Malware Analysis Report

1 EXECUTIVE SUMMARY

After the analysis of the given binary that is Tnnbtib.exe

Therefore its is an infected file.

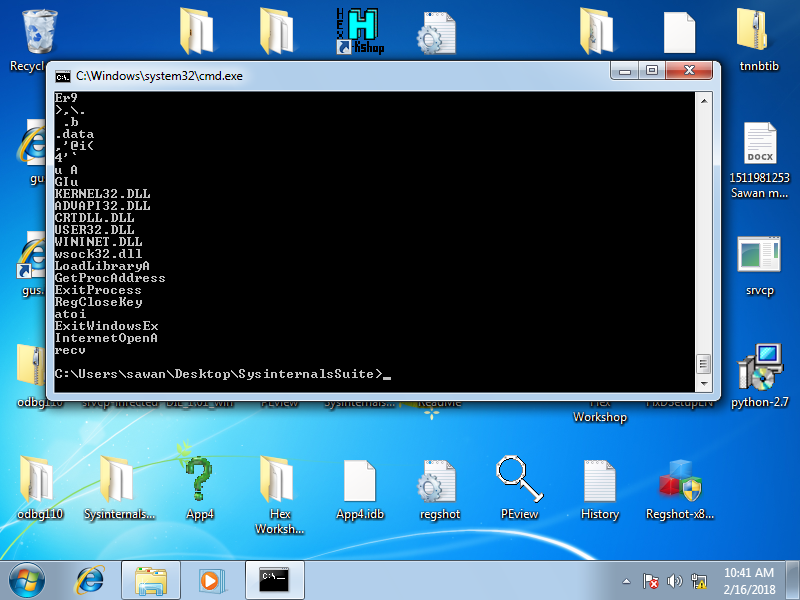
Name of file to be analysed: Tnnbtib.exe

* 1. STAGE 1: ANALYSIS OF THE ATTACHMENTS
  2. Static analysis of the file->

Strings analysis->

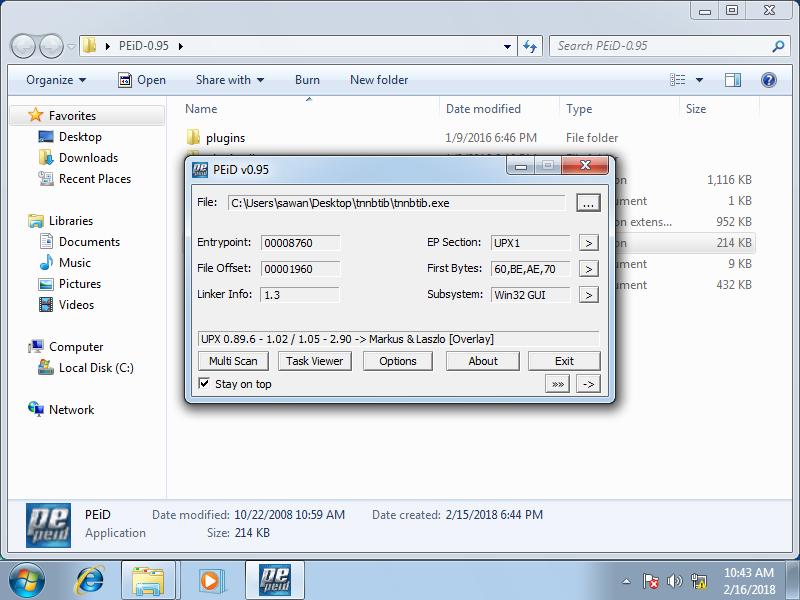


When I performed strings analysis to find the texts in the given file it shows us that it has ability to shutdown our system.

