Greetings Class,

As stated in Lecture, all you need to do for this assignment is replicate what I did with rip.exe and send me your screenshots (see Rubric).

Assignment

--Download rip.exe from Professor Ervin's OneDrive account.

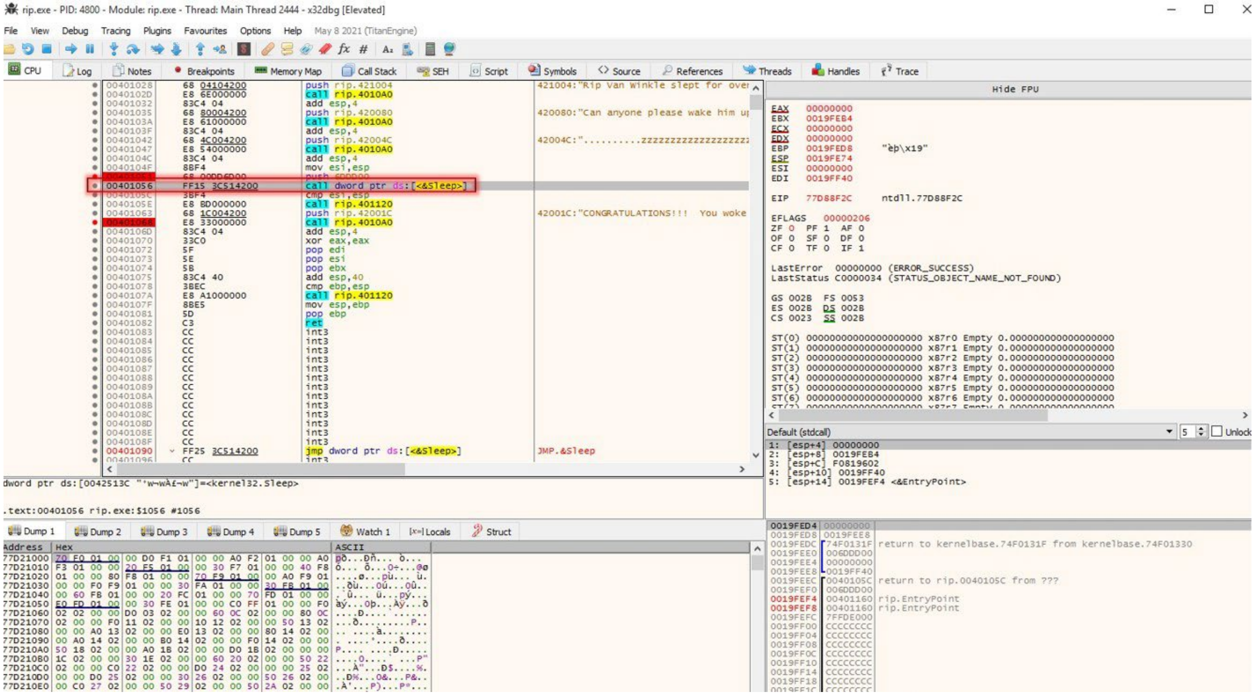
--Also, Install x64dbg to assist with your debugging efforts.

--To assist you, please reference Prof Ervin's lecture that demonstrates how to use x32dbg to debug and instrument executables. Additionally, how to use HxD to patch malware.

GRADING RUBRIC -- To receive full credit for this assignment, you must answer the following:

1. Use x32dbg to load rip.exe. Submit a screenshot of the debugger disassembly window showing the argument to the Sleep function.
2. Use HxD to patch rip.exe to no longer sleep. Submit a screenshot highlighting your HxD modifications.
3. Save a copy of your new modifications (i.e. rip2.exe) and execute at the command-line. Submit a screenshot showing that you woke RIP up.

1. Used x32dbg to load `rip.exe`. Below is a screenshot of the debugger disassembly window showing the argument to the Sleep function.


