**Static Malware Analysis Using PEstudio**

**PeStudio**

PeStudio is an initial Malware Assessment Tool.PeStudio is a free tool which can be used to perform static analysis of any Windows application and reveals not only Raw-data, but also Indicators of Trust. Executable files analyzed with PeStudio are never started. For this reason, you can analyze suspicious applications with PeStudio with no risk!

Depending on how it is started PeStudio has a Graphical User Interface (GUI) or a Character-Based User Interface (CUI), which is especially useful when performing batch-mode oriented parsing of executable files.

PeStudio has a set of unique features like looking-up for the image being analyzed on Virustotal, the possibility to start new instances of PeStudio with the dependencies of the image. PeStudio does a RAW access to the data of the Windows Portable Executable format. No Windows API is used to gather elements.

Many features are unique to PeStudio, e.g. the full integration of the Scan Report of VirusTotal, the ability to Query MSDN for imported functions, the ability to create an XML report of the image being analyzed, the detection of imported functions located outside of standard Sections tables, etc..

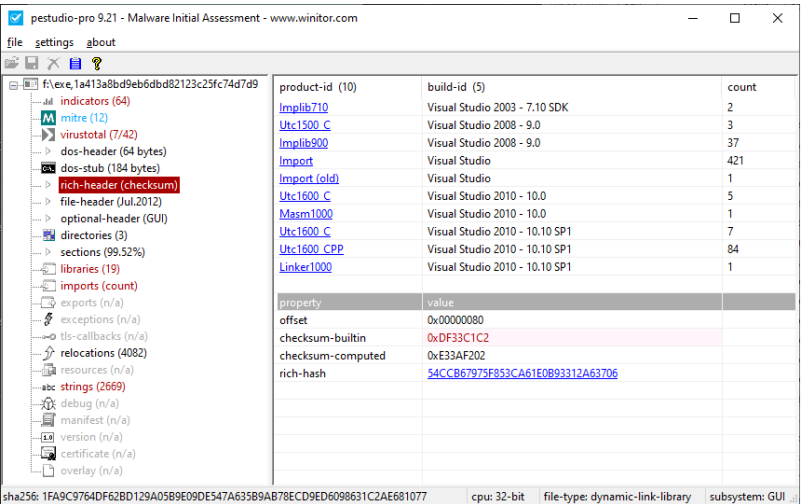
**PeStudio is a tool used for statically analyzing malware.**

* Requires no installation or opening of suspicious files
* No infection Risk
* No Sandbox needed

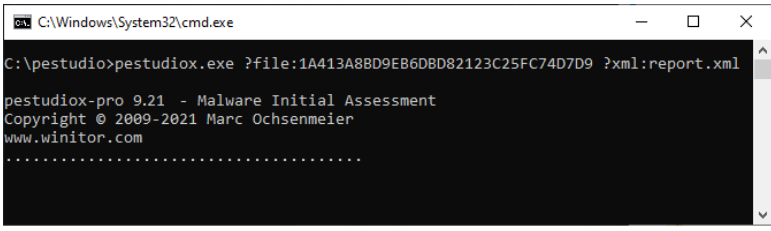
**Features of PeStudio**

* transform RAW data into information
* spot anomalies
* detect embedded files
* collect imports, exports, strings, resources, ..
* provide hints, indicators, groups, thresholds, ..
* provide **MITREattack** indicators
* retrieve scores from **Virustotal**
* consume configurations files
* create XML report

