**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.

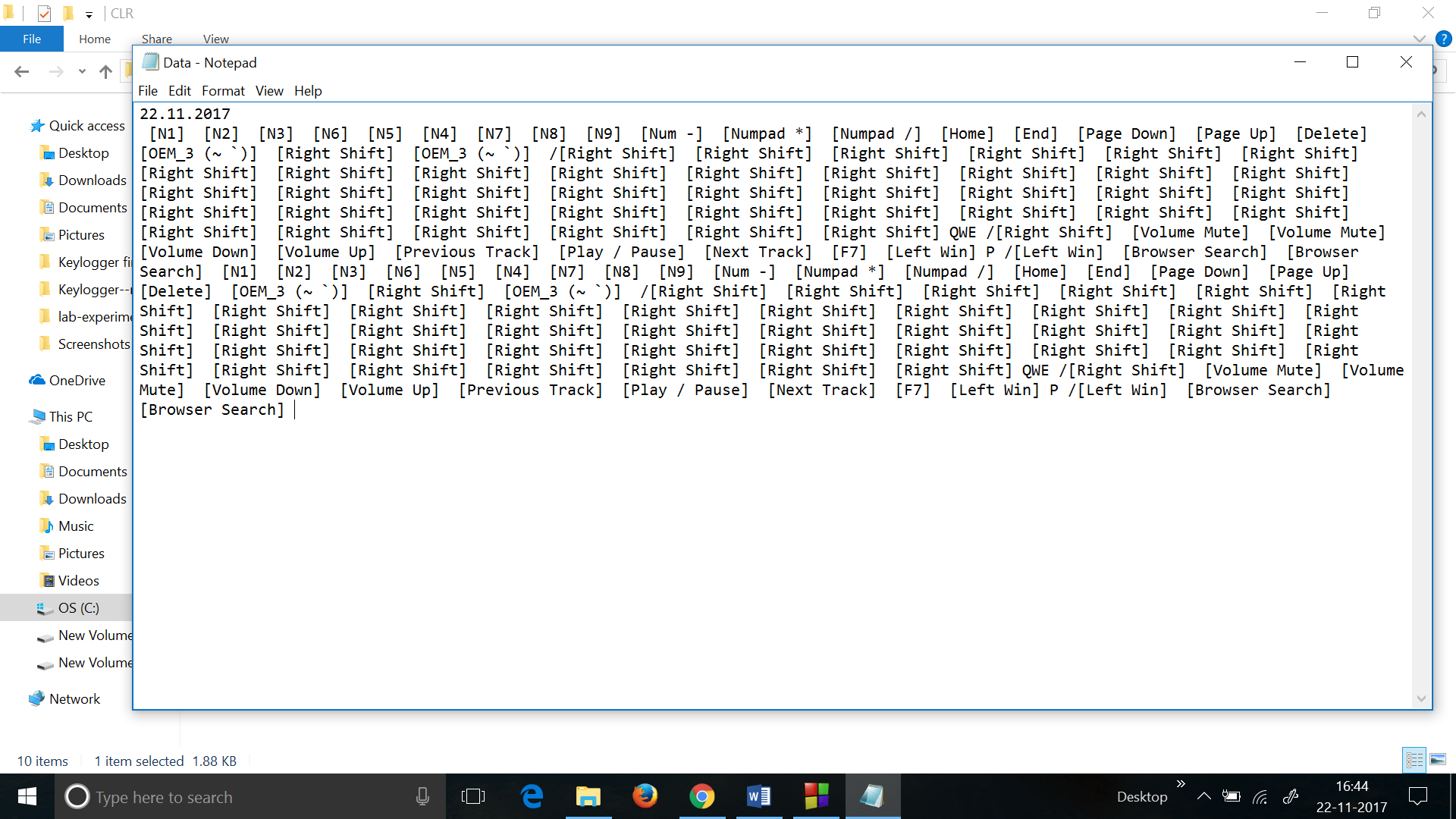
**Objective**

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