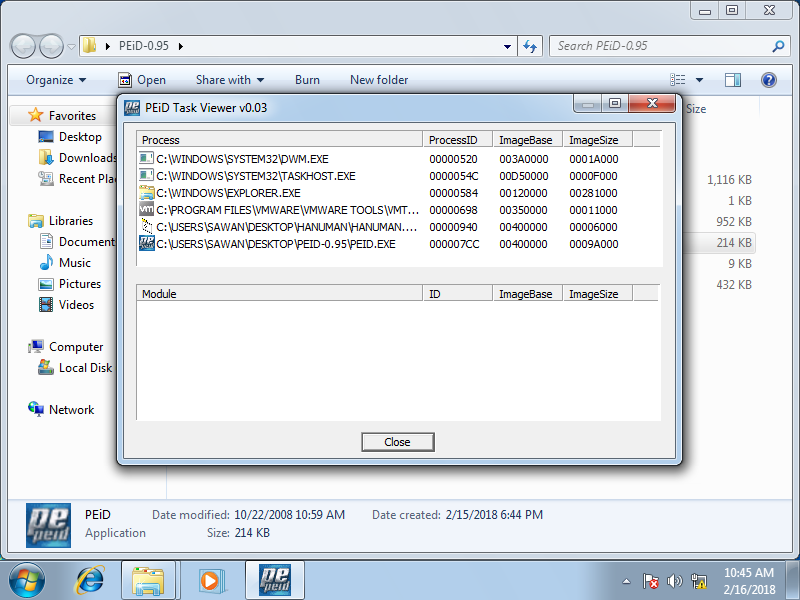


In strings it is also showing us that it is accessing the given dll files and accessing internet.

## PEid analysis->

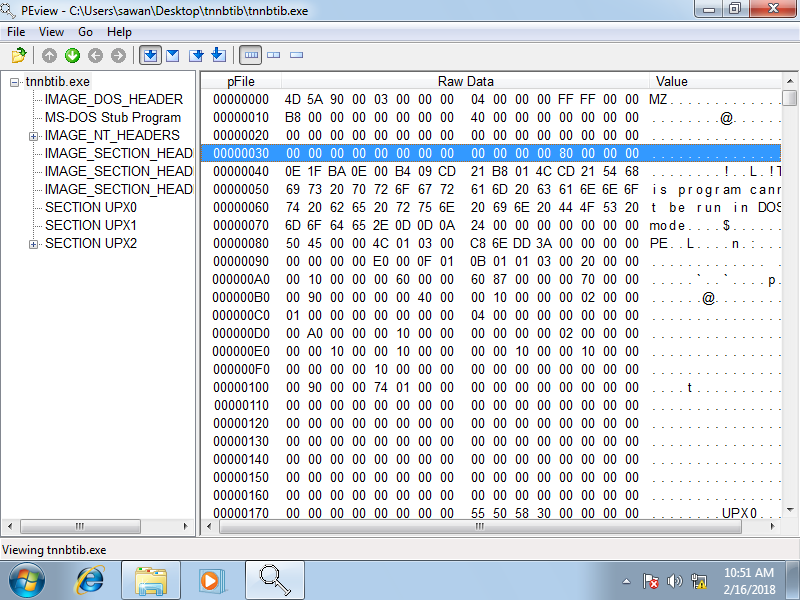


When we performed PEid analysis it is showing us the entry point address and the address of EP section, file offset value and the first bytes of the file.

