OOAD Project

Professor: Dr. Anil Shukla

Team 09:

Team Members:

Qazi Sajid Azam	*B16CS026*
Rahul Jindal	*B16CS027*
Saksham Gupta	*B16CS030*
Anurag Shah	*B16CS034*

KEYLOGGER

Introduction:

In its most basic definition it is something which captures the keystrokes typed on your keyboard. Typically, a software keylogger saves these keystrokes in a file (in our case the path to file is "C:\Users\USERNAME\AppData\Roaming\Microsoft\CLR") in encoded form. Keylogger then sends the file to specified email after decrypting the file. Thus, a keylogger may be used as a spyware to hack computers and steal data like username and password.

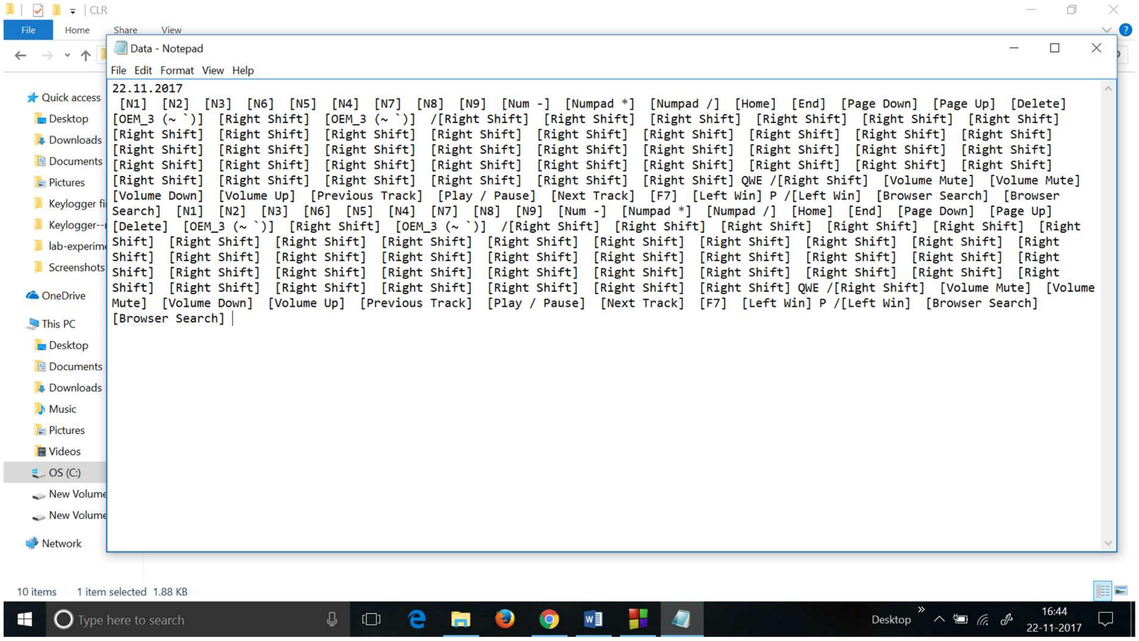
Objective

- To use features of C++ language and implement these in Keylogger.

CONTENTS

Features:

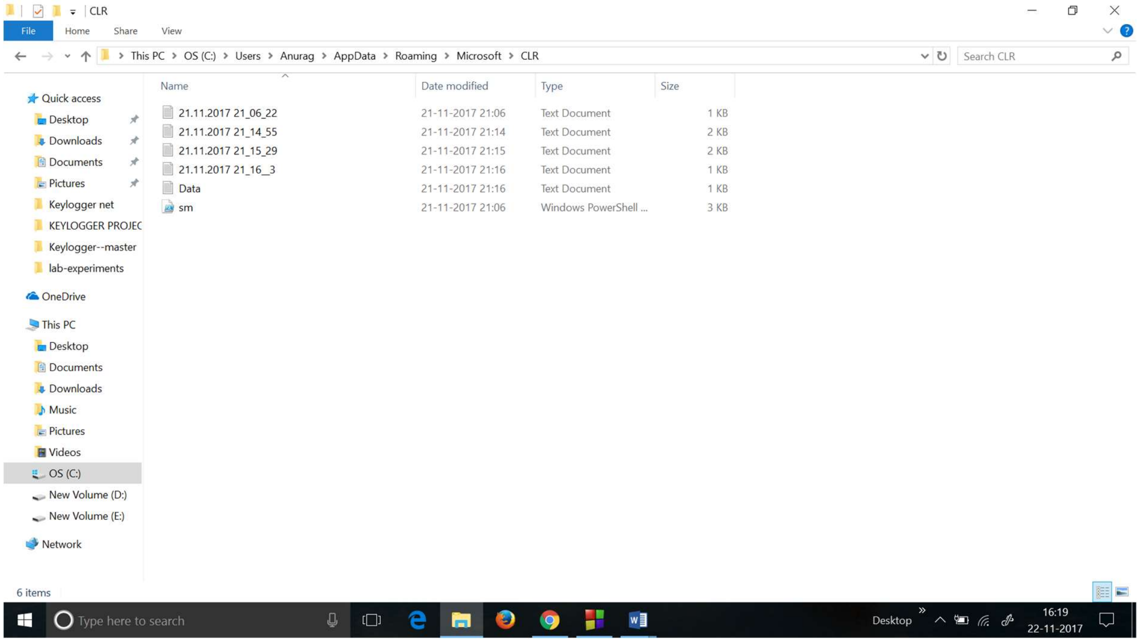
1) Detects and stores all the keystrokes and mouse clicks.



```
22.11.2017
 [N1]  [N2]  [N3]  [N6]  [N5]  [N4]  [N7]  [N8]  [N9]  [Num -]  [Numpad *]  [Numpad /]  [Home]  [End]  [Page Down]  [Page Up]  [Delete]
[OEM_3 (~ `)]  [Right Shift]  [OEM_3 (~ `)]  /[Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]
[Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]
[Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]
[Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]
[Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift] QWE /[Right Shift]  [Volume Mute]  [Volume Mute]
[Volume Down]  [Volume Up]  [Previous Track]  [Play / Pause]  [Next Track]  [F7]  [Left Win] P /[Left Win]  [Browser Search]  [Browser
Search]  [N1]  [N2]  [N3]  [N6]  [N5]  [N4]  [N7]  [N8]  [N9]  [Num -]  [Numpad *]  [Numpad /]  [Home]  [End]  [Page Down]  [Page Up]
[Delete]  [OEM_3 (~ `)]  [Right Shift]  [OEM_3 (~ `)]  /[Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right
Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right
Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right
Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right
Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift]  [Right Shift] QWE /[Right Shift]  [Volume Mute]  [Volume
Mute]  [Volume Down]  [Volume Up]  [Previous Track]  [Play / Pause]  [Next Track]  [F7]  [Left Win] P /[Left Win]  [Browser Search]
[Browser Search]
```

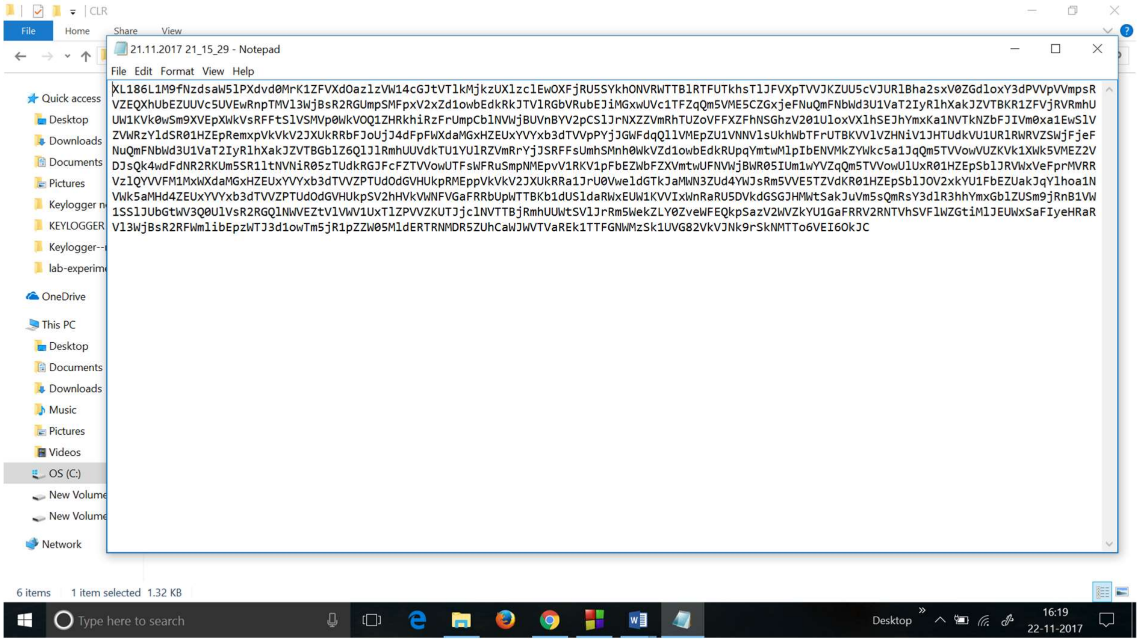
*This is a data.txt file made at same location which stores the keys as it is without encoding(Made for testing keylogger).

2) Encrypts the data and stores it in a specified file location.



