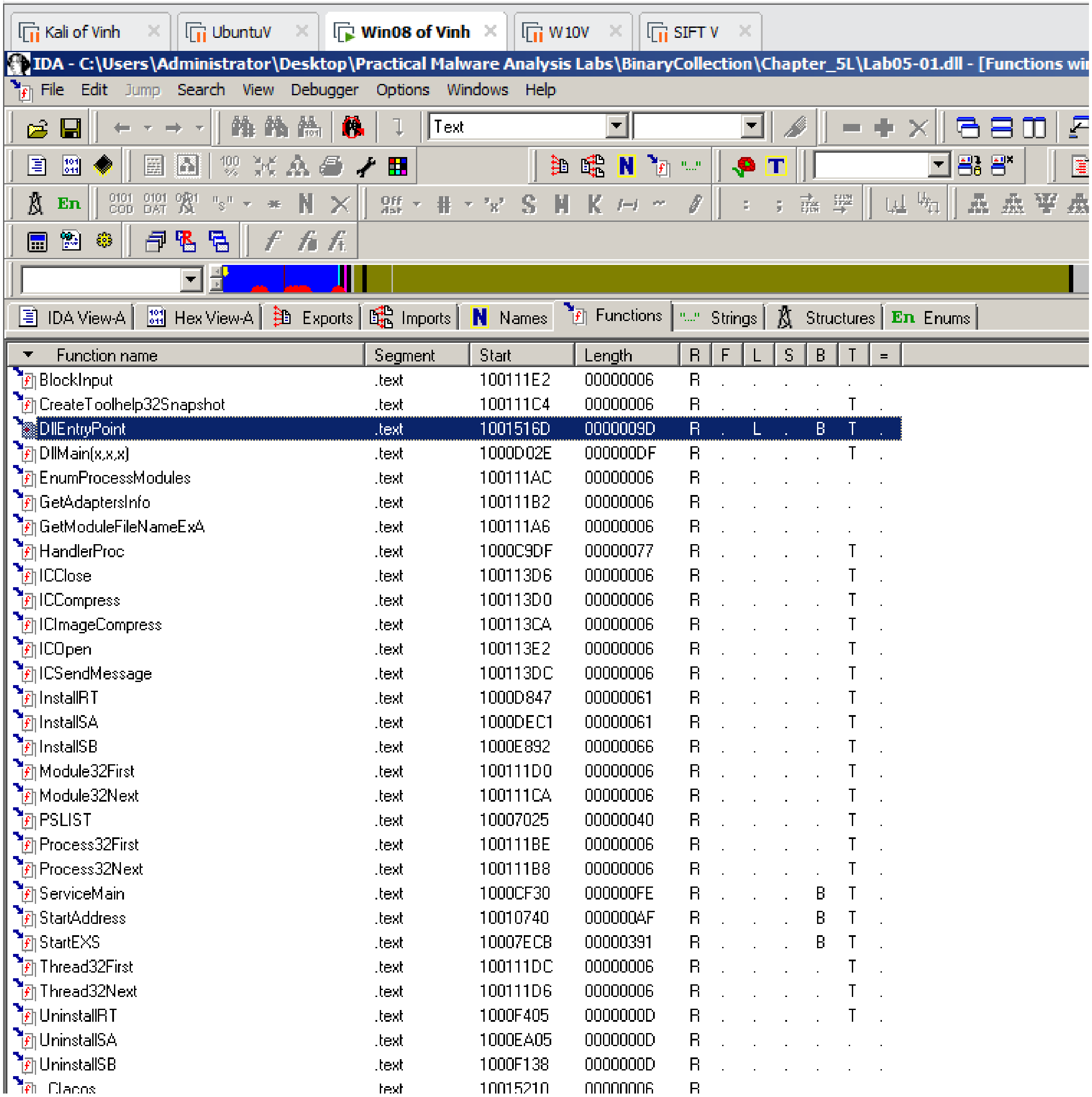
System DLL directory: C:\Windows

```
   532480    65 8192 allocating memory for b-tree...
   532480    65 8192 allocating memory for virtual array...
   262144    32 8192 allocating memory for name pointers...
-----------------------------------------------------------------
  1327104            total memory allocated

Loading IDP module C:\Program Files\IDA Free\procs\pc.w32 for processor metapc...OK
Autoanalysis subsystem has been initialized.
Possible file format: MS-DOS executable (EXE) (C:\Program Files\IDA Free\loaders\dos.ldw)
Possible file format: Portable executable for 80386 (PE) (C:\Program Files\IDA Free\loaders\pe.ldw)
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

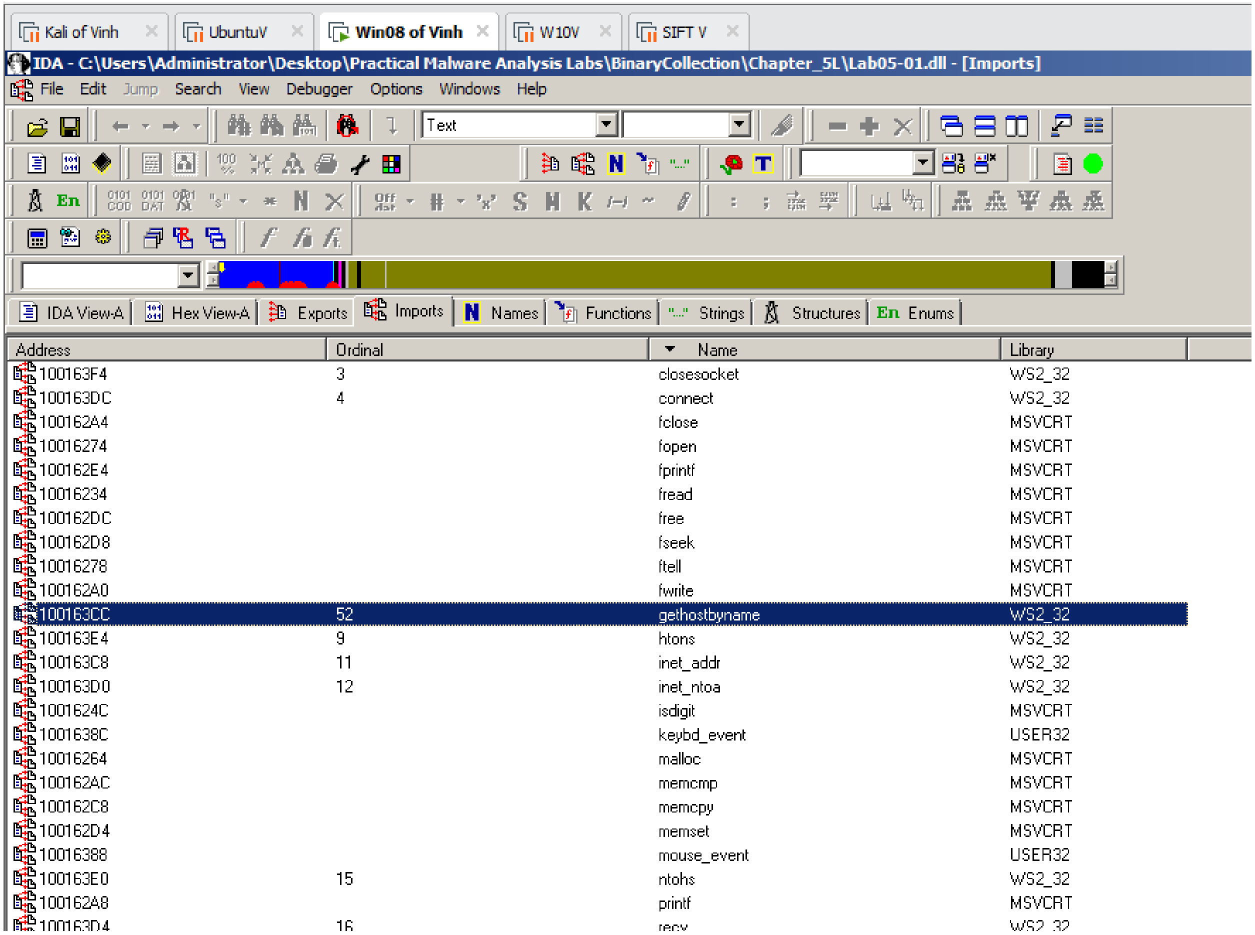
Q1: Finding the Address of DLL Main



IDA - C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_5L\Lab05-01.dll - [Functions wi

Function name	Segment	Start	Length	R	F	L	S	B	T	=
BlockInput	.text	100111E2	00000006	R	.	.	.	.	.	.
CreateToolhelp32Snapshot	.text	100111C4	00000006	R	.	.	.	.	T	.
DllEntryPoint	.text	1001516D	0000009D	R	.	L	.	B	T	.
DllMain(x,x,x)	.text	1000D02E	000000DF	R	.	.	.	.	T	.
EnumProcessModules	.text	100111AC	00000006	R	.	.	.	.	.	.
GetAdaptersInfo	.text	100111B2	00000006	R	.	.	.	.	.	.
GetModuleFileNameExA	.text	100111A6	00000006	R	.	.	.	.	.	.
