

LAB 03

Thầy Mai Hoàng Đình
Trường đại học FPT

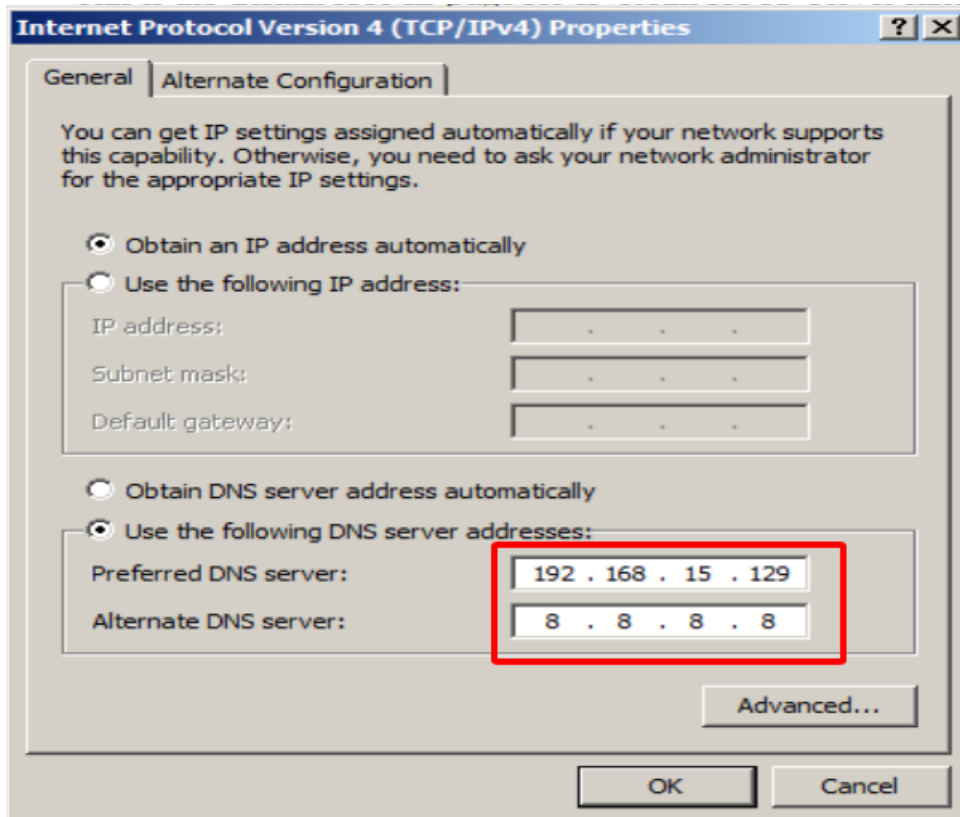
Người thực hiện

Đặng Hoàng Nguyên

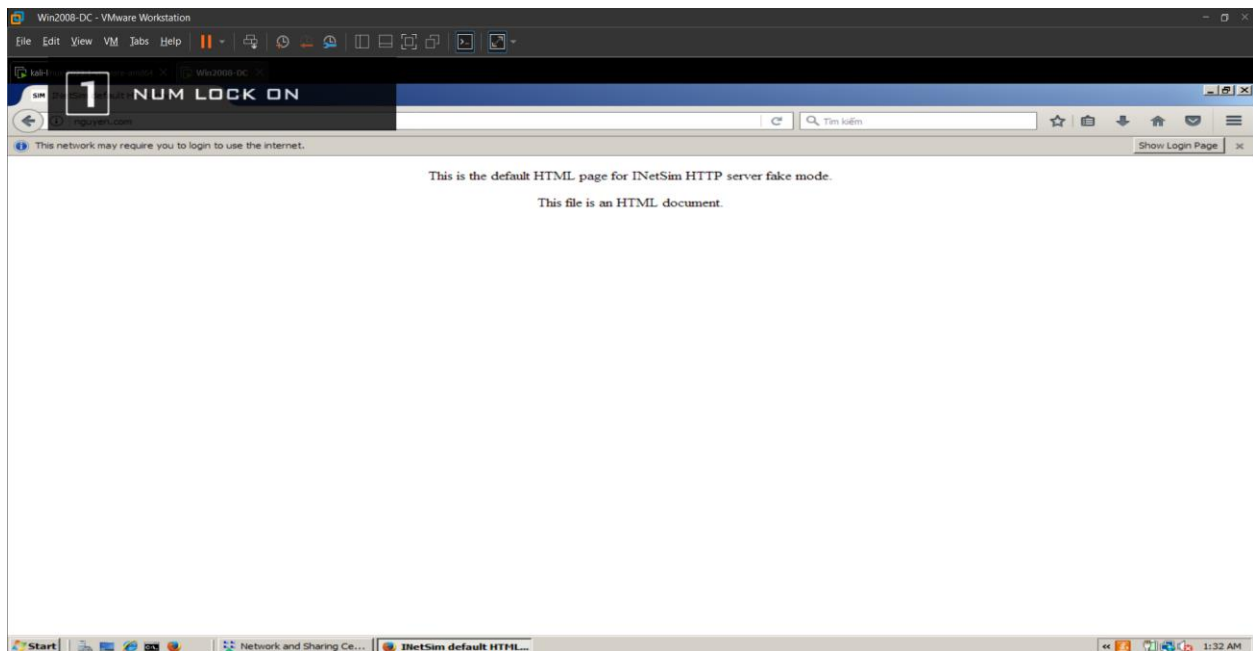
Basic Dynamic Techniques

Setting the DNS Server to 8.8.8.8

Trên máy ảo window 2008, vào trong Control Panel, mở “Network Connections” và chỉnh TCP/IP DNS dưới alternative là 8.8.8.8. DNS chính sẽ là máy chủ thật chứa inetsim, trong trường hợp này đó chính là máy kali



