



## Lab 1:

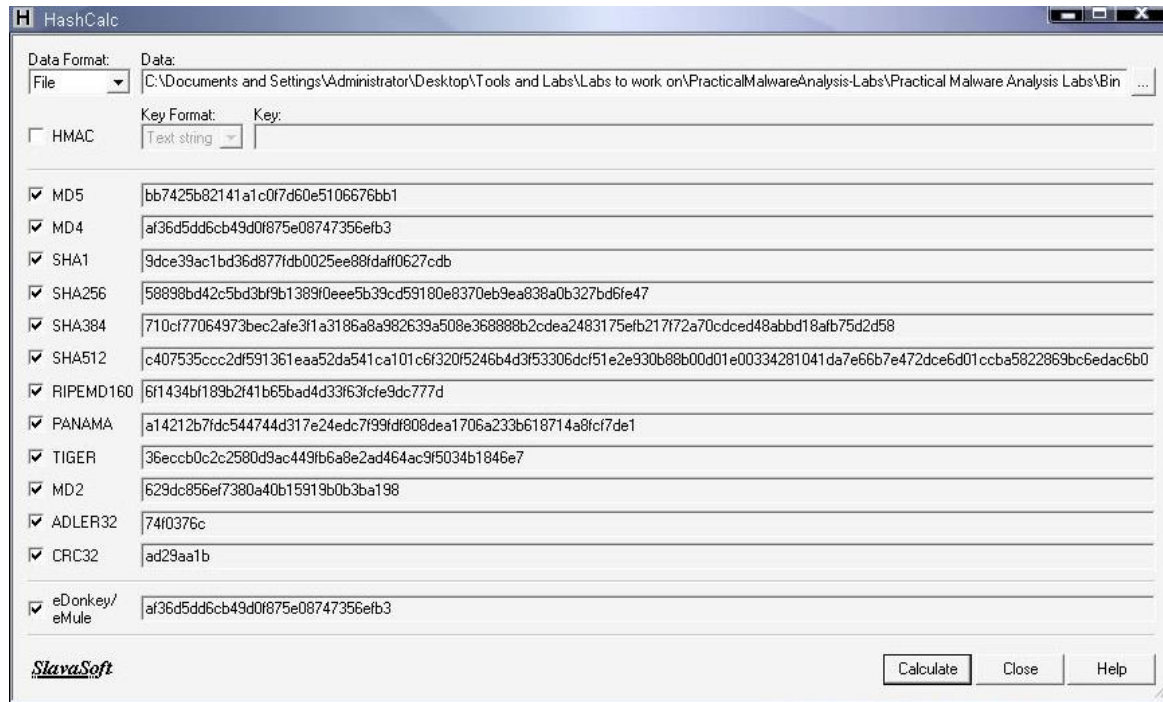


Figure 1 Lab01-1

## Lab 2:

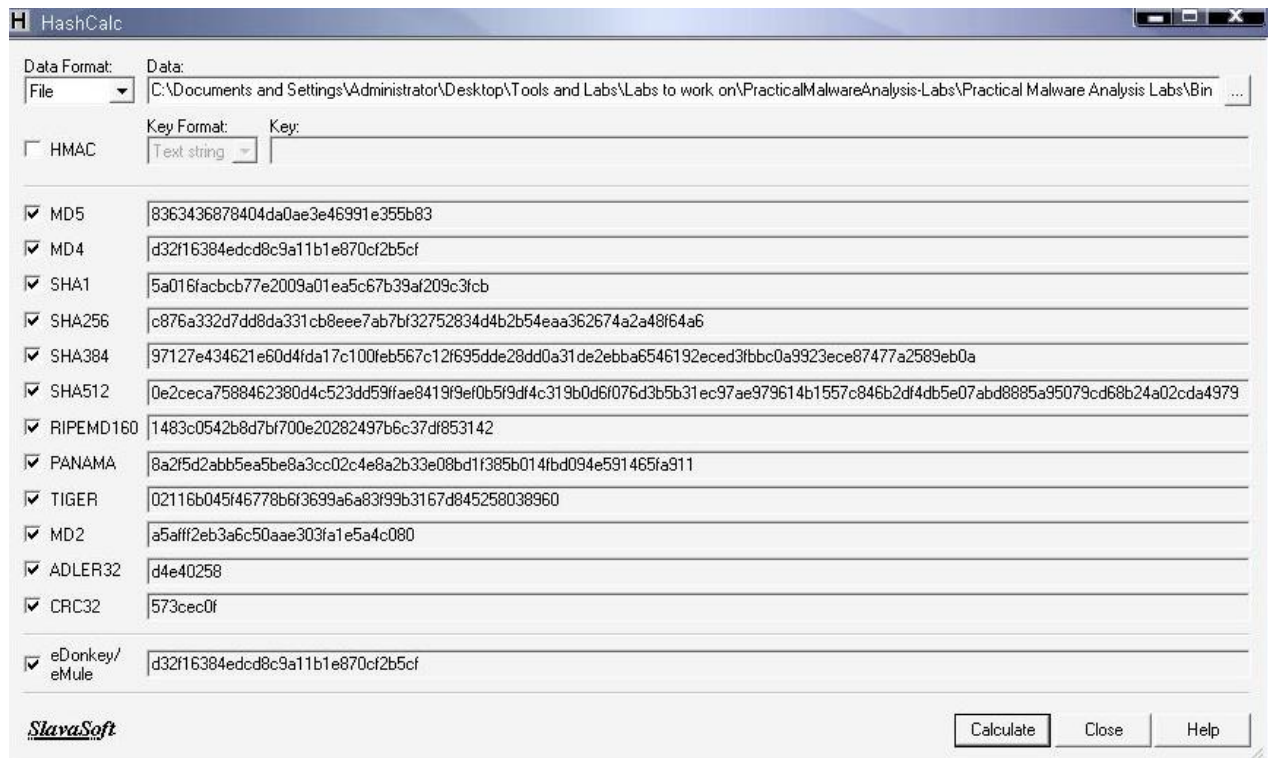


Figure 2 Lab01-2

## Lab 3:

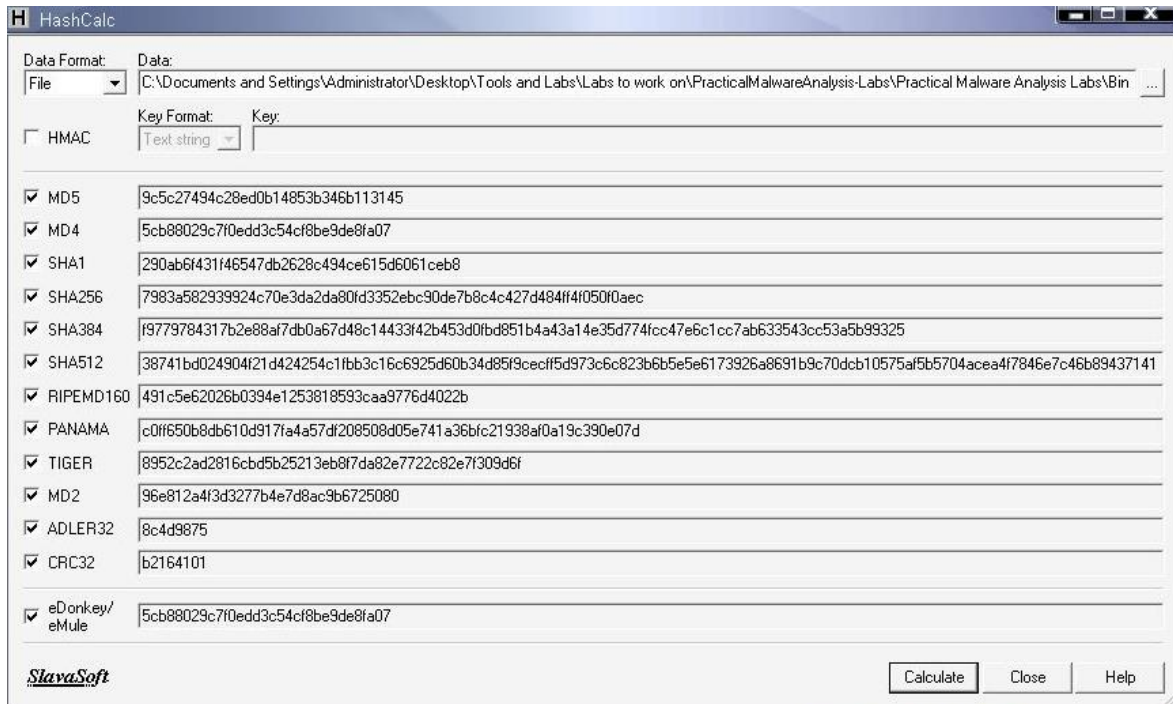


Figure 3 Lab01-3

## Lab 4:

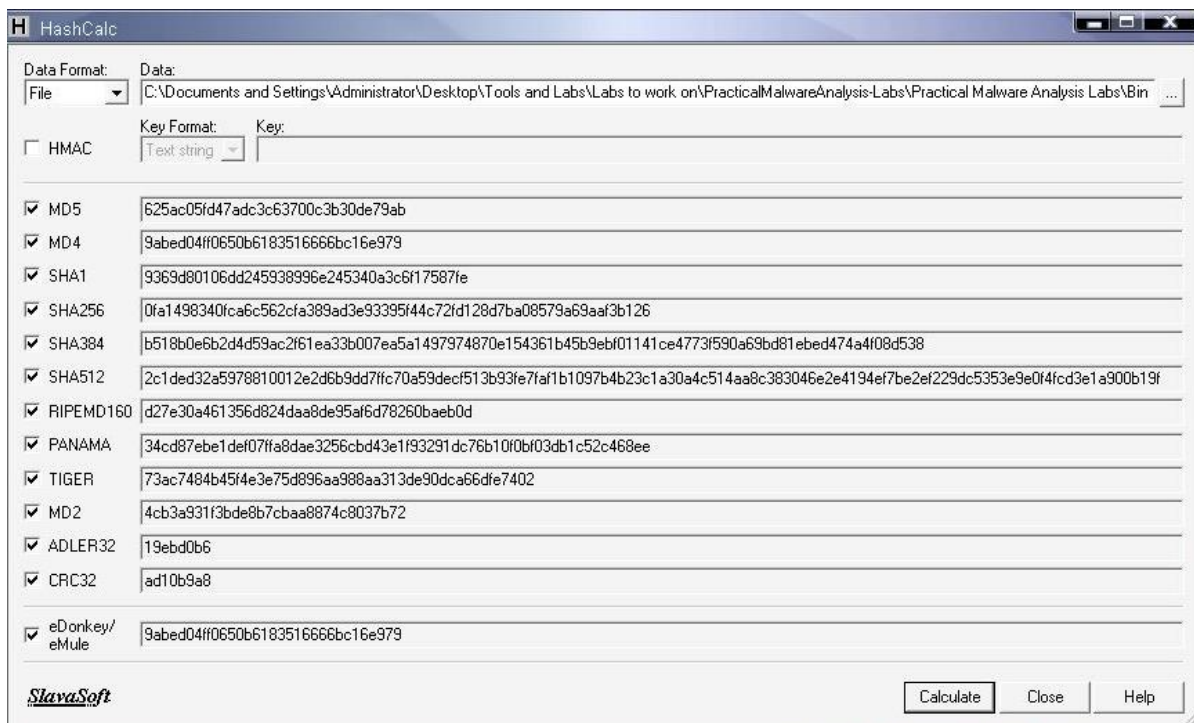


Figure 4 Lab01-4



