File Name: **Lab01-01.exe**
Date Stamp: 2010-12-19T08:16:19
No. of Sections: 3
The imports are:

1. KERNEL32.dll
2. MSVCRT.dll

Please click here for detailed imports.
The sections are :

Section Name	Virtual Address	Virtual Size	Actual Size
.text	0x1000	2416	4096
.rdata	0x2000	690	4096
.data	0x3000	252	4096

The virtual and raw size of the file can be used to decide if the file is packed or not. Except the .data section, if the program raises other size flags, the file may be packed.
Some conclusions about the file from the python program. The messages are presented as python lists.

- ['The size flags raised are', ['.text\x00\x00\x00', '.rdata\x00\x00', '.data\x00\x00\x00']]
- The strings could not be extracted due to absence of resource directory
- ['The match found with the existing signature database were = ', ['Armadillo v1.71']]

File Name: **Lab01-02.exe**
Date Stamp: 2011-01-19T08:10:41
No. of Sections: 3
The imports are:

1. KERNEL32.DLL
2. ADVAPI32.dll
3. MSVCRT.dll
4. WININET.dll

Please click here for detailed imports.
The sections are :

Section Name	Virtual Address	Virtual Size	Actual Size
UPX0	0x1000	16384	0
UPX1	0x5000	4096	1536
UPX2	0x6000	4096	512

The virtual and raw size of the file can be used to decide if the file is packed or not. Except the .data section, if the program raises other size flags, the file may be packed.
Some conclusions about the file from the python program. The messages are presented as python lists.

- ['The size flags raised are', ['UPX0\x00\x00\x00\x00', 'UPX1\x00\x00\x00\x00', 'UPX2\x00\x00\x00\x00']]

- The file has been packed with UPX
- The strings could not be extracted due to absence of resource directory
- ['The match found with the existing signature database were = ', None]

File Name: **Lab01-03.exe**
Date Stamp: 1969-12-31T16:00:00
No. of Sections: 3
The imports are:

1. KERNEL32.dll

Please click here for detailed imports.
The sections are :

Section Name	Virtual Address	Virtual Size	Actual Size
t	0x1000	12288	0
ta	0x4000	4096	652
a	0x5000	4096	512

The virtual and raw size of the file can be used to decide if the file is packed or not. Except the .data section, if the program raises other size flags, the file may be packed.
Some conclusions about the file from the python program. The messages are presented as python lists.

- ['The size flags raised are', ['\x00\x00\x00\x00t\x00\x00\x00', '\x00\x00\x00\x00ta\x00\x00', '\x00\x00\x00\x00a\x00\x00\x00']]
- The strings could not be extracted due to absence of resource directory
- ['The match found with the existing signature database were = ', ['FSG v1.00 (Eng) -> dulek/xt']]

File Name: **Lab01-04.exe**
Date Stamp: 2019-08-30T15:26:59
No. of Sections: 4
The imports are:

1. KERNEL32.dll
2. ADVAPI32.dll
3. MSVCRT.dll

Please click here for detailed imports.
The sections are :

Section Name	Virtual Address	Virtual Size	Actual Size
.text	0x1000	1824	4096
.rdata	0x2000	978	4096
.data	0x3000	332	4096
.rsrc	0x4000	16480	20480

The virtual and raw size of the file can be used to decide if the file is packed or not. Except the .data section, if the program raises other size flags, the file may be packed.
Some conclusions about the file from the python program. The messages are presented as python lists.

- ['The size flags raised are', ['.text\x00\x00\x00', '.rdata\x00\x00', '.data\x00\x00\x00', '.rsrc\x00\x00\x00']]
- ['The OS path strings extracted were = ', []]
- ['The URL extracted from strings were = ', []]
- ['The match found with the existing signature database were = ', ['Armadillo v1.71']]

File Name: **Lab03-01.exe**
Date Stamp: 2008-01-06T06:51:31
No. of Sections: 2
The imports are:

1. kernel32.dll

Please click here for detailed imports.
The sections are :

Section Name	Virtual Address	Virtual Size	Actual Size
.text	0x200	104	512
.data	0x400	5775	6144

The virtual and raw size of the file can be used to decide if the file is packed or not. Except the .data section, if the program raises other size flags, the file may be packed.
Some conclusions about the file from the python program. The messages are presented as python lists.

- ['The size flags raised are', []]
- The strings could not be extracted due to absence of resource directory
- ['The match found with the existing signature database were = ', None]

File Name: **Lab03-03.exe**
Date Stamp: 2011-04-08T10:54:23
No. of Sections: 4
The imports are:

1. KERNEL32.dll

Please click here for detailed imports.
The sections are :

Section Name	Virtual Address	Virtual Size	Actual Size
.text	0x1000	11926	12288
.rdata	0x4000	2290	4096
.data	0x5000	2012	4096
.rsrc	0x6000	24708	28672

The virtual and raw size of the file can be used to decide if the file is packed or not. Except the .data section, if the program raises other size flags, the file may be packed.
Some conclusions about the file from the python program. The messages are presented as python lists.

- ['The size flags raised are', ['.rdata\x00\x00', '.data\x00\x00\x00', '.rsrc\x00\x00\x00']]
- ['The OS path strings extracted were = ', []]
- ['The URL extracted from strings were = ', []]
- ['The match found with the existing signature database were = ', ['Armadillo v1.71']]

File Name: **Lab03-04.exe**
Date Stamp: 2011-10-18T11:46:44
No. of Sections: 3
The imports are:

1. KERNEL32.dll
2. ADVAPI32.dll
3. SHELL32.dll
4. WS2_32.dll

Please click here for detailed imports.
The sections are :

Section Name	Virtual Address	Virtual Size	Actual Size
.text	0x1000	37704	40960
.rdata	0xb000	3440	4096
.data	0xc000	16828	12288

The virtual and raw size of the file can be used to decide if the file is packed or not. Except the .data section, if the program raises other size flags, the file may be packed.
Some conclusions about the file from the python program. The messages are presented as python lists.

- ['The size flags raised are', ['.text\x00\x00\x00', '.data\x00\x00\x00']]
- The strings could not be extracted due to absence of resource directory
- ['The match found with the existing signature database were = ', ['Armadillo v1.71']]