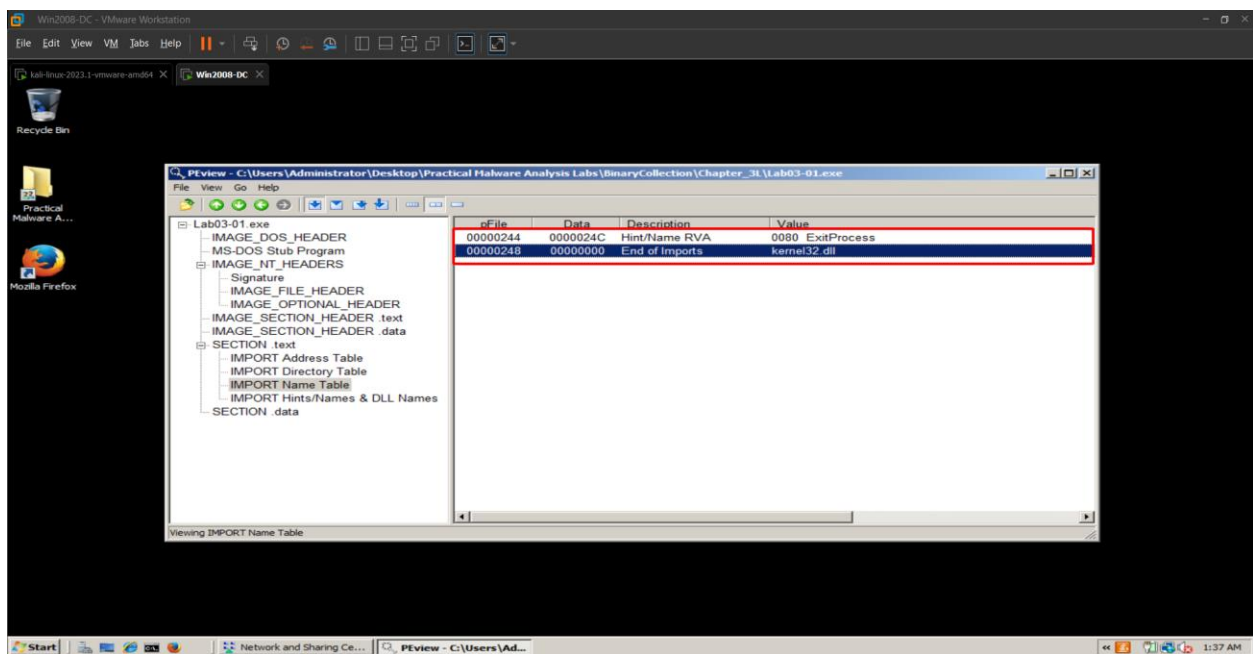
Thử nghiệm xem là đã vào được inetsim chưa bằng cách vào trong firefox để test xem coi inetsim đã chạy chưa. Bằng cách vào đường dẫn **nguyen.com**



Vậy là chúng ta đã bật inetsim thành công, tiếp theo đó, chúng ta sẽ tiến hành phân tích con malware này

Using PEvent

Đối tượng chúng ta cần quan tâm tới đó chính là con malware Lab003-01.exe. Bước đầu tiên sẽ load vào PEvent để check xem là con này nó đang sử dụng những gì

