**Refog or Spyrix or John the Ripper or Prey**

*By*

**Mehnaz Afrose**

**Report on Using Refog**

*A keylogger software*

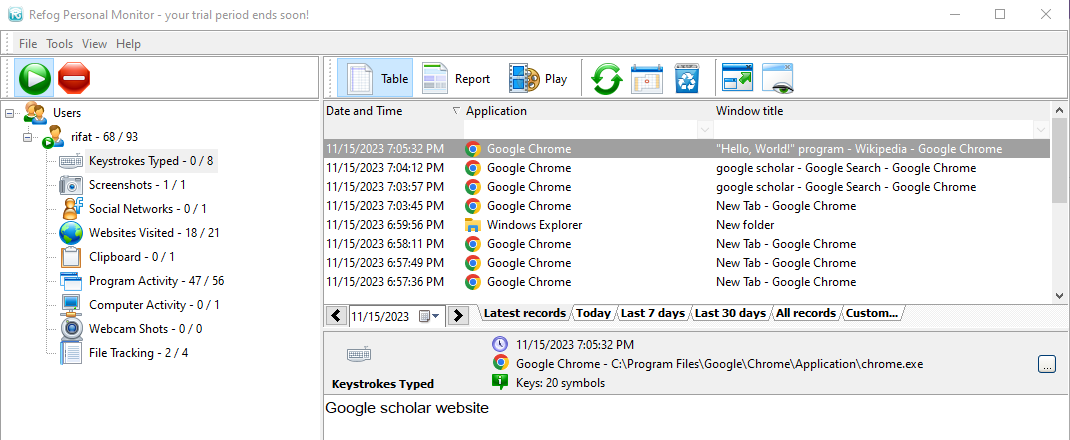
**Question 1: what did I do?**

At the very first step, I did some research about Refog and Spyrix software tools. Refog and Spyrex are both keylogger software tools. Keylogger tools are designed to track and capture keystrokes made on devices (Sukhram & Hayajneh, 2017). To know about how any keylogger works I found out that, once any keylogger installed in any device and run, it starts keeping records of every activity of all the keys pressed, including passwords, messages, websites visited, and other text entered. Then the user of this software can review this record log by logging in into the software account, or from the device itself (Tuli & Sahu, 2013). This tool can be used maliciously to steal personal data of any user by tracking down the inputs from the keyboard (Wood & Raj, 2010). Although it can be used in malicious activities, there is a significant use of beneficial deeds. These tools are used in identifying suspicious users, in forensic analysis of any cyber-attack, used by parents to monitor their children’s online activities to keep their kids safe, it can be used by office administration to track their employe behavior with proper consent, and so on (Kanwar, 2023).

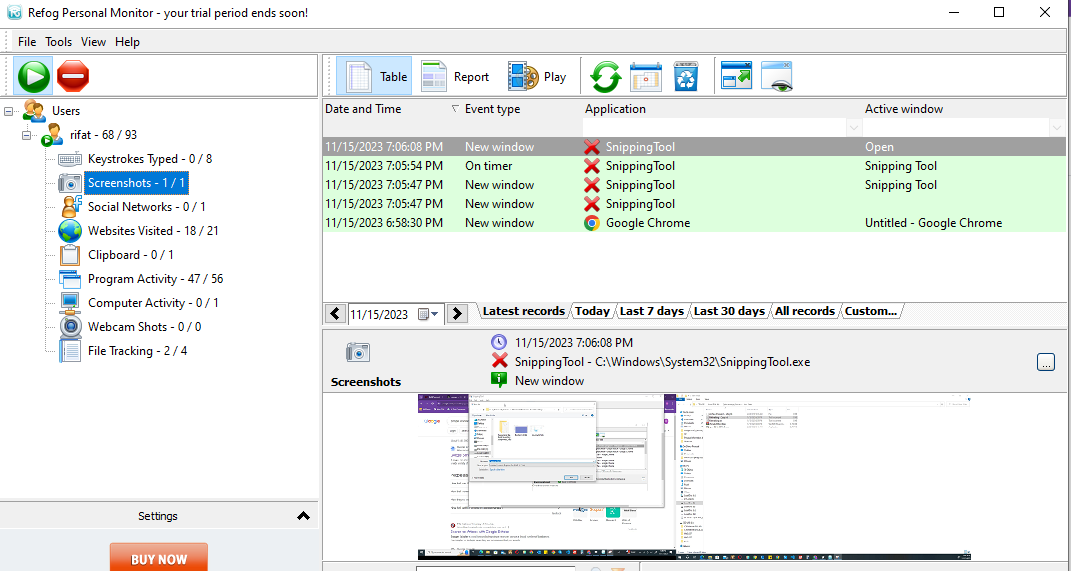
After knowing about keylogger software tools (in this case Refog and Spyrix), I watched two videos about how to use [Refog](https://www.youtube.com/watch?v=Y6KzM6Gj8n0&t=191s) and [Spyrix](https://www.youtube.com/watch?v=fxTb-I0X5WQ). Then I decided to use Refog keylogger. I went to the download link provided in WT class and downloaded the free version of this software. In the installation process I had to keep the real time protection off for my computer, otherwise it would detect Refog as a virus. Aftre the successful installation, I created an account for the online version. Also, I ran this software on my computer, started capturing every keystroke of my activity in this device.