This PC > OS (C:) > Users > Anurag > AppData > Roaming > Microsoft > CLR

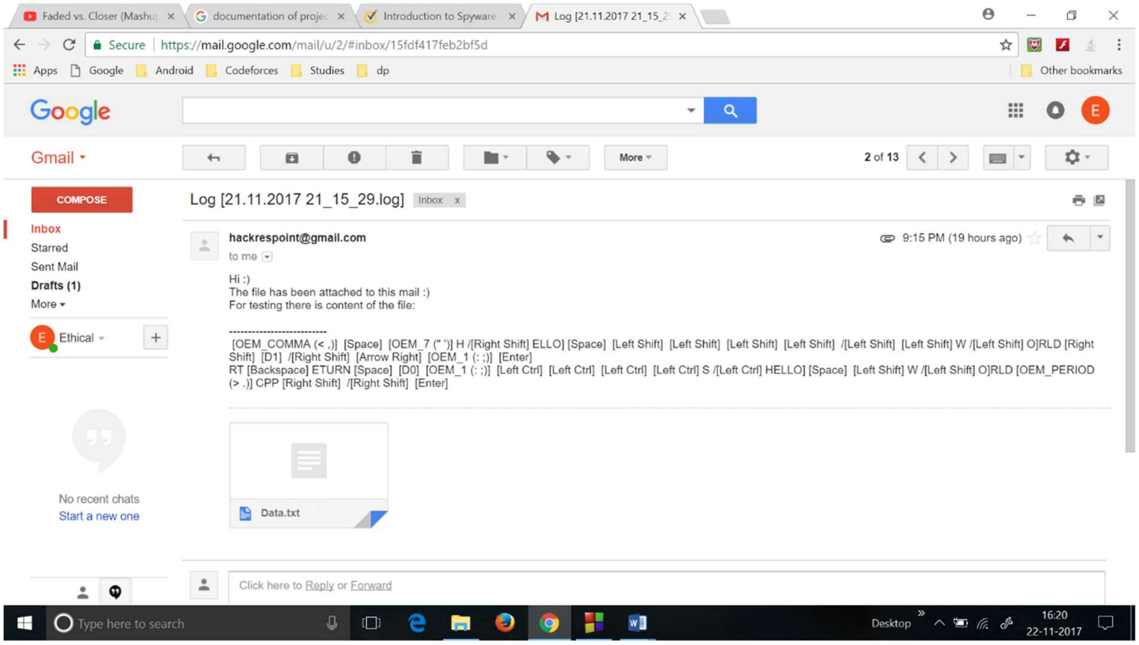
Name	Date modified	Type	Size
21.11.2017 21_06_22	21-11-2017 21:06	Text Document	1 KB
21.11.2017 21_14_55	21-11-2017 21:14	Text Document	2 KB
21.11.2017 21_15_29	21-11-2017 21:15	Text Document	2 KB
21.11.2017 21_16_3	21-11-2017 21:16	Text Document	1 KB
Data	21-11-2017 21:16	Text Document	1 KB
sm	21-11-2017 21:06	Windows PowerShell ...	3 KB



21.11.2017 21_15_29 - Notepad

XL186L1M9fNzdsaW5lPXdvd0MrK1ZFVXdOazlzVW14cGJtVTlkMjkzUXlzclEwOXFjRU5SYkhONVRWTTBlRTFUTkhsTlJFVXpTVVJKZUU5cVJURlBha2sxV0ZGdloxY3dPVVpVVmpsR
VZEQXhUbEZUUVc5UVEwRnpTMVl3WjBsR2RGUmpSMFpxV2xZd1owbEdkRkJTVlRGbVRubEJiMGxwUVc1TFZqQm5VME5CZGxjeFNuQmFNbWd3U1VaT2IyRlhXakJZVTBKR1ZFVjRVRmhU
UW1KVk0wSm9XVEpXWkVsRFFtSlVSMVp0WkVOQ1ZHRkhiRzFrUmpCblNVWjBUVnBYV2pCSlJrNXZZVmRhTUZoVFFXZFhNSGhzV201UloxVXlhSEJhYmxKa1NVTkNZbFJIVm0xa1EwSlV
ZVWRzYldSR01HZEpRemxpVkVkV2JXUkRRbFJoUjJ4dFpFWXdaMGxHZEUxYVYxb3dTVVpPYjJGWFdqQllVMEpZU1VNNVlsUkhWbTFrUTBKVVlVZHNiV1JHTUdkVU1URlRWRVZSWjFjeF
NuQmFNbWd3U1VaT2IyRlhXakJZVTBGblZ6QlJlRmhUUVdkTU1YUlRZVmRrYjJSRFFsUmhSMnh0WkVZd1owbEdkRUpqYmtwMlpIbENVMkZYWkc5a1JqQm5TVVowVUZKVk1XWk5VMEZ2V
DJsQk4wdFdNR2RKUm5SR1ltNVNiR05zTUdkRGJFcFZTVVowUTFsWFRuSmpNMEpvV1RKV1pFbEZWbFZXVmtwUFNVWjBWR05IUm1wYVZqQm5TVVowUlUxR01HZEpSblJRVWxVeFprMVRR
VzlQYVVFM1MxWXdaMGxHZEUxYVYxb3dTVVZPTUdOdGVHUkpRMEppVkVkV2JXUkRRa1JrU0VweldGTkJaMWN3ZUd4YWJsRm5VVE5TZVdKR01HZEpSblJOV2xkYU1FbEZUakJqYlhoa1N
VWk5aMHd4ZEUxYVYxb3dTVVZPTUdOdGVHUkpTV2hHVkVWNFVGaFRRbUpWTTBKb1dUSldaRWxFUW1KVVIxWnRaRU5DVkdGSGJHMWtSakJuVm5sQmRsY3dlR3hhYmxGblZUSm9jRnB1VW
1SSlJUbGtWV3Q0UlVsR2RGQlNWVEZtVlVWV1UxTlZPVVZKUTJjclNVTTBjRmhUUWtSVlJrRm5WekZLY0ZveWFEQkpSazV2WVZkYU1GaFRRV2RNVFhSSVFlWZGtiMlJEUWxSaFIyeHRaR
Vl3WjBsR2RFWmlibEpzWTJ3d1owTm5jR1pZZW05MldERTRNMDR5ZUhCaWJWVTVaREk1TTFGNWMzSk1UVG82VkVJNk9rSkNMTTo6VEI6OkJC

