NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

LAB 13

LAB 13: Study of malicious software using tools: Keylogger attack using a keylogger tool.

ROLL NO	52
NAME	Sarvesh Patil
CLASS	D15A
SUBJECT	Internet Security Lab
LO MAPPED	LO5: Use open-source tools to scan the network for vulnerabilities and simulate attacks.

NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

AIM:
Study of malicious software using tools: Keylogger attack using a keylogger tool.

INTRODUCTION:

MALICIOUS SOFTWARE:
The words “Malicious Software” coin the word “Malware” and the meaning remains the same. Malicious Software refers to any malicious program that causes harm to a computer system or network. Malicious Malware Software attacks a computer or network in the form of viruses, worms, trojans, spyware, adware, or rootkits.

Their mission is often targeted at accomplishing unlawful tasks such as robbing protected data, deleting confidential documents, or adding software without the user's consent.

KEYLOGGERS:
Keyloggers are a particularly insidious type of spyware that can record and steal consecutive keystrokes (and much more) that the user enters on a device. The term keylogger, or "keystroke logger," is self-explanatory: Software that logs what you type on your keyboard. However, keyloggers can also enable cybercriminals to eavesdrop on you, watch you on your system camera, or listen over your smartphone's microphone.

How do keyloggers work?
How a keylogger works depends on its type. Hardware and software keyloggers work differently due to their medium.

Most workstation keyboards plug into the back of the computer, keeping the connections out of the user's line of sight. A hardware keylogger may also come in the form of a module that is installed inside the keyboard itself. When the user types on the keyboard, the keylogger collects each keystroke and saves it as text in its own hard drive, which may have a memory capacity up to several gigabytes. The person who installed the keylogger must later return and physically remove the device to access the gathered information. There are also wireless keylogger sniffers that can intercept and decrypt data packets transferred between a wireless keyboard and its receiver. A common software keylogger typically consists of two files that get installed in the same directory: a dynamic link library (DLL) file that does the recording and an executable file that installs the DLL file and triggers it. The keylogger program records each keystroke the user types and periodically uploads the information over the internet to whoever installed the program. Hackers can design keylogging software to use keyboard application program interfaces (APIs) for another application, malicious script injection, or memory injection.

There are two main types of software keyloggers: user-mode keyloggers and kernel-mode keyloggers.

A user-mode keylogger uses a Windows API to intercept keyboard and mouse movements. GetAsyncKeyState or GetKeyState API functions might also be captured depending on the keylogger. These keyloggers require the attacker to actively monitor each key press.

A kernel mode keylogger is a more powerful and complex software keylogging method. It works with higher privileges and can be harder to locate in a system. Kernel mode keyloggers use filter drivers that can intercept keystrokes. They can also modify the internal Windows system through the kernel.

Some keylogging programs may also include functionality to record user data besides keystrokes, such as capturing anything that has been copied to the clipboard and taking screenshots of the user's screen or a single application.

KIDLOGGER:

KidLogger – is a parental control software compatible with the most used OS in the world. Install the app “Parental Time Control” for Android, Windows, or Mac and get all information about the activity of your PC, mobile, or tablet of your kids.

