ADDIS ABABA UNIVERISITY
ADDIS ABABA INSTITUTE OF TECHNOLOGY
SCHOOL OF INFORMATION TECHNOLOGY AND ENGINEERING

KEYLOGGER

Fundamentals of Cybersecurity Final Project

PREPARED BY:

Abel Seyoum	ATE/8832/12
Abebe Mihiretu	ATE/9421/12
Abdulfeta Sani	ATE/4581/12
Abenezer Genene	ATE/7579/12
Gizework Tezera	ATE/7612/12

ADVISOR: Mr. Temesgen Kitaw

Date: June 26, 2023

Abstract

Data security and recovery are critically important factors for many companies nowadays. There are numerous instances where data recovery is necessary, and keyloggers are often the preferred solution for these types of problems. Key logging, or keyboard capturing, involves recording keystrokes on a keyboard, usually without the user's knowledge, to monitor their actions. By using keylogger applications, users can retrieve data when a working file is damaged due to power loss or other reasons.

A keylogger is a surveillance application that tracks users and logs keystrokes, using log files to retrieve information. It can help in recalling a forgotten email or URL. In this key logger project, keystrokes are captured and sent to the admin's email address without the user's knowledge within a specific time frame.

Acknowledgement

We would like to express our deepest appreciation to our teacher, Temesgen Kitaw, for his guidance and support throughout the course of Fundamentals of Cybersecurity and this project. We would also like to thank our classmates and families for their valuable feedback and suggestions. Without their help, this project would not have been possible.

Table of Contents

List of Figures

Introduction

Background

The use of keyloggers dates back to the 1970s, when the Soviet Union developed a hardware keylogging device for electric typewriters. The keylogger, called the Selectric bug, tracked the movements of the printhead by measuring the magnetic field emitted by the movements of the printhead. The first computer keylogger was developed by then-graduate student Perry Kivolowitz in 1983 as a proof of concept.

Keyloggers, or keystroke loggers, are tools that record what a person types on a device. While there are legitimate and legal uses for keyloggers, many of their uses are malicious. In a keylogger attack, the keylogger software records every keystroke on the victim's device and sends it to the attacker.

Keyloggers can be used legally (some people even install them on their own devices), and you may have even used a computer with software installed to log keystrokes for monitoring and ensuring safe or approved use. However, it is also a form of data monitoring that hackers and identity thieves use to acquire people's personal information. Keyloggers are often used by cybercriminals to fetch sensitive information like banking details, login credentials for social media accounts, and credit card numbers.

A keylogger, sometimes called 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.

Objective

The main goal of this software is to monitor and record every keystroke made on the keyboard and log it on the user's computer or send it to the administrator via email. It offers data privacy and recovery services for all necessary IT infrastructures.

Purpose

The purpose of this document is to outline the requirements of the keylogger project, which is a tool that is in high demand by IT business infrastructures due to the need for cyber security and Computer Forensics. Key-loggers, which can come in both hardware and software forms, are used to capture and compile a record of all typed keys. The information obtained from keystroke loggers can be saved as a hidden file on the system or sent to the forensic analyst or administrator via email. Our keylogger project has features that include

- Monitoring keystrokes,
- Logging special keys

- Saving the logs as a hidden file on the system

Key-loggers can collect information before it is encrypted, making a forensic analyst's job easier. Most key-loggers work covertly within the system, allowing them to obtain typed information without the user's knowledge. Key-loggers play a significant role in cyber-security and provide a practical approach to understanding topics such as attacker goals, malware types and implementation, the role of malware in infection, and how stealth is achieved in an infected system.

Scope of Developing the Project

The scope of a keylogger project involves creating a software program that can monitor and record keystrokes and other relevant information on a computer system. The software should be capable of capturing login credentials, web history, application usage data, and other relevant information. It should be compatible with different operating systems and software applications and designed with security in mind to ensure that the captured data remains confidential and secure. Additionally, the project should comply with all applicable laws and regulations related to its use.

