A

Major Project Report on

Activity Monitoring Tool for Windows using Keystroke Logging

Submitted in the Partial Fulfillment of the Requirements
for the Award of the Degree of

BACHELOR OF TECHNOLOGY

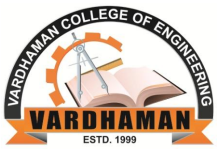
IN

COMPUTER SCIENCE AND ENGINEERING

Submitted by

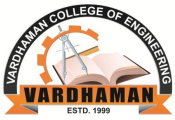
Asam Vivek Vardhan	**18881A0502**
Sajja Sai Teja	**18881A0553**

Under the esteemed guidance of
Dr. M. A. Jabbar
Professor & Head, CSE (AI & ML)



Department of Computer Science and Engineering
VARDHAMAN COLLEGE OF ENGINEERING, HYDERABAD
An Autonomous Institute, Affiliated to JNTUH

2021-22



VARDHAMAN COLLEGE OF ENGINEERING, HYDERABAD

An Autonomous Institute, Affiliated to JNTUH

Department of Computer Science and Engineering

CERTIFICATE

This is to certify that the project titled **Activity Monitoring Tool for Windows using Keystroke Logging** is carried out by

Asam Vivek Vardhan	**18881A0502**
Sajja Sai Teja	**18881A0553**

in partial fulfillment of the requirements for the award of the degree of **Bachelor of Technology** in **Computer Science and Engineering** during the year 2021-22.

Signature of the Supervisor
Dr. M. A. Jabbar
Professor & Head,
CSE (AI & ML)

Signature of the HOD
Dr. Ramesh Karnati
Associate Professor & Head,
CSE

Project Viva-voce held on _____

Internal Examiner **External Examiner**

Kacharam (V), Shamshabad (M), Ranga Reddy (Dist.)–501218, Hyderabad, T.S.
Ph: 08413-253335, 253201, Fax: 08413-253482, www.vardhaman.org

Acknowledgement

The satisfaction that accompanies the successful completion of the task would be put incomplete without the mention of the people who made it possible, whose constant guidance and encouragement crown all the efforts with success.

We wish to express our deep sense of gratitude to **Dr. M. A. Jabbar**, Professor & Head, CSE (AI & ML) and Project Supervisor, Vardhaman College of Engineering, for his able guidance and useful suggestions, which helped us in completing the project in time.

We are particularly thankful to **Dr. Ramesh Karnati**, the Head of the Department, Department of Computer Science and Engineering, his guidance, intense support and encouragement, which helped us to mould our project into a successful one.

We show gratitude to our honorable Principal **Dr. J.V.R. Ravindra**, for providing all facilities and support.

We avail this opportunity to express our deep sense of gratitude and heartful thanks to **Dr. Teegala Vijender Reddy**, Chairman and **Sri Teegala Upender Reddy**, Secretary of VCE, for providing a congenial atmosphere to complete this project successfully.

We also thank all the staff members of Computer Science and Engineering department for their valuable support and generous advice. Finally thanks to all our friends and family members for their continuous support and enthusiastic help.

Asam Vivek Vardhan

Sajja Sai Teja

Abstract

In recent years information and communication technology has become an important part of human life. Most of the organizations facing challenges in maintaining the security about information of company as behaviour of the employee have major effect on organization information security. We thought of building a tool which can monitors the employee's behavior without actually monitoring the employees. This paper mainly focuses to propose a real time key logger for monitoring the activities of employees within an organization. The real time key logger such as Activity Monitoring tool monitors the employee behavior based on the employee inputs such as Key logs, Screenshots, Microphone, System and Network information. Inputs from employee's stored in the employee system in the form of log files based on type of the input the employee encountered with the system and these files sent through email to admin. So that Employee's activities can be monitored easily and take the certain actions based on the company terms and conditions sent through email to admin against the employee to maintain security within organization effectively.

Keywords: Cybersecurity, Information Security, Detection, Tracking, Monitoring, Keylogger, Keystroke, Screenshots, Microphone, Network Information, System Information, Email.

Table of Contents

List of Tables

List of Figures

Abbreviations

Abbreviation	Description
VCE	Vardhaman College of Engineering
IEEE	Institute of Electrical and Electronics Engineers
PC	Personal Computer
CPU	Central Processing Unit
RAM	Random Access Memory
OS	Operating System
LOG	Log File
EMAIL	Electronic Mail
HTTP	Hypertext Transfer Protocol
MIME	Multipurpose Internet Mail Extensions
RE	Regular Expression
SMTPLIB	Simple Mail Transfer Protocol Library
TXT	Text File
XML	Extensible Markup Language
UML	Unified Modeling Language
ER MODEL	Entity-Relationship Model
DFD	Data Flow Diagram
API	Application programming interface
MB	Megabyte
DWM	Dynamic Wireless Medium
BIOS	Basic Input/Output System
BSD	Berkeley Software Distribution
CSRSS	Client-Server Runtime Process
DHCP	Dynamic Host Configuration Protocol
IP	Internet Protocol

TCP	Transmission Control Protocol
NETSH	Network shell
WAN	wide area network
IPV4	Internet Protocol version 4
IPV6	Internet Protocol version 6
IET	Institution of Engineering and Technology
WAV	Waveform Audio File Format
JPG	Joint Photographic Experts Group

CHAPTER 1

INTRODUCTION

1.1 Motivation

The processes or techniques of securing information through limiting information risk policies referred as information security. It invariably entails preventing or decreasing the likelihood of unauthorized/inappropriate data access, moreover as illicit data usage, disclosure, interruption, deletion, corruption, alteration, inspection, recording, or devaluation of knowledge [1].

Implementing correct security controls will initial assist a company in reducing risk to acceptable levels. Controls can take many forms, but all of them serve to secure the confidentiality, integrity, and accessibility of knowledge. data security implementations that are smart and embrace applicable security controls can have an enormous impact on academic degree organization's security. New methodologies and technologies are fast rising inside the discipline, allowing information security to be applied to a broader vary of problems at intervals academic degree organisation. Within an enterprise, information security are typically accustomed manufacture solutions that believe on necessary volumes of knowledge security and security controls [2].

Organisations have to be compelled to be compelled to resolve the protection of data from data security breaches once crime of knowledge occur internally. In most cases it is determined that thefts and sabotage [3] of knowledge are caused mostly by their workers itself. the foremost intention of employee was to make data leak to the third party persons for his or her personal finance. Organisations need to realized that it's basic responsibility to be taken from the employee to not theft and leak the direction and misuse them inside the suggests that of finance. despite the actual fact that organisation scan the protection of their data from a technology issue, but fail to understand the importance that management plays essential roles in protecting their systems

with the creation of knowledge.

The term "keystroke logging," often known as "keylogging," refers to the process of recording the keys that are pressed on a keyboard. This can be accomplished in a number of ways, employing a variety of hardware and software.

There are two basic types of keyloggers, hardware and software:

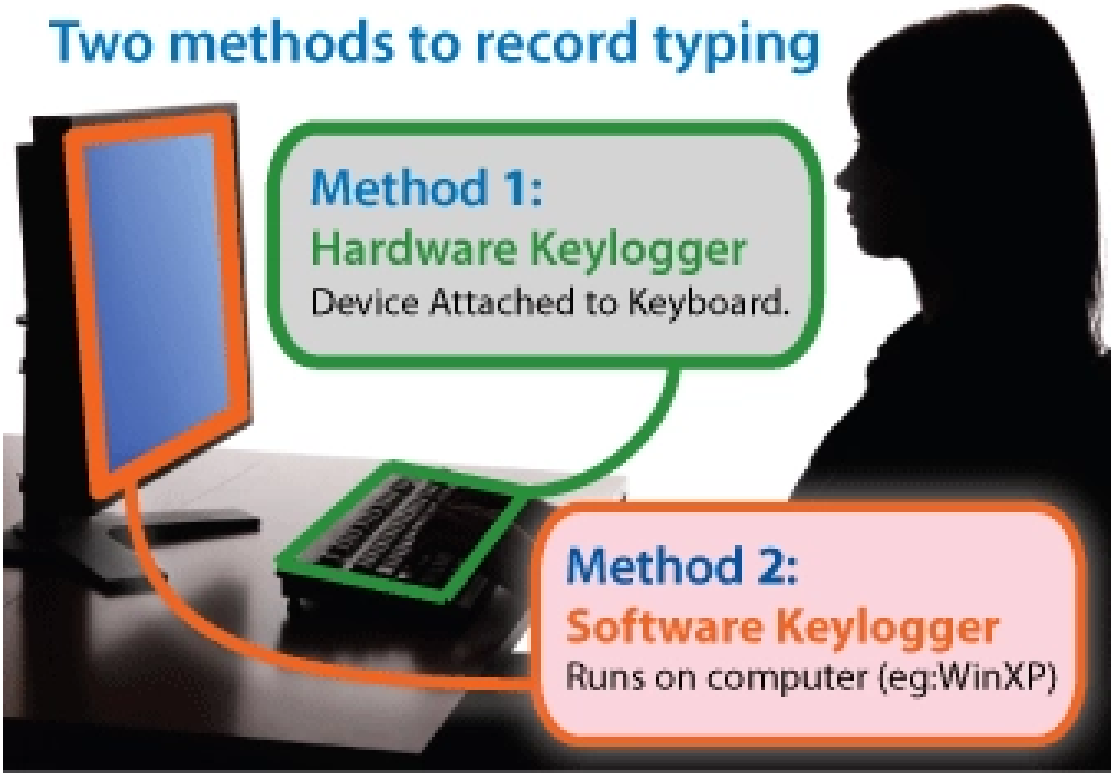


Figure 1.1: Types of Keylogger

1.1.1 Hardware Keyloggers

These can be achieved using BIOS-level firmware or through a device that connects a wired computer keyboard to a computer. A hardware-based keylogger saves all of the information it collects to its own internal memory, leaving no sign of its existence on the machine. One of the biggest benefits of a hardware key logger over a software one is that it can start recording keystrokes as soon as the computer is turned on. Hardware keyloggers are typically designed to fit in with the rest of the computer's wiring system.

They resemble a PS/2 or, more recently, a USB interface that simply plugs into the end of the keyboard cord and then into the computer, thus the inline designation. Both a PS/2 (left) and a USB (right) inline keylogger are shown in the images below.

Figure 1.2: PS/2 & USB

1.1.2 Software Keyloggers

Hypervisor-based, API-based, Form grabbing based, Memory injection based, and Kernel based are the five main types of software keyloggers. Loggers that are based on hypervisors can be included in a malware hypervisor that runs in the background of the operating system. They essentially become a virtual machine that the computer user is unaware of. Kernel-based logs are the most complicated to programmed and set up, but they also allow for the most variation. These loggers may function as a keyboard driver, allowing them to record everything typed on the keyboard. Rootkits, which could skip the working gadget kernel and provide the consumer unauthorized get admission to to the gadget hardware, are generally used.

1.2 Problem Definition

In most cases it is observed that thefts and sabotage [3] of information are caused mostly by their employees itself. Organisations need to realized that it is basic responsibility to be taken from the employee to not theft and leak the confidential information and misuse them in the means of finance. Now a days organisation have to resolve the protection of information from information security breaches when theft of information occur internally by resolving the employee's monitoring.

1. In today's world, security is crucial in terms of increasing technology to keep information secure within an organisation. By employing an activity monitoring tool, the activities of employees may be watched to keep information secure inside an organization [4].

2. Most of the organisations facing challenges in maintaining the security as Employee activities can have a major effect on securing the information within organizations. Activity Monitoring tool used to monitor the employee's Key logs, Screenshots, Microphone, System and Network information inputs within an organization [3].

1.3 Objective of Project

1. To Monitor the Employee's activities within an Organisation.

2. Activity Monitoring tool tracks Keyboard, Screenshot, Microphone, System and Network information inputs and generated the log files and forwarded these log files to admin Email.

3. The Main purpose of the tool is, to test the security of information systems.

1.4 Limitations of Project

The limitations of this project are:

1. As we are considering the few features for monitoring the Employee activities within an Organisation those features may be exhausted with new

technologies of violating the information security.

2. Any Employee within an organisation are aware of controlling the tool in an system encourages to theft the information of organisation and use it for their personal finance.

3. As we are using the Email for getting the log files from Employee for monitoring the Employee's activities we need an Internet connectivity necessary.

CHAPTER 2

LITERATURE SURVEY

2.1 Introduction

Information Security implementations for square measure sensible and embody appropriate security controls will have a effect on associate organization's security. Emerging techniques and tools, yet as new technologies and ways within the space, are permitting info security to be applied to a broader vary of issues within a corporation. info security are often accustomed build solutions that aid within the secure storage of huge amounts of knowledge yet because the implementation of the safety rules among a corporation.

Information security's sensible applications produce security results that can have a big impact on a company's bottom line. New techniques in the business square measure incessantly growing, gap up much unlimited possibilities for info security applications. Organizations that trust the confidentiality and security of their information. But, with the foremost powerful tools within the info security it's ascertained that information thefts square measure caused mostly by their employee.

Organizations have to resolve the protection of information from information security breaches when theft of information occur internally. In most cases it is observed that thefts and sabotage [3] of information are caused mostly by their employees itself. Organizations need to realized that it is basic responsibility to be taken from the employee to not theft and leak the confidential information and misuse them in the means of finance.

Keyloggers are used for both legal and illegal purposes [5].Attackers employ them to compromise user's privacy in order to steal personal data, but they can also be utilized in everyday life for legitimate purposes such as child monitoring, forensic investigation, and ethical hacking...

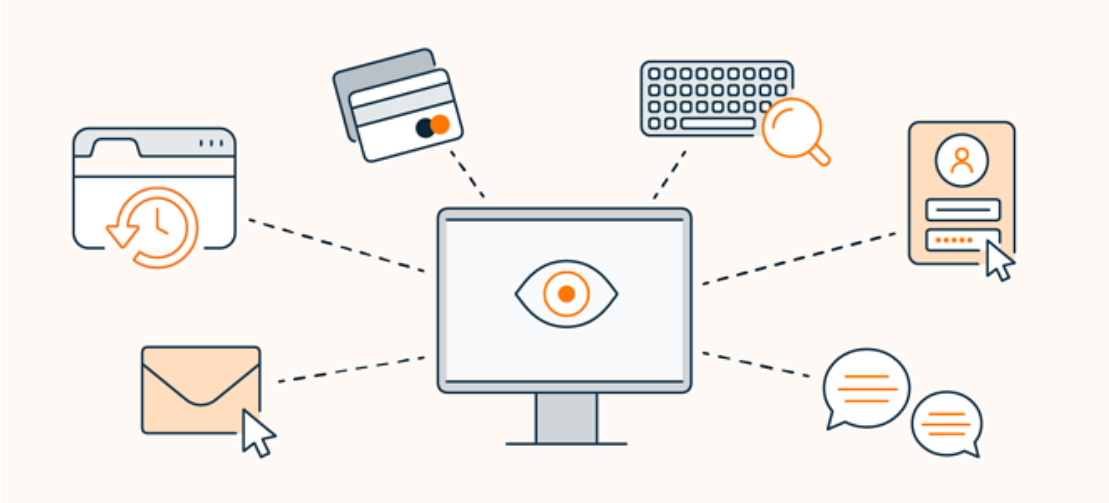


Figure 2.1: Use of Keylogger

In this project, we propose an activity monitoring tool which consist of python program with efficient modules to enhance the Information Security within an organization.

2.2 Existing System

Keyloggers have been around since the mid-1970s, when the Soviet Union invented the "Selectric bug" to target typewriters. Keyloggers have come a long way since then. In the previous ten years, there has been an increase in both efficiency and usability. As the name implies, keyloggers can only produce results if the keys are logged. When Microsoft Windows 8 was released in 2012, it came with a touchscreen personal keyboard, which posed a serious challenge.

S. Sagiroglu and G. Canbek proposed real time working of keylogger malware analysis to track the keyboard behaviour of a user. Keyloggers are versatile instruments that can be used for a variety of purposes. Keylogger attacks are not protected by standard security procedures for machine-to-machine connections. To combat keylogger invasions, human-to-machine interfaces must be explored. Employers and computer owners who utilise keyloggers wisely may be able to improve security, privacy, and efficiency in specific instances.

However, the potential benefits must be weighed against the potential negative consequences for staff, users, and children [3].

Tom Olzak proposed Key stroke logging (Key logging) examined how keyloggers work, he looked at the various types of keyloggers and how they differ. Finally, he explored ways to prevent keylogging and how to respond if a keylogger is discovered. Cybercriminals have evolved a variety of techniques for obtaining sensitive data from your endpoint devices. The capture of typed characters is known as keystroke logging, or keylogging. Document content, passwords, user IDs, and other potentially sensitive information are all examples of data that can be recorded. An attacker can collect valuable data without breaking into a hardened database or file server using this method [6].

A. Davis proposed Hardware keylogger Detection which detects the keyloggers based on the hardware devices. Keystroke logging is a way of capturing and recording computer user's keystrokes, including sensitive passwords, using hardware keyloggers. They can be accomplished either through BIOS-level firmware or with a device connected in between a computer keyboard and a computer. Hardware keyloggers are typically designed to fit in with the rest of the computer's wiring system. They resemble a PS/2 or, more recently, a USB interface that simply plugs into the end of the keyboard cord and then into the computer, thus the inline designation. [7].

Preeti Tulu and Priyanka Sahu proposed System monitoring and security using keylogger in which The goal of this paper is to provide an overview of some of the advantages that complete system network monitoring can provide to anyone. Keylogging programmes, often known as keyloggers, are a type of malware that monitors keyboard input in order to collect personal and secret information. Keystroke logging, often known as key logging, is the capture of typed characters/numbers. Passwords, user IDs, and other potentially sensitive information can all be recorded. The programme records all keystrokes (also known as Keystroke Logging) as well as the name of the application in which the keystrokes were typed. It also saves the window captions and any URLs visited with a web browser. This allows you to assess any text written by

your employee or user, regardless of whether it was created with a text editor, email client, or an online text control on a web page. You have access to all of your employees'/web users' websites and online account passwords. For easy monitoring, you can also enable automatic screenshot capture [4].

Christopher Wood and Rajendra Raj proposed Keyloggers in Cybersecurity Education in which Keylogger programmes seek to gather personal information by secretly capturing user input via keystroke monitoring and then distributing this information to others, often with malicious intent. As a result, keyloggers pose a substantial risk to both business and personal activities such as online banking, email, and chat. To deal with such hazards, users must be trained not only on this sort of malware, but also in the design, implementation, and monitoring of effective defences against various keylogger attacks [1].

2.3 Disadvantages of Existing System

The Main Disadvantage of Existing System is hardware keyloggers [7] and keyboard keyloggers [2]. As these keyloggers are not sufficient to efficiently monitor the activity and information security of employees within an organization.

2.4 Proposed System

In the proposed system, we introduced an Activity Monitoring tool used for tracking / monitoring Employee's activities within an organization [8]. In Activity monitoring tool we use different types of packages available in python such as logging, pathlib, subprocess, smtplib, sounddevice, shutil, requests, Process, ImageGrab, socket, os, re, time for monitoring Keyboard, Screenshots, Microphone, System and Network information inputs from employees, stored as logs in the employee system itself and forwarded these logs to admin Email [9]. After completely sending these logs to admin the logs are automatically deleted.

