

Bài 12. Thực hành phân tích mã độc

Học phần: ĐẢM BẢO VÀ AN TOÀN THÔNG TIN

NỘI DUNG

- 1. Lý thuyết phân tích mã độ**
- 2. Phân tích tĩnh**
- 3. Phân tích động**

1. Lý thuyết phân tích mã độc

+ Host-based signatures

- Xác định files hoặc registry keys ở máy nạn nhân

- Tập trung mã độc hệ thống

+ Network signatures

- Phát hiện mã độc bằng cách phân tích giao thông mạng

Static v. Dynamic Analysis

+ Static Analysis

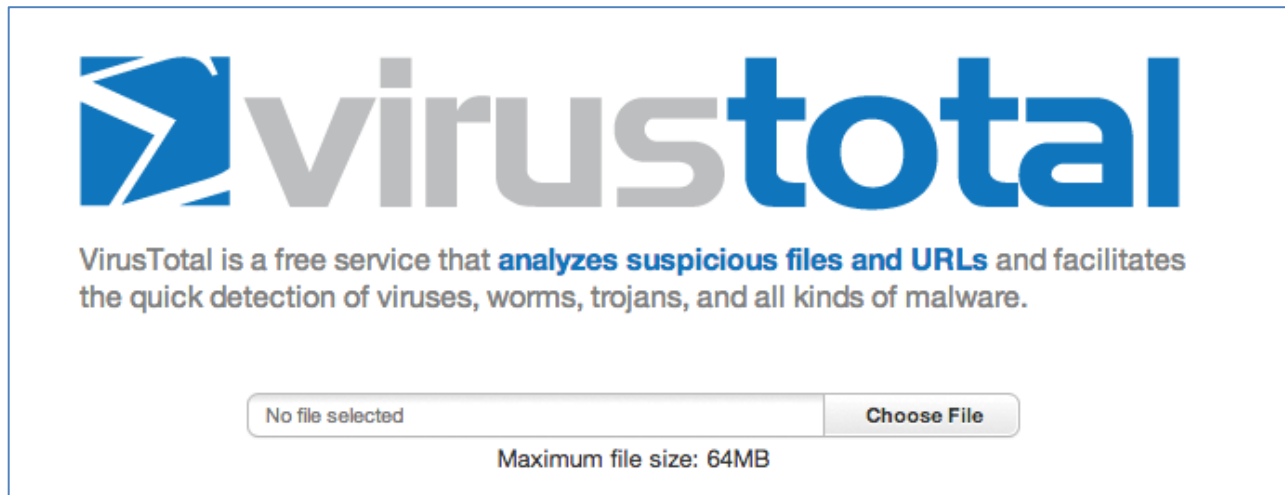
- Phân tích mã độc mà ko thực thi nó
- Một số công cụ : VirusTotal, strings, a disassembler like IDA Pro

+ Dynamic Analysis

- Chạy mã độc và giám sát ảnh hưởng của nó
- Sử dụng máy ảo và take snapshots
- Công cụ: RegShot, Process Monitor, Process Hacker, CaptureBAT
- RAM Analysis: Mandant Redline and Volatility

2. Basic Static Analysis

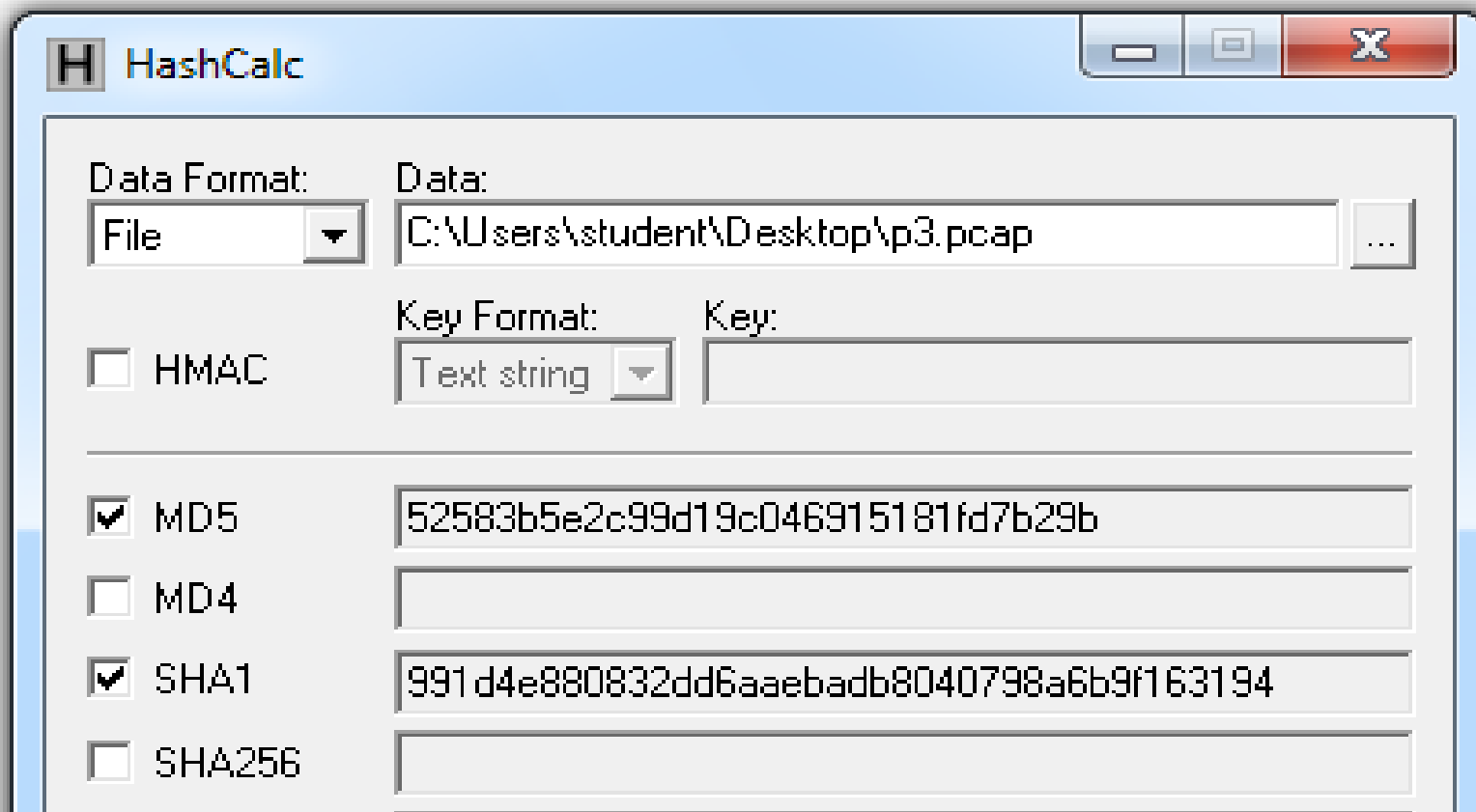
a. Antivirus scanning: virustotal, kaspersky, avast,...



b. Hashes (MD5 or SHA-1): xác định xem 1 file có bị thay đổi kích thước hay không

