**OBJECT ORIENTED ANALYSIS & DESIGN (B.TECH VI SEMESTER)**



C++ PROJECT

**KEYLOGGER**



DONE BY:

**HARSH GANDHI – 2015UCP1011**

**KUSHAL KRIPLANI – 2015UCP1017**

**MANDAR WANI – 2015UCP1043**

UNDER THE GUIDANCE OF: **Dr. NAMITA MITTAL**

**CONTENTS**

1. **Introduction ………………………………………………………….....…. 2**
2. **Technical Specs …………..…………………………………….….…..… 2**
3. **How does Key-Logger get on a computer? ..........…………….…… 2**
4. **Function of a Key-Logger ...…………………………………………… 3**
5. **How to Detect a Key-Logger? ……………………………………...… 3**
6. **Unethical use of Key-Logger …………………………………………. 4**
7. **Demonstration ……………………………………………………………. 5**
8. **Bibliography …………………………………………………………….... 7**

**INTRODUCTION**

A keylogger is a software program that records the keyboard keys the user presses, typically covertly, so that the user is unaware that his actions are being monitored. The recorded data can then be retrieved by the programmer.

Keyloggers are used in IT organizations to troubleshoot technical problems with computers and business networks. Keyloggers can also be used by a family (or business) to monitor the network usage of people without their direct knowledge. Finally, malicious individuals may use keyloggers on public computers to steal passwords or credit card information.

**TECHNICAL SPECS**

Technical Specifications:

1. Programming Language : **C++** (CPP)
2. Platform : **Windows**
3. Program Type : **Stealth Mode** (Background Process)

**HOW DOES A KEYLOGGER GET ON A COMPUTER?**

Keyloggers on most computers arrive as Malware through e-mail or drive links. If your computer gets compromised, the malware may have a keylogger or a function that downloads and runs the Keylogger on the victim’s system. It could also be installed by someone who has access to your personal computer. They are a popular form of malware, which are used by criminals to steal sensitive data of the user.

This is the reason why you should always be sure of the sources you’re downloading files from.

**FUNCTION OF A KEYLOGGER**

Keyloggers often run in the background in stealth mode, hence undetectable from the user, making notes of each keystroke entered by the user. The keystrokes are saved on a text file, which can be sent to the attacker at regular intervals, thus compromising the victim’s privacy.

At times, keyloggers are combined with a screenshot program, hence someone can read through the history of what has been typed along with the screenshots, to deduce the actions performed by the user.

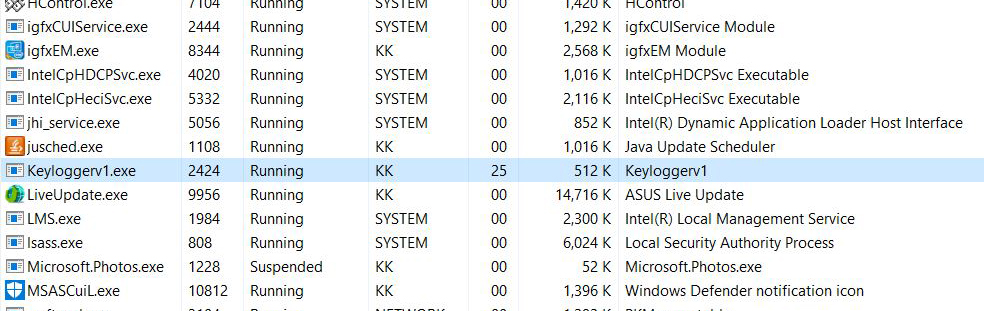
**HOW TO DETECT AND REMOVE A KEYLOGGER?**

Keylogger is essentially any type of malware. It can be avoided in the same away as that of any other malware. Prevention should be taken before downloading or running, any software from unknown sources.

The prevention methods could be as follows:

* **Detection Software** 
  + Anti-Keyloggers: A piece of software specially designed to detect keyloggers. This is done, by comparing all the files in the computer to a Database of Keyloggers.

Top anti-keyloggers include: Zemana AntiLogger, Ghostpress, etc.

* + Be careful where you go on the Internet. Files downloaded, by clicking on advertisements should be immediately deleted.
  + Anti-Virus and anti-spyware software provided by reputed brands, is the simplest way to detect a Keylogger or any other malware.
  + Consider, operating a virtual machine environment to browse the internet.
* Check **Task Manager** by pressing **CTRL+ALT+DEL** in Windows. Examine the tasks running, and if you are unfamiliar with any of them, look them up on a search engine. If they are from an unreliable source, end the task immediately.