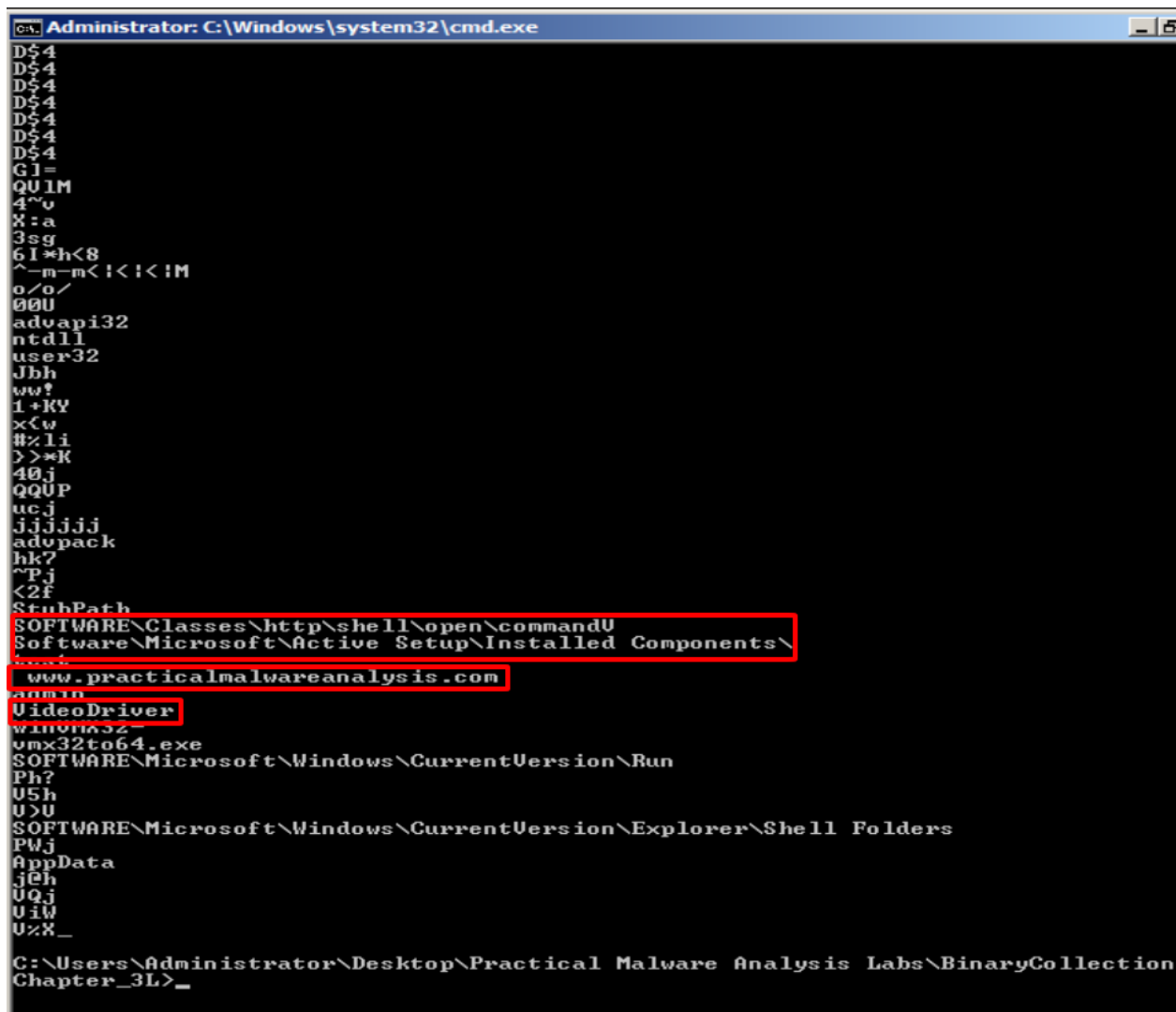


Thoạt nhìn qua ta có thể thấy rằng chương trình này sử dụng thư viện kernel32.dll và sử dụng function exitProcess của thư viện đó. Nhưng nếu xét trên phương diện một malware, không thể nào mà chỉ sử

dùng đúng một hàm của thư viện,, mà đây còn là exitProcess nữa, theo suy đoán ban đầu của em thì đoạn mã này đã bị pack. Đây chỉ là suy đoán ban đầu.

Using Strings

Bước tiếp theo đó chính là sử dụng strings để xem ngoài kernel32.dll ra thì nó sẽ có những gì. Trong đây ta có thể thấy là có một số dòng string nhìn có vẻ rất khả nghi



```
Administrator: C:\Windows\system32\cmd.exe
D$4
D$4
D$4
D$4
D$4
D$4
D$4
D$4
G1=
QU1M
4~v
X:a
3sg
61*eh<8
^~m~m<!<!!M
o/o/
00U
advapi32
ntdll
user32
Jbh
www?
1+KY
x<w
#%li
D>*K
40j
QQUP
ucj
jjjjjj
advpack
hk?
^Pj
<2f
StubPath
SOFTWARE\Classes\http\shell\open\commandU
Software\Microsoft\Active Setup\Installed Components\
www.practicalmalwareanalysis.com
admin
VideoDriver
winvnc32
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>_
```

Có vẻ như là nó sử dụng shell để kết nối tới một trang web nào đó, trang web đó có thể là practicalmalwareanalysis.com

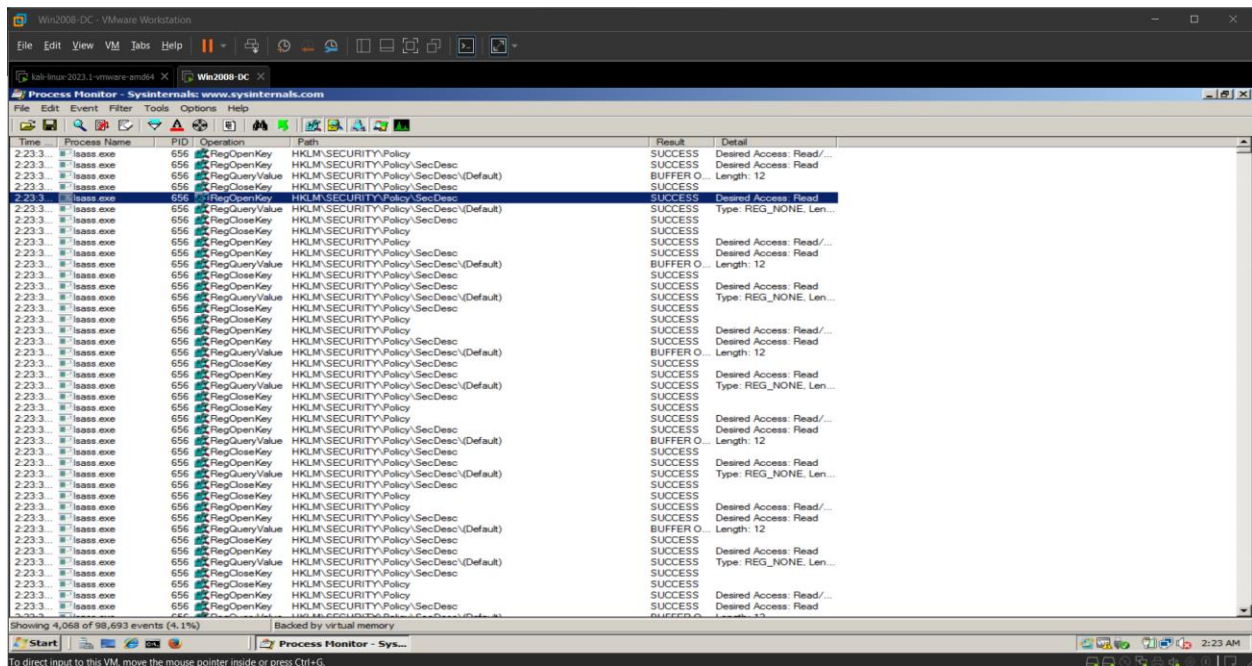
3. Run Process Explorer

Chúng ta sẽ bắt đầu chạy process explorer để xem tất cả các tiến trình đang chạy trên máy win 2008

