

HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA AN TOÀN THÔNG TIN

MODULE THỰC HÀNH
MÃ ĐỘC

BÀI THỰC HÀNH SỐ 03
Phân tích động cơ bản

Người thực hiện bài thực hành:

TS. Đặng Xuân Bảo

Hà Nội, 2020

MỤC LỤC

THÔNG TIN CHUNG VỀ BÀI THỰC HÀNH	3
CHUẨN BỊ BÀI THỰC HÀNH	4
PHÂN TÍCH ĐỘNG CƠ BẢN	5
1.1. Mô tả.....	5
1.2. Chuẩn bị.....	5
1.3. Phân tích động cơ bản.....	5
1.3.1. Đọc thông tin chung.....	5
1.3.2. Phân tích động cơ bản.....	6
1.3.2.1. Bật các công cụ phân tích	7
1.3.2.2. Chạy Lab03-01.exe và phân tích	10
Xử lý sự cố	Error! Bookmark not defined.

THÔNG TIN CHUNG VỀ BÀI THỰC HÀNH

Tên bài thực hành: Phân tích động cơ bản

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 Workstation 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.

PHÂN TÍCH ĐỘNG CƠ BẢN

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

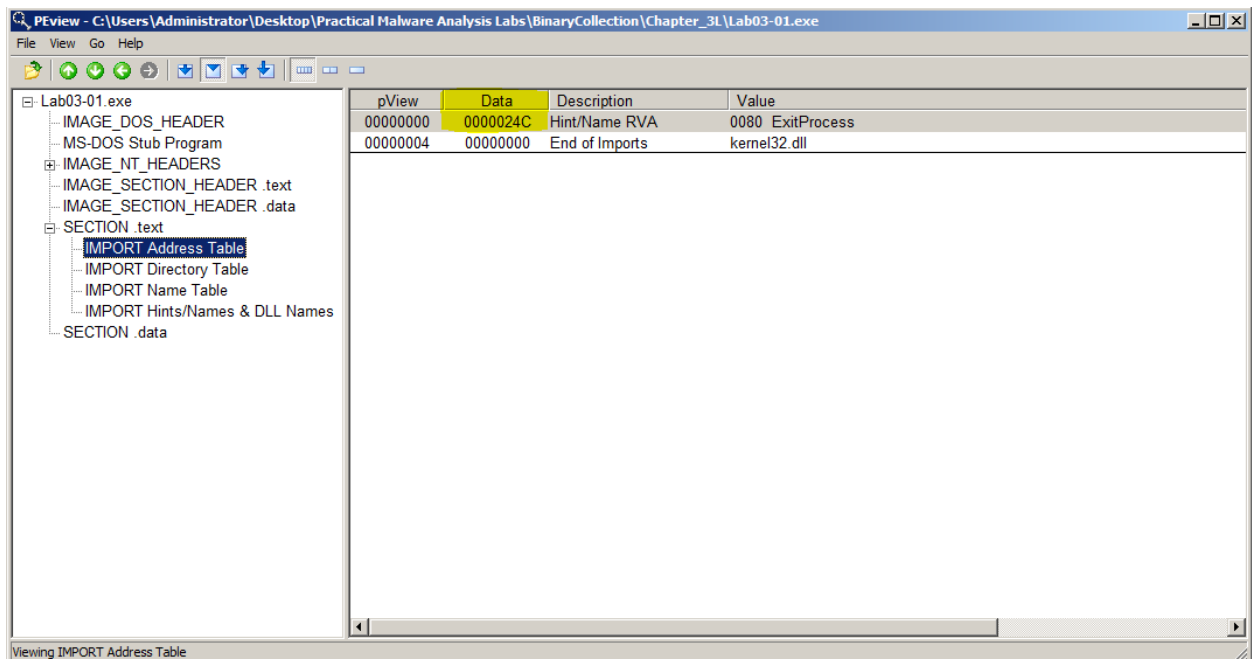
- Môi trường phân tích mã độc đã xây dựng trong Lab 1.

1.3. Phân tích động cơ bản

Tiến hành phân tích mẫu mã độc **Lab03-01.exe**.

1.3.1. Đọc thông tin chung

Đọc **Lab03-01.exe** với PView, trong phần IMPORT Address Table chỉ có giá trị kernel32.dll và hàm ExitProcess.