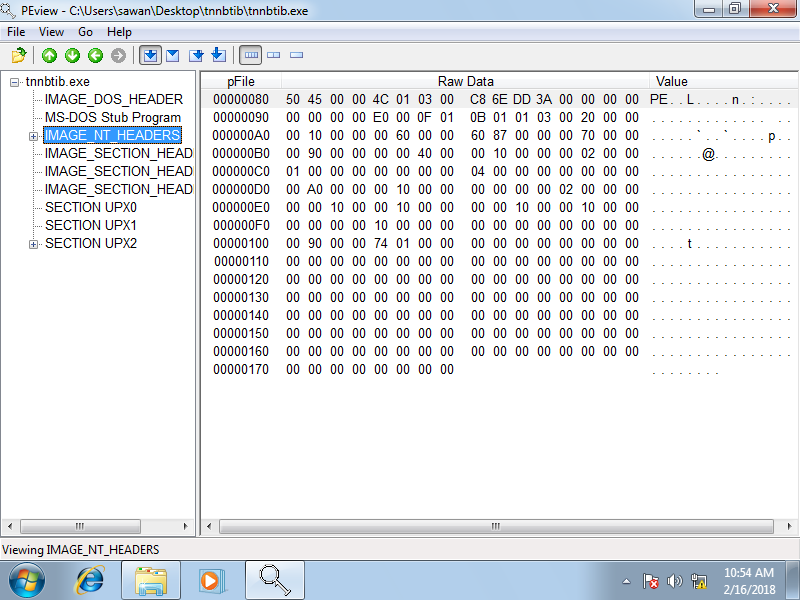


In this task viewer of PEid it is showing the path where the current file is being used and the image base,image size of the binary.

PEview analysis->



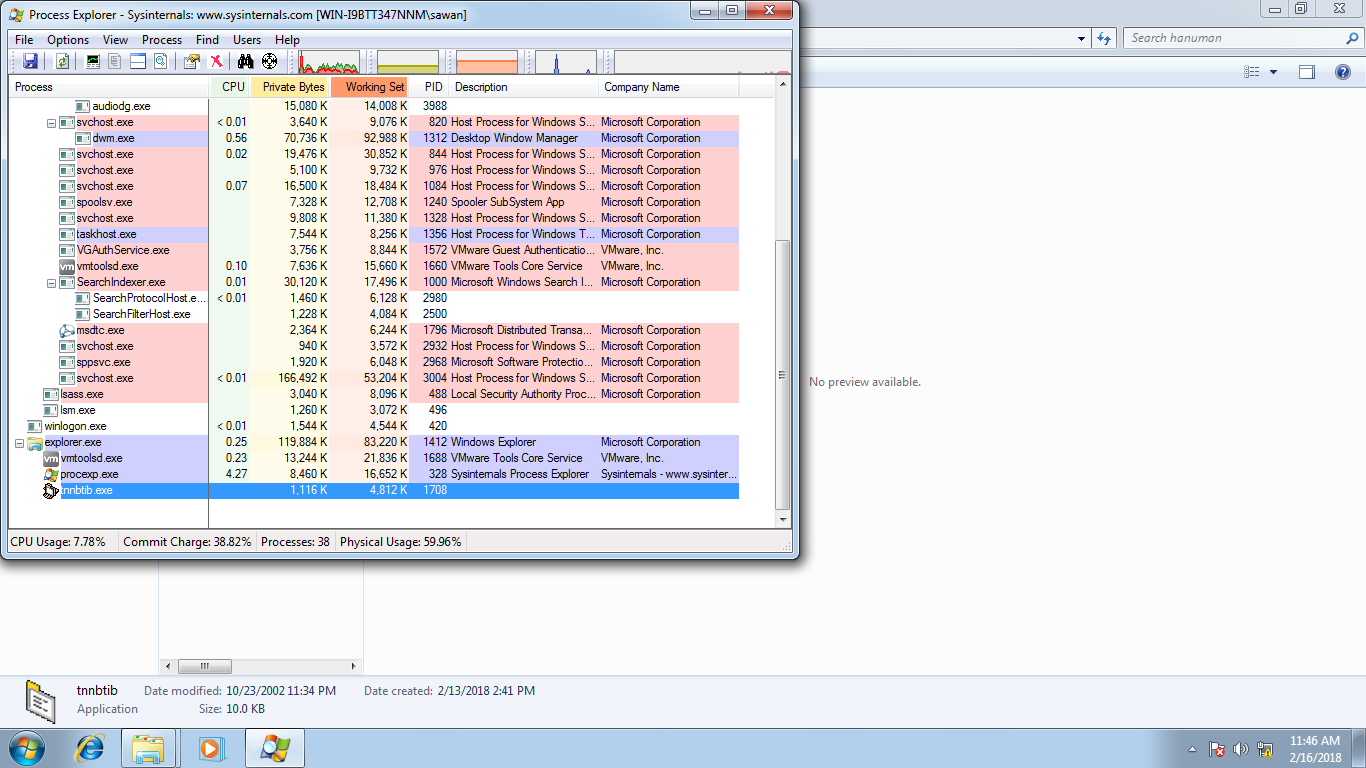
In the selected section the number 80 shows that the execution of the file starts at the pFile 80 value.



