

HỌC VIỆN KỸ THUẬT MẬT MÃ  
KHOA AN TOÀN THÔNG TIN  
-----

MODULE THỰC HÀNH  
MÃ ĐỘC

BÀI THỰC HÀNH SỐ 08

Phân tích một số kỹ thuật che giấu của mã độc

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 một số kỹ thuật che giấu mã độc.....	5
1.1. Mô tả .....	5
1.2. Chuẩn bị .....	5
1.3. Phân tích Lab13-01 .....	5

## **THÔNG TIN CHUNG VỀ BÀI THỰC HÀNH**

**Tên bài thực hành:** Phân tích một số kỹ thuật khởi chạy của mã độc

**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 một số kỹ thuật che giấu mã độc

## 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

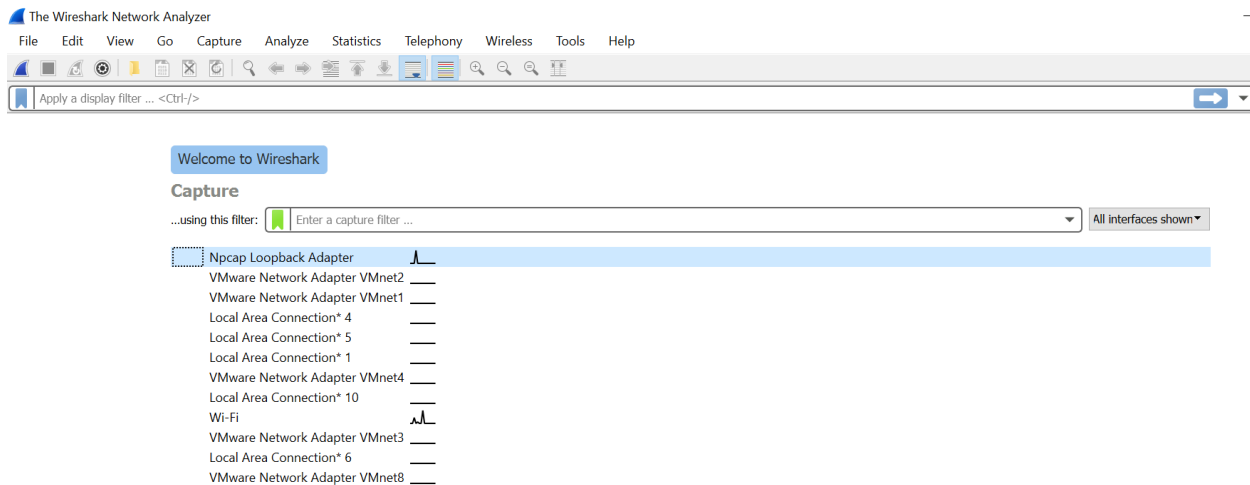
- Môi trường phân tích mã độc đã xây dựng trong Lab 1.

## 1.3. Phân tích Lab13-01

Trong bài thực hành này, chúng ta sẽ thực hành file Lab13-1.exe.

## SỬ DỤNG WIRESHARK ĐỂ BẮT ĐÈN HIỆU ( BEACON)

- Giới thiệu công cụ wireshark:
  - Công cụ wireshark được dùng để phân tích dữ liệu hệ thống mạng
  - Giao diện công cụ wireshark:



- Các chức năng chính của Wireshark:
  - + Phân tích chuyên sâu các giao thức mạng
  - + Thu thập dữ liệu từ nhiều nguồn tin

- + Đọc dữ liệu từ nhiều giao thức
- + Xuất dữ liệu sang nhiều định thức khác nhau
- Cách sử dụng Wireshark:
  - + Ở phần capture chọn interface mà bạn cần phân tích sau
- Khởi chạy file Lab13-01, điều chỉnh Wireshake để hiển thị hai đặc trưng sau:
  - GET/randomletter/HTTP/1.1
  - Host: www.practicalmalwareanalysis.com

Wireshark interface showing a packet capture on the http filter. The packet list shows a GET request to /V010LUpXQ1BQW1NY/. The packet details pane shows the Hypertext Transfer Protocol section with the request line and host field highlighted in red. The packet bytes pane shows the raw data of the request.