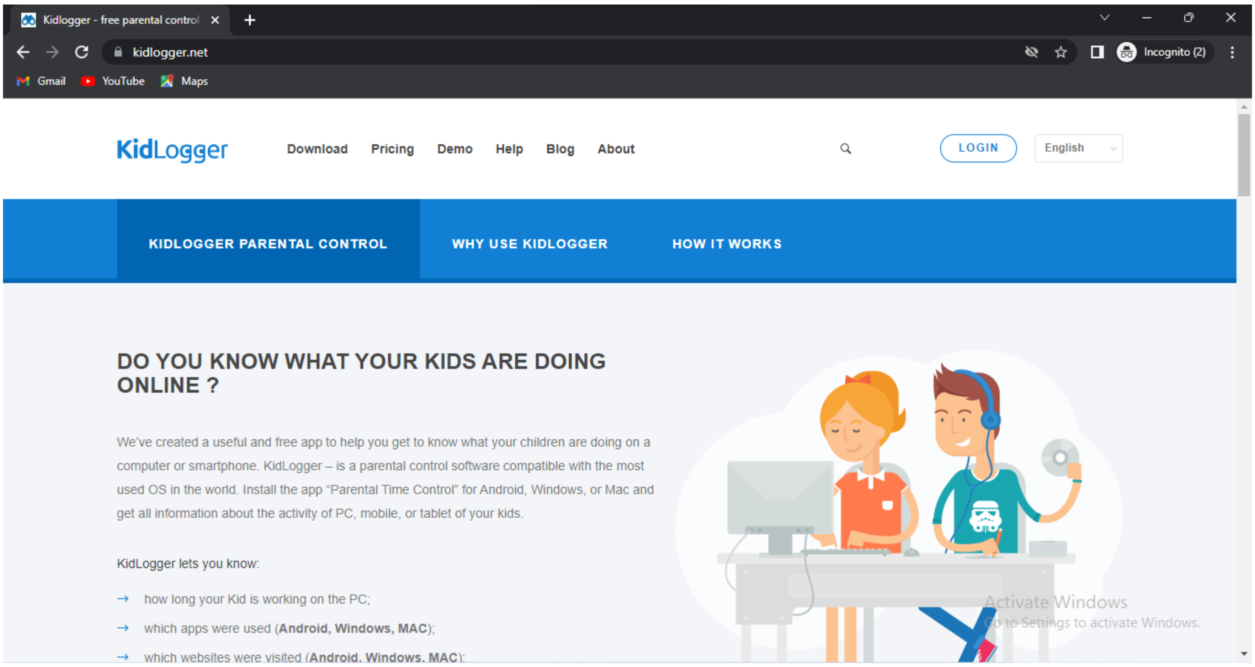
KidLogger lets you know:

- how long your Kid is working on the PC;
- which apps were used (Android, Windows, MAC);
- which websites were visited (Android, Windows, MAC);
- with whom he or she communicated (phone, SMS, Skype, Facebook) on Android phone;
- where has been (Android);
- what photos made (Android);
- and what I wrote to a friend (Android, MAC).

NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

RESULTS:

1. Install the Kidlogger tool from its official website to monitor user actions.



Kidlogger - free parental control

kidlogger.net

Gmail YouTube Maps

KidLogger Download Pricing Demo Help Blog About LOGIN English

KIDLOGGER PARENTAL CONTROL WHY USE KIDLOGGER HOW IT WORKS

DO YOU KNOW WHAT YOUR KIDS ARE DOING ONLINE ?

We've created a useful and free app to help you get to know what your children are doing on a computer or smartphone. KidLogger – is a parental control software compatible with the most used OS in the world. Install the app "Parental Time Control" for Android, Windows, or Mac and get all information about the activity of PC, mobile, or tablet of your kids.

KidLogger lets you know:

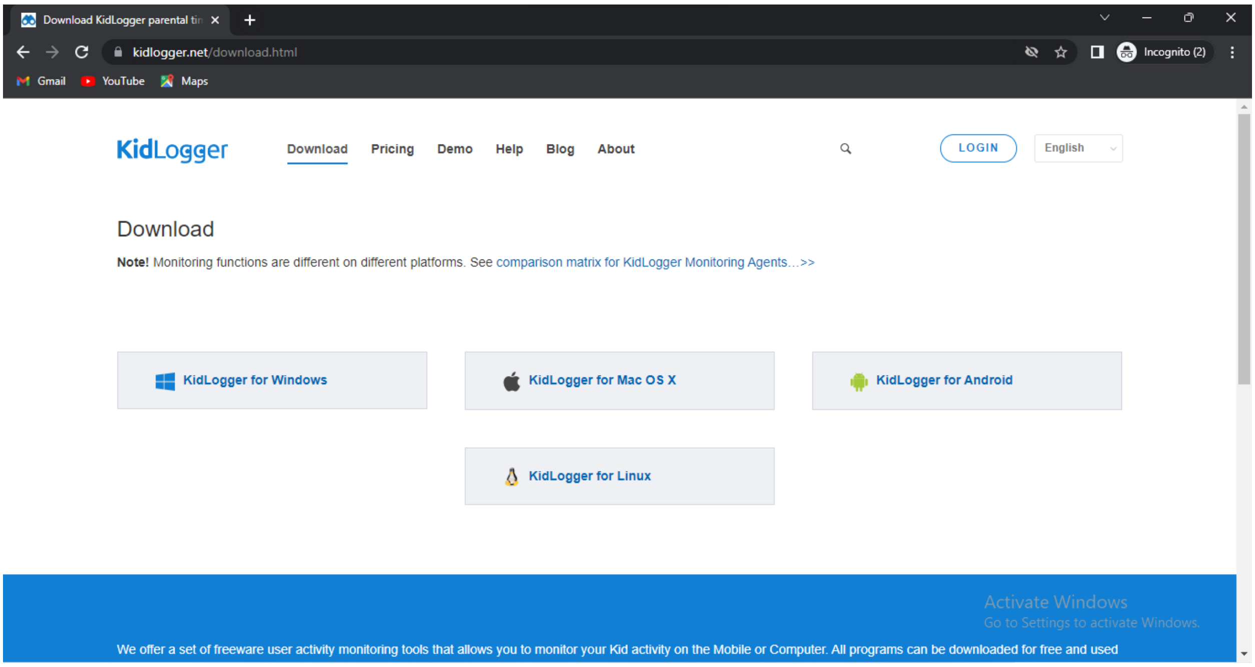
→ how long your Kid is working on the PC;