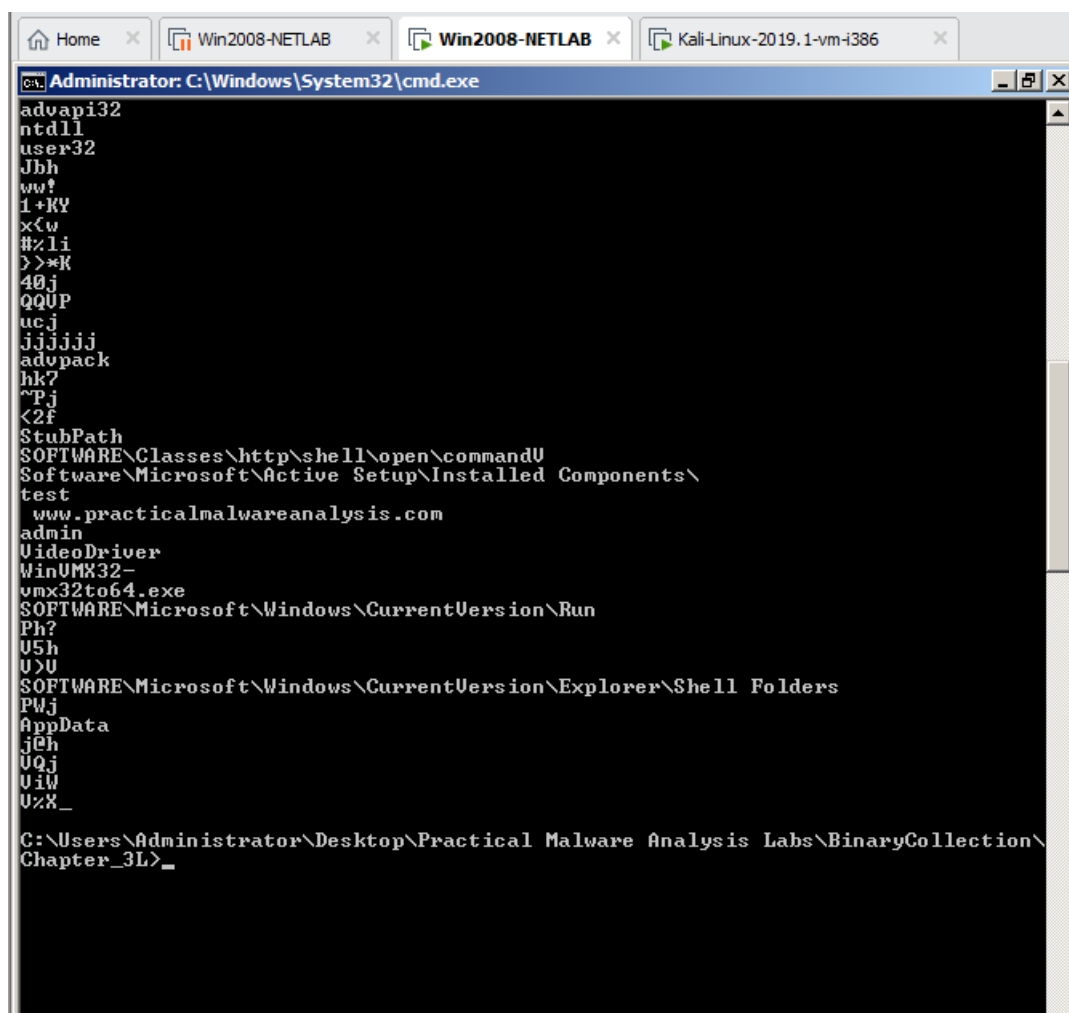


Sử dụng Strings kiểm tra các chuỗi trong **Lab03-01.exe**, lưu ý một số chuỗi sau:

- Vị trí đăng kí: SOFTWARE\Classes\http\shell\open\commandV
- URL: www.practicalmalwareanalysis.com
- VideoDriver

Lưu ý: Nếu mã độc bị nén, các chuỗi sẽ không đọc được.

Trên "advpack" có một chuỗi bắt đầu bằng "j".



```
Administrator: C:\Windows\System32\cmd.exe
advapi32
ntdll
user32
Jbh
ww?
1+KY
x<w
#%li
>>*K
40j
QQUP
ucj
jjjjjj
advpack
hk?
^Pj
<2f
StubPath
SOFTWARE\Classes\http\shell\open\commandU
Software\Microsoft\Active Setup\Installed Components\
test
www.practicalmalwareanalysis.com
admin
VideoDriver
WinUMX32-
vmx32to64.exe
SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Ph?
U5h
U>U
SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
PWj
AppData
jch
UQj
UiW
U%X_
C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\
Chapter_3L>_
```