Keyloggers are often used for malicious purposes and can be used to steal sensitive information such as passwords and credit card numbers. Therefore, it is important to use keyloggers only for legitimate purposes and with the consent of the user. Additionally, keyloggers can be detected by antivirus software and firewalls, so it is important to keep these programs up-to-date.

Overall, the scope of a keylogger project should be based on the specific needs and objectives of the project while taking into account the essential features and requirements outlined above.

Problem Identification

Cyber-security threats are ever-present, with hackers and other unauthorized individuals constantly seeking out vulnerabilities within systems. They aim to gain access to confidential data stored within the system, which can result in harm to the integrity of the data or even data loss. Additionally, the frequency of cybercrimes is on the rise. By obtaining chat logs or keystroke logs from a victim's laptop, it becomes possible to analyze their plans and develop the best approach towards eradicating or resolving the issue.

Project Function

The authorized use of a keylogger involves utilizing the software with the explicit knowledge and consent of the PC owner or security administrator. Typically, authorized monitoring software necessitates physical access to the computer and administrative privileges for proper

configuration and installation, which helps prevent unauthorized use of the program. Such software products often allow for the creation of a "packed" installation executable file, which can be delivered to the user's computer through various ethical and authorized methods. Upon installation, the software does not generate any messages or windows on the screen.

Operating Environment

The Keylogger software developed has the capability to operate on Windows and Linux operating systems. The basic input device is keyboard for this specific version that is developed which will later have other additional feature on the future versions of this Keylogger software like additional input devices mouse, and output devices monitor, mobile devices etc.

Features

The characteristics of the keylogger designed for this project include:

- Recording keystrokes
- Saving the logs as a hidden file on the system

Modules Used

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

- Pynput.keyboard is used for this specific project version.