**Question 2: What were the results?**

After capturing the keystrokes for almost ten minutes, I checked the resulting files. The first option was checking the keystrokes typed. I typed “Google scholarwebsite” to look for some research papers and Refog presented me with the exact result.

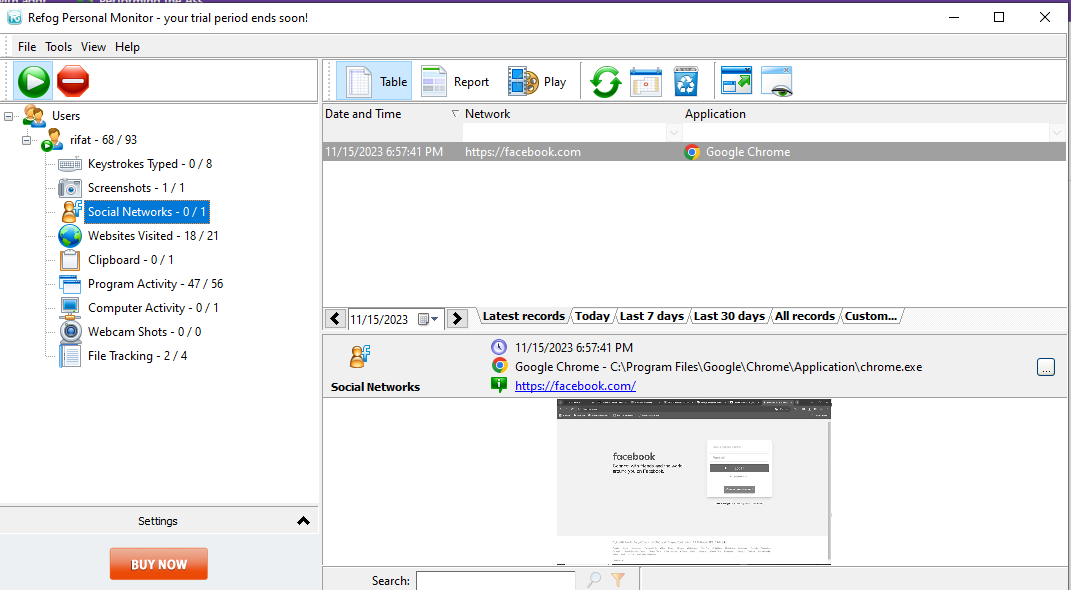
*Figure 1: Keystrokes Typed*

Then I checked which screenshot was taken from this computer. I used a sniping tool to capture screen shots. Refog showed me the result of what shots I took.



