**Experiment No: 4**

Student Name and Roll Number: Harshit Parashar/18CSU081

Semester /Section:5th semester/CS-V-CysA

Link to Code:

Date:03-09-2020

Faculty Signature:

Remarks:

**Objective**

Packer detection tool

**Program Outcome**

The students will learn how they can detect packed malware sample

**Problem Statement**

Automate detection of packed malware samples.

**Background Study:**

Packers are used to compress and/or encrypt executable to hide their internals from us. Packed pgm (compressed pgm) are a subset of obfuscated pgm (delay someone in understanding exactly what the code is doing, by renaming variables, etc). Whenever we talk about malware analysis it is important to discuss about Packers. A protection mechanism commonly used by malware. Packers were actually created in old days to save network bandwidth and speedily transmit the file over the network. It compresses the executable to reduce its size. When the executable is run, it is uncompressed in memory. Many modern hackers encrypts the program in addition of compressing it to add security protection

**Algorithm/ flowchart**

**Code**

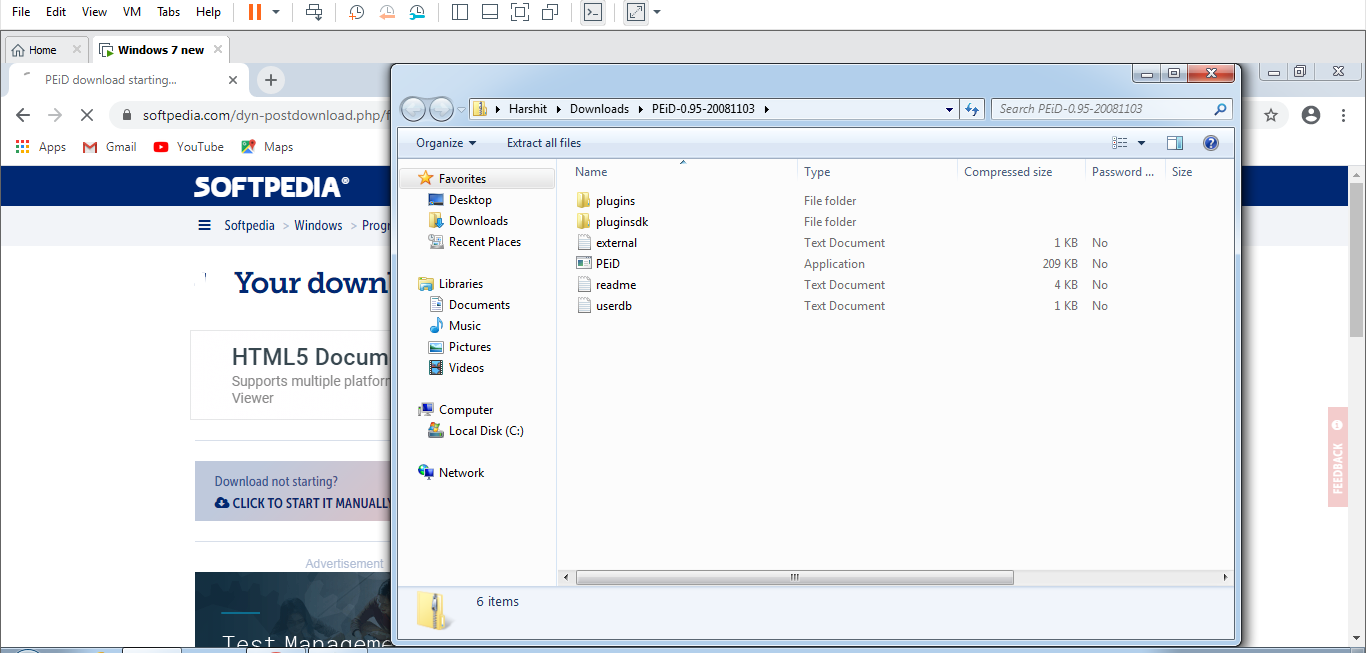
**Output: Screenshots**

**PEiD Tool**

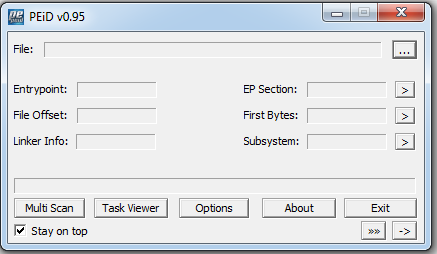
**STEP1#:Download the PEiD tool from source like softpedia.**



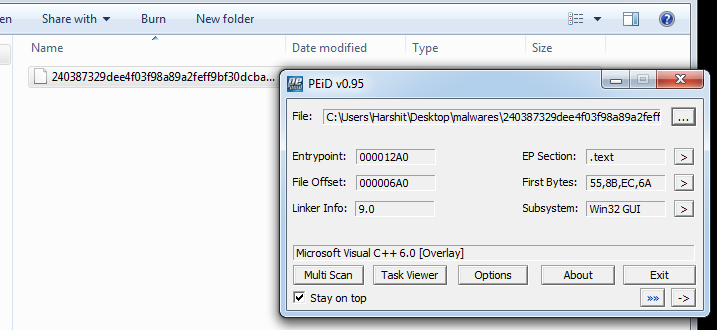
**STEP#2:After downloading the file Unzip the file .**