1.3.2. Phân tích động cơ bản

Các bước chung để tiến hành phân tích động bao gồm

- Bật các công cụ phân tích động

- Chạy mã độc và sử dụng các công cụ phân tích để theo dõi hoạt động của mã độc

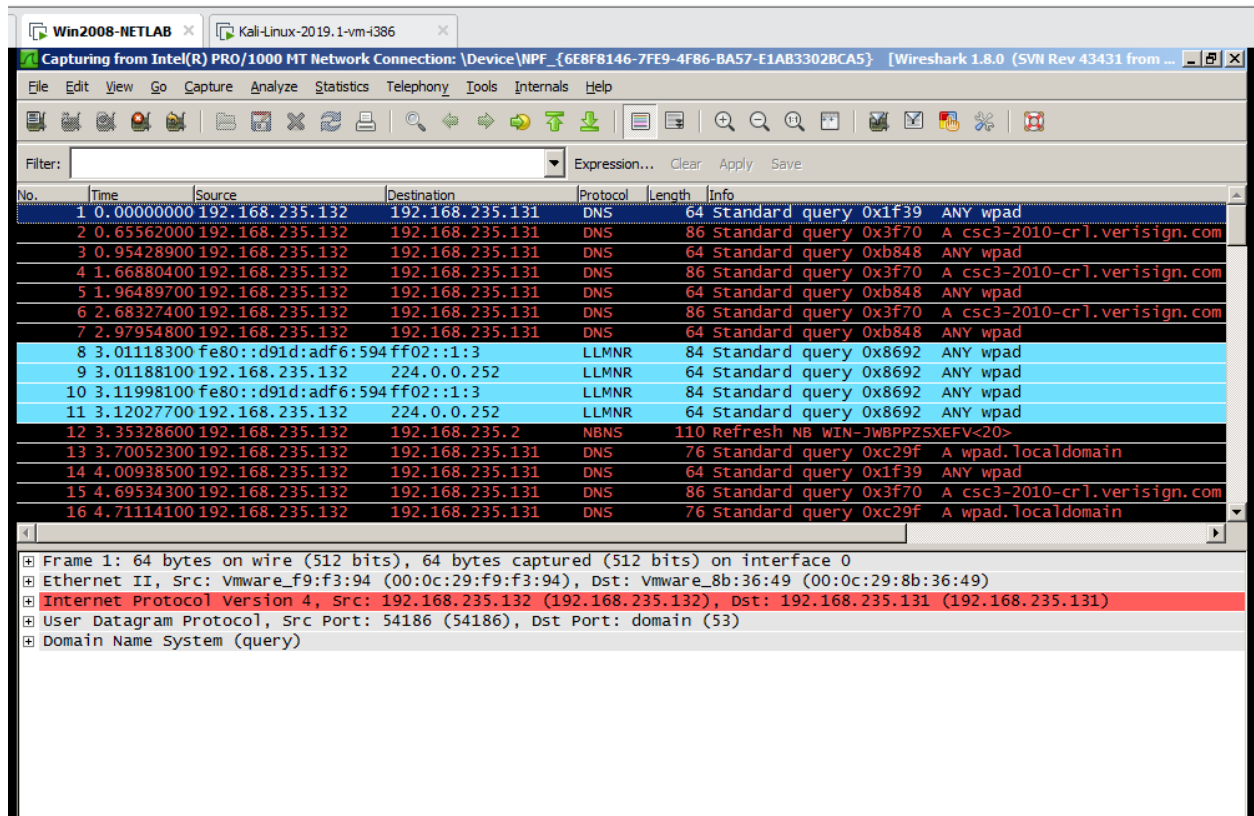
1.3.2.1. Bật các công cụ phân tích

Bật Process Explorer:

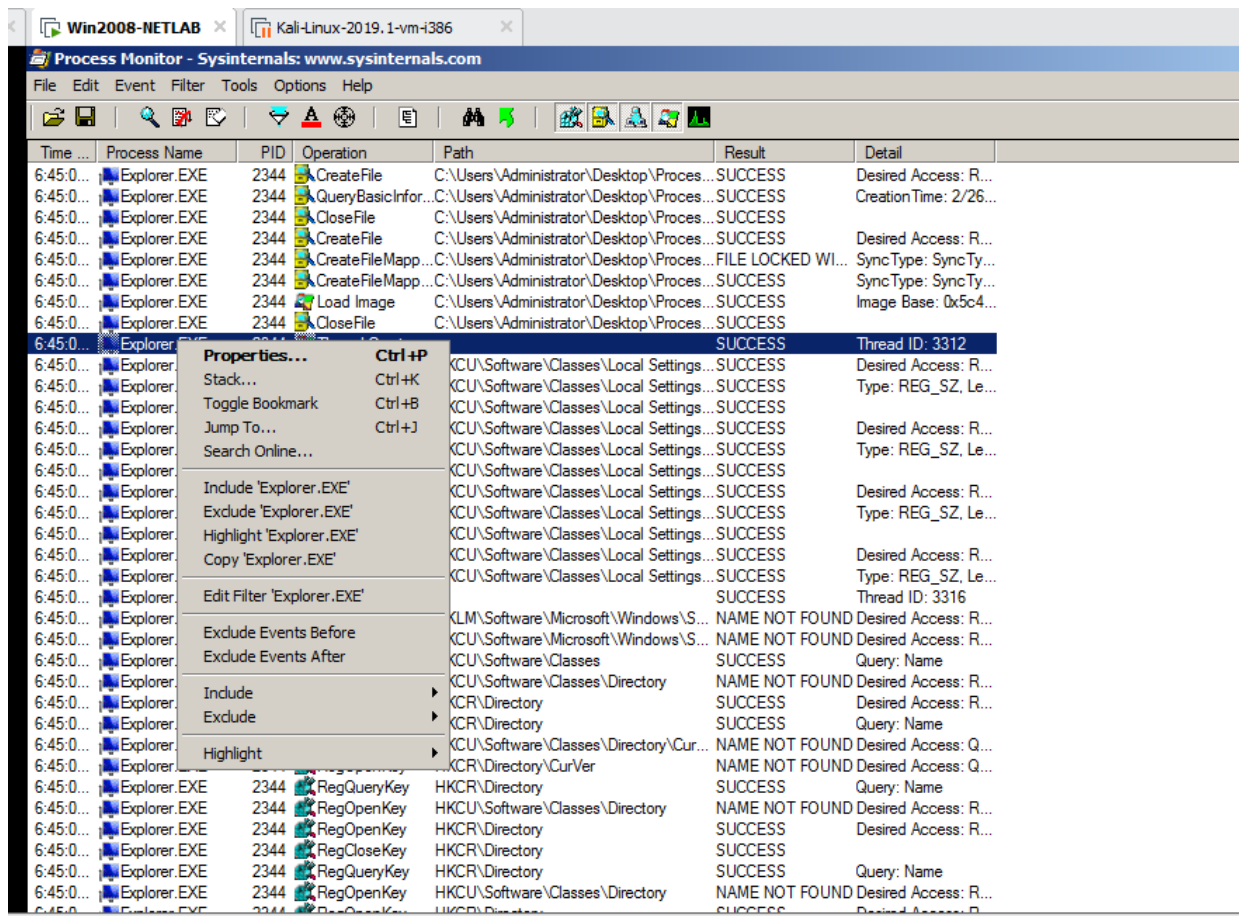
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	99.62	0 K	24 K	0		
System		0 K	3,032 K	4		
Interrupts	< 0.01	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		344 K	776 K	436	Windows Session Manager	Microsoft Corporation
csrss.exe		1,664 K	4,924 K	504	Client Server Runtime Process	Microsoft Corporation
csrss.exe	< 0.01	9,328 K	10,960 K	548	Client Server Runtime Process	Microsoft Corporation
wininit.exe		1,260 K	3,952 K	556	Windows Start-Up Application	Microsoft Corporation
services.exe		3,108 K	7,164 K	628	Services and Controller app	Microsoft Corporation
svchost.exe		3,308 K	6,656 K	808	Host Process for Windows S...	Microsoft Corporation
WmiPrvSE.exe		3,536 K	6,292 K	3752	WMI Provider Host	Microsoft Corporation
WmiPrvSE.exe		4,424 K	8,516 K	2912	WMI Provider Host	Microsoft Corporation
svchost.exe		3,172 K	6,532 K	868	Host Process for Windows S...	Microsoft Corporation
svchost.exe		6,804 K	8,336 K	960	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,976 K	4,948 K	988	Host Process for Windows S...	Microsoft Corporation
svchost.exe		20,408 K	26,004 K	1012	Host Process for Windows S...	Microsoft Corporation
taskeng.exe		2,120 K	5,892 K	1440	Task Scheduler Engine	Microsoft Corporation
taskeng.exe		3,048 K	7,528 K	2268	Task Scheduler Engine	Microsoft Corporation
wuauclt.exe		2,696 K	5,164 K	3560	Windows Update Automatic ...	Microsoft Corporation
SLsvc.exe		5,820 K	9,936 K	1024	Microsoft Software Licensing...	Microsoft Corporation
svchost.exe	< 0.01	8,016 K	12,812 K	1072	Host Process for Windows S...	Microsoft Corporation
svchost.exe		5,860 K	9,156 K	1124	Host Process for Windows S...	Microsoft Corporation
dmw.exe		1,452 K	4,136 K	2304	Desktop Window Manager	Microsoft Corporation
svchost.exe		14,332 K	16,072 K	1160	Host Process for Windows S...	Microsoft Corporation
svchost.exe		6,748 K	10,684 K	1340	Host Process for Windows S...	Microsoft Corporation
spoolsv.exe	< 0.01	6,200 K	10,616 K	1568	Spooler SubSystem App	Microsoft Corporation
ftpbasicssvr.exe	< 0.01	1,032 K	3,212 K	1632		
svchost.exe		1,736 K	4,908 K	1760	Host Process for Windows S...	Microsoft Corporation
svchost.exe		904 K	2,880 K	1776	Host Process for Windows S...	Microsoft Corporation
vmtoolsd.exe	< 0.01	8,628 K	14,324 K	1868	VMware Tools Core Service	VMware, Inc.
svchost.exe		632 K	2,304 K	1932	Host Process for Windows S...	Microsoft Corporation
dmhst.exe	< 0.01	6,236 K	12,668 K	1248	COM Surrogate	Microsoft Corporation
msdtc.exe	< 0.01	3,040 K	7,252 K	1920	MS DTCconsole program	Microsoft Corporation
lsass.exe		4,236 K	9,204 K	648	Local Security Authority Proc...	Microsoft Corporation