**CONTENTS**

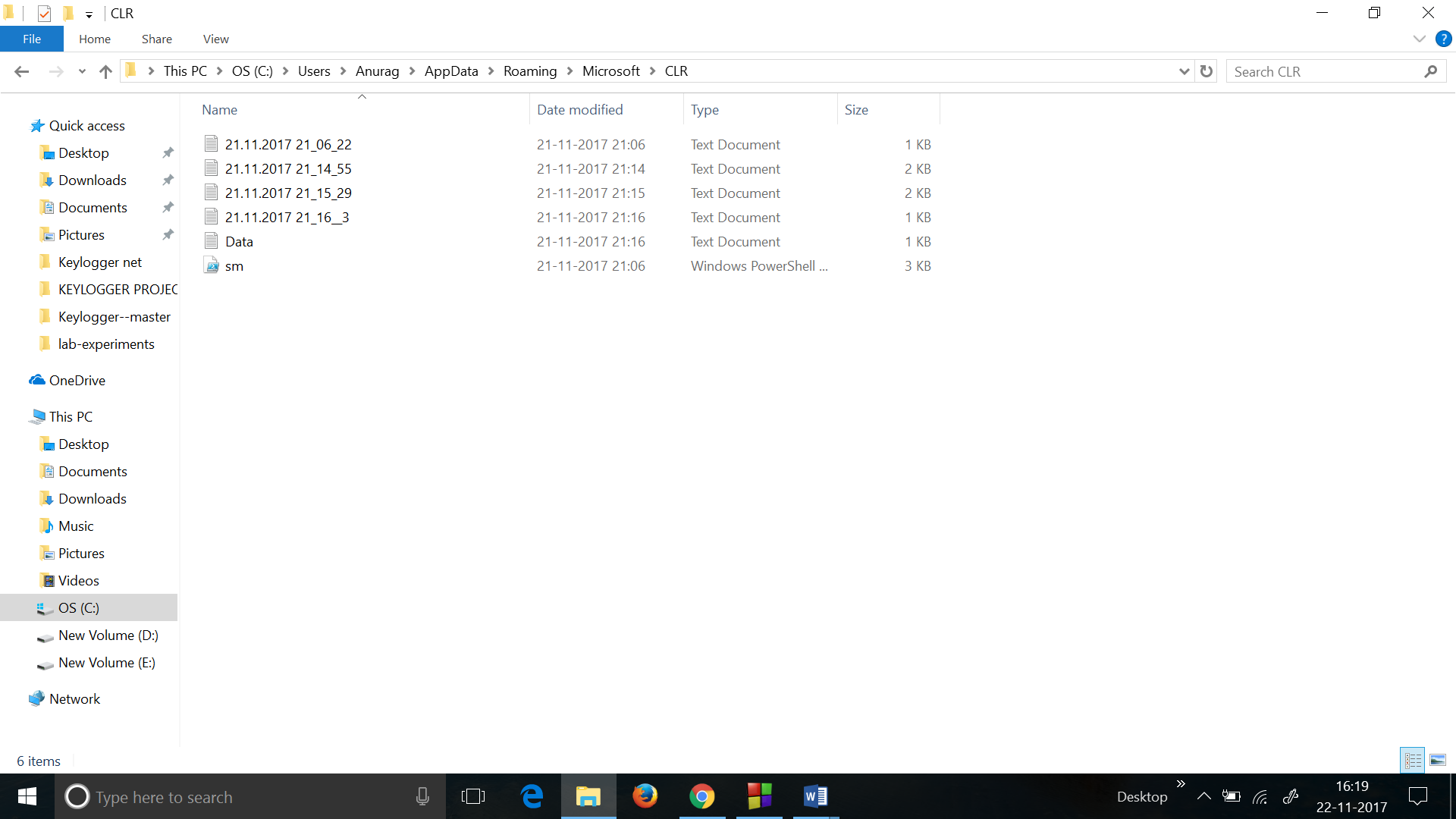
**Features:**

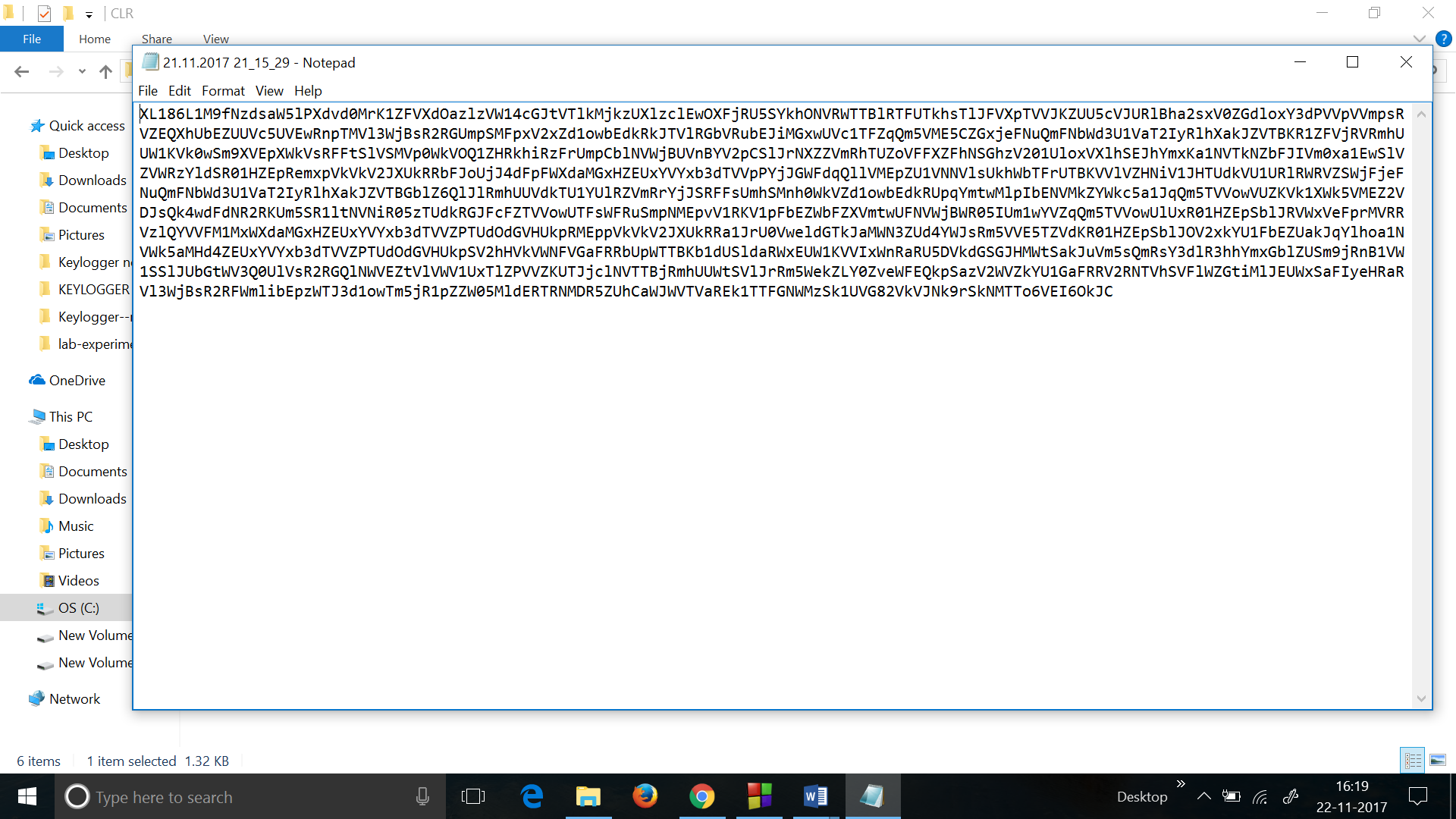
1. Detects and stores all the keystrokes and mouse clicks.



