Python Keylogger

A close-up of a keyboard

Description automatically generated with medium confidence

-Bolla Yeshwanth Reddy

# ABSTRACT

Keyloggers are type of a rootkit malware that capture typed keystroke events of the keyboard and save into log file, therefore, it is able to intercept sensitive information such as usernames, PINs, and passwords, thus transmits into malicious attacker without attracting the attention of users. A keylogger is a tool which is implemented to acquire the keystrokes entered by using keyboard. It is also a battery sized tool which is connected between keyboard and computer. The main purpose behind keylogger tool is to keep monitor that work computers are used for business and other purpose. This documentation presents an overview of keyloggers programs their characteristics and features .Also their uses in the software development.

**LIST OF FIGURES**

|  |  |  |
| --- | --- | --- |
| Fig. No. | Title | Pg.No. |
| 1 | Software Architecture | 14 |
| 2 | Use Case Diagram | 18 |
| 3 | Sequence Diagram | 20 |
| 4 | Activity Diagram | 22 |
| 5 | System Level Diagram | 23 |
| 6 | PyHook | 24 |

**Table of Contents**

S.No Topic Pg.No. 1. Introduction. 8

1. Software Requirement Specifications 14
2. Design. 17
3. Implementation. 25
4. Testing 35

[Conclusion. 39](#_TOC_250002)

[References 45](#_TOC_250001)

Appendix A-Abbrevations 46

Appendix B-Software installation 48

[Appendix C-Software Usage Process 50](#_TOC_250000)

### Chapter 1

**INTRODUCTION**

### Keylogger

A keylogger, sometimes called a keystroke logger or system monitor, is a type of surveillance technology used to monitor and record each keystroke typed on a specific computer's Keyboard. Keylogger software is also available for use on smart phones such as **Apple iphones** and **Android** devices.

### Types of Keyloggers

A hardware-based keylogger is a small device that serves as connector between the keyboard and the computer. The device is designed to resemble an ordinary keyboard PS/2 connector, part of the computer cabling or a USB adaptor, making it relatively easy for someone who wants to monitor a user's behavior to hide such a device.

A keylogging software program does not require physical access to the computer for installation. It can be purposefully downloaded by someone who wants to monitor activity on a particular computer, or it can be malware downloaded unwittingly and executed as part of rootkit or [remote administration Trojan (RAT)](https://searchsecurity.techtarget.com/definition/RAT-remote-access-Trojan).The rootkit can launch and operate stealthily in order to evade manual detection or antivirus scans.

### How do keyloggers work ?

How a keylogger works depends on the type of keylogger it is. Hardware and software keyloggers will work differently due to their medium.

Most workstation keyboards plug into the back of the computer, keeping the connections out of the user's line of sight. A hardware keylogger may also come in the form of a module that is installed inside the keyboard itself. When the user types on the keyboard, the keylogger collects each keystroke and saves it as text in its own miniature hard drive, which may have a memory capacity up to several gigabytes. The person who installed the keylogger must later return and physically remove the device in order to access the information that has been gathered. There are also wireless keylogger sniffers that can intercept and decrypt data packets transferred between a wireless keyboard and its receiver.

A common software keylogger typically consists of two files that get installed in the same directory: a dynamic link library (DLL) file that does all the recording and an executable file that installs the DLL file and triggers it to work. The keylogger program records each keystroke the user types and periodically uploads the information over the internet to whoever installed the program. There are many other ways that keylogging software can be designed to monitor keystrokes, including hooking keyboard application program interfaces (APIs) to another application, malicious script injection or memory injection. There are two main types of software keyloggers: user mode keyloggers and [kernel](https://searchdatacenter.techtarget.com/definition/kernel) mode keyloggers. A user mode keylogger will use a Windows API to intercept keyboard and mouse movements. GetAsyncKeyState or GetKeyState API functions might also be captured depending on the keylogger; however, these keyloggers require the attacker to monitor each keypress actively.

A kernel mode keylogger is a more powerful and complex software Keylogging method. It works with higher privileges and can be harder

to locate in a system.Kernel mode keyloggers will use filter drivers that can intercept keystrokes. They can also modify the internal Windows system through the kernel.

Some keylogging programs may also include functionality for recording user data besides keystrokes, such as capturing anything that has been copied to the clipboard and taking screenshots of the user's screen or a single application.

Remote- access software keyloggers can allow access to locally recorded data from a remote location. This communication can happen by using one of the following methods:

* + 1. Uploading the data to a website, database or FTP server.
    2. Periodically emailing data to a predefined email address.
    3. Wirelessly transmitting data through an attached hardware system.
    4. Software enabling remote login to your local machine.

### Existing System

It is likely that about one out of many large companies systematically monitors the computer , internet, or email use of its users employees. There are over hundreds of different products available today that will let organizations see what their users do at work on their "personal" computers, in their email, and on the internet. But what do such numbers really mean ? What does company monitoring of user/employee email, internet, and computer usage actually look like? What sorts of things can an organization/company see users do at their

computers, and what sorts of computer activities are currently invisible to work place monitoring?

### Proposed System

The keylogging program logs all keystrokes (aka Keystroke Logging) along with the name of the application in which the keystrokes were entered. U sing keylogger we prevent the miscellaneous use of system. Using this we capture all information in text and image form.

Key Terms: Email monitoring, Internet monitoring, Computer monitoring, Chats/IM is monitoring, Network monitoring, Document monitoring, Web site monitoring, Productivity monitoring, keylogging.

### Advantages of the proposed system

* + - * **Differentiate between Productivity and idleness:** If the performance of your organization is going down by the day, you have the right to feel concerned. Going one step further, you could indicate your concern by going after the culprit whose performance is deteriorating that of the whole organization. In order to do that, there is no better tool then Keylogger Software.
      * **Maintaing a check on your children:** If you only know what kind of activities your children are engaging themselves in while being on the Internet, it would be relatively easier for you to effortlessly track down their habits. After tracking their habits through Keylogger Software, it would be much easier for you to prevent them from being engaged in harmful activities on the Internet.

Most of the Keylogger software’s have no presence on the Task Manager. Also, for a person who is primarily unaware of the presence of a Keylogger Software on his/her Computer, it is virtually

impossible to uninstall this software since it does not feature even on the Add/Remove Programs list.

* + - * **Monitoring the activities of a particular person:** Stealing passwords of the Social Media Profiles of any person is unethical. However, keeping ethics at bay, Keylogger Software will give you a power which most of your acquaintances could only dream of.

You could not only steal their passwords but also keep using their Social Media Accounts without them even knowing. As a result, every time they do an activity on any of the Social Media platforms, you’re only a click away from knowing what it is.

* + - * **Ethical Hacking**: You could go to the Computer of anybody that you know and identify the weakness in their Security System. By doing so, you could note down whether these weakness is present on your computer or not.

Thus, after doing ethical hacking, you could carve out the vulnerability of your Personal Computer. Afterwards, you could draw some measures accordingly that would save your personal data from being in the hands of total strangers.

### Literature survey

Over the years, developer communities have grown across the world with different goals and missions but still with the general aim of providing a platform for developers to learn, interact, share ideas, support each other and grow. Some of the popular developer communities existing today are :

* + 1. **Dev.to**: DEV is a community of software developers helping one another out.DEV provides a place for developers to collaborate and network while learning and sharing their knowledge.
    2. **Women Who Code**: Women Who Code is an international nonprofit Organization that provides a global community for women in technology with events, coding resources, jobs, mentorship, and more. They aim to inspire, support, and help women develop technical skills and excel in their careers.
    3. **Site Point Community :** Site Point community is a community for web designers and developers to discuss everything web development from HTML, CSS, JavaScript, PHP, Photoshop, SEO, and more.
    4. **Indie Hackers**: Indie Hackers is a global community of developers who are sharing their projects, strategies, and revenue statistics behind their companies and side projects.

The limitations of existing developer communities are:

* + - * There is no proper provision for each user to have an exclusive

portfolio page where he/she can showcase their work and skill set.

* There is no online community for developers exclusive to a particular educational institution where students of different streams can collaborate.

## CHAPTER 2

**SOFTWARE REQUIREMENT SPECIFICATION**

### Functional Requirements

The following are various functional requirements of the project:

* User should be able to run the python script.
* User should be able to end the task(running process of python script) in the task manager.
* User should be able to login to the FTP server to retrieve log files ofkeystrokes ,also data like screenshots etc.
* User should be able to create host address for FTP login.

### Non - Functional Requirements

The following are various Non - Functional requirements of the project:

* + - **Pyhook package** : The pyHook package provides callbacks for global mouse and keyboard events in Windows. Python applications register event handlers for user input events such as left mouse down, left mouse up, key down, etc. and set the keyboard and/or mouse hook. The underlying C library reports information like the time of the event, thename of the window in which the event occurred, the value of

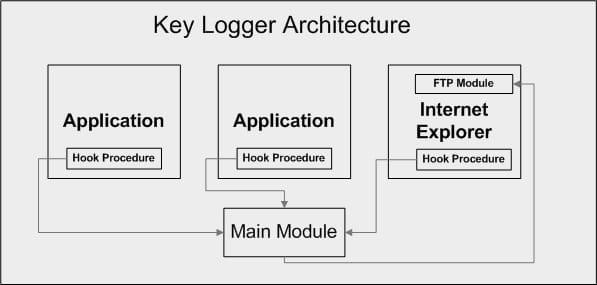
the event, any keyboard modifiers, etc. Package Pyhook consists of sub class namely HookMnager .This hook manager consists of classes like:

1. **HookConstants** : Stores internal windows hook constants including hook types, mappings from virtual keycode name to value and value to name, and event type value to name.
2. **HookEvent**: Holds information about a general hook event.
3. **HookManager:** Registers and manages callbacks for low level mouse and keyboard events.
4. **KeyboardEvent:** Holds information about a keyboard event.
5. **MouseEvent:** Holds information about a mouse event.
   * + **Python:** This keylogger software requires Python programming language to develop the code for its working. [Python](https://www.geeksforgeeks.org/python-programming-language/) is a widely used general-purpose, high level programming language. It was created by Guido van Rossum in 1991 and further developed by the Python Software Foundation. It was designed with an emphasis on code readability, and its syntax allows programmers to express their concepts in fewer lines of code. Python is a high-level, interpreted, interactive and object-oriented scripting language. Python is designed to be highly readable. It uses English keywords frequently where as other languages use punctuation, and it has fewer syntactical constructions than other languages.
       - **Python is Interpreted** − Python is processed at runtime by the interpreter. You do not need to compile your program before executing it. This is similar to PERL and PHP.
       - **Python is Interactive** − You can actually sit at a Python prompt and interact with the interpreter directly to write your programs.
       - **Python is Object-Oriented** − Python supports Object-Oriented style or technique of programming that encapsulates code within objects.
       - **Python is a Beginner's Language** − Python is a great language for the beginner-level programmers and supports the development of a wide range of applications from simple text processing to WWW browsers to games.
     + **Visual Studio:** The Visual Studio *integrated development environment* is a creative launching pad that you can use to edit, debug, and build code, and then publish an app. An integrated development environment (IDE)

is a feature-rich program that can be used for many aspects of software development. Over and above the standard editor and debugger that most IDEs provide, Visual Studio includes compilers, code completion tools, graphical designers, and many more features to ease the software development process. Several key tool windows you'll likely use in visual studio are:

* 1. **Solution Explorer** :It lets you view, navigate, and manage your code files. **Solution Explorer** can help organize your code by grouping the files into solutions and projects.
  2. The **editor window**, where you'll likely spend a majority of your time, displays file contents. This is where you can edit code or design a user interface such as a window with buttons and text boxes.
  3. **Team Explorer** lets you track work items and share code with others using version control technologies such as Git and Team Foundation Version Control (TFVC).