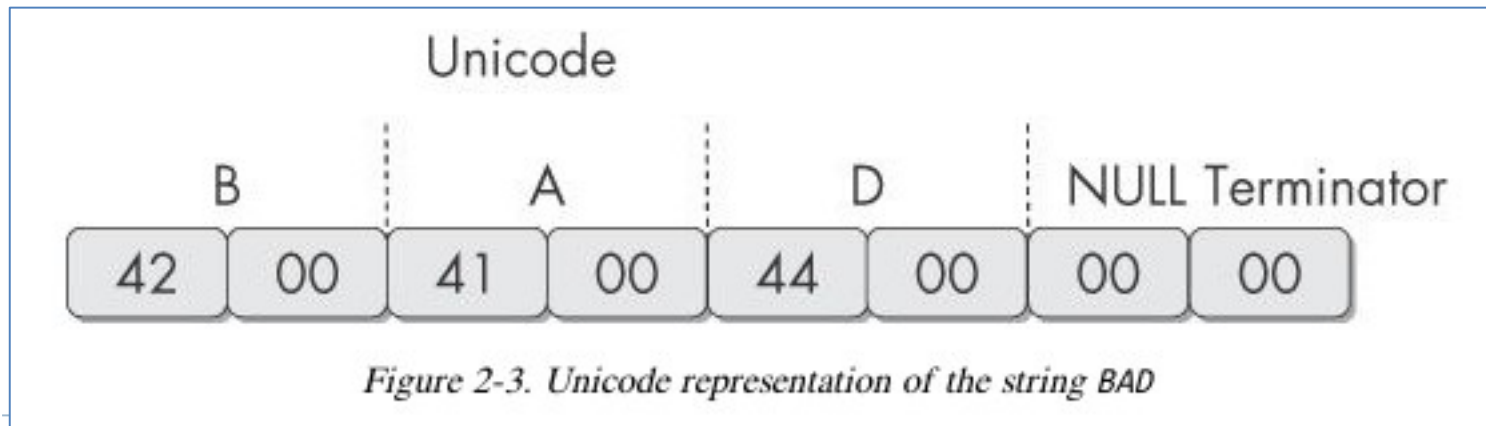
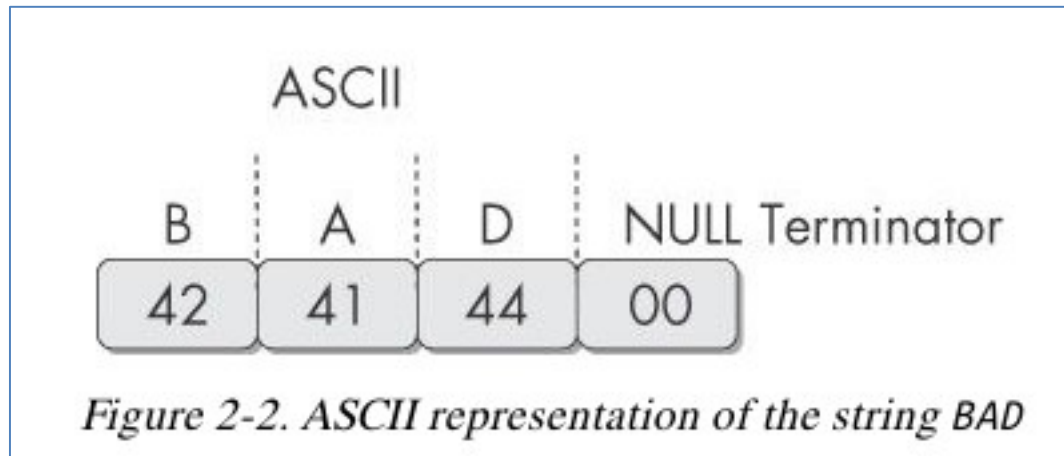
Basic Static Analysis

b. Hashes (MD5 or SHA-1): xác định xem 1 file có bị thay đổi kích thước hay không



Basic Static Analysis

c. Finding string: 1 chuỗi kết thúc bởi ký tự **null** (0x00)



Basic Static Analysis

c. Finding string

- Tìm kiếm các hàm của Windows mà mã độc thường gọi. Ví dụ: GDI32.DLL (Dynamic Link Library)

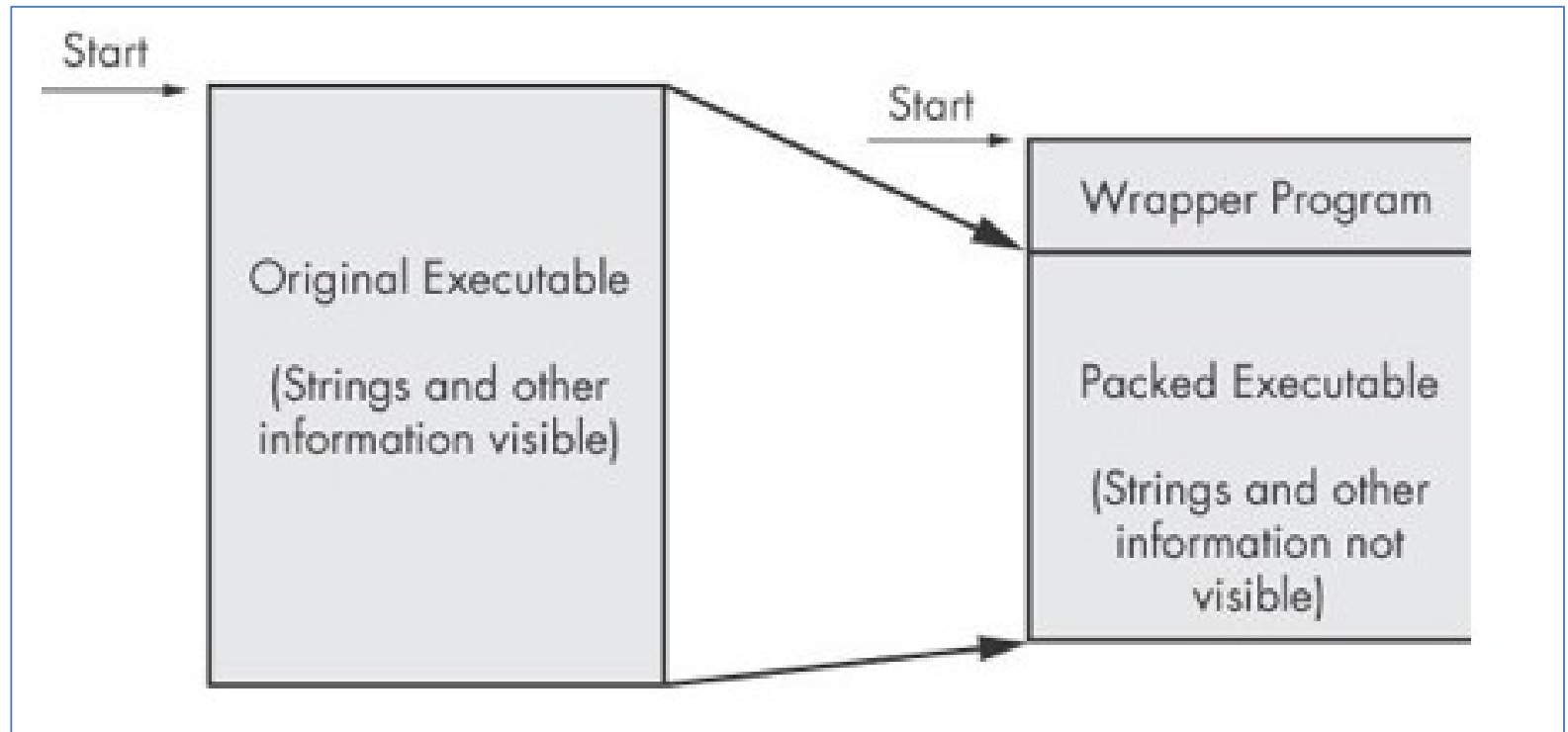
```
C:>strings bp6.ex_  
VP3  
VW3  
t$@  
D$4  
99.124.22.1 4  
e-@  
GetLayout 1  
GDI32.DLL 3  
SetLayout 2  
M}C  
Mail system DLL is invalid.!Send Mail failed to  
send message. 5
```


3. Dynamic Analysis

- PE files
- Dependency Walker
- Common DLLs
- Procmon: Filter on the malware executable name and clear all events just before running it
- Process Explorer
- Regshot
- Wireshark

Packing Files

Chương trình mã độc được nén như file zip, các kỹ thuật sử dụng strings không đọc được



Packing Files

Tool: UPX

```
root@kali: ~/126
File Edit View Search Terminal Help
root@kali:~/126# cat chatty.c
#include <stdio.h>
main()
{
char name[10];
printf("This program contains readable strings\n");
printf("Enter your name: ");
scanf("%s", name);
printf("Hello %s\n", name);
}

root@kali:~/126# gcc -static chatty.c -o chatty
root@kali:~/126# upx -o chatty-packed chatty
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2011
UPX 3.08 Markus Oberhumer, Laszlo Molnar & John Reiser Dec 12th 2011

File size      Ratio      Format      Name
-----
592800 -> 272588 45.98% linux/elf386 chatty-packed

Packed 1 file.
root@kali:~/126# ls -l
total 852
-rwxr-xr-x 1 root root 592800 Aug 16 20:34 chatty
-rw-r--r-- 1 root root 174 Aug 16 20:27 chatty.c
-rwxr-xr-x 1 root root 272588 Aug 16 20:34 chatty-packed
root@kali:~/126#
```