Here is the full view of the raw data and the pFile 80 where the execution of the file is being started.

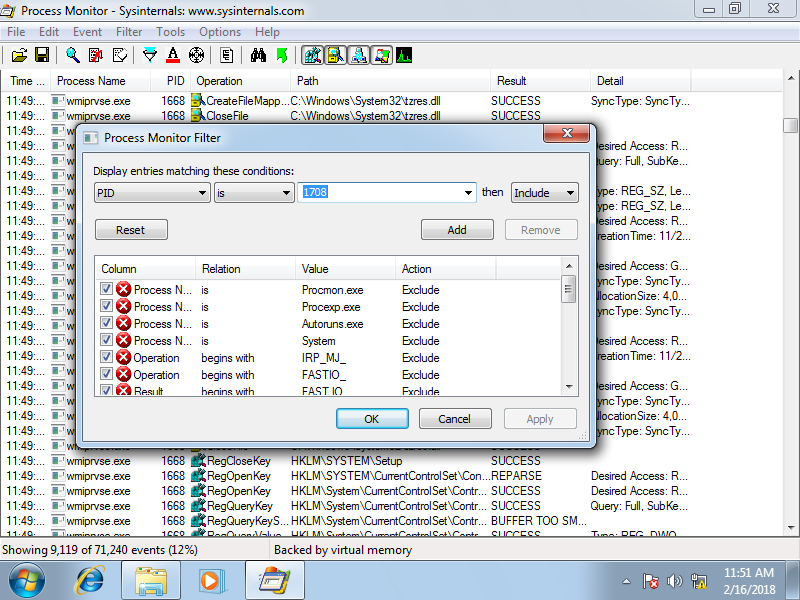
* 1. Dynamic analysis->

Process explorer



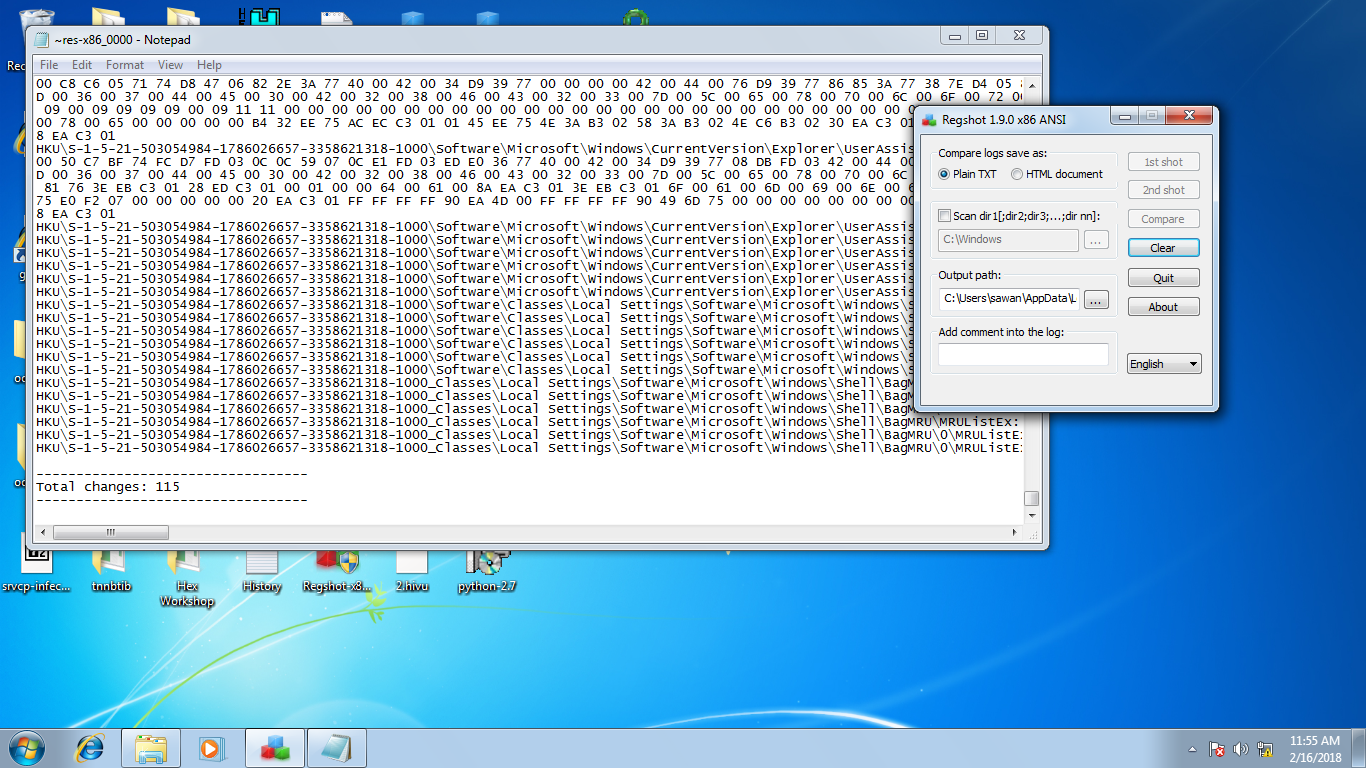
After running in process explorer we get to know about the PID of the given binary file.