## Software Architecture



#### Fig.1 :Software Architecture

Keystroke logging, often referred to as keylogging or keyboard capturing, is the action of recording (logging) the keys struck on a keyboard, typically covertly, so that the person using the keyboard is unaware that their actions are being monitored.

# CHAPTER 3

## DESIGN

The project deals with different modules namely **Pyhook** and **Pyscreenshot** which are discussed below in this chapter. Also the design of the keyloggers is explained through various UML diagrams below:

### USE CASE DIAGRAM

Use case diagrams consists of actors, use cases and their relationships.The diagram is used to model the system/subsystem of an application. A single use case diagram captur es a particular functionality of a system.

Diagram

Description automatically generated

#### Fig 2 :Use Case Diagram of Keylogger

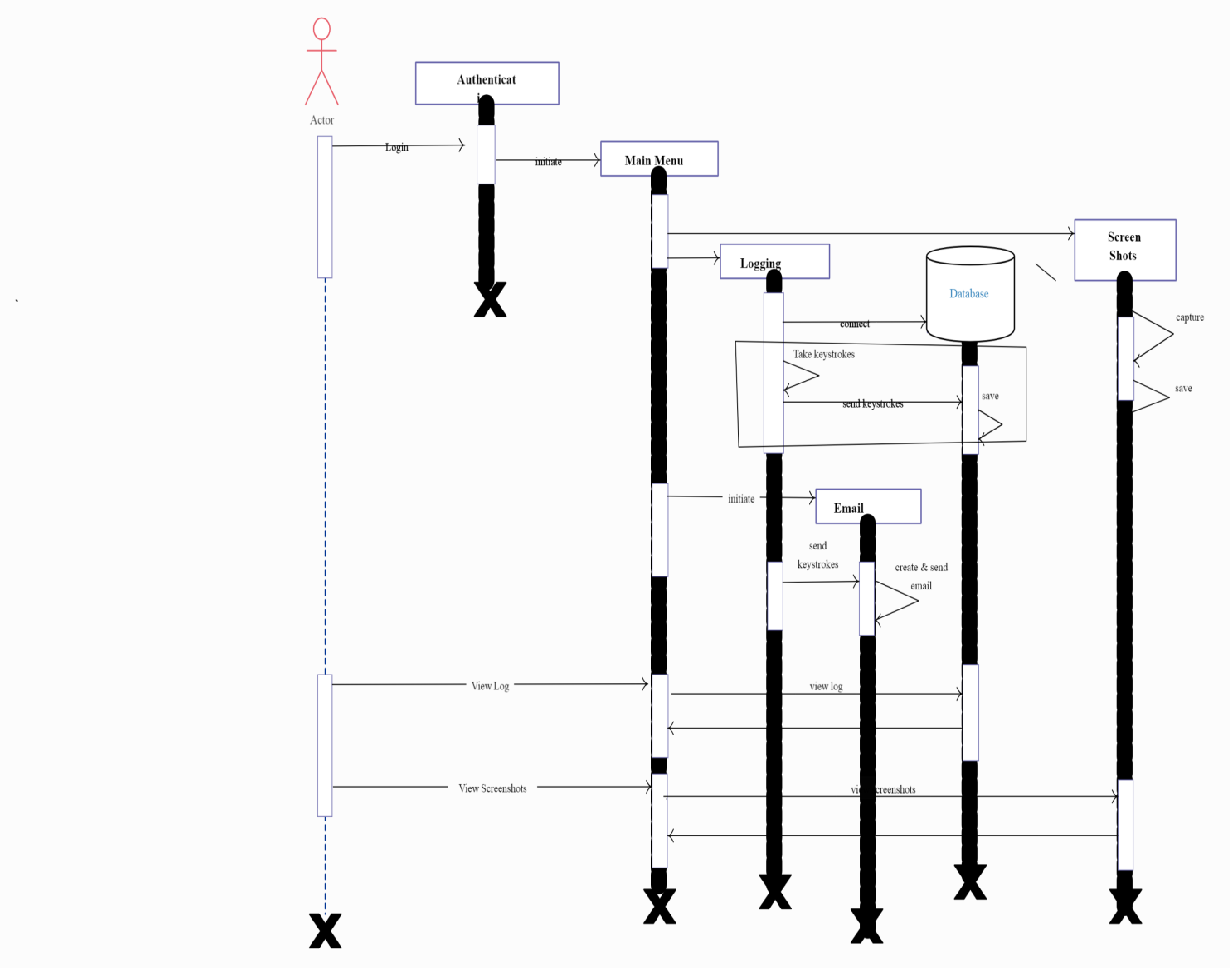
In the above Use case diagram:

* + - The actor after authentication can access the screen shots and log files from the other device
    - Also he can enable or disable the keylogger through home
    - Also an actor can change the location of the folder where the data have to be stored
    - An actor can also change the mail id to which all the log files and screenshots have to be received.



### SEQUENCE DIAGRAM

A **sequence diagram** shows object interactions arranged in time **sequence**. It depicts the objects and classes involved in the scenario and the **sequence** of messages exchanged between the objects needed to carry out the functionality of the scenario



#### Fig 3.Sequence Diagram of a Keylogger

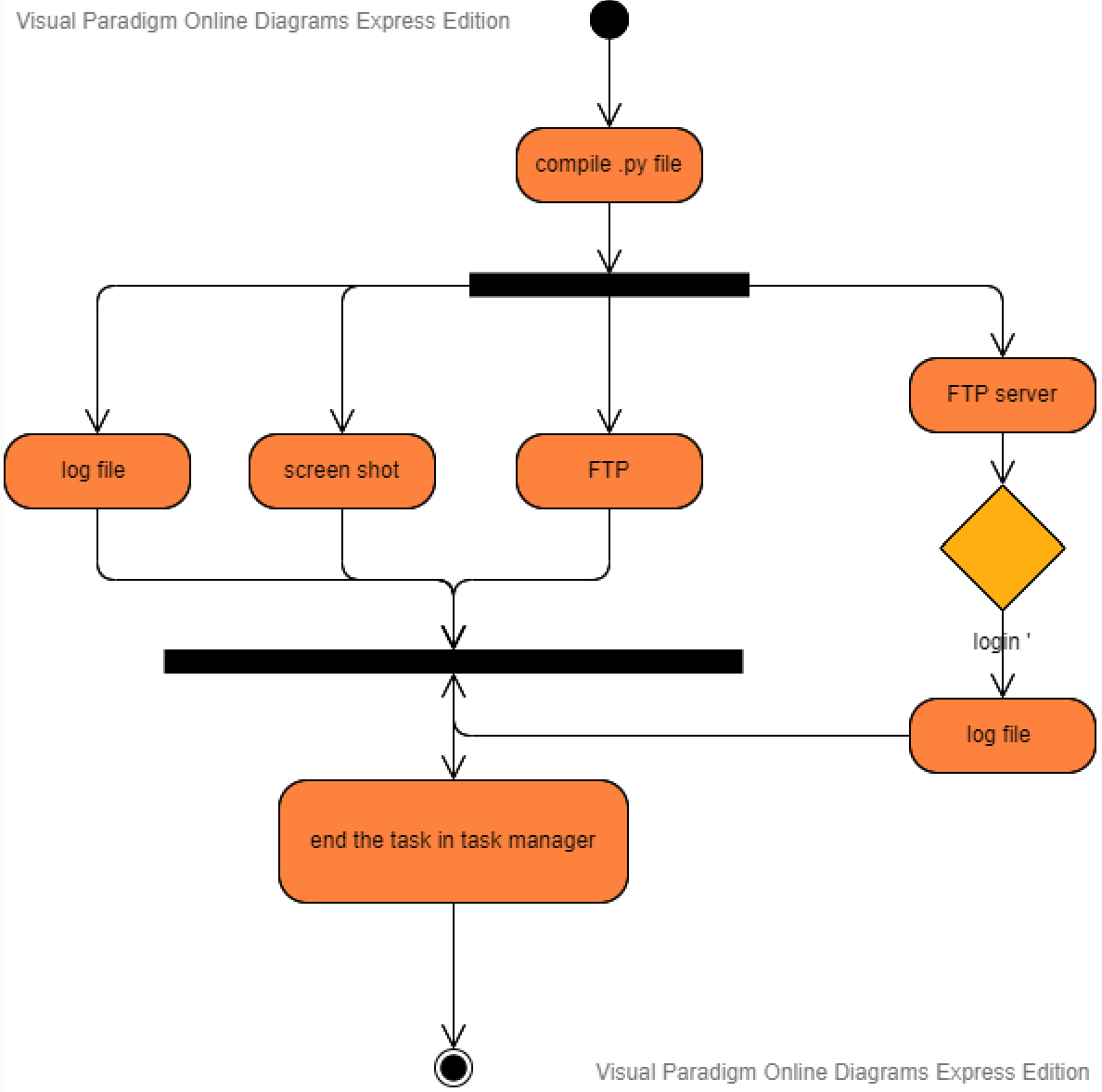
In the above Sequence diagram:

* + - Actor-User
    - Objects-Data Base, Main menu, Screenshots

The above sequence diagram depicts how the actor i.e. use acts upon the objects to retrieve the data from the other device by performing several tasks as shown in the diagram.