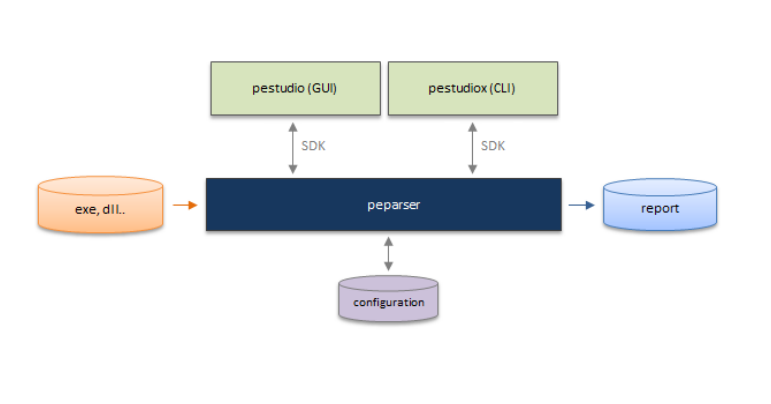
**PeStudio Supports Interactive Mode**

****

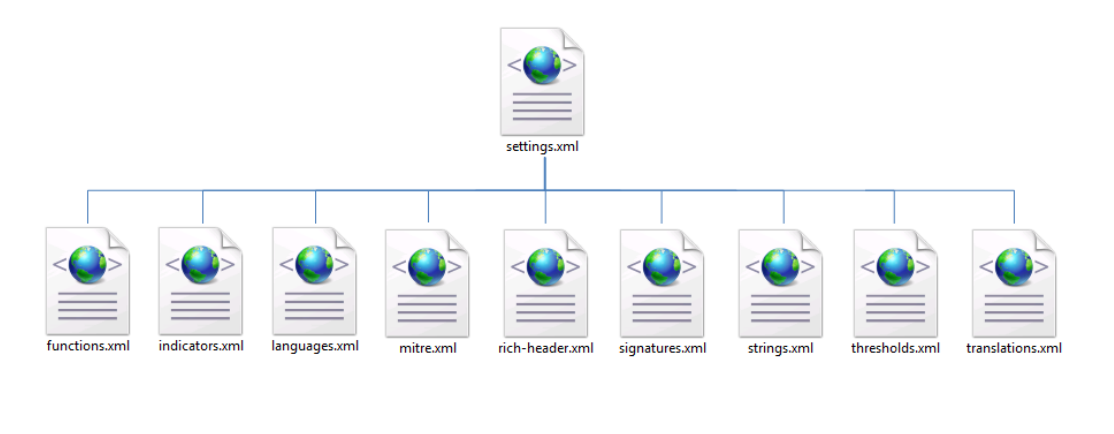
**PeStudio Supports Batch Mode**

****

**Architecture of PeStudio**

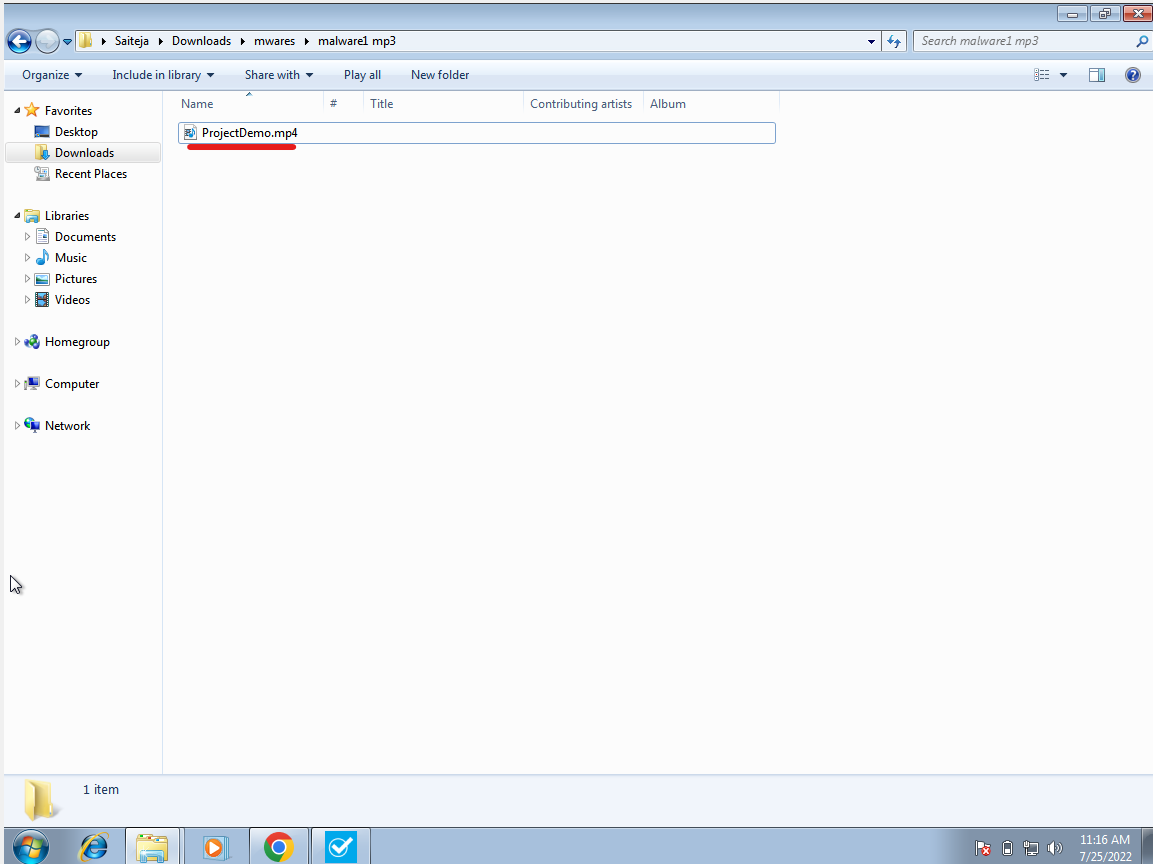
****

**Flexible Configuration**

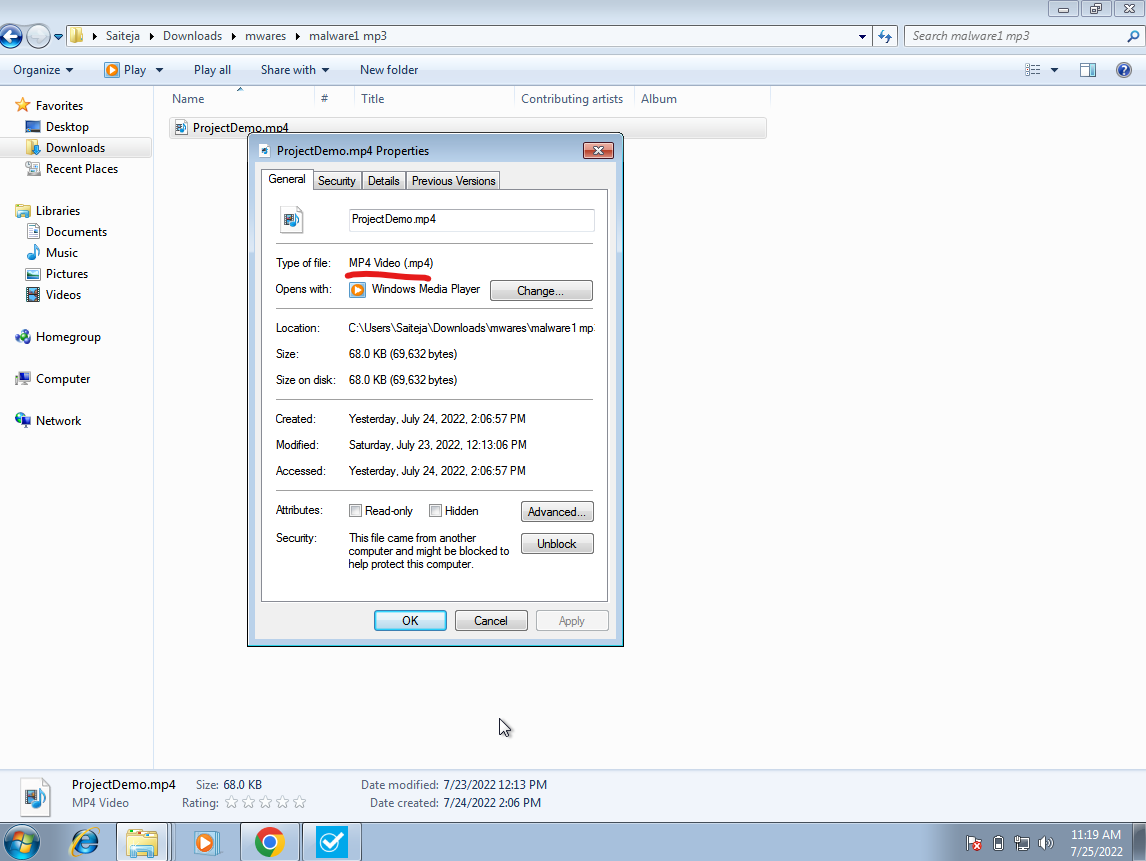
****

**Static Malware Analysis**

Malware spreads on computers **when you download or install an infected software**. They also enter your computer through an email or a link. Once malware enters the computer, it attaches itself to different files and overwrites the data.