HandlerProc	.text	1000C9DF	00000077	R	.	.	.	.	T	.
ICClose	.text	100113D6	00000006	R	.	.	.	.	T	.
ICCompress	.text	100113D0	00000006	R	.	.	.	.	T	.
ICImageCompress	.text	100113CA	00000006	R	.	.	.	.	T	.
ICOpen	.text	100113E2	00000006	R	.	.	.	.	T	.
ICSendMessage	.text	100113DC	00000006	R	.	.	.	.	T	.
InstallRT	.text	1000D847	00000061	R	.	.	.	.	T	.
InstallSA	.text	1000DEC1	00000061	R	.	.	.	.	T	.
InstallSB	.text	1000E892	00000066	R	.	.	.	.	T	.
Module32First	.text	100111D0	00000006	R	.	.	.	.	T	.
Module32Next	.text	100111CA	00000006	R	.	.	.	.	T	.
PSLIST	.text	10007025	00000040	R	.	.	.	.	T	.
Process32First	.text	100111BE	00000006	R	.	.	.	.	T	.
Process32Next	.text	100111B8	00000006	R	.	.	.	.	T	.
ServiceMain	.text	1000CF30	000000FE	R	.	.	.	B	T	.
StartAddress	.text	10010740	000000AF	R	.	.	.	B	T	.
StartEXS	.text	10007ECB	00000391	R	.	.	.	B	T	.
Thread32First	.text	100111DC	00000006	R	.	.	.	.	T	.
Thread32Next	.text	100111D6	00000006	R	.	.	.	.	T	.
UninstallRT	.text	1000F405	0000000D	R	.	.	.	.	T	.
UninstallSA	.text	1000EA05	0000000D	R	.	.	.	.	.	.
UninstallSB	.text	1000F138	0000000D	R	.	.	.	.	.	.
_CIacos	.text	10015210	00000006	R						

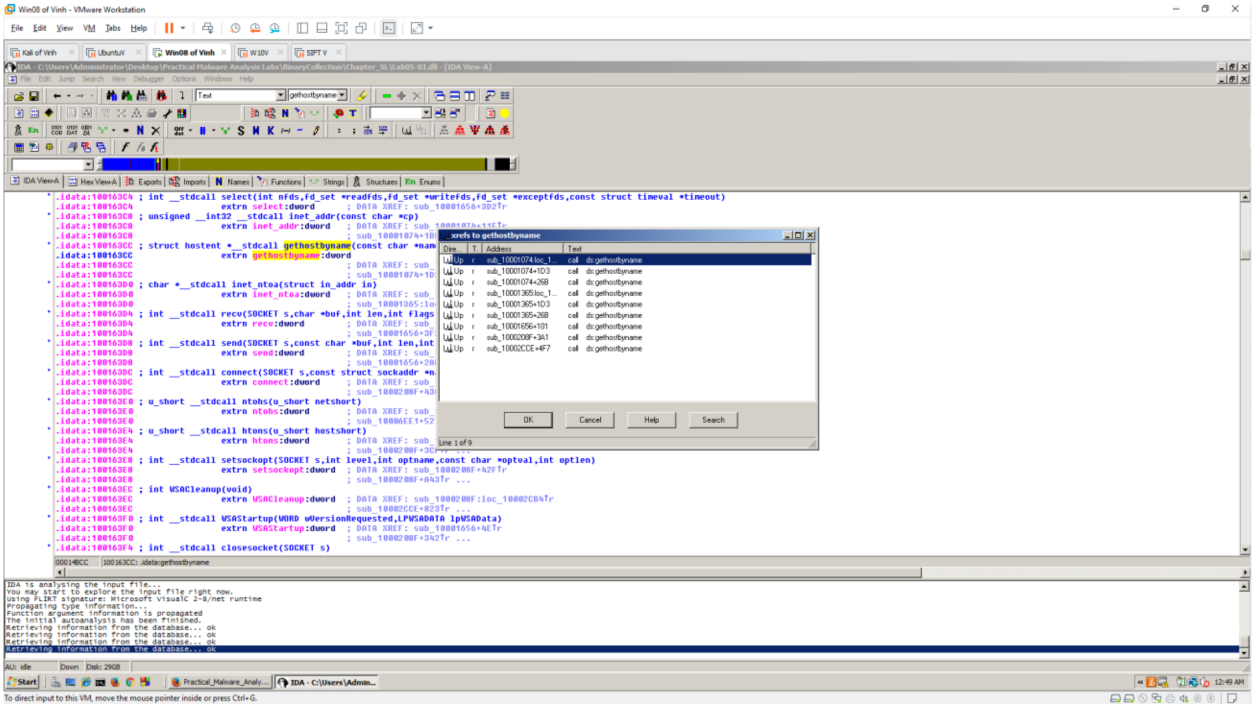
Q2: Find the import for gethostbyname


Kali of Vinh
UbuntuV
Win08 of Vinh
W10V
SIFT V
IDA - C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_5L\Lab05-01.dll - [Imports]
File Edit Jump Search View Debugger Options Windows Help
Text
IDA View-A
Hex View-A
Exports
Imports
Names
Functions
Strings
Structures
Enums

Address	Ordinal	Name	Library
100163F4	3	closesocket	WS2_32
100163DC	4	connect	WS2_32
100162A4		fclose	MSVCRT
10016274		fopen	MSVCRT
100162E4		fprintf	MSVCRT
10016234		fread	MSVCRT
100162DC		free	MSVCRT
100162D8		fseek	MSVCRT
10016278		ftell	MSVCRT
100162A0		fwrite	MSVCRT
100163CC	52	gethostbyname	WS2_32
100163E4	9	htons	WS2_32
100163C8	11	inet_addr	WS2_32
100163D0	12	inet_ntoa	WS2_32
1001624C		isdigit	MSVCRT
1001638C		keybd_event	USER32
10016264		malloc	MSVCRT
100162AC		memcmp	MSVCRT
100162C8		memcpy	MSVCRT
100162D4		memset	MSVCRT
10016388		mouse_event	USER32
100163E0	15	ntohs	WS2_32
100162A8		printf	MSVCRT
100163D4	16	recv	WS2_32

Q3: How many functions call gethostbyname?

- 9


Win08 of Vinh - VMware Workstation
File Edit View VM Tabs Help
Kali of Vinh
UbuntuV
Win08 of Vinh
W10V
SIFT V
IDA - C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_5L\Lab05-01.dll - [IDA View-A]
File Edit Jump Search View Debugger Options Windows Help
Text
gethostbyname
IDA View-A
Hex View-A
Exports
Imports
Names
Functions
Strings
Structures
Enums
xrefs to gethostbyname
OK
Cancel
Help
Search
Start
Practical_Malware_Analy...
IDA - C:\Users\Admin...
12:49 AM

```
.idata:100163C4 ; int __stdcall select(int nfds,fd_set *readfds,fd_set *writefds,fd_set *exceptfds,const struct timeval *timeout)
.idata:100163C4                 extrn select:dword      ; DATA XREF: sub_10001656+3D2↑r
.idata:100163C8 ; unsigned __int32 __stdcall inet_addr(const char *cp)
.idata:100163C8                 extrn inet_addr:dword   ; DATA XREF: sub_10001074+11F↑r
.idata:100163C8                                         ; sub_10001074+1B
.idata:100163CC ; struct hostent *__stdcall gethostbyname(const char *nam
.idata:100163CC                 extrn gethostbyname:dword
.idata:100163CC                                         ; DATA XREF: sub_
.idata:100163CC                                         ; sub_10001074+1D
.idata:100163D0 ; char *__stdcall inet_ntoa(struct in_addr in)
.idata:100163D0                 extrn inet_ntoa:dword   ; DATA XREF: sub_
.idata:100163D0                                         ; sub_10001365:lo
.idata:100163D4 ; int __stdcall recv(SOCKET s,char *buf,int len,int flags
.idata:100163D4                 extrn recv:dword        ; DATA XREF: sub_
.idata:100163D4                                         ; sub_10001656+3F
.idata:100163D8 ; int __stdcall send(SOCKET s,const char *buf,int len,int
.idata:100163D8                 extrn send:dword        ; DATA XREF: sub_
.idata:100163D8                                         ; sub_10001656+2A
.idata:100163DC ; int __stdcall connect(SOCKET s,const struct sockaddr *n
.idata:100163DC                 extrn connect:dword     ; DATA XREF: sub_
.idata:100163DC                                         ; sub_1000208F+43
.idata:100163E0 ; u_short __stdcall ntohs(u_short netshort)
.idata:100163E0                 extrn ntohs:dword       ; DATA XREF: sub_
.idata:100163E0                                         ; sub_10006EE1+52
.idata:100163E4 ; u_short __stdcall htons(u_short hostshort)
.idata:100163E4                 extrn htons:dword       ; DATA XREF: sub_
.idata:100163E4                                         ; sub_1000208F+3C
.idata:100163E8 ; int __stdcall setsockopt(SOCKET s,int level,int optname,const char *optval,int optlen)
.idata:100163E8                 extrn setsockopt:dword  ; DATA XREF: sub_1000208F+42F↑r
.idata:100163E8                                         ; sub_1000208F+A43↑r ...