Software Used

- Languages: Python
- Tools: PyCharm, Python 3.11

Code and Implementation Screenshot

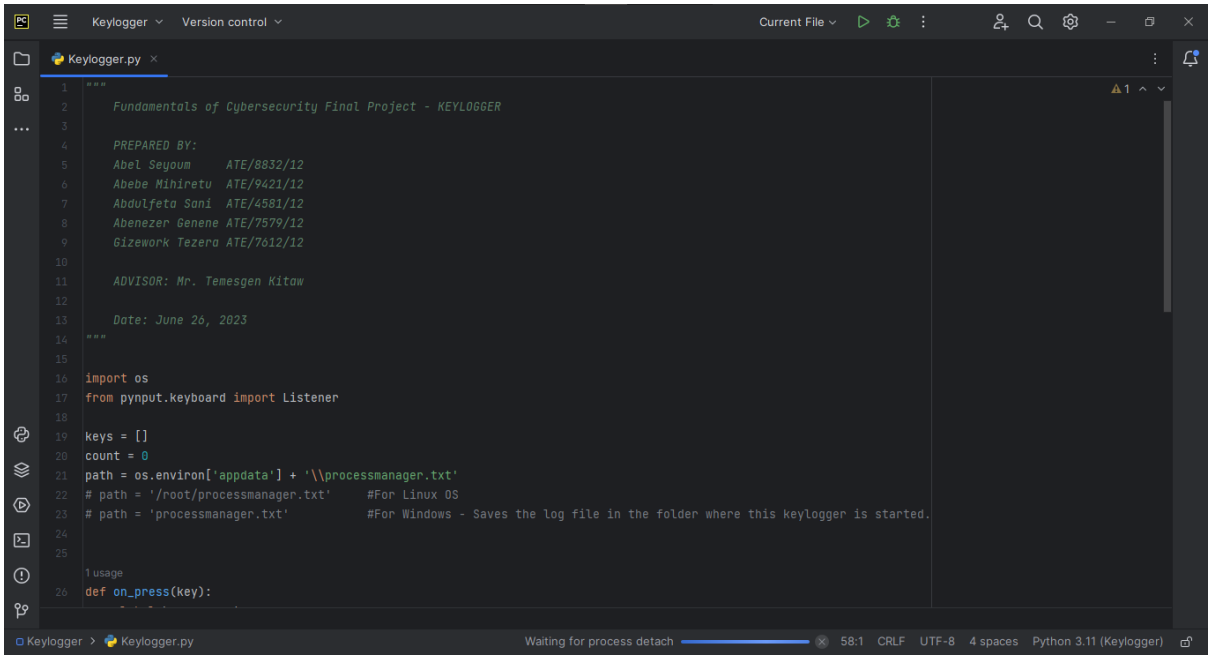

Table 1: Development environment and code screenshot 1

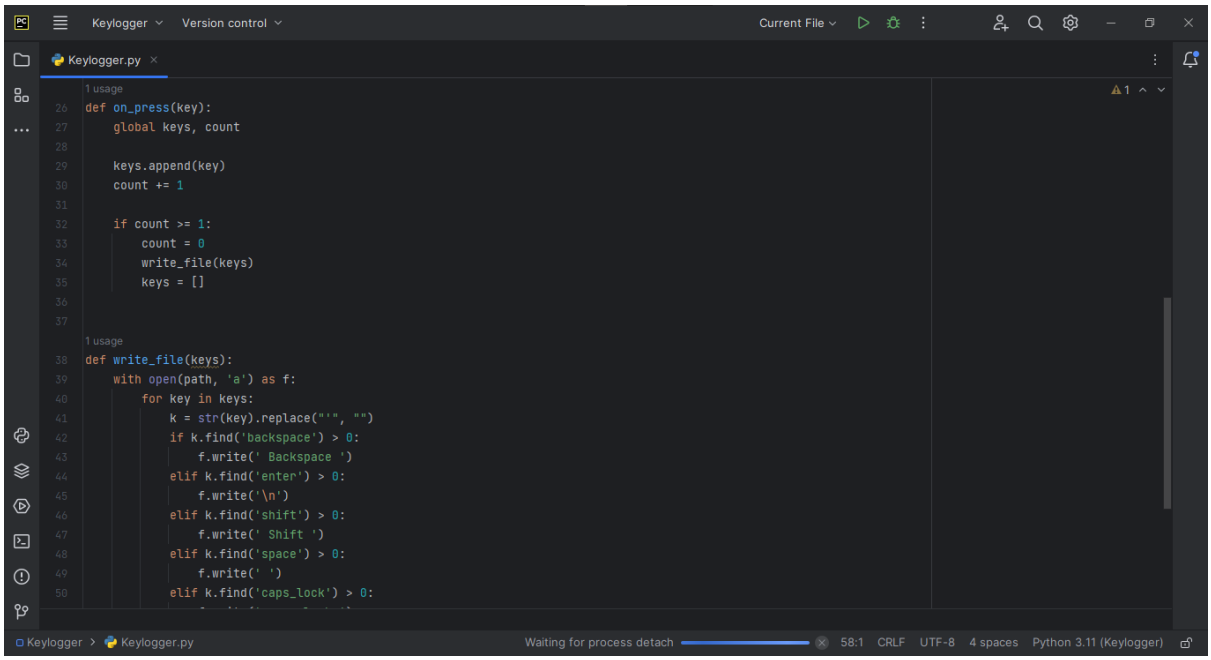

Table 2: Development environment and code screenshot 2

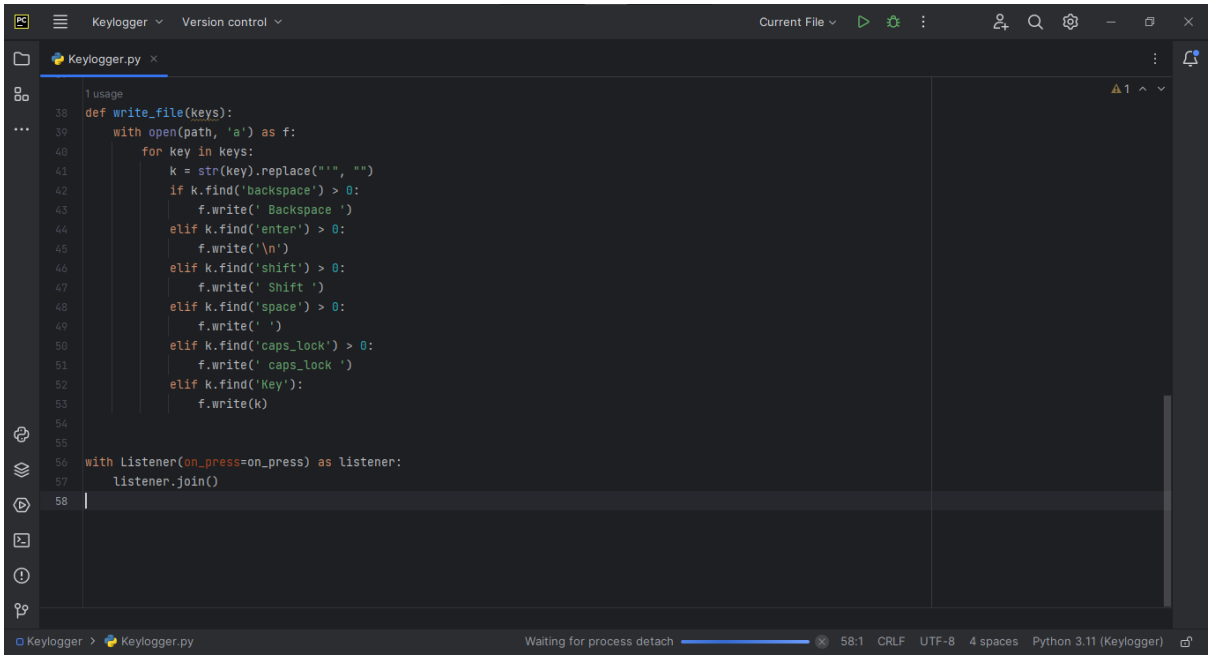

Table 3: Development environment and code screenshot 3