Here we have a video called **ProjectDemo.mp4**

If we look at the file properties, it is in **.mp4** format which is a video file

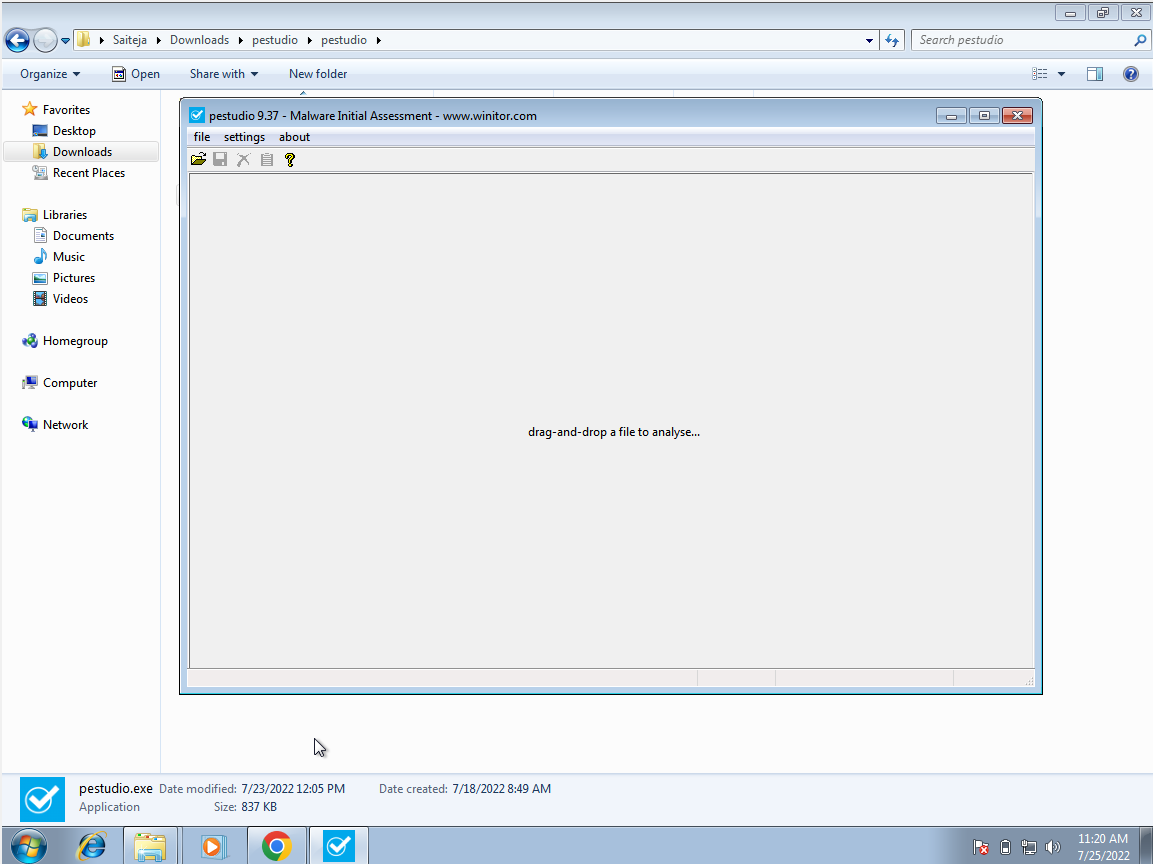
I have a sense of suspicion about this video that it may be malicious

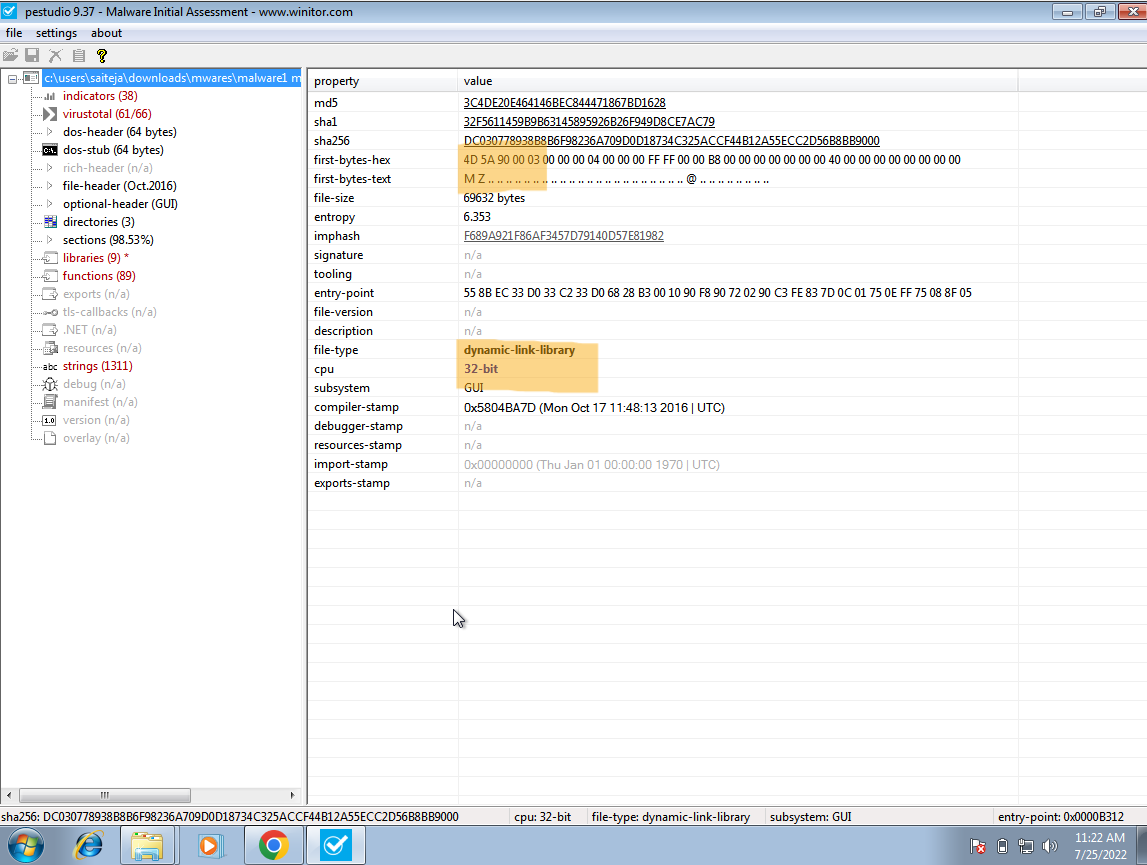
Now we have to analyze whether it is a malware or not.