No.	Time	Source	Destination	Protocol	Length	Info
55	28.150...	192.168.67.145	192.0.78.24	HTTP	154	GET /V010LUpXQ1BQW1NY/ HTTP/1.1
58	28.185...	192.0.78.24	192.168.67.145	HTTP	461	HTTP/1.1 301 Moved Permanently
123	41.058...	192.168.67.145	192.35.177.64	HTTP	193	GET /roots/ HTTP/1.1
126	41.290...	192.35.177.64	192.168.67.145	HTTP	166	HTTP/1.1 200 OK
168	53.683...	192.168.67.145	118.69.17.31	HTTP	354	GET /msdown/ HTTP/1.1
217	54.224...	118.69.17.31	192.168.67.145	HTTP	1082	HTTP/1.1 200 OK
259	66.415...	192.168.67.145	118.69.17.29	HTTP	301	GET /MFEwTzI HTTP/1.1
262	66.433...	118.69.17.29	192.168.67.145	OCSP	391	Response
302	78.581...	192.168.67.145	118.69.17.63	HTTP	311	GET /MFMwUTI HTTP/1.1
304	78.896...	118.69.17.63	192.168.67.145	OCSP	967	Response
335	100.48...	192.168.67.145	192.0.78.24	HTTP	154	GET /V010LUpXQ1BQW1NY/ HTTP/1.1

Internet Protocol Version 4, Src: 192.168.67.145, Dst: 192.0.78.24

Transmission Control Protocol, Src Port: 1031, Dst Port: 80, Seq: 1, Ack: 1, Len: 100

Hypertext Transfer Protocol

GET /V010LUpXQ1BQW1NY/ HTTP/1.1\r\n

User-Agent: Mozilla/4.0\r\n

Host: www.practicalmalwareanalysis.com\r\n

[Full request URI: http://www.practicalmalwareanalysis.com/V010LUpXQ1BQW1NY/]

[HTTP request 1/1]

[Response in frame: 58]

0000 00 50 56 f7 f9 62 00 0c 29 20 07 1b 08 00 45 00 ·PV·b· ) ···E·

0010 00 8c 00 5f 40 00 80 06 e7 ba c0 a8 43 91 c0 00 ···\_@· ····C·

0020 4e 18 04 07 00 50 3a 8a 8d 41 24 de 41 d2 50 18 N· ·P:· ·A\$·A·P·

0030 fa f0 4e 70 00 00 47 45 54 20 2f 56 30 6c 4f 4c ··Np·GE T /V010L

0040 55 70 58 51 6c 42 51 57 6c 4e 59 2f 20 48 54 54 UpXQ1BQW 1NY/ HTT

0050 50 2f 31 2e 31 0d 0a 55 73 65 72 2d 41 67 65 6e P/1.1·U ser-Agen

0060 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 34 2e 30 0d 0a t: Mozil la/4.0·