Detecting Packers with PEiD

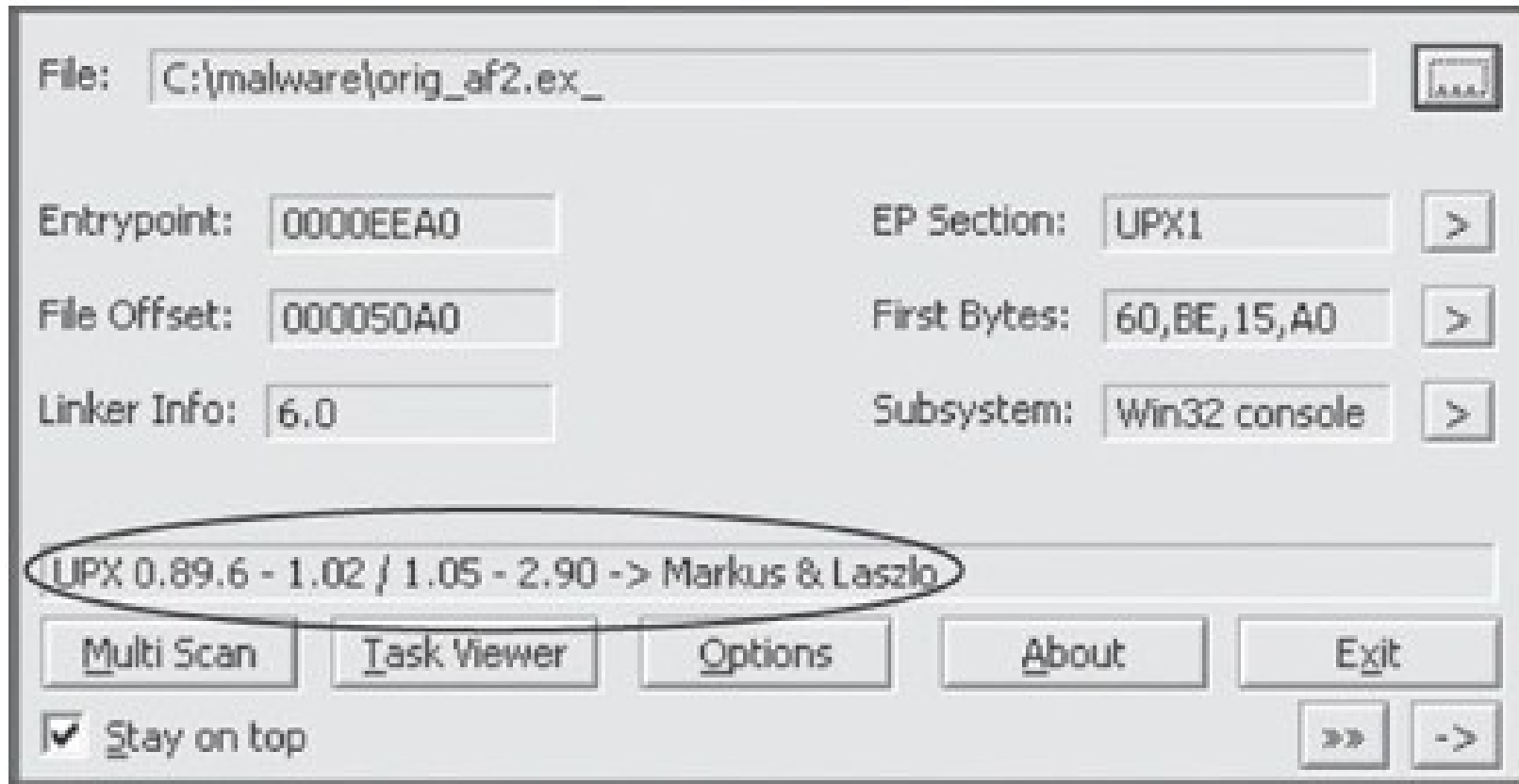
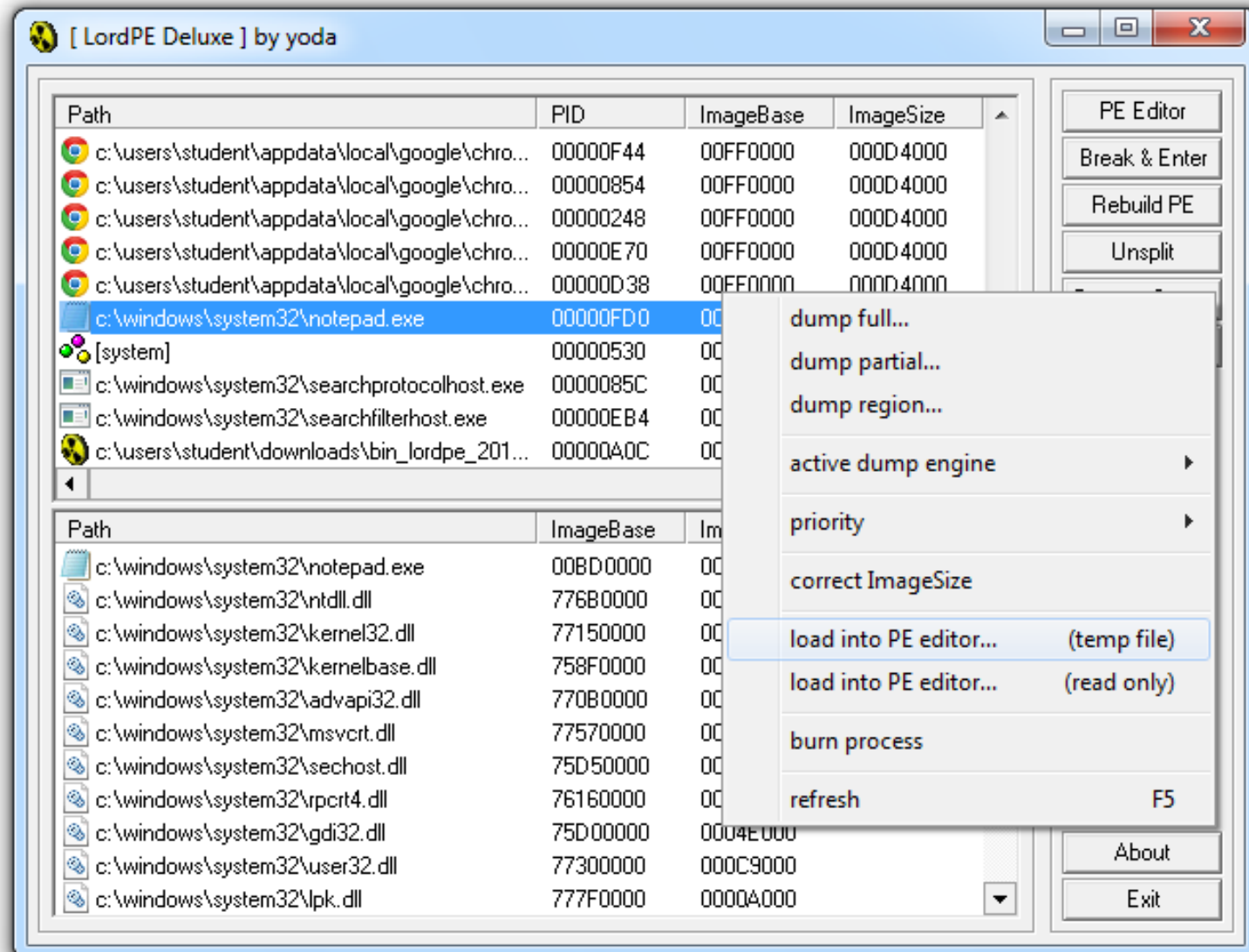


