HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA AN TOÀN THÔNG TIN

MODULE THỰC HÀNH
MÃ ĐỘC

BÀI THỰC HÀNH SỐ 04

Sử dụng IDA Pro phân tích mã độc

Người thực hiện bài thực hành:

TS. Đặng Xuân Bảo

Hà Nội, 2020

MỤC LỤC

THÔNG TIN CHUNG VỀ BÀI THỰC HÀNH

Tên bài thực hành: Sử dụng IDA Pro phân tích mã độc

Học phần: Mã độc

Số lượng sinh viên cùng thực hiện:

Địa điểm thực hành: Phòng máy

Yêu cầu:

- Yêu cầu phần cứng:
  - Máy tính với cấu hình tối thiểu: CPU 2.0 GHz, RAM 4GB, HDD 500GB
- Yêu cầu phần mềm trên máy:
  - Hệ điều hành Windows 10
  - VMware Worstation 15.0
- Yêu cầu kết nối mạng LAN: có
- Yêu cầu kết nối mạng Internet: có

CHUẨN BỊ BÀI THỰC HÀNH

Đối với giảng viên

Trước buổi học, giảng viên (người hướng dẫn thực hành) cần kiểm tra sự phù hợp của điều kiện thực tế của phòng thực hành với các yêu cầu của bài thực hành.

Ngoài ra không đòi hỏi gì thêm.

Đối với sinh viên

Trước khi bắt đầu thực hành, cần tạo các bản sao của máy ảo để sử dụng. Đồng thời xác định vị trí lưu trữ các công cụ đã chỉ ra trong phần yêu cầu.

Sử dụng IDA Pro phân tích mã độc

1.1. Mô tả

Bài thực hành hướng dẫn sinh viên sử dụng một số công cụ trong việc phân tích động một số mẫu mã độc đơn giản..

1.2. Chuẩn bị

- Môi trường phân tích mã độc đã xây dựng trong Lab 1.