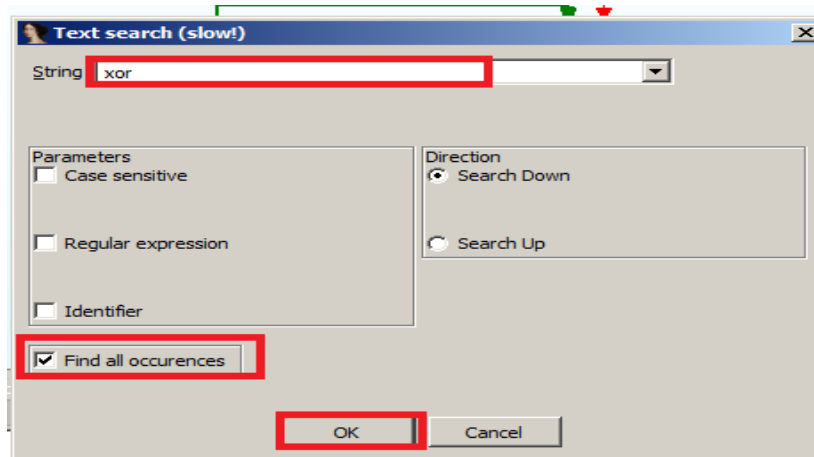
## CÔNG CỤ STRING

- Sử dụng string để kiểm tra các chuỗi trong file Lab13-01.

```
Administrator: C:\Windows\System32\cmd.exe
tiW
Yt<
%~i@
Xi@
_ ^]l
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/-
EEE
<8P%
700WP
'h
ppxxxx
(null)
(null)
runtime error
TLOSS error
SING error
DOMAIN error
R6028
- unable to initialize heap
R6027
- not enough space for lowio initialization
R6026
- not enough space for stdio initialization
R6025
- pure virtual function call
```

## CÔNG CỤ IDA PRO

- Mở file Lab13-01 trong IDA Pro, chọn Options, chọn General, tích “Line Prefixes”, chọn OK.
- Nhấp vào cửa sổ “IDA View-A” để kích hoạt nó.
- Từ thanh menu, chọn “Search”, “text”
- Trong hộp “Text Search”, nhập xor, và tích “Find All occurrences”



- Một danh sách hiển thị các vị trí sử dụng lệnh XOR sẽ xuất hiện như hình dưới.

Address	Function	Instruction
.text:00401007	sub_401000	xor ecx, ecx
.text:0040101C	sub_401000	xor edx, edx
.text:00401029	sub_401000	xor ecx, ecx
.text:0040104E	sub_401000	xor eax, eax
.text:0040105C	sub_401000	xor edx, edx
.text:0040108D	sub_401000	xor ecx, ecx
.text:004011B4	sub_401190	xor eax, eax
.text:004011B8	sub_401190	xor eax, 3Bh
.text:004011D6	sub_4011C9	xor eax, eax
.text:004012A2	sub_4011C9	xor al, al
.text:004012E6	sub_4011C9	xor al, al
.text:004012FA	sub_4011C9	xor al, al
.text:00401332	sub_401300	xor eax, eax
.text:00401350	sub_401300	xor eax, eax
.text:0040138E	sub_401300	xor eax, eax
.text:00401463	_main	xor eax, eax
.text:004021E5		xor ecx, ecx
.text:00402202		xor edx, edx
.text:00402BE2		xor dh, [eax]
.text:00402BE6		xor [eax], dh

Line 1 of 20

- Nhấp đúp vào xor eax 3Bh, sẽ hiển thị theo hình dưới.



```

00401190
00401190
00401190 ; Attributes: bp-based frame
00401190
00401190 sub_401190 proc near
00401190
00401190 var_4= dword ptr -4
00401190 arg_0= dword ptr 8
00401190 arg_4= dword ptr 0Ch
00401190
00401190 push    ebp
00401191 mov     ebp, esp
00401193 push    ecx
00401194 mov     [ebp+var_4], 0
0040119B jmp     short loc_4011A6

```

```

004011A6
004011A6 loc_4011A6:
004011A6 mov     ecx, [ebp+var_4]
004011A9 cmp     ecx, [ebp+arg_4]
004011AC jnb     short loc_4011C5

```

```

004011AE mov     edx, [ebp+arg_0]
004011B1 add     edx, [ebp+var_4]
004011B4 xor     eax, eax
004011B6 mov     al, [edx]
004011B8 xor     eax, 3Bh
004011BB mov     ecx, [ebp+arg_0]
004011BE add     ecx, [ebp+var_4]
004011C1 mov     [ecx], al
004011C3 jmp     short loc_40119D