## Lab 1:

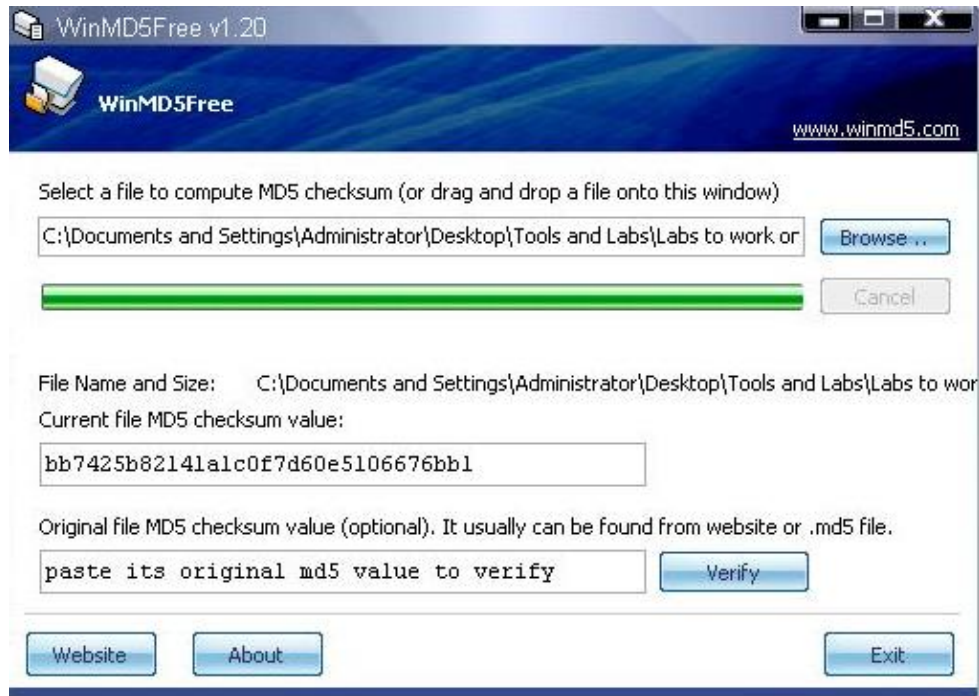


Figure 5 Lab01-1

## Lab 2:

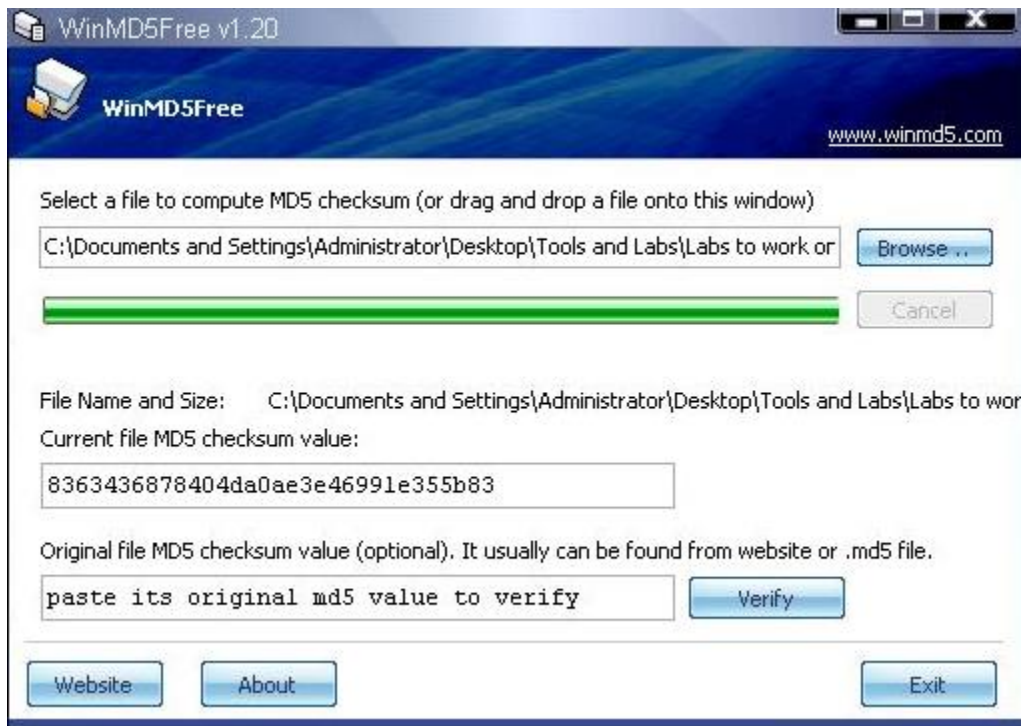


Figure 6 Lab01-2

### **Lab 3:**

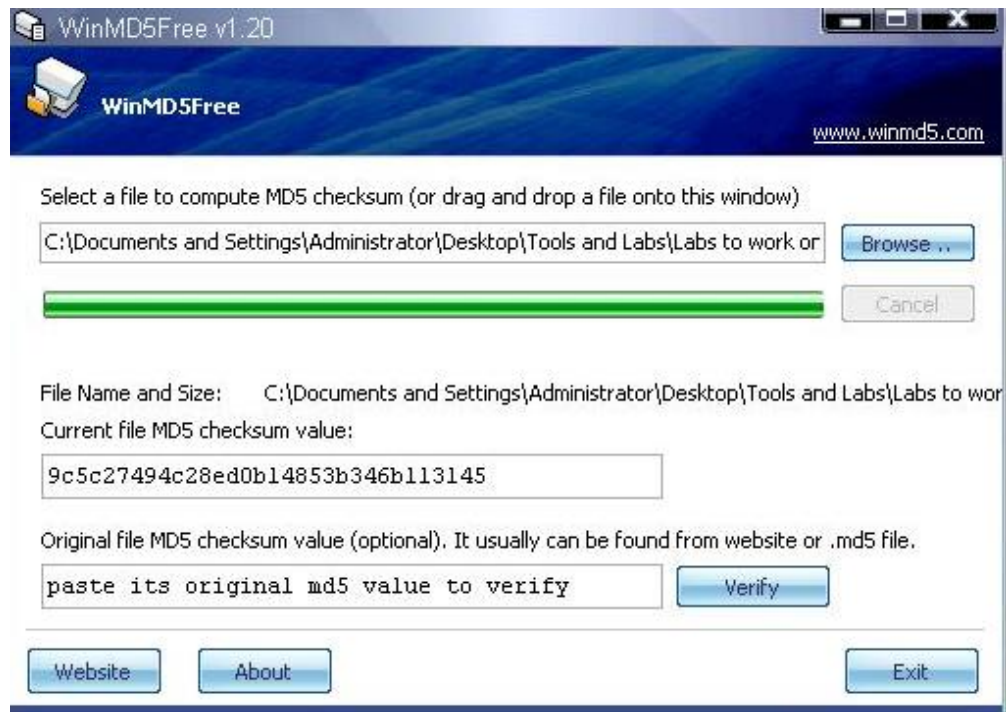


Figure 7 Lab01-3

### **Lab 4:**

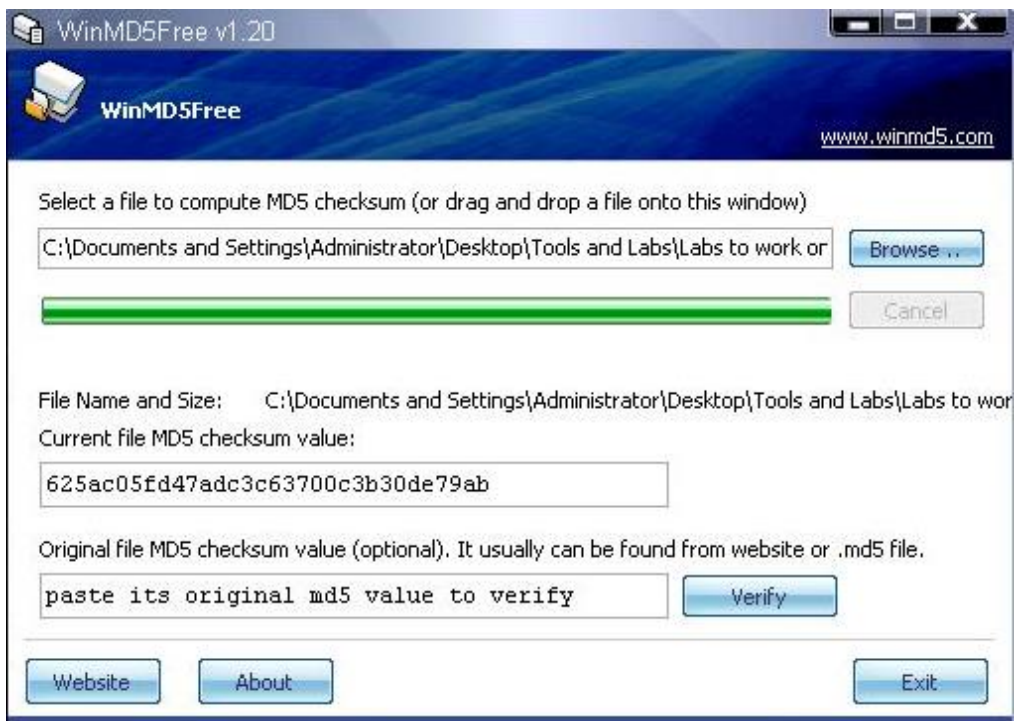
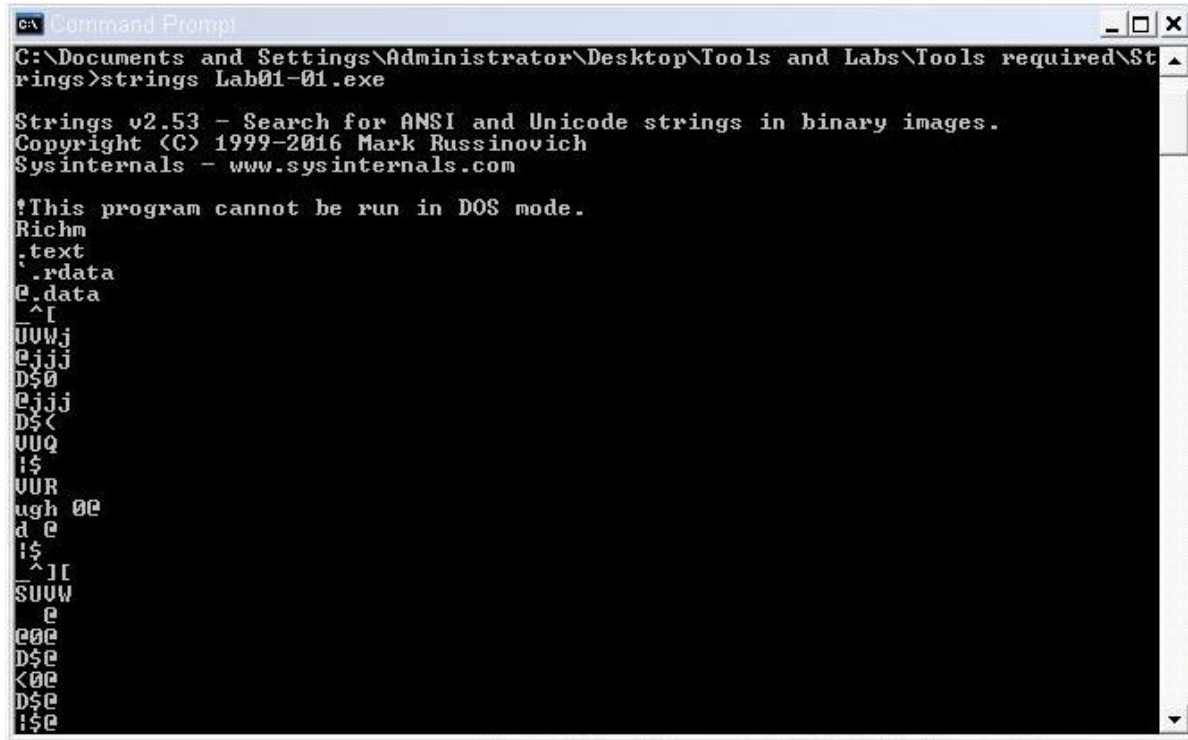