rip.exe - PID: 4800 - Module: rip.exe - Thread: Main Thread 2444 - x32dbg [Elevated]
File View Debug Tracing Plugins Favourites Options Help May 8 2021 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace
Hide FPU
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals Struct

```
00401028   68 04104200     push rip.421004               421004:"Rip Van Winkle slept for over
0040102D   E8 6E000000     call rip.4010A0
00401032   83C4 04         add esp,4
00401035   68 80004200     push rip.420080               420080:"Can anyone please wake him up
0040103A   E8 61000000     call rip.4010A0
0040103F   83C4 04         add esp,4
00401042   68 4C004200     push rip.42004C               42004C:"..........zzzzzzzzzzzzzzzzzzz
00401047   E8 54000000     call rip.4010A0
0040104C   83C4 04         add esp,4
0040104F   8BF4            mov esi,esp
00401051   68 00DD6D00     push 6DDD00
00401056   FF15 3C514200   call dword ptr ds:[<&Sleep>]
0040105C   3BF4            cmp esi,esp
0040105E   E8 BD000000     call rip.401120
00401063   68 1C004200     push rip.42001C               42001C:"CONGRATULATIONS!!!  You woke
00401068   E8 33000000     call rip.4010A0
0040106D   83C4 04         add esp,4
00401070   33C0            xor eax,eax
00401072   5F              pop edi
00401073   5E              pop esi
00401074   5B              pop ebx
00401075   83C4 40         add esp,40
00401078   3BEC            cmp ebp,esp
0040107A   E8 A1000000     call rip.401120
0040107F   8BE5            mov esp,ebp
00401081   5D              pop ebp
00401082   C3              ret
00401083   CC              int3
00401084   CC              int3
00401085   CC              int3
00401086   CC              int3
00401087   CC              int3
00401088   CC              int3
00401089   CC              int3
0040108A   CC              int3
0040108B   CC              int3
0040108C   CC              int3
0040108D   CC              int3
0040108E   CC              int3
0040108F   CC              int3
00401090   FF25 3C514200   jmp dword ptr ds:[<&Sleep>]   JMP.&Sleep
00401096   CC              int3

dword ptr ds:[0042513C "'w¬wÀ£¬w"]=<kernel32.Sleep>

.text:00401056 rip.exe:$1056 #1056
```