```

```

004011C5
004011C5 loc_4011C5:
004011C5 mov     esp, ebp
004011C7 pop     ebp
004011C8 retn
004011C8 sub_401190 endp
004011C8

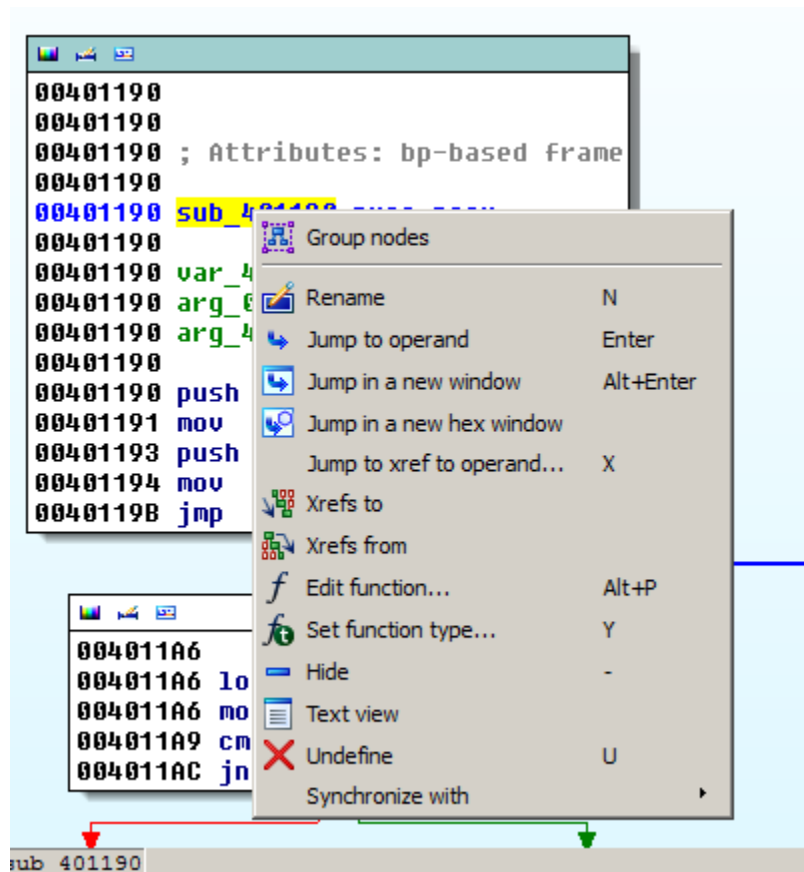