.idata:100163EC ; int WSACleanup(void)
.idata:100163EC                 extrn WSACleanup:dword  ; DATA XREF: sub_1000208F:loc_10002CB4↑r
.idata:100163EC                                         ; sub_10002CCE+823↑r ...
.idata:100163F0 ; int __stdcall WSAStartup(WORD wVersionRequested,LPWSADATA lpWSAData)
.idata:100163F0                 extrn WSAStartup:dword  ; DATA XREF: sub_10001656+4E↑r
.idata:100163F0                                         ; sub_1000208F+342↑r ...
.idata:100163F4 ; int __stdcall closesocket(SOCKET s)
```

Dire...	T.	Address	Text
Up	r	sub_10001074:loc_1...	call ds:gethostbyname
Up	r	sub_10001074+1D3	call ds:gethostbyname
Up	r	sub_10001074+26B	call ds:gethostbyname
Up	r	sub_10001365:loc_1...	call ds:gethostbyname
Up	r	sub_10001365+1D3	call ds:gethostbyname
Up	r	sub_10001365+26B	call ds:gethostbyname
Up	r	sub_10001656+101	call ds:gethostbyname
Up	r	sub_1000208F+3A1	call ds:gethostbyname
Up	r	sub_10002CCE+4F7	call ds:gethostbyname

Line 1 of 9

00014BCC 100163CC: .idata:gethostbyname

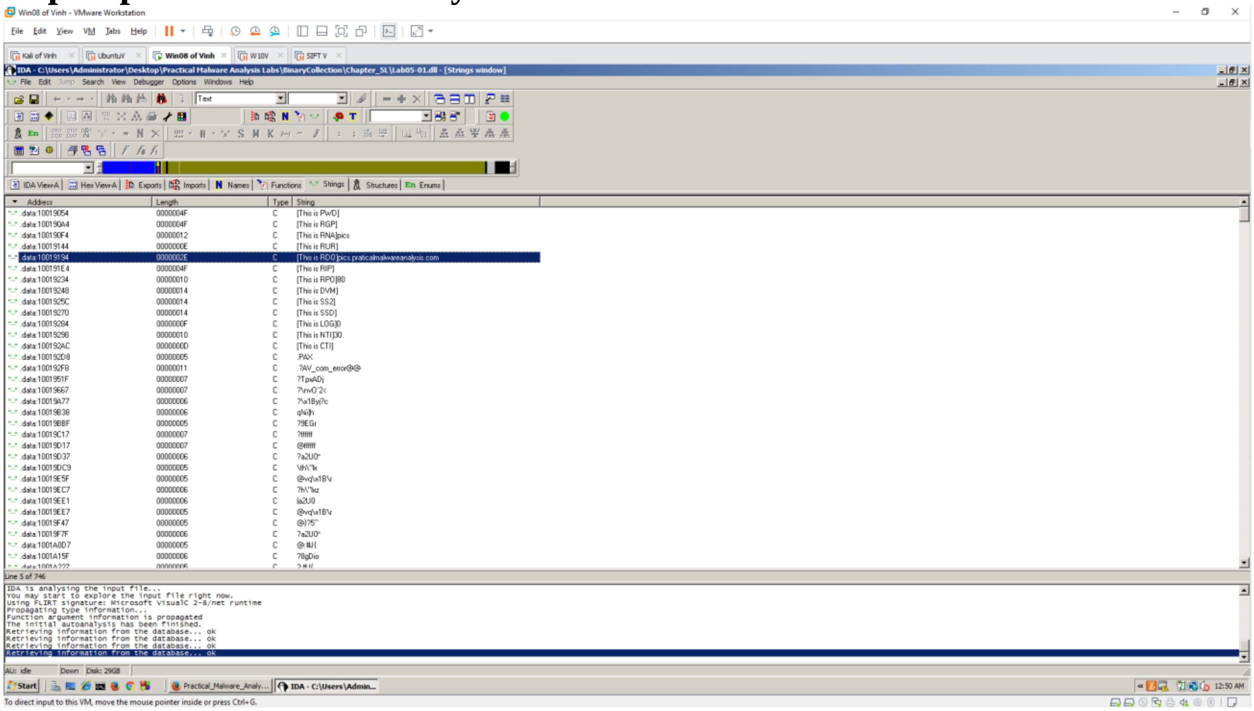
```
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: Microsoft VisualC 2-8/net runtime
Propagating type information...
Function argument information is propagated
The initial autoanalysis has been finished.
Retrieving information from the database... ok
Retrieving information from the database... ok
Retrieving information from the database... ok
Retrieving information from the database... ok
```

AU: idle Down Disk: 29GB

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Q4. Focusing on the call to gethostbyname located at 0x10001757, can you figure out which DNS request will be made?

- pics.praticalmalwareanalysis.com


Win08 of Vinh - VMware Workstation
File Edit View VM Tabs Help
Kali of Vinh
UbuntuV
Win08 of Vinh
W10V
SIFT V
IDA - C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_5L\Lab05-01.dll - [Strings window]
File Edit Jump Search View Debugger Options Windows Help
Text
IDA View-A
Hex View-A
Exports
Imports
Names
Functions
Strings
Structures
Enums
Start
Practical_Malware_Analy...
IDA - C:\Users\Admin...
12:50 AM

Address	Length	Type	String
.data:10019054	0000004F	C	[This is PWD]
.data:100190A4	0000004F	C	[This is RGP]
.data:100190F4	00000012	C	[This is RNA]pics
.data:10019144	0000000E	C	[This is RUR]
.data:10019194	0000002E	C	[This is RDO]pics.praticalmalwareanalysis.com
.data:100191E4	0000004F	C	[This is RIP]
.data:10019234	00000010	C	[This is RPO]80
.data:10019248	00000014	C	[This is DVM]
.data:1001925C	00000014	C	[This is SS2]
.data:10019270	00000014	C	[This is SSD]
.data:10019284	0000000F	C	[This is LOG]0
.data:10019298	00000010	C	[This is NTI]30
.data:100192AC	0000000D	C	[This is CTI]
.data:100192D8	00000005	C	.PAX
.data:100192F8	00000011	C	.?AV_com_error@@
.data:1001951F	00000007	C	?TpxADj
.data:10019667	00000007	C	?\vwO'2<
.data:10019A77	00000006	C	?\x1Byj?c
.data:10019B38	00000006	C	q%i}h
.data:10019BBF	00000005	C	?9EGr
.data:10019C17	00000007	C	?ffffff
.data:10019D17	00000007	C	@ffffff
.data:10019D37	00000006	C	?a2U0"
.data:10019DC9	00000005	C	\th\"lx
.data:10019E5F	00000005	C	@vq\x1B\r
.data:10019EC7	00000006	C	?h\"lxz
.data:10019EE1	00000006	C	la2U0
.data:10019EE7	00000005	C	@vq\x1B\r
.data:10019F47	00000005	C	@)?5^
.data:10019F7F	00000006	C	?a2U0^
.data:1001A0D7	00000005	C	@:#J{
.data:1001A15F	00000006	C	?8gDio
.data:1001A227	00000005	C	?:#J(

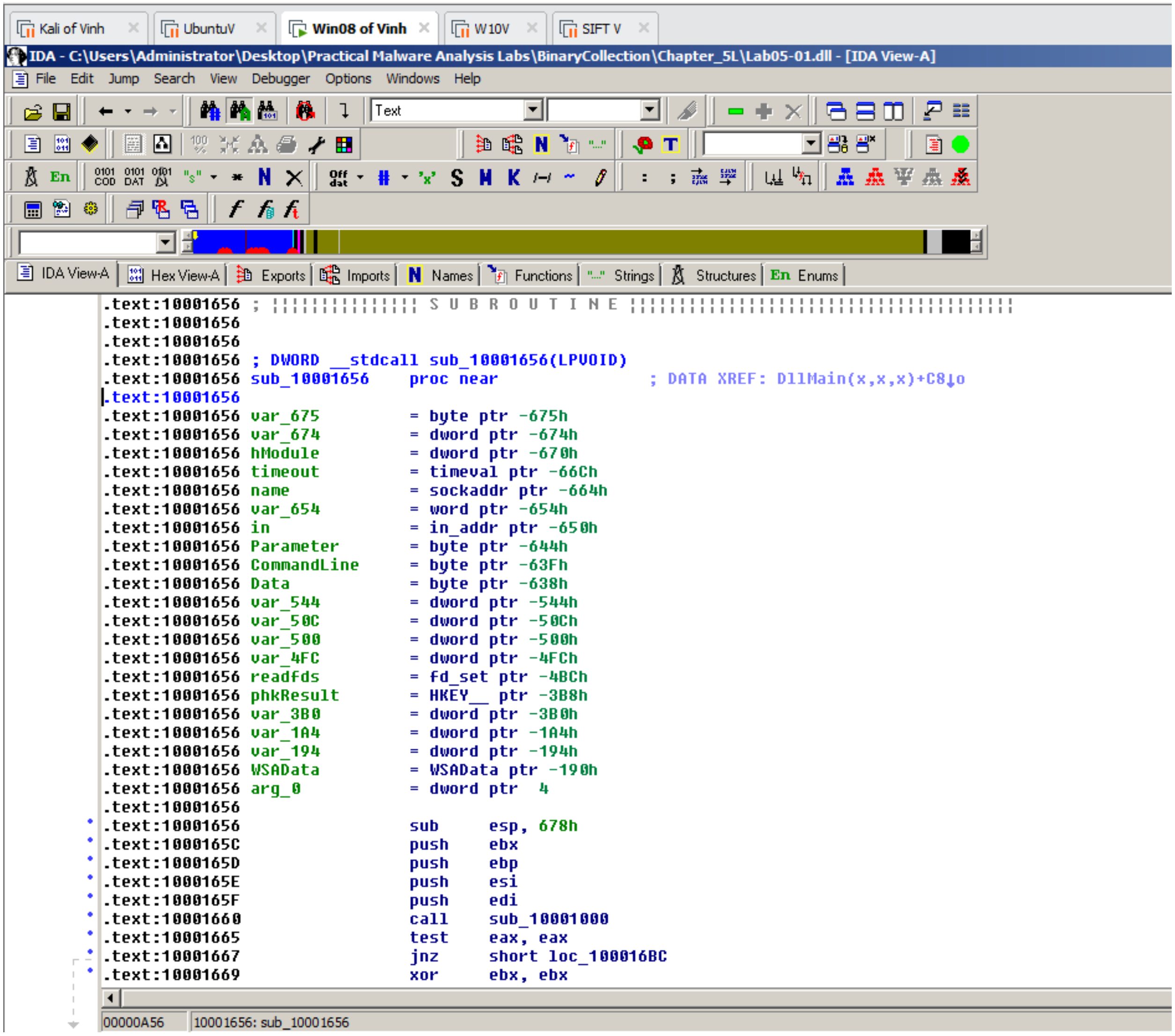
Line 5 of 746

```
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.