Bật Wireshark

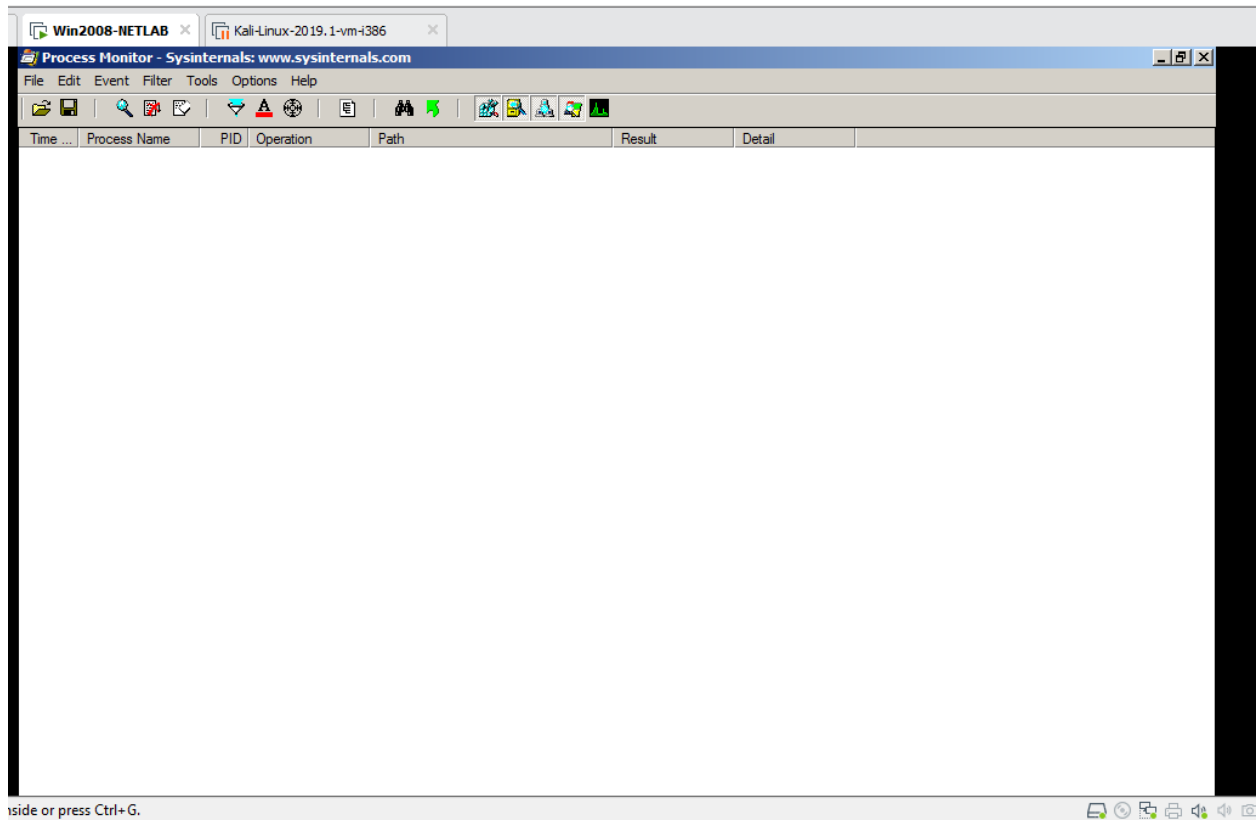
Khởi động Wireshark và bắt đầu chụp các gói từ giao diện đi đến máy Linux, thường là "Local Area Connection".



