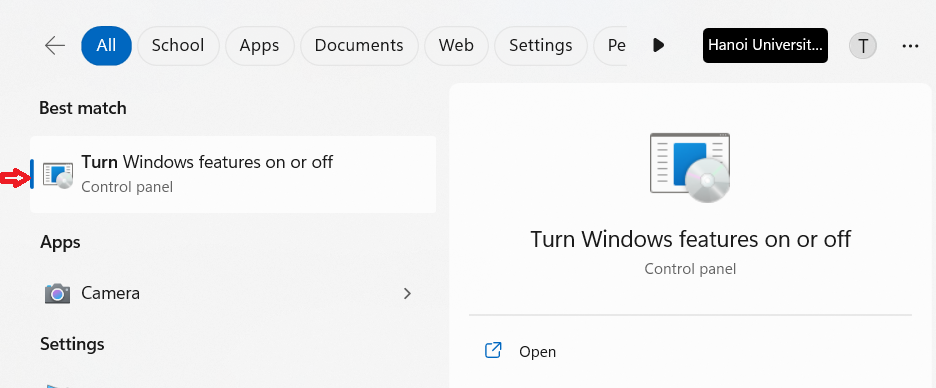
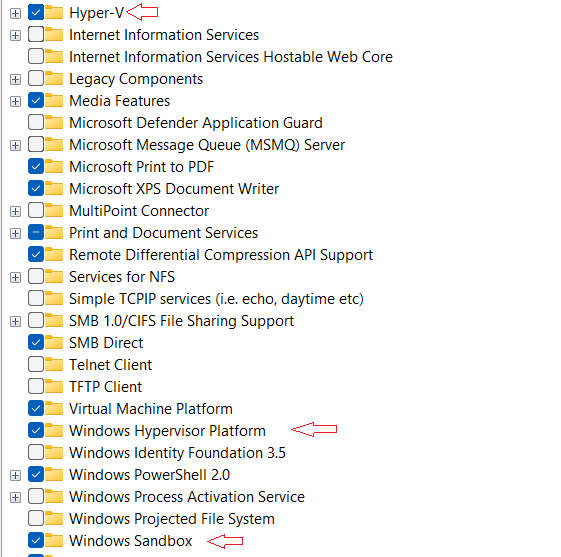
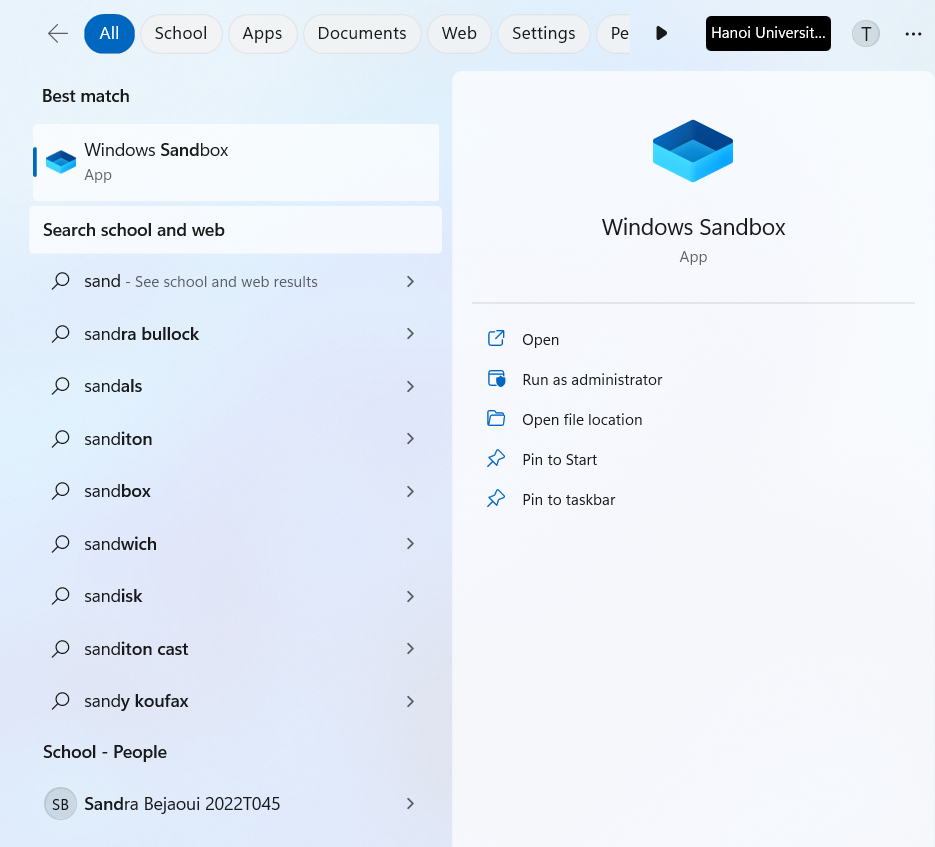
Sandbox cài đặt và thực hành phân tích động cơ bản 1 số file mã độc

