TERM PAPER

ON

Ethical Hacking

Virus Detecting System

SUBMITTED TO

AMITY SCHOOL OF ENGINEERING AND TECHNOLOGY



GUIDED BY: SUBMITTED BY:

Mr. DEEPAK KUMAR TARANJOT SINGH

(A12405216178)

Content

1. What is an Antivirus ?

2. What is a Virus ?

3. What is MD5 Hash ?

4. Antivirus

- Idea

- Making

- Working

- Maintaining

5. Causes of Infected Systems

6. Prevention from Viruses

7. Conclusion

What is an Antivirus?

Safety and security of computer system is the basic but at the same time a very important role of any Antivirus. The properties of an Antivirus also include detection, prevention and destruction of foreign malicious viruses and softwares. Exposing vulnerabilities like passwords, personal information, credit card details, security numbers, personal details and imposing great deal of harm to the operating system is what virus can do when it attacks a system. Identity thefts are prominent and the information is illegally used and affects the person whom it actually belongs to like credit being destroyed.

There are numerous different types of virus threats, including Spyware, Adware, Phishing, Rootkit Hacker Tools, Bots&Botnets and Ransomware. Antivirus software offer protection users need from potential harms and viruses the lurk in cyber space. One can be installed on computers, laptops, tablets and smartphones.

The effectiveness of the antivirus software depends upon whether it is being frequently updated or not. Updating of antivirus software is undoubtedly very important and this is because viruses are growing and to maintain the repulsive behavior of the antivirus toward the new viruses.

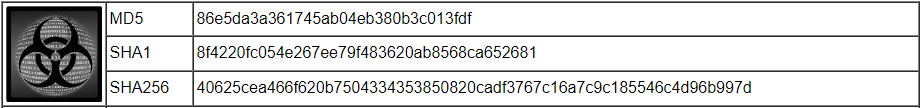
What is a Virus ?

A malware with the ability to copy itself and spread between numerous systems is called Virus. Spreading of virus has a direct result on the system with which the corrupted program gets dispatched to. A virus spreads through vulnerabilities in any software application or loopholes in on any web application. Virus can be used to take information,damage host systems and frameworks, take credits, and that is just a small part of this larger problem.

It can be in the form of executable code, substance, dynamic substance, and other programs.

What is a MD5 Hash ?

MD5 hashes work on an [algorithm](https://whatis.techtarget.com/definition/algorithm) which is a one-way cryptographic [function](https://whatis.techtarget.com/definition/function) that accepts a message of any length as input and returns as output of a fixed-length [digest](https://searchsecurity.techtarget.com/definition/digest-authentication) value to be used as an authentication for the message.



Originally these were used as secure cryptographic hash algorithms which authenticated digital signatures. MD5 has been deprecated for uses including verification of data integrity and detect unintentional [data corruption](https://searchsqlserver.techtarget.com/definition/data-corruption).

Antivirus

Idea

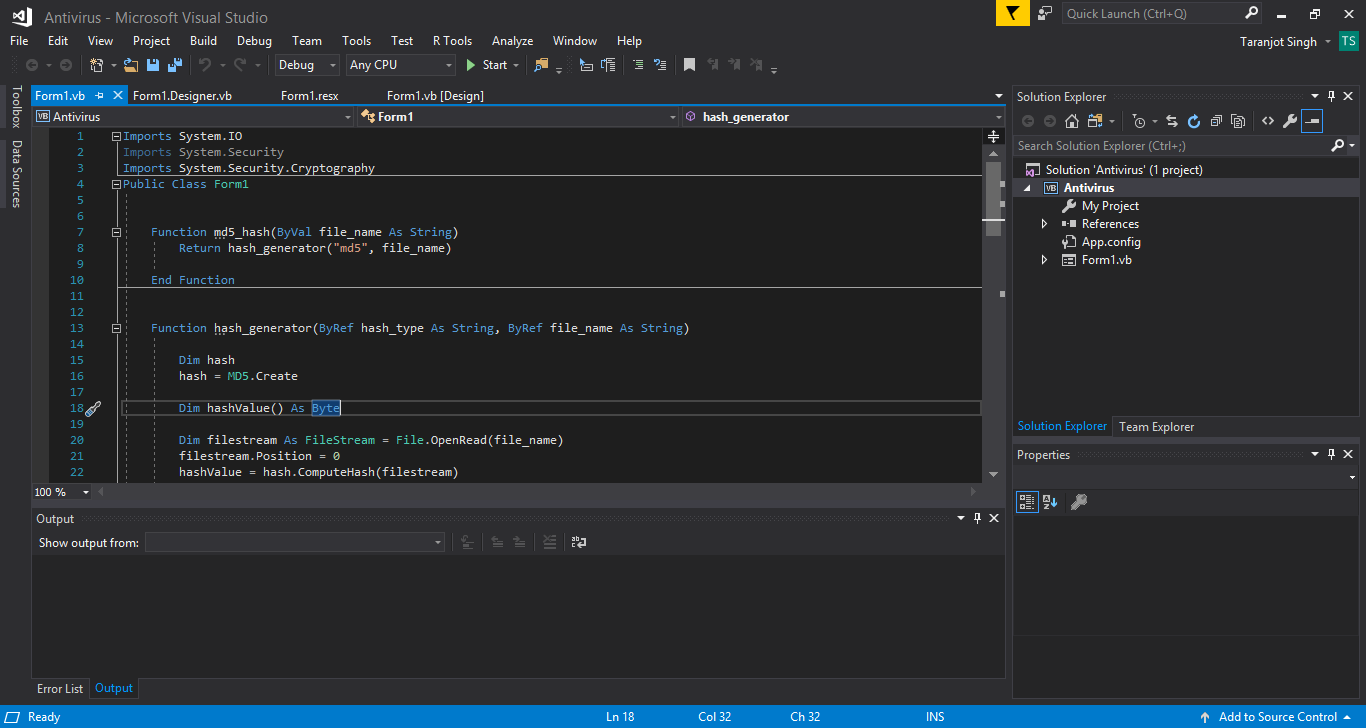
The idea is to make an antivirus which can browse a file and then detect if the file is infected with some kind of a virus or not