3) Waits for network connection and sends the mail containing the decrypted text of the keystrokes made by the user and also sends an attachment containing the decrypted data.



Log [21.11.2017 21_15_29.log]

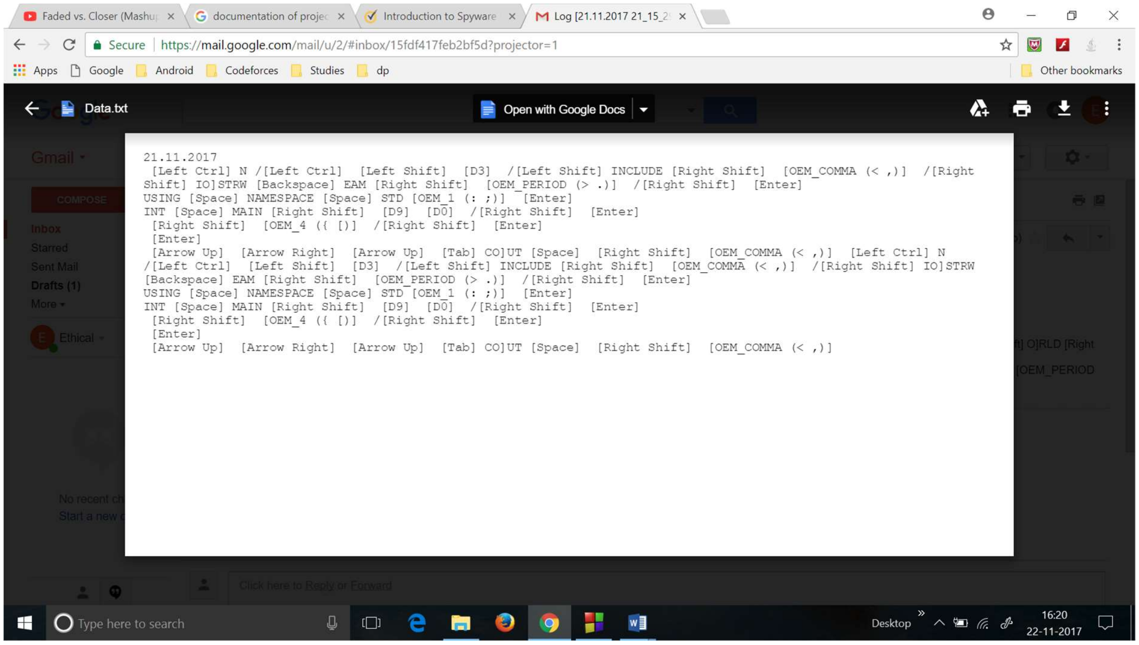
hackrespoint@gmail.com

to me

9:15 PM (19 hours ago)

```
Hi :)
The file has been attached to this mail :)
For testing there is content of the file:

---------------------------
 [OEM_COMMA (< ,)]  [Space]  [OEM_7 (" ')] H /[Right Shift] ELLO] [Space]  [Left Shift]  [Left Shift]  [Left Shift]  [Left Shift]  /[Left Shift]  [Left Shift] W /[Left Shift] O]RLD [Right Shift]  [D1]  /[Right Shift]  [Arrow Right]  [OEM_1 (: ;)]  [Enter]
RT [Backspace] ETURN [Space]  [D0]  [OEM_1 (: ;)]  [Left Ctrl]  [Left Ctrl]  [Left Ctrl]  [Left Ctrl] S /[Left Ctrl] HELLO] [Space]  [Left Shift] W /[Left Shift] O]RLD [OEM_PERIOD (> .)] CPP [Right Shift]  /[Right Shift]  [Enter]
```

