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

KEYLOGGER

C++ PROJECT

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

DONE BY:

HARSH GANDHI – 2015UCP1011
KUSHAL KRIPLANI – 2015UCP1017
MANDAR WANI – 2015UCP1043

CONTENTS

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.

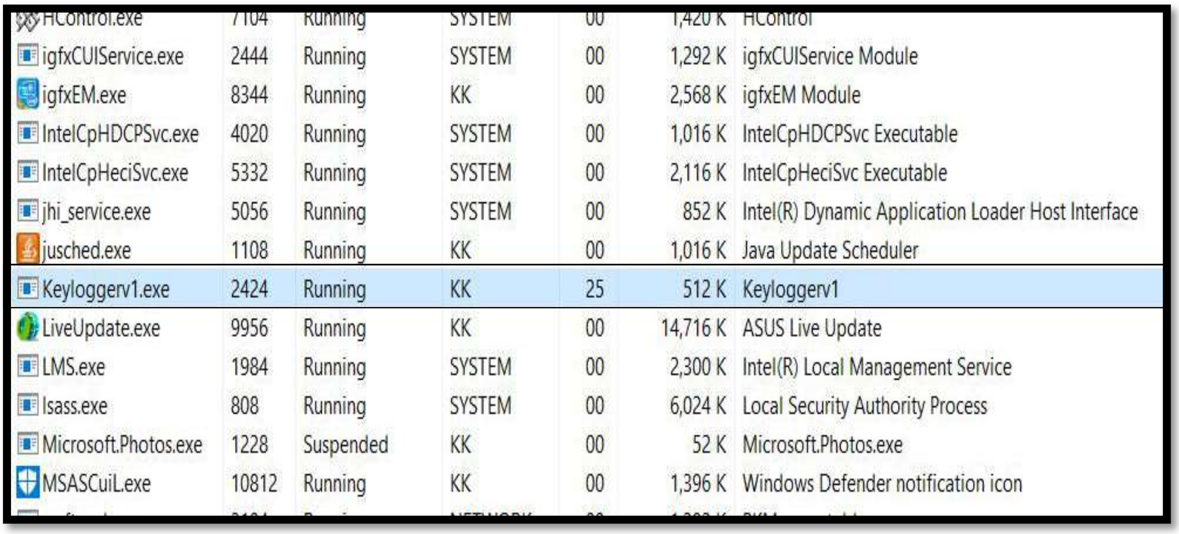
Top anti-keyloggers include: Zemana AntiLogger, Ghostpress, etc.

- 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.



HControl.exe	7104	Running	SYSTEM	00	1,420 K	HControl
igfxCUIService.exe	2444	Running	SYSTEM	00	1,292 K	igfxCUIService Module
igfxEM.exe	8344	Running	KK	00	2,568 K	igfxEM Module
IntelCpHDCPSvc.exe	4020	Running	SYSTEM	00	1,016 K	IntelCpHDCPSvc Executable
IntelCpHeciSvc.exe	5332	Running	SYSTEM	00	2,116 K	IntelCpHeciSvc Executable
jhi_service.exe	5056	Running	SYSTEM	00	852 K	Intel(R) Dynamic Application Loader Host Interface
jusched.exe	1108	Running	KK	00	1,016 K	Java Update Scheduler
Keyloggerv1.exe	2424	Running	KK	25	512 K	Keyloggerv1
LiveUpdate.exe	9956	Running	KK	00	14,716 K	ASUS Live Update
LMS.exe	1984	Running	SYSTEM	00	2,300 K	Intel(R) Local Management Service
lsass.exe	808	Running	SYSTEM	00	6,024 K	Local Security Authority Process
Microsoft.Photos.exe	1228	Suspended	KK	00	52 K	Microsoft.Photos.exe
MSASCuiL.exe	10812	Running	KK	00	1,396 K	Windows Defender notification icon

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.