Figure 8 Lab01-4





## Lab 1:



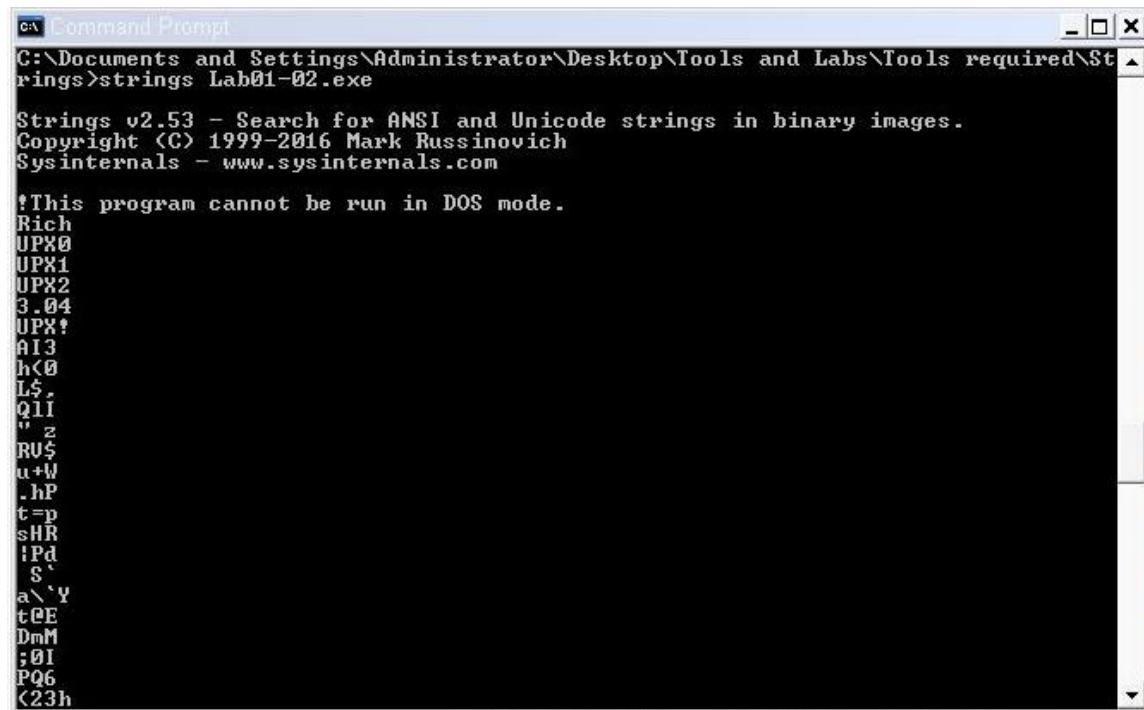
```
C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Tools required\Strings>strings Lab01-01.exe

Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

!This program cannot be run in DOS mode.
Richm
: text
: .rdata
@.data
^I
UUWj
@jjj
D$0
@jjj
D$<
UUQ
i$
UUR
ugh 00
d e
i$
^I
SUUV
e
000
D$e
<00
D$e
i$e
```

Figure 9 Lab01-1

## Lab 2:



```
C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Tools required\Strings>strings Lab01-02.exe

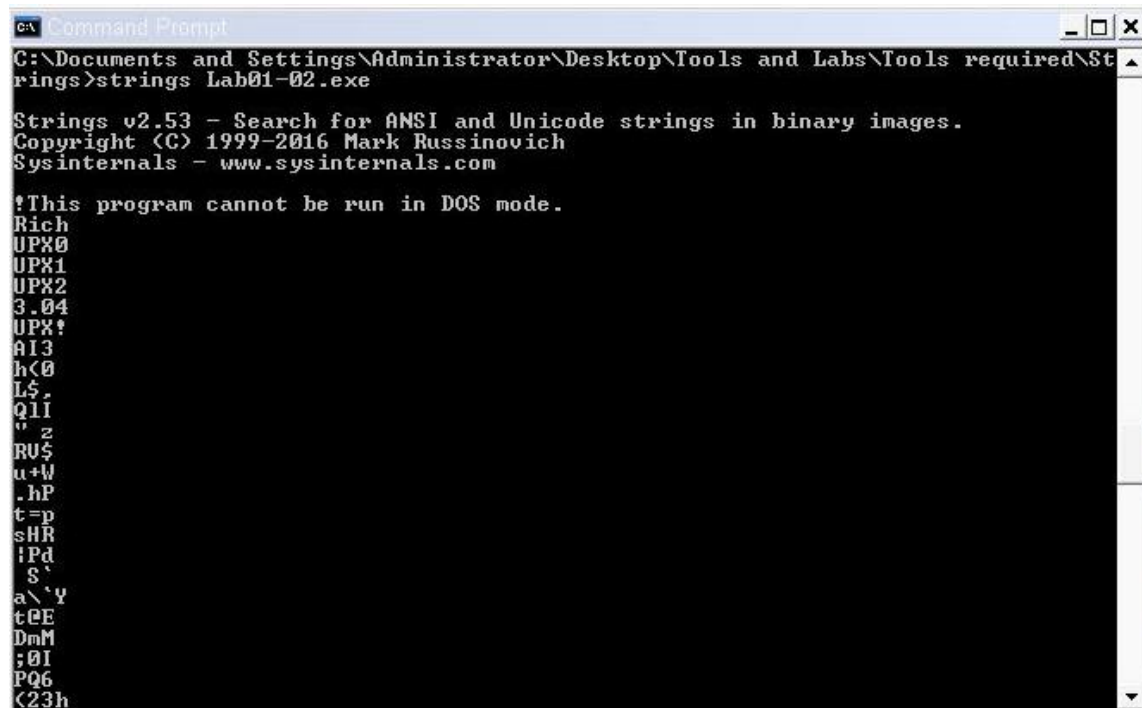
Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

!This program cannot be run in DOS mode.
Rich
UPX0
UPX1
UPX2
3.04
UPX!
AI3
h<0
L$,
QII
" z
RU$
u+w
.hP
t=p
sHR
iPd
S'
a\'Y
tEE
DmM
;0I
PQ6
<23h
```

Figure 10 Lab01-2



### Lab 3:



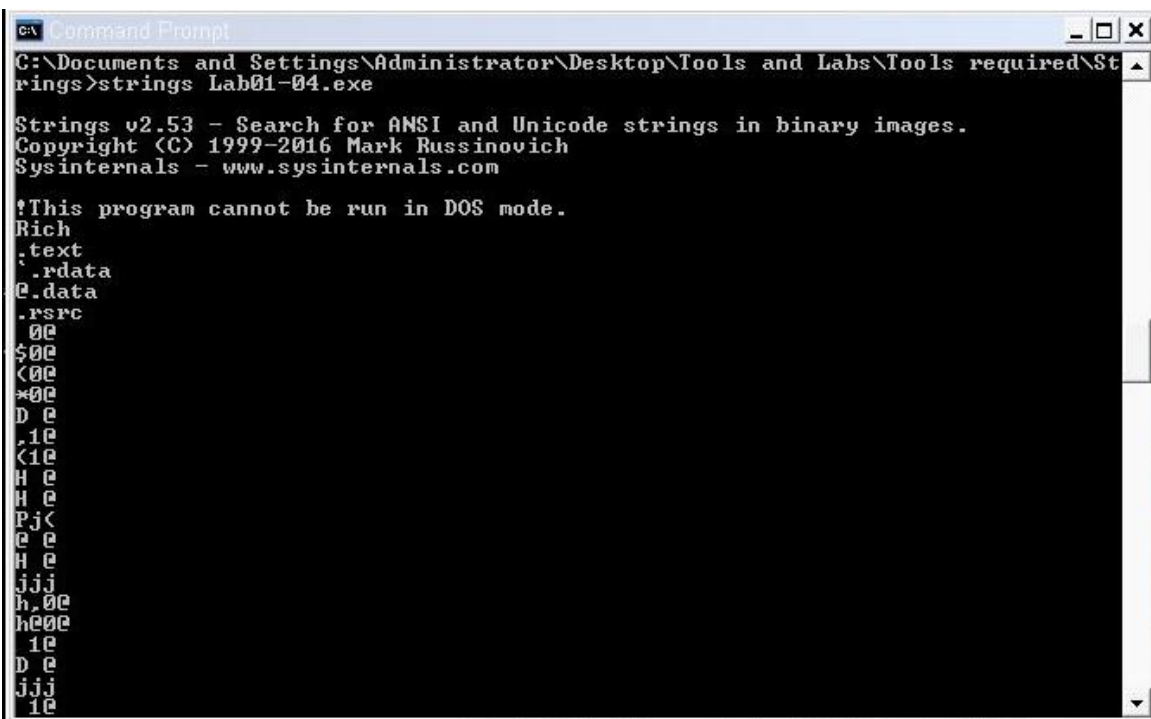
```
C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Tools required\Strings>strings Lab01-02.exe

Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

!This program cannot be run in DOS mode.
Rich
UPX0
UPX1
UPX2
3.04
UPX!
AI3
h<0
L$
Q1I
" z
RU$
u+W
.hP
t=p
sHR
!Pd
S`
a\'Y
t0E
DmM
;0I
PQ6
<23h
```