Bật Process Monitor



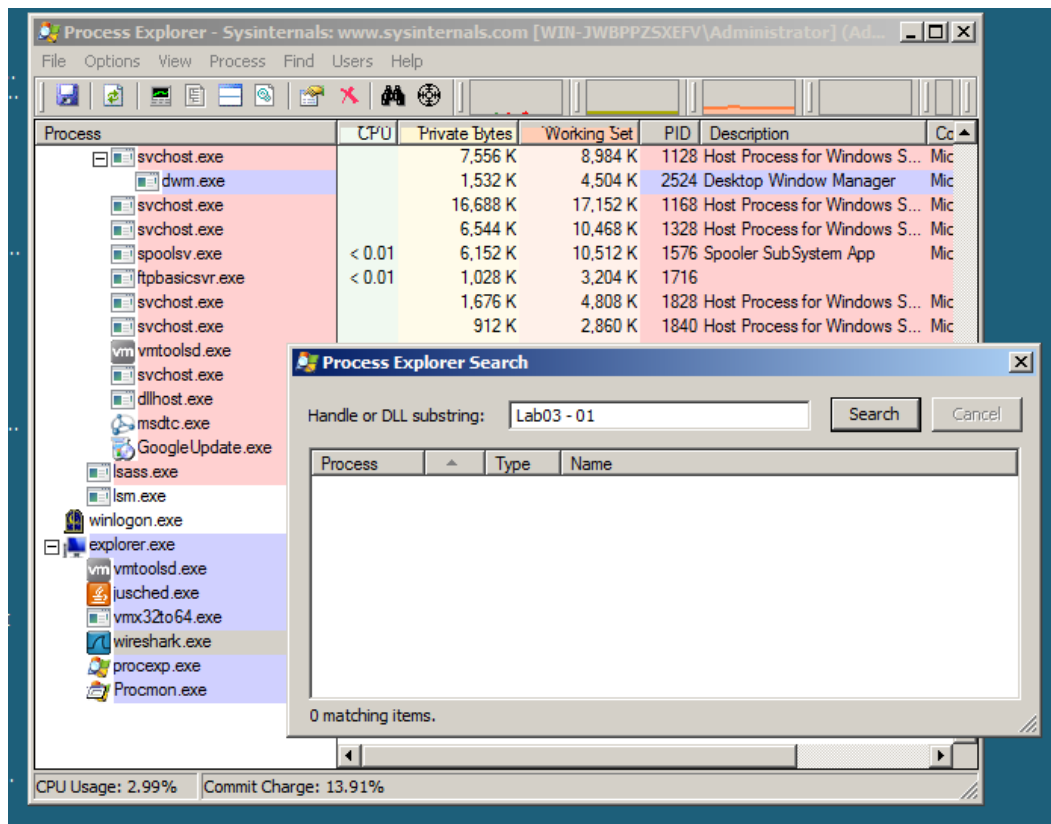
Trong Process Monitor, bấm chuột phải vào tên của một trong các tiến trình đang chạy, chọn Exclude “Explorer.exe” để loại trừ tiến trình này khỏi danh sách quan sát. Tiến hành loại trừ tất cả các tiến trình đang chạy.