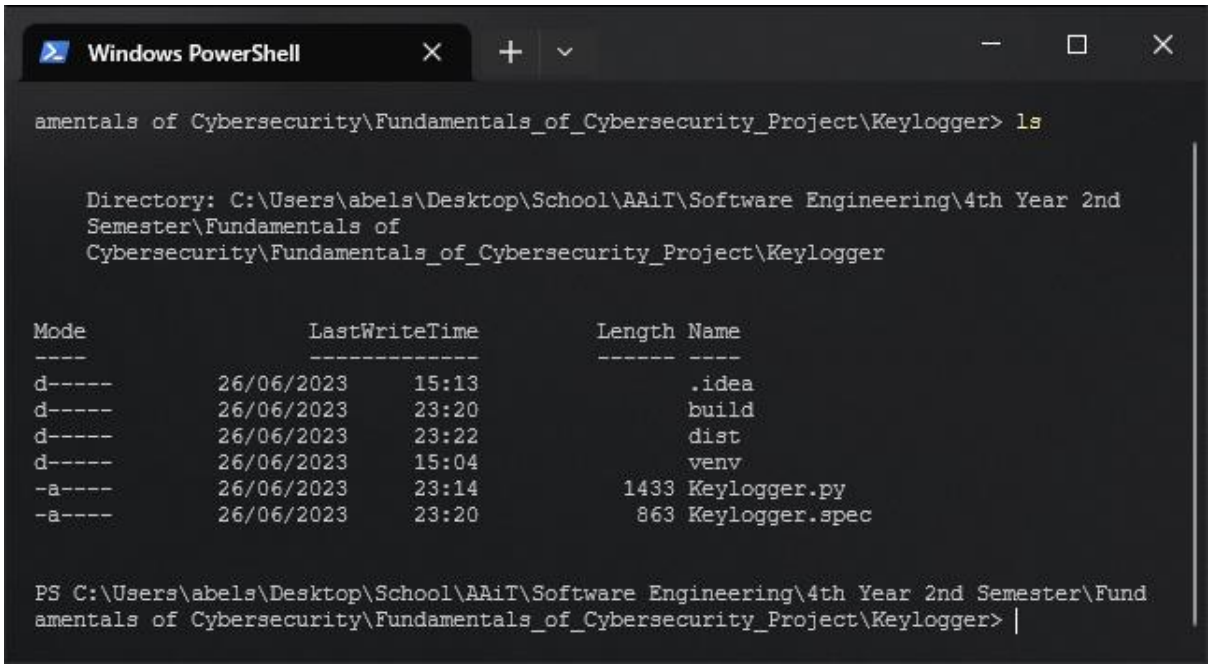

Table 4: Checking file lists on project directory

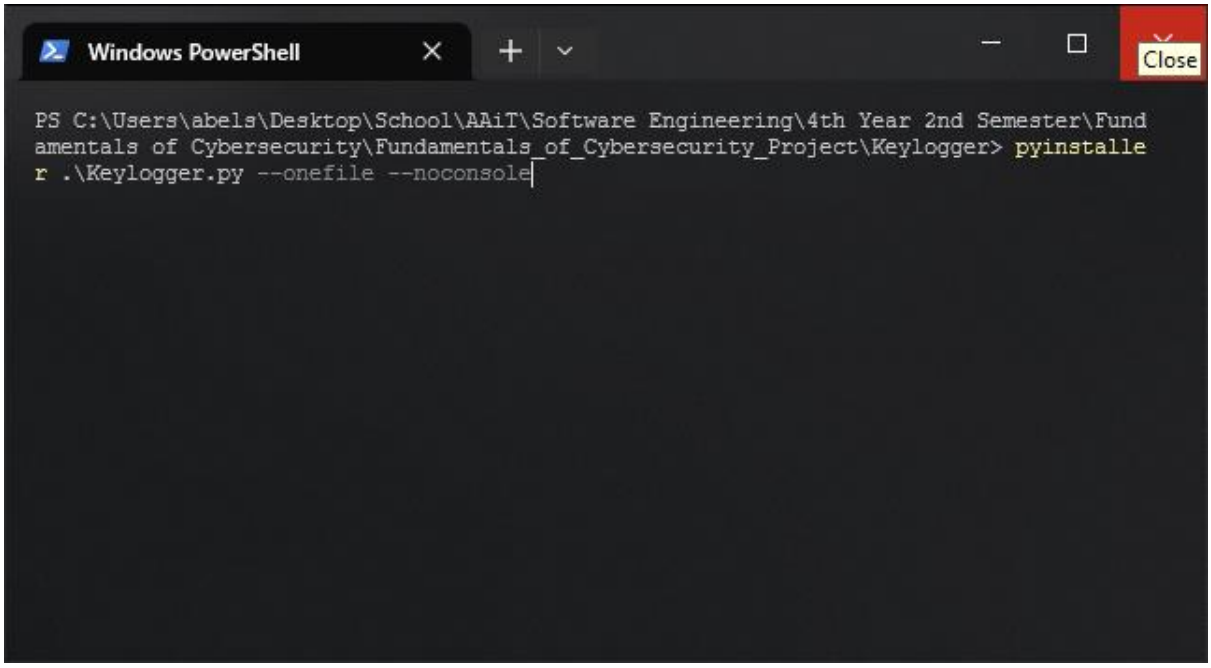

Table 5: Process of converting the Keylogger.py file to an executable file

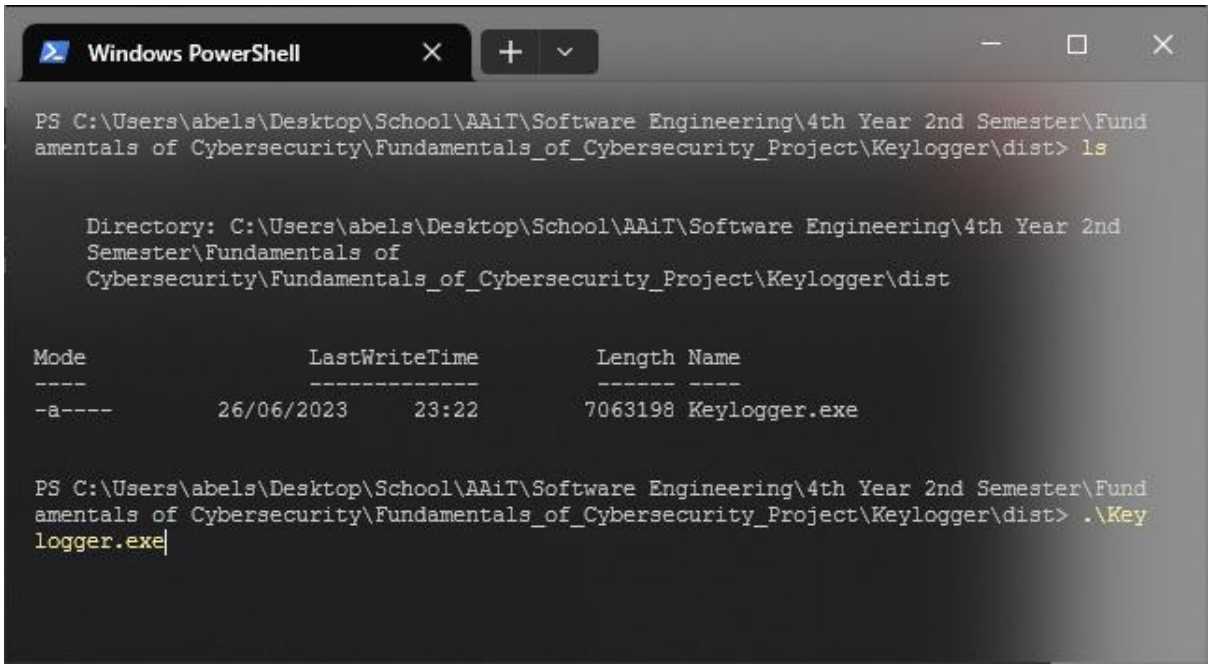

Table 6: Running the Keylogger executable file

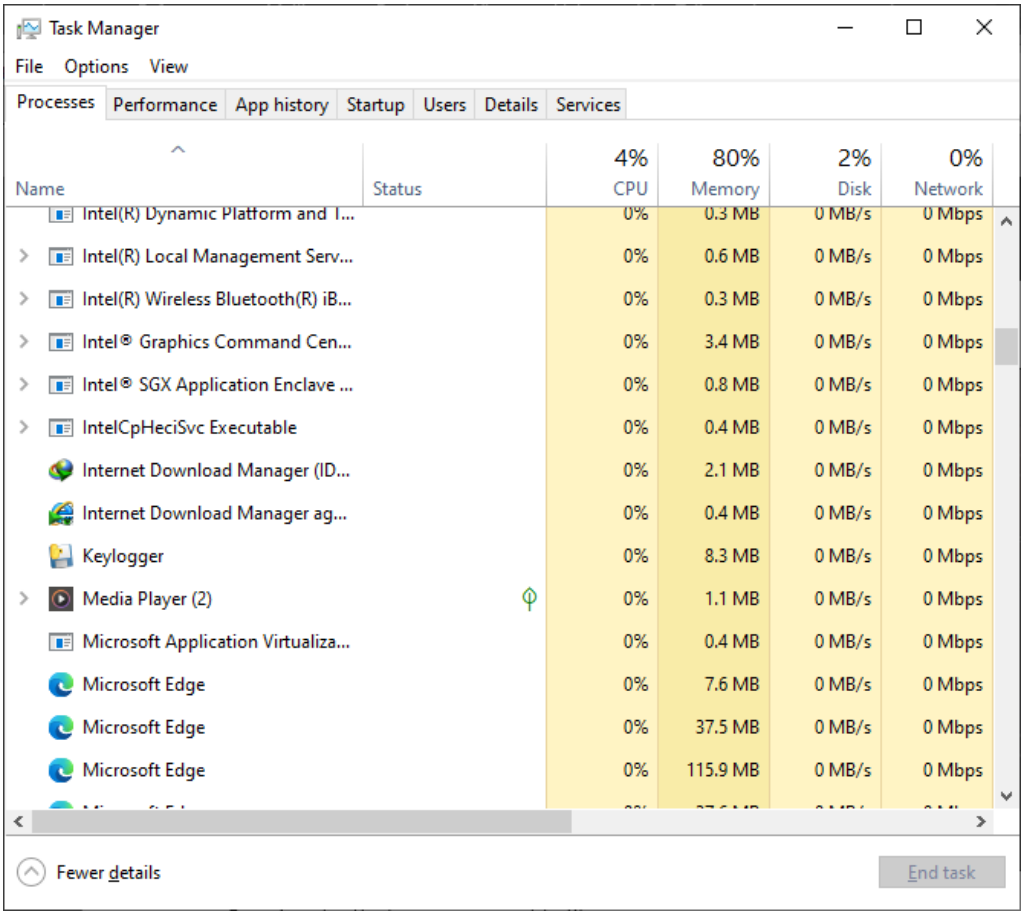

Table 7: Checking if the Keylogger software is up and running