Data.txt

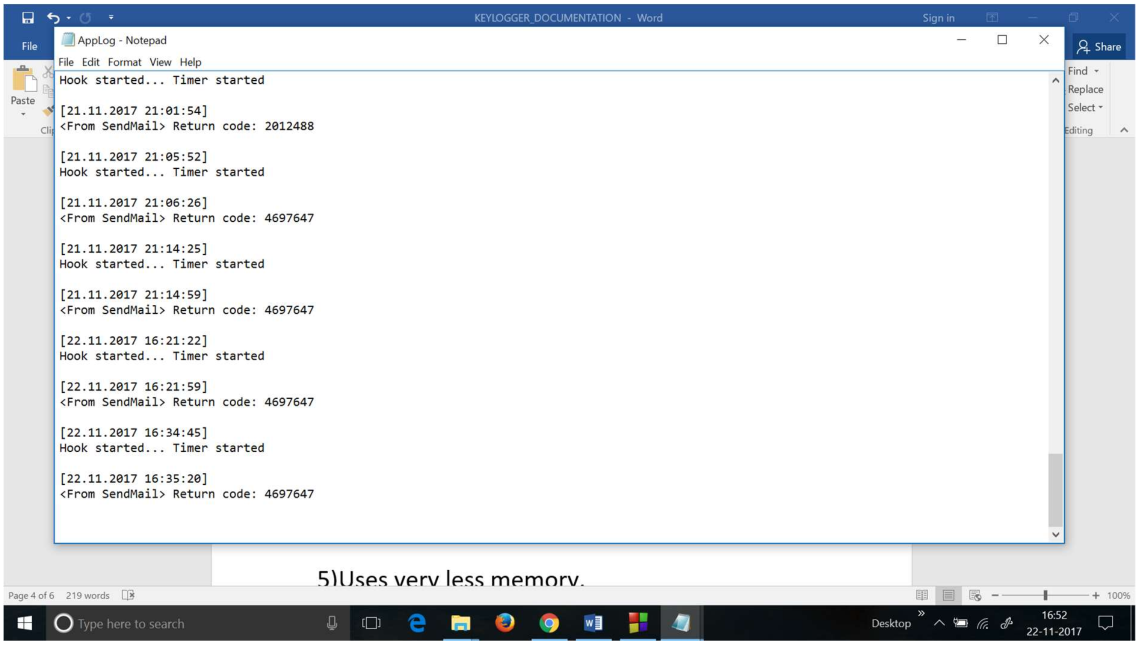


Data.txt

```
21.11.2017
 [Left Ctrl] N /[Left Ctrl]  [Left Shift]  [D3]  /[Left Shift] INCLUDE [Right Shift]  [OEM_COMMA (< ,)]  /[Right
Shift] IO]STRW [Backspace] EAM [Right Shift]  [OEM_PERIOD (> .)]  /[Right Shift]  [Enter]
USING [Space] NAMESPACE [Space] STD [OEM_1 (: ;)]  [Enter]
INT [Space] MAIN [Right Shift]  [D9]  [D0]  /[Right Shift]  [Enter]
 [Right Shift]  [OEM_4 ({ [)]  /[Right Shift]  [Enter]
 [Enter]
 [Arrow Up]  [Arrow Right]  [Arrow Up]  [Tab] CO]UT [Space]  [Right Shift]  [OEM_COMMA (< ,)]  [Left Ctrl] N
/[Left Ctrl]  [Left Shift]  [D3]  /[Left Shift] INCLUDE [Right Shift]  [OEM_COMMA (< ,)]  /[Right Shift] IO]STRW
[Backspace] EAM [Right Shift]  [OEM_PERIOD (> .)]  /[Right Shift]  [Enter]
USING [Space] NAMESPACE [Space] STD [OEM_1 (: ;)]  [Enter]
INT [Space] MAIN [Right Shift]  [D9]  [D0]  /[Right Shift]  [Enter]
 [Right Shift]  [OEM_4 ({ [)]  /[Right Shift]  [Enter]
 [Enter]
 [Arrow Up]  [Arrow Right]  [Arrow Up]  [Tab] CO]UT [Space]  [Right Shift]  [OEM_COMMA (< ,)]
```