*The above image depicts that the Keylogger is running in the background, actively recording the user’s keystrokes. Hence, to stop this we need to terminate the process.*

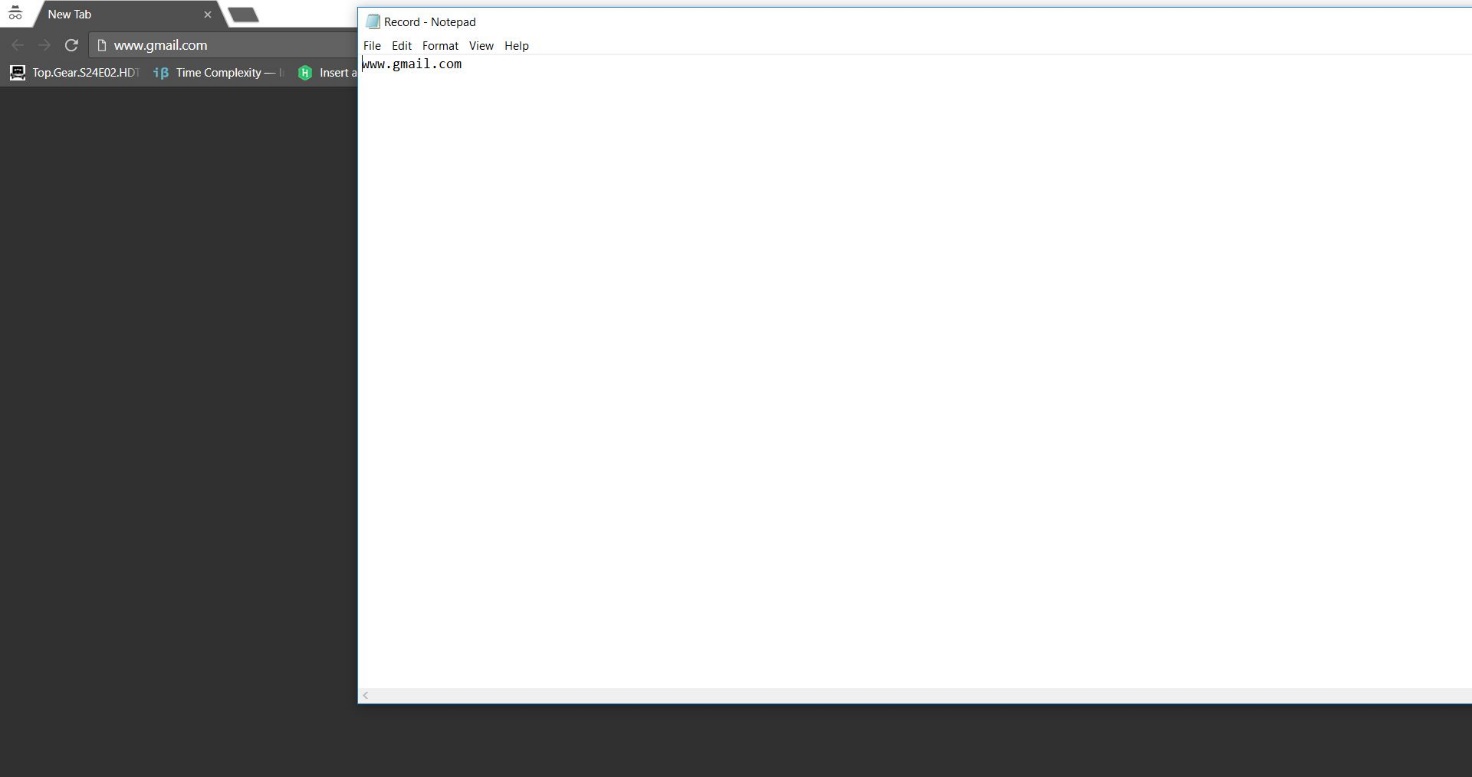
* **Scan** your hard disk for the most recent files stored. Look at the contents of any files that update often, as they might be logs. Delete such files immediately.
* Use your **system configuration utility** to view which programs are loaded at computer start-up. You can access this list by typing “msconfig” into the run box.