Process monitor



In this we will use the filter by pid to monitor the process.

REGSHOT

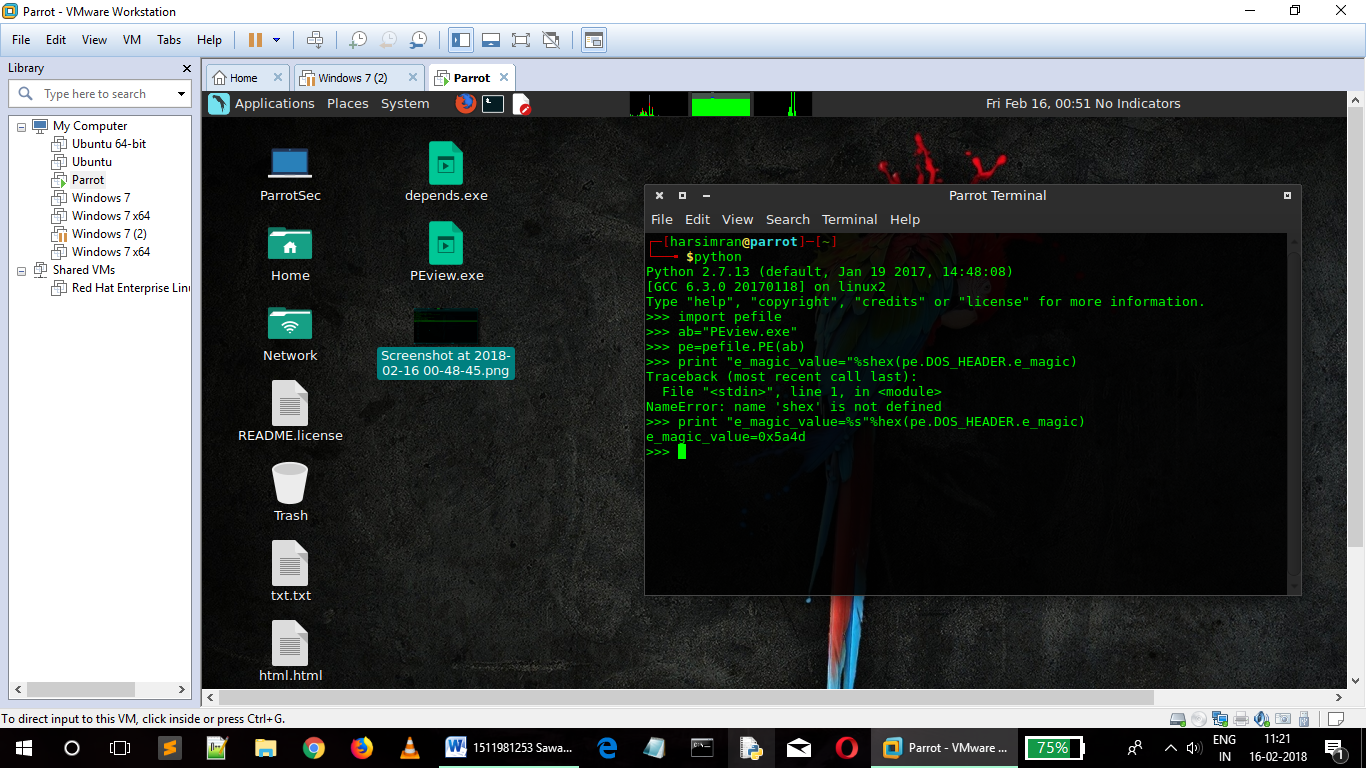


In this first we took shot without executing the binary and then 2nd shot after executing the binary