Figure 2-5. The PEiD program

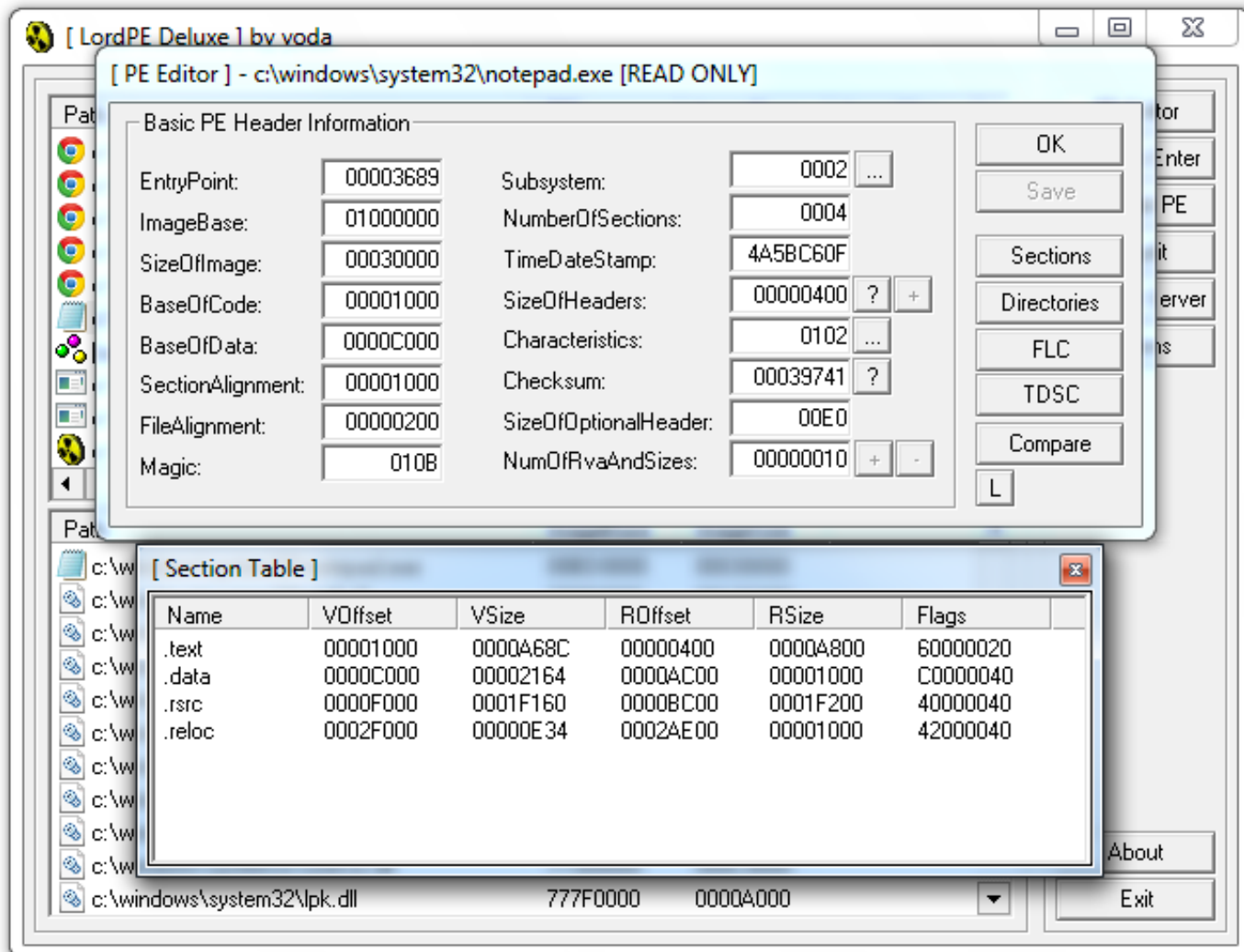
Portable Executable Files (PE Files)

- Là cấu trúc dữ liệu chứa thông tin cần thiết cho Windows để tải tệp
- Hầu hết các file thực thi trên windows định dạng file PE
- PE header:
 - + Chứa thông tin về code
 - + Loại ứng dụng
 - + Yêu cầu thư viện đi kèm
 - + Yêu cầu không gian bộ nhớ