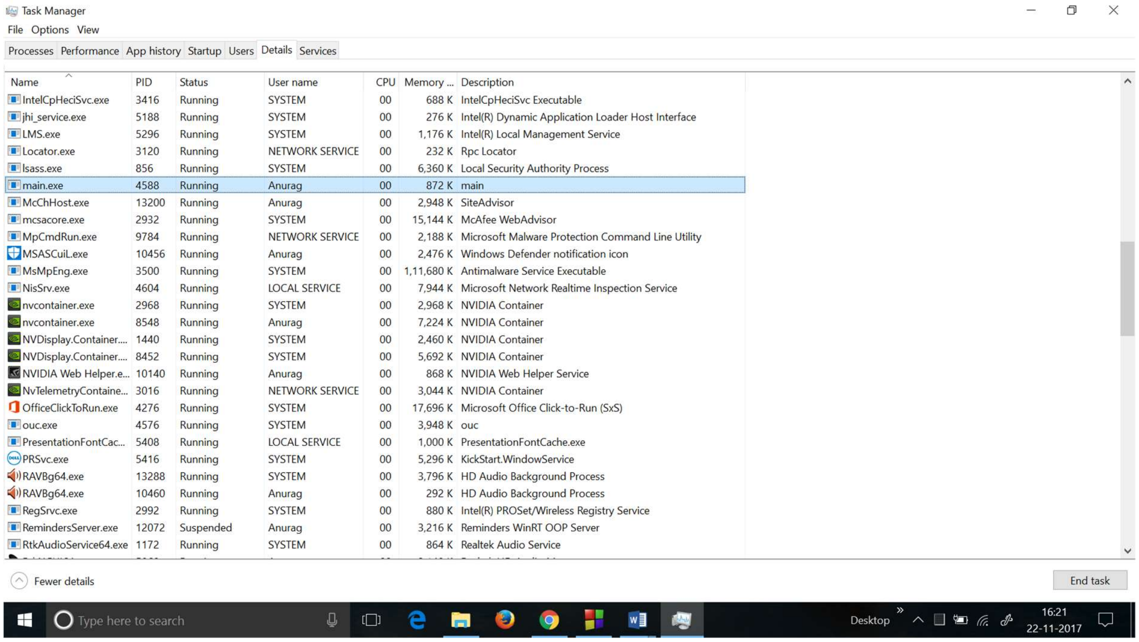
*This is the attachment which was sent in the mail.

4) Creates a Log file(AppLog) which is used for debugging. All the errors as well as events are appended in this file.



```
Hook started... Timer started

[21.11.2017 21:01:54]
<From SendMail> Return code: 2012488

[21.11.2017 21:05:52]
Hook started... Timer started

[21.11.2017 21:06:26]
<From SendMail> Return code: 4697647

[21.11.2017 21:14:25]
Hook started... Timer started

[21.11.2017 21:14:59]
<From SendMail> Return code: 4697647

[22.11.2017 16:21:22]
Hook started... Timer started

[22.11.2017 16:21:59]
<From SendMail> Return code: 4697647

[22.11.2017 16:34:45]
Hook started... Timer started

[22.11.2017 16:35:20]
<From SendMail> Return code: 4697647
```

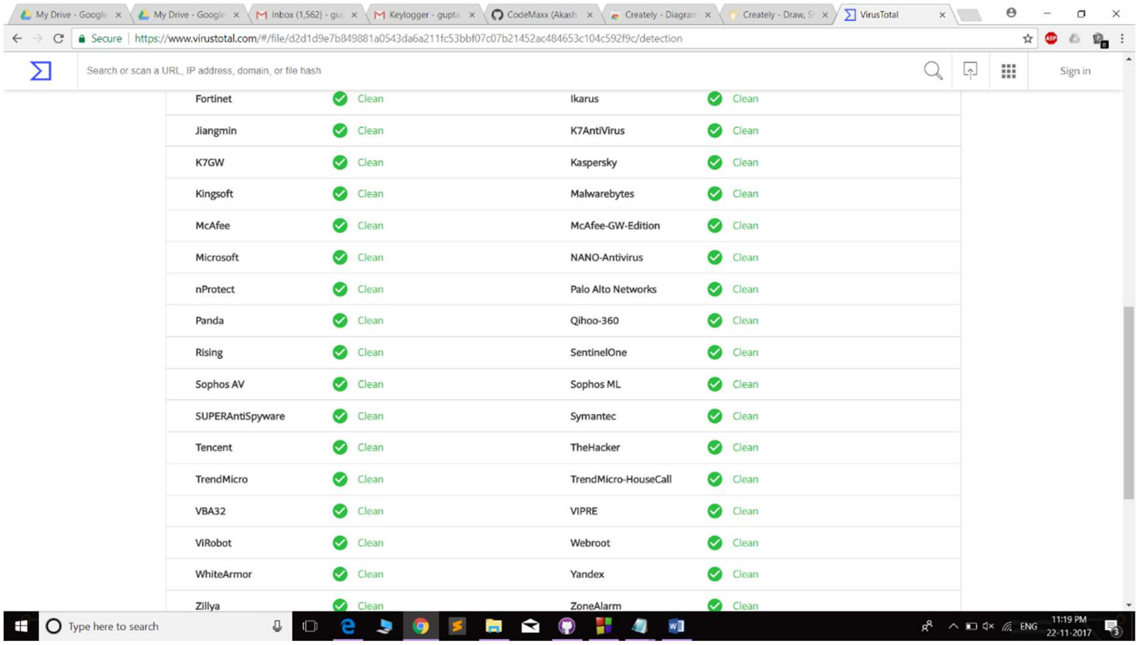
5) Uses very less memory.