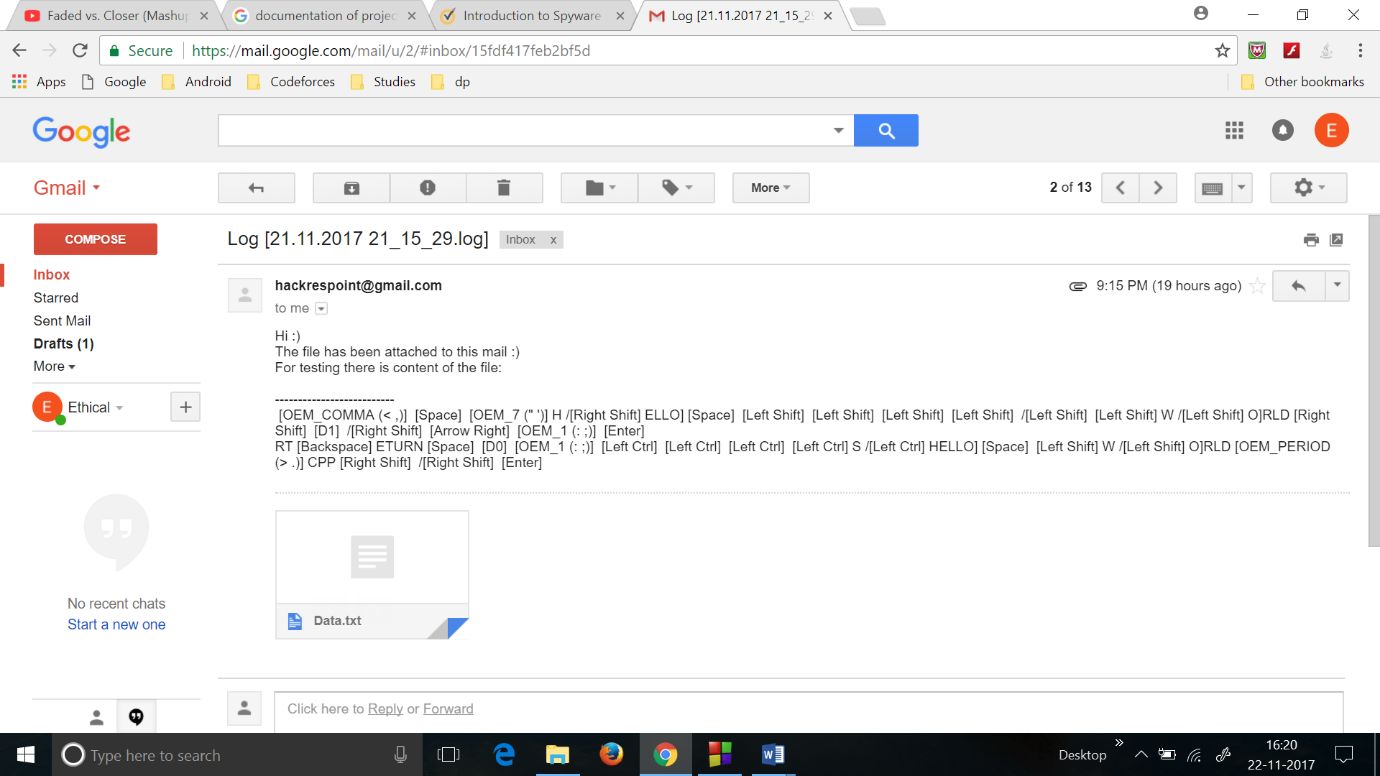
\*This is a data.txt file made at same location which stores the keys as it is without encoding(Made