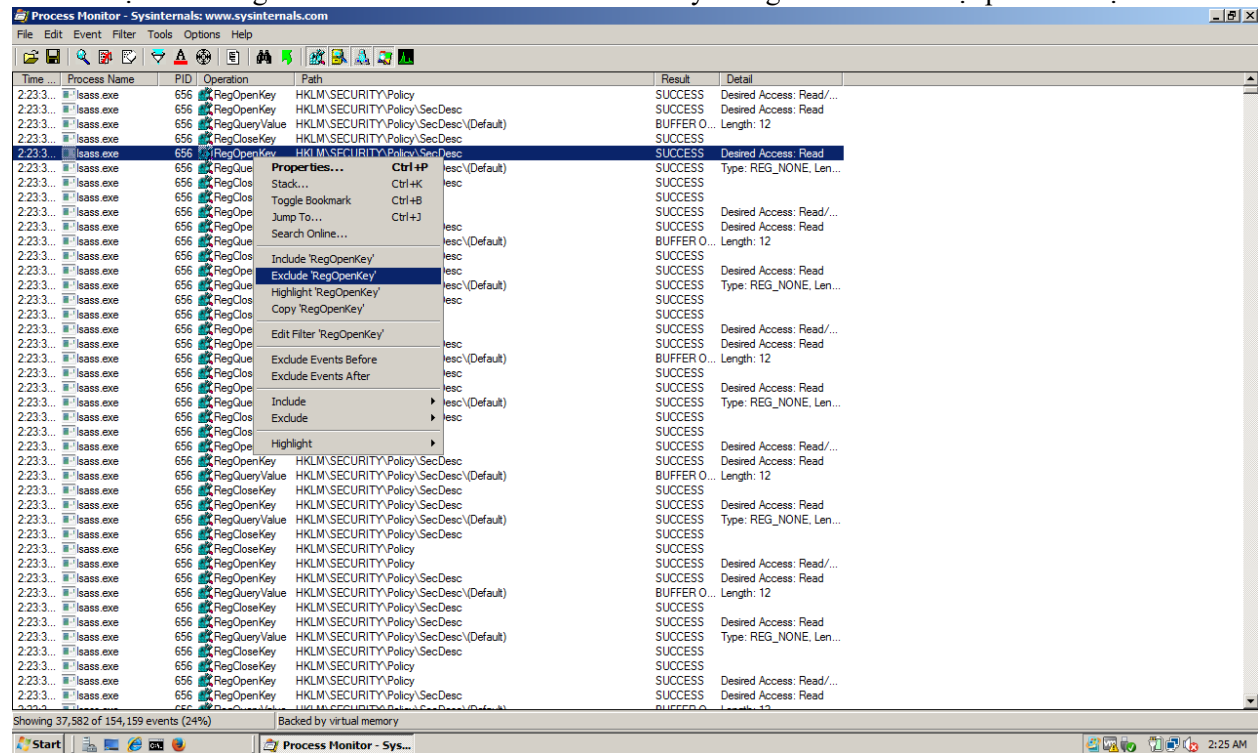
Lưu ý: trước khi làm bước cuối trong việc chuẩn bị phân tích con malware này, chúng ta phải vào trong C:\Windows\System32\vmx32to64.exe để xóa file vmx32to64.exe trong chế độ safe mode. Sau đó vào bên trong máy ảo bình thường

5. Start Process Monitor

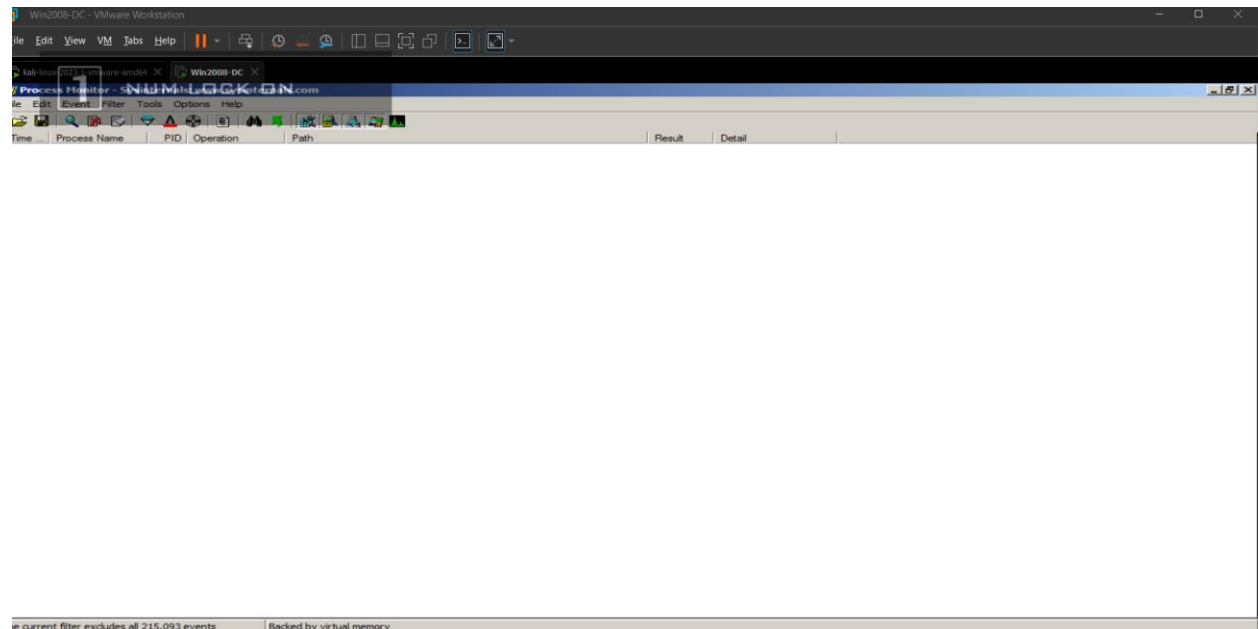
Bắt đầu mở Process Monitor ở bước cuối cùng trước khi phân tích con malware. Mục đích sử dụng process monitor trước bật con malware lên tại vì khi active con malware, nó có thể sẽ giả những tiến trình khác làm cho chúng ta không biết được những tiến trình gì nó sử dụng để fake khi con malware được mwor lên



Sau đó loại trừ những tiến trình nào mà nó default của máy. Bằng cách click chuột phải và chọn exclude