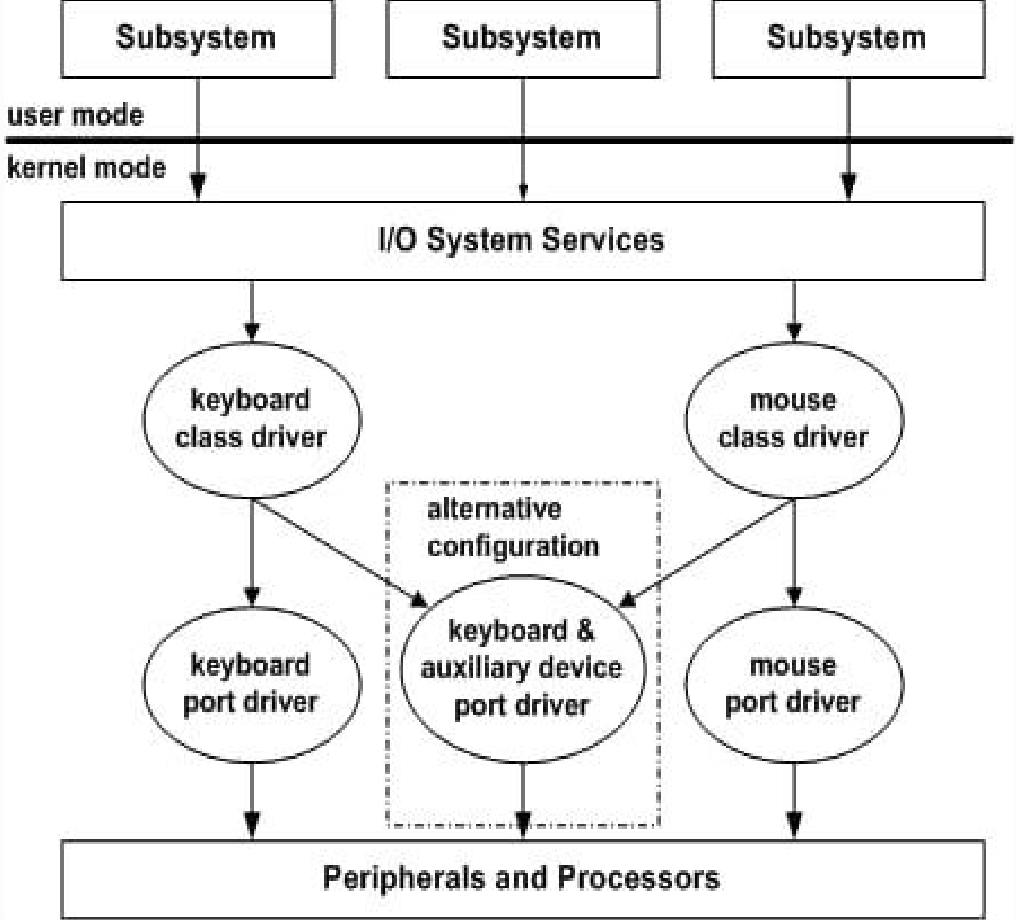
### ACTIVITY DIAGRAM

An Activity Diagram is basically a flowchart to represent the flow from one **activity** to another **activity**. The **activity** can be described as an operation of the system. The basic purpose of **activity diagrams** is to capture the dynamic behavior of the system.. It is also called object-oriented flowchart.



#### Fig 4.Activity Diagram of a Keylogger.

* 1. **SYSTEM LEVEL DIAGRAM**



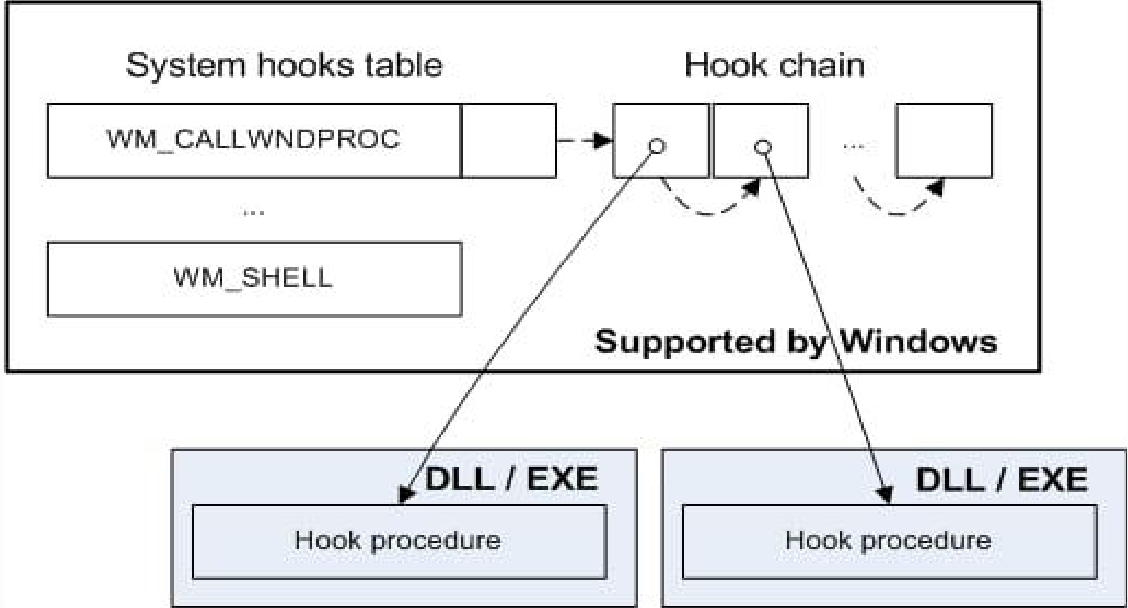
**Fig 5.System level diagram of a KeyLogger**

Regardless of how the keyboard is physically connected, keyboard drivers use keyboard class system drivers to process data. This happens regardless of the hardware used. Actually, these drivers are called class drivers because they support system requirements independent of the hardware requirements of a specific class of device.

The corresponding functional driver (port driver) supports the execution of input/ output operations in correlation with the device being used. In x86

Windows this is implemented in a single system keyboard driver (i8042) and mouse driver.

### PyHook System Diagram



#### Fig 6.pyHook internal function

The pyHook package provides callbacks for global mouse and keyboard events in Windows. Python applications register event handlers for user input events such as left mouse down, left mouse up, key down, etc. and set the keyboard and/or mouse hook. The underlying C library reports information like the time of the event, the name of the window in which the event occurred, the value of the event, any keyboard modifiers, etc.

# Chapter 4 IMPLEMENATION

Keylogger concept can be implemented by the following steps:

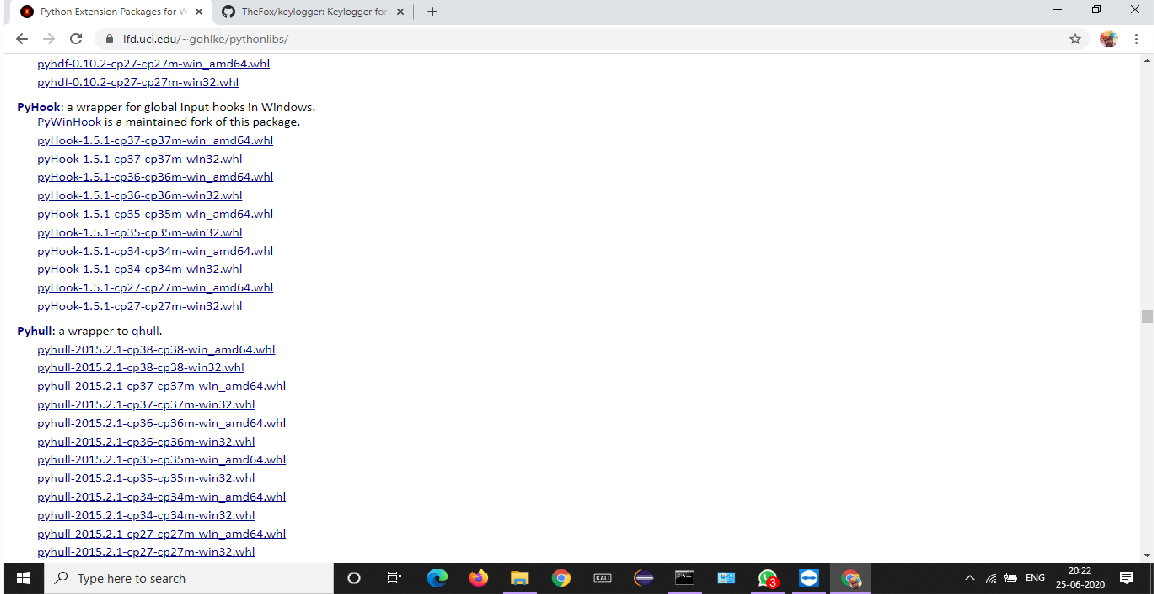
#### Step 1:

You must install python and some modules which includes :

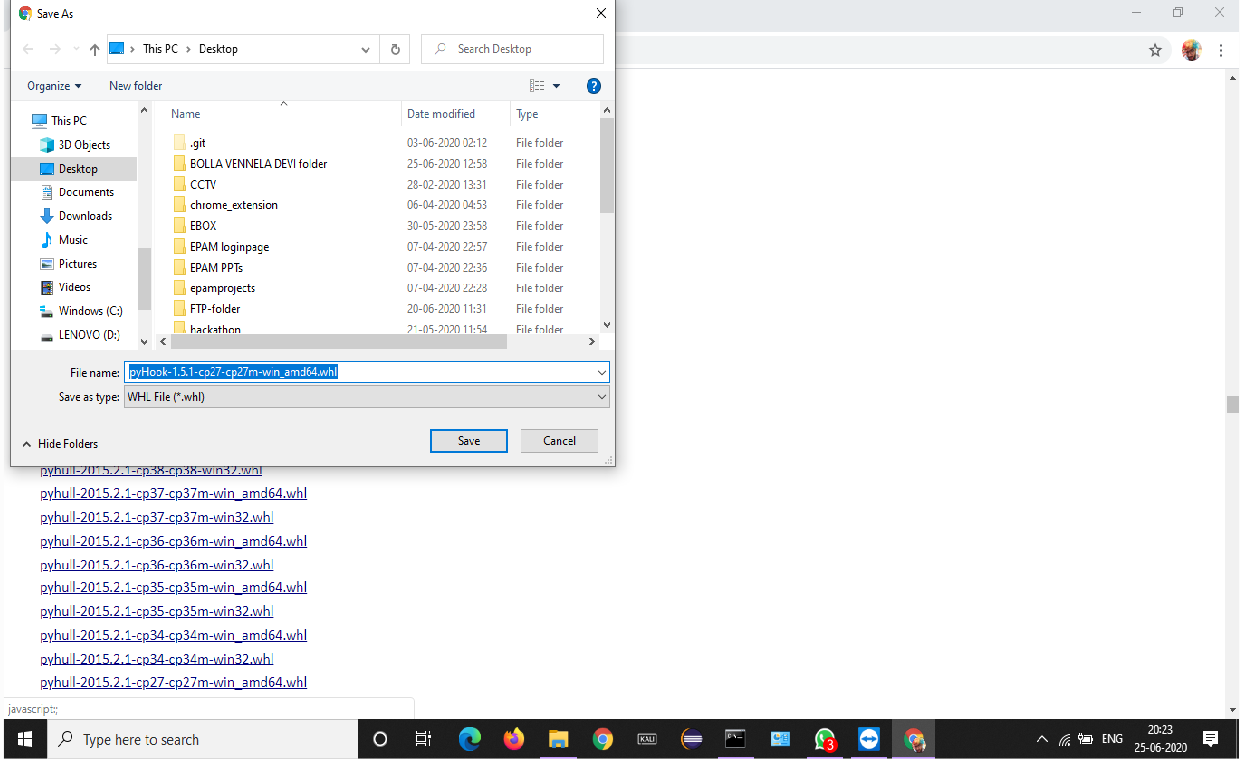
* + - Python 3.6.4
    - pyHook
    - pyscreenshot
    - pythoncom
    - pywin32