→ which apps were used (**Android, Windows, MAC**);

→ which websites were visited (**Android, Windows, MAC**);

Activate Windows
Go to Settings to activate Windows.

2. Select the download link according to the type of operating system you have.



Download KidLogger parental tir

kidlogger.net/download.html

Gmail YouTube Maps

KidLogger Download Pricing Demo Help Blog About LOGIN English

Download

Note! Monitoring functions are different on different platforms. See comparison matrix for KidLogger Monitoring Agents...>>

KidLogger for Windows

KidLogger for Mac OS X

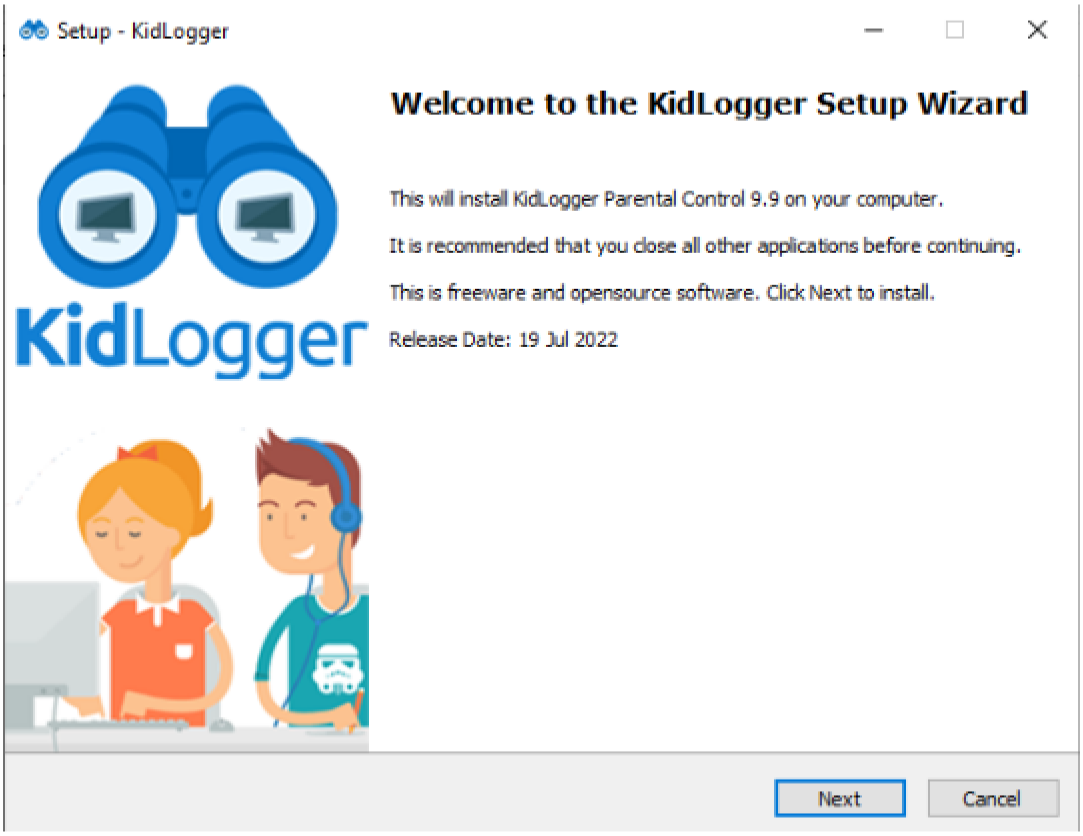
KidLogger for Android

KidLogger for Linux