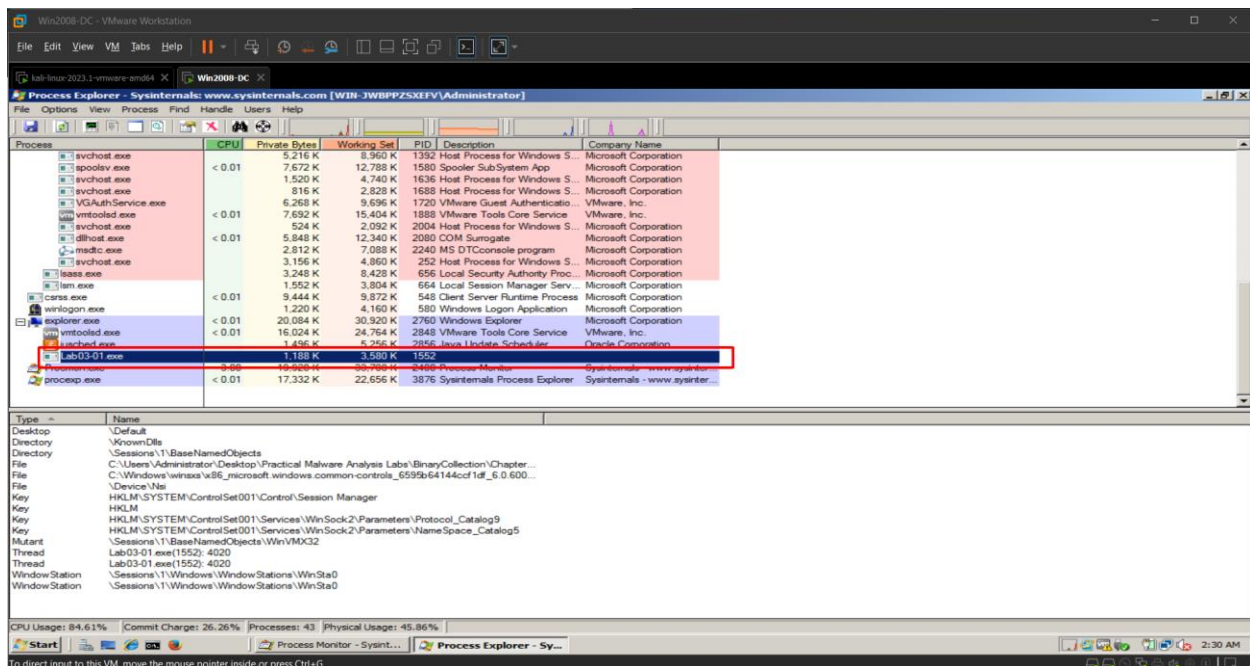


Sau khi exclude hết tất cả các tiến trình binifh thường ở trên máy, ta có được

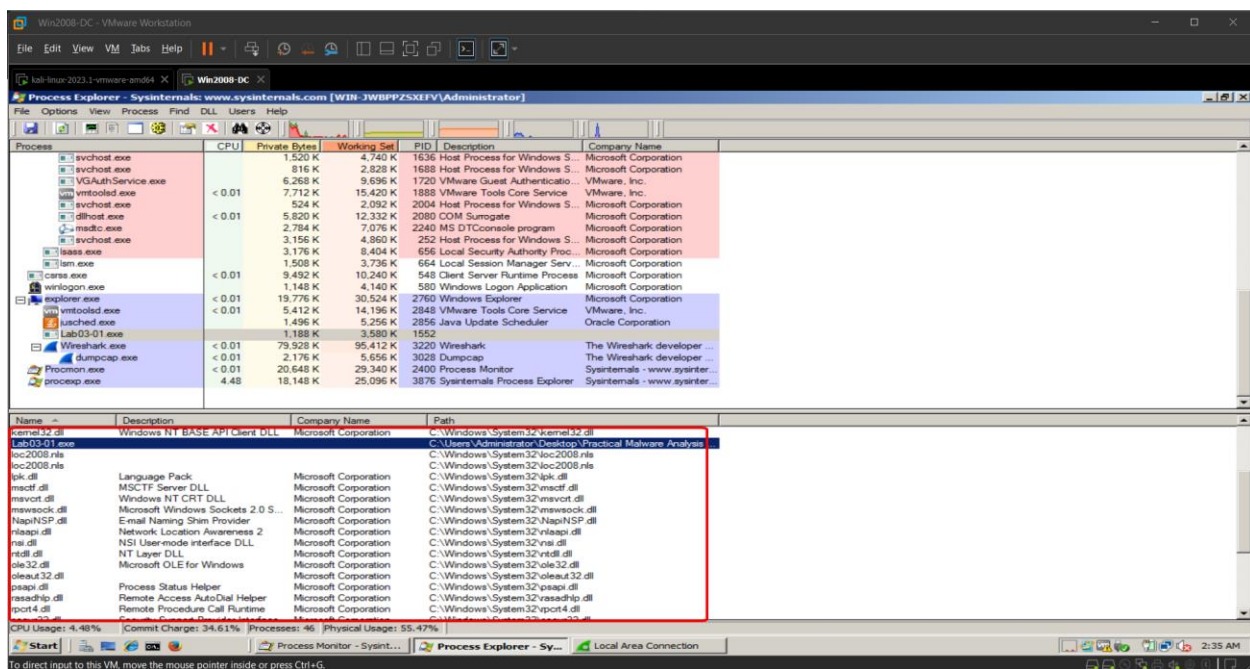


Sau bước này, ta sẽ tiến hành chạy con malware

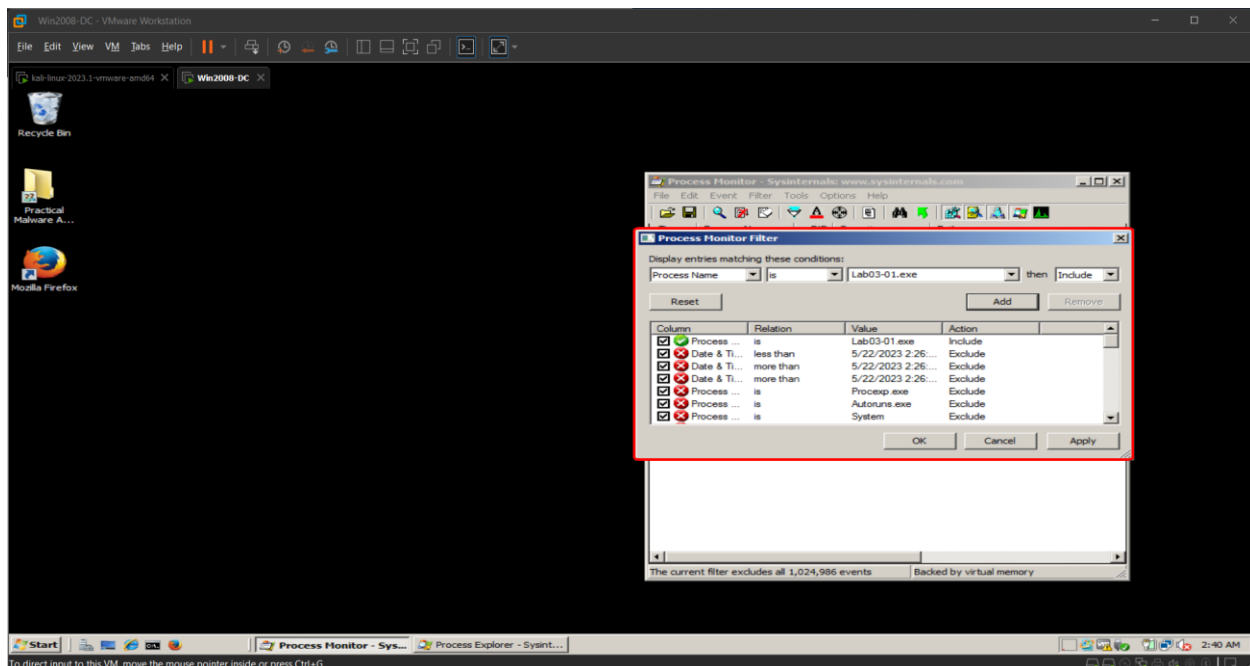
Vào trong process explorer, chọn View → Lower Pane View, Handles



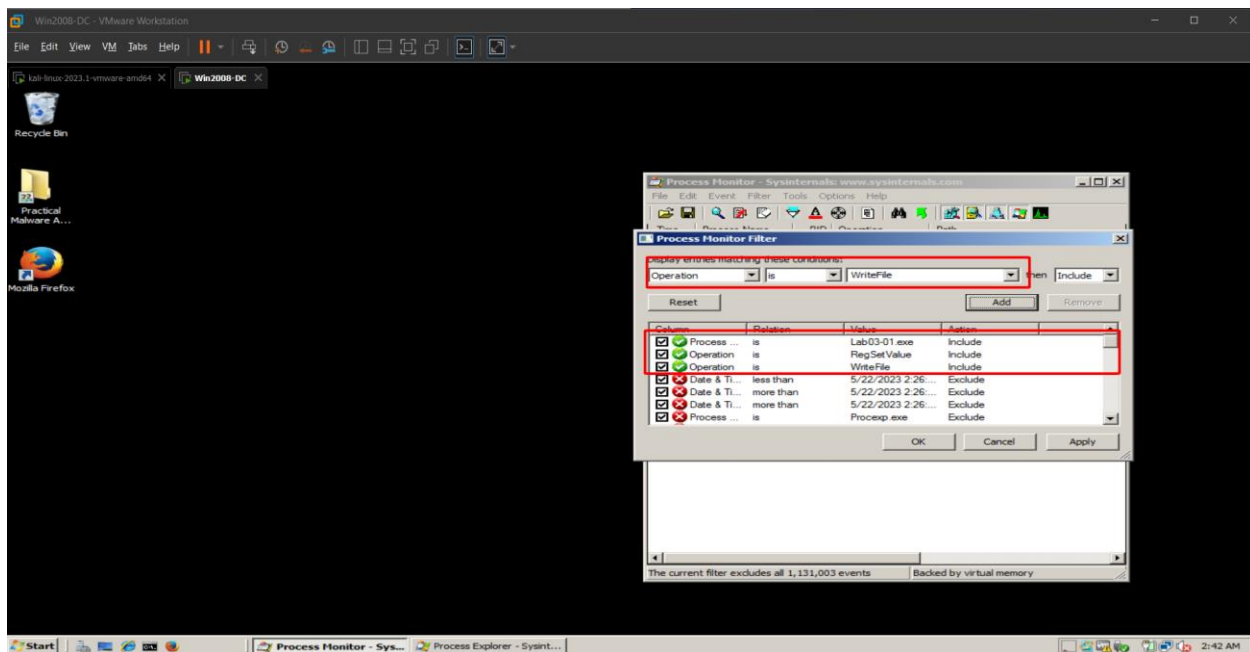