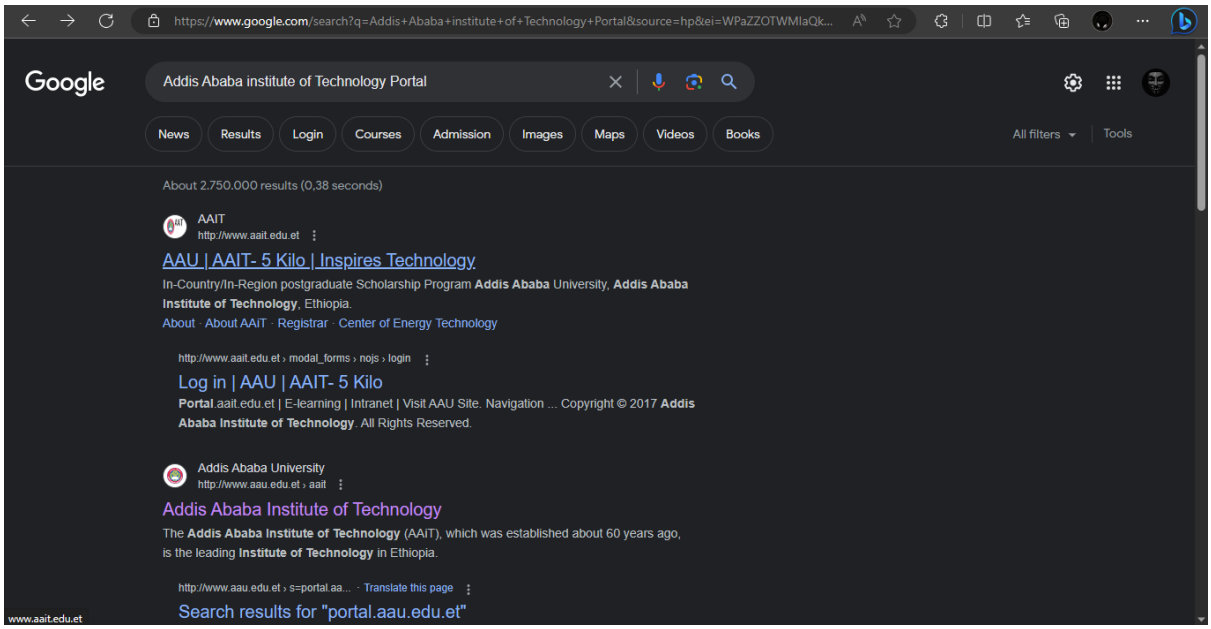

Table 8: Testing if the Keylogger is working and logging

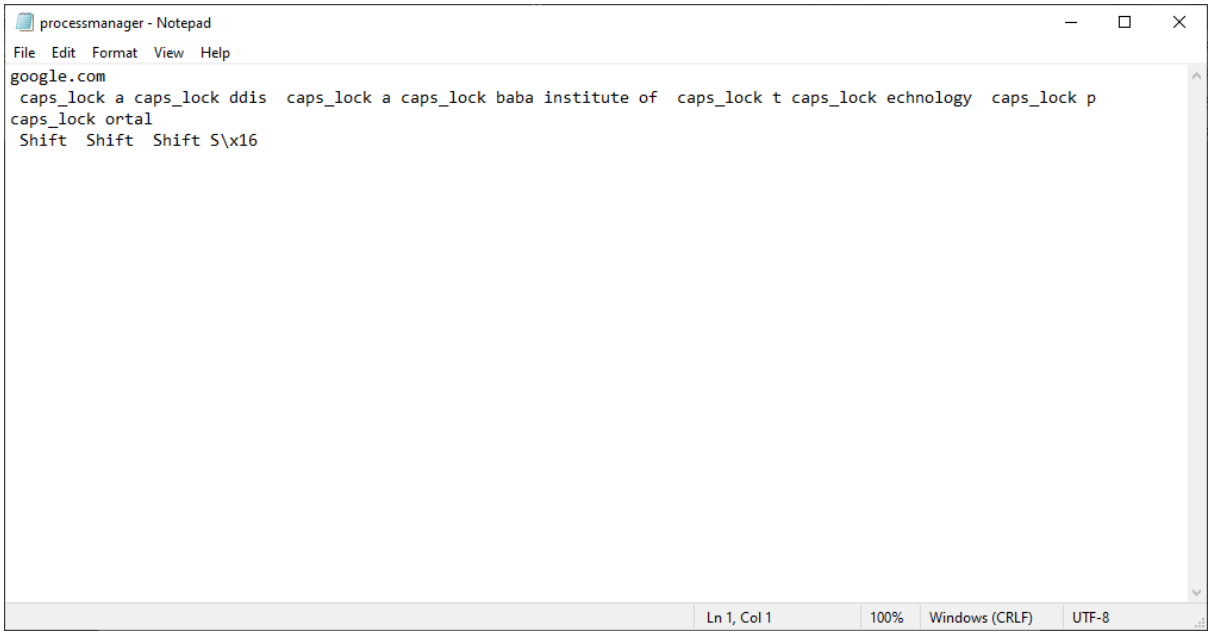

Table 9: Checking the log file stored in the computer system

Conclusion

A keylogger is a type of surveillance software or hardware device that has the capability to record every keystroke. A keylogger recorder can record instant messages, e-mail, and any information you type at any time using your keyboard. The log file created by the keylogger can then be stored on the system or sent to a specified receiver. There are two types of keyloggers namely Hardware Keyloggers & Software Keyloggers. This project demonstrates how a keylogger software works and records data. This can be used to monitor user's activity for companies with the proper authorization. It can also be used for malicious activity by an attacker and be used to steal sensitive information for the victim without the knowledge of the user or victim.

In conclusion, a keylogger can be a useful tool for monitoring computer activity and capturing important information such as login credentials and web history. However, it is important to develop and use keyloggers responsibly and ethically to avoid any legal or ethical issues.

Note: We have pushed the source code for our Keylogger project on GitHub additional to the compressed (zip file) source code we will attaching here with this document.

GitHub: Kali-Brook-SE/Fundamentals_of_Cybersecurity_Final_Project-Keylogger (github.com)

Reference

https://www.youtube.com/

https://www.google.com/