Lab 14: Data Encoding

Course Name: Malware Analysis and Reverse Engineering (IAM302)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 29/2/2023

Purpose

You will practice the techniques in chapter 13

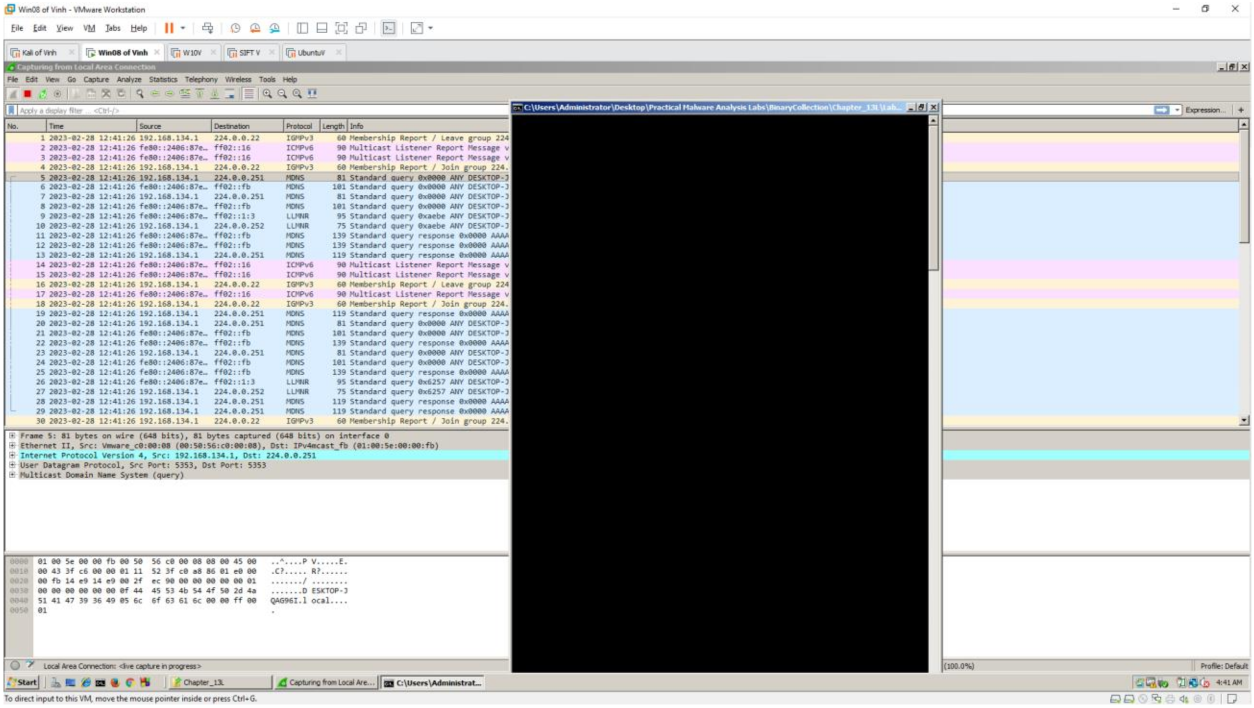
What you need:

- A Windows machine with the tools we have been using installed.

Beacons

- The book recommends running the malware with another VM simulating the Internet with inetsim, but I don't see any good reason to bother with that. I just connected a VM to the real Internet and ran the malware.

Launch the Lab13-01.exe file

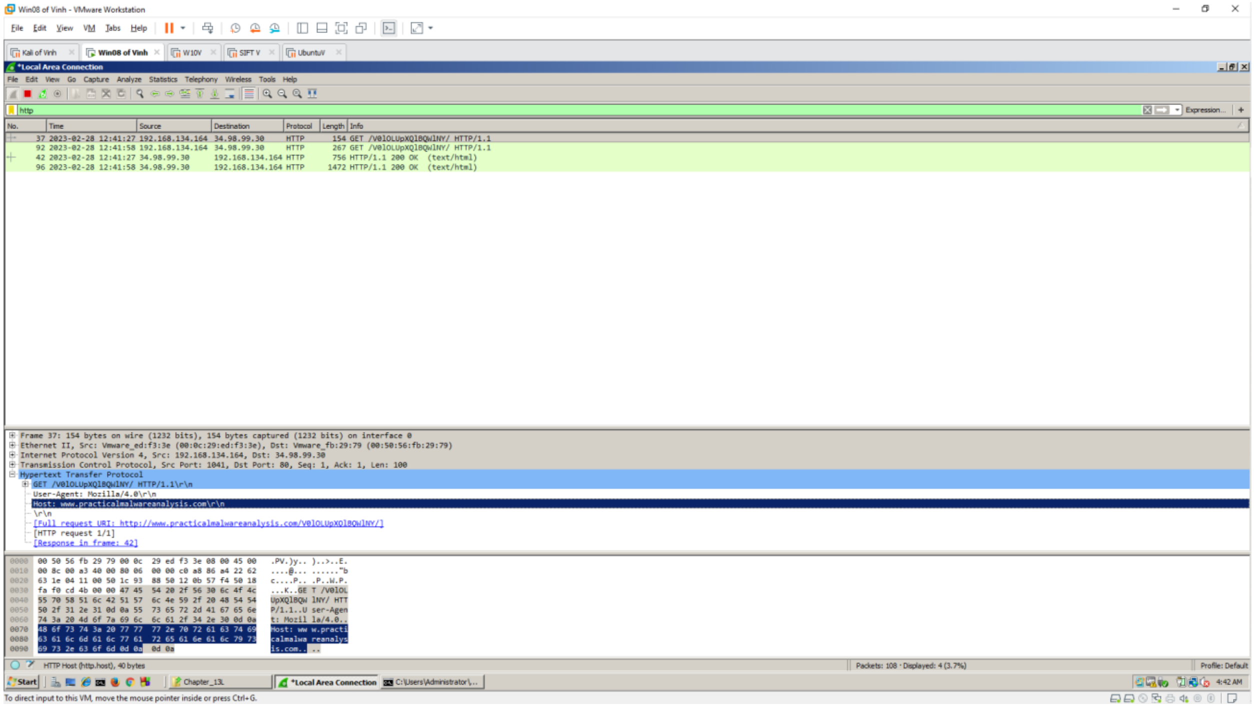

Win08 of Vinh - VMware Workstation
Kali of Vinh
Win08 of Vinh
W10V
SIFT V
UbuntuV
Capturing from Local Area Connection
C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_13L\Lab...
Apply a display filter ... <Ctrl-/>
Local Area Connection: <live capture in progress>
Start
Chapter_13L
Capturing from Local Are...
C:\Users\Administrat...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
No.  Time                Source              Destination   Protocol  Length Info
   1 2023-02-28 12:41:26 192.168.134.1       224.0.0.22    IGMPv3       60 Membership Report / Leave group 224
   2 2023-02-28 12:41:26 fe80::2406:87e…     ff02::16      ICMPv6       90 Multicast Listener Report Message v
   3 2023-02-28 12:41:26 fe80::2406:87e…     ff02::16      ICMPv6       90 Multicast Listener Report Message v
   4 2023-02-28 12:41:26 192.168.134.1       224.0.0.22    IGMPv3       60 Membership Report / Join group 224.
   5 2023-02-28 12:41:26 192.168.134.1       224.0.0.251   MDNS         81 Standard query 0x0000 ANY DESKTOP-J
   6 2023-02-28 12:41:26 fe80::2406:87e…     ff02::fb      MDNS        101 Standard query 0x0000 ANY DESKTOP-J
   7 2023-02-28 12:41:26 192.168.134.1       224.0.0.251   MDNS         81 Standard query 0x0000 ANY DESKTOP-J
   8 2023-02-28 12:41:26 fe80::2406:87e…     ff02::fb      MDNS        101 Standard query 0x0000 ANY DESKTOP-J
   9 2023-02-28 12:41:26 fe80::2406:87e…     ff02::1:3     LLMNR        95 Standard query 0xaebe ANY DESKTOP-J
  10 2023-02-28 12:41:26 192.168.134.1       224.0.0.252   LLMNR        75 Standard query 0xaebe ANY DESKTOP-J
  11 2023-02-28 12:41:26 fe80::2406:87e…     ff02::fb      MDNS        139 Standard query response 0x0000 AAAA
  12 2023-02-28 12:41:26 fe80::2406:87e…     ff02::fb      MDNS        139 Standard query response 0x0000 AAAA
  13 2023-02-28 12:41:26 192.168.134.1       224.0.0.251   MDNS        119 Standard query response 0x0000 AAAA
  14 2023-02-28 12:41:26 fe80::2406:87e…     ff02::16      ICMPv6       90 Multicast Listener Report Message v
  15 2023-02-28 12:41:26 fe80::2406:87e…     ff02::16      ICMPv6       90 Multicast Listener Report Message v
  16 2023-02-28 12:41:26 192.168.134.1       224.0.0.22    IGMPv3       60 Membership Report / Leave group 224
  17 2023-02-28 12:41:26 fe80::2406:87e…     ff02::16      ICMPv6       90 Multicast Listener Report Message v
  18 2023-02-28 12:41:26 192.168.134.1       224.0.0.22    IGMPv3       60 Membership Report / Join group 224.
  19 2023-02-28 12:41:26 192.168.134.1       224.0.0.251   MDNS        119 Standard query response 0x0000 AAAA
  20 2023-02-28 12:41:26 192.168.134.1       224.0.0.251   MDNS         81 Standard query 0x0000 ANY DESKTOP-J
  21 2023-02-28 12:41:26 fe80::2406:87e…     ff02::fb      MDNS        101 Standard query 0x0000 ANY DESKTOP-J
  22 2023-02-28 12:41:26 fe80::2406:87e…     ff02::fb      MDNS        139 Standard query response 0x0000 AAAA
  23 2023-02-28 12:41:26 192.168.134.1       224.0.0.251   MDNS         81 Standard query 0x0000 ANY DESKTOP-J
  24 2023-02-28 12:41:26 fe80::2406:87e…     ff02::fb      MDNS        101 Standard query 0x0000 ANY DESKTOP-J
  25 2023-02-28 12:41:26 fe80::2406:87e…     ff02::fb      MDNS        139 Standard query response 0x0000 AAAA
  26 2023-02-28 12:41:26 fe80::2406:87e…     ff02::1:3     LLMNR        95 Standard query 0x6257 ANY DESKTOP-J
  27 2023-02-28 12:41:26 192.168.134.1       224.0.0.252   LLMNR        75 Standard query 0x6257 ANY DESKTOP-J
  28 2023-02-28 12:41:26 192.168.134.1       224.0.0.251   MDNS        119 Standard query response 0x0000 AAAA
  29 2023-02-28 12:41:26 192.168.134.1       224.0.0.251   MDNS        119 Standard query response 0x0000 AAAA
  30 2023-02-28 12:41:26 192.168.134.1       224.0.0.22    IGMPv3       60 Membership Report / Join group 224.
```