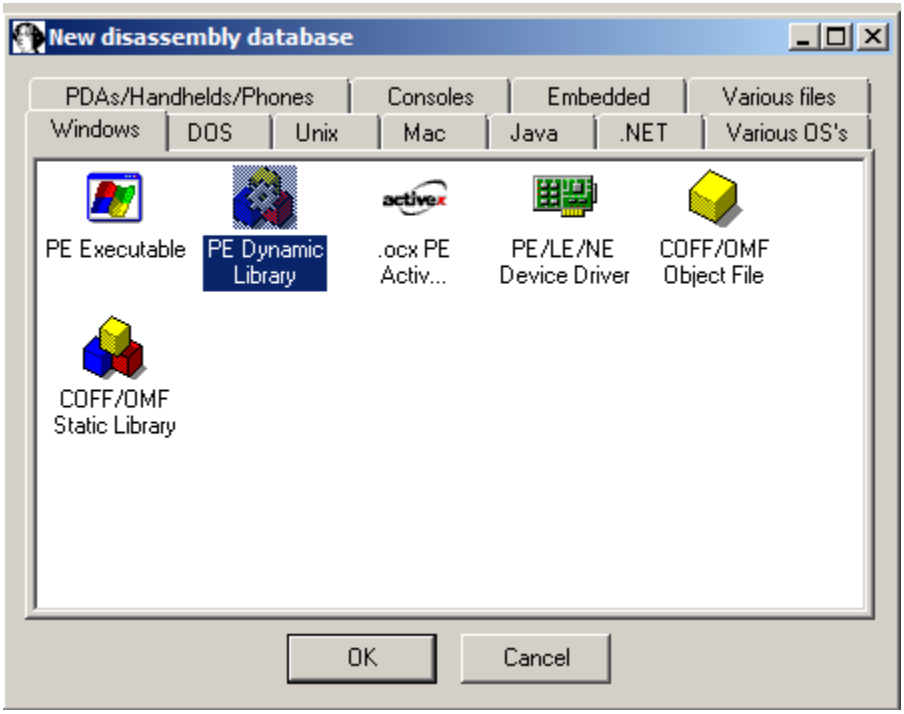
1.3. Phân tích Lab05-01

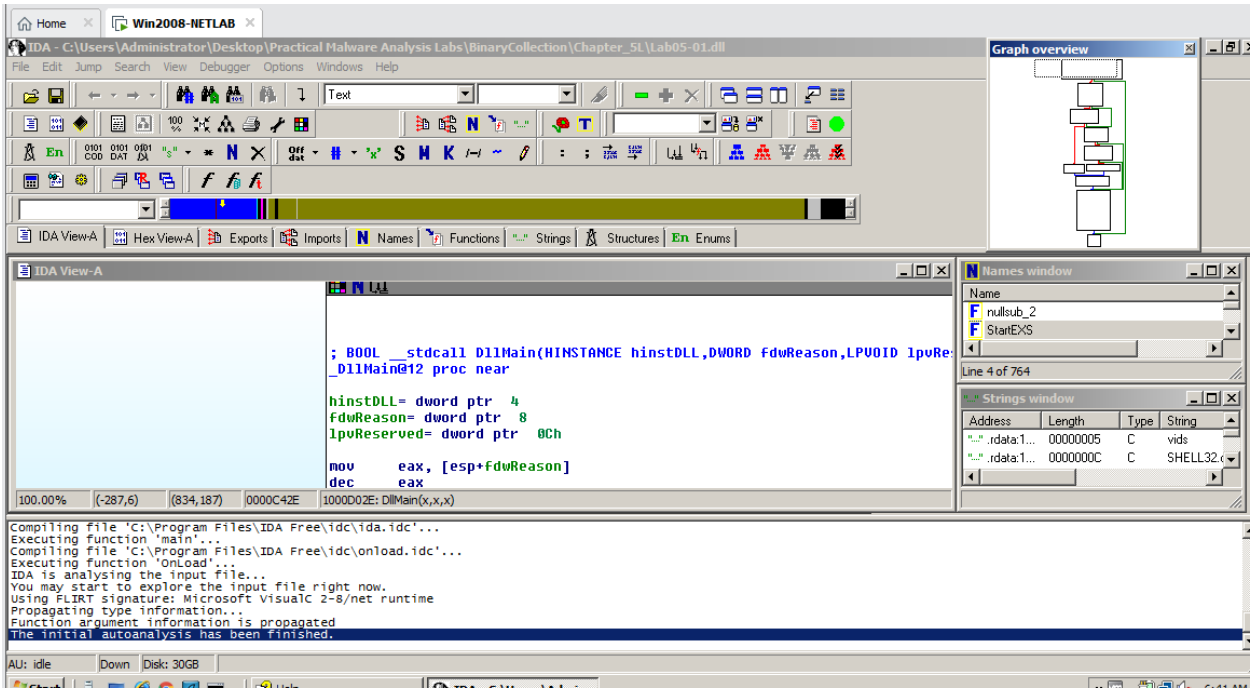
Thực hiện các yêu cầu với Lab05-01.dll có trong tài liệu Practical Malware Analysis.

Dùng IDA Pro đọc Lab05-01.dll

Trên giao diện IDA Pro, chọn OK, tiếp đến là OK. Sau đó ta chọn vào biểu tượng "**PE Dynamic Library",** chọn **OK.**

Đưa con trỏ chuột tới Lab05-01.dll và mở thư mục đó.