Below Figure, Employee activity monitoring tool for organizations describes how

the admin monitors the employee's within an organisation ans monitored the employee activities and get those activities through email. In this project we fetch the activities of employee such as Keylogs(keyboard inputs), Screenshots, Microphone, System information and network information. Based on these log information the admin can take necessary action on employee up to some extent. So that information security within an organisation is efficient.

Figure 2.2: Employee activity monitoring tool for organizations

CHAPTER 3

ANALYSIS

3.1 Software Requirement Specification

3.1.1 Software Requirements

Product perspectives and features, operating systems and environments, graphics requirements, design constraints, and user documentation are all included in the functional requirements or general description documentation.
Applying requirements and implementation constraints gives you a complete picture of your project in terms of its strengths and weaknesses and how to deal with them.

Python

Python is a general purpose programming language that is interpreted. Python has a polymorphic notation and automatic memory management. It has a large and extensive standard library as well as supports instrument, impulsive, functional, and procedural programming paradigms. Python is handled by the interpreter. Python is interactive. You can write a program by sitting at the Python prompt and interacting directly with the interpreter. Python also recognizes the importance of development pace. Access to powerful structures that avoid costly code iterations is just as important as readable and concise code. This is also related to maintainability. It may be a nonsensical number, but it indicates the amount of code that needs to be scanned, read, and / or understood in order to fix the problem or change its behavior. Python is also commonly used in the data science domain of data analytics. B. Matplotlib, Pandas, Numpy. Python is a simple and efficient programming language that hackers use to develop scripts on Kali Linux. Some of these cybersecurity penetration testing tools such as Metasploit, Burpsuit Pentester, Nessus, and Sqlinjectors are written in Python.

Python is chosen by security specialists for developing security infrastructures because of this. As it has almost hundreds of modules used in artificial intelligence and machine learning challenges, Java is a reference to python, which is an extension of it.

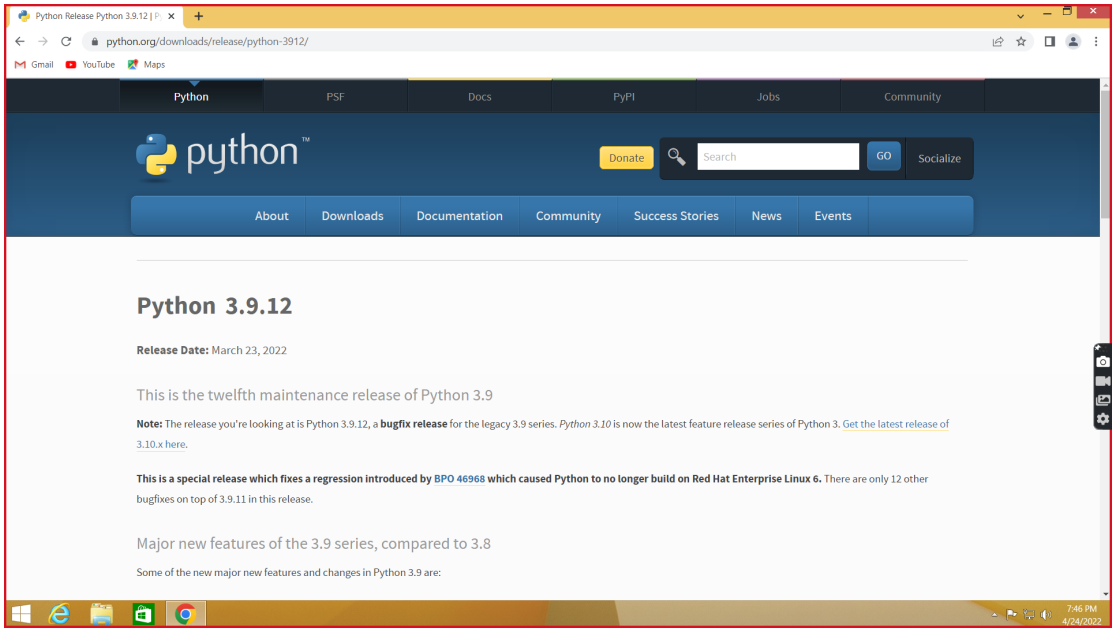


Figure 3.1: Python Installation

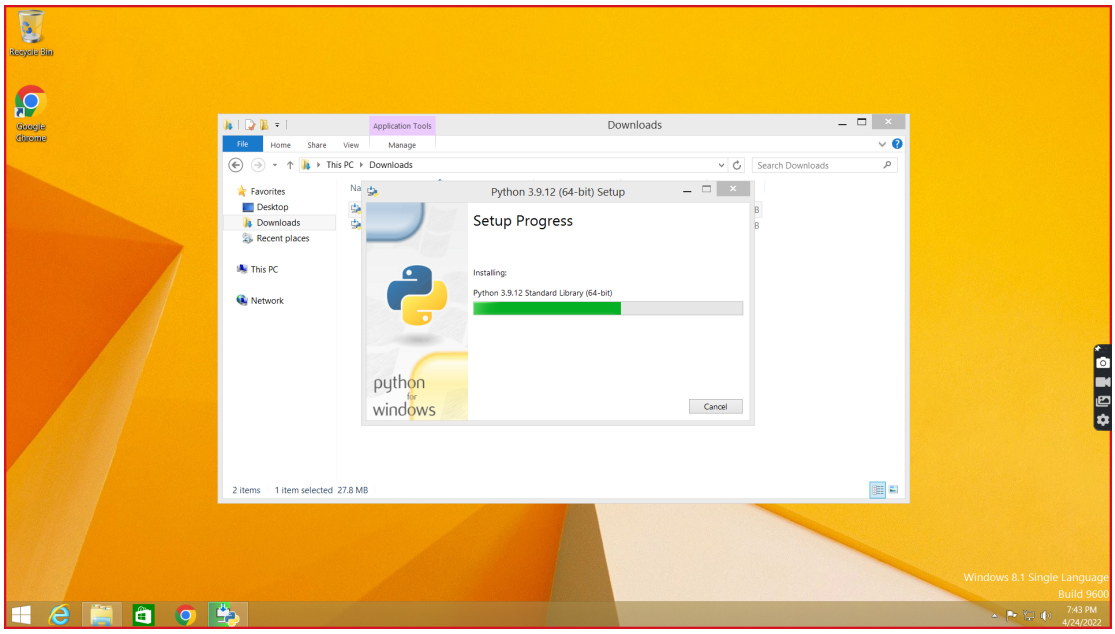


Figure 3.2: Python Installation

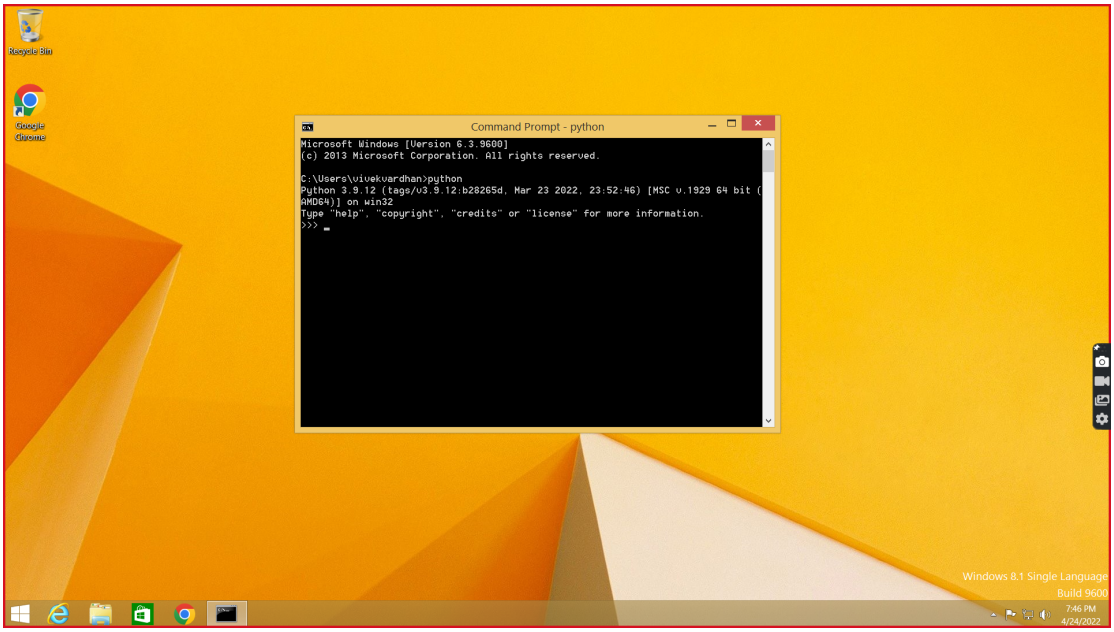


Figure 3.3: Python Installation

Modules Used in Project

logging

Logging is a means of tracking of events when a software runs. The logging functions used in project are logging.DEBUG() means Detailed information and logging.INFO() means Confirmation that things are working as expected. As key listeners used to track key strokes from keyboard,logging modules helps to configure first then store data in files. Logs are a record of events that occur in your organization's systems. The log consists of events which are recorded . Log management rules and processes must be established by organisations. For successful log management activities, businesses must adopt standard methods. Organizations must identify logging criteria and goals as part of the planning process. Organizations must next design rules that clearly identify the necessary needs and recommended recommendations for log management activities such as log production, submission, storage, analysis, and disposal, based on these findings. Organizations must also ensure that log management requirements and recommendations are included in and supported by applicable policies and procedures. Administrators of the organisation must offer the resources they require to build protocol management plans, rules,

and procedures.

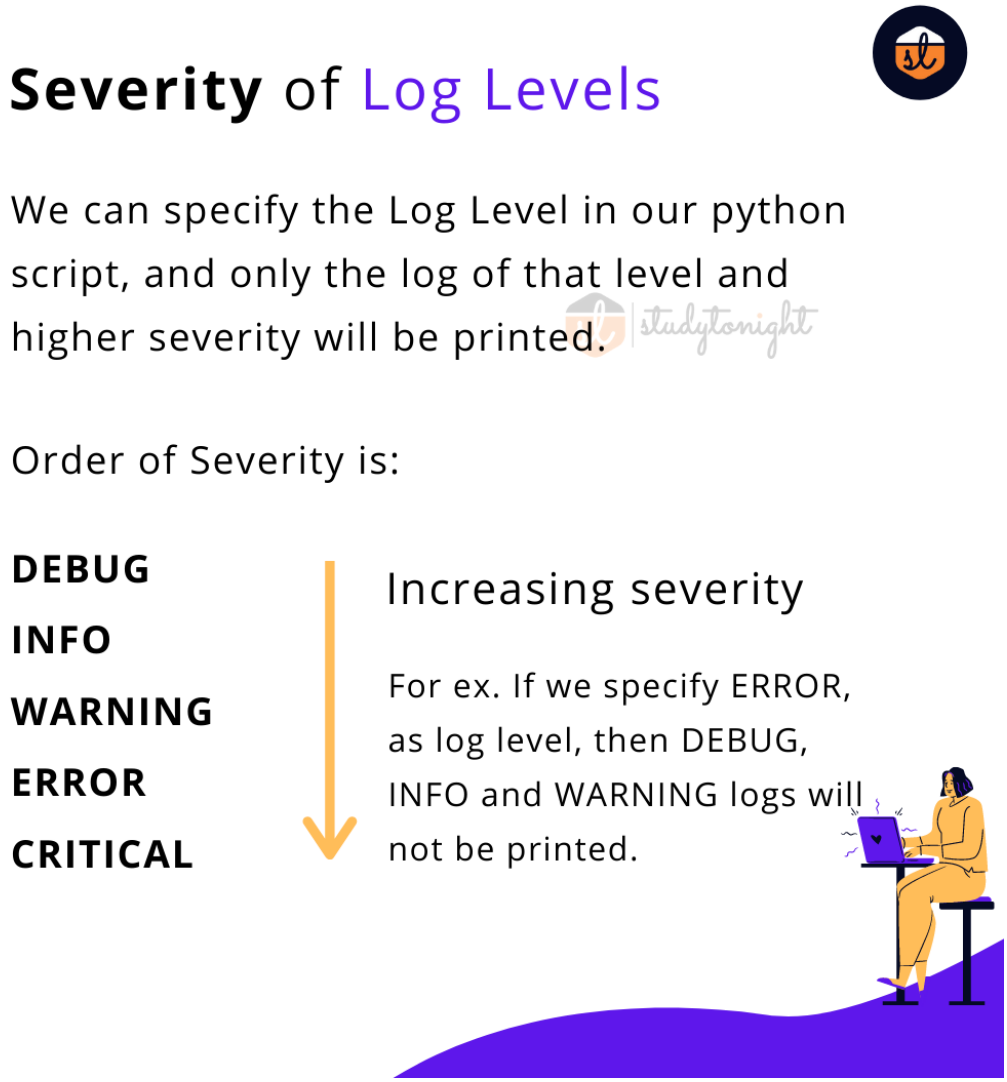


Figure 3.4: Logging Library

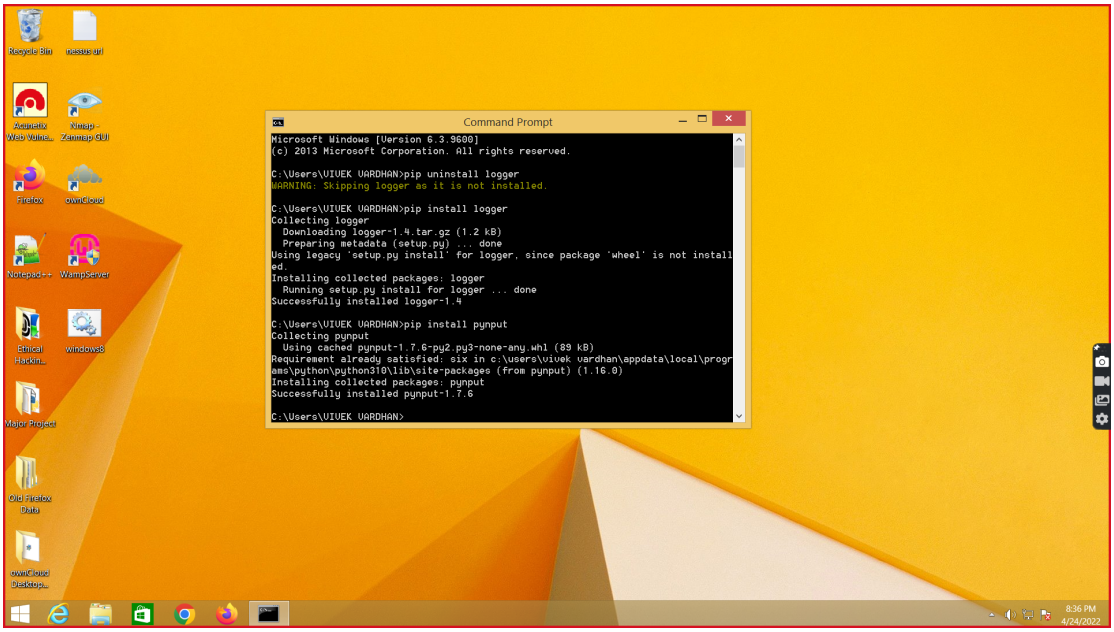


Figure 3.5: Logging Library

Pathlib

Pathlib is a Python module that provides an object API for manipulating files and directories. Pathlib library provides various classes for representing the file system paths with semantics appropriate for different operating systems, Pure paths, which give purely computational operations without I/O, and concrete paths, which inherit from pure pathways but additionally provide I/O operations, are the two types of path classes. For a variety of reasons, interacting with the file system and working with files is essential. Reading and writing files may be all that is required in the most basic cases, but more complex activities are occasionally required. Maybe you need to see all files in a specific type of directory, find a file's parent directory, or create a new file name that doesn't exist. It's difficult to write a Python script without using the file system in some way. It might be as simple as reading a data file into a pandas DataFrame or as complex as processing hundreds of files in a deeply nested directory tree. Python's standard library contains a number of useful functions for this purpose, including the pathlib module. One of the benefits of the pathlib module is that it makes creating routes without the

use of os.joindir more easier.

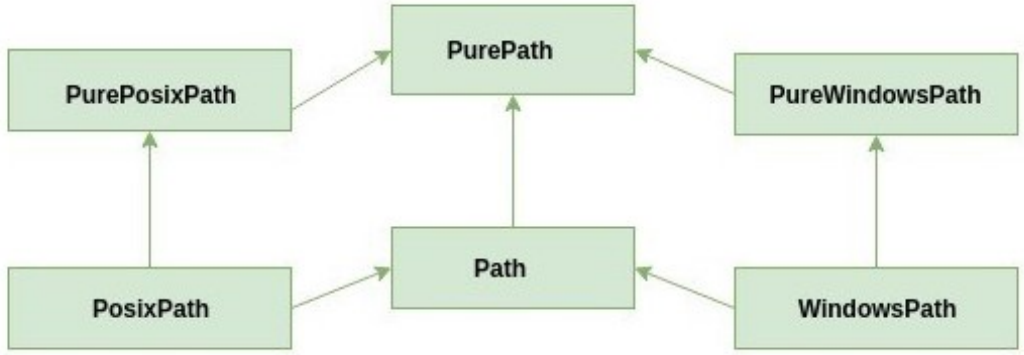


Figure 3.6: Pathlib Package

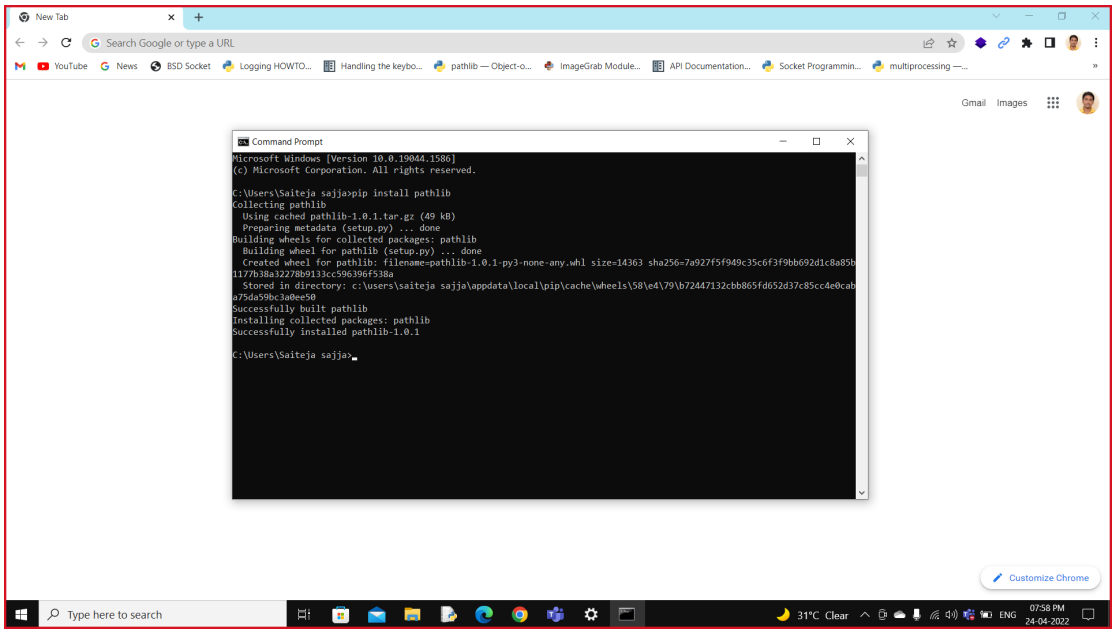


Figure 3.7: Pathlib Library

smtplib

The smtplib module defines an Simple Mail Transfer Protocol(SMTP) client session object that can be used to send mail to any machine which have internet

connection with an SMTP listener. Using SMTP we can send formatted text in an email message not all audio,video (only support a single body of ASCII text). It creates an SMTP client session object that may be used to send email to any internet machine that has an SMTP server. It uses the ports 25,465,587 and 2525 with 587 being the default mail submission port and standard secure SMTP port; modern email servers use 587 for secure email submission for delivery; this uses the mail submission agent; starttls is a way to upgrade a plain text connection to an encrypted connection instead of using a separate port for encrypted communication. SMTP (Simple Mail Transfer Protocol) is an internet standard TCP/IP protocol for sending electronic mail from a sender to one or more recipients. HOSTNAME, USERNAME, PASSWORD, and PORT NUMBER are required to connect to an SMTP mail server. A SMTP connection is encapsulated by the SMTP object. smtplib. [host, port, local hostname, timeout] SMTP([host, port, local hostname, timeout] SMTP([host, port, local_Login to the SMTP Server is required for STMP Authentication. SMTP.login SMTP.login SMTP.login (username, password). TLS should be enabled for security reasons. It will use starttls() to encrypt all commands.To send mail to recipients, use the sendmail() function. mailto: (from, to, msg).