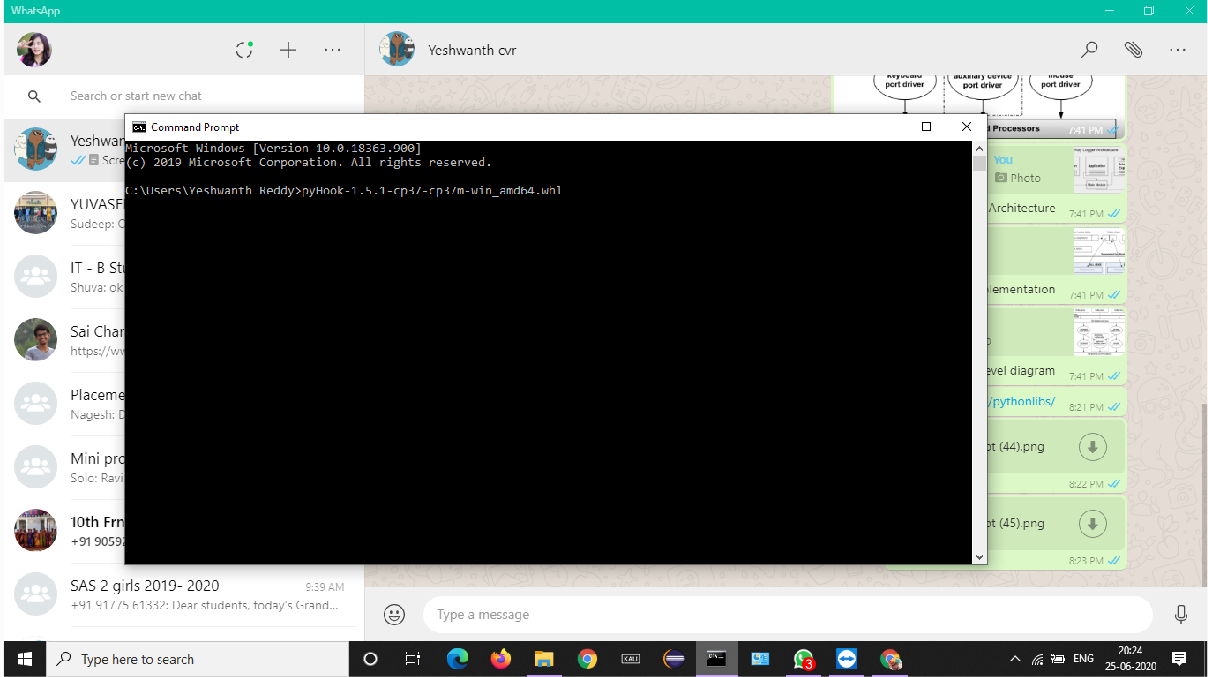
**Fig 4.1 Installation of the python software in Computer**



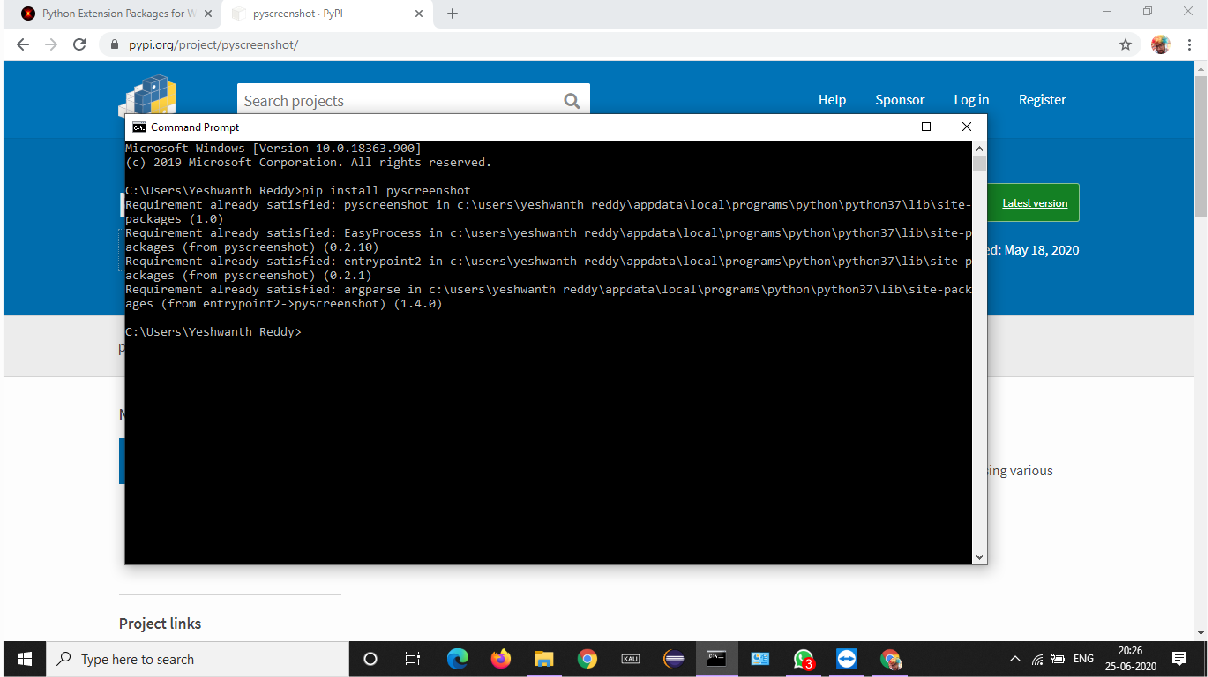
#### Fig 4.2 Download of pyhook package



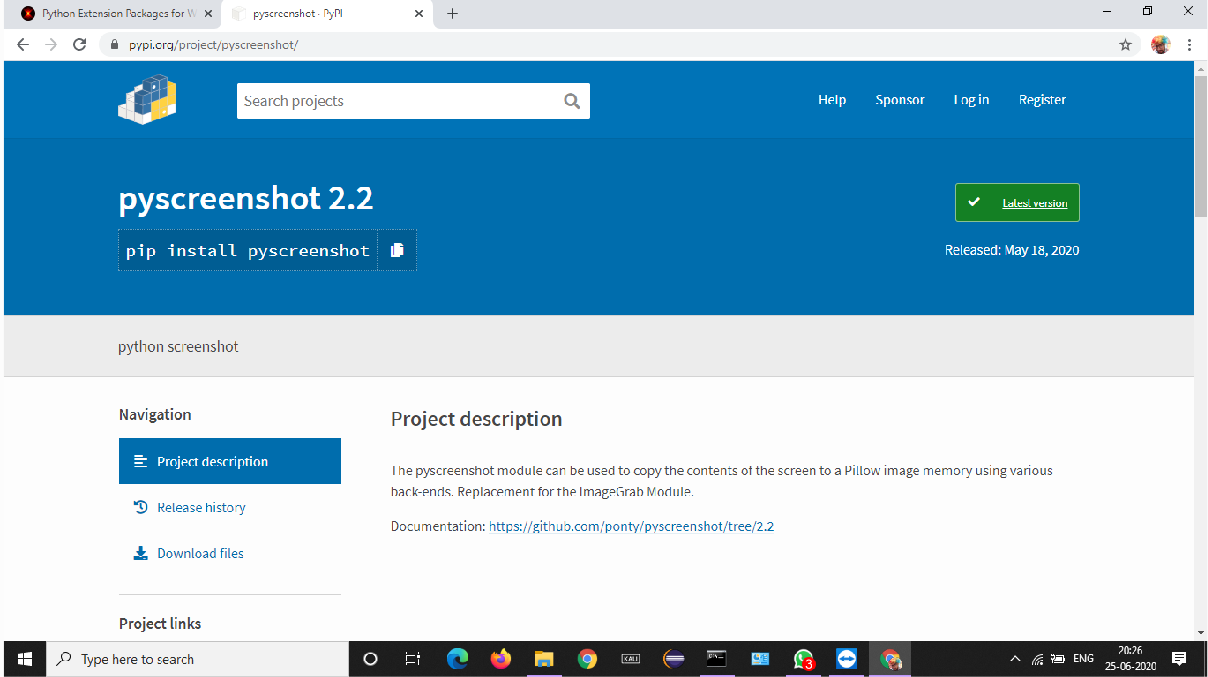
**Fig 4.3 Saving the pyhook package files in a folder after downloading**



**Fig 4.4 Installation of pyhook package files**



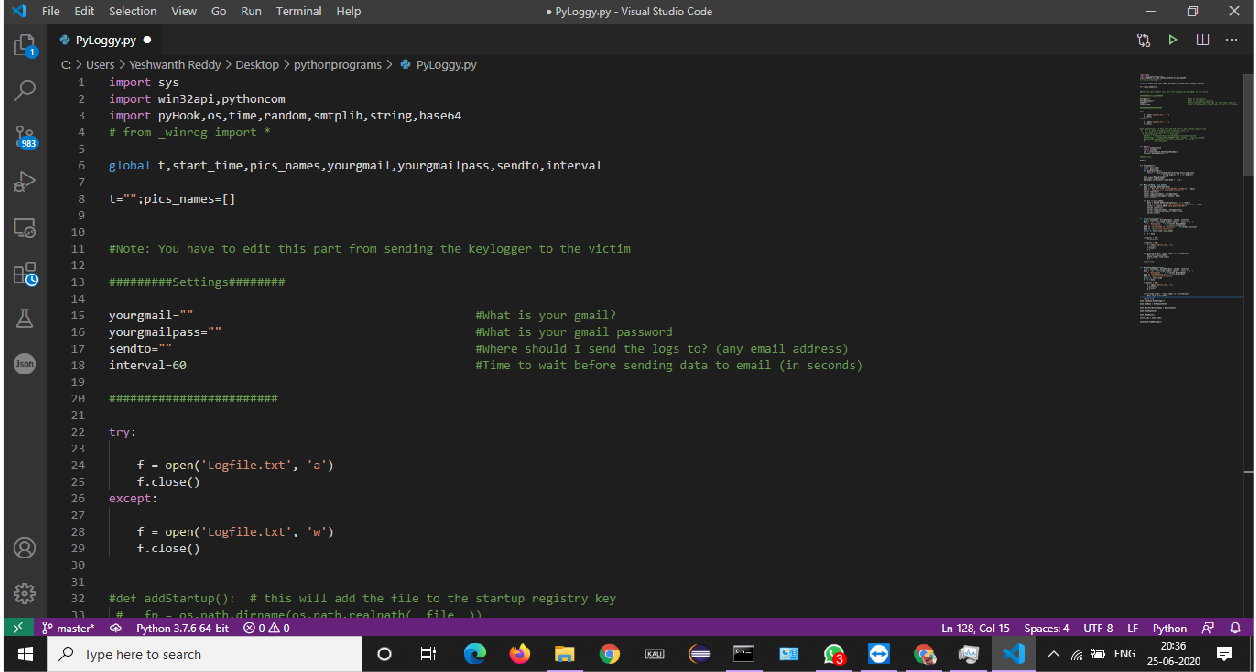
**Fig 4.5 Installation of Pyscreenshot**

