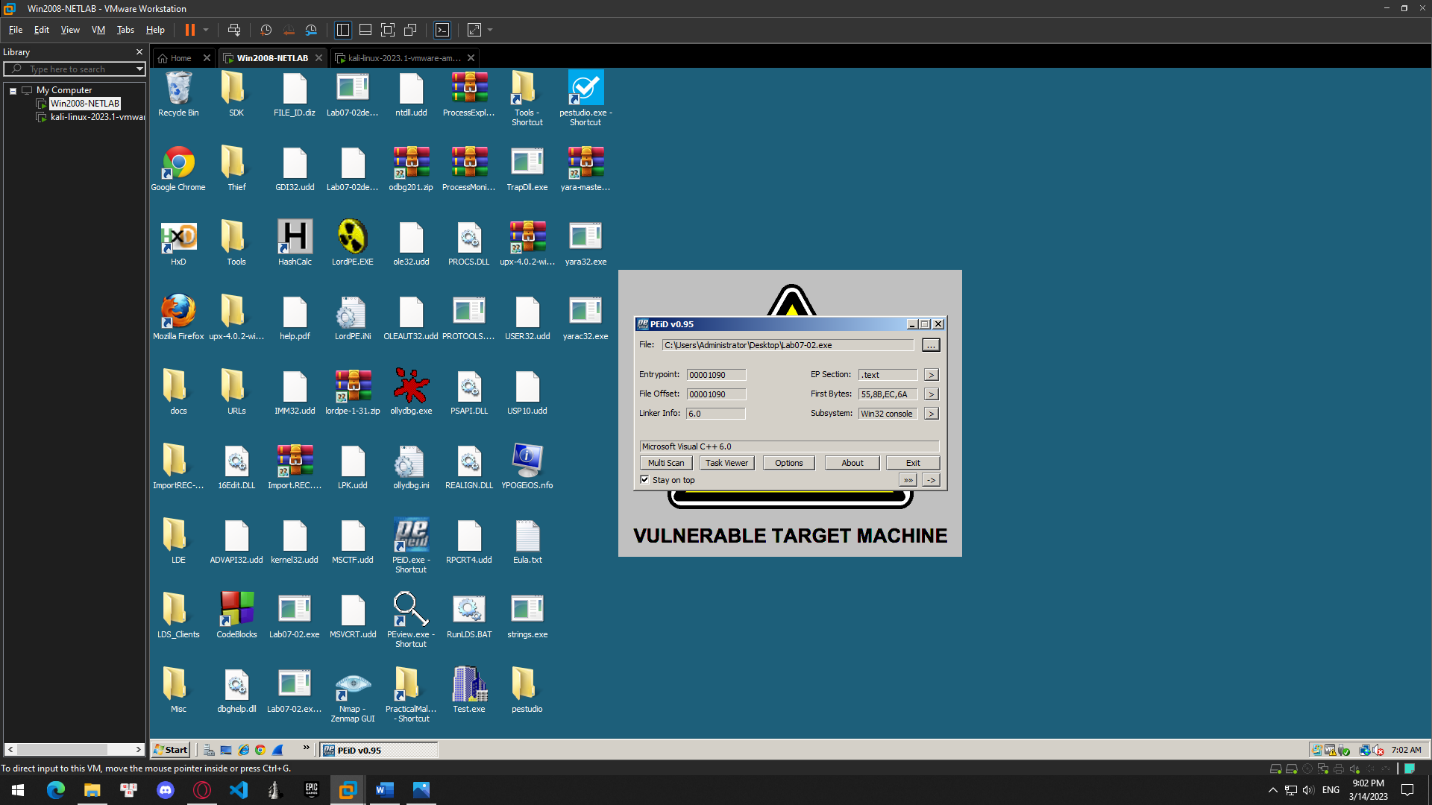
**Bản báo cáo TestLab\_IAM302**

**Họ tên : Nguyễn Nhật Huy**

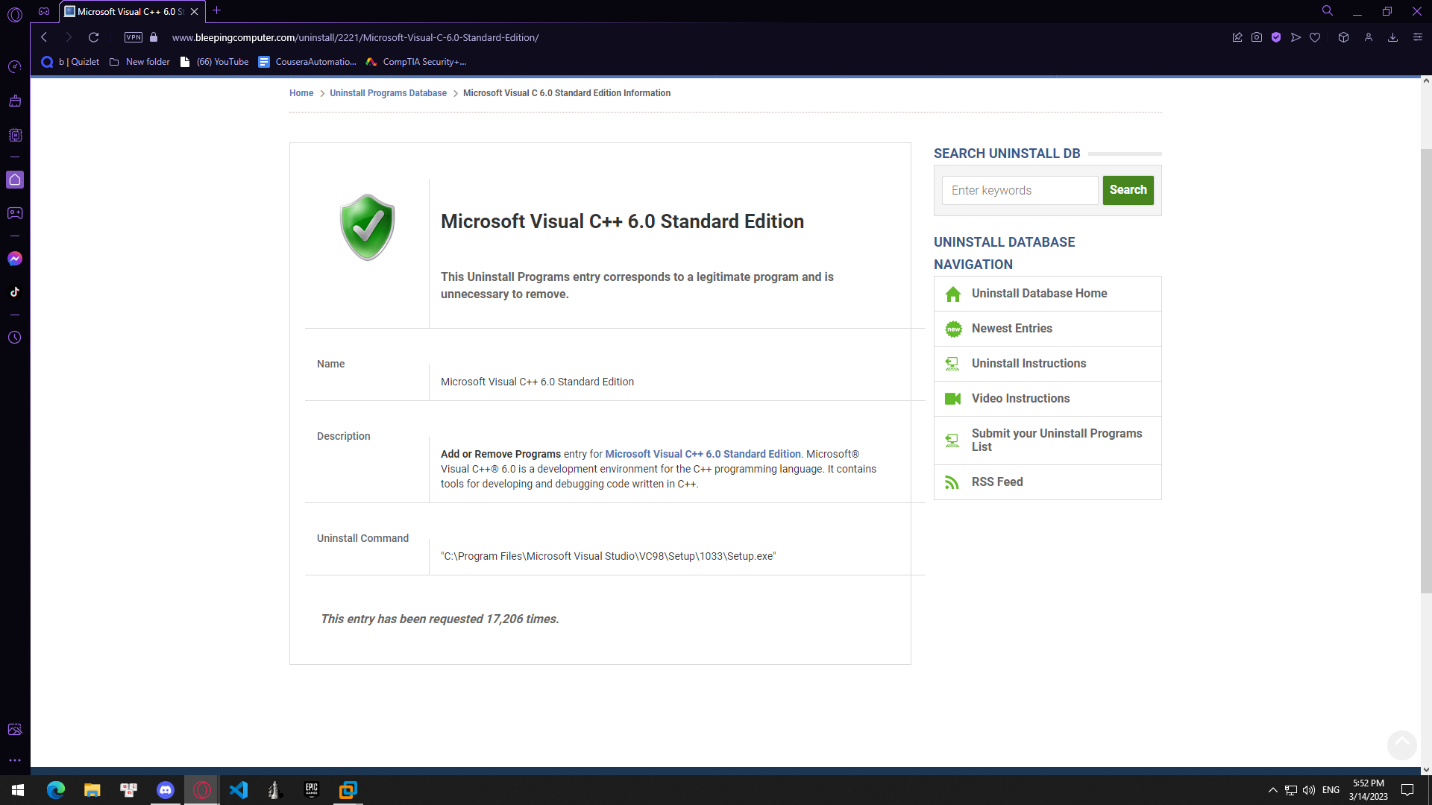
**Lớp : IA1604**

**Mã độc phân tích :** **Lab07-02.exe**

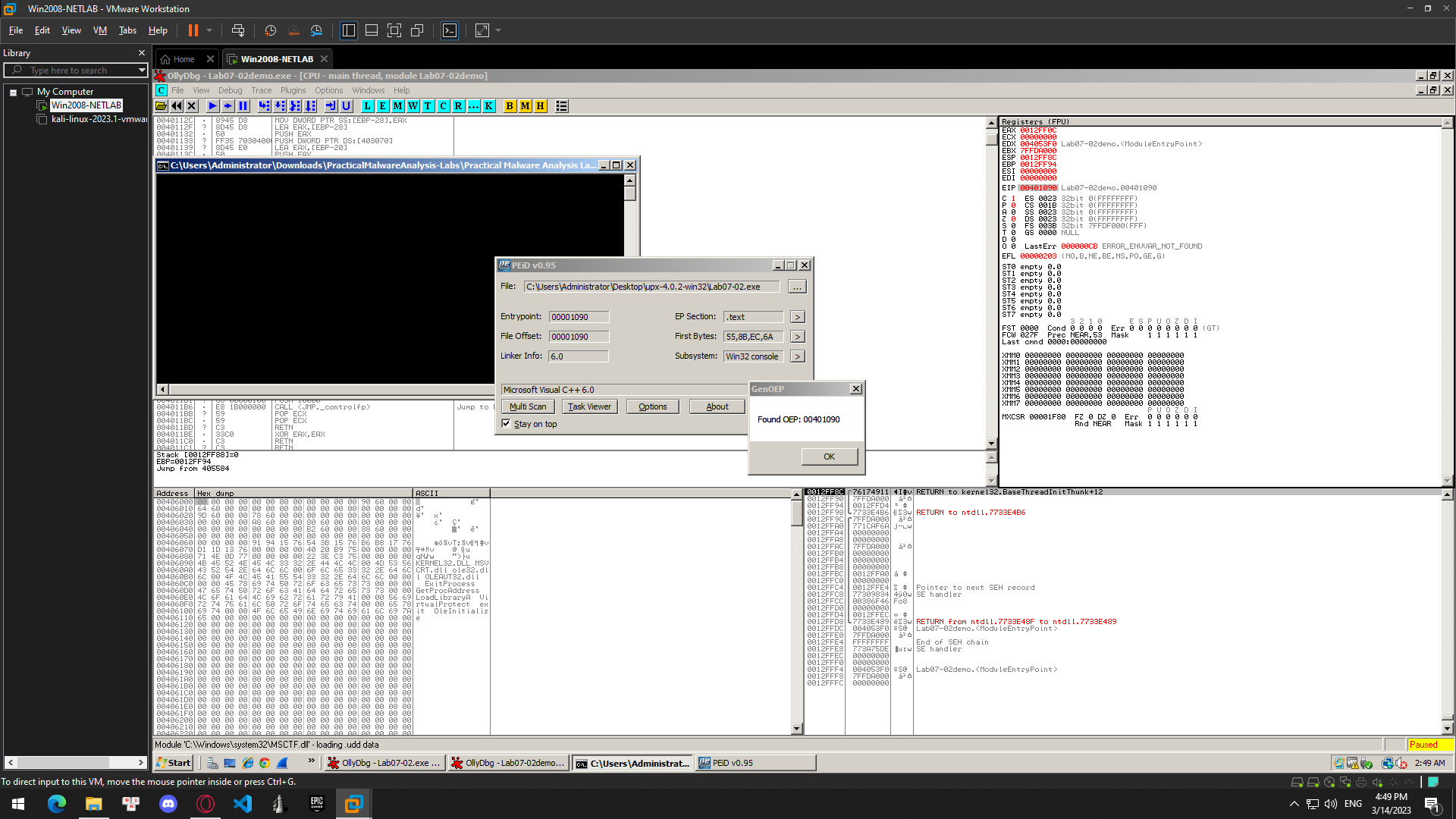
1. Mã độc có bị pack hay không? Chỉ ra 2 dấu hiệu (kết quả phân tích trên 2 công cụ khác nhau) chứng minh.

Đầu tiên em dò trên PeID file gốc xem file có bị pack hay chưa và nó cho kết quả là 

