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

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 Worstation 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

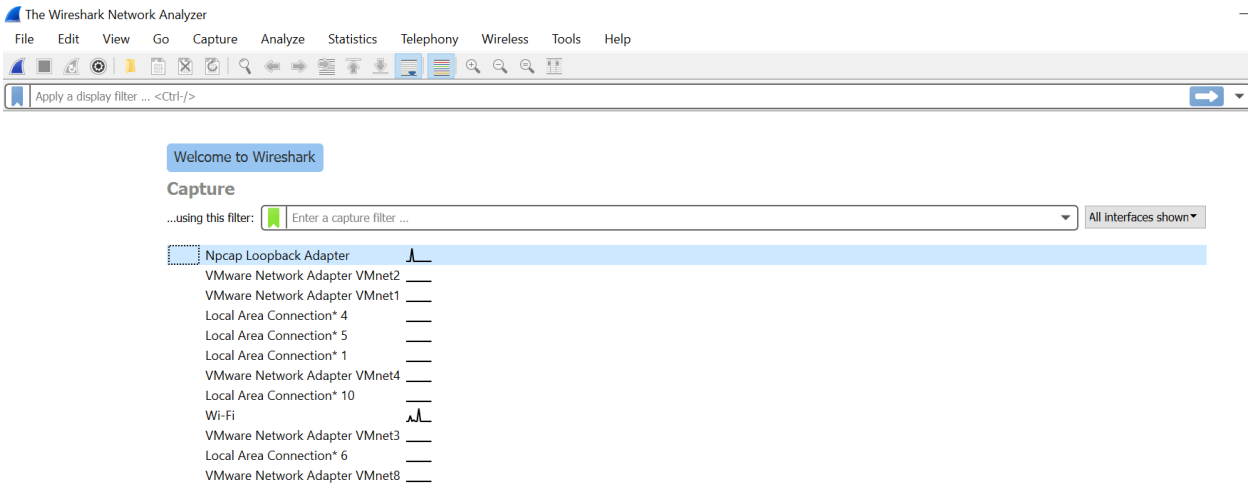
- Môi trường phân tích mã độc đã xây dựng trong Lab 1.

1.3. Phân tích Lab13-01

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

SỬ DỤNG WIRESHARE 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:

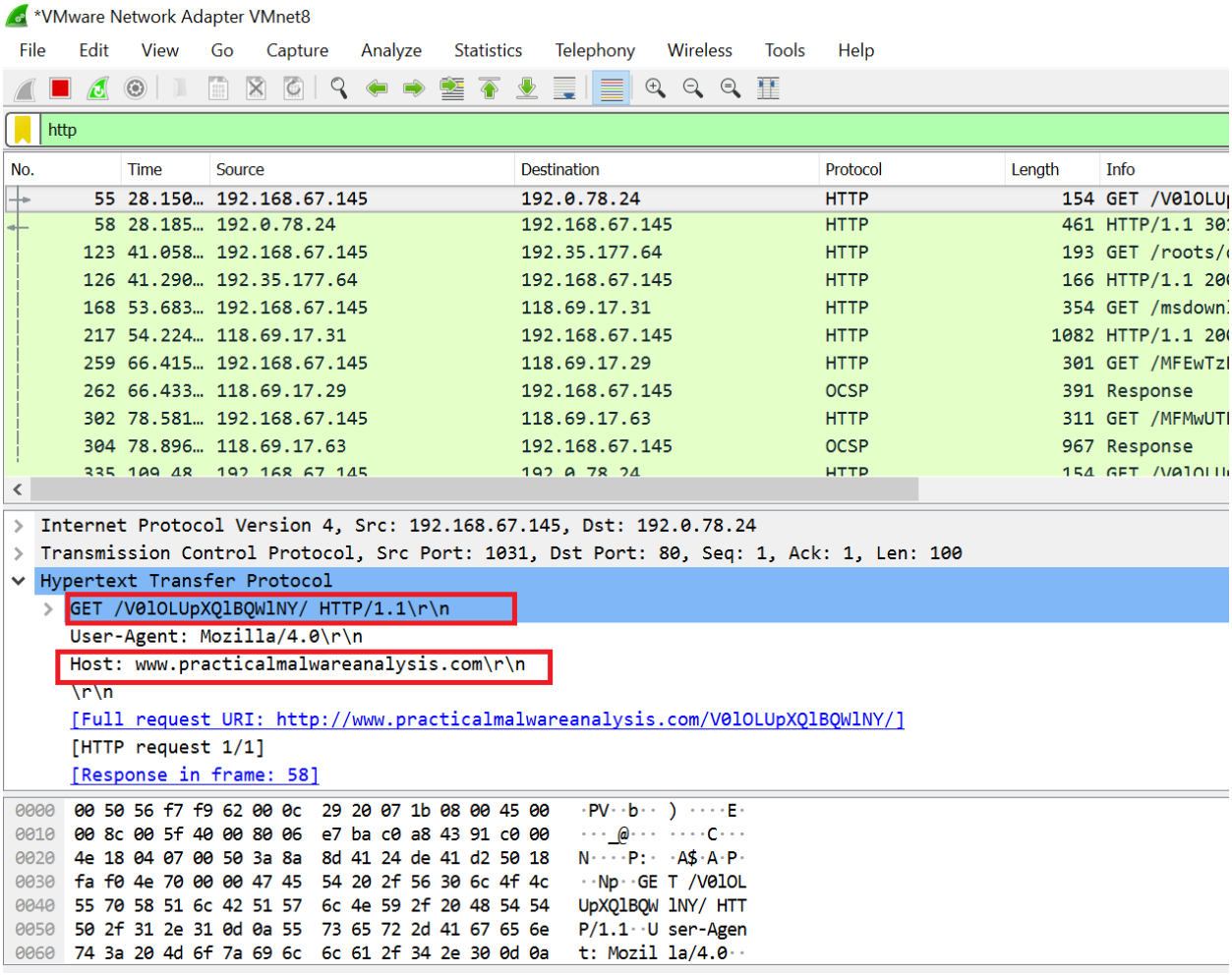


  - Các chức năng chính của Wireshark:
    + Phân tích chuyên sâu các giao thức mạng
    + Thu thập dữ liệu từ nhiều nguồn tin

+ Đọc dữ liệu từ nhiều giao thức
