Lab 2: Unpacking (5%)

What you need:

- The Malware Analysis Virtual Machine you prepared in a previous project

Malware Samples

This project uses files in this folder:

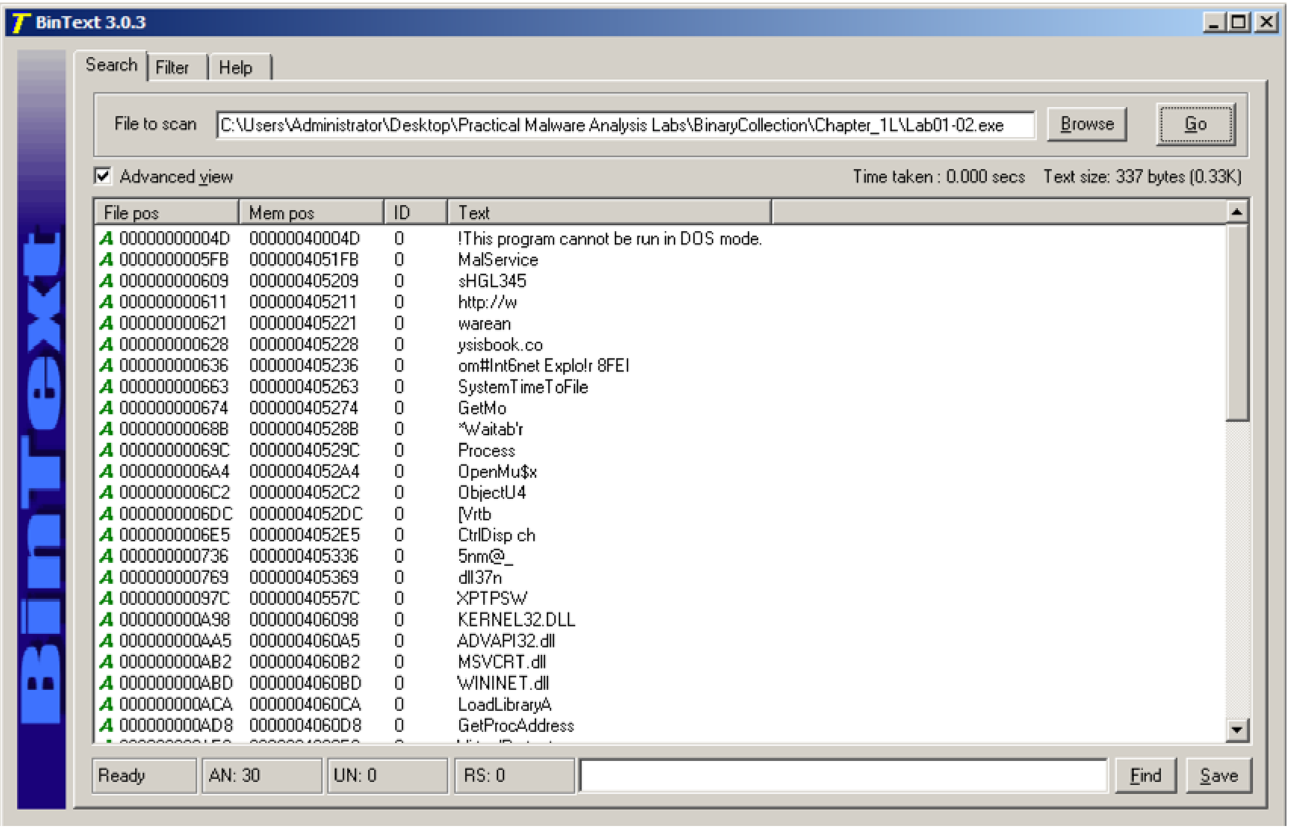
C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L

Examining the Strings in Lab01-02.exe with BinText

Examine the strings in **Lab01-02.exe** with BinText.

There are only a few strings, and they call only a few ordinary Windows API commands, as shown below.

These strings aren't from the malware--they are from the UPX packer, as we will show below.