Figure 11 Lab01-3

### Lab 4:



```
C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Tools required\Strings>strings Lab01-04.exe

Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

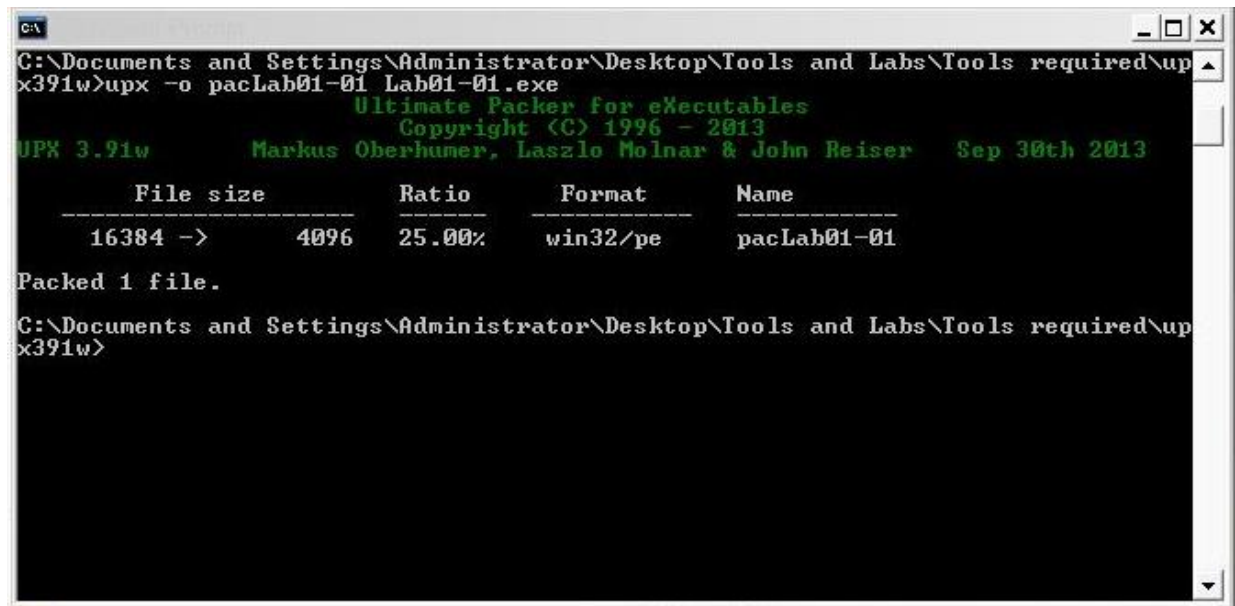
!This program cannot be run in DOS mode.
Rich
.text
.rdata
.data
.rsrc
00
$00
<00
*00
D 0
.10
<10
H 0
H 0
Pj<
e 0
H 0
jjj
h.00
h000
10
D 0
jjj
10
```

Figure 12 Lab01-4



## Compress

### Lab 1:



```
C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Tools required\upx391w>upx -o pacLab01-01 Lab01-01.exe
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2013
UPX 3.91w Markus Oberhumer, Laszlo Molnar & John Reiser Sep 30th 2013

  File size   Ratio   Format   Name
-----
  16384 ->   4096  25.00%  win32/pe  pacLab01-01

Packed 1 file.

C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Tools required\upx391w>
```

Figure 13 Lab01-1

### Lab 2:



```
C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Tools required\St
rings>cd C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Tools re
quired\upx391w

C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Tools required\upx391w>upx -o pacLab01-02 Lab01-02.exe
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2013
UPX 3.91w Markus Oberhumer, Laszlo Molnar & John Reiser Sep 30th 2013

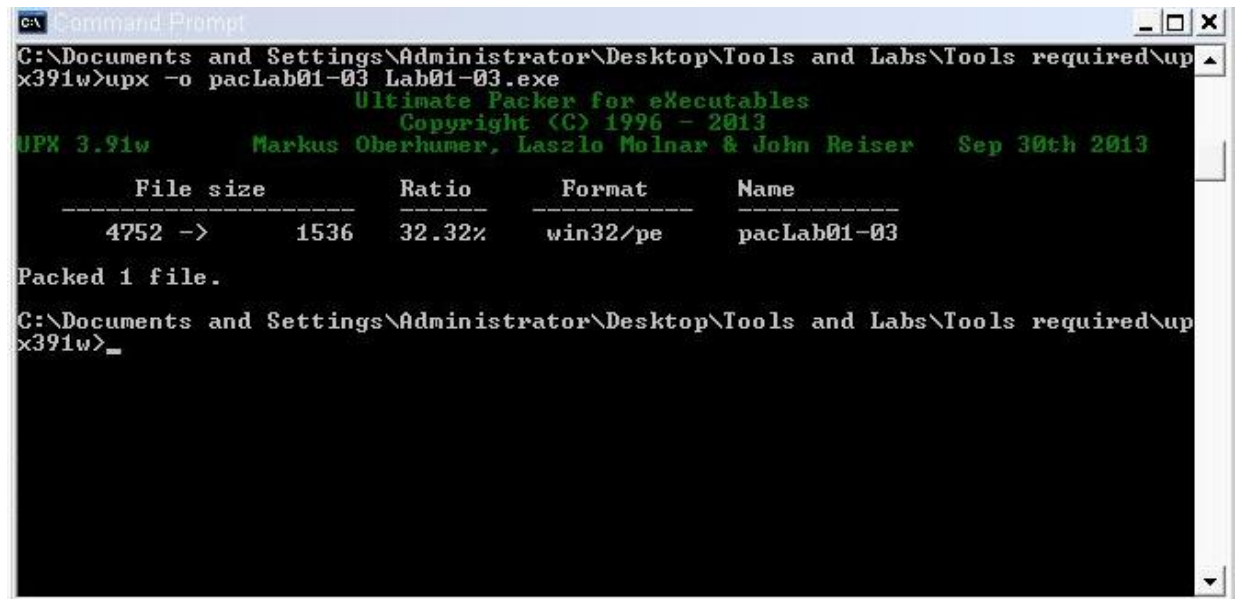
  File size   Ratio   Format   Name
-----
upx: Lab01-02.exe: AlreadyPackedException: already packed by UPX

Packed 1 file: 0 ok, 1 error.

C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Tools required\upx391w>
```

Figure 14 Lab01-2

### Lab 3:



```
C:\> Command Prompt
C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Tools required\up
x391w>upx -o pacLab01-03 Lab01-03.exe
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2013
UPX 3.91w Markus Oberhumer, Laszlo Molnar & John Reiser Sep 30th 2013

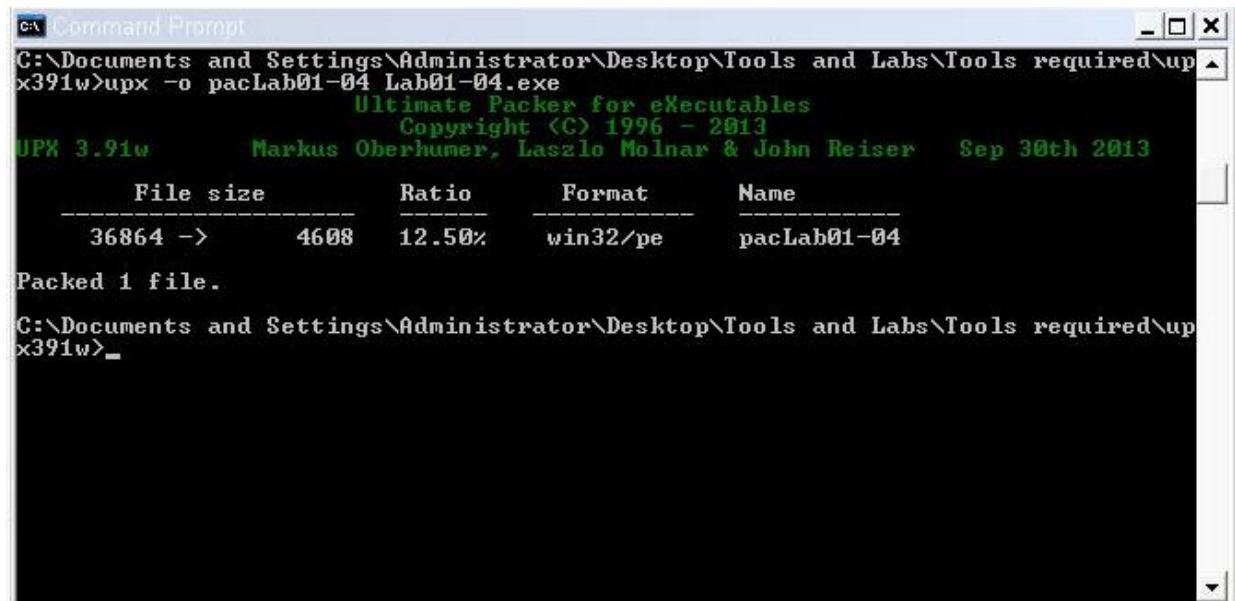
File size      Ratio      Format      Name
-----
4752 ->    1536    32.32%    win32/pe    pacLab01-03

Packed 1 file.

C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Tools required\up
x391w>_
```