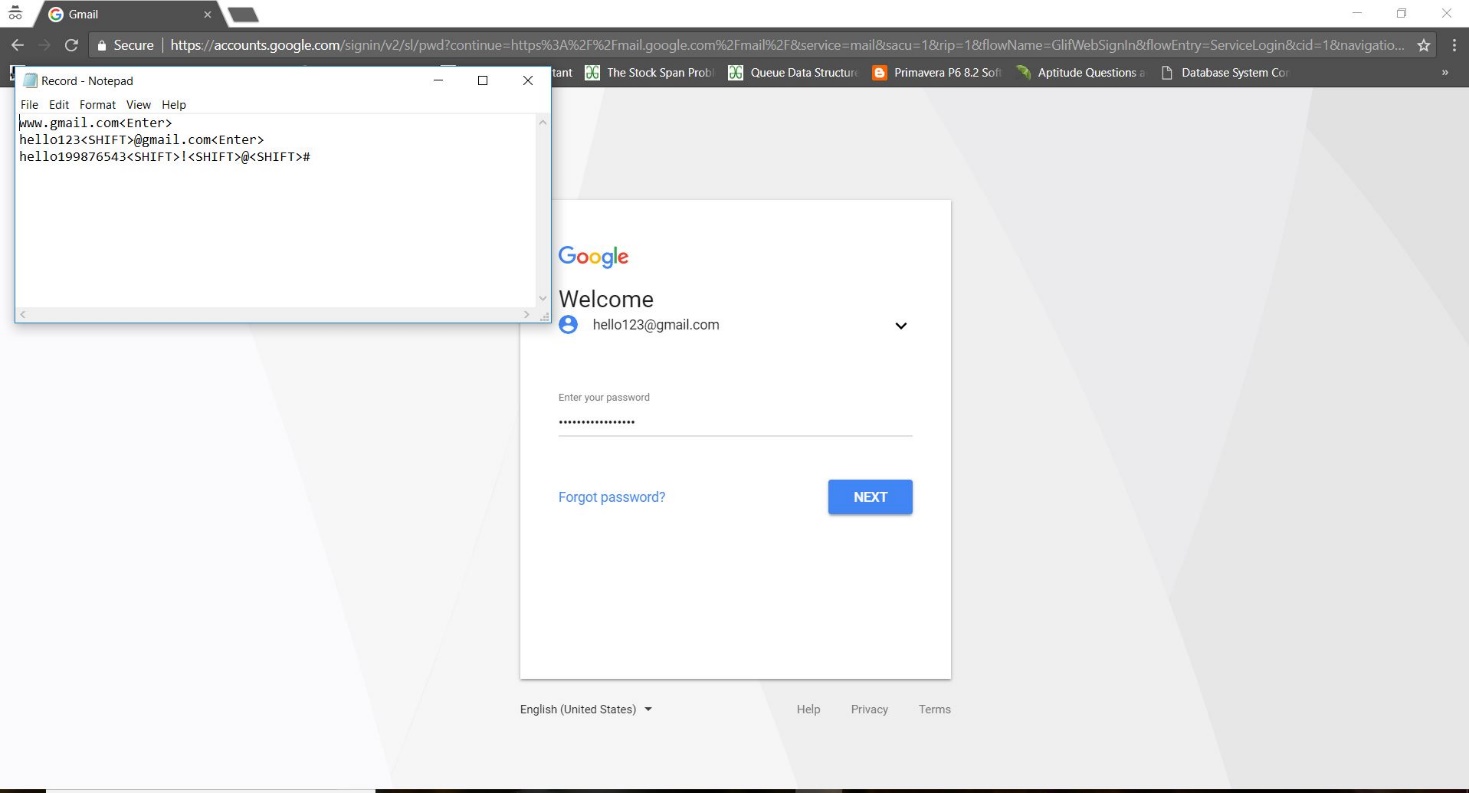
**UNETHICAL USE OF KEY-LOGGER**

Remote- access software keyloggers can allow access to locally recorded data from a remote location.