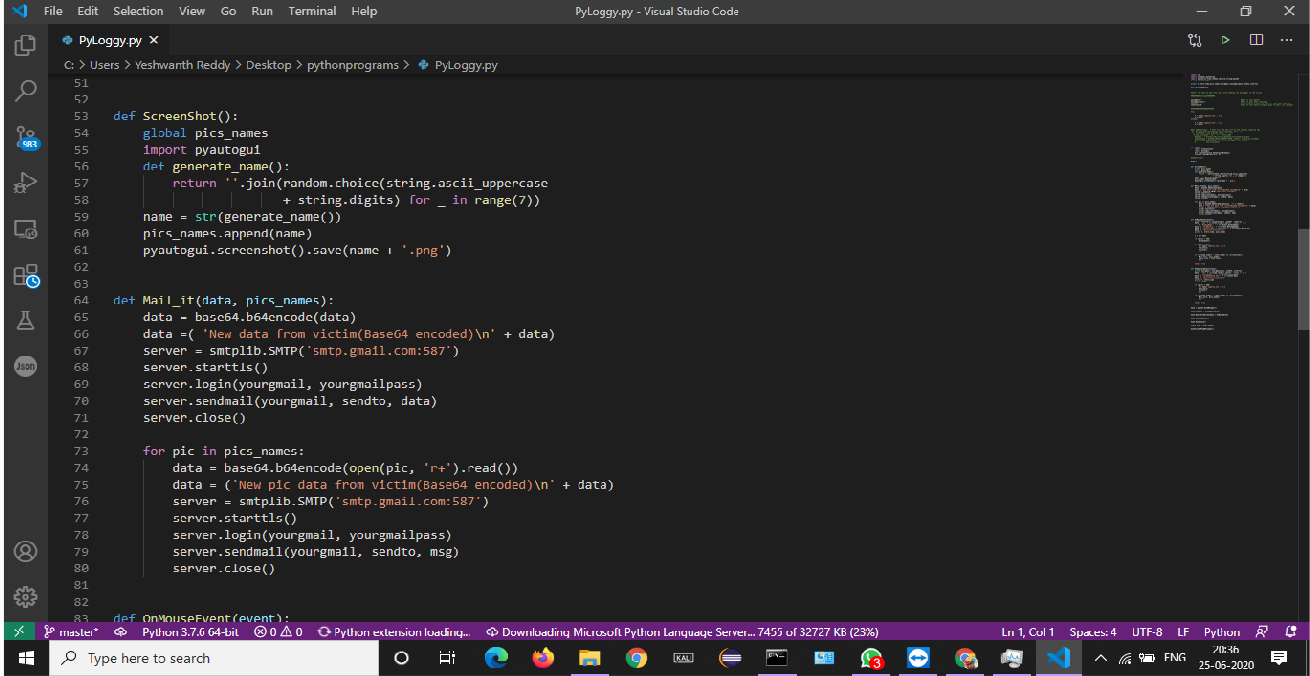


**Fig 4.6 Copy installation files link from pyscreenshot 2.2**

**Step 2:**

Once you have all the python files installed open up ide and create a new script. Then enter the following code:





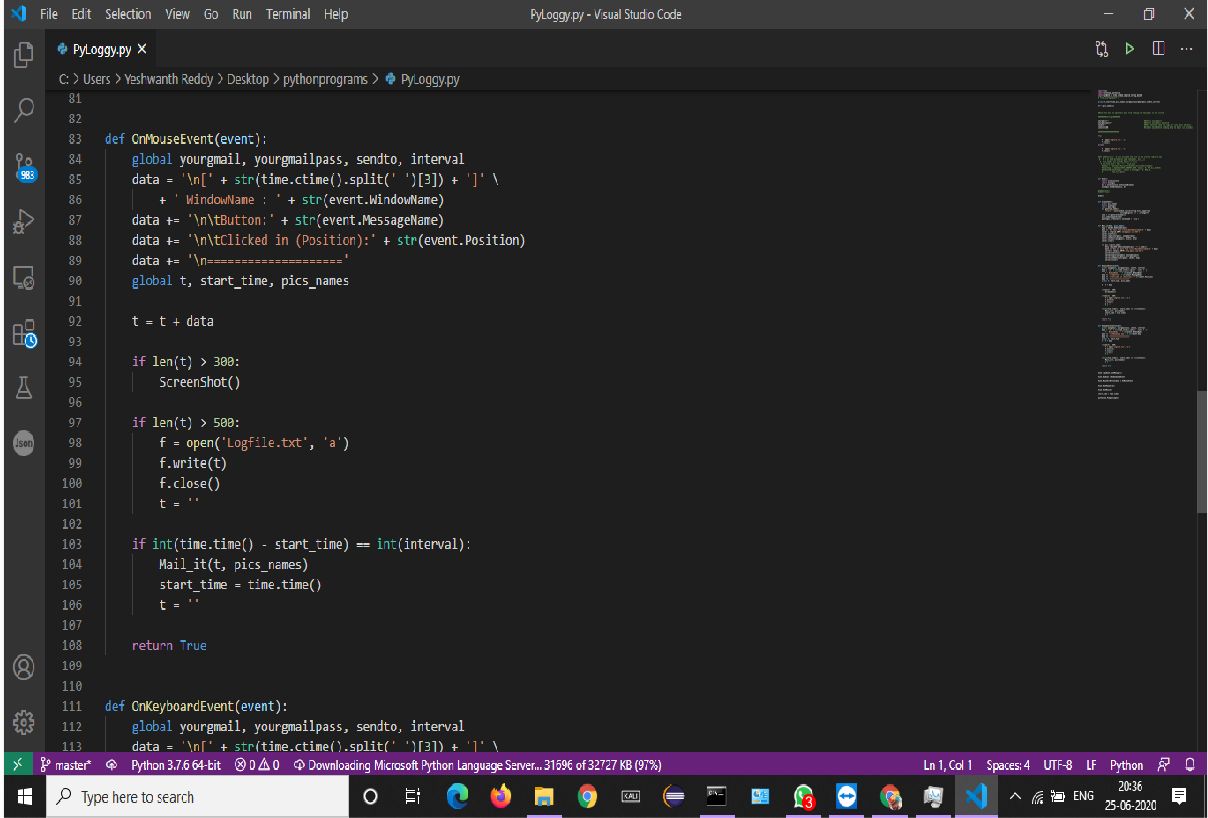
#### Fig 4.6 Python code

1. **ScreenShot():**

This function uses pyscreenshot module and captures the Screenshots until we end the task in the task manager.

#### Mail\_it():

This function uses SMTP library and sends the data i.e. log files and screenshots to the mail of the host at with a time lapse of 200 seconds between each mail.



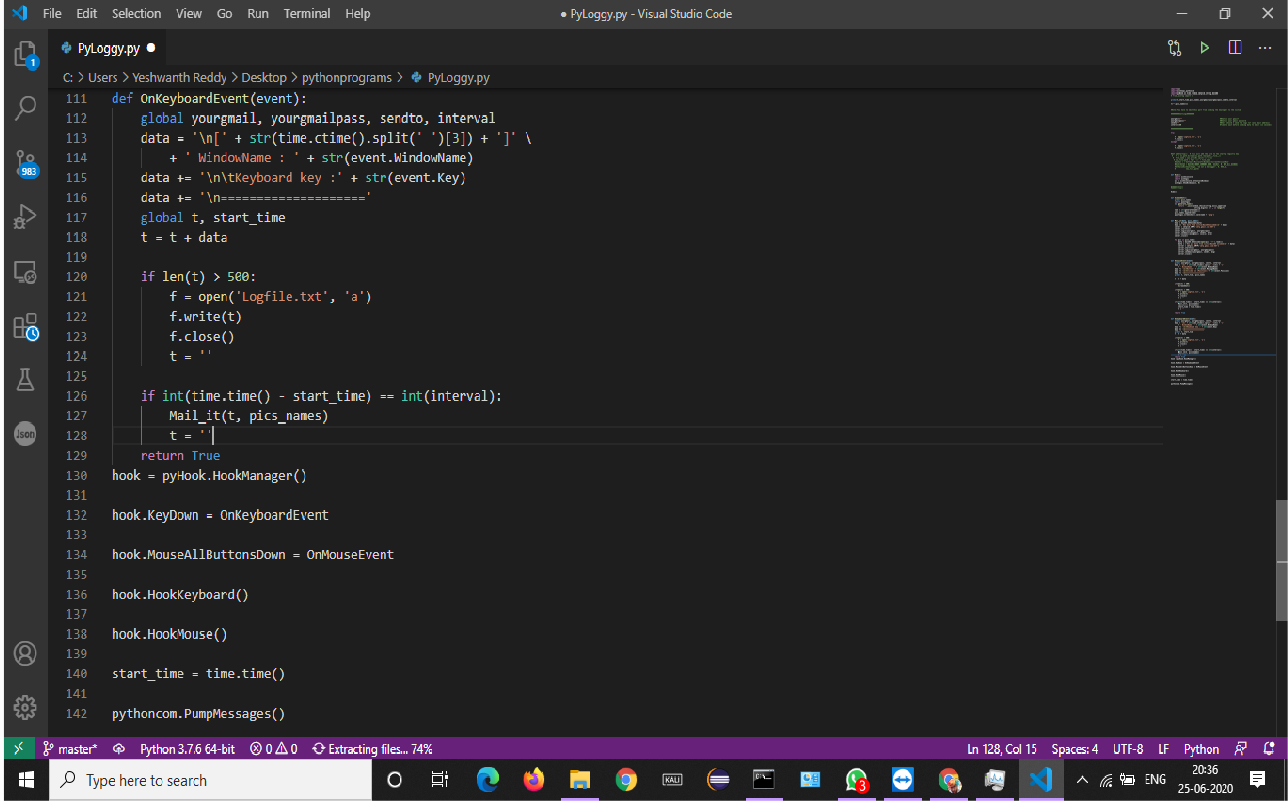
#### Fig 4.7 Python code

1. **onMouseEvent(event):**

This function gives us the information about the co- ordinates of the mouse pointer at every instant of time in the log file.

#### onKeyboardEvent(event):

This function enables us to capture the keystrokes of the data typed and is stored in the log file.