File to scan: C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L\Lab01-02.exe

☑ Advanced view

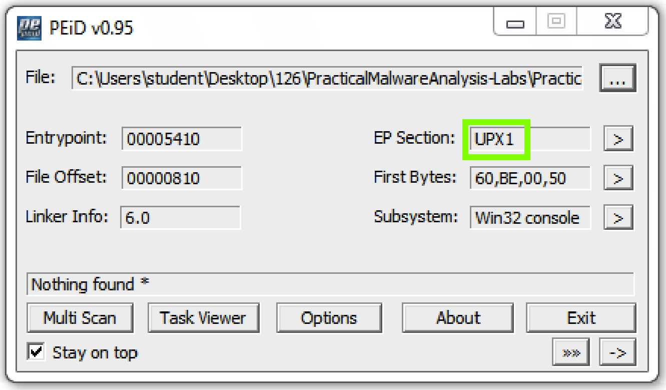
Time taken : 0.000 secs Text size: 337 bytes (0.33K)

File pos	Mem pos	ID	Text
A 00000000004D	00000040004D	0	!This program cannot be run in DOS mode.
A 0000000005FB	0000004051FB	0	MalService
A 000000000609	000000405209	0	sHGL345
A 000000000611	000000405211	0	http://w
A 000000000621	000000405221	0	warean
A 000000000628	000000405228	0	ysisbook.co
A 000000000636	000000405236	0	om#Int6net Explo!r 8FEI
A 000000000663	000000405263	0	SystemTimeToFile
A 000000000674	000000405274	0	GetMo
A 00000000068B	00000040528B	0	^Waitab'r
A 00000000069C	00000040529C	0	Process
A 0000000006A4	0000004052A4	0	OpenMu$x
A 0000000006C2	0000004052C2	0	ObjectU4
A 0000000006DC	0000004052DC	0	[Vrtb
A 0000000006E5	0000004052E5	0	CtrlDisp ch
A 000000000736	000000405336	0	5nm@_
A 000000000769	000000405369	0	dll37n
A 00000000097C	00000040557C	0	XPTPSW
A 000000000A98	000000406098	0	KERNEL32.DLL
A 000000000AA5	0000004060A5	0	ADVAPI32.dll
A 000000000AB2	0000004060B2	0	MSVCRT.dll
A 000000000ABD	0000004060BD	0	WININET.dll
A 000000000ACA	0000004060CA	0	LoadLibraryA
A 000000000AD8	0000004060D8	0	GetProcAddress

Ready AN: 30 UN: 0 RS: 0

Examining the File with PEiD

Run PEiD on the file. It shows that the file is packed with UPX, as shown in the "EP Section" below.



File: C:\Users\student\Desktop\126\PracticalMalwareAnalysis-Labs\Practic

Entrypoint: 00005410 EP Section: UPX1

File Offset: 00000810 First Bytes: 60,BE,00,50

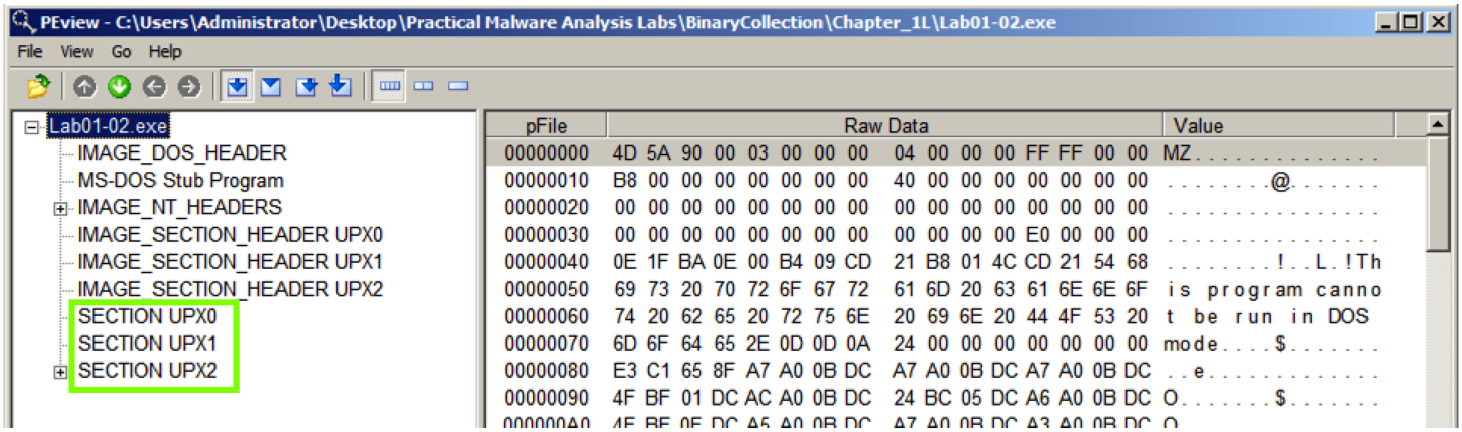
Linker Info: 6.0 Subsystem: Win32 console

