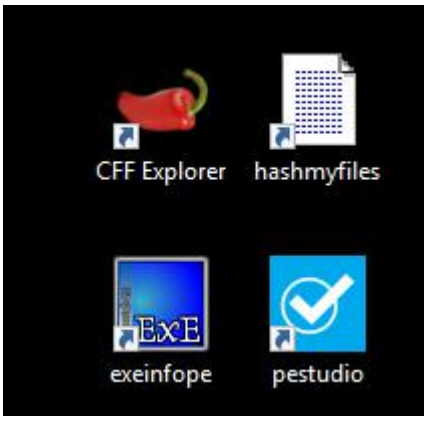
DIGITAL FORENSICS II
Experiment 10

Submitted to: Mr. Keshav Kaushik
Submitted by: Kashish Srivastava
500067405
R134218079

Aim: Pony Malware Analysis

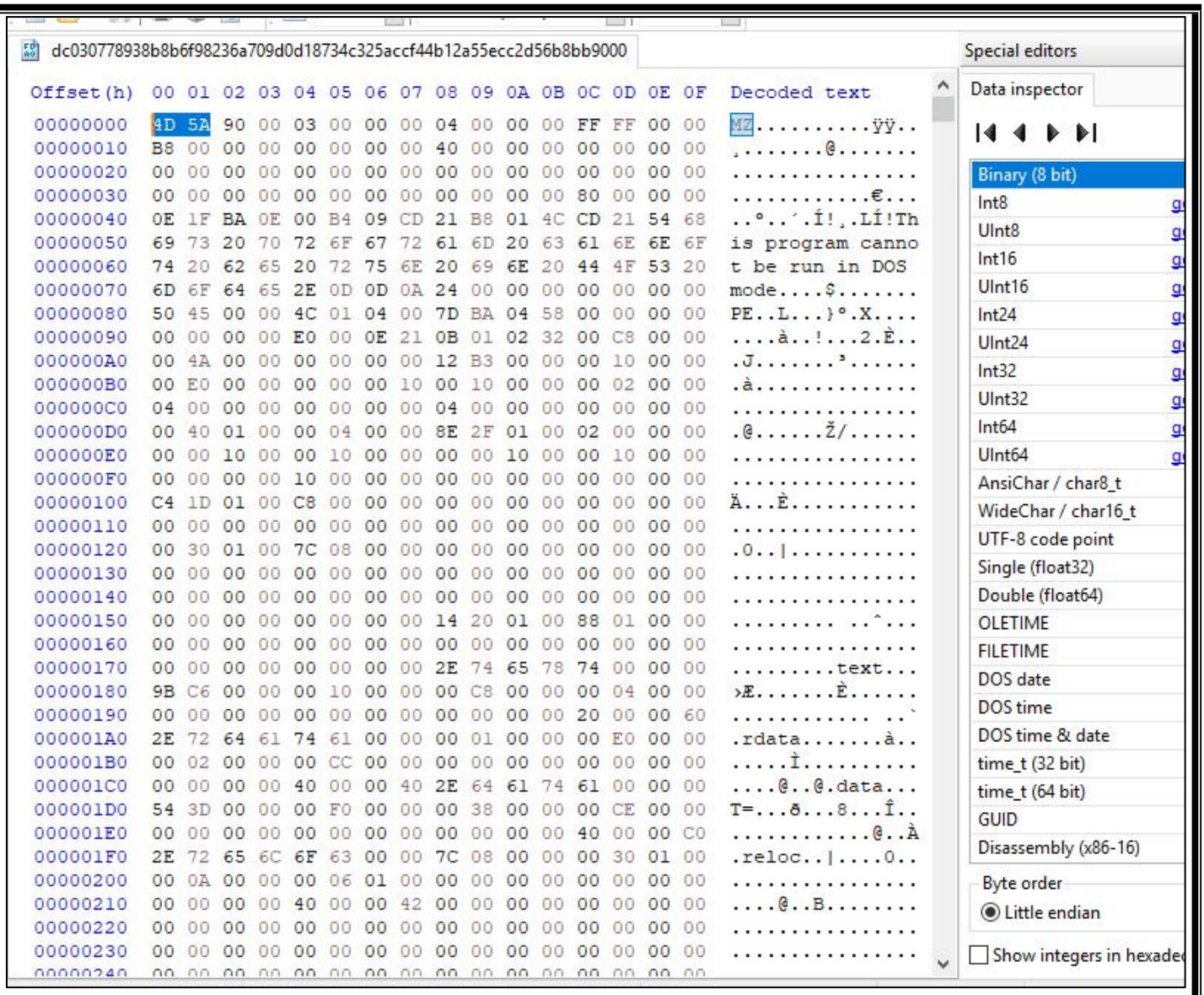
We are going to perform static malware analysis using exeinfo PE