Malware Analysis can be done by using different types of analyzing tools like wireshark,PEstudio,Cuckoo Sandbox etc.

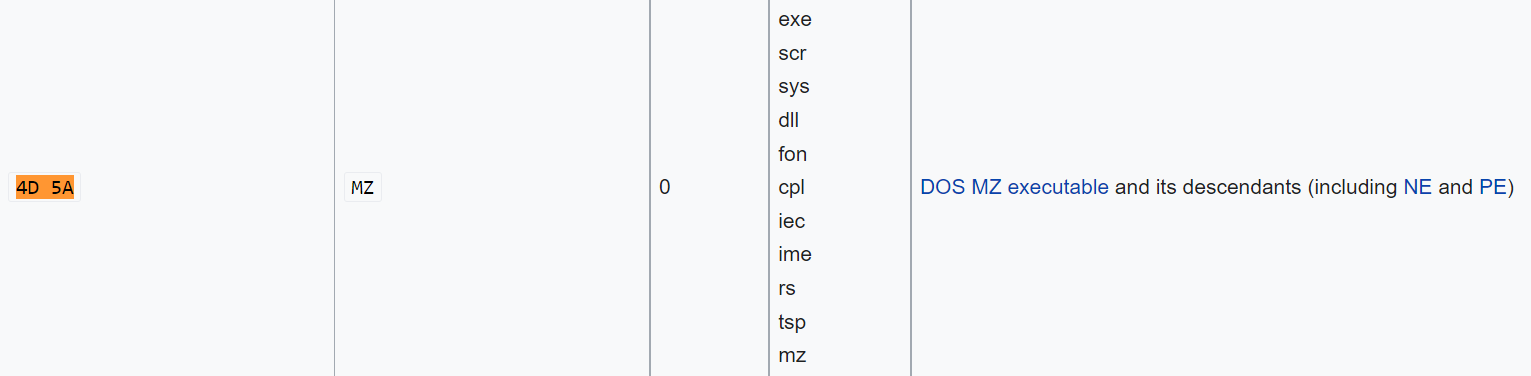
Let’s analyze this file to check if it contain any malicious data by using **PEstudio** tool

PeStudio is a tool used for statically analyzing malware and is one of my [favourite tools for malware analysis.](https://www.varonis.com/blog/malware-analysis-tools/?hsLang=en) It provides so much information about the sample and gives me a wealth of information for me to start building out my report. This is great for the initial triage of a malware sample.

* Let's open **PeStudio**
* Drag and Drop the file which needs to be analyzed in the PEstudio and start analyzing the suspicious file
* After drag and dropping of the suspicious file we see the **MainTab** of the PeStudio

Here the first byte in Hex Shows **4D 5A** and first byte in text as **MZ**

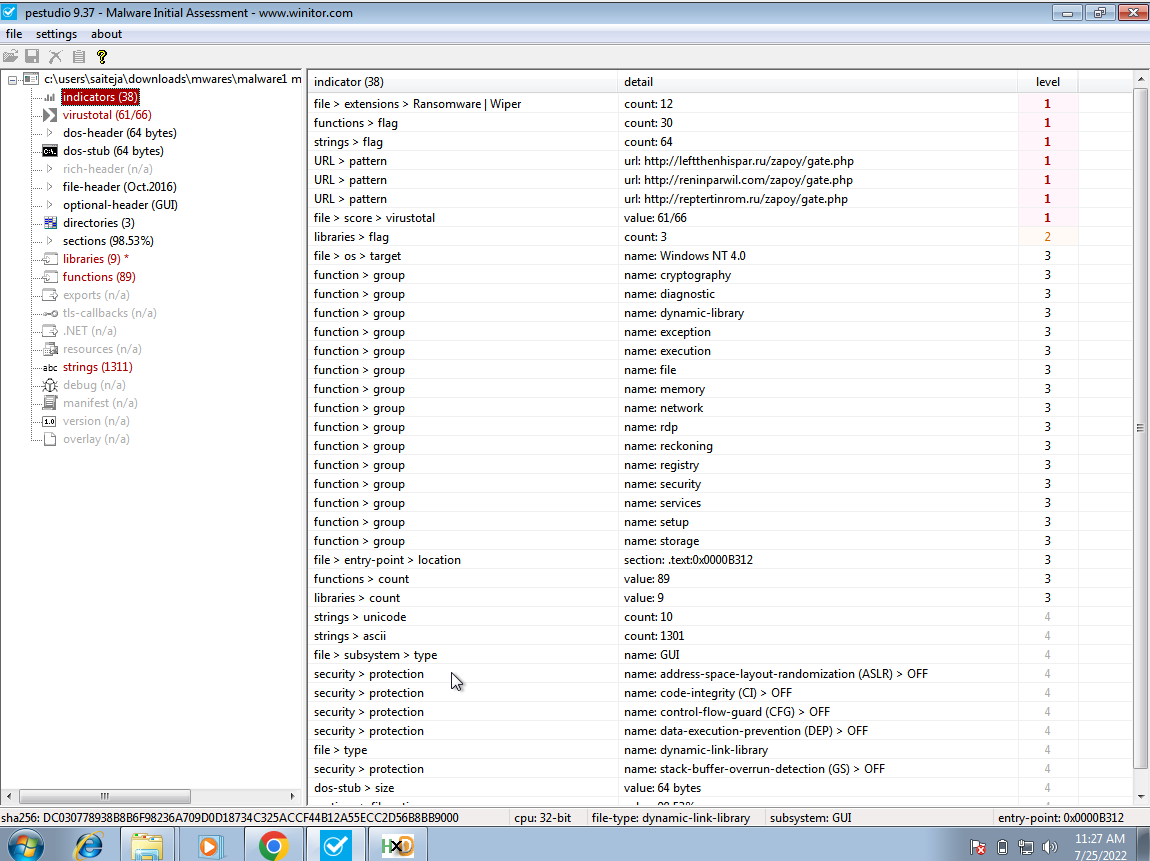
If we check these in File Signatures List in google, we can get to know that this is an **executable file.**



This confirms our suspicion on the **ProjectDemo.mp4** file as the malicious file because .mp4 files which are **videos** can’t be executable but here our ProjectDemo.mp4 is executable

**Entropy** is 6.353,File entropy **measures the randomness of the data in a file** and is used to determine whether a file contains hidden data or suspicious scripts. The scale of randomness is from 0, not random, to 8, totally random, such as an encrypted file. It also shows the submitted file is 32 bit executable and **GUI** based with **dynamic-link-library** file type.