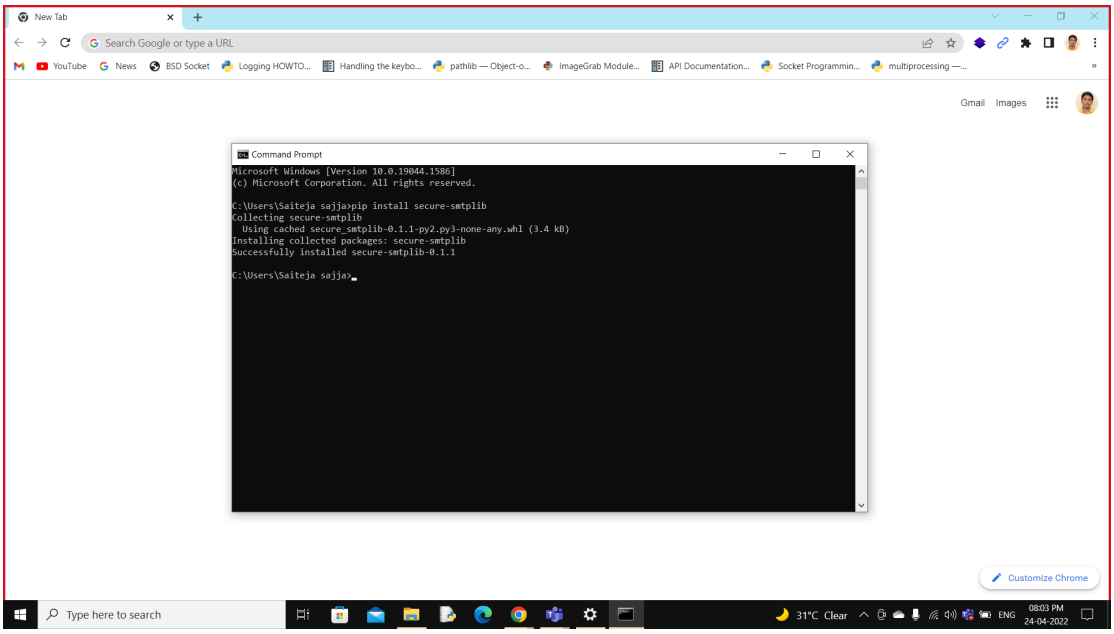


Figure 3.8: Smtplib Library

sounddevice

Python may be used for a wide range of activities. One of them is in the process of developing a speech recorder. The sounddevice module in Python can be used to record and play audio. This module, in conjunction with the wavio or scipy modules, allows you to save recorded audio. The sounddevice module provides functions to play and record NumPy arrays that contain audio signals. The sounddevice holds audio data with sampling frequency (44100 (or) 48000 frames per second default) by using numpyarray. The sounddevice functions are sounddevice.rec(), sounddevice.wait(). We need to specify a few variables before we can start the recorder. The first is the audio sampling frequency (which is usually 44100 or 48000 frames per second), and the second is the recording time. We must set a duration in seconds so that the recording stops after that time. We're all set to start the recorder now. It will save the captured audio to a NumPy array. The audio recording is now complete. So let's try to save it. We can use either the scipy or the wavio modules to store the audio file.

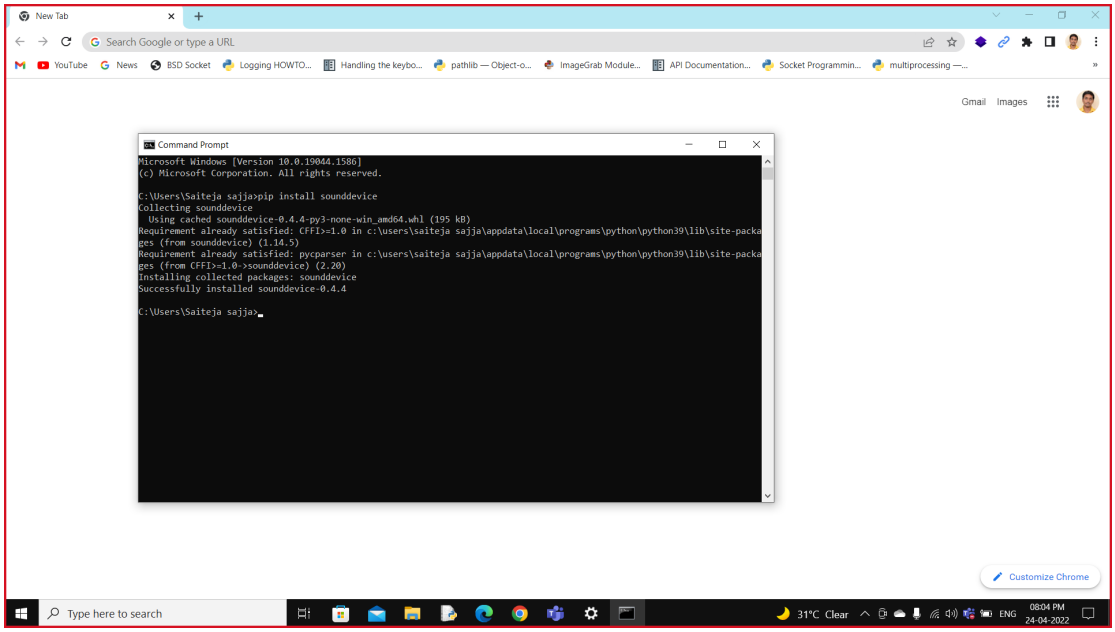


Figure 3.9: Sounddevice Library

shutil

The Shutil module enables you to do high-level file operations such as copy, create, and remote operations on a file. It is included in Python's core utility modules. This module facilitates in the automation of file and folder copying and deletion. The shutil module used for file copying and removal. The shutil function is shutil.rmtree() helps to delete entire directory.

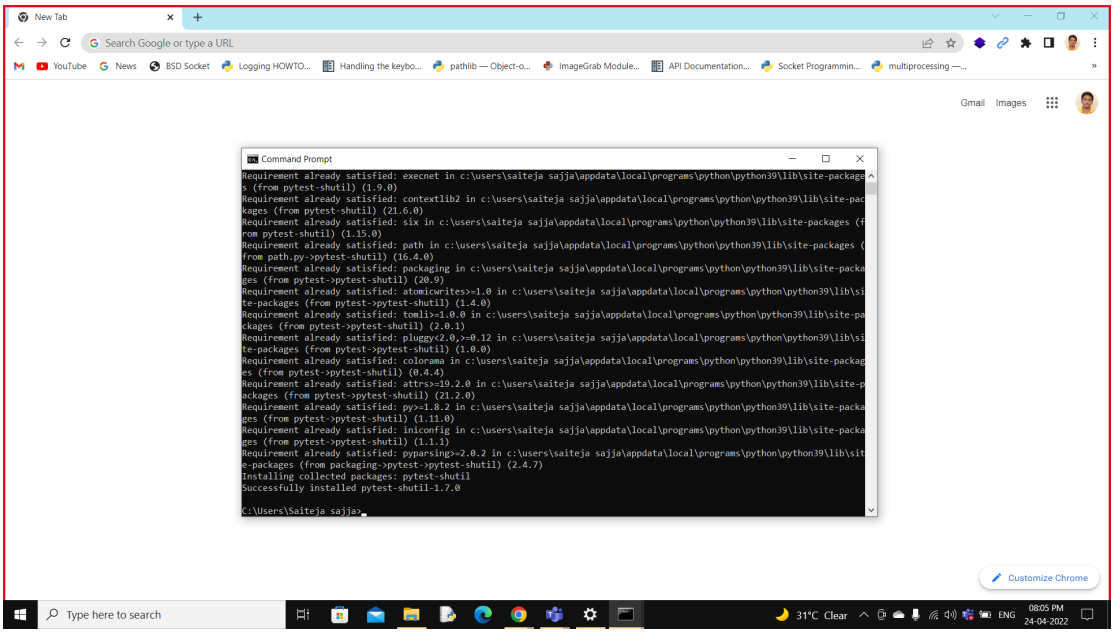


Figure 3.10: Shutil Library

requests

The requests module used for sending HTTP request easily. Using the GET, POST, PUT, PATCH, or HEAD protocols, the Python requests module includes built-in methods for making HTTP requests to a specified URI. A Http request is used to get data from a certain URI or to send data to a server. Between a client and a server, it functions as a request-response protocol. The GET technique is used to retrieve data from a server using a certain URI. The encoded user information attached to the page request is sent using the GET method. The POST request method asks a web server to accept the data in the request message's body, most often for storage. The

PUT method asks for the enclosed entity to be saved at the specified URI. The DELETE method deletes the resource specified from the system. The HEAD method expects a response that is similar to a GET request but does not include the body. It's utilised to modify a person's capabilities. The PATCH request must only include the modifications to the resource, not the complete resource. The requests function requests.get() is used for fetching the IP address. This module was used to store network and system information. It includes headers, from and to data, multipart files, and other contexts. Some of the methods with arguments are get(url), head(url), post(url) and put(url).

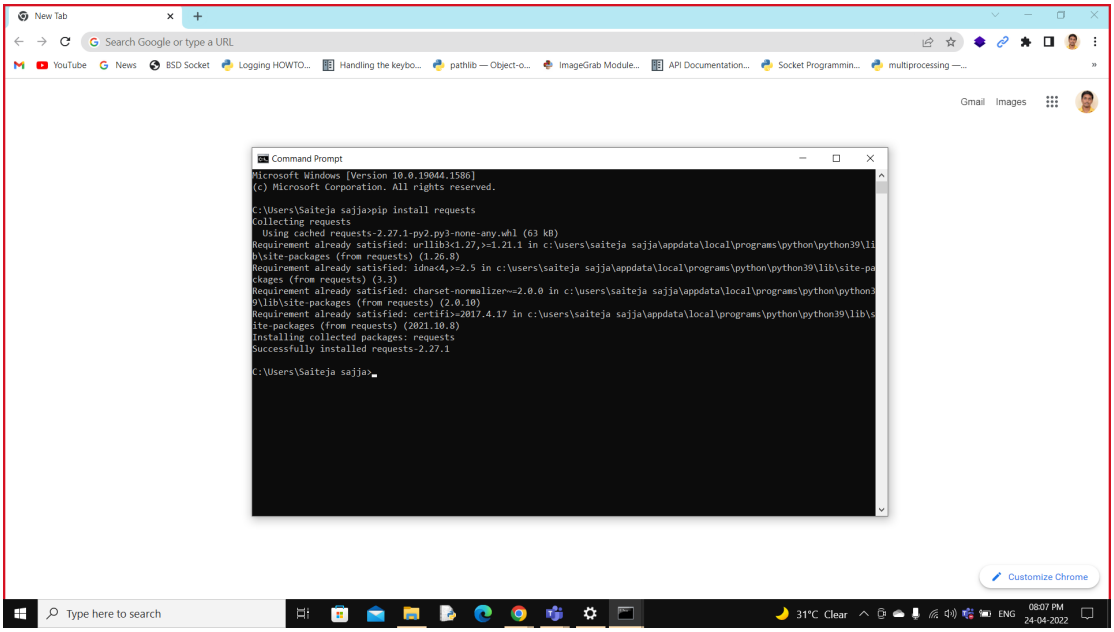


Figure 3.11: Requests Library

Process

The Process module used for implementing the multiprocessing which supports spawning processes using an API similar to the threading module. The ability of a system to execute many processors at the same time is referred to as multiprocessing. Applications in a multiprocessing system are separated into smaller routines that function independently. The operating system sends these threads to the processors, which enhances system performance. To start a

process, we make an object of the Process class. It requires the following arguments: target: process args: the arguments that will be provided to the target function. p1 = multiprocessing.Process(target=rect, args=(20,)), p2 = multiprocessing.Process(target=circle, args=(20,)). We use the start function of the Process class to initiate a process. p1.start() , p2.start(). When the processes begin, the existing software continues to run. We utilise the join function to halt the execution of the current programme until a procedure is completed. p1.join() , p2.join(). As a result, the present programme will first wait for p1 to finish before proceeding to p2. When they are finished, the current program's next statements are executed. In multiprocessing, processes are spawned by creating a Process object and control the process using differnt functions like process.start(), process.join(), process.terminate().

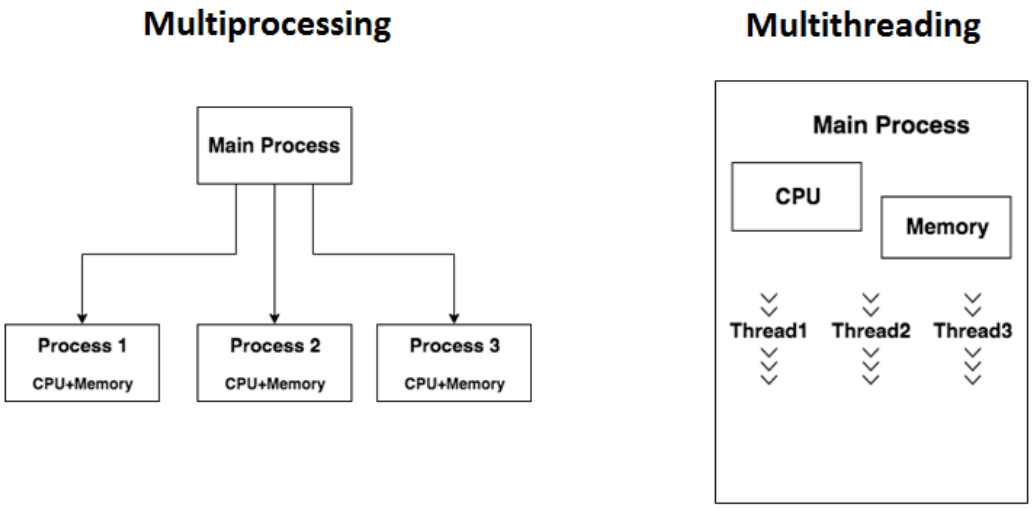


Figure 3.12: Multiprocessing Library

ImageGrab

PIL has a submodule called Imagegrab (python Imaging library). For the Python programming language, there is an image processing package. Lightweight image processing tools are included for editing, generating, and saving photos. The ImageGrab module is used for capturing the contents of the screen or the clipboard. The Python Imaging Library (PIL) gives

image editing capabilities to the Python interpreter. The ImageGrab module can be used to copy screen or clipboard items to a PIL image memory.The PIL.ImageGrab.grab() method captures a screen shot. On Windows, the pixels inside the bounding box are returned as a "RGB" image, but on macOS, they are returned as "RGBA." The full screen is copied if the boundary box is not specified.. The PIL.screenshot.save() is used to save the captured images in the specified location.

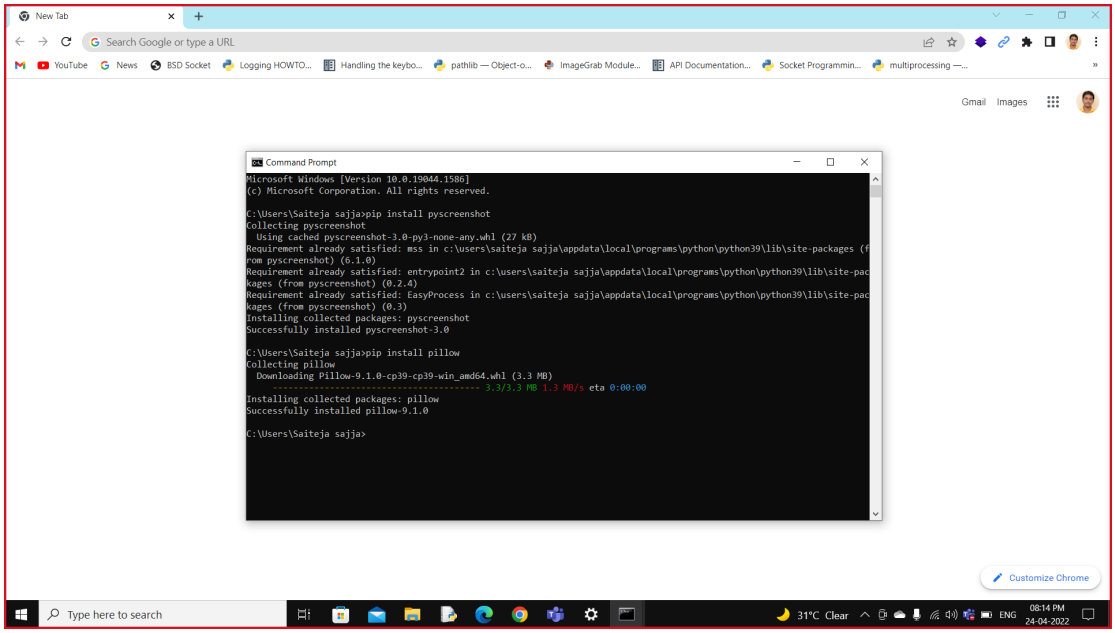


Figure 3.13: ImageGrab(PIL & pyscreenshot) Library

os

The Python OS module enables communication between the user and the operating system. It includes a number of useful OS functions that may be used to complete OS-based tasks and collect operating system-related information. The operating system is a standard utility module in Python. This module provides a portable means of gaining access to operating system-specific functionality. This os module mainly used in interacting with the operating system. We used the os.walk function since it walks from top to bottom or bottom to up in a directory tree to produce file names.

re

A Regular Expression (RegEx) is a specific sequence of letters that uses a search pattern to find a string or set of strings. It can identify the presence or absence of text by comparing it to a specified pattern, and it can also partition a pattern into one or more sub-patterns. Python provides the re package, which enables the use of regex in Python. Its primary function is to perform a search, which necessitates the use of a regular expression and a string. In this scenario, it returns either the first match or none. The re module can be used to check if a string contained specific pattern. The function is re.compile(). Because regex expressions are commonly used for pattern matching, we used them to match the file types and append them to the mail payload to convey data in a logical manner.