LordPE Demo

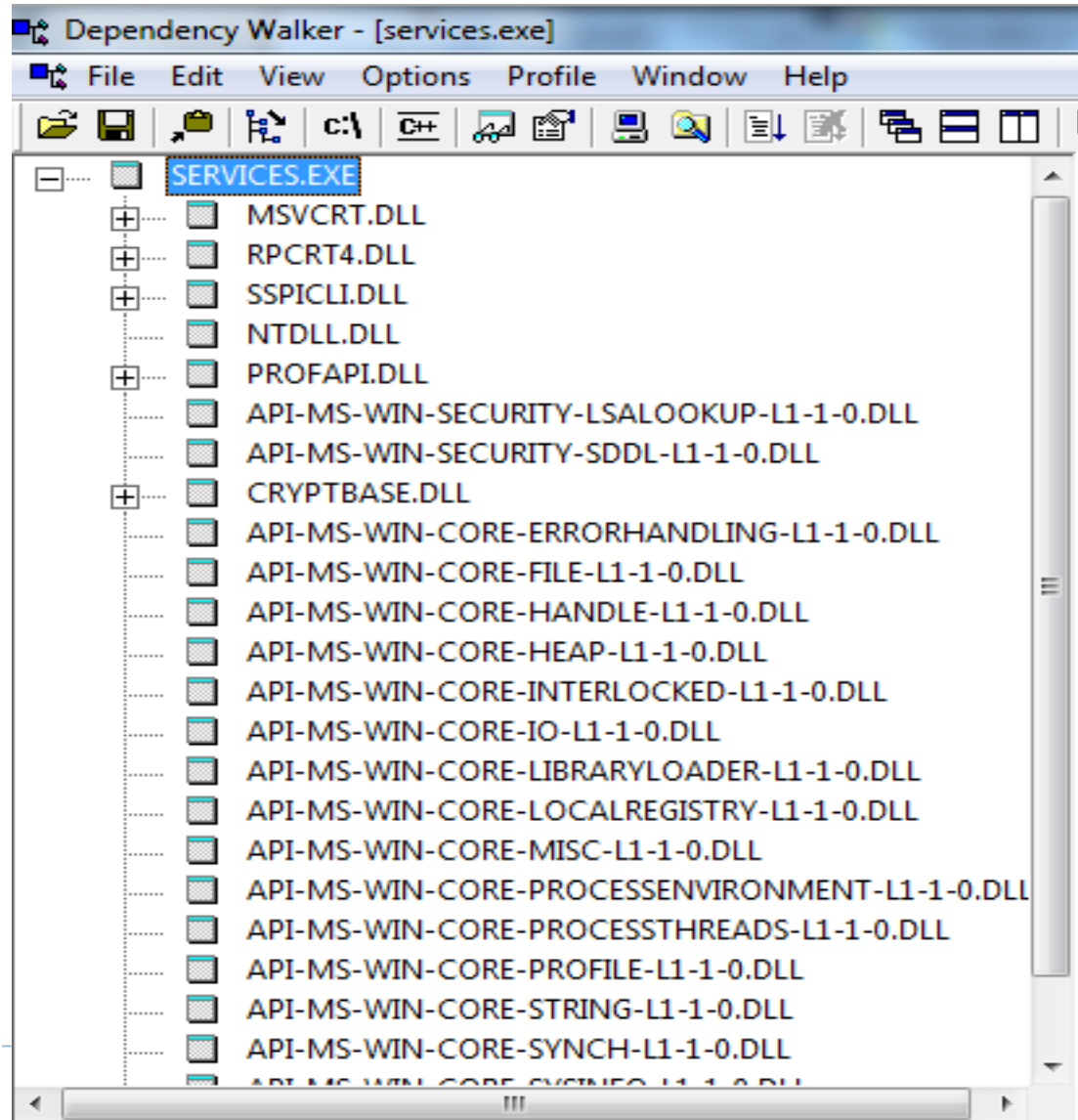


LordPE Demo



Dependency Walker

- Chương trình thông thường có nhiều DLLs
- Mã độc có ít DLLs



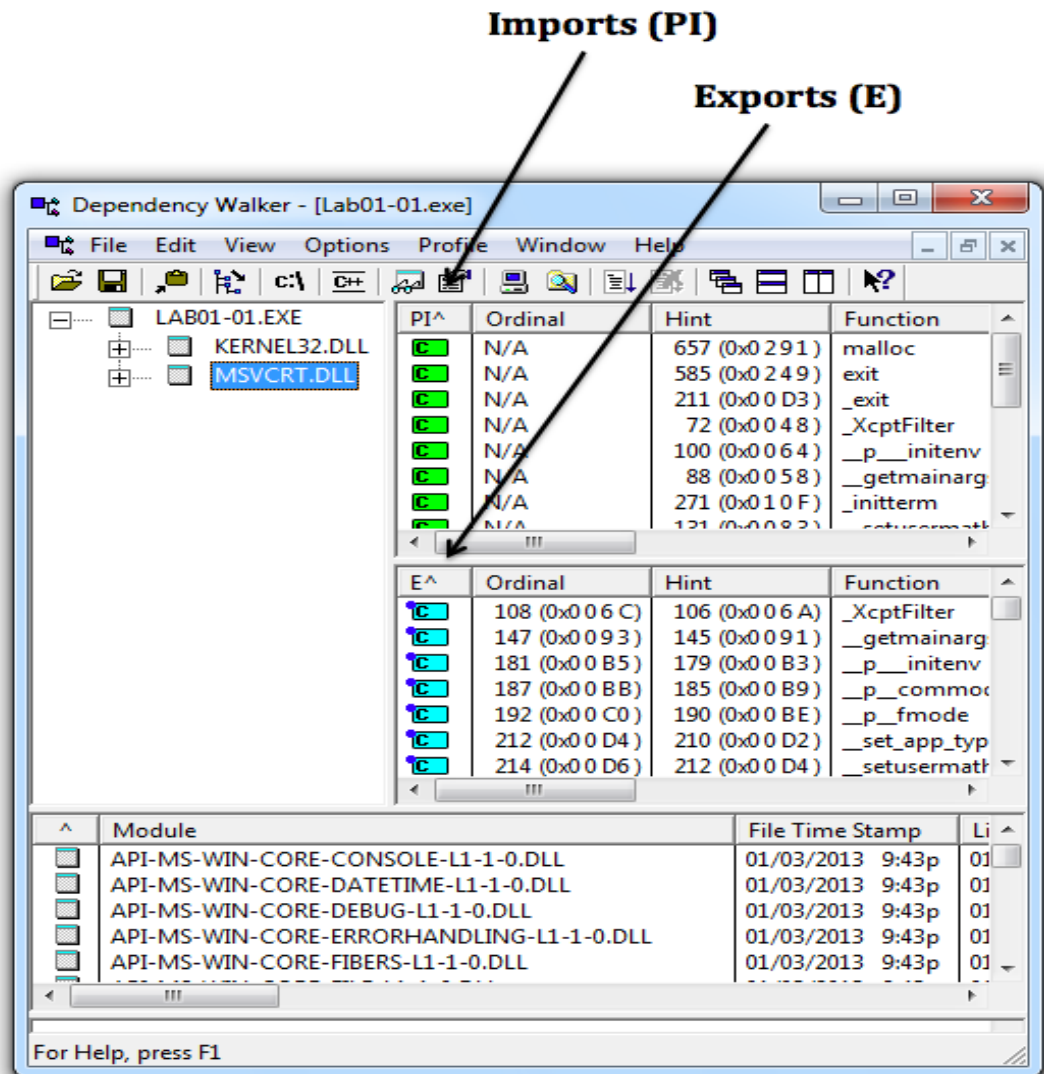
Dependency Walker

Ví dụ: file chứa mã
độc



Dependency Walker

Imports & Exports in Dependency Walker



Common DLLs

Table 2-1. Common DLLs

DLL	Description
<i>Kernel32.dll</i>	This is a very common DLL that contains core functionality, such as access and manipulation of memory, files, and hardware.
<i>Advapi32.dll</i>	This DLL provides access to advanced core Windows components such as the Service Manager and Registry.
<i>User32.dll</i>	This DLL contains all the user-interface components, such as buttons, scroll bars, and components for controlling and responding to user actions.
<i>Gdi32.dll</i>	This DLL contains functions for displaying and manipulating graphics.

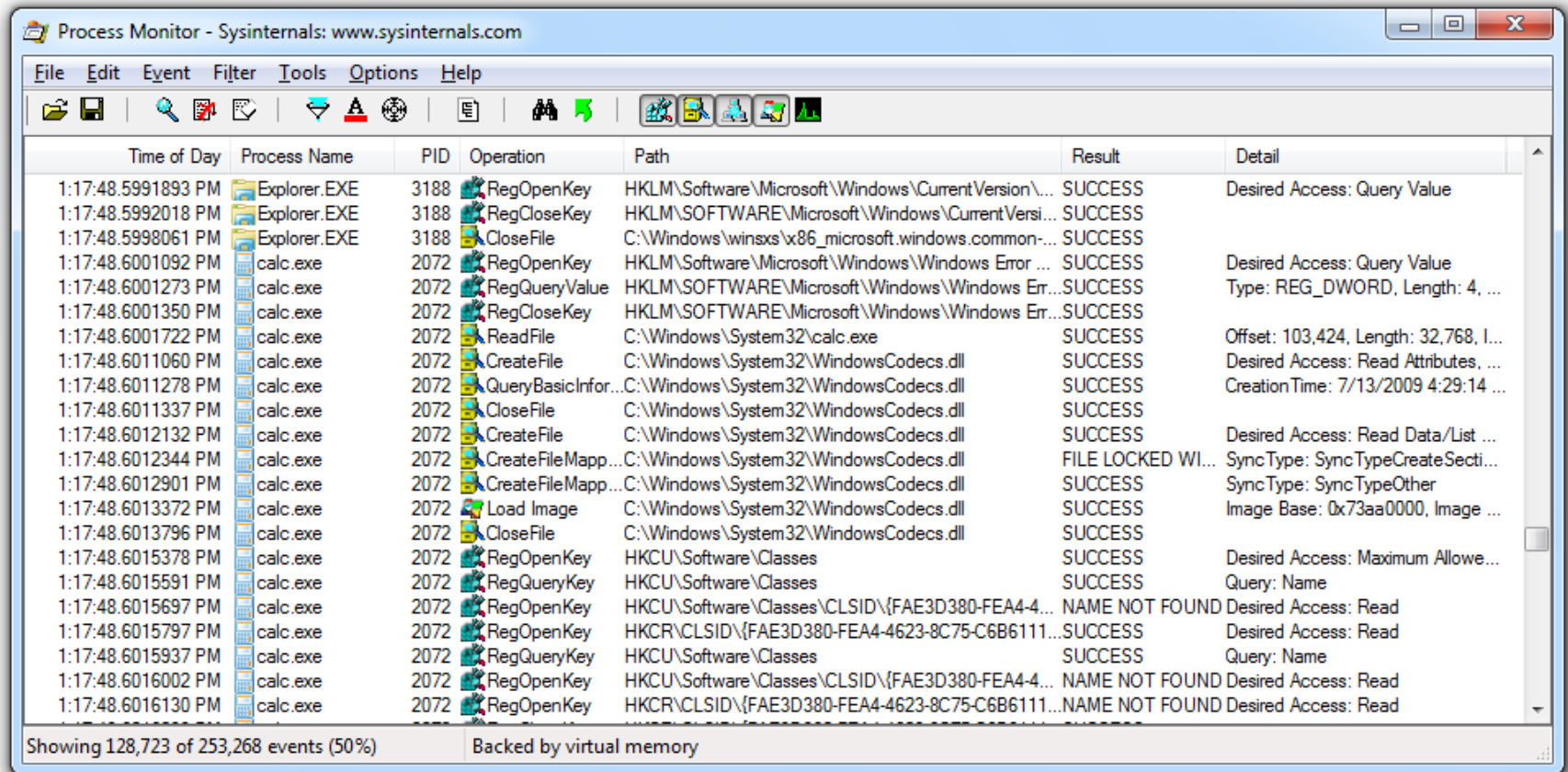
Common DLLs

Ntdll.dll This DLL is the interface to the Windows kernel. Executables generally do not import this file directly, although it is always imported indirectly by *Kernel32.dll*. If an executable imports this file, it means that the author intended to use functionality not normally available to Windows programs. Some tasks, such as hiding functionality or manipulating processes, will use this interface.

WSock32.dll These are networking DLLs. A program that accesses and either of these most likely connects to a network or
Ws2_32.dll performs network-related tasks.

Wininet.dll This DLL contains higher-level networking functions that implement protocols such as FTP, HTTP, and NTP.

Process Monitor



The screenshot shows the Process Monitor application window with the title bar 'Process Monitor - Sysinternals: www.sysinternals.com'. The menu bar includes File, Edit, Event, Filter, Tools, Options, and Help. The toolbar contains icons for file operations, search, and process management. The main table displays a list of events with columns for Time of Day, Process Name, PID, Operation, Path, Result, and Detail. The events are filtered to show only those from Explorer.EXE and calc.exe. The status bar at the bottom indicates 'Showing 128,723 of 253,268 events (50%)' and 'Backed by virtual memory'.