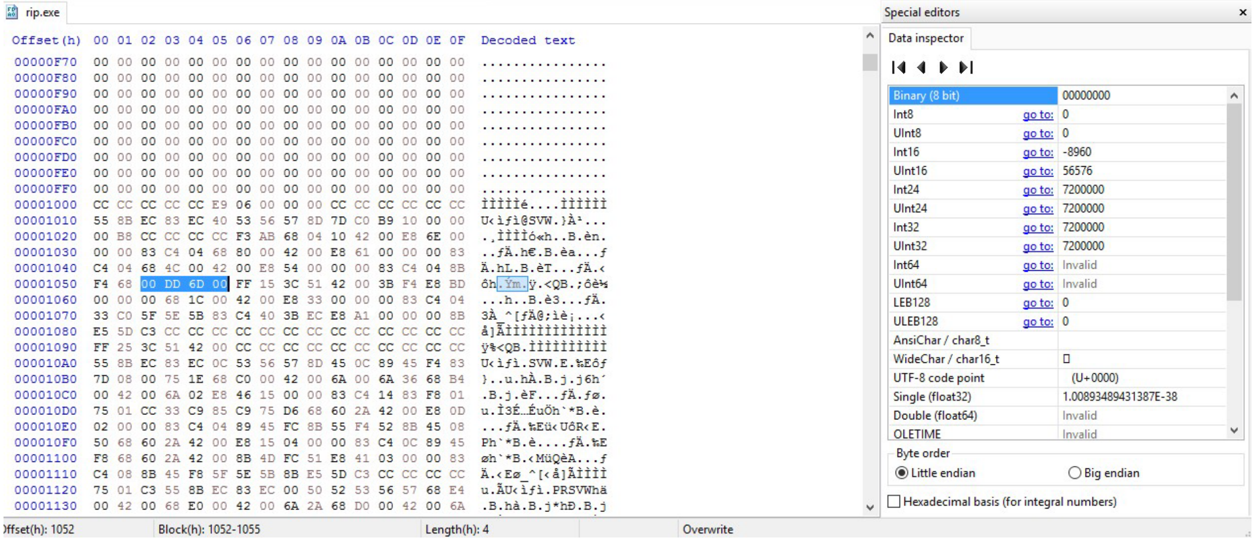
```
EAX     00000000
EBX     0019FEB4
ECX     00000000
EDX     00000000
EBP     0019FED8        "èþ\x19"
ESP     0019FE74
ESI     00000000
EDI     0019FF40

EIP     77D88F2C        ntdll.77D88F2C

EFLAGS    00000206
ZF 0  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1

LastError  00000000 (ERROR_SUCCESS)
LastStatus C0000034 (STATUS_OBJECT_NAME_NOT_FOUND)

GS 002B  FS 0053
ES 002B  DS 002B
CS 0023  SS 002B

ST(0) 00000000000000000000 x87r0 Empty 0.000000000000000000
ST(1) 00000000000000000000 x87r1 Empty 0.000000000000000000
ST(2) 00000000000000000000 x87r2 Empty 0.000000000000000000
ST(3) 00000000000000000000 x87r3 Empty 0.000000000000000000
ST(4) 00000000000000000000 x87r4 Empty 0.000000000000000000
ST(5) 00000000000000000000 x87r5 Empty 0.000000000000000000
ST(6) 00000000000000000000 x87r6 Empty 0.000000000000000000
```

```
Default (stdcall)                5  □ Unlock
1: [esp+4] 00000000
2: [esp+8] 0019FEB4
3: [esp+C] F0819602
4: [esp+10] 0019FF40
5: [esp+14] 0019FEF4 <&EntryPoint>
```

```
Address   Hex                                               ASCII
77D21000  70 F0 01 00 00 D0 F1 01 00 00 A0 F2 01 00 00 A0  pð...Ðñ... ò...
77D21010  F3 01 00 00 20 F5 01 00 00 30 F7 01 00 00 40 F8  ó... õ...0÷...@ø
77D21020  01 00 00 80 F8 01 00 00 70 F9 01 00 00 A0 F9 01  .....ø...pù... ù.
77D21030  00 00 F0 F9 01 00 00 30 FA 01 00 00 30 FB 01 00  ..ðù...0ú...0û..
77D21040  00 60 FB 01 00 00 20 FC 01 00 00 70 FD 01 00 00  .`û... ü...pý...
77D21050  E0 FD 01 00 00 30 FE 01 00 00 C0 FF 01 00 00 F0  àý...0þ...Àÿ...ð
77D21060  02 02 00 00 D0 03 02 00 00 60 0C 02 00 00 80 0C  ....Ð....`......
77D21070  02 00 00 F0 11 02 00 00 10 12 02 00 00 50 13 02  ...ð.........P..
77D21080  00 00 A0 13 02 00 00 E0 13 02 00 00 80 14 02 00  .. ....à........
77D21090  00 A0 14 02 00 00 B0 14 02 00 00 F0 14 02 00 00  . ....°....ð....
77D210A0  50 18 02 00 00 A0 1B 02 00 00 D0 1B 02 00 00 00  P.... ....Ð.....
77D210B0  1C 02 00 00 30 1E 02 00 00 60 20 02 00 00 50 22  ....0....` ...P"
77D210C0  02 00 00 C0 22 02 00 00 D0 24 02 00 00 00 25 02  ...À"...Ð$....%.
77D210D0  00 00 D0 25 02 00 00 30 26 02 00 00 50 26 02 00  ..Ð%...0&...P&..
77D210E0  00 C0 27 02 00 00 50 29 02 00 00 50 2A 02 00 00  .À'...P)...P*...
```

```
0019FED4  00000000
0019FED8  0019FEE8
0019FEDC  74F0131F  return to kernelbase.74F0131F from kernelbase.74F01330
0019FEE0  006DDD00
0019FEE4  00000000
0019FEE8  0019FF40
0019FEEC  0040105C  return to rip.0040105C from ???
0019FEF0  006DDD00
0019FEF4  00401160  rip.EntryPoint
0019FEF8  00401160  rip.EntryPoint
0019FEFC  7FFDE000
0019FF00  CCCCCCCC
0019FF04  CCCCCCCC
0019FF08  CCCCCCCC
0019FF0C  CCCCCCCC
0019FF10  CCCCCCCC
0019FF14  CCCCCCCC
0019FF18  CCCCCCCC
```