for testing keylogger).

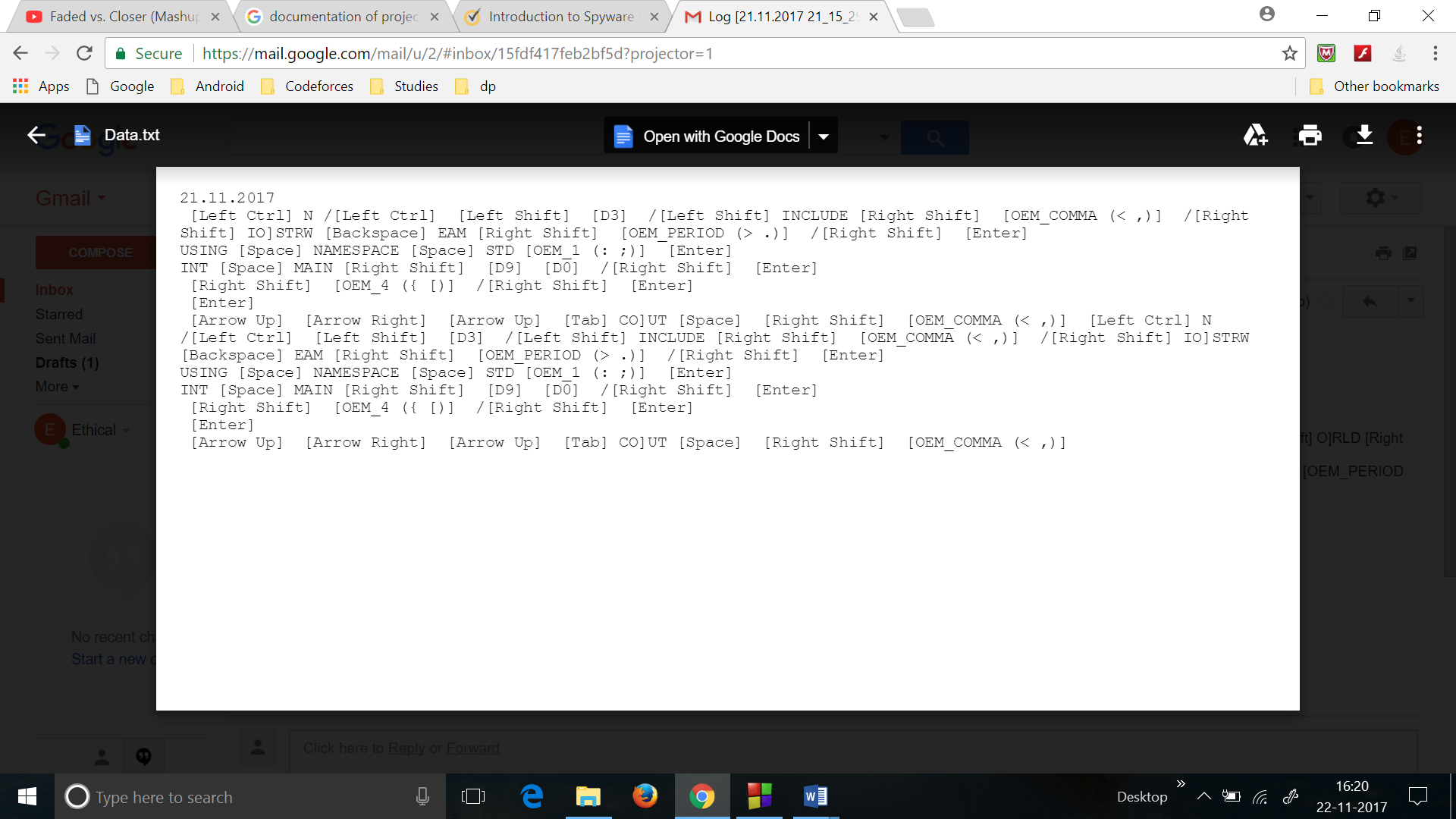
1. Encrypts the data and stores them in a specified file location.