Time of Day	Process Name	PID	Operation	Path	Result	Detail
1:17:48.5991893 PM	Explorer.EXE	3188	RegOpenKey	HKLM\Software\Microsoft\Windows\CurrentVersion\...	SUCCESS	Desired Access: Query Value
1:17:48.5992018 PM	Explorer.EXE	3188	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersi...	SUCCESS	
1:17:48.5998061 PM	Explorer.EXE	3188	CloseFile	C:\Windows\winsxs\x86_microsoft.windows.common...	SUCCESS	
1:17:48.6001092 PM	calc.exe	2072	RegOpenKey	HKLM\Software\Microsoft\Windows\Windows Error ...	SUCCESS	Desired Access: Query Value
1:17:48.6001273 PM	calc.exe	2072	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\Windows Err...	SUCCESS	Type: REG_DWORD, Length: 4, ...
1:17:48.6001350 PM	calc.exe	2072	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows\Windows Err...	SUCCESS	
1:17:48.6001722 PM	calc.exe	2072	ReadFile	C:\Windows\System32\calc.exe	SUCCESS	Offset: 103,424, Length: 32,768, I...
1:17:48.6011060 PM	calc.exe	2072	CreateFile	C:\Windows\System32\WindowsCodecs.dll	SUCCESS	Desired Access: Read Attributes, ...
1:17:48.6011278 PM	calc.exe	2072	QueryBasicInfor...	C:\Windows\System32\WindowsCodecs.dll	SUCCESS	CreationTime: 7/13/2009 4:29:14 ...
1:17:48.6011337 PM	calc.exe	2072	CloseFile	C:\Windows\System32\WindowsCodecs.dll	SUCCESS	
1:17:48.6012132 PM	calc.exe	2072	CreateFile	C:\Windows\System32\WindowsCodecs.dll	SUCCESS	Desired Access: Read Data/List ...
1:17:48.6012344 PM	calc.exe	2072	CreateFileMapp...	C:\Windows\System32\WindowsCodecs.dll	FILE LOCKED WI...	SyncType: SyncTypeCreateSecti...
1:17:48.6012901 PM	calc.exe	2072	CreateFileMapp...	C:\Windows\System32\WindowsCodecs.dll	SUCCESS	SyncType: SyncTypeOther
1:17:48.6013372 PM	calc.exe	2072	Load Image	C:\Windows\System32\WindowsCodecs.dll	SUCCESS	Image Base: 0x73aa0000, Image ...
1:17:48.6013796 PM	calc.exe	2072	CloseFile	C:\Windows\System32\WindowsCodecs.dll	SUCCESS	
1:17:48.6015378 PM	calc.exe	2072	RegOpenKey	HKCU\Software\Classes	SUCCESS	Desired Access: Maximum Allowe...
1:17:48.6015591 PM	calc.exe	2072	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
1:17:48.6015697 PM	calc.exe	2072	RegOpenKey	HKCU\Software\Classes\CLSID\{FAE3D380-FEA4-4...	NAME NOT FOUND	Desired Access: Read
1:17:48.6015797 PM	calc.exe	2072	RegOpenKey	HKCR\CLSID\{FAE3D380-FEA4-4623-8C75-C6B6111...	SUCCESS	Desired Access: Read
1:17:48.6015937 PM	calc.exe	2072	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
1:17:48.6016002 PM	calc.exe	2072	RegOpenKey	HKCU\Software\Classes\CLSID\{FAE3D380-FEA4-4...	NAME NOT FOUND	Desired Access: Read
1:17:48.6016130 PM	calc.exe	2072	RegOpenKey	HKCR\CLSID\{FAE3D380-FEA4-4623-8C75-C6B6111...	NAME NOT FOUND	Desired Access: Read