and then we hit compare tab in the regshot and analysed that there are 115 changes in our system after the execution of the binary file.

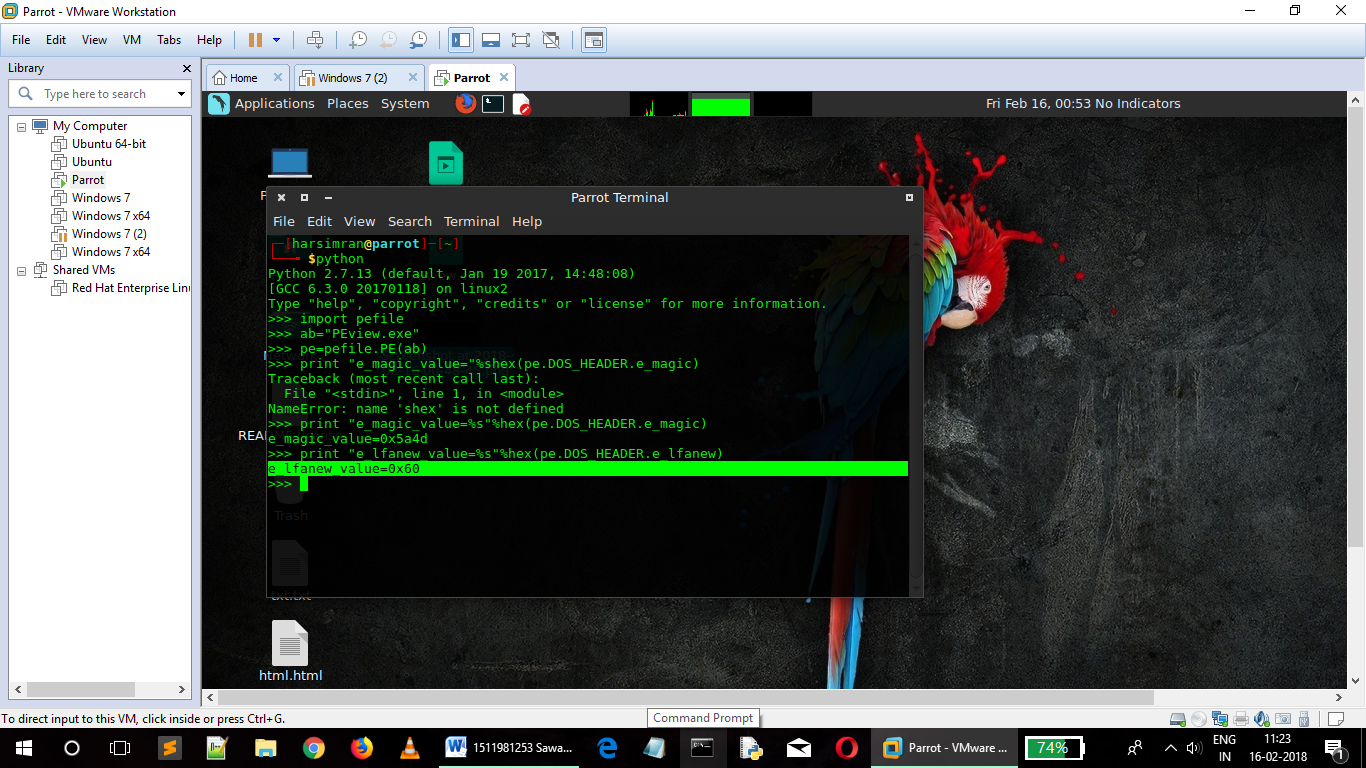
==========================================================