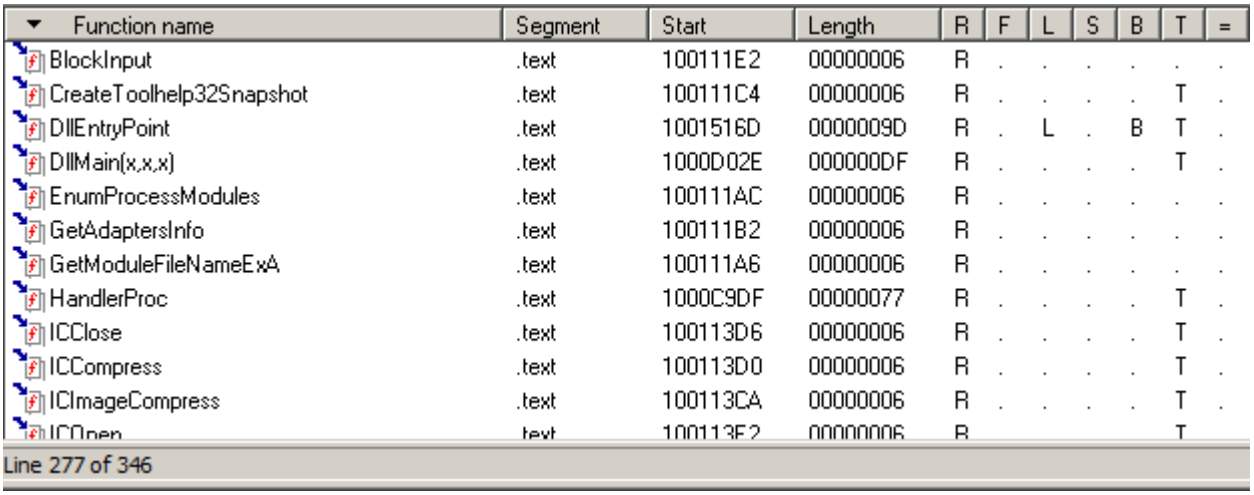

Home
Win2008-NETLAB
IDA - C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_5L\Lab05-01.dll
File Edit Jump Search View Debugger Options Windows Help
Graph overview
IDA View-A Hex View-A Exports Imports Names Functions Strings Structures Enums
IDA View-A
; BOOL __stdcall DllMain(HINSTANCE hinstDLL,DWORD fdwReason,LPVOID lpvRe
_DllMain@12 proc near
hinstDLL= dword ptr 4
fdwReason= dword ptr 8
lpvReserved= dword ptr 0Ch
mov eax, [esp+fdwReason]
dec eax
100.00% (-287,6) (834,187) 0000C42E 1000D02E: DllMain(x,x,x)
Names window
Name
nullsub_2
StartEXS
Line 4 of 764
Strings window
Address Length Type String
.rdata:1... 00000005 C vids
.rdata:1... 0000000C C SHELL32.
Compiling file 'C:\Program Files\IDA Free\idc\ida.idc'...
Executing function 'main'...
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.
AU: idle Down Disk: 30GB

Q 1: Tìm địa chỉ DLLMain

Trên IDA Pro, ta chọn "**Windows**", tiếp đến "**Functions window**".

Chọn tiêu đề "**Function name**" để sắp xếp theo tên.

Vị trí của DLLMain sẽ được hiển thị như hình bên dưới:



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	

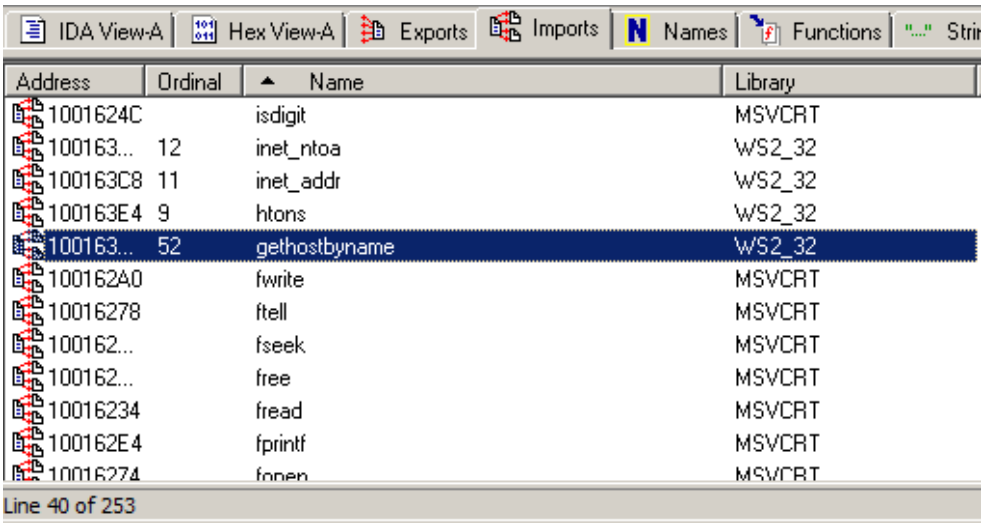
Line 277 of 346

Q 2: Tìm import cho gethostbyname

Trên IDA Pro, chọn **Windows**, **Imports**. Chọn **Name** để sắp xếp theo tên. Tìm "gethostbyname" (Lưu ý chữ hoa và chữ thường được sắp xếp riêng biệt).

Mở rộng cột Address để hiển thị toàn bộ.