Retrieving information from the database... ok
Retrieving information from the database... ok
Retrieving information from the database... ok
Retrieving information from the database... ok
```

AU: idle Down Disk: 29GB

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

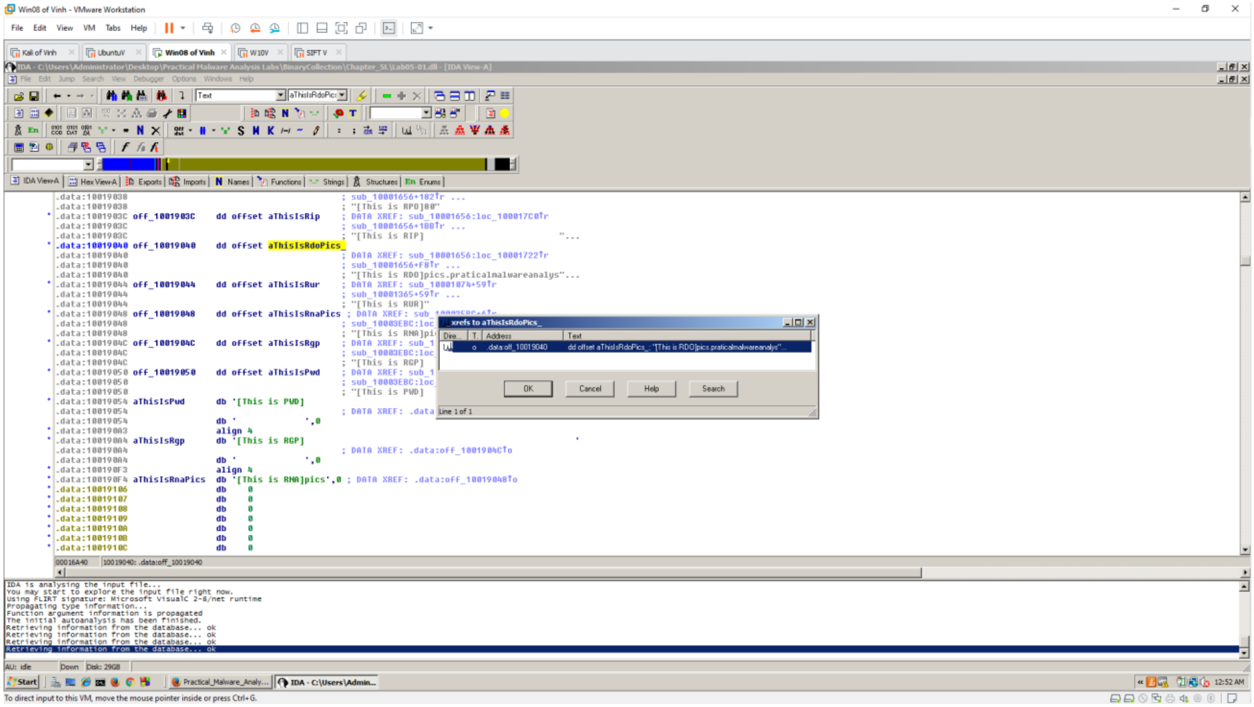
Q5: Count Local Variables for the Subroutine at 0x10001656


Kali of Vinh
UbuntuV
Win08 of Vinh
W10V
SIFT V
IDA - C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_5L\Lab05-01.dll - [IDA View-A]
File Edit Jump Search View Debugger Options Windows Help
Text
IDA View-A
Hex View-A
Exports
Imports
Names
Functions
Strings
Structures
Enums
00000A56
10001656: sub_10001656

```
.text:10001656 ; ¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦ S U B R O U T I N E ¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦
.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 hModule         = dword ptr -670h
.text:10001656 timeout         = timeval ptr -66Ch
.text:10001656 name            = sockaddr ptr -664h
.text:10001656 var_654         = word ptr -654h
.text:10001656 in              = in_addr ptr -650h
.text:10001656 Parameter       = byte ptr -644h
.text:10001656 CommandLine     = byte ptr -63Fh
.text:10001656 Data            = byte ptr -638h
.text:10001656 var_544         = dword ptr -544h
.text:10001656 var_50C         = dword ptr -50Ch
.text:10001656 var_500         = dword ptr -500h
.text:10001656 var_4FC         = dword ptr -4FCh
.text:10001656 readfds         = fd_set ptr -4BCh
.text:10001656 phkResult       = HKEY__ 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
.text:10001656
.text:10001656                 sub     esp, 678h
.text:1000165C                 push    ebx
.text:1000165D                 push    ebp
.text:1000165E                 push    esi
.text:1000165F                 push    edi
.text:10001660                 call    sub_10001000
.text:10001665                 test    eax, eax
.text:10001667                 jnz     short loc_100016BC
.text:10001669                 xor     ebx, ebx
```

Q6: How many parameters has IDA Pro recognized for the subroutine at 0x10001656?

- 1



IDA - C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_5L\Lab05-01.dll - [IDA View-A]

```
.data:10019038                                  ; sub_10001656+182↑r ...
.data:10019038                                  ; "[This is RPO]80"
.data:1001903C off_1001903C    dd offset aThisIsRip     ; DATA XREF: sub_10001656:loc_100017C0↑r
.data:1001903C                                  ; sub_10001656+1BB↑r ...
.data:1001903C                                  ; "[This is RIP]                    "...
.data:10019040 off_10019040    dd offset aThisIsRdoPics_
.data:10019040                                  ; DATA XREF: sub_10001656:loc_10001722↑r
.data:10019040                                  ; sub_10001656+F8↑r ...
.data:10019040                                  ; "[This is RDO]pics.praticalmalwareanalys"...
.data:10019044 off_10019044    dd offset aThisIsRur     ; DATA XREF: sub_10001074+59↑r
.data:10019044                                  ; sub_10001365+59↑r ...
.data:10019044                                  ; "[This is RUR]"
.data:10019048 off_10019048    dd offset aThisIsRnaPics ; DATA XREF: sub_
.data:10019048                                  ; sub_10003EBC:loc
.data:10019048                                  ; "[This is RNA]pi
.data:1001904C off_1001904C    dd offset aThisIsRgp     ; DATA XREF: sub_1
.data:1001904C                                  ; sub_10003EBC:loc
.data:1001904C                                  ; "[This is RGP]
.data:10019050 off_10019050    dd offset aThisIsPwd     ; DATA XREF: sub_1
.data:10019050                                  ; sub_10003EBC:loc
.data:10019050                                  ; "[This is PWD]
.data:10019054 aThisIsPwd      db '[This is PWD]
.data:10019054                                  ; DATA XREF: .data
.data:10019054                 db '                 ',0
.data:100190A3                 align 4
.data:100190A4 aThisIsRgp      db '[This is RGP]
.data:100190A4                                  ; DATA XREF: .data:off_1001904C↑o
.data:100190A4                 db '                 ',0
.data:100190F3                 align 4
.data:100190F4 aThisIsRnaPics  db '[This is RNA]pics',0 ; DATA XREF: .data:off_10019048↑o
.data:10019106                 db    0
.data:10019107                 db    0
.data:10019108                 db    0
.data:10019109                 db    0
.data:1001910A                 db    0
.data:1001910B                 db    0
.data:1001910C                 db    0
00016A40  10019040: .data:off_10019040
```

xrefs to aThisIsRdoPics_

Dire...	T.	Address	Text
U	o	.data:off_10019040	dd offset aThisIsRdoPics_; "[This is RDO]pics.praticalmalwareanalys"...