+ Xuất dữ liệu sang nhiều định thức khác nhau

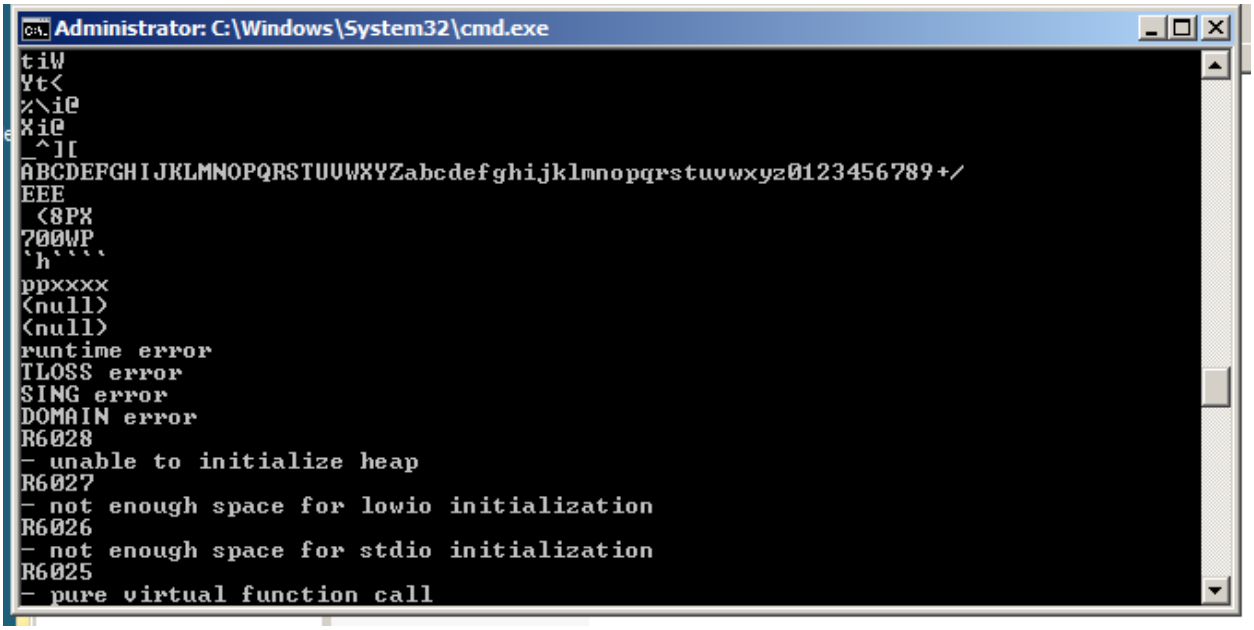
- Cách sử dụng Wireshark:
  + Ở phần capture chọn interface mà bạn cần phân tích sau