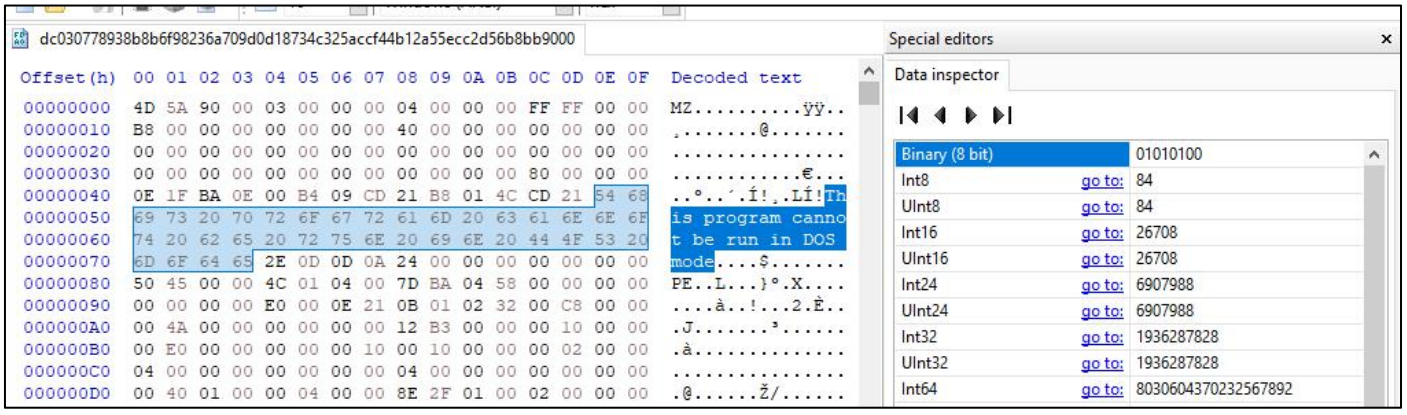
As we know the first step in Static analysis will be the **File type identification**, we will be doing this will a couple of tools, named as HxD, Exeinfo PE.

In this method we will be analysing the sample malware without executing or running it, we will be analysing the file in static condition, Extract as much of Data like strings, PE headers, etc.

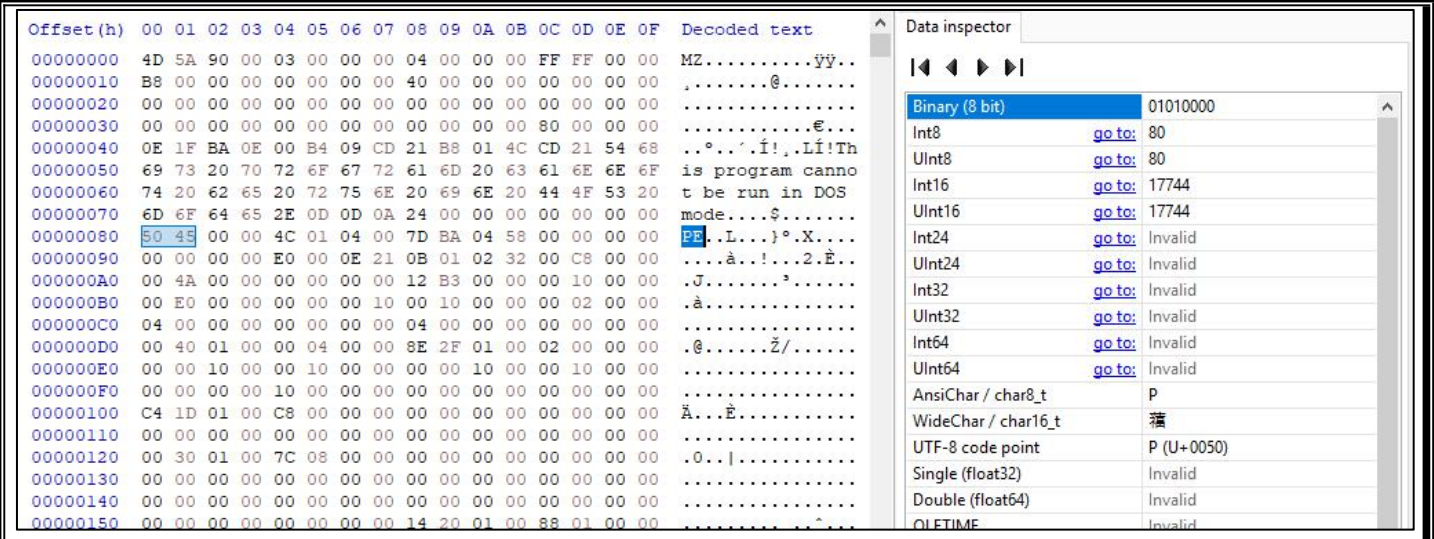
1. Identifying File type
2. Generating Hash
3. Strings
4. Packing & obfuscation
5. PEHeaders