Figure 15 Lab01-3

### Lab 4:



```
C:\> Command Prompt
C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Tools required\up
x391w>upx -o pacLab01-04 Lab01-04.exe
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2013
UPX 3.91w Markus Oberhumer, Laszlo Molnar & John Reiser Sep 30th 2013

File size      Ratio      Format      Name
-----
36864 ->    4608    12.50%    win32/pe    pacLab01-04

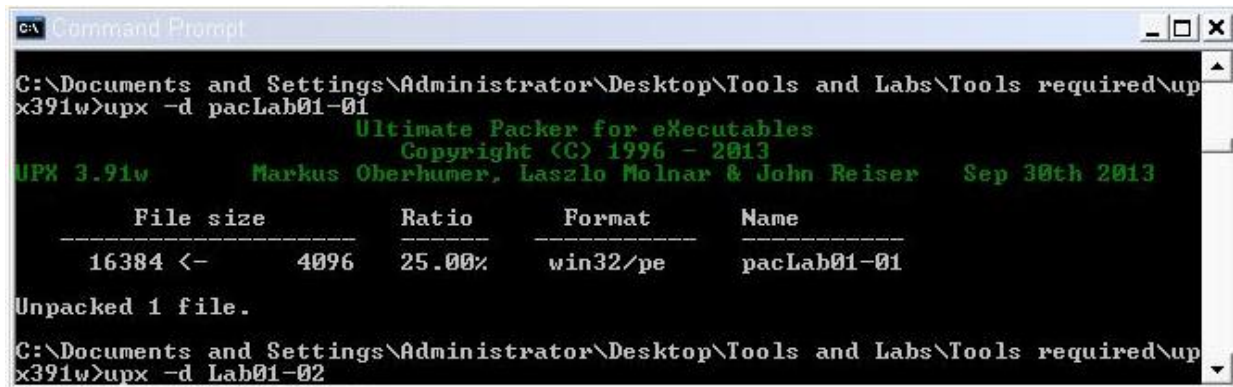
Packed 1 file.

C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Tools required\up
x391w>_
```

Figure 16 Lab01-4

## Uncompress

### Lab 1:



```
C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Tools required\upx391w>upx -d pacLab01-01
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2013
UPX 3.91w Markus Oberhumer, Laszlo Molnar & John Reiser Sep 30th 2013

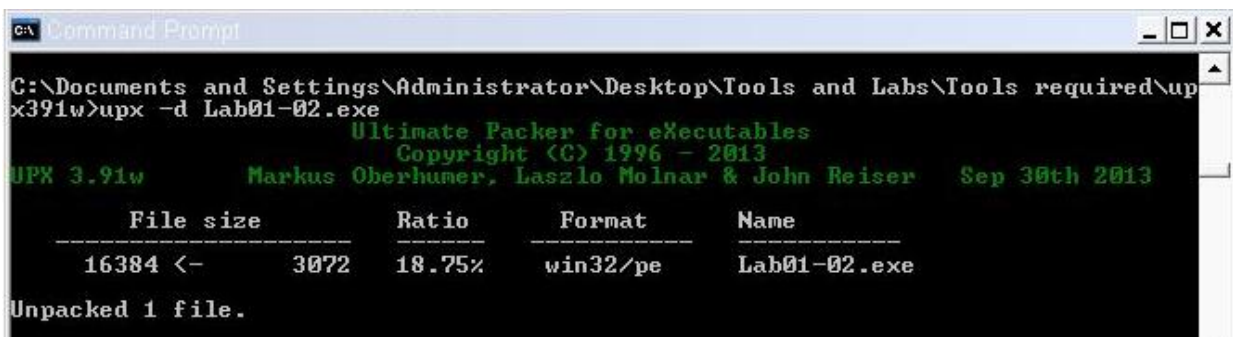
  File size      Ratio      Format      Name
  -----
  16384 <-      4096      25.00%      win32/pe      pacLab01-01

Unpacked 1 file.

C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Tools required\upx391w>upx -d Lab01-02
```

Figure 17 Lab01-1

### Lab 2:



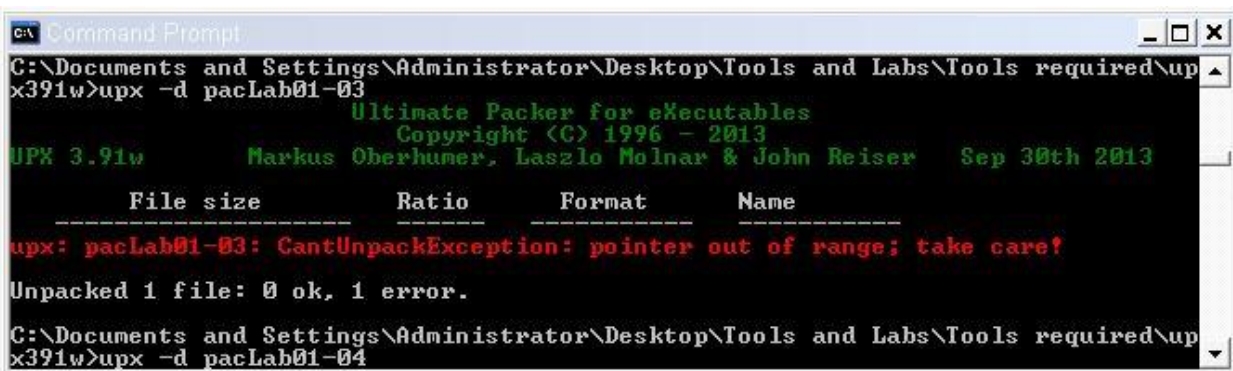
```
C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Tools required\upx391w>upx -d Lab01-02.exe
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2013
UPX 3.91w Markus Oberhumer, Laszlo Molnar & John Reiser Sep 30th 2013

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

Unpacked 1 file.
```

Figure 18 Lab01-2

### Lab 3:



```
C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Tools required\upx391w>upx -d pacLab01-03
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2013
UPX 3.91w Markus Oberhumer, Laszlo Molnar & John Reiser Sep 30th 2013

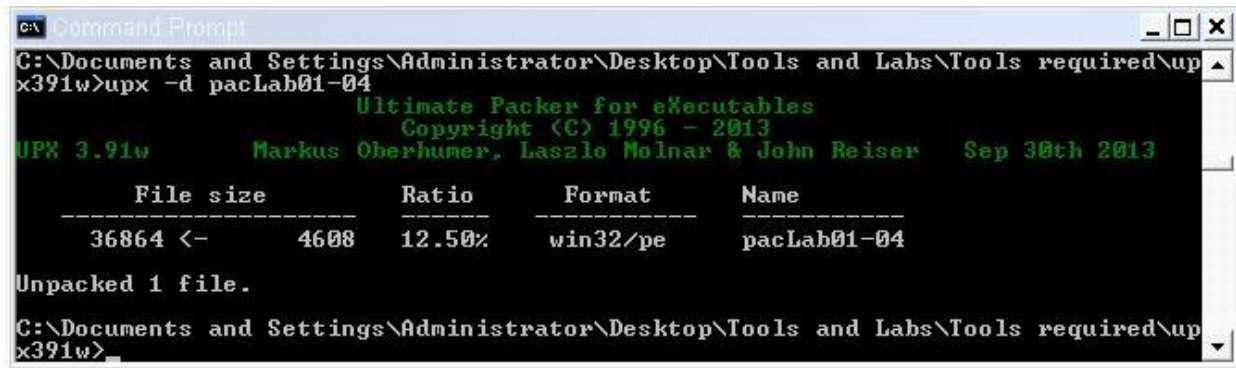
  File size      Ratio      Format      Name
  -----
upx: pacLab01-03: CantUnpackException: pointer out of range; take care!

Unpacked 1 file: 0 ok, 1 error.

C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Tools required\upx391w>upx -d pacLab01-04
```

Figure 19 Lab01-3

## Lab 4:



```
C:\ Command Prompt
C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Tools required\up
x391w>upx -d pacLab01-04
      Ultimate Packer for eXecutables
      Copyright (C) 1996 - 2013
UPX 3.91w      Markus Oberhumer, Laszlo Molnar & John Reiser      Sep 30th 2013

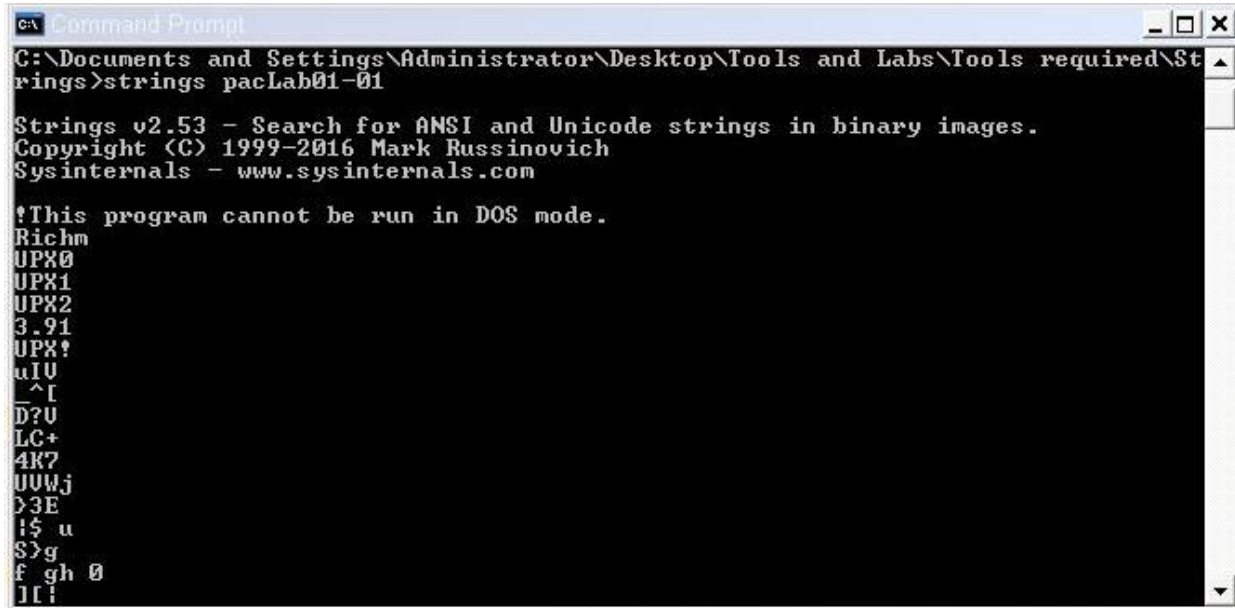
      File size      Ratio      Format      Name
      -----
      36864 <-      4608      12.50%      win32/pe      pacLab01-04

Unpacked 1 file.
C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Tools required\up
x391w>
```