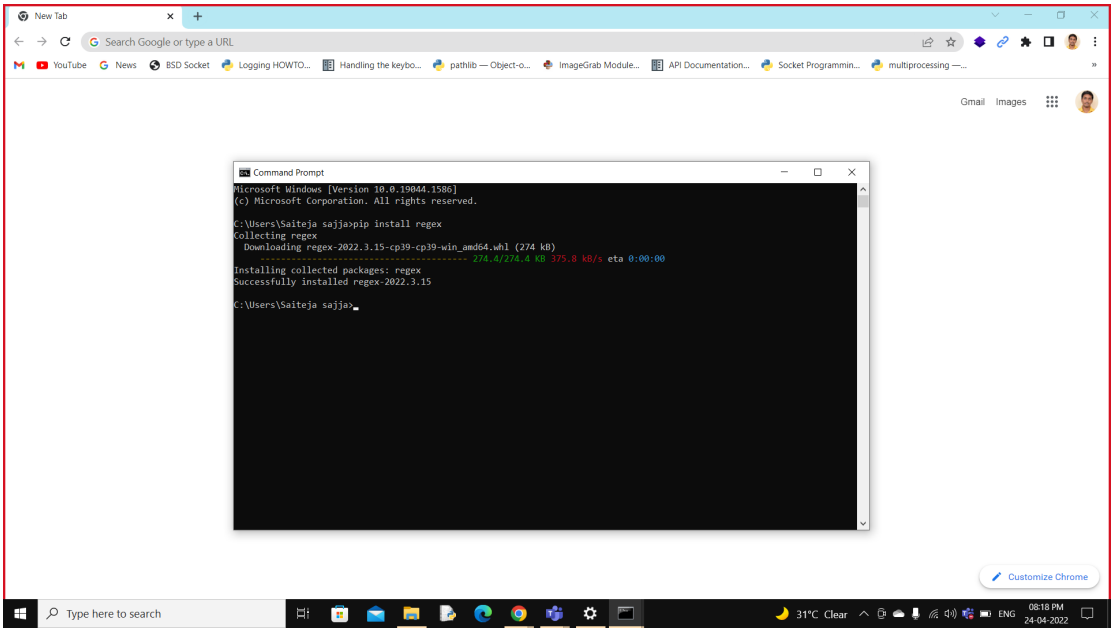


Figure 3.14: Regrex Library

time

Python has defined a module named "time" that allows us to handle a wide range of time-related operations, such as conversions and representations, which are important in a wide range of real-world applications. The start of time is

defined as 1 January, 12:00 a.m., 1970, and is referred to as the "epoch" in Python. The time module various time-related functions like time.sleep(). It returns the number of seconds passed since epoch.

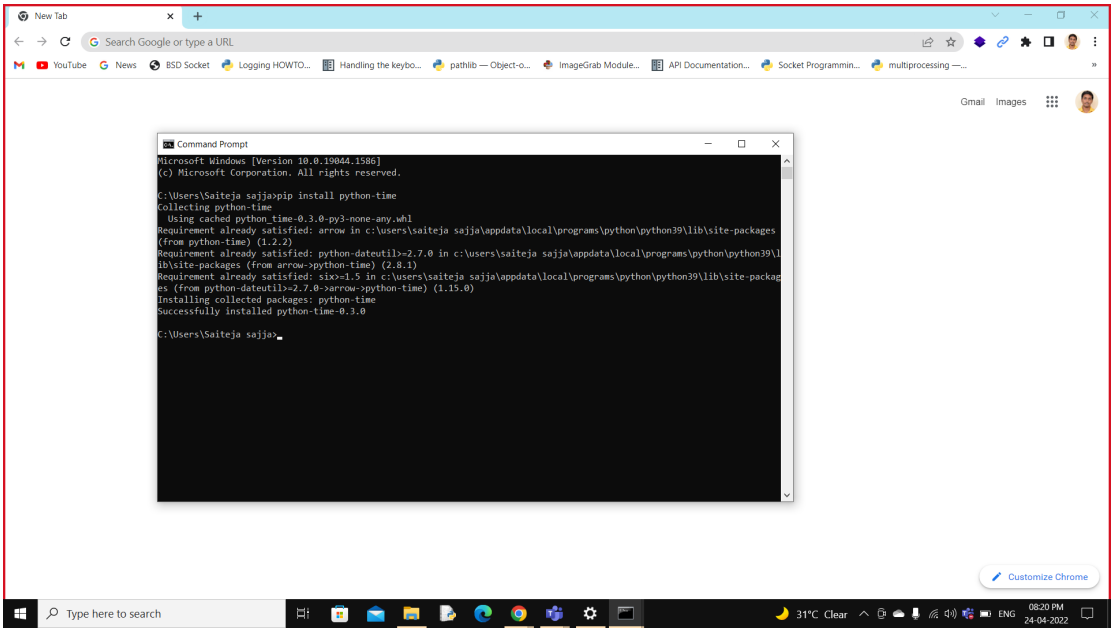


Figure 3.15: Time Library

subprocess

You can use the subprocess module to spawn new processes and connect them to the input / output / error pipes to get the return code. stdout used for Capturing the stdout from the child process and stderr used for Capturing stderr from the child process. The process creation and management is handled by the function called subprocess.Popen(). Each subprocess are differentiated in form of parent and child process,where at each level of hierarchy parents and child's process interchange and communicates output to leaf to its root.In this we used the following methods in Popen such as Popen.communicate for Interacting with process: Send data to stdin. Read data from stdout and stderr, until endoffile is reached and some of the limiting arguments for the sub processes the timeout argument is passed to Popen.communicate(). When the timeout expires, the child process terminates and waits. When the child process terminates, the TimeoutExpired exception is thrown again. The

communication function is used to initiate a 60 second timeout for the shell. Output, error = System_Info.Communicate (timeout = 15).

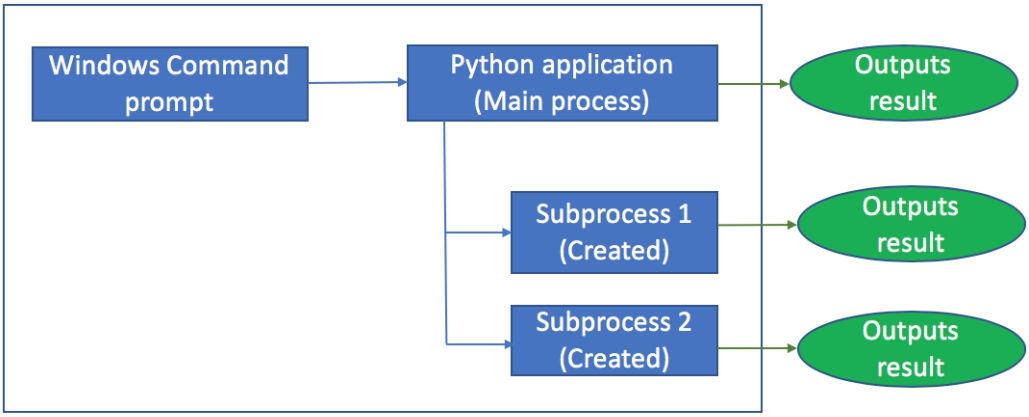


Figure 3.16: Multiprocessing and Subprocess Library

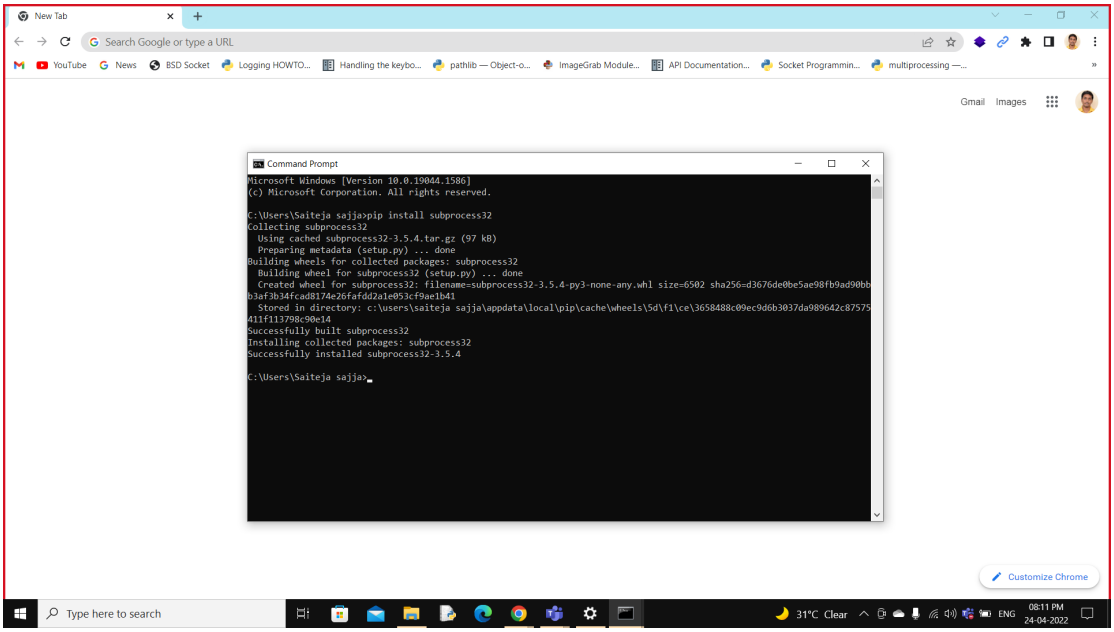


Figure 3.17: Subprocess Library

MIME

The MIME module is Multipurpose Internet Mail Extension is an email application program that extends the email messages format to handle the

jobs.Using MIME we can send multiple attachments within a single email message,including binary files, audio, video, etc.

email.MIME, this module is part of the legacy (Compat32) email API.you get a message object structure by passing a file or some text to a parser, which parses the text and returns the root message object In this the messages are converted to objects after performing the operations on objects converted to normal message.

MIME consists of classes like, email.mime.base.MIMEBase as this is the base class for all the MIME-specific subclasses of Message. email.mime.multipart .MIMEMultipart for a subclass of MIMEBase, this is an intermediate base class for MIME messages that are multipart. Optional _subtype defaults to mixed, but can be used to specify the subtype of the message. A Content-Type header of multipart / _subtype will be added to the message object. email.mime.text.MIMEText The MIMEText class, a subclass of MIMENon-Multipart, is used to create MIME objects for the main type of Text.

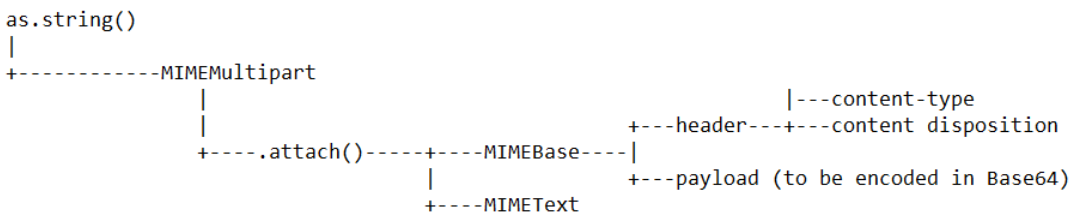


Figure 3.18: MIME Diagram

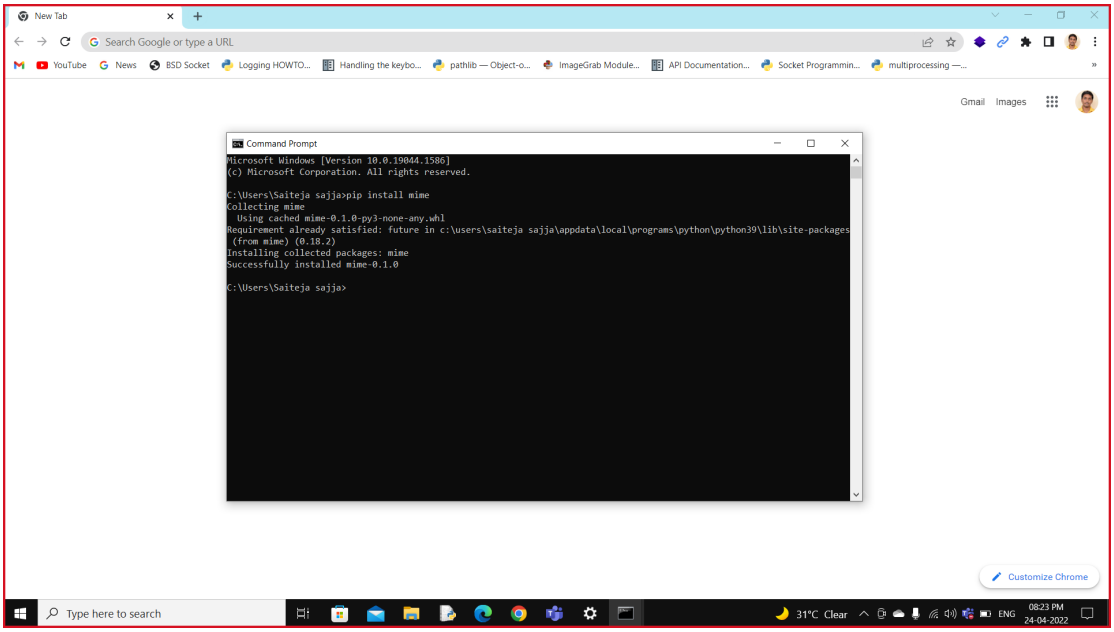


Figure 3.19: MIME Package

socket

The backbone of networking is sockets. They let data to be transferred between two separate applications or devices. When you open your browser, for example, you are establishing a connection with the server for the purpose of data transfer. The socket module in the Python Standard Library provides a BSD socket interface counterpart. For constructing full-fledged network applications, including client and server programmes, the socket module includes many objects, constants, functions, and related exceptions. While such constructs as functions, classes, and methods are listed here, let us begin by developing a sample client programme using Python's socket module and then progress to a client-server example in Python. The socket module provides access to the BSD socket interface and socket() function returns a socket object whose methods implement the various socket system calls. BSD API is a set of standard function calls that can be used in an application. They allow programmers to extend their products over internet communication. The functions are socket.gethostname(), socket.gethostbyname().

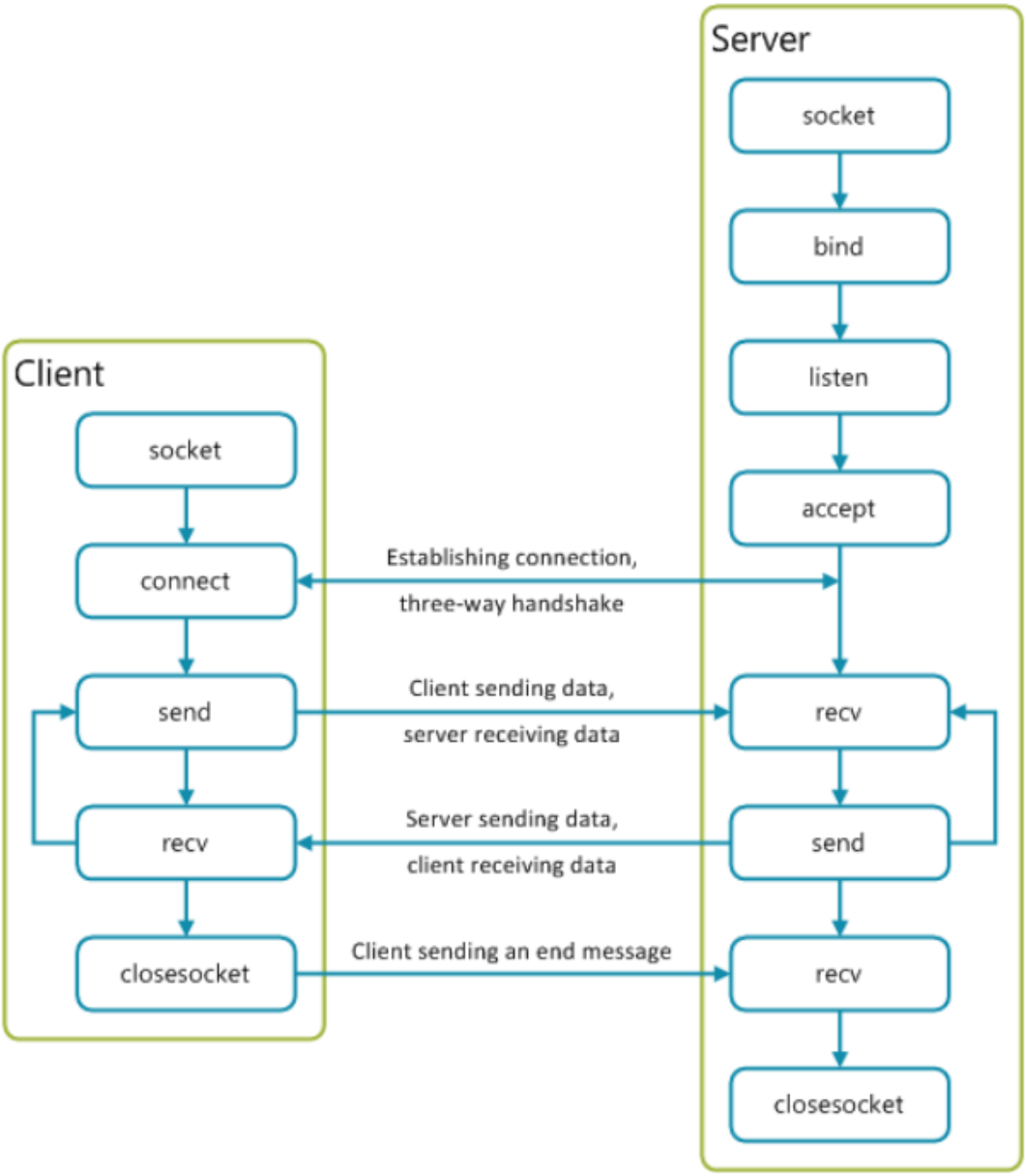


Figure 3.20: Flow Diagram for BSD Sockets Communication using TCP

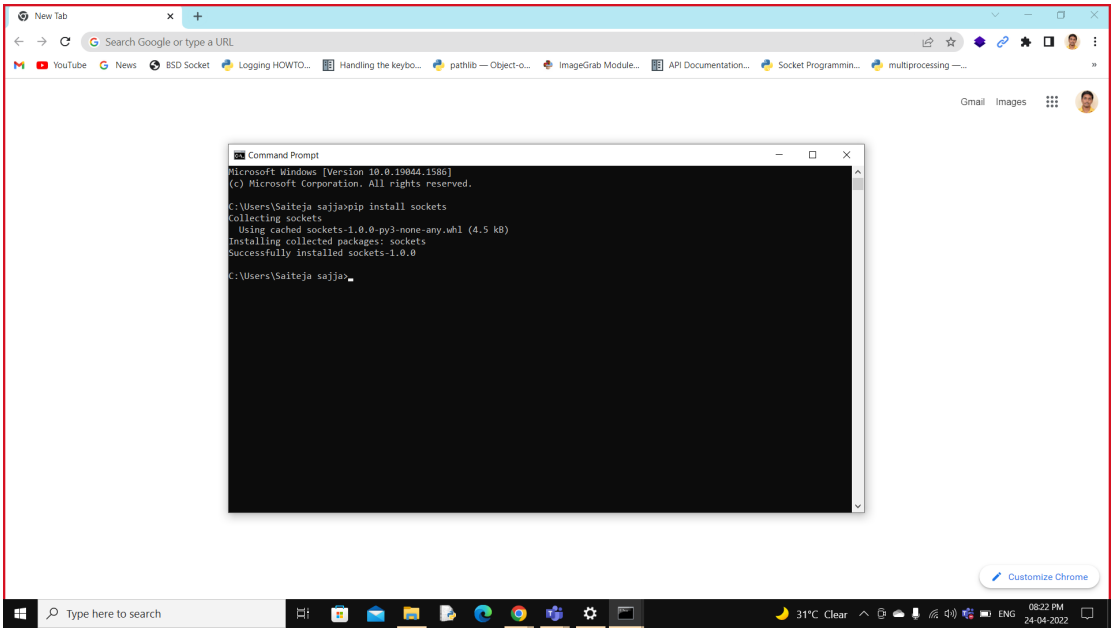


Figure 3.21: Socket Library

3.2 Content Diagram or Architecture of Project

In this proposed system, we introduced an Activity Monitoring tool used for tracking Employee's activities within an organization. Now a days the Information security is at most important within an organisation. To maintain the confidentiality, integrity or availability of information within an organisation depends on the Employee activities. we proposed an activity monitoring tool which consist of python program to enhance the Information Security within an organization. With the help of the Activity monitoring tool, the inputs like Keyboard, Screenshots, System-information, Network-information are monitored and stored as logs in the specified employee system directory and those logs from that directory are sent to the admin Email.