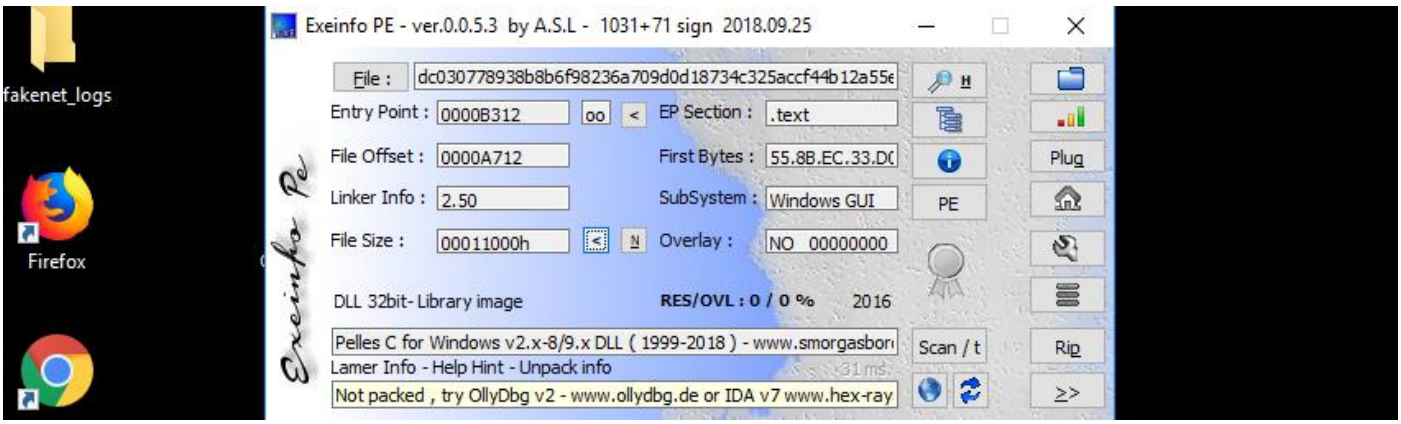
The first two bytes of the malware are 4D 5A which proves it is a PE file.
we can clearly see the Header text contains a string saying **“This program cannot be run in DOS mode”**.

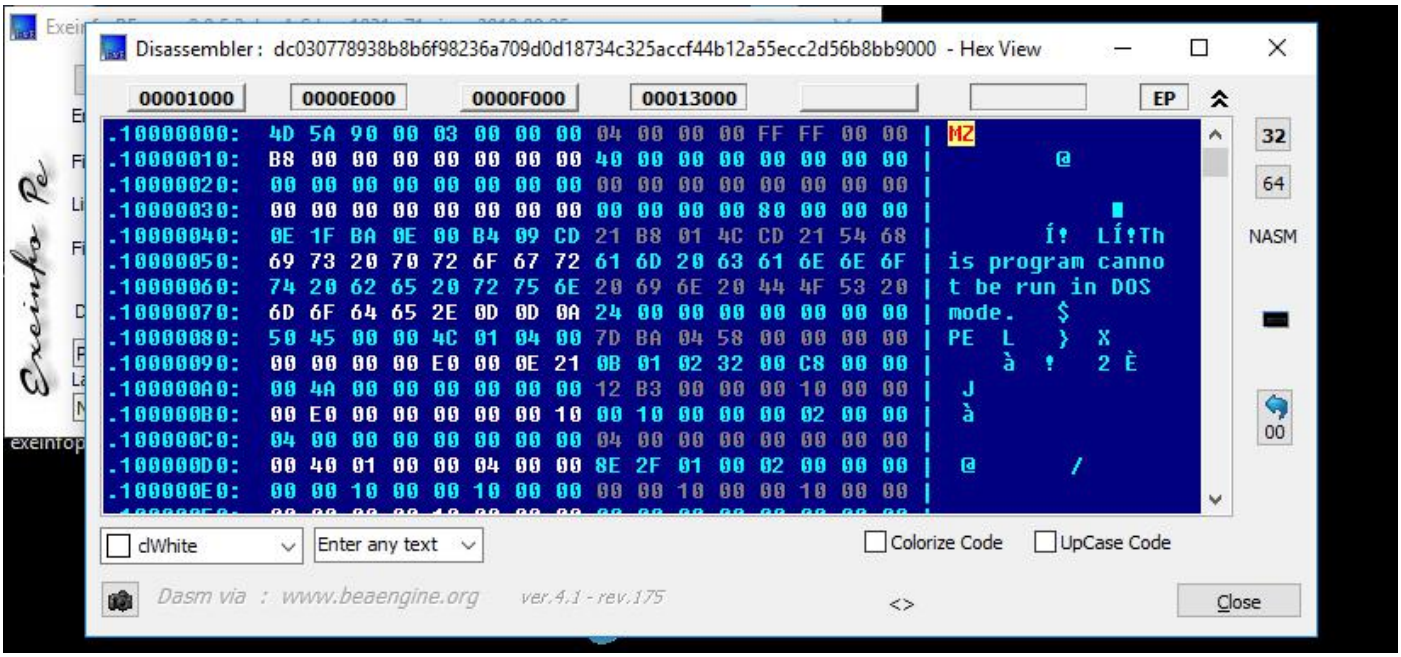


Next to that string, there it goes the PE header that’s where Portable Executable header Starts.