2. Used HxD to patch `rip.exe` to no longer sleep.



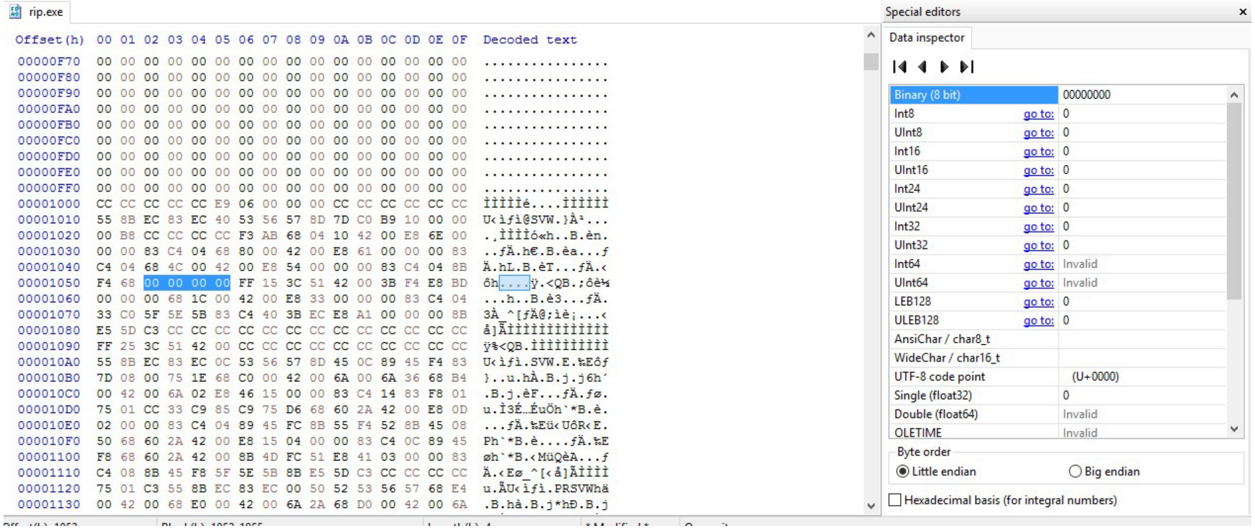
```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00000F70  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000F80  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000F90  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000FA0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000FB0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000FC0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000FD0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000FE0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000FF0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00001000  CC CC CC CC CC E9 06 00 00 00 CC CC CC CC CC CC  ÌÌÌÌÌé....ÌÌÌÌÌÌ
00001010  55 8B EC 83 EC 40 53 56 57 8D 7D C0 B9 10 00 00  U‹ìƒì@SVW.}À¹...
00001020  00 B8 CC CC CC CC F3 AB 68 04 10 42 00 E8 6E 00  .¸ÌÌÌÌó«h..B.èn.
00001030  00 00 83 C4 04 68 80 00 42 00 E8 61 00 00 00 83  ..ƒÄ.h€.B.èa...ƒ
00001040  C4 04 68 4C 00 42 00 E8 54 00 00 00 83 C4 04 8B  Ä.hL.B.èT...ƒÄ.‹
00001050  F4 68 00 DD 6D 00 FF 15 3C 51 42 00 3B F4 E8 BD  ôh.Ým.ÿ.<QB.;ôè½
00001060  00 00 00 68 1C 00 42 00 E8 33 00 00 00 83 C4 04  ...h..B.è3...ƒÄ.
00001070  33 C0 5F 5E 5B 83 C4 40 3B EC E8 A1 00 00 00 8B  3À_^[ƒÄ@;ìè¡...‹
00001080  E5 5D C3 CC CC CC CC CC CC CC CC CC CC CC CC CC  å]ÃÌÌÌÌÌÌÌÌÌÌÌÌÌ
00001090  FF 25 3C 51 42 00 CC CC CC CC CC CC CC CC CC CC  ÿ%<QB.ÌÌÌÌÌÌÌÌÌÌ
000010A0  55 8B EC 83 EC 0C 53 56 57 8D 45 0C 89 45 F4 83  U‹ìƒì.SVW.E.‰Eôƒ
000010B0  7D 08 00 75 1E 68 C0 00 42 00 6A 00 6A 36 68 B4  }..u.hÀ.B.j.j6h´
000010C0  00 42 00 6A 02 E8 46 15 00 00 83 C4 14 83 F8 01  .B.j.èF...ƒÄ.ƒø.
000010D0  75 01 CC 33 C9 85 C9 75 D6 68 60 2A 42 00 E8 0D  u.Ì3É…ÉuÖh`*B.è.
000010E0  02 00 00 83 C4 04 89 45 FC 8B 55 F4 52 8B 45 08  ...ƒÄ.‰Eü‹UôR‹E.
000010F0  50 68 60 2A 42 00 E8 15 04 00 00 83 C4 0C 89 45  Ph`*B.è....ƒÄ.‰E
00001100  F8 68 60 2A 42 00 8B 4D FC 51 E8 41 03 00 00 83  øh`*B.‹MüQèA...ƒ
00001110  C4 08 8B 45 F8 5F 5E 5B 8B E5 5D C3 CC CC CC CC  Ä.‹Eø_^[‹å]ÃÌÌÌÌ
00001120  75 01 C3 55 8B EC 83 EC 00 50 52 53 56 57 68 E4  u.ÃU‹ìƒì.PRSVWhä
00001130  00 42 00 68 E0 00 42 00 6A 2A 68 D0 00 42 00 6A  .B.hà.B.j*hÐ.B.j

Offset(h): 1052    Block(h): 1052-1055    Length(h): 4    Overwrite
```