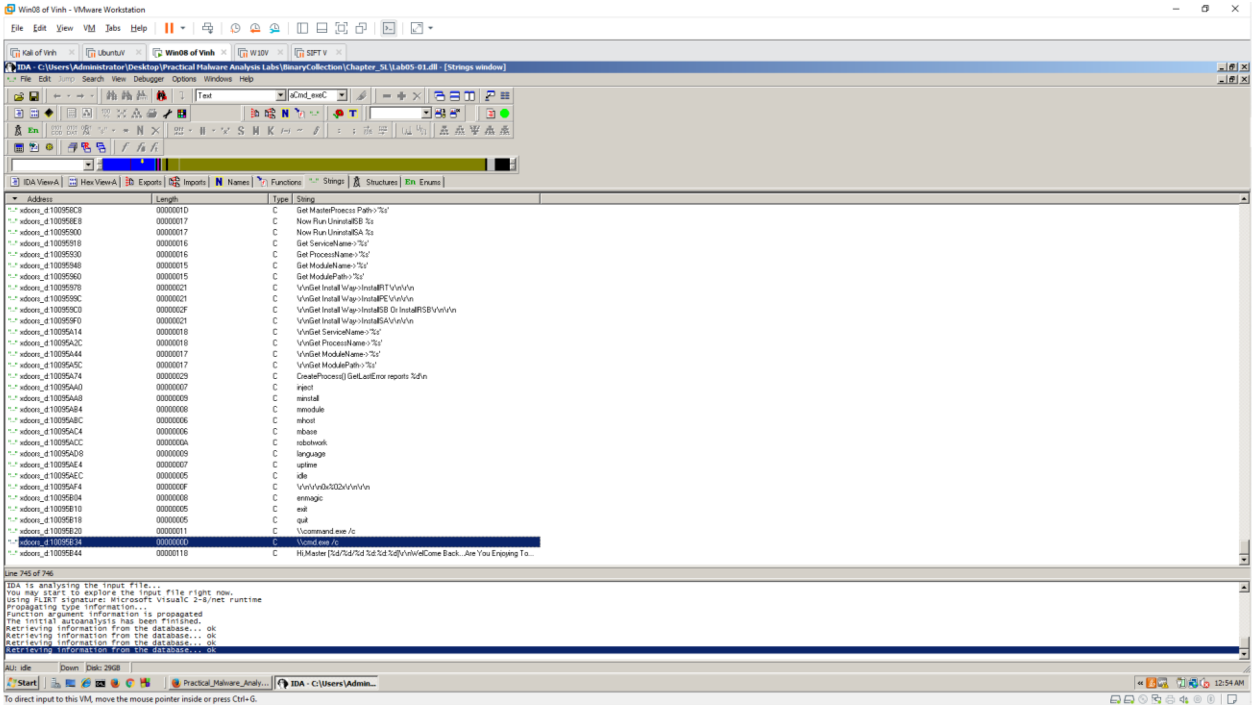
Line 1 of 1

```
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.
Retrieving information from the database... ok
Retrieving information from the database... ok
Retrieving information from the database... ok
Retrieving information from the database... ok
```

AU: idle Down Disk: 29GB

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Q7: Use the Strings window to locate the string \cmd.exe /c in the disassembly. Where is it located?



IDA - C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_5L\Lab05-01.dll - [Strings window]

Address	Length	Type	String
xdoors_d:100958C8	0000001D	C	Get MasterProecss Path->'%s'
xdoors_d:100958E8	00000017	C	Now Run UninstallSB %s
xdoors_d:10095900	00000017	C	Now Run UninstallSA %s
xdoors_d:10095918	00000016	C	Get ServiceName->'%s'
xdoors_d:10095930	00000016	C	Get ProcessName->'%s'
xdoors_d:10095948	00000015	C	Get ModuleName->'%s'
xdoors_d:10095960	00000015	C	Get ModulePath->'%s'
xdoors_d:10095978	00000021	C	\r\nGet Install Way->InstallRT\r\n\r\n
xdoors_d:1009599C	00000021	C	\r\nGet Install Way->InstallPE\r\n\r\n
xdoors_d:100959C0	0000002F	C	\r\nGet Install Way->InstallSB Or InstallRSB\r\n\r\n
xdoors_d:100959F0	00000021	C	\r\nGet Install Way->InstallSA\r\n\r\n
xdoors_d:10095A14	00000018	C	\r\nGet ServiceName->'%s'
xdoors_d:10095A2C	00000018	C	\r\nGet ProcessName->'%s'
xdoors_d:10095A44	00000017	C	\r\nGet ModuleName->'%s'
xdoors_d:10095A5C	00000017	C	\r\nGet ModulePath->'%s'
xdoors_d:10095A74	00000029	C	CreateProcess() GetLastError reports %d\n
xdoors_d:10095AA0	00000007	C	inject
xdoors_d:10095AA8	00000009	C	minstall
xdoors_d:10095AB4	00000008	C	mmodule
xdoors_d:10095ABC	00000006	C	mhost
xdoors_d:10095AC4	00000006	C	mbase
xdoors_d:10095ACC	0000000A	C	robotwork
xdoors_d:10095AD8	00000009	C	language
xdoors_d:10095AE4	00000007	C	uptime
xdoors_d:10095AEC	00000005	C	idle
xdoors_d:10095AF4	0000000F	C	\r\n\r\n0x%02x\r\n\r\n
xdoors_d:10095B04	00000008	C	enmagic
xdoors_d:10095B10	00000005	C	exit
xdoors_d:10095B18	00000005	C	quit
xdoors_d:10095B20	00000011	C	\\command.exe /c
xdoors_d:10095B34	0000000D	C	\\cmd.exe /c
xdoors_d:10095B44	00000118	C	Hi,Master [%d/%d/%d %d:%d:%d]\r\nWelCome Back...Are You Enjoying To...

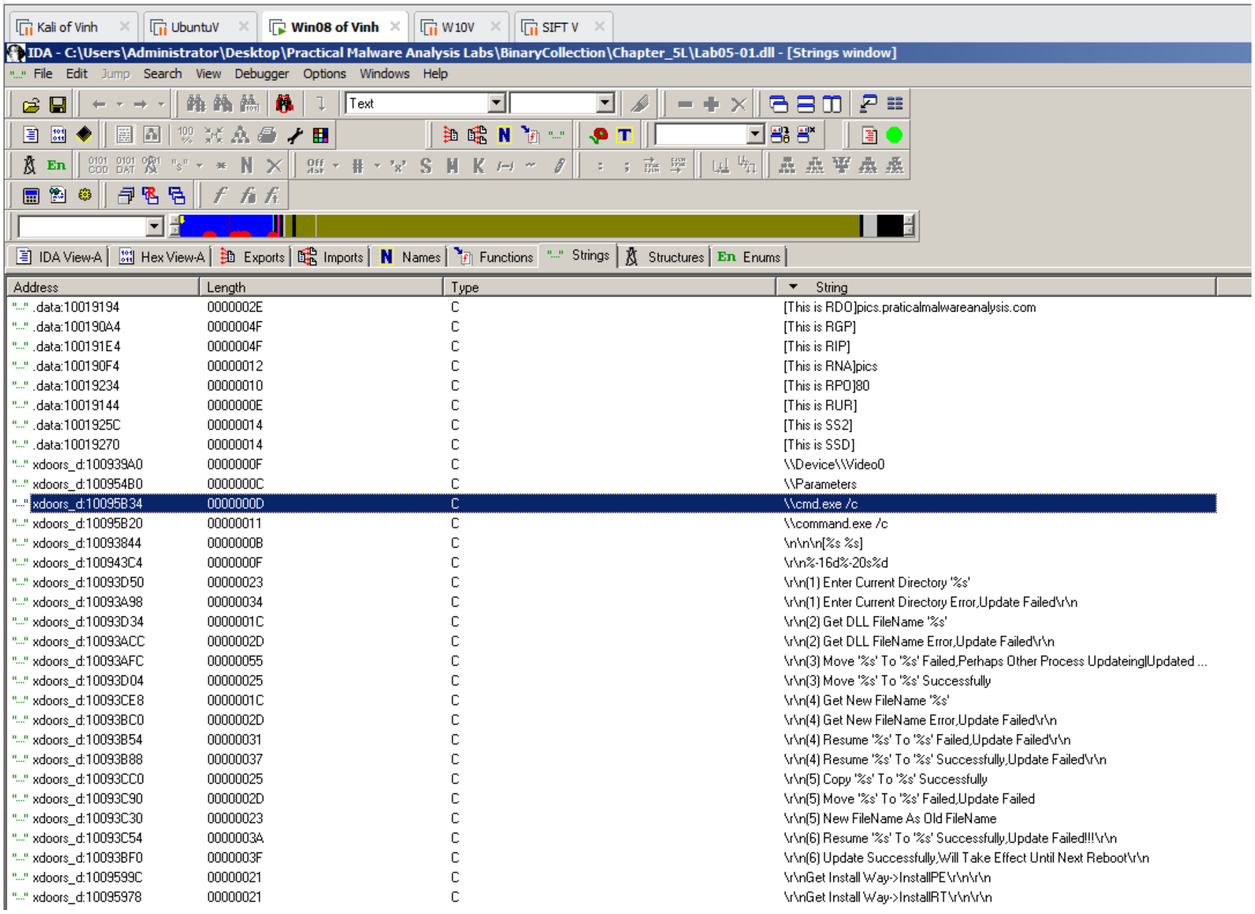
Line 745 of 746

```
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.