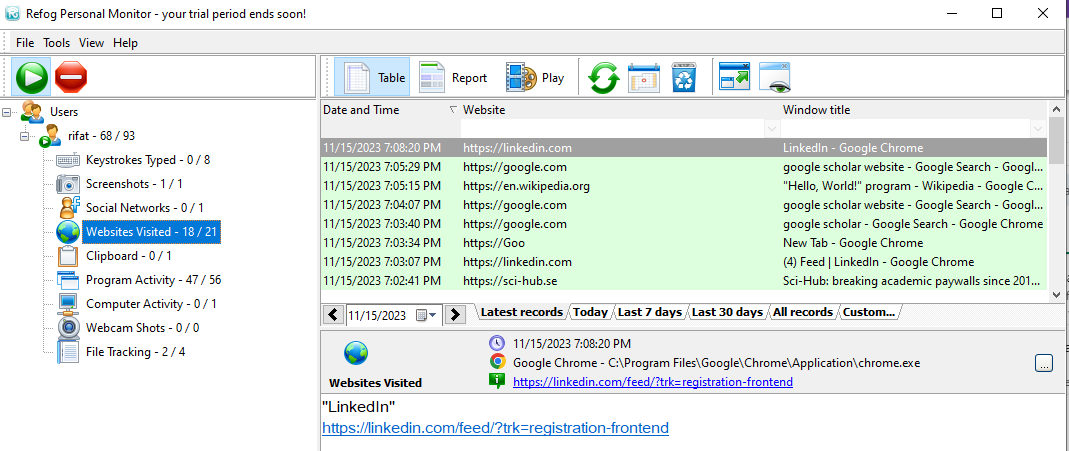
*Figure 2: Screenshot records*

In my browser, I browsed Facebook and LinkedIn. In the social network records, it only showed Facebook search. It can understand LinkedIn is not a social media platform. This feature of Refog of being able to identify and differentiate between key features of different webpages is amazing.



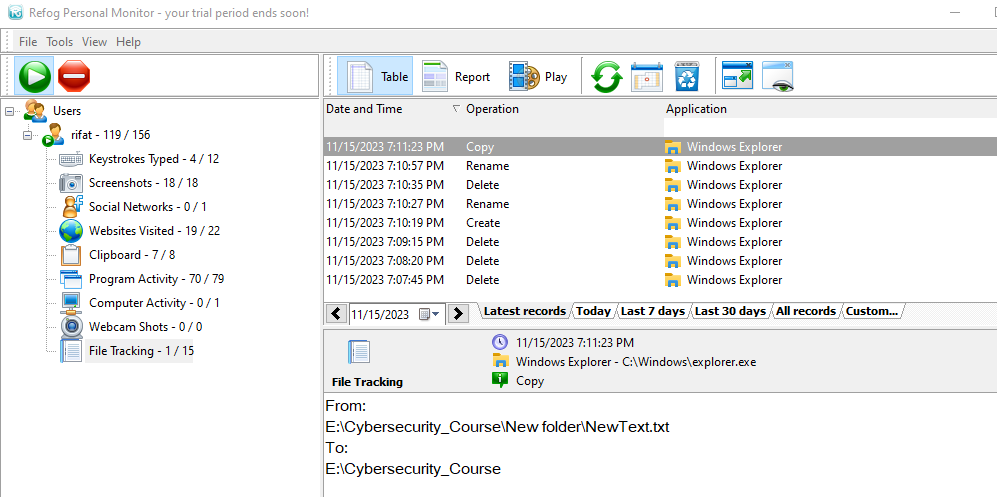
*Figure 3: Social Networks*

.