Showing 128,723 of 253,268 events (50%) Backed by virtual memory

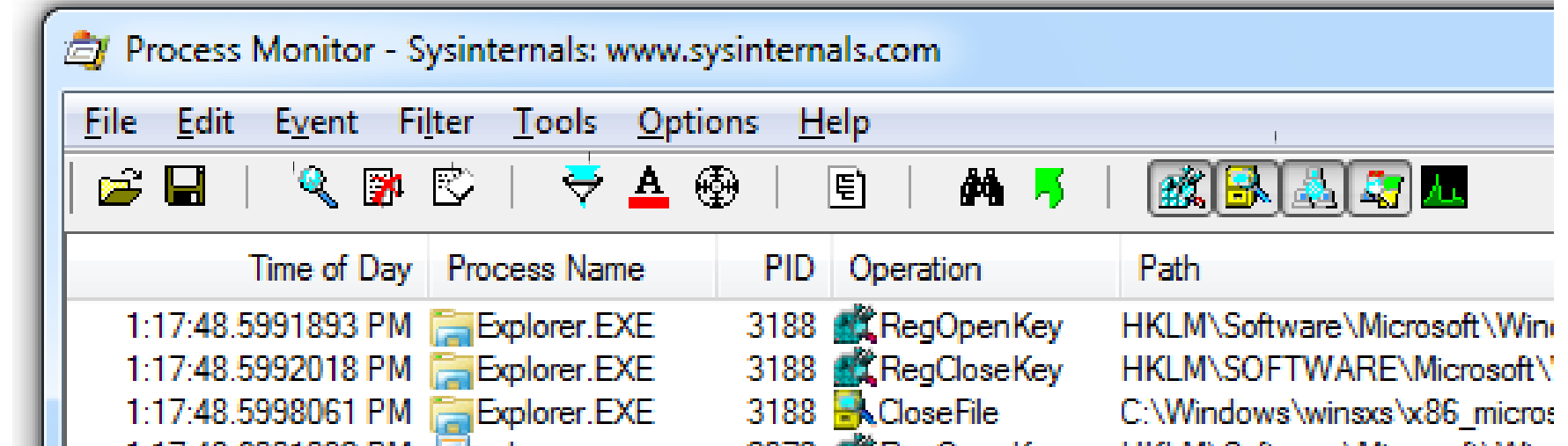
Process Monitor Toolbar

**Start/Stop
Capture**

Erase

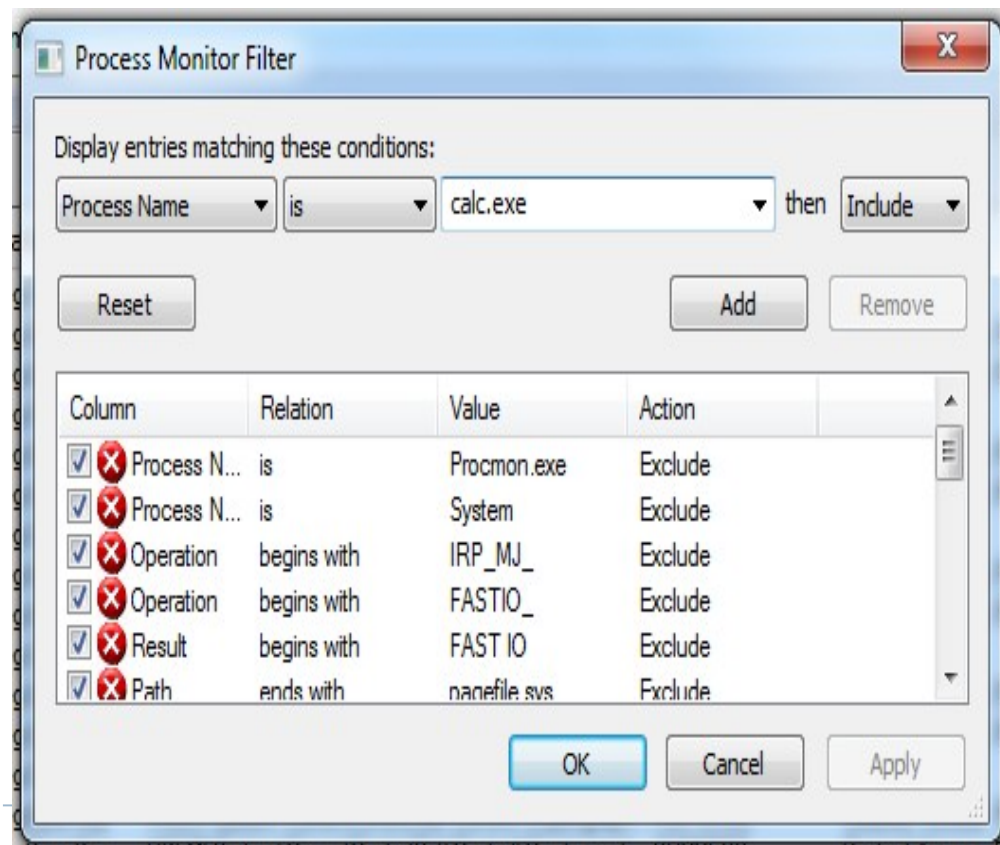
Filter

**Default Filters
Registry, File system, Network,
Processes**

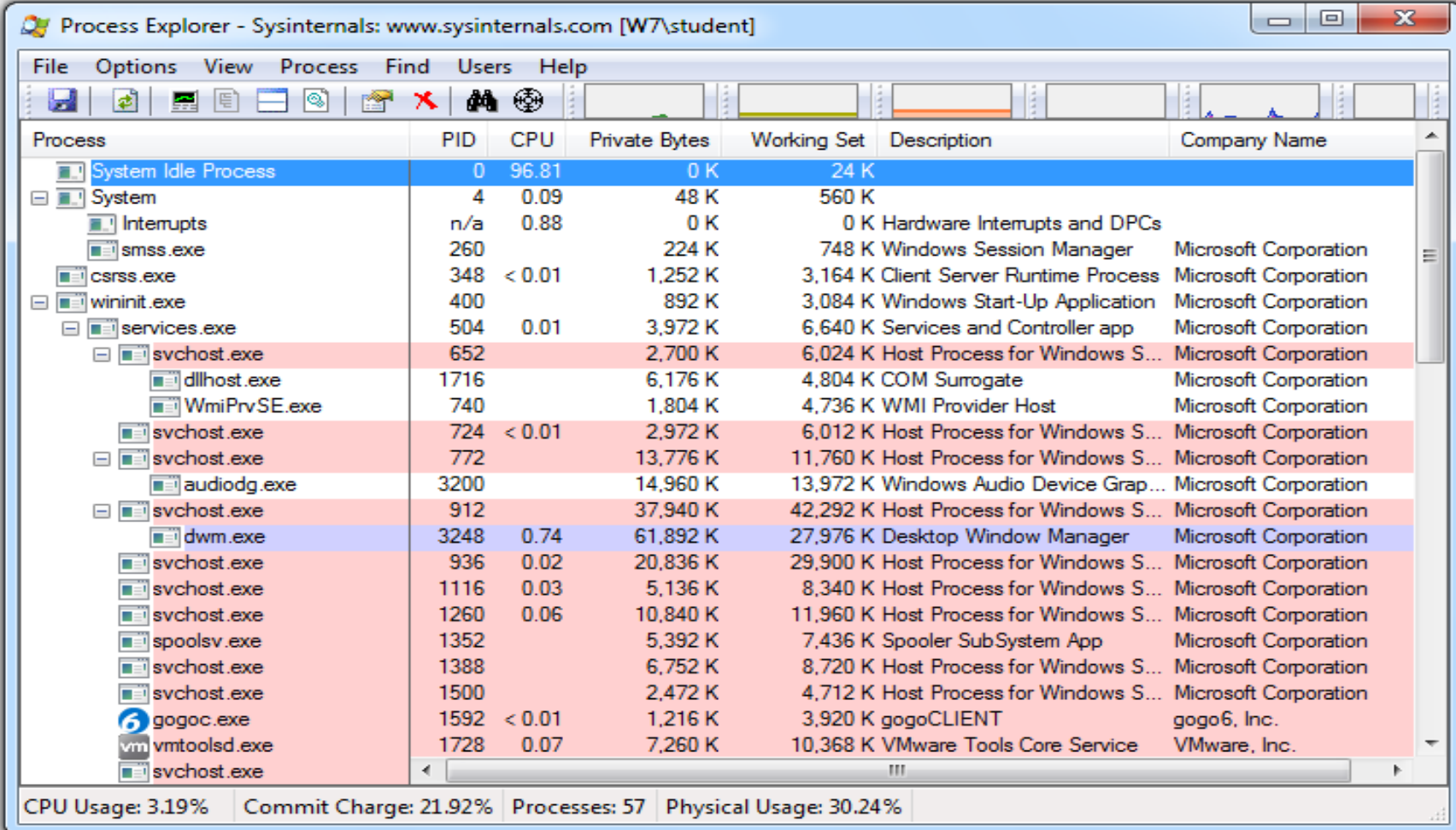


Filter with Include

- Right-click mỗi Process Name và click **Exclude**



Process Explorer



Process Explorer - Sysinternals: www.sysinternals.com [W7\student]

File Options View Process Find Users Help

Process	PID	CPU	Private Bytes	Working Set	Description	Company Name
System Idle Process	0	96.81	0 K	24 K		
System	4	0.09	48 K	560 K		
Interrupts	n/a	0.88	0 K	0 K	Hardware Interrupts and DPCs	
smss.exe	260		224 K	748 K	Windows Session Manager	Microsoft Corporation
csrss.exe	348	< 0.01	1,252 K	3,164 K	Client Server Runtime Process	Microsoft Corporation
wininit.exe	400		892 K	3,084 K	Windows Start-Up Application	Microsoft Corporation
services.exe	504	0.01	3,972 K	6,640 K	Services and Controller app	Microsoft Corporation
svchost.exe	652		2,700 K	6,024 K	Host Process for Windows S...	Microsoft Corporation
dllhost.exe	1716		6,176 K	4,804 K	COM Surrogate	Microsoft Corporation
WmiPrvSE.exe	740		1,804 K	4,736 K	WMI Provider Host	Microsoft Corporation
svchost.exe	724	< 0.01	2,972 K	6,012 K	Host Process for Windows S...	Microsoft Corporation
svchost.exe	772		13,776 K	11,760 K	Host Process for Windows S...	Microsoft Corporation
audiodg.exe	3200		14,960 K	13,972 K	Windows Audio Device Grap...	Microsoft Corporation
svchost.exe	912		37,940 K	42,292 K	Host Process for Windows S...	Microsoft Corporation
dwm.exe	3248	0.74	61,892 K	27,976 K	Desktop Window Manager	Microsoft Corporation
svchost.exe	936	0.02	20,836 K	29,900 K	Host Process for Windows S...	Microsoft Corporation
svchost.exe	1116	0.03	5,136 K	8,340 K	Host Process for Windows S...	Microsoft Corporation
svchost.exe	1260	0.06	10,840 K	11,960 K	Host Process for Windows S...	Microsoft Corporation
spoolsv.exe	1352		5,392 K	7,436 K	Spooler SubSystem App	Microsoft Corporation
svchost.exe	1388		6,752 K	8,720 K	Host Process for Windows S...	Microsoft Corporation
svchost.exe	1500		2,472 K	4,712 K	Host Process for Windows S...	Microsoft Corporation
gogoc.exe	1592	< 0.01	1,216 K	3,920 K	gogoCLIENT	gogo6, Inc.
vmtoolsd.exe	1728	0.07	7,260 K	10,368 K	VMware Tools Core Service	VMware, Inc.
svchost.exe						

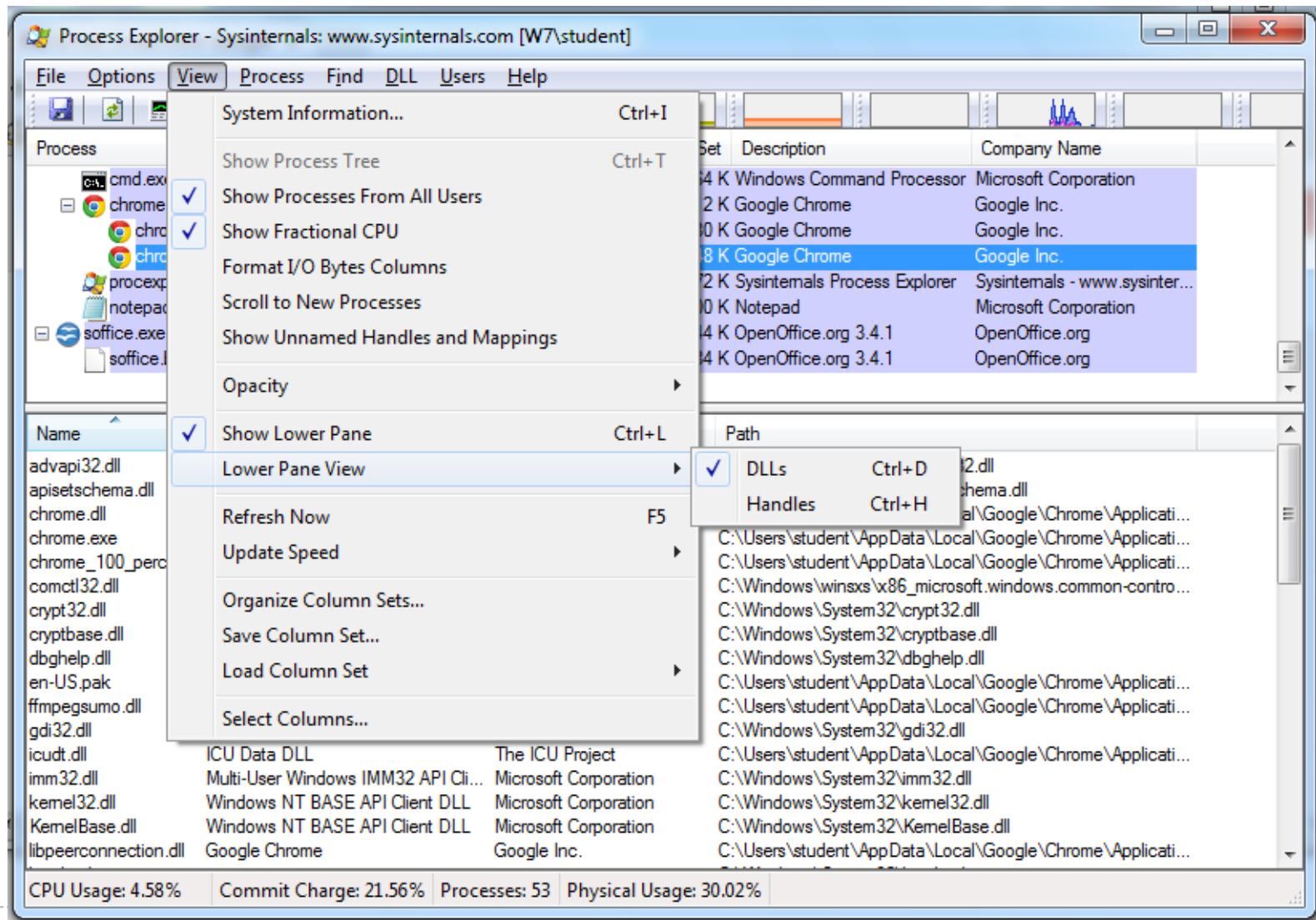
CPU Usage: 3.19% Commit Charge: 21.92% Processes: 57 Physical Usage: 30.24%