```
⊞ Frame 5: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
⊞ Ethernet II, Src: Vmware_c0:00:08 (00:50:56:c0:00:08), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
⊞ Internet Protocol Version 4, Src: 192.168.134.1, Dst: 224.0.0.251
⊞ User Datagram Protocol, Src Port: 5353, Dst Port: 5353
⊞ Multicast Domain Name System (query)
```

```
0000  01 00 5e 00 00 fb 00 50  56 c0 00 08 08 00 45 00   ..^....P V.....E.
0010  00 43 3f c6 00 00 01 11  52 3f c0 a8 86 01 e0 00   .C?..... R?......
0020  00 fb 14 e9 14 e9 00 2f  ec 90 00 00 00 00 00 01   ......./ ........
0030  00 00 00 00 00 00 0f 44  45 53 4b 54 4f 50 2d 4a   .......D ESKTOP-J
0040  51 41 47 39 36 49 05 6c  6f 63 61 6c 00 00 ff 00   QAG96I.l ocal....
0050  01                                                 .
```

Wireshark

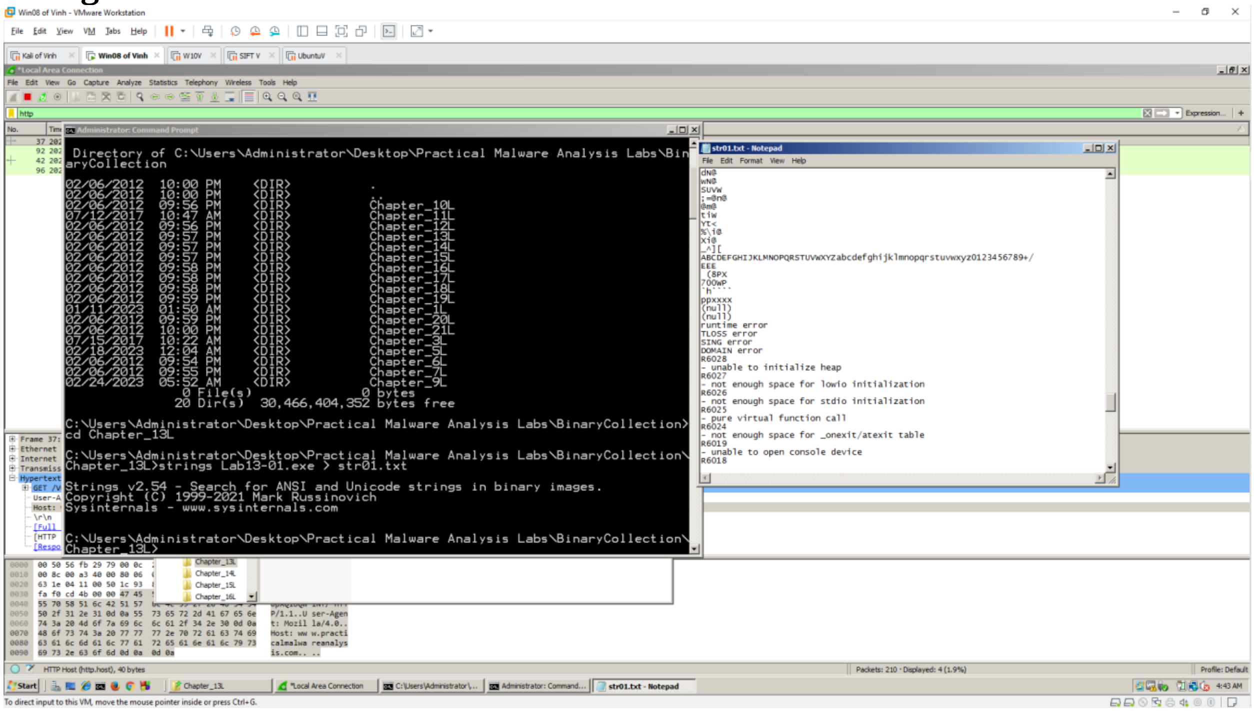

Win08 of Vinh - VMware Workstation
File Edit View VM Tabs Help
Kali of Vinh
Win08 of Vinh
W10V
SIFT V
UbuntuV
*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
HTTP Host (http.host), 40 bytes
Packets: 108 · Displayed: 4 (3.7%)
Profile: Default
Start
Chapter_13L
*Local Area Connection
C:\Users\Administrator\...
4:42 AM
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
No.  Time                Source           Destination      Protocol Length Info
  37 2023-02-28 12:41:27 192.168.134.164 34.98.99.30      HTTP      154 GET /V0lOLUpXQlBQWlNY/ HTTP/1.1
  92 2023-02-28 12:41:58 192.168.134.164 34.98.99.30      HTTP      267 GET /V0lOLUpXQlBQWlNY/ HTTP/1.1
  42 2023-02-28 12:41:27 34.98.99.30     192.168.134.164 HTTP      756 HTTP/1.1 200 OK  (text/html)
  96 2023-02-28 12:41:58 34.98.99.30     192.168.134.164 HTTP     1472 HTTP/1.1 200 OK  (text/html)
```

```
Frame 37: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) on interface 0
Ethernet II, Src: Vmware_ed:f3:3e (00:0c:29:ed:f3:3e), Dst: Vmware_fb:29:79 (00:50:56:fb:29:79)
Internet Protocol Version 4, Src: 192.168.134.164, Dst: 34.98.99.30
Transmission Control Protocol, Src Port: 1041, Dst Port: 80, Seq: 1, Ack: 1, Len: 100
Hypertext Transfer Protocol
  GET /V0lOLUpXQlBQWlNY/ HTTP/1.1\r\n
  User-Agent: Mozilla/4.0\r\n
  Host: www.practicalmalwareanalysis.com\r\n
  \r\n
  [Full request URI: http://www.practicalmalwareanalysis.com/V0lOLUpXQlBQWlNY/]
  [HTTP request 1/1]
  [Response in frame: 42]
```

```
0000  00 50 56 fb 29 79 00 0c  29 ed f3 3e 08 00 45 00   .PV.)y.. )..>..E.
0010  00 8c 00 a3 40 00 80 06  00 00 c0 a8 86 a4 22 62   ....@... ......"b
0020  63 1e 04 11 00 50 1c 93  88 50 12 0b 57 f4 50 18   c....P.. .P..W.P.
0030  fa f0 cd 4b 00 00 47 45  54 20 2f 56 30 6c 4f 4c   ...K..GE T /V0lOL
0040  55 70 58 51 6c 42 51 57  6c 4e 59 2f 20 48 54 54   UpXQlBQW lNY/ 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..
0070  48 6f 73 74 3a 20 77 77  77 2e 70 72 61 63 74 69   Host: ww w.practi
0080  63 61 6c 6d 61 6c 77 61  72 65 61 6e 61 6c 79 73   calmalwa reanalys
0090  69 73 2e 63 6f 6d 0d 0a  0d 0a                     is.com.. ..
```

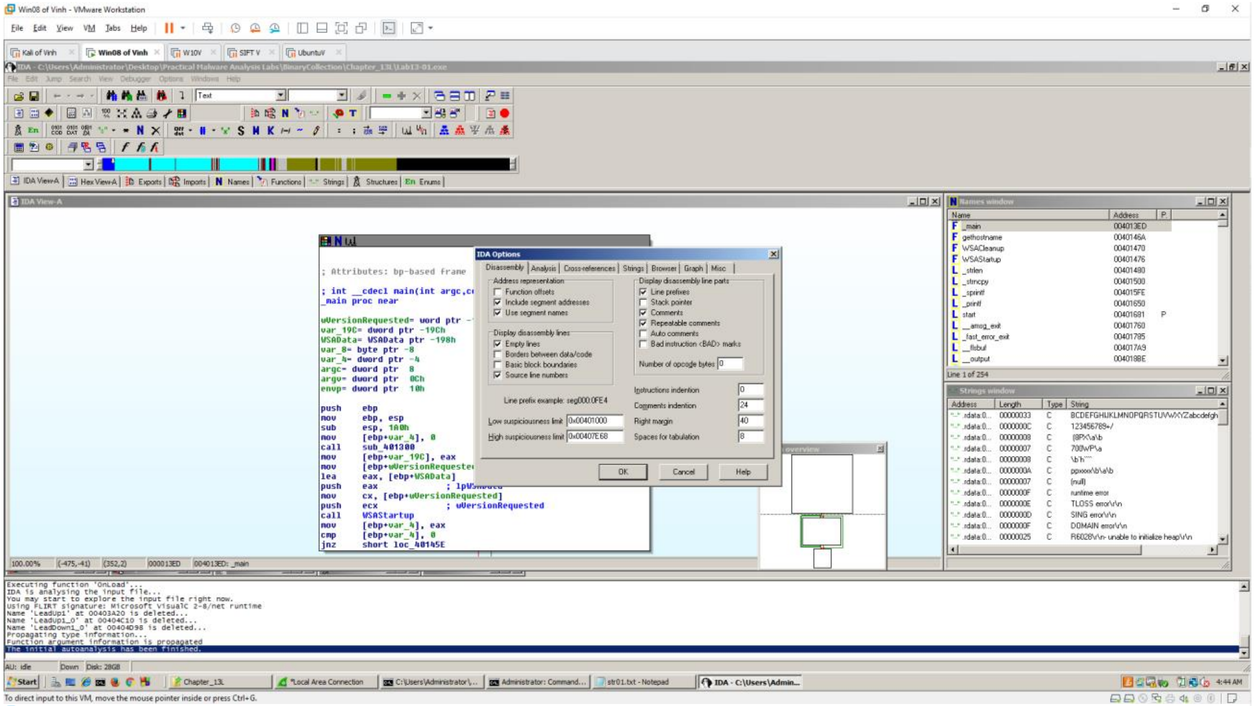
Strings


Win08 of Vinh - VMware Workstation
File Edit View VM Tabs Help
Kali of Vinh
Win08 of Vinh
W10V
SIFT V
UbuntuV
*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
Administrator: Command Prompt
str01.txt - Notepad
File Edit Format View Help
Chapter_13L
Chapter_14L
Chapter_15L
Chapter_16L
HTTP Host (http.host), 40 bytes
Packets: 210 · Displayed: 4 (1.9%)
Profile: Default
Start
Chapter_13L
*Local Area Connection
C:\Users\Administrator\...
Administrator: Command...
str01.txt - Notepad
4:43 AM
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
 Directory of C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection

02/06/2012  10:00 PM    <DIR>          .
02/06/2012  10:00 PM    <DIR>          ..
02/06/2012  09:56 PM    <DIR>          Chapter_10L
07/12/2017  10:47 AM    <DIR>          Chapter_11L
02/06/2012  09:56 PM    <DIR>          Chapter_12L
02/06/2012  09:57 PM    <DIR>          Chapter_13L
02/06/2012  09:57 PM    <DIR>          Chapter_14L
02/06/2012  09:57 PM    <DIR>          Chapter_15L
02/06/2012  09:58 PM    <DIR>          Chapter_16L
02/06/2012  09:58 PM    <DIR>          Chapter_17L
02/06/2012  09:58 PM    <DIR>          Chapter_18L
02/06/2012  09:59 PM    <DIR>          Chapter_19L
01/11/2023  01:50 AM    <DIR>          Chapter_1L
02/06/2012  09:59 PM    <DIR>          Chapter_20L
02/06/2012  10:00 PM    <DIR>          Chapter_21L
07/15/2017  10:22 AM    <DIR>          Chapter_3L
02/18/2023  12:04 AM    <DIR>          Chapter_5L
02/06/2012  09:54 PM    <DIR>          Chapter_6L
02/06/2012  09:55 PM    <DIR>          Chapter_7L
02/24/2023  05:52 AM    <DIR>          Chapter_9L
               0 File(s)              0 bytes
              20 Dir(s)  30,466,404,352 bytes free

C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection>
cd Chapter_13L

C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\
Chapter_13L>strings Lab13-01.exe > str01.txt

Strings v2.54 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2021 Mark Russinovich
Sysinternals - www.sysinternals.com


C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\
Chapter_13L>
```

```
dN@
wN@
SUVW
;=@n@
@m@
tiW
Yt<
%\i@
Xi@
_^][
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
EEE
 (8PX
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
R6024
- not enough space for _onexit/atexit table
R6019
- unable to open console device
R6018
```

IDA Pro



Win08 of Vinh - VMware Workstation

IDA - C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_13L\Lab13-01.exe

```
; Attributes: bp-based frame

; int __cdecl main(int argc,c
_main proc near

wVersionRequested= word ptr -
var_19C= dword ptr -19Ch
WSAData= WSAData ptr -198h
var_8= byte ptr -8
var_4= dword ptr -4
argc= dword ptr  8
argv= dword ptr  0Ch
envp= dword ptr  10h

push    ebp
mov     ebp, esp
sub     esp, 1A0h
mov     [ebp+var_4], 0
call    sub_401300
mov     [ebp+var_19C], eax
mov     [ebp+wVersionRequeste
lea     eax, [ebp+WSAData]
push    eax             ; lpWSAData
mov     cx, [ebp+wVersionRequested]
push    ecx             ; wVersionRequested
call    WSAStartup
mov     [ebp+var_4], eax
cmp     [ebp+var_4], 0
jnz     short loc_40145E
```

IDA Options

Disassembly | Analysis | Cross-references | Strings | Browser | Graph | Misc

Address representation
- □ Function offsets
- ☑ Include segment addresses
- ☑ Use segment names

Display disassembly lines
- ☑ Empty lines
- □ Borders between data/code
- □ Basic block boundaries
- ☑ Source line numbers

Line prefix example: seg000:0FE4

Low suspiciousness limit: 0x00401000
High suspiciousness limit: 0x00407E68

Display disassembly line parts
- ☑ Line prefixes
- □ Stack pointer
- ☑ Comments
- ☑ Repeatable comments
- □ Auto comments
- □ Bad instruction <BAD> marks

Number of opcode bytes: 0

Instructions indention: 0
Comments indention: 24
Right margin: 40
Spaces for tabulation: 8

Names window

Name	Address	P
F _main	004013ED	
F gethostname	0040146A	
F WSACleanup	00401470	
F WSAStartup	00401476	
L _strlen	00401480	
L _strncpy	00401500	
L _sprintf	004015FE	
L _printf	00401650	
L start	00401681	P
L __amsg_exit	00401760	
L _fast_error_exit	00401785	
L __flsbuf	004017A9	
L __output	0040188E	

Line 1 of 254

Strings window

Address	Length	Type	String
.rdata:0...	00000033	C	BCDEFGHIJKLMNOPQRSTUVWXYZabcdefgh
.rdata:0...	0000000C	C	123456789+/
.rdata:0...	00000008	C	(8PX\a\b
.rdata:0...	00000007	C	700WP\a
.rdata:0...	00000008	C	\b`h````
.rdata:0...	0000000A	C	ppxxxx\b\a\b
.rdata:0...	00000007	C	(null)
.rdata:0...	0000000F	C	runtime error
.rdata:0...	0000000E	C	TLOSS error\r\n
.rdata:0...	0000000D	C	SING error\r\n
.rdata:0...	0000000F	C	DOMAIN error\r\n
.rdata:0...	00000025	C	R6028\r\n- unable to initialize heap\r\n

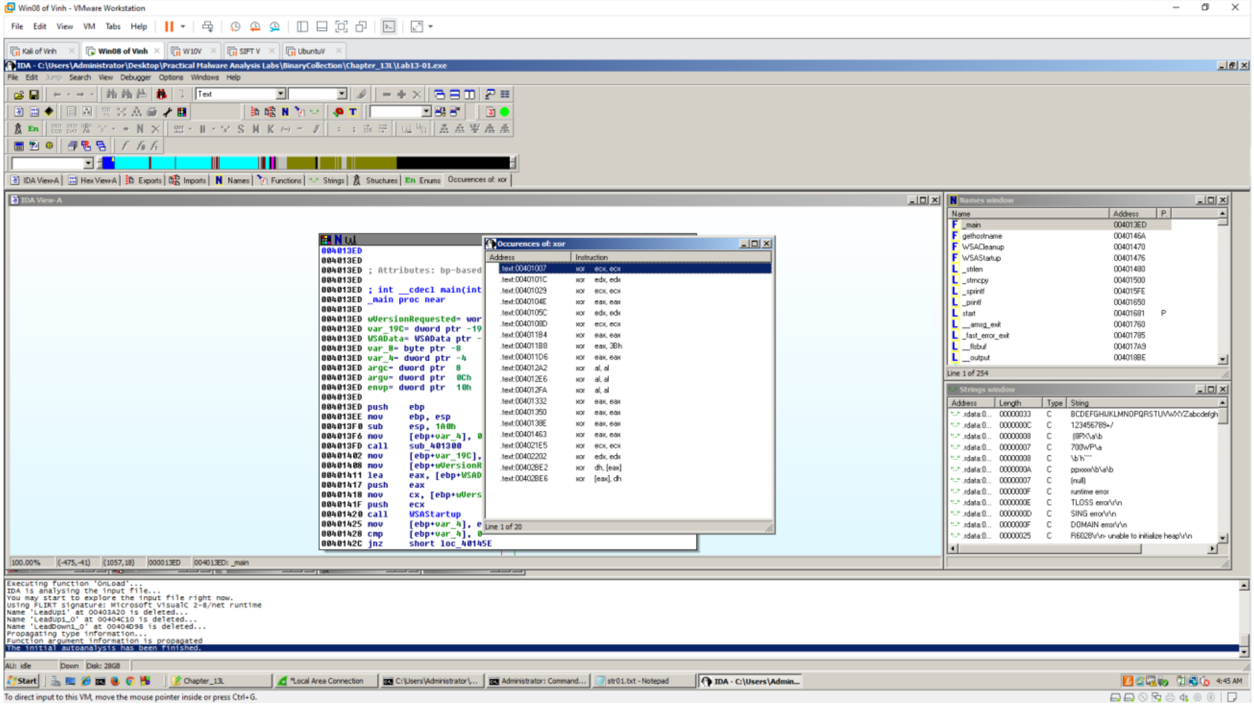
100.00% (-475,-41) (352,2) 000013ED 004013ED: _main

```
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: Microsoft VisualC 2-8/net runtime
Name 'LeadUp1' at 00403A20 is deleted...
Name 'LeadUp1_0' at 00404C10 is deleted...
Name 'LeadDown1_0' at 00404D98 is deleted...
Propagating type information...
Function argument information is propagated
The initial autoanalysis has been finished.
```

AU: idle Down Disk: 28GB

4:44 AM

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



Win08 of Vinh - VMware Workstation

IDA - C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_13L\Lab13-01.exe