#### Fig 4.7 Python code

1. **pyHook.HookManager():**

This method is to create an object which helps in capturing keystrokes and present this in the log file.

#### pythoncom.PumpMessages():

Pumps all messages for the current thread until a WM\_QUIT message is encountered.

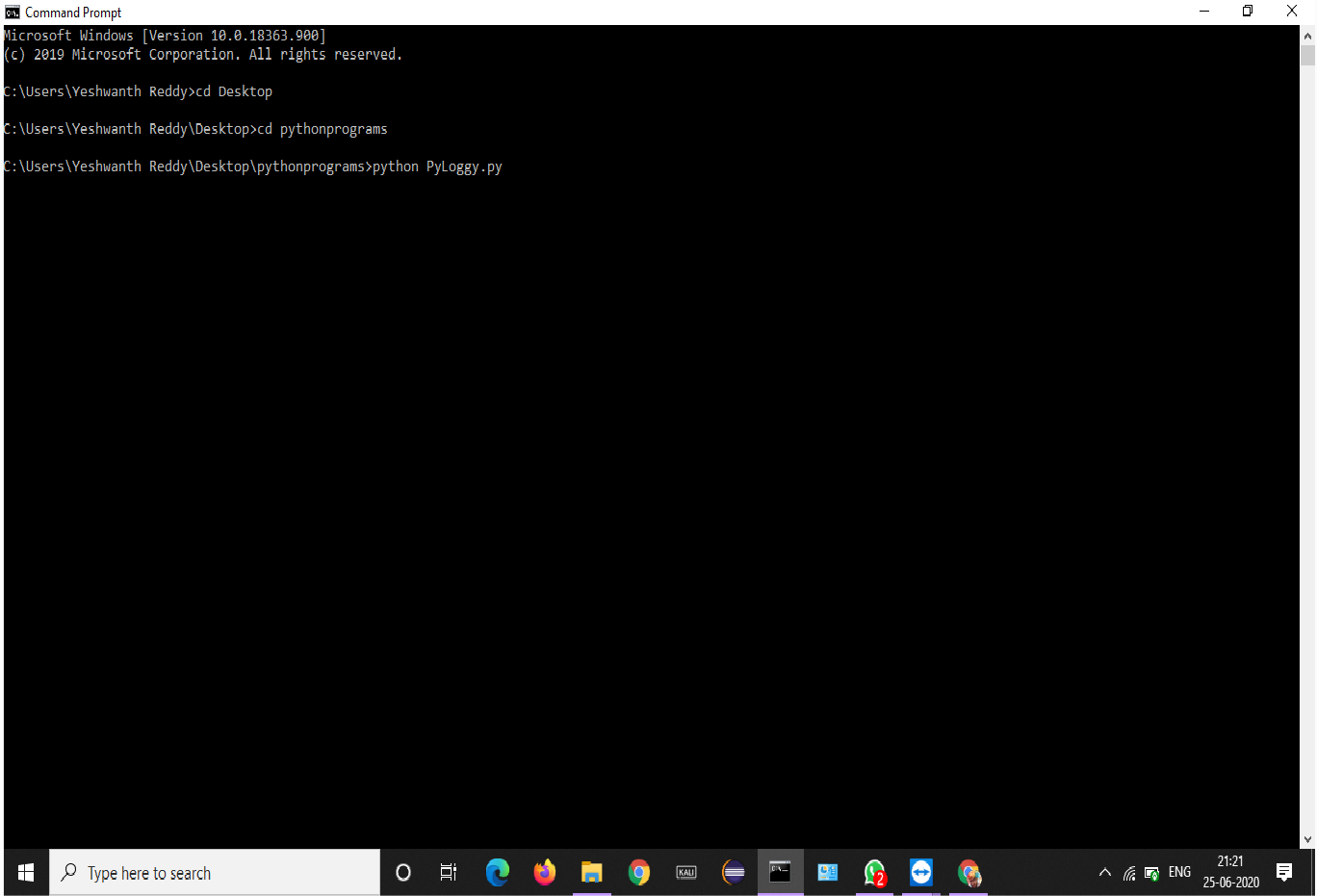
#### Step 3:

After entering the code save it with .py extension in a folder .

#### Fig 4.8 Saving the python program file ina folder

**Step 4:**

Now open the command prompt and run the above code based on the filepath,so that it runs in the background.



#### Fig 4.9 Running the code in the command prompt

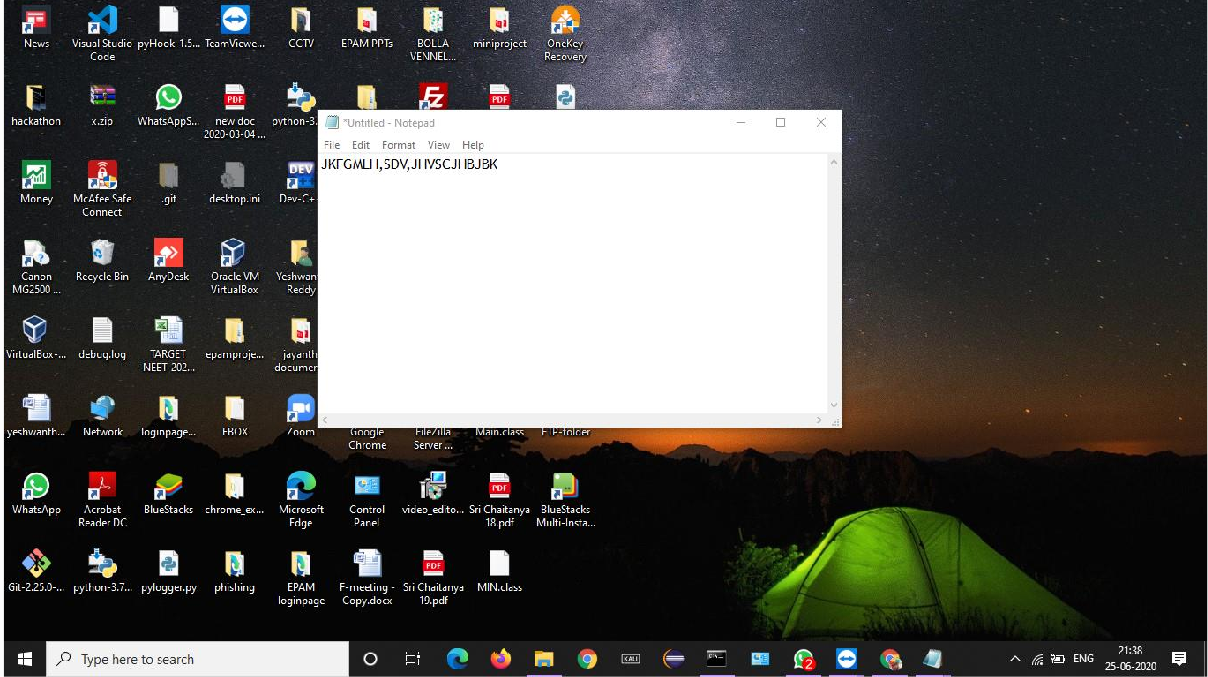
**Chapter 5**

**TESTING**

The project is tested upon various test cases whose details and corresponding results are described in this chapter.

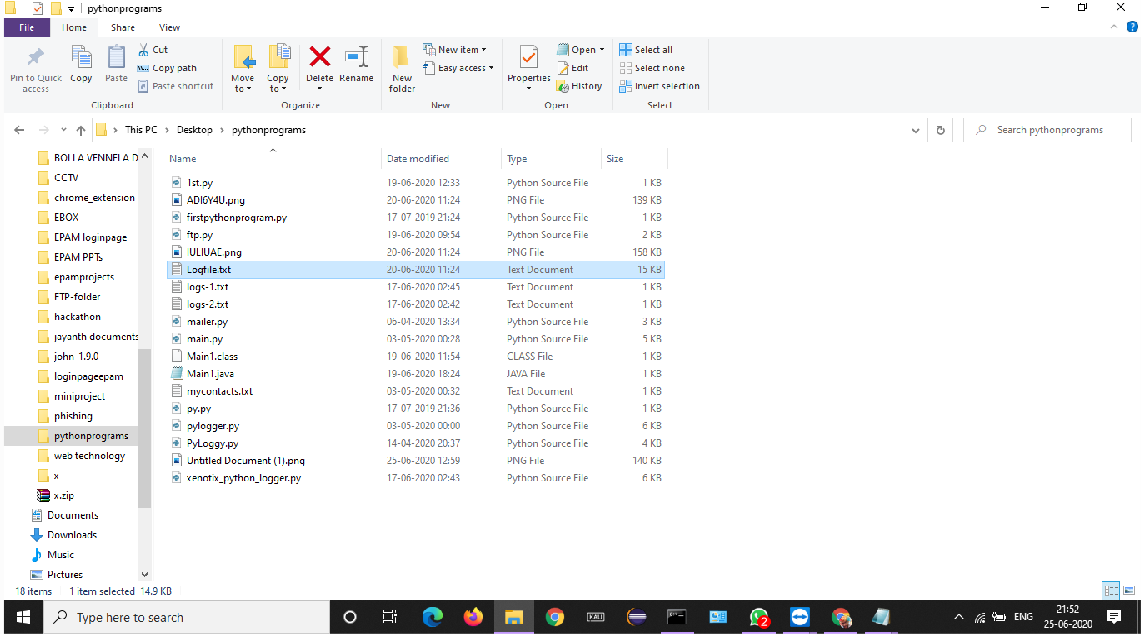
#### Sample Test Case 1:

**O**pen notepad and type any text in it



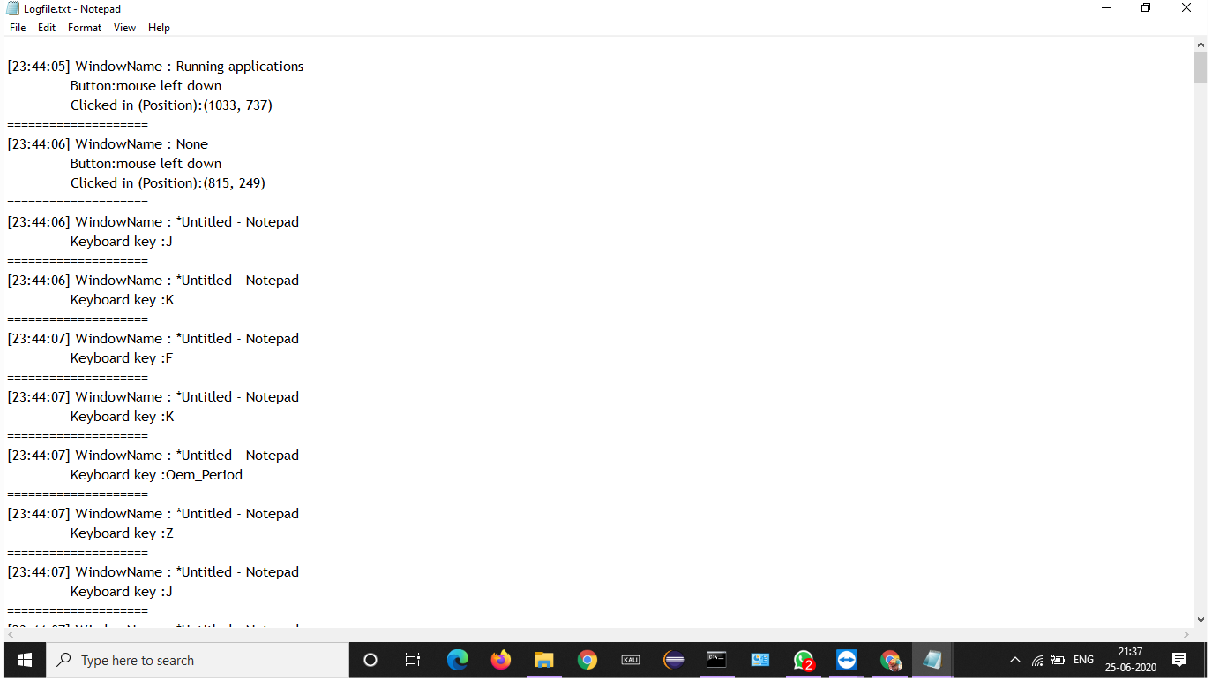
#### Fig 5.1 Entering some text into the notepad

Now this data gets stored into a log file with **.txt** extention in the folder where our python program is saved



#### Fig 5.2 Log file of the text we have entered

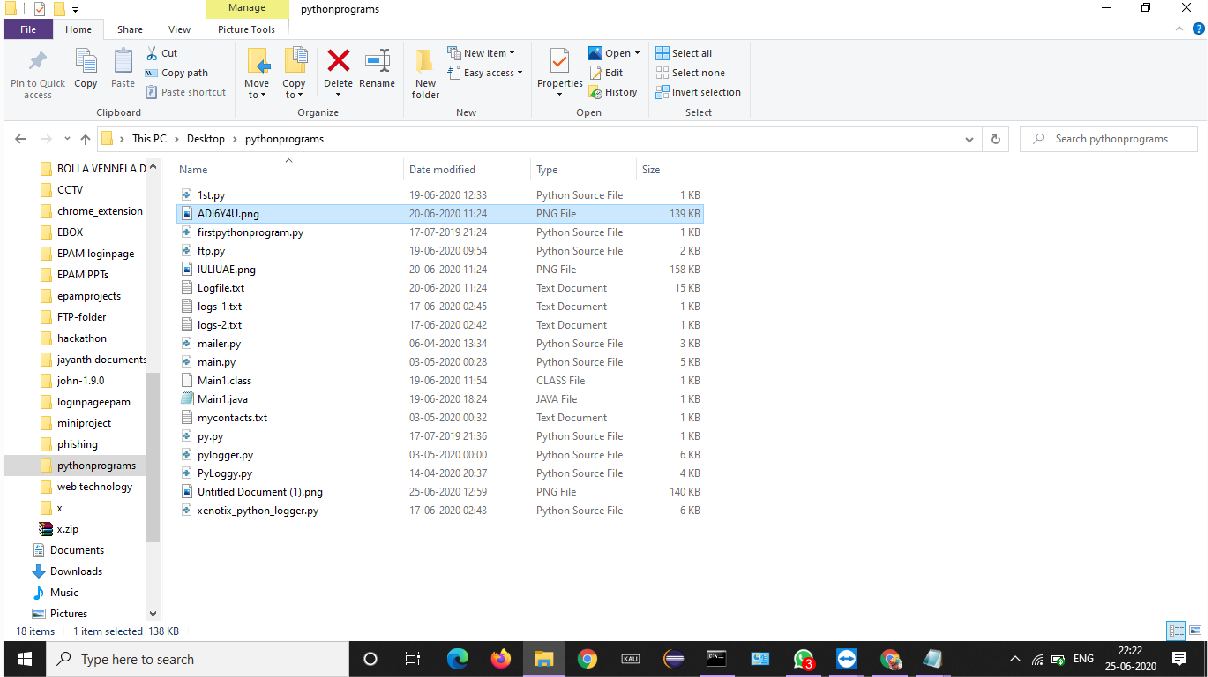
This logfile consists of the keystrokes of the text we have entered in the notepad. It is shown below:



#### Fig 5.3 Log file

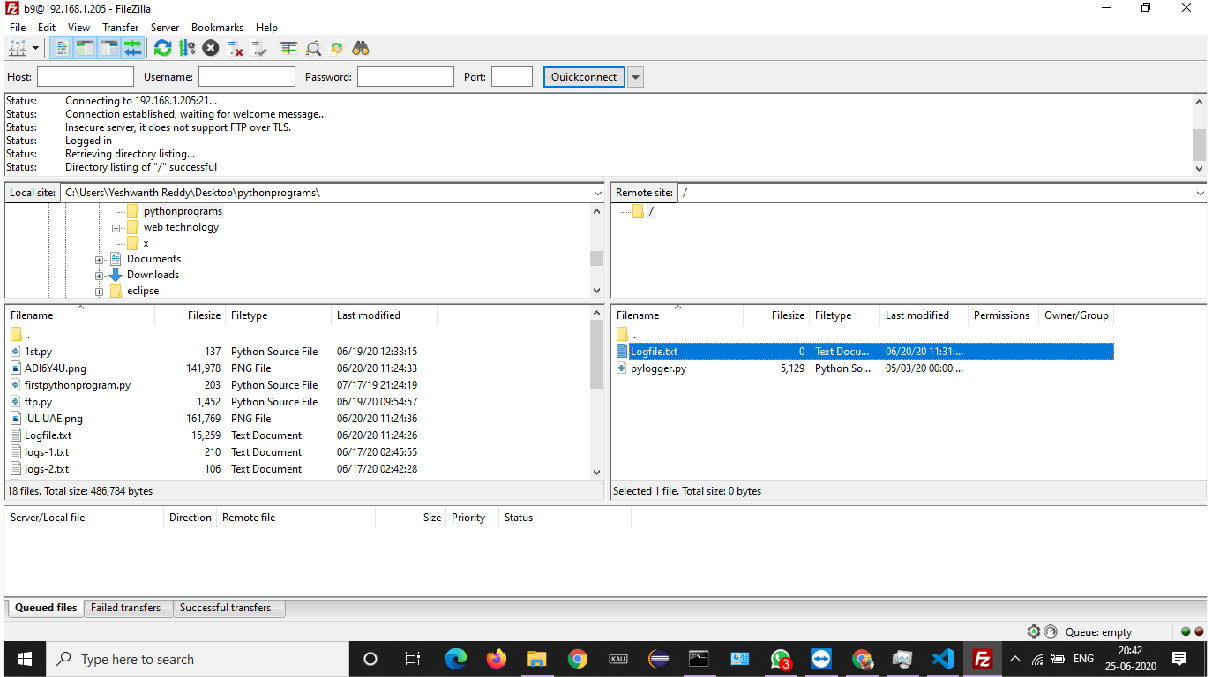
Also the screenshots of the window are captured are captured and stored with

.png extension in the same folder.It is shown below:



#### Fig 5.4 Screenshots stored in .png format

This process of capturing screenshots continues unless we end the process in the task manager .Also the log file is transferred to the host through FTP(File Transfer Protocol)server .This process is shown below:

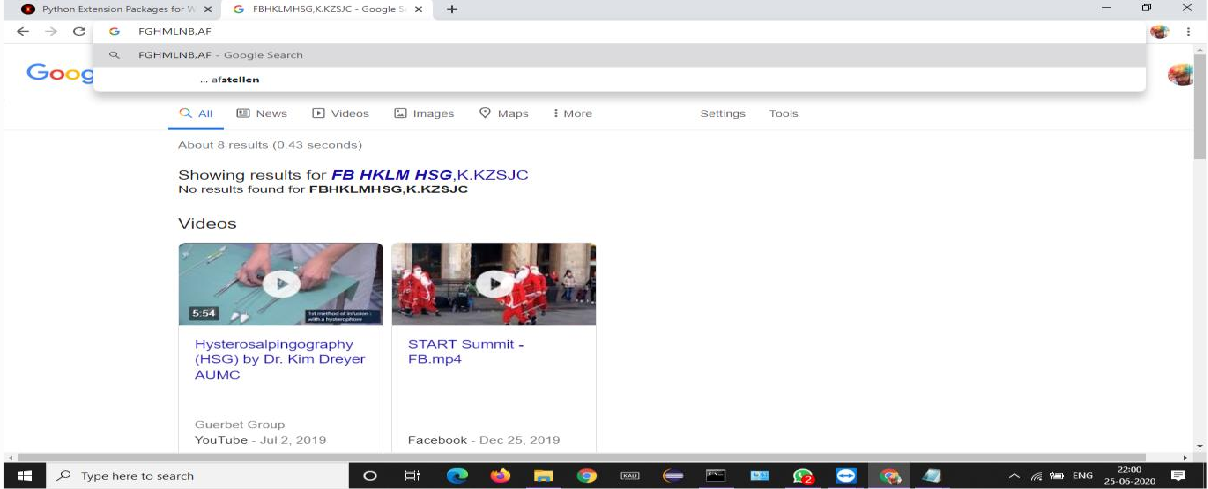


#### Fig 5.5 Log files are transferred through FTP to host

These log files are sent to host at regular intervals of time through FTP. The time lapse between the intervals of sending the log files is 200 seconds.