1. 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.

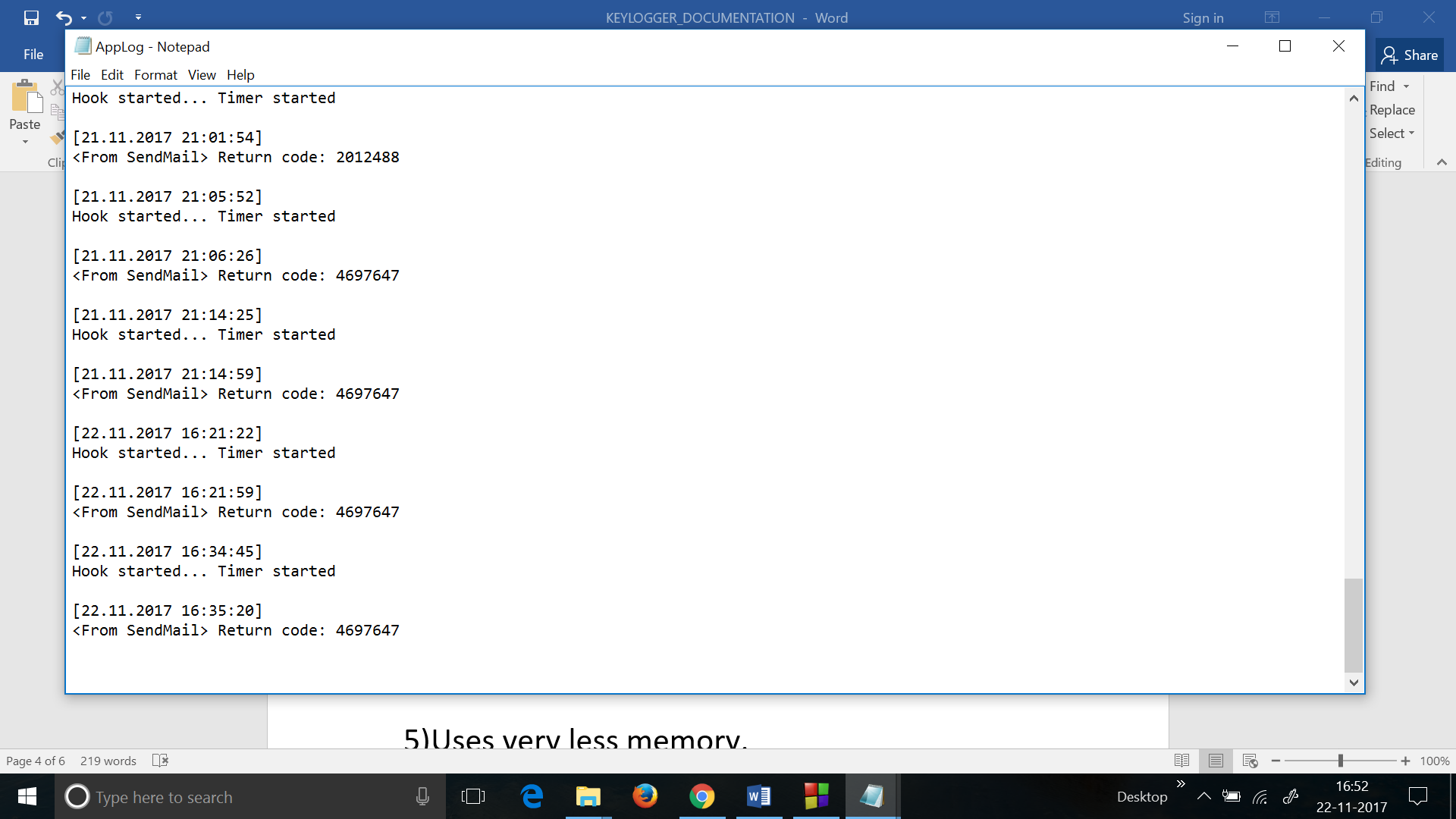




