An Evaluation of Keylogger Software Against Virtual Keyboards

Testing the Security of Virtual Keyboards using Keylogger Software

Ethan Hastie

CMP320: Ethical Hacking 3

BSc Ethical Hacking Year 3

2020/21

Note that Information contained in this document is for educational purposes.

.

Abstract

Keyloggers are one of the most malicious tools used by attackers to eavesdrop on victims. Data such as passwords and personal information can be leaked without the user's knowledge, making this one of the most effective methods of gaining information on a target. There are many methods that can be used to combat against keyloggers. One of these are virtual keyboards. These can be purchased from a third-party vendor or built into the operating system. Instead of using a physical keyboard, the virtual keyboard is a software program that can be used in the same way a physical keyboard can enter data. These programs are said to protect against keyloggers because they are not the physical keyboard. This paper looks to investigate how effective keylogger software is in circumventing virtual keyboards and determine if they are safe in protecting against data exposure.

For testing, this looked at using each software-based keylogger against some virtual keyboards and finding if these are vulnerable to keystroke and screen logging. Where data may be entered, such as search engines, these were used as the basis for testing each virtual keyboard against the keylogger software. The results from this investigation showed that virtual keyboard were able to be easily defeated by most popular keylogger software used in this investigation, with data such as keystrokes and key presses being able to be recorded, either through the data themselves such as keystrokes or through key presses found in screenshots recorded by the application themselves. It was clear that most of these virtual keyboards were not designed with security in mind and that recent keyloggers were able to easily circumvent virtual keyboards due to recent improvements. Other countermeasures such as anti-virus software could therefore be more reliable at preventing keylogger tools from executing on the victim's machines, thereby preventing data leakages.

.

+Contents

.

.

1 INTRODUCTION

1.1 BACKGROUND

The ability to spy on an unsuspecting user without their knowledge can be a powerful tool and an effective method of compromising a network. A user who is unaware of their actions being monitored on their computer can have their personal data logged and captured by cybercriminals. This includes login or banking details which left exposed to an attacker can cause damaging effects to victims and severely infringe upon their privacy. The tool that can be used to perform this malicious attack is called a keylogger (What is Keystroke Logging and Keyloggers?, n.d.). A keylogger is a tool that can be installed on a victim's device and retrieve user input from a computer keyboard and store this data in a log file so that it can be viewed later. Data such as keyboard strokes, screenshots of the user's screen and clipboard values may be captured by the keylogger. Rather than retrieving this data locally, it can be it can be sent remotely via email or a through the File Transfer Protocol (FTP). It is one of the most common types of malware used by cyber attackers and comes in two main forms (Mohanty, 2020). One of these are hardware keyloggers with hardware devices such as a USB device acting as the keylogger. This would then be plugged into a victim's device manually or embedded into the architecture itself. In 2017, it was discovered that a keylogger was found in over 460 HP Laptop models. However, it was disabled by default and could be enabled to record data by activating it within the Windows Registry (Humphries, 2017). Hardware keyloggers suffer as a result as data cannot be accessed remotely as physical access is required to extract the data. On the other hand, software keyloggers are more popular compared to hardware-based keyloggers as they are much easier to spread and can be effective at adapting to the target operating system. Keyloggers may also come with advanced features including screen grabbing or screen capture which periodically captures the screen (Waterson, 2020), the ability to log cut, copy and paste operations and file operations. This means almost any actions taken on a computer can be logged (Sagiroglu and Canbek, 2009). A visit to an infected website, text message, file attachment are some methods that can be used by an attacker to deploy keyloggers on victims. This may be combined as part of a Trojan payload along with other malware such as adware or ransomware (Keyloggers - How keyloggers work & how to detect?, n.d.). It is therefore advised to victims to be vigilant of unsuspecting attachments to ensure they are not manipulated to click on these attachments or visit infected websites as part of social engineering attacks.

Despite keyloggers being used in a harmful manner, it is important to understand that this is not always the case. The software itself is legal to possess and there are legitimate uses of it today. For example, they may be used to monitor employee activity within an organisation or to help troubleshoot technical issues by an IT department. Employers must make sure that their employees are aware of their right to monitor employee activity and they can claim that this protects their personal assets and information from being misused. Therefore, it makes it

hard for an employee to argue that this acts an invasion of their privacy. Within UK law, it is legal for individuals and organisations to install keyloggers on any device if they rightfully own it. It is therefore illegal to install this software on a third-party device without their prior knowledge (Is using a keylogger software legal? – An overview about the legal situation in different countries, 2020). Since keylogger software is publicly available, both free and commercial, it means there are a wide range of options available which can make keylogger detection harder to perform by anti-virus software because of newer software signatures (StickyPassword, 2015).

There are methods that can be used to defeat keylogger programs (Waterson, 2020), but it is important to recognise that not all may work. Methods such as firewalls help to prevent keyloggers from transmitting data outside of a computer network and may also stop keyloggers in their tracks. However, this doesn't help detect keyloggers and if an attacker is located inside the network this may prove useless. Anti-virus and anti-spyware software may be used to detect and remove such malicious software. Particularly with sensitive information such as passwords, password managers have an auto fill feature to fill forms with passwords which make it difficult for keyloggers to track. On Windows, programs such as Task Manager can be used to investigate any suspicious processes within the computer and can be immediately deleted if they are not stealthy operations. One of the least known methods used in defending against keyloggers are virtual keyboards (Bhardwaj and Goundar, 2020). An example of this includes the Windows built-in keyboard software called 'Windows On-Screen Keyboard' which can be seen below:

Figure 1 Windows Built-In Virtual Keyboard 'On Screen Keyboard'

Instead of using a physical keyboard, a virtual keyboard is a physical program within the computer that can be installed via available products or built in, as with Windows keyboard, and can be used in the place of a physical keyboard to input data into the computer. These are built-in on phones or tablets since these devices don't have access to a physical keyboard which can be accessed via the touchscreen interface to enter data. On a desktop interface, they can help users with disabilities as they may not be able to use the physical keyboard. They may also be used for other purposes such as users who write in different character sets or alphabets. It can be a good countermeasure against keyloggers although screen-logging may render this obsolete. Screen-logging keyloggers will take screenshots periodically to capture the user's pressed keys, which depending on how the virtual keyboard is setup and the colour of the pressed keys can make it easy to determine what key was pressed. In

addition, some advanced keyloggers already possess the ability to capture data from virtual keyboards. However, even with a successful intrusion into a victim's device, virtual keyboards can act as a last line defense should prevention software fail to detect keylogger tools. Despite the security some virtual keyboards may offer, they can be extremely hard to use compared to physical keyboards, although this may be less of an issue when using phones or tablets. They may then only be used to enter sensitive data, such as passwords, to avoid keyloggers.

This investigation aims to evaluate different keylogger software against multiple virtual keyboards to determine how effective software-based keyloggers are in circumventing virtual keyboards as a defence method against keylogger tools. The testing will include keystroke and screen logging and will investigate if keystrokes are able to be extracted from virtual keyboards and if screenshot logging will determine pressed keys from the virtual keyboard.

1.2 AIM

To evaluate how successful keylogger software will be in circumventing virtual keyloggers the following must be performed:

- Test virtual keyboards for keystroke logging
- Test virtual keyboards for screen logging

These guidelines should be used to determine if keylogger software is successful in bypassing virtual keyboards. The testing should show the safety of the virtual keyboards according to these two factors.

2 PROCEDURE

2.1 OVERVIEW OF PROCEDURE – ENVIRONMENT SETUP

A Windows 64-bit virtual machine was created that was used to install the keylogger and virtual keyboards necessary for testing. A testing email account was also created which was used to sign up and install the tools that were tested.

2.2 OVERVIEW OF PROCEDURE – TESTING

Table 1 Testing Scores

Number	Colour	Description
1		The keylogger software managed to overcome the virtual keyboard.
2		The virtual keyboard protected against the keylogger in a satisfactory method.
3		The keylogger was not successful in capturing data from the virtual keyboard.

Table 1 shows how the keyloggers were scored during testing. Within Table 1, if a virtual keyboard was able to be circumvented, this would be marked with the colour corresponding to Number 1. If data was captured from the virtual keyboard but was unreliable because not every keystroke was captured, then this was marked with the colour corresponding to Number 2. Finally, if no data was captured from the virtual keyboard and was able to defend against the keylogger this was marked with the colour corresponding to Number 3.

2.3 OVERVIEW OF PROCEDURE – KEYLOGGER SOFTWARE

2.3.1 Spyrix Keylogger

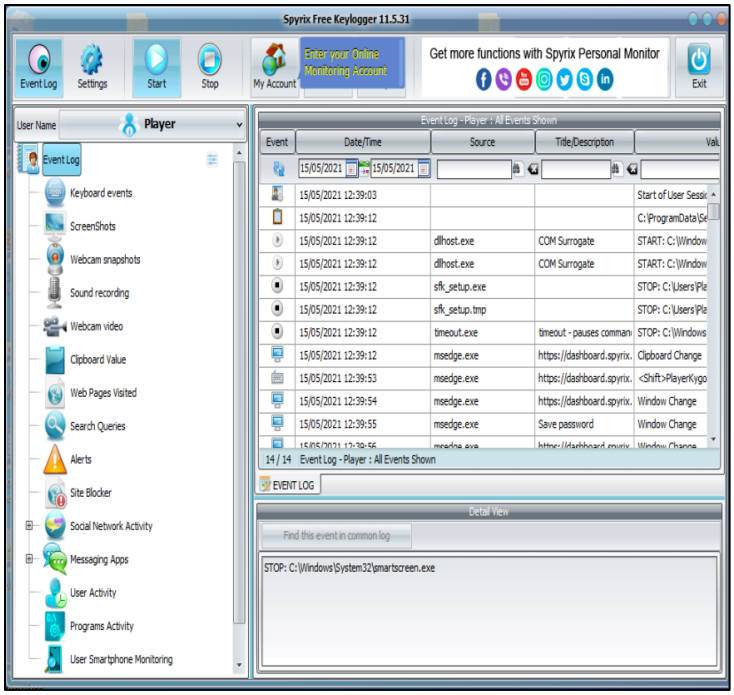

Figure 2 Spyrix Keylogger User Interface

Figure 2 shows the user interface of Spyrix Free Keylogger (Spyrix Free Keylogger, 2021) which was available on https://spyrix.com. The software allowed for remote cloud monitoring which could be accessed via a browser and any device, although this was not used as the local version was more effective. Data such as visited websites, URLs, removable drives can be viewed using a secure portal on a browser. In addition, the tool also possesses a hidden mode meaning it won't be visible in the computers ongoing processes, but this was only available in the commercial version. It also has a live viewing feature allowing a user to monitor a user's activity in real time, which could be used to circumvent virtual keyboards. The setup instructions can be viewed in Appendix B Figures 1-1 and 1-2. The user interface showed many options such as keyboard events and screenshot data which can be seen below:

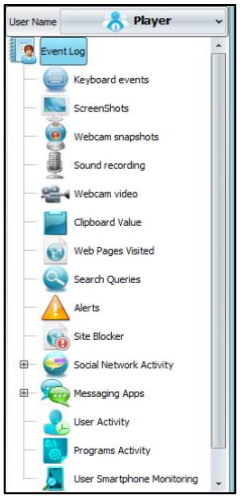

Figure 3 Event Window

Detailed log events could also be viewed. This data was represented through columns such as type of event, date and time of the event, source (name of file), title/description and value. An example seen below shows every event which took place within the machine. Events such as keystrokes and changing windows were able to be viewed easily:

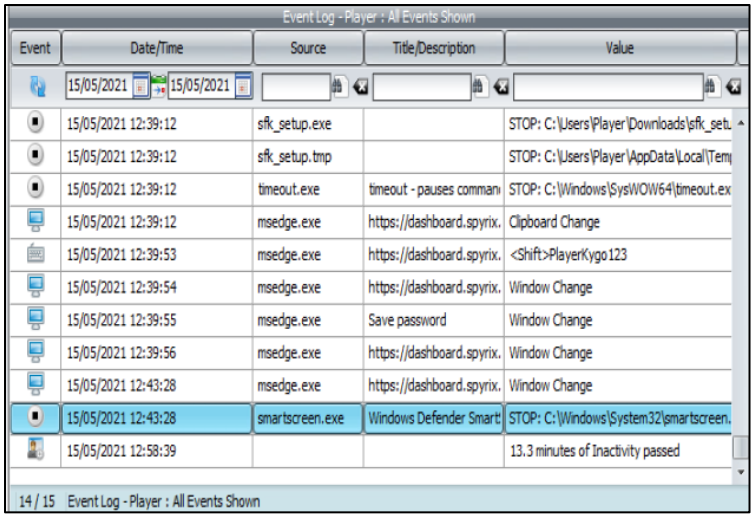

Figure 4 Event Log Window

Figure 4 highlighted that logs collected within Spyrix Keylogger (Spyrix Free Keylogger, 2021) could be filtered for data. Remote viewing could also be used. Using a browser, this was logged into allowing for remote viewing of the machine's events:

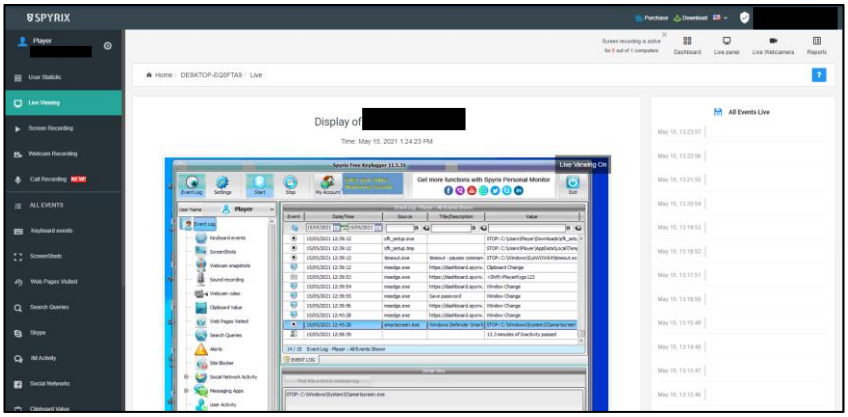

Figure 5 Remote Spyrx Keylogger Interface Accessed via Browser

Figure 5 shows the options that can be viewed under the remote interface of the software, including live viewing features. Setup instructions can be viewed in Appendix B Figures 1-1 – 1-3.

2.3.2 Actual Keylogger

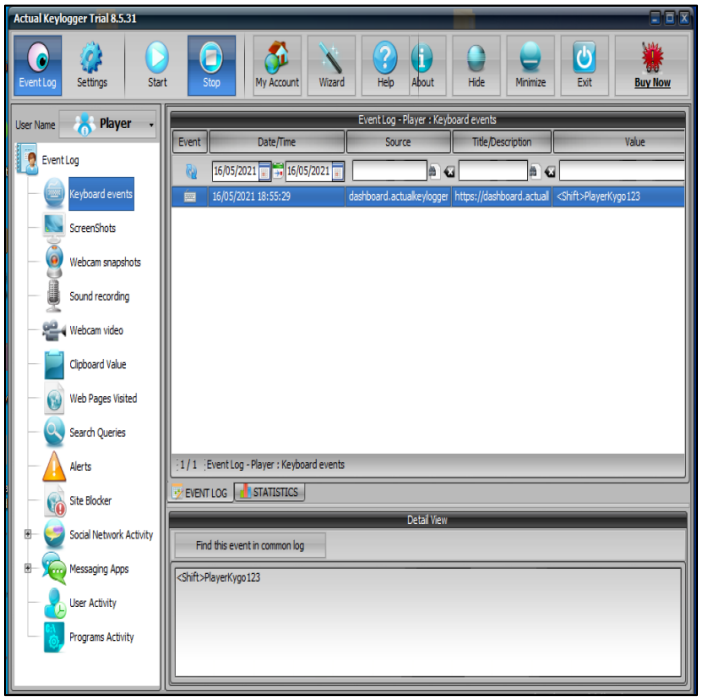

Figure 6 Actual Keylogger User Interface

Figure 6 shows Actual Keylogger (Actual Keylogger, n.d.) which was available at https://www.actualkeylogger.com/. It recorded all keystrokes, running and closed programs, visited websites, print, clipboard and possessed screenshot capabilities. Data can be forwarded via email, FTP

or through the LAN, although this was not required. The software can be useful for a wide range of audiences such as parents, system admins and can provide extra utility for users on their own machines acting as data recovery. The setup instructions can be viewed in Appendix B Figures 1-4 – 1-10.

2.3.3 Refog Personal Monitor

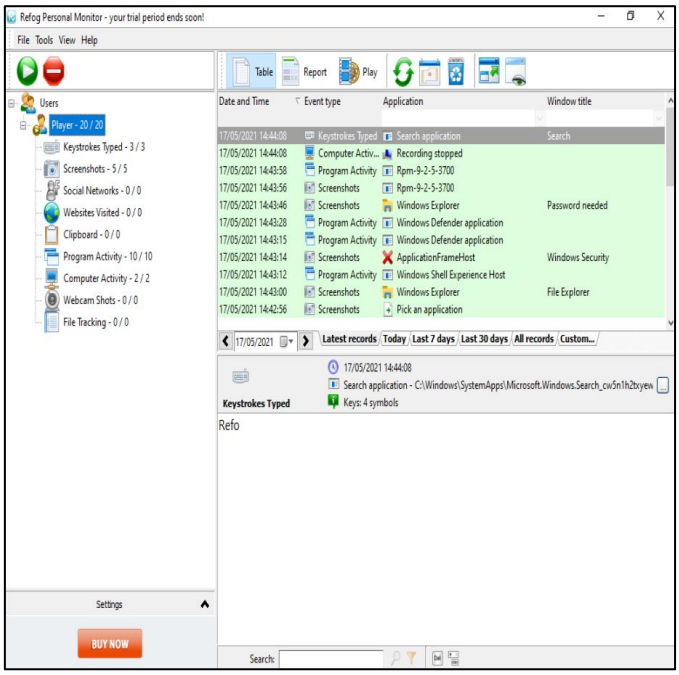

Figure 7 Refog Personal Monitor User Interface

Figure 7 shows Refog Personal Monitor (Refog Personal Monitor, n.d.) which was available at https://www.refog.com/. It also has screenshot capabilities and stealth capabilities. The left window can be used to view the different types of data from the keylogger program. This can be seen below:

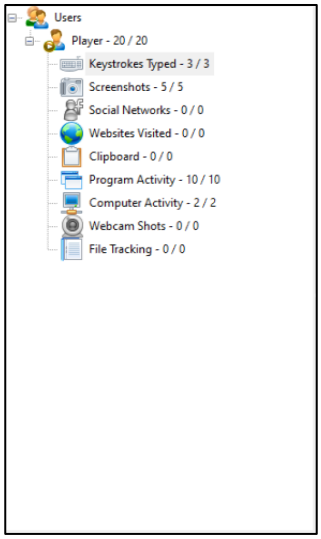

Figure 8 Different Data Collected by Refog Personal Monitor

Figure 8 shows the left active window in the application, with data such as keystrokes and screenshots being able to be viewed. When clicked on a section in the left active, this brought up a window showing detailed logs:

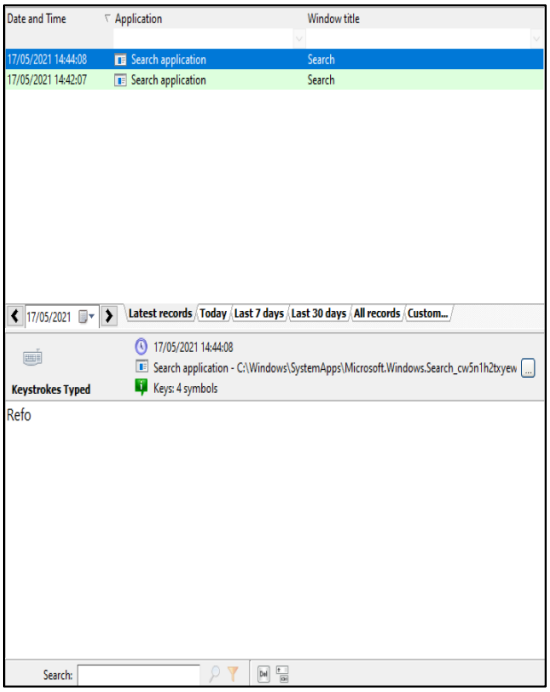

Figure 9 Event Log Window in Refog Personal Monitor

Figure 9 shows the detailed logs that can be viewed. The setup instructions can be viewed in Appendix B Figures 1-11 – 1-16.