* Như vậy là file chưa bị pack cũng như em tra trên mạng thì file là legit



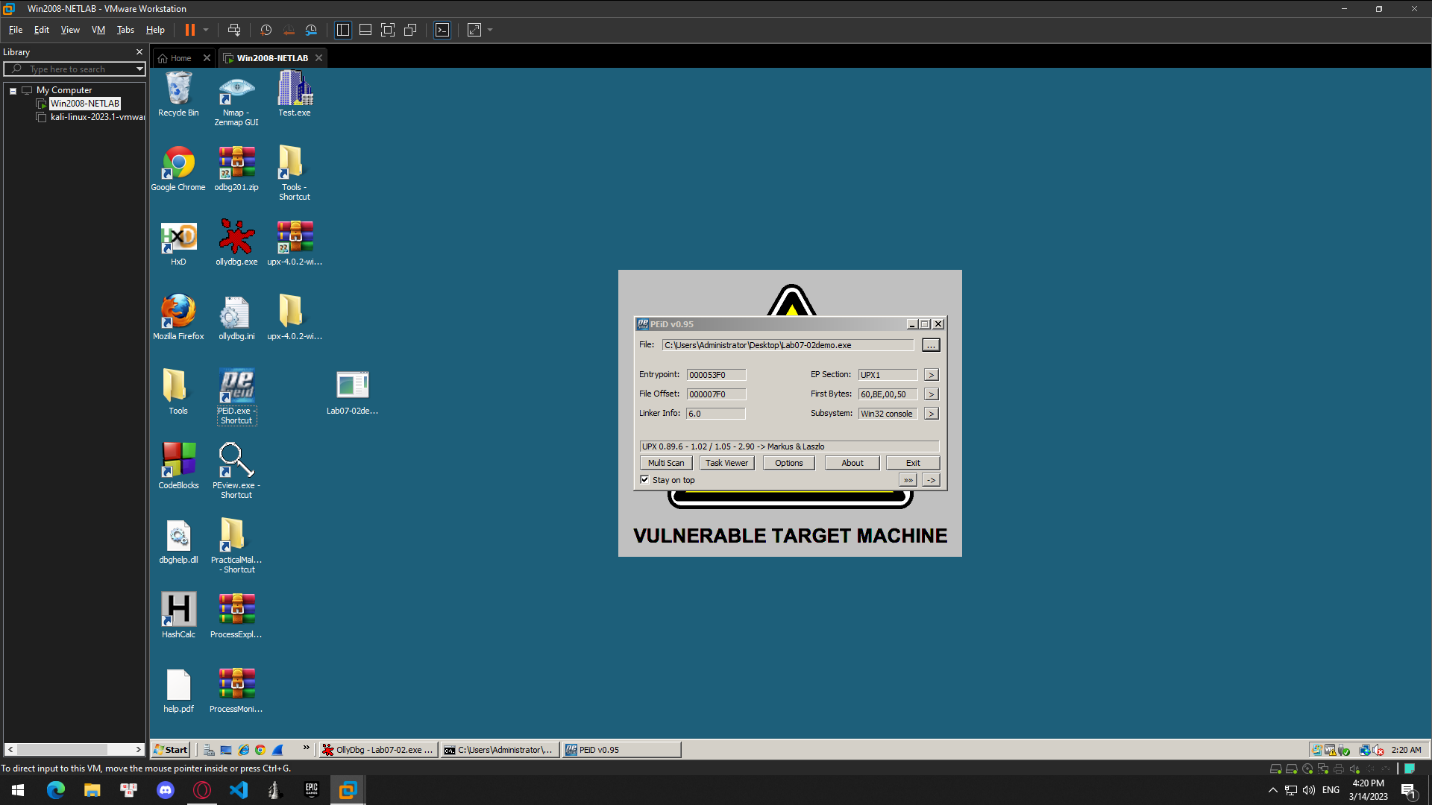
Vì mình mới chỉ dò qua file gốc nên không biết nó như nào nên em tìm OEP của nó và ra kq là