– Khởi chạy file Lab13-01, điều chỉnh Wireshake để hiển thị hai đặc trưng sau:
  - GET/randomletter/HTTP/1.1
  - Host: www.practicalmalwareanylysis.com



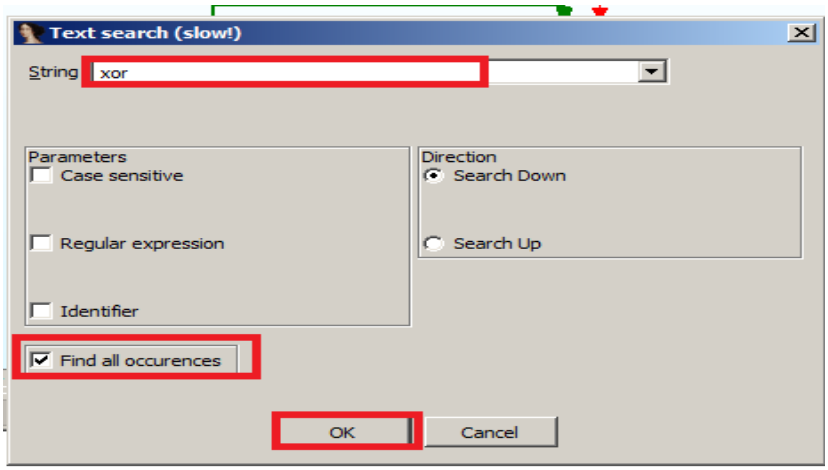
CÔNG CỤ STRING

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



CÔNG CỤ IDA PRO

- Mở file Lab13-01 trong IDA Pro, chọn Options, chọn General, tích "Line Prefixs", 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"