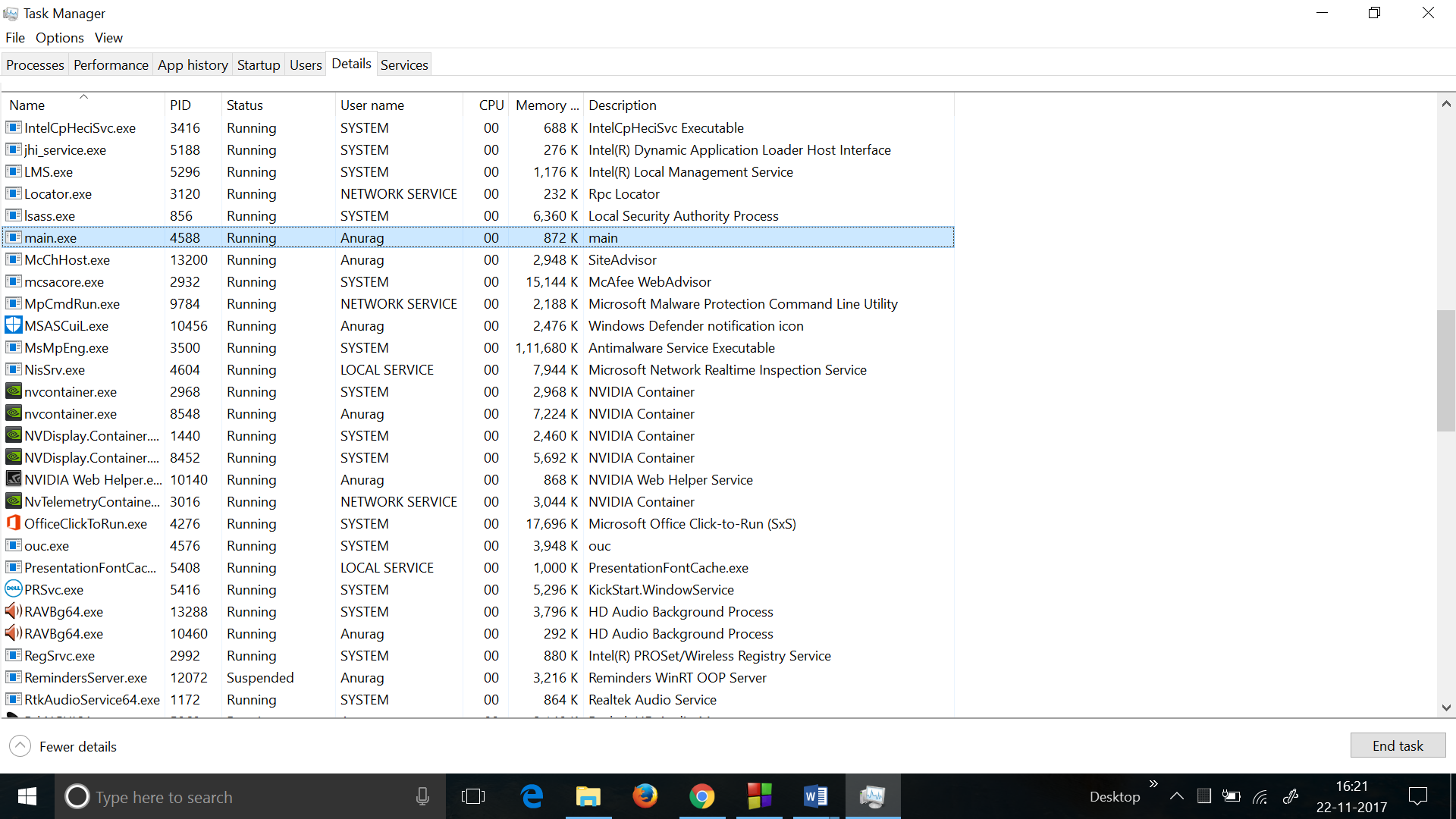
\*This is the attachment which was sent in the mail.