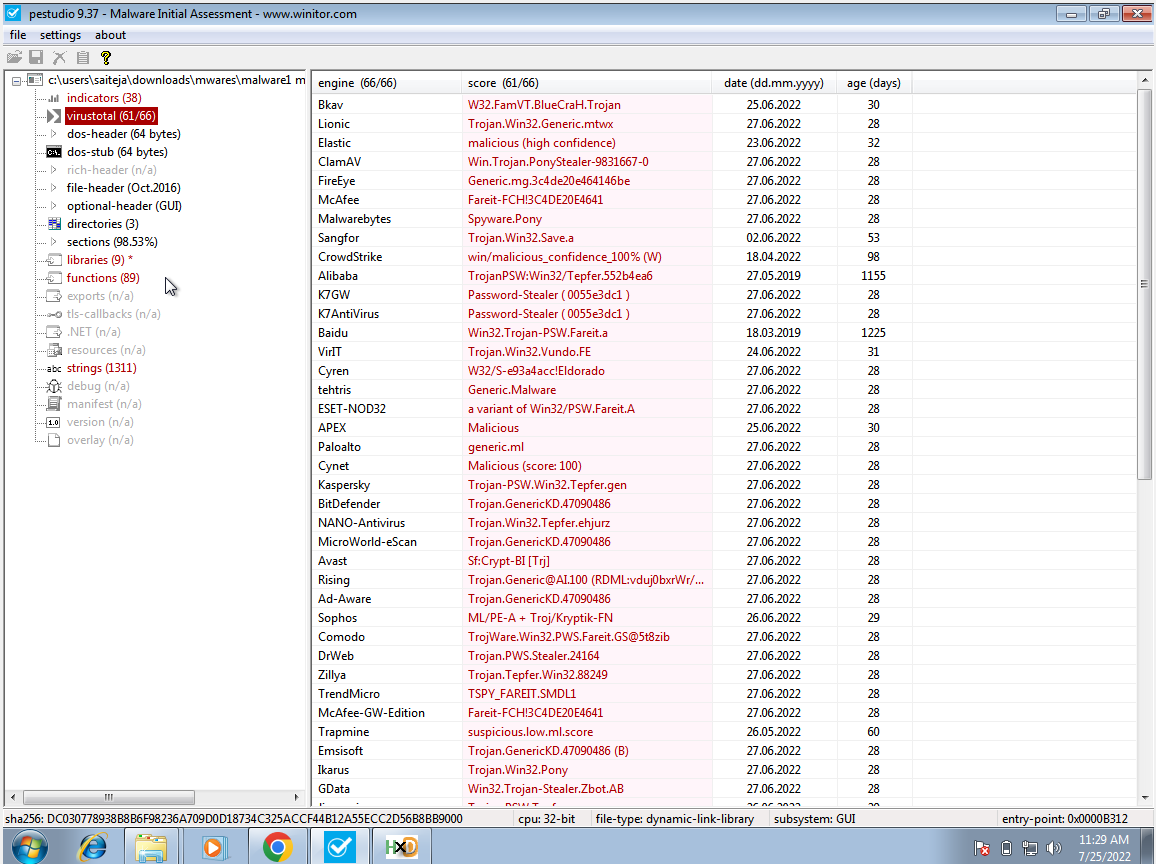
* Next tab in the **PeStudio** is **indicator Tab**

****

Indicator tab highlights data within the file that may be malicious and of interest to the malware analyst.This shows the indicators it has been identified and mark them on the scale of 1 to 3, 1 being highly malicious.

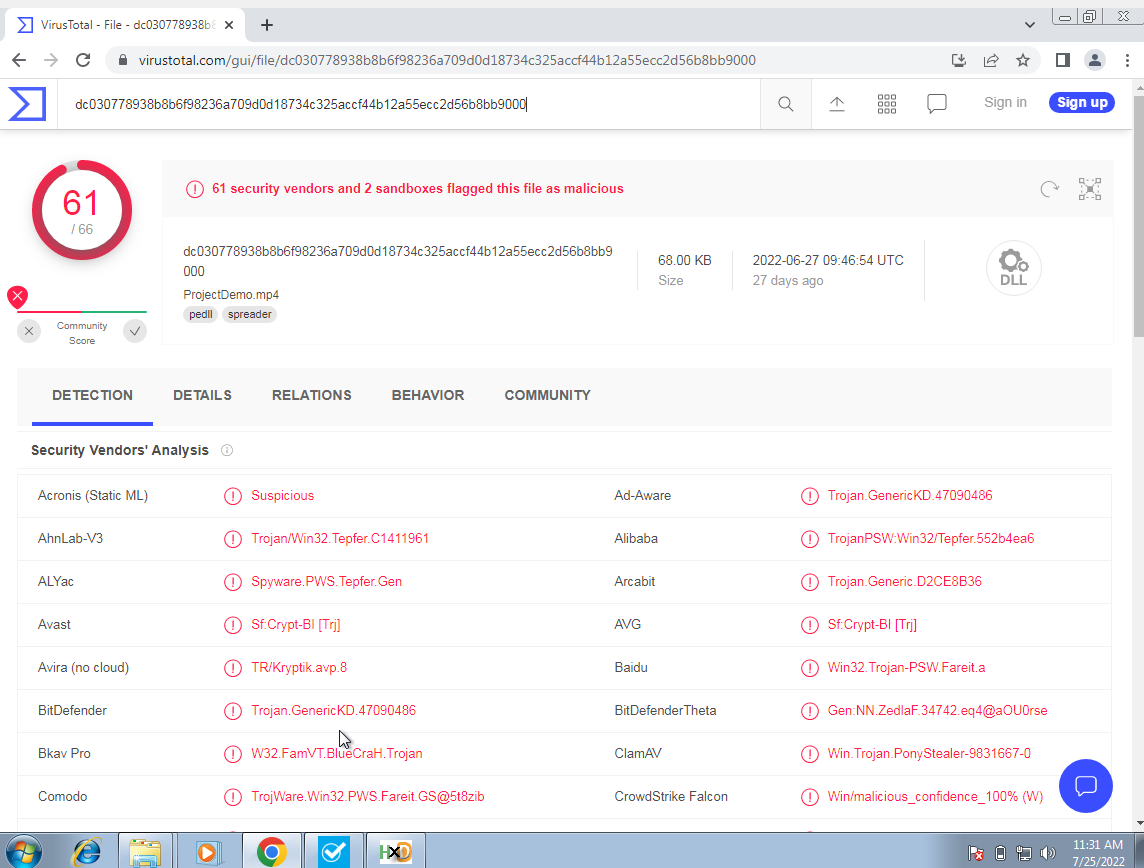
* Next tab in the **PeStudio** is **VirusTotal**

The **VirusTotal** checks the submitted file for the malicious content in some of the popularly used antivirus engines. It identifies files that match certain hash, antivirus detections, metadata, submission file names, file format structural properties, file size, etc. If the file content matches with a certain antivirus engine’s data then **PeStudio** shows it in **red.** It also shows how many engines have detected contents of the malware in this file.