Vào Turn Windows features on or off



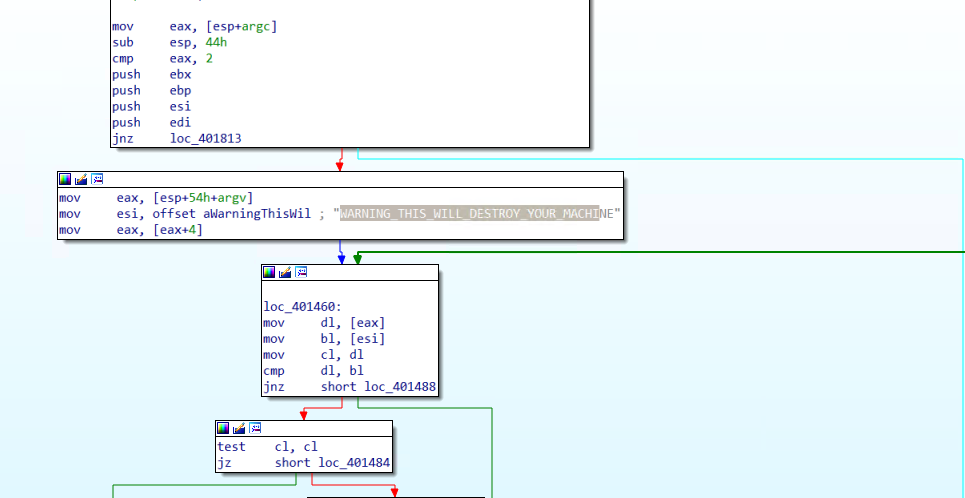


Tích vào 3 mục trên và khởi động lại máy



Khởi động sandbox

Lab01-01.exe

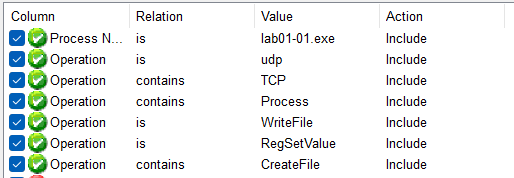


Hình 1 kiểm tra tham số

Chương trình kiểm tra tham số đầu vào nếu tham số là “WARNING\_THIS\_WILL\_DESTROY\_YOUR\_MACHINE” chương trình sẽ thực hiện hành vi độc hại.

trong bài này em chỉ tập trung vào phân tích động vì vậy không đi sau vào việc sử dụng IDA để phân tích mã độc.

Sau khi xác định được tham số để thực thi file mã độc này tiến hành mở Process Monitor để quan sát các hành vi của mã độc