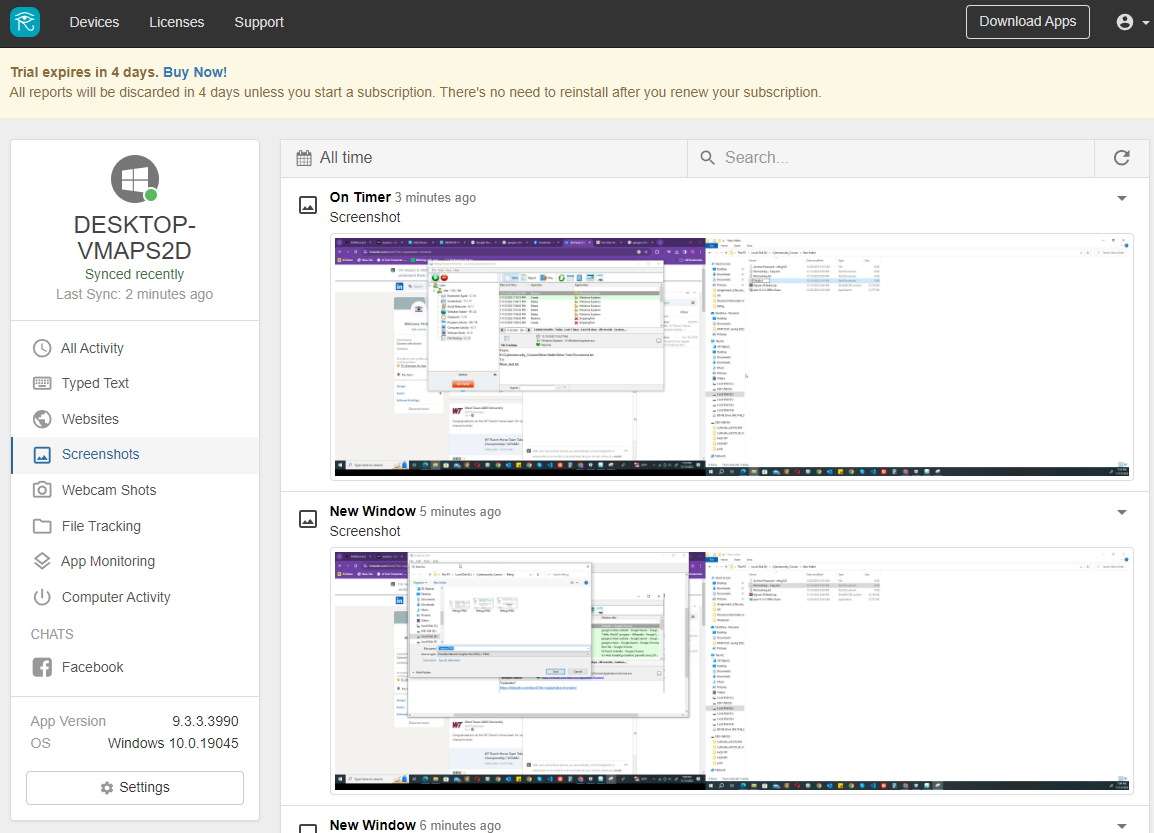
*Figure 4: Published LinkedIn in website visited section*

To examine that, if I create a new file, rename it, or copy the file, Refog can trace this action or not, I created a new text file, renamed it, copied it, and then deleted the file. Then I clicked the file tracking option of Refog. It showed the report of every action.



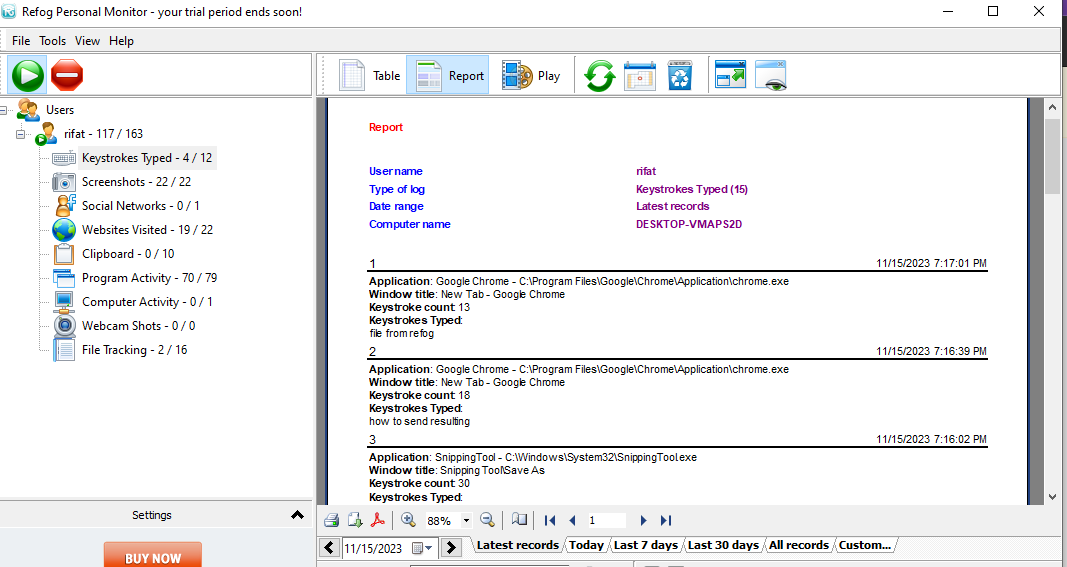
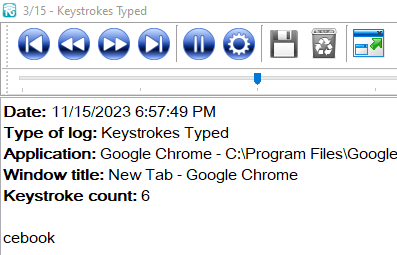
*Figure 5: File tracking*