We offer a set of freeware user activity monitoring tools that allows you to monitor your Kid activity on the Mobile or Computer. All programs can be downloaded for free and used

Activate Windows
Go to Settings to activate Windows.

NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52



Welcome to the KidLogger Setup Wizard

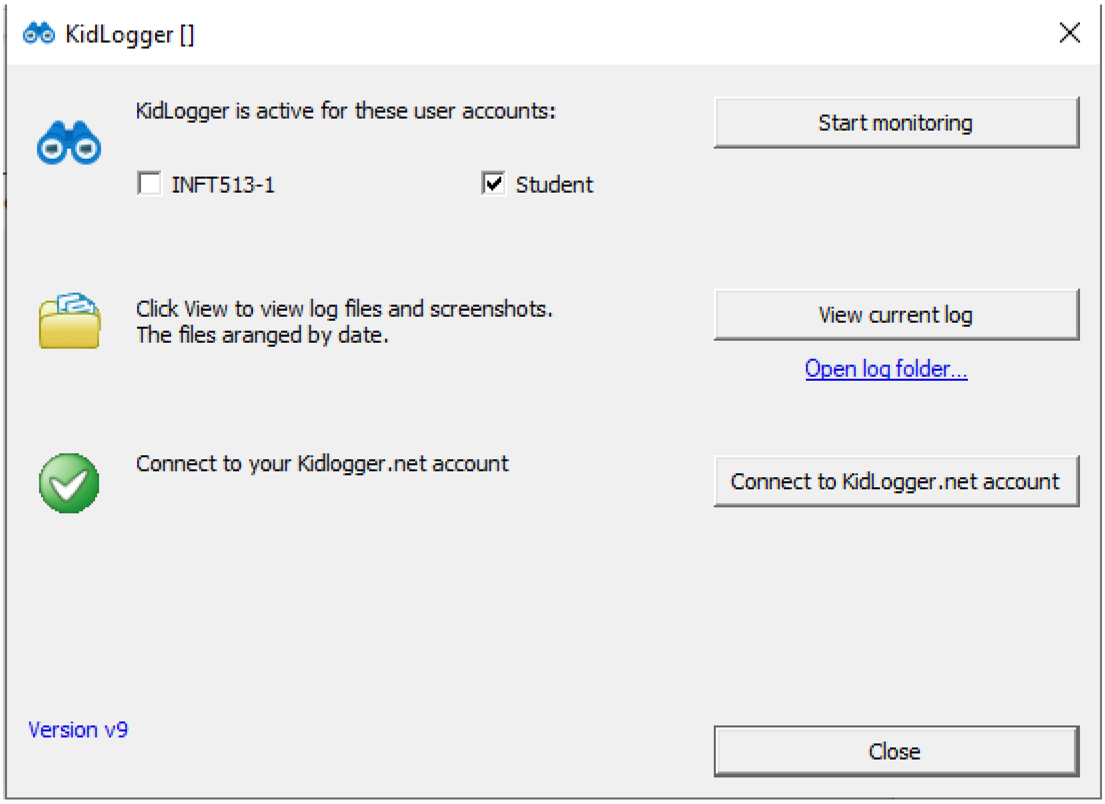
This will install KidLogger Parental Control 9.9 on your computer.

It is recommended that you close all other applications before continuing.

This is freeware and opensource software. Click Next to install.

Release Date: 19 Jul 2022

3. The following interface will be displayed once you install it in your system. It also displays various users currently active on your system.



