

**Reverse Engineering**

**Keylogger Detector**

Zaid Afaneh 20160039

Nadeem Dahabreh 20150885

**What is a Keylogger ?** What is a keylogger? At its most basic definition, a keylogger is a function which records or keystrokes on a computer. Taken at this basic level, a keylogger looks absolutely harmless. In the hands of a hacker or a cybercriminal, a keylogger is a potent tool to steal away your information. We'll talk about how a keylogger works, how cybercriminals install it on your computer, and what you can do to avoid being a victim. You'll know what is a keylogger when we're done.

**What is a Windows API ?**

It's a set of functions and data structures that a Windows program can use to ask Windows to do something, like opening a file, displaying a message, etc. Pretty much everything that a Windows program does involves calling various API functions. Collectively, all the API functions that Windows makes available are called "The Windows API".

**What is the Relation between a Keylogger and an API ?**

Keylogger use windows API to be able to read keystrokes from keyboard, in more detailed manner a keylogger uses a Windows Hook API which can intercept any interrupts in the OS and will be able to log every keystrokes with the help of another APIs for intercepting keystrokes, (GetKeyState, GetKeyboardState, GetAsyncKeyState) are the most common APIs used for intercepting Keystrokes.

**Keyloggers we Tested our tool on:**

1- <https://github.com/GiacomoLaw/Keylogger>

2- <https://github.com/TheFox/keylogger>

3- <https://github.com/MinhasKamal/StupidKeylogger>

4- HW3 MALWARES

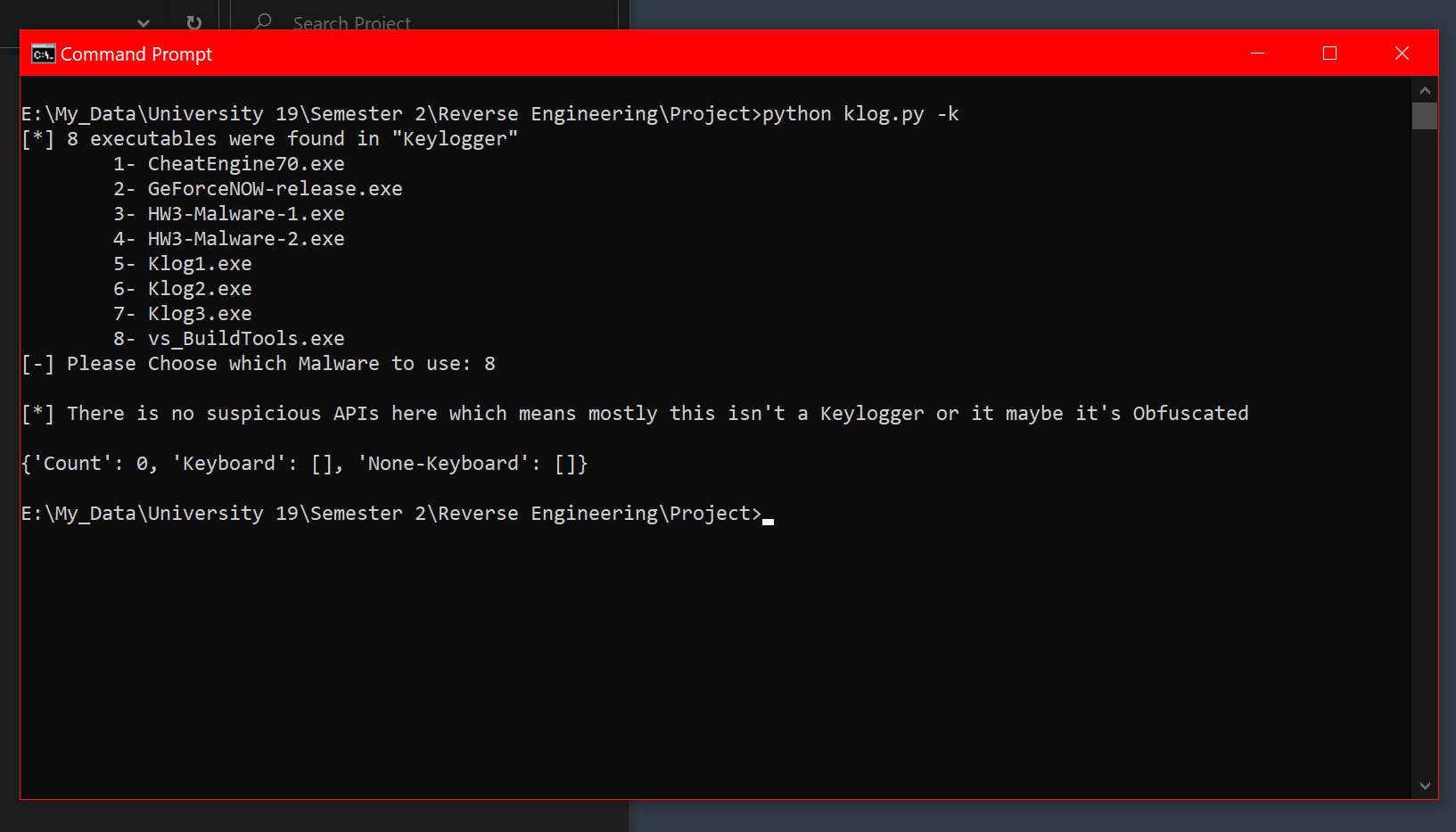
**About the code:**

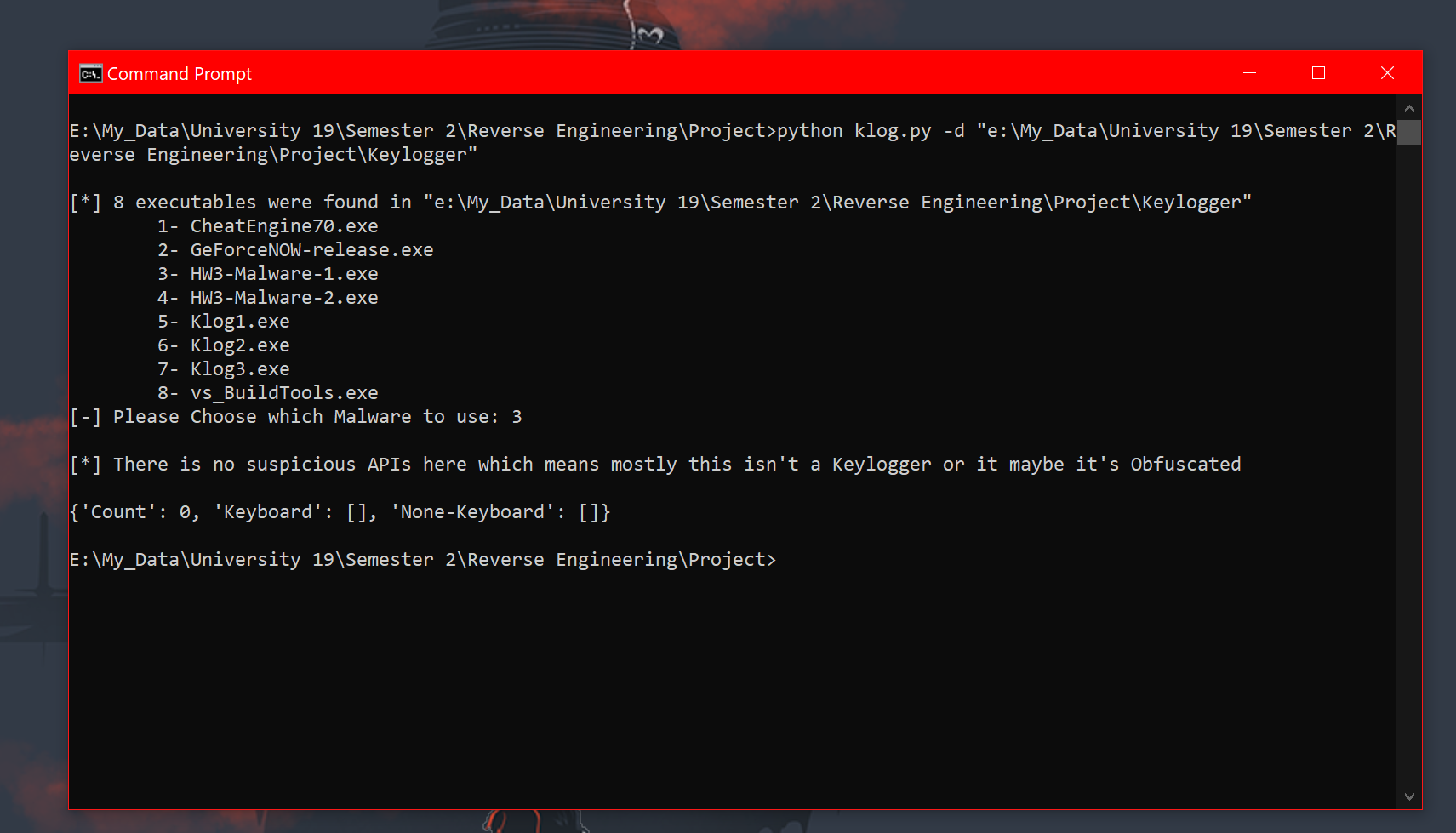
We wrote the code in a way that at the end, the result is in JSON format which can be used as a response of API for future use in case we wanted to do a website where u upload the executable and it returns a result.