****

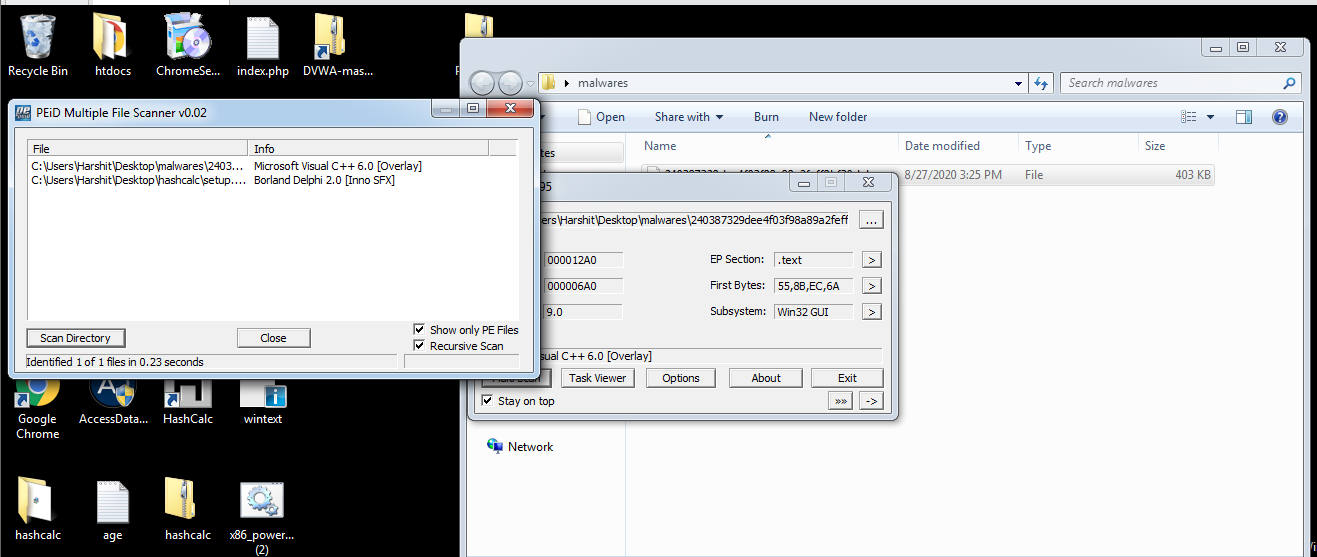
**STEP#3:Run the application.**



**STEP#4:Import/open the malware sample by drag and drop.**

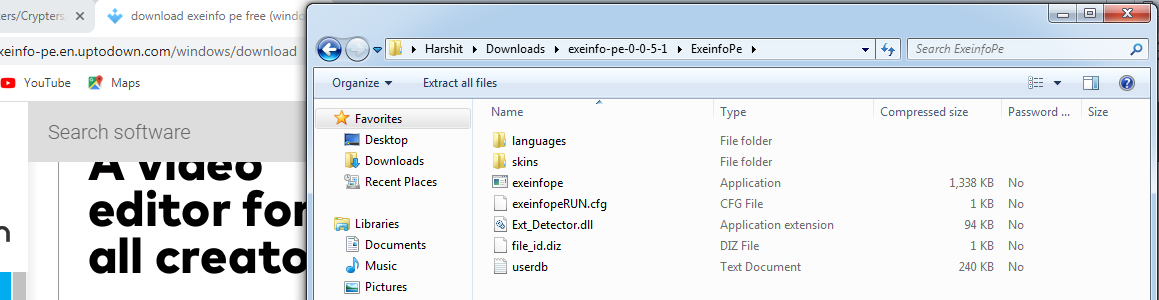


**STEP#5:A nalyze the sample it shows whether the file is unpacked or packed, along with other information.**

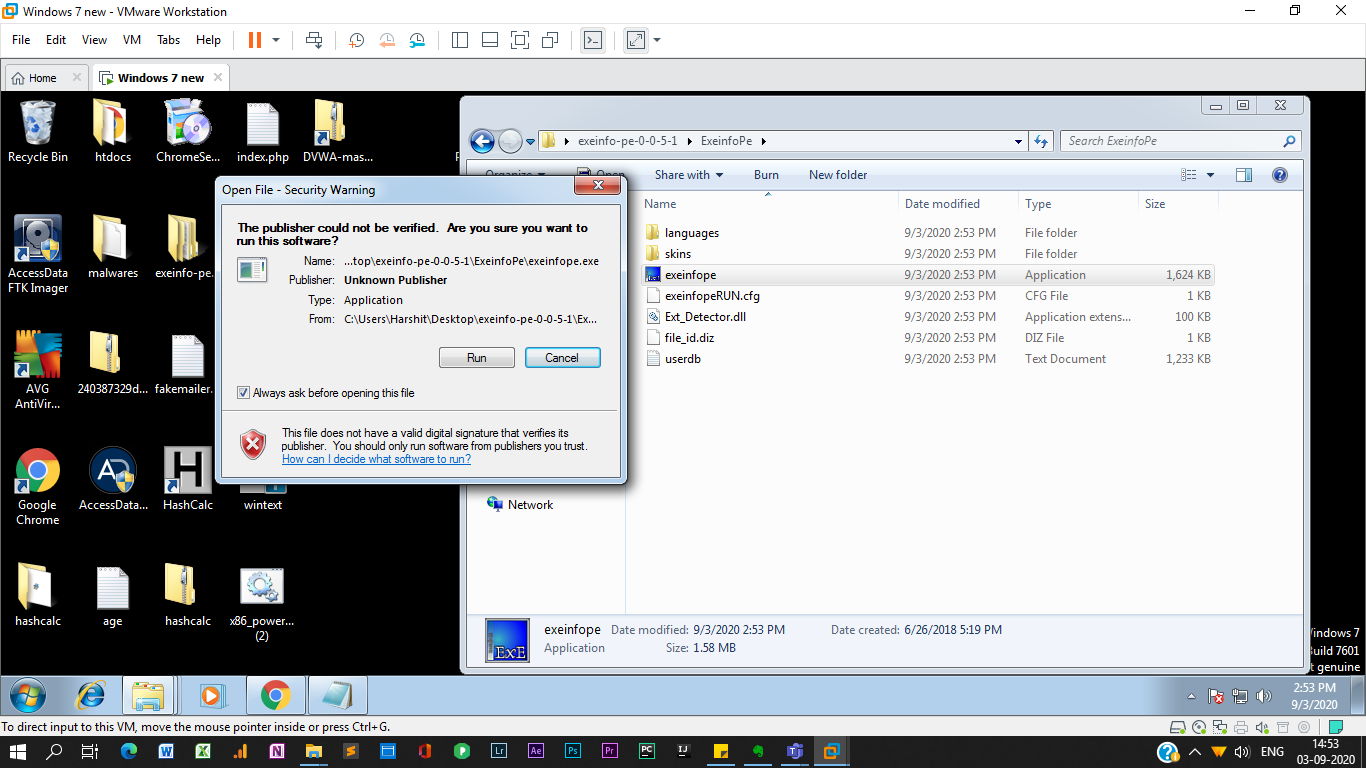


**ExeinfoPe Tool**

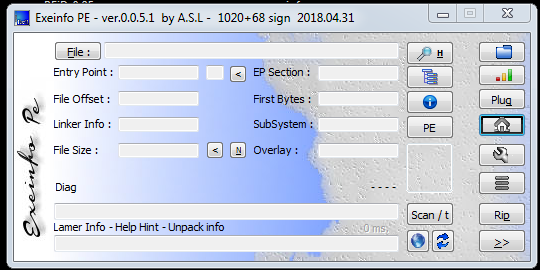
**STEP#1:Install the tool form the source uptodown.com**



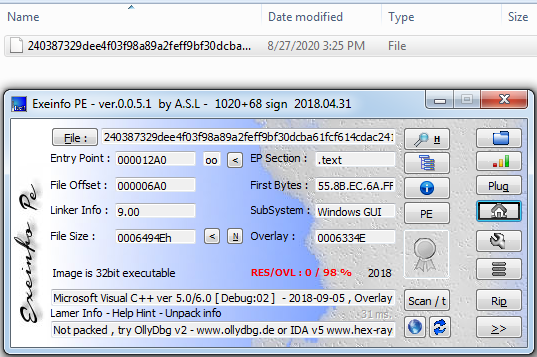
**STEP#2:Unzip the file .**

****

**STEP#3:Run the application**



**STEP#4:Open or drag and drop the malware sample in the application. And start analysing, it shows that the file is unpacked and various other details like file size.**



**Suggested Question Bank**

**Preparatory Questions**

1. Is there any easy way to split Packed and Unpacked PE file from an folder ?

Yes we can do in dynamic analysis, as we run the malware it will come to its original state, thereafter we can split the files.

2. Data masking is also known as \_\_\_\_\_\_\_\_\_

a) **Data obfuscation** is the answer

b) Data copying

c) Data breaching

d) Data duplicating

3. What is crypto malware?

It is a latest malware which has been found ,it requires only CPU cycle to do the best work,it is also called silent threat.

4. Write down the tools to detect to packed malware.

PEiD

TRiD

Exeinfo

5. Packed malware contains less number of strings in comparison to unpacked malware. justify your answer.

Yes packed malware contains less number of strings because while packing ,all the stings get zipped , and only remain string in the header,which seems less,while unpacking the file or executing,they transform themselves and come to original size.