Binary (8 bit)		00000000
Int8	go to:	0
UInt8	go to:	0
Int16	go to:	-8960
UInt16	go to:	56576
Int24	go to:	7200000
UInt24	go to:	7200000
Int32	go to:	7200000
UInt32	go to:	7200000
Int64	go to:	Invalid
UInt64	go to:	Invalid
LEB128	go to:	0
ULEB128	go to:	0
AnsiChar / char8_t		
WideChar / char16_t		□
UTF-8 code point		(U+0000)
Single (float32)		1.00893489431387E-38
Double (float64)		Invalid
OLETIME		Invalid

Byte order
● Little endian ○ Big endian

□ Hexadecimal basis (for integral numbers)

Without modifications via HxD

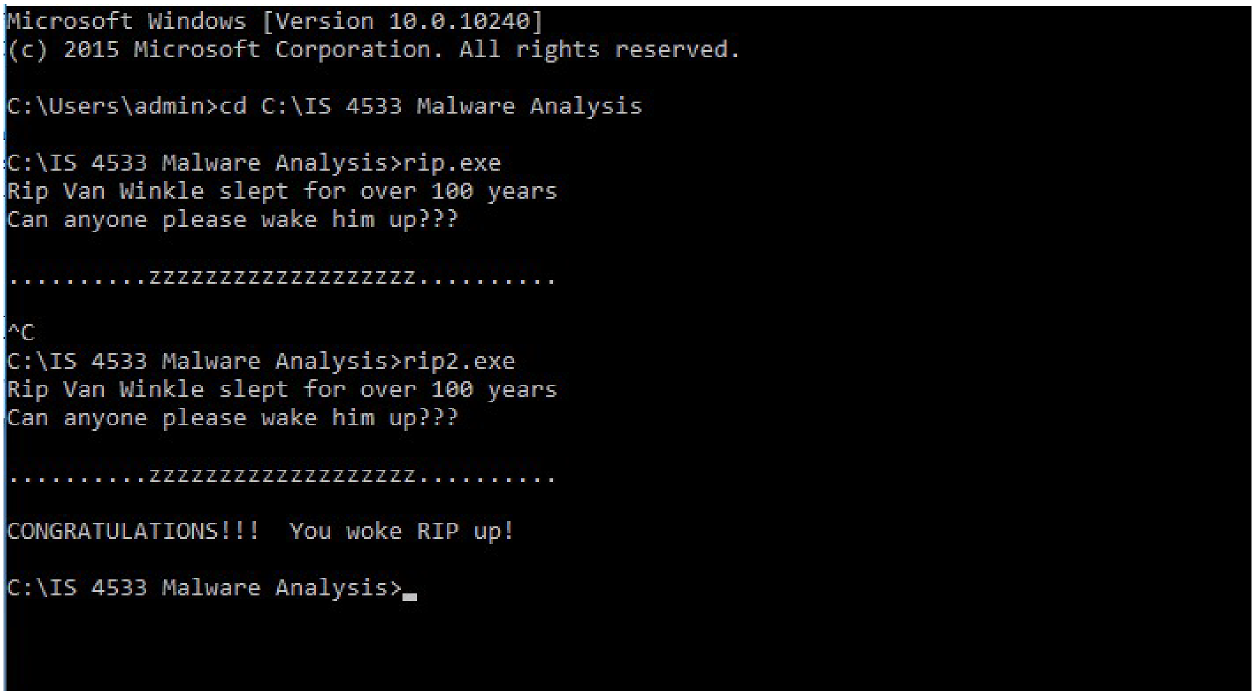


```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000F70  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000F80  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000F90  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000FA0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000FB0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000FC0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000FD0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000FE0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000FF0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00001000  CC CC CC CC CC E9 06 00 00 00 CC CC CC CC CC CC  ÌÌÌÌÌé....ÌÌÌÌÌÌ
00001010  55 8B EC 83 EC 40 53 56 57 8D 7D C0 B9 10 00 00  U‹ìƒì@SVW.}À¹...
00001020  00 B8 CC CC CC CC F3 AB 68 04 10 42 00 E8 6E 00  .¸ÌÌÌÌó«h..B.èn.
00001030  00 00 83 C4 04 68 80 00 42 00 E8 61 00 00 00 83  ..ƒÄ.h€.B.èa...ƒ
00001040  C4 04 68 4C 00 42 00 E8 54 00 00 00 83 C4 04 8B  Ä.hL.B.èT...ƒÄ.‹
00001050  F4 68 00 00 00 00 FF 15 3C 51 42 00 3B F4 E8 BD  ôh....ÿ.<QB.;ôè½
00001060  00 00 00 68 1C 00 42 00 E8 33 00 00 00 83 C4 04  ...h..B.è3...ƒÄ.
00001070  33 C0 5F 5E 5B 83 C4 40 3B EC E8 A1 00 00 00 8B  3À_^[ƒÄ@;ìè¡...‹
00001080  E5 5D C3 CC CC CC CC CC CC CC CC CC CC CC CC CC  å]ÃÌÌÌÌÌÌÌÌÌÌÌÌÌ
00001090  FF 25 3C 51 42 00 CC CC CC CC CC CC CC CC CC CC  ÿ%<QB.ÌÌÌÌÌÌÌÌÌÌ
000010A0  55 8B EC 83 EC 0C 53 56 57 8D 45 0C 89 45 F4 83  U‹ìƒì.SVW.E.‰Eôƒ
000010B0  7D 08 00 75 1E 68 C0 00 42 00 6A 00 6A 36 68 B4  }..u.hÀ.B.j.j6h´
000010C0  00 42 00 6A 02 E8 46 15 00 00 83 C4 14 83 F8 01  .B.j.èF...ƒÄ.ƒø.
000010D0  75 01 CC 33 C9 85 C9 75 D6 68 60 2A 42 00 E8 0D  u.Ì3É…ÉuÖh`*B.è.
000010E0  02 00 00 83 C4 04 89 45 FC 8B 55 F4 52 8B 45 08  ...ƒÄ.‰Eü‹UôR‹E.
000010F0  50 68 60 2A 42 00 E8 15 04 00 00 83 C4 0C 89 45  Ph`*B.è....ƒÄ.‰E
00001100  F8 68 60 2A 42 00 8B 4D FC 51 E8 41 03 00 00 83  øh`*B.‹MüQèA...ƒ
00001110  C4 08 8B 45 F8 5F 5E 5B 8B E5 5D C3 CC CC CC CC  Ä.‹Eø_^[‹å]ÃÌÌÌÌ
00001120  75 01 C3 55 8B EC 83 EC 00 50 52 53 56 57 68 E4  u.ÃU‹ìƒì.PRSVWhä
00001130  00 42 00 68 E0 00 42 00 6A 2A 68 D0 00 42 00 6A  .B.hà.B.j*hÐ.B.j
```