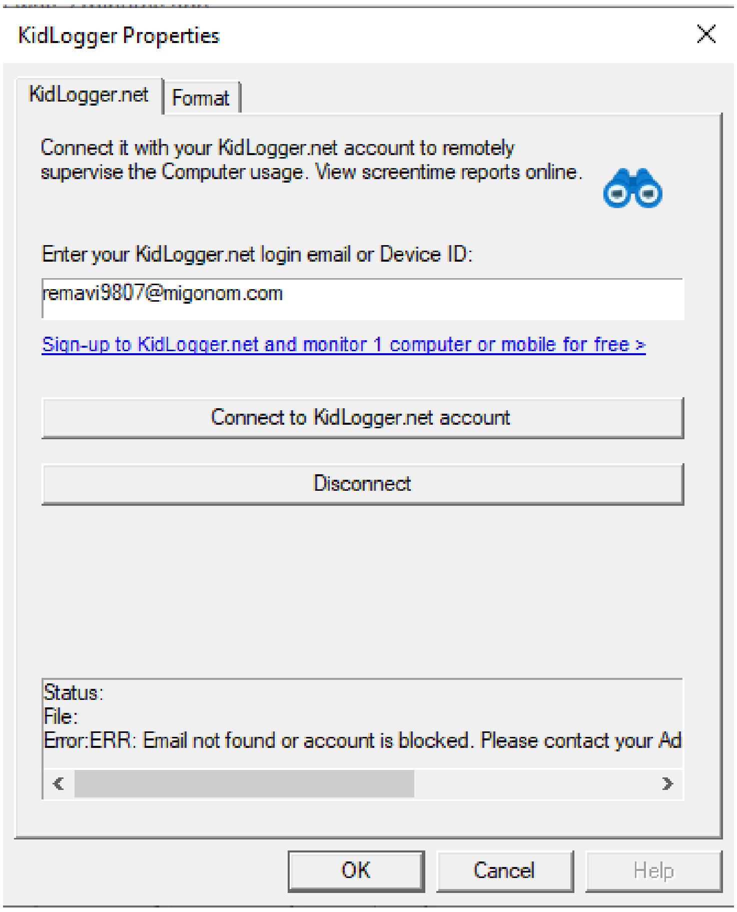
KidLogger is active for these user accounts:

☐ INFT513-1 ☑ Student

Click View to view log files and screenshots.
The files aranged by date.

Connect to your Kidlogger.net account

4. You need to login into the Kidlogger account to successfully connect your system with your account.



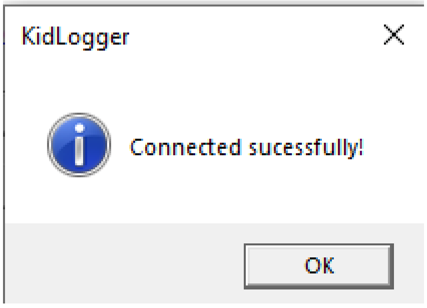
Connect it with your KidLogger.net account to remotely supervise the Computer usage. View screentime reports online.

Enter your KidLogger.net login email or Device ID:

remavi9807@migonom.com

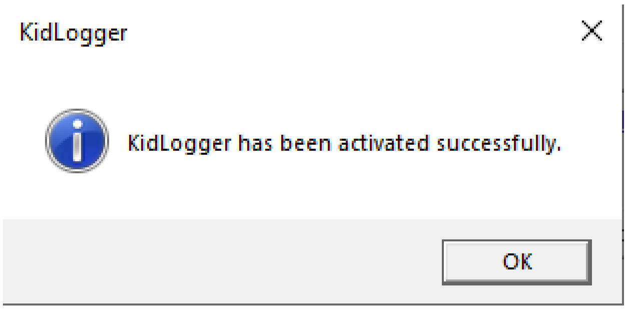
Sign-up to KidLogger.net and monitor 1 computer or mobile for free >

```
Status:
File:
Error:ERR: Email not found or account is blocked. Please contact your Ad
```