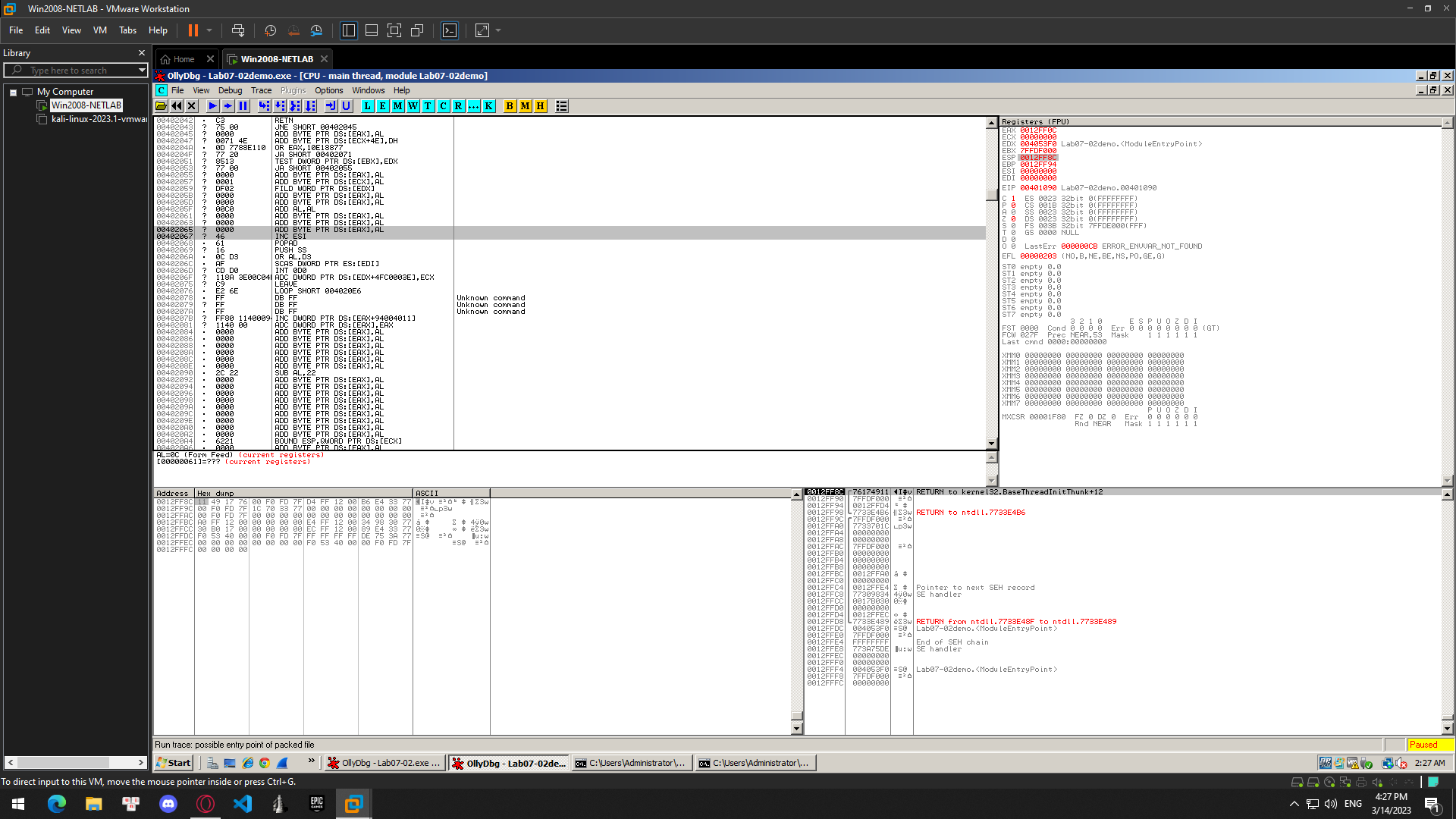


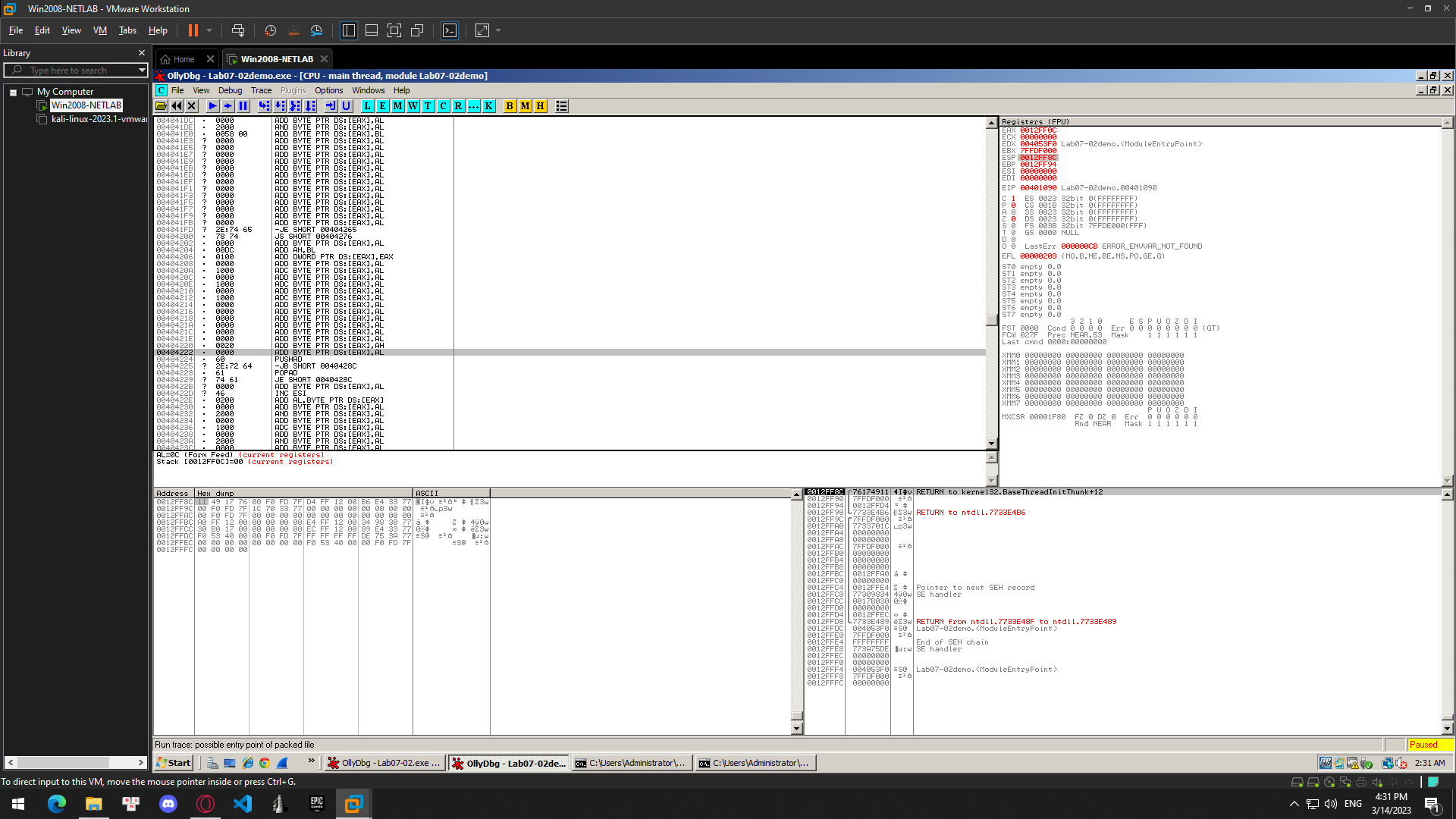
Sau đấy em sẽ pack file này để giải nén dữ liệu gốc trước khi file thực sự được thực thi vì

- File sẽ được thực thi ở một OEP (Original Entry Point) mới ( đoạn code được đưa vào cuối file khi Pack)  
- Nó sẽ lưu lại trạng thái của các thanh ghi hiện tại bằng lệnh PUSHAD.  
- Toàn bộ nội dung được Pack sẽ được giải nén.  
- “Import table” sẽ được sửa lại cho đúng với file thực thi ban đầu  
- Giá trị các thanh ghi được lưu lại trước đó sẽ được khôi phục bằng lệnh POPAD.  
- EIP nhảy đến OEP của file trước khi Pack, lúc này chương trình sẽ chính thức được thực thi.