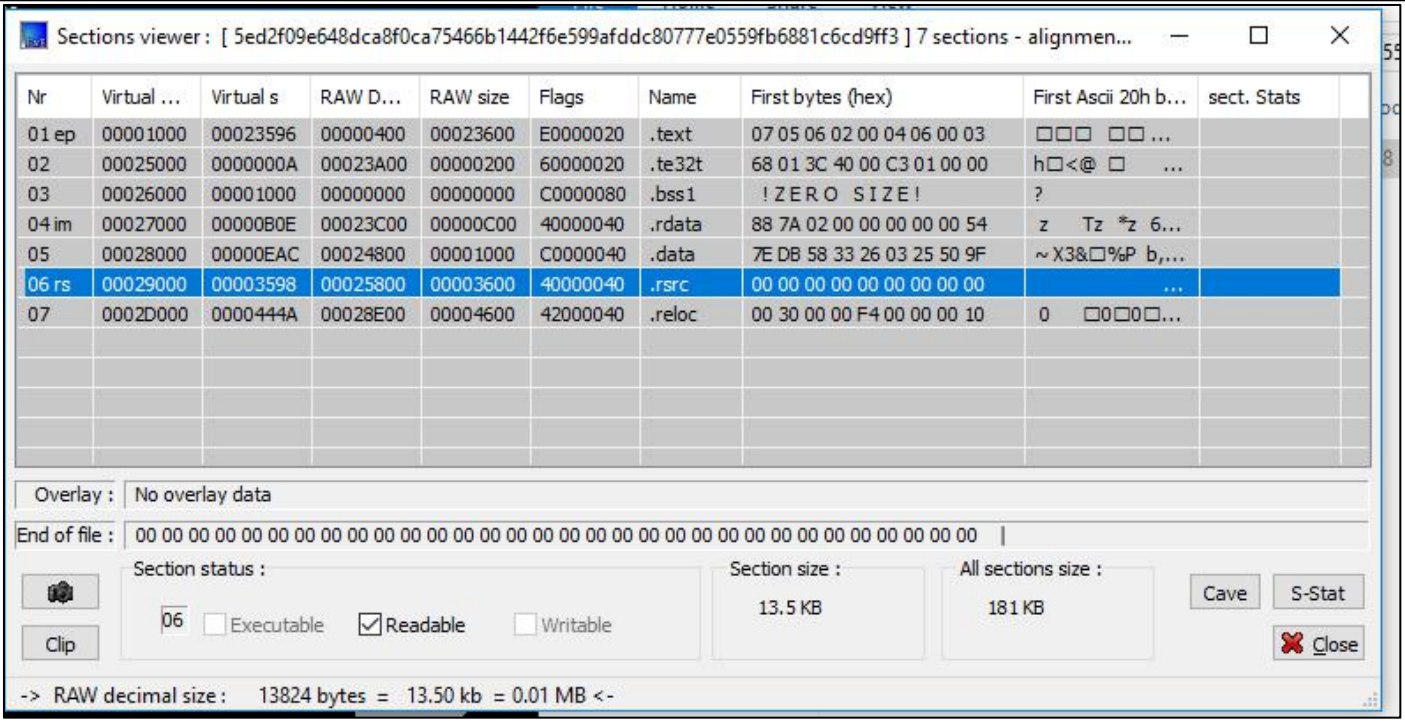


Next, You can Drag the malware sample into Exeinfo PE launcher to check additional details like whether its packed or not, and we can check for the sections also,