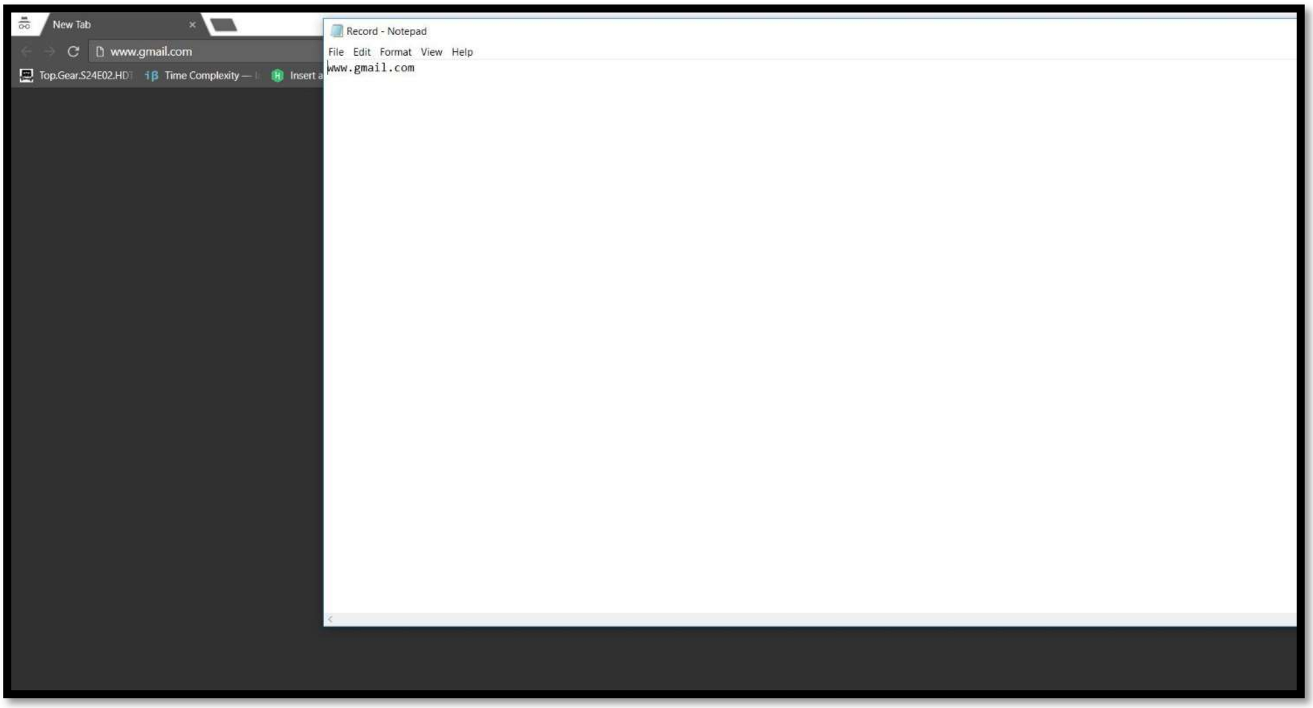
- **Scan** your hard disk for the most recent files stored. Look at the contents of any files that update often, as they might be logs. Delete such files immediately.
- Use your **system configuration utility** to view which programs are loaded at computer start-up. You can access this list by typing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

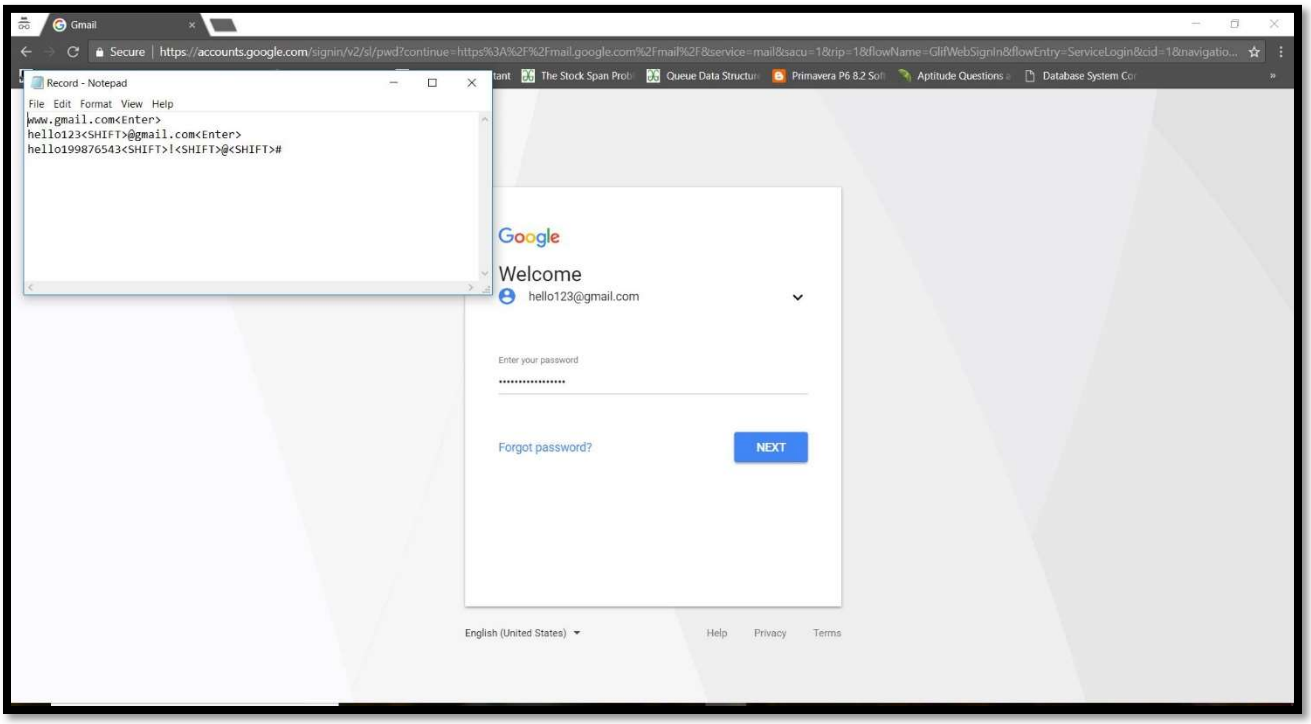
A Keylogger can be illegal if you are using it for criminal purposes such as stealing personal data and financial information. It is also illegal if you are installing as malware on the person's PC without their knowledge.