QUESTION2

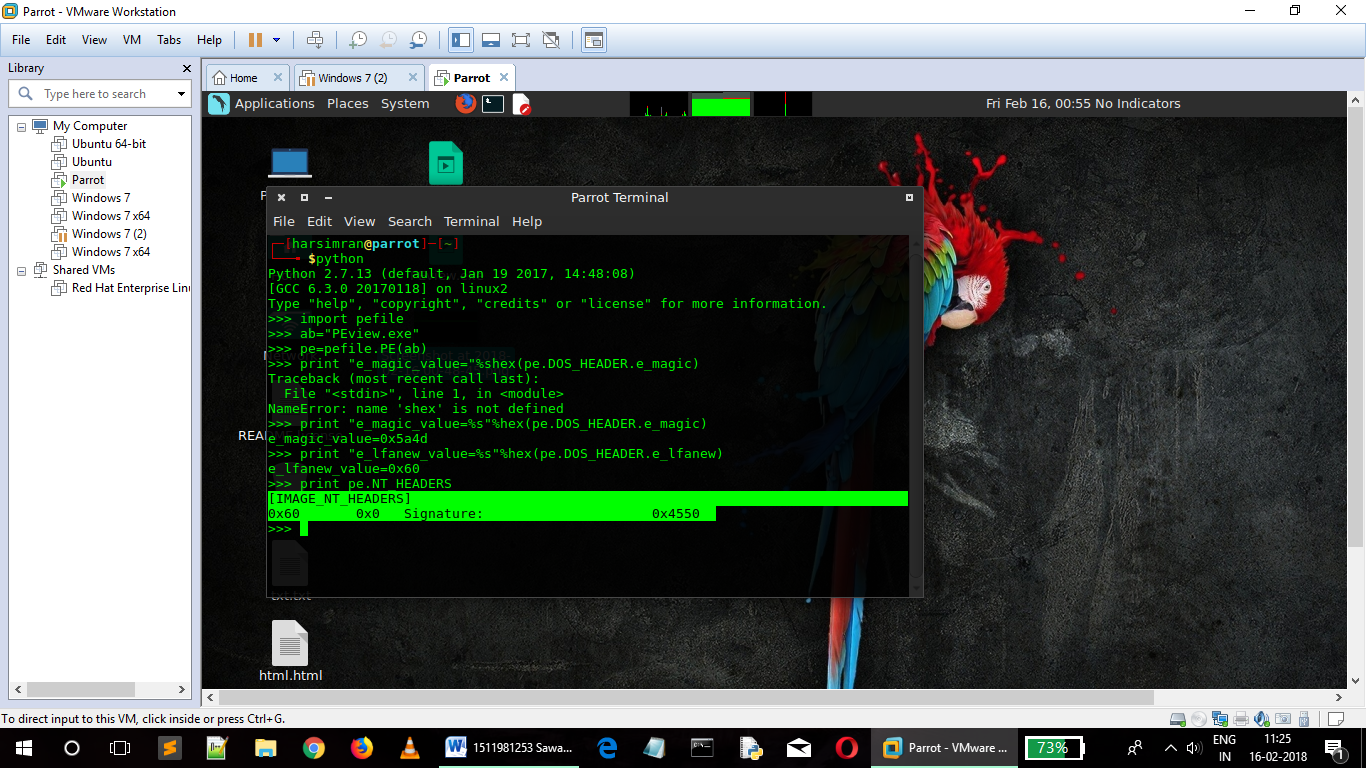
1. E\_magic



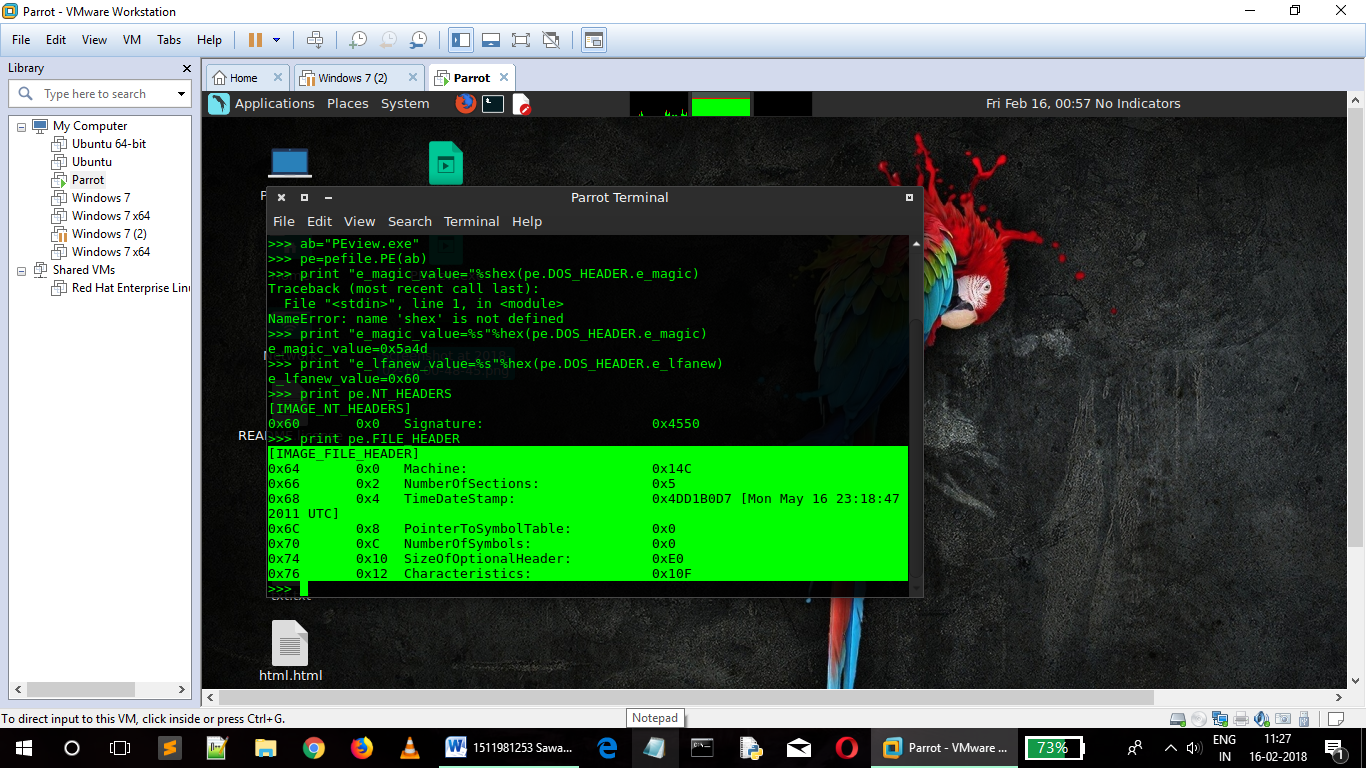
b)e\_lfanew



c)image nt headers



d)file header



Python program:

import pefile

ab=”Peview.exe”

pe=pefile.PE(ab)

print “e\_magic\_value=%s”%hex(pe.DOS\_HEADER.e\_magic)

print “e\_lfanew\_value=%s”%hex(pe.DOS\_HEADER.e\_lfanew)

print pe.FILE\_HEADER

for section in pe.section:

print “\t”+section.name

print pe.section[0]

==================================================

QUESTION 3:

.data

var1:

.asciz "Hello\n"

var2:

.asciz "welcome\n"

.text

.globl \_start

\_start:

.type Print,@function

Print:

movl $4,%eax

movl $1,%ebx

int $0x80

ret

\_start:

nop

#print Hword

movl $var1,%ecx

movl $6,%edx

call Print

#print Hword1

movl $var2,%ecx

movl $8,%edx

call Print

movl $1,%eax

movl $0,%ebx

int $0x80