Hình 2 thiết lập Filter Process Monitor

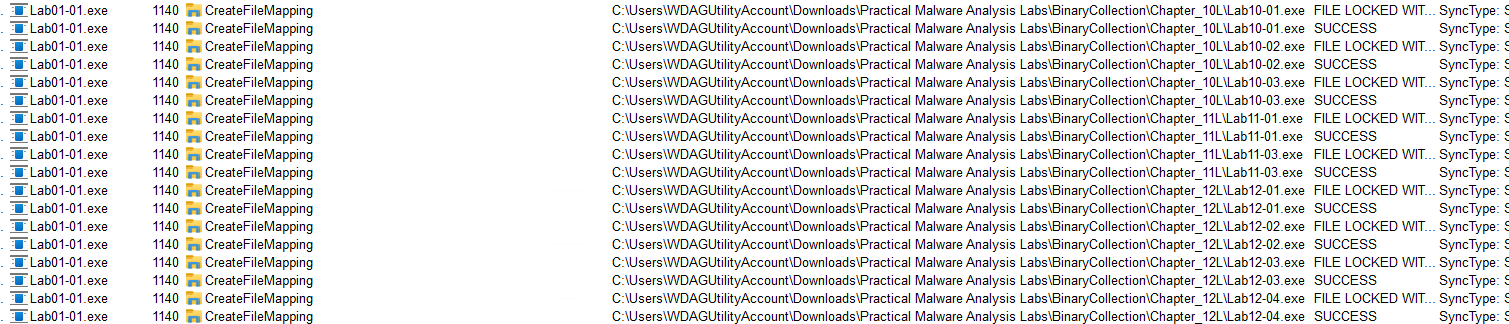
Thiết lập process name là lab01-01.exe chính là tên file

Với Operation

* Process : quan sát quá trình hình thành tiến trình, kiểm tra mã độc có tạo ra các tiến trình con không
* RegSetValue : kiểm tra registry xem mã độc có thiết lập các giá trị để tự động khởi chạy hay không
* CreateFile, CreateFileMaping, WriteFile: kiểm tra mã độc có thực hiện chỉnh sửa file, tạo file nào không
* TCP,UDP kiểm tra kết nối mạng của mã độc



Hình 3 kết quả quan sát process Monitor



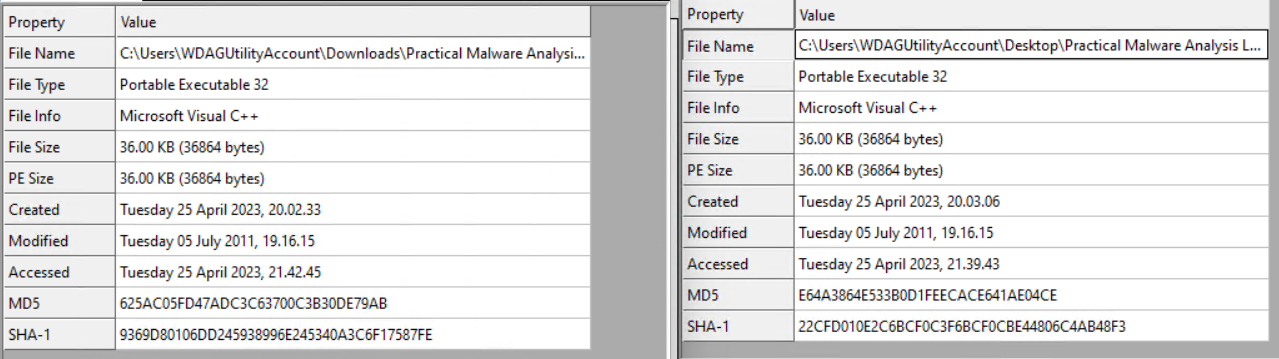
Hình 4 kết quả quan sát Process Monitor

Từ kết quả quan sát trên ta có thể đưa ra 1 số kết luận về mã độc này sẽ

Tạo 1 file có tên là kerne123.dll trong file system của máy ( file này có tên khá giống với hệ thống kernel123.dll )

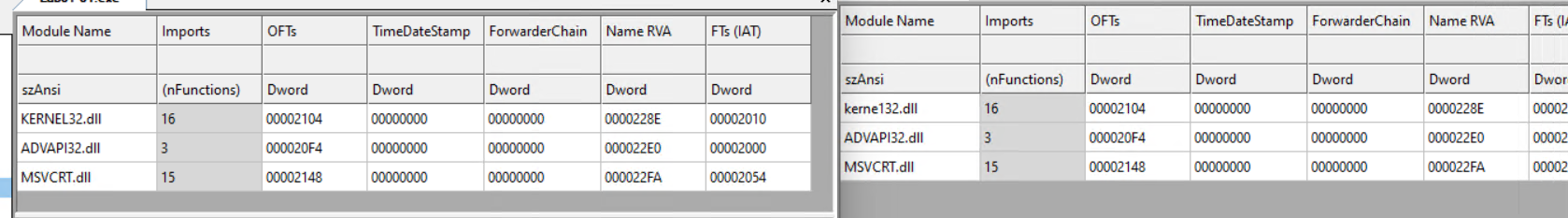
Chỉnh sửa các file thực thi

Dùng CFF explorer để check thông tin 1 file bị sửa đổi ta có nhận xét file đã bị thay đổi nhưng kích thước không bị thay đổi.