Process Explorer

Bôi màu:

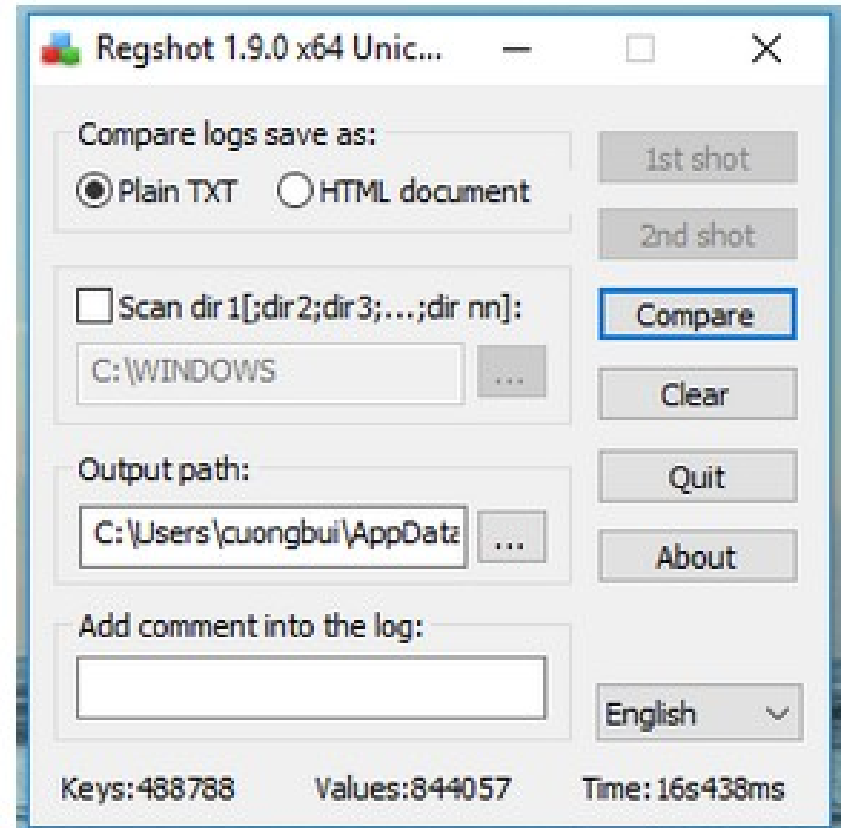
- Services are pink
- Processes are blue
- New processes are green briefly
- Terminated processes are red

Process Explorer - DLL mode



Regshot

Regshot cho phép so sánh nội dung Registry qua các bản ảnh được ghi lại. Các điểm khác biệt trên Registry có thể giúp chúng ta tìm ra những thông tin Registry bị thêm, sửa, xóa trong quá trình thực thi mã độc



Sử dụng Regshot để so sánh sự thay đổi trên hệ thống

Packet Sniffing with Wireshark

The image displays the Wireshark network protocol analyzer interface. The main window shows a list of captured packets, with a filter set to 'http'. The packet list includes various HTTP requests and responses, such as GET requests for images and HTML pages. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII. In the background, a web browser window is visible, showing the 'samsclass.info' website with the name 'Sam Bowne'.

Wireshark Interface Details:

- Filter: http
- Packet List (Selected: 1101):

No.	Time	Source	Destination	Protocol	Info
1101	7.515707	192.168.119.154	23.65.1.224	HTTP	GET /f.gif?_id=137745723/561
1106	7.537336	18.181.0.31	192.168.119.154	HTTP	HTTP/1.1 200 OK (PNG)
1108	7.557449	93.184.216.139	192.168.119.154	HTTP	[TCP Retransmission] Cont
1110	7.590291	23.65.1.224	192.168.119.154	HTTP	HTTP/1.1 200 OK (GIF89a)
1111	7.691258	23.65.1.224	192.168.119.154	HTTP	[TCP Retransmission] HTTP/
1189	36.858744	192.168.119.154	199.16.156.21	HTTP	GET /widgets/timelines/pag
1193	36.881799	192.168.119.154	199.16.156.21	HTTP	GET /widgets/timelines/pag
1196	36.954204	199.16.156.21	192.168.119.154	HTTP	HTTP/1.1 200 OK (applicat
1199	37.045979	199.16.156.21	192.168.119.154	HTTP	HTTP/1.1 200 OK (applicat
1369	96.750725	192.168.119.154	199.16.156.21	HTTP	GET /widgets/timelines/pag
1373	96.772892	192.168.119.154	199.16.156.21	HTTP	GET /widgets/timelines/pag
1376	96.846439	199.16.156.21	192.168.119.154	HTTP	HTTP/1.1 200 OK (applicat
1381	96.944497	199.16.156.21	192.168.119.154	HTTP	HTTP/1.1 200 OK (applicat
- Packet Details (Selected: 48):
 - Frame 48: 437 bytes on wire (3496 bits), 437 bytes captured (3496 bits)
 - Ethernet II, Src: Vmware_52:34:92 (00:0c:29:52:34:92), Dst: Vmware_e3:22:f1 (00:50:56:00:00:00)
 - Internet Protocol Version 4, Src: 192.168.119.154 (192.168.119.154), Dst: 141.101.11
- Packet Bytes: 0000 00 50 56 e3 22 f1 00 0c 29 52 34 92 08 00 45 00 .PV."...)R4...E. 0010 01 a7 10 25 40 00 80 06 00 00 c0 a8 77 9a 8d 65 ...%@...w...e 0020 75 98 05 a9 00 50 0c 80 cd 2e dc ff 73 93 50 18 u....P...S.P. 0030 fa f0 3c da 00 00 47 45 54 20 2f 20 48 54 54 50 ..<...GE T / HTTP 0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 73 61 6d 73 /1.1..Ho st: sams 0050 63 6c 61 73 73 2e 69 6e 66 6f 0d 0a 43 6f 6e 6e class.in fo..Conn 0060 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 ection: keep-ali 0070 76 65 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 ve..Acce pt: text 0080 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f /html,ap plicatio 0090 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c n/xhtml1+ xml,appl 00a0 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e ication/ xml:a=0.

Finding the Code in IDA Pro

Address	Length	Type	String
"..." .text:00...	00000F76	C
"..." .rdata:0...	00000014	C	YOURNAME-8a: %d %d\n
"..." .rdata:0...	0000001B	C	tack around the variable '
"..." .rdata:0...	00000011	C	'was corrupted.
"..." .rdata:0...	0000000E	C	he variable '

```
.rdata:00415858 ; char aYourname8aDD[]
.rdata:00415858 aYourname8aDD db 'YOURNAME-8a: %d %d',0Ah,0 ; DATA XREF: wmain+32fo
.rdata:0041586C align 10h
.rdata:00415870 a__native_start:
.rdata:00415870 unicode 0,
.rdata:004158C0 db 0
.rdata:004158C1 db 0
.rdata:004158C2 db 0
.rdata:004158C3 db 0
.rdata:004158C4 db 0
.rdata:004158C5 db 0
.rdata:004158C6 db 0
.rdata:004158C7 db 0
.rdata:004158C8 db 0
```

```
mov     eax, 0CCCCCCCCh
rep stosd
mov     [ebp+var_8], 2
mov     esi, esp
mov     eax, [ebp+var_8]
push    eax
mov     ecx, i
push    ecx
push    offset aYourname8aDD ; "YOURNAME-8a: %d %d\n"
call    ds:__imp_printf
```

HỎI VÀ ĐÁP