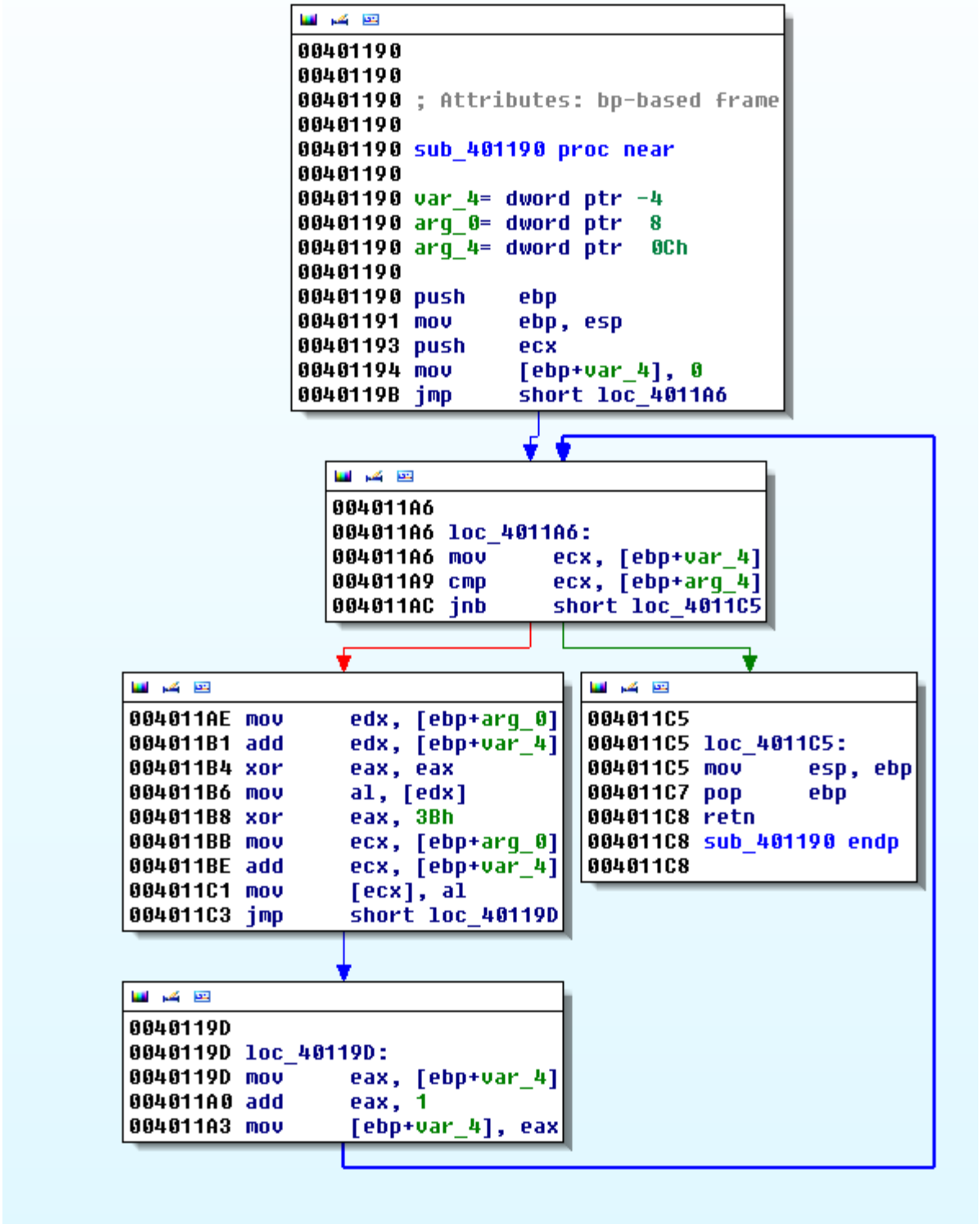


- Một danh sách hiển thị các vị trí sử dụng lệnh XOR sẽ xuất hiện như hình dưới.