```

```

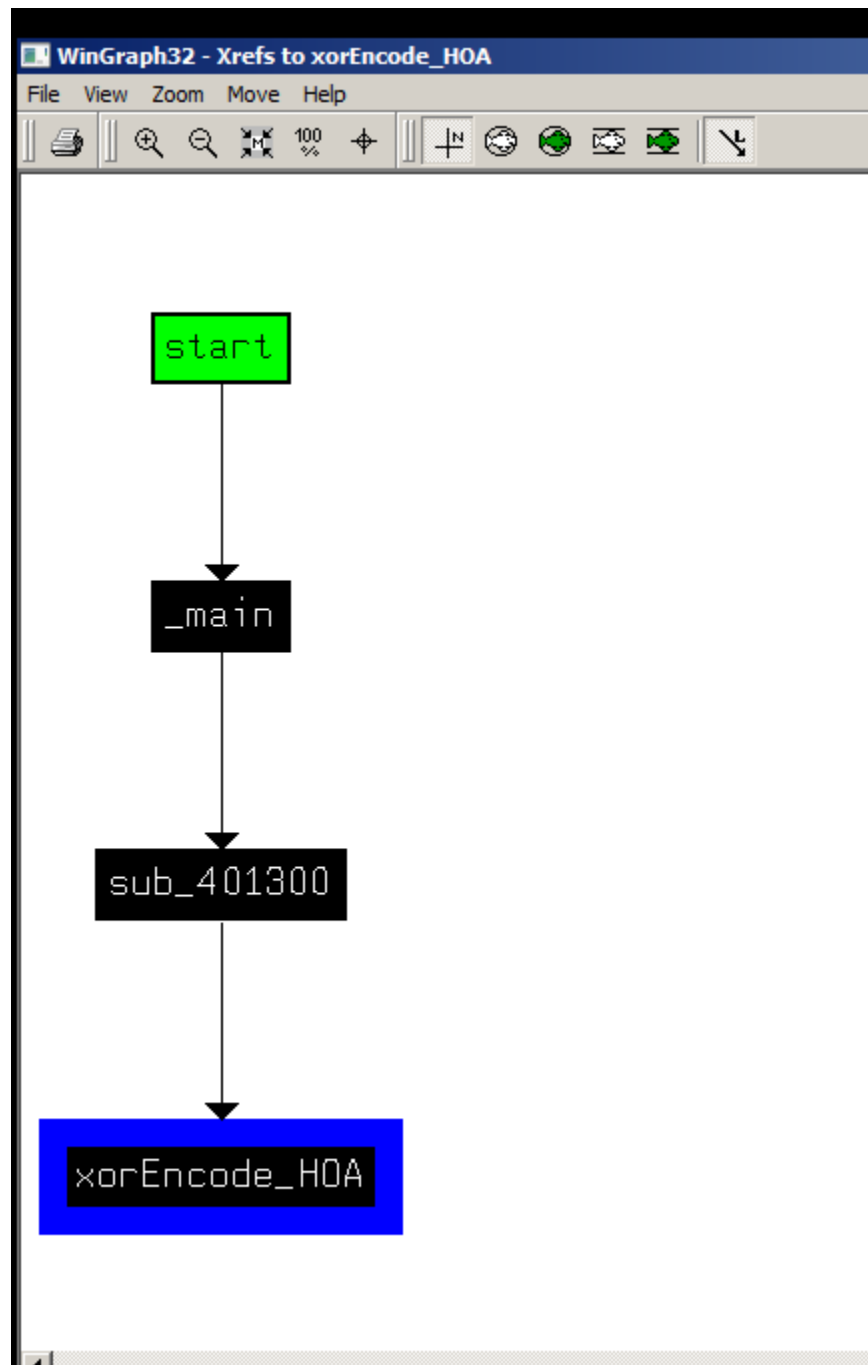
0040119D
0040119D loc_40119D:
0040119D mov     eax, [ebp+var_4]
004011A0 add     eax, 1
004011A3 mov     [ebp+var_4], eax