The Basic Architecture Diagram represents that the admin who is monitoring the employee activities enter his credentials in the tool to get the stored logs from employee system. When the employee started working with the system all his work will be monitored based on types of files like keylogs, microphone, screenshots, system and network information of formats txt, wav, jpg, txt and xml respectively. These files are stored in the specified path in

employee system and the tool with respect to the operating system forward these files to the admin email which is specified previously. Based on these logs information, the employee activities will be monitored frequently with help of keylogs, microphone, screenshots, system and network information inputs and action can be taken by the admin based on employee activities. The logs generated in the employee system will be automatically deleted after sending the logs to the admin email successfully.

Hence, the data theft will not be happen within an organization and information related to the organisation will be secured. Organisation can resolve the protection of information from information security breaches when theft of information by using this activity monitoring tool.

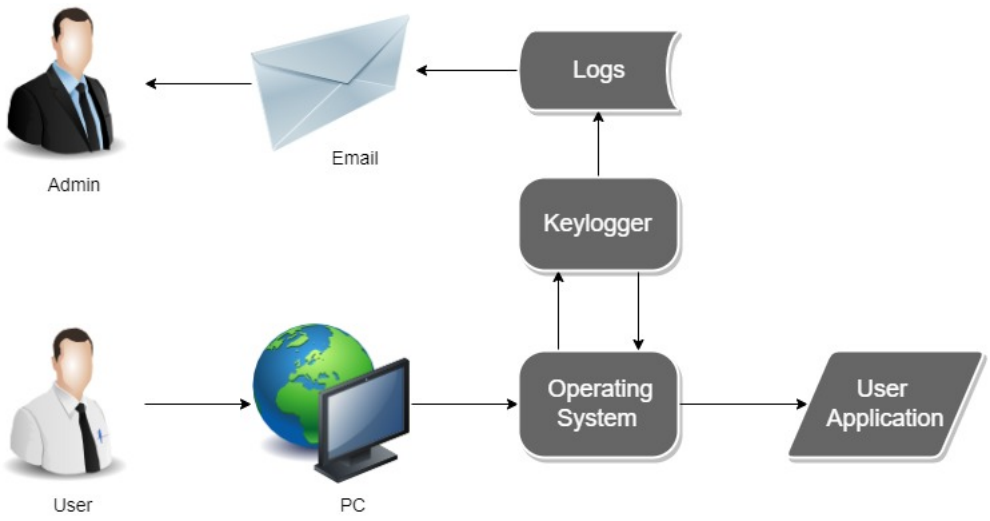


Figure 3.22: Basic Architecture Diagram

3.3 Methodology

The following are the methods, approaches to obtain the output [10]:

1. First the Activity monitoring tool is installed in the employee system, and admin enters his email and password to get the employee's activities into his email.

2. Then the tool start running on the employee system generates the logs and stored on the employee Desktop/Laptop in the specified path based on the type of files.

3. The logs which are generated on the employee system are keyboard, screenshot, microphone, system and network information inputs used for monitoring the employee activities.

4. The pressed keys on the keyboard are saved as.txt format in the chosen directory as keylogs.

5. Every 15 seconds, a screenshot is taken and saved as a picture in the chosen directory as Screenshots.

6. Every 10 seconds, the microphone input is recorded and saved as .wav format in the chosen directory as Recording.

7. Employee System information are saved as .txt format in the chosen directory as system_information.

8. Employee network information are saved as .xml format in the chosen directory as network_information.

9. The files are now aggregated and forwarded to the admin via email based on the file type using regex magic from the chosen directory.

10. The tool automatically deletes the all files in the directory and then loops back to the beginning to repeat the procedure..

CHAPTER 4

DESIGN

4.1 Introduction

Here in this proposed system, we introduced an Activity Monitoring tool for monitoring Employee's activities within an organization. In Activity monitoring tool we use different types of python packages such as logging, pathlib, subprocess, smtplib, sounddevice, shutil, requests, Process, ImageGrab, socket, os, re, time for monitoring Keyboard, Screenshots, Microphone, System information and Network information inputs from employees, stored as logs in the specified directory in the employee system and sent these logs to admin Email.

The logs received by the admin via Email used for maintaining the information security within an organisation.

4.2 DFD / UML Diagrams

Below are the Class Diagram, Data Flow Diagram, Use Case Diagram, Activity Diagram, Sequence Diagram of our system as it helps to capture the functional requirements and easily traceable. Also helps to development guidelines to programmers, to a test case and finally into user documentation. "Unified Modeling Language" is acronym of UML. The Unified Modeling Language (UML) is a standard language for describing, visualising, constructing, and documenting software system artefacts, as well as business modelling and other non-software systems.

4.2.1 Class Diagram

Below Figure, Class Diagram represents that the class diagram of the Activity monitoring tool. The class diagram is used to refine the use case diagram

and specify the detailed design of the system. The class diagram categorises the actors in the use case diagram as a series of interconnected classes. The class link or correlation could be "is-a" or "has-a." Each class in the class diagram may be capable of carrying out certain functions. The functions of the class are referred to as the class's "methods.". In this diagram describes about two classes are Admin, Employee both have the attributes are email and password and the methods are tracking Employee inputs and monitored logs are stored in Employee system and another method is sending of these logs to the admin.

Figure 4.1: Class Diagram of Proposed System

4.2.2 Data Flow Diagram

Below Figure, Data Flow Diagram below depicts the use case models for the Interaction monitoring tool. A bubble chart is alternative term for a DFD. It is a simple graphical formality for depicting a scheme of the data it receives, the processing it performs with that data, and the output it produces as a result. The flow diagram is one of the most important modelling tools (DFD). It's used to personalize the many parts of the system. These components include the method, the data used against the process, some external entity than communicates, or the information flows inside this system. In this diagram it describes that sequence of steps for sending the logs to the admin email which are generated on the user system when the activity monitoring tool installed and start monitoring the user inputs.

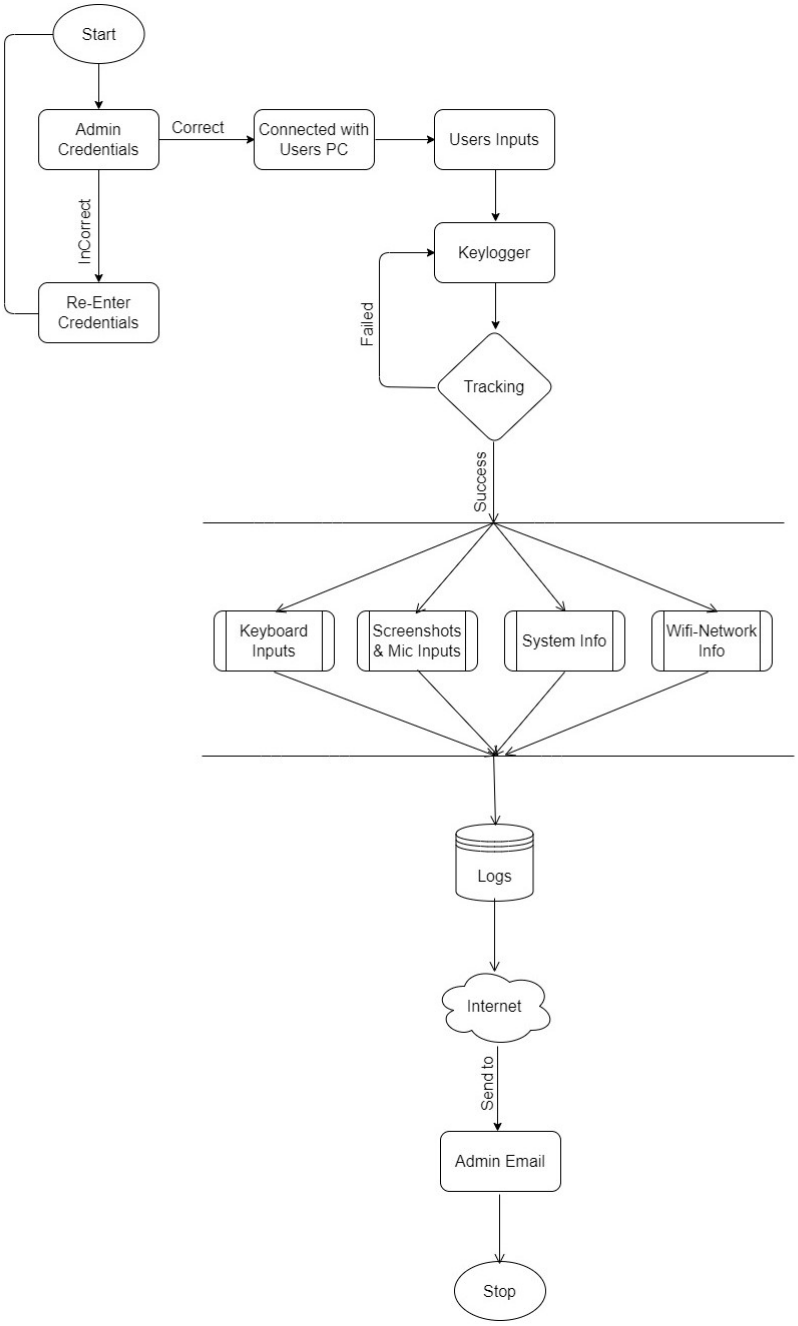


Figure 4.2: Basic Data Flow Diagram of Proposed System

4.2.3 Use Case Diagram

Below Figure, Use Case Diagram represents that the use case diagram of the Activity monitoring tool. A Use Case is a type of behavioural diagram that is defined by and produced from a UML Use-case analysis. Its goal is to provide a visual depiction of the functions that are required in terms of actors,

objectives (as represented by use cases), and any connections between the two use cases. In this diagram the actors are User and admin. The operations are Installing of the tool, Inputs from user monitored, monitored inputs formed as logs in the user system and generated logs are forwarded to admin Email.

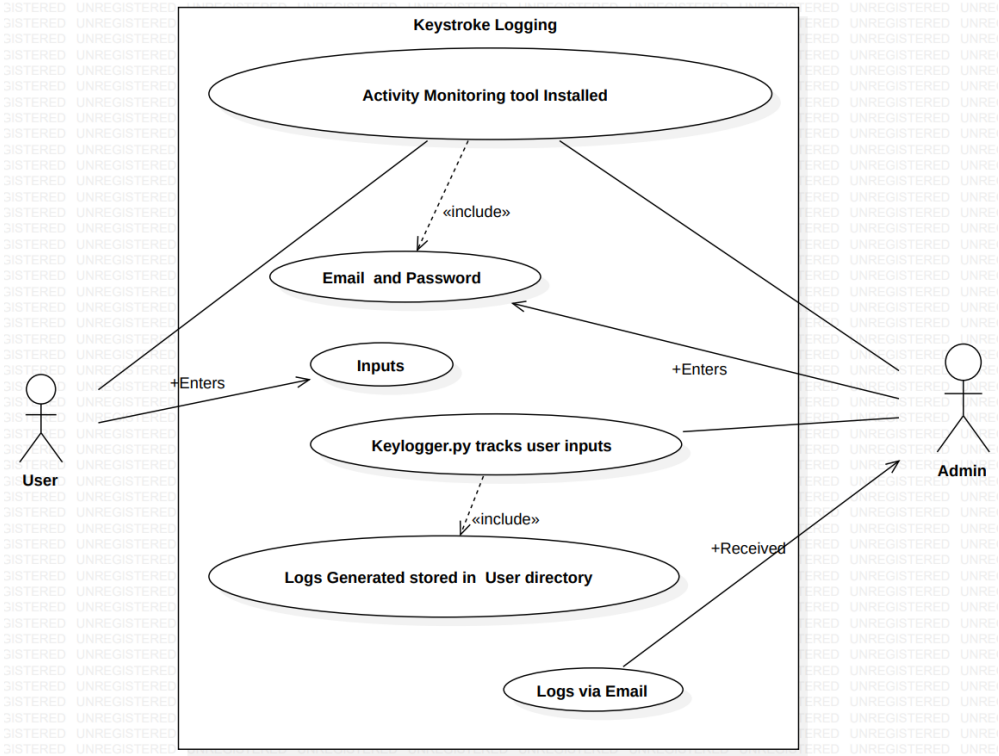


Figure 4.3: Use Case Diagram of Proposed System

4.2.4 Activity Diagram

Below Figure, Activity diagram depicts how the processes flow in the system's. An activity diagram includes activities, actions, transitions, initial and final states, and guard conditions same like as state diagram. In this diagram the follow will based on the activities first entering Admin email and password, Run activity monitoring tool and then its starts tracking inputs where a scenario arises like decision taken whether it is tracking keyboard inputs or tracking screenshots or tracking microphone inputs or tracking system and network information. Then all the required ones are checked tracked and then generates logs in employee's system and forwards these log files to admin email.

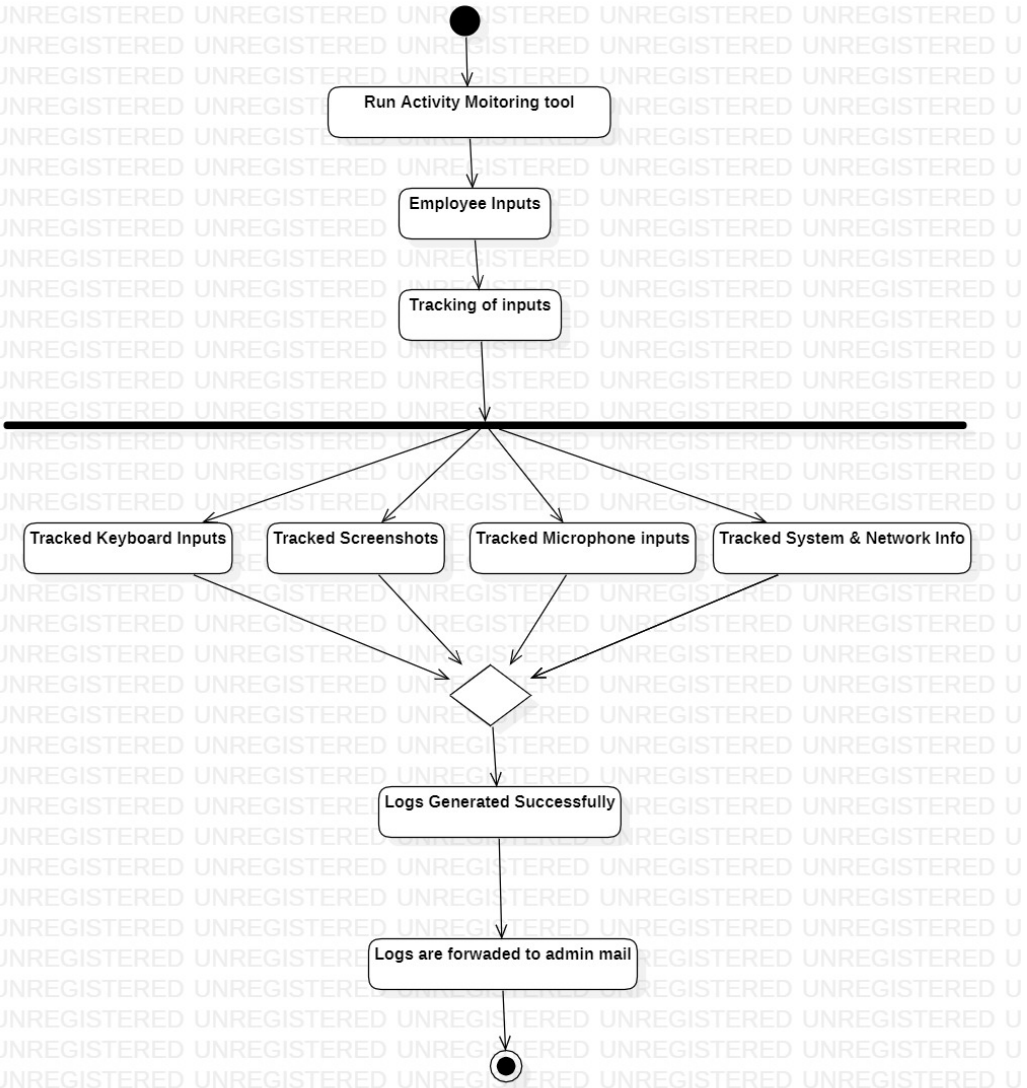


Figure 4.4: Activity Diagram of Proposed System

4.2.5 Sequence Diagram

Below Figure, Sequence diagram depicts how the interaction between the admin and employee. Sequence diagrams simply show the order in which things interact, or the order in which they occur. Sequence diagrams are also sometimes referred to as event diagrams or event scenarios. The sequence diagram shows how and in what order the components of the system work together. Business people and software engineers frequently use these diagrams to document and understand requirements for new and current systems. In

this diagram, admin enter his credentials in tool which is installed on the employee system then employee start working on his system with this tool the logs are generated on the employee system such as keyboard, screenshot for every 15 seconds, microphone for every 10 minutes, system and network information inputs used for monitoring the employee activities. All these log files are send to admin email and admin take necessary actions on the employee and The tool automatically deletes the all files in the directory and then loops back to the beginning to repeat the procedure.