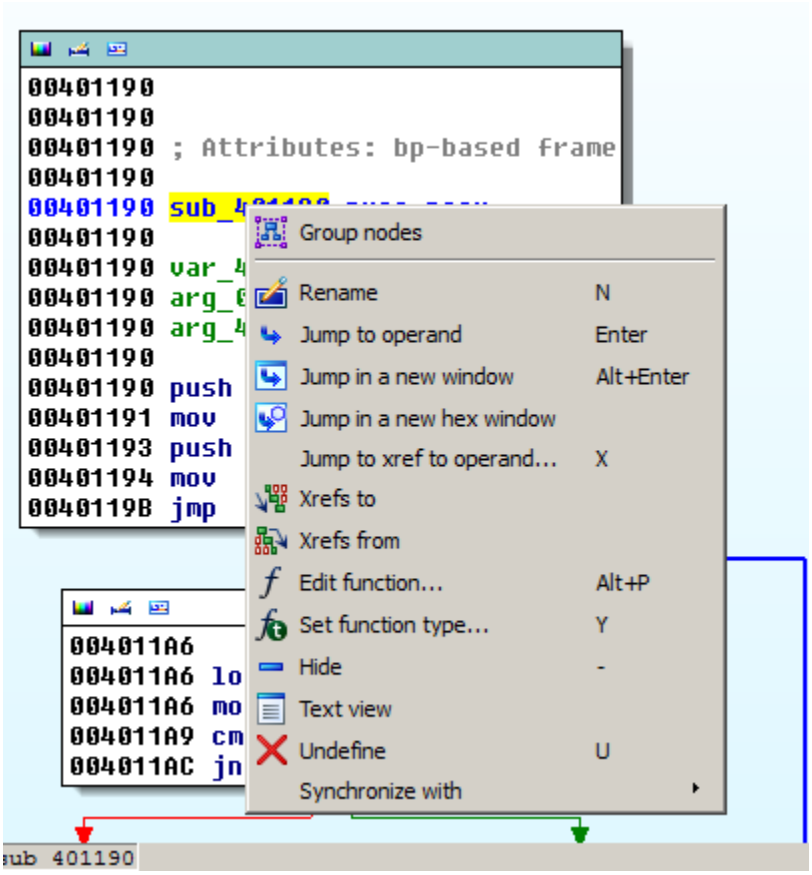
Address	Function	Instruction	
.text:00401007	sub_401000	xor	ecx, ecx
.text:0040101C	sub_401000	xor	edx, edx
.text:00401029	sub_401000	xor	ecx, ecx
.text:0040104E	sub_401000	xor	eax, eax
.text:0040105C	sub_401000	xor	edx, edx
.text:0040108D	sub_401000	xor	ecx, ecx
.text:004011B4	sub_401190	xor	eax, eax
.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

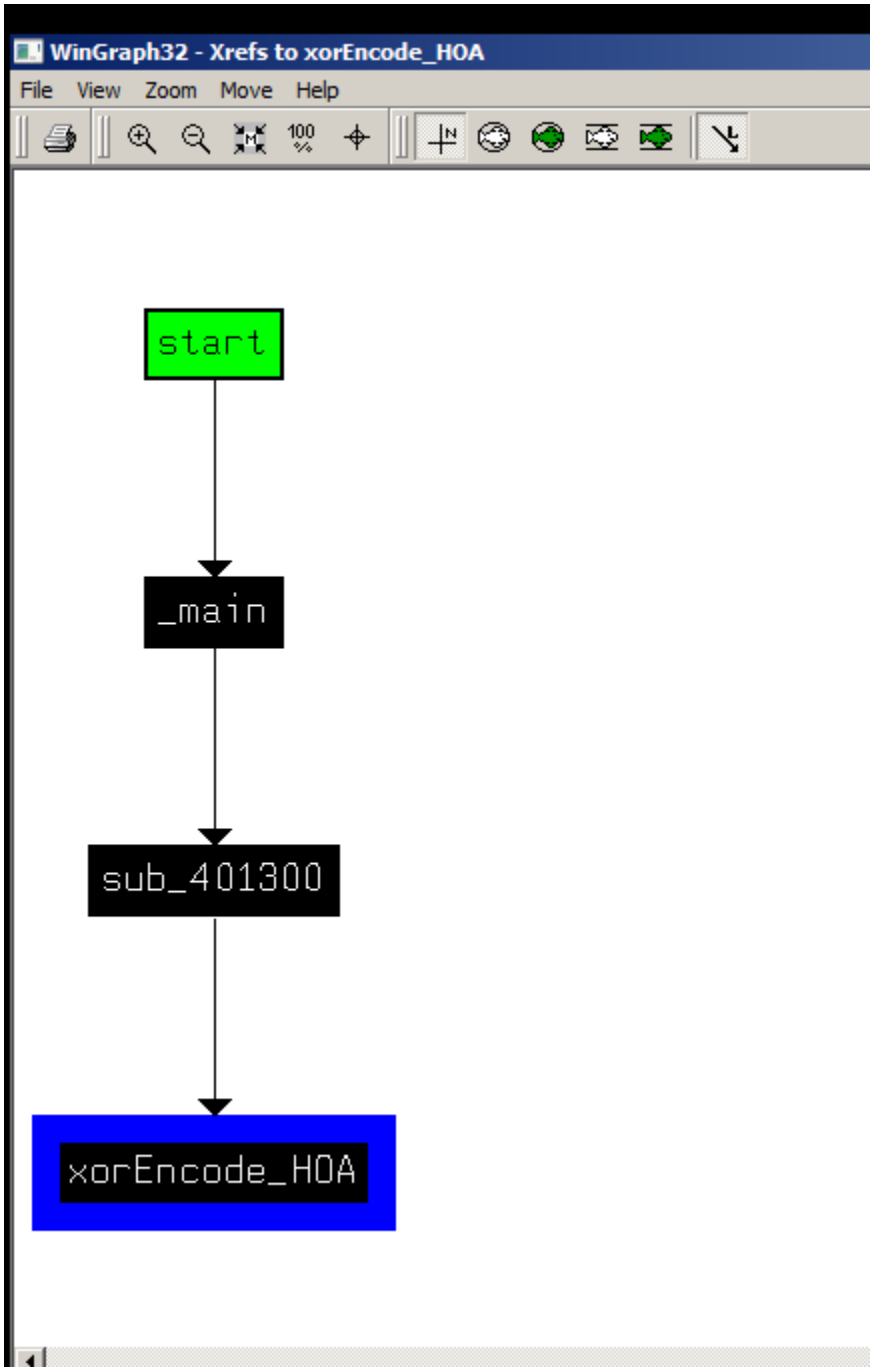
- Nhấp đúp vào xor eax 3Bh, sẽ hiển thị theo hình dưới.