```
004013ED
004013ED
004013ED ; Attributes: bp-based
004013ED
004013ED ; int __cdecl main(int
004013ED _main proc near
004013ED
004013ED wVersionRequested= wor
004013ED var_19C= dword ptr -19
004013ED WSAData= WSAData ptr -
004013ED var_8= byte ptr -8
004013ED var_4= dword ptr -4
004013ED argc= dword ptr  8
004013ED argv= dword ptr  0Ch
004013ED envp= dword ptr  10h
004013ED
004013ED push    ebp
004013EE mov     ebp, esp
004013F0 sub     esp, 1A0h
004013F6 mov     [ebp+var_4], 0
004013FD call    sub_401300
00401402 mov     [ebp+var_19C],
00401408 mov     [ebp+wVersionR
00401411 lea     eax, [ebp+WSAD
00401417 push    eax
00401418 mov     cx, [ebp+wVers
0040141F push    ecx
00401420 call    WSAStartup
00401425 mov     [ebp+var_4], e
00401428 cmp     [ebp+var_4], 0
0040142C jnz     short loc_40145E
```

Occurences of: xor

Address	Instruction
.text:00401007	xor ecx, ecx
.text:0040101C	xor edx, edx
.text:00401029	xor ecx, ecx
.text:0040104E	xor eax, eax
.text:0040105C	xor edx, edx
.text:0040108D	xor ecx, ecx
.text:004011B4	xor eax, eax
.text:004011B8	xor eax, 3Bh
.text:004011D6	xor eax, eax
.text:004012A2	xor al, al
.text:004012E6	xor al, al
.text:004012FA	xor al, al
.text:00401332	xor eax, eax
.text:00401350	xor eax, eax
.text:0040138E	xor eax, eax
.text:00401463	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

Names window

Name	Address	P
F _main	004013ED	
F gethostname	0040146A	
F WSACleanup	00401470	
F WSAStartup	00401476	
L _strlen	00401480	
L _strncpy	00401500	
L _sprintf	004015FE	
L _printf	00401650	
L start	00401681	P
L __amsg_exit	00401760	
L _fast_error_exit	00401785	
L __flsbuf	004017A9	
L __output	0040188E	

Line 1 of 254

Strings window

Address	Length	Type	String
.rdata:0...	00000033	C	BCDEFGHIJKLMNOPQRSTUVWXYZabcdefgh
.rdata:0...	0000000C	C	123456789+/
.rdata:0...	00000008	C	(8PX\a\b
.rdata:0...	00000007	C	700WP\a
.rdata:0...	00000008	C	\b`h````
.rdata:0...	0000000A	C	ppxxxx\b\a\b
.rdata:0...	00000007	C	(null)
.rdata:0...	0000000F	C	runtime error
.rdata:0...	0000000E	C	TLOSS error\r\n
.rdata:0...	0000000D	C	SING error\r\n
.rdata:0...	0000000F	C	DOMAIN error\r\n
.rdata:0...	00000025	C	R6028\r\n- unable to initialize heap\r\n

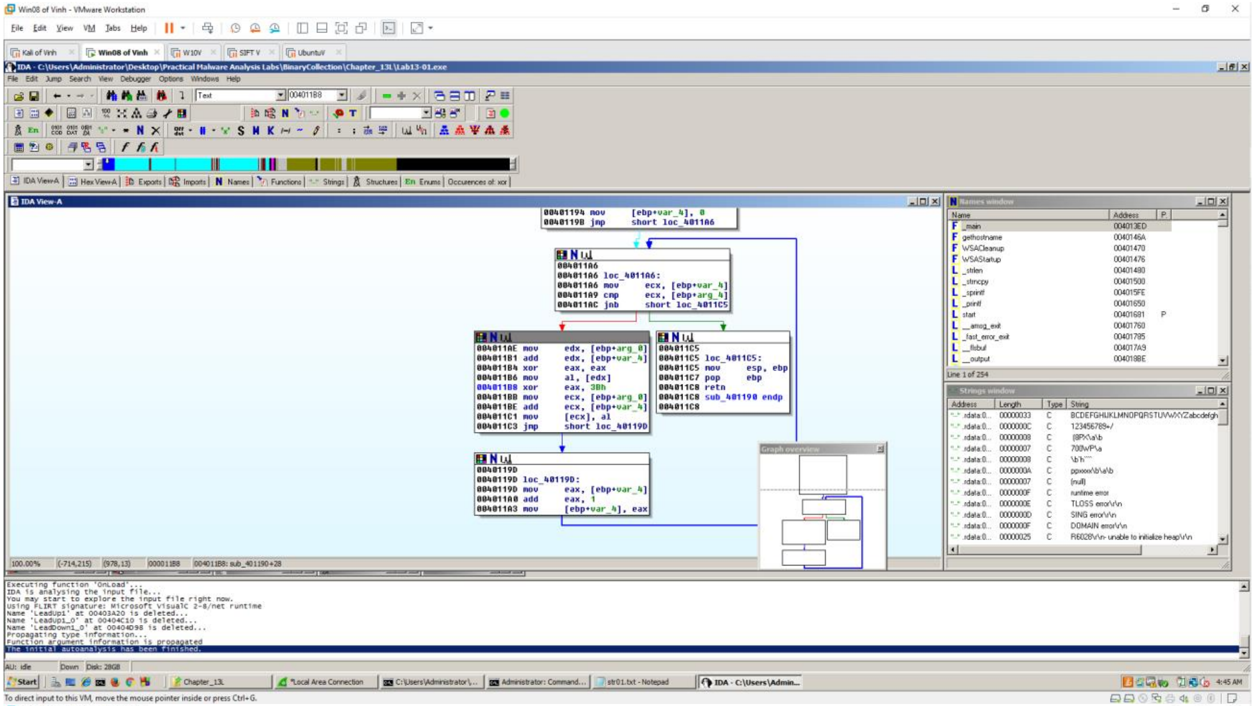
100.00% (-475,-41) (1057,18) 000013ED 004013ED: _main

```
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: Microsoft VisualC 2-8/net runtime
Name 'LeadUp1' at 00403A20 is deleted...
Name 'LeadUp1_0' at 00404C10 is deleted...
Name 'LeadDown1_0' at 00404D98 is deleted...
Propagating type information...
Function argument information is propagated
The initial autoanalysis has been finished.
```

AU: idle Down Disk: 28GB

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

4:45 AM



Win08 of Vinh - VMware Workstation

IDA - C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_13L\Lab13-01.exe

```
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
```

100.00% (-714,215) (978,13) 000011B8 004011B8: sub_401190+28

Names window

	Name	Address	P
F	_main	004013ED	
F	gethostname	0040146A	
F	WSACleanup	00401470	
F	WSAStartup	00401476	
L	_strlen	00401480	
L	_strncpy	00401500	
L	_sprintf	004015FE	
L	_printf	00401650	
L	start	00401681	P
L	__amsg_exit	00401760	
L	_fast_error_exit	00401785	
L	__flsbuf	004017A9	
L	__output	0040188E	

Line 1 of 254

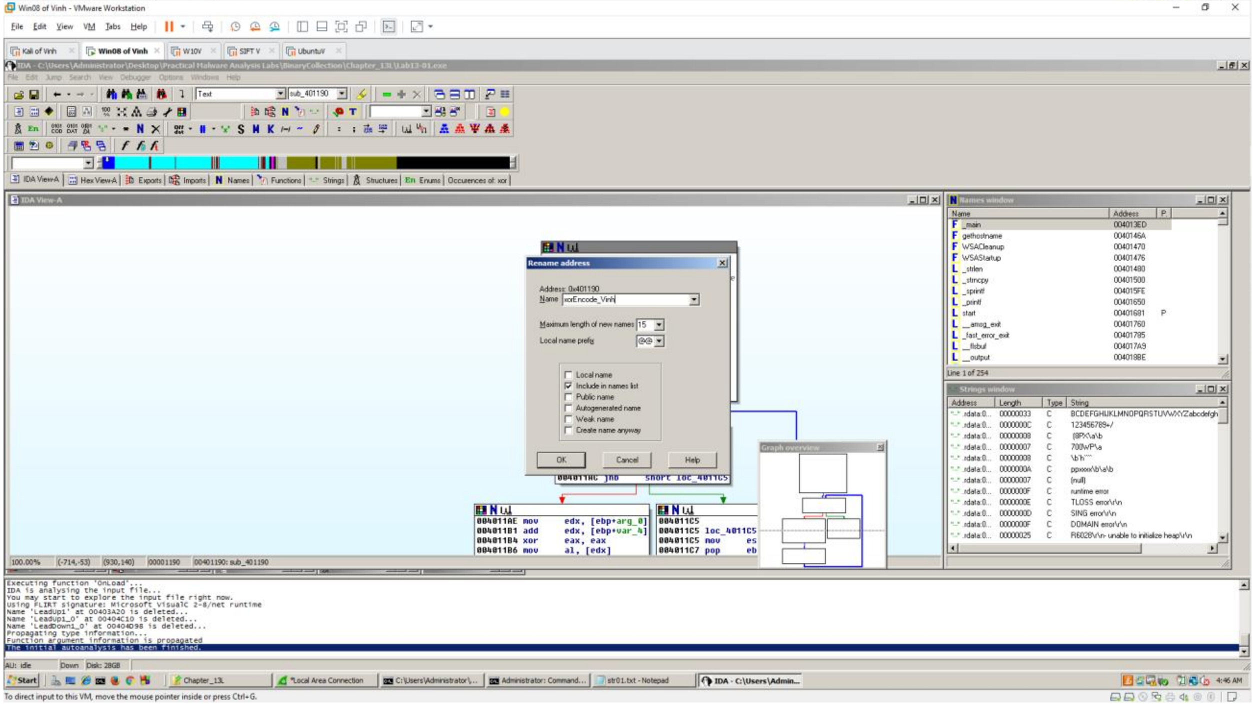
Strings window

Address	Length	Type	String
.rdata:0...	00000033	C	BCDEFGHIJKLMNOPQRSTUVWXYZabcdefgh
.rdata:0...	0000000C	C	123456789+/
.rdata:0...	00000008	C	(8PX\a\b
.rdata:0...	00000007	C	700WP\a
.rdata:0...	00000008	C	\b`h````
.rdata:0...	0000000A	C	ppxxxx\b\a\b
.rdata:0...	00000007	C	(null)
.rdata:0...	0000000F	C	runtime error
.rdata:0...	0000000E	C	TLOSS error\r\n
.rdata:0...	0000000D	C	SING error\r\n
.rdata:0...	0000000F	C	DOMAIN error\r\n
.rdata:0...	00000025	C	R6028\r\n- unable to initialize heap\r\n

```
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: Microsoft VisualC 2-8/net runtime
Name 'LeadUp1' at 00403A20 is deleted...
Name 'LeadUp1_0' at 00404C10 is deleted...
Name 'LeadDown1_0' at 00404D98 is deleted...
Propagating type information...
Function argument information is propagated
The initial autoanalysis has been finished.
```

AU: idle Down Disk: 28GB

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



Win08 of Vinh - VMware Workstation

IDA - C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_13L\Lab13-01.exe

Rename address

Address: 0x401190
Name xorEncode_Vinh

Maximum length of new names 15
Local name prefix @@

☐ Local name
☑ Include in names list
☐ Public name
☐ Autogenerated name
☐ Weak name
☐ Create name anyway