Then I checked how the online monitoring was. I logged in with my email and password in the Refog profile. It showed the exact same results as from the application installed on the computer. That means I can monitor every keystroke far from the device by using an external browser.



*Figure 6: Monitoring with external browser*

Refog can create an elaborate report of every activity done in this device. It also presents the report with video slides.

*Figure 7: Report Figure 8: Slideshow presentation*

**Question 3: what did I learn?**

Keylogger tolls, in this case Refog, can be a Highly beneficial tool to monitor keystrokes made by user in any specific device. It has some amazing functions, such as a detailed report with each activity, which time the activity was done. It can be a great tool to keep children safe from malicious consequences of online use by monitoring their activity. But it can cause devastating consequences if used with deliberate malice.

**Report on John the Ripper**

*A password cracking software*

**Question 1: what did I do?**

I researched John the Ripper and came to know that this software is a tool to crack passwords offline and developed by Openwall project in 1996 ([How to use the John the Ripper password cracker](https://www.techtarget.com/searchsecurity/tutorial/How-to-use-the-John-the-Ripper-password-cracker#:~:text=John%20the%20Ripper%20is%20an,long%20list%20of%20password%20formats.)). Someone says the name “John the Ripper” came from another hacking tool called Jack The Cracker, or Cracker Jack, and someone says this name is a reference to the infamous serial killer Jack the Ripper and conveys the idea of "ripping" or breaking passwords ([Hacking Tools: John The Ripper](https://systemweakness.com/hacking-tools-john-the-ripper-806a196e3af5)).

How John the Ripper works: It cracks the passwords using a systematic guessing, such as trying the combination of familiar words, combination characters, or precomputed tables of hashed passwords to match against encrypted passwords ([John the Ripper explained: An essential password cracker for your hacker toolkit](https://www.csoonline.com/article/569533/john-the-ripper-explained-an-essential-password-cracker-for-your-hacker-toolkit.html)).

I watched some videos [How to install John The Ripper tool in Windows 10](https://www.youtube.com/watch?v=KBvBp5b3eCg) for installing John the Ripper, [how to hack WinZip or winrar password by using john the ripper in windows](https://www.youtube.com/watch?v=tkTgqW71r1U) , and [Password Cracking With John The Ripper](https://www.youtube.com/watch?v=XjVYl1Ts6XI) to know about how to crack a password.

Installation of John the Ripper:

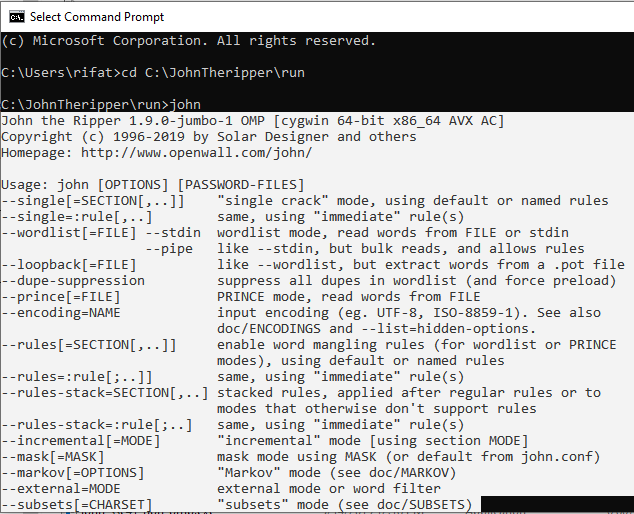
John the Ripper is advanced software. So, the installation process was very intricate. I needed to find the correct version for my computer first, then I installed it in the command prompt and modified the environmental variables path.