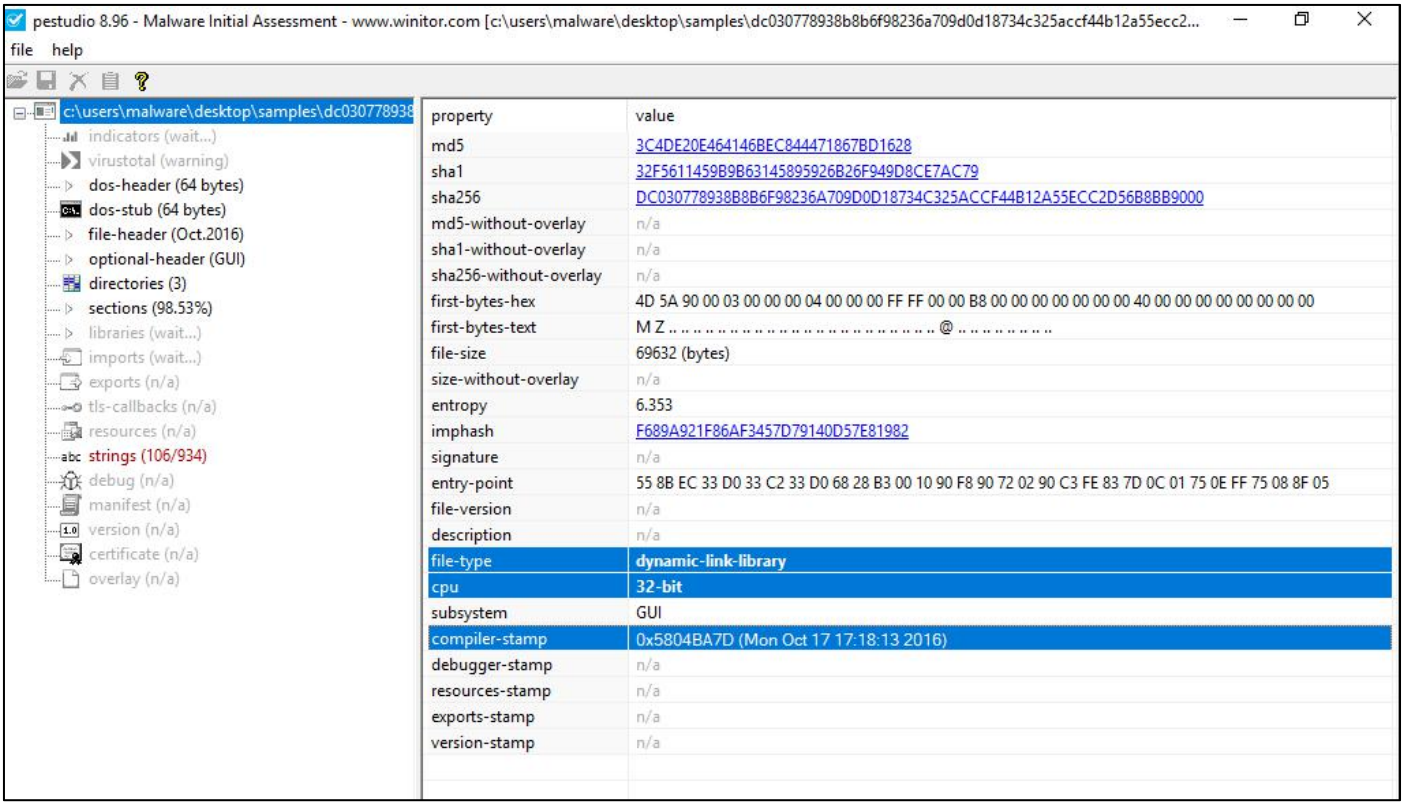
We can use the Dis-assembler in this application too to check for the Hex Values, and PE header and the header string as we did with HxD application.



We can inspect the sections details in this tool by