DEMONSTRATION



```
www.gmail.com
```

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


Gmail
Secure
https://accounts.google.com/signin/v2/sl/pwd?continue=https%3A%2F%2Fmail.google.com%2Fmail%2F&service=mail&sacu=1&rip=1&flowName=GlifWebSignIn&flowEntry=ServiceLogin&cid=1&navigatio...
Record - Notepad
File Edit Format View Help
Google
Forgot password?
NEXT
English (United States)
Help
Privacy
Terms

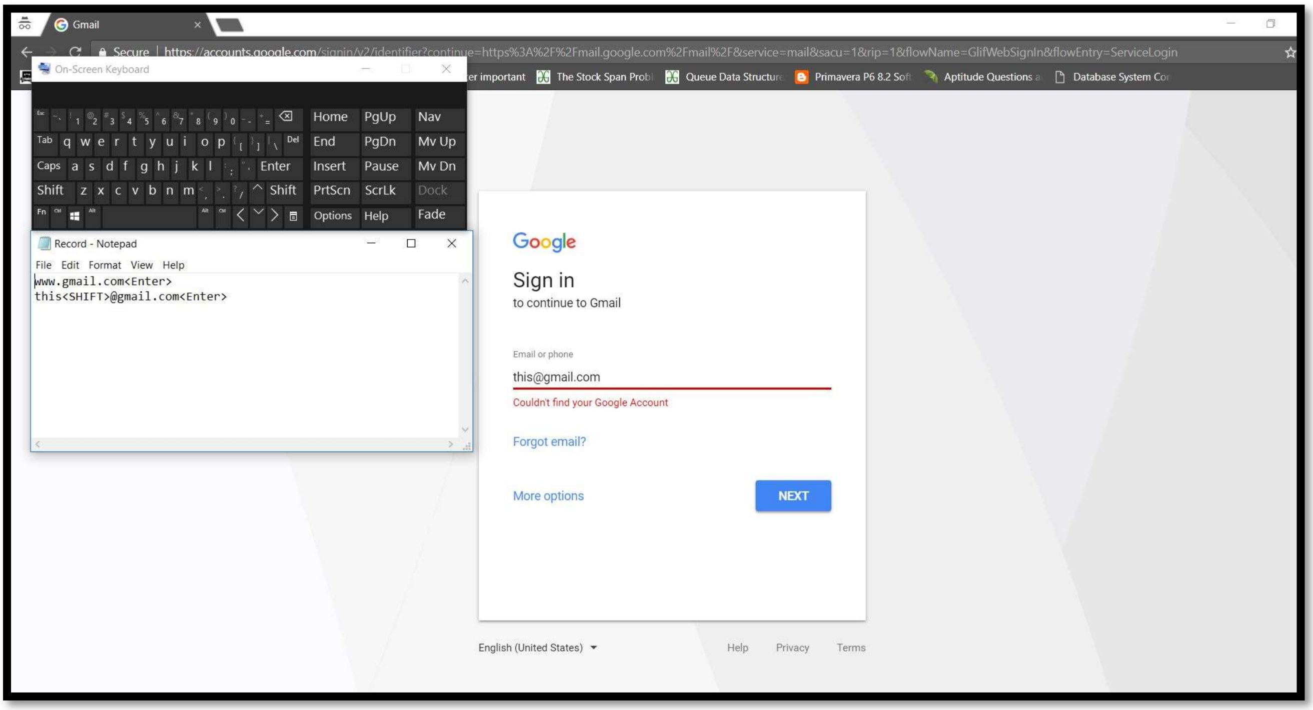
```
www.gmail.com<Enter>
hello123<SHIFT>@gmail.com<Enter>
hello199876543<SHIFT>!<SHIFT>@<SHIFT>#
```

Welcome

hello123@gmail.com

Enter your password: ••••••••••••••••

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.



Gmail
Secure
https://accounts.google.com/signin/v2/identifier?continue=https%3A%2F%2Fmail.google.com%2Fmail%2F&service=mail&sacu=1&rip=1&flowName=GlifWebSignIn&flowEntry=ServiceLogin
On-Screen Keyboard
Record - Notepad
File Edit Format View Help
Google

```
www.gmail.com<Enter>
this<SHIFT>@gmail.com<Enter>
```

Sign in

to continue to Gmail

Email or phone: this@gmail.com

Couldn't find your Google Account

Forgot email?
More options
NEXT
English (United States)
Help
Privacy
Terms

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