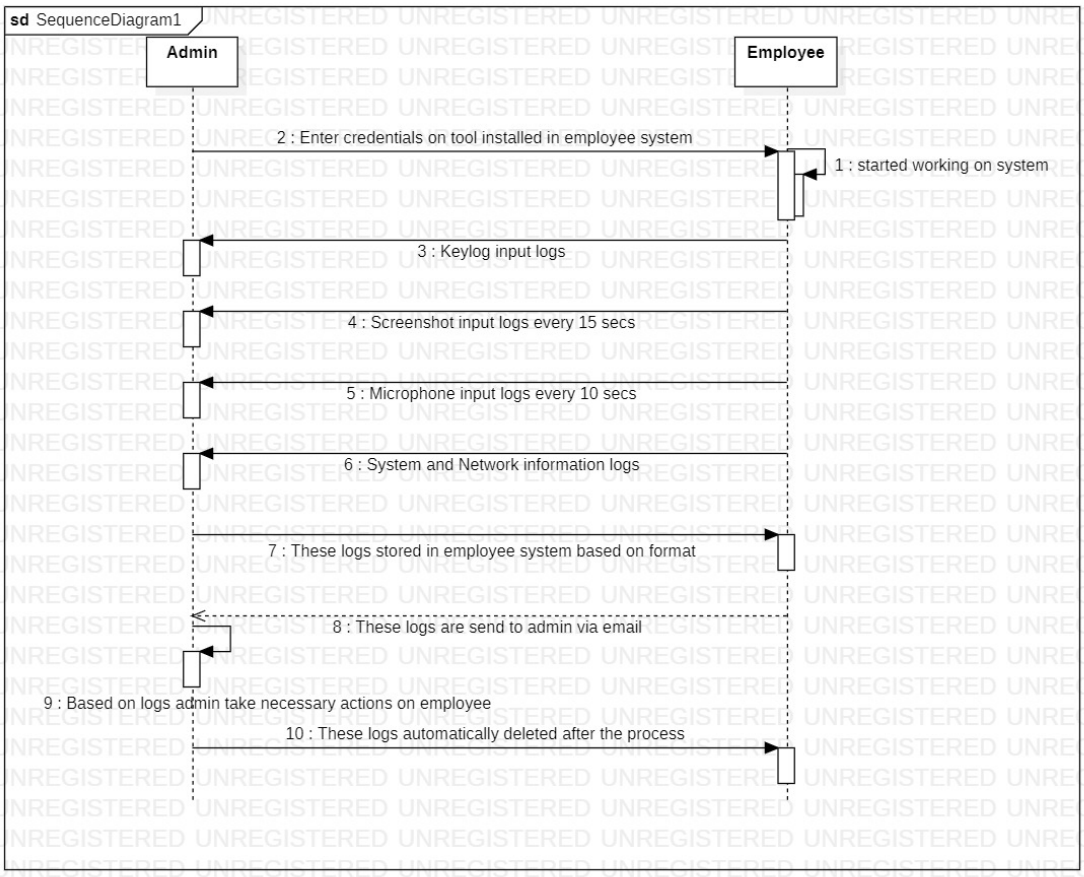


Figure 4.5: Sequence Diagram of Proposed System

CHAPTER 5

IMPLEMENTATION AND RESULTS

5.1 Introduction

In this system, we have developed application, compatible for windows OS and implemented on different files like keylogs, microphone, screenshots, system and network information of formats txt, wav, jpg, txt and xml respectively varying from 1MB to 30 MB of file size to monitor the Employee activities by using the tool which consisting of the python as the python consist of powerful libraries and methodologies like logging for tracking keyboard inputs, Pathlib for storing the logs in the specified directory, Process for multiprocessing , subprocess for generating new processes and fetch the results by generated processes, Imagegrab for capturing the images on screen, sounddevice for recording the audio signals, smtplib for sending mail to any machine which have internet connection with an SMTP listener, requests for sending HTTP request, shutil for file copying and removal, socket for getting access to BSD socket interface, os for interaction of tool interface with operating system, re is regular expression used for pattern matching, mime for extending email messaging and time for time-related functions. With all these powerful libraries the implementation of the tool is easy and the employee's activities can be monitored by the admin easily.

5.2 Method of Implementation

5.2.1 Output Screens and Result Analysis

Below Output Screen, depicts about the Logs directory created in the employee system automatically with the help of Pathlib library used for storing the keylogs, screenshot, microphone, system_information and network_information files and from this Logs directory itself the files are sent over email to admin.

The employee activities are tracked and placed under this directory.

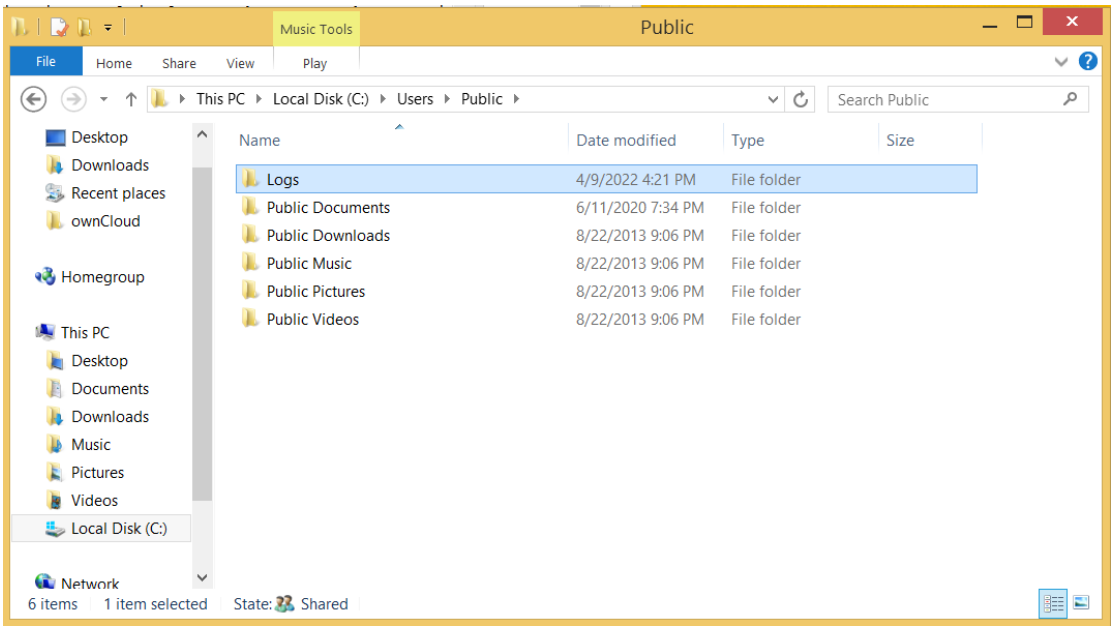


Figure 5.1: Logs Folder

Below Output Screen, conveys that the employee activities which are we considered to monitor the employee by using inputs such as key logs, microphone, screenshots, system and network information which are tracked by activity monitoring tool and placed in the Logs directory which was created in above figure. The files in the Logs directory of different format based on the formats the files are separated and stored under logs directory in the employee system as keylogs of format .txt, screenshots of format .jpg, microphone of format .wav, system_information of format .txt and network_information of format .xml. As these files are sent over internet to the admin email which are stored under Log directory based on format by using regex magic.

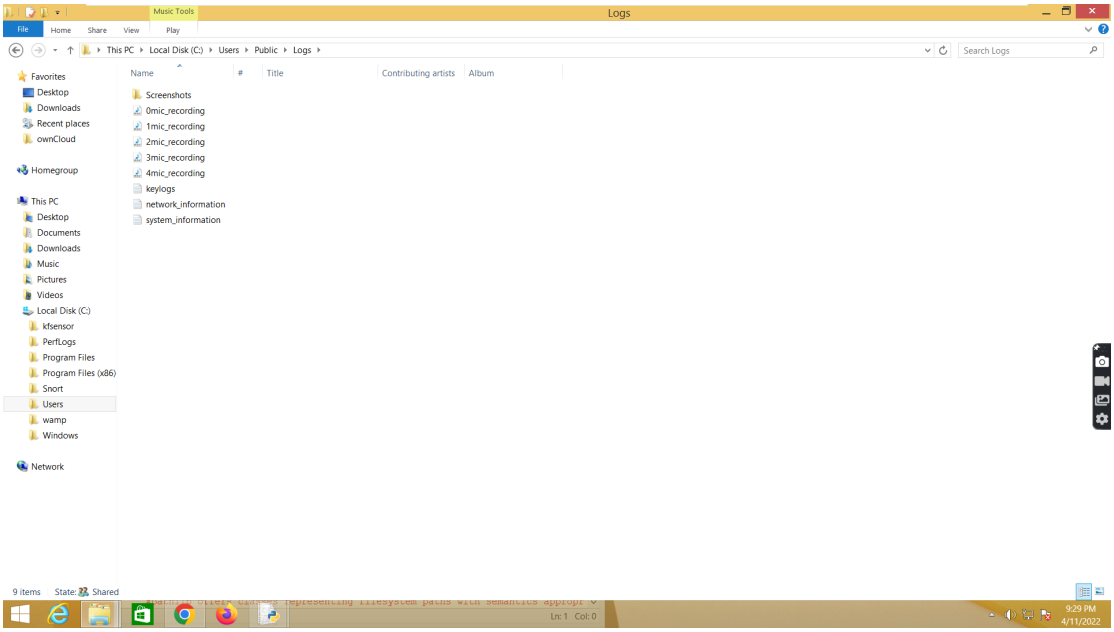


Figure 5.2: Logs Generation

As we can depicts from below Output Screen, that the keylog are stored with format of .txt. In that .txt file the output is observed in the format of date, time and the characters typed in the keyboard. For example, when we type keys on the keyboard we observe that these are displayed character by character accordingly, keys like backspace, capslock, shift, alt, ctrl, fn, esc etc stored in format of key.type of key.

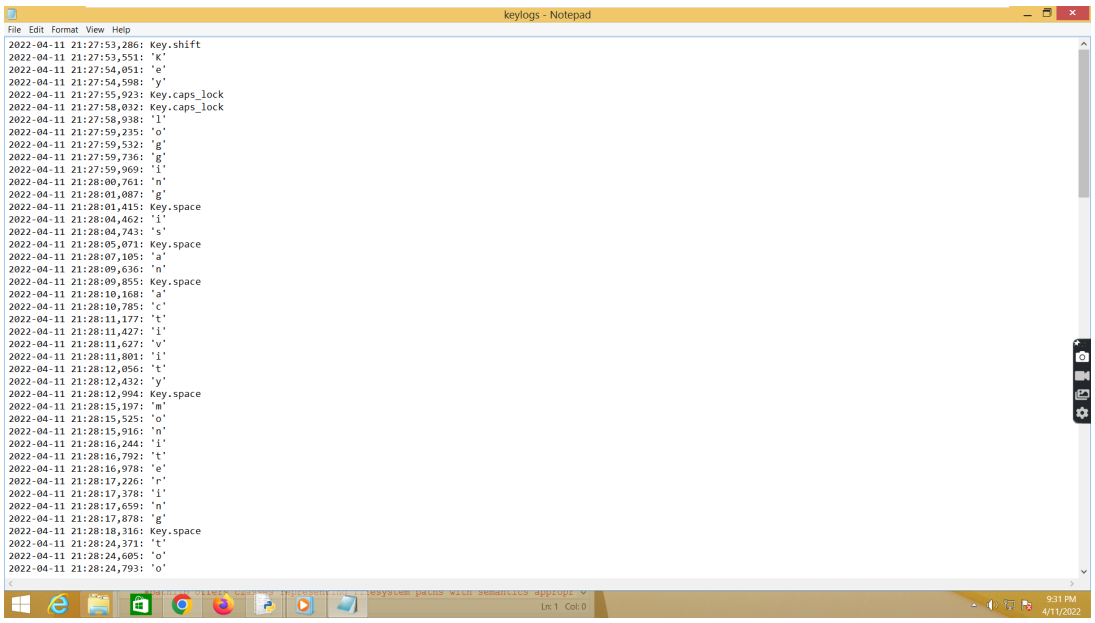


Figure 5.3: Keylog(keyboard)

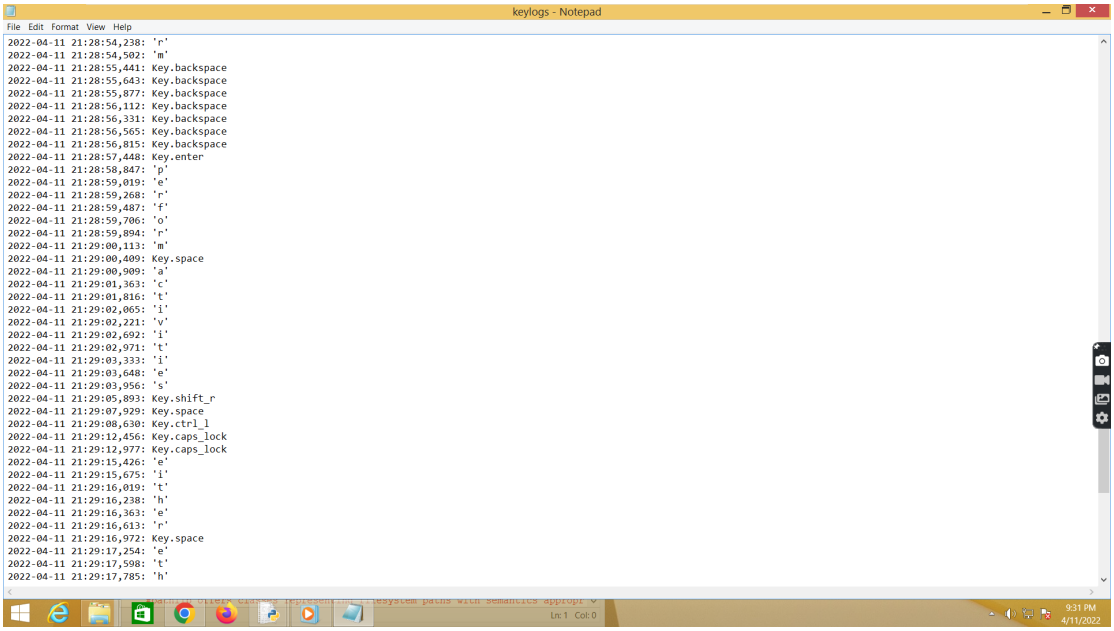


Figure 5.4: Keylog(keyboard)-1

Below Output Screen, Screenshots tracked by module Image Grab and stored in separate screenshots folder path under logs directory as jpg format. At every n seconds screenshots are tracked and stored in screenshots folder. We have made to capture the screen for every 5 seconds and those can be observed in the screenshots folder.

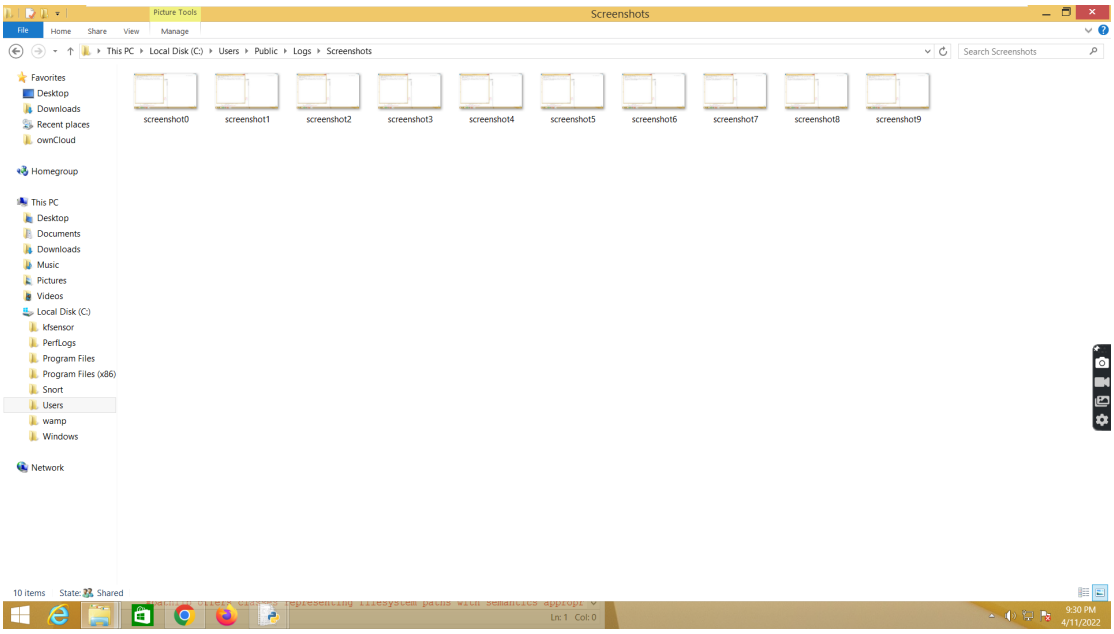


Figure 5.5: Screenshot

Below Output Screen, depicts about microphone recordings tracked by module sounddevice and stored under logs directory as wav format. At every n seconds microphone audio signals are tracked and stored in directory. We have made to capture the voice for every 10 seconds and those can be observed in the logs directory.

Sampling frequency is fixed for sound waves input as 44100 because at that rate the sound waves are clear and that is standard for calculation purpose internally. Every 10 seconds the recording is stored in wav format with recording count.

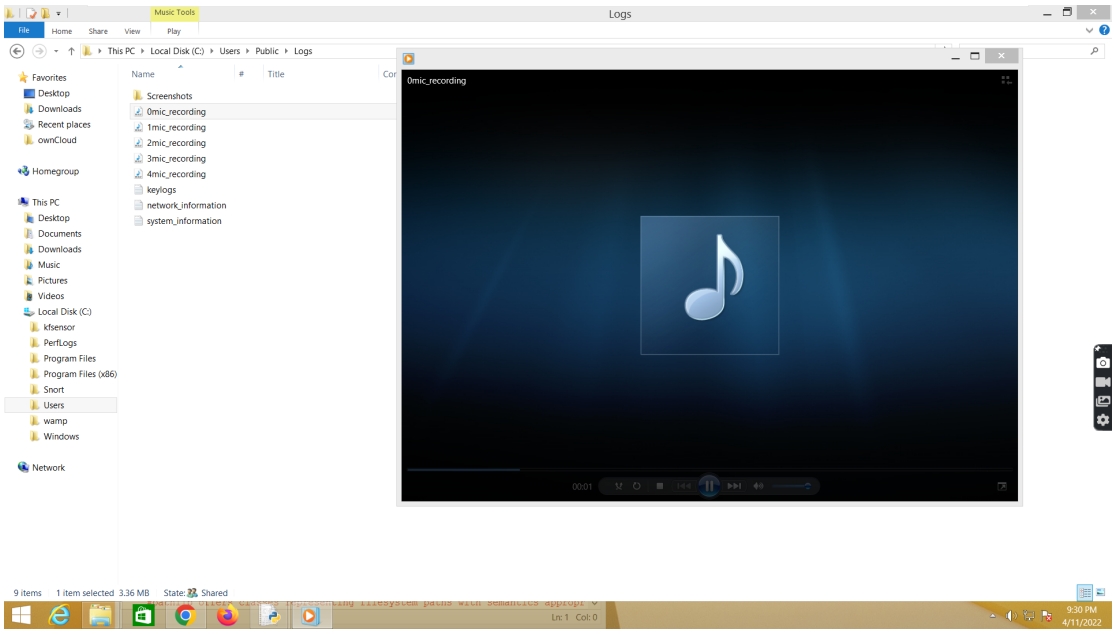


Figure 5.6: Microphone

In the below Output Screen, that system information is retrieved by the commands such as system-info, tasklist, sc, query etc. Using the Multiprocessing module the keylogs, screenshots and microphone inputs are processed as process, but for system information, subprocess is used to spawn the output and we get output such as host name, os version, Manufacturer, Configuration, Build type, BIOS version, Processors, Boot Type, System Boot Directories etc. If any errors countered in system information the errors are seen in error_logs in Logs directory.