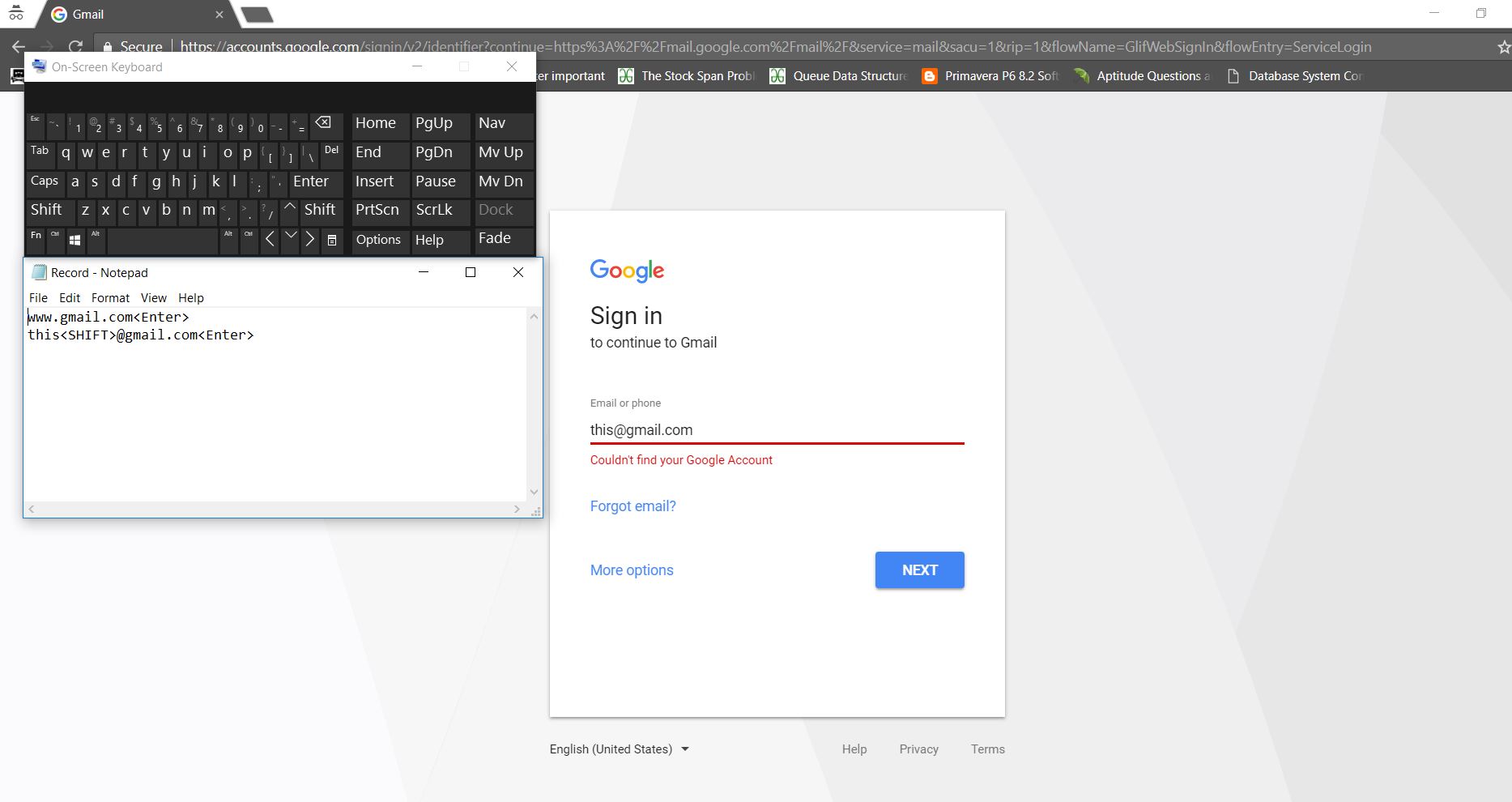
A Keylogger can be illegal if you are using it for criminal purposes such as stealing personal data and financial information. It is also illegal if you are installing as malware on the person's PC without their knowledge.

**DEMONSTRATION**

*The above figure has keylogger running in the background. It stores the typed text “www.gmail.com” in a text file named “Record.txt”.*



*The above image is a prime example of how a keylogger can be used to get passwords and other sensitive data of the user without user’s knowledge.*

*The above image depicts that the keylogger can keep track of keystrokes generated via windows virtual keyboard as well.*

**BIBLIOGRAPHY**

1. **Wikipedia**
2. **SecureList**
3. **LifeWire**
4. **Search Security/ Tech Target**
5. **Keyloggers (www.keyloggers.com)**
6. **Securing Tomorrow**
7. **Wiki How**
8. **Vera Code**