Binary (8 bit)		00000000
Int8	go to:	0
UInt8	go to:	0
Int16	go to:	0
UInt16	go to:	0
Int24	go to:	0
UInt24	go to:	0
Int32	go to:	0
UInt32	go to:	0
Int64	go to:	Invalid
UInt64	go to:	Invalid
LEB128	go to:	0
ULEB128	go to:	0
AnsiChar / char8_t		
WideChar / char16_t		
UTF-8 code point		(U+0000)
Single (float32)		0
Double (float64)		Invalid
OLETIME		Invalid

With modifications via HxD, changed `00 DD 6D 00` *to* `00 00 00 00`

3. Saved a copy of my new modifications as `rip2.exe` and executed at the command-line. Below is a screenshot depicting that I woke `RIP` up.



```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\admin>cd C:\IS 4533 Malware Analysis

C:\IS 4533 Malware Analysis>rip.exe
Rip Van Winkle slept for over 100 years
Can anyone please wake him up???

..........zzzzzzzzzzzzzzzzzzz..........

^C
C:\IS 4533 Malware Analysis>rip2.exe
Rip Van Winkle slept for over 100 years
Can anyone please wake him up???

..........zzzzzzzzzzzzzzzzzzz..........

CONGRATULATIONS!!!  You woke RIP up!

C:\IS 4533 Malware Analysis>
```