After the installation, I created a password protected zip file, whose password I was about to crack by John the Ripper.

After the first password cracking attempt, I created another password protected file with more complex password.

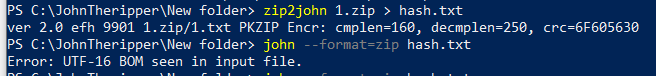
**Question 2: What were the results?**

Although the installation process was successful, the program “john” was not running in the command prompt. After several trials I closed the command prompt and tried to run the program using windows power shell. This time I was successful in running the program. Then I again tried to run it using command prompt, and after several attempts I was successful.



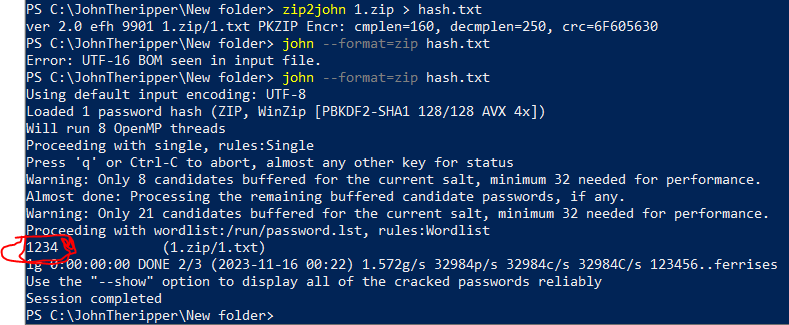
*Figure 9: Successfully run “john”*

After running “john” I tried to crack the password of my previously created password protected file 1.zip. I used “zip2john” tool for this purpose. After running the command, I received a hash for the password in the output and saved that hash into a text file hash.txt. When I tried to run the final command “zip2john 1.zip > hash.txt” the output was showing error. After several trials, I closed the command prompt, and tried to run the process in windows power shell again. This time PowerShell was also showing an error message “ UTF-16 BOM seen in input file”.



*Figure 10: UTF version error*

Then I searched online how to change the version of UTF to run this command, found out that I needed the version of 8 instead of 16. I saved the hash.txt file int notepad++, there was the option to change the version from UTF-16 to UTF-8 and ran the process again. This time John the Ripper successfully cracked the password. I used a simple password so that it does not take exceedingly long time.



*Figure 11: Password cracking successful*

When I tried another password protected file with a more complex password, this time it was showing the same error as the hash.txt version. Again, I changed the version in the same way. But this time it was not working.



*Figure 12: Password cracking unsuccessful*

**Question 3: what did I learn?**

First, John the Ripper is an advanced tool to use. From the very root step finding the perfect version to the end step utilizing the software to achieve desired result was a very prolific and rewarding. I got the chance to know how to solve different errors step by step, which proved to be incredibly enlightening and empowering.

By using John the Ripper, I gained insights into the vulnerabilities of weak passwords. It provides the understanding that how easily certain passwords can be cracked using different techniques like dictionary attacks or brute force methods. We can understand the importance of using strong and complicated passwords. The more complex the password, the longer it takes to crack.

**Report on Prey**

*A tracking software*

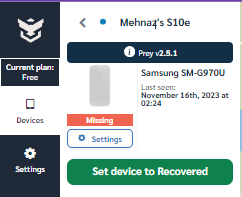
**Question 1: what did I do?**

I looked on the internet to know about “Prey.” "Prey" is a tracking and security software designed to help recover lost or stolen devices. It allows users to remotely track and locate their devices, such as laptops, smartphones, or tablets, if they are lost or stolen ([Overview: What is Prey and How Can it Help You?](https://help.preyproject.com/article/185-overview-what-is-prey#:~:text=Prey%20is%20a%20cross%2Dplatform,device%20(except%20for%20iOS.))) I also came to know about how it works. Prey works by sending signals or reports to a control panel, usually accessed through a web interface or another device, providing information on the device's location, network details, and sometimes even photos taken from the device's camera. This information assists in recovering the device or aiding law enforcement in locating it. Additionally, Prey may offer options to remotely lock the device, wipe sensitive data, or trigger alarms to prevent unauthorized access ([Your mobile security kit](https://preyproject.com/how-it-works#:~:text=Reacting%20to%20theft%20or%20loss&text=Prey%20will%20track%20and%20get%20Missing%20Reports%20to%20help%20retrieve%20it.&text=Use%20Prey's%20Missing%20Reports%2C%20with,a%20recovery%20with%20the%20police!)).