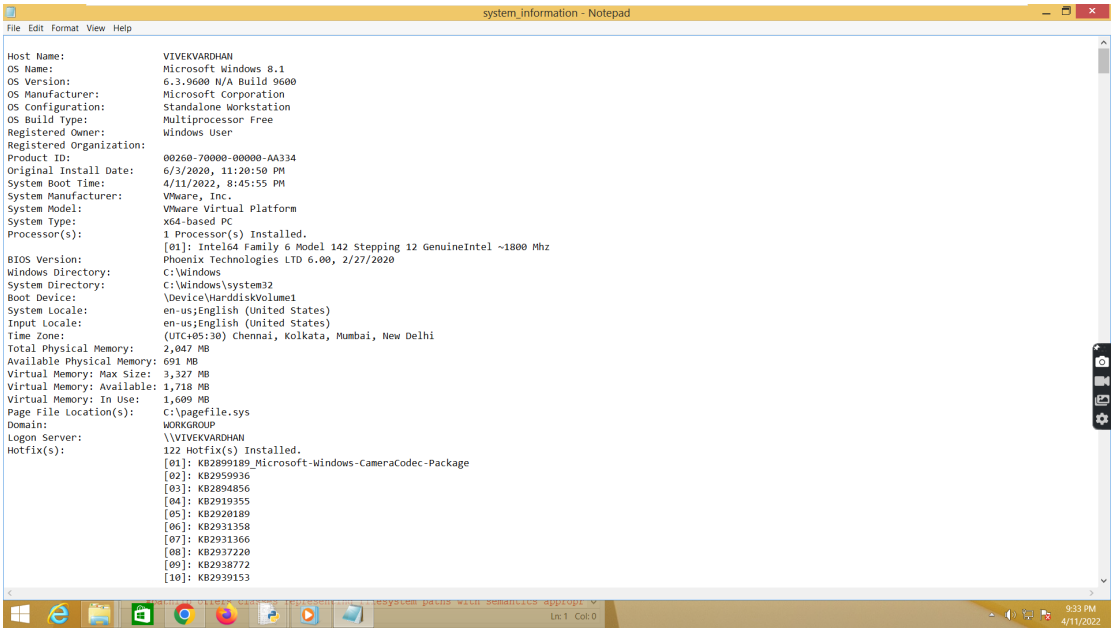


Figure 5.7: System Information

In the below Output Screen, it is observed that the process that are running are being tracked and saved, which says that the activities performed by task manager are observed such as system idle processes, services like svchost, explorer, dasHost, etc and console related sessions such as csrss, winlogon, dwm, etc. If any errors countered in system information the errors are seen in error_logs in Logs directory.

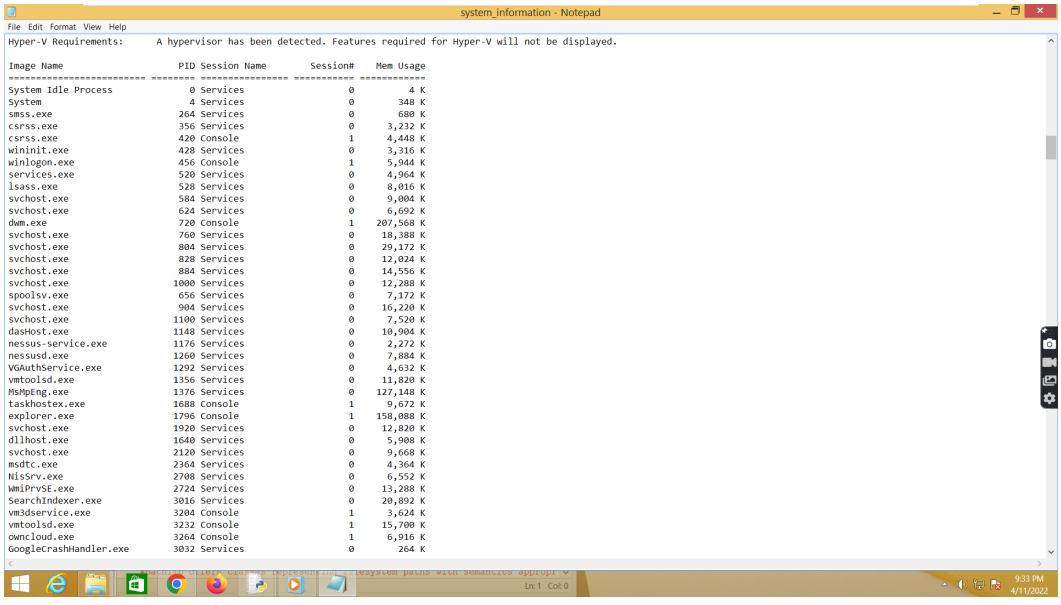


Figure 5.8: System Information-1

In the below Output Screen, it is observed that network information is retrieved by the commands such as netsh, WAN, ipconfig, getmac, route, profile, /all, arp etc.Using the Multiprocessing module the keylogs, screenshots and microphone inputs are processed as process, but for network information, subprocess is used to spawn the output and we get output such as connection specific dns suffix and its description, physical address, auto configuration dhcp enabling, ipv6 address, subnet mask, default gate way, dhcp client-server information, dns servers, tcp / ip connections. If any errors countered in network information the errors are seen in error_logs in Logs directory.

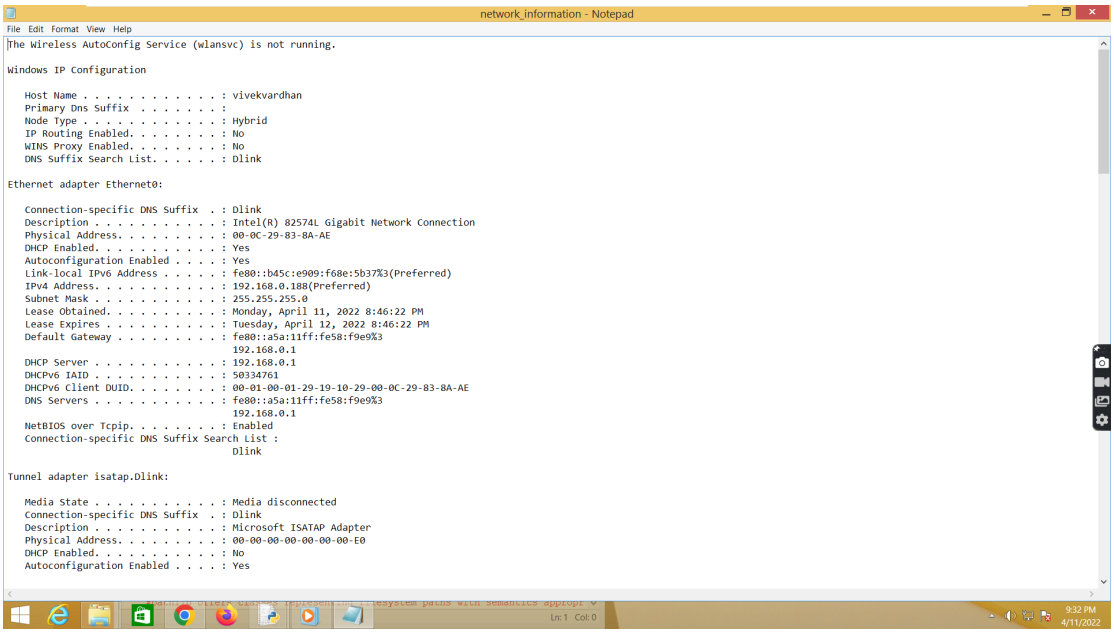


Figure 5.9: Network Information

The below Output Screen, Network Information depicts that IPV4 route table shows active roots in the network such as network destination, netmask, gateway, interface, metrics and it shows persistent roots if any and also IPv6 route table with active roots . The information about the network over an system is stored as .xml format all the network information over internet also and formed as log in employee system in specified path. If any errors countered in gathering the network information due to no internet connection and other module issue to fetch the information the errors are seen in error_logs in Logs directory.

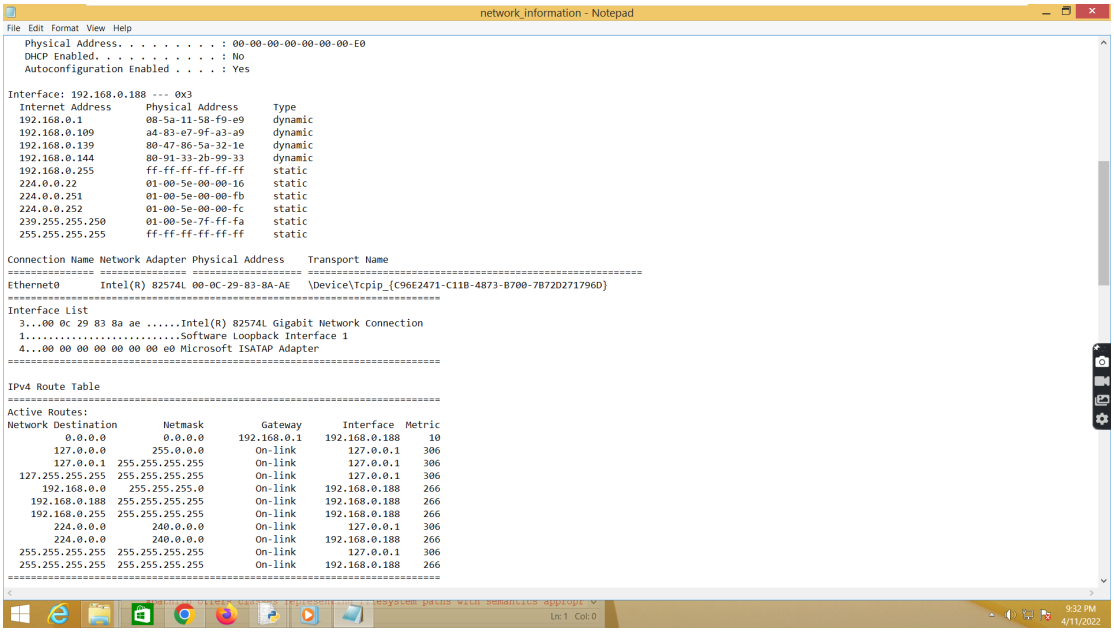


Figure 5.10: Network Information-1

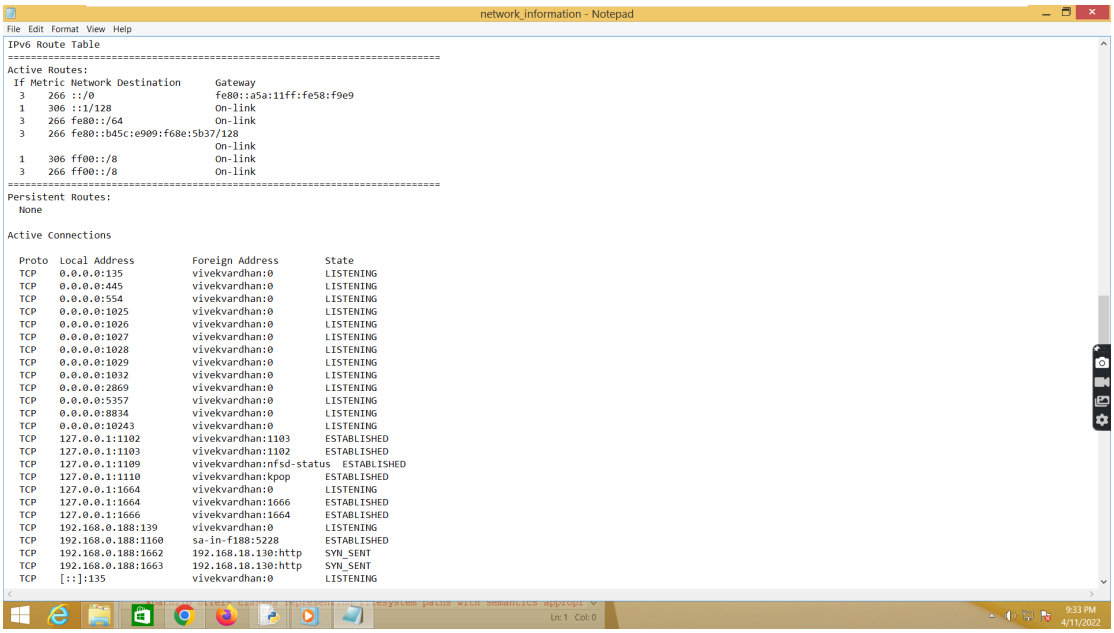


Figure 5.11: Network Information-2

Below Output Screen, describes that the logs which were generated internally in system are being sent to the admin email using modules such as MIME Multipart which sub divides into MIME Base, MIME Text. MIME Base contains header and payload, header contains content type and content

disposition where as payload contains encoding base64. Using SMTP protocol the data in object format is converted into string and sent using tls which is highly secure where email and password are provided and sent into mail. The following files from Log directory are keylogs, Screenshots, Microphone files, Network information and system information. It takes at least of 10 to 20 minutes of time to observe the data in mail provided the Internet connectivity speed. Below figure is an example for files from Log directory are forwarded to admin email.

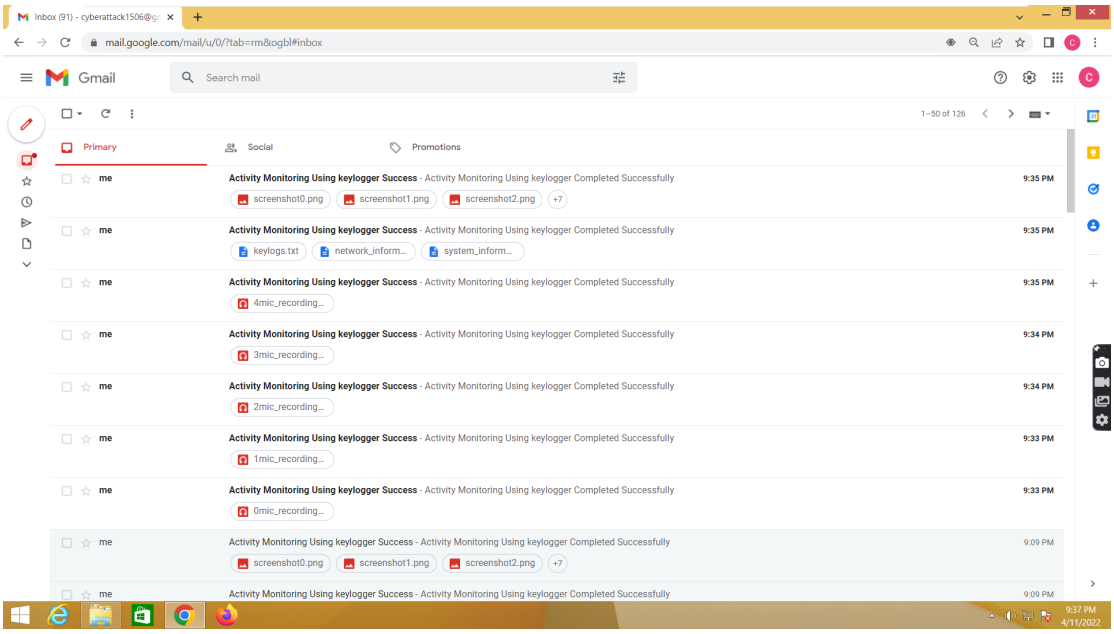


Figure 5.12: Logs in Admin Email

Below Output Screen, Keylogs, System and Network Information in email says that the files related to .txt format and .xml format of keylogs, system_information and network_information respectively are sent in combined way and other formats are send based on their type of file, as we use regex magic modules for checking and matching the file format accordingly and are sent respectively. As key logs,network information and system information are of .txt format and .xml format so, they are combined and sent at combinely. MIME Base has application used with octet stream with attaching filename and its related properties.

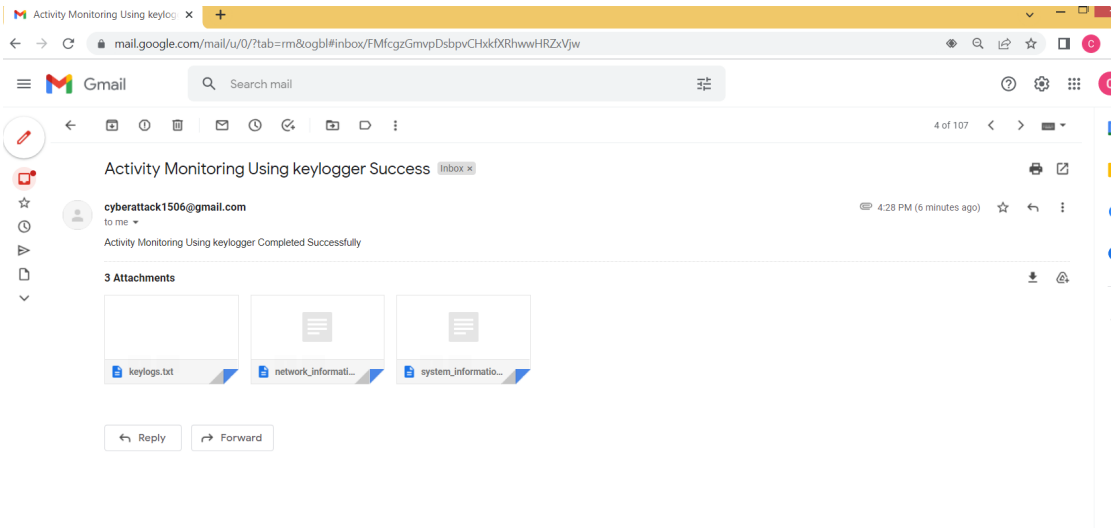


Figure 5.13: Keylogs, System and Network Information in Email

Below Output Screen, Screenshots in email depicts that the screenshots folder of format jpg so they are taken as one and sent in one mail, this is possible with regex magic as it represents pattern matching accordingly. So, the .jpg format files are grouped by regex magic and sent to admin email. Screenshots take medium time compared to recordings and more time to .txt format files because of its size. SMTP port 587 which is latest and most secure port of Gmail server. Even Screenshots are internally converted into standard part by MIME Multipart module and finally displayed in original format.

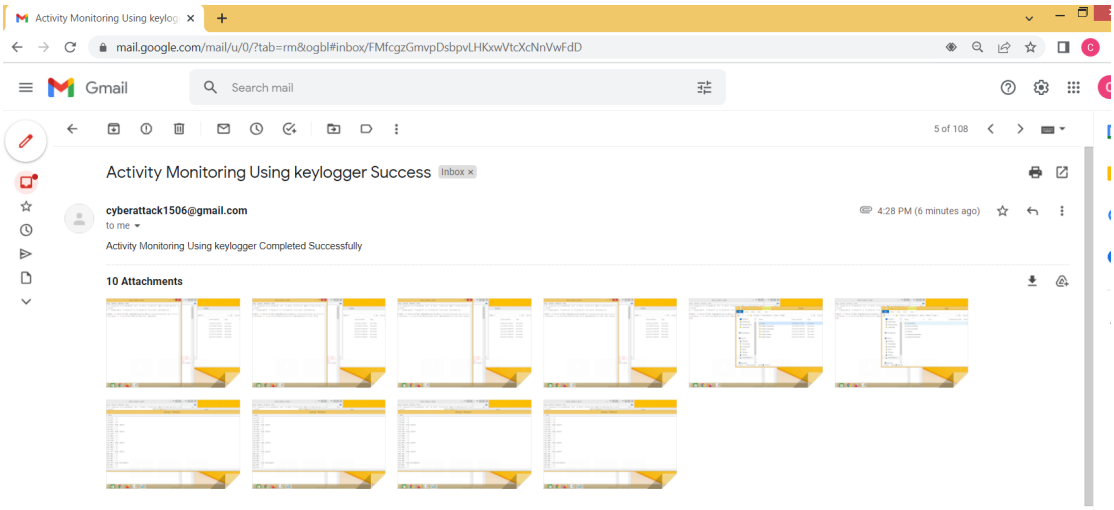


Figure 5.14: Screenshots in Email

Below Output Screen, Microphone in email conveys us that Microphone files of audio signals are recorded using numpy arrays and default frequency and fps which are of format wav are sent as separate composition in a single mail to the admin email. As microphone files are of larger size they take more time compared to text and jpg formats. Each file of duration 10 seconds are sent and listenable. We should enable auto refresh for every interval in browser in order to lookup for latest files.