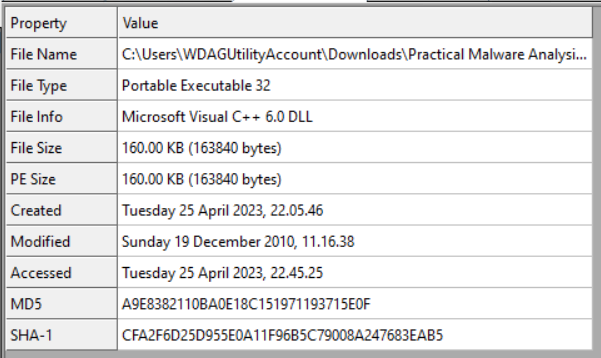
Hình 5 kiểm tra thông tin cơ bản của trước và sau khi bị thay đổi do mã độc

Kiểm tra kĩ hơn ta thấy thông tin import table đã bị thay đổi từ kernel23.dll thành kerne123.dll

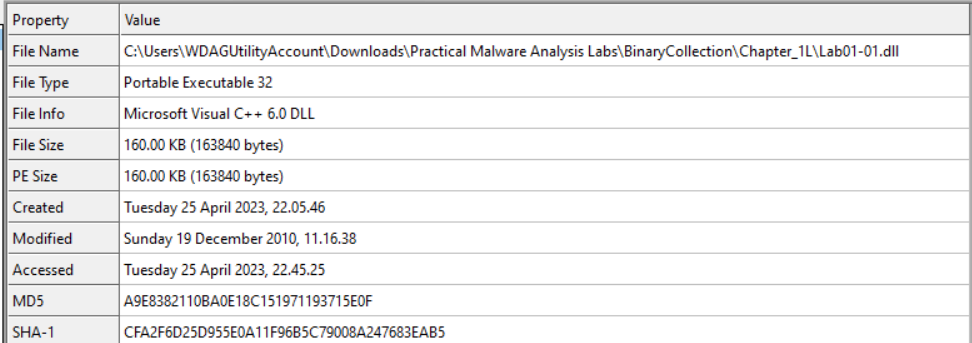


Hình 6 thông tin import table

Ta kiểm tra thông tin file kerne123.dll và file lab01-01.dll

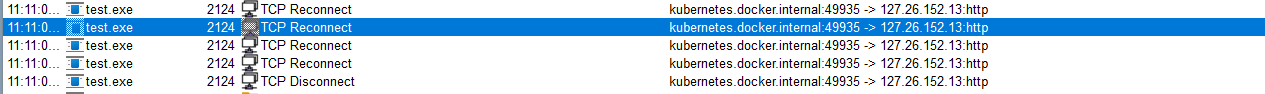


Hình 7 thông tin file lab01-01.dll



Hình 8 thông tin file kerne123.dll

Thử chạy 1 file đã bị sửa đổi đây hoàn toàn là 1 file sạch



Hình 9 kết quả quan sát hành vi file bị mã độc chỉnh sửa

tạo kết nối tới địa chỉ 127.26.152.13

Từ đây ta xác định được hành vi và mục đích của mã độc:

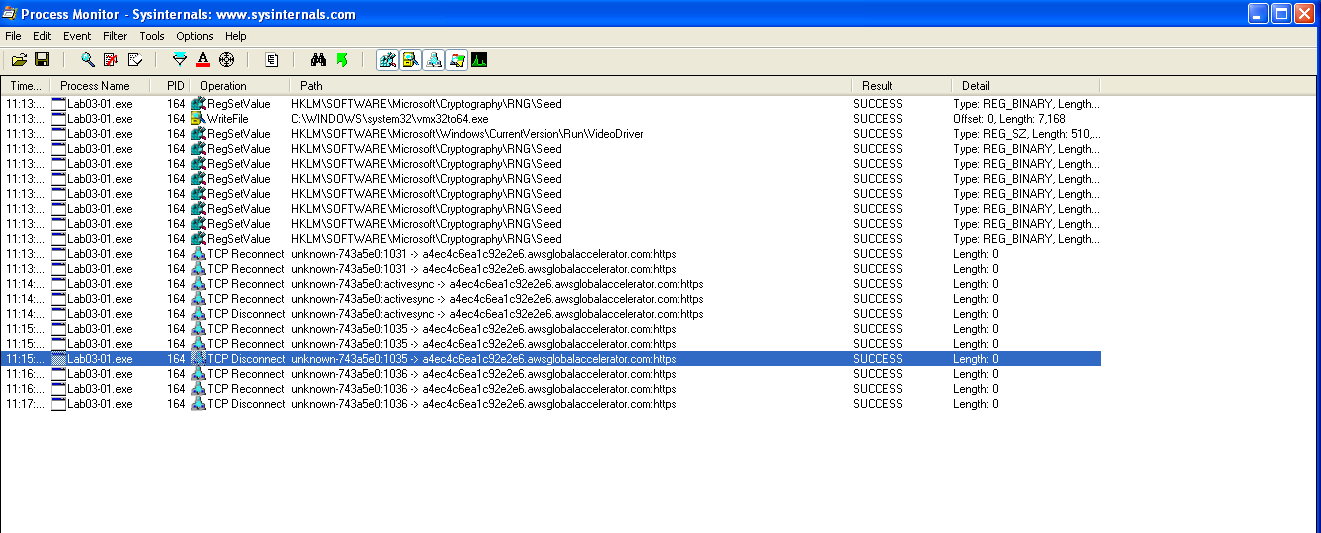
Dựa trên file lab01-01.dll đi kèm tạo file kerne123.dll vào “C:\Windows\SysWOW64”. Nó tìm kiếm các file import kernel32.dll sửa thành kerne123.dll Sự thay đổi này không làm ảnh hưởng tới chức năng của các chương trình trên chỉ có lúc chạy các chương trình này mã độc sẽ tạo kết nối tới địa chỉ 127.26.152.13

Các bài lab khác không chạy được trên win10 hoặc ko thực hiện đầy đủ hành vi độc hại trên win 10 vì vậy cài đặt máy ảo winxp để phân tích ( đây cũng là hệ điều hành mà cuốn sách khuyến nghị)