using the small icon (second one below the magnifier icon), it seems this file is having some resource file in it.

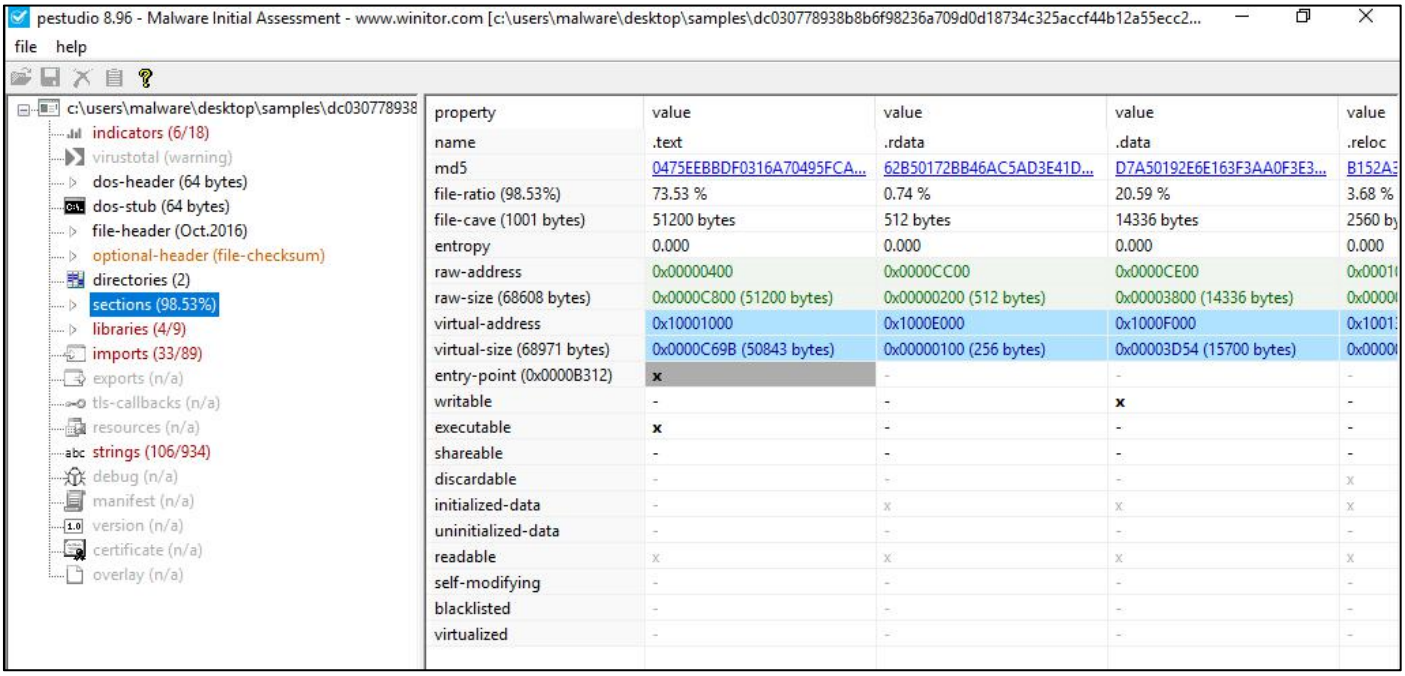
Next Step in the flow is Analyzing PE HEADER, lets find out what we can get more in this.