Nothing found *

Examining the File with PEview

Run PEview on the file. The file has sections labeled **UPX0**, **UPX1**, and **UPX2**, as shown below.

These are section names produced by the UPX packer.


PEview - C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L\Lab01-02.exe
File View Go Help
Lab01-02.exe
IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
IMAGE_SECTION_HEADER UPX0
IMAGE_SECTION_HEADER UPX1
IMAGE_SECTION_HEADER UPX2
SECTION UPX0
SECTION UPX1
SECTION UPX2

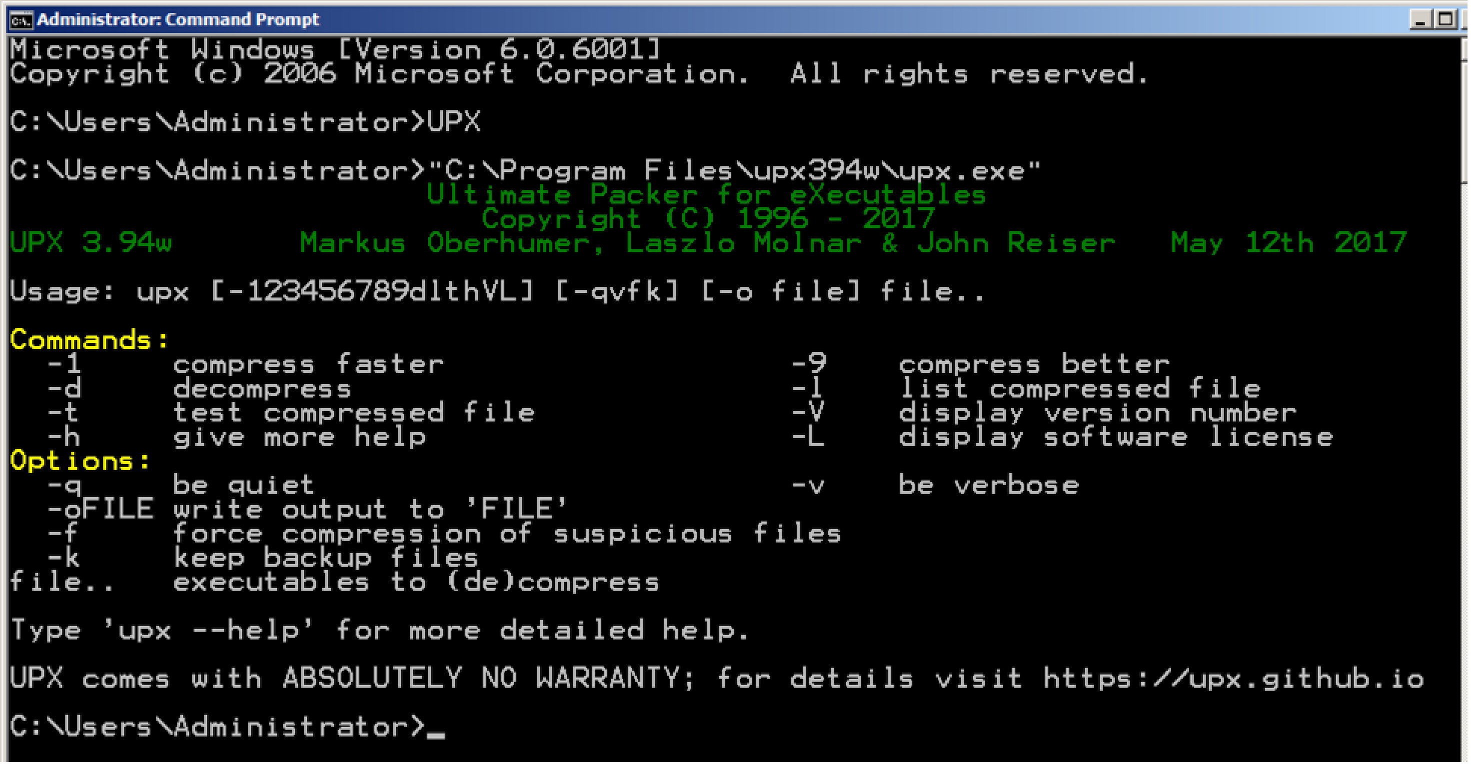
```
pFile     Raw Data                                         Value
00000000  4D 5A 90 00 03 00 00 00  04 00 00 00 FF FF 00 00  MZ..............
00000010  B8 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00  ........@.......
00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000030  00 00 00 00 00 00 00 00  00 00 00 00 E0 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....$.......
00000080  E3 C1 65 8F A7 A0 0B DC  A7 A0 0B DC A7 A0 0B DC  ..e.............
00000090  4F BF 01 DC AC A0 0B DC  24 BC 05 DC A6 A0 0B DC  O.......$.......
000000A0  4F BF 0F DC A5 A0 0B DC  A7 A0 0B DC A3 A0 0B DC  O
```