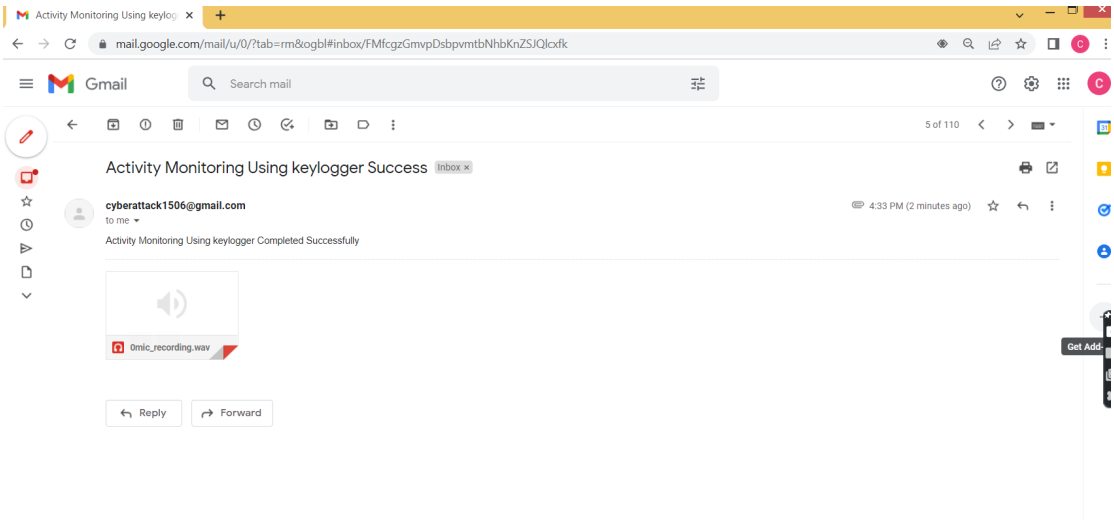


Figure 5.15: Microphone in Email

In Below Output Screen, we can observe that logs files in the Log directory is deleted after the whole process is completed based on the information in the email the admin take necessary actions on employee. These files are deleted because all the files such as screenshots, microphone recordings, keylogs ,network information, system information even with the Logs directory which all these files in it are sent successfully to admin email, as the module shutil used for file creation and deletion. So we use the delete function in shutil module which deletes once its confirmation of sending all files into email was successful. Once all the Multiprocesses assigned to each tasks / inputs are completed. After their termination, shutil deletes total directory and all files in that directory will be deleted.

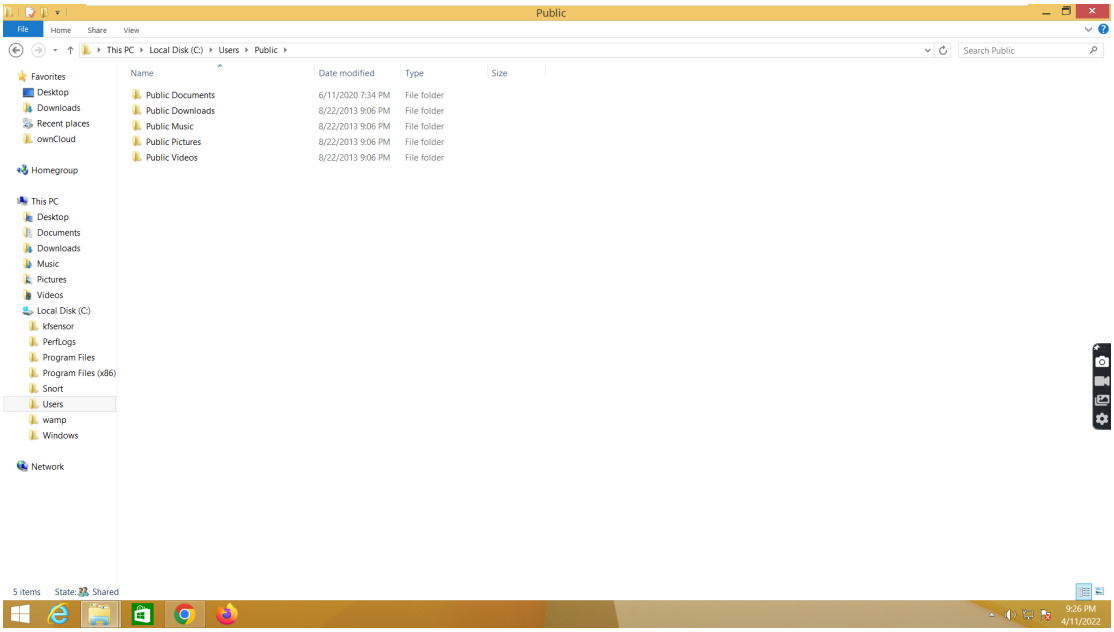


Figure 5.16: Logs folder Deleted

Below graph depicts that use of keyloggers from 2000. As the Keyloggers have been around since the mid-1970s, when the Soviet Union invented the "Selectric bug" to target typewriters. Keyloggers have come along way since then. In the previous ten years, there has been an increase in both efficiency and usability. As the name implies, keyloggers can only produce results if the keys are logged. When Microsoft Windows 8 was released in 2012, it came with a touchscreen personal keyboard, which posed a serious challenge. The usage of key loggers are increasing year by year as the companies with high advanced security tools also the data theft is happening because of the employee within an organisation. As the Keyloggers are used for both legal and illegal purposes [4]. Attackers employ them to compromise user's privacy in order to steal personal data, but they can also be utilised in everyday life for legitimate purposes such as child monitoring, forensic investigation, and ethical hacking.

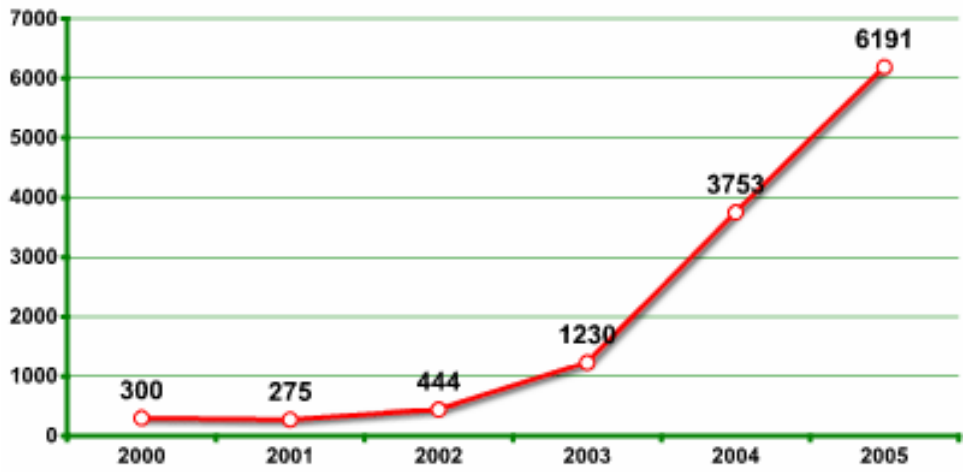


Figure 5.17: Analysis of keylogging functionality by IT security companies

CHAPTER 6

TESTING & VALIDATION

6.1 Introduction

In this testing phase, we need our application to run only when logs are generated by monitoring the employee events and when the logs are send to the admin email. Testing is a way to verify that your actual software product is compatible. Confirm that the expected requirements and software products are defective freedom. You must run the software / system components manually. An automated tool for evaluating one or more properties of interest. Purpose of Software testing, on the other hand, aims to identify errors, gaps, or missing requirements.

Types of Tests

Functional Testing

Requirements are required to define the features that a network or component seem to have. Functional tests ensure that the features under examination are available as stated in the business needs, documentations, and user manuals in a systematic manner. Test cases are developed and prepared with the goal of focusing on requirements, vital capabilities, or type of test scenarios. Furthermore, thorough coverage of Workflow flows, data fields, standard procedures, and following processes must be considered during testing. Before functional testing is done, further tests are identified, and the effective value of existing tests is determined.

Unit Testing

Unit tests concentrate verification efforts on the tiniest software components. This is a module for design. Within a module, unit tests follow a specified path. Full coverage and maximum error detection are ensured by the control

structure. This test examines each module separately to confirm that it is operational. As a group, we have rights. As a result, the name refers to a unit test. Each module is separately tested in this test, and the modules and interface are examined for conformity with the design criteria. Every significant processing path is put to the test to see if it produces the intended outcomes. All error handling paths should be thoroughly tested

Integration Testing

Validation and programme development are two difficulties that integration testing solves. A variety of high-level tests are run after the software has been incorporated. The primary purpose of this testing procedure is to obtain unit-tested modules and to construct the programme structure specified by the design.

System Testing

The purpose of the test is to find faults. Testing is the process of attempting to find all of a product's flaws or vulnerabilities. Components, sub-assemblies, assemblies, and/or finished goods are all examples of finished goods. This is the act of putting software through its paces in order to ensure that it meets the needs and expectations of its users. Don't let yourself down in a bad way. There are several types of testing. Each test type corresponds to a certain test requirement.

User Acceptance Testing

User acceptance testing is a vital element of any project that necessitates a significant amount of end-user participation. Check that the system meets the functional requirements as well. User Acceptance Testing (UAT) is a sort of testing in which the end user or customer verifies and accepts the software system before it is deployed to production. UAT is done at the end of the testing process, after functional, integration, and system testing. The basic goal of UAT is to verify the entire business process. Graphical errors,

misspellings, and system testing are not addressed. User Acceptance Testing is done in a separate testing environment with data that is similar to what is used in production.

- When: After system test
- WHO: User and Customer Product Team
- Method: Black box method

Smoke Testing

Smoke testing is used to check stability of the system. Smoke testing, also known as build verification testing or build acceptance testing, is a non-exhaustive software analysis that ensures that the most crucial aspects of a programme operate properly but does not go into deeper detail. Smoke testing refers to the preliminary inspection of software after it has been produced but before it is released. This sort of testing identifies basic and critical faults in an application prior to performing critical testing.

- When: After new features are added or fixed
- WHO: Developers and testers

Sanity Testing

Sanity Testing are run when you receive a software build with minor changes to your code or functionality. Regression testing includes sanity testing. Sanity testing is done to confirm that the code changes are functioning properly. Sanity testing is a check to see if the build's testing can continue or not. During the sanity testing phase, the team's primary goal is to validate the application's functionality rather than to perform extensive testing. Sanity testing is typically performed on builds where immediate production deployment is required, such as a critical bug repair. The primary objective of sanity testing is to ensure that the changes or new functionality perform as expected. If the sanity test fails, the testing team rejects the software product to save time and money.

- When: Minor changes will be made
- WHO: Developers and testers

Regression Testing

Regression testing is performed to validate that the modifications are made to the software work as expected and without effecting existing functionality. Regression testing is a type of testing that is used to guarantee that a change in software code does not impair the product's current functionality. This is done to ensure that the product continues to function properly in the face of new functionality, bug fixes, or changes to existing features. Previously executed test cases are re-executed to validate the impact of the modification. Regression Testing is a type of Software Testing in which test cases are re-executed to confirm that the program's previous functionality is still functioning and that the new changes have not introduced any new flaws.

- When: Added new feature.
- WHO: Developers and testers.

Alpha Testing

A sort of acceptance test is the alpha test. Before the product is released to the general public or the general public, this test is run to uncover any potential flaws or bugs. The goal of these tests is to use BlackBox and WhiteBox approaches to emulate real users. The purpose is to do tasks that a normal user would complete. Alpha testing tests your application as development nears completion. As a result of the alpha test, minor design changes can be made. This is done in the lab environment of the developer's site. The developer observes the user and identifies the problem. Testers are inside the organization and are primarily internal software QA and test teams. This type of test is only referred to as alpha because it is performed at the conclusion of software development and prior to beta testing.

White Box Testing

White Box Testing is a sort of testing in which the software tester is familiar with the software's inner workings, structure, and language, or at the very least its aim. It has a purpose. It's utilised to evaluate sites that aren't accessible

from the black box level. White box testing is used by both developers and testers. It helps them determine which lines of code are executed and which are not. This could indicate a logical gap or a typo, both of which can have catastrophic consequences. That each independent path within a module has been tested at least once. All logical decisions have their true and false values validated. Internal data structure validity is ensured by all loops that are executed at their boundaries and within their operational constraints.

Black Box Testing

Black box testing is the technique of evaluating software without knowing anything about the inner workings, structure, or language of the module being tested. Black box tests, like the majority of other types of tests, require a definitive source document, such as a specification or requirements document. It's a testing technique that treats the programs under test as if it were a black box. There is no way to "look" into it. Regardless of how the software works, the test generates inputs and responds to outputs. Because it exercises a system from beginning to end, black box testing is a powerful testing technique.

Beta Testing

Beta testing is also a type of acceptance test performed by a specific group of actual users of your application. This is the final stage of testing and will be run in a production or real environment. To achieve this type of testing, the software is shared with a small number of external members or customers who do not belong to the organization. They provide feedback on product design, functionality, and overall quality. These tests are very useful because they get reviews directly from the people who actually use the product after the final release and reduce the risk of software failure. There are different types of beta tests, including traditional beta tests, public beta tests, technical beta tests, centralized and post-release beta tests.

Non-Functional Testing

Non-functional testing is a type of software testing that examines the non-functional aspects of a software programme (performance, ease of use, reliability, etc.). It's designed to see if the system can handle Non-Functional parameters that aren't covered by functional tests.

Non-Functional Testing Parameters

Security : The parameter specifies how a device is covered from intentional and accidental assaults from each inner and outside sources. Security Testing is used to affirm this.

Reliability : The diploma to which a software program device plays the prescribed capabilities with out fail over time. Reliability trying out is used to affirm this.

Survivability : In the occasion of a device failure, the parameter guarantees that the software program device maintains to paintings and recovers. Recovery Testing verifies this.

Availability : The value of this option affects how reliant the user can be on the system during its operation. Stability Testing verifies this.

Usability : The ease with which a user may interact with a system to learn, operate, and prepare inputs and outputs. This has been verified by Usability Testing.

Scalability : The word refers to the extent to which a software application‘s processing capability can be expanded to meet increased demand. Scalability testing is used to verify this.

The testing phase can be divide in two ways one is for logs generation and another one is about forwarding these logs to email.

The logs generation will be successful when the powerful python libraries such as logging, ImageGrab, sounddevice, process, subprocess work efficiently by generating the inputs which are to be monitored like keylogs, screenshots,

microphone, system and network information as txt, jpg, wav, txt, xml respectively stored in the Logs directory. If any error triggered in the above inputs the error_log folder will be triggered in the Logs directory.

Forwarding of these logs to email is based on the MIME, smtp python libraries and also there must be internet connection. The files in the Logs directory of various formats, so with respect to the format the files are forwarded to the admin email with the help of the regex magic by pattern matching as .txt files of system_information, keylogs and .xml of network_information ar grouped and forwarded to the mail. .wav files of audio recordings are sent separately and screenshot files are sent separately to admin email.

6.2 Design of Test Cases and Scenarios

6.2.1 Scenario – 1

If the inputs such as keylogs, screenshots, microphone, system_information, network_information are captured according to their formats are stored as log files. Hence log files are generated successfully.

6.2.2 Scenario – 2

If the inputs such as keylogs, screenshots, microphone, system_information, network_information encounter any error then error_log is created. Hence log files are failed.

6.2.3 Scenario – 3

After Capturing of the log files, these log files are forwarded to the admin email so that monitoring of the employee activities is possible.

6.2.4 Scenario – 4

After Capturing of the log files, if the log files are not forwarded to the admin email due to any internet issues or any library issue then monitoring of the employee activities is not possible.

Test Cases				
Test Case ID	Test Scenario	Test Case	Test Data	Result
CS_MP_01	Generating log files	Log files Creation	Modules taken input Successfully	Log files Generated Successfully
CS_MP_02	Generating log files	Log files Creation	Modules thrown Error	Log files Generation Failed
CS_MP_03	Detection of files in Email	Validation of Email and Password	Valid Information	Log files Sent Successfully
CS_MP_04	Detection of files in Email	Validation of Email and Password	Invalid Information	Log files Sending Failed

Table 6.1: Test Cases for Activity Monitoring Tool

CHAPTER 7

CONCLUSION

In this project, we proposed an activity monitoring tool for monitoring employee's behaviour with the inputs are Keyboard, Screenshot, Microphone, System information, Network information. As the Attackers employ them to compromise users' privacy in order to steal personal data, but they can also be utilised in everyday life for legitimate purposes such as child monitoring, forensic investigation, and ethical hacking. With the help of this tool, we can monitor employee's behaviour like When the employee started working with the system all his work will be monitored based on different types of files like keylogs, microphone, screenshots, system and network information of formats txt, wav, jpg, txt and xml respectively. These files are stored in the specified path in employee system and the tool with respect to the operating system forward these files to the admin email which is specified previously. Based on these logs information, the employee activities will be monitored frequently with help of keylogs, microphone, screenshots, system and network information inputs and action can be taken by the admin based on employee activities.

The Main Advantage of Activity Monitoring tool for windows using keystroke logging is to maintain Information security with an organization.

REFERENCES

[1] Christopher Wood and Rajendra Raj. "Keyloggers in Cybersecurity Education." In: *Security and Management*. Citeseer. 2010, pp. 293–299.

[2] C Wood and RK Raj. "Sample keylogging programming projects". In: (2010).

[3] Seref Sagiroglu and Gurol Canbek. "Keyloggers: Increasing threats to computer security and privacy". In: *IEEE technology and society magazine* 28.3 (2009), pp. 10–17.

[4] Preeti Tuli and Priyanka Sahu. "System monitoring and security using keylogger". In: *International Journal of Computer Science and Mobile Computing* 2.3 (2013), pp. 106–111.

[5] S Murugan and K Kuppusamy. "System and methodology for unknown malware attack". In: *International Conference on Sustainable Energy and Intelligent Systems (SEISCON 2011)*. IET. 2011, pp. 803–804.

[6] Tom Olzak. "Keystroke logging (keylogging)". In: *Adventures in Security, April* 8 (2008), pp. 1–6.

[7] Andy Davis. "Hardware keylogger Detection". In: *Smith Square London* (2007).

[8] Oleg Zaitsev. "Skeleton keys: the purpose and applications of keyloggers". In: *Network Security* 2010.10 (2010), pp. 12–17.

[9] Yahye Abukar Ahmed, Mohd Aizaini Maarof, Fuad Mire Hassan, and Mohamed Muse Abshir. "Survey of Keylogger technologies". In: *International journal of computer science and telecommunications* 5.2 (2014).

[10] G Canbek. "Analysis, design and implementation of keyloggers and anti-keyloggers". In: *Gazi University, Institute Of Science And Technology, M. Sc. thesis (in Turkish)* (2005), p. 103.