1. Creates a Log file(AppLog) which is used for debugging.

All the errors as well as events are appended in this file.

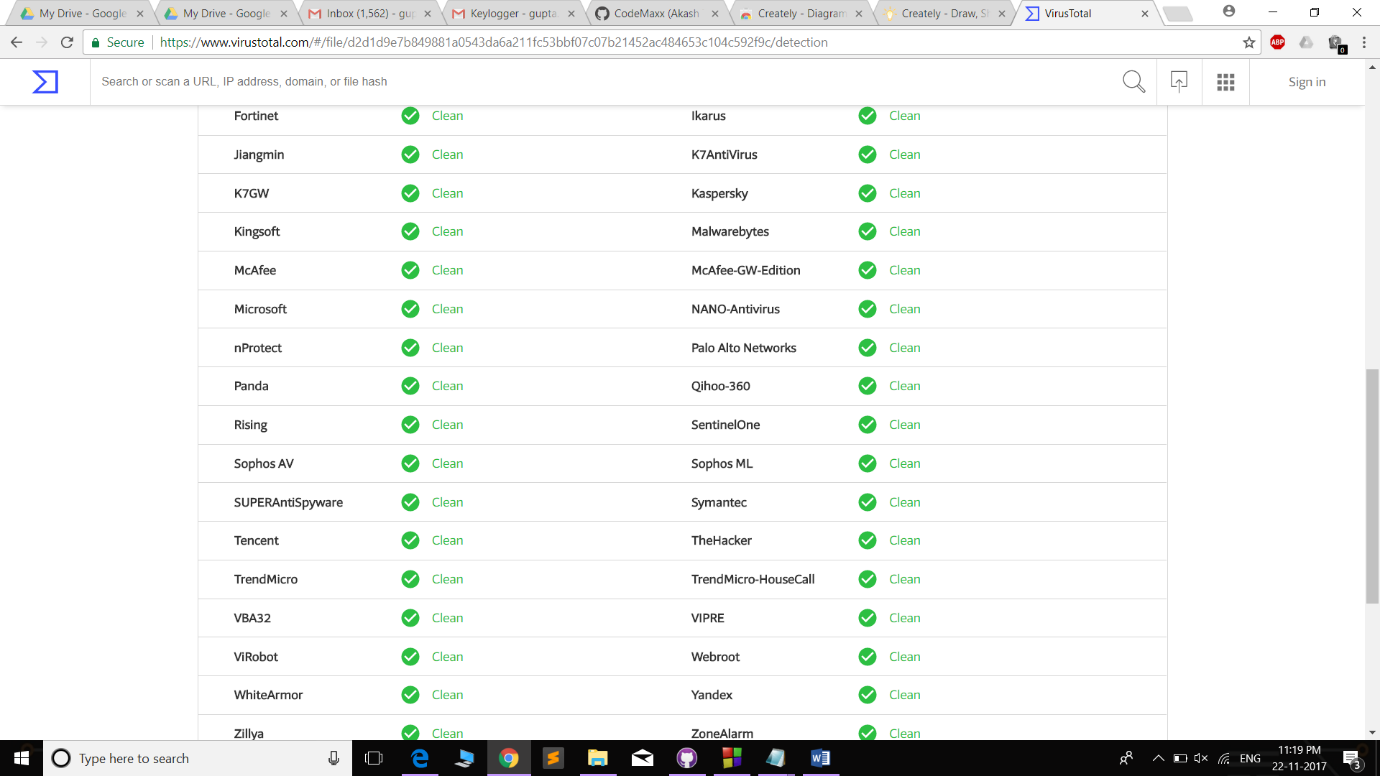


1. Uses very less memory.



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

1. It is completely undetectable by most of the Antiviruses.



**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 and write to log file for debugging reasons.

It includes 4 functions in a namespace named IO

1. GetOurPath

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

1. MkOneDr

Makes one Directory at the path provided to it.