Figure 20 Lab01-4

## Compressed Binaries Using Strings

### Lab 1:



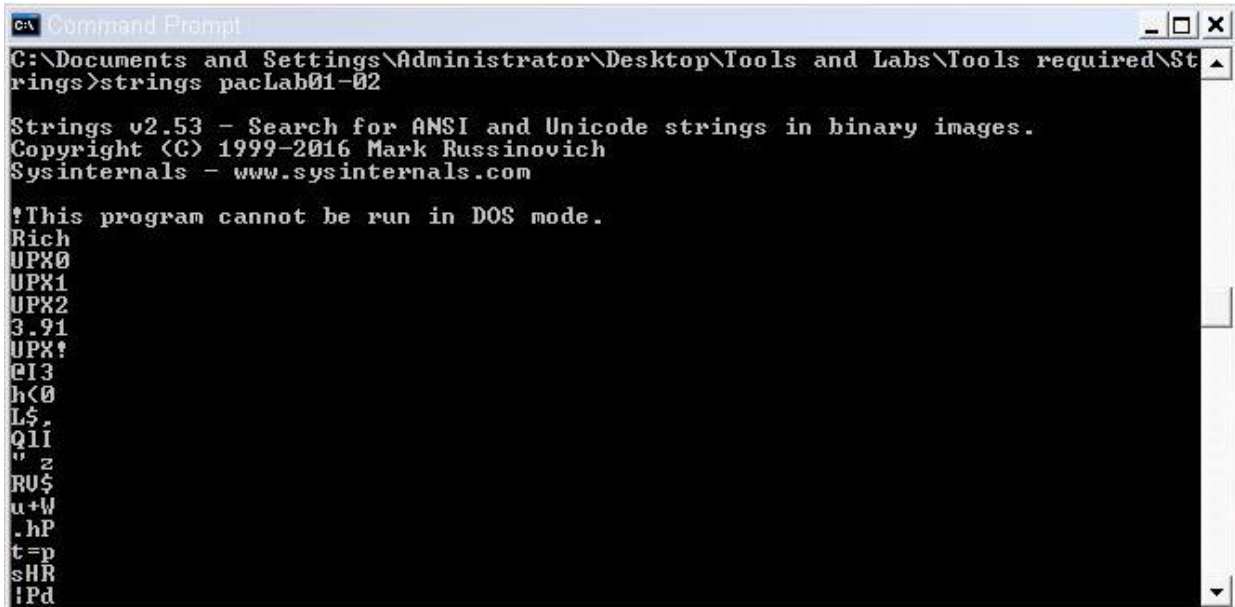
```
C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Tools required\Strings>strings paclab01-01

Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

!This program cannot be run in DOS mode.
Richm
UPX0
UPX1
UPX2
3.91
UPX!
uIU
^I
D?U
LC+
4K7
UUWj
D3E
i$ u
S>g
f gh 0
l[]
```

Figure 21 Lab01-1

### Lab 2:



```
C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Tools required\Strings>strings paclab01-02

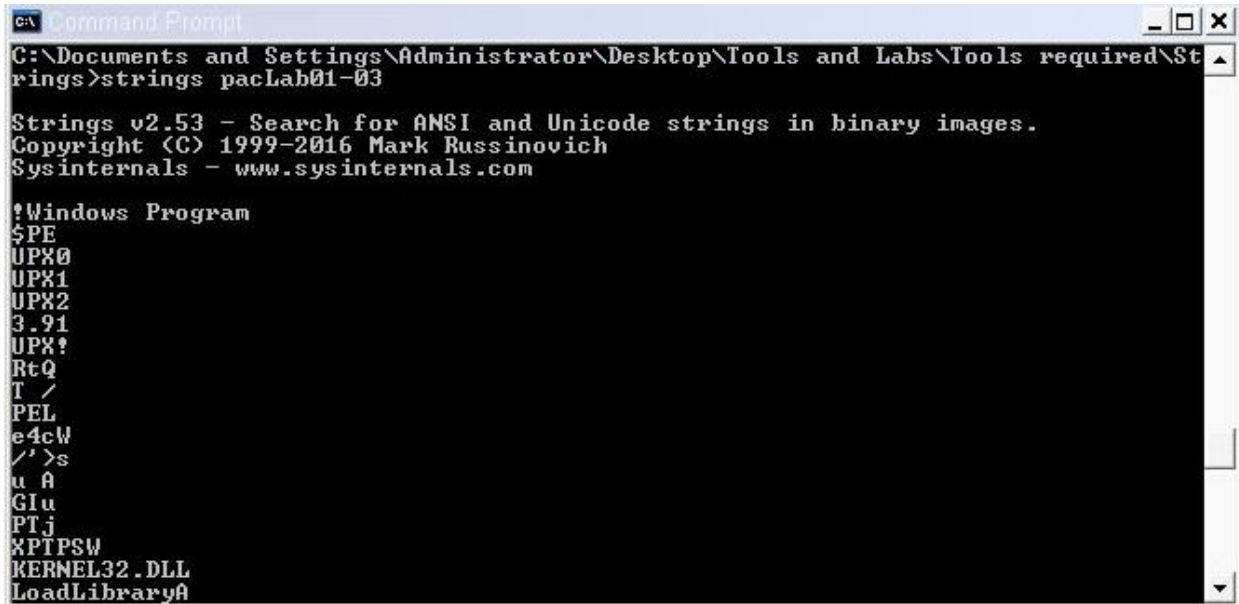
Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

!This program cannot be run in DOS mode.
Rich
UPX0
UPX1
UPX2
3.91
UPX!
e13
h<0
L$,
Q11
z
RU$
u+W
.hP
t=p
sHR
!Pd
```

Figure 22 Lab01-2



### Lab 3:



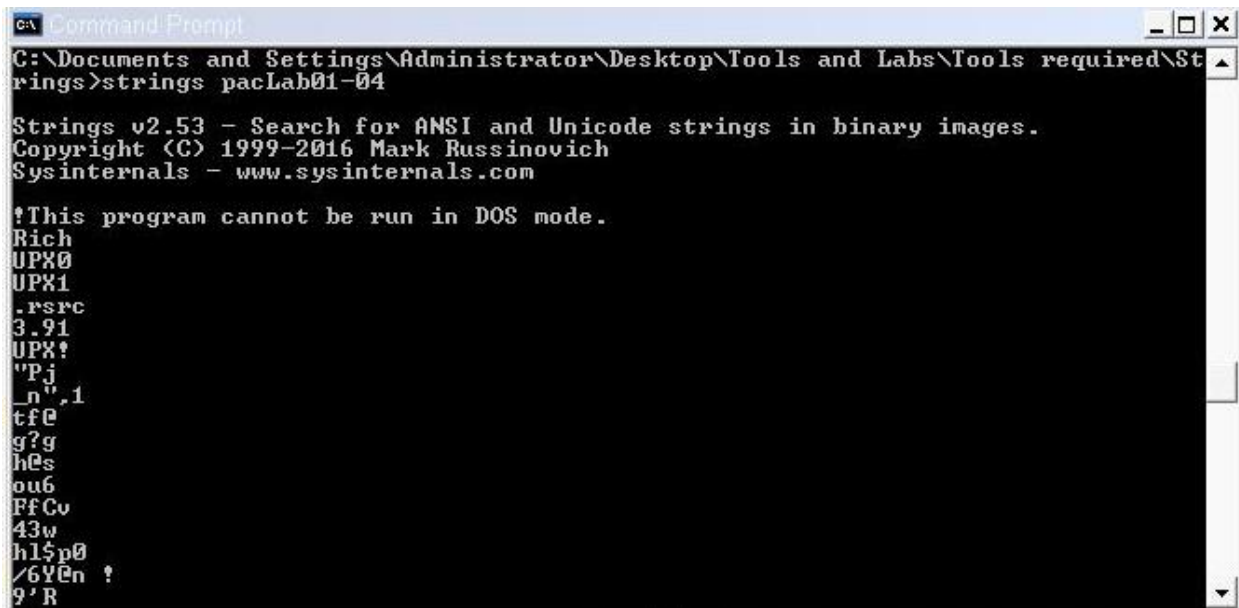
```
C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Tools required\Strings>strings pacLab01-03

Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

!Windows Program
$PE
UPX0
UPX1
UPX2
3.91
UPX!
RtQ
T /
PEL
e4cW
/'>s
u A
Glu
PTj
XPTPSW
KERNEL32.DLL
LoadLibraryA
```

Figure 23 Lab01-3

### Lab 4:



```
C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Tools required\Strings>strings pacLab01-04

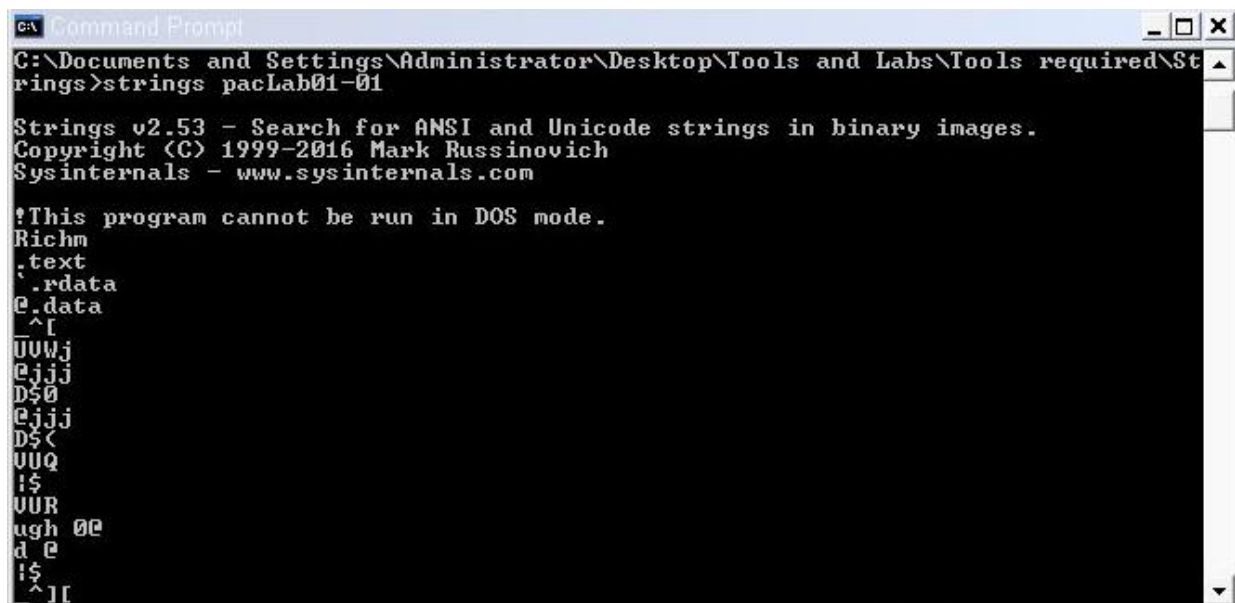
Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

!This program cannot be run in DOS mode.
Rich
UPX0
UPX1
.rsrc
3.91
UPX!
"Pj
_n",1
tfe
g?g
hes
ou6
FFCv
43w
h15p0
/6YEn ?
9'R
```