We can do this step by using the malware sample in pestudio tool, drag and open the malware sample file in pestudio.



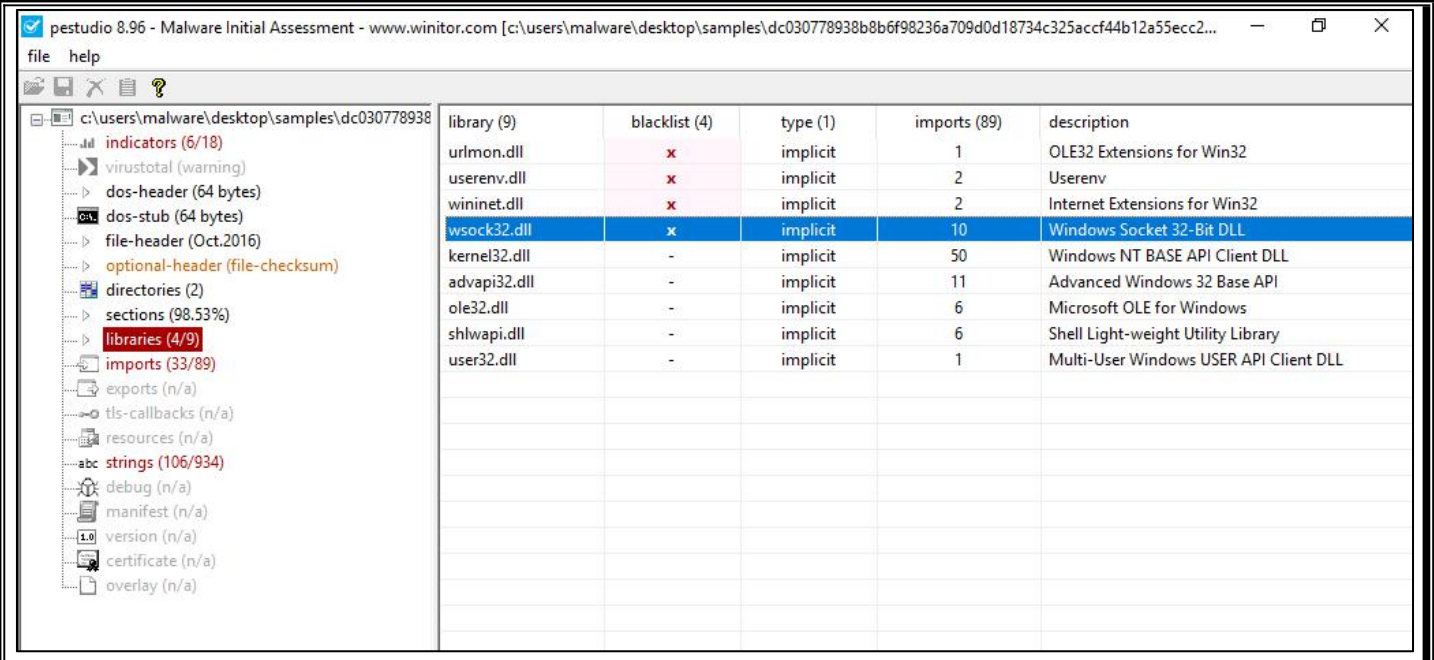
PE HEADER STRUCTURE

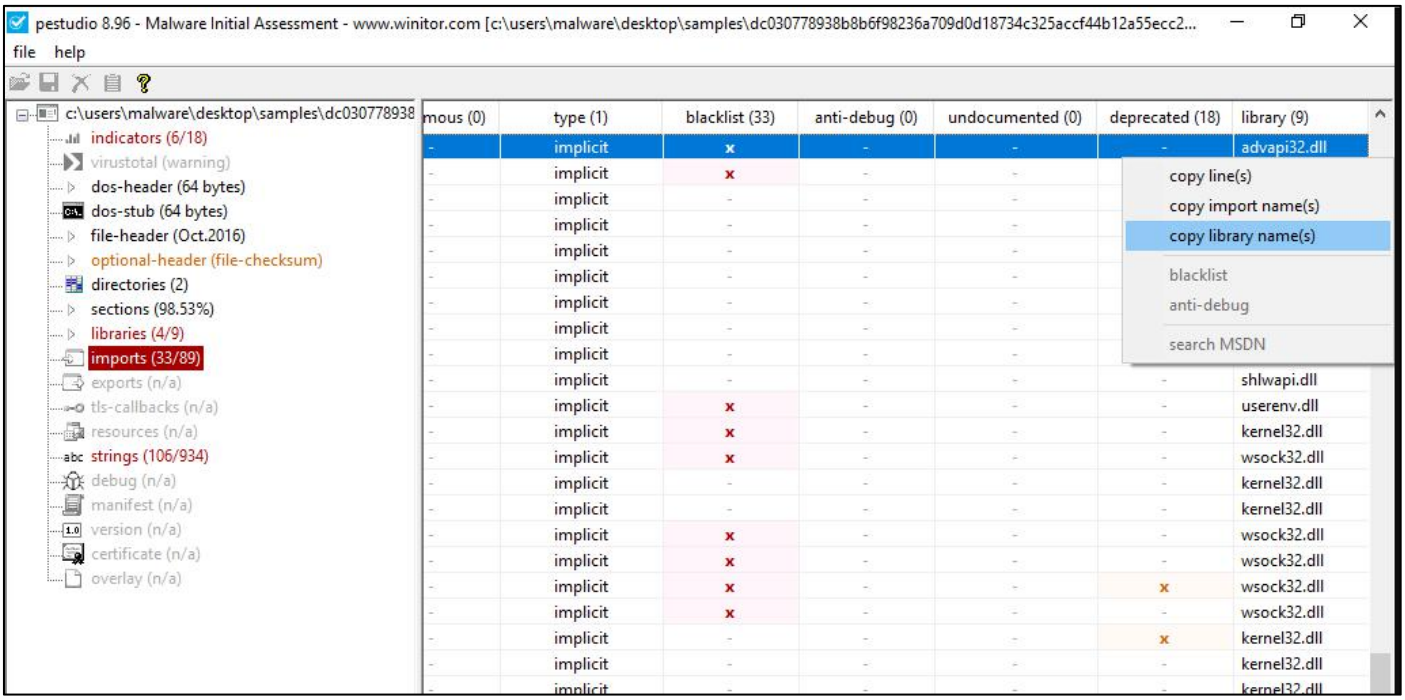
MZ Header/DOS Header	Executable Binary
DOS stub	Prints a message (Program cannot run in DOS mode)
PE File Heder(Signature)	Define exe as PE
Image optional Header	Important info like subsystem and entry point
Section Table	How to load the executable into memory
Sections	Executable sections of code and data



PE SECTIONS

.code/.text	Executable code
.data	Stores data(R/W)
.rdata	Stores data (Read only)
.idata	Stores import data
.edata	Stores export data
.rsc	Stores resources(strings and icons)