=> Em sẽ pack bằng UPX và ta có được file sau

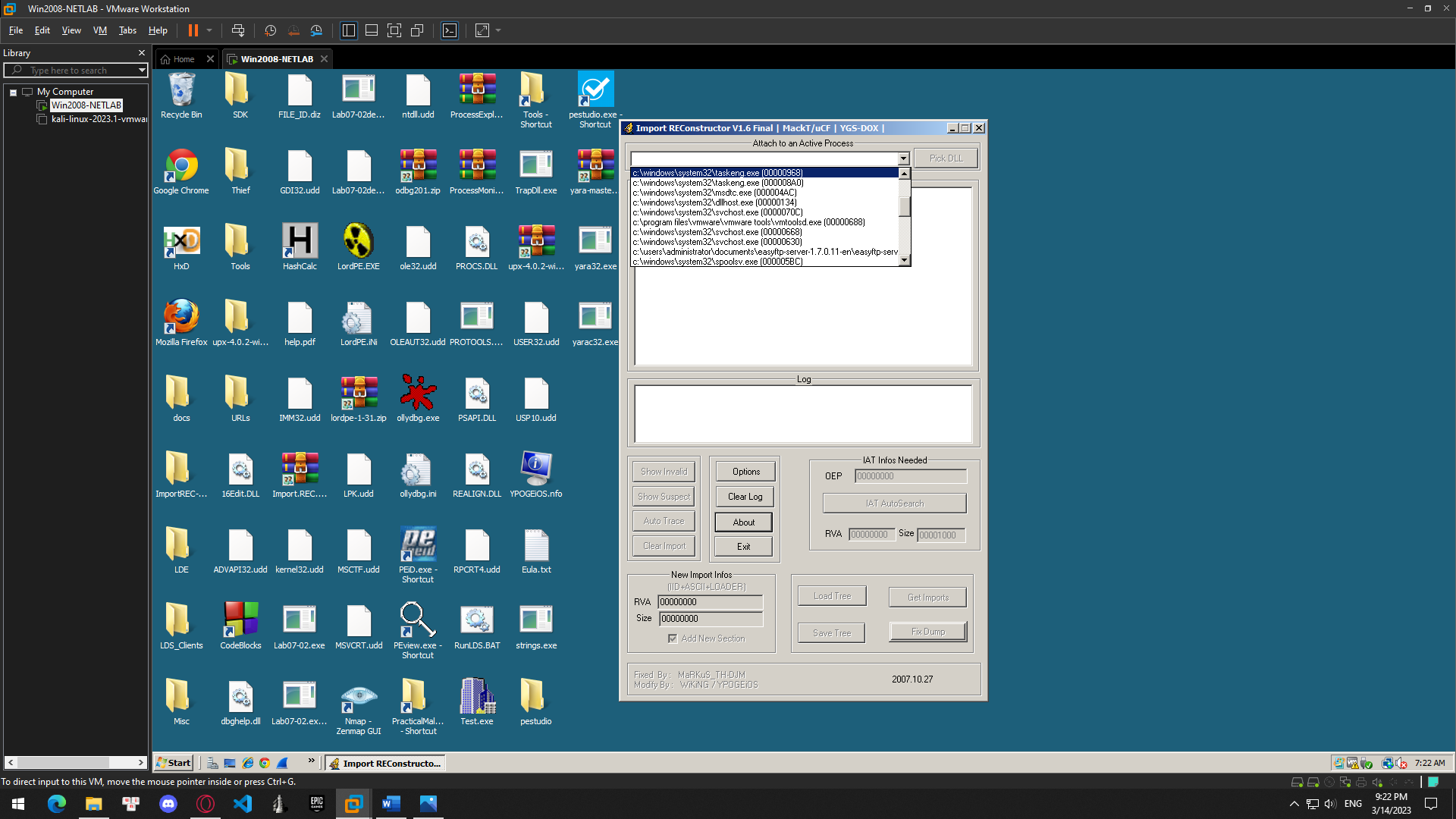
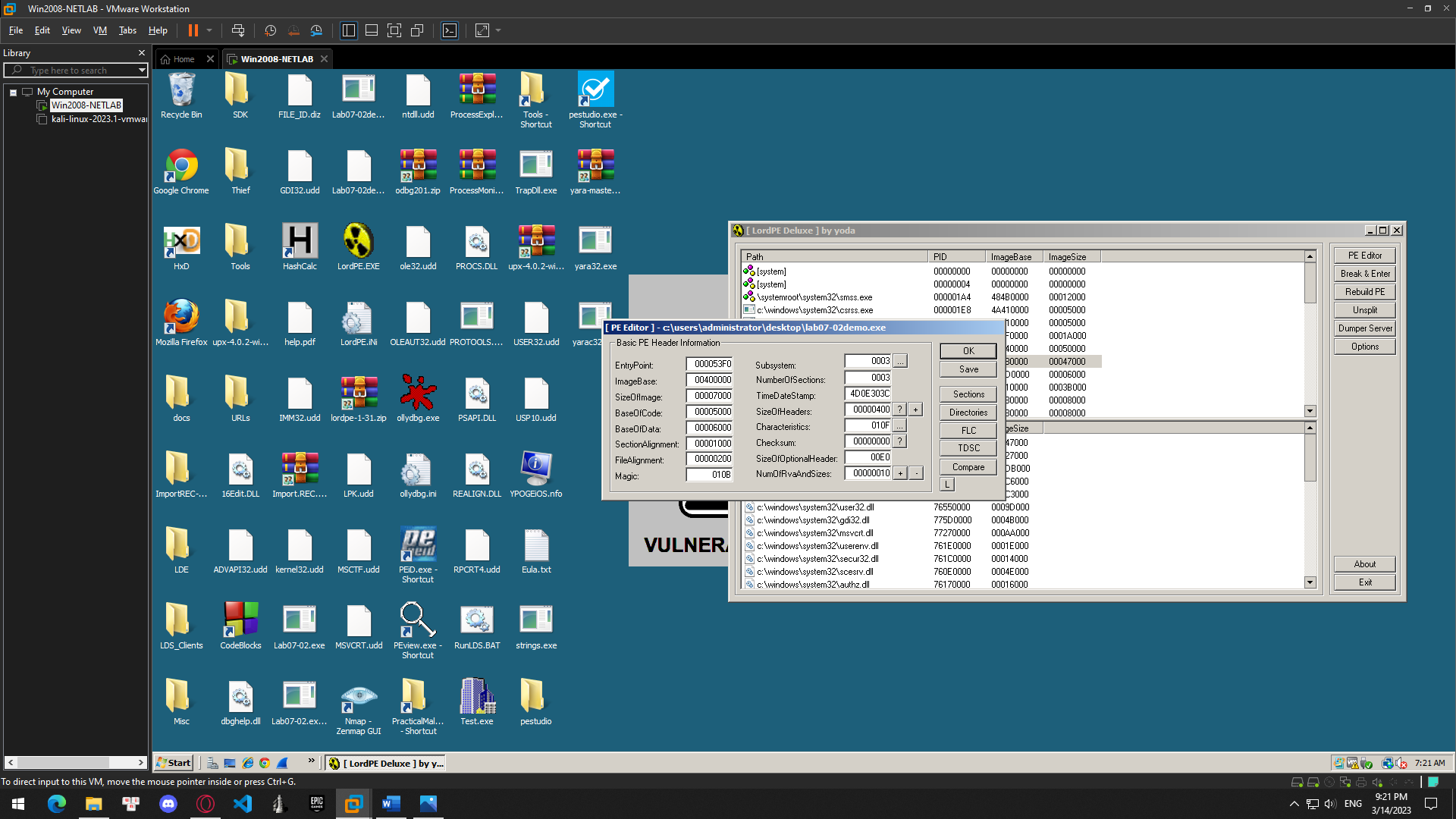


Bây giờ chúng ta load nó vào Olly để debug tìm OEP thực sự của nó

câu lệnh PUSHAD và POPAD. Thường là 2 câu lệnh bắt đầu và kết thúc công việc giải mã đoạn code thực thi của chương trình gốc.Nhưng ở đây khi thực thi 2 câu lệnh này thì ta không thấy ở comment để dẫn đến đoạn code OEP