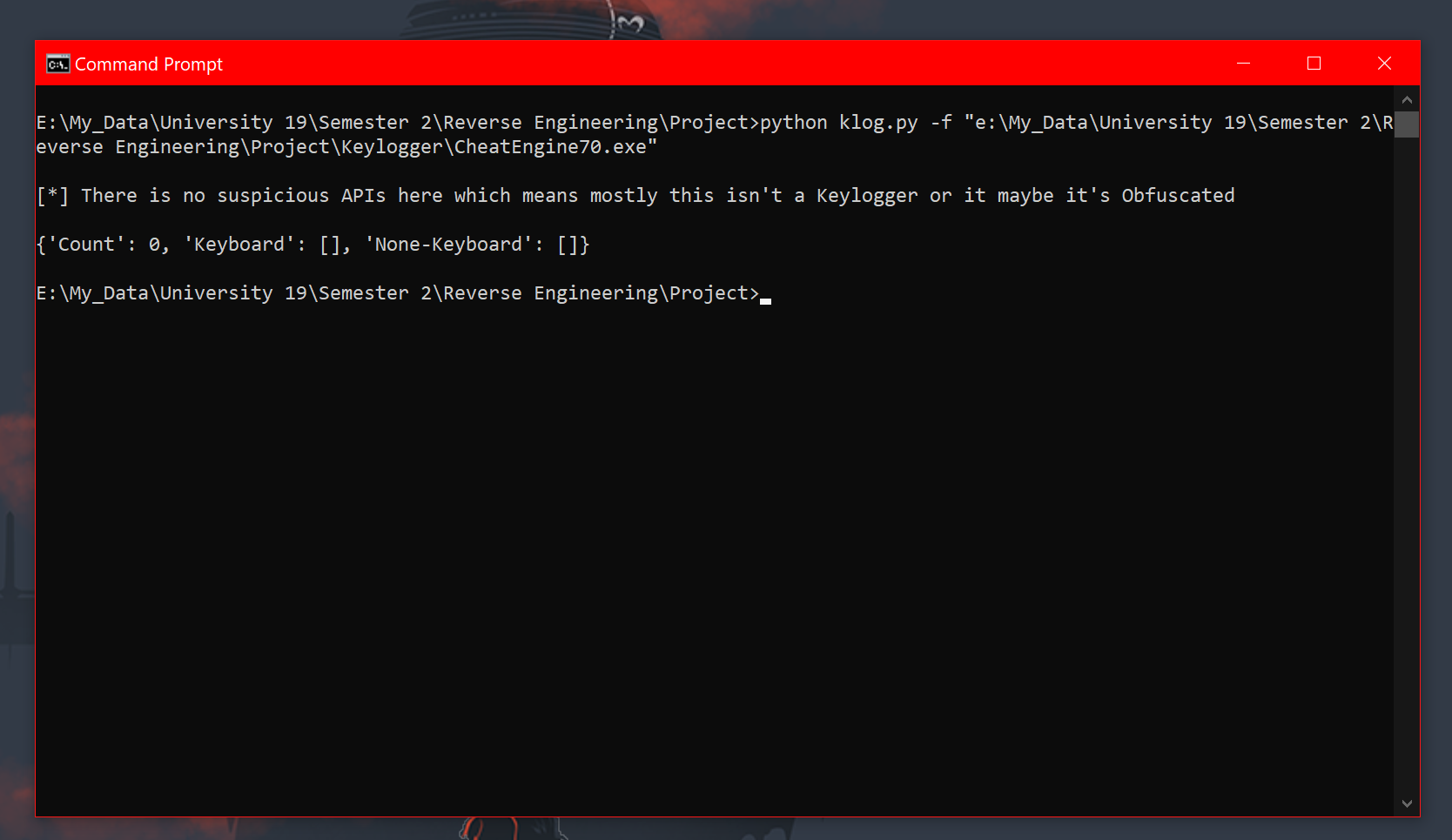
**Our Code:**

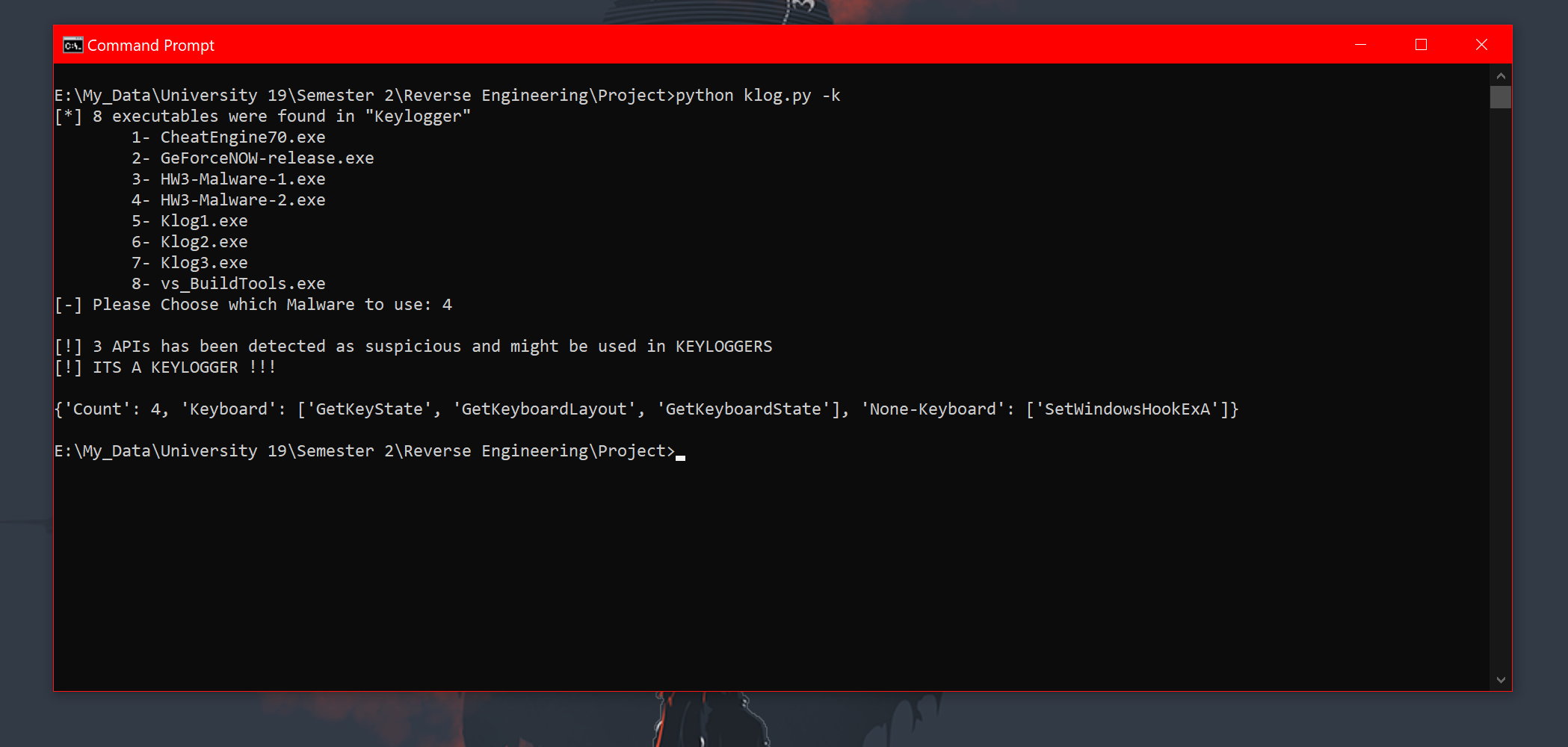
[**https://github.com/ZaidAfane3/Klog\_Detector**](https://github.com/ZaidAfane3/Klog_Detector)

**Some Results of the Tool:**

****

****

****

****