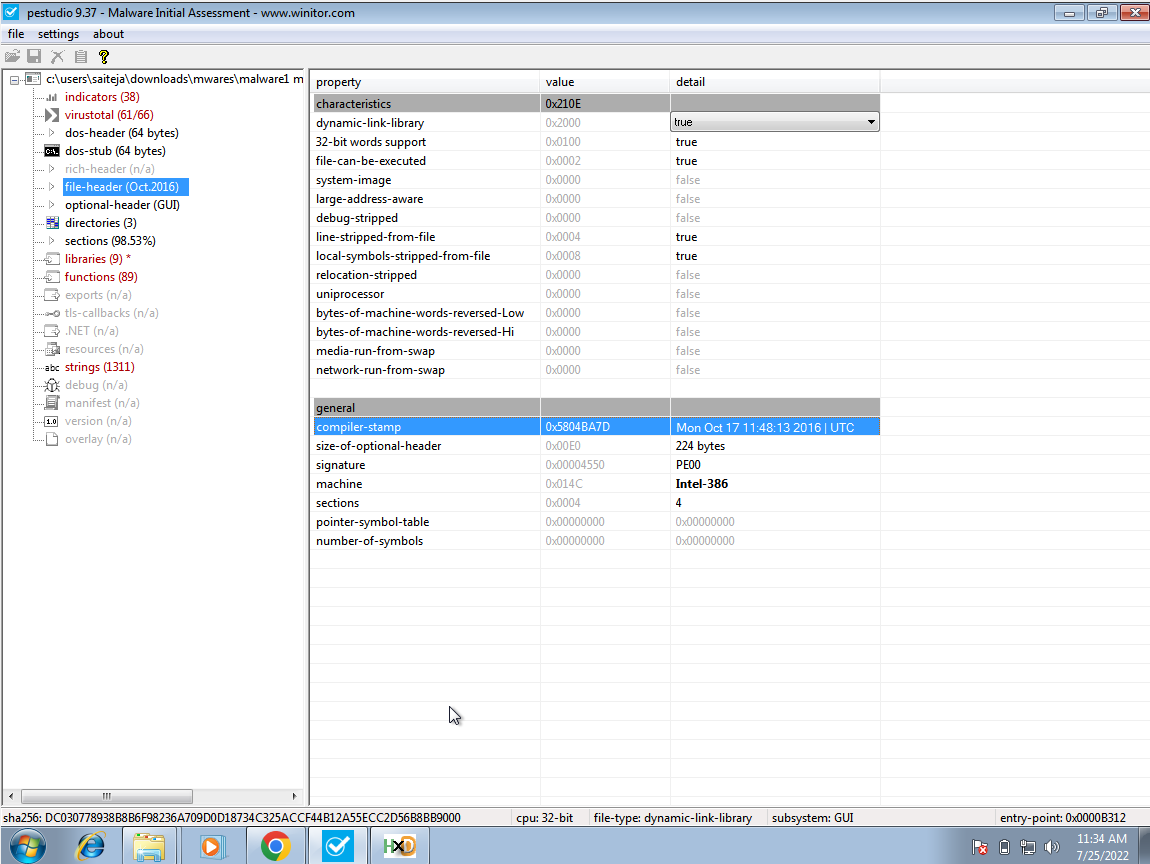
The picture shows out of 66 antivirus engines 61 engines detected that our ProjectDemo.mp4 has malicious content.

We can do this Detection of malware in several antivirus engines online by uploading suspicious files in [**https://www.virustotal.com/gui/home/upload**](https://www.virustotal.com/gui/home/upload)