Retrieving information from the database... ok
Retrieving information from the database... ok
Retrieving information from the database... ok
Retrieving information from the database... ok
```

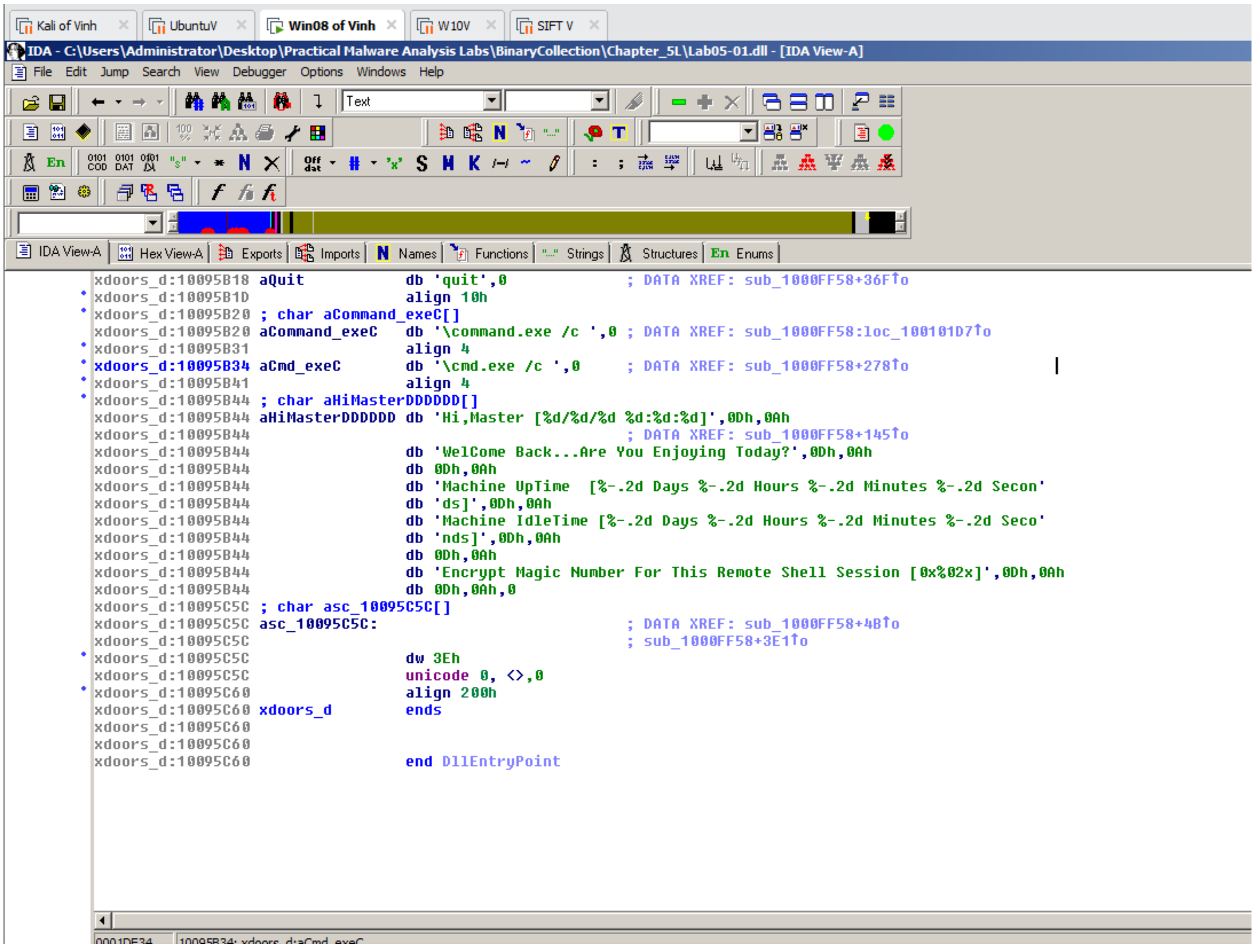
AU: idle Down Disk: 29GB

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Q8: Finding the Purpose of the Code that References \cmd.exe /c

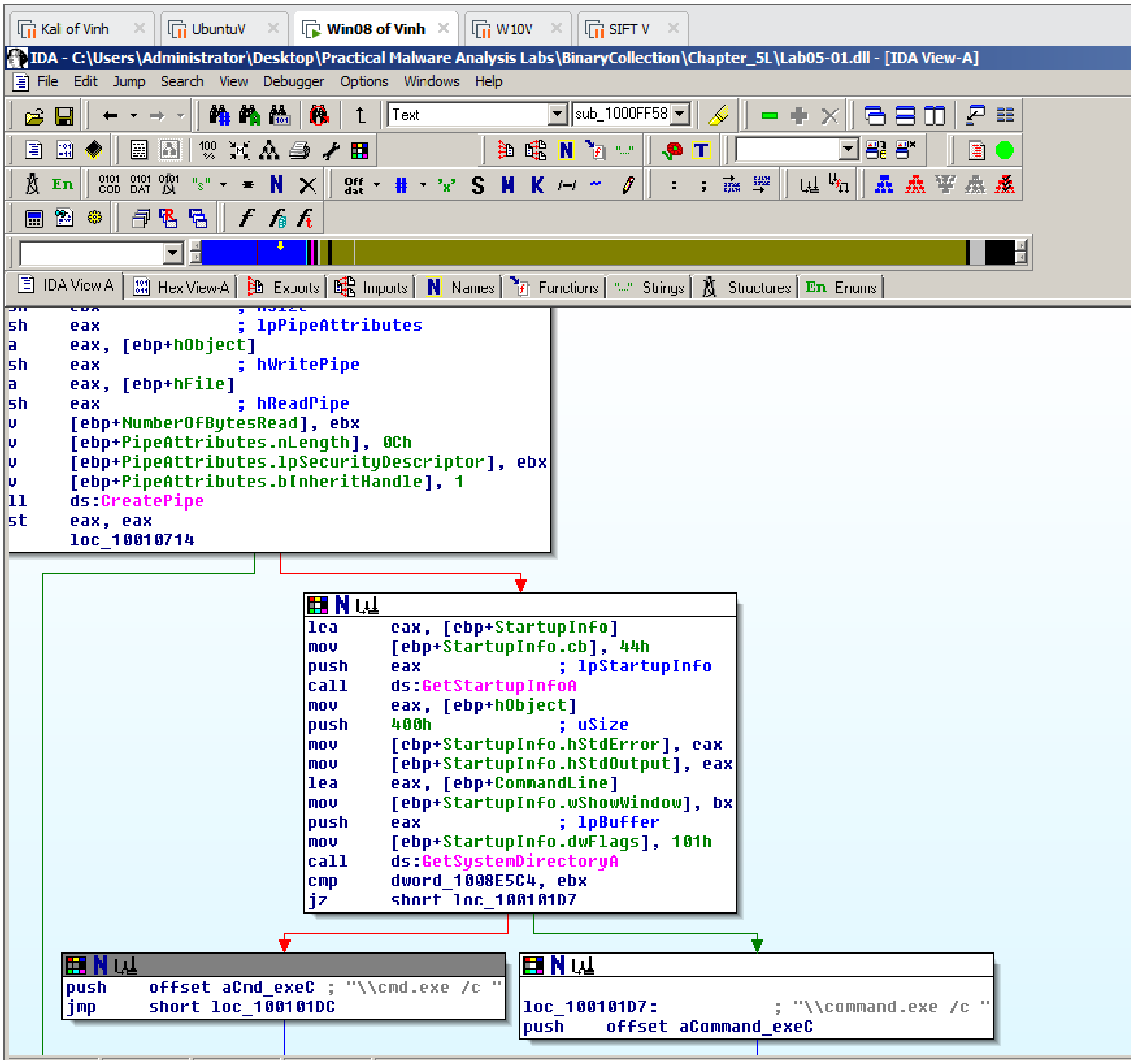

Kali of Vinh
UbuntuV
Win08 of Vinh
W10V
SIFT V
IDA - C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_5L\Lab05-01.dll - [Strings window]
File Edit Jump Search View Debugger Options Windows Help
Text
IDA View-A
Hex View-A
Exports
Imports
Names
Functions
Strings
Structures
Enums

Address	Length	Type	String
.data:10019194	0000002E	C	[This is RDO]pics.praticalmalwareanalysis.com
.data:100190A4	0000004F	C	[This is RGP]
.data:100191E4	0000004F	C	[This is RIP]
.data:100190F4	00000012	C	[This is RNA]pics
.data:10019234	00000010	C	[This is RPO]80
.data:10019144	0000000E	C	[This is RUR]
.data:1001925C	00000014	C	[This is SS2]
.data:10019270	00000014	C	[This is SSD]
xdoors_d:100939A0	0000000F	C	\\Device\\Video0
xdoors_d:100954B0	0000000C	C	\\Parameters
xdoors_d:10095B34	0000000D	C	\\cmd.exe /c
xdoors_d:10095B20	00000011	C	\\command.exe /c
xdoors_d:10093844	0000000B	C	\n\n\n[%s %s]
xdoors_d:100943C4	0000000F	C	\r\n%-16d%-20s%d
xdoors_d:10093D50	00000023	C	\r\n(1) Enter Current Directory '%s'
xdoors_d:10093A98	00000034	C	\r\n(1) Enter Current Directory Error,Update Failed\r\n
xdoors_d:10093D34	0000001C	C	\r\n(2) Get DLL FileName '%s'
xdoors_d:10093ACC	0000002D	C	\r\n(2) Get DLL FileName Error,Update Failed\r\n
xdoors_d:10093AFC	00000055	C	\r\n(3) Move '%s' To '%s' Failed,Perhaps Other Process Updateing|Updated ...