Lab03-01.exe

Mở Process Monitor và cài đặt filter như bài lab01-01.exe

Thực thi file lab03-01.exe và quan sát Process Monitor



Hình kết quả quan sát hành vi mã độc bằng Process Monitor

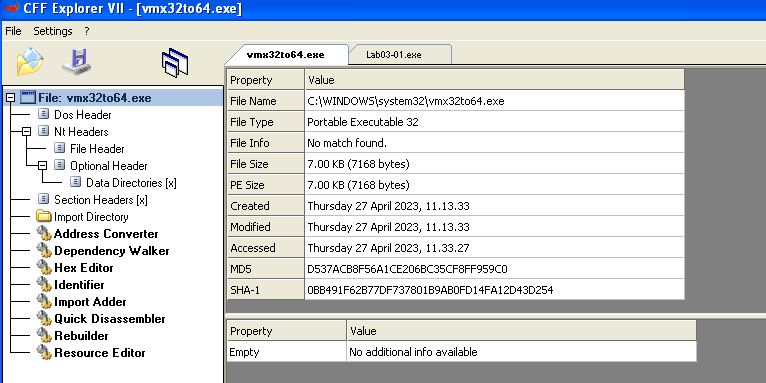
Mã độc thực hiện 3 hành vi đặc trưng

* Write File
* RegSetValue
* TCP connect

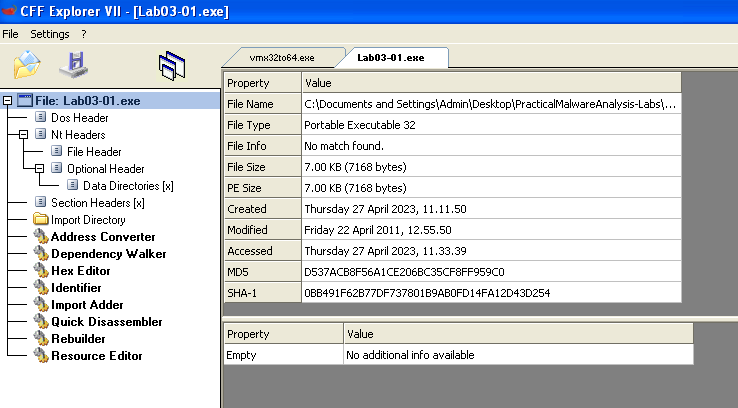
**File vmx32to64.exe**

Vmx32to64.exe là file mã độc drop ra trong quá trình thực thi của mình

Dùng CFF exployer để kiểm tra thông tin file mã độc vừa mới drop này



Hình thông tin file vmx32to64.exe

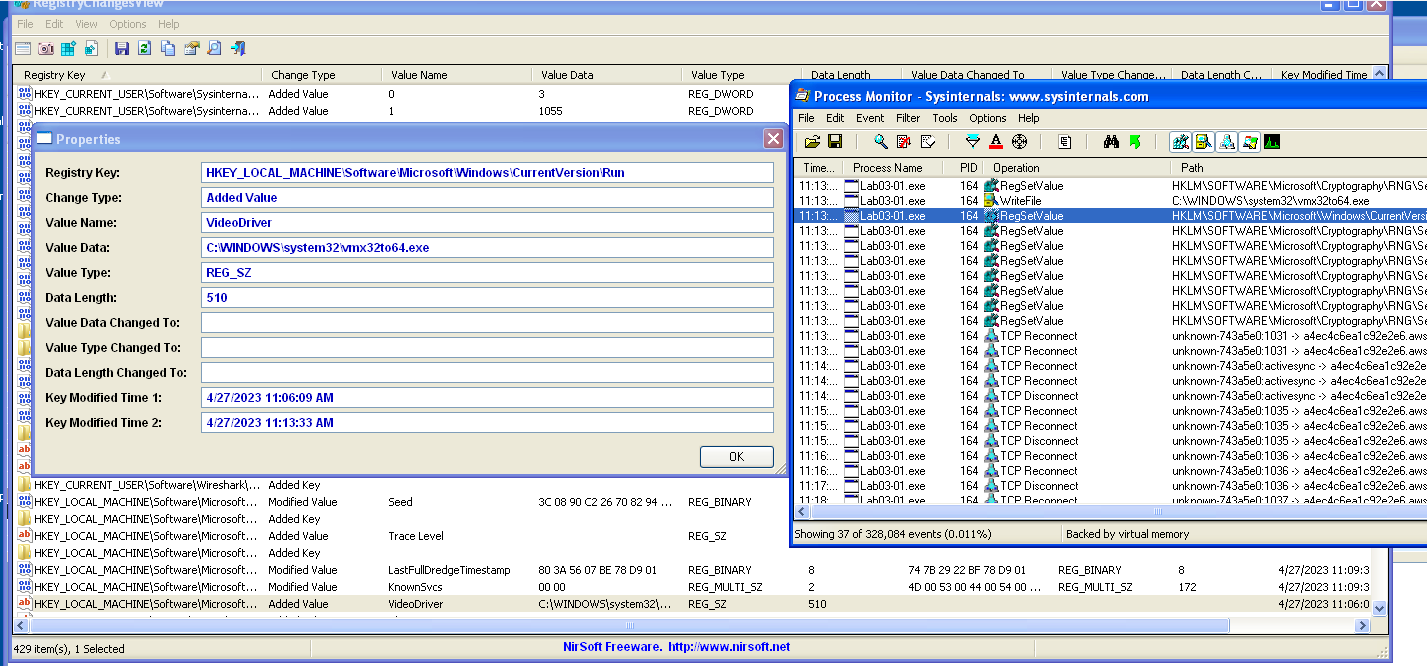


Hình thông tin file mã độc lab03-01.exe

Nhận thấy file vmx32to64.exe hoàn toàn giống với file Lab03-01.exe