Unpacking the File with UPX

Open a Command Prompt window and execute this command:

```
UPX
```

You see a UPX help message, as shown below:

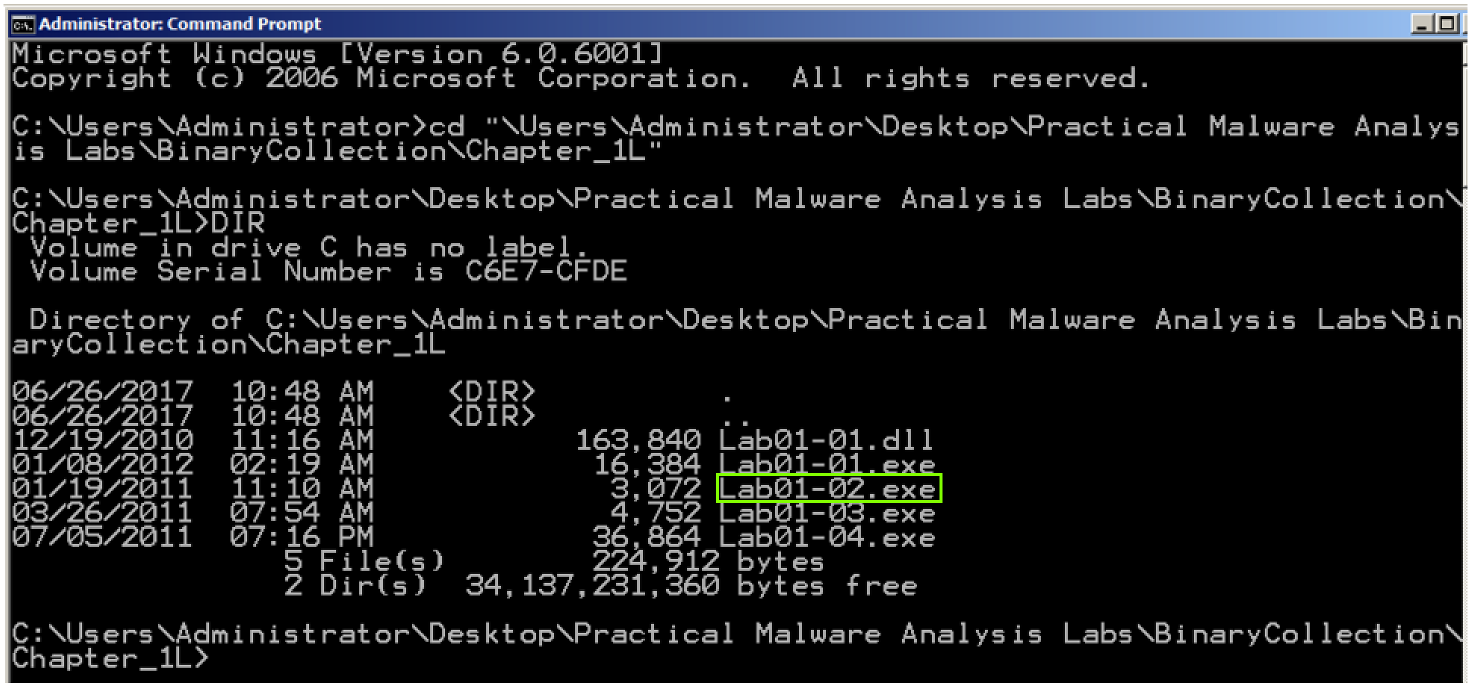


```
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>UPX

C:\Users\Administrator>"C:\Program Files\upx394w\upx.exe"
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2017
UPX 3.94w       Markus Oberhumer, Laszlo Molnar & John Reiser   May 12th 2017

Usage: upx [-123456789dlthVL] [-qvfk] [-o file] file..

Commands:
  -1     compress faster                           -9    compress better
  -d     decompress                                -l    list compressed file
  -t     test compressed file                      -V    display version number
  -h     give more help                            -L    display software license
Options:
  -q     be quiet                                  -v    be verbose
  -oFILE write output to 'FILE'
  -f     force compression of suspicious files
  -k     keep backup files
file..   executables to (de)compress

Type 'upx --help' for more detailed help.

UPX comes with ABSOLUTELY NO WARRANTY; for details visit https://upx.github.io

C:\Users\Administrator>_
```