xdoors_d:10093D04	00000025	C	\r\n(3) Move '%s' To '%s' Successfully
xdoors_d:10093CE8	0000001C	C	\r\n(4) Get New FileName '%s'
xdoors_d:10093BC0	0000002D	C	\r\n(4) Get New FileName Error,Update Failed\r\n
xdoors_d:10093B54	00000031	C	\r\n(4) Resume '%s' To '%s' Failed,Update Failed\r\n
xdoors_d:10093B88	00000037	C	\r\n(4) Resume '%s' To '%s' Successfully,Update Failed\r\n
xdoors_d:10093CC0	00000025	C	\r\n(5) Copy '%s' To '%s' Successfully
xdoors_d:10093C90	0000002D	C	\r\n(5) Move '%s' To '%s' Failed,Update Failed
xdoors_d:10093C30	00000023	C	\r\n(5) New FileName As Old FileName
xdoors_d:10093C54	0000003A	C	\r\n(6) Resume '%s' To '%s' Successfully,Update Failed!!!\r\n
xdoors_d:10093BF0	0000003F	C	\r\n(6) Update Successfully,Will Take Effect Until Next Reboot\r\n
xdoors_d:1009599C	00000021	C	\r\nGet Install Way->InstallPE\r\n\r\n
xdoors_d:10095978	00000021	C	\r\nGet Install Way->InstallRT\r\n\r\n



Kali of Vinh
UbuntuV
Win08 of Vinh
W10V
SIFT V
IDA - C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_5L\Lab05-01.dll - [IDA View-A]
File Edit Jump Search View Debugger Options Windows Help
Text
IDA View-A
Hex View-A
Exports
Imports
Names
Functions
Strings
Structures
Enums
0001DF34
10095B34: xdoors_d:aCmd_exeC

```
xdoors_d:10095B18 aQuit           db 'quit',0             ; DATA XREF: sub_1000FF58+36F↑o
xdoors_d:10095B1D                 align 10h
xdoors_d:10095B20 ; char aCommand_exeC[]
xdoors_d:10095B20 aCommand_exeC   db '\command.exe /c ',0 ; DATA XREF: sub_1000FF58:loc_100101D7↑o
xdoors_d:10095B31                 align 4
xdoors_d:10095B34 aCmd_exeC       db '\cmd.exe /c ',0     ; DATA XREF: sub_1000FF58+278↑o
xdoors_d:10095B41                 align 4
xdoors_d:10095B44 ; char aHiMasterDDDDDD[]
xdoors_d:10095B44 aHiMasterDDDDDD db 'Hi,Master [%d/%d/%d %d:%d:%d]',0Dh,0Ah
xdoors_d:10095B44                                         ; DATA XREF: sub_1000FF58+145↑o
xdoors_d:10095B44                 db 'WelCome Back...Are You Enjoying Today?',0Dh,0Ah
xdoors_d:10095B44                 db 0Dh,0Ah
xdoors_d:10095B44                 db 'Machine UpTime  [%-.2d Days %-.2d Hours %-.2d Minutes %-.2d Secon'
xdoors_d:10095B44                 db 'ds]',0Dh,0Ah
xdoors_d:10095B44                 db 'Machine IdleTime [%-.2d Days %-.2d Hours %-.2d Minutes %-.2d Seco'
xdoors_d:10095B44                 db 'nds]',0Dh,0Ah
xdoors_d:10095B44                 db 0Dh,0Ah
xdoors_d:10095B44                 db 'Encrypt Magic Number For This Remote Shell Session [0x%02x]',0Dh,0Ah
xdoors_d:10095B44                 db 0Dh,0Ah,0
xdoors_d:10095C5C ; char asc_10095C5C[]
xdoors_d:10095C5C asc_10095C5C:                           ; DATA XREF: sub_1000FF58+4B↑o
xdoors_d:10095C5C                                         ; sub_1000FF58+3E1↑o
xdoors_d:10095C5C                 dw 3Eh
xdoors_d:10095C5C                 unicode 0, <>,0
xdoors_d:10095C60                 align 200h
xdoors_d:10095C60 xdoors_d        ends
xdoors_d:10095C60
xdoors_d:10095C60
xdoors_d:10095C60                 end DllEntryPoint
```



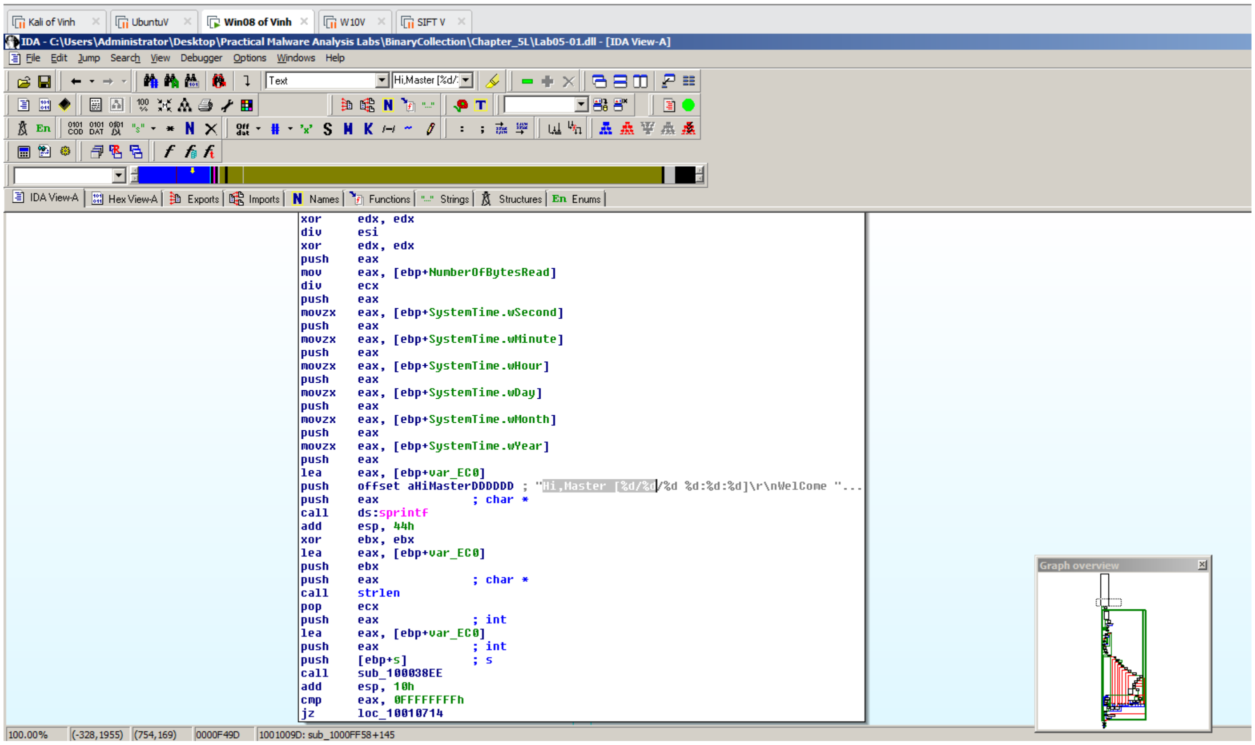
```
sh     eax                    ; lpPipeAttributes
a      eax, [ebp+hObject]
sh     eax                    ; hWritePipe
a      eax, [ebp+hFile]
sh     eax                    ; hReadPipe
v      [ebp+NumberOfBytesRead], ebx
v      [ebp+PipeAttributes.nLength], 0Ch
v      [ebp+PipeAttributes.lpSecurityDescriptor], ebx
v      [ebp+PipeAttributes.bInheritHandle], 1
ll     ds:CreatePipe
st     eax, eax
       loc_10010714
```

```
lea     eax, [ebp+StartupInfo]
mov     [ebp+StartupInfo.cb], 44h
push    eax             ; lpStartupInfo
call    ds:GetStartupInfoA
mov     eax, [ebp+hObject]
push    400h            ; uSize
mov     [ebp+StartupInfo.hStdError], eax
mov     [ebp+StartupInfo.hStdOutput], eax
lea     eax, [ebp+CommandLine]
mov     [ebp+StartupInfo.wShowWindow], bx
push    eax             ; lpBuffer
mov     [ebp+StartupInfo.dwFlags], 101h
call    ds:GetSystemDirectoryA
cmp     dword_1008E5C4, ebx
jz      short loc_100101D7