Name	PID	Status	User name	CPU	Memory ...	Description
IntelCpHeciSvc.exe	3416	Running	SYSTEM	00	688 K	IntelCpHeciSvc Executable
jhi_service.exe	5188	Running	SYSTEM	00	276 K	Intel(R) Dynamic Application Loader Host Interface
LMS.exe	5296	Running	SYSTEM	00	1,176 K	Intel(R) Local Management Service
Locator.exe	3120	Running	NETWORK SERVICE	00	232 K	Rpc Locator
lsass.exe	856	Running	SYSTEM	00	6,360 K	Local Security Authority Process
main.exe	4588	Running	Anurag	00	872 K	main
McChHost.exe	13200	Running	Anurag	00	2,948 K	SiteAdvisor
mcsacore.exe	2932	Running	SYSTEM	00	15,144 K	McAfee WebAdvisor
MpCmdRun.exe	9784	Running	NETWORK SERVICE	00	2,188 K	Microsoft Malware Protection Command Line Utility
MSASCuiL.exe	10456	Running	Anurag	00	2,476 K	Windows Defender notification icon
MsMpEng.exe	3500	Running	SYSTEM	00	1,11,680 K	Antimalware Service Executable
NisSrv.exe	4604	Running	LOCAL SERVICE	00	7,944 K	Microsoft Network Realtime Inspection Service
nvcontainer.exe	2968	Running	SYSTEM	00	2,968 K	NVIDIA Container
nvcontainer.exe	8548	Running	Anurag	00	7,224 K	NVIDIA Container
NVDisplay.Container....	1440	Running	SYSTEM	00	2,460 K	NVIDIA Container
NVDisplay.Container....	8452	Running	SYSTEM	00	5,692 K	NVIDIA Container
NVIDIA Web Helper.e...	10140	Running	Anurag	00	868 K	NVIDIA Web Helper Service
NvTelemetryContaine...	3016	Running	NETWORK SERVICE	00	3,044 K	NVIDIA Container
OfficeClickToRun.exe	4276	Running	SYSTEM	00	17,696 K	Microsoft Office Click-to-Run (SxS)
ouc.exe	4576	Running	SYSTEM	00	3,948 K	ouc
PresentationFontCac...	5408	Running	LOCAL SERVICE	00	1,000 K	PresentationFontCache.exe
PRSvc.exe	5416	Running	SYSTEM	00	5,296 K	KickStart.WindowService
RAVBg64.exe	13288	Running	SYSTEM	00	3,796 K	HD Audio Background Process
RAVBg64.exe	10460	Running	Anurag	00	292 K	HD Audio Background Process
RegSrvc.exe	2992	Running	SYSTEM	00	880 K	Intel(R) PROSet/Wireless Registry Service
RemindersServer.exe	12072	Suspended	Anurag	00	3,216 K	Reminders WinRT OOP Server
RtkAudioService64.exe	1172	Running	SYSTEM	00	864 K	Realtek Audio Service

*The name of program is main.exe which is using just 872KB of space.

6) It is completely undetectable by most of the Antiviruses.



Fortinet	✓ Clean	Ikarus	✓ Clean
Jiangmin	✓ Clean	K7AntiVirus	✓ Clean
K7GW	✓ Clean	Kaspersky	✓ Clean
Kingsoft	✓ Clean	Malwarebytes	✓ Clean
McAfee	✓ Clean	McAfee-GW-Edition	✓ Clean
Microsoft	✓ Clean	NANO-Antivirus	✓ Clean
nProtect	✓ Clean	Palo Alto Networks	✓ Clean
Panda	✓ Clean	Qihoo-360	✓ Clean
Rising	✓ Clean	SentinelOne	✓ Clean
Sophos AV	✓ Clean	Sophos ML	✓ Clean
SUPERAntiSpyware	✓ Clean	Symantec	✓ Clean
Tencent	✓ Clean	TheHacker	✓ Clean
TrendMicro	✓ Clean	TrendMicro-HouseCall	✓ Clean
VBA32	✓ Clean	VIPRE	✓ Clean
ViRobot	✓ Clean	Webroot	✓ Clean
WhiteArmor	✓ Clean	Yandex	✓ Clean
Zillya	✓ Clean	ZoneAlarm	✓ Clean

Implementation:

Keylogger has been implemented using C++11 language and Windows API.

We have created seven header files under this project which are as follows:

1) IO.H
2) Timer.h
3) Base64.h
4) Helper.h
5) KeyConstants.h
6) SendMail.h
7) KeybHook.h

The short description of each header file is given below.

1) **IO.h**

This header file is used to make the files/directories required to store the data.

It includes 4 functions in a namespace named IO:-

i) GetOurPath

Used to get the path where the file will be stored.

ii) MkOneDr

Makes one Directory at the path provided to it.

iii) MkDir

It is used to check and create if necessary all the folders in the intermediate path to make sure that the files are stored properly.