Và ngoài ra sau khi mà sử dụng Handles, chúng ta sẽ xem tới các dll



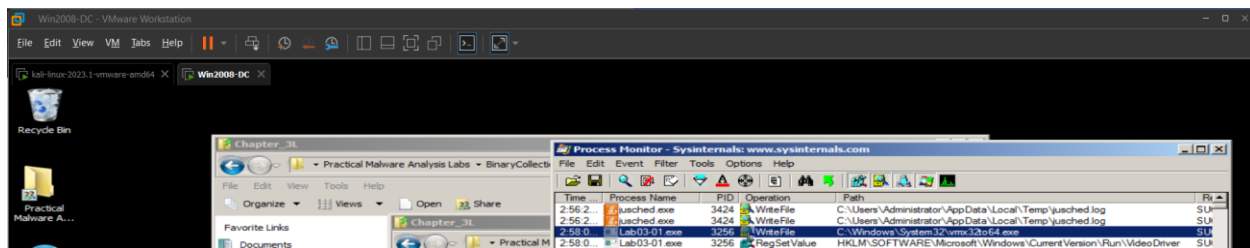
Đúng như phỏng đoán ban đầu, thì chương trình này đã bị pack, vì sau khi mở chương trình lên thì dll được xem bởi process ban đầu thì chỉ có kernel32, mà ở đây sau khi chạy chương trình, ta có thể thấy rằng là chương trình đã mở ra và sử dụng nhiều dll khác.