Execute these commands to move to the directory containing the malware samples, and list the files there:

```
cd "\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L"

DIR
```

You see several malware samples, including **Lab01-02.exe**, as shown below:

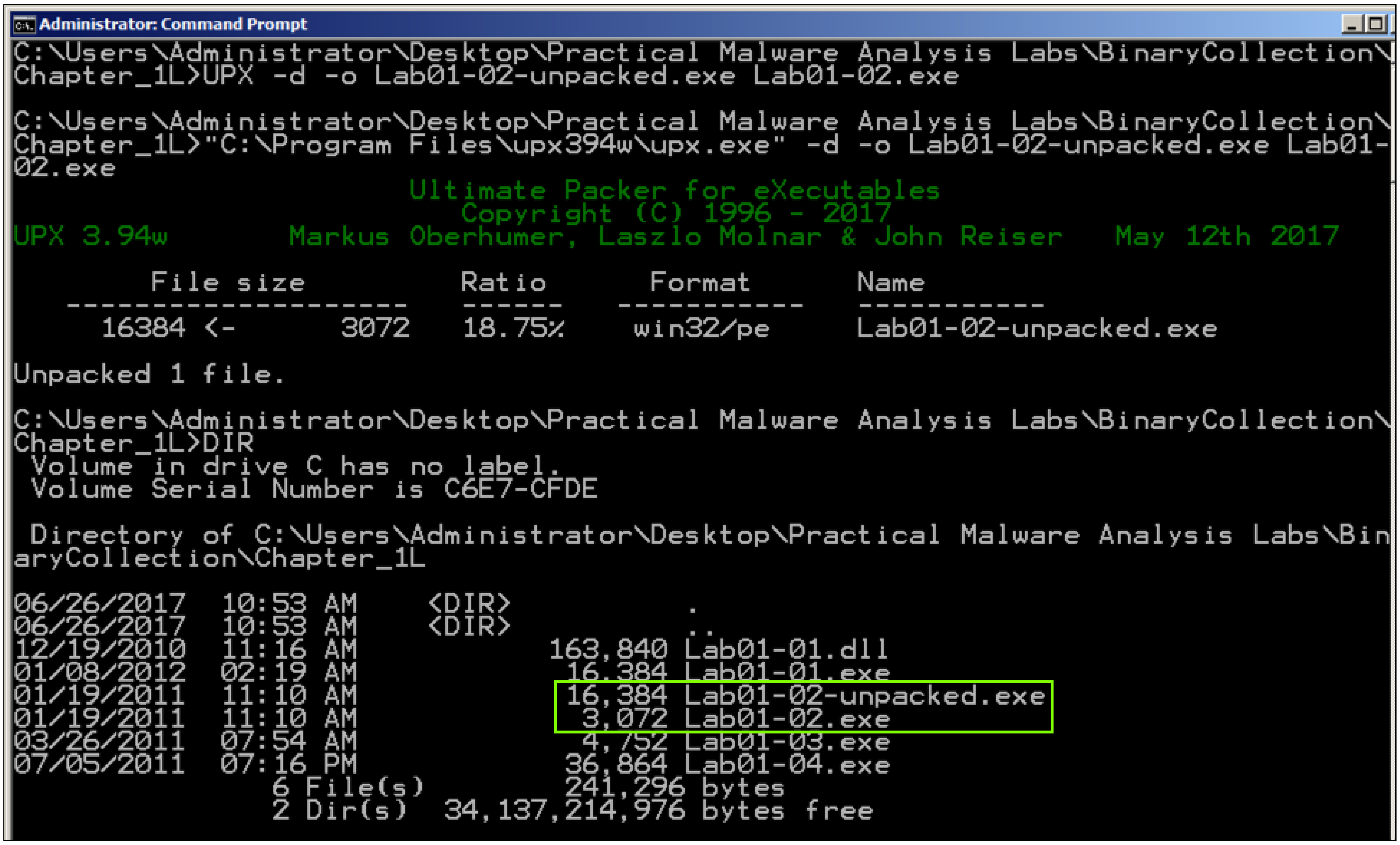


```
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>cd "\Users\Administrator\Desktop\Practical Malware Analys
is Labs\BinaryCollection\Chapter_1L"

C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\
Chapter_1L>DIR
 Volume in drive C has no label.
 Volume Serial Number is C6E7-CFDE

 Directory of C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\Bin
aryCollection\Chapter_1L

06/26/2017  10:48 AM    <DIR>          .
06/26/2017  10:48 AM    <DIR>          ..
12/19/2010  11:16 AM           163,840 Lab01-01.dll
01/08/2012  02:19 AM            16,384 Lab01-01.exe
01/19/2011  11:10 AM             3,072 Lab01-02.exe
03/26/2011  07:54 AM             4,752 Lab01-03.exe
07/05/2011  07:16 PM            36,864 Lab01-04.exe
               5 File(s)        224,912 bytes
               2 Dir(s)  34,137,231,360 bytes free

C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\
Chapter_1L>
```