```
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]

004011C5
004011C5 loc_4011C5
004011C5 mov     es
004011C7 pop     eb
```

100.00% (-714,-53) (930,140) 00001190 00401190: sub_401190

Names window

	Name	Address	P
F	_main	004013ED	
F	gethostname	0040146A	
F	WSACleanup	00401470	
F	WSAStartup	00401476	
L	_strlen	00401480	
L	_strncpy	00401500	
L	_sprintf	004015FE	
L	_printf	00401650	
L	start	00401681	P
L	__amsg_exit	00401760	
L	_fast_error_exit	00401785	
L	__flsbuf	004017A9	
L	__output	0040188E	

Line 1 of 254

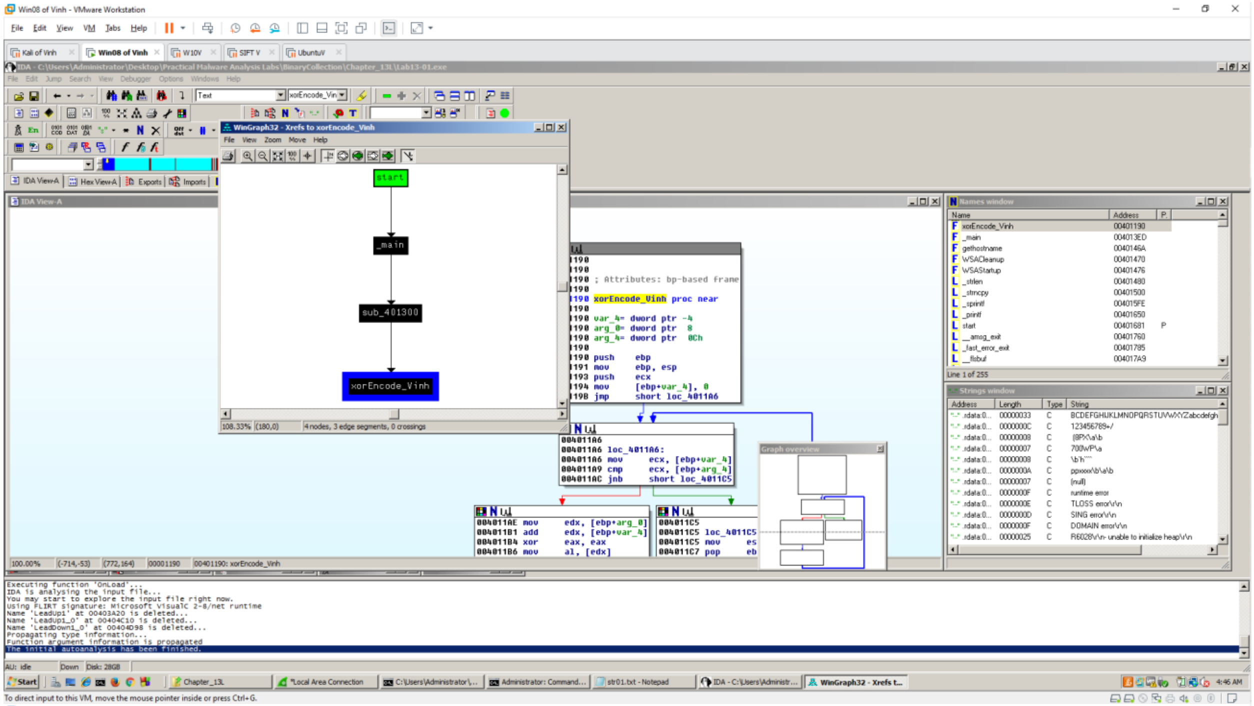
Strings window

Address	Length	Type	String
.rdata:0...	00000033	C	BCDEFGHIJKLMNOPQRSTUVWXYZabcdefgh
.rdata:0...	0000000C	C	123456789+/
.rdata:0...	00000008	C	(8PX\a\b
.rdata:0...	00000007	C	700WP\a
.rdata:0...	00000008	C	\b`h````
.rdata:0...	0000000A	C	ppxxxx\b\a\b
.rdata:0...	00000007	C	(null)
.rdata:0...	0000000F	C	runtime error
.rdata:0...	0000000E	C	TLOSS error\r\n
.rdata:0...	0000000D	C	SING error\r\n
.rdata:0...	0000000F	C	DOMAIN error\r\n
.rdata:0...	00000025	C	R6028\r\n- unable to initialize heap\r\n

```
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: Microsoft VisualC 2-8/net runtime
Name 'LeadUp1' at 00403A20 is deleted...
Name 'LeadUp1_0' at 00404C10 is deleted...
Name 'LeadDown1_0' at 00404D98 is deleted...
Propagating type information...
Function argument information is propagated
The initial autoanalysis has been finished.
```

AU: idle Down Disk: 28GB

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Win08 of Vinh - VMware Workstation
File Edit View VM Tabs Help
Kali of Vinh
Win08 of Vinh
W10V
SIFT V
UbuntuV
IDA - C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_13L\Lab13-01.exe
File Edit Jump Search View Debugger Options Windows Help
Text
xorEncode_Vin
IDA View-A
Hex View-A
Exports
Imports
WinGraph32 - Xrefs to xorEncode_Vinh
File View Zoom Move Help
start
_main
sub_401300
xorEncode_Vinh
108.33%
(180,0)
4 nodes, 3 edge segments, 0 crossings
Names window
Strings window
Graph overview
100.00%
(-714,-53)
(772,164)
00001190
00401190: xorEncode_Vinh
AU: idle
Down
Disk: 28GB
Start
Chapter_13L
*Local Area Connection
C:\Users\Administrator\...
Administrator: Command...
str01.txt - Notepad
IDA - C:\Users\Administr...
WinGraph32 - Xrefs t...
4:46 AM
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
)190
)190
)190 ; Attributes: bp-based frame
)190
)190 xorEncode_Vinh proc near
)190
)190 var_4= dword ptr -4
)190 arg_0= dword ptr  8
)190 arg_4= dword ptr  0Ch
)190
)190 push    ebp
)191 mov     ebp, esp
)193 push    ecx
)194 mov     [ebp+var_4], 0
)19B 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]
```

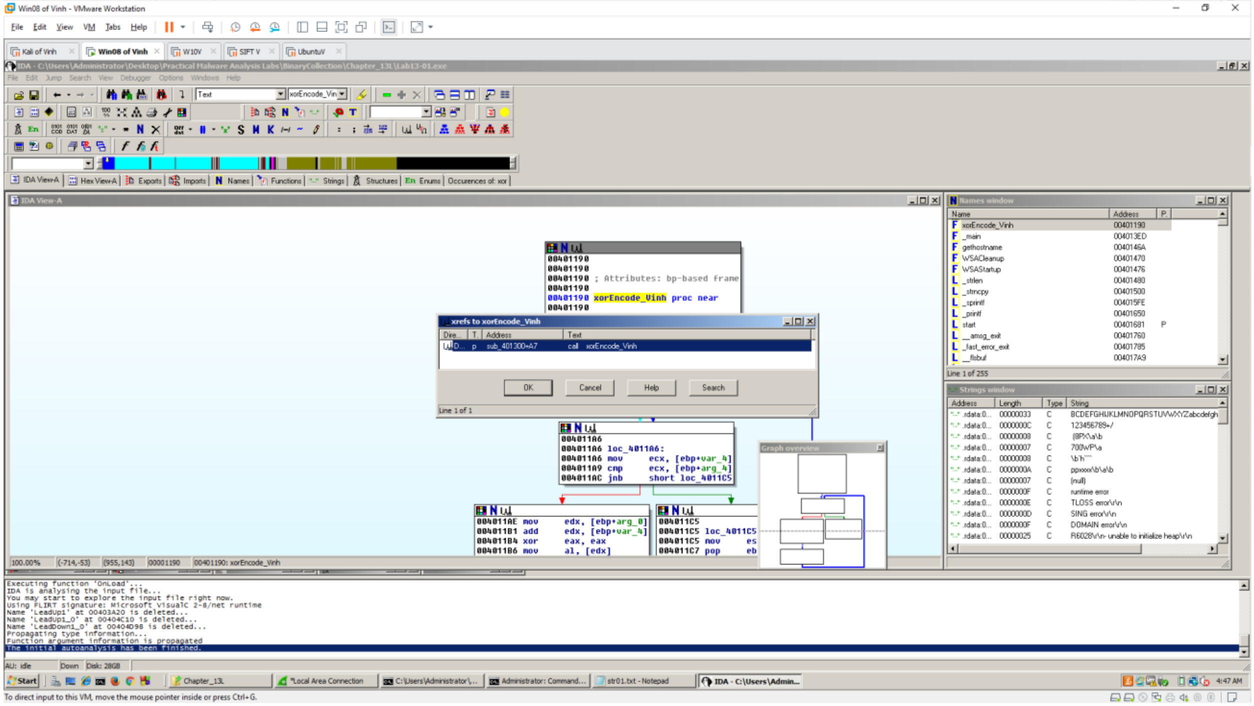
```
004011C5
004011C5 loc_4011C5
004011C5 mov     es
004011C7 pop     eb
```

Name	Address	P.
xorEncode_Vinh	00401190	
_main	004013ED	
gethostname	0040146A	
WSACleanup	00401470	
WSAStartup	00401476	
_strlen	00401480	
_strncpy	00401500	
_sprintf	004015FE	
_printf	00401650	
start	00401681	P
__amsg_exit	00401760	
_fast_error_exit	00401785	
__flsbuf	004017A9	