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

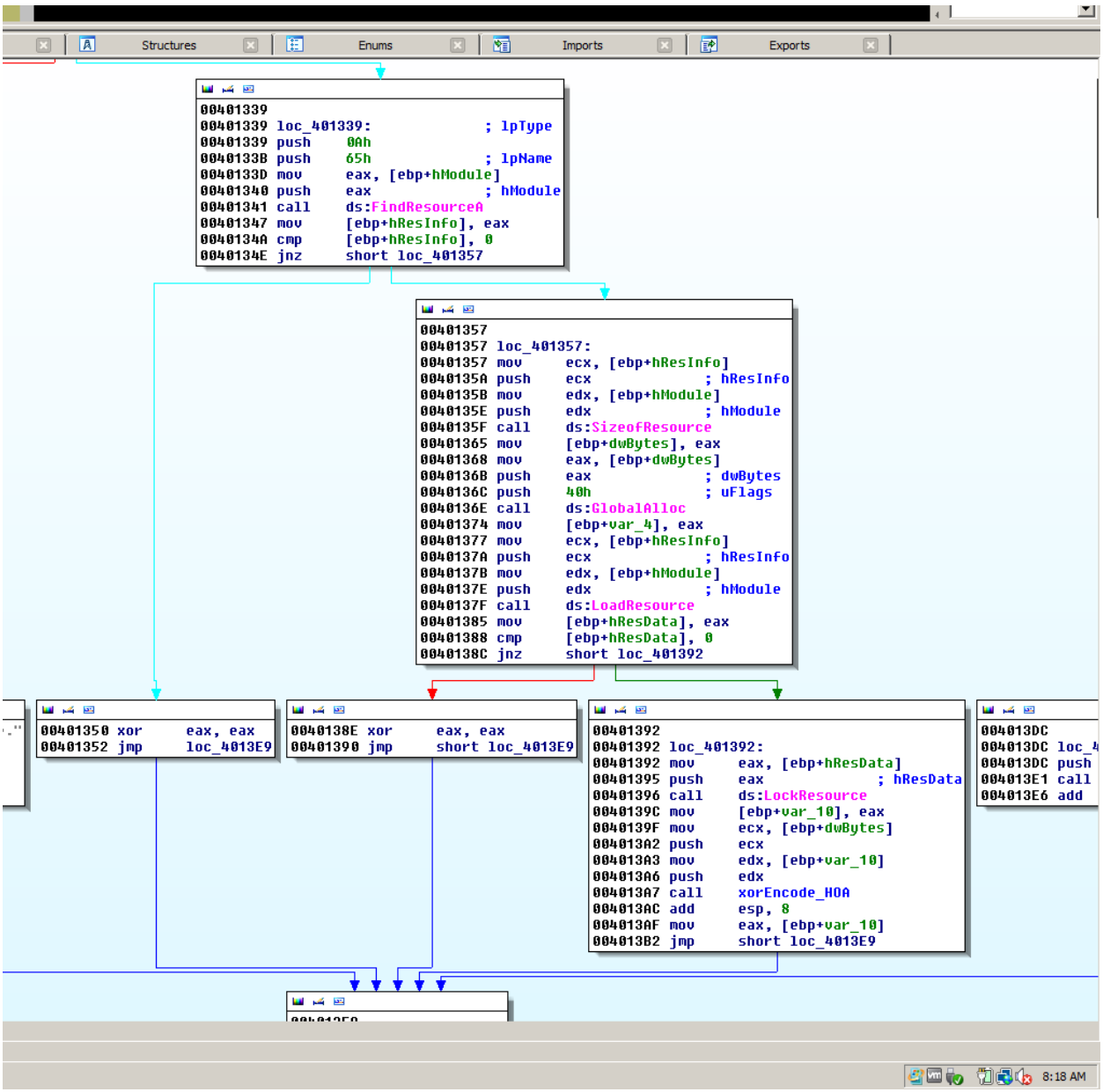
- Trong hộp trên cùng của hàm, nhấp chuột phải vào sub_401190 và bấm đổi tên theo hình bên dưới.



