Errata for *Practical Malware Analysis* (updated to 16th printing)

**Page 10:** The two MD5 sums that read:
373e7a863a1a345c60edb9e20ec3231
should now read:
373e7a863a1a345c60edb9e20ec32311

**Page 54:** Figure 3-10 has been updated as follows:

![Figure 3-10](image)

**Page 66:** In Figure 4-1, “move” should now read “mov”

**Page 74:** The sentence which reads:

... instruction such as lea ebx, [eax*5+5], where eax is a number, rather than a memory address. This instruction is the functional equivalent of ebx = (eax+1)*5, but the former is
shorter or more efficient for the compiler to use instead of a total of four instructions (for example \texttt{inc eax; mov ecx, 5; mul ecx; mov ebx, eax}).

should now read:

\ldots instruction such as \texttt{lea ebx, [eax*4+4]}, where \texttt{eax} is a number, rather than a memory address. This instruction is the functional equivalent of \texttt{ebx = (eax+1)*4}, but the former is shorter or more efficient for the compiler to use instead of a total of four instructions (for example \texttt{inc eax; mov ecx, 4; mul ecx; mov ebx, eax}).

**Page 76:** The sentence that begins:
The instruction \texttt{nop} is actually a pseudonym for \texttt{xchg eax, eax} . . .

should now read:
The instruction \texttt{nop} is actually a pseudonym for \texttt{xchg eax, eax} . . .

**Page 79:** In Figure 4-8, the stack layout which reads:

\begin{verbatim}
Local Variable N
\ldots
Local Variable 1
Local Variable 2
Old EBP
Return Address
Argument 1
Argument 2
\ldots
Argument N
\end{verbatim}

should now read:

\begin{verbatim}
Local Variable N
\ldots
Local Variable 2
Local Variable 1
Old EBP
\end{verbatim}
In the last paragraph, the sentence which reads:
This works in the same way as `cmpsb`, but it compares the byte located at address ESI to AL, rather than to EDI.
should now read:
This works in the same way as `cmpsb`, but it compares the byte located at address EDI to AL, rather than to ESI.

“Table 4-12” should now read “Listing 4-2”

In Listing 6-1, “Total” should now read “total”

In Listings 6-4 and 6-5, the first two lines which read:
```
00401006 mov dword ptr [ebp-4], 0
0040100D mov dword ptr [ebp-8], 1
```
should now read:
```
00401006 mov dword ptr [ebp-4], 1
0040100D mov dword ptr [ebp-8], 2
```

The sentence which reads:
The `lpStartupInfo` structure for the process stores the standard output (1), standard input (2), and standard error (3) that will be used for the new process.
should now read:
The `lpStartupInfo` structure for the process stores the standard output (2), standard input (3), and standard error (1) that will be used for the new process.
Page 178: The sentence that ends with:
... and 0x411001 if the language is Chinese.
should now read:
... and 0x41100A if the language is Chinese.

Page 237: For technical accuracy, Listing 11-2 should include additional “...” breaks, so that it reads:

```
1000123F push offset LibFileName ; "samsrv.dll"
10001244 call esi ; LoadLibraryA
...
10001248 push offset aAdvapi32_dll_0 ; "advapi32.dll"
...
10001251 call esi ; LoadLibraryA
...
1000125B push offset ProcName ; "SamIConnect"
10001260 push ebx ; hModule
...
10001265 call esi ; GetProcAddress
...
10001281 push offset aSamrqueryinfor ; "SamrQueryInformationUser"
10001286 push ebx ; hModule
...
1000128C call esi ; GetProcAddress
...
100012C2 push offset aSamigetprivate ; "SamIGetPrivateData"
100012C7 push ebx ; hModule
...
100012CD call esi ; GetProcAddress
100012CF push offset aSystemfunction ; "SystemFunction025"
100012D4 push edi ; hModule
...
100012DA call esi ; GetProcAddress
100012DC push offset aSystemfuncti_0 ; "SystemFunction027"
100012E1 push edi ; hModule
...
100012E7 call esi ; GetProcAddress
```
Page 258: In the first line of Listing 12-3, `CREATE_SUSPEND` should now read `CREATE_SUSPENDED`.

Page 263: In the penultimate sentence of the first paragraph, `Sleep` should now read `SleepEx`.

Page 290: In Listing 13-10, `cbuf = f.read()` should now read `cbuf = cfile.read()`.

Page 338: “JZ -7” in Figure 15-5 should now read “JZ -6” and the opcodes underneath that text which read “74 F9” should now read “74 FA”

and the 3rd line of the listing which reads:

```
74 F9 jz short near ptr sub_4011C0+1
```

should now read:

```
74 FA jz short near ptr sub_4011C0+2
```

Page 339: The 7th line of the first listing which reads:

```
F9 db 0F9h
```

should now read:

```
FA db 0FAh
```

Page 363: Under “Inserting INT 2D,” “Listing 16-10” should instead read “Listing 16-9”.

Page 376: The text which reads “0x5668” should now read “0x5658” (once in the first paragraph and once in the third paragraph).

Page 440: In Question 3, the sentence that begins with:

“At 0x4036F0, there is a function call that takes the string . . .”

should now read:

“The function 0x4036F0 is called multiple times and each time it takes the string . . .”

Page 447: Both instances of “|WOW64” should now read “\Sys\WOW64”
**Page 448:** “C:\Windows\WOW64” should now read “C:\Windows\SysWOW64”

**Page 471:** The link to download PEview has been updated to: http://wjradburn.com/software/

**Page 499:** In the first paragraph:

View › Graphs › Xrefs From

should now read:

View › Graphs › User Xrefs Chart

**Page 514:** The last sentence of the page which reads:

If the call fails, the program exits.

should now read:

If the call succeeds, the program exits.

**Page 523:** The sentence which ends with:

. . . function to sleep for 60 seconds.

should now read:

. . . function to sleep for about 394 seconds.

**Page 566:** The sentence that begins with:

If you perform a full analysis of 0x4025120 . . .

should now read:

If you perform a full analysis of 0x402510 . . .

**Page 649:** At the beginning of the second paragraph, the sentence that begins with:

The two functions (sub_4012F2 and sub_401369) . . .

should now read:

The two functions (sub_40130F and sub_401386) . . .

**Page 651:** In Listing 15-12L (as well as in the disassembly of the corresponding lab), we added

add edx, 8 between the lines 00401202 and 00401208.
**Page 675:** In the first sentence of the second full paragraph on the page, “0x5668” should now read “0x5658”

**Page 680:** At the end of the second paragraph, “on page 670” should now read “on page 678”