* Khả năng cao là file chưa bị pack

Em kiểm tra thêm trên IAT và LordPE thì file không thực thi kể cả mình chạy file

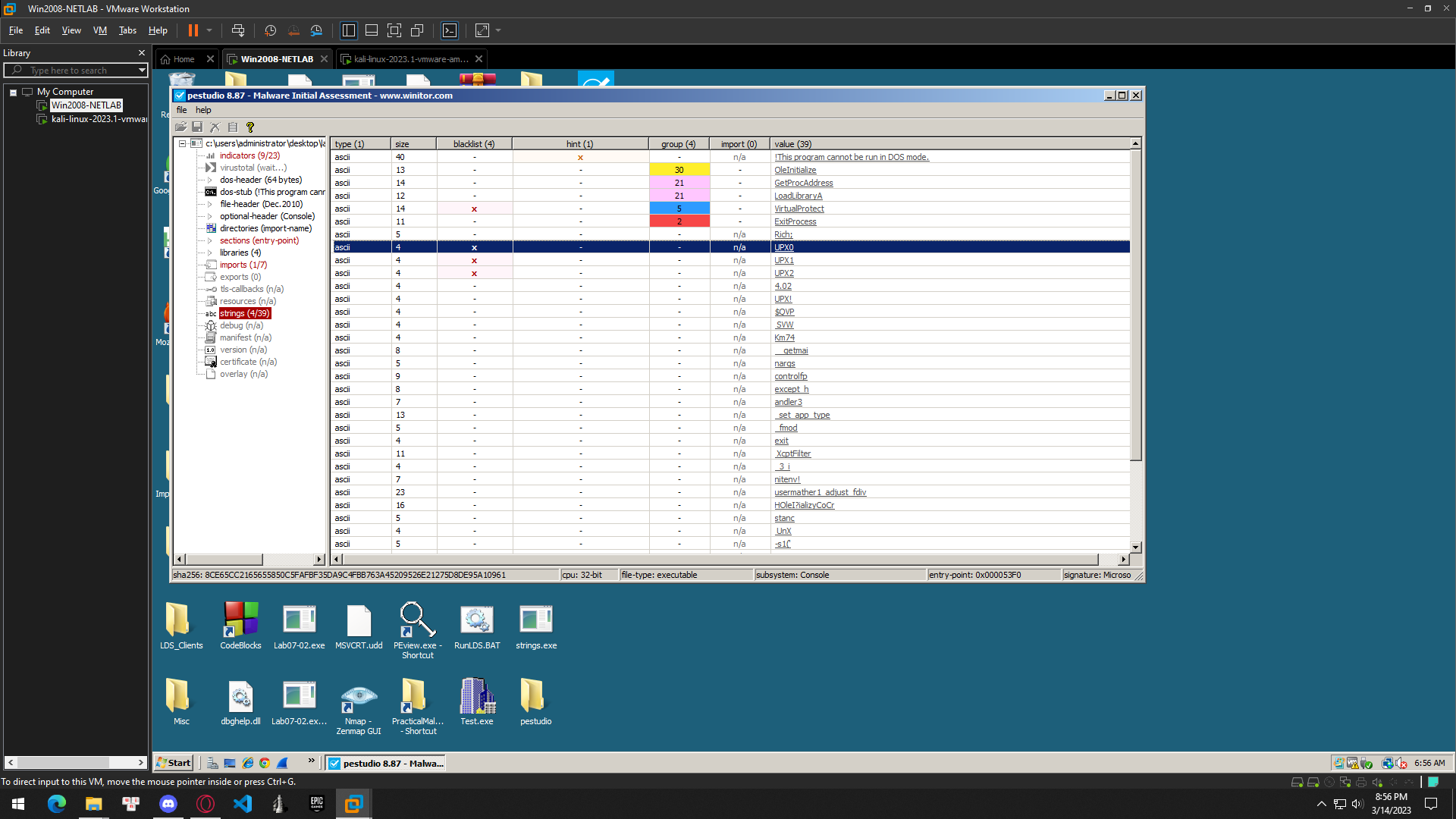


=> Mã độc không bị pack

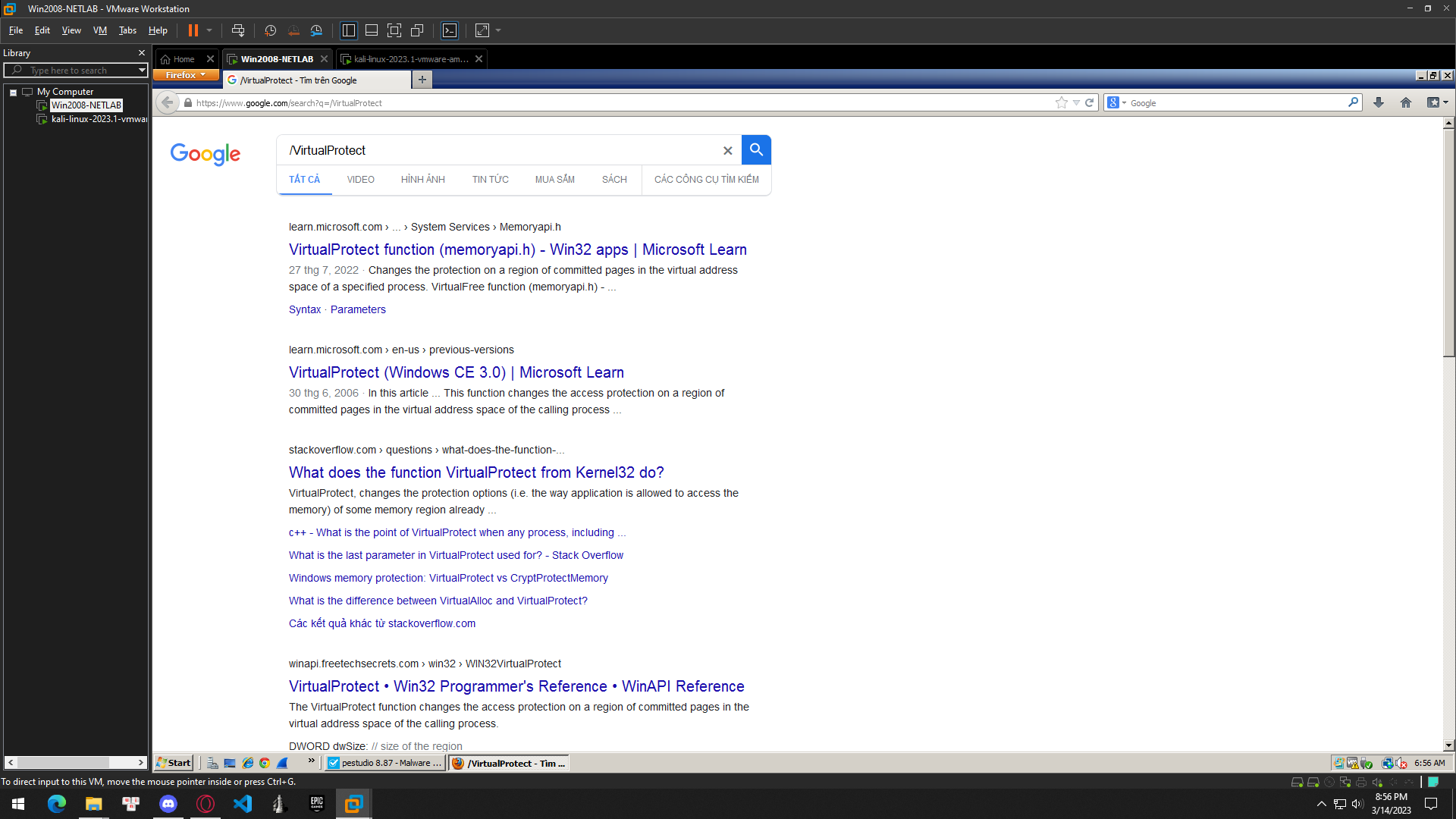
**2.** Mã độc thực hiện hành vi gì? (hành vi về mạng, hành vi tạo/sửa/xóa file, hành vi thay đổi registry, lây nhiễm vào đâu….) Với mỗi hành vi minh chứng bằng kết quả phân tích tĩnh và phân tích động**.**