Vị trí của Gethostbyname sẽ được hiển thị như hình bên dưới:



IDA View-A | Hex View-A | Exports | Imports | Names | Functions | Strin

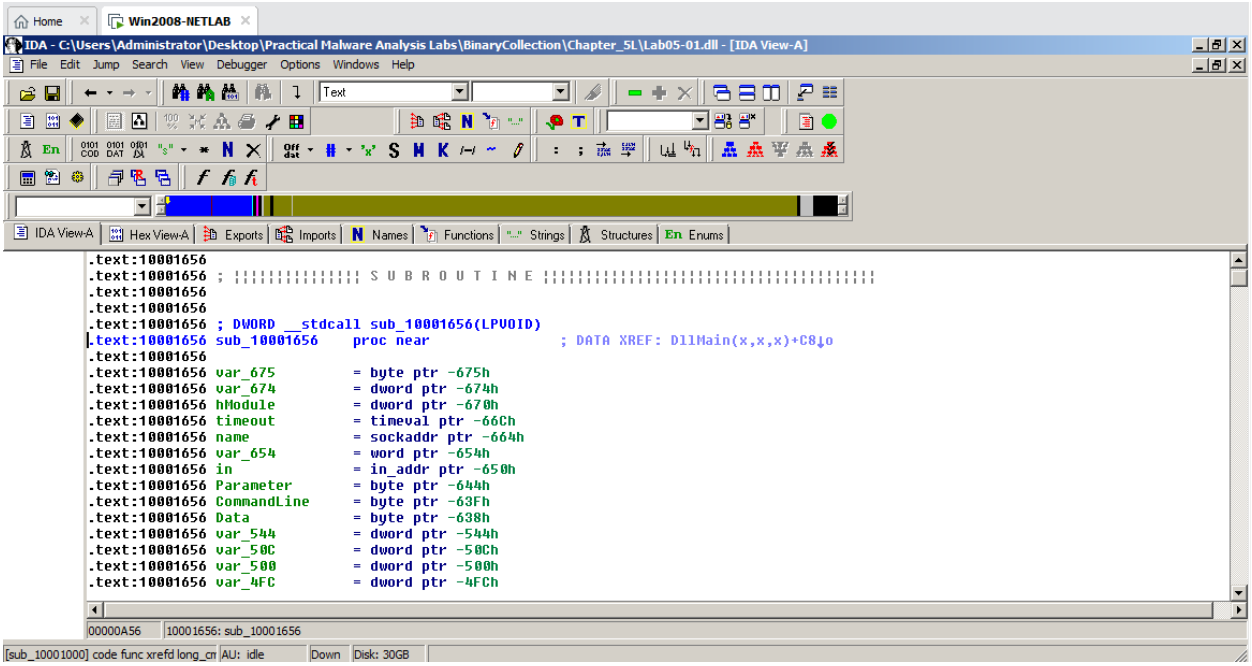
Address	Ordinal	Name	Library
1001624C		isdigit	MSVCRT
100163...	12	inet_ntoa	WS2_32
100163C8	11	inet_addr	WS2_32
100163E4	9	htons	WS2_32
100163...	52	gethostbyname	WS2_32
100162A0		fwrite	MSVCRT
10016278		ftell	MSVCRT
100162...		fseek	MSVCRT
100162...		free	MSVCRT
10016234		fread	MSVCRT
100162E4		fprintf	MSVCRT
10016274		fopen	MSVCRT

Line 40 of 253

Q 5: Đếm các biến cục bộ cho chương trình con tại 0x10001656

Trên IDA Pro, chọn **Windows**, "**IDA View-A**". Nhấn phím **SPACEBAR** để xem văn bản.