```

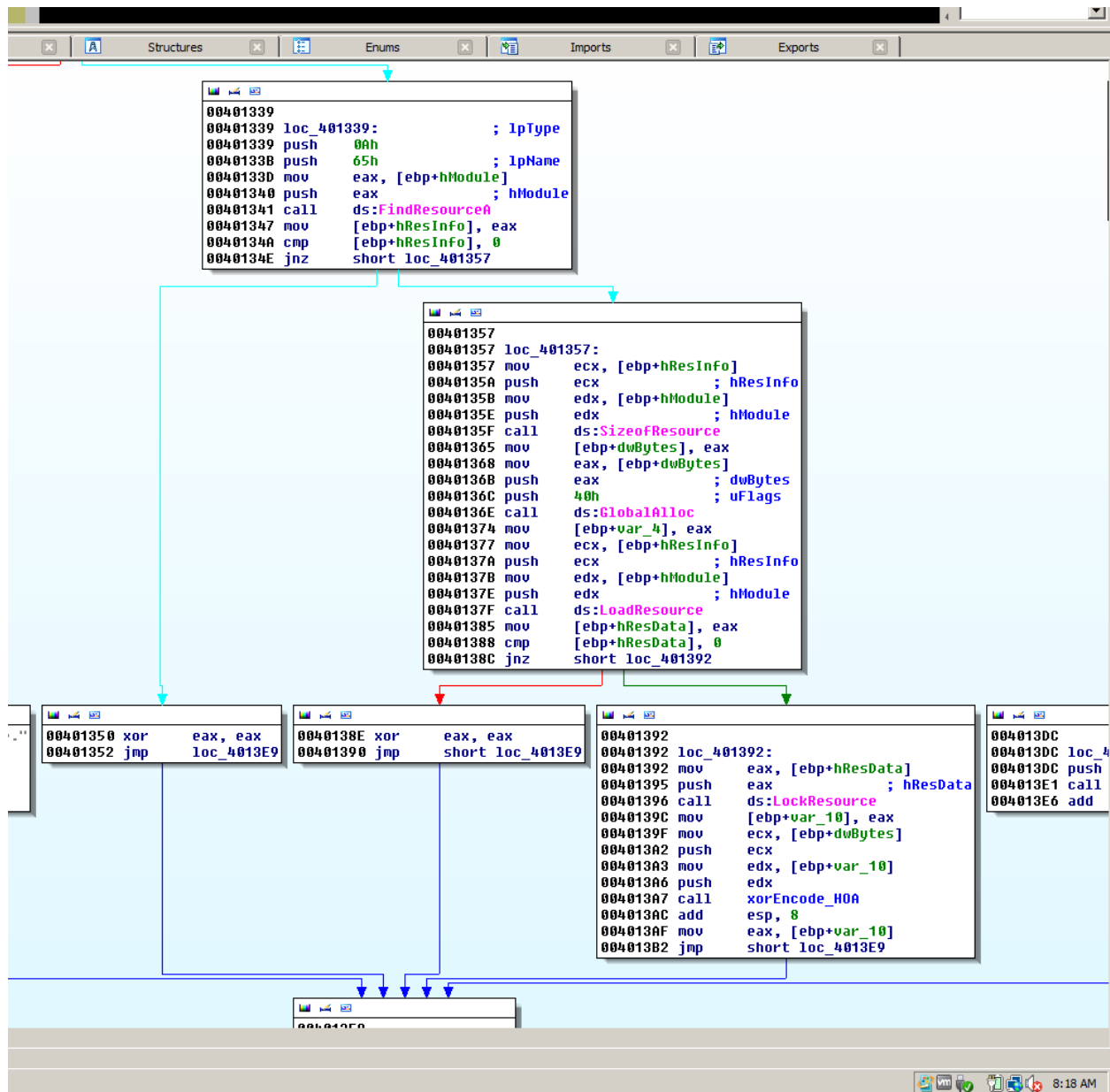
- Trong hộp trên cùng của hàm, nhấp chuột phải vào sub\_401190 và bấm đổi tên theo hình bên dưới.



- Nhập tên mới của thành xorEncode\_YOURNAME.
- Nhấp chuột phải vào xorEncode-YOURNAME và nhấp vào “Chart of xrefs to”
- Một biểu đồ hiển thị bốn hộp xuất hiện , kết thúc bằng một hộp chứa tên bạn.



- Nhấp chuột phải vào xorEncode\_YOURNAME ( ở đây là xorEncode\_HOA) và chọn “Jump to xref to operand”
- Một hộp hiện lên địa chỉ của xref, chọn OK
- Hàm này, như hiển thị bên dưới