Making

The making involves a tool and language knowledge which include

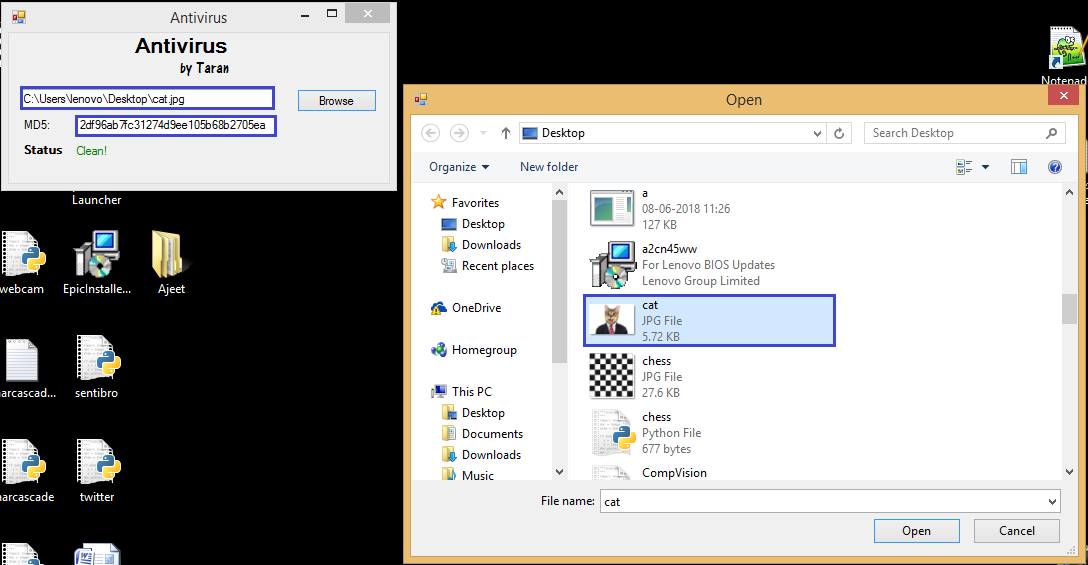
-Visual Studio 2017

-Visual Basic

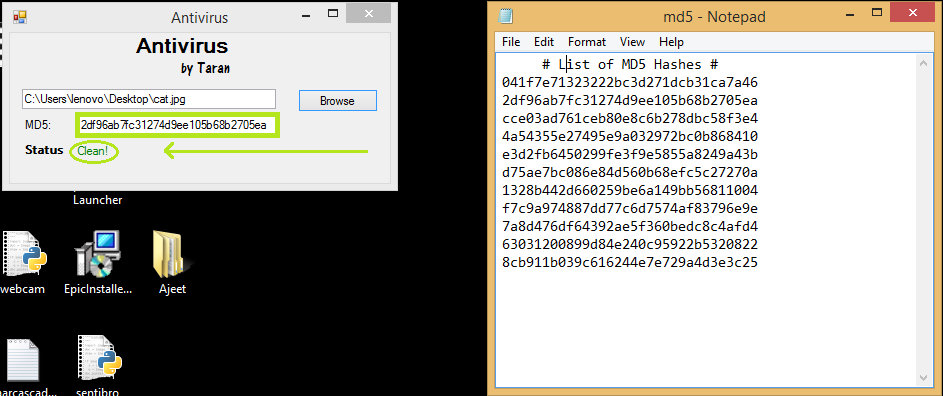


Working

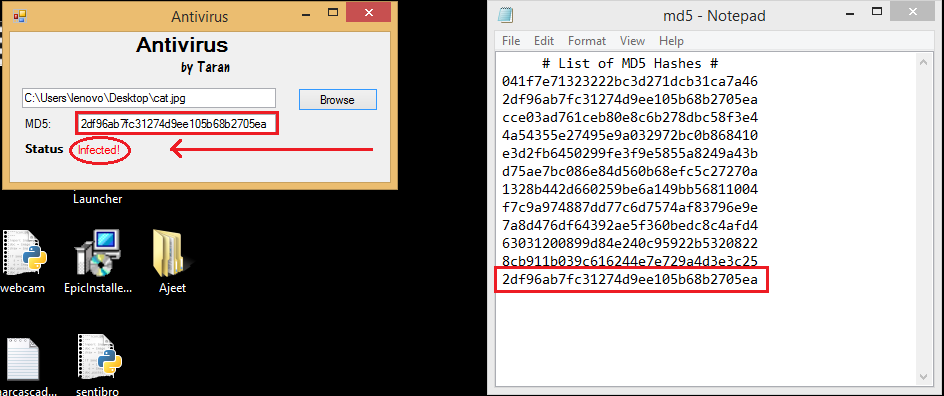
1. Clicking Browse enables to explore a file which one wants to get detected