- 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

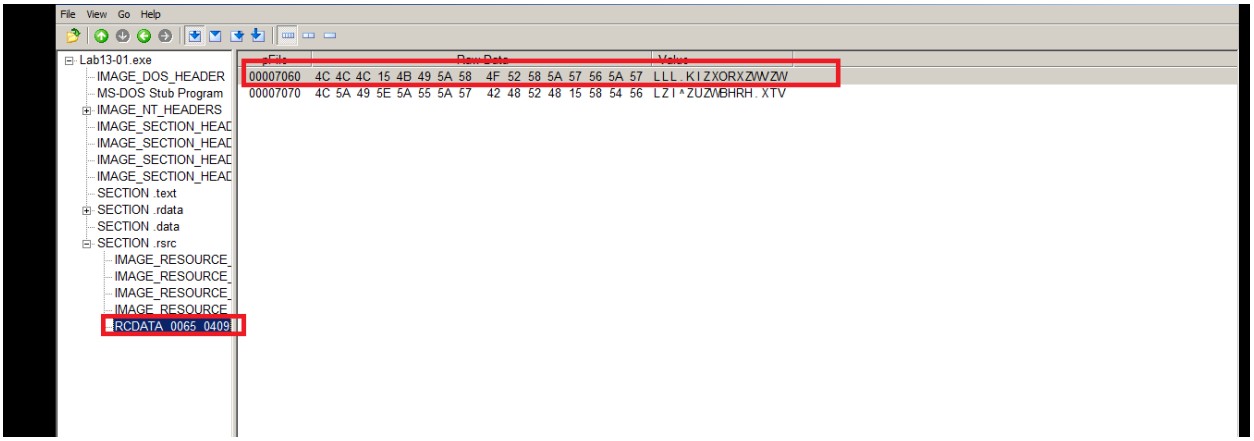


- Mã này tải một tài nguyên được mã hóa

CÔNG CỤ PEVIEW

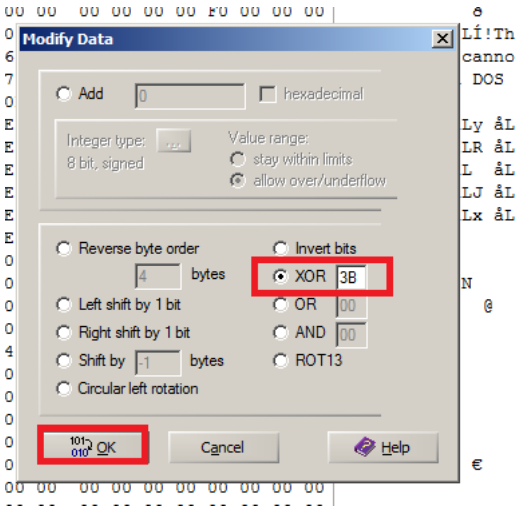
- Mở file Lab13-01 trong PEView.
- Trong khung bên trái , chọn tài nguyên RCDATA 0065 0409.

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

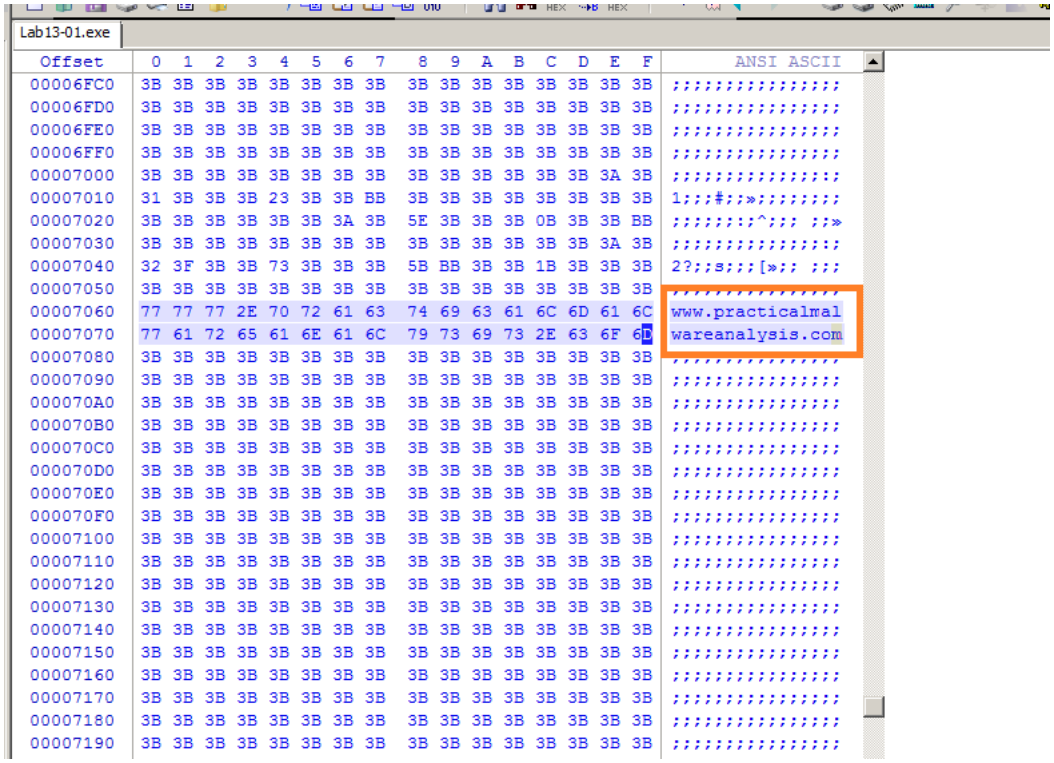


CÔNG CỤ WINHEX

- 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	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	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	6D	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	;;;;;;;;;;;;;;;;