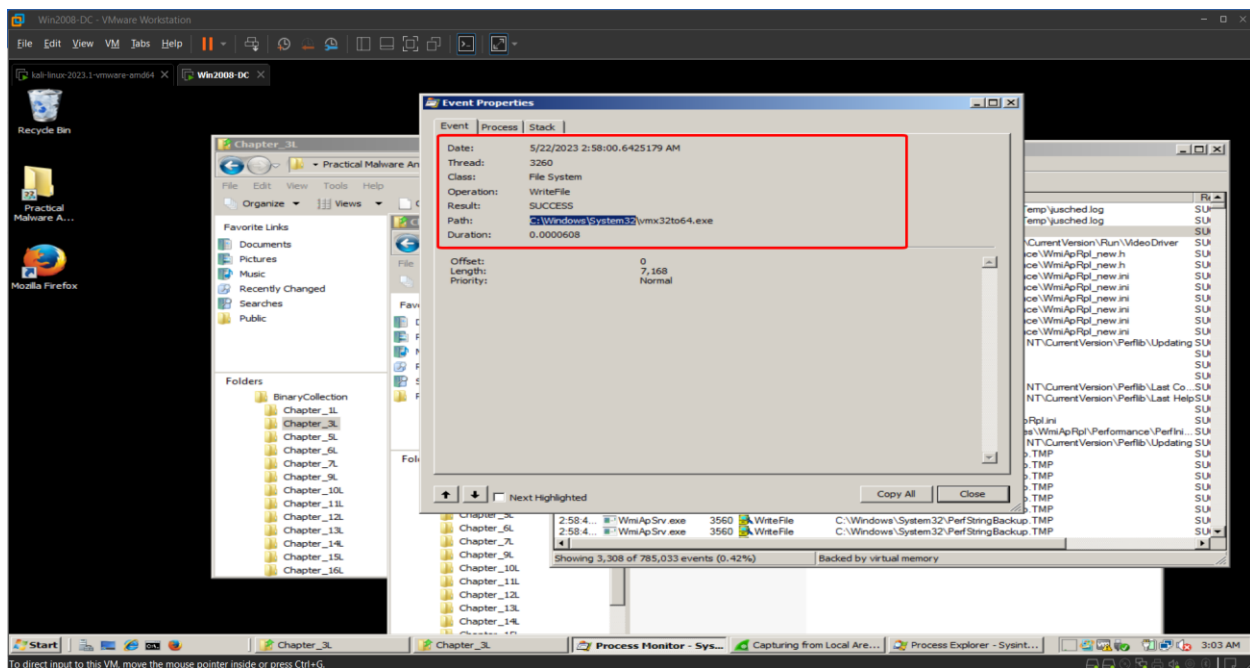
Tiếp tục sử dụng Process Monitor để có thể xem con Lab03-1.exe đang làm gì. Nhấn tổ hợp Ctrl+L chọn phần Process Name và search Lab03-01.exe sau đó thêm hai filter là RegSetValue và WriteFile của Operation



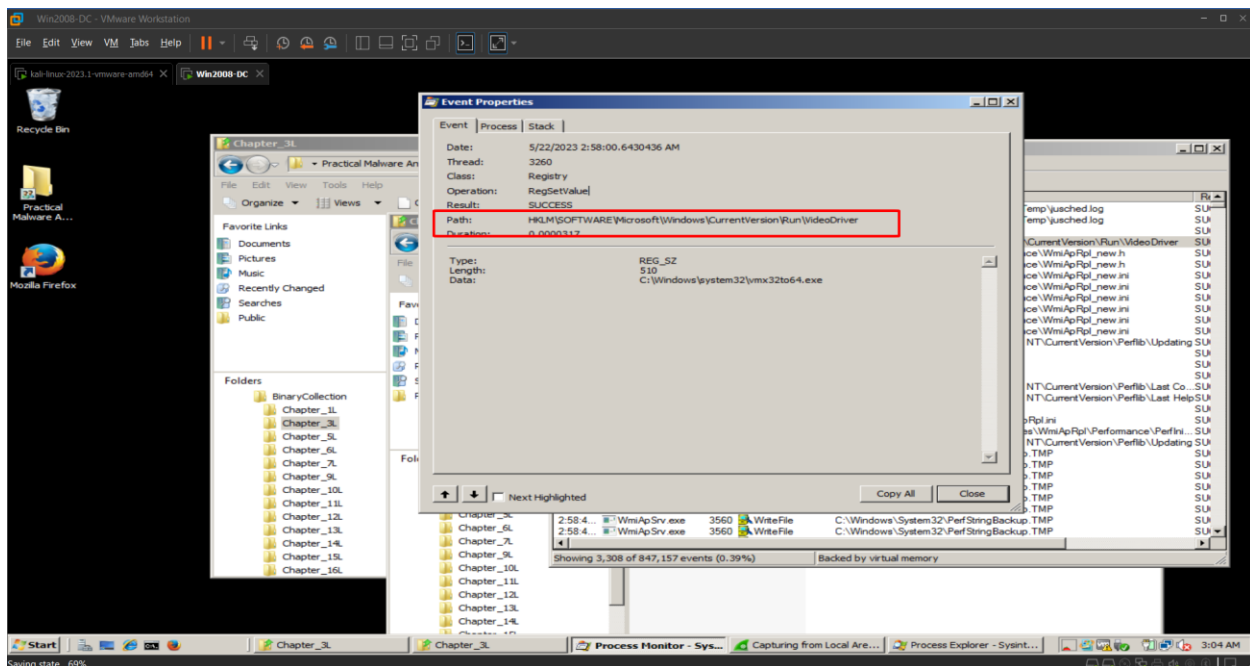
Đây là setting hoàn chỉnh để filter ra, và ta có kết quả