Execute these commands to unpack the file, and list the files again:

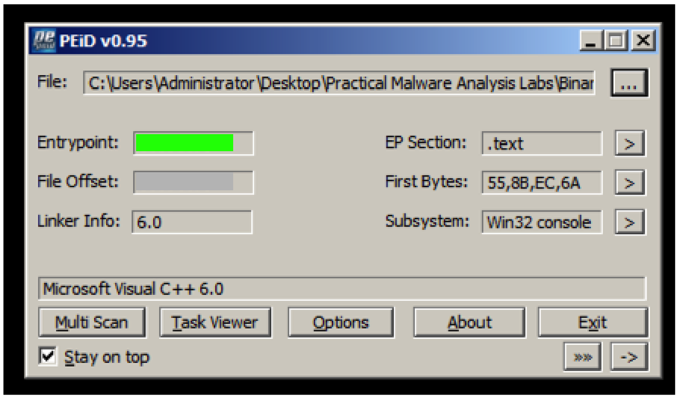
```
UPX -d -o Lab01-02-unpacked.exe Lab01-02.exe

DIR
```

The unpacked file is much larger than the original file, as shown below:



```
C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\
Chapter_1L>UPX -d -o Lab01-02-unpacked.exe Lab01-02.exe

C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\
Chapter_1L>"C:\Program Files\upx394w\upx.exe" -d -o Lab01-02-unpacked.exe Lab01-
02.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2017
UPX 3.94w       Markus Oberhumer, Laszlo Molnar & John Reiser   May 12th 2017

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
     16384 <-      3072   18.75%    win32/pe     Lab01-02-unpacked.exe

Unpacked 1 file.

C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\
Chapter_1L>DIR
 Volume in drive C has no label.
 Volume Serial Number is C6E7-CFDE

 Directory of C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\Bin
aryCollection\Chapter_1L

06/26/2017  10:53 AM    <DIR>          .
06/26/2017  10:53 AM    <DIR>          ..
12/19/2010  11:16 AM           163,840 Lab01-01.dll
01/08/2012  02:19 AM            16,384 Lab01-01.exe
01/19/2011  11:10 AM            16,384 Lab01-02-unpacked.exe
01/19/2011  11:10 AM             3,072 Lab01-02.exe
03/26/2011  07:54 AM             4,752 Lab01-03.exe
07/05/2011  07:16 PM            36,864 Lab01-04.exe
               6 File(s)        241,296 bytes
               2 Dir(s)  34,137,214,976 bytes free
```

Analyze the unpacked file with PEiD. It now is regognized as a "Microsoft Visual C++ 6.0" file, as shown below.