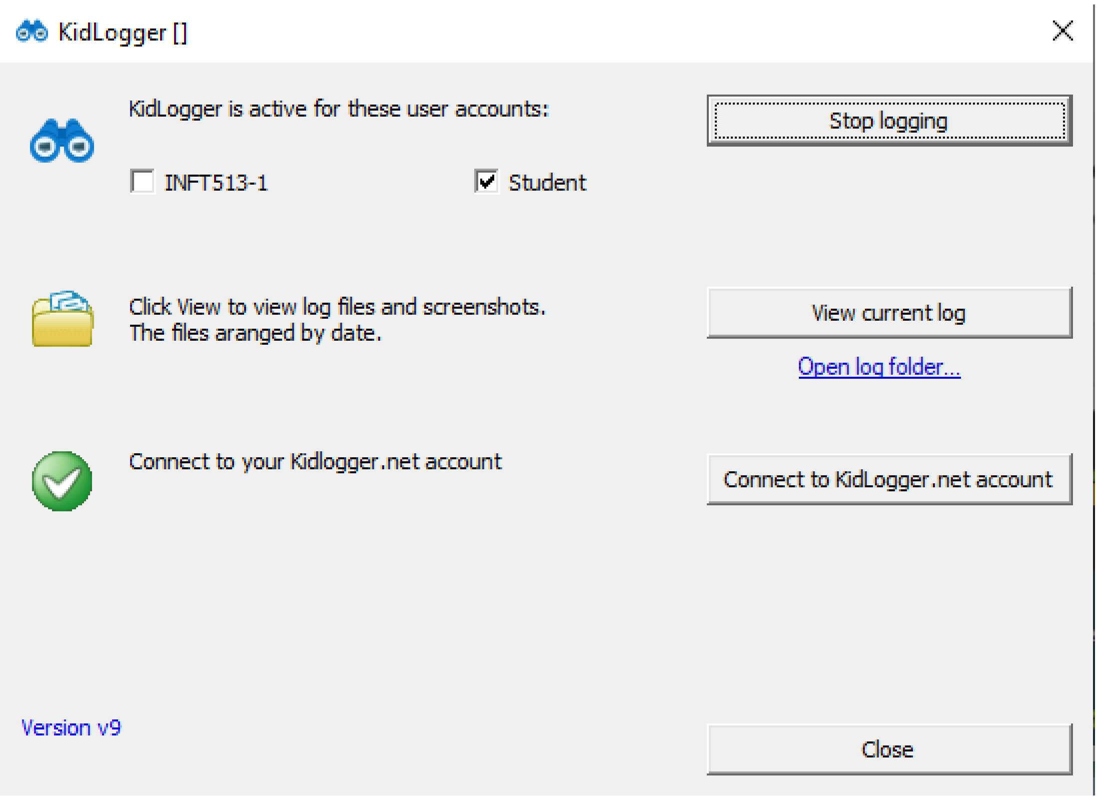
Connected sucessfully!

5. Once you configure all the changes, the following message will pop up.



KidLogger has been activated successfully.

6. Now we will start monitoring one of the users of your system.



KidLogger []

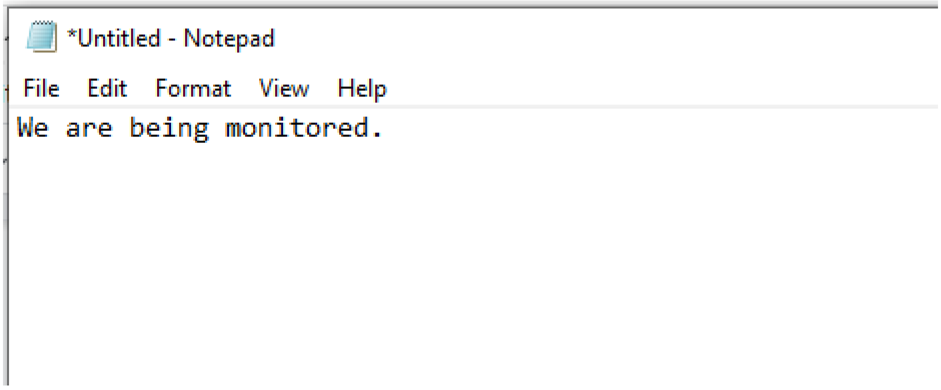
KidLogger is active for these user accounts:

□ INFT513-1 ☑ Student

Click View to view log files and screenshots.
The files arranged by date.