Figure 24 Lab01-4

## Uncompressed Binaries Using Strings

### Lab 1:



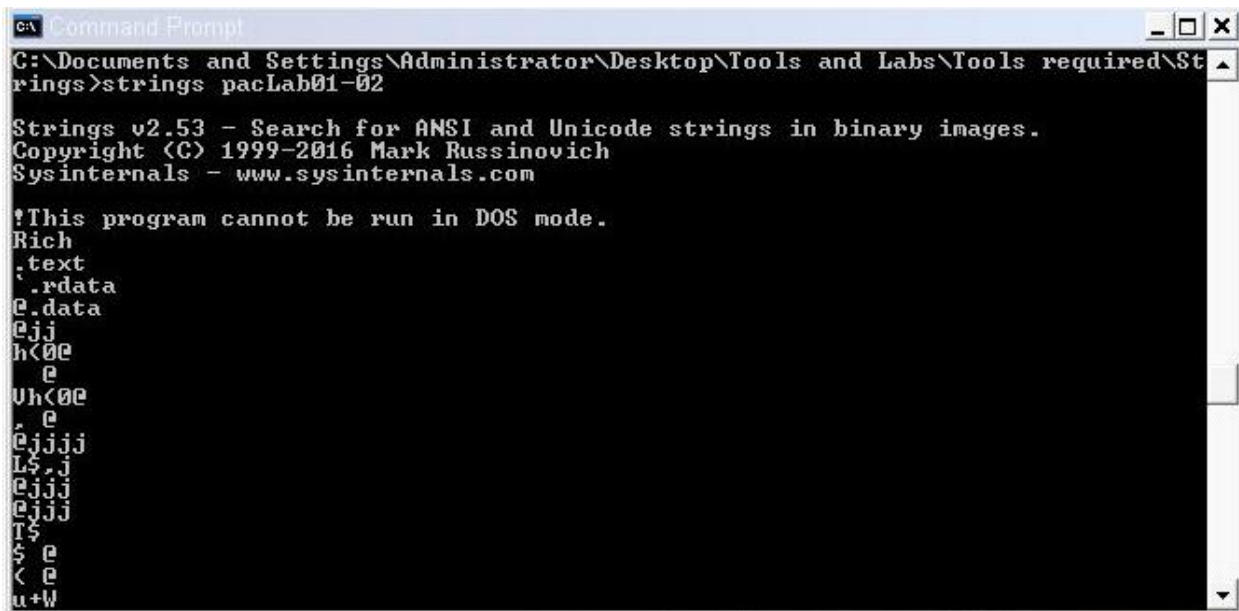
```
C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Tools required\Strings>strings pacLab01-01

Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

!This program cannot be run in DOS mode.
Richm
.text
.rdata
.data
^
UUWj
ejjj
D$0
ejjj
D$<
UUQ
I$
UUR
ugh 00
d e
I$
^
^
```

Figure 25 Lab01-1

### Lab 2:



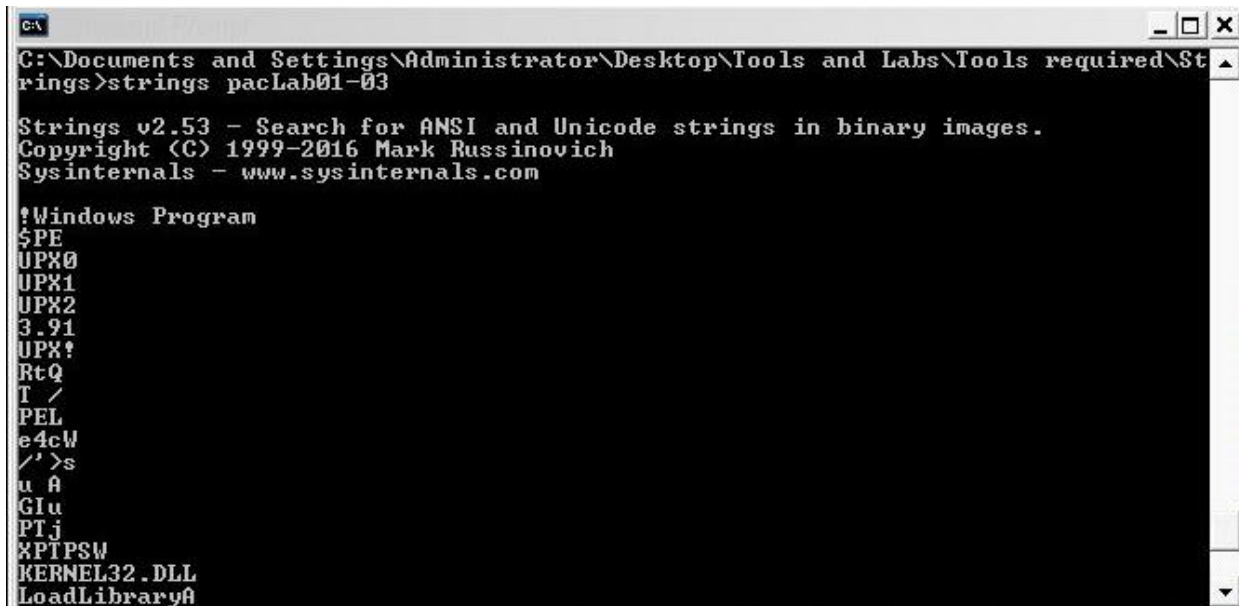
```
C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Tools required\Strings>strings pacLab01-02

Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

!This program cannot be run in DOS mode.
Rich
.text
.rdata
.data
ejj
h<00
e
Uh<00
e
ejjjj
L$.j
ejjj
ejjj
I$
$.e
< e
u+W
```

Figure 26 Lab01-2

### Lab 3:



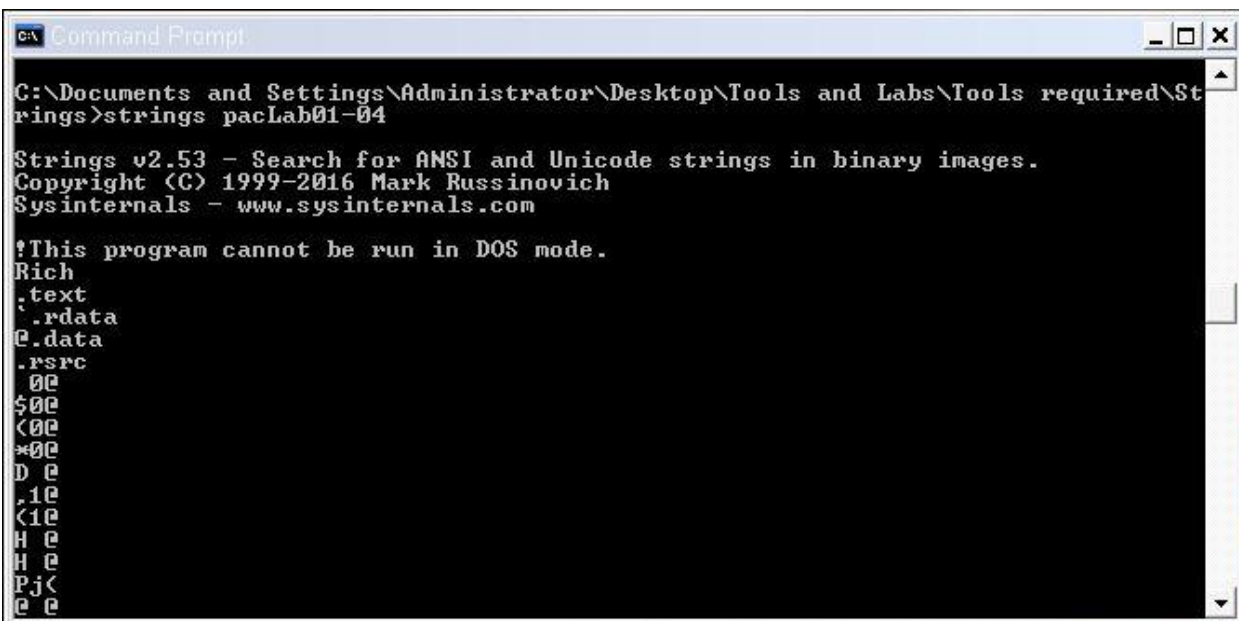
```
C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Tools required\Strings>strings pacLab01-03

Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

!Windows Program
$PE
UPX0
UPX1
UPX2
3.91
UPX!
RtQ
T /
PEL
e4cW
/>s
u A
GIu
PTj
XPTPSW
KERNEL32.DLL
LoadLibraryA
```

Figure 27 Lab01-3

### Lab 4:



```
C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Tools required\Strings>strings pacLab01-04

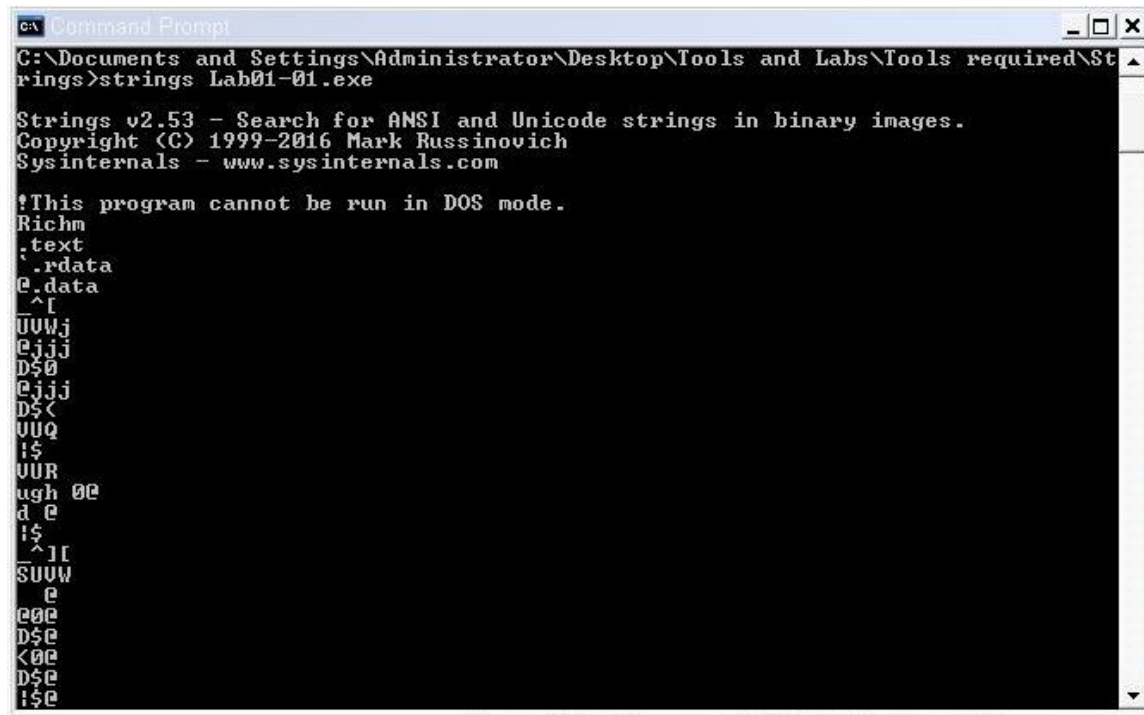
Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

!This program cannot be run in DOS mode.
Rich
.text
.rdata
.data
.rsrc
000
$000
<000
*000
D 0
,10
<10
H 0
H 0
Pj<
0 0
```