1. Once the path is set, a part of the code made using Visual Basic Language will enable the Antivirus to extract the MD5 hash of the file from the file’s properties
2. The code will then check the md5.txt file which contains a list of MD5 hashes which are known to have harmful properties
3. If the MD5 hash extracted from the browsed file **does not exist**in .txt file; the Status will change to CLEAN!



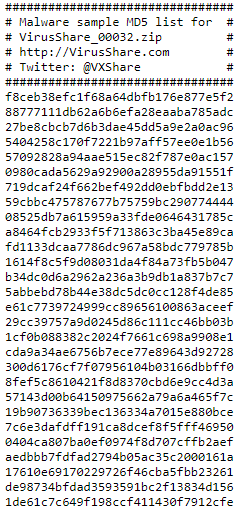
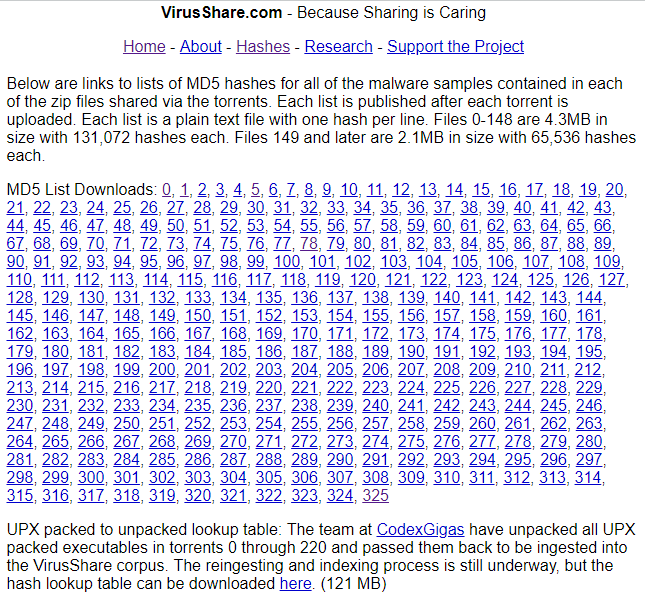
1. But if the MD5 hash extracted from the browsed file **exists** in .txt file; the Status will change to INFECTED!



Maintaining

This can be said to be the most important part where regular updates to the .txt file are required to keep the Antivirus working and help it detect any new viruses.

This can be done by Browsing the MD5 hashes of the viruses which have been detected recently and adding them to your .txt file



Causes of Infected Systems

Web customers should be watchful in light of the way that it's not by and large ensured. Normal advanced related infringement are on highlights . Being an Internet User, it is moreover our own obligation to think about the sorts of substance which prompts malware downloads and hampering the customers security.

To diminish these sorts of malware a part of the going with exercises can help :

Spams one gets in mail

Associations can make the exchanging of records and diverse reports beneficial. Regardless, in light of the intrinsic shortcomings of Internet-based email, there is no affirmation that a message you have gotten is truly from the source email address or that the association was not balanced in travel. The principle secure decisions are to use a pariah archive advantage, (for instance, ShareFile, DropBox, Box, OneDrive, Google Drive, et cetera.) or use email encryption and modernized imprints, (for instance, S/MIME or PGP).

Social Hyperlinks

Fake records are to a great degree unavoidable on social locales. Especially if a URL shortening organization is being utilized. Malignant destinations get opened when one ticks on such associations. Do whatever it takes not to tap on such associations. Use a web list and request the name of the hyperlink instead of tapping on the association. Tapping on such hyperlinks might be a welcome for dangerous substance to your PC.

Third Party Downloads

There is a risk in procuring any sort of archive from any region other than affirmed provider, merchant or dealer. The pariah record encouraging destinations can moreover download compacted, exchanged off or spoiled types of the archive. Persistently look out the primary source. This will amazingly in diminishing the risk of being hit by malware softwares.

Prevention from Viruses

1. Install Antivirus or Malware Software

2. Keep your Antivirus Up to Date

3. Run Regularly scheduled scan with Antivirus

4. Think before you Click

5. Keep your Personal Information safe

6. Don’t use Open WiFi

7. Back Up files

8. Use Strong Passwords

9. Avoid entertaining Pop ups

10. Secure your surroundings

Conclusion

This Software Application can Browse any file of your system and Detect MD5 hashes of known viruses giving confirmations whether the browsed file is

INFECTED! or CLEAN!