Connect to your Kidlogger.net account

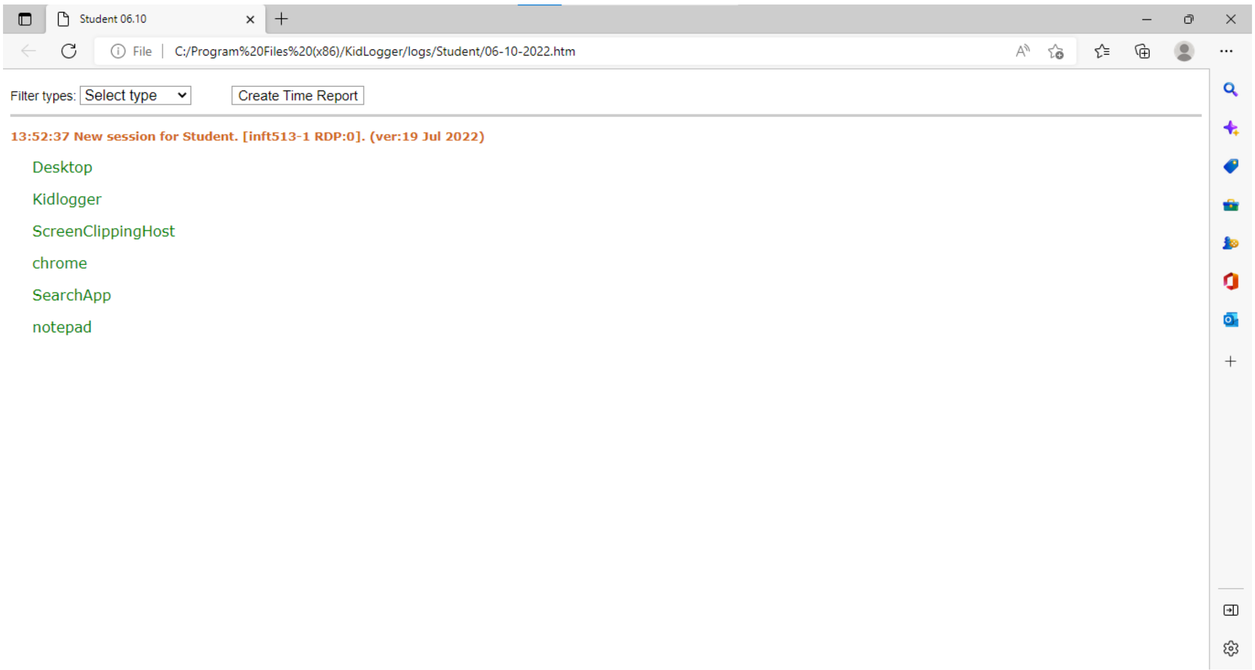
7. We will perform some actions on the system once we start monitoring to verify if our activities are tracked or not.



*Untitled - Notepad

```
We are being monitored.
```

8. Now we will check all the actions performed by us by checking the logs folder present in our user folder in kidlogger.