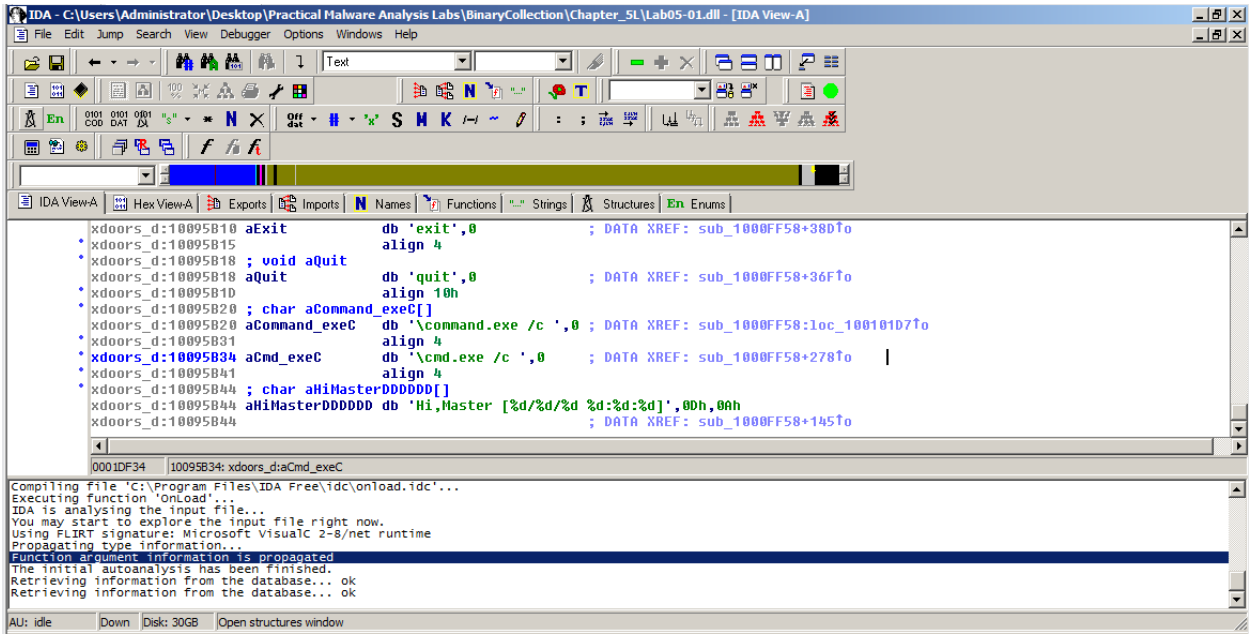
Nhấn "**g**" để tiếp tục. Nhập địa chỉ **0x10001656** và nhấn **OK**. Cuộn lên để hiển thị các bình luận IDA được thêm vào đầu hàm, liệt kê các biến cục bộ của nó, như được hiển thị bên dưới:



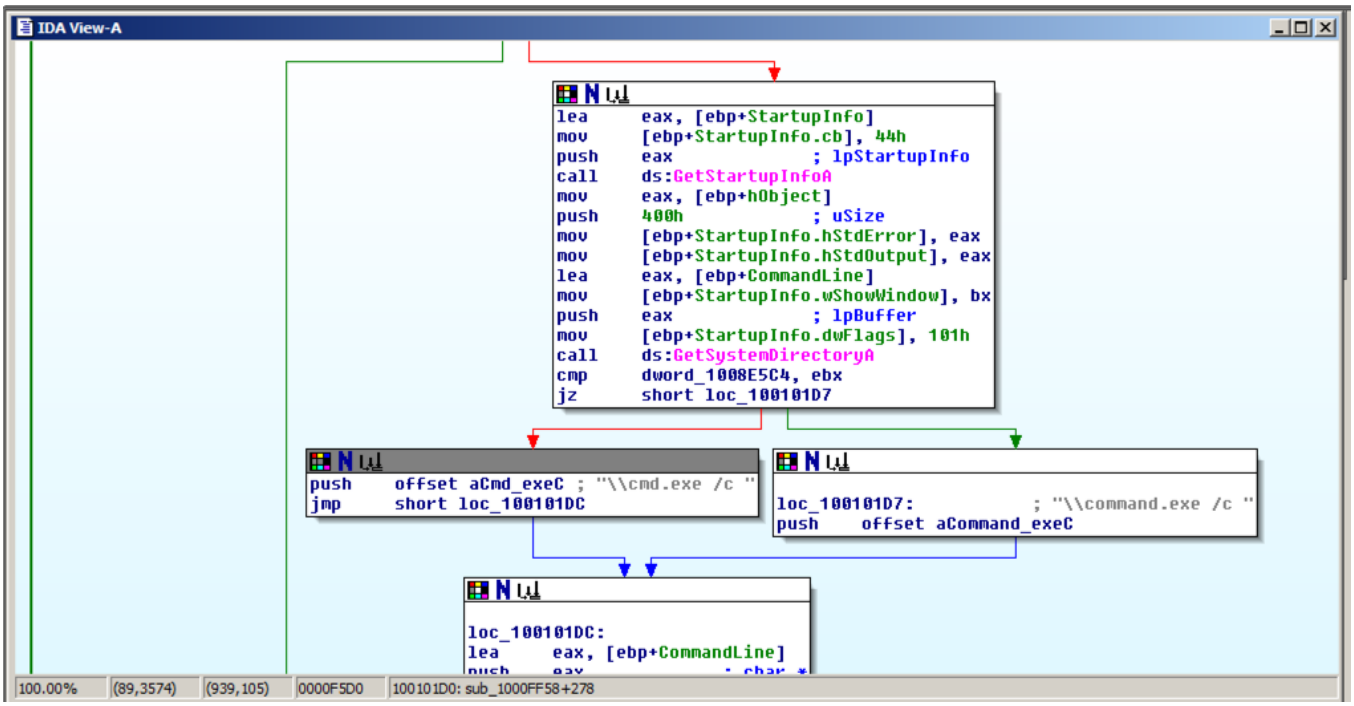
Q 8: Tìm mục đích của mã \cmd.exe /c

Trong IDA Pro, chọn **Windows**, **Strings**. Mở rộng cửa sổ giao diện. Sắp xếp theo **String**. Tìm chuỗi "**\\cmd.exe /c**" và kích đúp vào chuỗi đó. Hàm được mở trong chế độ văn bản như hình dưới.

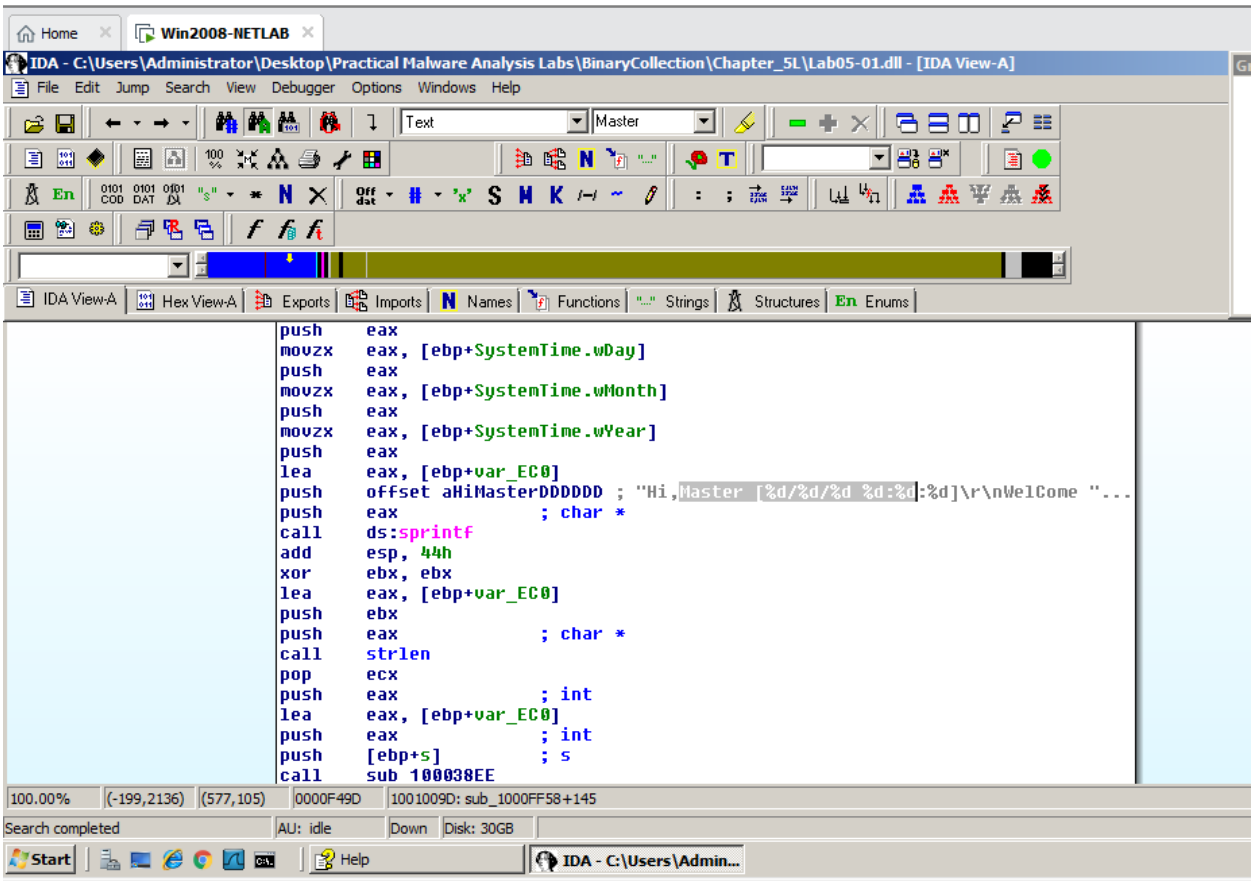
Trong dòng chứa "**\\cmd.exe /c",** kích đúp vào địa chỉ bên phải của "XREF"