****

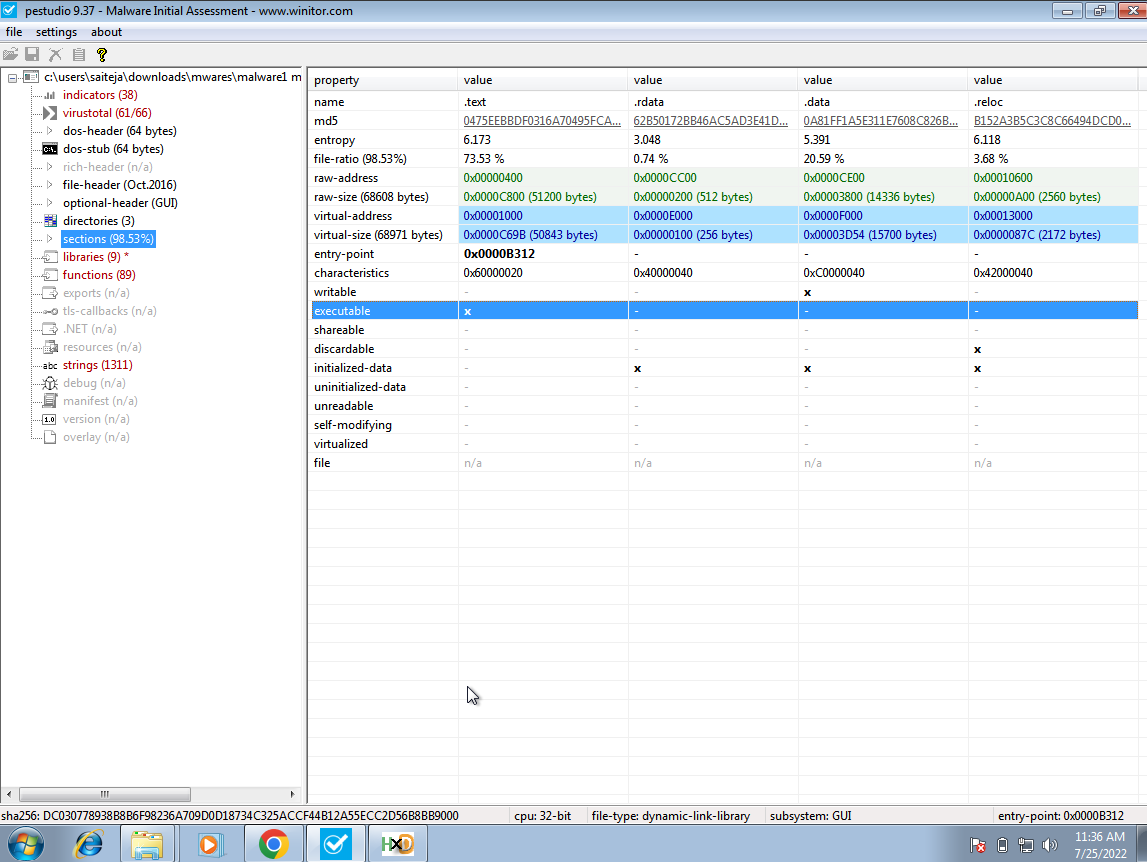
* Next tab is **FileHeader**

This shows the **Compiler Stamp** of the submitted file. Compiler stamp gives the information about when was the submitted file was compiled for the first time.Malware analyst can't be completely rely on this stamp as this compile stamp can be forged by using certain tools



This picture shows that our ProjectDemo.mp4 was first compiled on **17th OCT 2016, 11:48:13 UTC**

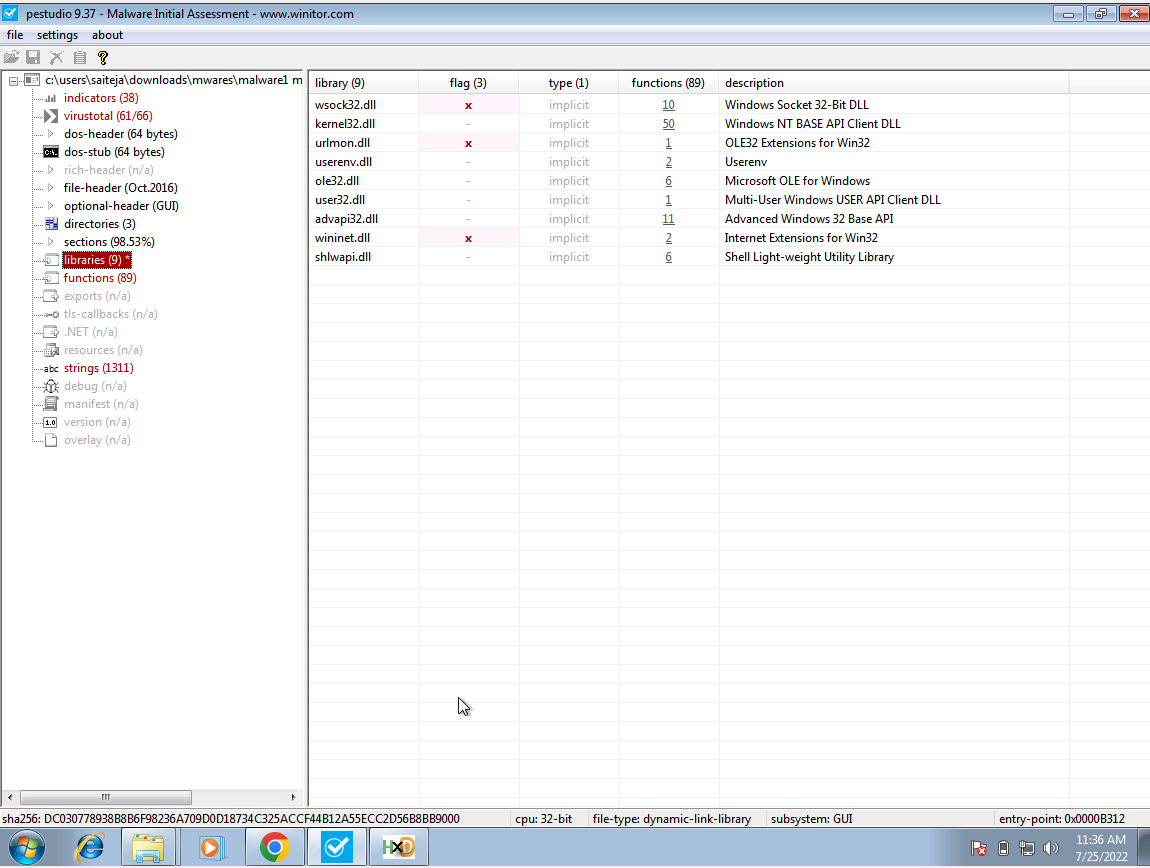
* Next tab is **Sections Tab**

The sections tab displays the various sections which make up the executable file.

In the above Image, **.text** section contains highest entropy and file ratio, this indicates that most of the **malware** is being stored in this section. We can also see that it is marked with **X** in some locations which indicates that certain sections have certain properties. In this file **.text** section has **executable property.**