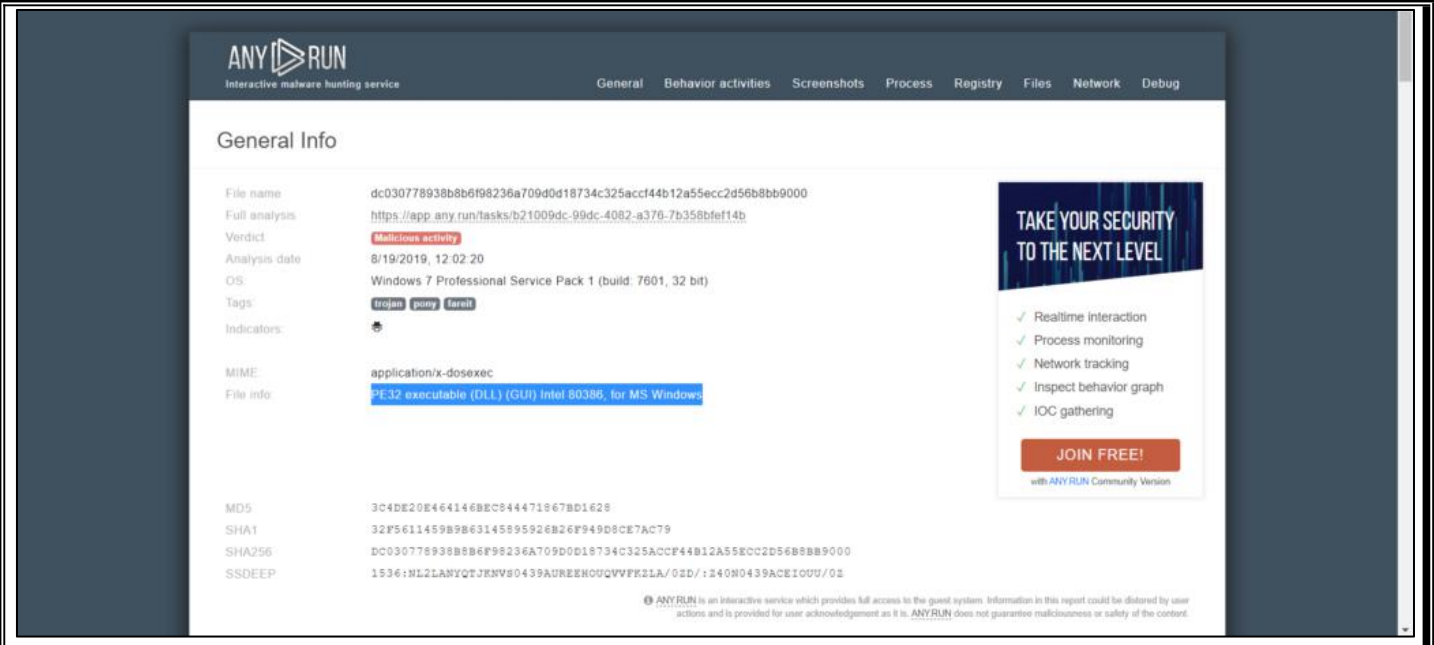


Libraries and Imports – what libraries and imports are being used, what information do they give us about functionality of malware.

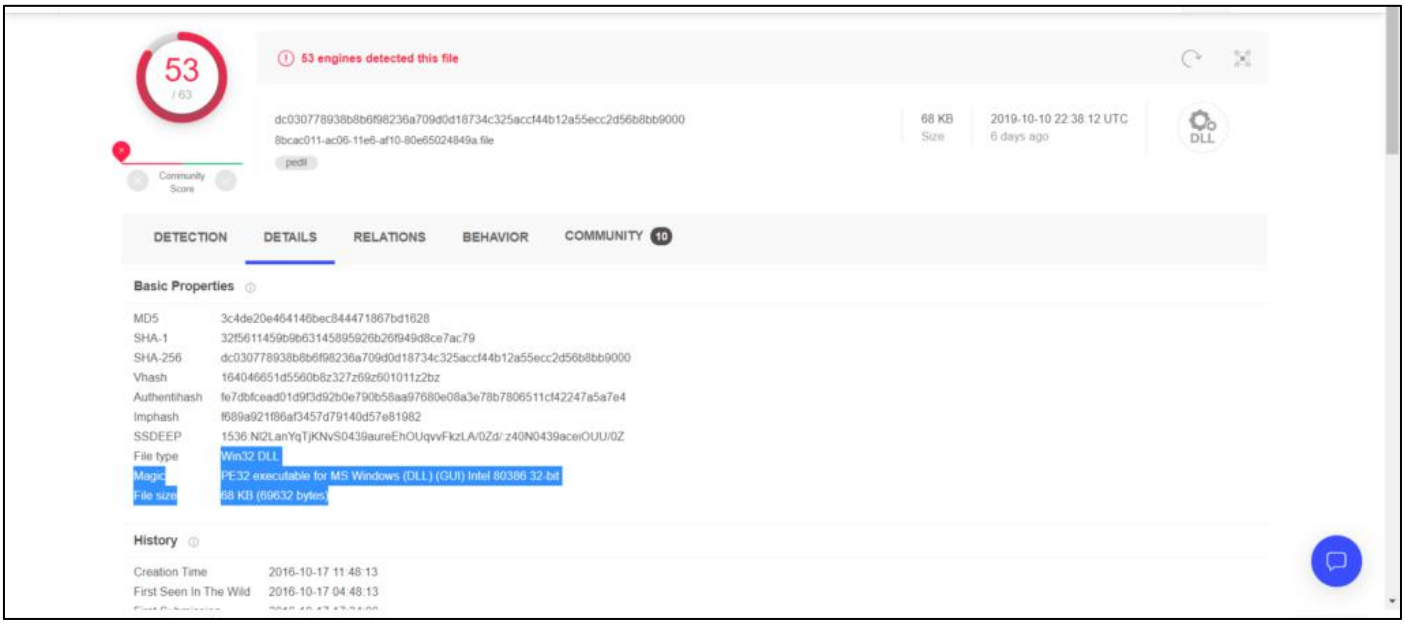
Import file will be having Socket information

Resources Section – Attacker can utilize the resource section to store malicious file and payload, droppers and configuration files etc. Some malware have resources section, some don't.

Strings – Strings block will list you all the strings available in the Sample.



Just copy Hash and put it in virus total.com and google it to analyze the hashed files. We look for the pony malware file type.



In virus total website we can see where the malware is first found and the history about it.