+ Về Phân tích tĩnh :

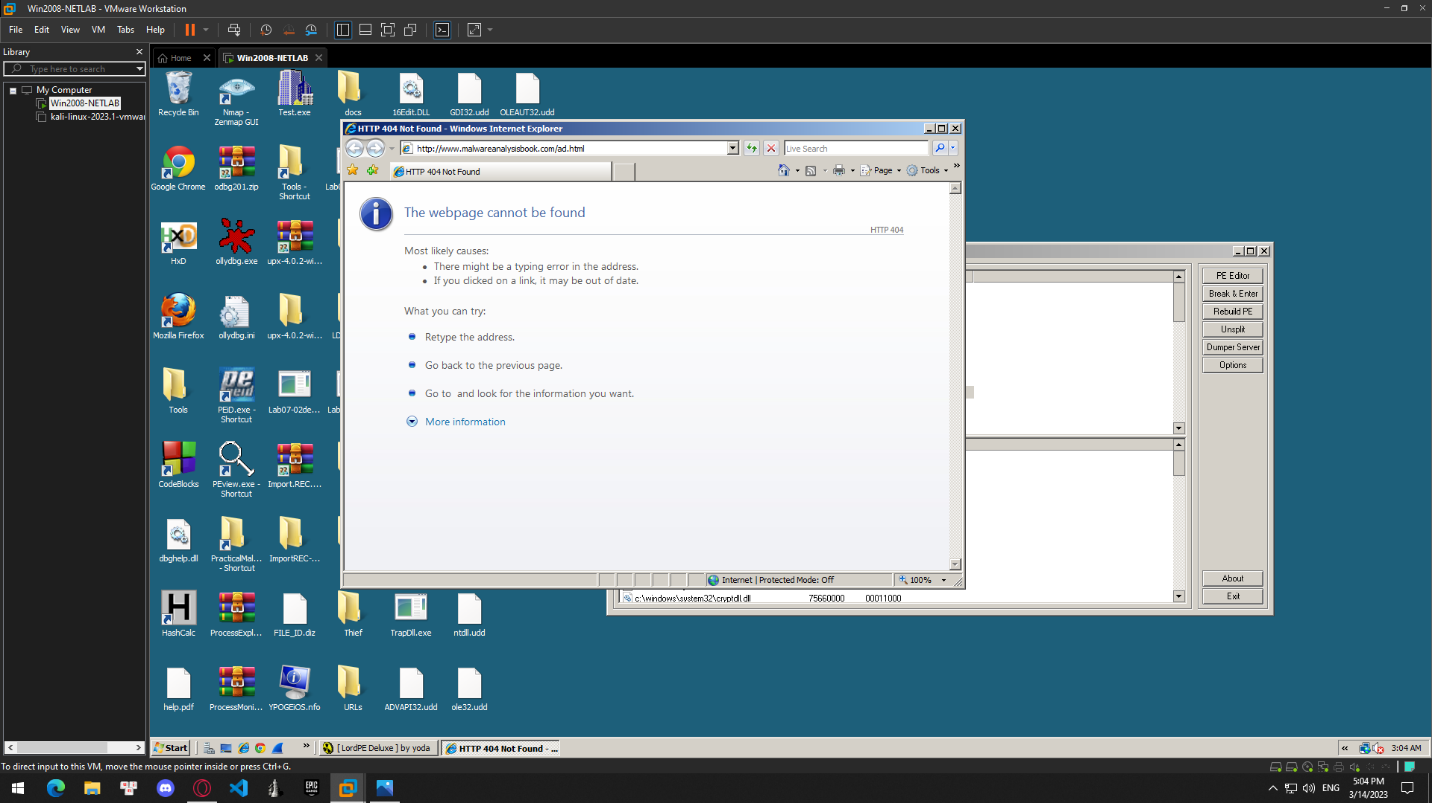
Em sử dụng MIA để kiểm tra cũng như sử dụng để tạo dấu hiệu YARA rules để kiểm tra mã độc Lab07-02.exe



Có thể thấy trong blacklist ta có UPX0 -3 và virtualprotect => trong lúc Pack Bằng UPX thì nó sinh ra trong Lab07-02

Virtualprotect em tra được trên mạng thì nó cho kết quả là Win32

+ Về Phân tích động :

Sau khi chạy thử file unpack và pack em nhận được kết quả đó chính là 

Có vẻ như đây là

Chương trình hiển thị một trang web quảng cáo cho người dùng.

Chương trình kết thúc thực thi sau khi hiển thị quảng cáo.