Double click vào vmx32to64.exe ta sẽ thấy được những thông tin cơ bản của con malware



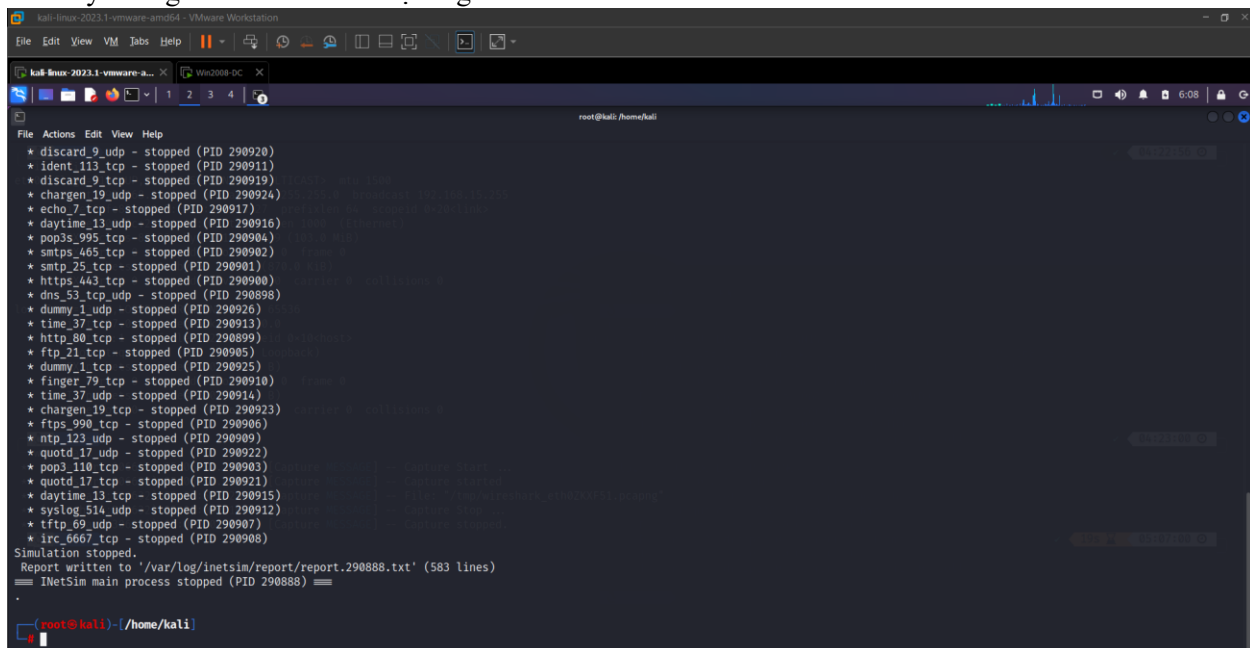
Sau đó nhấn vào xem Videodriver, đây là một thứ có bên trong của con malware. Ta sẽ thấy được rằng hành vi của con malware này rất đáng ngờ



Setting của nó đã được lưu vào registry, sau khi mỗi lần khởi động lên thì VideoDriver sẽ hoạt động

Viewing INetSim Logs

Khi này chúng ta sẽ inet sim để đọc log của con malware



File nó có tên là report.29088.txt để có thể đọc log

```
kali-linux-2023.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali Linux 2023.1-vmware-amd64 - Win2008-DC
root@kali: /home/kali
File Actions Edit View Help
* daytime_13_udp - stopped (PID 290916)
* pop3s_995_tcp - stopped (PID 290904)
* smtps_465_tcp - stopped (PID 290902)
* smtp_25_tcp - stopped (PID 290901)
* https_443_tcp - stopped (PID 290900)
* dns_53_tcp_udp - stopped (PID 290898)
* dummy_1_udp - stopped (PID 290926)
* time_37_tcp - stopped (PID 290913)
* http_80_tcp - stopped (PID 290899)
* ftp_21_tcp - stopped (PID 290905)
* dummy_1_tcp - stopped (PID 290925)
* finger_79_tcp - stopped (PID 290910)
* time_37_udp - stopped (PID 290914)
* chargen_19_tcp - stopped (PID 290923)
* ftps_990_tcp - stopped (PID 290906)
* ntp_123_udp - stopped (PID 290909)
* quotd_17_udp - stopped (PID 290922)
* pop3_110_tcp - stopped (PID 290903)
* quotd_17_tcp - stopped (PID 290921)
* daytime_13_tcp - stopped (PID 290915)
* syslog_514_udp - stopped (PID 290912)
* tftp_69_udp - stopped (PID 290907)
* irc_6667_tcp - stopped (PID 290908)
Simulation stopped.
Report written to '/var/log/inetSim/report/report.290888.txt' (583 lines)
== InetSim main process stopped (PID 290888) ==

(root@kali) ~/home/kali
# cat /var/log/inetSim/report/report.290888.txt | grep "www.practicalmalwareanalysis.com"
2023-05-22 05:28:09 DNS connection, type: A, class: IN, requested name: www.practicalmalwareanalysis.com
2023-05-22 05:58:00 DNS connection, type: A, class: IN, requested name: www.practicalmalwareanalysis.com

(root@kali) ~/home/kali
#
```

Sử dụng câu lệnh grep để lọc ra những dòng nào có www.practicalmalwareanalysis.com

Using Wireshark

Dùng wireshark mở từ đầu xem thu thập được những gì bằng cách gõ “frame contains practicalmalwareanalysis” em không biết vì lý do gì nhưng mặc dù thử lại rất nhiều lần nhưng vẫn không bắt được các gói khác, trừ hai gói này ra.