Line 1 of 255

Address	Length	Type	String
.rdata:0...	00000033	C	BCDEFGHIJKLMNOPQRSTUVWXYZabcdefgh
.rdata:0...	0000000C	C	123456789+/
.rdata:0...	00000008	C	(8PX\a\b
.rdata:0...	00000007	C	700WP\a
.rdata:0...	00000008	C	\b'h````
.rdata:0...	0000000A	C	ppxxxx\b\a\b
.rdata:0...	00000007	C	(null)
.rdata:0...	0000000F	C	runtime error
.rdata:0...	0000000E	C	TLOSS error\r\n
.rdata:0...	0000000D	C	SING error\r\n
.rdata:0...	0000000F	C	DOMAIN error\r\n
.rdata:0...	00000025	C	R6028\r\n- unable to initialize heap\r\n

```
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: Microsoft VisualC 2-8/net runtime
Name 'LeadUp1' at 00403A20 is deleted...
Name 'LeadUp1_0' at 00404C10 is deleted...
Name 'LeadDown1_0' at 00404D98 is deleted...
Propagating type information...
Function argument information is propagated
The initial autoanalysis has been finished.
```



```
00401190
00401190
00401190 ; Attributes: bp-based frame
00401190
00401190 xorEncode_Vinh proc near
00401190
```

xrefs to xorEncode_Vinh

Dire...	T.	Address	Text
D...	p	sub_401300+A7	call xorEncode_Vinh

Line 1 of 1

```
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]
```

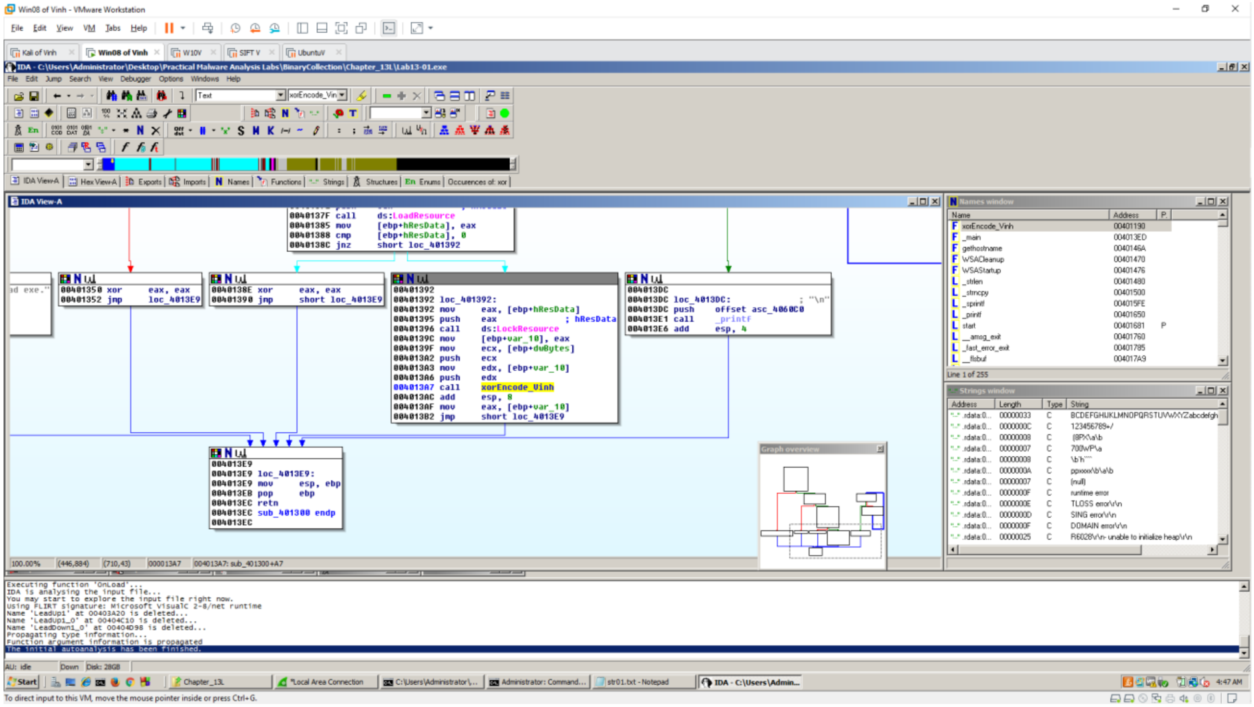
```
004011C5
004011C5 loc_4011C5
004011C5 mov     es
004011C7 pop     eb
```

Name	Address	P.
xorEncode_Vinh	00401190	
_main	004013ED	
gethostname	0040146A	
WSACleanup	00401470	
WSAStartup	00401476	
_strlen	00401480	
_strncpy	00401500	
_sprintf	004015FE	
_printf	00401650	
start	00401681	P
__amsg_exit	00401760	
_fast_error_exit	00401785	
__flsbuf	004017A9	

Line 1 of 255

Address	Length	Type	String
.rdata:0...	00000033	C	BCDEFGHIJKLMNOPQRSTUVWXYZabcdefgh
.rdata:0...	0000000C	C	123456789+/
.rdata:0...	00000008	C	(8PX\a\b
.rdata:0...	00000007	C	700WP\a
.rdata:0...	00000008	C	\b'h````
.rdata:0...	0000000A	C	ppxxxx\b\a\b
.rdata:0...	00000007	C	(null)
.rdata:0...	0000000F	C	runtime error
.rdata:0...	0000000E	C	TLOSS error\r\n
.rdata:0...	0000000D	C	SING error\r\n
.rdata:0...	0000000F	C	DOMAIN error\r\n
.rdata:0...	00000025	C	R6028\r\n- unable to initialize heap\r\n

```
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: Microsoft VisualC 2-8/net runtime
Name 'LeadUp1' at 00403A20 is deleted...
Name 'LeadUp1_0' at 00404C10 is deleted...
Name 'LeadDown1_0' at 00404D98 is deleted...
Propagating type information...
Function argument information is propagated
The initial autoanalysis has been finished.
```


Win08 of Vinh - VMware Workstation
File Edit View VM Tabs Help
Kali of Vinh
Win08 of Vinh
W10V
SIFT V
UbuntuV
IDA - C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_13L\Lab13-01.exe
File Edit Jump Search View Debugger Options Windows Help
Text
xorEncode_Vin
IDA View-A
Hex View-A
Exports
Imports
Names
Functions
Strings
Structures
Enums
Occurences of: xor
IDA View-A
Graph overview
Start
Chapter_13L
*Local Area Connection
C:\Users\Administrator\...
Administrator: Command...
str01.txt - Notepad
IDA - C:\Users\Admin...
4:47 AM
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
0040137F call    ds:LoadResource
00401385 mov     [ebp+hResData], eax
00401388 cmp     [ebp+hResData], 0
0040138C jnz     short loc_401392
```

```
ad exe."
```

```
00401350 xor     eax, eax
00401352 jmp     loc_4013E9
```

```
0040138E xor     eax, eax
00401390 jmp     short loc_4013E9
```

```
00401392
00401392 loc_401392:
00401392 mov     eax, [ebp+hResData]
00401395 push    eax             ; hResData
00401396 call    ds:LockResource
0040139C mov     [ebp+var_10], eax
0040139F mov     ecx, [ebp+dwBytes]
004013A2 push    ecx
004013A3 mov     edx, [ebp+var_10]
004013A6 push    edx
004013A7 call    xorEncode_Vinh
004013AC add     esp, 8
004013AF mov     eax, [ebp+var_10]
004013B2 jmp     short loc_4013E9
```

```
004013DC
004013DC loc_4013DC:                  ; "\n"
004013DC push    offset asc_4060C0
004013E1 call    _printf
004013E6 add     esp, 4
```

```
004013E9
004013E9 loc_4013E9:
004013E9 mov     esp, ebp
004013EB pop     ebp
004013EC retn
004013EC sub_401300 endp
004013EC
```

100.00% (446,884) (710,43) 000013A7 004013A7: sub_401300+A7

Names window

Name	Address	P.
F xorEncode_Vinh	00401190	
F _main	004013ED	
F gethostname	0040146A	
F WSACleanup	00401470	
F WSAStartup	00401476	
L _strlen	00401480	
L _strncpy	00401500	
L _sprintf	004015FE	
L _printf	00401650	
L start	00401681	P
L __amsg_exit	00401760	
L _fast_error_exit	00401785	
L __flsbuf	004017A9	

Line 1 of 255

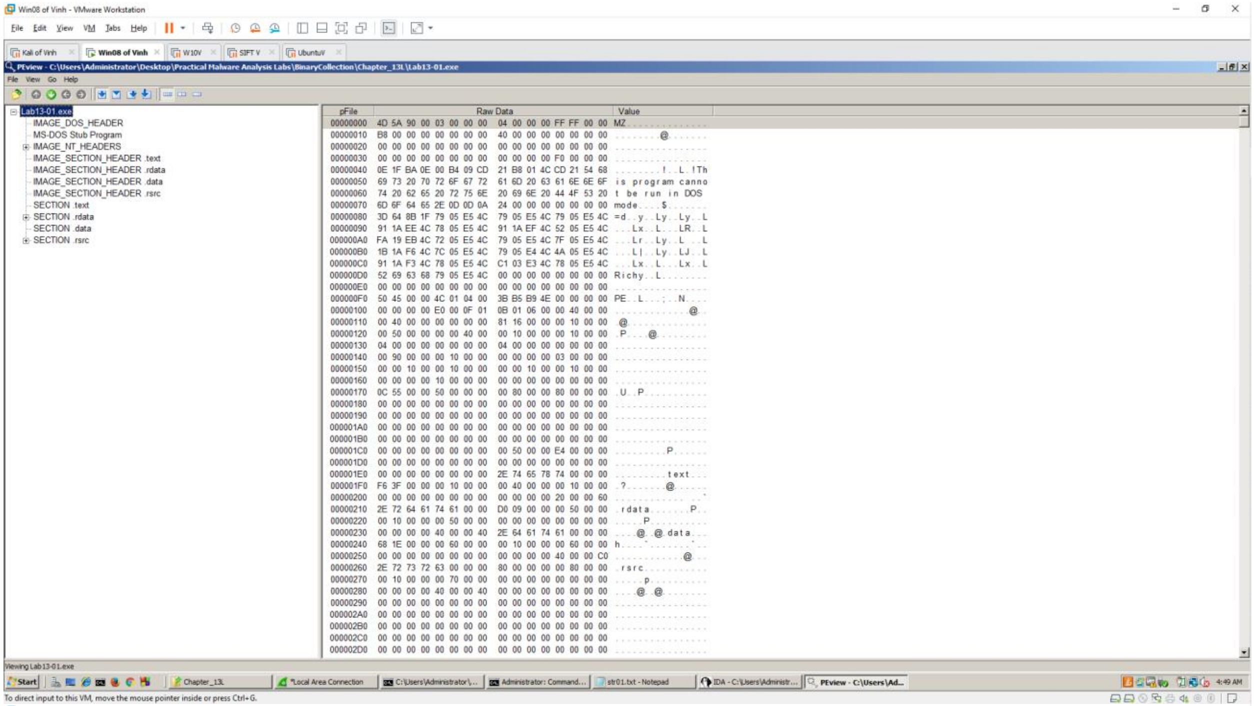
Strings window

Address	Length	Type	String
.rdata:0...	00000033	C	BCDEFGHIJKLMNOPQRSTUVWXYZabcdefgh
.rdata:0...	0000000C	C	123456789+/
.rdata:0...	00000008	C	(8PX\a\b
.rdata:0...	00000007	C	700WP\a
.rdata:0...	00000008	C	\b`h````
.rdata:0...	0000000A	C	ppxxxx\b\a\b
.rdata:0...	00000007	C	(null)
.rdata:0...	0000000F	C	runtime error
.rdata:0...	0000000E	C	TLOSS error\r\n
.rdata:0...	0000000D	C	SING error\r\n
.rdata:0...	0000000F	C	DOMAIN error\r\n
.rdata:0...	00000025	C	R6028\r\n- unable to initialize heap\r\n