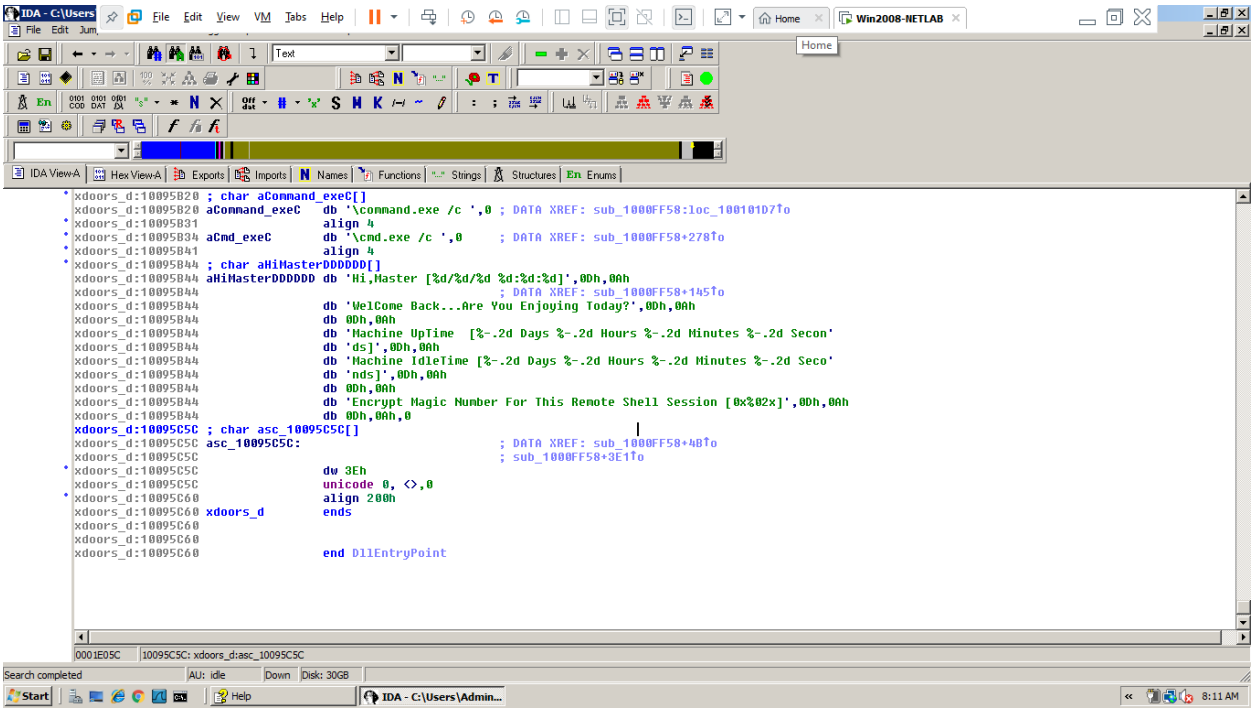
Nhấn phím **SPACEBAR** để bật chế độ xem biểu đồ.



Kéo chế độ xem biểu đồ xuống để xem các chương trình con trước nó, bạn sẽ thấy đoạn văn bản bắt đầu bằng "Hi, Master", như hiển thị bên dưới.



Kích đúp chuột vào "**aHiMasterDDDD**" để thấy thông tin đầy đủ. Phân tích kết quả hiển thị trong hình dưới đây.


IDA - C:\Users
File Edit View VM Tabs Help
Home
Win2008-NETLAB
Text
IDA View-A
Hex View-A
Exports
Imports
Names
Functions
Strings
Structures
Enums
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
0001E05C
10095C5C: xdoors_d:asc_10095C5C
Search completed
AU: idle
Down
Disk: 30GB
Start
Help
IDA - C:\Users\Admin...
8:11 AM