Figure 28 Lab01-4

## Original Binaries Using Strings

### Lab 1:

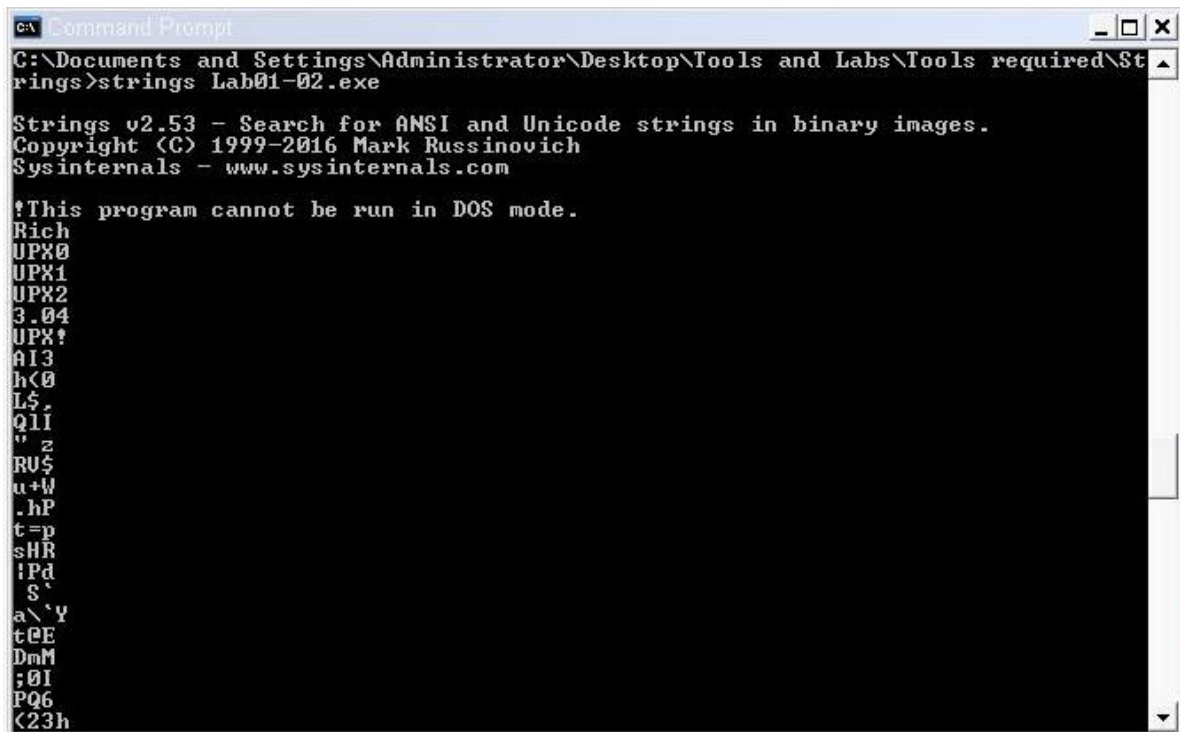


```
C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Tools required\Strings>strings Lab01-01.exe

Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

!This program cannot be run in DOS mode.
Richm
.text
.rdata
.data
^I
UUWj
ejjj
D$0
ejjj
D$<
UUQ
!$
UUR
ugh 00
d 0
!$
^I
SUUV
0
000
D$0
<00
D$0
!$0
```

### Lab 2:

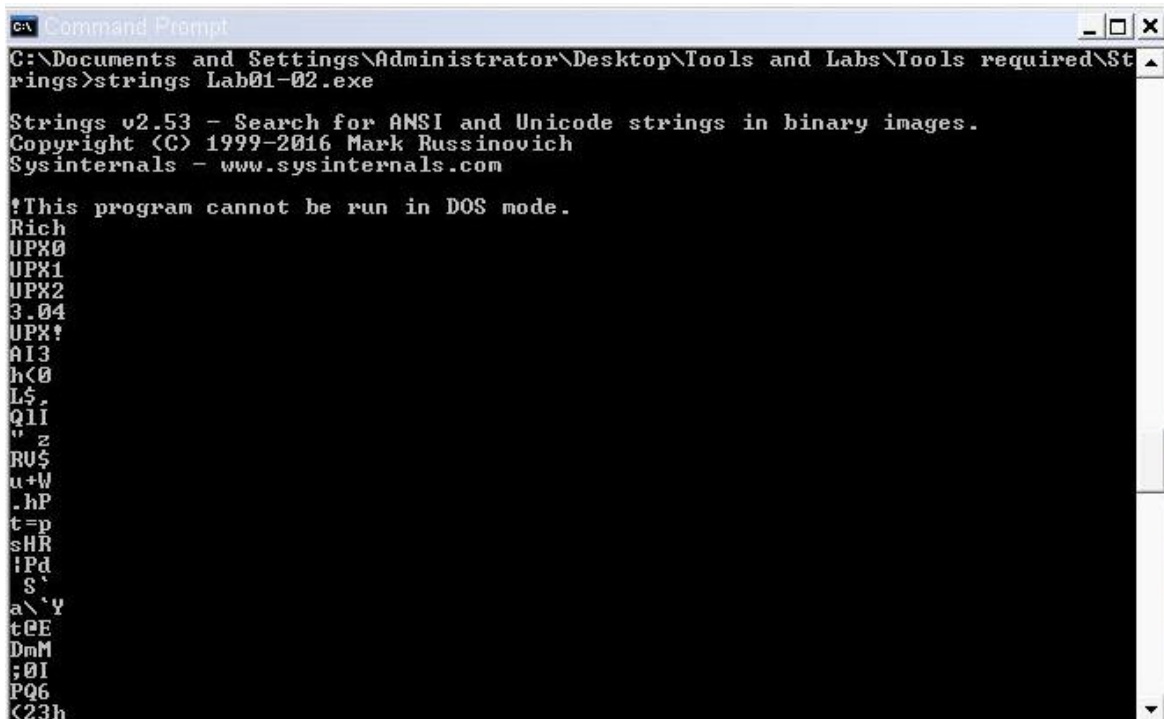


```
C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Tools required\Strings>strings Lab01-02.exe

Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

!This program cannot be run in DOS mode.
Rich
UPX0
UPX1
UPX2
3.04
UPX!
AI3
h<0
L$.
Q1I
" z
RU$
u+w
.hP
t=p
sHR
iPd
S`
a\`Y
t0E
DmM
;0I
PQ6
<23h
```

### Lab 3:

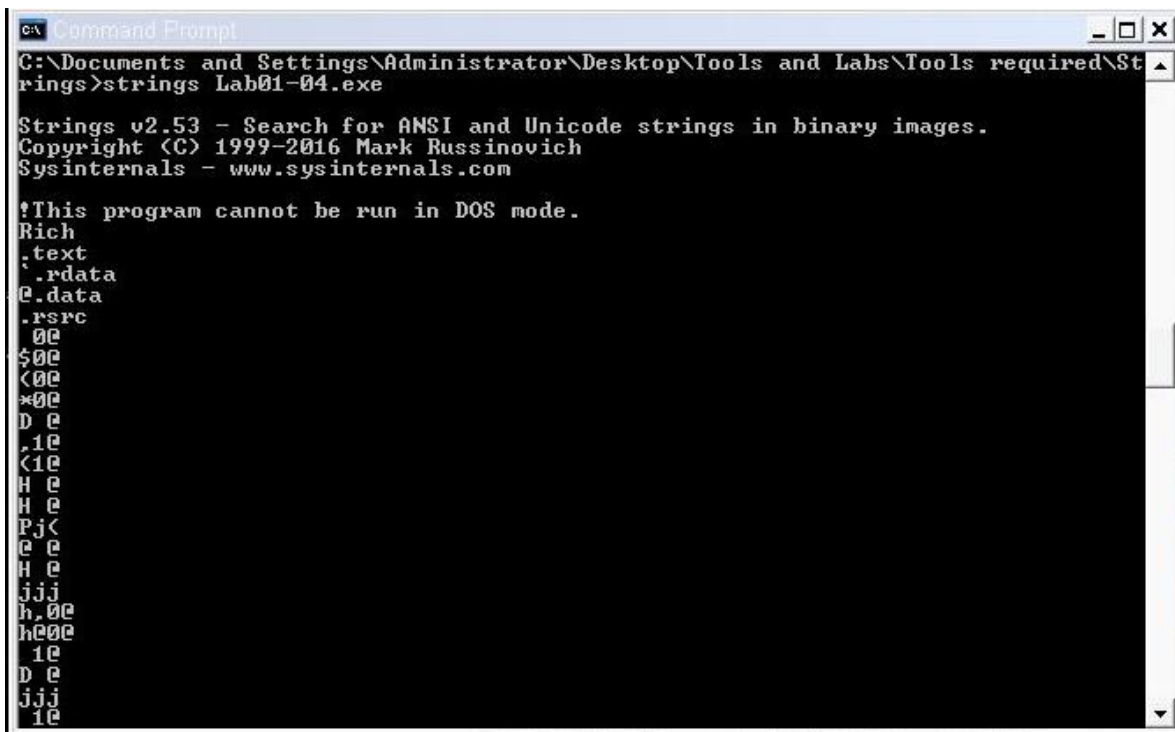


```
C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Tools required\Strings>strings Lab01-02.exe

Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

!This program cannot be run in DOS mode.
Rich
UPX0
UPX1
UPX2
3.04
UPX!
a13
h<0
L$.
Q11
" z
RU$
u+W
.hP
t=p
sHR
!Pd
!S`
a\`Y
tEE
DmM
;0I
PQ6
<23h
```

### Lab 4:



```
C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Tools required\Strings>strings Lab01-04.exe

Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

!This program cannot be run in DOS mode.
Rich
.text
.rdata
.e.data
.rsrc
00e
$00e
<00e
*00e
D 0e
.1e
<1e
H 0e
H 0e
Pj<
e 0e
H 0e
jjj
h,00e
h00e
1e
D 0e
jjj
1e
```