2.3.4 Iwantsoft Keylogger

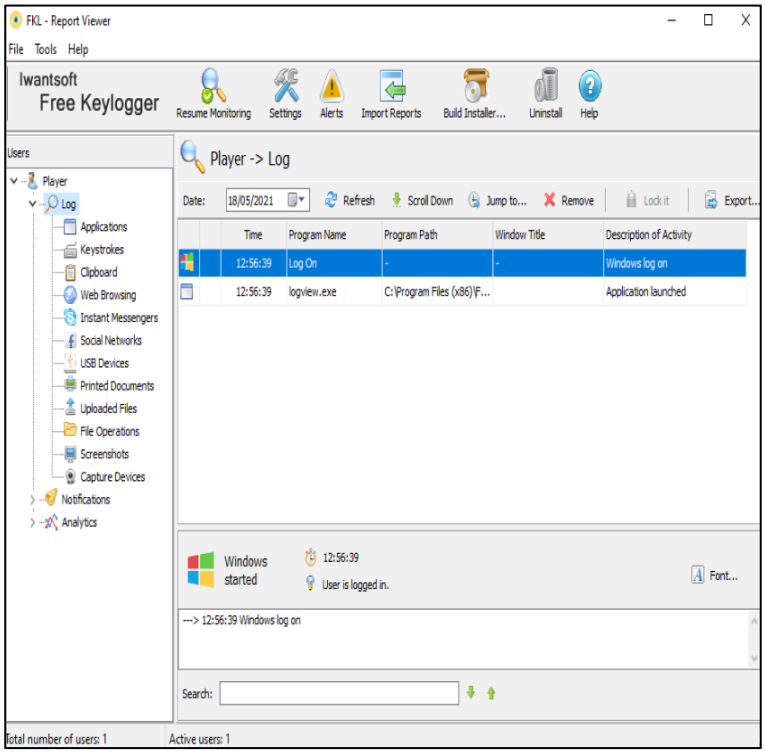

Figure 10 IwantSoft Free Keylogger User Interface

Figure 10 shows Iwantsoft Free Keylogger (Iwantsoft Free Keylogger, n.d.) which was available at https://www.iwantsoft.com/. IWANTSOFT offered a free and commercial version, with the latter possessing more advanced features such as screenshot capture, remote data collection and recording audio and webcam data. Example data that can be monitored in Iwantsoft Keylogger can be seen below. Data such as application events can be seen in the event window:

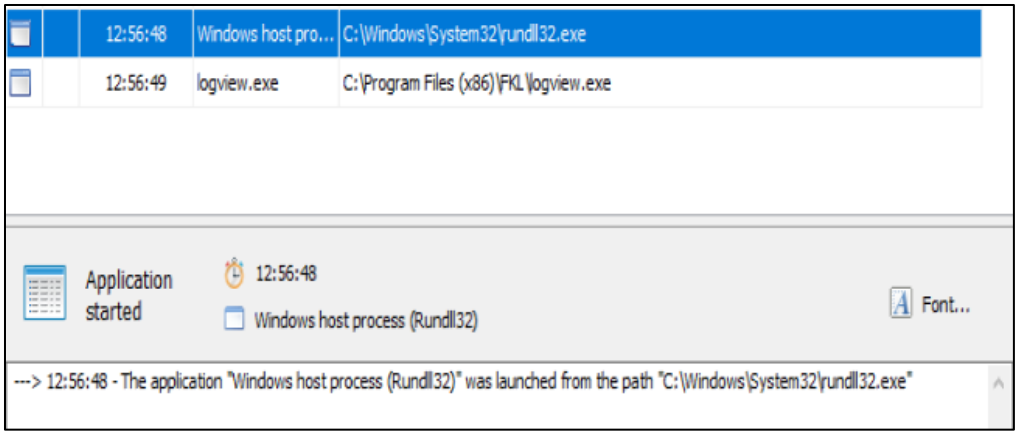

Figure 11 Event Logs

Figure 11 shows a file called rundll32.exe being executed within the machine. Setup instructions for this keylogger can be viewed in Appendix B Figures 1-17 and 1-18.

2.3.5 Revealer Keylogger

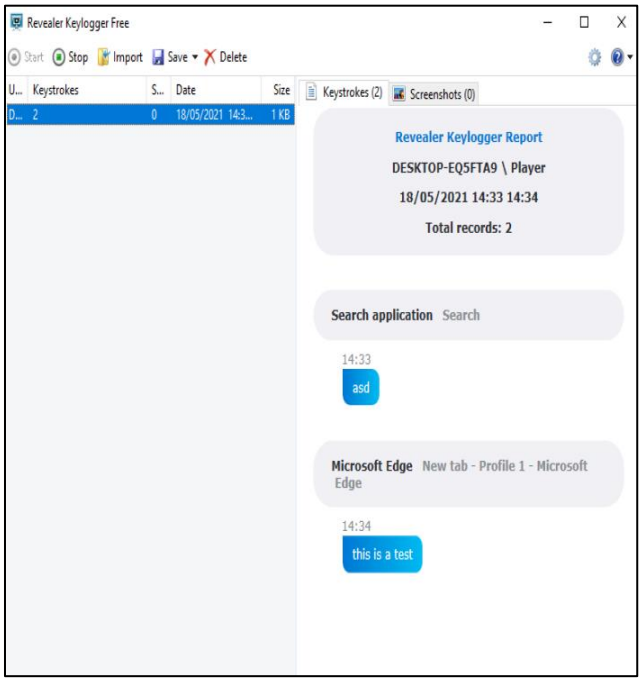

Figure 12 Revealer Keylogger Free User Interface

Figure 12 shows Revealer Keylogger Free (Revealer Keylogger Free, 2021) which was available at https://www.logixoft.com/en-gb/index. It offers free and commercial versions and certain features

were locked behind a paywall such as screenshot logging. Therefore, the screenshot feature could not be tested. Setup instructions for this keylogger can be viewed in Appendix B Figures 1-19 – 1-22.

2.3.6 KidLogger

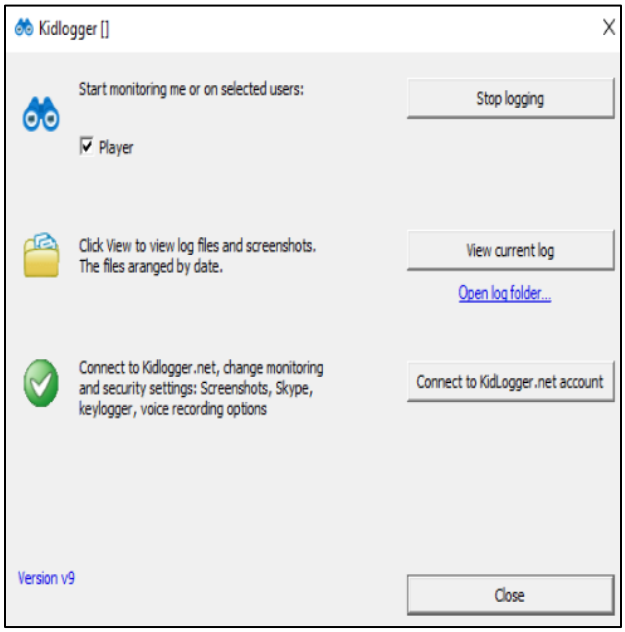

Figure 13 KidLogger Main Menu

Figure 13 shows KidLogger (KidLogger, n.d.) which was available at https://kidlogger.net/. This functions as another method of parental control and can be used to monitor activity on devices. Important setting configurations can be set, as seen below:

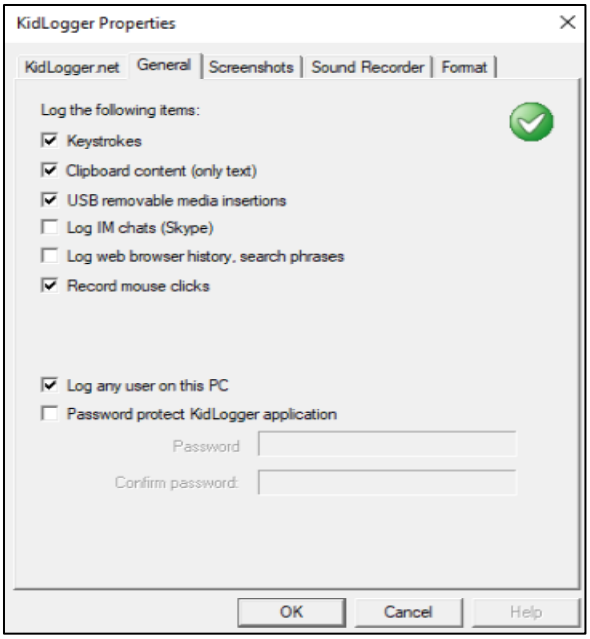

Figure 14 KidLogger General Settings

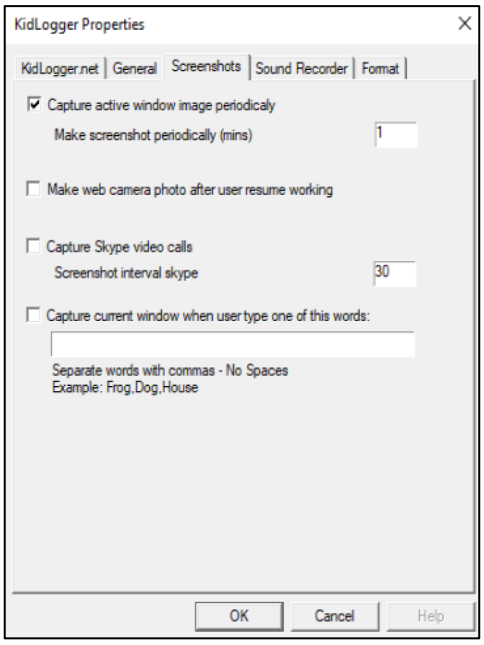

Figure 15 KidLogger Screenshots Settings

Figures 14 and 15 highlight important settings to configure the KidLogger (KidLogger, n.d.). This included activity keystrokes and setting the time of peridiocally taking screenshots. Logs were able to be viewed using the browser, which can be seen below:

Figure 16 Logs from KidLogger

Figure 16 shows the captured logs from the user Player. The setup for this software can be seen in Appendix B Figures 1-23 – 1-25.

2.3.7 Best Free Keylogger

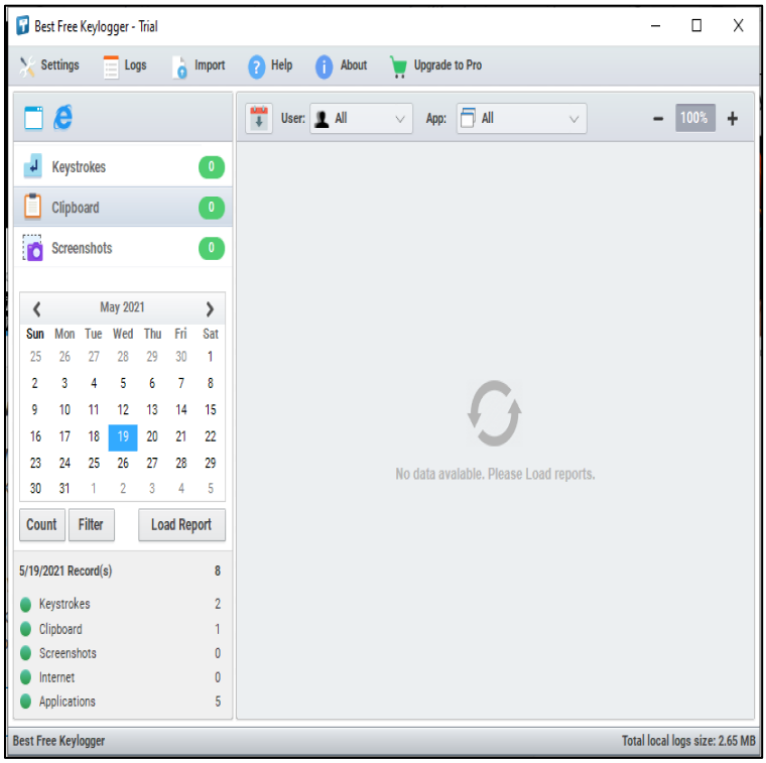

Figure 17 Best Free Keylogger User Interface

Figure 17 shows the Best Free Keylogger (Best Free Keylogger, n.d.) which was available at https://bestxsoftware.com/. Logs can be viewed as seen below:

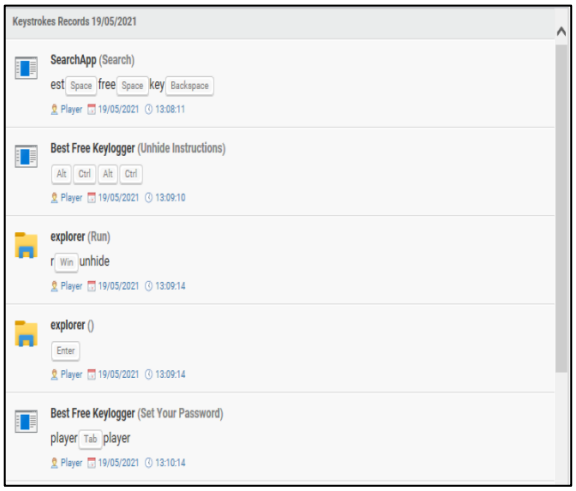

Figure 18 Event Logs Recorded using Best Free Keylogger

Setup instructions can be viewed in Appendix B Figures 1-26 – 1-32.

2.4 Overview of Procedure – Virtual Keyboards

2.4.1 Free Virtual Keyboard

Figure 19 Free Virtual Keyboard User Interface

Figure 19 showed the example user interface within Free Virtual Keyboard (Free Virtual Keyboard, 2015). This was accessed via https://www.mediafreeware.com/free-virtual-keyboard.html.

2.4.2 Windows On-Screen Keyboard

Figure 20 Windows On-Screen Keyboard

Figure 20 showed the user interface within Windows On-Screen Keyboard. No setup was required as this was a program within Windows 10.

2.4.3 Comfort On-Screen Keyboard Lite

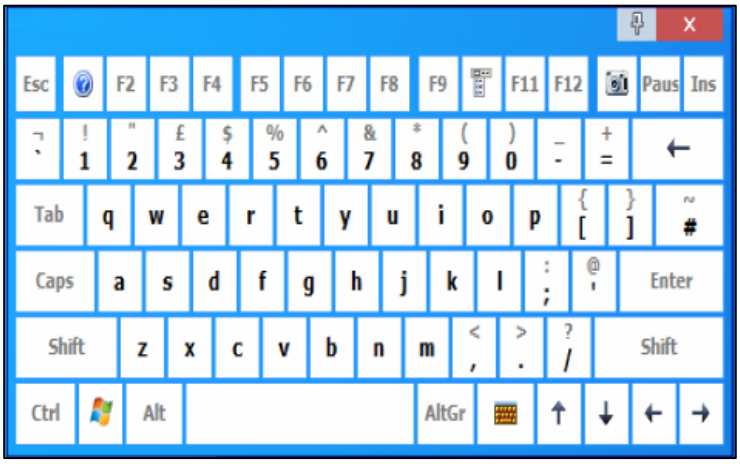

Figure 21 Comfort On-Screen Keyboard Lite User Interface

Figure 21 showed the user interface for Comfort On-Screen Keyboard-Lite. It was available via https://comfort-on-screen-keyboard.en.uptodown.com/windows.

2.4.4 Touch-It Virtual Keyboard

Figure 22 Touch-It Virtual Keyboard User Interface

Figure 22 showed Touch-It Virtual Keyboard (Touch-It Virtual Keyboard, 2020) interface. This was available at https://chessware.ch/virtual-keyboard/.

2.4.5 Neo's SafeKeys

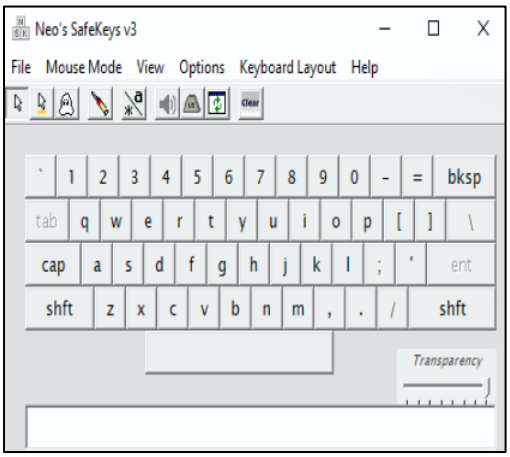

Figure 23 Neo's SafeKeys User Interface

Figure 23 showed Neo's SafeKeys (Neo's SafeKeys, n.d.). It was available at https://www.aplin.com.au/. This was known as one of the most secure virtual keyboards that would be used to defend against keyloggers, both hardware and software. In the documentation for the tool, it described it offered protection against clipboard loggers, screen loggers, mouse position keyloggers and field-scraping. Aplin Software, the creator of Neo's Safekeys, provides documentation for the tool which can be viewed at https://www.aplin.com.au/neos-safekeys-v3/how-neos-safekeys-v3-works. Compared to other virtual keyboards on this list, it functioned slightly differently as data was not entered through the interface and instead data was inserted through drag and drop methods. The 'Mouse Mode' option that was used Hidden Mouse and Hover Entry. This was proven to work against keystroke logging and provided good protection against screen logger features. Since data could be entered into the keyboard, this was not visible and was represented by asterisks:

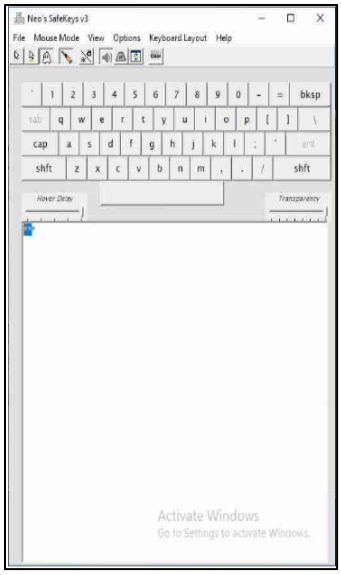

Figure 24 Secure Handling of Data within Neo's SafeKeys

Figure 24 shows the data which was hidden by asterisks by the program. The top menu allows for user settings to be modified easily.

2.4.6 Hot Virtual Keyboard

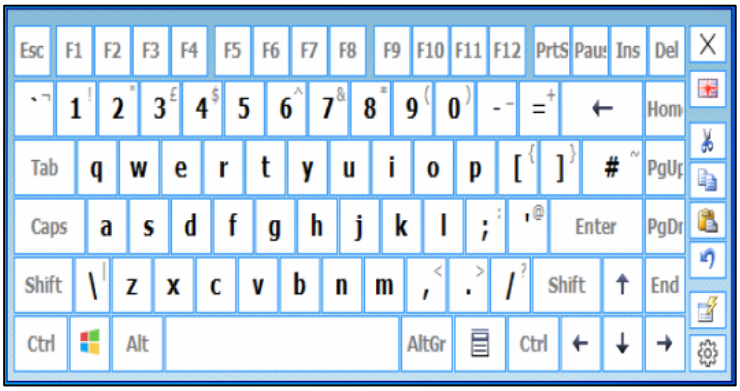

Figure 25 Hot Virtual Keyboard

Figure 19 showed Hot Virtual Keyboard (Hot Virtual Keyboard, 2021). It was available at https://hotvirtualkeyboard.com/.

2.5 SPYRIX FREE KEYLOGGER

2.5.1 Summary

Table 2 Keystroke Logging Results using Spyrix Keylogger

	Free Virtual Keyboard	Microsoft On-Screen Keyboard	Comfort On-Screen Keyboard Lite	Touch-It Virtual Keyboard	Neo's Safekeys	Hot Virtual Keyboard
Spyrix Free Keylogger						

Table 3 Screen Logging Results using Spyrix Keylogger

	Free Virtual Keyboard	Microsoft On-Screen Keyboard	Comfort On-Screen Keyboard Lite	Touch-It Virtual Keyboard	Neo's Safekeys	Hot Virtual Keyboard
Spyrix Free Keylogger						

Tables 2 and 3 show the results of testing Spyrix Free Keylogger against multiple virtual keyboards. The procedure for how these tests were carried out can be seen below.