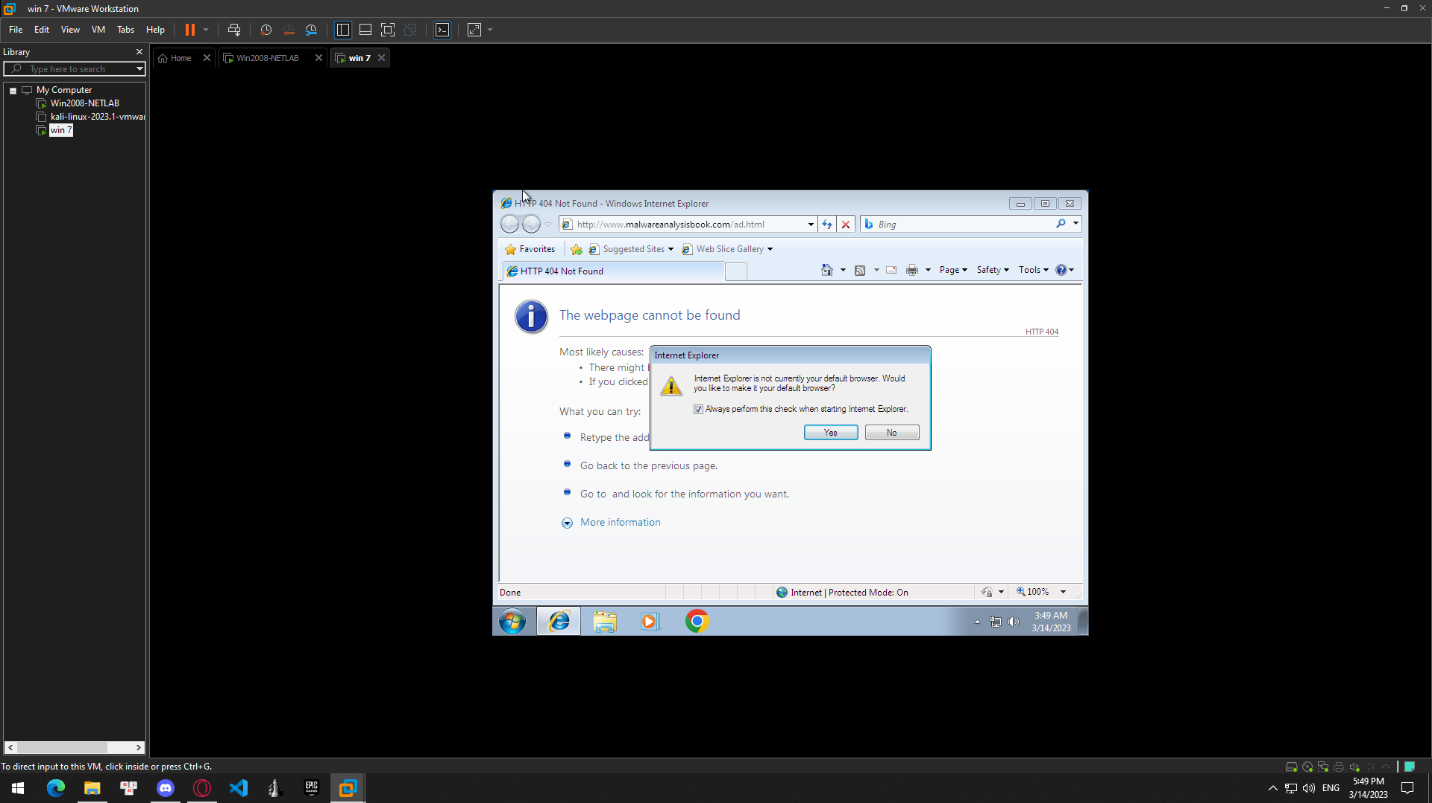
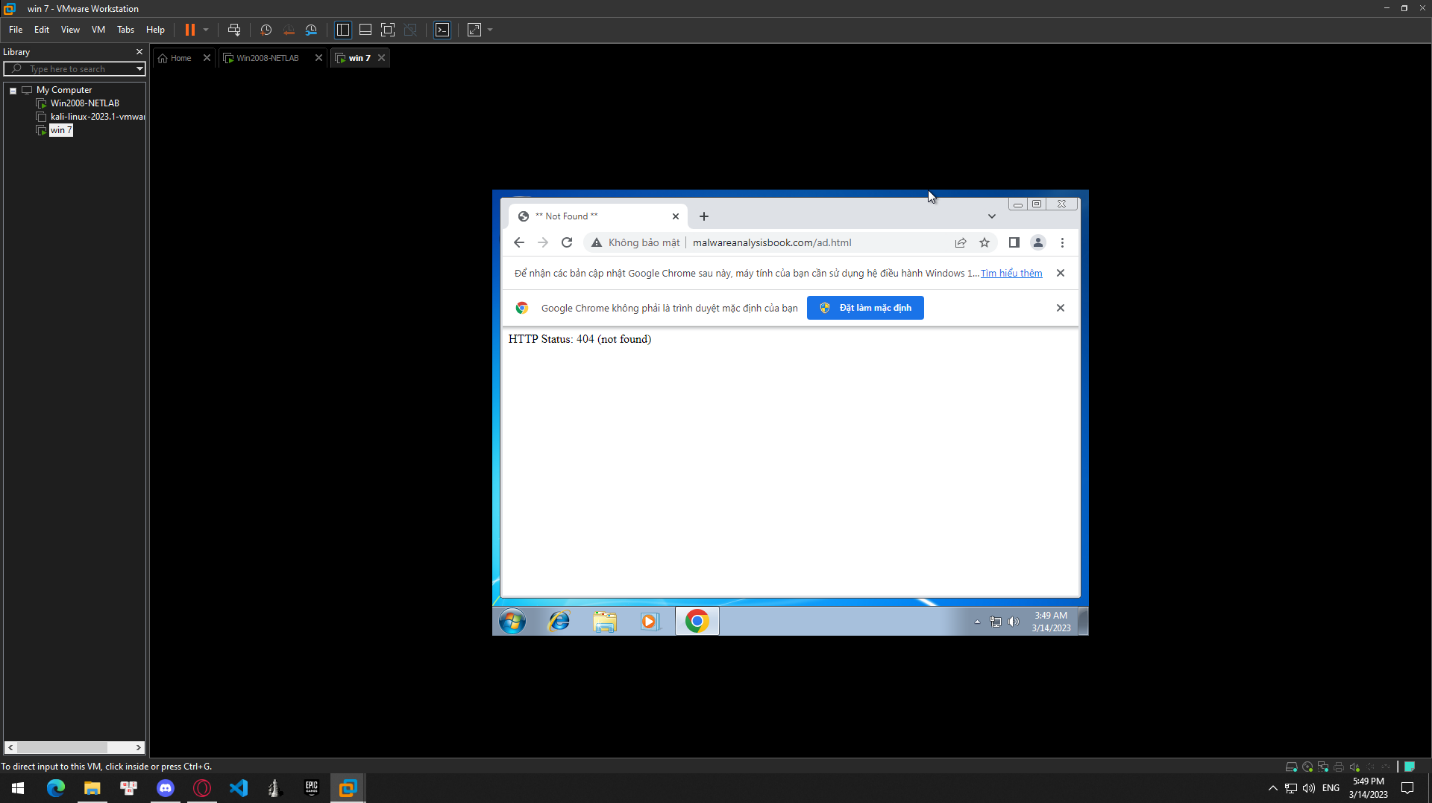
* Mã Độc thực hiện hành vi về mạng

3.Sử dụng hệ thống sandbox phân tích lại mã độc và đối chiếu với kết quả của yêu cầu 1, 2

Sử dụng sandbox thì giống với cái phân tích động

Chương trình hiển thị một trang web quảng cáo cho người dùng.

Chương trình kết thúc thực thi sau khi hiển thị quảng cáo



4.Tạo dấu hiệu nhận dạng trên YARA với mã độc trên.

Rule Lab07-02\_ru

{

meta :

Description = “Detects Rule Lab07-02\_ru”

Author = “Markus & Laszlo”

Reference = “www.malwareanalysisbook.com/ad.html”

Hash = “3f050d40174517359bd590c0e6ab7448”

Date = “Sun Dec 19 08:18:04 2010”

strings:

$mz = { 4d 5a}

$s1 = “UPX0”

$s2 = “UPX1”

$s3 = “UPX3”

$s4 = “www.malwareanalysisbook.com/ad.html”

condition:

($mz at 0, $s1 or $s2 or $s3 or $s4 )

}