**Registry “HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\VideoDriver”**

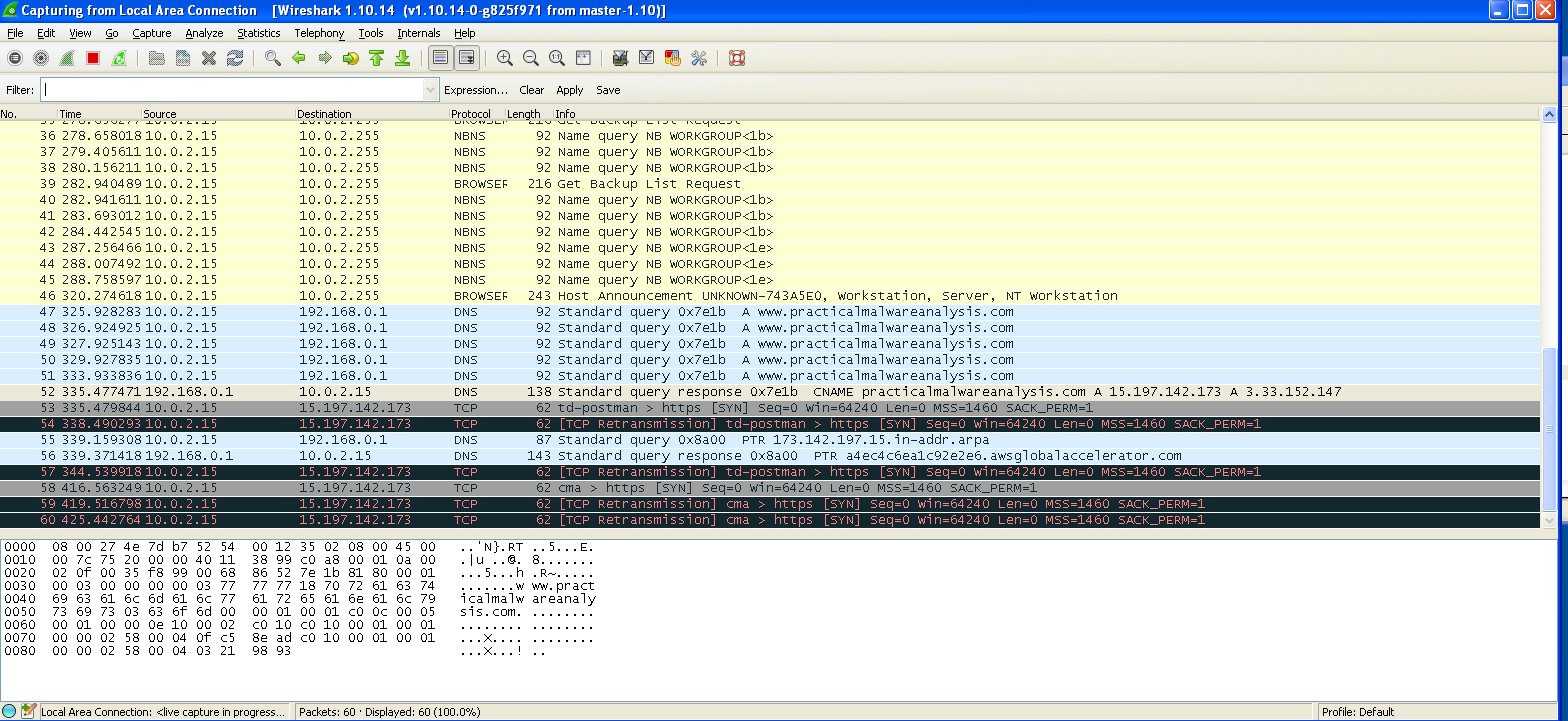
Kiểm tra chi tiết hơn về registry này bằng registry change view



Mã độc tạo registry với key “HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\VideoDriver

” và value “C:\WINDOWS\system32\vmx32to64.exe” mục đích là để mã độc tự động thực khởi chạy khi máy tính được khởi động

**TCP**



Dùng wire shark để bắt và phân tích gói tin

Ta có thể thấy mã độc sử dụng mã độc sử dụng DSN để phân giải tên miền [www.practicalmalwareanalysis.com](http://www.practicalmalwareanalysis.com) đây khả năng cao là máy chủ điều khiển mã độc.