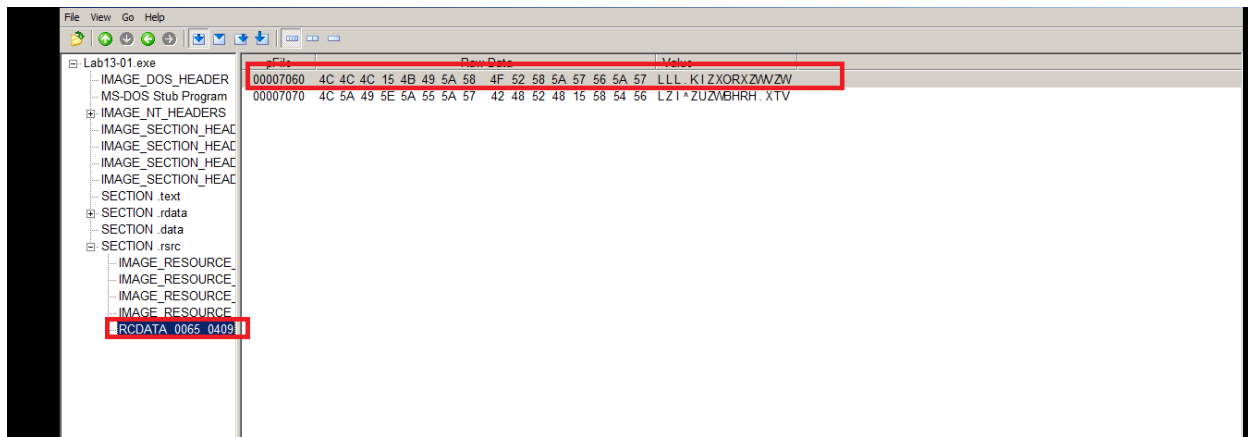


- Mã này tải một tài nguyên được mã hóa

## CÔNG CỤ PEVIEW

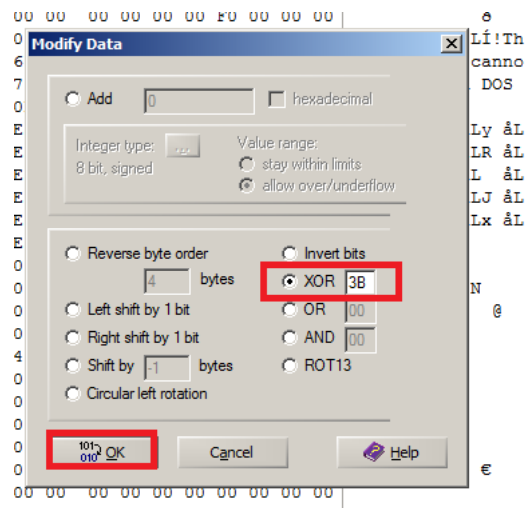
- Mở file Lab13-01 trong PEView.
- Trong khung bên trái, chọn tài nguyên RCDATA 0065 0409.

- Trong khung bên phải, tìm địa chỉ bắt đầu 00007060, như hiển thị hình bên dưới.



## CÔNG CỤ WINHEX

- Trong Winhex, chọn File, Open Lab13-01, chú ý từ bytes 7060 đến bytes 707F, chọn Edit, chọn Modify.
- Trong “Modify Block Data” chọn “XOR” và nhập khóa “3B”, rồi chọn OK



- Chuỗi được giải mã sẽ xuất hiện phía bên phải.

```
Lab13-01.exe
Offset  0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  ANSI ASCII
00006FC0  3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B  :
00006FD0  3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B  :
00006FE0  3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B  :
00006FF0  3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B  :
00007000  3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3A 3B  :
00007010  31 3B 3B 3B 23 3B 3B BB 3B 3B 3B 3B 3B 3B 3B 3B 1::#::»::
00007020  3B 3B 3B 3B 3B 3B 3A 3B 5E 3B 3B 3B 0B 3B 3B BB  :
00007030  3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3A 3B  :
00007040  32 3F 3B 3B 73 3B 3B 3B 5B BB 3B 3B 1B 3B 3B 3B 2?::s::[::»::
00007050  3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B  :
00007060  77 77 77 2E 70 72 61 63 74 69 63 61 6C 6D 61 6C  www.practicalmal
00007070  77 61 72 65 61 6E 61 6C 79 73 69 73 2E 63 6F 6E  wareanalysis.com
00007080  3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B  :
00007090  3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B  :
000070A0  3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B  :
000070B0  3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B  :
000070C0  3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B  :
000070D0  3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B  :
000070E0  3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B  :
000070F0  3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B  :
00007100  3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B  :
00007110  3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B  :
00007120  3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B  :
00007130  3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B  :
00007140  3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B  :
00007150  3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B  :
00007160  3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B  :
00007170  3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B  :
00007180  3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B  :
00007190  3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B  :
```