1. 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.

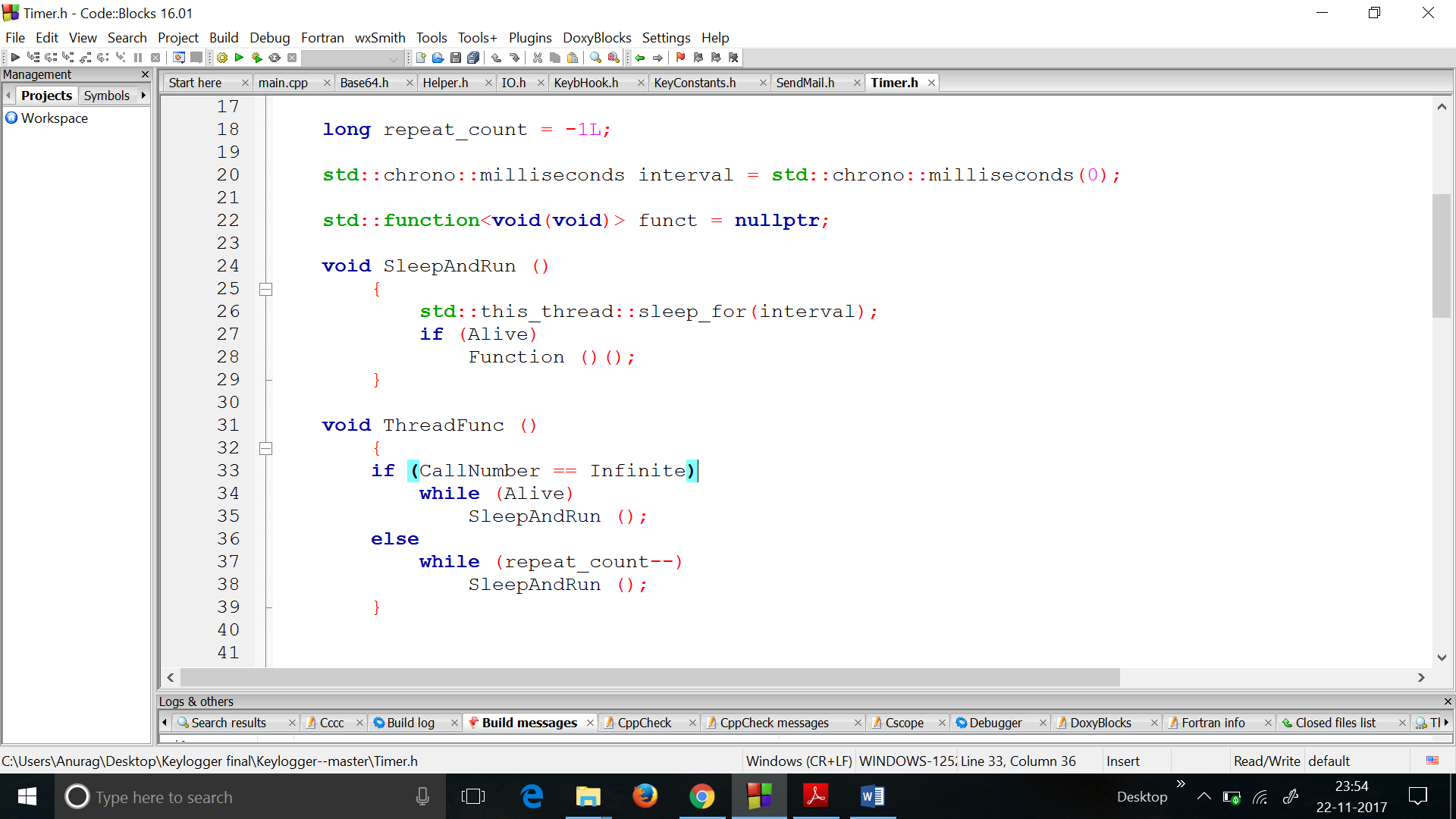
iv) WriteLog

Writes to AppLog.txt for debugging purpose.

**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 function of Timer class is as shown below.



namely ThreadFunc() and SleepAndRun().

**3) Base64.h**

i) base64\_encode()

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

1. 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:

1. DateTime struct

This is used to get the present date and time.

1. WriteAppLog(/\*parameters\*/)

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

1. 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.