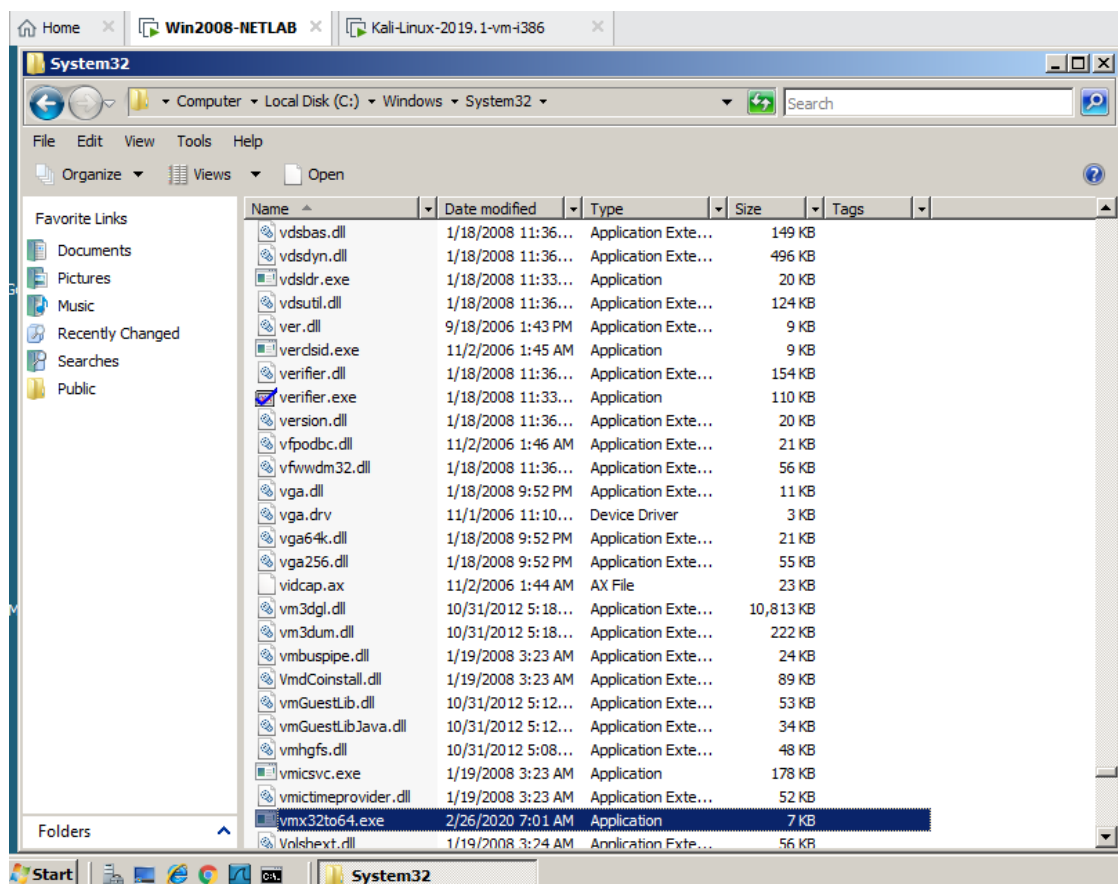
1.3.2.2. Chạy Lab03-01.exe và phân tích

Cho mã độc Lab03-01.exe khởi chạy.

Trong Process Explorer, ở khung trên cùng, tìm Lab03-01.exe.



Nếu tiến trình Lab03-01.exe không xuất hiện trong Process Explorer, điều đó có thể có nghĩa là phần mềm độc hại đã được chạy trên VM này. Để làm cho phần mềm độc hại chạy lại đúng cách, khởi động lại VM, nhấn F8, vào Chế độ Safe Mode và xóa tệp này: C:\Windows\System32\vmx32to64.exe (có thể xóa trực tiếp rồi khởi động lại máy ảo).



Sau đó khởi động lại VM ở chế độ bình thường.

Trong Process Explorer, bấm View, "Lower Pane View", Handles.

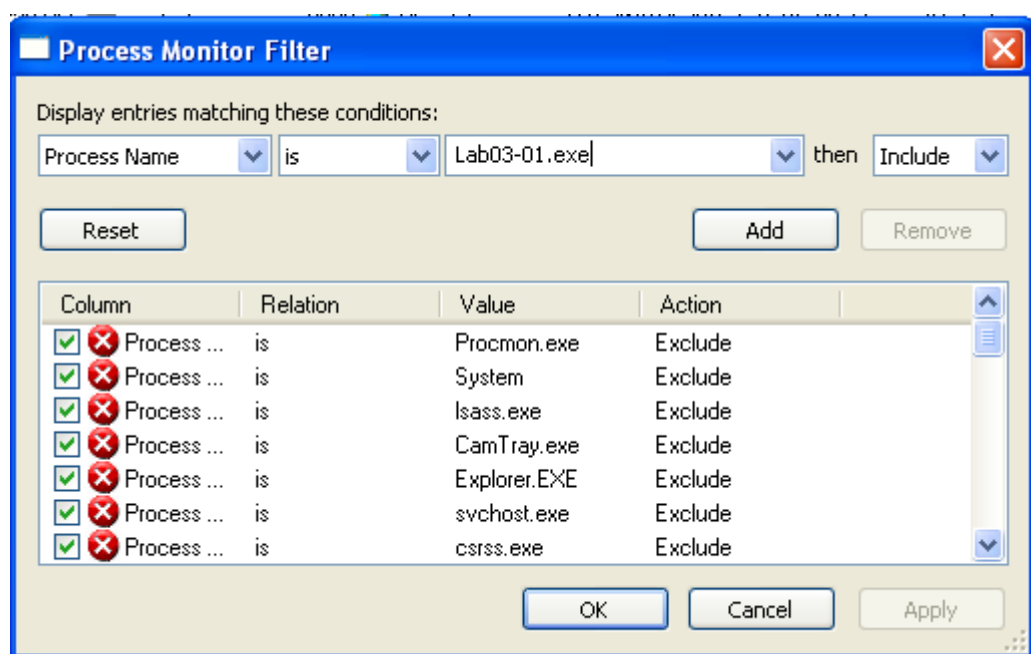
Đọc và giải thích các kết quả hiện ra trong Lower Pane của Process Explorer

Xem các quy trình độc hại trong Process Monitor

Trong Process Monitor, nhấp vào biểu tượng kính lúp trên thanh công cụ để dừng chụp sự kiện

Trong Process Monitor, chọn **Filter, Filter**. Nhập bộ lọc cho "**Process Name**" là **Lab03-01.exe**, Include, như hình dưới đây

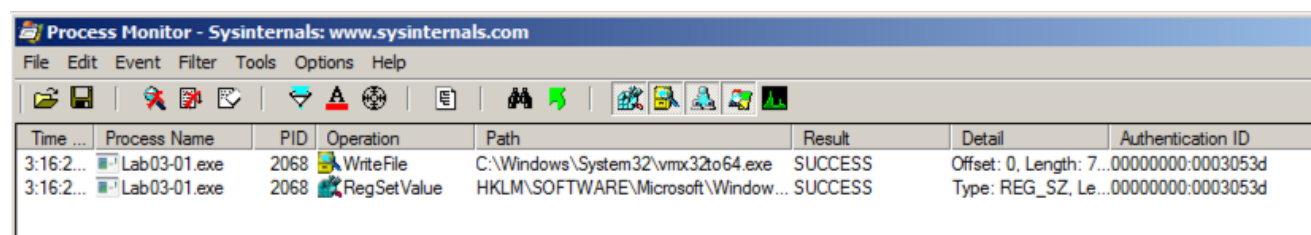
Chọn **Add** để thêm bộ lọc.