File: C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\Binar

Entrypoint: [redacted]

File Offset: [redacted]

Linker Info: 6.0

EP Section: .text

First Bytes: 55,8B,EC,6A

Subsystem: Win32 console

Microsoft Visual C++ 6.0

☑ Stay on top

Flag PMA 102.1: Entrypoint (10 pts)

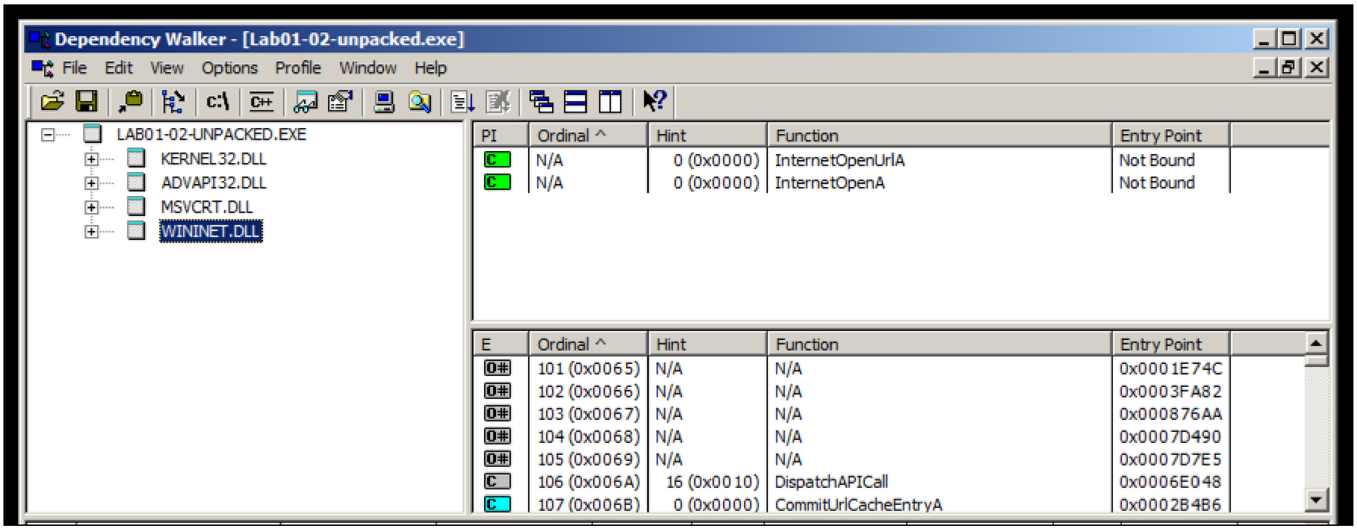
On the left side of the PeID box, find the **Entrypoint** value, which is covered by a green box in the image above. That's the flag.

Imports

Find the unpacked file's imports with Dependency Walker.

The imports from KERNEL32.DLL, ADVAPI32.DLL, and MSVCRT.DLL are uninformative generic functions used by almost every program.

However, the WININET.DLL imports are **InternetOpenUrlA** and **InternetOpenA**, as shown below. This indicates that the malware connects to a URL.



Dependency Walker - [Lab01-02-unpacked.exe]
File Edit View Options Profile Window Help

- LAB01-02-UNPACKED.EXE
  - KERNEL32.DLL
  - ADVAPI32.DLL
  - MSVCRT.DLL
  - WININET.DLL

PI	Ordinal ^	Hint	Function	Entry Point
C	N/A	0 (0x0000)	InternetOpenUrlA	Not Bound
C	N/A	0 (0x0000)	InternetOpenA	Not Bound