After gathering all the information about Prey, I installed the android version on my mobile phone and created a prey account. To understand how this antitheft software works I set my device status “missing” and changed the settings to provide me the missing report in every two minutes.

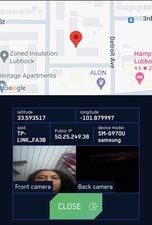
**Question 2: What were the results?**

When I installed Prey, I changed the device status to "missing.”



*Figure 13: Device is missing*

Within a couple of seconds, the front camera took a picture and sent the location of the device with the picture it took.



*Figure 14: First report with picture and location*

After two minutes it sent another descriptive report, which included pictures from both front camera and back camera, Wi-Fi router signals from nearby areas of the device which it can captured, location map, and so on. It was sending missing reports every two minutes unless I logged on into the account and marked the device “recovered.” After that it sent the final email report claiming that the device had been recovered.

**Question 3: what did I learn?**

I learnt from this assignment that “Prey” is an extremely useful antitheft software application, by which I can recover my smart devices from hidden/stolen condition. If I had known about this application earlier, I would have been able to recover some valuable devices which had been missing a couple of months ago.

Reference:

1. Sukhram, D., & Hayajneh, T. (2017). KeyStroke logs: Are strong passwords enough? In 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON) (pp. 619-625). New York, NY, USA. doi:10.1109/UEMCON.2017.8249051
2. Tuli, P., & Sahu, P. (2013). System monitoring and security using keylogger. International Journal of Computer Science and Mobile Computing, 2(3), 106-111.
3. Wood, C., & Raj, R. (2010, July). Keyloggers in Cybersecurity Education. In Security and Management (pp. 293-299).
4. Kanwar, A. K. (2023). An analysis of Key Logger.
5. [Refog Keylogger - Monitoring Software Tutorial](https://www.youtube.com/watch?v=Y6KzM6Gj8n0&t=191s)
6. [Spyrix Personal Monitor. Activity monitor. How it works](https://www.youtube.com/watch?v=fxTb-I0X5WQ)
7. [How to use the John the Ripper password cracker](https://www.techtarget.com/searchsecurity/tutorial/How-to-use-the-John-the-Ripper-password-cracker#:~:text=John%20the%20Ripper%20is%20an,long%20list%20of%20password%20formats.)
8. [Hacking Tools: John The Ripper](https://systemweakness.com/hacking-tools-john-the-ripper-806a196e3af5)
9. [John the Ripper explained: An essential password cracker for your hacker toolkit](https://www.csoonline.com/article/569533/john-the-ripper-explained-an-essential-password-cracker-for-your-hacker-toolkit.html)
10. [How to install John The Ripper tool in Windows 10](https://www.youtube.com/watch?v=KBvBp5b3eCg)
11. [how to hack WinZip or winrar password by using john the ripper in windows](https://www.youtube.com/watch?v=tkTgqW71r1U)
12. [Password Cracking With John The Ripper](https://www.youtube.com/watch?v=XjVYl1Ts6XI)
13. [Overview: What is Prey and How Can it Help You?](https://help.preyproject.com/article/185-overview-what-is-prey#:~:text=Prey%20is%20a%20cross%2Dplatform,device%20(except%20for%20iOS.))
14. [Your mobile security kit](https://preyproject.com/how-it-works#:~:text=Reacting%20to%20theft%20or%20loss&text=Prey%20will%20track%20and%20get%20Missing%20Reports%20to%20help%20retrieve%20it.&text=Use%20Prey's%20Missing%20Reports%2C%20with,a%20recovery%20with%20the%20police!)