```
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: Microsoft VisualC 2-8/net runtime
Name 'LeadUp1' at 00403A20 is deleted...
Name 'LeadUp1_0' at 00404C10 is deleted...
Name 'LeadDown1_0' at 00404D98 is deleted...
Propagating type information...
Function argument information is propagated
The initial autoanalysis has been finished.
```

AU: idle Down Disk: 28GB

PEview

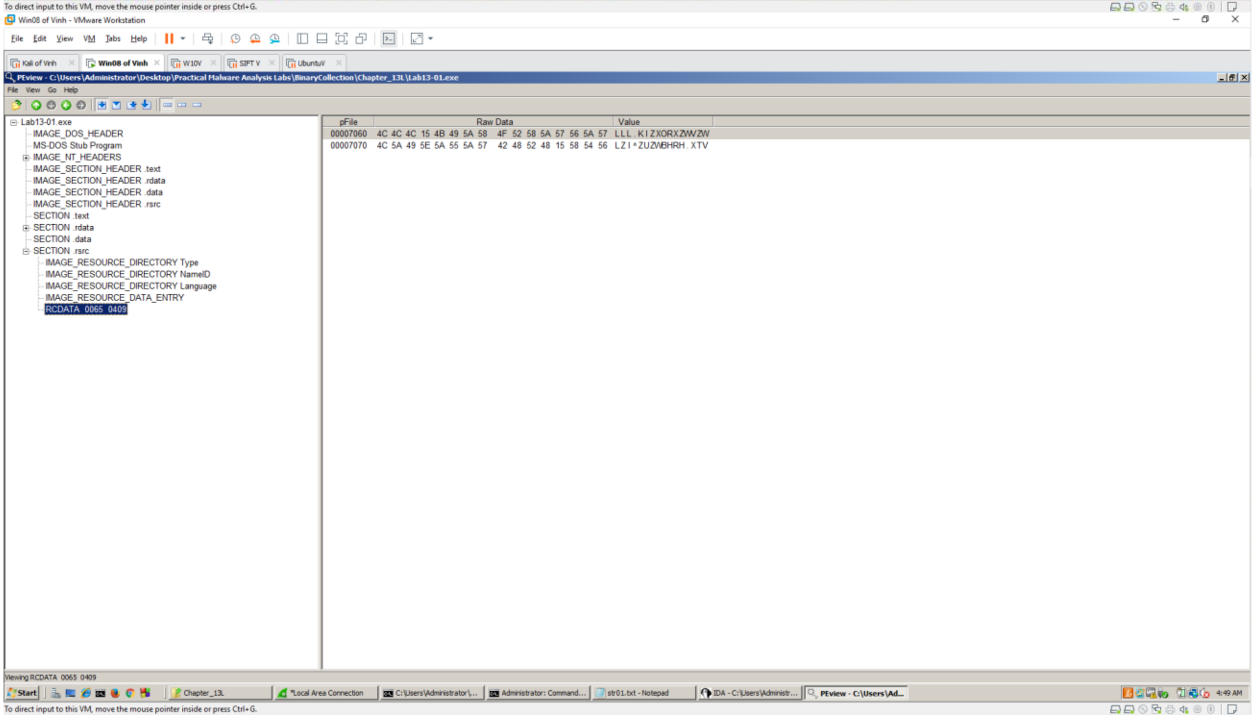


PEview - C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_13L\Lab13-01.exe

```
Lab13-01.exe
  IMAGE_DOS_HEADER
  MS-DOS Stub Program
  IMAGE_NT_HEADERS
  IMAGE_SECTION_HEADER .text
  IMAGE_SECTION_HEADER .rdata
  IMAGE_SECTION_HEADER .data
  IMAGE_SECTION_HEADER .rsrc
  SECTION .text
  SECTION .rdata
  SECTION .data
  SECTION .rsrc
```

```
pFile     Raw Data                                          Value
00000000  4D 5A 90 00 03 00 00 00  04 00 00 00 FF FF 00 00  MZ..............
00000010  B8 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00  ........@.......
00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000030  00 00 00 00 00 00 00 00  00 00 00 00 F0 00 00 00  ................
00000040  0E 1F BA 0E 00 B4 09 CD  21 B8 01 4C CD 21 54 68  ........!..L.!Th
00000050  69 73 20 70 72 6F 67 72  61 6D 20 63 61 6E 6E 6F  is program canno
00000060  74 20 62 65 20 72 75 6E  20 69 6E 20 44 4F 53 20  t be run in DOS 
00000070  6D 6F 64 65 2E 0D 0D 0A  24 00 00 00 00 00 00 00  mode....$.......
00000080  3D 64 8B 1F 79 05 E5 4C  79 05 E5 4C 79 05 E5 4C  =d..y..Ly..Ly..L
00000090  91 1A EE 4C 78 05 E5 4C  91 1A EF 4C 52 05 E5 4C  ...Lx..L...LR..L
000000A0  FA 19 EB 4C 72 05 E5 4C  79 05 E5 4C 7F 05 E5 4C  ...Lr..Ly..L...L
000000B0  1B 1A F6 4C 7C 05 E5 4C  79 05 E4 4C 4A 05 E5 4C  ...L|..Ly..LJ..L
000000C0  91 1A F3 4C 78 05 E5 4C  C1 03 E3 4C 78 05 E5 4C  ...Lx..L...Lx..L
000000D0  52 69 63 68 79 05 E5 4C  00 00 00 00 00 00 00 00  Richy..L........
000000E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000000F0  50 45 00 00 4C 01 04 00  3B B5 B9 4E 00 00 00 00  PE..L...;..N....
00000100  00 00 00 00 E0 00 0F 01  0B 01 06 00 00 40 00 00  .............@..
00000110  00 40 00 00 00 00 00 00  81 16 00 00 00 10 00 00  .@..............
00000120  00 50 00 00 00 00 40 00  00 10 00 00 00 10 00 00  .P....@.........
00000130  04 00 00 00 00 00 00 00  04 00 00 00 00 00 00 00  ................
00000140  00 90 00 00 00 10 00 00  00 00 00 00 03 00 00 00  ................
00000150  00 00 10 00 00 10 00 00  00 00 10 00 00 10 00 00  ................
00000160  00 00 00 00 10 00 00 00  00 00 00 00 00 00 00 00  ................
00000170  0C 55 00 00 50 00 00 00  00 80 00 00 80 00 00 00  .U..P...........
00000180  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000190  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000001A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000001B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000001C0  00 00 00 00 00 00 00 00  00 50 00 00 E4 00 00 00  .........P......
000001D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000001E0  00 00 00 00 00 00 00 00  2E 74 65 78 74 00 00 00  .........text...
000001F0  F6 3F 00 00 00 10 00 00  00 40 00 00 00 10 00 00  .?.......@......
00000200  00 00 00 00 00 00 00 00  00 00 00 00 20 00 00 60  ............ ..`
00000210  2E 72 64 61 74 61 00 00  D0 09 00 00 00 50 00 00  .rdata.......P..
00000220  00 10 00 00 00 50 00 00  00 00 00 00 00 00 00 00  .....P..........
00000230  00 00 00 00 40 00 00 40  2E 64 61 74 61 00 00 00  ....@..@.data...
00000240  68 1E 00 00 00 60 00 00  00 10 00 00 00 60 00 00  h....`.......`..
00000250  00 00 00 00 00 00 00 00  00 00 00 00 40 00 00 C0  ............@...
00000260  2E 72 73 72 63 00 00 00  80 00 00 00 00 80 00 00  .rsrc...........
00000270  00 10 00 00 00 70 00 00  00 00 00 00 00 00 00 00  .....p..........
00000280  00 00 00 00 40 00 00 40  00 00 00 00 00 00 00 00  ....@..@........
00000290  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000002A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000002B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000002C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000002D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
```

Viewing Lab13-01.exe



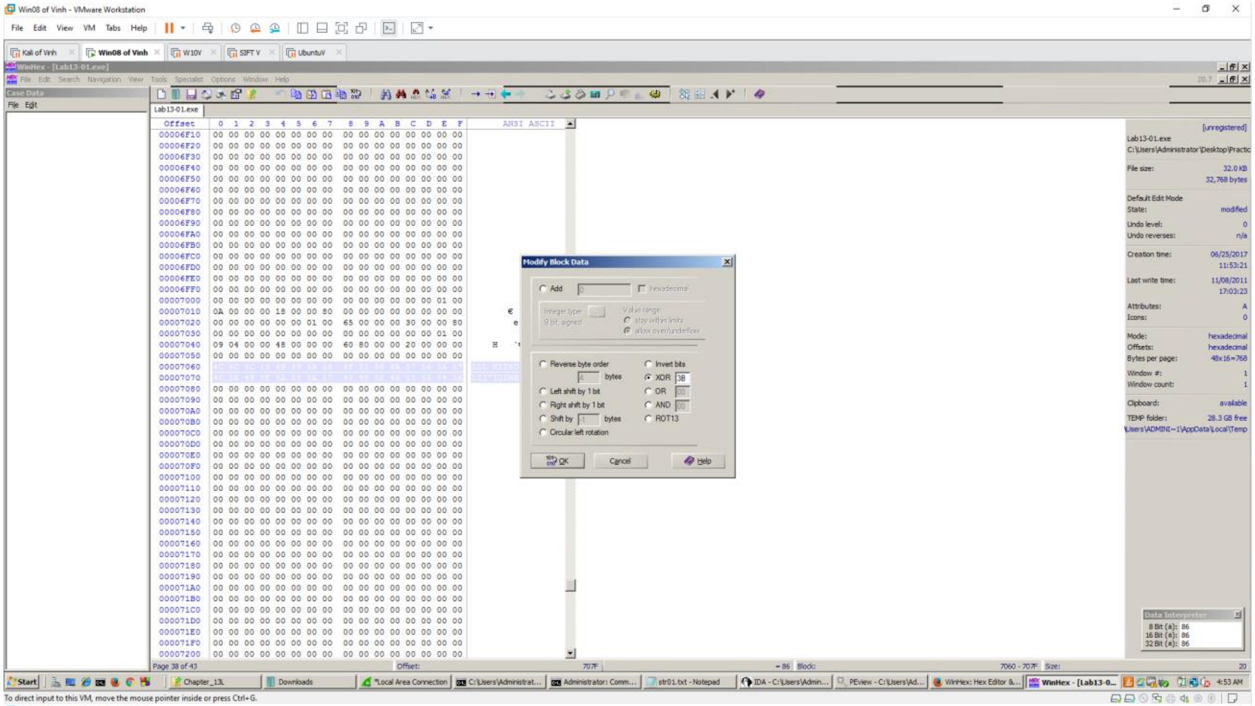
PEview - C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_13L\Lab13-01.exe