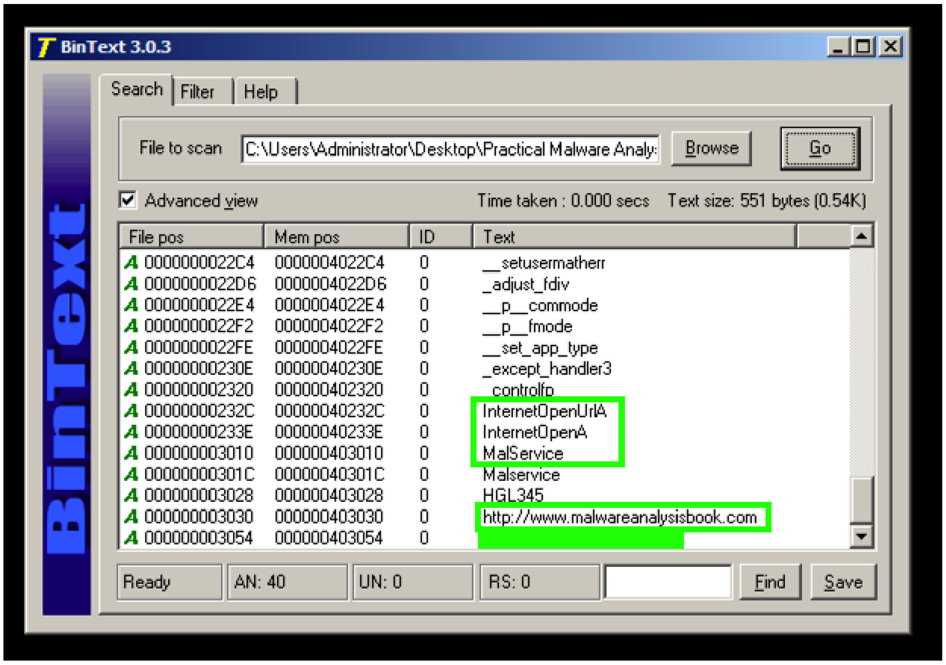
E	Ordinal ^	Hint	Function	Entry Point
0#	101 (0x0065)	N/A	N/A	0x0001E74C
0#	102 (0x0066)	N/A	N/A	0x0003FA82
0#	103 (0x0067)	N/A	N/A	0x000876AA
0#	104 (0x0068)	N/A	N/A	0x0007D490
0#	105 (0x0069)	N/A	N/A	0x0007D7E5
C	106 (0x006A)	16 (0x0010)	DispatchAPICall	0x0006E048
C	107 (0x006B)	0 (0x0000)	CommitUrlCacheEntryA	0x0002B4B6

Flag PMA 102.2: Strings (5 pts)

Find the strings in the unpacked file.

You should see the API names **InternetOpenURLA** and **InternetOpenA**, and the Command-and-Control URL **http://www.malwareanalysisbook.com**, as shown below.

These suggest that infected machines will connect to **http://www.malwareanalysisbook.com**. The name of the running service, **MalService**, is also visible.



File to scan: C:\Users\Administrator\Desktop\Practical Malware Analy

☑ Advanced view

Time taken : 0.000 secs Text size: 551 bytes (0.54K)

File pos	Mem pos	ID	Text
A 0000000022C4	0000004022C4	0	__setusermatherr
A 0000000022D6	0000004022D6	0	_adjust_fdiv
A 0000000022E4	0000004022E4	0	__p__commode
A 0000000022F2	0000004022F2	0	__p__fmode
A 0000000022FE	0000004022FE	0	__set_app_type
A 00000000230E	00000040230E	0	_except_handler3
A 000000002320	000000402320	0	_controlfp
A 00000000232C	00000040232C	0	InternetOpenUrlA
A 00000000233E	00000040233E	0	InternetOpenA
A 000000003010	000000403010	0	MalService
A 00000000301C	00000040301C	0	Malservice
A 000000003028	000000403028	0	HGL345
A 000000003030	000000403030	0	http://www.malwareanalysisbook.com
A 000000003054	000000403054	0	[redacted]

Ready | AN: 40 | UN: 0 | RS: 0

The last string is covered by a green box in the image above. That's the flag.

Flag PMA 102.3: Packer (10 pts)

Find the packer used for sample **Lab01-03.exe**.

Ignore everything except the primary packer name, which consists of three capital letters. That's the flag.

Posted 8-21-18
Chal 3.3 added 8-28-18
Chal 3.3 number fixed 9-11-18