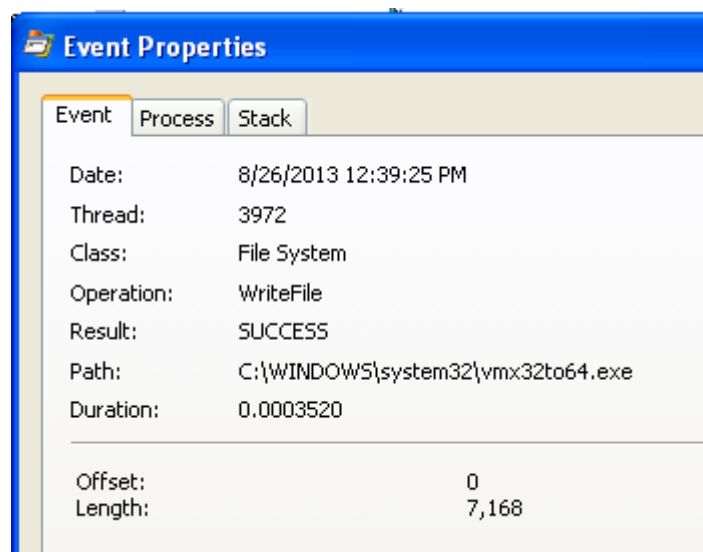
Thêm 2 bộ lọc:

- **Operation of RegSetValue**
- **Operation of WriteFile**

Nếu sử dụng Windows XP có thêm 8 sự kiện với đường dẫn kết thúc bằng "Cryptography\RNG\Seed".



Nháy đúp vào sự kiện với đường dẫn kết thúc bằng **vmx32to64.exe**. Bảng Properties cho thấy rằng sự kiện này tạo ra một tệp có tên **vmx32to64.exe**, như hiển thị bên dưới: sự kiện này đã sao chép phần mềm độc hại vào một tệp có tên **vmx32to64.exe**, do đó tên tệp là một dấu hiệu nhận biết hữu ích.



Bấm đúp vào với một Đường dẫn kết thúc bằng **VideoDriver**.

Hành động này tạo ra một khóa Run mới trong sổ đăng ký có tên "VideoDriver" với giá trị "C:\WINDOWS\system32\vmx32to64.exe" - giúp mã độc khởi chạy khi máy khởi động lại.

Xem nhật ký INetSim

Trên máy Kali Linux, bấm vào cửa sổ đang chạy inetsim.

Nhấn tổ hợp **Ctrl+C**. Một thông báo xuất hiện cho bạn biết tệp Report nằm ở đâu, như hiển thị bên dưới:


```

* daytime_13_udp - stopped (PID 3404)
* daytime_13_tcp - stopped (PID 3403)
* time_37_udp - stopped (PID 3402)
* time_37_tcp - stopped (PID 3401)
* pop3s_995_tcp - stopped (PID 3392)
* syslog_514_udp - stopped (PID 3400)
* ident_113_tcp - stopped (PID 3399)
* finger_79_tcp - stopped (PID 3398)
* ntp_123_udp - stopped (PID 3397)
* ftps_990_tcp - stopped (PID 3394)
* ftp_21_tcp - stopped (PID 3393)
* pop3_110_tcp - stopped (PID 3391)
* smtps_465_tcp - stopped (PID 3390)
* smtp_25_tcp - stopped (PID 3389)
* https_443_tcp - stopped (PID 3388)
* http_80_tcp - stopped (PID 3387)
* dns_53_tcp_udp - stopped (PID 3386)
* tftp_69_udp - stopped (PID 3395)
* irc_6667_tcp - stopped (PID 3396)
Simulation stopped.
Report written to '/var/log/inetsim/report/report.3384.txt'
=== INetSim main process stopped (PID 3384) ===

```

Trong máy Linux, thực hiện lệnh thay thế "report.3384.txt" bằng tên sinh viên.

nano /var/log/inetsim/report/report.3384.txt

Cuộn xuống phía dưới sẽ thấy các kết nối DNS tới **www.practicalmalwareanalysis.com**:

```

GNU nano 2.2.6      File: /var/log/inetsim/report/report.3384.txt
2013-08-26 15:39:05 DNS connection, type: AAAA, class: IN, requested name: tools.google.com.localdomain
2013-08-26 15:39:05 DNS connection, type: A, class: IN, requested name: tools.google.com
2013-08-26 15:39:05 HTTP connection, method: POST, URL: http://tools.google.com/service/update2?v=6:SUuBTQoZakwr$
2013-08-26 15:39:05 DNS connection, type: A, class: IN, requested name: wpad.localdomain
2013-08-26 15:39:05 DNS connection, type: PTR, class: IN, requested name: 255.255.255.255.in-addr.arpa
2013-08-26 15:39:05 DNS connection, type: PTR, class: IN, requested name: 254.119.168.192.in-addr.arpa
2013-08-26 15:39:10 HTTP connection, method: POST, URL: http://tools.google.com/service/update2?v=6:Jzw2L3wWgF-d$
2013-08-26 15:39:25 DNS connection, type: A, class: IN, requested name: www.practicalmalwareanalysis.com
2013-08-26 15:41:20 DNS connection, type: PTR, class: IN, requested name: 255.119.168.192.in-addr.arpa
2013-08-26 15:42:32 DNS connection, type: PTR, class: IN, requested name: 1.119.168.192.in-addr.arpa
2013-08-26 15:51:55 DNS connection, type: A, class: IN, requested name: www.practicalmalwareanalysis.com
2013-08-26 16:06:55 DNS connection, type: A, class: IN, requested name: www.practicalmalwareanalysis.com
2013-08-26 16:06:55 Last simulated date in log file

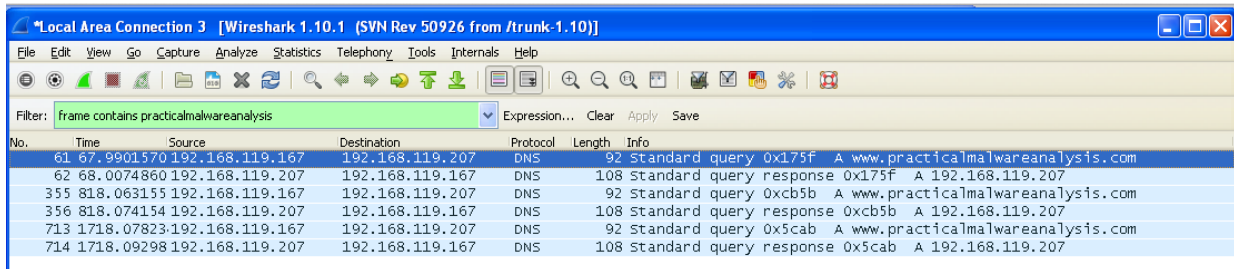
```