```

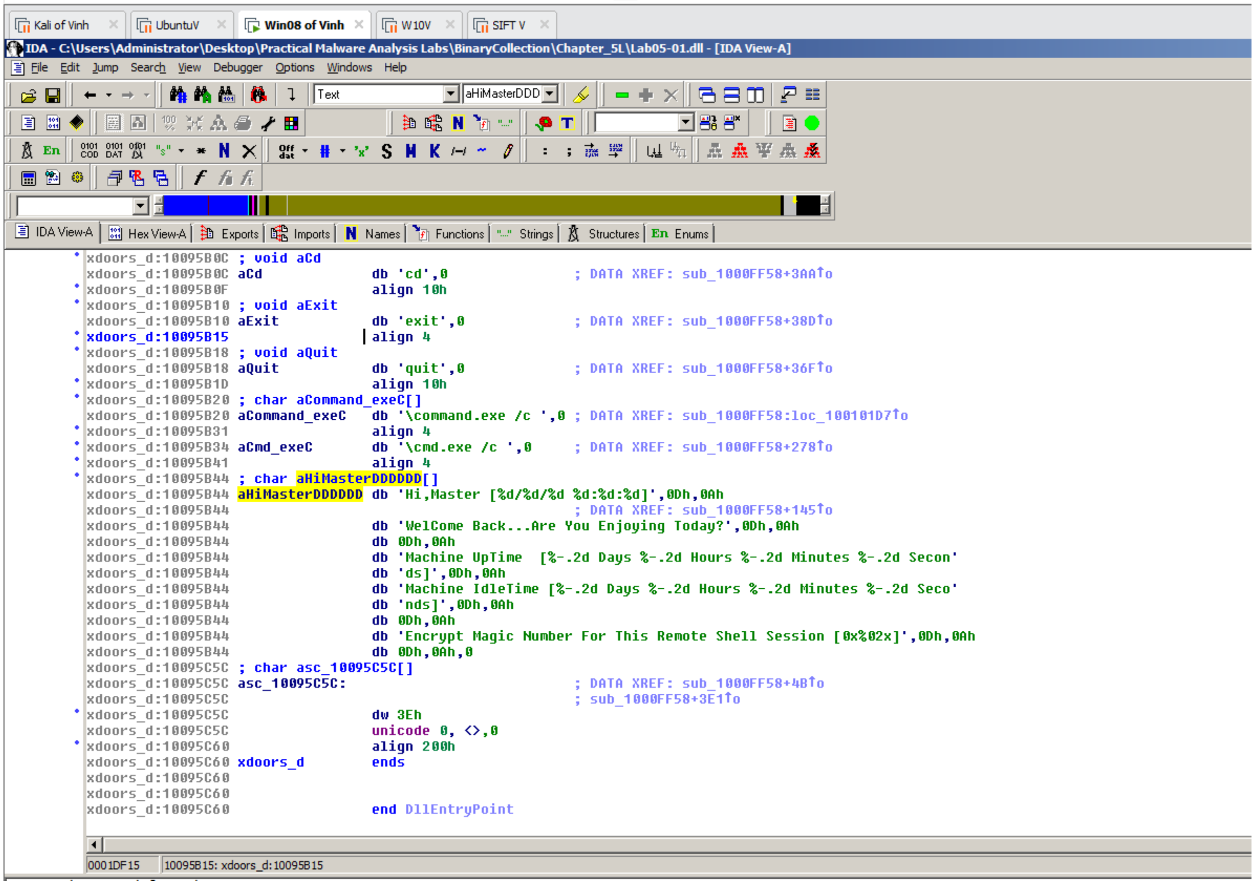
```
push    offset aCmd_exeC ; "\\cmd.exe /c "
jmp     short loc_100101DC
```

```

loc_100101D7:               ; "\\command.exe /c "
push    offset aCommand_exeC
```


Kali of Vinh
UbuntuV
Win08 of Vinh
W10V
SIFT V
IDA - C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_5L\Lab05-01.dll - [IDA View-A]
File Edit Jump Search View Debugger Options Windows Help
Text
Hi,Master [%d/
IDA View-A
Hex View-A
Exports
Imports
Names
Functions
Strings
Structures
Enums
Graph overview
100.00%
(-328,1955)
(754,169)
0000F49D
1001009D: sub_1000FF58+145

```
xor     edx, edx
div     esi
xor     edx, edx
push    eax
mov     eax, [ebp+NumberOfBytesRead]
div     ecx
push    eax
movzx   eax, [ebp+SystemTime.wSecond]
push    eax
movzx   eax, [ebp+SystemTime.wMinute]
push    eax
movzx   eax, [ebp+SystemTime.wHour]
push    eax
movzx   eax, [ebp+SystemTime.wDay]
push    eax
movzx   eax, [ebp+SystemTime.wMonth]
push    eax
movzx   eax, [ebp+SystemTime.wYear]
push    eax
lea     eax, [ebp+var_EC0]
push    offset aHiMasterDDDDDD ; "Hi,Master [%d/%d/%d %d:%d:%d]\r\nWelCome "...
push    eax             ; char *
call    ds:sprintf
add     esp, 44h
xor     ebx, ebx
lea     eax, [ebp+var_EC0]
push    ebx
push    eax             ; char *
call    strlen
pop     ecx
push    eax             ; int
lea     eax, [ebp+var_EC0]
push    eax             ; int
push    [ebp+s]         ; s
call    sub_100038EE
add     esp, 10h
cmp     eax, 0FFFFFFFFh
jz      loc_10010714
```


Kali of Vinh
UbuntuV
Win08 of Vinh
W10V
SIFT V
IDA - C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_5L\Lab05-01.dll - [IDA View-A]
File Edit Jump Search View Debugger Options Windows Help
Text
aHiMasterDDD
IDA View-A
Hex View-A
Exports
Imports
Names
Functions
Strings
Structures
Enums
0001DF15
10095B15: xdoors_d:10095B15

```
xdoors_d:10095B0C ; void aCd
xdoors_d:10095B0C aCd             db 'cd',0               ; DATA XREF: sub_1000FF58+3AA↑o
xdoors_d:10095B0F                 align 10h
xdoors_d:10095B10 ; void aExit
xdoors_d:10095B10 aExit           db 'exit',0             ; DATA XREF: sub_1000FF58+38D↑o
xdoors_d:10095B15                 align 4
xdoors_d:10095B18 ; void aQuit
xdoors_d:10095B18 aQuit           db 'quit',0             ; DATA XREF: sub_1000FF58+36F↑o
xdoors_d:10095B1D                 align 10h
xdoors_d:10095B20 ; char aCommand_exeC[]
xdoors_d:10095B20 aCommand_exeC   db '\command.exe /c ',0 ; DATA XREF: sub_1000FF58:loc_100101D7↑o
xdoors_d:10095B31                 align 4
xdoors_d:10095B34 aCmd_exeC       db '\cmd.exe /c ',0     ; DATA XREF: sub_1000FF58+278↑o
xdoors_d:10095B41                 align 4
xdoors_d:10095B44 ; char aHiMasterDDDDDD[]
xdoors_d:10095B44 aHiMasterDDDDDD db 'Hi,Master [%d/%d/%d %d:%d:%d]',0Dh,0Ah
xdoors_d:10095B44                                         ; DATA XREF: sub_1000FF58+145↑o
xdoors_d:10095B44                 db 'WelCome Back...Are You Enjoying Today?',0Dh,0Ah
xdoors_d:10095B44                 db 0Dh,0Ah
xdoors_d:10095B44                 db 'Machine UpTime  [%-.2d Days %-.2d Hours %-.2d Minutes %-.2d Secon'
xdoors_d:10095B44                 db 'ds]',0Dh,0Ah
xdoors_d:10095B44                 db 'Machine IdleTime [%-.2d Days %-.2d Hours %-.2d Minutes %-.2d Seco'
xdoors_d:10095B44                 db 'nds]',0Dh,0Ah
xdoors_d:10095B44                 db 0Dh,0Ah
xdoors_d:10095B44                 db 'Encrypt Magic Number For This Remote Shell Session [0x%02x]',0Dh,0Ah
xdoors_d:10095B44                 db 0Dh,0Ah,0
xdoors_d:10095C5C ; char asc_10095C5C[]
xdoors_d:10095C5C asc_10095C5C:                           ; DATA XREF: sub_1000FF58+4B↑o
xdoors_d:10095C5C                                         ; sub_1000FF58+3E1↑o
xdoors_d:10095C5C                 dw 3Eh
xdoors_d:10095C5C                 unicode 0, <>,0
xdoors_d:10095C60                 align 200h
xdoors_d:10095C60 xdoors_d        ends
xdoors_d:10095C60
xdoors_d:10095C60
xdoors_d:10095C60                 end DllEntryPoint
```