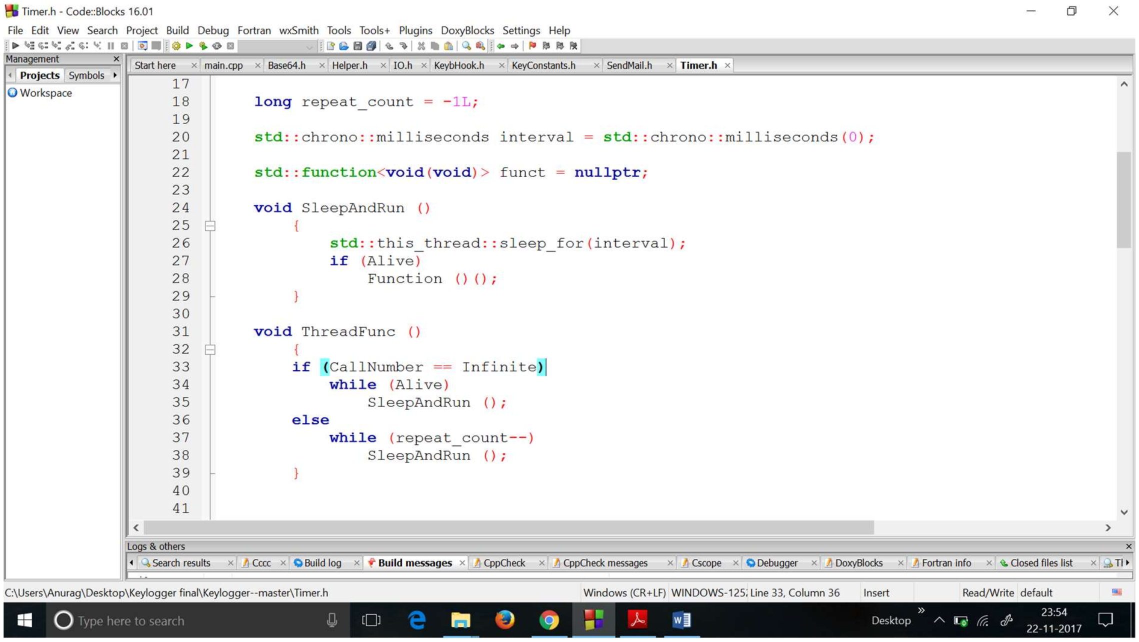
iv) WriteLog

Writes the data in encrypted form to the file.

2) **Timer.h**

It runs a function in a thread for a specified number of times with specified interval between respective executions.

The most important functions of Timer class, namely ThreadFunc() and SleepAndRun() is as shown below.


Timer.h - Code::Blocks 16.01
File Edit View Search Project Build Debug Fortran wxSmith Tools Tools+ Plugins DoxyBlocks Settings Help
Management
Projects Symbols
Workspace
Start here main.cpp Base64.h Helper.h IO.h KeybHook.h KeyConstants.h SendMail.h Timer.h
Logs & others
Search results Cccc Build log Build messages CppCheck CppCheck messages Cscope Debugger DoxyBlocks Fortran info Closed files list
Type here to search
Desktop
23:54
22-11-2017

```
long repeat_count = -1L;

std::chrono::milliseconds interval = std::chrono::milliseconds(0);

std::function<void(void)> funct = nullptr;

void SleepAndRun ()
    {
        std::this_thread::sleep_for(interval);
        if (Alive)
            Function ()();
    }

void ThreadFunc ()
    {
    if (CallNumber == Infinite)
        while (Alive)
            SleepAndRun ();
    else
        while (repeat_count--)
            SleepAndRun ();
    }
```

C:\Users\Anurag\Desktop\Keylogger final\Keylogger--master\Timer.h Windows (CR+LF) WINDOWS-125; Line 33, Column 36 Insert Read/Write default

3) Base64.h

i) base64_encode()

This function is used to encode the data in 64-bit encryption.

ii) base64_decode()

This function is used to decode the encrypted data. The screenshot of the encrypted file is attached above in Features.

4) Helper.h

This header file contains all the secondary/Helping functions required for execution of program under the Helper namespace.

This file includes:

i) DateTime struct

This is used to get the present date and time.

ii) WriteAppLog(/*parameters*/)

This is used to write to log file the message received for debugging.

iii) ToString()

This function is used to convert everything sent to it in string.

5) KeyConstants.h

This file contains the information about every key i.e. it’s key value, virtual key name and User-friendly name.

6) SendMail.h

This header file is used to send the mail to user using Windows PowerShell feature.

The main function used is SendMail()

7)KeybHook.h

This is used to integrate all the header files created and make the keylogger work properly.

Execution starts in main.cpp and the header files are used in the course of working of the program. Compiling our code in Windows yields an executable “main.exe” file which can be run as a standard Windows application to execute our program.

Applications:

Keylogger finds extensive use in the field of security and ethical hacking. Some of these uses are listed below:

- Business administration and workforce monitoring
- Parental control
- Personal system monitoring and file security
- May be used to combat cyber crime
- Monitoring public systems
- Preventing machine abuse at school/office etc.

Disclaimer:

Keylogger also has potential to be used as a malware for illegal purposes. We must take care not to violate any rules and regulations when using such software. We have made this software for purely educational purposes.