2.5.2 Free Virtual Keyboard

Free Virtual Keyboard was not able to defend against Spyrix (Spyrix Free Keylogger, 2021) and data such as keystrokes and screen capture were able to be used to counteract against this. Keystroke data was able to be captured, which can be seen below:

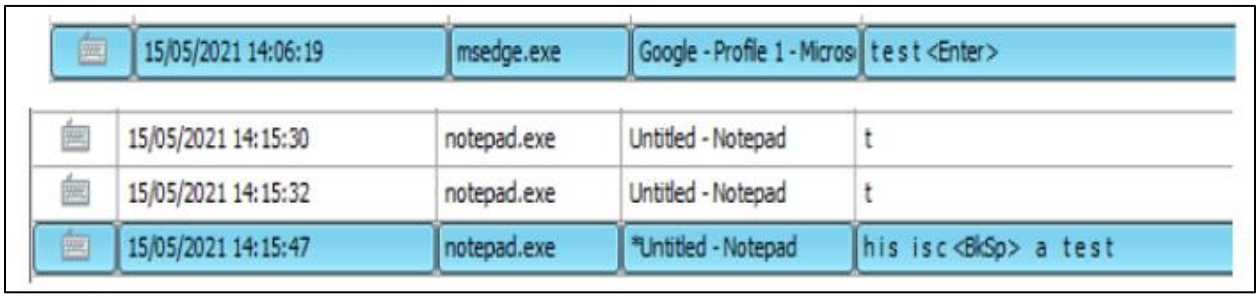

Figure 26 Captured Keystrokes from Free Virtual Keyboard

Figure 26 showed that the Free Virtual Keyboard were not successful in stopping keystroke recordings. Due to how the keyboard responded to pressed keys, the screenshot feature was able to record this. However, due to the timing of the screenshots taking place, this would be unreliable and so it would not be able to capture every pressed key:

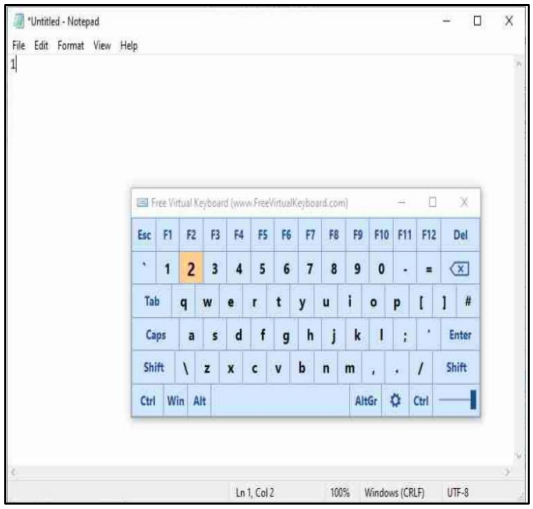

Figure 27 Screengrab of Pressed Key in FVK taken from Spyrix

Figure 27 shows a screenshot obtained via the screengrab feature which shows that the number 2 was pressed. Other results can be seen in Appendix A Figures 1-1 and 1-2.

2.5.3 Windows On-Screen Keyboard

Spyrix (Spyrix Free Keylogger, 2021) was able to record data from the windows virtual keyboard, proving that it was not effective against keyloggers:

Figure 28 Captured Data from Windows On-Screen Keyboard

Figure 28 shows the recorded keystrokes from this virtual keyboard. The screenshot feature seemed to capture pressed keys, which was easily identified due to the change in colour for a pressed key. Settings could be configured for this keyboard that would stop the highlighting of pressed keys. It couldn't record every single pressed key via the screenshot, making this unreliable. This can be seen below:

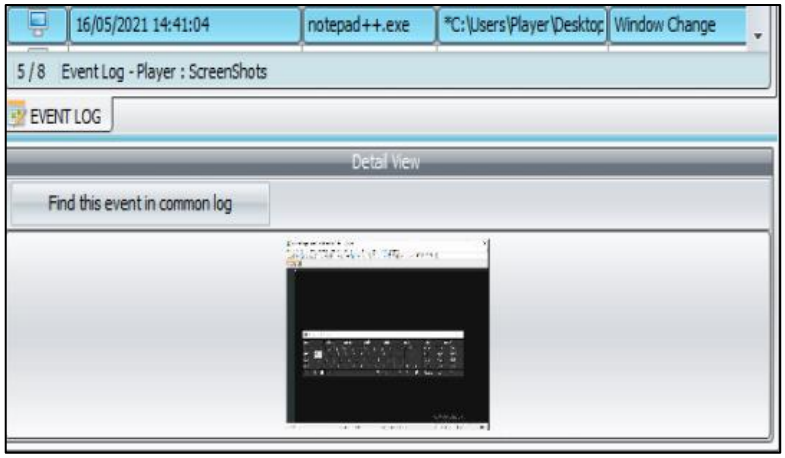

Figure 29 Record of Pressed Key in Notepad

Figure 29 showed that the software was able to record pressed keys using screenshots. The full image shown in Figure 29 can be viewed in Appendix A Figure 1-3.

2.5.4 Comfort On-Screen Keyboard-Lite

Like FVK and Windows On-Screen Keyboard, it also possessed highlighting for pressed keys. This made it easy for Spyrix (Spyrix Free Keylogger, 2021) to record pressed keys using its screengrab features. It proved vulnerable to keystroke and screen logging, which can be seen here:

	16/05/2021 14:50:17	notepad++.exe	C:\Users\Player\Desktop\	q
	16/05/2021 14:50:34	notepad++.exe	*C:\Users\Player\Desktop	e r t y u i o p l k j h f d s z x c v b n m
	16/05/2021 14:50:55	msedge.exe	New tab - Profile 1 - Micro	a z s w e d v f r t g b n h y u j m k i o p l

Figure 30 Keystrokes Recorded from Comfort On-Screen Keyboard-Lite

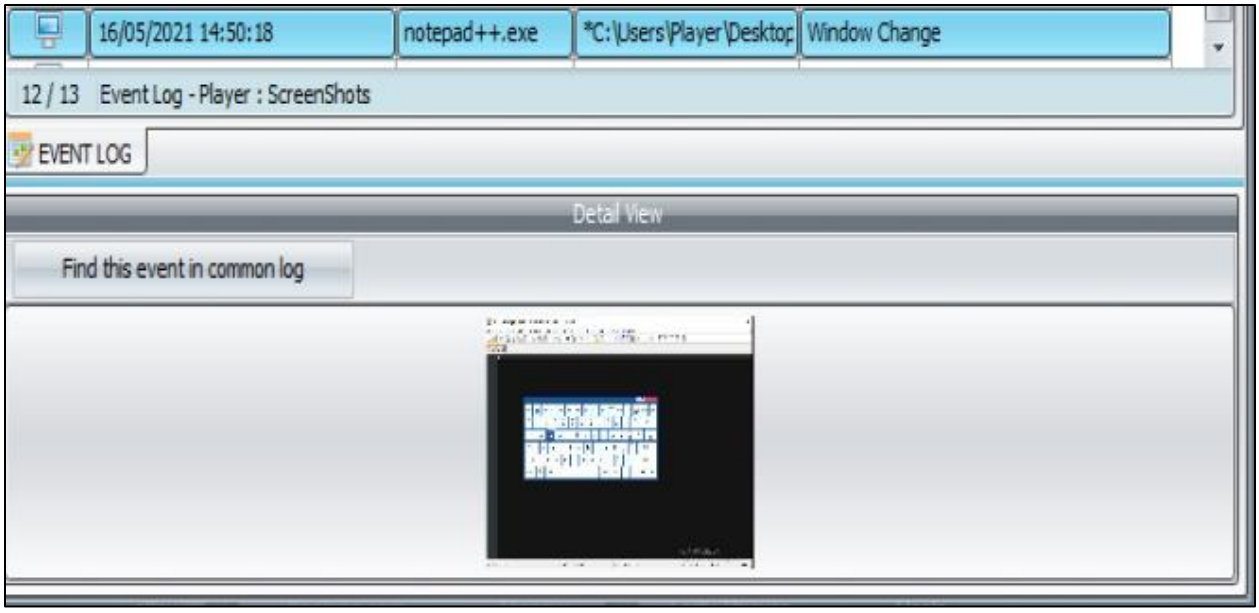

Figure 31 Evidence of Key Press within Screenshot

The full image seen in Figure 31 can be viewed in Appendix A Figure 1-4.

2.5.5 Touch-It Virtual Keyboard

Surpisingly, this application managed to defend against Spyrix (Spyrix Free Keylogger, 2021) keystroke and screengrab features. Due to the nature of the keyboard, it was hard to tell from the screen grab if a key was pressed and no data was recorded from the keystrokes that were pressed. The usage of this keyboard against Spyrix can be seen in Appendix Figure 1-5 and 1-6.

2.5.6 Neo's SafeKeys

Like Touch-It Virtual Keyboard, this keyboard was also successful in protecting against Spyrix Keylogger (Spyrix Free Keylogger, 2021). The usage of Neo's Safekeys can be seen in Appendix A Figures 1-7, 1-8 and 1-9.

2.5.7 Hot Virtual Keyboard

This was not able to defend against keystroke and screen logging:

	16/05/2021 15:29:20	notepad++.exe	*C:\Users\Player\Desktop	e 5 s s 8 <Caps Lock> <Caps Lock>
	16/05/2021 15:29:28	notepad++.exe	*C:\Users\Player\Desktop	c b k u
	16/05/2021 15:29:37	msedge.exe	New tab - Profile 1 - Micro	q e l] g m . p o j x \ a e 5

Figure 32 Data Captured from Hot Virtual Keyboard using Spyrix

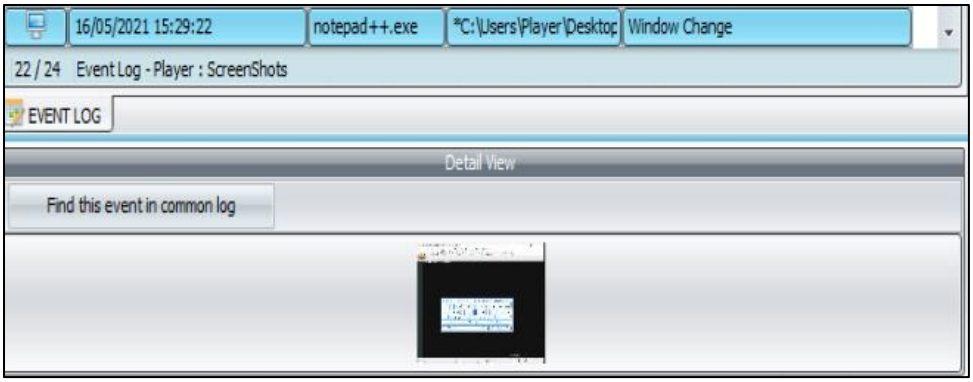

Figure 33 Evidence of Screenshot showing Hot Virtual Keyboard

Key presses were also be able to be distinguished easily due to the change in colour. The full image seen in Figure 33 can be seen can be viewed in Appendix A Figure 1-10.

2.6 ACTUAL KEYLOGGER

2.6.1 Summary

Table 4 Keystroke Logging Results using Actual Keylogger

	Free Virtual Keyboard	Microsoft On-Screen Keyboard	Comfort On-Screen Keyboard Lite	Touch-It Virtual Keyboard	Neo's Safekeys	Hot Virtual Keyboard
Actual Keylogger						

Table 5 Screen Logging Results using Actual Keylogger

	Free Virtual Keyboard	Microsoft On-Screen Keyboard	Comfort On-Screen Keyboard Lite	Touch-It Virtual Keyboard	Neo's Safekeys	Hot Virtual Keyboard
Actual Keylogger						

Tables 4 and 5 show the results of how successful Actual Keylogger (Actual Keylogger, n.d.) was against circumventing virtual keyboards. It was able to overcome multiple virtual keyboards, although there was one instance where data from Touch-It Virtual Keyboard was not all recorded, showing that it was not as effective compared to other results in this test. It was of note that the program was able to detect Neo's Safekeys using the Hidden Mouse and Hover Entry Mode, so this was changed to hover entry mode so each time a key was wanting to be pressed the mouse would hover over it. The usage of Actual Keylogger (Actual Keylogger, n.d.) against the virtual keyboards can be seen in Appendix A Figures 1-11 – 1-22.

2.7 REFOG PERSONAL MONITOR

2.7.1 Summary

Table 6 Keystroke Logging Results using Refog Personal Monitor

	Free Virtual Keyboard	Microsoft On-Screen Keyboard	Comfort On-Screen Keyboard Lite	Touch-It Virtual Keyboard	Neo's Safekeys	Hot Virtual Keyboard
Refog Personal Monitor						

Table 7 Screen Logging Results using Refog Personal Monitor

	Free Virtual Keyboard	Microsoft On-Screen Keyboard	Comfort On-Screen Keyboard Lite	Touch-It Virtual Keyboard	Neo's Safekeys	Hot Virtual Keyboard
Refog Personal Monitor						

Tables 6 and 7 show the results of using Refog Personal Monitor (Refog Personal Monitor, n.d.) against the virtual keyboards. It was able to record keystrokes from nearly every virtual keyboard, although was unable to record pressed keys using the screengrab feature. The usage of Refog Personal Monitor (Refog Personal Monitor, n.d.) against the virtual keyboards can be seen in Appendix A Figures 1-23 – 1-29.

2.8 IWANTSOFT KEYLOGGER

2.8.1 Summary

Table 8 Keystroke Logging Results using Iwantsoft Keylogger

	Free Virtual Keyboard	Microsoft On-Screen Keyboard	Comfort On-Screen Keyboard Lite	Touch-It Virtual Keyboard	Neo's Safekeys	Hot Virtual Keyboard
Iwantsoft Keylogger						

Table 8 showed the results of Iwantsoft Keylogger (Iwantsoft Keylogger, n.d.) against the virtual keyboards. It was able to record keystrokes entered from some virtual keyboards but this keylogger was unreliable as data was not immediately recognised. Only when data was deleted did this manage to appear within the logs shown in Iwantsoft. The usage of Iwantsoft Keylogger against the virtual keyboards can be seen in Appendix A Figures 1-30 – 1-34.

2.9 REVEALER KEYLOGGER

2.9.1 Summary

Table 9 Keystroke Logging Results using Revealer Keylogger

	Free Virtual Keyboard	Microsoft On-Screen Keyboard	Comfort On-Screen Keyboard Lite	Touch-It Virtual Keyboard	Neo's Safekeys	Hot Virtual Keyboard
Revealer Keylogger						

Table 9 showed the results of Revealer Keylogger (Revealer Keylogger Free, 2021) against the virtual keyboards. It was able to record keystrokes from nearly every keyboard, with the exception being Neo's SafeKeys. The usage of Revealer Keylogger can be seen in Appendix A Figures 1-35 – 1-39.

2.10 KIDLOGGER

2.10.1 Summary

Table 10 Keystroke Logging Results using KidLogger

	Free Virtual Keyboard	Microsoft On-Screen Keyboard	Comfort On-Screen Keyboard Lite	Touch-It Virtual Keyboard	Neo's Safekeys	Hot Virtual Keyboard
KidLogger						

Table 11 Screen Logging Results using KidLogger

	Free Virtual Keyboard	Microsoft On-Screen Keyboard	Comfort On-Screen Keyboard Lite	Touch-It Virtual Keyboard	Neo's Safekeys	Hot Virtual Keyboard
KidLogger						

Tables 10 and 11 showed the results of the use of KidLogger (KidLogger, n.d.) against the virtual keyboards. It was successful against some virtual keyboards, although failed to capture pressed keys using its screenshot feature. The usage of KidLogger against virtual keyboards can be seen in Appendix A Figures 1-40 – 1-49.

2.11 BEST FREE KEYLOGGER

2.11.1 Summary

Table 12 Results of Keystroke Logging using Best Free Keylogger

	Free Virtual Keyboard	Microsoft On-Screen Keyboard	Comfort On-Screen Keyboard Lite	Touch-It Virtual Keyboard	Neo's Safekeys	Hot Virtual Keyboard
Best Free Keylogger						

Table 12 showed the results of the use of Best Free Keylogger (Best Free Keylogger, n.d.) against the virtual keyboards. It had very similar results to KidLogger (KidLogger, n.d.) and was able to capture data from most keyboards. Even though the professional trial version was installed, the screenshot testing was too unreliable as screenshots were not being recorded by the application, so this was ignored. The usage of Best Free Keylogger can be seen in Appendix A Figures 1-50 – 1-53.

3 RESULTS

3.1 RESULTS FOR KEYSTROKE LOGGING

Table 13 Results of Keystroke Logging against Virtual Keyboards

	Free Virtual Keyboard	Microsoft On-Screen Keyboard	Comfort On-Screen Keyboard Lite	Touch-It Virtual Keyboard	Neo's Safekeys	Hot Virtual Keyboard
Spyrix Free Keylogger						
Actual Keylogger						
Refog Personal Monitor						
Iwantsoft Free Keylogger						
Revealer Keylogger						
KidLogger						
Best Free Keylogger						

Table 13 shows the overall results of testing done on each virtual keyboard with the keylogger software. There were noticeable results, including the failed attempts to capture data from Neo's SafeKeys. There were also some results that showed that the keylogger had managed to capture some data from the keyboard, although not all individual data.

3.2 RESULTS FOR SCREEN LOGGING

Table 14 Results of Screen Logging against Virtual Keyboards

	Free Virtual Keyboard	Microsoft On-Screen Keyboard	Comfort On-Screen Keyboard Lite	Touch-It Virtual Keyboard	Neo's SafeKeys	Hot Virtual Keyboard
Spyrix Free Keylogger						
Actual Keylogger						
Refog Personal Monitor						
KidLogger						

Table 14 shows the results of the screen logging tests, which highlighted Refog Personal Monitor had the weakest screenshot feature due to its unreliability. Neo's SafeKeys was able to defend against the keyloggers due to its secure configuration settings that allowed for multiple methods of entering data, which was also protected on screen using asterisks.

4 DISCUSSION

4.1 GENERAL DISCUSSION

In 2017, Raymond.cc investigated the security of virtual keyboards. They found that Microsoft On-Screen Keyboard was able to be easily defeated by twelve of the most popular commercial paid keylogger available at the time. Within this investigation, Microsoft On-Screen Keyboard also proved to be one of the most vulnerable to keylogger software, both in keystroke and screen logging tests. This could easily have been fixed however could be modified within the settings to stop highlighting individual key presses. This could have provided sufficient protection against screen logging. There was no protection at all against keystroke logging, making this one of the most insecure programs alongside Free Virtual Keyboard and Hot Virtual Keyboard. These two virtual keyboards were clearly designed for accessibility, rather than for security purposes. There were a couple of instances within testing where keyloggers were able to record some data from key presses. One instance of this was where Touch-It Virtual Keyboard was tested against Actual Keylogger and Iwantsoft Keylogger. It was clear from this that although the keylogger was able to extract data from keystrokes, it was unreliable. On the other hand, this still makes Touch-It Virtual Keyboard unreliable in its protection against keylogger software.