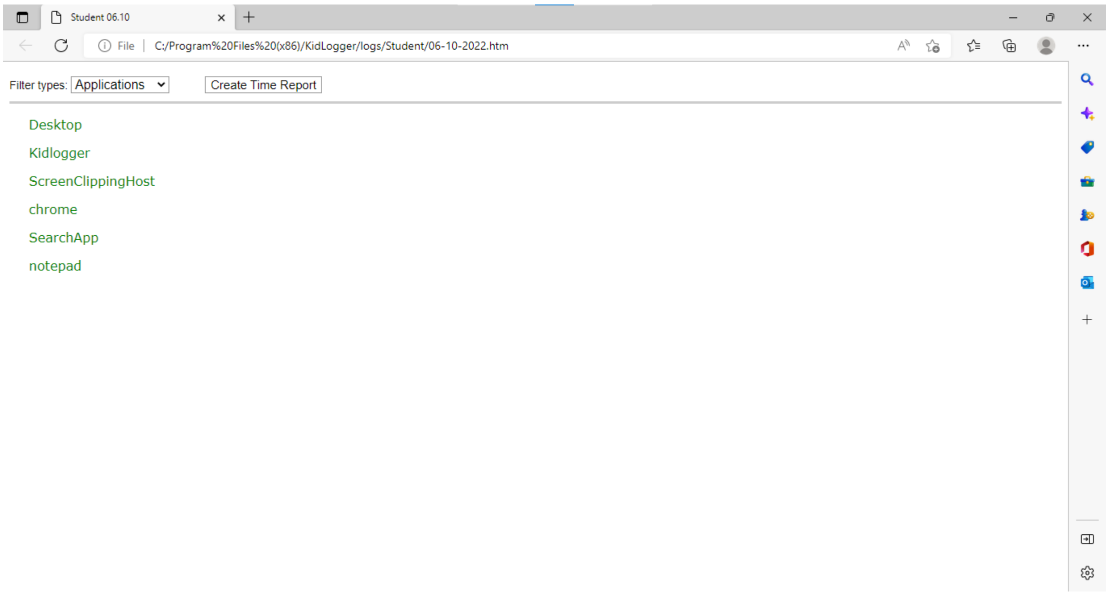
Student 06.10
File
C:/Program%20Files%20(x86)/KidLogger/logs/Student/06-10-2022.htm
Create Time Report

Filter types: Select type

13:52:37 New session for Student. [inft513-1 RDP:0]. (ver:19 Jul 2022)

Desktop
Kidlogger
ScreenClippingHost
chrome
SearchApp
notepad

9. To check specific actions we will select the Applications type in the filters.



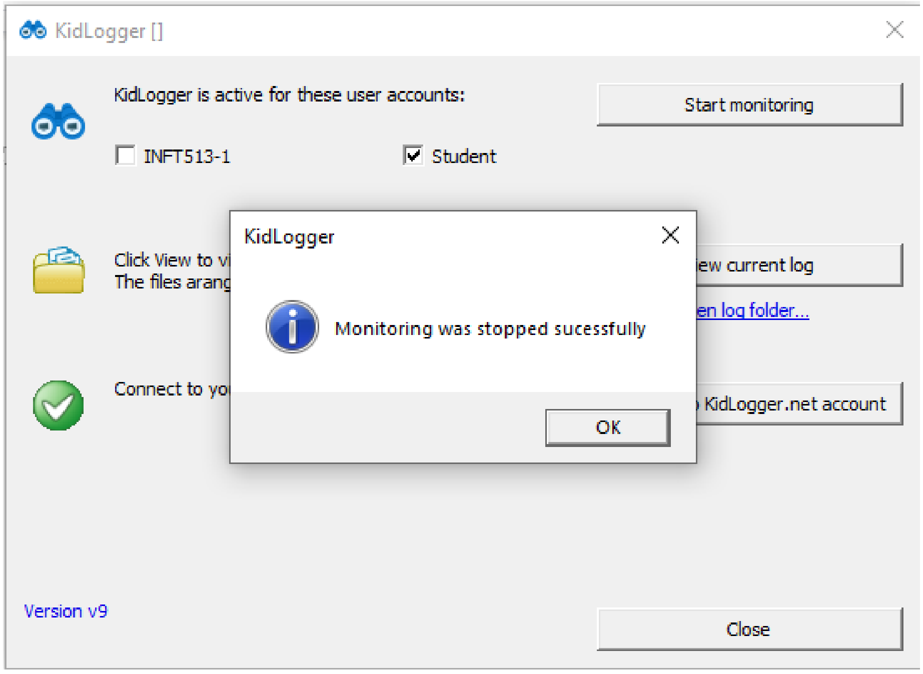
Student 06.10
File
C:/Program%20Files%20(x86)/KidLogger/logs/Student/06-10-2022.htm
Create Time Report

Filter types: Applications

Desktop
Kidlogger
ScreenClippingHost
chrome
SearchApp
notepad

NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

10. Once we verify all the actions, we will stop monitoring the user.



KidLogger is active for these user accounts:

□ INFT513-1 ☑ Student

KidLogger

Monitoring was stopped sucessfully

CONCLUSION:
Thus we have successfully understood the concept and working of keylogger using an application called kidlogger.