```
Lab13-01.exe
  IMAGE_DOS_HEADER
  MS-DOS Stub Program
  IMAGE_NT_HEADERS
  IMAGE_SECTION_HEADER .text
  IMAGE_SECTION_HEADER .rdata
  IMAGE_SECTION_HEADER .data
  IMAGE_SECTION_HEADER .rsrc
  SECTION .text
  SECTION .rdata
  SECTION .data
  SECTION .rsrc
    IMAGE_RESOURCE_DIRECTORY Type
    IMAGE_RESOURCE_DIRECTORY NameID
    IMAGE_RESOURCE_DIRECTORY Language
    IMAGE_RESOURCE_DATA_ENTRY
    RCDATA  0065  0409
```

```
pFile     Raw Data                                          Value
00007060  4C 4C 4C 15 4B 49 5A 58  4F 52 58 5A 57 56 5A 57  LLL.KIZXORXZWVZW
00007070  4C 5A 49 5E 5A 55 5A 57  42 48 52 48 15 58 54 56  LZI^ZUZWBHRH.XTV
```

Viewing RCDATA 0065 0409

WinHex



Win08 of Vinh - VMware Workstation

WinHex - [Lab13-01.exe]

```
  Offset   0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
00006F10  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00006F20  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00006F30  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00006F40  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00006F50  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00006F60  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00006F70  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00006F80  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00006F90  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00006FA0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00006FB0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00006FC0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00006FD0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00006FE0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00006FF0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00007000  00 00 00 00 00 00 00 00  00 00 00 00 00 00 01 00
00007010  0A 00 00 00 18 00 00 80  00 00 00 00 00 00 00 00         €
00007020  00 00 00 00 00 00 01 00  65 00 00 00 30 00 00 80          e
00007030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 01 00
00007040  09 04 00 00 48 00 00 00  60 80 00 00 20 00 00 00     H   `
00007050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00007060  4C 4C 4C 15 4B 49 5A 58  4F 52 58 5A 57 56 5A 57   LLL.KIZXO
00007070  4C 5A 49 5E 5A 55 5A 57  42 48 52 48 15 58 54 56   LZI^ZUZW
00007080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00007090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000070A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000070B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000070C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000070D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000070E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000070F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00007100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00007110  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00007120  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00007130  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00007140  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00007150  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00007160  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00007170  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00007180  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00007190  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000071A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000071B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000071C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000071D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000071E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000071F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00007200  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

Modify Block Data

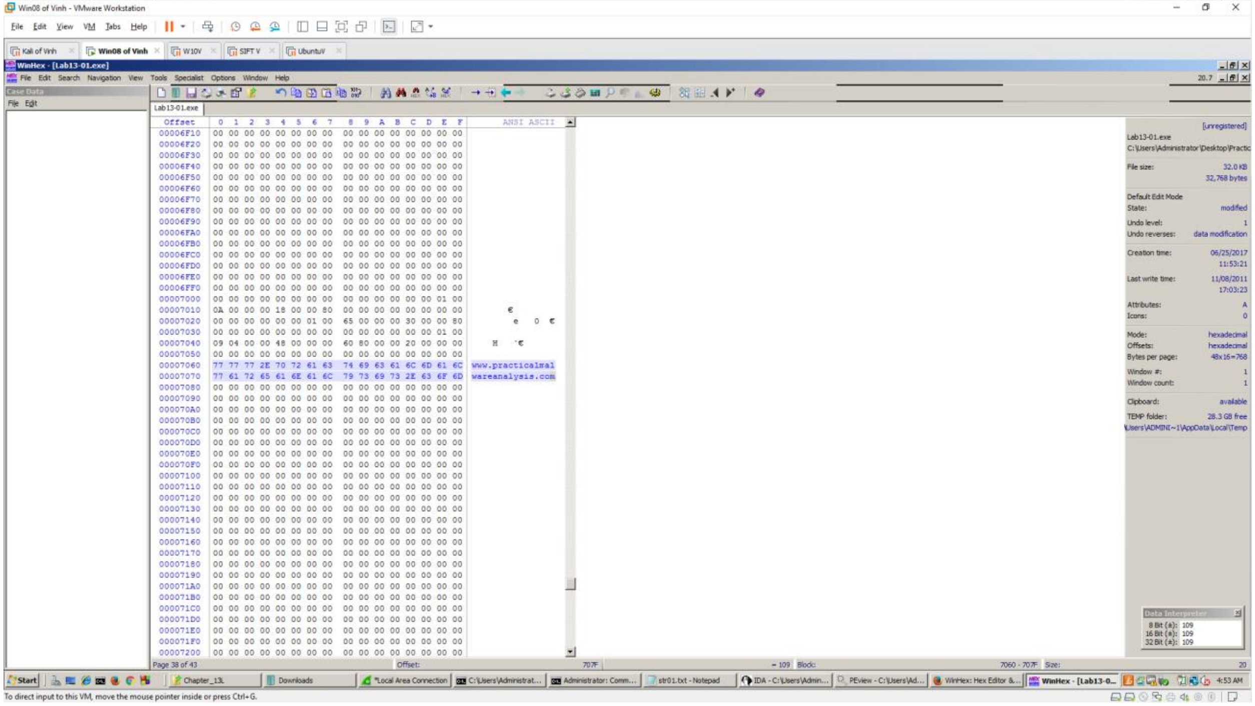
- ○ Add 0 □ hexadecimal
- Integer type: 8 bit, signed
- Value range: ○ stay within limits ● allow over/underflow
- ○ Reverse byte order 4 bytes
- ○ Invert bits
- ● XOR 3B
- ○ Left shift by 1 bit
- ○ OR 00
- ○ Right shift by 1 bit
- ○ AND 00
- ○ Shift by 1 bytes
- ○ ROT13
- ○ Circular left rotation

OK Cancel Help

Lab13-01.exe
C:\Users\Administrator\Desktop\Practic
File size: 32.0 KB, 32,768 bytes
Default Edit Mode
State: modified
Undo level: 0
Undo reverses: n/a
Creation time: 06/25/2017 11:53:21
Last write time: 11/08/2011 17:03:23
Attributes: A
Icons: 0
Mode: hexadecimal
Offsets: hexadecimal
Bytes per page: 48x16=768
Window #: 1
Window count: 1
Clipboard: available
TEMP folder: 28.3 GB free \Users\ADMINI~1\AppData\Local\Temp

Data Interpreter
8 Bit (±): 86
16 Bit (±): 86
32 Bit (±): 86

Page 38 of 43 Offset: 707F = 86 Block: 7060 - 707F Size: 20



Win08 of Vinh - VMware Workstation

WinHex - [Lab13-01.exe]

```
  Offset   0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
00006F10  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00006F20  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00006F30  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00006F40  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00006F50  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00006F60  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00006F70  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00006F80  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00006F90  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00006FA0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00006FB0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00006FC0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00006FD0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00006FE0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00006FF0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00007000  00 00 00 00 00 00 00 00  00 00 00 00 00 00 01 00
00007010  0A 00 00 00 18 00 00 80  00 00 00 00 00 00 00 00         €
00007020  00 00 00 00 00 00 01 00  65 00 00 00 30 00 00 80          e   0  €
00007030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 01 00
00007040  09 04 00 00 48 00 00 00  60 80 00 00 20 00 00 00     H   `€
00007050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
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  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00007090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000070A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000070B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000070C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000070D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000070E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000070F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00007100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00007110  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00007120  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00007130  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00007140  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00007150  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00007160  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00007170  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00007180  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00007190  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000071A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000071B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000071C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000071D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000071E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000071F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00007200  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

Lab13-01.exe
C:\Users\Administrator\Desktop\Practic
File size: 32.0 KB, 32,768 bytes
Default Edit Mode
State: modified
Undo level: 1
Undo reverses: data modification
Creation time: 06/25/2017 11:53:21
Last write time: 11/08/2011 17:03:23
Attributes: A
Icons: 0
Mode: hexadecimal
Offsets: hexadecimal
Bytes per page: 48x16=768
Window #: 1
Window count: 1
Clipboard: available
TEMP folder: 28.3 GB free \Users\ADMINI~1\AppData\Local\Temp

Data Interpreter
8 Bit (±): 109
16 Bit (±): 109
32 Bit (±): 109

Page 38 of 43 Offset: 707F = 109 Block: 7060 - 707F Size: 20