The most secure virtual keyboard found during testing was Neo's SafeKeys, which was designed for security purposes. Its use of the drag and drop method protected against keystroke logging, with its additional features for data protection protecting against screen logging. This made it an excellent countermeasure to keylogger software. The testing that Raymond.cc conducted showed that Neo's drag and drop method was very safe and no data was leaked from keystrokes, which also proved to be the same in this testing. Although Refog Keylogger didn't have very strong screen logging features, it made up for this in its keystroke capturing capacity as it was able to capture data from nearly every keyboard, making it one of the most effective for its keylogger features alongside Revealer Keylogger and KidLogger. Iwantsoft Keylogger proved to be one of the most difficult software keyloggers to test as many of the keyboards that were tested had keystrokes recorded from them but not all data was captured, making this keylogger unreliable in keystroke capturing. It was also of note that Touch-It Virtual Keyboard and Neo's SafeKeys were able to defend against screen logging in all screenshot tests. The user interface for Touch-It Virtual Keyboard made it difficult to effectively analyse if a key had been pressed within the application. The quality of the screenshots within the applications made it difficult to pinpoint. In addition, Neo's SafeKeys was found to be very secure against screenlogging. When data was entered, this was hidden by asterisks meaning that even keystroke logging would not be able to view this data and screenshots would show the obfuscated data. Actual Keylogger was able to show pressed keys in Neo's SafeKeys for one test, although the use of the hover mode as part of the mouse mode settings was able to pass undetected through the screenshot feature as individual keys that would be pressed would need to be hovered over for five seconds, which in combination with the hidden mouse feature, meant that no important screenshot data was obtained. This reinforced that Neo's SafeKeys was the most secure virtual keyboard that failed tests against the keylogger software. It would be hard to come to a conclusion on the most effective keylogger as these results varied from each tool.

Another abnormality was within Hot Virtual Keyboard where tests conducted against Actual Keylogger and Iwantsoft Keylogger where not all data was being recorded to the keylogger. There were some instances with Iwantsoft Keylogger where the software functioned incorrectly as when data was entered through the virtual keyboards it initially did not appear in the logs, although when it was deleted this immediately appeared. This made it unreliable for most of the testing for screenshot capture. If virtual keyboards should be used for keylogger protection, careful consideration should be taken into the choice of the keyboard. The virtual keyboard should be incorporated with security features such as Neo's SafeKeys, as others were unsuccessful against keylogger software and thus these were able to circumvent the safety of virtual keyboards.

4.2 COUNTERMEASURES (FOR A PROJECT IN ETHICAL HACKING)

The results of the investigation showed that the keyloggers that were used to conduct testing were obsolete against Neo's SafeKeys. Since it had multiple configuration options, it was able to defend against keyloggers using multiple methods. It was unique in that the drag and drop method was able to circumvent all keyloggers used, while other keyboards entered data using key presses.

Additional countermeasures that would severely disrupt the effectiveness of keylogger software include anti-keylogger software such as SpyShelter (SpyShelter - Anti Keylogger, n.d.) which can notify users if any keylogger captures any actions. Another anti-keylogger software that could be used is KeyScrambler (KeyScrambler, 2021). Any data such as keyboard strokes can be fed through KeyScrambler which encrypts data and is sent to the keylogger.

4.3 CONCLUSIONS

Overall, virtual keyboards can be easily circumvented by keylogger software and is not a reliable protection method against such malware. They should not be used to protect against keyloggers unless there are security settings incorporated into them. Neo's SafeKeys is a suitable method of protecting data when it is entered through the keyboard, making it the most viable virtual keyboard. Spyrix Keylogger, Actual Keylogger and KidLogger proved to be the most successful in screen logging against the virtual keyboards, making these keyloggers have the most effective screen logging features. Refog Personal Monitor and Revealer Keylogger proved to be the most successful, however, in capturing keystrokes from the virtual keyboards, making these the most effective against normal keystroke logging.

4.4 FUTURE WORK

With a greater amount of time available, the investigation would have incorporated more tools that would have been used to gain a better insight into the efficacy of keylogger software against virtual keyboards. Examples of virtual keyboards that could have been included in this investigation were On-Screen Keyboard Portable, Click-N-Type, Oxynger KeyShield, Mouse Only Keyboard and Anti-Keylogger Virtual Keyboard. Some antivirus software like Kaspersky, eScan and Panda come with virtual keyboards, so the investigation could have been expanded to include these. Other software keyloggers could also

have been used such as Windows Keylogger, KidInspector, Ardamax Keylogger, Basic Key Logger and BlackBox Express. Since there was an issue with Best Free Keylogger screenshot features, this could be improved in the future to include these tests to show if it was successful against virtual keyboards. Hardware keyloggers could also have been employed within this investigation, however in the future the testing could look at investigating popular hardware keyloggers and testing their efficiency against virtual keyboards. Research could also look at creating a software keylogger and testing how successful this is with other popular tools. In addition, research could also investigate the efficacy of software and hardware keyloggers against anti-virus software. Rather than looking to minimise data leakage using virtual keyboards when a keylogger is installed on a machine, the investigation could expand to evaluating the success rate at which anti-virus software is able to prevent keylogger tools from executing.

4.5 CALL TO ACTION

The results of this investigation showed that keylogger software was able to circumvent most virtual keyboards. Should any further information be required, this can be provided using the following details seen below.

Contact details:

01456 519 498

pen_testered@gmail.com

REFERENCES

www.kaspersky.co.uk. n.d. *What is Keystroke Logging and Keyloggers?*. [online] Available at: <https://www.kaspersky.co.uk/resource-center/definitions/keylogger> [Accessed 3 March 2021].

Mohanty, A., 2020. *How Dangerous Are Keyloggers?* | *TechEntice*. [online] My Windows Hub. Available at: <https://mywindowshub.com/how-dangerous-are-keyloggers/> [Accessed 2 March 2021].

Sagiroglu, S. and Canbek, G., 2009. *Keyloggers Increasing Threats to Computer Security and Privacy*. Ankara, pp.11, 12.

Humphries, M., 2017. *Keylogger Discovered on HP Laptops*. [online] PCMAG. Available at: <https://www.pcmag.com/news/keylogger-discovered-on-hp-laptops> [Accessed 1 March 2021].

Waterson, D., 2020. *How keyloggers work and how to defeat them*. [online] Bcs.org. Available at:<https://www.bcs.org/content-hub/how-keyloggers-work-and-how-to-defeat-them/> [Accessed 1 March 2021].

Author, G., 2015. *Is your antivirus software protecting you against keyloggers?*. [online] StickyPassword.com. Available at: <https://www.stickypassword.com/blog/is-your-antivirus-software-protecting-you-against-keyloggers-3083> [Accessed 4 March 2021].

Bhardwaj, A. and Goundar, S., 2020. Keyloggers: silent cyber security weapons. *Network Security*, 2020(2), pp.14-19.

2015. *Free Virtual Keyboard*. Ellensburg: Media Freeware.

2007. *On-Screen Keyboard Portable*. N/A: PortableApps.

2020. *Touch-It Virtual Keyboard*. Chessware.

n.d. *Neo's SafeKeys*. Aplin Software.

2021. *Hot Virtual Keyboard*. Vancouver: Comfort Software.

2021. *Spyrix Free Keylogger*. California: Spyrix Inc.

n.d. *Actual Keylogger*. N/A: Actual Keylogger.

n.d. *Refog Personal Monitor*. Unknown: Refog.

n.d. *Iwantsoft Free Keylogger*. N/A: IWANTSOFT.

2021. *Revealer Keylogger Free*. France: Logixoft.

2021. *KidLogger*. Moldova: Rohos Software.

n.d. *Best Keylogger Pro*. N/A: BESTX SOFTWARE.

n.d. *SpyShelter - Anti Keylogger*. Unknown: SpyShelter.

n.d. *KeyScrambler*. Unknown: QFX Software.

BIBLIOGRAPHY

Sagiroglu, S. and Canbek, G., 2009. *Keyloggers Increasing Threats to Computer Security and Privacy*. [online] N/A. Available at: <https://www.researchgate.net/publication/224591822_Keyloggers_Increasing_Threats_to_Computer_Security_and_Privacy> [Accessed 1 March 2021]

Dadkhah, M. and Jazi, M., 2014. A Novel Approach to Deal With Keyloggers. *Oriental Journal of Computer Science & Technology*, 7(1), p.25-28.

Raymond.cc. n.d.. *5 Virtual Keyboards Tested to Determine their Effectiveness Against Keyloggers*. [online] Available at: <https://www.raymond.cc/blog/how-to-beat-keyloggers-to-protect-your-identity/> [Accessed 2 March 2021].

Paterson, J., 2017. *Top 10 Free Keyloggers for Windows 2021*. [online] Medium. Available at: <https://janetcpatterson.medium.com/top-10-free-keyloggers-for-windows-a2a6b7f9130> [Accessed 2 March 2021].

Subramanyam, K., Frank, C. and Galli, D., n.d. *Keyloggers: The Overlooked Threat to Computer Security*. [online] Thevespiary.org. Available at: <http://www.thevespiary.org/rhodium/Rhodium/Vespiary/talk/files/911-Keyloggers0283.pdf> [Accessed 18 May 2021].

Riddhi, S., 2017. *Top 8 Best Free On Screen Virtual Keyboards for windows*. [online] Thegeekpage.com. Available at: <https://thegeekpage.com/free-on-screen-virtual-keyboards/> [Accessed 2 March 2021].

APPENDICES

APPENDIX A – PRACTICAL

Spyrix Keylogger:

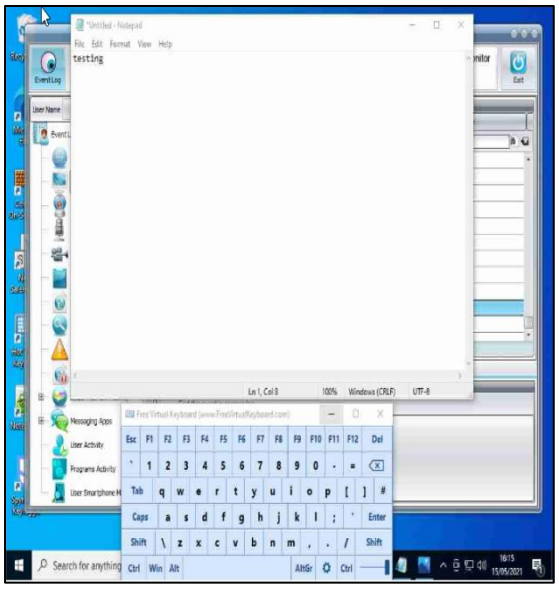

Figure 1-1 Screenshot Obtained via Spyrix in Full Screen

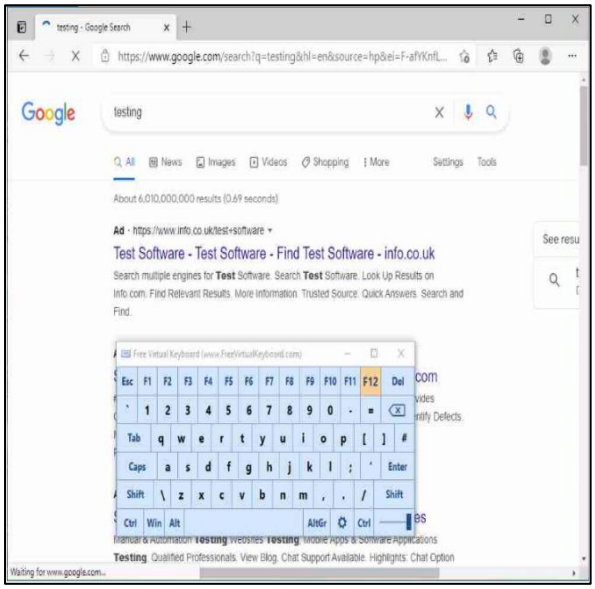

Figure 1-2 Keystrokes Presses Captured from Free Virtual Keyboard

Figure 1-3 Record of Pressed Key from Spyrix

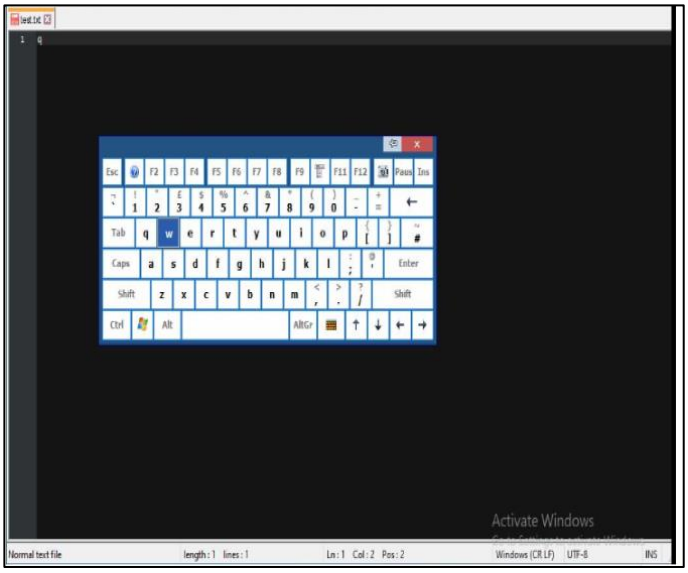

Figure 1-4 Key Press recorded from Spyrix using Comfort On-Screen Keyboard Lite

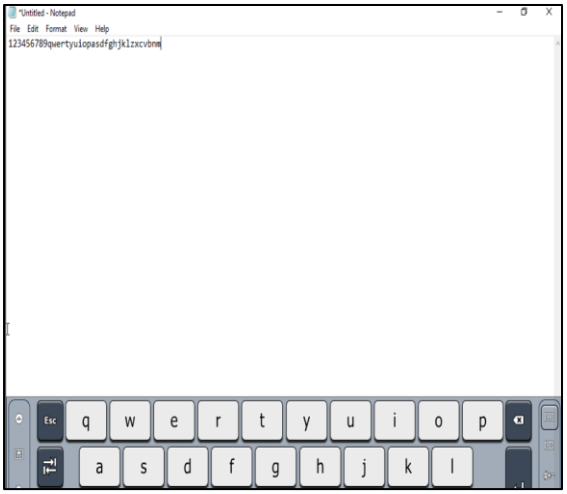

Figure 1-5 Entering Data via Touch-It Virtual Keyboard into Notepad

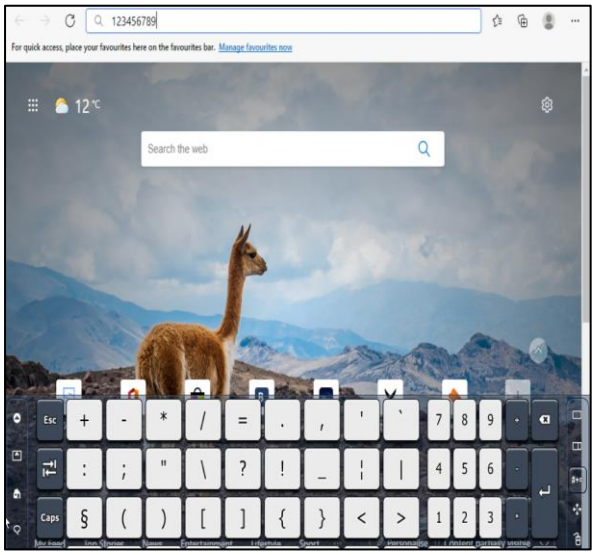

Figure 1-6 Entering Data via Touch-It Virtual Keyboard into Browser

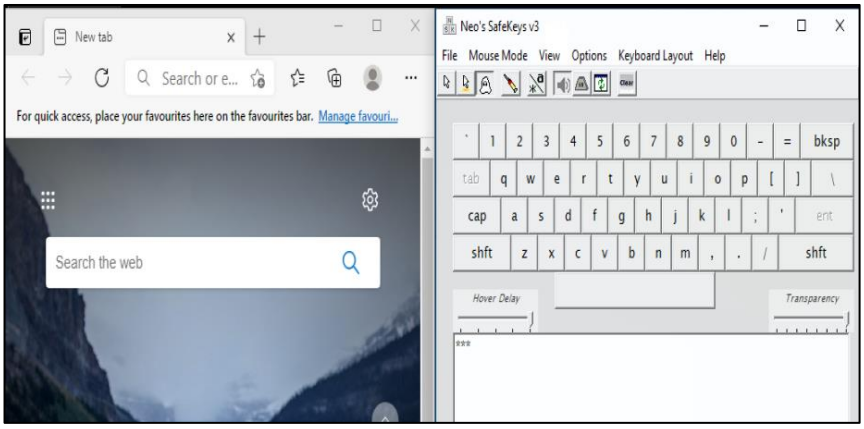

Figure 1-7 Using Neo's SafeKeys

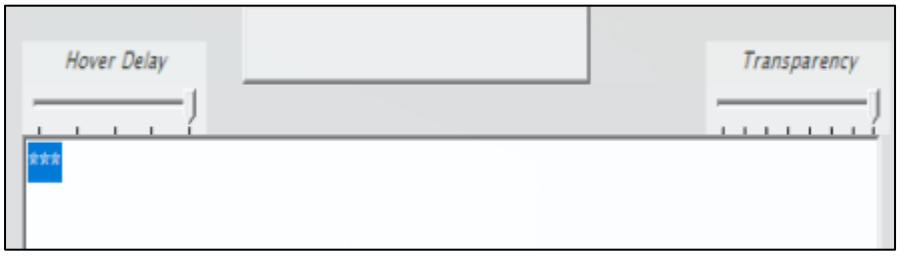

Figure 1-8 Data Represented by Asterisk Symbols

Figure 1-9 Neo's Drag and Drop Mode

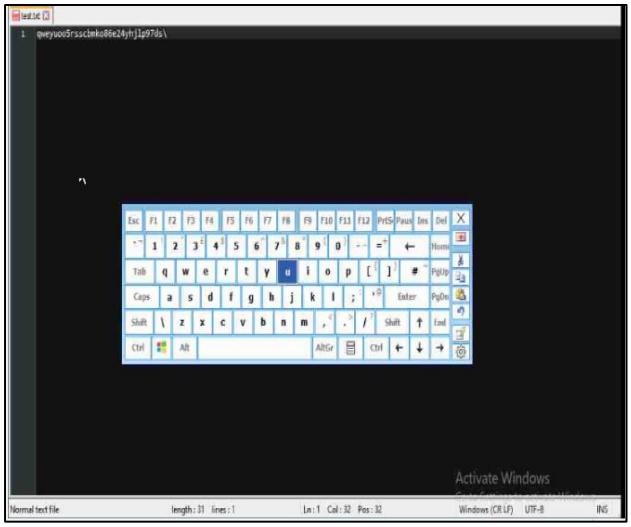

Figure 1-10 Captured Pressed Keys using Spyrix

Actual Keylogger:

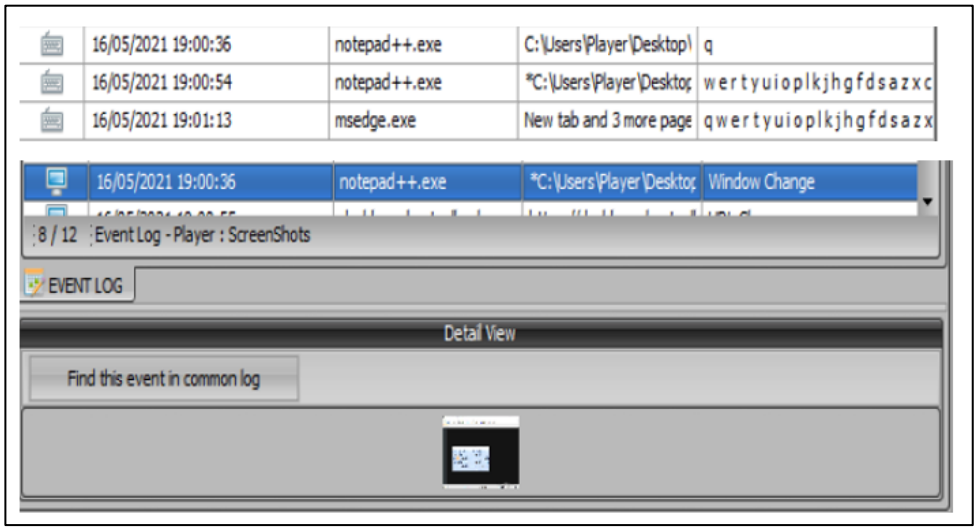

Figure 1-11 Free Virtual Keyboard Results

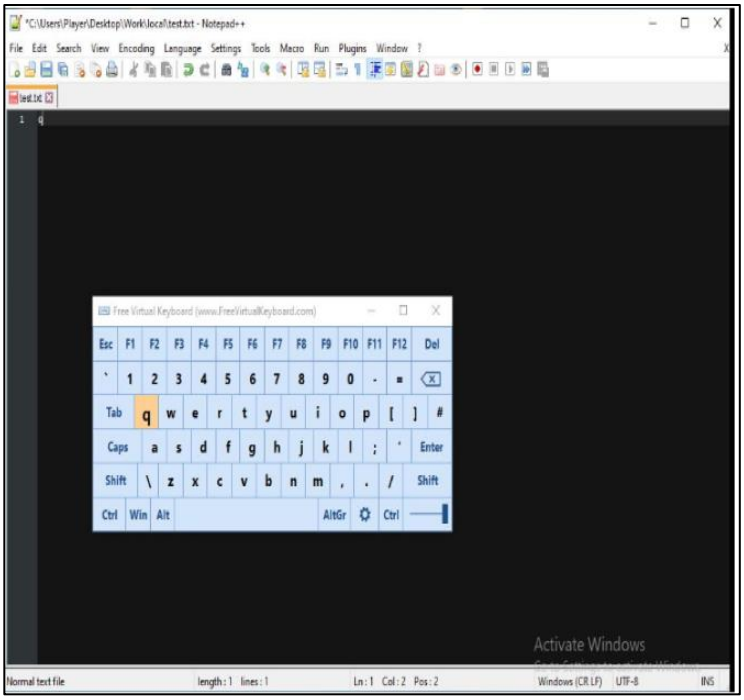

Figure 1-12 Capturing User's Pressed Keys from FVK

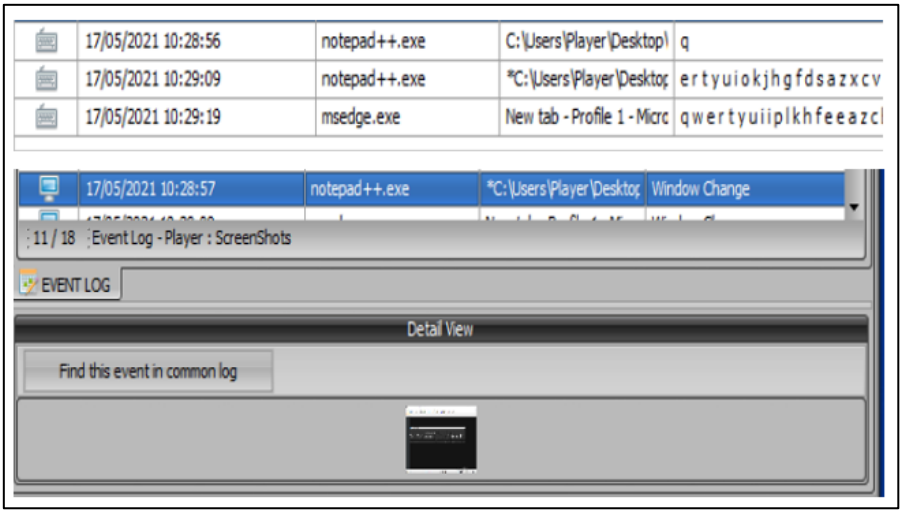

Figure 1-13 Windows On-Screen Keyboard Results

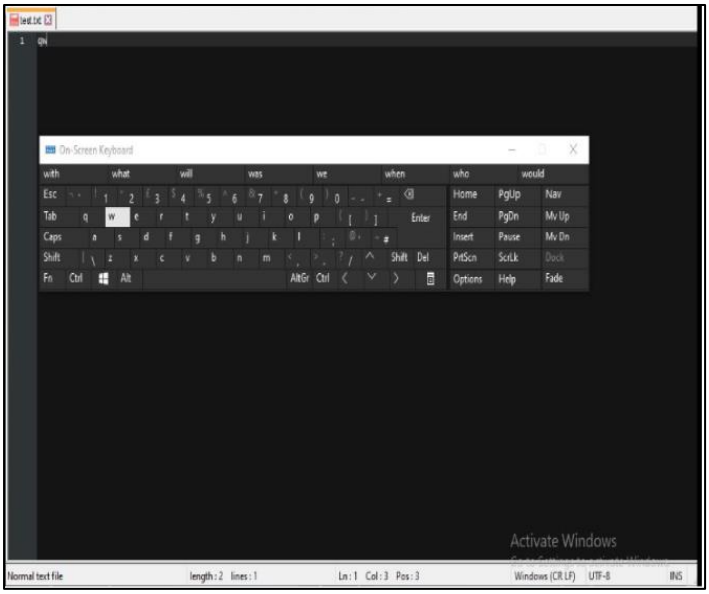

Figure 1-14 Capturing Pressed Keys from Windows On-Screen Keyboard

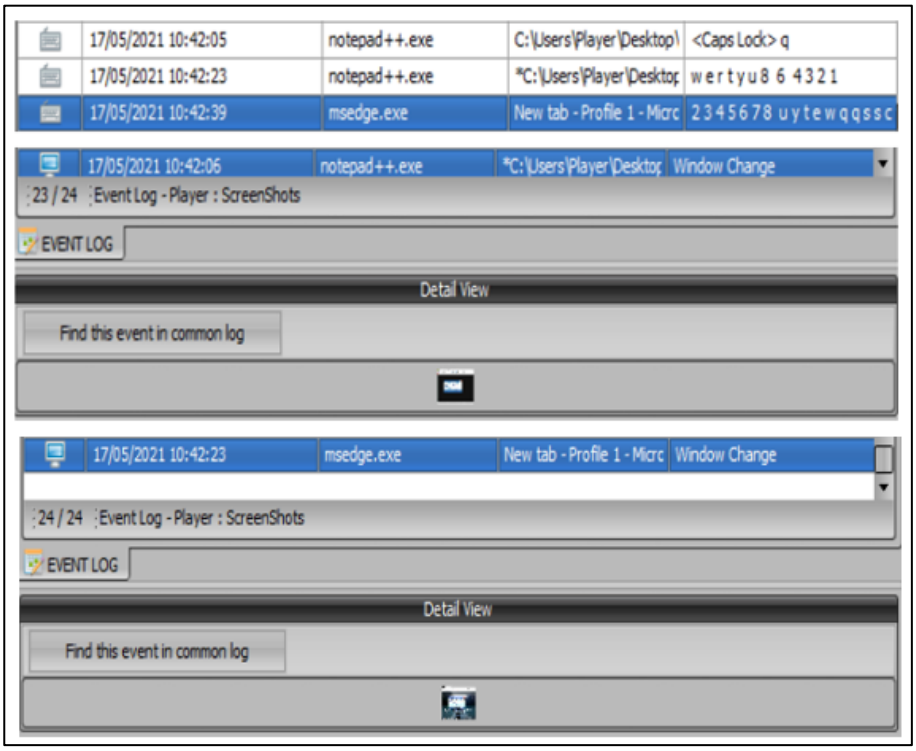

Figure 1-15 Comfort On-Screen Keyboard Lite Results

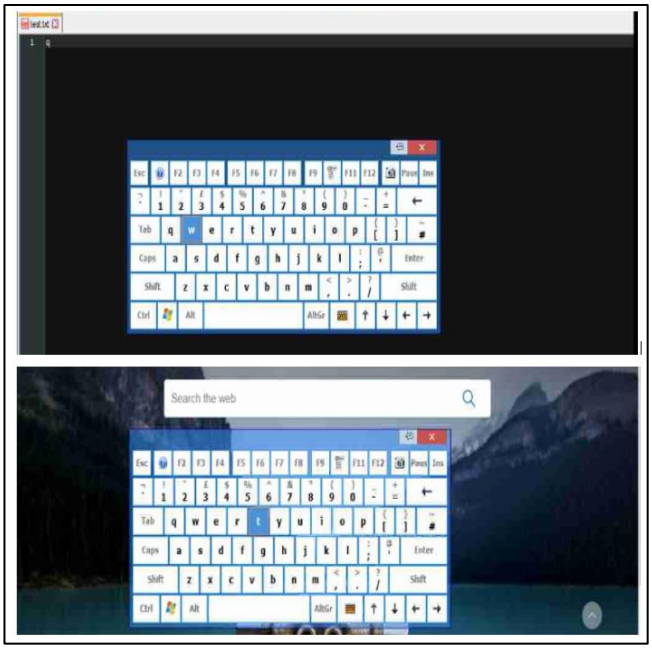

Figure 1-16 Capturing Pressed Keys from Comfort On-Screen Keyboard Lite

	17/05/2021 11:16:33	notepad++.exe	*C:\Users\Player\Desktop	a
	17/05/2021 11:47:07	msedge.exe	New tab - Profile 1 - Micro	2

Figure 1-17 Touch-It Virtual Keyboard Results

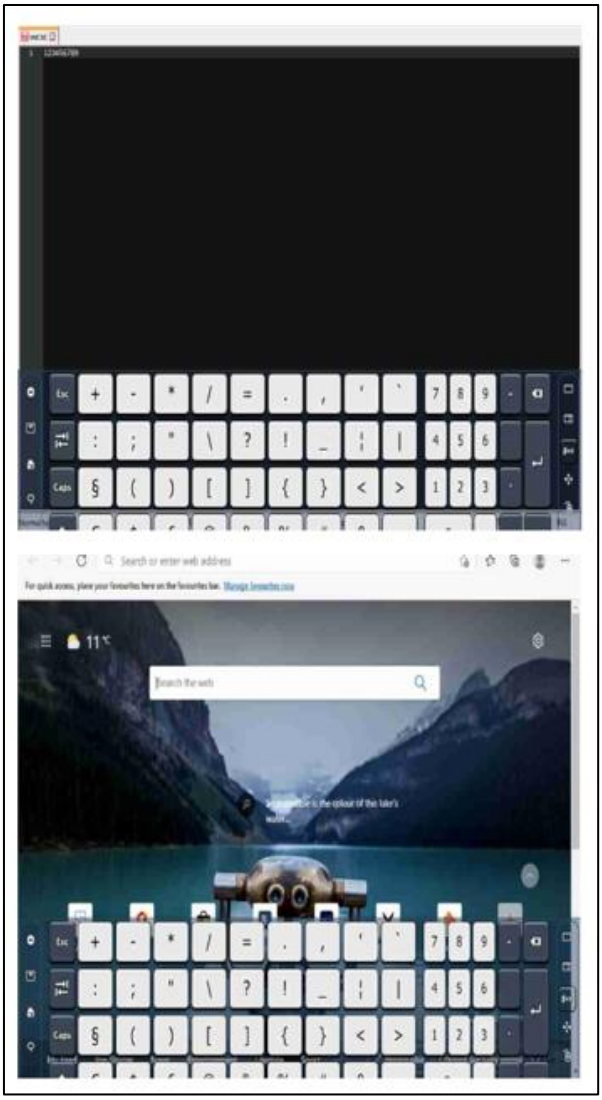

Figure 1-18 Usage of Touch-It Virtual Keyboard

Figure 1-19 Actual Keylogger showing pressed key within Neo's SafeKeys

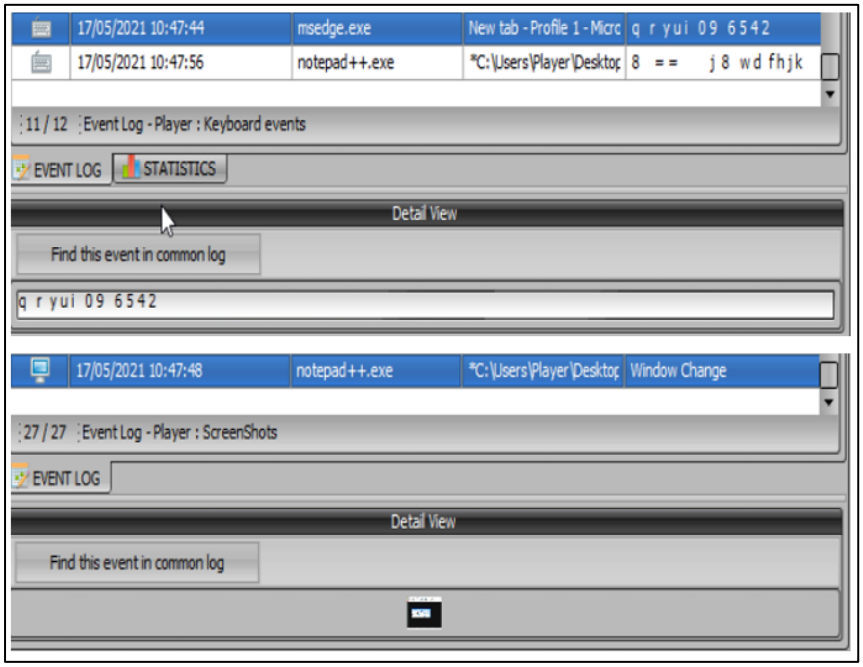

Figure 1-20 Hot Virtual Keyboard Results

Figure 1-21 Capturing Pressed Keys from Hot Virtual Keyboard

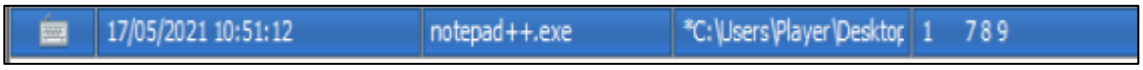

Figure 1-22 Abnormality with Hot Virtual Keyboard (Actual Keylogger)

Refog Personal Monitor:

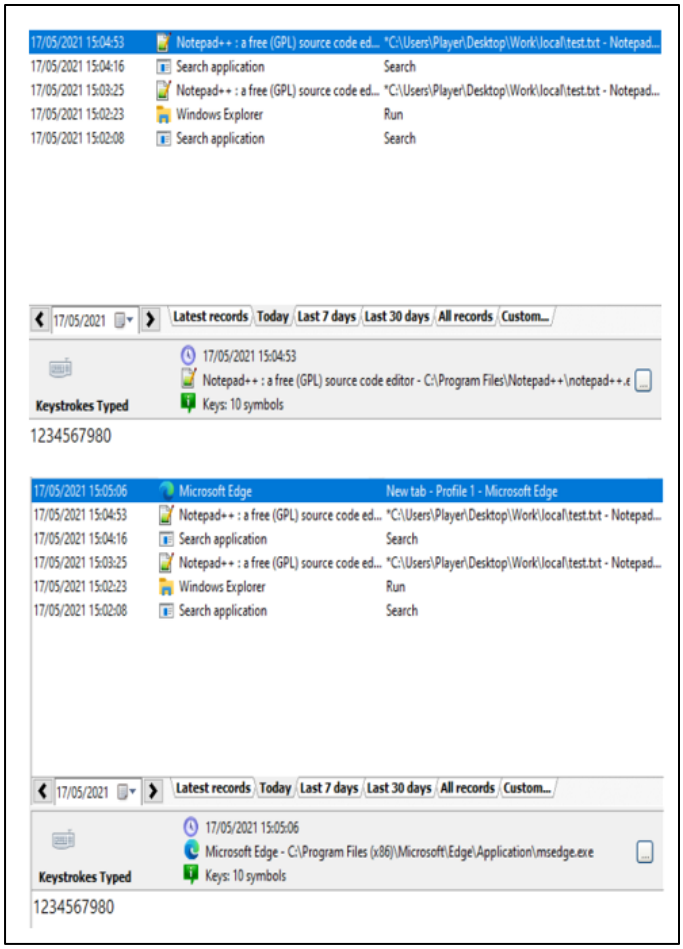

Figure 1-23 Free Virtual Keyboard Results (Keystrokes)

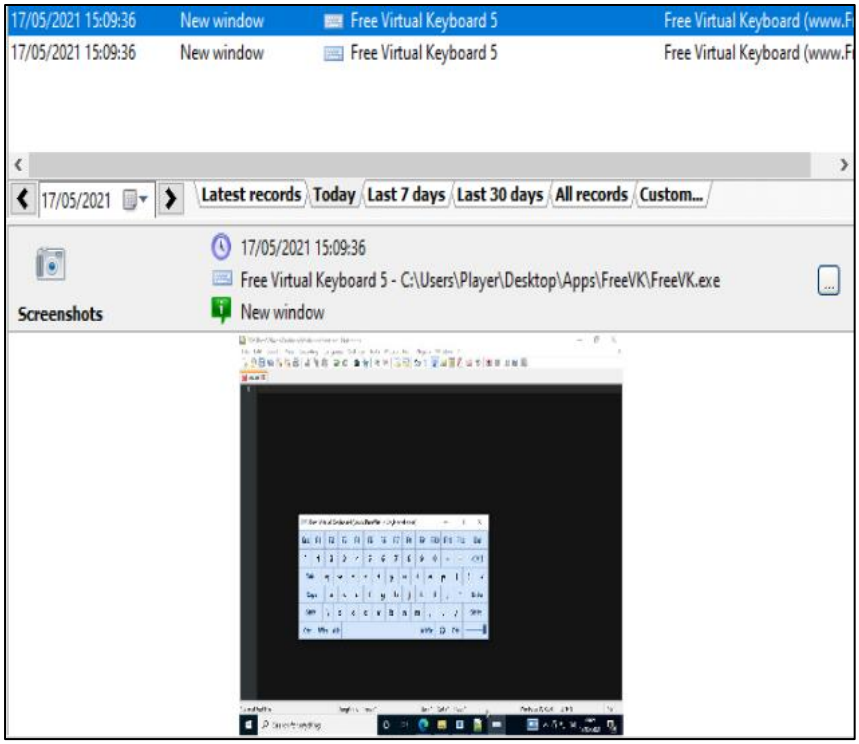

Figure 1-24 Unsuccessful Attempt at Screenshotting Free Virtual Keyboard

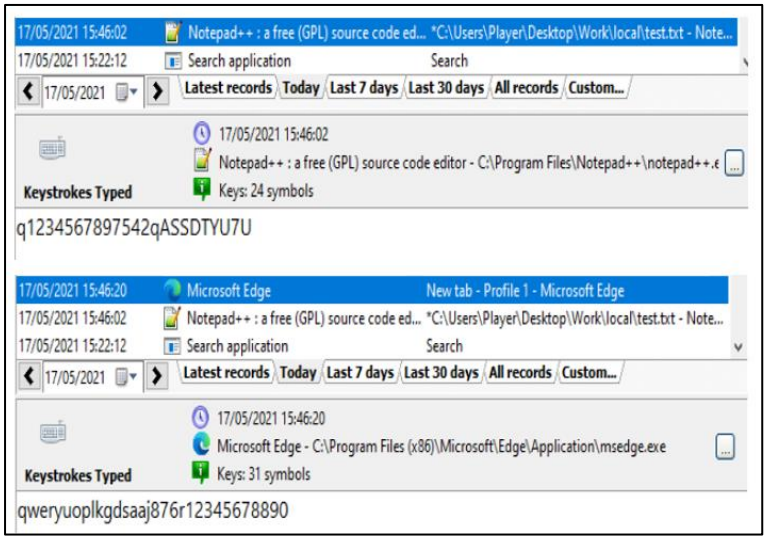

Figure 1-25 Microsoft On-Screen Keyboard Results (Keystrokes)

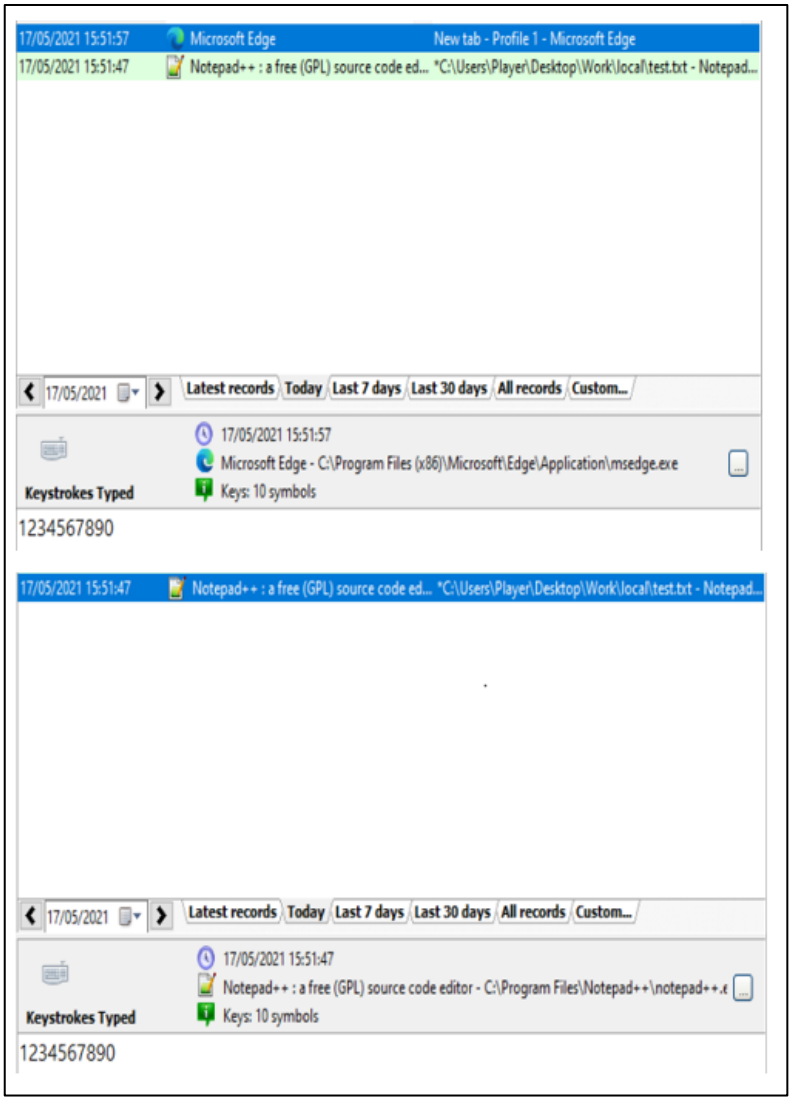

Figure 1-25 Comfort On-Screen Keyboard Lite Results (Keystrokes)