Xem các kết nối mạng trong Wireshark

Trong máy Windows (hoặc Kali linux), trong Wireshark, chọn **Capture, Stop**.

Ở phía trên bên trái của cửa sổ Wireshark, trong Filter, nhập bộ lọc của khung chứa **practicalmalwareanalysis**

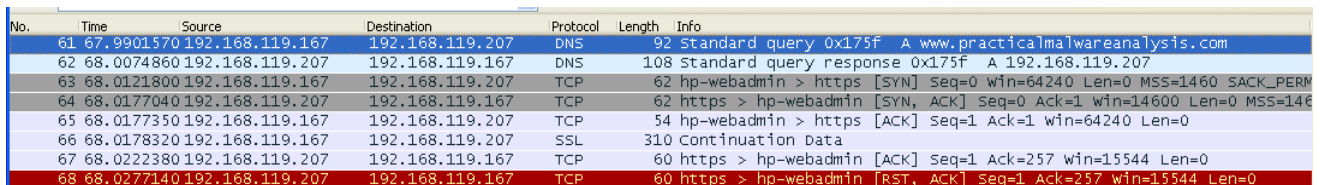
Nhấn Enter để xem các gói được lọc, như hiển thị bên dưới.



No.	Time	Source	Destination	Protocol	Length	Info
61	67.9901570	192.168.119.167	192.168.119.207	DNS	92	Standard query 0x175f A www.practicalmalwareanalysis.com
62	68.0074860	192.168.119.207	192.168.119.167	DNS	108	Standard query response 0x175f A 192.168.119.207
355	818.063155	192.168.119.167	192.168.119.207	DNS	92	Standard query 0xcb5b A www.practicalmalwareanalysis.com
356	818.074154	192.168.119.207	192.168.119.167	DNS	108	Standard query response 0xcb5b A 192.168.119.207
713	1718.07823	192.168.119.167	192.168.119.207	DNS	92	Standard query 0x5cab A www.practicalmalwareanalysis.com
714	1718.09298	192.168.119.207	192.168.119.167	DNS	108	Standard query response 0x5cab A 192.168.119.207

Nhập vào dòng hiển thị yêu cầu DNS đầu tiên cho `www.practicalmalwareanalysis.com` -- trong ví dụ trên, nó là gói 61.

Ở phần trên cùng của Wireshark, nhấp vào nút Clear để xóa bộ lọc. Các gói theo yêu cầu DNS xuất hiện, như hiển thị bên dưới.



No.	Time	Source	Destination	Protocol	Length	Info
61	67.9901570	192.168.119.167	192.168.119.207	DNS	92	Standard query 0x175f A www.practicalmalwareanalysis.com
62	68.0074860	192.168.119.207	192.168.119.167	DNS	108	Standard query response 0x175f A 192.168.119.207
63	68.0121800	192.168.119.167	192.168.119.207	TCP	62	hp-webadmin > https [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
64	68.0177040	192.168.119.207	192.168.119.167	TCP	62	https > hp-webadmin [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460
65	68.0177350	192.168.119.167	192.168.119.207	TCP	54	hp-webadmin > https [ACK] Seq=1 Ack=1 Win=64240 Len=0
66	68.0178320	192.168.119.167	192.168.119.207	SSL	310	Continuation data
67	68.0222380	192.168.119.207	192.168.119.167	TCP	60	https > hp-webadmin [ACK] Seq=1 Ack=257 win=15544 Len=0
68	68.0277140	192.168.119.207	192.168.119.167	TCP	60	https > hp-webadmin [RST, ACK] Seq=1 Ack=257 win=15544 Len=0

Có một bắt tay TCP, nhưng không có kết nối HTTPS. Một kết nối HTTPS thực có chứa nhiều gói hơn, chẳng hạn như "Client Hello", "Server Hello" và "Change Crypt Spec".

Tìm gói SYN được gửi đến cổng https, có thể được đánh dấu là "443". Trong ví dụ trên, nó là gói 63. Nhấp chuột phải vào nó và nhấp vào "Follow TCP", ta thấy "Stream Content" chứa 256 byte gói ngẫu nhiên, như hiển thị bên dưới. Đây là các ký hiệu và được phần mềm độc hại sử dụng để thông báo cho máy chủ Command and Control rằng máy bị nhiễm và sẵn sàng sử dụng.

Vì dữ liệu là ngẫu nhiên, kết quả thu được có thể khác nhau, nhưng nó phải có kích thước 256 byte.