* Next tab is **Libraries Tab**

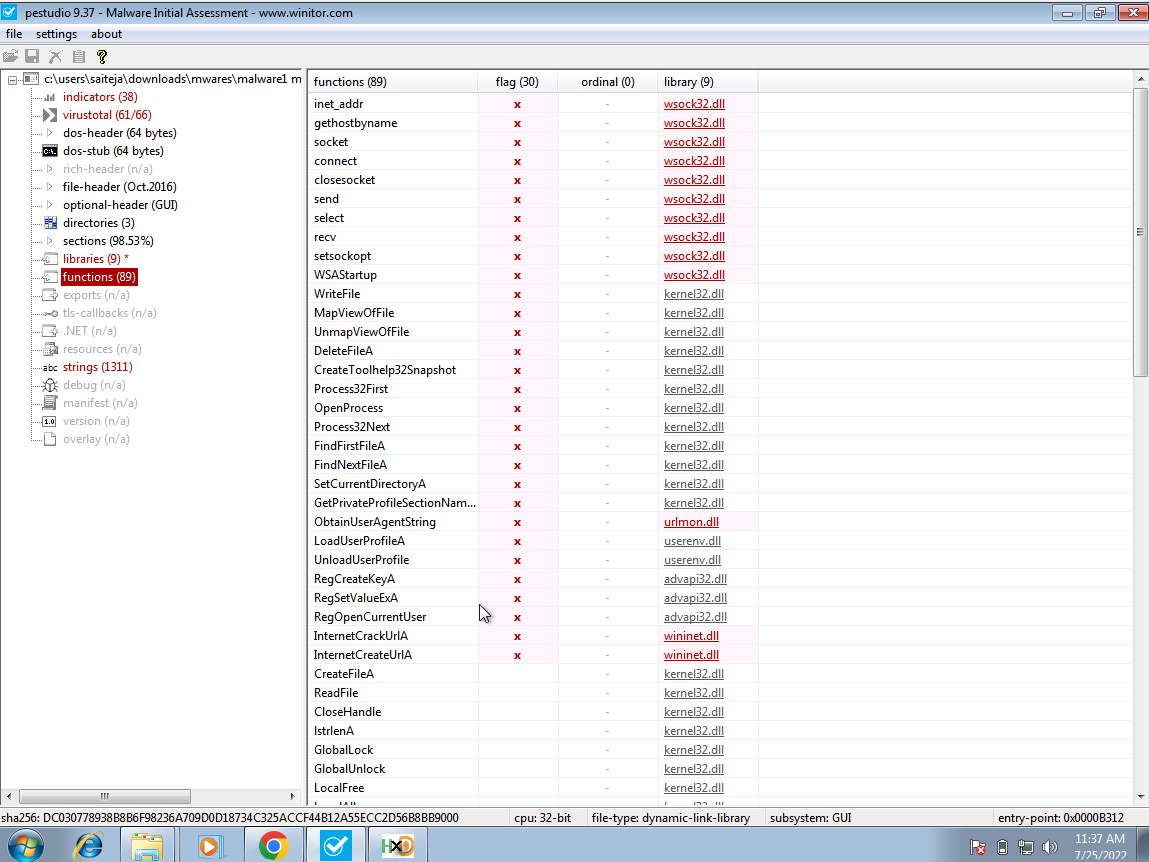
The libraries tab is useful as it displays what DLL's (Dynamic Link Library) are being imported by the malware. Each library contain different functions



Here some of the DLL's are flagged with **X** meaning that they may be being used for malicious purposes by the malware .

In the above Image, libraries like wsock32.dll, kernal32.dll, urlmon.dll, wininet.dll are being imported by the malware. **wsock32.dll, urlmon.dll, wininet.dll** are marked with **X** because they are being used for the malicious purpose by the malware

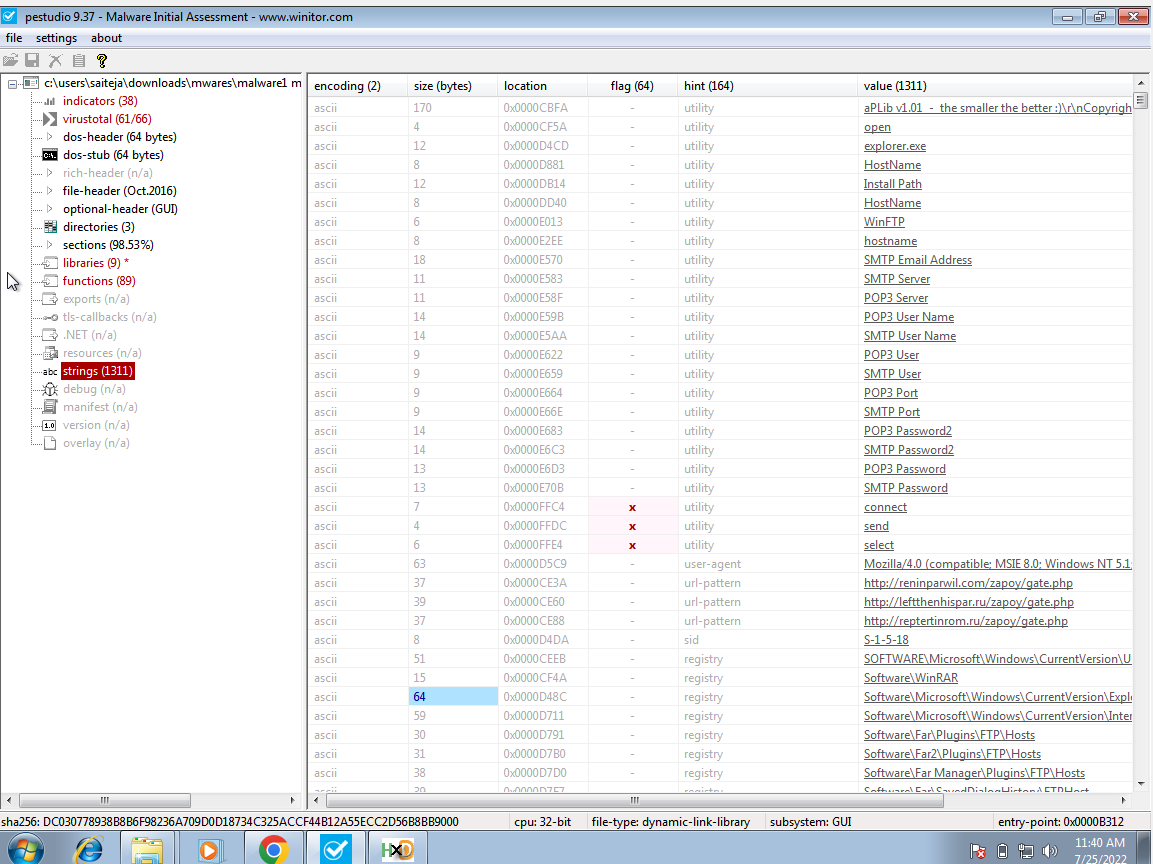
* Next tab is **Functions tab**

It indicates the functionalities that are being imported by the malware which could used for malicious purposes.

Above image shows some of the functionalities imported by the malware. Those functions include **WriteFile, DeleteFile, OpenProcess, LoadUserProfile, Sleep, ExitProcess, CreateDirectory, GetSystemInfo** etc.

* Next tab is **Strings** tab

The strings tab lists any human-readable strings that PeStudio has identified within the binary. PeStudio will tell you what type of string has been found, where it resides in the binary



The above image indicates that there are strings like **Software\Microsoft\Windows\CurrentVersion\Run**.This is a common run key used by malware authors to automatically launch the malware if the device is rebooted.**Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0)** is a user-agent.if a unique user-agent was identified then start searching for this user-agent within the organizations proxy logs to identify any additional compromised hosts.

**Conclusion**

By analyzing the malware statically, we can get to know if a file is malicious or not. If yes, then we get to know about its functionalities without executing and without viewing actual instructions of the suspicious file. By this analysis we get to know about the capabilities of the malicious file and also about the havoc this malicious file can create by infiltrating into our systems.