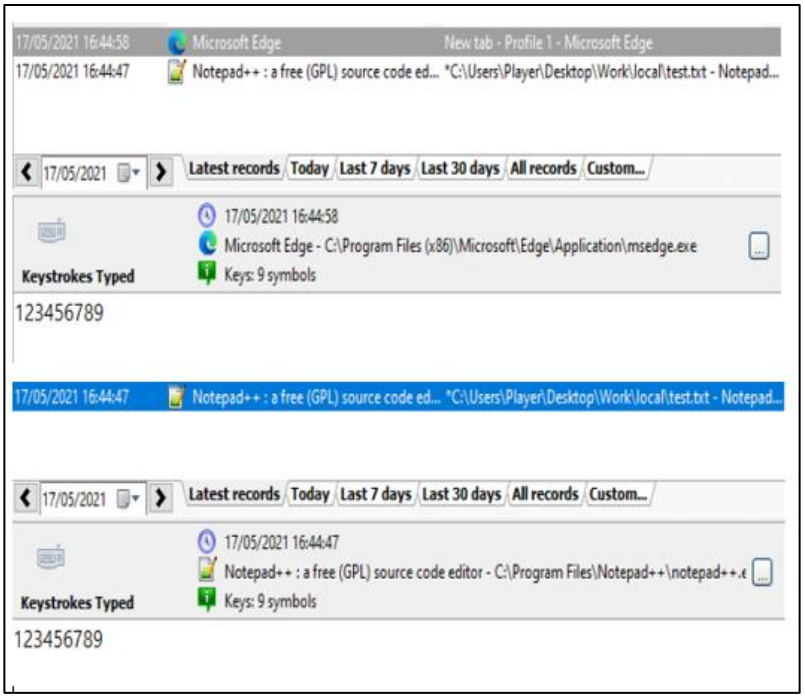

Figure 1-26 Touch-It Virtual Keyboard Results

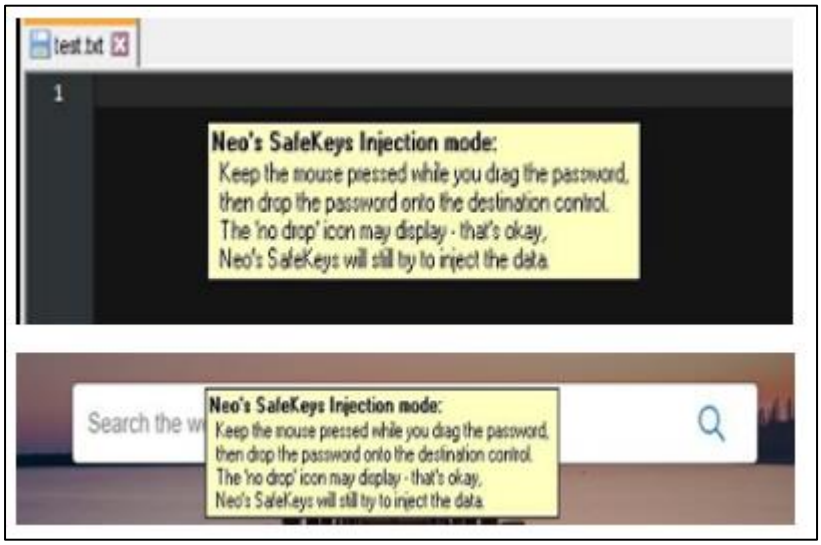

Figure 1-27 Neo's SafeKeys Usage

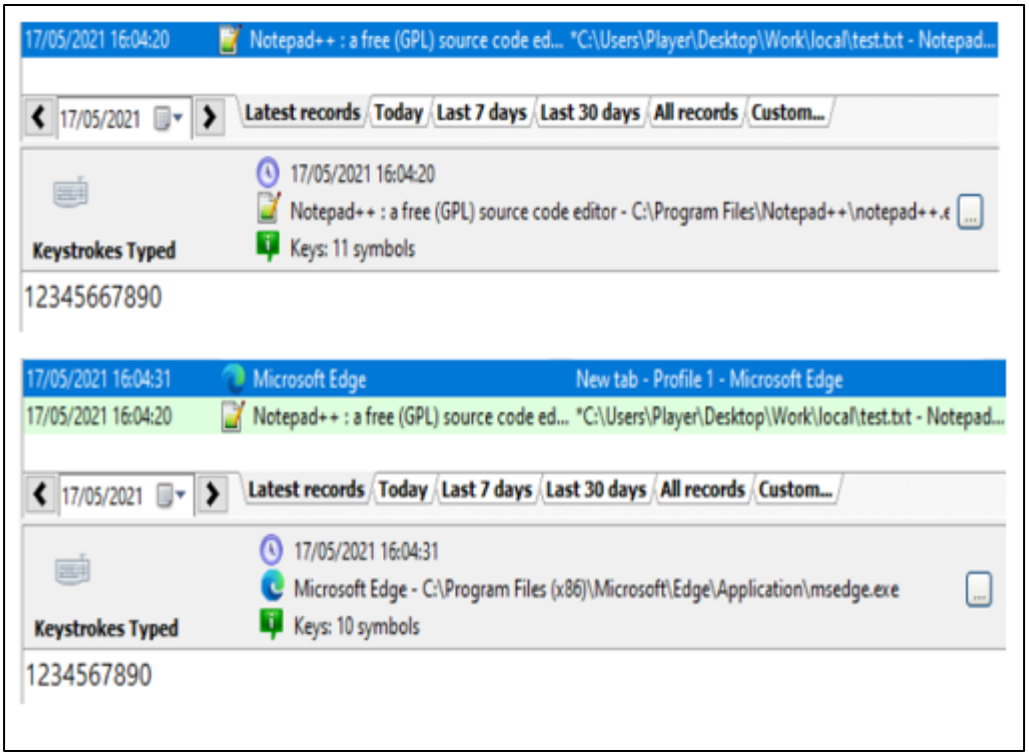

Figure 1-28 Hot Virtual Keyboard Results (Keystrokes)

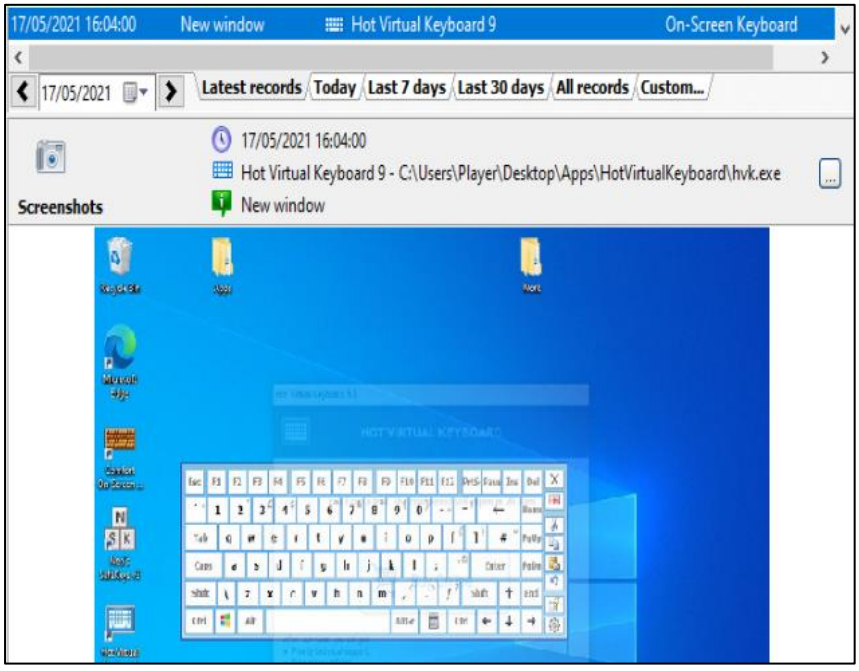

Figure 1-29 Unsuccessful Attempt to Screenshot Hot Virtual Keyboard

Iwantsoft Keylogger:

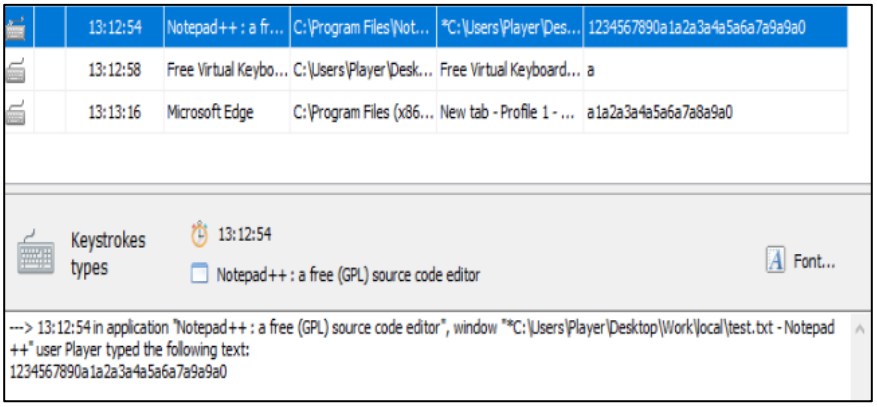

Figure 1-30 Results of Free Virtual Keyboard

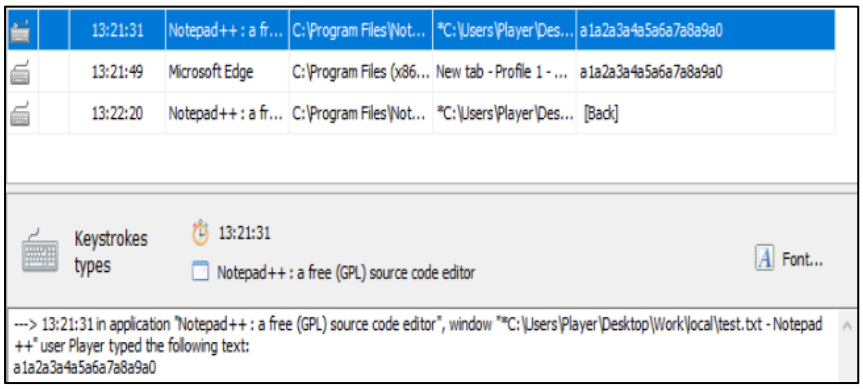

Figure 1-31 Results of Windows On-Screen Virtual Keyboard

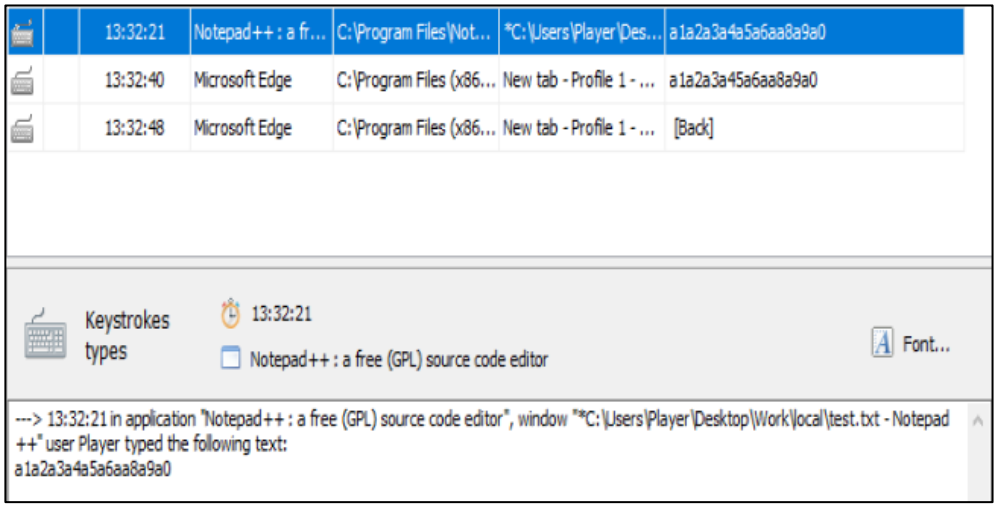

Figure 1-32 Results of Comfort On-Screen Virtual Keyboard Lite

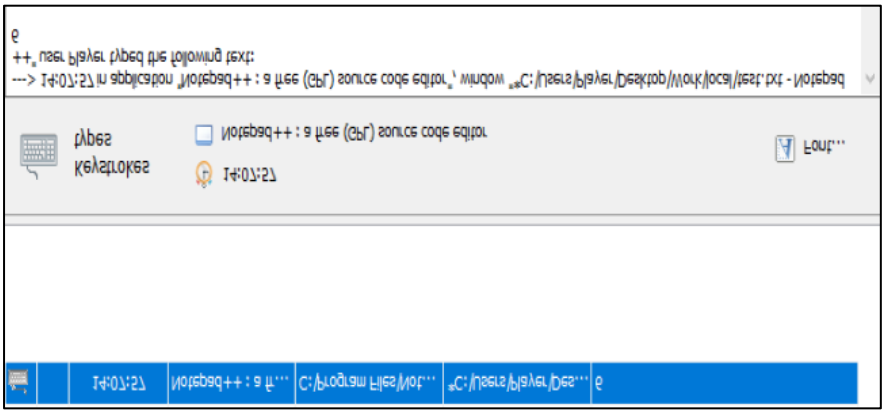

Figure 1-33 Results of Touch-It Virtual Keyboard

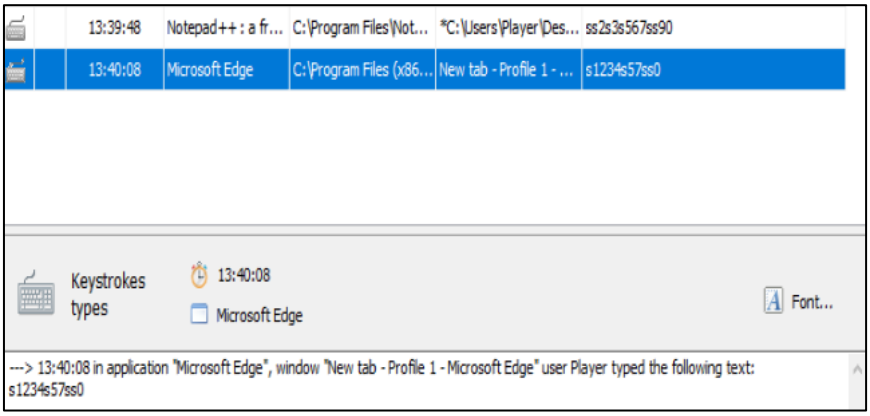

Figure 1-34 Results of Hot Virtual Keyboard

Revealer Keylogger:

Figure 1-35 Results of Free Virtual Keyboard

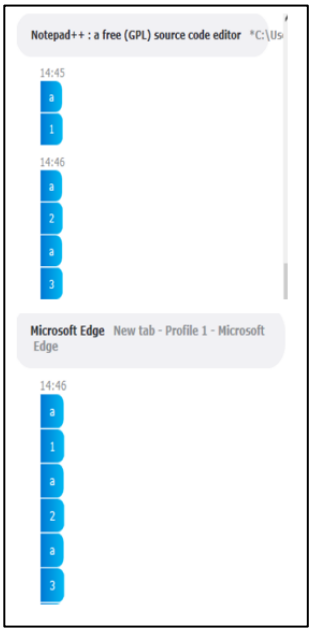

Figure 1-36 Results of Windows On-Screen Virtual Keyboard

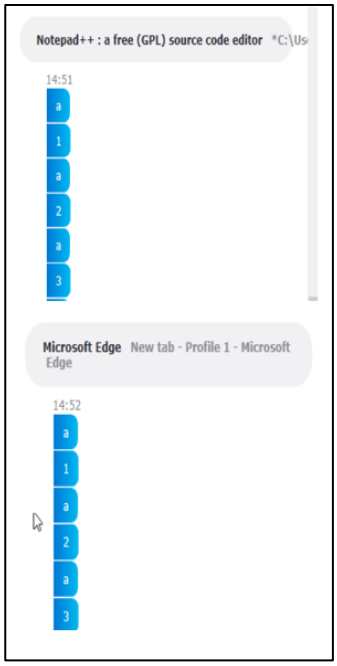

Figure 1-37 Results of Comfort On-Screen Virtual Keyboard

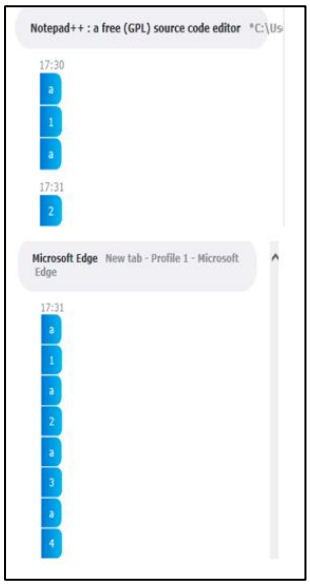

Figure 1-38 Results of Touch-It Virtual Keyboard

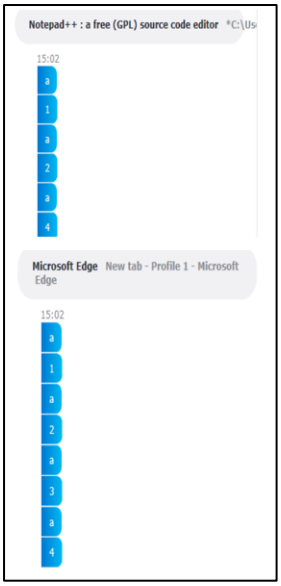

Figure 1-39 Results of Hot Virtual Keyboard

KidLogger:

Figure 1-40 Results of Free Virtual Keyboard

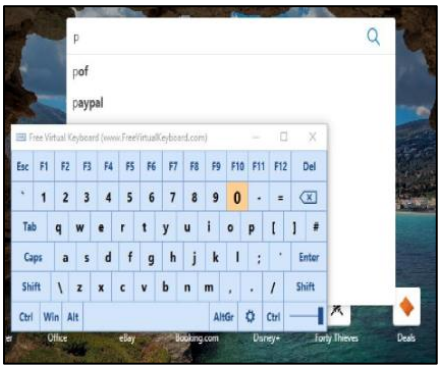

Figure 1-41 Captured Pressed Keys in Free Virtual Keyboard

p01p02p03p04p05p06p06p07p08p09p10

u1u12u3u4u5u6u7u8u9u0c1cwc2x3c4c6c7c9xw1x2x3x4x5x6x7x8x9x1

Figure 1-42 Results of Windows On-Screen Keyboard

Figure 1-43 Captured Pressed Keys in Windows On-Screen Keyboard

*C:\Users\Player\Desktop\Work\local\test.txt - Notepad++

a1a2a3a4a5a6a8a9a0a1a2a3a4a5a6a8a9a0

aq1q2q3q4q5q6q7q8q9q0q1q2q3q4q5q6q7q9q0

Figure 1-44 Results of Comfort On-Screen Keyboard Lite

Figure 1-45 Captured Pressed Keys in Comfort On-Screen Keyboard Lite

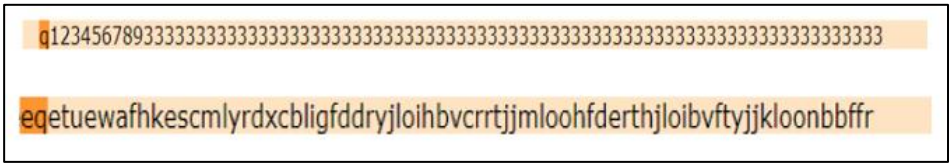

Figure 1-46 Results of Touch-It Virtual Keyboard

Figure 1-47 Screenshot Obtained from KidLogger showing Touch-It Virtual Keyboard

Figure 1-48 Usage of Neo's SafeKeys Marked within KidLogger

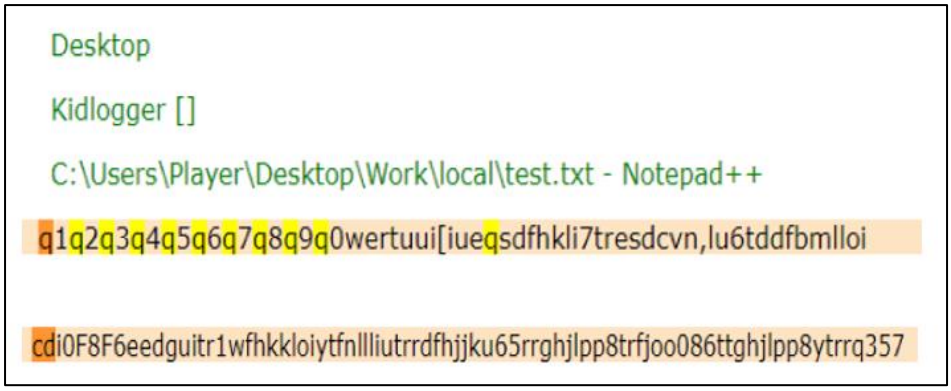

Figure 1-49 Results of Hot Virtual Keyboard

Best Free Keylogger:

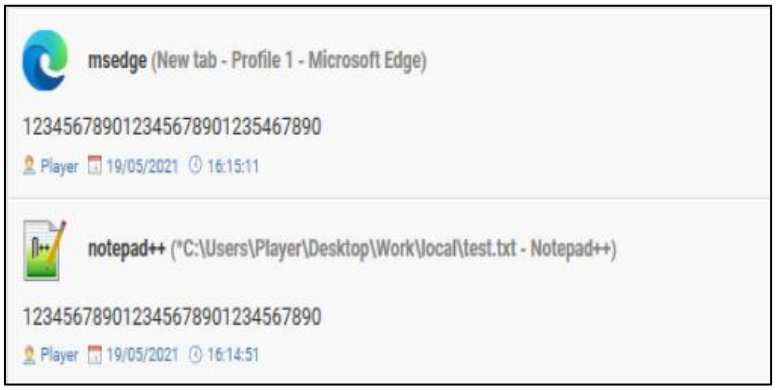

Figure 1-50 Results of Free Virtual Keyboard

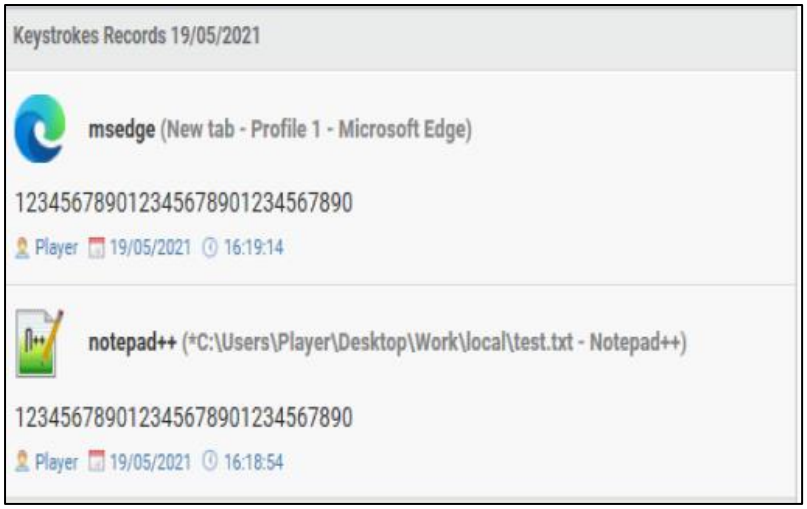

Figure 1-51 Results of Windows On-Screen Virtual Keyboard

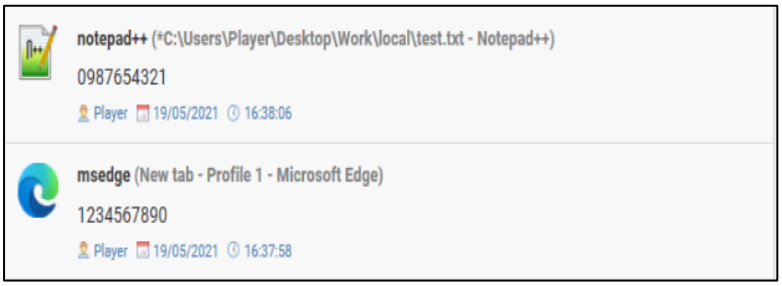

Figure 1-52 Results of Comfort On-Screen Virtual Keyboard

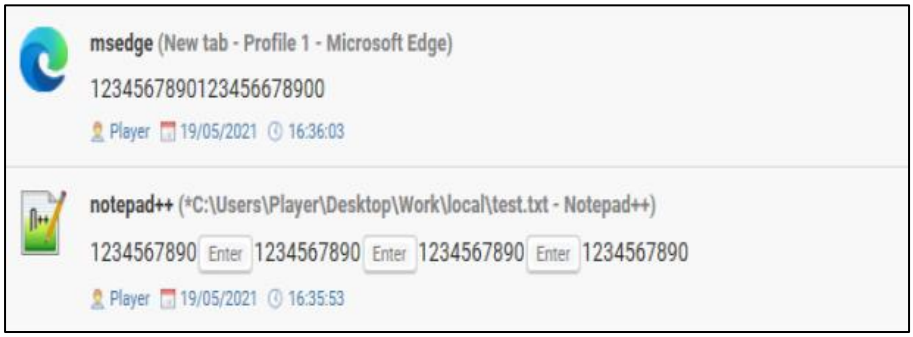

Figure 1-53 Results of Hot Virtual Keyboard

APPENDIX B – SETUP

Spyrix Keylogger Setup:

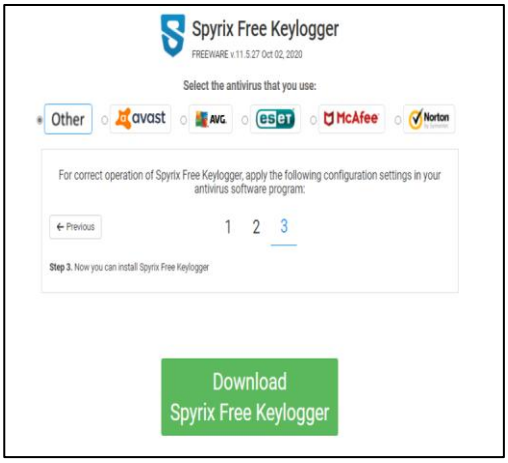

Figure 1-1 Installation of Spyrix Free Keylogger

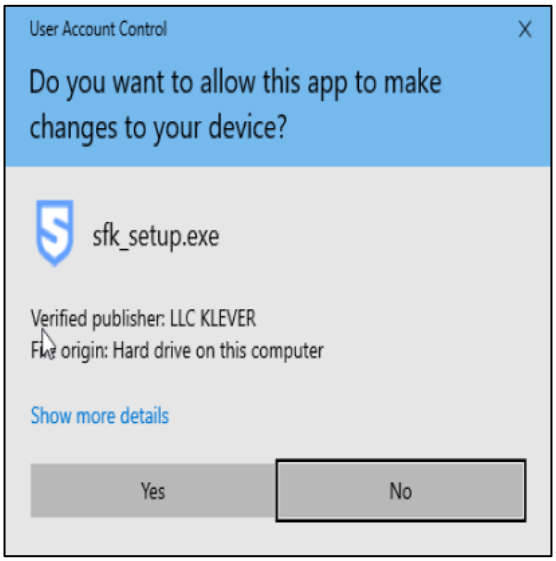

Figure 1-2 Spyrix Free Keylogger Setup Window

Figure 1-3 Spyrix Email Address Form

Actual Keylogger Setup:

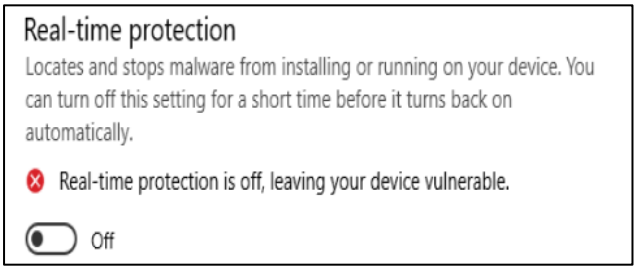

Figure 1-4 Disabling Anti-Virus Protection

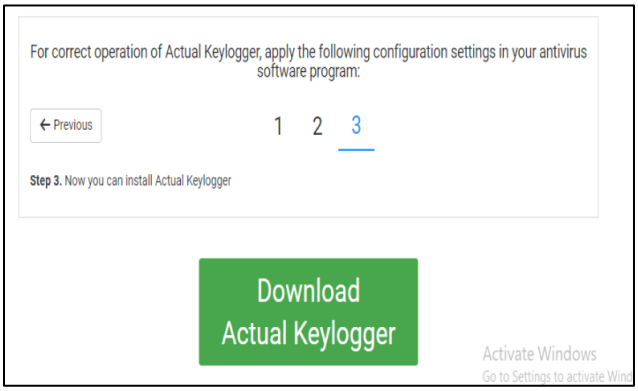

Figure 1-5 Download of Actual Keylogger

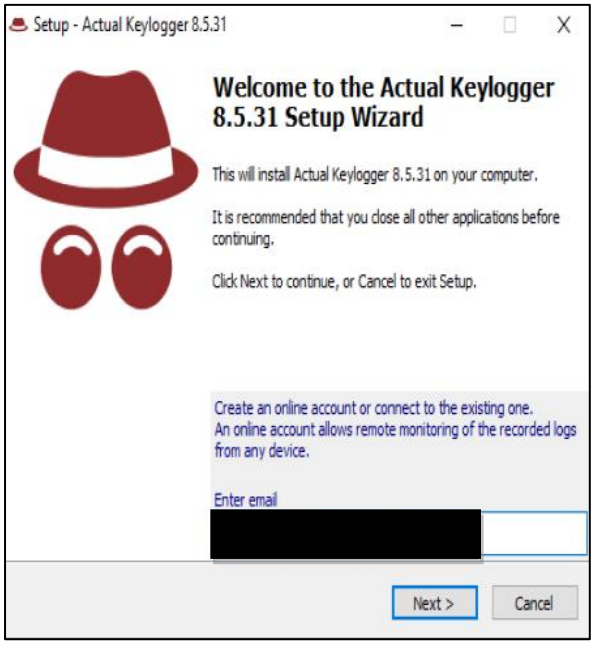

Figure 1-6 Actual Keylogger Form

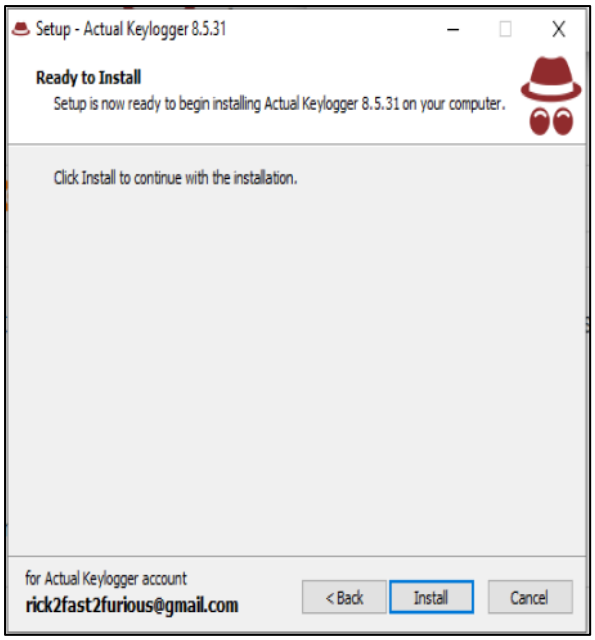

Figure 1-7 Confirmation of Install

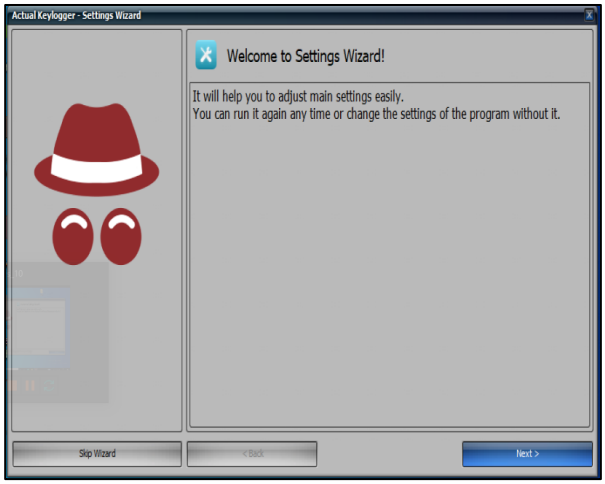

Figure 1-8 Actual Keylogger Settings Wizard

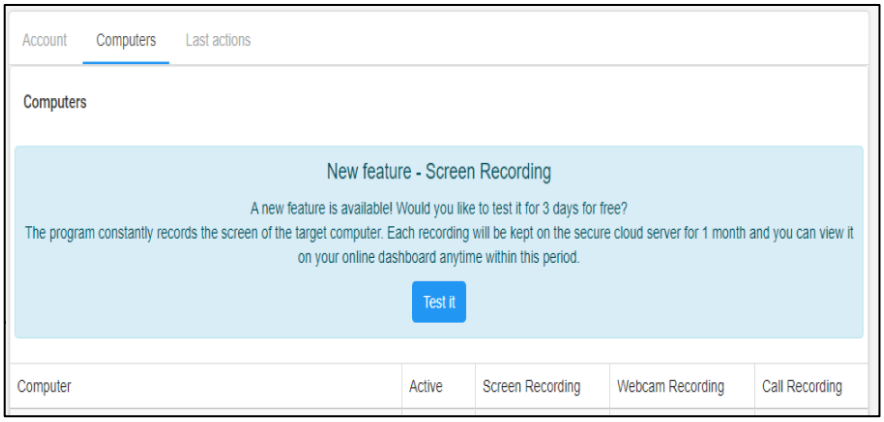

Figure 1-9 Remote Features

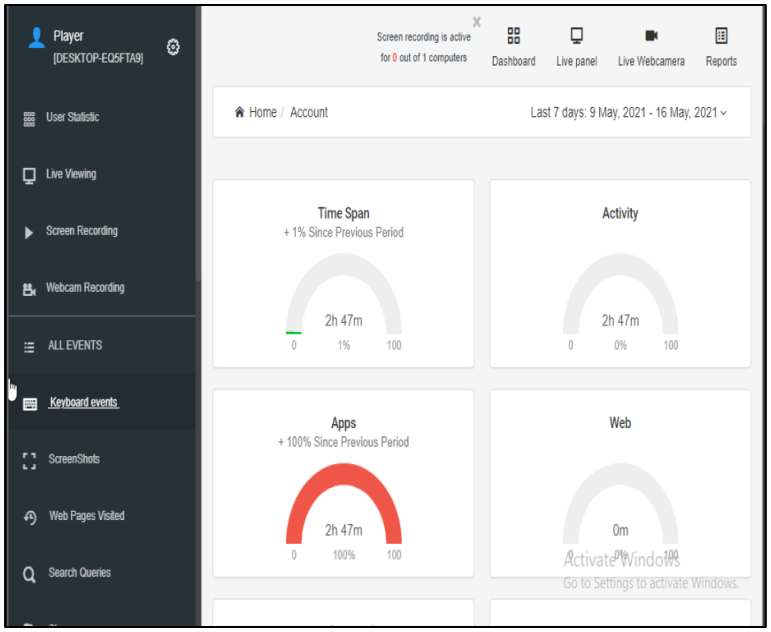

Figure 1-10 Remote Menu

Refog Personal Monitor Setup:

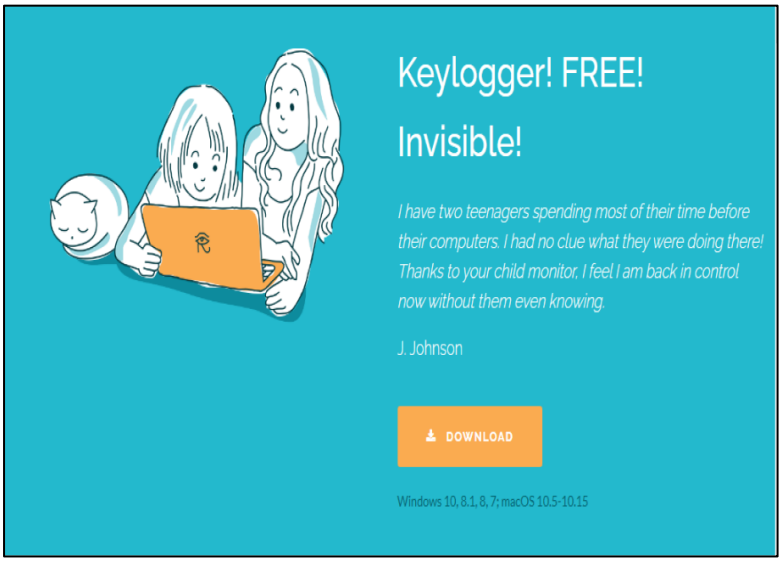

Figure 1-11 Refog Personal Monitor Homepage

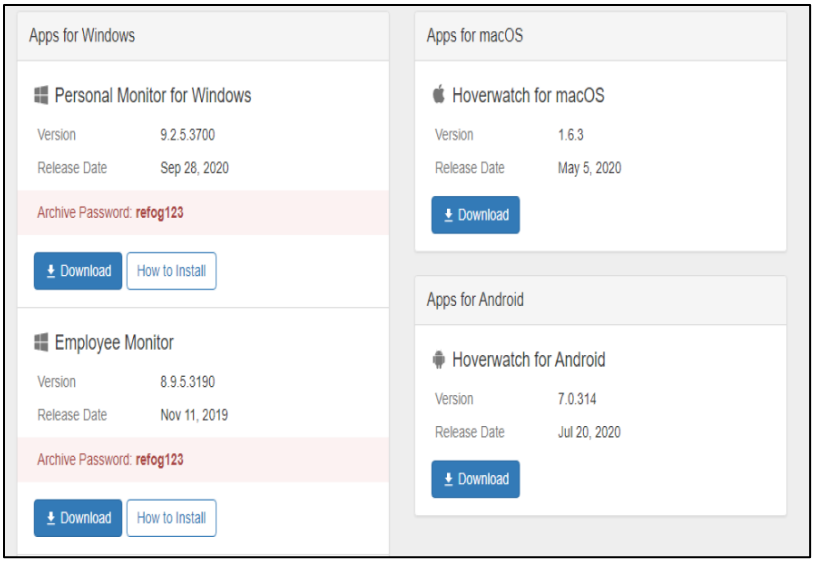

Figure 1-12 Download Options

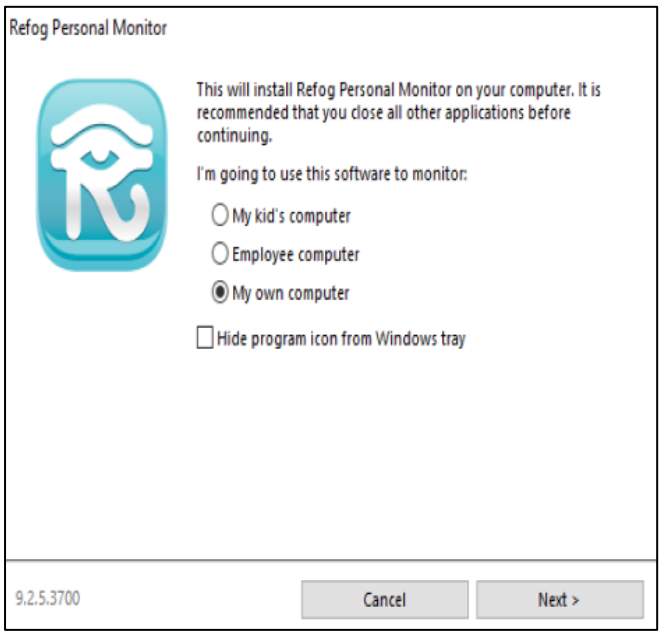

Figure 1-13 Specifying Usage of Personal Monitor

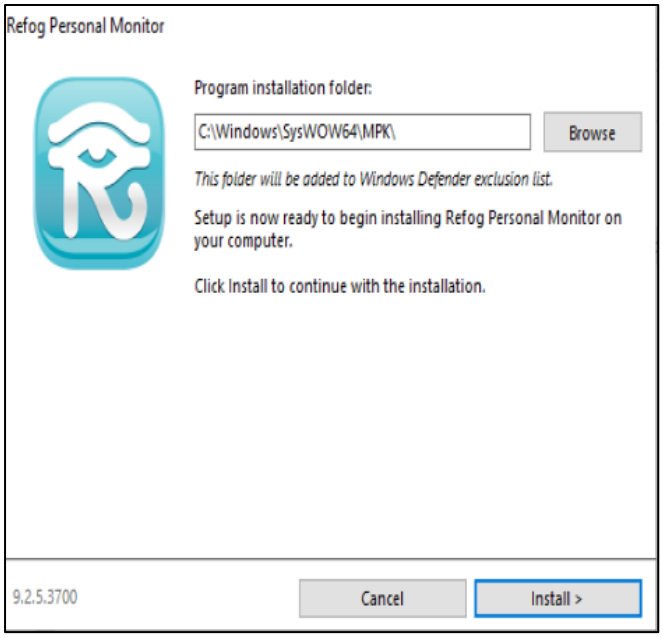

Figure 1-14 Installation Folder

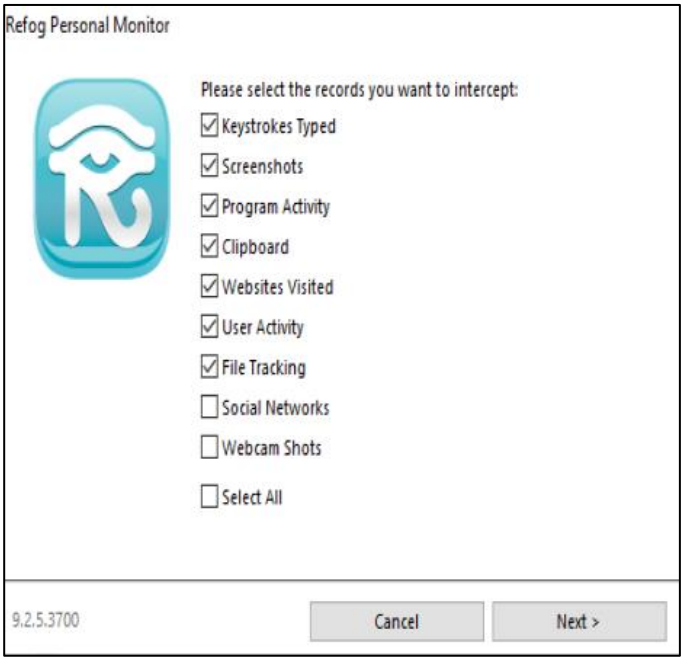

Figure 1-15 Selecting Methods for Data Collection in Refog Personal Monitor

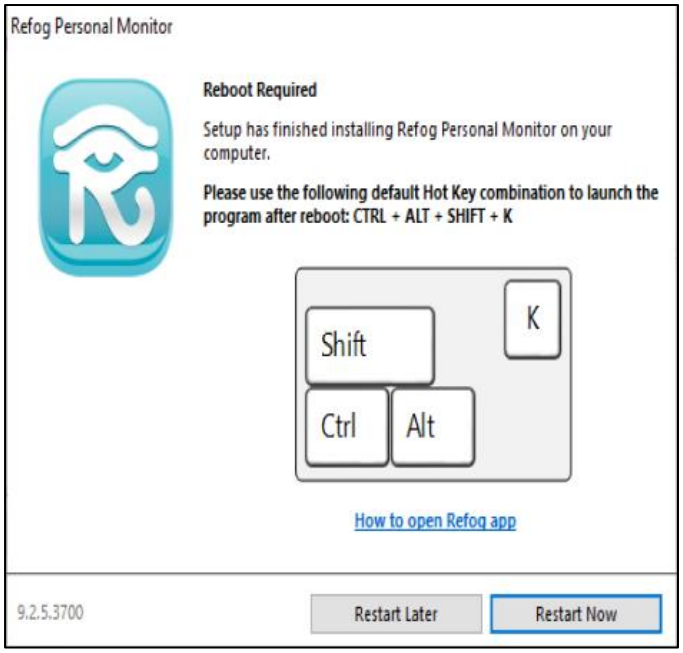

Figure 1-16 Instruction to Start Program

Iwantsoft Keylogger Setup:

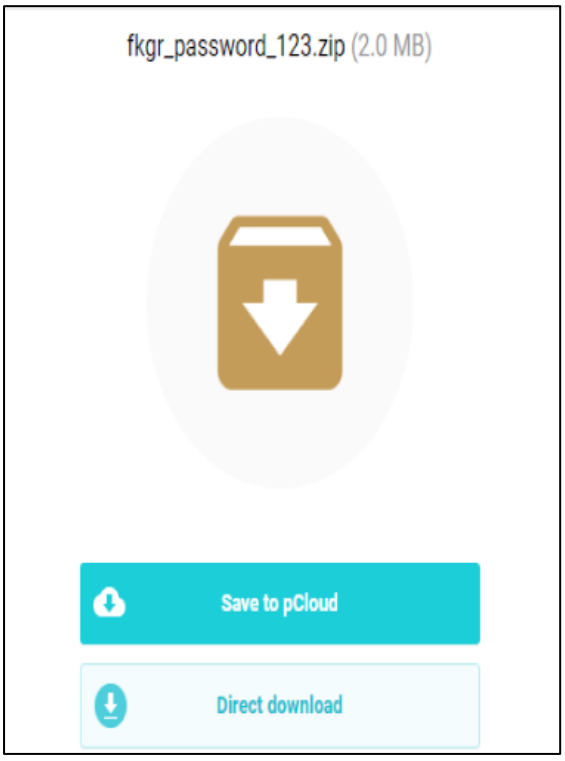

Figure 1-17 Downloading Iwantsoft Keylogger

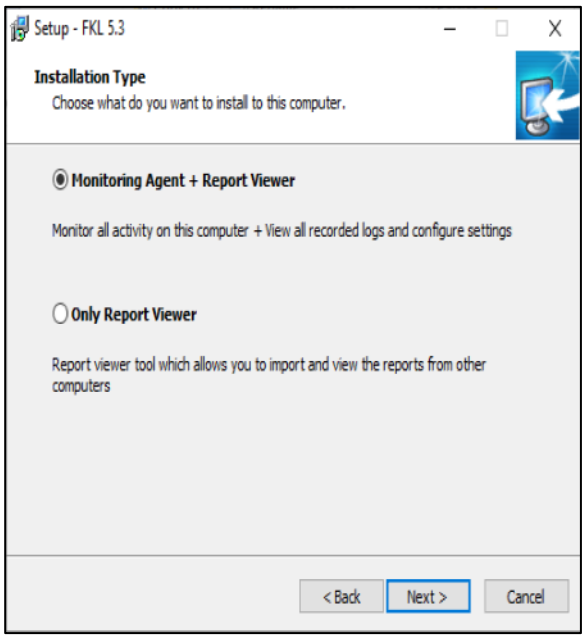

Figure 1-18 Installation Type (Monitoring Agent + Report Viewer)

Revealer Keylogger Setup:

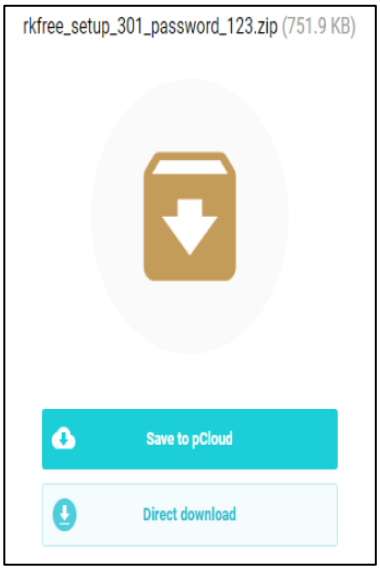

Figure 1-19 Revealer Keylogger Download

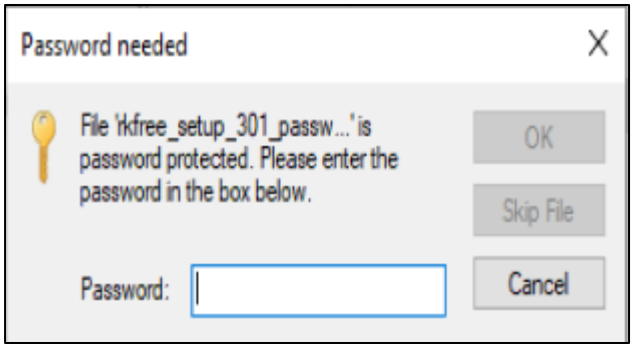

Figure 1-20 Password Protected Form

Figure 1-21 Install Screen

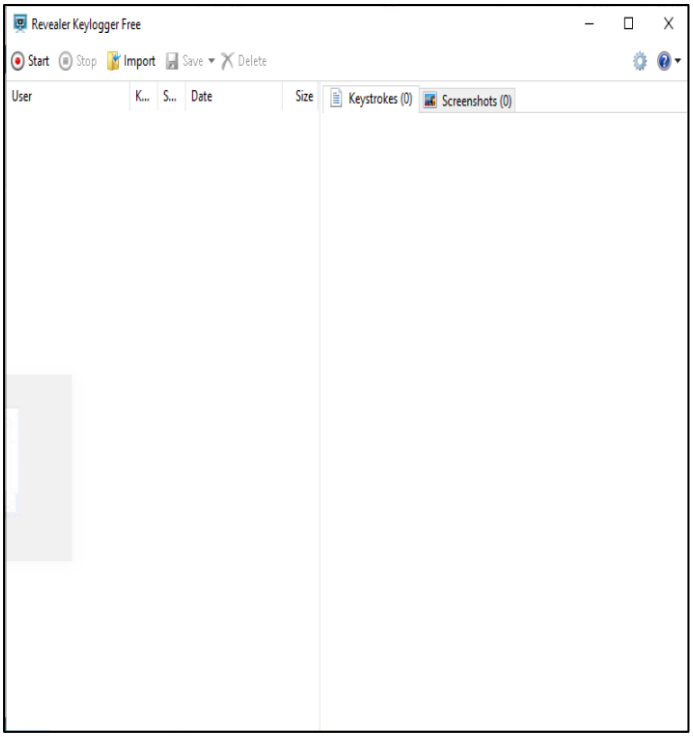

Figure 1-22 User Interface

KidLogger Setup:

Figure 1-23 Download for KidLogger Windows

Figure 1-24 KidLogger Setup Wizard

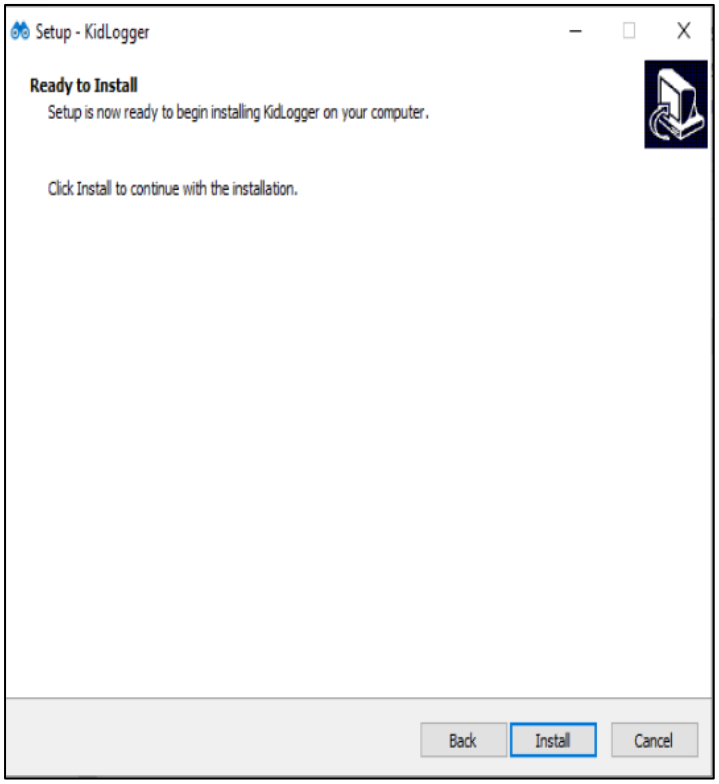

Figure 1-25 Install for KidLogger Windows

Best Free Keylogger Setup:

Figure 1-26 Download for Best Free Keylogger

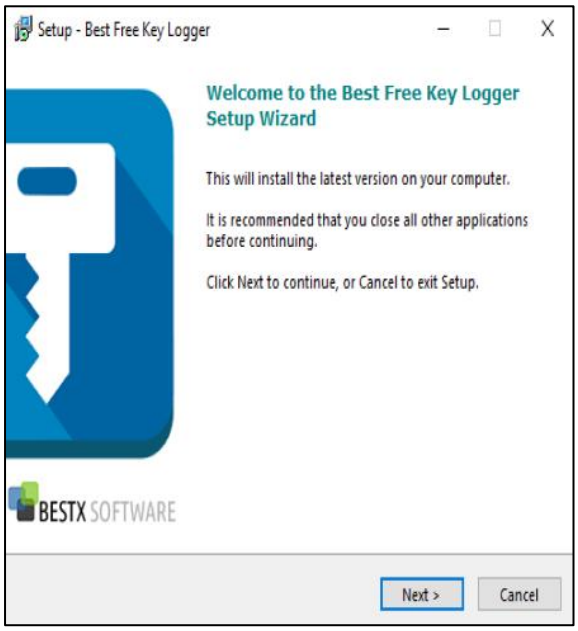

Figure 1-27 Best Free Keylogger Setup Wizard

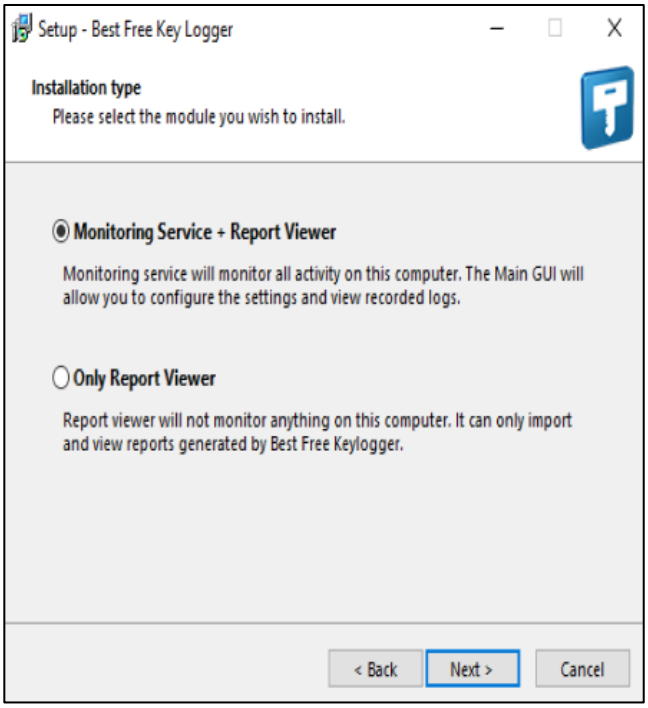

Figure 1-28 Setup Options

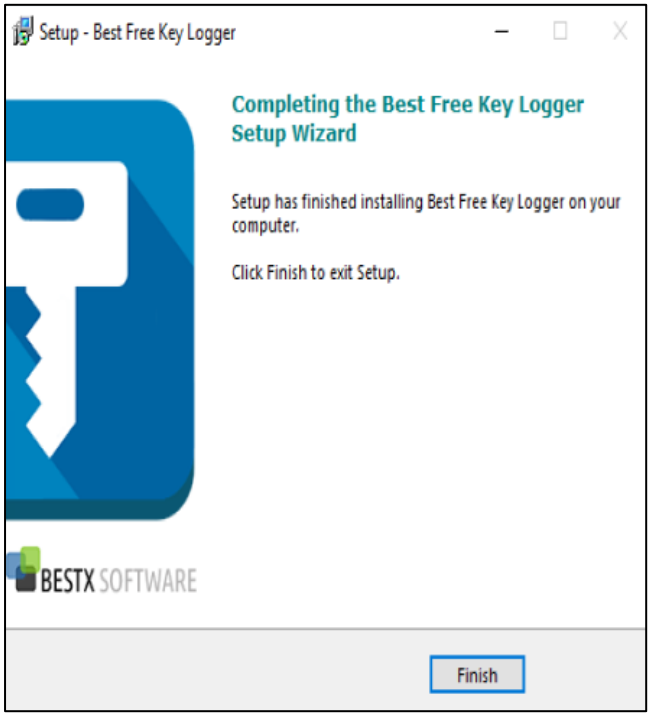

Figure 1-29 Finish Install

Figure 1-30 Verification of Install of Best Free Keylogger

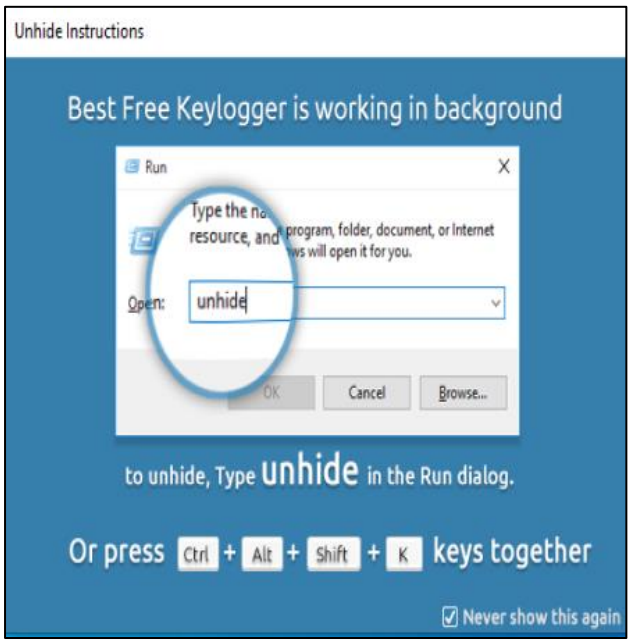

Figure 1-31 Unhide Instructions (Optional)

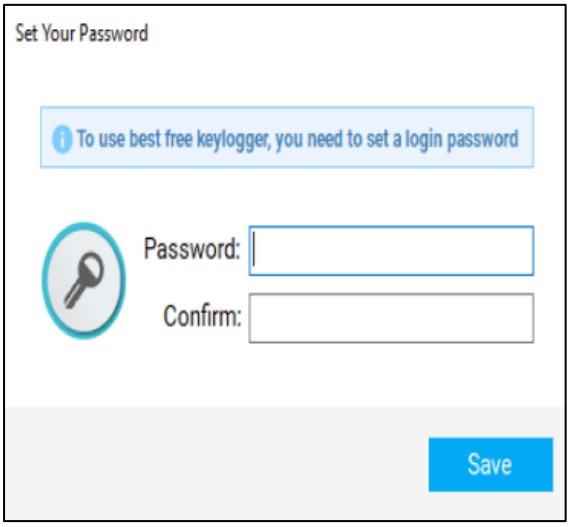

Figure 1-32 Setting a Password