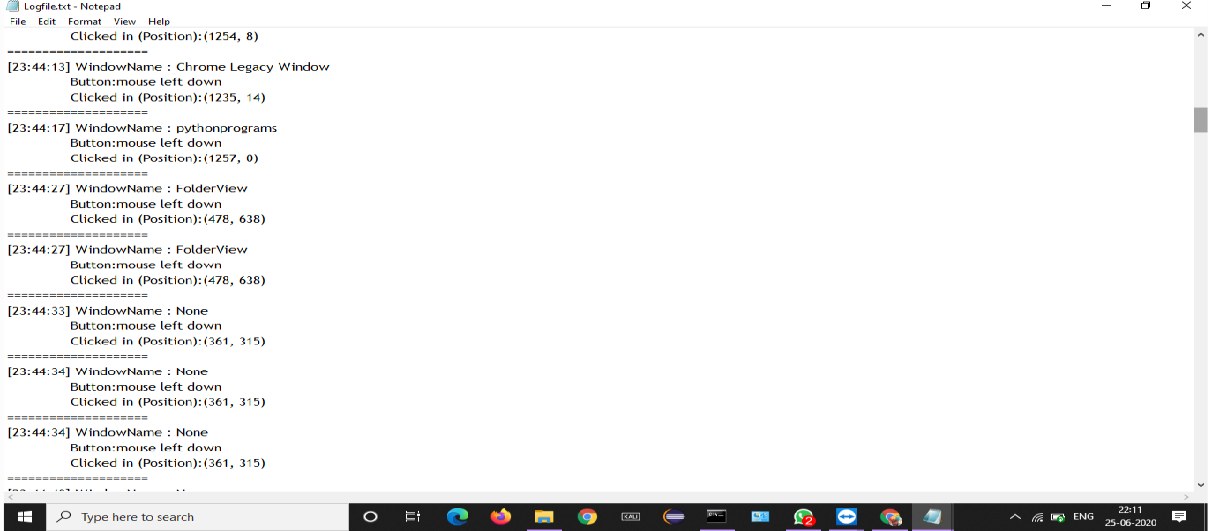
**Sample Test Case 2:**

Open google chrome tab, type any text in search box



#### Fig 5.6 Text entered in search box

Now, a log file based on the above search text will be stored in .txt format in the folder where our python file is stored



#### Fig 5.7 Log file of the text entered in google search box

# CONCLUSION

Software keyloggers may be augmented with features that capture userinformation without relying on keyboard key presses as the sole input. Some ofthese features include:

* **Clipboard logging:** Anything that has been copied to the clipboard can be captured by the program.
* **Screenlogging:** Screenshots are taken to capture graphics-based information. Applications with screen logging abilities may take screenshots of the whole screen, of just one application, or even just around the mouse cursor. They may take these screenshots periodically or in response to user behaviors (for example, when a user clicks the mouse). A practical application that is used by some keyloggers with this screen logging ability, is to take small screenshots around where a mouse has just clicked; thus defeating web-based keyboards (for example, the web-based screen keyboards that are often used by banks), and any web-based on- screen keyboard without screenshot protection.
* Programmatically capturing the text in a control. The Microsoft Windows API allows programs to request the text 'value' in some controls. This means that some passwords may be captured, even if they are hidden behind password masks (usually asterisks).
* The recording of every program/folder/window opened including a screenshot of every website visited.
* The recording of search engines queries, instant messenger conversations, FTP downloads and other Internet-based activities (including the bandwidth used)

# References

* + [https://www.researchgate.net/journal/0278- 0097\_IEEE\_Technology\_and\_Society\_Magazine](https://www.researchgate.net/journal/0278-0097_IEEE_Technology_and_Society_Magazine)
  + <https://www.geeksforgeeks.org/introduction-to-keyloggers/>
  + [https://tutorialspoint.dev/language/python/design-a-keylogger-in-](https://tutorialspoint.dev/language/python/design-a-keylogger-in-python) [python](https://tutorialspoint.dev/language/python/design-a-keylogger-in-python)

*)*

## Appendix A – Abbreviations

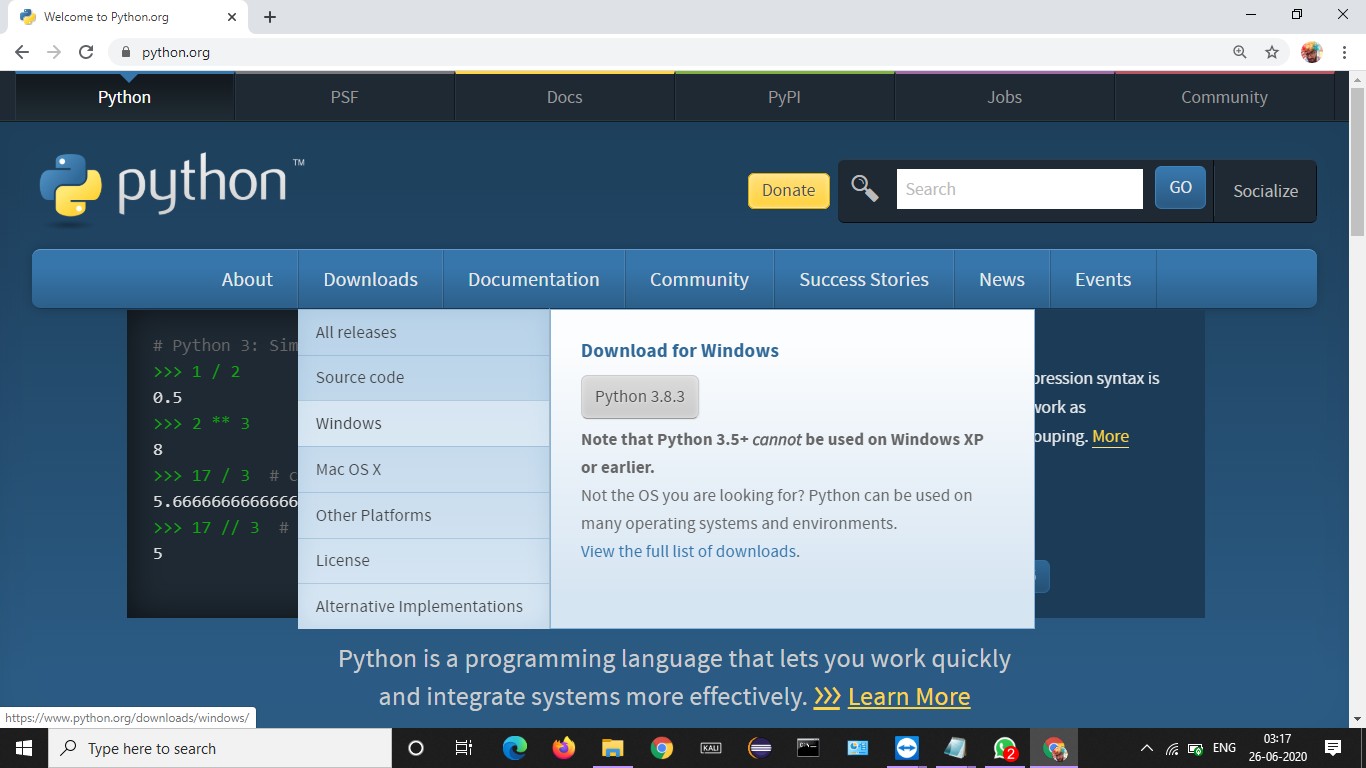
* + FTP-File Transfer Protocol
  + SMTP-Simple Mail Transfer Protocol
  + COM-Component Object Model
  + API-Application Program Interface
  + OS- Operating System

## Appendix B – Software installations

#### Python installation:

**Step 1 -** Download the Python 3 Installer

Open a browser window and navigate to the Download page for Windows at **python.org.**

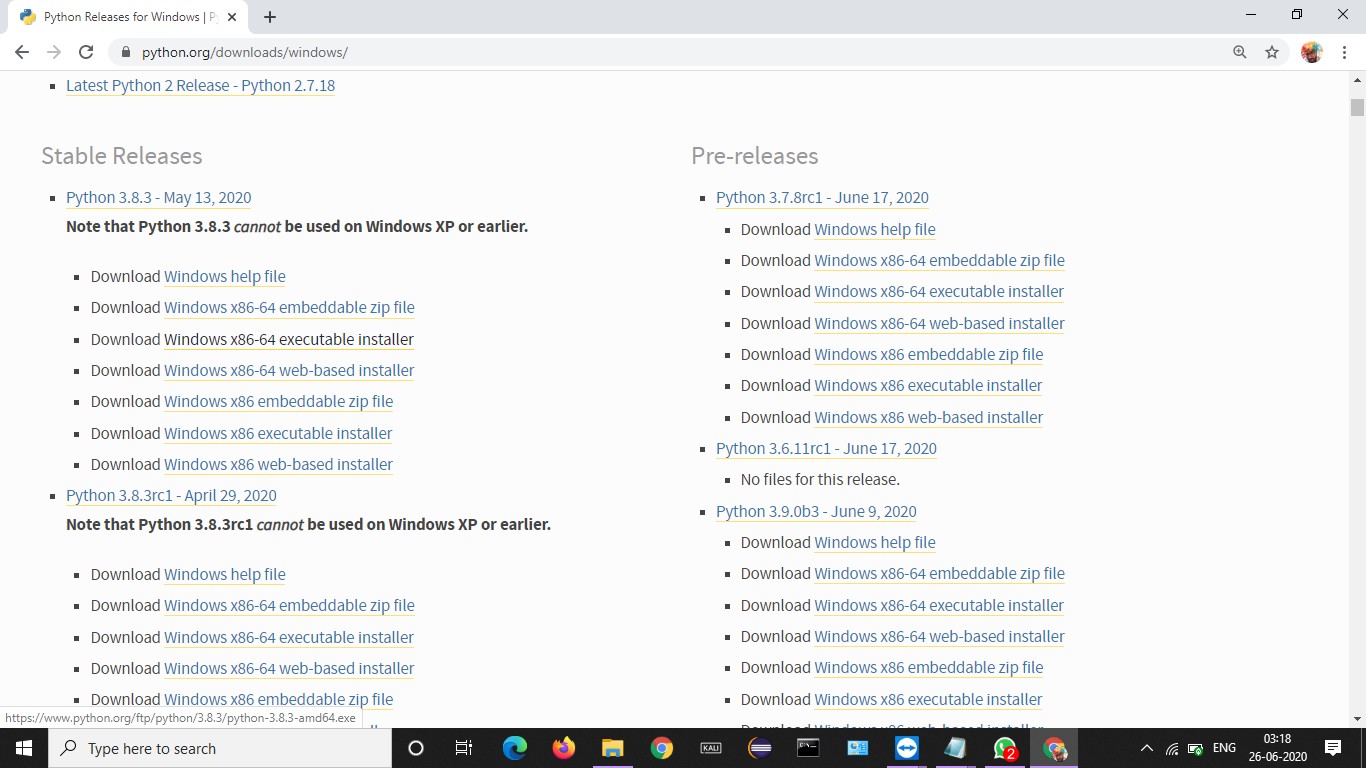


#### Fig a: Downloading python software

1. Underneath the heading at the top that says **Python Releases for Windows**, click on the link for the **Latest Python 3 Release – Python**

**3.x.x**. (As of this writing, the latest is Python 3.6.5.)

1. Scroll to the bottom and select either **Windows x86-64 executable installer** for 64-bit or **Windows x86 executable installer** for 32-bit



#### Fig b : Choosing the version of Python software

**Step 2- Run the Installer**

Once you have chosen and downloaded an installer, simply run it by double-clicking on the downloaded file. A dialog should appear that looks something like this:



#### Fig c: Installing the Python

Then just click **Install Now**. That should be all there is to it. A few minutes later you should have a working Python 3 installation on your system.

## Appendix C – Software Usage Process

* 1. Create a python file store with .py extension in a folder
  2. Run the python in the command prompt by mentioning the specified path
  3. This python runs in the background until the task is ended in the task manager
  4. pyHook helps in keyStroking and storing it in a log file .
  5. .File transfer protocol helps in transferring the log files and screenshots to the host (Server) address.